NSFOCUS Firewall Series
System Log Messages Reference

Contents

AAA messages

This section contains AAA messages.

AAA_FAILURE

Message text	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA failed.
Variable fields	$1: AAA type. $2: AAA scheme. $3: Service. $4: Username.
Severity level	5
Example	AAA/5/AAA_FAILURE: -AAAType=AUTHOR-AAADomain=domain1-Service=login-UserName=cwf@system; AAA failed.
Explanation	An AAA request was rejected. The following are the common reasons: • No response was received from the server. • The username or password was incorrect. • The service type that the user applied for was incorrect.
Recommended action	**1.** Verify that the device is correctly connected to the server. **2.** Enter the correct username and password. **3.** Verify that the server settings are the same as the settings on the device. **4.** If the problem persists, contact NSFOCUS Support.

AAA_LAUNCH

Message text	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA launched.
Variable fields	$1: AAA type. $2: AAA scheme. $3: Service. $4: Username.
Severity level	6
Example	AAA/6/AAA_LAUNCH: -AAAType=AUTHEN-AAADomain=domain1-Service=login-UserName=cwf@system; AAA launched.
Explanation	An AAA request was received.
Recommended action	No action is required.

AAA_SUCCESS

Message text	-AAAType=[STRING]-AAADomain=[STRING]-Service=[STRING]-UserName=[STRING]; AAA succeeded.
Variable fields	$1: AAA type. $2: AAA scheme. $3: Service. $4: Username.
Severity level	6
Example	AAA/6/AAA_SUCCESS: -AAAType=AUTHOR-AAADomain=domain1-Service=login-UserName=cwf@system; AAA succeeded.
Explanation	An AAA request was accepted.
Recommended action	No action is required.

ACL messages

This section contains ACL messages.

ACL_ACCELERATE_NO_RES

Message text	Failed to accelerate [STRING] ACL [UINT32]. The resources are insufficient.
Variable fields	$1: ACL type. $2: ACL number.
Severity level	4
Example	ACL/4/ACL_ACCELERATE_NO_RES: Failed to accelerate IPv6 ACL 2001. The resources are insufficient.
Explanation	Hardware resources were insufficient for accelerating an ACL.
Recommended action	Delete some rules or disabled ACL acceleration for other ACLs to release hardware resources.

ACL_ACCELERATE_NONCONTIGUOUSMASK

Message text	Failed to accelerate ACL [UINT32]. ACL acceleration supports only contiguous wildcard masks.
Variable fields	$1: ACL number.
Severity level	4
Example	ACL/4/ACL_ACCELERATE_NONCONTIGUOUSMASK: Failed to accelerate ACL 2001. ACL acceleration supports only contiguous wildcard masks.
Explanation	ACL acceleration failed because rules containing noncontiguous wildcard masks exist in the ACL.
Recommended action	Check the ACL rules and delete the unsupported configuration.

ACL_ACCELERATE_NOT_SUPPORT

Message text	Failed to accelerate [STRING] ACL [UINT32]. The operation is not supported.
Variable fields	$1: ACL type. $2: ACL number.
Severity level	4
Example	ACL/4/ACL_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 ACL 2001. The operation is not supported.
Explanation	ACL acceleration failed because the system does not support ACL acceleration.
Recommended action	No action is required.

ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP

Message text	Failed to accelerate IPv6 ACL [UINT32]. ACL acceleration does not support the rules that contain the hop-by-hop keywords.
Variable fields	$1: ACL number.
Severity level	4
Example	ACL/4/ACL_ACCELERATE_NOT_SUPPORTHOPBYHOP: Failed to accelerate IPv6 ACL 2001. ACL acceleration does not support the rules that contain the hop-by-hop keywords.
Explanation	ACL acceleration failed for the IPv6 ACL because rules containing the **hop-by-hop** keyword exist in the ACL.
Recommended action	Check the ACL rules and delete the unsupported configuration.

ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG

Message text	Failed to accelerate IPv6 ACL [UINT32]. ACL acceleration does not support specifying multiple TCP flags in one rule.
Variable fields	$1: ACL number.
Severity level	4
Example	ACL/4/ACL_ACCELERATE_NOT_SUPPORTMULTITCPFLAG: Failed to accelerate IPv6 ACL 2001. ACL acceleration does not support specifying multiple TCP flags in one rule.
Explanation	ACL acceleration failed for the IPv6 ACL because rules containing multiple TCP flags exist in the ACL.
Recommended action	Check the ACL rules and delete the unsupported configuration.

ACL_ACCELERATE_UNK_ERR

Message text	Failed to accelerate [STRING] ACL [UINT32].
Variable fields	$1: ACL type. $2: ACL number.
Severity level	4
Example	ACL/4/ACL_ACCELERATE_UNK_ERR: Failed to accelerate IPv6 ACL 2001.
Explanation	ACL acceleration failed because of an unknown error.
Recommended action	No action is required.

ACL_DYNRULE_COMMENT

Message text	The comment of [STRING], which was generated dynamically, can't be added or deleted manually.
Variable fields	$1: Dynamic ACL rule information.
Severity level	6
Example	ACL/6/ACL_DYNRULE_COMMENT: The comment of IPv4 ACL 3000 rule 1, which was generated dynamically, can't be added or deleted manually.
Explanation	The comment of a dynamic ACL rule can't be added or deleted manually.
Recommended action	No action is required.

ACL_DYNRULE_MDF

Message text	[STRING], which was generated dynamically, was deleted or modified manually.
Variable fields	$1: Dynamic ACL rule information.
Severity level	5
Example	ACL/5/ACL_DYNRULE_MDF: IPv4 ACL 3000 rule 1, which was generated dynamically, was deleted or modified manually.
Explanation	A dynamic ACL rule was deleted or modified manually.
Recommended action	Make sure deleting or modifying the dynamic ACL rule does not affect ongoing services on the network.

ACL_IPV6_STATIS_INFO

Message text	IPv6 ACL [UINT32] [STRING] [UINT64] packet(s).
Variable fields	$1: ACL number. $2: ID and content of an IPv6 ACL rule. $3: Number of packets that matched the rule.
Severity level	6
Example	ACL/6/ACL_IPV6_STATIS_INFO: IPv6 ACL 2000 rule 0 permit source 1:1::/64 logging 1000 packet(s).
Explanation	The number of packets matching the IPv6 ACL rule changed.
Recommended action	No action is required.

ACL_NO_MEM

Message text	Failed to configure [STRING] ACL [UINT] due to lack of memory.
Variable fields	$1: ACL type. $2: ACL number.
Severity level	3
Example	ACL/3/ACL_NO_MEM: Failed to configure ACL 2001 due to lack of memory.
Explanation	Configuring the ACL failed because memory is insufficient.
Recommended action	Use the **`display memory-threshold`** command to check the memory usage.

ACL_RULE_REACH_MAXNUM

Message text	The maximum number of rules in [STRING] ACL [UNIT32] already reached.
Variable fields	$1: ACL type. $2: ACL number.
Severity level	5
Example	ACL/5/ACL_RULE_REACH_MAXNUM:The maximum number of rules in IPv4 ACL 3000 already reached.
Explanation	A dynamic ACL rule failed to be added because the maximum number of rules in the ACL already reached.
Recommended action	Delete unused ACL rules.

ACL_RULE_SUBID_EXCEED

Message text	The rule ID in [STRING] ACL [UNIT32] is out of range.
Variable fields	$1: ACL type. $2: ACL number.
Severity level	5
Example	ACL/5/ ACL_RULE_SUBID_EXCEED: The rule ID in IPv4 ACL 3000 is out of range.
Explanation	A dynamic ACL rule failed to be added because the rule ID is out of range.
Recommended action	Modify the rule numbering step for the ACL.

ACL_STATIS_INFO

Message text	ACL [UINT32] [STRING] [UINT64] packet(s).
Variable fields	$1: ACL number. $2: ID and content of an IPv4 ACL rule. $3: Number of packets that matched the rule.
Severity level	6
Example	ACL/6/ACL_STATIS_INFO: ACL 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
Explanation	The number of packets matching the IPv4 ACL rule changed.
Recommended action	No action is required.

ADVPN messages

This section contains ADVPN messages.

ADVPN_SESSION_DELETED

Message text	An ADVPN tunnel was deleted: tunnel interface=[STRING], private addr=[STRING], public addr=[STRING], peer private addr=[STRING], peer public addr=[STRING], type=[STRING], last state=[STRING], last state duration=[STRING], domain name=[STRING], ADVPN group name=[STRING].
Variable fields	$1: Tunnel interface name. $2: Private address of the ADVPN tunnel. $3: Public address of the ADVPN tunnel. $4: Peer private address of the ADVPN tunnel. $5: Peer public address of the ADVPN tunnel. $6: ADVPN tunnel type. $7: Last state of the ADVPN tunnel. $8: Duration for the last state of the ADVPN tunnel, in the format of xH yM zS. $9: ADVPN domain name. $10: ADVPN group name.
Severity level	4
Example	ADVPN/4/ADVPN_SESSION_DELETED: An ADVPN tunnel was deleted: tunnel interface=888, private addr=112.168.60.56, public addr=192.168.60.137,peer private addr=112.168.60.18, peer public addr=192.168.60.11,type=Spoke-Hub, last state=Success, last state duration=0H 8M 8S,domain name=abc, ADVPN group name=
Explanation	An ADVPN tunnel was deleted.
Recommended action	Check the network connectivity and configuration.

ADVPN_SESSION_STATE_CHANGED

Message text	ADVPN tunnel state changed from [STRING] to [STRING]: tunnel interface=[STRING], private addr=[STRING], public addr=[STRING], peer private addr=[STRING], peer public addr=[STRING], type=[STRING], last state=[STRING], last state duration=[STRING], domain name=[STRING], ADVPN group name=[STRING].
Variable fields	$1: Original state of the ADVPN tunnel. $2: New state of the ADVPN tunnel. $3: Tunnel interface name. $4: Private address of the ADVPN tunnel. $5: Public address of the ADVPN tunnel. $6: Peer private address of the ADVPN tunnel. $7: Peer public address of the ADVPN tunnel. $8: ADVPN tunnel type. $9: Last state of the ADVPN tunnel. $10: Duration for the last state of the ADVPN tunnel, in the format of xH yM zS. $11: ADVPN domain name. $12: ADVPN group name.
Severity level	4
Example	ADVPN/4/ADVPN_SESSION_STATE_CHANGED: ADVPN tunnel state changed from Establishing to Success: tunnel interface=888, private addr=112.168.60.56, public addr=192.168.60.137,peer private addr=112.168.60.18, peer public addr=192.168.60.11,type=Spoke-Hub, last state=Establishing, last state duration=0H 0M 5S,domain name=abc, ADVPN group name=
Explanation	The state of an ADVPN tunnel was changed.
Recommended action	Check the network connectivity and configuration.

AFT

This section contains AFT messages.

AFT_V4TOV6_FLOW

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];AFTSrcIPv6Addr(1005)=[IPADDR];AFTSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];AFTDstIPv6Addr(1009)=[IPADDR];AFTDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];SrcVPNInstance(1042)=[STRING];DstVPNInstance(1043)=[STRING];BeginTime(1013)=[STRING];EndTime(1014)=[STRING];Event(1048)=[STRING].
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Source IPv4 address. $4: Source port number. $5: Source IPv6 address after AFT translation. $6: Source port number after AFT translation. $7: Destination IPv4 address. $8: Destination port number. $9: Destination IPv6 address after AFT translation. $10: Destination port number after AFT translation. $11: Total number of incoming packets. $12: Total number of incoming bytes. $13: Total number of outgoing packets. $14: Total number of outgoing bytes. $15: Source VPN instance name. $16: Destination VPN instance name. $17: Time when the session was created. $18: Time when the session was removed. $19: Event description: o Session created. o Session deleted.
Severity level	6
Example	aft/6/AFT_V4TOV6_FLOW: Protocol(1001)=UDP;Application(1002)=sip;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;AFTSrcIPv6Addr(1005)=100::1;AFTSrcPort(1006)=1024;DstIPAddr(1007)=20.20.20.1;DstPort(1008)=21;AFTDstIPv6Addr(1009)=100::1414:1401;AFTDstPort(1010)=21;InitPktCount(1044)=1;InitByteCount(1046)=50;RplyPktCount(1045)=0;RplyByteCount(1047)=0;SrcVPNInstance(1042)=;DstVPNInstance(1043)=;BeginTime(1013)=03182024082546;EndTime(1014)=;Event(1048)=Session created.
Explanation	This message is sent when an IPv4-initiated session is created or removed.
Recommended action	No action is required.

AFT_V6TOV4_FLOW

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];AFTSrcIPAddr(1005)=[IPADDR];AFTSrcPort(1006)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];AFTDstIPAddr(1009)=[IPADDR];AFTDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];SrcVPNInstance(1042)=[STRING];DstVPNInstance(1043)=[STRING];BeginTime(1013)=[STRING];EndTime(1014)=[STRING];Event(1048)=[STRING].
Variable fields	$1: Protocol type. $2: Application protocol name. $2: Source IPv6 address. $3: Source port number. $4: Source IPv4 address after AFT translation. $5: Source port number after AFT translation. $6: Destination IPv6 address. $7: Destination port number. $8: Destination IPv4 address after AFT translation. $9: Destination port number after AFT translation. $10: Total number of incoming packets. $11: Total number of incoming bytes. $12: Total number of outgoing packets. $13: Total number of outgoing bytes. $14: Source VPN instance name. $15: Destination VPN instance name. $16: Time when the session was created. $17: Time when the session was removed. $18: Event description: o Session created. o Session deleted.
Severity level	6
Example	aft/6/AFT_V6TOV4_FLOW: Protocol(1001)=TCP;Application(1002)=general_tcp;SrcIPv6Addr(1036)=100::c613:102;SrcPort(1004)=1024;AFTSrcIPAddr(1005)=101.1.1.14;AFTIPSrcPort(1006)=1025;DstIPv6Addr(1037)=100::6;DstPort(1008)=1025;AFTDstIPAddr(1009)=101.1.1.1;AFTDstPort(1010)=1025;InitPktCount(1044)=1;InitByteCount(1046)=110;RplyPktCount(1047)=0;RplyByteCount(1047)=0;SrcVPNInstance(1042)=;DstVPNInstance(1043)=;BeginTime(1013)=03182024082901;EndTime(1014)=;Event(1048)=Session created.
Explanation	This message is sent when an IPv6-initiated session is created or removed.
Recommended action	No action is required.

ANCP messages

This section contains ANCP messages.

ANCP_INVALID_PACKET

Message text	-NeighborName=[STRING]-State=[STRING]-MessageType=[STRING]; The [STRING] value [STRING] is wrong, and the value [STRING] is expected.
Variable fields	$1: ANCP neighbor name. $2: Neighbor state. $3: Message type. $4: Field. $5: Wrong value of the field. $6: Expected value of the field.
Severity level	6
Example	ANCP/6/ANCP_INVALID_PACKET: -NeighborName=Dslam-State=SYNSENT-MessageType=SYNACK; The Sender Instance value 0 is wrong, and the value 1 is expected.
Explanation	The system received an adjacency message that had a field with a wrong value.
Recommended action	No action is required.

ANTIVIRUS messages

This section contains antivirus messages.

ANTIVIRUS_IPV4_INTERZONE

Message text	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPAddr(1003)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; VirusName(1085)=[STRING]; VirusID(1086)=[UINT32]; VirusCategory(1182)=[STRING]; Severity(1087)=[STRING]; MD5(1129)=[STRING]; Action(1053)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; FileName(1097)=[STRING]; FileType(1096)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; RealSrcMacAddr(1204)=[STRING]; RealDstMacAddr(1205)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application layer protocol name. $3: Source IPv4 address. $4: Source port number. $5: Destination IPv4 address. $6: Destination port number. $7: Receiving VPN instance. $8: Source security zone name. $9: Destination security zone name. $10: Username. $11: Policy name. $12: Virus name. $13: Virus ID. $14: Virus category. $15: Severity level: o LOW. o MEDIUM. o HIGH. o CRITICAL. $16: MD5 value. $17: Action: o Reset & Logging. o Permit & Logging. o Redirect & Logging. $18: Direction of matching packets: o original. o reply. $19: Actual source IPv4 address. $20: File name. $21: File type. $22: Source MAC address. $23: Destination MAC address. $24: Real source MAC address. (This field displays a value only when the MAC address learning through a Layer 3 device is enabled.) $25: Real destination MAC address. (This field displays a value only when the

	MAC address learning through a Layer 3 device is enabled.) $26: VLAN ID. $27: VXLAN ID. $28: Source location. $29: Destination location.
Severity level	4
Example	ANTI-VIR/4/ANTIVIRUS_IPV4_INTERZONE:-Context=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPAddr(1003)=100.10.10.40; SrcPort(1004)=56690; DstIPAddr(1007)=200.10.10.40; DstPort(1008)=80; RcvVPNInstance(1042)=; SrcZoneName(1025)=spf; DstZoneName(1035)=spf; UserName(1113)=abc; PolicyName(1079)=av; VirusName(1085)=MODIFIED-EICAR-Test-File; VirusID(1086)=95; VirusCategory(1182)=Worm; Severity(1087)=MEDIUM; MD5(1129)=d41d8cd98f00b204e9800998ecf8427e; Action(1053)=Reset & Logging; HitDirection(1115)=original; RealSrcIP(1100)=10.10.10.10,20.20.20.20; FileName(1097)=123.pptx; FileType(1096)=pptx; SrcMacAddr(1021)= 021a-c501-0001; DstMacAddr(1022)=741f-4a93-02ac; RealSrcMacAddr(1204)=; RealDstMacAddr(1205)=; VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is sent when an IPv4 packet matches a virus signature.
Recommended action	No action is required.

ANTIVIRUS_IPV6_INTERZONE

Message text	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=-[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; VirusName(1085)=[STRING]; VirusID(1086)=[UINT32]; VirusCategory(1182)=[STRING]; Severity(1087)=[STRING]; MD5(1129)=[STRING]; Action(1053)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; FileName(1097)=[STRING]; FileType(1096)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; RealSrcMacAddr(1204)=[STRING]; RealDstMacAddr(1205)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application layer protocol name. $3: Source IPv6 address. $4: Source port number. $5: Destination IPv6 address. $6: Destination port number. $7: Receiving VPN instance. $8: Source security zone name. $9: Destination security zone name. $10: Username. $11: Policy name. $12: Virus name. $13: Virus ID. $14: Virus category. $15: Severity level: o LOW. o MEDIUM. o HIGH. o CRITICAL. $16: MD5 value. $17: Action: o Reset & Logging. o Permit & Logging. o Redirect & Logging. $18: Direction of matching packets: o original. o reply. $19: Actual source IPv6 address. $20: File name. $21: File type. $22: Source MAC address. $23: Destination MAC address. $24: Real source MAC address. (This field displays a value only when the MAC address learning through a Layer 3 device is enabled.) $25: Real destination MAC address. (This field displays a value only when the

	MAC address learning through a Layer 3 device is enabled.) $26: VLAN ID. $27: VXLAN ID. $28: Source location. $29: Destination location.
Severity level	4
Example	ANTI-VIR/4/ANTIVIRUS_IPV6_INTERZONE:-Context=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPv6Addr(1036)=100::40; SrcPort(1004)=56690; DstIPv6Addr(1037)=200::40; DstPort(1008)=80; RcvVPNInstance(1042)=; SrcZoneName(1025)=spf; DstZoneName(1035)=spf; UserName(1113)=aaa; PolicyName(1079)=av; VirusName(1085)=MODIFIED-EICAR-Test-File; VirusID(1086)=95; VirusCategory(1182)=Worm; Severity(1087)=MEDIUM; MD5(1129)=d41d8cd98f00b204e9800998ecf8427e; Action(1053)=Reset & Logging; HitDirection(1115)=original; RealSrcIP(1100)=10::1; FileName(1097)=123.pptx; FileType(1096)=pptx; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; RealSrcMacAddr(1204)=[STRING]; RealDstMacAddr(1205)=[STRING];VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is sent when an IPv6 packet matches a virus signature.
Recommended action	No action is required.

ANTIVIRUS_WARNING

Message text	Updated the antivirus signature library successfully.
Variable fields	N/A
Severity level	4
Example	ANTI-VIR/4/ANTIVIRUS_WARNING: -Context=1; Updated the antivirus signature library successfully.
Explanation	This message is sent when the antivirus signature library is immediately or locally updated.
Recommended action	No action is required.

ANTIVIRUS_WARNING

Message text	Rolled back the antivirus signature library successfully.
Variable fields	N/A
Severity level	4
Example	ANTI-VIR/4/ANTIVIRUS_WARNING: -Context=1; Rolled back the antivirus signature library successfully.
Explanation	This message is sent when the antivirus signature library is rolled back to the previous version or the factory version.
Recommended action	No action is required.

ANTIVIRUS_WARNING

Message text	Failed to update the antivirus signature library because no valid license was found for the antivirus feature.
Variable fields	N/A
Severity level	4
Example	ANTI-VIR/4/ANTIVIRUS_WARNING: -Context=1; Failed to update the antivirus signature library because no valid license was found for the antivirus feature.
Explanation	This message is sent when one of the following antivirus signature library upgrade failure occurs: • Web-based or CLI-based immediate upgrade failed because no valid license is found. • Web-based local upgrade failed because no valid license is found.
Recommended action	No action is required.

APMGR messages

This section contains access point management messages.

AP_CREATE_FAILURE

Message text	Failed to create an AP with entity ID [UINT32] and model [STRING]. Reason: Region code is not available.
Variable fields	$1: AP ID. $2: AP model.
Severity level	6
Example	APMGR/6/AP_CREATE_FAILURE: Failed to create an AP with entity ID 1 and model WA2620i-AGN. Reason: Region code is not available.
Explanation	The system fails to create an AP because the AP is not specified with a region code.
Recommended action	Specify a region code in global configuration view.

AP_REBOOT_REASON

Message text	AP in Run state is rebooting. Reason: The physical status of the radio is down.
Variable fields	N/A
Severity level	6
Example	APMGR/6/AP_REBOOT_REASON: AP in Run state is rebooting. Reason: The physical status of the radio is down.
Explanation	The AP is rebooting because a physical radio interface of the AP is in down state.
Recommended action	Verify that radio settings on the AP are correct after the reboot.

APMGR_ADDBAC_INFO

Message text	Add BAS AC [STRING].
Variable fields	$1: MAC address of the BAS AC.
Severity level	6
Example	APMGR/6/APMGR_ADDBAC_INFO: Add BAS AC 3ce5-a616-28cd.
Explanation	The BAS AC was connected to the master AC.
Recommended action	No action is required.

APMGR_AP_CFG_FAILED

Message text	Failed to reset AP [STRING]. Reason: The AP is writing an image file into the flash.
Variable fields	$1: AP name.
Severity level	4
Example	APMGR/4/APMGR_CFG_FAILD: Failed to reset AP ap2. Reason: The AP is writing an image file into the flash.
Explanation	AP reset failed because the AP is writing an image file into the flash.
Recommended action	Restart the AP after the AP finishes writing an image file into the flash.

APMGR_AP_ONLINE

Message text	The AP failed to come online in discovery stage. Reason: AP model [$1] is not supported.
Variable fields	$1: AP model.
Severity level	6
Example	APMGR/6/APMGR_AP_ONLINE: The AP failed to come online in discovery stage. Reason: AP model wa2620i-AGN is not supported.
Explanation	The AP fails to come online because its model is not supported by the AC and the AC cannot receive discovery requests from the AP.
Recommended action	No action is required.

APMGR_DELBAC_INFO

Message text	Delete BAS AC [STRING].
Variable fields	$1: MAC address of the BAS AC.
Severity level	6
Example	APMGR/6/APMGR_DELBAC_INFO: Delete BAS AC 3ce5-a616-28cd.
Explanation	The BAS AC was disconnected from the master AC.
Recommended action	No action is required.

APMGR_GET_AP_MODEL_FAILURE

Message text	Failed to get an AP model because no region code is configured globally or for AP group [STRING].
Variable fields	$1: AP group name.
Severity level	6
Example	APMGR/6/APMGR_GET_AP_MODEL_FAILURE: Failed to get an AP model because no region code is configured globally or for AP group g2.
Explanation	Failed to obtain the models of APs in an AP group because no region code is specified.
Recommended action	Specify a global region code or specify a region code for the AP group.

APMGR_LOG_ADD_AP_FAIL

Message text	AP [STRING] failed to come online using serial ID [STRING]: MAC address [STRING] is being used by AP [STRING].
Variable fields	$1: AP name. $2: Serial ID. $3: MAC address. $4: AP name.
Severity level	4
Example	APMGR/4/APMGR_LOG_ADD_AP_FAIL: AP ap1 failed to come online using serial ID 01247ef96: MAC address 0023-7961-5201 is being used by AP ap2.
Explanation	The AP failed to come online because a manual AP that has the same MAC address already exists on the AC.
Recommended action	Delete either the manual AP that has the MAC address or the serial ID.

APMGR_LOG_LACOFFLINE

Message text	Local AC [STRING] went offline. State changed to Idle.
Variable fields	$1: Name of the local AC.
Severity level	6
Example	APMGR/6/APMGR_LOG_LACOFFLINE: Local AC ac1 went offline. State changed to Idle.
Explanation	The local AC went offline. The state of the local AC changed to Idle.
Recommended action	**5.** If the local AC went offline abnormally, check the debugging information to locate the problem and resolve it. **6.** If the problem persists, contact NSFOCUS Support.

APMGR_LOG_LACONLINE

Message text	Local AC [STRING] went online. State changed to Run.
Variable fields	$1: Name of the local AC.
Severity level	6
Example	APMGR/6/APMGR_LOG_LACONLINE: Local AC ac1 went online. State changed to Run..
Explanation	The local AC came online. The state of the local AC changed to Run.
Recommended action	No action is required.

APMGR_LOG_MEMALERT

Message text	The memory usage of the AC has reached the threshold.
Variable fields	N/A
Severity level	4
Example	APMGR/4/APMGR_LOG_MEMALERT: The memory usage of the AC has reached the threshold.
Explanation	The AP failed to come online because the memory utilization exceeded the limit.
Recommended action	Stop creating manual APs and prevent APs from coming online.

APMGR_LOG_NOLICENSE

Message text	AP failed to come online in [STRING]. Reason: No license for the [STRING].
Variable fields	$1: AP state: • discover. • join. $2: AP type: • common AP. • WTU AP.
Severity level	6
Example	APMGR/6/APMGR_LOG_NOLICENSE: AP failed to come online in discover. Reason: No license for the common AP.
Explanation	The AP failed to come online because the number of APs allowed by the license on the AC has reached the upper limit.
Recommended action	Purchase an upgrade license for AP number extension.

APMGR_LOG_OFFLINE

Message text	AP [STRING] went offline. State changed to Idle.
Variable fields	$1: AP name.
Severity level	6
Example	APMGR/6/APMGR_LOG_OFFLINE: AP ap1 went offline. State changed to Idle.
Explanation	The AP went offline. The state of the AP changed to Idle.
Recommended action	If the AP went offline abnormally, check the debugging information to locate the problem and resolve it.

APMGR_LOG_ONLINE

Message text	AP [STRING] came online. State changed to Run.
Variable fields	$1: AP name.
Severity level	6
Example	APMGR/6/APMGR_LOG_ONLINE: AP ap1 came online. State changed to Run.
Explanation	The AP came online. The state of the AP changed to Run.
Recommended action	No action is required.

APMGR_LOG_ONLINE_FAILED

Message text	[STRING] ([STRING]) failed to come online in join state. Reason: [STRING] ([STRING]) was offline.
Variable fields	$1: Name of a WTU or WAP. $2: Serial ID of a WTU or WAP. $3: Name of the connected WT or SPM. $4: Serial ID of the connected WT or SPM.
Severity level	6
Example	• APMGR/6/APMGR_AP_ONLINE_FAILED: WTU (219801A0WA916BQ12535) failed to come online in join state. Reason: WT (219801A11UC173000153) was offline. • APMGR/6/APMGR_AP_ONLINE_FAILED: WAP (219801A0VW916AG00254) failed to come online in join state. Reason: SPM (219801A13DB05B0004350) was offline.
Explanation	• The WTU cannot come online because its connected WT is offline. • The WAP cannot come online because its connected SPM is offline.
Recommended action	Make the WT or SPM come online.

APMGR_REACH_MAX_APNUMBER

Message text	An AP failed to come online: Maximum number of APs already reached.
Variable fields	N/A
Severity level	4
Example	APMGR/4/APMGR_REACH_MAX_APNEMBER: An AP failed to come online: Maximum number of APs already reached.
Explanation	An AP failed to come online because the number of APs on the AC already reached the upper limit.
Recommended action	No action is required.

APMGR_ERROR

Message text	Failed to install WLAN feature package. Reason: Insufficient hardware resources.
Variable fields	N/A
Severity level	6
Example	APMGR/6/ERROR: Failed to install WLAN feature package. Reason: Insufficient hardware resources.
Explanation	The system failed to install the WLAN feature package because of insufficient hardware resources.
Recommended action	To resolve the problem: **7.** Uninstall the WLAN feature package. **8.** Locate the reason that causes hardware resource exhaustion and remove the issue. **9.** Reinstall the WLAN feature package. **10.** If the problem persists, contact NSFOCUS Support.

CWC_AP_DOWN

Message text	CAPWAP tunnel to AC [STRING] went down. Reason: [STRING].
Variable fields	$1: AC IP address. $2: Reason: • Added AP IP address. • Deleted AP IP address. • AP interface used for CAPWAP tunnel went down. • AP config changed. • AP was reset. • Number of echo retransmission attempts exceeded the limit. • No license for the AP. • Full retransmission queue. • Data channel timer expired. • Backup AC IP address changed. • Backup tunnel changed to master tunnel. • Failed to change backup tunnel to master tunnel. • Backup method changed. • N/A.
Severity level	6
Example	CWC/6/CWC_AP_DOWN: CAPWAP tunnel to AC 192.168.10.1 went down. Reason: AP was reset.
Explanation	The CAPWAP tunnel between the AP and the AC was terminated for a specific reason.
Recommended action	Examine the network connection between the AP and the AC.

CWC_AP_UP

Message text	[STRING] CAPWAP tunnel to AC [STRING] went up.
Variable fields	$1: Tunnel type: • Master. • Backup. $2: AC IP address.
Severity level	6
Example	CWC/6/CWC_AP_UP: Master CAPWAP tunnel to AC 192.168.10.1 went up.
Explanation	The AP was connected to the AC successfully and entered Run state.
Recommended action	No action is required.

CWC_AP_REBOOT

Message text	AP in state [STRING] is rebooting. Reason: [STRING]
Variable fields	$1: AP state. $2: Reason: • Image was downloaded successfully. • Reset by admin. • Reset by CloudTunnel, • Reset on cloud, • The radio status was incorrect, • WT was offline, • Stayed in idle state for a long time.
Severity level	6
Example	CWC/6/CWC_AP_REBOOT: AP in State Run is rebooting. Reason: Reset by admin.
Explanation	The AP rebooted for a specific reason.
Recommended action	No action is required.

CWC_IMG_DOWNLOAD_COMPLETE

Message text	System software image file [STRING] downloading through the CAPWAP tunnel to AC [STRING] completed.
Variable fields	$1: Image file name. $2: AC IP address.
Severity level	6
Example	CWC/6/CWC_IMG_DOWNLOAD_COMPLETE: System software image file 5800.ipe downloading through the CAPWAP tunnel to AC 192.168.10.1 completed.
Explanation	The AP downloaded the image file from the AC successfully.
Recommended action	No action is required.

CWS_IMG_DOWNLOAD_FAILED

Message text	Failed to download image file [STRING1] for [STRING2] [STRING3].
Variable fields	$1: Image file name. $2: AP or local AC. $3: Name of the AP or local AC.
Severity level	6
Example	CWS/6/CWS_IMG_DOWNLOAD_FAILED: Failed to download image file wa4300.ipe for AP ap1.
Explanation	The AP or the local AC failed to download the image file from the AC.
Recommended action	No action is required.

CWC_IMG_DOWNLOAD_START

Message text	Started to download the system software image file [STRING] through the CAPWAP tunnel to AC [STRING].
Variable fields	$1: Image file name. $2: AC IP address.
Severity level	6
Example	CWC/6/CWC_IMG_DOWNLOAD_START: Started to download the system software image file 5800.ipe through the CAPWAP tunnel to AC 192.168.10.1.
Explanation	The AP started to download the image file from the AC.
Recommended action	Make sure the AP is correctly connected to the AC.

CWC_IMG_NO_ENOUGH_SPACE

Message text	Insufficient flash memory space for downloading system software image file [STRING].
Variable fields	$1: Image file name.
Severity level	6
Example	CWC/6/CWC_IMG_NO_ENOUGH_SPACE: Insufficient flash memory space for downloading system software image file 5800.ipe.
Explanation	The AP failed to download the image file from the AC because of insufficient flash memory.
Recommended action	Delete files not in use from the AP.

CWC_LOCALAC_DOWN

Message text	CAPWAP tunnel to Central AC [STRING] went down. Reason: [STRING].
Variable fields	$1: IP address of the central AC. $2: Reason: • Added local AC IP address. • Deleted local AC IP address. • Local AC interface used for CAPWAP tunnel went down. • Local AC config changed. • N/A
Severity level	4
Example	CWC/4/CWC_LOCALAC_DOWN: CAPWAP tunnel to Central AC 2.2.2.1 went down. Reason: Local AC config changed.
Explanation	The CAPWAP tunnel between the central AC and the local AC was terminated for a specific reason.
Recommended action	To resolve the problem: **11.** Examine the network connection between the central AC and the local AC. **12.** Verify that the central AC is correctly configured. **13.** Verify that the local AC is correctly configured. **14.** If the problem persists, contact NSFOCUS Support.

CWC_LOCALAC_UP

Message text	CAPWAP tunnel to Central AC [STRING] went up.
Variable fields	$1: IP address of the central AC.
Severity level	6
Example	CWC/6/CWC_LOCALAC_UP: CAPWAP tunnel to Central AC 2.2.2.1 went up.
Explanation	The central AC has established a CAPWAP tunnel with the local AC.
Recommended action	No action is required.

CWC_RUN_DOWNLOAD_COMPLETE

Message text	File [STRING] successfully downloaded through the CAPWAP tunnel to AC [STRING].
Variable fields	$1: File name. $2: AC IP address.
Severity level	6
Example	CWC/6/CWC_RUN_DOWNLOAD_COMPLETE: File ac.cfg successfully downloaded through the CAPWAP tunnel to AC 192.168.10.1.
Explanation	The AP downloaded the file from the AC successfully.
Recommended action	No action is required.

CWC_RUN_DOWNLOAD_START

Message text	Started to download the file [STRING] through the CAPWAP tunnel to AC [STRING].
Variable fields	$1: File name. $2: AC IP address.
Severity level	6
Example	CWC/6/CWC_RUN_DOWNLOAD_START: Started to download the file ac.cfg through the CAPWAP tunnel to AC 192.168.10.1.
Explanation	The AP started to download the file from the AC.
Recommended action	Make sure the AP is correctly connected to the AC.

CWC_RUN_NO_ENOUGH_SPACE

Message text	Insufficient flash memory space for downloading file [STRING].
Variable fields	$1: File name.
Severity level	6
Example	CWC/6/CWC_RUN_NO_ENOUGH_SPACE: Insufficient flash memory space for downloading file ac.cfg.
Explanation	The AP failed to download the file from the AC because of insufficient flash memory.
Recommended action	Delete files not in use from the AP.

CWS_AP_DOWN

Message text	CAPWAP tunnel to AP [STRING] went down. Reason: [STRING].
Variable fields	$1: AP name. $2: Reason: • Neighbor dead timer expired. • AP was reset by admin. • AP was reset by CloudTunnel. • AP was reset on cloud. • WT was offline. • AP was deleted. • Serial number changed. • Processed join request in Run state. • Failed to retransmit message. • Received WTP tunnel down event from AP. • Backup AC closed the backup tunnel. • Backup AP upgrade failed. • AC is inactive. • Tunnel switched. • N/A.
Severity level	6
Example	CWS/6/CWS_AP_DOWN: CAPWAP tunnel to AP ap1 went down. Reason: AP was reset by admin.
Explanation	The AP went offline for a specific reason.
Recommended action	To resolve the problem: **15.** Examine the network connection between the AP and the AC. **16.** Verify that the AP is correctly configured. **17.** Verify that the AC is correctly configured. **18.** If the problem persists, contact NSFOCUS Support.

CWS_AP_UP

Message text	[STRING] CAPWAP tunnel to AP [STRING] went up.
Variable fields	$1: Tunnel type: • Master. • Backup. $2: AP name or serial ID.
Severity level	6
Example	CWS/6/CWS_AP_UP: Backup CAPWAP tunnel to AP ap1 went up.
Explanation	The AP came online and entered Run state.
Recommended action	No action is required.

CWS_IMG_DOWNLOAD_COMPLETE

Message text	System software image file [STRING] downloading through the CAPWAP tunnel for AP [STRING] completed.
Variable fields	$1: Image file name. $2: AP name.
Severity level	6
Example	CWS/6/CWS_IMG_DOWNLOAD_COMPLETE: System software image file 5800.ipe downloading through the CAPWAP tunnel for AP ap2 completed.
Explanation	The AP downloaded the image file from the AC successfully.
Recommended action	No action is required.

CWS_IMG_DOWNLOAD_FAILED

Message text	Failed to download image file [STRING] for the AP. AC memory is not enough.
Variable fields	$1: Name of an image file.
Severity level	6
Example	CWS/6/CWS_IMG_DOWNLOAD_FAILED: Failed to download image file wa4300anchor.ipe for the AP. AC memory is not enough.
Explanation	The AP failed to download an image file from the AC because of insufficient AC memory.
Recommended action	No action is required.

CWS_IMG_DOWNLOAD_START

Message text	AP [STRING] started to download the system software image file [STRING].
Variable fields	$1: AP name. $2: Image file name.
Severity level	6
Example	CWS/6/CWS_IMG_DOWNLOAD_START: AP ap1 started to download the system software image file 5800.ipe.
Explanation	The AP started to download the image file from the AC.
Recommended action	No action is required.

CWS_IMG_OPENFILE_FAILED

Message text	Failed to open the image file [STRING].
Variable fields	$1: Path of the image file to be downloaded to the AP.
Severity level	3
Example	CWS/3/CWS_IMG_OPENFILE_FAILED: Failed to open the image file slot1#cfa0:/wa5600.ipe.
Explanation	The AP failed to open the image file downloaded from the AC.
Recommended action	No action is required.

CWS_LOCALAC_DOWN

Message text	CAPWAP tunnel to local AC [STRING] went down. Reason: [STRING].
Variable fields	$1: IP address of the local AC. $2: Reason: • Neighbor dead timer expired. • Local AC was deleted. • Serial number changed. • Processed join request in Run state. • Failed to retransmit message. • N/A
Severity level	4
Example	CWS/4/CWS_LOCALAC_DOWN: CAPWAP tunnel to local AC 1.1.1.1 went down. Reason: Local AC was deleted.
Explanation	The CAPWAP tunnel between the central AC and the local AC was terminated for a specific reason.
Recommended action	To resolve the problem: **19.** Examine the network connection between the central AC and the local AC. **20.** Verify that the central AC is correctly configured. **21.** Verify that the local AC is correctly configured. **22.** If the problem persists, contact NSFOCUS Support.

CWS_LOCALAC_UP

Message text	CAPWAP tunnel to local AC [STRING] went up.
Variable fields	$1: IP address of the local AC.
Severity level	6
Example	CWS/6/CWS_LOCALAC_UP: CAPWAP tunnel to local AC 1.1.1.1 went up.
Explanation	The central AC has established a CAPWAP tunnel with the local AC.
Recommended action	No action is required.

CWS_RUN_DOWNLOAD_COMPLETE

Message text	File [STRING] successfully downloaded through the CAPWAP tunnel for AP [STRING].
Variable fields	$1: File name. $2: AP name.
Severity level	6
Example	CWS/6/CWS_RUN_DOWNLOAD_COMPLETE: File ac.cfg successfully downloaded through the CAPWAP tunnel for AP ap2.
Explanation	The AP downloaded the file from the AC successfully.
Recommended action	No action is required.

CWS_RUN_DOWNLOAD_START

Message text	AP [STRING] started to download the file [STRING].
Variable fields	$1: AP name. $2: File name.
Severity level	6
Example	CWS/6/CWS_RUN_DOWNLOAD_START: AP ap1 started to download the file ac.cfg.
Explanation	The AP started to download the file from the AC.
Recommended action	No action is required.

RADIO

Message text	APMGR/6/RADIO: Current channel usage [UINT32] of radio [CHAR] on AP [STRING] exceeded the threshold.
Variable fields	$1: Current channel usage. $2: Radio ID. $3: AP name.
Severity level	6
Example	APMGR/6/RADIO: Current channel usage 63% of radio 2 on AP ap1 exceeded the threshold.
Explanation	The current channel usage on a radio has exceeded the channel usage threshold.
Recommended action	Execute the **channel** command to switch the working channel to a channel with low usage.

Application account extraction messages

This section contains application account extraction messages.

USER-NETLOG

Message text	Protocol(1001)= [STRING];SrcIPAddr(1003)= [IPADDR];SrcPort(1004)= [UINT16];DstIPAddr(1007)= [IPADDR];DstPort(1008)= [UINT16]; User(1098)=%s; Application(1002)= [STRING]; Account(1101)= [STRING].
Variable fields	$1: Protocol address. $2: Source IP address. $3: Source port number. $4: Destination IP address. $5: Destination port number. $6: Username. $7: Application name. $8: User account.
Severity level	6
Example	UDPI/6/USER-NETLOG:-Chassis=1-Slot=5.1;Protocol(1001)=UDP;SrcIPAddr (1003)=22.1.1.2;SrcPort(1004)=0;DstIPAddr(1007)=21.1.1.2;DstPort(1008)=6 5297;User(1098)=22.1.1.2; Application(1002)=ZhenAiWang; Account(1101)=72753475.
Explanation	This message is generated when a packet matches application account characteristics.
Recommended action	None

APR messages

This section contains APR messages.

NBAR_WARNING

Message text	Updated the APR signature library successfully.
Variable fields	N/A
Severity level	4
Example	NBAR/4/NBAR_WARNING: -Context=1; Updated the APR signature library successfully.
Explanation	The APR signature library was updated successfully. The device outputs this log message for one of the following conditions: • The triggered update operation succeeds. • The local update operation succeeds.
Recommended action	No action is required.

NBAR_WARNING

Message text	Rolled back the APR signature library successfully.
Variable fields	N/A
Severity level	4
Example	NBAR/4/NBAR_WARNING: -Context=1; Rolled back the APR signature library successfully.
Explanation	The APR signature library was rolled back successfully to the last version or the factory version.
Recommended action	No action is required.

NBAR_WARNING

Message text	Failed to update the APR signature library because no valid license was found for the NBAR feature.
Variable fields	N/A
Severity level	4
Example	NBAR/4/NBAR_WARNING: -Context=1; Failed to update the APR signature library because no valid license was found for the NBAR feature.
Explanation	The APR signature library update failed because no valid license was found for updating the APR signature library. The device outputs this log message for one of the following conditions: • Failed to perform a triggered update operation. • Failed to perform a local update operation through the Web interface.
Recommended action	No action is required.

NBAR_WARNING

Message text	Failed to update the APR signature library because the target signature library failed to be downloaded.
Variable fields	N/A
Severity level	4
Example	NBAR/4/NBAR_WARNING: -Context=1; Failed to update the APR signature library because the target signature library failed to be downloaded.
Explanation	The device failed to update the APR signature library because the target signature library failed to be downloaded.
Recommended action	No action is required.

ARP messages

This section contains ARP messages.

ARP_ACTIVE_ACK_NO_REPLY

Message text	No ARP reply from IP [STRING] was received on interface [STRING].
Variable fields	$1: IP address. $2: Interface name.
Severity level	6
Example	ARP/6/ARP_ACTIVE_ACK_NO_REPLY: No ARP reply from IP 192.168.10.1 was received on interface GigabitEthernet1/0/1.
Explanation	The ARP active acknowledgement feature did not receive an ARP reply after it sent an ARP request to the sender IP of an ARP message. This message indicates the risk of attacks.
Recommended action	**23.** Verify that the learned ARP entries on the device are consistent with the existing legal devices. When gateways and servers are on the network, check the ARP entries for these devices first. **24.** If the ARP entries are correct and the attack continues, contact NSFOCUS Support.

ARP_ACTIVE_ACK_NOREQUESTED_REPLY

Message text	Interface [STRING] received from IP [STRING] an ARP reply that was not requested by the device.
Variable fields	$1: Interface name. $2: IP address.
Severity level	6
Example	ARP/6/ARP_ACTIVE_ACK_NOREQUESTED_REPLY: Interface GigabitEthernet1/0/1 received from IP 192.168.10.1 an ARP reply that was not requested by the device.
Explanation	The ARP active acknowledgement feature received an unsolicited ARP reply from a sender IP. This message indicates the risk of attacks.
Recommended action	No action is required. The device discards the ARP reply automatically.

ARP_BINDRULETOHW_FAILED

Message text	Failed to download binding rule to hardware on the interface [STRING], SrcIP [IPADDR], SrcMAC [MAC], VLAN [UINT16], Gateway MAC [MAC].
Variable fields	$1: Interface name. $2: Source IP address. $3: Source MAC address. $4: VLAN ID. $5: Gateway MAC address.
Severity level	5
Example	ARP/5/ARP_BINDRULETOHW_FAILED: Failed to download binding rule to hardware on the interface Ethernet1/0/1, SrcIP 1.1.1.132, SrcMAC 0015-E944-A947, VLAN 1, Gateway MAC 00A1-B812-1108.
Explanation	The system failed to set a binding rule to the hardware on an interface. The message is sent in any of the following situations: • The resources are not sufficient for the operation. • The memory is not sufficient for the operation. • A hardware error occurs.
Recommended action	To resolve the problem: **25.** Execute the **display qos-acl resource** command to check if the ACL resources for the operation are sufficient. o If yes, proceed to step 2. o If no, delete unnecessary configuration to release ACL resources. If no configuration can be deleted, proceed to step 2. **26.** Execute the **display memory** command to check if the memory for the operation is sufficient. o If yes, proceed to step 3. o If no, delete unnecessary configuration to release memory. If no configuration can be deleted, proceed to step 3. **27.** Delete the configuration and perform the operation again.

ARP_DYNAMIC

Message text	The maximum number of dynamic ARP entries for the device reached.
Variable fields	N/A
Severity level	6
Example	The maximum number of dynamic ARP entries for the device reached.
Explanation	This message is displayed when the maximum number of dynamic ARP entries on the device is reached.
Recommended action	No action is required.

ARP_DYNAMIC_IF

Message text	The maximum number of dynamic ARP entries for interface [STRING] reached.
Variable fields	$1: Interface name.
Severity level	6
Example	The maximum number of dynamic ARP entries for interface GigabitEthernet3/0/1 reached.
Explanation	This message is displayed when maximum number of dynamic ARP entries on an interface is reached.
Recommended action	No action is required.

ARP_DYNAMIC_SLOT

Message text	The maximum number of dynamic ARP entries for [STRING] reached.
Variable fields	$1: Slot number (in standalone mode) or chassis number and slot number (in IRF mode).
Severity level	6
Example	The maximum number of dynamic ARP entries for slot 2 reached. The maximum number of dynamic ARP entries for chassis 1 slot 2 reached.
Explanation	This message is displayed when the maximum number of dynamic ARP entries on a slot is reached.
Recommended action	No action is required.

ARP_HOST_IP_CONFLICT

Message text	The host [STRING] connected to interface [STRING] cannot communicate correctly, because it uses the same IP address as the host connected to interface [STRING].
Variable fields	$1: IP address. $2: Interface name. $3: Interface name.
Severity level	4
Example	ARP/4/ARP_HOST_IP_CONFLICT: The host 1.1.1.1 connected to interface GigabitEthernet1/0/1 cannot communicate correctly, because it uses the same IP address as the host connected to interface GigabitEthernet1/0/2.
Explanation	The sender IP address in a received ARP message conflicted with the IP address of a host connected to another interface.
Recommended action	Check whether the hosts that send the ARP messages are legitimate. Disconnect the illegal host from the network.

ARP_RATE_EXCEEDED

Message text	The ARP packet rate ([UINT32] pps) exceeded the rate limit ([UINT32] pps) on interface [STRING] in the last [UINT32] seconds.
Variable fields	$1: ARP packet rate. $2: ARP limit rate. $3: Interface name. $4: Interval time.
Severity level	4
Example	ARP/4/ARP_RATE_EXCEEDED: The ARP packet rate (100 pps) exceeded the rate limit (80 pps) on interface GigabitEthernet1/0/1 in the last 10 seconds.
Explanation	An interface received ARP messages at a higher rate than the rate limit.
Recommended action	Verify that the hosts at the sender IP addresses are legitimate.

ARP_SENDER_IP_INVALID

Message text	Sender IP [STRING] was not on the same network as the receiving interface [STRING].
Variable fields	$1: IP address. $2: Interface name.
Severity level	6
Example	ARP/6/ARP_SENDER_IP_INVALID: Sender IP 192.168.10.2 was not on the same network as the receiving interface GigabitEthernet1/0/1.
Explanation	The sender IP of a received ARP message was not on the same network as the receiving interface.
Recommended action	Verify that the host at the sender IP address is legitimate.

ARP_SENDER_MAC_INVALID

Message text	Sender MAC [STRING] was not identical to Ethernet source MAC [STRING] on interface [STRING].
Variable fields	$1: MAC address. $2: MAC address. $3: Interface name.
Severity level	6
Example	ARP/6/ARP_SENDER_MAC_INVALID: Sender MAC 0000-5E14-0E00 was not identical to Ethernet source MAC 0000-5C14-0E00 on interface GigabitEthernet1/0/1.
Explanation	An interface received an ARP message. The sender MAC address in the message body was not identical to the source MAC address in the Ethernet header.
Recommended action	Verify that the host at the sender MAC address is legitimate.

ARP_SRC_MAC_FOUND_ATTACK

Message text	An attack from MAC [STRING] was detected on interface [STRING].
Variable fields	$1: MAC address. $2: Interface name.
Severity level	6
Example	ARP/6/ARP_SRC_MAC_FOUND_ATTACK: An attack from MAC 0000-5E14-0E00 was detected on interface GigabitEthernet1/0/1.
Explanation	The source MAC-based ARP attack detection feature received more ARP packets from the same MAC address within 5 seconds than the specified threshold. This message indicates the risk of attacks.
Recommended action	Verify that the host at the source MAC address is legitimate.

ARP_TARGET_IP_INVALID

Message text	Target IP [STRING] was not the IP of the receiving interface [STRING].
Variable fields	$1: IP address. $2: Interface name.
Severity level	6
Example	ARP/6/ARP_TARGET_IP_INVALID: Target IP 192.168.10.2 was not the IP of the receiving interface GigabitEthernet1/0/1.
Explanation	The target IP address of a received ARP message was not the IP address of the receiving interface.
Recommended action	Verify that the host at the sender IP address is legitimate.

DUPIFIP

Message text	Duplicate address [STRING] on interface [STRING], sourced from [STRING].
Variable fields	$1: IP address. $2: Interface name. $3: MAC Address.
Severity level	6
Example	ARP/6/DUPIFIP: Duplicate address 1.1.1.1 on interface Ethernet1/1/1, sourced from 0015-E944-A947.
Explanation	ARP detected a duplicate address. The sender IP in the received ARP packet was being used by the receiving interface.
Recommended action	Modify the IP address configuration.

DUPIP

Message text	IP address [STRING] conflicted with global or imported IP address, sourced from [STRING].
Variable fields	$1: IP address. $2: MAC Address.
Severity level	6
Example	ARP/6/DUPIP: IP address 30.1.1.1 conflicted with global or imported IP address, sourced from 0000-0000-0001.
Explanation	The sender IP address of the received ARP packet conflicted with the global or imported IP address.
Recommended action	Modify the IP address configuration.

DUPVRRPIP

Message text	IP address [STRING] conflicted with VRRP virtual IP address on interface [STRING], sourced from [STRING].
Variable fields	$1: IP address. $2: Interface name. $3: MAC address.
Severity level	6
Example	ARP/6/DUPVRRPIP: IP address 1.1.1.1 conflicted with VRRP virtual IP address on interface Ethernet1/1/1, sourced from 0015-E944-A947.
Explanation	The sender IP address of the received ARP packet conflicted with the VRRP virtual IP address.
Recommended action	Modify the IP address configuration.

ASPF messages

This section contains ASPF messages.

ASPF_IPV4_DNS

Message text	SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];DomainName(1099)=[STRING];Action(1053)=[STRING];Reason(1056)=[STRING].
Variable fields	$1: Source IPv4 address. $2: Destination IPv4 address. $3: VPN instance name. $4: Local address of a DS-Lite tunnel. $5: Domain name. $6: Action on the detected illegal packets: • **drop**—Drops illegal packets. • **logging**—Generates log messages. • **none**—Does not process the packets and allows illegal packets to pass. $7: Reason why the message was generated: • Invalid DNS RR. • Failed to check DNS header flag. • Failed to check DNS header ID.
Severity level	6
Example	ASPF/6/ASPF_IPV4_DNS:SrcIPAddr(1003)=1.1.1.3;DstIPAddr(1007)=2.1.1.2;RcvVPNInstance(1042)=vpn;RcvDSLiteTunnelPeer(1040)=dstunnel1;DomainName(1099)=www.nsfocus.com.cn;Action(1053)=drop,logging;Reason(1056)=Check DNS RR invalid.
Explanation	ASPF inspection for DNS is configured. The device takes a specific action on IPv4 packets that are determined to be illegal for a reason.
Recommended action	No action is required.

ASPF_IPV6_DNS

Message text	SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];DomainName(1099)=[STRING];Action(1053)=[STRING];Reason(1056)=[STRING].
Variable fields	$1: Source IPv6 address. $2: Destination IPv6 address. $3: VPN instance name. $4: Domain name. $5: Action on the detected illegal packets: • **drop**—Drops illegal packets. • **logging**—Generates log messages. • **none**—Does not process the packet and allows illegal packets to pass. $6: Reason why the message was generated: • Invalid DNS RR. • Failed to check DNS header flag. • Failed to check DNS header ID.
Severity level	6
Example	ASPF/6/ASPF_IPV6_DNS:SrcIPv6Addr(1036)=2001::1;DstIPv6Addr(1037)=3001::1;RcvVPNInstance(1042)=vpn;DomainName(1099)=www.nsfocus.com.cn;Action(1053)=drop,logging;Reason(1056)=Check DNS RR invalid.
Explanation	ASPF inspection for DNS is configured. The device takes a specific action on IPv6 packets that are determined to be illegal for a reason.
Recommended action	No action is required.

ATK messages

This section contains attack detection and prevention messages.

ATK_ICMP_ADDRMASK_REQ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_ADDRMASK_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=17;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP address mask request logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_ADDRMASK_REQ_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=17;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP address mask requests of the same attributes, this message is sent only when the first request is received. If log aggregation is disabled, this message is sent every time an ICMP address mask request is received.
Recommended action	No action is required.

ATK_ICMP_ADDRMASK_REQ_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_ADDRMASK_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=17;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP address mask requests of the same attributes, this message is sent only when the first request is received. If log aggregation is disabled, this message is sent every time an ICMP address mask request is received.
Recommended action	No action is required.

ATK_ICMP_ADDRMASK_REQ_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_ADDRMASK_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=17;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP address mask request logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_ADDRMASK_RPL

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_ADDRMASK_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=18;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP address mask reply logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_ADDRMASK_RPL_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=18;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP address mask replies of the same attributes, this message is sent only when the first reply is received. If log aggregation is disabled, this message is sent every time an ICMP address mask reply is received.
Recommended action	No action is required.

ATK_ICMP_ADDRMASK_RPL_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_ADDRMASK_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=18;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP address mask replies of the same attributes, this message is sent only when the first reply is received. If log aggregation is disabled, this message is sent every time an ICMP address mask reply is received.
Recommended action	No action is required.

ATK_ICMP_ADDRMASK_RPL_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_ADDRMASK_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=18;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP address mask reply logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_ECHO_REQ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_ECHO_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=8;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP echo request logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_ECHO_REQ_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_ECHO_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=8;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP echo requests of the same attributes, this message is sent only when the first request is received. If log aggregation is disabled, this message is sent every time an ICMP echo request is received.
Recommended action	No action is required.

ATK_ICMP_ECHO_REQ_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_ECHO_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=8;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP echo requests of the same attributes, this message is sent only when the first request is received. If log aggregation is disabled, this message is sent every time an ICMP echo request is received.
Recommended action	No action is required.

ATK_ICMP_ECHO_REQ_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_ECHO_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=8;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP echo request logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_ECHO_RPL

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_ECHO_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=0;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP echo reply logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_ECHO_RPL_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_ECHO_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=0;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP echo replies of the same attributes, this message is sent only when the first reply is received. If log aggregation is disabled, this message is sent every time an ICMP echo reply is received.
Recommended action	No action is required.

ATK_ICMP_ECHO_RPL_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_ECHO_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=0;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP echo replies of the same attributes, this message is sent only when the first reply is received. If log aggregation is disabled, this message is sent every time an ICMP echo reply is received.
Recommended action	No action is required.

ATK_ICMP_ECHO_RPL_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_ECHO_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=0;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP echo reply logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IP address. $3: Destination port number. $4: Name of the receiving VPN instance. $5: Rate limit. $6: Actions against the attack. $7: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_ICMP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of ICMP packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_ICMP_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IP address. $4: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_ICMP_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of ICMP packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_ICMP_INFO_REQ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_INFO_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=15;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP information request logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_INFO_REQ_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_INFO_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=15;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP information requests of the same attributes, this message is sent only when the first request is received. If log aggregation is disabled, this message is sent every time an ICMP information request is received.
Recommended action	No action is required.

ATK_ICMP_INFO_REQ_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_INFO_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=15;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP information requests of the same attributes, this message is sent only when the first request is received. If log aggregation is disabled, this message is sent every time an ICMP information request is received.
Recommended action	No action is required.

ATK_ICMP_INFO_REQ_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_INFO_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=15;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP information request logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_INFO_RPL

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_INFO_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=16;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP information reply logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_INFO_RPL_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_INFO_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=16;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP information replies of the same attributes, this message is sent only when the first reply is received. If log aggregation is disabled, this message is sent every time an ICMP information reply is received.
Recommended action	No action is required.

ATK_ICMP_INFO_RPL_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_INFO_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=16;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP information replies of the same attributes, this message is sent only when the first reply is received. If log aggregation is disabled, this message is sent every time an ICMP information reply is received.
Recommended action	No action is required.

ATK_ICMP_INFO_RPL_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_INFO_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=16;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP information reply logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_LARGE

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/3/ATK_ICMP_LARGE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when large ICMP packet logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_LARGE_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/3/ATK_ICMP_LARGE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for large ICMP packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a large ICMP packet is received.
Recommended action	No action is required.

ATK_ICMP_LARGE_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_LARGE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for large ICMP packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a large ICMP packet is received.
Recommended action	No action is required.

ATK_ICMP_LARGE_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/3/ATK_ICMP_LARGE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when large ICMP packet logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_PARAPROBLEM

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_PARAPROBLEM:SubModule(1127)=SINGLE;IcmpType(1062)=12;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP parameter problem logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_PARAPROBLEM_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_PARAPROBLEM_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=12;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP parameter problem packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP parameter problem packet is received.
Recommended action	No action is required.

ATK_ICMP_PARAPROBLEM_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_PARAPROBLEM_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=12;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP parameter problem packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP parameter problem packet is received.
Recommended action	No action is required.

ATK_ICMP_PARAPROBLEM_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_PARAPROBLEM_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=12;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP parameter problem logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_PINGOFDEATH

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_ICMP_PINGOFDEATH:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for ICMP packets larger than 65535 bytes with the MF flag set to 0.
Recommended action	No action is required.

ATK_ICMP_PINGOFDEATH_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_ICMP_PINGOFDEATH_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the ping of death attack. The attack uses ICMP packets larger than 65535 bytes with the MF flag set to 0. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_ICMP_PINGOFDEATH_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_ICMP_PINGOFDEATH_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the ping of death attack. The attack uses ICMP packets larger than 65535 bytes with the MF flag set to 0. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_ICMP_PINGOFDEATH_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_ICMP_PINGOFDEATH_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for ICMP packets larger than 65535 bytes with the MF flag set to 0.
Recommended action	No action is required.

ATK_ICMP_REDIRECT

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_REDIRECT:SubModule(1127)=SINGLE;IcmpType(1062)=5;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP redirect logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_REDIRECT_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_REDIRECT_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=5;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP redirect packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP redirect packet is received.
Recommended action	No action is required.

ATK_ICMP_REDIRECT_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_REDIRECT_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=5;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP redirect packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP redirect packet is received.
Recommended action	No action is required.

ATK_ICMP_REDIRECT_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_REDIRECT_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=5;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP redirect logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_SMURF

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_ICMP_SMURF:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for ICMP echo requests whose destination IP address is one of the following addresses: • A broadcast or network address of A, B, or C class. • An IP address of D or E class. • The broadcast or network address of the network where the receiving interface resides.
Recommended action	No action is required.

ATK_ICMP_SMURF_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_ICMP_SMURF_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the smurf attack. The attack uses ICMP echo requests with the destination IP address being one of the following addresses: • A broadcast or network address of A, B, or C class. • An IP address of D or E class. • The broadcast or network address of the network where the receiving interface resides. If log aggregation is enabled, for requests of the same attributes, this message is sent only when the first request is received. If log aggregation is disabled, this message is sent every time a request is received.
Recommended action	No action is required.

ATK_ICMP_SMURF_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_ICMP_SMURF_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the smurf attack. The attack uses ICMP echo requests with the destination IP address being one of the following addresses: • A broadcast or network address of A, B, or C class. • An IP address of D or E class. • The broadcast or network address of the network where the receiving interface resides. If log aggregation is enabled, for requests of the same attributes, this message is sent only when the first request is received. If log aggregation is disabled, this message is sent every time a request is received.
Recommended action	No action is required.

ATK_ICMP_SMURF_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_ICMP_SMURF_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for ICMP echo requests whose destination IP address is one of the following addresses: • A broadcast or network address of A, B, or C class. • An IP address of D or E class. • The broadcast or network address of the network where the receiving interface resides.
Recommended action	No action is required.

ATK_ICMP_SOURCEQUENCH

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_SOURCEQUENCH:SubModule(1127)=SINGLE;IcmpType(1062)=4;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP source quench logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_SOURCEQUENCH_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=4;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP source quench packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP source quench packet is received.
Recommended action	No action is required.

ATK_ICMP_SOURCEQUENCH_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_SOURCEQUENCH_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=4;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP source quench packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP source quench packet is received.
Recommended action	No action is required.

ATK_ICMP_SOURCEQUENCH_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_SOURCEQUENCH_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=4;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP source quench logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_TIMEEXCEED

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_TIMEEXCEED:SubModule(1127)=SINGLE;IcmpType(1062)=11;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP time exceeded logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_TIMEEXCEED_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_TIMEEXCEED_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=11;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP time exceeded packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP time exceeded packet is received.
Recommended action	No action is required.

ATK_ICMP_TIMEEXCEED_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_TIMEEXCEED_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=11;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP time exceeded packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP time exceeded packet is received.
Recommended action	No action is required.

ATK_ICMP_TIMEEXCEED_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_TIMEEXCEED_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=11;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP time exceeded logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_TRACEROUTE

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	4
Example	ATK/3/ATK_ICMP_TRACEROUTE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for ICMP time exceeded packets of code 0.
Recommended action	No action is required.

ATK_ICMP_TRACEROUTE_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	4
Example	ATK/3/ATK_ICMP_TRACEROUTE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP time exceeded packets of code 0 of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP time exceeded packet of code 0 is received.
Recommended action	No action is required.

ATK_ICMP_TRACEROUTE_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	4
Example	ATK/3/ATK_ICMP_TRACEROUTE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP time exceeded packets of code 0 of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP time exceeded packet of code 0 is received.
Recommended action	No action is required.

ATK_ICMP_TRACEROUTE_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	4
Example	ATK/3/ATK_ICMP_TRACEROUTE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for ICMP time exceeded packets of code 0.
Recommended action	No action is required.

ATK_ICMP_TSTAMP_REQ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_TSTAMP_REQ:SubModule(1127)=SINGLE;IcmpType(1062)=13;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP timestamp logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_TSTAMP_REQ_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=13;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP timestamp packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP timestamp packet is received.
Recommended action	No action is required.

ATK_ICMP_TSTAMP_REQ_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_TSTAMP_REQ_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=13;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP timestamp packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP timestamp packet is received.
Recommended action	No action is required.

ATK_ICMP_TSTAMP_REQ_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_TSTAMP_REQ_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=13;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP timestamp logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_TSTAMP_RPL

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_TSTAMP_RPL:SubModule(1127)=SINGLE;IcmpType(1062)=14;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP timestamp reply logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_TSTAMP_RPL_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=14;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP timestamp replies of the same attributes, this message is sent only when the first reply is received. If log aggregation is disabled, this message is sent every time an ICMP timestamp reply is received.
Recommended action	No action is required.

ATK_ICMP_TSTAMP_RPL_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_TSTAMP_RPL_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=14;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP timestamp replies of the same attributes, this message is sent only when the first reply is received. If log aggregation is disabled, this message is sent every time an ICMP timestamp reply is received.
Recommended action	No action is required.

ATK_ICMP_TSTAMP_RPL_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_TSTAMP_RPL_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=14;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP timestamp reply logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_TYPE

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_TYPE:SubModule(1127)=SINGLE;IcmpType(1062)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for user-defined ICMP packets.
Recommended action	No action is required.

ATK_ICMP_TYPE_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_TYPE_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for user-defined ICMP packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a user-defined ICMP packet is received.
Recommended action	No action is required.

ATK_ICMP_TYPE_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_TYPE_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for user-defined ICMP packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a user-defined ICMP packet is received.
Recommended action	No action is required.

ATK_ICMP_TYPE_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_TYPE_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for user-defined ICMP packets.
Recommended action	No action is required.

ATK_ICMP_UNREACHABLE

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_UNREACHABLE:SubModule(1127)=SINGLE;IcmpType(1062)=3;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP destination unreachable logs are aggregated.
Recommended action	No action is required.

ATK_ICMP_UNREACHABLE_RAW

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_UNREACHABLE_RAW:SubModule(1127)=SINGLE;IcmpType(1062)=3;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP destination unreachable packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP destination unreachable packet is received.
Recommended action	No action is required.

ATK_ICMP_UNREACHABLE_RAW_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMP_UNREACHABLE_RAW_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=3;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMP destination unreachable packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMP destination unreachable packet is received.
Recommended action	No action is required.

ATK_ICMP_UNREACHABLE_SZ

Message text	SubModule(1127)=SINGLE;IcmpType(1062)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMP message type. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMP_UNREACHABLE_SZ:SubModule(1127)=SINGLE;IcmpType(1062)=3;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011091319;EndTime_c(1012)=20131011091819;AtkTimes(1054)=2.
Explanation	This message is sent when ICMP destination unreachable logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_DEST_UNREACH

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_DEST_UNREACH:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 destination unreachable logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_DEST_UNREACH_RAW

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 destination unreachable packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 destination unreachable packet is received.
Recommended action	No action is required.

ATK_ICMPV6_DEST_UNREACH_RAW_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_DEST_UNREACH_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 destination unreachable packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 destination unreachable packet is received.
Recommended action	No action is required.

ATK_ICMPV6_DEST_UNREACH_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_DEST_UNREACH_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=133;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 destination unreachable logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_ECHO_REQ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_ECHO_REQ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 echo request logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_ECHO_REQ_RAW

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 echo requests of the same attributes, this message is sent only when the first request is received. If log aggregation is disabled, this message is sent every time an ICMPv6 echo request is received.
Recommended action	No action is required.

ATK_ICMPV6_ECHO_REQ_RAW_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_ECHO_REQ_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 echo requests of the same attributes, this message is sent only when the first request is received. If log aggregation is disabled, this message is sent every time an ICMPv6 echo request is received.
Recommended action	No action is required.

ATK_ICMPV6_ECHO_REQ_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_ECHO_REQ_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=128;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 echo request logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_ECHO_RPL

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_ECHO_RPL:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 echo reply logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_ECHO_RPL_RAW

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 echo replies of the same attributes, this message is sent only when the first reply is received. If log aggregation is disabled, this message is sent every time an ICMPv6 echo reply is received.
Recommended action	No action is required.

ATK_ICMPV6_ECHO_RPL_RAW_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_ECHO_RPL_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 echo replies of the same attributes, this message is sent only when the first reply is received. If log aggregation is disabled, this message is sent every time an ICMPv6 echo reply is received.
Recommended action	No action is required.

ATK_ICMPV6_ECHO_RPL_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_ECHO_RPL_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=129;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 echo reply logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IPv6 address. $3: Destination port number. $4: Name of the receiving VPN instance. $5: Rate limit. $6: Actions against the attack. $7: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_ICMPV6_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1007)=2002::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of ICMPv6 packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_ICMPV6_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IPv6 address. $3: Destination port number. $4: Name of the receiving VPN instance. $5: Rate limit. $6: Actions against the attack. $7: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_ICMPV6_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1007)=2002::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of ICMPv6 packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_ICMPV6_GROUPQUERY

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPQUERY:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 multicast listener query logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_GROUPQUERY_RAW

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 multicast listener queries of the same attributes, this message is sent only when the first query is received. If log aggregation is disabled, this message is sent every time an ICMPv6 multicast listener query is received.
Recommended action	No action is required.

ATK_ICMPV6_GROUPQUERY_RAW_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPQUERY_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 multicast listener queries of the same attributes, this message is sent only when the first query is received. If log aggregation is disabled, this message is sent every time an ICMPv6 multicast listener query is received.
Recommended action	No action is required.

ATK_ICMPV6_GROUPQUERY_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPQUERY_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=130;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 multicast listener query logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_GROUPREDUCTION

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPREDUCTION:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 multicast listener done logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_GROUPREDUCTION_RAW

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 multicast listener done packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 multicast listener done packet is received.
Recommended action	No action is required.

ATK_ICMPV6_GROUPREDUCTION_RAW_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPREDUCTION_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 multicast listener done packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 multicast listener done packet is received.
Recommended action	No action is required.

ATK_ICMPV6_GROUPREDUCTION_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPREDUCTION_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=132;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 multicast listener done logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_GROUPREPORT

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPREPORT:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 multicast listener report logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_GROUPREPORT_RAW

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 multicast listener reports of the same attributes, this message is sent only when the first report is received. If log aggregation is disabled, this message is sent every time an ICMPv6 multicast listener report is received.
Recommended action	No action is required.

ATK_ICMPV6_GROUPREPORT_RAW_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPREPORT_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 multicast listener reports of the same attributes, this message is sent only when the first report is received. If log aggregation is disabled, this message is sent every time an ICMPv6 multicast listener report is received.
Recommended action	No action is required.

ATK_ICMPV6_GROUPREPORT_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_GROUPREPORT_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=131;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 multicast listener report logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_LARGE

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	5
Example	ATK/3/ATK_ICMPV6_LARGE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when large ICMPv6 packet logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_LARGE_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	5
Example	ATK/3/ATK_ICMPV6_LARGE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for large ICMPv6 packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a large ICMPv6 packet is received.
Recommended action	No action is required.

ATK_ICMPV6_LARGE_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	5
Example	ATK/3/ATK_ICMPV6_LARGE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for large ICMPv6 packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a large ICMPv6 packet is received.
Recommended action	No action is required.

ATK_ICMPV6_LARGE_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	5
Example	ATK/3/ATK_ICMPV6_LARGE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when large ICMPv6 packet logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_PACKETTOOBIG

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_PACKETTOOBIG:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 packet too big logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_PACKETTOOBIG_RAW

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 packet too big packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 packet too big packet is received.
Recommended action	No action is required.

ATK_ICMPV6_PACKETTOOBIG_RAW_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_PACKETTOOBIG_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 packet too big packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 packet too big packet is received.
Recommended action	No action is required.

ATK_ICMPV6_PACKETTOOBIG_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_PACKETTOOBIG_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=136;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 packet too big logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_PARAPROBLEM

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_PARAPROBLEM:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 parameter problem logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_PARAPROBLEM_RAW

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 parameter problem packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 parameter problem packet is received.
Recommended action	No action is required.

ATK_ICMPV6_PARAPROBLEM_RAW_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_PARAPROBLEM_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 parameter problem packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 parameter problem packet is received.
Recommended action	No action is required.

ATK_ICMPV6_PARAPROBLEM_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_PARAPROBLEM_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=135;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 parameter problem logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_TIMEEXCEED

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_TIMEEXCEED:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 time exceeded logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_TIMEEXCEED_RAW

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 time exceeded packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 time exceeded packet is received.
Recommended action	No action is required.

ATK_ICMPV6_TIMEEXCEED_RAW_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_TIMEEXCEED_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for ICMPv6 time exceeded packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 time exceeded packet is received.
Recommended action	No action is required.

ATK_ICMPV6_TIMEEXCEED_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_TIMEEXCEED_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=134;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when ICMPv6 time exceeded logs are aggregated.
Recommended action	No action is required.

ATK_ICMPV6_TRACEROUTE

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	4
Example	ATK/3/ATK_ICMPV6_TRACEROUTE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for ICMPv6 time exceeded packets of code 0.
Recommended action	No action is required.

ATK_ICMPV6_TRACEROUTE_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	4
Example	ATK/3/ATK_ICMPV6_TRACEROUTE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435.
Explanation	If log aggregation is enabled, for ICMPv6 time exceeded packets of code 0 of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 time exceeded packet of code 0 is received.
Recommended action	No action is required.

ATK_ICMPV6_TRACEROUTE_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	4
Example	ATK/3/ATK_ICMPV6_TRACEROUTE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435.
Explanation	If log aggregation is enabled, for ICMPv6 time exceeded packets of code 0 of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an ICMPv6 time exceeded packet of code 0 is received.
Recommended action	No action is required.

ATK_ICMPV6_TRACEROUTE_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	4
Example	ATK/3/ATK_ICMPV6_TRACEROUTE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for ICMPv6 time exceeded packets of code 0.
Recommended action	No action is required.

ATK_ICMPV6_TYPE

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_TYPE:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for user-defined ICMPv6 packets.
Recommended action	No action is required.

ATK_ICMPV6_TYPE _RAW_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_TYPE_RAW_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for user-defined ICMPv6 packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a user-defined ICMPv6 packet is received.
Recommended action	No action is required.

ATK_ICMPV6_TYPE_RAW

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_ICMPV6_TYPE_RAW:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for user-defined ICMPv6 packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a user-defined ICMPv6 packet is received.
Recommended action	No action is required.

ATK_ICMPV6_TYPE_SZ

Message text	SubModule(1127)=SINGLE;Icmpv6Type(1064)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: ICMPv6 message type. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_ICMPV6_TYPE_SZ:SubModule(1127)=SINGLE;Icmpv6Type(1064)=38;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=5600::12;DstIPv6Addr(1037)=1200:0:3400:0:5600:0:7800:0;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011100935;EndTime_c(1012)=20131011101435;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for user-defined ICMPv6 packets.
Recommended action	No action is required.

ATK_IP_OPTION

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IP_OPTION:SubModule(1127)=SINGLE;IPOptValue(1061)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with a user-defined IP option.
Recommended action	No action is required.

ATK_IP_OPTION_RAW

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IP_OPTION_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=38;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with a user-defined IP option and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with a user-defined IP option is received.
Recommended action	No action is required.

ATK_IP_OPTION_RAW_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IP_OPTION_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with a user-defined IP option and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with a user-defined IP option is received.
Recommended action	No action is required.

ATK_IP_OPTION_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IP_OPTION_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=38;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with a user-defined IP option.
Recommended action	No action is required.

ATK_IP4_ACK_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_ACK_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 ACK packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_ACK_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_ACK_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 ACK packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_DIS_PORTSCAN

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Protocol name. $4: Destination IP address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_DIS_PORTSCAN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=UDP;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
Explanation	This message is sent when an IPv4 distributed port scan attack is detected.
Recommended action	No action is required.

ATK_IP4_DIS_PORTSCAN_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Protocol name. $4: Destination IP address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_DIS_PORTSCAN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
Explanation	This message is sent when an IPv4 distributed port scan attack is detected.
Recommended action	No action is required.

ATK_IP4_DNS_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_DNS_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 DNS queries sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_DNS_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_DNS_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 DNS queries sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_FIN_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_FIN_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 FIN packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_FIN_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_FIN_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 FIN packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_FRAGMENT

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	4
Example	ATK/3/ATK_IP4_FRAGMENT:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 packets with an offset smaller than 5 but bigger than 0.
Recommended action	No action is required.

ATK_IP4_FRAGMENT_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack.
Severity level	4
Example	ATK/3/ATK_IP4_FRAGMENT_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
Explanation	This message is for the IPv4 fragment attack. The attack uses IPv4 packets with an offset smaller than 5 but bigger than 0. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_FRAGMENT_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack.
Severity level	4
Example	ATK/3/ATK_IP4_FRAGMENT_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
Explanation	This message is for the IPv4 fragment attack. The attack uses IPv4 packets with an offset smaller than 5 but bigger than 0. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_FRAGMENT_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	4
Example	ATK/3/ATK_IP4_FRAGMENT_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 packets with an offset smaller than 5 but bigger than 0.
Recommended action	No action is required.

ATK_IP4_HTTP_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_HTTP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 HTTP Get packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_HTTP_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_HTTP_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 HTTP Get packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_IMPOSSIBLE

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_IMPOSSIBLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 packets whose source IPv4 address is the same as the destination IPv4 address.
Recommended action	No action is required.

ATK_IP4_IMPOSSIBLE_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_IMPOSSIBLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
Explanation	This message is for the IPv4 impossible packet attack. The attack uses IPv4 packets whose source IPv4 address is the same as the destination IPv4 address. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_IMPOSSIBLE_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_IMPOSSIBLE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
Explanation	This message is for the IPv4 impossible packet attack. The attack uses IPv4 packets whose source IPv4 address is the same as the destination IPv4 address. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_IMPOSSIBLE_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_IMPOSSIBLE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 packets whose source IPv4 address is the same as the destination IPv4 address.
Recommended action	No action is required.

ATK_IP4_IPSWEEP

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Protocol name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_IPSWEEP:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009060657.
Explanation	This message is sent when an IPv4 sweep attack is detected.
Recommended action	No action is required.

ATK_IP4_IPSWEEP_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Protocol name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_IPSWEEP_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009060657.
Explanation	This message is sent when an IPv4 sweep attack is detected.
Recommended action	No action is required.

ATK_IP4_PORTSCAN

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];DstIPAddr(1007)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Protocol name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Name of the receiving VPN instance. $7: Destination IP address. $8: Actions against the attack. $9: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_PORTSCAN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;DstIPAddr(1007)=6.1.1.5;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
Explanation	This message is sent when an IPv4 port scan attack is detected.
Recommended action	No action is required.

ATK_IP4_PORTSCAN_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];RcvVPNInstance(1042)=[STRING];DstIPAddr(1007)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Protocol name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Name of the receiving VPN instance. $7: Destination IP address. $8: Actions against the attack. $9: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_PORTSCAN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPAddr(1003)=9.1.1.5;SndDSLiteTunnelPeer(1041)=--;RcvVPNInstance(1042)=vpn1;DstIPAddr(1007)=6.1.1.5;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009052955.
Explanation	This message is sent when an IPv4 port scan attack is detected.
Recommended action	No action is required.

ATK_IP4_RST_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_RST_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 RST packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_RST_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_RST_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 RST packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_SLOW_ATTACK

Message text	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_SLOW_ATTACK:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 HTTP slow attack packets sent to a destination within the detection period exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_SLOW_ATTACK_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_SLOW_ATTACK_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 HTTP slow attack packets sent to a destination within the detection period exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_SYN_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_SYN_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 SYN packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_SYN_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Source IP address. $3: Destination IP address. $4: Destination port number. $5: Name of the receiving VPN instance. $6: Rate limit. $7: Actions against the attack. $8: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_SYN_FLOOD_SZ:SrcZoneName(1025)=Trust;SrcIPAddr(1003)=2.3.3.1;SrcPort(1004)=25;DstIPAddr(1007)=6.1.1.5;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 SYN packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_SYNACK_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_SYNACK_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 SYN-ACK packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_SYNACK_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_SYNACK_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 SYN-ACK packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_TCP_ALLFLAGS

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_ALLFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets that have all flags set.
Recommended action	No action is required.

ATK_IP4_TCP_ALLFLAGS_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 TCP packets that have all flags set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_ALLFLAGS_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_ALLFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 TCP packets that have all flags set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_ALLFLAGS_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_ALLFLAGS_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets that have all flags set.
Recommended action	No action is required.

ATK_IP4_TCP_FINONLY

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_FINONLY:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets that have only the FIN flag set.
Recommended action	No action is required.

ATK_IP4_TCP_FINONLY_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_FINONLY_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 TCP packets that have only the FIN flag set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_FINONLY_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_FINONLY_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 TCP packets that have only the FIN flag set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_FINONLY_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_FINONLY_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets that have only the FIN flag set.
Recommended action	No action is required.

ATK_IP4_TCP_INVALIDFLAGS

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_INVALIDFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets that have invalid flag settings. Invalid flag settings include: • The RST and FIN flags are both set. • The RST and SYN flags are both set. • The RST, FIN, and SYN flags are all set. • The PSH, RST, and FIN flags are all set. • The PSH, RST, and SYN flags are all set. • The PSH, RST, SYN, and FIN flags are all set. • The ACK, RST, and FIN flags are all set. • The ACK, RST, and SYN flags are all set. • The ACK, RST, SYN, and FIN flags are all set. • The ACK, PSH, SYN, and FIN flags are all set. • The ACK, PSH, RST, and FIN flags are all set. • The ACK, PSH, RST, and SYN flags are all set.
Recommended action	No action is required.

ATK_IP4_TCP_INVALIDFLAGS_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 TCP packets that have invalid flag settings. Invalid flag settings include: • The RST and FIN flags are both set. • The RST and SYN flags are both set. • The RST, FIN, and SYN flags are all set. • The PSH, RST, and FIN flags are all set. • The PSH, RST, and SYN flags are all set. • The PSH, RST, SYN, and FIN flags are all set. • The ACK, RST, and FIN flags are all set. • The ACK, RST, and SYN flags are all set. • The ACK, RST, SYN, and FIN flags are all set. • The ACK, PSH, SYN, and FIN flags are all set. • The ACK, PSH, RST, and FIN flags are all set. • The ACK, PSH, RST, and SYN flags are all set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 TCP packets that have invalid flag settings. Invalid flag settings include: • The RST and FIN flags are both set. • The RST and SYN flags are both set. • The RST, FIN, and SYN flags are all set. • The PSH, RST, and FIN flags are all set. • The PSH, RST, and SYN flags are all set. • The PSH, RST, SYN, and FIN flags are all set. • The ACK, RST, and FIN flags are all set. • The ACK, RST, and SYN flags are all set. • The ACK, RST, SYN, and FIN flags are all set. • The ACK, PSH, SYN, and FIN flags are all set. • The ACK, PSH, RST, and FIN flags are all set. • The ACK, PSH, RST, and SYN flags are all set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_INVALIDFLAGS_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_INVALIDFLAGS_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets that have invalid flag settings. Invalid flag settings include: • The RST and FIN flags are both set. • The RST and SYN flags are both set. • The RST, FIN, and SYN flags are all set. • The PSH, RST, and FIN flags are all set. • The PSH, RST, and SYN flags are all set. • The PSH, RST, SYN, and FIN flags are all set. • The ACK, RST, and FIN flags are all set. • The ACK, RST, and SYN flags are all set. • The ACK, RST, SYN, and FIN flags are all set. • The ACK, PSH, SYN, and FIN flags are all set. • The ACK, PSH, RST, and FIN flags are all set. • The ACK, PSH, RST, and SYN flags are all set.
Recommended action	No action is required.

ATK_IP4_TCP_LAND

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_LAND:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets whose source IP address is the same as the destination IP address.
Recommended action	No action is required.

ATK_IP4_TCP_LAND_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_LAND_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the IPv4 land attack. The attack uses IPv4 TCP packets whose source IP address is the same as the destination IP address. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_LAND_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_LAND_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the IPv4 land attack. The attack uses IPv4 TCP packets whose source IP address is the same as the destination IP address. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_LAND_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_LAND_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets whose source IP address is the same as the destination IP address.
Recommended action	No action is required.

ATK_IP4_TCP_NULLFLAG

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_NULLFLAG:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=4.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets that have no flag set.
Recommended action	No action is required.

ATK_IP4_TCP_NULLFLAG_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 TCP packets that have no flag set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_NULLFLAG_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_NULLFLAG_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 TCP packets that have no flag set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_NULLFLAG_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_NULLFLAG_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=4.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets that have no flag set.
Recommended action	No action is required.

ATK_IP4_TCP_SYNFIN

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_SYNFIN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets that have SYN and FIN flags set.
Recommended action	No action is required.

ATK_IP4_TCP_SYNFIN_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_SYNFIN_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 TCP packets that have SYN and FIN flags set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_SYNFIN_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_SYNFIN_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 TCP packets that have SYN and FIN flags set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_SYNFIN_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_SYNFIN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets that have SYN and FIN flags set.
Recommended action	No action is required.

ATK_IP4_TCP_WINNUKE

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_WINNUKE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=5.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets with destination port 139, the URG flag set, and a nonzero Urgent Pointer.
Recommended action	No action is required.

ATK_IP4_TCP_WINNUKE_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_WINNUKE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the IPv4 WinNuke attack. The attack uses IPv4 TCP packets with destination port 139, the URG flag set, and a nonzero Urgent Pointer. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_WINNUKE_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_WINNUKE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the IPv4 WinNuke attack. The attack uses IPv4 TCP packets with destination port 139, the URG flag set, and a nonzero Urgent Pointer. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TCP_WINNUKE_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TCP_WINNUKE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=5.
Explanation	This message is sent when logs are aggregated for IPv4 TCP packets with destination port 139, the URG flag set, and a nonzero Urgent Pointer.
Recommended action	No action is required.

ATK_IP4_TEARDROP

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TEARDROP:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 overlapping fragments.
Recommended action	No action is required.

ATK_IP4_TEARDROP_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TEARDROP_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for IPv4 overlapping fragments of the same attributes, this message is sent only when the first overlapping fragment is received. If log aggregation is disabled, this message is sent every time an IPv4 overlapping fragment is received.
Recommended action	No action is required.

ATK_IP4_TEARDROP_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_TEARDROP_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for IPv4 overlapping fragments of the same attributes, this message is sent only when the first overlapping fragment is received. If log aggregation is disabled, this message is sent every time an IPv4 overlapping fragment is received.
Recommended action	No action is required.

ATK_IP4_TEARDROP_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_TEARDROP_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for IPv4 overlapping fragments.
Recommended action	No action is required.

ATK_IP4_TINY_FRAGMENT

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	4
Example	ATK/3/ATK_IP4_TINY_FRAGMENT:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=6.
Explanation	This message is sent when logs are aggregated for IPv4 packets with a datagram smaller than 68 bytes and the MF flag set.
Recommended action	No action is required.

ATK_IP4_TINY_FRAGMENT_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack.
Severity level	4
Example	ATK/3/ATK_IP4_TINY_FRAGMENT_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
Explanation	This message is for the IPv4 tiny fragment attack. The attack uses IPv4 packets with a datagram smaller than 68 bytes and the MF flag set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TINY_FRAGMENT_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack.
Severity level	4
Example	ATK/3/ATK_IP4_TINY_FRAGMENT_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging.
Explanation	This message is for the IPv4 tiny fragment attack. The attack uses IPv4 packets with a datagram smaller than 68 bytes and the MF flag set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_TINY_FRAGMENT_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	4
Example	ATK/3/ATK_IP4_TINY_FRAGMENT_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=TCP;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=6.
Explanation	This message is sent when logs are aggregated for IPv4 packets with a datagram smaller than 68 bytes and the MF flag set.
Recommended action	No action is required.

ATK_IP4_UDP_BOMB

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_BOMB:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv4 UDP packets in which the length value in the IP header is larger than the IP header length plus the length in the UDP header.
Recommended action	No action is required.

ATK_IP4_UDP_BOMB_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_BOMB_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 UDP bomb attack. The attack uses IPv4 UDP packets in which the length value in the IP header is larger than the IP header length plus the length in the UDP header. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_UDP_BOMB_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_BOMB_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 UDP bomb attack. The attack uses IPv4 UDP packets in which the length value in the IP header is larger than the IP header length plus the length in the UDP header. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_UDP_BOMB_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_BOMB_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv4 UDP packets in which the length value in the IP header is larger than the IP header length plus the length in the UDP header.
Recommended action	No action is required.

ATK_IP4_UDP_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IP address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 UDP packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_UDP_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Source IP address. $3: Destination IP address. $4: Name of the receiving VPN instance. $5: Rate limit. $6: Actions against the attack. $7: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_FLOOD_SZ:SrcZoneName(1025)=Trust;SrcIPAddr(1003)=2.3.3.1;DstIPAddr(1007)=6.1.1.5;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv4 UDP packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP4_UDP_FRAGGLE

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_FRAGGLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=11.
Explanation	This message is sent when logs are aggregated for IPv4 UDP packets with source port 7 and destination port 19.
Recommended action	No action is required.

ATK_IP4_UDP_FRAGGLE_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 UDP fraggle attack. The attack uses IPv4 UDP packets with source port 7 and destination port 19. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_UDP_FRAGGLE_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_FRAGGLE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 UDP fraggle attack. The attack uses IPv4 UDP packets with source port 7 and destination port 19. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_UDP_FRAGGLE_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_FRAGGLE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=11.
Explanation	This message is sent when logs are aggregated for IPv4 UDP packets with source port 7 and destination port 19.
Recommended action	No action is required.

ATK_IP4_UDP_SNORK

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_SNORK:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv4 UDP packets with source port 7, 19, or 135, and destination port 135.
Recommended action	No action is required.

ATK_IP4_UDP_SNORK_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_SNORK_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 UDP snork attack. The attack uses IPv4 UDP packets with source port 7, 19, or 135, and destination port 135. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_UDP_SNORK_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_SNORK_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv4 UDP snork attack. The attack uses IPv4 UDP packets with source port 7, 19, or 135, and destination port 135. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP4_UDP_SNORK_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP4_UDP_SNORK_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131011074913;EndTime_c(1012)=20131011075413;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv4 UDP packets with source port 7, 19, or 135, and destination port 135.
Recommended action	No action is required.

ATK_IP6_ACK_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_ACK_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 ACK packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_ACK_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_ACK_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 ACK packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_DIS_PORTSCAN

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Protocol name. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_DIS_PORTSCAN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=UDP;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009100928.
Explanation	This message is sent when an IPv6 distributed port scan attack is detected.
Recommended action	No action is required.

ATK_IP6_DIS_PORTSCAN_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Protocol name. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_DIS_PORTSCAN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009100928.
Explanation	This message is sent when an IPv6 distributed port scan attack is detected.
Recommended action	No action is required.

ATK_IP6_DNS_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_DNS_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 DNS queries sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_DNS_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rat limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_DNS_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 DNS queries sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_EXHEADER_ABNORMAL

Message text	SubModule(1127)=[STRING];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	5
Example	ATK/5/ATK_IP6_EXHEADER_ABNORMAL:SubModule(1127)=SINGLE;RcvIfName(1023)=Ethernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for abnormal IPv6 extension header attack packets.
Recommended action	No action is required.

ATK_IP6_EXHEADER_ABNORMAL_RAW

Message text	SubModule(1127)=[STRING];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: VPN instance name $6: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IP6_EXHEADER_ABNORMAL_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=Ethernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
Explanation	This message is for the abnormal IPv6 extension header attack. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_EXHEADER_ABNORMAL_RAW_SZ

Message text	SubModule(1127)=[STRING];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: VPN instance name. $6: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IP6_EXHEADER_ABNORMAL_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
Explanation	This message is for the abnormal IPv6 extension header attack. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_EXHEADER_ABNORMAL_SZ

Message text	SubModule(1127)=[STRING];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	5
Example	ATK/5/ATK_IP6_EXHEADER_ABNORMAL_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for abnormal IPv6 extension header attack packets.
Recommended action	No action is required.

ATK_IP6_EXHEADER_EXCEED

Message text	SubModule(1127)=[STRING];IPv6ExtHdrLimitValue(1142)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Upper limit of IPv6 extension headers. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_IP6_EXHEADER_EXCEED:SubModule(1127)=SINGLE;RcvIfName(1023)=Ethernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 extension header exceeded attack packets.
Recommended action	No action is required.

ATK_IP6_EXHEADER_EXCEED_RAW

Message text	SubModule(1127)=[STRING];IPv6ExtHdrLimitValue(1142)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Upper limit of IPv6 extension headers. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: VPN instance name. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IP6_EXHEADER_EXCEED_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=Ethernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
Explanation	This message is for the IPv6 extension header exceeded attack. This attack uses packets in which the number of extension headers exceeds the upper limit. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_EXHEADER_EXCEED_RAW_SZ

Message text	SubModule(1127)=[STRING];IPv6ExtHdrLimitValue(1142)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Upper limit of IPv6 extension headers. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: VPN instance name $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IP6_EXHEADER_EXCEED_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging.
Explanation	This message is for the IPv6 extension header exceeded attack. This attack uses packets in which the number of extension headers exceeds the upper limit. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_EXHEADER_EXCEED_SZ

Message text	SubModule(1127)=[STRING];IPv6ExtHdrLimitValue(1142)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Upper limit of IPv6 extension headers. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_IP6_EXHEADER_EXCEED_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=--;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 extension header exceeded attack packets.
Recommended action	No action is required.

ATK_IP6_FIN_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_FIN_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 FIN packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_FIN_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_FIN_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 FIN packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_FRAGMENT

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Protocol type. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	4
Example	ATK/3/ATK_IP6_FRAGMENT:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 packets with an offset smaller than 5 but bigger than 0.
Recommended action	No action is required.

ATK_IP6_FRAGMENT_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Protocol type. $7: Actions against the attack.
Severity level	4
Example	ATK/3/ATK_IP6_FRAGMENT_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging.
Explanation	This message is for the IPv6 fragment attack. The attack uses IPv6 packets with an offset smaller than 5 but bigger than 0. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_FRAGMENT_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Protocol type. $7: Actions against the attack.
Severity level	4
Example	ATK/3/ATK_IP6_FRAGMENT_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging.
Explanation	This message is for the IPv6 fragment attack. The attack uses IPv6 packets with an offset smaller than 5 but bigger than 0. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_FRAGMENT_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Protocol type. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	4
Example	ATK/3/ATK_IP6_FRAGMENT_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 packets with an offset smaller than 5 but bigger than 0.
Recommended action	No action is required.

ATK_IP6_HTTP_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_HTTP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 HTTP Get packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_HTTP_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_HTTP_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 HTTP Get packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_IMPOSSIBLE

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Protocol type. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_IMPOSSIBLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 packets whose source IPv6 address is the same as the destination IPv6 address.
Recommended action	No action is required.

ATK_IP6_IMPOSSIBLE_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Protocol type. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_IMPOSSIBLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging.
Explanation	This message is for the IPv6 impossible packet attack. The attack uses IPv6 packets whose source IPv6 address is the same as the destination IPv6 address. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_IMPOSSIBLE_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Protocol type. $7: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_IMPOSSIBLE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging.
Explanation	This message is for the IPv6 impossible packet attack. The attack uses IPv6 packets whose source IPv6 address is the same as the destination IPv6 address. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_IMPOSSIBLE_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Protocol type. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_IMPOSSIBLE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=1::1;RcvVPNInstance(1042)=;Protocol(1001)=IPv6-ICMP;Action(1053)=logging;BeginTime_c(1011)=20131011103335;EndTime_c(1012)=20131011103835;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 packets whose source IPv6 address is the same as the destination IPv6 address.
Recommended action	No action is required.

ATK_IP6_IPSWEEP

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Protocol name. $4: Source IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_IPSWEEP:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100639.
Explanation	This message is sent when an IPv6 sweep attack is detected.
Recommended action	No action is required.

ATK_IP6_IPSWEEP_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING]
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Protocol name. $4: Source IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_IPSWEEP_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100639.
Explanation	This message is sent when an IPv6 sweep attack is detected.
Recommended action	No action is required.

ATK_IP6_PORTSCAN

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];DstIPv6Addr(1037)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Protocol name. $4: Source IPv6 address. $5: Name of the receiving VPN instance. $6: Destination IPv6 address. $7: Actions against the attack. $8: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_PORTSCAN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;Protocol(1001)=UDP;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;DstIPv6Addr(1037)=2::2;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100455.
Explanation	This message is sent when an IPv6 port scan attack is detected.
Recommended action	No action is required.

ATK_IP6_PORTSCAN_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING];DstIPv6Addr(1037)=[IPADDR];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Protocol name. $4: Source IPv6 address. $5: Name of the receiving VPN instance. $6: Destination IPv6 address. $7: Actions against the attack. $8: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_PORTSCAN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;Protocol(1001)=TCP;SrcIPv6Addr(1036)=1::5;RcvVPNInstance(1042)=;DstIPv6Addr(1037)=2::2;Action(1053)=logging,block-source;BeginTime_c(1011)=20131009100455.
Explanation	This message is sent when an IPv6 port scan attack is detected.
Recommended action	No action is required.

ATK_IP6_RST_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_RST_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 RST packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_RST_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_RST_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 RST packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_SLOW_ATTACK

Message text	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_SLOW_ATTACK:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv6 HTTP slow attack packets sent to a destination within the detection period exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_SLOW_ATTACK_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_SLOW_ATTACK_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009093351.
Explanation	This message is sent when the number of IPv6 HTTP slow attack packets sent to a destination within the detection period exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_SYN_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_SYN_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 SYN packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_SYN_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_SYN_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 SYN packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_SYNACK_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_SYNACK_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 SYN-ACK packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_SYNACK_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_SYNACK_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 SYN-ACK packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_TCP_ALLFLAGS

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_ALLFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets that have all flags set.
Recommended action	No action is required.

ATK_IP6_TCP_ALLFLAGS_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 TCP packets that have all flags set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_ALLFLAGS_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_ALLFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 TCP packets that have all flags set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_ALLFLAGS_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_ALLFLAGS_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets that have all flags set.
Recommended action	No action is required.

ATK_IP6_TCP_FINONLY

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_FINONLY:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets that have only the FIN flag set.
Recommended action	No action is required.

ATK_IP6_TCP_FINONLY_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_FINONLY_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 TCP packets that have only the FIN flag set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_FINONLY_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_FINONLY_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 TCP packets that have only the FIN flag set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_FINONLY_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_FINONLY_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets that have only the FIN flag set.
Recommended action	No action is required.

ATK_IP6_TCP_INVALIDFLAGS

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_INVALIDFLAGS:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets that have invalid flag settings. Invalid flag settings include: • The RST and FIN flags are both set. • The RST and SYN flags are both set. • The RST, FIN, and SYN flags are all set. • The PSH, RST, and FIN flags are all set. • The PSH, RST, and SYN flags are all set. • The PSH, RST, SYN, and FIN flags are all set. • The ACK, RST, and FIN flags are all set. • The ACK, RST, and SYN flags are all set. • The ACK, RST, SYN, and FIN flags are all set. • The ACK, PSH, SYN, and FIN flags are all set. • The ACK, PSH, RST, and FIN flags are all set. • The ACK, PSH, RST, and SYN flags are all set.
Recommended action	No action is required.

ATK_IP6_TCP_INVALIDFLAGS_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 TCP packets that have invalid flag settings. Invalid flag settings include: • The RST and FIN flags are both set. • The RST and SYN flags are both set. • The RST, FIN, and SYN flags are all set. • The PSH, RST, and FIN flags are all set. • The PSH, RST, and SYN flags are all set. • The PSH, RST, SYN, and FIN flags are all set. • The ACK, RST, and FIN flags are all set. • The ACK, RST, and SYN flags are all set. • The ACK, RST, SYN, and FIN flags are all set. • The ACK, PSH, SYN, and FIN flags are all set. • The ACK, PSH, RST, and FIN flags are all set. • The ACK, PSH, RST, and SYN flags are all set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 TCP packets that have invalid flag settings. Invalid flag settings include: • The RST and FIN flags are both set. • The RST and SYN flags are both set. • The RST, FIN, and SYN flags are all set. • The PSH, RST, and FIN flags are all set. • The PSH, RST, and SYN flags are all set. • The PSH, RST, SYN, and FIN flags are all set. • The ACK, RST, and FIN flags are all set. • The ACK, RST, and SYN flags are all set. • The ACK, RST, SYN, and FIN flags are all set. • The ACK, PSH, SYN, and FIN flags are all set. • The ACK, PSH, RST, and FIN flags are all set. • The ACK, PSH, RST, and SYN flags are all set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_INVALIDFLAGS_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_INVALIDFLAGS_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets that have invalid flag settings. Invalid flag settings include: • The RST and FIN flags are both set. • The RST and SYN flags are both set. • The RST, FIN, and SYN flags are all set. • The PSH, RST, and FIN flags are all set. • The PSH, RST, and SYN flags are all set. • The PSH, RST, SYN, and FIN flags are all set. • The ACK, RST, and FIN flags are all set. • The ACK, RST, and SYN flags are all set. • The ACK, RST, SYN, and FIN flags are all set. • The ACK, PSH, SYN, and FIN flags are all set. • The ACK, PSH, RST, and FIN flags are all set. • The ACK, PSH, RST, and SYN flags are all set.
Recommended action	No action is required.

ATK_IP6_TCP_LAND

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_LAND:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets whose source IPv6 address is the same as the destination IPv6 address.
Recommended action	No action is required.

ATK_IP6_TCP_LAND_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_LAND_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the IPv6 land attack. The attack uses IPv6 TCP packets whose source IPv6 address is the same as the destination IPv6 address. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_LAND_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_LAND_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the IPv6 land attack. The attack uses IPv6 TCP packets whose source IPv6 address is the same as the destination IPv6 address. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_LAND_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_LAND_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets whose source IPv6 address is the same as the destination IPv6 address.
Recommended action	No action is required.

ATK_IP6_TCP_NULLFLAG

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_NULLFLAG:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets that have no flag set.
Recommended action	No action is required.

ATK_IP6_TCP_NULLFLAG_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 TCP packets that have no flag set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_NULLFLAG_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_NULLFLAG_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 TCP packets that have no flag set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_NULLFLAG_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_NULLFLAG_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets that have no flag set.
Recommended action	No action is required.

ATK_IP6_TCP_SYNFIN

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_SYNFIN:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets that have SYN and FIN flags set.
Recommended action	No action is required.

ATK_IP6_TCP_SYNFIN_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_SYNFIN_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 TCP packets that have SYN and FIN flags set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_SYNFIN_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_SYNFIN_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=2000::1;DstIPv6Addr(1037)=2003::200;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 TCP packets that have SYN and FIN flags set. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_SYNFIN_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $4: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_SYNFIN_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets that have SYN and FIN flags set.
Recommended action	No action is required.

ATK_IP6_TCP_WINNUKE

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_WINNUKE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets with destination port 139, the URG flag set, and a nonzero Urgent Pointer.
Recommended action	No action is required.

ATK_IP6_TCP_WINNUKE_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_WINNUKE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the IPv6 WinNuke attack. The attack uses IPv6 TCP packets with destination port 139, the URG flag set, and a nonzero Urgent Pointer. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_WINNUKE_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $5: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_WINNUKE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for the IPv6 WinNuke attack. The attack uses IPv6 TCP packets with destination port 139, the URG flag set, and a nonzero Urgent Pointer. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_TCP_WINNUKE_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_TCP_WINNUKE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 TCP packets with destination port 139, the URG flag set, and a nonzero Urgent Pointer.
Recommended action	No action is required.

ATK_IP6_UDP_FLOOD

Message text	RcvIfName(1023)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Receiving interface name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_UDP_FLOOD:RcvIfName(1023)=GigabitEthernet0/0/2;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 UDP packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_UDP_FLOOD_SZ

Message text	SrcZoneName(1025)=[STRING];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];UpperLimit(1049)=[UINT32];Action(1053)=[STRING];BeginTime_c(1011)=[STRING].
Variable fields	$1: Source security zone name. $2: Destination IPv6 address. $3: Name of the receiving VPN instance. $4: Rate limit. $5: Actions against the attack. $6: Start time of the attack.
Severity level	3
Example	ATK/3/ATK_IP6_UDP_FLOOD_SZ:SrcZoneName(1025)=Trust;DstIPv6Addr(1037)=2::2;RcvVPNInstance(1042)=;UpperLimit(1049)=10;Action(1053)=logging;BeginTime_c(1011)=20131009100434.
Explanation	This message is sent when the number of IPv6 UDP packets sent to a destination per second exceeds the rate limit.
Recommended action	No action is required.

ATK_IP6_UDP_FRAGGLE

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_UDP_FRAGGLE:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 UDP packets with source port 7 and destination port 19.
Recommended action	No action is required.

ATK_IP6_UDP_FRAGGLE_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 UDP fraggle attack. The attack uses IPv6 UDP packets with source port 7 and destination port 19. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_UDP_FRAGGLE_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_UDP_FRAGGLE_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 UDP fraggle attack. The attack uses IPv6 UDP packets with source port 7 and destination port 19. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_UDP_FRAGGLE_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_UDP_FRAGGLE_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 UDP packets with source port 7 and destination port 19.
Recommended action	No action is required.

ATK_IP6_UDP_SNORK

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_UDP_SNORK:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 UDP packets with source port 7, 19, or 135, and destination port 135.
Recommended action	No action is required.

ATK_IP6_UDP_SNORK_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_UDP_SNORK_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 UDP snork attack. The attack uses IPv6 UDP packets with source port 7, 19, or 135, and port 135. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_UDP_SNORK_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IP6_UDP_SNORK_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	This message is for IPv6 UDP snork attack. The attack uses IPv6 UDP packets with source port 7, 19, or 135, and port 135. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet is received.
Recommended action	No action is required.

ATK_IP6_UDP_SNORK_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Name of the receiving VPN instance. $6: Actions against the attack. $7: Start time of the attack. $8: End time of the attack. $9: Attack times.
Severity level	3
Example	ATK/3/ATK_IP6_UDP_SNORK_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 UDP packets with source port 7, 19, or 135, and destination port 135.
Recommended action	No action is required.

ATK_IPOPT_ABNORMAL

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	3
Example	ATK/3/ATK_IPOPT_ABNORMAL:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011072002;EndTime_c(1012)=20131011072502;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with more than two IP options.
Recommended action	No action is required.

ATK_IPOPT_ABNORMAL_RAW

Message text	SubModule(1127)=SINGLE;RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Receiving interface name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IPOPT_ABNORMAL_RAW:SubModule(1127)=SINGLE;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	This message is for packets that each has more than two IP options. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with more than two IP options is received.
Recommended action	No action is required.

ATK_IPOPT_ABNORMAL_RAW_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack.
Severity level	3
Example	ATK/3/ATK_IPOPT_ABNORMAL_RAW_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	This message is for packets that each has more than two IP options. If log aggregation is enabled, for packets of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with more than two IP options is received.
Recommended action	No action is required.

ATK_IPOPT_ABNORMAL_SZ

Message text	SubModule(1127)=SINGLE;SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: Source security zone name. $3: Source IP address. $4: IP address of the peer DS-Lite tunnel interface. $5: Destination IP address. $6: Name of the receiving VPN instance. $7: Protocol type. $8: Actions against the attack. $9: Start time of the attack. $10: End time of the attack. $11: Attack times.
Severity level	3
Example	ATK/3/ATK_IPOPT_ABNORMAL_SZ:SubModule(1127)=SINGLE;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011072002;EndTime_c(1012)=20131011072502;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with more than two IP options.
Recommended action	No action is required.

ATK_IPOPT_LOOSESRCROUTE

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)= [UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_LOOSESRCROUTE:SubModule(1127)=SINGLE;IPOptValue(1061)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 131.
Recommended action	No action is required.

ATK_IPOPT_LOOSESRCROUTE_RAW

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=131;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 131 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 131 is received.
Recommended action	No action is required.

ATK_IPOPT_LOOSESRCROUTE_RAW_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_LOOSESRCROUTE_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=131;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 131 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 131 is received.
Recommended action	No action is required.

ATK_IPOPT_LOOSESRCROUTE_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)= [UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_LOOSESRCROUTE_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=131;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 131.
Recommended action	No action is required.

ATK_IPOPT_RECORDROUTE

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_RECORDROUTE:SubModule(1127)=SINGLE;IPOptValue(1061)=7;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 7.
Recommended action	No action is required.

ATK_IPOPT_RECORDROUTE_RAW

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_RECORDROUTE_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=7;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 7 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 7 is received.
Recommended action	No action is required.

ATK_IPOPT_RECORDROUTE_RAW_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_RECORDROUTE_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=7;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 7 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 7 is received.
Recommended action	No action is required.

ATK_IPOPT_RECORDROUTE_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_RECORDROUTE_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=7;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 7.
Recommended action	No action is required.

ATK_IPOPT_ROUTEALERT

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_ROUTEALERT:SubModule(1127)=SINGLE;IPOptValue(1061)=148;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 148.
Recommended action	No action is required.

ATK_IPOPT_ROUTEALERT_RAW

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_ROUTEALERT_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=148;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 148 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 148 is received.
Recommended action	No action is required.

ATK_IPOPT_ROUTEALERT_RAW_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_ROUTEALERT_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=148;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 148 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 148 is received.
Recommended action	No action is required.

ATK_IPOPT_ROUTEALERT_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_ROUTEALERT_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=148;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 148.
Recommended action	No action is required.

ATK_IPOPT_SECURITY

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_SECURITY:SubModule(1127)=SINGLE;IPOptValue(1061)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131009091022;EndTime_c(1012)=20131009091522;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for packets with IP option 130.
Recommended action	No action is required.

ATK_IPOPT_SECURITY_RAW

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_SECURITY_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=130;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 130 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 130 is received.
Recommended action	No action is required.

ATK_IPOPT_SECURITY_RAW_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_SECURITY_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=130;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 130 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 130 is received.
Recommended action	No action is required.

ATK_IPOPT_SECURITY_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_SECURITY_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=130;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131009091022;EndTime_c(1012)=20131009091522;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for packets with IP option 130.
Recommended action	No action is required.

ATK_IPOPT_STREAMID

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_STREAMID:SubModule(1127)=SINGLE;IPOptValue(1061)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 136.
Recommended action	No action is required.

ATK_IPOPT_STREAMID_RAW

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_STREAMID_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=136;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 136 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 136 is received.
Recommended action	No action is required.

ATK_IPOPT_STREAMID_RAW_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_STREAMID_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=136;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 136 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 136 is received.
Recommended action	No action is required.

ATK_IPOPT_STREAMID_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_STREAMID_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=136;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 136.
Recommended action	No action is required.

ATK_IPOPT_STRICTSRCROUTE

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_STRICTSRCROUTE:SubModule(1127)=SINGLE;IPOptValue(1061)=137;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 137.
Recommended action	No action is required.

ATK_IPOPT_STRICTSRCROUTE_RAW

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=137;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 137 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 137 is received.
Recommended action	No action is required.

ATK_IPOPT_STRICTSRCROUTE_RAW_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_STRICTSRCROUTE_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=137;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 137 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 137 is received.
Recommended action	No action is required.

ATK_IPOPT_STRICTSRCROUTE_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_STRICTSRCROUTE_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=137;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 137.
Recommended action	No action is required.

ATK_IPOPT_TIMESTAMP

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_TIMESTAMP:SubModule(1127)=SINGLE;IPOptValue(1061)=68;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 68.
Recommended action	No action is required.

ATK_IPOPT_TIMESTAMP_RAW

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];RcvIfName(1023)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Receiving interface name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_TIMESTAMP_RAW:SubModule(1127)=SINGLE;IPOptValue(1061)=68;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 68 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 68 is received.
Recommended action	No action is required.

ATK_IPOPT_TIMESTAMP_RAW_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPOPT_TIMESTAMP_RAW_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=68;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging.
Explanation	If log aggregation is enabled, for packets with IP option 68 and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time a packet with IP option 68 is received.
Recommended action	No action is required.

ATK_IPOPT_TIMESTAMP_SZ

Message text	SubModule(1127)=SINGLE;IPOptValue(1061)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPAddr(1003)=[IPADDR];SndDSLiteTunnelPeer(1041)=[STRING];DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];Protocol(1001)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IP option value. $3: Source security zone name. $4: Source IP address. $5: IP address of the peer DS-Lite tunnel interface. $6: Destination IP address. $7: Name of the receiving VPN instance. $8: Protocol type. $9: Actions against the attack. $10: Start time of the attack. $11: End time of the attack. $12: Attack times.
Severity level	5
Example	ATK/5/ATK_IPOPT_TIMESTAMP_SZ:SubModule(1127)=SINGLE;IPOptValue(1061)=68;SrcZoneName(1025)=Trust;SrcIPAddr(1003)=9.1.1.1;SndDSLiteTunnelPeer(1041)=--;DstIPAddr(1007)=6.1.1.1;RcvVPNInstance(1042)=;Protocol(1001)=RAWIP;Action(1053)=logging;BeginTime_c(1011)=20131011063123;EndTime_c(1012)=20131011063623;AtkTimes(1054)=3.
Explanation	This message is sent when logs are aggregated for packets with IP option 68.
Recommended action	No action is required.

ATK_IPV6_EXT_HEADER

Message text	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IPv6 extension header value. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_IPV6_EXT_HEADER:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 packets with a user-defined extension header.
Recommended action	No action is required.

ATK_IPV6_EXT_HEADER _RAW

Message text	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IPv6 extension header value. $3: Receiving interface name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPV6_EXT_HEADER_RAW:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;RcvIfName(1023)=GigabitEthernet0/0/2;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for IPv6 packets with a user-defined extension header and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an IPv6 packet with a user-defined extension header is received.
Recommended action	No action is required.

ATK_IPV6_EXT_HEADER_RAW_SZ

Message text	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Sub module name. $2: IPv6 extension header value. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack.
Severity level	5
Example	ATK/5/ATK_IPV6_EXT_HEADER_RAW_SZ:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging.
Explanation	If log aggregation is enabled, for IPv6 packets with a user-defined extension header and of the same attributes, this message is sent only when the first packet is received. If log aggregation is disabled, this message is sent every time an IPv6 packet with a user-defined extension header is received.
Recommended action	No action is required.

ATK_IPV6_EXT_HEADER_SZ

Message text	SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=[UINT32];SrcZoneName(1025)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING];Action(1053)=[STRING];BeginTime_c(1011)=[STRING];EndTime_c(1012)=[STRING];AtkTimes(1054)=[UINT32].
Variable fields	$1: Sub module name. $2: IPv6 extension header value. $3: Source security zone name. $4: Source IPv6 address. $5: Destination IPv6 address. $6: Name of the receiving VPN instance. $7: Actions against the attack. $8: Start time of the attack. $9: End time of the attack. $10: Attack times.
Severity level	5
Example	ATK/5/ATK_IPV6_EXT_HEADER_SZ:SubModule(1127)=SINGLE;IPv6ExtHeader(1066)=43;SrcZoneName(1025)=Trust;SrcIPv6Addr(1036)=1::1;DstIPv6Addr(1037)=2::11;RcvVPNInstance(1042)=;Action(1053)=logging;BeginTime_c(1011)=20131009103631;EndTime_c(1012)=20131009104131;AtkTimes(1054)=2.
Explanation	This message is sent when logs are aggregated for IPv6 packets with a user-defined extension header.
Recommended action	No action is required.

ATM

This section contains ATM messages.

ATM_PVCDOWN

Message text	Interface [STRING] PVC [UINT16]/[UINT16] status is down.
Variable fields	$1: Name of the interface to which the PVC belongs. $2: VPI value of the PVC. $3: VCI value of the PVC.
Severity level	5
Example	ATM/5/ATM_PVCDOWN: Interface ATM2/0/2 PVC 0/100 status is down.
Explanation	The PVC state became down. Possible reasons include the following: • The ATM interface to which the PVC belongs went down. • The OAM state of the PVC became down. • The PVC had been manually shut down.

Recommended action	Use the **display atm pvc-info** command to display detailed information about the PVC and take relevant actions:
	• If the interface state is down, take the following actions:
	  ○ Make sure both the local and remote ATM interfaces are up by using the **display interface atm** command. If the interfaces have been manually shut down, execute the **undo shutdown** command in interface view to bring them up.
	  ○ Make sure the two interfaces are correctly connected.
	• If the OAM state is down, take the following actions:
	  ○ Make sure the VPI/VCI value of the remote PVC is the same as the VPI/VCI value of the local PVC.
	  ○ Make sure the OAM configuration of the remote PVC is consistent with the OAM configuration of the local PVC. For example, if one end is configured as the OAM CC cell sink, the other end must be configured as the OAM CC cell source.
	  ○ Make sure the remote PVC is up. If the remote PVC has been manually shut down, execute the **undo shutdown** command in PVC view to bring it up.
	  ○ Make sure the two ends are correctly connected.
	  ○ If the two routers are connected through an ATM network, in addition to the previous check items, you must check the forwarding rule of the ATM network. If the ATM network cannot reach the PVC, the PVC cannot come up.
	• If the PVC state is down, check if the local PVC has been manually shut down. To bring up the PVC, execute the **undo shutdown** command in PVC view.

ATM_PVCUP

Message text	Interface [STRING] PVC [UINT16]/[UINT16] status is up.
Variable fields	$1: Name of the interface to which the PVC belongs. $2: VPI value of the PVC. $3: VCI value of the PVC.
Severity level	5
Example	ATM/5/ATM_PVCUP: Interface ATM2/0/2 PVC 0/100 status is up.
Explanation	The PVC state became up.
Recommended action	No action is required.

AUDIT messages

This section contains application audit and management messages.

AUDIT_RULE_MATCH_AS_IPV4_LOG (system log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Destination IPv4 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Account. $14: Content $15: Client type. $16: Application software version. $17: Action name: Permit or Deny. $18: VLAN ID. $19: VXLAN ID. $20: Source location. $21: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_AS_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=tonghuashun;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for an entertainment or stock application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_FILE_IPV4_LOG (system log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],FileName(1097)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Destination IPv4 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Account. $14: File name $15: Client type. $16: Application software version. $17: Action name: Permit or Deny. $18: VLAN ID. $19: VXLAN ID. $20: Source location. $21: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_FILE_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=ftp;Behavior(1101)=UploadFile;BehaviorContent(1102)={Account(1103)=ghj123,FileName(1097)=abc.txt};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for a file transfer application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_FORUM_IPV4_LOG (system log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Destination IPv4 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Account. $14: Content. $15: Client type. $16: Application software version. $17: Action name: Permit or Deny. $18: VLAN ID. $19: VXLAN ID. $20: Source location. $21: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_FORUM_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=SinaWeibo;Behavior(1101)=Comment;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for a social networking application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_IM_IPV4_LOG (system log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING],FileName(1097)=[STRING],FileSize(1105)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Destination IPv4 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Account. $14: Content. $15: File name. $16: File size. $17: Client type. $18: Application software version. $19: Action name: Permit or Deny. $20: VLAN ID. $21: VXLAN ID. $22: Source location. $23: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_IM_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=QQ;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=12345678,Content(1104)=test,FileName(1097)=text,FileSize(1105)=152389};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for an IM application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_MAIL_IPV4_LOG (system log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Sender_addr(1106)=[STRING],Receiver_addr(1107)=[STRING],Subject(1108)=[STRING],Body(1109)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Destination IPv4 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Sender. $14: Receiver. $15: Subject. $16: Body. $17: Client type. $18: Application software version. $19: Action name: Permit or Deny. $20: VLAN ID. $21: VXLAN ID. $22: Source location. $23: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_MAIL_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=smtp;Behavior(1101)=SendMail;BehaviorContent(1102)={Sender_addr(1106)="wb"<wb@ubuntu.wb>,Receiver_addr(1107)=<wb@ubuntu.wb>,Subject(1108)=test,Body(1109)=abc};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for an email application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_OTHER_IPV4_LOG (system log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Password(1112)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)= [STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Destination IPv4 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Account. $14: Password. $15: Content. $16: Client type. $17: Application software version. $18: Action name: Permit or Deny. $19: VLAN ID. $20: VXLAN ID. $21: Source location. $22: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_OTHER_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=Telnet;Behavior(1101)=Download;BehaviorContent(1102)={Account(1103)=hjk123456,Password(1112)=hhh123,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for an unclassified application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_SEARCH_IPV4_LOG (system log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Keyword(1095)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Destination IPv4 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Keyword. $14: Client type. $15: Application software version. $16: Action name: Permit or Deny. $17: VLAN ID. $18: VXLAN ID. $19: Source location. $20: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_SEARCH_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=BaiduSearch;Behavior(1101)=Search;BehaviorContent(1102)={Keyword(1095)=12345678};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for a search engine application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_AS_IPV4_LOG (fast log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Source IPv4 address after NAT. $5: Source port number after NAT. $6: Destination IPv4 address. $7: Destination port number. $8: Destination IPv4 address after NAT. $9: Destination port number after NAT. $10: Source security zone name. $11: Destination security zone name. $12: Username. $13: Application audit and management policy name. $14: Application name. $15: Application behavior. $16: Application behavior content. $17: Account. $18: Content $19: Client type. $20: Application software version. $21: Action name: Permit or Deny. $22: VLAN ID. $23: VXLAN ID. $24: Source location. $25: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_AS_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=tonghuashun;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for an entertainment or stock application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_FILE_IPV4_LOG (fast log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],FileName(1097)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Source IPv4 address after NAT. $5: Source port number after NAT. $6: Destination IPv4 address. $7: Destination port number. $8: Destination IPv4 address after NAT. $9: Destination port number after NAT. $10: Source security zone name. $11: Destination security zone name. $12: Username. $13: Application audit and management policy name. $14: Application name. $15: Application behavior. $16: Application behavior content. $17: Account. $18: File name $19: Client type. $20: Application software version. $21: Action name: Permit or Deny. $22: VLAN ID. $23: VXLAN ID. $24: Source location. $25: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_FILE_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=ftp;Behavior(1101)=UploadFile;BehaviorContent(1102)={Account(1103)=ghj123,FileName(1097)=abc.txt};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for a file

	transfer application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_FORUM_IPV4_LOG (fast log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Source IPv4 address after NAT. $5: Source port number after NAT. $6: Destination IPv4 address. $7: Destination port number. $8: Destination IPv4 address after NAT. $9: Destination port number after NAT. $10: Source security zone name. $11: Destination security zone name. $12: Username. $13: Application audit and management policy name. $14: Application name. $15: Application behavior. $16: Application behavior content. $17: Account. $18: Content. $19: Client type. $20: Application software version. $21: Action name: Permit or Deny. $22: VLAN ID. $23: VXLAN ID. $24: Source location. $25: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_FORUM_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=SinaWeibo;Behavior(1101)=Comment;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for a

	social networking application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_IM_IPV4_LOG (fast log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING],FileName(1097)=[STRING],FileSize(1105)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Source IPv4 address after NAT. $5: Source port number after NAT. $6: Destination IPv4 address. $7: Destination port number. $8: Destination IPv4 address after NAT. $9: Destination port number after NAT. $10: Source security zone name. $11: Destination security zone name. $12: Username. $13: Application audit and management policy name. $14: Application name. $15: Application behavior. $16: Application behavior content. $17: Account. $18: Content. $19: File name. $20: File size. $21: Client type. $22: Application software version. $23: Action name: Permit or Deny. $24: VLAN ID. $25: VXLAN ID. $26: Source location. $27: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_IM_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=QQ;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=12345678,Content(1104)=test,FileName(1097)=text,FileSize(1105)=152389};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;

Explanation	This message is generated when an IPv4 packet matches an audit rule for an IM application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_MAIL_IPV4_LOG (fast log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Sender_addr(1106)=[STRING],Receiver_addr(1107)=[STRING],Subject(1108)=[STRING],Body(1109)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Source IPv4 address after NAT. $5: Source port number after NAT. $6: Destination IPv4 address. $7: Destination port number. $8: Destination IPv4 address after NAT. $9: Destination port number after NAT. $10: Source security zone name. $11: Destination security zone name. $12: Username. $13: Application audit and management policy name. $14: Application name. $15: Application behavior. $16: Application behavior content. $17: Sender. $18: Receiver. $19: Subject. $20: Body. $21: Client type. $22: Application software version. $23: Action name: Permit or Deny. $24: VLAN ID. $25: VXLAN ID. $26: Source location. $27: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_MAIL_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=smtp;Behavior(1101)=SendMail;BehaviorContent(1102)={Sender_addr(1106)="wb"<wb@ubuntu.wb>,Receiver_addr(1107)=<wb@ubuntu.wb>,Subject(1108)=test,Body(1109)=abc};Client(1110)=PC;SoftVersion(

	1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for an email application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_OTHER_IPV4_LOG (fast log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Password(1112)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Source IPv4 address after NAT. $5: Source port number after NAT. $6: Destination IPv4 address. $7: Destination port number. $8: Destination IPv4 address after NAT. $9: Destination port number after NAT. $10: Source security zone name. $11: Destination security zone name. $12: Username. $13: Application audit and management policy name. $14: Application name. $15: Application behavior. $16: Application behavior content. $17: Account. $18: Password. $19: Content. $20: Client type. $21: Application software version. $22: Action name: Permit or Deny. $23: VLAN ID. $24: VXLAN ID. $25: Source location. $26: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_OTHER_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=Telnet;Behavior(1101)=Download;BehaviorContent(1102)={Account(1103)=hjk123456,Password(1112)=hhh123,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;

Explanation	This message is generated when an IPv4 packet matches an audit rule for an unclassified application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_SEARCH_IPV4_LOG (fast log)

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Keyword(1095)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Source IPv4 address after NAT. $5: Source port number after NAT. $6: Destination IPv4 address. $7: Destination port number. $8: Destination IPv4 address after NAT. $9: Destination port number after NAT. $10: Source security zone name. $11: Destination security zone name. $12: Username. $13: Application audit and management policy name. $14: Application name. $15: Application behavior. $16: Application behavior content. $17: Keyword. $18: Client type. $19: Application software version. $20: Action name: Permit or Deny. $21: VLAN ID. $22: VXLAN ID. $23: Source location. $24: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_SEARCH_IPV4_LOG:Protocol(1001)=TCP;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;NATSrcIPAddr(1005)=200.20.20.2;NATSrcPort(1006)=50753;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;NATDstIPAddr(1009)=192.168.56.2;NATDstPort(1010)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=BaiduSearch;Behavior(1101)=Search;BehaviorContent(1102)={Keyword(1095)=12345678};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv4 packet matches an audit rule for a search engine application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_AS_IPV6_LOG (system log) (fast log)

Message text	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv6 address. $3: Source port number. $4: Destination IPv6 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Account. $14: Content $15: Client type. $16: Application software version. $17: Action name: Permit or Deny. $18: VLAN ID. $19: VXLAN ID. $20: Source location. $21: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_AS_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=tonghuashun;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv6 packet matches an audit rule for an entertainment or stock application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_FILE_IPV6_LOG (system log) (fast log)

Message text	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],FileName(1097)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv6 address. $3: Source port number. $4: Destination IPv6 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Account. $14: File name $15: Client type. $16: Application software version. $17: Action name: Permit or Deny. $18: VLAN ID. $19: VXLAN ID. $20: Source location. $21: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_FILE_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=ftp;Behavior(1101)=UploadFile;BehaviorContent(1102)={Account(1103)=ghj123,FileName(1097)=abc.txt};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv6 packet matches an audit rule for a file transfer application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_FORUM_IPV6_LOG (system log) (fast log)

Message text	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv6 address. $3: Source port number. $4: Destination IPv6 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Account. $14: Content. $15: Client type. $16: Application software version. $17: Action name: Permit or Deny. $18: VLAN ID. $19: VXLAN ID. $20: Source location. $21: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_FORUM_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=SinaWeibo;Behavior(1101)=Comment;BehaviorContent(1102)={Account(1103)=hjk123456,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv6 packet matches an audit rule for a social networking application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_IM_IPV6_LOG (system log) (fast log)

Message text	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Content(1104)=[STRING],FileName(1097)=[STRING],FileSize(1105)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv6 address. $3: Source port number. $4: Destination IPv6 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Account. $14: Content. $15: File name. $16: File size. $17: Client type. $18: Application software version. $19: Action name: Permit or Deny. $20: VLAN ID. $21: VXLAN ID. $22: Source location. $23: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_IM_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=QQ;Behavior(1101)=Login;BehaviorContent(1102)={Account(1103)=12345678,Content(1104)=test,FileName(1097)=text,FileSize(1105)=152389};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv6 packet matches an audit rule for an IM application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_MAIL_IPV6_LOG (system log) (fast log)

Message text	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Sender_addr(1106)=[STRING],Receiver_addr(1107)=[STRING],Subject(1108)=[STRING],Body(1109)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv6 address. $3: Source port number. $4: Destination IPv6 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Sender. $14: Receiver. $15: Subject. $16: Body. $17: Client type. $18: Application software version. $19: Action name: Permit or Deny. $20: VLAN ID. $21: VXLAN ID. $22: Source location. $23: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_MAIL_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=smtp;Behavior(1101)=SendMail;BehaviorContent(1102)={Sender_addr(1106)="wb"<wb@ubuntu.wb>,Receiver_addr(1107)=<wb@ubuntu.wb>,Subject(1108)=test,Body(1109)=abc};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv6 packet matches an audit rule for an email application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_OTHER_IPV6_LOG (system log) (fast log)

Message text	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Account(1103)=[STRING],Password(1112)=[STRING],Content(1104)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv6 address. $3: Source port number. $4: Destination IPv6 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Account. $14: Password. $15: Content. $16: Client type. $17: Application software version. $18: Action name: Permit or Deny. $19: VLAN ID. $20: VXLAN ID. $21: Source location. $22: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_OTHER_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=Telnet;Behavior(1101)=Download;BehaviorContent(1102)={Account(1103)=hjk123456,Password(1112)=hhh123,Content(1104)=hello};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv6 packet matches an audit rule for an unclassified application.
Recommended action	No action is required.

AUDIT_RULE_MATCH_SEARCH_IPV6_LOG (system log) (fast log)

Message text	Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];PolicyName(1079)=[STRING];Application(1002)=[STRING];Behavior(1101)=[STRING];BehaviorContent(1102)={Keyword(1095)=[STRING]};Client(1110)=[STRING];SoftVersion(1111)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Source IPv4 address. $3: Source port number. $4: Destination IPv4 address. $5: Destination port number. $6: Source security zone name. $7: Destination security zone name. $8: Username. $9: Application audit and management policy name. $10: Application name. $11: Application behavior. $12: Application behavior content. $13: Keyword. $14: Client type. $15: Application software version. $16: Action name: Permit or Deny. $17: VLAN ID. $18: VXLAN ID. $19: Source location. $20: Destination location.
Severity level	6
Example	AUDIT/6/AUDIT_RULE_MATCH_SEARCH_IPV6_LOG:Protocol(1001)=TCP;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=hjp;PolicyName(1079)=policy1;Application(1002)=BaiduSearch;Behavior(1101)=Search;BehaviorContent(1102)={Keyword(1095)=12345678};Client(1110)=PC;SoftVersion(1111)=;Action(1053)=Deny;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated when an IPv6 packet matches an audit rule for a search engine application.
Recommended action	No action is required.

AUTOCFG messages

This section contains automatic configuration messages.

AUTOCFG_URL_EXECUTE_FAILURE

Message text	URL-based automatic configuration failed at command line [STRING] and stopped.
Variable fields	$1: Command line that failed to be executed.
Severity level	4
Example	AUTOCFG/4/AUTOCFG_URL_EXECUTE_FAILURE: URL-based automatic configuration failed at command line "system-view" and stopped.
Explanation	The automatic configuration process stopped at a command line that failed to be executed. The following command lines were not executed.
Recommended action	Record the log message and contact the technical support.

AUTOCFG_URL_EXECUTE_SUCCESS

Message text	URL-based automatic configuration finished successfully.
Variable fields	None
Severity level	6
Example	AUTOCFG/6/AUTOCFG_URL_EXECUTE_SUCCESS: URL-based automatic configuration finished successfully.
Explanation	A URL-based automatic configuration process finished successfully.
Recommended action	No action is required.

AUTOCFG_URL_START_FAILED

Message text	URL-based automatic configuration service by [STRING] from [STRING] failed.
Variable fields	$1: Username. $2: IP address.
Severity level	5
Example	AUTOCFG/6/AUTOCFG_URL_START_FAILED: URL-based automatic configuration service by admin from 192.168.111.250 failed.
Explanation	A user failed to start URL-based automatic device configuration.
Recommended action	Verify that the username and password are correct.

AUTOCFG_URL_START_SUCCESS

Message text	URL-based automatic configuration started by [STRING] from [STRING].
Variable fields	$1: Username. $2: IP address.
Severity level	6
Example	AUTOCFG/6/AUTOCFG_URL_START_SUCCESS: URL-based automatic configuration started by admin from 192.168.111.250.
Explanation	A user started URL-based automatic device configuration successfully.
Recommended action	No action is required.

AVC messages

This section contains bandwidth management messages.

AVC_MATCH_IPV4_LOG

Message text	Application(1002)=[STRING];UserName(1113)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[USHORT];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[USHORT];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];VistTime(1114)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Application name. $2: User name. $3: Source IPv4 address. $4: Source port number. $5: Destination IPv4 address. $6: Destination port number. $7: Source security zone. $8: Destination security zone. $9: Policy name. $10: Hit time. $11: Rule action. $12: VLAN ID. $13: VXLAN ID. $14: Source location. $15: Destination location.
Severity level	6
Example	AVC/6/AVC_MATCH_IPV4_LOG:Application(1002)=App;UserName(1113)=User1;SrcIPAddr(1003)=12.2.2.2;SrcPort(1004)=5141;DstIPAddr(1007)=13.1.1.14;DstPort(1008)=5784;SrcZoneName(1025)=whx;DstZoneName(1035)=hea;PolicyName(1079)=aaa;VistTime(1114)=Wed, 22 May 2019 16:43:47;Action(1053)=drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated and sent to the log host as a fast output log when a packet matches a traffic rule.
Recommended action	None.

AVC_MATCH_IPV6_LOG

Message text	Application(1002)=[STRING];UserName(1113)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[USHORT];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[USHORT];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];VistTime(1114)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Application name. $2: User name. $3: Source IPv6 address. $4: Source port number. $5: Destination IPv6 address. $6: Destination port number. $7: Source security zone. $8: Destination security zone. $9: Policy name. $10: Hit time. $11: Rule action. $12: VLAN ID. $13: VXLAN ID. $14: Source location. $15: Destination location.
Severity level	6
Example	AVC/6/AVC_MATCH_IPV6_LOG:Application(1002)=App;UserName(1113)=User1;SrcIPv6Addr(1036)=12::2;SrcPort(1004)=5141;DstIPv6Addr(1037)=13::4;DstPort(1008)=5784;SrcZoneName(1025)=whx;DstZoneName(1035)=hea;PolicyName(1079)=aaa;VistTime(1114)= Wed, 22 May 2019 16:52:08; Action(1053)=drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is generated and sent to the log host as a fast output log when a packet matches a traffic rule.
Recommended action	None.

AVC_THRESHOLDWARNING_FASTLOGGING_FMT

Message text	SrcIPAddr(1003)=[IPADDR];PolicyName(1079)=[STRING];ProfileName(1158)=[STRING];DeviceInfo(1159)=[STRING];BandwidthUpperLimit(1160)=[UINT32];BandwidthLowerLimit(1161)=[UINT32];UpperWarningValue(1162)=[UINT32];LowerWarningValue(1163)=[UINT32];CurRateValue(1164)=[UINT32];WarningTime(1165)=[STRING];WarningDuration(1166)=[UINT32];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];
Variable fields	$1: Source IPv4 address. $2: Traffic policy name. $3: Traffic profile name. $4: Device information. $5: Maximum bandwidth threshold in kbps. $6: Minimum bandwidth threshold in kbps. $7: Actual rate in kbps that exceeds the maximum bandwidth threshold. $8: Actual rate in kbps that falls below the minimum bandwidth threshold. $9: Current traffic rate in kbps. $10: Warning time when the device detected a threshold violation. $11: Warning duration. (length of time the threshold violation lasted). $12: VLAN ID. $13: VXLAN ID. $14: Source location.
Severity level	6
Example	AVC/6/AVC_THRESHOLDWARNING_FASTLOGGING_FMT:SrcIPAddr(1003)=192.168.1.8;PolicyName(1079)=a;ProfileName(1158)=p;DeviceInfo(1159)=YuShi;BandwidthUpperLimit(1160)=8366;BandwidthLowerLimit(1161)=2091;UpperWarningValue(1162)=6;LowerWarningValue(1163)=6;CurRateValue(1164)=6;WarningTime(1165)=Fri, 8 Oct 2019 17:38:32;WarningDuration(1166)=7;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;
Explanation	This message is generated and sent to the log host as a fast output log if a threshold violation occurs one minute or more after the previous threshold violation.
Recommended action	None.

AVC_THRESHOLDWARNING_FASTLOGGING_IPV6FMT

Message text	SrcIPv6Addr(1036)=[IPADDR];PolicyName(1079)=[STRING];ProfileName(1158)=[STRING];DeviceInfo(1159)=[STRING];BandwidthUpperLimit(1160)=[UINT32];BandwidthLowerLimit(1161)=[UINT32];UpperWarningValue(1162)=[UINT32];LowerWarningValue(1163)=[UINT32];CurRateValue(1164)=[UINT32];WarningTime(1165)=[STRING];WarningDuration(1166)=[UINT32];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];Location(1209)=[STRING];
Variable fields	$1: Source IPv6 address. $2: Traffic policy name. $3: Traffic profile name. $4: Device information. $5: Maximum bandwidth threshold in kbps. $6: Minimum bandwidth threshold in kbps. $7: Actual rate in kbps that exceeds the maximum bandwidth threshold. $8: Actual rate in kbps that falls below the minimum bandwidth threshold. $9: Current traffic rate in kbps. $10: Warning time (time when the device detected a threshold violation). $11: Warning duration (length of time the threshold violation lasted). $12: VLAN ID. $13: VXLAN ID. $14: Location.
Severity level	6
Example	AVC/6/AVC_THRESHOLDWARNING_FASTLOGGING_IPV6FMT:SrcIPv6Addr(1036)=2001::1;PolicyName(1079)=a;ProfileName(1158)=p;DeviceInfo(1159)=YuShi;BandwidthUpperLimit(1160)=8366;BandwidthLowerLimit(1161)=2091;UpperWarningValue(1162)=6;LowerWarningValue(1163)=6;CurRateValue(1164)=6;WarningTime(1165)=Fri, 8 Oct 2019 17:38:32;WarningDuration(1166)=7;VlanID(1175)=400;VNI(1213)=--;Location(1209)=China Macao;
Explanation	This message is generated and sent to the log host as a fast output log if a threshold violation occurs more than one minute after the previous threshold violation occurred.
Recommended action	None.

BFD messages

This section contains BFD messages.

BFD_CHANGE_FSM

Message text	Sess[STRING], Ver, Sta: [STRING]->[STRING], Diag: [STRING]
Variable fields	$1: Source address, destination address, interface, and message type of the BFD session. $2: Name of FSM before changing. $3: Name of FSM after changing. $4: Diagnostic information: • **0 (No Diagnostic)**. • **1 (Control Detection Time Expired)**—A control-mode BFD session goes down, because local detection times out. • **2 (Echo Function Failed)**—An echo-mode BFD session goes down, because local detection times out or the source IP address of echo packets is deleted. • **3 (Neighbor Signaled Session Down)**—The remote end notifies the local end of BFD session down. • **7 (Administratively Down)**—The BFD session is shut down administratively on the local end.
Severity level	5
Example	BFD/5/BFD_CHANGE_FSM:Sess[20.0.4.2/20.0.4.1,LD/RD:533/532, Interface:Vlan204, SessType:Ctrl, LinkType:INET], Ver.1, Sta: INIT->UP, Diag: 0 (No Diagnostic).
Explanation	The FSM of the BFD session has been changed. This informational message appears when a BFD session comes up or goes down. Unexpected session loss might indicate high error or packet loss rates in the network.
Recommended action	Check for incorrect BFD configuration or network congestion.

BFD_REACHED_UPPER_LIMIT

Message text	The total number of BFD sessions [ULONG] reached the upper limit. Can't create a new session.
Variable fields	$1: Total number of BFD sessions.
Severity level	5
Example	BFD/5/BFD_REACHED_UPPER_LIMIT: The total number of BFD session 100 reached upper limit.
Explanation	The total number of BFD sessions has reached the upper limit.
Recommended action	Check the BFD session configuration.

BGP messages

This section contains BGP messages.

BGP_EXCEED_ROUTE_LIMIT

Message text	BGP.[STRING]: The number of routes from peer [STRING] ([STRING]) exceeds the limit [UINT32].
Variable fields	$1: VPN instance name. This field is blank for the public network. $2: IP address of the BGP peer. $3: Address family of the BGP peer. $4: Maximum number of routes.
Severity level	4
Example	BGP/4/BGP_EXCEED_ROUTE_LIMIT: BGP.vpn1: The number of routes from peer 1.1.1.1 (IPv4-UNC) exceeds the limit 100.
Explanation	The number of routes received from a peer exceeded the maximum number of routes that can be received from the peer.
Recommended action	Determine whether it is caused by attacks: • If yes, configure the device to defend against the attacks. • If not, increase the maximum number of routes.

BGP_REACHED_THRESHOLD

Message text	BGP.[STRING]: The proportion of prefixes received from peer [STRING] ([STRING]) to maximum allowed prefixes reached the threshold value ([UINT32]%).
Variable fields	$1: VPN instance name. This field is blank for the public network. $2: IP address of the BGP peer. $3: Address family of the BGP peer. $4: Percentage of received routes to the maximum allowed routes.
Severity level	5
Example	BGP/5/BGP_REACHED_THRESHOLD: BGP.vpn1: The proportion of prefixes received from peer 1.1.1.1 (IPv4-UNC) to maximum allowed prefixes reached the threshold value (60%).
Explanation	The percentage of received routes to the maximum allowed routes reached the threshold.
Recommended action	Determine whether it is caused by attacks: • If yes, configure the device to defend against the attacks. • If not, increase the threshold value or the maximum number of routes that can be received from the peer.

BGP_MEM_ALERT

Message text	BGP process received system memory alert [STRING] event.
Variable fields	$1: Type of the memory alarm, stop and start.
Severity level	5
Example	BGP/5/BGP_MEM_ALERT: BGP process received system memory alert start event.
Explanation	BGP received a memory alarm.
Recommended action	If BGP received a system memory alert start event, check the system memory and try to free some memory by adjusting modules that occupied too much memory.

BGP_PEER_LICENSE_REACHED

Message text	Number of peers in Established state reached the license limit.
Variable fields	N/A
Severity level	5
Example	BGP/5/BGP_PEER_LICENSE_REACHED: Number of peers in Established state reached the license limit.
Explanation	The number of peers in Established state reached the license limit.
Recommended action	Determine whether a new license is required.

BGP_ROUTE_LICENSE_REACHED

Message text	Number of [STRING] routes reached the license limit.
Variable fields	$1: BGP address family: • **IPv4-UNC public**—IPv4 unicast routes for the public network. • **IPv6-UNC public**—IPv6 unicast routes for the public network. • **IPv4 private**—IPv4 unicast routes, VPNv4 routes, and nested VPN routes for the private network. • **IPv6 private**—IPv6 unicast routes and VPNv6 routes for the private network.
Severity level	5
Example	BGP/5/BGP_ROUTE_LICENSE_REACHED: Number of IPv4-UNC public routes reached the license limit.
Explanation	The number of routes in the specified address family reached the license limit.
Recommended action	Determine whether a new license is required. After the number of routes in the specified family falls below the license limit or the license limit increases, you must manually restore the discarded routes.

BGP_STATE_CHANGED

Message text	• **Text 1**: BGP.[STRING]: [STRING] state has changed from [STRING] to [STRING]. • **Text 2**: BGP.[STRING]: [STRING] state has changed from [STRING] to [STRING] for [STRING].
Variable fields	In text 1: $1: VPN instance name. This field is blank for the public network. $2: IP address of the BGP peer. $3: Name of FSM before the state change. $4: Name of FSM after the state change. In text 2: $1: VPN instance name. This field is blank for the public network. $2: IP address of the BGP peer. $3: Name of FSM before the state change. $4: Name of FSM after the state change. $5: Reason for the state change.
Severity level	5
Example	BGP/5/BGP_STATE_CHANGED: BGP.vpn1:192.99.0.2 state has changed from OPENCONFIRM to ESTABLISHED.
Explanation	The FSM of a BGP peer has changed. This informational message appears when a BGP peer comes up or goes down.
Recommended action	If a peer goes down unexpectedly, determine whether an error or packet loss occurs.

BLS messages

This section contains blacklist messages.

BLS_DIP_BLOCK

Message text	DstIPAddr(1007)=[IPADDR];RcvVPNInstance(1042)=[STRING];SndDSLite TunnelPeer(1041)=[STRING].
Variable fields	$1: Blacklisted destination IPv4 address. $2: VPN instance name. $3: Peer address of the DS-Lite tunnel.
Severity level	3
Example	BLS/3/BLS_DIP_BLOCK:DstIPAddr(1007)=1.1.1.5;RcvVPNInstance(1042) =;SndDSLiteTunnelPeer(1041)=--.
Explanation	This message is sent when an IPv4 destination blacklist entry is hit. Logs are sent every 30 seconds.
Recommended action	No action is required.

BLS_DIPV6_BLOCK

Message text	DstIPv6Addr(1037)=[IPADDR];RcvVPNInstance(1042)=[STRING].
Variable fields	$1: Blacklisted destination IPv6 address. $2: VPN instance name.
Severity level	3
Example	BLS/3/BLS_DIPV6_BLOCK: DstIPv6Addr(1037)=200::3;RcvVPNInstance(1042)=.
Explanation	This message is sent when an IPv6 destination blacklist entry is hit. Logs are sent every 30 seconds.
Recommended action	No action is required.

BLS_ENTRY_ADD

Message text	SrcIPAddr(1003)=[IPADDR]; SndDSLiteTunnelPeer(1041)=[STRING]; RcvVPNInstance(1042)=[STRING]; TTL(1055)=[STRING]; Reason(1056)=[STRING].
Variable fields	$1: Blacklisted IP address. $2: Peer address of the DS-Lite tunnel. $3: VPN instance name. $4: TTL of a blacklist entry. $5: Reason why the blacklist entry was added.
Severity level	5
Example	BLS/5/BLS_ENTRY_ADD: -Context=1; SrcIPAddr(1003)=1.1.1.6; SndDSLiteTunnelPeer(1041)=--; RcvVPNInstance(1042)=; TTL(1055)=; Reason(1056)=Configuration. BLS/5/BLS_ENTRY_ADD: -Context=1; SrcIPAddr(1003)=9.1.1.5; SndDSLiteTunnelPeer(1041)=--; RcvVPNInstance(1042)=vpn1; TTL(1055)=10; Reason(1056)=Scan behavior detected.
Explanation	A blacklist entry was added. The message is sent when a blacklist entry is manually configured or dynamically created according to the scanning result.
Recommended action	No action is required.

BLS_ENTRY_DEL

Message text	SrcIPAddr(1003)=[IPADDR]; SndDSLiteTunnelPeer(1041)=[STRING]; RcvVPNInstance(1042)=[STRING]; Reason(1056)=[STRING].
Variable fields	$1: Blacklisted IP address. $2: Peer address of the DS-Lite tunnel. $3: VPN instance name. $4: Reason why the blacklist entry was deleted.
Severity level	5
Example	BLS/5/BLS_ENTRY_DEL: -Context=1; SrcIPAddr(1003)=1.1.1.3; SndDSLiteTunnelPeer(1041)=--; RcvVPNInstance(1042)=; Reason(1056)=Configuration. BLS/5/BLS_ENTRY_DEL: -Context=1; SrcIPAddr(1003)=9.1.1.5; SndDSLiteTunnelPeer(1041)=--; RcvVPNInstance(1042)=vpn1; Reason(1056)=Aging.
Explanation	A blacklist entry was deleted. The message is sent when a blacklist entry is manually deleted or dynamically deleted due to the aging.
Recommended action	No action is required.

BLS_IP_BLOCK

Message text	SrcIPAddr(1003)=[IPADDR];RcvVPNInstance(1042)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING].
Variable fields	$1: Blacklisted source IPv4 address. $2: VPN instance name. $3: Peer address of the DS-Lite tunnel.
Severity level	3
Example	BLS/3/BLS_IP_BLOCK:SrcIPAddr(1003)=1.1.1.3;RcvVPNInstance(1042)=;SndDSLiteTunnelPeer(1041)=--.
Explanation	This message is sent when an IPv4 source blacklist entry or the address object group-based blacklist entry is hit. Logs are sent every 30 seconds.
Recommended action	No action is required.

BLS_IPV6_BLOCK

Message text	SrcIPv6Addr(1036)=[IPADDR];RcvVPNInstance(1042)=[STRING].
Variable fields	$1: Blacklisted source IPv6 address. $2: VPN instance name.
Severity level	3
Example	BLS/3/BLS_IPV6_BLOCK: SrcIPv6Addr(1036)=200::2;RcvVPNInstance(1042)=.
Explanation	This message is sent when an IPv6 source blacklist entry is hit. Logs are sent every 30 seconds.
Recommended action	No action is required.

BLS_IPV6_ENTRY_ADD

Message text	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1042)=[STRING]; TTL(1055)=[STRING]; Reason(1056)=[STRING].
Variable fields	$1: Blacklisted IPv6 address. $2: VPN instance name. $3: TTL of a blacklist entry. $4: Reason why the blacklist entry was added.
Severity level	5
Example	BLS/5/BLS_IPV6_ENTRY_ADD: -Context=1; SrcIPv6Addr(1036)=2::2; RcvVPNInstance(1042)=; TTL(1055)=; Reason(1056)=Configuration. BLS/5/BLS_IPV6_ENTRY_ADD: -Context=1; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1042)=; TTL(1055)=10; Reason(1056)=Scan behavior detected.
Explanation	A blacklist entry was added. The message is sent when a blacklist entry is manually configured or dynamically created according to the scanning result.
Recommended action	No action is required.

BLS_IPV6_ENTRY_DEL

Message text	SrcIPv6Addr(1036)=[IPADDR]; RcvVPNInstance(1042)=[STRING]; Reason(1056)=[STRING].
Variable fields	$1: Blacklisted IPv6 address. $2: VPN instance name. $3: Reason why the blacklist entry was deleted.
Severity level	5
Example	BLS/5/BLS_IPV6_ENTRY_DEL: -Context=1; SrcIPv6Addr(1036)=2::2; RcvVPNInstance(1042)=; Reason(1056)=Configuration. BLS/5/BLS_IPV6_ENTRY_DEL: -Context=1; SrcIPv6Addr(1036)=1::5; RcvVPNInstance(1042)=; Reason(1056)= Aging.
Explanation	A blacklist entry was deleted. The message is sent when a blacklist entry is manually deleted or dynamically deleted due to the aging.
Recommended action	No action is required.

BLS_ENTRY_USER_ADD

Message text	User(1098)=[STRING]; TTL(1055)=[STRING]; Reason(1056)=[STRING]; DomainName(1099) =[STRING].
Variable fields	$1: Username in the user blacklist entry. $2: User blacklist entry aging time. $3: Reason why the user blacklist entry was added. $4: Name of the user identification domain to which the user belongs.
Severity level	5
Example	BLS/5/BLS_ENTRY_USER_ADD: User(1098)=user1; TTL(1055)=10; Reason(1056)=Configuration; DomainName(1099)=domain1.
Explanation	A user blacklist entry was added. The message is sent when a user blacklist entry is manually added.
Recommended action	No action is required.

BLS_ENTRY_USER_DEL

Message text	User(1098)=[STRING]; Reason(1056)=[STRING]; DomainName(1099)=[STRING].
Variable fields	$1: Username in the user blacklist entry. $2: Reason why the blacklist entry was deleted: • **Configuration**—Manual deletion. • **Aging**—Ageout. $3: Name of the user identification domain to which the user belongs.
Severity level	5
Example	BLS/5/BLS_ENTRY_USER_DEL: User(1098)=user1; Reason(1056)=Configuration; DomainName(1099)=domain1. BLS/5/BLS_ENTRY_USER_DEL: User(1098)=user1; Reason(1056)=Aging; DomainName(1099)=domain1.
Explanation	A user blacklist entry was deleted. The message is sent when a user blacklist entry is manually deleted or dynamically deleted due to the aging.
Recommended action	No action is required.

BLS_USER_IP_BLOCK

Message text	User(1098)=[STRING];SrcIPAddr(1003)=[IPADDR];DomainName(1099)=[STRING]; RcvVPNInstance(1042)=[STRING];SrcMacAddr(1021)=[STRING].
Variable fields	$1: Name of the blacklisted user. $2: User IPv4 address. $3: Name of the identity domain to which the user belongs. $4: VPN instance name. $5: User MAC address.
Severity level	3
Example	BLS/3/BLS_USER_IP_BLOCK: User(1098)=user1;SrcIPAddr(1003)=1.1.1.6;DomainName(1099)=; RcvVPNInstance(1042)=;SrcMacAddr(1021)= 38ad-bea7-829a.
Explanation	This message is sent when an IPv4 user blacklist entry is hit. Logs are sent every 30 seconds.
Recommended action	No action is required.

BLS_USER_IPV6_BLOCK

Message text	User(1098)=[STRING];SrcIPAddr(1003)=[IPADDR];DomainName(1099)=[STRING];RcvVPNInstance(1042)=[STRING];SrcMacAddr(1021)=[STRING].
Variable fields	$1: Name of the blacklisted user. $2: User IPv6 address. $3: Name of the identity domain to which the user belongs. $4: VPN instance name. $5: User MAC address.
Severity level	3
Example	BLS/3/BLS_USER_IPV6_BLOCK:User(1098)=user2;SrcIPAddr(1003)=1.1.1.7;DomainName(1099)=;RcvVPNInstance(1042)=;SrcMacAddr(1021)=38ad-bea7-829b.
Explanation	This message is sent when an IPv6 user blacklist entry is hit. Logs are sent every 30 seconds.
Recommended action	No action is required.

CC defense messages

This section contains CC defense messages through fast log output.

CC_MATCH_IPV4_LOG

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];PolicyName(1079)=[STRING];RuleName(1080)=[STRING];ProtectedURL(1136)=[STRING];HitSrcIPAddr(1137)=[IPADDR];HitTime(1138)=[STRING];RequestRate(1139)=[UINT32];RequestConcentration(1140)=[UINT32];Action(1053)=[STRING];BlockTime(1141)=[UINT32];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Source IP address. $4: Source port number. $5: Destination IP address. $6: Destination port number. $7: CC defense policy name. $8: CC defense rule name. $9: Protected path matched. $10: Source IP address matched. $11: Time when the protected path is matched. $12: Request rate. $13: Request concentration ratio. $14: Actions on the matching packet. Available actions are: o Block. o Permit. $15: Block period. $16: VLAN ID. $17: VXLAN ID. $18: Source location. $19: Destination location.
Severity level	6
Example	CC-DEFENSE/6/CC_MATCH_IPV4_LOG:Protocol(1001)=TCP;Application(1002)=SouhuNews;SrcIPAddr(1003)=112.1.1.2;SrcPort(1004)=3887;DstIPAddr(1007)=114.1.1.2;DstPort(1008)=80;PolicyName(1079)=1;RuleName(1080)=test;ProtectedURL(1136)=news.sohu.com/upload/itoolbar/itoolbar.index.loader.20140923.js;HitSrcIPAddr(1137)=112.1.1.2;HitTime(1138)=1480691551;RequestRate(1139)=10;RequestConcentration(1140)=150;Action(1053)=Block;BlockTime(1141)=300;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is sent when an IPv4 packet matches a CC defense rule, and a detection item threshold is reached.
Recommended action	No action is required.

CC_MATCH_IPV6_LOG

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];PolicyName(1079)=[STRING];RuleName(1080)=[STRING];ProtectedURL(1136)=[STRING];HitSrcIPv6Addr(1037)=[IPADDR];HitTime(1138)=[STRING];RequestRate(1139)=[UINT32];RequestConcentration(1140)=[UINT32];Action(1053)=[STRING];BlockTime(1141)=[UINT32];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Source IP address. $4: Source port number. $5: Destination IP address. $6: Destination port number. $7: CC defense policy name. $8: CC defense rule name. $9: Protected path matched. $10: Source IP address matched. $11: Time when the protected path is matched. $12: Request rate. $13: Request concentration ratio. $14: Actions on the matching packet. Available actions are: o Block. o Permit. $15: Block period. $16: VLAN ID. $17: VXLAN ID. $18: Source location. $19: Destination location.
Severity level	4
Example	CC-DEFENSE/6/CC_MATCH_IPV6_LOG:Protocol(1001)=TCP;Application(1002)=SouhuNews;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;PolicyName(1079)=1;RuleName(1080)=test;ProtectedURL(1136)=news.sohu.com/upload/itoolbar/itoolbar.index.loader.20140923.js;HitSrcIPv6Addr(1137)=1:2:3:4:5:6:7:8;HitTime(1138)=1480691551;RequestRate(1139)=150;RequestConcentration(1140)=20;Action(1053)=Block;BlockTime(1141)=300;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is sent when an IPv6 packet matches a CC defense rule and a detection item threshold is reached.
Recommended action	No action is required.

CFD messages

This section contains CFD messages.

CFD_CROSS_CCM

Message text	MEP [UINT16] in SI [INT32] received a cross-connect CCM. It's SrcMAC is [MAC], SeqNum is [INT32], RMEP is [UINT16], MD ID is [STRING], MA ID is [STRING].
Variable fields	$1: Service instance ID. $2: Local MEP ID. $3: Source MAC address. $4: Sequence number. $5: Remote MEP ID. $6: MD ID. If no MD ID is available, "without ID" is displayed. $7: MA ID.
Severity level	6
Example	CFD/6/CFD_CROSS_CCM: MEP 13 in SI 10 received a cross-connect CCM. Its SrcMAC is 0011-2233-4401, SeqNum is 78, RMEP is 12, MD ID is without ID, MA ID is 0.
Explanation	A MEP received a cross-connect CCM containing a different MA ID or MD ID.
Recommended action	Check the configurations of MEPs on both ends. Make sure the MEPs have consistent configurations, including MD, MA, and level.

CFD_ERROR_CCM

Message text	MEP [UINT16] in SI [INT32] received an error CCM. It's SrcMAC is [MAC], SeqNum is [INT32], RMEP is [UINT16], MD ID is [STRING], MA ID is [STRING].
Variable fields	$1: Service instance ID. $2: Local MEP ID. $3: Source MAC address. $4: Sequence number. $5: Remote MEP ID. $6: MD ID. If no MD ID is available, "without ID" is displayed. $7: MA ID.
Severity level	6
Example	CFD/6/CFD_ERROR_CCM: MEP 2 in SI 7 received an error CCM. Its SrcMAC is 0011-2233-4401, SeqNum is 21, RMEP is 2, MD ID is 7, MA ID is 1.
Explanation	A MEP received an error CCM containing an unexpected MEP ID or lifetime.
Recommended action	Check the CCM configuration. Make sure the CCM intervals are consistent on both ends, and the remote MEP ID is included in the MEP list of the local end.

CFD_REACH_LOWERLIMIT

Message text	[STRING] reached or fell below the lower limit [STRING] on MEP [UINT16] in service instance [INT32].
Variable fields	$1: Monitored indicator: ○ Bit error ratio. ○ Far-end frame loss ratio. ○ Near-end frame loss ratio. ○ Frame delay. $2: Threshold. $3: Local MEP ID. $4: Service instance ID.
Severity level	6
Example	CFD/6/ CFD_REACH_LOWERLIMIT: Bit error ratio reached or fell below the lower limit 4% on MEP 2 in service instance 3.
Explanation	This message is generated when a monitored indicator reaches or falls below the lower limit.
Recommended action	No action is required.

CFD_REACH_UPPERLIMIT

Message text	[STRING] reached or exceeded the upper limit [STRING] on MEP [UINT16] in service instance [INT32].
Variable fields	$1: Monitored indicator: ○ Bit error ratio. ○ Far-end frame loss ratio. ○ Near-end frame loss ratio. ○ Frame delay. $2: Threshold. $3: Local MEP ID. $4: Service instance ID.
Severity level	6
Example	CFD/6/ CFD_REACH_UPPERLIMIT: Bit error ratio reached or exceeded the upper limit 80% on MEP in service instance 3.
Explanation	This message is generated when a monitored indicator reaches or exceeds the upper limit.
Recommended action	No action is required.

CFD_LOST_CCM

Message text	MEP [UINT16] in SI [INT32] failed to receive CCMs from RMEP [UINT16].
Variable fields	$1: Local MEP ID. $2: Service instance ID. $3: Remote MEP ID.
Severity level	6
Example	CFD/6/CFD_LOST_CCM: MEP 1 in SI 7 failed to receive CCMs from RMEP 2.
Explanation	A MEP failed to receive CCMs within 3.5 sending intervals because the link is faulty or the remote MEP does not send CCM within 3.5 sending intervals.
Recommended action	Check the link status and the configuration of the remote MEP. If the link is down or faulty (becomes unidirectional, for example), restore the link. If the remote MEP is configured with the same service instance, make sure the CCM sending intervals are consistent on both ends.

CFD_RECEIVE_CCM

Message text	MEP [UINT16] in SI [INT32] received CCMs from RMEP [UINT16]
Variable fields	$1: Local MEP ID. $2: Service instance ID. $3: Remote MEP ID.
Severity level	6
Example	CFD/6/CFD_RECEIVE_CCM: MEP 1 in SI 7 received CCMs from RMEP 2.
Explanation	A MEP received CCMs from a remote MEP.
Recommended action	No action is required.

CFGLOG messages

This section contains configuration log messages.

CFGLOG_CFGOPERATE

Message text	-Client=[STRING]-User=[STRING]-IPAddr=[STRING]-Role=[STRING];Config in [STRING] changed: -Old setting=[STRING]; -New setting=[STRING];
Variable fields	$1: Configuration method. The supported configuration methods include CLI, NETCONF, SNMP, CWMP, and Web. $2: Name of the user that changed the configuration. This field displays two asterisks (**) if the user does not use scheme authentication, which requires a username for login. $3: IP address of the user that changed the configuration. This field displays two asterisks (**) if the user logged in to the device through the console port. $4: User role of the user that changed the configuration. $5: Configuration change location. $6: Old setting. $7: New setting. If one operation causes multiple settings to change, the $5, $6, and $7 fields might be displayed one time for each setting change.
Severity level	6
Example	CFGLOG/6/CFGLOG_CFGOPERATE: -Client=CLI-User=**-IPAddr=**-Role=network-admin; Config in system changed: -Old setting=sysname Device -New setting=sysname Test.
Explanation	A user changed the configuration on the device.
Recommended action	No action is required.

CFGMAN messages

This section contains configuration management messages.

CFGMAN_ARCHIVE_FAIL

Message text	Failed to archive the running configuration to a remote server: Location=[STRING]
Variable fields	$1: URL of the remote server that stores the configuration archives. If the server is an FTP server, the URL is in the format of **ftp://***username@server-IP*[:*port-number*]/*file-path*. If the server IP is an IPv6 address, the IPv6 address is enclosed within a pair of brackets ([]). If the server is a TFTP server, the URL does not contain the username field.
Severity level	4
Example	CFGMAN/4/CFGMAN_ARCHIVE_FAIL: Failed to archive the running configuration to a remote server: Location=ftp://admin@192.168.21.21[:21]/test/
Explanation	The device failed to archive the running configuration to a remote server.
Recommended action	**28.** Verify that the device can create temporary configuration archives locally. For this purpose, you can verify that the device can archive the running configuration by using the local archiving feature. **29.** Verify that the remote server is accessible. **30.** Verify that the remote server has sufficient storage space.

CFGMAN_CFGCHANGED

Message text	-EventIndex=[INT32]-CommandSource=[INT32]-ConfigSource=[INT32]-ConfigDestination=[INT32]; Configuration changed.
Variable fields	$1: Event index in the range of 1 to 2147483647. $2: Configuration change source: ○ **cli**—The configuration change came from the CLI. ○ **snmp**—The configuration change came from SNMP or was a configuration database change detected by SNMP. ○ **other**—The configuration change came from other sources. $3: Source configuration: ○ **erase**—Deleting or renaming a configuration file. ○ **running**—Saving the running configuration. ○ **commandSource**—Copying a configuration file. ○ **startup**—Saving the running configuration to the next-startup configuration file. ○ **local**—Saving the running configuration to a local file. ○ **networkFtp**—Using FTP to transfer and save a configuration file to the device as the running configuration or next-startup configuration file. ○ **hotPlugging**—A card hot swapping caused the configuration to be deleted or become ineffective. $4: Destination configuration: ○ **erase**—Deleting or renaming a configuration file. ○ **running**—Saving the running configuration. ○ **commandSource**—Copying a configuration file. ○ **startup**—Saving the running configuration to the next-startup configuration file. ○ **local**—Saving the running configuration to a local file. ○ **networkFtp**—Using FTP to transfer and save a configuration file to the device as the running configuration or next-startup configuration file. ○ **hotPlugging**—A card hot swapping caused the configuration to be deleted or become ineffective.
Severity level	5
Example	CFGMAN/5/CFGMAN_CFGCHANGED: -EventIndex=[6]-CommandSource=[snmp]-ConfigSource=[startup]-ConfigDestination=[running]; Configuration changed.
Explanation	The running configuration changed in the past 10 minutes.
Recommended action	No action is required.

CFGMAN_OPTCOMPLETION

Message text	-OperateType=[INT32]-OperateTime=[INT32]-OperateState=[INT32]-OperateEndTime=[INT32]; Operation completed.
Variable fields	$1: Operation type: ○ **running2startup**—Saves the running configuration to the next-startup configuration file. ○ **startup2running**—Loads the configuration in the next-startup configuration file. ○ **running2net**—Saves the running configuration to a host on the network. ○ **net2running**—Transfers a configuration file from a host on the network and loads the configuration. ○ **net2startup**—Transfers a configuration file from a host on the network and specifies the file as the next-startup configuration file. ○ **startup2net**—Copies the next-startup configuration file to a host on the network. $2: Operation start time. $3: Operation status: ○ **InProcess**—Operation is in progress. ○ **success**—Operation succeeded. ○ **InvalidOperation**—Invalid operation. ○ **InvalidProtocol**—Invalid protocol. ○ **InvalidSource**—Invalid source file name. ○ **InvalidDestination**—Invalid destination file name. ○ **InvalidServer**—Invalid server address. ○ **DeviceBusy**—The device is busy. ○ **InvalidDevice**—Invalid device address. ○ **DeviceError**—An error occurred on the device. ○ **DeviceNotWritable**—The storage medium on the device is write protected. ○ **DeviceFull**—The device does not have enough free storage space for the file. ○ **FileOpenError**—Failed to open the file. ○ **FileTransferError**—Failed to transfer the file. ○ **ChecksumError**—File checksum error. ○ **LowMemory**—The memory space is not sufficient. ○ **AuthFailed**—User authentication failed. ○ **TransferTimeout**—Transfer timed out. ○ **UnknownError**—An unknown error occurred. ○ **invalidConfig**—Invalid configuration. $4: Operation end time.
Severity level	5
Example	CFGMAN/5/CFGMAN_OPTCOMPLETION: -OperateType=[running2startup]-OperateTime=[248]-OperateState=[success]-OperateEndTime=[959983]; Operation completed.
Explanation	The device is performing or has completed an operation.
Recommended action	If the operation is not successful, locate and resolve the problem.

CFGMAN_REPLACE_CANCEL

Message text	Configuration rollback from remote server was canceled: Replacement file=[STRING]
Variable fields	$1: URL of the replacement configuration file on the remote rollback server. If the server is an FTP server, the URL is in the format of **ftp://***username@server-IP*[:*port-number*]/*file-path*. If the server IP is an IPv6 address, the IPv6 address is enclosed within a pair of brackets ([]). If the server is a TFTP server, the URL does not contain the username field.
Severity level	5
Example	CFGMAN/5/CFGMAN_REPLACE_CANCEL: Configuration rollback from remote server was canceled: Replacement file=ftp://admin@192.168.21.21[:21]/test/startup.cfg
Explanation	This event occurs if the rollback schedule expires before it could be executed because the system date or time is changed backward.
Recommended action	Reconfigure the remote configuration rollback parameters as needed.

CFGMAN_REPLACE_FAIL

Message text	Failed to replace running configuration with a remote configuration file: File=[STRING]
Variable fields	$1: URL of the replacement configuration file on the remote rollback server. If the server is an FTP server, the URL is in the format of **ftp://***username@server-IP*[:*port-number*]/*file-path*. If the server IP is an IPv6 address, the IPv6 address is enclosed within a pair of brackets ([]). If the server is a TFTP server, the URL does not contain the username field.
Severity level	4
Example	CFGMAN/4/CFGMAN_REPLACE_FAIL: Failed to replace running configuration with a remote configuration file: File=ftp://admin@192.168.21.21[:21]/test/startup.cfg
Explanation	The system failed to replace the running configuration with a configuration file on the remote rollback server.
Recommended action	**31.** Verify that the remote server is accessible. **32.** Verify that the replacement configuration file exists in the file path on the server. **33.** Verify that the device has sufficient storage space. **34.** Verify that the content and format of the replacement configuration file are compatible with the device.

CFGMAN_REPLACE_SOON

Message text	The system will replace running configuration with a remote file in 1 minute: File=[STRING]
Variable fields	$1: URL of the replacement configuration file on the remote rollback server. If the server is an FTP server, the URL is in the format of **ftp://***username@server-IP*[:*port-number*]/*file-path*. If the server IP is an IPv6 address, the IPv6 address is enclosed within a pair of brackets ([]). If the server is a TFTP server, the URL does not contain the username field.
Severity level	5
Example	CFGMAN/5/CFGMAN_REPLACE_SOON: The system will replace running configuration with a remote file in 1 minute: File=ftp://admin@192.168.21.21[:21]/test/startup.cfg
Explanation	The system has a configuration rollback schedule and it will replace the running configuration with a remote file in 1 minute.
Recommended action	Execute the **undo configuration replace server file** command to cancel the rollback schedule if it is not desirable.

CGROUP messages

This section contains interface collaboration messages.

CGROUP_STATUS_CHANGE

Message text	The status of collaboration group [UINT32] is [STRING].
Variable fields	$1: Collaboration group ID. $2: Collaboration group state: down or up.
Severity level	6
Example	CGROUP/6/CGROUP_STATUS_CHANGE: The status of collaboration group 1 is up.
Explanation	The status of collaboration group 1 is up or down.
Recommended action	Check the links.

CONNLMT messages

This section contains connection limit messages.

CONNLMT_IPV4_OVERLOAD

Message text	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];UpperLimit(1049)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];Action(1053)=[STRING];
Variable fields	$1: Global, or interface name. $2: Transport layer protocol type. $3: Source IP address. $4: Destination IP address. $5: Service port number. $6: Source VPN instance name. $7: Destination VPN instance name. $8: Peer tunnel ID. $9: Upper threshold. $10: Rule ID. $11: Event message. $12: Permit or deny new connections.
Severity level	6
Example	CONNLMT/6/CONNLMT_IPV4_OVERLOAD: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPAddr(1003)=10.10.10.1;DstIPAddr(1007)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;UpperLimit(1049)=1000;LimitRuleNum(1051)=1;Event(1048)=Exceeded upper threshold;Action(1053)=Permit new connections;
Explanation	The number of concurrent connections exceeded the upper threshold.
Recommended action	No action is required.

CONNLMT_IPV4_RECOVER

Message text	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];DropPktCount(1052)=[UINT32];LowerLimit(1050)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];
Variable fields	$1: Global, or interface name. $2: Transport layer protocol type. $3: Source IP address. $4: Destination IP address. $5: Service port number. $6: Source VPN instance name. $7: Destination VPN instance name. $8: Peer tunnel ID. $9: Number of dropped packets. $10: Lower threshold. $11: Rule ID. $12: Event message.
Severity level	6
Example	CONNLMT/6/CONNLMT_IPV4_RECOVER: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPAddr(1003)=10.10.10.1;DstIPAddr(1007)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;DropPktCount(1052)=306004;LowerLimit(1050)=10;LimitRuleNum(1051)=1;Event(1048)=Dropped below lower threshold;
Explanation	The number of concurrent connections dropped below the lower threshold from the upper threshold.
Recommended action	No action is required.

CONNLMT_IPV6_OVERLOAD

Message text	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];UpperLimit(1049)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];Action(1053)=[STRING];
Variable fields	$1: Global, or interface name. $2: Transport layer protocol type. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Service port number. $6: Source VPN instance name. $7: Destination VPN instance name. $8: Peer tunnel ID. $9: Upper threshold. $10: Rule ID. $11: Event message. $12: Permit or deny new connections.
Severity level	6
Example	CONNLMT/6/CONNLMT_IPV6_OVERLOAD: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPv6Addr(1036)=2001::1;DstIPv6Addr(1037)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;UpperLimit(1049)=1000;LimitRuleNum(1051)=1;Event(1048)=Exceeded upper threshold;Action(1053)=Permit new connections;
Explanation	The number of concurrent connections exceeded the upper threshold.
Recommended action	No action is required.

CONNLMT_IPV6_RECOVER

Message text	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];DropPktCount(1052)=[UINT32];LowerLimit(1050)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];
Variable fields	$1: Global, or interface name. $2: Transport layer protocol type. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Service port number. $6: Source VPN instance name. $7: Destination VPN instance name. $8: Peer tunnel ID. $9: Number of dropped packets. $10: Lower threshold. $11: Rule ID. $12: Event message.
Severity level	6
Example	CONNLMT/6/CONNLMT_IPV6_RECOVER: RcvIfName(1023)=Global;Protocol(1001)=;SrcIPAddr(1003)=2001::1;DstIPAddr(1007)=;ServicePort(1071)=;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;DropPktCount(1052)=306004;LowerLimit(1050)=10;LimitRuleNum(1051)=1;Event(1048)=Dropped below lower threshold;
Explanation	The number of concurrent connections dropped below the lower threshold from the upper threshold.
Recommended action	No action is required.

CONNLMT_IPV4_RATELIMIT

Message text	RcvIfName(1023)=[STRING];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];LimitRate(1073)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];Action(1053)=[STRING];
Variable fields	$1: Global, or interface name. $2: Transport layer protocol type. $3: Source IPv4 address. $4: Destination IPv4 address. $5: Service port number. $6: Source VPN instance name. $7: Destination VPN instance name. $8: Peer tunnel ID. $9: Upper rate limit. $10: Rule ID. $11: Event message. $12: Permit or deny new connections.
Severity level	6
Example	CONNLMT/6/CONNLMT_IPV4_RATELIMIT: -MDC=1; RcvIfName(1023)=M-GigabitEthernet0/0/0;Protocol(1001)=;SrcIPAddr(1003)=;DstIPAddr(1007)=;ServicePort(1071)=; RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;LimitRate(1073)=10;LimitRuleNum(1051)=1;Event(1048)=Exceeded rate limit;Action(1053)=Permit new connections;
Explanation	Connections are established at a rate higher than the rate limit. The message is output only at the first time if the event takes place consecutively.
Recommended action	No action is required.

CONNLMT_IPV6_RATELIMIT

Message text	RcvIfName(1023)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];ServicePort(1071)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];LimitRate(1073)=[UINT32];LimitRuleNum(1051)=[UINT16];Event(1048)=[STRING];
Variable fields	$1: Global, or interface name. $2: Transport layer protocol type. $3: Source IPv6 address. $4: Destination IPv6 address. $5: Service port number. $6: Source VPN instance name. $7: Destination VPN instance name. $8: Peer tunnel ID. $9: Upper rate limit. $10: Rule ID. $11: Event message.
Severity level	6
Example	CONNLMT/6/CONNLMT_IPV6_RATELIMIT: -MDC=1; RcvIfName(1023)=M-GigabitEthernet0/0/0;Protocol(1001)=;SrcIPAddr(1036)=;DstIPAddr(1037)=;ServicePort(1071)=; RcvVPNInstance(1042)=;SndVPNInstance(1043)=;SndDSLiteTunnelPeer(1041)=;LimitRate(1073)=10;LimitRuleNum(1051)=1;Event(1048)=Exceeded rate limit;
Explanation	Connections are established at a rate higher than the rate limit. The message is output only at the first time if the event takes place consecutively.
Recommended action	No action is required.

CONTEXT messages

This section contains context messages.

CAR_MODIFY

Message text	-Context=[UINT]; The throughput of context [STRING]([UINT]) is changed to [UINT] kbps/pps.
Variable fields	$1: Context ID. $2: Context name. $3: Context ID. $4: Throughput threshold of the context.
Severity level	6
Example	For the default context: CAR/6/CAR_MODIFY: The throughput of context slb128(128) is changed to 66666 pps. For a non-default context: CAR/6/CAR_MODIFY: -Context=128; The throughput of context slb128(128) is changed to 66666 pps.
Explanation	The throughput threshold of a context changed.
Recommended action	No action is required.

CAR_DESTROY

Message text	-Context=[UINT]; The throughput of context [STRING]([UINT]) is changed to default.
Variable fields	$1: Context ID. $2: Context name. $3: Context ID.
Severity level	6
Example	For the default context: CAR/6/CAR_DESTROY: The throughput of context slb128(128) is changed to default. For a non-default context: CAR/6/CAR_ DESTROY:-Context=128; The throughput of context slb128(128) is changed to default.
Explanation	The default throughput threshold was restored for a context.
Recommended action	No action is required.

SIB_BROADCAST_DROP

Message text	Dropped [UINT] broadcast packets of context [UINT].
Variable fields	$1: Number of dropped broadcast packets. $2: Context ID.
Severity level	6
Example	SIB/6/SIB_BROADCAST_DROP: Dropped 65478 broadcast packets of context 1.
Explanation	Some broadcast packets were dropped on a context.
Recommended action	No action is required.

SIB_CORE_ATTACK_DROP

Message text	Dropped [UINT] packets because of core attack.
Variable fields	$1: Number of dropped unicast packets.
Severity level	6
Example	SIB/6/ SIB_CORE_ATTACK_DROP: Dropped 65478 packets because of core attack.
Explanation	Some unicast packets were dropped on the device.
Recommended action	No action is required.

SIB_MAC_DUPLICATE

Message text	The new MAC address ([STRING]) of interface [STRING] is already used as the VRRP group MAC address on interface [STRING] of context = [UINT].
Variable fields	$1: MAC address. $2: Interface name. $3: Interface name. $4: Context ID.
Severity level	3
Example	SIB/3/SIB_MAC_DUPLICATE: The new MAC address (a234-2345-0902) of interface GigabitEthernet1/0/0 is already used as the VRRP group MAC address on interface GigabitEthernet1/0/1 of context = 2.
Explanation	The new physical MAC address of an interface is the same as the virtual MAC address of another interface in a VRRP group on a context.
Recommended action	Change the physical MAC address of the interface.

SIB_MAC_DUPLICATE

Message text	The VRRP group MAC address ([STRING]) is already used as the MAC address of interface [STRING] on context = [UINT].
Variable fields	$1: MAC address. $2: Interface name. $3: Context ID.
Severity level	3
Example	SIB/3/SIB_MAC_DUPLICATE: The VRRP group MAC address (a234-2345-0902) is already used as the MAC address of interface GigabitEthernet1/0/0 on context = 2.
Explanation	On a context, the virtual MAC address of an interface in a VRRP group is the same as the physical MAC address of the interface.
Recommended action	Change the virtual MAC address of the interface in the VRRP group.

SIB_MULTICAST_DROP

Message text	Dropped [UINT] multicast packets of context [UINT].
Variable fields	$1: Number of dropped multicast packets. $2: Context ID.
Severity level	6
Example	SIB/6/SIB_MULTICAST_DROP: Dropped 750036 multicast packets of context 1.
Explanation	Some multicast packets were dropped on a context.
Recommended action	No action is required.

DAC

This section contains data analysis center (DAC) messages.

DAC_STORE_STATE_STOREFULL

Message text	DPI/4/DAC_STORE_STATE_STOREFULL: The total storage usage reached 98%.
Severity level	4
Example	DPI/4/DAC_STORE_STATE_STOREFULL: The total storage usage reached 98%.
Explanation	The total storage usage reached 98%.
Recommended action	No action is required.

DAC_STORE_STATE_FULL

Message text	DPI/4/DAC_STORE_STATE_FULL: The [STRING] alarm threshold (AlarmThreshold(1121)=[STRING]) for StoreName(1119)=[STRING] was reached.
Variable fields	$1: Threshold type: • storage time-based. • storage space-based. $2: Threshold value. $3: Service name.
Severity level	4
Example	DPI/4/DAC_STORE_STATE_FULL: The storage space-based alarm threshold (AlarmThreshold(1121)=80%) for StoreName(1119)=audit was reached. DPI/4/DAC_STORE_STATE_FULL: The storage time-based alarm threshold (AlarmThreshold(1121)=30 days) for StoreName(1119)=audit was reached.
Explanation	The data analysis center checks the storage space of each service to determine if the storage space-based threshold is reached on an per five minute basis. This message is sent if the storage space-based threshold of a service is reached.
Recommended action	No action is required.

DAC_STORE_DELETE_FILE

Message text	DPI/4/DAC_STORE_DELETE_FILE: Deleted data from the storage space of the [STRING] service because the [STRING] alarm threshold was reached.
Variable fields	$1: Service name. $2: Threshold type: • storage time-based. • storage space-based.
Severity level	4
Example	DPI/4/DAC_STORE_DELETE_FILE: Deleted data from the storage space of the audit service because the storage time-based alarm threshold was reached.
Explanation	This message is sent when one of the following events occur: • The expired data of a service was deleted when the storage time-based threshold was exceeded。 • The earliest data was deleted when the storage space-based threshold was exceeded.
Recommended action	No action is required.

DAC_HDD_FULL

Message text	DPI/4/DAC_HDD_FULL: New logs will be saved in [STRING] because less than 1 GB of free space is left in the disk.
Variable fields	$1: Name of the storage media file system: • hda0: • hda1: • hdb0: • hdb1: • usba0: • usbb0: • usbc0: • memory
Severity level	4
Example	DPI/4/DAC_OP_REPORT: New logs will be saved in memory because less than 1 GB of free space is left in the disk.
Explanation	The data analysis center will save new service data in memory because less than 1 GB of free space was left in the disk.
Recommended action	No action is required.

DEV messages

This section contains device management messages.

AUTOSWITCH_FAULT

Message text	[STRING] automatically switches between active and standby, and a fault occurs during the switching.
Variable fields	$1: Chassis number.
Severity level	1
Example	DEV/1/AUTO_SWITCH_FAULT: Chassis 1 automatically switches between active and standby, and a fault occurs during the switching, please contact technical support.
Explanation	A fault occurred during an automatic active/standby switchover of a device.
Recommended action	**35.** Manually restart the device to clear the fault. **36.** Before restarting the device, execute the javascript:infosearch(3077425) command to collect and save diagnostic information for troubleshooting. **37.** After the device restart, execute the **`display device`** command to identify the device status. If the device status is not **Normal**, contact NSFOCUS Support.

AUTOSWITCH_FAULT_REBOOT

Message text	[STRING] automatically switches between active and standby, and a fault occurs during the switching, the device will immediately restart [STRING] to restore the fault.
Variable fields	$1: Chassis number. $2: Chassis number and slot number or slot number.
Severity level	1
Example	DEV/1/AUTO_SWITCH_FAULT_REBOOT: Chassis 1 automatically switches between active and standby, and a fault occurs during the switching, the device will immediately restart chassis 1 slot 0 to restore the fault.
Explanation	A fault occurred during an active/standby switchover of a device. The device will automatically restart the faulty card to clear the fault.
Recommended action	Execute the **`display device`** command after the faulty card restarts to identify the card status. If the card status is not **Normal**, contact NSFOCUS Support.

BOARD_REBOOT

Message text	Board is rebooting on [STRING].
Variable fields	$1: Chassis number and slot number or slot number.
Severity level	5
Example	DEV/5/BOARD_REBOOT: Board is rebooting on slot 1.
Explanation	A card was manually or automatically rebooted.
Recommended action	If an unexpected automatic reboot occurred, perform the following tasks: **38.** Execute the **`display version`** command after the card starts up. **39.** Check the **Last reboot reason** field for the reboot reason. **40.** If an exception caused the reboot, contact HP Support.

BOARD_REMOVED

Message text	Board was removed from [STRING], type is [STRING].
Variable fields	$1: Chassis number and slot number or slot number. $2: Card type.
Severity level	3
Example	DEV/3/BOARD_REMOVED: Board was removed from slot 1, type is LSQ1FV48SA.
Explanation	An LPU or a standby MPU was removed from a member device, causing the device to leave the IRF fabric.
Recommended action	If the LPU or MPU was not manually removed, perform the following tasks: **41.** Verify that the card is securely seated. **42.** Replace the card if the message persists. **43.** Reboot the device to make it join the IRF fabric. **44.** If the problem persists, contact HP Support.

BOARD_RUNNING_FAULT

Message text	[STRING] is detected to be faulty.
Variable fields	$1: Chassis number and slot number or slot number.
Severity level	1
Example	DEV/1/ BOARD_FAULT_REBOOT: Chassis 1 slot 0 is detected to be faulty, please contact technical support.
Explanation	A card is faulty during the device operation.
Recommended action	**45.** Manually reboot the card to clear the fault. **46.** Before rebooting the card, execute the javascript:infosearch(3077425) command to collect and save diagnostic information for troubleshooting. **47.** After the card reboots, execute the **`display device`** command to identify the card status. If the card status is not **Normal**, contact NSFOCUS Support.

BOARD_RUNNING_FAULT_REBOOT

Message text		[STRING] is detected to be faulty, the device will immediately restart [STRING] to recover from the fault.
Variable fields		$1: Chassis number and slot number or slot number. $2: Chassis number and slot number or slot number.
Severity level		1
Example		DEV/1/ BOARD_RUNNING_FAULT_REBOOT: Chassis 1 slot 0 is detected to be faulty, the device will immediately restart chassis 1 slot 0 to recover from the fault.
Explanation		A card is faulty during device operation, and the device will reboot the card immediately to clear the fault.
Recommended action		After the card reboots, execute the **`display device`** command to identify the card status. If the card status is not **Normal**, contact NSFOCUS Support.

BOARD_STATE_FAULT

Message text	Board state changed to Fault on [STRING], type is [STRING].
Variable fields	$1: Chassis number and slot number or slot number. $2: Card type.
Severity Level	2
Example	DEV/2/BOARD_STATE_FAULT: Board state changed to Fault on slot 1, type is LSQ1FV48SA.
Exp	The card was starting up (initializing or loading software) or was not operating correctly.

Explanation	
Recommended action	• If the card was newly installed, wait for the card to start up. The required startup time varies by card model and software version and is typically less than 10 minutes. • If the card was not newly installed, contact HP Support.

BOARD_STATE_NORMAL

Message text	Board state changed to Normal on [STRING], type is [STRING].
Variable fields	$1: Chassis number and slot number or slot number. $2: Card type.
Severity level	5
Example	DEV/5/BOARD_STATE_NORMAL: Board state changed to Normal on slot 1, type is LSQ1FV48SA.
Explanation	A newly installed LPU or standby MPU completed initialization (on a single-CPU card) or the main CPU completed initialization (on a multi-CPU card).
Recommended action	No action is required.

CFCARD_INSERTED

Message text	CF card was inserted in [STRING] CF card slot [INT32].
Variable fields	$1: Chassis number and slot number or slot number. $2: CF card slot number.
Severity level	4
Example	DEV/4/CFCARD_INSERTED: CF card was inserted in slot 1 CF card slot 1.
Explanation	A CF card was installed.
Recommended action	No action is required.

CFCARD_REMOVED

Message text	CF card was removed from [STRING] CF card slot [INT32].
Variable fields	$1: Chassis number and slot number or slot number. $2: CF card slot number.
Severity level	3
Example	DEV/3/CFCARD_REMOVED: CF card was removed from slot 1 CF card slot 1.
Explanation	A CF card was removed.
Recommended action	If the CF card was not manually removed, perform the following tasks: **48.** Verify that the card is securely seated. **49.** Replace the card if the message persists. **50.** If the problem persists, contact HP Support.

CHASSIS_REBOOT

Message text	Chassis [INT32] is rebooting now.
Variable fields	$1: Chassis number.
Severity level	5
Example	DEV/5/CHASSIS_REBOOT: Chassis 1 is rebooting now.
Explanation	The chassis was manually or automatically rebooted.
Recommended action	If an unexpected automatic reboot occurs, perform the following tasks: 51. Execute the **`display version`** command after the chassis starts up. 52. Check the **Last reboot reason** field for the reboot reason. 53. If an exception caused the reboot, contact HP Support.

DEV_CLOCK_CHANGE

	Message text	-User=[STRING]-IPAddr=[IPADDR]; System clock changed from [STRING] to [STRING].
	Variable fields	$1: Username of the login user. $2: IP address of the login user. $3: Old time. $4: New time.
	Severity level	5
	Example	DEV/5/DEV_CLOCK_CHANGE: -User=admin-IPAddr=192.168.1.2; System clock changed from 15:49:52 01/02/2013 to 15:50:00 01/02/2013.
	Explanation	The system time changed.
	Recommended action	No action is required.

DEV_FAULT_TOOLONG

Message text	Card in [STRING] is still in Fault state for [INT32] minutes.
Variable fields	$1: Chassis number and slot number or slot number. $2: Time duration during which the card stayed in Fault state.
Severity level	4
Example	DEV/4/DEV_FAULT_TOOLONG: Card in slot 1 is still in Fault state for 60 minutes.
Explanation	A card stayed in Fault state for a long period of time.
Recommended action	**54.** Reboot the card. **55.** If the problem persists, contact HP Support.

FAN_ABSENT

Message text	Pattern 1: Fan [INT32] is absent. Pattern 2: Chassis [INT32] fan [INT32] is absent.
Variable fields	Pattern 1: $1: Fan tray number. Pattern 2: $1: Chassis number. $2: Fan tray number.
Severity level	3
Example	DEV/3/FAN_ABSENT: Fan 2 is absent.
Explanation	A fan tray was not in place.
Recommended action	**56.** Check the fan tray slot: ○ If the fan tray slot is empty, the temperature might have increased and the system recommends that you install a fan tray. ○ If a fan tray is present, verify that the fan tray is securely seated. **57.** Replace the fan tray if the message persists. **58.** If the problem persists, contact HP Support.

FAN_DIRECTION_NOT_PREFERRED

Message text	Fan [INT32] airflow direction is not preferred on [STRING], please check it.
Variable fields	$1: Fan tray number. $2: Chassis number and slot number or slot number.
Severity level	1
Example	DEV/1/FAN_DIRECTION_NOT_PREFERRED: Fan 1 airflow direction is not preferred on slot 1, please check it.
Explanation	The airflow direction of the fan tray is different from the airflow direction setting.
Recommended action	**59.** Verify that the airflow direction setting is correct. **60.** Verify that the fan tray model provides the same airflow direction as the configured setting. **61.** If the problem persists, contact HP Support.

FAN_FAILED

Message text	Pattern 1: Fan [INT32] failed. Pattern 2: Chassis [INT32] fan [INT32] failed.
Variable fields	Pattern 1: $1: Fan tray number. Pattern 2: $1: Chassis number. $2: Fan tray number.
Severity level	2
Example	DEV/2/FAN_FAILED: Fan 2 failed.
Explanation	The fan tray stopped because of an exception.
Recommended action	Replace the fan tray.

FAN_RECOVERED

Message text	Pattern 1: Fan [INT32] recovered. Pattern 2: Chassis [INT32] fan [INT32] recovered.
Variable fields	Pattern 1: $1: Fan tray number. Pattern 2: $1: Chassis number. $2: Fan tray number.
Severity level	5
Example	DEV/5/FAN_RECOVERED: Fan 2 recovered.
Explanation	The fan tray started to operate correctly after it was installed.
Recommended action	No action is required.

MAD_ DETECT

Message text	Multi-active devices detected, please fix it.
Variable fields	N/A
Severity level	1
Example	DEV/1/MAD_DETECT: Multi-active devices detected, please fix it.
Explanation	Multiple member devices were found active.
Recommended action	**62.** Use the **display irf** command to view which member devices have left the original IRF fabric. **63.** Use the **display irf link** command to locate the IRF link with problems. **64.** Fix the IRF link in DOWN state.

MAD_PROC

	Message text	[STRING] protocol detected MAD conflict: Local health value=[UINT32], Peer health value=[UINT32].
	Variable fields	$1: Protocol that detected the MAD conflict, ARP, ND, LACP, or BFD. $2: Current health value of the local IRF. $3: Current health value of the peer IRF.
	Severity level	6
	Example	DEV/6/MAD_PROC: ARP protocol detected MAD conflict: Local health value=1, Peer health value=0.
	Explanation	ARP, ND, LACP, or BFD detected a MAD conflict on the IRF fabric. A health value of 0 indicates that the IRF fabric is healthy. A greater health value indicates a worse health situation.
	Recommended action	No action is required.

POWER_ABSENT

Message text	Pattern 1: Power [INT32] is absent. Pattern 2: Chassis [INT32] power [INT32] is absent.
Variable fields	Pattern 1: $1: Power supply number. Pattern 2: $1: Chassis number. $2: Power supply number.
Severity level	3
Example	DEV/3/POWER_ABSENT: Power 1 is absent.
Explanation	A power supply was removed.
Recommended action	**65.** Check the power supply slot. ○ If the power supply slot is empty, install a power supply. ○ If a power supply is present, verify that the power supply is securely seated. **66.** If the problem persists, replace the power supply. **67.** If the problem persists, contact HP Support.

POWER_FAILED

	Message text	Pattern 1: Power [INT32] failed. Pattern 2: Chassis [INT32] power [INT32] failed.
	Variable fields	Pattern 1: $1: Power supply number. Pattern 2: $1: Chassis number. $2: Power supply number.
	Severity level	2
	Example	DEV/2/POWER_FAILED: Power 1 failed.
	Explanation	A power supply failed.
	Recommended action	Replace the power supply.

POWER_FAILED_SHUTDOWN

Message text	Pattern 1: Power [INT32] shutdown. Reason: temperature of the power is too high. Pattern 2: Chassis [INT32] power [INT32] shutdown. Reason: temperature of the power is too high.
Variable fields	Pattern 1: $1: Power supply number. Pattern 2: $1: Chassis number. $2: Power supply number.
Severity level	2
Example	DEV/2/POWER_FAILED_SHUTDOWN: Power 1 shutdown. Reason: temperature of the power is too high.
Explanation	A power supply was shut down because its temperature is too high. The status of the power supply changed to FAILED.
Recommended action	Verify that the power supply is well ventilated and cooled.

POWER_MONITOR_ABSENT

Message text	Pattern 1: Power monitor unit [INT32] is absent. Pattern 2: Chassis [INT32] power monitor unit [INT32] is absent.
Variable fields	Pattern 1: $1: Power monitoring module number. Pattern 2: $1: Chassis number. $2: Power monitoring module number.
Severity level	3
Example	DEV/3/POWER_MONITOR_ABSENT: Power monitor unit 1 is absent.
Explanation	A power monitoring module was removed.
Recommended action	**68.** Check the power monitoring module slot. ○ If the power monitoring module slot is empty, install a power monitoring module. ○ If a power monitoring module is present, verify that the power monitoring module is securely seated. **69.** If the problem persists, replace the power monitoring module. **70.** If the problem persists, contact HP Support.

POWER_MONITOR_FAILED

Message text	Pattern 1: Power monitor unit [INT32] failed. Pattern 2: Chassis [INT32] power monitor unit [INT32] failed.
Variable fields	Pattern 1: $1: Power monitoring module number. Pattern 2: $1: Chassis number. $2: Power monitoring module number.
Severity level	2
Example	DEV/2/POWER_MONITOR_FAILED: Power monitor unit 1 failed.
Explanation	A power monitoring module failed.
Recommended action	Replace the power monitoring module.

POWER_MONITOR_RECOVERED

Message text	Pattern 1: Power monitor unit [INT32] recovered. Pattern 2: Chassis [INT32] power monitor unit [INT32] recovered.
Variable fields	Pattern 1: $1: Power monitoring module number. Pattern 2: $1: Chassis number. $2: Power monitoring module number.
Severity level	5
Example	DEV/5/POWER_MONITOR_RECOVERED: Power monitor unit 1 recovered.
Explanation	The power monitoring module started to operate correctly after it was installed.
Recommended action	No action is required.

POWER_RECOVERED

Message text		Pattern 1: Power [INT32] recovered. Pattern 2: Chassis [INT32] power [INT32] recovered.
Variable fields		Pattern 1: $1: Power supply number. Pattern 2: $1: Chassis number. $2: Power supply number.
Severity level		5
Example		DEV/5/POWER_RECOVERED: Power 1 recovered.
Explanation		The power supply started to operate correctly after it was installed.
Recommended action		No action is required.

RPS_ABSENT

Message text	Pattern 1: RPS [INT32] is absent. Pattern 2: Chassis [INT32] RPS [INT32] is absent.
Variable fields	Pattern 1: $1: RPS number. Pattern 2: $1: Chassis number. $2: RPS number.
Severity level	3
Example	DEV/3/RPS_ABSENT: RPS 1 is absent.
Explanation	An RPS was removed.
Recommended action	**71.** Check the RPS slot. ○ If the RPS slot is empty, install an RPS. ○ If an RPS is present, verify that the RPS is securely seated. **72.** If the problem persists, replace the RPS. **73.** If the problem persists, contact HP Support.

RPS_NORMAL

	Message text	Pattern 1: RPS [INT32] is normal. Pattern 2: Chassis [INT32] RPS [INT32] is normal.
	Variable fields	Pattern 1: $1: RPS number. Pattern 2: $1: Chassis number. $2: RPS number.
	Severity level	5
	Example	DEV/5/RPS_NORMAL: RPS 1 is normal.
	Explanation	The RPS started to operate correctly after it was installed.
	Recommended action	No action is required.

SUBCARD_FAULT

Message text	Subcard state changed to Fault on [STRING] subslot [INT32], type is [STRING].
Variable fields	$1: Chassis number and slot number or slot number. $2: Subslot number. $3: Subcard type.
Severity Level	2
Example	DEV/2/SUBCARD_FAULT: Subcard state changed to Fault on slot 1 subslot 1, type is MIM-1ATM-OC3SML.
Exp	The subcard failed, or its status changed to **Fault** after it was rebooted.

lanation	
Recommended action	Track the status of the subcard. • If the status of the subcard changes to **Normal** later, no action is required. • If the status is always **Fault**, replace the subcard.

SUBCARD_INSERTED

Message text	Subcard was inserted in [STRING] subslot [INT32], type is [STRING].
Variable fields	$1: Chassis number and slot number or slot number. $2: Subslot number. $3: Subcard type.
Severity level	4
Example	DEV/4/SUBCARD_INSERTED: Subcard was inserted in slot 1 subslot 1, type is MIM-1ATM-OC3SML.
Explanation	A subcard was installed.
Recommended action	No action is required.

SUBCARD_REBOOT

Message text	Subcard is rebooting on [STRING] subslot [INT32].
Variable fields	$1: Chassis number and slot number or slot number. $2: Subslot number.
Severity level	5
Example	DEV/5/SUBCARD_REBOOT: Subcard is rebooting on slot 1 subslot 1.
Exp	The subcard was manually or automatically rebooted.

Explanation	
Recommended action	• If the subcard operates correctly after it starts up, no action is required. • If you want to know the reboot reason or the subcard keeps rebooting, contact HP Support.

SUBCARD_REMOVED

Message text	Subcard was removed from [STRING] subslot [INT32], type is [STRING].
Variable fields	$1: Chassis number and slot number or slot number. $2: Subslot number. $3: Subcard type.
Severity level	3
Example	DEV/3/SUBCARD_REMOVED: Subcard was removed from slot 1 subslot 1, type is MIM-1ATM-OC3SML.
Explanation	A subcard was removed.
Recommended action	If the subcard was not manually removed, perform the following tasks: **74.** Verify that the subcard is securely seated. **75.** Replace the subcard if the message persists. **76.** If the problem persists, contact HP Support.

SYSTEM_REBOOT

Message text	System is rebooting now.
Variable fields	N/A
Severity level	5
Example	DEV/5/SYSTEM_REBOOT: System is rebooting now.
Explanation	The system was manually or automatically rebooted.
Recommended action	If an unexpected automatic reboot occurred, perform the following tasks: 77. Execute the **display version** command after the system starts up. 78. Check the **Last reboot reason** field for the reboot reason. 79. If an exception caused the reboot, contact HP Support.

TEMPERATURE_ALARM

	Message text	Pattern 1: Temperature is greater than the high-temperature alarming threshold on sensor [STRING] [USHOT]. Current temperature is [INT32] degrees centigrade. Pattern 2: Temperature is greater than the high-temperature alarming threshold on [STRING] sensor [STRING] [USHOT]. Current temperature is [INT32] degrees centigrade. Pattern 3: Temperature is greater than the high-temperature alarming threshold on [STRING] [STRING] sensor [STRING] [USHOT]. Current temperature is [INT32] degrees centigrade.
	Variable fields	Pattern 1: $1: Sensor type. $2: Sensor number. $3: Current temperature in centigrade. Pattern 2: $1: Slot number. $2: Sensor type. $3: Sensor number. $4: Current temperature in centigrade. Pattern 3: $1: Chassis number. $2: Slot number. $3: Sensor type. $4: Sensor number. $5: Current temperature in centigrade.
	Severity level	4
	Example	DEV/4/TEMPERATURE_ALARM: Temperature is greater than the

	high-temperature alarming threshold on slot 1 sensor inflow 1. Current temperature is 80 degrees centigrade.
Explanation	A sensor's temperature exceeded the high-temperature alarming threshold. The ambient temperature was too high or the fan tray was not operating correctly.
Recommended action	**80.** Verify that the ambient temperature is normal and the ventilation system is operating correctly. **81.** Use the **`display fan`** command to verify that the fan trays are in position and operating correctly. If a fan tray is missing, install the fan tray. If a fan tray does not operate correctly, replace it.

TEMPERATURE_LOW

	Message text	Pattern 1: Temperature is less than the low-temperature threshold on sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade. Pattern 2: Temperature is less than the low-temperature threshold on [STRING] sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade. Pattern 3: Temperature is less than the low-temperature threshold on [STRING] [STRING] sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade.
	Variable fields	Pattern 1: $1: Sensor type. $2: Sensor number. $3: Current temperature in centigrade. Pattern 2: $1: Slot number. $2: Sensor type. $3: Sensor number. $4: Current temperature in centigrade. Pattern 3: $1: Chassis number. $2: Slot number. $3: Sensor type. $4: Sensor number. $5: Current temperature in centigrade.
	Severity level	4

Example	DEV/4/TEMPERATURE_LOW: Temperature is less than the low-temperature threshold on slot 1 sensor inflow 1. Current temperature is -10 degrees centigrade.
Explanation	A sensor's temperature fell below the low-temperature threshold.
Recommended action	Adjust the ambient temperature higher.

TEMPERATURE_NORMAL

	Message text	Pattern 1: Temperature changed to normal on sensor [STRING] [INT32]. Pattern 2: Temperature changed to normal on [STRING] sensor [STRING] [INT32]. Pattern 3: Temperature changed to normal on [STRING] [STRING] sensor [STRING] [INT32].
	Variable fields	Pattern 1: $1: Sensor type. $2: Sensor number. Pattern 2: $1: Slot number. $2: Sensor type. $3: Sensor number. Pattern 3: $1: Chassis number. $2: Slot number. $3: Sensor type. $4: Sensor number.
	Severity level	5
	Example	DEV/5/TEMPERATURE_NORMAL: Temperature changed to normal on slot 1 sensor inflow 1.
	Explanation	A sensor's temperature was normal (between the low-temperature threshold and the high-temperature warning threshold).
	Recommended action	No action is required.

TEMPERATURE_SHUTDOWN

	Message text	Pattern 1: Temperature is greater than the high-temperature shutdown threshold on sensor [STRING] [INT32]. The slot will be powered off automatically. Current temperature is [INT32] degrees centigrade. Pattern 2: Temperature is greater than the high-temperature shutdown threshold on [STRING] sensor [STRING] [INT32]. The slot will be powered off automatically. Current temperature is [INT32] degrees centigrade. Pattern 3: Temperature is greater than the high-temperature shutdown threshold on [STRING] [STRING] sensor [STRING] [INT32]. The slot will be powered off automatically. Current temperature is [INT32] degrees centigrade.
	Variable fields	Pattern 1: $1: Sensor type. $2: Sensor number. $3: Current temperature in centigrade. Pattern 2: $1: Slot number. $2: Sensor type. $3: Sensor number. $4: Current temperature in centigrade. Pattern 3: $1: Chassis number. $2: Slot number. $3: Sensor type. $4: Sensor number. $5: Current temperature in centigrade.
	Severity level	2
	Example	DEV/2/TEMPERATURE_SHUTDOWN: Temperature is greater

	than the high-temperature shutdown threshold on slot 1 sensor inflow 1. The slot will be powered off automatically. Current temperature is 60 degrees centigrade.
Explanation	A sensor's temperature exceeded the high-temperature shutdown threshold. The ambient temperature was too high or the fan tray was not operating correctly.
Recommended action	**82.** Verify that the ambient temperature is normal and the ventilation system is operating correctly. **83.** Use the **`display fan`** command to verify that the fan trays are in position and operating correctly. If a fan tray is missing, install the fan tray. If a fan tray does not operate correctly, replace it.

TEMPERATURE_WARNING

	Message text	Pattern 1: Temperature is greater than the high-temperature warning threshold on sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade. Pattern 2: Temperature is greater than the high-temperature warning threshold on [STRING] sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade. Pattern 3: Temperature is greater than the high-temperature warning threshold on [STRING] [STRING] sensor [STRING] [INT32]. Current temperature is [INT32] degrees centigrade.
	Variable fields	Pattern 1: $1: Sensor type. $2: Sensor number. $3: Current temperature in centigrade. Pattern 2: $1: Slot number. $2: Sensor type. $3: Sensor number. $4: Current temperature in centigrade. Pattern 3: $1: Chassis number. $2: Slot number. $3: Sensor type. $4: Sensor number. $5: Current temperature in centigrade.
	Severity level	4
	Example	DEV/4/TEMPERATURE_WARNING: Temperature is greater than the high-temperature warning

	threshold on slot 1 sensor inflow 1. Current temperature is 50 degrees centigrade.
Explanation	A sensor's temperature exceeded the high-temperature warning threshold. The ambient temperature was too high or the fan tray was not operating correctly.
Recommended action	**84.** Verify that the ambient temperature is normal and the ventilation system is operating correctly. **85.** Use the **`display fan`** command to verify that the fan trays are in position and operating correctly. If a fan tray is missing, install the fan tray. If a fan tray does not operate correctly, replace it.

TIMER_CREATE_FAILED_FIRST

Message text	The process with PID [UINT] failed to create a timer. Reason for the failure:[STRING].
Variable fields	$1: PID of the process. $2: Reason for the first timer creation failure. The value is "Maximum number of timers already reached."
Severity Level	4
Example	DEV/4/TIMER_CREATE_FAILED_FIRST: The process with PID 70 failed to create a timer. Reason for the failure: Maximum number of timers already reached.
Exp	The system outputs this message when a process fails to create a timer for the first time.

lanation	The system uses the following mechanism to avoid frequent output of messages that report timer creation failures: • The system outputs a TIMER_CREATE_FAILED_FIRST message when a process fails to create a timer for the first time. • If a timer creation failure occurs again 15 minutes after the first failure, the system outputs a TIMER_CREATE_FAILED_MORE message. • The TIMER_CREATE_FAILED_MORE message records last time when the timer creation failure message was generated, and the number of timer creation failures between the last and current messages that report timer creation failures. The system does not generate log messages about timer creation failures that occurred within the 15 minutes.
Recommended acti	**86.** Restart the device to recover the service module corresponding to the process. **87.** If the problem persists, contact HP Support.

o **n**	

TIMER_CREATE_FAILED_MORE

Message text	The process with PID [UINT] failed to create a timer:[UINT] consecutive failures since [STRING].Reason for the failure:[STRING].
Variable fields	$1: PID of the process. $2: Number of timer creation failures between the last and current messages that report time creation failures. $3: Last time when the creation failure log message was generated. $4: Reason for this timer creation failure. The value is "Maximum number of timers already reached."
Severity Level	4
Example	DEV/4/TIMER_CREATE_FAILED_MORE: The process with PID 70 failed to create a timer:2 consecutive failures since 2019/11/21 16:00:00.Reason for the failure: Maximum number of timers already reached.
Exp	The system outputs this message when a process fails to create a timer again 15 minutes after the

Explanation	first-time creation failure. The system uses the following mechanism to avoid frequent output of messages that report timer creation failures: • The system outputs a TIMER_CREATE_FAILED_FIRST message when a process fails to create a timer for the first time. • If a timer creation failure occurs again 15 minutes after the first failure, the system outputs a TIMER_CREATE_FAILED_MORE message. • The TIMER_CREATE_FAILED_MORE message records last time when the timer creation failure message was generated, and the number of timer creation failures between the last and current messages that report timer creation failures. The system does not generate log messages about timer creation failures that occurred within the 15 minutes.
Recommended act	**88.** Restart the device to recover the service module corresponding to the process. **89.** If the problem persists, contact HP Support.

ion	

VCHK_VERSION_INCOMPATIBLE

Message text	Software version of [STRING] is incompatible with that of the MPU.
Variable fields	$1: Chassis number and slot number or slot number.
Severity level	1
Example	DEV/1/VCHK_VERSION_INCOMPATIBLE: Software version of slot 1 is incompatible with that of the MPU.
Explanation	A PEX that was starting up detected that its software version is incompatible with the parent device's software version.
Recommended action	Specify a set of startup software images for the PEX. Make sure the images are compatible with the parent device's software images.

DFILTER messages

This section contains data filtering syslog messages.

DFILTER_IPV4_LOG

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];DataDirection(1081)=[STRING];RuleName(1080)=[STRING];PolicyName(1079)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZone(1025)=[STRING];DstZone(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];FileName(1097)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Data direction. Available values are: o Upload. o Download. o Both. $4: Rule name. $5: Policy name. $6: Source IP address. $7: Source port number. $8: Destination IP address. $9: Destination port number. $10: Source security zone. $11: Destination security zone. $12: Name of the identity user. $13: Action applied to the packet. Available actions are: o Permit. o Drop. $14: File name. $15: VLAN ID $16: VXLAN ID $17: Source location. $18: Destination location.
Severity level	6
Example	DFILTER/6/DFILTER_IPV4_LOG:-MDC=1;Protocol(1001)=TCP;Application(1002)=SMTP;DataDirection(1081)=upload;RuleName(1080)=ruletest;PolicyName(1079)=policytest;SrcIPAddr(1003)=21.22.23.20;SrcPort(1004)=51396;DstIPAddr(1007)=25.26.27.20;DstPort(1008)=25;SrcZone(1025)=in;DstZone(1035)=in;UserName(1113)=abc;Action(1053)=drop;FileName(1097)=123.txt;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	An IPv4 packet matched a data filtering rule.
Recommended action	No action is required.

DFILTER_IPV6_LOG

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];DataDirection(1081)=[STRING];RuleName(1080)=[STRING];PolicyName(1079)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZone(1025)=[STRING];DstZone(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];FileName(1097)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Data direction. Available values are: o Upload. o Download. o Both. $4: Rule name. $5: Policy name. $6: Source IPv6 address. $7: Source port number. $8: Destination IPv6 address. $9: Destination port number. $10: Source security zone. $11: Destination security zone. $12: Username. $13:Action applied to the packet. Available actions are: o Permit. o Drop. $14: File name. $15: VLAN ID $16: VXLAN ID $17: Source location. $18: Destination location.
Severity level	6
Example	DFILTER/6/DFILTER_IPV6_LOG:-MDC=1;Protocol(1001)=TCP;Application(1002)=SMTP;DataDirection(1081)=upload;RuleName(1080)=ruletest;PolicyName(1079)=policytest;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZone(1025)=in;DstZone(1035)=in;UserName(1113)=aaa;Action(1053)=drop;FileName(1097)=123.txt;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	An IPv6 packet matched a data filtering rule.
Recommended action	No action is required.

DHCP

This section contains DHCP messages.

DHCP_NOTSUPPORTED

Message text	Failed to apply filtering rules for DHCP packets because some rules are not supported.
Variable fields	N/A
Severity level	3
Example	DHCP/3/DHCP_NOTSUPPORTED: Failed to apply filtering rules for DHCP packets because some rules are not supported.
Explanation	The system failed to apply filtering rules for DHCP packets because some rules are not supported on the device.
Recommended action	No action is required.

DHCP_NORESOURCES

Message text	Failed to apply filtering rules for DHCP packets because hardware resources are insufficient.
Variable fields	N/A
Severity level	3
Example	DHCP/3/DHCP_NORESOURCES: Failed to apply filtering rules for DHCP packets because hardware resources are insufficient.
Explanation	The system failed to apply filtering rules for DHCP packets because the hardware resources are insufficient.
Recommended action	Release hardware resources and then apply the rules again.

DHCPS messages

This section contains DHCP server messages.

DHCPS_ALLOCATE_IP

Message text	DHCP server received a DHCP client's request packet on interface [STRING], and allocated an IP address [IPADDR](lease [UINT32] seconds) for the DHCP client(MAC [MAC]) from [STRING] pool.
Variable fields	$1: Name of the interface on which DHCP server is configured. $2: IPv4 address assigned to the DHCP client. $3: Lease duration of the assigned IPv4 address. $4: MAC address of the DHCP client. $5: Name of the address pool to which the assigned IPv4 address belongs.
Severity level	5
Example	DHCPS/5/DHCPS_ALLOCATE_IP: DHCP server received a DHCP client's request packet on interface Ethernet0/2, and allocated an IP address 1.0.0.91(lease 86400 seconds) for the DHCP client(MAC 0000-0000-905a) from p1 pool.
Explanation	The DHCP server assigned an IPv4 address with a lease to a DHCP client.
Recommended action	No action is required.

DHCPS_CONFLICT_IP

Message text	A conflict IP [IPADDR] from [STRING] pool was detected by DHCP server on interface [STRING].
Variable fields	$1: IPv4 address that is in conflict. $2: Name of the address pool to which the conflicting IPv4 address belongs. $3: Name of the interface on which DHCP server is configured.
Severity level	5
Example	DHCPS/5/DHCPS_CONFLICT_IP: A conflict IP 100.1.1.1 from p1 pool was detected by DHCP server on interface Ethernet0/2.
Explanation	The DHCP server deleted a conflicting IPv4 address from an address pool.
Recommended action	No action is required.

DHCPS_EXTEND_IP

Message text	DHCP server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IP [IPADDR], MAC [MAC]).
Variable fields	$1: Name of the interface on which DHCP server is configured. $2: Name of the address pool to which the client's IPv4 address belongs. $3: IPv4 address of the DHCP client. $4: MAC address of the DHCP client.
Severity level	5
Example	DHCPS/5/DHCPS_EXTEND_IP: DHCP server received a DHCP client's request packet on interface Ethernet0/2, and extended lease from p1 pool for the DHCP client (IP 1.0.0.91, MAC 0000-0000-905a).
Explanation	The DHCP server extended the lease for a DHCP client.
Recommended action	No action is required.

DHCPS_FILE

Message text	Failed to save DHCP client information due to lack of storage resources.
Variable fields	N/A
Severity level	4
Example	DHCPS/4/DHCPS_FILE: Failed to save DHCP client information due to lack of storage resources.
Explanation	The DHCP server failed to back up DHCP bindings to the backup file due to lack of storage resources.
Recommended action	Delete unnecessary files to release resources.

DHCPS_RECLAIM_IP

Message text	DHCP server reclaimed a [STRING] pool's lease(IP [IPADDR], lease [UINT32] seconds), which is allocated for the DHCP client (MAC [MAC]).
Variable fields	$1: Name of the address pool to which the assigned IPv4 address belongs. $2: IPv4 address assigned to the DHCP client. $3: Lease duration of the assigned IPv4 address. $4: MAC address of the DHCP client.
Severity level	5
Example	DHCPS/5/DHCPS_RECLAIM_IP: DHCP server reclaimed a p1 pool's lease(IP 1.0.0.91, lease 86400 seconds), which is allocated for the DHCP client (MAC 0000-0000-905a).
Explanation	The DHCP server reclaimed the IPv4 address assigned to a DHCP client.
Recommended action	No action is required.

DHCPS_VERIFY_CLASS

Message text	Illegal DHCP client-PacketType=[STRING]-ClientAddress=[MAC];
Variable fields	$1: Type of the packet. $2: Hardware address of the DHCP client.
Severity level	5
Example	DHCPS/5/DHCPS_VERIFY_CLASS: Illegal DHCP client-PacketType= DHCPDISCOVER-ClientAddress=0000-5e01-0104;
Explanation	The DHCP server verified that the DHCP client was not on the user class whitelist.
Recommended action	Check the validity of the DHCP client.

DHCPS6 messages

This section contains DHCPv6 server messages.

DHCPS6_ALLOCATE_ADDRESS

Message text	DHCPv6 server received a DHCPv6 client's request packet on interface [STRING], and allocated an IPv6 address [IPADDR] (lease [UINT32] seconds) for the DHCP client(DUID [HEX], IAID [HEX]) from [STRING] pool.
Variable fields	$1: Name of the interface on which DHCPv6 server is configured. $2: IPv6 address assigned to the DHCPv6 client. $3: Lease duration of the assigned IPv6 address. $4: DUID of the DHCPv6 client. $5: IAID of the DHCPv6 client. $6: Name of the address pool to which the assigned IPv6 address belongs.
Severity level	5
Example	DHCPS6/5/DHCPS6_ALLOCATE_ADDRESS: DHCPv6 server received a DHCPv6 client's request packet on interface Ethernet0/2, and allocated an IPv6 address 2000::3(lease 60 seconds) for the DHCP client(DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f) from p1 pool.
Explanation	The DHCPv6 server assigned an IPv6 address with a lease to a DHCPv6 client.
Recommended action	No action is required.

DHCPS6_ALLOCATE_PREFIX

Message text	DHCPv6 server received a DHCPv6 client's request packet on interface [STRING], and allocated an IPv6 prefix [IPADDR] (lease [UINT32] seconds) for the DHCP client(DUID [HEX], IAID [HEX]) from [STRING] pool.
Variable fields	$1: Name of the interface on which DHCPv6 server is configured. $2: IPv6 prefix assigned to the DHCPv6 client. $3: Lease duration of the assigned IPv6 prefix. $4: DUID of the DHCPv6 client. $5: IAID of the DHCPv6 client. $6: Name of the address pool to which the assigned IPv6 prefix belongs.
Severity level	5
Example	DHCPS6/5/DHCPS6_ALLOCATE_PREFIX: DHCPv6 server received a DHCPv6 client's request packet on interface Ethernet0/2, and allocated an IPv6 prefix 2000::(lease 60 seconds) for the DHCP client(DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f) from p1 pool.
Explanation	The DHCPv6 server assigned an IPv6 prefix with a lease to a DHCPv6 client.
Recommended action	No action is required.

DHCPS6_CONFLICT_ADDRESS

Message text	A conflict IPv6 address [IPADDR] from [STRING] pool was detected by DHCPv6 server on interface [STRING].
Variable fields	$1: IPv6 address that is in conflict. $2: Name of the address pool to which the conflicting IPv6 address belongs. $3: Name of the interface on which DHCPv6 server is configured.
Severity level	5
Example	DHCPS6/5/DHCPS6_CONFLICT_ADDRESS: A conflict IPv6 address 33::1 from p1 pool was detected by DHCPv6 server on interface Ethernet0/2.
Explanation	The DHCPv6 server deleted a conflicting IPv6 address from an address pool.
Recommended action	No action is required.

DHCPS6_EXTEND_ADDRESS

Message text	DHCPv6 server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IPv6 address [IPADDR], DUID [HEX], IAID [HEX]).
Variable fields	$1: Name of the interface on which DHCPv6 server is configured. $2: Name of the address pool to which the client's IPv6 address belongs. $3: IPv6 address of the DHCPv6 client. $4: DUID of the DHCPv6 client. $5: IAID of the DHCPv6 client.
Severity level	5
Example	DHCPS6/5/DHCPS6_EXTEND_ADDRESS: DHCPv6 server received a DHCP client's request packet on interface Ethernet0/2, and extended lease from p1 pool for the DHCP client (IPv6 address 2000::3, DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
Explanation	The DHCPv6 server extended the address lease for a DHCPv6 client.
Recommended action	No action is required.

DHCPS6_EXTEND_PREFIX

Message text	DHCPv6 server received a DHCP client's request packet on interface [STRING], and extended lease from [STRING] pool for the DHCP client (IPv6 prefix [IPADDR], DUID [HEX], IAID [HEX]).
Variable fields	$1: Name of the interface on which DHCPv6 server is configured. $2: Name of the address pool to which the client's IPv6 prefix belongs. $3: IPv6 prefix of the DHCPv6 client. $4: DUID of the DHCPv6 client. $5: IAID of the DHCPv6 client.
Severity level	5
Example	DHCPS6/5/DHCPS6_EXTEND_PREFIX: DHCPv6 server received a DHCP client's request packet on interface Ethernet0/2, and extended lease from p1 pool for the DHCP client (IPv6 prefix 2000::, DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
Explanation	The DHCPv6 server extended the prefix lease for a DHCPv6 client.
Recommended action	No action is required.

DHCPS6_FILE

Message text	Failed to save DHCP client information due to lack of storage resources.
Variable fields	N/A
Severity level	4
Example	DHCPS6/4/DHCPS6_FILE: Failed to save DHCP client information due to lack of storage resources.
Explanation	The DHCPv6 server failed to back up DHCPv6 bindings to the backup file due to lack of storage resources.
Recommended action	Delete unnecessary files to release resources.

DHCPS6_RECLAIM_ADDRESS

Message text	DHCPv6 server reclaimed a [STRING] pool's lease(IPv6 address [IPADDR], lease [UINT32] seconds), which is allocated for the DHCPv6 client (DUID [HEX], IAID [HEX]).
Variable fields	$1: Name of the address pool to which the assigned IPv6 address belongs. $2: IPv6 address assigned to the DHCPv6 client. $3: Lease duration of the assigned IPv6 address. $4: DUID of the DHCPv6 client. $5: IAID of the DHCPv6 client.
Severity level	5
Example	DHCPS6/5/DHCPS6_RECLAIM_ADDRESS: DHCPv6 server reclaimed a p1 pool’s lease(IPv6 address 2000::3, lease 60 seconds), which is allocated for the DHCPv6 client (DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
Explanation	The DHCPv6 server reclaimed the IPv6 address assigned to a DHCPv6 client.
Recommended action	No action is required.

DHCPS6_RECLAIM_PREFIX

Message text	DHCPv6 server reclaimed a [STRING] pool's lease(IPv6 prefix [IPADDR], lease [INTEGER] seconds), which is allocated for the DHCPv6 client (DUID [HEX], IAID [HEX]).
Variable fields	$1: Name of the address pool to which the assigned IPv6 prefix belongs. $2: IPv6 prefix assigned to the DHCPv6 client. $3: Lease duration of the assigned IPv6 prefix. $4: DUID of the DHCPv6 client. $5: IAID of the DHCPv6 client.
Severity level	5
Example	DHCPS6/5/DHCPS6_RECLAIM_PREFIX: DHCPv6 server reclaimed a p1 pool's lease(IPv6 prefix 2000::, lease 60 seconds), which is allocated for the DHCPv6 client (DUID 0001000118137c37b4b52facab5a, IAID 10b4b52f).
Explanation	The DHCPv6 server reclaimed the IPv6 prefix assigned to a DHCPv6 client.
Recommended action	No action is required.

DHCPSP4

This section contains DHCP snooping messages.

DHCPSP4_FILE

Message text	Failed to save DHCP client information due to lack of storage resources.
Variable fields	N/A
Severity level	4
Example	DHCPSP4/4/DHCPSP4_FILE: Failed to save DHCP client information due to lack of storage resources.
Explanation	The DHCP snooping device failed to back up DHCP snooping entries to the backup file due to lack of storage resources.
Recommended action	Delete unnecessary files to release resources.

DHCPSP6

This section contains DHCPv6 snooping messages.

DHCPSP6_FILE

Message text	Failed to save DHCP client information due to lack of storage resources.
Variable fields	N/A
Severity level	4
Example	DHCPSP6/4/DHCPSP6_FILE: Failed to save DHCP client information due to lack of storage resources.
Explanation	The DHCPv6 snooping device failed to back up DHCPv6 snooping entries to the backup file due to lack of storage resources.
Recommended action	Delete unnecessary files to release resources.

DIAG messages

This section contains diagnostic messages.

CORE_EXCEED_THRESHOLD

Message text	Usage of CPU [int]core [int] exceeded the threshold ([string]).
Variable fields	$1: CPU number. $2: CPU core number. $3: CPU core usage threshold.
Severity level	1
Example	DIAG/1/CORE_EXCEED_THRESHOLD: Usage of CPU 0 core 2 exceeded the threshold (1%).
Explanation	The device samples CPU core usage at intervals and calculates the average value during each CPU core usage statistics interval. If the value during an interval is greater than the CPU core usage threshold, the device generates this log message.
Recommended action	If this message appears frequently, perform the tasks: **90.** Execute the **`display process`** command to display process status information. **91.** Execute the **`display cpu-usage configuration`** command to display the CPU core usage threshold settings. **92.** Use the **`monitor cpu-usage threshold`** command to adjust the CPU core usage threshold settings as required.

CORE_RECOVERY

Message text	Core usage alarm CPU [int]core [int]removed.
Variable fields	$1: CPU number. $2: CPU core number.
Severity level	5
Example	DIAG/5/CORE_RECOVERY: Core usage alarm CPU 0 core 1 removed.
Explanation	The CPU core usage dropped below the CPU core usage threshold. The alarm was removed.
Recommended action	No action is required.

CPU_EXCEED_THRESHOLD

Message text	CPU usage threshold has been exceeded.
Variable fields	N/A
Severity level	1
Example	DIAG/1/CPU_EXCEED_THRESHOLD: CPU usage threshold has been exceeded.
Explanation	A CPU usage alarm occurred. This message is sent when the CPU usage exceeds the CPU usage alarm threshold.
Recommended action	Verify that appropriate CPU usage alarm thresholds are set. To view the CPU usage alarm thresholds, use the **`display current-configuration	include "monitor cpu-usage threshold"`** command. To change the CPU usage alarm thresholds, use the **`monitor cpu-usage threshold`** command.

CPU_RECOVER_THRESHOLD

Message text	CPU usage has dropped down to normal levels.
Variable fields	N/A
Severity level	1
Example	DIAG/1/CPU_RECOVER_THRESHOLD: CPU usage has dropped down to normal levels.
Explanation	A CPU usage alarm was removed. This message is sent when the CPU usage drops to or below the CPU usage recovery threshold.
Recommended action	No action is required.

CPU_USAGE_LASTMINUTE

Message text	CPU usage was [STRING] in last minute.
Variable fields	$1: CPU usage in percentage.
Severity level	5
Example	DIAG/5/CPU_USAGE_LASTMINUTE: CPU usage was 10% in last minute.
Explanation	Average CPU usage in last minute.
Recommended action	No action is required.

DIAG_DEADLOOP_DETECT

Message text	Dead loop detected on [string] cpu [int] core [int].
Variable fields	$1: Chassis number and slot number or slot number. $2: CPU number. $3: CPU core number.
Severity level	0
Example	DIAG/0/ DIAG_DEADLOOP_DETECT: Deadloop detected on slot 1 cpu 0 core 0.
Explanation	A kernel thread deadloop was detected.
Recommended action	Troubleshoot the relevant processes.

DIAG_STORAGE_BELOW_THRESHOLD

Message text	The usage of [STRING] ([UINT32]%) has dropped below the threshold of [UINT32]%.
Variable fields	$1: Name of the storage medium, for example, flash. $2: Usage of the storage medium. $3: Usage threshold of the storage medium.
Severity level	4
Example	DIAG/4/DIAG_STORAGE_BELOW_THRESHOLD: The usage of flash (90%) has dropped below the threshold of 95%.
Explanation	The usage of the storage medium was below or equal to the threshold.
Recommended action	No action is required.

DIAG_STORAGE_EXCEED_THRESHOLD

Message text	The usage of [STRING] ([UINT32]%) exceeded the threshold of [UINT32]%.
Variable fields	$1: Name of the storage medium, for example, flash. $2: Usage of the storage medium. $3: Usage threshold of the storage medium.
Severity level	4
Example	DIAG/4/DIAG_STORAGE_EXCEED_THRESHOLD: The usage of flash (96%) exceeded the threshold of 95%.
Explanation	The usage of the storage medium exceeded the threshold.
Recommended action	For files not in use, for example, log files and history software packages, execute the **`delete /unreserved`** command to delete the files or back up the files and then execute the **`delete /unreserved`** command to delete the files.

MEM_ALERT

Message text	system memory info: total used free shared buffers cached Mem: [ULONG] [ULONG] [ULONG] [ULONG] [ULONG] [ULONG] -/+ buffers/cache: [ULONG] [ULONG] Swap: [ULONG] [ULONG] [ULONG] Lowmem: [ULONG] [ULONG] [ULONG]

Variable fields	• **Mem**—Memory information of the whole system:
	  ○ $1: Total size of allocatable physical memory. The system physical memory contains allocatable physical memory and unallocatable physical memory. Unallocatable physical memory is mainly used for kernel code storage, kernel management, and running of basic functions. Allocatable physical memory is used for such tasks as running service modules and storing files. The size of unallocatable physical memory is automatically calculated based on the system operation requirements. The size of allocatable physical memory is the total physical memory size minus the unallocatable physical memory size.
	  ○ $2: Size of the physical memory used by the system.
	  ○ $3: Size of free physical memory of the system.
	  ○ $4: Total size of physical memory shared by processes.
	  ○ $5: Size of physical memory used for buffers.
	  ○ $6: Size of physical memory used for caches.
	• **-/+ buffers/cache**—Memory usage information of applications:
	  ○ $7: -/+ Buffers/Cache:used = Mem:Used – Mem:Buffers – Mem:Cached, which indicates the size of physical memory used by applications.
	  ○ $8: -/+ Buffers/Cache:free = Mem:Free + Mem:Buffers + Mem:Cached, which indicates the size of physical memory available for applications.
	• **Swap**—Swap memory usage information:
	  ○ $9: Total size of swap memory.
	  ○ $10: Size of used swap memory.
	  ○ $11: Size of free swap memory.
	• **Lowmem**—Low memory usage information:
	  ○ $12: Total size of low memory.
	  ○ $13: Size of used low memory.
	  ○ $14: Size of free low memory.

Severity level	4
Example	DIAG/4/MEM_ALERT: system memory info: total used free shared buffers cached Mem: 1784424 920896 863528 0 0 35400 -/+ buffers/cache: 885496 898928 Swap: 0 0 0 Lowmem: 735848 637896 97952
Explanation	A memory alarm was generated, displaying memory usage information. The system generates this message when the used memory is greater than or equal to the minor, severe, or critical threshold of memory usage.
Recommended action	You can perform the following tasks to help remove the alarm:

	• Verify that appropriate alarm thresholds are set. To view the alarm thresholds, use the **display memory-threshold** command. Then you can use the **memory-threshold** command to modify the alarm thresholds if required. • Verify that the device is not under attack by checking the ARP table and routing table. • Examine and optimize the network, for example, reduce the number of routes, or replace the device with a higher-performance device.

MEM_BELOW_THRESHOLD

Message text	Memory usage has dropped below [STRING] threshold.
Variable fields	$1: Memory usage threshold name: minor, severe, or critical.
Severity level	1
Example	DIAG/1/MEM_BELOW_THRESHOLD: Memory usage has dropped below critical threshold.
Explanation	A memory alarm was removed. The message is sent when the system free memory is greater than a memory alarm recovery threshold.
Recommended action	No action is required.

MEM_EXCEED_THRESHOLD

Message text	Memory [STRING] threshold has been exceeded.
Variable fields	$1: Memory usage threshold name: minor, severe, or critical.
Severity level	1
Example	DIAG/1/MEM_EXCEED_THRESHOLD: Memory minor threshold has been exceeded.
Explanation	A memory alarm was notified. When the used memory size is greater than or equal to the minor, severe, or critical threshold of memory usage, the system generates this message and notifies services modules to perform auto repair, such as releasing memory and stopping requesting memory.
Recommended action	You can perform the following tasks to help remove the alarm: • Verify that appropriate alarm thresholds are set. To view the alarm thresholds, use the **display memory-threshold** command. Then you can use the **memory-threshold** command to modify the alarm thresholds if required. • Verify that the device is not under attack by checking the ARP table and routing table. • Examine and optimize the network, for example, reduce the number of routes or replace the device with a higher-performance device.

MEM_USAGE_EXCEED_THRESHOLD

Message text	Memory usage threshold has been exceeded.
Variable fields	N/A
Severity level	1
Example	DIAG/1/MEM_USAGE_EXCEED_THRESHOLD: Memory usage threshold has been exceeded.
Explanation	A memory usage alarm occurred. The message is sent when the memory usage exceeds the memory usage alarm threshold.
Recommended action	**93.** Verify that an appropriate memory alarm threshold is set. To view the memory alarm threshold, use the **display memory-threshold** command. To change the memory alarm threshold, use the **memory-threshold usage** command. **94.** Verify that the device is not under attack by checking the ARP table and routing table. **95.** Examine and optimize the network, for example, reduce the number of routes or replace the device with a higher-performance device.

MEM_USAGE_RECOVER_THRESHOLD

Message text	Memory usage has dropped down to normal levels.
Variable fields	N/A
Severity level	1
Example	DIAG/1/MEM_USAGE_RECOVER_THRESHOLD: Memory usage has dropped down to normal levels.
Explanation	A memory usage alarm was removed. This message is sent when the memory usage drops to or below the memory usage alarm threshold.
Recommended action	No action is required.

MEM_USAGE

Message text	Current memory usage is [STRING].
Variable fields	$1: Memory usage in percentage.
Severity level	5
Example	DIAG/5/MEM_USAGE: Current memory usage is 10%.
Explanation	Current memory usage of the device.
Recommended action	No action is required.

DIM engine messages

This section contains DPI engine messages.

DIM_SIGNATURE_WARNING

Message text	DIM/4/DIM_SIGNATURE_WARNING: Failed to write a signature file to the flash memory due to insufficient storage space.
Severity level	4
Example	DPI/4/DIM_SIGNATURE_WARNING: Failed to write a signature file to the flash memory due to insufficient storage space.
Explanation	This message is generated when a signature library fails to be updated or rolled back due to insufficient storage space in the flash memory.
Recommended action	Release some storage space in the flash memory before updating or rolling back a signature library.

DIM_ACTIVE_WARNING

Message text	DIM/4/DIM_ACTIVE_WARNING: The device fails to activate the DPI engine due to insufficient memory space after the free-memory normal state threshold is reached. DPI services were no longer in effect.
Severity level	4
Example	DPI/4/DIM_ACTIVE_WARNING: The device fails to activate the DPI engine due to insufficient memory space after the free-memory normal state threshold is reached. DPI services were no longer in effect.
Explanation	This message is generated when the device fails to activate the DPI engine due to insufficient memory space.
Recommended action	Release some storage space and then execute the **inspect activate** command.

DLDP messages

This section contains DLDP messages.

DLDP_AUTHENTICATION_FAILED

Message text	The DLDP packet failed the authentication because of unmatched [STRING] field.
Variable fields	$1: Authentication field. • **AUTHENTICATION PASSWORD**—Authentication password mismatch. • **AUTHENTICATION TYPE**—Authentication type mismatch. • **INTERVAL**—Advertisement interval mismatch.
Severity level	5
Example	DLDP/5/DLDP_AUTHENTICATION_FAILED: The DLDP packet failed the authentication because of unmatched INTERVAL field.
Explanation	The packet authentication failed. Possible reasons include unmatched authentication type, unmatched authentication password, and unmatched advertisement interval.
Recommended action	Check the DLDP authentication type, authentication password, and advertisement interval are consistent with peer end.

DLDP_LINK_BIDIRECTIONAL

Message text	DLDP detected a bidirectional link on interface [STRING].
Variable fields	$1: Interface name.
Severity level	6
Example	DLDP/6/DLDP_LINK_BIDIRECTIONAL: DLDP detected a bidirectional link on interface Ethernet1/1.
Explanation	DLDP detected a bidirectional link on an interface.
Recommended action	No action is required.

DLDP_LINK_UNIDIRECTIONAL

Message text	DLDP detected a unidirectional link on interface [STRING]. [STRING].
Variable fields	$1: Interface name. $2: Action according to the port shutdown mode: • DLDP automatically blocked the interface. • Please manually shut down the interface.
Severity level	3
Example	DLDP/3/DLDP_LINK_UNIDIRECTIONAL: DLDP detected a unidirectional link on interface Ethernet1/1. DLDP automatically blocked the interface.
Explanation	DLDP detected a unidirectional link on an interface.
Recommended action	Check for incorrect cable connection, cable falloff, or other problems.

DLDP_NEIGHBOR_AGED

Message text	A neighbor on interface [STRING] was deleted because the neighbor was aged. The neighbor's system MAC is [MAC], and the port index is [UINT16].
Variable fields	$1: Interface name. $2: MAC address. $3: Port index.
Severity level	5
Example	DLDP/5/DLDP_NEIGHBOR_AGED: A neighbor on interface Ethernet1/1 was deleted because the neighbor was aged. The neighbor's system MAC is 000f-e269-5f21, and the port index is 1.
Explanation	The interface deleted an aged neighbor.
Recommended action	No action is required.

DLDP_NEIGHBOR_CONFIRMED

Message text	A neighbor was confirmed on interface [STRING]. The neighbor's system MAC is [MAC], and the port index is [UINT16].
Variable fields	$1: Interface name. $2: MAC address. $3: Port index.
Severity level	6
Example	DLDP/6/DLDP_NEIGHBOR_CONFIRMED: A neighbor was confirmed on interface Ethernet1/1. The neighbor's system MAC is 000f-e269-5f21, and the port index is 1.
Explanation	The interface detected a confirmed neighbor.
Recommended action	No action is required.

DLDP_NEIGHBOR_DELETED

Message text	A neighbor on interface [STRING] was deleted because a [STRING] packet arrived. The neighbor's system MAC is [MAC], and the port index is [UINT16].
Variable fields	$1: Interface name. $2: Packet type, DISABLE or LINKDOWN. $3: MAC address. $4: Port index.
Severity level	5
Example	DLDP/5/DLDP_NEIGHBOR_DELETED: A neighbor on interface Ethernet1/1 was deleted because a DISABLE packet arrived. The neighbor's system MAC is 000f-e269-5f21, and the port index is 1.
Explanation	The interface deleted a confirmed neighbor because it received a DISABLE or LINKDOWN packet.
Recommended action	No action is required.

DNS

This section contains DNS messages.

DNS_SNOOPING_LOG

Message text	UserName=[STRING], UserGroup=[STRING], SrcDeviceType=[STRING], SrcOs=[STRING], SrcMAC=[UINT64], SrcIPAddr=[UINT32], SrcPort=[UINT16], DstIPAddr=[UINT32], DstPort=[UINT16], Domain=[STRING], ResponseContent=[UINT32], Protocol=[UINT16], ReqByteCount=[UINT64], ResByteCount=[UINT64], ReqPktCount=[UINT64], ResPktCount=[UINT64], ResponseCode=[UINT4], ResquestID=[UINT16], ResponseID=[UINT16], ReqType=[UINT16], Direction=[UINT16], ResFirstAnswerTTL=[UINT32].
Variable fields	$1: Username. $2: User group name. $3: Device type. $4: Device operating system. $5: Source MAC address. $6: Source IP address. $7: Source port number. $8: Destination IP address. $9: Destination port number. $10: Domain name to translate. $11: Returned content. $12: Protocol. $13: Request bytes. $14: Response bytes. $15: Request packets. $16: Response packets. $17: Response code. Options include: • **0**—Success. • **1**—Invalid format. • **2**—Invalid server. • **3**—Invalid name. • **4**—Type not supported by the domain name server. • **5**—Request rejected by the domain name server because of policy configurations. For example, the domain name server does not respond to specific requesters. $18: Request ID. $19: Response ID. $20: Request type. $21: Packet direction. Options include: • **0**—Request. • **1**—Response. • **2**—Bidirectional. $22: First TTL in the Answer field of the response.
Severity level	6
Example	DNS/6/DNS_SNOOPING_LOG: UserName=, UserGroup=, SrcDeviceType=, SrcOs=, SrcMAC=0000-0000-0000, SrcIPAddr=3.3.3.1, SrcPort=9931, DstIPAddr=3.3.3.2, DstPort=53, Domain=tt, ResponseContent=1.1.1.1, Protocol=17, ReqByteCount=20, ResByteCount=36, ReqPktCount=1, ResPktCount=1, ResponseCode=0, ResquestID=44569, ResponseID=44569, ReqType=1, Direction=2, ResFirstAnswerTTL=3600.

Message text	UserName=[STRING], UserGroup=[STRING], SrcDeviceType=[STRING], SrcOs=[STRING], SrcMAC=[UINT64], SrcIPAddr=[UINT32], SrcPort=[UINT16], DstIPAddr=[UINT32], DstPort=[UINT16], Domain=[STRING], ResponseContent=[UINT32], Protocol=[UINT16], ReqByteCount=[UINT64], ResByteCount=[UINT64], ReqPktCount=[UINT64], ResPktCount=[UINT64], ResponseCode=[UINT4], ResquestID=[UINT16], ResponseID=[UINT16], ReqType=[UINT16], Direction=[UINT16], ResFirstAnswerTTL=[UINT32].
Explanation	The device outputs the log message to the fast log output module every 5 seconds or after a DNS session finishes (both request and response are received). Then, the fast log output module reports the message to the log host for other modules to analyze DNS traffic. For the system to output the log message, you must use the **dns snooping log enable** command to enable DNS snooping logging. For the log message to be sent to the log host successfully, you must use the **customlog host** command to configure fast log output parameters, and use the **customlog format dns** command to enable fast log output for DNS.
Recommended action	No action is required.

DOT1X messages

This section contains 802.1X messages.

DOT1X_LOGIN_FAILURE

Message text	-IfName=[STRING]-MACAddr=[STRING]-VLANId=[STRING]-UserName=[STRING] -ErrCode=[STRING]; The user failed the 802.1X authentication. Reason: [STRING].
Variable fields	$1: Interface type and number. $2: MAC address. $3: VLAN ID. $4: Username. $5: Error code: ○ **1**—The user went offline. ○ **2**—Port status error. ○ **3**—Client reboot. This code is reserved for future use. ○ **4**—Reauthentication failure. ○ **5**—Deauthorization by the device. ○ **6**—Port went down and then came up again. ○ **7**—The user was logged off because the device and the server were inconsistent in authorization data. ○ **8**—Username or password error or lack of device information on the server. ○ **9**—Online handshake failure (the device has not received any handshake packets from the user). ○ **10**—The user was logged off by the idle cut feature. ○ **11**—The session timeout timer assigned by the server expired. ○ **12**—The server forcibly logged the user off. ○ **13**—Real-time accounting failure. ○ **14**—Other errors. ○ **15**—Offline caused by an interface event. $6: Failure cause: ○ Authorization Mac-Address process failed. ○ Authorization VLAN process failed. ○ Authorization ACL process failed. ○ Authorization UserProfile process failed.
Severity level	6
Example	DOT1X/6/DOT1X_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/1-MACAddr=0000-0001-0020-VLANId=2-Username=aaa-ErrCode=5; The user failed the 802.1X authentication. Reason: Authorization ACL process failed.
Explanation	The user failed 802.1X authentication.
Recommended action	Resolve the issue depending on the failure cause.

DOT1X_LOGIN_SUCC

Message text	-IfName=[STRING]-MACAddr=[STRING]-AccessVLANId=[STRING]-AuthorizationVLANId=[STRING]-Username=[STRING]; The user passed 802.1X authentication and got online successfully.
Variable fields	$1: Interface type and number. $2: MAC address. $3: ID of the VLAN through which the user accesses the device. $4: Authorization VLAN ID. $5: Username.
Severity level	6
Example	DOT1X/6/DOT1X_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-AccessVLANId=444-AuthorizationVLANId=444-Username=aaa; The user passed 802.1X authentication and got online successfully.
Explanation	The user passed 802.1X authentication.
Recommended action	No action is required.

DOT1X_LOGOFF

Message text	-IfName=[STRING]-MACAddr=[STRING]-VLANId=[STRING]-Username=[STRING]-ErrCode=[STRING]; Session of the 802.1X user was terminated.
Variable fields	$1: Interface type and number. $2: MAC address. $3: VLAN ID. $4: Username. $5: Error code: ○ **1**—The user went offline. ○ **2**—Port status error. ○ **3**—Client reboot. This code is reserved for future use. ○ **4**—Reauthentication failure. ○ **5**—Deauthorization by the device. ○ **6**—Port went down and then came up again. ○ **7**—The user was logged off because the device and the server were inconsistent in authorization data. ○ **8**—Username or password error or lack of device information on the server. ○ **9**—Online handshake failure (the device has not received any handshake packets from the user). ○ **10**—The user was logged off by the idle cut feature. ○ **11**—The session timeout timer assigned by the server expired. ○ **12**—The server forcibly logged the user off. ○ **13**—Real-time accounting failure. ○ **14**—Other errors. ○ **15**—Offline caused by an interface event.
Severity level	6
Example	DOT1X/6/DOT1X_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANId=444-Username=aaa-ErrCode=11; Session of the 802.1X user was terminated.
Explanation	The 802.1X user was logged off.
Recommended action	Resolve the issue depending on the logoff cause. If the logoff was requested by the user, no action is required.

DOT1X_NOTENOUGH_EADFREEIP_RES

Message text	Failed to assign a rule for Free IP [IPADDR] on interface [STRING] due to lack of ACL resources.
Variable fields	$1: Free IP. $2: Interface type and number.
Severity level	3
Example	DOT1X/3/DOT1X_NOTENOUGH_EADFREEIP_RES: Failed to assign a rule for Free IP 1.1.1.0 on interface Ethernet3/1/2 due to lack of ACL resources.
Explanation	The device failed to assign an ACL rule to permit a free IP on an interface because of ACL resource shortage.
Recommended action	No action is required.

DOT1X_NOTENOUGH_EADFREERULE_RES

Message text	Failed to assign a rule for permitting DHCP and DNS packets on interface [STRING] due to lack of ACL resources.
Variable fields	$1: Interface type and number.
Severity level	3
Example	DOT1X/3/DOT1X_NOTENOUGH_EADFREERULE_RES: Failed to assign a rule for permitting DHCP and DNS packets on interface Ethernet3/1/2 due to lack of ACL resources.
Explanation	The device failed to assign an ACL rule to permit DHCP and DNS packets on an interface because of ACL resource shortage.
Recommended action	No action is required.

DOT1X_NOTENOUGH_EADPORTREDIR_RES

Message text	Failed to assign a rule for redirecting HTTP packets on interface [STRING] due to lack of ACL resources.
Variable fields	$1: Interface type and number.
Severity level	3
Example	DOT1X/3/DOT1X_NOTENOUGH_EADPORTREDIR_RES: Failed to assign a rule for redirecting HTTP packets on interface Ethernet3/1/2 due to lack of ACL resources.
Explanation	The device failed to assign an ACL rule to redirect HTTP packets on an interface because of ACL resource shortage.
Recommended action	No action is required.

DOT1X_NOTENOUGH_EADMACREDIR_RES

Message text	Failed to issue a rule for redirecting HTTP packets with source MAC address [MAC] on interface [STRING].
Variable fields	$1: Source MAC address of HTTP packets. $2: Interface type and number.
Severity level	3
Example	DOT1X/3/DOT1X_NOTENOUGH_EADMACREDIR_RES: Failed to issue a rule for redirecting HTTP packets with source MAC address 00e0-fc00-5915 on interface Ethernet3/1/2.
Explanation	The device failed to redirect HTTP packet with the designated source MAC on an interface because of ACL resource shortage.
Recommended action	No action is required.

DOT1X_NOTENOUGH_ENABLEDOT1X_RES

Message text	Failed to enable 802.1X feature on interface [STRING] due to lack of ACL resources.
Variable fields	$1: Interface type and number.
Severity level	3
Example	DOT1X/3/DOT1X_NOTENOUGH_ENABLEDOT1X_RES: Failed to enable 802.1X feature on interface Ethernet3/1/2 due to lack of ACL resources.
Explanation	Failed to enable 802.1X on an interface because of ACL resource shortage.
Recommended action	Disable 802.1X on the interface, and then re-enable 802.1X.

DOT1X_NOTSUPPORT_EADFREEIP_RES

Message text	Failed to assign a rule for free IP [IPADDR] on interface [STRING]: EAD assistant was not supported.
Variable fields	$1: IP address. $2: Interface type and number.
Severity level	3
Example	DOT1X/3/DOT1X_NOTSUPPORT_EADFREEIP_RES: Failed to assign a rule for free IP 1.1.1.0 on interface Ethernet3/1/2: EAD assistant was not supported.
Explanation	The device failed to assign an ACL rule to permit a free IP on an 802.1X-enabled interface because EAD assistant was not supported.
Recommended action	No action is required.

DOT1X_NOTSUPPORT_EADFREERULE_RES

Message text	Failed to assign a rule for permitting DHCP and DNS packets on interface [STRING]: EAD assistant was not supported.
Variable fields	$1: Interface type and number.
Severity level	3
Example	DOT1X/3/DOT1X_NOTSUPPORT_EADFREERULE_RES: Failed to assign a rule for permitting DHCP and DNS packets on interface Ethernet3/1/2: EAD assistant was not supported.
Explanation	The device failed to assign an ACL rule to permit DHCP and DNS packets on an 802.1X-enabled interface because EAD assistant was not supported.
Recommended action	No action is required.

DOT1X_NOTSUPPORT_EADMACREDIR_RES

Message text	Failed to assign a rule for redirecting HTTP packets with source MAC address [MAC] on interface [STRING]: EAD assistant was not supported.
Variable fields	$1: Source MAC address of HTTP packets. $2: Interface type and number.
Severity level	3
Example	DOT1X/3/DOT1X_NOTSUPPORT_EADMACREDIR_RES: Failed to assign a rule for redirecting HTTP packets with source MAC address 00e0-fc00-5915 on interface Ethernet3/1/2: EAD assistant was not supported.
Explanation	The device failed to assign an ACL rule to redirect HTTP packets with a specific source MAC address on an 802.1X-enabled interface because EAD assistant was not supported.
Recommended action	No action is required.

DOT1X_NOTSUPPORT_EADPORTREDIR_RES

Message text	Failed to assign a rule for redirecting HTTP packets on interface [STRING]: EAD assistant was not supported.
Variable fields	$1: Interface type and number.
Severity level	3
Example	DOT1X/3/DOT1X_NOTSUPPORT_EADPORTREDIR_RES: Failed to assign a rule for redirecting HTTP packets on interface Ethernet3/1/2: EAD assistant was not supported.
Explanation	The device failed to assign an ACL rule to redirect HTTP packets on an 802.1X-enabled interface because EAD assistant was not supported.
Recommended action	No action is required.

DOT1X_UNICAST_NOT_EFFECTIVE

Message text	The unicast trigger feature is enabled but is not effective on interface [STRING].
Variable fields	$1: Interface type and number.
Severity level	3
Example	DOT1X/3/DOT1X_UNICAST_NOT_EFFECTIVE: The unicast trigger feature is enabled but is not effective on interface Ethernet3/1/2.
Explanation	The unicast trigger setting does not take effect on an interface, because the interface does not support unicast trigger.
Recommended action	**96.** Reconnect the 802.1X clients to another interface that supports the unicast trigger feature. **97.** Enable the unicast trigger feature on the new interface.

DOT1X_WLAN_LOGIN_FAILURE

Message text	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[STRING]-VLANID=[STRING]; A user failed 802.1X authentication. Reason: [STRING].
Variable fields	$1: Username. $2: MAC address of the client. $3: SSID. $4: Name of the AP with which the client is associated. $5: ID of the radio with which the client is associated. $6: VLAN ID. $7: Reason that causes the authentication failure: • AAA processed authentication request and returned error code *code*. The values for *code* include: ○ **4**—Represents the error of nonexistent authentication domain. ○ **8**—Represents one of the following errors: Configuration error exists in the authentication domain, the preshared key configured on the authentication server is different from the preshared key configured on the device, authentication port 1812 is unavailable, or the authentication server and the device cannot reach each other. ○ **26**—Represents one of the following errors: The username or password is incorrect, the authentication type is incorrect, the device IP address is not added to the authentication server, or the authentication domain is not correctly configured on the service template. • AAA processed authorization request and returned error code *code*. The value for *code* is 8, which indicates that the server and the device cannot reach each other. • Received logoff request from the client. • Client timeout timer expired. • Server timeout timer expired. • Received logoff request while authenticating the client. • Received user security information and kicked off the client. • Accounting-update timer expired, and no responses were received from the server. • Kicked off the client when the idle timeout timer expired. • Authentication method error. • Kicked off the client because the server-assigned session timeout timer is 0. • Received session disconnection event. • Received nonexistent authorization VLAN group. • Client kicked out on expiration of the idle-cut timer because its total traffic had not reached the required minimum amount of traffic. • Had failed to obtain the client IP address before the accounting delay timer expired. • Unknown reason.
Severity level	5
Example	DOT1X/5/DOT1X_WLAN_LOGIN_FAILURE:-Username=Dot1X-UserMAC=3ce5-a616-28cd-SSID=text-wifi-APName=ap1-RadioID=2-VLANID=11; A user failed 802.1X authentication. Reason: AAA processed authentication request and returned error code 26.
Explanation	The client failed to pass 802.1X authentication for a specific reason.
Recommended action	To resolve the issue: **98.** Troubleshoot errors according to the returned failure reason. **99.** If the issue persists, contact NSFOCUS Support.

DOT1X_WLAN_LOGIN_SUCC

Message text	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[STRING]-VLANID=[STRING]; A user passed 802.1X authentication and came online.
Variable fields	$1: Username. $2: MAC address of the client. $3: SSID. $4: Name of the AP with which the client is associated. $5: ID of the radio with which the client is associated. $6: VLAN ID.
Severity level	6
Example	DOT1X/6/DOT1X_WLAN_LOGIN_SUCC:-Username=Dot1X-UserMAC=3ce5-a616-28cd-SSID=text-wifi-APName=ap1-RadioID=2-VLANID=11; A user passed 802.1X authentication and came online.
Explanation	The client came online after passing 802.1X authentication.
Recommended action	No action is required.

DOT1X_WLAN_LOGOFF

Message text	Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[STRING]-VLANID=[STRING]; Session for an 802.1X user was terminated. Reason: [STRING].
Variable fields	$1: Username. $2: MAC address of the client. $3: SSID. $4: Name of the AP with which the client is associated. $5: ID of the radio with which the client is associated. $6: VLAN ID. $7: Reason that causes the client logoff. • AAA processed authentication request and returned error code *code*. *Server reason: reason*. If the server does not return the failure cause, the *Server reason* variable is not available. The values for *code* include: ○ **4**—Represents the error of nonexistent authentication domain. ○ **8**—Represents one of the following errors: Configuration error exists in the authentication domain, the preshared key configured on the authentication server is different from the preshared key configured on the device, authentication port 1812 is unavailable, or the authentication server and the device cannot reach each other. ○ **26**—Represents one of the following errors: The username or password is incorrect, the authentication type is incorrect, the device IP address is not added to the authentication server, or the authentication domain is not correctly configured on the service template. • AAA processed authorization request and returned error code *code*. *Server reason: reason*. If the server does not return the failure cause, the *Server reason* variable is not available. The value for *code* is 8, which indicates that the server and the device cannot reach each other. • AAA processed accounting-start request and returned error code *code*. *Server reason: reason*. If the server does not return the failure cause, the *Server reason* variable is not available. The value for *code* is 8, which indicates that the server and the device cannot reach each other. • AAA processed accounting-update request and returned error code *code*. *Server reason: reason*. If the server does not return the failure cause, the *Server reason* variable is not available. The value for *code* is 8, which indicates that the server and the device cannot reach each other. • Received logoff request from the client. • User timer expired. • Server timer expired. • Received logoff request while authenticating the client. • Received user security information and kicked off the client. • Lost in shaking hands. • Accounting-update timer expired, and no responses were received from the server. • Kicked off the client when the idle timeout timer expired. • Authentication method error. • Kicked off the client because the server-assigned session timeout timer is 0. • Received session disconnection event. • Received disassociation frame in Run state: reason code=*code*. • Received deauthentication frame in Run state: reason

	code=*code*. • Received disassociation packet in Userauth state. • Received deauthentication packet in Userauth state. • Received client failure message with reason code=*code*. • Received client offline message with reason code=*code*. • Unknown reason.
Severity level	6
Example	DOT1X/6/DOT1X_WLAN_LOGOFF:-Username=Dot1X-UserMAC=3ce5-a616-28cd-SSID=text-wifi-APName=ap1-RadioID=2-VLANID=11; Session for an 802.1X user was terminated. Reason: Received logoff request from the client.
Explanation	The 802.1X authenticated client was logged off for a specific reason.
Recommended action	To resolve the issue: **100.** Check the debugging information to locate the logoff cause and remove the issue. If the logoff was requested by the client, no action is required. **101.** If the issue persists, contact NSFOCUS Support.

EDEV messages

This section contains messages for extended-device management.

EDEV_FAILOVER_GROUP_STATE_CHANGE

Message text	Status of stateful failover group [STRING] with ID [UINT32] changed to [STRING].
Variable fields	$1: Failover group name. $2: Failover group ID. $3: Failover group state.
Severity level	5
Example	EDEV/5/EDEV_FAILOVER_GROUP_STATE_CHANGE: Status of stateful failover group 123 with ID 0 changed to primary.
Explanation	The status of a failover group changed.
Recommended action	No action is required.

EIGRP messages

This section contains EIGRP messages.

RID_CHANGE

Message text	EIGRP [UINT32]: New elected router ID will take effect after EIGRP address family is reset.
Variable fields	$1: EIGRP process ID.
Severity level	5
Example	EIGRP/5/RID_CHANGE: EIGRP 1: New elected router ID will take effect after EIGRP address family is reset.
Explanation	A change of interface IP address causes the change of router ID for the EIGRP router. You must restart the EIGRP IPv4 address family to make the new router ID take effect.
Recommended action	Execute the **reset eigrp process** command to make the new router ID take effect.

PEER_CHANGE

Message text	EIGRP [UINT32]: Neighbor [STRING] ([STRING]) is [STRING]: [STRING].
Variable fields	$1: EIGRP process ID. $2: IP address of the neighbor router. $3: Interface that is connected to the neighbor router. $4: Neighbor state, **Up** or **Down**. $5: Reason for the EIGRP neighbor state change. For information about the neighbor state change reasons, see Table 1.
Severity level	5
Example	EIGRP/5/PEER_CHANGE: EIGRP 2: Neighbor 100.100.10.2 (GigabitEthernet1/0/1) is Up: New neighbor.
Explanation	The EIGRP neighbor state changed for a specific reason.
Recommended action	Take an action according to the neighbor state change reason. For more information, see Table 1.

Table 1 Neighbor state change reasons and recommended actions

Reason	Remarks	Recommended action
New neighbor	N/A	No action is required.
Interface down	N/A	Check the network connectivity.
Reset operation	The **reset eigrp process** or **reset eigrp peer** command was executed.	No action is required.
Delete operation	The process or address family was deleted.	No action is required.
Hold timer expired	N/A	Check the network status or check whether the hold timer is appropriate.
Maximum retransmission times reached	N/A	Check the network status.

Reason	Remarks	Recommended action
Inconsistent K values	N/A	Check whether the K values are consistent on both ends.
Neighbor restart	N/A	Check the network status and check whether an operation that affects neighbor relationship has been performed on the neighbor router.
Stuck in active	N/A	Check the network status and CPU usage on the neighbor router.
Peer termination	The neighbor actively terminated the neighbor relationship.	Check whether an operation that affects neighbor relationship has been performed on the neighbor router.
Configuration changed	N/A	Check whether the configuration is correct.
Process switchover	EIGRP process switchover occurred.	No action is required.
Insufficient memory	The memory threshold was reached.	Check system memory and release available memory by adjusting the modules that occupy too much memory.

ERPS messages

This section contains ERPS messages.

ERPS_STATE_CHANGED

Message text	Ethernet ring [UINT16] instance [UINT16] changed state to [STRING]
Variable fields	$1: ERPS ring ID. $2: ERPS instance ID. $3: ERPS instance status.
Severity level	6
Example	ERPS/4/ERPS_STATE_CHANGED: Ethernet ring 1 instance 1 changed state to Idle.
Explanation	The status of the ERPS instance changed.
Recommended action	No action is required.

ETHOAM messages

This section contains Ethernet OAM messages.

ETHOAM_CONNECTION_FAIL_DOWN

Message text	The link is down on interface [string] because a remote failure occurred on peer interface.
Variable fields	$1: Interface name.
Severity level	5
Example	ETHOAM/5/ETHOAM_CONNECTION_FAIL_DOWN: The link is down on interface Ethernet1/0/1 because a remote failure occurred on peer interface.
Explanation	The link goes down because a remote failure occurred on the peer interface.
Recommended action	Check the link status or the OAM status on the peer.

ETHOAM_CONNECTION_FAIL_TIMEOUT

Message text	Interface [string] removed the OAM connection because it received no Information OAMPDU before the timer times out.
Variable fields	$1: Interface name.
Severity level	5
Example	ETHOAM/5/ETHOAM_CONNECTION_FAIL_TIMEOUT: Interface Ethernet1/0/1 removed the OAM connection because it received no Information OAMPDU before the timer times out.
Explanation	The interface removed the OAM connection because it had not received Information OAMPDUs before the timer timed out.
Recommended action	Check the link status or the OAM status on the peer.

ETHOAM_CONNECTION_FAIL_UNSATISF

Message text	Interface [string] failed to establish an OAM connection because the peer doesn't match the capacity of the local interface.
Variable fields	$1: Interface name.
Severity level	3
Example	ETHOAM/3/ETHOAM_CONNECTION_FAIL_UNSATISF: Interface Ethernet1/0/1 failed to establish an OAM connection because the peer doesn't match the capacity of the local interface.
Explanation	Failed to establish an OAM connection because the peer does not match the OAM protocol state of the local interface.
Recommended action	Check the **State** field of the OAMPDUs sent from both ends.

ETHOAM_CONNECTION_SUCCEED

Message text	An OAM connection is established on interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_CONNECTION_SUCCEED: An OAM connection is established on interface Ethernet1/0/1.
Explanation	An OAM connection is established.
Recommended action	No action is required.

ETHOAM_DISABLE

Message text	Ethernet OAM is now disabled on interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_DISABLE: Ethernet OAM is now disabled on interface Ethernet1/0/1.
Explanation	Ethernet OAM is disabled.
Recommended action	No action is required.

ETHOAM_DISCOVERY_EXIT

Message text	OAM interface [string] quit the OAM connection.
Variable fields	$1: Interface name.
Severity level	5
Example	ETHOAM/5/ETHOAM_DISCOVERY_EXIT: OAM interface Ethernet1/0/1 quit the OAM connection.
Explanation	The local interface ended the OAM connection.
Recommended action	No action is required.

ETHOAM_ENABLE

Message text	Ethernet OAM is now enabled on interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_ENABLE: Ethernet OAM is now enabled on interface Ethernet1/0/1.
Explanation	Ethernet OAM is enabled.
Recommended action	No action is required.

ETHOAM_ENTER_LOOPBACK_CTRLLED

Message text	The local OAM entity enters remote loopback as controlled DTE on OAM interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_ENTER_LOOPBACK_CTRLLED: The local OAM entity enters remote loopback as controlled DTE on OAM interface Ethernet1/0/1.
Explanation	The local OAM entity enters remote loopback as controlled DTE after you enable OAM loopback on the peer end.
Recommended action	No action is required.

ETHOAM_ENTER_LOOPBACK_CTRLLING

Message text	The local OAM entity enters remote loopback as controlling DTE on OAM interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_ENTER_LOOPBACK_CTRLLING: The local OAM entity enters remote loopback as controlling DTE on OAM interface Ethernet1/0/1.
Explanation	The local OAM entity enters remote loopback as controlling DTE after you enable OAM loopback on the interface.
Recommended action	No action is required.

ETHOAM_LOCAL_DYING_GASP

Message text	A local Dying Gasp event has occurred on [string].
Variable fields	$1: Interface name.
Severity level	4
Example	ETHOAM/4/ETHOAM_LOCAL_DYING_GASP: A local Dying Gasp event occurred on interface Ethernet1/0/1.
Explanation	A local Dying Gasp event occurs when you reboot the local device or shut down the interface.
Recommended action	Do not use the link until it recovers.

ETHOAM_LOCAL_ERROR_FRAME

Message text	An errored frame event occurred on local interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME: An errored frame event occurred on local interface Ethernet1/0/1.
Explanation	An errored frame event occurred on the local interface.
Recommended action	Check the link between the local and peer ends.

ETHOAM_LOCAL_ERROR_FRAME_PERIOD

Message text	An errored frame period event occurred on local interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME_PERIOD: An errored frame period event occurred on local interface Ethernet1/0/1.
Explanation	An errored frame period event occurred on the local interface.
Recommended action	Check the link between the local and peer ends.

ETHOAM_LOCAL_ERROR_FRAME_SECOND

Message text	An errored frame seconds event occurred on local interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_LOCAL_ERROR_FRAME_SECOND: An errored frame seconds event occurred on local interface Ethernet1/0/1.
Explanation	An errored frame seconds event occurred on the local interface.
Recommended action	Check the link between the local and peer ends.

ETHOAM_LOCAL_LINK_FAULT

Message text	A local Link Fault event occurred on interface [string].
Variable fields	$1: Interface name.
Severity level	4
Example	ETHOAM/4/ETHOAM_LOCAL_LINK_FAULT: A local Link Fault event occurred on interface Ethernet1/0/1.
Explanation	A local Link Fault event occurred when the local link goes down.
Recommended action	Re-connect the Rx end of the fiber on the local interface.

ETHOAM_LOOPBACK_EXIT

Message text	OAM interface [string] quit remote loopback.
Variable fields	$1: Interface name.
Severity level	4
Example	ETHOAM/4/ETHOAM_LOOPBACK_EXIT: OAM interface Ethernet1/0/1 quit remote loopback.
Explanation	The OAM interface ended remote loopback after one of the following events occurred: • Remote loopback was disabled on the interface before the OAM connection was established. • The established OAM connection was torn down.
Recommended action	No action is required.

ETHOAM_LOOPBACK_EXIT_ERROR_STATU

Message text	OAM interface [string] quit remote loopback due to incorrect multiplexer or parser status.
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_LOOPBACK_EXIT_ERROR_STATU: OAM interface Ethernet1/0/1 quit remote loopback due to incorrect multiplexer or parser status.
Explanation	OAM interface Ethernet1/0/1 ended remote loopback due to incorrect multiplexer or parser status.
Recommended action	Disable and then re-enable Ethernet OAM on the OAM entity.

ETHOAM_LOOPBACK_NO_RESOURCE

Message text	OAM interface [string] can’t enter remote loopback due to insufficient resources.
Variable fields	$1: Interface name.
Severity level	4
Example	ETHOAM/4/ETHOAM_LOOPBACK_NO_RESOURCE: OAM interface Ethernet1/0/1 can’t enter remote loopback due to insufficient resources.
Explanation	The OAM interface cannot enter remote loopback due to insufficient resources when you execute the **oam remote-loopback start** command on the local or remote OAM entity.
Recommended action	To enable remote loopback on an interface, you must set the hardware forwarding resources on the interface. Enabling remote loopback on a large number of interfaces might cause insufficient resources. Disable remote loopback on other interfaces, and execute the **oam remote-loopback start** command on the interface again.

ETHOAM_LOOPBACK_NOT_SUPPORT

Message text	OAM interface [string] can’t enter remote loopback because the operation is not supported.
Variable fields	$1: Interface name.
Severity level	4
Example	ETHOAM/4/ETHOAM_LOOPBACK_NOT_SUPPORT: OAM interface Ethernet1/0/1 can't enter remote loopback because the operation is not supported.
Explanation	The OAM interface cannot enter remote loopback because the operation is not supported on the device.
Recommended action	No action is required.

ETHOAM_QUIT_LOOPBACK_CTRLLED

Message text	The local OAM entity quit remote loopback as controlled DTE on OAM interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_QUIT_LOOPBACK_CTRLLED: The local OAM entity quit remote loopback as controlled DTE on OAM interface Ethernet1/0/1.
Explanation	As the Loopback Control OAMPDUs receiving end, the local end quit remote loopback after you disabled OAM loopback on the peer end.
Recommended action	No action is required.

ETHOAM_QUIT_LOOPBACK_CTRLLING

Message text	The local OAM entity quit remote loopback as controlling DTE on OAM interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_QUIT_LOOPBACK_CONTROLLING: The local OAM entity quit remote loopback as controlling DTE on OAM interface Ethernet1/0/1.
Explanation	The local end quit remote loopback after you disabled OAM loopback on the local interface.
Recommended action	No action is required.

ETHOAM_REMOTE_CRITICAL

Message text	A remote Critical event occurred on interface [string].
Variable fields	$1: Interface name.
Severity level	4
Example	ETHOAM/4/ETHOAM_REMOTE_CRITICAL: A remote Critical event occurred on interface Ethernet1/0/1.
Explanation	A remote critical event occurred.
Recommended action	Do not use the link until it recovers.

ETHOAM_REMOTE_DYING_GASP

Message text	A remote Dying Gasp event occurred on interface [string].
Variable fields	$1: Interface name.
Severity level	4
Example	ETHOAM/4/ETHOAM_REMOTE_DYING_GASP: A remote Dying Gasp event occurred on interface Ethernet1/0/1.
Explanation	A remote Dying Gasp event occurred when you reboot the remote device and shut down the interface.
Recommended action	Do not use this link until it recovers.

ETHOAM_REMOTE_ERROR_FRAME

Message text	An errored frame event occurred on the peer interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME: An errored frame event occurred on the peer interface Ethernet1/0/1.
Explanation	An errored frame event occurred on the peer.
Recommended action	Check the link between the local and peer ends.

ETHOAM_REMOTE_ERROR_FRAME_PERIOD

Message text	An errored frame period event occurred on the peer interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME_PERIOD: An errored frame period event occurred on the peer interface Ethernet1/0/1.
Explanation	An errored frame period event occurred on the peer interface.
Recommended action	Check the link between the local and peer ends.

ETHOAM_REMOTE_ERROR_FRAME_SECOND

Message text	An errored frame seconds event occurred on the peer interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_REMOTE_ERROR_FRAME_SECOND: An errored frame seconds event occurred on the peer interface Ethernet1/0/1.
Explanation	An errored frame seconds event occurred on the peer.
Recommended action	Check the link between the local and peer ends.

ETHOAM_REMOTE_ERROR_SYMBOL

Message text	An errored symbol event occurred on the peer interface [string].
Variable fields	$1: Interface name.
Severity level	6
Example	ETHOAM/6/ETHOAM_REMOTE_ERROR_SYMBOL: An errored symbol event occurred on the peer interface Ethernet1/0/1.
Explanation	An errored symbol event occurred on the peer.
Recommended action	Check the link between the local and peer ends.

ETHOAM_REMOTE_EXIT

Message text	OAM interface [string] quit OAM connection because Ethernet OAM is disabled on the peer interface.
Variable fields	$1: Interface name.
Severity level	5
Example	ETHOAM/5/ETHOAM_REMOTE_EXIT: OAM interface Ethernet1/0/1 quit OAM connection because Ethernet OAM is disabled on the peer interface.
Explanation	The local interface ended the OAM connection because Ethernet OAM was disabled on the peer interface.
Recommended action	No action is required.

ETHOAM_REMOTE_FAILURE_RECOVER

Message text	Peer interface [string] recovered.
Variable fields	$1: Interface name.
Severity level	5
Example	ETHOAM/5/ETHOAM_REMOTE_FAILURE_RECOVER: Peer interface Ethernet1/0/1 recovered.
Explanation	The Link fault was cleared from the peer interface and the OAM connection was restored.
Recommended action	No action is required.

ETHOAM_REMOTE_LINK_FAULT

Message text	A remote Link Fault event occurred on interface [string].
Variable fields	$1: Interface name.
Severity level	4
Example	ETHOAM/4/ETHOAM_REMOTE_LINK_FAULT: A remote Link Fault event occurred on interface Ethernet1/0/1.
Explanation	A remote Link Fault event occurred when the remote link went down.
Recommended action	Reconnect the Rx end of the fiber on the remote interface.

ETHOAM_NO_ENOUGH_RESOURCE

Message text	The configuration failed on OAM interface [string] because of insufficient resources.
Variable fields	$1: Interface name.
Severity level	4
Example	ETHOAM/4/ETHOAM_NO_ENOUGH_RESOURCE: The configuration failed on OAM interface Ethernet1/0/1 because of insufficient resources.
Explanation	The configuration failed on the OAM interface because of insufficient system resources.
Recommended action	Remove useless configurations to release the resources, and execute the command again.

ETHOAM_NOT_CONNECTION_TIMEOUT

Message text	Interface [string] quit Ethernet OAM because it received no Information OAMPDU before the timer times out.
Variable fields	$1: Interface name.
Severity level	5
Example	ETHOAM/5/ETHOAM_NOT_CONNECTION_TIMEOUT: Interface Ethernet1/0/1 quit Ethernet OAM because it received no Information OAMPDU before the timer times out.
Explanation	The local interface ended Ethernet OAM because it had not received Information OAMPDUs before the timer timed out.
Recommended action	Check the link status and the OAM status on the peer.

EVB messages

This section contains EVB messages.

EVB_AGG_FAILED

Message text	Remove port [STRING] from aggregation group [STRING]. Otherwise, the EVB feature does not take effect.
Variable fields	$1: Port name. $2: Aggregation port name.
Severity level	6
Example	EVB/6/EVB_AGG_FAILED: Remove port GigabitEthernet5/0/5 from aggregation group Bridge-Aggregation5. Otherwise, the EVB feature does not take effect.
Explanation	EVB bridge fails to process a port in an aggregation group.
Recommended action	Remove the port from the aggregation group.

EVB_LICENSE_EXPIRE

Message text	The EVB feature's license will expire in [UINT32] days.
Variable fields	$1: Number of days.
Severity level	6
Example	EVB/6/EVB_LICENSE_EXPIRE: The EVB feature's license will expire in 15 days.
Explanation	The license for EVB will expire in the specified number of days.
Recommended action	Purchase and register a new license for the EVB feature.

EVB_VSI_OFFLINE

Message text	VSI [STRING] went offline.
Variable fields	$1: VSI interface/VSI aggregate interface name.
Severity level	6
Example	EVB/6/EVB_VSI_OFFLINE: VSI Schannel-Aggregation1:2.0 went offline.
Explanation	The VSI interface or VSI aggregate interface is deleted when either of the following events occurs: • The EVB bridge receives a VDP packet from the EVB station. • The EVB bridge has not received an acknowledgement after a VDP packet times out.
Recommended action	No action is required.

EVB_VSI_ONLINE

Message text	VSI [STRING] came online, status is [STRING].
Variable fields	$1: VSI interface/VSI aggregate interface name. $2: VSI status.
Severity level	6
Example	EVB/6/EVB_VSI_ONLINE: VSI Schannel-Aggregation1:2.0 came online, status is association.
Explanation	The EVB bridge receives a VDP packet and creates a VSI interface or VSI aggregate interface successfully.
Recommended action	No action is required.

EVIISIS messages

This section contains EVI IS-IS messages.

EVIISIS_LICENSE

Message text	The EVIISIS feature has [STRING] license.
Variable fields	$1: License state: ○ **available**—A valid license was found. ○ **no available**—The current license became invalid, or no valid license was found.
Severity level	5
Example	EVIISIS/5/EVIISIS_LICENSE: The EVIISIS feature has available license.
Explanation	This message is generated when EVI IS-IS license status changes. For example, an EVI IS-IS license is installed or becomes invalid.
Recommended action	Install a valid EVI IS-IS license if the current EVI IS-IS license is invalid or no license is available.

EVIISIS_NBR_CHG

Message text	EVIISIS [UINT32], [STRING] adjacency [STRING] ([STRING]), state changed to: [STRING].
Variable fields	$1: EVI IS-IS process ID. $2: EVI IS-IS neighbor level. $3: Neighbor system ID. $4: Interface name. $5: Adjacency state: ○ **up**—Adjacency was set up. ○ **initializing**—Neighbor state was initializing. ○ **down**—Adjacency was lost.
Severity level	5
Example	EVIISIS/5/EVIISIS_NBR_CHG: EVIISIS 1, Level-1 adjacency 0011.2200.1501 (Evi-Link0), state changed to: down.
Explanation	The EVI IS-IS adjacency state changed on an interface.
Recommended action	When the adjacency with a neighbor changes to **down** or **initializing** on an interface, check for EVI IS-IS configuration errors or loss of network connectivity.

FCLINK messages

This section contains FC link messages.

FCLINK_FDISC_REJECT_NORESOURCE

Message text	VSAN [UINT16], Interface [STRING]: An FDISC was rejected because the hardware resource is not enough.
Variable fields	$1: VSAN ID. $2: Interface name.
Severity level	4
Example	FCLINK/4/FCLINK_FDISC_REJECT_NORESOURCE: VSAN 1, Interface FC2/0/1: An FDISC was rejected because the hardware resource is not enough.
Explanation	An FDISC is received when the hardware resources are insufficient.
Recommended action	Reduce the number of nodes.

FCLINK_FLOGI_REJECT_NORESOURCE

Message text	VSAN [UINT16], Interface [STRING]: An FLOGI was rejected because the hardware resource is not enough.
Variable fields	$1: VSAN ID. $2: Interface name.
Severity level	4
Example	FCLINK/4/FCLINK_FLOGI_REJECT_NORESOURCE: VSAN 1, Interface FC2/0/1: An FLOGI was rejected because the hardware resource is not enough.
Explanation	An FLOGI is received when the hardware resources are insufficient.
Recommended action	Reduce the number of nodes.

FCOE messages

This section contains FCoE messages.

FCOE_INTERFACE_NOTSUPPORT_FCOE

Message text	Because the aggregate interface [STRING] has been bound to a VFC interface, assigning the interface [STRING] that does not support FCoE to the aggregate interface might cause incorrect processing.
Variable fields	$1: Aggregate interface name. $2: Ethernet interface name.
Severity level	4
Example	FCOE/4/FCOE_INTERFACE_NOTSUPPORT_FCOE: Because the aggregate interface Bridge-Aggregation 1 has been bound to a VFC interface, assigning the interface Ten-GigabitEthernet 2/0/1 that does not support FCoE to the aggregate interface might cause incorrect processing.
Explanation	This message is generated when an interface that does not support FCoE is assigned to an aggregate interface that has been bound to a VFC interface.
Recommended action	Assign an interface that supports FCoE to the aggregate interface, or remove the binding from the VFC interface.

FCZONE messages

This section contains FC zone messages.

FCZONE_HARDZONE_DISABLED

Message text	-VSAN=[UINT16]: No enough hardware resource for zone rule, switched to soft zoning.
Variable fields	$1: VSAN ID.
Severity level	4
Example	FCZONE/4/FCZONE_HARDZONE_DISABLED: -VSAN=2: No enough hardware resource for zone rule, switched to soft zoning.
Explanation	Insufficient hardware resources.
Recommended action	Activate a smaller zone set.

FCZONE_HARDZONE_ENABLED

Message text	-VSAN=[UINT16]: Hardware resource for zone rule is restored, switched to hard zoning.
Variable fields	$1: VSAN ID.
Severity level	6
Example	FCZONE/6/FCZONE_HARDZONE_ENABLED: -VSAN=2: Hardware resource for zone rule is restored, switched to hard zoning.
Explanation	Hard zoning is enabled in a VSAN because the hardware resources are restored.
Recommended action	No action is required.

FCZONE_ISOLATE_NEIGHBOR

Message text	-VSAN=[UINT16]; All the E ports connected to a neighbor were isolated because of merge failure, and the neighbor's switch WWN is [STRING].
Variable fields	$1: VSAN ID. $2: Neighbor's switch WWN.
Severity level	4
Example	FCZONE/4/FCZONE_ISOLATE_NEIGHBOR: -VSAN=2; All the E ports connected to a neighbor were isolated because of merge failure, and the neighbor's switch WWN is 10:00:00:11:22:00:0d:01.
Explanation	All E_Ports connected to a neighbor were isolated because a merge operation with the neighbor failed.
Recommended action	To resolve the problem: **102.** Use the **display current-configuration** command on the local switch and the neighbor switch to view their zoning configurations. **103.** Modify those noncompliant configurations on both switches to be compliant with merge rules. **104.** Execute the **shutdown** and **undo shutdown** command sequence on those isolated E_Ports to trigger a new merge operation.

FCZONE_ISOLATE_ALLNEIGHBOR

Message text	-VSAN=[UINT16]; The E ports connected to all neighbors were isolated, because the length of the locally generated MR packet exceeded the limit.
Variable fields	$1: VSAN ID.
Severity level	4
Example	FCZONE/4/FCZONE_ISOLATE_ALLNEIGHBOR: -VSAN=2; The E ports connected to all neighbors were isolated, because the length of the locally generated MR packet exceeded the limit.
Explanation	E_Ports connected to all neighbors were isolated because the length of the locally generated MR packet exceeded the limit.
Recommended action	To resolve the problem: **105.** Use the **display current-configuration** command on the local switch to view the zoning configuration. **106.** Delete unnecessary zoning configuration of the active zone set. **107.** Execute the **shutdown** and **undo shutdown** command sequence on those isolated E_Ports to trigger a new merge operation. Or **108.** Activate a smaller zone set. **109.** Execute the **shutdown** and **undo shutdown** command sequence on those isolated E_Ports to trigger a new merge operation.

FCZONE_ISOLATE_CLEAR_VSAN

Message text	-Interface=[STRING]-VSAN=[UINT16]; Isolation status was cleared.
Variable fields	$1: Interface name. $2: VSAN ID.
Severity level	6
Example	FCZONE/6/FCZONE_ISOLATE_CLEAR_VSAN: -Interface=Fc0/2/7-VSAN=2; Isolation status was cleared.
Explanation	The isolation status of an interface was cleared in a VSAN.
Recommended action	No action is required.

FCZONE_ISOLATE_CLEAR_ALLVSAN

Message text	-Interface=[STRING]; Isolation status was cleared in all supported VSANs.
Variable fields	$1: Interface name.
Severity level	6
Example	FCZONE/6/FCZONE_ISOLATE_CLEAR_ALLVSAN: -Interface=Fc0/2/7; Isolation status was cleared in all supported VSANs.
Explanation	The isolation status of an interface was cleared in all supported VSANs.
Recommended action	No action is required.

FCZONE_DISTRIBUTE_FAILED

Message text	-VSAN=[UINT16]; Zone distribution failed. The zoning configurations might consequently be inconsistent across the fabric.
Variable fields	$1: VSAN ID.
Severity level	4
Example	FCZONE/4/FCZONE_DISTRIBUTE_FAILED: -VSAN=2; Zone distribution failed. The zoning configurations might consequently be inconsistent across the fabric.
Explanation	A distribution operation failed. Consequently, the zoning configurations might be inconsistent across the fabric.
Recommended action	To resolve the problem if the distribution operation is triggered by using the **zoneset activate** command: **110.** Verify that the contents of the active zone set are consistent on all switches by using the **display current-configuration** command. **111.** Reactivate the zone set and distribute it to the entire fabric by using the **zoneset activate** command. To resolve the problem if the distribution operation is triggered by using the **zoneset distribute** command: **112.** Verify that the contents of the active zone set and zone database are consistent on all switches by using the **display current-configuration** command. **113.** Trigger a new complete distribution by using the **zoneset distribute** command. To resolve the problem if the distribution operation is triggered by a zoning mode switchover: **114.** Verify that the zoning mode is the same on all switches by using the **display zone status** command. **115.** Trigger a new complete distribution by using the **zoneset distribute** command.

File filtering messages

This section contains file filtering messages.

FFILTER_IPV4_LOG

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];DataDirection(1081)=[STRING];RuleName(1080)=[STRING];PolicyName(1079)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZone(1025)=[STRING];DstZone(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];Filetype(1096)=[STRING];FileName(1097)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Data direction. Available values are: o Upload. o Download. o Both. $4: Rule name. $5: Policy name. $6: Source IP address. $7: Source port number. $8: Destination IP address. $9: Destination port number. $10: Source security zone. $11: Destination security zone. $12: Identity username. $13: Action applied to on the packet. Available actions are: o Permit. o Drop. $14: File type. $15: File name. $16: VLAN ID. $17: VXLAN ID. $18: Source location. $19: Destination location.
Severity level	6
Example	FFILTER/6/FFILTER_IPV4_LOG:-MDC=1;Protocol(1001)=TCP;Application(1002)=SMTP;DataDirection(1081)=upload;RuleName(1080)=ruletest;PolicyName(1079)=policytest;SrcIPAddr(1003)=21.22.23.20;SrcPort(1004)=51396;DstIPAddr(1007)=25.26.27.20;DstPort(1008)=25;SrcZone(1025)=in;DstZone(1035)=in;UserName(1113)=abc;Action(1053)=drop;Filetype(1096)=txt;FileName(1097)=abc.txt;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	An IPv4 packet matched a file filtering rule.
Recommended action	No action is required.

FFILTER_IPV6_LOG

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];DataDirection(1081)=[STRING];RuleName(1080)=[STRING];PolicyName(1079)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZone(1025)=[STRING];DstZone(1035)=[STRING];UserName(1113)=[STRING];action(1053)=[STRING];Filetype(1096)=[STRING];FileName(1097)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Data direction. Available values are: o Upload. o Download. o Both. $4: Rule name. $5: Policy name. $6: Source IPv6 address. $7: Source port number. $8: Destination IPv6 address. $9: Destination port number. $10: Source security zone. $11: Destination security zone. $12: Identity username. $13: Action applied to on the packet. Available actions are: o Permit. o Drop. $14: File type. $15: File name. $16: VLAN ID. $17: VXLAN ID. $18: Source location. $19: Destination location.
Severity level	6
Example	FFILTER/6/FFILTER_IPV6_LOG:-MDC=1;Protocol(1001)=TCP;Application(1002)=SMTP;DataDirection(1081)=upload;RuleName(1080)=ruletest;PolicyName(1079)=policytest;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZone(1025)=in;DstZone(1035)=in;UserName(1113)=aaa;Action(1053)=drop;Filetype(1096)=txt;FileName(1097)=abc.txt;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	An IPv6 packet matched a file filtering rule.
Recommended action	No action is required.

FILTER messages

This section contains filter messages.

FILTER_EXECUTION_ICMP

Message text	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];Type(1067)=[STRING];Acl(1068)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];DstIPAddr(1007)=[IPADDR];IcmpType(1062)=[STRING]([UINT16]);IcmpCode(1063)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Receiving interface name. $2: Direction. $3: ACL type. $4: ACL number or name. $5: ACL rule ID. $6: Layer 4 protocol name. $7: Source IP address. $8: Destination IP address. $9: ICMP message type. $10: ICMP message code. $11: Match count. $12: Event information.
Severity level	6
Example	FILTER/6/FILTER_EXECUTION_ICMP: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;Type(1067)=IPv4;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;DstIPAddr(1007)=200.1.1.1;IcmpType(1062)=Echo(8);IcmpCode(1063)=0;MatchCount(1069)=1000;Event(1048)=Permit;
Explanation	ICMP packets matched the packet filter. This message is sent when the first ICMP packet of a flow matches the packet filter, and it will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_EXECUTION_ICMPV6

Message text	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];Type(1067)=[STRING];Acl(1068)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[IPADDR];DstIPv6Addr(1037)=[IPADDR];Icmpv6Type(1064)=[STRING]([UINT16]);Icmpv6Code(1065)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Receiving interface name. $2: Direction. $3: ACL type. $4: ACL number or name. $5: ACL rule ID. $6: Layer 4 protocol name. $7: Source IPv6 address. $8: Destination IPv6 address. $9: ICMPv6 message type. $10: ICMPv6 message code. $11: Match count. $12: Event information.
Severity level	6
Example	FILTER/6/FILTER_EXECUTION_ICMP: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;Type(1067)=IPv4;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;DstIPAddr(1007)=200.1.1.1;IcmpType(1062)=Echo(8);IcmpCode(1063)=0;MatchCount(1069)=1000;Event(1048)=Permit;
Explanation	ICMPv6 packets matched the packet filter. This message is sent when the first ICMPv6 packet of a flow matches the packet filter, and it will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_IPV4_EXECUTION

Message text	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];Type(1067)=[STRING];Acl(1068)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Receiving interface name. $2: Direction. $3: ACL type. $4: ACL number or name. $5: ACL rule ID. $6: Layer 4 protocol name. $7: Application name. $8: Source IP address. $9: Source port. $10: Destination IP address. $11: Destination port number. $12: Match count. $13: Event information.
Severity level	6
Example	FILTER/6/FILTER_IPV4_EXECUTION: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;Type(1067)=IPv4;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=Permit;
Explanation	Packets other than ICMP packets matched the packet filter. This message is sent when the first packet of a flow matches the packet filter, and it will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_IPV6_EXECUTION

Message text	RcvIfName(1023)=[STRING];Direction(1070)=[STRING];Type(1067)=[STRING];Acl(1068)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Receiving interface name. $2: Direction. $3: ACL type. $4: ACL number or name. $5: ACL rule ID. $6: Layer 4 protocol name. $7: Application name. $8: Source IPv6 address. $9: Source port number. $10: Destination IPv6 address. $11: Destination port number. $12: Match count. $13: Event information.
Severity level	6
Example	FILTER/6/FILTER_IPV6_EXECUTION: RcvIfName(1023)=GigabitEthernet2/0/2;Direction(1070)=inbound;Type(1067)=IPv6;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3001::1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=Permit;
Explanation	Packets other than ICMPv6 packets matched the packet filter. This message is sent when the first packet of a flow matches the packet filter, and it will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_IPV4_EXECUTION

Message text	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];ObjectPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: Type of the object policy. $4: Name of the object policy. $5: ID of the object policy rule. $6: Layer 4 protocol name. $7: Application name. $8: Source IP address. $9: Source port number. $10: Destination IP address. $11: Destination port number. $12: Match count. $13: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4;ObjectPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=permit;
Explanation	A flow matched an object policy. This message is sent when the first packet of a flow matches the object policy, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_IPV4_EXECUTION

Message text	SrcZoneName(1025)=zone1;DstZoneName(1035)=[STRING];Type(1067)=[STRING];Acl(1068)=[UINT16];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: ACL type. $4: ACL number or name. $5: ACL rule ID. $6: Layer 4 protocol name. $7: Application name. $8: Source IP address. $9: Source port number. $10: Destination IP address. $11: Destination port number. $12: Match count. $13: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4; Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp; SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1; DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=permit;
Explanation	A flow matched the packet filter. This message is sent when the first packet of a flow matches the packet filter, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_IPV4_EXECUTION

Message text	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];SecurityPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];SrcMacAddr(1021)=[STRING];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];VlanID(1175)=[UINT16];VNI(1211)=[UINT32];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: Security policy type. $4: Security policy name. $5: Security policy rule ID. $6: Layer 4 protocol name. $7: Application name. $8: Source IP address. $9: Source port number. $10: Source MAC address. $11: Destination IP address. $12: Destination port number. $13: VLAN ID. $14: VXLAN ID. $15: Match count. $16: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_IPV4_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4;SecurityPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;SrcMacAddr(1021)=000f-e267-76eb;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;VlanID(1175)=10;VNI(1211)=--;MatchCount(1069)=1000;Event(1048)=permit;
Explanation	A flow matched the security policy. This message is sent when the first packet of a flow matches the security policy, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_IPV6_EXECUTION

Message text	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];ObjectPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: Type of the object policy. $4: Name of the object policy. $5: ID of the object policy rule. $6: Layer 4 protocol name. $7: Application name. $8: Source IPv6 address. $9: Source port number. $10: Destination IPv6 address. $11: Destination port number. $12: Match count. $13: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_IPV6_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;ObjectPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=permit;
Explanation	A flow matched an object policy. This message is sent when the first packet of a flow matches the object policy, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_IPV6_EXECUTION

Message text	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];Acl(1068)=[UINT16];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: ACL type. $4: ACL number or name. $5: ACL rule ID. $6: Layer 4 protocol name. $7: Application name. $8: Source IPv6 address. $9: Source port number. $10: Destination IPv6 address. $11: Destination port number. $12: Match count. $13: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_IPV6_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=permit;
Explanation	A flow matched the packet filter. This message is sent when the first packet of a flow matches the packet filter, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_IPV6_EXECUTION

Message text	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];SecurityPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];VlanID(1175)=[UINT16];VNI(1211)=[UINT32];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: Security policy type. $4: Security policy name. $5: Security policy rule ID. $6: Layer 4 protocol name. $7: Application name. $8: Source IPv6 address. $9: Source port number. $10: Destination IPv6 address. $11: Destination port number. $12: VLAN ID. $13: VXLAN ID. $14: Match count. $15: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_IPV6_EXECUTION: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=TCP;Application(1002)=ftp;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026;VlanID(1175)=10;VNI(1211)=--;MatchCount(1069)=1000;Event(1048)=permit;
Explanation	A flow matched the security policy. This message is sent when the first packet of a flow matches the security policy, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_EXECUTION_ICMP

Message text	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];ObjectPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: Type of the object policy. $4: Name of the object policy. $5: ID of the object policy rule. $6: Layer 4 protocol name. $7: Source IP address. $8: Source port number. $9: Destination IP address. $10: Destination port number. $11: Match count. $12: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_EXECUTION_ICMP: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4;ObjectPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=permit;
Explanation	ICMP packets matched an object policy. This message is sent when the first ICMP packet of a flow matches the object policy, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_EXECUTION_ICMP

Message text	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];Acl(1068)=[UINT16];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: ACL type. $4: ACL number or name. $5: ACL rule ID. $6: Layer 4 protocol name. $7: Source IP address. $8: Source port number. $9: Destination IP address. $10: Destination port number. $11: Match count. $12: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_EXECUTION_ICMP: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;MatchCount(1069)=1000;Event(1048)=permit;
Explanation	ICMP packets matched the packet filter. This message is sent when the first ICMP packet of a flow matches the packet filter, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_EXECUTION_ICMP

Message text	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];SecurityPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPAddr(1003)=[STRING];SrcPort(1004)=[UINT16];SrcMacAddr(1021)=[STRING];DstIPAddr(1007)=[STRING];DstPort(1008)=[UINT16];VlanID(1175)=[UINT16];VNI(1211)=[UINT32];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: Security policy type. $4: Security policy name. $5: Security policy rule ID. $6: Layer 4 protocol name. $7: Source IP address. $8: Source port number. $9: Source MAC address. 10: Destination IP address. $11: Destination port number. $12: VLAN ID. $13: VXLAN ID. $14: Match count. $15: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_EXECUTION_ICMP: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv4;SecurityPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=ICMP;SrcIPAddr(1003)=100.1.1.1;SrcPort(1004)=1025;SrcMacAddr(1021)=dc4a-3e7d-91b1;DstIPAddr(1007)=200.1.1.1;DstPort(1008)=1026;VlanID(1175)=10;VNI(1211)=--;MatchCount(1069)=1000;Event(1048)=permit;
Explanation	ICMP packets matched the security policy. This message is sent when the first ICMP packet of a flow matches the security policy, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_EXECUTION_ICMPV6

Message text	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];ObjectPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: Type of the object policy. $4: Name of the object policy. $5: ID of the object policy rule. $6: Layer 4 protocol name. $7: Source IPv6 address. $8: Source port number. $9: Destination IPv6 address. $10: Destination port number. $11: Match count. $12: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_EXECUTION_ICMPV6: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;ObjectPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=ICMPV6;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026; MatchCount(1069)=1000;Event(1048)=permit;
Explanation	ICMPv6 packets matched an object policy. This message is sent when the first ICMPv6 packet of a flow matches the object policy, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_EXECUTION_ICMPV6

Message text	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];Acl(1068)=[UINT16];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: ACL type. $4: ACL number or name. $5: ACL rule ID. $6: Layer 4 protocol name. $7: Source IPv6 address. $8: Source port number. $9: Destination IPv6 address. $10: Destination port number. $11: Match count. $12: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_EXECUTION_ICMPV6: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;Acl(1068)=3000;RuleID(1078)=0;Protocol(1001)=ICMPV6;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026; MatchCount(1069)=1000;Event(1048)=permit;
Explanation	ICMPv6 packets matched the packet filter. This message is sent when the first ICMPv6 packet of a flow matches the packet filter, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FILTER_ZONE_EXECUTION_ICMPV6

Message text	SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];Type(1067)=[STRING];SecurityPolicy(1072)=[STRING];RuleID(1078)=[UINT32];Protocol(1001)=[STRING];SrcIPv6Addr(1036)=[STRING];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[STRING];DstPort(1008)=[UINT16];VlanID(1175)=[UINT16];VNI(1211)=[UINT32];MatchCount(1069)=[UINT32];Event(1048)=[STRING];
Variable fields	$1: Source security zone. $2: Destination security zone. $3: Security policy type. $4: Security policy name. $5: Security policy rule ID. $6: Layer 4 protocol name. $7: Source IPv6 address. $8: Source port number. $9: Destination IPv6 address. $10: Destination port number. $11: VLAN ID. $12: VXLAN ID. $13: Match count. $14: Event information.
Severity level	6
Example	FILTER/6/FILTER_ZONE_EXECUTION_ICMPV6: SrcZoneName(1025)=zone1;DstZoneName(1035)=zone2;Type(1067)=IPv6;SecurityPolicy(1072)=policy1;RuleID(1078)=0;Protocol(1001)=ICMPV6;SrcIPv6Addr(1036)=2001::1;SrcPort(1004)=1025;DstIPv6Addr(1037)=3000::1;DstPort(1008)=1026;VlanID(1175)=10;VNI(1211)=--;MatchCount(1069)=1000;Event(1048)=permit;
Explanation	ICMPv6 packets matched the security policy. This message is sent when the first ICMPv6 packet of a flow matches the security policy, and the message will be sent regularly for the flow.
Recommended action	No action is required.

FIPSNG messages

This section contains FIP snooping messages.

FIPSNG_HARD_RESOURCE_NOENOUGH

Message text	No enough hardware resource for FIP snooping rule.
Variable fields	N/A
Severity level	4
Example	FIPSNG/4/FIPSNG_HARD_RESOURCE_NOENOUGH: No enough hardware resource for FIP snooping rule.
Explanation	Hardware resources are insufficient.
Recommended action	No action is required.

FIPSNG_HARD_RESOURCE_RESTORE

Message text	Hardware resource for FIP snooping rule is restored.
Variable fields	N/A
Severity level	6
Example	FIPSNG/6/FIPSNG_HARD_RESOURCE_RESTORE: Hardware resource for FIP snooping is restored.
Explanation	Hardware resources for FIP snooping rules are restored.
Recommended action	No action is required.

FS messages

This section contains file system messages.

FS_UNFORMATTED_PARTITION

Message text	Partition [%s] is not formatted yet. Please format the partition first.
Variable fields	$1: Partition name.
Severity level	4
Example	FS/4/FS_UNFORMATED_PARTITION: Partition usba0: is not formatted yet. Please format the partition first.
Explanation	The partition is not formatted. You must format a partition before you can perform other operations on the partition.
Recommended action	Format the specified partition.

FTP messages

This section contains File Transfer Protocol messages.

FTP_ACL_DENY

Message text	The FTP Connection request from [IPADDR]([STRING]) was denied by ACL rule (rule ID=[INT32])
Variable fields	$1: IP address of the FTP client. $2: VPN instance to which the FTP client belongs. $3: ID of the rule that denied the FTP client. If an FTP client does not match created ACL rules, the device denies the client based on the default ACL rule.
Severity level	5
Example	FTP/5/FTP_ACL_DENY: The FTP connection request from 181.1.1.10 was denied by ACL rule (rule ID=20). FTP/5/FTP_ACL_DENY: The FTP connection request from 181.1.1.10 was denied by ACL rule (default rule).
Explanation	FTP access control ACLs control which FTP clients can access the FTP service on the device. The device sends this log message when it denies an FTP client.
Recommended action	No action is required.

FTP_REACH_SESSION_LIMIT

Message text	FTP client $1 failed to log in. The current number of FTP sessions is [NUMBER]. The maximum number allowed is ([NUMBER]).
Variable fields	$1: IP address of the FTP client. $2: Current number of FTP sessions. $3: Maximum number of FTP sessions allowed by the device.
Severity level	6
Example	FTP/6/FTP_REACH_SESSION_LIMIT: FTP client 1.1.1.1 failed to log in. The current number of FTP sessions is 10. The maximum number allowed (10).
Explanation	The number of FTP connections reached the limit.
Recommended action	**116.** Use the **display current-configuration | include session-limit** command to view the current limit for FTP connections. If the command does not display the limit, the device is using the default setting. **117.** If you want to set a greater limit, execute the **aaa session-limit** command. If you think the limit is proper, no action is required.

GLB messages

This section contains GLB messages.

GLB_SYNCGROUP_CMD_DENY

Message text	Configuration deployment is not allowed because of configuration conflicts on default synchronization group member devices. Please choose one device to execute the command: loadbalance default-syncgroup sync config.
Variable fields	None
Severity level	5
Example	NSFOCUS GLB/5/GLB_SYNCGROUP_CMD_DENY: Configuration deployment is not allowed because of configuration conflicts on default synchronization group member devices. Please choose one device to execute the command: loadbalance default-syncgroup sync config.
Explanation	Configuration deployment is not allowed because of configuration conflicts on default synchronization group members.
Recommended action	Execute the **`loadbalance default-syncgroup sync config`** command on any of the default synchronization group members.

GLB_SYNCGROUP_MEM_CONNECT

Message text	The default synchronization group member [STRING] connected to [STRING] successfully.
Variable fields	$1: Default synchronization group member name. $2: Default synchronization group member name.
Severity level	5
Example	GLB/5/GLB_SYNCGROUP_MEM_CONNECT: The default synchronization group member %s connected to %s successfully.
Explanation	Two default synchronization group members established a connection..
Recommended action	No action is required.

GLB_SYNCGROUP_MEM_DISCONNECT

Message text	The default synchronization group member [STRING] disconnected from [STRING] due to configuration changes.
Variable fields	$1: Default synchronization group member name. $2: Default synchronization group member name.
Severity level	5
Example	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT: The default synchronization group member site1 disconnected from site2 due to configuration changes.
Explanation	A connection between default synchronization group members disconnected due to configuration changes.
Recommended action	Check whether member communication capability is enabled and check the IP address and other settings.

GLB_SYNCGROUP_MEM_DISCONNECT

Message text	The default synchronization group member [STRING] disconnected from [STRING] due to timeout.
Variable fields	$1: Default synchronization group member name. $2: Default synchronization group member name.
Severity level	5
Example	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT:The default synchronization group member site1 disconnected from site2 due to timeout.
Explanation	A connection between default synchronization group members disconnected due to timeout.
Recommended action	Check the member configuration and network connectivity (whether the peer IP address can be successfully pinged).

GLB_SYNCGROUP_MEM_DISCONNECT

Message text	The default synchronization group member [STRING] disconnected from [STRING] due to a disconnect message.
Variable fields	$1: Default synchronization group member name. $2: Default synchronization group member name.
Severity level	5
Example	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT:The default synchronization group member site1 disconnected from site2 due to a disconnect message.
Explanation	A connection between default synchronization group members disconnected due to a disconnect message.
Recommended action	Check the configuration on the remote member if the connection cannot be re-established.

GLB_SYNCGROUP_MEM_DISCONNECT

Message text	The default synchronization group member [STRING] disconnected from [STRING] due to receiving an EPOLLHUP/EPOLLERR signal.
Variable fields	$1: Default synchronization group member name. $2: Default synchronization group member name.
Severity level	5
Example	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT:The default synchronization group member site1 disconnected from site2 due to receiving an EPOLLHUP/EPOLLERR signal.
Explanation	A connection between default synchronization group members disconnected due to receiving an EPOLLHUP/EPOLLERR signal.
Recommended action	Check the network connectivity if the connection cannot be automatically re-established.

GLB_SYNCGROUP_MEM_DISCONNECT

Message text	The default synchronization group member [STRING] disconnected from [STRING] due to disconnection of the TCP connection by the peer.
Variable fields	$1: Default synchronization group member name. $2: Default synchronization group member name.
Severity level	5
Example	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT:The default synchronization group member site1 disconnected from site2 due to disconnection of the TCP connection by the peer.
Explanation	A connection between default synchronization group members disconnected because the remote member closed the connection.
Recommended action	Check whether the IP address configuration is the same on the two ends.

GLB_SYNCGROUP_MEM_DISCONNECT

Message text	The default synchronization group member [STRING] failed to connect to [STRING] due to different member names.
Variable fields	$1: Default synchronization group member name. $2: Default synchronization group member name.
Severity level	5
Example	GLB/5/GLB_SYNCGROUP_MEM_DISCONNECT: The default synchronization group member %s failed to connect to %s due to different member names.
Explanation	Two default synchronization group members failed to establish a connection due to different member names.
Recommended action	Modify one member name to be the same as another member name..

GLB_SYNCGROUP_MEM_DOMAINCONFLICT

Message text	Failed to configure the domain name ([STRING]), because it had been used by the remote end.
Variable fields	$1: Default synchronization group member name.
Severity level	5
Example	NSFOCUS GLB/5/GLB_SYNCGROUP_MEM_DOMAINCONFLICT: Failed to configure the domain name (site1), because it had been used by the remote end.
Explanation	This message is generated when the domain name has been used by the remote end.
Recommended action	Configure an unused domain name.

GLB_SYNCGROUP_SYNC_CONFLICT

Message text	Inconsistent ([STRING]) configuration exists on the default synchronization group member devices during connection establishment. Please choose one device to execute the command: loadbalance default-syncgroup sync config. The value **some** indicates that the remote end detects inconsistent configurations.
Variable fields	$1: Inconsistent object: ○ **data-center**. ○ **global-dns-map**. ○ **global-isp**. ○ **global-proximity**. ○ **global-region**. ○ **global-reverse-zone**. ○ **global-topology**. ○ **global-vsp**. ○ **global-zone**. ○ **some**—The remote end detects inconsistent configurations.
Severity level	5
Example	NSFOCUS GLB/5/GLB_SYNCGROUP_SYNC_CONFLICT: Inconsistent configuration exists on the default synchronization group member devices during connection establishment. Please choose one device to execute the command: loadbalance default-syncgroup sync config.
Explanation	Inconsistent configuration exists on the default synchronization group member devices during connection establishment.
Recommended action	Execute the **`loadbalance default-syncgroup sync config`** command on any of the default synchronization group members.

gRPC

This section contains gRPC messages.

GRPC_ENABLE_WITHOUT_TLS

Message text	PKI domain [STRING] isn't associated with a valid local certificate. The gRPC process will start without the PKI domain.
Variable fields	$1: PKI domain name.
Severity level	4
Example	GRPC/4/GRPC_ENABLE_WITHOUT_TLS: PKI domain xxx isn't associated with a valid local certificate. The gRPC process will start without the PKI domain.
Explanation	The PKI domain did not have a valid local certificate, and gRPC started without using the PKI domain for secure communications between the device and collectors.
Recommended action	To use the PKI domain for secure communication with collectors, perform the following tasks: **118.** Verify that the PKI domain exists and has a valid local certificate. **119.** Execute the following commands in sequence: ○ **`undo grpc enable`** ○ **`grpc pki domain`** ○ **`grpc enable`**

HA messages

This section contains HA messages.

HA_BATCHBACKUP_FINISHED

Message text	Batch backup of standby board in [STRING] has finished.
Variable fields	$1: Chassis number and slot number or slot number. This field also displays the CPU number if multiple CPUs are available on a slot.
Severity level	5
Example	HA/5/HA_BATCHBACKUP_FINISHED: Batch backup of standby board in slot 1 has finished.
Explanation	Batch backup from the active MPU or CPU to the standby MPU or CPU has finished.
Recommended action	No action is required.

HA_BATCHBACKUP_STARTED

Message text	Batch backup of standby board in [STRING] started.
Variable fields	$1: Chassis number and slot number or slot number. This field also displays the CPU number if multiple CPUs are available on a slot.
Severity level	5
Example	HA/5/HA_BATCHBACKUP_STARTED: Batch backup of standby board in slot 1 started.
Explanation	Batch backup from the active MPU or CPU to the standby MPU or CPU has started.
Recommended action	No action is required.

HA_STANDBY_NOT_READY

Message text	Standby board in [STRING] is not ready, reboot ...
Variable fields	$1: Chassis number and slot number or slot number. This field also displays the CPU number if multiple CPUs are available on a slot.
Severity level	4
Example	HA/4/HA_STANDBY_NOT_READY: Standby board in slot 1 is not ready, reboot ...
Explanation	This message appears on the standby MPU or CPU. When batch backup is not complete on the standby MPU or CPU, performing active and standby MPU switchover results in restart of the active and standby MPUs or CPUs.
Recommended action	Do not perform active and standby MPU switchover before batch backup is complete on the standby MPU.

HA_STANDBY_TO_MASTER

Message text	Standby board in [STRING] changed to the master.
Variable fields	$1: Chassis number and slot number or slot number. This field also displays the CPU number if multiple CPUs are available on a slot.
Severity level	5
Example	HA/5/HA_STANDBY_TO_MASTER: Standby board in slot 1 changed to the master.
Explanation	An active and standby MPU switchover occurs. The standby MPU CPU changed to active.
Recommended action	No action is required.

HLTH messages

This section contains health monitoring messages.

LIPC_COMM_FAULTY

Message text	LIPC [STRING] between [STRING] and [STRING] might be faulty.
Variable fields	$1: LIPC communication type. Options include: ○ **unicast**—Unicast communication. ○ **broadcast**—Broadcast communication. ○ **topo**—Topology communication. $2: Chassis number and slot number and CPU number, or slot number and CPU number. A CPU number is present only if the slot supports multiple CPUs. $3: Chassis number and slot number and CPU number, or slot number and CPU number. A CPU number is present only if the slot supports multiple CPUs.
Severity level	4
Example	HLTH/4/LIPC_COMM_FAULTY: LIPC unicast between slot 1 and slot 2 might be faulty.
Explanation	An LIPC communication exception occurred.
Recommended action	Execute the **`display system health`** command to identify system health status. If the issue persists after 30 minutes, contact NSFOCUS Support.

LIPC_COMM_RECOVER

Message text	LIPC [STRING] between [STRING] and [STRING] recovered.
Variable fields	$1: LIPC communication type. Options include: ○ **unicast**—Unicast communication. ○ **broadcast**—Broadcast communication. ○ **topo**—Topology communication. $2: Chassis number and slot number and CPU number, or slot number and CPU number. A CPU number is present only if the slot supports multiple CPUs. $3: Chassis number and slot number and CPU number, or slot number and CPU number. A CPU number is present only if the slot supports multiple CPUs.
Severity level	6
Example	HLTH/6/LIPC_COMM_NORMAL: LIPC unicast between slot 1 and slot 2 recovered.
Explanation	The LIPC communication recovered.
Recommended action	No action is required.

HQOS messages

This section contains HQoS messages.

HQOS_DP_SET_FAIL

Message text	Failed to set drop profile [STRING] globally.
Variable fields	$1: Drop profile name.
Severity level	4
Example	HQOS/4/HQOS_DP_SET_FAIL: Failed to set drop profile b globally.
Explanation	The system failed to perform one of the following actions: • Apply a drop profile globally. • Modify a drop profile applied globally.
Recommended action	Check the drop profile settings.

HQOS_FP_SET_FAIL

Message text	Failed to set [STRING] in forwarding profile [STRING] globally.
Variable fields	$1: Policy type: • gts. • bandwidth. • queue. • drop profile. $2: Forwarding profile name.
Severity level	4
Example	HQOS/4/HQOS_FP_SET_FAIL: Failed to set gts in forwarding profile b globally.
Explanation	The system failed to perform one of the following actions: • Apply a forwarding profile globally. • Modify a forwarding profile applied globally.
Recommended action	Examine the forwarding profile, and make sure it is supported and has no conflicted contents.

HQOS_POLICY_APPLY_FAIL

Message text	Failed to apply some forwarding classes or forwarding groups in scheduler policy [STRING] to the [STRING] direction of interface [STRING].
Variable fields	$1: Scheduler policy name. $2: Policy direction: inbound or outbound. $3: Interface name.
Severity level	4
Example	HQOS/4/HQOS_POLICY_APPLY_FAIL: Failed to apply some forwarding classes or forwarding groups in scheduler policy b to the inbound direction of interface Ethernet3/1/2.
Explanation	The system failed to perform one of the following actions: • Apply a scheduler policy to a specific direction of an interface. • Modify a scheduler policy applied to a specific direction of an interface.
Recommended action	Use the **`display qos scheduler-policy diagnosis interface`** command to identify the nodes that failed to be applied and the failure causes, and modify the running configuration.

HQOS_POLICY_APPLY_FAIL

Message text	Failed to recover scheduler policy [STRING] to the [STRING] direction of interface [STRING] due to [STRING].
Variable fields	$1: Scheduler policy name. $2: Policy direction: inbound or outbound. $3: Interface name. $4: Cause.
Severity level	4
Example	HQOS/4/HQOS_POLICY_RECOVER_FAIL: Failed to recover scheduler policy b to the outbound direction of interface Ethernet3/1/2 due to conflicting with QoS configuration.
Explanation	The system failed to recover an applied scheduler policy after the card or device rebooted, because the scheduler policy conflicted with the QoS configuration on the interface.
Recommended action	Check the scheduler policy configuration according to the failure cause.

HTTPD messages

This section contains HTTP daemon messages.

HTTPD_CONNECT

Message text	[STRING] client [STRING] connected to the server successfully.
Variable fields	$1: Connection type, HTTP or HTTPS. $2: Client IP address.
Severity level	6
Example	HTTPD/6/HTTPD_CONNECT: HTTP client 192.168.30.117 connected to the server successfully.
Explanation	The HTTP or HTTPS server accepted the request from a client. An HTTP or HTTPS connection was set up.
Recommended action	No action is required.

HTTPD_CONNECT_TIMEOUT

Message text	[STRING] client [STRING] connection idle timeout.
Variable fields	$1: Connection type, HTTP or HTTPS. $2: Client IP address.
Severity level	6
Example	HTTPD/6/HTTPD_CONNECT_TIMEOUT: HTTP client 192.168.30.117 connection to server idle timeout.
Explanation	An HTTP or HTTPS connection was disconnected because the idle timeout timer expires.
Recommended action	No action is required.

HTTPD_DISCONNECT

Message text	[STRING] client [STRING] disconnected from the server.
Variable fields	$1: Connection type, HTTP or HTTPS. $2: Client IP address.
Severity level	6
Example	HTTPD/6/HTTPD_DISCONNECT: HTTP client 192.168.30.117 disconnected from the server.
Explanation	An HTTP or HTTPS client was disconnected from the server.
Recommended action	No action is required.

HTTPD_FAIL_FOR_ACL

Message text	[STRING] client [STRING] failed the ACL check and could not connect to the server.
Variable fields	$1: Connection type, HTTP or HTTPS. $2: Client IP address.
Severity level	6
Example	HTTPD/6/HTTPD_FAIL_FOR_ACL: HTTP client 192.168.30.117 failed the ACL check and cannot connect to the server.
Explanation	An HTTP or HTTPS client was filtered by the ACL.
Recommended action	No action is required.

HTTPD_FAIL_FOR_ACP

Message text	[STRING] client [STRING] was denied by the certificate access control policy and could not connect to the server.
Variable fields	$1: Connection type, HTTP or HTTPS. $2: Client IP address.
Severity level	6
Example	HTTPD/6/HTTPD_FAIL_FOR_ACP: HTTP client 192.168.30.117 was denied by the certificate attribute access control policy and could not connect to the server.
Explanation	An HTTP or HTTPS client was denied by the certificate access control policy.
Recommended action	No action is required.

HTTPD_REACH_CONNECT_LIMIT

Message text	[STRING] client [STRING] failed to connect to the server, because the number of connections reached the upper limit.
Variable fields	$1: Connection type, HTTP or HTTPS. $2: Client IP address.
Severity level	6
Example	HTTPD/6/HTTPD_REACH_CONNECT_LIMIT: HTTP client 192.168.30.117 failed to connect to the server, because the number of connections reached the upper limit.
Explanation	The number of connections reached the limit.
Recommended action	**120.** Use the **`display current-configuration | include session-limit`** command to view the current limit for connections of the specified type. If the command does not display the limit, the device is using the default setting. **121.** If you want to specify a greater limit, execute the **`aaa session-limit`** command. If you think the limit is proper, no action is required.

Identity messages

This section contains user identification messages.

IDENTITY_AUTO_IMPORT_FINISHED

Message text	Finished importing identity user accounts and groups automatically.
Variable fields	N/A
Severity level	5
Example	IDENTITY/5/IDENTITY_AUTO_IMPORT_FINISHED: Finished importing identity user accounts and groups automatically.
Explanation	The system finished importing identity user accounts and groups automatically.
Recommended action	No action is required.

IDENTITY_AUTO_IMPORT_START

Message text	Started to import identity user accounts and groups automatically.
Variable fields	N/A
Severity level	5
Example	IDENTITY/5/IDENTITY_AUTO_IMPORT_START: Started to import identity user accounts and groups automatically.
Explanation	The system automatically started to import identity user accounts and groups.
Recommended action	No action is required.

IDENTITY_CSV_IMPORT_FAILED

Message text	Failed to import identity user [STRING] to domain [STRING] from the .csv file.
Variable fields	$1: Identity username. $2: Identity domain name.
Severity level	5
Example	IDENTITY/5/IDENTITY_CSV_IMPORT_FAILED: Failed to import identity user network-us?er1 to domain system-domain from the .csv file.
Explanation	Failed to import an identity user account from a .csv file and stopped importing remaining identity user accounts.
Recommended action	**122.** Make sure no identity user account with the same name exists on the device. **123.** Make sure the identity domain name or the identity username does not contain invalid characters.

IDENTITY_IMC_IMPORT_FAILED_NO_MEMORY

Message text	Failed to obtain data from IMC. Reason: Not enough memory.
Variable fields	N/A
Severity level	5
Example	IDENTITY/5/IDENTITY_IMC_IMPORT_FAILED_NO_MEMORY: Failed to obtain data from IMC. Reason: Not enough memory.
Explanation	Failed to import identity user accounts and online identity user information from the IMC server because of insufficient memory.
Recommended action	No action is required.

IDENTITY_LDAP_IMPORT_FAILED_NO_MEMORY

Message text	Failed to obtain data from the LDAP server specified in scheme [STRING]. Reason: Not enough memory.
Variable fields	$1: LADP scheme name.
Severity level	5
Example	IDENTITY/5/IDENTITY_LDAP_IMPORT_FAILED_NO_MEMORY: Failed to obtain data from the LDAP server specified in scheme test. Reason: Not enough memory.
Explanation	Failed to import identity users and identity groups from an LDAP server because of insufficient memory.
Recommended action	No action is required.

IDENTITY_LDAP_IMPORT_GROUP_FAILED

Message text	Failed to import identity group [STRING] to domain [STRING] from the LDAP server specified in scheme [STRING].
Variable fields	$1: Identity group name. $2: Identity domain name. $3: LADP scheme name.
Severity level	5
Example	IDENTITY/5/IDENTITY_LDAP_IMPORT_GROUP_FAILED: Failed to import identity group group-na?me1 to domain system-domain from the LDAP server specified in scheme ldap-scheme1.
Explanation	Failed to import an identity group from the LDAP server specified in an LDAP scheme.
Recommended action	**124.** Make sure no identity group with the same group name exists on the device. **125.** Make sure the identity domain name or the identity group name does not contain invalid characters.

IDENTITY_LDAP_IMPORT_USER_FAILED

Message text	Failed to import identity user [STRING] to domain [STRING] from the LDAP server specified in scheme [STRING].
Variable fields	$1: Identity username. $2: Identity domain name. $3: LADP scheme name.
Severity level	5
Example	IDENTITY/5/IDENTITY_LDAP_IMPORT_USER_FAILED: Failed to import identity user user-na?me1 to domain system-domain from the LDAP server specified in scheme ldap-scheme1.
Explanation	Failed to import an identity user from the LDAP server specified in an LDAP scheme.
Recommended action	**126.** Make sure no identity user with the same name exists on the device. **127.** Make sure the identity domain name or the identity username does not contain invalid characters.

IFNET messages

This section contains interface management messages.

IF_JUMBOFRAME_WARN

Message text	The specified size of jumbo frames on the aggregate interface [STRING] is not supported on the member port [STRING].
Variable fields	$1: Aggregate interface name. $2: Member port name.
Severity level	3
Example	IFNET/3/IF_JUMBOFRAME_WARN: -MDC=1-Slot=3; The specified size of jumbo frames on the aggregate interface Bridge-Aggregation1 is not supported on the member port GigabitEthernet1/0/1.
Explanation	Some member ports do not support the jumbo frame size configured on the aggregate interface.
Recommended action	**128.** Identity the value range for the jumbo frame size supported on member ports. **129.** Specify a jumbo frame size supported by member ports for the aggregate interface.

INTERFACE_NOTSUPPRESSED

Message text	Interface [STRING] is not suppressed.
Variable fields	$1: Interface name.
Severity level	6
Example	IFNET/6/INTERFACE_NOTSUPPRESSED: Interface GigabitEthernet1/0/1 is not suppressed.
Explanation	The interface changed from suppressed state to unsuppressed state. When the interface is unsuppressed, the upper-layer services can detect the physical state changes of the interface.
Recommended action	No action is required.

INTERFACE_SUPPRESSED

Message text	Interface [STRING] was suppressed.
Variable fields	$1: Interface name.
Severity level	5
Example	IFNET/5/INTERFACE_SUPPRESSED: Interface GigabitEthernet1/0/1 was suppressed.
Explanation	The interface was suppressed because its state frequently changed. When the interface is suppressed, the upper-layer services cannot detect the physical state changes of the interface.
Recommended action	**130.** Check whether the network cable of the interface or peer interface is frequently plugged and unplugged. **131.** Configure physical state change suppression to adjust the suppression parameters.

LINK_UPDOWN

	Message text	Line protocol state on the interface [STRING] changed to [STRING].
	Variable fields	$1: Interface name. $2: State of link layer protocol, which can be up or down.
	Severity level	5
	Example	IFNET/5/LINK_UPDOWN: Line protocol state on the interface GigabitEthernet1/0/1 changed to down.
	Explanation	The link layer protocol state changed on an interface.
	Recommended action	When the link layer protocol state of an interface is down, use the **display interface** command to display the link layer protocol state and locate the reason for which the link layer protocol state changed to down on the interface.

PFC_WARNING

	Message text	On interface [STRING], the rate of [STRING] PFC packets of 802.1p priority [INTEGER] exceeded the PFC early-warning threshold [INTEGER] pps. The current rate is [INTEGER].
	Variable fields	$1: Interface name. $2: Alarm direction, which can be input or output. $3: 802.1p priority. $4: Rate threshold at which the interface receives or sends PFC frames, in pps. $5: Rate at which the interface receives or sends PFC frames, in pps.
	Severity level	4
	Example	IFNET/4/PFC_WARNING: On interface GigabitEthernet1/0/1, the rate of input PFC packets of 802.1p priority 1 exceeded the PFC early-warning threshold 50 pps. The current rate is 60.
	Explanation	The rate at which the interface receives or sends PFC frames reaches the early-warning threshold.
	Recommended action	No action is required.

PHY_UPDOWN

Message text	Physical state on the interface [STRING] changed to [STRING].
Variable fields	$1: Interface name. $2: Link state, which can be up or down.
Severity level	3
Example	IFNET/3/PHY_UPDOWN: Physical state on the interface GigabitEthernet1/0/1 changed to down.
Explanation	The physical state changed on an interface.
Recommended action	When the interface is physically down, check whether a physical link is present or whether the link fails.

PROTOCOL_UPDOWN

Message text	Protocol [STRING] state on the interface [STRING] changed to [STRING].
Variable fields	$1: Protocol name. $2: Interface name. $3: Protocol state, which can be up or down.
Severity level	5
Example	IFNET/5/PROTOCOL_UPDOWN: Protocol IPX state on the interface GigabitEthernet1/0/1 changed to up.
Explanation	The state of a protocol has been changed on an interface.
Recommended action	When the state of a network layer protocol is down, check the network layer protocol configuration.

STORM_CONSTRAIN_BELOW

Message text	[STRING] is in controlled status, [STRING] flux falls below its lower threshold [STRING].
Variable fields	$1: Interface name. $2: Packet type, which can be BC, MC, or UC. $3: Lower suppression threshold: • *lowerlimit*% • *lowerlimit* pps • *lowerlimit* kbps
Severity level	1
Example	IFNET/1/STORM_CONSTRAIN_BELOW: GigabitEthernet1/0/1 is in controlled status, BC flux falls below its lower threshold 90%.
Explanation	The port is in controlled state. Any type of traffic on the port drops below the lower threshold from above the upper threshold.
Recommended action	No action is required.

STORM_CONSTRAIN_CONTROLLED

Message text	[STRING] turned into controlled status, port status is controlled, packet type is [STRING], upper threshold is [STRING].
Variable fields	$1: Interface name. $2: Packet type, which can be BC, MC, or UC. $3: Upper suppression threshold: • *upperlimit*% • *upperlimit* pps • *upperlimit* kbps
Severity level	1
Example	IFNET/1/STORM_CONSTRAIN_CONTROLLED: GigabitEthernet1/0/1 turned into controlled status, port status is controlled, packet type is BC, upper threshold is 90%.
Explanation	The port is in controlled state. Any type of traffic on the port exceeds the upper threshold.
Recommended action	No action is required.

STORM_CONSTRAIN_EXCEED

Message text	[STRING] is in controlled status, [STRING] flux exceeds its upper threshold [STRING].
Variable fields	$1: Interface name. $2: Packet type, which can be BC, MC, or UC. $3: Upper suppression threshold: • *upperlimit*% • *upperlimit* pps • *upperlimit* kbps
Severity level	1
Example	IFNET/1/STORM_CONSTRAIN_EXCEED: GigabitEthernet1/0/1 is in controlled status, BC flux exceeds its upper threshold 90%.
Explanation	The port is in controlled state. Any type of traffic on the port drops below the lower threshold from above the upper threshold.
Recommended action	No action is required.

STORM_CONSTRAIN_NORMAL

Message text	[STRING] returned to normal status, port status is [STRING], packet type is [STRING], lower threshold is [STRING].
Variable fields	$1: Interface name. $2: Packet type, which can be BC, MC, or UC. $3: Lower suppression threshold: • *lowerlimit*% • *lowerlimit* pps • *lowerlimit* kbps
Severity level	1
Example	IFNET/1/STORM_CONSTRAIN_NORMAL: GigabitEthernet1/0/1 returned to normal status, port status is normal, packet type is BC, lower threshold is 10%.
Explanation	The port is in normal state. Any type of traffic on the port drops below the lower threshold from above the upper threshold.
Recommended action	No action is required.

TUNNEL_LINK_UPDOWN

Message text	Line protocol state on the interface [STRING] changed to [STRING].
Variable fields	$1: Interface name. $2: Protocol state, which can be up or down.
Severity level	5
Example	IFNET/5/TUNNEL_LINK_UPDOWN: Line protocol state on the interface Tunnel1 changed to down.
Explanation	The link layer protocol state changed on a tunnel interface.
Recommended action	When the link layer protocol state of a tunnel interface is down, use the **display interface** command to display the link layer protocol state and locate the reason for which the link layer protocol state changed to down on the tunnel interface.

TUNNEL_PHY_UPDOWN

Message text	Physical state on the interface [STRING] changed to [STRING].
Variable fields	$1: Interface name. $2: Protocol state, which can be up or down.
Severity level	3
Example	IFNET/3/TUNNEL_PHY_UPDOWN: Physical state on the interface Tunnel1 changed to down.
Explanation	The link layer state changed on a tunnel interface.
Recommended action	When the interface is physically down, check whether a physical link is present or whether the link fails.

VLAN_MODE_CHANGE

Message text	Dynamic VLAN [INT32] has changed to a static VLAN.
Variable fields	$1: VLAN ID.
Severity level	5
Example	IFNET/5/VLAN_MODE_CHANGE: Dynamic VLAN 20 has changed to a static VLAN.
Explanation	Creating a VLAN interface for a VLAN cause the dynamic VLAN to become a static VLAN.
Recommended action	No action is required.

IKE messages

This section contains IKE messages.

IKE_P1_SA_ESTABLISH_FAIL

Message text	Failed to establish phase 1 SA in [STRING] mode [STRING] state. Reason: [STRING]. SA information: • Role: [STRING] • Local IP: [STRING] • Local ID type: [STRING] • Local ID: [STRING] • Local port: [UINT32] • Retransmissions: [UINT32] • Remote IP: [STRING] • Remote ID type: [STRING] • Remote ID: [STRING] • Remote port: [UINT32] • Recived retransmissions: [UINT32] • Inside VPN instance: [STRING] • Outside VPN instance: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING] • Connection ID: [UINT32] • Tunnel ID: [UINT32] • IKE profile name: [STRING]
Variable fields	$1: Negotiation mode: main or aggressive. $2: State of the negotiation state machine. $3: Failure reason: o Failed to verify the peer signature. o HASH payload is missing. o Failed to verify the peer HASH. Local HASH is %s. Peer HASH is %s. o Signature payload is missing. o Failed to get subject name from certificate. o Failed to get certificate. o Failed to get local certificate. o Failed to get private key. o Failed to verify the peer certificate (%s). o Failed to get ID data for constructing ID payload. o Invalid ID payload length: %d. o Invalid ID payload with protocol %u and port %u. o Invalid ID type (%u). o Unsupported attribute %u. o Attribute %s is repeated. o Unsupported DOI %s. o Unsupported IPsec DOI situation (%u). o KE payload is missing. o Invalid KE payload length (%lu). o Invalid nonce payload length (%lu). o No available proposal. o Failed to parse the Cert Request payload. o The proposal payload must be the last payload in the SA payload, but it is found followed by the %s payload. o Unexpected protocol ID (%u) found in proposal payload.

	◦ No transform payload in proposal payload. ◦ Transform number is not monotonically increasing. ◦ Invalid transform ID (%s). ◦ No acceptable transform. ◦ Unexpected %s payload in proposal. ◦ Invalid SPI length (%d) in proposal payload. ◦ Only one transform is permitted in one proposal, but %u transforms are found. ◦ Failed to find matching proposal in profile %s. ◦ Failed to find proposal %u in profile %s. ◦ Failed to find keychain %s in profile %s. ◦ Retransmission timeout. ◦ Incorrect configuration. ◦ Failed to construct certificate request payload. ◦ An error notification is received. ◦ Failed to add tunnel. $4: Role, initiator or responder. $5-$9: Information about the local end. $10-$14: Information about the remote end. $15: Inside VPN instance. $16: Outside VPN instance. $17-$18: Initiator cookie and responder cookie. $19: Connection ID. $20: IKE tunnel ID. The default is 4294967295. $21: IKE profile name.

Severity level	6
Example	IKE/6/IKE_P1_SA_ESTABLISH_FAIL: Failed to establish phase 1 SA in main mode IKE_P1_STATE_SEND1 state. Reason: Failed to get certificate. SA information: • Role: Initiator • Local IP: 4.4.4.4 • Local ID type: IPV4_ADDR • Local ID: 4.4.4.4 • Local port: 500 • Retransmissions: 0 • Remote IP: 4.4.4.5 • Remote ID type: IPV4_ADDR • Remote ID: 4.4.4.5 • Remote port: 500 • Recived retransmissions: 0 • Inside VPN instance: aaa • Outside VPN instance : bbb • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Connection ID: 1 • Tunnel ID: 1 • IKE profile name: abc
Explanation	IKE failed to establish a phase 1 SA. This message also displays the failure reason and information about the SA.
Recommended action	Verify the IKE configuration on the local and remote ends.

IKE_P1_SA_TERMINATE

Message text	The IKE phase 1 SA was deleted. Reason: [STRING]. SA information: • Role: [STRING] • Local IP: [STRING] • Local ID type: [STRING] • Local ID: [STRING] • Local port: [UINT32] • Retransmissions: [UINT32] • Remote IP: [STRING] • Remote ID type: [STRING] • Remote ID: [STRING] • Remote port: [UINT32] • Recived retransmissions: [UINT32] • Inside VPN instance: [STRING] • Outside VPN instance: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING] • Connection ID: [UINT32] • Tunnel ID: [UINT32] • IKE profile name: [STRING]
Variable fields	$1: Reason for the deletion: ◦ DPD timeout. ◦ New IKE SA had been negotiated, and the old one was deleted. ◦ The IKE SA was redundant. ◦ An IKE SA deletion message was received from peer. ◦ IKE keepalive timed out. ◦ The IKE SA expired. ◦ Delete IKE SA by connection-id. ◦ All IKE SAs were deleted. ◦ The IKE SA in the GDOI group was deleted. $2: Role, initiator or responder. $3-$7: Information about the local end. $8-$12: Information about the remote end. $13: Inside VPN instance. $14: Outside VPN instance. $15-$16: Initiator cookie and responder cookie. $17: Connection ID. $18: IKE tunnel ID. The default is 4294967295. $19: IKE profile name.
Severity level	6
Example	IKE/6/IKE_P1_SA_TERMINATE: The IKE phase 1 SA was deleted. Reason: DPD timeout. SA information: • Role: Responder • Local IP: 4.4.4.4

	• Local ID type: IPV4_ADDR • Local ID: 4.4.4.4 • Local port: 500 • Retransmissions: 0 • Remote IP: 4.4.4.5 • Remote ID type: IPV4_ADDR • Remote ID: 4.4.4.5 • Remote port: 500 • Recived retransmissions: 0 • Inside VPN instance: aaa • Outside VPN instance: bbb • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Connection ID: 1 • Tunnel ID: 1 • IKE profile name: abc
Explanation	The IKE SA established in phase 1 was deleted. This message also displays the deletion reason and information about the SA.
Recommended action	No action is required.

IKE_P2_SA_ESTABLISH_FAIL

Message text	Failed to establish phase 2 SA in [STRING] state. Reason: [STRING]. SA information: • Role: [STRING]. • Local address: [STRING]. • Remote address: [STRING]. • Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] • Dest addr: Protocol:[STRING] Port: [UINT32] Protocol: [STRING] • Inside VPN instance: [STRING]. • Outside VPN instance: [STRING]. • Inbound AH SPI: [STRING] • Outbound AH SPI: [STRING] • Inbound ESP SPI: [STRING] • Outbound ESP SPI: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING]. • Message ID: [STRING]. • Connection ID: [UINT32]. • Tunnel ID: [UINT32].
Variable fields	$1: State of the negotiation state machine. $2: Failure reason: o Failed to construct ID payload. o Failed to calculate %s. o Failed to validate %s. o Failed to compute key material. o Incorrect configuration. o Failed to switch IPsec SA. o The nonce payload doesn't exist. o Invalid nonce payload length (%lu). o No valid DH group description in SA payload. o The KE payload doesn't exist. o Too many KE payloads. o The length of the KE payload doesn't match the DH group description. o Failed to send message to IPsec when getting SP. o Failed to send message to IPsec when getting SPI. o Failed to add phase 2 SA. o Retransmission of phase 2 packet timed out. o Collision detected in phase 2 negotiation. o No matching proposal found between the local and remote ends. o Transform number is not monotonically increasing. o Proposal payload has more transforms than specified in the proposal payload. o Proposal payload has less transforms than specified in the proposal payload. o Attribute %d is repeated in IPsec transform %d. o SA_LIFE_TYPE attribute is repeated in packet. o The SA_LIFE_TYPE attribute must be in front of the SA_LIFE_DURATION attribute. o Unsupported IPsec attribute %s. o The encapsulation mode must be specified in the IPsec transform set.

	○ Invalid SPI length (%u) in IPsec proposal. ○ Invalid SPI (%u) in IPsec proposal. ○ The Transform ID (%d) in transform %d doesn't match authentication algorithm %s (%u). ○ Failed to get SPI from proposal. ○ No transform in IPsec proposal. ○ A proposal payload contains more than one AH proposal. ○ Invalid next payload (%u) in proposal. ○ No ESP or AH proposal. ○ Unsupported DOI. ○ Unsupported IPsec DOI situation (%u). ○ Invalid IPsec proposal %u. ○ Failed to get IPsec policy when renegotiating IPsec SA. ○ Failed to get IPsec policy as phase 2 responder. $3: Role, initiator or responder. $4: Local IP address. $5: Remote IP address. $6-$11: Data flow-related parameters. $12: Inside VPN instance. $13: Outside VPN instance. $14: Inbound AH SPI. $15: Outbound AH SPI. $16: Inbound ESP SPI. $17: Outboundd ESP SPI. $18-$19: Initiator cookie and responder cookie. $20: Message ID. $21: Connection ID. $22: IKE tunnel ID. The default is 4294967295.

Severity level	6
Example	IKE/6/IKE_P2_SA_ESTABLISH_FAIL: Failed to establish phase 2 SA in IKE_P2_STATE_GETSPI state. Reason: Failed to get SPI from proposal. SA information: • Role: Responder • Local address: 2.2.2.2 • Remote address: 1.1.1.1 • Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP • Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP • Inside VPN instance: aaa • Outside VPN instance: bbb • Inbound AH SPI: 192365458 • Outbound AH SPI: 13654581 • Inbound ESP SPI: 292334583 • Outbound ESP SPI: 5923654586 • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Message ID: 0xa2b11c8e • Connection ID: 1 • Tunnel ID: 1
Explanation	IKE failed to establish a phase 2 SA. This message also displays the failure reason and information about the SA.
Recommended action	Verify the IKE and IPsec configurations on the local and remote ends.

IKE_P2_SA_TERMINATE

Example	The IKE phase 2 SA was deleted. Reason: [STRING]. SA information: • Role: [STRING] • Local address: [STRING] • Remote address: [STRING] • Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] • Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] • Inside VPN instance: [STRING] • Outside VPN instance: [STRING] • Inbound AH SPI: [STRING] • Outbound AH SPI: [STRING] • Inbound ESP SPI: [STRING] • Outbound ESP SPI: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING] • Message ID: [STRING] • Connection ID: [UINT32] • Tunnel ID: [UINT32]
Variable fields	$1: Reason for the deletion: o The SA expired. o An IPsec SA deletion message was received from peer. o New P2 SA had been negotiated, and the old one was deleted. o All P2 SAs were deleted. o The P2 SA was deleted by SPID. o The P2 SA was deleted by IFIndex. o The P2 SA was deleted by SA index. $2: Role, initiator or responder. $3: Local IP address. $4: Remote IP address. $5-$10: Data flow-related parameters. $11: Inside VPN instance. $12: Outside VPN instance. $13: Inbound AH SPI. $14: Outbound AH SPI. $15: Inbound ESP SPI. $16: Outboundd ESP SPI. $17-$18: Initiator cookie and responder cookie. $19: Message ID. $20: Connection ID. $21: IKE tunnel ID. The default is 4294967295.
Severity level	6
Example	IKE/6/IKE_P2_SA_TERMINATE: The IKE phase 2 SA was deleted. Reason: An IPsec SA deletion message was received.

Example	The IKE phase 2 SA was deleted. Reason: [STRING]. SA information: • Role: [STRING] • Local address: [STRING] • Remote address: [STRING] • Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] • Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] • Inside VPN instance: [STRING] • Outside VPN instance: [STRING] • Inbound AH SPI: [STRING] • Outbound AH SPI: [STRING] • Inbound ESP SPI: [STRING] • Outbound ESP SPI: [STRING] • Initiator Cookie: [STRING] • Responder Cookie: [STRING] • Message ID: [STRING] • Connection ID: [UINT32] • Tunnel ID: [UINT32]
	SA information: • Role: Responder • Local address: 2.2.2.2 • Remote address: 1.1.1.1 • Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP • Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP • Inside VPN instance: aaa • Outside VPN instance: bbb • Inbound AH SPI: 192365458 • Outbound AH SPI: 13654581 • Inbound ESP SPI: 292334583 • Outbound ESP SPI: 5923654586 • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Message ID: 0xa2b11c8e • Connection ID: 1 • Tunnel ID: 1
Explanation	An IKE phase 2 SA was deleted. This message also displays the deletion reason and information about the SA.
Recommended action	No action is required.

IKE_XAUTH_FAILE

Example	Failed to pass extended authentication in [STRING] mode [STRING] state. Reason: [STRING]. SA information: • Role: [STRING]. • Local IP: [STRING]. • Local ID type: [STRING]. • Local ID: [STRING]. • Local port: [UINT32]. • Retransmissions: [UINT32] • Remote IP: [STRING]. • Remote ID type: [STRING]. • Remote ID: [STRING]. • Remote port: [UINT32]. • Recived retransmissions: [UINT32] • Inside VPN instance: [STRING]. • Outside VPN instance: [STRING]. • Initiator Cookie: [STRING] • Responder Cookie: [STRING]. • Message ID: [STRING]. • Connection ID: [UINT32]
Variable fields	$1: Negotiation mode: main or aggressive. $2: State of the negotiation state machine. $3: Failure reason: ◦ Failed to verify the HASH payload. ◦ Failed to parse the attribute payload. $4: Role, initiator or responder. $5-$9: Information about the local end. $10-$14: Information about the remote end. $15: Inside VPN instance. $16: Outside VPN instance. $17-$18: Initiator cookie and responder cookie. $19: Message ID. $20: Connection ID.
Severity level	6
Example	IKE/6/IKE_XAUTU_FAILE: Failed to pass extended authentication, in main mode IKE_XAUTH_STATE_SET state. Reason: Failed to parse the attribute payload. SA information: • Role: Initiator • Local IP: 4.4.4.4 • Local ID type: IPV4_ADDR • Local ID: 4.4.4.4 • Local port: 500 • Retransmissions: 0 • Remote IP: 4.4.4.5 • Remote ID type: IPV4_ADDR

Example	Failed to pass extended authentication in [STRING] mode [STRING] state. Reason: [STRING]. SA information: • Role: [STRING]. • Local IP: [STRING]. • Local ID type: [STRING]. • Local ID: [STRING]. • Local port: [UINT32]. • Retransmissions: [UINT32] • Remote IP: [STRING]. • Remote ID type: [STRING]. • Remote ID: [STRING]. • Remote port: [UINT32]. • Recived retransmissions: [UINT32] • Inside VPN instance: [STRING]. • Outside VPN instance: [STRING]. • Initiator Cookie: [STRING] • Responder Cookie: [STRING]. • Message ID: [STRING]. • Connection ID: [UINT32]
	• Remote ID: 4.4.4.5 • Remote port: 500 • Recived retransmissions: 0 • Inside VPN instance: aaa • Outside VPN instance: bbb • Initiator Cookie: 4a42af47dbf0b2b1 • Responder Cookie: 8f8c1ff6645efbaf • Message ID: 0xa2b11c8e • Connection ID: 1
Explanation	Extended authentication failed. This message also displays the failure reason and information about the SA.
Recommended action	No action is required.

IMA

This section contains Integrity Measurements Architecture (IMA) messages.

IMA_ALLOCATE_FAILED

Message text	Failed to allocate resource for file [STRING].
Variable fields	$1: Name of the file of which you want to measure the integrity.
Severity level	4
Example	IMA/4/IMA_ALLOCATE_FAILED: Failed to allocate resource for file /sbin/tcsmd.
Explanation	IMA failed to allocate resources to the specified file.
Recommended action	Contact NSFOCUS Support.

IMA_DATA_ERROR

Message text	Can't collect data of file [STRING].
Variable fields	$1: Name of the file of which you want to measure the integrity.
Severity level	4
Example	IMA/4/IMA_DATA_ERROR: Can't collect data of file /sbin/tcsmd.
Explanation	IMA failed to open the specified file, read data from the file, or compute the hash value of the file.
Recommended action	Contact NSFOCUS Support.

IMA_FILE_HASH_FAILED

Message text	Hash value of file [STRING] is not consistent with that in the RM file.
Variable fields	$1: Name of the file of which you want to measure the integrity.
Severity level	4
Example	IMA/4/IMA_FILE_HASH_FAILED: Hash value of file /sbin/tcsmd is not consistent with that in the RM file.
Explanation	The computed hash value of the specified file is different from the hash value of the file stored in the RM file. The specified file is not trustworthy.
Recommended action	Contact NSFOCUS Support.

IMA_RM_FILE_MISS

Message text	File [STRING] is missing in the RM file.
Variable fields	$1: Name of the file of which you want to measure the integrity.
Severity level	4
Example	IMA/4/IMA_RM_FILE_MISS: File /sbin/tcsmd is missing in the RM file.
Explanation	IMA did not find information about the specified file in the RM file.
Recommended action	Contact NSFOCUS Support.

IMA_RM_HASH_MISS

Message text	Hash value of file [STRING] is missing in the RM file.
Variable fields	$1: Name of the file of which you want to measure the integrity.
Severity level	4
Example	IMA/4/IMA_RM_HASH_MISS: Hash value of file /sbin/tcsmd is missing in the RM file.
Explanation	IMA did not find the hash value of the specified file in the RM file. The hash algorithm used for integrity measurement of the specified file might not be supported in the RM.
Recommended action	Contact NSFOCUS Support.

IMA_TEMPLATE_ERROR

Message text	Failed to extend template hash value of file [STRING] to the PCR.
Variable fields	$1: Name of the file of which you want to measure the integrity.
Severity level	4
Example	IMA/4/IMA_TEMPLATE_ERROR: Failed to extend template hash value of file /sbin/tcsmd to the PCR.
Explanation	IMA failed to extend the template hash value of the specified file to the PCRs.
Recommended action	Contact NSFOCUS Support.

Introduction

This document includes the following system messages:

- Messages specific to Release xxx of the device.
- Messages for the NF software platform version based on which Release xxx was produced. Some platform system messages might not be available on the device.

This document is intended only for managing xxx. Do not use this document for any other device models.

This document assumes that the readers are familiar with data communications technologies and NSFOCUS networking products.

System log message format

By default, the system log messages use one of the following formats depending on the output destination:

- Log host (RFC 3164-compliant format):

  ```
  <PRI>TIMESTAMP Sysname %%vendorMODULE/severity/MNEMONIC: location; CONTENT
  ```

- Destinations except for the log host:

  ```
  Prefix TIMESTAMP Sysname MODULE/severity/MNEMONIC: CONTENT
  ```

NOTE:

Log message examples in this document use the format for destinations except the log host. They do not contain elements available only for the log host, including the location element.

Table 2 System log message elements

Element	Description
<PRI>	Priority identifier. This element is contained only in messages sent to the log host. It is calculated by using the following formula: *Priority identifier=facilityx8+severity* Where: • Facility is specified by using the **info-center loghost** command. A log host uses this parameter to identify log sources and filter log messages. • Severity represents the importance of the message. For more information about severity levels, see Table 3.
Prefix	Message type identifier. This element is contained only in the messages sent to non-log-host destinations. This element uses the following symbols to indicate message severity: • **Percentage sign (%)**—Informational and higher levels. • **Asterisk (*)**—Debug level.
TIMESTAMP	Date and time when the event occurred. The following are commands for configuring the timestamp format: • **Log host**—Use the **info-center timestamp loghost** command. • **Non-log-host destinations**—Use the **info-center timestamp** command.
Sysname	Name or IP address of the device that generated the message.
%%vendor	Manufacturer flag. This element is **%%10** for NSFOCUS. This element is contained only in messages sent to the log host.
MODULE	Name of the module that produced the message.
severity	Severity level of the message. (For more information about severity levels, see Table 3.)
MNEMONIC	Text string that uniquely identifies the system message. The maximum length is 32 characters.

Element	Description
location	Optional. This element identifies where the message occurred. This element is contained only in messages sent to the log host. This element presents location information about the message in the following format: *-attribute1=x-attribute2=y…-attributeN=z* The following are examples of location attributes: • -MDC=XX, which represents the MDC on which the message occurred. • -DevIp=XXX.XXX.XXX.XXX, which represents the source IP of the message. • -Slot=XX, which represents the slot on which the message occurred. • -Chassis=XX-Slot=XX, which represent the chassis and slot on which the message occurred. This element is separated from the CONTENT element by using a semicolon (;).
CONTENT	A description of the event or error. For variable fields in this element, this document uses the representations in Table 4.

System log messages are classified into eight severity levels from 0 to 7. The lower the number, the higher the severity.

Table 3 System log message severity levels

Level	Severity	Description
0	Emergency	The system is unusable. For example, the system authorization has expired.
1	Alert	Action must be taken immediately. For example, traffic on an interface exceeds the upper limit.
2	Critical	Critical condition. For example, the device temperature exceeds the upper limit, the power module fails, or the fan tray fails.
3	Error	Error condition. For example, the link state changes or a storage card is unplugged.
4	Warning	Warning condition. For example, an interface is disconnected, or the memory resources are used up.
5	Notification (Notice in RFC 3164)	Normal but significant condition. For example, a terminal logs in to the device, or the device reboots.
6	Informational	Informational message. For example, a command or a ping operation is executed.
7	Debug	Debugging message.

For variable fields in the message text, this document uses the representations in Table 4. The values are case insensitive, even though the representations are uppercase letters.

Table 4 Variable field representations

Representation	Information type
INT16	Signed 16-bit decimal number.

Representation	Information type
UINT16	Unsigned 16-bit decimal number.
INT32	Signed 32-bit decimal number.
UINT32	Unsigned 32-bit decimal number.
INT64	Signed 64-bit decimal number.
UINT64	Unsigned 64-bit decimal number.
DOUBLE	Two dot-separated signed 32-bit decimal numbers. The format is [INTEGER].[INTEGER].
HEX	Hexadecimal number.
CHAR	Single character.
STRING	Character string.
IPADDR	IP address.
MAC	MAC address.
DATE	Date.
TIME	Time.

Fast log message format

Log header formats

Table 5 shows the log header formats.

Table 5 Log header formats

Log type	Format	Example
Standard logs	`<PRI> Timestamp AppName %%10 SN:sn VsysId:id`	`<134> Apr 28 15:35:32 2020 NSFOCUS %%10 SN:10056879 VsysId:1`
Custom logs	**URL filtering Unicom format**: `PRI Vision HostName Timestamp AppName MsgID HostName Len`	`142 1 100.0.0.1 2020 Apr 28 15:35:43 NSFOCUS NAT444:SessionU 57`
	NAT CMCC format: `<PRI> Vision HostName Timestamp AppName ProcID MsgID`	`<142> 1 100.0.0.1 2020 Apr 28 15:35:32 NSFOCUS - NAT444:SessionA`
	NAT Unicom format: `<PRI> Vision HostName Timestamp AppName ProcID MsgID`	`<142> 1 100.0.0.1 2020 Apr 28 15:35:43 NSFOCUS - NAT444:SessionA`
	NAT Telecom format: `<PRI> Vision Timestamp HostName AppName ProcID MsgID`	`<134> 1 2020 Apr 28 15:35:38 100.0.0.1 NSFOCUS - NAT444:sessionbasedA`

Log field description

Table 6 displays descriptions of log fields in the header and content.

Table 6 Log field description

Field	Description
PRI	Log type code, The value is fixed to 134 for standard and NAT Telecom logs, and is fixed to 142 for URL filtering Unicom, NAT CMCC, and NAT Unicom logs.
Timestamp	Time when the log was generated. The timestamp format is *YYYY Mon DD hh:mm:ss*.
AppName	Name of the device that generated the log.
%%10	Vendor of the device.
SN	Serial number of the device. This field is available only after you execute the **customlog with-sn** command. You can obtain the device SN in the **DEVICE_SERIAL_NUMBER** field from the output of the **display device manuinfo** command.
VsysId	ID of the virtual system that generated the log.
HostName	Source IP address of the log.
MsgID	Log message type.
Len	Total length of the log header, in bytes.
ProcID	Reserved field. This field displays a hyphen (-).

Managing and obtaining system log messages

You can manage system log messages by using the information center.

By default, the information center is enabled. Log messages can be output to the console, monitor terminal, log buffer, log host, and log file.

To filter log messages, use the **info-center source** command to specify log output rules. A log output rule specifies the source modules and the lowest severity level of log messages that can be output to a destination. A log message is output if its severity level is higher than or equal to the specified level. For example, if you specify a severity level of 6 (informational), log messages that have a severity level from 0 to 6 are output.

For more information about using the information center, see the network management and monitoring configuration guide for the product.

Obtaining log messages from the console terminal

Access the device through the console port. Real-time log messages are displayed on the console terminal.

Obtaining log messages from a monitor terminal

Monitor terminals refer to terminals that access the device through the AUX, VTY, or TTY lines (for example, Telnet). To obtain log messages from a monitor terminal, use the following guidelines:

- To display log messages on the monitor terminal, you must configure the **terminal monitor** command.
- For monitor terminals, the lowest level of log messages that can be displayed is determined by both the **terminal logging level** and **info-center source** commands.

NOTE:

Settings for the **terminal monitor** and **terminal logging level** commands take effect only on the current login session. The default settings for the commands restore at a relogin.

Obtaining log messages from the log buffer

Use the **display logbuffer** command to display history log messages in the log buffer.

Obtaining log messages from the log file

By default, the log file feature automatically saves logs from the log file buffer to the log file every 24 hours. You can use the **info-center logfile frequency** command to change the automatic saving internal.

To manually save logs to the log file, use the **logfile save** command. The log file buffer is cleared each time a save operation is performed.

By default, you can obtain the log file from the **cfa0:/logfile/** path if the CF card is not partitioned. If the CF card is partitioned, the file path is **cfa1:/logfile/**.

To view the contents of the log file on the device, use the **more** command.

Obtaining log messages from a log host

Use the **info-center loghost** command to specify the service port number and IP address of a log host. To specify multiple log hosts, repeat the command.

For a successful log message transmission, make sure the specified port number is the same as the port number used on the log host. The default service port number is 514.

Software module list

Table 7 lists all software modules that might produce system log messages. This document uses "OPENSRC" to represent all open source modules.

Table 7 Software module list

Module name representation	Module name expansion
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
ADVPN	Auto Discovery Virtual Private Network
AFT	Address Family Translation
ANCP	Access Node Control Protocol
ANTIVIRUS	Anti-virus
APMGR	Access Point Management
APR	Application Recognition
ARP	Address Resolution Protocol
ASPF	Advanced Stateful Packet Filter
ATK	Attack Detection and Prevention

Module name representation	Module name expansion
ATM	Asynchronous Transfer Mode
AUDIT	Audit
AUTOCFG	Automatic configuration
AVC	Application Visibility Control
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BLS	Blacklist
CC	Challenge Collapsar Defense
CFD	Connectivity Fault Detection
CFGLOG	Configuration log
CFGMAN	Configuration Management
CGROUP	Collaboration Group
CONNLMT	Connection Limit
CONTEXT	Context
DAC	Data Analysis Center
DEV	Device Management
DFILTER	Data Filter
DHCP	Dynamic Host Configuration Protocol
DHCPS	DHCP Server
DHCPS6	DHCPv6 Server
DHCPSP4	DHCP Snooping
DHCPSP6	DHCPv6 Snooping
DIAG	Diagnosis
DIM	DPI Engine
DLDP	Device Link Detection Protocol
DOT1X	802.1X
EDEV	Extended-Device Management
EIGRP	Enhanced Interior Gateway Routing Protocol
ERPS	Ethernet Ring Protection Switching
ETHOAM	Ethernet Operation, Administration and Maintenance
EVB	Edge Virtual Bridging
EVIISIS	Ethernet Virtual Interconnect Intermediate System-to-Intermediate System
FCLINK	Fibre Channel Link
FCOE	Fibre Channel Over Ethernet
FCZONE	Fibre Channel Zone
FFILTER	File Filter

Module name representation	Module name expansion
FILTER	Filter
FIPSNG	FIP Snooping
FS	File System
FTP	File Transfer Protocol
GLB	Global Load Balancing
gRPC	Google Remote Procedure Call
HA	High Availability
HQOS	Hierarchical QoS
HTTPD	Hypertext Transfer Protocol Daemon
IDENTITY	Identity
IFNET	Interface Net Management
IKE	Internet Key Exchange
IMA	Integrity Measurements Architecture
IP6ADDR	IPv6 Addressing
IPADDR	IP Addressing
IPOE	IP over Ethernet
IPREPUTATION	IP Reputation
IPS	Intrusion Prevention System
IPSEC	IP Security
IPSG	IP Source Guard
IRDP	ICMP Router Discovery Protocol
IRF	Intelligent Resilient Framework
ISIS	Intermediate System-to-Intermediate System
ISSU	In-Service Software Upgrade
KDNS	Kernel Domain Name System
KHTTP	Kernel Hypertext Transfer Protocol
L2PT	Layer 2 Protocol Tunneling
L2TPV2	Layer 2 Tunneling Protocol Version 2
L2VPN	Layer 2 VPN
LAGG	Link Aggregation
LB	Load Balancing
LDP	Label Distribution Protocol
LIPC	Leopard Inter-process Communication
LLDP	Link Layer Discovery Protocol
LOAD	Load Management
LOGIN	Login
LPDT	Loopback Detection

Module name representation	Module name expansion
LS	Local Server
LSPV	LSP Verification
MAC	Media Access Control
MACA	MAC Authentication
MACSEC	MAC Security
MBFD	MPLS BFD
MBUF	Memory Buffer
MDC	Multitenant Device Context
MFIB	Multicast Forwarding Information Base
MGROUP	Mirroring Group
MPLS	Multiprotocol Label Switching
MTLK	Monitor Link
NAT	Network Address Translation
ND	Neighbor Discovery
NETCONF	Network Configuration Protocol
NETSHARE	NetShare Control
NQA	Network Quality Analyzer
NTP	Network Time Protocol
OBJP	Object Policy
OFP	OpenFlow Protocol
OPTMOD	Optical Module
OPENSRC(RSYNC)	Open Source (Remote Synchronization)
OSPF	Open Shortest Path First
OSPFV3	Open Shortest Path First Version 3
PBB	Provider Backbone Bridge
PBR	Policy-Based Routing
PCAPWARE	Packet Capture Wireshark
PCE	Path Computation Element
PEX	Port Extender
PFILTER	Packet Filter
PHYD	Physical Detection
PIM	Protocol Independent Multicast
PING	Packet Internet Groper
PKI	Public Key Infrastructure
PKT2CPU	Packet to CPU
PKTCPT	Packet Capture
PORTAL	Portal

Module name representation	Module name expansion
PORTSEC	Port Security
POSA	Point Of Sales
PPP	Point to Point Protocol
PREPROVISION	Preprovision
PTS	Platform Trust Services
PWDCTL	Password Control
QOS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RBM	Remote Backup Management
RDDC	Redundancy
RIP	Routing Information Protocol
RIPNG	Routing Information Protocol Next Generation
RM	Routing Management
RPR	Resilient Packet Ring
RRPP	Rapid Ring Protection Protocol
RTM	Real-Time Event Manager
SANDBOX	Sandbox
SCD	Server Connection Detection
SCM	Service Control Manager
SCRLSP	Static CRLSP
SECDIAG	Security Diagnose
SECP	Security Policy
SESSION	Session
SFLOW	Sampler Flow
SHELL	Shell
SLSP	Static LSP
SMLK	Smart Link
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSHC	Secure Shell Client
SSHS	Secure Shell Server
SSL VPN	Secure Sockets Layer Virtual Private Network
STAMGR	Station Management
STM	Stack Topology Management
STP	Spanning Tree Protocol
SYSEVENT	System Event
SYSLOG	System Log

Module name representation	Module name expansion
TAC	Trusted Access Control
TACACS	Terminal Access Controller Access Control System
TCSM	Trusted Computing Services Management
TELNETD	Telnet Daemon
TERMINAL	Terminal Identification
TRILL	Transparent Interconnect of Lots of Links
UDPI	User DPI
UFLT	URL Filter
VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol
VSRP	Virtual Service Redundancy Protocol
VXLAN	Virtual eXtensible LAN
WEB	Web
WEBCACHE	Web Cache
WFF	WLAN Fast Forwarding
WIPS	Wireless Intrusion Prevention System
WLANAUD	WLAN Audit
WMESH	WLAN Mesh
WRDC	Wireless Roaming Data Center
WSA	Wireless Spectrum Analysis

Using this document

This document categorizes system log messages by software module. The modules are ordered alphabetically. Except for OPENSRC, the system log messages for each module are listed in alphabetic order of their mnemonic names. The OPENSRC messages are unordered because they use the same mnemonic name (SYSLOG). For each OPENSRC message, the section title uses a short description instead of the mnemonic name.

This document explains messages in tables. Table 8 describes information provided in these tables.

Table 8 Message explanation table contents

Item	Content	Example
Message text	Presents the message description.	ACL [UINT32] [STRING] [UINT64] packet(s).
Variable fields	Briefly describes the variable fields in the order that they appear in the message text. The variable fields are numbered in the "$*Number*" form to help you identify their location in the message text.	$1: ACL number. $2: ID and content of an ACL rule. $3: Number of packets that matched the rule.
Severity level	Provides the severity level of the message.	6
Example	Provides a real message example. The	ACL/6/ACL_STATIS_INFO: ACL 2000

Item	Content	Example
	examples do not include the "<PRI>TIMESTAMP Sysname %%vendor" part or the "Prefix TIMESTAMP Sysname" part, because information in this part varies with system settings.	rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
Explanation	Explains the message, including the event or error cause.	Number of packets that matched an ACL rule. This message is sent when the packet counter changes.
Recommended action	Provides recommended actions. For informational messages, no action is required.	No action is required.

IP6ADDR messages

This section contains IPv6 addressing messages.

IP6ADDR_CREATEADDRESS_ERROR

Message text	Failed to create an address by the prefix. Reason: [STRING] on [STRING] and [STRING] on [STRING] overlap.
Variable fields	$1: IPv6 prefix. $2: Interface name. $3: IPv6 prefix. $4: Interface name.
Severity level	4
Example	IP6ADDR/4/IP6ADDR_CREATEADDRESS_ERROR: Failed to create an address by the prefix. Reason: 2001::/ 64 on GigabitEthernet1/0/2 and 2001::/64 on GigabitEthernet1/0/1 overlap.
Explanation	The device failed to use a prefix to generate an IPv6 address for an interface because the prefixes overlapped on this interface and another interface.
Recommended action	Cancel the IPv6 address configuration on the conflicting interface and configure the interface to generate an IPv6 address by using a different prefix.

IPADDR messages

This section contains IP addressing messages.

IPADDR_HA_EVENT_ERROR

Message text	A process failed HA upgrade because [STRING].
Variable fields	$1: HA upgrade failure reason: o IPADDR failed the smooth upgrade. o IPADDR failed to reupgrade to the master process. o IPADDR stopped to restart the timer. o IPADDR failed to upgrade to the master process. o IPADDR failed to restart the upgrade. o IPADDR failed to add the unicast object to the master task epoll. o IPADDR failed to create an unicast object. o IPADDR role switchover failed when the standby process switched to the master process. o IPADDR switchover failed when the master process switched to the standby process. o IPADDR HA upgrade failed. o IPADDR failed to set the interface filtering criteria. o IPADDR failed to register interface events. o IPADDR failed to subscribe port events. o IPADDR failed to add a VPN port event to the master epoll. o IRDP failed to open DBM. o IRDP failed to initiate a connection to the device management module. o IRDP failed to add the master task epoll with the handle used to connect to the device management module. o IRDP failed to register device management events. o IRDP failed to subscribe port events. o IRDP failed to add the master task epoll with the handle used to subscribe port events. o IRDP failed to set the interface filtering criteria. o IRDP failed to register interface events. o IRDP failed to register network events. o IRDP failed to create the interface control block storage handle. o IRDP failed to create the timer. o IRDP failed to add the master task epoll with the handle used to create the timer. o IRDP failed to set the schedule time for the timer. o IRDP failed to set the timer to unblocked status. o IRDP failed to create a timer instance.
Severity level	4
Example	IPADDR/4/IPADDR_HA_EVENT_ERROR: A process failed HA upgrade because IPADDR failed the smooth upgrade.
Explanation	A process failed HA upgrade and the message was sent to show the failure reason.
Recommended action	Please contact NSFOCUS Support.

IPADDR_HA_STOP_EVENT

Message text	The device received an HA stop event.
Variable fields	None.
Severity level	4
Example	IPADDR/4/IPADDR_HA_STOP_EVENT: The device received an HA stop event.
Explanation	This message is sent when the device receives an HA stop event.
Recommended action	Please contact NSFOCUS Support.

IPoE messages

This section contains IPoE messages.

IPoE_USER_LOGON_SUCCESS

Message text	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]; The user came online successfully.
Variable fields	$1: Username. $2: IP address. $3: Interface name. $4: Outer VLAN ID. $5: Inner VLAN ID. $6: MAC address.
Severity level	6
Example	IPOE/6/ IPOE_USER_LOGON_SUCCESS: -UserName=user1-IPAddr=1.1.0.1-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-FFFF; The user came online successfully.
Explanation	The user has come online successfully.
Recommended action	No action is required.

IPoE_USER_LOGON_FAILED

Message text	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; The user failed to come online.
Variable fields	$1: Username. $2: IP address. $3: Interface name. $4: Outer VLAN ID. $5: Inner VLAN ID. $6: MAC address. $7: Cause (see Table 9).
Severity level	6
Example	IPOE/6/IPOE_USER_LOGON_FAILED: -UserName=user1-IPAddr=N/A-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-FFFF-Reason=Authentication failed ; The user failed to come online.
Explanation	The user failed to come online.
Recommended action	See Table 9.

Table 9 Causes and recommended actions

Cause	Description	Recommended action
Authentication failed	N/A	**132.** Verify that the device communicates with the authentication server correctly. **133.** Verify that the username is correct. **134.** Verify that the password is correct. **135.** Verify that the authentication domain on the device is correct.
Authorization failed	N/A	**136.** Verify that the device communicates with the authorization server correctly. **137.** Verify that the authorization attributes deployed by the authorization server exist on the device and are configured correctly. **138.** Verify that the device supports the authorization attributes deployed by the authorization server.

IPoE_USER_LOGOFF_NORMAL

Message text	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; The user logged off.
Variable fields	$1: Username. $2: IP address. $3: Interface name. $4: Outer VLAN ID. $5: Inner VLAN ID. $6: MAC address. $7: Cause (see Table 10).
Severity level	6
Example	IPOE/6/IPOE_USER_LOGOFF_NORMAL: -UserName=user1-IPAddr=1.1.0.1-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-FFFF-Reason=DHCP user request; The user logged off.
Explanation	The user has gone offline normally.
Recommended action	See Table 10.

Table 10 Causes and recommend actions

Cause	Description	Recommended action
DHCP user request	The user requested to go offline.	Identify whether the user has gone offline.

IPoE_USER_LOGOFF_ABNORMAL

Message text	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; The user logged off abnormally.
Variable fields	$1: Username. $2: IP address. $3: Interface name. $4: Outer VLAN ID. $5: Inner VLAN ID. $6: MAC address. $7: Cause (see Table 11).
Severity level	6
Example	IPOE/6/IPOE_USER_LOGOFF_ABNORMAL: -UserName=user1-IPAddr=1.1.0.1-IfName=Bas-interface0-OuterVLAN=N/A-InnerVLAN=N/A-MACAddr=FFFF-FFFF-Reason=Session timeout; The user logged off abnormally.
Explanation	The user has gone offline abnormally.
Recommended action	See Table 11.

Table 11 Causes and recommend actions

Cause	Description	Recommended action
Admin reset	The access interface went down, and the dynamic IPoE sessions or the static IPoE sessions were deleted.	**139.** Identify whether the access interface has gone down. **140.** Identify whether the **reset ip subscriber session** command has been executed to delete the dynamic IPoE sessions. **141.** Identify whether the **undo ip subscriber session static** command has been executed to delete the static IPoE sessions. **142.** Identify whether new static users are added. **143.** Identify whether IPoE has been disabled by using the **undo ip subscriber { l2-connected | routed } enable** command.
Session timeout	The user session timed out or the traffic quota was used up.	Notify the user that the user session timed out or to renew the user account.

Cause	Description	Recommended action
Session idle cut	The user traffic did not reach the threshold within the specified period.	Identify whether the user has gone offline.
DHCP lease timeout	N/A.	Notify the user that the address lease has expired.
DHCP notify	The DHCP module notified the user to go offline.	Identify whether the user has gone offline.
User online detection failure	N/A.	Identify whether the user has gone offline.
AAA request	The RADIUS server requested the user to go offline.	No action is required.
Insufficient hardware resources	N/A.	Save the related log information locally and contact the support.
Interface down	N/A.	Verify that the network cable of the user access interface is correctly connected.
Interface shutdown	N/A.	Identify whether the **shutdown** command has been executed on the user access interface.
VSRP status change	N/A.	Identify whether the user has gone offline.
BRAS errors	The BRAS software errors caused the user to go offline.	**144.** Collect debugging information about the user login process by executing the following commands in sequence: ○ **terminal monitor** ○ **terminal debugging** ○ **debugging ip subscriber** **145.** Save the related log and debugging information locally and contact the support.

IPS messages

This section contains IPS messages through fast log output and syslog output.

IPS_IPV4_INTERZONE (syslog)(fast log)

Message text	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPAddr(1003)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPAddr(1007)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; AttackName(1088)=[STRING]; AttackID(1089)=[UINT32]; Category(1090)=[STRING]; Protection(1091)=[STRING]; SubProtection(1092)=[STRING]; Severity(1087)=[STRING]; Action(1053)=[STRING]; CVE(1075)=[STRING]; BID(1076)=[STRING]; MSB(1077)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; SubCategory(1124)=[STRING]; LoginUserName(1177)=[STRING]; LoginPwd(1178)=[STRING]; CapturePktName(1116)=[STRING]; HttpHost(1117)=[STRING]; HttpFirstLine(1118)=[STRING]; FileName(1097)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; RealSrcMacAddr(1204)=[STRING]; RealDstMacAddr(1205)=[STRING]; PayLoad(1135)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Source IP address. $4: Source port number. $5: Destination IP address. $6: Destination port number. $7: Source VPN instance name. $8: Source security zone name. $9: Destination security zone name. $10: Name of the identity user. $11: Policy name. $12: Attack name. $13: Attack ID. $14: Attack category. $15: Protected object type. $16: Protected object. $17: Severity level. Valid values are: o INVALID: Severity level not specified. o LOW. o MEDIUM. o HIGH. o CRITICAL. $18: Actions applied to the packet. Available actions are: o Block-Source. o Drop. o Reset. o Permit. o Redirect. o Capture. o Logging. $19: Common Vulnerabilities and Exposures (CVE). $20: Bugtraq ID (BID).

	$21: Microsoft Security Bulletins (MSB). $22: Packet direction: o original. o reply. $23: Original source IP address of the packet. $24: Attack subcategory. $25: Login username. $26: Login password. Support for this field depends on the device model. $27: Capture file name. $28: Host field. $29: Packet first line. $30: File name. $31: Source MAC address. $32: Destination MAC address. $33: Real source MAC address. The value for this field is displayed only when MAC address learning through a Layer 3 device is enabled. $34: Real destination MAC address. The value for this field is displayed only when MAC address learning through a Layer 3 device is enabled. $35: Event return value. $36: VLAN ID. $37: VXLAN ID. $38: Source location. $39: Destination location.
Severity level	4
Example	IPS/4/IPS_IPV4_INTERZONE:-Context=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPAddr(1003)=100.10.10.40; SrcPort(1004)=2999; DstIPAddr(1007)=200.10.10.40; DstPort(1008)=80; RcvVPNInstance(1042)=; SrcZoneName(1025)=spf; DstZoneName(1035)=spf; UserName(1113)=abc; PolicyName(1079)=ips; AttackName(1088)=WEB_CLIENT_Windows_Media_ASF_File_Download_SET; AttackID(1089)=5707; Category(1090)=Other; Protection(1091)=Other; SubProtection(1092)=Other; Severity(1087)=CRITICAL; Action(1053)=Reset & Logging; CVE(1075)=CVE-2014-6277 | CVE-2014-6278; BID(1076)=BID-22559; MSB(1077)=MS10-017; HitDirection(1115)=original; RealSrcIP(1100)=10.10.10.10,20.20.20.20; SubCategory(1124)=Other; LoginUserName(1177)=admin; LoginPwd(1178)=YW5nc2MxMDA2Vw==; CapturePktName(1116)=ips_100.10.10.40_20171205_101112_5707.pcap; HttpHost(1117)=www.shr.com; HttpFirstLine(1118)=/file/show.cgi%7cecho%20HSC/http_pic_300k.jpg; FileName(1097)=123.txt; SrcMacAddr(1021)= 021a-c501-0001; DstMacAddr(1022)=741f-4a93-02ac; RealSrcMacAddr(1204)=; RealDstMacAddr(1205)=; PayLoad(1135)=/file/show.cgi; VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is sent when an IPv4 packet matches an IPS signature.
Recommended action	No action is required.

IPS_IPV6_INTERZONE (syslog)(fast log)

Message text	Protocol(1001)=[STRING]; Application(1002)=[STRING]; SrcIPv6Addr(1036)=[IPADDR]; SrcPort(1004)=[UINT16]; DstIPv6Addr(1037)=[IPADDR]; DstPort(1008)=[UINT16]; RcvVPNInstance(1042)=-[STRING]; SrcZoneName(1025)=[STRING]; DstZoneName(1035)=[STRING]; UserName(1113)=[STRING]; PolicyName(1079)=[STRING]; AttackName(1088)=[STRING]; AttackID(1089)=[UINT32]; Category(1090)=[STRING]; Protection(1091)=[STRING]; SubProtection(1092)=[STRING]; Severity(1087)=[STRING]; Action(1053)=[STRING]; CVE(1075)=[STRING]; BID(1076)=[STRING]; MSB(1077)=[STRING]; HitDirection(1115)=[STRING]; RealSrcIP(1100)=[STRING]; SubCategory(1124)=[STRING]; LoginUserName(1177)=[STRING]; LoginPwd(1178)=[STRING]; CapturePktName(1116)=[STRING]; HttpHost(1117)=[STRING]; HttpFirstLine(1118)=[STRING]; FileName(1097)=[STRING]; SrcMacAddr(1021)=[STRING]; DstMacAddr(1022)=[STRING]; RealSrcMacAddr(1204)=[STRING]; RealDstMacAddr(1205)=[STRING]; PayLoad(1135)=[STRING]; VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Source IPv6 address. $4: Source port number. $5: Destination IP address. $6: Destination port number. $7: Source VPN instance name. $8: Source security zone name. $9: Destination security zone name. $10: Name of the identity user. $11: Policy name. $12: Attack name. $13: Attack ID. $14: Attack category. $15: Protected object type. $16: Protected object. $17: Severity level. Valid values are: o INVALID: Severity level not specified. o LOW. o MEDIUM. o HIGH. o CRITICAL. $18: Actions applied to the packet. Available actions are: o Block-Source. o Drop. o Reset. o Permit. o Redirect. o Capture. o Logging. $19: Common Vulnerabilities and Exposures (CVE). $20: Bugtraq ID (BID).

	$21: Microsoft Security Bulletins (MSB). $22: Packet direction: ○ original. ○ reply. $23: Original source IP address of the packet. $24: Attack subcategory. $25: Login username. $26: Login password. Support for this field depends on the device model. $27: Capture file name. $28: Host field. $29: Packet first line. $30: File name. $31: Source MAC address. $32: Destination MAC address. $33: Real source MAC address. The value for this field is displayed only when MAC address learning through a Layer 3 device is enabled. $34: Real destination MAC address. The value for this field is displayed only when MAC address learning through a Layer 3 device is enabled. $35: Event return value. $36: VLAN ID. $37: VXLAN ID. $38: Source location. $39: Destination location.
Severity level	4
Example	IPS/4/IPS_IPV6_INTERZONE:-Context=1; Protocol(1001)=TCP; Application(1002)=http; SrcIPv6Addr(1036)=100::40; SrcPort(1004)=2999; DstIPv6Addr(1037)=200::40; DstPort(1008)=80; RcvVPNInstance(1042)=; SrcZoneName(1025)=spf; DstZoneName(1035)=spf; UserName(1113)=aaa; PolicyName(1079)=ips; AttackName(1088)=WEB_CLIENT_Windows_Media_ASF_File_Download_SET; AttackID(1089)=5707; Category(1090)=Other; Protection(1091)=Other; SubProtection(1092)=Other; Severity(1087)=CRITICAL; Action(1053)=Reset & Logging; CVE(1075)=CVE-2014-6277 | CVE-2014-6278; BID(1076)=BID-22559; MSB(1077)=MS10-017; HitDirection(1115)=reply; RealSrcIP(1100)=10::1; SubCategory(1124)=Other; LoginUserName(1177)=admin; LoginPwd(1178)=YW5nc2MxMDA2Vw==; CapturePktName(1116)=ips_100::40_20171205_101112_5707.pcap; HttpHost(1117)=www.shr.com; HttpFirstLine(1118)=/file/show.cgi%7cecho%20HSC/http_pic_300k.jpg; FileName(1097)=123.txt; SrcMacAddr(1021)= 021a-c501-0001; DstMacAddr(1022)=741f-4a93-02ac; RealSrcMacAddr(1204)=; RealDstMacAddr(1205)=; PayLoad(1135)=/file/show.cgi; VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is sent when an IPv6 packet matches an IPS signature.
Recommended action	No action is required.

IPS_WARNING (syslog)

Message text	Updated the IPS signature library successfully.
Variable fields	N/A
Severity level	4
Example	IPS/4/IPS_WARNING: -Context=1; Updated the IPS signature library successfully.
Explanation	The IPS signature library was updated successfully through a manual offline update or triggered online update.
Recommended action	No action is required.

IPS_WARNING (syslog)

Message text	Rolled back the IPS signature library successfully.
Variable fields	N/A
Severity level	4
Example	IPS/4/IPS_WARNING: -Context=1; Rolled back the IPS signature library successfully.
Explanation	The IPS signature library was rolled back to the previous or factory default version successfully.
Recommended action	No action is required.

IPS_WARNING (syslog)

Message text	Failed to update the IPS signature library because no valid license was found for the IPS feature.
Variable fields	N/A
Severity level	4
Example	IPS/4/IPS_WARNING: -Context=1; Failed to update the IPS signature library because no valid license was found for the IPS feature.
Explanation	Failed to update the IPS signature library through immediate online update, local offline update, or scheduled online update, because no valid license can be found. For local offline update failures, this message is displayed only for operations performed on the Web interface.
Recommended action	No action is required.

IPS_WARNING (syslog)

Message text	SNORT rule may lost because lock failed during recover!
Variable fields	N/A
Severity level	4
Example	IPS/4/IPS_WARNING: -Context=1; SNORT rule may lost because lock failed during recover!
Explanation	Some Snort rules might be lost because of lock failure during configuration recovery.
Recommended action	No action is required.

IPS_WARNING (syslog)

Message text	The max of snort rule count is 1024.
Variable fields	N/A
Severity level	4
Example	IPS/4/IPS_WARNING: -Context=1; The max of snort rule count is 1024.
Explanation	The number of Snort rules already reached the upper limit (1024).
Recommended action	No action is required.

IPS_WARNING (syslog)

Message text	Import snort rule successfully.
Variable fields	N/A
Severity level	4
Example	IPS/4/IPS_WARNING: -Context=1; Import snort rule successfully.
Explanation	Snort rules were imported successfully.
Recommended action	No action is required.

IPS_WARNING (syslog)

Message text	Import snort rule completely,the total error rules [UINT32].
Variable fields	$1: Total number of user-defined Snort rules that cannot be imported.
Severity level	4
Example	IPS/4/IPS_WARNING: -Context=1; Import snort rule completely,the total error rules 10.
Explanation	The system finished importing Snort rules and failed to import some Snort rules.
Recommended action	No action is required.

IPS_WARNING (syslog)

Message text	Unload the user-defined snort rules successfully.
Variable fields	N/A
Severity level	4
Example	IPS/4/IPS_WARNING: -Context=1; Unload the user-defined snort rules successfully.
Explanation	The user-defined Snort rules were deleted successfully.
Recommended action	No action is required.

IPS_WARNING (syslog)

Message text	Copy SigPack file failed because flash is not enough.
Variable fields	N/A
Severity level	4
Example	IPS/4/IPS_WARNING: -Context=1; Copy SigPack file failed because flash is not enough.
Explanation	Failed to update the IPS signature library because the storage space is insufficient.
Recommended action	No action is required.

IPS_WARNING (syslog)

Message text	Failed to update signature package in phase [STRING].
Variable fields	$1: Update phase: • **UNKNOWN**—Unknown. • **DOWNLOAD**—Signature file download phase. • **GETURLFILE**—The system obtains the signature file path. • **PREPARE**—Signature library preparation phase. • **PARSE**—Signature library parsing phase. • **UNKNOWN**—Unknown.
Severity level	4
Example	IPS/4/IPS_WARNING: -Context=1; Failed to update signature package in phase PARSE.
Explanation	Failed to update the IPS signature library in a specific phase.
Recommended action	No action is required.

IPSEC messages

This section contains IPsec messages.

IPSEC_DEBUG_LOG

Message text	IPsec packet discarded, Src IP:[STRING], Dst IP:[STRING], SPI:[UINT32], SN:[UINT32], Cause:[STRING].
Variable fields	$1: Source IP address. $2: Destination IP address. $3: Security parameter index (SPI). $4: Sequence number of the packet. $5: Reason for dropping this packet: • Anti-replay checking failed. • AH authentication failed. • ESP authentication failed. • Invalid SA. • ESP decryption failed. • Source address of packet does not match the SA. • No ACL rule matched.
Severity level	6
Example	IPSEC/6/log: IPsec packet discarded, Src IP:1.1.1.2, Dest IP:1.1.1.4, SPI:1002, SN:0, Cause:ah authentication failed
Explanation	An IPsec packet was dropped.
Recommended action	No action is required.

IPSEC_FAILED_ADD_FLOW_TABLE

Message text	Failed to add flow-table due to [STRING].
Variable fields	$1: Reason for the failure.
Severity level	4
Example	IPSEC/4/IPSEC_FAILED_ADD_FLOW_TABLE: Failed to add flow-table due to no enough resource.
Explanation	Failed to add the flow table.
Recommended action	If the failure is caused by not enough hardware resources, contact NSFOCUS Support.

IPSEC_KD3P_LOGINFO

Message text	Anti-replay dropped a packet: src=[STRING]; time-sent=[STRING], [UINT32] [STRING] [UINT32] [UINT32]:[UINT32]:[UINT32] [UINT32]us; time-received=[STRING], [UINT32] [STRING] [UINT32] [UINT32]:[UINT32]:[UINT32] [UINT32]us; time-diff=[UINT32]us; window-size= +-[FLOAT]ms.
Variable fields	$1: Source IP address of the packet. $2: Day of the week on which the packet was sent. $3: Day of the month on which the packet was sent. $4: Month in which the packet was sent. $5: Year in which the packet was sent. $6: Hour at which the packet was sent. $7: Minute at which the packet was sent. $8: Second at which the packet was sent. $9: Microsecond at which the packet was sent. $10: Day of the week on which the packet was received. $11: Day of the month on which the packet was received. $12: Month in which the packet was received. $13: Year in which the packet was received. $14: Hour at which the packet was received. $15: Minute at which the packet was received. $16: Second at which the packet was received. $17: Microsecond at which the packet was received. $18: Interval between the time the packet was sent and the time it was received, in microseconds. $19: Half the anti-replay window size, in milliseconds.
Severity level	6
Example	IPSEC/6/log: Anti-replay dropped a packet: src=192.168.58.178;time-sent=Sat, 23 Apr 2016 11:17:29 594565us; time-received =Sat, 23 Apr 2016 11:17:26 707866us; time-diff=2886699us; window-size =+-2500ms.
Explanation	A packet was dropped. Possible reasons include: • The interval between the time the packet was sent and the time it was received exceeds the anti-replay window size. • Anti-replay is enabled on the receiving IPsec tunnel end but the received packet does not have an anti-replay header. • In tunnel mode, anti-replay is not enabled but the received packet has an anti-replay header.
Recommended action	No action is required.

IPSEC_SA_ESTABLISH

Message text	IPsec SA was established. SA information: Role: [STRING] Local address: [STRING] Remote address: [STRING] Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] Inside VPN instance: [STRING] Outside VPN instance: [STRING] Inbound AH SPI: [STRING] Outbound AH SPI: [STRING] Inbound ESP SPI: [STRING] Outbound ESP SPI: [STRING] ACL number: [UINT32] ACL name: [STRING]
Variable fields	$1: Role, initiator or responder. $2: Local IP address. $3: Remote IP address. $4-$9: Data flow related parameters. $10: Inside VPN instance. $11: Outside VPN instance. $12: Inbound AH SPI. $13: Outbound AH SPI. $14: Inbound ESP SPI. $15: Outbound ESP SPI. $16: ACL number. The default is 4294967295. This field is not displayed if the ACL name is displayed. $17: ACL name. This field is not displayed if the ACL number is displayed.
Severity level	6
Example	IPSEC/6/IPSEC_SA_ESTABLISH: IPsec SA was established. Role: Responder Local address: 2.2.2.2 Remote address: 1.1.1.1 Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb Inbound AH SPI: 192365458 Outbound AH SPI: 13654581 Inbound ESP SPI: 292334583 Outbound ESP SPI: 5923654586 ACL number: 3101
Explanation	An IPsec SA was established.

Recommended action	No action is required.

IPSEC_SA_ESTABLISH_FAIL

Message text	Failed to establish IPsec SA. Reason: [STRING]. SA information: Role: [STRING] Local address: [STRING] Remote address: [STRING] Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] Inside VPN instance: [STRING] Outside VPN instance: [STRING] Inbound AH SPI: [STRING] Outbound AH SPI: [STRING] Inbound ESP SPI: [STRING] Outbound ESP SPI: [STRING] ACL number: [UINT32] ACL name: [STRING]
Variable fields	$1: Failure reason: • Get SP: Required configuration is missing in the SP. SP ID=%u. • Get SP: The SP's local address doesn't match the local address configured in the IKE profile. SP ID=%u, SP's local address=%s, p2policy's local address=%s. • Get SP: The remote address doesn't exist. SP ID=%u, hostname=%s. • Get SP: The SP's remote address doesn't match the remote address configured in the IKE profile. SP ID=%u, SP's remote address=%s, p2policy's remote address=%s. • The policy contains incorrect ACL or IKE profile configuration. PolicyName=%s, Seqnum=%d. • Get SP: The SP doesn't have an IPsec transform set. • Get SP: Failed to create larval SA. • Create SA: Failed to fill the SA. • Create SA: Failed to create SA. • Create SA: Can't find SP. • Failed to create tunnel because a tunnel with the same index and sequence number already exists. Tunnel index=%d, tunnel seq=%d. • Failed to switch SA because the inbound SA can't be found. SPI=%u. • Failed to switch SA because the SA state is incorrect. • Failed to switch SA because the outbound SA can't be found. • Failed to switch SA because the

		outbound SA using another security protocol can't be found. • Failed to switch SA in kernel. • Failed to notify kernel of the link state change. • Number of IPsec tunnels reached the crypto capacity of the device. • Maximum number of IPsec tunnels already reached. • Failed to add IPsec tunnel to kernel. • Getting SP: IPsec is smoothing. • Getting SP: IPsec is not running. • Getting SP: Failed to find SP by index and sequence number. • Getting SP: Creating SA timed out. • Getting SP by interface: Target node not online. • Getting SP by mGRE: Failed to get interface. • Getting SP: Failed to get SP by mGRE because interface type was invalid. • Getting SP: Failed to get SP by mGRE because of no tunnel protection configuration. • Getting SP: Failed to get SP by mGRE because profile %s was not found. • Getting SP: Failed to get SP by mGRE because of wrong profile type. • Getting SP by mGRE: Failed to find profile SP by profile %s. • Getting SP: Failed to get SP by mgre. • Getting SP: Failed to get SP by SVTI because of invalid interface type. • Getting SP: Failed to get SP by SVTI because of no tunnel protection configuration with interface %s. • Getting SP: Failed to get SP by SVTI because profile %s was not found. • Getting SP: Failed to get SP by SVTI because of wrong type of profile %s. • Getting SP by SVTI: Failed to find profile SP by profile %s. • Getting SP: Failed to get SP by SVTI because SP type was not ISAKMP with profile %s. • Getting SP: Failed to match flow because renegotiation SP's index or Seqnum changed. • Getting SP: Failed to match SVTI flow because IKE profile was not match. • Getting SP: Failed to match SVTI flow because flow was not match with ACL. • Getting SP by SVTI: Failed to create larval SA. • Getting SP: Failed to get SP by SVTI with interface %s. • Getting SP by L3 interface: Failed to get interface data.

	• Getting SP: Failed to get SP by L3 interface because no SP entry was found by key. • Getting SP: Failed to get SP by L3 interface because no source interface SP entry was found by key. • Getting SP by L3 interface: Failed to match SP because SP's mode not ISAKMP. • Getting SP by L3 interface: Failed to match SP because SP negotiation not complete. • Getting SP: Rejected peer's request of any flow when SP's mode was isakmp template and no ACL was specified. • Getting SP by L3 interface: Failed to match SP because policy cannot be found by SP. • Getting SP by L3 interface: Failed to match SP because flow netmask check failed. • Getting SP by L3 interface: Failed to match SP because flow overlap check failed. • Getting SP by L3 interface: Failed to match SP because IKE profile was %s while IPsec used profile %s. • Getting SP: Failed to match flow because ACL not match. • Getting SP: Failed to match flow because renegotiation SP's index or Seqnum changed. $2: Role, initiator or responder. $3: Local IP address. $4: Remote IP address. $5-$10: Data flow related parameters. $11: Inside VPN instance. $12: Outside VPN instance. $13: Inbound AH SPI. $14: Outbound AH SPI. $15: Inbound ESP SPI. $16: Outbound ESP SPI. $17: ACL number. The default is 4294967295. This field is not displayed if the ACL name is displayed. $18: ACL name. This field is not displayed if the ACL number is displayed.

Severity level	6
Example	IPSEC/6/IPSEC_SA_ESTABLISH_FAIL: Failed to establish IPsec SA Reason: Failed to add IPsec tunnel. SA information: Role: Responder Local address: 2.2.2.2 Remote address: 1.1.1.1 Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb Inbound AH SPI: 192365458 Outbound AH SPI: 13654581 Inbound ESP SPI: 292334583 Outbound ESP SPI: 5923654586 ACL number: 3101
Explanation	Failed to establish an IPsec SA.
Recommended action	Verify the IPsec configurations on the local and peer devices.

IPSEC_SA_INITIATION

Message text	Began to establish IPsec SA. Local address: [STRING] Remote address: [STRING] Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] Inside VPN instance: [STRING] Outside VPN instance: [STRING] ACL number: [UINT32] ACL name: [STRING]
Variable fields	$1: Local IP address. $2: Remote IP address. $3-$8: Data flow related parameters. $9: Inside VPN instance. $10: Outside VPN instance. $11: ACL number. The default is 4294967295. This field is not displayed if the ACL name is displayed. $12: ACL name. This field is not displayed if the ACL number is displayed.
Severity level	6
Example	IPSEC/6/IPSEC_SA_INITIATION: Began to establish IPsec SA. Local address: 2.2.2.2 Remote address: 1.1.1.1 Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb ACL number: 3101
Explanation	An IPsec SA was to be established.
Recommended action	No action is required.

IPSEC_SA_TERMINATE

Message text	The IPsec SA was deleted. Reason: [STRING] SA information: • Role: [STRING] • Local address: [STRING] • Remote address: [STRING] • Sour addr: [STRING] Port: [UINT32] Protocol: [STRING] • Dest addr: [STRING] Port: [UINT32] Protocol: [STRING] • Inside VPN instance: [STRING] • Outside VPN instance: [STRING] • Inbound AH SPI: [STRING] • Outbound AH SPI: [STRING] • Inbound ESP SPI: [STRING] • Outbound ESP SPI: [STRING] • ACL number: [UINT32] • ACL name: [STRING]
Variable fields	$1: Reason for the deletion: • SA idle timeout • The **reset** command was executed • Internal event • Configuration change • An IKE SA deletion message was received $2: Role, initiator or responder. $3: Local IP address. $4: Remote IP address. $5-$10: Data flow related parameters. $11: Inside VPN instance. $12: Outside VPN instance. $13: Inbound AH SPI $14: Outbound AH SPI $15: Inbound ESP SPI $16: Outbound ESP SPI $17: ACL number. The default is 4294967295. This field is not displayed if the ACL name is displayed. $18: ACL name. This field is not displayed if the ACL number is displayed.
Severity level	6
Example	IPSEC/6/IPSEC_SA_TERMINATE: The IPsec SA was deleted. Reason: SA idle timeout. SA information: Role: initiator Local address: 2.2.2.2 Remote address: 1.1.1.1

	Sour addr: 192.168.2.0/255.255.255.0 Port: 0 Protocol: IP Dest addr: 192.168.1.0/255.255.255.0 Port: 0 Protocol: IP Inside VPN instance: aaa Outside VPN instance: bbb Inbound AH SPI: 192365458 Outbound AH SPI: 13654581 Inbound ESP SPI: 292334583 Outbound ESP SPI: 5923654586 ACL number: 3101
Explanation	An IPsec SA was deleted.
Recommended action	No action is required.

IPSG messages

This section contains IPSG messages.

IPSG_ADDENTRY_ERROR

Message text	Failed to add an IP source guard binding (IPv4 [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING]. Failed to add an IP source guard binding (IPv6 [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING].
Variable fields	$1: IP address. If you do not specify an IP address, this field is empty. $2: MAC address. If you do not specify a MAC address, this field displays **N/A**. $3: VLAN ID. If you do not specify a VLAN, this field displays **65535**. $4: Interface name. If you do not specify an interface, this field displays **N/A**. $5: Failure reasons. Available options include: o Feature not supported o Resources not sufficient o Resource conflict o Unknown error
Severity level	6
Example	IPSG/6/IPSG_ADDENTRY_ERROR: Failed to add an IP source guard binding (IPv4 1.1.1.1, MAC 0001-0001-0001, and VLAN 1) on interface Vlan-interface1. Resources not sufficient.
Explanation	IPSG failed to issue a static or dynamic IPSG binding. The message is sent in any of the following situations: • The IPSG feature is not supported. • The hardware resources are not sufficient for the operation. • The resource conflict occurs. • An unknown error occurs.
Recommended action	To resolve the problem, you can perform the following tasks: • Clear the memory to release hardware resources when the failure is caused by insufficient hardware resources. • Add the IPSG binding again if you are adding a static binding. • Verify that the ACL or QoS policy configuration does not conflict with the IPSG configuration when a resource conflict occurs. • Contact NSFOCUS Support if the failure is caused by an unknown error.

IPSG_DELENTRY_ERROR

Message text	Failed to delete an IP source guard binding (IPv4 [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING]. Failed to delete an IP source guard binding (IPv6 [STRING], MAC [STRING], and VLAN [UINT16]) on interface [STRING]. [STRING].
Variable fields	$1: IP address. If you do not specify an IP address, this field is empty. $2: MAC address. If you do not specify a MAC address, this field displays **N/A**. $3: VLAN ID. If you do not specify a VLAN, this field displays **65535**. $4: Interface name. If you do not specify an interface, this field displays **N/A**. $5: Failure reason. Available options include: ○ Feature not supported ○ Unknown error
Severity level	6
Example	IPSG/6/IPSG_DELENTRY_ERROR: Failed to delete an IP source guard binding (IPv4 1.1.1.1, MAC 0001-0001-0001, and VLAN 1) on interface Vlan-interface1. Unknown error.
Explanation	IPSG failed to delete a global static IPSG binding. The message is sent in any of the following situations: • The IPSG feature is not supported. • An unknown error occurs.
Recommended action	To resolve the problem, you can perform the following tasks: • Delete the global static IPSG binding again. • Contact NSFOCUS Support if the failure is caused by an unknown error.

IRDP messages

This section contains IRDP messages.

IRDP_EXCEED_ADVADDR_LIMIT

Message text	The number of advertisement addresses on interface [STRING] exceeded the limit 255.
Variable fields	$1: Interface name.
Severity level	6
Example	IRDP/6/IRDP_EXCEED_ADVADDR_LIMIT: The number of advertisement addresses on interface Ethernet1/1/0/2 exceeded the limit 255.
Explanation	The number of addresses to be advertised on an interface exceeds the upper limit.
Recommended action	Remove unused addresses on the interface.

IRF

This section contains IRF messages.

IRF_LINK_BLOCK

Message text	IRF port went blocked.
Variable fields	N/A
Severity level	2
Example	IRF/2/IRF_LINK_BLOCK: IRF port went blocked.
Explanation	The IRF port was blocked. A blocked IRF port cannot send and receive service packets, but it can send and receive IRF protocol packets. For example, this message appears on the member device that has the lower priority when an IRF member ID conflict is detected for member devices.
Recommended action	Check the IRF member ID on each member device for any conflict, and change the IRF member IDs of member devices to be unique.

IRF_LINK_DOWN

Message text	IRF port went down.
Variable fields	N/A
Severity level	3
Example	IRF/3/IRF_LINK_DOWN: IRF port went down.
Explanation	The IRF port went down.
Recommended action	Verify the following items: • Network interfaces have been bound to the IRF port. • The IRF network interfaces and the peer interfaces have Layer 2 connectivity.

IRF_LINK_UP

Message text	IRF port came up.
Variable fields	N/A
Severity level	6
Example	IRF/6/IRF_LINK_UP: IRF port came up.
Explanation	The IRF port came up.
Recommended action	No action is required.

IRF_MEMBER_LEFT

Message text	Member [STRING] left the IRF fabric.
Variable fields	$1: IRF member ID of the device.
Severity level	4
Example	IRF/4/IRF_MEMBER_LEFT: Member 2 left the IRF fabric.
Explanation	This message occurs when a member device left the IRF fabric.
Recommended action	No action is required.

IRF_MEMBERID_CONFLICT

Message text	IRF member ID conflict occurred. The ID [UINT32] has been used for another device with CPU-Mac: [STRING].
Variable fields	$1: IRF member ID of the device. $2: CPU MAC address of the device.
Severity level	4
Example	IRF/4/IRF_MEMBERID_CONFLICT:-slot = 5; IRF member ID conflict occurred, The ID 5 has been used for another device with CPU-Mac: 000c-29d7-c1ae.
Explanation	This message occurs when the device detects that it has the same IRF member ID as another device in the same broadcast domain.
Recommended action	Check the IRF member IDs and change the IRF member ID of a device. Make sure the member devices use unique member IDs.

IRF_MEMBERID_CONFLICT_REBOOT

Message text	IRF member ID conflict. For the device to join the IRF fabric,please change the device member ID to a unique one among all the IRF member devices and reboot the device.
Variable fields	N/A
Severity level	4
Example	IRF/4/IRF_MEMBERID_CONFLICT_REBOOT: IRF member ID conflict. For the device to join the IRF fabric,please change the device member ID to a unique one among all the IRF member devices and reboot the device.
Explanation	This message occurs if the device fails to join an IRF fabric because it is using the same member ID as another IRF member device. In this situation, the network ports on the device will be blocked until it re-joins the IRF fabric with a unique member ID.
Recommended action	**146.** Log in to the device that displayed this message. **147.** Change the member ID of the device to a unique one. **148.** Reboot the device to re-join the IRF fabric.

IRF_MERGE

Message text	IRF merge occurred.
Variable fields	N/A
Severity level	4
Example	IRF/4/IRF_MERGE: IRF merge occurred.
Explanation	IRF merge occurred.
Recommended action	No action is required.

IRF_MERGE_NEED_REBOOT

Message text	IRF merge occurred. This IRF system needs a reboot.
Variable fields	N/A
Severity level	4
Example	IRF/4/IRF_MERGE_NEED_REBOOT: IRF merge occurred. This IRF system needs a reboot.
Explanation	IRF merge occurred. This IRF fabric needs a reboot to complete the IRF merge because the master of this IRF fabric failed the master election for IRF merge.
Recommended action	Reboot the IRF fabric to complete the IRF merge.

IRF_MERGE_NOT_NEED_REBOOT

Message text	IRF merge occurred. This IRF system does not need to reboot.
Variable fields	N/A
Severity level	5
Example	IRF/5/IRF_MERGE_NOT_NEED_REBOOT: IRF merge occurred. This IRF system does not need to reboot.
Explanation	IRF merge occurred. This IRF fabric does not need to reboot because the master of this IRF fabric won the master election for IRF merge.
Recommended action	No action is required.

IRF_NEWMEMBER_JOIN

Message text	Member [STRING] joined the IRF fabric.
Variable fields	$1: IRF member ID of the device.
Severity level	4
Example	IRF/4/IRF_NEWMEMBER_JOIN: Member 2 joined the IRF fabric.
Explanation	This message occurs when a member device joined the IRF fabric.
Recommended action	No action is required.

ISIS messages

This section contains IS-IS messages.

ISIS_MEM_ALERT

Message text	ISIS Process received system memory alert [STRING] event.
Variable fields	$1: Type of the memory alarm.
Severity level	5
Example	ISIS/5/ISIS_MEM_ALERT: ISIS Process received system memory alert start event.
Explanation	IS-IS received a memory alarm.
Recommended action	Check the system memory and release memory for the modules that occupy too many memory resources.

ISIS_NBR_CHG

Message text	IS-IS [UINT32], [STRING] adjacency [STRING] [STRING], state changed to [STRING].
Variable fields	$1: IS-IS process ID. $2: Neighbor level. $3: Neighbor ID. $4: Interface name. $5: Current adjacency state. Options include **DOWN**, **UP**, and **INIT**.
Severity level	5
Example	ISIS/5/ISIS_NBR_CHG: IS-IS 1, Level-1 adjacency 0000.0000.8888 (Eth1/4/1/3), state changed to DOWN.
Explanation	The IS-IS adjacency state changed on an interface.
Recommended action	When the adjacency with a neighbor changes to **down** on an interface, check for IS-IS configuration errors and loss of network connectivity.

ISSU messages

This section contains ISSU messages.

ISSU_ROLLBACKCHECKNORMAL

Message text	The rollback might not be able to restore the previous version for [STRING] because the status is not normal.
Variable fields	$1: Chassis number and slot number or slot number.
Severity level	4
Example	ISSU/4/ISSU_ROLLBACKCHECKNORMAL: The rollback might not be able to restore the previous version for chassis 1 slot 2 because the state is not normal.
Explanation	While an ISSU was in switching state, a user executed the **issu rollback** command or the ISSU automatic-rollback timer expired. However, the status of the MPU was not normal.
Recommended action	No action is required.

ISSU_SWITCHOVER

Message text	Switchover completed on [STRING].
Variable fields	Pattern 1: $1: String **the device** or the name of an MDC or context. Pattern 2: $1: A string that indicates the slot number, CPU number, and MDC or context name. Pattern 3: $1: A string that indicates the chassis number, slot number, CPU number, and MDC or context name. The CPU number in this message is the number of a CPU on an extended module. It may not be the default CPU number. Support for the CPU number, MDC name, and context name depends on the device model.
Severity level	5
Example	Pattern 1: ISSU/5/ISSU_SWITCHOVER: Switchover completed on the device. Pattern 2: ISSU/5/ISSU_SWITCHOVER: Switchover completed on slot 1 CPU 1 in context a. Pattern 3: ISSU/5/ISSU_SWITCHOVER: Switchover completed on chassis 2 slot 3 in MDC a.
Explanation	A switchover was completed on the device or a slot. If MDCs or contexts are running on the device or slot, a switchover is completed only if the switchover is completed on all MDCs or contexts.
Recommended action	No action is required.

ISSU_UPGRADE

Message text	Upgrade completed on [STRING].
Variable fields	Pattern 1: $1: String **the device** or the name of an MDC or context. Pattern 2: $1: A string that indicates the slot number, CPU number, and MDC or context name. Pattern 3: $1: A string that indicates the chassis number, slot number, CPU number, and MDC or context name. The CPU number in this message is the number of a CPU on an extended module. It may not be the default CPU number. Support for the CPU number, MDC name, and context name depends on the device model.
Severity level	5
Example	Pattern 1: ISSU/5/ISSU_UPGRADE: Upgrade completed on the device. Pattern 2: ISSU/5/ISSU_UPGRADE: Upgrade completed on slot 1 CPU 1 in context a. Pattern 3: ISSU/5/ISSU_UPGRADE: Upgrade completed on chassis 2 slot 3 in MDC a.
Explanation	An ISSU was completed on the device or a slot. If MDCs or contexts are running on the device or slot, an ISSU is completed only if the ISSU is completed on all MDCs or contexts.
Recommended action	No action is required.

KDNS messages

This section contains KDNS messages.

KDNS_BIND_PORT_ALLOCETED

Message text	Failed to bind UDP [STRING] connection port [NUMBER] to VPN instance [STRING] for the DNS listener because the port has already been allocated.
Variable fields	$1: UDP port type: • IPv4 • IPv6 $2: UDP port number. $3: VPN instance name.
Severity level	3
Example	KDNS/3/KDNS_BIND_PORT_ALLOCETED: -MDC=1; Failed to bind UDP IPv4 connection port 53 to VPN instance vpn1 for the DNS listener because the port has already been allocated.
Explanation	The system failed to bind a UDP port to a DNS listener because the port has been used.
Recommended action	Bind a UDP port that has not been used.

KHTTP messages

This section contains KHTTP messages.

KHTTP_BIND_PORT_ALLOCETED

Message text	Failed to bind TCP connection [STRING]/[UINT32] to VPN instance [UINT32] because the port was already allocated.
Variable fields	$1: IP address. $2: Port number. $3: Index of a VPN instance.
Severity level	3
Example	KHTTP/3/KHTTP_BIND_PORT_ALLOCETED: Failed to bind TCP connection 192.168.30.117/10000 to VPN instance 0 because the port was already allocated.
Explanation	Failed to bind an IP address and a port number to a VPN instance because the port number was already allocated.
Recommended action	**149.** Display port information by executing the **`display tcp-proxy port-info`** or **`display ipv6 tcp-proxy port-info`** command. **150.** Rebind the TCP connection to the VPN instance by using an available port number.

KHTTP_BIND_ADDRESS_INUSED

Message text	Failed to bind TCP connection [STRING]/[UINT32] to VPN instance [UINT32] because the address was already used.
Variable fields	$1: IP address. $2: Port number. $3: Index of a VPN instance.
Severity level	3
Example	KHTTP/3/KHTTP_BIND_ADDRESS_INUSED: Failed to bind TCP connection 192.168.30.117/10000 to VPN instance 0 because the address was already used.
Explanation	Failed to bind an IP address and a port number to a VPN instance because the IP address was already used and cannot be reused.
Recommended action	**151.** Display IP address information by executing the **`display tcp-proxy`** command. **152.** Rebind the TCP connection to the VPN instance by using an unused or a reusable IP address.

L2PT messages

This section contains L2PT messages.

L2PT_SET_MULTIMAC_FAILED

Message text	Failed to set a tunnel destination MAC address to [MAC].
Variable fields	$1: MAC address.
Severity level	4
Example	L2PT/4/L2PT_SET_MULTIMAC_FAILED: Failed to set a tunnel destination MAC address to 010f-e200-0003.
Explanation	Failed to specify the destination multicast MAC address for tunneled packets.
Recommended action	No action is required.

L2PT_CREATE_TUNNELGROUP_FAILED

Message text	Failed to create a VLAN tunnel group for [STRING].
Variable fields	$1: Protocol name.
Severity level	4
Example	L2PT/4/L2PT_CREATE_TUNNELGROUP_FAILED: Failed to create a VLAN tunnel group for STP.
Explanation	Failed to create a VLAN tunnel group for a protocol.
Recommended action	No action is required.

L2PT_ADD_GROUPMEMBER_FAILED

Message text	Failed to add [STRING] as a member to the VLAN tunnel group for [STRING].
Variable fields	$1: Interface name. $2: Protocol name.
Severity level	4
Example	L2PT/4/L2PT_ADD_GROUPMEMBER_FAILED: Failed to add GigabitEthernet2/0/1 as a member to the VLAN tunnel group for STP.
Explanation	Failed to add an interface to a VLAN tunnel group for a protocol.
Recommended action	No action is required.

L2PT_ENABLE_DROP_FAILED

Message text	Failed to enable [STRING] packet drop on [STRING].
Variable fields	$1: Protocol name. $2: Interface name.
Severity level	4
Example	L2PT/4/L2PT_ENABLE_DROP_FAILED: Failed to enable STP packet drop on GigabitEthernet2/0/1.
Explanation	Failed to enable L2PT drop for a protocol on an interface.
Recommended action	No action is required.

L2TPv2 messages

This section contains L2TPv2 messages.

L2TPV2_TUNNEL_EXCEED_LIMIT

Message text	Number of L2TP tunnels exceeded the limit.
Variable fields	N/A
Severity level	4
Example	L2TPV2/4/L2TPV2_TUNNEL_EXCEED_LIMIT: Number of L2TP tunnels exceeded the limit.
Explanation	The number of established L2TP tunnels has reached the limit.
Recommended action	**153.** Perform one of the following tasks: ○ Execute the **reset l2tp tunnel** command to disconnect an idle tunnel. ○ Wait for the device to automatically disconnect an idle tunnel after the hello interval elapses. **154.** If the problem persists, contact NSFOCUS for support.

L2TPV2_SESSION_EXCEED_LIMIT

Message text	Number of L2TP sessions exceeded the limit.
Variable fields	N/A
Severity level	4
Example	L2TPV2/4/L2TPV2_SESSION_EXCEED_LIMIT: Number of L2TP sessions exceeded the limit.
Explanation	The number of established L2TP sessions has reached the limit.
Recommended action	No action is required.

L2VPN messages

This section contains L2VPN messages.

L2VPN_BGPVC_CONFLICT_LOCAL

Message text	Remote site ID [INT32] (From [STRING], route distinguisher [STRING]) conflicts with local site.
Variable fields	$1: ID of a remote site. $2: IP address of the remote site. $3: Route distinguisher of the remote site.
Severity level	5
Example	L2VPN/5/L2VPN_BGPVC_CONFLICT_LOCAL: Remote site ID 1 (From 1.1.1.1, route distinguisher 1:1) conflicts with local site.
Explanation	A remote site ID conflicted with the local site ID. This message is generated when one of the following situations occurs: • The received remote site ID is the same as the local site ID. • The local site ID is configured the same as a received remote site ID.
Recommended action	Modify the site ID configuration on the local device or remote device. Or, configure the remote site ID in a different VPLS instance than the local site ID.

L2VPN_BGPVC_CONFLICT_REMOTE

Message text	Remote site ID [INT32] (From [STRING], route distinguisher [STRING]) conflicts with another remote site.
Variable fields	$1: ID of a remote site. $2: IP address of the remote site. $3: Route distinguisher of the remote site.
Severity level	5
Example	L2VPN/5/L2VPN_BGPVC_CONFLICT_REMOTE: Remote site ID 1 (From 1.1.1.1, route distinguisher 1:1) conflicts with another remote site.
Explanation	Two remote site IDs conflicted. This message is generated when the received remote site ID is the same as another received remote site ID.
Recommended action	Modify the site ID configuration on one remote device. Or, configure the two remote site IDs in different VPLS instances.

L2VPN_HARD_RESOURCE_NOENOUGH

Message text	No enough hardware resource for L2VPN.
Variable fields	N/A
Severity level	4
Example	L2VPN/4/L2VPN_HARD_RESOURCE_NOENOUGH: No enough hardware resource for L2VPN.
Explanation	Hardware resources for L2VPN were insufficient.
Recommended action	Check whether unnecessary VSIs, PWs, or ACs had been generated. If yes, delete them.

L2VPN_HARD_RESOURCE_RESTORE

Message text	Hardware resources for L2VPN are restored.
Variable fields	N/A
Severity level	6
Example	L2VPN/6/L2VPN_HARD_RESOURCE_RESTORE: Hardware resources for L2VPN are restored.
Explanation	Hardware resources for L2VPN were restored.
Recommended action	No action is required.

L2VPN_LABEL_DUPLICATE

Message text	Incoming label [INT32] for a static PW in [STRING] [STRING] is duplicate.
Variable fields	$1: Incoming label value. $2: Type of L2VPN, Xconnect-group or VSI. $3: Name of the Xconnect-group or VSI.
Severity level	4
Example	L2VPN/4/L2VPN_LABEL_DUPLICATE: Incoming label 1024 for a static PW in Xconnect-group aaa is duplicate.
Explanation	The incoming label of a static PW in this Xconnect-group or VSI was occupied by another configuration, for example, by a static LSP or by a static CRLSP. This message is generated when one of the following events occurs: • When MPLS is enabled, configure a static PW with an incoming label which is occupied by another configuration. • Enable MPLS when a static PW whose incoming label is occupied by another configuration already exists.
Recommended action	Remove this static PW, and reconfigure it with another incoming label.

LAGG messages

This section contains link aggregation messages.

LAGG_ACTIVE

Message text	Member port [STRING] of aggregation group [STRING] changed to the active state.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_ACTIVE: Member port GE1/0/1 of aggregation group BAGG1 changed to the active state.
Explanation	A member port in an aggregation group changed to the Selected state.
Recommended action	No action is required.

LAGG_INACTIVE_AICFG

Message text	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the member port and the aggregate interface have different attribute configurations.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_INACTIVE_AICFG: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the member port and the aggregate interface have different attribute configurations.
Explanation	A member port in an aggregation group changed to the Unselected state because the member port and the aggregate interface had different attribute configurations.
Recommended action	Modify the attribute configurations of the member port to be consistent with the aggregate interface.

LAGG_INACTIVE_BFD

Message text	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the BFD session state of the port was down.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_INACTIVE_BFD: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the BFD session state of the port is down.
Explanation	A member port in an aggregation group changed to the Unselected state because the BFD session on the port became down.
Recommended action	To resolve the problem, you can perform the following tasks: • Verify that link failure has occurred and troubleshoot the failure. • Modify the port information and configuration for the port to have the same operational key and attribute configuration as the reference port.

LAGG_INACTIVE_CONFIGURATION

Message text	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the aggregation configuration of the port is incorrect.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_INACTIVE_CONFIGURATION: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the aggregation configuration of the port is incorrect.
Explanation	A member port in an aggregation group changed to the Unselected state because the member port and the aggregate interface had different aggregation configuration.
Recommended action	No action is required.

LAGG_INACTIVE_DUPLEX

Message text	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the duplex mode is different between the member port and the reference port.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_INACTIVE_DUPLEX: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the duplex mode is different between the member port and the reference port.
Explanation	A member port in an aggregation group changed to the Unselected state because the duplex mode was different between the member port and the reference port.
Recommended action	Change the duplex mode of the member port to be the same as the reference port.

LAGG_INACTIVE_HARDWAREVALUE

Message text	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because of the port's hardware restriction.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_INACTIVE_HARDWAREVALUE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because of the port's hardware restriction.
Explanation	A member port in an aggregation group changed to the Unselected state because of the port's hardware restriction.
Recommended action	No action is required.

LAGG_INACTIVE_LOWER_LIMIT

Message text	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of active ports is below the lower limit.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_INACTIVE_LOWER_LIMIT: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the number of active ports is below the lower limit.
Explanation	A member port in an aggregation group was placed in Unselected state because the required minimum number of Selected ports was not reached.
Recommended action	Make sure the minimum number of Selected ports is met.

LAGG_INACTIVE_PARTNER

Message text	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the aggregation configuration of its peer port is incorrect.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_INACTIVE_PARTNER: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the aggregation configuration of its peer port is incorrect.
Explanation	A member port in an aggregation group changed to the Unselected state because the port's partner changed to the Unselected state.
Recommended action	No action is required.

LAGG_INACTIVE_PHYSTATE

Message text	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the physical state of the port is down.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_INACTIVE_PHYSTATE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the physical state of the port is down.
Explanation	A member port in an aggregation group changed to the Unselected state because the port went down.
Recommended action	Bring up the member port.

LAGG_INACTIVE_RESOURCE_INSUFICIE

Message text	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because all aggregate resources are occupied.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_INACTIVE_RESOURCE_INSUFICIE: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because all aggregate resources are occupied.
Explanation	A member port in an aggregation group changed to the Unselected state because all aggregation resources were used.
Recommended action	No action is required.

LAGG_INACTIVE_SPEED

Message text	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the speed configuration of the port is incorrect.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_INACTIVE_SPEED: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the speed configuration of the port is incorrect.
Explanation	A member port in an aggregation group changed to the Unselected state because the speed was different between the member port and the reference port.
Recommended action	Change the speed of the member port to be the same as the reference port.

LAGG_INACTIVE_UPPER_LIMIT

Message text	Member port [STRING] of aggregation group [STRING] changed to the inactive state, because the number of active ports has reached the upper limit.
Variable fields	$1: Port name. $2: Link aggregation group type and ID.
Severity level	6
Example	LAGG/6/LAGG_INACTIVE_UPPER_LIMIT: Member port GE1/0/1 of aggregation group BAGG1 changed to the inactive state, because the number of active ports has reached the upper limit.
Explanation	The number of Selected ports reached the upper limit in a dynamic aggregation group. A member port in the aggregation group changed to the Unselected state because a more eligible port joined the aggregation group.
Recommended action	No action is required.

LB messages

This section contains LB messages.

LB_CHANGE_DEFAULTLG_STATE_VS

Message text	The state of link group associated with virtual server [STRING] ([STRING], port: [USHORT]) was changed, primary link group is [STRING], backup link group is [STRING], current link group is [STRING].
Variable fields	$1: Virtual server name. $2: Virtual server address. $3: Port number. $4: Primary link group name. $5: Backup link group name. $6: Current link group name.
Severity level	5
Example	LB/5/LB_CHANGE_DEFAULTLG_STATE_VS: -Context=1; The state of link group associated with virtual server VS (192.168.10.10, port: 20) was changed, primary link group is MF, backup link group is BF, current link group is CF.
Explanation	The state of the link group associated with a virtual server changed.
Recommended action	Check whether the availability criteria setting for the link group is changed. If the setting is not changed, check the network environment and link state.

LB_CHANGE_DEFAULTSF_STATE_VS

Message text	The state of server farm associated with virtual server [STRING] ([STRING], port: [USHORT]) was changed, primary server farm is [STRING], backup server farm is [STRING], current server farm is [STRING].
Variable fields	$1: Virtual server name. $2: Virtual server address. $3: Port number. $4: Primary server farm name. $5: Backup server farm name. $6: Current server farm name.
Severity level	5
Example	LB/5/LB_CHANGE_DEFAULTSF_STATE_VS: The state of server farm associated with virtual server VS (192.168.10.10, port: 20) was changed, primary server farm is MF, backup server farm is BF, current server farm is CF.
Explanation	The state of the server farm associated with a virtual server changed.
Recommended action	Check whether the availability criteria setting for the server farm is changed. If the setting is not changed, check the network environment and real server state.

LB_CHANGE_DS_HCSTATUS

Message text	The health state of DNS server [STRING] was changed to [STRING]. Last state was kept for [ULONG] seconds.
Variable fields	$1: DNS server name. $2: Health state of the DNS server: Active or Inactive. $3: Duration for a state in seconds.
Severity level	5
Example	LB/5/ LB_CHANGE_DS_HCSTATUS: The health state of DNS server DS was changed to Active. Last state was kept for 100 seconds.
Explanation	The health state of a DNS server changed, and the DNS server stayed in the previous state for a number of seconds.
Recommended action	Check the network environment and DNS server state when the health state of a DNS server is Inactive.

LB_CHANGE_DS_PROBERESULT

Message text	The probe result of DNS server [STRING] template [STRING] was changed to [STRING].
Variable fields	$1: DNS server name. $2: Name of the NQA template used by the health monitoring method. $3: Health monitoring result: Successful or Failed.
Severity level	5
Example	LB/5/LB_CHANGE_DS_PROBERESULT: The probe state of real server RS template ICMP was changed to Successful.
Explanation	The health monitoring result for a DNS server changed.
Recommended action	Check the network environment and DNS server state if the health monitoring result for a DNS server is Failed.

LB_CHANGE_DSQUOTE_HCSTATUS

Message text	The health state of (DNS server pool [STRING], DNS server pool member [STRING], port: [USHORT]) was changed to [STRING]. Last state was kept for [ULONG] seconds.
Variable fields	$1: DNS server pool name. $2: DNS server name. $3: Port number. $4: Health monitoring result: Active or Inactive. $5: Duration for the previous state in seconds.
Severity level	5
Example	LB/5/LB_CHANGE_DSQUOTE_HCSTATUS: The health state of (DNS server pool dp, DNS server dDNSs, port:33) was changed to Active. Last state was kept for 100 seconds.
Explanation	The health state of a DNS server pool member changed.
Recommended action	Check the network environment and DNS server pool member state when the health monitoring result changed to Inactive.

LB_CHANGE_DSQUOTE_PROBERESULT

Message text	The probe state of (DNS server pool [STRING], DNS server pool member [STRING], port: [USHORT]) template [STRING] was changed to [STRING].
Variable fields	$1: DNS server pool name. $2: DNS server name. $3: Port number. $4: Probe template name. $5: Health monitoring result: Successful or Failed.
Severity level	5
Example	LB/5/LB_CHANGE_DSQUOTE_PROBERESULT: The probe state of (DNS server pool SF, DNS server pool member ds, port: 20) template TEMPLATE was changed to Successful.
Explanation	The probe state of a DNS server pool member changed.
Recommended action	Check the network environment and DNS server pool member state when the health monitoring result changed to Failed.

LB_CHANGE_LG_STATE_ACTION

Message text	The state of link group associated with action [STRING] was changed, primary link group is [STRING], backup link group is [STRING], current link group is [STRING].
Variable fields	$1: LB action name. $2: Primary link group name. $3: Backup link group name. $4: Current link group name.
Severity level	5
Example	LB/5/LB_CHANGE_LG_STATE_ACTION: The state of link group associated with action ACT was changed, primary link group is MF, backup link group is BF, current link group is CF.
Explanation	The state of the link group associated with an LB action changed.
Recommended action	Check whether the availability criteria setting for the link group is changed. If the setting is not changed, check the network environment and link state.

LB_CHANGE_LG_STATUS

Message text	The number of available links in link group [STRING] reached the [STRING] percentage ([STRING]).
Variable fields	$1: Link group name. $2: Percentage type, upper or lower. $3: Percentage value. The value 0% means that no percentage value is configured.
Severity level	5
Example	LB/5/LB_CHANGE_LG_STATUS: The number of available links in link group lg1 reached the upper percentage (90%).
Explanation	This message is generated when the number of available links in a link group reaches the upper or lower percentage value.
Recommended action	Check the network environment and link state when the number of available links in a link group reaches the lower percentage value.

LB_CHANGE_LINK_BUSY_STATUS

Message text	The busy state of link [STRING] was changed to [STRING].
Variable fields	$1: Link name. $2: Link busy state: Busy or Normal.
Severity level	5
Example	LB/5/LB_CHANGE_LINK_BUSYSTATUS: The busy state of link LINK was changed to Normal.
Explanation	The busy state of a link changed.
Recommended action	No action is required.

LB_CHANGE_LINK_CONNNUM_OVER

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of link [STRING] was [UINT], which had reached the upper limit.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Link name. $5: Number of connections on the link.
Severity level	5
Example	LB/5/LB_CHANGE_LINK_CONNNUM_OVER: Chassis:0,Slot:1,CPU:1.The number of connections of link LINK was 100, which had reached the upper limit.
Explanation	The number of connections on a link reached the upper limit.
Recommended action	Check whether the maximum number of connections set by using the **`connection-limit max`** command is proper if this message is generated frequently. If the set value is proper, expand the link capacity.

LB_CHANGE_LINK_CONNRATE_OVER

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of link [STRING] was [UINT] per second, which had reached the upper limit.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Link name. $5: Connection establishment rate on the link.
Severity level	5
Example	LB/5/LB_CHANGE_LINK_CONNRATE_OVER: Chassis:0,Slot:1,CPU:1.The connection rate of link LINK was 100 per second, which had reached the upper limit.
Explanation	The connection establishment rate on a link reached the upper limit.
Recommended action	Check whether the maximum connection establishment rate set by using the **`rate-limit connection`** command is proper if this message is generated frequently. If the set value is proper, expand the link capacity.

LB_CHANGE_LINK_HCSTATUS

Message text	The health state of link [STRING] was changed to [STRING]. Last state was kept for [STRING] seconds.
Variable fields	$1: Link name. $2: Health state of the link: Active or Inactive. $3: Duration for the previous state in seconds.
Severity level	5
Example	LB/5/LB_CHANGE_LINK_HCSTATUS: The health state of link LINK was changed to Active. Last state was kept for 100 seconds.
Explanation	The health state of a link changed, and the link stayed in the previous state for a number of seconds.
Recommended action	Check the network environment and link state when the health state of a link is inactive.

LB_CHANGE_LINK_MEMORY_ALERT

Message text	LB link can't start proximity to probe because memory threshold has been exceeded.
Variable fields	None.
Severity level	5
Example	LB/5/LB_CHANGE_LINK_MEMORY_ALERT: LB link can't start proximity to probe because memory threshold has been exceeded.
Explanation	The device failed to execute proximity testing because the memory threshold had been exceeded.
Recommended action	Check the memory usage.

LB_CHANGE_LINK_PROBERESULT

Message text	The probe state of link [STRING] template [STRING] was changed to [STRING].
Variable fields	$1: Link name. $2: Name of the NQA template used by the health monitoring method. $3: Health monitoring result: Successful or Failed.
Severity level	5
Example	LB/5/LB_CHANGE_LINK_PROBERESULT: The probe state of link CNC template ICMP was changed to Successful.
Explanation	The health monitoring result for a link changed.
Recommended action	Check the network environment and link state if the health monitoring result for a link is Failed.

LB_CHANGE_LINK_SHUTDOWN

Message text	Chassis: [ChassisID],Slot: [SlotID],CPU: [CPUID]. The state of link [STRING] changed to down.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Link name.
Severity level	5
Example	LB/5/LB_CHANGE_LINK_SHUTDOWN: Chassis: 1,Slot: 2,CPU: 1. The state of link LINK changed to down.
Explanation	The state of a link changed to down.
Recommended action	Check the network environment and link state.

LB_CHANGE_LINKQUOTE_CONNNUM_OVER

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID]. The number of connections of link group member ([STRING]-[STRING]) was [USHORT], which had reached the upper limit.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Link group name. $5: Link name. $6: Number of connections.
Severity level	5
Example	LB/5/LB_CHANGE_LINKQUOTE_CONNNUM_OVER: Chassis:1,Slot:1,CPU:1]. The number of connections of link group member (LG- LINK) was 80, which had reached the upper limit.
Explanation	The number of connections on a link group member reached the upper limit.
Recommended action	Check the network environment and link group member state.

LB_CHANGE_LINKQUOTE_CONNRATE_OVER

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID]. The connection rate of link group member ([STRING]-[STRING]) was [USHORT] per second, which had reached the upper limit.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Link group name. $5: Link name. $6: Connection rate.
Severity level	5
Example	LB/5/LB_CHANGE_LINKQUOTE_CONNRATE_OVER: Chassis:1,Slot:1,CPU:2. The connection rate of link group member (LG-LINK) was 80 per second, which had reached the upper limit.
Explanation	The connection rate on a link group member reached the upper limit.
Recommended action	Check the network environment and link group member state.

LB_CHANGE_LINKQUOTE_HCSTATUS

Message text	The health state of (link group [STRING], link [STRING]) was changed to [STRING]. Last state was kept for [ULONG] seconds.
Variable fields	$1: Link group name. $2: Link name. $3: Health state: Active or Inactive. $4: Duration for the previous state in seconds.
Severity level	5
Example	LB/5/LB_CHANGE_LINKQUOTE_HCSTATUS: The health state of (link group LG, link LINK) was changed to Active. Last state was kept for 200 seconds.
Explanation	The health state of a link group member changed.
Recommended action	Check the network environment and link group member state when the health state changed to Inactive.

LB_CHANGE_LINKQUOTE_PROBERESULT

Message text	The probe state of (link group [STRING], link [STRING]) template [STRING] was changed to [STRING].
Variable fields	$1: Link group name. $2: Link name. $3: Probe template name. $4: Health monitoring result: Successful or Failed.
Severity level	5
Example	LB/5/LB_CHANGE_LINKQUOTE_PROBERESULT: The probe state of (link group LG, link LINK) template TEMPLATE was changed to Successful.
Explanation	The health monitoring result of a link group member changed.
Recommended action	Check the network environment and link group member state when the health monitoring result changed to Failed.

LB_CHANGE_READ_WRITE_STATE_VS

Message text	The state of server farm associated with virtual server [STRING] ([STRING], port: [USHORT]) was changed, read server farm is [STRING], write server farm is [STRING], current read-write server farm is [STRING].
Variable fields	$1: Virtual server name. $2: Virtual server address. $3: Port number. $4: Read server farm name. $5: Write server farm name. $6: Health state: Active or Inactive.
Severity level	5
Example	LB/5/ LB_CHANGE_READ_WRITE_STATE_VS: The state of server farm associated with virtual server vs (192.168.10.10, port: 20) was changed, read server farm is rsr, write server farm is rsw, current read-write server farm is Active.
Explanation	The health state of the read server farm and write server farm changed.
Recommended action	None.

LB_CHANGE_RS_CONNNUM_OVER

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of real server [STRING] ([STRING], port: [USHORT]) was [UINT], which had reached the upper limit.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Real server name. $5: Real server address. $6: Port number. $7: Number of connections on the real server.
Severity level	5
Example	LB/5/LB_CHANGE_RS_CONNNUM_OVER: Chassis:0,Slot:1,CPU:1.The number of connections of real server RS (192.168.10.10, port: 20) was 100, which had reached the upper limit.
Explanation	The number of connections on a real server reached the upper limit.
Recommended action	Check whether the maximum number of connections set by using the **`connection-limit max`** command is proper if this message is generated frequently. If the set value is proper, expand the real server capacity.

LB_CHANGE_RS_CONNRATE_OVER

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of real server [STRING] ([STRING], port: [USHORT]) was [UINT] per second, which had reached the upper limit.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Real server name. $5: Real server address. $6: Port number. $7: Connection establishment rate on the real server.
Severity level	5
Example	LB/5/LB_CHANGE_RS_CONNRATE_OVER: Chassis:0,Slot:1,CPU:1.The connection rate of real server RS (192.168.10.10, port: 20) was 100 per second, which had reached the upper limit.
Explanation	The connection establishment rate on a real server reached the upper limit.
Recommended action	Check whether the maximum connection establishment rate set by using the **`rate-limit connection`** command is proper if this message is generated frequently. If the set value is proper, expand the real server capacity.

LB_CHANGE_RS_HCSTATUS

Message text	The health state of real server [STRING] ([STRING], port: [USHORT]) was changed to [STRING]. Last state was kept for [STRING] seconds.
Variable fields	$1: Real server name. $2: Real server address. $3: Port number. $4: Health state of the real server: Active or Inactive. $5: Duration for a state in seconds.
Severity level	5
Example	LB/5/LB_CHANGE_RS_HCSTATUS: The health state of real server RS (192.168.10.10, port: 20) was changed to Active. Last state was kept for 100 seconds.
Explanation	The health state of a real server changed, and the real server stayed in the previous state for a number of seconds.
Recommended action	Check the network environment and real server state when the health state of a real server is inactive.

LB_CHANGE_RS_MEMORY_ALERT

Message text	LB can't start template [STRING] to probe because memory threshold has been exceeded.
Variable fields	$1: Probe template name.
Severity level	5
Example	LB/5/LB_CHANGE_RS_MEMORY_ALERT: LB can't start template TEMPLATE1 to probe because memory threshold has been exceeded.
Explanation	The device failed to execute a probe template for health monitoring because the memory threshold had been exceeded.
Recommended action	Check the memory usage.

LB_CHANGE_RS_MONITORRESULT

Message text	The state of (server farm [STRING], server farm member [STRING], [STRING], port: [UINT16]) monitored by probe template [STRING] was changed to [STRING].
Variable fields	$1: Server farm name. $2: Server farm member name. $3: Real server address. $4: Port number. $5: Probe template name. $6: Probe result: Normal, Busy, or Auto shutdown.
Severity level	5
Example	LB/5/LB_CHANGE_RS_MONITORRESULT: The state of (server farm sf, server farm member rs, 192.168.10.10, port:1) monitored by probe template rst was changed to Auto shutdown
Explanation	The health state of a server farm member changed.
Recommended action	No action is required.

LB_CHANGE_RS_PROBERESULT

Message text	The probe result of real server [STRING] ([STRING], port: [USHORT]) template type [STRING] name [STRING] was changed to [STRING].
Variable fields	$1: Real server name. $2: Real server address. $3: Port number. $4: Type of the NQA template used by the health monitoring method. $5: Name of the NQA template. $6: Health monitoring result: Successful or Failed.
Severity level	5
Example	LB/5/LB_CHANGE_RS_PROBERESULT: The probe state of real server RS (192.168.10.10, port: 20) template type ICMP name t1 was changed to Successful.
Explanation	The health monitoring result for a real server changed.
Recommended action	Check the network environment and real server state if the health monitoring result for a real server is Failed.

LB_CHANGE_RS_SHUTDOWN

Message text	Chassis: [ChassisID],Slot: [SlotID],CPU: [CPUID]. The state of real server [STRING] ([STRING], port: [USHORT]) changed to down.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Real server name. $5: Real server address. $6: Port number.
Severity level	5
Example	LB/5/LB_CHANGE_RS_SHUTDOWN: Chassis: 1,Slot: 1,CPU: 2. The state of real server RS (192.168.10.10, port: 20) changed to down.
Explanation	The state of a real server changed to down.
Recommended action	Check the network environment and real server state.

LB_CHANGE_RSQUOTE_CONNNUM_OVER

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID]. The number of connections of server farm member ([STRING]-[STRING]-[USHORT]) [STRING] was [USHORT], which had reached the upper limit.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Server farm name. $5: Real server name. $6: Port number. $7: Real server address. $8: Number of connections.
Severity level	5
Example	LB/5/LB_CHANGE_RSQUOTE_CONNNUM_OVER: Chassis:1,Slot:1,CPU:2. The number of connections of server farm member (SF-RS-1) 192.168.10.10 was 80, which had reached the upper limit.
Explanation	The number of connections on a server farm member reached the upper limit.
Recommended action	Check the network environment and server farm member state.

LB_RECOVERY_RSQUOTE_CONNNUM

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID]. The number of connections of server farm member ([STRING]-[STRING]-[USHORT]) [STRING] was [USHORT], which had returned to a normal level.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Server farm name. $5: Real server name. $6: Port number. $7: Real server address. $8: Number of connections.
Severity level	5
Example	LB/5/LB_RECOVERY_RSQUOTE_CONNNUM: Chassis:2,Slot:1,CPU:1. The number of connections of server farm member (SF-RS-33) 192.168.10.10 was 20, which had returned to a normal level.
Explanation	The number of connections on a server farm member fell to a normal level.
Recommended action	Check the network environment and server farm member state.

LB_CHANGE_RSQUOTE_CONNRATE_OVER

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of server farm member ([STRING]-[STRING]-[USHORT]) [STRING] was [USHORT] per second, which had reached the upper limit.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Server farm name. $5: Real server name. $6: Port number. $7: Real server address. $8: Connection rate.
Severity level	5
Example	LB/5/LB_CHANGE_RSQUOTE_CONNRATE_OVER: Chassis:1,Slot:2,CPU:1.The connection rate of server farm member (SF-RS-66) 192.168.10.10 was 80 per second, which had reached the upper limit.
Explanation	The connection rate on a server farm member reached the upper limit.
Recommended action	Check the network environment and server farm member state.

LB_CHANGE_RSQUOTE_HCSTATUS

Message text	The health state of (server farm [STRING], server farm member [STRING], [STRING], port:%[USHORT]) was changed to [STRING]. Last state was kept for [ULONG] seconds.
Variable fields	$1: Server farm name. $2: Real server name. $3: Real server address. $4: Port number. $5: Health monitoring result: Active or Inactive. $6: Duration for the previous state in seconds.
Severity level	5
Example	LB/5/LB_CHANGE_RSQUOTE_HCSTATUS: The health state of (server farm SF, server farm member RS, 192.168.10.10, port:33) was changed to Active. Last state was kept for 100 seconds.
Explanation	The health state of a server farm member changed.
Recommended action	Check the network environment and server farm member state when the health state changed to Inactive.

LB_CHANGE_RSQUOTE_PROBERESULT

Message text	The probe state of (server farm [STRING], server farm member [STRING], [STRING], port: [USHORT]) template [STRING] was changed to [STRING].
Variable fields	$1: Server farm name. $2: Real server name. $3: Real server address. $4: Port number. $5: Probe template name. $6: Health monitoring result: Successful or Failed.
Severity level	5
Example	LB/5/ LB_CHANGE_RSQUOTE_PROBERESULT: The probe state of (server farm SF, server farm member RS, 192.168.10.10, port: 20) template TEMPLATE was changed to Successful.
Explanation	The health state of a server farm member changed.
Recommended action	Check the network environment and server farm member state when the health monitoring result changed to Failed.

LB_CHANGE_SF_STATE_ACTION

Message text	The state of server farm associated with action [STRING] was changed, primary server farm is [STRING], backup server farm is [STRING], current server farm is [STRING].
Variable fields	$1: LB action name. $2: Primary server farm name. $3: Backup server farm name. $4: Current server farm name.
Severity level	5
Example	LB/5/LB_CHANGE_SF_STATE_ACTION: The state of server farm associated with action ACT was changed, primary server farm is MF, backup server farm is BF, current server farm is CF.
Explanation	The state of the server farm associated with an LB action changed.
Recommended action	Check whether the availability criteria setting for the server farm is changed. If the setting is not changed, check the network environment and real server state.

LB_CHANGE_SF_STATUS

Message text	The number of available real servers in server farm [STRING] reached the [STRING] percentage ([STRING]).
Variable fields	$1: Server farm name. $2: Percentage type, upper or lower. $3: Percentage value. The value 0% means that no percentage value is configured.
Severity level	5
Example	LB/5/LB_CHANGE_SF_STATUS: The number of available real servers in server farm sf1 reached the lower percentage (10%).
Explanation	This message is generated when the number of available real servers in a server farm reaches the upper or lower percentage value.
Recommended action	Check the network environment and server farm state when the number of available real servers in a server farm reaches the lower percentage value.

LB_CHANGE_VS_CONNNUM_OVER

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of virtual server [STRING] was [UINT], which had reached the upper limit.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Virtual server name. $5: Number of connections on the virtual server.
Severity level	5
Example	LB/5/LB_CHANGE_VS_CONNNUM_OVER: Chassis:0,Slot:1,CPU:1.The number of connections of virtual server RS was 100, which had reached the upper limit.
Explanation	The number of connections on a virtual server reached the upper limit.
Recommended action	Check whether the maximum number of connections set by using the **connection-limit max** command is proper if this message is generated frequently. If the set value is proper, expand the capacity of real servers associated with the virtual server.

LB_CHANGE_VS_CONNRATE_OVER

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of virtual server [STRING] was [UINT] per second, which had reached the upper limit.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Virtual server name. $5: Connection establishment rate on the virtual server.
Severity level	5
Example	LB/5/LB_CHANGE_VS_CONNRATE_OVER: Chassis:0,Slot:1,CPU:1.The connection rate of virtual server VS was 100 per second, which had reached the upper limit.
Explanation	The connection establishment rate on a virtual server reached the upper limit.
Recommended action	Check whether the maximum connection establishment rate set by using the **rate-limit connection** command is proper if this message is generated frequently. If the set value is proper, expand the capacity of real servers associated with the virtual server.

LB_LINK_FLOW

Message text	SIP=[STRING], SPort=[STRING], DIP= [STRING], DPort= [STRING], Proto= [STRING], App= [STRING], Link= [STRING] ([STRING]). SIP=[STRING], SPort=[STRING], DIP= [STRING], DPort= [STRING], Proto= [STRING], App= [STRING], Domain= [STRING], Link= [STRING] ([STRING]).
Variable fields	$1: Source IP address. $2: Source port number. $3: Destination IP address. $4: Destination port number. $5: Protocol. $6: Application name. $7: Domain name. $8: Link name. $9: Outbound next-hop IP address.
Severity level	6
Example	LB/6/LB _LINK_FLOW: SIP=192.168.3.10, SPort=8090, DIP=3.3.3.3, DPort=80, Proto=TCP, App=general_tcp, Link= link1 (6.6.6.6). LB/6/LB _LINK_FLOW: SIP=192.168.3.11, SPort=8080, DIP=2.2.2.2, DPort=80, Proto=TCP, App=http, Domain= www.aaa.com, Link= link2 (6.6.6.2).
Explanation	This message is generated when traffic is forwarded over the link.
Recommended action	No action is required.

LB_LINK_RECOVERFORM_SHUTDOWN

Message text	Chassis: [ChassisID],Slot: [SlotID],CPU: [CPUID]. The shutdown state of link [STRING] changed to normal.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Link name.
Severity level	5
Example	LB/5/ LB_LINK_RECOVERFORM_SHUTDOWN: Chassis: 1,Slot: 2,CPU: 1. The shutdown state of link lk changed to normal.
Explanation	The link changed from down to normal.
Recommended action	No action is required.

LB_LINK_STATE_ACTIVE

Message text	The state of link [STRING] is active.
Variable fields	$1: Link name.
Severity level	5
Example	LB/5/LB_LINK_STATE_ACTIVE: -MDC=1; The state of link lk is active.
Explanation	This message is generated after an IP address is configured, the health monitoring succeeds, or the **undo shutdown** command is executed.
Recommended action	No action is required.

LB_LINK_STATE_INACTIVE

Message text	The state of link [STRING] is inactive.
Variable fields	$1: Link name.
Severity level	5
Example	LB_LINK_STATE_INACTIVE: -MDC=1; The state of link lk is inactive.
Explanation	This message is generated after an IP address is removed from an interface, the health monitoring result changes, or the **shutdown** command is executed.
Recommended action	Check the link configuration and health monitoring configuration.

LB_NAT44_FLOW

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];
Variable fields	$1: Protocol type. $2: Source IP address. $3: Source port number. $4: Source IP address after translation. $5: Source port number after translation. $6: Destination IP address. $7: Destination port number. $8: Destination IP address after translation. $9: Destination port number after translation. $10: Source VPN instance name. $11: Destination VPN instance name.
Severity level	6
Example	LB/6/LB_NAT44_FLOW: Protocol(1001)=UDP;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=20.20.20.20;NATSrcPort(1006)=1024;DstIPAddr(1007)=20.20.20.1;DstPort(1008)=21;NATDstIPAddr(1009)=20.20.20.1;NATDstPort(1010)=21;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;
Explanation	This message is generated when a source or destination IPv4 address is translated into another IPv4 address. This message can only be displayed by executing the **`display logbuffer`** command.
Recommended action	No action is required.

LB_NAT46_FLOW

Message text	Protocol(1001)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPv6Addr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPv6Addr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];
Variable fields	$1: Protocol type. $2: Source IP address. $3: Source port number. $4: Source IP address after translation. $5: Source port number after translation. $6: Destination IP address. $7: Destination port number. $8: Destination IP address after translation. $9: Destination port number after translation. $10: Source VPN instance name. $11: Destination VPN instance name.
Severity level	6
Example	LB/6/LB_NAT46_FLOW: Protocol(1001)=UDP;SrcIPAddr(1003)=20.20.20.1;SrcPort(1004)=1024;NATSrcIPv6Addr(1005)=2002::1;NATSrcPort(1006)=1024;DstIPAddr(1007)=30.30.30.1;DstPort(1008)=21;NATDstIPv6Addr(1009)=3002::1;NATDstPort(1010)=21;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;
Explanation	This message is generated when a source or destination IPv4 address is translated into an IPv6 address. This message can only be displayed by executing the **`display logbuffer`** command.
Recommended action	No action is required.

LB_NAT64_FLOW

Message text	Protocol(1001)=[STRING];SrcIPv6Addr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPv6Addr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];
Variable fields	$1: Protocol type. $2: Source IP address. $3: Source port number. $4: Source IP address after translation. $5: Source port number after translation. $6: Destination IP address. $7: Destination port number. $8: Destination IP address after translation. $9: Destination port number after translation. $10: Source VPN instance name. $11: Destination VPN instance name.
Severity level	6
Example	LB/6/LB_NAT64_FLOW: Protocol(1001)=UDP;SrcIPv6Addr(1003)=1001::1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=20.20.20.1;NATSrcPort(1006)=1024;DstIPv6Addr(1007)=3001::1;DstPort(1008)=21;NATDstIPAddr(1009)=30.30.30.1;NATDstPort(1010)=21;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;
Explanation	This message is generated when a source or destination IPv6 address is translated into an IPv4 address. This message can only be displayed by executing the **`display logbuffer`** command.
Recommended action	No action is required.

LB_NAT66_FLOW

Message text	Protocol(1001)=[STRING];SrcIPv6Addr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPv6Addr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPv6Addr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPv6Addr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];
Variable fields	$1: Protocol type. $2: Source IP address. $3: Source port number. $4: Source IP address after translation. $5: Source port number after translation. $6: Destination IP address. $7: Destination port number. $8: Destination IP address after translation. $9: Destination port number after translation. $10: Source VPN instance name. $11: Destination VPN instance name.
Severity level	6
Example	LB/6/LB_NAT66_FLOW: Protocol(1001)=UDP;SrcIPv6Addr(1003)=1001::1;SrcPort(1004)=1024;NATSrcIPv6Addr(1005)=2002::1;NATSrcPort(1006)=1024;DstIPv6Addr(1007)=3001::1;DstPort(1008)=21;NATDstIPv6Addr(1009)=3002::1;NATDstPort(1010)=21;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;
Explanation	This message is generated when a source or destination IPv6 address is translated into another IPv6 address. This message can only be displayed by executing the **`display logbuffer`** command.
Recommended action	No action is required.

LB_PROTECTION_POLICY_CK (fast log output)

Message text	The virtual server [STRING] detected the visits of user (IP = [STRING], [STRING] = [STRING], URL = [STRING]) exceeding the threshold.
Variable fields	$1: Virtual server name. $2: Source IP address. $3: Cookie name. $4: Cookie value. $5: Protected URL.
Severity level	6
Example	NSFOCUS LB/6/LB _PROTECTION_POLICY_CK: The virtual server vs detected the visits of user (IP = 10.10.10.10, JSESSIONID = A43E0142B4, URL = www.abc.com) exceeding the threshold.
Explanation	This message is generated when the number of times a user accesses a URL exceeds the specified threshold.
Recommended action	No action is required.

LB_PROTECTION_POLICY_IP (fast log output)

Message text	The virtual server [STRING] detected the visits of user (IP = [STRING], URL = [STRING]) exceeding the threshold.
Variable fields	$1: Virtual server name. $2: Source IP address. $3: Protected URL.
Severity level	6
Example	NSFOCUS LB/6/LB _PROTECTION_POLICY_IP: The virtual server vs detected the visits of user (IP = 10.10.10.10, URL = www.abc.com) exceeding the threshold.
Explanation	This message is generated when the number of times a user accesses a URL exceeds the specified threshold.
Recommended action	No action is required.

LB_RECOVERY_LINK_CONNNUM

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of link [STRING] was [UINT], which had returned to a normal level.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Link name. $5: Number of connections on the link.
Severity level	5
Example	LB/5/LB_RECOVERY_LINK_CONNNUM: Chassis:0,Slot:1,CPU:1.The number of connections of link LINK was 100, which had returned to a normal level.
Explanation	The number of connections on a link dropped below the upper limit.
Recommended action	No action is required.

LB_RECOVERY_LINK_CONNRATE

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of link [STRING] was [UINT] per second, which had returned to a normal level.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Link name. $5: Connection establishment rate on the link.
Severity level	5
Example	LB/5/LB_RECOVERY_LINK_CONNRATE: Chassis:0,Slot:1,CPU:1.The connection rate of link LINK was 100 per second, which had returned to a normal level.
Explanation	The connection establishment rate on a link dropped below the upper limit.
Recommended action	No action is required.

LB_RECOVERY_LINKQUOTE_CONNNUM

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of link group member ([STRING]-[STRING]) was [USHORT], which had returned to a normal level.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Link group name. $5: Link name. $6: Number of connections.
Severity level	5
Example	LB/5/LB_RECOVERY_LINKQUOTE_CONNNUM: Chassis:1,Slot:1,CPU:2.The number of connections of link group member (LG-LINK) was 10, which had returned to a normal level.
Explanation	The number of connections on a link group member fell to a normal level.
Recommended action	Check the network environment and link group member state.

LB_RECOVERY_LINKQUOTE_CONNRATE

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID]. The connection rate of link group member ([STRING]- [STRING]) was [USHORT] per second, which had returned to a normal level.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Link group name. $5: Link name. $6: Connection rate.
Severity level	5
Example	LB/5/LB_CHANGE_LINKQUOTE_CONNRATE_RECOVERY: Chassis: 0,Slot:1,CPU:1. The connection rate of link group member (LG- LINK) was 80 per second, which had returned to a normal level.
Explanation	The connection rate on a link group member fell to a normal level.
Recommended action	Check the network environment and link group member state.

LB_RECOVERY_RS_CONNNUM

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of real server [STRING] ([STRING], port: [USHORT]) was [UINT], which had returned to a normal level.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Real server name. $5: Real server address. $6: Port number. $7: Number of connections on the real server.
Severity level	5
Example	LB/5/LB_RECOVERY_RS_CONNNUM: Chassis:0,Slot:1,CPU:1.The number of connections of real server RS (192.168.10.10, port: 20) was 100, which had returned to a normal level.
Explanation	The number of connections on a real server dropped below the upper limit.
Recommended action	No action is required.

LB_RECOVERY_RS_CONNRATE

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of real server [STRING] ([STRING], port: [USHORT]) was [UINT] per second, which had returned to a normal level.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Real server name. $5: Real server address. $6: Port number. $7: Connection establishment rate on the real server.
Severity level	5
Example	LB/5/LB_RECOVERY_RS_CONNRATE: Chassis:0,Slot:1,CPU:1.The connection rate of real server RS (192.168.10.10, port: 20) was 100 per second, which had returned to a normal level.
Explanation	The connection establishment rate on a real server dropped below the upper limit.
Recommended action	No action is required.

LB_RECOVERY_RSQUOTE_CONNRATE

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of server farm member ([STRING]-[STRING]-[USHORT]) [STRING] was [USHORT] per second, which had returned to a normal level.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Server farm name. $5: Real server name. $6: Port number. $7: Real server address. $8: Connection rate.
Severity level	5
Example	LB/5/LB_RECOVERY_RSQUOTE_CONNRATE: Chassis: 1,Slot:1,CPU:1.The connection rate of server farm member (SF-RS-80) 192.168.10.10 was 10 per second, which had returned to a normal level.
Explanation	The connection rate on a server farm member fell to a normal level.
Recommended action	Check the network environment and server farm member state.

LB_RECOVERY_VS_CONNNUM

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The number of connections of virtual server [STRING] ([STRING], port: [USHORT]) was [UINT], which had returned to a normal level.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Virtual server name. $5: Real server address. $6: Port number. $7: Number of connections on the virtual server.
Severity level	5
Example	LB/5/LB_RECOVERY_VS_CONNNUM: Chassis:0,Slot:1,CPU:1.The number of connections of virtual server VS (192.168.10.10, port: 20) was 100, which had returned to a normal level.
Explanation	The number of connections on a virtual server dropped below the upper limit.
Recommended action	No action is required.

LB_RECOVERY_VS_CONNRATE

Message text	Chassis:[ChassisID],Slot:[SlotID],CPU:[CPUID].The connection rate of virtual server [STRING] ([STRING], port: [USHORT]) was [UINT] per second, which had returned to a normal level.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Virtual server name. $5: Real server address. $6: Port number. $7: Connection establishment rate on the virtual server.
Severity level	5
Example	LB/5/LB_RECOVERY_VS_CONNRATE: Chassis:0,Slot:1,CPU:1.The connection rate of virtual server VS (192.168.10.10, port: 20) was 100 per second, which had returned to a normal level.
Explanation	The connection establishment rate on a virtual server dropped below the upper limit.
Recommended action	No action is required.

LB_RS_RECOVERFORM_SHUTDOWN

Message text	Chassis: [ChassisID],Slot: [SlotID],CPU: [CPUID]. The shutdown state of real server [STRING] ([STRING], port: [USHORT]) changed to normal.
Variable fields	$1: IRF member ID. $2: Slot number of the card. $3: CPU number. $4: Real server name. $5: Real server address. $6: Port number.
Severity level	5
Example	LB/5/LB_RS_RECOVERFORM_SHUTDOWN: Chassis: 1,Slot: 1,CPU: 2. The shutdown state of real server rs1 (192.168.10.10, port: 20) changed to normal.
Explanation	The real server changed from down to normal.
Recommended action	No action is required.

LDP messages

This section contains LDP messages.

LDP_MPLSLSRID_CHG

Message text	Please reset LDP sessions if you want to make the new MPLS LSR ID take effect.
Variable fields	N/A
Severity level	5
Example	LDP/5/LDP_MPLSLSRID_CHG: -MDC=1; Please reset LDP sessions if you want to make the new MPLS LSR ID take effect.
Explanation	If you configure an LDP LSR ID by using the **lsr-id** command in LDP view or LDP-VPN instance view, LDP uses the LDP LSR ID. Otherwise, LDP uses the MPLS LSR ID configured by the **mpls lsr-id** command. This message is sent when the following situations occur: • No LDP LSR ID is configured by using the **lsr-id** command. • The MPLS LSR ID is modified.
Recommended action	**155.** Execute the **display mpls ldp parameter** command to display the LSR ID. **156.** Verify that the LSR ID is the same as the configured MPLS LSR ID. If they are not the same, reset LDP sessions by executing the **reset mpls ldp** command.

LDP_SESSION_CHG

Message text	Session ([STRING], [STRING]) is [STRING].
Variable fields	$1: Peer's LDP ID. Value 0.0.0.0:0 indicates that the peer's LDP ID cannot be obtained. $2: VPN instance's name. Value **public instance** indicates that the session belongs to the public network. $3: State of the session, **up** or **down**. When the state is **down**, this field also displays the reason for the down state error. Possible reasons include: • interface not operational. • MPLS disabled on interface. • LDP disabled on interface. • LDP auto-configure disabled on interface. • VPN instance changed on interface. • LDP instance deleted. • targeted peer deleted. • L2VPN disabled targeted peer. • TE tunnel disabled targeted peer. • session protection disabled targeted peer. • process deactivated. • failed to receive the initialization message. • graceful restart reconnect timer expired. • failed to recover adjacency by NSR. • failed to upgrade session by NSR. • closed the GR session. • keepalive hold timer expired. • adjacency hold timer expired. • session reset manually. • TCP connection down. • received a fatal notification message. • internal error. • memory in critical state. • transport address changed on interface.
Severity level	5
Example	LDP/5/LDP_SESSION_CHG: Session (22.22.22.2:0, public instance) is up. LDP/5/LDP_SESSION_CHG: Session (22.22.22.2:0, VPN instance: vpn1) is down (hello hold timer expired).
Explanation	The session state changed.
Recommended action	When the session state is up, no action is required. When the session state is down, check the interface state, link state, and other configurations depending on the reason displayed.

LDP_SESSION_GR

Message text	Session ([STRING], [STRING]): ([STRING]).
Variable fields	$1: Peer's LDP ID. Value 0.0.0.0:0 indicates that the peer's LDP ID cannot be obtained. $2: VPN instance's name. Value **public instance** indicates that the session belongs to the public network. $3: State of the session graceful restart: o Start reconnection. o Reconnection failed. o Start recovery. o Recovery completed.
Severity level	5
Example	LDP/5/LDP_SESSION_GR: Session (22.22.22.2:0, VPN instance: vpn1): Start reconnection.
Explanation	State of the session graceful restart. When a GR-capable LDP session is down, the LDP GR started. This message is generated during the GR of the LDP session, indicating the current GR state.
Recommended action	Check for the reason of session graceful restart, which can be obtained from the LDP_SESSION_CHG log message. When the graceful restart state **Reconnection failed** is displayed, verify the interface state, link state, and other configurations according to the reason for the session graceful restart. No action is required for other graceful restart states.

LDP_SESSION_SP

Message text	Session ([STRING], [STRING]): ([STRING]).
Variable fields	$1: Peer's LDP ID. Value 0.0.0.0:0 indicates that the peer's LDP ID cannot be obtained. $2: VPN instance's name. Value **public instance** indicates that the session belongs to the public network. $3: State of the session protection: o Hold up the session. o Session recovered successfully. o Session recovery failed.
Severity level	5
Example	LDP/5/LDP_SESSION_SP: Session (22.22.22.2:0, VPN instance: vpn1): Hold up the session.
Explanation	When the last link adjacency of the session was lost, session protection started. This message is generated during the session protection process, indicating the current session protection state.
Recommended action	Verify the interface state and link state.

LIPC messages

This section contains LIPC messages.

PORT_CHANGE

Message text	STCP: Node where the listening port number [INTGER] (MDC: [INTGER] VRF: [INTGER]) resides changed from LIP [INTGER] to LIP [INTGER].
Variable fields	$1: LIPC global port number. $2: Name of the MDC where the LIPC global port resides. $3: Name of the VRF to which the LIPC global port belongs. $4: Name of the old LIPC node where the LIPC global port resides. $5: Name of the new LIPC node where the LIPC global port resides.
Severity level	5
Example	LIPC/5/PORT_CHANGE: STCP: Node where the listening port number 620 (MDC: 1 VRF: 1) resides changed from LIP 1 to LIP 3.
Explanation	STCP assigns an LIPC global port number as a listening port number to each service module as requested. Typically, a service module listens to the port number only on the LIPC node where the port has been requested. This message is generated if the service module listens to the port number on a different LIPC node. STCP will move the port number from the old LIPC node to the new node.
Recommended action	No action is required.

LLDP messages

This section contains LLDP messages.

LLDP_CREATE_NEIGHBOR

Message text	[STRING] agent new neighbor created on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
Variable fields	$1: Agent type. $2: Port name. $3: Port ifIndex. $4: Neighbor's chassis ID. $5: Neighbor's port ID.
Severity level	6
Example	LLDP/6/LLDP_CREATE_NEIGHBOR: Nearest bridge agent new neighbor created on port Ten-GigabitEthernet10/0/15 (IfIndex 599), neighbor's chassis ID is 3822-d666-ba00, port ID is GigabitEthernet6/0/5.
Explanation	The port received an LLDP message from a new neighbor.
Recommended action	No action is required.

LLDP_DELETE_NEIGHBOR

Message text	[STRING] agent neighbor deleted on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
Variable fields	$1: Agent type. $2: Port name. $3: Port ifIndex. $4: Neighbor's chassis ID. $5: Neighbor's port ID.
Severity level	6
Example	LLDP/6/LLDP_DELETE_NEIGHBOR: Nearest bridge agent neighbor deleted on port Ten-GigabitEthernet10/0/15 (IfIndex 599), neighbor's chassis ID is 3822-d666-ba00, port ID is GigabitEthernet6/0/5.
Explanation	The port received a deletion message when a neighbor was deleted.
Recommended action	No action is required.

LLDP_LESS_THAN_NEIGHBOR_LIMIT

Message text	The number of [STRING] agent neighbors maintained by port [STRING] (IfIndex [UINT32]) is less than [UINT32], and new neighbors can be added.
Variable fields	$1: Agent type. $2: Port name. $3: Port ifIndex. $4: Maximum number of neighbors a port can maintain.
Severity level	6
Example	LLDP/6/LLDP_LESS_THAN_NEIGHBOR_LIMIT: The number of nearest bridge agent neighbors maintained by port Ten-GigabitEthernet10/0/15 (IfIndex 599) is less than 5, and new neighbors can be added.
Explanation	New neighbors can be added for the port because the limit has not been reached.
Recommended action	No action is required.

LLDP_NEIGHBOR_AGE_OUT

Message text	[STRING] agent neighbor aged out on port [STRING] (IfIndex [UINT32]), neighbor's chassis ID is [STRING], port ID is [STRING].
Variable fields	$1: Agent type. $2: Port name. $3: Port ifIndex. $4: Neighbor's chassis ID. $5: Neighbor's port ID.
Severity level	5
Example	LLDP/5/LLDP_NEIGHBOR_AGE_OUT: Nearest bridge agent neighbor aged out on port Ten-GigabitEthernet10/0/15 (IfIndex599), neighbor's chassis ID is 3822-d666-ba00, port ID is GigabitEthernet6/0/5.
Explanation	This message is generated when the port failed to receive LLDPDUs from the neighbor within a certain period of time.
Recommended action	Verify the link status or the receive/transmit status of LLDP on the peer.

LLDP_NEIGHBOR_AP_RESET

Message text	The neighboring AP of the [STRING] agent on port [STRING] (IfIndex [UINT32]) was restarted due to aging.
Variable fields	$1: Agent type. $2: Port name. $3: Port ifIndex.
Severity level	5
Example	LLDP/5/LLDP_NEIGHBOR_AP_RESET: The neighboring AP of the nearest bridge agent on port GigabitEthernet1/0/1 (IfIndex 599) was restarted due to aging.
Explanation	A neighboring AP aged out and was restarted.
Recommended action	No action is required.

LLDP_PVID_INCONSISTENT

Message text	PVID mismatch discovered on [STRING] (PVID [UINT32]), with [STRING] [STRING] (PVID [STRING]).
Variable fields	$1: Port name. $2: VLAN ID. $3: System name. $4: Port name. $5: VLAN ID.
Severity level	5
Example	LLDP/5/LLDP_PVID_INCONSISTENT: MDC=1; PVID mismatch discovered on Ten-GigabitEthernet0/2/6 (PVID 1), with Ten-GigabitEthernet0/2/7 (PVID 500).
Explanation	This message is generated when the PVID on the peer is different from the PVID of the local interface.
Recommended action	Configure the same PVID for the local and peer interfaces.

LLDP_REACH_NEIGHBOR_LIMIT

Message text	The number of [STRING] agent neighbors maintained by the port [STRING] (IfIndex [UINT32]) has reached [UINT32], and no more neighbors can be added.
Variable fields	$1: Agent type. $2: Port name. $3: Port ifIndex. $4: Maximum number of neighbors a port can maintain.
Severity level	5
Example	LLDP/5/LLDP_REACH_NEIGHBOR_LIMIT: The number of nearest bridge agent neighbors maintained by the port Ten-GigabitEthernet10/0/15 (IfIndex 599) has reached 5, and no more neighbors can be added.
Explanation	This message is generated when the port with its maximum number of neighbors reached received an LLDP packet.
Recommended action	No action is required.

LOAD messages

This section contains load management messages.

BOARD_LOADING

Message text	Board in chassis [INT32] slot [INT32] is loading software images.
Variable fields	$1: Chassis ID. $2: Slot ID.
Severity level	4
Example	LOAD/4/BOARD_LOADING: Board in chassis 1 slot 5 is loading software images.
Explanation	The card is loading software images during the boot process.
Recommended action	No action is required.

LOAD_FAILED

Message text	Board in chassis [INT32] slot [INT32] failed to load software images.
Variable fields	$1: Chassis ID. $2: Slot ID.
Severity level	3
Example	LOAD/3/LOAD_FAILED: Board in chassis 1 slot 5 failed to load software images.
Explanation	The card failed to load software images during the boot process.
Recommended action	**157.** Execute the **`display boot-loader`** command to identify the startup software images. **158.** Execute the **`dir`** command to verify that the startup software images exist. If the startup software images do not exist or are damaged, re-upload the software images to the device or set another one as the startup software images. **159.** If the problem persists, contract NSFOCUS Support.

LOAD_FINISHED

Message text	Board in chassis [INT32] slot [INT32] has finished loading software images.
Variable fields	$1: Chassis ID. $2: Slot ID.
Severity level	5
Example	LOAD/5/LOAD_FINISHED: Board in chassis 1 slot 5 has finished loading software images.
Explanation	The card has finished loading software images.
Recommended action	No action is required.

LOGIN messages

This section contains login messages.

LOGIN_ACCOUNTING_FAILED

Message text	Accounting failed for user [STRING] on [STRING] line.
Variable fields	$1: Username. $2: Line type.
Severity level	5
Example	LOGIN/5/LOGIN_ACCOUNTING_FAILED: Accounting failed for user **a1** on VTY line.
Explanation	Accounting failed for a user.
Recommended action	Verify that the accounting configuration for the user is correct.

LOGIN_AUTHORIZATION_FAILED

Message text	Authorization failed for user [STRING] on [STRING] line.
Variable fields	$1: Username. $2: Line type.
Severity level	5
Example	LOGIN/5/LOGIN_AUTHORIZATION_FAILED: Authorization failed for user **a1** on VTY line.
Explanation	Authorization failed for a user.
Recommended action	Verify that the authorization configuration for the user is correct.

LOGIN_FAILED

Message text	[STRING] failed to login from [STRING].
Variable fields	$1: Username. $2: Line name or IP address.
Severity level	5
Example	LOGIN/5/LOGIN_FAILED: TTY failed to log in from console0. LOGIN/5/LOGIN_FAILED: usera failed to log in from 192.168.11.22.
Explanation	A login attempt failed.
Recommended action	No action is required.

LOGIN_ INVALID_USERNAME_PWD

Message text	Invalid username or password from [STRING].
Variable fields	$1: User line name and user IP address.
Severity level	5
Example	LOGIN/5/LOGIN_INVALID_USERNAME_PWD: Invalid username or password from console0. LOGIN/5/LOGIN_INVALID_USERNAME_PWD: Invalid username or password from 192.168.11.22.
Explanation	A user entered an invalid username or password.
Recommended action	No action is required.

LOGIN_PASSWORD_CHECK_FAILED

Message text	The password of user [STRING] failed password control check on [STRING] line.
Variable fields	$1: Username. $2: Line type.
Severity level	5
Example	LOGIN/5/LOGIN_PASSWORD_CHECK_FAILED: The password of user **a1** failed password control check on VTY line.
Explanation	A password failed password control check.
Recommended action	**160.** Verify that the password control-related .dat files are available. **161.** Verify that the password meets the requirements of the password control feature.

LOGIN_RECORD_OBTAIN_FAILED

Message text	Failed to obtain login history records of user [STRING] on [STRING] line.
Variable fields	$1: Username. $2: Line type.
Severity level	5
Example	LOGIN/5/LOGIN_RECORD_OBTAIN_FAILED: Failed to obtain login history records of user **a1** on VTY line.
Explanation	The system failed to obtain the login history records of a user.
Recommended action	Contact NSFOCUS Support.

LPDT messages

This section contains loop detection messages.

LPDT_LOOPED

Message text	Loopback exists on [STRING].
Variable fields	$1: Port name.
Severity level	4
Example	LPDT/4/LPDT_LOOPED: Loopback exists on Ethernet 6/4/2.
Explanation	The first intra-VLAN loop was detected on a port.
Recommended action	Check the links and configuration on the device for the loop, and remove the loop.

LPDT_RECOVERED

Message text	Loopback on [STRING] recovered.
Variable fields	$1: Port name.
Severity level	5
Example	LPDT/5/LPDT_RECOVERED: Loopback on Ethernet 6/4/1 recovered.
Explanation	All intra-VLAN loops on a port were removed.
Recommended action	No action is required.

LPDT_VLAN_LOOPED

Message text	Loopback exists on [STRING] in VLAN [UINT16].
Variable fields	$1: Port name. $2: VLAN ID.
Severity level	4
Example	LPDT/4/LPDT_VLAN_LOOPED: Loopback exists on Ethernet6/4/1 in VLAN 1.
Explanation	A loop in a VLAN was detected on a port.
Recommended action	Check the links and configurations in the VLAN for the loop, and remove the loop.

LPDT_VLAN_RECOVERED

Message text	Loopback on [STRING] in VLAN [UINT16] recovered.
Variable fields	$1: Port name. $2: VLAN ID.
Severity level	5
Example	LPDT/5/LPDT_RECOVERED: Loopback on Ethernet6/4/1 in VLAN 1 recovered.
Explanation	A loop in a VLAN was removed on a port.
Recommended action	No action is required.

LS messages

This section contains Local Server messages.

LOCALSVR_PROMPTED_CHANGE_PWD

Message text	Please change the password of [STRING] [STRING], because [STRING].
Variable fields	$1: Password type: ○ **device management user**. ○ **user line**. ○ **user line class**. $2: Username, user line number, or user line class number. $3: Reason for password change: ○ the current password is a weak-password. ○ the current password is the default password. ○ it is the first login of the current user or the password had been reset. ○ the password had expired.
Severity level	6
Example	LOCALSVR/6/LOCALSVR_PROMPTED_CHANGE_PWD: Please change the password of device management user hhh, because the current password is a weak password.
Explanation	The device generated a log message to prompt a user to change the password of the user, user line, or user line class. The device will generate such a log message every 24 hours after the user logs in to the device if the password does not meet the password control requirements.
Recommended action	Change the user password as required: • If scheme authentication is used, change the local password of the user. • If password authentication is used, change the authentication password of the user line or user line class for the user.

LS_ADD_USER_TO_GROUP

Message text	Admin [STRING] added user [STRING] to group [STRING].
Variable fields	$1: Admin name. $2: Username. $3: User group name.
Severity level	4
Example	LS/4/LS_ADD_USER_TO_GROUP: Admin admin added user user1 to group group1.
Explanation	The administrator added a user into a user group.
Recommended action	No action is required.

LS_AUTHEN_FAILURE

Message text	User [STRING] from [STRING] failed authentication. [STRING]
Variable fields	$1: Username. $2: IP address. $3: Failure reason: ○ User not found. ○ Password verified failed. ○ User not active. ○ Access type mismatch. ○ Binding attribute is failed. ○ User in blacklist.
Severity level	5
Example	LS/5/LS_AUTHEN_FAILURE: User cwf@system from 192.168.0.22 failed authentication. "User not found."
Explanation	The local server rejected a user's authentication request.
Recommended action	No action is required.

LS_AUTHEN_SUCCESS

Message text	User [STRING] from [STRING] was authenticated successfully.
Variable fields	$1: Username. $2: IP address.
Severity level	6
Example	LS/6/LS_AUTHEN_SUCCESS: User cwf@system from 192.168.0.22 was authenticated successfully.
Explanation	The local server accepted a user's authentication request.
Recommended action	No action is required.

LS_DEL_USER_FROM_GROUP

Message text	Admin [STRING] delete user [STRING] from group [STRING].
Variable fields	$1: Admin name. $2: Username. $3: User group name.
Severity level	4
Example	LS/4/LS_DEL_USER_FROM_GROUP: Admin admin delete user user1 from group group1.
Explanation	The administrator deleted a user from a user group.
Recommended action	No action is required.

LS_DELETE_PASSWORD_FAIL

Message text	Failed to delete the password for user [STRING].
Variable fields	$1: Username.
Severity level	4
Example	LS/4/LS_DELETE_PASSWORD_FAIL: Failed to delete the password for user abcd.
Explanation	Failed to delete the password for a user.
Recommended action	Check the file system for errors.

LS_PWD_ADDBLACKLIST

Message text	User [STRING] was added to the blacklist due to multiple login failures, [STRING].
Variable fields	$1: Username. $2: Options include: ○ but could make other attempts. ○ and is permanently blocked. ○ and was temporarily blocked for [UINT32] minutes.
Severity level	4
Example	LS/4/LS_PWD_ADDBLACKLIST: User user1 was added to the blacklist due to multiple login failures, but could make other attempts.
Explanation	A user was added to the blacklist because of multiple login failures.
Recommended action	Check the user's password.

LS_PWD_CHGPWD_FOR_AGEDOUT

Message text	User [STRING] changed the password because it was expired.
Variable fields	$1: User name.
Severity level	4
Example	LS/4/LS_PWD_CHGPWD_FOR_AGEDOUT: User aaa changed the password because it was expired.
Explanation	A user changed the password because the password expired.
Recommended action	No action is required.

LS_PWD_CHGPWD_FOR_AGEOUT

Message text	User [STRING] changed the password because it was about to expire.
Variable fields	$1: Username.
Severity level	4
Example	LS/4/LS_PWD_CHGPWD_FOR_AGEOUT: User aaa changed the password because it was about to expire.
Explanation	A user changed the password because the password is about to expire.
Recommended action	No action is required.

LS_PWD_CHGPWD_FOR_COMPOSITION

Message text	User [STRING] changed the password because it had an invalid composition.
Variable fields	$1: Username.
Severity level	4
Example	LS/4/LS_PWD_CHGPWD_FOR_COMPOSITION: User aaa changed the password because it had an invalid composition.
Explanation	A user changed the password because it had an invalid composition.
Recommended action	No action is required.

LS_PWD_CHGPWD_FOR_FIRSTLOGIN

Message text	User [STRING] changed the password at the first login.
Variable fields	$1: Username.
Severity level	4
Example	LS/4/LS_PWD_CHGPWD_FOR_FIRSTLOGIN: User aaa changed the password at the first login.
Explanation	A user changed the password at the first login.
Recommended action	No action is required.

LS_PWD_CHGPWD_FOR_LENGTH

Message text	User [STRING] changed the password because it was too short.
Variable fields	$1: Username.
Severity level	4
Example	LS/4/LS_PWD_CHGPWD_FOR_LENGTH: User aaa changed the password because it was too short.
Explanation	A user changed the password because it was too short.
Recommended action	No action is required.

LS_PWD_FAILED2WRITEPASS2FILE

Message text	Failed to write the password records to file.
Variable fields	N/A
Severity level	4
Example	LS/4/LS_PWD_FAILED2WRITEPASS2FILE: Failed to write the password records to file.
Explanation	Failed to write the password records to file.
Recommended action	No action is required.

LS_PWD_MODIFY_FAIL

Message text	Admin [STRING] from [STRING] could not modify the password for user [STRING], because [STRING].
Variable fields	$1: Admin name. $2: IP address. $3: Username. $4: Failure reason: ○ **old password is incorrect**—The old password is incorrect. ○ **password is too short**—The new password is too short. ○ **password has not minimum different chars**—The new password does not have enough number of different characters (a minimum of four different characters). ○ **invalid password composition**—The types and length of characters in the new password do not meet the password composition requirements. ○ **password has repeated chars**—The new password has three or more consecutive repeating characters. ○ **password contains username**—The new password includes the username. ○ **new password must be different from any previous password by a minimum of four chars**—The new password must be different from the passwords stored in the history records by a minimum of four characters. ○ **new password must be different from old password by a minimum of four chars**—The new password must be different from the old password by a minimum of four characters. ○ **password used already**—The new password is the same as the old password or a history password. ○ **password is in update-wait time**—The password has been modified within a minimum password update interval. ○ **entered passwords did not match**—The confirm password is inconsistent with the new password. ○ **unknown error**—Unknown error.
Severity level	4
Example	LS/4/LS_PWD_MODIFY_FAIL: Admin admin from 1.1.1.1 could not modify the password for user user1, because passwords do not match.
Explanation	An administrator failed to modify a user's password.
Recommended action	No action is required.

LS_PWD_MODIFY_SUCCESS

Message text	Admin [STRING] from [STRING] modify the password for user [STRING] successfully.
Variable fields	$1: Admin name. $2: IP address. $3: Username.
Severity level	6
Example	LS/6/LS_PWD_MODIFY_SUCCESS: Admin admin from 1.1.1.1 modify the password for user abc successfully.
Explanation	An administrator successfully changed a user's password.
Recommended action	No action is required.

LS_REAUTHEN_FAILURE

Message text	User [STRING] from [STRING] failed reauthentication.
Variable fields	$1: Username. $2: IP address.
Severity level	5
Example	LS/5/LS_REAUTHEN_FAILURE: User abcd from 1.1.1.1 failed reauthentication.
Explanation	A user failed reauthentication because the old password entered for reauthentication is invalid.
Recommended action	Check the old password.

LS_UPDATE_PASSWORD_FAIL

Message text	Failed to update the password for user [STRING].
Variable fields	$1: Username.
Severity level	4
Example	LS/4/LS_UPDATE_PASSWORD_FAIL: Failed to update the password for user abc.
Explanation	Failed to update the password for a user.
Recommended action	Check the file system for errors.

LS_USER_CANCEL

Message text	User [STRING] from [STRING] cancelled inputting the password.
Variable fields	$1: Username. $2: IP address.
Severity level	5
Example	LS/5/LS_USER_CANCEL: User 1 from 1.1.1.1 cancelled inputting the password.
Explanation	The user cancelled inputting the password or did not input the password in 90 seconds.
Recommended action	No action is required.

LS_USER_PASSWORD_EXPIRE

Message text	User [STRING]'s login idle timer timed out.
Variable fields	$1: Username.
Severity level	5
Example	LS/5/LS_USER_PASSWORD_EXPIRE: User 1's login idle timer timed out.
Explanation	The login idle time for a user expired.
Recommended action	No action is required.

LS_USER_ROLE_CHANGE

Message text	Admin [STRING] [STRING] user role [STRING] for [STRING].
Variable fields	$1: Admin name. $2: Admin operation, which can be **added** or **deleted**. $3: User role. $4: Username.
Severity level	4
Example	LS/4/LS_USER_ROLE_CHANGE: Admin admin added user role network-admin for abcd.
Explanation	The administrator added a user role for a user.
Recommended action	No action is required.

LSPV messages

This section contains LSP verification messages.

LSPV_PING_STATIS_INFO

Message text	Ping statistics for [STRING]: [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packets loss, round-trip min/avg/max = [UINT32]/[UINT32]/[UINT32] ms.
Variable fields	$1: FEC. $2: Number of echo requests sent. $3: Number of echo replies received. $4: Percentage of the non-replied packets to the total requests. $5: Minimum round-trip delay. $6: Average round-trip delay. $7: Maximum round-trip delay.
Severity level	6
Example	LSPV/6/LSPV_PING_STATIS_INFO: Ping statistics for FEC 192.168.1.1/32: 5 packets transmitted, 5 packets received, 0.0% packets loss, round-trip min/avg/max = 1/2/5 ms.
Explanation	Ping statistics for an LSP tunnel or a PW. This message is generated when the **ping mpls** command is executed.
Recommended action	If no reply is received, verify the connectivity of the LSP tunnel or the PW.

MAC messages

This section contains MAC messages.

MAC_NOTIFICATION

Message text	Message format 1: MAC address [STRING] in VLAN [UNIT32] has moved from port [STRING] to port [STRING] for [UNIT32] times. Message format 2: MAC address [STRING] in VSI [STRING] has moved from [STRING] service-instance [UNIT32] to [STRING] service-instance [UNIT32] for [UNIT32] times.
Variable fields	Message format 1: $1: MAC address. $2: VLAN ID. $3: Interface name. $4: Interface name. $5: Number of MAC address moves. Message format 2: $1: MAC address. $2: VSI name. $3: Interface name. $4: Ethernet service instance ID. $5: Interface name. $6: Ethernet service instance ID. $7: Number of MAC address moves.
Severity level	4
Example	Message format 1: MAC/4/MAC_NOTIFICATION: MAC address 0000-0012-0034 in VLAN 500 has moved from port GE1/0/1 to port GE1/0/2 for 1 times Message format 2: MAC/4/MAC_NOTIFICATION: MAC address 0010-9400-0002 in VSI vpna has moved from Twenty-FiveGigE1/0/1 service-instance 40 to Twenty-FiveGigE1/0/3 service-instance 30 for 152499 times.
Explanation	A MAC address moved between two interfaces or Ethernet service instances.
Recommended action	No action is required.

MAC_TABLE_FULL_GLOBAL

Message text	The number of MAC address entries exceeded the maximum number [UINT32].
Variable fields	$1: Maximum number of MAC addresses.
Severity level	4
Example	MAC/4/MAC_TABLE_FULL_GLOBAL: The number of MAC address entries exceeded the maximum number 1024.
Explanation	The number of entries in the global MAC address table exceeded the maximum number supported by the table.
Recommended action	No action is required.

MAC_TABLE_FULL_PORT

Message text	The number of MAC address entries exceeded the maximum number [UINT32] for interface [STRING].
Variable fields	$1: Maximum number of MAC addresses. $2: Interface name.
Severity level	4
Example	MAC/4/MAC_TABLE_FULL_PORT: The number of MAC address entries exceeded the maximum number 1024 for interface GigabitEthernet2/0/32.
Explanation	The number of entries in the MAC address table for an interface exceeded the maximum number supported by the table.
Recommended action	No action is required.

MAC_TABLE_FULL_VLAN

Message text	The number of MAC address entries exceeded the maximum number [UINT32] in VLAN [UINT32].
Variable fields	$1: Maximum number of MAC addresses. $2: VLAN ID.
Severity level	4
Example	MAC/4/MAC_TABLE_FULL_VLAN: The number of MAC address entries exceeded the maximum number 1024 in VLAN 2.
Explanation	The number of entries in the MAC address table for a VLAN exceeded the maximum number supported by the table.
Recommended action	No action is required.

MACA messages

This section contains MAC authentication messages.

MACA_ENABLE_NOT_EFFECTIVE

Message text	The MAC authentication feature is enabled but is not effective on interface [STRING].
Variable fields	$1: Interface type and number.
Severity level	3
Example	MACA/3/MACA_ENABLE_NOT_EFFECTIVE: The MAC authentication feature is enabled but is not effective on interface Ethernet3/1/2.
Explanation	MAC authentication configuration does not take effect on an interface, because the interface does not support MAC authentication.
Recommended action	**162.** Disable MAC authentication on the interface. **163.** Reconnect the connected devices to another interface that supports MAC authentication. **164.** Enable MAC authentication on the new interface.

MACA_LOGIN_FAILURE

		-IfName=[STRING]-MACAddr=[STRING]-VLANId=[STRING]-UserName=[STRING]-UserNameFormat=[STRING]; The user failed the MAC address authentication. Reason: [STRING].
		$1: Interface type and number. $2: MAC address. $3: VLAN ID. $4: Username. $5: User account format: o **Fixed**—Shared user account. o **MAC address**—MAC-based user account. $6: Failure cause: o Authorization Mac-Address process failed. o Authorization VLAN process failed. o Authorization ACL process failed. o Authorization UserProfile process failed. o Authentication process failed.
		6
		MACA/6/MACA_LOGIN_FAILURE: -IfName=GigabitEthernet1/0/1-MACAddr=0000-0000-0001-VLANId=1-UserName=0000-0000-0001-UserNameFormat=MAC address; The user failed the MAC address authentication. Reason: Authorization VLAN process failed.
		The user failed MAC authentication.

	Resolve the issue depending on the failure cause.

MACA_LOGIN_SUCC

		-IfName=[STRING]-MACAddr=[STRING]-AccessVLANId=[STRING]-AuthorizationVLANID=[STRING]-UserName=[STRING]-UserNameFormat=[STRING]; The user passed MAC address authentication and got online successfully.
		$1: Interface type and number. $2: MAC address. $3: ID of the VLAN through which the user accesses the device. $4: Authorization VLAN ID. $5: Username. $6: User account format: o **Fixed**—Shared user account. o **MAC address**—MAC-based user account.
		6
		MACA/6/MACA_LOGIN_SUCC:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-AccessVLANId=444-AuthorizationVLANID=444-UserName=00-10-84-00-22-b9-UserNameFormat=MAC address; The user passed MAC address authentication and got online successfully.
		The user passed MAC authentication.

	No action is required.

MACA_LOGOFF

	-IfName=[STRING]-MACAddr=[STRING]-VLANId=[STRING]-UserName=[STRING]-UserNameFormat=[STRING]; Session of the MAC-AUTH user was terminated.
	$1: Interface type and number. $2: MAC address. $3: VLAN ID. $4: Username. $5: User account format: o **Fixed**—Shared user account. o **MAC address**—MAC-based user account.
	6
	MACA/6/MACA_LOGOFF:-IfName=GigabitEthernet1/0/4-MACAddr=0010-8400-22b9-VLANId=444-UserName=00-10-84-00-22-b9-UserNameFormat=MAC address; Session of the MAC-AUTH user was terminated.
	The MAC authentication user was logged off.

	Resolve the issue depending on the logoff cause. If the logoff was requested by the user, no action is required.

MACSEC messages

This section contains MACsec messages.

MACSEC_MKA_KEEPALIVE_TIMEOUT

Message text	The live peer with SCI [STRING] and CKN [STRING] aged out on interface [STRING].
Variable fields	$1: SCI. $2: CKN. $3: Interface name.
Severity level	4
Example	MACSEC/4/MACSEC_MKA_KEEPALIVE_TIMEOUT: The live peer with SCI 00E00100000A0006 and CKN 80A0EA0CB03D aged out on interface GigabitEthernet1/0/1.
Explanation	A live peer aged out on an interface, because the local participant had not received any MKA packets from the peer before the keepalive timer expired. The local participant removed the peer information from the port.
Recommended action	Check the link between the local participant and the live peer for link failure. If the link is down, recover the link.

MACSEC_MKA_PRINCIPAL_ACTOR

Message text	The actor with CKN [STRING] became principal actor on interface [STRING].
Variable fields	$1: CKN. $2: Interface name.
Severity level	6
Example	MACSEC/6/MACSEC_MKA_PRINCIPAL_ACTOR: The actor with CKN 80A0EA0CB03D became principal actor on interface GigabitEthernet1/0/1.
Explanation	The actor with the highest key server priority became the principal actor.
Recommended action	No action is required.

MACSEC_MKA_SAK_REFRESH

Message text	The SAK has been refreshed on interface [STRING].
Variable fields	$1: Interface name.
Severity level	6
Example	MACSEC/6/MACSEC_MKA_SAK_REFRESH: The SAK has been refreshed on interface GigabitEthernet1/0/1.
Explanation	The participant on the interface derived or received a new SAK.
Recommended action	No action is required.

MACSEC_MKA_SESSION_REAUTH

Message text	The MKA session with CKN [STRING] was re-authenticated on interface [STRING].
Variable fields	$1: CKN. $2: Interface name.
Severity level	6
Example	MACSEC/6/MACSEC_MKA_SESSION_REAUTH: The MKA session with CKN 80A0EA0CB03D was re-authenticated on interface GigabitEthernet1/0/1.
Explanation	The interface performed 802.1X reauthentication. After the 802.1X reauthentication, the participants received a new CAK, and used it to re-establish the MKA session.
Recommended action	No action is required.

MACSEC_MKA_SESSION_SECURED

Message text	The MKA session with CKN [STRING] was secured on interface [STRING].
Variable fields	$1: CKN. $2: Interface name.
Severity level	6
Example	MACSEC/6/MACSEC_MKA_SESSION_SECURED: The MKA session with CKN 80A020EA0CB03D was secured on interface GigabitEthernet1/0/1.

Explanation	The MKA session on the interface was secured. Packets are encrypted and transmitted in cipher text. The event occurs in the following situations:
	• The MKA session state changes from unsecured to secured.
	• The local participant and the peer negotiate a new MKA session when the following conditions exist:
	  ○ Both the key server and the peer support MACsec.
	  ○ A minimum of one participant is enabled with the MACsec desire feature.

Recommended action	No action is required.

MACSEC_MKA_SESSION_START

Message text	The MKA session with CKN [STRING] started on interface [STRING].
Variable fields	$1: CKN. $2: Interface name.
Severity level	6
Example	MACSEC/6/MACSEC_MKA_SESSION_START: The MKA session with CKN 80A020EA0CB03D started on interface GigabitEthernet1/0/1.
Explanation	The MKA session negotiation was initiated. Possible reasons include: • New CAK is available after MKA is enabled. • The user re-establishes the MKA session. • The interface that failed MKA session negotiation receives an MKA packet.
Recommended action	No action is required.

MACSEC_MKA_SESSION_STOP

Message text	The MKA session with CKN [STRING] stopped on interface [STRING].
Variable fields	$1: CKN. $2: Interface name.
Severity level	5
Example	MACSEC/5/MACSEC_MKA_SESSION_STOP: The MKA session with CKN 80A020EA0CB03D stopped on interface GigabitEthernet1/0/1.
Explanation	The MKA session was terminated. Possible reasons include: • The user removes or re-establishes the MKA session on the interface. • The link associated to the session is down.
Recommended action	**165.** Use the **`display mka session`** command to check whether the session exists: o If the session has been re-established, ignore the message. o If the session does not exist and is not removed by the user, check the link associated with the session for link failure. **166.** Recover the link if the link is down.

MACSEC_MKA_SESSION_UNSECURED

Message text	The MKA session with CKN [STRING] was not secured on interface [STRING].
Variable fields	$1: CKN. $2: Interface name.
Severity level	5
Example	MACSEC/5/MACSEC_MKA_SESSION_UNSECURED: The MKA session with CKN 80A020EA0CB03D was not secured on interface GigabitEthernet1/0/1.
Explanation	The MKA session on the interface was not secured. Packets are transmitted in plain text. The event occurs in the following situations: • The MKA session state changes from secured to unsecured. • The local participant and the peer negotiate a new MKA session when the following conditions exist: o The key server and the peer are not both MACsec capable. o No participant is enabled with the MACsec desire feature.
Recommended action	To secure the MKA session, perform the following tasks: • Verify that both the key server and the peer support MACsec. • Verify that a minimum of one participant is enabled with the MACsec desire feature.

MBFD messages

This section contains MPLS BFD messages.

MBFD_TRACEROUTE_FAILURE

Message text	[STRING] is failed. ([STRING].)
Variable fields	$1: LSP information. $2: Reason for the LSP failure.
Severity level	5
Example	MBFD/5/MBFD_TRACEROUTE_FAILURE: LSP (LDP IPv4: 22.22.2.2/32, nexthop: 20.20.20.2) is failed. (Replying router has no mapping for the FEC.) MBFD/5/MBFD_TRACEROUTE_FAILURE: TE tunnel (RSVP IPv4: Tunnel1) is failed. (No label entry.)
Explanation	LSP/MPLS TE tunnel failure was detected by periodic MPLS tracert. This message is generated when the system receives an MPLS echo reply with an error return code.
Recommended action	Verify the configuration for the LSP or MPLS TE tunnel.

MBUF messages

This section contains MBUF messages.

DBL_FREE

Message text	MBUF address: [HEX] repeated release! Seq: [UINT32], CPU ID: [UINT32], [STRING]: [STRING] Seq: [UINT32], CPU ID: [UINT32], [STRING]: [STRING] Seq: [UINT32], CPU ID: [UINT32], [STRING]: [STRING] Seq: [UINT32], CPU ID: [UINT32], [STRING]: [STRING] Seq: [UINT32], CPU ID: [UINT32], [STRING]: [STRING]
Variable fields	$1: Mbuf address $2: Stack sequence number $3: ID of the CPU where the stack resides $4: Mbuf allocation or deallocation tracing (Alloc trace or Free trace) $5: Stack information $6: Stack sequence number $7: ID of the CPU where the stack resides $8: Mbuf allocation or deallocation tracing (Alloc trace or Free trace) $9: Stack information $10: Stack sequence number $11: ID of the CPU where the stack resides $12: Mbuf allocation or deallocation tracing (Alloc trace or Free trace) $13: Stack information $14: Stack sequence number $15: ID of the CPU where the stack resides $16: Mbuf allocation or deallocation tracing (Alloc trace or Free trace) $17: Stack information $18: Stack sequence number $19: ID of the CPU where the stack resides $20: Mbuf allocation or deallocation tracing (Alloc trace or Free trace) $21: Stack information
Severity level	2
Example	MBUF/2/DBL_FREE: MBUF address: 0x854f9380 repeated release! Seq: 411, CPU ID: 1, Alloc trace: bdae759c bd2becbc bd2ba850 bd2bb718 bd368d04 bd3695e4 bd369bf8 bd358dc8 bd3295b0 bd29e0f4 Seq: 412, CPU ID: 1, Free trace: bdae759c bd2becbc bd2bc020 bd369298 bd3695e4 bd369bf8 bd358dc8 bd3295b0 bd29e0f4 bd2a1e8c Seq: 413, CPU ID: 1, Free trace: bdae759c bd2becbc bd2bc020 bd3692ac bd3695e4 bd369bf8 bd358dc8 bd3295b0 bd29e0f4 bd2a1e8c Seq: 409, CPU ID: 1, Alloc trace: bdae759c bd2becbc bd2ba850 bd2bc26c bd2d3320 bd105fc4 bd007b44 bd006c88 bd102264 400646b8 Seq: 410, CPU ID: 1, Free trace: bdae759c bd2becbc bd2baefc bd2d3344 bd105fc4 bd007b44 bd006c88 bd102264 400646b8 400651b8
Explanation	An mbuf has been repeatedly released. This message records information about the five stacks that most recently used the mbuf.
Recommended action	Locate the process that repeatedly released the mbuf based on the stack information in the log message.

MBUF_DATA_BLOCK_CREATE_FAIL

Message text	Failed to create an MBUF data block because of insufficient memory. Failure count: [UINT32].
Variable fields	$1: Failure count.
Severity level	2
Example	MBUF/2/MBUF_DATA_BLOCK_CREATE_FAIL: Failed to create an MBUF data block because of insufficient memory. Failure count: 128.
Explanation	The message is output when the system fails to create an MBUF data block 1 minute or more after the most recent creation failure.
Recommended action	**167.** Execute the **`display system internal kernel memory pool	include mbuf`** command in probe view to view the number of the allocated MBUF data blocks. **168.** Execute the **`display memory`** command in system view to display the total size of the system memory. **169.** Determine whether an excessive number of MBFU data blocks are allocated by comparing the size of the allocated MBUF data blocks with that of the system memory. o If it is not an excessive number, use the memory management commands to check for the memory-intensive modules. o If it is an excessive number, go to step 170. **170.** Execute the **`display system internal mbuf socket statistics`** command in probe view to view the number of the MBUF data blocks buffered in the socket. Determine whether a process has too many MBUF data blocks buffered in the socket buffer. o If it is too many, locate the reason why the MBUF data blocks cannot be released from the socket buffer. o If it is not too many, use other means to locate the reasons for excessive allocation of MBUF data blocks. **171.** If the problem persists, contact NSFOCUS Support.

STEPMEM

Message text	MBUF address [HEX] MBUF block address [HEX] STEP ON MEMORY! Stack :[STRING]
Variable fields	$1: Mbuf address $2: Mbuf block address $3: Stack information
Severity level	2
Example	MBUF/2/STEPMEM: MBUF address 780bd380 MBUF block address 780bd388 STEP ON MEMORY! Stack :bdae759c bd2be938 bd2b7ce4 bd2bbf8c bac531ec bcfe4270 bd141b94 bdaecd50 bd2a0ca4 bd2a157c bd2a1c54 bd369048 bd3695e4 bd369bf8 bd358dc8 bd3295b0
Explanation	An mbuf was overwrittern.
Recommended action	Locate the process that overwrote the memory based on the stack information in the log message. Further locating is required when one of the following conditions exists: • The mbuf was used by another process after being placed back in the MBUF queue. • The stack recorded in the log was not the one that caused the memory overwriting.

MDC messages

This section contains MDC messages.

MDC_CREATE_ERR

Message text	Failed to create MDC [UINT16] for insufficient resources.
Variable fields	$1: MDC ID.
Severity level	5
Example	MDC/5/MDC_CREATE_ERR: -Slot=1; Failed to create MDC 2 for insufficient resources.
Explanation	The standby MPU did not have enough resources to create the MDC. At startup, the standby MPU obtains MDC configuration information from the active MPU. If the standby MPU does not have enough resources to create an MDC, it outputs this log message.
Recommended action	**172.** Use the **display mdc resource** command to display the CPU, memory, and disk space resources on the standby MPU. **173.** Perform one of the following tasks: ○ If the memory space is insufficient, increase the memory space. If the disk space is insufficient, delete unused files. ○ Use the **undo mdc** command to delete the specified MDC. ○ Replace the standby MPU with an MPU that has sufficient resources.

MDC_CREATE

Message text	MDC [UINT16] was created.
Variable fields	$1: MDC ID.
Severity level	5
Example	MDC/5/MDC_CREATE: MDC 2 was created.
Explanation	An MDC was created successfully.
Recommended action	No action is required.

MDC_DELETE

Message text	MDC [UINT16] was deleted.
Variable fields	$1: MDC ID.
Severity level	5
Example	MDC/5/MDC_DELETE: MDC 2 was deleted.
Explanation	An MDC was deleted successfully.
Recommended action	No action is required.

MDC_KERNEL_EVENT_TOOLONG

Message text	[STRING] [UINT16] kernel event in sequence [STRING] function [STRING] failed to finish within [UINT32] minutes.
Variable fields	$1: MDC ID. $2: Kernel event phase. $3: Address of the function corresponding to the kernel event. $4: Time duration.
Severity level	4
Example	MDC/4/MDC_KERNEL_EVENT_TOOLONG: Slot=1; MDC 2 kernel event in sequence 0x4fe5 function 0xff245e failed to finish within 15 minutes.
Explanation	A kernel event stayed unfinished for a long period of time.
Recommended action	**174.** Reboot the card in the specified slot. **175.** If the problem persists, contact HP Support.

MDC_LICENSE_EXPIRE

Message text	The MDC feature's license will expire in [UINT32] days.
Variable fields	$1: Number of days, in the range of 1 to 30.
Severity level	5
Example	MDC/5/MDC_LICENSE_EXPIRE: The MDC feature’s license will expire in 5 days.
Explanation	The license for the MDC feature was about to expire.
Recommended action	Install a new license.

MDC_NO_FORMAL_LICENSE

Message text	The feature MDC has no formal license.
Variable fields	N/A
Severity level	5
Example	MDC/5/MDC_NO_FORMAL_LICENSE: The feature MDC has no formal license.
Explanation	The standby MPU became the active MPU but it did not have a formal license. The MDC feature has a free trial period. To use the feature after the period elapses, you must install a license for the standby MPU.
Recommended action	Install a formal license.

MDC_NO_LICENSE_EXIT

Message text	The MDC feature is being disabled, because it has no license.
Variable fields	N/A
Severity level	5
Example	MDC/5/MDC_NO_LICENSE_EXIT: The MDC feature is being disabled, because it has no license.
Explanation	The MDC feature was disabled because the license for the MDC feature expired or was uninstalled.
Recommended action	Install the required license.

MDC_OFFLINE

Message text	MDC [UINT16] is offline now.
Variable fields	$1: MDC ID.
Severity level	5
Example	MDC/5/MDC_OFFLINE: MDC 2 is offline now.
Explanation	An MDC was stopped.
Recommended action	No action is required.

MDC_ONLINE

Message text	MDC [UINT16] is online now.
Variable fields	$1: MDC ID.
Severity level	5
Example	MDC/5/MDC_ONLINE: MDC 2 is online now.
Explanation	An MDC was started.
Recommended action	No action is required.

MDC_STATE_CHANGE

Message text	MDC [UINT16] status changed to [STRING].
Variable fields	$1: MDC ID. $2: MDC status: ○ **updating**–The system is assigning interface cards to the MDC (executing the **location** command). ○ **stopping**–The system is stopping the MDC (executing the **undo mdc start** command). ○ **inactive**–The MDC is inactive. ○ **starting**–The system is starting the MDC (executing the **mdc start** command). ○ **active**–The MDC is operating correctly.
Severity level	5
Example	MDC/5/MDC_STATE_CHANGE: MDC 2 status changed to active.
Explanation	The status of an MDC changed.
Recommended action	No action is required.

MFIB messages

This section contains MFIB messages.

MFIB_MEM_ALERT

Message text	MFIB process received system memory alert [STRING] event.
Variable fields	$1: Type of the memory alert event.
Severity level	5
Example	MFIB/5/MFIB_MEM_ALERT: MFIB process receive system memory alert start event.
Explanation	The MFIB module received a memory alert event from the system.
Recommended action	**176.** Check the system memory to make sure the memory usage does not exceed the thresholds. **177.** Release memory for the modules that occupy too many memory resources.

MGROUP messages

This section contains mirroring group messages.

MGROUP_APPLY_SAMPLER_FAIL

Message text	Failed to apply the sampler for mirroring group [UINT16], because the sampler resources are insufficient.
Variable fields	$1: Mirroring group ID.
Severity level	3
Example	MGROUP/3/MGROUP_APPLY_SAMPLER_FAIL: Failed to apply the sampler for mirroring group 1, because the sampler resources are insufficient.
Explanation	A sampler was not applied to the mirroring group because the sampler resources were insufficient.
Recommended action	No action is required.

MGROUP_RESTORE_CPUCFG_FAIL

Message text	Failed to restore configuration for mirroring CPU of [STRING] in mirroring group [UINT16], because [STRING]
Variable fields	$1: Slot number. $2: Mirroring group ID. $3: Failure reason.
Severity level	3
Example	MGROUP/3/MGROUP_RESTORE_CPUCFG_FAIL: Failed to restore configuration for mirroring CPU of chassis 1 slot 2 in mirroring group 1, because the type of the monitor port in the mirroring group is not supported.
Explanation	When the CPU of the card in the slot is the source CPU in the mirroring group, configuration changes after the card is removed. When the card is reinstalled into the slot, restoring the source CPU configuration might fail.
Recommended action	Check for the failure reason. If the reason is that the system does not support the changed configuration, delete the unsupported configuration, and reconfigure the source CPU in the mirroring group.

MGROUP_RESTORE_IFCFG_FAIL

Message text	Failed to restore configuration for interface [STRING] in mirroring group [UINT16], because [STRING]
Variable fields	$1: Interface name. $2: Mirroring group ID. $3: Failure reason.
Severity level	3
Example	MGROUP/3/MGROUP_RESTORE_IFCFG_FAIL: Failed to restore configuration for interface Ethernet3/1/2 in mirroring group 1, because the type of the monitor port in the mirroring group is not supported.
Explanation	When the interface of the card in the slot is the monitor port in the mirroring group, configuration changes after the card is removed. When the card is reinstalled into the slot, restoring the monitor port configuration might fail.
Recommended action	Check for the failure reason. If the reason is that the system does not support the changed configuration, delete the unsupported configuration, and reconfigure the monitor port in the mirroring group.

MGROUP_SYNC_CFG_FAIL

Message text	Failed to restore configuration for mirroring group [UINT16] in [STRING], because [STRING]
Variable fields	$1: Mirroring group ID. $2: Slot number. $3: Failure reason.
Severity level	3
Example	MGROUP/3/MGROUP_SYNC_CFG_FAIL: Failed to restore configuration for mirroring group 1 in chassis 1 slot 2, because monitor resources are insufficient.
Explanation	When the complete mirroring group configuration was synchronized on the card in the slot, restoring configuration failed because resources on the card were insufficient.
Recommended action	Delete the mirroring group.

MPLS messages

This section contains MPLS messages.

MPLS_HARD_RESOURCE_NOENOUGH

Message text	No enough hardware resource for MPLS.
Variable fields	N/A
Severity level	4
Example	MPLS/4/MPLS_HARD_RESOURCE_NOENOUGH: No enough hardware resource for MPLS.
Explanation	Hardware resources for MPLS were insufficient.
Recommended action	Check whether unnecessary LSPs had been generated. If yes, configure or modify the LSP generation policy, label advertisement policy, and label acceptance policy to filter out unnecessary LSPs.

MPLS_HARD_RESOURCE_RESTORE

Message text	Hardware resources for MPLS are restored.
Variable fields	N/A
Severity level	6
Example	MPLS/6/MPLS_HARD_RESOURCE_RESTORE: Hardware resources for MPLS are restored.
Explanation	Hardware resources for MPLS were restored.
Recommended action	No action is required.

MTLK messages

This section contains Monitor Link messages.

MTLK_UPLINK_STATUS_CHANGE

Message text	The uplink of monitor link group [UINT32] is [STRING].
Variable fields	$1: Monitor link group ID. $2: Monitor Link group status, up or down.
Severity level	6
Example	MTLK/6/MTLK_UPLINK_STATUS_CHANGE: The uplink of monitor link group 1 is up.
Explanation	The uplink of a monitor link group went up or down.
Recommended action	Troubleshoot the uplink when it fails.

NAT messages

This section contains NAT messages.

NAT_ADDR_BIND_CONFLICT

Message text	Invalid configuration on interface [STRING]: [STRING]. Reason: Global IP addresses already bound to another service card.
Variable fields	$1: Interface name. $2: NAT address group
Severity level	4
Example	NAT/4/NAT_ADDR_BIND_CONFLICT: Invalid configuration on interface Ethernet0/0/2: nat outbound address-group 1. Reason: Global IP addresses already bound to another service card.
Explanation	The NAT configuration did not take effect, because the global IP addresses that the interface references have been bound to another service card.
Recommended action	If multiple interfaces reference the same global IP addresses, you must specify the same service card to process NAT traffic passing through these interfaces. To resolve the problem: **178.** Use the **display nat all** command to check the current configuration. **179.** Remove the service card configuration on the interface. **180.** Specify the same service card for interfaces referencing the same global IP addresses.

NAT_ADDRGRP_MEMBER_CONFLICT

Message text	The address range in address group [UINT16] overlaps with the address range in address group [UINT16].
Variable fields	$1: NAT address group ID. $2: NAT address group ID.
Severity level	4
Example	NAT/4/NAT_ADDRGRP_MEMBER_CONFLICT: The address range in address group 1 overlaps with the address range in address group 2.
Explanation	This message is sent if addresses in NAT address groups overlap.
Recommended action	Modify IP addresses in conflicting NAT address groups.

NAT_ADDRGRP_RESOURCE_EXHAUST

Message text	The address resources of [STRING] address group [INTEGER] are not enough.
Variable fields	$1: Address translation mode: • NO-PAT • EIM $2: Address group ID.
Severity level	4
Example	NAT/4/NAT_ADDRGRP_RESOURCE_EXHAUST: The address resources of NO-PAT address group 1 are not enough.
Explanation	The address resources for the NO-PAT or EIM mode are not enough.
Recommended action	Please add address resources.

NAT_FAILED_ADD_FLOW_RULE

Message text	Failed to add flow-table due to: [STRING].
Variable fields	$1: Reason for the failure.
Severity level	4
Example	NAT/4/NAT_FAILED_ADD_FLOW_TABLE: Failed to add flow-table due to: Not enough resources are available to complete the operation.
Explanation	The system failed to deploy flow entries. Possible reasons include insufficient hardware resources or memory.
Recommended action	Contact NSFOCUS Support.

NAT_FAILED_ADD_FLOW_TABLE

Message text	Failed to add flow-table due to [STRING].
Variable fields	$1: Failure reason: • no enough resource. • The item already exists.
Severity level	4
Example	NAT/4/NAT_FAILED_ADD_FLOW_TABLE: Failed to add flow-table due to no enough resource.
Explanation	The system failed to add a flow table due to insufficient hardware resources or NAT address overlapping.
Recommended action	If the failure is caused by insufficient hardware resources, contact NSFOCUS Support. If the failure is caused by address overlapping, reconfigure the NAT addresses. Make sure the NAT address ranges do not overlap.

NAT_FLOW

		Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NatSrcIPAddr(1005)=[IPADDR];NatSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NatDstIPAddr(1009)=[IPADDR];NatDstPort(1010)=[UINT16];UserName(1113)=[STRING];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];
		$1: Protocol type. $2: Application layer protocol name. $3: Application service type. $4: Source IP address. $5: Source port number. $6: Source IP address after translation. $7: Source port number after translation. $8: Destination IP address. $9: Destination port number. $10: Destination IP address after translation. $11: Destination port number after translation. $12: Name of identity users. $13: Total number of incoming packets. $14: Total number of incoming bytes. $15: Total number of outgoing packets. $16: Total number of outgoing bytes. $17: Source VPN instance name. $18: Destination VPN instance name. $19: Source DS-Lite tunnel. $20: Destination DS-Lite tunnel. $21: Time when the session is created. $22: Time when the session is removed. $23: Event type. $24: Event description: ○ Session created. ○ Active flow threshold. ○ Normal over. ○ Aged for timeout. ○ Aged for reset or config-change. ○ Other.

		6
		NAT/6/NAT_FLOW: Protocol(1001)=TCP;Application(1002)=http;Category(1174)=Protocol;SrcIPAddr(1003)=46.2.1.77;SrcPort(1004)=63419;NatSrcIPAddr(1005)=146.2.1.190;NatSrcPort(1006)=50805;DstIPAddr(1007)=64.2.1.26;DstPort(1008)=80;NatDstIPAddr(1009)=64.2.1.26;NatDstPort(1010)=80;InitPktCount(1044)=1;InitByteCount(1046)=56;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=09072021103948;EndTime_e(1014)=;Event(1048)=(8)Session created;
		This message is sent in one of the following conditions: • A NAT session is created or removed. • Regularly during a NAT session. • The traffic threshold or aging time of a NAT session is reached.
		No action is required.

NAT_INTERFACE_RESOURCE_EXHAUST

Message text	The address resources of Easy-IP-EIM interface [STRING] are not enough.
Variable fields	$1: Interface name.
Severity level	4
Example	NAT/4/NAT_INTERFACE_RESOURCE_EXHAUST: The address resources of EASY-IP-EIM interface Route-Aggregation1 are not enough.
Explanation	The address resources for the Easy-IP-EIM mode on the interface are not enough.
Recommended action	Please add address resources.

NAT_NOPAT_IP_USAGE_ALARM

Message text		Address group [UINT16], total IP addresses [UINT16], used IP addresses [UINT16], usage rate over [UINT16]%.
Variable fields		$1: NAT address group ID. $2: Number of total IP addresses in the NAT address group. $3: Number of used IP addresses in the NAT address group. $4: IP usage of the NAT address group.
Severity level		6
Example		NAT/6/NAT_NOPAT_IP_USAGE_ALARM: -Context=1; Address group 1, total IP addresses 10, used IP addresses 9, usage rate over 90%.
Explanation		This message is sent when the IP usage of the NAT address group in NO-PAT mode exceeded the threshold.
Recommended action		No action is required.

NAT_PORTBLOCKGRP_ADDRESS_WARNING

Message text	Insufficient memory due to large [STRING] address range in port block group [UINT16]. Please reconfigure the [STRING] address range.
Variable fields	$1: Address type: • **local**—Private IP address. • **global**—Public IP address $2: Number of the static port block group. $3: Address type: • **local**—Private IP address. • **global**—Public IP address.
Severity level	4
Example	NAT/4/NAT_PORTBLOCKGRP_ADDRESS_WARNING: Insufficient memory due to large local address range in port block group 0. Please reconfigure the local address range.
Explanation	The device does not have enough memory for the static port block group because the private or public address range in this port block group is too large.
Recommended action	Modify the private or public address range in the port block group.

NAT_SERVER_INVALID

Message text		The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server on this interface.
Variable fields		N/A
Severity level		4
Example		NAT/4/NAT_SERVER_INVALID: The NAT server with Easy IP is invalid because its global settings conflict with that of another NAT server on this interface.
Explanation		The NAT Server with Easy IP did not take effect because its global settings conflict with that the global settings of another NAT Server on the same interface.
Recommended action		Modify the NAT Server configuration on the interface. The combination of protocol type, global IP addresses and global ports must be unique for each NAT Server on the same interface.

NAT_SERVICE_CARD_RECOVER_FAILURE

Message text	Pattern 1: Failed to recover the configuration of binding the service card on slot [UINT16] to interface [STRING], because [STRING]. Pattern 2: Failed to recover the configuration of binding the service card on chassis [UINT16] slot [UINT16] to interface [STRING], because [STRING].
Variable fields	Pattern 1: $1: Slot number. $2: Interface name. $3: Reasons why restoring the binding between the service card and the interface fails. Pattern 2: $1: Chassis number. $2: Slot number. $3: Interface name. $4: Reasons why restoring the binding between the service card and the interface fails.
Severity level	4
Example	NAT/4/NAT_SERVICE_CARD_RECOVER_FAILURE: Failed to recover the configuration of binding the service card on slot 3 to interface GigabitEthernet0/0/2, because NAT service is not supported on this service card.
Explanation	Restoring the binding between the service card and the interface failed.
Recommended action	• If the operation fails because the NAT addresses have already been bound to another service card: ○ Use the **display nat all** command to check the current configuration. ○ Specify the same service card for interfaces

Message text		Pattern 1: Failed to recover the configuration of binding the service card on slot [UINT16] to interface [STRING], because [STRING]. Pattern 2: Failed to recover the configuration of binding the service card on chassis [UINT16] slot [UINT16] to interface [STRING], because [STRING].
		referencing the same NAT addresses. • Check the service card for hardware problems if the failure is caused by one of the following reasons: ○ NAT service is not supported on this service card. ○ The hardware resources are not enough. ○ Unknown error.

NAT444_PORTBLOCK_USAGE_ALARM

Message text	Address group [UINT16], total port blocks [UINT16], active port blocks [UINT16], usage rate over [UINT16]%.
Variable fields	$1: Address group ID. $2: Number of port blocks in the address group. $3: Number of assigned port blocks in the address group. $4: Port block usage.
Severity level	6
Example	NAT/6/NAT444_PORTBLOCK_USAGE_ALARM: -Context=1; Address group 1003, total port blocks 10, active port blocks 9, usage rate over 90%.
Explanation	This message is sent when the port block usage assigned by dynamic NAT444 exceeds the specified threshold.
Recommended action	Please add port block resources.

ND messages

This section contains ND messages.

ND_CONFLICT

Message text	[STRING] is inconsistent.
Variable fields	$1: Configuration type: o M_FLAG. o O_FLAG. o CUR_HOP_LIMIT. o REACHABLE TIME. o NS INTERVAL. o MTU. o PREFIX VALID TIME. o PREFIX PREFERRED TIME.
Severity level	6
Example	ND/6/ND_CONFLICT: PREFIX VALID TIME is inconsistent
Explanation	The configuration information in the received router advertisement was not consistent with the configuration on the device. A message is sent if an inconsistency is detected.
Recommended action	Verify that the configurations on the device and the neighboring router are consistent.

ND_DUPADDR

Message text	Duplicate address: [STRING] on the interface [STRING].
Variable fields	$1: IPv6 address that is to be assigned to the interface. $2: Name of the interface.
Severity level	6
Example	ND/6/ND_DUPADDR: Duplicate address: 33::8 on interface Vlan-interface9.
Explanation	The IPv6 address that was to be assigned to the interface is being used by another device.
Recommended action	Assign another IPv6 address to the interface.

ND_HOST_IP_CONFLICT

Message text	The host [STRING] connected to interface [STRING] cannot communicate correctly, because it uses the same IPv6 address as the host connected to interface [STRING].
Variable fields	$1: IPv6 global unicast address of the host. $2: Name of the interface. $3: Name of the interface.
Severity level	4
Example	ND/4/ND_HOST_IP_CONFLICT: The host 2::2 connected to interface GigabitEthernet1/0/1 cannot communicate correctly, because it uses the same IPv6 address as the host connected to interface GigabitEthernet1/0/1.
Explanation	The IPv6 global unicast address of the host is being used by another host that connects to the same interface.
Recommended action	Disconnect the host and assign another IPv6 global unicast address to the host.

ND_MAC_CHECK

Message text	Packet received on interface [STRING] was dropped because source MAC [STRING] was inconsistent with link-layer address [STRING].
Variable fields	$1: Receiving interface of the ND packet. $2: Source MAC address in the Ethernet frame header of the ND packet. $3: Source link-layer address in the ND packet.
Severity level	6
Example	ND/6/ND_MAC_CHECK: Packet received on interface Ethernet2/0/2 was dropped because source MAC 0002-0002-0001 was inconsistent with link-layer address 0002-0002-0002.
Explanation	The device dropped an ND packet because source MAC consistency check detected that source MAC address and the source link-layer address are not the same in the packet.
Recommended action	Verify the validity of the ND packet originator.

ND_SET_PORT_TRUST_NORESOURCE

Message text	Not enough resources to complete the operation.
Variable fields	N/A
Severity level	6
Example	ND/6/ND_SET_PORT_TRUST_NORESOURCE: Not enough resources to complete the operation.
Explanation	Failed to execute the command because driver resources were not enough.
Recommended action	Release the driver resources and execute the command again.

ND_SET_VLAN_REDIRECT_NORESOURCE

Message text	Not enough resources to complete the operation.
Variable fields	N/A
Severity level	6
Example	ND/6/ND_SET_VLAN_REDIRECT_NORESOURCE: Not enough resources to complete the operation.
Explanation	Failed to execute the command because driver resources were not enough.
Recommended action	Release the driver resources and execute the command again.

ND_MAXNUM_IF

Message text	The number of dynamic neighbor entries on interface [STRING] has reached the maximum.
Variable fields	$1: Interface name.
Severity level	6
Example	The number of dynamic neighbor entries on interface GigabitEthernet3/0/1 has reached the maximum.
Explanation	The number of dynamic neighbor entries on the interface has reached the upper limit.
Recommended action	No action is required.

ND_MAXNUM_DEV

Message text	The number of dynamic neighbor entries for the device has reached the maximum.
Variable fields	N/A
Severity level	6
Example	The number of dynamic neighbor entries for the device has reached the maximum.
Explanation	The number of dynamic neighbor entries on the device has reached the upper limit.
Recommended action	No action is required.

NETCONF messages

This section contains NETCONF messages.

CLI

Message text	User ([STRING], [STRING][STRING]) performed an CLI operation: [STRING] operation result=[STRING][STRING]
Variable fields	$1: Username or user line type. • If scheme login authentication was performed for the user, this field displays the username. • If no login authentication was performed or password authentication was performed, this field displays the user line type, such as VTY. $2: User IP address or user line type and relative number. • For a Telnet or SSH user, this field displays the IP address of the user. • For a user who logged in through the console or AUX port, this field displays the user line type and the relative line number, such as console0. $3: ID of the NETCONF session. This field is not displayed for Web and RESTful sessions. $4: Message ID of the NETCONF request. This field is not displayed for Web and RESTful sessions. $5: Operation result, **Succeeded** or **Failed**. $6: Cause for an operation failure. This field is displayed only if the failure is caused by a known reason.
Severity level	6
Example	XMLSOAP/6/CLI: -MDC=1; User (test, 169.254.5.222, session ID=1) performed an CLI operation: message ID=101, operation result=Succeeded.
Explanation	After a CLI command is executed by using NETCONF, the device outputs this message to show the operation result.
Recommended action	No action is required.

EDIT-CONFIG

Message text	User ([STRING], [STRING], session ID [UINT16]) performed an edit-config operation: message ID=[STRING], operation result=Succeeded. Or User ([STRING], [STRING], session ID [UINT16]) performed an edit-config operation: message ID=[STRING], operation result=Failed. [STRING] Or User ([STRING], [STRING], session ID [UINT16]) performed an edit-config operation: message ID=[STRING], operation result=Failed, XPath=[STRING], error message=[STRING].
Variable fields	$1: Username or user line type. o If scheme login authentication was performed for the user, this field displays the username. o If no login authentication was performed or password authentication was performed, this field displays the user line type, such as VTY. $2: User IP address or user line type and relative line number. o For a Telnet or SSH user, this field displays the IP address of the user. o For a user who logged in through the console or AUX port, this field displays the user line type and the relative line number, such as console0. $3: ID of the NETCONF session. $4: Message ID of the NETCONF request. $5: Error message or XPath expression for an incorrect row. o This field displays an error message if the **verbose** keyword is not specified in the **netconf log** command and the failure is caused by a known reason. o This field displays an XPath expression if the **verbose** keyword is specified in the **netconf log** command. $6: Error message. This field is displayed only if the **verbose** keyword is specified in the **netconf log** command.
Severity level	6
Example	XMLSOAP/6/EDIT-CONFIG: -MDC=1; User (test, 192.168.100.20, session ID 1) performed an edit-config operation: message ID=101, operation result=Succeeded.
Explanation	The device outputs this log message for each NETCONF setting in an <edit-config> operation to show the configuration result.
Recommended action	No action is required.

NETCONF_MSG_DEL

Message text	A NETCONF message was dropped. Reason: Packet size exceeded the upper limit.
Variable fields	N/A
Severity level	7
Example	NETCONF/7/NETCONF_MSG_DEL: A NETCONF message was dropped. Reason: Packet size exceeded the upper limit.
Explanation	The system dropped a NETCONF request message that was received from a NETCONF over SSH client or at the XML view. The reason is that the message size exceeded the upper limit.
Recommended action	**181.** Reduce the size of the request message. For example, delete blank spaces, carriage returns, and tab characters. **182.** Contact NSFOCUS Support to segment the request message and then re-encapsulate the segments before sending them to the device.

ROW-OPERATION

Message text	User ([STRING], [STRING][STRING])[STRING] operation=[STRING] [STRING] [STRING], result=[STRING]. No attributes. Or User ([STRING], [STRING],[STRING]),[STRING] operation=[STRING] [STRING] [STRING], result=[STRING]. Attributes: [STRING].
Variable fields	$1: Username or user line type. o If scheme login authentication was performed for the user, this field displays the username. o If no login authentication was performed or password authentication was performed, this field displays the user line type, such as VTY. $2: User IP address or user line type and relative line number. o For a Telnet or SSH user, this field displays the IP address of the user. o For a user who logged in through the console or AUX port, this field displays the user line type and the relative line number, such as console0. $3: ID of the NETCONF session. If there is no session ID, this field is not displayed. $4: Message ID of the NETCONF request. If there is no message ID, this field is not displayed. $5: NETCONF row operation name. $6: Module name and table name. $7: Index information enclosed in a pair of parentheses. If there is not an index, this field is not displayed. If there are multiple indexes, the indexes are separated by commas. $8: Result of the NETCONF row operation, **Succeeded** or **Failed**. $9: Attribute column information. If there is no attribute column, this field is not displayed.
Severity level	6
Example	XMLSOAP/6/EDIT-CONFIG: User (test, 192.168.100.20, session ID 1), message ID=1, operation=create Ifmgr/Interfaces (IfIndex="GigabitEthernet1/0/1"), result=Succeeded. Attributes: Description="This is Desc1", AdminDown=1, Speed=1.
Explanation	The device outputs this log message for each NETCONF row operation. Only action and set operations support this log message.
Recommended action	No action is required.

REPLY

Message text	Sent a NETCONF reply to the client: Session ID=[UINT16], Content=[STRING]. Or Sent a NETCONF reply to the client: Session ID=[UINT16], Content (partial)=[STRING].
Variable fields	$1: ID of the NETCONF session. This field displays a hyphen (-) before the NETCONF session is established. $2: NETCONF packet that the device sent to the NETCONF client.
Severity level	7
Example	XMLSOAP/7/REPLY: -MDC=1; Sent a NETCONF reply to the client: Session ID=2, Content=</env:Body></env:Envelope>.
Explanation	When sending a NETCONF packet to a client, the device outputs this log message for NETCONF debugging purposes. If a NETCONF packet cannot be sent in one log message, the device uses multiple log messages and adds the **partial** flag in each log message.
Recommended action	No action is required.

THREAD

Message text	Maximum number of NETCONF threads already reached.
Variable fields	N/A
Severity level	3
Example	XMLCFG/3/THREAD: -MDC=1; Maximum number of NETCONF threads already reached.
Explanation	The number of NETCONF threads already reached the upper limit.
Recommended action	Please try again later.

NETSHARE messages

This section contains NetShare control messages.

NETSHARE_IPV4_LOG

Message text	SrcIPAddr(1003)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];TerminalNum(1125)=[UINT16];PolicyName(1079)=[STRING];Action(1053)=[STRING];FreezeTime(1126)=[UINT16].
Variable fields	$1: Source IP address. $2: Username. $3: Source VPN instance name. $4: Number of terminals sharing the IP address. $5: NetShare control policy name. $6: Action on the shared IP address: **Freeze**. $7: Time the IP address will be frozen, in minutes.
Severity level	6
Example	NETSHARE/6/NETSHARE_IPV4_LOG:SrcIPAddr(1003)=65.1.1.100;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;TerminalNum(1125)=5;PolicyName(1079)=test;Action(1053)=Freeze;FreezeTime(1126)=120min.
Explanation	The number of terminals sharing the IPv4 address exceeded the limit set in the NetShare control policy. This message is sent when the IPv4 address is frozen according to the action set in the policy or is manually frozen.
Recommended action	No action is required.

NETSHARE_IPV4_LOG

Message text	SrcIPAddr(1003)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];TerminalNum(1125)=[UINT16];PolicyName(1079)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Source IP address. $2: Username. $3: Source VPN instance name. $4: Number of terminals sharing the IP address. $5: NetShare control policy name. $6: Action on the shared IP address. The value can be: o **Permit.** o **Unfreeze**.
Severity level	6
Example	NETSHARE/6/NETSHARE_IPV4_LOG:SrcIPAddr(1003)=65.1.1.100;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;TerminalNum(1125)=5;PolicyName(1079)=test;Action(1053)=Permit.
Explanation	The number of terminals sharing the IPv4 address exceeded the limit set in the NetShare control policy. This message is sent when the packet is permitted to pass through according to the action in the policy or is manually unfrozen.
Recommended action	No action is required.

NETSHARE_IPV6_LOG

Message text	SrcIPv6Addr(1036)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];TerminalNum(1125)=[UINT16];PolicyName(1079)=[STRING];Action(1053)=[STRING];FreezeTime(1126)=[UINT16].
Variable fields	$1: Source IP address. $2: Username. $3: Source VPN instance name. $4: Number of terminals sharing the IP address. $5: NetShare control policy name. $6: Action on the shared IP address: **Freeze**. $7: Time the IP address will be frozen, in minutes.
Severity level	6
Example	NETSHARE/6/NETSHARE_IPV6_LOG:SrcIPv6Addr(1036)=3001::2;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;TerminalNum(1125)=5;PolicyName(1079)=test;Action(1053)=Freeze;FreezeTime(1126)=120min.
Explanation	The number of terminals sharing the IPv6 address exceeded the limit set in the NetShare control policy. This message is sent when the IPv6 address is frozen according to the action set in the policy or is manually frozen.
Recommended action	No action is required.

NETSHARE_IPV6_LOG

Message text	SrcIPv6Addr(1036)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];TerminalNum(1125)=[UINT16];PolicyName(1079)=[STRING];Action(1053)=[STRING].
Variable fields	$1: Source IP address. $2: Username. $3: Source VPN instance name. $4: Number of terminals sharing the IP address. $5: NetShare control policy name. $6: Action to take on the shared IP address. The value can be: o **Permit.** o **Unfreeze**.
Severity level	6
Example	NETSHARE/6/NETSHARE_IPV6_LOG:SrcIPv6Addr(1036)=3001::2;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;TerminalNum(1125)=5;PolicyName(1079)=test;Action(1053)=Permit.
Explanation	The number of terminals sharing the IPv6 address exceeded the limit set in the NetShare control policy. This message is sent when the packet is permitted to pass through according to the action set in the policy or is manually unfrozen.
Recommended action	No action is required.

NETSHARE_IPV4_BLS_LOG

Message text	SrcIPAddr(1003)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];PolicyName(1079)=[STRING].
Variable fields	$1: Source IP address. $2: Username. $3: Source VPN instance name. $4: NetShare control policy name.
Severity level	6
Example	NETSHARE/6/NETSHARE_IPV4_BLS_LOG:SrcIPAddr(1003)=65.1.1.100;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;PolicyName(1079)=test.
Explanation	This message is sent when a packet is detected from a frozen IPv4 address.
Recommended action	No action is required.

NETSHARE_IPV6_BLS_LOG

Message text	SrcIPv6Addr(1036)=[IPADDR];UserName(1113)=[STRING];RcvVPNInstance(1042)=[STRING];PolicyName(1079)=[STRING].
Variable fields	$1: Source IP address. $2: Username. $3: Source VPN instance name. $4: NetShare control policy name.
Severity level	6
Example	NETSHARE/6/NETSHARE_IPV6_BLS_LOG:SrcIPv6Addr(1036)=3001::2;UserName(1113)=test;RcvVPNInstance(1042)=vpn1;PolicyName(1079)=test.
Explanation	This message is sent when a packet is detected from a frozen IPv6 address.
Recommended action	No action is required.

NQA messages

This section contains NQA messages.

NQA_ENTRY_PROBE_RESULT

Message text	Reaction entry [STRING] of NQA entry admin-name [STRING] operation-tag [STRING]: [STRING].
Variable fields	$1: ID of the NQA reaction entry. The value range is 1 to 10. $2: Admin name of the NQA entry. $3: Operation tag of the NQA entry. $4: Test result. The value can be: o Probe-pass: Succeeded. o Probe-fail: Failed.
Severity level	6
Example	NQA/6/NQA_ENTRY_PROBE_RESULT Reaction entry 1 of NQA entry admin-name 1 operation-tag 1: Probe-pass.
Explanation	A change in the monitoring result of an NQA reaction entry was detected.
Recommended action	If the test result is Probe-fail, check the network environment.

NQA_LOG_UNREACHABLE

Message text	Server [STRING] unreachable.
Variable fields	$1: IP address of the NQA server.
Severity level	6
Example	NQA/6/NQA_LOG_UNREACHABLE: Server 192.168.30.117 unreachable.
Explanation	An unreachable server was detected.
Recommended action	Check the network environment.

NQA_SCHEDULE_FAILURE

Message text	NQA entry ([STRING]-[STRING]): Failed to start the scheduled NQA operation because port [STRING] used by the operation is not available.
Variable fields	$1: Admin name of the NQA operation. $2: Operation tag of the NQA operation. $3: Port number.
Severity level	6
Example	NQA/6/NQA_SCHEDULE_FAILURE: NQA entry (admin-tag): Failed to start the scheduled NQA operation because port 10000 used by the operation is not available.
Explanation	Failed to start a scheduled NQA operation because the port number used by the operation is not available.
Recommended action	Change the port number of the NQA operation or disable the service that uses the port number.

NQA_SET_DRIVE_FAIL

Message text	NQA entry admin-name [STRING] operation-tag [STRING]: [STRING].
Variable fields	$1: Admin name of the NQA entry. $2: Operation tag of the NQA entry. $3: Reason for the failure to issue the NQA operation to driver: ○ Operation failed due to configuration conflicts. ○ Operation failed because the driver was not ready to perform the operation. ○ Operation not supported. ○ Not enough resources to complete the operation. ○ Operation failed due to an unkonwn error.
Severity level	6
Example	NQA/6/ NQA_SET_DRIVE_ FAIL NQA entry admin-name 1 operation-tag 1: Not enough resources to complete the operation.
Explanation	Failed to issue the NQA operation to driver.
Recommended action	Follow the instructions to check the configuration.

NQA_SEVER_FAILURE

Message text	Failed to enable the NQA server because listening port [STRING] is not available.
Variable fields	$1: Port number.
Severity level	6
Example	NQA/6/NQA_SEVER_FAILURE: Failed to enable the NQA server because listening port 10000 is not available.
Explanation	Failed to enable the NQA server because the port number specified for a listening service is not available.
Recommended action	Change the port number of the listening service or disable the service that uses the port number.

NQA_START_FAILURE

Message text	NQA entry ([STRING]-[STRING]): [STRING]
Variable fields	$1: Admin name of the NQA operation. $2: Operation tag of the NQA operation. $3: Failure reason: • Operation failed due to configuration conflicts. • Operation failed because the driver was not ready to perform the operation. • Operation not supported. • Not enough resources to complete the operation. • Operation failed due to an unknown error.
Severity level	6
Example	NQA/6/NQA_START_FAILURE: NQA entry 1-1: Operation failed due to configuration conflicts.
Explanation	The message is sent when the system fails to issue an NQA operation to the drive because of the configuration conflicts.
Recommended action	**183.** Examine the parameters for the incorrect settings, modify the settings, and restart the Y.1564 operation. **184.** If the problem persists, contact NSFOCUS Support.

NQA_TWAMP_LIGHT_PACKET_INVALID

Message text	NQA TWAMP Light test session [UINT32] index [UINT32]: The number of packets captured for statistics collection is invalid.
Variable fields	$1: Test session ID. $2: Serial number of the statistics data.
Severity level	6
Example	NQA/6/ NQA_TWAMP_LIGHT_PACKET_INVALID: NQA TWAMP Light test session 1 index 7: The number of packets captured for statistics collection is invalid.
Explanation	The number of probe packets was invalid in the TWAMP Light test because the test collection interval was shorter than the packet sending interval.
Recommended action	Verify that the test collection interval is no less than the packet sending interval.

NQA_TWAMP_LIGHT_REACTION

Message text	NQA TWAMP Light test session [UINT32] reaction entry [UINT32]: Detected continual violation of the [STRING] [STRING] threshold for a threshold violation monitor time of [UINT32] ms.
Variable fields	$1: Test session ID. $2: Reaction entry ID. $3: Reaction entry type: • Two-way delay. • Two-way loss. • Two-way jitter. $4: Threshold violation value: • **upper**—Be equal to or greater than the upper threshold limit. • **lower**—Be equal to or less than the lower threshold limit. $5: Statistics collection interval.
Severity level	6
Example	NQA/6/NQA_TWAMP_LIGHT_REACTION: NQA TWAMP Light test session 1 reaction entry 1: Detected continual violation of the two-way loss upper threshold for a threshold violation monitor time of 2000 ms.
Explanation	In a TWAMP test, the device monitors the test result, and starts the monitoring time when either of the following conditions is met: • The monitoring result goes beyond the upper threshold limit. • The monitoring result drops below the lower threshold limit from a monitoring result higher than the lower limit. If either condition is always true during the monitoring time, a threshold violation occurs.

Message text	NQA TWAMP Light test session [UINT32] reaction entry [UINT32]: Detected continual violation of the [STRING] [STRING] threshold for a threshold violation monitor time of [UINT32] ms.
Recommended action	No action is required.

NQA_TWAMP_LIGHT_START_FAILURE

Message text	NQA TWAMP Light test session [UINT32]: Failed to start the test session. Please check the parameters.
Variable fields	$1: Test session ID.
Severity level	6
Example	NQAS/6/NQA_TWAMP_LIGHT_START_FAILURE: NQA TWAMP Light test session 1: Failed to start the test session, Please check the parameters.
Explanation	This message is sent when the TWAMP Light responder failed to start the test session. The message asks you to examine the parameter settings.
Recommended action	**185.** Execete the **display this** command to examine the parameter settings of the **test-session command.** **186.** Re-execute the **test-session command with the required parameters according** to your net**work requirements.**

NTP messages

This section contains NTP messages.

NTP_CLOCK_CHANGE

Message text	System clock changed from [STRING] to [STRING], the NTP server's IP address is [STRING].
Variable fields	$1: Time before synchronization. $2: Time after synchronization. $3: IP address.
Severity level	5
Example	NTP/5/NTP_CLOCK_CHANGE: System clock changed from 02:12:58 12/28/2012 to 02:29:12 12/28/2012, the NTP server's IP address is 192.168.30.116.
Explanation	The NTP client has synchronized its time to the NTP server.
Recommended action	No action is required.

NTP_LEAP_CHANGE

Message text	System Leap Indicator changed from [UINT32] to [UINT32] after clock update.
Variable fields	$1: Original Leap Indicator. $2: Current Leap Indicator.
Severity level	5
Example	NTP/5/NTP_LEAP_CHANGE: System Leap Indicator changed from 00 to 01 after clock update.
Explanation	The system Leap Indicator changed. For example, the NTP status changed from unsynchronized to synchronized. NTP Leap Indicator is a two-bit code warning of an impending leap second to be inserted in the NTP timescale. The bits are set before 23:59 on the day of insertion and reset after 00:00 on the following day. This causes the number of seconds (rolloverinterval) in the day of insertion to be increased or decreased by one.
Recommended action	No action is required.

NTP_SOURCE_CHANGE

Message text	NTP server's IP address changed from [STRING] to [STRING].
Variable fields	$1: IP address of the original time source. $2: IP address of the new time source.
Severity level	5
Example	NTP/5/NTP_SOURCE_CHANGE: NTP server's IP address changed from 1.1.1.1 to 1.1.1.2.
Explanation	The system changed the time source.
Recommended action	No action is required.

NTP_SOURCE_LOST

Message text	Lost synchronization with NTP server with IP address [STRING].
Variable fields	$1: IP address.
Severity level	5
Example	NTP/5/NTP_SOURCE_LOST: Lost synchronization with NTP server with IP address 1.1.1.1.
Explanation	The clock source of the NTP association is in unsynchronized state or it is unreachable.
Recommended action	**187.** Verify the NTP server and network connection. **188.** For NTP server failures: ○ Use the **`ntp-service unicast-server`** command to specify a new NTP server. ○ Use the **`ntp-service multicast-client`** command to configure the device to operate in NTP multicast client mode and receive NTP multicast packets from a new NTP server. **189.** If the problem persists, contract NSFOCUS Support.

NTP_STRATUM_CHANGE

Message text	System stratum changed from [UINT32] to [UINT32] after clock update.
Variable fields	$1: Original stratum. $2: Current stratum.
Severity level	5
Example	NTP/5/NTP_STRATUM_CHANGE: System stratum changed from 6 to 5 after clock update.
Explanation	System stratum has changed.
Recommended action	No action is required.

OBJP messages

This section contains object policy messages.

OBJP_ACCELERATE_NO_RES

Message text	Failed to accelerate [STRING] object-policy [STRING]. The resources are insufficient.
Variable fields	$1: Object policy version. $2: Object policy name.
Severity level	4
Example	OBJP/4/OBJP_ACCELERATE_NO_RES: Failed to accelerate IPv6 object-policy a. The resources are insufficient.
Explanation	Object policy acceleration failed because of insufficient hardware resources.
Recommended action	Delete unnecessary rules or disable acceleration for other object policies to release hardware resources.

OBJP_ACCELERATE_NOT_SUPPORT

Message text	Failed to accelerate [STRING] object-policy [STRING]. The operation is not supported.
Variable fields	$1: Object policy version. $2: Object policy name.
Severity level	4
Example	OBJP/4/OBJP_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 object-policy a. The operation is not supported.
Explanation	Object policy acceleration failed because the system did not support acceleration.
Recommended action	No action is required.

OBJP_ACCELERATE_UNK_ERR

Message text	Failed to accelerate [STRING] object-policy [STRING].
Variable fields	$1: Object policy version. $2: Object policy name.
Severity level	4
Example	OBJP/4/OBJP_ACCELERATE_UNK_ERR: Failed to accelerate IPv6 object-policy a.
Explanation	Object policy acceleration failed because of a system failure.
Recommended action	No action is required.

OBJP_RULE_CREATE_SUCCESS

Message text	RuleName(1080)=[STRING];Type(1067)=[STRING];Action(1053)=[STRING];
Variable fields	$1: Rule name. $2: Rule type. $3: Action for the rule.
Severity level	6
Example	OBJP/6/OBJP_RULE_CREATE_SUCCESS: RuleName(1080)=zone1-zone2;Type(1067)=IPv4;Action(1053)=Permit;
Explanation	An object policy rule was created successfully.
Recommended action	No action is required.

OBJP_RULE_CREATE_FAIL

Message text	RuleName(1080)=[STRING];Type(1067)=[STRING];Action(1053)=[STRING];
Variable fields	$1: Rule name. $2: Rule type. $3: Action for the rule.
Severity level	6
Example	OBJP/6/OBJP_RULE_CREATE_FAIL: RuleName(1080)=zone1-zone2;Type(1067)=IPv4;Action(1053)=Permit;
Explanation	An object policy rule failed to be created.
Recommended action	No action is required.

OBJP_RULE_UPDATE_SUCCESS

Message text	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING]; Action(1053)=[STRING];
Variable fields	$1: Rule name. $2: Rule ID. $3: Rule type. $4: Action for the rule.
Severity level	6
Example	OBJP/6/OBJP_RULE_UPDATE_SUCCESS: RuleName(1080)=zone1-zone2;RuleID(1078)=1;Type(1067)=IPv4;Action(1053)=Permit;
Explanation	An object policy rule was modified successfully.
Recommended action	No action is required.

OBJP_RULE_UPDATE_FAIL

Message text	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING];Action(1053)=[STRING];
Variable fields	$1: Rule name. $2: Rule ID. $3: Rule type. $4: Action for the rule.
Severity level	6
Example	OBJP/6/OBJP_RULE_UPDATE_FAIL: RuleName(1080)=zone1-zone2;RuleID[1078]=1;Type(1067)=IPv4;Action(1053)=Permit;
Explanation	An object policy rule failed to be modified.
Recommended action	No action is required.

OBJP_RULE_DELETE_SUCCESS

Message text	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING];
Variable fields	$1: Rule name. $2: Rule ID. $3: Rule type.
Severity level	6
Example	OBJP/6/OBJP_RULE_DELETE_SUCCESS: RuleName(1080)=zone1-zone2;RuleID(1078)=1;Type(1067)=IPv4;
Explanation	An object policy rule was deleted successfully.
Recommended action	No action is required.

OBJP_RULE_DELETE_FAIL

Message text	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING];
Variable fields	$1: Rule name. $2: Rule ID. $3: Rule type.
Severity level	6
Example	OBJP/6/OBJP_RULE_DELETE_FAIL: RuleName(1080)=zone1-zone2;RuleID(1078)=1;Type(1067)=IPv4;
Explanation	An object policy rule failed to be deleted.
Recommended action	No action is required.

OBJP_RULE_CLRSTAT_SUCCESS

Message text	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING];
Variable fields	$1: Rule name. $2: Rule ID. $3: Rule type.
Severity level	6
Example	OBJP/6/OBJP_RULE_CLRSTAT_SUCCESS: RuleName(1080)=zone1-zone2;RuleID(1078)=1;Type(1067)=IPv4;
Explanation	Statistics for an object policy rule were cleared successfully.
Recommended action	No action is required.

OBJP_RULE_CLRSTAT_FAIL

Message text	RuleName(1080)=[STRING];RuleID(1078)=[UINT32];Type(1067)=[STRING];
Variable fields	$1: Rule name. $2: Rule ID. $3: Rule type.
Severity level	6
Example	OBJP/6/OBJP_RULE_CLRSTAT_FAIL: RuleName(1080)=zone1-zone2;RuleID(1078)=1;Type(1067)=IPv4;
Explanation	Statistics for an object policy rule failed to be cleared.
Recommended action	No action is required.

OBJP_APPLY_POLICY_FAIL

Message text	Failed to apply [STRING] object policy [STRING]. The object policy does not exist.
Variable fields	$1: Object policy version. $2: Object policy name.
Severity level	4
Example	OBJP/4/OBJP_APPLY_POLICY_FAIL: Failed to apply IPv4 object policy a. The object policy does not exist.
Explanation	An object policy failed to be applied because the object policy doesn't exist.
Recommended action	No action is required.

OBJP_APPLAY_INFO

Message text	Failed to apply policy [STRING]. Reason: [STRING].
Variable fields	$1: Object policy name. $2: Failure reason.
Severity level	4
Example	OBJP/4/OBJP_APPLAY_INFO: Failed to apply policy P1. Reason: The operation is not supported.
Explanation	An object policy failed to be applied.
Recommended action	No action is required.

OFP messages

This section contains OpenFlow messages.

OFP_ACTIVE

Message text	Activate openflow instance [UINT16].
Variable fields	$1: Instance ID.
Severity level	5
Example	OFP/5/OFP_ACTIVE: Activate openflow instance 1.
Explanation	A command is received from comsh to activate an OpenFlow instance.
Recommended action	No action is required.

OFP_ACTIVE_FAILED

Message text	Failed to activate instance [UINT16].
Variable fields	$1: Instance ID.
Severity level	4
Example	OFP/4/OFP_ACTIVE_FAILED: Failed to activate instance 1.
Explanation	An OpenFlow instance cannot be activated.
Recommended action	No action is required.

OFP_CONNECT

Message text	Openflow instance [UINT16], controller [CHAR] is [STRING].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Connection status: **connected** or **disconnected**.
Severity level	5
Example	OFP/5/OFP_CONNECT: Openflow instance 1, controller 0 is connected.
Explanation	The connection status with a controller is changed in an OpenFlow instance.
Recommended action	No action is required.

OFP_FAIL_OPEN

Message text	Openflow instance [UINT16] is in fail [STRING] mode.
Variable fields	$1: Instance ID. $2: Connection interruption mode: **secure** or **standalone**.
Severity level	5
Example	OFP/5/OFP_FAIL_OPEN: Openflow instance 1 is in fail secure mode.
Explanation	An activated instance cannot connect to any controller or is disconnected from all controllers. The connection interrupt mode is also displayed.
Recommended action	No action is required.

OFP_FAIL_OPEN_FAILED

Message text	OpenFlow instance [UINT16]: [STRING] fail-open mode configuration failed and the secure mode is restored.
Variable fields	$1: Instance ID. $2: Connection interruption mode, which is **standalone**.
Severity level	4
Example	OFP/4/OFP_FAIL_OPEN_FAILED: OpenFlow instance 1: standalone fail-open mode configuration failed and the secure mode is restored.
Explanation	Because of insufficient resources, the configuration of standalone connection interruption mode (set by using the **`fail-open mode`** command) for an OpenFlow instance failed and the default secure mode was restored.
Recommended action	Contact NSFOCUS Support.

OFP_FLOW_ADD

Message text	Openflow instance [UINT16] controller [CHAR]: add flow entry [UINT32], xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Rule ID. $4: XID. $5: Cookie of the flow entry. $6: Table ID.
Severity level	5
Example	OFP/5/OFP_FLOW_ADD: Openflow instance 1 controller 0: add flow entry 1, xid 0x1, cookie 0x0, table id 0.
Explanation	A flow entry is to be added to a flow table, according to a flow table modification message that has passed the packet check.
Recommended action	No action is required.

OFP_FLOW_ADD_DUP

Message text	Openflow instance [UINT16] controller [CHAR]: add duplicate flow entry [UINT32], xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Rule ID. $4: XID. $5: Cookie. $6: Table ID.
Severity level	5
Example	OFP/5/OFP_FLOW_ADD_DUP: Openflow instance 1 controller 0: add duplicate flow entry 1, xid 0x1, cookie 0x1, table id 0.
Explanation	A duplicate flow entry was added.
Recommended action	No action is required.

OFP_FLOW_ADD_FAILED

Message text	Openflow instance [UINT16] controller [CHAR]: failed to add flow entry [UINT32], table id [CHAR].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Rule ID. $4: Table ID.
Severity level	4
Example	OFP/4/OFP_FLOW_ADD_FAILED: Openflow instance 1 controller 0: failed to add flow entry1, table id 0.
Explanation	Failed to add a flow entry.
Recommended action	No action is required.

OFP_FLOW_ADD_TABLE_MISS

Message text	Openflow instance [UINT16] controller [CHAR]: add table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
Variable fields	$1: Instance ID. $2: Controller ID. $3: XID. $4: Cookie of the flow entry. $5: Table ID.
Severity level	5
Example	OFP/5/OFP_FLOW_ADD_TABLE_MISS: Openflow instance 1 controller 0: add table miss flow entry, xid 0x1, cookie 0x0, table id 0.
Explanation	A table-miss flow entry is to be added to a flow table, according to a flow table modification message that has passed the packet check.
Recommended action	No action is required.

OFP_FLOW_ADD_TABLE_MISS_FAILED

Message text	Openflow instance [UINT16] controller [CHAR]: failed to add table miss flow entry, table id [CHAR].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Table ID.
Severity level	4
Example	OFP/4/OFP_FLOW_ADD_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to add table miss flow entry, table id 0.
Explanation	Failed to add a table-miss flow entry.
Recommended action	No action is required.

OFP_FLOW_DEL

Message text	Openflow instance [UINT16] controller [CHAR]: delete flow entry, xid 0x[HEX], cookie 0x[HEX], table id [STRING].
Variable fields	$1: Instance ID. $2: Controller ID. $3: XID. $4: Cookie of the flow entry. $5: Table ID.
Severity level	5
Example	OFP/5/OFP_FLOW_DEL: Openflow instance 1 controller 0: delete flow entry, xid 0x1, cookie 0x0, table id 0.
Explanation	A list of flow entries are to be deleted, according to a flow table modification message that has passed the packet check.
Recommended action	No action is required.

OFP_FLOW_DEL_L2VPN_DISABLE

Message text	[UINT32] flow entries in table [UINT8] of instance [UINT16] were deleted because L2VPN was disabled.
Variable fields	$1: Number of flow entries that were deleted. $2: Table ID. $3: Instance ID.
Severity level	5
Example	OFP/5/OFP_FLOW_DEL_L2VPN_DISABLE: 5 flow entries in table 1 of instance 1 were deleted because L2VPN was disabled.
Explanation	A list of flow entries were deleted because L2VPN was disabled.
Recommended action	No action is required.

OFP_FLOW_DEL_TABLE_MISS

Message text	Openflow instance [UINT16] controller [CHAR]: delete table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [STRING].
Variable fields	$1: Instance ID. $2: Controller ID. $3: XID. $4: Cookie of the flow entry. $5: Table ID.
Severity level	5
Example	OFP/5/OFP_FLOW_DEL_TABLE_MISS: Openflow instance 1 controller 0: delete table miss flow entry, xid 0x1, cookie 0x0, table id 0.
Explanation	A list of table-misses flow entries are to be deleted, according to a flow table modification message that has passed the packet check.
Recommended action	No action is required.

OFP_FLOW_DEL_TABLE_MISS_FAILED

Message text	Openflow instance [UINT16] controller [CHAR]: failed to delete table miss flow entry, table id [STRING].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Table ID.
Severity level	4
Example	OFP/4/OFP_FLOW_DEL_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to delete table miss flow entry, table id 0.
Explanation	Failed to delete a table-miss flow entry.
Recommended action	No action is required.

OFP_FLOW_DEL_VSIIF_DEL

Message text	[UINT32] flow entries in table [UINT8] of instance [UINT16] were deleted because the Vsi-interface in VSI [STRING] was deleted.
Variable fields	$1: Number of flow entries that were deleted. $2: Table ID. $3: Instance ID. $4: VSI name.
Severity level	5
Example	OFP/5/OFP_FLOW_DEL_VSIIF_DEL: 5 flow entries in table 1 of instance 1 were deleted because the Vsi-interface in VSI VSI-OFP was deleted.
Explanation	A list of flow entries were deleted because a VSI interface was deleted.
Recommended action	No action is required.

OFP_FLOW_DEL_VXLAN_DEL

Message text	[UINT32] flow entries in table [UINT8] of instance [UINT16] were deleted because a tunnel (ifindex [UINT32]) in VXLAN [UINT32] was deleted.
Variable fields	$1: Number of flow entries that were deleted. $2: Table ID. $3: Instance ID. $4: Index of a tunnel interface. $5: VXLAN ID.
Severity level	5
Example	OFP/5/OFP_FLOW_DEL_VXLAN_DEL: 5 flow entries in table 1 of instance 1 were deleted because a tunnel (ifindex 1693) in VXLAN 1000 was deleted.
Explanation	A list of flow entries were deleted because a VXLAN tunnel was deleted.
Recommended action	No action is required.

OFP_FLOW_MOD

Message text	Openflow instance [UINT16] controller [CHAR]: modify flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
Variable fields	$1: Instance ID. $2: Controller ID. $3: XID. $4: Cookie of the flow entry. $5: Table ID.
Severity level	5
Example	OFP/5/OFP_FLOW_MOD: Openflow instance 1 controller 0: modify flow entry, xid 0x1, cookie 0x0, table id 0.
Explanation	A list of flow entries are to be modified, according to a flow table modification message that has passed the packet check.
Recommended action	No action is required.

OFP_FLOW_MOD_FAILED

Message text	Openflow instance [UINT16] controller [CHAR]: failed to modify flow entry, table id [CHAR].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Table ID.
Severity level	4
Example	OFP/4/OFP_FLOW_MOD_FAILED: Openflow instance 1 controller 0: failed to modify flow entry, table id 0.
Explanation	Failed to modify a flow entry.
Recommended action	The controller must retry to modify the flow entry. If the flow entry still cannot be modified, the controller will delete it.

OFP_FLOW_MOD_TABLE_MISS

Message text	Openflow instance [UINT16] controller [CHAR]: modify table miss flow entry, xid 0x[HEX], cookie 0x[HEX], table id [CHAR].
Variable fields	$1: Instance ID. $2: Controller ID. $3: XID. $4: Cookie of the flow entry. $5: Table ID.
Severity level	5
Example	OFP/5/OFP_FLOW_MOD_TABLE_MISS: Openflow instance 1 controller 0: modify table miss flow entry, xid 0x1, cookie 0x0, table id 0.
Explanation	A list of flow entries are to be modified, according to a flow table modification message that has passed the packet check.
Recommended action	No action is required.

OFP_FLOW_MOD_TABLE_MISS_FAILED

Message text	Openflow instance [UINT16] controller [CHAR]: failed to modify table miss flow entry, table id [CHAR].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Table ID.
Severity level	4
Example	OFP/4/OFP_FLOW_MOD_TABLE_MISS_FAILED: Openflow instance 1 controller 0: failed to modify table miss flow entry, table id 0.
Explanation	Failed to modify a table-miss flow entry.
Recommended action	The controller must retry to modify the table-miss flow entry. If the entry still cannot be modified, the controller will delete it.

OFP_FLOW_RMV_GROUP

Message text	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted with a group_mod message.
Variable fields	$1: Rule ID. $2: Table ID. $3: Instance ID.
Severity level	5
Example	OFP/5/OFP_FLOW_RMV_GROUP: The flow entry 1 in table 0 of instance 1 was deleted with a group_mod message.
Explanation	A flow entry was deleted due to a group modification message.
Recommended action	No action is required.

OFP_FLOW_RMV_HARDTIME

Message text	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted because of a hard-time expiration.
Variable fields	$1: Rule ID. $2: Table ID. $3: Instance ID.
Severity level	5
Example	OFP/5/OFP_FLOW_RMV_HARDTIME: The flow entry 1 in table 0 of instance 1 was deleted because of a hard-time expiration.
Explanation	A flow entry was deleted because of a hard time expiration.
Recommended action	No action is required.

OFP_FLOW_RMV_IDLETIME

Message text	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted because of an idle-time expiration.
Variable fields	$1: Rule ID. $2: Table ID. $3: Instance ID.
Severity level	5
Example	OFP/5/OFP_FLOW_RMV_IDLETIME: The flow entry 1 in table 0 of instance 1 was deleted because of an idle-time expiration.
Explanation	A flow entry was deleted because of an idle time expiration.
Recommended action	No action is required.

OFP_FLOW_RMV_METER

Message text	The flow entry [UINT32] in table [CHAR] of instance [UINT16] was deleted with a meter_mod message.
Variable fields	$1: Rule ID. $2: Table ID. $3: Instance ID.
Severity level	5
Example	OFP/5/OFP_FLOW_RMV_GROUP: The flow entry 1 in table 0 of instance1 was deleted with a meter_mod message.
Explanation	A flow entry was deleted due to a meter modification message.
Recommended action	No action is required.

OFP_GROUP_ADD

Message text	Openflow instance [UINT16] controller [CHAR]: add group [STRING], xid 0x[HEX].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Group ID. $4: XID.
Severity level	5
Example	OFP/5/OFP_GROUP_ADD: Openflow instance 1 controller 0: add group 1, xid 0x1.
Explanation	A group entry is to be added to a group table, according to a group table modification message that has passed the packet check.
Recommended action	No action is required.

OFP_GROUP_ADD_FAILED

Message text	Openflow instance [UINT16] controller [CHAR]: failed to add group [STRING].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Group ID.
Severity level	4
Example	OFP/4/OFP_GROUP_ADD_FAILED: Openflow Instance 1 controller 0: failed to add group 1.
Explanation	Failed to add a group entry.
Recommended action	No action is required.

OFP_GROUP_DEL

Message text	Openflow instance [UINT16] controller [CHAR]: delete group [STRING], xid [HEX].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Group ID. $4: XID.
Severity level	5
Example	OFP/5/OFP_GROUP_DEL: Openflow instance 1 controller 0: delete group 1, xid 0x1.
Explanation	A group entry is to be deleted, according to a group table modification message that has passed the packet check.
Recommended action	No action is required.

OFP_GROUP_MOD

Message text	Openflow instance [UINT16] controller [CHAR]: modify group [STRING], xid 0x[HEX].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Group ID. $4: XID.
Severity level	5
Example	OFP/5/OFP_GROUP_MOD: Openflow instance 1 controller 0: modify group 1, xid 0x1.
Explanation	A group entry is to be modified, according to a group table modification message that has passed the packet check.
Recommended action	No action is required.

OFP_GROUP_MOD_FAILED

Message text	Openflow instance [UINT16] controller [CHAR]: failed to modify group [STRING].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Group ID.
Severity level	4
Example	OFP/4/OFP_GROUP_MOD_FAILED: Openflow instance 1 controller 0: failed to modify group 1.
Explanation	Failed to modify a group entry.
Recommended action	The controller must retry to modify the group. If the group still cannot be modified, the controller will delete it.

OFP_METER_ADD

Message text	Openflow instance [UINT16] controller [CHAR]: add meter [STRING], xid 0x[HEX].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Meter ID. $4: XID.
Severity level	5
Example	OFP/5/OFP_METER_ADD: Openflow instance 1 controller 0: add meter 1, xid 0x1.
Explanation	A meter entry is to be added to a meter table.
Recommended action	No action is required.

OFP_METER_ADD_FAILED

Message text	Openflow instance [UINT16] controller [CHAR]: failed to add meter [STRING].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Meter ID.
Severity level	4
Example	OFP/4/OFP_METER_ADD_FAILED: Openflow Instance 1 controller 0: failed to add meter 1.
Explanation	Failed to add a meter entry.
Recommended action	No action is required.

OFP_METER_DEL

Message text	Openflow instance [UINT16] controller [CHAR]: delete meter [STRING], xid 0x[HEX].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Meter ID. $4: XID.
Severity level	5
Example	OFP/5/OFP_METER_DEL: Openflow instance 1 controller 0: delete meter 1, xid 0x1.
Explanation	A meter entry is to be deleted, according to a meter table modification message that has passed the packet check.
Recommended action	No action is required.

OFP_METER_MOD

Message text	Openflow instance [UINT16] controller [CHAR]: modify meter [STRING], xid 0x[HEX].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Meter ID. $4: XID.
Severity level	5
Example	OFP/5/OFP_METER_MOD: Openflow Instance 1 controller 0: modify meter 1, xid 0x1.
Explanation	A meter entry is to be modified, according to a meter table modification message that has passed the packet check.
Recommended action	No action is required.

OFP_METER_MOD_FAILED

Message text	Openflow instance [UINT16] controller [CHAR]: failed to modify meter [STRING].
Variable fields	$1: Instance ID. $2: Controller ID. $3: Meter ID.
Severity level	4
Example	OFP/4/OFP_METER_MOD_FAILED: Openflow instance 1 controller 0: failed to modify meter 1.
Explanation	Failed to modify a meter entry.
Recommended action	The controller must retry to modify the meter entry. If the meter entry still cannot be modified, the controller will delete it.

OFP_MISS_RMV_GROUP

Message text	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted with a group_mod message.
Variable fields	$1: Table ID. $2: Instance ID.
Severity level	5
Example	OFP/5/OFP_MISS_RMV_GROUP: The table-miss flow entry in table 0 of instance 1 was deleted with a group_mod message.
Explanation	The table-miss flow entry was deleted due to a group modification message.
Recommended action	No action is required.

OFP_MISS_RMV_HARDTIME

Message text	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted because of a hard-time expiration.
Variable fields	$1: Table ID. $2: Instance ID.
Severity level	5
Example	OFP/5/OFP_MISS_RMV_HARDTIME: The table-miss flow entry in table 0 of instance 1 was deleted because of a hard-time expiration.
Explanation	The table-miss flow entry was deleted because of a hard time expiration.
Recommended action	No action is required.

OFP_MISS_RMV_IDLETIME

Message text	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted because of an idle-time expiration.
Variable fields	$1: Table ID. $2: Instance ID.
Severity level	5
Example	OFP/5/OFP_MISS_RMV_IDLETIME: The table-miss flow entry in table 0 of instance 1 was deleted because of an idle-time expiration.
Explanation	The table-miss flow entry was deleted because of an idle time expiration.
Recommended action	No action is required.

OFP_MISS_RMV_METER

Message text	The table-miss flow entry in table [CHAR] of instance [UINT16] was deleted with a meter_mod message.
Variable fields	$1: Table ID. $2: Instance ID.
Severity level	5
Example	OFP/5/OFP_MISS_RMV_METER: The table-miss flow entry in table 0 of instance 1 was deleted with a meter_mod message.
Explanation	The table-miss flow entry was deleted due to a meter modification message.
Recommended action	No action is required.

OPENSRC (RSYNC) messages

This section contains OPENSRC RSYNC messages.

Synchronization success

Message text	Rsync transfer statistics(sn=[STRING]):Src files([STRING]::[STRING]) sync transfer successfully.
Variable fields	$1: Sequence number of the device. $2: IPv4 address of the server. $3: Files or folders to be synchronized on the server.
Severity level	5
Example	OPENSRC/5/SYSLOG: -MDC=1; Rsync transfer statistics(sn=2013AYU0711103):Src files(1.1.1.13::test/dir1) sync transfer successfully.
Explanation	The file synchronization succeeded.
Recommended action	No action is required.

Synchronization failure

Message text	Rsync error(sn=[STRING]):Src files([STRING]::[STRING]) [NUMBER] files transfer failed.
Variable fields	$1: Sequence number of the device. $2: IPv4 address of the server. $3: Files or folders to be synchronized on the server. $4: Number of files that failed to be synchronized.
Severity level	5
Example	OPENSRC/5/SYSLOG: -MDC=1; Rsync transfer statistics(sn=2013AYU0711103):Src files(1.1.1.13::test/dir1) 2 files transfer failed.
Explanation	The device failed to synchronize files from the server and recorded the number of files that failed to be synchronized.
Recommended action	Take actions according to the failure reasons displayed in the synchronization error log.

Synchronization error

Message text	Rsync error(sn=[STRING]): [STRING].
Variable fields	$1: Sequence number of the device. $2: Failure reasons. Available options include: ○ **error starting client-server protocol**—The RSYNC process on the device has malfunctioned and cannot provide synchronization services. ○ **error in socket IO**—An error occurred to the socket for synchronization. ○ **error in file IO**—An error occurred during file system reading. ○ **some files/attrs were not transferred (see previous errors)**—Some files or file attributes failed to be synchronized. ○ **error allocating core memory buffers**—An error occurred in memory application. ○ **timeout waiting for daemon connection**—The request for connection to the server timed out.
Severity level	5
Example	OPENSRC/5/SYSLOG: -MDC=1; Rsync error(sn=2013AYU0711103): error starting client-server protocol .
Explanation	The device recorded the synchronization failure reasons.
Recommended action	To resolve the problem, you can perform the following tasks: • Verify that the **rsync** command syntax is correct. • Verify that the server is reachable. • Verify that the local disk is not full. • Verify that the user is authorized to perform the synchronization.

OPTMOD messages

This section contains transceiver module messages.

BIAS_HIGH

Message text	[STRING]: Bias current is high.
Variable fields	$1: Interface type and number.
Severity level	2
Example	OPTMOD/2/BIAS_HIGH: GigabitEthernet1/0/13: Bias current is high.
Explanation	The bias current of the transceiver module exceeded the high threshold.
Recommended action	**190.** Execute the **display transceiver diagnosis interface** command to verify that the bias current of the transceiver module has exceeded the high threshold. **191.** Execute the **display transceiver alarm interface** command to verify that a high bias current alarm for the transceiver module has been generated and not cleared. **192.** Replace the transceiver module.

BIAS_LOW

Message text	[STRING]: Bias current is low.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/BIAS_LOW: GigabitEthernet1/0/13: Bias current is low.
Explanation	The bias current of the transceiver module went below the low threshold.
Recommended action	**193.** Execute the **display transceiver diagnosis interface** command to verify that the bias current of the transceiver module is below the low threshold. **194.** Execute the **display transceiver alarm interface** command to verify that a low bias current alarm for the transceiver module has been generated and not cleared. **195.** Replace the transceiver module.

BIAS_NORMAL

Message text	[STRING]: Bias current is normal.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/BIAS_NORMAL: GigabitEthernet1/0/13: Bias current is normal.
Explanation	The bias current of the transceiver module returned to the acceptable range.
Recommended action	No action is required.

CFG_ERR

Message text	[STRING]: Transceiver type and port configuration mismatched.
Variable fields	$1: Interface type and number.
Severity level	3
Example	OPTMOD/3/CFG_ERR: GigabitEthernet1/0/13: Transceiver type and port configuration mismatched.
Explanation	The transceiver module type does not match the port configurations.
Recommended action	Check for the transceiver module type and the current port configurations. If they mismatch, replace the transceiver module or update the port configurations.

CHKSUM_ERR

Message text	[STRING]: Transceiver information checksum error.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/CHKSUM_ERR: GigabitEthernet1/0/13: Transceiver information checksum error .
Explanation	Checksum verification on the register information on the transceiver module failed.
Recommended action	Replace the transceiver module, or contact NSFOCUS Support.

FIBER_SFPMODULE_INVALID

Message text	[STRING]: This transceiver module is not compatible with the interface card. HP does not guarantee the correct operation of the transceiver module. The transceiver module will be invalidated in [UINT32] days. Please replace it with a compatible one as soon as possible.
Variable fields	$1: Interface type and number. $2: Number of days that the transceiver module will be invalid.
Severity level	4
Example	OPTMOD/4/FIBER_SFPMODULE_INVALID: GigabitEthernet1/0/13: This transceiver module is not compatible with the interface card. HP does not guarantee the correct operation of the transceiver module. The transceiver module will be invalidated in 3 days. Please replace it with a compatible one as soon as possible.
Explanation	The transceiver module is not compatible with the interface card.
Recommended action	Replace the transceiver module.

FIBER_SFPMODULE_NOWINVALID

Message text	[STRING]: This is not a supported transceiver for this platform. HP does not guarantee the normal operation or maintenance of unsupported transceivers. Please review the platform datasheet on the HP web site or contact your HP sales rep for a list of supported transceivers.
Variable fields	$1: Interface type and number.
Severity level	4
Example	OPTMOD/4/FIBER_SFPMODULE_NOWINVALID: GigabitEthernet1/0/13: This is not a supported transceiver for this platform. HP does not guarantee the normal operation or maintenance of unsupported transceivers. Please review the platform datasheet on the HP web site or contact your HP sales rep for a list of supported transceivers.
Explanation	The system does not support the transceiver module.
Recommended action	Replace the transceiver module.

IO_ERR

Message text	[STRING]: The transceiver information I/O failed.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/IO_ERR: GigabitEthernet1/0/13: The transceiver information I/O failed.
Explanation	The device failed to access the register information of the transceiver module.
Recommended action	Execute the **display transceiver diagnosis interface** and **display transceiver alarm interface** commands. If both commands fail to be executed, the transceiver module is faulty. Replace the transceiver module.

MOD_ALM_OFF

Message text	[STRING]: [STRING] was removed.
Variable fields	$1: Interface type and number. $2: Fault type.
Severity level	5
Example	OPTMOD/5/MOD_ALM_OFF: GigabitEthernet1/0/13: Module_not_ready was removed..
Explanation	A fault was removed from the transceiver module.
Recommended action	No action is required.

MOD_ALM_ON

Message text	[STRING]: [STRING] was detected.
Variable fields	$1: Interface type and number. $2: Fault type.
Severity level	5
Example	OPTMOD/5/MOD_ALM_ON: GigabitEthernet1/0/13: Module_not_ready wasdetected.
Explanation	A fault was detected on the transceiver module.
Recommended action	**196.** Execute the **display transceive alarm interface** command to verify that a corresponding alarm for the fault has been generated and not cleared. **197.** Replace the transceiver module.

MODULE_IN

Message text	[STRING]: The transceiver is [STRING].
Variable fields	$1: Interface type and number. $2: Type of the transceiver module.
Severity level	4
Example	OPTMOD/4/MODULE_IN: GigabitEthernet1/0/13: The transceiver is 1000_BASE_T_AN_SFP.
Explanation	When a transceiver module is inserted, the OPTMOD module generates the message to display the transceiver module type.
Recommended action	No action is required.

MODULE_OUT

Message text	[STRING]: Transceiver absent.
Variable fields	$1: Interface type and number.
Severity level	4
Example	OPTMOD/4/MODULE_OUT: GigabitEthernet1/0/13: The transceiver is absent.
Explanation	The transceiver module was removed.
Recommended action	No action is required.

OPTMOD_COUNTERFEIT_MOUDULE

Message text	The following might be counterfeited NSFOCUS transceivers. Please contact the supplier to verify their authenticity. NSFOCUS reserves the right to pursue legal actions. [STRING]: Transceiver type [STRING], SN [STRING].
Variable fields	$1: Interface type and number. $2: Transceiver type. $3: Transceiver sequence number.
Severity level	3
Example	OPTMOD/3/OPTMOD_COUNTERFEIT_MODULE: The following might be counterfeited NSFOCUS transceivers. Please contact the supplier to verify their authenticity. NSFOCUS reserves the right to pursue legal actions. GigabitEthernet1/0/1: Transceiver type 1000_BASE_SX_SFP, SN 2013AYU0711103. GigabitEthernet1/0/2: Transceiver type 1000_BASE_SX_SFP, SN 2013AYU0711103.
Explanation	This log is generated when a probably counterfeited NSFOCUS transceiver module is detected. For a counterfeit NSFOCUS transceiver module, you cannot obtain any data from the **`display transceiver diagnosis`** command.
Recommended action	Contact Technical Support.

OPTMOD_MODULE_CHECK

Message text	An NSFOCUS transceiver is detected. Please go to the website www.nsfocus.com.cn to verify its authenticity.
Variable fields	N/A
Severity level	6
Example	OPTMOD/6/OPTMOD_MODULE_CHECK: An NSFOCUS transceiver is detected. Please go to the website www.nsfocus.com.cn to verify its authenticity.
Explanation	The log is generated when an NSFOCUS transceiver module is detected. It reminds the user to verify the authenticity of the transceiver module from the NSFOCUS website (www.nsfocus.com.cn).
Recommended action	No action is required.

PHONY_MODULE

Message text	[STRING]: A non-NSFOCUS transceiver is detected. Please confirm the label of the transceiver. If there is an NSFOCUS Logo, it is suspected to be a counterfeit NSFOCUS transceiver. This transceiver is not sold by NSFOCUS. NSFOCUS does not guarantee the correct operation of the module or assume maintenance responsibility.
Variable fields	$1: Interface type and number.
Severity level	4
Example	OPTMOD/4/PHONY_MODULE: GigabitEthernet1/0/1: A non-NSFOCUStransceiver is detected. Please confirm the label of the transceiver. If there is an NSFOCUS Logo, it is suspected to be a counterfeit NSFOCUS transceiver. This transceiver is not sold by NSFOCUS. NSFOCUS does not guarantee the correct operation of the module or assume maintenance responsibility.
Explanation	This log is generated when a non-NSFOCUS transceiver module is detected.
Recommended action	Purchase and use genuine NSFOCUS transceiver modules for the device.

RX_ALM_OFF

Message text	STRING]: [STRING] was removed.
Variable fields	$1: Interface type and number. $2: RX fault type.
Severity level	5
Example	OPTMOD/5/RX_ALM_OFF: GigabitEthernet1/0/13: RX_not_ready was removed.
Explanation	An RX fault was removed from the transceiver module.
Recommended action	No action is required.

RX_ALM_ON

Message text	[STRING]: [STRING] was detected.
Variable fields	$1: Interface type and number. $2: RX fault type.
Severity level	5
Example	OPTMOD/5/RX_ALM_ON: GigabitEthernet1/0/13: RX_not_ready was detected.
Explanation	An RX fault was detected on the transceiver module.
Recommended action	**198.** Execute the **display transceiver alarm interface** command to verify that a corresponding alarm for the fault has been generated and not cleared. **199.** Replace the transceiver module.

RX_POW_HIGH

Message text	[STRING]: RX power is high.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/RX_POW_HIGH: GigabitEthernet1/0/13: RX power is high.
Explanation	The RX power of the transceiver module exceeded the high threshold.
Recommended action	**200.** Execute the **display transceiver diagnosis interface** command to verify that the RX power of the transceiver module has exceeded the high threshold. **201.** Execute the **display transceiver alarm interface** command to verify that a high RX power alarm for the transceiver module has been generated and not cleared. **202.** Replace the transceiver module.

RX_POW_LOW

Message text	[STRING]: RX power is low.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/RX_POW_LOW: GigabitEthernet1/0/13: RX power is low.
Explanation	The RX power of the transceiver module went below the low threshold.
Recommended action	**203.** Execute the **display transceiver diagnosis interface** command to verify that the RX power of the transceiver module is below the low threshold. **204.** Execute the **display transceiver alarm interface** command to verify that a low RX power alarm for the transceiver module has been generated and not cleared. **205.** Replace the transceiver module.

RX_POW_NORMAL

Message text	[STRING]: RX power is normal.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/RX_POW_NORMAL: GigabitEthernet1/0/13: RX power is normal.
Explanation	The RX power of the transceiver module returned to the acceptable range.
Recommended action	No action is required.

TEMP_HIGH

Message text	[STRING]: Temperature is high.
Variable fields	$1: Interface type and number
Severity level	5
Example	OPTMOD/5/TEMP_HIGH: GigabitEthernet1/0/13: Temperature is high.
Explanation	The temperature of the transceiver module exceeded the high threshold.
Recommended action	**206.** Verify that the fan trays are operating correctly. ○ If there are no fan trays, install fan trays. ○ If the fan trays fail, replace the fan trays. **207.** Verify that the ambient temperature is in the acceptable range. If it is out of the acceptable range, take measures to lower the temperature. **208.** Replace the transceiver module.

TEMP_LOW

Message text	[STRING]: Temperature is low.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/TEMP_LOW: GigabitEthernet1/0/13: Temperature is low.
Explanation	The temperature of the transceiver module went below the low threshold.
Recommended action	**209.** Verify that the ambient temperature is in the acceptable range. If it is out of the acceptable range, take measures to raise the temperature. **210.** Replace the transceiver module.

TEMP_NORMAL

Message text	[STRING]: Temperature is normal.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/TEMP_NORMAL: GigabitEthernet1/0/13: Temperature is normal.
Explanation	The temperature of the transceiver module returned to the acceptable range.
Recommended action	No action is required.

TX_ALM_OFF

Message text	[STRING]: [STRING] was removed.
Variable fields	$1: Interface type and number. $2: TX fault type.
Severity level	5
Example	OPTMOD/5/TX_ALM_OFF: GigabitEthernet1/0/13: TX_fault was removed.
Explanation	A TX fault was removed from the transceiver module.
Recommended action	No action is required.

TX_ALM_ON

Message text	[STRING]: [STRING] was detected.
Variable fields	$1: Interface type and number. $2: TX fault type.
Severity level	5
Example	OPTMOD/5/TX_ALM_ON: GigabitEthernet1/0/13: TX_fault was detected.
Explanation	A TX fault was detected on the transceiver module.
Recommended action	**211.** Execute the **`display transceiver alarm interface`** command to verify that a corresponding alarm for the fault has been generated and not cleared. **212.** Replace the transceiver module.

TX_POW_HIGH

Message text	[STRING]: TX power is high.
Variable fields	$1: Interface type and number.
Severity level	2
Example	OPTMOD/2/TX_POW_HIGH: GigabitEthernet1/0/13: TX power is high.
Explanation	The TX power of the transceiver module exceeded the high threshold.
Recommended action	**213.** Execute the **display transceiver diagnosis interface** command to verify that the TX power of the transceiver module has exceeded the high threshold. **214.** Execute the **display transceiver alarm interface** command to verify that a high TX power alarm for the transceiver module has been generated and not cleared. **215.** Replace the transceiver module.

TX_POW_LOW

Message text	[STRING]: TX power is low.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/TX_POW_LOW: GigabitEthernet1/0/13: TX power is low.
Explanation	The TX power of the transceiver module went below the low threshold.
Recommended action	**216.** Execute the **display transceiver diagnosis interface** command to verify that the TX power of the transceiver module is below the low threshold. **217.** Execute the **display transceiver alarm interface** command to verify that a low TX power alarm for the transceiver module has been generated and not cleared. **218.** Replace the transceiver module.

TX_POW_NORMAL

Message text	[STRING]: TX power is normal.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/TX_POW_NORMAL: GigabitEthernet1/0/13: TX power is normal.
Explanation	The TX power of the transceiver module returned to the acceptable range.
Recommended action	No action is required.

TYPE_ERR

Message text	[STRING]: The transceiver type is not supported by port hardware.
Variable fields	$1: Interface type and number.
Severity level	3
Example	OPTMOD/3/TYPE_ERR: GigabitEthernet1/0/13: The transceiver type is not supported by port hardware.
Explanation	The transceiver module is not supported by the port.
Recommended action	Replace the transceiver module.

VOLT_HIGH

Message text	[STRING]: Voltage is high.
Variable fields	$1: Interface type and number
Severity level	5
Example	OPTMOD/5/VOLT_HIGH: GigabitEthernet1/0/13: Voltage is high.
Explanation	The voltage of the transceiver module exceeded the high threshold.
Recommended action	**219.** Execute the **display transceiver diagnosis interface** command to verify that the voltage of the transceiver module has exceeded the high threshold. **220.** Execute the **display transceiver alarm interface** command to verify that a high voltage alarm for the transceiver module has been generated and not cleared. **221.** Replace the transceiver module.

VOLT_LOW

Message text	[STRING]: Voltage is low.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/VOLT_LOW: GigabitEthernet1/0/13: Voltage is low.
Explanation	The voltage of the transceiver module went below the low threshold.
Recommended action	**222.** Execute the **display transceiver diagnosis interface** command to verify that the voltage of the transceiver module is below the low threshold. **223.** Execute the **display transceiver alarm interface** command to verify that a low voltage alarm for the transceiver module has been generated and not cleared. **224.** Replace the transceiver module.

VOLT_NORMAL

Message text	[STRING]: Voltage is normal.
Variable fields	$1: Interface type and number.
Severity level	5
Example	OPTMOD/5/VOLT_NORMAL: GigabitEthernet1/0/13: Voltage is normal.
Explanation	The voltage of the transceiver module returned to the acceptable range.
Recommended action	No action is required.

OSPF messages

This section contains OSPF messages.

OSPF_IP_CONFLICT_INTRA

Message text	OSPF [UINT16] Received newer self-originated network-LSAs. Possible conflict of IP address [IPADDR] in area [STRING] on interface [STRING].
Variable fields	$1: OSPF process ID. $2: IP address. $3: OSPF area ID. $4: Interface name.
Severity level	6
Example	OSPF/6/OSPF_IP_CONFLICT_INTRA: OSPF 1 Received newer self-originated network-LSAs. Possible conflict of IP address 11.1.1.1 in area 0.0.0.1 on interface GigabitEthernet0/0/3.
Explanation	The interfaces on two devices in the same OSPF area might have the same primary IP address. At least one of the devices is a DR.
Recommended action	Modify IP address configuration after you make sure no router ID conflict occurs in the same OSPF area.

OSPF_RTRID_CONFLICT_INTRA

Message text	OSPF [UINT16] Received newer self-originated router-LSAs. Possible conflict of router ID [STRING] in area [STRING].
Variable fields	$1: OSPF process ID. $2: Router ID. $3: OSPF area ID.
Severity level	6
Example	OSPF/6/OSPF_RTRID_CONFLICT_INTRA: OSPF 1 Received newer self-originated router-LSAs. Possible conflict of router ID 11.11.11.11 in area 0.0.0.1.
Explanation	Two indirectly connected devices in the same OSPF area might have the same router ID.
Recommended action	Modify the router ID on one device and use the **reset ospf process** command to make the new router ID take effect.

OSPF_RTRID_CONFLICT_INTER

Message text	OSPF [UINT16] Received newer self-originated ase-LSAs. Possible conflict of router ID [STRING].
Variable fields	$1: OSPF process ID. $2: Router ID.
Severity level	6
Example	OSPF/6/OSPF_RTRID_CONFILICT_INTER: OSPF 1 Received newer self-originated ase-LSAs. Possible conflict of router ID 11.11.11.11.
Explanation	Two indirectly connected devices in the same OSPF area might have the same router ID. One of the devices is an ASBR.
Recommended action	Modify the router ID on one device and use the **reset ospf process** command to make the new router ID take effect.

OSPF_DUP_RTRID_NBR

Message text	OSPF [UINT16] Duplicate router ID [STRING] on interface [STRING], sourced from IP address [IPADDR].
Variable fields	$1: OSPF process ID. $2: Router ID. $3: Interface name. $4: IP address.
Severity level	6
Example	OSPF/6/OSPF_DUP_RTRID_NBR: OSPF 1 Duplicate router ID 11.11.11.11 on interface GigabitEthernet0/0/3, sourced from IP address 11.2.2.2.
Explanation	Two directly connected devices were configured with the same router ID.
Recommended action	Modify the router ID on one device and use the **reset ospf process** command to make the new router ID take effect.

OSPF_LAST_NBR_DOWN

Message text	OSPF [UINT32] Last neighbor down event: Router ID: [STRING] Local address: [STRING] Remote address: [STRING] Reason: [STRING]
Variable fields	$1: OSPF process ID. $2: Router ID. $3: Local IP address. $4: Neighbor IP address. $5: Reason.
Severity level	6
Example	OSPF/6/OSPF_LAST_NBR_DOWN: OSPF 1 Last neighbor down event: Router ID: 2.2.2.2 Local address: 10.1.1.1 Remote address: 10.1.1.2 Reason: Dead Interval timer expired.
Explanation	The device records the OSPF neighbor down event caused by a specific reason.
Recommended action	• When a down event occurred because of configuration changes (for example, interface parameter changes), check for the configuration errors. • When a down event occurred because of dead interval expiration, check for the dead interval configuration error and loss of network connectivity. • When a down event occurred because of BFD session down, check for the BFD detection time configuration error and loss of network connectivity. • When a down event occurred because of interface status changes, check for loss of network connectivity.

OSPF_MEM_ALERT

Message text	OSPF Process received system memory alert [STRING] event.
Variable fields	$1: Type of the memory alarm.
Severity level	5
Example	OSPF/5/OSPF_MEM_ALERT: OSPF Process received system memory alert start event.
Explanation	OSPF received a memory alarm.
Recommended action	Check the system memory and release memory for the modules that occupy too many memory resources.

OSPF_NBR_CHG

Message text	OSPF [UINT32] Neighbor [STRING] ([STRING]) changed from [STRING] to [STRING].
Variable fields	$1: OSPF process ID. $2: Neighbor router ID. $3: Interface name. $4: Old adjacency state. $5: New adjacency state.
Severity level	5
Example	OSPF/5/OSPF_NBR_CHG: OSPF 1 Neighbor 2.2.2.2 (Vlan-interface100) changed from Full to Down.
Explanation	The OSPF adjacency state changed on an interface.
Recommended action	When the adjacency with a neighbor changes from **Full** to another state on an interface, check for OSPF configuration errors and loss of network connectivity.

OSPF_RT_LMT

Message text	OSPF [UINT32] route limit reached.
Variable fields	$1: OSPF process ID.
Severity level	4
Example	OSPF/4/OSPF_RT_LMT: OSPF 1 route limit reached.
Explanation	The number of routes of an OSPF process reached the upper limit.
Recommended action	**225.** Check for network attacks. **226.** Reduce the number of routes.

OSPF_RTRID_CHG

Message text	OSPF [UINT32] New router ID elected, please restart OSPF if you want to make the new router ID take effect.
Variable fields	$1: OSPF process ID.
Severity level	5
Example	OSPF/5/OSPF_RTRID_CHG: OSPF 1 New router ID elected, please restart OSPF if you want to make the new router ID take effect.
Explanation	The OSPF router ID was changed because the user had changed the router ID or the interface IP address used as the router ID had changed.
Recommended action	Use the **reset ospf process** command to make the new router ID take effect.

OSPF_VLINKID_CHG

Message text	OSPF [UINT32] Router ID changed, reconfigure Vlink on peer
Variable fields	$1: OSPF process ID.
Severity level	5
Example	OSPF/5/OSPF_VLINKID_CHG:OSPF 1 Router ID changed, reconfigure Vlink on peer
Explanation	A new OSPF router ID takes effect.
Recommended action	Check and modify the virtual link configuration on the peer router to match the new router ID.

OSPFV3 messages

This section contains OSPFv3 messages.

OSPFV3_LAST_NBR_DOWN

Message text	OSPFv3 [UINT32] Last neighbor down event: Router ID: [STRING] Local interface ID: [UINT32] Remote interface ID: [UINT32] Reason: [STRING].
Variable fields	$1: OSPFv3 process ID. $2: Router ID. $3: Local interface ID. $4: Remote interface ID. $5: Reason.
Severity level	6
Example	OSPFV3/6/OSPFV3_LAST_NBR_DOWN: OSPFv3 1 Last neighbor down event: Router ID: 2.2.2.2 Local interface ID: 1111 Remote interface ID: 2222 Reason: Dead Interval timer expired.
Explanation	The device records the OSPFv3 neighbor down event caused by a specific reason.
Recommended action	• When a down event occurred because of configuration changes (for example, interface parameter changes), check for the configuration errors. • When a down event occurred because of dead interval expiration, check for the dead interval configuration error and loss of network connectivity. • When a down event occurred because of BFD session down, check for the BFD detection time configuration error and loss of network connectivity. • When a down event occurred because of interface status changes, check for loss of network connectivity.

OSPFV3_MEM_ALERT

Message text	OSPFV3 Process received system memory alert [STRING] event.
Variable fields	$1: Type of the memory alarm.
Severity level	5
Example	OSPFV3/5/OSPFV3_MEM_ALERT: OSPFV3 Process received system memory alert start event.
Explanation	OSPFv3 received a memory alarm.
Recommended action	Check the system memory and release memory for the modules that occupy too many memory resources.

OSPFV3_NBR_CHG

	Message text	OSPFv3 [UINT32] Neighbor [STRING] ([STRING]) received [STRING] and its state from [STRING] to [STRING].
	Variable fields	$1: Process ID. $2: Neighbor router ID. $3: Interface name. $4: Neighbor event. $5: Old adjacency state. $6: New adjacency state.
	Severity level	5
	Example	OSPFV3/5/OSPFV3_NBR_CHG: OSPFv3 1 Neighbor 2.2.2.2 (Vlan100) received 1-Way and its state from Full to Init.
	Explanation	The OSPFv3 adjacency state changed on an interface.
	Recommended action	When the adjacency with a neighbor changes from **Full** to another state on an interface, check for OSPFv3 configuration errors and loss of network connectivity.

OSPFV3_RT_LMT

Message text	OSPFv3 [UINT32] route limit reached.
Variable fields	$1: Process ID.
Severity level	5
Example	OSPFV3/5/OSPFV3_RT_LMT:OSPFv3 1 route limit reached.
Explanation	The number of routes of an OSPFv3 process reached the upper limit.
Recommended action	**227.** Check for network attacks. **228.** Reduce the number of routes.

PBB messages

This section contains PBB messages.

PBB_JOINAGG_WARNING

Message text	Because the aggregate interface [STRING] has been configured with PBB, assigning the interface [STRING] that does not support PBB to the aggregation group will cause incorrect processing.
Variable fields	$1: Aggregation group name. $2: Interface name.
Severity level	4
Example	PBB/4/PBB_JOINAGG_WARNING: Because the aggregate interface Bridge-Aggregation1 has been configured with PBB, assigning the interface Ten-GigabitEthernet9/0/30 that does not support PBB to the aggregation group will cause incorrect processing.
Explanation	Assigning an interface that does not support PBB to an aggregation group that has been configured with PBB will cause incorrect processing. If an aggregate interface is a PBB uplink port, all its members should support PBB.
Recommended action	Remove the interface from the aggregation group.

PBR messages

This section contains PBR messages.

PBR_HARDWARE_ERROR

Message text	Failed to update policy [STRING] due to [STRING].
Variable fields	$1: Policy name. $2: Hardware error reasons: • **insufficient hardware resources**. • **unsupported operations**. • **insufficient hardware resources and unsupported operations**.
Severity level	4
Example	PBR/4/PBR_HARDWARE_ERROR: Failed to update policy aaa due to insufficient hardware resources and not supported operations.
Explanation	The device failed to update PBR configuration.
Recommended action	Modify the PBR policy configuration according to the failure reason.

PCAPWARE messages

This section contains PCAPWARE messages.

PCAPWARE_STOP

Message text	Phe packet capture stopped because [STRING].
Variable fields	$1: Reason why packet capture stopped: ○ the packet file size exceeded the storage limit. ○ the interface went down.
Severity level	5
Example	PCAPWARE/5/PCAPWARE_STOP: Packet capture stopped because the packet file size exceeded the storage limit.
Explanation	The packet capture stopped because the maximum storage space for .cap files on the device was reached.
Recommended action	Use one of the following methods: • Increase the maximum storage space for .cap files on the device. • Export the existing .cap files on the device. • Save the .cap files to a remote file server. • Bring up the interface.

PCE messages

This section contains PCE messages.

PCE_PCEP_SESSION_CHG

Message text	Session ([STRING], [STRING]) is [STRING].

Variable fields	$1: Peer address of the session.
	$2: VPN instance name. Value **unknown** indicates that the VPN instance cannot be obtained.
	$3: State of the session, **up** or **down**. When the state is **down**, this field also displays the reason for the down state error. Possible reasons include:
	• TCP connection down.
	• received a close message. The device receives a close message from the peer when the peer encounters one of the following situations:
	  ○ No explanation provided. (The session is closed because the idle time of the session exceeds three minutes.)
	  ○ DeadTimer expired.
	  ○ Reception of a malformed PCEP message.
	  ○ Reception of an unacceptable number of unknown requests/replies.
	  ○ Reception of an unacceptable number of unrecognized PCEP messages.
	• reception of a malformed PCEP message.
	• internal error.
	• memory in critical state.
	• dead timer expired.
	• process deactivated.
	• remote peer unavailable/untriggered.
	• reception of an unacceptable number of unrecognized PCEP messages.
	• reception of an unacceptable number of unknown requests/replies.
	• PCE address changed.
	• initialization failed.

Severity level	5
Example	PCE/5/PCE_PCEP_SESSION_CHG: Session (22.22.22.2, public instance) is up. PCE/5/PCE_PCEP_SESSION_CHG: Session (22.22.22.2, public instance) is down (dead timer expired).
Explanation	The session state changed.
Recommended action	When the session state is up, no action is required. When the session state is down, verify the network and configuration according to the reason displayed.

PEX messages

This section contains PEX messages.

PEX_CONFIG_ERROR

Message text	PEX port [UINT32] discarded a REGISTER request received from [STRING] through interface [STRING]. Reason: The PEX was not assigned an ID, or the PEX was assigned an ID equal to or greater than the maximum value ([UINT32]).
Variable fields	$1: PEX port ID. $2: PEX model. $3: Name of a PEX physical interface. $4: Maximum virtual slot or chassis number for the PEX model.
Severity level	4
Example	PEX/4/PEX_CONFIG_ERROR: PEX port 1 discarded a REGISTER request received from PEX-S5120HI-S5500HI through interface Ten-GigabitEthernet10/0/31. Reason: The PEX was not assigned an ID, or the PEX was assigned an ID equal to or greater than the maximum value 130.
Explanation	This message is generated in the following situations: • The PEX is not assigned a virtual slot or chassis number. • The PEX is assigned a virtual slot or chassis number that is greater than the maximum value allowed for the PEX model.
Recommended action	Use the **associate** command to assign a valid virtual slot or chassis number to the PEX. Make sure the slot or chassis number is within the value range for the PEX model.

PEX_CONNECTION_ERROR

Message text	PEX port [UINT32] discarded a REGISTER request received from [STRING] through interface [STRING]. Reason: Another PEX has been registered on the PEX port.
Variable fields	$1: PEX port ID. $2: PEX model. $3: Name of a PEX physical interface.
Severity level	4
Example	PEX/4/PEX_CONNECTION_ERROR: PEX port 1 discarded a REGISTER request received from PEX-S5120HI-S5500HI through interface Ten-GigabitEthernet10/0/31. Reason: Another PEX has been registered on the PEX port.
Explanation	This message is generated if a PEX port is connected to multiple PEXs.
Recommended action	Reconnect PEXs to ensure sure that only one PEX is connected to the PEX port.

PEX_LINK_BLOCK

	Message text	Status of [STRING] changed from [STRING] to blocked.
	Variable fields	$1: Name of a PEX physical interface. $2: Data link status of the interface.
	Severity level	4
	Example	PEX/4/PEX_LINK_BLOCK: Status of Ten-GigabitEthernet2/0/1 changed from forwarding to blocked.
	Explanation	Data link of the PEX physical interface has changed to blocked. The blocked state is a transitional state between forwarding and down. In blocked state, a PEX physical interface can forward protocol packets, but it cannot forward data packets. This state change occurs in one of the following situations: • Incorrect physical connection: ○ The PEX physical links on a PEX are connected to different PEX ports on the parent device. ○ The PEX port on the parent device contains physical links to different PEXs. • The data link is forced to the blocked state. In the startup phase, a PEX blocks the link of a PEX physical interface if the interface is physically up, but it is not used for loading startup software. • The physical state of the interface is up, but the PEX connection between

		the PEX and the parent device has been disconnected. The PEX and the parent device cannot receive PEX heartbeat packets from each other.
	Recommended action	If a down PEX link changes from blocked to up quickly, you do not need to take action. If the link stays in blocked state, check the PEX cabling to verify that: • The PEX's all PEX physical interfaces are connected to the physical interfaces assigned to the same PEX port on the parent device. • The PEX port contains only physical links to the same PEX. If a forwarding PEX link stays in blocked state when it is changing to the down state, verify that an IRF fabric split has occurred. When an IRF fabric split occur, a PEX link is be blocked if it is connected to the Recovery-state IRF member device.

PEX_LINK_DOWN

Message text	Status of [STRING] changed from [STRING] to down.
Variable fields	$1: Name of a PEX physical interface. $2: Data link status of the interface.
Severity level	4
Example	PEX/4/PEX_LINK_DOWN: Status of Ten-GigabitEthernet2/0/1 changed from forwarding to down.
Explanation	Data link of the PEX physical interface has changed to the down state and cannot forward any packets. The following are common reasons for this state change: • Physical link fails. • The interface is shut down administratively. • The system reboots.
Recommended action	If the interface has been shut down administratively or in the down state because of a system reboot, use the **undo shutdown** command to bring up the interface as needed. If the interface is down because of a physical link failure, verify that the cable has been securely connected and is in good condition.

PEX_LINK_FORWARD

Message text	Status of [STRING] changed from [STRING] to forwarding.
Variable fields	$1: Name of a PEX physical interface. $2: Data link status of the interface.
Severity level	5
Example	PEX/5/PEX_LINK_FORWARD: Status of Ten-GigabitEthernet2/0/1 changed from blocked to forwarding.
Explanation	Data link of the PEX physical interface has changed to the forwarding state and can forward data packets. This link state change occurs when one of the following events occurs: • The link is detected again after it changes to the blocked state. • The PEX finishes loading startup software images from the parent device through the interface.
Recommended action	No action is required.

PEX_REG_JOININ

	Message text	PEX ([STRING]) registered successfully on PEX port [UINT32].
	Variable fields	$1: Virtual slot or chassis number of a PEX. $2: PEX port ID.
	Severity level	5
	Example	PEX/5/PEX_REG_JOININ: PEX (slot 101) registered successfully on PEX port 1.
	Explanation	The PEX has been registered successfully. You can configure and manage the PEX attached to the PEX port on the parent device as if the PEX was an interface card.
	Recommended action	No action is required.

PEX_REG_LEAVE

	Message text	PEX ([STRING]) unregistered on PEX port [UINT32].
	Variable fields	$1: Virtual slot or chassis number of a PEX. $2: PEX port ID.
	Severity level	4
	Example	PEX/4/PEX_REG_LEAVE: PEX (slot 101) unregistered on PEX port 1.
	Explanation	The PEX has been unregistered. You cannot operate the PEX from the parent device. A PEX unregister event occurs when one of the following events occurs: • The PEX reboots. • All physical interfaces in the PEX port are down. For example, all physical interfaces are shut down administratively, or all the physical links are disconnected. • The PEX fails to start up within 30 minutes. • Link detection fails on all physical interfaces in the PEX port.
	Recommended action	If the event occurs because the PEX reboots or PEX physical interfaces are shut down administratively, use the **undo shutdown** command to bring up the interfaces as needed. To resolve the issue that occurs for any other reasons: • Use the **display device**

		command to verify that the virtual slot or chassis number of the PEX is present and the state is correct. • Use the **`display pex-port`** command to verify that the PEX physical interfaces are configured correctly and in a correct state. • Use the **`display interface`** command to verify that the physical state of the PEX physical interfaces is up. If the **Current state** field displays down, check the cabling for a physical link failure.

PEX_REG_REQUEST

Message text		Received a REGISTER request on PEX port [UINT32] from PEX ([STRING]).
Variable fields		$1: PEX port ID. $2: Virtual slot or chassis number of a PEX.
Severity level		5
Example		PEX/5/PEX_REG_REQUEST: Received a REGISTER request on PEX port 1 from PEX (slot 101).
Explanation		The PEX sent a registration request to the parent device. This event occurs when the PEX starts up after PEX configuration is completed and the PEX device is connected to the patent device correctly. The parent device will allow the PEX to load startup software images after it receives a REGISTER request.
Recommended action		No action is required.

PFILTER messages

This section contains packet filter messages.

PFILTER_APPLYUSER_FAIL

		[STRING]; Failed to apply [STRING] ACL [STRING] to the [STRING] direction of user profile [STRING]. Reason: [STRING].
		$1: User identity. $2: ACL type. $3: ACL number or name. $4: Traffic direction. $5: User profile name. $6: Failure cause.
		3
		PFILTER/3/PFILTER_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN="N/A"-Port=GigabitEthernet5/1/5; Failed to apply IPv4 ACL 2000 to the inbound direction of user profile u1. Reason: The resources are insufficient. PFILTER/3/ PFILTER_APPLYUSER_NO_RES: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN="N/A"-Port=Gigabi

	tEthernet5/1/5; Failed to apply IPv6 ACL 2000 to the outbound direction of user profile u1. Reason: Packet filtering is not supported for user profiles.
	The system failed to apply an ACL to the user profile for packet filtering for one of the following reasons: • The resources are insufficient. • The device does not support applying an ACL to the user profile for packet filtering.
	• If the resources are insufficient, delete some ACL rules to release resources. • If the device does not support the operation, apply the ACL to the interface on which the user comes online.

PFILTER_GLB_ RES_CONFLICT

Message text	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction globally. [STRING] ACL [UINT] has already been applied globally.
Variable fields	$1: ACL type. $2: ACL number. $3: Traffic direction. $4: ACL type. $5: ACL number.
Severity level	3
Example	PFILTER/3/PFILTER_GLB_ RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction globally. IPv6 ACL 3000 has already been applied globally.
Explanation	The system failed to perform one of the following actions because an ACL of the same type (IPv4 ACL, IPv6 ACL, or MAC ACL) has already been applied: • Applying the ACL to a specific direction globally. • Updating the ACL applied to a specific direction globally.
Recommended action	Remove the ACL of the same type.

PFILTER_GLB_IPV4_DACT_NO_RES

Message text	Failed to apply or refresh the IPv4 default action to the [STRING] direction globally. The resources are insufficient.
Variable fields	$1: Traffic direction.
Severity level	3
Example	PFILTER/3/PFILTER_GLB_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction globally. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying the IPv4 default action to a specific direction globally. • Updating the IPv4 default action applied to a specific direction globally.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_GLB_IPV4_DACT_UNK_ERR

Message text	Failed to apply or refresh the IPv4 default action to the [STRING] direction globally.
Variable fields	$1: Traffic direction.
Severity level	3
Example	PFILTER/3/PFILTER_GLB_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction globally.
Explanation	The system failed to perform one of the following actions due to an unknown error: • Applying the IPv4 default action to a specific direction globally. • Updating the IPv4 default action applied to a specific direction globally.
Recommended action	No action is required.

PFILTER_GLB_IPV6_DACT_NO_RES

Message text	Failed to apply or refresh the IPv6 default action to the [STRING] direction globally. The resources are insufficient.
Variable fields	$1: Traffic direction.
Severity level	3
Example	PFILTER/3/PFILTER_GLB_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction globally. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying the IPv6 default action to a specific direction globally. • Updating the IPv6 default action applied to a specific direction globally.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_GLB_IPV6_DACT_UNK_ERR

Message text	Failed to apply or refresh the IPv6 default action to the [STRING] direction globally.
Variable fields	$1: Traffic direction.
Severity level	3
Example	PFILTER/3/PFILTER_GLB_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction globally.
Explanation	The system failed to perform one of the following actions due to an unknown error: • Applying the IPv6 default action to a specific direction globally. • Updating the IPv6 default action applied to a specific direction globally.
Recommended action	No action is required.

PFILTER_GLB_MAC_DACT_NO_RES

Message text	Failed to apply or refresh the MAC default action to the [STRING] direction globally. The resources are insufficient.
Variable fields	$1: Traffic direction.
Severity level	3
Example	PFILTER/3/PFILTER_GLB_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction globally. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying the MAC default action to a specific direction globally. • Updating the MAC default action applied to a specific direction globally.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_GLB_MAC_DACT_UNK_ERR

Message text	Failed to apply or refresh the MAC default action to the [STRING] direction globally.
Variable fields	$1: Traffic direction.
Severity level	3
Example	PFILTER/3/PFILTER_GLB_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction globally.
Explanation	The system failed to perform one of the following actions due to an unknown error: • Applying the MAC default action to a specific direction globally. • Updating the MAC default action applied to a specific direction globally.
Recommended action	No action is required.

PFILTER_GLB_NO_RES

Message text	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally. The resources are insufficient.
Variable fields	$1: ACL type. $2: ACL number. $3: ACL rule ID. $4: Traffic direction.
Severity level	3
Example	PFILTER/3/PFILTER_GLB_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying an ACL rule to a specific direction globally. • Updating an ACL rule applied to a specific direction globally.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_GLB_NOT_SUPPORT

Message text	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally. The ACL is not supported.
Variable fields	$1: ACL type. $2: ACL number. $3: ACL rule ID. $4: Traffic direction.
Severity level	3
Example	PFILTER/3/PFILTER_GLB_NOT_SUPPORT: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally. The ACL is not supported.
Explanation	The system failed to perform one of the following actions because the ACL rule is not supported: • Applying an ACL rule to a specific direction globally. • Updating an ACL rule applied to a specific direction globally.
Recommended action	Verify the ACL configuration and remove the settings that are not supported.

PFILTER_GLB_UNK_ERR

Message text	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction globally.
Variable fields	$1: ACL type. $2: ACL number. $3: ACL rule ID. $4: Traffic direction.
Severity level	3
Example	PFILTER/3/PFILTER_GLB_UNK_ERR: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction globally.
Explanation	The system failed to perform one of the following actions due to an unknown error: • Applying an ACL rule to a specific direction globally. • Updating an ACL rule applied to a specific direction globally.
Recommended action	No action is required.

PFILTER_IF_IPV4_DACT_NO_RES

Message text	Failed to apply or refresh the IPv4 default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
Variable fields	$1: Traffic direction. $2: Interface name.
Severity level	3
Example	PFILTER/3/PFILTER_IF_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying the IPv4 default action to a specific direction of an interface. • Updating the IPv4 default action applied to a specific direction of an interface.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_IF_IPV4_DACT_UNK_ERR

Message text	Failed to apply or refresh the IPv4 default action to the [STRING] direction of interface [STRING].
Variable fields	$1: Traffic direction. $2: Interface name.
Severity level	3
Example	PFILTER/3/PFILTER_IF_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction of interface Ethernet 3/1/2.
Explanation	The system failed to perform one of the following actions because an unknown error: • Applying the IPv4 default action to a specific direction of an interface. • Updating the IPv4 default action applied to a specific direction of an interface.
Recommended action	No action is required.

PFILTER_IF_IPV6_DACT_NO_RES

Message text	Failed to apply or refresh the IPv6 default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
Variable fields	$1: Traffic direction. $2: Interface name.
Severity level	3
Example	PFILTER/3/PFILTER_IF_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying the IPv6 default action to a specific direction of an interface. • Updating the IPv6 default action applied to a specific direction of an interface.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_IF_IPV6_DACT_UNK_ERR

Message text	Failed to apply or refresh the IPv6 default action to the [STRING] direction of interface [STRING].
Variable fields	$1: Traffic direction. $2: Interface name.
Severity level	3
Example	PFILTER/3/PFILTER_IF_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction of interface Ethernet 3/1/2.
Explanation	The system failed to perform one of the following actions due to an unknown error: • Applying the IPv6 default action to a specific direction of an interface. • Updating the IPv6 default action applied to a specific direction of an interface.
Recommended action	No action is required.

PFILTER_IF_MAC_DACT_NO_RES

Message text	Failed to apply or refresh the MAC default action to the [STRING] direction of interface [STRING]. The resources are insufficient.
Variable fields	$1: Traffic direction. $2: Interface name.
Severity level	3
Example	PFILTER/3/PFILTER_IF_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying the MAC default action to a specific direction of an interface. • Updating the MAC default action applied to a specific direction of an interface.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_IF_MAC_DACT_UNK_ERR

Message text	Failed to apply or refresh the MAC default action to the [STRING] direction of interface [STRING].
Variable fields	$1: Traffic direction. $2: Interface name.
Severity level	3
Example	PFILTER/3/PFILTER_IF_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction of interface Ethernet 3/1/2.
Explanation	The system failed to perform one of the following actions due to an unknown error: • Applying the MAC default action to a specific direction of an interface. • Updating the MAC default action applied to a specific direction of an interface.
Recommended action	No action is required.

PFILTER_IF_NO_RES

Message text	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING]. The resources are insufficient.
Variable fields	$1: ACL type. $2: ACL number. $3: ACL rule ID. $4: Traffic direction. $5: Interface name.
Severity level	3
Example	PFILTER/3/PFILTER_IF_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying an ACL rule to a specific direction of an interface. • Updating an ACL rule applied to a specific direction of an interface.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_IF_NOT_SUPPORT

Message text	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING]. The ACL is not supported.
Variable fields	$1: ACL type. $2: ACL number. $3: ACL rule ID. $4: Traffic direction. $5: Interface name.
Severity level	3
Example	PFILTER/3/PFILTER_IF_NOT_SUPPORT: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2. The ACL is not supported.
Explanation	The system failed to perform one of the following actions because the ACL rule is not supported: • Applying an ACL rule to a specific direction of an interface. • Updating an ACL rule applied to a specific direction of an interface.
Recommended action	Verify the ACL configuration and remove the settings that are not supported.

PFILTER_IF_RES_CONFLICT

Message text	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction of interface [STRING]. [STRING] ACL [UINT] has already been applied to the interface.
Variable fields	$1: ACL type. $2: ACL number. $3: Traffic direction. $4: Interface name. $5: ACL type. $6: ACL number.
Severity level	3
Example	PFILTER/3/PFILTER_IF_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction of interface Ethernet 3/1/2. IPv6 ACL 3000 has already been applied to the interface.
Explanation	The system failed to perform one of the following actions because an ACL of the same type (IPv4 ACL, IPv6 ACL, or MAC ACL) has already been applied: • Applying the ACL to a specific direction of an interface. • Updating the ACL applied to a specific direction of an interface.
Recommended action	Remove the ACL of the same type.

PFILTER_IF_UNK_ERR

Message text	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of interface [STRING].
Variable fields	$1: ACL type. $2: ACL number. $3: ACL rule ID. $4: Traffic direction. $5: Interface name.
Severity level	3
Example	PFILTER/3/PFILTER_IF_UNK_ERR: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of interface Ethernet 3/1/2.
Explanation	The system failed to perform one of the following actions due to an unknown error: • Applying an ACL rule to a specific direction of an interface. • Updating an ACL rule applied to a specific direction of an interface.
Recommended action	No action is required.

PFILTER_IPV6_STATIS_INFO

Message text	[STRING] ([STRING]): Packet-filter IPv6 [UINT32] [STRING] [STRING] [UINT64] packet(s).
Variable fields	$1: Destination to which packet filter applies. $2: Traffic direction. $3: ACL number. $4: ID and content of an ACL rule. $5: Number of packets that matched the rule.
Severity level	6
Example	PFILTER/6/PFILTER_IPV6_STATIS_INFO: Ethernet0/4/0 (inbound): Packet-filter IPv6 2000 rule 0 permit source 1:1::/64 logging 1000 packet(s).
Explanation	The number of packets matching the packet-filter IPv6 ACL rule changed.
Recommended action	No action is required.

PFILTER_STATIS_INFO

Message text	[STRING] ([STRING]): Packet-filter [UINT32] [STRING] [UINT64] packet(s).
Variable fields	$1: Destination to which packet filter applies. $2: Traffic direction. $3: ACL number. $4: ID and content of an ACL rule. $5: Number of packets that matched the rule.
Severity level	6
Example	PFILTER/6/PFILTER_STATIS_INFO: Ethernet0/4/0 (inbound): Packet-filter 2000 rule 0 permit source 1.1.1.1 0 logging 10000 packet(s).
Explanation	The number of packets matching the packet-filter IPv4 ACL rule changed.
Recommended action	No action is required.

PFILTER_VLAN_IPV4_DACT_NO_RES

Message text	Failed to apply or refresh the IPv4 default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
Variable fields	$1: Traffic direction. $2: VLAN ID.
Severity level	3
Example	PFILTER/3/PFILTER_VLAN_IPV4_DACT_NO_RES: Failed to apply or refresh the IPv4 default action to the inbound direction of VLAN 1. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying the IPv4 default action to a specific direction of a VLAN. • Updating the IPv4 default action applied to a specific direction of a VLAN.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_VLAN_IPV4_DACT_UNK_ERR

Message text	Failed to apply or refresh the IPv4 default action to the [STRING] direction of VLAN [UINT16].
Variable fields	$1: Traffic direction. $2: VLAN ID.
Severity level	3
Example	PFILTER/3/PFILTER_VLAN_IPV4_DACT_UNK_ERR: Failed to apply or refresh the IPv4 default action to the inbound direction of VLAN 1.
Explanation	The system failed to perform one of the following actions due to an unknown error: • Applying the IPv4 default action to a specific direction of a VLAN. • Updating the IPv4 default action applied to a specific direction of a VLAN.
Recommended action	No action is required.

PFILTER_VLAN_IPV6_DACT_NO_RES

Message text	Failed to apply or refresh the IPv6 default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
Variable fields	$1: Traffic direction. $2: VLAN ID.
Severity level	3
Example	PFILTER/3/PFILTER_VLAN_IPV6_DACT_NO_RES: Failed to apply or refresh the IPv6 default action to the inbound direction of VLAN 1. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying the IPv6 default action to a specific direction of a VLAN. • Updating the IPv6 default action applied to a specific direction of a VLAN.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_VLAN_IPV6_DACT_UNK_ERR

Message text	Failed to apply or refresh the IPv6 default action to the [STRING] direction of VLAN [UINT16].
Variable fields	$1: Traffic direction. $2: VLAN ID.
Severity level	3
Example	PFILTER/3/PFILTER_VLAN_IPV6_DACT_UNK_ERR: Failed to apply or refresh the IPv6 default action to the inbound direction of VLAN 1.
Explanation	The system failed to perform one of the following actions due to an unknown error: • Applying the IPv6 default action to a specific direction of a VLAN. • Updating the IPv6 default action applied to a specific direction of a VLAN.
Recommended action	No action is required.

PFILTER_VLAN_MAC_DACT_NO_RES

Message text	Failed to apply or refresh the MAC default action to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
Variable fields	$1: Traffic direction. $2: VLAN ID.
Severity level	3
Example	PFILTER/3/PFILTER_VLAN_MAC_DACT_NO_RES: Failed to apply or refresh the MAC default action to the inbound direction of VLAN 1. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying the MAC default action to a specific direction of a VLAN. • Updating the MAC default action applied to a specific direction of a VLAN.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_VLAN_MAC_DACT_UNK_ERR

Message text	Failed to apply or refresh the MAC default action to the [STRING] direction of VLAN [UINT16].
Variable fields	$1: Traffic direction. $2: VLAN ID.
Severity level	3
Example	PFILTER/3/PFILTER_VLAN_MAC_DACT_UNK_ERR: Failed to apply or refresh the MAC default action to the inbound direction of VLAN 1.
Explanation	The system failed to perform one of the following actions due to an unknown error: • Applying the MAC default action to a specific direction of a VLAN. • Updating the MAC default action applied to a specific direction of a VLAN.
Recommended action	No action is required.

PFILTER_VLAN_NO_RES

Message text	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16]. The resources are insufficient.
Variable fields	$1: ACL type. $2: ACL number. $3: ACL rule ID. $4: Traffic direction. $5: VLAN ID.
Severity level	3
Example	PFILTER/3/PFILTER_VLAN_NO_RES: Failed to apply or refresh IPv6 ACL 2000 rule 1 to the inbound direction of VLAN 1. The resources are insufficient.
Explanation	The system failed to perform one of the following actions because hardware resources are insufficient: • Applying an ACL rule to a specific direction of a VLAN. • Updating an ACL rule applied to a specific direction of a VLAN.
Recommended action	Use the **display qos-acl resource** command to check hardware resource usage.

PFILTER_VLAN_NOT_SUPPORT

Message text	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16]. The ACL is not supported.
Variable fields	$1: ACL type. $2: ACL number. $3: ACL rule ID. $4: Traffic direction. $5: VLAN ID.
Severity level	3
Example	PFILTER/3/PFILTER_VLAN_NOT_SUPPORT: Failed to apply or refresh ACL 2000 rule 1 to the inbound direction of VLAN 1. The ACL is not supported.
Explanation	The system failed to perform one of the following actions because the ACL rule is not supported: • Applying an ACL rule to a specific direction of a VLAN. • Updating an ACL rule applied to a specific direction of a VLAN.
Recommended action	Verify the ACL configuration and remove the settings that are not supported.

PFILTER_VLAN_RES_CONFLICT

Message text	Failed to apply or refresh [STRING] ACL [UINT] to the [STRING] direction of VLAN [UINT16]. [STRING] ACL [UINT] has already been applied to the VLAN.
Variable fields	$1: ACL type. $2: ACL number. $3: Traffic direction. $4: VLAN ID. $5: ACL type. $6: ACL number.
Severity level	3
Example	PFILTER/3/PFILTER_VLAN_RES_CONFLICT: Failed to apply or refresh IPv6 ACL 2000 to the inbound direction of VLAN 1. IPv6 ACL 3000 has already been applied to the VLAN.
Explanation	The system failed to perform one of the following actions because an ACL of the same type (IPv4 ACL, IPv6 ACL, or MAC ACL) has already been applied: • Applying the ACL to a specific direction of a VLAN. • Updating the ACL applied to a specific direction of a VLAN.
Recommended action	Remove the ACL of the same type.

PFILTER_VLAN_UNK_ERR

Message text	Failed to apply or refresh [STRING] ACL [UINT] [STRING] to the [STRING] direction of VLAN [UINT16].
Variable fields	$1: ACL type. $2: ACL number. $3: ACL rule ID. $4: Traffic direction. $5: VLAN ID.
Severity level	3
Example	PFILTER/3/PFILTER_VLAN_UNK_ERR: Failed to apply or refresh ACL 2000 rule 1 to the inbound direction of VLAN 1.
Explanation	The system failed to perform one of the following actions due to an unknown error: • Applying an ACL rule to a specific direction of a VLAN. • Updating an ACL rule applied to a specific direction of a VLAN.
Recommended action	No action is required.

PHYD messages

This section contains PHYD messages.

DRV

Message text	-Slot=3.1; [STRING] : Detected hardware fast-forwarding status error. Info saved in [STRING]
Variable fields	$1: Slot ID. $2: Name of the file saving hardware fast-forwarding status errors.
Severity level	2
Example	PHYD/2/DRV: -Slot=3.1; chassis %d slot %d cpu 1 : Detected hardware fast-forwarding status error. Info saved in chassis(1)_slot(1)_fpga(1)_regs_dump_count_1.
Explanation	The system monitors hardware fast-forwarding status at intervals. When detecting an error, the system records the error information and displays this message.
Recommended action	Save the abnormal file and observe the card status.

Message text	-Slot=3.1; [STRING] : Detected hardware fast-forwarding status error 5 times. Rebooting now.
Variable fields	$1: Slot ID.
Severity level	2
Example	PHYD/2/DRV: -Slot=3.1; chassis %d slot %d cpu 1 : Detected hardware fast-forwarding status error 5 times. Now rebooting.
Explanation	The system monitors hardware fast-forwarding status at intervals. After detecting continuous errors for five times, the system displays this message and reboots the card.
Recommended action	After the card is rebooted, save the abnormal files and observe the service status.

Message text	-Slot=2.1; Detected receiving interface [STRING] status abnormal on hardware fast-forwarding [STRING]. Checkpoint [STRING] failed.
Variable fields	$1: Interface ID. $2: Hardware fast-forwarding engine chip ID. $3: Checkpoint ID.
Severity level	4
Example	PHYD/4/DRV: -Chassis=2-Slot=2.1; Detected receiving interface HGport[2] status abnormal on hardware fast-forwarding chip0. Checkpoint 2 failed.
Explanation	The system monitors the receiving interface status of the hardware fast forwarding at intervals. When detecting an error, the system displays this message.
Recommended action	If the services are not influenced by the error, observe the card status.

Message text	Detected sending interface [STRING] status abnormal on hardware fast-forwarding [STRING].
Variable fields	$1: Interface ID. $2: Hardware fast-forwarding engine chip ID.
Severity level	4
Example	PHYD/4/DRV: -Chassis=2-Slot=2.1; Detected sending interface HGport[1] status abnormal on hardware fast-forwarding chip0
Explanation	The system monitors the sending interface status of the hardware fast forwarding at intervals. When detecting an error, the system displays this message.
Recommended action	If the services are not influenced by the error, observe the card status.

Message text	Detected [STRING] status abnormal on hardware fast-forwarding [STRING]. Receiving status: [STRING]; sending status: [STRING].
Variable fields	$1: Interface ID. $2: Hardware fast-forwarding engine chip ID. $3: State. $4: State.
Severity level	4
Example	PHYD/4/DRV: -Chassis=2-Slot=2.1; Detected HGport[2] status abnormal on hardware fast-forwarding chip0. Receiving status:OK; sending status: ERROR.
Explanation	The system monitors the HiGig interface status of the hardware fast forwarding at intervals. When detecting an error, the system displays this message.
Recommended action	If the services are not influenced by the error, observe the card status.

Message text	-Slot=3.1; Detected uneven distribution of sessions on hardware fast-forwarding [STRING]. DDR[STRING]: [STRING] sessions (max); DDR [STRING]: [STRING] sessions (min).
Variable fields	$1: Hardware fast-forwarding engine chip ID. $2: DDR interface ID. $3: Number of sessions. $4: DDR interface ID. $5: Number of sessions.
Severity level	4
Example	PHYD/4/DRV: -Chassis=1-Slot=4.1; Detected uneven distribution of sessions on hardware fast-forwarding chip0. DDR[22]: 112022 sessions (max); DDR [28]: 10257 sessions (min).
Explanation	The system monitors the hardware fast forwarding session status at intervals. When detecting an error, the system displays this message.
Recommended action	If the services are not influenced by the error, observe the card status.

Message text	Detected [STRING] channel[STRING] ddr_mod[STRING] exintf table status abnormal
Variable fields	$1: Chip ID. $2: Channel ID. $3: DDR ID.
Severity level	4
Example	PHYD/4/DRV: -Slot=2.1; Detected chip0 channel[0] ddr mod[10] exintf table status abnormal
Explanation	The system monitors the hardware fast-forwarding entry status at intervals. When detecting an error, the system displays this message.
Recommended action	Save the abnormal file and observe the card status.

PIM messages

This section contains PIM messages.

PIM_NBR_DOWN

Message text	[STRING]: Neighbor [STRING] ([STRING]) is down.
Variable fields	$1: VPN instance name. If the PIM neighbor belongs to the public network, this field is not displayed. $2: IP address of the PIM neighbor. $3: Interface name.
Severity level	5
Example	PIM/5/PIM_NBR_DOWN: Neighbor 10.1.1.1(Vlan-interface10) is down.
Explanation	A PIM neighbor went down.
Recommended action	Check the PIM configuration and network status.

PIM_NBR_UP

Message text	[STRING]: Neighbor [STRING] ([STRING]) is up.
Variable fields	$1: VPN instance name. If the PIM neighbor belongs to the public network, this field is not displayed. $2: IP address of the PIM neighbor. $3: Interface name.
Severity level	5
Example	PIM/5/PIM_NBR_UP: Neighbor 10.1.1.1(Vlan-interface10) is up.
Explanation	A PIM neighbor came up.
Recommended action	No action is required.

PING messages

This section contains ping messages.

PING_STATISTICS

Message text	[STRING] statistics for [STRING]: [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packet loss, round-trip min/avg/max/std-dev = [DOUBLE]/[DOUBLE]/[DOUBLE]/[DOUBLE] ms.
Variable fields	$1: Ping or ping6. $2: IP address, IPv6 address, or host name for the destination. $3: Number of sent echo requests. $4: Number of received echo replies. $5: Percentage of the non-replied packets to the total request packets. $6: Minimum round-trip delay. $7: Average round-trip delay. $8: Maximum round-trip delay. $9: Standard deviation round-trip delay.
Severity level	6
Example	PING/6/PING_STATISTICS: Ping statistics for 192.168.0.115: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms.
Explanation	A user uses the **ping** command to identify whether a destination in the public network is reachable.
Recommended action	If there is no packet received, identify whether the interface is down.

PING_VPN_STATISTICS

Message text	[STRING] statistics for [STRING] in VPN instance [STRING] : [UINT32] packets transmitted, [UINT32] packets received, [DOUBLE]% packet loss, round-trip min/avg/max/std-dev = [DOUBLE]/[DOUBLE]/[DOUBLE]/[DOUBLE] ms.
Variable fields	$1: Ping or ping6. $2: IP address, IPv6 address, or host name for the destination. $3: VPN instance name. $4: Number of sent echo requests. $5: Number of received echo replies. $6: Percentage of the non-replied packets to the total request packets. $7: Minimum round-trip delay. $8: Average round-trip delay. $9: Maximum round-trip delay. $10: Standard deviation round-trip delay.
Severity level	6
Example	PING/6/PING_VPN_STATISTICS: Ping statistics for 192.168.0.115 in VPN instance vpn1: 5 packets transmitted, 5 packets received, 0.0% packet loss, round-trip min/avg/max/std-dev = 0.000/0.800/2.000/0.748 ms.
Explanation	A user uses the **ping** command to identify whether a destination in a private network is reachable.
Recommended action	If there is no packet received, identify whether the interface is down and identify whether a valid route exists in the routing table.

PKI messages

This section contains PKI messages.

REQUEST_CERT_FAIL

Message text	Failed to request [STRING] certificate of domain [STRING].
Variable fields	$1: Certificate purpose. $2: PKI domain name.
Severity level	5
Example	PKI/5/REQUEST_CERT_FAIL: Failed to request general certificate of domain abc.
Explanation	Failed to request certificate for a domain.
Recommended action	Check the configuration of the device and CA server, and the network between them.

REQUEST_CERT_SUCCESS

Message text	Request [STRING] certificate of domain [STRING] successfully.
Variable fields	$1: Certificate purpose. $2: PKI domain name.
Severity level	5
Example	PKI/5/REQUEST_CERT_SUCCESS: Request general certificate of domain abc successfully.
Explanation	Successfully requested certificate for a domain.
Recommended action	No action is required.

PKT2CPU messages

This section contains PKT2CPU messages.

PKT2CPU_NO_RESOURCE

Message text	-Interface=[STRING]-ProtocolType=[UINT32]-MacAddr=[STRING]; The resources are insufficient. -Interface=[STRING]-ProtocolType=[UINT32]-SrcPort=[UINT32]-DstPort=[UINT32]; The resources are insufficient.
Variable fields	$1: Interface type and number. $2: Protocol type. $3: MAC address or source port. $4: Destination port.
Severity level	4
Example	PKT2CPU/4/PKT2CPU_NO_RESOURCE: -Interface=Ethernet0/0/2-ProtocolType=21-MacAddr=0180-c200-0014; The resources are insufficient.
Explanation	Hardware resources were insufficient.
Recommended action	Cancel the configuration.

PKTCPT messages

This section contains packet capture messages.

PKTCPT_AP_OFFLINE

Message text	Failed to start packet capture. Reason: AP was offline.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_AP_OFFLINE: Failed to start packet capture. Reason: AP was offline.
Explanation	Packet capture failed to start because the AP configured with packet capture was offline.
Recommended action	**229.** Verify the AP configuration, and restart packet capture after the AP comes online. **230.** If the problem persists, contact NSFOCUS Support.

PKTCPT_AREADY_EXIT

Message text	Failed to start packet capture. Reason: The AP was uploading frames captured during the previous capturing operation.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_AREADY_EXIT: Failed to start packet capture. Reason: The AP was uploading frames captured during the previous capturing operation.
Explanation	When packet capture is stopped on the AC, the fit AP might be still uploading the captured frames. This message is generated when the user restarted packet capture at that time.
Recommended action	**231.** Restart packet capture later. **232.** If the problem persists, contact NSFOCUS Support.

PKTCPT_CONN_FAIL

Message text	Failed to start packet capture. Reason: Failed to connect to the FTP server.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_CONN_FAIL: Failed to start packet capture. Reason: Failed to connect to the FTP server.
Explanation	Packet capture failed to start because the device failed to be connected to the FTP server in the same network segment.
Recommended action	**233.** Verify that the URL of the FTP server is valid. Possible reasons for an invalid URL include the specified IP address does not exist or is not the FTP server address, and the specified FTP server port is disabled. **234.** Verify that the domain name resolution is successful. **235.** Verify that the FTP server is reachable for the device configured with packet capture. **236.** Verify that the FTP server is online. **237.** If the problem persists, contact NSFOCUS Support.

PKTCPT_INVALID_FILTER

Message text	Failed to start packet capture. Reason: Invalid expression for matching packets to be captured.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_INVALD_FILTER: Failed to start packet capture. Reason: Invalid expression for matching packets to be captured.
Explanation	Packet capture failed to start because the capture filter expression was invalid.
Recommended action	**238.** Correct the capture filter expression. **239.** If the problem persists, contact NSFOCUS Support.

PKTCPT_LOGIN_DENIED

Message text	Packet capture aborted. Reason: FTP server login failure.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_LOGIN_DENIED: Packet capture aborted. Reason: FTP server login failure.
Explanation	Packet capture stopped because the user failed to log in to the FTP server.
Recommended action	**240.** Verify the username and password. **241.** If the problem persists, contact NSFOCUS Support.

PKTCPT_MEMORY_ALERT

Message text	Packet capture aborted. Reason: Memory threshold reached.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_MEMORY_ALERT: Packet capture aborted. Reason: Memory threshold reached.
Explanation	Packet capture stopped because the memory threshold was reached.
Recommended action	N/A

PKTCPT_OPEN_FAIL

Message text	Failed to start packet capture. Reason: File for storing captured frames not opened.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_OPEN_FAIL: Failed to start packet capture. Reason: File for storing captured frames not opened.
Explanation	Packer capture failed to start because the file for storing the captured frames cannot be opened.
Recommended action	**242.** Verify that the user has the write permission to the file. If the user does not have the write permission, assign the permission to the user. **243.** Verify that the specified file has been created and is not used by another feature. If the file is used by another feature, use another file. **244.** If the problem persists, contact NSFOCUS Support.

PKTCPT_OPERATION_TIMEOUT

Message text	Failed to start or continue packet capture. Reason: Operation timed out.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_OPERATION_TIMEOUT: Failed to start or continue packet capture. Reason: Operation timed out.
Explanation	This message is generated when one of the following situations occurs: • Packet capture failed to start because the FTP server in a different network segment is not reachable and the connection timed out. • Packet capture stopped because the FTP server in a different network segment is offline and uploading the captured frames timed out.
Recommended action	**245.** Verify that the FTP server is reachable. **246.** Verify that the FTP server is online. **247.** If the problem persists, contact NSFOCUS Support.

PKTCPT_SERVICE_FAIL

Message text	Failed to start packet capture. Reason: TCP or UDP port binding faults.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_SERVICE_FAIL: Failed to start packet capture. Reason: TCP or UDP port binding faults.
Explanation	Packet capture failed to start because an error occurs during TCP or UDP port binding.
Recommended action	**248.** Verify that Wireshark has been closed before you start packet capture. If it is not closed, close Wireshark, and then restart packet capture. **249.** Bind a new TCP or UDP port, and then restart packet capture. **250.** If the problem persists, contact NSFOCUS Support.

PKTCPT_UNKNOWN_ERROR

Message text	Failed to start or continue packet capture. Reason: Unknown error.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_UNKNOWN_ERROR: Failed to start or continue the packet capture. Reason: Unknown error.
Explanation	Packet capture failed to start or packet capture stopped because of an unknown error.
Recommended action	N/A

PKTCPT_UPLOAD_ERROR

Message text	Packet capture aborted. Reason: Failed to upload captured frames.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_UPLOAD_ERROR: Packet capture aborted. Reason: Failed to upload captured frames.
Explanation	Packet capture stopped because the capture failed to upload the captured frames.
Recommended action	**251.** Verify that the FTP working directory is not changed. **252.** Verify that the user has the write permission to the file on the FTP server. **253.** Verify that the FTP server is online. **254.** Verify that the FTP server is reachable. **255.** Verify that the FTP server has enough memory space. **256.** Verify that the packet capture is not stopped during the upload of captured frames. **257.** If the problem persists, contact NSFOCUS Support.

PKTCPT_WRITE_FAIL

Message text	Packet capture aborted. Reason: Not enough space to store captured frames.
Variable fields	N/A
Severity level	6
Example	PKTCPT/6/PKTCPT_WRITE_FAIL: Packet capture aborted. Reason: Not enough space to store captured frames.
Explanation	Packet capture stopped because the memory space is not enough for storing captured frames.
Recommended action	**258.** Delete unnecessary files to release the space. **259.** If the problem persists, contact NSFOCUS Support.

Portal messages

This section contains portal messages.

PORTAL_USER_LOGOFF

Message text	UserName=[STRING], IPAddr=[IPADDR], IfName=[STRING], OuterVLAN=[UINT16], InnerVLAN=[UINT16], MACAddr=[MAC], Reason=[STRING], Input Octets=[UINT32], Output Octets=[UINT32], Input Gigawords=[UINT32], Output Gigawords=[UINT32], IPv6Input Octets=[UINT32], IPv6Output Octets=[UINT32], IPv6 Input Gigawords=[UINT32],IPv6Output Gigawords=[UINT32], SessionTime=[UINT32]; User logged off.
Variable fields	$1: Username. $2: IP address. $3: Interface name. $4: Outer VLAN ID. $5: Inner VLAN ID. $6: MAC address. $7: Reason for user offline, see Table 12. $8: Statistics of the user's upstream IPv4 traffic, in bytes. $9: Statistics of the user's downstream IPv4 traffic, in bytes. $10: Statistics of the user's upstream IPv4 traffic. The measurement unit is 4G bytes. $11: Statistics of the user's downstream IPv4 traffic. The measurement unit is 4G bytes. $12: Statistics of the user's upstream IPv6 traffic, in bytes. $13: Statistics of the user's downstream IPv6 traffic, in bytes. $14: Statistics of the user's upstream IPv6 traffic. The measurement unit is 4G bytes. $15: Statistics of the user's downstream IPv6 traffic. The measurement unit is 4G bytes. $16: Online duration of the user, in seconds.
Severity level	6
Example	PORTAL/6/PORTAL_USER_LOGOFF: -MDC=1; UserName=abc, IPAddr=1.1.1.2, IfName=Route-Aggregation1023.4000, OuterVLAN=N/A, InnerVLAN=4000, MACAddr=0230-0103-5601, Reason=User request, Input Octets=100, Output Octets=200, Input Gigawords=100, Output Gigawords=200, IPv6Input Octets=100, IPv6Output Octets=200, IPv6Input Gigawords=100, IPv6Output Gigawords=200, SessionTime=200; User logged off.
Explanation	A portal user went offline. Whether IPv6-related fields are displayed depends on the configuration of the **`portal user-log traffic-separate`** command. For more information, see portal commands in *Security Command Reference*.
Recommended action	Choose the recommended action according to the reason (see Table 12).

Table 12 Reasons that a user goes offline and recommended actions

Reason	Description	Recommended action
User request.	The user requested to be offline.	No action is required.
DHCP relay deleted.	The DHCP relay entry was deleted.	Verify that the DHCP server configuration is correct.

Reason	Description	Recommended action
Idle timeout.	The traffic of the user in the specified period of time does not reach the idle cut traffic threshold.	No action is required.
Session timeout.	The user's online time has reached the session timeout time assigned by the server.	No action is required.
User detection failure.	The user failed online detection.	No action is required.
Force logout by RADIUS server.	The RADIUS server logged out the user.	No action is required.
Interface down.	• The state of the access interface became Down or Deactive. • The access interface is a VLAN interface and a Layer 2 port left the VLAN.	• Verify that a cable is correctly inserted to the user access interface, and the access interface is not shut down by using the **shutdown** command. • Verify that the user access interface card or subcard operates normally. • Verify that portal roaming is enabled on the user access Layer 2 Ethernet interface.
Failed to assign a user rule.	N/A.	Release memory to ensure enough hardware memory space.
Authorization info changed.	Authorization information changed for the user. For example, the authorization ACL or user profile was deleted.	No action is required.
Force logout by access device.	The device logged out the user.	Make sure portal authentication functions normally on the user access interface.
User info synchronization failure.	The device failed to synchronize user information with the server.	• Make sure the user heartbeat interval configured on the portal authentication server is not greater than the user synchronization detection timeout configured on the access device. • Verify that the server is reachable.
User recovery failure.	User information recovery failed.	• Verify that the user access interface is up. • Verify that portal authentication is enabled on the user access interface. • Verify that the session timeout timer for the user does not expire.
Authorization ACL for the online user changed.	N/A	• Verify that the authorization ACL for the user is correctly assigned. • Verify that strict checking on authorized ACLs is disabled.

Reason	Description	Recommended action
Authorization user profile for the online user changed.	N/A	• Verify that the authorization user profile for the user is correctly assigned by using the **display user profile** command. • Verify that strict checking on authorized user profiles is disabled.
Accounting update failure.	Failed to update accounting for the user.	• Verify that the device can correctly communicate with the accounting server. • Verify that the status of the accounting server is active.
Failed to start accounting.	Failed to start accounting for the user.	• Verify that the device can correctly communicate with the accounting server. • Verify that the status of the accounting server is active.
User traffic reached threshold.	Traffic of the user reached the traffic threshold set by the server.	No action is required.
Authorization VPN instance deleted.	The authorization VPN instance was deleted.	No action is required.

PORTAL_USER_LOGON_FAIL

Message text	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; User failed to get online.
Variable fields	$1: Username. $2: IP address. $3: Interface name. $4: Outer VLAN ID. $5: Inner VLAN ID. $6: MAC address. $7: Login failure reason, see Table 13.
Severity level	6
Example	PORTAL/6/PORTAL_USER_LOGON_FAIL: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=100-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason= Authentication Failed : 4; User failed to get online.
Explanation	A portal user failed to come online.
Recommended action	Choose the recommended action according to the reason, see Table 13.

Table 13 Reasons that a user fails to come online and recommended actions

Reason	Description	Recommended action
Authorization failure.	Authorization failed, or authorization attributes deployment failed.	• Verify that the device can correctly communicate with the authorization server. • Verify that the authorization user attributes exist on the device and are correctly configured. • Verify that the device supports the authorization user attributes.
Received logout request.	The user received a logout request from the portal server during the login process.	Verify that the device can correctly communicate with the AAA server.
Authentication failure.	Authentication failed.	• Verify that the device can correctly communicate with the authentication server. • Verify that the shared key is the same on the device and the authentication server. • Verify that the username is valid. • Verify that the password for the username is correct. • Verify that the authentication domain on the device is correct.
Other error.	Unknown error.	N/A

PORTAL_USER_LOGON_SUCCESS

Message text	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]:User got online successfully.
Variable fields	$1: Username. $2: IP address. $3: Interface name. $4: Outer VLAN ID. $5: Inner VLAN ID. $6: MAC address.
Severity level	6
Example	PORTAL/6/PORTAL_USER_LOGON_SUCCESS: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=100-InnerVLAN=4000-MACAddr=0230-0103-5601; User got online successfully.
Explanation	A portal user came online successfully.
Recommended action	No action is required.

PORTSEC messages

This section contains port security messages.

PORTSEC_PORTMODE_NOT_EFFECTIVE

Message text	The port security mode is configured but is not effective on interface [STRING].
Variable fields	$1: Interface type and number.
Severity level	3
Example	PORTSEC/3/PORTSEC_PORTMODE_NOT_EFFECTIVE: The port security mode is configured but is not effective on interface Ethernet3/1/2.
Explanation	The port security mode does not take effect on an interface, because the interface does not support this mode.
Recommended action	**260.** Remove the problem by using one of the following methods: ○ Change the port security mode to another mode that is supported by the interface. ○ Reconnect the connected devices to another interface that supports this port security mode, and configure the port security mode on the new interface. **261.** If the problem persists, contact NSFOCUS Support.

PORTSEC_NTK_NOT_EFFECTIVE

Message text	The NeedToKnow feature is configured but is not effective on interface [STRING].
Variable fields	$1: Interface type and number.
Severity level	3
Example	PORTSEC/3/PORTSEC_NTK_NOT_EFFECTIVE: The NeedToKnow feature is configured but is not effective on interface Ethernet3/1/2.
Explanation	The NeedToKnow mode does not take effect on an interface, because the interface does not support the NeedToKnow mode.
Recommended action	**262.** Remove the problem depending on the network requirements: ○ If the NeedToKnow feature is not required, disable the NeedToKnow feature on the interface. ○ If the NeedToKnow feature is required, reconnect the connected devices to another interface that supports the NeedToKnow mode. Then, configure the NeedToKnow mode on the new interface. **263.** If the problem persists, contact NSFOCUS Support.

POSA

This section contains POSA module messages.

POSA_TCPLISTENPORT_NOT_OPEN

Message text	Failed to open TCP listening port for terminal [STRING].
Variable fields	$1: POS terminal template ID.
Severity level	3
Example	POSA/3/POSA_TCPLISTENPORT_NOT_OPEN: Failed to open TCP listening port for terminal 1.
Explanation	The device failed to open the TCP listening port for POS terminal template 1.
Recommended action	**264.** Delete POS terminal template 1. **265.** Re-create a POS terminal template by using an unused TCP port number.

PPP messages

This section contains PPP messages.

IPPOOL_ADDRESS_EXHAUSTED

Message text	The address pool [STRING] was exhausted.
Variable fields	$1: Pool name.
Severity level	5
Example	PPP/5/IPPOOL_ADDRESS_EXHAUSTED: The address pool aaa was exhausted.
Explanation	This message is generated when the last address is assigned from the pool.
Recommended action	Add addresses to the pool.

PPPOES_MAC_THROTTLE

Message text	The MAC [STRING] triggered MAC throttle on interface [STRING].
Variable fields	$1: MAC address. $2: Interface name.
Severity level	5
Example	PPPOES/5/PPPOES_MAC_THROTTLE: -MDC=1; The MAC 001b-21a8-0949 triggered MAC throttle on interface GigabitEthernet1/0/1.
Explanation	The maximum number of PPPoE session requests from a user within the monitoring time reached the PPPoE access limit on the access interface. The access interface discarded the excessive requests.
Recommended action	**266.** Check the PPPoE access limit on the access interface that is configured by using the **`pppoe-server throttle per-mac`** command. **267.** View the time left for the blocking user on the access interface by executing the **`display pppoe-server throttled-mac`** command. **268.** If the problem persists, contact the support.

PPP_USER_LOGON_SUCCESS

Message text	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]; The user came online successfully.
Variable fields	$1: Username. $2: IP address. $3: Interface name. $4: Outer VLAN ID. $5: Inner VLAN ID. $6: MAC address.
Severity level	6
Example	PPP/6/PPP_USER_LOGON_SUCCESS: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601; The user came online successfully.
Explanation	The user has come online successfully.
Recommended action	No action is required.

PPP_USER_LOGON_FAILED

Message text	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; The user failed to come online.
Variable fields	$1: Username. $2: IP address. $3: Interface name. $4: Outer VLAN ID. $5: Inner VLAN ID. $6: MAC address. $7: Cause (see Table 14).
Severity level	5
Example	PPP/5/PPP_USER_LOGON_FAILED: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=Authentication failed; The user failed to come online.
Explanation	The user failed to come online.
Recommended action	See Table 14.

Table 14 Causes and recommended actions

Cause	Description	Recommended action
Authentication method error	The authentication method was configured incorrectly, possibly because the authentication method requested by users is inconsistent with the authentication method configured on the interface.	Verify that the authentication method is configured correctly.
AAA access limit reached	The upper limit of concurrent logins using the same local user name is reached.	**269.** Check the number of concurrent online users using the current local user name. **270.** Modify the upper limit of the concurrent logins using the current local user name to a greater value by executing the **`access-limit`** command.
The local user does not exist	The local user was not configured.	**271.** Verify that the dial-in user is a legal user. **272.** Add the local user if the user is a legal user but the corresponding local user does not exist on the device.
Local authentication failed: wrong password	The local authentication was rejected because of the incorrect password.	**273.** Verify that the username is correct. **274.** Verify that the password is correct.
No AAA response during authentication	The device did not receive an AAA response from the authentication server during the authentication timeout time.	**275.** Verify that the device communicates with the authentication server correctly. **276.** Verify that the authentication server operates correctly. **277.** Verify that the shared key on the device is the same as the shared key on the authentication server.
RADIUS authentication reject	The RADIUS server returned an access-reject packet.	**278.** Verify that the username is correct. **279.** Verify that the password is correct.
AAA authorization information error	Failed to add user authorization information.	Verify that the authorization attributes deployed by the authorization server exist on the device and are configured correctly.
Authentication request to AAA failed	The device failed to send the authentication request to the AAA server.	**280.** Verify that the device communicates with the authentication server correctly. **281.** Verify that the authentication server operates correctly.
Accounting request to AAA failed	The device failed to send the accounting request to the AAA server.	**282.** Verify that the device communicates with the accounting server correctly. **283.** Verify that the accounting server operates correctly.
No authentication ACK from AAA	The device failed to receive the authentication acknowledgment packet from the AAA server.	**284.** Verify that the device communicates with the authentication server correctly. **285.** Verify that the authentication server operates correctly.
TACACS authentication reject	The TACACS server returned an access-reject packet.	**286.** Verify that the username is correct. **287.** Verify that the password is correct.

PPP_USER_LOGOFF

Message text	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; The user logged off.
Variable fields	$1: Username. $2: IP address. $3: Interface name. $4: Outer VLAN ID. $5: Inner VLAN ID. $6: MAC address. $7: Cause (see Table 15).
Severity level	6
Example	PPP/6/PPP_USER_LOGOFF: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=Use request; The user logged off.
Explanation	The user has gone offline normally.
Recommended action	No action is required.

Table 15 Causes

Cause	Description
User request	The user connection was terminated at the user's request.

PPP_USER_LOGOFF_ABNORMAL

Message text	-UserName=[STRING]-IPAddr=[IPADDR]-IfName=[STRING]-OuterVLAN=[UINT16]-InnerVLAN=[UINT16]-MACAddr=[MAC]-Reason=[STRING]; The user logged off abnormally.
Variable fields	$1: Username. $2: IP address. $3: Interface name. $4: Outer VLAN ID. $5: Inner VLAN ID. $6: MAC address. $7: Cause (see Table 16).
Severity level	6
Example	PPP/6/PPP_USER_LOGOFF_ABNORMAL: -UserName=abc-IPAddr=1.1.1.2-IfName=Route-Aggregation1023.4000-OuterVLAN=1000-InnerVLAN=4000-MACAddr=0230-0103-5601-Reason=Lost Carrier; The user logged off abnormally.
Explanation	The user has gone offline abnormally.
Recommended action	See Table 16.

Table 16 Causes and recommended actions

Cause	Description	Recommended action
Lost carrier	The keepalive packets were lost, possibly because the link between the user device and the device connecting to the BAS fails.	Save the related log information locally and contact the support.
Lost service	The service server (for example, L2TP) terminated the service.	No action is required.
Admin reset	The user session was temporarily terminated by the administrator by executing the **shutdown** command because of management reasons.	No action is required.
BAS request	Unknown reasons.	Save the related log information locally and contact the support.
Session timeout	The user session timed out.	Notify the user that the traffic quota is used up or to renew the user account.
Traffic quota limit reached	The user traffic limit was reached.	Notify the user that the traffic is used up or to renew the user account.
Logged off by the RADIUS server	The AAA server logged off the user.	No action is required.
Accounting update failure	The accounting update failed.	**288.** Verify that the device communicates with the accounting server correctly. **289.** Verify that the accounting server operates correctly.
No AAA response during realtime accounting	The user did not receive the response from the accounting server during the timeout time. (In the realtime accounting	**290.** Verify that the device communicates with the accounting server correctly.

Cause	Description	Recommended action
	phase.)	**291.** Verify that the accounting server operates correctly.
No AAA response for accounting start	The user did not receive the response from the accounting server during the timeout time. (In the accounting start phase.)	**292.** Verify that the device communicates with the accounting server correctly. **293.** Verify that the accounting server operates correctly.
No AAA response for accounting stop	The user did not receive the response from the accounting server during the timeout time. (In the accounting stop phase.)	**294.** Verify that the device communicates with the accounting server correctly. **295.** Verify that the accounting server operates correctly.
PPP negotiation terminated	The PPP negotiation was terminated.	Verify that the configuration is correct.
Repeated LCP negotiation packets	Repeated LCP negotiation packets were received.	Disconnect the client and initiate a connection again.
The interface that the user accesses goes down	N/A.	**296.** Verify that the network cable of the user access interface is correctly connected. **297.** Verify the user access card or subcard has no errors or is in position.
The interface that the user accesses is shut down	N/A.	Verify that the **shutdown** command is not executed on the user access interface.
Session idle cut	The user traffic did not reach the threshold within the specified period.	No action is required.

PREPROVISION messages

This section contains preprovision messages.

PREPROVISION_SLOT_MISMATCH

Message text	Preprovision check on slot [UINT32] failed because of mismatching model or interface information: Preprovisioned model=[STRING], installed model=[STRING]. Preprovisioned interface type=[STRING], actual interface type=[STRING].
Variable fields	$1: Slot number of a member device. $2: Model of a preprovisioned device. $3: Model of an installed device. $4: Preprovisioned interface information on a member device. $5: Preprovisioned interface information on a member device.
Severity level	3
Example	PREPROVISION/3/PREPROVISION_SLOT_MISMATCH: Preprovision check on slot 2 failed because of mismatching model or interface information: Preprovisioned model=MPU, installed model=MPU. Preprovisioned interface type=GE-GE, actual interface type=XGE-XGE.
Explanation	Preprovisioning check failed because the model of the installed member device is not consistent with the preprovisioned model or the actual interface information is not consistent with preprovisioned interface information.
Recommended action	Install a member device of the specified model.

PREPROVISION_SUBSLOT_MISMATCH

Message text	Preprovision check on slot [UINT32] subslot [UINT32] failed because of mismatching model or interface information: Preprovisioned model=[STRING], installed model=[STRING]. Preprovisioned interface type=[STRING], actual interface type=[STRING].
Variable fields	$1: Slot number of a member device. $2: Subslot number of a subcard. $3: Model of a preprovisioned subcard. $4: Model of an installed subcard. $5: Preprovisioned interface information on a subcard. $6: Actual interface information on a subcard.
Severity level	3
Example	PREPROVISION/3/PREPROVISION_SLOT_MISMATCH: Preprovision check on slot 2 subslot 1 failed because of mismatching model or interface information: Preprovisioned model=EXTEND-CARD, installed model= EXTEND-CARD. Preprovisioned interface type=XGE, actual interface type=GE.
Explanation	Preprovisioning check failed because the model of the installed subcard is not consistent with the preprovisioned model or the actual interface information is not consistent with preprovisioned interface information.
Recommended action	Install a subcard of the specified model.

PTS

This section contains Platform Trust Services (PTS) messages.

PTS_AK_AUTH_FAILED

Message text	Inconsistent authorization data for attestation key [STRING].
Variable fields	$1: AK name.
Severity level	4
Example	PTS/4/PTS_AK_AUTH_FAILED: Inconsistent authorization data for attestation key abc.
Explanation	The authorization data specified for the **`integrity report attestation-key`** command is different from the authorization data specified for the AK when the AK was created. The command for creating a key is **`key create`**.
Recommended action	Specify the same authorization data for the **`integrity report attestation-key`** command as the authorization data you specified when you created the key.

PTS_AK_INVALID

Message text	The attestation key [STRING] is incorrect.
Variable fields	$1: AK name.
Severity level	4
Example	PTS/4/PTS_AK_INVALID: The attestation key abc is incorrect.
Explanation	The specified AK is invalid.
Recommended action	Specify a valid AK for TC reporting.

PTS_AK_NO_CERT

Message text	No certificate file found for attestation key [STRING].
Variable fields	$1: AK name.
Severity level	4
Example	PTS/4/PTS_AK_NO_CERT: No certificate file found for attestation key abc.
Explanation	No certificate was found for the AK.
Recommended action	Use the manager to sign an AK certificate for the AK of the device.

PTS_AK_NO_EXIST

Message text	Attestation key [STRING] doesn't exist.
Variable fields	$1: AK name.
Severity level	4
Example	PTS/4/PTS_AK_NO_EXIST: The attestation key abc doesn't exist.
Explanation	The AK does not exist.
Recommended action	Use the **`key create`** command to create the AK.

PTS_AK_NO_LOAD

Message text	The attestation key [STRING] is not loaded.
Variable fields	$1: AK name.
Severity level	4
Example	PTS/4/PTS_AK_NO_LOAD: The attestation key abc is not loaded.
Explanation	The AK is not loaded to the TC chip.
Recommended action	Use the **`key load`** command to load the AK to the TC chip.

PTS_BTW_PCR_FAILED

Message text	Hash value computed based on BootWare IML is not consistent with that in PCR ([UINT]).
Variable fields	$1: PCR index.
Severity level	4
Example	PTS/4/PTS_BTW_PCR_FAILED: Hash value computed based on BootWare IML is not consistent with that in PCR(0).
Explanation	The hash value computed by using the BootWare IML for the basic or extended segment is different from the hash value stored in the PCR. The BootWare is not trustworthy.
Recommended action	Contact NSFOCUS Support.

PTS_CHECK_RM_VERSION_FAILED

Message text	Version the RM file [STRING] is not supported.
Variable fields	$1: RM file name.
Severity level	4
Example	PTS/4/PTS_CHECK_RM_VERSION_FAILED: Version the RM file BOOTWARE_BASIC_52B.rm is not supported.
Explanation	The device does not support the RM file version.
Recommended action	Contact NSFOCUS Support.

PTS_CREATE_AGED_TIMER_FAILED

Message text	Failed to create PTS session ageing timer.
Variable fields	N/A
Severity level	4
Example	PTS/4/PTS_CREATE_AGED_TIMER_FAILED: Failed to create PTS session ageing timer.
Explanation	PTS failed to create the session aging timer.
Recommended action	**298.** Execute the **undo pts** command and the **pts** command in turn to restart the PTS service. **299.** If the problem persists, contact NSFOCUS Support.

PTS_CREATE_CHECK_TIMER_FAILED

Message text	Failed to create server check timer.
Variable fields	N/A
Severity level	4
Example	PTS/4/PTS_CREATE_CHECK_TIMER_FAILED: Failed to create server check timer.
Explanation	PTS failed to create the server check timer.
Recommended action	**1.** Execute the **undo pts** command and the **pts** command in turn to restart the PTS service. **2.** If the problem persists, contact NSFOCUS Support.

PTS_CREATE_CONTEXT_FAILED

Message text	Failed to create TSS context.
Variable fields	N/A
Severity level	4
Example	PTS/4/PTS_CREATE_CONTEXT_FAILED: Failed to create TSS context.
Explanation	PTS failed to create the TPM software stack context.
Recommended action	Contact NSFOCUS Support.

PTS_CREATE_EPOLL_FAILED

Message text	Failed to create epoll service.
Variable fields	N/A
Severity level	3
Example	PTS/3/PTS_CREATE_EPOLL_FAILED: Failed to create epoll service.
Explanation	PTS failed to create the epoll service.
Recommended action	**1.** Execute the **undo pts** command and the **pts** command in turn to restart the PTS service. **2.** If the problem persists, contact NSFOCUS Support.

PTS_CREATE_HASH_FAILED

Message text	Failed to create hash table.
Variable fields	N/A
Severity level	3
Example	PTS/3/PTS_CREATE_HASH_FAILED: Failed to create hash table.
Explanation	PTS failed to create the hash table.
Recommended action	**1.** Execute the **undo pts** command and the **pts** command in turn to restart the PTS service. **2.** If the problem persists, contact NSFOCUS Support.

PTS_CREATE_SELFVERIFY_COUNTER_FAILED

Message text	Failed to create selfverify counter.
Variable fields	N/A
Severity level	4
Example	PTS/4/PTS_CREATE_SELFVERIFY_COUNTER_FAILED: Failed to create selfverify counter.
Explanation	PTS failed to create the integrity self-verification IML counter. The integrity self-verification feature is not available.
Recommended action	**1.** Execute the **undo pts** command and the **pts** command in turn to restart the PTS service. **2.** If the problem persists, contact NSFOCUS Support.

PTS_CREATE_SELFVERIFY_TIMER_FAILED

Message text	Failed to create selfverify timer.
Variable fields	N/A
Severity level	4
Example	PTS/4/PTS_CREATE_SELFVERIFY_TIMER_FAILED: Failed to create selfverify timer.
Explanation	PTS failed to create the integrity self-verification timer. The periodic integrity self-verification feature is not available.
Recommended action	• Contact NSFOCUS Support. • Use the **integrity selfverify** command to manually perform an integrity self-verification.

PTS_CREATE_SOCKET_FAILED

Message text	Failed to create socket service.
Variable fields	N/A
Severity level	3
Example	PTS/3/PTS_CREATE_SOCKET_FAILED: Failed to create socket service.
Explanation	PTS failed to create the socket service.
Recommended action	**1.** Execute the **undo pts** command and the **pts** command in turn to restart the PTS service. **300.** If the problem persists, contact NSFOCUS Support.

PTS_CREATE_TIMER_FAILED

Message text	Failed to create timer.
Variable fields	N/A
Severity level	4
Example	PTS/4/PTS_CREATE_TIMER_FAILED: Failed to create timer.
Explanation	PTS failed to create a timer. PTS generates this log message whenever it fails to create a timer.
Recommended action	**1.** Execute the **undo pts** command and the **pts** command in turn to restart the PTS service. **2.** If the problem persists, contact NSFOCUS Support.

PTS_FILE_HASH_FAILED

Message text	Hash value of file [STRING] is not consistent with that in the RM file.
Variable fields	$1: Name of the file of which you want to measure the integrity.
Severity level	4
Example	PTS/4/PTS_FILE_HASH_FAILED: Hash value of file /sbin/ls is not consistent with that in the RM file.
Explanation	The hash value computed for the specified file is different from the hash value of the file stored in the RM file. The file is not trustworthy.
Recommended action	Contact NSFOCUS Support.

PTS_LOAD_KEY_FAILED

Message text	Failed to load attestation key [STRING].
Variable fields	$1: AK name.
Severity level	4
Example	PTS/4/PTS_LOAD_KEY_FAILED: Failed to load attestation key abc.
Explanation	PTS failed to load the AK name to the TPM.
Recommended action	**1.** Verify that the AK exists and is enabled. To display AK information, use the **display tcsm key name** command. **2.** If the problem persists, contact NSFOCUS Support.

PTS_PARSE_IML_FAILED

Message text	Failed to parse IML.
Variable fields	N/A
Severity level	4
Example	PTS/4/PTS_PARSE_IML_FAILED: Failed to parse IML.
Explanation	PTS failed to parse an IML.
Recommended action	**1.** Execute the **`undo pts`** command and the **`pts`** command in turn to restart the PTS service. **2.** If the problem persists, contact NSFOCUS Support.

PTS_PKG_PCR_FAILED

Message text	Hash value computed based on Package IML is not consistent with that in PCR ([UINT]).
Variable fields	$1: PCR index.
Severity level	4
Example	PTS/4/PTS_PKG_PCR_FAILED: Hash value computed based on Package IML is not consistent with that in PCR (12).
Explanation	The hash value computed by using the NF image IML is different from the hash value stored in the PCR. The NF images are not trustworthy.
Recommended action	Contact NSFOCUS Support.

PTS_READ_PCR_FAILED

Message text	Failed to read PCR ([UINT]).
Variable fields	$1: PCR index.
Severity level	4
Example	PTS/4/PTS_READ_PCR_FAILED: Failed to read PCR(0).
Explanation	PTS failed to read PCR data.
Recommended action	Contact NSFOCUS Support.

PTS_RM_FILE_FAILED

Message text	Wrong signature for RM file [STRING].
Variable fields	$1: RM file name.
Severity level	4
Example	PTS/4/PTS_RM_FILE_FAILED: Wrong signature for RM file BOOTWARE_BASIC_52B.rm.
Explanation	The signature for the RM file is incorrect.
Recommended action	Contact NSFOCUS Support.

PTS_RUNTIME_PCR_FAILED

Message text	Hash value computed based on runtime IML is not consistent with that in PCR ([UINT]).
Variable fields	$1: PCR index.
Severity level	4
Example	PTS/4/PTS_RUNTIME_PCR_FAILED: Hash value computed based on runtime IML is not consistent with that in PCR (10).
Explanation	The hash value computed by using the runtime IML is different from the hash value stored in the PCR. The runtime-related executable files are not trustworthy.
Recommended action	Contact NSFOCUS Support.

PTS_SELFVERIFY_FAILED

Message text	Failed to start integrity selfverify. Reason: TPM doesn't exist or isn't enabled.
Variable fields	N/A
Severity level	4
Example	PTS/4/PTS_SELFVERIFY_FAILED: Failed to start integrity selfverify because TPM does not exist or is not enabled.
Explanation	Because the TPM did not exist or was disabled, the integrity self-verification failed.
Recommended action	Verify that the TPM is available. To display relevant information, use the **`display tcsm trusted-computing-chip`** command.

PTS_SELFVERIFY_START_FAILED

Message text	Failed to start selfverify.
Variable fields	N/A
Severity level	4
Example	PTS/4/PTS_SELFVERIFY_START_FAILED: Failed to start selfverify.
Explanation	PTS failed to start integrity self-verification.
Recommended action	**1.** Start integrity self-verification again. **2.** If the problem persists, contact NSFOCUS Support.

PTS_TEMPLATE_HASH_FAILED

Message text	Calculated template hash value of [STRING] is not consistent with that in IML.
Variable fields	$1: Name of the file of which you want to measure the integrity.
Severity level	4
Example	PTS/4/PTS_TEMPLATE_HASH_FAILED: Calculated template hash value of /sbin/ls is not consistent with that in IML.
Explanation	The template hash value computed by using parameters including the measurement time and the hash value of the program file is different from the template hash value in the IML. The IML might have been tempered with.
Recommended action	Contact NSFOCUS Support.

PWDCTL messages

This section contains password control messages.

PWDCTL_ADD_BLACKLIST

Message text	[STRING] was added to the blacklist for wrong password input.
Variable fields	$1: Username.
Severity level	6
Example	PWDCTL/6/PWDCTL_ADD_BLACKLIST: hhh was added to the blacklist for wrong password input.
Explanation	The user entered an incorrect password. It failed to log in to the device and was added to the password control blacklist.
Recommended action	No action is required.

PWDCTL_CHANGE_PASSWORD

Message text	[STRING] changed the password because [STRING].
Variable fields	$1: Username. $2: The reasons for changing password. • it was the first login of the account. • the password had expired. • the password was too short. • the password was not complex enough. • the password was default password.
Severity level	6
Example	PWDCTL/6/PWDCTL_CHANGE_PASSWORD: hhh changed the password because It is the first login of the account.
Explanation	The user changed the password for some reason. For example, the user changed the password because it is the first login of the user's account.
Recommended action	No action is required.

PWDCTL_DELETEBLACLIST

Message text	User [STRING] was deleted from blacklist.
Variable fields	$1: Username.
Severity level	3
Example	PWDCTL/3/PWDCTL_DELETEBLACLIST: User hhh was deleted from blacklist.
Explanation	The user account was removed from the blacklist.
Recommended action	No action is required.

PWDCTL_FAILED_COPYFILE

Message text	Failed to copy the password records to all backup files.
Variable fields	N/A
Severity level	3
Example	PWDCTL/3/PWDCTL_FAILED_COPYFILE: Failed to copy the password records to backup file.
Explanation	The device failed to copy a password to a file on the standby MPU.
Recommended action	Verify that the storage space of the file system on the standby MPU is sufficient.

PWDCTL_FAILED_PROCMSG

Message text	Failed to process request message.
Variable fields	N/A
Severity level	3
Example	PWDCTL/3/PWDCTL_FAILED_PROCMSG: Failed to process request message.
Explanation	The password management daemon failed to process a request message.
Recommended action	Contact Technical Support.

PWDCTL_FAILED_TO_WRITEPWD

Message text	Failed to write the password records to file.
Variable fields	N/A
Severity level	6
Example	PWDCTL/6/PWDCTL_FAILED_TO_WRITEPWD: Failed to write the password records to file.
Explanation	The device failed to write a password to a file.
Recommended action	Check the file system of the device for memory space insufficiency.

PWDCTL_LOCKBLACKLIST

Message text	User [STRING] was [STRING] minutes for achieve maximum login attempts.
Variable fields	$1: Username. $2: The locking action to be taken after the user fails the maximum number of consecutive login attempts: • **locked in** *time-value* **minutes**—Locks the user account for a period of time. When the locking timer expires, users can use this user account to log in. • **permanently locked**—Locks the user account permanently.
Severity level	3
Example	**301.** PWDCTL/3/PWDCTL_LOCKBLACKLIST: User hhh was locked in 1 minutes for achieve maximum login attempts. **302.** PWDCTL/3/PWDCTL_LOCKBLACKLIST: User hhh was permanently locked for achieve maximum login attempts.
Explanation	The action to be taken after the user fails the maximum number of consecutive login attempts depends on the **`password-control login-attempt exceed`** command.
Recommended action	No action is required.

PWDCTL_NOTIFYWRITEFILE

Message text	Notification of writing password records to file failed.
Variable fields	N/A
Severity level	3
Example	PWDCTL/3/PWDCTL_NOTIFYWRITEFILE: Notification of writing password records to file failed.
Explanation	The device failed to deliver the notification of writing a password to a file.
Recommended action	Contact Technical Support.

PWDCTL_RECFORMATCONV

Message text	Failed to convert the password record format.
Variable fields	N/A
Severity level	3
Example	PWDCTL/3/PWDCTL_RECFORMATCONV: Failed to convert the password record format.
Explanation	Converting password record format failed.
Recommended action	Contact Technical Support.

PWDCTL_UNLOCKBLACKLIST

Message text	User [STRING] was unlocked due to lock-time aged.
Variable fields	$1: Username.
Severity level	3
Example	PWDCTL/3/PWDCTL_UNLOCKBLACKLIST: User hhh was unlocked due to lock-time aged.
Explanation	The user account is unlocked after the locking timer expires.
Recommended action	No action is required.

PWDCTL_UPDATETIME

Message text	Last login time updated after clock update.
Variable fields	N/A
Severity level	6
Example	PWDCTL/6/PWDCTL_UPDATETIME: Last login time updated after clock update.
Explanation	The most recent login time has been updated.
Recommended action	No action is required.

PWDCTL_USERINLOCKING

Message text	User [STRING] is locking for maximum times failure logged in.
Variable fields	$1: Username.
Severity level	3
Example	PWDCTL/3/PWDCTL_USERINLOCKING: User hhh is locking for maximum times failure logged in.
Explanation	The user makes login attempts during the locking period after the maximum number of consecutive login attempts is reached.
Recommended action	No action is required.

QOS messages

This section contains QoS messages.

QOS_AUTHCAR_APPLYUSER_FAIL

Message text	[STRING]; Failed to apply the authorized CAR to the user. Reason: [STRING].
Variable fields	$1: User identity. $2: Failure cause: ○ The resources are insufficient.
Severity level	4
Example	QOS/4/QOS_AUTHCAR_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN="N/A"-Port=GigabitEthernet5/1/5; Failed to apply the authorized CAR to the user. Reason: The resources are insufficient.
Explanation	This message is generated in the following situations: • The DAE client fails to issue the authorized CAR action when a user comes online. • The DAE client fails to modify the authorized CAR action for online user.
Recommended action	Modify the parameters of the authorized CAR action.

QOS_CAR_APPLYUSER_FAIL

Message text	[STRING]; Failed to apply the [STRING] CAR in [STRING] profile [STRING] to the user. Reason: [STRING].
Variable fields	$1: User identity. $2: Application direction. $3: Profile type. $4: Profile name. $5: Failure cause: ○ The resources are insufficient.
Severity level	4
Example	QOS/4/QOS_CAR_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2-SVLAN=100-VPN="N/A"-Port=GigabitEthernet5/1/5; Failed to apply the inbound CAR in user profile a to the user. Reason: The resources are insufficient.
Explanation	The system failed to perform one of the following actions: • Apply a CAR policy when a user went online. • Modify a configured CAR policy or configure a new CAR policy when a user is online.
Recommended action	Delete the CAR policy from the profile or modify the parameters of the CAR policy.

QOS_CBWFQ_REMOVED

Message text	CBWFQ is removed from [STRING].
Variable fields	$1: Interface name.
Severity level	3
Example	QOS/3/QOS_CBWFQ_REMOVED: CBWFQ is removed from GigabitEthernet4/0/1.
Explanation	CBWFQ was removed from an interface because the maximum bandwidth or speed configured on the interface was below the bandwidth or speed required for CBWFQ.
Recommended action	Increase the bandwidth or speed and apply the removed CBWFQ again.

QOS_GTS_APPLYUSER_FAIL

Message text	[STRING]; Failed to apply GTS in user profile [STRING] to the user. Reason: [STRING].
Variable fields	$1: User identity. $2: User profile name. $3: Failure cause.
Severity level	4
Example	QOS/4/QOS_GTS_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply GTS in user profile a to the user. Reason: The resources are insufficient.
Explanation	The system failed to perform one of the following actions: • Apply a GTS action when a user went online. • Modify a configured GTS action or configure a new GTS action when a user is online.
Recommended action	Delete the GTS action from the user profile or modify the parameters of the GTS action.

QOS_NOT_ENOUGH_BANDWIDTH

Message text	Policy [STRING] requested bandwidth [UINT32](kbps). Only [UINT32](kbps) is available on [STRING].
Variable fields	$1: Policy name. $2: Required bandwidth for CBWFQ. $3: Available bandwidth on an interface. $4: Interface name.
Severity level	3
Example	QOS/3/QOS_NOT_ENOUGH_BANDWIDTH: Policy d requested bandwidth 10000(kbps). Only 80(kbps) is available on GigabitEthernet4/0/1.
Explanation	Configuring CBWFQ on an interface failed because the maximum bandwidth on the interface was less than the bandwidth required for CBWFQ.
Recommended action	Increase the maximum bandwidth configured for the interface or set lower bandwidth required for CBWFQ.

QOS_POLICY_APPLYCOPP_CBFAIL

Message text	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of control plane slot [UINT32]. [STRING].
Variable fields	$1: Name of a classifier-behavior association. $2: Policy name. $3: Application direction. $4: Slot number. $5: Failure cause.
Severity level	4
Example	QOS/4/QOS_POLICY_APPLYCOPP_CBFAIL: Failed to apply classifier-behavior d in policy b to the inbound direction of control plane slot 3. The behavior is empty.
Explanation	The system failed to perform one of the following actions: • Apply a classifier-behavior association to a specific direction of a control plane. • Update a classifier-behavior association applied to a specific direction of a control plane.
Recommended action	Modify the configuration of the QoS policy according to the failure cause.

QOS_POLICY_APPLYCOPP_FAIL

Message text	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of control plane slot [UINT32]. [STRING].
Variable fields	$1: Policy name. $2: Traffic direction. $3: Slot number. $4: Failure cause.
Severity level	4
Example	QOS/4/QOS_POLICY_APPLYCOPP_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of control plane slot 3. The operation is not supported.
Explanation	The system failed to perform one of the following actions: • Apply a QoS policy to a specific direction of a control plane. • Update a QoS policy applied to a specific direction of a control plane.
Recommended action	Modify the configuration of the QoS policy according to the failure cause.

QOS_POLICY_APPLYGLOBAL_CBFAIL

Message text	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction globally. [STRING].
Variable fields	$1: Name of a classifier-behavior association. $2: Policy name. $3: Traffic direction. $4: Failure cause.
Severity level	4
Example	QOS/4/QOS_POLICY_APPLYGLOBAL_CBFAIL: Failed to apply classifier-behavior a in policy b to the outbound direction globally. The behavior is empty.
Explanation	The system failed to perform one of the following actions: • Apply a classifier-behavior association to a specific direction globally. • Update a classifier-behavior association applied to a specific direction globally.
Recommended action	Modify the configuration of the QoS policy according to the failure cause.

QOS_POLICY_APPLYGLOBAL_FAIL

Message text	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction globally. [STRING].
Variable fields	$1: Policy name. $2: Traffic direction. $3: Failure cause.
Severity level	4
Example	QOS/4/QOS_POLICY_APPLYGLOBAL_FAIL: Failed to apply or refresh QoS policy b to the inbound direction globally. The operation is not supported.
Explanation	The system failed to perform one of the following actions: • Apply a QoS policy to a specific direction globally. • Update a QoS policy applied to a specific direction globally.
Recommended action	Modify the configuration of the QoS policy according to the failure cause.

QOS_POLICY_APPLYIF_CBFAIL

Message text	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of interface [STRING]. [STRING].
Variable fields	$1: Name of a classifier-behavior association. $2: Policy name. $3: Traffic direction. $4: Interface name. $5: Failure cause: o The behavior is empty. o The classifier is empty.
Severity level	4
Example	QOS/4/QOS_POLICY_APPLYIF_CBFAIL: Failed to apply classifier-behavior b in policy b to the inbound direction of interface Ethernet3/1/2. The behavior is empty.
Explanation	The system failed to perform one of the following actions: • Apply a classifier-behavior association to a specific direction of an interface. • Update a classifier-behavior association applied to a specific direction of an interface.
Recommended action	Modify the configuration of the QoS policy according to the failure cause.

QOS_POLICY_APPLYIF_FAIL

Message text	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of interface [STRING]. [STRING].
Variable fields	$1: Policy name. $2: Traffic direction. $3: Interface name. $4: Failure cause.
Severity level	4
Example	QOS/4/QOS_POLICY_APPLYIF_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of interface Ethernet3/1/2. The operation is not supported.
Explanation	The system failed to perform one of the following actions: • Apply a QoS policy to a specific direction of an interface. • Update a QoS policy applied to a specific direction of an interface.
Recommended action	Modify the configuration of the QoS policy according to the failure cause.

QOS_POLICY_APPLYUSER_FAIL

Message text	[STRING]; Failed to apply the [STRING] QoS policy [STRING] in user profile [STRING] to the user.Reason: [STRING].
Variable fields	$1: User identity. $2: Application direction. $3: QoS policy name. $4: User profile name. $5: Failure cause.
Severity level	4
Example	QOS/4/QOS_POLICY_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-CVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply the inbound QoS policy p in user profile a to the user.Reason: The QoS policy is not supported.
Explanation	The system failed to perform one of the following actions: • Issue the settings of a QoS policy when a user went online. • Modify an applied QoS policy or apply a new QoS policy when a user is online.
Recommended action	Remove the QoS policy from the user profile or modify the parameters of the QoS policy.

QOS_POLICY_APPLYVLAN_CBFAIL

Message text	Failed to apply classifier-behavior [STRING] in policy [STRING] to the [STRING] direction of VLAN [UINT32]. [STRING].
Variable fields	$1: Name of a classifier-behavior association. $2: Policy name. $3: Application direction. $4: VLAN ID. $5: Failure cause.
Severity level	4
Example	QOS/4/QOS_POLICY_APPLYVLAN_CBFAIL: Failed to apply classifier-behavior b in policy b to the inbound direction of VLAN 2. The behavior is empty.
Explanation	The system failed to perform one of the following actions: • Apply a classifier-behavior association to a specific direction of a VLAN. • Update a classifier-behavior association applied to a specific direction of a VLAN.
Recommended action	Modify the configuration of the QoS policy according to the failure cause.

QOS_POLICY_APPLYVLAN_FAIL

Message text	Failed to apply or refresh QoS policy [STRING] to the [STRING] direction of VLAN [UINT32]. [STRING].
Variable fields	$1: Policy name. $2: Application direction. $3: VLAN ID. $4: Failure cause.
Severity level	4
Example	QOS/4/QOS_POLICY_APPLYVLAN_FAIL: Failed to apply or refresh QoS policy b to the inbound direction of VLAN 2. The operation is not supported.
Explanation	The system failed to perform one of the following actions: • Apply a QoS policy to a specific direction of a VLAN. • Update a QoS policy applied to a specific direction of a VLAN.
Recommended action	Modify the configuration of the QoS policy according to the failure cause.

QOS_QMPROFILE_APPLYUSER_FAIL

Message text	[STRING]; Failed to apply queue management profile [STRING] in session group profile [STRING] to the user. Reason: [STRING].
Variable fields	$1: User identity. $2: Queue scheduling profile name. $3: Session group profile name. $4: Failure cause.
Severity level	4
Example	QOS/4/QOS_QMPROFILE_APPLYUSER_FAIL: -MAC=1111-2222-3333-IP=192.168.1.2/16-SVLAN=100-Port=GigabitEthernet5/1/5; Failed to apply queue management profile b in session group profile a to the user. Reason: The QMProfile is not supported.
Explanation	The system failed to perform one of the following actions: • Issue the settings of a queue scheduling profile when a user went online. • Modify an applied queue scheduling profile or apply a new queue scheduling profile when a user is online.
Recommended action	Remove the queue scheduling profile from the session group profile or modify the parameters of the queue scheduling profile.

QOS_QMPROFILE_MODIFYQUEUE_FAIL

Message text	Failed to configure queue [UINT32] in queue management profile [STRING]. [STRING].
Variable fields	$1: Queue ID. $2: Profile name. $3: Failure cause.
Severity level	4
Example	QOS/4/QOS_QMPROFILE_MODIFYQUEUE_FAIL: Failed to configure queue 1 in queue management profile myqueue. The value is out of range.
Explanation	The system failed to modify a queue in a queue scheduling profile successfully applied to an interface because the new parameter was beyond port capabilities.
Recommended action	Remove the queue scheduling profile from the interface, and then modify the parameters for the queue.

QOS_POLICY_REMOVE

Message text	QoS policy [STRING] failed to be applied to [STRING].
Variable fields	$1: QoS policy name. $2: A hub-spoke tunnel on a tunnel interface.
Severity level	4
Example	QOS/4/QOS_POLICY_REMOVE: QoS policy p1 failed to be applied to ADVPN session Tunnel1 192.168.0.3.
Explanation	This message is generated when a QoS policy applied to a hub-spoke tunnel on a tunnel interface failed to be modified.
Recommended action	Check the configuration according to the failure cause.

QOS_POLICY_ACTIVATE

Message text	QoS policy [STRING] was successfully applied to [STRING].
Variable fields	$1: QoS policy name. $2: A hub-spoke tunnel on a tunnel interface.
Severity level	4
Example	QOS/4/QOS_POLICY_ACTIVATE: QoS policy p1 was successfully applied to ADVPN session Tunnel1 192.168.0.3.
Explanation	This message is generated when a QoS policy applied to a hub-spoke tunnel on a tunnel interface is successfully modified.
Recommended action	No action is required.

RADIUS messages

This section contains RADIUS messages.

RADIUS_ACCT_SERVER_DOWN

Message text	RADIUS accounting server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
Variable fields	$1: IP address of the accounting server. $2: Port number of the accounting server. $3: VPN instance name. This field displays **public** if the server belongs to the public network.
Severity level	4
Example	RADIUS/4/RADIUS_ACCT_SERVER_DOWN: RADIUS accounting server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
Explanation	An accounting server became blocked.
Recommended action	**303.** Verify that the accounting server has started up. **304.** Ping the accounting server to verify that the server is reachable. If the server is not reachable, check the link for connectivity issues and resolve the issues. **305.** Collect logs and diagnostic logs, and then contact NSFOCUS Support.

RADIUS_ACCT_SERVER_UP

Message text	RADIUS accounting server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
Variable fields	$1: IP address of the accounting server. $2: Port number of the accounting server. $3: VPN instance name. This field displays **public** if the server belongs to the public network.
Severity level	6
Example	RADIUS/6/RADIUS_ACCT_SERVER_UP: RADIUS accounting server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
Explanation	An accounting server became active.
Recommended action	No action is required.

RADIUS_AUTH_FAILURE

Message text	User [STRING] at [STRING] failed authentication.
Variable fields	$1: Username. $2: IP address.
Severity level	5
Example	RADIUS/5/RADIUS_AUTH_FAILURE: User abc@system at 192.168.0.22 failed authentication.
Explanation	An authentication request was rejected by the RADIUS server.
Recommended action	No action is required.

RADIUS_AUTH_SERVER_DOWN

Message text	RADIUS authentication server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
Variable fields	$1: IP address of the authentication server. $2: Port number of the authentication server. $3: VPN instance name. This field displays **public** if the server belongs to the public network.
Severity level	4
Example	RADIUS/4/RADIUS_AUTH_SERVER_DOWN: RADIUS authentication server was blocked: Server IP= 1.1.1.1, port=1812, VPN instance=public.
Explanation	An authentication server became blocked.
Recommended action	**306.** Verify that the authentication server has started up. **307.** Ping the authentication server to verify that the server is reachable. If the server is not reachable, check the link for connectivity issues and resolve the issues. **308.** Collect logs and diagnostic logs, and then contact NSFOCUS Support.

RADIUS_AUTH_SERVER_UP

Message text	RADIUS authentication server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
Variable fields	$1: IP address of the authentication server. $2: Port number of the authentication server. $3: VPN instance name. This field displays **public** if the server belongs to the public network.
Severity level	6
Example	RADIUS/6/RADIUS_AUTH_SERVER_UP: RADIUS authentication server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
Explanation	An authentication server became active.
Recommended action	No action is required.

RADIUS_AUTH_SUCCESS

Message text	User [STRING] at [STRING] was authenticated successfully.
Variable fields	$1: Username. $2: IP address.
Severity level	6
Example	RADIUS/6/RADIUS_AUTH_SUCCESS: User abc@system at 192.168.0.22 was authenticated successfully.
Explanation	An authentication request was accepted by the RADIUS server.
Recommended action	No action is required.

RADIUS_REMOVE_SERVER_FAIL

Message text	Failed to remove servers in scheme [STRING].
Variable fields	$1: Scheme name.
Severity level	4
Example	RADIUS/4/RADIUS_REMOVE_SERVER_FAIL: Failed to remove servers in scheme abc.
Explanation	Failed to remove servers from a RADIUS scheme.
Recommended action	No action is required.

RBM messages

This section contains RBM messages for the hot backup feature.

CFG_BATCH_SYNC

Message text	Configuration synchronization didn't complete due to configuration file sending exception.
Variable fields	N/A
Severity level	6
Example	RBM/6/ CFG_BATCH_SYNC: -Context=1; Configuration synchronization didn't complete due to configuration file sending exception.
Explanation	The device failed to synchronize configuration with the peer because an exception occurred in sending configuration files.
Recommended action	Manually back up configuration to the peer.

CFG_BATCH_SYNC

Message text	Started batch configuration synchronization.
Variable fields	N/A
Severity level	6
Example	RBM/6/ CFG_BATCH_SYNC: -Context=1; Started batch configuration synchronization.
Explanation	The device started to bulk back up configuration to the peer.
Recommended action	Do not perform any operation on the device during bulk configuration backup.

CFG_BATCH_SYNC

Message text	Finished batch configuration synchronization.
Variable fields	N/A
Severity level	6
Example	RBM/6/ CFG_BATCH_SYNC: -Context=1; Finished batch configuration synchronization.
Explanation	Bulk configuration synchronization finished.
Recommended action	No action is required.

CFG_BATCH_SYNC

Message text	Configuration synchronization failed! Device Role both is primary.
Variable fields	N/A
Severity level	6
Example	RBM/6/ CFG_BATCH_SYNC: -Context=1; Configuration synchronization failed! Device Role both is primary.
Explanation	Configuration backup failed because both the device and its peer were primary devices.
Recommended action	Assign the secondary role to the device or the peer.

CFG_COMPARE

Message text	Started configuration consistency check.
Variable fields	N/A
Severity level	6
Example	RBM/6/CFG_COMPARE: Started configuration consistency check.
Explanation	The configuration consistency check started.
Recommended action	No action is required.

CFG_COMPARE

Message text	Finished configuration consistency check.
Variable fields	N/A
Severity level	6
Example	RBM/6/CFG_COMPARE: Finished configuration consistency check.
Explanation	The configuration consistency check finished.
Recommended action	No action is required.

CFG_COMPARE

Message text	The following modules have inconsistent configuration: [STRING].
Variable fields	$1: Module name.
Severity level	6
Example	RBM/6/CFG_COMPARE: The following modules have inconsistent configuration: NAT.
Explanation	The configuration consistency check result was displayed.
Recommended action	No action is required.

CFG_COMPARE

Message text	Configuration consistency check didn't complete due to configuration file sending exception.
Variable fields	N/A
Severity level	6
Example	RBM/6/CFG_COMPARE: -Context=1; Configuration consistency check didn't complete due to configuration file sending exception.
Explanation	Configuration consistency check failed because an exception occurred in sending configuration files.
Recommended action	Manually perform configuration consistency check.

DEVICE_ROLE

Message text	The two member devices have the same role. Please assign different roles to them.
Variable fields	N/A
Severity level	6
Example	RBM/6/DEVICE_ROLE: -Context=1; The two member devices have the same role. Please assign different roles to them.
Explanation	The device and its peer have the same hot backup role.
Recommended action	Assign different hot backup roles to the device and its peer.

RBM_CFG_CONFLICT

Message text	VLAN or interface monitoring configuration exists. For the HA group to collaborate with VRRP and routing protocols, first delete the VLAN or interface monitoring configuration.
Variable fields	N/A
Severity level	1
Example	RBM/1/ RBM_CFG_CONFLICT: -Context=1; VLAN or interface monitoring configuration exists. For the HA group to collaborate with VRRP and routing protocols, first delete the VLAN or interface monitoring configuration.
Explanation	Hot backup failed to collaborate with VRRP and routing protocols, because VLAN or interface monitoring configuration exists.
Recommended action	Delete the VLAN or interface monitoring configuration.

RBM_CFG_ROLLBCK

Message text	Please perform configuration synchronization after configuration rollback is finished.
Variable fields	N/A
Severity level	6
Example	RBM/6/RBM_CFG_ROLLBCK: -Context=1; Please perform configuration synchronization after configuration rollback is finished.
Explanation	Configuration rollback was finished. You must perform configuration synchronization to maintain configuration consistency between the primary and secondary devices.
Recommended action	No action is required.

RBM_CHANNEL

Message text	Local IP=[STRING], remote IP=[STRING], status=[STRING].
Variable fields	$1: Local IPv4 address used for setting up the RBM control channel. $2: Peer IPv4 address used for setting up the RBM control channel. $3: Status of the RBM control channel. • **Connected**. • **Disconnected**.
Severity level	1
Example	RBM/1/RBM_CHANNEL: Local IP=1.1.1.1, remote IP=1.1.1.2, status=Connected.
Explanation	The device displayed information about the RBM control channel.
Recommended action	If the RBM control channel is disconnected, verify that the local and peer IPv4 addresses are correct and verify network connectivity between the device and its peer.

RBM_CHANNEL

Message text	Local IPv6=[STRING], remote IPv6=[STRING], status=[STRING].
Variable fields	$1: Local IPv6 address used for setting up the RBM control channel. $2: Peer IPv6 address used for setting up the RBM control channel. $3: Status of the RBM control channel. • **Connected**. • **Disconnected**.
Severity level	1
Example	RBM/1/RBM_CHANNEL: Local IPv6=2001::1, remote IPv6=2001::2,status=Connected.
Explanation	The device displayed information about the RBM control channel.
Recommended action	If the RBM control channel is disconnected, verify that the local and peer IPv4 addresses are correct and verify network connectivity between the device and its peer.

RBM_CHANNEL_BIND_FAILED

Message text	Failed to bind IP address [STRING] and port [UINT16] to the RBM channel.
Variable fields	$1: IP address. $2: Port number.
Severity level	6
Example	RBM/6/RBM_CHANNEL_BIND_FAILED: -Context=1; Failed to bind IP address 1.1.1.2 and port 50001 to the RBM channel.
Explanation	Failed to bind the IP address and port number to the RBM channel. The port has been used by another application.
Recommended action	Modify the local IP address or the port number associated with the peer IP address.

RDDC messages

This section contains RDDC messages.

RDDC_ACTIVENODE_CHANGE

Message text	Redundancy group [STRING] active node changed to [STRING], because of [STRING].
Variable fields	$1: Redundancy group name. $2: Active node information. $3: Status change reason: o manual switchover o group's configuration changed o node's weight changed
Severity level	5
Example	RDDC/5/RDDC_ACTIVENODE_CHANGE: Redundancy group 1 active node changed to node 1 (chassis 1), because of manual switchover.
Explanation	The active node in the redundancy group changed because of manual switchover, configuration change of the group, or weight change of the node.
Recommended action	No action is required.

RIP messages

This section contains RIP messages.

RIP_MEM_ALERT

Message text	RIP Process received system memory alert [STRING] event.
Variable fields	$1: Type of the memory alarm.
Severity level	5
Example	RIP/5/RIP_MEM_ALERT: RIP Process received system memory alert start event.
Explanation	RIP received a memory alarm.
Recommended action	Check the system memory and release memory for the modules that occupy too many memory resources.

RIP_RT_LMT

Message text	RIP [UINT32] Route limit reached
Variable fields	$1: Process ID.
Severity level	6
Example	RIP/6/RIP_RT_LMT: RIP 1 Route limit reached.
Explanation	The number of routes of a RIP process reached the upper limit.
Recommended action	**309.** Check for network attacks. **310.** Reduce the number of routes.

RIPNG messages

This section contains RIPng messages.

RIPNG_MEM_ALERT

Message text	RIPng Process received system memory alert [STRING] event.
Variable fields	$1: Type of the memory alarm.
Severity level	5
Example	RIPNG/5/RIPNG_MEM_ALERT: RIPNG Process received system memory alert start event.
Explanation	RIPng received a memory alarm.
Recommended action	Check the system memory and release memory for the modules that occupy too many memory resources.

RIPNG_RT_LMT

Message text	RIPng [UINT32] Route limit reached
Variable fields	$1: Process ID
Severity level	6
Example	RIPNG/6/RIPNG_RT_LMT: RIPng 1 Route limit reached.
Explanation	The number of routes of a RIPng process reached the upper limit.
Recommended action	**311.** Check for network attacks. **312.** Reduce the number of routes.

RIR

This section contains RIR messages.

RIR_BANDWIDTH_TOMAXIMUM

RIR_CFG_CHANGED

	• Link index or link type change. • Link preference or link primary or backup role change. • Per-session expected bandwidth change. • Other configuration changes, for example, SLA configuration changes, that cause a link from qualified to unqualified or from unqualified to qualified for the service requirements.

RIR_LINK_SELECT

		-SrcIPAddr=[IPADDR]-SrcPort=[UINT16]-DstIPAddr=[IPADDR]-DstPort=[UINT16]-Protocol=[STRING]-FlowID=[UINT32]. Selected tunnel [UINT32] for the session.
		$1: Source IP address of the session. $2: Source port number of the session. $3: Destination IP address of the session. $4: Destination port number of the session. $5: Session protocol. Values: o TCP. o UDP. o ICMP. o IPv4. o Other. $6: ID of the flow template to which the session belongs. $7: Tunnel interface number.
		6
		RIR/6/RIR_LINK_S

		ELECT: -SrcIPAddr=55.1.1.2-SrcPort=51457-DstIPAddr=11.1.1.1-DstPort=8-Protocol=ICMP-FlowID=1. Selected tunnel 1 for the session.
		RIR selected a link for the session.
		No action is required.

RIR_LINKFAULT

RIR_QUALITY_DELAY

		-FlowID=[UINT32]-Tunnel=[UINT32]-DetectedDelay=[UINT32]ms-Del

		ayThreshold=[UINT32]ms.Thelinkbecameunqualifiedbecausethelinkdelaydet

		ectedbyNQA washigherthanthelinkdelaythresholdintheSLA.

	$1: ID of the flow template.$2: Tunnel interface number.$3: Link delay det

	ectedbyNQA.$4:Linkdelaythresholdinthe SLA associatedwiththeflow temp

	late.

	6
	RIR/6/RIR_QUALITY_DELAY:-FlowID=2-Tunnel=1-Detec

	tedDelay=100ms-DelayThreshold=50ms.Thelinkbecameunqualifiedbecauseth

	elinkdelaydetectedbyNQA washigherthanthelinkdelaythresholdinthe SLA.

	The link became unqualified because the link delay detected by NQA was higher than a

	nthelinkdelaythresholdintheSLA associatedwiththeflow template.

	No action is required.

RIR_QUALITY_JITTER

		-FlowID=[UINT32]-Tunnel=[UINT32]-DetectedJitter=[UINT32]ms-Jit

		erThreshold=[UINT32]ms. The linkbecame unqualified because the linkjitt

		erwashigherthan the jitterthreshold in the SLA.

	$1:ID of the flow template.$2:Tunnel interface number.$3:Link jittered

	etected by NQA. $4: Jitter threshold in the SLA associated with the flow

	template.

	6
	RIR/6/RIR_QUALITY_JITTER:-FlowID=2-Tunnel=1-Dete

	ctedJitter=100 ms-JitterThreshold=50 ms. The linkbecame unqualified bec

	ause the link jitter was higher than the jitter threshold in the SLA.

	The link became unqualified because the link jitter detected by NQA was high

		her than the jitter threshold in the SLA associated with the flow temp

	late.
	No action is required.

RIR_QUALITY_OTHER

RIR_QUALITY_PKTLOSS

		-FlowID=[UINT32]-Tunnel=[UINT32]-DetectedPktLoss=[UINT32]‰-PktLossThreshold=[UINT32]‰. The link became unqualified because the packet loss ratio detected by NQA was higher than the packet loss threshold in the SLA.
		$1: ID of the flow template. $2: Tunnel interface number. $3: Packet loss ratio detected by NQA. $4: Packet loss

		threshold in the SLA associated with the flow template.

		6
		RIR/6/RIR_QUALITY_PKTLOSS:-FlowID=2-Tunnel=1-DetectedPktLoss=100‰-PktLossThreshold=50‰. The link became unqualified because the packet loss ratio detected by NQA was higher than the packet loss threshold in the SLA.
		The link became unqualified because the

		packet loss ratio detected by NQA was higher than the packet loss threshold in the SLA associated with the flow template.
		No action is required.

RM messages

This section contains RM messages.

RM_ACRT_REACH_LIMIT

Message text	Max active [STRING] routes [UINT32] reached in URT of [STRING]
Variable fields	$1: IPv4 or IPv6. $2: Maximum number of active routes. $3: VPN instance name.
Severity level	4
Example	RM/4/RM_ACRT_REACH_LIMIT: Max active IPv4 routes 100000 reached in URT of VPN1
Explanation	The number of active routes reached the upper limit in the unicast routing table of a VPN instance.
Recommended action	Remove unused active routes.

RM_ACRT_REACH_THRESVALUE

Message text	Threshold value [UINT32] of max active [STRING] routes reached in URT of [STRING]
Variable fields	$1: Threshold of the maximum number of active routes in percentage. $2: IPv4 or IPv6. $3: VPN instance name.
Severity level	4
Example	RM/4/RM_ACRT_REACH_THRESVALUE: Threshold value 50% of max active IPv4 routes reached in URT of vpn1
Explanation	The percentage of the maximum number of active routes was reached in the unicast routing table of a VPN instance.
Recommended action	Modify the threshold value or the route limit configuration.

RM_THRESHLD_VALUE_REACH

Message text	Threshold value [UINT32] of active [STRING] routes reached in URT of [STRING]
Variable fields	$1: Maximum number of active routes. $2: IPv4 or IPv6. $3: VPN instance name.
Severity level	4
Example	RM/4/RM_THRESHLD_VALUE_REACH: Threshold value 10000 of active IPv4 routes reached in URT of vpn1
Explanation	The number of active routes reached the threshold in the unicast routing table of a VPN instance.
Recommended action	Modify the route limit configuration.

RPR messages

This section contains RPR messages.

RPR_EXCEED_MAX_SEC_MAC

Message text	A maximum number of secondary MAC addresses exceeded defect is present on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	4
Example	RPR/4/RPR_EXCEED_MAX_SEC_MAC: A maximum number of secondary MAC addresses exceeded defect is present on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The number of RPR secondary MAC addresses on the ring has reached the upper limit.
Recommended action	Disable VRRP on RPR stations.

RPR_EXCEED_MAX_SEC_MAC_OVER

Message text	A maximum number of secondary MAC addresses exceeded defect is cleared on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	5
Example	RPR/5/RPR_EXCEED_MAX_SEC_MAC_OVER: A maximum number of secondary MAC addresses exceeded defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The number of secondary MAC addresses on the ring has dropped below the upper limit.
Recommended action	No action is required.

RPR_EXCEED_MAX_STATION

Message text	A maximum number of stations exceeded defect is present on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	4
Example	RPR/4/RPR_EXCEED_MAX_STATION: A maximum number of stations exceeded defect is present on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The number of RPR stations on the ring has reached the upper limit.
Recommended action	Remove some RPR stations.

RPR_EXCEED_MAX_STATION_OVER

Message text	A maximum number of stations exceeded defect is cleared on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	5
Example	RPR/5/RPR_EXCEED_MAX_STATION_OVER: A maximum number of stations exceeded defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The number of RPR stations on the ring has dropped below the upper limit.
Recommended action	No action is required.

RPR_EXCEED_RESERVED_RATE

Message text	An excess reserved rate defect is present on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	3
Example	RPR/3/RPR_EXCEED_RESERVED_RATE: An excess reserved rate defect is present on ringlet0 corresponding to RPR logical interface RPR-Router1.
Explanation	The reserved bandwidth for the RPR station was greater than the total bandwidth of the RPR ring.
Recommended action	Reduce the reserved bandwidth.

RPR_EXCEED_RESERVED_RATE_OVER

Message text	An excess reserved rate defect is cleared on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	5
Example	RPR/5/RPR_EXCEED_RESERVED_RATE_OVER: An excess reserved rate defect is cleared on ringlet0 corresponding to RPR logical interface RPR-Router1.
Explanation	The reserved bandwidth for the RPR station was smaller than the total bandwidth of the RPR ring.
Recommended action	No action is required.

RPR_IP_DUPLICATE

Message text	A duplicate IP address defect is present on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	3
Example	RPR/3/RPR_IP_DUPLICATE: A duplicate IP address defect is present on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	Another RPR station used the same IP address.
Recommended action	Locate the RPR station, and change its IP address.

RPR_IP_DUPLICATE_OVER

Message text	A duplicate IP address defect is cleared on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	5
Example	RPR/5/RPR_IP_DUPLICATE_OVER: A duplicate IP address defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The duplicate IP address defect was cleared.
Recommended action	No action is required.

RPR_JUMBO_INCONSISTENT

Message text	A jumbo configuration defect is present on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	6
Example	RPR/6/RPR_JUMBO_INCONSISTENT: A jumbo configuration defect is present on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	An RPR station used different Jumbo frame configuration.
Recommended action	Locate the RPR station and change its Jumbo frame configuration.

RPR_JUMBO_INCONSISTENT_OVER

Message text	A jumbo configuration defect is cleared on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	6
Example	RPR/6/RPR_JUMBO_INCONSISTENT_OVER: A jumbo configuration defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The Jumbo frame configuration inconsistency defect was cleared.
Recommended action	No action is required.

RPR_MISCABLING

Message text	A miscabling defect is present on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	3
Example	RPR/3/RPR_MISCABLING: A miscabling defect is present on ringlet0 corresponding to RPR logical interface RPR-Router1.
Explanation	The west port of an RPR station was not connected to the east port of anther RPR station.
Recommended action	Examine the physical port connection of the two RPR stations.

RPR_MISCABLING_OVER

Message text	A miscabling defect is cleared on ringlet0/ringlet1 corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	5
Example	RPR/5/RPR_MISCABLING_OVER: A miscabling defect is cleared on ringlet0 corresponding to RPR logical interface RPR-Router1.
Explanation	The RPR physical port connection defect was cleared.
Recommended action	No action is required.

RPR_PROTECTION_INCONSISTENT

Message text	A protection configuration defect is present on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	3
Example	RPR/3/RPR_PROTECTION_INCONSISTENT: A protection configuration defect is present on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	An RPR station used different protection mode.
Recommended action	Locate the RPR station and change its protection mode.

RPR_PROTECTION_INCONSISTENT_OVER

Message text	A protection configuration defect is cleared on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	5
Example	RPR/5/RPR_PROTECTION_INCONSISTENT_OVER: A protection configuration defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The protection mode inconsistency defect was cleared.
Recommended action	No action is required.

RPR_SEC_MAC_DUPLICATE

Message text	A duplicate secondary MAC addresses defect is present on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	3
Example	RPR/3/RPR_SEC_MAC_DUPLICATE: A duplicate secondary MAC addresses defect is present on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	Another RPR station used the same secondary MAC address.
Recommended action	Locate the RPR station, and change its secondary MAC address.

RPR_SEC_MAC_DUPLICATE_OVER

Message text	A duplicate secondary MAC addresses defect is cleared on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	5
Example	RPR/5/RPR_SEC_MAC_DUPLICATE_OVER: A duplicate secondary MAC addresses defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The duplicate secondary MAC address defect was cleared.
Recommended action	No action is required.

RPR_TOPOLOGY_INCONSISTENT

Message text	An inconsistent topology defect is present on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	3
Example	RPR/3/RPR_TOPOLOGY_INCONSISTENT: An inconsistent topology defect is present on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The topology information collected by the ports on the PRP stations was different.
Recommended action	Execute the **shutdown** command and then the **undo shutdown** command on the ports to collect topology information again.

RPR_TOPOLOGY_INCONSISTENT_OVER

Message text	An inconsistent topology defect is cleared on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	5
Example	RPR/5/RPR_TOPOLOGY_INCONSISTENT_OVER: An inconsistent topology defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The topology information inconsistency defect was cleared.
Recommended action	No action is required.

RPR_TOPOLOGY_INSTABILITY

Message text	A topology instability defect is present on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	4
Example	RPR/4/RPR_TOPOLOGY_INSTABILITY: A topology instability defect is present on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The RPR ring topology was unstable.
Recommended action	No action is required.

RPR_TOPOLOGY_INSTABILITY_OVER

Message text	A topology instability defect is cleared on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	5
Example	RPR/5/RPR_TOPOLOGY_INSTABILITY_OVER: A topology instability defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The RPR ring topology was stable.
Recommended action	No action is required.

RPR_TOPOLOGY_INVALID

Message text	A topology invalid defect is present on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	4
Example	RPR/4/RPR_TOPOLOGY_INVALID: A topology invalid defect is present on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The topology information collected by the RPR stations was invalid.
Recommended action	Execute the **shutdown** command and then the **undo shutdown** command on the RPR stations to collect topology information again.

RPR_TOPOLOGY_INVALID_OVER

Message text	A topology invalid defect is cleared on the ring corresponding to RPR logical interface [STRING].
Variable fields	$1: Interface name.
Severity level	5
Example	RPR/5/RPR_TOPOLOGY_INVALID_OVER: A topology invalid defect is cleared on the ring corresponding to RPR logical interface RPR-Router1.
Explanation	The topology information collected by the RPR stations was valid.
Recommended action	No action is required.

RRPP messages

This section contains RRPP messages.

RRPP_RING_FAIL

Message text	Ring [UINT32] in Domain [UINT32] failed.
Variable fields	$1: Ring ID. $2: Domain ID.
Severity level	4
Example	RRPP/4/RRPP_RING_FAIL: Ring 1 in Domain 1 failed.
Explanation	A ring failure occurred in the RRPP domain.
Recommended action	Check each RRPP node to clear the network fault.

RRPP_RING_RESTORE

Message text	Ring [UINT32] in Domain [UINT32] recovered.
Variable fields	$1: Ring ID. $2: Domain ID.
Severity level	4
Example	RRPP/4/RRPP_RING_RESTORE: Ring 1 in Domain 1 recovered.
Explanation	The ring in the RRPP domain was recovered.
Recommended action	No action is required.

RTM messages

This section contains RTM messages.

RTM_TCL_NOT_EXIST

Message text	Failed to execute Tcl-defined policy [STRING] because the policy's Tcl script file was not found.
Variable fields	$1: Name of a Tcl-defined policy.
Severity level	4
Example	RTM/4/RTM_TCL_NOT_EXIST: Failed to execute Tcl-defined policy aaa because the policy's Tcl script file was not found.
Explanation	The system did not find the Tcl script file for the policy while executing the policy.
Recommended action	**313.** Verify that the Tcl script file exists. **314.** Reconfigure the policy.

RTM_TCL_MODIFY

Message text	Failed to execute Tcl-defined policy [STRING] because the policy's Tcl script file had been modified.
Variable fields	$1: Name of a Tcl-defined policy.
Severity level	4
Example	RTM/4/RTM_TCL_MODIFY: Failed to execute Tcl-defined policy aaa because the policy's Tcl script file had been modified.
Explanation	The Tcl script file for the policy was modified.
Recommended action	Reconfigure the policy, or modify the Tcl script to be the same as it was when it was bound with the policy.

RTM_TCL_LOAD_FAILED

Message text	Failed to load the Tcl script file of policy [STRING].
Variable fields	$1: Name of a Tcl-defined policy.
Severity level	4
Example	RTM/4/RTM_TCL_LOAD_FAILED: Failed to load the Tcl script file of policy [STRING].
Explanation	The system failed to load the Tcl script file for the policy to memory.
Recommended action	No action is required.

Sandbox messages

This section contains sandbox messages through fast log output.

SANDBOX_DETECTION_IPV4_LOG

Message text	SandboxType(1143)=[STRING];FileType(1096)=[STRING];FileName(1097)=[STRING];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];TrtType(1144)=[STRING];Severity(1087)=[STRING];MD5(1129)=[STRING];BeginTime_c(1011)=[STRING];ThreatDir(1170)=[UINT16];AttackName(1088)=[STRING];ThreatAct(1171)=[STRING];ThreatFmly(1172)=[UINT16];StatusCode(1167)=[STRING];ThreatHttpContentLen(1173)=[STRING];RealSrcIP(1100)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Sandbox type: ○ AV. ○ Windows. ○ Win64. ○ WEB. ○ Office. $2: File type. $3: File name. $4: Protocol type. $5: Application protocol name. $6: Source IPv4 address. $7: Source port number. $8: Destination IPv4 address. $9: Destination port number. $10: Source security zone name. $11: Destination security zone name. $12: Name of the identity user. $13: Threat type: ○ UNKNOWN. ○ KNOWN. ○ NORMAL. No threats exist in the file. $14: Severity level: ○ NOTHREAT. ○ LOW. ○ MEDIUM. ○ HIGH. $15: MD5 value. $16: Generation time of the sandbox inspection log. $17: File transfer direction: ○ **download**—From the server to the client. ○ **upload**—From the client to the server. $18: Threat name. $19: Threat action. See Table 17 for the threat act field value. (The value for the threat act field varies by the software version of the sandbox. Table 17 uses the ESS 6701 as an example.) $20: Threat family. See Table 18 for the threat family field value. $21: HTTP/HTTPS response status code. $22: Value for the Content-Length field of the HTTP/HTTPS packet.

	$23: Real source IP address. $24: VLAN ID. $25: VXLAN ID. $26: Source location. $27: Destination location.
Severity level	6
Example	SANDBOX/6/SANDBOX_DETECTION_IPV4_LOG:SandboxType(1143)=WEB;FileType(1096)=exe;FileName(1097)=abc.exe;Protocol(1001)=TCP;Application(1002)=http;SrcIPAddr(1003)=192.168.7.15;SrcPort(1004)=4790;DstIPAddr(1007)=192.168.15.252;DstPort(1008)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=abc;TrtType(1144)=UNKNOWN;Severity(1087)=HIGH;MD5(1129)=c4ab18ce0dbd4c911ae501753d0bda89;BeginTime_c(1011)=20180320091510;ThreatDir(1170)=download;AttackName(1088)=;ThreatAct(1171)=;ThreatFmly(1172)=0;StatusCode(1167)=200;ThreatHttpContentLen(1173)=22087;RealSrcIP(1100)=2.2.2.2,3.2.2.2,3.2.2.2,2.2.2.2,2.2.2.2,2.2.2.2,2.2.2.2,2.2.2.2,3.3.3.2;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is sent when the sandbox inspection log is generated.
Recommended action	No action is required.

SANDBOX_DETECTION_IPV6_LOG

Message text	SandboxType(1143)=[STRING];FileType(1096)=[STRING];FileName(1097)=[STRING];Protocol(1001)=[STRING];Application(1002)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];TrtType(1144)=[STRING];Severity(1087)=[STRING];MD5(1129)=[STRING];BeginTime_c(1011)=[STRING];ThreatDir(1170)=[UINT16];AttackName(1088)=[STRING];ThreatAct(1171)=[STRING];ThreatFmly(1172)=[UINT16];StatusCode(1167)=[STRING];ThreatHttpContentLen(1173)=[STRING];RealSrcIP(1100)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Sandbox type: ○ AV. ○ Windows. ○ Win64. ○ WEB. ○ Office. $2: File type. $3: File name. $4: Protocol type. $5: Application protocol name. $6: Source IPv6 address. $7: Source port number. $8: Destination IPv6 address. $9: Destination port number. $10: Source security zone name. $11: Destination security zone name. $12: Name of the identity user. $13: Threat type: ○ UNKNOWN. ○ KNOWN. ○ NORMAL. No threats exist in the file. $14: Severity level: ○ NOTHREAT. ○ LOW. ○ MEDIUM. ○ HIGH. $15: MD5 value. $16: Generation time of the sandbox inspection log. $17: File transfer direction: ○ **download**—From the server to the client. ○ **upload**—From the client to the server. $18: Threat name. $19: Threat action. See Table 17 for the threat act field value. (The value for the threat act field varies by the software version of the sandbox. Table 17 uses the ESS 6701 as an example.) $20: Threat family. See Table 18 for the threat family field value. $21: HTTP/HTTPS response status code. $22: Value for the Content-Length field of the HTTP/HTTPS packet.

	$23: Real source IP address. $24: VLAN ID. $25: VXLAN ID. $26: Source location. $27: Destination location.
Severity level	6
Example	SANDBOX/6/SANDBOX_DETECTION_IPV6_LOG:SandboxType(1143)=WEB;FileType(1096)=exe;FileName(1097)=abc.exe;Protocol(1001)=TCP;Application(1002)=http;SrcIPv6Addr(1036)=100::40;SrcPort(1004)=4790;DstIPv6Addr(1037)=200::40;DstPort(1008)=80;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=abc;TrtType(1144)=UNKNOWN;Severity(1087)=HIGH;MD5(1129)=c4ab18ce0dbd4c911ae501753d0bda89;BeginTime_c(1011)=20180320091510;ThreatDir(1170)=download;AttackName(1088)=;ThreatAct(1171)=;ThreatFmly(1172)=0;StatusCode(1167)=200;ThreatHttpContentLen(1173)=22087;RealSrcIP(1100)=3::3;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	This message is sent when the sandbox inspection log is generated.
Recommended action	No action is required.

Table 17 Value for the threat act field

ID	Threat action
1	Enable autorun after the device starts.
2	Inject to other processes remotely.
3	Reduce the firewall security level or add whitelist entries.
4	Bypass User Account Control (UAC) to obtain the administrator privilege.
5	Disable the system protection mechanism.
6	Detect whether the antivirus software is installed or running in the system.
7	Detect whether the file runs in the sandbox or is debugged by the debugger.
8	Delete local files.
9	DLL hijacking or image hijacking.
10	Replace the file to be an EXE file or a DLL file.
11	The file uses a name similar to a key process for counterfeiting.
12	Infect the existing PE files.
13	Load the driver.
14	Modify the security policies of the IE browser.
15	Add or modify a Windows account.
16	Add or modify a Windows service.
17	Suspicious network connection.
18	Create a suspicious process and release a suspicious file.
19	Release an executable program.
20	Automatic shutdown, automatic restart, or automatic logout.
21	The PE file execution releases a script file.

22	Modify the hosts file.
23	Hook the key functions of the program.
24	Promote the privilege of the program.
25	The script file uses the PowerShell.
26	Malicious network behaviors of the script file.
27	Access sensitive files, such as the files storing the browser username and password.
28	Using the Android software consumes the call charge.
29	Malicious commercials on the Android software.
30	The Android software steals user privacy.
31	File faking.
32	Modify the file hidden attribute.
33	Malicious network behaviors of an executable file.
34	Malicious shortcut files.
35	Suspicious macro viruses.
200	Viruses.
201	Spyware.
202	Worms.
203	Backdoors.
204	Ransomware.
205	Downloader.
206	Malicious commercials.
207	Malicious scripts.
208	Malicious files with vulnerabilities.
209	Virus generator.
210	Shell software.
211	Heuristic behaviors.
212	Riskware.
213	Phishing.
214	Macro viruses.
215	Other threat types.

Table 18 Value for the threat family field

ID	Threat family
0	Others
1	Viruses
2	Trojans
3	Worms
4	Backdoors

5	Ransomware
6	Downloader
7	Malicious commercials
8	Malicious scripts
9	Macro viruses
10	Malicious files with vulnerabilities
11	Phishing
12	Riskware
13	Shell software
14	Heuristic behaviors
15	Digital currency
16	Botnets
17	APT intelligence
18	Malicious domain names generated by DGA

SCD

This section contains server connection detection (SCD) messages.

SCD_IPV4

Message text	Protocol(1001)=[STRING];ServerIPAddr(1003)=[STRING];DstIPAddr(1007)=[STRING];DstPort(1008)=[STRING]; Illegal server connection.
Variable fields	$1: Protocol type. $2: Server IP address. $3: Destination IP address of the server-initiated connection. $4: Destination port number of the server-initiated connection.
Severity level	6
Example	SCD/6/SCD_IPV4:-Context=1;Protocol(1001)=TCP;ServerIPAddr(1003)=192.168.105.1;DstIPAddr(1007)=192.168.105.111;DstPort(1008)=80; Illegal server connection.
Explanation	This message is sent when an illegal server-initiated connection is detected.
Recommended action	Check the illegal connection and decide whether to allow the connection based on your network services. For example, you can configure a security policy to block such connections.

SCMD messages

This section contains SCM messages.

PROCESS_ABNORMAL

Message text	The process [STRING] exited abnormally. ServiceName=[STRING], ExitCode=[STRING], KillSignal=[STRING], StartTime=[STRING], StopTime=[STRING].
Variable fields	$1: Process name. $2: Service name defined in the script. $3: Process exit code. If the process was closed by a signal, this field displays **NA**. $4: Signal that closed the process. If the process was not closed by a signal, this field displays **NA**. $5: Time when the process was created. $6: Time when the process was closed.
Severity level	4
Example	SCMD/4/PROCESS_ABNORMAL: The process diagd exited abnormally. ServiceName=DIAG, ExitCode=1, KillSignal=NA, StartTime=2019-03-06 14:18:06, StopTime=2019-03-06 14:35:25.
Explanation	A service exited abnormally.
Recommended action	**315.** Use the **`display process`** command to identify whether the process exists. If the process exists, the process has recovered. Typically, a process restarts automatically after it exits abnormally. **316.** If the process has not recovered or has recovered but you want to find the reasons, perform the following tasks: **a.** Execute the **`view /var/log/trace.log > trace.log`** command in probe view, and transfer the generated file **trace.log** from the device to a PC through FTP or TFTP. To use FTP, set the transfer mode to binary. **b.** Contact NSFOCUS Support. Do not reboot the device so NSFOCUS Support can help you locate the problem.

PROCESS_ACTIVEFAILED

Message text	The standby process [STRING] failed to switch to the active process due to uncompleted synchronization, and was restarted.
Variable fields	$1: Process name.
Severity level	4
Example	SCMD/4/PROCESS_ACTIVEFAILED: The standby process [STRING] failed to switch to the active process due to uncompleted synchronization, and was restarted.
Explanation	The standby process failed to switch to the active process because the active process exited abnormally when the standby process has not completed synchronization. The standby process was restarted.
Recommended action	No action is required.

PROCESS_CORERECORD

Message text	Exceptions occurred with process [STRING]. A core dump file was generated.
Variable fields	$1: Process name.
Severity level	4
Example	SCMD/4/PROCESS_CORERECORD: Exceptions occurred with process diagd. A core dump file was generated.
Explanation	Exceptions occurred with the process and a core dump file was generated. The core dump file contains information relevant to the process exceptions. You can use the file for troubleshooting.
Recommended action	**317.** Execute the **`display exception context`** command to collect process exception information, and save the information to a file. **318.** Execute the **`display exception filepath`** command to display the core file. **319.** Transfer the core file and the file that stores the process exception information to a PC through FTP or TFTP. To use FTP, set the transfer mode to binary. **320.** Contact NSFOCUS Support. Do not reboot the device so NSFOCUS Support can help you locate the problem.

SCM_ABNORMAL_REBOOT

Message text	Failed to restore process [STRING]. Reboot [STRING].
Variable fields	$1: Process name. $2: Chassis number and slot number, slot number, or string **the system**.
Severity level	3
Example	SCMD/3/SCM_ABNORMAL_REBOOT: Failed to restore process ipbased. Reboot slot 1.
Explanation	While the device or slot was rebooting, the specified process quitted abnormally and failed to recover after multiple automatic restart attempts. The device or slot will reboot automatically.
Recommended action	**321.** After the device or slot starts up, use the **`display process`** command to verify that the process has recovered. **322.** If the problem persists, contact NSFOCUS Support.

SCM_ABNORMAL_REBOOTMDC

Message text	Failed to restore process [STRING] on [STRING] [UINT16]. Rebooting [STRING] [UINT16].
Variable fields	$1: Process name. $2: Device type, **MDC** or **context**. $3: ID of the MDC or context. $4: Device type, **MDC** or **context**. $5: ID of the MDC or context.
Severity level	3
Example	SCMD/3/SCM_ABNORMAL_REBOOTMDC: Failed to restore process ipbased on MDC 2. Rebooting MDC 2.
Explanation	The process exited abnormally during the startup of the MDC on the active MPU or the context on the main security engine in the security engine group. If the process cannot restore after multiple automatic restart attempts, the MDC or context will restart automatically. This message will be output in MDC 1 or Context 1.
Recommended action	**323.** Use the **`display process`** command to verify that the process has restored after the card restarts. **324.** If the problem persists, contact NSFOCUS Support.

SCM_ABORT_RESTORE

Message text	Failed to restore process [STRING]. Restoration aborted.
Variable fields	$1: Process name.
Severity level	3
Example	SCMD/3/SCM_ABORT_RESTORE: Failed to restore process ipbased. Restoration aborted.
Explanation	The process exited abnormally during the system operation. If the process cannot restore after multiple automatic restart attempts, the device will not restore the process.
Recommended action	**325.** Use the **display process log** command in any view to display the details about process exit. **326.** Restart the card or the MDC where the process is located. **327.** Provide the output from the **display process log** command to NSFOCUS Support.

SCM_INSMOD_ADDON_TOOLONG

Message text	Failed to finish loading [STRING] in [UINT32] minutes.
Variable fields	$1: Kernel file name. $2: File loading duration.
Severity level	4
Example	SCMD/4/SCM_INSMOD_ADDON_TOOLONG: Failed to finish loading addon.ko in 30 minutes.
Explanation	Kernel file loading timed out during device startup.
Recommended action	**328.** Restart the card. **329.** Contact NSFOCUS Support.

SCM_KERNEL_INIT_TOOLONG

Message text	Kernel init in sequence [STRING] function [STRING] is still starting for [UINT32] minutes.
Variable fields	$1: Kernel event phase. $2: Address of the function corresponding to the kernel event. $3: Time duration.
Severity level	4
Example	SCMD/4/SCM_KERNEL_INIT_TOOLONG: Kernel init in sequence 0x25e7 function 0x6645ffe2 is still starting for 15 minutes.
Explanation	A function at a phase during kernel initialization ran too long.
Recommended action	**330.** Restart the card. **331.** Contact NSFOCUS Support.

SCM_KILL_PROCESS

Message text	Pattern 1: The process [STRING] was killed because it failed to stop within [STRING]. Pattern 2: The process [STRING] on [STRING] [UINT16] was killed because it failed to stop within [STRING].
Variable fields	Pattern 1: $1: Process name. $2: Time that elapsed after the process received the stop signal and before the device output this log message. Pattern 2: $1: Process name. $2: Object type, **MDC** or **context**. $3: ID of the MDC or context. $4: Time that elapsed after the process received the stop signal and before the device output this log message.
Severity level	6
Example	SCMD/6/SCM_KILL_PROCESS: The process stamgrd was killed because it failed to stop within 30 minutes.
Explanation	If a process does not stop after running a specific period of time, the system will kill the process.
Recommended action	**332.** After the system, MDC, or context operates stably, use the **`display process`** command to identify whether the process has recovered. **333.** If the process does not recover, contact NSFOCUS Support.

SCM_PROCESS_STARTING_TOOLONG

Message text	Pattern 1: The process [STRING] has not finished starting in [UINT32] hours. Pattern 2: The process [STRING] on [STRING] [UINT16] has not finished starting in [UINT32] hours.
Variable fields	Pattern 1: $1: Process name. $2: Time duration. Pattern 2: $1: Process name. $2: Device type, **MDC** or **context**. $3: ID of the MDC or context. $4: Time duration.
Severity level	4
Example	SCMD/4/ SCM_PROCESS_STARTING_TOOLONG: The process ipbased has not finished starting in 1 hours.
Explanation	The process initialization takes a long time and has not been finished. Too many processes have been configured or the process is abnormal.
Recommended action	**334.** Wait 6 hours and then verify that the process has been started. **335.** Restart the card/MDC/context, and then use the **`display process`** command to verify that the process has restored. **336.** Contact NSFOCUS Support.

SCM_PROCESS_STILL_STARTING

Message text	Pattern 1: The process [STRING] is still starting for [UINT32] minutes. Pattern 2: The process [STRING] on [STRING] [UINT16] is still starting for [UINT32] minutes.
Variable fields	Pattern 1: $1: Process name. $2: Time duration. Pattern 2: $1: Process name. $2: Device type, **MDC** or **context**. This field is not displayed on devices that do not support MDCs or contexts. $3: ID of the MDC or context. This field is not displayed on devices that do not support MDCs or contexts. $4: Time duration.
Severity level	6
Example	SCMD/6/SCM_PROCESS_STILL_STARTING: The process ipbased on MDC 2 is still starting for 20 minutes.
Explanation	A process is always in startup state.
Recommended action	No action is required.

SCM_SKIP_PROCESS

Message text	Pattern 1: The process [STRING] was skipped because it failed to start within 6 hours. Pattern 2: The process [STRING] on [STRING] [UINT16] was skipped because it failed to start within 6 hours.
Variable fields	Pattern 1: $1: Process name. Pattern 2: $1: Process name. $2: Object type, **MDC** or **context**. $3: ID of the MDC or context.
Severity level	3
Example	SCMD/3/SCM_SKIP_PROCESS: The process ipbased was skipped because it failed to start within 6 hours.
Explanation	A process has not completed its startup within six hours during the card/MDC/context startup, skip this process and go on with the startup.
Recommended action	**337.** Restart the card/MDC/context. **338.** Use the **`display process`** command to verify that the process has restored. **339.** Contact NSFOCUS Support.

SCRLSP messages

This section contains static CRLSP messages.

SCRLSP_LABEL_DUPLICATE

Message text	Incoming label [INT32] for static CRLSP [STRING] is duplicate.
Variable fields	$1: Incoming label value. $2: Static CRLSP name.
Severity level	4
Example	SCRLSP/4/SCRLSP_LABEL_DUPLICATE: Incoming label 1024 for static CRLSP aaa is duplicate.
Explanation	The incoming label of a static CRLSP was occupied by another configuration, for example, by a static PW or by a static LSP. This message is generated when one of the following events occurs: • When MPLS is enabled, configure a static CRLSP with an incoming label which is occupied by another configuration. • Enable MPLS when a static CRLSP whose incoming label is occupied by another configuration already exists.
Recommended action	Remove this static CRLSP, and reconfigure it with another incoming label.

SECDIAG

This section contains security diagnosis messages.

MONITOR_CONCURRENCY_EXCEED

Message text	Number of concurrent sessions reached the threshold [STRING] on [STRING]
Variable fields	$1: Threshold for the number of concurrent sessions. $2: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in standalone mode.) $2: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Centralized IRF devices.) $2: Chassis ID and slot ID in the **chassis** xx **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in IRF mode.)
Severity level	1
Example	SECDIAG/1/MONITOR_CONCURRENCY_EXCEED: Number of concurrent sessions reached the threshold 3000 on slot 1. (Distributed devices in standalone mode.) (Centralized IRF devices.)
Explanation	The number of concurrent sessions exceeded the configured threshold.
Recommended action	Decrease the number of concurrent sessions or add new devices to share the load.

MONITOR_CONCURRENCY_BELOW

Message text	Number of concurrent sessions dropped below the threshold on [STRING].
Variable fields	$1: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in standalone mode.) $1: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Centralized IRF devices.) $1: Chassis ID and slot ID in the **chassis** xx **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in IRF mode.)
Severity level	1
Example	SECDIAG/1/MONITOR_CONCURRENCY_BELOW: Number of concurrent sessions dropped below the threshold on slot 3 CPU 1. (Distributed devices in standalone mode.) (Centralized IRF devices.)
Explanation	The number of concurrent sessions decreased below the configured threshold.
Recommended action	No action is required.

MONITOR_CONNECTION_EXCEED

Message text	Session establishment rate reached the threshold [STRING] on [STRING].
Variable fields	$1: Session establishment rate threshold. $2: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in standalone mode.) $2: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Centralized IRF devices.) $2: Chassis ID and slot ID in the **chassis** xx **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in IRF mode.)
Severity level	1
Example	SECDIAG/1/MONITOR_CONNECTION_EXCEED: Session establishment rate reached the threshold 600 on slot 3 CPU 1. (Distributed devices in standalone mode.) (Centralized IRF devices.)
Explanation	The session establishment rate exceeded the configured threshold.
Recommended action	Decrease the session establishment rate or add new devices to share the load.

MONITOR_CONNECTION_BELOW

Message text	Session establishment rate dropped below the threshold on [STRING].
Variable fields	$1: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in standalone mode.) $1: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Centralized IRF devices.) $1: Chassis ID and slot ID in the **chassis** xx **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in IRF mode.)
Severity level	1
Example	SECDIAG/1/MONITOR_CONNECTION_BELOW: Session establishment rate dropped below the threshold on slot 3 CPU 1. (Distributed devices in standalone mode.) (Centralized IRF devices.)
Explanation	The session establishment rate decreased below the configured threshold.
Recommended action	No action is required.

MONITOR_SECP_IPV4_EXCEED

Message text	Number of IPv4 security policy rules reached the threshold [STRING].
Variable fields	$1: IPv4 security policy rule threshold.
Severity level	1
Example	SECDIAG/1/MONITOR_SECP_IPV4_EXCEED: Number of IPv4 security policy rules reached the threshold 500.
Explanation	The number of IPv4 security policy rules exceeded the configured threshold.
Recommended action	Decrease the number of IPv4 security policy rules or add new devices to provide higher rule capacity.

MONITOR_SECP_IPV4_BELOW

Message text	Number of IPv4 security policy rules dropped below the threshold.
Variable fields	N/A
Severity level	1
Example	SECDIAG/1/MONITOR_SECP_IPV4_BELOW: Number of IPv4 security policy rules dropped below the threshold.
Explanation	The number of IPv4 security policy rules decreased below the configured threshold.
Recommended action	No action is required.

MONITOR_SECP_IPV6_EXCEED

Message text	Number of IPv6 security policy rules reached the threshold [STRING].
Variable fields	$1: IPv6 security policy rule threshold.
Severity level	1
Example	SECDIAG/1/MONITOR_SECP_IPV6_EXCEED: Number of IPv6 security policy rules reached the threshold 200.
Explanation	The number of IPv6 security policy rules exceeded the configured threshold.
Recommended action	Decrease the number of IPv6 security policy rules or add new devices to provide higher rule capacity.

MONITOR_SECP_IPV6_BELOW

Message text	Number of IPv6 security policy rules dropped below the threshold.
Variable fields	N/A
Severity level	1
Example	SECDIAG/1/MONITOR_SECP_IPV6_BELOW: Number of IPv6 security policy rules dropped below the threshold.
Explanation	The number of IPv6 security policy rules decreased below the configured threshold.
Recommended action	No action is required.

MONITOR_CONTEXT_EXCEED

Message text	Number of contexts reached the threshold [STRING].
Variable fields	$1: Context usage threshold.
Severity level	1
Example	SECDIAG/1/MONITOR_CONTEXT_EXCEED: Number of contexts reached the threshold 60.
Explanation	The number of contexts exceeded the configured threshold.
Recommended action	Decrease the number of contexts or add new devices to share the load.

MONITOR_CONTEXT_BELOW

Message text	Number of created contexts dropped below the threshold.
Variable fields	N/A
Severity level	1
Example	SECDIAG/1/MONITOR_CONTEXT_BELOW: Number of created contexts dropped below the threshold.
Explanation	The number of contexts decreased below the configured threshold.
Recommended action	No action is required.

MONITOR_NAT_EXCEED

Message text	Number of NAT server mappings and static NAT mappings reached the threshold [STRING].
Variable fields	$1: NAT mapping threshold.
Severity level	1
Example	SECDIAG/1/MONITOR_NAT_EXCEED: Number of NAT server mappings and static NAT mappings reached the threshold 200.
Explanation	The number of NAT mappings exceeded the configured threshold.
Recommended action	Decrease the number of NAT mappings or add new devices to provide higher NAT mapping capacity.

MONITOR_NAT_BELOW

Message text	Number of NAT server mappings and static NAT mappings dropped below the threshold.
Variable fields	N/A
Severity level	1
Example	SECDIAG/1/MONITOR_NAT_BELOW: Number of NAT server mappings and static NAT mappings dropped below the threshold.
Explanation	The number of NAT mappings decreased below the configured threshold.
Recommended action	No action is required.

MONITOR_BAGG_EXCEED

Message text	Number of Layer 2 aggregate interfaces reached the threshold [STRING].
Variable fields	$1: Layer 2 aggregate interface usage threshold.
Severity level	1
Example	SECDIAG/1/MONITOR_BAGG_EXCEED: Number of Layer 2 aggregate interfaces reached the threshold 20.
Explanation	The number of Layer 2 aggregate interfaces exceeded the configured threshold.
Recommended action	Decrease the number of Layer 2 aggregate interfaces or add new devices to share the load.

MONITOR_BAGG_BELOW

Message text	Number of Layer 2 aggregate interfaces dropped below the threshold.
Variable fields	N/A
Severity level	1
Example	SECDIAG/1/MONITOR_BAGG_BELOW: Number of Layer 2 aggregate interfaces dropped below the threshold.
Explanation	The number of Layer 2 aggregate interfaces decreased below the configured threshold.
Recommended action	No action is required.

MONITOR_RAGG_EXCEED

Message text	Number of Layer 3 aggregate interfaces reached the threshold [STRING].
Variable fields	$1: Layer 3 aggregate interface usage threshold.
Severity level	1
Example	SECDIAG/1/MONITOR_RAGG_EXCEED: Number of Layer 3 aggregate interfaces reached the threshold 10.
Explanation	The number of Layer 3 aggregate interfaces exceeded the configured threshold.
Recommended action	Decrease the number of Layer 3 aggregate interfaces or add new devices to share the load.

MONITOR_RAGG_BELOW

Message text	Number of Layer 3 aggregate interfaces dropped below the threshold.
Variable fields	N/A
Severity level	1
Example	SECDIAG/1/MONITOR_RAGG_BELOW: Number of Layer 3 aggregate interfaces dropped below the threshold.
Explanation	The number of Layer 3 aggregate interfaces decreased below the configured threshold.
Recommended action	No action is required.

MONITOR_BLADE_THROUGHPUT_EXCEED

Message text	Total throughput of blade interfaces reached the threshold [STRING] on [STRING].
Variable fields	$1: Inner interface throughput threshold. $2: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in standalone mode.) $2: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Centralized IRF devices.) $2: Chassis ID and slot ID in the **chassis** xx **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in IRF mode.)
Severity level	1
Example	SECDIAG/1/MONITOR_BLADE_THROUGHPUT_EXCEED: Total throughput of blade interfaces reached the threshold 1500 on slot 3 CPU 1. (Distributed devices in standalone mode.) (Centralized IRF devices.)
Explanation	The inner interface throughput exceeded the configured threshold.
Recommended action	Decrease the inner interface throughput or add new devices to share the load.

MONITOR_BLADE_THROUGHPUT_BELOW

Message text	Total throughput of blade interfaces dropped below the threshold on [STRING].
Variable fields	$1: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in standalone mode.) $1: Slot ID in the **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Centralized IRF devices.) $1: Chassis ID and slot ID in the **chassis** xx **slot** xx **cpu** xx format. If only one CPU is available, the **cpu** xx section is not displayed. (Distributed devices in IRF mode.)
Severity level	1
Example	SECDIAG/1/MONITOR_BLADE_THROUGHPUT_BELOW: Total throughput of blade interfaces dropped below the threshold on slot 3 CPU 1. (Distributed devices in standalone mode.) (Centralized IRF devices.)
Explanation	The inner interface throughput decreased below the configured threshold.
Recommended action	No action is required.

MONITOR_QACL_EXCEED

Message text	QACL usage reached the threshold [STRING] on [STRING]: Total slices=[STRING], Remaining single slices=[STRING], Remaining double slices=[STRING], Remaining MQC entries=[STRING], Remaining OpenFlow entries=[STRING].
Variable fields	$1: QACL resource usage threshold. $2: Slot ID in the **slot** xx **cpu** xx **core** xx format. (Distributed devices in standalone mode.) $2: Slot ID in the **slot** xx **cpu** xx **core** xx format. (Centralized IRF devices.) $2: Chassis ID and slot ID in the **chassis** xx **slot** xx **cpu** xx **core** xx format. (Distributed devices in IRF mode.)
Severity level	1
Example	SECDIAG/1/MONITOR_QACL_EXCEED: QACL usage reached the threshold 80 on slot 5 CPU 1 core 2: Total slices=10. Remaining single slices=1. Remaining double slices=0. Remaining MQC entries=512. Remaining OpenFlow entries=256. (Distributed devices in standalone mode.) (Centralized IRF devices.)
Explanation	The QACL resource usage exceeded the configured threshold.
Recommended action	Decrease the QACL resource usage or add new devices to share the load.

MONITOR_QACL_BELOW

Message text	QACL usage dropped below the threshold on [STRING].
Variable fields	$1: Slot ID in the **slot** xx **cpu** xx **core** xx format. (Distributed devices in standalone mode.) (Centralized IRF devices.) $1: Chassis ID and slot ID in the **chassis** xx **slot** xx **cpu** xx **core** xx format. (Distributed devices in IRF mode.)
Severity level	1
Example	SECDIAG/1/MONITOR_QACL_BELOW: QACL usage dropped below the threshold on slot 5 CPU 1 core 2. (Distributed devices in standalone mode.) (Centralized IRF devices.)
Explanation	The QACL resource usage decreased below the configured threshold.
Recommended action	No action is required.

MONITOR_BANDWIDTH_EXCEED

Message text	Inbound traffic exceeded the total bandwidth usage threshold [STRING] Mbps.
Variable fields	$1: Inbound bandwidth usage threshold.
Severity level	1
Example	SECDIAG/1/MONITOR_BANDWIDTH_EXCEED: Inbound traffic exceeded the total bandwidth usage threshold 100 Mbps
Explanation	The total inbound bandwidth was equal to or greater than the threshold within a period.
Recommended action	Decrease the total inbound traffic or add new devices to share the load.

MONITOR_BANDWIDTH_BELOW

Message text	Inbound traffic dropped below total bandwidth usage threshold.
Variable fields	N/A
Severity level	1
Example	SECDIAG/1/MONITOR_BANDWIDTH_BELOW: Inbound traffic dropped below total bandwidth usage threshold.
Explanation	After the device sent bandwidth usage alarms, the total inbound bandwidth decreased below the inbound bandwidth usage threshold.
Recommended action	No action is required.

SECP messages

This section contains security policy messages.

SECP_ACCELERATE_NO_RES

Message text	Failed to accelerate [STRING] security-policy. The resources are insufficient.
Variable fields	$1: Security policy version.
Severity level	4
Example	SECP/4/SECP_ACCELERATE_NO_RES: Failed to accelerate IPv6 security-policy. The resources are insufficient.
Explanation	Security policy rule matching acceleration failed because of insufficient hardware resources.
Recommended action	Delete unnecessary rules or disable acceleration for the security policy of the other version to release hardware resources.

SECP_ACCELERATE_NOT_SUPPORT

Message text	Failed to accelerate [STRING] security-policy. The operation is not supported.
Variable fields	$1: Security policy version.
Severity level	4
Example	SECP/4/SECP_ACCELERATE_NOT_SUPPORT: Failed to accelerate IPv6 security-policy. The operation is not supported.
Explanation	Security policy rule matching acceleration failed because the system does not support acceleration.
Recommended action	No action is required.

SECP_ACCELERATE_UNK_ERR

Message text	Failed to accelerate [STRING] security-policy.
Variable fields	$1: Security policy version.
Severity level	4
Example	SECP/4/SECP_ACCELERATE_UNK_ERR: Failed to accelerate IPv6 security-policy.
Explanation	Security policy rule matching acceleration failed because of a system failure.
Recommended action	No action is required.

SESSION messages

This section contains session messages.

DENY_SESSION_IPV4_FLOW

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];VlanID(1175)= [UNIT16];VNI(1213)= [UNIT32];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Application service type. $4: Source IP address. $5: Source port number. $6: Source IP address after translation. $7: Source port number after translation. $8: Destination IP address. $9: Destination port number. $10: Destination IP address after translation. $11: Destination port number after translation. $12: Total number of inbound packets. $13: Total number of inbound bytes. $14: Total number of outbound packets. $15: Total number of outbound bytes. $16: Source VPN instance name. $17: Destination VPN instance name. $18: Source DS-Lite tunnel. $19: Destination DS-Lite tunnel. $20: Time when the session is created. $21: Time when the session is removed. $22: Event type. $23: Event description: o Session created. o Normal over. o Aged for timeout. o Other. $24: VLAN ID. $25: VXLAN ID.
Severity level	6
Example	SESSION/6/DENY_SESSION_IPV4_FLOW:Protocol(1001)=UDP;Application(1002)=sip;Category(1174)=aaa;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=10.10.10.1;NATSrcPort(1006)=1024;DstIPAddr(1007)=20.20.20.1;DstPort(1008)=21;NATDstIPAddr(1009)=20.20.20.1;NATDstPort(1010)=21;InitPktCount(1044)=1;InitByteCount(1046)=50;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=03182024082546;EndTime_e(1014)=;Event(1048)=(8)Session created;VlanID(1175)=10;VNI(1213)=--;

Explanation	This message is sent when an IPv4 deny session is created or removed.
Recommended action	No action is required.

DENY_SESSION_IPV6_FLOW

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];VlanID(1175)= [UNIT16];VNI(1213)= [UNIT32];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Application service type. $4: Source IPv6 address. $5: Source port number. $6 Destination IPv6 address. $7: Destination port number. $8: Total number of inbound packets. $9: Total number of inbound bytes. $10: Total number of outbound packets. $11: Total number of outbound bytes. $12: Source VPN instance name. $13: Destination VPN instance name. $14: Time when the session is created. $15: Time when the session is removed. $16: Event type. $17: Event description: o Session created. o Normal over. o Aged for timeout. o Other. $18: VLAN ID. $19: VXLAN ID.
Severity level	6
Example	SESSION/6/DENY_SESSION_IPV6_FLOW: Protocol(1001)=UDP;Application(1002)=sip;Category(1174)=aaa;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=1024;DstIPv6Addr(1037)=3001::2;DstPort(1008)=53; InitPktCount(1044)=1;InitByteCount(1046)=110;RplyPktCount(1047)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;BeginTime_e(1013)=03182024082901;EndTime_e(1014)=;Event(1048)=(8)Session created;VlanID(1175)=10;VNI(1213)=--;
Explanation	This message is sent when an IPv6 deny session is created or removed.
Recommended action	No action is required.

SESSION_IPV4_FLOW

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];VlanID(1175)= [UNIT16];VNI(1213)= [UNIT32];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Application service type. $4 Source IP address. $5: Source port number. $6: Source IP address after translation. $7: Source port number after translation. $8: Destination IP address. $9: Destination port number. $10: Destination IP address after translation. $11: Destination port number after translation. $12: Total number of inbound packets. $13: Total number of inbound bytes. $14: Total number of outbound packets. $15: Total number of outbound bytes. $16: Source VPN instance name. $17: Destination VPN instance name. $18: Source DS-Lite tunnel. $19: Destination DS-Lite tunnel. $20: Time when the session is created. $21: Time when the session is removed. $22: Event type. $23: Event description: o Session created. o Active flow threshold. o Normal over. o Aged for timeout. o Aged for reset or config-change. o Other. $24: VLAN ID. $25: VXLAN ID.
Severity level	6
Example	SESSION/6/SESSION_IPV4_FLOW:Protocol(1001)=UDP;Category(1174)=aaa;Application(1002)=sip;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=10.10.10.1;NATSrcPort(1006)=1024;DstIPAddr(1007)=20.20.20.1;DstPort(1008)=21;NATDstIPAddr(1009)=20.20.20.1;NATDstPort(1010)=21;InitPktCount(1044)=1;InitByteCount(1046)=50;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_

	e(1013)=03182024082546;EndTime_e(1014)=;Event(1048)=(8)Session created;VlanID(1175)=10;VNI(1213)=--;
Explanation	This message is sent in one of the following conditions: • An IPv4 session is created or removed. • Periodically during an IPv4 session. • The traffic-based or time-based threshold of an IPv4 session is reached.
Recommended action	No action is required.

SESSION_IPV6_FLOW

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];VlanID(1175)= [UNIT16];VNI(1213)= [UNIT32];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Application service type. $4: Source IPv6 address. $5: Source port number. $6: Destination IP address. $7: Destination port number. $8: Total number of inbound packets. $9: Total number of inbound bytes. $10: Total number of outbound packets. $11: Total number of outbound bytes. $12: Source VPN instance name. $13: Destination VPN instance name. $14: Time when the session is created. $15: Time when the session is removed. $16: Event type. $17: Event description: o Session created. o Active flow threshold. o Normal over. o Aged for timeout. o Aged for reset or config-change. o Other. $18: VLAN ID. $19: VXLAN ID.
Severity level	6
Example	SESSION/6/SESSION_IPV6_FLOW: Protocol(1001)=UDP;Application(1002)=sip;Category(1174)=aaa;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=1024;DstIPv6Addr(1037)=3001::2;DstPort(1008)=53;InitPktCount(1044)=1;InitByteCount(1046)=110;RplyPktCount(1047)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;BeginTime_e(1013)=03182024082901;EndTime_e(1014)=;Event(1048)=(8)Session created;VlanID(1175)=10;VNI(1213)=--;
Explanation	This message is sent in one of the following conditions: • An IPv6 session is created or removed. • Periodically during an IPv6 session. • The traffic-based or time-based threshold of an IPv6 session is reached.

Recommended action	No action is required.

SESSION_IPV4_TRAFFIC

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];RcvDSLiteTunnelPeer(1040)=[STRING];SndDSLiteTunnelPeer(1041)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];VlanID(1175)= [UNIT16];VNI(1213)= [UNIT32];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Application service type. $4 Source IP address. $5: Source port number. $6: Source IP address after translation. $7: Source port number after translation. $8: Destination IP address. $9: Destination port number. $10: Destination IP address after translation. $11: Destination port number after translation. $12: Total number of inbound packets. $13: Total number of inbound bytes. $14: Total number of outbound packets. $15: Total number of outbound bytes. $16: Source VPN instance name. $17: Destination VPN instance name. $18: Source DS-Lite tunnel. $19: Destination DS-Lite tunnel. $20: Time when the session is created. $21: Time when the session is removed. $22: Event type. $23: Event description: o Session created. o Active flow threshold. o Normal over. o Aged for timeout. o Aged for reset or config-change. o Other. $24: VLAN ID. $25: VXLAN ID.
Severity level	6
Example	SESSION/6/SESSION_IPV4_TRAFFIC:Protocol(1001)=UDP;Category(1174)=aaa;Application(1002)=sip;SrcIPAddr(1003)=10.10.10.1;SrcPort(1004)=1024;NATSrcIPAddr(1005)=10.10.10.1;NATSrcPort(1006)=1024;DstIPAddr(1007)=20.20.20.1;DstPort(1008)=21;NATDstIPAddr(1009)=20.20.20.1;NATDstPort(1010)=21;InitPktCount(1044)=1;InitByteCount(1046)=50;RplyPktCount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;RcvDSLiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTi

	me_e(1013)=03182024082546;EndTime_e(1014)=;Event(1048)=(8)Session created;VlanID(1175)=10;VNI(1213)=--;
Explanation	This message is sent in one of the following conditions: • An IPv4 session is created or removed. • The device periodically generates this log message for an IPv4 session. • The traffic-based or time-based threshold for an IPv4 session is reached.
Recommended action	No action is required.

SESSION_IPV6_TRAFFIC

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];Category(1174)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];InitPktCount(1044)=[UINT32];InitByteCount(1046)=[UINT32];RplyPktCount(1045)=[UINT32];RplyByteCount(1047)=[UINT32];RcvVPNInstance(1042)=[STRING];SndVPNInstance(1043)=[STRING];BeginTime_e(1013)=[STRING];EndTime_e(1014)=[STRING];Event(1048)=([UNIT16])[STRING];VlanID(1175)= [UNIT16];VNI(1213)= [UNIT32];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Application service type. $4: Source IPv6 address. $5: Source port number. $6: Destination IP address. $7: Destination port number. $8: Total number of inbound packets. $9: Total number of inbound bytes. $10: Total number of outbound packets. $11: Total number of outbound bytes. $12: Source VPN instance name. $13: Destination VPN instance name. $14: Time when the session is created. $15: Time when the session is removed. $16: Event type. $17: Event description: o Session created. o Active flow threshold. o Normal over. o Aged for timeout. o Aged for reset or config-change. o Other. $18: VLAN ID. $19: VXLAN ID.
Severity level	6
Example	SESSION/6/SESSION_IPV6_TRAFFIC: Protocol(1001)=UDP;Application(1002)=sip;Category(1174)=aaa;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=1024;DstIPv6Addr(1037)=3001::2;DstPort(1008)=53;InitPktCount(1044)=1;InitByteCount(1046)=110;RplyPktCount(1047)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=;BeginTime_e(1013)=03182024082901;EndTime_e(1014)=;Event(1048)=(8)Session created;VlanID(1175)=10;VNI(1213)=--;
Explanation	This message is sent in one of the following conditions: • An IPv6 session is created or removed. • The device periodically generates this log message for an IPv6 session. • The traffic-based or time-based threshold for

	an IPv6 session is reached.
Recommended action	No action is required.

SESSION_LIMIT

Message text	Pattern 1: -Context=1; The number of concurrent unicast sessions reached the upper limit on [STRING]. Pattern 2： -[STRING]; The number of concurrent unicast sessions reached the upper limit. Pattern 3： -Context=1; The session rate reached the upper limit on[STRING]. Pattern 4： -[STRING]; The session rate reached the upper limit. Pattern 5： -Context=1; The number of deny sessions reached the upper limit on [STRING]. Pattern 6： -[STRING]; The number of deny sessions reached the upper limit. Pattern 7： -Context=1; The deny session rate reached the upper limit on [STRING]. Pattern 8： -[STRING]; The deny session rate reached the upper limit.
Variable fields	$1: Context ID and vSystem ID
Severity level	6
Example	SESSION/6/SESSION_LIMIT: -Context=1; The number of concurrent unicast sessions reached the upper limit on vSystem 2 of context 2. SESSION/6/SESSION_LIMIT: -Context=2; vSystem=2; The number of concurrent unicast sessions reached the upper limit. SESSION/6/SESSION_LIMIT: -Context=1; The session rate reached the upper limit on vSystem 2 of context 2. SESSION/6/SESSION_LIMIT: -Context=2; vSystem=2; The session rate reached the upper limit. SESSION/6/SESSION_LIMIT: -Context=1; The number of deny sessions reached the upper limit on context 2. SESSION/6/SESSION_LIMIT: -Context=2; The number of deny sessions reached the upper limit. SESSION/6/SESSION_LIMIT: -Context=1; The deny session rate reached the upper limit on context 2. SESSION/6/SESSION_LIMIT: -Context=2; The deny session rate reached the upper limit.
Explanation	Pattern 1: This message is generated on default contexts when the number of concurrent unicast sessions reached the upper limit for non-default contexts and vSystems. Pattern 2: This message is generated on non-default contexts and vSystems when the number of concurrent unicast sessions reached the upper limit. Pattern 3: This message is generated on default contexts when the session creation rate reached the upper limit for non-default contexts and vSystems.

	Pattern 4: This message is generated on non-default contexts and vSystems when the session creation rate reached the upper limit. Pattern 5: This message is generated on default contexts when the number of concurrent deny sessions reached the upper limit for non-default contexts. Pattern 6: This message is generated on non-default contexts when the number of concurrent deny sessions reached the upper limit. Pattern 7: This message is generated on default contexts when the deny session creation rate reached the upper limit for non-default contexts. Pattern 8: This message is generated on non-default contexts when deny session creation rate reached the upper limit.
Recommended action	No action is required.

SFLOW messages

This section contains sFlow messages.

SFLOW_HARDWARE_ERROR

Message text	Failed to [STRING] on interface [STRING] due to [STRING].
Variable fields	$1: Configuration item: update sampling mode $2: Interface name. $3: Failure reason: not supported operation
Severity level	4
Example	SFLOW/4/SFLOW_HARDWARE_ERROR: Failed to update sampling mode on interface GigabitEthernet1/0/1 due to not supported operation.
Explanation	The configuration failed because the device does not support the fixed flow sampling mode.
Recommended action	Specify the random flow sampling mode.

SHELL messages

This section contains shell messages.

SHELL_CMD

Message text	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Command is [STRING]
Variable fields	$1: User line type and number. If there is not user line information, this field displays ******. $2: IP address. If there is not IP address information, this field displays ******. $3: Username. If there is not username information, this field displays ******. $4: Command string.
Severity level	6
Example	SHELL/6/SHELL_CMD: -Line=aux0-IPAddr=**-User=**; Command is quit
Explanation	A command was executed.
Recommended action	No action is required.

SHELL_CMD_CONFIRM

Message text	Confirm option of command [STRING] is [STRING].
Variable fields	$1: Command string. $2: Confirm option.
Severity level	6
Example	SHELL/6/SHELL_CMD_CONFIRM: Confirm option of command save is no.
Explanation	A user selected a confirmation option for a command.
Recommended action	No action is required.

SHELL_CMD_EXECUTEFAIL

Message text	-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] failed to be executed.
Variable fields	$1: Username. $2: IP address. $3: Command string. $4: Command view.
Severity level	4
Example	SHELL/4/SHELL_CMD_EXECUTEFAIL: -User=**-IPAddr=192.168.62.138; Command save in view system failed to be executed.
Explanation	A command deployed by a background program failed to be executed.
Recommended action	No action is required.

SHELL_CMD_INPUT

Message text	Input string for the [STRING] command is [STRING].
Variable fields	$1: Command string. $2: String entered by the user.
Severity level	6
Example	SHELL/6/SHELL_CMD_INPUT: Input string for the save command is startup.cfg. SHELL/6/SHELL_CMD_INPUT: Input string for the save command is CTRL_C. SHELL/6/SHELL_CMD_INPUT: Input string for the save command is the Enter key.
Explanation	A user responded to the input requirement of a command.
Recommended action	No action is required.

SHELL_CMD_INPUT_TIMEOUT

Message text	Operation timed out: Getting input for the [STRING] command.
Variable fields	$1: Command string.
Severity level	6
Example	SHELL/6/SHELL_CMD_INPUT_TIMEOUT: Operation timed out: Getting input for the fdisk command.
Explanation	The user did not respond to the input requirement of a command before the timeout timer expired.
Recommended action	No action is required.

SHELL_CMD_MATCHFAIL

Message text	-User=[STRING]-IPAddr=[STRING]; Command [STRING] in view [STRING] failed to be matched.
Variable fields	$1: Username. $2: IP address. $3: Command string. $4: Command view.
Severity level	4
Example	SHELL/4/SHELL_CMD_MATCHFAIL: -User=**-IPAddr=192.168.62.138; Command description 10 in view system failed to be matched.
Explanation	The command string has errors, or the view does not support the command.
Recommended action	Enter the correct command string. Make sure the command is supported in the view.

SHELL_CMDDENY

Message text	-Line=[STRING]-IPAddr=[STRING]-User=[STRING]; Command=[STRING] is denied.
Variable fields	$1: User line type and number. If there is not user line information, this field displays ******. $2: IP address. If there is not IP address information, this field displays ******. $3: Username. If there is not username information, this field displays ******. $4: Command string.
Severity level	5
Example	SHELL/5/SHELL_CMDDENY: -Line=vty0-IPAddr=192.168.62.138-User=**; Command vlan 10 is permission denied.
Explanation	The user did not have the right to execute the command.
Recommended action	No action is required.

SHELL_CMDFAIL

Message text	The [STRING] command failed to restore the configuration.
Variable fields	$1: Command string.
Severity level	6
Example	SHELL/6/SHELL_CMDFAIL: The “vlan 1024” command failed to restore the configuration.
Explanation	A command was not restored during a configuration rollback from a .cfg file.
Recommended action	No action is required.

SHELL_COMMIT

Message text	The configuration has been committed.
Variable fields	N/A
Severity level	5
Example	SHELL/5/SHELL_COMMIT: The configuration has been committed.
Explanation	The commit operation succeeded.
Recommended action	No action is required.

SHELL_COMMIT_DELAY

Message text	A configuration rollback will be performed in [INT32] minutes.
Variable fields	$1: Configuration commit delay timer.
Severity level	5
Example	SHELL/5/SHELL_COMMIT_DELAY: A configuration rollback will be performed in 3 minutes.
Explanation	The configuration commit delay timer was set successfully.
Recommended action	Complete and commit the configuration before the timer expires. If you cannot complete the configuration, execute the **`configuration commit delay`** command again to delay the expiration.

SHELL_COMMIT_REDELAY

Message text	The commit delay has been reset, a configuration rollback will be performed in [INT32] minutes.
Variable fields	$1: Configuration commit delay timer reconfigured.
Severity level	5
Example	SHELL/5/SHELL_COMMIT_REDELAY: The commit delay has been reset, a configuration rollback will be performed in 3 minutes.
Explanation	The configuration commit delay timer was reconfigured before the timer expires.
Recommended action	No action is required.

SHELL_COMMIT_ROLLBACK

Message text	The configuration commit delay is overtime, a configuration rollback will be performed.
Variable fields	N/A
Severity level	5
Example	SHELL/5/SHELL_COMMIT_ROLLBACK: The configuration commit delay is overtime, a configuration rollback will be performed.
Explanation	The configuration commit delay timer expired. A configuration rollback will occur.
Recommended action	Stop configuring the device and wait for the rollback to finish.

SHELL_COMMIT_ROLLBACKDONE

Message text	The configuration rollback has been performed.
Variable fields	N/A
Severity level	5
Example	SHELL/5/SHELL_COMMIT_ROLLBACKDONE: The configuration rollback has been performed.
Explanation	The configuration rollback was finished.
Recommended action	You can continue to configure the device as required.

SHELL_COMMIT_ROLLBACKFAILED

Message text	Settings for some commands were not rolled back upon expiration of the configuration commit delay timer. Reason: Configuration rollback is not supported for those commands.
Variable fields	N/A
Severity level	5
Example	SHELL/5/SHELL_COMMIT_ROLLBACKFAILED: Settings for some commands were not rolled back upon expiration of the configuration commit delay timer. Reason: Configuration rollback is not supported for those commands.
Explanation	A configuration rollback occurred when the configuration commit delay timer expired. However, some commands were not rolled back.
Recommended action	Read SHELL log messages to identify the commands that failed to be rolled back.

SHELL_COMMIT_WILLROLLBACK

Message text	A configuration rollback will be performed in 1 minute. To retain the configuration you have made after executing the configuration commit delay command, execute the commit command.
Variable fields	N/A
Severity level	5
Example	SHELL/5/SHELL_COMMIT_WILLROLLBACK: A configuration rollback will be performed in 1 minute. To retain the configuration you have made after executing the configuration commit delay command, execute the commit command.
Explanation	A configuration rollback will be performed in 1 minute.
Recommended action	Complete the configuration within 1 minute and commit the configuration, or execute the **`configuration commit delay`** command again to delay the expiration.

SHELL_CRITICAL_CMDFAIL

Message text	-User=[STRING]-IPAddr=[STRING]; Command=[STRING] .
Variable fields	$1: Username. $2: IP address. $3: Command string.
Severity level	6
Example	SHELL/6/SHELL_CRITICAL_CMDFAIL: -User=admin-IPAddr=169.254.0.7; Command is save.
Explanation	A command failed to be executed.
Recommended action	No action is required.

SHELL_LOGIN

Message text	[STRING] logged in from [STRING].
Variable fields	$1: Username. $2: User line type and number.
Severity level	5
Example	SHELL/5/SHELL_LOGIN: Console logged in from console0.
Explanation	A user logged in.
Recommended action	No action is required.

SHELL_LOGOUT

Message text	[STRING] logged out from [STRING].
Variable fields	$1: Username. $2: User line type and number.
Severity level	5
Example	SHELL/5/SHELL_LOGOUT: Console logged out from console0.
Explanation	A user logged out.
Recommended action	No action is required.

SLSP messages

This section contains static LSP messages.

SLSP_LABEL_DUPLICATE

Message text	Incoming label [INT32] for static LSP [STRING] is duplicate.
Variable fields	$1: Incoming label value. $2: Static LSP name.
Severity level	4
Example	SLSP/4/SLSP_LABEL_DUPLICATE: Incoming label 1024 for static LSP aaa is duplicate.
Explanation	The incoming label of a static LSP was occupied by another configuration, for example, by a static PW or by a static CRLSP. This message is generated when one of the following events occurs: • When MPLS is enabled, configure a static LSP with an incoming label which is occupied by another configuration. • Enable MPLS when a static LSP whose incoming label is occupied by another configuration already exists.
Recommended action	Remove this static LSP, and reconfigure it with another incoming label.

SMLK messages

This section contains Smart Link messages.

SMLK_LINK_SWITCH

Message text	Status of port [STRING] in smart link group [UINT16] changes to active.
Variable fields	$1: Port name. $2: Smart link group ID.
Severity level	4
Example	SMLK/4/SMLK_LINK_SWITCH: Status of port GigabitEthernet0/1/4 in smart link group 1 changes to active.
Explanation	The port takes over to forward traffic after the original active port fails.
Recommended action	Remove the network faults.

SNMP messages

This section contains SNMP messages.

AGENTX

Message text	Failed to initiate AgentX. Another service is using the AgentX listening port.
Variable fields	N/A
Severity level	4
Example	SNMP/4/AGENTX: Failed to initiate AgentX. Another service is using the AgentX listening port.
Explanation	AgentX is initiated when SNMP is enabled. The AgentX listening port is TCP port 705. If the port is occupied by another service, AgentX failes to be initiated.
Recommended action	**340.** Execute the **display tcp verbose** command to identify the process that occupies TCP port 705. **341.** Diable the feature running the process. **342.** Renable SNMP.

SNMP_ACL_RESTRICTION

Message text	SNMP [STRING] from [STRING] is rejected due to ACL restriction.
Variable fields	$1: SNMP community/usm-user/group. $2: IP address of the NMS.
Severity level	3
Example	SNMP/3/SNMP_ACL_RESTRICTION: SNMP community public from 192.168.1.100 is rejected due to ACL restrictions.
Explanation	SNMP packets are denied because of ACL restrictions.
Recommended action	Check the ACL configuration on the SNMP agent, and check if the agent was attacked.

SNMP_AUTHENTICATION_FAILURE

Message text	Failed to authenticate SNMP message.
Variable fields	N/A
Severity level	4
Example	SNMP/4/SNMP_AUTHENTICATION_FAILURE: Failed to authenticate SNMP message.
Explanation	An NMS failed to be authenticated by the agent.
Recommended action	No action is required.

SNMP_GET

Message	-seqNO=[UINT32]-srcIP=[STRING]-op=GET-node=[STRING]-value =[STRING]; The agent received a message.
Variable	$1: Sequence number of an SNMP operation log. $2: IP address of the NMS. $3: MIB object name and OID. $4: Value field of the request packet.
Severity	6
Example	SNMP/6/SNMP_GET: -seqNO=1-srcIP=192.168.28.28-op=GET-node=sysLocation(1.3.6.1.2.1.1.6.0)-value=; The agent received a message.
Explanati	SNMP received a Get request from an NMS. The system logs SNMP operations only when SNMP logging is enabled.
Recomme	No action is required.

SNMP_INFORM_LOST

Message text	Inform failed to reach NMS through [STRING]: Inform [STRING][STRING].
Variable fields	$1: NMS host address and port number. $2: Notification name and OID. $3: Variable-binding field of notifications. • If no MIB object exists, NMS host address and port number and notification name and OID are displayed. • If MIB objects are included, " with " are displayed before the MIB object and OID. MIB objects are separated by semicolons (;).
Severity level	3
Example	SNMP/3/SNMP_INFORM_LOST: Inform failed to reach NMS through 192.168.111.222(163): Inform coldStart(1.3.6.1.6.3.1.1.5.1).
Explanation	If the SNMP agent sends an Inform packet to an NMS and does not receive any response, the SNMP agent determines that the NMS is unreachable. The agent will print the message for issue location. If a message is oversized, the system will automatically fragment the message and add a location identifier "-PART=xx" to each fragment before sending them. xx represents the sequence number of a fragment.
Recommended action	Identify whether the SNMP agent and the NMS are reachable to each other.

SNMP_NOTIFY

Message	Notification [STRING][STRING].
Variable	$1: Notification name and OID. $2: Variable-binding field of notifications. ○ If no MIB object exists, only notification name and OID are displayed. ○ If MIB objects are included, " with " are displayed before the MIB object and OID. MIB objects are separated by semicolons (;).
Severity	6
Example	Example of a complete message: SNMP/6/SNMP_NOTIFY: Notification nsfocusLogIn(1.3.6.1.4.1.25506.2.2.1.1.3.0.1) with nsfocusTerminalUserName(1.3.6.1.4.1.25506.2.2.1.1.2.1.0)=;nsfocusTerminalSource(1.3.6.1.4.1.25506.2.2.1.1.2.2.0)=Console. Example of a fragmented message: SNMP/6/SNMP_NOTIFY: -MDC=1; -PART=1; Notification syslogMsgNotification(1.3.6.1.2.1.192.0.1) with syslogMsgFacility(1.3.6.1.2.1.192.1.2.1.2.1)=23;syslogMsgSeverity(1.3.6.1.2.1.192.1.2.1.3.1)=6;syslogMsgVersion(1.3.6.1.2.1.192.1.2.1.4.1)=1;syslogMsgTimeStamp(1.3.6.1.2.1.192.1.2.1.5.1)=07-e2-04-12-12-26-35-00-00-00-2d-00-00[hex];syslogMsgHostName(1.3.6.1.2.1.192.1.2.1.6.1)=NSFOCUS;syslogMsgAppName(1.3.6.1.2.1.192.1.2.1.7.1)=SHELL;syslogMsgProcID(1.3.6.1.2.1.192.1.2.1.8.1)=-;syslogMsgMsgID(1.3.6.1.2.1.192.1.2.1.9.1)=SHELL_CMD;syslogMsgSDParams(1.3.6.1.2.1.192.1.2.1.10.1)=4;syslogMsgMsg(1.3.6.1.2.1.192.1.2.1.11.1)= Command is snmp-agent trap enable syslog;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.1.12.83.121.115.76.111.99.64.50.53.53.48.54.3.77.68.67)=1;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.2.12.65.112.112.76.111.99.64.50.53.53.48.54.4.76.105.110.101)=con0. SNMP/6/SNMP_NOTIFY: -MDC=1; -PART=2; Notification syslogMsgNotification(1.3.6.1.2.1.192.0.1) with syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.3.12.65.112.112.76.111.99.64.50.53.53.48.54.6.73.80.65.100.100.114)=**;syslogMsgSDParamValue(1.3.6.1.2.1.192.1.3.1.4.1.4.12.65.112.112.76.111.99.64.50.53.53.48.54.4.85.115.101.114)=**.
Explanatio	The SNMP agent sent a notification. The system logs SNMP operations only when SNMP logging is enabled. If a message is oversized, the system will automatically fragment

Message	Notification [STRING][STRING].
	the message and add a location identifier "-PART=xx" to each fragment before sending them. xx represents the sequence number of a fragment.
Recommen	No action is required.

SNMP_SET

Mes	-seqNO=[UINT32]-srcIP=[STRING]-op=SET-errorIndex=[UINT32]-errorStatus=[STRING]-node=[STRING]-value=[STRING]; The agent received a message.
Vari	$1: Sequence number of an SNMP operation log. $2: IP address of the NMS. $3: Error index of the Set operation. $4: Error status of the Set operation. $5: MIB object name and OID. $6: Value of the MIB object changed by the Set operation.
Seve	6
Exa	SNMP/6/SNMP_SET: -seqNO=3-srcIP=192.168.28.28-op=SET-errorIndex=0-errorStatus=noError-node=sysLocation(1.3.6.1.2.1.1.6.0)-value=Hangzhou China; The agent received a message.
Expl	SNMP received a Set request from an NMS. The system logs SNMP operations only when SNMP logging is enabled.
Rec	No action is required.

Mes	-seqNO=[UINT32]-srcIP=[STRING]-op=SET-errorIndex=[UINT32]-errorStatus=[STRING]-node=[STRING]-value=[STRING]; The agent received a message.

SNMP_USM_NOTINTIMEWINDOW

Message text	-User=[STRING]-IPAddr=[STRING]; SNMPv3 message is not in the time window.
Variable fields	$1: Username. $2: IP address of the NMS.
Severity level	4
Example	SNMP/4/SNMP_USM_NOTINTIMEWINDOW: -User=admin-IPAddr=169.254.0.7; SNMPv3 message is not in the time window.
Explanation	The SNMPv3 message is not in the time window.
Recommended action	No action is required.

SSH messages

This section contains Secure Shell (SSH) messages.

SSH_WEAK_CIPHER_ALGORITHM

Message text	SSH is configured to support CBC encryption, which may allow an attacker to recover the plaintext message from the ciphertext.
Variable fields	N/A
Severity level	5
Example	SSH/5/SSH_WEAK_CIPHER_ALGORITHM: SSH is configured to support CBC encryption, which may allow an attacker to recover the plaintext message from the ciphertext.
Explanation	The SSH client or server is configured with insecure encryption algorithms, such as 3DES-CBC, 128-bit AES-CBC, 256-bit AES-CBC, and DES-CBC.
Recommended action	Use the **ssh2 algorithm cipher** command to configure secure encryption algorithms.

SSH_WEAK_MAC_ALGORITHM

Message text	SSH is configured to support MD5 or 96-bit HMAC algorithms, which are weak.
Variable fields	N/A
Severity level	5
Example	SSH/5/SSH_WEAK_MAC_ALGORITHM: SSH is configured to support MD5 or 96-bit HMAC algorithms, which are weak.
Explanation	The SSH client or server is configured with weak HMAC algorithms, such as HMAC-MD5, HMAC-MD5-96, and HMAC-SHA1-96.
Recommended action	Use the **ssh2 algorithm mac** command to configure strong HMAC algorithms.

SSHC messages

This section contains SSH client messages.

SSHC_ALGORITHM_MISMATCH

Message text	Failed to log in to SSH server [STRING] because of [STRING] algorithm mismatch.
Variable fields	$1: IP address of the SSH client. $2: Type of the algorithm, including encryption, key exchange, MAC, and public key.
Severity level	6
Example	SSHC/6/SSHC_ALGORITHM_MISMATCH: Failed to log in to SSH server 192.168.30.11 because of encryption algorithm mismatch.
Explanation	The SSH client failed to log in to the SSH server because they used different algorithms.
Recommended action	Make sure the SSH client and the SSH server use the same algorithm.

SSHS messages

This section contains SSH server messages.

SSHS_ACL_DENY

Message text	The SSH connection request from [IPADDR]([STRING]) was denied by ACL rule (rule ID=[INT16]).
Variable fields	$1: IP address of the SSH client. $2: VPN instance to which the IP address of the SSH client belongs. $3: ID of the ACL rule that denies the login of the SSH client. If the SSH client is denied by the default rule, **default rule** is displayed in this field.
Severity level	5
Example	SSHS/5/SSH_ACL_DENY: The SSH connection request from 181.1.1.10 was denied by ACL rule (rule ID=20). SSHS/5/SSH_ACL_DENY: The SSH connection request from 181.1.1.11 was denied by ACL rule (default rule).
Explanation	An SSH client failed to connect to the SSH server because the client's IP address matched a deny rule of the SSH login control ACL.
Recommended action	No action is required.

SSHS_ALGORITHM_MISMATCH

Message text	SSH client [STRING] failed to log in because of [STRING] algorithm mismatch.
Variable fields	$1: IP address of the SSH client. $2: Type of the algorithm, including encryption, key exchange, MAC, and public key.
Severity level	6
Example	SSHS/6/SSHS_ALGORITHM_MISMATCH: SSH client 192.168.30.117 failed to log in because of encryption algorithm mismatch.
Explanation	The SSH client failed to log in to the SSH server because they used different algorithms.
Recommended action	Make sure the SSH client and the SSH server use the same algorithm.

SSHS_AUTH_EXCEED_RETRY_TIMES

Message text	SSH user [STRING] (IP: [STRING]) failed to log in, because the number of authentication attempts exceeded the upper limit.
Variable fields	$1: User name. $2: IP address of the SSH client.
Severity level	6
Example	SSHS/6/SSHS_AUTH_EXCEED_RETRY_TIMES: SSH user David (IP: 192.168.30.117) failed to log in, because the number of authentication attempts exceeded the upper limit.
Explanation	The number of authentication attempts by an SSH user reached the upper limit.
Recommended action	Prompt the SSH user to use the correct login data to try again.

SSHS_AUTH_FAIL

Message text	SSH user [STRING] (IP: [STRING]) didn't pass public key authentication for [STRING].
Variable fields	$1: Username. $2: IP address of the SSH client. $3: Failure reasons: ○ Wrong public key algorithm. ○ Wrong public key. ○ Wrong digital signature.
Severity level	5
Example	SSHS/5/SSHS_AUTH_FAIL: SSH user David (IP: 192.168.30.117) didn't pass public key authentication for wrong public key algorithm.
Explanation	An SSH user failed the publickey authentication.
Recommended action	Tell the SSH user to try to log in again.

SSHS_AUTH_TIMEOUT

Message text	Authentication timed out for [IPADDR].
Variable fields	$1: IP address of the SSH client.
Severity level	6
Example	SSHS/6/SSHS_AUTH_TIMEOUT: Authentication timed out for 1.1.1.1.
Explanation	The authentication timeout timer expired, and the SSH user failed the authentication.
Recommended action	Make sure the SSH user enters correct authentication information before the authentication timeout timer expires.

SSHS_CONNECT

Message text	SSH user [STRING] (IP: [STRING]) connected to the server successfully.
Variable fields	$1: Username. $2: IP address of the SSH client.
Severity level	6
Example	SSHS/6/SSHS_CONNECT: SSH user David (IP: 192.168.30.117) connected to the server successfully.
Explanation	An SSH user logged in to the server successfully.
Recommended action	No action is required.

SSHS_DECRYPT_FAIL

Message text	The packet from [STRING] failed to be decrypted with [STRING].
Variable fields	$1: IP address of the SSH client. $2: Encryption algorithm, such as AES256-CBC.
Severity level	5
Example	SSHS/5/SSHS_DECRYPT_FAIL: The packet from 192.168.30.117 failed to be decrypted with aes256-cbc.
Explanation	A packet from an SSH client failed to be decrypted.
Recommended action	No action is required.

SSHS_DISCONNECT

Message text	SSH user [STRING] (IP: [STRING]) disconnected from the server.
Variable fields	$1: Username. $2: IP address of the SSH client.
Severity level	6
Example	SSHS/6/SSHS_DISCONNECT: SSH user David (IP: 192.168.30.117) disconnected from the server.
Explanation	An SSH user logged out.
Recommended action	No action is required.

SSHS_ENCRYPT_FAIL

Message text	The packet to [STRING] failed to be encrypted with [STRING].
Variable fields	$1: IP address of the SSH client. $2: Encryption algorithm, such as aes256-cbc.
Severity level	5
Example	SSHS/5/SSHS_ENCRYPT_FAIL: The packet to 192.168.30.117 failed to be encrypted with aes256-cbc.
Explanation	A packet to an SSH client failed to be encrypted.
Recommended action	No action is required.

SSHS_LOG

Message text	Authentication failed for [STRING] from [STRING] port [INT32] because of invalid username or wrong password.
Variable fields	$1: IP address of the SSH client. $2: Username. $3: Port number.
Severity level	6
Example	SSHS/6/SSHS_LOG: Authentication failed for David from 140.1.1.46 port 16266 because of invalid username or wrong password.
Explanation	An SSH user failed password authentication because the username or password was wrong.
Recommended action	No action is required.

SSHS_MAC_ERROR

Message text	SSH server received a packet with wrong message authentication code (MAC) from [STRING].
Variable fields	$1: IP address of the SSH client.
Severity level	6
Example	SSHS/6/SSHS_MAC_ERROR: SSH server received a packet with wrong message authentication code (MAC) from 192.168.30.117.
Explanation	The SSH server received a packet with a wrong MAC from a client.
Recommended action	No action is required.

SSHS_REACH_SESSION_LIMIT

Message text	SSH client [STRING] failed to log in. The number of SSH sessions is [NUMBER], and exceeded the limit ([NUMBER]).
Variable fields	$1: IP address of the SSH client. $2: Number of SSH clients that have logged in to the SSH server. $3: Maximum number of SSH clients that the SSH server supports.
Severity level	6
Example	SSHS/6/SSHS_REACH_SESSION_LIMIT: SSH client 192.168.30.117 failed to log in. The number of SSH sessions is 10, and exceeded the limit (10).
Explanation	The number of SSH sessions reached the upper limit.
Recommended action	No action is required.

SSHS_REACH_USER_LIMIT

Message text	SSH client [STRING] failed to log in, because the number of users reached the upper limit.
Variable fields	$1: IP address of the SSH client.
Severity level	6
Example	SSHS/6/SSHS_REACH_USER_LIMIT: SSH client 192.168.30.117 failed to log in, because the number of users reached the upper limit.
Explanation	The number of SSH users reached the upper limit.
Recommended action	No action is required.

SSHS_SCP_OPER

Message text	User [STRING] at [IPADDR] requested operation: [STRING].
Variable fields	$1: Username. $2: IP address of the SCP client. $3: Requested file operations: ○ **get file "*name*"'**—Downloads the file *name* from the SCP server. ○ **put file "*name*"**—Uploads the file *name* to the SCP server.
Severity level	6
Example	SSHS/6/SSHS_SCP_OPER: -MDC=1; User user1 at 1.1.1.1 requested operation: put file "aa".
Explanation	The SCP sever received an operation request from an SCP client.
Recommended action	No action is required.

SSHS_SFTP_OPER

Message text	User [STRING] at [IPADDR] requested operation: [STRING].
Variable fields	$1: Username. $2: IP address of the SFTP client. $3: Requested operations on a file or directory: ○ **open dir "*path*"**—Opens the directory *path*. ○ **open "*file*" (attribute code *code*) in *MODE* mode**—Opens the file *file* with the attribute code *code* in mode *MODE*. ○ **remove file "*path*"**—Deletes the file *path*. ○ **mkdir "*path*" (attribute code *code*)**—Creates a new directory *path* with the attribute code *code*. ○ **rmdir "*path*"**—Deletes the directory *path*. ○ **rename old "*old-name*" to new "*new-name*"**—Changes the name of a file or folder from *old-name* to *new-name*.
Severity level	6
Example	SSHS/6/SSHS_SFTP_OPER: User user1 at 1.1.1.1 requested operation: open dir "flash:/".
Explanation	The SFTP sever received an operation request from an SFTP client.
Recommended action	No action is required.

SSHS_SRV_UNAVAILABLE

Message text	The [STRING] server is disabled or the [STRING] service type is not supported.
Variable fields	$1: Service type: Stelnet, SCP, SFTP, or NETCONF.
Severity level	6
Example	SSHS/6/SSHS_SRV_UNAVAILABLE: The SCP server is disabled or the SCP service type is not supported.
Explanation	The Stelnet, SCP, SFTP, or NETCONF over SSH service was not available. The server was terminating the connection.
Recommended action	Check the service status or user configuration.

SSHS_VERSION_MISMATCH

Message text	SSH client [STRING] failed to log in because of version mismatch.
Variable fields	$1: IP address of the SSH client.
Severity level	6
Example	SSHS/6/SSHS_VERSION_MISMATCH: SSH client 192.168.30.117 failed to log in because of version mismatch.
Explanation	The SSH client failed to log in to the SSH server because they used different SSH versions.
Recommended action	Make sure the SSH client and the SSH server use the same SSH version.

SSL VPN messages

This section contains SSL VPN messages.

SSLVPN_ADD_CONTENT_TYPE

Message text	Set the content type for file policy [STRING] in context [STRING].
Variable fields	$1: File policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_CONTENT_TYPE: Set the content type for file policy fp1 in context ctx1.
Explanation	The type of file to be rewritten was set for a file policy.
Recommended action	No action is required.

SSLVPN_ADD_CONTENT_TYPE_FAILED

Message text	Failed to set the content type for file policy [STRING] in context [STRING].
Variable fields	$1: File policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_CONTENT_TYPE_FAILED: Failed to set the content type for file policy fp1 in context ctx1.
Explanation	Failed to set the type of file to be rewritten for a file policy.
Recommended action	No action is required.

SSLVPN_ADD_CONTEXT

Message text	Created SSL VPN context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_CONTEXT: Created SSL VPN context ctx1.
Explanation	An SSL VPN context was created.
Recommended action	No action is required.

SSLVPN_ADD_CONTEXT_FAILED

Message text	Failed to create SSL VPN context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_CONTEXT_FAILED: Failed to create SSL VPN context ctx1.
Explanation	Failed to create an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_EXCROUTEITEM

Message text	Added exclude route (IP [STRING] mask [STRING]) to route list [STRING] in context [STRING].
Variable fields	$1: Destination IP address of the route. $2: Subnet mask of the route. $3: Route list name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_EXCROUTEITEM: Added exclude route (IP 10.0.0.0 mask 255.0.0.0) to route list rtlist in context ctx1.
Explanation	An exclude route was added to a route list in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_EXCROUTEITEM_FAILED

Message text	Failed to add exclude route (IP [STRING] mask [STRING]) to route list [STRING] in context [STRING]
Variable fields	$1: Destination IP address of the route. $2: Subnet mask of the route. $3: Route list name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_EXCROUTEITEM_FAILED: Failed to add exclude route (IP 10.0.0.0 mask 255.0.0.0) to route list rtlist in context ctx1.
Explanation	Failed to add an exclude route to a route list in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_FILEPOLICY

Message text	Created file policy [STRING] in context [STRING].
Variable fields	$1: File policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_FILEPOLICY: Created file policy fp1 in context ctx1.
Explanation	A file policy was created.
Recommended action	No action is required.

SSLVPN_ADD_FILEPOLICY_FAILED

Message text	Failed to create file policy [STRING] in context [STRING].
Variable fields	$1: File policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_FILEPOLICY_FAILED: Failed to create file policy fp1 in context ctx1.
Explanation	Failed to create a file policy.
Recommended action	No action is required.

SSLVPN_ADD_GATEWAY

Message text	Created SSL VPN gateway [STRING].
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_GATEWAY: Created SSL VPN gateway gw1.
Explanation	An SSL VPN gateway was created.
Recommended action	No action is required.

SSLVPN_ADD_GATEWAY_FAILED

Message text	Failed to create SSL VPN gateway [STRING]
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_GATEWAY_FAILED: Failed to create SSL VPN gateway gw1.
Explanation	Failed to create an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_ADD_INCROUTEITEM

Message text	Added include route (IP [STRING] mask [STRING]) to route list [STRING] in context [STRING].
Variable fields	$1: Destination IP address of the route. $2: Subnet mask of the route. $3: Route list name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_INCROUTEITEM: Added include route (IP 10.0.0.0 mask 255.0.0.0) to route list rtlist in context ctx1.
Explanation	An include route was added to a route list in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_INCROUTEITEM_FAILED

Message text	Failed to add include route (IP [STRING] mask [STRING]) to route list [STRING] in context [STRING]
Variable fields	$1: Destination IP address of the route. $2: Subnet mask of the route. $3: Route list name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_INCROUTEITEM_FAILED: Failed to add include route (IP 10.0.0.0 mask 255.0.0.0) to route list rtlist in context ctx1.
Explanation	Failed to add an include route to a route list in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_IPADDRESSPOOL

Message text	Created IP address pool [STRING] start-IP [STRING] end-IP [STRING].
Variable fields	$1: Name of the IP address pool. $2: Start IP address of the address pool. $3: End IP address of the address pool.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_IPADDRESSPOOL: Created IP address pool pool1 start-IP 20.1.1.1 end-IP 20.1.1.100.
Explanation	An address pool was created.
Recommended action	No action is required.

SSLVPN_ADD_IPADDRESSPOOL_FAILED

Message text	Failed to create IP address pool [STRING] start-IP [STRING] end-IP [STRING]
Variable fields	$1: Name of the IP address pool. $2: Start IP address of the address pool. $3: End IP address of the address pool.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_IPADDRESSPOOL_FAILED: Failed to create IP address pool pool1 start-IP 20.1.1.1 end-IP 20.1.1.100.
Explanation	Failed to create an address pool.
Recommended action	Verify that the address pool to be created does not contain addresses that are already contained in existing address pools.

SSLVPN_ADD_IPTUNNELACIF

Message text	Specified SSL VPN AC interface [STRING] in context [STRING].
Variable fields	$1: Number of an SSL VPN AC interface. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_IPTUNNELACIF: Specified SSL VPN AC interface SSLVPN-AC1 in context ctx.
Explanation	An SSL VPN AC interface was specified in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_IPTUNNELACIF_FAILED

Message text	Failed to specify SSL VPN AC interface [STRING] in context [STRING]
Variable fields	$1: Number of an SSL VPN AC interface. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_IPTUNNELACIF_FAILED: Failed to specify SSL VPN AC interface SSLVPN-AC1 in context ctx.
Explanation	Failed to specify an SSL VPN AC interface in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_IPV4_RANGE

Message text	Specified IPv4 address range (start-IP [STRING] end-IP [STRING]) for SNAT pool [STRING].
Variable fields	$1: Start IPv4 address of the SSL VPN SNAT address pool. $2: End IPv4 address of the SSL VPN SNAT address pool. $3: SNAT address pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_IPV4_RANGE: Specified IPv4 address range (start-IP 192.168.1.1 end-IP 192.168.1.10) for SNAT pool sp1.
Explanation	An IPv4 address range was specified for an SSL VPN SNAT address pool.
Recommended action	No action is required.

SSLVPN_ADD_IPV4_RANGE_FAILED

Message text	Failed to specify IPv4 address range (start-IP [STRING] end-IP [STRING]) for SNAT pool [STRING].
Variable fields	$1: Start IPv4 address of the SSL VPN SNAT address pool. $2: End IPv4 address of the SSL VPN SNAT address pool. $3: SNAT address pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_IPV4_RANGE_FAILED: Failed to specify IPV4 address range (start-IP 192.168.1.1 end-IP 192.168.1.10) for SNAT pool sp1.
Explanation	Failed to specify the IPv4 address range for an SSL VPN SNAT address pool.
Recommended action	No action is required.

SSLVPN_ADD_IPV6_RANGE

Message text	Specified IPv6 address range (start-IP [STRING] end-IP [STRING]) for SNAT pool [STRING].
Variable fields	$1: Start IPv6 address of the SSL VPN SNAT address pool. $2: End IPv6 address of the SSL VPN SNAT address pool. $3: SNAT address pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_IPV6_RANGE: Specified IPv6 address range (start-IP 2000::1 end-IP 2000::10) for SNAT pool sp1.
Explanation	An IPv6 address range was specified for an SSL VPN SNAT address pool.
Recommended action	No action is required.

SSLVPN_ADD_IPV6_RANGE_FAILED

Message text	Failed to specify IPv6 address range (start-IP [STRING] end-IP [STRING]) for SNAT pool [STRING].
Variable fields	$1: Start IPv6 address of the SSL VPN SNAT address pool. $2: End IPv6 address of the SSL VPN SNAT address pool. $3: SNAT address pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_IPV6_RANGE_FAILED: Failed to specify IPv6 address range (start-IP 2000::1 end-IP 2000::10) for SNAT pool sp1.
Explanation	Failed to specify the IPv6 address range for an SSL VPN SNAT address pool.
Recommended action	No action is required.

SSLVPN_ADD_LOCALPORT

Message text	Added port forwarding entry local-port [STRING] local-name [STRING] remote-server [STRING] remote-port [STRING] [STRING] in port forwarding list [STRING] in context [STRING].
Variable fields	$1: Local port number. $2: Local address or local host name. $3: IP address or domain name of a TCP service on an internal server. $4: Port number of the TCP service. $5: Description of the port forwarding entry. This field is empty if no description is configured. $6: Port forwarding list name. $7: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_ADD_LOCALPORT: Added port forwarding entry local-port 80 local-name 127.0.0.1 remote-server 192.168.20.35 remote-port 80 in port forwarding list pflist1 in context ctx. • SSLVPN/6/SSLVPN_ADD_LOCALPORT: Added port forwarding entry local-port 80 local-name 127.0.0.1 remote-server 192.168.20.35 remote-port 80 description http in port forwarding list pflist1 in context ctx.
Explanation	A port forwarding entry was added to a port forwarding list.
Recommended action	No action is required.

SSLVPN_ADD_LOCALPORT_FAILED

Message text	Failed to add port forwarding entry local-port [STRING] local-name [STRING] remote-server [STRING] remote-port [STRING] [STRING] in port forwarding list [STRING] in context [STRING]
Variable fields	$1: Local port number. $2: Local address or local host name. $3: IP address or domain name of a TCP service on an internal server. $4: Port number of the TCP service. $5: Description of the port forwarding entry. This field is empty if no description is configured. $6: Port forwarding list name. $7: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_LOCALPORT_FAILED: Failed to add port forwarding entry ocal-port 80 local-name 127.0.0.1 remote-server 192.168.20.34 remote-port 80 in port forwarding list pflist1 in context ctx. SSLVPN/6/SSLVPN_ADD_LOCALPORT_FAILED: Failed to add port forwarding entry local-port 80 local-name 127.0.0.1 remote-server 192.168.20.34 remote-port 80 description http in port forwarding list pflist1 in context ctx.
Explanation	Failed to add a port forwarding entry to a port forwarding list.
Recommended action	No action is required.

SSLVPN_ADD_NEWCONTENT

Message text	Specified new content [STRING] for rewrite rule [STRING] in file policy [STRING] in context [STRING].
Variable fields	$1: New content used to replace the old content. $2: Rewrite rule name. $3: File policy name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_NEWCONTENT: Specified new content sslvpn rewrite htmlcode(d); for rewrite rule rw in file policy fp in context ctx.
Explanation	The new content used to replace the old content was specified for a rewrite rule.
Recommended action	No action is required.

SSLVPN_ADD_NEWCONTENT_FAILED

Message text	Failed to specify new content [STRING] for rewrite rule [STRING] in file policy [STRING] in context [STRING].
Variable fields	$1: New content used to replace the old content. $2: Rewrite rule name. $3: File policy name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_NEWCONTENT_FAILED: Failed to specify new content sslvpn rewrite htmlcode(d); for rewrite rule rw in file policy fp in context ctx.
Explanation	Failed to specify the new content used to replace the old content for a rewrite rule.
Recommended action	No action is required.

SSLVPN_ADD_OLDCONTENT

Message text	Specified old content [STRING] for rewrite rule [STRING] in file policy [STRING] in context [STRING].
Variable fields	$1: Old file content to be replaced. $2: Rewrite rule name. $3: File policy name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_OLDCONTENT: Specified old content a.b.c.innerHTML = d; for rewrite rule rw in file policy fp in context ctx.
Explanation	The old file content to be replaced was specified for a rewrite rule.
Recommended action	No action is required.

SSLVPN_ADD_OLDCONTENT_FAILED

Message text	Failed to specify old content [STRING] for rewrite rule [STRING] in file policy [STRING] in context [STRING].
Variable fields	$1: Old file content to be replaced. $2: Rewrite rule name. $3: File policy name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_OLDCONTENT_FAILED: Failed to specify old content a.b.c.innerHTML = d; for rewrite rule rw in file policy fp in context ctx.
Explanation	Failed to specify the old file content to be replaced for a rewrite rule.
Recommended action	No action is required.

SSLVPN_ADD_PORTFWD

Message text	Created port forwarding list [STRING] in context [STRING].
Variable fields	$1: Port forwarding list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_PORTFWD: Created port forwarding list pf in context ctx1.
Explanation	A port forwarding list was created.
Recommended action	No action is required.

SSLVPN_ADD_PORTFWD_FAILED

Message text	Failed to create port forwarding list [STRING] in context [STRING]
Variable fields	$1: Port forwarding list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_PORTFWD_FAILED: Failed to create port forwarding list pf in context ctx1.
Explanation	Failed to create a port forwarding list.
Recommended action	No action is required.

SSLVPN_ADD_PORTFWD_ITEM

Message text	Created port forwarding item [STRING] in context [STRING].
Variable fields	$1: Port forwarding item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_PORTFWD_ITEM: Created port forwarding item pfitem in context ctx1.
Explanation	A port forwarding item was created.
Recommended action	No action is required.

SSLVPN_ADD_PORTFWD_ITEM_FAILED

Message text	Failed to create port forwarding item [STRING] in context [STRING]
Variable fields	$1: Port forwarding item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_PORTFWD_ITEM_FAILED: Failed to create port forwarding item pfitem in context ctx1.
Explanation	Failed to create a port forwarding item.
Recommended action	No action is required.

SSLVPN_ADD_PYGROUP

Message text	Created policy group [STRING] in context [STRING].
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_PYGROUP: Created policy group pg in context ctx1.
Explanation	A policy group was created in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_PYGROUP_FAILED

Message text	Failed to create policy group [STRING] in context [STRING]
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_PYGROUP_FAILED: Failed to create policy group pg in context ctx1.
Explanation	Failed to create a policy group in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_REFER_PFWDITEM

Message text	Assigned port forwarding item [STRING] to port forwarding list [STRING] in context [STRING].
Variable fields	$1: Port forwarding item name. $2: Port forwarding list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFER_PFWDITEM: Assigned port forwarding item pfitem1 to port forwarding list pflist1 in context ctx1.
Explanation	A port forwarding item was assigned to a port forwarding list.
Recommended action	No action is required.

SSLVPN_ADD_REFER_PFWDITEM_FAILED

Message text	Failed to assign port forwarding item [STRING] to port forwarding list [STRING] in context [STRING].
Variable fields	$1: Port forwarding item name. $2: Port forwarding list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFER_PFWDITEM_FAILED: Failed to assign port forwarding item pfitem1 to port forwarding list pflist1 in context ctx1.
Explanation	Failed to assign a port forwarding item to a port forwarding list.
Recommended action	No action is required.

SSLVPN_ADD_REFER_SCUTLIST

Message text	Assigned shortcut list [STRING] to policy group [STRING] in context [STRING].
Variable fields	$1: Shortcut list name. $2: SSL VPN policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFER_SCUTLIST: Assigned shortcut list scutlist1 to policy group pg in context ctx1.
Explanation	A shortcut list was assigned to an SSL VPN policy group.
Recommended action	No action is required.

SSLVPN_ADD_REFERIPACL

Message text	Added IP access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING].
Variable fields	$1: IP version for the ACL. The value can be IPv6 or null. A null value represents IPv4. $2: Advanced ACL number. $3: Policy group name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERIPACL: Added IP access filter ACL 3000 in policy group pgroup in context ctx1.
Explanation	An ACL for IP access filtering was specified in a policy group.
Recommended action	No action is required.

SSLVPN_ADD_REFERIPACL_FAILED

Message text	Failed to add IP access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING]
Variable fields	$1: IP version for the ACL. The value can be IPv6 or null. A null value represents IPv4. $2: Advanced ACL number. $3: Policy group name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERIPACL_FAILED: Failed to add IP access filter ACL 3000 in policy group pgroup in context ctx1.
Explanation	Failed to specify an ACL for IP access filtering in a policy group.
Recommended action	No action is required.

SSLVPN_ADD_REFERPORTFWD

Message text	Specified port forwarding list [STRING] for policy-group [STRING] in context [STRING].
Variable fields	$1: Port forwarding list name. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERPORTFWD: Specified port forwarding list pf for policy-group pg in context ctx1.
Explanation	A port forwarding list was assigned to a policy group.
Recommended action	No action is required.

SSLVPN_ADD_REFERPORTFWD_FAILED

Message text	Failed to specify port forwarding list [STRING] for policy-group [STRING] in context [STRING]
Variable fields	$1: Port forwarding list name. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERPORTFWD_FAILED: Failed to specify port forwarding list pf for policy-group pg in context ctx1.
Explanation	Failed to assign a port forwarding list to a policy group.
Recommended action	Make sure a port forwarding list exists before you assign it to a policy group.

SSLVPN_ADD_REFERSCUTLIST_FAILED

Message text	Failed to assign shortcut list [STRING] to policy group [STRING] in context [STRING].
Variable fields	$1: Shortcut list name. $2: SSL VPN policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERSCUTLIST_FAILED: Failed to assign shortcut list scutlist1 to policy group pg in context ctx1.
Explanation	Failed to assign a shortcut list to an SSL VPN policy group.
Recommended action	No action is required.

SSLVPN_ADD_REFERSHORTCUT

Message text	Assigned shortcut [STRING] to shortcut list [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: Shortcut list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERSHORTCUT: Assigned shortcut shortcut1 to shortcut list scutlist1 in context ctx1.
Explanation	A shortcut was assigned to a shortcut list.
Recommended action	No action is required.

SSLVPN_ADD_REFERSHORTCUT_FAILED

Message text	Failed to assign shortcut [STRING] to shortcut list [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: Shortcut list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERSHORTCUT_FAILED: Failed to assign shortcut shortcut1 to shortcut list scutlist1 in context ctx1.
Explanation	Failed to assign a shortcut to a shortcut list.
Recommended action	No action is required.

SSLVPN_ADD_REFERSNATPOOL

Message text	Specified SNAT pool [STRING] for context [STRING].
Variable fields	$1: SNAT address pool name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERSNATPOOL: Specified SNAT pool sp1 for context ctx1.
Explanation	A SNAT address pool was assigned to an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_REFERSNATPOOL_FAILED

Message text	Failed to specify SNAT pool [STRING] for context [STRING].
Variable fields	$1: SNAT address pool name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERSNATPOOL_FAILED: Failed to specify SNAT pool sp1 for context ctx1.
Explanation	Failed to assign a SNAT address pool to an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_REFERTCPACL

Message text	Added TCP access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING].
Variable fields	$1: IP version for the ACL. The value can be IPv6 or null. A null value represents IPv4. $2: Advanced ACL number. $3: Policy group name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERTCPACL: Added TCP access filter ACL 3000 in policy group pgroup in context ctx1.
Explanation	An ACL for TCP access filtering was specified in a policy group.
Recommended action	No action is required.

SSLVPN_ADD_REFERTCPACL_FAILED

Message text	Failed to add TCP access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING]
Variable fields	$1: IP version for the ACL. The value can be IPv6 or null. A null value represents IPv4. $2: Advanced ACL number. $3: Policy group name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERTCPACL_FAILED: Failed to add TCP access filter ACL 3000 in policy group pgroup in context ctx1
Explanation	Failed to specify an ACL for TCP access filtering in a policy group.
Recommended action	No action is required.

SSLVPN_ADD_REFERURIACL

Message text	Added [STRING] access filter URI ACL [STRING] to policy group [STRING] in context [STRING].
Variable fields	$1: SSL VPN access mode. Options are: • IP access. • Web access. • TCP access. $2: URI ACL name. $3: Policy group name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERURIACL: Added IP access filter URI ACL uacl to policy group pgroup in context ctx1.
Explanation	A URI ACL was specified for IP, Web, or TCP access filtering in a policy group.
Recommended action	No action is required.

SSLVPN_ADD_REFERURIACL_FAILED

Message text	Failed to add [STRING] access filter URI ACL [STRING] to policy group [STRING] in context [STRING].
Variable fields	$1: SSL VPN access mode. Options are: • IP access • Web access. • TCP access. $2: URI ACL name. $3: Policy group name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERURIACL_FAILED: Failed to add IP access filter URI ACL uacl to policy group pgroup in context ctx1.
Explanation	Failed to specify a URI ACL for IP, Web, or TCP access filtering in a policy group.
Recommended action	No action is required.

SSLVPN_ADD_REFERURLLIST

Message text	Specified URL list [STRING] for policy-group [STRING] in context [STRING].
Variable fields	$1: URL list name. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERURLLIST: Specified URL list urllist for policy-group pg in context ctx1.
Explanation	A URL list was assigned to a policy group.
Recommended action	No action is required.

SSLVPN_ADD_REFERURLLIST_FAILED

Message text	Failed to specify URL list [STRING] for policy-group [STRING] in context [STRING]
Variable fields	$1: URL list name. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERURLLIST_FAILED: Failed to specify URL list urllist for policy-group pg in context ctx1.
Explanation	Failed to assign a URL list to a policy group.
Recommended action	Verity that a URL list exists before you assign it to a policy group.

SSLVPN_ADD_REFERWEBACL

Message text	Added Web access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING].
Variable fields	$1: IP version for the ACL. The value can be IPv6 or null. A null value represents IPv4. $2: Advanced ACL number. $3: Policy group name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERWEBACL: Added Web access filter ACL 3000 in policy group pgroup in context ctx1.
Explanation	An ACL for Web accessing filtering was specified in a policy group.
Recommended action	No action is required.

SSLVPN_ADD_REFERWEBACL_FAILED

Message text	Failed to add Web access filter [STRING] ACL [STRING] in policy group [STRING] in context [STRING]
Variable fields	$1: IP version for the ACL. The value can be IPv6 or null. A null value represents IPv4. $2: Advanced ACL number. $3: Policy group name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REFERWEBACL_FAILED: Failed to add Web access filter ACL 3000 in policy group pgroup in context ctx1.
Explanation	Failed to specify an ACL for Web accessing filtering in a policy group.
Recommended action	No action is required.

SSLVPN_ADD_REWRITE_RULE

Message text	Created rewrite rule [STRING] in file policy [STRING] in context [STRING].
Variable fields	$1: Rewrite rule name. $2: File policy name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REWRITE_RULE: Created rewrite rule rw in file policy fp in context ctx.
Explanation	A rewrite rule was created.
Recommended action	No action is required.

SSLVPN_ADD_REWRITE_RULE_FAILED

Message text	Failed to create rewrite rule [STRING] in file policy [STRING] in context [STRING].
Variable fields	$1: Rewrite rule name. $2: File policy name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_REWRITE_RULE_FAILED: Failed to create rewrite rule rw in file policy fp in context ctx.
Explanation	Failed to create a rewrite rule.
Recommended action	No action is required.

SSLVPN_ADD_ROUTELIST

Message text	Created IP-route-list [STRING] in context [STRING].
Variable fields	$1: Route list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_ROUTELIST: Created IP-route-list rtlist in context ctx1.
Explanation	A route list was created in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_ROUTELIST_FAILED

Message text	Failed to create IP-route-list [STRING] in context [STRING]
Variable fields	$1: Route list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_ROUTELIST_FAILED: Failed to create IP-route-list rtlist in context ctx1.
Explanation	Failed to create a route list in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_ROUTEREFER

Message text	Configured access-route [STRING] in policy-group [STRING] in context [STRING].
Variable fields	$1: Route to be issued to clients. Valid values are: • Route in the format of *ip-address mask*. • Force-all. This setting forces all traffic to be sent to the SSL VPN gateway. • Route list name in the format of **ip-route-list** *list-name.* All routes in the route list will be issued to clients. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_ADD_ROUTEREFER: Configured access-route ip-route-list rtlist in policy-group pg in context ctx. • SSLVPN/6/SSLVPN_ADD_ROUTEREFER: Configured access-route 1.0.0.0 255.240.0.0 in policy-group pg in context ctx. • SSLVPN/6/SSLVPN_ADD_ROUTEREFER: Configured access-route force-all in policy-group pg in context ctx.
Explanation	Routes to be issued to clients were specified in a policy group.
Recommended action	No action is required.

SSLVPN_ADD_ROUTEREFER_FAILED

Message text	Failed to configure access-route [STRING] in policy-group [STRING] in context [STRING]
Variable fields	$1: Route to be issued to clients. Valid values are: • Route in the format of *ip-address mask*. • Force-all. This setting forces all traffic to be sent to the SSL VPN gateway. • Route list name in the format of **ip-route-list** *list-name.* All routes in the route list will be issued to clients. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_ADD_ROUTEREFER_FAILED: Failed to configure access-route ip-route-list rtlist in policy-group pg in context ctx. • SSLVPN/6/SSLVPN_ADD_ROUTEREFER_FAILED: Failed to configure access-route 1.0.0.0 255.240.0.0 in policy-group pg in context ctx. • SSLVPN/6/SSLVPN_ADD_ROUTEREFER_FAILED: Failed to configure access-route force-all in policy-group pg in context ctx.
Explanation	Failed to specify a route or a route list to be issued to clients in a policy group.
Recommended action	Verify that a route list exists before you specify it in a policy group.

SSLVPN_ADD_SERVERURL

Message text	Specified URL [STRING] for URL item [STRING] in context [STRING].
Variable fields	$1: URL string. $2: URL item name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_SERVERURL: Specified URL www.abc.com for URL item item1 in context ctx1.
Explanation	Configured the URL for a URL item.
Recommended action	No action is required.

SSLVPN_ADD_SERVERURL_FAILED

Message text	Failed to specify URL [STRING] for URL item [STRING] in context [STRING].
Variable fields	$1: URL string. $2: URL item name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_SERVERURL_FAILED: Failed to specify URL www.abc.com for URL item item1 in context ctx1.
Explanation	Failed to configure the URL for a URL item.
Recommended action	No action is required.

SSLVPN_ADD_SHORTCUT

Message text	Created shortcut [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_SHORTCUT: Created shortcut shortcut1 in context ctx1.
Explanation	A shortcut was created.
Recommended action	No action is required.

SSLVPN_ADD_SHORTCUT_FAILED

Message text	Failed to create shortcut [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_SHORTCUT_FAILED: Failed to create shortcut shortcut1 in context ctx1.
Explanation	Failed to create a shortcut.
Recommended action	No action is required.

SSLVPN_ADD_SHORTCUTLIST

Message text	Created shortcut list [STRING] in context [STRING].
Variable fields	$1: Shortcut list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_SHORTCUTLIST: Created shortcut list scutlist1 in context ctx1.
Explanation	A shortcut list was created.
Recommended action	No action is required.

SSLVPN_ADD_SHORTCUTLIST_FAILED

Message text	Failed to create shortcut list [STRING] in context [STRING].
Variable fields	$1: Shortcut list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_SHORTCUTLIST_FAILED: Failed to create shortcut list scutlist1 in context ctx1.
Explanation	Failed to create a shortcut list.
Recommended action	No action is required.

SSLVPN_ADD_SNATPOOL

Message text	Created SSL VPN SNAT pool [STRING].
Variable fields	$1: SNAT address pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_SNATPOOL: Created SSL VPN SNAT pool sp1.
Explanation	An SSL VPN SNAT address pool was created.
Recommended action	No action is required.

SSLVPN_ADD_SNATPOOL_FAILED

Message text	Failed to create SSL VPN SNAT pool [STRING].
Variable fields	$1: SNAT address pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_SNATPOOL_FAILED: Failed to create SSL VPN SNAT pool sp1.
Explanation	Failed to create an SSL VPN SNAT address pool.
Recommended action	No action is required.

SSLVPN_ADD_URIACL

Message text	Created URI ACL [STRING] in context [STRING].
Variable fields	$1: URI ACL name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_URIACL: Created URI ACL uacl in context ctx1.
Explanation	A URI ACL was created.
Recommended action	No action is required.

SSLVPN_ADD_URIACL_FAILED

Message text	Failed to create URI ACL [STRING] in context [STRING].
Variable fields	$1: URI ACL name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_URIACL_FAILED: Failed to create URI ACL uacl in context ctx1.
Explanation	Failed to create a URI ACL.
Recommended action	No action is required.

SSLVPN_ADD_URIACL_RULE

Message text	Added rule [UINT32] to URI ACL [STRING] in context [STRING].
Variable fields	$1: Rule ID. $2: URI ACL name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_URIACL_RULE: Added rule 5 to URI ACL uacl in context ctx1.
Explanation	A rule was added to a URI ACL.
Recommended action	No action is required.

SSLVPN_ADD_URIACL_RULE_FAILED

Message text	Failed to add rule [UINT32] to URI ACL [STRING] in context [STRING].
Variable fields	$1: Rule ID. $2: URI ACL name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_URIACL_RULE_FAILED: Failed to add rule 5 to URI ACL uacl in context ctx1.
Explanation	Failed to add a rule to a URI ACL.
Recommended action	No action is required.

SSLVPN_ADD_URL

Message text	Set URL (URL [STRING]) for file policy [STRING] in context [STRING].
Variable fields	$1: URL of the file to be rewritten. $2: File policy name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_URL: Set URL (URL http://192.168.1.1:8080/test.js) for file policy fp1 in context ctx1.
Explanation	The URL of the file to be rewritten was set for a file policy.
Recommended action	No action is required.

SSLVPN_ADD_URL_FAILED

Message text	Failed to set URL (URL [STRING]) for file policy [STRING] in context [STRING].
Variable fields	$1: URL of the file to be rewritten. $2: File policy name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_URL_FAILED: Failed to set URL (URL http://192.168.1.1:8080/test.js) for file policy fp1 in context ctx1.
Explanation	Failed to set the URL of the file to be rewritten for a file policy.
Recommended action	No action is required.

SSLVPN_ADD_URLITEM

Message text	Created URL item [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_URLITEM: Created URL item item1 in context ctx1.
Explanation	Created a URL item.
Recommended action	No action is required.

SSLVPN_ADD_URLITEM_FAILED

Message text	Failed to create URL item [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_URLITEM_FAILED: Failed to create URL item item1 in context ctx1.
Explanation	Failed to create a URL item.
Recommended action	No action is required.

SSLVPN_ADD_URLLIST

Message text	Created URL list [STRING] in context [STRING].
Variable fields	$1: URL list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_URLLIST: Created URL list urllist in context ctx1.
Explanation	A URL list was created.
Recommended action	No action is required.

SSLVPN_ADD_URLLIST_FAILED

Message text	Failed to create URL list [STRING] in context [STRING]
Variable fields	$1: URL list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_URLLIST_FAILED: Failed to create URL list urllist in context ctx1.
Explanation	Failed to create a URL list.
Recommended action	No action is required.

SSLVPN_ADD_USER

Message text	Failed to create user [STRING] in context [STRING].
Variable fields	$1: Username. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_USER_FAILED: Failed to create user user1 in context ctx1.
Explanation	Failed to create an SSL VPN user in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ADD_USER_FAILED

Message text	Created user [STRING] in context [STRING].
Variable fields	$1: Username. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ADD_USER: Created user user1 in context ctx1.
Explanation	An SSL VPN user was created in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_AAADOMAIN

Message text	Specified AAA domain [STRING] for context [STRING].
Variable fields	$1: ISP domain name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_AAADOMAIN: Specified AAA domain myserver for context ctx1.
Explanation	An ISP domain was specified for authentication, authorization, and accounting of SSL VPN users in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_AAADOMAIN_FAILED

Message text	Failed to specify AAA domain [STRING] for context [STRING].
Variable fields	$1: ISP domain name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_AAADOMAIN_FAILED: Failed to specify AAA domain myserver for context ctx1.
Explanation	Failed to specify an ISP domain for authentication, authorization, and accounting of SSL VPN users in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_AUTHMODE

Message text	Configured authentication use [STRING] in context [STRING].
Variable fields	$1: Authentication mode, which indicates the authentication methods required for users to log in to the SSL VPN context. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_AUTHMODE: Configured authentication use all in context ctx1.
Explanation	Configured the authentication mode of an SSL VPN context. • The **all** mode indicates that a user must pass all enabled authentication methods to log in to the SSL VPN context. • The **any-one** mode indicates that a user can log in to the SSL VPN context after passing any enabled authentication method.
Recommended action	No action is required.

SSLVPN_CFG_AUTHMODE_FAILED

Message text	Failed to configure authentication use [STRING] in context [STRING].
Variable fields	$1: Authentication mode, which indicates the authentication methods required for users to log in to the SSL VPN context. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_AUTHMODE_FAILED: Failed to configure authentication use all in context ctx1.
Explanation	Failed to configure the authentication mode of an SSL VPN context. • The **all** mode indicates that a user must pass all enabled authentication methods to log in to the SSL VPN context. • The **any-one** mode indicates that a user can log in to the SSL VPN context after passing any enabled authentication method.
Recommended action	No action is required.

SSLVPN_CFG_BINDIP

Message text	Bound IP addresses [STRING] to user [STRING] in context [STRING].
Variable fields	$1: IP address list. $2: SSL VPN username. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_BINDIP: Bound IP addresses 10.1.1.1,10.1.1.3-10.1.1.5 to user user1 in context ctx1.
Explanation	IP addresses were bound to an SSL VPN user.
Recommended action	No action is required.

SSLVPN_CFG_BINDIP_FAILED

Message text	Failed to bind IP addresses [STRING] to user [STRING] in context [STRING].
Variable fields	$1: IP address list. $2: SSL VPN username. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_BINDIP_FAILED: Failed to bind IP addresses 10.1.1.1,10.1.1.3-10.1.1.5 to user user1 in context ctx1.
Explanation	Failed to bind IP addresses to an SSL VPN user.
Recommended action	No action is required.

SSLVPN_CFG_BINDIPAUTO

Message text	Set the number of IP addresses automatically bound to user [STRING] in context [STRING] to [UINT32].
Variable fields	$1: SSL VPN username. $2: SSL VPN context name. $3: Number of IP addresses to be automatically bound to the user.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_BINDIPAUTO: Set the number of IP addresses automatically bound to user user1 in context ctx1 to 3.
Explanation	The number of IP addresses to be automatically bound to an SSL VPN user was specified.
Recommended action	No action is required.

SSLVPN_CFG_BINDIPAUTO_FAILED

Message text	Failed to set the number of IP addresses automatically bound to user [STRING] in context [STRING] to [UINT32].
Variable fields	$1: SSL VPN username. $2: SSL VPN context name. $3: Number of IP addresses to be automatically bound to the user.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_BINDIPAUTO_FAILED: Failed to set the number of IP addresses automatically bound to user user1 in context ctx1 to 3.
Explanation	Failed to set the number of IP addresses to be automatically bound to an SSL VPN.
Recommended action	No action is required.

SSLVPN_CFG_CERTATTRIBUTE

Message text	Specified the attribute [STRING] as the certificate user name in context [STRING].
Variable fields	$1: Certificate attribute used as the SSL VPN username. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_ CERTATTRIBUTE: Specified the attribute cn as the certificate user name in context ctx1.
Explanation	A certificate attribute was specified as the SSL VPN username.
Recommended action	No action is required.

SSLVPN_CFG_CERTATTRIBUTE_FAILED

Message text	Failed to specify the attribute [STRING] as the certificate user name in context [STRING].
Variable fields	$1: Certificate attribute used as the SSL VPN username. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_CERTATTRIBUTE_FAILED: Failed to specify the attribute cn as the certificate user name in context ctx1.
Explanation	Failed to specify a certificate attribute as the SSL VPN username.
Recommended action	No action is required.

SSLVPN_CFG_CTXUSERMAX

Message text	Set the maximum number of connections to [STRING] for each session in context [STRING].
Variable fields	$1: Maximum number of concurrent connections per session. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_CTXUSERMAX: Set the maximum number of connections to 50 for each session in context ctx1.
Explanation	The maximum number of concurrent connections per session was set in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_CTXUSERMAX_FAILED

Message text	Failed to set the maximum number of connections to [STRING] for each session in context [STRING].
Variable fields	$1: Maximum number of concurrent connections per session. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_CTXUSERMAX_FAILED: Failed to set the maximum number of connections to 50 for each session in context ctx1.
Explanation	Failed to set the maximum number of concurrent connections per session in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_CONTEXT_USERMAXIMUM

Message text	Configured the maximum number of SSL VPN users in context [UINT32].
Variable fields	$1: Context ID.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_CONTEXT_USERMAXIMUM: Configured the maximum number of SSL VPN users in context 2.
Explanation	The maximum number of SSL VPN users was set in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_CONTEXT_USERMAXIMUM_FAILED

Message text	Failed to configure the maximum number of SSL VPN users in context [UINT32].
Variable fields	$1: Context ID.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_CONTEXT_USERMAXIMUM_FAILED: Failed to configure the maximum number of SSL VPN users in context 2.
Explanation	Failed to configure the maximum number of SSL VPN users in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_CONTEXTVPN

Message text	Associated VPN instance [STRING] with context [STRING].
Variable fields	$1: VPN instance name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_CONTEXTVPN: Associated VPN instance vpn1 with context ctx1.
Explanation	An SSL VPN context was associated with a VPN instance.
Recommended action	No action is required.

SSLVPN_CFG_CONTEXTVPN_FAILED

Message text	Failed to associate VPN instance [STRING] with context [STRING]
Variable fields	$1: VPN instance name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_CONTEXTVPN_FAILED: Failed to associate VPN instance vpn1 with context ctx1.
Explanation	Failed to associate an SSL VPN context with a VPN instance.
Recommended action	No action is required.

SSLVPN_CFG_CTX_WEBPAGECUST_FAIL

Message text	Failed to specify template [STRING] for SSL VPN webpage customization in context [STRING].
Variable fields	$1: Webpage template name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_CTX_WEBPAGECUST_FAIL: Failed to specify template user1 for SSL VPN webpage customization in context a.
Explanation	Failed to specify an SSL VPN webpage template for an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_CTX_WEBPAGECUST

Message text	Specified template [STRING] for SSL VPN webpage customization in context [STRING].
Variable fields	$1: Webpage template name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_CTX_WEBPAGECUST: Specified template user1 for SSL VPN webpage customization in context a.
Explanation	An SSL VPN webpage template was successfully specified for an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_CTXGATEWAY

Message text	Configured gateway [STRING] [domain [STRING] | virtual-host [STRING]] in context [STRING].
Variable fields	$1: SSL VPN gateway name. $2: Domain name. $3: Virtual host name. $4: SSL VPN context name. Parameters $2 and $3 cannot be both configured. This message displays parameter $2, $3, or neither, depending on the configuration.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_CTXGATEWAY: Configured gateway gw domain domain1 in context ctx1. • SSLVPN/6/SSLVPN_CFG_CTXGATEWAY: Configured gateway gw virtual-host myhost1 in context ctx1. • SSLVPN/6/SSLVPN_CFG_CTXGATEWAY: Configured gateway gw in context ctx1.
Explanation	An SSL VPN context was associated with an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CFG_CTXGATEWAY_FAILED

Message text	Failed to configure gateway [STRING] [domain [STRING] | virtual-host [STRING]] in context [STRING]
Variable fields	$1: SSL VPN gateway name. $2: Domain name. $3: Virtual host name. $4: SSL VPN context name. Parameters $2 and $3 cannot be both configured. This message displays parameter $2, $3, or neither, depending on the configuration.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_CTXGATEWAY_FAILED: Failed to configure gateway gw domain domain1 in context ctx1. • SSLVPN/6/SSLVPN_CFG_CTXGATEWAY_FAILED: Failed to configure gateway gw virtual-host myhost1 in context ctx1. • SSLVPN/6/SSLVPN_CFG_CTXGATEWAY_FAILED: Failed to configure gateway gw in context ctx1.
Explanation	Failed to associate an SSL VPN context with an SSL VPN gateway.
Recommended action	**343.** Make sure the SSL VPN gateway to be associated already exists. **344.** Identify the number of SSL VPN gateways associated with the SSL VPN context. If the number reaches the maximum and you want to associate a new gateway, remove an existing gateway association.

SSLVPN_CFG_DEFAULTPGROUP

Message text	Configured default-policy-group [STRING] in context [STRING].
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_DEFAULTPGROUP: Configured default-policy group pgroup in context ctx1.
Explanation	A policy group was specified as the default policy group in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_DEFAULTPGROUP_FAILED

Message text	Failed to configure default-policy-group [STRING] in context [STRING].
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_DEFAULTPGROUP_FAILED: Failed to configure default-policy-group pgroup in context ctx1.
Explanation	Failed to specify a policy group as the default policy group in an SSL VPN context.
Recommended action	Verify that a policy group exists before you specify it as the default policy group in an SSL VPN context.

SSLVPN_CFG_DNSSERVER

Message text	Specified [STRING] DNS server [STRING] in context [STRING].
Variable fields	$1: DNS server type, primary or secondary. $2: IP address of the DNS server. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_DNSSERVER: Specified primary DNS server 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CFG_DNSSERVER: Specified secondary DNS server 1.1.1.2 in context ctx.
Explanation	A DNS server was specified for IP access in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_DNSSERVER_FAILED

Message text	Failed to specify [STRING] DNS server [STRING] in context [STRING]
Variable fields	$1: DNS server type, primary or secondary. $2: IP address of the DNS server. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_DNSSERVER_FAILED: Failed to specify primary DNS server 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CFG_DNSSERVER_FAILED: Failed to specify secondary DNS server 1.1.1.2 in context ctx.
Explanation	Failed to specify a DNS server for IP access in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_EMOSERVER

Message text	Specified EMO server address [STRING] and port [STRING] in context [STRING].
Variable fields	$1: Host name or IPv4 address of the EMO server. $2: Port number of the EMO server. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_EMOSERVER: Specified EMO server address 10.10.1.1 and port 9058 in context ctx1. • SSLVPN/6/SSLVPN_CFG_EMOSERVER: Specified EMO server address host and port 9058 in context ctx1.
Explanation	An EMO server was specified for mobile clients in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_EMOSERVER_FAILED

Message text	Failed to specify EMO server address [STRING] and port [STRING] in context [STRING].
Variable fields	$1: Host name or IPv4 address of the EMO server. $2: Port number of the EMO server. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_EMOSERVER_FAILED: Failed to specify EMO server address 10.10.1.1 and port 9058 in context ctx1. • SSLVPN/6/SSLVPN_CFG_EMOSERVER_FAILED: Failed to specify EMO server address host and port 9058 in context ctx1.
Explanation	Failed to specify an EMO server for mobile clients in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_GATEWAYVPN

Message text	Specify VPN instance [STRING] for gateway [STRING].
Variable fields	$1: Name of the VPN instance to which the SSL VPN gateway belongs. $2: Name of the SSL VPN gateway.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_GATEWAYVPN: Specify VPN instance vpn1 for gateway gw1.
Explanation	A VPN instance was specified for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CFG_GATEWAYVPN_FAILED

Message text	Failed to specify VPN instance [STRING] for gateway [STRING]
Variable fields	$1: Name of the VPN instance to which the SSL VPN gateway belongs. $2: Name of the SSL VPN gateway.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_GATEWAYVPN_FAILED: Failed to specify VPN instance vpn1 for gateway gw1.
Explanation	Failed to specify a VPN instance for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CFG_GLB_WEBPAGECUST_FAIL

Message text	Failed to specify template [STRING] for global SSL VPN webpage customization.
Variable fields	$1: Webpage template name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_GLB_WEBPAGECUST_FAIL: Failed to specify template user1 for global SSL VPN webpage customization.
Explanation	Failed to specify a global SSL VPN webpage template.
Recommended action	No action is required.

SSLVPN_CFG_GLB_WEBPAGECUST

Message text	Specified template [STRING] for global SSL VPN webpage customization.
Variable fields	$1: Webpage template name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_GLB_WEBPAGECUST: Specified template user1 for global SSL VPN webpage customization.
Explanation	A global SSL VPN webpage template was specified successfully.
Recommended action	No action is required.

SSLVPN_CFG_GWIPADDRESS

Message text	Configured IP address [STRING] and port [STRING] for gateway [STRING].
Variable fields	$1: IP address of the SSL VPN gateway. $2: Port number of the SSL VPN gateway. $3: Name of the SSL VPN gateway.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_GWIPADDRESS: Configured IP address 10.10.1.1 and port 8000 for gateway gw1.
Explanation	An IP address and port number were specified for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CFG_GWIPADDRESS_FAILED

Message text	Failed to configure IP address [STRING] and port [STRING] for gateway [STRING]
Variable fields	$1: IP address of the SSL VPN gateway. $2: Port number of the SSL VPN gateway. $3: Name of the SSL VPN gateway.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_GWIPADDRESS_FAILED: Failed to configure IP address 10.10.1.1 and port 8000 for gateway gw1.
Explanation	Failed to specify the IP address and port number for an SSL VPN gateway.
Recommended action	**345.** Verify that the IP address specified for the SSL VPN gateway is not used by another gateway. **346.** Verify that the port specified for the SSL VPN gateway is different from the HTTP-redirect port.

SSLVPN_CFG_GWIPV6ADDRESS

Message text	Configured IPv6 address [STRING] and port [STRING] for gateway [STRING].
Variable fields	$1: IPv6 address of the SSL VPN gateway. $2: Port number of the SSL VPN gateway. $3: Name of the SSL VPN gateway.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_GWIPV6ADDRESS: Configured IPv6 address 1::1 and port 1027 for gateway gw1.
Explanation	An IPv6 address and port number were specified for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CFG_GWIPV6ADDRESS_FAILED

Message text	Failed to configure IPv6 address [STRING] and port [STRING] for gateway [STRING].
Variable fields	$1: IPv6 address of the SSL VPN gateway. $2: Port number of the SSL VPN gateway. $3: Name of the SSL VPN gateway.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_GWIPV6ADDRESS_FAILED: Failed to configure IPv6 address 1::1 and port 1027 for gateway gw1.
Explanation	Failed to specify the IPv6 address and port number for an SSL VPN gateway.
Recommended action	**347.** Verify that the IP address specified for the SSL VPN gateway is not used by another gateway. **348.** Verify that the port specified for the SSL VPN gateway is different from the HTTP-redirect port.

SSLVPN_CFG_HTTPREDIRECT

Message text	Configured HTTP-redirect port [STRING] in gateway [STRING].
Variable fields	$1: HTTP redirection port number. $2: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_HTTPREDIRECT: Configured HTTP-redirect port 8000 in gateway gw.
Explanation	HTTP redirection was enabled.
Recommended action	No action is required.

SSLVPN_CFG_HTTPREDIRECT_FAILED

Message text	Failed to configure HTTP-redirect port [STRING] in gateway [STRING]
Variable fields	$1: HTTP port number. $2: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_HTTPREDIRECT_FAILED: Failed to configure HTTP-redirect port 8000 in gateway gw.
Explanation	Failed to enable HTTP redirection for a port on an SSL VPN gateway.
Recommended action	Verify that the specified HTTP port number is not used by other redirection services.

SSLVPN_CFG_IMCADDRESS

Message text	Configured the IP address [STRING] port number [STRING], and VPN instance [STRING] of the iMC server in context [STRING].
Variable fields	$1: IP address of the IMC server for SMS message authentication. $2: Port number of the IMC server. $3: VPN instance to which the IMC server belongs. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_IMCADDRESS: Configured the IP address 10.10.1.1 port number 8080 and VPN instance vpn1 of the iMC server in context ctx1.
Explanation	An IMC server for SMS message authentication was configured in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_IMCADDRESS_FAILED

Message text	Failed to configure the IP address [STRING] port number [STRING], and VPN instance [STRING] of the IMC server in context [STRING].
Variable fields	$1: IP address of the IMC server for SMS message authentication. $2: Port number of the IMC server for SMS message authentication. $3: VPN instance to which the IMC server belongs. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_IMCADDRESS_FAILED: Failed to configure the IP address 10.10.1.1 port number 8080 and VPN instance vpn1 of the IMC server in context ctx1.
Explanation	Failed to configure an IMC server for SMS message authentication in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_IPAC_WEBRESPUSH

Message text	Enabled automatic pushing of Web resources after IP access client login in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_IPAC_WEBRESPUSH: Enabled automatic pushing of Web resources after IP access client login in context ctx.
Explanation	Enabled automatic webpage pushing of accessible resources after IP access client login in an SSL VPN context..
Recommended action	No action is required.

SSLVPN_CFG_IPAC_WEBRESPUSH_FAIL

Message text	Failed to enable automatic pushing of Web resources after IP access client login in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_IPAC_WEBRESPUSH_FAIL: Failed to enable automatic pushing of Web resources after IP access client login in context ctx.
Explanation	Failed to enable automatic webpage pushing of accessible resources after IP access client login in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_IPCLIENT_AUTOACT

Message text	Enabled automatic IP access client startup after Web login in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_IPCLIENT_AUTOACT: Enabled automatic IP access client startup after Web login in context ctx.
Explanation	Enabled automatic IP access client startup after Web login in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_IPCLIENT_AUTOACT_FAIL

Message text	Failed to enable automatic IP access client startup after Web login in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_IPCLIENT_AUTOACT_FAIL: Failed to enable automatic IP access client startup after Web login in context ctx.
Explanation	Failed to enable automatic IP access client startup after Web login in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_IPTNL_RATE-LIMIT

Message text	Set the IP tunnel [STRING] rate limit to [UINT32] [STRING] in context [STRING].
Variable fields	$1: SSL VPN IP access traffic direction: • Upstream. • Downstream. $2: Rate limit value. $3: Unit of mesurement for the rate limit: • kbps. • pps. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_IPTNL_RATE-LIMIT: Set the IP tunnel upstream rate limit to 1000 kbps in context ctx. SSLVPN/6/SSLVPN_CFG_IPTNL_RATE-LIMIT: Set the IP tunnel downstream rate limit to 1000 pps in context ctx.
Explanation	Set a rate limit for IP access upstream or downstream traffic.
Recommended action	No action is required.

SSLVPN_CFG_IPTNL_RATE-LIMIT_FAIL

Message text	Failed to set the IP tunnel [STRING] rate limit to [UINT32] [STRING] in context [STRING].
Variable fields	$1: SSL VPN IP access traffic direction: • Upstream. • Downstream. $2: Rate limit value. $3: Unit of mesurement for the rate limit: • kbps. • pps. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_IPTNL_RATE-LIMIT_FAIL: Failed to set the IP tunnel upstream rate limit to 1000 kbps in context ctx. SSLVPN/6/SSLVPN_CFG_IPTNL_RATE-LIMIT_FAIL: Failed to set the IP tunnel downstream rate limit to 1000 pps in context ctx.
Explanation	Failed to set a rate limit for IP access upstream or downstream traffic.
Recommended action	No action is required.

SSLVPN_CFG_IPTUNNELPOOL

Message text	Specified address-pool [STRING] mask [STRING] in context [STRING].
Variable fields	$1: Name of the address pool. $2: Mask length or mask of the address pool. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_IPTUNNELPOOL: Specified address-pool pool1 mask 255.255.255.0 in context ctx.
Explanation	An address pool for IP access was specified in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_IPTUNNELPOOL_FAILED

Message text	Failed to specify address-pool [STRING] mask [STRING] in context [STRING]
Variable fields	$1: Name of the address pool. $2: Mask length or mask of the address pool. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_IPTUNNELPOOL_FAILED: Failed to specify address-pool pool1 mask 255.255.255.0 in context ctx.
Explanation	Failed to specify an address pool for IP address in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_KEEPALIVE

Message text	Configured IP Tunnel keepalive interval [STRING] seconds in context [STRING].
Variable fields	$1: Keepalive interval in seconds. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_KEEPALIVE: Configured IP Tunnel keepalive interval 50 seconds in context ctx.
Explanation	The keepalive interval for IP access was set in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_KEEPALIVE_FAILED

Message text	Failed to configure IP Tunnel keepalive interval [STRING] seconds in context [STRING]
Variable fields	$1: Keepalive interval in seconds. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_KEEPALIVE_FAILED: Failed to configure IP Tunnel keepalive interval 50 seconds in context ctx.
Explanation	Failed to set the keepalive interval for IP access in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_LOCALPORT

Message text	Configured port forwarding instance local-port [STRING] local-name [STRING] remote-server [STRING] remote-port [STRING] [STRING] for port forwarding item [STRING] in context [STRING].
Variable fields	$1: Local port number. $2: Local address or local host name. $3: IP address or domain name of a TCP service on an internal server. $4: Port number of the TCP service. $5: Description of the port forwarding instance. This field is not displayed if no description is configured. $6: Name of the port forwarding item for which the port forwarding instance is configured. $7: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_LOCALPORT: Configured port forwarding instance local-port 80 local-name 127.0.0.1 remote-server 192.168.20.35 remote-port 80 for port forwarding item pfitem1 in context ctx. • SSLVPN/6/SSLVPN_CFG_LOCALPORT: Configured port forwarding instance local-port 80 local-name 127.0.0.1 remote-server 192.168.20.35 remote-port 80 description http for port forwarding item pfitem1 in context ctx.
Explanation	A port forwarding instance was configured for a port forwarding item.
Recommended action	No action is required.

SSLVPN_CFG_LOCALPORT_FAILED

Message text	Failed to configure port forwarding instance local-port [STRING] local-name [STRING] remote-server [STRING] remote-port [STRING] [STRING] for port forwarding item [STRING] in context [STRING]
Variable fields	$1: Local port number. $2: Local address or local host name. $3: IP address or domain name of a TCP service on an internal server. $4: Port number of the TCP service $5: Description of the port forwarding instance. This field is not displayed if no description is configured. $6: Name of the port forwarding item for which the port forwarding instance is configured. $7: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_LOCALPORT_FAILED: Failed to configure port forwarding instance local-port 80 local-name 127.0.0.1 remote-server 192.168.20.34 remote-port 80 for port forwarding item pfitem1 in context ctx. • SSLVPN/6/SSLVPN_CFG_LOCALPORT_FAILED: Failed to configure port forwarding instance local-port 80 local-name 127.0.0.1 remote-server 192.168.20.34 remote-port 80 description http for port forwarding item pfitemt1 in context ctx.
Explanation	Failed to configure a port forwarding instance for a port forwarding item.
Recommended action	No action is required.

SSLVPN_CFG_LOGINMESSAGE

Message text	Configured SSL VPN [STRING] login message [STRING] in context [STRING].
Variable fields	$1: Language used on the login page, English or Chinese. $2: Welcome message on the login page. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_LOGINMESSAGE: Configured SSL VPN English login message Welcome in context ctx1.
Explanation	A login welcome message was configured in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_LOGINMESSAGE_FAILED

Message text	Failed to configure SSL VPN [STRING] login message [STRING] in context [STRING]
Variable fields	$1: Language used on the login page, English or Chinese. $2: Login welcome message on the login page. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_LOGINMESSAGE_FAILED: Failed to configure SSL VPN English login message Welcome in context ctx1.
Explanation	Failed to configure the login welcome message in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_LOGO

Message text	Configured SSL VPN logo [STRING] [STRING] in context [STRING].
Variable fields	$1: If a logo is configured, this field displays **file**. If no logo is configured, this field displays **none**. $2: Log file name. This field is not displayed if the $1 field displays **none**. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_LOGO: Configured SSL VPN logo file 1.jpg in context ctx1. • SSLVPN/6/SSLVPN_CFG_LOGO: Configured SSL VPN logo none in context ctx1.
Explanation	A logo to be displayed on SSL VPN webpages was specified.
Recommended action	No action is required.

SSLVPN_CFG_LOGO_FAILED

Message text	Failed to configure SSL VPN logo [STRING] [STRING] in context [STRING]
Variable fields	$1: If a logo is configured, this field displays **file**. If no logo is configured, this field displays **none**. $2: Log file name. This field is not displayed if $1 displays **none**. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_LOGO_FAILED: Failed to configure SSL VPN logo file 1.jpg in context ctx1. • SSLVPN/6/SSLVPN_CFG_LOGO_FAILED: Failed to configure SSL VPN logo none in context ctx1.
Explanation	Failed to specify a logo to be displayed on SSL VPN webpages.
Recommended action	Verify that the size of the logo file does not exceed the maximum file size limit.

SSLVPN_CFG_MAXONLINES

Message text	Set the maximum number of concurrent connections to [STRING] for each SSL VPN user in context [STRING].
Variable fields	$1: Maximum number of concurrent connections for each SSL VPN user. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_MAXONLINES: Set the maximum number of concurrent connections to 50 for each SSL VPN user in context ctx1.
Explanation	The maximum number of concurrent connections for each SSL VPN user was set in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_MAXONLINES_FAILED

Message text	Failed to set maximum number of concurrent connections to [STRING] for each SSL VPN user in context [STRING].
Variable fields	$1: Maximum concurrent connections for each SSL VPN user. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_MAXONLINES_FAILED: Failed to set maximum number of concurrent connections to 50 for each SSL VPN user in context ctx1.
Explanation	Failed to set the maximum number of concurrent connections for each SSL VPN user in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_MAXUSERS

Message text	Set the maximum number of sessions to [STRING] in context [STRING].
Variable fields	$1: Maximum number of sessions supported in an SSL VPN context. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_MAXUSERS: Set the maximum number of sessions to 500 in context ctx1.
Explanation	The maximum number of supported sessions was set in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_MAXUSERS_FAILED

Message text	Failed to set maximum number of sessions to [STRING] in context [STRING]
Variable fields	$1: Maximum number of sessions supported in an SSL VPN context. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_MAXUSERS_FAILED: Failed to set maximum number of sessions to 500 in context ctx1.
Explanation	Failed to set the maximum number of supported sessions in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_MSGSERVER

Message text	Specified message server address [STRING] and port [STRING] in context [STRING].
Variable fields	$1: Host name or IPv4 address of the message server. $2: Port number of the message server. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_MSGSERVER: Specified message server address 10.10.1.1 and port 8000 in context ctx1. • SSLVPN/6/SSLVPN_CFG_MSGSERVER: Specified message server address host and port 8000 in context ctx1.
Explanation	A message server was specified for mobile clients in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_MSGSERVER_FAILED

Message text	Failed to specify message server address [STRING] and port [STRING] in context [STRING]
Variable fields	$1: Host name or IPv4 address of the message server. $2: Port number of the message server. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_MSGSERVER_FAILED: Failed to specify message server address 10.10.1.1 and port 8000 in context ctx1. • SSLVPN/6/SSLVPN_CFG_MSGSERVER_FAILED: Failed to specify message server address host and port 8000 in context ctx1.
Explanation	Failed to specify a message server for mobile clients in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_PFWDEXECUTION

Message text	Configured script [STRING] for port forwarding item [STRING] in context [STRING].
Variable fields	$1: Script of the resource for a port forwarding item. $2: Port forwarding item name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_PFWDEXECUTION: Configured script url('http://127.0.0.1') for port forwarding item pfitem1 in context ctx.
Explanation	A resource was configured for a port forwarding item.
Recommended action	No action is required.

SSLVPN_CFG_PFWDEXECUTION_FAILED

Message text	Failed to configure script [STRING] for port forwarding item [STRING] in context [STRING].
Variable fields	$1: Script of the resource for a port forwarding item. $2: Port forwarding item name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_PFWDEXECUTION_FAILED: Failed to configure script url('http://127.0.0.1') for port forwarding item pfitem1 in context ctx.
Explanation	Failed to configure a resource path for a port forwarding item.
Recommended action	No action is required.

SSLVPN_CFG_SCUTEXECUTION

Message text	Configured script [STRING] for shortcut [STRING] in context [STRING].
Variable fields	$1: Script of the resource associated with a shortcut. $2: Shortcut name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_SCUTEXECUTION: Configured script url('http://10.0.0.1') for shortcut shortcut1 in context ctx.
Explanation	A resource was associated with a shortcut.
Recommended action	No action is required.

SSLVPN_CFG_SCUTEXECUTION_FAILED

Message text	Failed to configure script [STRING] for shortcut [STRING] in context [STRING].
Variable fields	$1: Script of the resource associated with a shortcut. $2: Shortcut name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_SCUTEXECUTION_FAILED: Failed to configure script url('http://10.0.0.1') for shortcut shortcut1 in context ctx.
Explanation	Failed to associate a resource with a shortcut.
Recommended action	No action is required.

SSLVPN_CFG_SHORTCUTDESC

Message text	Configured description [STRING] for shortcut [STRING] in context [STRING].
Variable fields	$1: Description of a shortcut. $2: Shortcut name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_SHORTCUTDESC: Configured description shortcut shortcut1 for shortcut shortcut1 in context ctx.
Explanation	A description was configured for a shortcut.
Recommended action	No action is required.

SSLVPN_CFG_SHORTCUTDESC_FAILED

Message text	Failed to configure description [STRING] for shortcut [STRING] in context [STRING].
Variable fields	$1: Description of a shortcut. $2: Shortcut name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_SHORTCUTDESC_FAILED: Failed to configure description shortcut shortcut1 for shortcut shortcut1 in context ctx.
Explanation	Failed to configure a description for a shortcut.
Recommended action	No action is required.

SSLVPN_CFG_SSLCLIENT

Message text	Specified SSL client policy [STRING] for context [STRING].
Variable fields	$1: SSL client policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_SSLCLIENT: Specified SSL client policy ssl for context ctx1.
Explanation	An SSL client policy was specified for an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_SSLCLIENT_FAILED

Message text	Failed to specify SSL client policy [STRING] for context [STRING].
Variable fields	$1: SSL client policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_SSLCLIENT_FAILED: Failed to specify SSL client policy ssl for context ctx1.
Explanation	Failed to specify an SSL client policy for an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_SSLSERVER

Message text	Specified SSL server policy [STRING] for gateway [STRING].
Variable fields	$1: SSL server policy name. $2: Name of the SSL VPN gateway.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_SSLSERVER: Specified SSL server policy ssl for gateway gw1.
Explanation	An SSL server policy was specified for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CFG_SSLSERVER_FAILED

Message text	Failed to specify SSL server policy [STRING] for gateway [STRING]
Variable fields	$1: SSL server policy name. $2: Name of the SSL VPN gateway.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_SSLSERVER_FAILED: Failed to specify SSL server policy ssl for gateway gw1.
Explanation	Failed to specify an SSL server policy for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CFG_TIMEOUTIDLE

Message text	Configured session idle timeout to [STRING] minutes in context [STRING].
Variable fields	$1: Idle timeout timer for SSL VPN sessions. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_TIMEOUTIDLE: Configured session idle timeout to 50 minutes in context ctx1.
Explanation	The idle timeout timer for SSL VPN sessions was set in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_TIMEOUTIDLE_FAILED

Message text	Failed to configure session idle timeout to [STRING] minutes in context [STRING]
Variable fields	$1: Idle timeout timer for SSL VPN sessions. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_TIMEOUTIDLE_FAILED: Failed to configure session idle timeout to 50 minutes in context ctx1.
Explanation	Failed to set the idle timeout timer for SSL VPN sessions in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_TITLE

Message text	Configured SSL VPN page [STRING] title [STRING] in context [STRING].
Variable fields	$1: Language used on the login page, English or Chinese. $2: Title displayed on SSL VPN webpages. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_TITLE: Configured SSL VPN page English title Mytitle in context ctx1.
Explanation	The title to be displayed on SSL VPN webpages was configured in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_TITLE_FAILED

Message text	Failed to configure SSL VPN page [STRING] title [STRING] in context [STRING]
Variable fields	$1: Language used on the login page, English or Chinese. $2: Title displayed on SSL VPN webpages. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_TITLE_FAILED: Failed to configure SSL VPN page English title Mytitle in context ctx1.
Explanation	Failed to configure the title to be displayed on SSL VPN webpages in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_TRAFFICTHRESHOLD

Message text	Set the idle-cut traffic threshold to [STRING] Kilobytes in context [STRING].
Variable fields	$1: Idle-cut traffic threshold value. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_TRAFFICTHRESHOLD: Set the idle-cut traffic threshold to 100 Kilobytes in context ctx1.
Explanation	The SSL VPN session idle-cut traffic threshold was set in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_TRAFFICTHRESHOLD_FAIL

Message text	Failed to set the idle-cut traffic threshold to [STRING] Kilobytes in context [STRING].
Variable fields	$1: Idle-cut traffic threshold value. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_TRAFFICTHRESHOLD_FAIL: Failed to set the idle-cut traffic threshold to 100 Kilobytes in context ctx1.
Explanation	Failed to set the SSL VPN session idle-cut traffic threshold in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_URLLISTHEAD

Message text	Configured heading [STRING] for URL-list [STRING] in context [STRING].
Variable fields	$1: URL list heading name. $2: URL list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_URLLISTHEAD: Configured heading urlhead for URL-list urllist in context ctx1.
Explanation	A heading was configured for a URL list.
Recommended action	No action is required.

SSLVPN_CFG_URLLISTHEAD_FAILED

Message text	Failed to configure heading [STRING] for URL-list [STRING] in context [STRING]
Variable fields	$1: URL list heading name. $2: URL list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CFG_URLLISTHEAD_FAILED: Failed to configure heading urlhead for URL-list urllist in context ctx1.
Explanation	Failed to configure a heading for a URL list.
Recommended action	No action is required.

SSLVPN_CFG_WINSSERVER

Message text	Specified [STRING] WINS server [STRING] in context [STRING].
Variable fields	$1: WINS server type, primary or secondary. $2: IPv4 address of the WINS server. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_WINSSERVER: Specified primary WINS server primary 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CFG_WINSSERVER: Specified secondary WINS server secondary 1.1.1.2 in context ctx.
Explanation	A WIN server for IP access was specified in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CFG_WINSSERVER_FAILED

Message text	Failed to specify [STRING] WINS server [STRING] in context [STRING]
Variable fields	$1: WINS server type, primary or secondary. $2: IPv4 address of the WINS server. $3: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CFG_WINSSERVER_FAILED: Failed to specify primary WINS server 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CFG_WINSSERVER_FAILED: Failed to specify secondary WINS server 1.1.1.2 in context ctx.
Explanation	Failed to specify a WINS server for IP access in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_AAADOMAIN

Message text	Deleted the AAA domain specified for context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_AAADOMAIN: Deleted the AAA domain specified for context ctx1.
Explanation	The ISP domain configuration was removed from an SSL VPN context. The SSL VPN context will use the default ISP domain for authentication, authorization, and accounting of SSL VPN users.
Recommended action	No action is required.

SSLVPN_CLR_AAADOMAIN_FAILED

Message text	Failed to delete the AAA domain specified for context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_AAADOMAIN_FAILED: Failed to delete the AAA domain specified for context ctx1.
Explanation	Failed to remove the ISP domain configuration from an SSL VPN context. The SSL VPN context still uses the specified ISP domain for authentication, authorization, and accounting of SSL VPN users.
Recommended action	No action is required.

SSLVPN_CLR_AUTHMODE

Message text	Configured authentication use all in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_AUTHMODE: Configured authentication use all in context 2.
Explanation	The authentication mode of an SSL VPN context was set to all. A user must pass all enabled authentication methods to log in to the SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_AUTHMODE_FAILED

Message text	Failed to configure authentication use all in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_AUTHMODE_FAILED: Failed to configure authentication use all in context 2.
Explanation	Failed to specify the authentication mode of an SSL VPN context as **all**, which indicates that a user must pass all enabled authentication methods to log in to the SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_BINDIP

Message text	Deleted IP address binding configuration for user [STRING] in context [STRING].
Variable fields	$1: SSL VPN username. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_BINDIP: Deleted IP address binding configuration for user user1 in context ctx1.
Explanation	The IP address binding configuration was deleted for an SSL VPN user.
Recommended action	No action is required.

SSLVPN_CLR_BINDIP_FAILED

Message text	Failed to delete IP address binding configuration for user [STRING] in context [STRING].
Variable fields	$1: SSL VPN username. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_BINDIP_FAILED: Failed to delete IP address binding configuration for user user1 in context ctx1.
Explanation	Failed to delete the IP address binding configuration for an SSL VPN user.
Recommended action	No action is required.

SSLVPN_CLR_CERTATTRIBUTE

Message text	Specified the attribute cn as the certificate user name in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_CERTATTRIBUTE: Specified the attribute cn as the certificate user name in context ctx1.
Explanation	The CN attribute of the certificate was specified as the SSL VPN username.
Recommended action	No action is required.

SSLVPN_CLR_CERTATTRIBUTE_FAILED

Message text	Failed to specify the attribute cn as the certificate user name in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_CERTATTRIBUTE_FAILED: Failed to specify the attribute cn as the certificate user name in context ctx1.
Explanation	Failed to specify the CN attribute of the certificate as the SSL VPN username.
Recommended action	No action is required.

SSLVPN_CLR_CONTEXT_USERMAX

Message text	Deleted the maximum number of SSL VPN users in context [UINT32].
Variable fields	$1: Context ID.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_CONTEXT_USERMAX: Deleted the maximum number of SSL VPN users in context 2.
Explanation	The maximum number of SSL VPN users configuration was removed from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_CONTEXT_USERMAX_FAILED

Message text	Failed to delete the maximum number of SSL VPN users in context [UINT32].
Variable fields	$1: Context ID.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_CONTEXT_USERMAX_FAILED: Failed to delete the maximum number of SSL VPN users in context 2.
Explanation	Failed to remove the maximum number of SSL VPN users configuration from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_CONTEXTVPN

Message text	Deleted the associated VPN instance in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_CONTEXTVPN: Deleted the associated VPN instance in context ctx1.
Explanation	The association between an SSL VPN context and a VPN instance was removed.
Recommended action	No action is required.

SSLVPN_CLR_CONTEXTVPN_FAILED

Message text	Failed to delete the associated VPN instance in context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_CONTEXTVPN_FAILED: Failed to delete the associated VPN instance in context ctx1.
Explanation	Failed to remove the association between an SSL VPN context and a VPN instance.
Recommended action	No action is required.

SSLVPN_CLR_CTXGATEWAY

Message text	Deleted gateway in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_CTXGATEWAY: Deleted gateway in context ctx1.
Explanation	An SSL VPN gateway was deleted.
Recommended action	No action is required.

SSLVPN_CLR_CTXGATEWAY_FAILED

Message text	Failed to delete gateway in context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_CTXGATEWAY_FAILED: Failed to delete gateway in context ctx1.
Explanation	Failed to delete an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CLR_DEFAULT_PGROUP

Message text	Deleted default-policy-group in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_DEFAULT_PGROUP: Deleted default-policy-group in context ctx1.
Explanation	The default policy group configuration was removed from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_DEFAULT_PGROUP_FAILED

Message text	Failed to delete default-policy-group in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_DEFAULT_PGROUP_FAILED: Failed to delete default-policy-group in context ctx1.
Explanation	Failed to remove the default policy group configuration from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_DNSSERVER

Message text	Deleted [STRING] DNS server in context [STRING].
Variable fields	$1: DNS server type, primary or secondary. $2: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CLR_DNSSERVER: Deleted primary DNS server in context ctx. • SSLVPN/6/SSLVPN_CLR_DNSSERVER: Deleted secondary DNS server in context ctx.
Explanation	The DNS server configuration was removed from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_DNSSERVER_FAILED

Message text	Failed to delete [STRING] DNS server in context [STRING]
Variable fields	$1: DNS server type, primary or secondary. $2: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CLR_DNSSERVER_FAILED: Failed to delete primary DNS server in context ctx. • SSLVPN/6/SSLVPN_CLR_DNSSERVER_FAILED: Failed to delete secondary DNS server in context ctx.
Explanation	Failed to remove the DNS server configuration from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_EMOSERVER

Message text	Deleted EMO server in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_EMOSERVER: Deleted emo-server in context ctx1.
Explanation	The Endpoint Mobile Office (EMO) server configuration was removed from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_EMOSERVER_FAILED

Message text	Failed to delete EMO server in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_EMOSERVER_FAILED: Failed to delete EMO server in context ctx1.
Explanation	Failed to remove the Endpoint Mobile Office (EMO) server configuration from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_GATEWAYVPN

Message text	Deleted VPN instance for gateway [STRING].
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_GATEWAYVPN: Deleted VPN instance for gateway gw1.
Explanation	The VPN instance configuration was removed for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CLR_GATEWAYVPN_FAILED

Message text	Failed to delete VPN instance for gateway [STRING].
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_GATEWAYVPN_FAILED: Failed to delete VPN instance for gateway gw1.
Explanation	Failed to remove the VPN instance configuration for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CLR_GWIPADDRESS

Message text	Deleted IP address of gateway [STRING].
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_GWIPADDRESS: Deleted IP address of gateway gw1.
Explanation	The IP address of an SSL VPN gateway was deleted.
Recommended action	No action is required.

SSLVPN_CLR_GWIPADDRESS_FAILED

Message text	Failed to delete IP address of gateway [STRING]
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_GWIPADDRESS_FAILED: Failed to delete IP address of gateway gw1.
Explanation	Failed to delete the IP address of an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CLR_GWIPV6ADDRESS

Message text	Deleted IPv6 address of gateway [STRING].
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_GWIPV6ADDRESS: Deleted IPv6 address of gateway gw1.
Explanation	The IPv6 address of an SSL VPN gateway was deleted.
Recommended action	No action is required.

SSLVPN_CLR_GWIPV6ADDRESS_FAILED

Message text	Failed to delete IPv6 address of gateway [STRING]
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_GWIPV6ADDRESS_FAILED: Failed to delete IPv6 address of gateway gw1.
Explanation	Failed to delete the IPv6 address of an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CLR_HTTPREDIRECT

Message text	Disabled HTTP-redirect in gateway [STRING].
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_HTTPREDIRECT: Disabled HTTP-redirect in gateway gw.
Explanation	HTTP redirection was disabled for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CLR_HTTPREDIRECT_FAILED

Message text	Failed to disable HTTP-redirect in gateway [STRING]
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_HTTPREDIRECT_FAILED: Failed to disable HTTP-redirect in gateway gw.
Explanation	Failed to disable HTTP redirection for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CLR_IMCADDRESS

Message text	Deleted the IP address of the iMC server in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_IMCADDRESS: Deleted the IP address of the iMC server in context ctx1.
Explanation	The IMC server configuration for SMS message authentication was removed from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_IMCADDRESS_FAILED

Message text	Failed to delete the IP address of the iMC server in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_IMCADDRESS_FAILED: Failed to delete the IP address of the iMC server in context ctx1.
Explanation	Failed to remove the IMC server configuration for SMS message authentication from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_IPAC_WEBRESPUSH

Message text	Disabled automatic pushing of Web resources after IP access client login in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_IPAC_WEBRESPUSH: Disabled automatic pushing of Web resources after IP access client login in context ctx.
Explanation	Disabled automatic webpage pushing of accessible resources after IP access client login in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_IPAC_WEBRESPUSH_FAIL

Message text	Failed to disable automatic pushing of Web resources after IP access client login in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_IPAC_WEBRESPUSH_FAIL: Failed to disable automatic pushing of Web resources after IP access client login in context ctx.
Explanation	Failed to disable automatic webpage pushing of accessible resources after IP access client login in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_IPCLIENT_AUTOACT

Message text	Disabled automatic IP access client startup after Web login in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_IPCLIENT_AUTOACT: Disabled automatic IP access client startup after Web login in context ctx.
Explanation	Disabled automatic IP access client startup after Web login in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_IPCLIENT_AUTOACT_FAIL

Message text	Failed to disable automatic IP access client startup after Web login in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_IPCLIENT_AUTOACT_FAIL: Failed to disable automatic IP access client startup after Web login in context ctx.
Explanation	Failed to disable automatic IP access client startup after Web login in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_IPTNL_RATE-LIMIT

Message text	Deleted the rate limit configuration for IP tunnel [STRING] traffic in context [STRING].
Variable fields	$1: SSL VPN IP access traffic direction: • Upstream. • Downstream. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_IPTNL_RATE-LIMIT: Deleted the rate limit configuration for IP tunnel upstream traffic in context ctx. SSLVPN/6/SSLVPN_CLR_IPTNL_RATE-LIMIT: Deleted the rate limit configuration for IP tunnel downstream traffic in context ctx.
Explanation	Deleted the rate limit setting for IP access upstream or downstream traffic.
Recommended action	No action is required.

SSLVPN_CLR_IPTNL_RATE-LIMIT_FAIL

Message text	Failed to delete the rate limit configuration for IP tunnel [STRING] traffic in context [STRING].
Variable fields	$1: SSL VPN IP access traffic direction: • Upstream. • Downstream. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_IPTNL_RATE-LIMIT_FAIL: Failed to delete the rate limit configuration for IP tunnel upstream traffic in context ctx. SSLVPN/6/SSLVPN_CLR_IPTNL_RATE-LIMIT_FAIL: Failed to delete the rate limit configuration for IP tunnel downstream traffic in context ctx.
Explanation	Failed to delete the rate limit setting for IP access upstream or downstream traffic.
Recommended action	No action is required.

SSLVPN_CLR_IPTUNNELPOOL

Message text	Deleted address-pool in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_IPTUNNELPOOL: Deleted address-pool in context ctx.
Explanation	The IP access address pool configuration was removed from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_IPTUNNELPOOL_FAILED

Message text	Failed to delete address-pool in context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_IPTUNNELPOOL_FAILED: Failed to delete address-pool in context ctx.
Explanation	Failed to remove the IP access address pool configuration from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_LOCALPORT

Message text	Deleted the port forwarding instance used by port forwarding item [STRING] in context [STRING].
Variable fields	$1: Port forwarding item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_LOCALPORT: Deleted the port forwarding instance used by port forwarding item pfitem1 in context ctx.
Explanation	The port forwarding instance used by a port forwarding item was deleted.
Recommended action	No action is required.

SSLVPN_CLR_LOCALPORT_FAILED

Message text	Failed to delete the port forwarding instance used by port forwarding item [STRING] in context [STRING]
Variable fields	$1: Port forwarding item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_LOCALPORT_FAILED: Failed to delete the port forwarding instance used by port forwarding item pfitem1 in context ctx.
Explanation	Failed to delete the port forwarding instance used by a port forwarding item.
Recommended action	No action is required.

SSLVPN_CLR_LOGO

Message text	Configured SSL VPN logo NSFOCUS in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_LOGO: Configured SSL VPN logo NSFOCUS in context ctx1.
Explanation	The logo to be displayed on SSL VPN webpages was set to NSFOCUS.
Recommended action	No action is required.

SSLVPN_CLR_LOGO_FAILED

Message text	Failed to configure SSL VPN logo NSFOCUS in context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_LOGO_FAILED: Failed to configure SSL VPN logo NSFOCUS in context ctx1.
Explanation	Failed to set the logo to be displayed on SSL VPN webpages to NSFOCUS.
Recommended action	No action is required.

SSLVPN_CLR_MSGSERVER

Message text	Deleted message server in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_MSGSERVER: Deleted message server in context ctx1.
Explanation	The message server configuration was removed from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_MSGSERVER_FAILED

Message text	Failed to delete message server in context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_MSGSERVER_FAILED: Failed to delete message server in context ctx1.
Explanation	Failed to remove the message server configuration from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_PFWDEXECUTION

Message text	Deleted the script for port forwarding item [STRING] in context [STRING].
Variable fields	$1: Port forwarding item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_PFWDEXECUTION: Deleted the script for port forwarding item pfitem1 in context ctx.
Explanation	The resource specified for a port forwarding item was deleted.
Recommended action	No action is required.

SSLVPN_CLR_PFWDEXECUTION_FAILED

Message text	Failed to delete the script for port forwarding item [STRING] in context [STRING].
Variable fields	$1: Port forwarding item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_PFWDEXECUTION_FAILED: Failed to delete the script for port forwarding item pfitem1 in context ctx.
Explanation	Failed to delete the resource specified for a port forwarding item.
Recommended action	No action is required.

SSLVPN_CLR_SCUTDESCRIPTION

Message text	Deleted the description for shortcut [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_SCUTDESCRIPTION: Deleted the description for shortcut shortcut1 in context ctx.
Explanation	The description configured for shortcut was deleted.
Recommended action	No action is required.

SSLVPN_CLR_SCUTDESCRIPTION_FAILED

Message text	Failed to delete the description for shortcut [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_SCUTDESCRIPTION_FAILED: Failed to delete the description for shortcut shortcut1 in context ctx.
Explanation	Failed to delete the description configured for a shortcut.
Recommended action	No action is required.

SSLVPN_CLR_SCUTEXECUTION

Message text	Deleted the script for shortcut [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_SCUTEXECUTION: Deleted the script for shortcut shortcut1 in context ctx.
Explanation	The association between a resource and a shortcut was deleted.
Recommended action	No action is required.

SSLVPN_CLR_SCUTEXECUTION_FAILED

Message text	Failed to delete the script for shortcut [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_SCUTEXECUTION_FAILED: Failed to delete the script for shortcut shortcut1 in context ctx.
Explanation	Failed to delete the association between a resource and a shortcut.
Recommended action	No action is required.

SSLVPN_CLR_SSLCLIENT

Message text	Deleted the SSL client policy specified for context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_SSLCLIENT: Deleted the SSL client policy specified for context ctx1.
Explanation	The SSL client policy configuration was removed from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_SSLCLIENT_FAILED

Message text	Failed to delete SSL client policy for context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_SSLCLIENT_FAILED: Failed to delete SSL client policy for context ctx1.
Explanation	Failed to remove the SSL client policy configuration from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_SSLSERVER

Message text	Deleted the SSL server policy specified for gateway [STRING].
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_SSLSERVER: Deleted the SSL server policy specified for gateway gw1.
Explanation	The SSL server policy configuration was removed for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CLR_SSLSERVER_FAILED

Message text	Failed to delete SSL server policy for gateway [STRING]
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_SSLSERVER_FAILED: Failed to delete SSL server policy for gateway gw1.
Explanation	Failed to remove the SSL server policy configuration for an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_CLR_TRAFFICTHRESHOLD

Message text	Deleted the idle-cut traffic threshold in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_TRAFFICTHRESHOLD: Deleted the idle-cut traffic threshold in context ctx1.
Explanation	Removed the SSL VPN session idle-cut traffic threshold setting in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_TRAFFICTHRESHOLD_FAIL

Message text	Failed to delete the idle-cut traffic threshold in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_CLR_TRAFFICTHRESHOLD_FAIL: Failed to delete the idle-cut traffic threshold in context ctx1.
Explanation	Failed to remove the SSL VPN session idle-cut traffic threshold setting in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_WINSSERVER

Message text	Deleted [STRING] WINS server in context [STRING].
Variable fields	$1: WINS server type, primary or secondary. $2: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CLR_WINSSERVER: Deleted primary WINS server 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CLR_WINSSERVER: Deleted secondary WINS server 1.1.1.2 in context ctx.
Explanation	The WINS server configuration was removed from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_CLR_WINSSERVER_FAILED

Message text	Failed to delete [STRING] WINS server in context [STRING]
Variable fields	$1: WINS server type, primary or secondary. $2: SSL VPN context name.
Severity level	6
Example	• SSLVPN/6/SSLVPN_CLR_WINSSERVER_FAILED: Failed to delete primary WINS server 1.1.1.1 in context ctx. • SSLVPN/6/SSLVPN_CLR_WINSSERVER_FAILED: Failed to delete secondary WINS server 1.1.1.2 in context ctx.
Explanation	Failed to remove the WINS server configuration from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_CONTENT_TYPE

Message text	Deleted the content type configuration for file policy [STRING] in context [STRING].
Variable fields	$1: File policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_CONTENT_TYPE: Deleted the content type configuration for file policy fp1 in context ctx1.
Explanation	The content type configuration was deleted for a file policy.
Recommended action	No action is required.

SSLVPN_DEL_CONTENT_TYPE_FAILED

Message text	Failed to delete the content type configuration for file policy [STRING] in context [STRING].
Variable fields	$1: File policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_CONTENT_TYPE_FAILED: Failed to delete the content type configuration for file policy fp1 in context ctx1.
Explanation	Failed to delete the content type configuration for a file policy.
Recommended action	No action is required.

SSLVPN_DEL_CONTEXT

Message text	Deleted SSL VPN context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_CONTEXT: Deleted SSL VPN context ctx1.
Explanation	An SSL VPN context was deleted.
Recommended action	No action is required.

SSLVPN_DEL_CONTEXT_FAILED

Message text	Failed to delete SSL VPN context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_CONTEXT_FAILED: Failed to delete SSL VPN context ctx1.
Explanation	Failed to delete an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_EXCROUTEITEM

Message text	Deleted exclude route (IP [STRING] mask [STRING]) from route list [STRING] in context [STRING].
Variable fields	$1: Destination IP address of the route. $2: Subnet mask of the route. $3: Route list name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_EXCROUTEITEM: Deleted exclude route (IP 10.0.0.0 mask 255.0.0.0) from route list rtlist in context ctx1.
Explanation	An exclude route was removed from a route list configured in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_EXCROUTEITEM_FAILED

Message text	Failed to delete exclude route (IP [STRING] mask [STRING]) from route list [STRING] in context [STRING]
Variable fields	$1: Destination IP address of the route. $2: Subnet mask of the route. $3: Route list name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_EXCROUTEITEM_FAILED: Failed to delete exclude route (IP 10.0.0.0 mask 255.0.0.0) from route list rtlist in context ctx1.
Explanation	Failed to remove an exclude route from a route list configured in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_FILEPOLICY

Message text	Deleted file policy [STRING] in context [STRING].
Variable fields	$1: File policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_FILEPOLICY: Deleted file policy fp1 in context ctx1.
Explanation	A file policy was deleted.
Recommended action	No action is required.

SSLVPN_DEL_FILEPOLICY_FAILED

Message text	Failed to delete file policy [STRING] in context [STRING].
Variable fields	$1: File policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_FILEPOLICY_FAILED: Failed to delete file policy fp1 in context ctx1.
Explanation	Failed to delete a file policy.
Recommended action	No action is required.

SSLVPN_DEL_GATEWAY

Message text	Deleted SSL VPN gateway [STRING].
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_GATEWAY: Deleted SSL VPN gateway gw1.
Explanation	An SSL VPN gateway was deleted.
Recommended action	No action is required.

SSLVPN_DEL_GATEWAY_FAILED

Message text	Failed to delete SSL VPN gateway [STRING]
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_GATEWAY_FAILED: Failed to delete SSL VPN gateway gw1.
Explanation	Failed to delete an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_DEL_INCROUTEITEM

Message text	Deleted inlcude route (IP [STRING] mask [STRING]) from route list [STRING] in context [STRING].
Variable fields	$1: Destination IP address of the route. $2: Subnet mask of the route. $3: Route list name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_INCROUTEITEM: Deleted include route (IP 10.0.0.0 mask 255.0.0.0) from route list rtlist in context ctx1.
Explanation	An include route was removed from a route list configured in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_INCROUTEITEM_FAILED

Message text	Failed to delete include route (IP [STRING] mask [STRING]) from route list [STRING] in context [STRING]
Variable fields	$1: Destination IP address of the route. $2: Subnet mask of the route. $3: Route list name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_INCROUTEITEM_FAILED: Failed to delete include route (IP 10.0.0.0 mask 255.0.0.0) from route list rtlist in context ctx1.
Explanation	Failed to remove an include route from a route list configured in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_IPADDRESSPOOL

Message text	Deleted IP address pool [STRING].
Variable fields	$1: Name of the IP address pool.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_IPADDRESSPOOL: Deleted IP address pool pool1.
Explanation	An address pool was deleted.
Recommended action	No action is required.

SSLVPN_DEL_IPADDRESSPOOL_FAILED

Message text	Failed to delete IP address pool [STRING]
Variable fields	$1: Name of the IP address pool.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_IPADDRESSPOOL_FAILED: Failed to delete IP address pool pool1.
Explanation	Failed to delete an address pool.
Recommended action	No action is required.

SSLVPN_DEL_IPTUNNELACIF

Message text	Deleted SSL VPN AC interface in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_IPTUNNELACIF: Deleted SSL VPN AC interface in context ctx.
Explanation	The SSL VPN AC interface configuration for IP access was removed from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_IPTUNNELACIF_FAILED

Message text	Failed to delete SSL VPN AC interface in context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_IPTUNNELACIF_FAILED: Failed to delete SSL VPN AC interface in context ctx.
Explanation	Failed to remove the SSL VPN AC interface configuration for IP access from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_IPV4_RANGE

Message text	Deleted the IPv4 address range of SNAT pool [STRING].
Variable fields	$1: SNAT address pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_IPV4_RANGE: Deleted IPv4 address range of SNAT pool sp1.
Explanation	The IPv4 address range configuration was removed for an SSL VPN SNAT address pool.
Recommended action	No action is required.

SSLVPN_DEL_IPV4_RANGE_FAILED

Message text	Failed to delete the IPv4 address range of SNAT pool [STRING].
Variable fields	$1: SNAT address pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_IPV4_RANGE_FAILED: Failed to delete IPv4 address range of SNAT pool sp1.
Explanation	Failed to remove the IPv4 address range configuration for an SSL VPN SNAT address pool.
Recommended action	No action is required.

SSLVPN_DEL_IPV6_RANGE

Message text	Deleted IPv6 address range of SNAT pool [STRING].
Variable fields	$1: SNAT pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_IPV6_RANGE: Deleted IPv6 address range of SNAT pool sp1.
Explanation	The IPv6 address range configuration was removed for an SSL VPN SNAT address pool.
Recommended action	No action is required.

SSLVPN_DEL_IPV6_RANGE_FAILED

Message text	Failed to delete IPv6 address range of SNAT pool [STRING].
Variable fields	$1: SNAT pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_IPV6_RANGE_FAILED: Failed to delete IPv6 address range of SNAT pool sp1.
Explanation	Failed to remove the IPv6 address range configuration for an SSL VPN SNAT address pool.
Recommended action	No action is required.

SSLVPN_DEL_LOCALPORT

Message text	Deleted port forwarding entry local-port [STRING] local-name [STRING] in port forwarding list [STRING] in context [STRING].
Variable fields	$1: Local port number. $2: Local address or local host name. $3: Port forwarding list name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_LOCALPORT: Deleted port forwarding entry local-port 80 local-name 127.0.0.1 in port forwarding list pflist1 in context ctx.
Explanation	A port forwarding entry was deleted from a port forwarding list.
Recommended action	No action is required.

SSLVPN_DEL_LOCALPORT_FAILED

Message text	Failed to delete port forwarding entry local-port [STRING] local-name [STRING] in port forwarding list [STRING] in context [STRING]
Variable fields	$1: Local port number. $2: Local address or local host name. $3: Port forwarding list name. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_LOCALPORT_FAILED: Failed to delete port forwarding entry local-port 80 local-name 127.0.0.1 in port forwarding list pflist1 in context ctx.
Explanation	Failed to delete a port forwarding entry from a port forwarding list.
Recommended action	No action is required.

SSLVPN_DEL_NEWCONTENT

Message text	Deleted the new content configuration for rewrite rule [STRING] in file policy [STRING] in context [STRING].
Variable fields	$1: Rewrite rule name. $2: File policy name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_NEWCONTENT: Deleted the new content configuration for rewrite rule rw in file policy fp in context ctx.
Explanation	The new content configuration was deleted for a rewrite rule.
Recommended action	No action is required.

SSLVPN_DEL_NEWCONTENT_FAILED

Message text	Failed to delete the new content configuration for rewrite rule [STRING] in file policy [STRING] in context [STRING].
Variable fields	$1: Rewrite rule name. $2: File policy name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_NEWCONTENT_FAILED: Failed to delete the new content configuration for rewrite rule rw in file policy fp in context ctx.
Explanation	Failed to delete the new content configuration for a rewrite rule.
Recommended action	No action is required.

SSLVPN_DEL_OLDCONTENT

Message text	Deleted the old content configuration for rewrite rule [STRING] in file policy [STRING] in context [STRING].
Variable fields	$1: Rewrite rule name. $2: File policy name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_OLDCONTENT: Deleted the old content configuration for rewrite rule rw in file policy fp in context ctx.
Explanation	The old content configuration was deleted for a rewrite rule.
Recommended action	No action is required.

SSLVPN_DEL_OLDCONTENT_FAILED

Message text	Failed to delete the old content configuration for rewrite rule [STRING] in file policy [STRING] in context [STRING].
Variable fields	$1: Rewrite rule name. $2: File policy name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_OLDCONTENT_FAILED: Failed to delete the old content configuration for rewrite rule rw in file policy fp in context ctx.
Explanation	Failed to delete the old content configuration for a rewrite rule.
Recommended action	No action is required.

SSLVPN_DEL_PORTFWD

Message text	Deleted port forwarding list [STRING] in context [STRING].
Variable fields	$1: Port forwarding list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_PORTFWD: Deleted port forwarding list pf in context ctx1.
Explanation	A port forwarding list was deleted from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_PORTFWD_FAILED

Message text	Failed to delete port forwarding list [STRING] in context [STRING]
Variable fields	$1: Port forwarding list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_PORTFWD_FAILED: Failed to delete port forwarding list pf in context ctx1.
Explanation	Failed to delete a port forwarding list from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_PORTFWD_ITEM

Message text	Deleted port forwarding item [STRING] in context [STRING].
Variable fields	$1: Port forwarding item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_PORTFWD_ITEM: Deleted port forwarding item pfitem in context ctx1.
Explanation	A port forwarding item was deleted.
Recommended action	No action is required.

SSLVPN_DEL_PORTFWD_ITEM_FAILED

Message text	Failed to delete port forwarding item [STRING] in context [STRING]
Variable fields	$1: Port forwarding item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_PORTFWD_ITEM_FAILED: Failed to delete port forwarding item pfitem in context ctx1.
Explanation	Failed to delete a port forwarding item.
Recommended action	No action is required.

SSLVPN_DEL_PYGROUP

Message text	Deleted policy group [STRING] in context [STRING].
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_PYGROUP: Deleted policy group pg in context ctx1.
Explanation	An SSL VPN policy group was deleted.
Recommended action	No action is required.

SSLVPN_DEL_PYGROUP_FAILED

Message text	Failed to delete policy group [STRING] in context [STRING]
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_PYGROUP_FAILED: Failed to delete policy group pg in context ctx1.
Explanation	Failed to delete an SSL VPN policy group.
Recommended action	Verify that the policy group is not being used by SSL VPN users.

SSLVPN_DEL_REFERIPACL

Message text	Deleted IP access filter in policy group [STRING] in context [STRING].
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERIPACL: Deleted IP access filter in policy group pgroup in context ctx1.
Explanation	The IP access filtering configuration was removed from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERIPACL_FAILED

Message text	Failed to delete IP access filter in policy group [STRING] in context [STRING]
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERIPACL_FAILED: Failed to delete IP access filter in policy group pgroup in context ctx1
Explanation	Failed to remove the IP access filtering configuration from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERPFWDITEM

Message text	Removed port forwarding item [STRING] from port forwarding list [STRING] in context [STRING].
Variable fields	$1: Port forwarding item name. $2: Port forwarding list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERPFWDITEM: Removed port forwarding item pfitem1 from port forwarding list pflist1 in context ctx1.
Explanation	A port forwarding item was removed from a port forwarding list.
Recommended action	No action is required.

SSLVPN_DEL_REFERPFWDITEM_FAILED

Message text	Failed to remove port forwarding item [STRING] from port forwarding list [STRING] in context [STRING].
Variable fields	$1: Port forwarding item name. $2: Port forwarding list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERPFWDITEM_FAILED: Failed to remove port forwarding item pfitem1 from port forwarding list pflist1 in context ctx1.
Explanation	Failed to remove a port forwarding item from a port forwarding list.
Recommended action	No action is required.

SSLVPN_DEL_REFERPORTFWD

Message text	Deleted port forwarding list used by policy-group [STRING] in context [STRING].
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERPORTFWD: Deleted port forwarding list used by policy-group pg in context ctx1.
Explanation	The port forwarding list configuration was removed from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERPORTFWD_FAILED

Message text	Failed to delete port forwarding list used by policy-group [STRING] in context [STRING]
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERPORTFWD_FAILED: Failed to delete port forwarding list used by policy-group pg in context ctx1.
Explanation	Failed to remove the port forwarding list configuration from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERSCUTLIST

Message text	Removed shortcut list from policy group [STRING] in context [STRING].
Variable fields	$1: SSL VPN policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERSCUTLIST: Removed shortcut list from policy group pg in context ctx1.
Explanation	A shortcut list was removed from an SSL VPN policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERSCUTLIST_FAILED

Message text	Failed to remove shortcut list from policy group [STRING] in context [STRING].
Variable fields	$1: SSL VPN policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERSCUTLIST_FAILED: Failed to remove shortcut list from policy group pg in context ctx1.
Explanation	Failed to remove a shortcut list from an SSL VPN policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERSHORTCUT

Message text	Removed shortcut [STRING] from shortcut list [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: Shortcut list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERSHORTCUT: Removed shortcut shortcut1 from shortcut list scutlist1 in context ctx1.
Explanation	A shortcut was removed from a shortcut list.
Recommended action	No action is required.

SSLVPN_DEL_REFERSHORTCUT_FAILED

Message text	Failed to remove shortcut [STRING] from shortcut list [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: Shortcut list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERSHORTCUT_FAILED: Failed to remove shortcut shortcut1 from shortcut list scutlist1 in context ctx1.
Explanation	Failed to remove a shortcut from a shortcut list.
Recommended action	No action is required.

SSLVPN_DEL_REFERSNATPOOL

Message text	Deleted the SNAT pool used in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERSNATPOOL: Deleted the SNAT pool used in context ctx1.
Explanation	The SNAT address pool configuration was removed from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_REFERSNATPOOL_FAILED

Message text	Failed to delete the SNAT pool used in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERSNATPOOL_FAILED: Failed to delete the SNAT pool used in context cxt1.
Explanation	Failed to remove the SNAT address pool configuration from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_REFERTCPACL

Message text	Deleted TCP access filter in policy group [STRING] in context [STRING].
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERTCPACL: Deleted TCP access filter in policy group pgroup in context ctx1.
Explanation	The TCP access filtering configuration was removed from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERTCPACL_FAILED

Message text	Failed to delete TCP access filter in policy group [STRING] in context [STRING]
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERTCPACL_FAILED: Failed to delete TCP access filter in policy group pgroup in context ctx1.
Explanation	Failed to remove the TCP access filtering configuration from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERURIACL

Message text	Deleted [STRING] access filter URI ACL from policy group [STRING] in context [STRING].
Variable fields	$1: SSL VPN access mode. Options are: • IP access. • Web access. • TCP access. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERURIACL: Deleted IP access filter URI ACL from policy group pgroup in context ctx1.
Explanation	The URI ACL used for IP, Web, or TCP access filtering was removed from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERURIACL_FAILED

Message text	Failed to delete [STRING] access filter URI ACL from policy group [STRING] in context [STRING].
Variable fields	$1: SSL VPN access mode. Options are: • IP access. • Web access. • TCP access. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERURIACL_FAILED: Failed to delete IP access filter URI ACL from policy group pgroup in context ctx1.
Explanation	Failed to remove the URI ACL used for IP, Web, or TCP access filtering from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERURLITEM

Message text	Deleted URL item [STRING] from URL list [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: URL list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERURLITEM: Deleted URL item item1 from URL list list1 in context ctx1.
Explanation	Removed a URL item from a URL list.
Recommended action	No action is required.

SSLVPN_DEL_REFERURLITEM_FAILED

Message text	Failed to delete URL item [STRING] from URL list [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: URL list name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERURLITEM_FAILED: Failed to delete URL item item1 from URL list list1 in context ctx1.
Explanation	Failed to remove a URL item from a URL list.
Recommended action	No action is required.

SSLVPN_DEL_REFERURLLIST

Message text	Deleted URL list [STRING] used by policy-group [STRING] in context [STRING].
Variable fields	$1: URL list name. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERURLLIST: Deleted URL list urllist used by policy-group pg in context ctx1.
Explanation	A URL list was removed from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERURLLIST_FAILED

Message text	Failed to delete URL list [STRING] used by policy-group [STRING] in context [STRING]
Variable fields	$1: URL list name. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERURLLIST_FAILED: Failed to delete URL list urllist used by policy-group pg in context ctx1.
Explanation	Failed to remove a URL list from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERWEBACL

Message text	Deleted Web access filter in policy group [STRING] in context [STRING].
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERWEBACL: Deleted Web access filter in policy group pgroup in context ctx1.
Explanation	The Web access filtering configuration was removed from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REFERWEBACL_FAILED

Message text	Failed to delete Web access filter in policy group [STRING] in context [STRING]
Variable fields	$1: Policy group name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REFERWEBACL_FAILED: Failed to delete Web access filter in policy group pgroup in context ctx1
Explanation	Failed to remove the Web access filtering configuration from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_REWRITE_RULE

Message text	Deleted rewrite rule [STRING] from file policy [STRING] in context [STRING].
Variable fields	$1: Rewrite rule name. $2: File policy name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REWRITE_RULE: Deleted rewrite rule rw from file policy fp in context ctx.
Explanation	A rewrite rule was deleted.
Recommended action	No action is required.

SSLVPN_DEL_REWRITE_RULE_FAILED

Message text	Failed to delete rewrite rule [STRING] from file policy [STRING] in context [STRING].
Variable fields	$1: Rewrite rule name. $2: File policy name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_REWRITE_RULE_FAILED: Failed to delete rewrite rule rw from file policy fp in context ctx.
Explanation	Failed to delete a rewrite rule.
Recommended action	No action is required.

SSLVPN_DEL_ROUTELIST

Message text	Deleted IP-route-list [STRING] in context [STRING].
Variable fields	$1: Route list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_ROUTELIST: Deleted IP-route-list rtlist in context ctx1.
Explanation	A route list was deleted from an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DEL_ROUTELIST_FAILED

Message text	Failed to delete IP-route-list [STRING] in context [STRING]
Variable fields	$1: Route list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_ROUTELIST_FAILED: Failed to delete IP-route-list rtlist in context ctx1.
Explanation	Failed to delete a route list from an SSL VPN context,
Recommended action	No action is required.

SSLVPN_DEL_ROUTEREFER

Message text	Deleted access routes [STRING] in policy-group [STRING] in context [STRING].
Variable fields	$1: The value can be **force-all** or null. The value of **force-all means to delete the route entries forcibly**. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_ROUTEREFER: Deleted access routes in policy-group pg in context ctx.
Explanation	Access routes were deleted from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_ROUTEREFER_FAILED

Message text	Failed to delete access routes [STRING] in policy-group [STRING] in context [STRING]
Variable fields	$1: The value can be **force-all** or null. The value of **force-all means to delete the route entries forcibly**. $2: Policy group name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_ROUTEREFER_FAILED: Failed to delete access routes in policy-group pg in context ctx.
Explanation	Failed to delete access routes from a policy group.
Recommended action	No action is required.

SSLVPN_DEL_SERVERURL

Message text	Deleted URL [STRING] from URL item [STRING] in context [STRING].
Variable fields	$1: URL string. $2: URL item name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_SERVERURL: Deleted URL www.abc.com from URL item item1 in context ctx1.
Explanation	Deleted the URL configuration from a URL item.
Recommended action	No action is required.

SSLVPN_DEL_SERVERURL_FAILED

Message text	Failed to delete URL [STRING] from URL item [STRING] in context [STRING].
Variable fields	$1: URL string. $2: URL item name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_SERVERURL_FAILED: Failed to delete URL www.abc.com from URL item item1 in context ctx1.
Explanation	Failed to delete the URL configuration from a URL item.
Recommended action	No action is required.

SSLVPN_DEL_SHORTCUT

Message text	Deleted shortcut [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_SHORTCUT: Deleted shortcut shortcut1 in context ctx1.
Explanation	A shortcut was deleted.
Recommended action	No action is required.

SSLVPN_DEL_SHORTCUT_FAILED

Message text	Failed to delete shortcut [STRING] in context [STRING].
Variable fields	$1: Shortcut name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_SHORTCUT_FAILED: Failed to delete shortcut shortcut1 in context ctx1.
Explanation	Failed to delete a shortcut.
Recommended action	No action is required.

SSLVPN_DEL_SHORTCUTLIST

Message text	Deleted shortcut list [STRING] in context [STRING].
Variable fields	$1: Shortcut list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_SHORTCUTLIST: Deleted shortcut list scutlist1 in context ctx1.
Explanation	A shortcut list was deleted.
Recommended action	No action is required.

SSLVPN_DEL_SHORTCUTLIST_FAILED

Message text	Failed to delete shortcut list [STRING] in context [STRING].
Variable fields	$1: Shortcut list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_SHORTCUTLIST_FAILED: Failed to delete shortcut list scutlist1 in context ctx1.
Explanation	Failed to delete a shortcut list.
Recommended action	No action is required.

SSLVPN_DEL_SNATPOOL

Message text	Deleted SSL VPN SNAT pool [STRING].
Variable fields	$1: SNAT pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_SNATPOOL: Deleted SSL VPN SNAT pool sp1.
Explanation	A SNAT address pool was deleted.
Recommended action	No action is required.

SSLVPN_DEL_SNATPOOL_FAILED

Message text	Failed to delete SSL VPN SNAT pool [STRING].
Variable fields	$1: SNAT pool name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_SNATPOOL_FAILED: Failed to delete SSL VPN SNAT pool sp1.
Explanation	Failed to delete a SNAT address pool.
Recommended action	No action is required.

SSLVPN_DEL_URIACL

Message text	Deleted URI ACL [STRING] in context [STRING].
Variable fields	$1: URI ACL name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URIACL: Deleted URI ACL uacl in context ctx1.
Explanation	A URI ACL was deleted.
Recommended action	No action is required.

SSLVPN_DEL_URIACL_FAILED

Message text	Failed to delete URI ACL [STRING] in context [STRING].
Variable fields	$1: URI ACL name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URIACL_FAILED: Failed to delete URI ACL uacl in context ctx1.
Explanation	Failed to delete a URI ACL.
Recommended action	No action is required.

SSLVPN_DEL_URIACL_RULE

Message text	Deleted rule [UINT32] from URI ACL [STRING] in context [STRING].
Variable fields	$1: Rule ID. $2: URI ACL name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URIACL_RULE: Deleted rule 5 from URI ACL uacl in context ctx1.
Explanation	A rule was deleted from a URI ACL.
Recommended action	No action is required.

SSLVPN_DEL_URIACL_RULE_FAILED

Message text	Failed to delete rule [UINT32] from URI ACL [STRING] in context [STRING].
Variable fields	$1: Rule ID. $2: URI ACL name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URIACL_RULE_FAILED: Failed to delete rule 5 from URI ACL uacl in context ctx1.
Explanation	Failed to delete a rule from a URI ACL.
Recommended action	No action is required.

SSLVPN_DEL_URL

Message text	Deleted the URL configuration for file policy [STRING] in context [STRING].
Variable fields	$1: File policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URL: Deleted the URL configuration for file policy fp1 in context ctx1.
Explanation	The file URL configuration was deleted for a file policy.
Recommended action	No action is required.

SSLVPN_DEL_URL_FAILED

Message text	Failed to delete the URL configuration for file policy [STRING] in context [STRING].
Variable fields	$1: File policy name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URL_FAILED: Failed to delete the URL configuration for file policy fp1 in context ctx1.
Explanation	Failed to delete the file URL configuration for a file policy.
Recommended action	No action is required.

SSLVPN_DEL_URLITEM

Message text	Deleted URL item [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URLITEM: Deleted URL item item1 in context ctx1.
Explanation	Deleted a URL item.
Recommended action	No action is required.

SSLVPN_DEL_URLITEM_FAILED

Message text	Failed to delete URL item [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URLITEM_FAILED: Failed to delete URL item item1 in context ctx1.
Explanation	Failed to delete a URL item.
Recommended action	No action is required.

SSLVPN_DEL_URLLIST

Message text	Deleted URL list [STRING] in context [STRING].
Variable fields	$1: URL list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URLLIST: Deleted URL list urllist in context ctx1.
Explanation	A URL list was deleted.
Recommended action	No action is required.

SSLVPN_DEL_URLLIST_FAILED

Message text	Failed to delete URL list [STRING] in context [STRING]
Variable fields	$1: URL list name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URLLIST_FAILED: Failed to delete URL list urllist in context ctx1.
Explanation	Failed to delete a URL list.
Recommended action	No action is required.

SSLVPN_DEL_URLMAPPING

Message text	Deleted URL mapping from URL item [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URLMAPPING: Deleted URL mapping from URL item item1 in context ctx1.
Explanation	Removed the URL mapping configuration from a URL item.
Recommended action	No action is required.

SSLVPN_DEL_URLMAPPING_FAILED

Message text	Failed to delete URL mapping from URL item [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_URLMAPPING_FAILED: Failed to delete URL mapping from URL item item1 in context ctx1.
Explanation	Failed to remove the URL mapping configuration from a URL item.
Recommended action	No action is required.

SSLVPN_DEL_USER

Message text	Deleted user [STRING] in context [STRING].
Variable fields	$1: SSL VPN username. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_USER: Deleted user user1 in context ctx1.
Explanation	An SSL VPN user was deleted.
Recommended action	No action is required.

SSLVPN_DEL_USER_FAILED

Message text	Failed to delete user [STRING] in context [STRING].
Variable fields	$1: SSL VPN username. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DEL_USER_FAILED: Failed to delete user user1 in context ctx1.
Explanation	Failed to delete an SSL VPN user.
Recommended action	No action is required.

SSLVPN_DISABLE_CONTEXT

Message text	Disabled service in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_CONTEXT: Disabled service in context ctx1.
Explanation	An SSL VPN context was disabled.
Recommended action	No action is required.

SSLVPN_DISABLE_CONTEXT_FAILED

Message text	Failed to disable service in context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_CONTEXT_FAILED: Failed to disable service in context ctx1.
Explanation	Failed to disable an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_CRTAUTH

Message text	Disabled certificate-authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_CRTAUTH: Disabled certificate-authentication in context ctx1.
Explanation	Certificate authentication was disabled in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_CRTAUTH_FAILED

Message text	Failed to disable certificate-authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_CRTAUTH_FAILED: Failed to disable certificate-authentication in context ctx1.
Explanation	Failed to disable certificate authentication in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_DYNAMICPWD

Message text	Disabled dynamic-password in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_DYNAMICPWD: Disabled dynamic-password in context ctx1.
Explanation	Dynamic password verification was disabled in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_DYNAMICPWD_FAILED

Message text	Failed to disable dynamic-password in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_DYNAMICPWD_FAILED: Failed to disable dynamic-password in context ctx1.
Explanation	Failed to disable dynamic password verification in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_GATEWAY

Message text	Disabled service in gateway [STRING].
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_GATEWAY: Disabled service in gateway gw1.
Explanation	An SSL VPN gateway was disabled.
Recommended action	No action is required.

SSLVPN_DISABLE_GATEWAY_FAILED

Message text	Failed to disable service in gateway [STRING]
Variable fields	$1: SSL VPN gateway name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_GATEWAY_FAILED: Failed to disable service in gateway gw1.
Explanation	Failed to disable an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_DISABLE_GLOBAL_LOG

Message text	Disabled SSL VPN logging globally.
Variable fields	No action is required.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_GLOBAL_LOG: Disabled SSL VPN logging globally.
Explanation	The SSL VPN global logging feature was disabled.
Recommended action	No action is required.

SSLVPN_DISABLE_GLOBAL_LOG_FAILED

Message text	Failed to disable SSL VPN logging globally.
Variable fields	No action is required.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_GLOBAL_LOG_FAILED: Failed to disable SSL VPN logging globally.
Explanation	Failed to disable the SSL VPN global logging feature.
Recommended action	No action is required.

SSLVPN_DISABLE_GLOBALURLMASKING

Message text	Disabled global URL masking in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_GLOBALURLMASKING: Disabled global URL masking in context ctx1.
Explanation	Disabled global URL masking in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_GLOBALURLMASKING_FAILED

Message text	Failed to disable global URL masking in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_GLOBALURLMASKING_FAILED: Failed to disable global URL masking in context ctx1.
Explanation	Failed to disable global URL masking in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_IPTNL_LOG_FAIL

Message text	Failed to disable IP tunnel access logging in context [STRING]. Log type is [STRING].
Variable fields	$1: SSL VPN context name. $2: Log type: • CONNECTION-CLOSE. • PACKET-DROP.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_IPTNL_LOG_FAIL: Failed to disable IP tunnel access logging in context ctx1. Log type is CONNECTION-CLOSE.
Explanation	Failed to disable logging for IP access connection close events or IP access packet drop events.
Recommended action	No action is required.

SSLVPN_DISABLE_IPTNL_LOG

Message text	Disabled IP tunnel access logging in context [STRING]. Log type is [STRING].
Variable fields	$1: SSL VPN context name. $2: Log type: • CONNECTION-CLOSE. • PACKET-DROP.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_IPTNL_LOG: Disabled IP tunnel access logging in context ctx1. Log type is CONNECTION-CLOSE.
Explanation	Disabled logging for IP access connection close events or IP access packet drop events.
Recommended action	No action is required.

SSLVPN_DISABLE_PWDAUTH

Message text	Disabled password authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_PWDAUTH: Disabled password authentication in context ctx1.
Explanation	Disabled password authention in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_PWDAUTH_FAILED

Message text	Failed to disable password authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_PWDAUTH_FAILED: Failed to disable password authentication in context ctx1.
Explanation	Failed to disable password authention in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_SMSIMC

Message text	Disabled iMC SMS message authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_SMSIMC: Disabled iMC SMS message authentication in context ctx1.
Explanation	IMC SMS message authentication was disabled in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_SMSIMC_FAILED

Message text	Failed to disable iMC SMS message authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_SMSIMC_FAILED: Failed to disable IMC SMS message authentication in context ctx1.
Explanation	Failed to disable IMC SMS message authentication in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_URLMASKING

Message text	Disabled URL masking for URL item [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_URLMASKING: Disabled URL masking for URL item item1 in context ctx1.
Explanation	Disabled URL masking for a URL item.
Recommended action	No action is required.

SSLVPN_DISABLE_URLMASKING_FAILED

Message text	Failed to disable URL masking for URL item [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_URLMASKING_FAILED: Failed to disable URL masking for URL item item1 in context ctx1.
Explanation	Failed to disable URL masking for a URL item.
Recommended action	No action is required.

SSLVPN_DISABLE_VERIFYCODE

Message text	Disabled code verification in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_VERIFYCODE: Disabled code verification in context ctx1.
Explanation	Code verification was disabled in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DISABLE_VERIFYCODE_FAILED

Message text	Failed to disable code verification in context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_DISABLE_VERIFYCODE_FAILED: Failed to disable code verification in context ctx1.
Explanation	Failed to disable code verification in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_DOMAIN_URLMAPPING

Message text	Configured domain mapping for URL item [STRING] in context [STRING]: mapped domain name=[STRING], URL rewriting=[STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name. $3: Mapped domain name. $4: Whether absolute path rewriting is enabled. Options are: • enabled. • disabled.
Severity level	6
Example	SSLVPN/6/SSLVPN_DOMAIN_URLMAPPING: Configured domain mapping for URL item item1 in context ctx1: mapped domain name=www.abc.com, URL rewriting=enabled.
Explanation	Configured the domain mapping method for the URL in a URL item.
Recommended action	No action is required.

SSLVPN_DOMAIN_URLMAPPING_FAILED

Message text	Failed to configure domain mapping for URL item [STRING] in context [STRING]: mapped domain name=[STRING], URL rewriting=[STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name. $3: Mapped domain name. $4: Whether absolute path rewriting is enabled. Options are: • enabled. • disabled.
Severity level	6
Example	SSLVPN/6/SSLVPN_DOMAIN_URLMAPPING_FAILED: Failed to configure domain mapping for URL item **item1** in context **ctx1**: mapped domain name=www.abc.com, URL rewriting=enabled.
Explanation	Failed to configure the domain mapping method for the URL in a URL item.
Recommended action	No action is required.

SSLVPN_ENABLE_CONTEXT

Message text	Enabled service in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_CONTEXT: Enabled service in context ctx1.
Explanation	An SSL VPN context was enabled.
Recommended action	No action is required.

SSLVPN_ENABLE_CONTEXT_FAILED

Message text	Failed to enable service in context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_CONTEXT_FAILED: Failed to enable service in context ctx1.
Explanation	Failed to enable an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_CRTAUTH

Message text	Enabled certificate-authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_CRTAUTH: Enabled certificate-authentication in context ctx1.
Explanation	Certification authentication was enabled in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_CRTAUTH_FAILED

Message text	Failed to enable certificate-authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_CRTAUTH_FAILED: Failed to enable certificate-authentication in context ctx1.
Explanation	Failed to enable certification authentication in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_DYNAMICPWD

Message text	Enabled dynamic-password in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_DYNAMICPWD: Enabled dynamic password verification in context ctx1.
Explanation	Dynamic password verification was enabled in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_DYNAMICPWD_FAILED

Message text	Failed to enable dynamic-password in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_DYNAMICPWD_FAILED: Failed to enable dynamic-password in context ctx1.
Explanation	Failed to enable dynamic password verification in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_FORCELOGOUT

Message text	Enabled force logout in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_FORCELOGOUT: Enabled force logout in context ctx1.
Explanation	The force logout feature was enabled. When a login is attempted but logins using the account reach the limit, this feature logs out a user using that account to allow the new login.
Recommended action	No action is required.

SSLVPN_ENABLE_FORCELOGOUT_FAILED

Message text	Failed to enable force logout in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_FORCELOGOUT_FAILED: Failed to enable force logout in context ctx1.
Explanation	Failed to enable the force logout feature. When a login is attempted but logins using the account reach the limit, this feature logs out a user using that account to allow the new login.
Recommended action	No action is required.

SSLVPN_ENABLE_GATEWAY

Message text	Enabled service in gateway [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_GATEWAY: Enabled service in gateway gw1.
Explanation	An SSL VPN gateway was enabled.
Recommended action	No action is required.

SSLVPN_ENABLE_GATEWAY_FAILED

Message text	Failed to enable service in gateway [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_GATEWAY_FAILED: Failed to enable service in gateway gw1.
Explanation	Failed to enable an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_ENABLE_GLOBAL_LOG

Message text	Enabled SSL VPN logging globally.
Variable fields	No action is required.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_GLOBAL_LOG: Enabled SSL VPN logging globally.
Explanation	The SSL VPN global logging feature was enabled.
Recommended action	No action is required.

SSLVPN_ENABLE_GLOBAL_LOG_FAILED

Message text	Failed to enable SSL VPN logging globally.
Variable fields	No action is required.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_GLOBAL_LOG_FAILED: Failed to enable SSL VPN logging globally.
Explanation	Failed to enable the SSL VPN global logging feature.
Recommended action	No action is required.

SSLVPN_ENABLE_GLOBALURLMASKING

Message text	Enabled global URL masking in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_GLOBALURLMASKING: Enabled global URL masking in context ctx1.
Explanation	Enabled global URL masking in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_GLOBALURLMASKING_FAILED

Message text	Failed to enable global URL masking in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_GLOBALURLMASKING_FAILED: Failed to enable global URL masking in context ctx1.
Explanation	Failed to enable global URL masking in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_IPTNL_LOG

Message text	Enabled IP tunnel access logging in context [STRING]. Log type is [STRING].
Variable fields	$1: SSL VPN context name. $2: Log type: • CONNECTION-CLOSE. • PACKET-DROP.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_IPTNL_LOG: Enabled IP tunnel access logging in context ctx1. Log type is CONNECTION-CLOSE.
Explanation	Enabled logging for IP access connection close events or IP access packet drop events.
Recommended action	No action is required.

SSLVPN_ENABLE_IPTNL_LOG_FAIL

Message text	Failed to enable IP tunnel access logging in context [STRING]. Log type is [STRING].
Variable fields	$1: SSL VPN context name. $2: Log type: • CONNECTION-CLOSE. • PACKET-DROP.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_IPTNL_LOG_FAIL: Failed to enable IP tunnel access logging in context ctx1. Log type is CONNECTION-CLOSE.
Explanation	Failed to enable logging for IP access connection close events or IP access packet drop events.
Recommended action	No action is required.

SSLVPN_ENABLE_PWDAUTH

Message text	Enabled password authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_PWDAUTH: Enabled password authentication in context ctx1.
Explanation	Password authentication was enabled in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_PWDAUTH_FAILED

Message text	Failed to enable password authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_PWDAUTH_FAILED: Failed to enable password authentication in context ctx1.
Explanation	Failed to enable password authentication in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_SMSIMC

Message text	Enabled iMC SMS message authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_SMSIMC: Enabled IMC SMS message authentication in context ctx1.
Explanation	IMC SMS message authentication was enabled in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_SMSIMC_FAILED

Message text	Failed to enable iMC SMS message authentication in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_SMSIMC_FAILED: Failed to enable iMC SMS message authentication in context ctx1.
Explanation	Failed to enable IMC SMS message authentication in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_URLMASKING

Message text	Enabled URL masking for URL item [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_URLMASKING: Enabled URL masking for URL item item1 in context ctx1.
Explanation	Enabled URL masking for a URL item.
Recommended action	No action is required.

SSLVPN_ENABLE_URLMASKING_FAILED

Message text	Failed to enable URL masking for URL item [STRING] in context [STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_URLMASKING_FAILED: Failed to enable URL masking for URL item item1 in context ctx1.
Explanation	Failed to enable URL masking for a URL item.
Recommended action	No action is required.

SSLVPN_ENABLE_VERIFYCODE

Message text	Enabled code verification in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_VERIFYCODE: Enabled code verification in context ctx1.
Explanation	Code verification was enabled in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_ENABLE_VERIFYCODE_FAILED

Message text	Failed to enable code verification in context [STRING]
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_ENABLE_VERIFYCODE_FAILED: Failed to enable code verification in context ctx1.
Explanation	Failed to enable code verification in an SSL VPN context.
Recommended action	No action is required.

SSLVPN_IP_RESOURCE_DENY

Message text	User [STRING] of context [STRING] from [STRING] denied to access [STRING]:[STRING].
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address. $4: IP address of the requested resource. $5: Port number of the requested resource.
Severity level	6
Example	SSLVPNK/6/SSLVPN_IP_RESOURCE_DENY: User abc of context ctx1 from 192.168.200.130 denied to access 10.1.1.255:137.
Explanation	A user was denied access to specific IP resources, possibly caused by ACL-based access filtering.
Recommended action	Verify that access to the requested resource is not denied by the ACL rules used for IP access filtering.

SSLVPN_IP_RESOURCE_FAILED

Message text	User [STRING] of context [STRING] from [STRING] failed to access [STRING]:[STRING].
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address. $4: IP address of the requested resource. $5: Port number of the requested resource.
Severity level	6
Example	SSLVPNK/6/SSLVPN_IP_RESOURCE_FAILED: User abc of context ctx1 from 192.168.200.130 failed to access 10.1.1.255:137.
Explanation	A user failed to access IP resources, possibly caused by network problems.
Recommended action	Verify that a route is available to reach the requested IP resource.

SSLVPN_IP_RESOURCE_PERMIT

Message text	User [STRING] of context [STRING] from [STRING] permitted to access [STRING]:[STRING].
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address. $4: IP address of the requested resource. $5: Port number of the requested resource.
Severity level	6
Example	SSLVPNK/6/SSLVPN_IP_RESOURCE_PERMIT: User abc of context ctx1 from 192.168.200.130 permitted to access 10.1.1.255:137.
Explanation	A user accessed IP resources.
Recommended action	No action is required.

SSLVPN_IPAC_ALLOC_ADDR_FAIL

Message text	Failed to allocate IP address to user [STRING] at [STRING] in context [STRING]. Reason: [STRING].
Variable fields	$1: Username. $2: User IP address. $3: SSL VPN context name. $4: Reason why the SLS VPN gateway failed to allocate an IP address to the VNIC of the client. Options are: • Failed to obtain system resource data. • No address is available in the address pool. • Failed to obtain address pool. • Available addresses in the address pool have been bound to other users.
Severity level	6
Example	SSLVPN/6/SSLVPN_IPAC_ALLOC_ADDR_FAIL: Failed to allocate IP address to user abc at 192.168.68.10 in context ctx. Reason: Failed to obtain system resource data.
Explanation	The SSL VPN gateway failed to allocate an IP address to the VNIC of the IP access client.
Recommended action	**349.** Verify that the device is operating correctly. **350.** Verify that the address pool is configured. **351.** Verify that the address pool has available addresses. **352.** Verify that the available addresses are not bound to other users.

SSLVPN_IPAC_ALLOC_ADDR_SUCCESS

Message text	IP address [STRING] successfully allocated to user [STRING] at [STRING] in context [STRING].
Variable fields	$1: IP address that the SSL VPN gateway allocated to the VNIC of the client. $2: Username. $3: User IP address. $4: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_IPAC_ALLOC_ADDR_SUCCESS: IP address 10.1.1.1 successfully allocated to user abc at 192.168.68.10 in context ctx.
Explanation	The SSL VPN gateway allocated an IP address to the VNIC of the IP access client successfully.
Recommended action	No action is required.

SSLVPN_IPAC_CONN_CLOSE

Message text	IP connection was [STRING]. Reason: [STRING].
Variable fields	$1: Connection close type. Options are: • closed. • aborted. $2: Reason why the connection was closed. Options are: • User logout. • Failure to find peer. • Handshake failed. • Change of IP address pool. • Failure to receive data. • Local retransmission timeout. • Local keepalive timeout. • Local probe timeout. • Received FIN from peer. • Received RST from peer. • No authorized policy group. • Allocated address was bound to another user. • Failure to update client configuration. • Deleted old peer. • Other.
Severity level	6
Example	SSLVPNK/6/SSLVPN_IPAC_CONN_CLOSE: IP connection was closed. Reason: User logout.
Explanation	The reason for the close of an IP connection was logged.
Recommended action	No action is required.

SSLVPN_IPAC_PACKET_DROP

Message text	Dropped [STRING] IP connection [STRING] packets in context [STRING]. Reason: [STRING].
Variable fields	$1: Number of dropped packets. $2: Dropped packet type: • request. • reply. $3: SSL VPN context name. $4: Reason for the packet drop: • Context rate limit. • Buffer insufficient.
Severity level	6
Example	SSLVPN/6/SSLVPN_IPAC_PACKET_DROP: Dropped 5 IP connection request packets in context ctx1. Reason: Context rate limit.
Explanation	The reason for IP access packet drop was logged.
Recommended action	No action is required.

SSLVPN_IPAC_RELEASE_ADDR_SUCCESS

Message text	User [STRING] at [STRING] in context [STRING] released IP address [STRING].
Variable fields	$1: Username. $2: User IP address. $3: SSL VPN context name. $4: IP address that the SSL VPN gateway allocated to the VNIC of the client.
Severity level	6
Example	SSLVPN/6/SSLVPN_IPAC_RELEASE_ADDR_SUCCESS: User abc at 192.168.68.10 in context ctx released IP address 10.1.1.1.
Explanation	The SSL VPN gateway released the allocated IP address from the VNIC of the IP access client successfully.
Recommended action	No action is required.

SSLVPN_PORT_URLMAPPING

Message text	Configured port mapping for URL item [STRING] in context [STRING]: mapped gateway name=[STRING], virtual host name=[STRING], URL rewriting=[STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name. $3: Mapped SSL VPN gateway name. $4: Virtual host name. $5: Whether absolute path rewriting is enabled. Options are: • enabled. • disabled.
Severity level	6
Example	SSLVPN/6/SSLVPN_PORT_URLMAPPING: Configured port mapping for URL item **item1** in context **ctx1**: mapped gateway name=www.abc.com, virtual host name=vhost1, URL rewriting=enabled.
Explanation	Configured the port mapping method for the URL in a URL item.
Recommended action	No action is required.

SSLVPN_PORT_URLMAPPING_FAILED

Message text	Failed to configure port mapping for URL item [STRING] in context [STRING]: mapped gateway name=[STRING], virtual host name=[STRING], URL rewriting=[STRING].
Variable fields	$1: URL item name. $2: SSL VPN context name. $3: Mapped SSL VPN gateway name. $4: Virtual host name. $5: Whether absolute path rewriting is enabled. Options are: • enabled. • disabled.
Severity level	6
Example	SSLVPN/6/SSLVPN_PORT_URLMAPPING_FAILED: Failed to configure port mapping for URL item item1 in context ctx1: mapped gateway name=gw1, virtual host name=vhost1, URL rewriting=enabled.
Explanation	Failed to configure the port mapping method for the URL in a URL item.
Recommended action	No action is required.

SSLVPN_SERVICE_UNAVAILABLE

Message text	SSL VPN service was unavailable. Reason: [STRING].
Variable fields	$1: Reason why the SSL VPN service was unavailable. Options are: • SSL VPN context not enabled. • No available SSL VPN contexts.
Severity level	6
Example	SSLVPNK/6/SSLVPN_SERVICE_UNAVAILABLE: SSL VPN service was unavailable. Reason: SSL VPN context not enabled.
Explanation	The reason for the unavailability of an SSL VPN service was logged.
Recommended action	If the reason is **SSL VPN context not enabled**, enter SSL VPN context view and use the **`service enable`** command to enable the context. If the reason is **No available SSL VPN contexts**, verify that the SSL VPN gateway to which the user is connected is associated with SSL VPN contexts.

SSLVPN_TCP_RESOURCE_DENY

Message text	User [STRING] of context [STRING] from [STRING] denied to access [STRING]:[STRING] (server-IP=[STRING],port-number=[STRING]).
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address. $4: Address of the remote server. $5: Port number of the remote server. $6: IP address of the remote server. $7: Port number of the remote server.
Severity level	6
Example	SSLVPNK/6/SSLVPN_TCP_RESOURCE_DENY: User abc of context ctx1 from 192.168.200.130 denied to access 10.1.1.255:137 (server-IP=10.1.1.255,port-number=137).
Explanation	A user was denied access to specific TCP resources, possibly caused by ACL-based access filtering.
Recommended action	Verify that access to the requested resource is not denied by the ACL rules used for TCP access filtering.

SSLVPN_TCP_RESOURCE_FAILED

Message text	User [STRING] of context [STRING] from [STRING] failed to access [STRING]:[STRING] (server-IP=[STRING],port-number=[STRING]).
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address. $4: IP address of the remote server. $5: Port number of the remote server. $6: IP address of the remote server. $7: Port number of the remote server.
Severity level	6
Example	SSLVPNK/6/SSLVPN_TCP_RESOURCE_FAILED: User abc of context ctx1 from 192.168.200.130 failed to access 10.1.1.255:137 (server-IP=10.1.1.255,port-number=137).
Explanation	A user failed to access TCP resources, possibly caused by network problems or DNS resolution failures.
Recommended action	**353.** Verify that a route is available to reach the requested TCP resource. **354.** Verify that a DNS server is available for domain name resolution.

SSLVPN_TCP_RESOURCE_PERMIT

Message text	User [STRING] of context [STRING] from [STRING] permitted to access [STRING]:[STRING] (server-IP=[STRING],port-number=[STRING]).
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address. $4: Address of the remote server. $5: Port number of the remote server. $6: IP address of the remote server. $7: Port number of the remote server.
Severity level	6
Example	SSLVPNK/6/SSLVPN_TCP_RESOURCE_PERMIT: User abc of context ctx1 from 192.168.200.130 permitted to access 10.1.1.255:137 (server-IP=10.1.1.255,port-number=137).
Explanation	A user accessed TCP resources.
Recommended action	No action is required.

SSLVPN_UNDO_FORCELOGOUT

Message text	Disabled force logout in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_UNDO_FORCELOGOUT: Disabled force logout in context ctx1.
Explanation	The force logout feature was disabled. When a login is attempted but logins using the account reach the limit, this feature logs out a user using that account to allow the new login.
Recommended action	No action is required.

SSLVPN_UNDO_FORCELOGOUT_FAILED

Message text	Failed to disable force logout in context [STRING].
Variable fields	$1: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_UNDO_FORCELOGOUT_FAILED: Failed to disable force logout in context ctx1.
Explanation	Failed to disable the force logout feature. When a login is attempted but logins using the account reach the limit, this feature logs out a user using that account to allow the new login.
Recommended action	No action is required.

SSLVPN_URLITEM_ADD_URIACL

Message text	Specified URI ACL [STRING] for URL item [STRING] in context [STRING].
Variable fields	$1: URI ACL used by the URL item. $2: URL item name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_URLITEM_ADD_URIACL: Specified URI ACL uriacl1 for URL item item1 in context ctx1.
Explanation	Specified a URI ACL for a URL item.
Recommended action	No action is required.

SSLVPN_URLITEM_ADD_URIACL_FAILED

Message text	Failed to specify URI ACL [STRING] for URL item [STRING] in context [STRING].
Variable fields	$1: URI ACL used by the URL item. $2: URL item name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_URLITEM_ADD_URIACL_FAILED: Failed to specify URI ACL uriacl1 for URL item item1 in context ctx1.
Explanation	Failed to specify a URI ACL for a URL item.
Recommended action	No action is required.

SSLVPN_URLITEM_DEL_URIACL

Message text	Removed URI ACL [STRING] from URL item [STRING] in context [STRING].
Variable fields	$1: URI ACL used by the URL item. $2: URL item name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_URLITEM_DEL_URIACL: Removed URI ACL uriacl1 from URL item item1 in context ctx1.
Explanation	Removed the URI ACL configuration from a URL item.
Recommended action	No action is required.

SSLVPN_URLITEM_DEL_URIACL_FAILED

Message text	Failed to remove URI ACL [STRING] from URL item [STRING] in context [STRING].
Variable fields	$1: URI ACL used by the URL item. $2: URL item name. $3: SSL VPN context name.
Severity level	6
Example	SSLVPN/6/SSLVPN_URLITEM_DEL_URIACL_FAILED: Failed to remove URI ACL uriacl1 from URL item item1 in context ctx1.
Explanation	Failed to remove the URI ACL configuration from a URL item.
Recommended action	No action is required.

SSLVPN_USER_LOGIN

Message text	User [STRING] of context [STRING] logged in from [STRING].
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address.
Severity level	5
Example	SSLVPN/5/SSLVPN_USER_LOGIN: User abc of context ctx logged in from 192.168.200.31.
Explanation	A user logged in to an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_USER_LOGINFAILED

Message text	User [STRING] of context [STRING] failed to log in from [STRING]. Reason: [STRING].
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address. $4: Reason for the login failure: • Authentication failed. Reason: incorrectusername or password, authentication server error, or number of users reaching the maximum allowed by an account. • Authentication failed. Reason: The account expires. • Authorization failed. • Accounting failed. • Number of online users exceeded the limit. • Failed to get SMS message code from IMC server. • Maximum number of concurrent online connections for the user already reached. • Login timed out. • The authentication server is not reachable. • The authorization server is not reachable. • The accounting server is not reachable. • Other.
Severity level	5
Example	SSLVPN/5/SSLVPN_USER_LOGINFAILED: User abc of context ctx failed to log in from 192.168.200.31.
Explanation	A user failed to log in to an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_USER_LOGOUT

Message text	User [STRING] of context [STRING] logged out from [STRING]. Reason: [STRING].
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address. $4: Reason for user logout: • Idle timeout. • A logout request was received from the Web browser. • A logout request was received from the client. • Forced logout. • A new login was attempted and logins using the account reach the maximum. • Accounting update failed. • Accounting session timed out. • Interface went down. • ADM request was received. • Idle cut for traffic not reach the minimum required amount.
Severity level	5
Example	SSLVPN/5/SSLVPN_USER_LOGOUT: User abc of context ctx logged out from 192.168.200.31. Reason: A logout request was received from the Web browser.
Explanation	A user logged out of an SSL VPN gateway.
Recommended action	No action is required.

SSLVPN_USER_NUMBER

Message text	The number of SSL VPN users reached the upper limit.
Variable fields	None.
Severity level	6
Example	SSLVPN/6/SSLVPN_USER_NUMBER: The number of SSL VPN users reached the upper limit.
Explanation	The number of SSL VPN users reached the upper limit.
Recommended action	No action is required.

SSLVPN_WEB_RESOURCE_DENY

Message text	User [STRING] of context [STRING] from [STRING] denied to access [STRING] (server-IP=[STRING],port-number=[STRING]).
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address. $4: URL of the requested resource. $5: IP address of the Web server that provides the requested resource. $6: Port number of the Web server.
Severity level	6
Example	SSLVPNK/6/SSLVPN_WEB_RESOURCE_DENY: User abc of context ctx1 from 192.168.200.130 denied to access http://192.168.0.2:80/ (server-IP=192.168.0.2,port-number=80).
Explanation	A user was denied access to specific Web resources, possibly caused by ACL-based access filtering.
Recommended action	Verify that access to the requested resource is not denied by the ACL rules used for Web access filtering.

SSLVPN_WEB_RESOURCE_FAILED

Message text	User [STRING] of context [STRING] from [STRING] failed to access [STRING] (server-IP=[STRING],port-number=[STRING]).
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address. $4: URL of the requested resource. $5: IP address of the Web server that provides the requested resource. $6: Port number of the Web server.
Severity level	6
Example	SSLVPNK/6/SSLVPN_WEB_RESOURCE_FAILED: User abc of context ctx1 from 192.168.200.130 failed to access http://192.168.0.2:80/ (server-IP=192.168.0.2,port-number=80).
Explanation	A user failed to access Web resources, possibly caused by network problems or DNS resolution failures.
Recommended action	**355.** Verify that a route is available to reach the requested Web resource. **356.** Verify that a DNS server is available for domain name resolution.

SSLVPN_WEB_RESOURCE_PERMIT

Message text	User [STRING] of context [STRING] from [STRING] permitted to access [STRING] (server-IP=[STRING],port-number=[STRING]).
Variable fields	$1: Username. $2: SSL VPN context name. $3: User IP address. $4: URL of the requested resource. $5: IP address of the Web server that provides the requested resource. $6: Port number of the Web server.
Severity level	6
Example	SSLVPNK/6/SSLVPN_WEB_RESOURCE_PERMIT: User abc of context ctx1 from 192.168.200.130 permitted to access http://192.168.0.2:80/ (server-IP=192.168.0.2,port-number=80).
Explanation	A user accessed Web resources.
Recommended action	No action is required.

STAMGR messages

This section contains station management messages.

STAMGR_ADD_FAILVLAN

Message text	-SSID=[STRING]-UserMAC=[STRING]-APName=[STRING]-RadioID=[STRING]; Added a user to the Fail VLAN [STRING].
Variable fields	$1: SSID. $2: MAC address of the client. $3: Name of the AP associated with the client. $4: ID of the radio associated with the client. $5: ID of the Fail VLAN.
Severity level	5
Example	STAMGR/5/STAMGR_ADD_FAILVLAN:-SSID=text-wifi-UserMAC=3ce5-a616-28cd-APName=ap1-RadioID=2; Added a user to the Fail VLAN 5.
Explanation	The client failed to pass the authentication and was assigned to the Auth-Fail VLAN.
Recommended action	No action is required.

STAMGR_ADDBAC_INFO

Message text	Add BAS AC [STRING].
Variable fields	$1: MAC address of the BAS AC.
Severity level	6
Example	STAMGR/6/STAMGR_ADDBAC_INFO: Add BAS AC 3ce5-a616-28cd.
Explanation	The BAS AC was connected to the master AC.
Recommended action	No action is required.

STAMGR_ADDSTA_INFO

Message text	Add client [STRING].
Variable fields	$1: MAC address of the client.
Severity level	6
Example	STAMGR/6/STAMGR_ADDSTA_INFO: Add client 3ce5-a616-28cd.
Explanation	The client was connected to the BAS AC.
Recommended action	No action is required.

STAMGR_AUTHORACL_FAILURE

Message text	-SSID=[STRING]-UserMAC=[STRING]-APName=[STRING]-RadioID=[STRING]; Failed to assign an ACL [STRING]. Reason: [STRING].
Variable fields	$1: SSID. $2: MAC address of the client. $3: Name of the AP associated with the client. $4: ID of the radio associated with the client. $5: ACL number. $6: Reason: • The ACL doesn't exist. • This type of ACL is not supported. • The memory resource is not enough. • The ACL conflicts with other ACLs. • The ACL doesn't contain any rules. • The OpenFlow tunnel was not established. • The OpenFlow table is full. • Unknown reason. Error code *code* was returned.
Severity level	5
Example	STAMGR/5/STAMGR_AUTHORACL_FAILURE:-SSID=text-wifi-UserMAC=3ce5-a616-28cd-APName=ap1-RadioID=2; Failed to assign an ACL 2000. Reason: The ACL doesn’t exist.
Explanation	The authentication server failed to assign an ACL to the client.
Recommended action	No action is required.

STAMGR_AUTHORUSERPROFILE_FAILURE

Message text	-SSID=[STRING]-UserMAC=[STRING]-APName=[STRING]-RadioID=[STRING]; Failed to assign user profile [STRING]. Reason: [STRING].
Variable fields	$1: SSID. $2: MAC address of the client. $3: Name of the AP associated with the client. $4: ID of the radio associated with the client. $5: Name of the authorization user profile. $6: Failure cause: • The user profile doesn't exist. • No user profiles are created on the device. • The memory resource is not enough. • The OpenFlow tunnel was not established. • Unknown reason. Error code *code* was returned.
Severity level	5
Example	STAMGR/5/STAMGR_AUTHORUSERPROFILE_FAILURE:-SSID=text-wifi-UserMAC=3ce5-a616-28cd-APName=ap1-RadioID=2; Failed to assign user profile aaa. Reason: No user profiles are created on the device.
Explanation	The authentication server failed to assign a user profile to the client.
Recommended action	No action is required.

STAMGR_BSS_FAILURE

Message text	-APID=[STRING]-RadioID=[STRING]-WLANID=[STRING]-STName=[STRING]; The number of BSSs exceeded the upper limit.
Variable fields	$1: AP ID. $2: Radio ID. $3: WLAN ID. $4: Service template name.
Severity level	6
Example	STAMGR/6/SERVICE_BSS_FAILURE: -APID=1-RadioID=2-WLANID=3-STName=1; The number of BSSs exceeded the upper limit.
Explanation	The number of AP radios using this service template has exceeded the upper limit.
Recommended action	No action is required.

STAMGR_CLIENT_FAILURE

Message text	Client [STRING] failed to come online from BSS [STRING] with SSID [STRING] on AP [STRING] Radio ID [STRING] Reason: [STRING].
Variable fields	$1: MAC address of the client. $2: BSSID. $3: SSID defined in the service template. $4: Name of the AP associated with the client. $5: ID of the radio associated with the client. $6: Reasons for the client's failure to come online. Table 19 describes the possible reasons.
Severity level	5
Example	STAMGR/6/STAMGR_CLIENT_FAILURE: Client 3303-c2af-b8d2 failed to come online from BSS 0023-12ef-78dc with SSID 1 on AP ap1 Radio ID 2 Reason: Unknown reason.
Explanation	The client failed to come online from the BSS for a specific reason.
Recommended action	To resolve the issue: **357.** Check the debugging information to locate the issue and resolve it. **358.** If the issue persists, contact NSFOCUS Support.

Table 19 Possible failure reasons

Possible reasons
Unknown error.
Failed to process open authentication packet from the client.
Failed to send responses when the AC successfully processed open authentication packet from the client.
Failed to create state timer when the AC received authentication packet in Unauth state.
Failed to refresh state timer when the AC received authentication packet in Unauth state.
Received association packet Unauth state.
Received deauthentication packet with reason code *code* in Unauth state*:* • **1**—Unknown reason. • **3**—Client is removed from BSS and is deauthenticated. • **6**—Incorrect frame. • **9**—Received association or reassociation request before authentication is complete. • **13**—Invalid IE.
Received dissociation packet with reason code *code in* Unauth state*:* • **1**—Unknown reason. • **2**—Prior authentication is invalid. • **4**—Inactivity timer expired. • **5**—Insufficient resources. • **7**—Incorrect frame. • **8**—Client is removed from BSS and is disassociated. • **10**—Failed to negotiate the Power Capability IE. • **11**—BSS management switchover.
Received Auth failure packet in Unauth state.
Received state timer timeout in Unauth state.

Possible reasons
Received deauthentication packet with reason code *code* in Auth state*:* • **1**—Unknown reason. • **3**—Client is removed from BSS and is deauthenticated. • **6**—Incorrect frame. • **9**—Received association or reassociation request before authentication is complete. • **13**—Invalid IE.
Received authentication packet with inconsistent authentication algorithm or shared key in Auth state.
Received state timer timeout in Auth state.
Failed to process Add Mobile message when client association succeeded in Auth state.
Received inconsistent authentication algorithm or share key in Userauth state.
Failed to check association request when the AC received association packet in Userauth state.
Failed to process IE when the AC received association packet in Userauth state.
Failed to send association responses when the AC received association packet in Userauth state.
Failed to process Add Mobile message when client association succeeded in Userauth state.
Received deauthentication packet with reason code *code* in Userauth state*:* • **1**—Unknown reason. • **3**—Client is removed from BSS and is deauthenticated. • **6**—Incorrect frame. • **9**—Received association or reassociation request before authentication is complete. • **13**—Invalid IE.
Received dissociation packet with reason code *code* in Userauth state*:* • **1**—Unknown reason. • **2**—Prior authentication is invalid. • **4**—Inactivity timer expired. • **5**—Insufficient resources. • **7**—Incorrect frame. • **8**—Client is removed from BSS and is disassociated. • **10**—Failed to negotiate the Power Capability IE. • **11**—BSS management switchover.
Client authentication failed in Userauth state.
Failed to get backup client data while using AP private data to upgrade client.
Failed to set kernel forwarding table while using AP private data to upgrade client.
Failed to add MAC while using AP private data to upgrade client.
Failed to create keepalive and idle timeout timers while using AP private data to upgrade client.
Failed to set kernel forwarding table while upgrading client without using AP private data.
Failed to add MAC while upgrading client without using AP private data.
Failed to activate client while upgrading client without using AP private data.
Failed to synchronize client information to configuration thread while upgrading client without using AP private data.
Failed to create keepalive and idle timeout timers while upgrading client without using AP private data.
Failed to add MAC during inter-device client smooth creation.
Failed to set kernel forwarding table during inter-device client smooth creation.

Possible reasons
Failed to send Add Mobile message during inter-device client smooth creation.
Failed to get AP type during inter-device client smooth creation.
Failed to recover service data while recovering running client data from database.
Failed to synchronize data to service thread while recovering basic client data from database.
Failed to add MAC when hierarchy device received upstream Add Mobile message.
Failed to set kernel forwarding table when hierarchy device received upstream Add Mobile message.
Failed to synchronize upstream message when hierarchy device received upstream Add Mobile message.
Failed to create client when hierarchy device received upstream Add Mobile message.
Failed to add MAC when hierarchy device received downstream Add Mobile message.
Failed to synchronize data to service thread when hierarchy device received downstream Add Mobile message.
Failed to set kernel forwarding table when hierarchy device received downstream Add Mobile message.
Failed to send down add pbss to driver when hierarchy device received downstream Add Mobile message.
Failed to synchronize downstream message when hierarchy device received downstream Add Mobile message.
Failed to create client when hierarchy device received downstream Add Mobile message.
Failed to create interval statistics timer when hierarchy device received downstream Add Mobile message.
Failed to obtain AP private data when hierarchy device received downstream Add Mobile message.
Failed to advertise Add Mobile message.
Failed to activate client when hierarchy device received downstream client state synchronization message.
Failed to get AP type when hierarchy device received downstream client state synchronization message.
Failed to synchronize downstream message when hierarchy device received downstream client state synchronization message.
The radio was in down state when hierarchy device received downstream Add Mobile message.
Hierarchy device failed to process the upstream Add Mobile message.
Hierarchy device failed to process downstream Add Mobile message.
Failed to process service thread during inter-device client smooth creation.
Failed to create client during inter-device smooth.
Failed to process upstream client state synchronization message in Userauth state.
Failed to process downstream client state synchronization message in Userauth state.
Hierarchy device failed to process upstream client state synchronization message.
Hierarchy device failed to process downstream client state synchronization message.
AC received message for deleting the client entry.
Fit AP received message for deleting the client.
Different old and new region codes.
Failed to update IGTK.
Failed to update GTK.
Failed to generate IGTK when the first client came online.

Possible reasons
TKIP is used to authenticate all clients.
Channel changed.
BssDelAllSta event logged off client normally.
AP down.
Radio down.
Service template disabled.
Service template unbound.
Created BSS during master AC switchover process.
Updated BSS base information when BSS was in deactive state.
Intrusion protection.
Local AC or AP deleted BSS.
BssDelAllSta event logged off client abnormally.
Received VLAN deleted event.
CM received message for logging off client from AM.
The **`reset wlan client`** command was executed to log off the client.
Deleted private data on AP: DBM database recovered.
Failed to synchronize authentication succeeded message downstream.
Client RSSI was lower than the threshold and was decreasing.
Configured whitelist for the first time or executed the **`reset wlan client all`** command.
Received client offline websocket message.
WMAC logged off all clients associated with the radio.
Timer for sending deassociation message timed out.
The client is in blacklist or deleted from whitelist.
Client was added to the dynamic blacklist.
Failed to roam out.
Implemented inter-AC roaming for the first time.
Successfully roamed to another BSS.
Failed to roam in.
Roaming process received a message for logging off the client.
Roaming process processed Down event and logged off roam-in clients.
Roaming failure.
Successfully performed roaming but failed to recover authentication data.
Roaming timed out.
Seamless roaming failed.
Logged off clients that performed inter- or intra-AC roaming.
Failed to process AccessCtrlChk. Configure permitted AP group or permitted SSID.
Synchronized client information to process and logged off client.

Possible reasons
Failed to synchronize client state to uplink devices.
Local AC or remote AP received Add Mobile message updated BSS and logged off clients.
Upgraded HA and logged off all clients.
Synchronized BSS data during master/backup AC switchover process.
Failed to synchronize service template data during master/backup AC switchover process.
BSS aging timer timed out.
Remote AP deleted non-local forwarding BSS.
Failed to find configuration data when synchronizing data.
BSS was deleted: BSS synchronization examination failed or there was no BSS data to be updated.
Failed to get BSS by using WLAN ID.
Unbound inherited service template.
STAMGR process was down automatically or manually.
Deleted redundant clients.
Failed to process authorized doing nodes.
Authorization failed.
NSS value in Operating Mode Notification Action packet doesn't support mandatory VHT-MCS.
Number of sent SA requests exceeded the permitted threshold.
Local AC came online again and deleted all clients associated with the BSS.
Failed to upgrade hot-backup.
The illegally created BSS was deleted.
Failed to process requests when receiving UserAuth Success message.
Failed to get AP type when receiving UserAuth Successful message.
Failed to notify client of the recovery of basic client data from database.
Failed to recover basic client data from database.
Client already existed when the AC received Auth packet from the client and checked online clients.
Client already existed during FT Over-the-DS authentication.
SKA authentication failed.
Deadline timer timed out during FT authentication.
Failed to send the response for the successful shared key authentication to the client.
Failed to get FT data during FT authentication.
FT authentication was performed and BSS does not support FT.
Failed to process FT authentication-success result.
Failed to process FT authentication.
Maximum number of clients already reached when remote request message was received.
Failed to fill authorization information while processing authorization message.
Failed to process key negotiation during 802.1X authentication.
Invalid session key length during 802.1X authentication.

Possible reasons
802.1X authentication failed.
802.1X server was unreachable.
User timer timed out during 802.1X authentication.
Server timer timed out during 802.1X authentication.
802.1X authentication configuration error.
Received nonexistent authorization VLAN group during 802.1X authentication.
MAC authentication failed.
MAC server was unreachable.
Session time is zero during MAC authentication.
Server timer timed out during MAC authentication.
802.1X authentication failed and the return code is *code*.
MAC authentication failed and the return code is *code*.
Authorization failed for 802.1X authentication and the return code is *code*.
Authorization failed for MAC authentication and the return code is *code*.
Accounting start failed for 802.1X authentication and the return code is *code*.
Accounting start failed for MAC authentication and the return code is *code*.
Accounting update failed for 802.1X authentication and the return code is *code*.
Accounting update failed for MAC authentication and the return code is *code*.
Failed to receive client EAP request for 802.1X authentication.
Failed to receive server response for 802.1X authentication.
Failed to receive server response for MAC authentication.
Received client log-off packet during 802.1X authentication.
802.1X client handshake failed.
Incorrect 802.1X authentication method.

STAMGR_CLIENT_OFFLINE

Message text	Client [STRING] went offline from BSS [STRING] with SSID [STRING] on AP [STRING] Radio ID [STRING]. State changed to Unauth. Reason [STRING]
Variable fields	$1: MAC address of the client. $2: BSSID. $3: SSID defined in the service template. $4: Name of the AP associated with the client. $5: ID of the radio associated with the client. $6: Reason why the client goes offline. Table 20 describes the possible reasons.
Severity level	6
Example	STAMGR/6/STAMGR_CLIENT_OFFLINE: Client 0023-8933-2147 went offline from BSS 0023-12ef-78dc with SSID abc on AP ap1 Radio ID 2. State changed to Unauth. Reason: Radio down.
Explanation	The client went offline from the BSS for a specific reason. The state of the client changed to Unauth.
Recommended action	To resolve the issue: **359.** Examine whether the AP and its radios operate correctly if the client went offline abnormally. If the logoff was requested by the client, no action is required. **360.** If they do not operate correctly, check the debugging information to locate the issue and resolve it. **361.** If the issue persists, contact NSFOCUS Support.

Table 20 Possible logoff reasons

Possible reasons
Received disassociation frame in Run state: reason code=String.
Unknown reason.
Different old and new region codes.
Failed to update IGTK.
Failed to update GTK.
Failed to generate IGTK when the first client came online.
TKIP is used to authenticate all clients.
Channel changed.
BssDelAllSta event logged off client normally.
Radio down.
Service template disabled.
Service template unbound.
Created BSS during master/backup AC switchover process.
Updated BSS base information when BSS was in deactive state.
Intrusion protection.
Local AC or AP deleted BSS.

Possible reasons
BssDelAllSta event logged off client abnormally.
Received VLAN deleted event.
CM received message for logging off client from AM.
The **reset wlan client** command was executed to log off the client.
DBM database failed to recover client operation data.
Deleted private data on AP: DBM database recovered.
Received deauthentication frame in Run state: reason code=String.
Failed to process (re)association request in Run state.
Unmatched authentication algorithm in received authentication message.
Idle timer timeout.
Keepalive timer timeout.
Received authentication failure message.
Failed to synchronize authentication succeeded message downstream.
Client RSSI was lower than the threshold and was marked as decreasing.
Configured whitelist for the first time or executed the **reset wlan client all** command.
Received client offline websocket message.
WMAC logged off all clients associated with the radio.
Timer for sending disassociation message timed out.
The client is in blacklist or deleted from whitelist.
Client was added to the dynamic blacklist.
Failed to roam out.
Implemented inter-AC roaming for the first time.
Successfully roamed to another BSS.
Failed to roam in.
Roaming process received a message for logging off the client.
Roaming process processed Down event and logged off roam-in clients.
Roaming failure.
Successfully performed roaming but failed to recover authentication data.
Roaming timed out.
Seamless roaming failed.
Logged off clients that performed inter- or intra-AC roaming.
Failed to process AccessCtrlChk when configured permitted AP group or permitted SSID.
Synchronized client information to process and logged off client in Run state.
Failed to synchronize client state to uplink/downlink devices.
Local AC or remote AP received add mobile message, updated BSS, and logged off clients in Run state.
Upgraded HA and logged off all clients.
Synchronized BSS data during master/backup AC switchover process.

Possible reasons
Failed to synchronize service template data during master/backup AC switchover process.
BSS aging timer timed out.
Remote AP deleted non-local forwarding BSS.
Failed to find configuration data when synchronizing data.
BSS was deleted: BSS synchronization examination failed or there was no BSS data to be updated.
Failed to get BSS by using WLAN ID.
Unbound inherited service template.
STAMGR process was down automatically or manually.
Deleted redundant clients.
Failed to process authorized doing nodes.
Authorization failed.
NSS value in Operating Mode Notification Action packet doesn't support mandatory VHT-MCS.
Number of sent SA requests exceeded the permitted threshold.
Fit AP received message for deleting the client.
Local AC came online again and deleted all clients associated with the BSS.
Failed to upgrade hot backup.
The illegally created BSS was deleted.
Failed to process requests when receiving UserAuth Success message.
Failed to get AP type when receiving UserAuth Success message.
The client doesn't support mandatory rate.
Disabled access services for 802.11b clients.
The client doesn't support mandatory VHT-MCS.
Enabled the client dot11ac-only feature.
Disabled MUTxBF.
Disabled SUTxBF.
The client doesn't support mandatory MCS.
Channel bandwidth changed.
Disabled the client dot11n-only feature.
Disabled short GI.
Disabled the A-MPDU aggregation method.
Disabled the A-MSDU aggregation method.
Disabled STBC.
Disabled LDPC.
The MIMO capacity decreased, and the MCS supported by the AP can't satisfy the client's negotiated MCS.
The MIMO capacity decreased, and the VHT-MCS supported by the AP can't satisfy the client's negotiated VHT-MCS.
Hybrid capacity increased, which kicked off clients associated with other radios with lower Hybrid capacity.

Possible reasons
Failed to add MAC address.
The roaming entry doesn't exist while the AC was processing the roaming request during client smooth reconnection.
Home AC processed the move out response message to update the roaming entry and notified the foreign AC to force the client offline during an inter-AC roaming.
The associated AC left from the mobility group and deleted roam-in entries and roaming entries of the client.
Executed the **`reset wlan mobility roaming`** command.
Kicked client because of roaming to another BSSID.
The roaming entry doesn't exist while the AC was processing the Add Preroam message during client smooth reconnection.
Deleted roaming entries of clients in the fail VLAN while processing a fail VLAN delete event.
Deleted the roaming entry of the client while processing a client delete event.
Moving to another SSID on the same radio.
Kicked off the client because Oasis platform microservice deleted the password entry.
Time expired for learning client IPv4 address through DHCP.
AP triggered (idle timeout).
AP triggered (channel change).
AP triggered (bandwidth change).
Received log-off packet from 802.1X authentication client.
802.1X client handshake failed.
Accounting update timed out for the 802.1X authentication client.
Accounting update timed out for the MAC authentication client.
802.1X authentication client idle cut on AP.
MAC authentication client idle cut on AP.
Session timeout timer expired for the 802.1X authentication client.
Session timeout timer expired for the MAC authentication client.
Received client disassociation message from server for the 802.1X authentication client.
Received client disassociation message from server for the MAC authentication client.
Received nonexistent authorization VLAN group for the 802.1X authentication client.
Received nonexistent authorization VLAN group for the MAC authentication client.
Total client traffic failed to reach the minimum traffic threshold.
Failed to obtain the client IP address before the accounting delay timer expired.

STAMGR_CLIENT_ONLINE

Message text	Client [STRING] went online from BSS [STRING] VLAN [STRING] with SSID [STRING] on AP [STRING] Radio ID [STRING]. State changed to Run.
Variable fields	$1: MAC address of the client. $2: BSSID. $3: VLAN ID. $4: SSID defined in the service template. $5: Name of the AP associated with the client. $6: ID of the radio associated with the client.
Severity level	6
Example	STAMGR/6/STAMGR_CLIENT_ONLINE: Client 0023-8933-2147 went online from BSS 0023-12ef-78dc VLAN 1 with SSID abc on AP ap1 Radio ID 2. State changed to Run.
Explanation	The client came online from the BSS. The state of the client changed to Run.
Recommended action	No action is required.

STAMGR_CLIENT_SNOOPING

Message text	Detected client IP change: Client MAC: [SRTING], IP: [STRING], [STRING], [STRING], Username: [STRING], AP name: [STRING], Radio ID [UCHAR], Channel number: [UINT32], SSID: [STRING], BSSID: [STRING].
Variable fields	$1: MAC address of the client. $2: Current IP address of the client. $3: Used IP address of the client. $4: Used IP address of the client. $5: Username of the client. $6: Name of the AP associated with the client. $7: ID of the radio associated with the client. $8: ID of the channel used by the client. $9: SSID of the service template associated with the client. $10: BSSID of the service template associated with the client.
Severity level	6
Example	STAMGR_CLIENT_SNOOPING: Detected client IP change: Client MAC: 31ac-11ea-17ff,IP: 4.4.4.4, IP: 1.1.1.1, IP: 2.2.2.2,IP: -NA-,User name: test, AP name: ap1, Radio ID: 1, Channel number: 161,SSID: 123, BSSID: 25c8-3dd5-261a.
Explanation	IP change was detected for a specific client.
Recommended action	No action is required.

STAMGR_DELBAC_INFO

Message text	Delete BAS AC [STRING].
Variable fields	$1: MAC address of the BAS AC.
Severity level	6
Example	STAMGR/6/STAMGR_DELBAC_INFO: Delete BAS AC 3ce5-a616-28cd.
Explanation	The BAS AC was disconnected from the master AC.
Recommended action	No action is required.

STAMGR_DELSTA_INFO

Message text	Delete client [STRING].
Variable fields	$1: MAC address of the client.
Severity level	6
Example	STAMGR/6/STAMGR_DELSTA_INFO: Delete client 3ce5-a616-28cd.
Explanation	The client was disconnected from the BAS AC.
Recommended action	No action is required.

STAMGR_MACA_LOGIN_FAILURE

Message text	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; A user failed MAC authentication. Reason: [STRING].

Variable fields	$1: Username.
	$2: MAC address of the client.
	$3: SSID.
	$4: Name of the AP associated with the client.
	$5: ID of the radio associated with the client.
	$6: VLAN ID.
	$7: Username format:
	• fixed.
	• MAC address.
	$8: Reason for the authentication failure:
	• AAA processed authentication request and returned error code *code*.
	  ○ **4**—Represents one of the following errors: nonexistent authentication domain, service type error, or incorrect username or password.
	  ○ **8**—Represents one of the following errors: no IP addresses are added to the authentication server, preshared keys configured on the authentication server are different from preshared keys configured on the device, or the authentication server and the device cannot reach each other.
	  ○ **26**—Configuration error exists in the authentication domain.
	• AAA processed authorization request and returned error code *code*.
	  ○ **8**—The authentication server and the device cannot reach each other.
	• Client timeout timer expired.
	• Received user security information and kicked off the client.
	• Accounting-update timer expired, and no responses were received from the server.
	• Kicked off the client when the idle timeout timer expired.
	• Authentication method error.
	• Kicked off the client because the server-assigned session timeout timer is 0.
	• Received session disconnection event.
	• Received nonexistent authorization VLAN group.
	• Client kicked out on expiration of the idle-cut timer because its total traffic had not reached the required minimum amount of traffic.
	• Had failed to obtain the client IP address before the accounting delay timer expired.
	• Unknown reason.

Severity level	5
Example	STAMGR/5/STAMGR_MACA_LOGIN_FAILURE:-Username=MAC-UserMAC=3ce5-a616-28cd-SSID=text-wifi-APName=ap1-RadioID=2-VLANID=11-UsernameFormat=fixed; A user failed MAC authentication. Reason: AAA processed authentication request and returned error code 8.
Explanation	The client failed to pass MAC authentication for a specific reason.
Recommended action	To resolve the issue: **362.** Examine the network connection between the device and the AAA server. **363.** Verify that the AAA server works correctly. **364.** Verify that the AAA server is configured with the correct username and password.

	365. Troubleshoot errors one by one according to the returned error code during authentication. **366.** If the issue persists, contact NSFOCUS Support.

STAMGR_MACA_LOGIN_SUCC

Message text	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; A user passed MAC authentication and came online.
Variable fields	$1: Username. $2: MAC address of the client. $3: SSID. $4: Name of the AP associated with the client. $5: ID of the radio associated with the client. $6: VLAN ID. $7: Username format: • fixed. • MAC address.
Severity level	6
Example	STAMGR/6/STAMGR_MACA_LOGIN_SUCC:-Username=MAC-UserMAC=3ce5-a616-28cd-SSID=text-wifi-APName=ap1-RadioID=2-VLANID=11-UsernameFormat=fixed; A user passed MAC authentication and came online.
Explanation	The client came online after passing MAC authentication.
Recommended action	No action is required.

STAMGR_MACA_LOGOFF

Message text	-Username=[STRING]-UserMAC=[STRING]-SSID=[STRING]-APName=[STRING]-RadioID=[STRING]-VLANID=[STRING]-UsernameFormat=[STRING]; Session for a MAC authentication user was terminated. Reason: [STRING].
Variable fields	$1: Username. $2: MAC address of the client. $3: SSID. $4: Name of the AP associated with the client. $5: ID of the radio associated with the client. $6: VLAN ID. $7: Username format: • fixed. • MAC address. $6: Reason why the client is logged off. • AAA processed authentication request and returned error code *code*. *Server reason: reason*. The *reason* field represents the reason returned from the server and is available only when the server returned a reason. Available error codes include: ○ **4**—Represents one of the following errors: nonexistent authentication domain, service type error, or incorrect username or password. ○ **8**—Represents one of the following errors: no IP addresses are added to the authentication server, preshared keys configured on the authentication server are different from preshared keys configured on the device, or the authentication server and the device cannot reach each other. ○ **26**—Configuration error exists in the authentication domain. • AAA processed authorization request and returned error code *code*. *Server reason: reason*. The *reason* field represents the reason returned from the server and is available only when the server returned a reason. Available error codes include: ○ **8**—The authentication server and the device cannot reach each other. • AAA processed accounting-start request and returned error code *code*. *Server reason: reason*. The *reason* field represents the reason returned from the server and is available only when the server returned a reason. Available error codes include: ○ **8**—The authentication server and the device cannot reach each other. • AAA processed accounting-update request and returned error code *code*. *Server reason: reason*. The *reason* field represents the reason returned from the server and is available only when the server returned a reason. Available error codes include: ○ **8**—The authentication server and the device cannot reach each other. • Client timeout timer expired. • Received user security information and kicked off the client. • Lost in shaking hands. • Accounting-update timer expired, and no responses were received from the server. • Kicked off the client when the idle timeout timer expired. • Authentication method error. • Kicked off the client because the server-assigned session timeout timer is

	0. • Received session disconnection event. • Received disassociation frame in Run state: reason code=*code*. • Received deauthentication frame in Run state: reason code=*code*. • Received disassociation packet in Userauth state. • Received deauthentication packet in Userauth state. • Received client failure message with reason code=*code*. • Received client offline message with reason code=*code*. • Unknown reason.
Severity level	6
Example	STAMGR/6/STAMGR_MACA_LOGOFF:-Username=MAC-UserMAC=3ce5-a616-28cd-SSID=text-wifi-APName=ap1-RadioID=2-VLANID=11-UsernameFormat=fixed; Session for a MAC authentication user was terminated. Reason: Received user security information and kicked off the client.
Explanation	The MAC authenticated client was logged off for a specific reason.
Recommended action	To resolve the issue: **367.** Check the debugging information to locate the logoff cause and remove the issue. If the logoff was requested by the client, no action is required. **368.** If the issue persists, contact NSFOCUS Support.

STAMGR_ROAM_FAILED

Message text	Client [MAC] on AP [STRING] Radio ID [STRING] failed to roam with reason code [UINT32].
Variable fields	$1: MAC address of the client. $2: Name of the AP associated with the client. $3: ID of the radio associated with the client. $4: Reason code for the roaming failure: • **1**—Failed to select a roaming policy. • **2**—Insufficient memory resources. • **3**—Network communication failures. • **4**—Lack of local roaming entries. • **5**—Failed to add a VLAN.
Severity level	4
Example	STAMGR/4/STAMGR_ROAM_FAILED: Client 001f-3ca8-1092 on AP ap1 Radio ID 2 failed to roam with reason code 1.
Explanation	The client failed to roam for a specific reason.
Recommended action	To resolve the issue, depending on the reason code: • **1**—Use the **display wlan client verbose** command to verify that the authentication method has changed. • **2**—Use the **display process memory** command to check memory resource usage for each module. • **3**—Use the **display wlan mobility group** command to check the IACTP tunnel state. • **4**—Use the **display wlan mobility group** command to check the IACTP tunnel state. • **5**—Check the **trace.log** file for VLAN adding failure reason.

STAMGR_ROAM_SUCCESS

Message text	Client [MAC] roamed from BSSID [MAC] on AP [STRING] Radio ID [STRING] of AC IP [IPADDR] to BSSID [MAC] on AP [STRING] Radio ID [STRING] of AC IP [IPADDR] successfully.
Variable fields	$1: MAC address of the client. $2: BSSID of the AP associated with the client before roaming. $3: Name of the AP associated with the client before roaming. $4: ID of the radio associated with the client before roaming. $5: IP address of the AC associated with the client before roaming. $6: BSSID of the AP associated with the client after roaming. $7: Name of the AP associated with the client after roaming. $8: ID of the radio associated with the client after roaming. $9: IP address of the AC associated with the client after roaming.
Severity level	6
Example	STAMGR/6/STAMGR_ROAM_SUCCESS: Client 0021-005f-dffd roamed from BSSID 000f-e289-6ad0 on AP ap1 Radio ID 2 of AC IP 172.25.0.81 to BSSID 000f-e2ab-baf0 on AP ap2 Radio ID 2 of AC IP 172.25.0.82 successfully.
Explanation	The client roamed successfully.
Recommended action	No action is required.

STAMGR_SERVICE_FAILURE

Message text	Service failure occurred on BSS [STRING] after service template [STRING] with SSID [STRING] was bound to radio [STRING] on AP [STRING] with AP ID [STRING]. Reason: [STRING], code=0x[STRING].
Variable fields	$1: BSSID. $2: Name of the service template. $3: SSID defined in the service template. $4: Radio ID. $5: AP name. $6: AP ID. $7: Reason for the service failure, as described in Table 21. $8: Error code.
Severity level	6
Example	STAMGR/6/SERVICE_FAILURE: Service failure occurred on BSS 0023-12ef-78dc after service template st1 with SSID st1ssid was bound to radio 1 on AP ap1 with AP ID 1. Reason: Failed to activate BSS when AP came online, code=0x61140001.
Explanation	After the AP came online, BSS activation failed for a specific reason with error code 0x61140001.
Recommended action	To resolve the issue: **369.** Check the debugging information to locate the failure cause and remove the issue. **370.** If the issue persists, contact NSFOCUS Support.

Table 21 Possible service failure reasons

Possible reasons
Failed to create a BSS interface during smooth BSS interface creation.
Replied with failure to transmit interface creation node during smooth BSS interface creation.
Failed to set forwarding location during smooth recovery of AP data.
Failed to initiate a series of locations during smooth recovery of AP data.
Failed to send message of creating BSS interface to worker thread during smooth recovery of AP data.
Failed to create handle during smooth recovery of AP data.
Failed to activate BSS during smooth recovery of AP data.
Failed to set kernel forwarding table during smooth recovery of AP data.
Failed to create BSS node when AP came online.
Failed to create BSS handle when AP came online.
Insufficient memory for creating BSS node when AP came online.
Failed to get radio private data while creating BSS node in general process.
Failed to initiate a series of locations while creating BSS node in general process.
Failed to set kernel forwarding table while creating BSS node in general process.
Failed to create BSS node during smooth recovery of BSS data.
Failed to get AP location while recovering BSS running data from DBM.
Failed to get radio private data while recovering BSS running data from DBM.
Failed to add BSS index to interface index while recovering BSS running data from DBM.
Failed to create BSS handle when hierarchy device received Add WLAN message.
Failed to initiate a series of locations when hierarchy device received Add WLAN message.
Failed to set forwarding location when hierarchy device received Add WLAN message.
Failed to send message to worker thread when hierarchy device received Add WLAN message.
Failed to set kernel forwarding table when hierarchy device received Add WLAN message.
Failed to activate BSS when hierarchy device received Add WLAN message.
Failed to issue Add WLAN message when hierarchy device received Add WLAN message.
Failed to activate BSS when service template was bound.
Failed to create BSS node when service template was bound.
Failed to create BSS handle when service template was bound.
Failed to add bind node to mapped radio list of the service template while recovering service template binding information for service thread from pending database.
Failed to create BSS node while recovering service template binding information for service thread from pending database.
Failed to add bind node to mapped radio list of the service template while creating BSS from Merger.
Failed to create BSS node while creating BSS from Merger.
Failed to apply for memory while creating BSS node.
Failed to calculate BSSID while creating BSS node.
Service thread received interface creation failure while creating BSS interface during smooth recovery of AP

Possible reasons
data.
Failed to add BSS index to interface index while creating BSS interface during smooth recovery of AP data.
Failed to add VLAN on the interface while creating BSS interface during smooth recovery of AP data.
Failed to set the source MAC address of the interface while creating BSS interface during smooth recovery of AP data.
Failed to set kernel forwarding table while creating BSS interface during smooth recovery of AP data.
Failed to activate BSS while creating BSS interface during smooth recovery of AP data.
Replied with failure to transmit interface creation node when hierarchy device created an interface accordingly.
Failed to create BSS interface when BSS created an interface accordingly.
Failed to add BSS index to interface index when BSS created an interface accordingly.
Failed to add VLAN on the interface when BSS created an interface accordingly.
Failed to set source MAC address of the interface when BSS created an interface accordingly.
Failed to set kernel forwarding table when BSS created an interface accordingly.
Failed to issue ADD BSS message when BSS created an interface accordingly.
Replied with failure to transmit interface creation node when hierarchy device created an interface accordingly for an invalid interface.
Created BSS rollback for failed resources while issuing ADD BSS message callback.
Failed to enable packet socket while recovering BSS running data from DBM.
Failed to create BSS node while recovering BSS running data from DBM.
Failed to initiate BSS while creating BSS node.
Failed to activate BSS when service template was enabled.
Invalid BSS interface index while upgrading BSS with AP private data.
Failed to upgrade backup BSS to real BSS while upgrading BSS with AP private data.
Failed to set kernel forwarding table while upgrading BSS with AP private data.
Failed to activate BSS while upgrading BSS with AP private data.
Invalid BSS interface index while upgrading BSS without AP private data.
Failed to set kernel forwarding table while upgrading BSS without AP private data.
Failed to activate BSS while upgrading BSS without AP private data.
Failed to create BSS interface while creating general BSS process.
Failed to activate BSS during smooth recovery of BSS data.
Failed to activate BSS while recovering service template binding information for service thread from pending database.
Failed to activate BSS while creating BSS from Merger.
Failed to activate BSS when AP came online.
Failed to activate BSS when other module sent activation request.
Failed to activate BSS when other module received activation request.
Failed to send response node of creating interface while creating interface during smooth recovery of AP data.

Possible reasons
Failed to add BSS index to interface index when hierarchy device created an interface accordingly.
Failed to add VLAN on the interface when hierarchy device created an interface accordingly.
Failed to set source MAC address of the interface when hierarchy device created an interface accordingly.
Failed to set kernel forwarding table when hierarchy device created an interface accordingly.
Failed to activate BSS when hierarchy device created an interface accordingly.
Failed to issue Add BSS message when hierarchy device created an interface accordingly.
Insufficient memory when hierarchy device received BSS creation message.
Failed to fill BSS basic data when hierarchy device received BSS creation message.
Failed to initiate BSS service phase when hierarchy device received BSS creation message.
Failed to receive Add WLAN message when hierarchy device received BSS creation message.
Failed to get radio private data because of invalid AP ID when hierarchy device received BSS creation message.
Failed to get radio private data because of invalid radio ID when hierarchy device received BSS creation message.
Failed to get radio private data when hierarchy device received Add WLAN message.
Failed to issue message when hierarchy device received Add WLAN message.
Failed to get BSS data through WLAN ID during smooth recovery of BSS data.
Failed to issue Add WLAN message while creating BSS node in general process.
Failed to create BSS interface when hierarchy device created an interface accordingly.
Failed to create BSS interface when hierarchy device created an interface accordingly for an invalid interface.
Failed to set forwarding location while creating BSS node in general process.
Replied with failure to transmit interface creation node when BSS created an interface accordingly.
Failed to update BSS key data when hierarchy device received Add WLAN message.
Replied with failure to transmit interface creation node when BSS created an interface accordingly for an existing BSS.

STAMGR_SERVICE_OFF

Message text	BSS [STRING] was deleted after service template [STRING] with SSID [STRING] was unbound from radio [STRING] on AP [STRING]. Reason: [STRING].
Variable fields	$1: BSSID. $2: Name of the service template. $3: SSID defined in the service template. $4: Radio ID. $5: AP name. $6: Reason for the BSS deletion. • Unknown reason. • AP down. • Deleted BSS with the Delete mark when inter-AC BSS smooth ended. • Hierarchy device received BSS delete message. • Deleted AP private data from APMGR when AP smooth ended. • WLAS was triggered, and service was shut down temporarily. • Intrusion protection was triggered, and service was shut down permanently. • Service module received Update WLAN message when BSS was inactive. • Disabled service template. • Unbound service template. • Deleted BSS with the Delete mark when inter-AC AP smooth ended. • BSS aging timer timed out. • Deleted non-local forwarding BSS when AP enabled with remote AP went offline. • Failed to find configuration data while synchronizing data. • AP did not come online or service template was disabled. • Failed to find the WLAN ID from APMGR while BSS was smoothing WLAN ID. • Unbound inherited service template. • The stamgr process became down automatically or was shut down manually. • Failed to use AP private data to upgrade backup BSS. • Failed to upgrade backup BSS. • Failed to synchronize service template data to the Merger bind list while upgrading backup data.
Severity level	6
Example	STAMGR/6/SERVICE_OFF: BSS 0023-12ef-78dc was deleted after service template st1 with SSID st1ssid was unbound from radio 1 on AP ap1. Reason: Failed to find configuration data while synchronizing data.
Explanation	The BSS was deleted for a specific reason.
Recommended action	To resolve the issue: **371.** Verify that the BSS is deleted as requested. If the BSS is deleted as requested, no action is required. **372.** Locate the deletion cause and remove the issue if the BSS is deleted abnormally, **373.** If the issue persists, contact NSFOCUS Support.

STAMGR_SERVICE_ON

Message text	BSS [STRING] was created after service template [STRING] with SSID [STRING] was bound to radio [STRING] on AP [STRING].
Variable fields	$1: BSSID. $2: Name of the service template. $3: SSID defined in the service template. $4: Radio ID. $5: AP name.
Severity level	6
Example	STAMGR/6/SERVICE_ON: BSS 0023-12ef-78dc was created after service template st1 with SSID 1 was bound to radio 1 on AP ap1.
Explanation	The BSS was created.
Recommended action	No action is required.

STAMGR_STA_ADDMOB_LKUP_ENDOFIOCTL

Message text	APID=[UINT32]-MAC=[STRING]-BSSID=[STRING]; AC doesn't need to send client information to uplink device: Client information already arrived at the end of the IOCTL tunnel.
Variable fields	$1: ID of the AP associated with the client. $2: MAC address of the client. $3: BSSID of the service template associated with the client.
Severity level	7
Example	STAMGR/7/STAMGR_STA_ADDMOB_LKUP_ENDOFIOCTL: APID=667-MAC=d4f4-6f69-d7a1-BSSID=600b-0301-d5a0; The AC doesn't need to send client information to uplink device: Client information already arrived at the end of the IOCTL tunnel.
Explanation	The AC does not need to send client information to the uplink device because client information already arrived at the end of the IOCTL tunnel.
Recommended action	To resolve the issue depending on the network infrastructure: • **Fit AP+AC network**—No action is required if this message is output. If no message is output, locate the issue according to the debugging information and resolve the issue. • **AC hierarchical network**—No action is required if this message is output by the central AC. If this message is output by a local AC, locate the issue according to the debugging information and resolve the issue.

STAMGR_STAIPCHANGE_INFO

Message text	IP address of client [STRING] changed to [STRING].
Variable fields	$1: MAC address of the client. $2: New IP address of the client.
Severity level	6
Example	STAMGR/6/STAMGR_STAIPCHANGE_INFO: IP address of client 3ce5-a616-28cd changed to 4.4.4.4.
Explanation	The IP address of the client was updated.
Recommended action	No action is required.

STAMGR_TRIGGER_IP

Message text	-SSID=[STRING]-UserMAC=[STRING]-APName=[STRING]-RadioID=[STRING]-VLANID=[STRING]; Intrusion protection triggered. Action: [STRING].
Variable fields	$1: SSID. $2: MAC address of the client. $3: Name of the AP associated with the client. $4: ID of the radio associated with the client. $5: ID of the access VLAN. $6: Action: • Added the user to the blocked MAC address list. • Closed the user's BSS temporarily. • Closed the user's BSS permanently.
Severity level	5
Example	STAMGR/5/STAMGR_TRIGGER_IP:-SSID=text-wifi-UserMAC=3ce5-a616-28cd-APName=ap1-RadioID=2-VLANID=11; Intrusion protection triggered, the intrusion protection action: added a user to the list of Block-MAC.
Explanation	Intrusion protection was triggered and the action was displayed.
Recommended action	No action is required.

STM messages

This section contains IRF messages.

STM_AUTO_UPDATE_FAILED

Message text	Pattern 1: Slot [UINT32] auto-update failed. Reason: [STRING]. Pattern 2: Chassis [UINT32] slot [UINT32] auto-update failed. Reason: [STRING].
Variable fields	Pattern 1: $1: IRF member ID. $2: Failure reason: ○ **Timeout when loading**—The IRF member device failed to complete loading software within the required time period. ○ **Wrong description when loading**—The file description in the software image file does not match the current attributes of the software image. This issue might occur when the file does not exist or is corrupted. ○ **Disk full when writing to disk**—The subordinate device does not have sufficient storage space. Pattern 2: $1: IRF member ID. $2: Slot number of an MPU. $3: Failure reason: ○ **Timeout when loading**—The MPU failed to complete loading software within the required time period. ○ **Wrong description when loading**—The file description in the software image file does not match the current attributes of the software image. This issue might occur when the file does not exist or is corrupted. ○ **Disk full when writing to disk**—The MPU does not have sufficient storage space.
Severity level	4
Example	STM/4/STM_AUTO_UPDATE_FAILED: Slot 5 auto-update failed. Reason: Timeout when loading.
Explanation	Pattern 1: Software synchronization from the master failed on a subordinate device. Pattern 2: Software synchronization from the global active MPU failed on a standby MPU.
Recommended action	**374.** Remove the issue depending on the failure reason: ○ If the failure reason is **Timeout when loading**, verify that all IRF links are up. ○ If the failure reason is **Wrong description when loading**, download the software images again. ○ If the failure reason is **Disk full when writing to disk**, delete unused files to free the storage

		space. **375.** Upgrade software manually for the device or MPU to join the IRF fabric, and then connect the device to the IRF fabric.

STM_AUTO_UPDATE_FINISHED

Message text	Pattern 1: File loading finished on slot [UINT32]. Pattern 2: File loading finished on chassis [UINT32] slot [UINT32].
Variable fields	Pattern 1: $1: IRF member ID. Pattern 2: $1: IRF member ID. $2: Slot number of an MPU.
Severity level	5
Example	STM/5/STM_AUTO_UPDATE_FINISHED: File loading finished on slot 3.
Explanation	Pattern 1: The member device finished loading software images. Pattern 2: The MPU finished loading software images.
Recommended action	No action is required.

STM_AUTO_UPDATING

Message text	Pattern 1: Don't reboot the slot [UINT32]. It is loading files. Pattern 2: Don't reboot the chassis [UINT32] slot [UINT32]. It is loading files.
Variable fields	Pattern 1: $1: IRF member ID. Pattern 2: $1: IRF member ID. $2: Slot number of an MPU.
Severity level	5
Example	STM/5/STM_AUTO_UPDATING: Don't reboot the slot 2. It is loading files.
Explanation	Pattern 1: The member device is loading software images. To avoid software upgrade failure, do not reboot the member device. Pattern 2: The MPU is loading software images. To avoid software upgrade failure, do not reboot the MPU.
Recommended action	No action is required.

STM_HELLOPKT_NOTSEND

Message text	Hello thread hasn't sent packets for [UINT32] seconds.
Variable fields	$1: Time value.
Severity level	5
Example	STM/5/STM_HELLOPKT_NOTSEND: Hello thread hasn't sent packets for 10 seconds.
Explanation	The hello thread has not sent packets for a period of time. When you receive this message, identify the cause of the issue as soon as possible. If this situation persists and causes the failure of heatbeat detection between IRF fabric members, the IRF fabric will split.
Recommended action	This issue typically occurs when the Hello thread cannot obtain CPU time. To resolve this issue: **376.** Execute the **display cpu-usage** command in short intervals to identify the CPU usage. **377.** If high CPU usage persists, check for attacks or abnormal processes and decrease the CPU usage to the acceptable range. **378.** If the issue persists, contact NSFOCUS Support.

STM_HELLOPKT_NOTRCV

Message text	Hello thread hasn't received packets for [UINT] seconds.
Variable fields	$1: Time value.
Severity level	5
Example	STM/5/STM_HELLOPKT_NOTRCV: Hello thread hasn't received packets for 10 seconds.
Explanation	The hello thread has not received packets for a period of time. When you receive this message, identify the cause of the issue as soon as possible. If this situation persists and causes the failure of heatbeat detection between IRF fabric members, the IRF fabric will split.
Recommended action	**379.** Execute the **display irf link** command to verify that the state of IRF links is correct. **380.** Execute the **display irf topology** command to verify that the neighbor state is correct. **381.** Verify that the neighbor devices have sent hello packets to the local device. **382.** If a neighbor device has not sent hello packets to the local device for a period of time, check its log for the STM_HELLOPKT_NOTSEND message. **383.** Take the recommended action for the message to resolve the issue.

STM_LINK_DOWN

Message text	IRF port [UINT32] went down.
Variable fields	$1: IRF port name.
Severity level	3
Example	STM/3/STM_LINK_DOWN: IRF port 2 went down.
Explanation	This event occurs when all physical interfaces bound to an IRF port are down.
Recommended action	Check the physical interfaces bound to the IRF port. Make sure a minimum of one member physical interface is up.

STM_LINK_TIMEOUT

Message text	IRF port [UINT32] went down because the heartbeat timed out.
Variable fields	$1: IRF port name.
Severity level	2
Example	STM/2/STM_LINK_TIMEOUT: IRF port 1 went down because the heartbeat timed out.
Explanation	The IRF port went down because of heartbeat timeout.
Recommended action	Check the IRF link for link failure.

STM_LINK_UP

Message text	IRF port [UINT32] came up.
Variable fields	$1: IRF port name.
Severity level	6
Example	STM/6/STM_LINK_UP: IRF port 1 came up.
Explanation	An IRF port came up.
Recommended action	No action is required.

STM_MERGE

Message text	IRF merge occurred.
Variable fields	N/A
Severity level	4
Example	STM/4/STM_MERGE: IRF merge occurred.
Explanation	IRF merge occurred.
Recommended action	No action is required.

STM_MERGE_NEED_REBOOT

Message text	IRF merge occurred. This IRF system needs a reboot.
Variable fields	N/A
Severity level	4
Example	STM/4/STM_MERGE_NEED_REBOOT: IRF merge occurred. This IRF system needs a reboot.
Explanation	You must reboot the current IRF fabric for IRF merge, because it failed in the master election.
Recommended action	Log in to the IRF fabric, and use the **reboot** command to reboot the IRF fabric.

STM_MERGE_NOT_NEED_REBOOT

Message text	IRF merge occurred. This IRF system does not need to reboot.
Variable fields	N/A
Severity level	5
Example	STM/5/STM_MERGE_NOT_NEED_REBOOT: IRF merge occurred. This IRF system does not need to reboot.
Explanation	You do not need to reboot the current IRF fabric for IRF merge, because it was elected the master.
Recommended action	Reboot the IRF fabric that has failed in the master election to finish the IRF merge.

STM_SAMEMAC

Message text	Failed to stack because of the same bridge MAC addresses.
Variable fields	N/A
Severity level	4
Example	STM/4/STM_SAMEMAC: Failed to stack because of the same bridge MAC addresses.
Explanation	Failed to set up the IRF fabric because some member devices are using the same bridge MAC address.
Recommended action	**384.** Verify that IRF bridge MAC persistence is disabled on the member devices. To disable this feature, use the **undo irf mac-address persistent** command. **385.** If the problem persists, contact NSFOCUS Support.

STM_SOMER_CHECK

Message text	Neighbor of IRF port [UINT32] cannot be stacked.
Variable fields	$1: IRF port name.
Severity level	3
Example	STM/3/STM_SOMER_CHECK: Neighbor of IRF port 1 cannot be stacked.
Explanation	The neighbor connected to the IRF port cannot form an IRF fabric with the device.
Recommended action	Check the following items: • The device models can form an IRF fabric. • The IRF settings are correct. For more information, see the IRF configuration guide for the device.

STP messages

This section contains STP messages.

STP_BPDU_PROTECTION

Message text	BPDU-Protection port [STRING] received BPDUs.
Variable fields	$1: Interface name.
Severity level	4
Example	STP/4/STP_BPDU_PROTECTION: BPDU-Protection port Ethernet1/0/4 received BPDUs.
Explanation	A BPDU-guard-enabled port received BPDUs.
Recommended action	Check whether the downstream device is a terminal and check for possible attacks from the downstream device or other devices.

STP_BPDU_RECEIVE_EXPIRY

Message text	Instance [UINT32]'s port [STRING] received no BPDU within the rcvdInfoWhile interval. Information of the port aged out.
Variable fields	$1: Instance ID. $2: Interface name.
Severity level	5
Example	STP/5/STP_BPDU_RECEIVE_EXPIRY: Instance 0's port GigabitEthernet0/4/1 received no BPDU within the rcvdInfoWhile interval. Information of the port aged out.
Explanation	The state of a non-designated port changed because the port did not receive a BPDU within the max age.
Recommended action	Check the STP status of the upstream device and possible attacks from other devices.

STP_CONSISTENCY_RESTORATION

Message text	Consistency restored on VLAN [UINT32]'s port [STRING].
Variable fields	$1: VLAN ID. $2: Interface name.
Severity level	6
Example	STP/6/STP_CONSISTENCY_RESTORATION: Consistency restored on VLAN 10's port GigabitEthernet0/1/1.
Explanation	Port link type or PVID inconsistency was removed on a port.
Recommended action	No action is required.

STP_DETECTED_TC

Message text	[STRING] [UINT32]'s port [STRING] detected a topology change.
Variable fields	$1: Instance or VLAN. $2: Instance ID or VLAN ID. $3: Interface name.
Severity level	6
Example	STP/6/STP_DETECTED_TC: Instance 0's port GigabitEthernet0/1/1 detected a topology change.
Explanation	The MSTP instance or VLAN to which a port belongs had a topology change, and the local end detected the change.
Recommended action	Identify the topology change cause and handle the issue. For example, if the change is caused by a link down event, recover the link.

STP_DISABLE

Message text	STP is now disabled on the device.
Variable fields	N/A
Severity level	6
Example	STP/6/STP_DISABLE: STP is now disabled on the device.
Explanation	STP was globally disabled on the device.
Recommended action	No action is required.

STP_DISCARDING

Message text	Instance [UINT32]'s port [STRING] has been set to discarding state.
Variable fields	$1: Instance ID. $2: Interface name.
Severity level	6
Example	STP/6/STP_DISCARDING: Instance 0's port Ethernet1/0/2 has been set to discarding state.
Explanation	MSTP calculated the state of ports within an instance, and a port was set to the discarding state.
Recommended action	No action is required.

STP_ENABLE

Message text	STP is now enabled on the device.
Variable fields	N/A
Severity level	6
Example	STP/6/STP_ENABLE: STP is now enabled on the device.
Explanation	STP was globally enabled on the device.
Recommended action	No action is required.

STP_FORWARDING

Message text	Instance [UINT32]'s port [STRING] has been set to forwarding state.
Variable fields	$1: Instance ID. $2: Interface name.
Severity level	6
Example	STP/6/STP_FORWARDING: Instance 0's port Ethernet1/0/2 has been set to forwarding state.
Explanation	MSTP calculated the state of ports within an instance, and a port was set to the forwarding state.
Recommended action	No action is required.

STP_LOOP_PROTECTION

Message text	Instance [UINT32]'s LOOP-Protection port [STRING] failed to receive configuration BPDUs.
Variable fields	$1: Instance ID. $2: Interface name.
Severity level	4
Example	STP/4/STP_LOOP_PROTECTION: Instance 0's LOOP-Protection port Ethernet1/0/2 failed to receive configuration BPDUs.
Explanation	A loop-guard-enabled port failed to receive configuration BPDUs.
Recommended action	Check the STP status of the upstream device and possible attacks from other devices.

STP_NOT_ROOT

Message text	The current switch is no longer the root of instance [UINT32].
Variable fields	$1: Instance ID.
Severity level	5
Example	STP/5/STP_NOT_ROOT: The current switch is no longer the root of instance 0.
Explanation	The current switch is no longer the root bridge of an instance. It received a superior BPDU after it was configured as the root bridge.
Recommended action	Check the bridge priority configuration and possible attacks from other devices.

STP_NOTIFIED_TC

Message text	[STRING] [UINT32]'s port [STRING] was notified of a topology change.
Variable fields	$1: Instance or VLAN. $2: Instance ID or VLAN ID. $3: Interface name.
Severity level	6
Example	STP/6/STP_NOTIFIED_TC: Instance 0's port GigabitEthernet0/1/1 was notified of a topology change.
Explanation	The neighboring device on a port notified the current device that a topology change occurred in the instance or VLAN to which the port belongs.
Recommended action	Identify the topology change cause and handle the issue. For example, if the change is caused by a link down event, recover the link.

STP_PORT_TYPE_INCONSISTENCY

Message text	Access port [STRING] in VLAN [UINT32] received PVST BPDUs from a trunk or hybrid port.
Variable fields	$1: Interface name. $2: VLAN ID.
Severity level	4
Example	STP/4/STP_PORT_TYPE_INCONSISTENCY: Access port GigabitEthernet0/1/1 in VLAN 10 received PVST BPDUs from a trunk or hybrid port.
Explanation	An access port received PVST BPDUs from a trunk or hybrid port.
Recommended action	Check the port link type setting on the ports.

STP_PVID_INCONSISTENCY

Message text	Port [STRING] with PVID [UINT32] received PVST BPDUs from a port with PVID [UINT32].
Variable fields	$1: Interface name. $2: VLAN ID. $3: VLAN ID.
Severity level	4
Example	STP/4/STP_PVID_INCONSISTENCY: Port GigabitEthernet0/1/1 with PVID 10 received PVST BPDUs from a port with PVID 20.
Explanation	A port received PVST BPDUs from a remote port with a different PVID.
Recommended action	Verify that the PVID is consistent on both ports.

STP_PVST_BPDU_PROTECTION

Message text	PVST BPDUs were received on port [STRING], which is enabled with PVST BPDU protection.
Variable fields	$1: Interface name.
Severity level	4
Example	STP/4/STP_PVST_BPDU_PROTECTION: PVST BPDUs were received on port GigabitEthernet0/1/1, which is enabled with PVST BPDU protection.
Explanation	In MSTP mode, a port enabled with PVST BPDU guard received PVST BPDUs.
Recommended action	Identify the device that sends the PVST BPDUs.

STP_ROOT_PROTECTION

Message text	Instance [UINT32]'s ROOT-Protection port [STRING] received superior BPDUs.
Variable fields	$1: Instance ID. $2: Interface name.
Severity level	4
Example	STP/4/STP_ROOT_PROTECTION: Instance 0's ROOT-Protection port Ethernet1/0/2 received superior BPDUs.
Explanation	A root-guard-enabled port received BPDUs that are superior to the BPDUs generated by itself.
Recommended action	Check the bridge priority configuration and possible attacks from other devices.

STP_STG_NUM_DETECTION

Message text	STG count [UINT32] is smaller than the MPU's STG count [UINT32].
Variable fields	$1: Number of STGs on a card. $2: Number of STGs on the MPU.
Severity level	4
Example	STP/4/STP_STG_NUM_DETECTION: STG count 64 is smaller than the MPU's STG count 65.
Explanation	The system detected that the STG count on a card was smaller than that on the MPU.
Recommended action	Make sure the number of spanning tree instances is not larger than the smallest card-specific STG count. For example, if the number of spanning tree instances is m and the smallest STG count among cards is n, m cannot be larger than n.

SYSEVENT

This section contains system event messages.

EVENT_TIMEOUT

Message text	Module [UINT32]'s processing for event [UINT32] timed out. Module [UINT32]'s processing for event [UINT32] on [STRING] timed out.
Variable fields	$1: Module ID. $2: Event ID. $3: MDC *MDC-ID* or Context *Context-ID*.
Severity level	6
Example	SYSEVENT/6/EVENT_TIMEOUT: -MDC=1; Module 0x1140000's processing for event 0x20000010 timed out. SYSEVENT/6/EVENT_TIMEOUT: -Context=1; Module 0x33c0000's processing for event 0x20000010 on context 16 timed out.
Explanation	A module's processing for an event timed out. Logs generated on the default MDC or context for the default MDC or context do not include the MDC *MDC-ID* or Context *Context-ID*. Logs generated on the default MDC or context for a non-default MDC or context include the MDC *MDC-ID* or Context *Context-ID*. Logs generated on a non-default MDC or context for the local MDC or context do not include the MDC *MDC-ID* or Context *Context-ID*.
Recommended action	No action is required.

SYSLOG messages

This section contains syslog messages.

ENCODING

Message text	Set the character set encoding to [STRING] for syslog messages.
Variable fields	$1: Character set encoding, which can be UTF-8 or GB18030.
Severity level	6
Example	SYSLOG/6/ENCODING: Set the character set encoding to UTF-8 for syslog messages.
Explanation	Set the character set encoding to UTF-8 for syslog messages.
Recommended action	For the user' login terminal to correctly display Chinese characters in log messages received from the information center, make sure the information center and the terminal use the same character set encoding.

SYSLOG_LOGBUFFER_FAILURE

Message text	Log cannot be sent to the logbuffer because of communication timeout between syslog and DBM processes.
Variable fields	N/A
Severity level	4
Example	SYSLOG/4/SYSLOG_LOGBUFFER_FAILURE: Log cannot be sent to the logbuffer because of communication timeout between syslog and DBM processes.
Explanation	Failed to output logs to the logbuffer because of the communication timeout between syslog and DBM processes.
Recommended action	Contact NSFOCUS Support.

SYSLOG_LOGFILE_FULL

Message text	Log file space is full.
Variable fields	N/A
Severity level	4
Example	SYSLOG/4/SYSLOG_LOGFILE_FULL: Log file space is full.
Explanation	The log file space is full.
Recommended action	Back up the log file and remove it, and then bring up interfaces if needed.

SYSLOG_RESTART

Message text	System restarted -- [STRING] [STRING] Software.
Variable fields	$1: Company name. $2: Software name.
Severity level	6
Example	SYSLOG/6/SYSLOG_RESTART: System restarted -- NSFOCUS Software
Explanation	A system restart log was created.
Recommended action	No action is required.

TAC messages

This section contains TAC messages.

LB_TAC_AUTH (fast log output)

Message text	User = STRING, MessageType = STRING, IP = STRING, URL = STRING, Result = STRING, Time = STRING
Variable fields	$1: Username. $2: Message type: ○ **AppAuth**—Application authentication. ○ **ApiAuth**—API authentication. $3: User IP address. $4: URL of the application or API. $5: Authentication result: ○ **AUTH_DENY**—Access denied. ○ **AUTH_PERMIT**—Access permitted. ○ **AUTH_REAUTH**—Reauthentication required. $6: Authentication time.
Severity level	6
Example	NSFOCUS LB/6/ TAC_AUTH: User = admin, MessageType = AppAuth, IP = , URL = http://6.6.6.6:8080/, Result = AUTH_PERMIT, Time = 20200402154737
Explanation	This message is generated after an authentication operation is performed.
Recommended action	No action is required.

LB_TAC_NOTIFY_OFFLINE (fast log output)

Message text	MessageType = STRING, User = STRING, IP = STRING, Time = STRING
Variable fields	$1: Message type: ○ **AppUserOffline**—An application user went offline. ○ **ApiUserOffline**—An API user went offline. $1: Username. $3: User IP address. $4: Time when the user went offline.
Severity level	6
Example	NSFOCUS LB/6/ TAC_NOTIFY_OFFLINE: MessageType = ApiUserOffline, User = mAMz8WqXHtBa4R7slIbLNrEiYvuwecnf, IP = 10.1.1.1, Time = 20200401095819
Explanation	This message is generated when a user goes offline.
Recommended action	No action is required.

LB_TAC_NOTIFY_PERMISSIONUPDOWN (fast log output)

Message text	MessageType = STRING, User = STRING, IP = STRING, Time = STRING, UrlCnt = [UINT16], UrlList = { STRING, STRING,…}
Variable fields	$1: Message type: ○ **AppUserAccessPermitted**—The permission of the application user changed to access permitted. ○ **ApiUserAccessPermitted**—The permission of the API user changed to access permitted. ○ **AppUserAccessDenied**—The permission of the application user changed to access denied. ○ **ApiUserAccessDenied**—The permission of the API user changed to access denied. $1: Username. $3: User IP address. $4: Time when the permission changed. $5: Number of application or API URLs for the permission change $6: URL list.
Severity level	6
Example	NSFOCUS LB/6/ TAC_NOTIFY_PERMISSIONUPDOWN: MessageType = ApiUserAccessDenied, User = user1, IP = 10.1.1.1, Time = 20200401095819, UrlCnt = 2, UrlList = {http://2.0.0.2:8080/spg_api/app1_api1,http://2.0.0.2:8080/spg_api/app2_api2, }
Explanation	This message is generated when the permission of a user changes.
Recommended action	No action is required.

TACACS messages

This section contains TACACS messages.

TACACS_ACCT_SERVER_DOWN

Message text	TACACS accounting server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
Variable fields	$1: IP address of the accounting server. $2: Port number of the accounting server. $3: VPN instance name. This field displays **public** if the server belongs to the public network.
Severity level	4
Example	TACACS/4/TACACS_ACCT_SERVER_DOWN: TACACS accounting server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
Explanation	An accounting server became blocked.
Recommended action	**386.** Verify that the accounting server has started up. **387.** Ping the accounting server to verify that the server is reachable. If the server is not reachable, check the link for connectivity issues and resolve the issues. **388.** Collect logs and diagnostic logs, and then contact NSFOCUS Support.

TACACS_ACCT_SERVER_UP

Message text	TACACS accounting server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
Variable fields	$1: IP address of the accounting server. $2: Port number of the accounting server. $3: VPN instance name. This field displays **public** if the server belongs to the public network.
Severity level	6
Example	TACACS/6/TACACS_ACCT_SERVER_UP: TACACS accounting server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
Explanation	An accounting server became active.
Recommended action	No action is required.

TACACS_AUTH_FAILURE

Message text	User [STRING] at [STRING] failed authentication.
Variable fields	$1: Username. $2: IP address.
Severity level	5
Example	TACACS/5/TACACS_AUTH_FAILURE: User cwf@system at 192.168.0.22 failed authentication.
Explanation	An authentication request was rejected by the TACACS server.
Recommended action	No action is required.

TACACS_AUTH_SERVER_DOWN

Message text	TACACS authentication server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
Variable fields	$1: IP address of the authentication server. $2: Port number of the authentication server. $3: VPN instance name. This field displays **public** if the server belongs to the public network.
Severity level	4
Example	TACACS/4/TACACS_AUTH_SERVER_DOWN: TACACS authentication server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
Explanation	An authentication server became blocked.
Recommended action	**389.** Verify that the authentication server has started up. **390.** Ping the authentication server to verify that the server is reachable. If the server is not reachable, check the link for connectivity issues and resolve the issues. **391.** Collect logs and diagnostic logs, and then contact NSFOCUS Support.

TACACS_AUTH_SERVER_UP

Message text	TACACS authentication server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
Variable fields	$1: IP address of the authentication server. $2: Port number of the authentication server. $3: VPN instance name. This field displays **public** if the server belongs to the public network.
Severity level	6
Example	TACACS/6/TACACS_AUTH_SERVER_UP: TACACS authentication server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
Explanation	An authentication server became active.
Recommended action	No action is required.

TACACS_AUTH_SUCCESS

Message text	User [STRING] at [STRING] was authenticated successfully.
Variable fields	$1: Username. $2: IP address.
Severity level	6
Example	TACACS/6/TACACS_AUTH_SUCCESS: User cwf@system at 192.168.0.22 was authenticated successfully.
Explanation	An authentication request was accepted by the TACACS server.
Recommended action	No action is required.

TACACS_AUTHOR_SERVER_DOWN

Message text	TACACS authorization server was blocked: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
Variable fields	$1: IP address of the authorization server. $2: Port number of the authorization server. $3: VPN instance name. This field displays **public** if the server belongs to the public network.
Severity level	4
Example	TACACS/4/TACACS_AUTHOR_SERVER_DOWN: TACACS authorization server was blocked: Server IP=1.1.1.1, port=1812, VPN instance=public.
Explanation	An authorization server became blocked.
Recommended action	**392.** Verify that the authorization server has started up. **393.** Ping the authorization server to verify that the server is reachable. If the server is not reachable, check the link for connectivity issues and resolve the issues. **394.** Collect logs and diagnostic logs, and then contact NSFOCUS Support.

TACACS_AUTHOR_SERVER_UP

Message text	TACACS authorization server became active: Server IP=[STRING], port=*[UINT32]*, VPN instance=[STRING].
Variable fields	$1: IP address of the authorization server. $2: Port number of the authorization server. $3: VPN instance name. This field displays **public** if the server belongs to the public network.
Severity level	6
Example	TACACS/6/TACACS_AUTHOR_SERVER_UP: TACACS authorization server became active: Server IP=1.1.1.1, port=1812, VPN instance=public.
Explanation	An authorization server became active.
Recommended action	No action is required.

TACACS_REMOVE_SERVER_FAIL

Message text	Failed to remove servers in scheme [STRING].
Variable fields	$1: Scheme name.
Severity level	4
Example	TACACS/4/TACACS_REMOVE_SERVER_FAIL: Failed to remove servers in scheme abc.
Explanation	Failed to remove servers from a TACACS scheme.
Recommended action	No action is required.

TCSM

This section contains Trusted Computing Services Management (TCSM) messages.

TCSM_CERT_BROKEN

Message text	Certificate [STRING] is missing or corrupted.
Variable fields	$1: Certificate name.
Severity level	3
Example	TCSM/3/TCSM_CERT_BROKEN: Certificate ak1-cert is missing or corrupted.
Explanation	A certificate stored in a storage medium is lost or corrupted.
Recommended action	• If the certificate is user defined, perform the following tasks: **a.** Replace the storage medium. **b.** From the manager, sign a new certificate for the TCSM key of the device. • If the certificate is system defined, contact NSFOCUS Support.

TCSM_KEY_BROKEN

Message text	Key [STRING] is corrupted or missing.
Variable fields	$1: Key name.
Severity level	3
Example	TCSM/3/TCSM_KEY_BROKEN: Key abc is corrupted or missing.
Explanation	A key file stored in a storage medium is lost or corrupted.
Recommended action	• If the key is user defined, perform the following tasks: **c.** Use the **`key destroy`** command to destroy the key. **d.** As a best practice, replace the storage medium. • If the key is system defined, contact NSFOCUS Support.

TCSM_KEY_HIERARCHY_BROKEN

Message text	Key hierarchy of [STRING] is corrupted.
Variable fields	$1: Key name
Severity level	3
Example	TCSM/3/TCSM_KEY_HIERARCHY_BROKEN: Key hierarchy of abc is corrupted.
Explanation	An upper-level key of the specified key is corrupted.
Recommended action	**3.** Use the **`key destroy`** command to destroy the specified key and its upper-level keys. **4.** As a best practice, replace the storage medium.

TCSM_TSS_SVC_DOWN

Message text	TSS service is down.
Variable fields	N/A
Severity level	3
Example	TCSM/3/TCSM_TSS_SVC_DOWN: TSS service is down.
Explanation	The TPM software stack process is down.
Recommended action	Contact NSFOCUS Support.

TCSM_TSS_SVC_UP

Message text	TSS service is up.
Variable fields	N/A
Severity level	5
Example	TCSM/5/TCSM_TSS_SVC_DOWN: TSS service is up.
Explanation	The TPM software stack process is up.
Recommended action	No action is required.

TELNETD messages

This section contains Telnet daemon messages.

TELNETD_ACL_DENY

Message text	The Telnet Connection request from [IPADDR]([STRING]) was denied by ACL rule (rule ID=[INT32])
Variable fields	$1: IP address of the Telnet client. $2: VPN instance to which the Telnet client belongs. $3: ID of the rule that denied the Telnet client. If a Telnet client does not match created ACL rules, the device denies the client based on the default ACL rule.
Severity level	5
Example	TELNETD/5/TELNETD_ACL_DENY:The Telnet connection request from 181.1.1.10 was denied by ACL rule (rule ID=20). TELNETD/5/TELNETD_ACL_DENY:The Telnet connection request from 181.1.1.10 was denied by ACL rule (default rule).
Explanation	Telnet login control ACLs control which Telnet clients can access the Telnet service on the device. The device sends this log message when it denies a Telnet client.
Recommended action	No action is required.

TELNETD_REACH_SESSION_LIMIT

Message text	Telnet client $1 failed to log in. The current number of Telnet sessions is [NUMBER]. The maximum number allowed is ([NUMBER]).
Variable fields	$1: IP address of the Telnet client. $2: Current number of Telnet sessions. $3: Maximum number of Telnet sessions allowed by the device.
Severity level	6
Example	TELNETD/6/TELNETD_REACH_SESSION_LIMIT: Telnet client 1.1.1.1 failed to log in. The current number of Telnet sessions is 10. The maximum number allowed is (10).
Explanation	The number of Telnet connections reached the limit.
Recommended action	**395.** Use the **display current-configuration | include session-limit** command to view the current limit for Telnet connections. If the command does not display the limit, the device is using the default setting. **396.** If you want to set a greater limit, execute the **aaa session-limit** command. If you think the limit is proper, no action is required.

TERMINAL messages

This section contains terminal identification messages through fast log output.

TERMINAL_CHANGED_LOG_IP

Message text	IPAddr(1145)=[IPADDR];PhyInterface(1148)=[STRING];OldMAC(1147)=[STRING];NewMAC(1168)=[STRING];OldVendor(1149)=[STRING];NewVendor(1150)=[STRING];OldType(1151)=[STRING];NewType(1152)=[STRING];OldModel(1153)=[STRING];NewModel(1154)=[STRING];OldSerialNum(1155)=[STRING];NewSerialNum(1156)=[STRING];OldTrmlID(1157)=[UINT32];NewTrmlID(1169)=[UINT32];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];Location(1209)=[STRING];
Variable fields	$1: Terminal IPv4 address. $2: Physical interface for terminal access. $3: Old terminal MAC address. $4: New terminal MAC address. $5: Old vendor. $6: New vendor. $7: Old type. $8: New type. $9: Old model. $10: New model. $11: Old serial number. $12: New serial number. $13: Old vendor ID. $14: New vendor ID. $15: VLAN ID. $16: VXLAN ID. $17: Location.
Severity level	4
Example	TERMINAL/4/TERMINAL_CHANGED_LOG_IP:IPAddr(1145)=1.1.1.1;PhyInterface(1148)=g2/0/0;OldMAC(1147)=0800-2786-a375;NewMAC(1168)=0800-2786-a376;OldVendor(1149)=DAHUA;NewVendor(1150)=HIKVISION;OldType(1151)=camera;NewType(1152)=camera;OldModel(1153)=DH-ITC2013;NewModel(1154)=DS-2CD3;OldSerialNum(1155)=1122;NewSerialNum(1156)=2233;OldTrmlID(1157)=123456;NewTrmlID(1169)=123457;VlanID(1175)=400;VNI(1213)=--;Location(1209)=China Macao;
Explanation	The device generates and sends a log when it detects a terminal information change. Then the device keeps silence for one minute and does not send any log even it detects information changes of this terminal. When the one minute silence timer elapses, the device again can send logs for another information change of this terminal.
Recommended action	No action is required.

TERMINAL_CHANGED_LOG_IPV6

Message text	IPv6Addr(1146)=[IPADDR];PhyInterface(1148)=[STRING];OldMAC(1147)=[STRING];NewMAC(1168)=[STRING];OldVendor(1149)=[STRING];NewVendor(1150)=[STRING];OldType(1151)=[STRING];NewType(1152)=[STRING];OldModel(1153)=[STRING];NewModel(1154)=[STRING];OldSerialNum(1155)=[STRING];NewSerialNum(1156)=[STRING];OldTrmlID(1157)=[UINT32];NewTrmlID(1169)=[UINT32];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];Location(1209)=[STRING];
Variable fields	$1: Terminal IPv6 address. $2: Physical interface for terminal access. $3: Old terminal MAC address. $4: New terminal MAC address. $5: Old vendor. $6: New vendor. $7: Old type. $8: New type. $9: Old model. $10: New model. $11: Old serial number. $12: New serial number. $13: Old vendor ID. $14: New vendor ID. $15: VLAN ID. $16: VXLAN ID. $17: Location.
Severity level	4
Example	TERMINAL/4/CHANGED_LOG_IPV6:IPv6Addr(1146)=2001::1;PhyInterface(1148)=g2/0/0;OldMAC(1147)=0800-2786-a375;NewMAC(1168)=0800-2786-a376;OldVendor(1149)=DAHUA;NewVendor(1150)=HIKVISION;OldType(1151)=camera;NewType(1152)=camera;OldModel(1153)=DH-ITC2013;NewModel(1154)=DS-2CD3;OldSerialNum(1155)=1122;NewSerialNum(1156)=2233;OldTrmlID(1157)=123456;NewTrmlID(1169)=123457;VlanID(1175)=400;VNI(1213)=--;Location(1209)=China Macao;
Explanation	The device generates and sends a log when it detects a terminal information change. Then the device keeps silence for one minute and does not send any log even it detects information changes of this terminal. When the one minute silence timer elapses, the device again can send logs for another information change of this terminal.
Recommended action	No action is required.

TRILL messages

This section contains TRILL messages.

TRILL_DUP_SYSTEMID

Message text	Duplicate system ID [STRING] in [STRING] PDU sourced from RBridge 0x[HEX].
Variable fields	$1: System ID. $2: PDU type. $3: Source RBridge's nickname.
Severity level	5
Example	TRILL/5/TRILL_DUP_SYSTEMID: Duplicate system ID 0011.2200.1501 in LSP PDU sourced from RBridge 0xc758.
Explanation	The local RBridge received an LSP or IIH PDU that has the same system ID as the local RBridge. The possible reasons include: • The same system ID is assigned to the local RBridge and the remote RBridge. • The local RBridge received a self-generated LSP PDU with an old nickname.
Recommended action	Please check the RBridge system IDs on the campus network.

TRILL_INTF_CAPABILITY

Message text	The interface [STRING] does not support TRILL.
Variable fields	$1: Interface name.
Severity level	4
Example	TRILL/4/TRILL_INTF_CAPABILITY: The interface GigabitEthernet0/1/3 does not support TRILL.
Explanation	An interface that does not support TRILL is assigned to a link aggregation group.
Recommended action	Remove the interface that does not support TRILL from the link aggregation group.

TRILL_LICENSE_EXPIRED

Message text	The TRILL feature is being disabled, because its license has expired.
Variable fields	N/A
Severity level	5
Example	TRILL/5/TRILL_LICENSE_EXPIRED: The TRILL feature is being disabled, because its license has expired.
Explanation	The TRILL license has expired.
Recommended action	Check the TRILL license.

TRILL_MEM_ALERT

Message text	TRILL process receive system memory alert [STRING] event.
Variable fields	$1: Type of the memory alert event.
Severity level	5
Example	TRILL/5/TRILL_MEM_ALERT: TRILL process receive system memory alert start event.
Explanation	TRILL receives a memory alert event from the system.
Recommended action	Check the system memory.

TRILL_NBR_CHG

Message text	TRILL [UINT32], [STRING] adjacency [STRING] ([STRING]), state changed to [STRING].
Variable fields	$1: TRILL process ID. $2: Neighbor level. $3: Neighbor system ID. $4: Interface name. $5: Current neighbor state: ○ **up**—The neighbor has been established, and can operate correctly. ○ **initializing**—The neighbor is being initialized. ○ **down**—The neighbor is down.
Severity level	5
Example	TRILL/5/TRILL_NBR_CHG: TRILL 1, Level-1 adjacency 0011.2200.1501 (GigabitEthernet0/1/3), state changed to down.
Explanation	The state of a TRILL neighbor changed.
Recommended action	When the neighbor state changed to down or initializing, please check the TRILL configuration and network status according to the reason for the neighbor state change.

TRILL_NO_LICENSE

Message text	The TRILL feature has no license.
Variable fields	N/A
Severity level	5
Example	TRILL/5/TRILL_NO_LICENSE: The TRILL feature has no license.
Explanation	The TRILL feature has no license.
Recommended action	Install a valid license for TRILL.

UFLT messages

This section contains URL filtering messages through fast log output and syslog output.

UFLT_MATCH_IPV4_LOG (syslog)

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];URL(1093)=[STRING];URLCategory(1094)=[STRING];PolicyName(1079)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: URL content. $4: URL category name. $5: URL filtering policy name. $6: Source IP address. $7: Source port number. $8: Destination IP address. $9: Destination port number. $10: Source security zone. $11: Destination security zone. $12: Name of the identity user. $13: Actions applied to the packet. Available actions are: o Block-Source. o Permit. o Drop. o Reset. o Redirect. $14: VLAN ID. $15: VXLAN ID. $16: Source location. $17: Destination location.
Severity level	6
Example	UFLT/6/UFLT_MATCH_IPV4_LOG:Protocol(1001)=TCP;Application(1002)=http;URL(1093)=google.com;URLCategory(1094)=Fashion&Beauty;PolicyName(1079)=policy1;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=abc;Action(1053)=Drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	An IPv4 packet matched a URL filtering rule.
Recommended action	No action is required.

UFLT_MATCH_IPV6_LOG (syslog)

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];URL(1093)=[STRING];URLCategory(1094)=[STRING];PolicyName(1079)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: URL content. $4: URL category name. $5: URL filtering policy name. $6: Source IPv6 address. $7: Source port number. $8: Destination IPv6 address. $9: Destination port number. $10: Source security zone. $11: Destination security zone. $12: Username. $13: Actions applied to the packet. Available actions are: o Block-Source. o Permit. o Drop. o Reset. o Redirect. $14: VLAN ID. $15: VXLAN ID. $16: Source location. $17: Destination location.
Severity level	6
Example	UFLT/6/UFLT_MATCH_IPV6_LOG:Protocol(1001)=TCP;Application(1002)=http;URL(1093)=google.com;URLCategory(1094)=Fashion&Beauty;PolicyName(1079)=policy1;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=aaa;Action(1053)=Drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	An IPv6 packet matched a URL filtering rule.
Recommended action	No action is required.

UFLT_NOT_MATCH_IPV4_LOG (syslog)

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];URL(1093)=[STRING];URLCategory(1094)=[STRING];PolicyName(1079)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: URL content. $4: URL category name. This field displays **Unknown** if no matching URL category is found for the packet. $5: URL filtering policy name. $6: Source IP address. $7: Source port number. $8: Destination IP address. $9: Destination port number. $10: Source security zone. $11: Destination security zone. $12: Username. $13: Actions applied to the packet. Available actions are: o Block-Source. o Permit. o Drop. o Reset. o Redirect. $14: VLAN ID. $15: VXLAN ID. $16: Source location. $17: Destination location.
Severity level	6
Example	UFLT/6/UFLT_NOT_MATCH_IPV4_LOG:Protocol(1001)=TCP;Application(1002)=http;URL(1093)=google.com;URLCategory(1094)=Unknown;PolicyName(1079)=policy1;SrcIPAddr(1003)=1.2.3.4;SrcPort(1004)=8080;DstIPAddr(1007)=6.1.1.1;DstPort(1008)=8080;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=abc;Action(1053)=Drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	No matching URL filtering rule was found for an IPv4 packet.
Recommended action	No action is required.

UFLT_NOT_MATCH_IPV6_LOG (syslog)

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];URL(1093)=[STRING];URLCategory(1094)=[STRING];PolicyName(1079)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];UserName(1113)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: URL content. $4: URL category name. $5: URL filtering policy name. $6: Source IPv6 address. $7: Source port number. $8: Destination IPv6 address. $9: Destination port number. $10: Source security zone. $11: Destination security zone. $12: Username. $13: Actions applied to the packet. Available actions are: o Block-Source. o Permit. o Drop. o Reset. o Redirect. $14: VLAN ID. $15: VXLAN ID. $16: Source location. $17: Destination location.
Severity level	6
Example	UFLT/6/UFLT_NOT_MATCH_IPV6_LOG:Protocol(1001)=TCP;Application(1002)=http;URL(1093)=google.com;URLCategory(1094)=Unknown;PolicyName(1079)=policy1;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=spf;DstZoneName(1035)=spf;UserName(1113)=aaa;Action(1053)=Drop;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	No matching URL filtering rule was found for an IPv6 packet.
Recommended action	No action is required.

UFLT_WARNING (syslog)

Message text	Updated the URL filtering signature library successfully.
Variable fields	N/A
Severity level	4
Example	UFLT/4/UFLT_WARNING: -Context=1; Updated the URL filtering signature library successfully.
Explanation	The URL filtering signature library was updated successfully through a manual offline update or triggered online update.
Recommended action	No action is required.

UFLT_WARNING (syslog)

Message text	Rolled back the URL filtering signature library successfully.
Variable fields	N/A
Severity level	4
Example	UFLT/4/UFLT_WARNING: -Context=1; Rolled back the URL filtering signature library successfully.
Explanation	The URL filtering signature library was rolled back to the previous or factory default version successfully.
Recommended action	No action is required.

UFLT_WARNING (syslog)

Message text	No available license to update URL signature.
Variable fields	N/A
Severity level	4
Example	UFLT/4/UFLT_WARNING: -Context=1; No available license to update URL signature.
Explanation	Failed to update the URL filtering signature library because no license is available.
Recommended action	No action is required.

UFLT_WARNING (syslog)

Message text	The signature library version is not compatible with the software version. Please use a compatible signature library version on the device.
Variable fields	N/A
Severity level	4
Example	UFLT/4/UFLT_WARNING: -Context=1; The signature library version is not compatible with the software version. Please use a compatible signature library version on the device.
Explanation	Failed to update the URL filtering signature library because the signature library version is not compatible with the software version.
Recommended action	No action is required.

UFLT_WARNING (syslog)

Message text	Failed to update signature package in phase [STRING].
Variable fields	$1: Update phase: ○ **DOWNLOAD**—Signature file download phase. ○ **GETURLFILE**—The system obtains the signature file path. ○ **PREPARE**—Signature library preparation phase. ○ **PARSE**—Signature library parsing phase. ○ **UNKNOWN**—Unknown.
Severity level	4
Example	UFLT/4/UFLT_WARNING: -Context=1; Failed to update signature package in phase DOWNLOAD.
Explanation	Failed to update the URL filtering signature library in a specific phase.
Recommended action	No action is required.

UFLT_WARNING (syslog)

Message text	uflt Copy SigPack file failed because flash is not enough.
Variable fields	N/A
Severity level	4
Example	UFLT/4/UFLT_WARNING: -Context=1; uflt Copy SigPack file failed because flash is not enough.
Explanation	Failed to update the URL filtering signature library because the storage space is insufficient.
Recommended action	No action is required.

UFLT_MATCH_IPV4_LOG (fast log)

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];UserName(1113)=[STRING];SrcMacAddr(1021)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];URLParentCategory(1128)=[STRING];URLCategory(1094)=[STRING];URL(1093)=[STRING];VistTime(1114)=[STRING];Client(1110)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Username. $4: Source MAC address. $5: Source IP address. $6: Source port number. $7: Source IP address after NAT. $8: Source port number after NAT. $9: Destination IP address. $10: Destination port number. $11: Destination IP address after NAT. $12: Destination port number after NAT. $13: Source security zone. $14: Destination security zone. $15: URL filtering policy name. $16: URL parent category name. $17: URL subcategory name. $18: URL content. $19: Access time. $20: Client type. This field is not supported in the current software version. $21: Actions applied to the packet. Available actions are: o Block-Source. o Permit. o Drop. o Reset. o Redirect. $14: VLAN ID. $15: VXLAN ID. $16: Source location. $17: Destination location.
Severity level	6
Example	UFLT/6/UFLT_MATCH_IPV4_LOG:Protocol(1001)=TCP;Application(1002)=SouhuNews;UserName(1113)=;SrcMacAddr(1021)=08-00-27-11-93-78;SrcIPAddr(1003)=112.1.1.2;SrcPort(1004)=3887;NATSrcIPAddr(1005)=112.1.1.2;NATSrcPort(1006)=3887;DstIPAddr(1007)=114.1.1.2;DstPort(1008)=80;NATDstIPAddr(1009)=114.1.1.2;NATDstPort(1010)=80;SrcZoneName(1025)=in;DstZoneName(1035)=out;PolicyName(1079)=1;URLParentCategory(1128)=SearchEngines&Portals;URLCategory(1094)=SearchEngines&Portals;URL(1093)=news.sohu.com/upload/itoolbar/itoolbar.index.loader.20140923.js;VistTi

	me(1114)=1480688515;Client(1110)=;Action(1053)=Permit;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	An IPv4 packet matched a URL filtering rule.
Recommended action	No action is required.

UFLT_MATCH_IPV6_LOG (fast log)

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];UserName(1113)=[STRING];SrcMacAddr(1021)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];URLParentCategory(1128)=[STRING];URLCategory(1094)=[STRING];URL(1093)=[STRING];VistTime(1114)=[STRING];Client(1110)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Username. $4: Source MAC address. $5: Source IPv6 address. $6: Source port number. $7: Destination IPv6 address. $8: Destination port number. $9: Source security zone. $10: Destination security zone. $11: URL filtering policy name. $12: URL parent category name. $13: URL subcategory name. $14: URL content. $15: Access time. $16: Client type. This field is not supported in the current software version. $17: Actions applied to the packet. Available actions are: o Block-Source. o Permit. o Drop. o Reset. o Redirect. $14: VLAN ID. $15: VXLAN ID. $16: Source location. $17: Destination location.
Severity level	6
Example	UFLT/6/UFLT_MATCH_IPV6_LOG:Protocol(1001)=TCP;Application(1002)=SouhuNews;UserName(1113)=;SrcMacAddr(1021)=08-00-27-11-93-78;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=in;DstZoneName(1035)=out;PolicyName(1079)=1;URLParentCategory(1128)=SearchEngines&Portals;URLCategory(1094)=SearchEngines&Portals;URL(1093)=news.sohu.com/upload/itoolbar/itoolbar.index.loader.20140923.js;VistTime(1114)=1480688515;Client(1110)=;Action(1053)=Permit; VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	An IPv6 packet matched a URL filtering rule.
Recommended action	No action is required.

UFLT_NOT_MATCH_IPV4_LOG (fast log)

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];UserName(1113)=[STRING];SrcMacAddr(1021)=[STRING];SrcIPAddr(1003)=[IPADDR];SrcPort(1004)=[UINT16];NATSrcIPAddr(1005)=[IPADDR];NATSrcPort(1006)=[UINT16];DstIPAddr(1007)=[IPADDR];DstPort(1008)=[UINT16];NATDstIPAddr(1009)=[IPADDR];NATDstPort(1010)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];URLParentCategory(1128)=[STRING];URLCategory(1094)=[STRING];URL(1093)=[STRING];VistTime(1114)=[STRING];Client(1110)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Username. $4: Source MAC address. $5: Source IP address. $6: Source port number. $7: Source IP address after NAT. $8: Source port number after NAT. $9: Destination IP address. $10: Destination port number. $11: Destination IP address after NAT. $12: Destination port number after NAT. $13: Source security zone. $14: Destination security zone. $15: URL filtering policy name. $16: URL parent category name. If no category is matched, this field displays a hyphen (-). $17: URL subcategory name. If no subcategory is matched, this field displays **Unknown**. $18: URL content. $19: Access time. $20: Client type. This field is not supported in the current software version. $21: Actions applied to the packet. Available actions are: o Block-Source. o Permit. o Drop. o Reset. o Redirect. $22: VLAN ID. $23: VXLAN ID. $24: Source location. $25: Destination location.
Severity level	6
Example	UFLT/6/UFLT_NOT_MATCH_IPV4_LOG:Protocol(1001)=TCP;Application(1002)=SouhuNews;UserName(1113)=;SrcMacAddr(1021)=08-00-27-11-93-78;SrcIPAddr(1003)=112.1.1.2;SrcPort(1004)=3887;NATSrcIPAddr(1005)=112.1.1.2;NATSrcPort(1006)=3887;DstIPAddr(1007)=114.1.1.2;DstPort(1008)=80;NATDstIPAddr(1009)=114.1.1.2;NATDstPort(1010)=80;SrcZoneName(1025)=in;DstZoneName(1035)=out;PolicyName(1079)=1;URLParentCategory(112

	8)=-;URLCategory(1094)=Unknown;URL(1093)=news.sohu.com/upload/itoolbar/index/toolbar_bg_130315.gif;VistTime(1114)=1480691551;Client(1110)=;Action(1053)=Permit;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	No matching URL filtering rule was found for an IPv4 packet.
Recommended action	No action is required.

UFLT_NOT_MATCH_IPV6_LOG (fast log)

Message text	Protocol(1001)=[STRING];Application(1002)=[STRING];UserName(1113)=[STRING];SrcMacAddr(1021)=[STRING];SrcIPv6Addr(1036)=[IPADDR];SrcPort(1004)=[UINT16];DstIPv6Addr(1037)=[IPADDR];DstPort(1008)=[UINT16];SrcZoneName(1025)=[STRING];DstZoneName(1035)=[STRING];PolicyName(1079)=[STRING];URLParentCategory(1128)=[STRING];URLCategory(1094)=[STRING];URL(1093)=[STRING];VistTime(1114)=[STRING];Client(1110)=[STRING];Action(1053)=[STRING];VlanID(1175)=[UINT32];VNI(1213)=[UINT32];SrcLocation(1209)=[STRING];DstLocation(1214)=[STRING];
Variable fields	$1: Protocol type. $2: Application protocol name. $3: Username. $4: Source MAC address. $5: Source IPv6 address. $6: Source port number. $7: Destination IPv6 address. $8: Destination port number. $9: Source security zone. $10: Destination security zone. $11: URL filtering policy name. $12: URL parent category name. If no category is matched, this field displays a hyphen (**-**). $13: URL category name. If no subcategory is matched, this field displays **Unknown**. $14: URL content. $15: Access time. $16: Client type. This field is not supported in the current software version. $17: Actions applied to the packet. Available actions are: o Block-Source. o Permit. o Drop. o Reset. o Redirect. $18: VLAN ID. $19: VXLAN ID. $20: Source location. $21: Destination location.
Severity level	6
Example	UFLT/6/UFLT_NOT_MATCH_IPV6_LOG:Protocol(1001)=TCP;Application(1002)=SouhuNews;UserName(1113)=;SrcMacAddr(1021)=08-00-27-11-93-78;SrcIPv6Addr(1036)=2001::2;SrcPort(1004)=51396;DstIPv6Addr(1037)=3001::2;DstPort(1008)=25;SrcZoneName(1025)=in;DstZoneName(1035)=out;PolicyName(1079)=1;URLParentCategory(1128)=-;URLCategory(1094)=Unknown;URL(1093)=news.sohu.com/upload/itoolbar/itoolbar.index.loader.20140923.js;VistTime(1114)=1480688515;Client(1110)=;Action(1053)=Permit;VlanID(1175)=400;VNI(1213)=--;SrcLocation(1209)=China Macao;DstLocation(1214)=SaintKittsandNevis;
Explanation	No matching URL filtering rule was found for an IPv6 packet.
Recommended action	No action is required.

VLAN messages

This section contains VLAN messages.

VLAN_FAILED

Message text	Failed to add interface [STRING] to the default VLAN.
Variable fields	$1: Interface name.
Severity level	4
Example	VLAN/4/VLAN_FAILED: Failed to add interface S-Channel4/2/0/19:100 to the default VLAN.
Explanation	An S-channel interface was created when hardware resources were insufficient. The S-channel interface failed to be assigned to the default VLAN.
Recommended action	No action is required.

VLAN_VLANMAPPING_FAILED

	The configuration failed because of resource insufficiency or conflicts on [STRING].
	$1: Interface name.
	4
	VLAN/4/VLAN_VLANMAPPING_FAILED: The configuration failed because of resource insufficiency or conflicts on GigabitEthernet1/0/1.
	Part of or all VLAN mapping configurations on the interface were lost because of one of the following

	occurrences: • Hardware resources were insufficient for the interface. • The interface joined or left a Layer 2 aggregation group.
	No action is required.

VLAN_VLANSTRIP_REG_DIFF_CONFIG

Message text	The value of the vlan-strip register is different from the configuration on interface [STRING].
Variable fields	$1: Interface name.
Severity level	3
Example	VLAN/3/VLAN_VLANSTRIP_REG_DIFF_CONFIG: The value of the vlan-strip register is different from the configuration on interface GigabitEthernet1/0/1.
Explanation	The VLAN tag stripping configuration on an interface is different from the value of the vlan-strip register.
Recommended action	Check the operating environments of VMs and hosts, and configure VLAN tag stripping again.

VLAN_VLANTRANSPARENT_FAILED

	The configuration failed because of resource insufficiency or conflicts on [STRING].
	$1: Interface name.
	4
	VLAN/4/VLAN_VLANTRANSPARENT_FAILED: The configuration failed because of resource insufficiency or conflicts on GigabitEthernet1/0/1.
	Part of or all VLAN transparent transmission configurations on the interface were lost because of one

	of the following occurrences: • Hardware resources were insufficient for the interface. • The interface joined or left a Layer 2 aggregation group.
	No action is required.

VRRP messages

This section contains VRRP messages.

VRRP_AUTH_FAILED

Message text	Authentication failed in [STRING] virtual router [UINT32] (configured on [STRING]): [STRING].
Variable fields	$1: VRRP version. $2: VRRP group number. $3: Name of the interface where the VRRP group is configured. $4: Error information details.
Severity level	6
Example	VRRP/6/VRRP_AUTH_FAILED: Authentication failed in IPv4 virtual router 10 (configured on Ethernet0/0): Authentication type mismatch.
Explanation	A VRRP packet was received, but did not pass the authentication examination.
Recommended action	Check the configuration of the VRRP group on the specified interface. Make sure every router in the VRRP group uses the same authentication mode and authentication key.

VRRP_CONFIG_ERROR

Message text	The [STRING] virtual router [UINT32] (configured on [STRING]) detected a VRRP configuration error: [STRING].
Variable fields	$1: VRRP version. $2: VRRP group number. $3: Name of the interface where VRRP group is configured. $4: Error information details.
Severity level	6
Example	VRRP/6/VRRP_CONFIG_ERROR: The IPv4 virtual router 10 (configured on Ethernet0/0) detected a VRRP configuration error: Virtual IP address count mismatch.
Explanation	The VRRP group configuration is not correct. For example, the virtual IP address count of the VRRP group is not the same on the members.
Recommended action	Check the VRRP group configuration on the specified interface. Make sure every member in the VRRP group uses the same configuration.

VRRP_PACKET_ERROR

Message text	The [STRING] virtual router [UINT32] (configured on [STRING]) received an error packet: [STRING].
Variable fields	$1: VRRP version. $2: VRRP group number. $3: Interface where the VRRP group is configured. $4: Error information details.
Severity level	6
Example	VRRP/6/VRRP_PACKET_ERROR: The IPv4 virtual router 10 (configured on Ethernet0/0) received an error packet: CKSUM error.
Explanation	The VRRP group received an invalid VRRP packet. For example, the checksum was not correct.
Recommended action	Check the VRRP group configuration on the specified interface.

VRRP_STATUS_CHANGE

Message text	The status of [STRING] virtual router [UINT32] (configured on [STRING]) changed from [STRING] to [STRING]: [STRING].
Variable fields	$1: VRRP version. $2: VRRP group number. $3: Name of the interface where the VRRP group is configured. $4: Original status. $5: Current status. $6: Reason for status change: ○ **Interface event received**—An interface event was received. ○ **IP address deleted**—The virtual IP address has been deleted. ○ **The status of the tracked object changed**—The status of the associated track entry changed. ○ **VRRP packet received**—A VRRP advertisement was received. ○ **Current device has changed to IP address owner**—The current device has become the IP address owner. ○ **Master-down-timer expired**—The master down timer (3 × VRRP advertisement interval + Skew_Time) expired. ○ **Zero priority packet received**—A VRRP packet containing priority 0 was received. ○ **Preempt**—Preemption occurred.
Severity level	6
Example	VRRP/6/VRRP_STATUS_CHANGE: The status of IPv4 virtual router 10 (configured on Ethernet0/0) changed (from Backup to Master): Master-down-timer expired.
Explanation	The VRRP group status changed because of the following reasons: • An interface event was received. • The virtual IP address has been deleted. • The status of the associated track entry changed. • A VRRP advertisement was received. • The current device has become the IP address owner. • The master down timer (3 × VRRP advertisement interval + Skew_Time) expired. • A VRRP packet containing priority 0 was received. • Preemption occurred.
Recommended action	Check the VRRP group status to make sure it is operating correctly.

VRRP_VF_STATUS_CHANGE

Message text	The [STRING] virtual router [UINT32] (configured on [STRING]) virtual forwarder [UINT32] detected status change (from [STRING] to [STRING]): [STRING].
Variable fields	$1: VRRP version. $2: VRRP group number. $3: Name of the interface where the VRRP group is configured. $4: VF ID. $5: Original status of VF. $6: Current status of VF. $7: Reason for the status change.
Severity level	6
Example	VRRP/6/VRRP_VF_STATUS_CHANGE: The IPv4 virtual router 10 (configured on GigabitEthernet5/1) virtual forwarder 2 detected status change (from Active to Initialize): Weight changed.
Explanation	The status of the virtual forwarder has changed because the weight changed, the timeout timer expired, or VRRP went down.
Recommended action	Check the status of the track entry.

VRRP_VMAC_INEFFECTIVE

Message text	The [STRING] virtual router [UINT32] (configured on [STRING]) failed to add virtual MAC: [STRING].
Variable fields	$1: VRRP version. $2: VRRP group number. $3: Name of the interface where the VRRP group is configured. $4: Reason for the error.
Severity level	3
Example	VRRP/3/VRRP_VMAC_INEFFECTIVE: The IPv4 virtual router 10 (configured on Ethernet0/0) failed to add virtual MAC: Insufficient hardware resources.
Explanation	The virtual router failed to add a virtual MAC address.
Recommended action	Find out the root cause for the operation failure and fix the problem.

VSRP messages

This section contains VSRP messages.

VSRP_BIND_FAILED

Message text	Failed to bind the IP addresses and the port on VSRP peer [STRING].
Variable fields	$1: VSRP peer name.
Severity level	6
Example	VSRP/6/VSRP_BIND_FAILED: Failed to bind the IP addresses and the port on VSRP peer aaa.
Explanation	Failed to bind the IP addresses and the port when creating a TCP connection to the VSRP peer because the TCP port is in use.
Recommended action	No action is required.

VXLAN messages

This section contains VXLAN messages.

VXLAN_LICENSE_UNAVAILABLE

Message text	The VXLAN feature is disabled, because no licenses are valid.
Variable fields	N/A
Severity level	3
Example	VXLAN/3/VXLAN_LICENSE_UNAVAILABLE: The VXLAN feature is disabled, because no licenses are valid.
Explanation	VXLAN was disabled because no licenses were valid.
Recommended action	Install valid licenses for VXLAN.

WEB messages

This section contains Web messages.

LOGIN

Message text	[STRING] logged in from [STRING].
Variable fields	$1: Username of the user. $2: IP address of the user.
Severity level	5
Example	WEB/5/LOGIN: admin logged in from 127.0.0.1.
Explanation	A user logged in successfully.
Recommended action	No action is required.

LOGIN_FAILED

Message text	[STRING] failed to log in from [STRING].
Variable fields	$1: Username of the user. $2: IP address of the user.
Severity level	5
Example	WEB/5/LOGIN_FAILED: admin failed to log in from 127.0.0.1.
Explanation	A user failed to log in.
Recommended action	No action is required.

LOGOUT

Message text	[STRING] logged out from [STRING].
Variable fields	$1: Username of the user. $2: IP address of the user.
Severity level	5
Example	WEB/5/LOGOUT: admin logged out from 127.0.0.1.
Explanation	A user logged out successfully.
Recommended action	No action is required.

WEBCACHE messages

This section contains Web caching messages.

WEBCACHE_CHECK

Message text	Web caching is not available.Reason: The system is checking whether the Web cache directory is accessible. Please wait...
Variable fields	None
Severity level	4
Example	WEBCACHE/4/WEBCACHE_CHECK Web caching is not available. Reason: The system is checking whether the Web cache directory is accessible. Please wait...
Explanation	The Web caching feature was not available because the system was checking whether the Web cache directory was accessible.
Recommended action	Wait for the system to finish the check operation.

WEBCACHE_AVAILABLE

Message text	Web cache directory is accessible. Web caching is available now.
Variable fields	None
Severity level	6
Example	WEBCACHE/6/WEBCACHE_AVAILABLE: Web cache directory is accessible. Web caching is available now.
Explanation	The Web cache directory was accessible. The Web caching feature was available.
Recommended action	No action is required.

WEBCACHE_INAVAILABLE

Message text	Web caching is not available. Reason: The Web cache directory is not accessible.
Variable fields	None
Severity level	6
Example	WEBCACHE/6/WEBCACHE_INAVAILABLE: Web caching is not available. Reason: The Web cache directory is not accessible.
Explanation	Because the Web cache directory was not accessible, the Web caching feature was not available.
Recommended action	Use the **file-directory** command to specify a Web cache directory that is accessible.

WFF messages

This section contains WLAN fast forwarding (WFF) messages.

WFF_HARDWARE_INIT_FAILED

Message text	Firmware [UINT32] was set to pass-through mode because initialization failed.
Variable fields	$1: Firmware number.
Severity level	5
Example	WFF/5/WFF_HARDWARE_INIT_FAILED: Firmware 0 was set to pass-through mode because initialization failed.
Explanation	The pass-through mode was set for the firmware because of firmware initialization failure.
Recommended action	No action is required.

WFF_HARDWARE_IPC_FAILED

Message text	Firmware [UINT32] was set to pass-through mode because IPC check failed.
Variable fields	$1: Firmware number.
Severity level	5
Example	WFF/5/WFF_HARDWARE_IPC_FAILED: Firmware 0 was set to pass-through mode because IPC check failed.
Explanation	The pass-through mode was set for the firmware because of IPC check failure.
Recommended action	No action is required.

WFF_HARDWARE_LOOPBACK_FAILED

Message text	Firmware [UINT32] was set to pass-through mode because loopback check failed.
Variable fields	$1: Firmware number.
Severity level	5
Example	WFF/5/WFF_HARDWARE_LOOPBACK_FAILED: Firmware 0 was set to pass-through mode because loopback check failed.
Explanation	The pass-through mode was set for the firmware because of loopback check failure.
Recommended action	No action is required.

WFF_HARDWARE_PCIE_FAILED

Message text	Firmware [UINT32] was set to pass-through mode because PCIE check failed.
Variable fields	$1: Firmware number.
Severity level	5
Example	WFF/5/WFF_HARDWARE_LOOPBACK_FAILED: Firmware 0 was set to pass-through mode because PCIE check failed.
Explanation	The pass-through mode was set for the firmware because of a PCIE check failure.
Recommended action	No action is required.

WIPS messages

This section contains WIPS messages.

APFLOOD

Message text	-VSD=[STRING]; AP flood detected.
Variable fields	$1: VSD name.
Severity level	5
Example	WIPS/5/APFLOOD: -VSD=home; AP flood detected.
Explanation	The number of APs detected in the specified VSD reached the threshold.
Recommended action	Determine whether the device has suffered an attack.

AP_CHANNEL_CHANGE

Message text	-VSD=[STRING]-SrcMAC=[MAC]; Channel change detected.
Variable fields	$1: VSD name. $2: MAC address of the AP.
Severity level	5
Example	WIPS/5/AP_CHANNEL_CHANGE: -VSD=home-SrcMAC=1122-3344-5566; Channel change detected.
Explanation	The channel of the specified AP changed.
Recommended action	Determine whether the channel change is valid.

ASSOCIATEOVERFLOW

Message text	-VSD=[STRING]-SrcMAC=[MAC]; Association/Reassociation DoS attack detected.
Variable fields	$1: VSD name. $2: MAC address of the AP.
Severity level	5
Example	WIPS/5/ASSOCIATEOVERFLOW: -VSD=home-SrcMAC=1122-3344-5566; Association/Reassociation DoS attack detected.
Explanation	The specified AP sent an association response with the status code 17.
Recommended action	Determine whether the AP has suffered an attack.

WIPS_DOS

Message text	-VSD=[STRING]; [STRING] rate attack detected.
Variable fields	$1: VSD name. $2: Device type: AP or client.
Severity level	5
Example	WIPS/5/WIPS_DOS: -VSD=home; AP rate attack detected.
Explanation	The number of device entries learned within the specified interval reached the threshold.
Recommended action	Determine whether the device suffers an attack.

WIPS_FLOOD

Message text	-VSD=[STRING]-SrcMAC=[MAC]; [STRING] flood detected.
Variable fields	$1: VSD name. $2: Attacker's MAC address. $3: Flood attack type. Options include the following: • Association request • Authentication • Disassociation • Reassociation request • Deauthentication • Null data • Beacon • Probe request • BlockAck • CTS • RTS • EAPOL start
Severity level	5
Example	WIPS/5/WIPS_FLOOD: -VSD=home-SrcMAC=1122-3344-5566; Association request flood detected.
Explanation	The number of a specific type of packets detected within the specified interval reached the threshold.
Recommended action	Determine whether the packet sender is an authorized device.

HONEYPOT

Message text	-VSD=[STRING]-SrcMAC=[MAC]; Honeypot AP detected.
Variable fields	$1: VSD name. $2: MAC address of the AP.
Severity level	5
Example	WIPS/5/HONEYPOT: -VSD=home-SrcMAC=1122-3344-5566; Honeypot AP detected.
Explanation	The specified AP was detected as a honeypot AP.
Recommended action	Determine whether the device has suffered an attack.

HTGREENMODE

Message text	-VSD=[STRING]-SrcMAC=[MAC]; HT-Greenfield AP detected.
Variable fields	$1: VSD name. $2: MAC address of the AP.
Severity level	5
Example	WIPS/5/HTGREENMODE: -VSD=home-SrcMAC=1122-3344-5566; HT-Greenfield AP detected.
Explanation	The specified AP was detected as an HT-greenfield AP.
Recommended action	Determine whether the device has suffered an attack.

WIPS_MALF

Message text	-VSD=[STRING]-SrcMAC=[MAC]; Error detected: [STRING].
Variable fields	$1: VSD name. $2: Sender's MAC address. $3: Malformed packet type. Options include the following: • **invalid ie length**—Invalid IE length. • **duplicated ie**—Duplicate IE. • **redundant ie**—Redundant IE. • **invalid pkt length**—Invalid packet length. • **illegal ibss ess**—Abnormal IBSS and ESS setting. • **invalid source addr**—Invalid source MAC address. • **overflow eapol key**—Oversized EAPOL key. • **malf auth**—Malformed authentication request frame. • **malf assoc req**—Malformed association request frame. • **malf ht ie**—Malformed HT IE. • **large duration**—Oversized duration. • **null probe resp**—Malformed probe response frame. • **invalid deauth code**—Invalid deauthentication code. • **invalid disassoc code**—Invalid disassociation code. • **over flow ssid**—Oversized SSID. • **fata jack**—FATA-Jack.
Severity level	5
Example	WIPS/5/WIPS_MALF: -VSD=home-SrcMAC=1122-3344-5566; Error detected: fata jack.
Explanation	A malformed packet was detected.
Recommended action	Determine whether the packet sender is an authorized device.

MAN_IN_MIDDLE

Message text	-VSD=[STRING]-SrcMAC=[MAC]; Man-in-the-middle attack detected.
Variable fields	$1: VSD name. $2: MAC address of the client.
Severity level	5
Example	WIPS/5/MAN_IN_MIDDLE: -VSD=home-SrcMAC=1122-3344-5566; Man-in-the-middle attack detected.
Explanation	The specified client suffered a man-in-the-middle attack.
Recommended action	Determine whether the client has suffered a man-in-the-middle attack.

WIPS_ROGUE

Message text	-VSD=[STRING]-SrcMAC=[MAC]; Rogue AP detected by radio 1 of sensor [STRING] on channel 149 (RSSI=84).
Variable fields	$1: VSD name. $2: MAC address of the rogue AP.
Severity level	5
Example	WIPS/5/WIPS_ROGUE: -VSD=home-SrcMAC=1122-3344-5566; Rogue AP detected by radio 1 of sensor ap1 on channel 149 (RSSI=84).
Explanation	A rogue AP was detected.
Recommended action	Enable WIPS to take countermeasures against rogue APs.

WIPS_SPOOF

Message text	-VSD=[STRING]-SrcMAC=[MAC]; [STRING] detected.
Variable fields	$1: VSD name. $2: MAC address of the device being spoofed. $3: Spoofing attack type. Options include the following: • **AP spoofing AP**—A fake AP spoofs an authorized AP. • **AP spoofing client**—A fake AP spoofs an authorized client. • **AP spoofing ad-hoc**—A fake AP spoofs an Ad hoc device. • **Ad-hoc spoofing AP**—An Ad hoc device spoofs an authorized AP. • **Client spoofing AP**—A client spoofs an authorized AP.
Severity level	5
Example	WIPS/5/WIPS_SPOOF: -VSD=home-SrcMAC=1122-3344-5566; AP spoofing AP detected.
Explanation	A spoofing attack was detected.
Recommended action	Determine whether the packet sender is an authorized device.

WIPS_UNAUTH

Message text	-VSD=[STRING]-SrcMAC=[MAC];Unauthorized client detected by radio 1 of sensor [STRING] on channel 149 (RSSI=84).
Variable fields	$1: VSD name. $2: MAC address of the unauthorized client.
Severity level	5
Example	WIPS/5/WIPS_UNAUTH: -VSD=home-SrcMAC=1122-3344-5566; Unauthorized client detected by radio 1 of sensor ap1 on channel 149 (RSSI=84).
Explanation	An unauthorized client was detected.
Recommended action	Determine whether unauthorized clients exist.

WIPS_WEAKIV

Message text	-VSD=[STRING]-SrcMAC=[MAC]; Weak IV detected.
Variable fields	$1: VSD name. $2: Sender's MAC address.
Severity level	5
Example	WIPS/5/WIPS_WEAKIV: -VSD=home-SrcMAC=1122-3344-5566; Weak IV detected.
Explanation	A weak IV was detected.
Recommended action	Use a more secure encryption method to encrypt packets.

WIRELESSBRIDGE

Message text	-VSD=[STRING]-AP1=[MAC]-AP2=[MAC]]; Wireless bridge detected.
Variable fields	$1: VSD name. $2: MAC address of AP 1. $3: MAC address of AP 2.
Severity level	5
Example	WIPS/5/WIRELESSBRIDGE: -VSD=home-AP1=1122-3344-5566-AP2=7788-9966-5544; Wireless bridge detected.
Explanation	The specified APs set up a wireless bridge.
Recommended action	Determine whether the wireless bridge is valid.

WLANAUD messages

This section contains WLANAUD messages.

WLANAUD_CLIENT_ONLINE

Message text	• UserIP=[STRING], UserMAC=[STRING], APMAC=[STRING]. • UserMAC=[STRING], UserIP=[STRING], APName=[STRING], APMAC=[STRING], SSID=[STRING], BSSID=[STRING].
Variable fields	$1: IP address of the client. $2: MAC address of the client. $3: MAC address of the AP with which the client is associated. $4: Name of the AP with which the client is associated. $5: SSID with which the client is associated. $6: BSSID with which the client is associated.
Severity level	5
Example	• WLANAUD/5/WLAN_CLIENT_ONLINE: UserIP=192.168.0.1, UserMAC=0023-8933-2147, APMAC=31AC-11EA-17FF. • WLANAUD/5/WLAN_CLIENT_ONLINE: UserMAC=31ac-11ea-17ff, UserIP=192.168.0.1, APName=ap1, APMAC=000f-ea00-3350, SSID=zhongyan, BSSID=000f-ea00-3352.
Explanation	A client was associated with an AP.
Recommended action	No action is required.

WMESH messages

This section contains WLAN mesh messages.

MESH_ACTIVELINK_SWITCH

Message text	Switch an active link from [MAC] ([CHAR]) to [MAC] ([CHAR]): peer quantity = [UINT64], link quantity = [UINT16], switch reason = [UINT32].
Variable fields	$1: Mesh peer MAC address before active/standby link switchover. $2: RSSI on the link before active/standby link switchover. $3: Mesh peer MAC address after active/standby link switchover. $4: RSSI on the link after active/standby link switchover. $5: Mesh peer quantity after active/standby link switchover. $6: Mesh link quantity after active/standby link switchover. $7: Reason for link switchover: • **1**—First mesh link establishment. • **2**—Active switchover (MLSP link switchover optimization disabled). • **3**—Active switchover (MLSP link switchover optimization enabled). • **4**—Passive switchover or switchover after forced logoff.
Severity level	5
Example	WMESH/5/MESH_ACTIVELINK_SWITCH: Switch an active link from 50da-00d2-4b50 (55) to 50da-00d2-49e0 (74): peer quantity = 3, link quantity = 2, switch reason = 2.
Explanation	An active/standby mesh link switchover occurred.
Recommended action	No action is required.

MESH_LINKDOWN

Message text	Mesh link on interface [CHAR] is down: peer MAC = [MAC], RSSI = [CHAR], reason: [STRING] ([STRING]).
Variable fields	$1: Link interface number. $2: Mesh peer MAC address. $3: RSSI on the link. $4: Reason: • **AP status change**. • **Radio status change**. • **Mesh configuration change**—Mesh configuration, such as mesh profile or mesh policy, changed. • **Mesh BSS deleted**. • **Excessive RSSI**—The link RSSI has exceeded the link saturation RSSI. • **Weak RSSI**. • **Packet check failure**. • **Link keepalive failure**. • **Active link keepalive failure**. • **Worst link replaced when MLSP link limit is reached**. • **Neighbor zerocfg status change**—The state of a neighbor of the temporary link is changed from zero configuration to non-zero configuration. • **Neighbor refresh**. • **Mesh link established during scan initialization or auto channel scan**. • **Unknown reason**. $5: Link terminated by: • local. • peer.
Severity level	5
Example	WMESH/5/MESH_LINKDOWN: Mesh link on interface 50 is down: peer MAC = 50da-00d2-4b50, RSSI = 45, reason: AP status change (peer).
Explanation	A mesh link was terminated.
Recommended action	No action is required.

MESH_LINKUP

Message text	Mesh link on interface [CHAR] is up: peer MAC = [MAC], peer radio mode = [UINT32], RSSI = [CHAR].
Variable fields	$1: Link interface number. $2: Mesh peer MAC address. $3: Mesh peer radio mode: • **0**—Any mode except for 802.11n and 802.11ac. • **1**—802.11n. • **2**—802.11ac. $4: RSSI on the link.
Severity level	5
Example	WMESH/5/MESH_LINKUP: Mesh link on interface 51 is up: peer MAC = 50da-00d2-4b50, peer radio mode = 0, RSSI = 74.
Explanation	A mesh link was established.
Recommended action	No action is required.

MESH_REVOPEN_MAC

Message text	Received a link open request from AP [MAC] in confirm received state.
Variable fields	$1: AP MAC address.
Severity level	5
Example	WMESH/5/MESH_REVOPEN_MAC: Received a link open request from AP 50da-00d2-4b50 in confirm received state.
Explanation	The MP received a Link Open request in confirm received state.
Recommended action	No action is required.

WRDC messages

This section contains WRDC messages.

WRDC_USER_DELETE

Message text	-UserMAC=[STRING]-UserIP=[IPADDR]. A user was deleted.
Variable fields	$1: Client MAC address. $2: Client IP address.
Severity level	6
Example	WRDC/6/WRDC_USER_DELETE: -UserMAC=0021-0011-0033-UserIP=192.168.1.2. A user was deleted.
Explanation	The WLAN roaming center deleted a client entry after the client went offline from all ACs.
Recommended action	No action is required.

WRDC_USER_OFFLINE

Message text	-UserMAC=[STRING]-UserIP=[IPADDR]-ACIP =[IPADDR]; A user went offline. Reason: [STRING].
Variable fields	$1: Client MAC address. $2: Client IP address. $3: IP address of the AC from which the client came online. $4: Reason: • **User request**—The client requested to go offline. • **DHCP release**—The DHCP release of the client's IP address has expired. • **Other reason**.
Severity level	6
Example	WRDC/6/WRDC_USER_OFFLINE: -UserMAC=0021-0011-0033-UserIP=192.168.1.2-ACIP=192.168.3.1; A user went offline. Reason: User request.
Explanation	A client went offline.
Recommended action	No action is required.

WRDC_USER_ONLINE

Message text	-UserMAC=[STRING]-UserIP=[IPADDR]-ACIP=[IPADDR]. A user came online.
Variable fields	$1: Client MAC address. $2: Client IP address. $3: IP address of the AC from which the client came online.
Severity level	6
Example	WRDC/6/WRDC_USER_ONLINE: -UserMAC=0021-0011-0033-UserIP=192.168.1.2-ACIP=192.168.3.1. A user came online.
Explanation	A client came online.
Recommended action	No action is required.

WRDC_USER_ROAM

Message text	-UserMAC=[STRING]-UserIP=[IPADDR]. A user roamed from AC [IPADDR] to AC [IPADDR].
Variable fields	$1: Client MAC address. $2: Client IP address. $3: IP address of the AC from which the client came online before roaming. $4: IP address of the AC from which the client came online after roaming.
Severity level	6
Example	WRDC/6/WRDC_USER_ROAM: -UserMAC=0021-0011-0033-UserIP=192.168.1.2. A user roamed from AC 192.168.3.1 to AC 192.168.3.2.
Explanation	A client performed an inter-AC roaming.
Recommended action	No action is required.

WSA messages

This section contains Wireless Spectrum Analysis (WSA) messages.

WSA_DEVICE

Message text	[APID: UINT32, RADIOID: UCHAR]; [STRING] detected.
Variable fields	$1: AP ID. $2: Radio ID. $3: Interference devices. Options include the following: o Microwave ovens. o Microwave oven inverters. o Bluetooth devices. o Other fixed frequency devices. o Cordless phones using fixed frequency. o Video devices using fixed frequency. o Audio devices using fixed frequency. o Other hopper frequency devices. o Frequency-hopping cordless phone bases. o Frequency-hopping cordless networks (2.4 GHz). o Microsoft Xboxes. o Other devices. o Frequency-hopping cordless networks (5 GHz).
Severity level	5
Example	WSA/5/WSA_DEVICE: [APID: 1, RADIODID: 2]; Bluetooth devices detected.
Explanation	The radio interface of an AP detected an interference device.
Recommended action	Determine whether the device has suffered an attack.