Release Notes

Basic Information

Product Model	• NX3-200E/600E/800E • NX3-2010/2020/2020E • NX5-4020/4020E • NX5-6025/6025E • NX3-HD2500/NX5-HD4500/NX5-HD6500 • NX5-8000 • NX5-10000
Software Version	V4.5R90F02
Upgrade File	update_ADS_x86_V4.5R90F02_20200312.zip MD5 value: FBFCB5B7A7E41DFAEFBD61B1DAC4A47E
Release Date	2020-03-12
How to Obtain	Contact NSFOCUS technical support.

Version Mapping

Source Software Version	V4.5R90F02
Product Model	• NSF1100-1 • NSF1100-3 • NSF2800-2 • NSF2800-6 • NSF3600-4 • NSP-7224B • HTCA-6U
Network Traffic Analyzer (NTA) Version	V4.5R90F02
Management Platform Version	ADS M V4.5R90F02
Client	N/A
Other System or Tool	N/A
Documentation	NSFOCUS ADS User Guide (V4.5R90F02)

Changes of Functions in V4.5R90F02

1.1 Supported Models

- ADS NX3-200E/600E/800E
- ADS NX3-2010/2020/2020E
- ADS NX5-4020/4020E
- ADS NX5-6025/6025E
- ADS NX5-8000
- ADS NX5-10000
- ADS NX3-HD2500/NX5-HD4500/NX5-HD6500

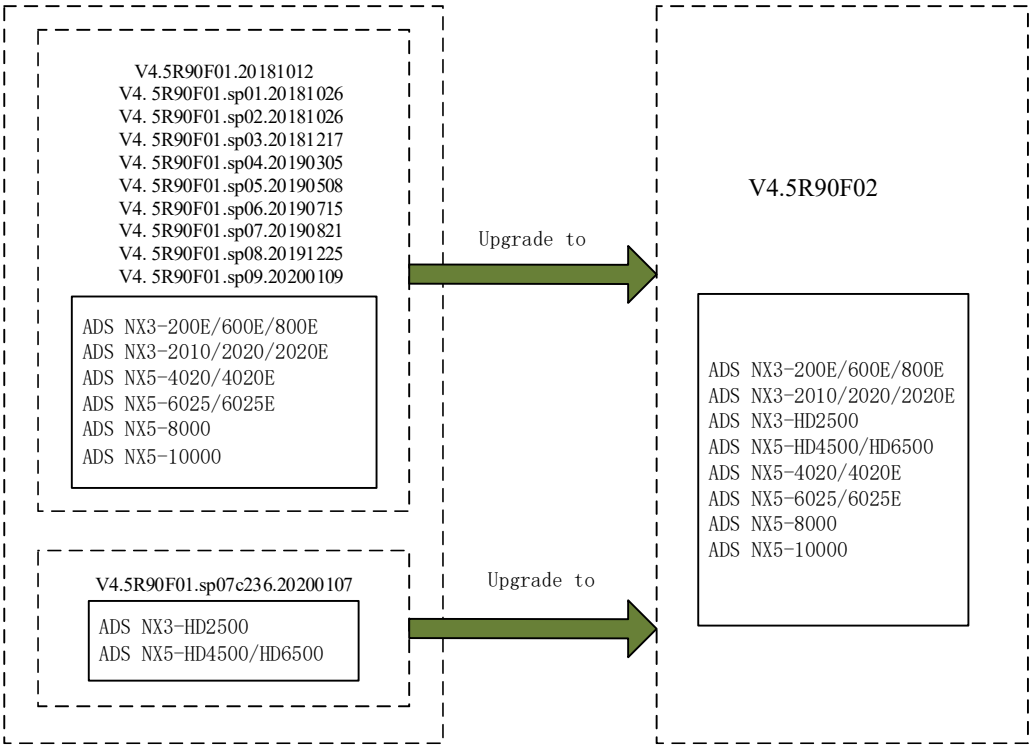
1.2 Support for Hardware Platforms

V4.5R90F02 inherits the uniform platform support feature from V4.5R90F01. In other words, a software version supports all hardware platforms.

For ADS NX3-200E/600E/800E, NX3-2010/2020/2020E, NX5-4020/4020E, NX5-6025/6025E, NX5-8000, and NX5-10000, you need to first upgrade them to V4.5R90F01 or

one of its SP versions (V4.5R90F01.20181012, V4.5R90F01.sp01.20181026, V4.5R90F01.sp02.20181026, V4.5R90F01.sp03.20181217, V4.5R90F01.sp04.20190305, V4.5R90F01.sp05.20190508, V4.5R90F01.sp06.20190715, V4.5R90F01.sp07.20190821, V4.5R90F01.sp08.20191225, or V4.5R90F01.sp09.20200109) before upgrading to V4.5R90F02.

For ADS NX3-HD2500/NX5-HD4500/NX5-HD6500, you can directly upgrade them from the current version (V4.5R90F01.sp07c236.20200107) to V4.5R90F02.



1.3 Function Changes in V4.5R90F02

1.3.1 New Functions

Function	Description
URL-specific protection	When configuring an HTTP protection policy for a group, users can select **Destination IP/Port** or **Destination IP/Port/URL** as the protection object.
Protection specific to mobile apps	In group-specific HTTP protection, HTTP GET protection is divided into unified protection and precision protection. The latter means that ADS will use different protection algorithms for PC-initiated and app-initiated traffic.
Real source IP filtering	Users can choose whether to implement blacklist/whitelist filtering for real source IP addresses indicated in the HTTP packet header.
Display of top 5 URLs by traffic	Users can choose to display top 5 URLs by traffic on the **Real-Time Monitoring** page of the web-based manager by running some CLI commands.

Display of group-specific traffic information	Users can specify a group to view its traffic information from various dimensions on the **Real-Time Monitoring** page of the web-based manager.
Policy statistics	In the attack log, the triggered policy of each event is listed and statistics of traffic dropped according to the policy are provided.
Cloud signaling	ADS can collaborate with the cloud cleaning center for protection against high-volume DDoS attacks.
ADS NX5-10000 supporting more management devices	ADS NX5-10000 supports up to 20 management devices.
Display of manual packet capture information and generation of policies accordingly	Users can view detailed information of packets captured in manually initiated tasks and further generate various protection policies.
Per-packet load balancing mode configurable via CLI commands	The per-packet load balancing mode is added and configurable via CLI commands for load sharing between injection interfaces.
New service interface information for the SNMP agent	OIDs of service interfaces can be obtained.
Anomalous packet filtering	Users can enable or disable filtering of invalid SYN packets, LAND packets, and/or packets destined for UDP port 80.
New commands in the console user interface to enable/disable the web service	Commands are provided in the console user interface to enable/disable the web service.
GeoIP library updated	The GeoIP library used by ADS is updated.
Destination IP addresses provided in the blacklist	Destination IP addresses targeted by source IP addresses blacklisted according to protection algorithms are displayed in the blacklist.
Reflection attack protection expanded	Two built-in rules are added for protection against CLDAP and MS SQL reflection attacks.
Port configurable for management by ADS M	Users can configure ADS to send data to a TCP port specified for ADS M.
Custom access user role added on the web-based manager	The custom access user's permissions for access to web pages depend on **admin**'s assignment.
Display of modules covered by the current license on the web-based manager	The license information includes authorized modules.
Support models change	Do not support the upgrade of listed models: ADS NX3-2010，ADS NX3-2020，ADS NX5-4020，ADS NX5-6025，ADS NX3-200E，ADS NX3-600E

1.3.2 Modified Functions

The following table lists functions modified in V4.5R90F02.

Function	V4.5R90F01	V4.5R90F02	Change Description
Top 10 destination IP addresses	Top 10 destination IP addresses are listed by attack traffic.	Top 10 destination IP addresses are listed by inbound traffic.	The statistical dimension changes to let users find out more about IP addresses receiving the most traffic.
Attack log display	The attack log provides the attack type and signature.	The attack log provides the attack type and protection policy.	Users can easily know which policy is triggered by an event. When parsing the attack log uploaded by ADS, third-party management platforms should be adapted to this change, providing descriptions about policies instead of attack signatures.
GeoIP rules	--	The GeoIP library is updated.	The GeoIP library contains more accurate information and adds/deletes a few countries/regions.
Invalid SYN packet alert switch	Users can control whether to display messages concerning invalid SYN packets in the attack log.	This function is removed.	The invalid SYN packet alert switch is removed in the new version. Instead, invalid SYN packet filtering is added and included in anomalous packet filtering rules. ADS will filter out invalid SYN packets and log related events only when this is enabled. By default, this function is enabled.

1.4 Main Functions in V4.5R90F02

1.4.1 URL-Specific Protection

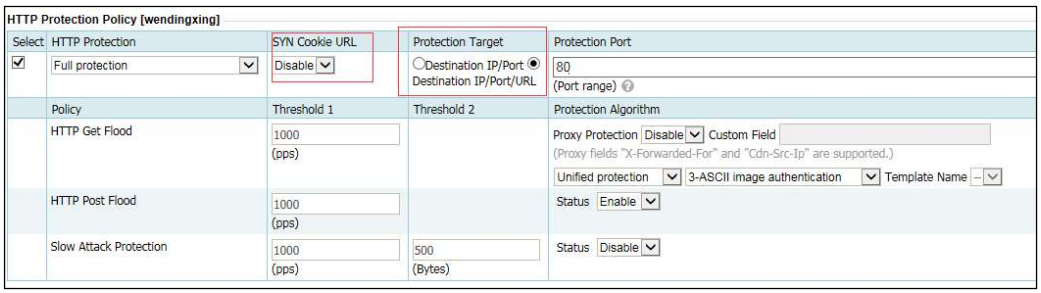
Function Description

A web server may provide many types of services, each of which is accessible via one or more URLs. In previous versions, users can protect their web servers by specifying destination IP addresses and destination ports as protection objects. In this case, when an attacker initiates a targeted attack on a limited range of URLs, ADS will still implement all-round protection for the web server.

In V4.5R90F02, **Destination IP/Port/URL** is added as a new option of the protection object. When this option is selected, ADS can implement protection only for the attacked URLs, thus reducing the consumption of its own resources and the impact on the customer's other services. This will ultimately improve the user experience.

Configuration

Policies > Protection Groups > *group name* > HTTP Protection Policy



Notes

- When **Destination IP/Port/URL** is selected, SYN cookie URL protection is automatically disabled.
- This function can be configured only in group-specific policies.

1.4.2 Protection Specific to Mobile Apps

Function Description

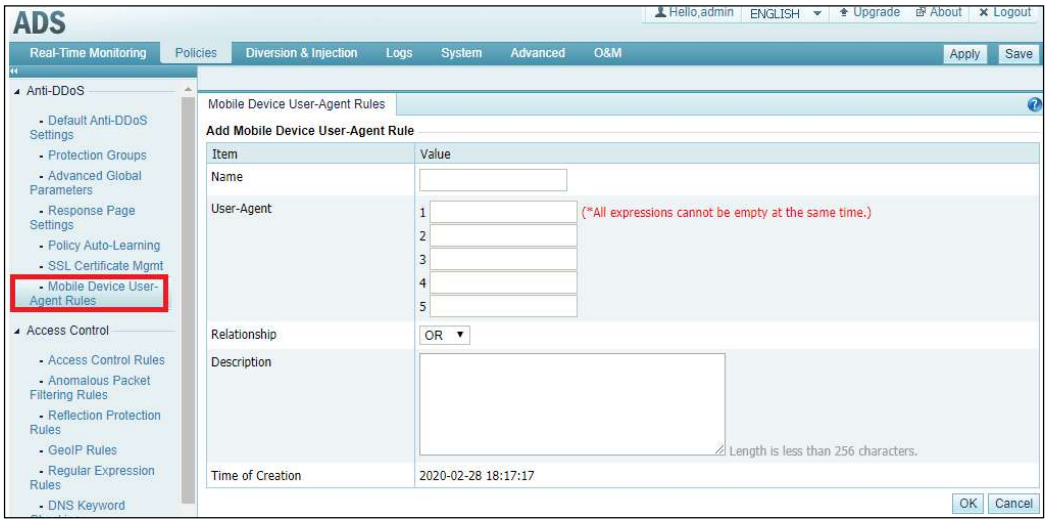
Currently, mobile apps usually do not use browser frameworks, but use some simplified underlying databases to access web servers. As mobile apps cannot well support network protocols, it is almost impossible to configure an appropriate HTTP protection policy for traffic initiated from these apps.

Considering the difference between PC browsers and mobile apps, the new version adds a function of identifying mobile apps via the user-agent field in packets so that users can choose to use different HTTP protections for PC-initiated and app-initiated traffic. This will improve the effect of HTTP protection policies for mobile apps.

Configuration

User-Agent Rule

Policies > Anti-DDoS > Mobile Device User-Agent Rules



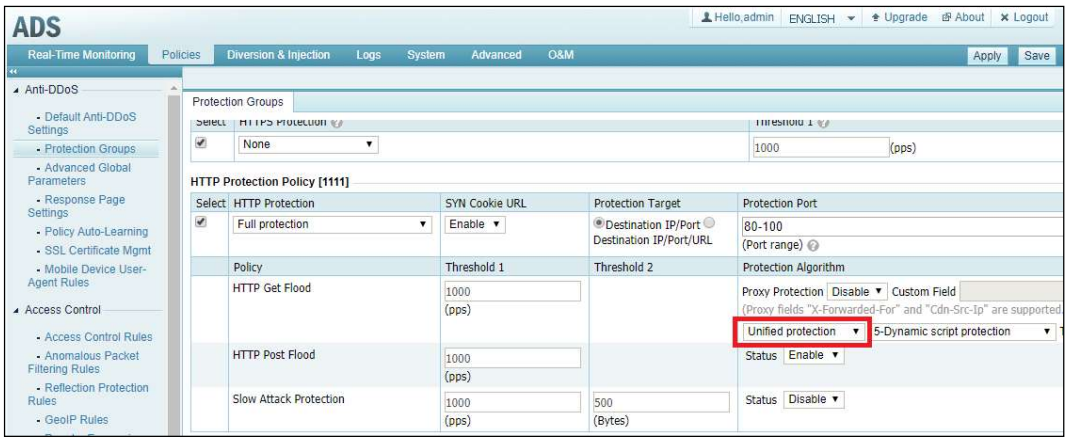
- Users can create or edit user-agent rules. A maximum of 32 such rules (including two default rules) can be configured.
- For each user-agent rule, one to five user-agent strings should be configured, with each containing a maximum of 100 characters.
- The relationship between these strings can be either of the following:
  - **AND**: indicates that packets whose user-agent field contains all strings typed here are deemed to be from mobile devices.
  - **OR**: indicates that packets whose user-agent field contains any of the strings typed here are deemed to be from mobile devices.

The system has two built-in user-agent rules, which can be edited, but cannot be deleted.

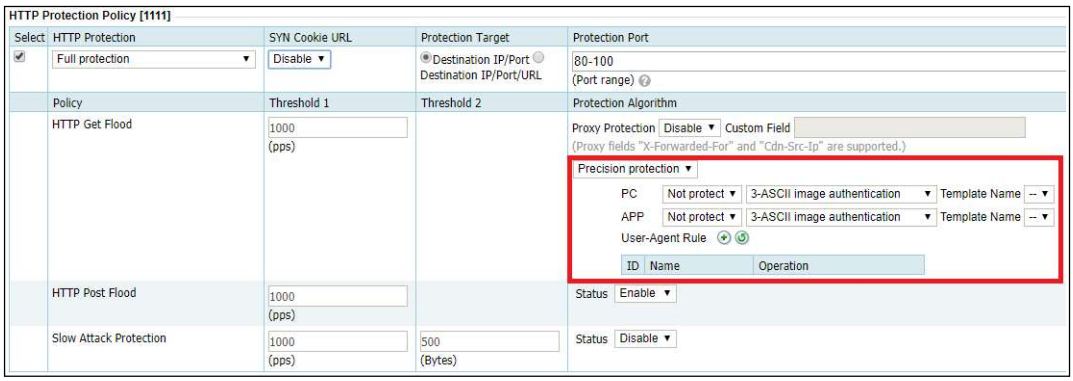
Group-Specific HTTP Protection Policy

Policies > Protection Groups > *group name* > HTTP Protection Policy

When **Unified protection** is selected, the configuration logic is the same as that in previous versions.



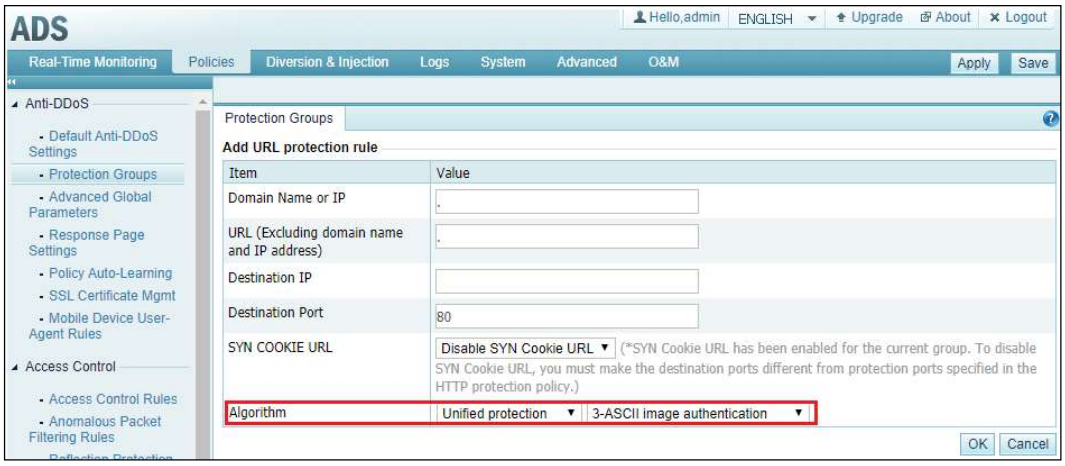
When **Precision protection** is selected:

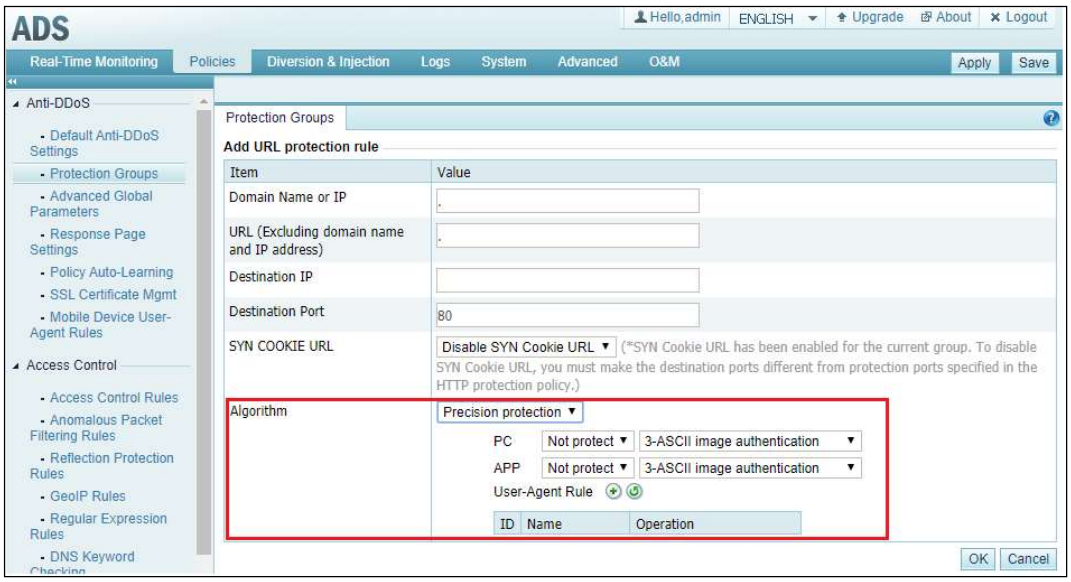


- One to five user-agent rules should be referenced.
- Packets matching any of the user-agent rules referenced here are deemed to be from mobile apps and will be checked against the app protection policy.
- Packets not matching any of the user-agent rules referenced here are deemed to be from PCs and will be checked against the PC protection policy.

Group-Specific URL Rule

Policies > Protection Groups > *group name* > URL Rule





The configuration logic of URL rules is the same as that of precision protection rules in the group-specific HTTP protection policy.

Notes

- When precision protection is enabled, if **Not protect** is selected for **PC** or **APP**, SYN cookie URL protection will be automatically disabled.
- This function can be configured only in group-specific policies.

1.4.3 Real Source IP Filtering

Function Description

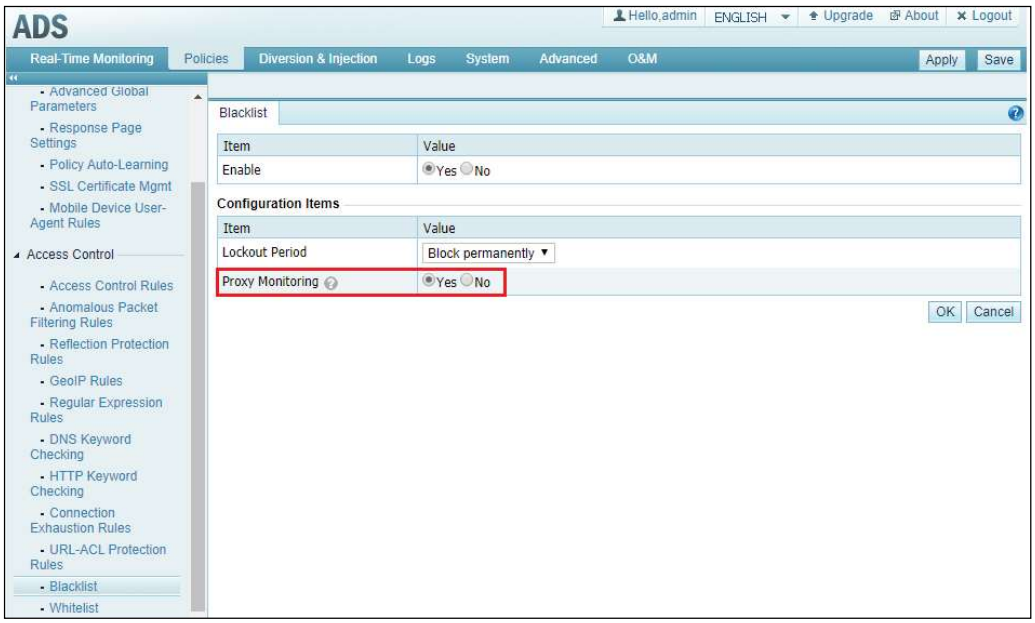
When a client accesses the web server via a proxy server, which can be a common proxy server, content delivery network (CDN), load balancer, or SSL offloading device, the IP header of such request packets does not indicate the client's IP address, but the IP address of the proxy server. Filtering packets based on IP addresses of proxy servers may lead ADS to mistakenly drop legitimate traffic or allow attack traffic to pass through.

To enhance protection against clients, a new function is added in this new version to filter packets based on clients' real source IP addresses that are extracted from HTTP packets. Specifically, this can be implemented by blacklisting/whitelisting of real source IP addresses and by rate limiting for HTTP GET packets. In this way, ADS's protection in the scenario that involves proxy servers is optimized.

Configuration

Blacklist Configuration

Policies > Access Control > Blacklist

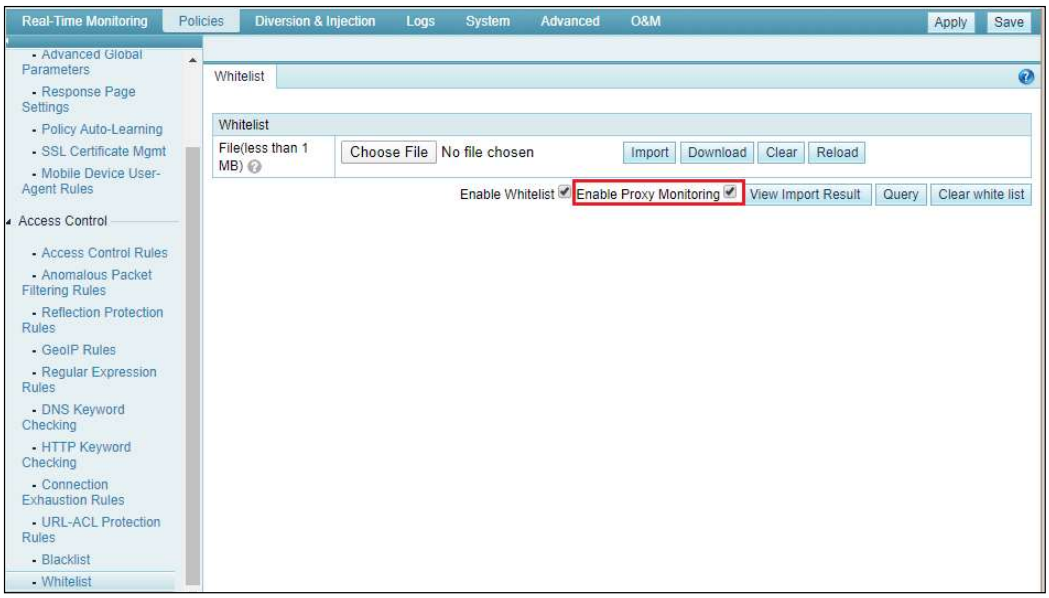


When **Proxy Monitoring** is set to **Yes**, ADS will parse HTTP packets to extract real source IP addresses before matching these addresses against the blacklist. Once finding a match, ADS will drop related packets.

Proxy monitoring is disabled by default.

Whitelist Configuration

Policies > Access Control > Whitelist



When the **Enable Proxy Monitoring** check box is selected, ADS will parse HTTP packets to extract real source IP addresses before matching these addresses against the whitelist. Once finding a match, ADS will pass related packets along.

Proxy monitoring is disabled by default.

Notes

- After the IP behavior control policy is enabled for an IP address, for clients intending to access this IP address, if they have passed ADS's proxy monitoring checks, their subsequent packets will be subject to GET packet rate limiting.
- For packets dropped according to proxy monitoring policies and because of real source IP filtering via the blacklist, source IP addresses displayed in the attack log are the real source IP addresses of clients.
- To extract real source IP addresses, ADS needs to parse HTTP packets, which is a time-consuming job. If protecting against real source IP addresses is not a required function, it is recommended that proxy monitoring of the blacklist/whitelist be disabled.

1.4.4 Real-Time Monitoring Page Optimized on the Web-based Manager

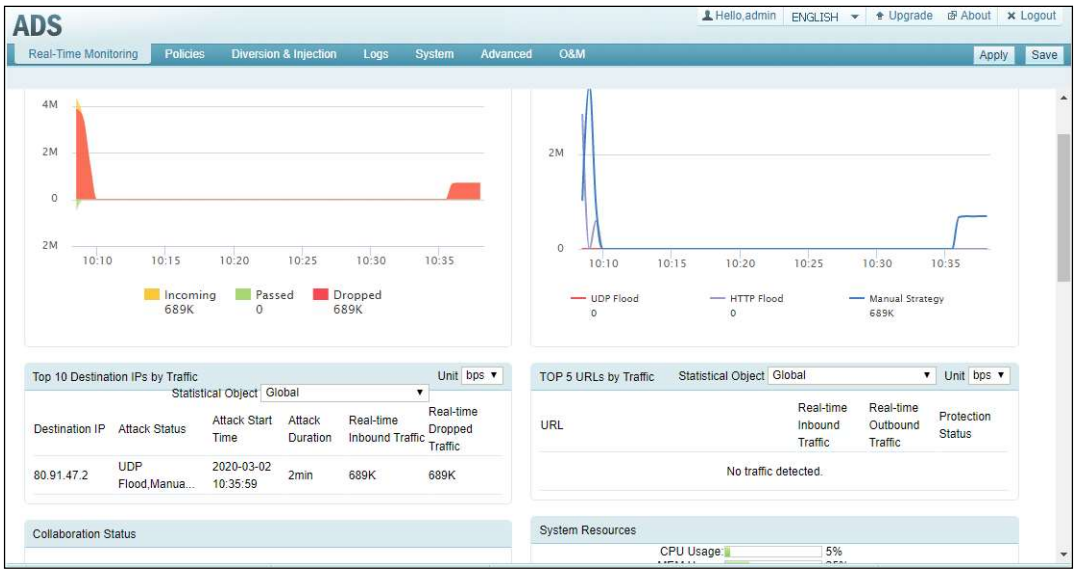
Function Description

Traffic statistics displayed on the **Real-Time Monitoring** page of the web-based manager have the following changes:

- ADS can display top 5 URLs by traffic, letting users learn in real time which web server receives the most traffic.
- ADS changes from display of top 10 destination IP addresses by attack traffic to that of top 10 destination IP addresses by inbound traffic, letting users know in real time not only attack information but also normal traffic in the case of no attack.
- All traffic statistics, no matter what type, can be displayed for a specific group, thus providing fine-grained information for real-time protections.

Involved Page

Real-Time Monitoring



The **Real-Time Monitoring** page displays more information:

- **Traffic Trend**: displays trends of traffic received (inbound), transmitted (passed), and dropped by ADS globally or for a specific group in the last 30 minutes.
- **Attack Traffic**: displays various types of attack traffic dropped by ADS globally or for a specific group in the last 30 minutes.
- **Top 10 Destination IPs by Traffic**: lists top 10 destination IP addresses with the largest inbound traffic in the last 30 seconds.
  - **Attack Status**: displayed as **--** if the current destination IP address is not under ADS's protection. If it is under ADS's protection, attack types detected in the last 30 seconds are displayed. When they are partially displayed, pointing to attack type characters displays all attack types.
  - **Attack Start Time**: time when the destination IP address was first attacked.
  - **Attack Duration**: difference between the current time and the attack start time.
  - **Real-time Inbound Traffic**: average incoming traffic of the destination IP address in the last 30 seconds.
  - **Real-time Dropped Traffic**: average traffic destined for the destination IP address dropped by ADS in the last 30 seconds.
- **Top 5 URLs by Traffic**: displays top 10 HTTP URLs with the most inbound traffic in the last 30 seconds. This panel is hidden by default. To display such information, users can run the **trafficstat set http_url_stat 1** command in the CLI window.
  - **URL**: HTTP URL, with up to 100 characters displayed.
  - **Real-time Inbound Traffic**: average inbound traffic of the URL in the last 30 seconds.
  - **Real-time Outbound Traffic**: average traffic passed by ADS on toward the URL in the last 30 seconds.
  - **Protection Status**: displayed as "Under protection" if some of the traffic is dropped by ADS; otherwise, "No cleaning" is displayed.

Notes

- The system dynamically adapts the sampling rate to the traffic volume, so minor errors may exist.
- On ADS NX3-200E/600E, NX3-2010/2020, NX5-4020, and NX5-6025, traffic statistics specific to a group and URL-related traffic statistics are unavailable.

1.4.5 Policy Statistics

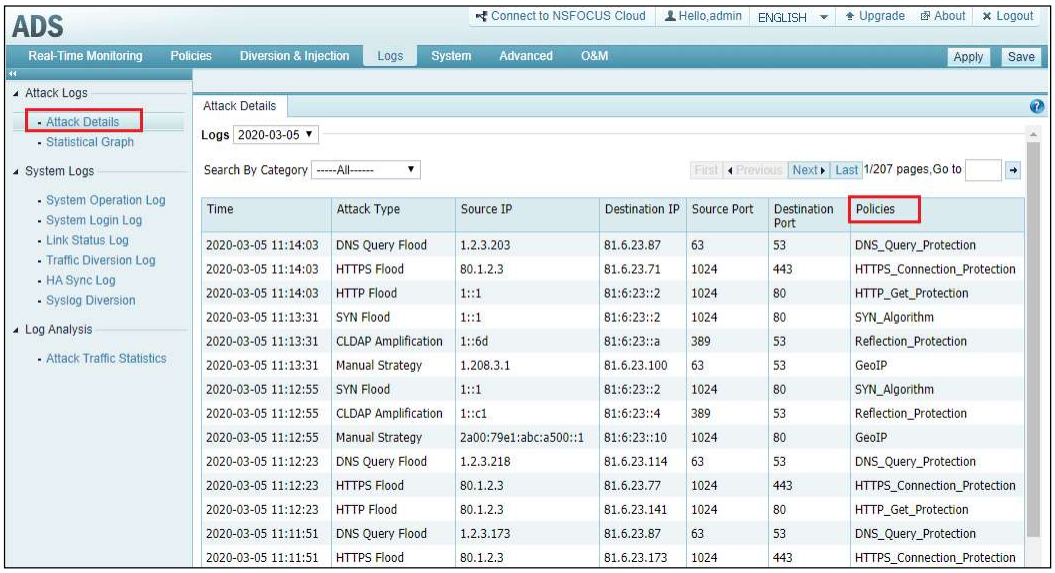
Function Description

In previous versions, if ADS drops packets during DDoS attack protection, a related message will be recorded in the attack log on the web-based manager, providing such information as the source/destination IP address, attack type, and attack signature that indicates the policy triggered. For legacy reasons, attack signatures were designed in such a way as to be too rough for users to understand. Besides, they do not have a one-to-one mapping with policies.

Therefore, attack signatures are deleted from attack log details, and policy names are provided instead. Besides, policy-specific statistics of packets dropped are available and destination IP-specific statistics uploaded to ADS M and third-party management devices cover policy information.

Involved Page

Logs > Attack Logs > Attack Details



Time	Attack Type	Source IP	Destination IP	Source Port	Destination Port	Policies
2020-03-05 11:14:03	DNS Query Flood	1.2.3.203	81.6.23.87	63	53	DNS_Query_Protection
2020-03-05 11:14:03	HTTPS Flood	80.1.2.3	81.6.23.71	1024	443	HTTPS_Connection_Protection
2020-03-05 11:14:03	HTTP Flood	1::1	81:6:23::2	1024	80	HTTP_Get_Protection
2020-03-05 11:13:31	SYN Flood	1::1	81:6:23::2	1024	80	SYN_Algorithm
2020-03-05 11:13:31	CLDAP Amplification	1::6d	81:6:23::a	389	53	Reflection_Protection
2020-03-05 11:13:31	Manual Strategy	1.208.3.1	81.6.23.100	63	53	GeoIP
2020-03-05 11:12:55	SYN Flood	1::1	81:6:23::2	1024	80	SYN_Algorithm
2020-03-05 11:12:55	CLDAP Amplification	1::c1	81:6:23::4	389	53	Reflection_Protection
2020-03-05 11:12:55	Manual Strategy	2a00:79e1:abc:a500::1	81:6:23::10	1024	80	GeoIP
2020-03-05 11:12:23	DNS Query Flood	1.2.3.218	81.6.23.114	63	53	DNS_Query_Protection
2020-03-05 11:12:23	HTTPS Flood	80.1.2.3	81.6.23.77	1024	443	HTTPS_Connection_Protection
2020-03-05 11:12:23	HTTP Flood	80.1.2.3	81.6.23.141	1024	80	HTTP_Get_Protection
2020-03-05 11:11:51	DNS Query Flood	1.2.3.173	81.6.23.87	63	53	DNS_Query_Protection
2020-03-05 11:11:51	HTTPS Flood	80.1.2.3	81.6.23.173	1024	443	HTTPS_Connection_Protection

Output of policy-specific statistics of packets dropped:

- Such data is exported as an XML file.
- The naming convention of such files is as follows: ADS-[*IP address of ADS*]-[*device ID of ADS*]-policy-traffic-date.xml (example: ADS-[10.66.2.4]-[C627-82D4-A3D9-7D11]-policy-traffic-20200212125436.xml).

Destination IP-specific statistics of packets dropped according to policies are exported as XML files of the following format:

```
<CollapsarData collapsarIP="10.66.2.4" timeStamp="1565589988" collapsarType="ADS-
xxx">
<protection policy stat begin time="1565589988" end time="1565590018">
      <dstip stat dstip="1.1.1.1" drop pps="100" drop bps="10000">
        <policy stat policy="ACK Protection" drop pps="50" drop bps="5000" />
        <policy stat policy="HTTP Get Protection" drop pps="50" drop bps="5000" />
      </dstip stat>

      <dstip_stat dstip="2.2.2.2" drop_pps="100" drop_bps="10000">
        <dstip_policy_stat policy="ACK Protection" drop_pps="50" drop_bps="5000" />
        <dstip_policy_stat policy="HTTP Get Protection" drop_pps="50"
drop_bps="5000" />
      </dstip_stat>
</protection_policy_stat>
</CollapsarData>
```

The following table describes XML elements.

Element	Description
protection_policy_stat	Protection policy, which may contain multiple **dstip_stat** fields

Element	Description
dstip_stat	Destination IP address, which may contain multiple **dstip_policy_stat** fields
dstip_policy_stat	Packets dropped according to the current policy

The following table describes element attributes.

Element	Attribute	Description
protection_policy_stat	begin_time	Start time of the statistics (in seconds)
	end_time	Ending time of the statistics (in seconds)
dstip_stat	dstip	Destination IP address
	drop_pps	Traffic destined for the destination IP address that has been dropped, in pps
	drop_bps	Traffic destined for the destination IP address that has been dropped, in bps
dstip_policy_stat	policy	Name of the policy
	drop_pps	Traffic dropped by the policy, in pps
	drop_bps	Traffic dropped by the policy, in bps

Notes

- The policy name is consistent with that on the web-based manager or in the CLI window. For details about a policy, see help information on the web-based manager.
- As the attack signature has been replaced with the policy name in the attack log, third-party platforms should be adapted accordingly when parsing the attack log uploaded by ADS.

1.4.6 Cloud Signaling

Function Description

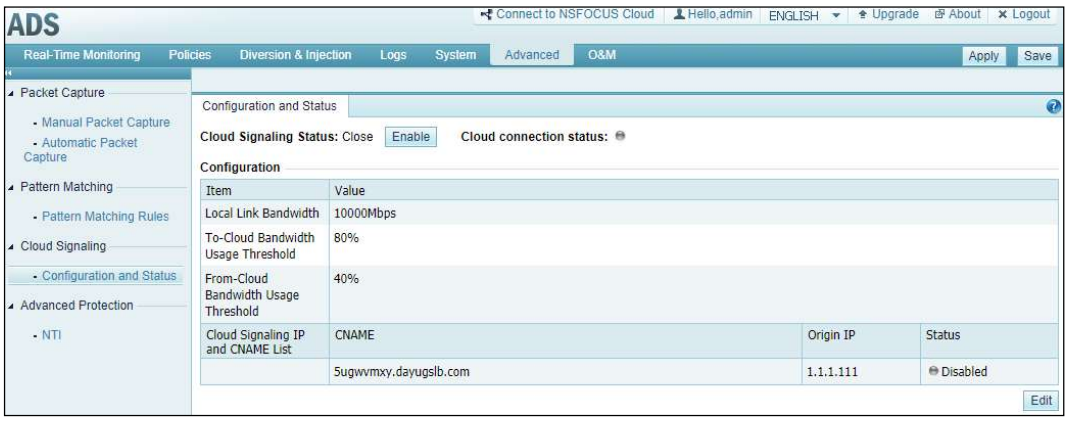
The cloud signaling function is added to implement coordinated protection against DDoS attacks between on-premises protection devices and the cloud cleaning center. For this purpose, the first step is to configure some parameters on the local ADS device and the cloud cleaning center for automatic switchover of traffic destined for the protected server. Specifically, when traffic is too large to be handled by the local device, it is automatically directed to the cloud cleaning center; when falling to a level acceptable for local cleaning, traffic is automatically switched back to the local device for cleaning.

For customers with insufficient ingress bandwidths or insufficient DDoS handling capacities, to mitigate volumetric DDoS attacks that may exhaust their bandwidth resources, a feasible option is cloud signaling that features coordinated protection between local ADS and the cloud cleaning center.

Configuration

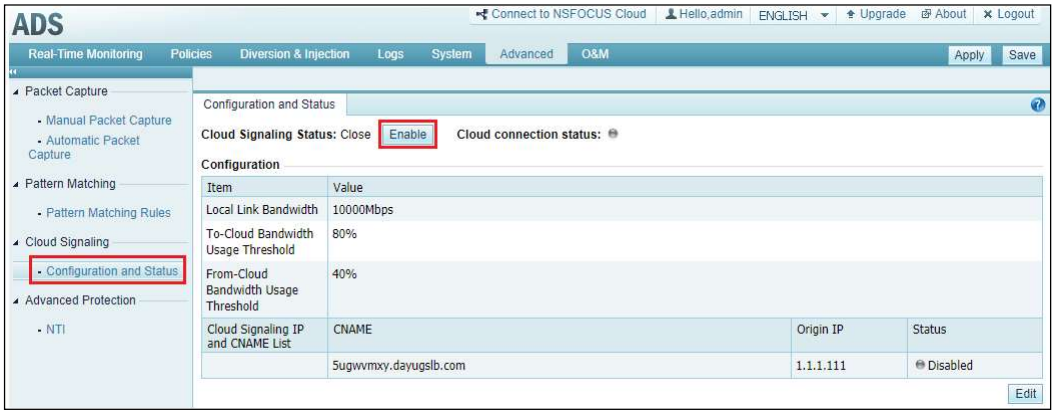
Advanced > Cloud Signaling > Configuration and Status

Configuring Cloud Signaling Parameters



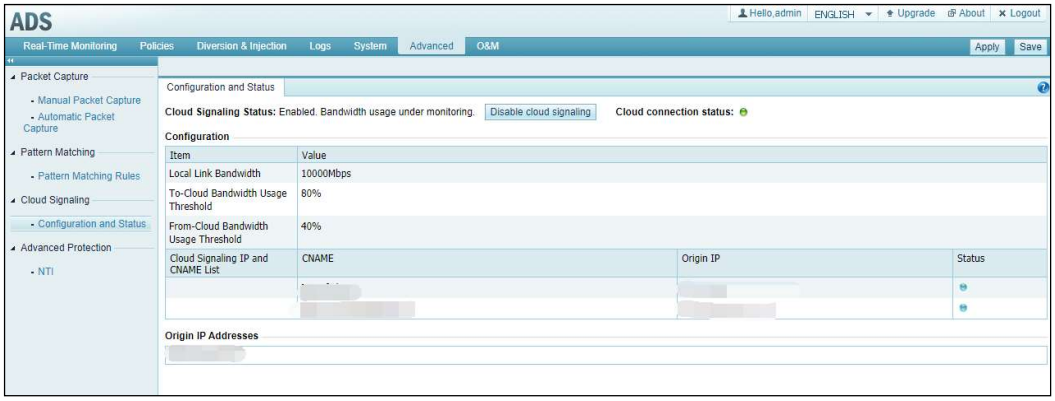
- Before enabling this function, configure parameters, including **Local Link Bandwidth**, **To-Cloud Bandwidth Usage Threshold**, **From-Cloud Bandwidth Usage Threshold**, and **Origin IP** of the server to be protected and the mapping **CNAME**. For specific CNAMEs, contact NSFOCUS technical support.
- At most 20 CNAMEs can be configured.
- For each CNAME, one to four origin IPv4 addresses can be configured. A CNAME can contain up to 256 characters.

Enabling Cloud Signaling



- After completing the configuration, click **Enable** to enable cloud signaling.
- Make sure the management interface of ADS properly connects to the Internet; otherwise, the function cannot be enabled.
- If the CNAME typed here is invalid, that is, not a CNAME provided by NSFOCUS, the function cannot be enabled.
- After this function is enabled, parameters cannot be edited again.

Rationale



- When receiving traffic that exceeds the to-cloud bandwidth usage threshold, ADS automatically forwards traffic to the cloud cleaning center for DDoS mitigation.
- When the traffic destined for the origin IP address falls below the from-cloud bandwidth usage threshold, ADS automatically takes over the job from the cloud cleaning center.

Notes

- This function requires ADS to collaborate with NSFOCUS Cloud, that is, the cloud cleaning center. Therefore, to use this function, users should contact NSFOCUS technical support for related configuration.
- This function works in reliance on CNAMEs. Therefore, it is applicable only to domain name-based web servers.

1.4.7 ADS NX5-10000 Supporting More Management Devices

Function Description

The number of management devices configurable for ADS NX5-10000 is increased to 20. These management devices include ADS M, ESPC/ESPP, and other third-party platforms.

Configuration

System > Local Settings > Management Mode > Management Mode

Notes

- ADS NX5-10000 can be managed by up to 20 devices simultaneously, but other models still support at most five management devices.
- ADS NX5-10000 can upload files, such as traffic statistics, to at most five management devices even if more than five management devices are configured.

1.4.8 ADS NX5-8000 Being Able to Be Deployed in In-Path Mode

Function Description

ADS NX5-8000 of the new version can be deployed in in-path mode.

1.4.9 Display of Manual Packet Capture Information and Generation of Policies Accordingly

Function Description

Settings and files of manual packet capture tasks are saved and displayed on the web-based manager. In addition, the summary and details of captured packets can be queried, allowing users to quickly generate static rules accordingly. This function has the following advantages:

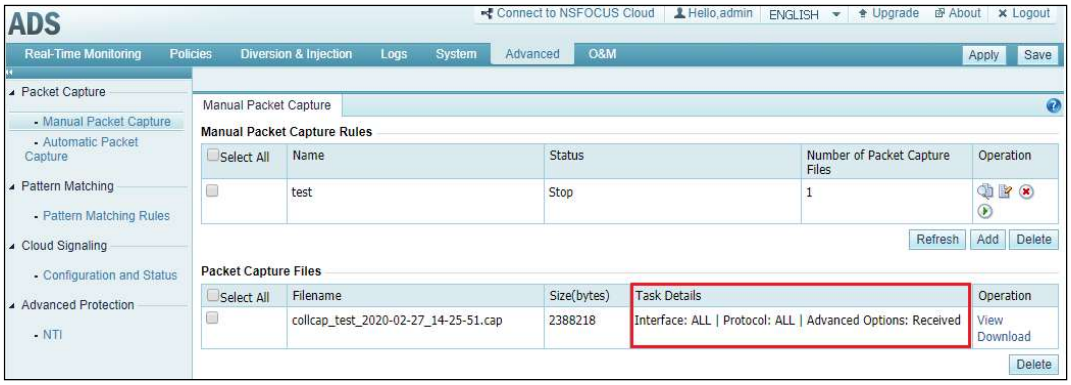
- When viewing captured packets, users can conveniently trace their sources by checking related task configuration parameters.
- Users can conveniently view contents of captured packets on the web-based manager of ADS without using such tools as Wireshark to rapidly locate faults.
- Users can rapidly configure various static protection rules based on packet contents.

Configuration

Advanced > Packet Capture > Manual Packet Capture

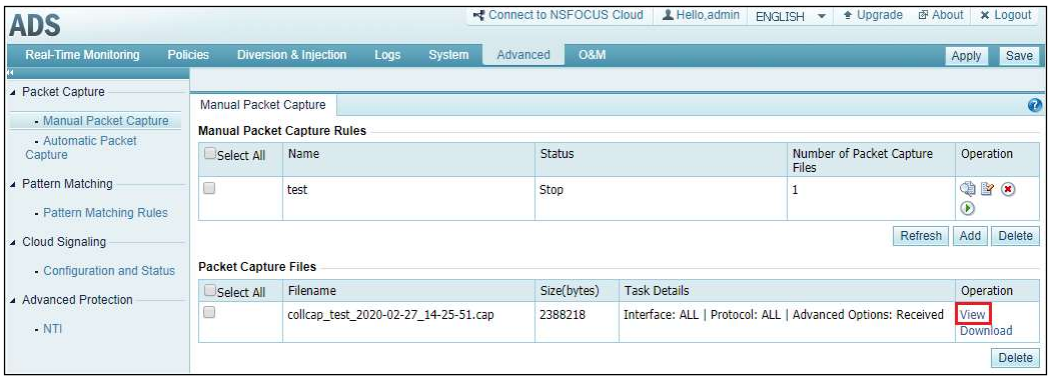
Packet Capture Parameters

Each packet capture file has related configuration parameters displayed on the web-based manager.



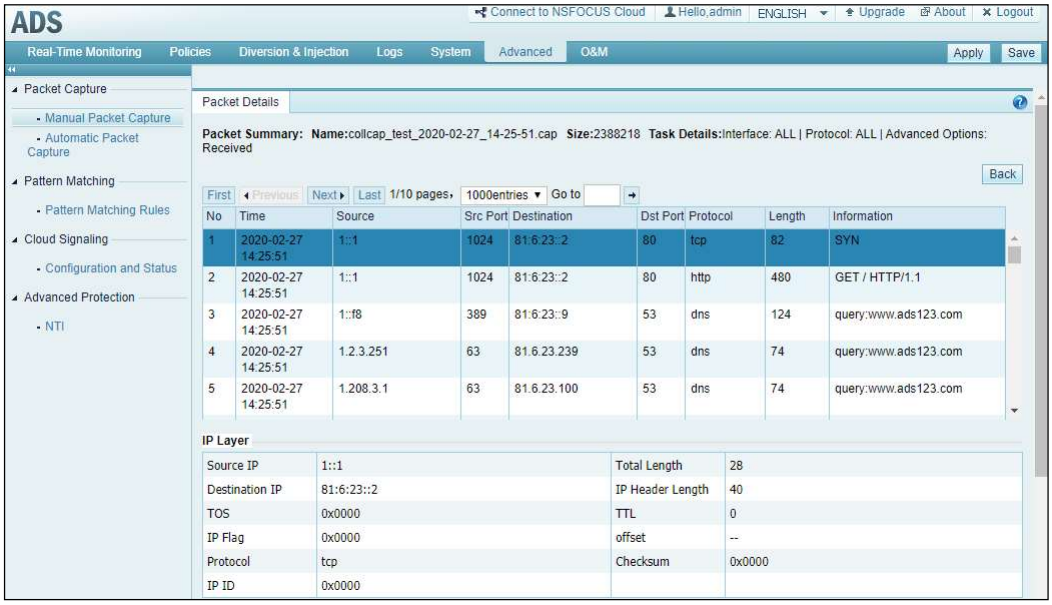
Packet Summary

Clicking **View** displays packet summary and details.



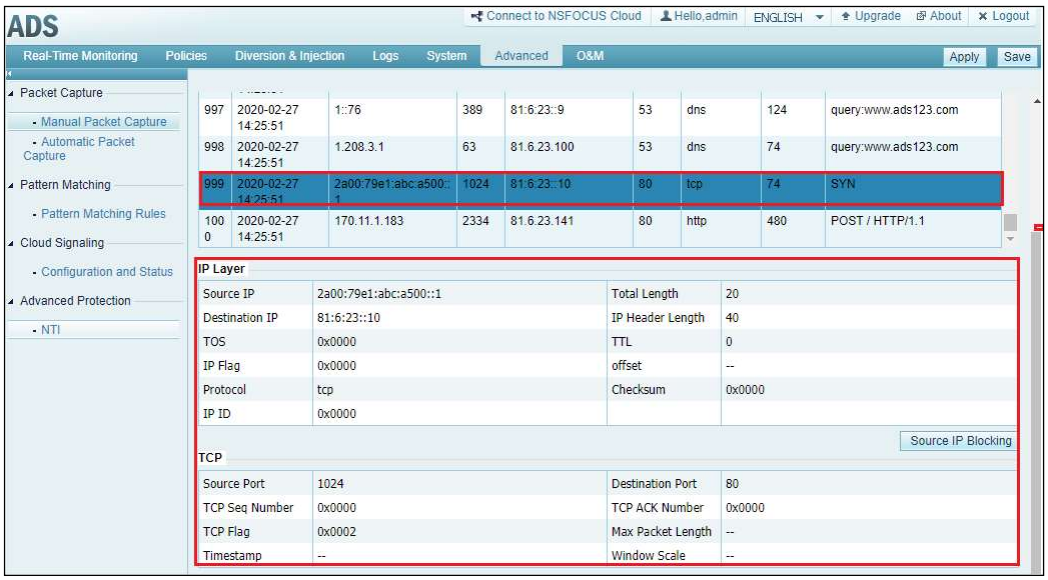
The **Packet Summary** area provides the packet capture time, quintuple, packet length, and summary information.

The packet summary information is displayed on multiple pages. Users can set the number of packets displayed on each page.



Packet Details

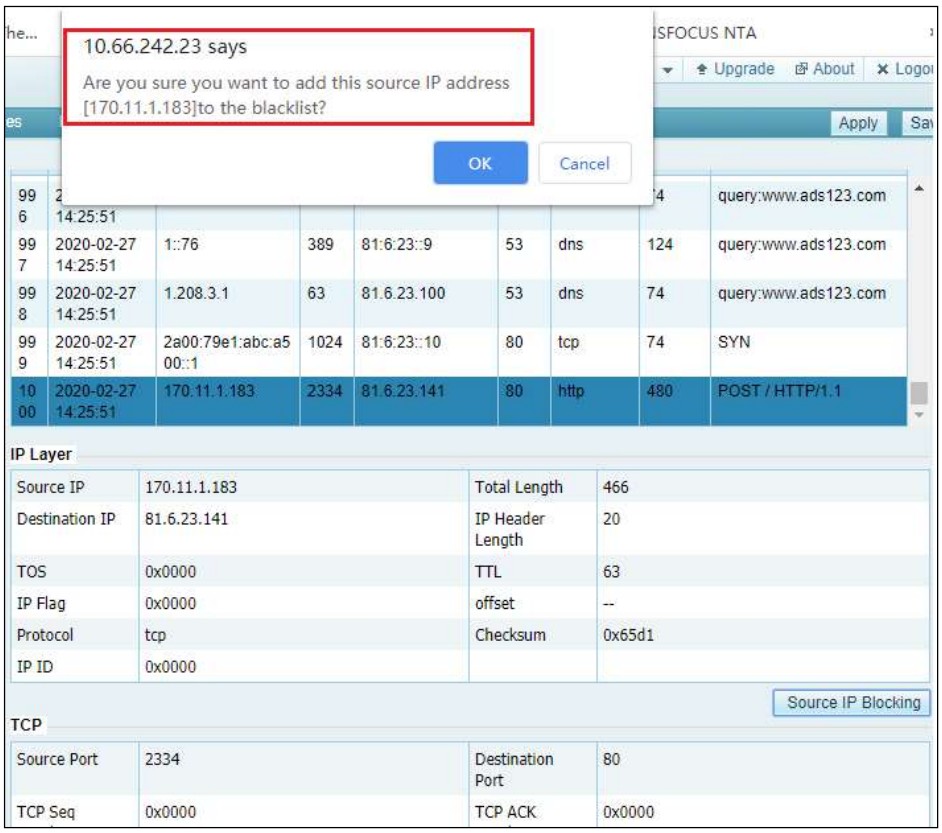
Clicking the line of a packet in the **Packet Summary** area displays details of this packet, including IP, TCP, HTTP, or DNS header information and payload data.



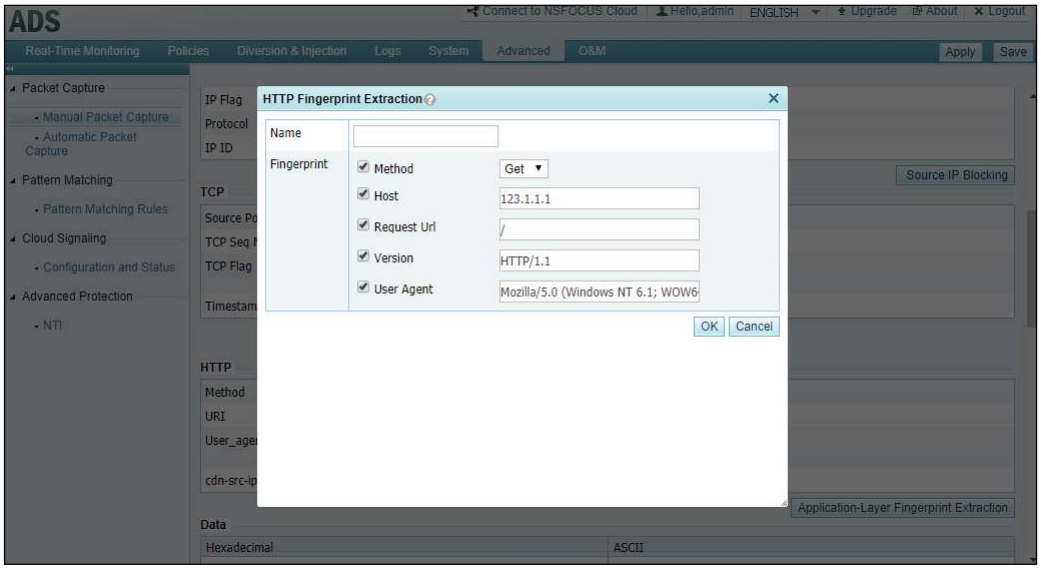
Generation of Static Rules

In each section showing details of a packet, clicking the function button generates a related static protection rule.

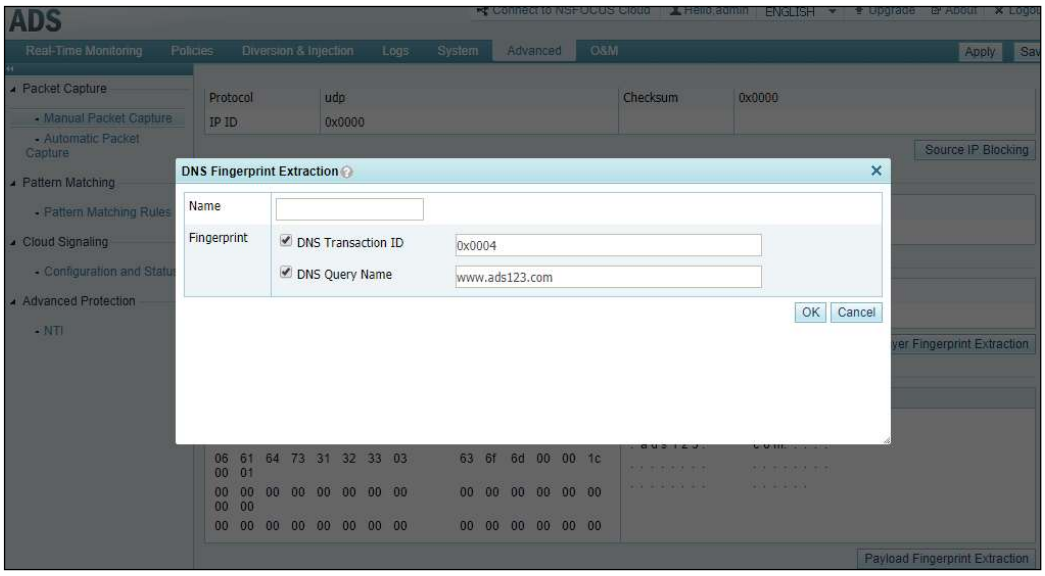
For example, a click on **Source IP Blocking** will add the source IP address of this packet to the blacklist.



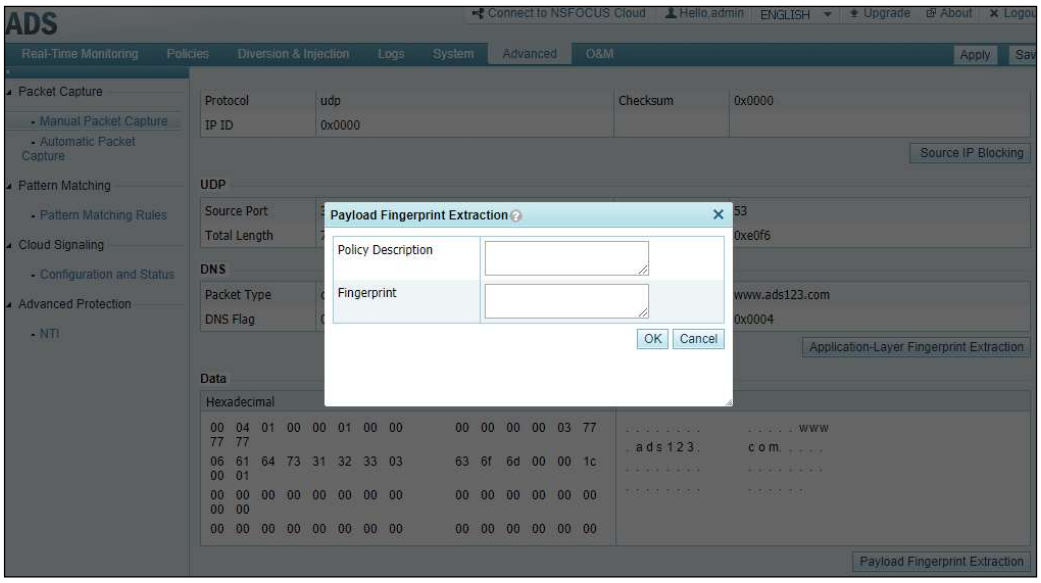
For an HTTP packet, a click on **Application-Layer Fingerprint Extraction** will generate an HTTP keyword checking rule.



For a DNS packet, a click on **Application-Layer Fingerprint Extraction** will generate a DNS keyword checking rule.



In the **Data** area, a click on **Payload Fingerprint Extraction** allows users to configure a pattern matching rule (packets whose source/destination IP address is 0.0.0.0 and protocol is the same as the current one will be dropped).



Notes

- Only the IP layer and data of such application-layer protocols as DNS and HTTP are parsed. ARP packets are not parsed.
- HTTP and DNS keyword checking rules generated here should be referenced in default or group-specific policies before taking effect.
- These changes apply only to manual packet capture tasks.

1.4.10 Per-Packet Load Balancing Mode Configurable via CLI Commands

Function Description

When multiple injection interfaces are configured for a destination IP address, ADS of previous versions can implement load balancing only based on source/destination IP addresses by default. For use in diverse scenarios, the new version adds per-packet load balancing.

Different modes of load balancing can be configured by running the following CLI commands:

- inject set load-balance src-dst-ip sets load balancing using source/destination IP.
- inject set load-balance per-packet sets per-packet load balancing.

Notes

By default, ADS implements load balancing based on source/destination IP addresses.

1.4.11 Service Interface Information Added for the SNMP Agent

Function Description

The management information base (MIB) of SNMP adds two OIDs: 1.3.6.1.4.1.19849.6.2.10 indicating the total number of interfaces on ADS and 1.3.6.1.4.1.19849.6.2.11 indicating traffic on interfaces. For details, see *PVD-ADS-V4.5R90F02 SNMP Description*.

1.4.12 Anomalous Packet Filtering

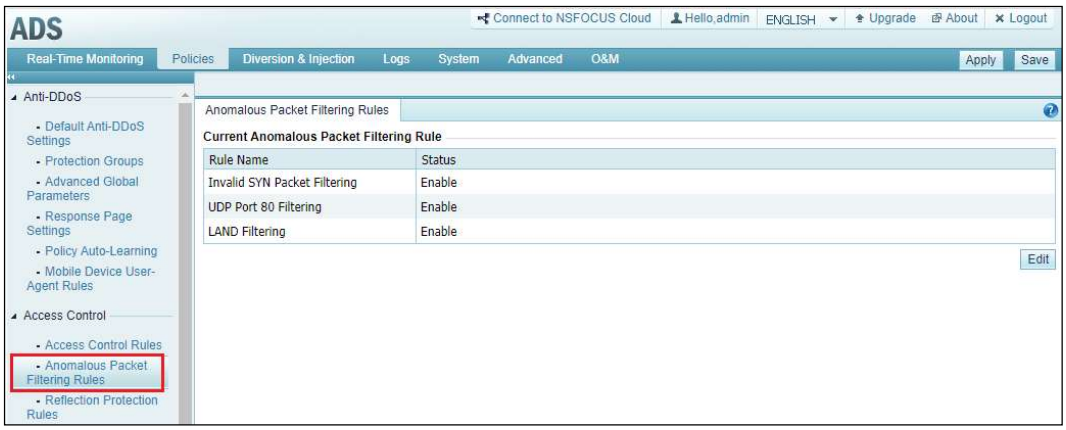
Function Description

In previous versions, ADS comes with default static checking rules. In the new version, these rules are incorporated into anomalous packet filtering rules for users to configure. Anomalous packet filtering covers the following types of packets:

- Invalid SYN packet: contains no options field in the TCP header.
- Packets with UDP port 80 as the destination port.
- LAND packet: has the same IP address as both the source and destination addresses.

Configuration

Policies > Access Control > Anomalous Packet Filtering Rules



After such a rule is enabled, matched packets will be dropped.

Notes

V4.5R90F00 optimizes extraction of attack log messages by preferentially listing attack events of different types. In addition, invalid SYN packet protection can be turned on or off. In this version, the invalid SYN packet alert switch is removed from **System > Local Settings > Basic Settings** to avoid the situation where invalid SYN packets are dropped, but no log is generated.

1.4.13 Commands Added in the Console User Interface to Enable/Disable the Web Service

Function Description

The new version allows users to enable/disable the web service via the console user interface.

Configuration

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

1.4.14 GeoIP Library Updated

Function Description

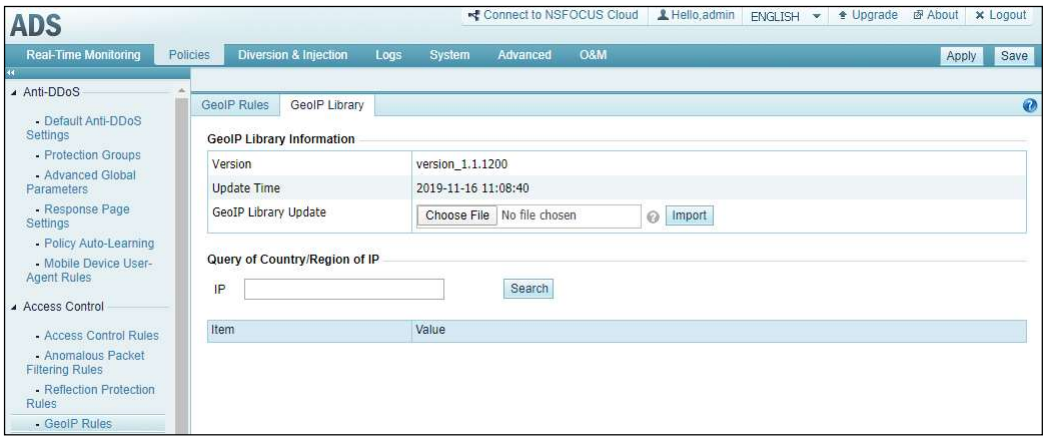
Based on a new database, the GeoIP library will be updated regularly subsequently to increase the accuracy of geographical information.

The GeoIP library can be updated by loading the latest update package.

The new version does not support export of the GeoIP library, but allows users to query the country/region in which an IP address is located.

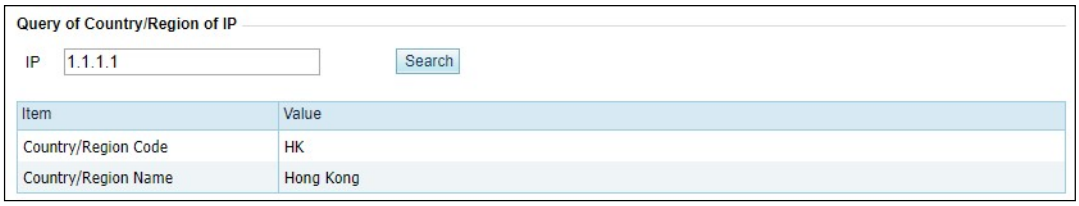
Configuration

Policies > Access Control > GeoIP Rules > GeoIP Library



The GeoIP library can be updated by loading the latest update package. The current version number of the library is displayed on the page.

Users can type an IP address to query its country/region.



Notes

In the process of updating the GeoIP library, the system may find that some countries or regions previously configured in GeoIP rules are missing in the update package, which is called rule conflicting. In this case, the system will display a message on the web UI, asking users whether to continue the update. If the update continues, conflicting rules will be automatically deleted.

1.4.15 Destination IP Addresses Provided in the Blacklist

Function Description

For packets that trigger a protection policy and have source IP address automatically added to the blacklist, their destination IP address is recorded and displayed in the blacklist query result.

When **Block permanently** is selected during blacklist configuration, IP addresses manually added to the blacklist will still be there after a system restart.

1.4.16 Reflection Attack Protection Expanded

Function Description

MS SQL and CLDAP reflection protection rules are added in the list of reflection protection rules. Attack types of CLDAP amplification and MS SQL amplification are added accordingly.

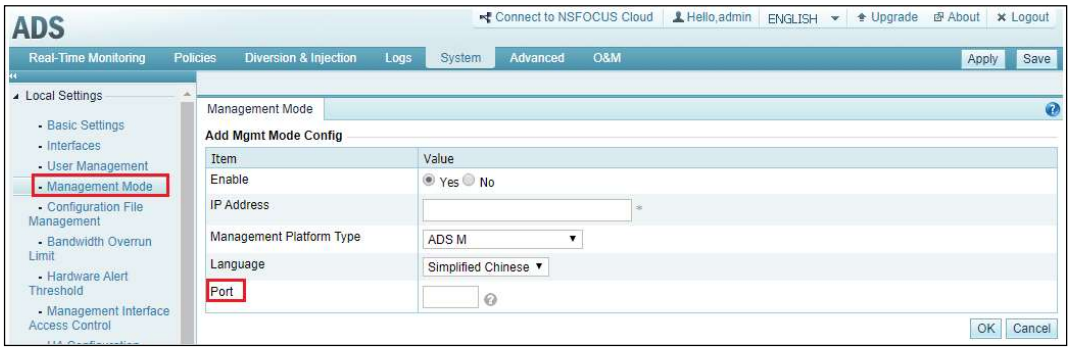
1.4.17 Port Configurable for Management by ADS M

Function Description

When selecting ADS M as the management platform, users can specify a port for such management.

Configuration

System > Local Settings > Management Mode > Management Mode



When adding ADS M as a new management device, users can specify a port as required for communication with ADS M. The default value is **443**.

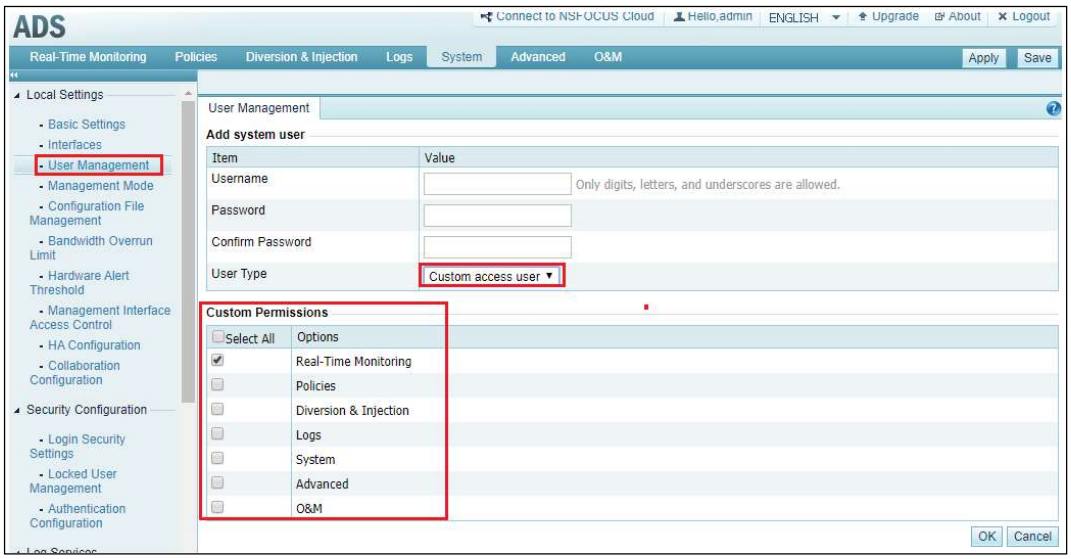
1.4.18 Custom Access User Role Added on the Web-based Manager

Function Description

A new user role is added, custom access user, whose permissions for using different modules of ADS are controlled by **admin**.

Configuration

System > Local Settings > User Management > System User



1.4.19 Display of Modules Covered by the Current License on the Web-based Manager

Function Description

Users can preview modules covered by the license being imported. They can also check what modules are authorized after the license is imported.

Involved Page

System > Others > License Info

Notes

Current authorized modules of ADS are IPv6 and NTI. There may be more authorized modules in subsequent versions.

1.4.20 Key Time Synchronization Events Logged

Function Description

To facilitate troubleshooting of faults concerning NTP time synchronization, the new version adds the function of logging key time synchronization events:

- First success in synchronization of time from the NTP server (including the first success after repeated failures)
- First failure to synchronize time from the NTP server (including the first failure after repeated successes)

1.4.21 New Model of External Bypass Switch Added

Function Description

BP2301 is added as a new model of external bypass switch. This model and the previously supported BP2201 belong to the same series. Users can choose which to use when configuring an external bypass switch.

Configuration

System > Local Settings > Bypass Configuration > External Bypass Configuration

1.5 Compatibility with NTA Versions

- ADS V4.5R90F02 can collaborate with NTA V4.5R90F02 and both support IPv4 and IPv6 addresses.

1.6 Supported Browsers

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

Version Upgrade

1 Upgrade from V4.5R90F01.20181012, V4.5R90F01.sp01.20181026, V4.5R90F01.sp02.20181026, V4.5R90F01.sp03.20181217, V4.5R90F01.sp04.20190305, V4.5R90F01.sp05.20190508, V4.590F01.sp06.20190715, V4.5R90F01.sp07.20190821, V4.5R90F01.sp08.20191225, V4.5R90F01.sp09.20200109, or V4.5R90F01.sp07c236.20200107

[Applicable Device Modes]

ADS NX3-200E/600E/800E, ADS NX3-2010/2020/2020E, ADS NX5-4020/4020E, ADS NX5-6025/6025E, ADS NX5-8000, ADS NX3-HD2500/NX5-HD4500/NX5-HD6500

[Upgrade Procedure]

The upgrade to V4.5R90F02 must be performed 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 drive.

Step 2 Install the update package **update_ADS_x86_V4.5R90F02_20200312.zip** (MD5: FBFCB5B7A7E41DFAEFBD61B1DAC4A47E) on ADS V4.5R90F01 or V4.5R90F01.sp0x.

Step 3 If the upgrade is successful, restart the device.

Step 4 Verify that the system version turns to **V4.5R90F02** in the status bar of the web-based manager.

----End

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

2 Rollback to V4. 5R90F01 or V4.5R90F01.sp0x

[Applicable Device Modes]

ADS NX3-200E/600E/800E, ADS NX3-2010/2020/2020E, ADS NX5-4020/4020E, ADS NX5-6025/6025E, ADS NX5-8000, ADS NX3-HD2500/NX5-HD4500/NX5-HD6500

[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.