# ADS V4.5R90F00

# Release Notes

Version: V4.5R90F00 (2017-12-18)

# Contents

# 1 Basic Information

| | |
|---|---|
| **Product Model** | ADS NX3-200E/600E/800E<br>ADS NX3-2010/2020/2020E<br>ADS NX5-4020/4020E/6025/6025E/8000 |
| **Software Version** | V4.5R90F00 |
| **Upgrade File** | ADS V4.5R90F00_201720180110<br>(MD5: 72812CD3C97F9A4B3531D057D7F2277F) |
| **Release Date** | 2017-12-18 |
| **How to Obtain** | Contact technical support personnel of NSFOCUS. |

# 2 Version Mapping

| | |
|---|---|
| **Source Software Version** | V4.5R90F00 |
| **Hardware Platform Model** | NSF1100-1<br>NSF1100-3<br>NSF2800-2<br>NSF2800-6<br>NSF3600-4 |
| **Network Traffic Analyzer Platform Version** | V4.5.61.2<br>V4.5R90F00 |
| **Management Platform Version** | ADS M V4.5R90F00 |
| **Client** | N/A |
| **Other System or Tool** | N/A |
| **Documentation** | NSFOCUS ADS User Guide (V4.5R90F00) |

# 3 Function Changes

V4.5R90F00 is applicable to the following device models:

- ADS NX3-200E/600E/800E
- ADS NX3-2010/2020/2020E
- ADS NX5-4020/4020E/6025/6025E/8000

## 3.1 Support for All Device Models on the X86 Hardware Platform

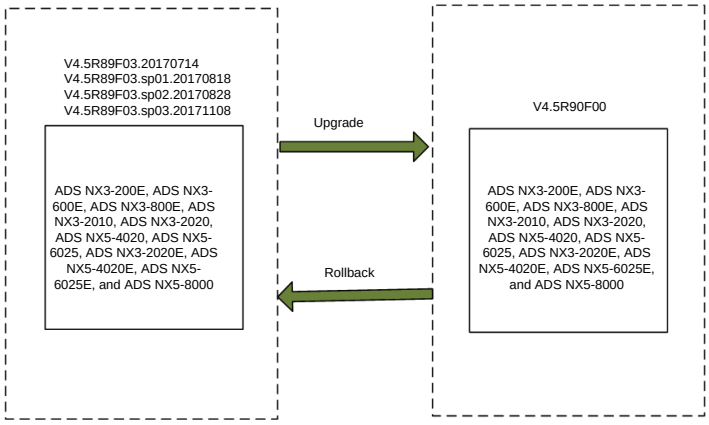
Like V4.5R89F03, V4.5R90F00 supports all device models on the X86 hardware platform.

V4.5R90F00 supports the following device models on the X86 hardware platform:

- ADS NX3-200E/600E/800E
- ADS NX3-2010/2020/2020E
- ADS NX5-4020/4020E/6025/6025E/8000

Prior to upgrade to V4.5R90F00, such devices need to be upgraded to V4.5R89F03 (V4.5R89F03.20170714) or V4.5R89F03.sp0x (V4.5R89F03.sp01.20170818, V4.5R89F03.sp02.20170828, or V4.5R89F03.sp03.20171108).

The upgrade path from V4.5R89F03 or V4.5R89F03.sp0x to V4.5R90F00 is shown as follows:



## 3.2 Overview of Changed Functions in V4.5R90F00

### 3.2.1 Optimizations and Additions in V4.5R90F00

| Function | Description |
|---|---|
| *HTTPS protection | V4.5R90F00 uses the original HTTPS protection policy as the HTTPS connection protection policy and also provides HTTPS application-layer protection. This new function decrypts HTTPS packets into HTTP packets, collects statistics of abnormal behaviors detected during the SSL/TLS handshake process, and protects against them with various HTTP algorithms. |
| *Packet capture | V4.5R90F00 allows concurrent manual packet capture tasks, automatic packet capture tasks, and simultaneous execution of tasks of both types. Besides, more packet filtering conditions are provided such as source IP segment, protocol ID, and TCP/UDP port. |
| Reflection protection policy | Global reflection protection rules can be created to block or limit the rate of UDP packets from a specific source port. Such rules can be referenced by certain protection group-specific policies to provide corresponding protection. |
| Addition of rate-limiting action in static filtering rules | For the HTTP keyword checking policy and DNS keyword checking policy, **Rate-limiting** is added as an option of **Action**.<br>For regular expression rules and pattern matching rules, **Rate-limiting** is added as an option of **Access Control**. |
| UDP regular expression protection policy | The UDP regular expression protection policy is added for protection groups. |
| Addition of tcpdump as a new method for network diagnosis | tcpdump is added as a new method for network diagnosis to capture packets on the management interface or other interfaces of ADS. |
| Optimization of the page for manual traffic diversion | The page of manual traffic diversion rules supports pagination and rule query, allowing users to manage specific rules among numerous ones in an easy and rapid way. |
| Login verification code | Verification codes can be used as a login authentication option. |
| Sequence of certain access control rules being adjustable | The priority of some access control rules can be adjusted on the web-based manager. |
| Optimization of the whitelist and blacklist | A hash collision handling mechanism is added for both the blacklist and whitelist. |
| Domain name allowed for ESPC/ESPP | Users are allowed to configure a domain name for NSFOCUS ESPC or ESPP. |
| Upgrade notes viewable after upgrade | Upgrade notes can be viewed after the system is restarted. |

### 3.2.2 Modified Functions

The following table lists functions modified in V4.5R90F00.

| Function | V4.5R89F03 | V4.5R90F00 |
|---|---|---|
| HTTPS protection | HTTPS protection | The original HTTPS protection policy is retained as the HTTPS connection protection policy. The HTTPS application-layer protection function is added and |

| Function | V4.5R89F03 | V4.5R90F00 |
|---|---|---|
| | | available only to certain device models. |
| Manual packet capture task | Only one manual packet capture task can run each time. | Multiple manual packet capture tasks can run simultaneously. The packet capture task name must be specified during task configuration. |
| Automatic packet capture task | Only one automatic packet capture task can run each time. | Multiple automatic packet capture tasks are supported. The packet capture task name must be specified during task configuration. |

## 3.3 Detailed Analysis of Changed Functions in V4.5R90F00

### 3.3.1 Optimization of HTTPS Protection

#### Function Description

As more and more Internet services are switched to the encrypted HTTPS from the plaintext HTTP, DDoS attacks against HTTPS ensue, including attacks targeting the SSL/TLS handshake and HTTPS services. To prevent those attacks, you can enable HTTPS application-layer protection to achieve advanced protection in a targeted manner.

This function has the following advantages:

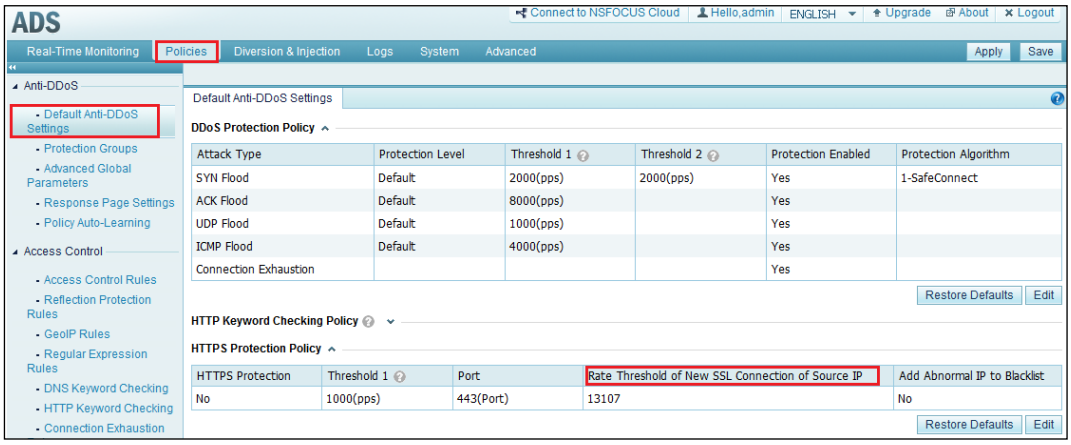
- It can protect against more covert attacks occurring during the SSL/TLS interaction process.
- It uses the existing HTTP algorithms to protect against HTTPS interaction attacks.
- An SSL certificate needs to be imported only for preventing the browser from reporting a security alert. Users can also import a different certificate (for example, a domain validation certificate) than that available on the server.
- It verifies the validity of clients only. If packets from a client are found legitimate, subsequent packets from this client are allowed to pass through, without any checks. Therefore, this function incurs no information leakage risks.

#### Configuration

1. Configure a default HTTPS protection policy as follows:

For default anti-DDoS settings, choose **Policies > Anti-DDoS > Default Anti-DDoS Settings > HTTPS Protection Policy**.

Figure 3-1 Default HTTPS protection policy

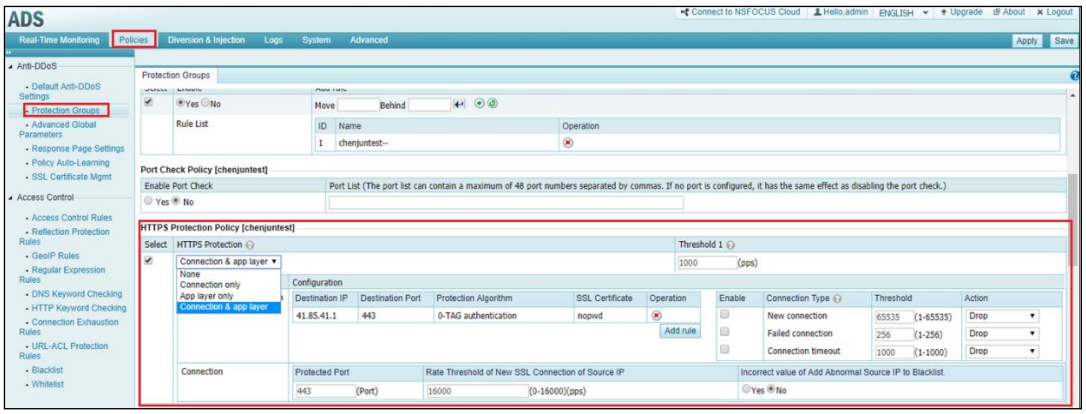



In V4.5F90F00, the **Rate Threshold of New SSL Connection of Source IP** parameter, which is provided in previous versions only for use (by the **setflag set https_change_cipher_spec_pkts <value>** command) in the CLI, is provided separately for the default HTTPS protection policy and group-specific HTTPS connection policy on the web-based manager.

2. Configure the HTTPS protection policy for a protection group as follows:

Choose **Policies > Protection Groups** and click in the **Edit Policy** column of a protection group. Then set parameters in the **HTTPS Protection Policy** area.

Figure 3-2 Configuring the HTTPS protection policy for a protection group




The group-specific HTTPS protection policy provides connection protection and application-layer protection.

The connection protection policy is configured in the same way as the default HTTPS protection policy.

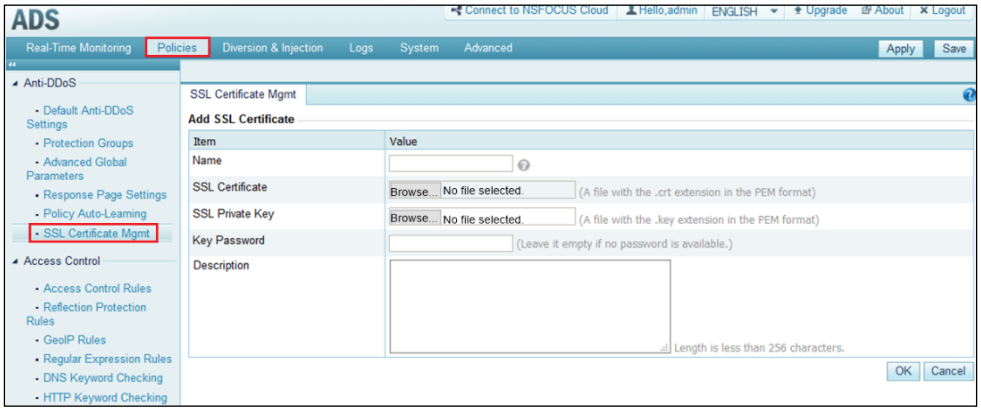
The application-layer protection policy works only for the specified HTTPS server (destination IP address+destination port). After the SSL certificate used by the server is imported, this policy, by using HTTPS algorithms, verifies clients attempting to access the server and controls SSL connections from these clients. If a client still fails to be authenticated by an HTTPS protection algorithm after the number of its new connections, failed

connections, or timeout connections exceeds the corresponding threshold, subsequent packets from the client will be dropped or its IP address will be added to the blacklist.

The application-layer protection configuration consists of importing an SSL certificate and creating an application-layer protection rule.

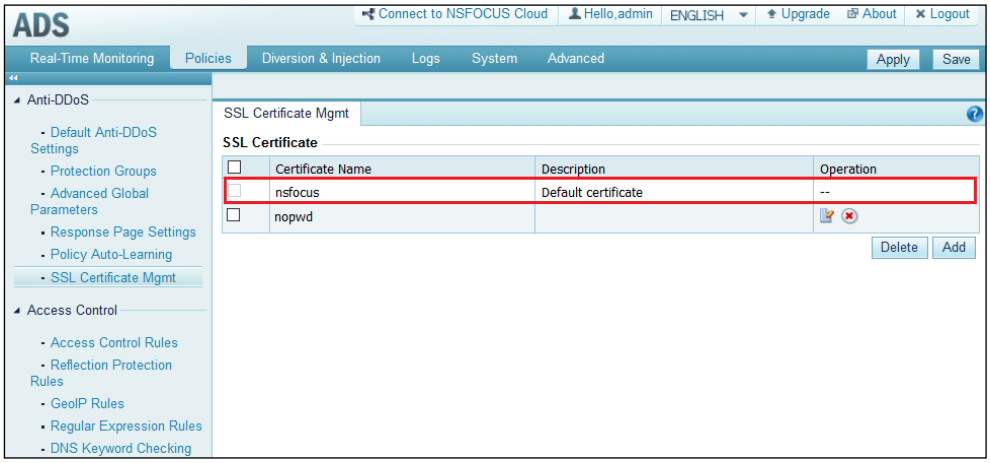
Choose **Policies > Anti-DDoS > SSL Certificate Mgmt** and import an SSL certificate.

Figure 3-3 Adding an SSL certificate




Before enabling HTTPS application-layer protection, you need to import an SSL certificate and the matching private key (only the PEM format is supported) of the server to be protected. A maximum of 20 pairs of SSL certificates and private keys are allowed here.

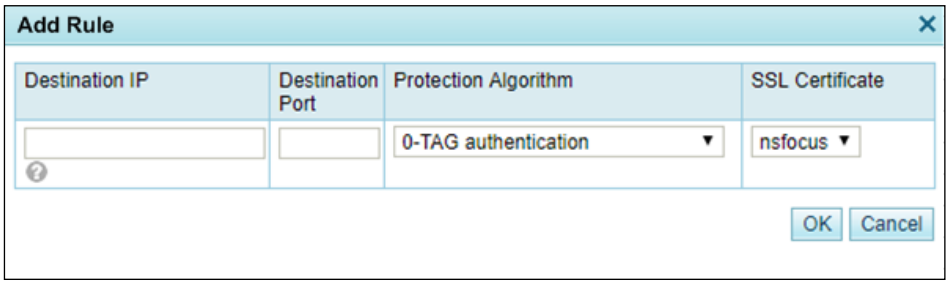
Figure 3-4 SSL certificate management




The system provides the default **nsfocus** certificate which cannot be modified or deleted.

In the **HTTPS Protection Policy** area on the page shown in Figure 3-2, click **Add rule** in the **HTTPS Protection Policy** area to create an HTTPS application-layer protection rule.

Figure 3-5 Creating an HTTPS application-layer protection rule




Parameters in the **Add Rule** dialog box are described as follows:

- **Destination IP**: IP address of the HTTPS server to be protected. The IP address specified here must be within the IP address range covered by the protection group.
- **Destination Port**: TCP port of the HTTP server to be protected.
- **Protection Algorithm**: HTTPS protection algorithm. HTTPS protection algorithms are actually HTTP protection algorithms.
- **SSL Certificate**: SSL certificate used by the HTTPS server.

## Notes

- Due to memory restrictions, HTTPS application-layer protection is available only to ADS 800E/2020E/4020E/6025E/8000.
- If both the HTTPS connection protection and application-layer protection are enabled for a protection group, only the destination IP address and port put under application-layer protection follow the application-layer protection rule, while other ports are checked against the connection protection policy.

# 3.3.2 Packet Capture Optimization

## Function Description

In previous versions, ADS supports at most one manual packet capture task and one automatic task and does not allow tasks in two modes to run simultaneously. This greatly decreases the protection efficiency. V4.5R90F00 allows concurrent manual tasks, concurrent automatic tasks, and simultaneous execution of tasks of both types. Besides, packet capture tasks provide more filtering conditions such as source IP segment, protocol ID, and TCP/UDP port.

This function has the following advantages:

- More packet filtering conditions are provided to make it easier to capture desired packets.
- Multiple manual packet capture tasks can be configured and run simultaneously, increasing protection efficiency.
- Multiple automatic packet capture tasks can run simultaneously, allowing users to learn details about multiple attack events at the same time.

## Configuration

1. Configure a manual packet capture task as follows:

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

Figure 3-6 Configuring a manual packet capture task

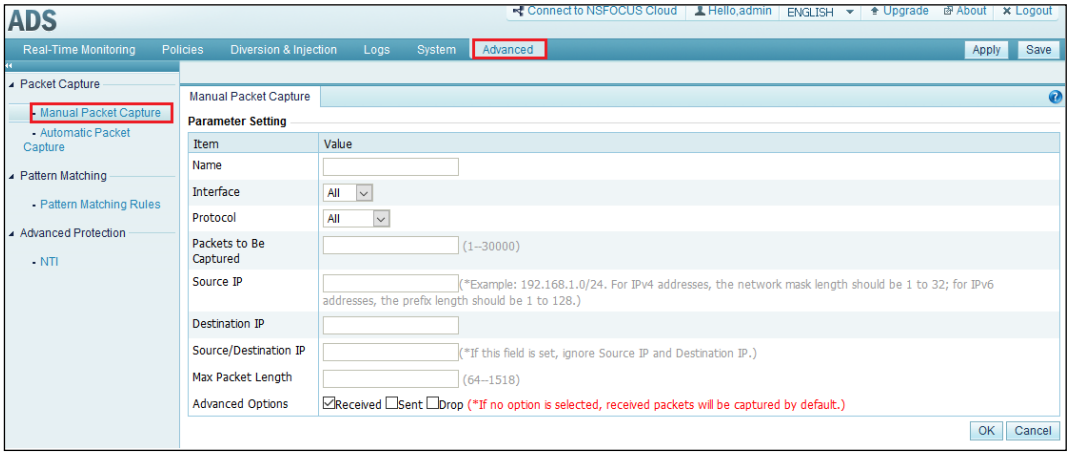
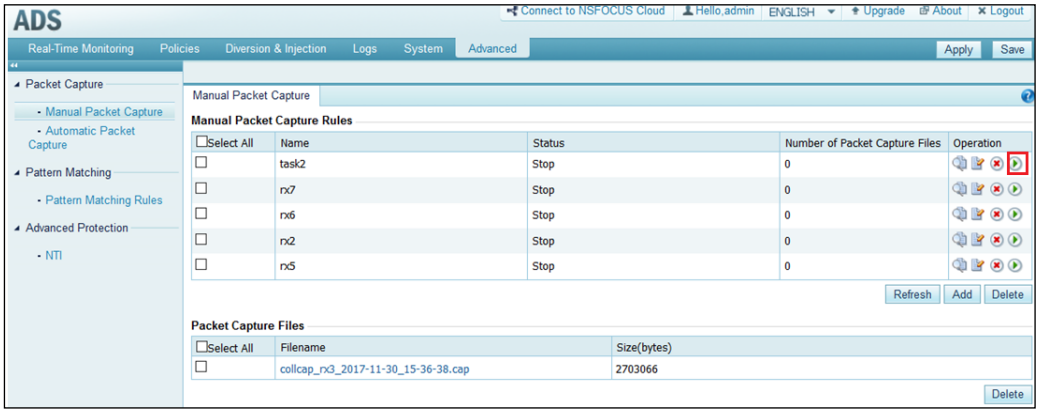



Figure 3-7 Starting a manual packet capture task




All files generated for manual packet capture tasks are managed in the **Packet Capture Files** area. Such files are named in the format of collcap_*task name_file generation time (YYYY-MM-DD_HH-MM-SS)*.cap.

2. Configure an automatic packet capture task as follows:

Choose **Advanced > Packet Capture > Automatic Packet Capture**, click **Add**, and configure parameters to create an automatic packet capture task.

Figure 3-8 Configuring an automatic packet capture task

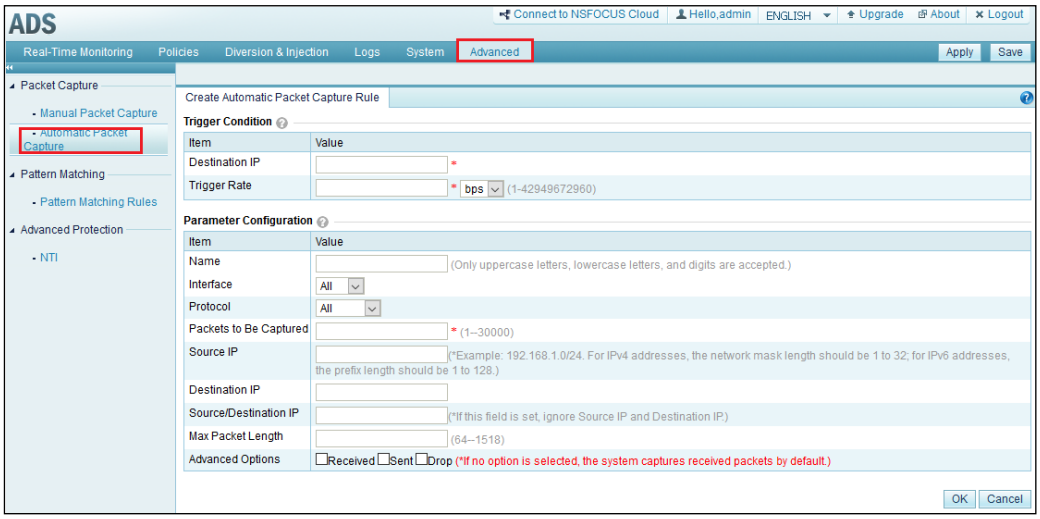
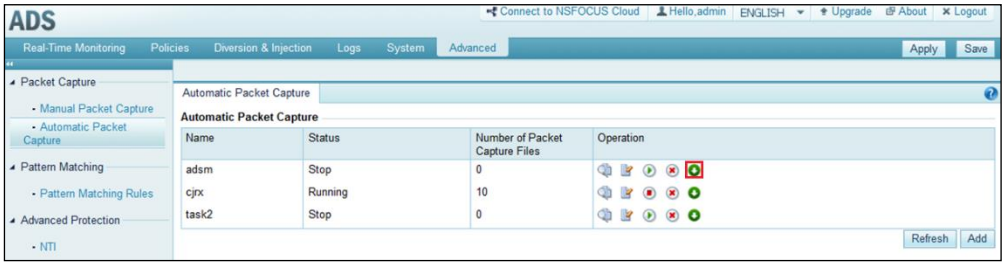



Figure 3-9 Managing an automatic packet capture task




Files generated for automatic packet capture tasks are managed separately. You can click to download or delete files of this task.

## Notes

Due to memory restrictions, the maximum number of packet capture tasks that can be created and the maximum number of packet capture files that can be saved vary with device models, as shown in the following table:

| | **Item** | **NX3-200E/600E**<br>**NX3-2020/2010**<br>**NX5-4020/6025** | **NX3-800E/2020E**<br>**NX5-4020E/6025E**<br>**NX5-8000** |
|---|---|---|---|
| Manual packet capture | Maximum number of packet capture tasks allowed | 6 | 6 |
| | Maximum number of concurrent packet capture tasks | 2 | 3 |
| | Maximum number of packet capture files saved | 5 | 10 |
| | Maximum number of packet capture | 2 | 3 |

| | Item | NX3-200E/600E<br>NX3-2020/2010<br>NX5-4020/6025 | NX3-800E/2020E<br>NX5-4020E/6025E<br>NX5-8000 |
|---|---|---|---|
| Automatic packet capture | tasks allowed | | |
| | Maximum number of concurrent packet capture tasks | 2 | 3 |
| | Maximum number of packet capture files saved for each task | 10 | 10 |

## 3.3.3 Reflection Protection Policy

### Function Description

Reflection attacks are a common type of DDoS attacks. In previous versions, such attacks are generally prevented by using global ACL rules to block packets from the specified source ports. This kind of protection method has poor ease-of-use and scalability.

To upgrade ADS's protection performance, dedicated rules should be provided to protect against reflection attacks. In V4.5R90F00, reflection protection is added as a separate function to block or limit the rate of UDP packets from specific ports. This function has the following advantages:

- Users can configure rules specific to reflection attack protection, which allows for better scalability.
- As an independent protection module for protection groups, the reflection protection policy provides targeted protection for specific users.

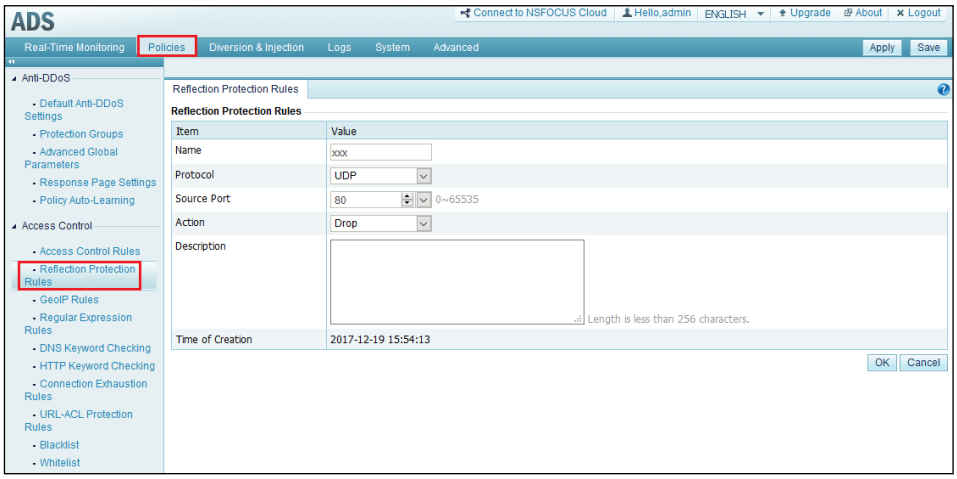
### Configuration

Reflection protection involves default reflection protection rules and group-specific reflection protection policy.

1. Configure reflection protection rules as follows:

Choose **Policies > Access Control > Reflection Protection Rules**, click **Add**, and configure parameters to create a reflection protection rule.

Figure 3-10 Configuring a reflection protection rule

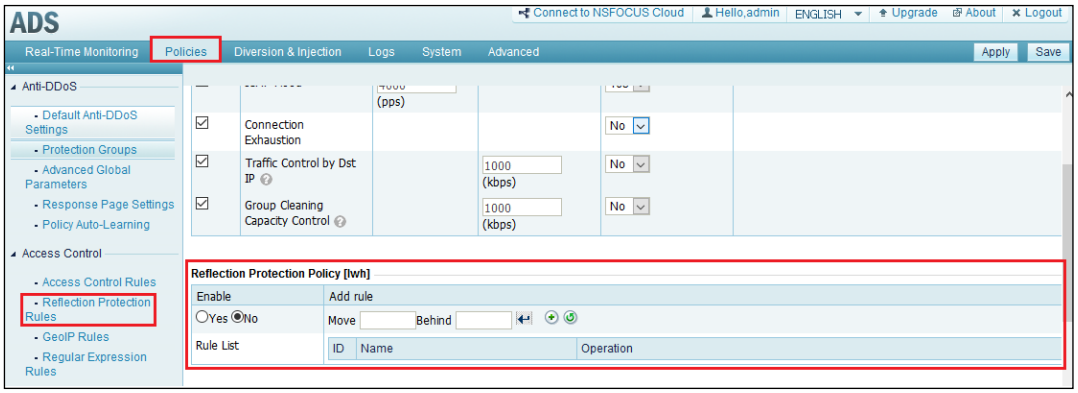



Initially, only CharGen, SSDP, NTP, DNS, SNMP, and MS SQL rules exist.

2. Configure a reflection protection policy for a protection group as follows:

Choose **Policies > Protection Groups**, click in the **Edit Policy** column of a protection group, and then set parameters in the **Reflection Protection Policy** area.

Figure 3-11 Configuring the reflection protection policy for a protection group




## 3.3.4 Rate Limiting Added as an Action for Static Rules

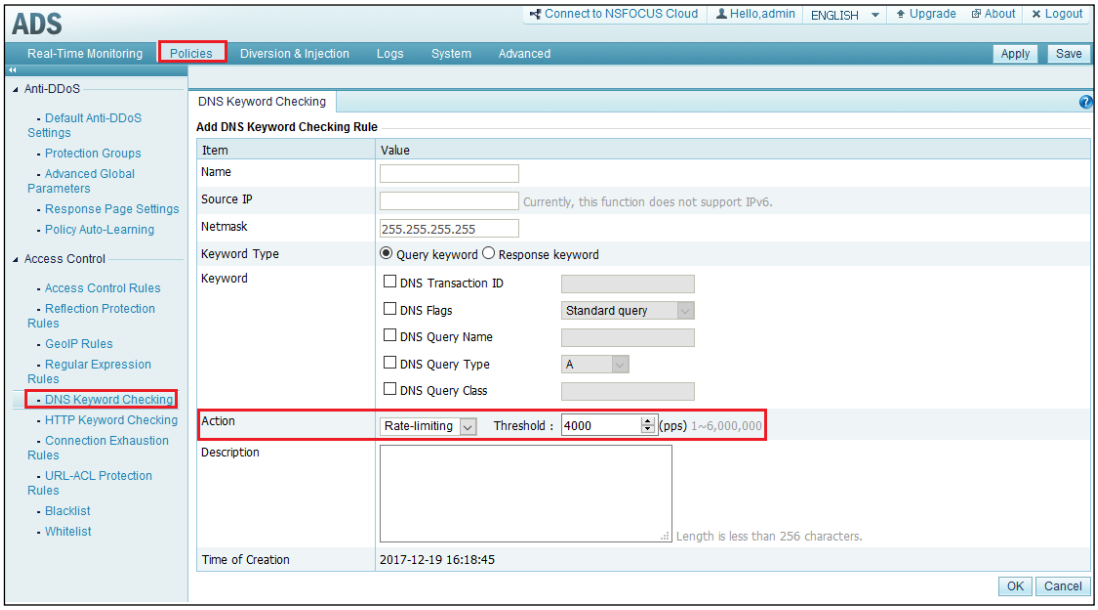
### Function Description

For protection against attacks that no intelligent protection algorithm can defeat, you can configure static filtering rules based on attack signatures. However, such rules do not provide very accurate protection. In previous versions, static rules provide only two actions: drop and add to the blacklist. In V4.5R90F00, the following types of static rules provide the rate limiting action to protect against attacks while ensuring legitimate users' access to the server: HTTP keyword checking rules, DNS keyword checking rules, regular expression rules, and pattern matching rules.

## Configuration

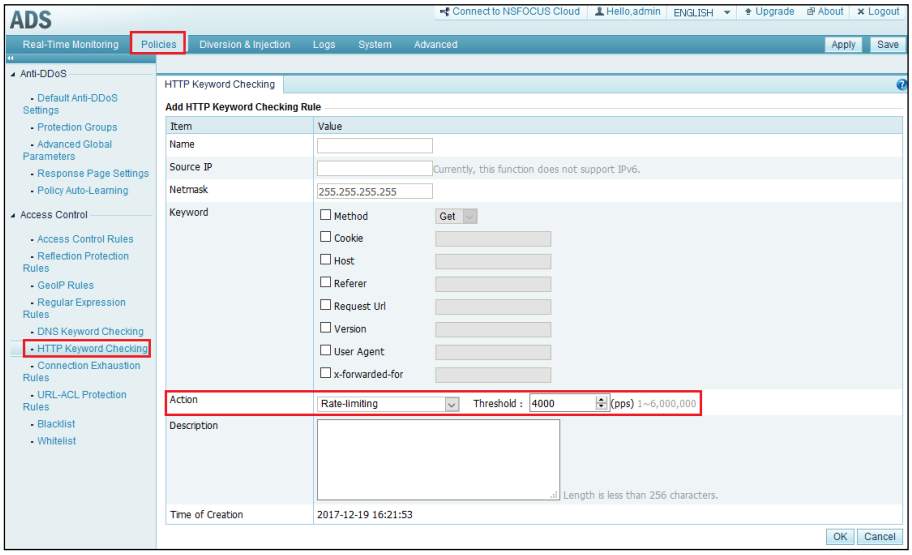
For a DNS keyword checking rule, choose **Policies > Access Control > DNS Keyword Checking**.

Figure 3-12 Configuring the rate limiting action for a DNS keyword checking rule



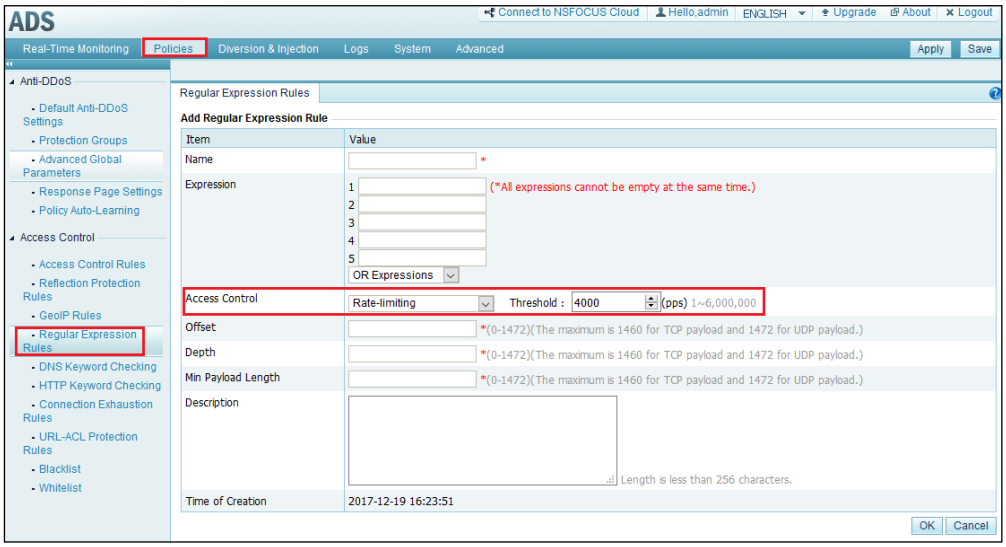

For an HTTP keyword checking rule, choose **Policies > Access Control > HTTP Keyword Checking**.

Figure 3-13 Configuring the rate limiting action for an HTTP keyword checking rule



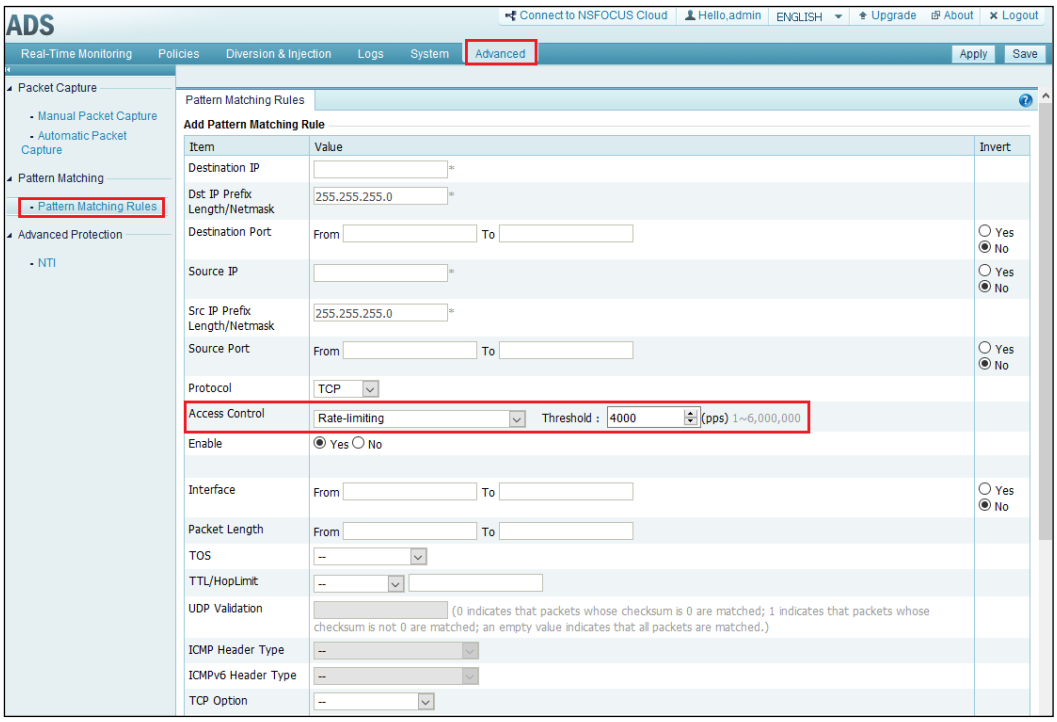

For a regular expression rule, choose **Policies > Access Control > Regular Expression Rules**.

Figure 3-14 Configuring the rate limiting action for a regular expression rule




For a pattern matching rule, choose **Advanced > Pattern Matching > Pattern Matching Rules**.

Figure 3-15 Configuring the rate limiting action for a pattern matching rule




## Notes

- HTTP keyword checking rules, DNS keyword checking rules, and regular expression rules can be applied globally or for a specific protection group. In the latter case, rate limiting applies to packets to or from a group, limiting the number of packets allowed to pass through per second.

- Pattern matching rules are applied globally. Therefore, rate limiting applies to all packets matching such a rule, limiting the number of packets allowed to pass through per second.

## 3.3.5 UDP Regular Expression Protection Policy

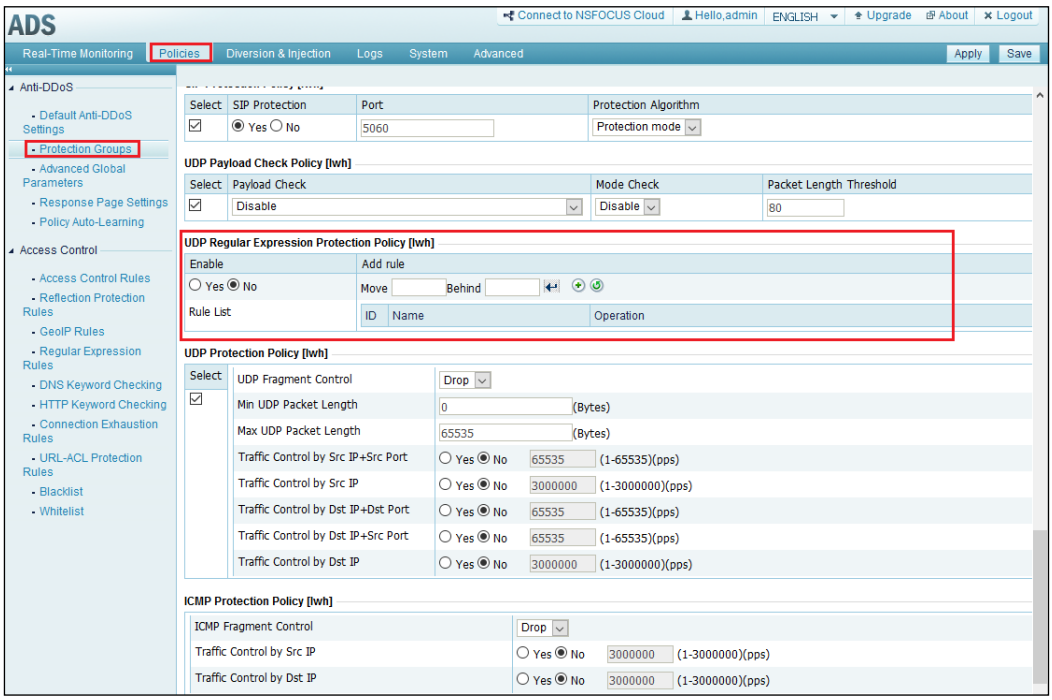
### Function Description

Regular expression rules are a common type of fuzzy matching rules. In previous versions, only TCP regular expression protection rules are supported. As the UDP-based attacks become more prevalent, V4.5R90F00 supports UDP regular expression protection rules as well.

### Configuration

Choose **Policies > Protection Groups**, click in the **Edit Policy** column, and configure parameters in the **UDP Regular Expression Protection Policy** area.

Figure 3-16 Configuring the UDP regular expression protection policy




### Notes

- For regular expression rules referenced by a UDP regular expression protection policy, the two access control actions, **Drop and disconnect** and **Drop** have the same protection result.
- For the sake of UDP protection, the maximum value of offset, depth, and minimum payload length in regular expression rules is increased to 1472.

# 3.3.6 Tcpdump Added as a New Method for Network Diagnosis

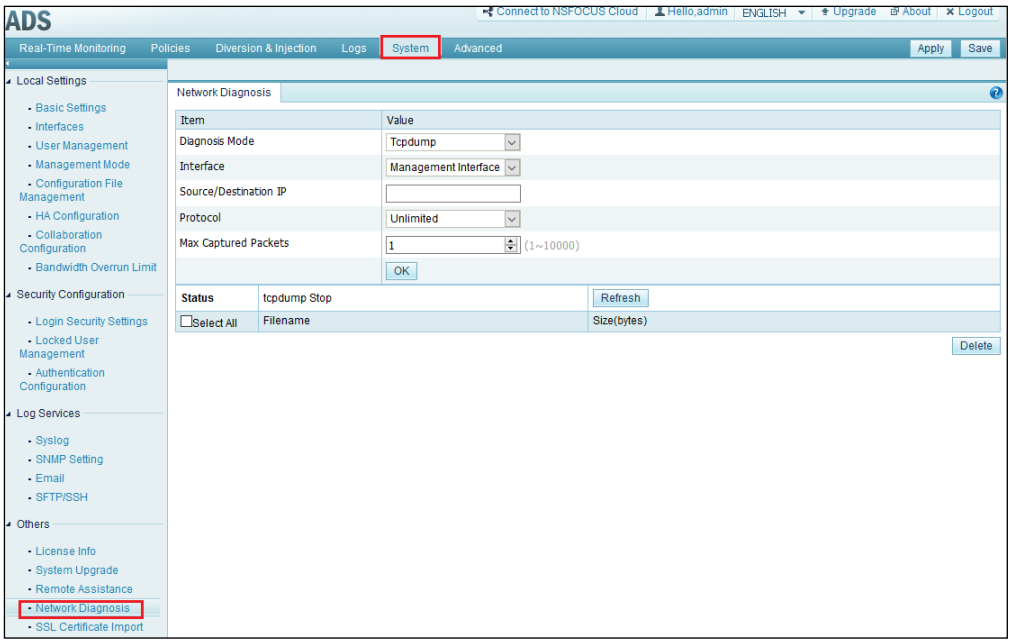
## Function Description

For on-site debugging of ADS deployed in out-of-path deployment mode, we often need to capture packets of specific protocols as well as ping and telnet packets that are received and sent by the local device. For this reason, tcpdump is added as a new method for network diagnosis in V4.5R90F00 to capture packets on the management interface or other interfaces of ADS.

## Configuration

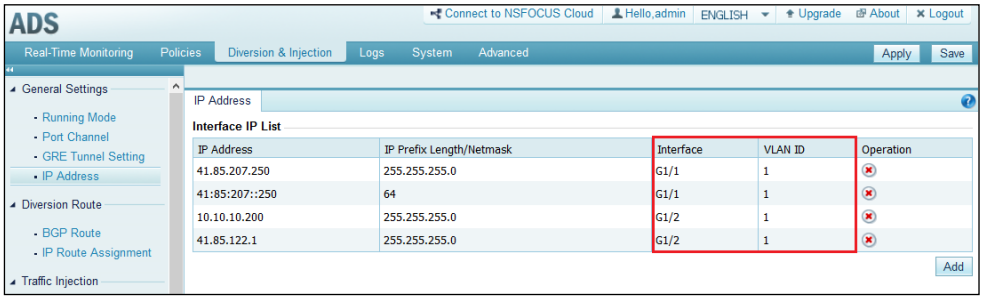
Choose **System > Network Diagnosis** and select **Tcpdump** for **Diagnosis Mode**.

Figure 3-17 Network diagnosis via packet capture with tcpdump




The tcpdump diagnosis function provides several parameters:

- **Interface**: including the management interface and the interfaces plus VLAN IDs provided by the interface IP address list.



- **Protocol**: Options include **Unlimited**, **TCP**, **UDP**, **ICMP**, and **ICMPv6**.
- At most five packet capture files can be saved.

## 3.3.7 Optimization of the Page of Manual Traffic Diversion

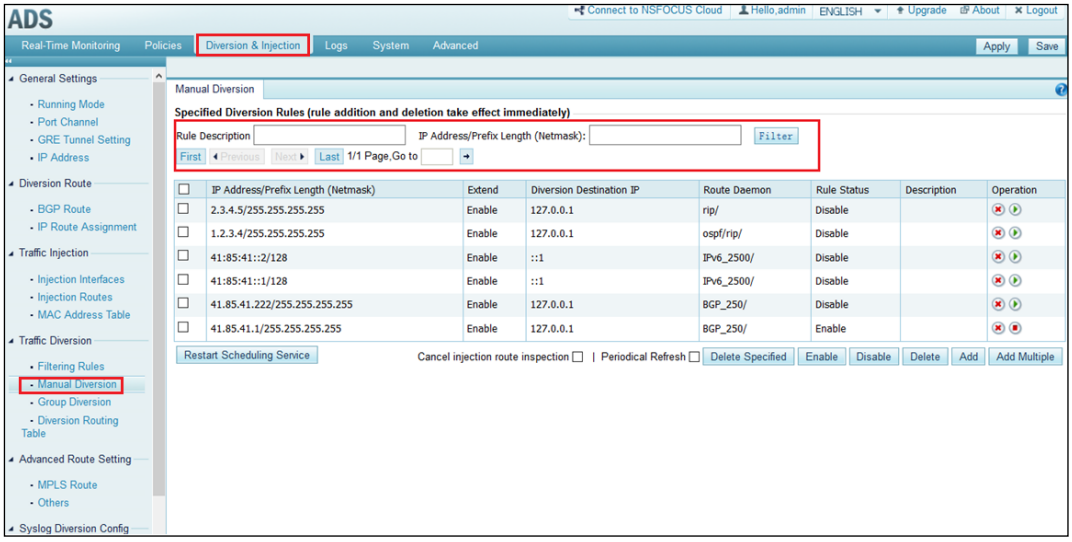
### Function Description

The page of manual traffic diversion rules supports pagination and rule query, allowing users to manage specific rules among numerous ones in an easy and rapid way.

### Configuration

Choose **Diversion & Injection > Traffic Diversion > Manual Diversion**.

Figure 3-18 Manual traffic diversion page




- The pagination mechanism is added to show at most 20 entries on each page.
- **Rule Description** supports fuzzy matching of the description specified with the **Description** parameter.
- **IP Address/Prefix Length** specifies an IP segment or an IP address and its netmask. For example, after you type **1.1.0.0/16** and click **Filter**, manual traffic diversion rules for this IP segment (1.1.1.0/24 and 1.1.1.1/32) will be retrieved. IPv6 addresses are also supported.
- If both **Rule Description** and **IP Address/Prefix Length** are specified, manual traffic diversion rules will be displayed only when they meet the two conditions.

## 3.3.8 Verification Codes Added as an Option for Login Authentication

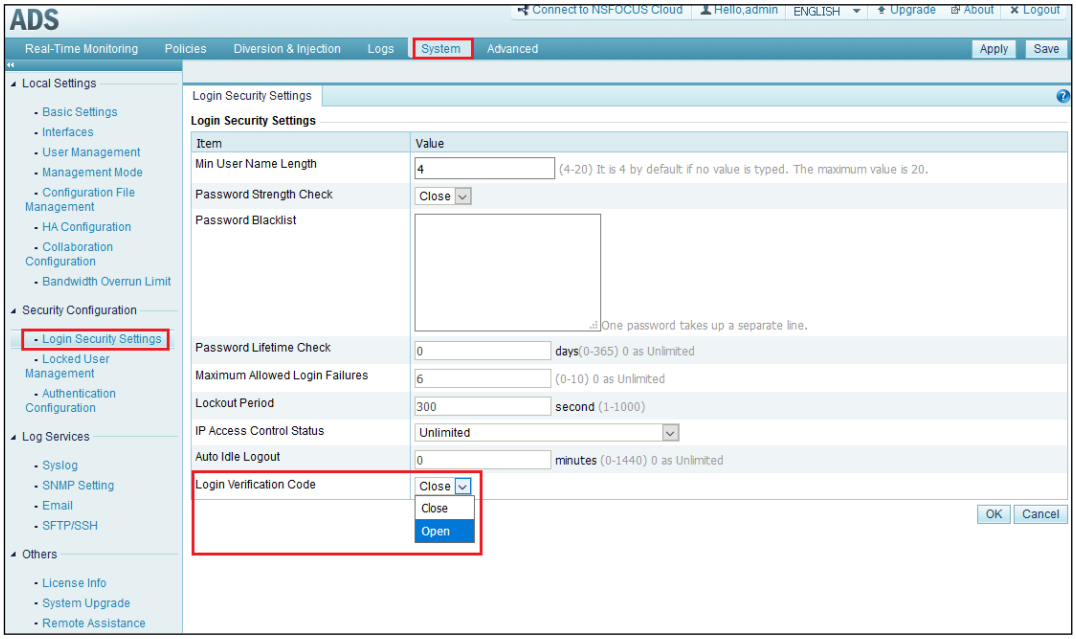
### Function Description

To enhance login security, verification codes are added as an option for user authentication on the login page. This option is disabled by default, and you can enable it manually.

## Configuration

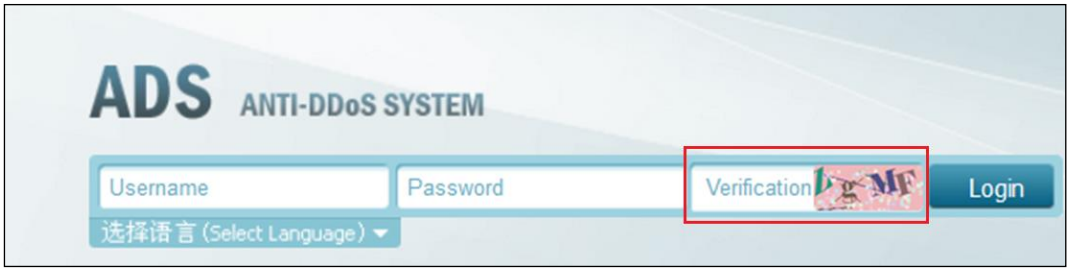
Choose **System > Login Security Settings** and select **Open** for **Login Verification Code**.

Figure 3-19 Using login verification codes




After the authentication with verification codes is enabled, users need to type the displayed verification codes upon login.

Figure 3-20 Verification codes displayed on the login page




## Notes

- If you cannot see the verification code clearly, click it to refresh.
- For a login to an ADS device from ADS M, no verification codes are displayed on the login page even if this function is enabled on ADS.

## 3.3.9 Sequence of Certain Access Control Rules Being Adjustable

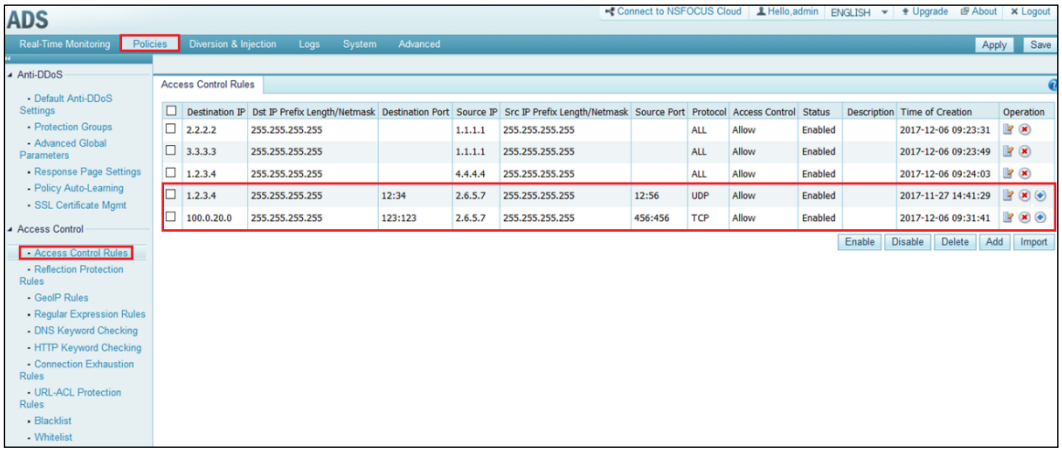
### Function Description

Access control rules are matched in a top-down manner. Such rules cannot be sorted as required by users in previous versions, and therefore it is impossible to adjust the priority of those rules. V4.5R90F00 allows users to adjust the sorting of certain access control rules to change their matching priority.

### Configuration

Choose **Policies > Access Control**.

Figure 3-21 Access control rules




### Notes

- Access control rules can be sorted as required only when the destination IP address is not 0.0.0.0 (indicates all destination IP addresses) and neither the source port nor destination port is empty.
- Access control rules can be moved up, down, or to the top or bottom.

## 3.3.10 Optimization of the Blacklist and Whitelist

### Function Description

The blacklist and whitelist are the most frequently used filtering rules during DDoS protection. V4.5R90F00 optimizes the whitelist and blacklist as follows:

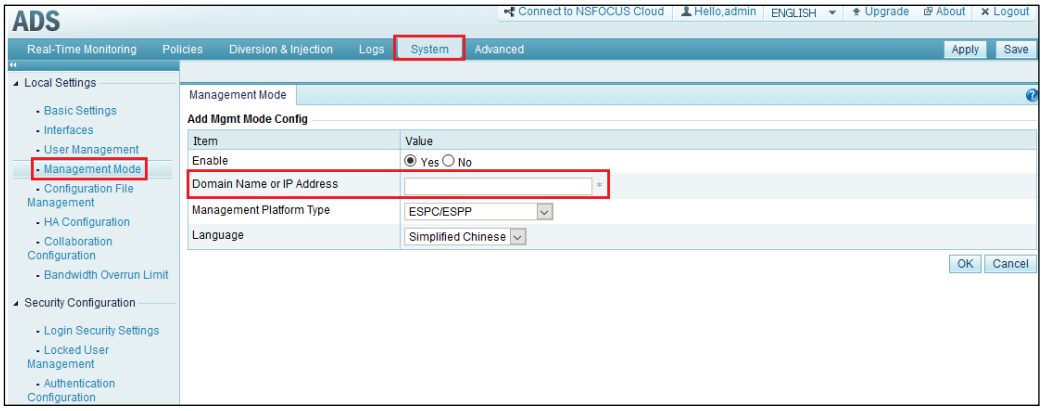
- The whitelist works independently and provides a collision handling mechanism. More IP addresses can be added to the whitelist.
- The blacklist has an increased capacity and provides a collision handling mechanism. Also, the number of blacklist entries doubles under equal conditions.

## 3.3.11 Domain Name Allowed for ESPC/ESPP

### Function Description

The domain name of NSFOCUS ESPC or ESPP may constantly change. For this reason, V4.5R90F00 allows users to enter the domain name of NSFOCUS ESPC or ESPP.

### Configuration



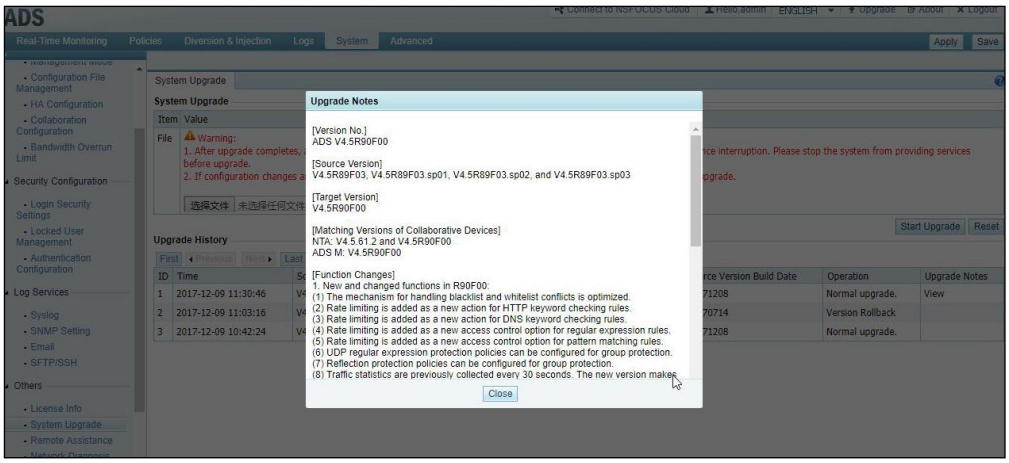

### Notes

You need to configure the domain name of ESPC or ESPP only when **Management Platform Type** is set to **ESPC/ESPP**.

## 3.3.12 Upgrade Notes Viewable After Upgrade

### Function Description

In V4.5R89F03, the system shows upgrade notes during upgrade, including the version number, function description, and things to note. However, the upgrade notes disappear after the upgrade. V4.5R90F00 adds a query interface on the web-based manager to allow users to check upgrade notes even after the upgrade.



### Notes

The upgrade notes are available only for the last upgrade package, but not for earlier ones.

## 3.4 Compatibility with NTA Versions

ADS V4.5R90F00 supports IPv4/IPv6 collaboration with NTA V4.5R90F00 and IPv4 collaboration with NTA V4.5.61.2.BF19 or V4.5.61.2.BF20.

## 3.5 Supported Browsers

Internet Explorer 9 and 10 and Chrome browsers are supported.

# 4 Version Upgrade

ADS can be upgraded to V4.5R90F00 from V4.5R89F03, V4.5R89F03.sp01, V4.5R89F03.sp02, or V4.5R89F03.sp03.

## 4.1 Upgrade from V4.5R89F03, V4.5R89F03.sp01, V4.5R89F03.sp02, or V4.5R89F03.sp03 to V4.5R89F01

The following models are supported:

- ADS NX3-200E/600E/800E
- ADS NX3-2010/2020/2020E
- ADS NX5-4020/4020E/6025/6025E/NX5-8000

The upgrade procedure is as follows:

**Step 1** Apply the upgrade package, **update_ADS_x86_V4.5R90F00_20180110.zip** (MD5: 72812CD3C97F9A4B3531D057D7F2277F), on the source version. After the system prompts that the upgrade succeeds, restart the device.

**Step 2** Verify that the system version is V4.5R90F00.

**----End**

| | |
|---|---|
| Note | If the upgrade fails in step 1, contact the technical support personnel of NSFOCUS. After the problem (if any) is resolved, run the rollback command in the CLI window to roll ADS back to the source version. If the rollback succeeds, the device will automatically restart. Then repeat the preceding steps to upgrade to V4.5R90F00. |

## 4.2 Rollback to V4.5R89F03 or V4.5R89F03.sp0x from V4.5R90F00

The following models are supported:

- ADS NX3-200E/600E/800E
- ADS NX3-2010/2020/2020E
- ADS NX5-4020/4020E/6025/6025E/NX5-8000

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

# A IPv4/IPv6 Support

The following table lists the support of modules in ADS V4.5R90F00 for IPv4 and IPv6.

| Module | Function | IPv4 | IPv6 |
|---|---|---|---|
| Real-Time Monitoring | | | |
| Policies | SYN flood detection | √ | √ |
| | ACK flood detection | √ | √ |
| | UDP flood detection | √ | √ |
| | ICMP flood detection | √ | √ |
| | HTTP protection | √ | √ |
| | HTTPS protection | √ | × |
| | DNS protection algorithms 1 and 2 | √ | √ |
| | DNS protection algorithm 3 | √ | × |
| | DNS protection algorithm 4 | √ | √ |
| | TCP control parameters | √ | √ |
| | TCP control parameters – TCP fragment control | √ | × |
| | IP behavior control | √ | × |
| | SIP protection – default DDoS | √ | × |
| | SIP protection – groups | √ | √ |
| | UDP payload check – payload check | √ | √ |
| | UDP payload check – mode check | √ | × |
| | UDP protection – UDP fragment control | √ | × |
| | ICMP fragment control | √ | × |
| | UDP protection – drop UDP fragments – groups | √ | × |
| | UDP protection – maximum packet length | √ | √ |
| | UDP protection – traffic control by Src IP + Src port | √ | √ |
| | UDP protection – traffic control by Dst IP + Dst port | √ | √ |
| | UDP protection – traffic control by Src IP | √ | √ |

| Module | Function | IPv4 | IPv6 |
|---|---|---|---|
| | UDP protection – traffic control by Dst IP | √ | √ |
| | UDP protection – minimum packet length | √ | √ |
| | UDP protection – traffic control by Dst IP + Src port | √ | √ |
| | ICMP traffic rate limiting | √ | √ |
| | Watermark protection | √ | × |
| | Protocol ID check | √ | √ |
| | Group traffic control | √ | √ |
| | Port check | √ | √ |
| | URL rules | √ | √ |
| | Advanced global parameters | √ | √ |
| | Policy auto-learning | √ | √ |
| | Access control rules | √ | √ |
| | Reflection protection rules | √ | √ |
| | GeoIP rules | √ | √ |
| | Regular expression rules | √ | × |
| | Hardware access control rules | √ | √ |
| | Connection exhaustion rules | √ | × |
| | URL-ACL protection rules | √ | √ |
| | Blacklist | √ | × |
| | Whitelist | √ | √ |
| | HTTP keyword checking | √ | × |
| | DNS keyword checking | √ | × |
| Diversion & Injection | Running mode | √ | √ |
| | Port channel configuration | √ | √ |
| | IP address configuration | √ | √ |
| | BGP diversion | √ | √ |
| | OSPF diversion | √ | √ |
| | ISIS diversion | √ | × |
| | RIP diversion | √ | × |
| | LDP diversion | √ | × |
| | IP route assignment | √ | √ |
| | Injection interface | √ | √ |
| | Layer 2 injection | √ | √ |

| Module | Function | IPv4 | IPv6 |
|---|---|---|---|
| | Layer 3 injection | √ | √ |
| | MPLS injection | √ | × |
| | MPLS VPN injection | √ | × |
| | GRE tunnel injection | √ | × |
| | MAC address table | √ | √ |
| | Filtering rules | √ | √ |
| | Manual diversion | √ | √ |
| | Group diversion | √ | √ |
| | Diversion routing table | √ | √ |
| | MPLS route | √ | × |
| | Syslog diversion configuration – collaboration with Genie devices | √ | × |
| | Syslog diversion configuration – collaboration with Arbor devices | √ | × |
| | Syslog diversion configuration – collaboration with Samurai devices | √ | × |
| | Syslog diversion configuration – collaboration with Kuanguang devices | √ | × |
| Collaboration | Collaboration with ADS M | √ | √ |
| | Collaboration with ESPP | √ | × |
| | Collaboration with NTA V4.5.61.2 | √ | × |
| | Collaboration with NTA V4.5R90F00 | √ | √ |
| Logs | Attack logs | √ | √ |
| | System operation logs | √ | √ |
| | System login logs | √ | √ |
| | Link status logs | — | — |
| | Traffic diversion logs | √ | √ |
| | HA synchronization logs | √ | √ |
| | Syslog diversion logs | √ | × |
| System | Basic settings | √ | √ |
| | Interface link configuration | — | — |
| | System user management | √ | √ |
| | Management mode configuration | √ | √ |
| | Configuration file management | √ | √ |
| | HA configuration | √ | √ |

| Module | Function | IPv4 | IPv6 |
|---|---|---|---|
| | Collaboration configuration | √ | × |
| | Bandwidth overrun limit | √ | × |
| | Login security settings | √ | × |
| | Locked user management | √ | × |
| | Authentication configuration | √ | √ |
| | Syslog configuration | √ | √ |
| | SNMP trap configuration | √ | √ |
| | SNMP agent setting | √ | × |
| | Email configuration | √ | √ |
| | SFTP/SSH log export | √ | × |
| | License interface | — | — |
| | License speed limit | — | — |
| | System upgrade | — | — |
| | Remote assistance | — | — |
| | SSL certificate import | — | — |
| | One-click information collection | — | — |
| | Version information | — | — |
| Advanced | Packet capture management | √ | √ |
| | Pattern matching rules | √ | √ |
| NTI | Upload | √ | √ |
| | Synchronization | √ | × |
| | Query | √ | × |