

Basic Information

Product Model	ADS NX3-800E, ADS NX3-2020E, ADS NX5-4020E, ADS NX5-6025E, ADS NX3-HD2500, ADS NX5-HD4500, ADS NX5-HD6500, ADS NX5-HD8500, ADS NX5-8000, ADS NX5-10000, ADS NX5-12000, ADS NX1-VN01
Software Version	V4.5R90F03
Upgrade File	update_ADS_x86_V4.5R90F03_20211203.zip
Md5	7be246439ec520b573ba9f2abf847413
SHA256SUM	77e04a12dad5dd63ffe2f97f6d7f65eccf4156afdf20821454e5811971a9dfe4
Release Date	2021-12-09
How to Obtain	Contact NSFOCUS technical support.

Version Mapping

Source Software Version	V4.5R90F03
Product Model	NSF1100-1, NSF1100-3, NSF2800-2, NSF2800-6, NSF3600-4, NSP-7224B, NSP-7124A, HTCA-6U, vADS
Network Traffic Analyzer Platform Version	V4.5R90F03
Management Platform	ADS M V4.5R90F03
Client	None
Other System or Tool	None
Documentation	NSFOCUS ADS User Guide (V4.5R90F03)

Function Changes

1 Changes of Functions in V4.5R90F03

Supported Models

- ADS NX3-800E
- ADS NX3-2020E/HD2500
- ADS NX5-4020E/6025E/HD4500/HD6500/HD8500
- ADS NX5-8000
- ADS NX5-10000/12000

- ADS NX1-VN01

1.1 Support for Hardware Platforms

V4.5R90F03 inherits the uniform platform support feature from V4.5R90F02. In other words, a software version supports all hardware platforms.

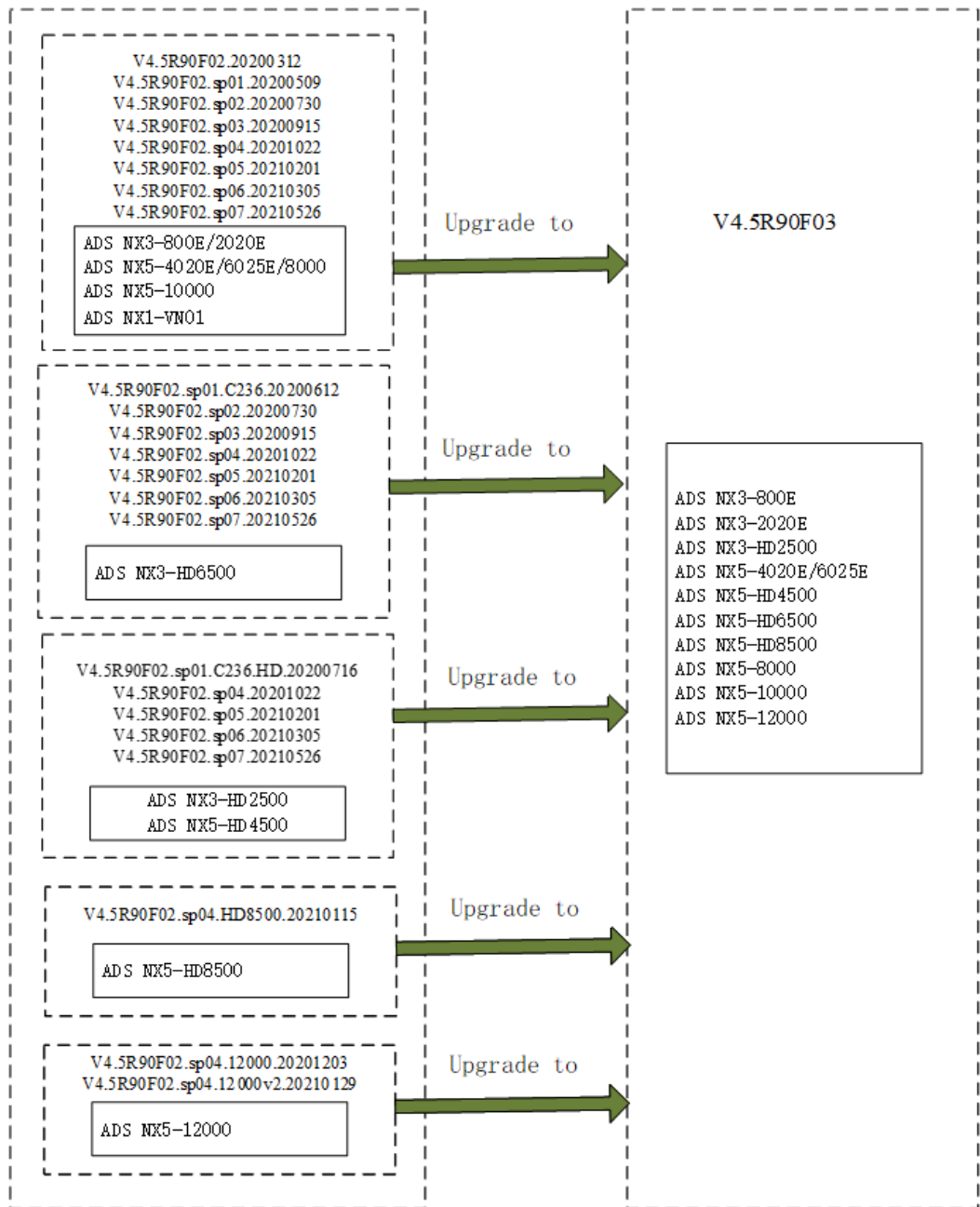
For ADS NX3-800E, NX3-2020E, NX5-4020E, NX5-6025E, NX5-8000, NX5-10000, and NX1-VN01, you need to first upgrade them to V4.5R90F02 or one of its SP versions (V4.5R90F02.20200312, V4.5R90F02.sp01.20200509, V4.5R90F02.sp02.20200730, V4.5R90F02.sp03.20200915, V4.5R90F02.sp04.20201022, V4.5R90F02.sp05.20210201, V4.5R90F02.sp06.20210305, and V4.5R90F02.sp07.20210526) before upgrading to V4.5R90F03.

For ADS NX5-HD6500, you can directly upgrade it from the current version (V4.5R90F02.sp01.C236.20200612, V4.5R90F02.sp01.20200509, V4.5R90F02.sp02.20200730, V4.5R90F02.sp03.20200915, V4.5R90F02.sp04.20201022, V4.5R90F02.sp05.20210201, V4.5R90F02.sp06.20210305, or V4.5R90F02.sp07.20210526) to V4.5R90F03.

For ADS NX3-HD2500 and NX5-HD4500, you can directly upgrade it from the current version (V4.5R90F02.sp01.C236.HD.20200716, V4.5R90F02.sp04.20201022, V4.5R90F02.sp05.20210201, V4.5R90F02.sp06.20210305, or V4.5R90F02.sp07.20210526) to V4.5R90F03.

For ADS NX3-HD8500, you can directly upgrade it from the current version (V4.5R90F02.sp04.HD8500.20210115) to V4.5R90F03.

For ADS NX5-12000, you can directly upgrade it from the current version (V4.5R90F02.sp04.12000.20201203 or V4.5R90F02.sp04.12000v2.20210129) to V4.5R90F03.



1.2 Function Changes in V4.5R90F03

1.2.1 New Functions

Function	Description
HTTP protection	The HTTP2-based DDoS protection function is added for the HTTPS protection policy.
TCP reflection attack protection	The SYN-ACK protection policy is added for protection against TCP reflection attacks.

DNS response protection	The DNS protection policy is added for protection for DNS responses.
Malformed HTTP packet protection	The invalid HTTP packet filtering rule is added as an anomalous packet filtering rule.
Rate limiting for fragments	The rate limiting action is added to TCP/UDP/ICMP fragment control policies.
Blacklists specific to protection groups	The blacklist module is restructured to support IP segment import. Blacklists targeting protection groups are added.
Default anti-DDoS policies replaced by the default protection group module	Default anti-DDoS policies are replaced by default protection group policies that are applicable to all protection objects other than custom protection groups.
Time sequence configurable for SYN time sequence check	The addition of the retransmission interval allows the SYN time sequence check to adapt to several operating systems.
VLAN-preferred injection	The VLAN-preferred injection function is added as an advanced option for injection routes.
Custom router ID allowed for BGP routes	Custom router IDs are allowed for BGP routes.
Contact information update	The contact phone numbers and email address are updated for the international customer service.
Configuration file import restriction	Configuration files, by default, cannot be imported across device models, versions, or running modes.
Addition of the Congo GMT+1 time zone	A time zone is added for Congo.
Increase in production groups concurrently learned by ADS	Protection groups that can be learned by ADS concurrently are increased to 15.
Group-specific Packet Fragmentation	ADS can fragment large packets injected back to the network

1.2.2 Optimized Functions in V4.5R90F03 After Upgrade from V4.5R90F02

The following table lists functions affected by upgrade from V4.5R90F02 to V4.5R90F03.

Function	V4.5R90F02	V4.5R90F03	Change
TCP reflection attack protection	Both SYN-ACK protection and ACK protection are implemented via ACK protection algorithms.	SYN-ACK protection is split from the ACK protection process.	A switch is added for SYN-ACK protection and several algorithms are added for protection enhancement.
Blacklists specific to protection groups	--	The blacklist module is restructured.	Blacklists can be added to target protection groups. Both IP addresses and IP addresses ranges can be added to the blacklists. The blacklists can be imported, exported, or searched.

Function	V4.5R90F02	V4.5R90F03	Change
Default anti-DDoS policies replaced by the default protection group module	--	The default anti-DDoS policy module is replaced by the default protection group module.	The default anti-DDoS policy module is replaced by the default protection group module to implement unified and flexible protection policy configurations.
Configuration file import restriction	Configuration files cannot be imported across device models or running modes.	Configuration files cannot be imported across device models running modes, or versions.	Configuration files, by default, can only be imported among devices of the same model that are of the same version and in the same operating mode.

1.3 Main Functions in V4.5R90F03

1.3.1 HTTP2 Protection

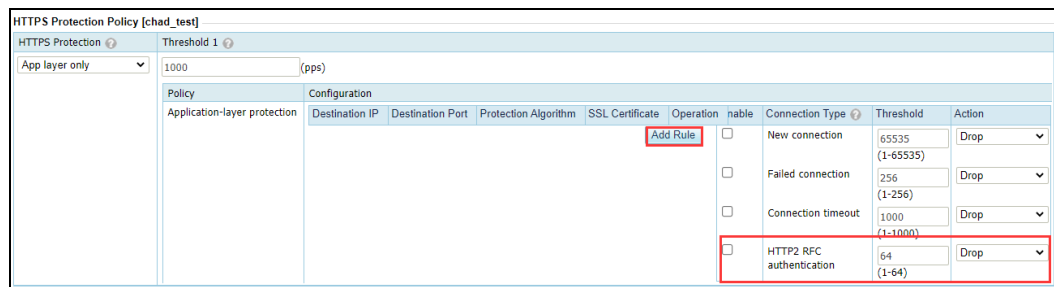
1. Function Description

For HTTPS protection, ADS establishes a TLS connection with a client in replace of the server, and then authenticates the client through the application-layer protocol HTTP. If the client properly responds to the HTTP packet from ADS, ADS deems this client reliable and will add it to the trust list so that it can directly communicate with the server.

In V4.5R90F03, the application-layer HTTPS protection function also supports HTTP2 so that users can choose to use HTTP or HTTP2 for client authentication. Also, the protocol can be determined through negotiations between ADS and the client. Meanwhile, when HTTP2 authentication is used, ADS authenticates the client's communications according to RFC7540 specifics and identifies and blocks noncompliant communications.

2. Configuration

Policy > Anti-DDoS > Protection Groups > Protection Policy > HTTPS Protection Policy



- If **HTTP2 RFC authentication** is selected, the system will authenticate HTTP2 communications. If login failures for an individual source IP address reach the specified threshold, the system will take the action as specified in the HTTP2 RFC authentication rule.
- You can click **Add Rule** to configure HTTPS protection rules. This function remains unchanged from the last version.

Destination IP	Destination Port	Protection Algorithm	SSL Certificate
		<input checked="" type="checkbox"/> HTTP algorithm 2-URL authentication	nsfocus
		<input type="checkbox"/> HTTP2 algorithm 0-HTTP2 frame protection	

- You can select the HTTP2 algorithm to enable the HTTP2 protection function. A rule can have both the HTTP and HTTP2 algorithms enabled.

3. Notes

- HTTP2 RFC authentication works only for rules with an HTTP2 protection algorithm enabled.
- If a rule has both HTTP and HTTP2 protection algorithms enabled, the actual application-layer protocol is determined through negotiations between ADS and the client. During protection, HTTP2 algorithms come before HTTP algorithms.

1.3.2 TCP Reflection Attack Protection

1. Function Description

The TCP protection policy can defend against ACK flood attacks and SYN-ACK flood attacks, but fails to work well for TCP reflection (SYN-ACK) attacks. With improved existing SYN-ACK protection algorithms and new ones, ADS V4.5R90F03 can effectively deal with TCP reflection attacks.

In addition, this version implements a series of optimizations for the ACK and SYN-ACK protection processes.

- SYN-ACK and ACK protection configurations are separated so that the SYN-ACK protection process is no longer bound by ACK protection algorithms.
- The SYN-ACK learning function is added to allow ADS, in non-protection state, to add certain legitimate IP addresses to the trust list through observation of behaviors of SYN-ACK packets.
- The SYN-ACK algorithm switch can be turned off. In this case, SYN-ACK packets are no longer handled by algorithms, but still need to be filtered through other policies.
- The reverse detection rate limitation function is added for both the SYN-ACK and ACK algorithms to prevent the algorithms from occupying excessive bandwidth resources.
- For the SYN-ACK control policy, the time sequence algorithm is optimized to provide a configurable retransmission interval.

2. Configuration

Policy > Protection Groups > Protection Policy > TCP Control Parameters.

TCP Control Parameters [th]	
Targeting	<input checked="" type="radio"/> Destination IP/Port <input type="radio"/> Destination IP
SYN Control	SYN Time Sequence Check <input checked="" type="radio"/> Yes <input type="radio"/> No
	Retransmission Interval <input type="text" value="22"/> (2750ms) ~ <input type="text" value="28"/> (3500ms)
	SYN Source Bandwidth Limit <input type="text" value="Disable"/> SYN Source IP Rate Limit <input type="text" value="0"/> (pps)
SYN-ACK Control	SYN-ACK Learning Mode <input type="radio"/> Yes <input checked="" type="radio"/> No
	Protection Algorithm <input type="text" value="Drop"/>
	Reverse Detection Rate <input type="radio"/> Yes <input checked="" type="radio"/> No <input type="text" value="32000"/> (pps)
ACK Control	ACK Learning Mode <input type="radio"/> Yes <input checked="" type="radio"/> No
	ACK Protection Algorithm <input type="text" value="Drop"/>
	Reverse Detection Rate <input type="radio"/> Yes <input checked="" type="radio"/> No <input type="text" value="32000"/> (pps)
	Retransmission Interval <input type="text" value="8"/> (1000ms) ~ <input type="text" value="24"/> (3000ms)
Other	RST Tx Rate <input type="text" value="100000"/> (pps)
	TCP Fragment Control <input type="text" value="Drop"/>

The SYN-ACK algorithm provides the following options:

- **Drop:** drops all SYN-ACK packets.
- **Close:** SYN-ACK packets will no longer be checked against the SYN-ACK protection algorithm, but still filtered by other protection policies.
- **Source authentication:** The basic SYN-ACK protection algorithm can defend against SYN-ACK flood attacks, but cannot effectively cope with TCP reflection attacks. This algorithm has minimal performance consumption.
- **Session check:** This algorithm can effectively deal with TCP reflection attacks. It has a better protection effect than the source authentication algorithm, but brings greater performance consumption.
- **ACK combined protection:** This algorithm must be used together with the ACK check algorithm. Such a combination delivers the best protection effect but causes greatest performance consumption.

The reverse detection rate limitation function is employed in both the ACK and SYN-ACK protection algorithms to restrict the rate of sending detection packets to the client, for the purpose of preventing the occupation of too much uplink bandwidth.

In addition, the check sequence used by the SYN-ACK algorithm can be adjusted. This configuration is unavailable on the web-based manager due to potential risks. For details, see the *NSFOCUS ADS V4.5R90F03 CLI Command Description* and *NSFOCUS ADS V4.5R90F03 Web API Description*.

3. Notes

- If the SYN-ACK protection algorithm is set to **ACK combined protection**, the ACK protection algorithm must be set to **ACK check**.
- It is advised not to change the retransmission interval of the SYN-ACK protection algorithm. If such change is required, you need to capture packets to determine the packet sending interval.

1.3.3 DNS Response Protection

1. Function Description

The DNS reply protection policy is added to V4.5R90F03 to make ADS more capable.

For DNS reply packets, ADS handles them by using two algorithms:

- **1-Default:** DNS reply packets are check against the UDP protection policy.
- **2-DNS retransmission:** The first DNS reply packet is dropped and the receiving timestamp of the packet is recorded. When receiving a resent DNS reply packet, ADS will check whether the real retransmission interval falls within a specified range. If yes, ADS allows the resent packet to pass through and determines whether to add the source IP address to the trust list according to the trust policy; if not, ADS will drop the packet. The DNS retransmission interval can be specified using a CLI command.

2. Configuration

Policy > Anti-DDoS > Protection Groups > a specific protection group > DNS Protection Policy > DNS Response Protection.

DNS Protection Policy[th]			
Protection Type	Enable	Parameter Configuration	
DNS Query Protection	<input checked="" type="radio"/> Yes <input type="radio"/> No	Protection Algorithm	2-TCP_BIT
		Reverse Detection Rate	32000 (pps)
DNS Response Protection	<input type="radio"/> Yes <input checked="" type="radio"/> No	Protection Algorithm	2-DNS retransmission
		Action	Accept+trust

3. Notes

- The retransmission interval (the unit is tick. Eight ticks equals 1 second) between a DNS reply packet and a DNS query packet can be in one of three ranges: (6,10), (11,21), and (35,45).
- The DNS reply retransmission authentication algorithm applies to common clients (web servers), but not applicable to recursive and authoritative DNS servers.

1.3.4 Malformed HTTP Packet Protection

1. Function Description

A malformed HTTP packet filtering rule is added to V4.5R90F03 so that ADS can deal with malformed HTTP packets according to the rule when detecting them.

Packets that meet the following conditions are deemed as malformed HTTP packets:

1. TCP-ACK packets with an HTTP port as the destination port.
2. For packets with an HTTP method, GET or POST, their payload length is greater than 20 bytes.
3. Packets can be parsed to obtain the HTTP method, URI, and HTTP version.
4. If the ASCII code value in an HTTP header is smaller than 32 and is not a space, carriage return, line feed, or tab, such HTTP packets are deemed malformed.

The malformed HTTP packet filtering rule contain three actions: **Disable**, **Enable**, and **Enable only in protection state**.

2. Configuration

Policy > Anti-DDoS > Protection Groups > a specific protection group > Anomalous Packet Filtering Rules > HTTP Filtering.

Anomalous Packet Filtering Rules [th]	
Invalid SYN Packet Filtering	Enable ▼
UDP Port 80 Filtering	Enable ▼
LAND Filtering	Enable ▼
HTTP Filtering	Disable ▼

3. Notes

HTTP Filtering can be set to **Enable only in protection state**, depending on the HTTP GET flood protection policy and HTTP POST flood protection policy.

1.3.5 Rate Limiting by Fragment Control Policies

1. Function Description

In earlier versions, TCP/UDP/ICMP fragment control policies contain two actions, **Drop** and **Accept**. In V4.5R90F03, these policies have an additional action, **Limit rate**, besides the existing two.

2. Configuration

Policy > Anti-DDoS > Protection Groups > a specific protection group > TCP Control Parameters > Other > TCP Fragment Control.

TCP Control Parameters [th]	
Targeting	<input checked="" type="radio"/> Destination IP/Port <input type="radio"/> Destination IP
SYN Control	SYN Time Sequence Check <input checked="" type="radio"/> Yes <input type="radio"/> No
	Retransmission Interval <input type="text" value="22"/> (2750ms) ~ <input type="text" value="28"/> (3500ms)
	SYN Source Bandwidth Limit <input type="text" value="Disable"/> SYN Source IP Rate Limit <input type="text" value="0"/>
SYN-ACK Control	SYN-ACK Learning Mode <input type="radio"/> Yes <input checked="" type="radio"/> No
	SYN-ACK Protection Algorithm <input type="text" value="Drop"/>
	Reverse Detection Rate <input type="radio"/> Yes <input checked="" type="radio"/> No <input type="text" value="32000"/> (pps)
ACK Control	ACK Learning Mode <input type="radio"/> Yes <input checked="" type="radio"/> No
	ACK Protection Algorithm <input type="text" value="Drop"/>
	Reverse Detection Rate <input type="radio"/> Yes <input checked="" type="radio"/> No <input type="text" value="32000"/> (pps)
	Retransmission Interval <input type="text" value="8"/> (1000ms) ~ <input type="text" value="24"/> (3000ms)
Other	RST Tx Rate <input type="text" value="100000"/> (pps)
	TCP Fragment Control <input type="text" value="Drop"/>

Policy > Anti-DDoS > Protection Groups > a specific protection group > UDP Protection Policy > UDP Fragment Control.

UDP Protection Policy[th]			
UDP Fragment Control	Drop		
Min UDP Packet Length	0	(Bytes)	
Max UDP Packet Length	65535	(Bytes)	
Traffic Control by Src IP+Src Port	<input type="radio"/> Yes <input checked="" type="radio"/> No	65535	(0-524280) <input checked="" type="radio"/> pps <input type="radio"/> bps
Traffic Control by Src IP	<input type="radio"/> Yes <input checked="" type="radio"/> No	3000000	(0-24000000) <input checked="" type="radio"/> pps <input type="radio"/> bps
Traffic Control by Dst IP+Dst Port	<input type="radio"/> Yes <input checked="" type="radio"/> No	65535	(0-524280) <input checked="" type="radio"/> pps <input type="radio"/> bps
Traffic Control by Dst IP+Src Port	<input type="radio"/> Yes <input checked="" type="radio"/> No	65535	(0-524280) <input checked="" type="radio"/> pps <input type="radio"/> bps
Traffic Control by Dst IP	<input type="radio"/> Yes <input checked="" type="radio"/> No	3000000	(0-24000000) <input checked="" type="radio"/> pps <input type="radio"/> bps

Policy > Anti-DDoS > Protection Groups > a specific protection group > ICMP Protection Policy > ICMP Fragment Control.

ICMP Protection Policy [th]			
ICMP Fragment Control	Drop		
Traffic Control by Src IP	<input type="radio"/> Yes <input checked="" type="radio"/> No	3000000	(1-24000000)(pps)
Traffic Control by Dst IP	<input type="radio"/> Yes <input checked="" type="radio"/> No	3000000	(1-24000000)(pps)

3. Notes

For fragment control policies, the default rate threshold is 100 pps.

1.3.6 Blacklists Targeting Protection Groups

1. Function Description

In earlier versions, the global blacklist does not treat protection groups in a differentiated way, nor support IP address ranges. In V4.5R90F03, blacklists are available to target production groups and accept IP address ranges.

- Both manual blacklist entries can be exported in a quick or detailed way.
- Manual blacklist entries can be added one by one or imported in bulk. During entry addition or import, you can set **Auto Block** to **Temporary** or **Permanent**.
- For blacklist entries added manually, the system calculates when the block period expires based on the current system time and the specified block period. Blacklist entries persist across the reboots.
- Manual blacklist entries allow IPv4 and IPv6 addresses and address ranges.
- Results of the last blacklist import can be viewed, including **Start Time**, **End Time**, **Progress**, **Total Entries**, **Successful Imports**, and **Failed Imports**.
- Desired entries can be located through blacklist retrieval based on conditions such as the IP address, IP address range, and block reason.

2. Configuration

Policy > Anti-DDoS > Protection Groups > a specific protection group > Blacklist.

Protection Groups									
Search By Group Name Or IP		Running Mode		All		Filter			
						First		1/1 pages.Go to	
<input type="checkbox"/> Select All	Group Name	Running Mode	IP List	Protection Policy	Access Policy	URL Rule	Auto-learning	Description	Delete
<input type="checkbox"/>	default_protection_group	Protect			Blacklist		-	all_users	
<input type="checkbox"/>	th	Protect			Blacklist		Not started	x	
<input type="checkbox"/>	chad_test	Protect			Blacklist		Not started	chad_test111	
<input type="checkbox"/>	unselect	Protect			Blacklist		Not started	chad_test	
<input type="checkbox"/>	test	Protect			Blacklist		Not started	chad_test	
<input type="checkbox"/>	select	Protect			Blacklist		Not started	chad_test	

Blacklist[th]	
Item	Value
Enable	Yes
Configuration Items	
Item	Value
Auto Block	Temporary: 120(minutes)
Proxy Monitoring	No

3. Notes

- If the entire IP list or the retrieved IP list is too long to be fully displayed, entries will be displayed in descending order of time and excessive ones will be omitted. IP addresses or address ranges, if added at the same time, will be displayed in ascending order.
- Before import, the blacklist must be enabled. The imported blacklist entries take effect immediately, with **Block Reason as Manual**. Imported entries are appended to the original blacklist and conflicting entries cannot be imported.
- If the upper limit of the blacklist is reached, the system displays the message "You have exceeded the maximum number of entries allowed in a blacklist." upon the addition of a new IP address.
- The global blacklist works for all protection targets, while group-specific blacklists only act on the protection groups.
- If you configure the blacklist for a protection group when the blacklist is disabled, the configuration still succeeds, but the system displays the message "The setting will take effect only after you enable the blacklist."
- During the protection process, blacklist entries are matched against packets in the following sequence: global manual entries -> global dynamic entries -> group-specific manual entries -> group-specific dynamic entries.

1.3.7 Default Protection Group Replacing Default Anti-DDoS Policies

1. Function Description

ADS V4.5R90F03 uses the default protection group to replace default anti-DDoS policies to manage anti-DDoS policies in a more unified way, resulting in enhanced ease of use (EOU).

2. Configuration

Policy > Anti-DDoS > Protection Groups > default_protection_group.

Select All	Group Name	Running Mode	IP List	Protection Policy	Access Policy	URL Rule	Auto-learning	Description	Delete
<input type="checkbox"/>	default_protection_group	Protect			Blacklist		-	all_users	
<input type="checkbox"/>	th	Protect			Blacklist		Not started	x	
<input type="checkbox"/>	chad_test	Protect			Blacklist		Not started	chad_test111	
<input type="checkbox"/>	unselect	Protect			Blacklist		Not started	chad_test	
<input type="checkbox"/>	test	Protect			Blacklist		Not started	chad_test	
<input type="checkbox"/>	select	Protect			Blacklist		Not started	chad_test	

3. Notes

- The default protection group is **default_protection_group**, for which the protected IP addresses are **0.0.0.0-0.0.0.0** and **::-::** and the description is **all_users**. This protection group is shown at the top of the table and cannot be deleted.
- The default protection group has the same settings as custom protection groups, except that it is in protection mode and does not support auto-learning and group diversion.
- Modules specific to protection groups, including the traffic trend, attack traffic trend, packet capture, top 10 destination IP addresses by traffic, and top 5 URLs, all involve the default protection group.
- For protection group retrieval by IP address, custom protection groups precede default ones.

1.3.8 Time Sequence Configurable for SYN Time Sequence Check

1. Function Description

The V2.4R90F03 version supports the SYN time sequence check function. By dropping the first SYN packet sent from the client and waiting for the packet to be retransmitted, ADS will preliminarily determine the reliability of the client based on the retransmission interval.

In versions earlier, ADS provides the retransmission interval range. In V2.4R90F03, the device allows users to specify a time frame.

2. Configuration

Policy > Protection Groups > Protection Policy > TCP Control Parameters.

TCP Control Parameters [th]	
Targeting	<input checked="" type="radio"/> Destination IP/Port <input type="radio"/> Destination IP
SYN Control	SYN Time Sequence Check <input checked="" type="radio"/> Yes <input type="radio"/> No Retransmission Interval <input type="text" value="22"/> (2750ms) ~ (3500ms) SYN Source Bandwidth Limit <input type="text" value="Disable"/> <input type="text" value="0"/> (pps)

3. Notes

For the **Retransmission Interval** parameter, the default value is recommended. If a custom value is indeed required, you are advised to analyze the client's behavior through packet capture before making any changes.

1.3.9 VLAN-Preferred Injection

1. Function Description

ADS allows users to configure multiple equal-cost routes for a destination IP address. Usually, packets are sent to this destination IP address along these routes for load balancing.

This function, to a certain extent, determines the routing of packets. If packets with a VLAN match multiple equal-cost routes, ADS prefers the route whose egress VLAN is identical with the VLAN of packets. If such routes do not exist, packets will be transmitted along the equal-cost routes in load balancing mode.

2. Configuration

Diversion & Injection > Traffic Injection > Injection Routes > Advanced Config.

Injection Routes	
Advanced Options	
Item	Value
Enable Injection MPLS Label Learning	No
Enable Longest Route Match	No
Enable Route Cache	No
Diversion-Interface-Preferred Injection	No
VLAN-Preferred Injection	No
Advanced Functions	
Item	Value
Injection Route Redundancy	Disable
Injection Connectivity Check	Disable
LDP Neighbor Status Check	Disable

3. Notes

- If this function is used, ADS will match packets against routes according to the longest subnet mask matching principle or the route addition sequence. Routes are selected by VLAN only when multiple matching equal-cost routes are found.
- This function may conflict with diversion-interface-preferred injection. For this reason, when both injection functions are enabled, the diversion-interface-preferred injection prevails.

1.3.10 Custom Router ID Allowed for BGP Routes

1. Function Description

In V4.5R90F03, the **Router-id** parameter is added to the BGP route configuration.

2. Configuration

Diversion & Injection > Diversion Route > BGP Route > Router-id

Item	Value
Name	<input type="text"/>
Type	Diversion
Local AS	<input type="text"/>
Local Port	179
Keepalive	60
Holdtime	180
Metric	100
Bind IP	80.91.35.1
Router-id	80.91.35.1
Management Port(3000~4000)	<input type="text"/>
No-advertise	<input checked="" type="radio"/> Yes <input type="radio"/> No
No-export	<input checked="" type="radio"/> Yes <input type="radio"/> No
Community	600:650 (*The default value is 600:650.)

OK Cancel

3. Notes

- For IPv4 BGP routes, **Router-id** is set to an IPv4 address.
- For IPv6 BGP routes, **Router-id** is set to **127.0.0.1**.
- System upgrade will cause BGP routes get disconnected. Therefore, you are advised to reconfigure BGP routes after system upgrade.

1.3.11 Configuration File Import Restriction

1. Function Description

Earlier versions allow configuration files to be imported across versions of devices of the same model that are in the same running mode. V4.5R90F03 places restrictions on configuration file import. Specifically, configuration files, by default can only be imported among devices of the same model that are of the same version and in the same operating mode.

2. Configuration

None.

3. Notes

None.

1.3.12 Addition of the Congo GMT+1 Time Zone

1. Function Description

V4.5R90F03 adds the Congo GMT+1 time zone.

2. Configuration

System > Local Settings > Time Zone > set the time zone.

Basic Settings	
Item	Value
Device ID	ADS
	IPv4 Configuration IPv6 Configuration
IP Address	10.66.250.250
Netmask	255.255.240.0
Gateway IP	10.66.250.254
	Primary Server Secondary Server
DNS Server	192.168.1.1
Time Server	
Web Server Port	443
System Date	2021-09-23 17:21
System ID	CD41-D230-41F2-D850
Forwarding Mode	No
NSFOCUS Cloud switch	Off
System Uptime	
Uptime	8:05 5 days
<input type="button" value="System Check"/> <input type="button" value="Restart Web Server"/> <input type="button" value="Restart Device"/> <input type="button" value="Edit"/>	
Region	
Region	EMEA
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	
Time Zone	
Time Zone	(GMT+01:00), Congo
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

3. Notes

None.

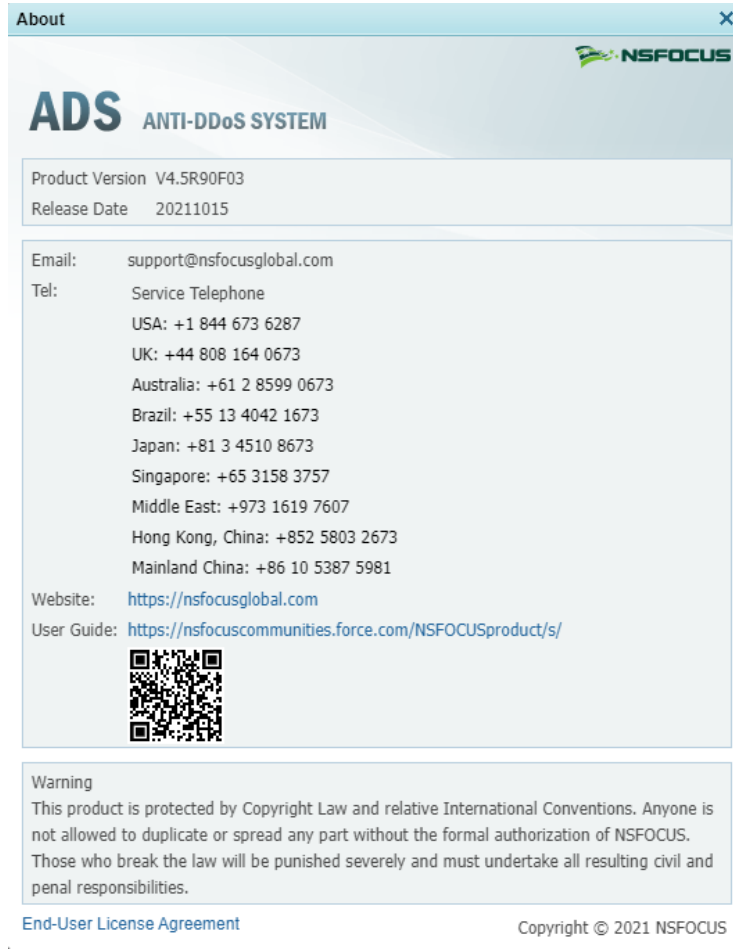
1.3.13 Contact Information Update

1. Function Description

This version updates the customer service hours in China as well as the customer service hotlines in China and other countries.

2. Configuration

About page



3. Notes

None.

1.3.14 Increase in Production Groups Concurrently Learned by ADS

1. Function Description

ADS can learn traffic of protection groups. Specifically, ADS observes the composition of traffic arriving at protection groups and analyzes and learns the thresholds of some major algorithms. In earlier versions, at most 10 protection groups can be selected for auto-learning.

In V4.5R90F03, a maximum of 15 protection groups can be learned at the same time.

2. Configuration

Policy > Protection Groups > Auto-learning

Select All	Group Name	Running Mode	IP List	Protection Policy	Access Policy	URL Rule	Auto-learning	Description	Delete
<input type="checkbox"/>	default_protection_group	Protect			Blacklist		-	all_users	
<input type="checkbox"/>	F203E29D89@300D9D0CC7	Protect			Blacklist		Not started	a	
<input type="checkbox"/>	182487DAD4@4793F7092C	Protect			Blacklist		Not started	g	
<input type="checkbox"/>	th	Protect			Blacklist		Not started	x	

3. Notes

The specification of this function refers to the number of protection groups that can be learned by ADS concurrently. Only protection groups engaged in ongoing learning are counted, while those in the learning completion state are excluded.

1.3.15 Group-specific Packet Fragmentation

1. Function Description

ADS can fragment large packets injected back to the network and allows users to configure related global and group-specific policies.

2. Configuration

This function is available only in the CLI window, implemented with **fragment** commands.

3. Notes

For a group with no fragmentation policy configured, the global fragmentation policy will apply.

2 Compatibility with NTA Versions

ADS V4.5R90F03 can collaborate with NTA V4.5R90F03 and both support IPv4 and IPv6 addresses.

3 Supported Browsers

Internet Explorer 9, 10, and 11

Chrome

Firefox

Version Upgrade

- Upgrade to V4.5R90F03 from V4.5R90F02.20200312, V4.5R90F02.sp01.20200509, V4.5R90F02.sp01.C236.20200612, V4.5R90F02.sp01.C236.HD.20200716, V4.5R90F02.sp02.20200730, V4.5R90F02.sp03.20200915, V4.5R90F02.sp04.20201022, V4.5R90F02.sp04.HD8500.20210115, V4.5R90F02.sp04.12000.20201203, V4.5R90F02.sp04.12000v2.20210129, V4.5R90F02.sp05.20210201, V4.5R90F02.sp06.20210305, and V4.5R90F02.sp07.20210526

V4.5R90F03 is also applicable to the following device models:

ADS NX3-800E, ADS NX3-2020E, ADS NX5-4020E, ADS NX5-6025E, ADS NX3-HD2500, ADS NX5-HD4500, ADS NX5-HD6500, ADS NX5-HD8500, ADS NX5-8000, ADS NX5-10000, ADS NX5-12000, ADS NX1-VN01

The upgrade to V4.5R90F03 must be completed in strict accordance with the following procedure:

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

Step 2: Apply the upgrade package, **update_ADS_x86_V4.5R90F03_20211203.zip** (MD5: 7BE246439EC520B573BA9F2ABF847413), on the source version. If the upgrade succeeds, restart the device.

Step 3: Verify that **System Version** is **V4.5R90F03** in the status bar of the web-based manager.

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

2 Rollback to V4.5R90F02 or V4.5R90F02 .sp0x From V4.5R90F03

V4.5R90F03 is also applicable to the following device models:

ADS NX3-800E, ADS NX3-2020E, ADS NX5-4020E, ADS NX5-6025E, ADS NX3-HD2500, ADS NX5-HD4500, ADS NX5-HD6500, ADS NX5-HD8500, ADS NX5-8000, ADS NX5-10000, ADS NX5-12000, ADS NX1-VN01

Rollback Method:

To roll back the version, run the **update rollback** command in the CLI window. If the rollback succeeds, the device automatically restarts. After the restart, the device rolls back to the previous version.