

Release Notes

Basic Information

Product Model	<ul style="list-style-type: none">• 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
Software Version	V4. 5R89F03
Upgrade File	update_ADS_x86_V4. 5R89F03_20170714. zip MD5: b37b0c74b42e7eb5df7480de38293aec
Release Date	2017-07-17
How to Obtain	Contact technical support personnel of NSFOCUS.

Version Mapping

Software Version	V4.5R89F03
Product Model	<ul style="list-style-type: none"> • NSF1100-1 • NSF1100-3 • NSF2800-2 • NSF2800-6 • NSF3600-4
NTA Version	<ul style="list-style-type: none"> • V4.5.61.2 • V4.5R89F03
Management Platform Version	ADS M V4.5R89F03
Client	None
Other System or Tool	None
Documentation	NSFOCUS ADS User Guide (V4.5R89F03)

Function Changes

1 Change Description

The following product models are supported:

- 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

1.1 Lists of Function Changes in V4.5R89F03

Functions Changed and Added in V4.5R89F03

Function	V4.5R83F02/IB02	V4.5R89F03	Description
Internationalizati	Partly	Changed	UI and online help of ADS are available in

Function	V4.5R83F02/IB02	V4.5R89F03	Description
on	internationalized		English and Japanese. ADS documentation is available in English.
Version upgrade	Version upgrade	Changed	After an upgrade package is uploaded, key version information and a message asking whether to continue the upgrade operation are displayed for confirmation.
SYN + ACK flood protection algorithms	SYN + ACK flood protection algorithms	Changed	SYN + ACK flood protection algorithms are optimized.
Wizard	N/A	Added	For the first login after the upgrade to V4.5R89F03, a configuration wizard pops out for users to configure the locality and time zone.
NSFOCUS Threat Intelligence (NTI)	Reputation cloud	Changed	NTI servers for the Chinese mainland and other countries or regions are added for users to choose from.
NSFOCUS Cloud	NSFOCUS Cloud	Changed	Access to NSFOCUS Cloud can be enabled according to the locality.
Port Channel Configuration in the CLI	N/A	Added	MAC addresses can be configured for port channels in the CLI.
Network diagnosis	N/A	Added	Network diagnosis and port check functions are added.
Collaborative diversion	Collaborative diversion	Changed	The configuration of the ADS-NTA collaboration duration is optimized.
System resources	System resources	Changed	Colors indicating changes in CPU and memory usage are changed.

Function Changes in V4.5R89F03 Compared with V4.5R89F02

Function	V4.5R89F02	V4.5R89F03
Manual diversion	The IPv6 prefix length range is 120–128.	The IPv6 prefix length range is 0–128.
Protection group	The IPv6 prefix length range is 112–128.	The IPv6 prefix length range is 1–128.
Injection route	The IPv6 prefix length should be 0 or in the range of 48–128.	The IPv6 prefix length range is 0–128.
Remote assistance	By default, this function is enabled.	By default, this function is disabled. After upgrade, the pre-upgrade configuration will remain effective.
Authentication synchronization	N/A	HTTP authentication synchronization is supported.

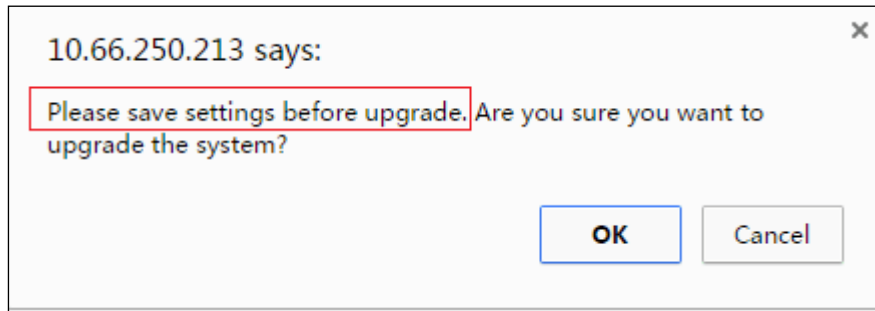
Function Changes in V4.5R89F03 Compared with V4.5R89IB2

Function	Description
DNS retransmission algorithm	The DNS retransmission algorithm is added to the DNS protection policy as a new DNS protection algorithm.
Supported device models	<p>Models supported by V4.5R89IB02:</p> <ul style="list-style-type: none"> • ADS NX3-2010 • ADS NX3-2020 • ADS NX5-4020 • ADS NX5-6025 • ADS NX5-8000 <p>Models supported by V4.5R89F03:</p> <ul style="list-style-type: none"> • 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
Configuration file	In the new version, configuration files can be sent to the user's specified FTP server as scheduled.
Optimization of the SNMP agent	The SNMP agent supports standard information specified in RFC 1213.
Access control	The access control function is optimized.
Link connectivity check	A new function is added to check whether link connectivity is real as it appears.
Resource monitoring	In the new version, the system can monitor the temperature of the mainboard, CPU, and fans, and it can also send alerts on exceptions via syslog.

1.2 Description of New and Changed Functions in V4.5R89F03

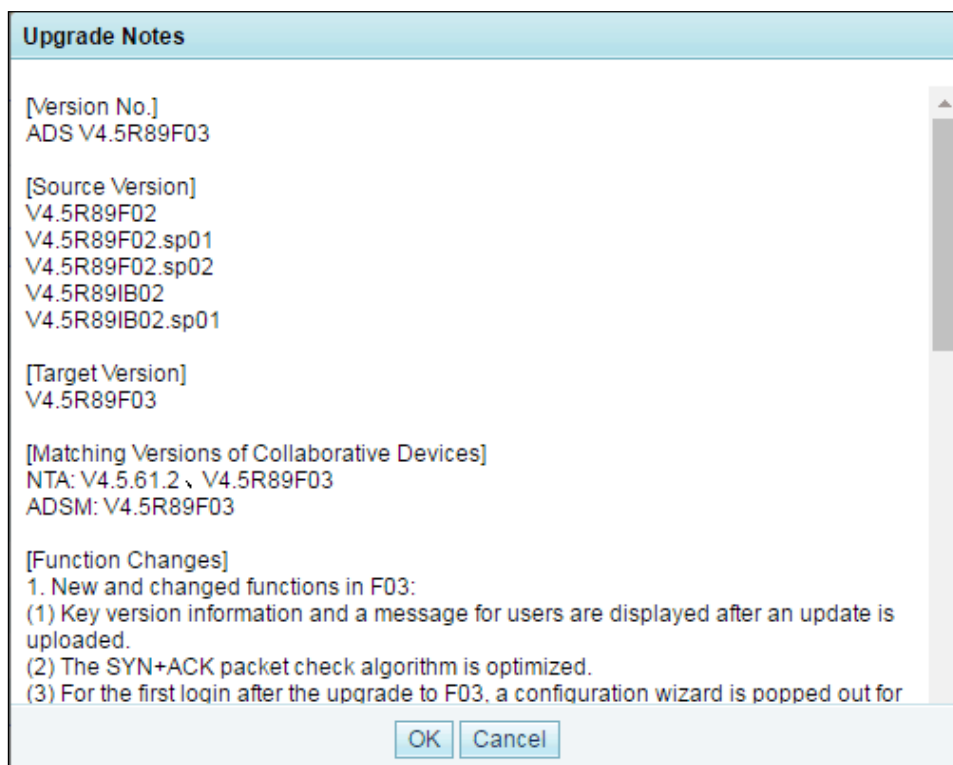
Key Version Information and Message for Users Displayed After Upload of an Update

After an update is uploaded, the following message is displayed to remind the user to save settings.

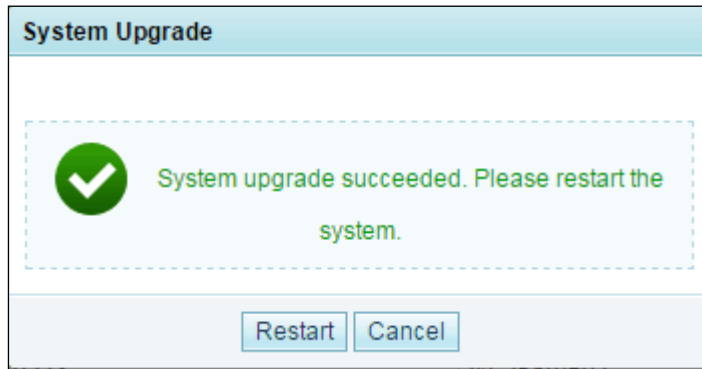


Then the following version-related information is displayed:

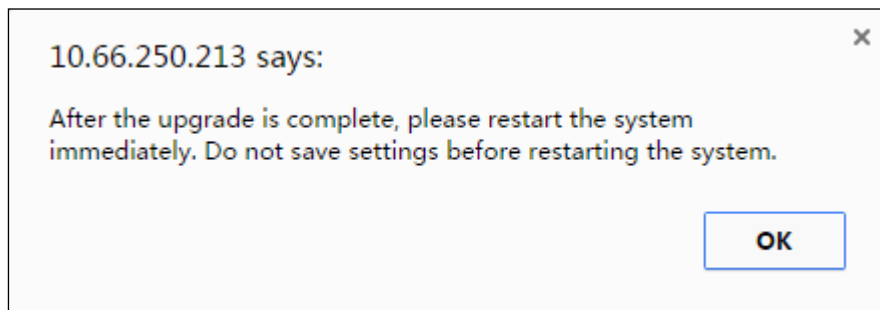
- Version number
- Versions that can be directly upgraded to V4.5R89F03
- Version to be upgraded to
- Compatible versions of collaborative devices
- Function description
- Important notes



After the user clicks **OK** and the installation is complete, the system displays a message, asking the user to restart the system.



In this case, the user is supposed to choose to restart the system. If the user, however, chooses not to restart the system immediately, the following message will be displayed.



Note

This function involves changes to the upgrade script and logic. This means that such changes can be seen only when V4.5R89F03 is upgraded to the next version. Therefore, though this function is added to V4.5R89F03, key version information and message for users do not appear in the process of installing the V4.5R89F03 upgrade package.

UI and Online Help Available in English and Japanese

No Japanese edition is made for the new functions in V4.5R89F02. The new version (V4.5R89F03) incorporates these functions and delivers some other new functions, which are available in both English and Japanese. The web-based manager supports Chinese, English, and Japanese, and the related user guide has been translated to English from Chinese.

Locality and Time Zone Configurable for the First Login After Upgrade

V4.5R89F03 requires configurations (such as the user locality and time zone) to be initialized for the first use in different regions. In this case, the system displays a wizard to walk users through the configuration process. Users need to set the UI language, locality (North America, LATAM, Asia Pacific, EMEA, or Chinese mainland), time zone, and system time according to the actual situation.

Feature Description

Conditions for Displaying Configuration Wizard	Users log in to a device for the first time after the device is upgraded to this version. A device of this version is produced. The user logs in as admin .
Configuration Sequence	For a newly upgraded device, set the locality, time zone, and system time successively. For a newly produced device, first set the preceding items and then change the initial password.
Other Functions Affected by Configuration Wizard	NTI: Users on the Chinese mainland use the server based in China and those in other countries/regions use the server in the USA. NSFOCUS Cloud: Users on the Chinese mainland use the server based in China and the function remains unchanged. It is unavailable for users in other regions. The service is disabled by default and this cannot be changed.

Configuration Procedure

Under **System > Local Settings > Basic Settings**, a **Region** area is added for users to select the actual locality.

For a newly produced ADS device or a device upgraded to V4.5R89F03, please first log in as **admin**. The configuration wizard appears only when users log in as **admin**. After the configuration is complete, the wizard will not appear during subsequent logins. However, if users do not click **OK** after configuration, the wizard will appear again when users log in as **admin**.

For login through other accounts, the system does not display the wizard. If **admin** does not log in after upgrade, the locality has the default value and other pre-upgrade settings remain effective.

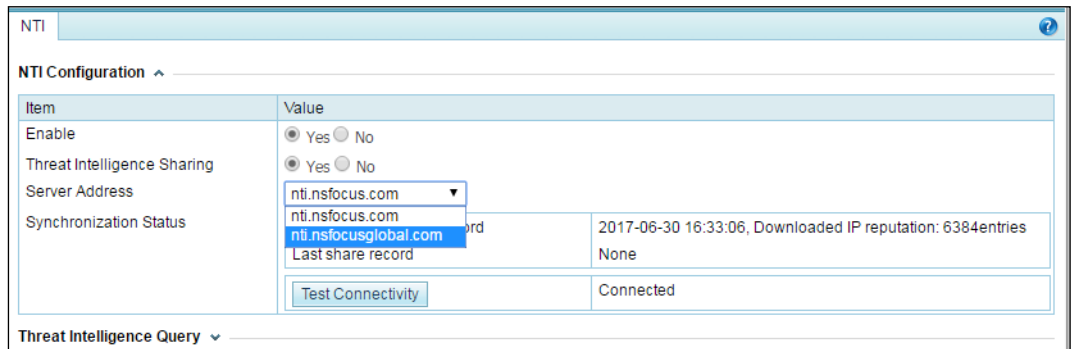
IP Reputation Module Renamed and Server Switch

V4.5R89F03 renames the IP Reputation module and modifies related parameters.

Previous Versions	V4.5R89F03
IP Reputation	NTI
Cloud IP Reputation	NTI
IP Reputation Configuration	NTI Configuration
Function Control (Open/Close)	Enable (Yes/No)
Last report record	Last share record

For use of ADS V4.5R89F03 in or outside of China, users need to connect to the appropriate server.

Function Control	Enabled by default.
Server Address	For use on the Chinese mainland: The default URL of the server is nti.nsfocus.com. For use in other countries/regions: The default URL of the server is nti.nsfocusglobal.com.



Adaptive Switch for Controlling Access to NSFOCUS Cloud

For use on the Chinese mainland:

- The web-based manager provides a switch to enable or disable access to NSFOCUS Cloud.
- Access to NSFOCUS Cloud is enabled by default after the device is produced.
- Access to NSFOCUS Cloud is enabled by default after the device is upgraded to this version.

For use in other countries/regions:

Access to NSFOCUS Cloud is disabled by default and this setting cannot be changed.

End User License Agreement

For details about the End User License Agreement (EULA), visit <https://cloud.nsfocus.com/#/krosa/views/initcdr/eula>.

MAC Addresses Configurable for Port Channel in the CLI

Currently, multiple ADS devices, when configured to work as a cluster, should appear to be a single logical device for users. For this purpose, MAC addresses of all devices in a cluster should be changed to the same. For earlier versions, this has to be done by technical support or R&D personnel who must log in to the background for manual operations. To avoid such trouble and simplify the operation, the new version supports change of MAC addresses in the CLI for implementation of the port channel.

The following CLI commands are added:

- `cluster set-portchannel-mac on/off` //Enables or disables the function of configuring the port channel MAC address.
- `cluster set- portchannel -mac <port-index> <mac-addr>` //Sets the MAC address of an interface.
- `cluster list-mac` //Views the currently valid MAC address of all interfaces in the channel group.

Therefore, now users can change the port channel MAC address through the web-based manager and the CLI:

1. On the web-based manager, select interfaces that will work as part of the channel group and configure a port channel.
2. In the CLI, type **cluster list-mac** to view the currently valid MAC address.
3. Type **cluster set-portchannel-mac on** to enable the MAC address configuration function.
4. Type **cluster set- portchannel -mac <port-index> <mac-addr>** to set the MAC address of an interface. (For example, if interfaces 3, 4, and 5 are part of a channel group, users just need to change the MAC address of interface 3. After the device is restarted, interfaces 4 and 5 will automatically have their MAC address changed to that of interface 3.)
5. Click **Save** on the web-based manager and then restart the system.
6. In the CLI, type **cluster list-mac** to check whether the new MAC address has taken effect.
7. If the cluster needs to be dissolved or modified, users must do as follows:
 - Type **cluster set-portchannel-mac off** to disable the MAC address configuration function.
 - Click **Save** on the web-based manager.
 - Restart the system.

Network Diagnosis and Port Checking

Network diagnosis and port checking are mainly used for troubleshooting during device maintenance. In earlier versions, for this purpose, users need to log in to the CLI or

background, which is troublesome. To improve the ease of use (EOU), the new version provides the two functions on the web-based manager.

Configuration page: **System > Others > Network Diagnosis**

Network Diagnosis	
Item	Value
Diagnosis Mode	Ping
IP	10.66.250.19
OK	
Diagnosis Result	
<pre> PING 10.66.250.19 (10.66.250.19): 56 data bytes 64 bytes from 10.66.250.19: seq=0 ttl=64 time=1.166 ms 64 bytes from 10.66.250.19: seq=1 ttl=64 time=0.453 ms 64 bytes from 10.66.250.19: seq=2 ttl=64 time=0.455 ms 64 bytes from 10.66.250.19: seq=3 ttl=64 time=0.458 ms --- 10.66.250.19 ping statistics --- 4 packets transmitted, 4 packets received, 0% packet loss round-trip min/avg/max = 0.453/0.633/1.166 ms </pre>	

Network Diagnosis	
Item	Value
Diagnosis Mode	Port Check
IP	
Port	
timeout	10 (0-30)(s)
OK	
Diagnosis Result	

Optimized Diversion Function

When ADS of an earlier version collaborates with NTA, the whole diversion process takes about 8 seconds from when NTA detects an attack and instructs ADS to perform the diversion till ADS completes the diversion. This is obviously very long. Therefore, this function is optimized for both NTA and ADS in the new version. The diversion duration is shortened to 2–3 seconds.

The optimization is made in the following aspects:

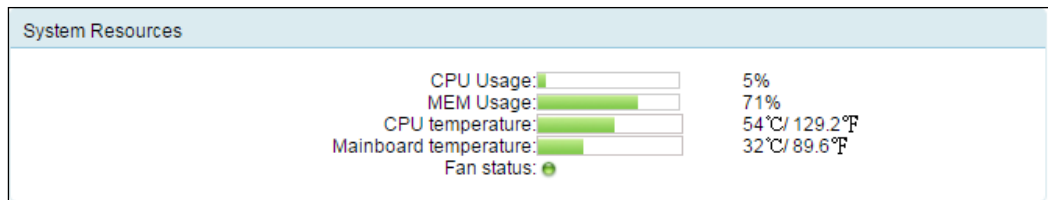
- The time is shortened for NTA or other traffic monitoring devices to issue a diversion notification to ADS.
- The time is shortened from roughly 6 seconds to 2 seconds for the issuance of a diversion notification to ADS from the web-based manager, ADS M, or a third-party API.

Use of Consistent Colors to Indicate CPU and Memory Usage

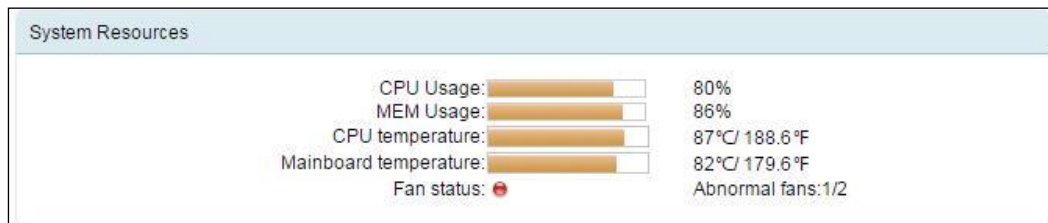
In earlier versions, the CPU usage bar is always green and the memory usage bar is always brown. However, the temperature bar shows green when the temperature is below the specified threshold and turns brown when the temperature is above the threshold. To unify the UI display, the new version adopts a uniform policy to show the usage/temperature of system resources.

CPU Usage	0–70%: green (normal); 71%–100%: brown (abnormal)
MEM Usage	0–80%: green (normal); 81%–100%: brown (abnormal)
CPU Temperature	0–70°C: green (normal); 71°C–100°C: brown (abnormal)
Mainboard Temperature	0–60°C: green (normal); 61°C–100°C: brown (abnormal)

Normal:



Abnormal:



1.3 Description of Major Function Changes in V4.5R89F03 from V4.5R89F02

"Modification of the limit on the IPv6 prefix length for protection group, manual diversion, and injection route configuration" is a new feature in V4.5R89IB02. "HTTP authentication synchronization" is a new feature in V4.5R89IB02SP01. The new version incorporates the two features and makes the following changes.

Feature	Change Description
Modification of the limit on the IPv6 prefix length for protection group, manual diversion, and injection route	V4.5R89IB02/IB02SP01: The manual traffic diversion policy applies to the whole IPv6 subnet specified and cannot work for individual IPv6 addresses in the subnet.

Feature	Change Description
configuration	V4.5R89F03: The preceding rule applies to IPv6 subnets with a prefix length of 0–119, but does not work for IPv6 subnets with a prefix length of 120–128.
HTTP authentication synchronization	V4.5R89IB02SP01: Synchronization states include local switch off, manager-side switch off, not synchronized, keepalive timeout, synchronization timeout, and normal. V4.5R89F03: Synchronized states are reduced to four, namely, synchronization switch off, not synchronized, synchronization timeout, and normal. Web API: For related changes, see the web API document.

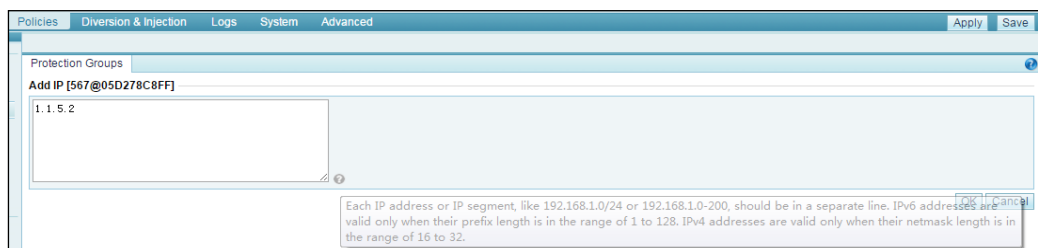
Modification of the Limit on the IPv6 Prefix Length for Protection Group, Manual Diversion, and Injection Route Configuration

Feature Description

Modification of the limit on the IPv6 prefix length for protection group configuration:

- Under **Policies > Protection Groups**, for the addition of IP addresses to a group, users can specify IPv6 addresses with a prefix length of 1–128. The system will verify the validity of the prefix length.
- Under **Policies > Protection Groups**, the tool tip for the **Add IP** text box expressly indicates that the valid range of the IPv6 prefix length is 1–128.
- For group objects, users can specify their own prefix length ranges as long as they fall within the preceding range, without affecting group-related functions.

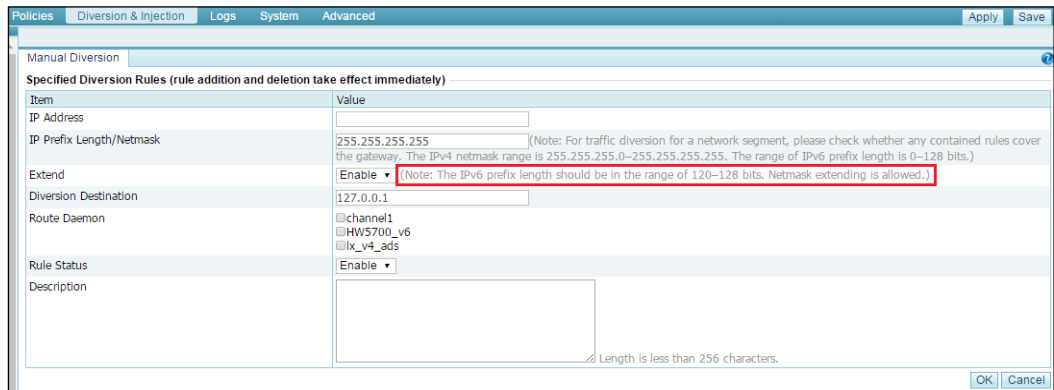
On the web-based manager, if an IPv6 subnet is specified with an IPv6 address and a prefix length like 8000::/1, the system will verify the validity of the prefix length, which must be in the range of 1 to 128. If an IPv6 address range is specified with two IP addresses linked by a hyphen like ::-ffff, the new version interprets it the same way as V4.5R89F02 does: The addresses in the range vary in the last 16 bits. If individual IPv6 addresses are specified, they work and mean the same as those in V4.5R89F02.



Modification of the limit on the IPv6 prefix length for manual diversion configuration:

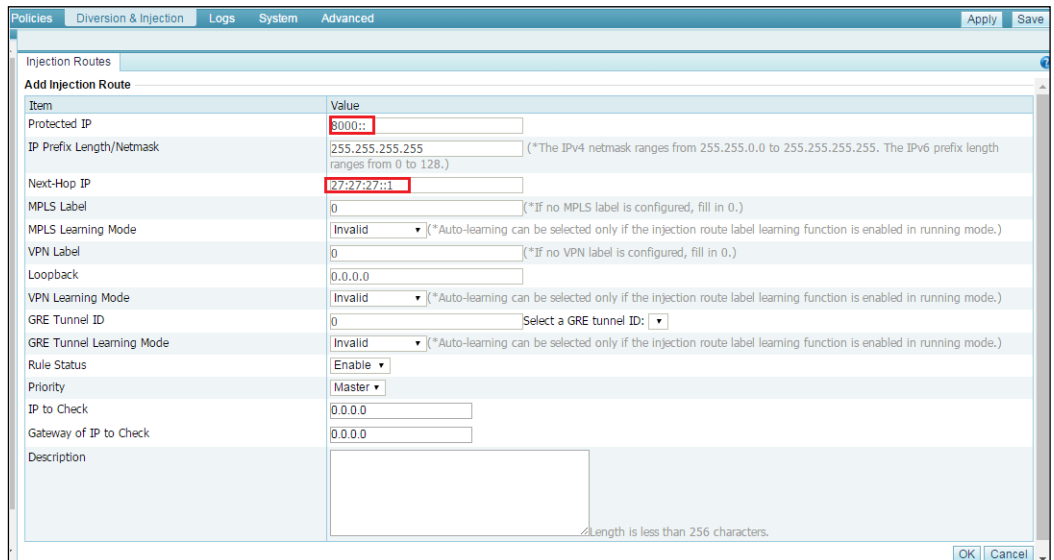
- Under **Diversion & Injection > Traffic Diversion > Manual Diversion**, IPv6 prefix length verification is canceled, allowing users to specify any prefix lengths within the range of 0–128.
- Under **Diversion & Injection > Traffic Diversion > Manual Diversion**, the tool tip for the **IP Prefix Length/Netmask** text box excludes the limit on the IPv6 prefix length.

- Under **Diversion & Injection > Traffic Diversion > Manual Diversion**, the **Extend** field can only have **Disable** as the value for IPv6 subnets with a prefix length of 0–119, indicating that the manual diversion policy applies to the whole IPv6 subnet specified, but does not work for individual IPv6 addresses in the subnet. However, if the specified IPv6 subnet has a prefix length of 120–128, the **Extend** field can be set to either **Disable** or **Enable**.
- For manual diversion, diversion routes involving IPv6 addresses with any prefix lengths in the range of 0–128 can be sent to the peer router.



Modification of the limit on the IPv6 prefix length for injection route configuration:

- Under **Diversion & Injection > Traffic Injection > Injection Routes**, to create an injection route, users can specify an IPv6 address with a prefix length of 0–128. The system will verify the validity of the prefix length.
- Under **Diversion & Injection > Traffic Injection > Injection Routes**, the tool tip for the **IP Prefix Length/Netmask** text box on the **Add Injection Route** page expressly indicates that the valid range of the IPv6 prefix length is 0–128.



Addition of the HTTP Authentication Synchronization Function

When load balancing policies are not configured based on source IP addresses in the front of an ADS cluster, ADS devices in the cluster may need to be repeatedly authenticated or fail to be authenticated. To resolve this problem, the new version has a new function: authentication synchronization.

Configuration Page

System > Local Settings > Management Mode > HTTP Authentication Synchronization

IP Address	Management Platform Type	Language	Enable	Operation
10.66.250.6	ADS M	Simplified Chinese	Yes	
10.66.250.244	ADS M	Simplified Chinese	Yes	
10.66.93.5	ADS M	Simplified Chinese	Yes	
10.66.61.100	Third-Party Management	Simplified Chinese	Yes	
10.66.250.237	ADS M	Simplified Chinese	Yes	

IP Address	Synchronization Status and Cause for Exception	Enable	Operation
10.66.250.6	Exception: synchronization timeout.	Yes	

CLI commands:

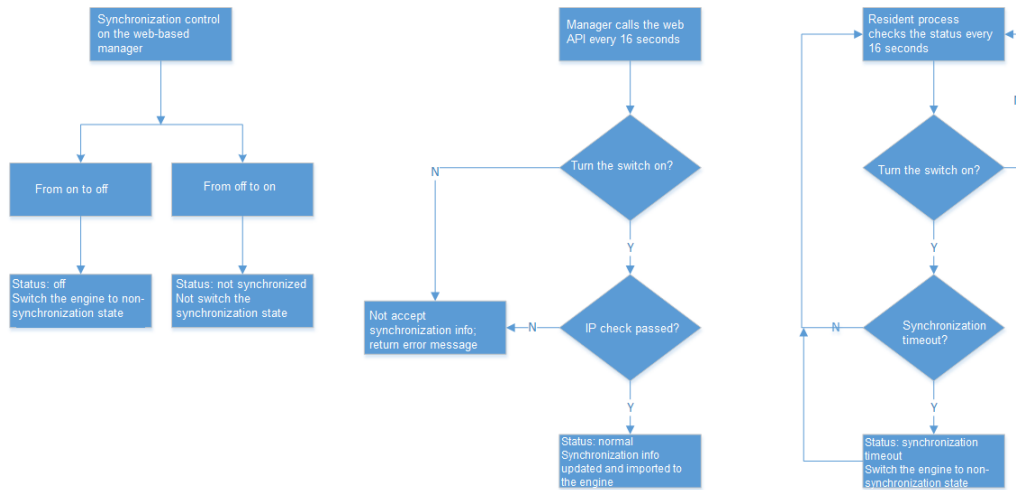
```

ADS#http-auth-sync ?
  set-local-switch    set local switch.
  set-remote-ip      set remote ip.
  show                show all http authentication synchronization configure and status.
  
```

The following table describes different HTTP authentication synchronization states.

State	Description
Normal	The synchronization is normal.
Not synchronized	Authentication information is not synchronized. This is displayed when the synchronization switch is turned on, but synchronization information fails to be received and the synchronization does not time out.
Synchronization disabled	The synchronization function is not enabled.
Synchronization timeout	No synchronization information is received within 48 seconds.

Flowchart



- By default, authentication synchronization is disabled.
- If the ADS cluster has no manager or has a manager that has not performed authentication synchronization, the algorithm for generating authentication code in the new version is the same as that in V4.5R89F02.
- After ADS M is disqualified as the manager of the ADS cluster, ADS devices will perceive the synchronization timeout in 48 seconds (a synchronization cycle is 16 seconds) and then resume the logic to the previous state (without authentication synchronization).

1.4 Description of Major Function Changes in V4.5R89F03 from V4.5R89IB02

All the following functions are the ones added to or modified in V4.5R89F02. They are listed here as a reference for function changes from V4.5R89IB02 to V4.5R89F03. The same information can also be found in the *ADS V4.5R89F02 Release Notes*. Considering that the new version inherits these functions from V4.5R89F02, we describe these functions with V4.5R89F02 in mind.

DNS Retransmission Algorithm

Feature Description

In earlier version, ADS provides three algorithms to filter DNS request packets:

- The default algorithm is, in nature, quite rough because it can only limit the UDP traffic rate.
- The CNAME protection algorithm is used to protect the authoritative DNS server.
- The TCP-BIT algorithm is used to protect the caching DNS server subject to strict restrictive conditions.

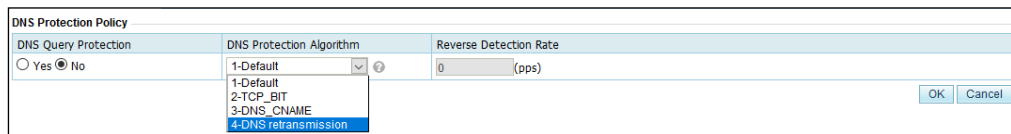
ADS requires that clients be able to initiate DNS queries over TCP. That is to say, only clients that can send TCP-based DNS requests can be authenticated by protection algorithm 2 of

ADS. However, not all clients can send DNS queries using TCP. Even if they can, they need to communicate with the server via port 53. For this reason, the server should open TCP port 53.

These greatly restrict the use of the TCP-BIT algorithm in actual scenarios. For better protection of the caching DNS server, the DNS retransmission algorithm is added to improve user experience in DNS attack protection.

Function Description

4-DNS retransmission is added as a new DNS protection algorithm for the default DNS protection policy and that for protection groups, as shown in the following figure.



For easy understanding, the name of the third DNS algorithm is changed to **3-DNS_CNAME**.

Advantages

- More DNS protection algorithms are available.
- A generic and viable algorithm is provided for protection of caching DNS servers.

Support for Devices of E Models

Currently, ADS 2010, 2020, 4020, 6025, 8000, 200E, and 600E support the mainstream x86 platform. Among such models, ADS 2010, 2020, 4020, 6025, and 8000 can be upgraded to R89F01CN, while ADS 200E and 600E can only be upgraded to several SP versions, but not R89F01CN. To solve this problem, a mainline version applicable to all above models is required, and this is why V4.5R89F02 was released. Now V4.5R89F03 inherits this feature of V4.5R89F02 and is also universally applicable.

In addition, ADS 2010, 2020, 4020, and 6025 work on the NSF2800-2 platform with too small memory (8 GB) and the CF card (2 GB). In a foreseeable time, as ADS provides more functions, the memory will become a more prominent bottleneck. To resolve this issue, on NSF2800-6 with a larger memory (32 GB) and CF card (8 GB), V4.5R89F02 supports ADS 2020E, 4020E, and 6025E which will replace ADS 2010/2020, 4020, and 6025 respectively in the future.

Also, ADS 200E and 600E work on the NSF1100-1 platform with too small memory (8 GB) and CF card (2 GB). In response to that, V4.5R89F02 supports ADS 800E on the NSF1100-3 platform with larger memory (16 GB) and CF card (8 GB) to replace ADS 200E/600E in the future.

The table lists the correspondence between hardware and software.

Hardware Platform	MEM	CF Card	Model	V4.5R89F00.sp02/sp03/sp04	V4.5R89F01CN/sp01	V4.5R89F02	V4.5R89F03
NSF2800-2	8 GB	2 GB	ADS NX3-2010	Support	Support	Support	Support
			ADS NX3-2020	Support	Support	Support	Support
			ADS NX5-4020	Support	Support	Support	Support
			ADS NX5-6025	Support	Support	Support	Support
NSF3600-4	64 GB	2 GB	ADS NX5-8000	Support	Support	Support	Support
NSF1100-1	8 GB	2 GB	ADS NX3-200E	Support	--	Support	Support
			ADS NX3-600E	Support	--	Support	Support
NSF1100-3	16 GB	8 GB	ADS NX3-800E	--	--	Support	Support
NSF2800-6	32 GB	8 GB	ADS NX3-2020E	--	--	Support	Support
			ADS NX5-4020E	--	--	Support	Support
			ADS NX5-6025E	--	--	Support	Support

Scheduled Backup of Configuration File

Function Description

During routine operation and maintenance, device configurations should be backed up for rapid business restoration in the case of maloperation or device failures. In earlier versions, ADS supports manual configuration backup only. However, automatic backup makes it possible to automate O&M, greatly increasing the work efficiency of O&M personnel and facilitating promotion.

V4.5R89F03 provides the automatic file backup function by sending configuration files to the specified FTP server on a scheduled basis to implement simple and efficient configuration backup.

Configuration Page

System > Local Settings > Configuration File Management > Configuration File Backup Settings

- The web-based manager provides backup-related parameters such as **FTP Server IP**, **Username**, **Password**, **Path**, and **Backup Frequency**.
- Options for **Backup Frequency** include **Daily**, **Weekly**, and **Monthly**.
 - When **Backup Frequency** is set to **Daily**, the configuration file will be sent to the FTP server at around 24:00 every day.
 - When **Backup Frequency** is set to **Weekly**, the configuration file will be sent to the FTP server at around 24:00 every Sunday.
 - When **Backup Frequency** is set to **Monthly**, the configuration file will be sent to the FTP server at around 24:00 on the first day of every month.
- Backup configuration files are named in the format of *IP address of the device_file generation time (YYYY-MM-DD)_collapsar.conf*.

Notes:

- The FTP server should grant relevant upload permissions for the specified user name.
- After the configuration is completed, you can click **Test Now** to check whether the settings are correct.

Support for RFC 1213 by SNMP Agent

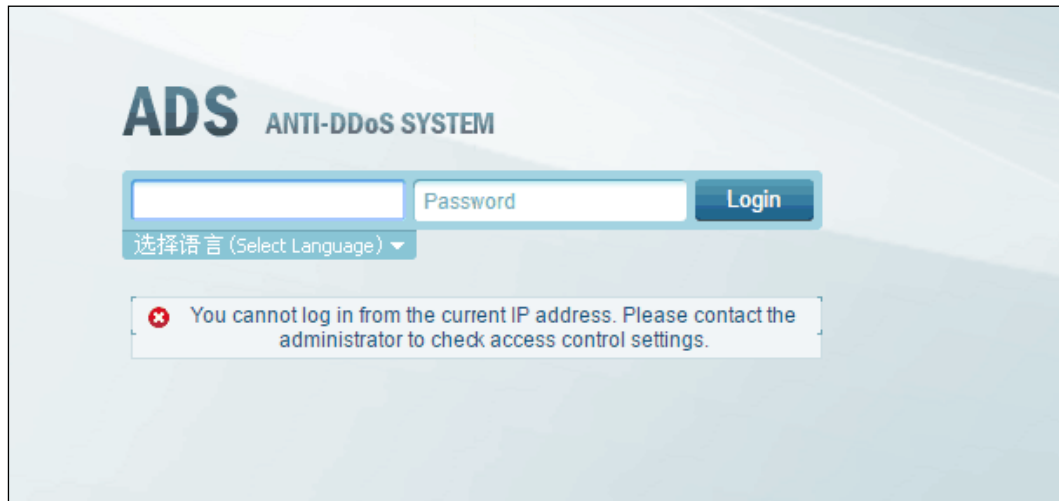
The SNMP agent's support for RFC 1213 indicates that it can obtain various fields given in RFC 1213 through a MIB browser (Windows) or SNMPWALK (Linux).

Compared with those in earlier versions, the SNMP agent in V4.5R89F02 can obtain variables specified in RFC 1213, in addition to retaining the memory usage and CPU usage of private OIDs of the company.

On ADS, RFC 1213 OIDs are of three types of object groups: system, interface, and IP address. For details, see the *PVD-ADS-V4.5R89F03 SNMP Description*.

Optimization of UI Display for Access Control

For earlier versions of ADS, a user's access from a blocked IP address is denied, with no display of a reason. This misleads the user into believing that there might be a bug or network problem. For V4.5R89F03, if a user accesses ADS from a blocked IP address, the system shows the reason for such a login failure before the account information is typed.



Remote Assistance Being Disabled by Default

With the remote assistance function of ADS, in the case of a system failure, you can enable SSH and log in to ADS via SSH to execute certain debugging commands for location and restoration. For earlier versions, this function is enabled by default.

For the sake of security, the remote assistance function is disabled on ADS V4.5R89F02 by default. This function needs to be enabled by a CLI user before being used. ADS V4.5R89F03 inherits this function.

Optimization of OAM Function for Checking Link Connectivity

Function Description

As a link connectivity issue may occur on an optical interface, V4.5R89F01 provides the OAM function for checking link connectivity: In a scenario where a Cisco router is configured as a peer device on which the OAM function is enabled, the OAM function needs to be enabled ADS to detect OAM packets. If no OAM packet is received in the specified time, ADS assumes that the link is abnormal and proactively shuts down the interface.

Notes

Compared with the previous configuration logic, the current CLI configuration in this regard retains three commands used to enable/disable the OAM function for checking the link connectivity and set the detection timeout period. For details, see the *ADS CLI User Guide*.

```
ADS#setflag set oam-check ?
  timeout          Set the oam check timeout threshold.
  open             Open oam check.
  close           Close oam check.
```



When this function is enabled on ADS, make sure that it is also enabled on the peer router. Once ADS shuts down the interface due to its failure to detect packets, ADS will not turn on this interface even if packets are received later. In this case, this interface needs to be enabled manually.

2 Changes to Web APIs

An API is added to implement the HTTP authentication synchronization function.

3 Compatibility with NTA Versions

- ADS V4.5R89F03 can collaborate with NTA 4.5R89F03 and both support IPv4 and IPv6 addresses.
- ADS V4.5R89F03 can collaborate with NTA V4.5.61.2.

4 Compatibility with ADS M Versions

ADS V4.5R89F03 can collaborate with ADS M V4.5R89F03.

5 Supported Browsers

Internet Explorer 9 and 10, Chrome, and Firefox browsers are supported.

6 Bugs Fixed in V4.5R89F03

Bug ID	Bug Description
Bug 110792	Under Advanced > Pattern Matching > Pattern Matching Rules , the GUI display of TCP flag configuration options should be optimized.
Bug 110840	[Web API] The API for deleting groups does not delete the related URL configuration files when deleting protection groups.
Bug 110997	[Translation] The tool tip for disabling ACK flood protection is not completely translated on the web-based manager.
Bug 111031	[External test] Units of measure are missing for both UDP protection and ICMP protection policies.
Bug 104793	When traffic is being diverted by ADS for an IP group, IP addresses can still be added to this group on ADS M.
Bug 105008	The built-in bypass is enabled by default after device restart.
Bug 104316	For an ADS cluster, ADS M fails to obtain the configured image verification template and synchronize it between ADS devices in this cluster.
Bug 104568	The manual diversion deletion process does not check the diversion status before deleting a diversion route.
Bug 111016	[NTA auto diversion for IPv6 addresses] When NTA dispatches an automatic diversion notification with a 128-bit hexadecimal IPv6 address, ADS fails to divert traffic and reports an error.
Bug 112231	[Injection route] After a user deletes an injection route and click Apply on the web-based manager, this injection route does not disappear from the injection routing table.

Bug ID	Bug Description
Bug 112109	[Whitelist] If a user clicks Reload , import results indicate that conflicting IP addresses are added to the trust list.
Bug 111782	[Remote assistance] After ADS is upgraded by installing an upgrade package, the remote assistance function is disabled.
Bug 116476	[SYN-ACK attack] Source IP addresses of SYN-ACK attacks are trusted by ADS.
Bug 112303	[Protection group] Attack traffic destined for an IP address that is added to the protection group does not hit any protection group policies but a global policy.
Bug 112113	[Protection group configuration in CLI] An error message is displayed in the CLI when a user attempts to add an IPv6 address to a protection group.
Bug 111989	[Manual traffic diversion configuration in CLI] When Extend is set to Enable , IPv6 addresses can be successfully added to manual diversion rules in the CLI.
Bug 116233	[HTTP authentication synchronization] During a normal synchronization, the synchronization status is displayed as Not synchronized .
Bug 112304	[Injection route] No matching injection route is found for the cleaned traffic, making it impossible for the traffic to be properly injected back to the network.
Bug 112114	[Protection group] The conflict check on IPv6 addresses in protection groups is not properly performed.
Bug 111991	[Protection group] Protection groups cannot be queried by IPv6 address.
Bug 116329	[Packet capture] ADS fails to capture SYN or ACK attack packets that are dropped.
Bug 116543	[HTTP authentication synchronization] The cluster name contains special characters and synchronization information cannot be properly dispatched.
Bug 116233	[HTTP authentication synchronization] During a normal synchronization, the synchronization status is displayed as Not synchronized .
Bug 112007	[Web API] The web API is unavailable on ADS as it returns "Authentication failed. You are not authorized to use this interface".
Bug 112213	[Protection group configuration via web APIs] When ADS M fails to dispatch region IP groups to ADS, the system displays "Incorrect netmask range".
Bug 112653	[Region IP group dispatch] When ADS M dispatches region IP groups to ADS, the system displays "Different network segments".
Bug 113943	[Vulnerability scanning] Nessus found a medium-risk vulnerability, namely, the SSL Medium Strength Cipher Suites Supported vulnerability.
Bug 116931	An error in the injection route module could cause the engine to stop working.
Bug 116140	The ACK flood protection performance needs to be improved.
Bug 117292	The bulk export of manual traffic diversion entries, if in large quantities, from ADS M may fail.
Bug 117988	Manual diversion instructions, when issued in cluster synchronization mode, take an unreasonably long time to take effect.
Bug 115548	Passwords are saved in plaintext.
Bug 118283	[CLI] During the addition of a manual diversion rule, the message explaining whether the rule can apply to individual IP addresses in the specified subnet according to the prefix length is incorrect.
Bug 118286	[CLI] The prefix length of IP addresses in protection groups should be checked.

Bug ID	Bug Description
Bug 118290	[CLI] The logic for determining the status of a group-related diversion route before deleting the route should be modified.
Bug 118297	[Web_API] The logic for determining the status of a group-related diversion route before deleting the route should be modified.
Bug 118714	[HTTP cluster synchronization] When HTTP authentication synchronization is enabled at different times on two ADS devices, the verification codes for dynamic script protection are inconsistent.
Bug 118078	[Collaboration with ADS M] ADS does not send XML files to ADS M.
Bug 119098	When disabled injection routes exist in the injection routing table, enabling injection route label learning crashes cfeapp.
Bug 117788	[ADS M (VM) collaborating with ADS E series] During the collaboration between ADS M (VM) and an ADS device of E series, the captured heartbeat information shows that the ADS's license cleaning capacity is 0.
Bug 119255	If an ADS device is configured with more than 2500 manual diversion rules, when the device is started, the engine status is displayed as "STOPPING" and more than one exception occurs.
Bug 115778	Sometimes ADS automatically switches to the bypass mode after running in in-path mode for some time.
Bug 122980	For SNMP agent configuration, the modified community value does not take effect and ADS does not respond to SNMP requests
Bug 122830	After the Apache service restarts, all processes previously started by the Apache service are killed. The size of files that supposed to be monitored by these processes will be unlimited, causing memory exhaustion and system exceptions.
Bug 122658	After the SNMP agent service is enabled, the size of the speed_snmp file keeps increasing.
Bug 122804	If a management platform is enabled under System > Local Settings > Management Mode and Attack Event Logs is selected for Syslog Type under System > Log Services > Syslog , after the specified management platform is disabled, a large number of flow files appear. If such files are not cleared in time, memory exhaustion will occur.

Version Upgrade

ADS can be upgraded to V4.5R89F03 from V4.5R88F02, V4.5R89F02.sp01, V4.5R89F02.sp02, V4.5R89F02.sp03, V4.5R89IB02, or V4.5R89IB02.sp01.

Upgrade from V4.5R89F02 or V4.5R89IB02 to V4.5R89F03

V4.5R89F03 is applicable to the following models:

- 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

The upgrade procedure is as follows:

Step 1 Install the patch package, **update_ADS_x86_V4.5R89F03_20170714.zip** (MD5: b37b0c74b42e7eb5df7480de38293aec) on ADS V4.5R89F02, V4.5R89F02.sp01, V4.5R89F02.sp02, V4.5R89F02.sp03, V4.5R89IB02, or V4.5R89IB02.sp01.

After the upgrade is complete, restart the device.

Step 2 Check whether **System Version** is **V4.5R89F03** in the status bar of the web-based manager.

 Note	<p>If the upgrade fails in step 1, contact the technical support personnel of NSFOCUS. After the problem (if any) is resolved, run the rollback command on the CLI to roll ADS back to the source version. If the rollback succeeds, the device will automatically restart. Then repeat the preceding steps to upgrade ADS to V4.5R89F03.</p>
--	---

---End

Notes

N/A

IPv4/IPv6 Support

The following table lists the support of modules in ADS V4.5R89F03 for IPv4 and IPv6.

Module	Description	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 rule	√	×
	IP behavior control	√	×
	SIP protection – default DDoS	√	×
	SIP protection – groups	√	√
	UDP payload check – payload check	√	√
	UDP payload check – mode check	√	×
	UDP protection – fragmented packet control	√	×
	ICMP fragment control	√	×
	UDP protection – maximum packet length	√	√
	UDP protection – traffic control based on the source IP address and source port	√	√
	UDP protection – traffic control based on the destination IP address and destination port	√	√
UDP protection – traffic control based on the source IP address	√	√	
UDP protection – traffic control based on the destination IP address	√	√	
UDP protection – minimum packet length	√	√	
UDP protection – traffic control based on the	√	√	

Module	Description	IPv4	IPv6
	destination IP address and source port		
	ICMP traffic rate limiting	√	√
	Watermark protection	√	×
	Protocol ID rules	√	√
	Group traffic control	√	√
	Port check	√	√
	URL Rule	√	√
	Advanced global parameters	√	√
	Policy auto-learning	√	√
	Access control rules	√	√
	GeoIP rules	√	√
	Regular expression rules	√	×
	Hardware access control rules	√	√
	Connection exhaustion rules	√	×
	URL-ACL protection rules	√	√
	Blacklist	√	×
	Whitelist	√	√
	HTTP keyword check	√	×
	DNS keyword check	√	×
Diversion & Injection	Running mode	√	√
	Port channel configuration	√	√
	IP address configuration	√	√
	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	Description	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 Kuangung devices	– √	×
Collaboration	Collaboration with ADS M	√	√
	Collaboration with ESPP	√	×
	Collaboration with NTA V4.5.61.2	√	×
	Collaboration with NTA V4.5R89F03	√	√
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	—	—
	User management	√	√
	Management mode configuration	√	√
	Configuration file management	√	√
	HA configuration	√	√
	Collaboration configuration	√	×
	Bandwidth overrun limit	√	×
	Login security settings	√	×

Module	Description	IPv4	IPv6
	Locked user management	√	×
	Authentication configuration	√	√
	Syslog setting	√	√
	SNMP trap configuration	√	√
	SNMP agent setting	√	×
	Email configuration	√	√
	SFTP/SSH log export	√	×
	License interface	—	—
	License-based speed limit	—	—
	System upgrade	—	—
	Remote assistance	—	—
	SSL certificate import	—	—
	One-click information collection	—	—
	Version information	—	—
Advanced	Packet capture	√	√
	Pattern matching rules	√	√
NSFOCUS Threat Intelligence	Upload	√	√
	Synchronization	√	×
	Search	√	×