Release Notes

Basic Information

Product Model	• ADS NX3-200E • ADS NX3-600E • ADS NX3-800E • ADS NX3-2010 • ADS NX3-2020 • ADS NX5-4020 • ADS NX5-6025 • ADS NX3-2020E • ADS NX5-4020E • ADS NX5-6025E • ADS NX5-8000 • ADS NX5-10000
Software Version	V4.5R90F01
Upgrade File	• ADS_x86_V4.5R90F00.patch-R90F00-to-R90F01.20180817.zip MD5 value: 4688f259c30b85263c3af720e7dc38b0 • update_ADS_x86_V4.5R90F01_20180917.zip MD5 value: 783d0d581ccc171874fce73594e06033 • update_ADS_10000_V4.5R89F00_20180815.tar.gz.en MD5 value: aeb03f64065b8ebe88cdc35744c7707b • update_ADS_10000_V4.5R90F01_20180917.tar.gz.en MD5 value: 7121eb608858f7c1444eb9e1b755870a
Release Date	2018-11-07
How to Obtain	Contact NSFOCUS technical support.

Version Mapping

Source Software Version	V4.5R90F01
Product Model	• NSF1100-1 • NSF1100-3 • NSF2800-2 • NSF2800-6 • NSF3600-4 • HTCA-6U
Network Traffic Analyzer Platform Version	• V4.5.61.2.BF19 • V4.5.61.2.BF20 • V4.5R90F01
Management Platform Version	ADS M V4.5R90F01
Client	None
Other System or Tool	None
Documentation	NSFOCUS ADS User Guide (V4.5R90F01)

Function Changes

1. Changes of Functions in V4.5R90F01

The following models are supported:

- ADS NX3-200E/600E/800E
- ADS NX3-2010/2020/2020E
- ADS NX5-4020/4020E/6025/6025E
- ADS NX5-8000
- ADS NX5-10000

1.1 Support for Hardware Platforms

The following table lists the mappings between product models and software versions:

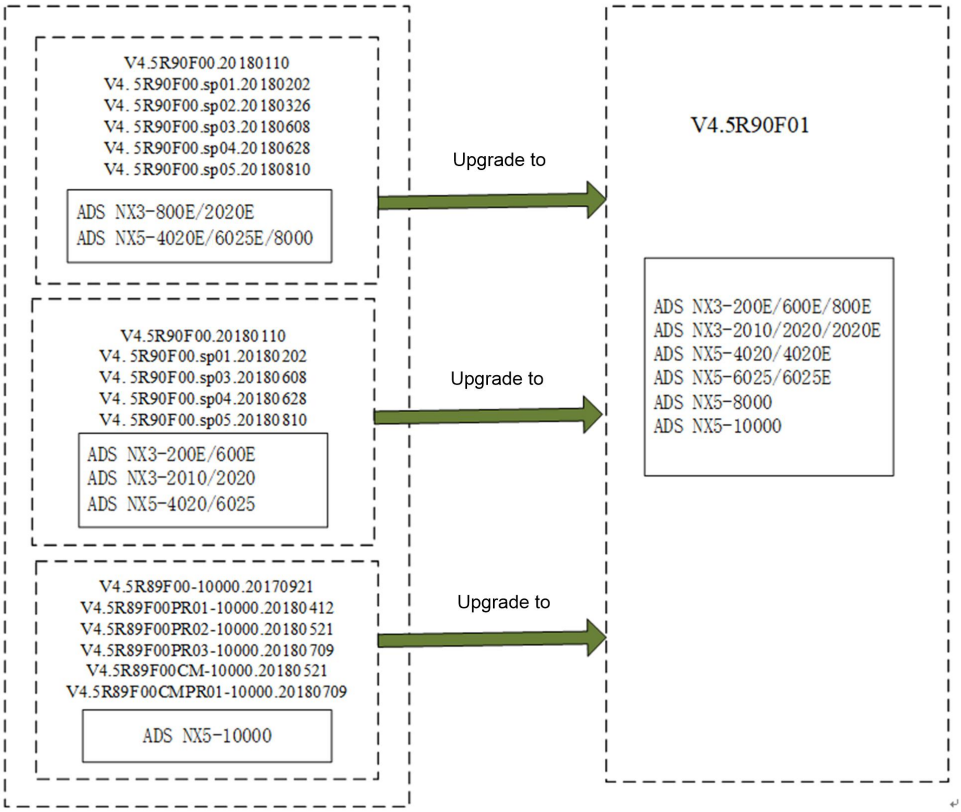
Product Model	V4.5R90F00	V4.5R89F00-10000/V4.5R89F00CM-10000	V4.5R90F01
ADS NX3-2010	Support	--	Support
ADS NX3-2020	Support	--	Support
ADS NX5-4020	Support	--	Support

Product Model	V4.5R90F00	V4.5R89F00-10000/V4.5R89F00CM-10000	V4.5R90F01
ADS NX5-6025	Support	--	Support
ADS NX5-8000	Support	--	Support
ADS NX3-200E	Support	--	Support
ADS NX3-600E	Support	--	Support
ADS NX3-800E	Support	--	Support
ADS NX3-2020E	Support	--	Support
ADS NX5-4020E	Support	--	Support
ADS NX5-6025E	Support	--	Support
ADS NX5-10000	--	Support	Support

From the preceding table, we can see that V4.5R90F01 is applicable to all hardware platforms supported by V4.5R90F00, V4.5R89F00-10000, and V4.5R89F00CM-10000 as well as their SP/PR versions. That is to say, V4.5R90F01 supports all ADS M models, including ADS NX3-200E, ADS NX3-600E, ADS NX3-800E, ADS NX3-2010, ADS NX3-2020, ADS NX5-4020, ADS NX5-6025, ADS NX3-2020E, ADS NX5-4020E, ADS NX5-6025E, ADS NX5-8000, and ADS NX5-10000.

For all preceding models available on the market except ADS NX5-10000, users need to first upgrade them to V4.5R90F00 or one of its SP versions (V4.5R90F00.20180110, V4. 5R90F00.sp01.20180202, V4.5R90F00.sp02.20180326, V4.5R90F00.sp03.20180608, V4.5R90F00.sp04.20180628, or V4.5R90F00.sp05.20180810) and then apply the upgrade package **V4.5R90F00.patch-R90F00-to-R90F01** before upgrade to V4.5R90F01. Note that some models do not support the upgrade to V4.5R90F01 from V4. 5R90F00.sp02.

For ADS NX5-10000, users need to first apply the patch package **V4.5R89F00.patch-to-R90F01** on a mainline version (V4.5R89F00-10000.20171026, V4.5R89F00PR01-10000.20180412, V4.5R89F00PR02-10000.20180521, V4.5R89F00PR03-10000.20180709, V4.5R89F00CM-10000.20180521, or V4.5R89F00CMPR01-10000.20180709) before upgrade to V4.5R90F01.



1.2 Overview of Function Changes in V4.5R90F01

1.2.1 New Functions

This document only describes differences between V4.5R90F01 and V4.5R90F00.

For ADS NX5-10000, users can also see the following documents for detailed function changes from upgrade from V4.5R89F00-10000 or V4.5R89F00CM-10000 to V4.5R90F01:

- PVD-ADS-V4.5R89F01CN Release Notes.doc
- PVD-ADS-V4.5R90F01 Release Notes.doc
- PVD-ADS-V4.5R89F03 Release Notes.doc
- PVD-ADS-V4.5R90F00 Release Note.doc

Function	Description
Attack type optimization	According to the DDoS attack classification standard universally acknowledged in the industry, attacks are re-classified into the same 25 types for both attack logs and attack events.
Optimization in manual packet capture	The capture duration parameter is added for manual packet capture tasks. When the capture duration runs out, the capture task stops.
Web operation and maintenance	An independent O&M module is added on the web-based manager. **Network Diagnosis** is moved from **System > Others** to the **O&M** module, where an interface is added respectively for checking the trust status of source IP addresses and the protection status of

Function	Description
	destination IP addresses/ports
Management interface access control	After management interface access control rules are configured, IP addresses beyond the allowed list will be denied access to ADS (whether via web, SSH, or ping).
Control of web access and SSH access to service interfaces	This function is added to enable or disable the control of web access and SSH access to each service interface.
More Web APIs	Web APIs are added for pattern matching configuration, query of the protection status of protection objects (destination IP addresses or destination IP addresses + ports), and query of the protection status of source IP addresses.
Device resource monitoring threshold configuration	Hardware resource alert threshold configurations are added to serve as a basis for hardware alert log sending via syslog and SNMP and system resource presentation on the **Real-Time Monitoring** page.
SeqCheck algorithm for SYN flood protection	The third SYN algorithm, SeqCheck, is added. When SYN algorithms 1 and 2 can do nothing about SYN flood attacks, users can try the new algorithm.
Increase of DNS keyword checking rules to 20 for a protection group	The maximum number of DNS keyword checking rules that can be referenced by a protection group is increased from 10 to 20.

1.2.2 Optimized Functions in V4.5R90F01 After Upgrade from V4.5R90F00

The following table lists functions affected by upgrade from V4.5R90F00 to V4.5R90F01.

Function	V4.5R90F00	V4.5R90F01	Description
Attack type optimization	Attacks are classified into 12 types for attack logs but 7 types for attack events.	Attacks are classified into 25 types for both attack logs and attack events.	Third-party management platforms, when parsing attack logs or attack events reported by ADS, can refer to this new attack classification method for adaptation.
Management interface access control	--	New function	Users can configure rules to allow or forbid specified source IP addresses to access the management interface. In the latter case, ADS drops any packets that are from the specified IP addresses and destined for its management interface.
Service interface access control	--	New function	This function controls whether service interfaces can be accessed via SSH or web.
SYN-SeqCheck algorithm	SYN flood protection	New SYN protection algorithm	A new SYN protection algorithm is added for algorithm diversification.
Hardware resource monitoring optimization	Different sets of hardware alert thresholds work for system resource	The same set of thresholds works simultaneously for system resource monitoring as well	Only one set of hardware alert thresholds are used across the system.

Function	V4.5R90F00	V4.5R90F01	Description
	monitoring in web mode as well as hardware resource alerting via syslog and SNMP traps.	as hardware resource alerting via syslog and SNMP traps.	
System time	Uses local time.	Uses UTC time.	After the upgrade, **make sure that the system time is calibrated** to avoid time incoherence before and after the upgrade.

1.3 Details of Function Changes in V4.5R90F01

1.3.1 Attack Type Optimization

1. Function Description

As DDoS attacks evolve, with the 12 attack log types and 7 attack event types previously defined in its protection mechanism, ADS cannot accurately identify new attack types that have emerged in recent years. Based on attack classification universally acknowledged in the industry, ADS V4.5R90F01 refines its original attack classification by expanding it to 25 attack types. In addition, it aligns attack log types with attack event types, both of which share the same meanings. In this way, ADS can record attack traffic logs more accurately.

2. Notes

- Due to the great changes made to attack types, a third-party platform should exercise caution in analysis of attack events exported from ADS to avoid mismatching attack types.
- For details on attack types, see the *PVD-ADS-V4.5R90F01 Attack Log Description*.

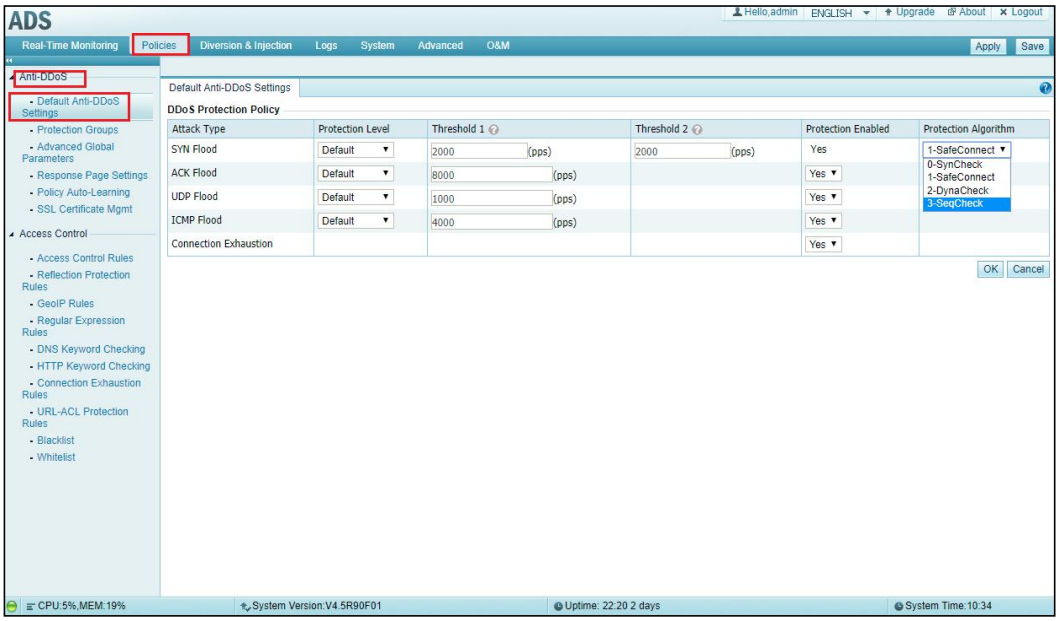
1.3.2 SYN-SeqCheck Algorithm

1. Function Description

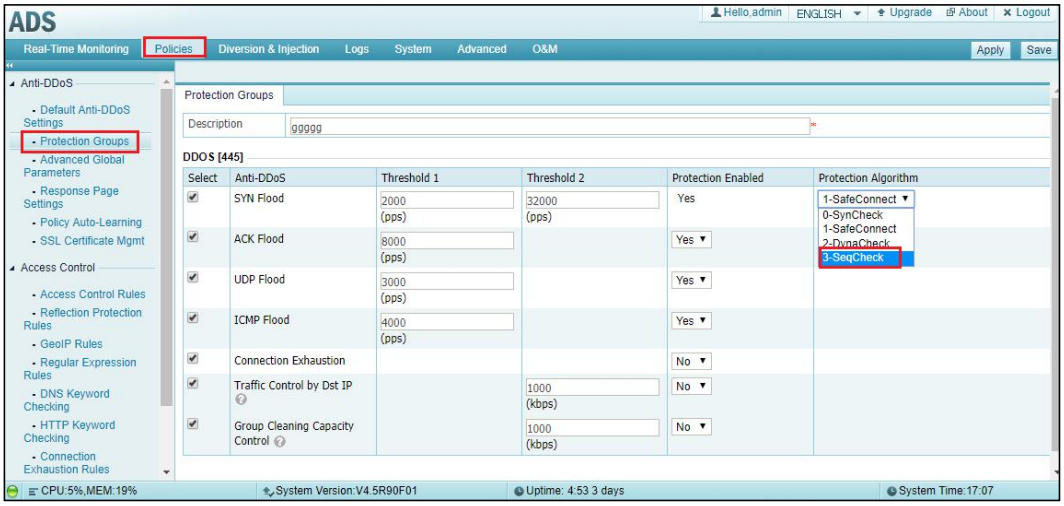
The SYN-SeqCheck algorithm is added for SYN protection. When SYN-SeqCheck is used, if clients do not attempt TCP retransmission after disconnection, ADS can still verify the authenticity of clients and at the same time allow real clients to use the same TCP connection to continue communicating with the server.

2. Configuration

- For the default setting: Choose **Policies > Anti-DDoS > Default Anti-DDoS Settings**.



- For group-specific setting: Choose **Policies > Anti-DDoS > Protection Groups** and then click in the **Edit Policy** column of a group.



3. Notes

When the SeqCheck algorithm is used, a few attack packets may be transparently transmitted to the server. In view of this, this new algorithm is used only when SYN algorithms 1 and 2 are incapable of dealing with attacks.

1.3.3 Hardware Resource Monitoring Optimization

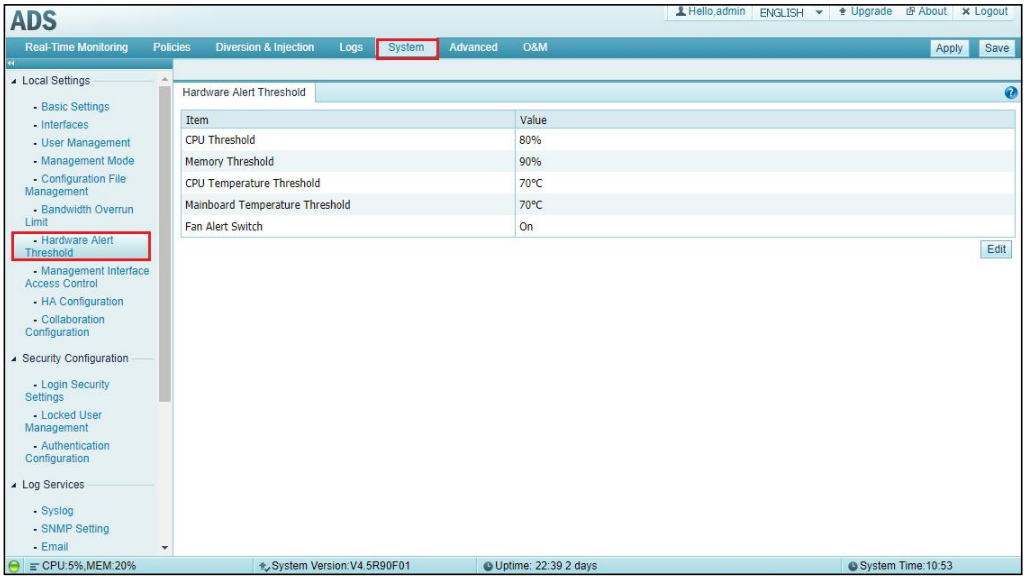
1. Function Description

Unified control is exercised over thresholds for the CPU usage, CPU temperature, memory usage, and mainboard temperature. Also, the fan alert switch is added.

- Monitoring information of the CPU usage, CPU temperature, memory usage, mainboard temperature, fan status, and power supply status (this is unique to ADS 8000) is displayed based on unified thresholds in the **System Resources** area of the **Real-Time Monitoring** page.
- If **Threshold exceeding alert** is selected for **Alert Type** on the **SNMP Trap Setting** page, alerts will be sent via SNMP traps when a threshold set on the **Hardware Alert Threshold** page is exceeded.
- If **Threshold exceeding alert** is selected for **Alert Type** on the **Syslog** page, alerts will be sent via syslog when a threshold set on the **Hardware Alert Threshold** page is exceeded.

2. Configuration

Choose **System > Local Settings > Hardware Alert Threshold**.



3. Notes

- Object identifiers (OIDs) are added to SNMP GET requests for respectively getting the CPU usage, memory usage, CPU temperature, mainboard temperature, fan status, and power supply status. For details, see the *PVD-ADS-V4.5R90F01 SNMP Description*.
- Some ADS 8000 devices support power supply alerts, but other devices do not and therefore display no such information.

1.3.4 Capture Duration Added for Manual Capture Tasks

1. Function Description

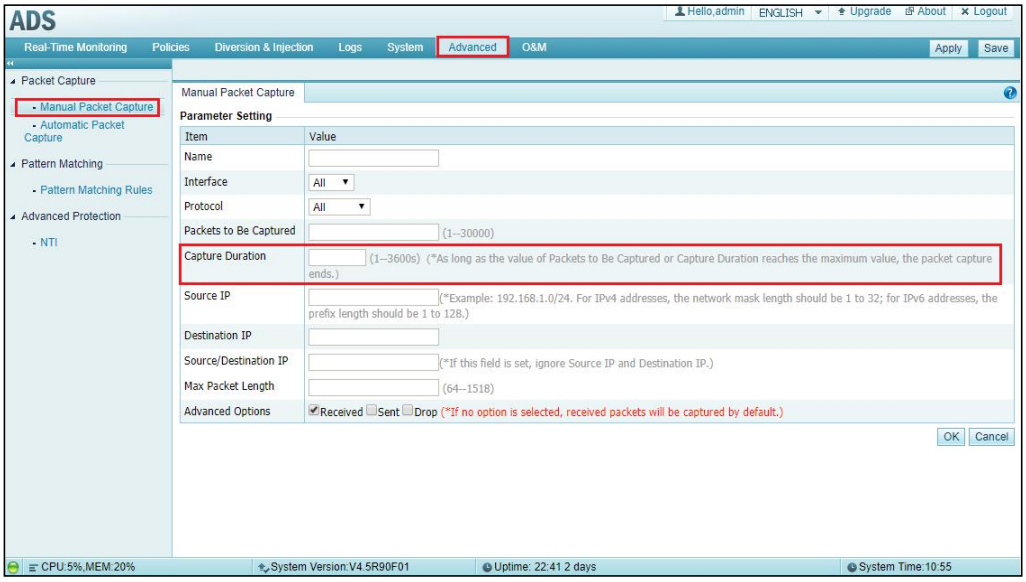
The **Capture Duration** parameter is added on the manual capture task configuration page. Users must configure this parameter or **Packets to Be Captured**, or they can configure both, with the following results:

- If only **Capture Duration** is configured, the packet capture task stops when the allowed capture duration runs out or when the number of packets to be captured reaches the maximum value allowed (30000), whichever comes earlier.
- If only **Packets to Be Captured** is configured, the packet capture task stops when the specified number of packets are captured.

- When both **Capture Duration** and **Packets to Be Captured** are configured, the packet capture task stops when either the allowed capture duration runs out or the specified number of packets are captured.

2. Configuration

Choose **Advanced > Packet Capture > Manual Packet Capture**.

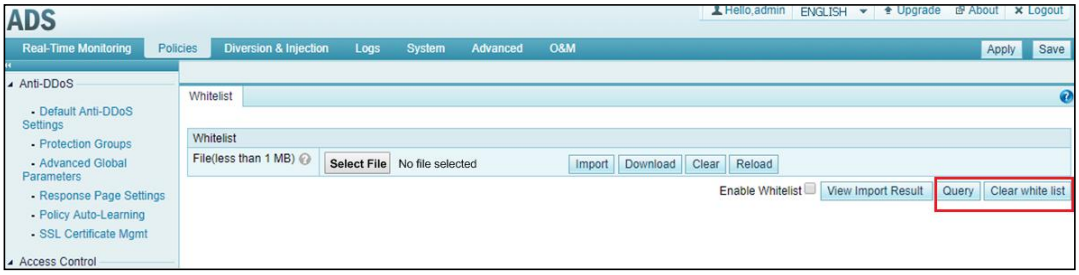


1.3.5 Changes to the Whitelist

1. Function Description

Some descriptions and functions are modified on the **Whitelist** page. Also, the function of querying the trust status of source IP addresses is separated from the whitelist.

- The **Clear Trust** button is changed to **Clear white list**.



- The function of checking whether an IP address exists in the whitelist is moved to the **Trusted IP** page under **O&M > Device Protection Status**.

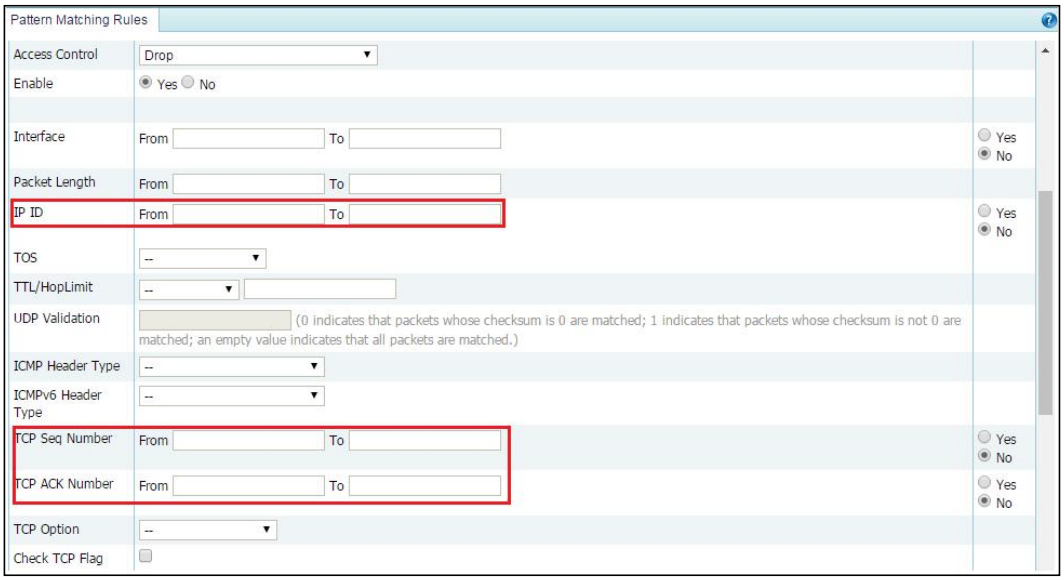
1.3.6 IP ID and TCP Seq/ACK Number Added for Pattern Matching

1. Function Description

To further improve the function of pattern matching, V4.5R90F01 adds three parameters: **IP ID**, **TCP Seq Number**, and **TCP ACK Number**, as shown in the following figure.

2. Configuration

Choose **Advanced > Pattern Matching > Pattern Matching Rules**.



1.3.7 New Web APIs

1. Function Description

The following web APIs are added. For details, see the *PVD-ADS-V4.5R90F01-Web API Description*.

- Web API for query of the protection status of destination IP addresses or destination IP addresses and ports
- Web API for query of the trust status of source IP addresses
- Web API for pattern matching

1.3.8 Increase of DNS Keyword Checking Rules to 20 for a Protection Group

1. Function Description

In previous versions, the DNS keyword checking policy can reference at most 10 DNS keyword checking rules for a protection group. V4.5R90F01 increases this number to 20.

1.3.9 Filtering of SYN-ACK Packets with Source Port 80

1. Function Description

The CLI command **globalpolicy set synack-filter** can be used to enable or disable the filtering of SYN-ACK packets with source port 80. After an advanced ACK algorithm is selected for the TCP control parameters protection policy and this function is enabled as well, ADS will directly drop SYN-ACK packets with the source port of 80.

This function is disabled by default.

1.3.10 O&M Page

1. Function Description

V4.5R90F01 adds an independent **O&M** page on the web-based manager.
Network Diagnosis is moved from **System > Others** to the **O&M** module, where an interface is added respectively for checking the trust status of source IP addresses and the protection status of destination IP addresses/ports, to facilitate system O&M and let users quickly learn the real-time protection status.

2. Configuration

Trusted IP:

Choose **O&M > Device Protection Status > Trusted IP**.

The trust status query API is added for query of the trust status of both IPv4 addresses and IPv6 addresses.

Protection status:

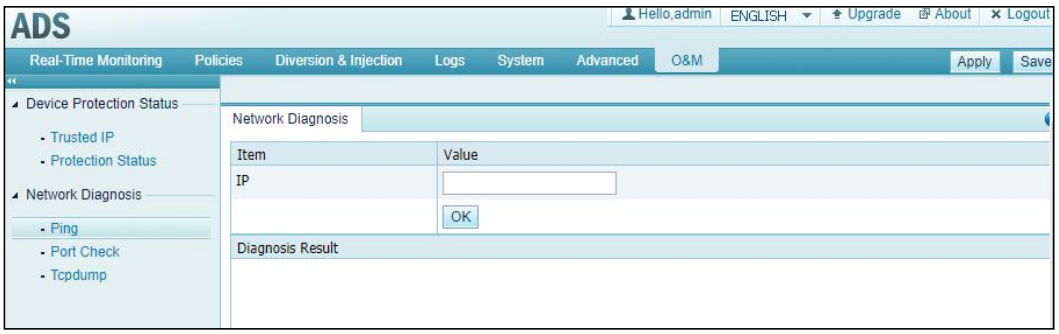
Choose **O&M > Device Protection Status > Protection Status**.

The protection status query API is added for query of protection status of destination IP addresses or destination IP addresses and ports. Both IPv4 and IPv6 addresses can be typed here.

Network diagnosis:

Choose **O&M > Network Diagnosis > Ping**.

The network diagnosis module provides the ping, port check, and tcpdump functions. For details, see the *ADS V4.5R90F00 Release Notes*.



1.3.11 Management Interface Access Control

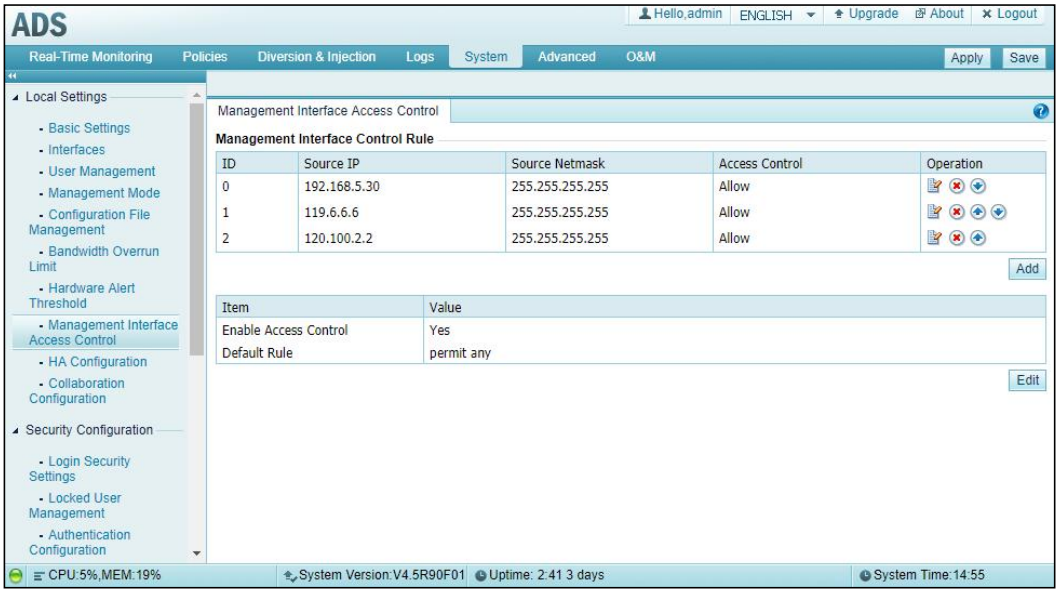
1. Function Description

V4.5R90F01 provides management interface (M interface) access control rules. Users can configure such rules to allow or forbid specified source IP addresses to access the management interface. In the latter case, ADS drops any packets that are from the specified IP addresses and destined for its management interface. Therefore, V4.5R90F01 provides a more secure access control mechanism, making it possible to hide the presence of ADS on the network.

2. Configuration

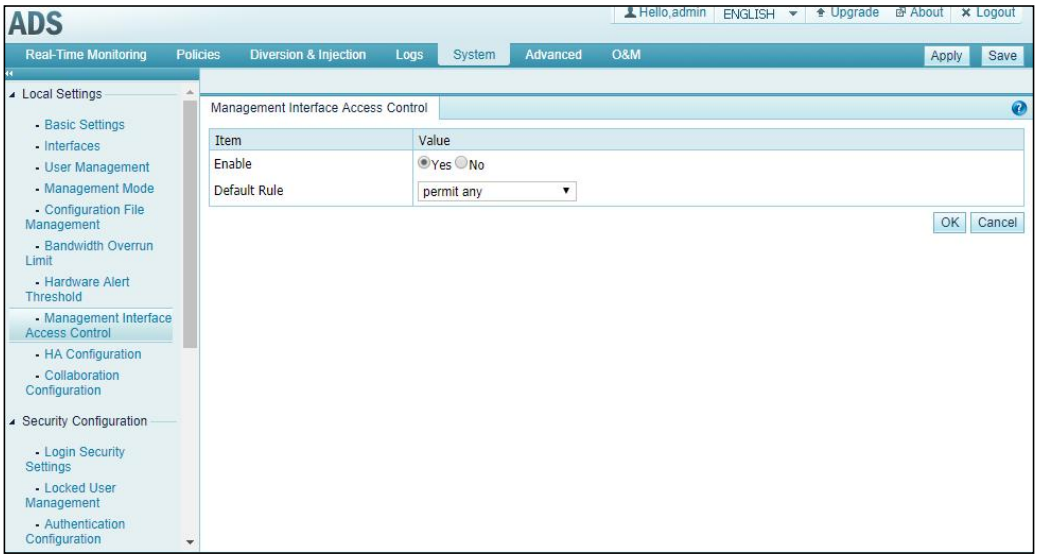
Choose **System > Management Interface Access Control**.

- View management interface access control rules.

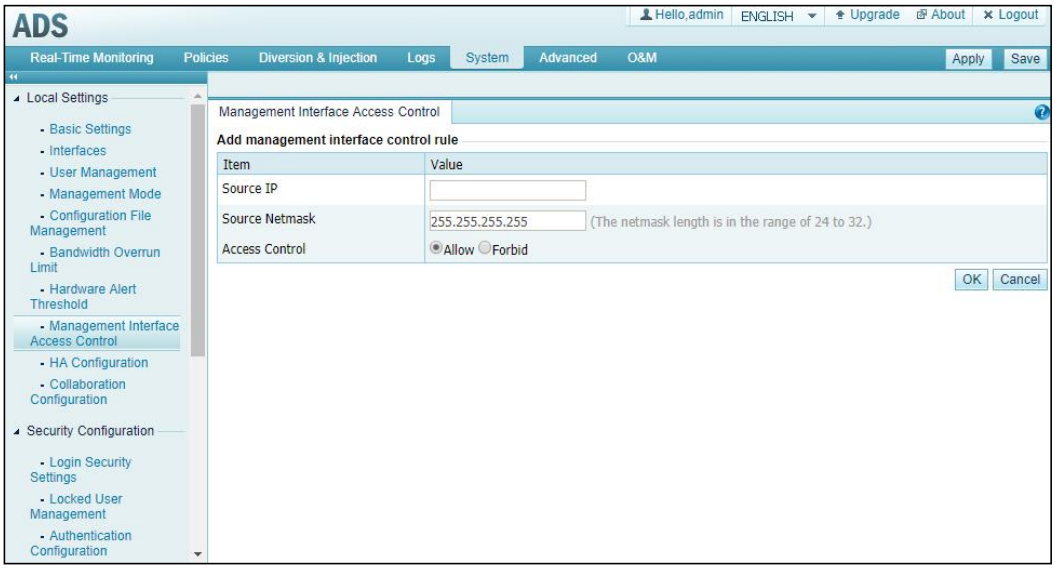


Priorities of these rules can be changed by moving the rules up or down.

- Edit the global access control rule (default rule: **permit any** and **deny all**).



- Create or edit a management interface access control rule.



- Enable or disable management interface access control via the console port.

```
Welcome to Nsfocus ADS
========================================
      1.  IPv4 Network setting
      2.  IPv6 Network setting
      3.  DNS setting
      4.  Console Password change
      5.  Datetime setting
      6.  All Default setting
      7.  Web Password Default setting
      8.  Console time out setting
      9.  Rollback system
      10. System state check
      11. Management interface ACL status
      12. Reboot System
      13. Logout
========================================
Your password is the initial password.
Please choose "Console Password Change" to customize a new one.
Input your selection:
```

After login to the console port as **admin**, select **11** to view the configured management interface access control rules and enable or disable this function.

```
The management interface ACL function has been enabled.
The default ACL action is permit
Management interface ACL list:
10.66.3.3            255.255.255.255     permit
1.2.3.4              255.255.255.255     permit
Do you want to disable management interface ACL function?[yes/no]
```

3. Notes

- Currently, management interface access control works only for IPv4 addresses.
- On the **Login Security Settings** page under **System > Security Configuration**, the **IP Access Control Status** parameter controls web access from source IP addresses to ADS. However, the management interface access control function controls any type of network connections from source IP addresses to the management interface of ADS.
- After management interface access control is enabled, the network diagnosis function may be unavailable. If this function is required, users should create a management interface access control rule to allow the IP address of the diagnosis object to access the management interface.
- A management interface access control rule, if misconfigured, may deny access from a specified IP address, whose access should have been allowed. As a result, this IP address will be unable to access the background or web-based manager of ADS, or successfully ping the management interface of ADS. In this case, the only solution is to log in to the console port to disable management interface access control.
- After management interface access control is enabled, some external IP addresses or domain names (including those of the DNS server and ADS M) will be automatically added to the list of allowed IP addresses. Therefore, this function has no impact on ADS's external connections.

1.3.12 Service Interface Access Control

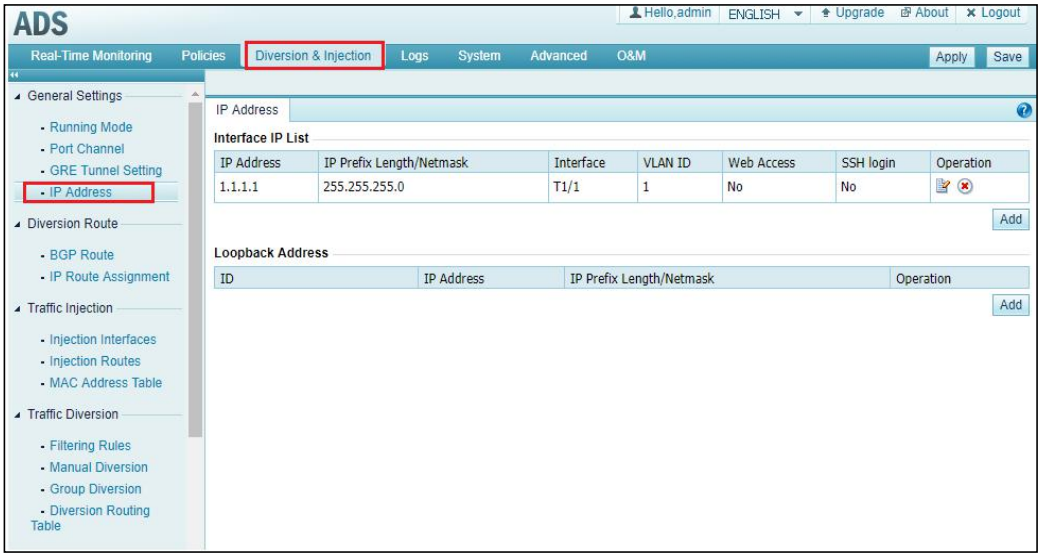
1. Function Description

V4.5R90F01 provides the service interface access control function for users to determine whether a service interface provides web access or SSH access. This function can prevent the scanning for and network intrusions into service interfaces.

2. Configuration

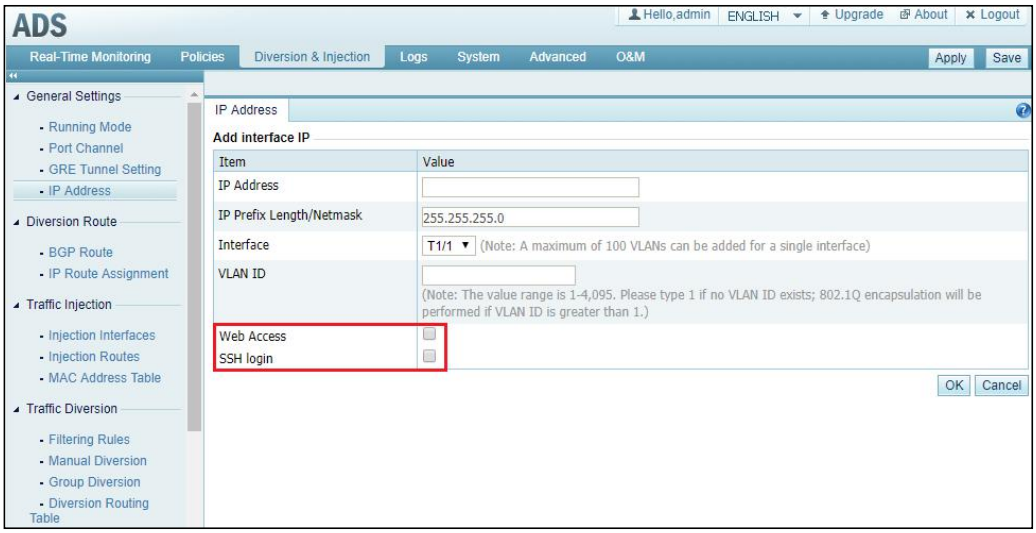
Choose **Diversion & Injection > General Settings > IP Address**.

- View the service interface access control function.



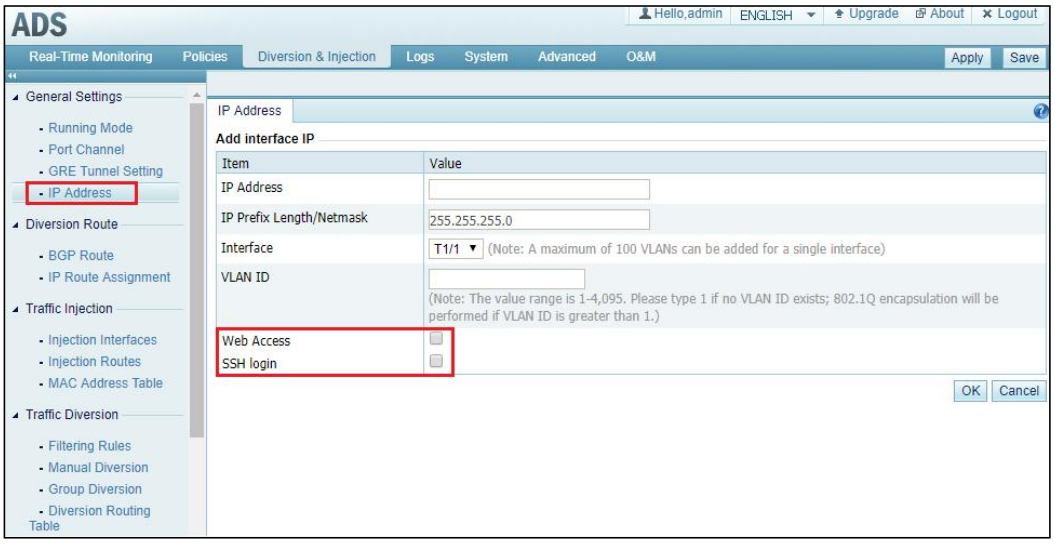
- Configure a service interface access control rule.

  When configuring an IP address for a service interface, users can determine whether this interface can be accessed via web or SSH.



- Edit a service interface access control rule.

  Users can modify a service interface access control rule by editing the IP address of a service interface.



3. Notes

Currently, service interface access control works only for IPv4 addresses.

2. Compatibility with NTA Versions

- ADS V4.5R90F01 can collaborate with NTA 4.5R90F01 and both support IPv4 and IPv6 addresses.
- ADS V4.5R90F01 can collaborate with NTA V4.5.61.2.BF19 and V4.5.61.2.BF20 and support only IPv4 addresses.

3. Supported Browsers

- Internet Explorer 9, 10, and 11
- Chrome
- Firefox

Version Upgrade

1 Upgrade from V4.5R90F00, V4.5R90F00.sp01, V4.5R90F00.sp02, V4.5R90F00.sp03, V4.5R90F00.sp04, or V4.5R90F00.sp05 to V4.5R90F01

V4.5R90F01 is applicable to the following models:

ADS NX3-200E, ADS NX3-600E, ADS NX3-800E, ADS NX3-2010, ADS NX3-2020, ADS NX3-2020E, ADS NX5-4020, ADS NX5-4020E, ADS NX5-6025, ADS NX5-6025E, and ADS NX5-8000

Note: ADS NX3-200E, ADS NX3-600E, ADS NX3-2010, ADS NX3-2020, ADS NX5-4020, and ADS NX5-6025 do not support the upgrade from V4.5R90F00.sp02.

The upgrade to V4.5R90F01 must be performed in strict accordance with the following procedure:

Step 1 Choose **System > Local Settings > Configuration File Management**. In the **Configuration File** area, click **Export** to save the exported configuration file to a local disk.

Step 2 Install the patch package **update_ADS_x86_V4.5R90F00.patch-R90F00-to-R90F01.20180817.zip** (MD5: 4688f259c30b85263c3af720e7dc38b0) on V4.5R90F00 or one of its SP versions.

After the system prompts that the upgrade is completed, restart the device.

Step 3 Install the upgrade package **update_ADS_x86_V4.5R90F01_201917.zip** (MD5: 783d0d581ccc171874fce73594e06033).

After the system prompts that the upgrade is completed, restart the device.

Step 4 Verify that the system version is V4.5R90F01.

Note: If the upgrade fails, please contact NSFOCUS technical support.

----End

2 Rollback to V4.5R90F00 from V4.5R90F01

V4.5R90F01 does not support the rollback to a previous version in a command line interface (CLI) window. If rollback is required, contact please contact NSFOCUS technical support and provide the configuration file exported in Step 1 to them.

3 Upgrade from V4.5R89F00-10000, V4.5R89F00PR01-10000, V4.5R89F00PR02-10000, V4.5R89F00PR03-10000, V4.5R89F00CM-10000, or V4.5R89F00CMPR01-10000 to V4.5R90F01

V4.5R90F01 is also applicable to ADS NX5-10000.

The upgrade to V4.5R90F01 must be performed in strict accordance with the following procedure:

Step 1 Choose **System > Local Settings > Config Import/Export**. In the **Configuration File** area, click **Export** to save the exported configuration file to a local disk.

Step 2 Install the upgrade package **update_ADS_10000_V4.5R89F00.patch-to-R90F01_20180815** (MD5: aeb03f64065b8ebe88cdc35744c7707b) on V4.5R89F00-10000 or one of its PR versions.

After the system prompts that the upgrade is completed, restart the device.

Step 3 Install the upgrade package, **update_ADS_10000_V4.5R90F01_20180917** (MD5: 7121eb608858f7c1444eb9e1b755870a).

After the system prompts that the upgrade is completed, restart the device.

Step 4 Verify that the system version is V4.5R90F01.

Note: If the upgrade fails, please contact NSFOCUS technical support.

----End

4 Rollback to V4.5R89F00-10000 from V4.5R90F01

V4.5R90F01 does not support the rollback to a previous version in a CLI window. If rollback is required, contact NSFOCUS technical support and provide the configuration file exported in Step 1 to them.

A IPv4/IPv6 Support

The following table lists all modules of ADS V4.5R90F01 and indicates whether they support IPv4 and IPv6.

Module	Function	IPv4	IPv6
Real-Time Monitoring			
Policies	SYN flood detection	√	√
	ACK flood detection	√	√
	UDP flood detection	√	√
	ICMP flood detection	√	√
	HTTP protection	√	√
	HTTPS protection	√	×
	DNS protection algorithms 1 and 2	√	√
	DNS protection algorithm 3	√	×
	DNS protection algorithm 4	√	√
	TCP control parameters	√	√
	TCP control parameters – TCP fragment control	√	×
	IP behavior control	√	×
	SIP protection – default DDoS	√	×
	SIP protection – groups	√	√
	UDP payload check – payload check	√	√
	UDP payload check – mode check	√	×
	UDP protection – UDP fragment control	√	×
	ICMP fragment control	√	×
	UDP protection – drop UDP fragments – groups	√	×
	UDP protection – maximum packet length	√	√
	UDP protection – traffic control by Src IP + Src port	√	√
	UDP protection – traffic control by Dst IP + Dst port	√	√
	UDP protection – traffic control by Src IP	√	√
	UDP protection – traffic control by Dst IP	√	√
	UDP protection – minimum packet length	√	√
	UDP protection – traffic control by Dst IP + Src port	√	√
	ICMP traffic rate limiting	√	√

Module	Function	IPv4	IPv6
	Watermark protection	√	×
	Protocol ID check	√	√
	Group traffic control	√	√
	Port check	√	√
	URL rules	√	√
	Advanced global parameters	√	√
	Policy auto-learning	√	√
	Access control rules	√	√
	Reflection protection rules	√	√
	GeoIP rules	√	√
	Regular expression rules	√	×
	Hardware access control rules	√	√
	Connection exhaustion rules	√	×
	URL-ACL protection rules	√	√
	Blacklist	√	×
	Whitelist	√	√
	HTTP keyword checking	√	×
	DNS keyword checking	√	×
Diversion & Injection	Running mode	√	√
	Port channel configuration	√	√
	IP address configuration	√	√
	Working interface access control (web and SSH)	√	×
	BGP diversion	√	√
	OSPF diversion	√	√
	ISIS diversion	√	×
	RIP diversion	√	×
	LDP diversion	√	×
	IP route assignment	√	√
	Injection interface	√	√
	Layer 2 injection	√	√
	Layer 3 injection	√	√
	MPLS injection	√	×
	MPLS VPN injection	√	×

Module	Function	IPv4	IPv6
	GRE tunnel injection	√	×
	MAC address table	√	√
	Filtering rules	√	√
	Manual diversion	√	√
	Group diversion	√	√
	Diversion routing table	√	√
	MPLS route	√	×
	Syslog diversion configuration – collaboration with Genie devices	√	×
	Syslog diversion configuration – collaboration with Arbor devices	√	×
	Syslog diversion configuration – collaboration with Samurai devices	√	×
	Syslog diversion configuration – collaboration with Kuanguang devices	√	×
Collaboration	Collaboration with ADS M	√	√
	Collaboration with ESPP	√	×
	Collaboration with NTA V4.5.61.2	√	×
	Collaboration with NTA V4.5R90F01	√	√
Logs	Attack logs	√	√
	System operation logs	√	√
	System login logs	√	√
	Link status logs	—	—
	Traffic diversion logs	√	√
	HA synchronization logs	√	√
	Syslog diversion logs	√	×
System	Basic settings	√	√
	Interface link configuration	—	—
	System user management	√	√
	Management mode configuration	√	√
	Configuration file management	√	√
	HA configuration	√	√
	Management interface access control	√	×
	Collaboration configuration	√	×
	Bandwidth overrun limit	√	×

Module	Function	IPv4	IPv6
	Login security settings	√	×
	Locked user management	√	×
	Authentication configuration	√	√
	Syslog configuration	√	√
	SNMP trap configuration	√	√
	SNMP agent setting	√	×
	Email configuration	√	√
	SFTP/SSH log export	√	×
	License interface	—	—
	License speed limit	—	—
	System upgrade	—	—
	Remote assistance	—	—
	SSL certificate import	—	—
	One-click information collection	—	—
	Version information	—	—
Advanced	Packet capture management	√	√
	Pattern matching rules	√	√
NTI	Upload	√	√
	Synchronization	√	×
	Query	√	×