1 Basic Information

Product Model	• ADS NX3-800E • ADS NX3-2020E • ADS NX5-4020E • ADS NX5-6025E • ADS NX5-HD1000 • ADS NX5-HD5000 • ADS NXT-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 NX1-VN01
Software Version	V4.5R90F05
Upgrade File	update_ADS_x86_V4.5R90F05_20231204.zip update_ADS_arm_V4.5R90F05_20231204.zip
MD5	962cc4653a83d4e44eda1d5f1e6351a8 update_ADS_x86_V4.5R90F05_20231204.zip 01c36883ba67ebf636f64bc40dc97aad update_ADS_arm_V4.5R90F05_20231204.zip
SHA256SUM	8a45cb62515546cc031754ddd155dd856c86ac88d2397ce5c4274db725fdf83e update_ADS_x86_V4.5R90F05_20231204.zip fa9d0b1836a6c72c18a5eca004bff396b578f1c46a6e71b00559035e8ac8cf77 update_ADS_arm_V4.5R90F05_20231204.zip
How to Obtain	Contact NSFOCUS technical support.

2 Version Mapping

Source Software Version	V4.5R90F05
Product Model	• NSF1100-3 • NSF2800-6 • NSF3600-4 • NSP-7224B • NSP-7124A • NSP-71C2A • NSP-72C2A • HTCA • NX1-VN • PHYTIUM-LY • PHYTIUM-D2000-GF
Network Traffic Analyzer Platform	NTA V4.5R90F05
Management Platform Version	ADS M V4.5R90F05
Client Software	None
Other System or Tool	None
Documentation	*NSFOCUS ADS V4.5R90F05 User Guide*

3 Function Changes

Applicable device models:

ADS NX3-800E/2020E/HD1000/HD2500

ADS NX5-4020E/6025E/HD4500/HD6500/HD8500/HD5000/HD6000

ADS NX5-8000

ADS NX5-HFA2000/HFB3000

ADS NX5-10000/12000/20000

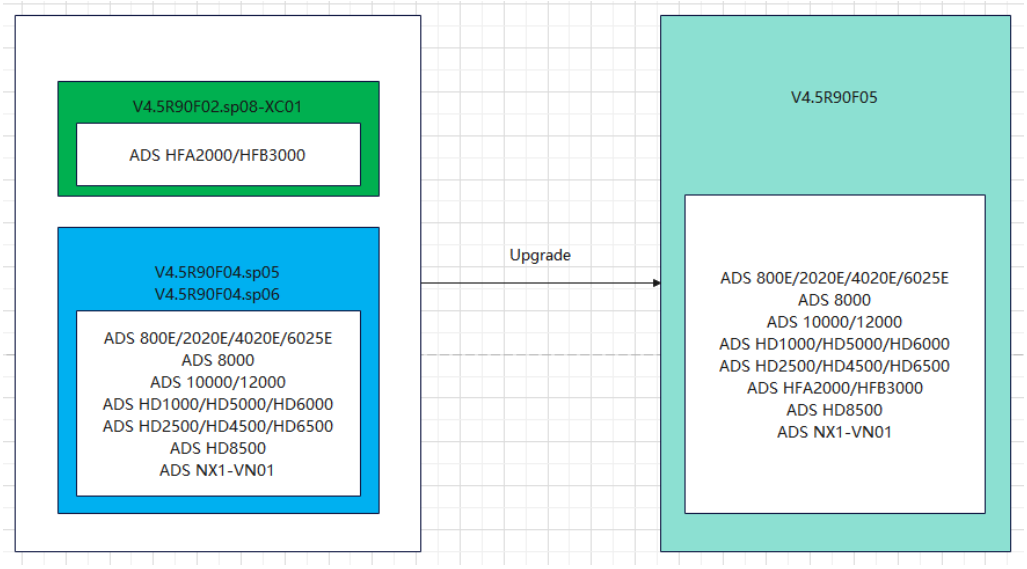
ADS NX1-VN01

3.1 Support for Hardware Platforms

In V4.5R90F05, a software version supports all hardware platforms.

For ADS NX3-800E, ADS NX3-2020E, ADS NX5-4020E, ADS NX5-6025E, ADS NX3-HD2500, ADS NX5-HD4500, ADS NX5-HD6500, ADS NX3-HD1000, ADS NX5-HD5000, ADS NX5-HD6000, ADS NX5-HD8500, ADS NX5-8000, ADS NX5-10000, ADS NX5-12000, and ADS NX1-VN01, you need to first upgrade them to V4.5R90F04.sp05 or V4.5R90F04.sp06 before upgrading to V4.5R90F05.

For ADS NX5-HFA2000, ADS NX5-HFB3000, you need to first upgrade them to V4.5R90F02.sp08-XC01 before upgrading to V4.5R90F05.



3.2 Function Changes

3.2.1 New/Optimized Functions

Function	Description
Traffic diversion	Both manual traffic diversion rules and the diversion route list now can be exported.
Programmable rules	Programmable rules are added to implement defenses at the data level. You can generate a rule of a specific programming language to match packets with signatures and protect against packets containing hidden rules or complex logic.
Fingerprint extraction from a packet capture file	The packet capture file of a manual or automatic packet capture task can be analyzed to extract payload fingerprints, which can be directly added to pattern matching rules.
Group traffic statistics	The group traffic statistics can be exported to an XML file for the use by a management platform.
Prioritized destination IP address	Destination IP addresses can be prioritized for traffic statistics. In this way, traffic of the prioritized IP address will be always counted.
Carpet bombing protection	Carpet bombing can be defended against.
Packet sampling ratio	The sampling ratio can be set for capturing packets. The packet sampling ratio allows the device to capture packets in a longer period. After the packet sampling ratio is set, a single packet capture file can better reflect the overall traffic situation.
Improved protection capability against zombie hosts	The underlying session monitoring is added, which is upgraded from source IP behavior monitoring. This provides more granular protection, including the rate limiting for DNS query and POST packets, and supports actions of rate limiting and blocklist.
Optimized automatic packet capture	The sampling ratio can be set for automatic packet capture tasks. In addition, options are provided for ADS to capture packets destined for a specific IP address or protection group, or whatever packets passing

	through the device.
Application layer protection – non-decrypted traffic protection	In the case of no certificate, the device detects whether a source IP address is abnormal by checking its session to large or specific resources and defends against HTTPS attacks without decrypting HTTPS packets.
More static rules supported	The concurrent connection of a connection exhaustion protection rule is increased from 64 to 512. The maximum numbers of DNS keyword checking rules, HTTP keyword checking rules, and regular expression rules are increased from 512 to 1024.
After-sales touchpoints	An email warning is sent when the license is about to expire.

3.2.2 Affected Functions

The following table lists functions affected by the upgrade.

Function	V4.5R90F04	V4.5R90F05	Impact
Protection groups	• Programmable rules and application layer protection – non-decrypted traffic protection are not supported. • The IP behavior control policy is rough.	• Programmable rules can be configured. • Application layer protection – non-decrypted traffic protection is added. • The IP behavior control is changed to botnet & IP behavior control, which implements refined rate limiting for more packet types.	None.
Manual packet capture	The sampling ratio is not supported.	The sampling ratio can be set for capturing packets.	None.
Automatic packet capture	The sampling ratio is not supported, and only the traffic of IP addresses can be captured.	The sampling ratio can be set for capturing packets. The object whose traffic will trigger an automatic packet capture task can be specified. Options include **Device**, **Group**, and **IP**.	None.

3.3 Description of Major Functions

3.3.1 Optimized Manual Traffic Diversion Rules

Function Description

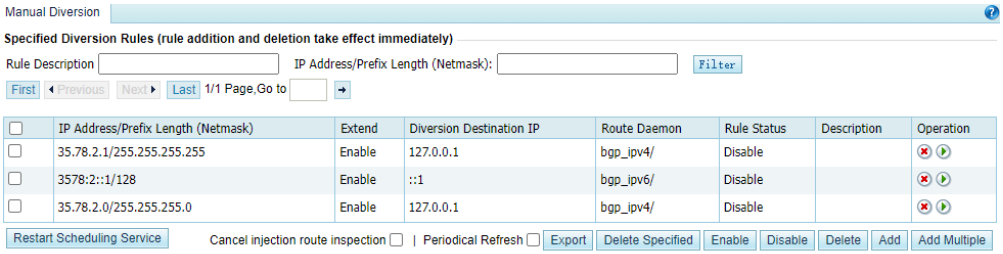
Both manual traffic diversion rules and the diversion routing list now can be exported to a TXT file.

You can open the file with a text editor and directly search for the desired data. In contrast, on the web-based manager, you can query data only based on available query fields.

The first line of the export file of manual traffic diversion rules describes data in each column. The data starts from the second line, which follows the same format specifications of the **Add Multiple** function. You can click **Add Multiple** on the **Manual Diversion** page and directly copy data from the export file to the text box under the **Diversion Route** area to add them again. To modify manual traffic diversion rules in batches, you can export them, modify data in the file, and then copy them to the text box of the **Add Multiple** function.

Related Pages

Choose **Diversion & Injection > Traffic Diversion > Manual Diversion** and click **Export**.



Notes

None.

3.3.2 Programmable Rules

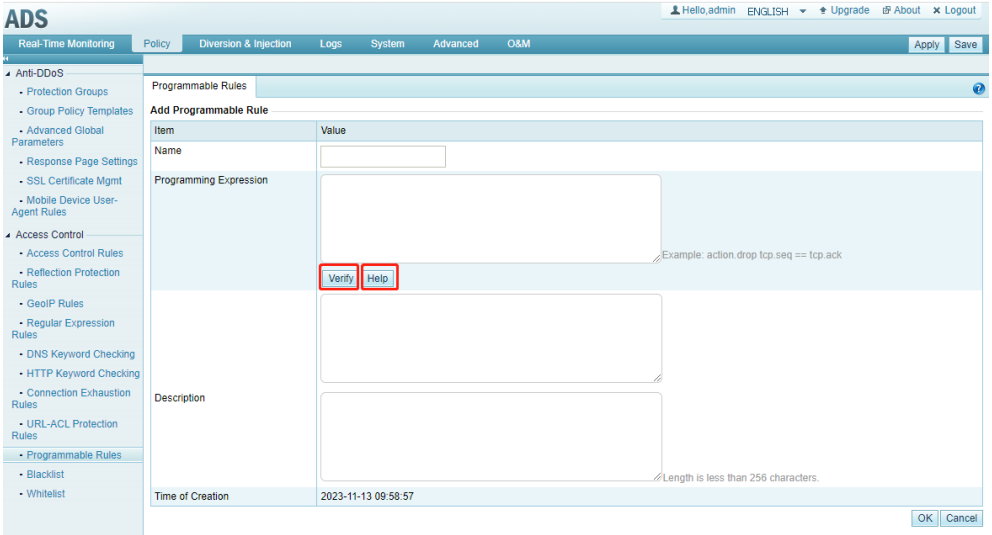
Function Description

Programmable rules are added to implement defenses at the data level. You can generate a rule of a specific programming language to match packets with signatures and protect against packets containing hidden rules or complex logic.

Related Pages

Choose **Policy > Access Control > Programmable Rules**.

Click **Add** to configure a programmable rule.



You can click **Help** to view the available fields on the page that appears. The syntax is the same as the packet filtering syntax of Wireshark.

Policies

Parameter Description

action.drop — drops packets. Example: action.drop ip.len == 20

action.drop_black — drops packets and adds source IP addresses to the blacklist. Example: action.drop_black ip.len == 20

action.accept — allows traffic to pass through. Example: action.accept ip.len == 20

action.accept_white — allows traffic to pass through and adds the IP address to the whitelist. Example: action.accept_white ip.len == 20

action.accept_trust_low — allows traffic to pass through and adds IP addresses to the low-level trust list. Example: action.accept_trust_low ip.len == 20

action.accept_trust_high — allows traffic to pass through and adds IP addresses to the high-level trust list. Example: action.accept_trust_high ip.len == 20

Eth Headers

Parameter Description

frame.len — obtains the frame length. Example: action.drop frame.len == 60

vlan.etype — obtains the VLAN packet type. Example: action.drop vlan.etype == 0x8100

vlan.id — obtains the VLAN ID. Example: action.drop vlan.id == 10

eth.addr — obtains the source or destination MAC address. Example: action.drop eth.addr == 7a:7b:c0:a8:c8:01

eth.dst — obtains the destination MAC address. Example: action.drop eth.dst == 7a:7b:c0:a8:c8:01

eth.src — obtains the source MAC address. Example: action.drop eth.src == 7a:7b:c0:a8:c8:01

eth.len — obtains the layer 2 packet length. Example: action.drop eth.len == 14

eth.type — obtains the protocol type. Example: action.drop eth.type == 0x800

IPv4 Headers

Parameter Description

ip.version — obtains the IPv4 version number. Example: action.drop ip.version == 4

ip.hdr_len — obtains the IPv4 header length. Example: action.drop ip.hdr_len == 20

ip.toss — obtains the IPv4 TOS. Example: action.drop ip.tos == 1

ip.len — obtains the total IPv4 packet length. Example: action.drop ip.len == 55

ip.id — obtains the IPv4 ID. Example: action.drop ip.id == 0xbb17

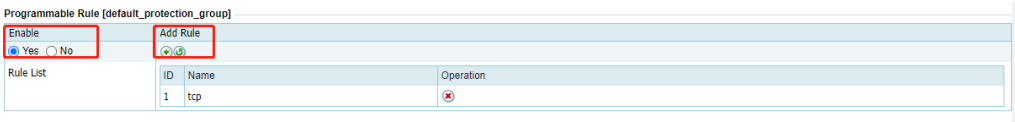
ip.dst — obtains the destination IPv4 address. Example: action.drop ip.dst == 97.47.2.3

ip.src — obtains the source IPv4 address. Example: action.drop ip.src == 1.2.3.4

ip.addr — obtains the source or destination IPv4 address. Example: action.drop ip.addr == 97.47.2.3

After the expression is complete, you can click **Verify** to check whether the expression typed is correct. The verification result is shown below.

The programmable rule configured can be referenced by a protection group.



Notes

A protection group can only reference one programmable rule.

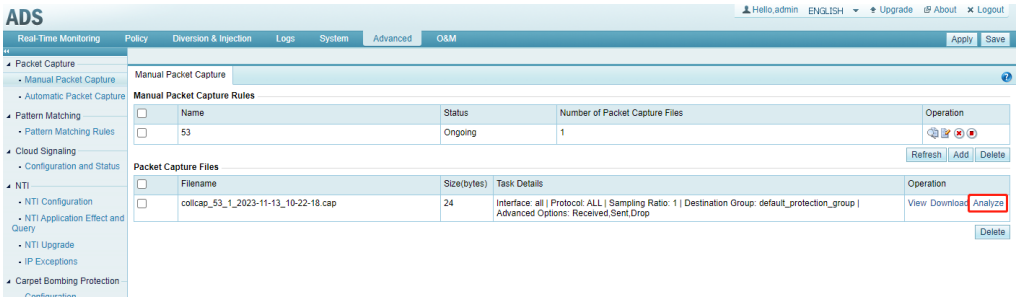
3.3.3 Fingerprint Extraction from a Packet Capture File

Function Description

The packet capture file of a manual or automatic packet capture task can be analyzed to extract payload fingerprints, which can be directly added to pattern matching rules.

Related Pages

Choose **Advanced > Packet Capture > Manual Packet Capture** and click **Analyze** in the **Operation** column.



Notes

- Currently, fingerprints can be extracted only from non-DNS query UDP packets.
- Only fingerprints longer than 4 bytes can be found.
- Fingerprints can be extracted only when the packet capture file contains at least 100 UDP packets.
- Up to 10 fingerprints can be extracted from one packet capture file.

3.3.4 Group Traffic Statistics

Function Description

The inbound traffic, outbound traffic, protocol traffic, and dropped traffic of a protection group can be counted and exported to an XML file. The file and other XML files containing other traffic statistics are compressed to a package and sent to ADS M for analysis and display.

Formats are as follows:

```
<CollapsarData collapsarIP="10.66.242.121" timeStamp="1679906777"
collapsarType="ADS-8000">
   <protection_group_stat begin_time="1679906777" end_time="1679906807">
      <group_stat group_name="mygroup" in_pkts="10" in_bytes="600" out_pkts="5"
out_bytes="300" drop_pkts="5" drop_bytes="300">
         <group_proto_stat>
            <proto_stat proto="TCP_SYN" in_pkts="10" in_bytes="600" out_pkts="5"
out_bytes="300" drop_pkts="5" drop_bytes="300" />
            <proto_stat proto="TCP_SYNACK" in_pkts="10" in_bytes="600" out_pkts="5"
out_bytes="300" drop_pkts="5" drop_bytes="300" />
            <!—Other protocols -->
         </group_proto_stat>
         <group_atk_stat>
            <atk_stat atk="SYN Flood" drop_pkts="5" drop_bytes="300" />
            <atk_stat atk="ACK Flood" drop_pkts="5" drop_bytes="300" />
            <!-- Other types -->
         </group_atk_stat>
         <group_policy_stat>
            <policy_stat policy="SYN_Algorithm" drop_pkts="5" drop_bytes="300" />
            <policy_stat policy="SYN_Algorithm_Cookie" drop_pkts="5"
drop_bytes="300" />
            <!-- Other types -->
         </group_atk_stat>
      </group_stat>
   </protection_group_stat>
   <attack_map>
      <attack_item value="SYN Flood" />
       <attack_item value="ACK Flood" />
      <attack_item value="FIN/RST Flood" />
      <attack_item value="TCP Misuse" />
      …(Other irrelevant data is omitted)
      <attack_item value="CLDAP Amplification" />
      <attack_item value="MS SQL Amplification" />
      <attack_item value="TI Strategy" />
   </attack_map>
   <proto_map>
      <proto_item value=”TCP_SYN”>
      <proto_item value=”TCP_SYNACK”>
      …(Other irrelevant data is omitted)
      <proto_item value=”ICMP”>
      <proto_item value=”OTHER”>
   </proto_map>
   <policy_map>
      <policy_item value=”SYN_Algorithm”>
      <policy_item value=”SYN_Algorithm_Cookie”>
      …(Other irrelevant data is omitted)
      <policy_item value=”TRANSID_REPEAT”>
      <policy_item value=”dyn”>
   </policy_map>
</CollapsarData>
```

Note	• If no traffic of a protocol, attack, or policy is generated, this type will not be included in the XML file. If the traffic of all subitems of a label is 0, this label is not included. • The **<attack_map>**, **<proto_map>**, and **<policy_map>** labels are the full list of attacks, protocols, and protection groups, indicating the respective types that ADS supports.

Related Pages

This function is enabled by default. No configuration is provided.

Notes

None.

3.3.5 Prioritized Destination IP Address

Function Description

The destination IP addresses/segments can be configured to be globally effective and prioritized for traffic statistics. The traffic of these IP addresses/segments will be preferentially counted and additionally displayed.

Related Pages

This is configured in the web API. For details, see the "Prioritized Destination IP Address" section of *NSFOCUS ADS Web API Description*.

Notes

None.

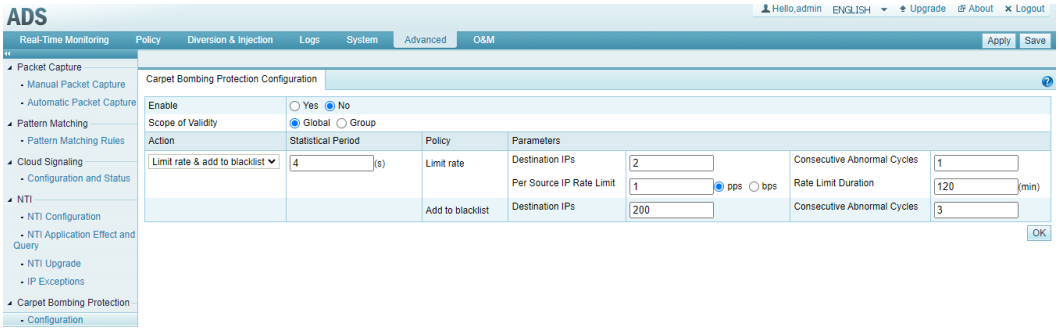
3.3.6 Carpet Bombing Protection

Function Description

Through the carpet combing protection, ADS counts the number of visits of a source IP address to destination IP addresses in a given period and determines whether the source IP address is abnormal. For the identified attack source, the system can add it to the blocklist or limit its rate, or do both.

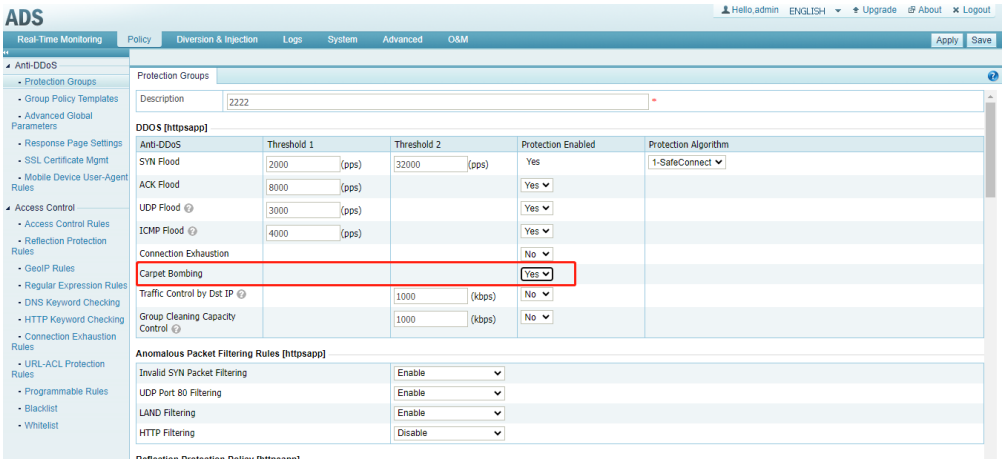
Related Pages

Choose **Advanced > Carpet Bombing Protection > Configuration**.



- **Enable**: Controls whether to enable the carpet bombing protection function. When it is set to **No**, carpet bombing will not be defended against.
- **Scope of Validity**: Specifies the application scope of the carpet bombing protection. Options include **Global** or **Group**. If **Group** is selected, you should also enable carpet bombing protection in policies configured for the group you want to protect from this type of attacks.
- Action: Specifies the action taken for carpet bombing protection. Options include **Limit rate**, **Add to blacklist**, and **Limit rate & add to blacklist**. The **Statistic Period** configuration is applicable to the **Limit rate** and **Add to blacklist** policies.
- **Destination IPs**: specifies maximum allowed number of destination IP addresses accessed by a single source IP address in the statistical period. The source IP address will be considered to be abnormal when the destination IP addresses it accesses reach or exceed the threshold. The **Destination IPs** for the **Limit rate** and **Add to blacklist** policies are irrelevant.
- **Consecutive Abnormal Cycles**: specifies the number of consecutive cycles after which the protection policy is triggered. When a source IP address accesses more IP addresses than the value of **Destination IPs** within the statistical period and this anomaly persists for the specified number of **Consecutive Abnormal Cycles**, the device limits its traffic or adds it to the blocklist.

After you select **Yes** for **Enable** and **Group** for **Scope of Validity**, you should also enable carpet bombing protection in policies configured for the group on the **Policy > Anti-DDoS > Protection Groups** page.



Notes

The thresholds for the rate limiting and blocklist policy are irrelevant. When the action is set to **Limit rate & add to blacklist**, ensure that the rate limiting policy is triggered before the blocklist policy to achieve better protection.

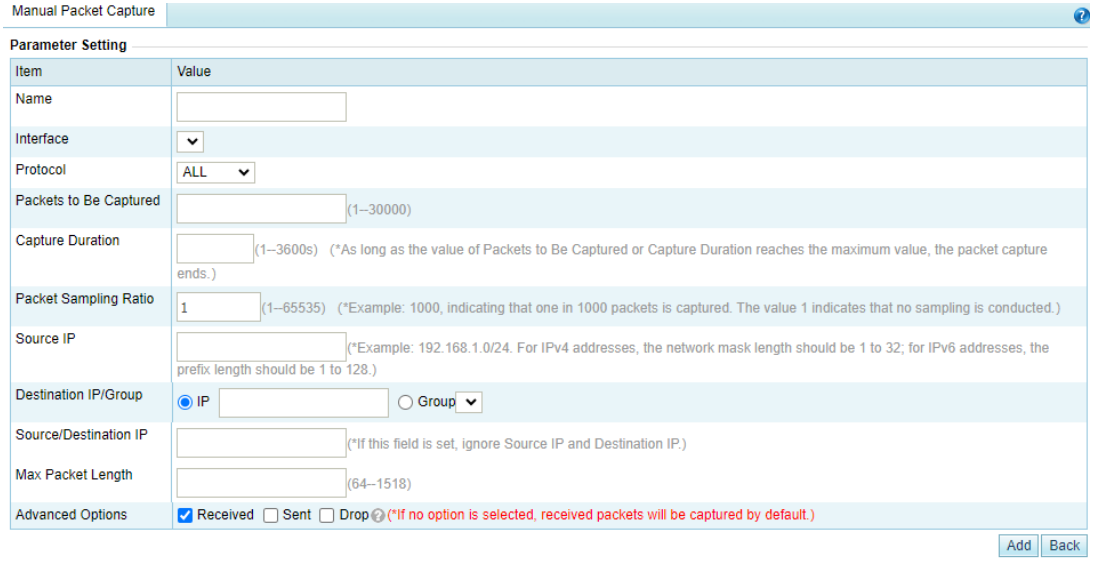
3.3.7 Packet Sampling Ratio

Function Description

The sampling ratio can be set for capturing packets. The packet sampling ratio allows the device to capture packets in a longer period. After the packet sampling ratio is set, a single packet capture file can better reflect the overall traffic situation.

Related Pages

Choose **Advanced > Packet Capture > Manual Packet Capture** and click **Add** to configure a manual packet capture task.



Choose **Advanced > Packet Capture > Automatic Packet Capture** and click **Add** in the **Rate-triggered Packet Capture** area to configure an automatic packet capture task.

Automatic Packet Capture

Trigger Condition

Item	Value
Object	Device
Trigger Rate	Rx Tx * bps (1-4294967960)

Parameter Configuration

Item	Value
Name	
Interface	ALL
Protocol	ALL
Packets to Be Captured	*(1--30000)
Packet Sampling Ratio	1 (1--65535) (*Example: 1000, indicating that one in 1000 packets is captured. The value 1 indicates that no sampling is conducted.)
Source IP	(*Example: 192.168.1.0/24. For IPv4 addresses, the network mask length should be 1 to 32; for IPv6 addresses, the prefix length should be 1 to 128.)
Destination IP/Group	IP Group default_protection_group
Source/Destination IP	(*If this field is set, ignore Source IP and Destination IP.)
Max Packet Length	(64--1518)
Advanced Options	Received Sent Drop (*If no option is selected, received packets will be captured by default.)
Upload to ADS M	Yes No

Add Back

Choose **Advanced > Packet Capture > Automatic Packet Capture** and click Modify in the **Attack-triggered Packet Capture** area to edit parameters.

Edited attack-triggered packet capture

Status

Item	Value
Enable	Yes No

Trigger Condition

Item	Value
Trigger Rate	100 * pps (1-4294967295)

Parameter Configuration

Item	Value
Capture Duration	20 *(1--300)
Packets to Be Captured	3000 *(1--30000)
Packet Sampling Ratio	1 (1--65535) (*Example: 1000, indicating that one in 1000 packets is captured. The value 1 indicates that no sampling is conducted.)
Upload Method	SFTP/SSH
Server IP	(IPv4/IPv6)
Username	
Password	Edit Password ((Not editing the password indicates that the original one is used.))
Path	(Fill in a UNIX absolute path, for example: /tmp/.)

OK Cancel

Both **Packet Capture Files** and **Packet Details** area display the sampling ratio for analysis.

Packet Capture Files

	Filename	Size(bytes)	Task Details	Operation
	collcap_53_1_2023-11-13_10-22-18.cap	311998	Interface: all | Protocol: ALL | Sampling Ratio: 1 | Destination Group: default_protection_group | Advanced Options: Received,Sent,Drop	View Download Analyze

Delete

Notes

None.

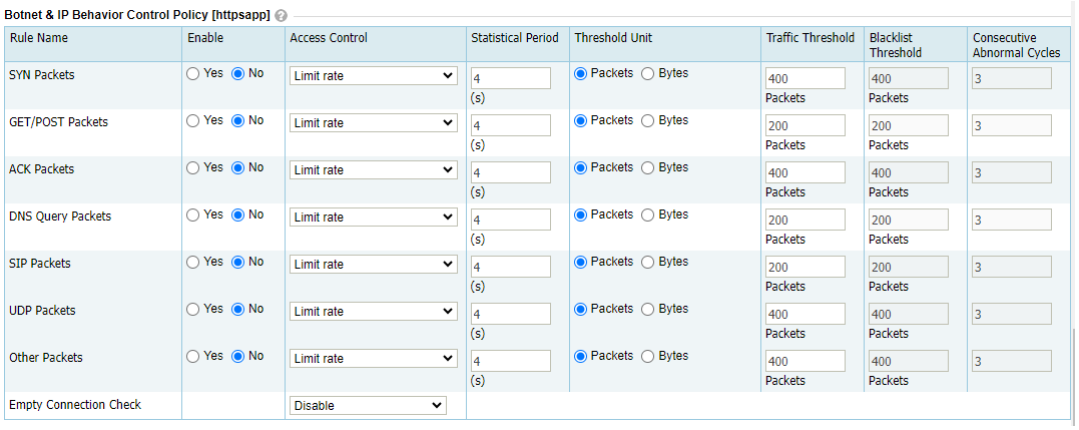
3.3.8 Improved Protection Capability Against Zombie Hosts

Function Description

The underlying session monitoring is added, which is upgraded from source IP address behavior monitoring. This provides more granular protection, including the rate limiting for DNS query and POST packets, and supports actions of rate limiting and blocklist.

Related Pages

Choose **Policy > Protection Groups**. Click in the **Protection Policy** column to configure parameters in the **Botnet & IP Behavior Control Policy** area.



Threshold Unit specifies how to measure the packet forwarding rate. You can select either **Packets** or **Bytes**. The unit selected will be used for **Traffic Threshold** and **Blacklist Threshold**.

The **Blacklist Threshold** and **Consecutive Abnormal Cycles** parameters are available only when **Access Control** is set to **Limit rate & add to blacklist**.

Notes

- For DNS query packets, when rate limiting is enabled for both DNS query and UDP packets, ADS first checks whether DNS query packets exceed the related threshold and if not, continues to check these packets against the UDP packet threshold.
- Similarly, for SIP packets, when rate limiting is enabled for both SIP and UDP packets, ADS first checks whether SIP packets exceed the related threshold and if not, continues to check these packets against the UDP packet threshold.

- After the upgrade, rate limiting is added for DNS query, SIP, and UDP packets, controlled by the **Enable** switch. For SYN packets, ACK packets, GET/POST packets, and other packets, the **Enable** switch remains for rate limiting and configurations change as follows:
  - **Limit rate** selected before the upgrade: After the upgrade, the action remains selected, both **Traffic Threshold** and **Blacklist Threshold** use the original threshold value, and **Consecutive Abnormal Cycles** is set to **3**.
  - **Drop and add to blacklist** selected before the upgrade: After the upgrade, the action changes to **Limit rate & add to blacklist**, both **Traffic Threshold** and **Blacklist Threshold** use the original threshold value, and **Consecutive Abnormal Cycles** is set to **1**.

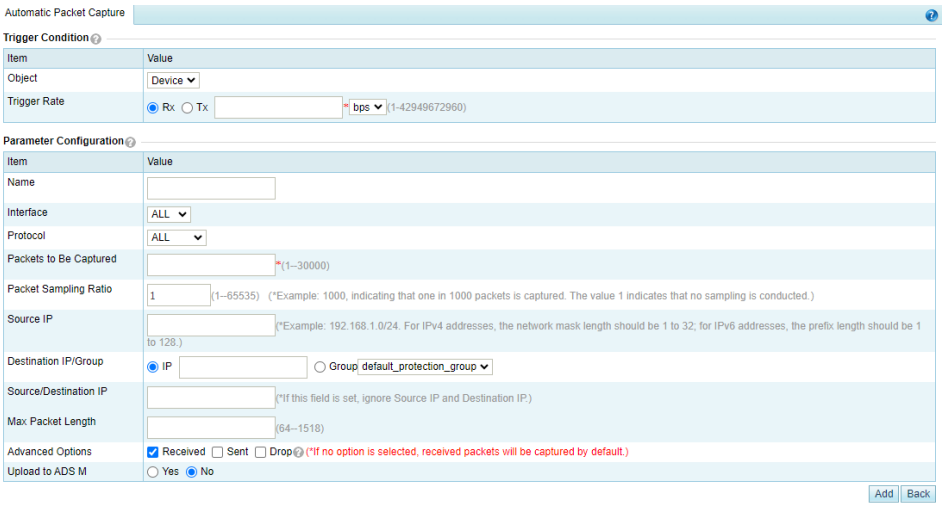
3.3.9 Optimized Automatic Packet Capture

Function Description

More parameters can be set for a rate-triggered automatic packet capture task. For example, the outbound traffic of a group or the device can also trigger an automatic packet capture task. Other parameters are the same as those for a manual packet capture task.

Related Pages

Choose **Advanced > Packet Capture > Automatic Packet Capture** and click **Add** in the **Rate-triggered Packet Capture** area to configure an automatic packet capture task.



Notes

None.

3.3.10 Application Layer Protection – Non-decrypted Traffic Protection

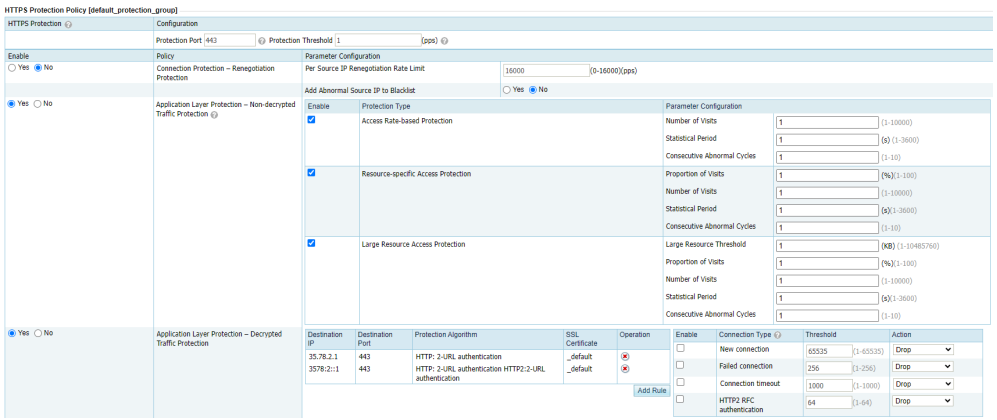
Function Description

The HTTPS protection policy of protection groups are more refined. The connection protection and application layer protection are changed to connection protection – renegotiation protection and application layer – decrypted traffic protection respectively.

The application layer protection – non-decrypted traffic protection is added, which includes access rate-based protection, resource-specific access protection, and large resource access protection. This type of protection checks HTTPS sessions from a source IP address without decrypting HTTPS packets and detects whether the IP address is a normal user or possible attacker.

Related Pages

Choose **Policy > Anti-DDoS > Protection Groups**. Click in the **Protection Policy** column to configure parameters in the **HTTPS Protection Policy** area.



Notes

All packets destined for ports specified in **Protection Port** are monitored with the algorithm of application layer protection – non-decrypted traffic protection. All packets matching the application layer protection – decrypted traffic protection rule are also monitored according to the application layer protection – non-decrypted traffic protection configurations.

When all protection algorithms are enabled for HTTPS protection, packets are first monitored according to configurations of connection protection – renegotiation protection and application layer – decrypted traffic protection, and then subject to the application layer protection – non-decrypted traffic protection configurations.

3.3.11 More Static Rules Supported

Function Description

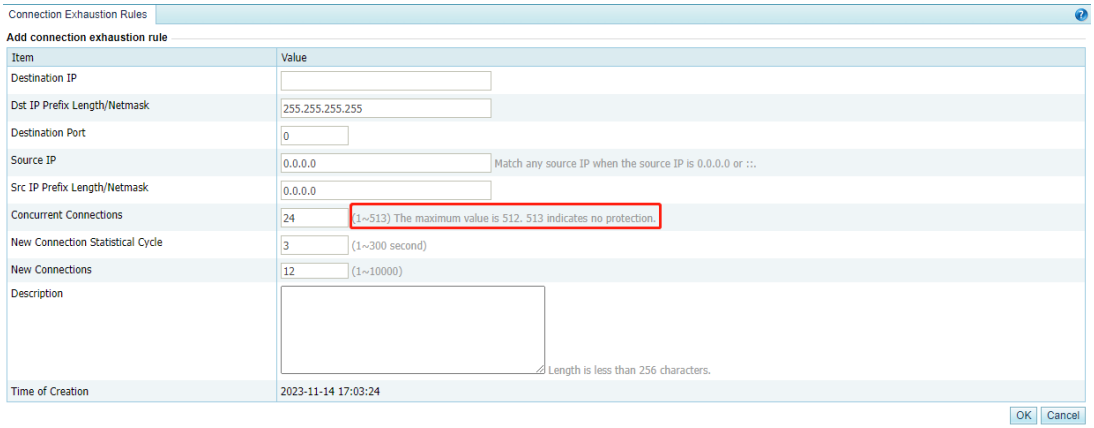
The number of concurrent connections of a connection exhaustion rule is increased to 512. The value **513** indicates no protection.

The maximum number of the following rules is increased to 1024:

- Regular expression rules
- DNS keyword checking rules
- HTTP keyword checking rules

Related Pages

Choose **Policy > Access Control > Connection Exhaustion Rules** and click **Add** to configure a connection exhaustion rule.



- Choose **Policy > Access Control > Regular Expression Rules**.
- Choose **Policy > Access Control > DNS Keyword Checking**.
- Choose **Policy > Access Control > HTTP Keyword Checking**.

Notes

None.

3.3.12 After-sales Touchpoint Requirements

Function Description

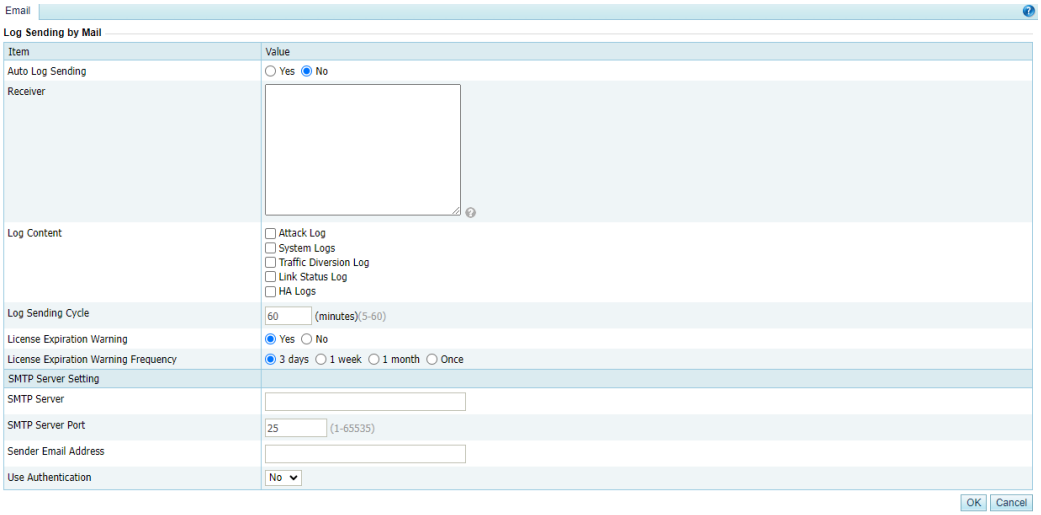
The license expiration warning is sent via email.

For a formal license, within 90 days before the license expires, the system sends the first warning via email. For a trial license, within seven days before the license expires, the system sends the first warning via email. Subsequently, the alert email will be sent according to the configured frequency.

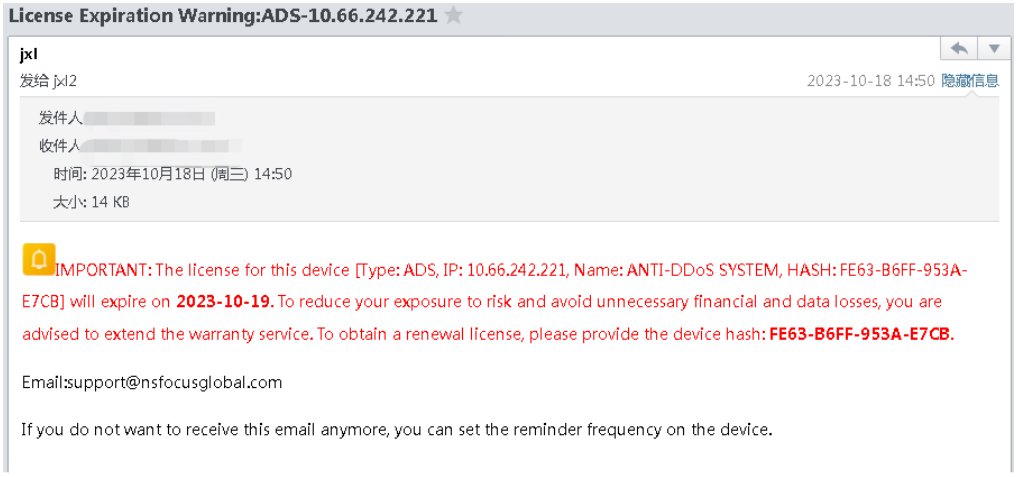
Alert email will also be sent when a formal or trial license expires. Subsequently, the alert email will be sent according to **License Expiration Warning Frequency** configured.

Related Pages

Choose **System > Log Services > Email**.



The following is a sample alert email:



Notes

The email language is determined by the region selected on the configuration wizard.

3.3.13 Power Supplay Status

Function Description

ADS NX5-HD5000 and NX5-HD6000 devices have one power supply indcator displayed on the web-based manager, which indicates the overall power supply status without distinguishing power supply 1 from power supply 2.

Related Pages

Choose **Real-Time Monitoring**. You can view the power supply indicator in the **System Resources** area.

Notes

None.

4 Compatiable NTA Versions

ADS can collaborate with NTA 4.5R90F05 for IPv4 and IPv6.

5 Supported Broswer Versions

You are advised to use a Microsoft Edge, Chrome, or Firefox browser.

6 Upgrade

Target Version

V4.5R90F05

Applicable Device Models

ADS NX3-800E

ADS NX3-2020E

ADS NX5-4020E

ADS NX5-6025E

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 NX1-VN01

Source Version

V4.5R90F04.sp05,V4.5R90F04.sp06

Upgrade Procedure

The upgrade to V4.5R90F05 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 drive.

Step 2 Install the patch package, **update_ADS_x86_V4.5R90F05_20231204.zip (**MD5: 962cc4653a83d4e44eda1d5f1e6351a8) on ADS V4.5R90F04SP05 or V4.5R90F04SP06.

When the system displays a message, prompting an upgrade success, restart the device.

Step 3 Verify that the system version turns to **V4.5R90F5** in the status bar of the web-based manager.

----End

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

Target Version

V4.5R90F05

Applicable Device Models

ADS NX5-HFA2000

ADS NX5-HFB3000

Source Version

V4.5R90F02.sp08-XC01

Upgrade Procedure

The upgrade to V4.5R90F05 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 drive.

Step 2 Install the patch package, **update_ADS_arm_V4.5R90F05_20231204.zip (**MD5: 01c36883ba67ebf636f64bc40dc97aad) on ADS V4.5R90F02SP08-XC01.

When the system displays a message, prompting an upgrade success, restart the device.

Step 3 Verify that the system version turns to **V4.5R90F5** in the status bar of the web-based manager.

----End

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

7 Rollback

ADS R4.5R90F05 does not support the rollback to a previous version in a CLI window. If rollback is required, contact NSFOCUS technical support, with the configuration file exported in Step 1 provided.