1 NSFOCUS ADS Release Notes

1. Basic Information

Product Model	• ADS NX3-HD1000 • ADS NX5-HD5000 • ADS NX5-HD6000 • ADS NX3-HD2500 • ADS NX5-HD4500 • ADS NX5-HD6500 • ADS NX5-HD8500 • ADS NX5-8000 • ADS NX5-10000 • ADS NX5-12000 • ADS NX5-20000 • ADS NX5-HFA2000 • ADS NX5-HFB3000 • ADS NX5-HFB6000 • ADS NX5-HFB8000 • ADS NX5-HFC6000 • ADS NX5-HFC8000 • ADS-NX5-HFG10000 • ADS NX1-VN01
Software Version	V4.5R90F07 Build: 50769

Upgrade File	• update_ADS_x86_V4.5R90F07_20251128.zip • MD5: 7d978a57c5fa55d98d64cb28e5028e03 • SHA256: 9e97e264905aabf30f9713b891cc98b1d923b1f976d69dd6199b032dca502716 • update_ADS_arm_V4.5R90F07_20251128.zip • MD5: e003bfa176478505319e9b748691c9c7 • SHA256: 61c737f5c4b08f414a349edd3f4c28ad7289f07eba0100783c006dcf64b15182 • update_ADS_hygon_V4.5R90F07_20251128.zip • MD5: fea56d436dc27f664f87166a342e45ed • SHA256: 51ec0ff95db102e6d16b00adbbfb2aa0eb26184ea27fef028cc4f0156e293e6e
Release Date	2025-11-30
How to Obtain	Obtain the upgrade file from the upgrade system or contact NSFOCUS technical support.

2. Version Mapping

Source Software Version	V4.5R90F06 and later
Product Model	• X86 platform: HD1000, HD5000, HD6000, HD2500, HD4500, HD6500, HD8500, 8000, 10000, 12000, and 20000 • Phytium platform: HFA2000 and HFB3000 • Hygon platform: HFB6000, HFB8000, HFC6000, HFC8000, and HFG10000
Management Platform	• ADS M: V4.5R90F07 • ADBOS: V4.5R90F07 • ISOP: V3.0R01F08SP03 and V3.0R02F00 • NPAI: 3.2.0
Software Client	None
Browser	• Edge • Chrome
Documentation	• NSFOCUS ADS V4.5R90F07 User Guide • NSFOCUS ADS V4.5R90F07 Deployment Guide

3. Satisfied Requirements and Fixed Bugs

3.1 Satisfied Requirements

Requirement ID	Description	Remarks

3.2 Fixed Bugs

Bug ID	Severity	Type	Function/Component	Description
ADS-58591	Normal	Defect	Policy	In in-path mode, traffic from the outgoing interface is mitigated, even though it should not be, when the reflection protection rule, programmable protection rule, allowlist, or LAND protection policy is triggered.
ADS-59875	Normal	Defect	Attack log	A large number of false attack logs are generated for a chassis device when multiple service boards become abnormal and there is no service traffic at all.
ADS-60017	Normal	Defect	Traffic diversion log	Occasionally, logs cannot be loaded on the web page.
ADS-57894	Normal	Defect	Manual traffic diversion	When multiple manual diversion rules that have overlapping IP addresses or IP ranges are all enabled, disabling one of these rules will cause the remaining enabled manual diversion rules to mismatch the active routes in the diversion routing table.
ADS-60001	Normal	Defect	Injection routes	When injection routes are synchronized with the secondary device in a cluster deployment, the disabled injection routes still take effect on the engine of the secondary device.
ADS-58953	Normal	Defect	External bypass	There is a small probability of failure when disabling the external bypass.
ADS-58523	Normal	Defect	Management interface access control	Occasionally, blocked IP addresses can still access the device.
ADS-54844	Normal	Defect	Chassis	Occasionally, chassis devices fail to update the license, obtain service board resources, and execute the **ipmitool** command.
ADS-58564	Normal	Defect	Group diversion	When users attempt to edit the diverted IP addresses of a protection group, the system prompts that editing is not allowed, followed by an "Undefined" error pop-up.
ADS-59915	Normal	Defect	System resources	The CPU temperature displayed on the **Real-Time Monitoring** Page of the HD4500 model is much lower than the actual temperature.
ADS-60065	Normal	Defect	Attack traffic statistics report	The traffic statistics displayed in the **Traffic Trend** and **Attack Traffic** charts are

Bug ID	Severity	Type	Function/Component	Description
				inaccurate.
ADS-60008	Normal	Defect	HA	Configuration synchronization is not performed as expected in active-active mode.
ADS-59876	Normal	Defect	GeoIP	After GeoIP rules are added to a configured protection group, these rules do not take effect until the protection group is configured again.
ADS-58951	Normal	Defect	System resources	The disk status indicator on the **Real-Time Monitoring** page of the web-based manager is red, but the disk is still functioning properly.
ADS-60071	Normal	Defect	User management	For TACACS+ authentication, the system prompts users to modify their password when it expires. However, password age verification does not apply to TACACS+ authentication.
ADS-60093	Normal	Defect	HA	After the IP address of the management interface is changed, **Local IP** on the **Modify Basic Settings** page cannot be changed.
ADS-60094	Normal	Defect	System	When the device is powered on with the hard drive removed, Apache fails to start, resulting in web pages being inaccessible.
ADS-60097	Normal	Defect	Compatibility	Some browsers do not support the UKEY authentication.

4. Opened Ports

Peer Device	Connection	Protocol	Service	Port	Opened by Default	Configurable
Browser or client	Requesting client – Apache	TCP	Apache	443	☑	☑
Client	Requesting client – SSH	TCP	CLI	22	□	□
Client	Requesting client – SSH	TCP	Remote assistance	Random	□	☑
Client	Requesting client – SNMP agent	TCP/UDP	SNMP agent	161	□	□
Diversion-purpose collaborating device	NTA – ADS	TCP	Diversion scheduling	8342	□	□

5. Function Changes

5.1 New Functions

New Function	Description
Hardware-side time sequence check	The hardware-side time sequence check feature is added in the hardware-side control policy configuration. You can configure it as required.
SYN-ACK/ACK/UDP/ICMP/DNS query/DNS reply time sequence check	The SYN-ACK, ACK, UDP, ICMP, DNS query, and DNS reply time sequence check features are added for protection groups. They can be configured to defend against bogus source attacks.
Botnet & IP connection anomaly detection	The botnet & IP connection anomaly detection function is added for protection groups. It can be configured to identify anomalous connections from the trusted source.
QUIC protection policy	The QUIC protection policy is added for protection groups. It can be configured to defend against attacks targeting the QUIC protocol.
Auto-learning of protection thresholds in the carpet bombing protection policy	The carpet bombing protection rule can auto learn the network segment-specific maximum packet count of various protocols, which can help improve configuration accuracy.
DNS protection in the carpet bombing protection policy	The UDP **Threshold 1** of the carpet bombing protection rule includes the count of DNS packets. DNS protection is also included in the network segment-specific protection.
Configuring carpet bombing protection by target type	The target type can be specified in the behavior-based carpet bombing protection policy. The destination port-based scanning protection is also supported.
GeoIP rule optimization	The protocol type, destination port, and one or more source locations can be configured for a GeoIP rule. GeoIP rules can be reordered.
Specifying multiple ports in the group-specific HTTPS protection policy	Multiple HTTPS ports or port ranges can be configured in an HTTPS protection policy to protect multiple application services.
Expanded method types in the HTTP keyword checking policy	New HTTP method options are added in the HTTP keyword checking rule configuration to expand the inspection scope.
Support for the hybrid IPv4/IPv6 proxy scenario	The hybrid IPv4/IPv6 proxy protection supports parsing of IPv4-over-IPv6 and IPv6-over-IPv4 packets.
Specifying a packet length range in the reflection protection rule	The package length range can be configured in a reflection protection rule for more precise control.
Adjusting the threat intelligence IP address range via the CLI	A CLI command can be used to modify the threat level of threat-intelligence IP addresses to be issued.
Expanded destination-IP traffic control threshold for protection groups	The destination-IP traffic control threshold for protection groups is increased.
BGP FlowSpec feature	The FlowSpec diversion and FlowSpec diversion routing table are added. The BGP FlowSpec feature enables more precise control traffic.
Port synchronization in IN/OUT interface pair configuration	In in-path mode, you can choose whether to enable port synchronization for an IN/OUT interface pair.

New Function	Description
SSL email transmission	Emails can be transmitted using SSL encryption to improve security.
Import and export of selected configuration files	Some configuration files can be exported and imported individually.
Export of access control rules	Access control rules can be exported.
Web API log query	Web API logs can be filtered by specific fields.
System restart prompt optimization	For operations that require a system restart, the system highlights a device restart prompt.
Some upgrade packages (V4.5R90F07 and later) do not require a device restart after the upgrade is complete.	Some upgrade packages do not require a device restart after the upgrade.
Viewing BGP/LDP configuration and neighbor status via the CLI	You can view the configuration and neighbor status of BGP or LDP via the CLI.
Reverse detection rate control switch in DNS query protection	The reverse detection rate control switch is added in DNS query protection configuration. You can use this switch to enable or disable reverse detection rate control.
Adding the source detection algorithm in DNS response protection	The source detection algorithm is added in DNS response protection configuration to authenticate the source IP address of DNS reply packets.
Adding the source detection algorithm in SYN-ACK protection	The source detection algorithm is added to authenticate the source IP address that initiates SYN-ACK packets.

5.2 Deleted Functions

Function	V4.5R90F06	V4.5R90F07	Change	Reason
Built-in blocklist	The built-in blocklist is available.	Deleted	The built-in blocklist is deleted and no longer effective.	Frequent changes to the blocklist may cause the built-in blocklist to no longer serve its intended purpose.
Log Level	Logs are categorized by different levels.	Deleted	The log level field is no longer displayed in the web-based manager. This change does not affect system functionality.	This is intended to avoid any misunderstanding.
Save button	The **Save** button is available.	Deleted	This change does not affect system functionality.	The device can now automatically save the configuration, eliminating the need for users to save it manually or do so frequently.

5.3 Modified Functions

Function	V4.5R90F06	V4.5R90F07	Change
Changing the threshold names in the anti-DDoS policy of protection groups	**Threshold 1** and **Threshold 2** in the DDoS policy	**Threshold 1** is changed to **Mitigation Threshold** and **Threshold 2** is changed to **Flow Control**. **Threshold 2** for SYN Flood is changed to **Reverse Detection Rate Control** of the SYN control in the TCP control parameters.	These changes do not affect system functionality. The reverse detection rate control switch is added for SYN control.
Support for configuring the netmask of the IP address for a third-party management platform	Netmask configuration is not supported.	Netmask configuration is supported.	This does not affect system functionality.
SSL certificate import	The name of the imported SSL certificate file cannot contain the period (.).	The name of the imported SSL certificate file can contain up to one period (.).	This does not affect system functionality.
Empty connection detection for protection groups	This feature is added in the botnet & IP behavior control policy configuration for protection groups.	Empty connection detection is removed from the botnet & IP behavior control policy to the botnet & IP connection anomaly detection.	Enhanced function.

6. Detailed Description of Function Changes

6.1 Hardware-Side Time Sequence Check

Function Description

The hardware-side time sequence check is added to the hardware control policy configuration. If the device supports smart NICs and has them installed, smart NICs will check whether the destination-IP time sequence check is configured. If such a configuration exists, the smart NICs will discard packets that arrive outside the allowed time sequence when traffic matches the configured time sequence check.

It should be noted that the hardware-side time sequence check configuration for the protected IP addresses will be issued to the smart NICs only when these IP addresses protected by ADS trigger a protocol-specific time sequence check. For the hardware-side time sequence check to take effect, the corresponding time sequence check function must be enabled for the protection group. When the hardware-side time sequence check is globally effective, you can precisely control which protocol-specific time sequence check configuration is issued. When the effective scope is limited to a protection group, the group's hardware-side time sequence

check is disabled by default. You can enable it for the specified group via the CLI, and finely control which protocol-specific time sequence check configuration is issued to the smart NIC.

This feature is also subject to the following conditions:

1. If the trust scope for trust control in the advanced global parameter settings is set to **Group**, the hardware-side time sequence check will not take effect.

2. If there is a non-drop setting in the global rules or group-specific access control rules, the hardware-side time sequence check will not take effect.

3. If the global or group-specific allowlist is enabled, the hardware-side time sequence check will not take effect.

4. If there is a non-drop setting in the global or group-specific GeoIP rules, the hardware-side time sequence check will not take effect.

5. If the programmable protection rules contain a non-drop setting, the hardware-side time sequence check will not take effect.

6. If the collaboration feature is enabled and the role is set to **Lower-level device**, the hardware-side time sequence check will not take effect.

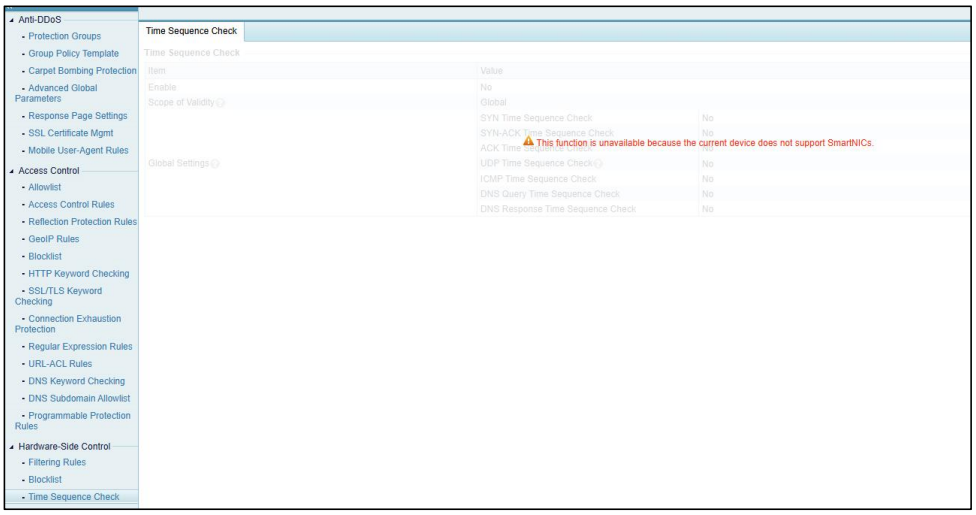
7. If the group-specific UDP session check or QUIC function is enabled, the hardware-side UDP time sequence check for the group's protected IP addresses will not take effect.

This function has the following advantages:

- Smart NICs feature certain algorithmic capabilities and enhanced functionality.
- Algorithm recognition is added in the hardware, allowing smart NICs to handle more scenarios.
- Packets are now dropped on the hardware side, improving the device's processing performance.

Configuration

Policy > Hardware-Side Control > Time Sequence Check



Post-Upgrade Notes

After the upgrade, hardware-side time sequence check is disabled by default.

6.2 SYN-ACK/ACK/UDP/ICMP/DNS Query/DNS Reply Time Sequence Check

Function Description

The SYN-ACK, ACK, UDP, ICMP, DNS query, and DNS reply time sequence check features are added in the protection group policy configuration. After this feature is enabled, the first packet of a session is discarded. If a retransmitted packet arrives within the specified retransmission interval, it passes the algorithm's verification. This feature configuration is also associated with the hardware-side time sequence check configuration. If the device is installed with smart NICs and has the hardware-side time sequence check enabled, and the setting is globally effective, the time sequence check configuration will also be issued to the smart NICs when ADS protection is triggered for the protected IP addresses, based on the time sequence check protection configuration.

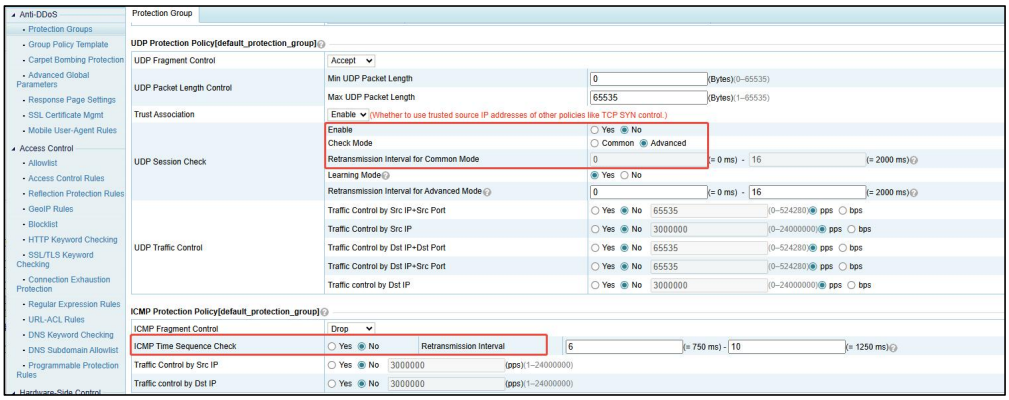
The following should be noted:

- The SYN time sequence check can be enabled only when the **3-SeqCheck** algorithm is not specified.
- The SYN-ACK time sequence check can be enabled only when the **Source detection** algorithm is specified.
- The ACK time sequence check can be enabled only when the **ACK check** algorithm is specified.
- The DNS query time sequence check can be enabled only when the DNS query protection algorithm is neither **1-Default** nor **4-DNS retransmission**.
- The DNS response time sequence check can be enabled only when the **Source detection** algorithm is specified.

Configuration

Policy > Anti-DDoS > Protection Groups

- For the DNS protection policy, configure the DNS query and DNS response time sequence check features.
- For the TCP control parameters, configure the SYN, SYN-ACK, and ACK time sequence check functions.
- For the UDP protection policy, configure the UDP time sequence check function. Setting the check mode to **Common** indicates that the time sequence check is configured.
- For the ICMP protection policy, configure the ICMP time sequence check function.



Post-Upgrade Notes

After the upgrade, the enabling status of the SYN time sequence check remains unchanged. If the SYN retransmission interval is set to a value greater than 255, the maximum value will be changed to 255. However, the time sequence check function is disabled for other protocols.

6.3 Botnet & IP Connection Anomaly Detection

Function Description

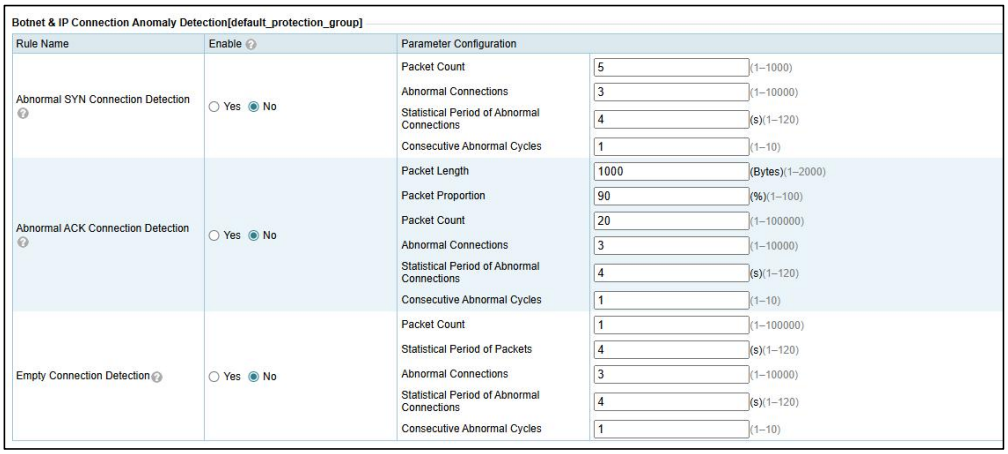
The botnet & IP connection anomaly detection feature is added for protection groups. This detection policy uses session tables to analyze TCP connection-specific attack traffic originating from trusted source IP addresses. It detects TCP connections with obvious attack signatures and identifies potential attack sources for blocking. The botnet & IP connection anomaly detection feature consists of the following:

- Abnormal SYN connection detection: Only a specified number of SYN packets are allowed in a single TCP connection. If the number of SYN packets in a single TCP connection exceeds the specified **Packet Count** value, the connection is considered abnormal. A source IP address is considered abnormal if the number of detected abnormal connections exceeds the configured **Abnormal Connections** value within a **Statistical Period of Abnormal Connections**. If a source IP address is detected abnormal for multiple consecutive cycles (exceeding the configured **Consecutive Abnormal Cycles** value, it will be blocked.
- Abnormal ACK connection detection: A TCP packet carrying data (including ACK, ACK/PUSH, and FIN) is considered excessively long if its length exceeds the configured **Packet Length** value. If the number of excessively long packets in a single TCP connection exceeds the configured **Packet Count** value and the proportion of excessively long packets exceeds the configured **Packet Proportion** value, the connection is considered abnormal. A source IP address is considered abnormal if the number of detected abnormal connections exceeds the configured **Abnormal Connections** value within a **Statistical Period of Abnormal Connections**. If a source IP address is detected abnormal for multiple consecutive cycles (exceeding the configured **Consecutive Abnormal Cycles** value, it will be blocked.
- Empty connection detection: A TCP connection is considered abnormal if the total number of sent messages is less than the configured **Packet Count** value within a **Statistical Period of Abnormal Connections**. A source IP address is considered abnormal if the number of detected abnormal connections exceeds the configured

Abnormal Connections value within a **Statistical Period of Abnormal Connections**. If a source IP address is detected abnormal for multiple consecutive cycles (exceeding the configured **Consecutive Abnormal Cycles** value, it will be blocked.

Configuration

Policy > Anti-DDoS > Protection Groups



Post-Upgrade Notes

The previous empty connection function in the botnet & IP behavior control policy is replaced by the empty connection detection function in the botnet & IP connection anomaly detection policy. The old empty connection function has been deleted. The enabling status of the new empty connection detection function will remain unchanged after the upgrade.

6.4 QUIC Protection Policy

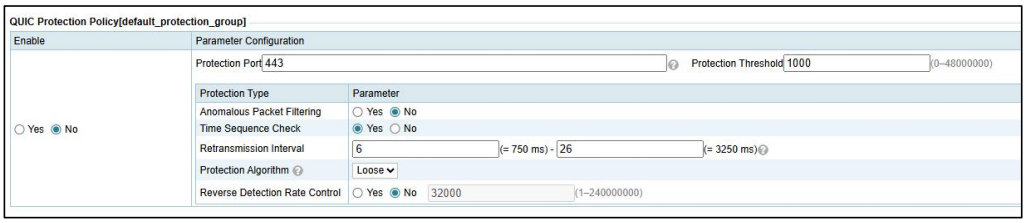
Function Description

The QUIC protection policy is added for protection groups to defend against attacks targeting the QUIC protocol. QUIC protection uses separate protection states and thresholds. It consists of the following:

- Abnormal packet filtering: After this is enabled, packets are inspected based on predefined rules. Packets that do not meet the conditions or cannot be parsed properly will be filtered out.
- Time sequence check: After this is enabled, the initial packet undergoes the first packet dropout and retransmission time sequence check. Packets that fail to meet the time sequence check rules will be discarded.
- Protection algorithm: After this is enabled, a reverse detection packet is sent to verify the initial packet. The source IP that passes the verification is added to the trusted IP list. If **Strict** is selected, all non-initial packets will be discarded before the source IP is added to the trusted IP list. If **Loose** is selected, such packets will be allowed through.

Configuration

Policy > Anti-DDoS > Protection Groups > QUIC Protection Policy



Post-Upgrade Notes

None.

6.5 Auto-Learning Protection Thresholds in the Carpet Bombing Protection Policy

Function Description

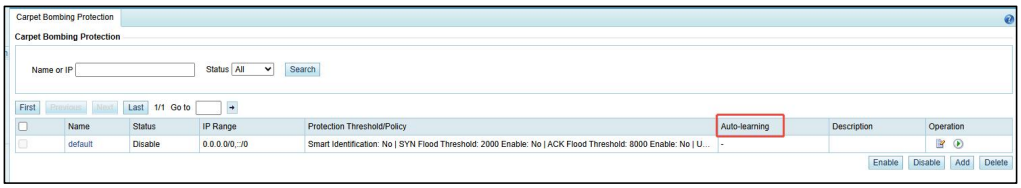
Non-default carpet bombing attack protection rules support the auto-learning function. After auto-learning is enabled, it automatically learns **Threshold 1** of the DDoS policy-based carpet bombing attack protection rules, that is, the network segment-specific mitigation threshold. If the issuing mode of the learned result is set to **Automatic**, the learned **Threshold 1** result will be automatically increased according to the configured **Percentage of Increase** value and will then be issued to the carpet bombing attack protection rules once the learning is complete. If the issuing mode is set to **Manual**, the learned result can be manually adjusted before being applied to the rules.

This function has the following advantages:

- Automatically learning network-segment traffic based on rules helps guide configuration more accurately and reduces the risk of false positives or false negatives.

Configuration

Policy > Anti-DDoS > Carpet Bombing Protection > Auto-learning



Post-Upgrade Notes

- The default rule does not support auto-learning.
- Before performing auto-learning of HTTP **Threshold 1**, specify the HTTP protection port. It is preferably the HTTP protection port configured for the protection group, corresponding to the IP range defined in the carpet bombing protection rules.

6.6 DNS Protection and Specifying Target Types in the Carpet Bombing Protection Policy

Function Description

In the carpet bombing protection rules, the **Threshold 1** value of DDoS policy-based UDP flood detection includes the number of detected DNS packets. When the number of network segment-specific UDP packets exceed the specified **Threshold 1** value, the DNS protection policy will be triggered to prevent DNS packet attacks.

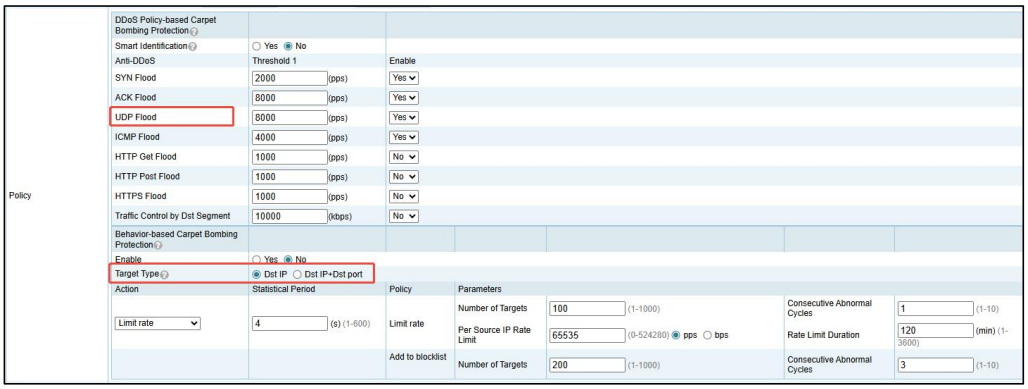
In the carpet bombing protection rules, you can specify the target in the behavior-based carpet bombing protection policy by target type (including **Dst IP** and **Dst IP + Dst port**). If **Dst IP** is selected, statistics will be collected based on the destination IP. If **Dst IP + Dst port** is selected, statistics will be collected based on both the destination IP address and destination port.

This function has the following advantages:

- Defends against DNS packet carpet bombing attacks.
- Supports behavior recognition in port-based scanning.

Configuration

Policy > Anti-DDoS > Carpet Bombing Protection > Auto-learning



Post-Upgrade Notes

For the behavior-based carpet bombing protection policy, the maximum number of targets is 1000. If the number of destination IPs before upgrade is greater than 1000, it will be adjusted to 1000 after the upgrade.

6.7 GeoIP Rule Optimization

Function Description

The enhanced GeoIP rule policy supports the configuration of protocols, ports, and multiple source geolocations and allows users to reorder rules. This significantly improves the flexibility and precision of GeoIP access control policies, enabling more precise traffic protection based on geolocation.

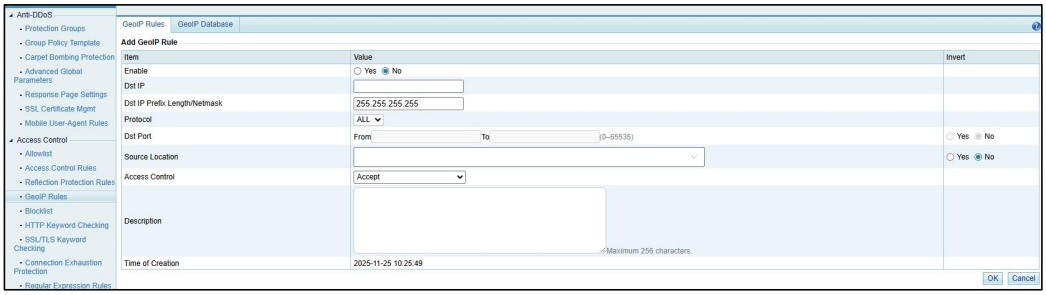
This function has the following advantages:

- **Matching by multi-geolocation**: A GeoIP rule can now include up to 16 countries or regions as matching conditions, greatly simplifying the configuration of multi-region protection.
- **Matching by protocol and port**: In addition to the previous GeoIP matching conditions, support for matching TCP/UDP protocols and destination ports (or port ranges), and the invert operation are added. This allows differentiated geolocation access policies for different services running on the same IP address, such as web services and API services.
- **GeoIP rule reordering** (moving up, down, to the top, or to the bottom): The system strictly follows the user-defined order to implement complex policy control logic.

Configuration

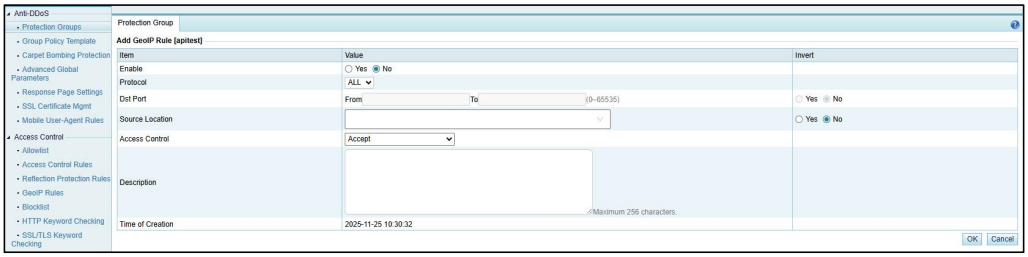
- Configure a global GeoIP rule:

  Policy > Access Control > GeoIP Rules



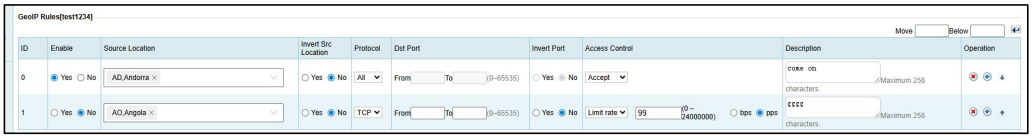
- Configure a GeoIP rule for protection groups:

  Policy > Anti-DDoS > Protection Groups > GeoIP Rules



- Add a policy template for protection groups:

  Policy > Anti-DDoS > Protection Group Template > GeoIP Rules



Post-Upgrade Notes

After reordering rules, you need to manually apply the changes to validate them.

6.8 Hybrid IPv4/IPv6 Proxy Scenario

Function Description

This function has the following advantages:

- Supports different IP protocol types for network layer and proxy addresses. For example, network layer addresses can be IPv4 while proxy addresses are IPv6, or vice versa.
- Supports various scenarios requiring proxy protection, such as blocklists, allowlists, HTTP proxy protection, HTTP keywords, and URL-ACL rules.

Configuration

Policy > Anti-DDoS > Protection Groups

Policy > Access Control > Allowlist

Policy > Access Control > Blocklist

Policy > Access Control > HTTP Keyword Checking

Policy > Access Control >URL-ACL Rules

Post-Upgrade Notes

None.

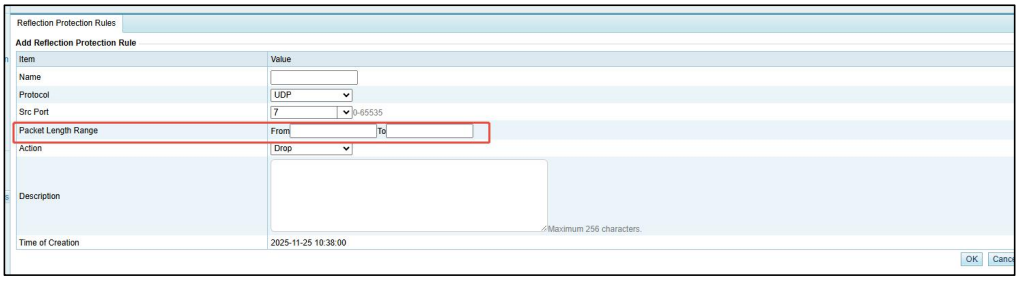
6.9 Specifying a Packet Length Range in the Reflection Protection Rule

Function Description

A packet length range is added to the reflection protection rule configuration. Configuring the packet length range helps prevent normal packets from being misclassified as reflection attacks, providing more precise protection. If the packet length range is not configured, it indicates that there is no limit on the packet length.

Configuration

Policy > Access Control > Reflection Protection Rules



Post-Upgrade Notes

None.

6.10 BGP FlowSpec

Function Description

BGP Flow Specification (BGP FlowSpec) is a functional extension of traditional BGP. Unlike traditional BGP that can only transmit IP prefix routes, BGP FlowSpec supports more refined traffic rules. It distributes these rules and actions to network devices through the BGP protocol, enabling all receiving devices to automatically execute the preset policies. It consists of two core parts:

- Traffic signatures: It defines target traffic in multiple dimensions, including source IP address, destination IP address, transport layer port (TCP/UDP), protocol type (TCP/UDP/ICMP), and DSCP value.
- Handling action: It performs predefined actions on traffic that matches the specified signatures. Common supported actions are **accept**, **discard**, **redirect**, **redirect_IP**, **traffic_marking**, and **rate_limit**.

This function has the following advantages:

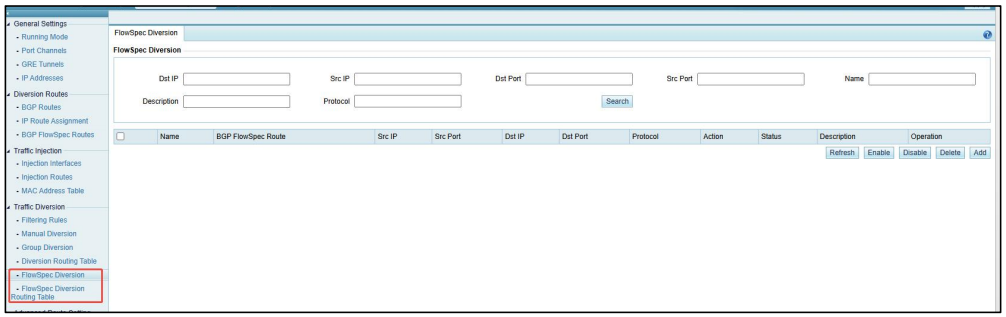
- High precision: Breaking through the limitations of traditional BGP control based solely on IP prefix, it can identify traffic based on multiple dimensions, such as ports, protocols, and IP addresses. This allows it to precisely locate application-specific traffic or anomalous traffic.
- Pre-protection: Protection policies can be deployed based on the signatures of common attack traffic to prevent such attacks from impacting user networks.
- Reducing costs: There is no need to establish separate traffic control policies on each device, which improves maintainability.
- Strong scalability: It seamlessly integrates with the existing BGP network architecture, without the need for additional dedicated protocols or devices. By leveraging existing BGP neighborships, it can distribute policies across the network, reducing network upgrade costs.

Configuration

Diversion & Injection > Diversion Routes > BGP FlowSpec Routes

Diversion & Injection > Traffic Diversion > FlowSpec Diversion

Diversion & Injection > Traffic Diversion > FlowSpec Diversion Routing Table



Post-Upgrade Notes

None.

6.11 Port Synchronization in IN/OUT Interface Pair Configuration

Function Description

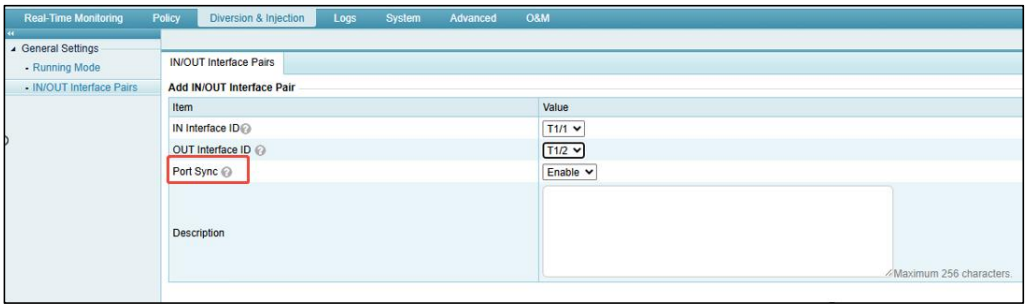
The port synchronization function is available in in-path mode. It can be enabled or disabled individually for different IN/OUT interface pairs.

This function has the following advantages:

- Port synchronization polices can be defined on a per-channel basis.

Configuration

Diversion & Injection > General Settings > IN/OUT Interface Pairs



Post-Upgrade Notes

None.

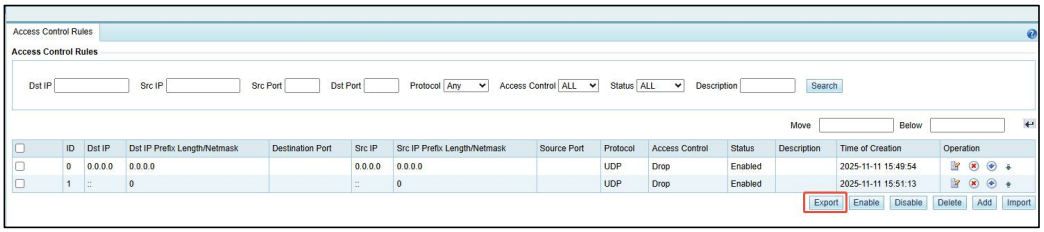
6.12 Exporting Access Control Rules

Function Description

On the **Access Control Rules** page, the **Export** button is added. You can click it to export all access control rules to a file and automatically download it. The file can be saved as a backup or re-imported into the system, with the first line of the exported file serving as the header.

Configuration

Policy > Access Control > Access Control Rules



Post-Upgrade Notes

None.

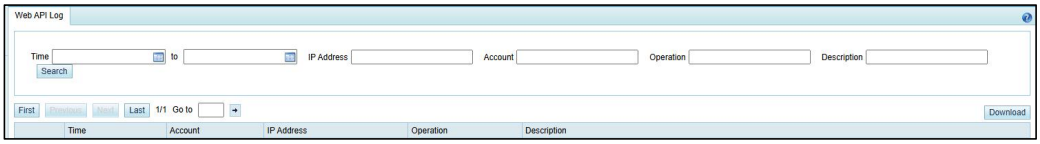
6.13 Web API Log Query

Function Description

On the **Web API Log** page, additional filtering conditions are added, allowing users to query logs more precisely.

Configuration

Logs > System Log > Web API Log



Post-Upgrade Notes

None.

6.14 Importing and Exporting Selected Configuration Files

Function Description

Configuration files can be imported or exported by service category. Users can import or export configuration files by service category or all configuration files, ensuring accurate recovery.

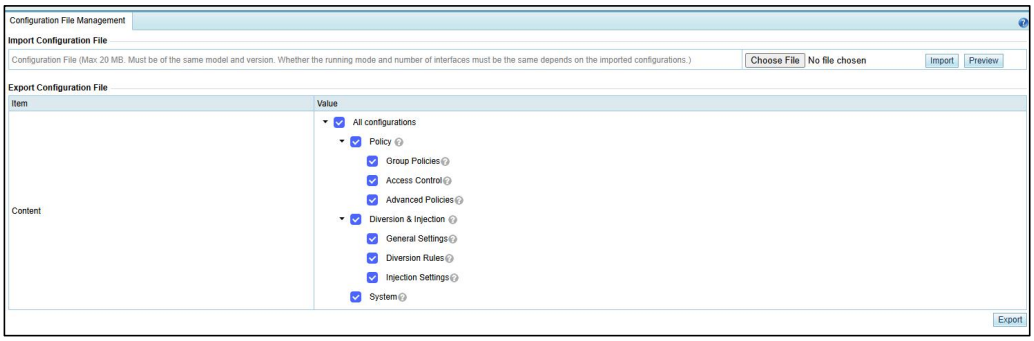
This function has the following advantages:

- **Export by category**: allows exporting configuration files by category, such as protection policies, diversion and injection configuration, and system management configuration.
- **Import by category**: enables the restoration of specific service configurations, ensuring that the system configuration after import remains consistent with the backup.

- **Preview**: allows users to view the contents of the exported file without importing it.

Configuration

System > Configuration File Management



Post-Upgrade Notes

- Ensure that the running mode of the target device matches the one specified in the configuration files before performing the import. If they mismatch, the import will fail.
- If the system prompts that the number of ports exceeds the limit, check that the number of current device ports is no less than the number of device ports listed in the exported configuration files.

6.15 Adding the Source Detection Algorithm in DNS Response Protection

Function Description

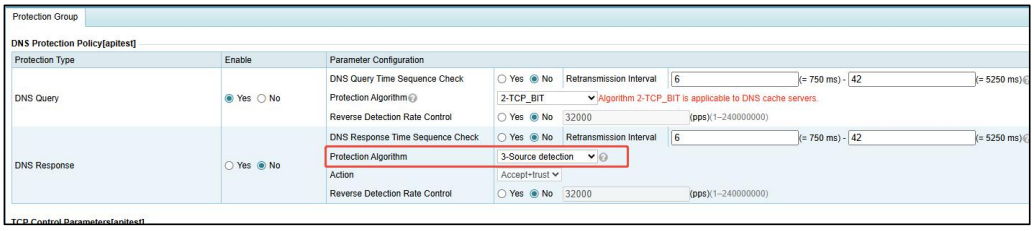
The source detection algorithm is added as a new option in the DNS response protection configuration for protection groups. This algorithm sends a DNS request to the source IP address of the received DNS response to verify the source. If a valid response is received, the source IP address is considered authenticated and added to the trusted IP list.

This function has the following advantages:

- Expands the DNS response protection algorithm options, allowing devices to handle more complex scenarios.
- Identifies bogus sources more effectively.

Configuration

Policy > Anti-DDoS > Protection Groups > DNS Protection Policy



Post-Upgrade Notes

None.

6.16 Adding the Source Detection Algorithm in SYN-ACK Protection

Function Description

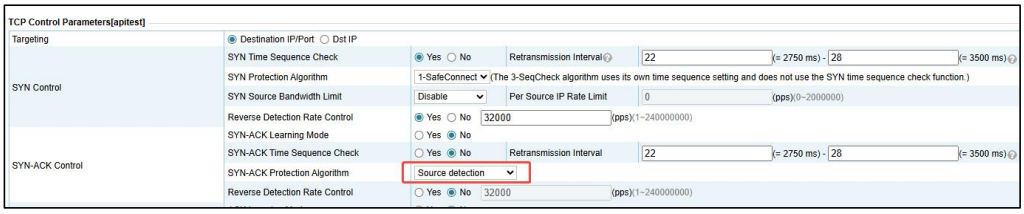
The source detection algorithm is added as a new SYN-ACK protection algorithm option in the TCP control parameter configuration. This algorithm sends a SYN message to the source IP address of the received SYN-ACK message to verify the source. If a valid response is received, the source IP address is considered authenticated and added to the trusted IP list.

This function has the following advantages:

- Expands the SYN-ACK protection algorithm options, allowing devices to handle more complex scenarios.
- Identifies bogus sources more effectively.

Configuration

Policy > Anti-DDoS > Protection Groups > TCP Control Parameters > SYN-ACK Control



Post-Upgrade Notes

None.

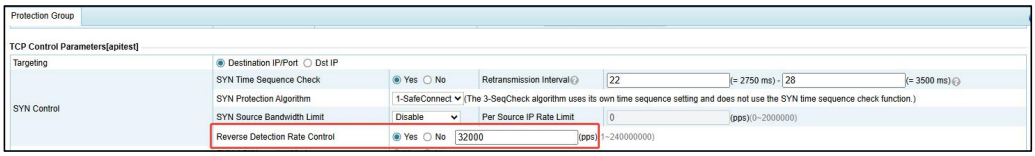
6.17 Threshold Change of the DDoS Policy for Protection Groups

Function Description

The **Threshold 1** parameter in the DDoS policy for protection groups is changed to **Mitigation Threshold** and the **Threshold 2** parameter is changed to **Flow Control** to better convey the intended meaning. In addition, the **Threshold 2** parameter for **SYN Flood** is replaced by **Reverse Detection Rate Control** for **SYN Control** in the TCP control parameters. The reverse detection rate control switch is added.

Configuration

Policy > Anti-DDoS > Protection Groups > TCP Control Parameters



Post-Upgrade Notes

If the actual **Threshold 2** value of SYN flood before the upgrade exceeds 12500000, the reverse detection rate control will be disabled after the upgrade. Otherwise, it will be enabled.

6.18 Adjusting the Matched Threat Intelligence IP Address Range via the CLI

Function Description

The **ip-reputation threat-level** command is added to obtain and define which threat level of IP addresses in the threat intelligence packet can be matched by the protection engine. When the threat level is set to **high**, only high-level IP addresses within the IP address range can be matched. When the threat level is set to **medium**, only high-level and medium-level IP addresses can be matched, with high-level IP addresses taking priority. When the threat level is set to **low**, IP addresses of all levels can be matched.

Note that the threat level setting for matching threat intelligence will take effect only after the next threat intelligence update.

Configuration

Via the CLI.

```
ADS#ip-reputation threat-level ?
  modify                        Set ip-reputation threat level
  get                           Get ip-reputation threat level
ADS#
```

Post-Upgrade Notes

None.

6.19 Viewing BGP/LDP Configuration and Neighbor Status via the CLI

Function Description

The **ldp config list** and **ldp status list** commands are added to obtain lDP configuration and neighbor status information. BGP related commands are added to obtain BGP configuration and neighbor status information.

Configuration

Via the CLI.

```
ADS#ldp ?
  config                        ldp configurations
  status                        ldp status
ADS#
ADS#bgp ?
  config                        bgp configurations
  neighbor                      bgp neighbor configurations
ADS#
```

Post-Upgrade Notes

None.

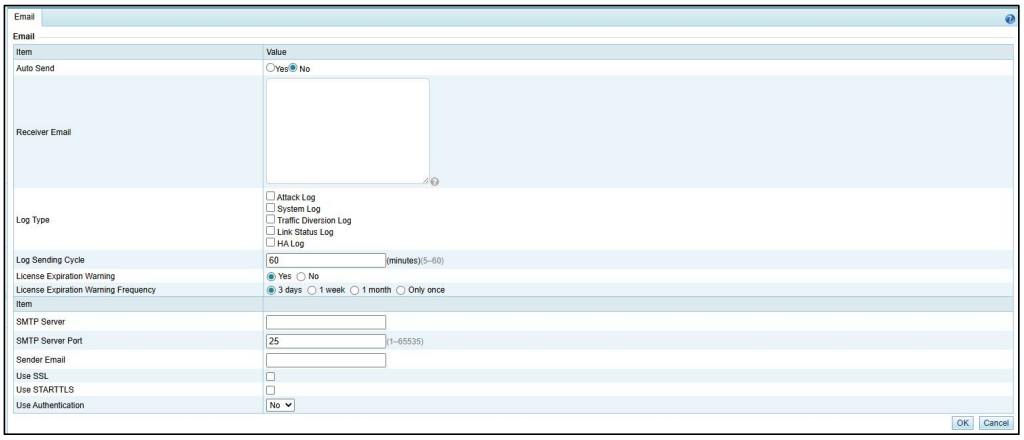
6.20 Email Encapsulation

Function Description

SSL and STARTTLS encryption options are added for email transmission, enhancing security and flexibility.

Configuration

System > Log Services > Email



Post-Upgrade Notes

- SSL and STARTTLS are disabled by default. You need to manually select them based on security requirements.
- Before enabling SSL or STARTTLS, check that the email server supports the chosen encryption method. Some servers may not support STARTTLS.

6.21 Deleting the Save button

Function Description

The **Save** button is deleted in the web-based manager. Currently, the configuration is automatically saved immediately after modification, preventing configuration loss caused by forgetting to click the **Save** button before restarting the device.

Note that the previous **Save** button includes the functionality of the **Apply** button. Clicking the **Save** button not only saves the configuration but also applies it. Although the **Save** button has been deleted in this version, some functional configurations still require clicking **Apply** to take effect. If a configuration does not take effect immediately, click **Apply** to issue it.

Configuration

The **Save** button is deleted in the upper-right corner of the web page.

Post-Upgrade Notes

None.

6.22 Other Functions

1. Specifying multiple ports in the group-specific HTTPS protection policy

   You can specify multiple ports in the HTTPS protection policy for protection groups.

2. Expanding HTTP method types in the HTTP keyword checking policy

   In the access control policy, the HTTP keyword checking rule macro expands the **Method** options available for a rule. In addition to GET and POST, it supports the PUT, DELETE, HEAD, OPTIONS, PATCH, TRACE, and CONNECT methods.

3. Increasing the destination IP traffic control threshold for protection groups

   The maximum threshold for destination IP traffic control of protection groups is 167 Gbps.

4. Optimizing the system restart prompt

   After completing the operation that requires a system restart, a prompt to restart the system is displayed in the upper-right corner of the web page.

5. Requiring no system restart after upgrade using some upgrade packages (V4.5R90F07 and later)

   If the upgrade package that is version R90F07 or later supports upgrading without a system restart, upgrading from version R90F07 will not require restarting the device.

6. Adding the reverse detection rate control switch in DNS query protection

   The reverse detection rate control switch is added in DNS query protection for protection groups. Use it to enable or disable reverse detection rate control.

7. Configuring the netmask of the IP address for the management platform

   You can configure the IP address as either IP address or IP/netmask under **System > Management Platform**.

8. SSL certificate import

   The file name of the SSL certificate to be imported can contain up to one period (.).

7. Version Application

7.1 Upgrade

7.1.1 Version Upgrade

Applicable Device Models

ADS NX3-HD1000, ADS NX5-HD5000, ADS NX5-HD6000, ADS NX3-HD2500, ADS NX5-HD4500, ADS NX5-HD6500, ADS NX5-HD8500, ADS NX5-8000, ADS NX5-10000, ADS NX5-12000, ADS NX5-20000, ADS NX5-HFA2000, ADS NX5-HFB3000, ADS NX5-HFB6000, ADS NX5-HFB8000, ADS NX5-HFC6000, ADS NX5-HFC8000, ADS-NX5-HFG10000, and ADS NX1-VN01

Constraints

- For the HFB6000, HFB0000, and HFC6000/HFC8000 models, the upgrade must be performed from V4.5R90F06 or later, using the **update_ADS_hygon_V4.5R90F07_20251128.zip** upgrade package.
- For the HFA2000 and HFB3000 models, the upgrade must be performed from V4.5R90F06SP03, using the **update_ADS_arm_V4.5R90F07_20251128.zip** upgrade package.
- Other models must be upgraded from V4.5R90F06 or later, using the **update_ADS_x86_V4.5R90F07_20251128.zip** upgrade package.

If the device's current version is lower than the upgrade base version for the corresponding model, first upgrade it to the base version according to the upgrade route, and then perform the upgrade using the corresponding upgrade package. Otherwise, the upgrade will fail.

Impact

The network connection will be interrupted in the upgrade process. Before upgrading a custom version, check whether customized functions will be affected by the upgrade.

Procedure

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

Step 2 On ADS, choose **System > Others > System Upgrade**, upload the corresponding package, and perform the upgrade.

Step 3 After the system prompts upgrade success, restart the device.

Step 4 After the device is restarted, verify the upgrade result. For details, see Upgrade Success Verification.

----End

Note: If the upgrade failed, contact NSFOCUS technical support.

Upgrade Success Verification

Log in to the web-based manager and choose **System > Others > System Upgrade**. In the **Upgrade History** list, verify that the target version is V4.5R90F07. Then go to **System > Others > System Info**, verify that the software version is V4.5R90F07.

What to Do in the Case of Upgrade Failure

If the upgrade failed, try using **Rollback system** in the console user interface or logging in to the CLI to perform a rollback operation.

7.1.2 Version Rollback

Applicable Device Models

ADS NX3-HD1000, ADS NX5-HD5000, ADS NX5-HD6000, ADS NX3-HD2500, ADS NX5-HD4500, ADS NX5-HD6500, ADS NX5-HD8500, ADS NX5-8000, ADS NX5-10000, ADS NX5-12000, ADS NX5-20000, ADS NX5-HFA2000, ADS NX5-HFB3000, ADS NX5-HFB6000, ADS NX5-HFB8000, ADS NX5-HFC6000, ADS NX5-HFC8000, ADS NX5-HFG10000, and ADS NX1-VN01

Procedure

To roll back the device from version V4.5R90F07 to the previous version, follow these steps:

Log in to the console user interface and select **Rollback system**, or log in to the CLI and run the **update rollback** command.

Rollback Success Verification

Log in to the web-based manager and choose **System > Others > System Upgrade**. In the **Upgrade History** list, verify that the target version is the one before the upgrade. Then go to **System > Others > System Info**, verify that the software version is also the one before the upgrade.

Impact

The network connection will be interrupted in the rollback process.

What to Do in the Case of Rollback Failure

If the rollback failed, contact NSFOCUS technical support.

7.2 Constraints

For devices with a 2G CF card, upgrading to this version is not supported. If the system prompts a pre-upgrade processing failure during the upgrade, check whether the device's CF card capacity is 2G. If so, contact after-sales personnel for a replacement before performing the upgrade.