NSFOCUS ADS M
User Guide

Version: V4.5R90F04 (2022-09-29)

Confidentiality: RESTRICTED

■ Statement

The purchased products, services, or features are stipulated in the contract made between NSFOCUS and the customer. Part of products, services, and features described in this document may not be within the purchased scope or the usage scope.

All information in this document is provided "AS-IS" without guarantees of any kind, express or implied. The information in this document is subject to change without notice. It may slightly differ from the actual product due to version upgrade or other reasons.

■ Disclaimer

Please read the disclaimer carefully before using the product. Once you use the product, you acknowledge and agree to all the contents of this disclaimer. NSFOCUS shall not assume any responsibility for any loss or damage in the following circumstances:

- Data loss and system availability reduction caused by the negligence or misconduct of the system O&M or management personnel, for example, they do not handle alerts that affect system stability and availability in a timely manner.

- Data loss and system availability reduction caused by the fact that the traffic exceeds the planned hardware capacity.

- Data loss and system availability reduction or unavailability caused by natural disasters (including but not limited to floods, fires, and earthquakes) or environmental factors (including but not limited to network disconnection and power outage).

Contents

Preface

Scope

This document describes all functions and usage of ADS NX3-M1600E and ADS-M NX3-HD2700 (ADS M) in detail. It provides guidance in use of ADS M products. Descriptions here may slightly differ from actual products due to version upgrade or other reasons.

Organization

Chapter	Overview
1 Overview	Describes ADS M briefly.
2 Web-based Manager	Describes the login method and layout of the web-based manager.
3 System Management	Describes how to perform system management and maintenance.
4 Traffic Monitoring	Describes in detail the traffic and attacks monitored by the managed devices.
5 Reports	Describes various types of reports and how to query these reports.
6 Logs	Describes how to view device logs.
7 Region Management	Describes how to configure device regions and region IP groups.
9 Device Management	Describes device management, policy configuration, and abnormal traffic detection.
10 Console-based System Management	Describes menus of the console management interface.
A Parameters	Describes parameters of policy templates.
B Default Parameters	Introduces default settings of ADS M.

Change History

Version	Description
V4.5R90F04	• Updated the structure based on the new template. • Added license expiration warning, web API logs, cluster GeoIP library, and cluster NTI, etc. • Modified access policies and DDoS attack alert rules.

Conventions

Convention	Description
Bold font	Keywords, names of screen elements like buttons, drop-down lists or fields, and user-entered text appear in bold font.
Italic font	Document titles, new or emphasized terms, and arguments for which you supply values are in italic font.
Note	Reminds users to take note.
Tip	Indicates a tip to make your operations easier.
Caution	Indicates a situation in which you might perform an action that could result in equipment damage or loss of data.
Warning	Indicates a situation in which you might perform an action that could result in bodily injury.
A > B	Indicates selection of menu options.

Technical Support

Hardware and Software Support

Email: support@nsfocusglobal.com

Cloud Mitigation Support

Email: cloud-support@nsfocusglobal.com

Phone:

- USA: +1-844-673-6287 or +1-844-NSFOCUS
- UK: +44 808 164 0673 or +44 808 164 0NSF
- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Netherlands: +31 85 208 2673 or +31 85 208 2NSF
- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757
- Hong Kong: +852 5803 2673 or +852 5803 2NSF
- Middle East: +973 1619 7607

Documentation Feedback

For any query regarding the usage of the documentation, you can contact us:

Email: info-support@nsfocus.com

1 Overview

ADS M is used to perform centralized management over ADS devices deployed in cluster mode and to generate reports. ADS M monitors traffic and operating status of multiple ADS devices, collects traffic information and attack alerts from these devices, and displays the collected information on the web-based manager. On the web-based manager, the administrator, in a unified way, can modify configuration files of ADS devices on ADS M and then dispatch these files to ADS devices.

2 Web-based Manager

This chapter mainly covers:

Section	Description
Login	Describes methods for logging in to the system.
Layout	Describes the web page layout.
Other Operations	Describes how to switch the language and reset the password.

2.1 Login

To log in to the web-based manager of ADS M, follow these steps:

Step 1 Make sure that your PC properly communicates with ADS M.

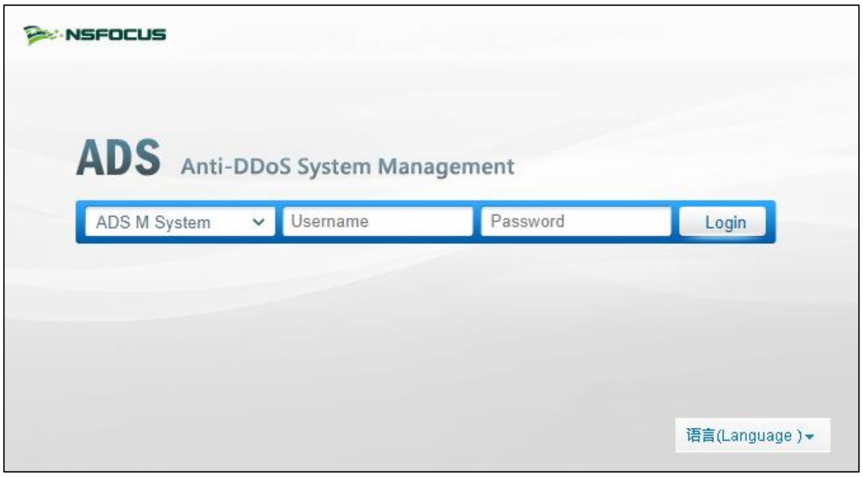
Step 2 Open a browser (for example, Chrome) and connect to the IP address of the management interface of ADS M over HTTPS, for example, type **https://192.168.1.100** in the address bar.

After you type the IP address and press **Enter**, a security alert page appears.

Step 3 Click **Advanced** and then **Proceed to xxxx (unsafe)**.

The login page of the web-based manager appears, as shown in Figure 2-1.

Figure 2-1 Login page



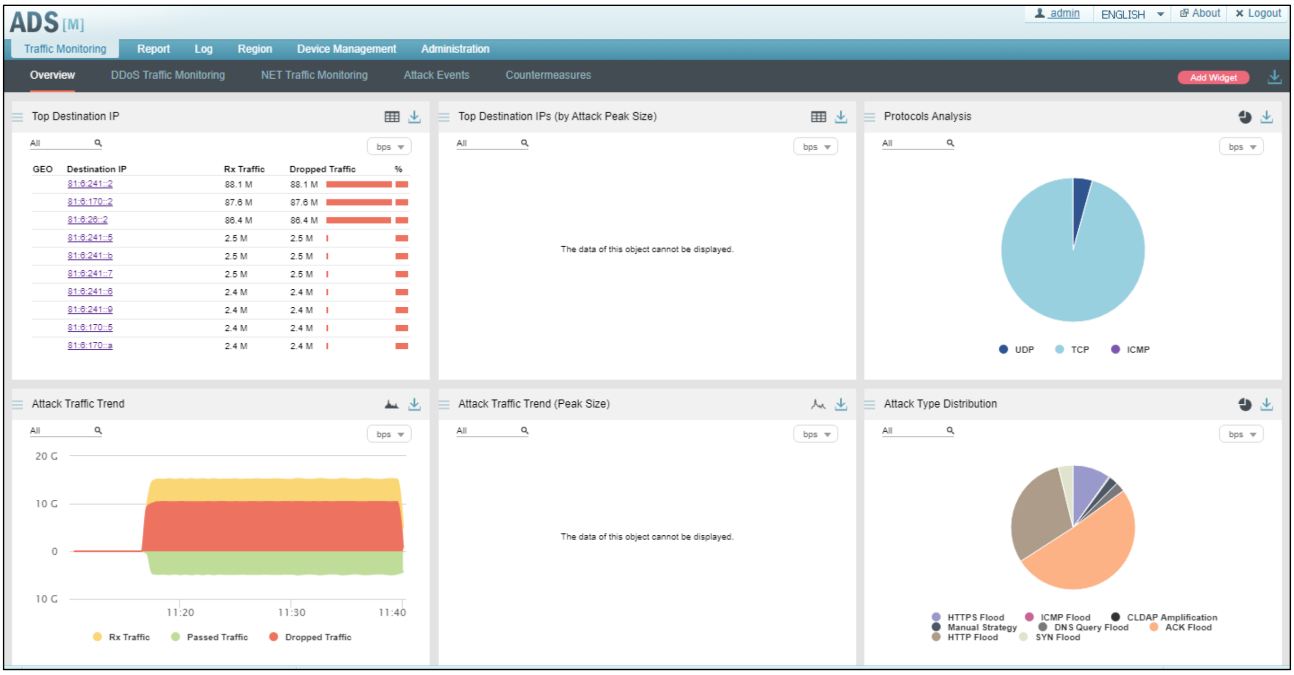
Step 4 Select **ADS M System**, type the correct user name and password, and then click **Login** or press **Enter** to log in to the web-based manager.

Note

- During the first login to ADS M that has just been upgraded to V4.5R90F00, the configuration wizard appears. You can log in to the system only after you set the locality, system time zone, and system time, but do not need to change the initial password. For details, see the *NSFOCUS ADS M Installation Guide*.
- During the first login to the web-based manager with the initial user name and password, the configuration wizard appears only after you change the initial password.

For the first login, you must import a valid license before using the system. After a successful login, the web-based manager appears, as shown in Figure 2-2.

Figure 2-2 Homepage



GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:241::2	88.1 M	88.1 M	
	81:6:170::2	87.6 M	87.6 M	
	81:6:26::2	86.4 M	86.4 M	
	81:6:241::5	2.5 M	2.5 M	
	81:6:241::b	2.5 M	2.5 M	
	81:6:241::7	2.5 M	2.5 M	
	81:6:241::6	2.4 M	2.4 M	
	81:6:241::9	2.4 M	2.4 M	
	81:6:170::5	2.4 M	2.4 M	
	81:6:170::a	2.4 M	2.4 M	

The data of this object cannot be displayed.

The data of this object cannot be displayed.

----End

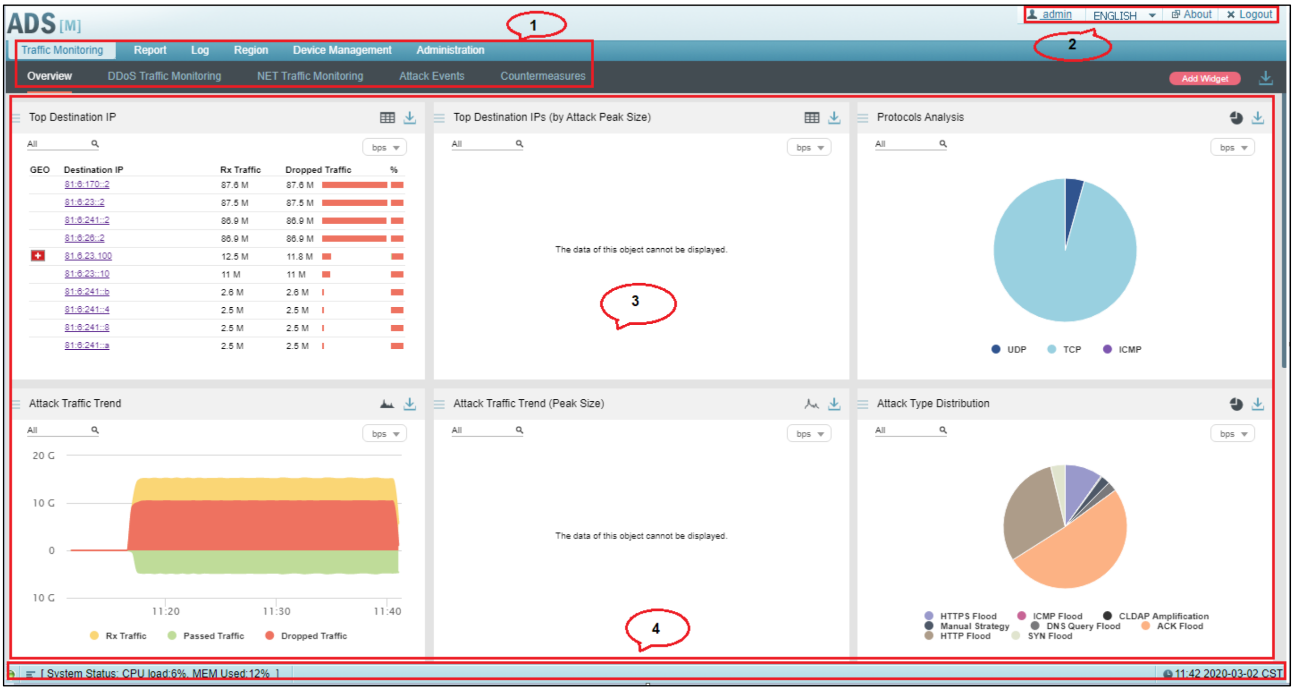
Caution

- The browser you use must support JavaScript, cookies, and frames.
- You are advised to use Internet Explorer 11 or later, Chrome, or Firefox and set the display resolution to 1280 x 700 or higher. If you use the IE-based tabbed browsers (such as MyIE and Maxthon), pages may be displayed improperly.
- You must change the password immediately after the first login.
- The system will return to the login page if you remain inactive on a page other than the five tab pages of the **Traffic Monitoring** module for over 10 minutes after successful login. The system does not automatically log you out of a tab page under **Traffic Monitoring** no matter how long you stay inactive on this page.
- For the first login, you must import a valid license before using the system. For how to import a license, see section 3.1.2 License.

2.2 Layout

Figure 2-3 shows the layout of the web-based manager.

Figure 2-3 Layout of the web-based manager



GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:170::2	87.6 M	87.6 M	
	81:6:23::2	87.5 M	87.5 M	
	81:6:241::2	86.9 M	86.9 M	
	81:6:26::2	86.9 M	86.9 M	
	81.6.23.100	12.5 M	11.8 M	
	81:6:23::10	11 M	11 M	
	81:6:241::b	2.6 M	2.6 M	
	81:6:241::4	2.5 M	2.5 M	
	81:6:241::8	2.5 M	2.5 M	
	81:6:241::a	2.5 M	2.5 M	

[System Status: CPU load:6%, MEM Used:12%]

Table 2-1 describes areas of the web-based manager.

Table 2-1 Webpage layout

No.	Area	Description
1	Menu bar	Main menus of the system.
2	Quick access bar	Provides buttons for common operations on the web-based manager. admin : enables you to modify your information. See section 3.2.1 User Management for details.

No.	Area	Description
		ENGLISH ▾: switches between languages. About : displays product information of ADS M devices. ✖ Logout : logs you out of the system.
3	Work area	Area where you can perform configurations and operations and view data.
4	Status bar	Displays the current system time and system status. Clicking in the left part of the status bar shows details of the CPU usage, memory usage, and data partition usage.

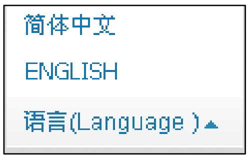
2.3 Other Operations

On the web-based manager, you can also switch the language and reset the password.

Switching the Language

On the login page shown in Figure 2-1, move the cursor to the **Language** button in the lower-right corner. Then all languages available are automatically displayed, as shown in Figure 2-4. Click the desired language. The interface language is now changed to the one that you selected.

Figure 2-4 Language options



Resetting the Password

On the login page shown in Figure 2-1, click **Forgot Password** in the lower-right corner. On the **Reset Password** page, type the correct user name and email address, and then click **Next**. After that, the system automatically sends a link for resetting the password to your registered email address.

Note	• Only the user **admin** can enable the password resetting function. In addition, the login page displays **Forgot Password** only after you enable **Reset Password** on the **Security Settings** page. For how to enable password resetting, see section 3.2.2 Security Settings. • When you reset the password, you must type the same email address as the one that you used to register. This email address must be a valid one; otherwise, you would not receive the password resetting email. • The password resetting function also requires a Simple Mail Transfer Protocol (SMTP) server. For details, see section 3.3.5 SMTP Server Configuration.

3 System Management

This chapter describes routine management and maintenance of ADS M via the web-based manager, mainly including:

Section	Description
Local Settings	Describes the basic configurations of ADS M.
User and Audit	Describes how to perform ADS M user management, security settings, authentication configuration as well as how to view audit logs.
Third-Party Interface	Describes the third-party interface configuration.
Diagnosis	Describes methods to diagnose ADS M faults.

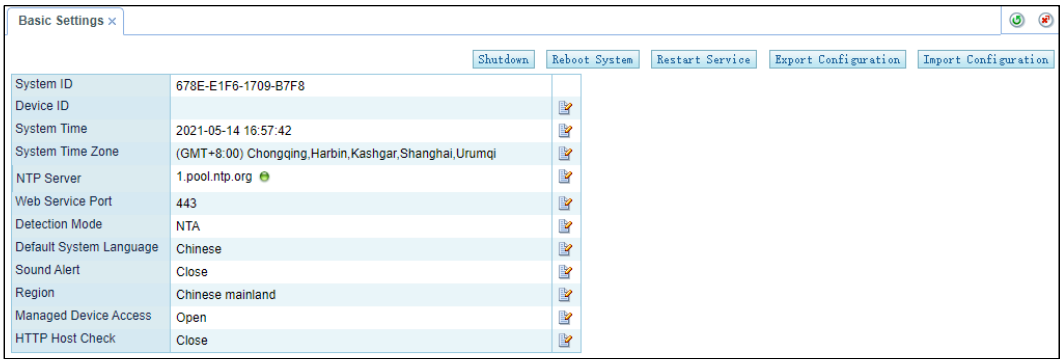
3.1 Local Settings

This section describes basic configurations of ADS M.

3.1.1 Basic Settings

Choose **Administration > Local Settings > Basic Settings**. As shown in Figure 3-1, the **Basic Settings** page displays basic system information. You can click 📝 to edit the device ID, system time, NTP server, and default system language, except system ID that identifies the system uniquely.

Figure 3-1 Basic system information



System ID	678E-E1F6-1709-B7F8
Device ID	
System Time	2021-05-14 16:57:42
System Time Zone	(GMT+8:00) Chongqing,Harbin,Kashgar,Shanghai,Urumqi
NTP Server	1.pool.ntp.org ●
Web Service Port	443
Detection Mode	NTA
Default System Language	Chinese
Sound Alert	Close
Region	Chinese mainland
Managed Device Access	Open
HTTP Host Check	Close

Table 3-1 describes detailed system information.

Table 3-1 Basic system information

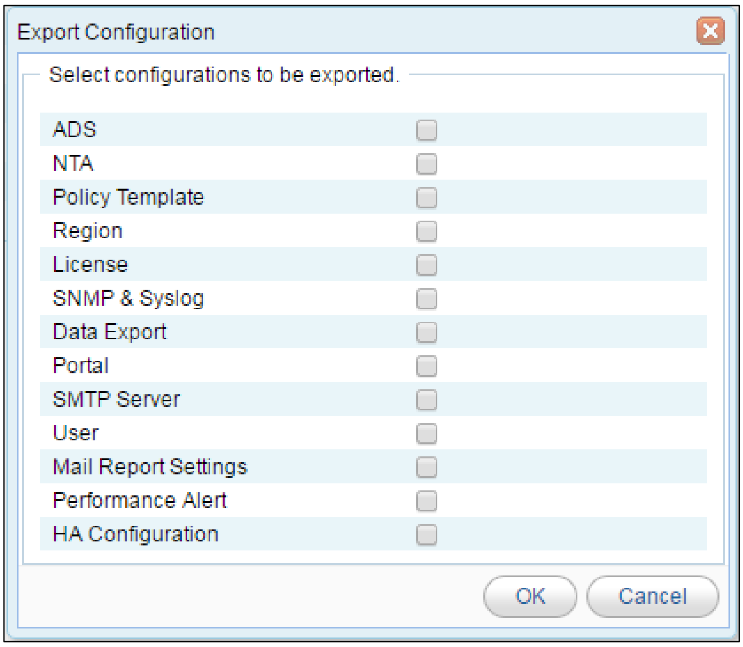
Parameter	Description
System ID	Hardware ID of ADS M.
Device ID	Name of ADS M.
System Time	Current system time, in the format of 2012-09-27 17:07:07. Changing the system time may cause a loss of certain data. Therefore, you must perform this operation with caution.
System Time Zone	Time zone of the system time. When daylight saving time (DST) is used, the page will prompts a message, indicating that the clock is automatically adjusted based on the DST.
NTP Server	IP address of the server with which ADS M synchronizes time. If **NTP Exception Alert** is turned on, once the NTP server becomes faulty, the system triggers an alert and generates a running alert log. For details, see section 3.1.8 Performance Alert Configuration of Managed Devices.
Web Service Port	Port via which you log in to the web-based manager of ADS M. The port number can be **80**, **443**, or any integer from 10000 to 65534. Assume that the IP address of ADS M is https://192.168.1.100. If the port number is changed to **80**, you need to type **https://192.168.1.100:80** in the address bar of the browser. Note Changing the web service port will cause the web-based manager of ADS M to restart. If the Portal is enabled, you also need to re-deploy the Portal.
Detection Mode	Detection mode adopted by the system. The default value is **NTA**, indicating that ADS M coordinates with NTA for traffic analysis. If there is no NTA, the default value is **None**, indicating that NTA coordination is unavailable.
Default System Language	Default language used by the system to save audit logs. The web-based manager supports both **Chinese** and **English**. The default language is **English**. The new default language takes effect only after the system is restarted.
Sound Alert	Controls whether to enable sound alerting. After sound alerting is enabled, the system makes a sound and displays an alert reminder box when either of the following conditions is met: • An attack alert or link status alert is generated by ADS. • A traffic alert is generated by NTA. For details about the sound alerting function, see section 4.1.6 Generating Sound Alerts.
Region	Country/Region where the device is used.
Managed Device Access	Enabled by default, indicating that you can directly access the managed ADS and/or NTA devices via ADS M. If this is disabled, you cannot access any managed devices via ADS M.
HTTP Host Check	Controls whether to enable the HTTP host check. This function is disabled by default. If the check is enabled, only interface IP addresses on the **Network**

Parameter	Description
	Settings page are used for web-based management.

In addition to adjusting basic system parameters, you can also perform the following operations:

- Shut down the system: Click **Shutdown** to shut down ADS M.
- Reboot the system: Click **Reboot System** to reboot ADS M.
- Restart system services: Click **Restart Service** to restart system service programs (including the web-based manager and engine) of ADS M. For example, after you change the default language, the system asks you to restart system services.
- Export configuration files: Click **Export Configuration** and select configuration items to be exported in the **Export Configuration** dialog box shown in Figure 3-2. Click **OK** to save the configuration file to a local disk drive.

Figure 3-2 Exporting configurations



Export Configuration

Select configurations to be exported.

ADS □
NTA □
Policy Template □
Region □
License □
SNMP & Syslog □
Data Export □
Portal □
SMTP Server □
User □
Mail Report Settings □
Performance Alert □
HA Configuration □

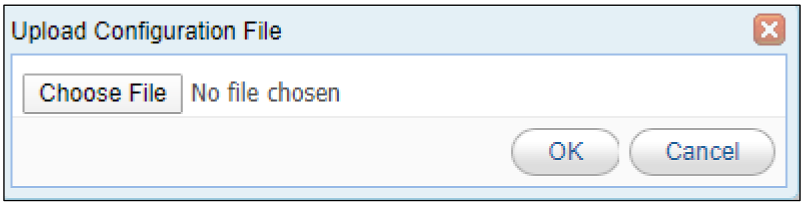
Note

The configuration files will be exported as an encrypted package which is not editable and can be used for backup or imported to the device.

- Import a configuration file.

  Click **Import Configuration** and upload a file in the **Upload Configuration File** dialog box shown in Figure 3-3 to overwrite the original configuration file. This operation reconfigures ADS devices, NTA devices, and policy templates.

Figure 3-3 Upload Configuration File dialog box



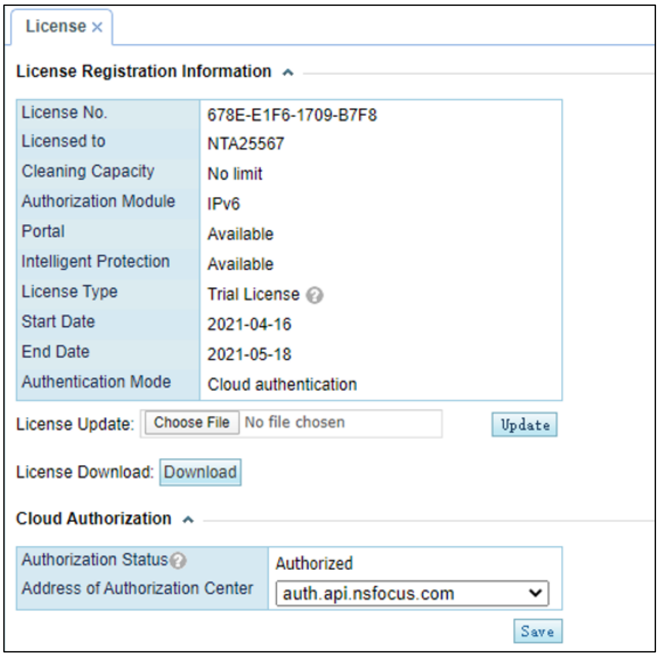
Note	
	• The imported configuration file takes effect only after the system restarts. • Certificates may be necessary to perform certain configurations. As different devices have different certificates, ensure that proper certificates are used. • The imported configuration file will overwrite the original one. Perform this operation with caution.

3.1.2 License

After an ADS M device is installed, you need to import a license before using it.

Choose **Administration** > **Local Settings** > **License**. On the **License** page, click **Choose File** to select a license file and then click **Update** to import a license. After it is imported, the **License** page displays the license information, as shown in Figure 3-4.

Figure 3-4 License page



License No.	678E-E1F6-1709-B7F8
Licensed to	NTA25567
Cleaning Capacity	No limit
Authorization Module	IPv6
Portal	Available
Intelligent Protection	Available
License Type	Trial License
Start Date	2021-04-16
End Date	2021-05-18
Authentication Mode	Cloud authentication

License Update: Choose File No file chosen Update

License Download: Download

Authorization Status	Authorized
Address of Authorization Center	auth.api.nsfocus.com

Table 3-2 describes license parameters.

Table 3-2 License parameters

Parameter		Description
License No.		License number of the current ADS M.
Licensed to		Customer that is authorized to use this system.
Cleaning Capacity		Maximum bandwidth allowed for traffic cleaning. **No limit** indicates no limit to the maximum bandwidth. Note This parameter is available only for an ADS M virtual machine.
Number of Monitored Devices		Maximum number of ADS devices that can be monitored by the current ADS M.
Authorization Module		Whether the IPv6 module is available.
Intelligent Protection		Whether intelligent protection is available.
Portal		Whether ADS Portal is available.
License Type		License type, which may be **Trial** or **Paid**.
Start Date		Start date of the license validity, which is usually the production date of the current license.
End Date		End date of the license validity. If a trial license expires, ADS M can be upgraded but no longer collects data of ADS devices under it. That is, ADS M loses the protection function. If a paid license expires, ADS M still works but cannot be upgraded.
Authentication Mode		Authentication mode, which can be local authentication or cloud authentication. This parameter is available only for ADS-M-VM. Meanwhile, ADS-M-VM can be used only after it is authenticated locally or connected to the cloud authorization center.
Ukey Hash		Hash of the USB flash drive inserted into host the device where the software of the locally authenticated device runs.
Authorization Status	Local	Local authorization status of the device. If local authentication is configured, ADS-M-VM, upon startup, sends authentication requests to the USB flash drive inserted to it. The local authorization status can be either of the following: • **Authorized**: The device is authorized and ready to use. • **Unauthorized**: The system cannot be upgraded, nor does it support device addition, region configuration, or traffic statistics.
	Cloud	Cloud authorization status. After you configure the address of the cloud authorization center, ADS-M-VM, upon startup, sends authentication requests to the cloud.

Parameter		Description
		• **Authorized**: indicates that the address of the cloud authorization center is correct and the connection to the cloud is properly established. Then, the device is available for use. • **Offline**: In the authorized state, if an incorrect authorization center address is typed, the authorization status turns to **Offline**. An offline device provides all functions except system upgrade within 30 days. Upon the expiry of the period, the device enters the unauthorized state. • **Unauthorized**: The system cannot be upgraded, nor does it support device addition, region configuration, or traffic statistics. • **Authentication failure**: The device provides all functions except system upgrade within 30 days. Upon the expiry of the period, the device enters the unauthorized state. During its operation, ADS-M-VM periodically sends authentication requests to the cloud to stay connected to the cloud.
Port		Port for local authentication. Make sure that ADS M has the same local authentication port as ADS or NTA collaborating with it.
Cloud Authorization Status		After you configure the address of the cloud authorization center, ADS-M-VM, upon startup, sends authentication requests to the cloud. • **Authorized**: indicates that the address of the cloud authorization center is correct and the connection to the cloud is properly established. Then, the device is available for use. • **Offline**: In the authorized state, if an incorrect authorization center address is typed, the authorization status turns to **Offline**. An offline device provides all functions except system upgrade within 30 days. Upon the expiry of the period, the device enters the unauthorized state. • **Unauthorized**: The system cannot be upgraded, nor does it support device addition, region configuration, or traffic statistics. • **Authentication failure**: The device provides all functions except system upgrade within 30 days. Upon the expiry of the period, the device enters the unauthorized state. During its operation, ADS-M-VM periodically sends authentication requests to the cloud to stay connected to the cloud.
Address of Authorization Center		URL of the cloud authorization server. • For use on the Chinese mainland, choose **auth.api.nsfocus.com**. • For use in other countries and regions, choose **auth.nsfocusglobal.com**.

Note

The system displays a warning when the license is about to expire. You can set a period during which you will not be reminded again. To use ADS M properly, you should timely import a new license as prompted.

- For a formal license, within 30 days before the license expires, the system displays the first warning. You will also receive the warning when the license has expired.
- For a trial license, within seven days before the license expires, the system displays the first warning.

3.1.3 System Upgrade

You can manually import the update file to upgrade ADS M. Before upgrading the system, do as follows to avoid possible update failures or data loss:

- Contact NSFOCUS technical support for an applicable upgrade package of ADS M. Make sure that the package matches your product.
- Go to the License page to check whether the license has expired.
- Check whether configuration files and data have been backed up. If not, go to the Data Storage page to back up them.

To upgrade ADS M, follow these steps:

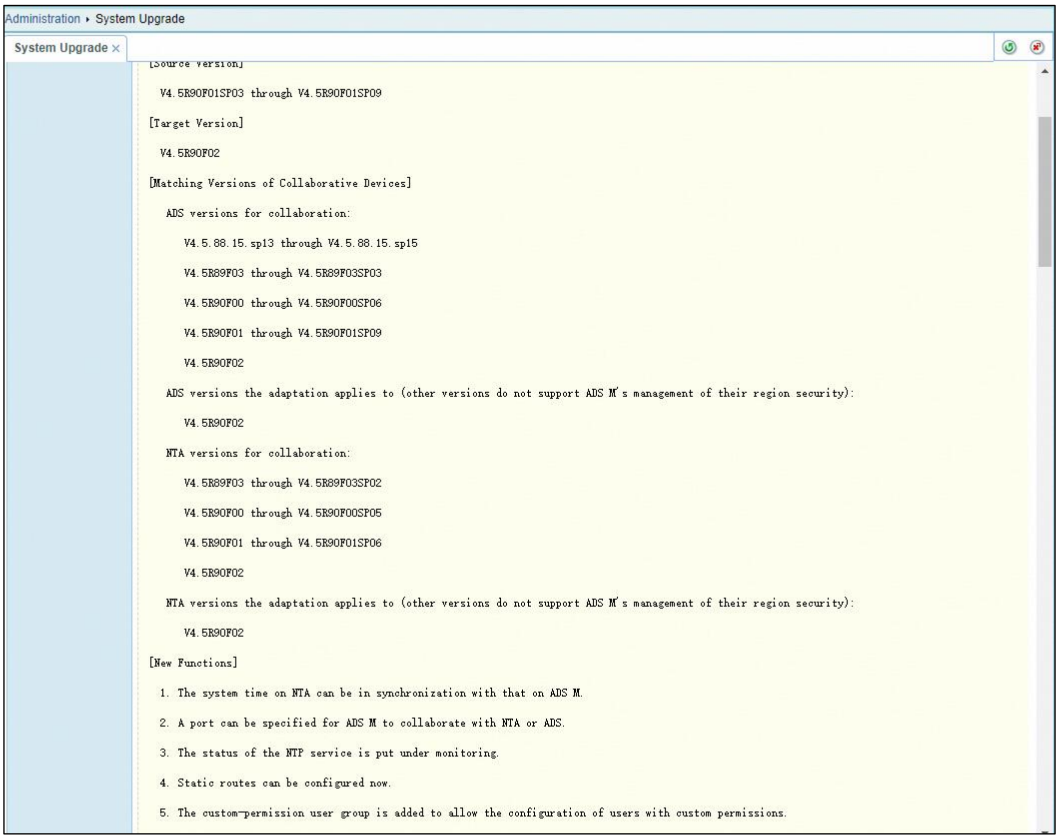
Step 1 Choose **Administration** > **Local Settings** > **System Upgrade**.

Step 2 Click **Browse** to select an upgrade package file.

Step 3 Click **Upload**.

After the upgrade package is uploaded, the system displays update-related information for you to confirm.

Figure 3-5 Upgrade confirmation



```
[Source Version]
  V4.5R90F01SP03 through V4.5R90F01SP09
[Target Version]
  V4.5R90F02
[Matching Versions of Collaborative Devices]
    ADS versions for collaboration:
        V4.5.88.15.sp13 through V4.5.88.15.sp15
        V4.5R89F03 through V4.5R89F03SP03
        V4.5R90F00 through V4.5R90F00SP06
        V4.5R90F01 through V4.5R90F01SP09
        V4.5R90F02
    ADS versions the adaptation applies to (other versions do not support ADS M's management of their region security):
        V4.5R90F02
    NTA versions for collaboration:
        V4.5R89F03 through V4.5R89F03SP02
        V4.5R90F00 through V4.5R90F00SP05
        V4.5R90F01 through V4.5R90F01SP06
        V4.5R90F02
    NTA versions the adaptation applies to (other versions do not support ADS M's management of their region security):
        V4.5R90F02
[New Functions]
  1. The system time on NTA can be in synchronization with that on ADS M.
  2. A port can be specified for ADS M to collaborate with NTA or ADS.
  3. The status of the NTP service is put under monitoring.
  4. Static routes can be configured now.
  5. The custom-permission user group is added to allow the configuration of users with custom permissions.
```

Step 4 Click **Confirm Upgrade**.

Then the upgrade proceeds. During the upgrade, the system displays a progress bar, indicating how much of the task has been completed.

Step 5 After the upgrade is complete, click **OK** in the dialog box, which prompts that the system service will be rebooted.

If the system does not prompt the upgrade success, wait about 3 minutes and then the system will automatically restart.

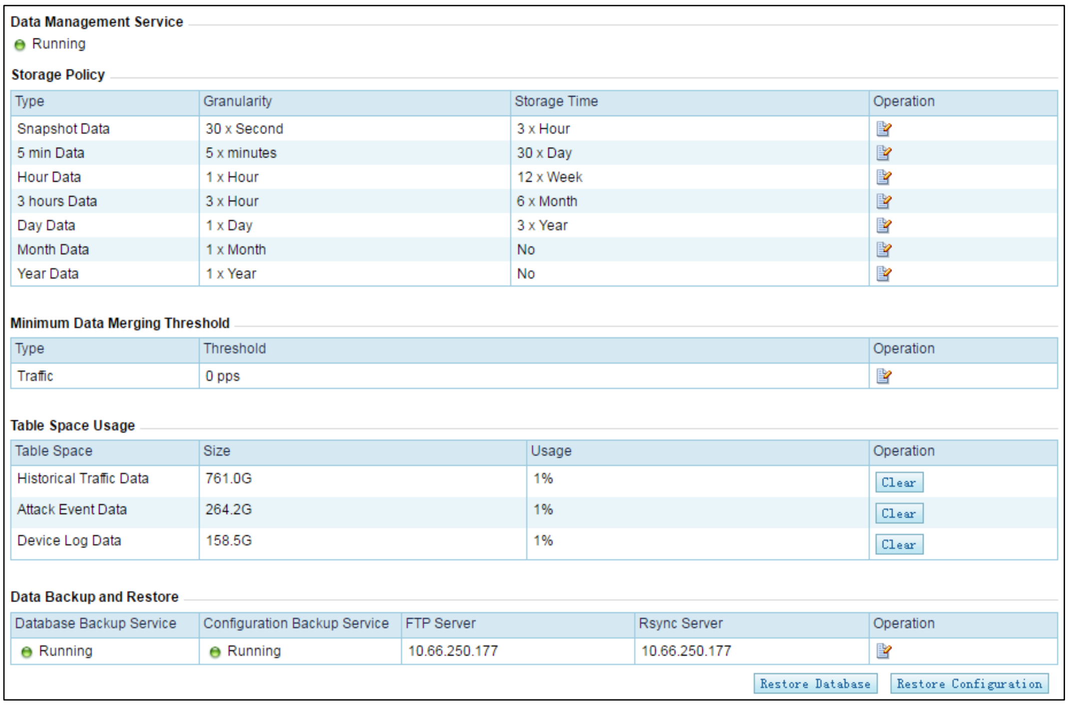
Step 6 Click in the **Operation** column of the upgrade package in the **Upgrade History** list to view information about the new version.

----End

3.1.4 Data Storage

Choose **Administration** > **Local Settings** > **Data Storage** to open the **Data Storage** page.

Figure 3-6 Data Storage page



Data Management Service

● Running

Storage Policy

Type	Granularity	Storage Time	Operation
Snapshot Data	30 x Second	3 x Hour	✎
5 min Data	5 x minutes	30 x Day	✎
Hour Data	1 x Hour	12 x Week	✎
3 hours Data	3 x Hour	6 x Month	✎
Day Data	1 x Day	3 x Year	✎
Month Data	1 x Month	No	✎
Year Data	1 x Year	No	✎

Minimum Data Merging Threshold

Type	Threshold	Operation
Traffic	0 pps	✎

Table Space Usage

Table Space	Size	Usage	Operation
Historical Traffic Data	761.0G	1%	Clear
Attack Event Data	264.2G	1%	Clear
Device Log Data	158.5G	1%	Clear

Data Backup and Restore

Database Backup Service	Configuration Backup Service	FTP Server	Rsync Server	Operation
● Running	● Running	10.66.250.177	10.66.250.177	✎

You can perform the following operations on the **Data Storage** page:

- View the data management service status.

  In the **Data Management Service** area, you can check whether the data management service is running or has stopped running.

- Edit data storage policies.

  In the **Storage Policy** area, click in the **Operation** column to edit the storage period of the corresponding data type.

Caution	If the storage time is **0**, it indicates that there is no limit to the data storage time. In addition, the system automatically clears out-of-date data.

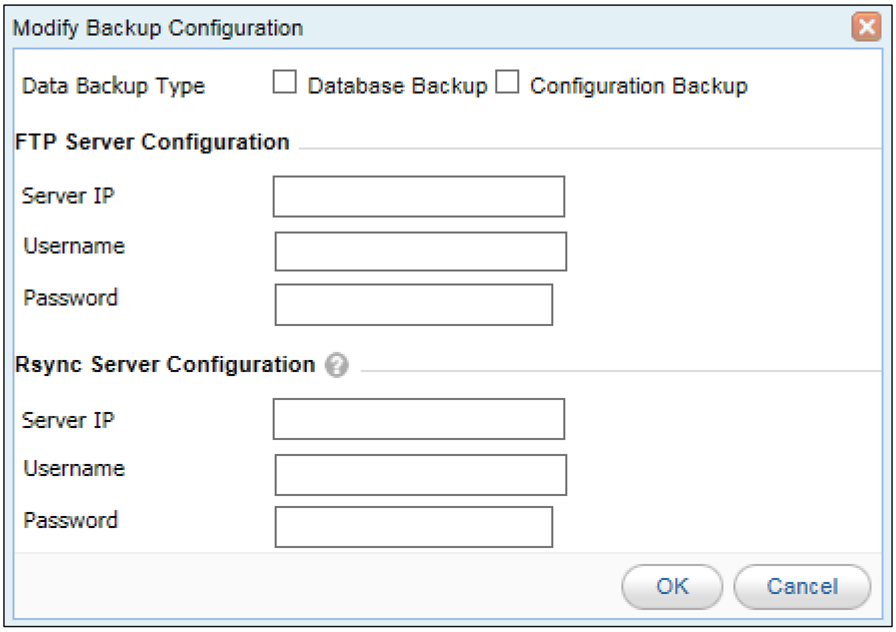
- Edit the minimum data merging threshold.

  In the **Minimum Data Merging Threshold** area, click 📝 in the **Operation** column to edit the minimum data merging threshold. Note that traffic below the specified threshold will be ignored during the merging.
- View the table space usage.

  In the **Table Space Usage** area, you can view the space used by historical traffic data, attack event data, and device log data as well as the related percentage of usage. Click **Clear** in the **Operation** column to delete the table space of a specific time.
- Manage data backup and restoration.
  - Modify the backup configuration.

    In the **Data Backup and Restore** area, click 📝 in the **Operation** column to edit the backup configuration in the dialog box shown in Figure 3-7.

Figure 3-7 Modifying the backup configuration



Modify Backup Configuration

Data Backup Type ☐ Database Backup ☐ Configuration Backup

FTP Server Configuration

Server IP

Username

Password

Rsync Server Configuration

Server IP

Username

Password

Select the data backup type and configure parameters of the FTP server and Rsync server.

Note	For **Data Backup Type**, if only **Configuration Backup** is selected, you need to configure the Rsync server; if only **Database Backup** is selected, you need to configure both the FTP server and the Rsync server.

  - Restore the database.

In the **Data Backup and Restore** area, click **Restore Database** below the table to restore the database information backed up on the server to the ADS M device.

- Apply the backup file for restoration.

  In the **Data Backup and Restore** area, click **Restore Configuration** below the table to restore the configuration files backed up on the server to the ADS M device. The ADS M configuration is backed up to the server at 23:50 each day.

3.1.5 Network Settings

ADS M supports both IPv4 and IPv6 configuration of the interface addresses, default gateway, and static routes. The following sections describe how to configure IPv4 and IPv6 network settings respectively.

3.1.5.1 Configuring IPv4 Network Settings

Interface Addresses of ADS NX3-M1600E and ADS-M NX3-HD2700

Figure 3-8 shows the front panel of ADS NX3-M1600E.

Figure 3-8 Front panel of ADS NX3-M1600E

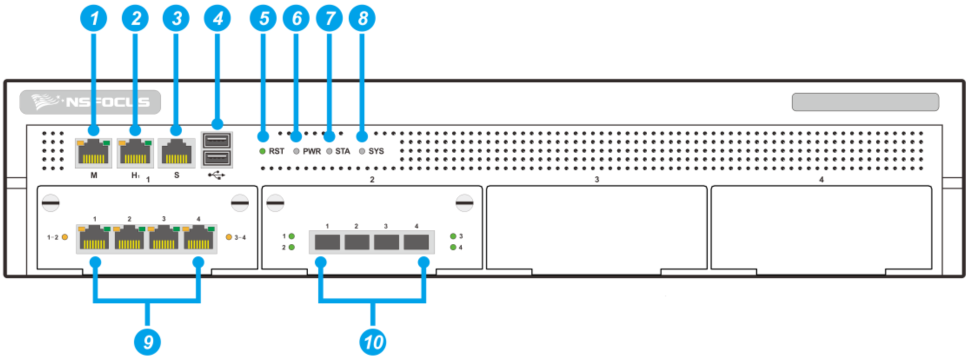


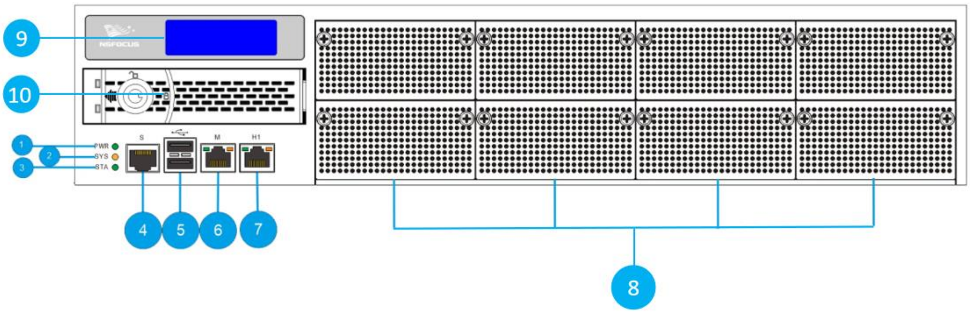
Table 3-3 describes the interfaces on the front panel of ADS NX3-M1600E.

Table 3-3 Front panel of ADS NX3-M1600E

① M: management port	② H: management port	③ Serial port (RJ45)	④ USB port
⑤ Reset LED	⑥ Power LED	⑦ Status LED	⑧ System LED
⑨ Working port: GE electrical (RJ45) Electrical ports are, from left to right, referred to as S1-1, S1-2, S1-3, and S1-4 on the web-based manager.	⑩ Working port: GE optical (SFP) Optical ports are, from left to right, referred to as S2-1, S2-2, S2-3, and S2-4 on the web-based manager.	–	–

Figure 3-9 shows the front panel of ADS-M NX3-HD2700.

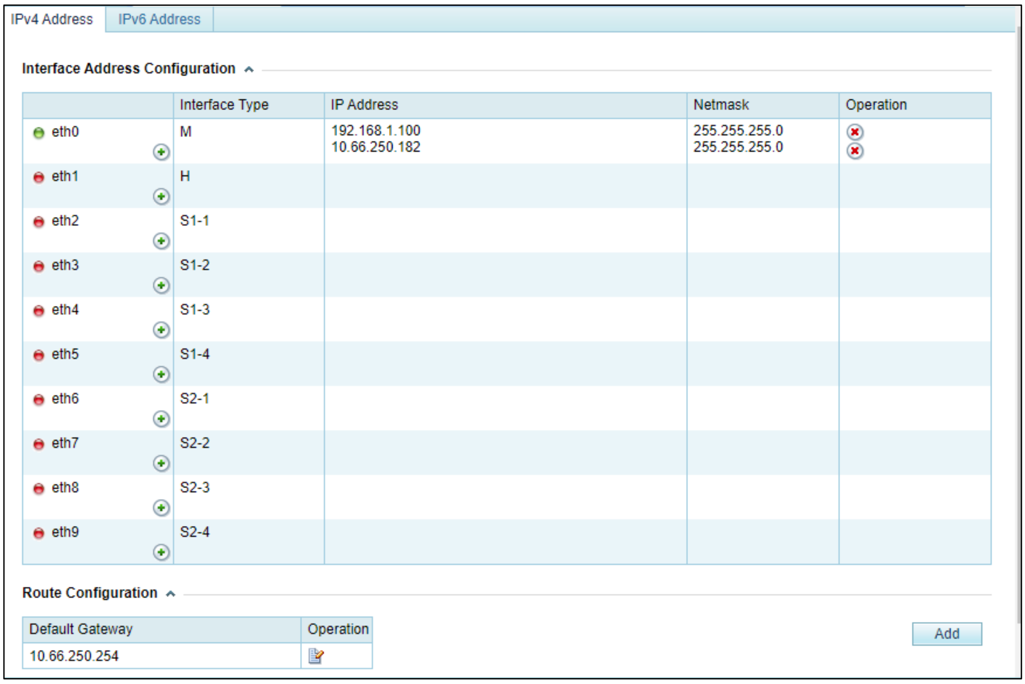
Figure 3-9 Front panel of ADS-M NX3-HD2700



① Power LED	② System LED	③ Status LED
④ Serial port (RJ45)	⑤ USB port	⑥ M: management port
⑦ Hot standby port	⑧ Expansion slot	⑨ Monitor
⑩ HDD caddy	–	–

ADS NX3-M1600E's network ports include M (1000M), H (1000M), four 1000M electrical, and four 1000M optical ports, whose indications on the front panel are listed in the **Interface Type** column on the **IPv4 Address** page under **Administration > Local Settings > Network Settings** of the web-based manager. These 1000M electrical ports (left) and optical ports (right) are respectively referred to as S1-1, S1-2, S1-3, S1-4, S2-1, S2-2, S2-3, and S2-4 on this page.

Figure 3-10 ADS NX3-M1600E – IPv4 address configuration



Interface Address Configuration

	Interface Type	IP Address	Netmask	Operation
eth0	M	192.168.1.100 10.66.250.182	255.255.255.0 255.255.255.0	✖ ✖
eth1	H			
eth2	S1-1			
eth3	S1-2			
eth4	S1-3			
eth5	S1-4			
eth6	S2-1			
eth7	S2-2			
eth8	S2-3			
eth9	S2-4			

Route Configuration

Default Gateway	Operation
10.66.250.254	

The interface LED on the left of the interface name indicates the network connection status of this interface.

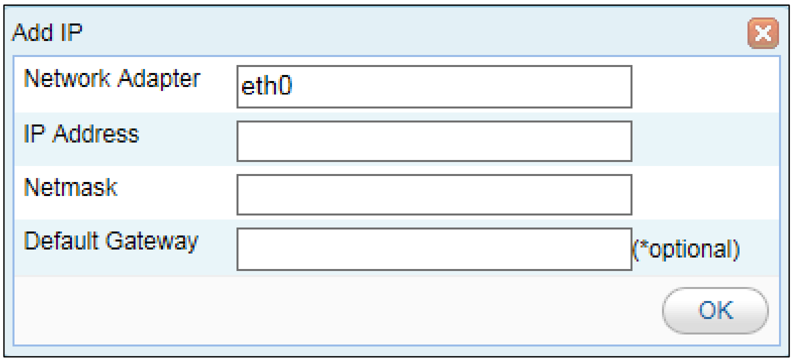
- 🟢: indicates that the network connection of the interface is up.
- 🔴: indicates that the network connection of the interface is down.

Though the device does not clearly specify roles of ports, M and H are recommended for configuration and management purposes and others are used as working interfaces.
Each interface can have two IP addresses. Initially, default parameters are displayed. You need to configure the IPv4 address and subnet mask for the network adapter.
To unbind the IP address from an interface, click ⊗ in the **Operation** column.

⚠ Caution	If the IP address of a management interface is deleted, you may be unable to access the web-based manager of ADS M.

On the interface list in Figure 3-10, click ⊕ next to an interface to configure the IPv4 address and other parameters for this interface, as shown in Figure 3-11.

Figure 3-11 ADS NX3-M1600E – Configuring an IPv4 interface address



Add IP

Network Adapter: eth0

IP Address:

Netmask:

Default Gateway: (*optional)

Table 3-4 describes parameters for configuring an IPv4 interface address.

Table 3-4 Parameters for configuring an IPv4 interface address

Parameter	Description
Network Adapter	Management interface or expansion interface of ADS M
IP Address	IP address of ADS M, which should be an IPv4 address here
Netmask	Subnet mask of the IPv4 address of ADS M
Default Gateway	IP address of the network gateway of the subnet where ADS M is on

Tip	After you change the IP address of the management interface, the current window may be unavailable. In this case, re-log in to the system from a new browser window.

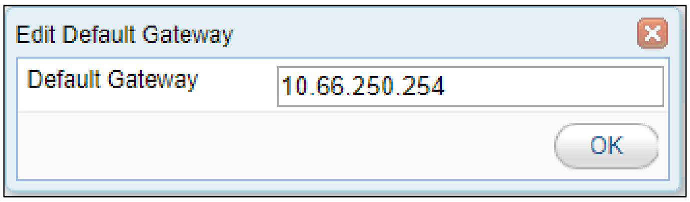
Default Gateway

To configure the IPv4 default gateway, follow these steps:

Step 1 In the **Route Configuration** area of the page shown in Figure 3-10, click 📝 in the **Operation** column.

Step 2 In the **Edit Default Gateway** dialog box, type an IPv4 address and click **OK**.

Figure 3-12 Configuring the default gateway


Edit Default Gateway

Default Gateway: 10.66.250.254

----End

Static Route

A static route is a route manually configured by the administrator. Such routes are used for small-scale networks that do not change constantly. As static routes cannot be adaptive to network changes, the administrator must manually adjust them once the network topology changes.

Choose **Administration** > **Local Settings** > **Network Settings**. In the **Route Configuration** area of the **IPv4 Address** page, click **Add** and configure parameters in the dialog box that appears.

Table 3-5 describes parameters for creating a static route.

Table 3-5 Parameters for creating a static route

Parameter	Description
Target	IPv4 address and netmask of the destination host, used to identify the destination address or network of IP packets. Note If you are configuring a static route for a network segment, you need to convert the netmask to a prefix length, such as 10.20.0.0/24.
Gateway or Next-Hop IP	Specifies the gateway for the static route, usually, the local IP address of the next-hop device.
Interface	Specifies the egress interface of the static route.

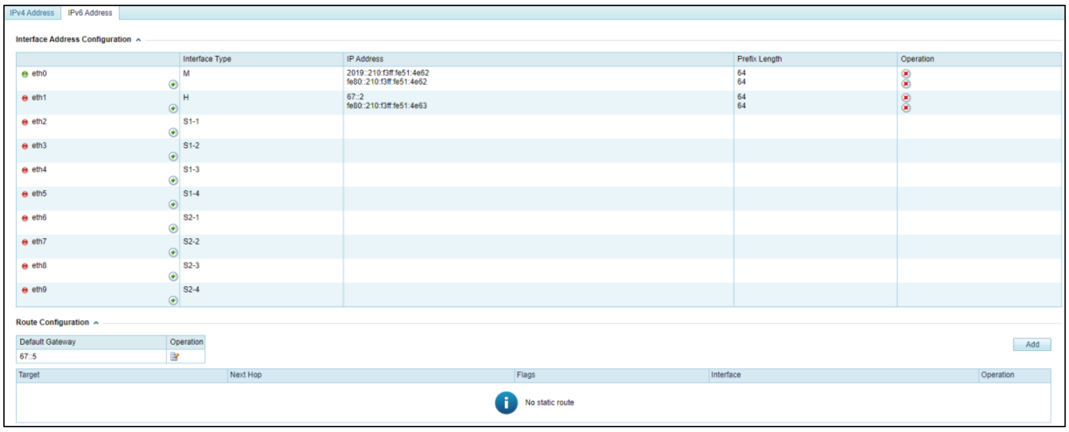
Parameter	Description
	If the interface goes Down, the system automatically switches to interface eth0.

3.1.5.2 Configuring IPv6 Network Settings

Interface Addresses of ADS NX3-M1600E and ADS-M NX3-HD2700

On the **Network Settings** page in Figure 3-10, click **IPv6 Address** to open the IPv6 address configuration page. See Figure 3-13.

Figure 3-13 IPv6 address configuration



Interface Address Configuration

	Interface Type	IP Address	Prefix Length	Operation
eth0 ⊕	M	2019::210:f3ff:fe51:4e62 fe80::210:f3ff:fe51:4e62	64 64	⊗ ⊗
eth1 ⊕	H	67::2 fe80::210:f3ff:fe51:4e63	64 64	⊗ ⊗
eth2 ⊕	S1-1			
eth3 ⊕	S1-2			
eth4 ⊕	S1-3			
eth5 ⊕	S1-4			
eth6 ⊕	S2-1			
eth7 ⊕	S2-2			
eth8 ⊕	S2-3			
eth9 ⊕	S2-4			

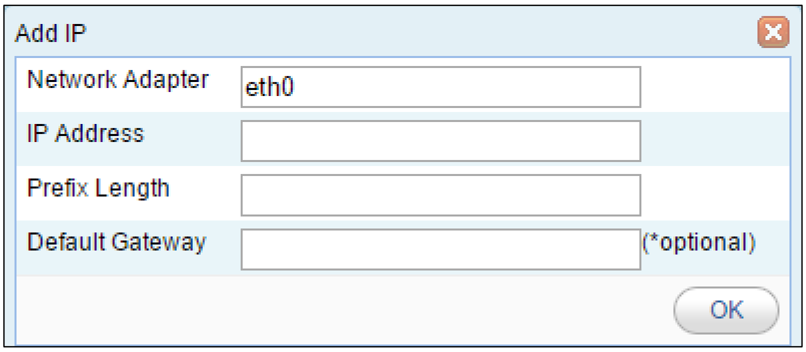
Route Configuration

Default Gateway	Operation
67::5	

Target	Next Hop	Flags	Interface	Operation
		No static route		

On the interface list in Figure 3-13, click ⊕ next to an interface to configure the IPv6 address and other parameters for this interface. See Figure 3-14.

Figure 3-14 Configuring an IPv6 interface address



Add IP

Network Adapter	eth0	
IP Address		
Prefix Length		
Default Gateway		(*optional)

Table 3-6 describes IPv6 network parameters.

Table 3-6 Parameters for configuring an interface in IPv6 mode

Parameter	Description
Network Adapter	Management interface or expansion interface of ADS M
IP Address	Specifies the IP address of ADS M, which should be an IPv6 address here
Prefix Length	Prefix length of the IPv6 address
Default Gateway	IP address of the network gateway of the subnet where ADS M is on

Tip

After you change the IP address of the management interface, the current window may be unavailable. In this case, re-log in to the system from a new browser window.

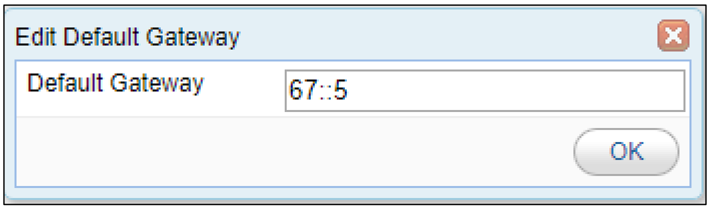
Default Gateway

To configure the IPv6 default gateway, follow these steps:

Step 1 In the **Route Configuration** area of the page shown in Figure 3-13, click 📝 in the **Operation** column.

Step 2 In the **Edit Default Gateway** dialog box, type an IPv6 address and click **OK**.

Figure 3-15 Configuring the default gateway



Edit Default Gateway

Default Gateway: 67::5

----End

Static Route

To configure an IPv6 static route, follow these steps:

Step 1 In the **Route Configuration** area of the page shown in Figure 3-13, click **Add**.

Step 2 In the **Add Static Route** dialog box, configure parameters.

Figure 3-16 Creating a static route

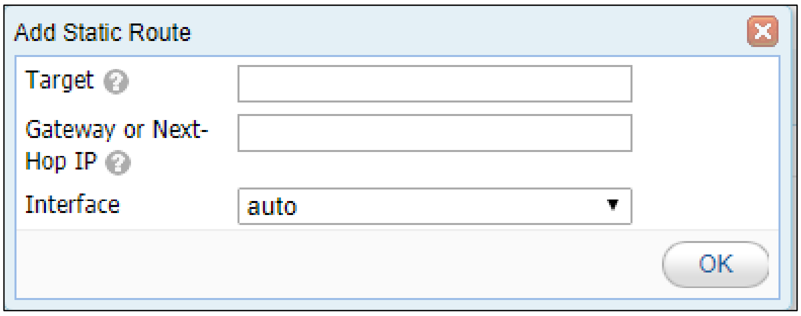


Table 3-7 describes parameters for creating a static route.

Table 3-7 Parameters for creating a static route

Parameter	Description
Target	IPv6 address and prefix of the destination host, used to identify the destination address or network of IP packets.
Gateway or Next-Hop IP	Specifies the gateway for the static route, usually, the local IP address of the next-hop device.
Interface	Specifies the egress interface of the static route. If the interface goes Down, the system automatically switches to interface eth0.

Step 3 Click **OK**.

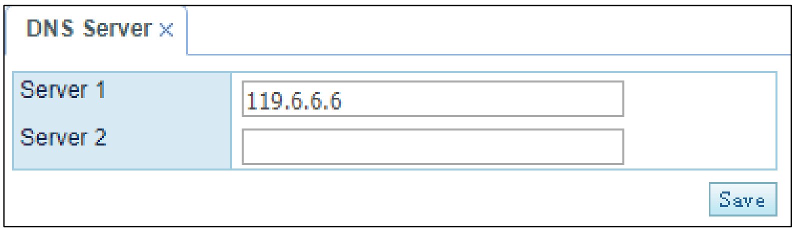
----End

3.1.6 DNS Server

As an essential and fundamental service, the DNS service is used to determine the mapping between host domain names and IP addresses. You are allowed to configure DNS servers for ADS M.

Choose **Administration** > **Local Settings** > **DNS Server** to open the **DNS Server** page. On this page, type the IP address (two IP addresses at most) of the DNS server of ADS M and click **Save**.

Figure 3-17 DNS Server page



Server 1: 119.6.6.6

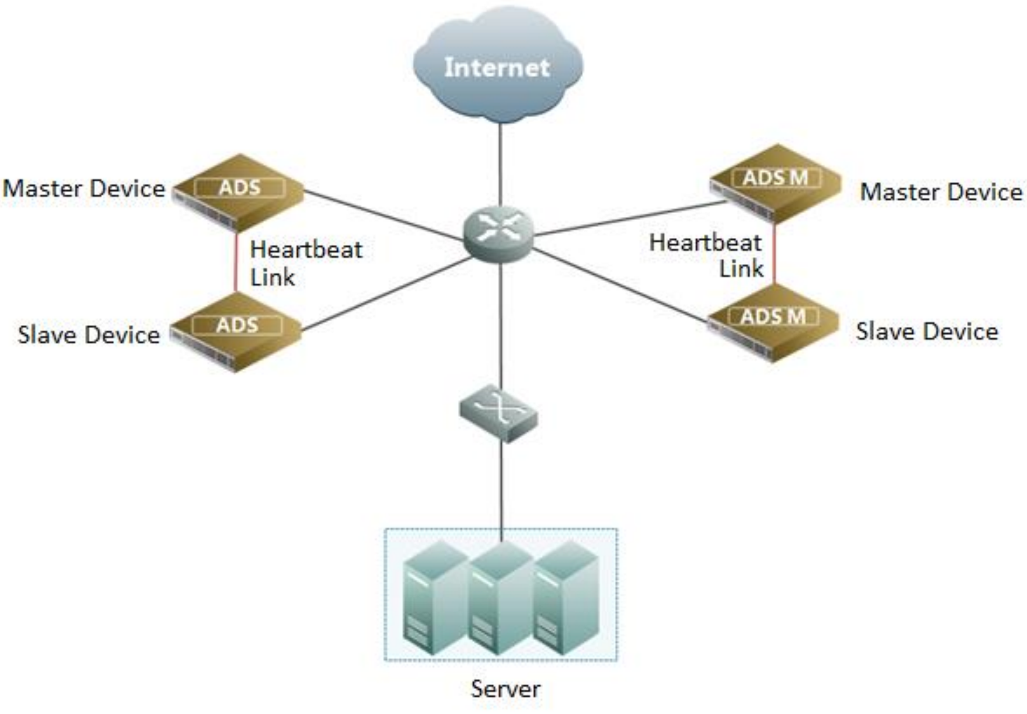
Server 2:

3.1.7 HA Configuration

Currently, ADS M supports the dual-system hot backup function, with one ADS M as the master device and the other as the slave device. By default, the master device handles all traffic and synchronizes heartbeat information and real-time status to the slave device that is only a backup device and does not handle services. If the master device fails, the slave device will take over all the services and traffic handled by the master device, ensuring business continuity to the maximum extent possible.

Routes must be reachable between the master and slave ADS M devices, and the two devices are connected via their heartbeat interfaces (management or work interface) to synchronize heartbeat information and configuration files. Figure 3-18 shows a simple topology for HA.

Figure 3-18 Topology for HA



Configuring HA

During the dual-system hot backup deployment, you must first configure interfaces on the master and slave devices (for details, see section 10.3.2 Configuring Network Settings):

- Configure the heartbeat interfaces (management interface or working interface).

  The heartbeat interfaces are used for the master device to synchronize configuration files to the slave device.

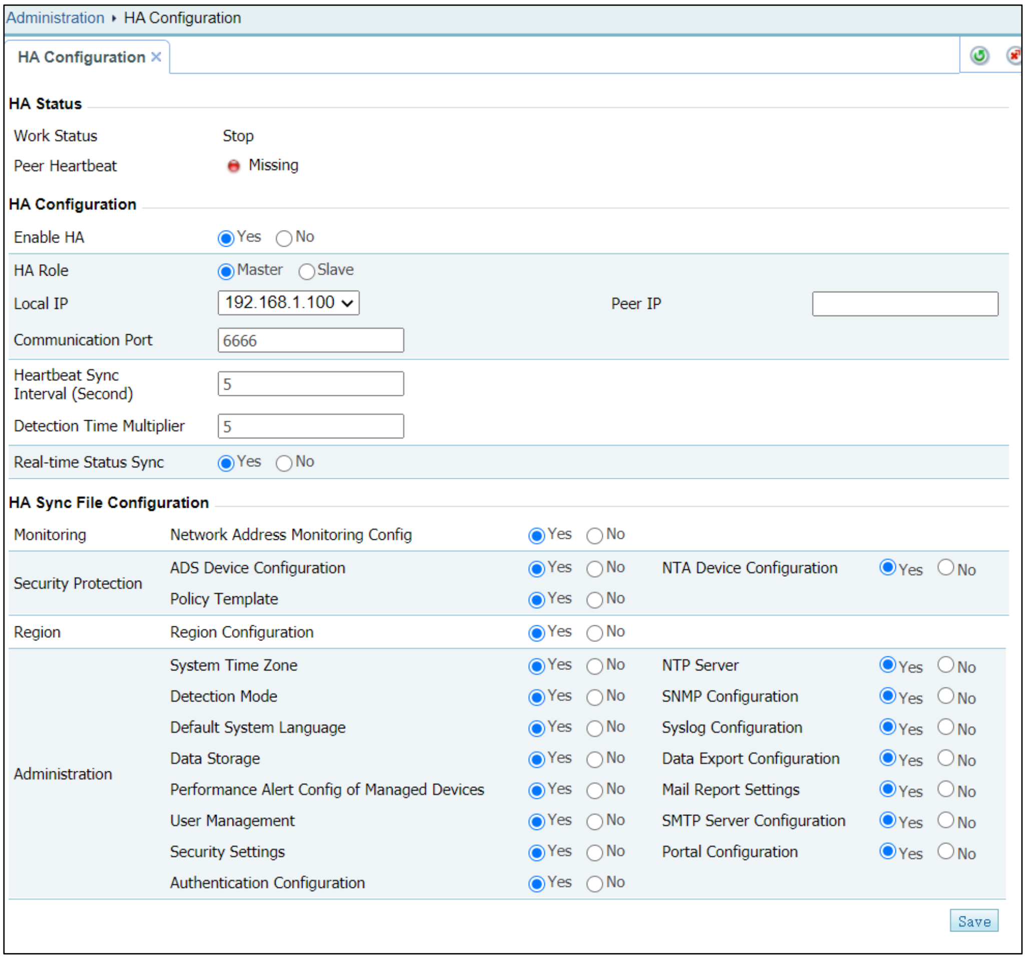
  Routes must be reachable between heartbeat interfaces of master and slave devices.
- Configure other communication interfaces.

After the interface configuration, enable the dual-system hot backup function and configure HA parameters by performing the following steps:

Step 1 Choose **Administration** > **Local Settings** > **HA Configuration**.

Step 2 Set HA parameters under **HA Configuration**.

Figure 3-19 HA Configuration page



Administration ▸ HA Configuration

HA Configuration ×

HA Status

Work Status: Stop

Peer Heartbeat: ● Missing

HA Configuration

Enable HA: ● Yes ○ No

HA Role: ● Master ○ Slave

Local IP: 192.168.1.100

Peer IP:

Communication Port: 6666

Heartbeat Sync Interval (Second): 5

Detection Time Multiplier: 5

Real-time Status Sync: ● Yes ○ No

HA Sync File Configuration

Monitoring	Network Address Monitoring Config	● Yes ○ No		
Security Protection	ADS Device Configuration	● Yes ○ No	NTA Device Configuration	● Yes ○ No
	Policy Template	● Yes ○ No		
Region	Region Configuration	● Yes ○ No		
Administration	System Time Zone	● Yes ○ No	NTP Server	● Yes ○ No
	Detection Mode	● Yes ○ No	SNMP Configuration	● Yes ○ No
	Default System Language	● Yes ○ No	Syslog Configuration	● Yes ○ No
	Data Storage	● Yes ○ No	Data Export Configuration	● Yes ○ No
	Performance Alert Config of Managed Devices	● Yes ○ No	Mail Report Settings	● Yes ○ No
	User Management	● Yes ○ No	SMTP Server Configuration	● Yes ○ No
	Security Settings	● Yes ○ No	Portal Configuration	● Yes ○ No
	Authentication Configuration	● Yes ○ No		

Table 3-8 describes HA parameters.

Table 3-8 HA parameters

Parameter	Description
Enable HA	Controls whether to enable the HA function. • **Yes**: indicates that the HA function is enabled. • **No**: indicates that the HA function is disabled.
HA Role	Role played by this device in dual-system hot backup mode. • **Master**: indicates that this device functions as the master device and starts to handle services immediately after HA is enabled and will not stop until a failover. • **Slave**: indicates that this device functions as the slave device. After HA is enabled, the slave device stays in the backup state without handling services, until a failover.

Parameter	Description
Local IP	IP address of the heartbeat interface of the current device. It can be an IPv4 or IPv6 address. This IP address can be the IP address of a management interface.
Peer IP	IP address of the heartbeat interface of the peer device. It can be an IPv4 or IPv6 address. This IP address can be the IP address of a management interface. Note Routes must be reachable between heartbeat interfaces of master and slave devices.
Communication Port	Port used by the device for communication with the peer. Note The master and slave devices must be configured with the same monitoring port.
Heartbeat Sync Interval (Second)	Interval for the device to synchronize keepalive messages to the peer device. Note The heartbeat synchronization intervals on the master and slave devices should be as close as possible. After an HA connection is established between the master and slave devices, the heartbeat synchronization interval on the slave device will automatically synchronized to that on the master device.
Detection Time Multiplier	Multiple of the heartbeat synchronization interval. This parameter, together with **Heartbeat Sync Interval (Second)**, determines whether the keepalive message times out. If the keepalive message from the peer is not detected within the specified period, this message is considered expired. After an HA connection is established between the master and slave devices, the detection time multiple on the slave device will be automatically synchronized with that on the master device.
Real-Time Status Sync	Whether to enable real-time status synchronization. **Real-Time Status Sync** should be enabled on both the master and slave devices so that files can be synchronized between the two devices. After an HA connection is established between the master and slave devices, the real-time status synchronization setting on the slave device will be automatically synchronized to that on the master device.

Step 3 In the **HA Sync File Configuration** area, select configuration files that need to be synchronized between the master and slave devices.

Step 4 Click **Save** to save the settings.

----End

Viewing HA Status

After HA is enabled, the HA working status and peer heartbeat status are displayed under **HA Status** shown in Figure 3-19. The working status can be one of the following:

- **Active**: indicates that the current device works as the master device.

- **Standby**: indicates that the current device works as the slave device.
- **Error**: indicates that the HA function is abnormal on the current device.
- **Stop**: indicates that the HA function is disabled or stopped on the current device.

The peer heartbeat status can be either of the following:

- **Normal**: indicates that the current device can receive heartbeat messages from the peer. The communication is normal.
- **Missing**: indicates that the current device cannot receive heartbeat messages from the peer. The communication is abnormal.

3.1.8 Performance Alert Configuration of Managed Devices

On the **Performance Alert Config of Managed Devices** page, you can set the CPU and memory usage thresholds corresponding to alert levels under **CPU/Memory Alert Configuration**.

- **Global** allows you to set alert thresholds for the CPU and memory usage of ADS M itself and all devices under ADS M.
- **ADS** allows you to set alert thresholds for the CPU and memory usage of all ADS devices under ADS M.
- **NTA** allows you to set alert thresholds for the CPU and memory usage of all NTA devices under ADS M.

After setting alert thresholds, you can view the status of CPU and memory usage alerts in the **Device Monitoring** area under **Traffic Monitoring > Overview**. For details, see section 4.1.5 Viewing the System Status Bar.

Under **Offline Time Threshold**, you can set the time threshold for triggering device offline alerts. When a device under ADS M remains offline for a period longer than specified, a device offline alert is generated and sent via syslog or email (syslog server and email settings should be completed in advance). For related configuration, see sections 3.3.2 Syslog and 3.3.4 Mail Alert Settings.

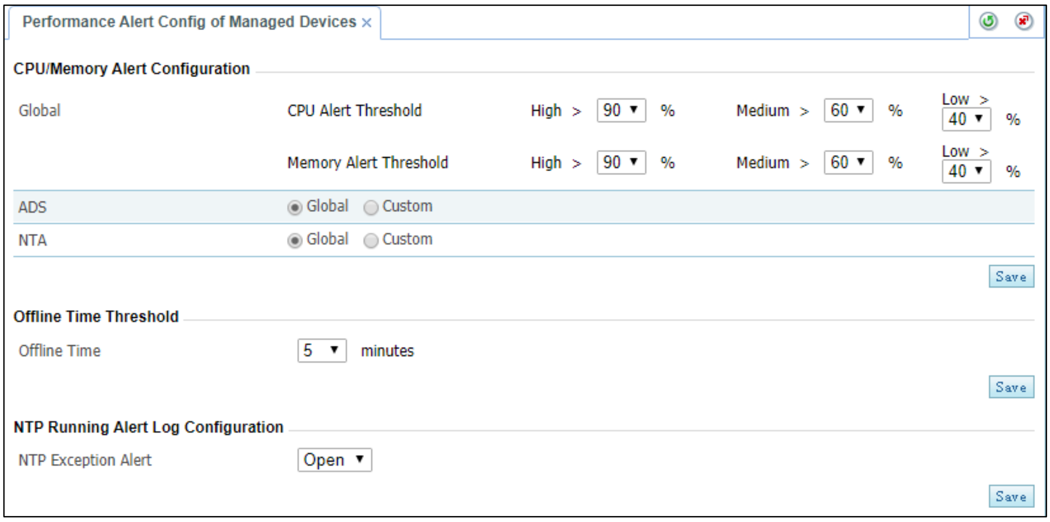
Under **NTP Running Alert Log Configuration**, you can enable NTP running alerting and logging. After this is enabled, ADS M triggers an alert and generates a related message when the NTP server works improperly. When the NTP server is resumed to the normal state, no related message will be logged.

To configure performance alert settings, follow these steps:

Step 1 Choose **Administration > Local Settings > Performance Alert Config of Managed Devices**.

Step 2 Set CPU and memory alert thresholds and the offline alert threshold, and enable or disable the NTP running alert log.

Figure 3-20 Performance Alert Config of Managed Devices page



CPU/Memory Alert Configuration

Global

CPU Alert Threshold High > 90 % Medium > 60 % Low > 40 %

Memory Alert Threshold High > 90 % Medium > 60 % Low > 40 %

ADS ● Global ○ Custom

NTA ● Global ○ Custom

Offline Time Threshold

Offline Time 5 minutes

NTP Running Alert Log Configuration

NTP Exception Alert Open

Step 3 Click **Save**.

----End

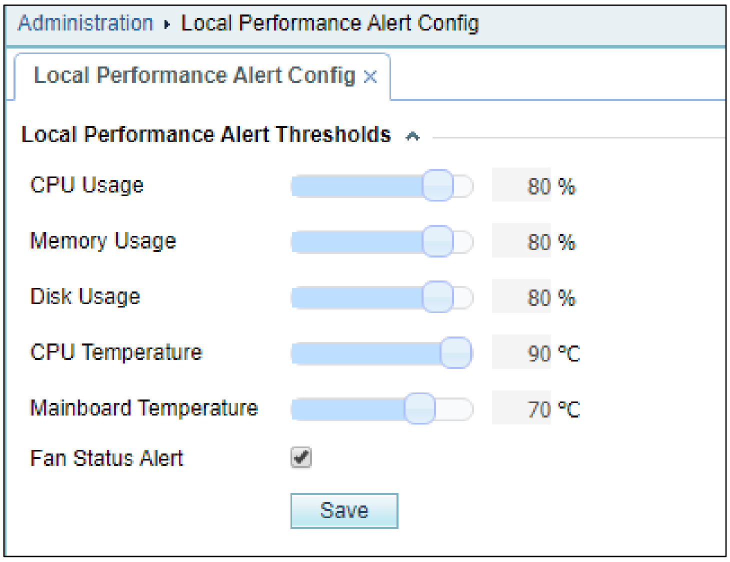
3.1.9 Local Performance Alert Configuration

To configure local performance alert thresholds, follow these steps:

Step 1 Choose **Administration** > **Local Settings** > **Local Performance Alert Config**.

Step 2 Configure parameters.

Figure 3-21 Local performance alert configuration



Administration ▸ Local Performance Alert Config
Local Performance Alert Config ×
Save

Local Performance Alert Thresholds

CPU Usage 80 %

Memory Usage 80 %

Disk Usage 80 %

CPU Temperature 90 °C

Mainboard Temperature 70 °C

Fan Status Alert ☑

Table 3-9 describes parameters on this page.

Table 3-9 Local performance alert parameters

Parameter	Description
CPU Usage	Specifies the percentage of CPU usage that will trigger an alert.
Memory Usage	Specifies the percentage of memory usage that will trigger an alert.
Disk Usage	Specifies the percentage of disk usage that will trigger an alert.
CPU Temperature	Specifies the temperature of the CPU that will trigger an alert.
Mainboard Temperature	Specifies the temperature of the motherboard that will trigger an alert.
Fan Status Alert	Controls whether to turn the fan switch on. If it is turned on, an alert will be triggered when a fan fails.

Step 3 Click **Save**.

Real-time system performance parameters are displayed in the system status bar. For details, see section 4.1.5 Viewing the System Status Bar.

If any of the performance thresholds is exceeded, the system will report an alert and log an alert message.

----End

3.1.10 Management Interface Access Control

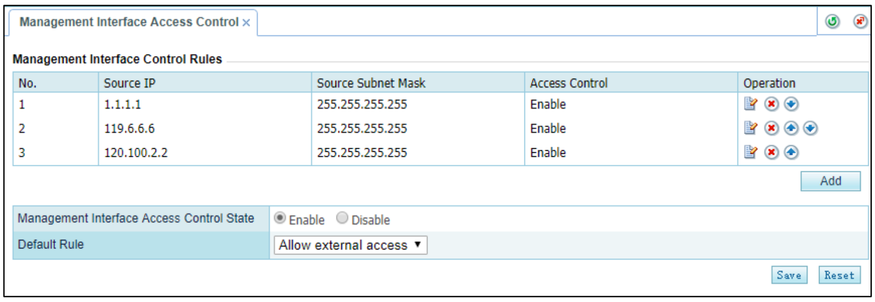
The management interface access control is disabled by default. After being enabled, it can be disabled via the console. After source IP addresses/segments are specified for access to the management interface, those beyond the specified range cannot access ADS M, whether via web, Telnet, or ping. In addition, the system can dynamically identify external IP addresses to which ADS M connects, such as NSFOCUS Cloud or other collaborative platforms, and allow access from these IP addresses.

3.1.10.1 Creating a Management Interface Access Control Rule

To create a management interface access control rule, follow these steps:

Step 1 Choose **System** > **Local Settings** > **Management Interface Access Control**.

Figure 3-22 Management Interface Access Control page



Management Interface Control Rules

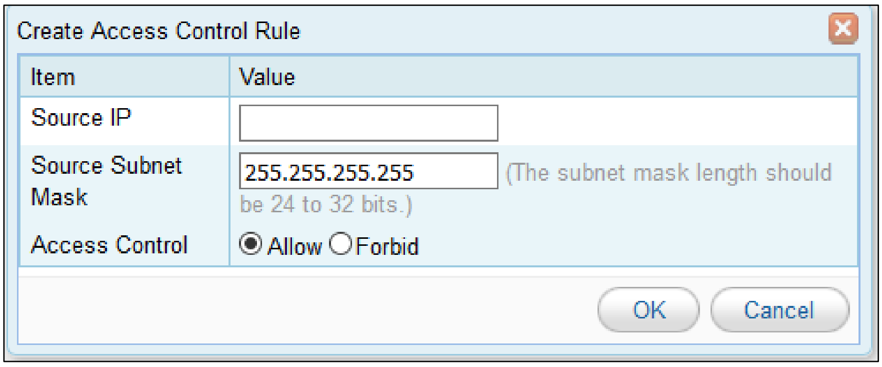
No.	Source IP	Source Subnet Mask	Access Control	Operation
1	1.1.1.1	255.255.255.255	Enable	
2	119.6.6.6	255.255.255.255	Enable	
3	120.100.2.2	255.255.255.255	Enable	

Management Interface Access Control State: ● Enable ○ Disable

Default Rule: Allow external access ▼

Step 2 Click **Add** and set parameters.

Figure 3-23 Creating a management interface access control rule



Create Access Control Rule

Item	Value
Source IP	
Source Subnet Mask	255.255.255.255 (The subnet mask length should be 24 to 32 bits.)
Access Control	● Allow ○ Forbid

Table 3-10 describes parameters for configuring a management interface access control rule.

Table 3-10 Parameters for creating a management interface access control rule

Parameter	Description
Source IP	Specifies a source IP address/segment that is allowed or forbidden to access ADS M. Only IPv4 is supported.
Source Subnet Mask	Specifies the subnet mask of the source IP address/segment.
Access Control	• **Allow**: allows the specified IP address/segment to access ADS M. • **Forbid**: forbids the specified IP address/segment to access ADS M.

Step 3 Click **OK**.

A new management interface access control rule is thus created.

Step 4 Edit the management interface access control function.

Table 3-11 describes parameters of for controlling the management interface access control function.

Table 3-11 Parameters for controlling the management interface access control function

Parameter	Description
Management Interface Access Control State	• **Enable**: enables the function. • **Disable**: disables the function.
Default Rule	• **Allow external access**: allows any IP addresses other than those denied access in management interface access control rules to access ADS M. • **Deny external access**: forbids any IP addresses other than those allowed access in management interface access control rules to access ADS M. After this option is selected, only IP addresses allowed access in management interface access control rules can access ADS M.

Step 5 After completing the configuration, click **Save** to save the settings.

----End

3.1.10.2 Changing the Rule Match Sequence

When there is more than one management interface access control rule, the rule on top is matched first and, if it is a hit, no other rules will be checked for a match. You can adjust the sequence of rules to change their priority. On the page shown in Figure 3-22, click ↑ or ↓ in the **Operation** column of a rule to move it up or down.

3.1.10.3 Editing a Management Interface Access Control Rule

You can edit parameter settings of a management interface access control rule after it is configured. To do that, follow these steps:

Step 1 On the page shown in Figure 3-22, click ✎ in the **Operation** column of a rule.

Step 2 Edit parameter settings and then click **OK** to save the changes and return to the rule list page.

----End

3.1.10.4 Deleting a Management Interface Access Control Rule

On the page shown in Figure 3-22, click ✖ in the **Operation** column of a rule and click **OK** in the confirmation dialog box to delete this rule.

3.1.11 SSL Certificate Replacement

The system has a built-in SSL certificate, which can be replaced.

To replace the built-in SSL certificate, follow these steps:

Step 1 Choose **Administration** > **Local Settings** > **SSL Certificate Replacement**.

Step 2 Type the correct password if a password is set for the private key of the SSL certificate to be imported; otherwise, leave it empty.

Step 3 Browse respectively to the SSL certificate file and private key file and then click **Open**.

Step 4 Click **Replace**.

After the certificate is replaced, the web service will restart automatically.

----End

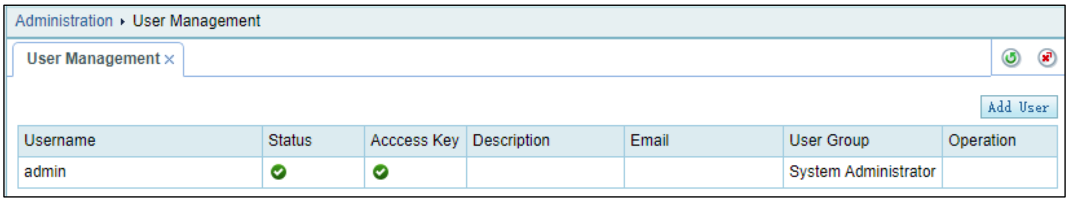
3.2 User and Audit

This section describes how to perform ADS M user management, security settings, authentication configuration as well as how to view audit logs.

3.2.1 User Management

Choose the **User Management** page displays all current users. Initially, only the default user **admin** is displayed.

Figure 3-24 User Management page



Username	Status	Acccess Key	Description	Email	User Group	Operation
admin	✓	✓			System Administrator	

Table 3-12 describes ADS M user groups and their respective permissions.

Table 3-12 ADS M user groups and their respective permissions

User Group	Permission
System administrator	Has all permissions for system management.
Device configuration administrator	Has permissions for managing device configurations and viewing system monitoring information.
Region administrator	Has permissions for configuring regions and viewing system monitoring information.
Audit user	Has permissions for viewing audit logs.
Custom access user	Has permissions assigned by **admin**.

Creating a User

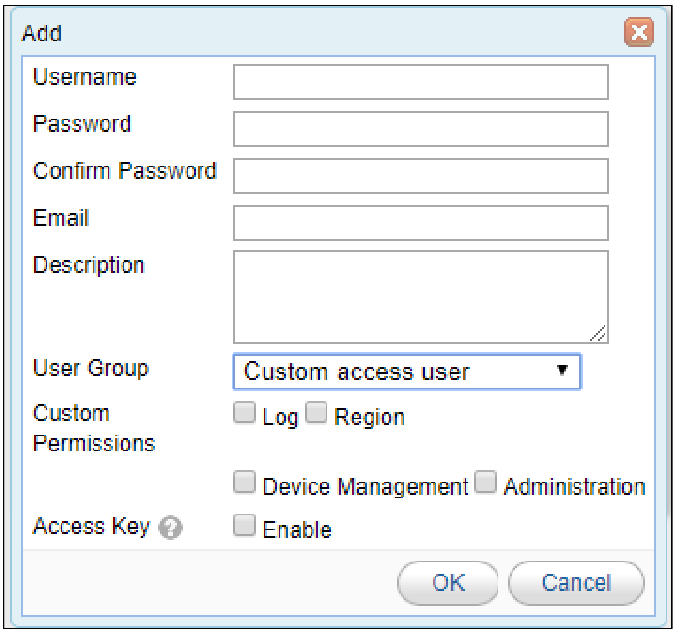
Only the user **admin** can create system administrators. Only system administrators can create device configuration administrators, region administrators, and auditors.

To create a user, follow these steps:

Step 1 Click **Add User** in the upper-right corner of the **User Management** page.

Step 2 Set parameters in the **Add** dialog box.

Figure 3-25 Creating a user



Add

Username

Password

Confirm Password

Email

Description

User Group: Custom access user ▼

Custom Permissions: □ Log □ Region □ Device Management □ Administration

Access Key: □ Enable

Table 3-13 Parameters for creating a user

Parameter	Description
Username	Specifies the user name. The user name must be 4 to 20 characters and cannot contain invalid characters such as the tab character, carriage return, \0, space, vertical bar (|), slash (/), angle bracket (<, or >), quotation mark (" or '), and semicolon (;).
Password	Specifies the password. The minimum length and strength of the password can be configured under **Administration** > **User and Audit** > **Security Settings**.
Confirm Password	Password confirmation. The password you type here must be the same as the one you typed for **Password**.
Email	A valid email address of the user. This parameter is optional.
Description	Brief description of this user. This parameter is optional.
User Group	User role. Different roles have different operation permissions. The custom access user's permissions depend on **admin**'s further selection of accessible modules.
Custom Permissions	Specifies one or more modules accessible to the custom access user. No matter which modules are selected, Traffic Monitoring and Report modules are available only for statistics viewing by default.
Access Key	Used for accessing the web API of ADS M. For details about configuration of the web API, contact NSFOCUS technical support. If this option is enabled, the user can view his or her own access key in the quick access bar in the upper-right corner of the web-based manager; if it is disabled, the user will have no access to traffic data. In other words, Traffic Monitoring and Report modules will not display any data.

Step 3 Click **OK**.

----End

Modifying User Information

Only user **admin** and other system administrators can modify information of all users. Other users can only modify their own information.

On the **User Management** page, click 📝 in the **Operation** column of a user to edit information of this user. Note that the user name cannot be changed. To edit the default system administrator **admin**, you need to log in to the system as **admin** and click admin in the quick access bar in the upper-right corner of the page.

Deleting a User

Only the user **admin** and other system administrators can delete users.

On the user list, click ⊗ in the **Operation** column to delete a user. The default system administrator **admin** cannot be deleted.

Disabling a User

Only the user **admin** and other system administrators can disable users.

By default, new users are enabled, that is, the **Status** column is displayed as ✓. On the user list, click ⊖ in the **Operation** column to disable a user. Then the icon is displayed as ⊖ in the **Status** column. Disabled users cannot log in to the web-based manager of ADS M. The default system administrator **admin** cannot be disabled.

Enabling a User

To enable a user that is disabled, click ✓ in the **Operation** column on the user list.

Note	Only the user **admin** and other system administrators can enable users.

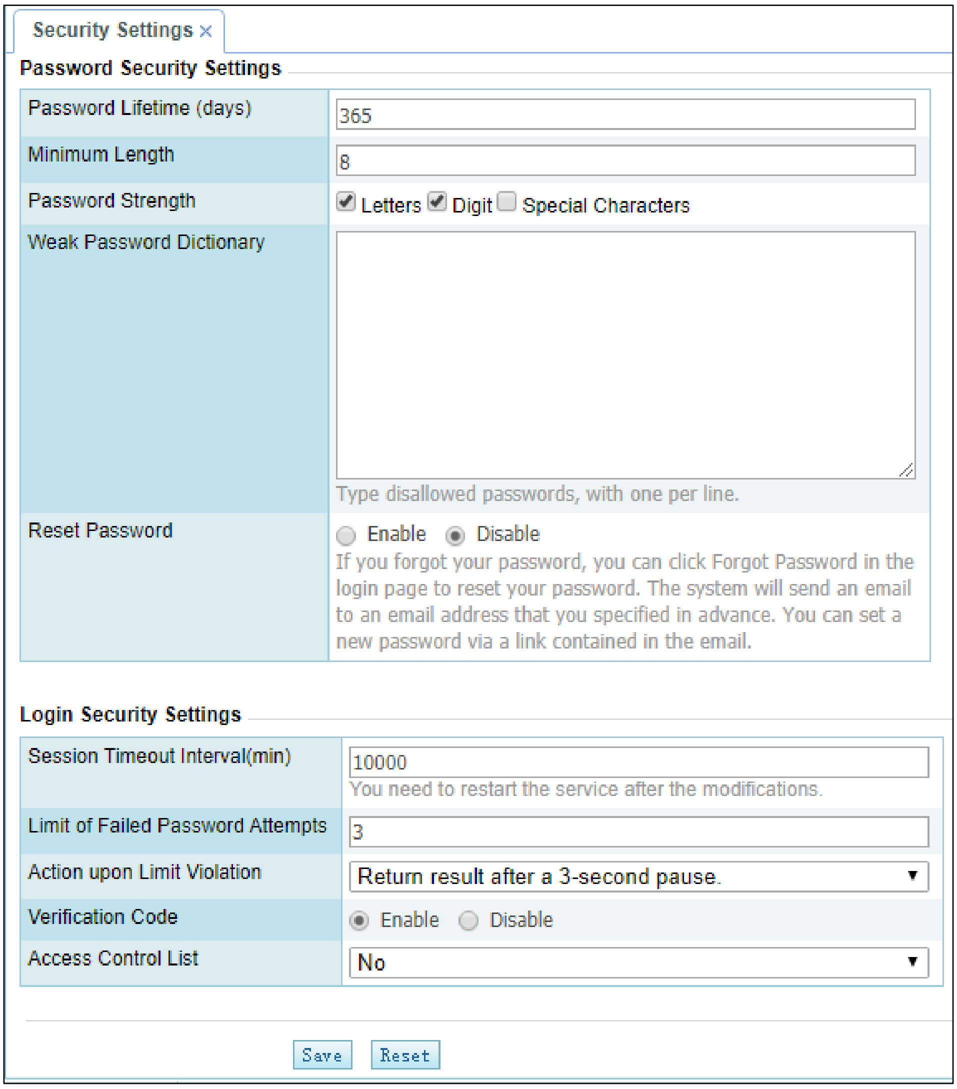
3.2.2 Security Settings

Only the system user **admin** can view and manage security settings. Therefore, this module is unavailable for other users.

Note	All users, including region users, can set **Password Strength** and **Weak Password Dictionary**, but **Login Security Settings** is configurable only for ADS M users.

Choose **Administration** > **User and Audit** > **Security Settings**. The **Security Settings** page appears, as shown in Figure 3-26.

Figure 3-26 Security settings



Password Security Settings

Password Lifetime (days)	365
Minimum Length	8
Password Strength	☑ Letters ☑ Digit □ Special Characters
Weak Password Dictionary	Type disallowed passwords, with one per line.
Reset Password	○ Enable ● Disable If you forgot your password, you can click Forgot Password in the login page to reset your password. The system will send an email to an email address that you specified in advance. You can set a new password via a link contained in the email.

Login Security Settings

Session Timeout Interval(min)	10000 You need to restart the service after the modifications.
Limit of Failed Password Attempts	3
Action upon Limit Violation	Return result after a 3-second pause. ▼
Verification Code	● Enable ○ Disable
Access Control List	No ▼

Table 3-14 describes parameters of security settings.

Table 3-14 Parameters of security settings

Parameter	Description
Password Lifetime (days)	Specifies the password validity. The value range is 0–65535. **0** indicates that there is no limit on the validity. The default value is **365** days.
Minimum Length	Specifies the minimum password length. The value is an integer ranging from 8 to 99, with **8** as the default.
Password Strength	Specifies the complexity of a password. By default, the password must contain letters and digits. Also, you can define that

Parameter	Description
	the password must contain at least two types of the following: letters, digits, and special characters.
Weak Password Dictionary	Specifies the passwords that are prohibited for use due to weak security. Each weak password should be in a separate line.
Reset Password	Controls whether the password resetting function is enabled. After this function is enabled, you can reset the password by email. For details about how to reset the password, see Resetting the Password in section 2.3 Other Operations.
Subject of Password Reset Email	Specifies the subject of the email message notifying password resetting. This can be defined by users.
Content of Password Reset Email	Specifies the content of the email message notifying password resetting. This can be defined by users, but the content must contain the string, ${url}; otherwise, password resetting would fail.
Session Timeout Interval(min)	Specifies how long a user can stay inactive before being automatically logged out of the system.
Limit of Failed Password Attempts	Specifies the maximum number of consecutive failed password attempts.
Action upon Limit Violation	Specifies the action that the system will take after the number of consecutive failed password attempts reaches the specified value. Values include the following: • **Return result after a 3-second pause** • **Lock client IP for 20 minutes**: The currently locked IP addresses are listed in the text box below. By default, a locked IP address will be automatically unlocked in 20 minutes. Alternatively, the administrator can delete a locked IP address from the list and then click **Save** to manually unlock this IP address.
Verification Code	Controls whether to enable the use of verification codes for login authentication. By default, it is disabled. • **Enable**: allows use of login verification codes, indicating that a user can successfully log in to ADS M only after typing a correct verification code. • **Disable**: disables use of verification codes for login authentication.
Access Control List	Specifies whether to allow a client to access the system. It has the following values: • **No**: indicates any clients can access to the system. • **Permit access from the following IP addresses**: indicates that only clients with IP addresses included in the text box below can access the system. • **Deny access from following IPs**: indicates that clients with IP addresses included in the text box below cannot access the system. When you access ADS from a blocked IP address, the system displays "You cannot log in from the current IP address. Ccontact the administrator to check access control settings." on the login page. Note After the access control list is successfully modified, you are advised to wait at least 3 minutes for the settings to take effect.

3.2.3 Authentication Configuration

ADS M supports local authentication and third-party server authentication for user authentication.

Note

- When local authentication is used, users can access ADS M using the user name and password configured under **Administration** > **User and Audit** > **User Management**.
- When third-party server authentication is used, users must add the user name and password configured on the third-party server to ADS M and use such user name and password to access ADS M.

Choose **Administration > User and Audit > Authentication Configuration**. Select an authentication method and configure parameters.

Table 3-15 describes parameters for configuring the authentication.

Table 3-15 Parameters for configuring the authentication

Parameter	Description
Authentication Mode	Specifies the authentication mode, which can be **Local Authentication**, **Radius Authentication**, **TACACS+**, or **LDAP**.
Authentication Server	Specifies the IP address or domain name of the authentication server. Both IPv4 and IPv6 addresses are supported. Note You can enter a domain name when **Authentication Mode** is set to **LDAP**.
Authentication Port	Specifies the port on which the authentication server listens for authentication requests.
Protocol Type	Specifies the authentication protocol of the authentication server. The options vary with the authentication server. Note This parameter is required when **Authentication Mode** is set to **Radius Authentication**, **TACACS+**, or **LDAP**.
Shared Key	Specifies the shared key that serves as a password of the authentication server. The shared key configured on ADS must be the same as that configured on the authentication server; otherwise, ADS cannot communicate with the server. Note This parameter is required when **Authentication Mode** is set to **Radius Authentication** or **TACACS+**.
Authentication Hold-in Time	Specifies the authentication duration, after which ADS returns the success or failure of the authentication information.

Parameter	Description
	Note This parameter is required when **Authentication Mode** is set to **TACACS+**.
Base DN	Specifies the top of the LDAP directory tree, namely, the base directory. Note This parameter is required when **Authentication Mode** is set to **LDAP**.
Username	Specifies the name of the LDAP user. Note This parameter is optional when **Authentication Mode** is set to **LDAP**.
Password	Specifies the password of the LDAP user. Note This parameter is optional when **Authentication Mode** is set to **LDAP**.

Step 2 Click **Save** to save the settings.

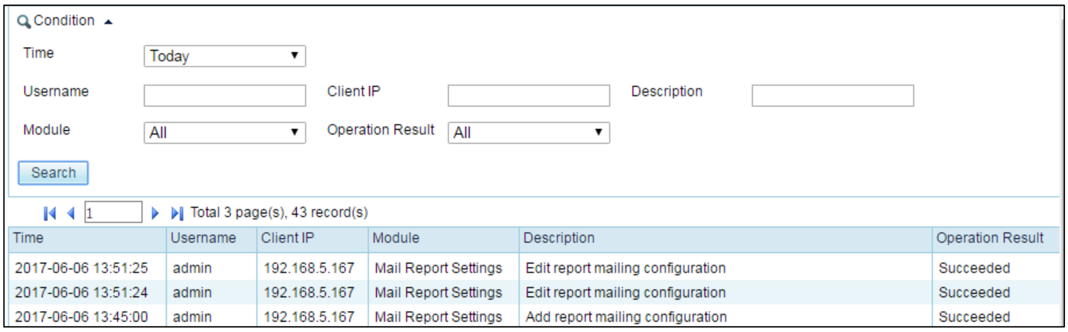
----End

3.2.4 Audit Log

Audit logs refer to all audit logs generated during ADS M operation and user operations. Only the system administrator can view audit logs.

Choose **Administration** > **User and Audit** > **Audit Log** to open the **Audit Log** page, as shown in Figure 3-27. By default, no audit log is available. After you click **Search**, all audit logs of ADS M are displayed, including generation time, user name, client IP address, functional module, operation result, and log description.

Figure 3-27 Audit log



Condition ▲

Time: Today ▼

Username:

Client IP:

Description:

Module: All ▼

Operation Result: All ▼

Search

1 Total 3 page(s), 43 record(s)

Time	Username	Client IP	Module	Description	Operation Result
2017-06-06 13:51:25	admin	192.168.5.167	Mail Report Settings	Edit report mailing configuration	Succeeded
2017-06-06 13:51:24	admin	192.168.5.167	Mail Report Settings	Edit report mailing configuration	Succeeded
2017-06-06 13:45:00	admin	192.168.5.167	Mail Report Settings	Add report mailing configuration	Succeeded

Table 3-16 describes audit log parameters.

Table 3-16 Audit log parameters

Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Username	Specifies the login user name. The full user name is required because fuzzy query is not allowed here.
Client IP	Specifies the IP address of the user device. The full IP address is required because fuzzy query is not allowed here.
Module	Specifies the functional module whose logs are queried.
Description	Specifies the keyword of logs to be queried.
Operation Result	Specifies the result of the operations performed on the client. **All** indicates that all operation result logs are displayed.

3.3 Third-Party Interface

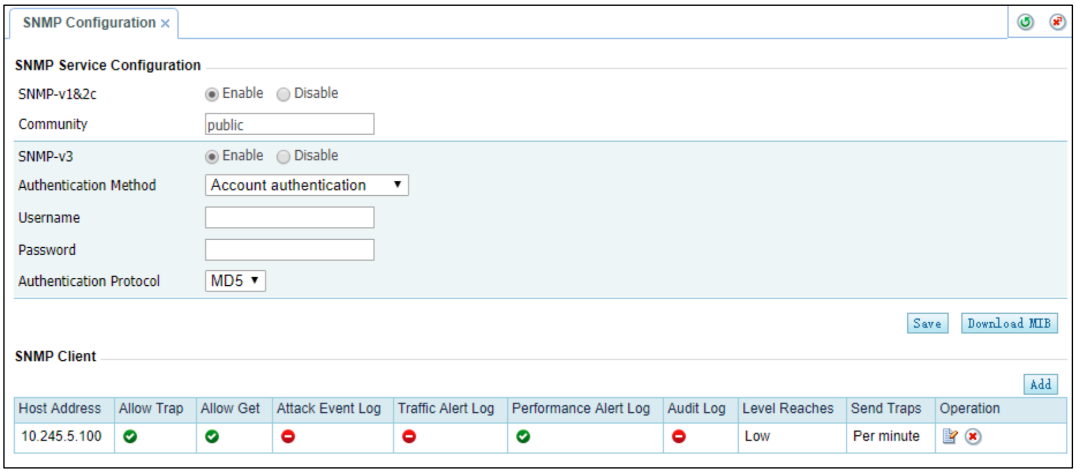
ADS M exchanges data with external systems via SNMP and syslog interfaces. The third-party interface configuration includes configuration of an SNMP server, syslog server, SMTP server, and other servers.

3.3.1 SNMP Configuration

ADS M supports management via the Simple Network Management Protocol (SNMP). ADS M can not only respond to queries from the SNMP manager as an agent by returning information about its running status, but also send trap messages to the SNMP manager.

Choose **Administration** > **Third-Party Interface** > **SNMP Configuration** to open the **SNMP Configuration** page. If an SNMP server is configured, the system automatically displays the client IP addresses that access ADS M through SNMP, as shown in Figure 3-28.

Figure 3-28 SNMP configuration



SNMP Service Configuration

SNMP-v1&2c	● Enable ○ Disable
Community	public
SNMP-v3	● Enable ○ Disable
Authentication Method	Account authentication ▼
Username	
Password	
Authentication Protocol	MD5 ▼

SNMP Client

Host Address	Allow Trap	Allow Get	Attack Event Log	Traffic Alert Log	Performance Alert Log	Audit Log	Level Reaches	Send Traps	Operation
10.245.5.100	✓	✓	⛔	⛔	✓	⛔	Low	Per minute	✎ ✖

Downloading a MIB File

On the page shown in Figure 3-28, click **Download MIB** in the lower-right corner of the **SNMP Service Configuration** area. In the dialog box that appears, click **Save**. Then the MIB file is downloaded to the local disk drive.

Configuring an SNMP Server

On the **SNMP Configuration** page, set SNMP client IP addresses and related parameters, and click **Save** to save the settings.

Table 3-17 describes parameters for configuring an SNMP server.

Table 3-17 Parameters for configuring an SNMP server

Parameter	Description
SNMP-v1&2c	Controls whether SNMPv1 and SNMPv2c are enabled for management.
Community	Specifies the community supported by the SNMP agent. This parameter is required when **SNMP-v1&2c** is set to **Enable**.
SNMP-v3	Controls whether SNMPv3 is enabled for management. Note When both **SNMP-v1&2c** and **SNMP-v3** are set to **Enable**, ADS M uses SNMP-v3 for authentication.
Authentication Method	Specifies the authentication method when **SNMP-v3** is set to **Enable**, which can be **No authentication**, **Account authentication**, or **Private key authentication**.
Username	Specifies the SNMP V3 user name.
Password	Specifies the password for user authentication via SNMPv3. This parameter is required when **Authentication Method** is set to **Account authentication** or **Private key authentication**.
Authentication	Specifies the protocol used for user authentication via SNMPv3, which can be **MD5**

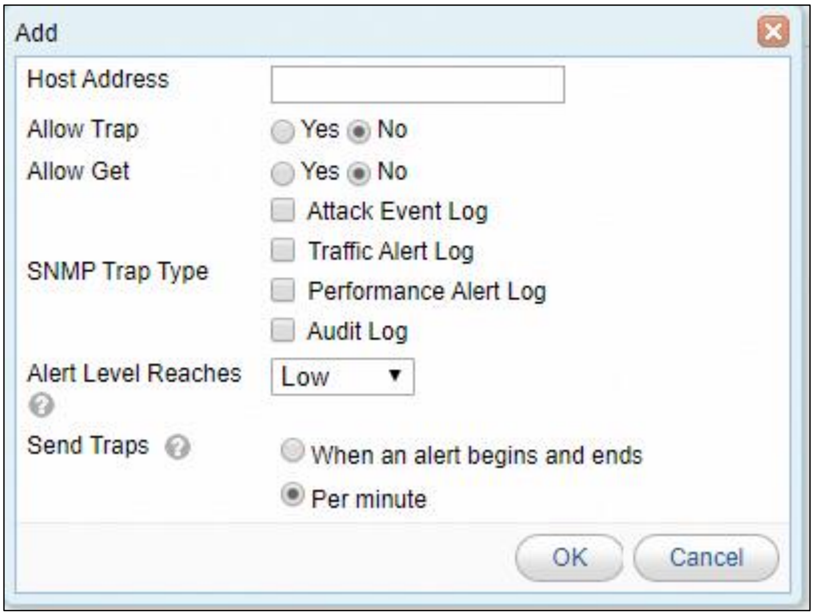
Parameter	Description
Protocol	or **SHA**. This parameter is required when **Authentication Method** is set to **Account authentication** or **Private key authentication**.
Private Key Protocol	The DES protocol is used by default and cannot be changed. This parameter is required only when **Authentication Method** is set to **Private key authentication**.
Private Key Password	Specifies the encrypted key password used during data transmission. This parameter is required only when **Authentication Method** is set to **Private key authentication**.

Configuring an SNMP Client

Step 1 Click **Add** in the **SNMP Client** area shown in Figure 3-28.

A dialog box appears, as shown in Figure 3-29.

Figure 3-29 Adding an SNMP client



Add

Host Address

Allow Trap ○ Yes ● No

Allow Get ○ Yes ● No

SNMP Trap Type □ Attack Event Log □ Traffic Alert Log □ Performance Alert Log □ Audit Log

Alert Level Reaches Low

Send Traps ○ When an alert begins and ends ● Per minute

Step 2 Configure parameters in the dialog box.

Table 3-18 Parameters for configuring an SNMP client

Parameter	Description
Host Address	Specifies the IP address of the client that accesses ADS M through SNMP. Both the IPv4 and IPv6 addresses are allowed.
Allow Trap	Controls whether to allow the client to send trap messages to ADS M.
Allow Get	Controls whether to allow ADS M to acquire information about the client through

Parameter	Description
	SNMP GET messages.
SNMP Trap Type	Specifies the type of SNMP trap messages, which can be **Attack Event Log**, **Traffic Alert Log**, **Performance Alert Log**, or **Audit Log**.
Alert Level Reaches	Specifies the alert level, which can be **Low**, **Medium**, or **High**. Logs of alerts of the specified level and above will be sent via SNMP traps. If no alerts reach the specified level, no logs are sent.
Send Traps	Interval of sending logs via SNMP traps. • **When an alert begins and ends**: sends a log respectively when the alert starts and ends once a specified threshold is exceeded. • **Per minute**: sends logs every minute. This parameter is valid only for attack event logs and traffic alert logs.

Step 3 Click **OK** to save the settings.

A SNMP client, after being created, can be edited and deleted.

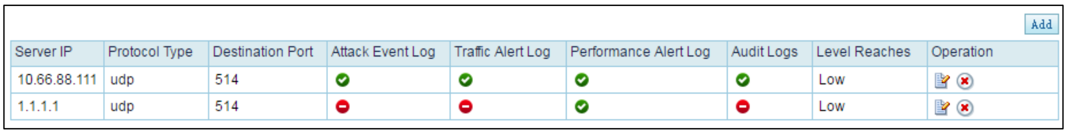
----End

3.3.2 Syslog Configuration

If the syslog server is used to transmit data between ADS M and devices under it, you need to configure syslog settings.

Choose **Administration** > **Third-Party Interface** > **Syslog Configuration** to open the **Syslog Configuration** page.

Figure 3-30 Syslog configuration

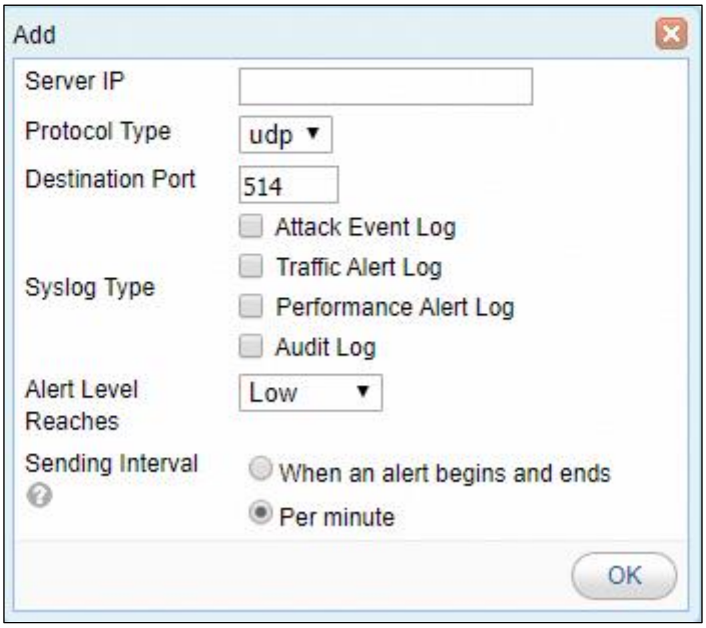


Server IP	Protocol Type	Destination Port	Attack Event Log	Traffic Alert Log	Performance Alert Log	Audit Logs	Level Reaches	Operation
10.66.88.111	udp	514	✓	✓	✓	✓	Low	✎ ⊗
1.1.1.1	udp	514	⊖	⊖	✓	⊖	Low	✎ ⊗

Adding a Syslog Server

On the **Syslog Configuration** page shown in Figure 3-30, click **Add** to add a syslog server.

Figure 3-31 Adding a syslog server



Add

Server IP:

Protocol Type: udp

Destination Port: 514

Syslog Type:
□ Attack Event Log
□ Traffic Alert Log
□ Performance Alert Log
□ Audit Log

Alert Level Reaches: Low

Sending Interval:
○ When an alert begins and ends
● Per minute

Table 3-19 describes syslog server parameters.

Table 3-19 Syslog server parameters

Parameter	Description
Server IP	Specifies the IP address of the syslog server.
Protocol Type	Specifies the protocol used for data transmission. By default, the UDP protocol is used.
Destination Port	Specifies the port of the syslog server.
Syslog Type	Specifies the type of data transmitted by the syslog server. Values are **Attack Event Log**, **Traffic Alert Log**, **Performance Alert Log**, and **Audit Log**. **Traffic Alert Log** is available only when ADS M works in NTA detection mode.
Alert Level Reaches	Specifies the alert level, which can be **Low**, **Medium**, or **High**. Logs of alerts of the specified level and above will be sent to the syslog server. If no alerts reach the specified level, no logs are sent.
Sending Interval	Interval of sending logs to the syslog server. • **When an alert begins and ends**: sends logs respectively when the alert starts and ends once a specified threshold is exceeded. • **Per minute**: sends logs every minute. This parameter is valid only for attack event logs.

Editing a Syslog Server

On the **Syslog Configuration** page shown in Figure 3-30, click ✎ in the **Operation** column of a syslog server to edit all its parameters, except **Server IP**.

Deleting a Syslog Server

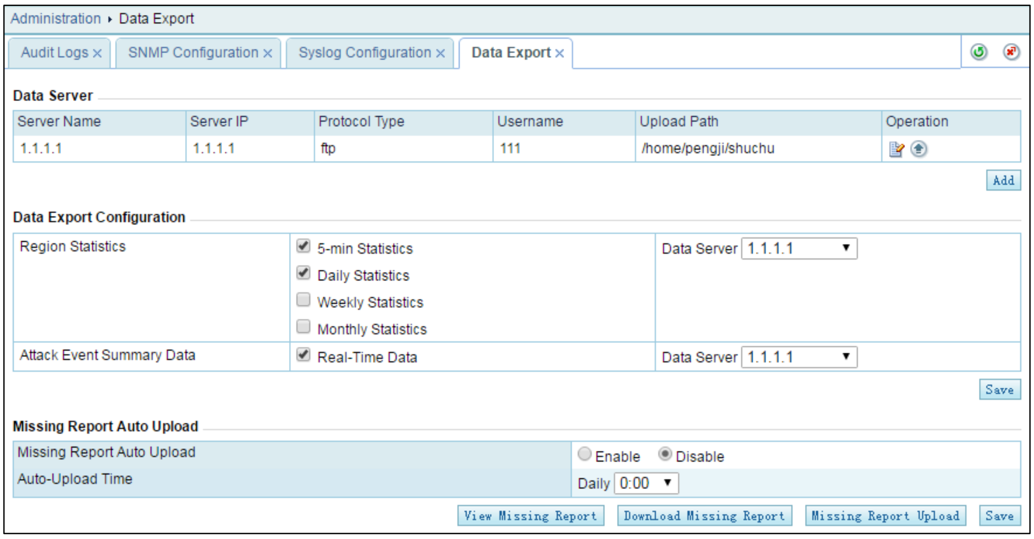
On the **Syslog Configuration** page shown in Figure 3-30, click ✖ in the **Operation** column of a syslog server and then click **OK** in the confirmation dialog box to delete this syslog server.

3.3.3 Data Export

Under **Administration** > **Third-Party Interface** > **Data Export**, you can export the data and upload it to a remote server for access by other users. You can add a data server and upload the reports generated by ADS M to it, as shown in Figure 3-32.

For missing reports that failed to be uploaded to the specified data server, you can configure automatic or manual upload for them.

Figure 3-32 Data export



Administration ▸ Data Export

Data Server

Server Name	Server IP	Protocol Type	Username	Upload Path	Operation
1.1.1.1	1.1.1.1	ftp	111	/home/pengji/shuchu	✎ ⊕

Data Export Configuration

Region Statistics	☑ 5-min Statistics ☑ Daily Statistics □ Weekly Statistics □ Monthly Statistics	Data Server 1.1.1.1 ▾
Attack Event Summary Data	☑ Real-Time Data	Data Server 1.1.1.1 ▾

Missing Report Auto Upload

Missing Report Auto Upload	○ Enable ● Disable
Auto-Upload Time	Daily 0:00 ▾

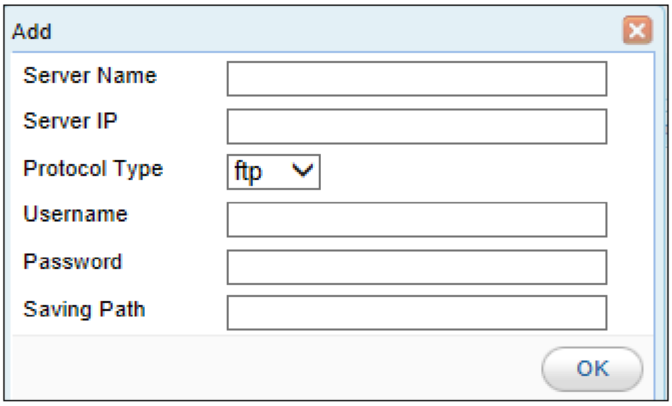
Adding a Data Server

You can export data only after a data server is configured.

Step 1 On the **Data Export** page shown in Figure 3-32, click **Add** to the lower right of the data server list.

Step 2 In the **Add** dialog box, configure parameters.

Figure 3-33 Adding a data server



Add

Server Name	
Server IP	
Protocol Type	ftp
Username	
Password	
Saving Path	

Table 3-20 describes parameters for adding a data server.

Table 3-20 Parameters for adding a data server

Parameter	Description
Server Name	Specifies the data server name.
Server IP	Specifies the IP address of the data server.
Protocol Type	Specifies the protocol used for data transmission, which can be **ftp**, **sftp**, or **scp**. By default, the FTP protocol is used.
Username	Specifies the user name for logging in to the remote data server.
Password	Specifies the password for logging in to the remote data server.
Saving Path	Specifies the path for saving the data uploaded to the remote data server.

Step 3 Click **OK** to complete the configuration.

----End

Editing a Remote Data Server

On the data server list, click 📝 in the **Operation** column to edit settings of a remote data server.

Deleting a Remote Data Server

On the data server list, click ☒ in the **Operation** column and then click **OK** in the confirmation dialog box to delete a remote data server.

Uploading Data to a Remote Data Server

On the data server list, click ⬆ in the **Operation** column to test whether files can be uploaded to a remote data server.

Configuring Data Export

Step 1 In the **Data Export Configuration** area, select the type of data to be exported and the server to which the data is uploaded.

Step 2 Click **Save** to complete the configuration.

----End

Configuring Missing Report Upload

Step 1 In the **Missing Report Auto Upload** area, set **Missing Report Auto Upload** to **Enable**.

Step 2 Specify the upload time and then click **Save** to save the settings.

----End

For missing reports that failed to be uploaded automatically, click **Missing Report Upload** to manually upload them to the data server. You can also click **View Missing Report** and **Download Missing Report** to view and download missing reports respectively.

3.3.4 Mail Alert Settings

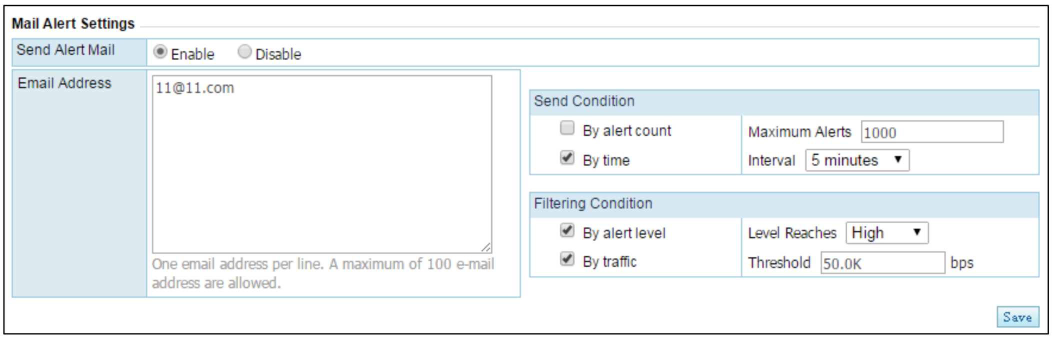
You can configure mail settings on the **Mail Alert Settings** page.

To configure alert mail settings, perform these steps:

Step 1 Choose **Administration** > **Third-Party Interface** > **Mail Alert Settings**.

Step 2 Set **Send Alert Mail** to **Enable**, and specify email addresses that receive alert mails, and set mail sending and filtering conditions for alert mails.

Figure 3-34 Mail alert settings



Mail Alert Settings

Send Alert Mail: ● Enable ○ Disable

Email Address: 11@11.com

One email address per line. A maximum of 100 e-mail address are allowed.

Send Condition

☐ By alert count — Maximum Alerts: 1000

☑ By time — Interval: 5 minutes ▼

Filtering Condition

☑ By alert level — Level Reaches: High ▼

☑ By traffic — Threshold: 50.0K bps

Note

Alerts of ADS devices and alerts related to HA are all high-level alerts. Alerts from NTA devices can be classified into low-level, medium-level, and high-level.

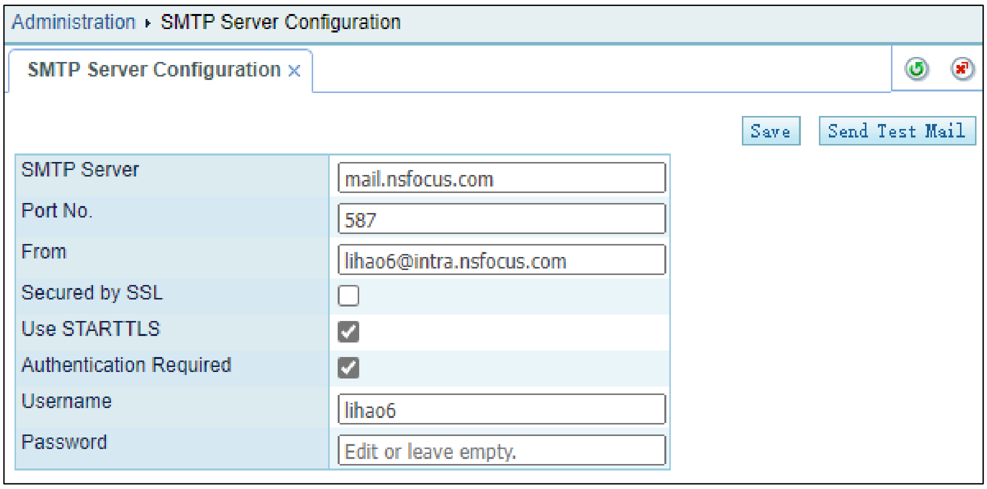
Step 3 Click **Save** to complete the configuration.

----End

3.3.5 SMTP Server Configuration

After enabling **Reset Password** (**Administration > User and Audit > Security Settings**), you must configure an SMTP server for sending the password resetting link to the user's email address. Figure 3-35 is the page for configuring an SMTP server for sending mails. You can modify related values in text boxes as required and then click **Save** in the upper-right corner.

Figure 3-35 SMTP server configuration



Administration ▸ SMTP Server Configuration
SMTP Server Configuration ×
Save
Send Test Mail

SMTP Server: mail.nsfocus.com
Port No.: 587
From: lihao6@intra.nsfocus.com
Secured by SSL: □
Use STARTTLS: ☑
Authentication Required: ☑
Username: lihao6
Password: Edit or leave empty.

Table 3-21 lists parameters for configuring an SMTP server.

Table 3-21 Parameters for configuring an SMTP server

Parameter	Description
SMTP Server	Specifies the IP address or domain name of the SMTP server that sends emails.
Port No.	Specifies the port of the SMTP server.
From	Specifies the email address from which emails are sent.
Username	Specifies the user name of the account from which emails are sent. This parameter is required only when **Authentication Required** is selected.
Password	Specifies the password of the account from which emails are sent. This parameter requires a value only when **Authentication Required** is selected.
Secured by SSL	Controls whether a security password is required for the email sender for identity authentication.
Use STARTTLS	STARTTLS used by the email sender for authentication.

3.3.6 Portal Configuration

The ADS M administrator sets an ADS Portal account for users in a region and then configures and deploys the Portal as required. After that, the customer's hosts in the region can learn network monitoring information of the region via ADS Portal.

Choose **Administration > Third-Party Interface > Portal Configuration** to perform the following operations regarding the Portal:

- Deploying the portal
- Configuring portal authentication parameters
- Replacing the logo
- Replacing the SSL certificate
- Configuring login security parameters

For details about how to perform these operations, see the "Managing the Portal" section of *NSFOCUS ADS Portal User Guide*.

3.3.7 File Download

You can download the file that describes data interfaces from the web-based manager of ADS M.

Choose **Administration > Third-Party Interface > File Download** and click 💾 in the **Operation** column to download the file to a local disk drive.

3.4 Diagnosis

This section describes methods to diagnose ADS M faults.

3.4.1 Debug Information Collection

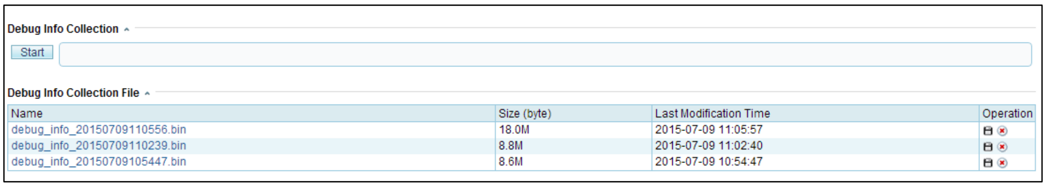
When ADS M fails, you can collect debug information, including the device's basic information and configuration information, for which a compressed file is generated. You can download this file and send it to NSFOCUS technical support for fault diagnosis.

Choose **Administration > Diagnosis > Debug Info Collection**. Then click **Start** on the **Debug Info Collection** page to collect information about the current device. The generated information file will be saved in the debug information file list. See Figure 3-36.

You can click 💾 in the **Operation** column to download the file to a local disk drive.

A maximum of five debug information files are listed on the **Debug Info Collection** page. If more files are generated, the file with the earliest **Last Modification Time** will be deleted automatically.

Figure 3-36 Debug information collection



Name	Size (byte)	Last Modification Time	Operation
debug_info_20150709110556.bin	18.0M	2015-07-09 11:05:57	💾 ⊗
debug_info_20150709110239.bin	8.8M	2015-07-09 11:02:40	💾 ⊗
debug_info_20150709105447.bin	8.6M	2015-07-09 10:54:47	💾 ⊗

3.4.2 Network Diagnosis

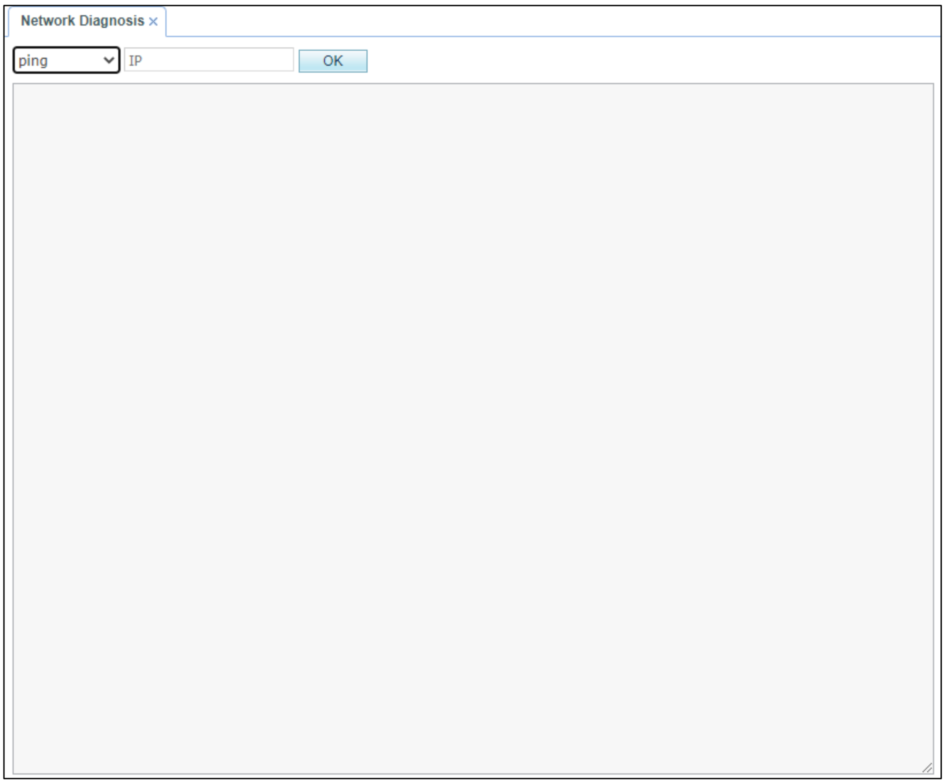
When ADS M becomes faulty or cannot be connected, you can use the following analysis tools:

- ping: checks whether an IPv4 host is alive or connects to the network.
- ping6: checks whether an IPv6 host is alive or connects to the network.
- traceroute: tracks the route packets taken from a network to an IPv4 address.
- Traceroute6: tracks the route packets taken from a network to an IPv6 address.
- telnet: checks whether the peer port is reachable.

To perform network diagnosis, follow these steps:

Step 1 Choose **Administration** > **Diagnosis** > **Network Diagnosis**.

Figure 3-37 Network Diagnosis page



Step 2 Select a tool and type an IPv4 or IPv6 address (and a port number if **telnet** is selected) in the **IP** text box.

Step 3 Click **OK**.

The check result is then displayed in the text box below.

----End

3.4.3 Remote Assistance

When ADS M becomes faulty, you can enable the remote assistance function, allowing NSFOCUS technical support to provide remote support.

By default, this function is disabled. You need to enable it before using the function.

To enable the remote assistance function, follow these steps:

Step 1 Choose **Administration > Diagnosis > Remote Assistance**.

Step 2 Click **Open** and configure the following parameters for remote access.

You can configure at most three IP addresses.

- **Port**: enter a port number in the range of 1024–65535, excluding 50022. Leaving it empty indicates that a random port will be used.
- **Allowed IP**: you can configure at most three IP addresses.

Step 3 Click **OK** to complete the configuration.

Then the login key, its QR code, and port used by the specified IP address for remote access to ADS M are displayed below.

----End

4 Traffic Monitoring

The Traffic Monitoring module provides the following information:

Section	Description
Overview	Displays monitoring information regarding traffic, attack events, and status information of the managed devices (NTA and ADS).
DDoS Traffic Monitoring	Displays traffic information of specified IP addresses, protection groups, regions, region IP groups, and ADS.
Network Traffic Monitoring	Displays traffic information of a specified IP group, region, regional IP group, and NTA device.
Attack Events	Displays attack information of specified IP addresses, protection groups, regions, region IP groups, and ADS.
Countermeasures	Displays statistics of traffic dropped by ADS.

4.1 Overview

After you log in to the web-based manager, the **Overview** page appears, displaying the following monitoring information:

- Six types of traffic and six types of attack events detected by ADS
- Top NTA alerts
- System status of NTA and ADS

Table 4-1 describes in detail the monitoring information on the **Overview** page.

Table 4-1 Monitoring information displayed on the Overview page

Category	Monitoring Information	Description
DDoS traffic	Top destination IP addresses	Displays in real time top 10 protected IP addresses ranked according to traffic dropped by ADS in the last 30 seconds, letting users know which IP addresses see the largest traffic or are most severely attacked.
	Top regions by attack traffic	Displays in real time top 10 protected regions ranked according to traffic dropped by ADS in the last 30 seconds, letting users know which regions see the largest traffic or are most severely attacked.
	Protocol analysis	Provides an overview of TCP, UDP, and ICMP traffic handled by

Category	Monitoring Information	Description
		ADS in the last 30 minutes as well as details about each type of traffic.
	Attack traffic trend	Displays the trends of traffic received, dropped, and forwarded by ADS in the last 30 minutes.
	Attack traffic trend (peak size)	Displays the trends of traffic destined for an IP address or region that has been received, dropped, and passed by ADS in the last 30 minutes.
	Top destination IPs (by attack peak size)	Displays top 10 protected IP addresses of an object ranked according to traffic dropped by ADS in the last 30 seconds, letting users know which IP addresses of the object see the largest traffic or are most severely attacked.
Attack events	Top source countries	Displays in real time top 10 attack source countries/regions ranked according to attack traffic dropped by ADS in the last 30 seconds.
	Attack traffic	Displays the trend of attack traffic handled by ADS in the last 30 minutes and traffic statistics of various attack types at each point of time.
	Top NTA alerts	Displays in real time top 5 traffic alerts generated by NTA in the last 30 seconds.
	Top ongoing attack events	Displays in real time top 10 ongoing attack events handled by ADS in the last 30 seconds.
	Top 10 source IP addresses	Displays in real time top 10 source IP addresses ranked according to traffic dropped by ADS in the last 30 seconds.
	Attack type distribution	Displays in real time all attack types handled by ADS in the last 30 seconds and the percentage of each type of attack traffic to the total attack traffic.
Devices	Device monitoring	Displays in real time the status, CPU usage, and memory usage of NTA and ADS in the last 30 seconds.
Network traffic	Top NTA regions by traffic	Displays traffic in the last 30 minutes received and transmitted by regions configured on NTA under monitoring of ADS M.
	Trend of traffic on NTA	Displays trends of traffic in the last 30 minutes received and transmitted by NTA under monitoring of ADS M.

4.1.1 Adding a Panel

The **Overview** page can present the following panels:

- Attack Traffic Trend
- Protocols Analysis
- Top Destination IP
- Top Region Attack Traffic
- Attack Traffic Trend (Peak Size)
- Top Destination IPs (by Attack Peak Size)
- Top Source Countries
- Attack Traffic
- Top NTA Alerts

- Top Ongoing Attack Events
- Top 10 Source IP
- Attack Type Distribution
- Device Monitoring
- Top NTA Region Traffic
- NTA Traffic Trend

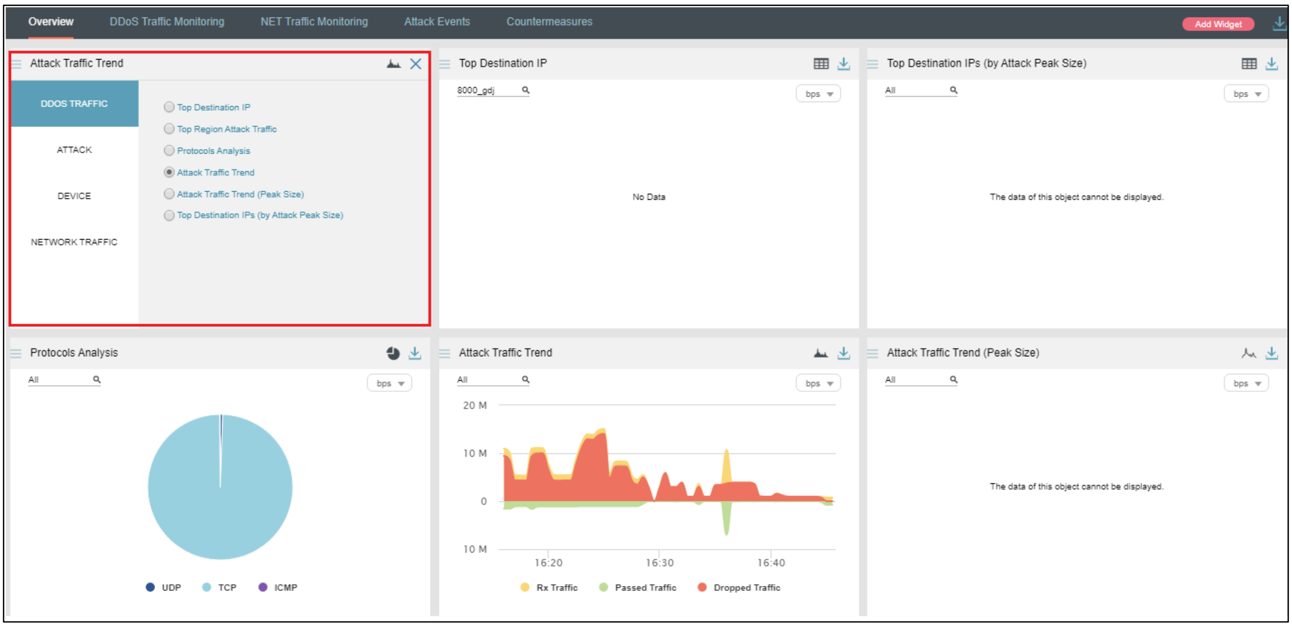
You can add panels as required by performing the following steps:

Step 1 Choose **Traffic Monitoring** > **Overview**.

Step 2 Click **Add Widget** in the upper-right corner of the page.

Then a box appears in the upper-left corner, as shown in Figure 4-1, for you to choose a panel to display on the **Overview** page.

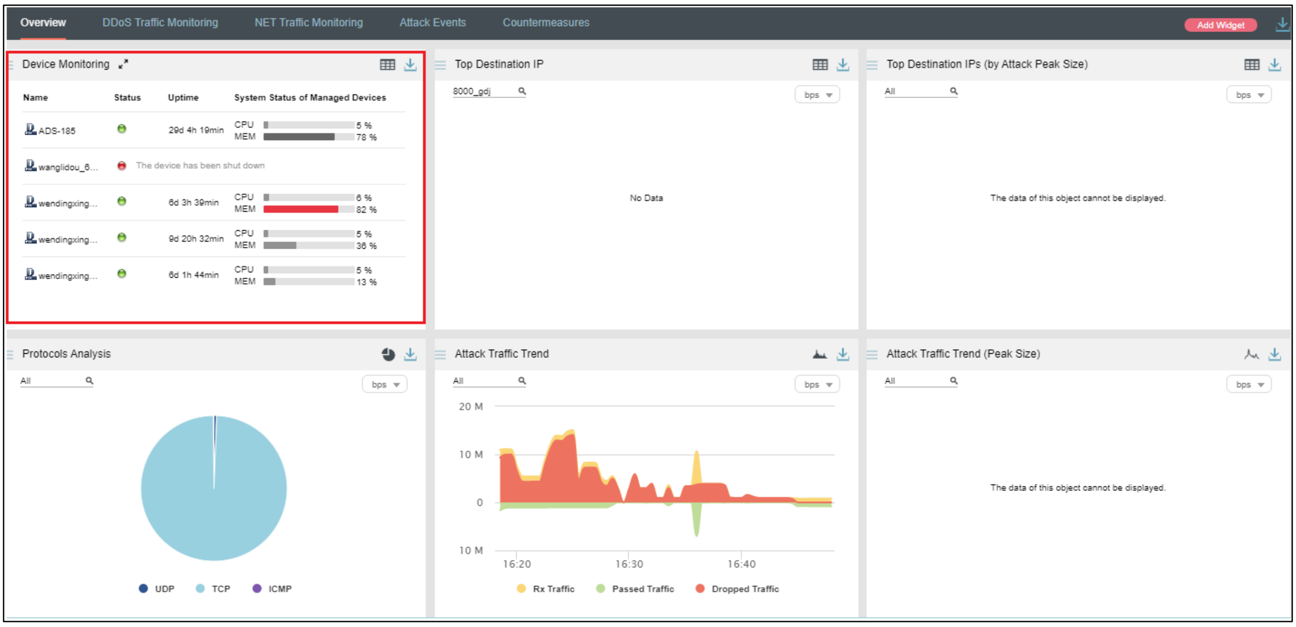
Figure 4-1 Adding a panel



Step 3 Select a category (DDOS TRAFFIC, ATTACK, DEVICE, or NETWORK TRAFFIC) from the left pane and then click a panel in the right pane.

Then the new panel appears on the **Overview** page. For example, if you select **DEVICE** and **Device Monitoring** respectively, the **Device Monitoring** panel appears in the upper-left corner, as shown in Figure 4-2.

Figure 4-2 New panel displayed



Name	Status	Uptime	System Status of Managed Devices
ADS-185	●	29d 4h 19min	CPU 5 % MEM 78 %
wanglidou_6...	●	The device has been shut down	
wendingxing...	●	6d 3h 39min	CPU 6 % MEM 82 %
wendingxing...	●	9d 20h 32min	CPU 5 % MEM 36 %
wendingxing...	●	6d 1h 44min	CPU 5 % MEM 13 %

----End

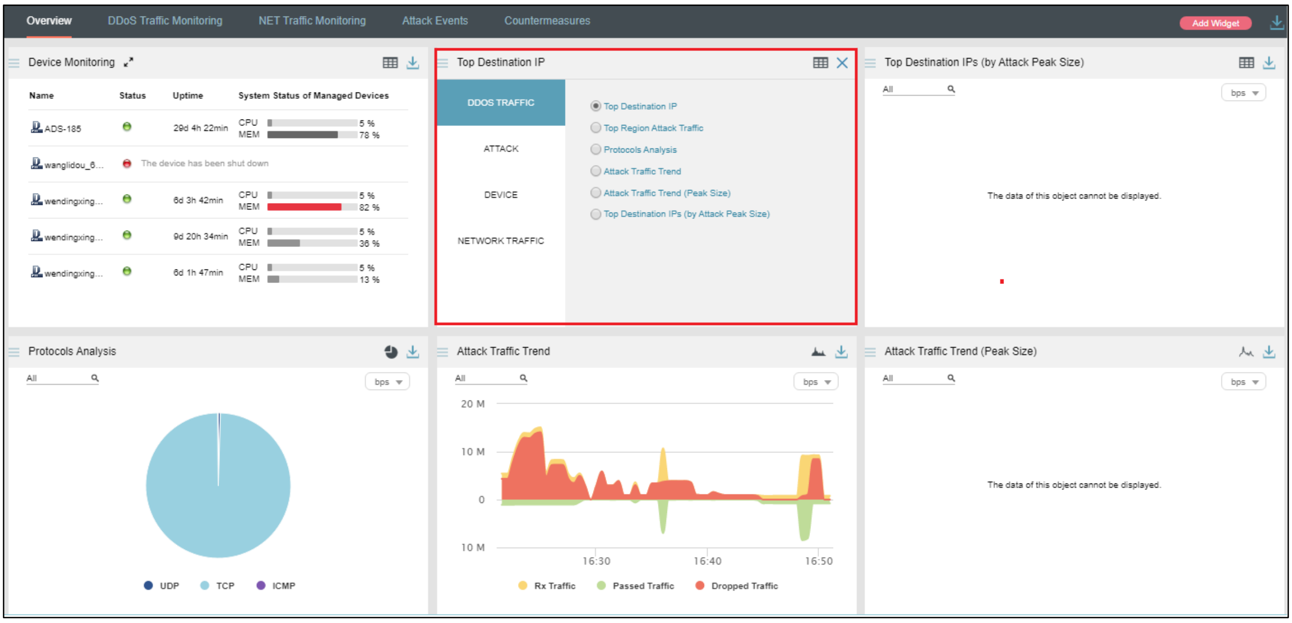
4.1.2 Replacing a Panel

You can change a panel by performing the following steps:

Step 1 On the **Overview** page, click ≡ in the upper-left corner of a panel, for example, **Top Destination IP**.

Then the panel flips around, as shown in Figure 4-3.

Figure 4-3 Reversed panel



● Top Destination IP

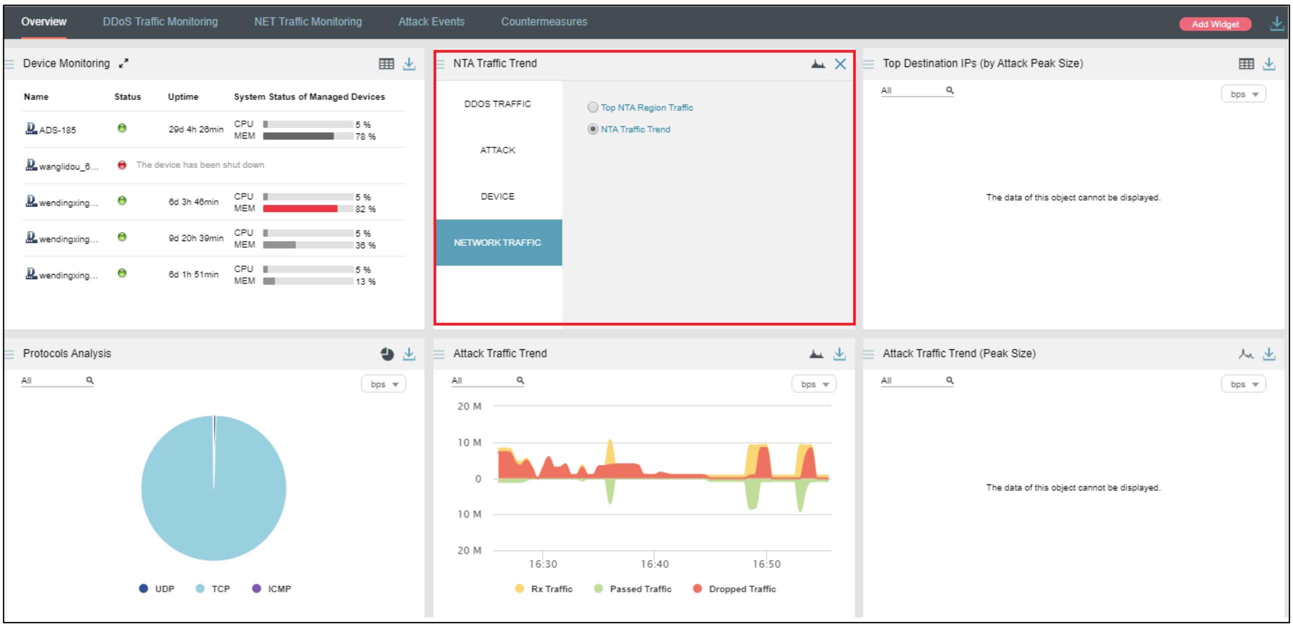
Name	Status	Uptime	System Status of Managed Devices
ADS-185	●	29d 4h 22min	CPU 5 % MEM 78 %
wanglidou_6...	●	The device has been shut down	
wendingxing...	●	6d 3h 42min	CPU 5 % MEM 82 %
wendingxing...	●	9d 20h 34min	CPU 5 % MEM 36 %
wendingxing...	●	6d 1h 47min	CPU 5 % MEM 13 %

The data of this object cannot be displayed.

The data of this object cannot be displayed.

Step 2 Specify another panel to display, for example, **NTA Traffic Trend** under **NETWORK TRAFFIC**, as shown in Figure 4-4.

Figure 4-4 Specifying another panel to display



● NTA Traffic Trend

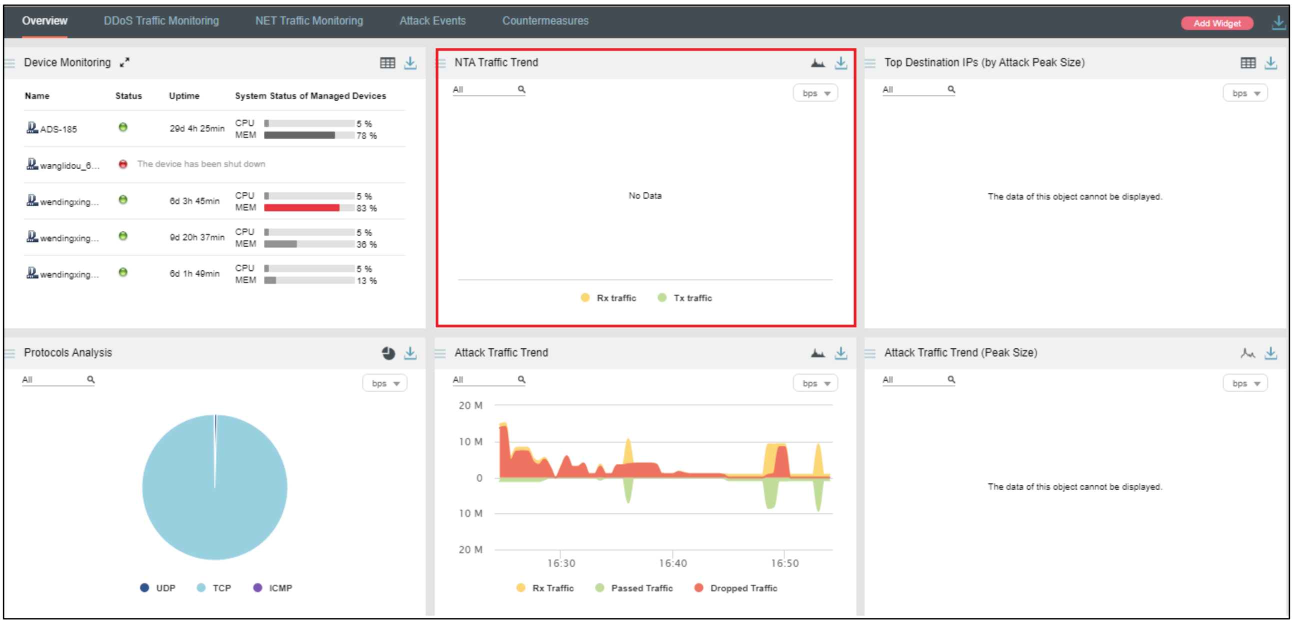
Name	Status	Uptime	System Status of Managed Devices
ADS-185	●	29d 4h 26min	CPU 5 % MEM 78 %
wanglidou_6...	●	The device has been shut down	
wendingxing...	●	6d 3h 46min	CPU 5 % MEM 82 %
wendingxing...	●	9d 20h 39min	CPU 5 % MEM 36 %
wendingxing...	●	6d 1h 51min	CPU 5 % MEM 13 %

The data of this object cannot be displayed.

The data of this object cannot be displayed.

Then the selected panel appears, as shown in Figure 4-5.

Figure 4-5 New panel displayed



Name	Status	Uptime	System Status of Managed Devices
ADS-185	●	29d 4h 25min	CPU 5 % MEM 78 %
wanglidou_6...	●	The device has been shut down	
wendingxing...	●	6d 3h 45min	CPU 5 % MEM 83 %
wendingxing...	●	9d 20h 37min	CPU 5 % MEM 36 %
wendingxing...	●	6d 1h 49min	CPU 5 % MEM 13 %

No Data

The data of this object cannot be displayed.

The data of this object cannot be displayed.

----End

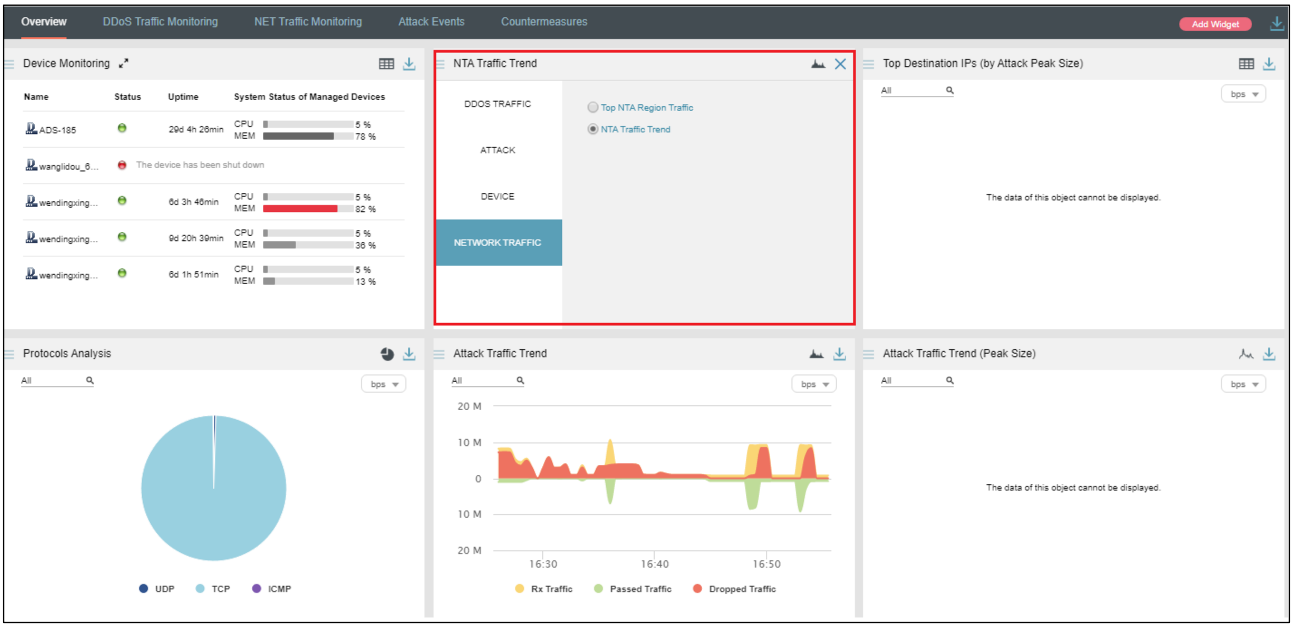
4.1.3 **Deleting a Panel**

You can delete an unnecessary panel by performing the following steps:

Step 1 On the **Overview** page, click ☰ in the upper-left corner of the unnecessary panel.

Then the panel flips around, as shown in Figure 4-6.

Figure 4-6 Reversed panel



Name	Status	Uptime	System Status of Managed Devices
ADS-185	●	29d 4h 26min	CPU 5 % MEM 78 %
wanglidou_6...	●	The device has been shut down	
wendingxing...	●	6d 3h 46min	CPU 5 % MEM 82 %
wendingxing...	●	9d 20h 39min	CPU 5 % MEM 36 %
wendingxing...	●	6d 1h 51min	CPU 5 % MEM 13 %

Step 2 Click ✕ in the upper-right corner of the panel.

Then the panel disappears.

----End

4.1.4 Downloading a Report

You can export panel-specific reports and then download them in PDF format to a local disk drive. In addition, you can export an integrated report that provides data of all panels.

The procedure is as follows:

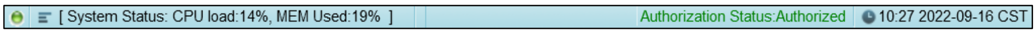
On the **Overview** page, export a report of data displayed on a single panel or an integrated report of data displayed on all panels.

- Click ⤓ in the upper-right corner of a panel and then click HTML or PDF to export data of this panel as an HTML or PDF report.
- Click ⤓ in the upper-right corner of the page and then click HTML or PDF to download all data displayed on this page as an HTML or PDF report.

4.1.5 Viewing the System Status Bar

The system status bar at the bottom of the web-based manager displays the system service status (● indicates that the device works properly), system status (CPU usage and memory usage), and system time, as shown in Figure 4-7.

Figure 4-7 System status bar



● [System Status: CPU load:14%, MEM Used:19%] Authorization Status:Authorized 10:27 2022-09-16 CST

Clicking system status information in the left of the status bar shows details such as CPU usage and temperature, memory usage, motherboard temperature, fan status, temporary data partition, database partition, and file data partition. Clicking system status information in the status bar again will hide it.

Items in red indicate that the specified threshold is exceeded. For alert details, see section 3.1.9 Local Performance Alert Configuration.

4.1.6 Generating Sound Alerts

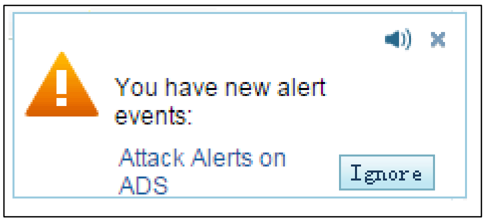
After sound alerting is enabled, the system makes a sound and displays an alert reminder box, as shown in Figure 4-8, when either of the following conditions is met:

- An attack alert or link status alert is generated by ADS.
- A traffic alert is generated by NTA.

In the box shown in this figure, you can perform the following operations:

- Click 🔊 to disable sound alerting.
- Click ✕ to close this box.
- Click **Ignore** to ignore this new alert.

Figure 4-8 Sound alert



You have new alert events:

Attack Alerts on ADS

For how to disable sound alerting, see section 3.1.1 Basic Settings.

4.1.7 Viewing Attack Traffic Trends

The **Attack Traffic Trend** panel shows trends of traffic received, forwarded, and dropped by ADS in the last 30 minutes.

Data on this panel refreshes every 30 seconds.

4.1.7.1 Understanding Data on the Panel

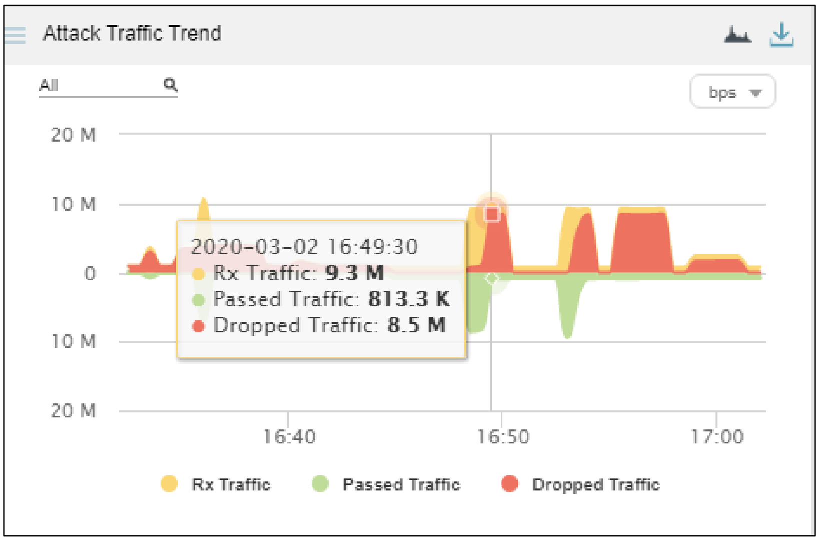
In the **Attack Traffic Trend** graph,

- The x-axis indicates time, spanning the last 30 minutes.
- The y-axis indicates traffic:
  - Traffic above 0: The yellow color indicates the total traffic received by ADS and the red color indicates dropped traffic.
  - Traffic below 0: The green color indicates legitimate traffic allowed by ADS to pass through.

4.1.7.2 Viewing Traffic at a Random Point of Time

Pointing to a random point in the **Attack Traffic Trend** graph displays the specific time and values of incoming traffic, forwarded traffic, and dropped traffic, as shown in Figure 4-9.

Figure 4-9 Detailed traffic information at a specific point of time



2020-03-02 16:49:30
● Rx Traffic: **9.3 M**
● Passed Traffic: **813.3 K**
● Dropped Traffic: **8.5 M**

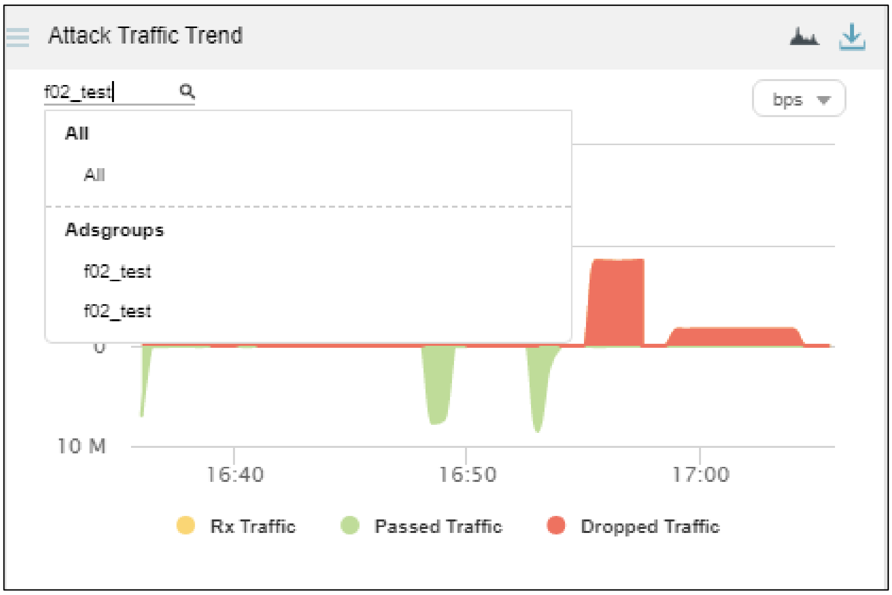
4.1.7.3 Viewing Traffic of a Specified Object

By default, the **Attack Traffic Trend** graph presents trends of traffic handled by all ADS devices. You can view real-time traffic trends of a specified region, regional IP group, ADS device, ADS-protected group, or IPv4/IPv6 address.

Step 1 On the page shown in Figure 4-9, type a character string and then press **Enter**.

The system displays all objects containing the typed character string, as shown in Figure 4-10.

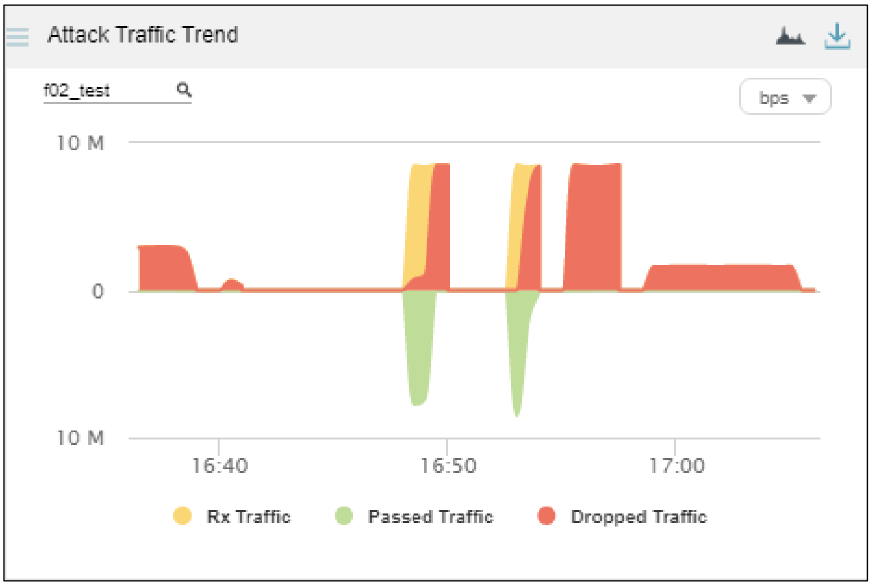
Figure 4-10 Specifying an object to view its attack traffic trend



Step 2 Select an object and press **Enter**.

Traffic trends of the specified object are displayed, as shown in Figure 4-11.

Figure 4-11 Real-time traffic trends of a specified object

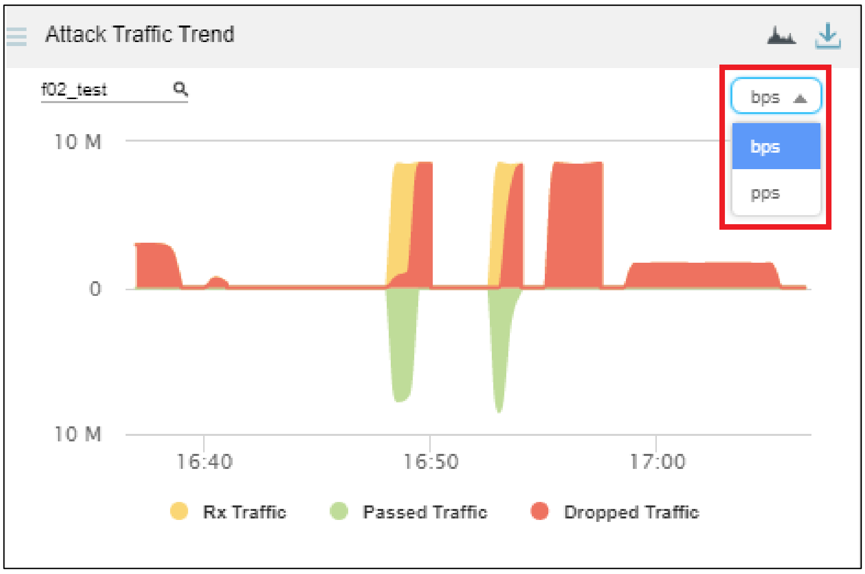


----End

4.1.7.4 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Attack Traffic Trend** panel to display traffic data in pps, as shown in Figure 4-12.

Figure 4-12 Switching the traffic unit



4.1.7.5 Downloading a Report

Click in the upper-right corner of the **Attack Traffic Trend** panel and then click HTML or PDF to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.8 Viewing Protocol-Specific Traffic

The **Protocols Analysis** panel provides an overview of TCP, UDP, and ICMP traffic handled by ADS in the last 30 minutes as well as details about each type of traffic.

Data on this panel refreshes every 30 seconds.

4.1.8.1 Understanding Data on the Panel

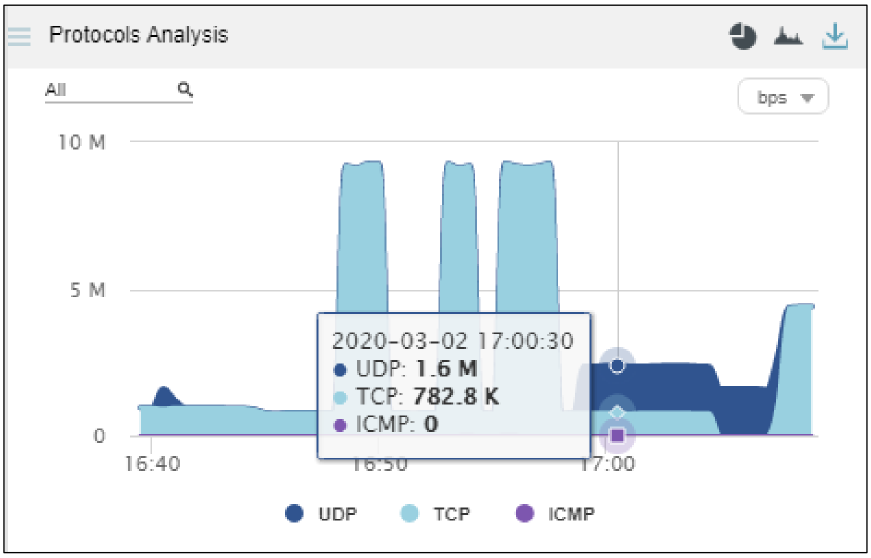
In the **Protocols Analysis** graph,

- The x-axis indicates time, spanning the last 30 minutes.
- The y-axis indicates traffic. UDP, TCP, and ICMP traffic is presented in dark blue, light blue, and purple respectively.

4.1.8.2 Viewing Traffic of Different Protocols at a Random Point of Time

Pointing to a random point in the **Protocols Analysis** graph displays the time and values of UDP traffic, TCP traffic, and ICMP traffic, as shown in Figure 4-13.

Figure 4-13 Traffic of different protocols at a specific point of time



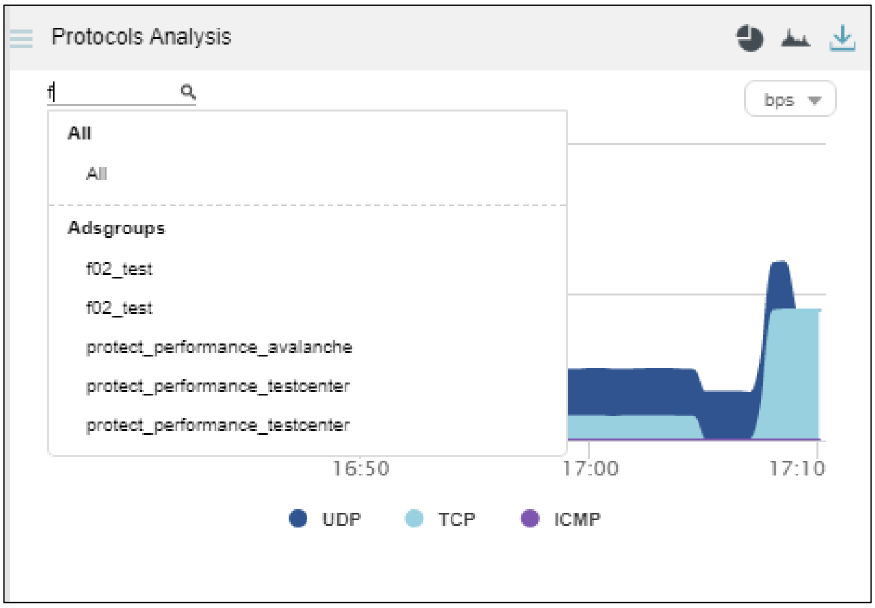
4.1.8.3 Viewing Traffic of a Specified Object

By default, the **Protocols Analysis** graph presents traffic of various protocols based on data collected from all ADS devices. You can specify a region, region IP group, ADS device, ADS-protected group, or IPv4 or IPv6 address to view its real-time, protocol-specific traffic.

Step 1 On the page shown in Figure 4-13, type a character string and then press **Enter**.

The system displays all objects containing the typed character string, as shown in Figure 4-14.

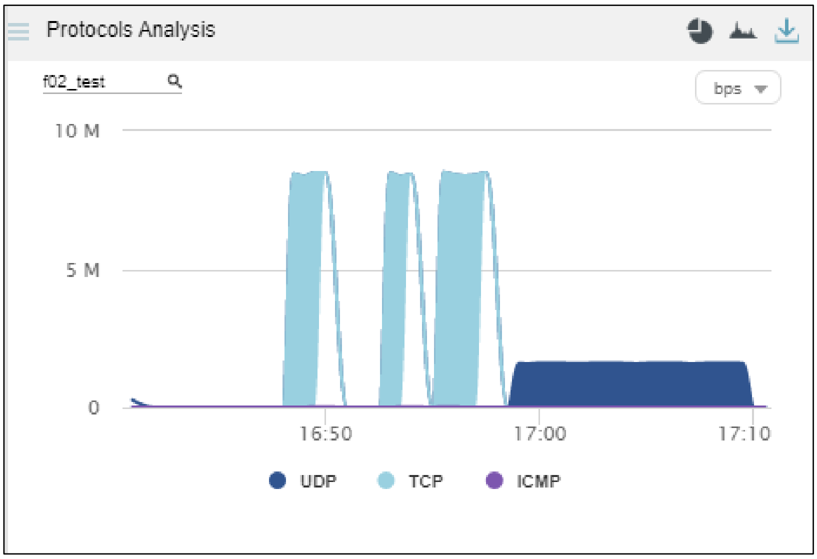
Figure 4-14 Searching for an object


Protocols Analysis
f
bps
All
All
Adsgroups
f02_test
f02_test
protect_performance_avalanche
protect_performance_testcenter
protect_performance_testcenter
16:50
17:00
17:10
UDP
TCP
ICMP

Step 2 Select an object and press **Enter**.

Traffic trends of the specified object in the last 30 minutes are displayed, as shown in Figure 4-15.

Figure 4-15 Real-time traffic trends of a specified object

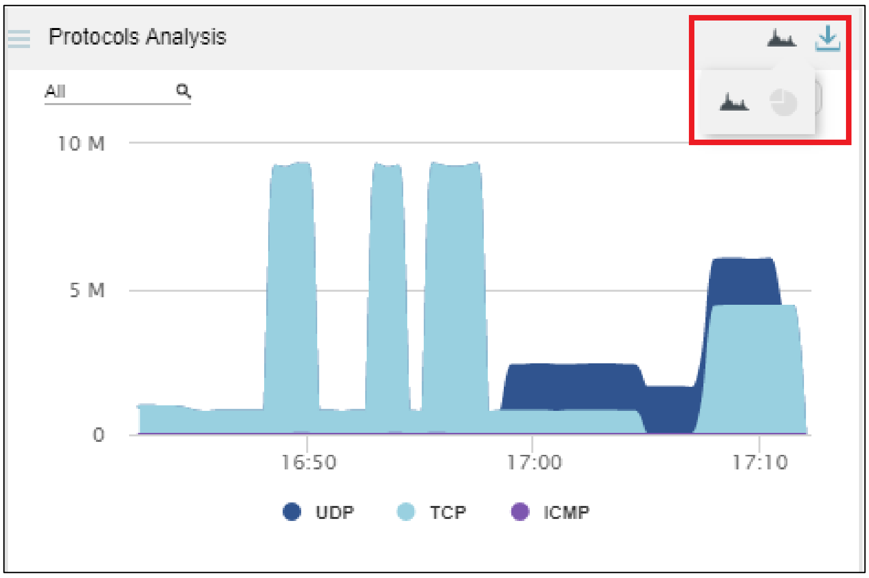


----End

4.1.8.4 Switching the Display Mode

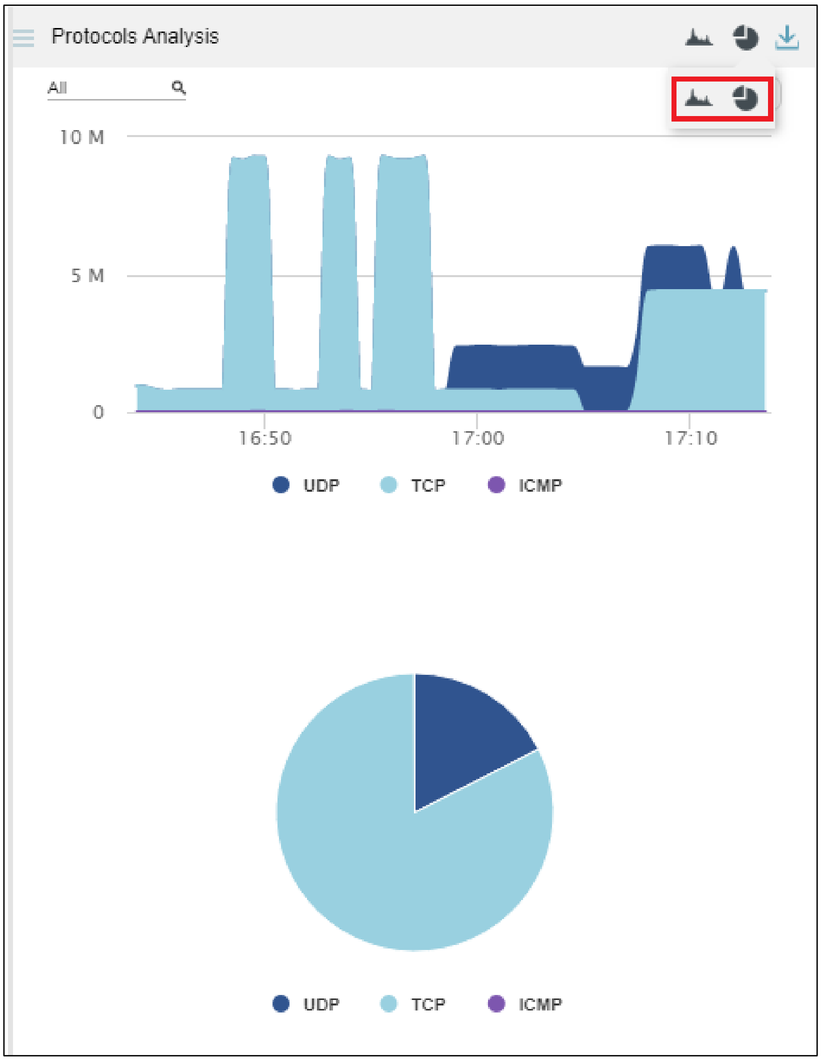
By default, protocol-specific traffic data is presented in an area graph. You can click and/or to display real-time traffic data in an area graph and/or pie chart, as shown in Figure 4-16.

Figure 4-16 Switching the display mode



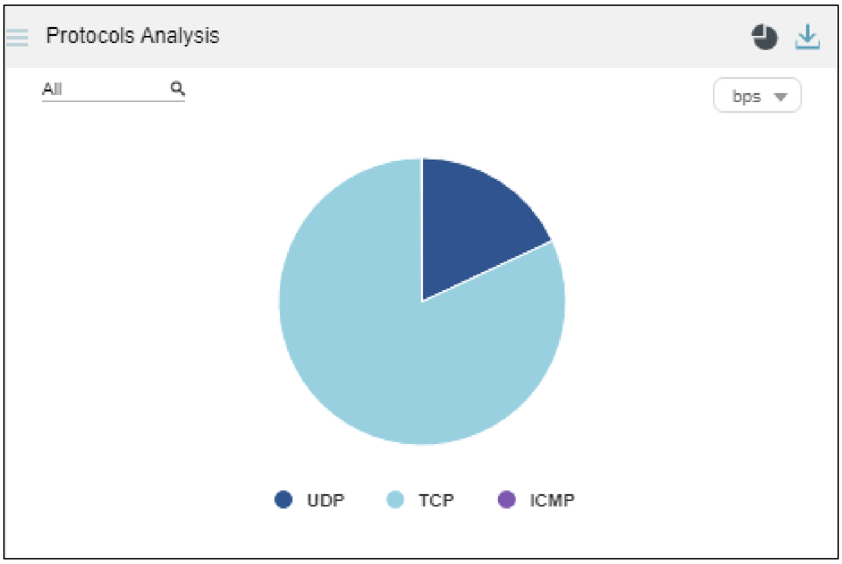
In Figure 4-16, 📈 appears normal, while ◕ appears dimmed. Therefore, data is presented only in an area graph. After you click ◕, this icon turns ◕. In this case, traffic data is presented in both an area graph and pie chart, as shown in Figure 4-17.

Figure 4-17 Display of traffic data in an area graph and pie chart



Clicking 📈 makes this icon dimmed and hides the area graph, as shown in Figure 4-18.

Figure 4-18 Display of traffic data in a pie chart

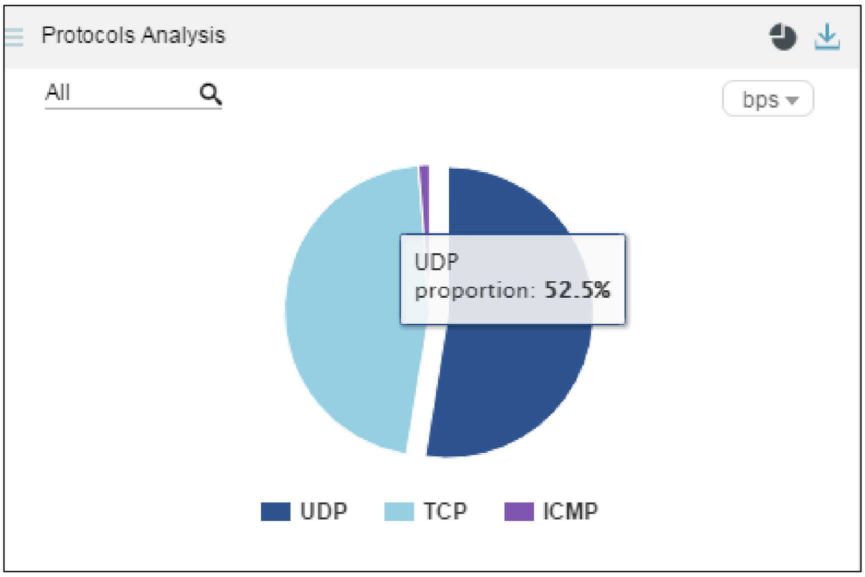


4.1.8.5 Viewing the Percentage of Protocol-Specific Traffic

Pointing to a random point in the pie chart displays the protocol name and the percentage of protocol-specific traffic to the total traffic.

Clicking in this area separates this area from other areas, as shown in Figure 4-19.

Figure 4-19 Area representing traffic of a protocol separated from other areas



4.1.8.6 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Protocols Analysis** panel to display traffic data in pps.

4.1.8.7 Downloading a Report

Click ⬇ in the upper-right corner of the **Protocols Analysis** panel and then click HTML or PDF to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.9 Viewing Traffic of Top Destination IP Addresses

The **Top Destination IP** panel displays in real time top 10 destination IP addresses with the largest traffic dropped by ADS in the last 30 seconds, letting users know which IP addresses see the largest traffic or are most severely attacked.

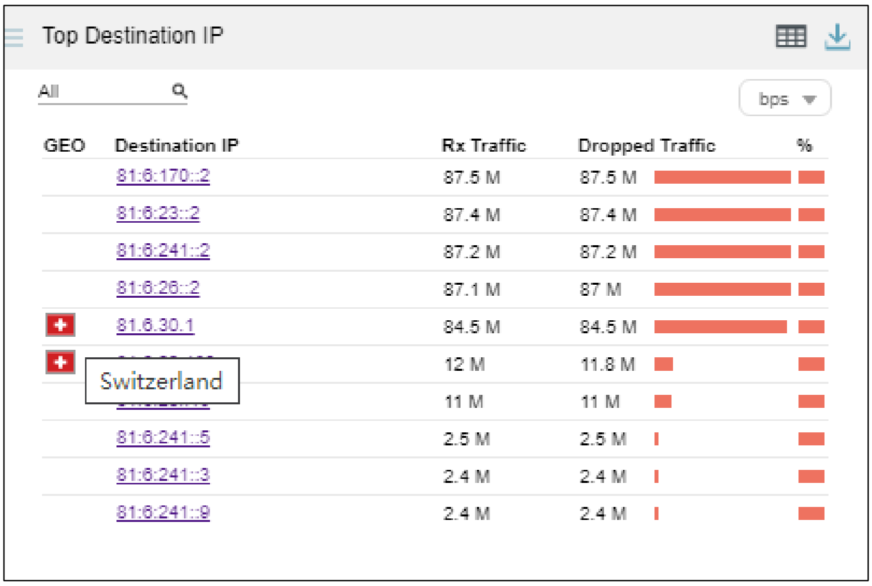
Data on this panel refreshes every 30 seconds.

4.1.9.1 Understanding Data on the Panel

The list ranks top 10 destination IP addresses according to traffic dropped by ADS in the last 30 seconds.

- **GEO**: shows the national flag icons. Pointing to a national flag displays the corresponding country name, as shown in Figure 4-20.

Figure 4-20 Display of the country name



Top Destination IP

All

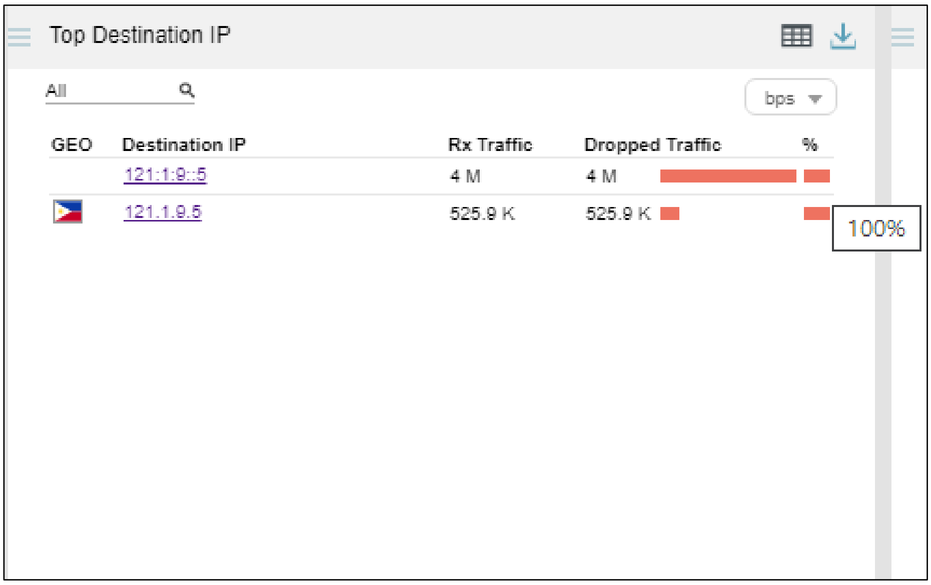
bps ▾

GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:170::2	87.5 M	87.5 M	
	81:6:23::2	87.4 M	87.4 M	
	81:6:241::2	87.2 M	87.2 M	
	81:6:26::2	87.1 M	87 M	
🇨🇭	81.6.30.1	84.5 M	84.5 M	
🇨🇭	[illegible]	12 M	11.8 M	
	[illegible]	11 M	11 M	
	81:6:241::5	2.5 M	2.5 M	
	81:6:241::3	2.4 M	2.4 M	
	81:6:241::9	2.4 M	2.4 M	

- **Destination IP**: shows destination IP addresses. Clicking an IP address opens the **Traffic Monitoring** tab page, where you can view more details about traffic destined for this IP address. For details, see section 4.1.9.2 Viewing Comprehensive Traffic Information of a Specified Object.
- **Rx Traffic**: shows the value of traffic received by ADS in the last 30 seconds.
- **Dropped Traffic**: shows the value of traffic dropped by ADS in the last 30 seconds. The red bar to the right of the traffic value indicates the volume of dropped traffic. A longer bar indicates more traffic dropped.

- **%**: shows the percentage of forwarded traffic and that of dropped traffic to incoming traffic. When you point to a bar in this column, the specific percentage is displayed. In a bar, green indicates legitimate traffic and red indicates dropped traffic. As shown in Figure 4-21, the percentage of dropped traffic for 121:1:9::5 is 100%.

Figure 4-21 Percentage of dropped traffic to incoming traffic



GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	121:1:9::5	4 M	4 M 🟥	🟥
	121.1.9.5	525.9 K	525.9 K 🟥	🟥

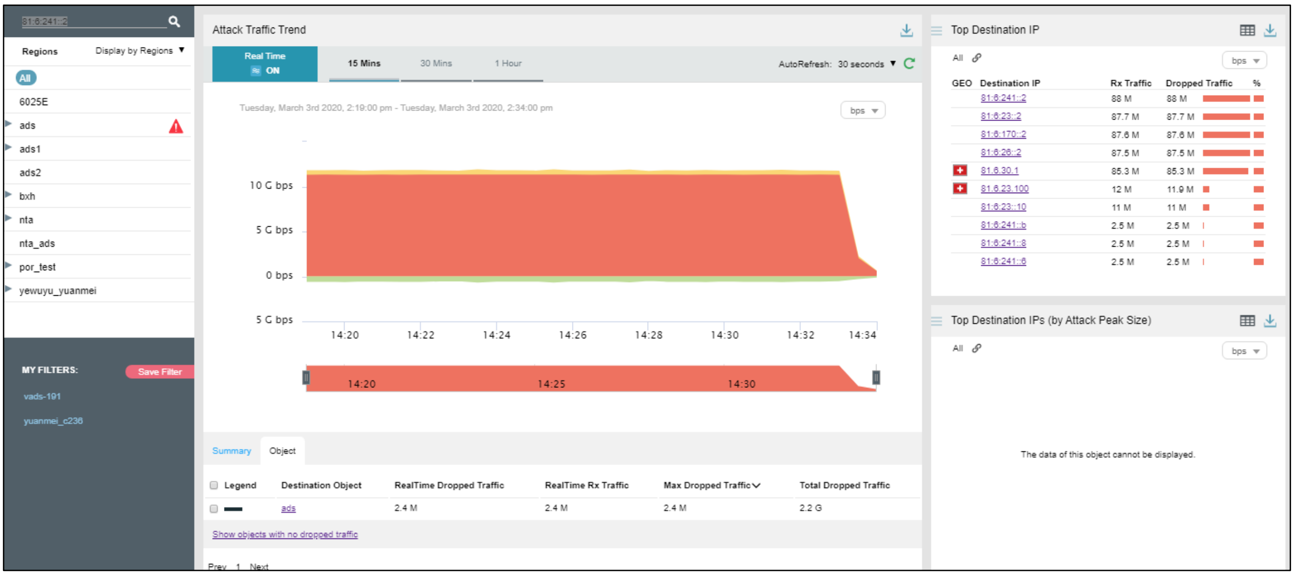
4.1.9.2 Viewing Comprehensive Traffic Information of a Specified Object

You can conveniently view comprehensive traffic information of a top 10 destination IP address and that of a specified object by performing the following steps:

Step 1 On the page shown in Figure 4-20, click an IP address, for example, **81:6:241::2**.

The **DDoS Traffic Monitoring** page is displayed, with the IP address in question already in the search box, as shown in Figure 4-22.

Figure 4-22 Traffic of a specific IP address



Tuesday, March 3rd 2020, 2:19:00 pm - Tuesday, March 3rd 2020, 2:34:00 pm

Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
▬	ads	2.4 M	2.4 M	2.4 M	2.2 G

Show objects with no dropped traffic

Top Destination IP

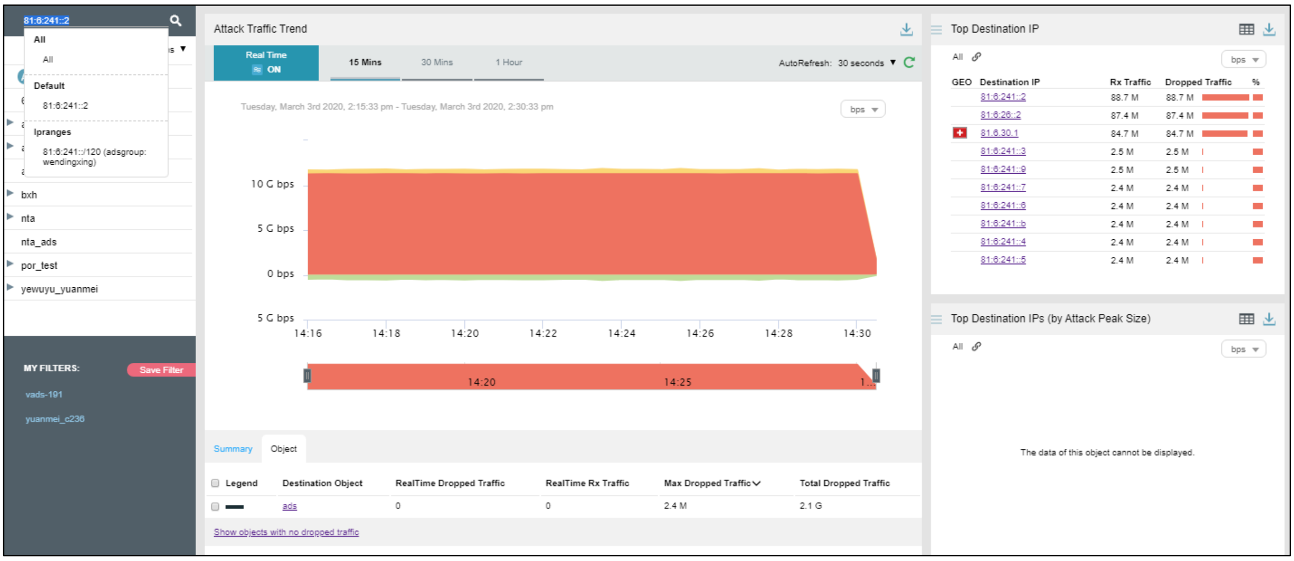
GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:241::2	88 M	88 M	
	81:6:23::2	87.7 M	87.7 M	
	81:6:170::2	87.6 M	87.6 M	
	81:6:26::2	87.5 M	87.5 M	
🇨🇭	81.6.30.1	85.3 M	85.3 M	
🇨🇭	81.6.23.100	12 M	11.9 M	
	81:6:23::10	11 M	11 M	
	81:6:241::b	2.5 M	2.5 M	
	81:6:241::8	2.5 M	2.5 M	
	81:6:241::6	2.5 M	2.5 M	

The data of this object cannot be displayed.

Step 2 Click in the search box.

The system displays all objects containing the current IP address, as shown in Figure 4-23.

Figure 4-23 Searching for objects containing the current IP address



Tuesday, March 3rd 2020, 2:15:33 pm - Tuesday, March 3rd 2020, 2:30:33 pm

Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
▬	ads	0	0	2.4 M	2.1 G

Show objects with no dropped traffic

Top Destination IP

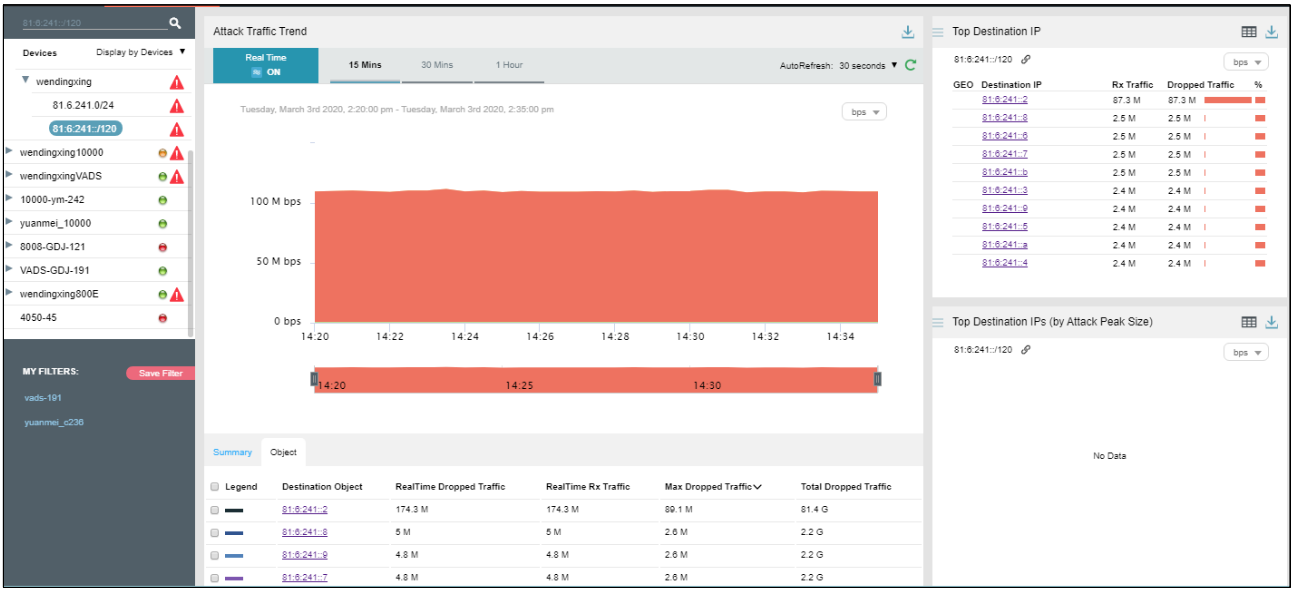
GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:241::2	88.7 M	88.7 M	
	81:6:26::2	87.4 M	87.4 M	
🇨🇭	81.6.30.1	84.7 M	84.7 M	
	81:6:241::3	2.5 M	2.5 M	
	81:6:241::9	2.5 M	2.5 M	
	81:6:241::7	2.4 M	2.4 M	
	81:6:241::6	2.4 M	2.4 M	
	81:6:241::b	2.4 M	2.4 M	
	81:6:241::4	2.4 M	2.4 M	
	81:6:241::5	2.4 M	2.4 M	

The data of this object cannot be displayed.

Step 3 Select an object and press **Enter**.

Comprehensive traffic information of the specified object is displayed, as shown in Figure 4-24.

Figure 4-24 Viewing traffic information of a specified object



Top Destination IP

81:6:241::/120

GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:241::2	87.3 M	87.3 M	
	81:6:241::8	2.5 M	2.5 M	
	81:6:241::6	2.5 M	2.5 M	
	81:6:241::7	2.5 M	2.5 M	
	81:6:241::b	2.5 M	2.5 M	
	81:6:241::3	2.4 M	2.4 M	
	81:6:241::9	2.4 M	2.4 M	
	81:6:241::5	2.4 M	2.4 M	
	81:6:241::a	2.4 M	2.4 M	
	81:6:241::4	2.4 M	2.4 M	

□ Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
□	81:6:241::2	174.3 M	174.3 M	89.1 M	81.4 G
□	81:6:241::8	5 M	5 M	2.6 M	2.2 G
□	81:6:241::9	4.8 M	4.8 M	2.6 M	2.2 G
□	81:6:241::7	4.8 M	4.8 M	2.6 M	2.2 G

----End

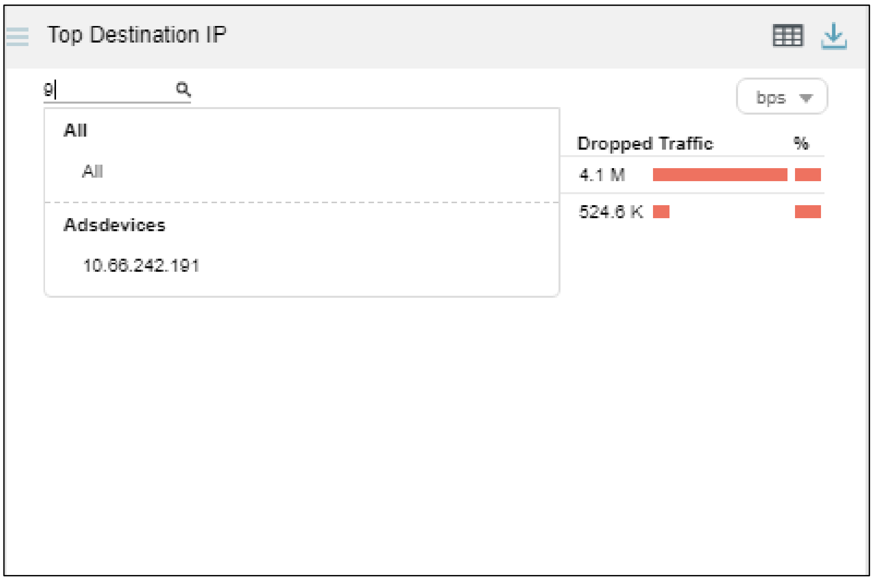
4.1.9.3 Viewing Top Destination IP Addresses of a Specified Object

By default, the **Top 10 Destination IP** panel presents top 10 destination IP addresses based on data collected from all ADS devices. You can specify a region, region IP group, ADS device, or ADS-protected group to view its top destination IP addresses ranked according to traffic dropped in the last 30 minutes. You can also specify a destination IPv4 or IPv6 address to view its traffic information in the last 30 minutes.

Step 1 On the page shown in Figure 4-24, type a character string and then press **Enter**.

The system automatically displays all objects containing the typed character string, as shown in Figure 4-25.

Figure 4-25 Searching for an object



Top Destination IP

g|

All

All

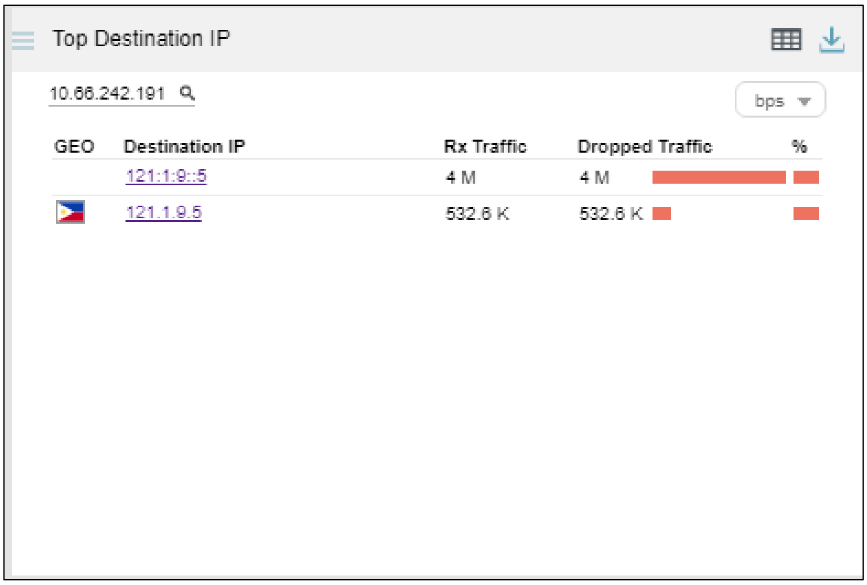
Adsdevices

10.66.242.191

Step 2 Select an object and press **Enter**.

Then destination IP addresses associated with the specified object are displayed, ranked in descending order of traffic dropped by ADS in the last 30 minutes.

Figure 4-26 Top destination IP addresses associated with a specified object



Top Destination IP

10.66.242.191

GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	121:1:9::5	4 M	4 M	
	121.1.9.5	532.6 K	532.6 K	

----End

4.1.9.4 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top Destination IP** panel to display traffic data in pps.

4.1.9.5 Downloading a Report

Click ⤓ in the upper-right corner of the **Top Destination IP** panel and then click HTML or PDF to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.10 Viewing Attack Traffic of Top Regions

The **Top Region Attack Traffic** panel presents in real time top 10 regions with the largest traffic dropped by ADS in the last 30 seconds, letting users know which regions see the largest traffic or are most severely attacked.

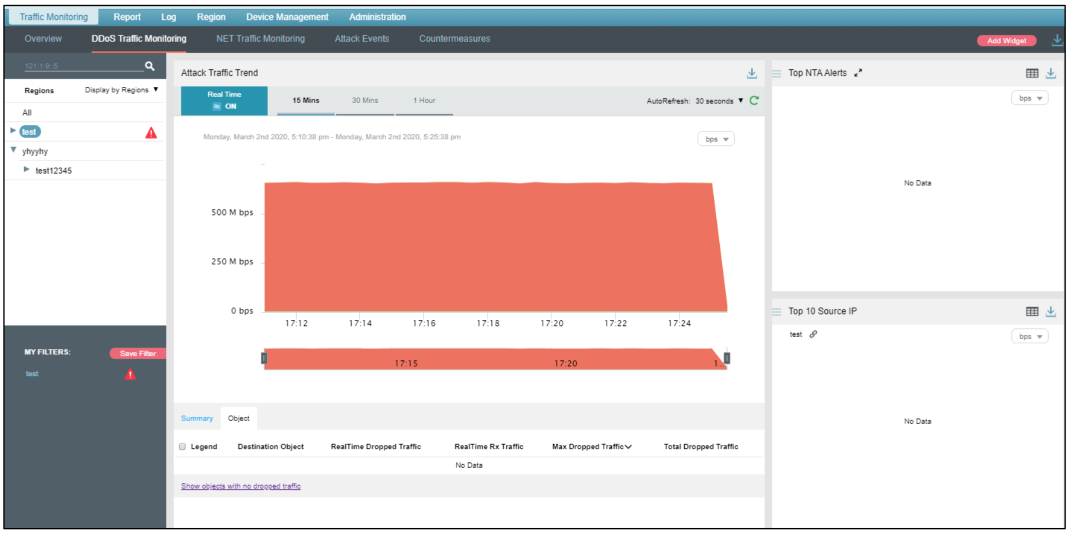
Data on this panel refreshes every 30 seconds.

4.1.10.1 Understanding Data on the Panel

The list ranks top 10 regions according to traffic dropped by ADS in the last 30 seconds.

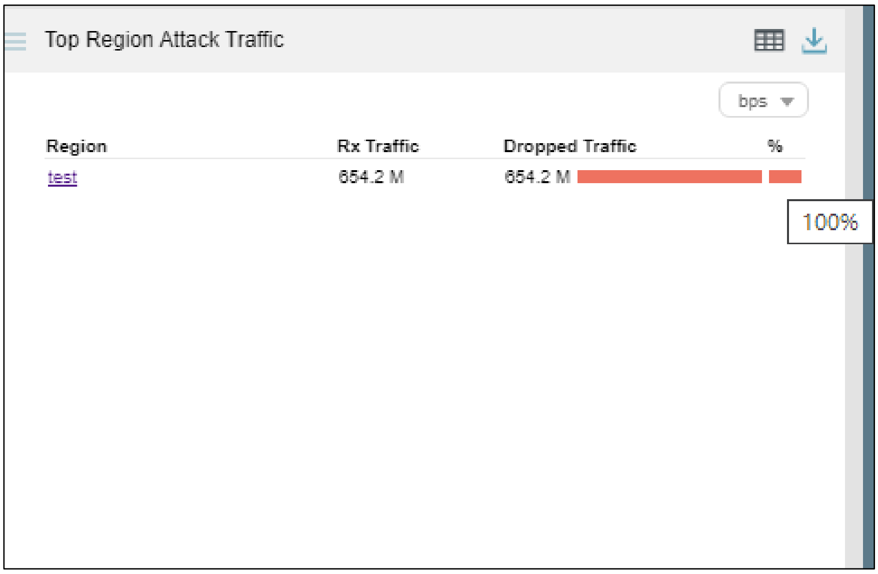
- **Region**: region for which traffic is dropped by ADS. Clicking a region name, for example, **test**, opens the **DDoS Traffic Monitoring** tab page, where you can view more details about traffic destined for this region, as shown in Figure 4-27.

Figure 4-27 Traffic of a specific region



- **Rx Traffic**: shows the value of traffic received by ADS in the last 30 seconds.
- **Dropped Traffic**: shows the value of traffic dropped by ADS in the last 30 seconds. The red bar to the right of the traffic value indicates the volume of dropped traffic. A longer bar indicates more traffic dropped.
- **%**: shows the percentage of forwarded traffic and that of dropped traffic to incoming traffic. When you point to a bar in this column, the specific percentage is displayed. In a bar, green indicates legitimate traffic and red indicates dropped traffic. As shown in Figure 4-28, the percentage of dropped traffic for "test" is 100%.

Figure 4-28 Percentage of dropped traffic for a specific region



Top Region Attack Traffic

bps ▼

Region	Rx Traffic	Dropped Traffic	%
test	654.2 M	654.2 M	🟥

100%

4.1.10.2 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top Region Traffic** panel to display traffic data in pps.

4.1.10.3 Downloading a Report

Click ⤓ in the upper-right corner of the **Top Region Traffic** panel and then click HTML or PDF to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.11 Viewing Attack Traffic Trend (Peak Size)

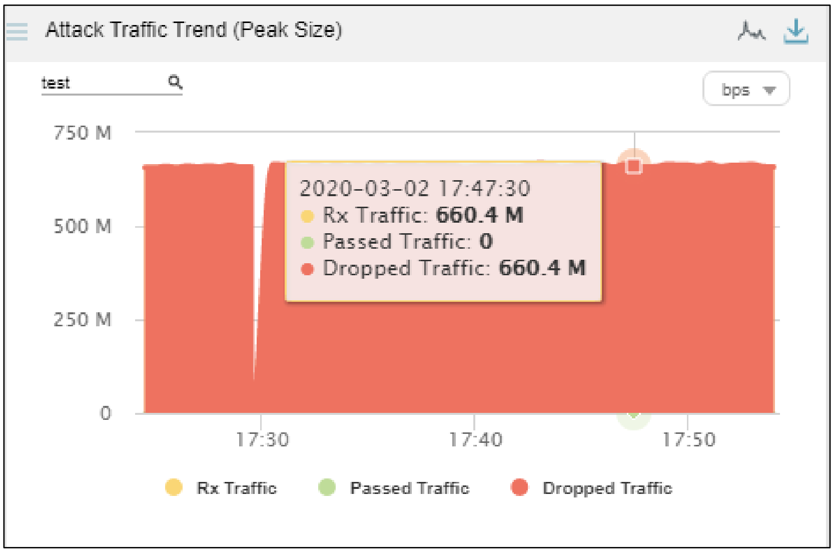
The **Attack Traffic Trend (Peak Size)** panel displays traffic trends of a specific IP address or region in the last 30 minutes, including the received, passed, and dropped traffic, as shown in Figure 4-29.

Note	This panel provides traffic information of only a specific IP address or region. You cannot view global traffic information or traffic information of a specified device.

Data on this panel refreshes every 30 seconds.

The method of viewing attack traffic trends (peak size) is the same as that of viewing attack traffic trends. For details, see section 4.1.7 Viewing Attack Traffic Trends.

Figure 4-29 Attack Traffic Trend (Peak Size) panel



4.1.12 Viewing Top Destination IPs (by Attack Peak Size)

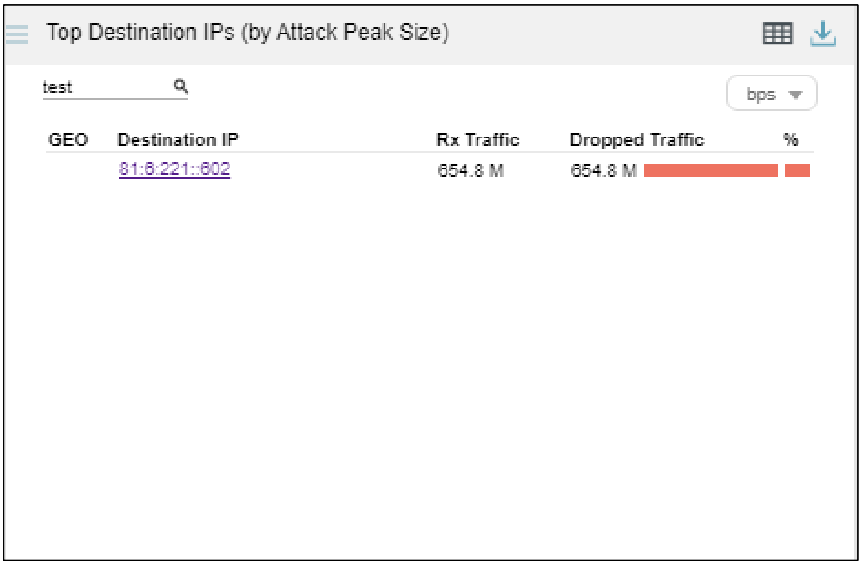
The **Top Destination IPs (by Attack Peak Size)** panel displays top 10 destination IP addresses of an object with the most traffic dropped in the last 30 seconds, as shown in Figure 4-30, letting users know which IP addresses of the object receive the most traffic or are most severely attacked.

Note	This panel provides traffic information of only a specific IP address or region. You cannot view global traffic information or traffic information of a specified device.

Data on this panel refreshes every 30 seconds.

The method of viewing top destination IP addresses (by attack peak size) is the same as that of viewing top destination IP addresses. For details, see section 4.1.9 Viewing Traffic of Top Destination IP Addresses.

Figure 4-30 Top Destination IPs (by Attack Peak Size) panel



Top Destination IPs (by Attack Peak Size)

test

bps

GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:221::602	654.8 M	654.8 M 🟥	🟥

4.1.13 Viewing Traffic of Top Source Countries/Regions

The **Top Source Countries** panel presents in real time top 10 source countries/regions with the largest attack traffic dropped by ADS in the last 30 seconds.

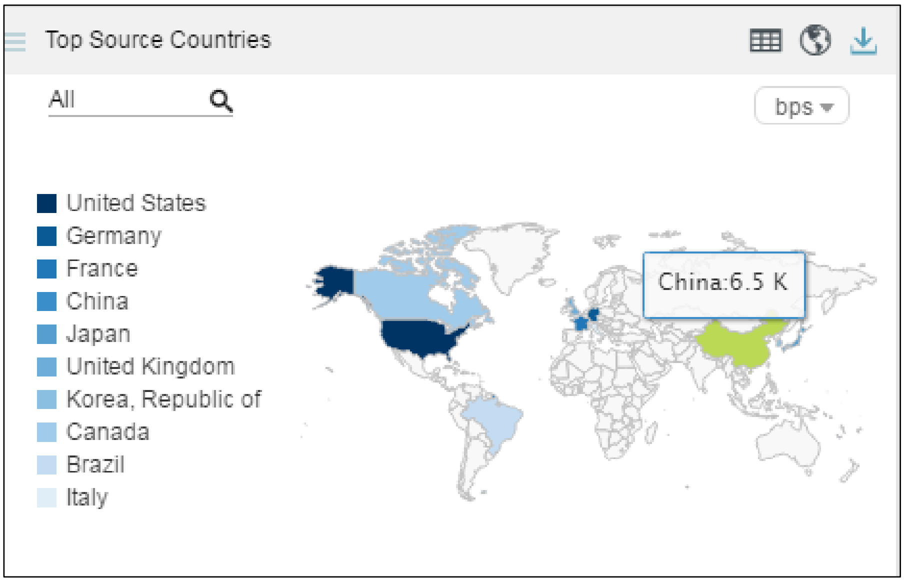
Data on this panel refreshes every 30 seconds.

4.1.13.1 Understanding Data Displayed in a Map

Top 10 source countries/regions are ranked on the left according to attack traffic handled by ADS, indicated with a color that shades from dark blue to very light blue. On the right, areas of these countries/regions are indicated in a map with the same colors.

Pointing to the area of a top 10 country/region changes its color to green and displays the country/region name and the volume of traffic dropped by ADS, as shown in Figure 4-31.

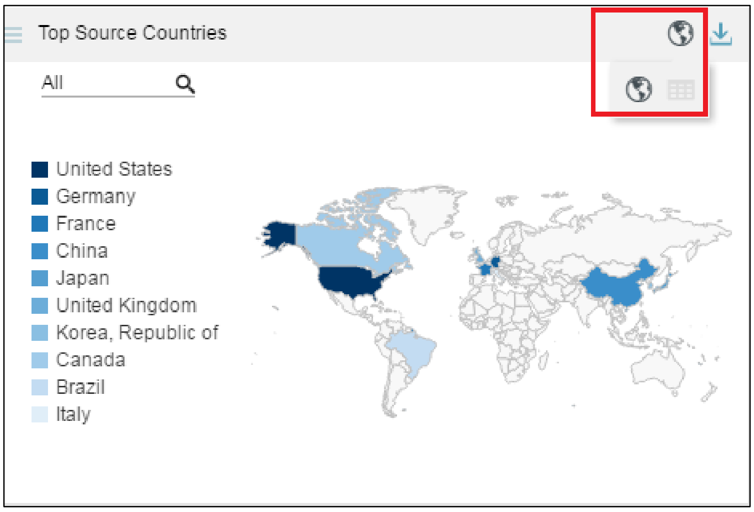
Figure 4-31 Display of the volume of attack traffic from a country



4.1.13.2 Switching the Display Mode

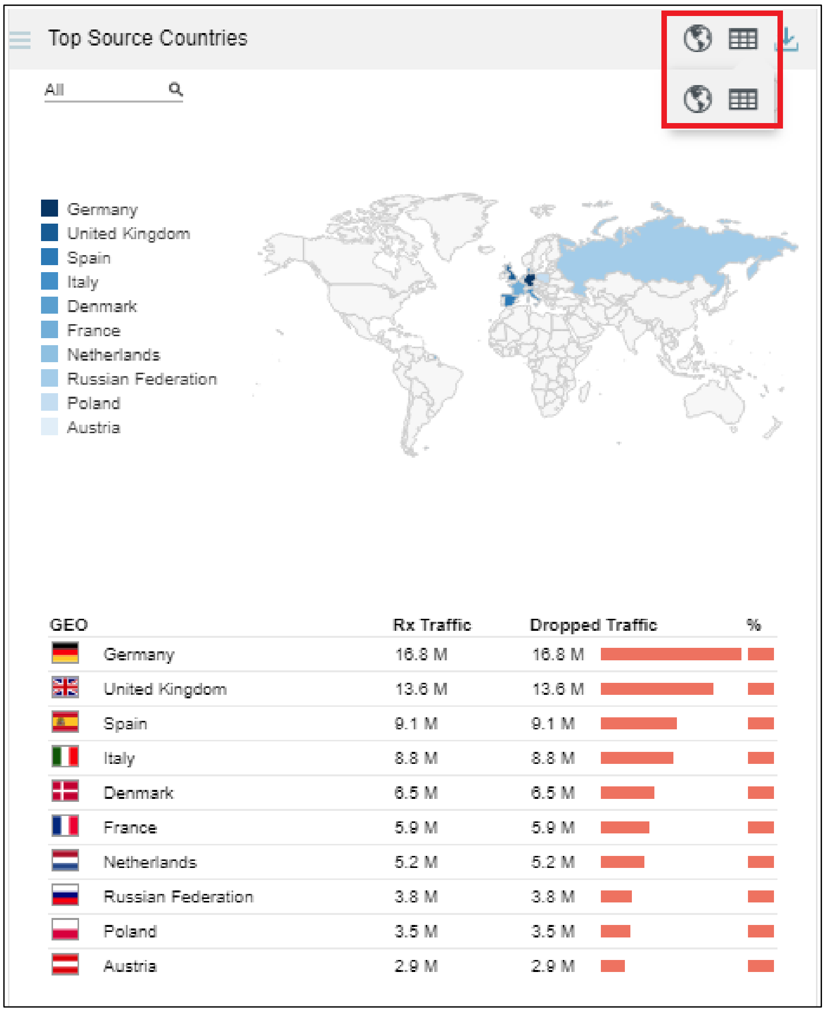
By default, traffic of top 10 source countries is presented in a map of the world. You can click 🌐 in the upper-right corner of the **Top Source Countries** panel to choose a display mode (list or map) or both modes, as shown in Figure 4-32.

Figure 4-32 Switching the display mode



In Figure 4-32, 🌐 appears normal, while ▦ appears dimmed. Therefore, data is presented only in a map. After you click ▦, this icon turns ▦. In this case, traffic data is presented in both a map and a list, as shown in Figure 4-33.

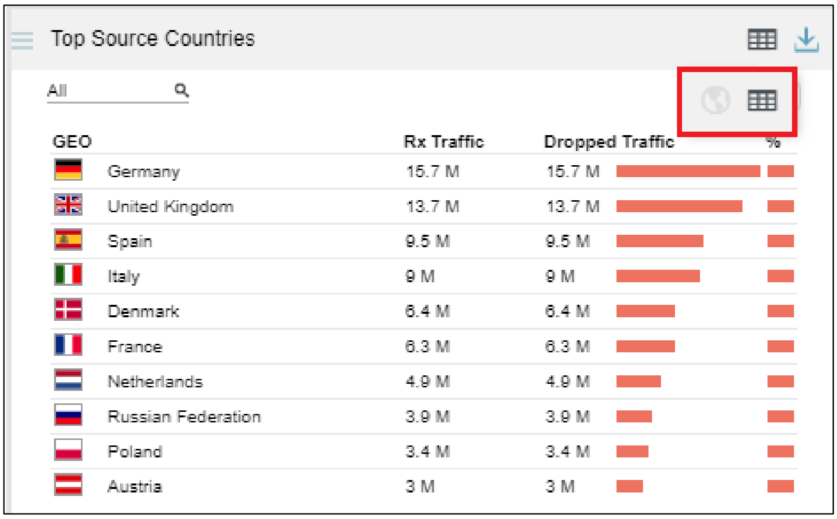
Figure 4-33 Display of traffic data in both a map and a list



GEO	Rx Traffic	Dropped Traffic	%
Germany	16.8 M	16.8 M	
United Kingdom	13.6 M	13.6 M	
Spain	9.1 M	9.1 M	
Italy	8.8 M	8.8 M	
Denmark	6.5 M	6.5 M	
France	5.9 M	5.9 M	
Netherlands	5.2 M	5.2 M	
Russian Federation	3.8 M	3.8 M	
Poland	3.5 M	3.5 M	
Austria	2.9 M	2.9 M	

Clicking 🌐 makes this icon dimmed and hides the map, as shown in Figure 4-34.

Figure 4-34 Display of traffic data only in a list



Top Source Countries

All

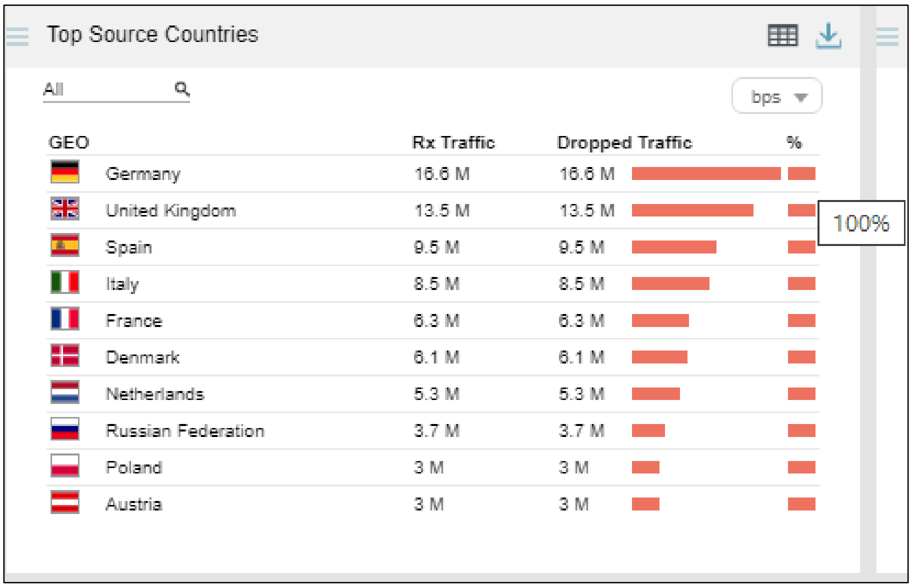
GEO	Rx Traffic	Dropped Traffic	%
Germany	15.7 M	15.7 M	🟥
United Kingdom	13.7 M	13.7 M	🟥
Spain	9.5 M	9.5 M	🟥
Italy	9 M	9 M	🟥
Denmark	6.4 M	6.4 M	🟥
France	6.3 M	6.3 M	🟥
Netherlands	4.9 M	4.9 M	🟥
Russian Federation	3.9 M	3.9 M	🟥
Poland	3.4 M	3.4 M	🟥
Austria	3 M	3 M	🟥

4.1.13.3 Viewing the List of Top Source Countries

The list ranks top 10 countries according to traffic dropped by ADS in the last 30 seconds.

- **GEO**: shows national flag icons. Pointing to an icon displays the country name, as shown in Figure 4-20.
- **Rx Traffic**: shows the traffic received by ADS from a country in the last 30 seconds.
- **Dropped Traffic**: shows the traffic dropped by ADS for the country in the last 30 seconds. The red bar to the right of the traffic value also indicates the dropped traffic. A longer bar indicates more traffic dropped.
- **%**: shows the percentage of forwarded traffic and that of dropped traffic to incoming traffic. Pointing to a bar in this column displays a specific percentage. In a bar, green indicates legitimate traffic and red indicates dropped traffic. As shown in Figure 4-35, the percentage of dropped traffic for Germany is 100%.

Figure 4-35 Percentage of dropped traffic of a source country



Top Source Countries

All

bps

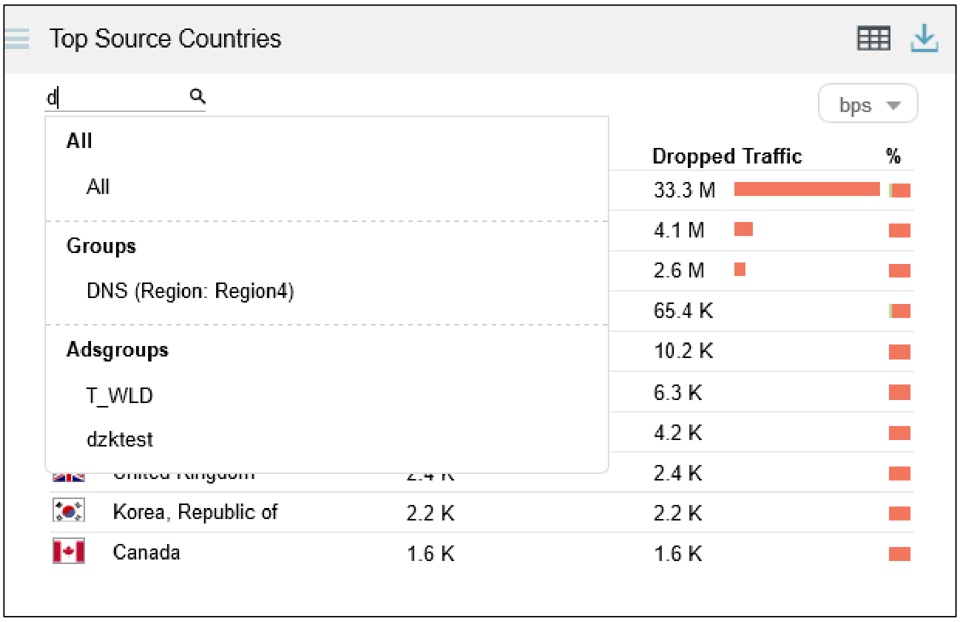
GEO	Rx Traffic	Dropped Traffic	%
Germany	16.6 M	16.6 M	
United Kingdom	13.5 M	13.5 M	100%
Spain	9.5 M	9.5 M	
Italy	8.5 M	8.5 M	
France	6.3 M	6.3 M	
Denmark	6.1 M	6.1 M	
Netherlands	5.3 M	5.3 M	
Russian Federation	3.7 M	3.7 M	
Poland	3 M	3 M	
Austria	3 M	3 M	

4.1.13.4 Viewing Top Source Countries Associated with a Specified Object

By default, the **Top Source Countries** panel presents top 10 source countries based on data collected from all ADS devices. You can specify a region, region IP group, ADS device or ADS-protected group, or IPv4 or IPv6 address to view its top 10 source countries ranked according to traffic dropped by all ADS devices in the last 30 seconds.

On the page shown in Figure 4-36, after you type a character string, the system displays all objects containing the typed character string.

Figure 4-36 Searching for a specific object



Top Source Countries

d

bps

All

All

Groups

DNS (Region: Region4)

Adsgroups

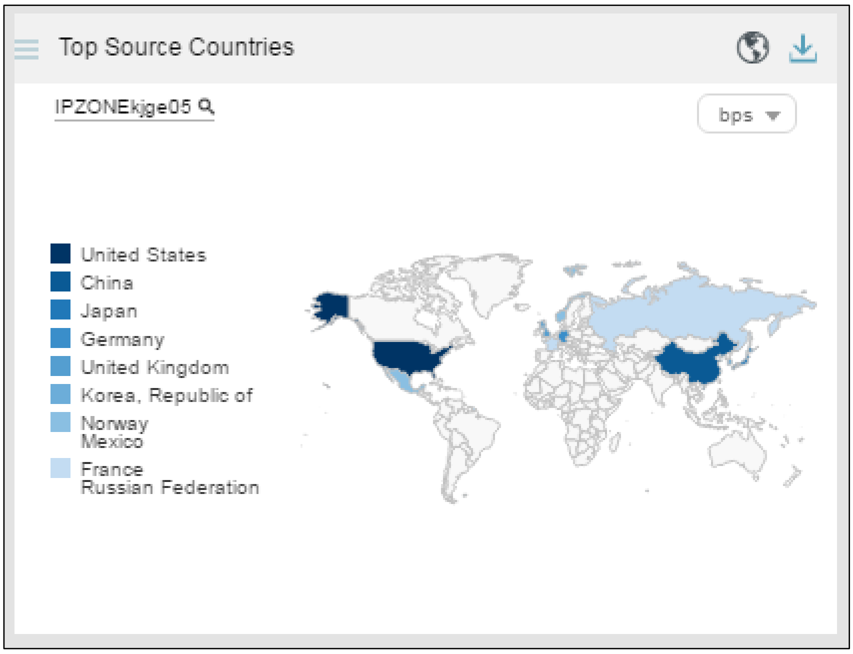
T_WLD

dzktest

		Dropped Traffic	%
		33.3 M	
		4.1 M	
		2.6 M	
		65.4 K	
		10.2 K	
		6.3 K	
		4.2 K	
United Kingdom	2.4 K	2.4 K	
Korea, Republic of	2.2 K	2.2 K	
Canada	1.6 K	1.6 K	

After you click a desired object, the panel displays the traffic of top source countries associated with the object.

Figure 4-37 Traffic of top source countries associated with a specific object



4.1.13.5 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top Source Countries** panel to display traffic data in pps.

4.1.13.6 Downloading a Report

Click ⤓ in the upper-right corner of the **Top Source Countries** panel and then click HTML or PDF to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.14 Viewing Attack Traffic

The **Attack Traffic** panel shows the graph of attack traffic detected by ADS devices in the last 30 minutes. Data on this panel refreshes every 30 seconds.

4.1.14.1 Understanding Data on the Panel

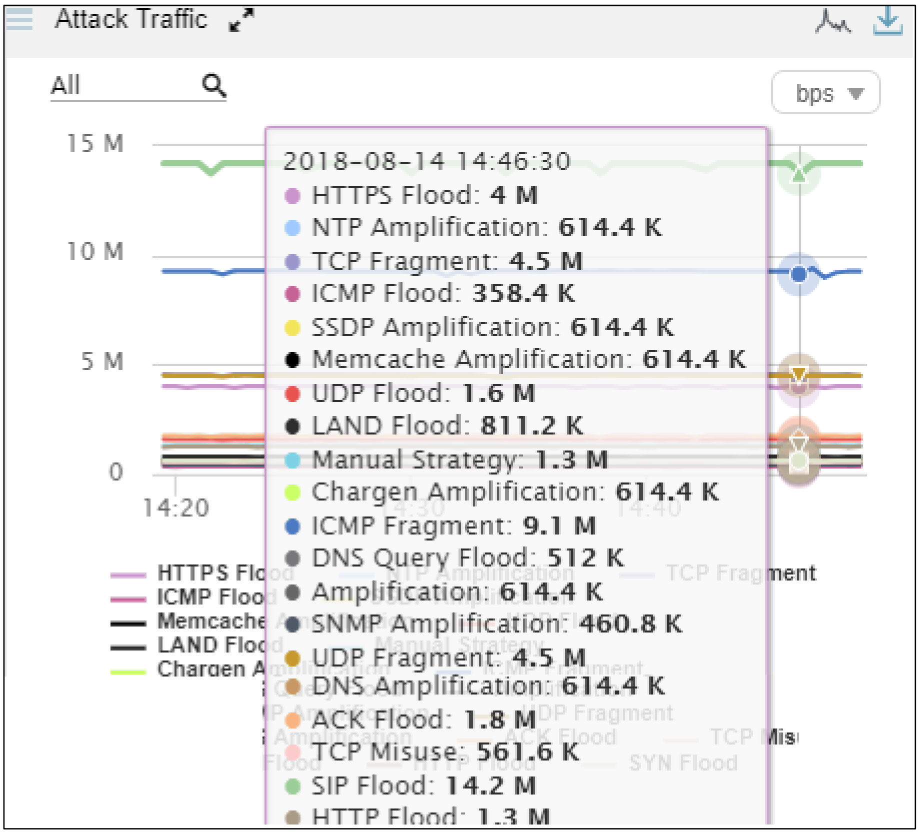
In the **Attack Traffic** graph,

- The x-axis indicates time, spanning 30 minutes.
- The y-axis indicates attack traffic. Various types of attack traffic are indicated by curves in different colors.

4.1.14.2 Viewing Traffic at a Specific Point of Time

Pointing to a specific time point displays the traffic of each attack type at this specific time point.

Figure 4-38 Traffic at a specific point of time



Attack Traffic

All

bps

2018-08-14 14:46:30
- HTTPS Flood: **4 M**
- NTP Amplification: **614.4 K**
- TCP Fragment: **4.5 M**
- ICMP Flood: **358.4 K**
- SSDP Amplification: **614.4 K**
- Memcache Amplification: **614.4 K**
- UDP Flood: **1.6 M**
- LAND Flood: **811.2 K**
- Manual Strategy: **1.3 M**
- Chargen Amplification: **614.4 K**
- ICMP Fragment: **9.1 M**
- DNS Query Flood: **512 K**
- Amplification: **614.4 K**
- SNMP Amplification: **460.8 K**
- UDP Fragment: **4.5 M**
- DNS Amplification: **614.4 K**
- ACK Flood: **1.8 M**
- TCP Misuse: **561.6 K**
- SIP Flood: **14.2 M**
- HTTP Flood: **1.3 M**

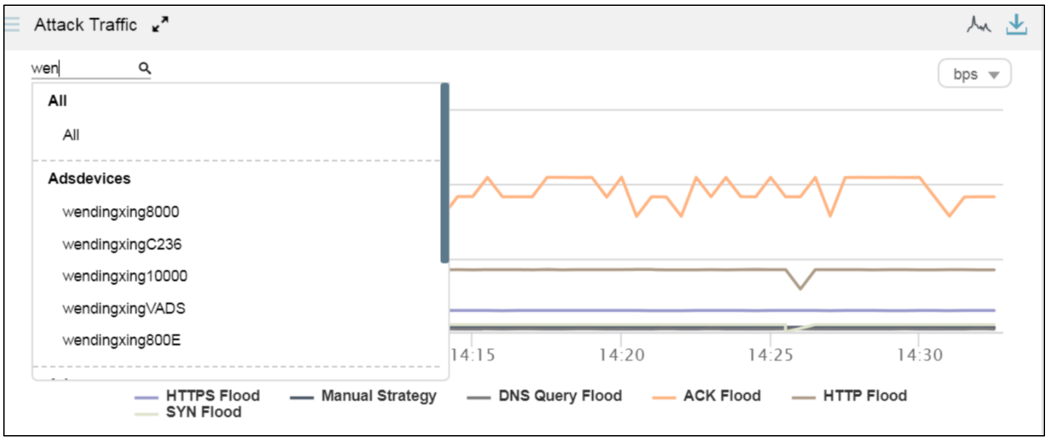
4.1.14.3 Viewing Attack Traffic of a Specified Object

By default, the **Attack Traffic** graph presents attack traffic trends detected by all ADS devices. You can specify a region, region IP group, ADS device, ADS-protected group, or IPv4 or IPv6 address to view its attack traffic trend in the last 30 minutes.

Step 1 On the page shown in Figure 4-38, type a character string.

The system displays all objects containing the typed character string.

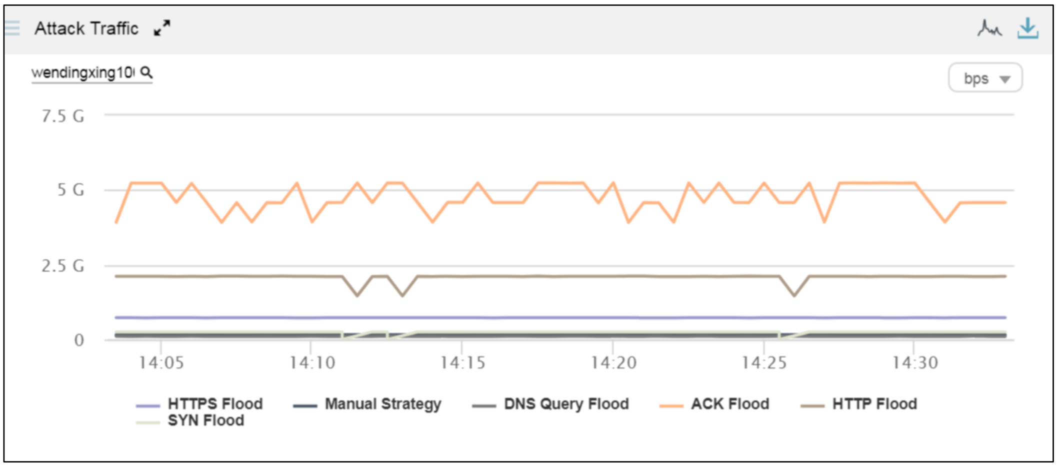
Figure 4-39 Searching for an object



Step 2 Click a desired object.

The panel displays the attack traffic trend of the object in the last 30 minutes.

Figure 4-40 Attack traffic trend of a specified object



----End

4.1.14.4 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Attack Traffic** panel to display traffic data in pps.

4.1.14.5 Downloading a Report

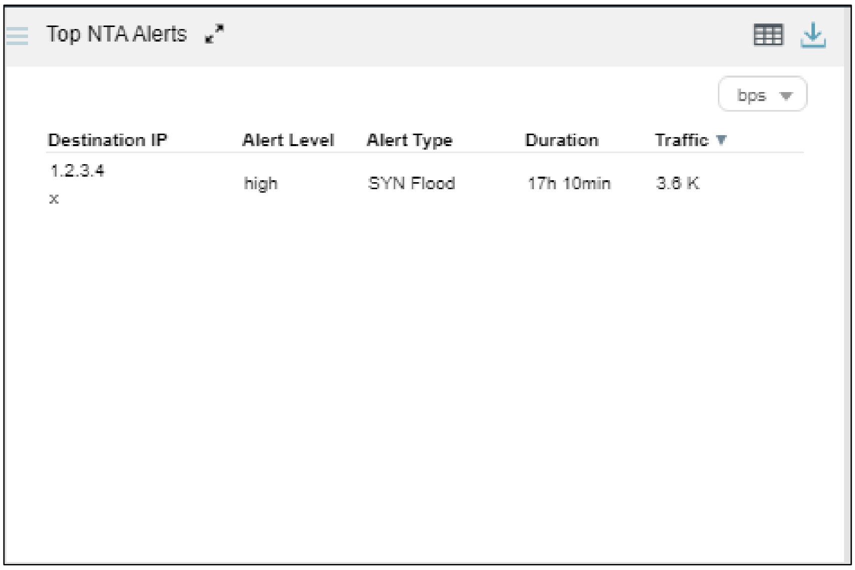
Click ⤓ in the upper-right corner of the **Attack Traffic** panel and then click HTML or PDF to export data of this panel an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.15 Viewing Top Alerts Reported by NTA

The **Top NTA Alerts** panel shows top 5 traffic alerts reported by NTA devices in real time.

Data on this panel refreshes every 30 seconds.

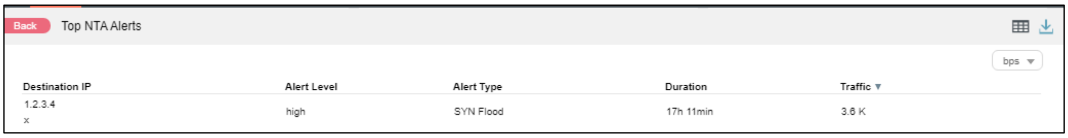
Figure 4-41 Top alerts reported by NTA



Destination IP	Alert Level	Alert Type	Duration	Traffic ▼
1.2.3.4 x	high	SYN Flood	17h 10min	3.6 K

Clicking ⤢ displays more details about these alerts, as shown in Figure 4-42.

Figure 4-42 More details about alerts generated by NTA



Destination IP	Alert Level	Alert Type	Duration	Traffic ▼
1.2.3.4 x	high	SYN Flood	17h 11min	3.6 K

4.1.15.1 Understanding Data on the Panel

The **Top NTA Alerts** panel shows top 5 alerts reported by NTA. The alert table contains the following information:

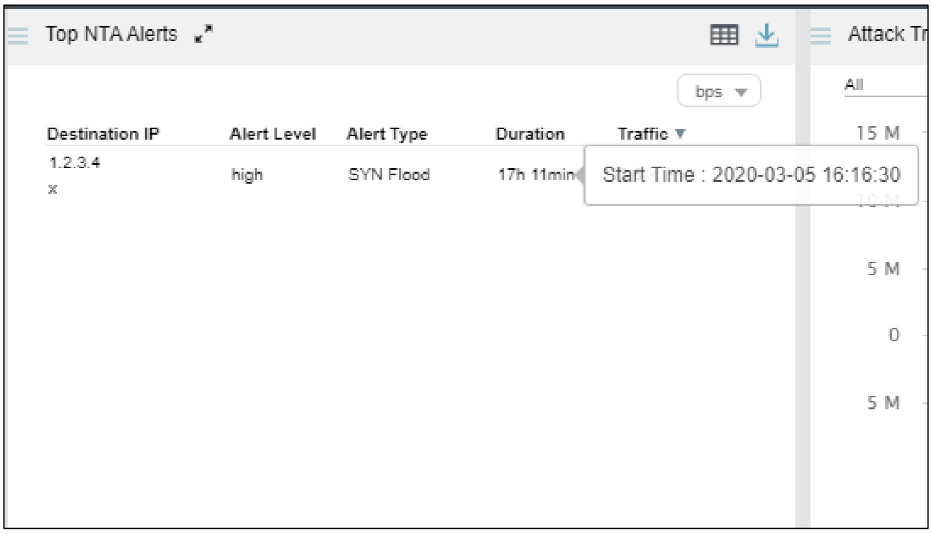
- **Destination IP**: shows the attacked destination IP address and the name of the NTA device that reports this alert.
- **Alert Level**: shows the alert level, which can be **high**, **mid**, or **low**. The alert level is determined by the deviation of the actual traffic value from the specified threshold. As thresholds vary with NTA devices, alert levels of these devices are determined by different deviations.
- **Alert Type**: shows the alert type, which can be one of the following:
  - **DDoS attack**: indicates that the alert is triggered when NTA detects a DDoS attack. The type of the DDoS attack is also displayed, for example, **SYN Flood**.
  - **Region traffic alert:** indicates that the alert is triggered by abnormal incoming or outgoing region traffic.

- **IP group traffic alert**: indicates that the alert is triggered by abnormal traffic received or sent by an IP group.

Note	For details about alert levels and alert types of NTA, see the corresponding description in the *NSFOCUS NTA User Guide*.

- **Duration**: shows the duration of the alert from the start time to current time. Pointing to a specific duration displays the start time of the attack against the destination IP address, as shown in Figure 4-43.

Figure 4-43 Start time of an alert reported by NTA

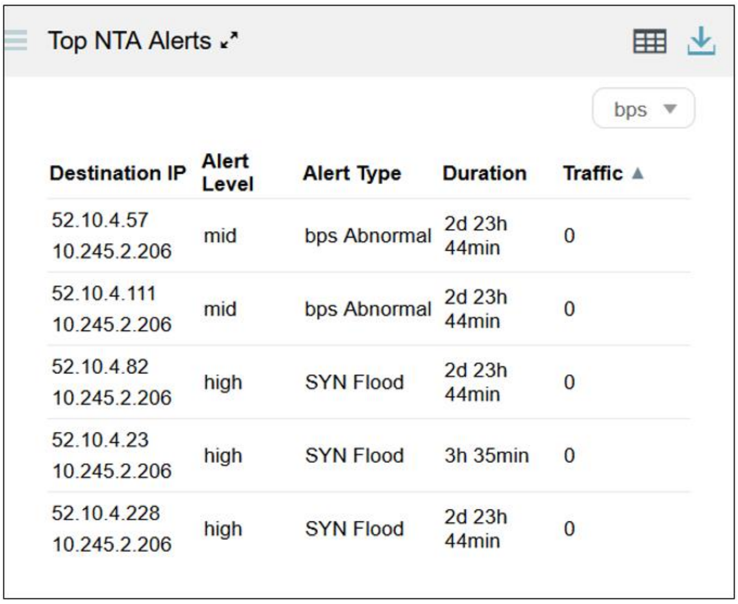


Destination IP	Alert Level	Alert Type	Duration	Traffic ▼
1.2.3.4 x	high	SYN Flood	17h 11min	

Start Time : 2020-03-05 16:16:30

- **Traffic**: shows the traffic at the start time of the alert. By default, top alerts are ranked in descending order of largest traffic detected by ADS devices in the last 30 seconds. In this case, after you click **Traffic**, the ▲ icon is displayed and the top alerts are ranked in ascending order of smallest traffic detected by ADS devices in the last 30 seconds.

Figure 4-44 Top alerts reported by NTA in terms of smallest traffic



Destination IP	Alert Level	Alert Type	Duration	Traffic ▲
52.10.4.57 10.245.2.206	mid	bps Abnormal	2d 23h 44min	0
52.10.4.111 10.245.2.206	mid	bps Abnormal	2d 23h 44min	0
52.10.4.82 10.245.2.206	high	SYN Flood	2d 23h 44min	0
52.10.4.23 10.245.2.206	high	SYN Flood	3h 35min	0
52.10.4.228 10.245.2.206	high	SYN Flood	2d 23h 44min	0

4.1.15.2 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top NTA Alerts** panel to display traffic data in pps.

4.1.15.3 Downloading a Report

Click ⤓ in the upper-right corner of the **Top NTA Alerts** panel and then click HTML or PDF to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.16 Viewing Top Ongoing Attack Events

The **Top Ongoing Attack Events** panel shows top 10 ongoing attack events ranked according to attack traffic detected by all ADS devices in the last 30 seconds.

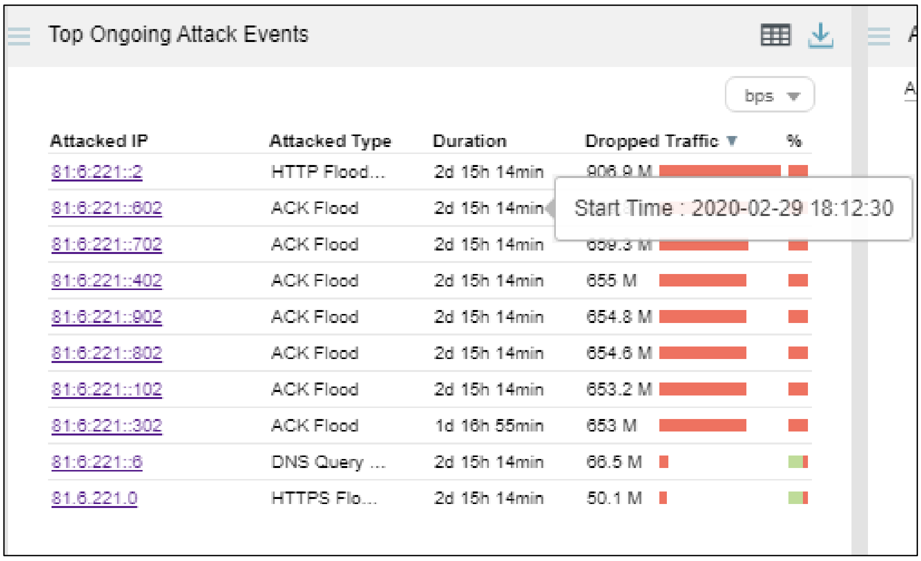
Data on this panel refreshes every 30 seconds.

4.1.16.1 Understanding Data on the Panel

The **Top Ongoing Attack Events** panel shows top 10 ongoing attack events according to traffic dropped by ADS in the last 30 seconds. By default, these events are listed in descending order of dropped traffic.

- **Attacked IP**: shows the attacked IP address. Clicking an IP address, you can view its detailed attack event information on an individual page. For details, see section 4.1.16.2 Viewing Attack Events Specific to an IP Address.
- **Attack Type**: shows the specific attack type.
- **Duration**: shows the duration from the time when an alert is triggered to the time when the data is refreshed. Pointing to a duration displays the attack start time of the IP address, as shown in Figure 4-45.

Figure 4-45 Start time of an ongoing attack event


Top Ongoing Attack Events

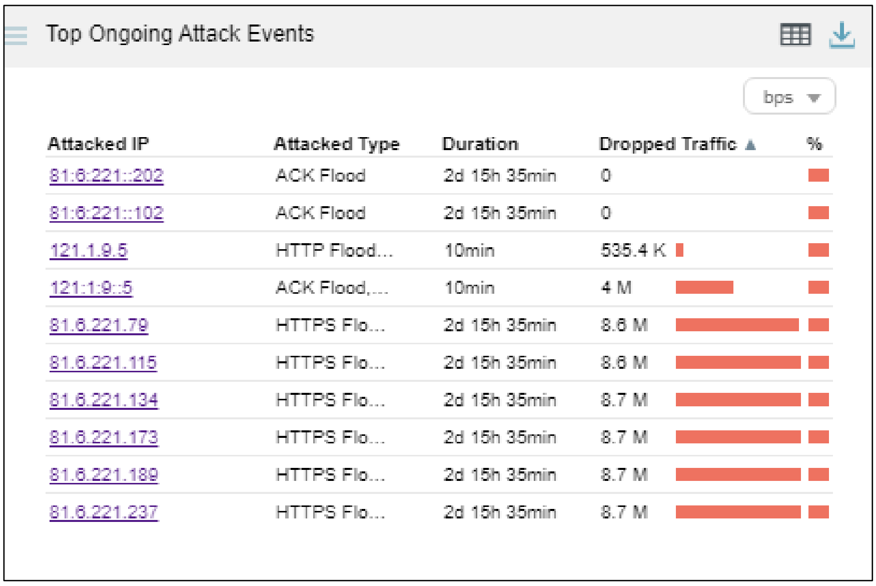
bps

Attacked IP	Attacked Type	Duration	Dropped Traffic ▼	%
81:6:221::2	HTTP Flood...	2d 15h 14min	906.9 M	🟥
81:6:221::602	ACK Flood	2d 15h 14min		
81:6:221::702	ACK Flood	2d 15h 14min	659.3 M	🟥
81:6:221::402	ACK Flood	2d 15h 14min	655 M	🟥
81:6:221::902	ACK Flood	2d 15h 14min	654.8 M	🟥
81:6:221::802	ACK Flood	2d 15h 14min	654.6 M	🟥
81:6:221::102	ACK Flood	2d 15h 14min	653.2 M	🟥
81:6:221::302	ACK Flood	1d 16h 55min	653 M	🟥
81:6:221::6	DNS Query ...	2d 15h 14min	66.5 M	🟩🟥
81.6.221.0	HTTPS Flo...	2d 15h 14min	50.1 M	🟩🟥

Start Time : 2020-02-29 18:12:30

- **Dropped Traffic**: By default, top 10 ongoing attack events are listed in descending order of traffic dropped by ADS. In this case, the ▼ icon is displayed to the right of **Dropped Traffic** and this column shows the total maximum traffic dropped by all ADS devices in the last 30 seconds. The red bar also indicates the total value. After you click **Dropped Traffic**, the ▲ icon is displayed and this column shows the total minimum traffic dropped by all ADS devices in the last 30 seconds.

Figure 4-46 Top ongoing attack events by total minimum dropped traffic

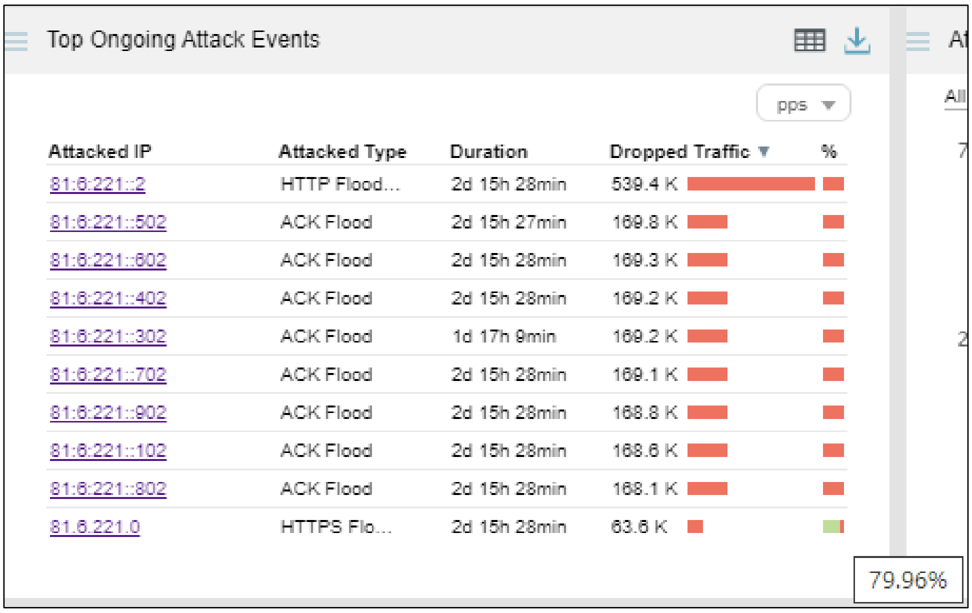

Top Ongoing Attack Events

bps

Attacked IP	Attacked Type	Duration	Dropped Traffic ▲	%
81:6:221::202	ACK Flood	2d 15h 35min	0	🟥
81:6:221::102	ACK Flood	2d 15h 35min	0	🟥
121.1.9.5	HTTP Flood...	10min	535.4 K	🟥
121:1:9::5	ACK Flood,...	10min	4 M	🟥
81.6.221.79	HTTPS Flo...	2d 15h 35min	8.6 M	🟥
81.6.221.115	HTTPS Flo...	2d 15h 35min	8.6 M	🟥
81.6.221.134	HTTPS Flo...	2d 15h 35min	8.7 M	🟥
81.6.221.173	HTTPS Flo...	2d 15h 35min	8.7 M	🟥
81.6.221.189	HTTPS Flo...	2d 15h 35min	8.7 M	🟥
81.6.221.237	HTTPS Flo...	2d 15h 35min	8.7 M	🟥

- **%**: shows the percentage of forwarded traffic and that of dropped traffic to incoming traffic. Pointing to a bar in this column displays the specific percentage. In a bar, green indicates legitimate traffic and red indicates dropped traffic. As shown in Figure 4-47, the percentage of dropped traffic for 81.6.221.0 is 79.96%.

Figure 4-47 Percentage of forwarded traffic in an ongoing attack event



Top Ongoing Attack Events

Attacked IP	Attacked Type	Duration	Dropped Traffic ▼	%
81:6:221::2	HTTP Flood...	2d 15h 28min	539.4 K	
81:6:221::502	ACK Flood	2d 15h 27min	169.8 K	
81:6:221::602	ACK Flood	2d 15h 28min	169.3 K	
81:6:221::402	ACK Flood	2d 15h 28min	169.2 K	
81:6:221::302	ACK Flood	1d 17h 9min	169.2 K	
81:6:221::702	ACK Flood	2d 15h 28min	169.1 K	
81:6:221::902	ACK Flood	2d 15h 28min	168.8 K	
81:6:221::102	ACK Flood	2d 15h 28min	168.6 K	
81:6:221::802	ACK Flood	2d 15h 28min	168.1 K	
81.6.221.0	HTTPS Flo...	2d 15h 28min	63.6 K	

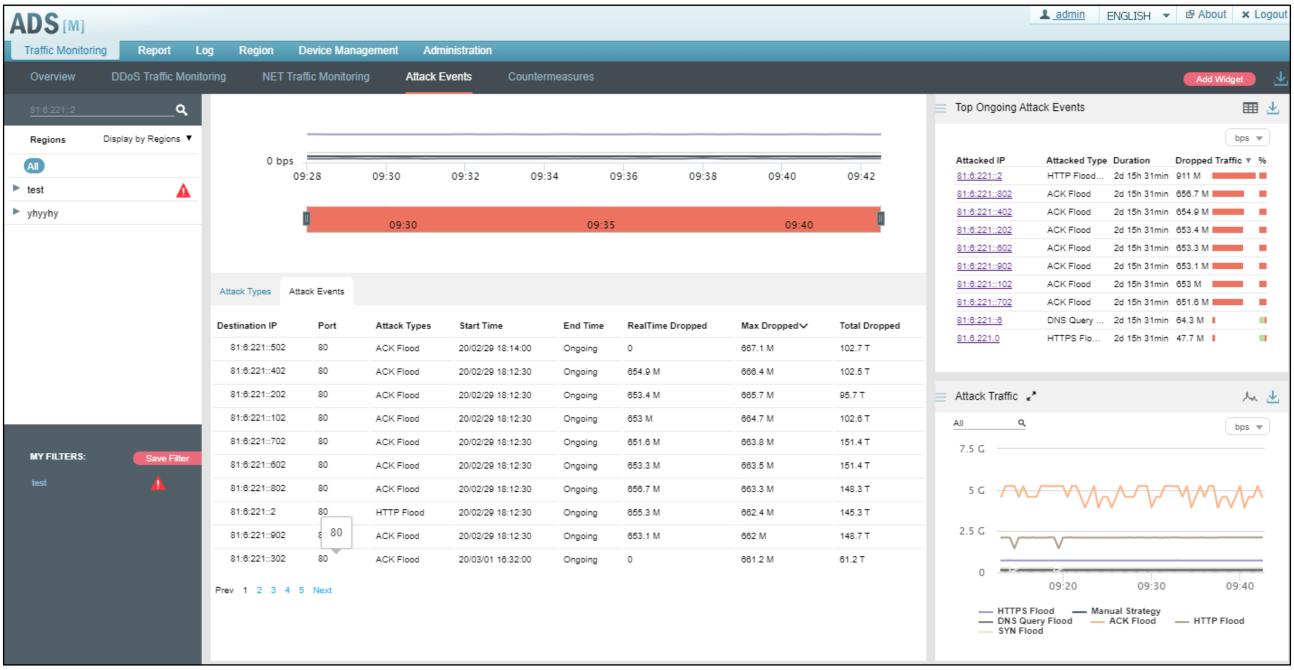
4.1.16.2 Viewing Attack Events Specific to an IP Address

You can conveniently view traffic of an IP address listed in the **Top Ongoing Attack Events** panel by performing the following steps:

Step 1 On the page shown in Figure 4-47, click an IP address, for example, **81:6:221::2**.

The **Attack Events** page is displayed, with the IP address in question already in the search box in the left, as shown in Figure 4-48.

Figure 4-48 Attack traffic targeting an IP address



Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:221::502	80	ACK Flood	20/02/29 18:14:00	Ongoing	0	667.1 M	102.7 T
81:6:221::402	80	ACK Flood	20/02/29 18:12:30	Ongoing	654.9 M	666.4 M	102.5 T
81:6:221::202	80	ACK Flood	20/02/29 18:12:30	Ongoing	653.4 M	665.7 M	95.7 T
81:6:221::102	80	ACK Flood	20/02/29 18:12:30	Ongoing	653 M	664.7 M	102.6 T
81:6:221::702	80	ACK Flood	20/02/29 18:12:30	Ongoing	651.6 M	663.8 M	151.4 T
81:6:221::602	80	ACK Flood	20/02/29 18:12:30	Ongoing	653.3 M	663.5 M	151.4 T
81:6:221::802	80	ACK Flood	20/02/29 18:12:30	Ongoing	656.7 M	663.3 M	148.3 T
81:6:221::2	80	HTTP Flood	20/02/29 18:12:30	Ongoing	655.3 M	662.4 M	145.3 T
81:6:221::902	80	ACK Flood	20/02/29 18:12:30	Ongoing	653.1 M	662 M	148.7 T
81:6:221::302	80	ACK Flood	20/03/01 16:32:00	Ongoing	0	661.2 M	61.2 T

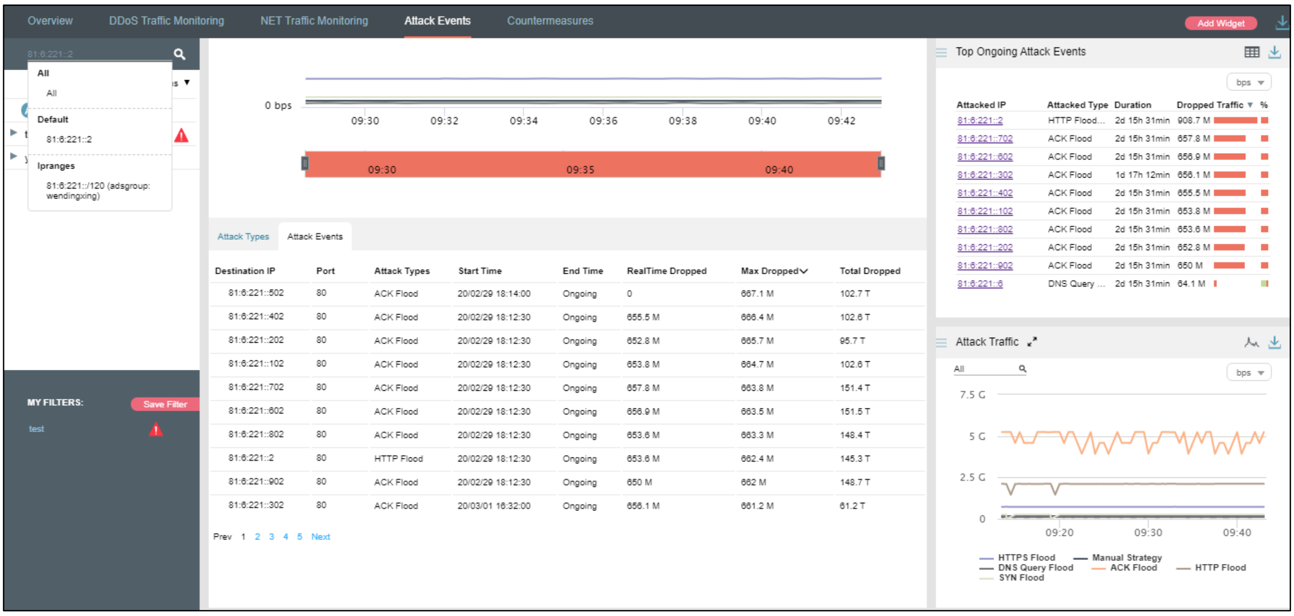
Prev 1 2 3 4 5 Next

Attacked IP	Attacked Type	Duration	Dropped Traffic	%
81:6:221::2	HTTP Flood...	2d 15h 31min	911 M	
81:6:221::802	ACK Flood	2d 15h 31min	656.7 M	
81:6:221::402	ACK Flood	2d 15h 31min	654.9 M	
81:6:221::202	ACK Flood	2d 15h 31min	653.4 M	
81:6:221::602	ACK Flood	2d 15h 31min	653.3 M	
81:6:221::902	ACK Flood	2d 15h 31min	653.1 M	
81:6:221::102	ACK Flood	2d 15h 31min	653 M	
81:6:221::702	ACK Flood	2d 15h 31min	651.6 M	
81:6:221::6	DNS Query ...	2d 15h 31min	64.3 M	
81.6.221.0	HTTPS Flo...	2d 15h 31min	47.7 M	

Step 2 Click in the search box.

The system displays all objects containing the current IP address.

Figure 4-49 Searching for an IP address object



Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:221::502	80	ACK Flood	20/02/29 18:14:00	Ongoing	0	667.1 M	102.7 T
81:6:221::402	80	ACK Flood	20/02/29 18:12:30	Ongoing	655.5 M	666.4 M	102.6 T
81:6:221::202	80	ACK Flood	20/02/29 18:12:30	Ongoing	652.8 M	665.7 M	95.7 T
81:6:221::102	80	ACK Flood	20/02/29 18:12:30	Ongoing	653.8 M	664.7 M	102.6 T
81:6:221::702	80	ACK Flood	20/02/29 18:12:30	Ongoing	657.8 M	663.8 M	151.4 T
81:6:221::602	80	ACK Flood	20/02/29 18:12:30	Ongoing	656.9 M	663.5 M	151.5 T
81:6:221::802	80	ACK Flood	20/02/29 18:12:30	Ongoing	653.6 M	663.3 M	148.4 T
81:6:221::2	80	HTTP Flood	20/02/29 18:12:30	Ongoing	653.6 M	662.4 M	145.3 T
81:6:221::902	80	ACK Flood	20/02/29 18:12:30	Ongoing	650 M	662 M	148.7 T
81:6:221::302	80	ACK Flood	20/03/01 16:32:00	Ongoing	656.1 M	661.2 M	61.2 T

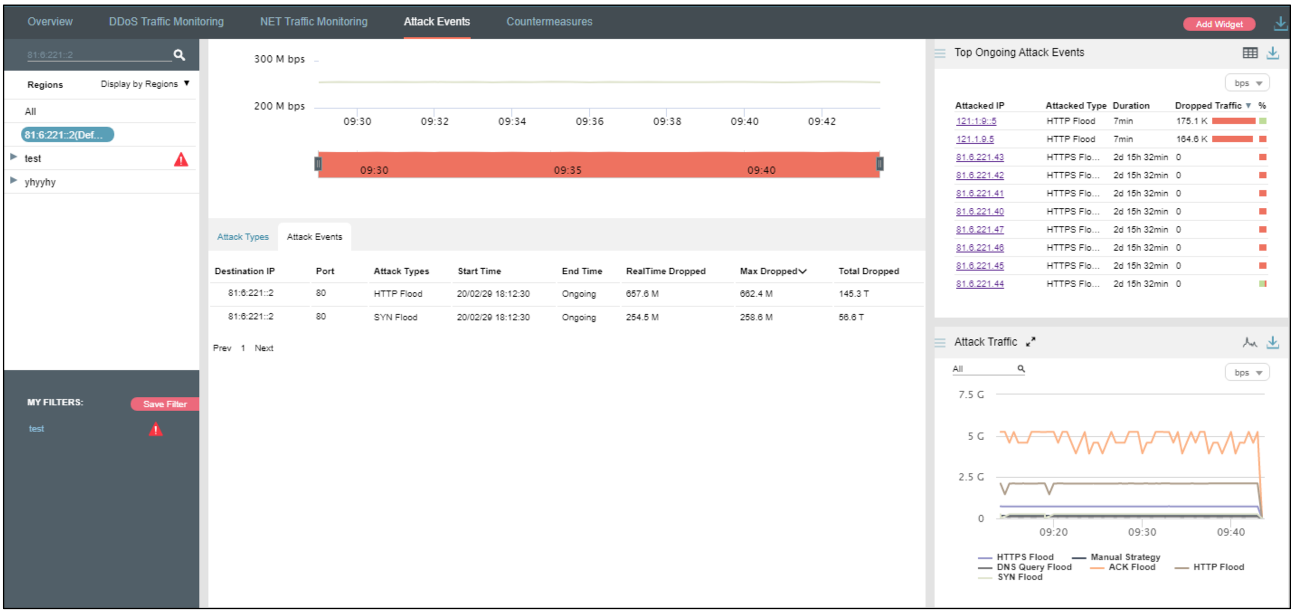
Prev 1 2 3 4 5 Next

Attacked IP	Attacked Type	Duration	Dropped Traffic	%
81:6:221::2	HTTP Flood...	2d 15h 31min	908.7 M	
81:6:221::702	ACK Flood	2d 15h 31min	657.8 M	
81:6:221::602	ACK Flood	2d 15h 31min	656.9 M	
81:6:221::302	ACK Flood	1d 17h 12min	656.1 M	
81:6:221::402	ACK Flood	2d 15h 31min	655.5 M	
81:6:221::102	ACK Flood	2d 15h 31min	653.8 M	
81:6:221::802	ACK Flood	2d 15h 31min	653.6 M	
81:6:221::202	ACK Flood	2d 15h 31min	652.8 M	
81:6:221::902	ACK Flood	2d 15h 31min	650 M	
81:6:221::6	DNS Query ...	2d 15h 31min	64.1 M	

Step 3 Select the desired IP address object and then press **Enter**.

The attack event information of this IP address is displayed, as shown in Figure 4-50.

Figure 4-50 Attack event information of an IP address



Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:221::2	80	HTTP Flood	20/02/29 18:12:30	Ongoing	657.6 M	662.4 M	145.3 T
81:6:221::2	80	SYN Flood	20/02/29 18:12:30	Ongoing	254.5 M	258.6 M	56.6 T

Attacked IP	Attacked Type	Duration	Dropped Traffic	%
121:1:9::5	HTTP Flood	7min	175.1 K	
121.1.9.5	HTTP Flood	7min	164.6 K	
81.6.221.43	HTTPS Flo...	2d 15h 32min	0	
81.6.221.42	HTTPS Flo...	2d 15h 32min	0	
81.6.221.41	HTTPS Flo...	2d 15h 32min	0	
81.6.221.40	HTTPS Flo...	2d 15h 32min	0	
81.6.221.47	HTTPS Flo...	2d 15h 32min	0	
81.6.221.46	HTTPS Flo...	2d 15h 32min	0	
81.6.221.45	HTTPS Flo...	2d 15h 32min	0	
81.6.221.44	HTTPS Flo...	2d 15h 32min	0	

----End

4.1.16.3 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top Ongoing Attack Events** panel to display traffic data in pps.

4.1.16.4 Downloading a Report

Click in the upper-right corner of the **Top Ongoing Attack Events** panel and then click or to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.17 Viewing Top 10 Source IP Addresses

The **Top 10 Source IP Addresses** panel shows top 10 source IP addresses ranked according to traffic dropped by ADS in the last 30 seconds.

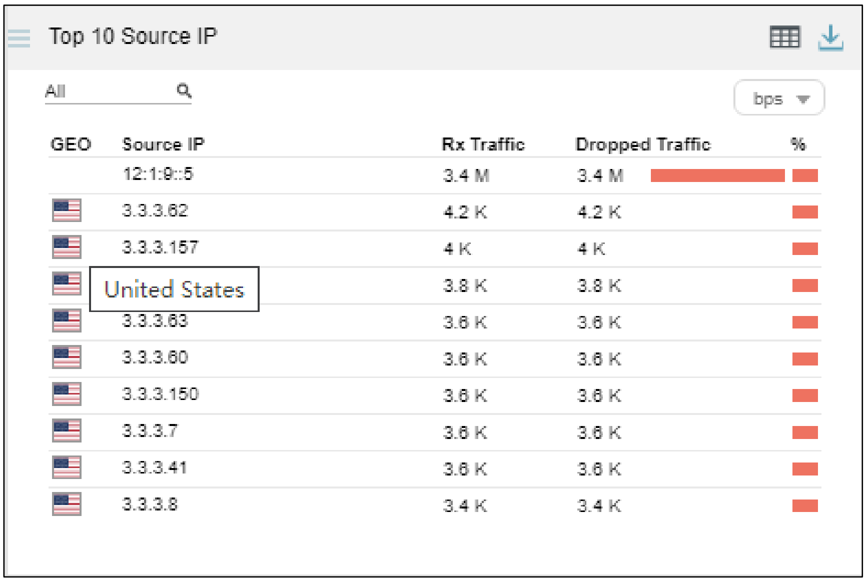
Data on this panel refreshes every 30 seconds.

4.1.17.1 Understanding Data on the Panel

The table ranks top 10 source IP addresses according to traffic dropped by ADS in the last 30 seconds.

- **GEO**: shows the national flag icons. Pointing to an icon displays the country name, as shown in Figure 4-51.

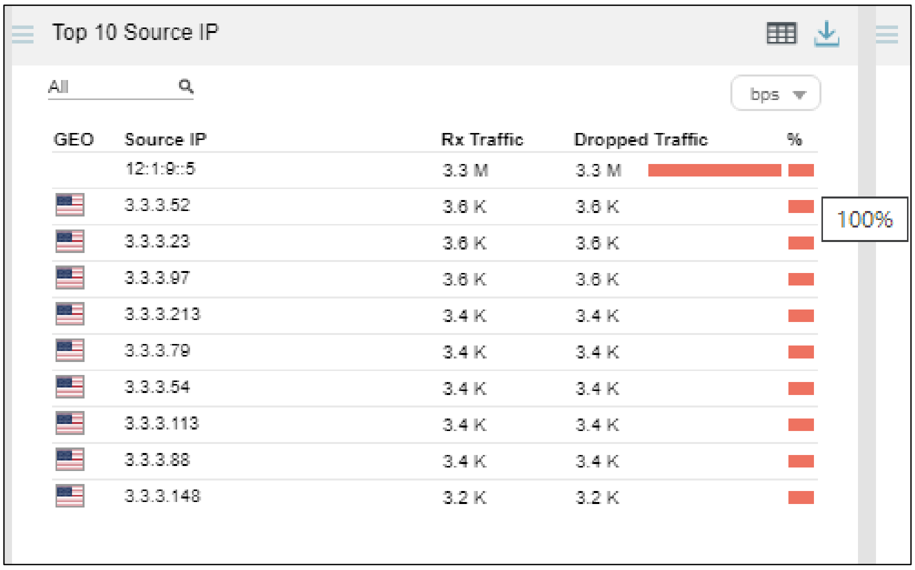
Figure 4-51 Display of the country name



GEO	Source IP	Rx Traffic	Dropped Traffic	%
	12:1:9::5	3.4 M	3.4 M 🟥	🟥
🇺🇸	3.3.3.62	4.2 K	4.2 K	🟥
🇺🇸	3.3.3.157	4 K	4 K	🟥
🇺🇸		3.8 K	3.8 K	🟥
🇺🇸	3.3.3.63	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.60	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.150	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.7	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.41	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.8	3.4 K	3.4 K	🟥

- **Source IP**: shows source IP addresses.
- **Rx Traffic**: shows the total traffic received by ADS devices in the last 30 seconds.
- **Dropped Traffic**: shows the total maximum traffic dropped by all ADS devices in the last 30 seconds. The red bar to the right of the traffic value also indicates the maximum value. A longer bar indicates more traffic dropped.
- **%**: shows the percentage of forwarded traffic and that of dropped traffic to incoming traffic. Pointing to a bar in this column displays the specific percentage. In a bar, green indicates legitimate traffic and red indicates dropped traffic. As shown in Figure 4-52, the percentage of dropped traffic for 12:1:9::5 is 100%.

Figure 4-52 Percentage of dropped traffic of a source IP address



GEO	Source IP	Rx Traffic	Dropped Traffic	%
	12:1:9::5	3.3 M	3.3 M 🟥	🟥
🇺🇸	3.3.3.52	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.23	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.97	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.213	3.4 K	3.4 K	🟥
🇺🇸	3.3.3.79	3.4 K	3.4 K	🟥
🇺🇸	3.3.3.54	3.4 K	3.4 K	🟥
🇺🇸	3.3.3.113	3.4 K	3.4 K	🟥
🇺🇸	3.3.3.88	3.4 K	3.4 K	🟥
🇺🇸	3.3.3.148	3.2 K	3.2 K	🟥

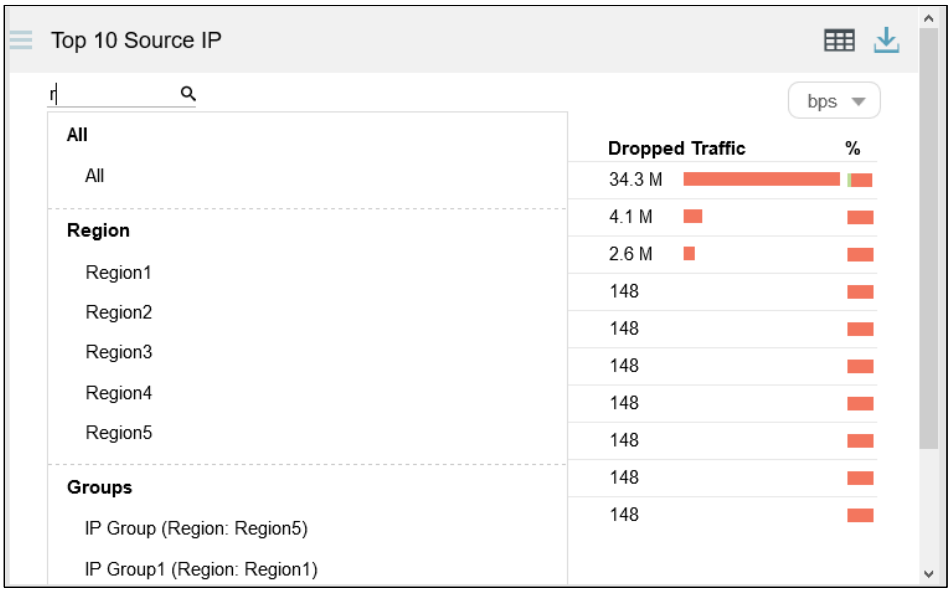
4.1.17.2 Viewing Traffic of a Specific Object

By default, the **Top 10 Source IP** panel presents top 10 source IP addresses based on data collected from all ADS devices. You can specify a region, region IP group, ADS device, or ADS-protected group to view its top source IP addresses ranked according to traffic dropped in the last 30 minutes. You can also specify a source IPv4 or IPv6 address to view its traffic information in the last 30 minutes.

Step 1 On the page shown in Figure 4-52, type a character string and then press **Enter**.

The system displays all objects containing the typed character string.

Figure 4-53 Searching for an object



Top 10 Source IP

r

bps

All

All

Region

Region1

Region2

Region3

Region4

Region5

Groups

IP Group (Region: Region5)

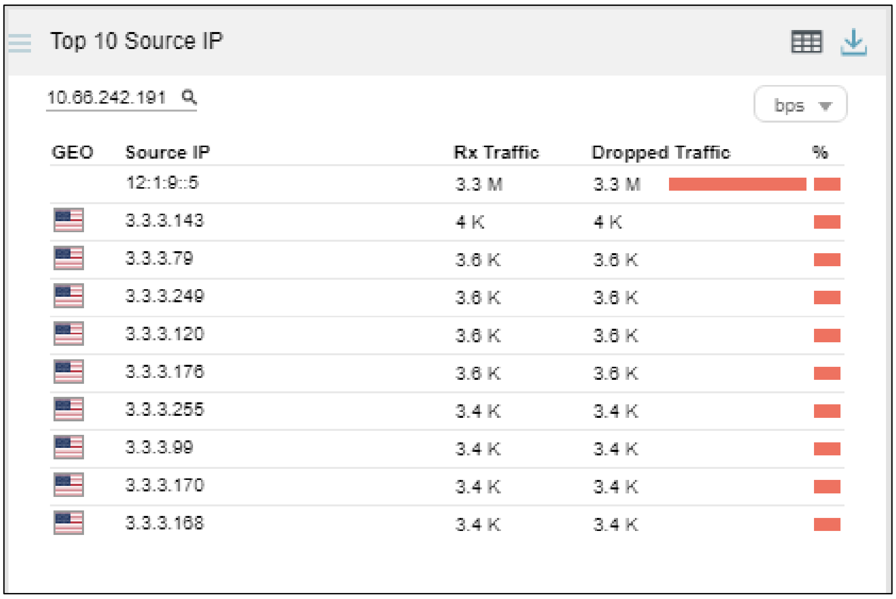
IP Group1 (Region: Region1)

Dropped Traffic	%
34.3 M	
4.1 M	
2.6 M	
148	
148	
148	
148	
148	
148	
148	

Step 2 Select an object and press **Enter**.

Then source IP addresses associated with the specified object are listed in descending order of traffic handled by ADS in the last 30 minutes.

Figure 4-54 Traffic of top 10 source IP addresses associated with a specific object



Top 10 Source IP

10.66.242.191

bps

GEO	Source IP	Rx Traffic	Dropped Traffic	%
	12:1:9::5	3.3 M	3.3 M	🟥
🇺🇸	3.3.3.143	4 K	4 K	🟥
🇺🇸	3.3.3.79	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.249	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.120	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.176	3.6 K	3.6 K	🟥
🇺🇸	3.3.3.255	3.4 K	3.4 K	🟥
🇺🇸	3.3.3.99	3.4 K	3.4 K	🟥
🇺🇸	3.3.3.170	3.4 K	3.4 K	🟥
🇺🇸	3.3.3.168	3.4 K	3.4 K	🟥

----End

4.1.17.3 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top 10 Source IP** panel to display traffic data in pps.

4.1.17.4 Downloading a Report

Click ⤓ in the upper-right corner of the **Top 10 Source IP** panel and then click HTML or PDF to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.18 Viewing Attack Type Distribution

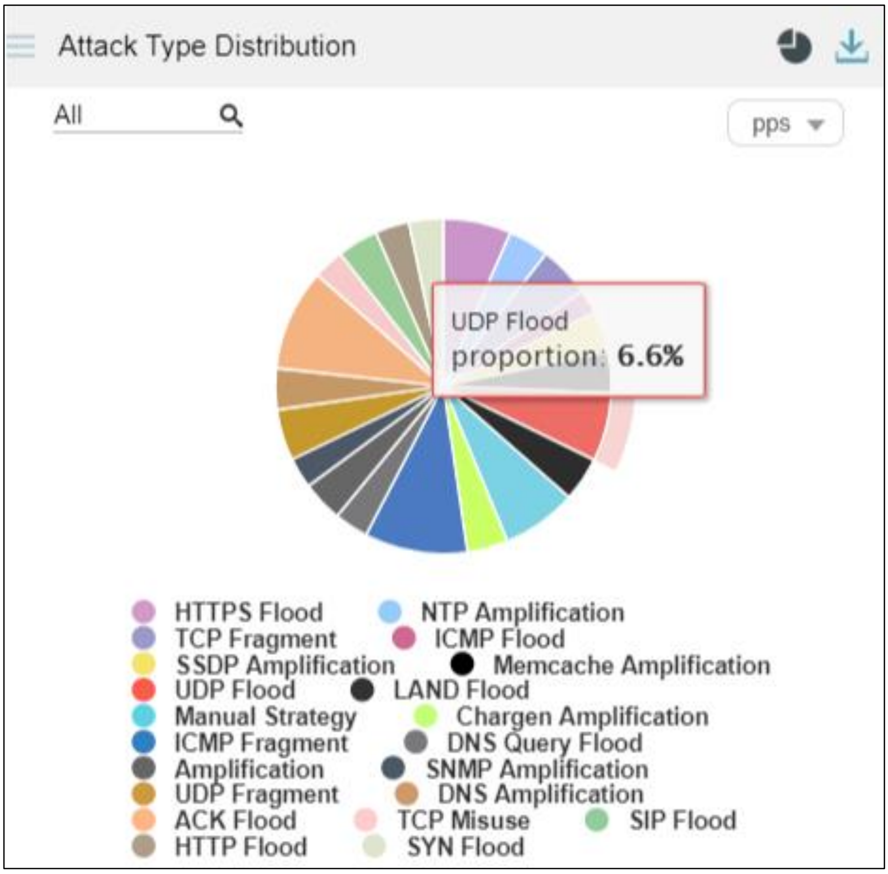
The **Attack Type Distribution** panel shows the percentage of traffic of each attack type to the total traffic detected by ADS in the last 30 seconds.

Each attack type is shown in a different color and data on this panel refreshes every 30 seconds.

4.1.18.1 Viewing the Percentage of Traffic of an Attack Type

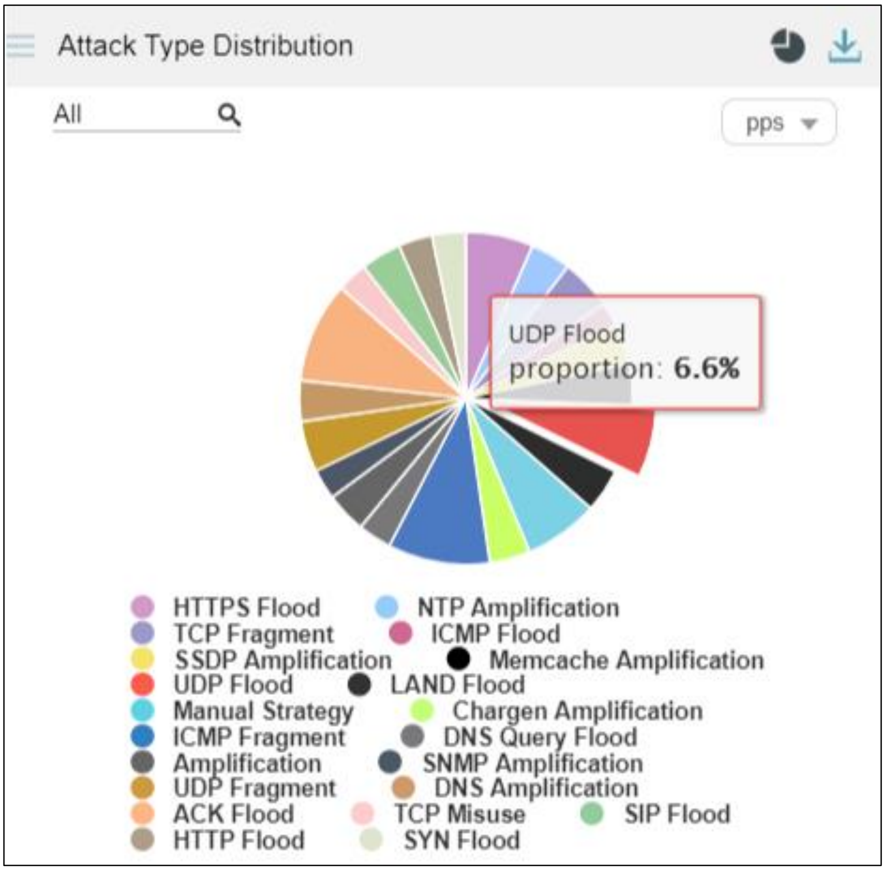
Pointing to the area of a specific attack type displays the percentage of traffic of this attack type to the total traffic, as shown in Figure 4-55.

Figure 4-55 Percentage of traffic of an attack type



Clicking in this area separates this area from other areas, as shown in Figure 4-56.

Figure 4-56 Separating the area of an attack type from other areas



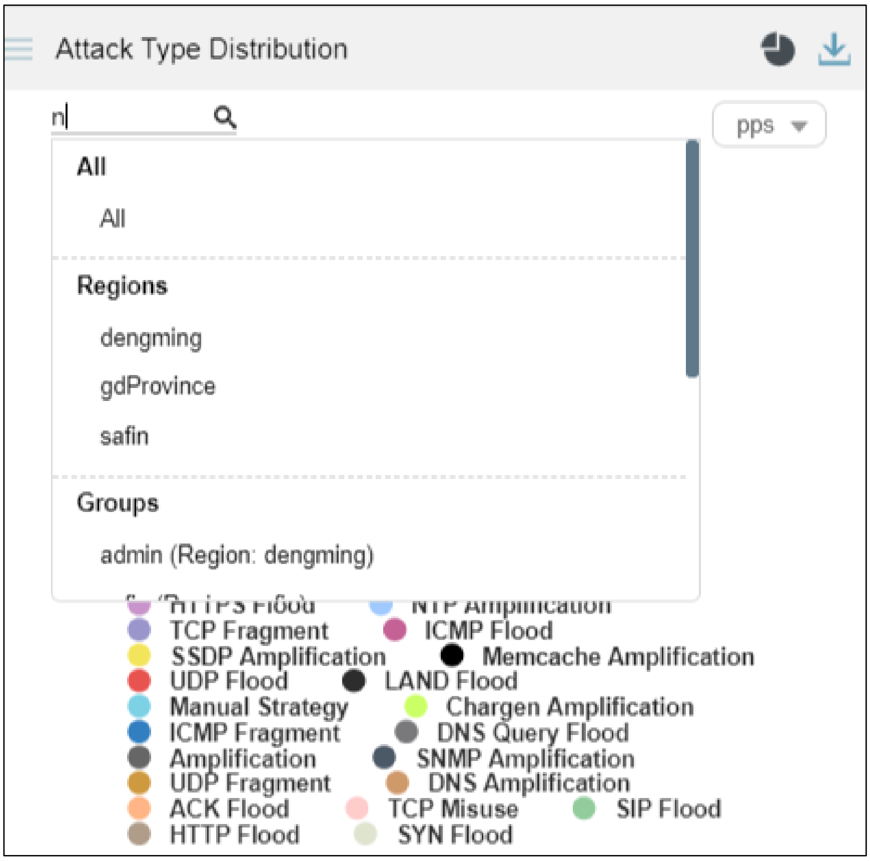
4.1.18.2 Viewing Attack Type Distribution of a Specified Object

By default, the **Attack Type Distribution** graph presents the distribution of attack types based on data collected from all ADS devices. You can specify a region, region IP group, ADS device, ADS-protected group, or IPv4 or IPv6 address to view its attack type distribution in the last 30 minutes.

Step 1 On the page shown in Figure 4-55, type a character string.

The system displays all objects containing the typed character string, as shown in Figure 4-57.

Figure 4-57 Searching for an object



Attack Type Distribution

n

pps

All

All

Regions

dengming

gdProvince

safin

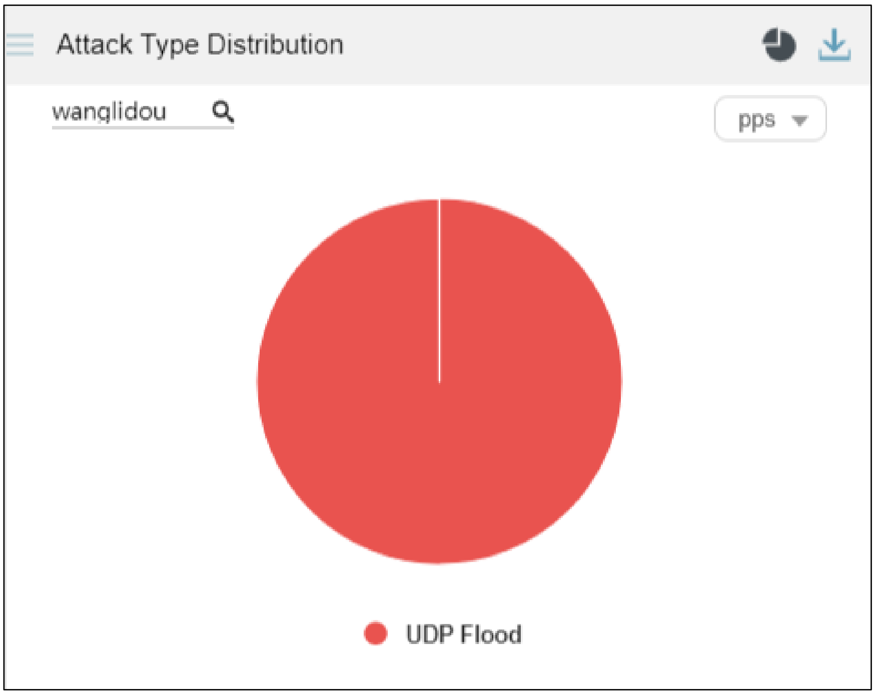
Groups

admin (Region: dengming)

Step 2 Select an object and press **Enter**.

Then the attack type distribution of a specified object in the last 30 minutes is displayed.

Figure 4-58 Attack type distribution of a specified object



----End

4.1.18.3 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Attack Type Distribution** panel to display traffic data in pps.

4.1.18.4 Downloading a Report

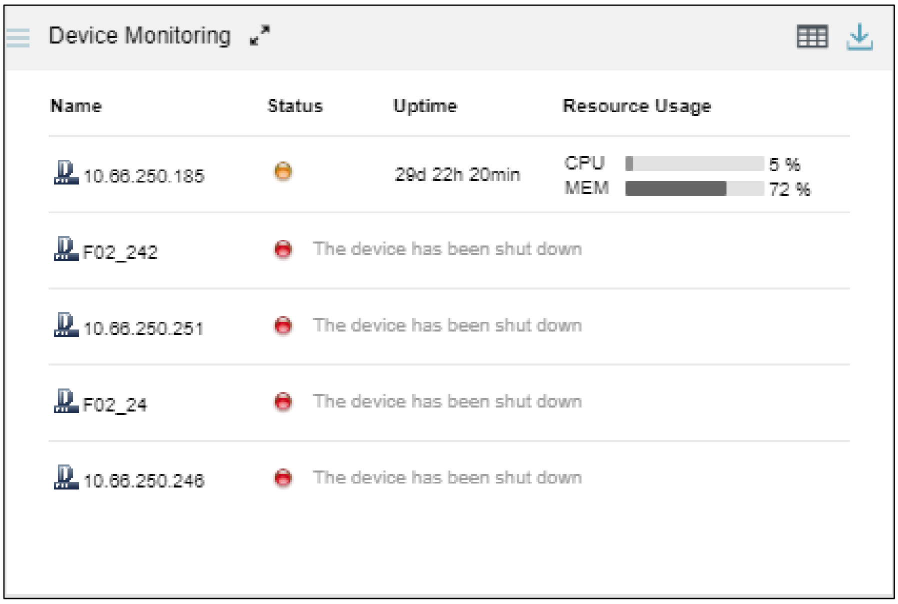
Click ⤓ in the upper-right corner of the **Attack Type Distribution** panel and then click HTML or PDF to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.19 Viewing Device Monitoring Information

The **Device Monitoring** panel shows the detailed monitoring information collected from ADS devices and NTA devices in the last 30 seconds, as shown in Figure 4-59.

Data on this panel refreshes every 30 seconds.

Figure 4-59 Device monitoring information

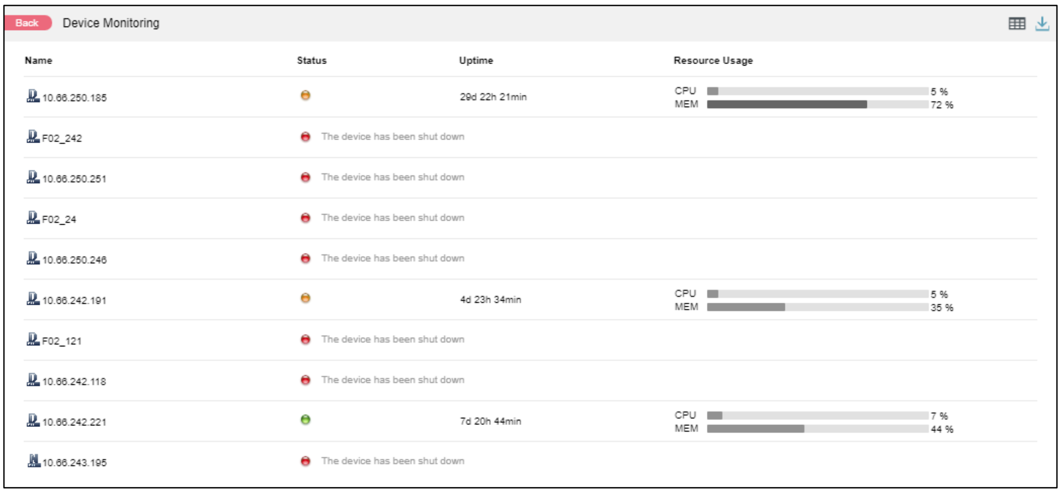


Device Monitoring

Name	Status	Uptime	Resource Usage
10.66.250.185	●	29d 22h 20min	CPU 5 % MEM 72 %
F02_242	● The device has been shut down		
10.66.250.251	● The device has been shut down		
F02_24	● The device has been shut down		
10.66.250.246	● The device has been shut down		

Clicking ⤢ displays more details about the monitored devices, as shown in Figure 4-60.

Figure 4-60 More details about the monitored devices



Device Monitoring

Name	Status	Uptime	Resource Usage
10.66.250.185	●	29d 22h 21min	CPU 5 % MEM 72 %
F02_242	● The device has been shut down		
10.66.250.251	● The device has been shut down		
F02_24	● The device has been shut down		
10.66.250.246	● The device has been shut down		
10.66.242.191	●	4d 23h 34min	CPU 5 % MEM 35 %
F02_121	● The device has been shut down		
10.66.242.118	● The device has been shut down		
10.66.242.221	●	7d 20h 44min	CPU 7 % MEM 44 %
10.66.243.195	● The device has been shut down		

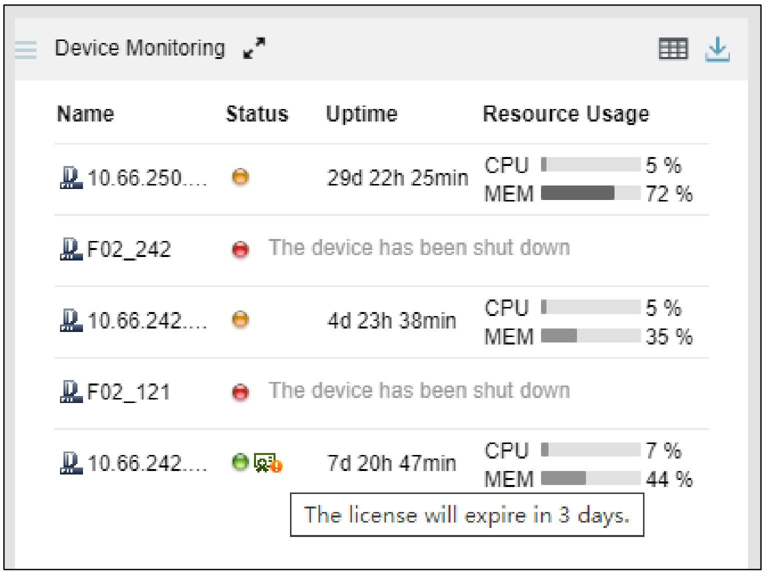
4.1.19.1 Understanding Data on the Panel

The **Device Monitoring** panel shows detailed monitoring information collected from all ADS devices and NTA devices.

- **Name**: shows the name of an NTA or ADS device.
- **Status**: shows whether the device is online.
  - When the device is online and properly connected, the ● icon is displayed.
  - When the device is offline, **The device has been shut down** is displayed in the **Status** column, but no status icon appears.

- If the time of an online device is not synchronized with that of ADS M, the ● icon is displayed.
- If the license of a device is about to expire, the ● icon is displayed. Pointing to this icon displays the license information.

Figure 4-61 License expiration reminder



Device Monitoring ⤢

Name	Status	Uptime	Resource Usage
10.66.250....	●	29d 22h 25min	CPU 5 % MEM 72 %
F02_242	● The device has been shut down		
10.66.242....	●	4d 23h 38min	CPU 5 % MEM 35 %
F02_121	● The device has been shut down		
10.66.242....	● ●	7d 20h 47min	CPU 7 % MEM 44 %

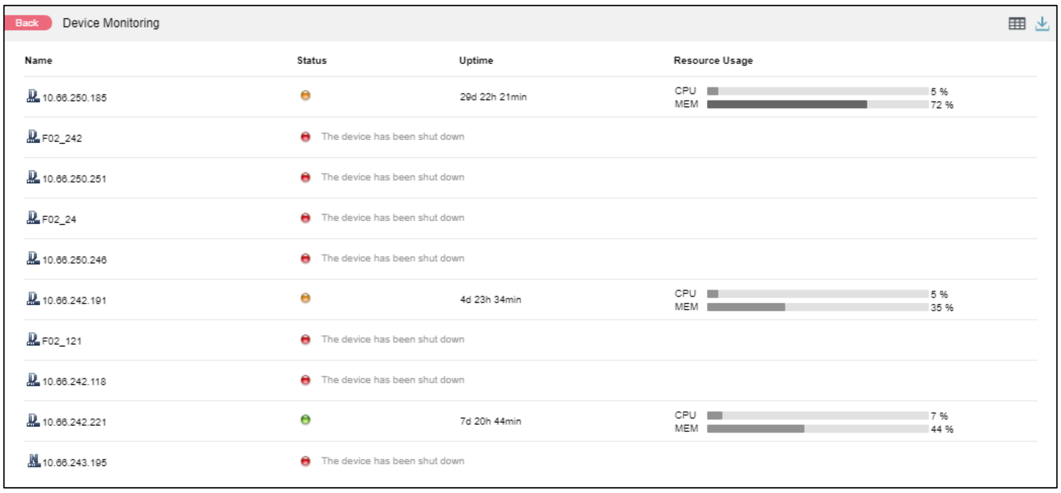
The license will expire in 3 days.

- **Uptime**: shows how long the system has been running continuously. The uptime is available only for online devices.
- **Resource Usage**: shows the CPU/memory usage. Such information is available only to online devices.

  If the CPU or memory usage exceeds 80%, the bar turns red.

You can click ⤢ to switch to the full screen mode, as shown in Figure 4-62.

Figure 4-62 Device monitoring information in full screen mode



Back Device Monitoring

Name	Status	Uptime	Resource Usage
10.66.250.185	●	29d 22h 21min	CPU 5 % MEM 72 %
F02_242	● The device has been shut down		
10.66.250.251	● The device has been shut down		
F02_24	● The device has been shut down		
10.66.250.246	● The device has been shut down		
10.66.242.191	●	4d 23h 34min	CPU 5 % MEM 35 %
F02_121	● The device has been shut down		
10.66.242.118	● The device has been shut down		
10.66.242.221	●	7d 20h 44min	CPU 7 % MEM 44 %
10.66.243.195	● The device has been shut down		

You can click **Back** to return to the normal panel display mode.

4.1.19.2 Downloading a Report

Click in the upper-right corner of the **Device Monitoring** panel and then click or to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.20 Viewing Traffic of Top NTA Regions

The **Top NTA Region Traffic** panel presents in real time top 10 NTA's regions with the largest network traffic in the last 30 seconds, making it convenient for users to learn which regions receive or transmit the largest network traffic.

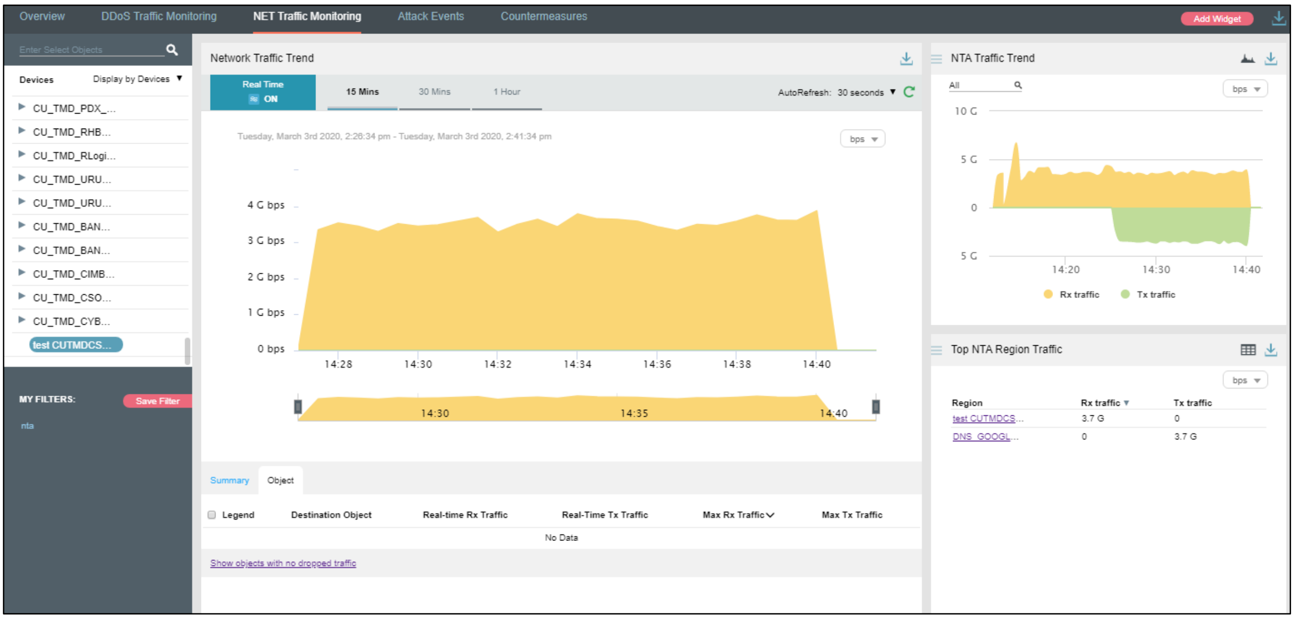
Data on this panel refreshes every 30 seconds.

4.1.20.1 Understanding Data on the Panel

The list ranks NTA's top 10 regions according to network traffic generated in the last 30 seconds.

- **Region**: region that receives or transmits traffic. Clicking a region name opens the **NET Traffic Monitoring** tab page, where you can view more details about this region's traffic, as shown in Figure 4-63.

Figure 4-63 Traffic of a specific region



AutoRefresh: 30 seconds ▼

□ Legend	Destination Object	Real-time Rx Traffic	Real-Time Tx Traffic	Max Rx Traffic	Max Tx Traffic
No Data					

Region	Rx traffic ▼	Tx traffic
test CUTMDCS...	3.7 G	0
DNS_GOOGL...	0	3.7 G

- **Rx traffic**: traffic received by NTA in the last 30 seconds
- **Tx traffic**: traffic transmitted by NTA in the last 30 seconds

4.1.20.2 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **Top NTA Region Traffic** panel to display traffic data in pps.

4.1.20.3 Downloading a Report

Click ⤓ in the upper-right corner of the **Top NTA Region Traffic** panel and then click HTML or PDF to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.1.21 Viewing Trends of Traffic on NTA

The **NTA Traffic Trend** panel shows trends of traffic received and transmitted in the last 30 minutes by NTA under monitoring of ADS M.

Data on this panel refreshes every 30 seconds.

4.1.21.1 Understanding Data on the Panel

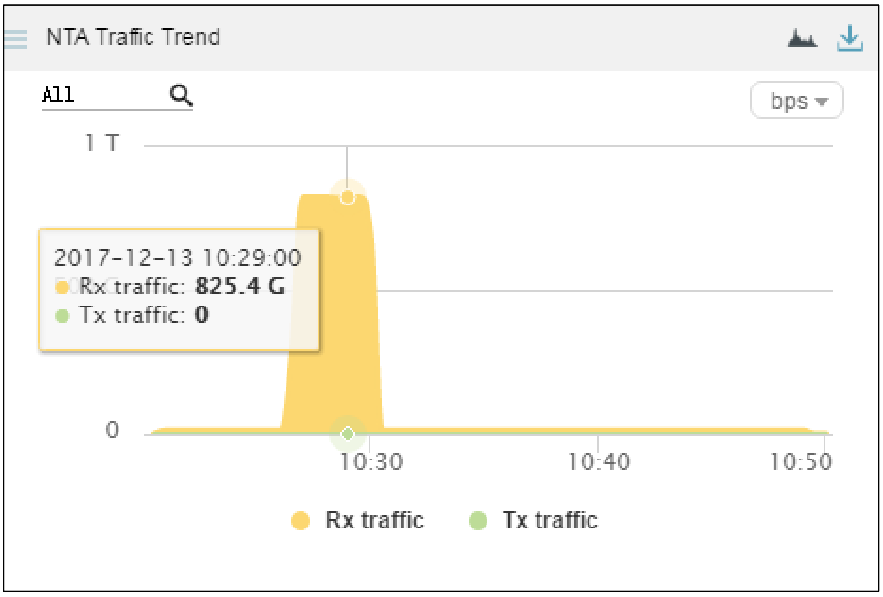
In the **NTA Traffic Trend** graph,

- The x-axis indicates time, spanning the last 30 minutes.
- The y-axis indicates traffic:
  - The yellow area represents the total traffic received.
  - The green area represents the total traffic transmitted.

4.1.21.2 Viewing Traffic at a Random Point of Time

Pointing to a random point in the **NTA Traffic Trend** graph displays the specific time, incoming traffic, outgoing traffic, and dropped traffic, as shown in Figure 4-64.

Figure 4-64 Detailed traffic information at a specific point of time



2017-12-13 10:29:00
● Rx traffic: **825.4 G**
● Tx traffic: **0**

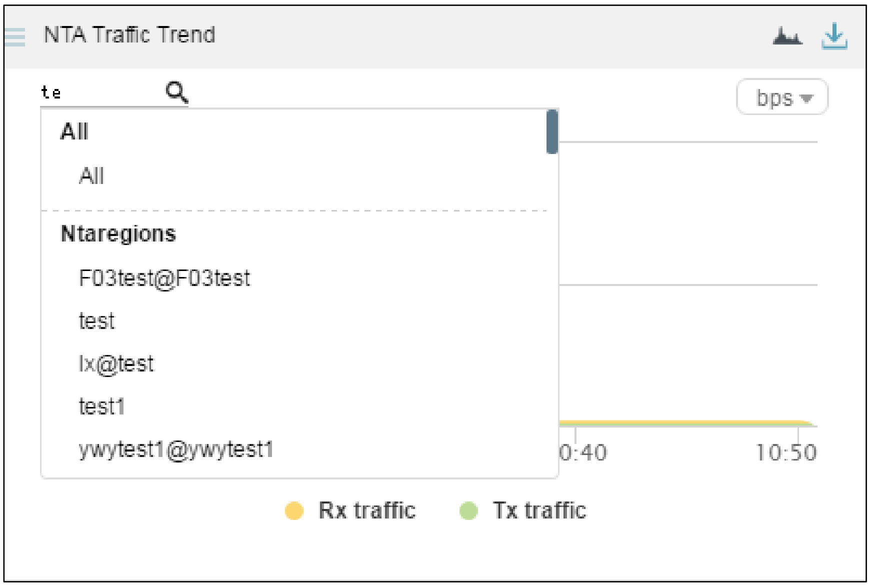
4.1.21.3 Viewing Traffic of a Specified Object

By default, the **NTA Traffic Trend** graph presents trends of traffic handled by all NTA devices under monitoring of ADS M. You can view real-time traffic trends of a specified region, regional IP group, and NTA device.

Step 1 On the page shown in Figure 4-64, type a character string and then press **Enter**.

The system displays all objects containing the typed character string, as shown in Figure 4-65.

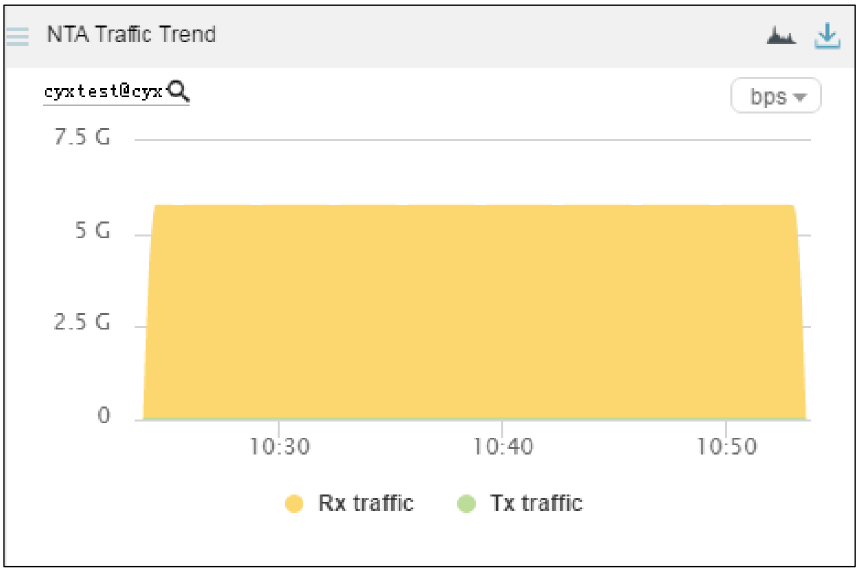
Figure 4-65 Searching for an object



Step 2 Select an object and press **Enter**.

Traffic trends of the specified object are displayed, as shown in Figure 4-66.

Figure 4-66 Real-time traffic trends of a specified object



----End

4.1.21.4 Switching the Traffic Unit

The default traffic unit is **bps**. You can select **pps** from the drop-down list in the upper-right corner of the **NTA Traffic Trend** panel to display traffic data in pps.

4.1.21.5 Downloading a Report

Click ⤓ in the upper-right corner of the **NTA Traffic Trend** panel and then click HTML or PDF to export data of this panel as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.2 DDoS Traffic Monitoring

Note	ADS M presents attack traffic based on data uploaded by ADS devices.

Under **Traffic Monitoring > DDoS Traffic Monitoring**, you can do as follows:

- View real-time and historical attack traffic trends of all objects or a specified region, regional IP group, ADS device, ADS-protected group, or IP address.
- View or add panels.
- Configure filters.

IP addresses under the default protection group do not belong to any regions or ADS-protected groups. To view attack traffic information of such an IP address, you need to expressly indicate the IP address before the system displays such information.

Attack traffic information includes real-time traffic information and historical traffic information. By default, attack traffic information is displayed by region.

4.2.1 Viewing Real-Time Attack Traffic Information

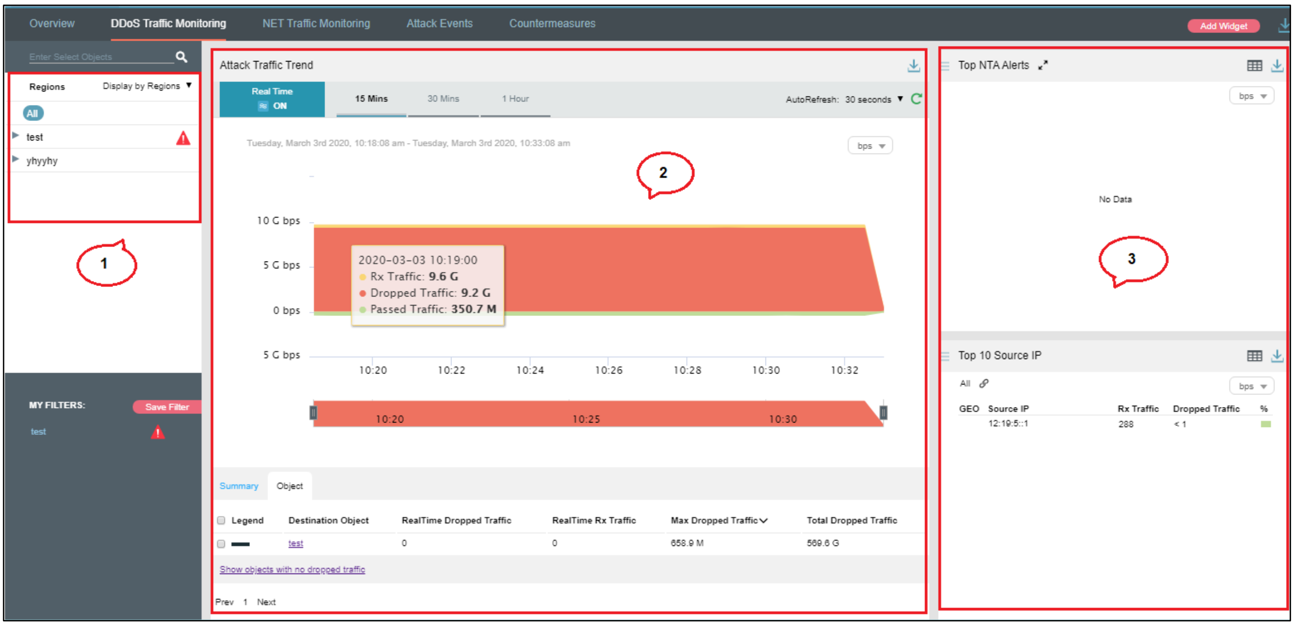
To view real-time attack traffic information, follow these steps:

Step 1 Choose **Traffic Monitoring** > **DDoS Traffic Monitoring**.

Real-time attack traffic information of all objects is displayed by default, including **Attack Traffic Trend**, **Top Destination IP**, and **Protocols Analysis** panels.

In real-time mode, trends of traffic in the last 15 minutes is displayed by default. You can click **30 Mins** or **1 Hour** to view the attack traffic trend of the last 30 minutes or last hour.

Figure 4-67 Attack traffic information of all objects



Tuesday, March 3rd 2020, 10:18:08 am - Tuesday, March 3rd 2020, 10:33:08 am

2020-03-03 10:19:00
● Rx Traffic: **9.6 G**
● Dropped Traffic: **9.2 G**
● Passed Traffic: **350.7 M**

□ Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
□ ▬	test	0	0	658.9 M	569.6 G

GEO	Source IP	Rx Traffic	Dropped Traffic	%
	12:19:5::1	288	< 1	🟩

Table 4-2 describes areas of the **DDoS Traffic Monitoring** page.

Table 4-2 Layout for the DDoS Traffic Monitoring page

No.	Description
1	List of objects
2	Traffic trend
3	Panels

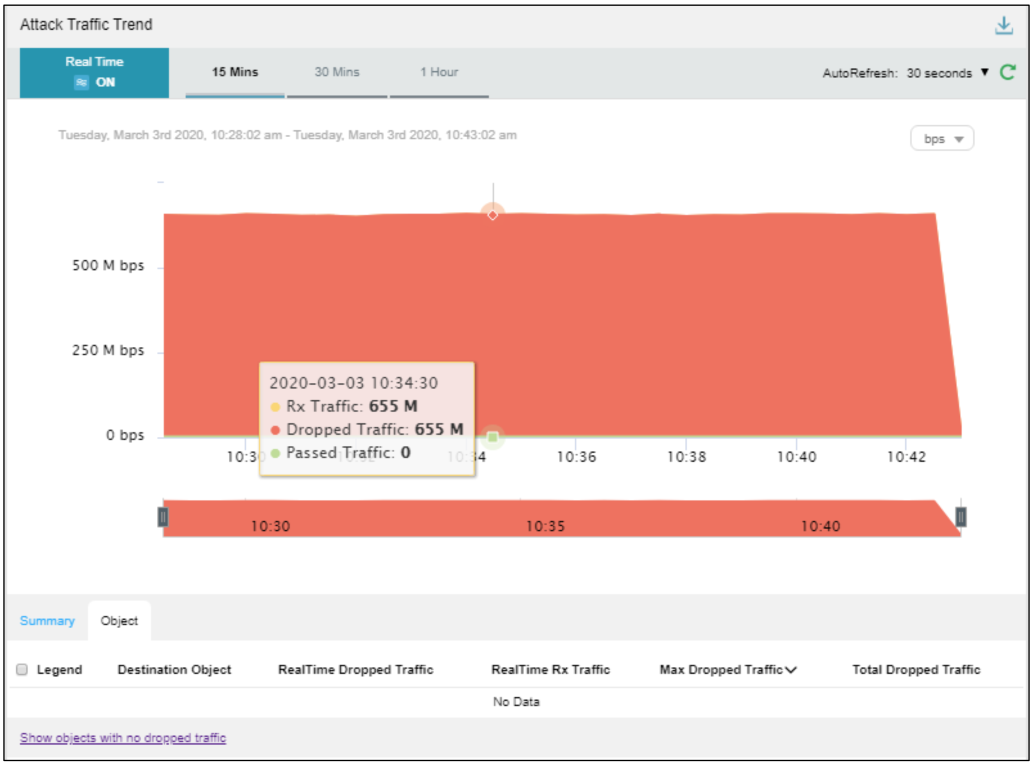
On the **DDoS Traffic Monitoring** page, the **Object** tab page ranks regions in descending order of traffic dropped by ADS.

Table 4-3 Real-time attack traffic trend – parameters on the Objects tab page

Parameter	Description
Legend	Shows various shades of blue from dark to light, indicating the total dropped traffic. A darker blue indicates more traffic dropped.
Destination Object	Indicates the traffic monitoring object.
RealTime Dropped Traffic	Indicates traffic (in bps or pps) dropped by ADS for the object.
RealTime Rx Traffic	Indicates traffic (in bps or pps) received by the object in real time.
Max Dropped Traffic	Indicates the maximum traffic (in bps or pps) dropped by ADS for the object in the statistical period.
Total Dropped Traffic	Indicates the total traffic (in bits) dropped by ADS for the object in the statistical period. The traffic unit is bit.

Step 2 On the **Object** tab page shown in Figure 4-67, select one or more objects to view traffic dropped by ADS for them. See Figure 4-68.

Figure 4-68 Real-time traffic trend graph of a specified object



☐ Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
			No Data		

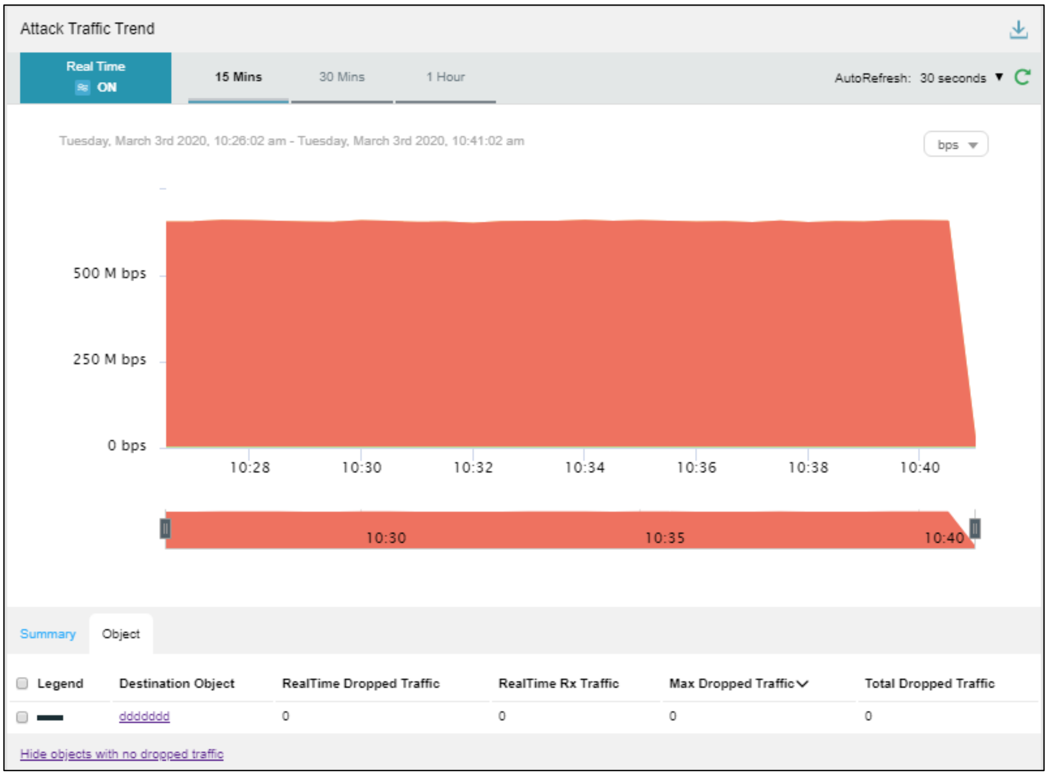
Show objects with no dropped traffic

By default, only the objects with traffic dropped by ADS are displayed.

Step 3 Click **Show objects with no dropped traffic** to display objects with traffic dropped by ADS and objects with no traffic dropped.

Clicking **Hide objects with no dropped traffic** hides objects with no traffic dropped.

Figure 4-69 Real-time attack traffic trend graph of all objects



AutoRefresh: 30 seconds

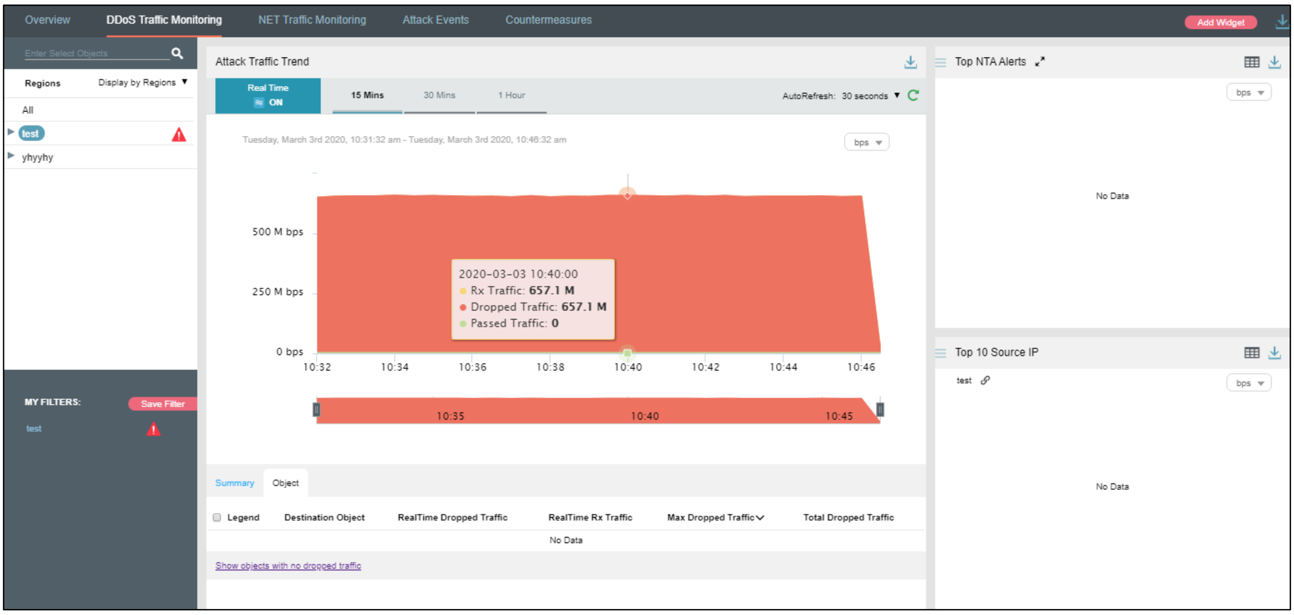
Tuesday, March 3rd 2020, 10:26:02 am - Tuesday, March 3rd 2020, 10:41:02 am

☐ Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
☐ ▬	ddddddd	0	0	0	0

Hide objects with no dropped traffic

Step 4 Point to a random point in the attack traffic trend graph to display the total traffic received, passed, and dropped by ADS at a specific point of time for specified objects, as shown in Figure 4-70.

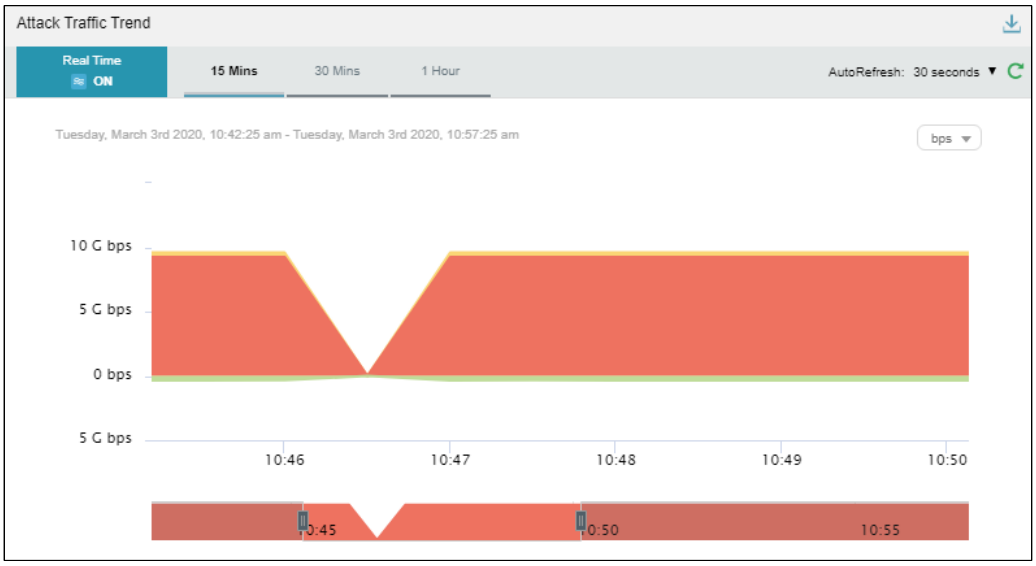
Figure 4-70 DDoS attack traffic information at a specific time



☐ Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
No Data					

Step 5 Below the attack traffic trend graph, drag ▯ to view a finer-granularity traffic trend.

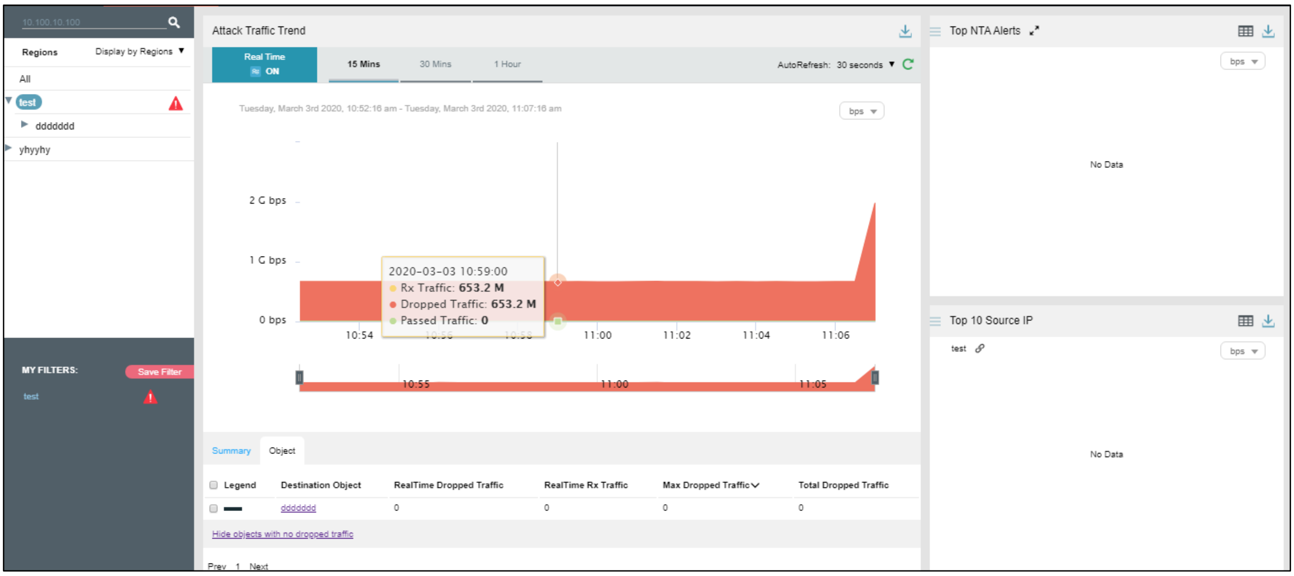
Figure 4-71 Finer-granularity traffic information



Step 6 Click a link of a region or IP group in the **Destination Object** column.

Traffic information of IP addresses in the region or IP group is displayed, including **Attack Traffic Trend**, **Top Destination IP**, and **Protocols Analysis**.

Figure 4-72 Traffic information of a specific region



□ Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
□ ▬	ddddddd	0	0	0	0

Step 7 On the page shown in Figure 4-67, click **Summary**.

The average and total are displayed for dropped traffic, passed traffic, and received traffic in the statistical period.

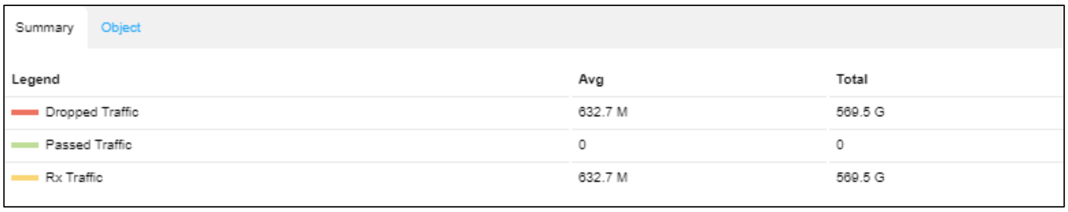
Clicking the bar or text in the **Legend** column hides or displays the corresponding traffic in the attack traffic trend graph. By default, all three types of traffic are displayed. A dimmed legend indicates that this type of traffic is hidden.

Table 4-4 describes parameters on the **Summary** tab page.

Table 4-4 Real-time traffic trend – parameters on the Summary tab page

Parameter	Description
Legend	Legends for dropped traffic, passed traffic, and received traffic.
Avg	Average traffic dropped, passed, or received. The traffic unit is bps or pps.
Total	Total traffic dropped, passed, or received. The traffic unit is bit.

Figure 4-73 Summary of real-time attack traffic monitoring

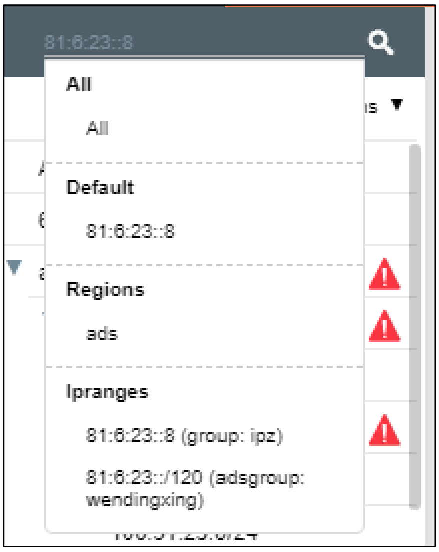


Legend	Avg	Total
🟥 Dropped Traffic	632.7 M	569.5 G
🟩 Passed Traffic	0	0
🟨 Rx Traffic	632.7 M	569.5 G

Step 8 Type an IP address in the search bar in the left pane shown Figure 4-67.

Then the traffic monitoring information of the region to which the IP address in question belongs appears.

Figure 4-74 Searching for information associated with an IP address



81:6:23::8

All

All

Default

81:6:23::8

Regions

ads

Ipranges

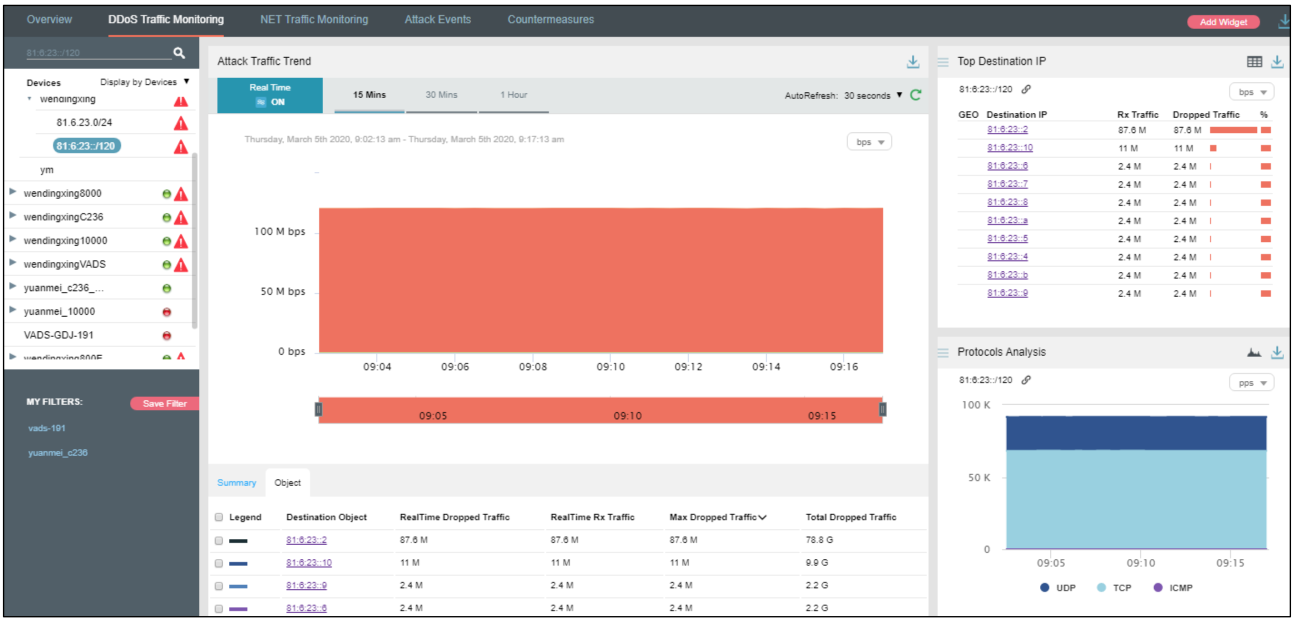
81:6:23::8 (group: ipz)

81:6:23::/120 (adsgroup: wendingxing)

Step 9 Click an IP address in the list.

Then the panels concerning this IP address, including **Attack Traffic Trend**, **Top Destination IP**, and **Protocols Analysis**, are displayed, as shown in Figure 4-75.

Figure 4-75 Real-time traffic monitoring of an IP address



Thursday, March 5th 2020, 9:02:13 am - Thursday, March 5th 2020, 9:17:13 am

Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
▬	81:6:23::2	87.6 M	87.6 M	87.6 M	78.8 G
▬	81:6:23::10	11 M	11 M	11 M	9.9 G
▬	81:6:23::9	2.4 M	2.4 M	2.4 M	2.2 G
▬	81:6:23::6	2.4 M	2.4 M	2.4 M	2.2 G

81:6:23::/120

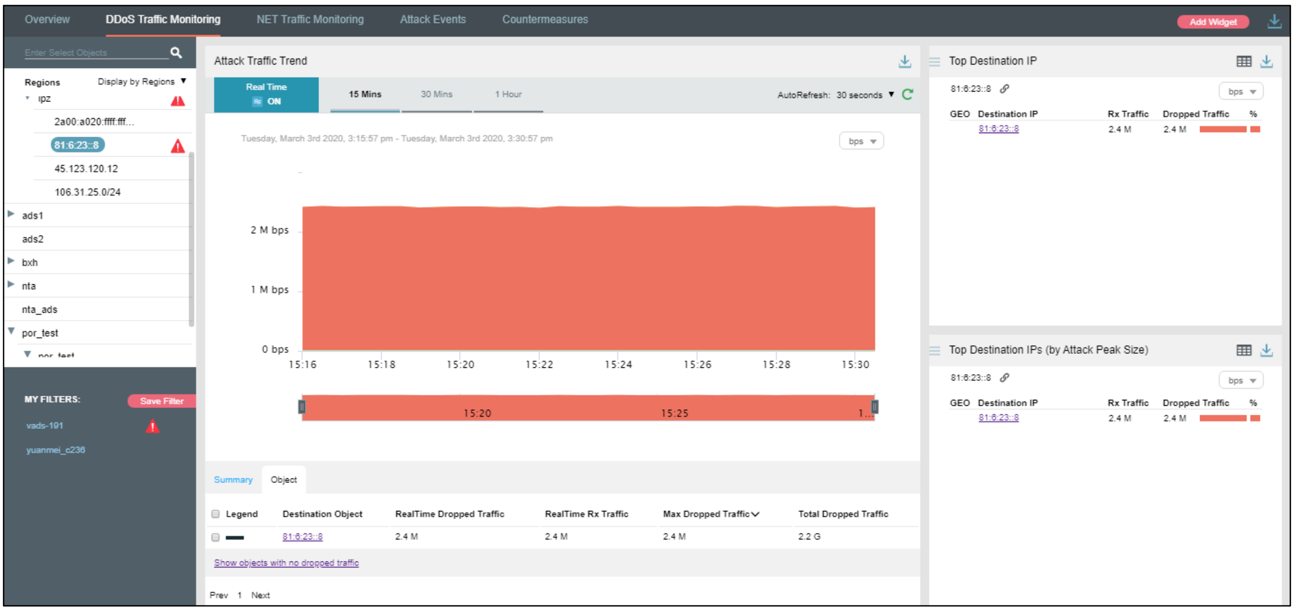
GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:23::2	87.6 M	87.6 M	
	81:6:23::10	11 M	11 M	
	81:6:23::6	2.4 M	2.4 M	
	81:6:23::7	2.4 M	2.4 M	
	81:6:23::8	2.4 M	2.4 M	
	81:6:23::a	2.4 M	2.4 M	
	81:6:23::5	2.4 M	2.4 M	
	81:6:23::4	2.4 M	2.4 M	
	81:6:23::b	2.4 M	2.4 M	
	81:6:23::9	2.4 M	2.4 M	

----End

4.2.2 Viewing Region-Specific Traffic Information

On the page shown in Figure 4-67, clicking a region in the left pane displays traffic information of the region and of all IP groups and IP addresses in this region. You can further view historical and real-time traffic trends and panels of a selected region, IP group under a region, or IP address. For example, you can choose **ads** > **ipz** > **81:6:23::8** to view traffic information of IP address 81:6:23::8.

Figure 4-76 DDoS Traffic Monitoring page



Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
☐ ▬	81:6:23::8	2.4 M	2.4 M	2.4 M	2.2 G

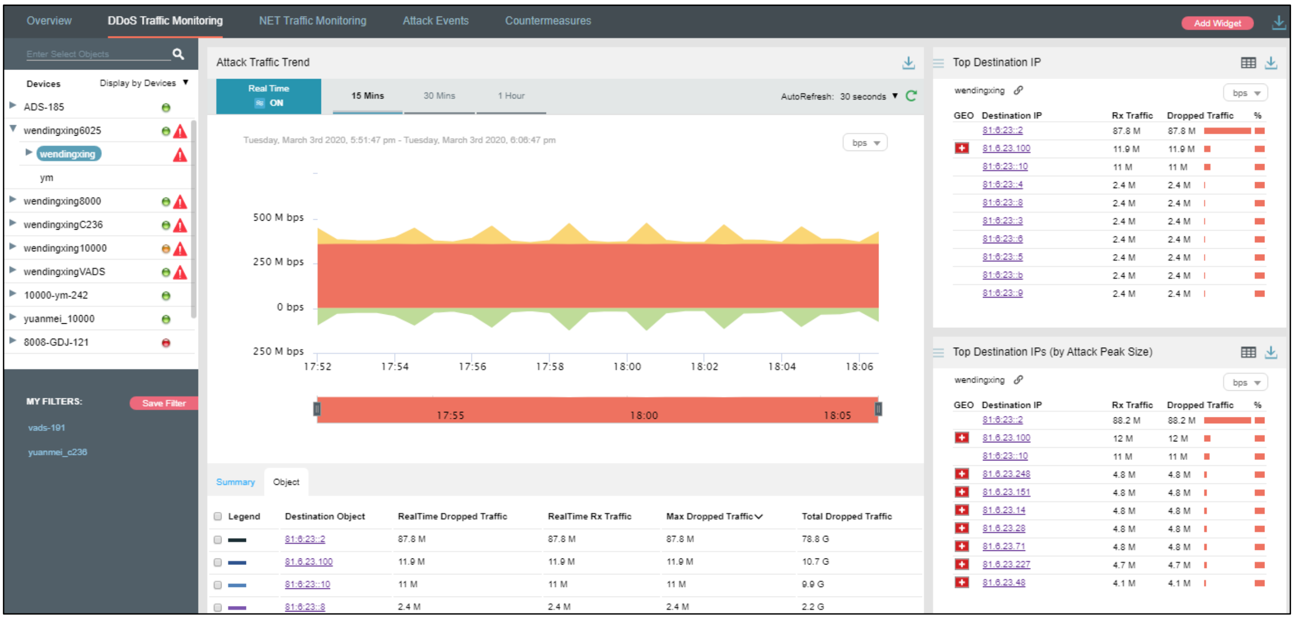
GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:23::8	2.4 M	2.4 M	🟥

GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:23::8	2.4 M	2.4 M	🟥

4.2.3 Viewing Device-Specific Traffic Information

On the page shown in Figure 4-67, you can select **Display by Devices** from the drop-down list in the left pane and then select a device to view real-time attack traffic information of an ADS device, ADS-protected group, and specific IP addresses under a protection group. You can view historical and real-time attack traffic trends and panels of a selected ADS, ADS-protected group, and IP address under a protection group. For example, you can choose **wendingxing6025 > wendingxing** to view traffic information of group **wendingxing** protected by device wendingxing6025.

Figure 4-77 Device-specific traffic information



□ Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
□	81:6:23::2	87.8 M	87.8 M	87.8 M	78.8 G
□	81.6.23.100	11.9 M	11.9 M	11.9 M	10.7 G
□	81:6:23::10	11 M	11 M	11 M	9.9 G
□	81:6:23::8	2.4 M	2.4 M	2.4 M	2.2 G

Top Destination IP

GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:23::2	87.8 M	87.8 M	
🟥	81.6.23.100	11.9 M	11.9 M	
	81:6:23::10	11 M	11 M	
	81:6:23::4	2.4 M	2.4 M	
	81:6:23::8	2.4 M	2.4 M	
	81:6:23::3	2.4 M	2.4 M	
	81:6:23::6	2.4 M	2.4 M	
	81:6:23::5	2.4 M	2.4 M	
	81:6:23::b	2.4 M	2.4 M	
	81:6:23::9	2.4 M	2.4 M	

Top Destination IPs (by Attack Peak Size)

GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:23::2	88.2 M	88.2 M	
🟥	81.6.23.100	12 M	12 M	
	81:6:23::10	11 M	11 M	
🟥	81.6.23.248	4.8 M	4.8 M	
🟥	81.6.23.151	4.8 M	4.8 M	
🟥	81.6.23.14	4.8 M	4.8 M	
🟥	81.6.23.28	4.8 M	4.8 M	
🟥	81.6.23.71	4.8 M	4.8 M	
🟥	81.6.23.227	4.7 M	4.7 M	
🟥	81.6.23.48	4.1 M	4.1 M	

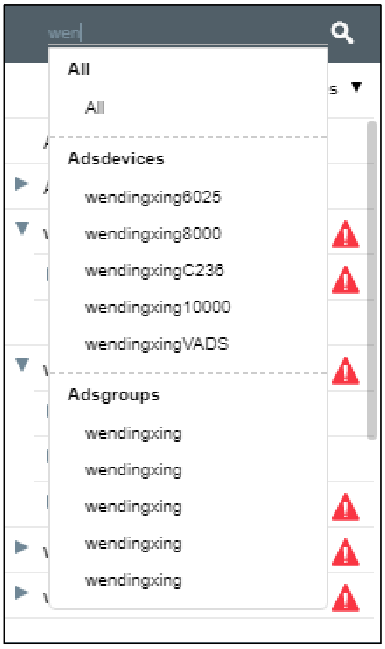
4.2.4 Viewing Object-Specific Traffic Information

By default, the **Attack Traffic Trend** graph displays attack traffic trends of all ADS devices monitored by ADS M. You can view the real-time attack traffic trends of a specified region, region IP group, ADS device, ADS-protected group, or IP address.

Step 1 On the page shown in Figure 4-67, type a character string and then press **Enter**.

The system displays all objects containing the typed character string.

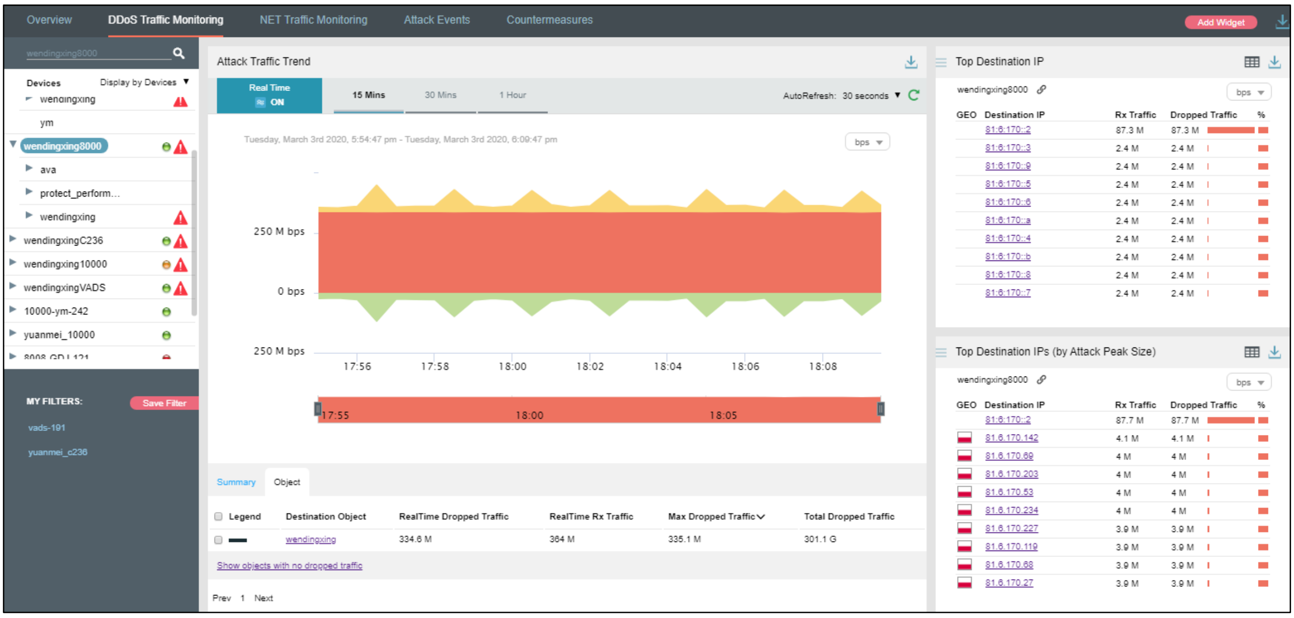
Figure 4-78 Searching for a traffic monitoring object



Step 2 Select an object to be queried, such as **wendingxing8000**, and then press **Enter**.

Traffic information of the selected object is displayed.

Figure 4-79 Traffic information of a specified object



Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
▬	wendingxing	334.6 M	364 M	335.1 M	301.1 G

Top Destination IP

GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:170::2	87.3 M	87.3 M	
	81:6:170::3	2.4 M	2.4 M	
	81:6:170::9	2.4 M	2.4 M	
	81:6:170::5	2.4 M	2.4 M	
	81:6:170::6	2.4 M	2.4 M	
	81:6:170::a	2.4 M	2.4 M	
	81:6:170::4	2.4 M	2.4 M	
	81:6:170::b	2.4 M	2.4 M	
	81:6:170::8	2.4 M	2.4 M	
	81:6:170::7	2.4 M	2.4 M	

Top Destination IPs (by Attack Peak Size)

GEO	Destination IP	Rx Traffic	Dropped Traffic	%
	81:6:170::2	87.7 M	87.7 M	
	81.6.170.142	4.1 M	4.1 M	
	81.6.170.69	4 M	4 M	
	81.6.170.203	4 M	4 M	
	81.6.170.53	4 M	4 M	
	81.6.170.234	4 M	4 M	
	81.6.170.227	3.9 M	3.9 M	
	81.6.170.119	3.9 M	3.9 M	
	81.6.170.68	3.9 M	3.9 M	
	81.6.170.27	3.9 M	3.9 M	

----End

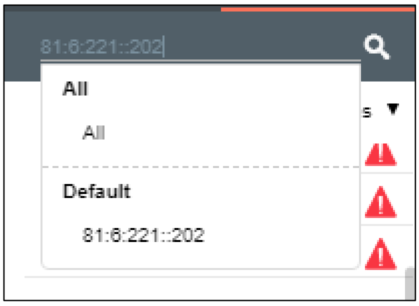
4.2.5 Viewing Traffic Information of an IP Address in the Default Protection Group

IP addresses under the default protection group do not belong to any regions or ADS-protected groups. To view traffic information of such an IP address, you need to expressly indicate the IP address before the system displays such information.

Step 1 On the page shown in Figure 4-67, type an IP address (such as **81:6:221::202**) and then press **Enter**.

The system displays all objects containing this IP address.

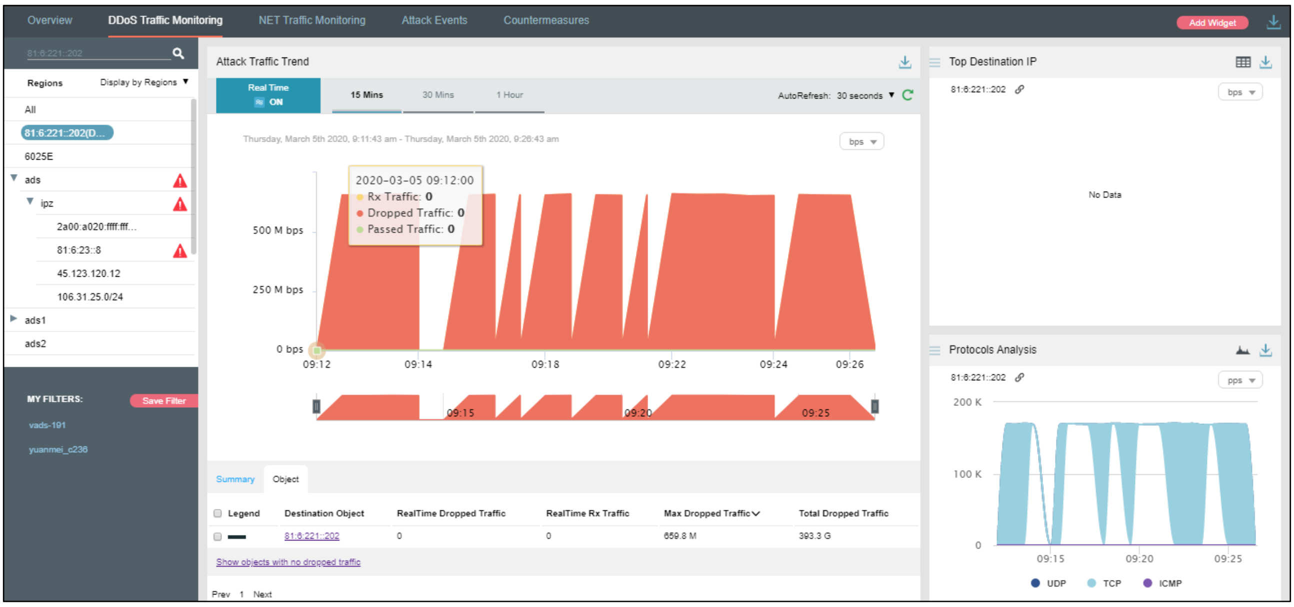
Figure 4-80 Searching for a traffic monitoring object



Step 2 Select the object to be queried and then press **Enter**.

Attack traffic information of this IP address is displayed.

Figure 4-81 Attack traffic information of an IP address in the default protection group



2020-03-05 09:12:00
Rx Traffic: 0
Dropped Traffic: 0
Passed Traffic: 0

□ Legend	Destination Object	RealTime Dropped Traffic	RealTime Rx Traffic	Max Dropped Traffic	Total Dropped Traffic
□ ▬	81:6:221::202	0	0	659.8 M	393.3 G

Show objects with no dropped traffic

----End

4.2.6 Viewing Historical Attack Traffic Trends

To view historical attack traffic trends, follow these steps:

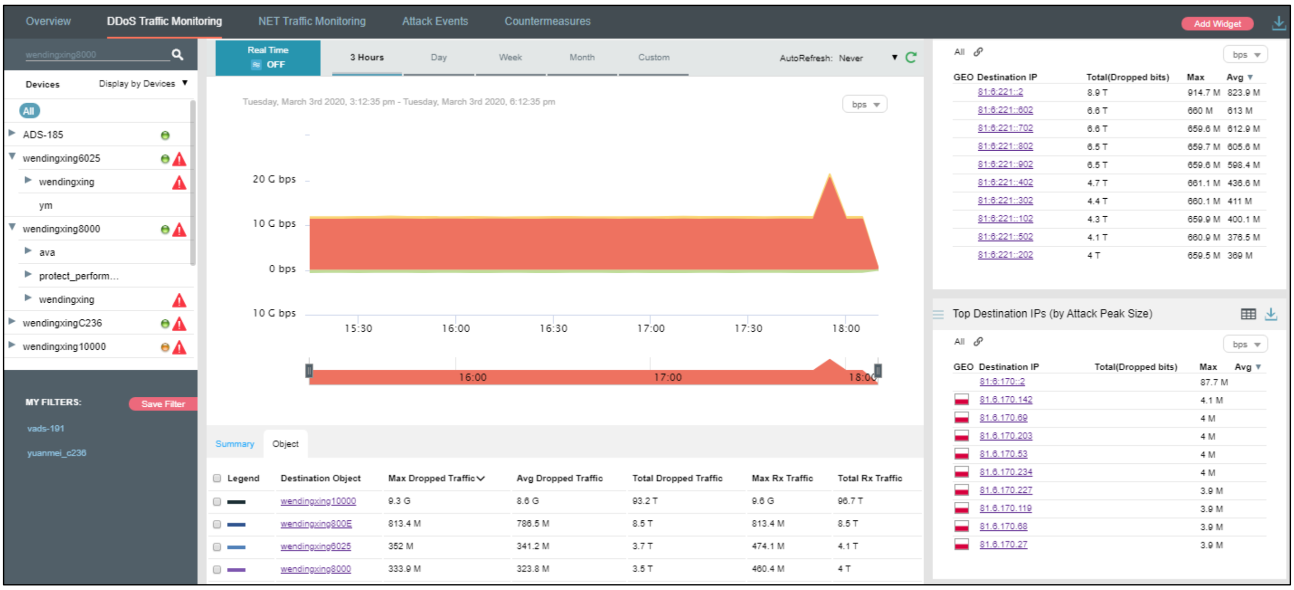
Step 1 On the page shown in Figure 4-67, click **ON** for **Real Time** in the **Attack Traffic Trend** area to disable the real-time mode and enable the historical mode.

Clicking **OFF** for **Real Time** enables the real-time mode again.

In historical mode, attack traffic trend graphs and panels with the icon 🔗 display historical data.

By default, the traffic attack trend graph displays traffic data in the last 3 hours. Clicking **Day**, **Week**, **Month**, or **Custom** displays attack traffic trend graphs in the last day, week, month, or a custom period.

Figure 4-82 Historical attack traffic – objects



Legend	Destination Object	Max Dropped Traffic	Avg Dropped Traffic	Total Dropped Traffic	Max Rx Traffic	Total Rx Traffic
▬	wendingxing10000	9.3 G	8.6 G	93.2 T	9.6 G	96.7 T
▬	wendingxing800E	813.4 M	786.5 M	8.5 T	813.4 M	8.5 T
▬	wendingxing6025	352 M	341.2 M	3.7 T	474.1 M	4.1 T
▬	wendingxing8000	333.9 M	323.8 M	3.5 T	460.4 M	4 T

GEO	Destination IP	Total(Dropped bits)	Max	Avg
	81:6:221::2	8.9 T	914.7 M	823.9 M
	81:6:221::602	6.6 T	660 M	613 M
	81:6:221::702	6.6 T	659.6 M	612.9 M
	81:6:221::802	6.5 T	659.7 M	605.6 M
	81:6:221::902	6.5 T	659.6 M	598.4 M
	81:6:221::402	4.7 T	661.1 M	436.6 M
	81:6:221::302	4.4 T	660.1 M	411 M
	81:6:221::102	4.3 T	659.9 M	400.1 M
	81:6:221::502	4.1 T	660.9 M	376.5 M
	81:6:221::202	4 T	659.5 M	369 M

GEO	Destination IP	Total(Dropped bits)	Max	Avg
	81:6:170::2		87.7 M	
🟥	81.6.170.142		4.1 M	
🟥	81.6.170.69		4 M	
🟥	81.6.170.203		4 M	
🟥	81.6.170.53		4 M	
🟥	81.6.170.234		4 M	
🟥	81.6.170.227		3.9 M	
🟥	81.6.170.119		3.9 M	
🟥	81.6.170.68		3.9 M	
🟥	81.6.170.27		3.9 M	

The object list shows region names and detailed traffic information in descending order of dropped traffic volume.

Table 4-5 Historical attack traffic trend – parameters on the Objects tab page

Parameter	Description
Legend	Shows various shades of blue from dark to light, indicating the total dropped traffic. A darker blue indicates more traffic dropped.
Destination Object	Indicates the traffic monitoring object.
Max Dropped Traffic	Indicates the maximum traffic (in bps or pps) dropped by ADS for the object in the statistical period.
Avg Dropped Traffic	Indicates the average traffic (in bps or pps) dropped by ADS for the object in the statistical period.
Total Dropped Traffic	Indicates the total traffic (in bits) dropped by ADS for the object in the statistical period.

Parameter	Description
Max Rx Traffic	Indicates the maximum traffic (in bps or pps) received by ADS for the object in the statistical period.
Total Rx Traffic	Indicates the total traffic (in bits) received by ADS for the object in the statistical period.

Step 2 On the page shown in Figure 4-82, click **Summary**.

The summary of the historical attack traffic trend graph is displayed, including the average and total dropped, forwarded, and received traffic in the statistical period.

Clicking the bar or text in the **Legend** column hides or displays this type of traffic in the attack traffic trend graph. By default, all types of traffic are displayed. A dimmed color indicates that this type of traffic is not displayed. Otherwise, the traffic is displayed.

----End

4.2.7 Switching the Traffic Unit

By default, traffic is expressed in bps in the attack traffic trend graph. On the page shown in Figure 4-67, you can select **pps** from the drop-down list in the upper-right corner of the **Attack Traffic Trend** panel to display traffic data in pps.

4.2.8 Refreshing the Attack Traffic Trend Graph

By default, the attack traffic trend graph automatically refreshes every 30 seconds in real time mode. On the page shown in Figure 4-67, you can select **Never** from the **AutoRefresh** drop-down list in the upper-right corner of the **Attack Traffic Trend** panel. In this case, the attack traffic trend graph can be refreshed only by clicking ↻.

By default, the attack traffic trend graph does not automatically refresh in historical mode. On the page shown in Figure 4-67, you can select **Every 5 min** from the **AutoRefresh** drop-down list in the upper-right corner of the **Attack Traffic Trend** panel. In this case, the attack traffic trend graph will refresh every 5 minutes.

4.2.9 Downloading a Traffic Trend Report

On the page shown in Figure 4-67, you can click ⤓ in the upper-right corner and then click HTML or PDF to export the current data of the attack traffic trend graph as an HTML or PDF report. For details, see 4.1.4 Downloading a Report.

4.2.10 Managing Filters

Filters are provided for users to define objects of their concern, so that they can find monitored objects more conveniently. After being created, filters are displayed in the filter list. You can click a filter to view traffic information of the object specified by the filter.

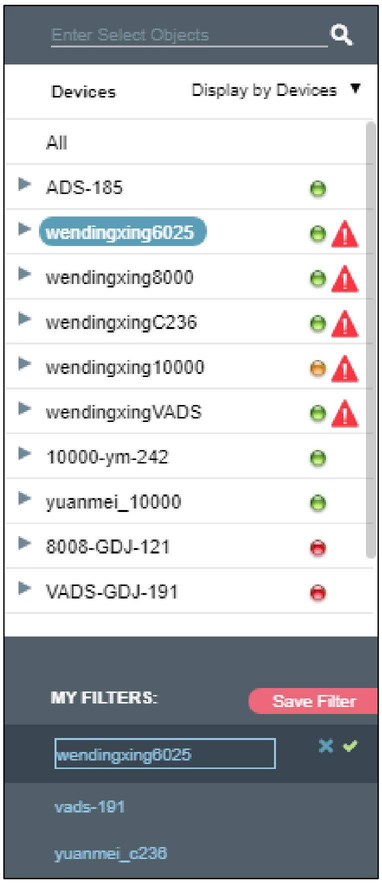
Any queried objects, such as a region, region IP group, ADS device, ADS-protected group, or IP address can be configured as a filter. But **All** and **Default** cannot be configured as a filter. You can configure multiple filters.

4.2.10.1 Configuring a Filter

To configure a filter, follow these steps:

Step 1 On the page shown in Figure 4-67, select an object from the left pane, such as **wendingxing6025**, and then click **Save Filter**.

Figure 4-83 Adding a filter



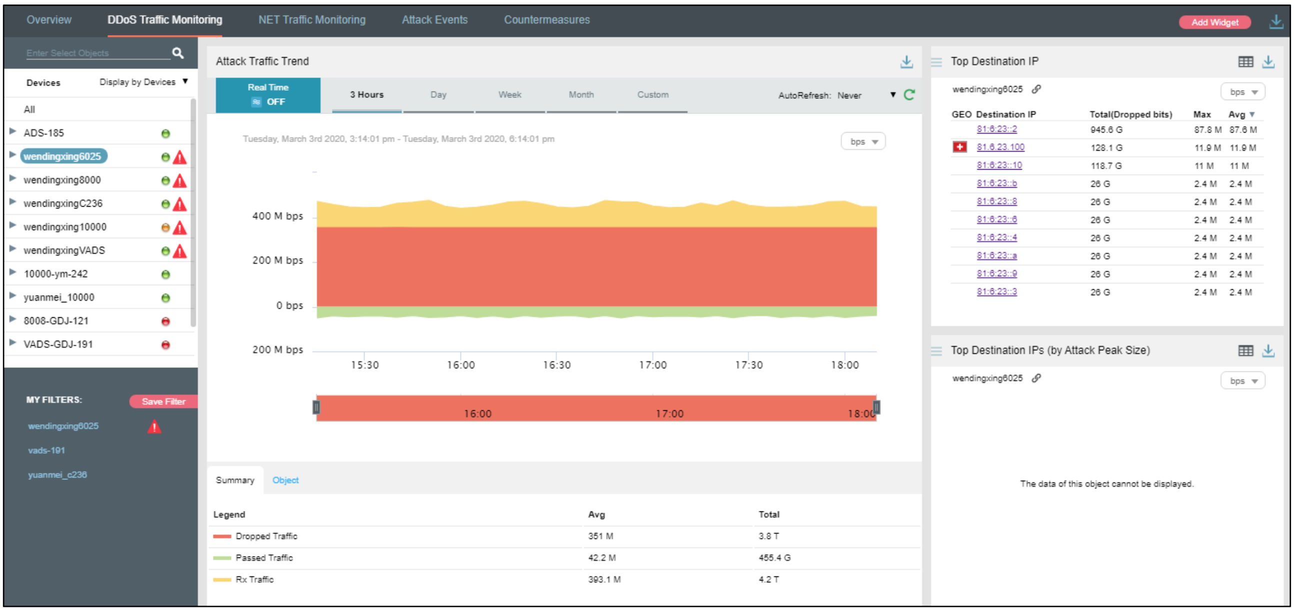
Step 2 Type the filter name.

By default, the object name is displayed as the filter name. You can use the default name or type a new one.

Step 3 Click ✓ and click **Confirm** in the dialog box that appears.

Step 4 Click **wendingxing6025** in the filter list to view its traffic information.

Figure 4-84 Viewing a filter



AutoRefresh: Never

Tuesday, March 3rd 2020, 3:14:01 pm - Tuesday, March 3rd 2020, 6:14:01 pm

Legend	Avg	Total
🟥 Dropped Traffic	351 M	3.8 T
🟩 Passed Traffic	42.2 M	455.4 G
🟨 Rx Traffic	393.1 M	4.2 T

wendingxing6025

GEO	Destination IP	Total(Dropped bits)	Max	Avg
	81:6:23::2	945.6 G	87.8 M	87.6 M
🇨🇭	81.6.23.100	128.1 G	11.9 M	11.9 M
	81:6:23::10	118.7 G	11 M	11 M
	81:6:23::b	26 G	2.4 M	2.4 M
	81:6:23::8	26 G	2.4 M	2.4 M
	81:6:23::6	26 G	2.4 M	2.4 M
	81:6:23::4	26 G	2.4 M	2.4 M
	81:6:23::a	26 G	2.4 M	2.4 M
	81:6:23::9	26 G	2.4 M	2.4 M
	81:6:23::3	26 G	2.4 M	2.4 M

The data of this object cannot be displayed.

----End

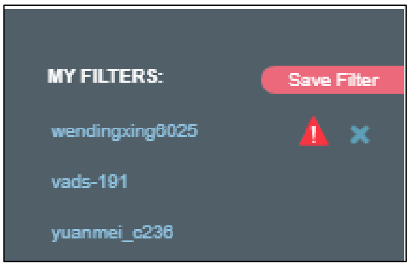
4.2.10.2 Deleting a Filter

To delete a filter, follow these steps:

Step 1 On the page shown in Figure 4-84, point to a filter name

The icon ✖ appears.

Figure 4-85 Deleting a filter



Step 2 Click ✖ and then **Confirm** in the dialog box that appears.

----End

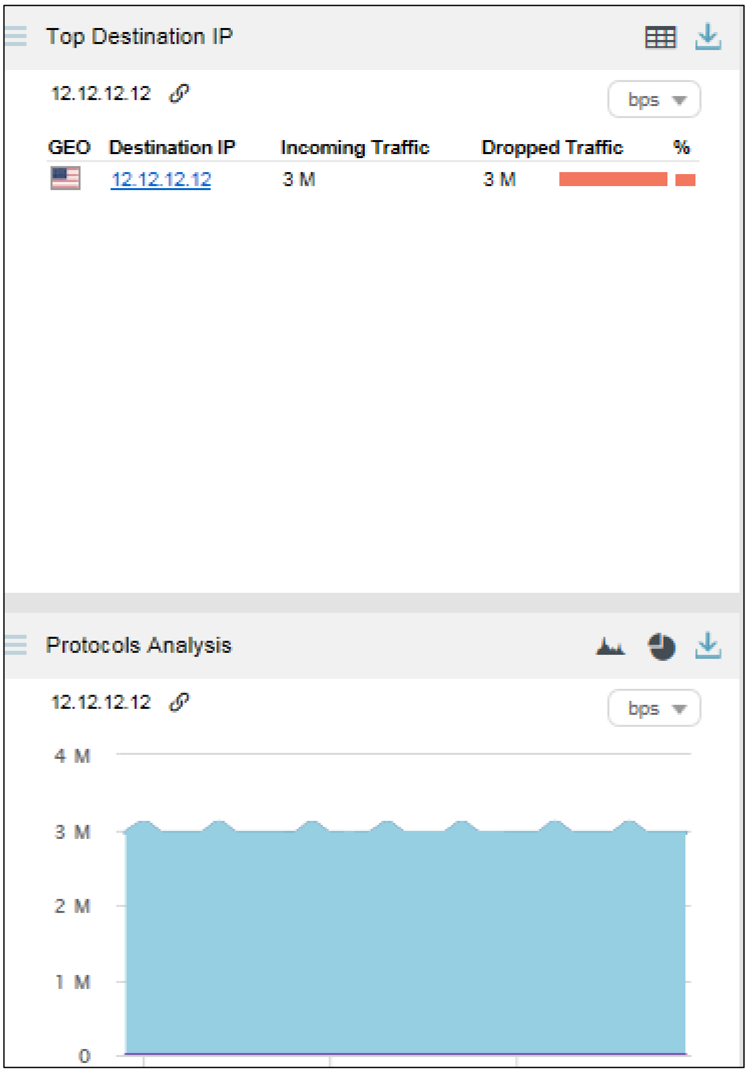
4.2.11 Managing Panels

By default, **Top Destination IP** and **Protocols Analysis** panels are displayed under **Traffic Monitoring > DDoS Traffic Monitoring**, as shown in Figure 4-86.

A panel with the icon 🔗 indicates that when the selected object and statistical period change, the object and statistical period of this panel will change accordingly. A panel without the icon 🔗 indicates the opposite.

You can add panels as required. For how to add, edit, and delete panels, see section 4.1 Overview.

Figure 4-86 Default panels on the DDOS Attack Traffic Monitoring page



Top Destination IP

12.12.12.12 🔗

GEO	Destination IP	Incoming Traffic	Dropped Traffic	%
🇺🇸	12.12.12.12	3 M	3 M	🟥

Protocols Analysis

12.12.12.12 🔗

4.3 Network Traffic Monitoring

Note	ADS M presents network traffic based on data uploaded by NTA devices.

Under **Traffic Monitoring > NET Traffic Monitoring**, you can do as follows:

- View real-time and historical network traffic trends of all objects or a specified region, regional IP group, NTA device, or IP address.
- View or add panels.
- Configure filters.

IP addresses under the default protection group do not belong to any regions or IP groups. To view network traffic information of such an IP address, you need to expressly specify the IP address before the system displays its information.

Network traffic information includes real-time traffic information and historical traffic information. By default, network traffic information is displayed by region.

4.3.1 Viewing Real-Time Network Traffic Information

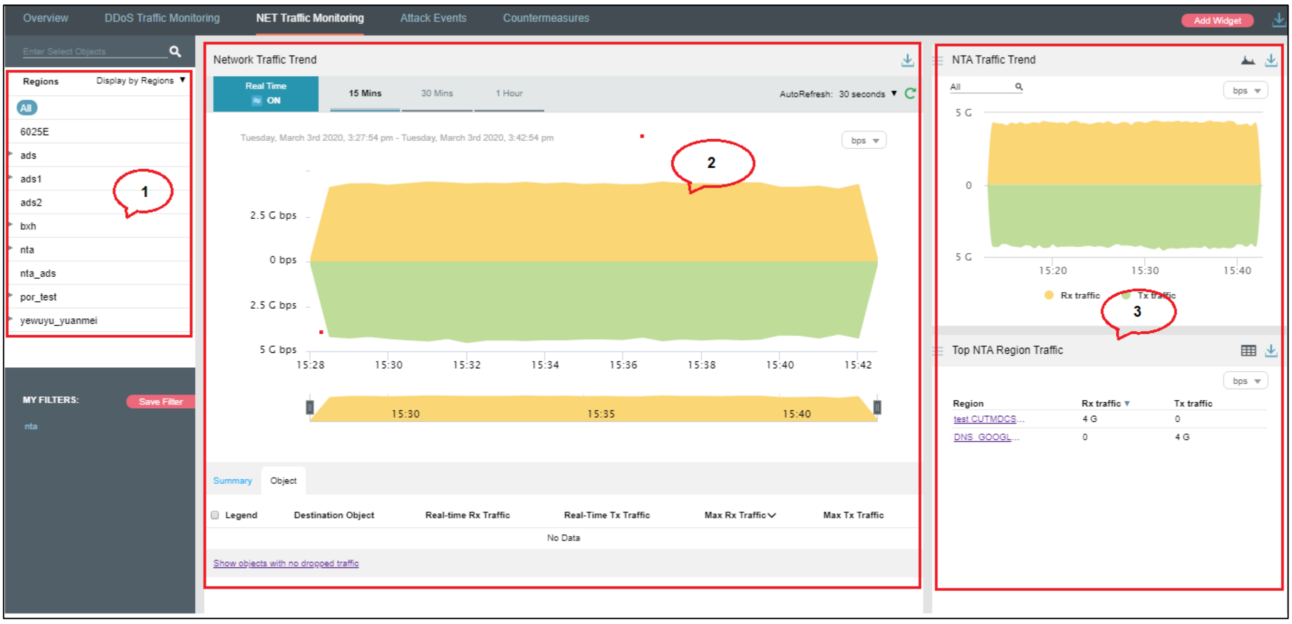
To view real-time network traffic information, follow these steps:

Step 1 Choose **Traffic Monitoring > NET Traffic Monitoring**.

By default, real-time network traffic information of all monitoring objects is displayed, including **Network Traffic Trend**, **NTA Traffic Trend**, and **Top NTA Region Traffic** panels, as shown in Figure 4-87.

In real-time mode, the network traffic trend in the last 15 minutes is displayed by default. You can click **30 Mins** or **1 Hour** to view the network traffic trend of the last 30 minutes or last hour.

Figure 4-87 Network traffic information of all objects



□ Legend	Destination Object	Real-time Rx Traffic	Real-Time Tx Traffic	Max Rx Traffic	Max Tx Traffic
No Data					

Region	Rx traffic	Tx traffic
test CUTMDCS...	4 G	0
DNS_GOOGL...	0	4 G

Table 4-6 describes areas of the **DDoS Traffic Monitoring** page.

Table 4-6 Layout for the DDoS Traffic Monitoring page

No.	Description
1	List of objects
2	Traffic trend
3	Panels

On the **NET Traffic Monitoring** page, the **Object** list ranks regions in descending order of real-time network traffic detected.

Table 4-7 Real-time network traffic trend – parameters on the Objects tab page

Parameter	Description
Legend	Shows various shades of blue from dark to light, indicating the total dropped traffic. A darker blue indicates more traffic dropped.
Destination Object	Indicates the traffic monitoring object.
Real-Time Rx Traffic	Indicates traffic (in bps or pps) received by the object in real time.
Real-Time Tx Traffic	Indicates traffic (in bps or pps) transmitted by the object in real time.
Max Rx Traffic	Indicates the maximum traffic (in bps or pps) received by the object in the statistical period.
Max Tx Traffic	Indicates the maximum traffic (in bps or pps) transmitted by the object in the statistical period.

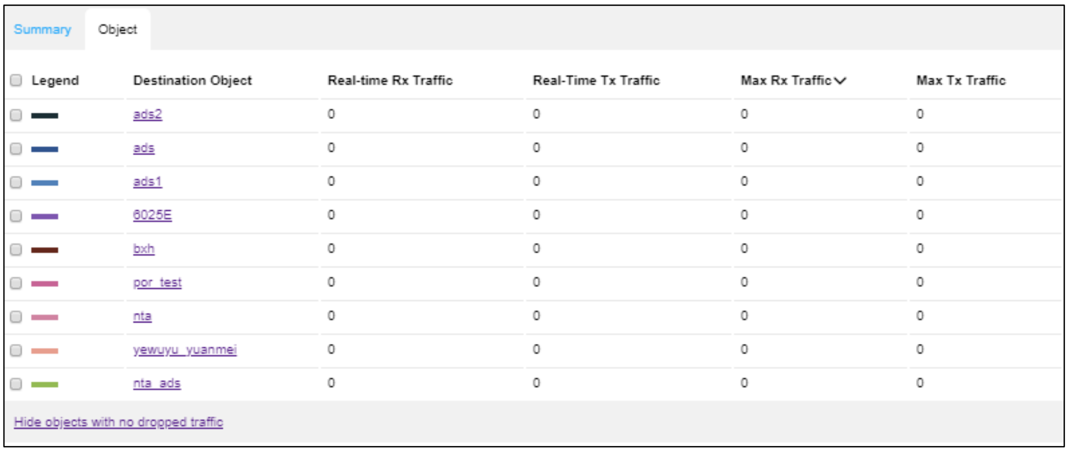
Step 2 On the **Object** tab page shown in Figure 4-87, select one or more objects to view its or their real-time network traffic.

By default, only the objects with traffic dropped by ADS are displayed.

Step 3 Click **Show objects with no dropped traffic** to show all objects. See Figure 4-88.

Clicking **Hide objects with no dropped traffic** displays only objects with traffic dropped by ADS, but hides objects with no traffic dropped.

Figure 4-88 Real-time network traffic trend graph of all objects



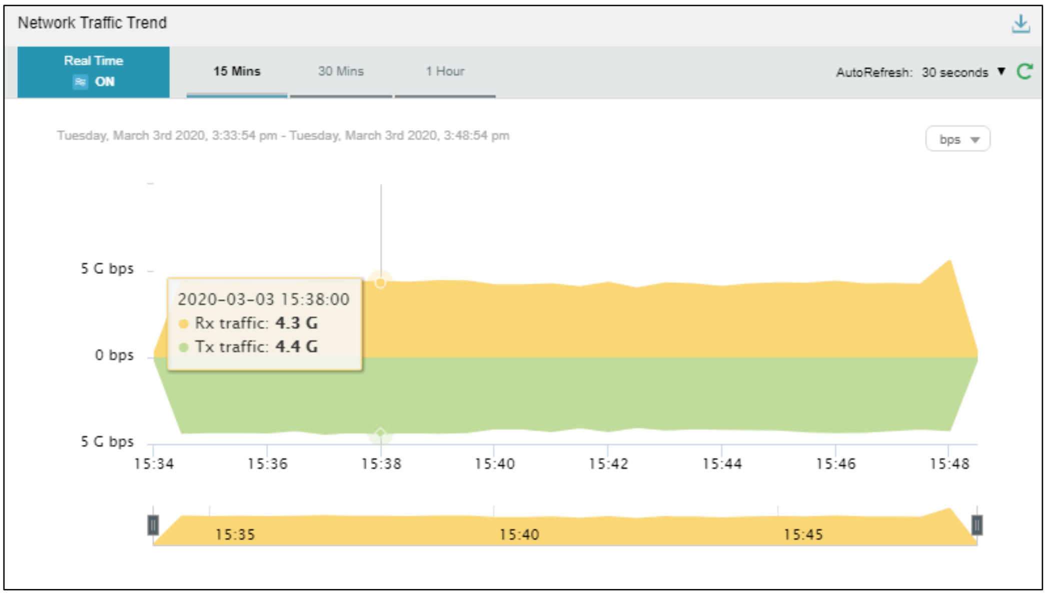
Summary | Object

□ Legend	Destination Object	Real-time Rx Traffic	Real-Time Tx Traffic	Max Rx Traffic	Max Tx Traffic
□ ▬	ads2	0	0	0	0
□ ▬	ads	0	0	0	0
□ ▬	ads1	0	0	0	0
□ ▬	6025E	0	0	0	0
□ ▬	bxh	0	0	0	0
□ ▬	por_test	0	0	0	0
□ ▬	nta	0	0	0	0
□ ▬	yewuyu_yuanmei	0	0	0	0
□ ▬	nta_ads	0	0	0	0

Hide objects with no dropped traffic

Step 4 Point to a random point in the network traffic trend graph to view the incoming traffic, outgoing traffic, and dropped traffic at the specific point of time, as well as real-time traffic dropped for the specified object. See Figure 4-89.

Figure 4-89 Network traffic information at a specific time



Network Traffic Trend

Real Time ON | 15 Mins | 30 Mins | 1 Hour

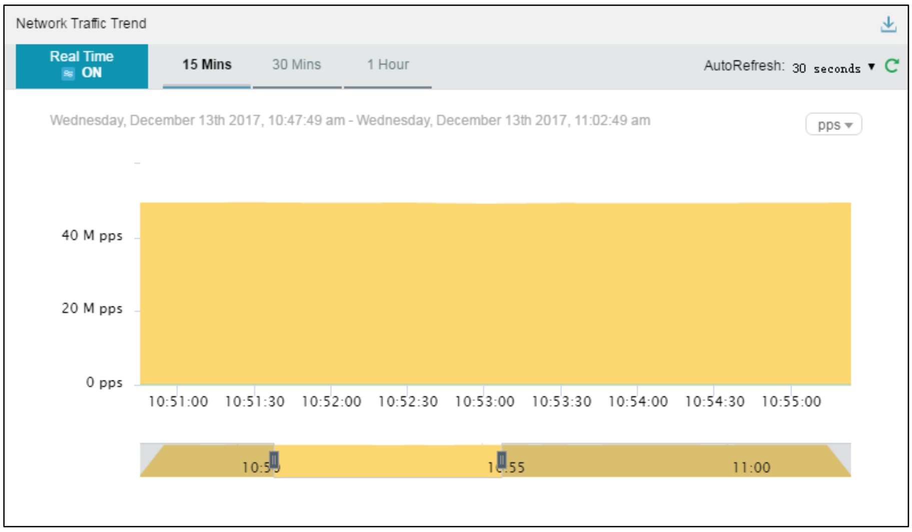
AutoRefresh: 30 seconds

Tuesday, March 3rd 2020, 3:33:54 pm - Tuesday, March 3rd 2020, 3:48:54 pm

2020-03-03 15:38:00
● Rx traffic: **4.3 G**
● Tx traffic: **4.4 G**

Step 5 Below the network traffic trend graph, drag ▯ to view a finer-granularity network traffic trend.

Figure 4-90 Finer-granularity network traffic information



AutoRefresh: 30 seconds

Wednesday, December 13th 2017, 10:47:49 am - Wednesday, December 13th 2017, 11:02:49 am

Step 6 On the page shown in Figure 4-88, click **Summary**.

The average and total traffic received and transmitted in the statistical period are displayed.

Clicking the bar or text in the **Legend** column hides or displays this type of traffic in the traffic trend graph. By default, all types of traffic are displayed. A dimmed color indicates that this type of traffic is not displayed. Otherwise, the traffic is displayed.

Table 4-8 describes parameters on the **Summary** tab page.

Table 4-8 Real-time network traffic trend – parameters on the Summary tab page

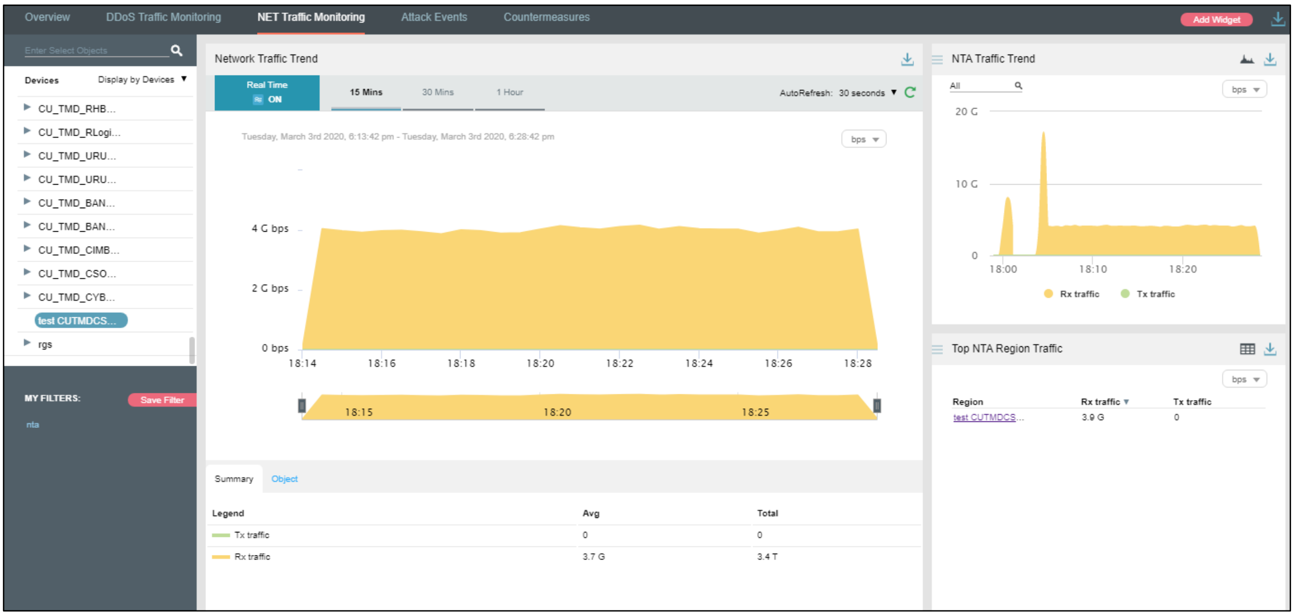
Parameter	Description
Legend	Colors representing transmitted and received traffic
Avg	Average traffic transmitted and received by the object
Total	Total traffic transmitted and received by the object

----End

4.3.2 Viewing Device-Specific Network Traffic Information

In the left pane of the **NET Traffic Monitoring** page, select **Display by Devices**. Then all NTA devices and regions and regional IP groups configured on these devices are listed. 🟠 indicates that time of this device is not synchronized. 🔴 indicates that this device is offline. 🟢 indicates that this device is online. You can select an NTA device or a region/regional IP group under an NTA device to view its real-time and historical network traffic trends and panels. For example, select **10.66.243.171 > test CUTMDCS**…. Then network traffic information of region "test CUTMDCS…" under device 10.66.241.171 is displayed, as shown in Figure 4-91.

Figure 4-91 Device-specific network traffic information



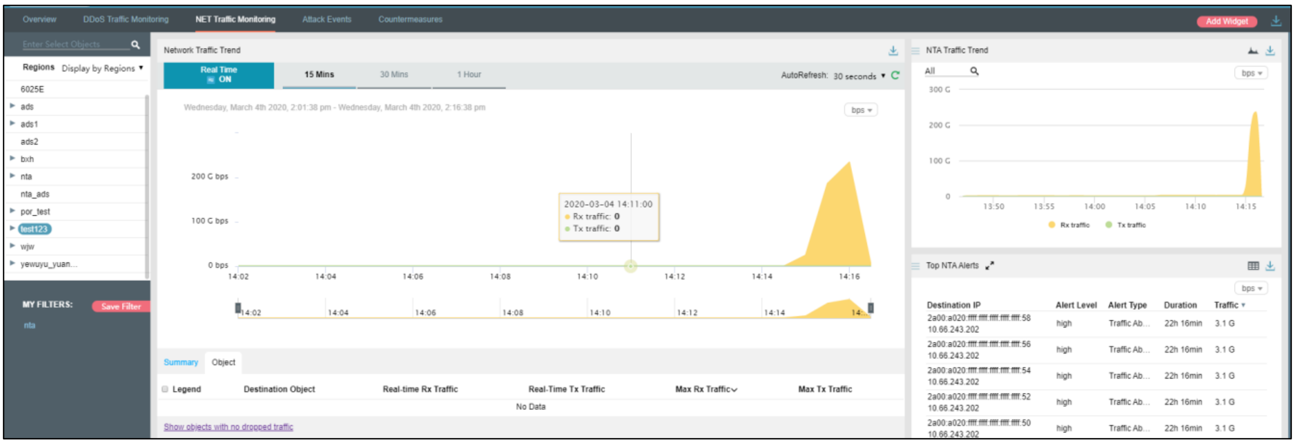
Legend	Avg	Total
Tx traffic	0	0
Rx traffic	3.7 G	3.4 T

Region	Rx traffic	Tx traffic
test CUTMDCS...	3.9 G	0

4.3.3 Viewing Region-Specific Network Traffic Information

In the left pane of the **NET Traffic Monitoring** page, select **Display by Regions**. Then all regions and IP groups and IP addresses in these regions are displayed. You can select a region, an IP group, or an IP address to view its real-time and historical network traffic trends and panels. For example, select **test123**. Then network traffic information of region test123 is displayed, as shown in Figure 4-92.

Figure 4-92 Region-specific network traffic information



Legend	Destination Object	Real-time Rx Traffic	Real-Time Tx Traffic	Max Rx Traffic	Max Tx Traffic
No Data					

Destination IP	Alert Level	Alert Type	Duration	Traffic
2a00:a020:ffff:ffff:ffff:ffff:ffff:58 10.66.243.202	high	Traffic Ab...	22h 16min	3.1 G
2a00:a020:ffff:ffff:ffff:ffff:ffff:56 10.66.243.202	high	Traffic Ab...	22h 16min	3.1 G
2a00:a020:ffff:ffff:ffff:ffff:ffff:54 10.66.243.202	high	Traffic Ab...	22h 16min	3.1 G
2a00:a020:ffff:ffff:ffff:ffff:ffff:52 10.66.243.202	high	Traffic Ab...	22h 16min	3.1 G
2a00:a020:ffff:ffff:ffff:ffff:ffff:50 10.66.243.202	high	Traffic Ab...	22h 16min	3.1 G

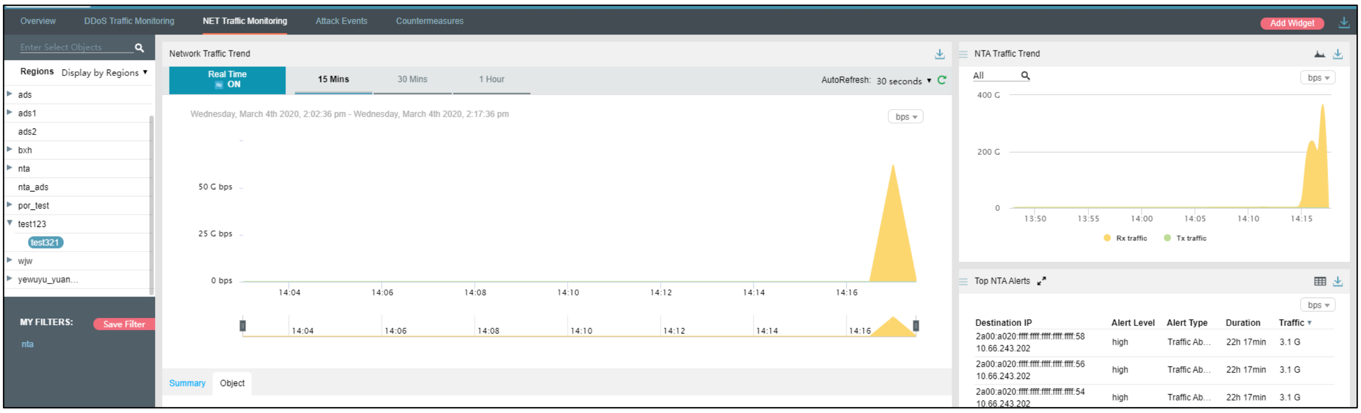
4.3.4 Viewing IP Group-Specific Network Traffic Information

Step 1 In the left pane of the **NET Traffic Monitoring** page, select **Display by Devices**.

Step 2 From the device list displayed, select an IP group under an NTA device.

Then real-time network traffic information of this IP group is displayed, as shown in Figure 4-93.

Figure 4-93 IP group-specific network traffic information



Wednesday, March 4th 2020, 2:02:36 pm - Wednesday, March 4th 2020, 2:17:36 pm

Destination IP	Alert Level	Alert Type	Duration	Traffic
2a00:a020:ffff:ffff:ffff:ffff:ffff:58 10.66.243.202	high	Traffic Ab...	22h 17min	3.1 G
2a00:a020:ffff:ffff:ffff:ffff:ffff:56 10.66.243.202	high	Traffic Ab...	22h 17min	3.1 G
2a00:a020:ffff:ffff:ffff:ffff:ffff:54 10.66.243.202	high	Traffic Ab...	22h 17min	3.1 G

----End

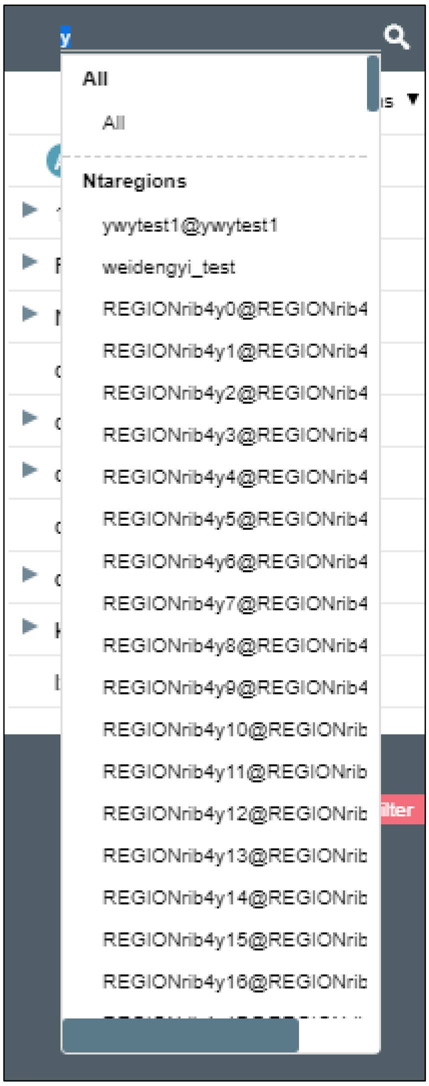
4.3.5 Viewing Object-Specific Network Traffic Information

By default, the **Attack Traffic Trend** graph displays network traffic trends of all NTA devices monitored by ADS M. You can specify an object, namely a region, regional IP group, or NTA device, to view its real-time network traffic trends.

Step 1 In the left pane, type a character string and then press **Enter**.

The system displays all objects containing the typed character string, as shown in Figure 4-94.

Figure 4-94 Searching for a network traffic monitoring object



All

All

Ntaregions

ywytest1@ywytest1

weidengyi_test

REGIONrib4y0@REGIONrib4

REGIONrib4y1@REGIONrib4

REGIONrib4y2@REGIONrib4

REGIONrib4y3@REGIONrib4

REGIONrib4y4@REGIONrib4

REGIONrib4y5@REGIONrib4

REGIONrib4y6@REGIONrib4

REGIONrib4y7@REGIONrib4

REGIONrib4y8@REGIONrib4

REGIONrib4y9@REGIONrib4

REGIONrib4y10@REGIONrib

REGIONrib4y11@REGIONrib

REGIONrib4y12@REGIONrib

REGIONrib4y13@REGIONrib

REGIONrib4y14@REGIONrib

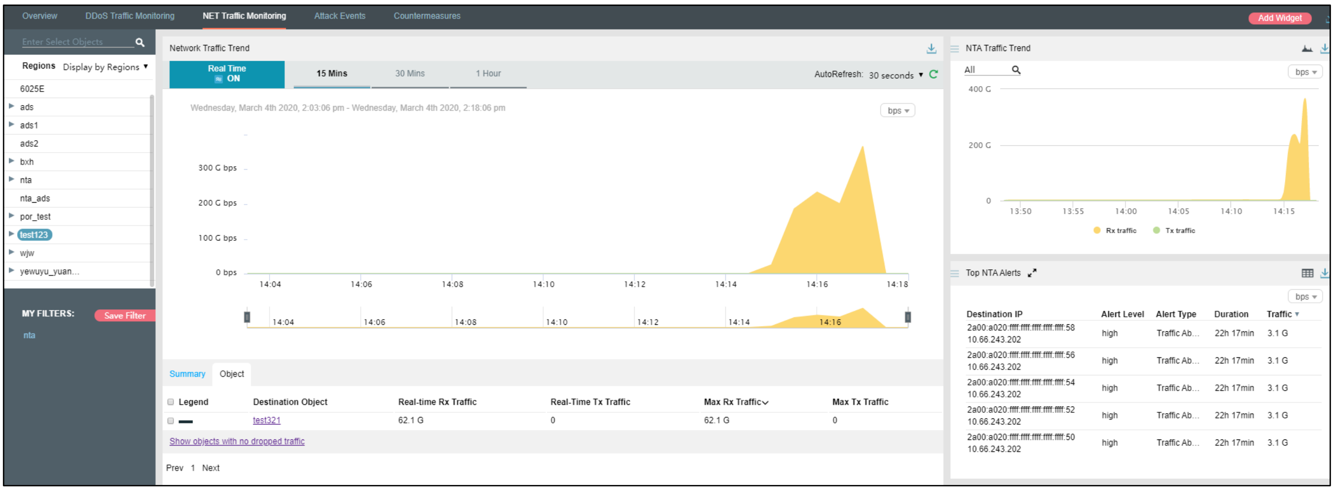
REGIONrib4y15@REGIONrib

REGIONrib4y16@REGIONrib

Step 2 Select an object to be queried, such as **test123**, and then press **Enter**.

Network traffic information of the selected object is displayed, as shown in Figure 4-95.

Figure 4-95 Object-specific network traffic information



□ Legend	Destination Object	Real-time Rx Traffic	Real-Time Tx Traffic	Max Rx Traffic	Max Tx Traffic
□ ▬	test321	62.1 G	0	62.1 G	0

Destination IP	Alert Level	Alert Type	Duration	Traffic
2a00:a020:ffff:ffff:ffff:ffff:ffff:58 10.66.243.202	high	Traffic Ab...	22h 17min	3.1 G
2a00:a020:ffff:ffff:ffff:ffff:ffff:56 10.66.243.202	high	Traffic Ab...	22h 17min	3.1 G
2a00:a020:ffff:ffff:ffff:ffff:ffff:54 10.66.243.202	high	Traffic Ab...	22h 17min	3.1 G
2a00:a020:ffff:ffff:ffff:ffff:ffff:52 10.66.243.202	high	Traffic Ab...	22h 17min	3.1 G
2a00:a020:ffff:ffff:ffff:ffff:ffff:50 10.66.243.202	high	Traffic Ab...	22h 17min	3.1 G

----End

4.3.6 Viewing Historical Network Traffic Trends

To view historical network traffic trends, follow these steps:

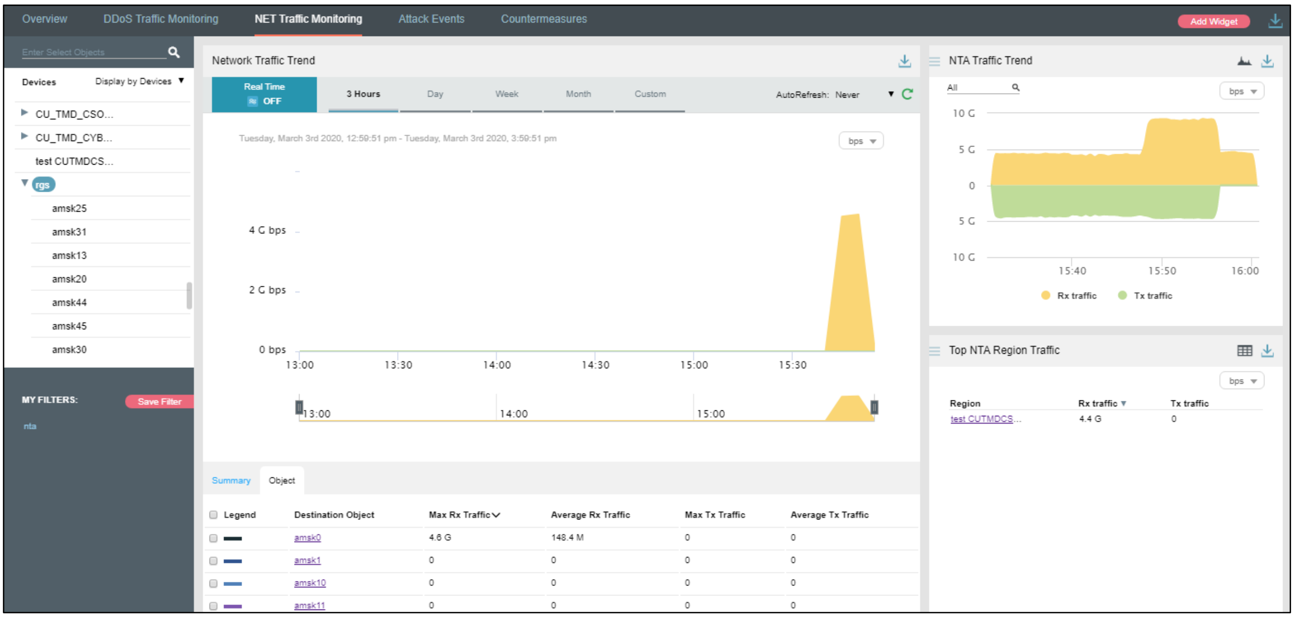
Step 1 On the **NET Traffic Monitoring** page, click **ON** for **Real Time** in the **Network Traffic Trend** area to disable the real-time mode and enable the historical mode. See Figure 4-96.

Clicking **OFF** for **Real Time** enables the real-time mode again.

In historical mode, both the network traffic trend graph and panels with the icon 🔗 display historical data.

By default, the network traffic trend graph displays network traffic data in the last 3 hours. Clicking **Day**, **Week**, **Month**, or **Custom** displays the network traffic trend in the last day, week, month, or a custom period.

Figure 4-96 Historical network traffic – objects



□ Legend	Destination Object	Max Rx Traffic	Average Rx Traffic	Max Tx Traffic	Average Tx Traffic
□ ▬	amsk0	4.6 G	148.4 M	0	0
□ ▬	amsk1	0	0	0	0
□ ▬	amsk10	0	0	0	0
□ ▬	amsk11	0	0	0	0

Region	Rx traffic	Tx traffic
test CUTMDCS...	4.4 G	0

The **Object** tab page provides detailed network traffic information of regions, which are ranked in descending order of traffic volume.

Table 4-9 Historical network traffic trend – parameters on the Objects tab page

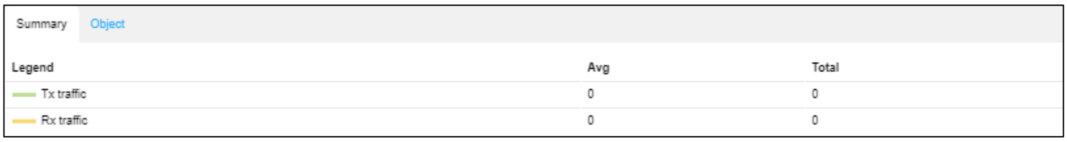
Parameter	Description
Legend	Shows various shades of blue from dark to light, indicating the total dropped traffic. A darker blue indicates more traffic dropped.
Destination Object	Indicates the traffic monitoring object.
Max Rx Traffic	Indicates the maximum traffic (in bps or pps) received by the object in the statistical period.
Average Rx Traffic	Indicates the average traffic (in bps or pps) received by the object in the statistical period.
Max Tx Traffic	Indicates the maximum traffic (in bps or pps) transmitted by the object in the statistical period.
Average Tx Traffic	Indicates the average traffic (in bps or pps) transmitted by the object in the statistical period.

Step 2 On the page shown in Figure 4-96, click **Summary**.

The average and total traffic received and transmitted in the statistical period are displayed, as shown in Figure 4-97.

Clicking the bar or text in the **Legend** column hides or displays this type of traffic in the network traffic trend graph. By default, all types of network traffic are displayed. A dimmed color indicates that this type of traffic is not displayed. Otherwise, the traffic is displayed. Table 4-8 describes parameters on the **Summary** tab page.

Figure 4-97 Historical network traffic – summary



Summary Object

Legend	Avg	Total
Tx traffic	0	0
Rx traffic	0	0

----End

4.3.7 Switching the Traffic Unit

By default, traffic is expressed in bps in network traffic trend graphs. You can select **pps** from the drop-down list in the upper-right corner of the **Network Traffic Trend** area to display traffic in pps.

4.3.8 Refreshing the Traffic Trend Graph

By default, the network traffic trend graph automatically refreshes every 30 seconds in real-time mode. On the **NET Traffic Monitoring** page, you can select **Never** from the **AutoRefresh** drop-down list in the upper-right corner of the **Network Traffic Trend** panel. In this case, the network traffic trend graph does not refresh unless you click ⟳.

By default, the network traffic trend graph is not refreshed in historical mode. On the **NET Traffic Monitoring** page, you can select **Every 5 min** from the **AutoRefresh** drop-down list in the upper-right corner of the **Network Traffic Trend** panel. In this case, the network traffic trend graph will automatically refresh every 5 minutes.

4.3.9 Downloading a Traffic Trend Report

On the **NET Traffic Monitoring** page, you can click ⤓ in the upper-right corner of the **Network Traffic Trend** graph and then click HTML or PDF to download the current data of the network traffic trend graph as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.3.10 Managing Filters

Filters are provided for users to define objects of their concern, so that they can find monitored objects more conveniently. After being created, filters are displayed in the filter list. You can click a filter to view traffic information of the object specified by the filter.

Any queried object, such as a region, regional IP group, or NTA device, can be configured as a filter. But **All** and **Default** cannot be configured as a filter. You can configure multiple filters.

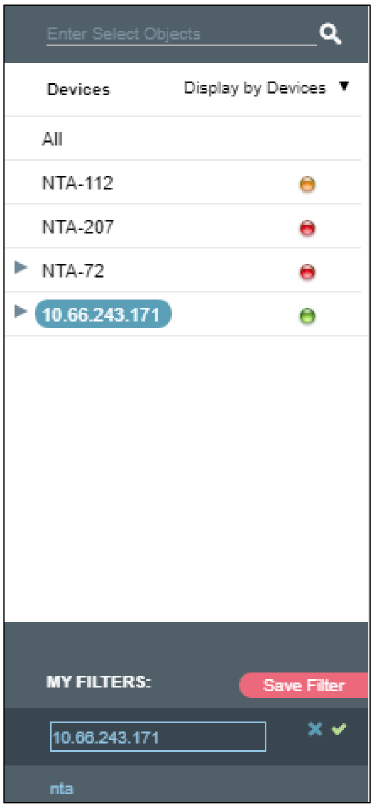
4.3.10.1 Configuring a Filter

To configure a filter, follow these steps:

Step 1 On the **NET Traffic Monitoring** page, select an object from the left pane, such as **10.66.243.171**, and then click **Save Filter**.

Then **10.66.243.171** appears in the filter list, as shown in Figure 4-98.

Figure 4-98 Creating a filter



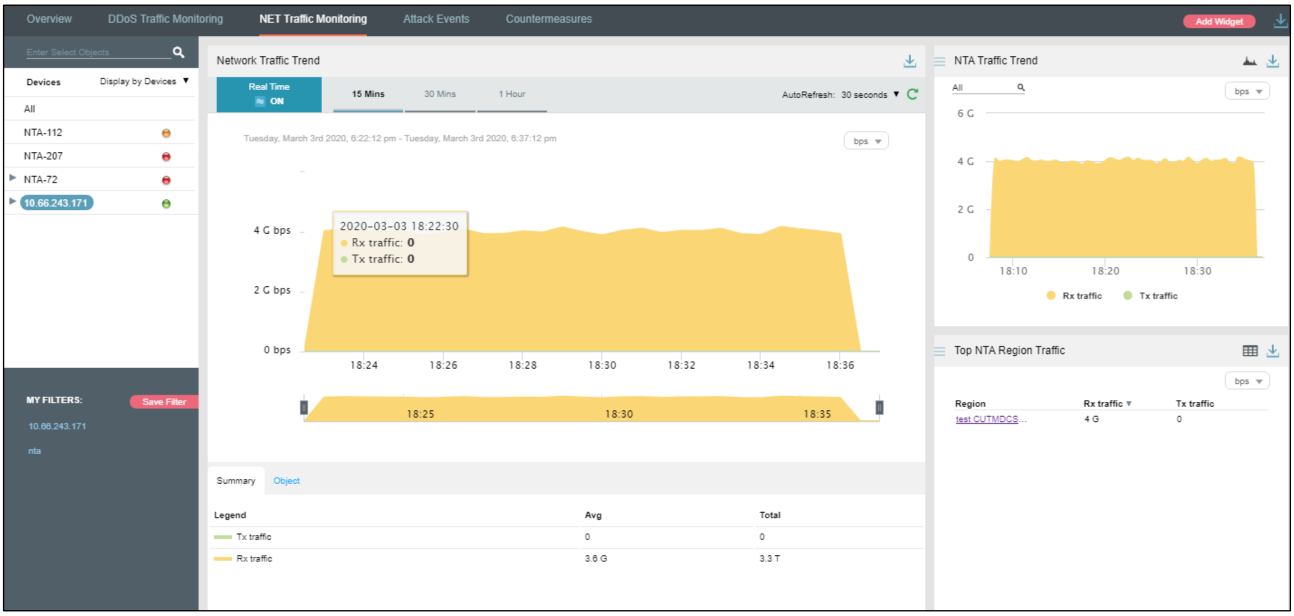
Step 2 Type the filter name.

By default, the object name is displayed as the filter name. You can use the default name or type a new one.

Step 3 Click ✓ and click **Confirm** in the dialog box that appears.

Step 4 Click **10.66.243.171** in the filter list to view its traffic information. See Figure 4-99.

Figure 4-99 Filtered network traffic information



Legend	Avg	Total
Tx traffic	0	0
Rx traffic	3.6 G	3.3 T

Region	Rx traffic	Tx traffic
test CUTMDCS...	4 G	0

----End

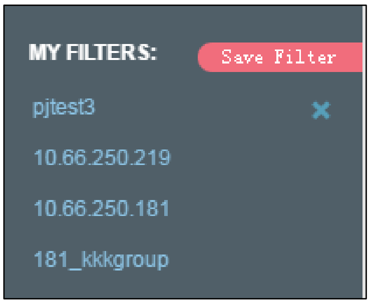
4.3.10.2 Deleting a Filter

To delete a filter, follow these steps:

Step 1 On the page shown in Figure 4-99, point to a filter name.

The icon ✖ appears, as shown in Figure 4-100.

Figure 4-100 Deleting a filter



Step 2 Click ✖ and then **Confirm** in the dialog box that appears.

----End

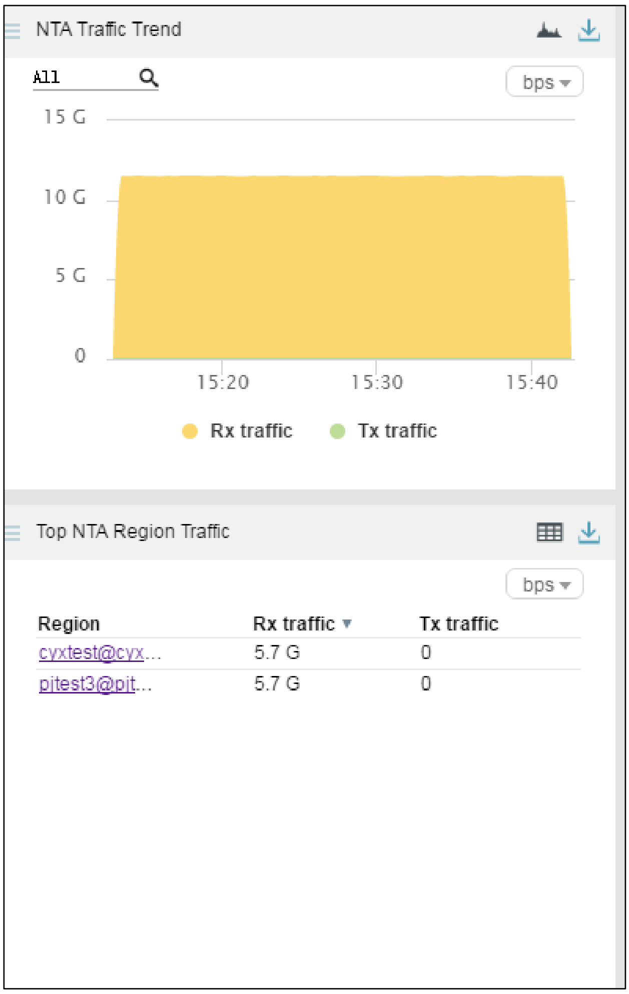
4.3.11 Managing Panels

On the **NET Traffic Monitoring** page, **NTA Traffic Trend** and **Top NTA Region Traffic** panels are displayed by default, as shown in Figure 4-101.

A panel with the icon 🔗 indicates that when the selected object and statistical period change, the object and statistical period of this panel will change accordingly. A panel without the icon 🔗 indicates the opposite.

You can add panels as required. For details about how to add, edit, and delete a panel, see section 4.1 Overview.

Figure 4-101 Default panels displayed on the NET Traffic Monitoring page



Region	Rx traffic ▾	Tx traffic
cyxtest@cyx...	5.7 G	0
pjtest3@pjt...	5.7 G	0

4.4 Attack Events

Under **Traffic Monitoring > Attack Events**, you can do as follows:

- View real-time and historical attack events of all objects or a specified region, region IP group, ADS device, ADS-protected group, or IP address.
- View or add panels.
- Configure filters.

By default, when **Display by Regions** is selected, attack event information of all monitored regions is displayed in real time mode.

4.4.1 Viewing Attack Events in Real Time Mode

To view attack events in real time mode, follow these steps:

Step 1 Choose **Traffic Monitoring** > **Attack Events**.

By default, attack traffic information of all monitored objects is displayed in real time mode, including top source countries, top 10 source IP addresses, and attack type distribution, as shown in Figure 4-102.

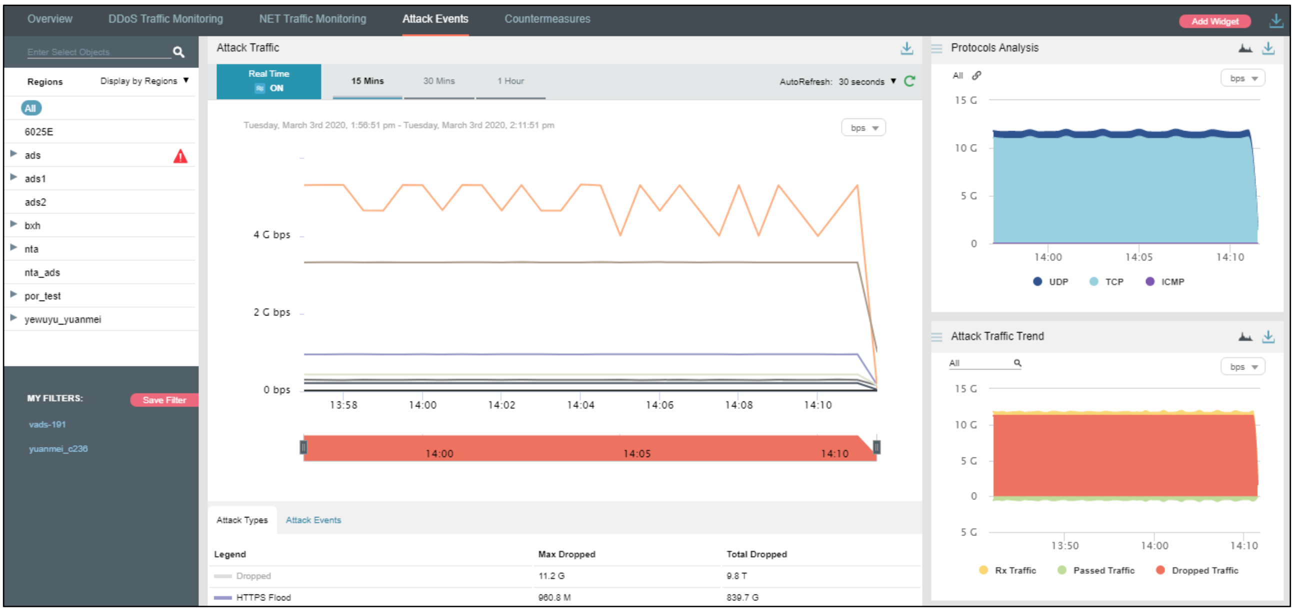
On the **Attack Types** tab page, attack type names and information of dropped traffic are displayed.

Clicking the bar or text in the **Legend** column hides or displays such type of attack traffic in the attack traffic trend graph. By default, all types of attack traffic are displayed. A dimmed color indicates that this type of attack traffic is not displayed. Otherwise, the attack traffic is displayed.

Table 4-10 Attack type parameters

Parameter	Description
Legend	Shows various colors, indicating different attack types, which correspond to those displayed in the attack traffic trend graph.
Max Dropped	Indicates the maximum traffic (in bps or pps) dropped by ADS for the object in the statistical period.
Total Dropped	Indicates the total traffic (in bits) dropped by ADS for the object in the statistical period.

Figure 4-102 Attack Events page – Attack Types panel

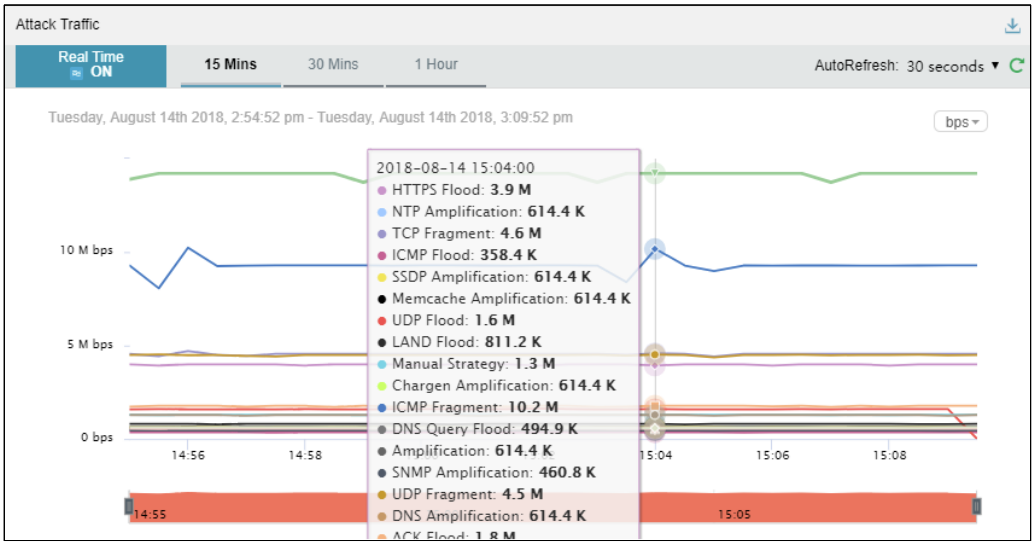


Legend	Max Dropped	Total Dropped
Dropped	11.2 G	9.8 T
HTTPS Flood	960.8 M	839.7 G

Step 2 Point to the attack traffic trend graph.

Detailed information about the time, real-time total dropped traffic, and real-time dropped traffic of a specific attack type is displayed, as shown in Figure 4-103.

Figure 4-103 Attack traffic information of a specific time

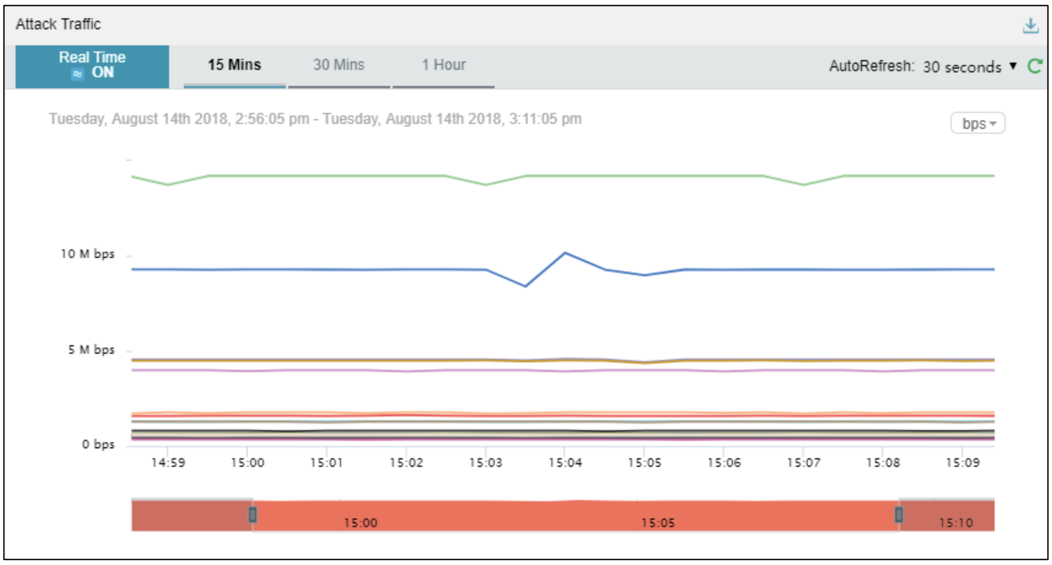


Tuesday, August 14th 2018, 2:54:52 pm - Tuesday, August 14th 2018, 3:09:52 pm

2018-08-14 15:04:00
- HTTPS Flood: **3.9 M**
- NTP Amplification: **614.4 K**
- TCP Fragment: **4.6 M**
- ICMP Flood: **358.4 K**
- SSDP Amplification: **614.4 K**
- Memcache Amplification: **614.4 K**
- UDP Flood: **1.6 M**
- LAND Flood: **811.2 K**
- Manual Strategy: **1.3 M**
- Chargen Amplification: **614.4 K**
- ICMP Fragment: **10.2 M**
- DNS Query Flood: **494.9 K**
- Amplification: **614.4 K**
- SNMP Amplification: **460.8 K**
- UDP Fragment: **4.5 M**
- DNS Amplification: **614.4 K**
- ACK Flood: **1.8 M**

Step 3 Below the attack traffic trend graph, drag ‖ to view a finer-granularity traffic trend.

Figure 4-104 Finer-granularity traffic monitoring information



Tuesday, August 14th 2018, 2:56:05 pm - Tuesday, August 14th 2018, 3:11:05 pm

Step 4 On the page shown in Figure 4-102, click **Attack Events** below the attack traffic trend graph.

The ongoing attack events and their details are displayed, as shown in Figure 4-105.

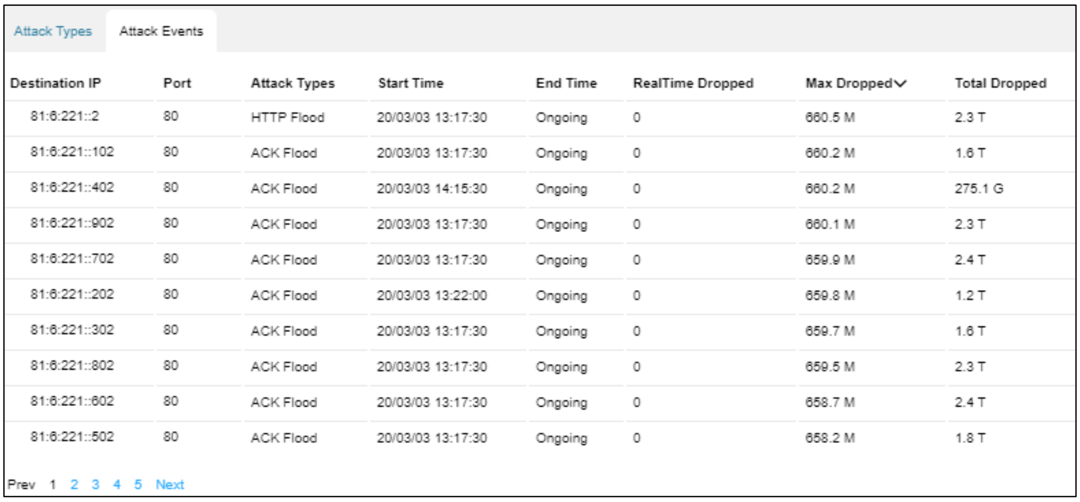
On the attack event list, attack events are displayed in descending order of dropped traffic volume.

Note	Attack events are defined as follows: • Attacks of different types targeting the same IP address are counted as separate events. • Attacks of the same type targeting different IP addresses are counted as separate events. • Attacks of different types targeting different IP addresses are counted as separate events. • Attacks of the same type targeting the same IP address are counted as one event.

Table 4-11 Attack event parameters

Parameter	Description
Destination IP	Indicates the attacked IP address.
Port	Indicates the attacked port of the attacked IP address.
Attack Types	Indicates the type of the attack.
Start Time	Indicates the time when the attack begins.
End Time	Indicates the time when the attack ends.
RealTime Dropped	Indicates the traffic (in bps or pps) dropped by ADS for the object.
Max Dropped	Indicates the maximum traffic (in bps or pps) dropped by ADS for the object.
Total Dropped	Indicates the total traffic (in bits) dropped by ADS for the object.

Figure 4-105 Attack traffic – attack events



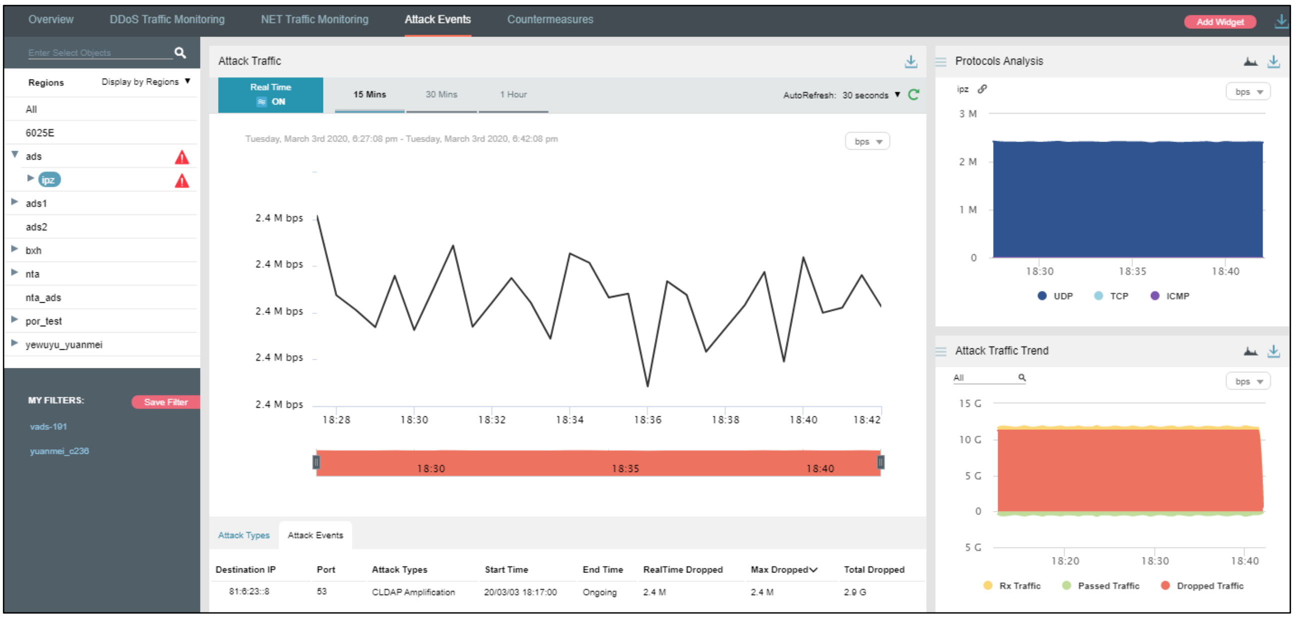
Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:221::2	80	HTTP Flood	20/03/03 13:17:30	Ongoing	0	660.5 M	2.3 T
81:6:221::102	80	ACK Flood	20/03/03 13:17:30	Ongoing	0	660.2 M	1.6 T
81:6:221::402	80	ACK Flood	20/03/03 14:15:30	Ongoing	0	660.2 M	275.1 G
81:6:221::902	80	ACK Flood	20/03/03 13:17:30	Ongoing	0	660.1 M	2.3 T
81:6:221::702	80	ACK Flood	20/03/03 13:17:30	Ongoing	0	659.9 M	2.4 T
81:6:221::202	80	ACK Flood	20/03/03 13:22:00	Ongoing	0	659.8 M	1.2 T
81:6:221::302	80	ACK Flood	20/03/03 13:17:30	Ongoing	0	659.7 M	1.6 T
81:6:221::802	80	ACK Flood	20/03/03 13:17:30	Ongoing	0	659.5 M	2.3 T
81:6:221::602	80	ACK Flood	20/03/03 13:17:30	Ongoing	0	658.7 M	2.4 T
81:6:221::502	80	ACK Flood	20/03/03 13:17:30	Ongoing	0	658.2 M	1.8 T

----End

4.4.2 Viewing Region-Specific Attack Events

On the page shown in Figure 4-102, clicking a region in the left pane displays attack traffic information of the region and of all IP groups and IP addresses in this region. You can further view historical and real-time attack traffic trends and panels of a selected region, IP group under a region, or IP address. For example, if you choose **Regions** > **ads** > **ipz**, you can view attack events of **ipz**.

Figure 4-106 Region-specific attack events

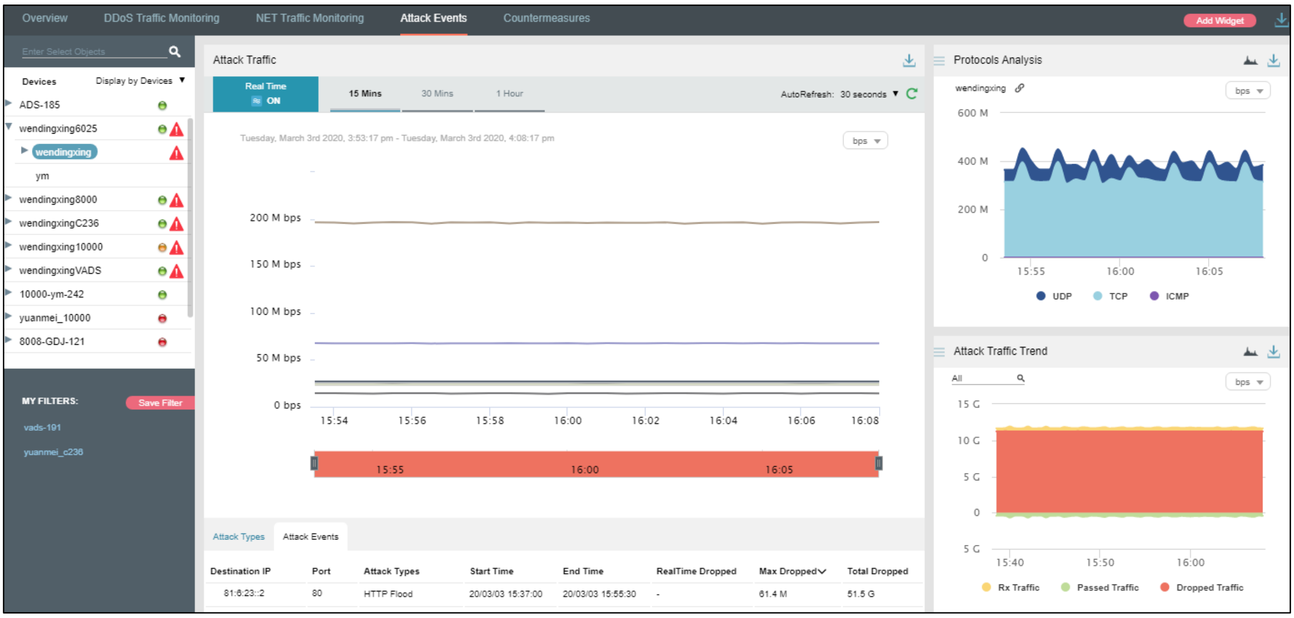


Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:23::8	53	CLDAP Amplification	20/03/03 18:17:00	Ongoing	2.4 M	2.4 M	2.9 G

4.4.3 Viewing Device-Specific Attack Events

On the page shown in Figure 4-102, you can select **Display by Devices** from the drop-down list in the left pane and then select a device to view real-time attack events of this ADS device, ADS-protected groups, and specific IP addresses under a protection group. You can view real-time and attack traffic trends and panels of a selected ADS, ADS-protected group, and IP address under a protection group. For example, you can choose **Devices** > **wendingxing6025** > **wendingxing** to view attack event information of group **wendingxing** under device **wendingxing6025**.

Figure 4-107 Device-specific attack events



Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:23::2	80	HTTP Flood	20/03/03 15:37:00	20/03/03 15:55:30	-	61.4 M	51.5 G

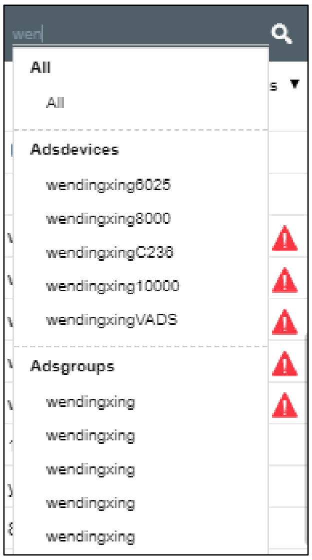
4.4.4 Viewing Object-Specific Attack Events

By default, the **Attack Events** tab page displays attack traffic trends of all ADS devices monitored by ADS M. You can view the real-time traffic trends of a specified region, regional IP group, ADS device, ADS-protected group, or IP address.

Step 1 On the page shown in Figure 4-102, type a character string and then press **Enter**.

The system displays all objects containing the typed character string, as shown in Figure 4-108.

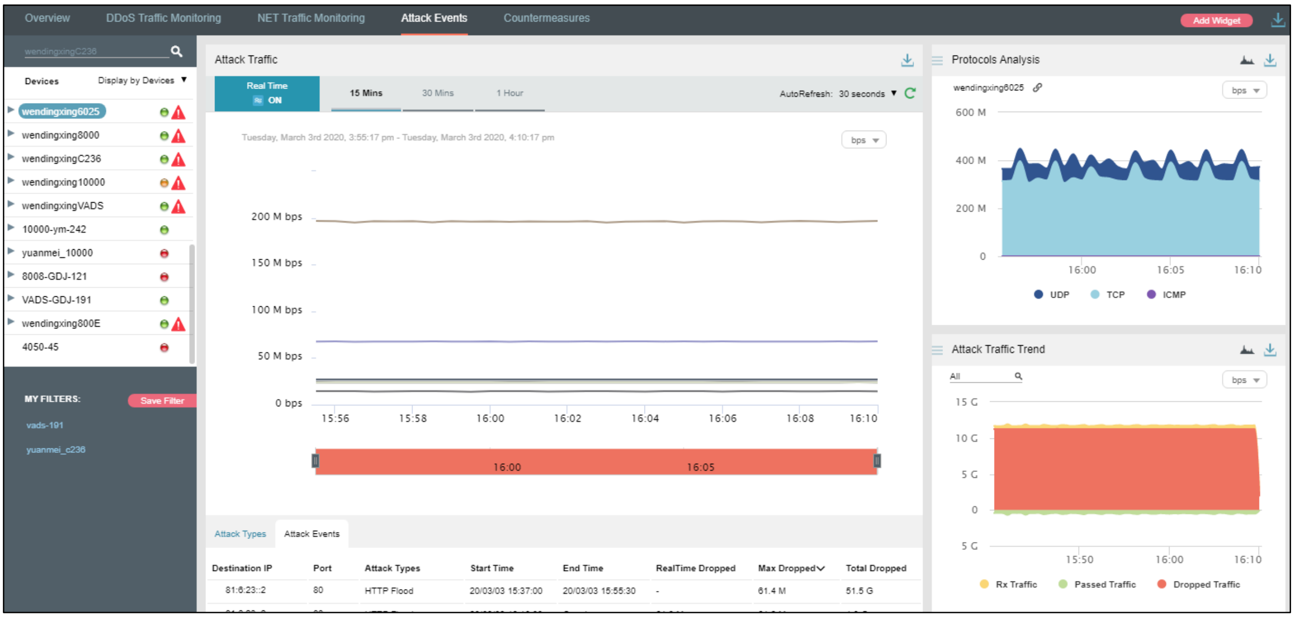
Figure 4-108 Searching for attack event objects



Step 2 Select an object to be queried, such as **wendingxing6025**, and then press **Enter**.

Traffic information of the selected object is displayed, as shown in Figure 4-109.

Figure 4-109 Object-specific attack event information



Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:23::2	80	HTTP Flood	20/03/03 15:37:00	20/03/03 15:55:30	-	61.4 M	51.5 G

----End

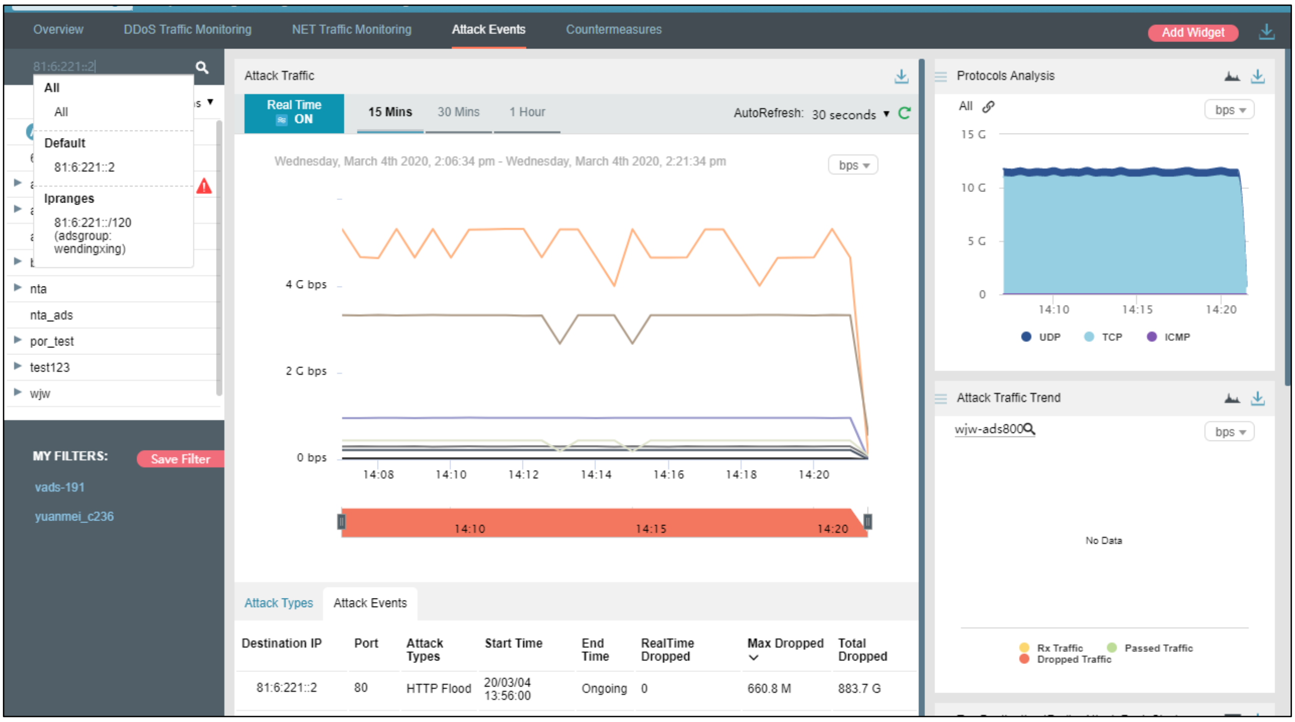
4.4.5 Viewing Attack Event Information of an IP Address in the Default Protection Group

IP addresses under the default protection group do not belong to any regions or ADS-protected groups. To view attack traffic monitoring information of such an IP address, you need to expressly indicate the IP address before the system displays such information.

Step 1 On the page shown in Figure 4-102, type an IP address (such as **81:6:221::2**) and then press **Enter**.

The system displays all objects containing this IP address, as shown in Figure 4-110.

Figure 4-110 Searching for attack event objects

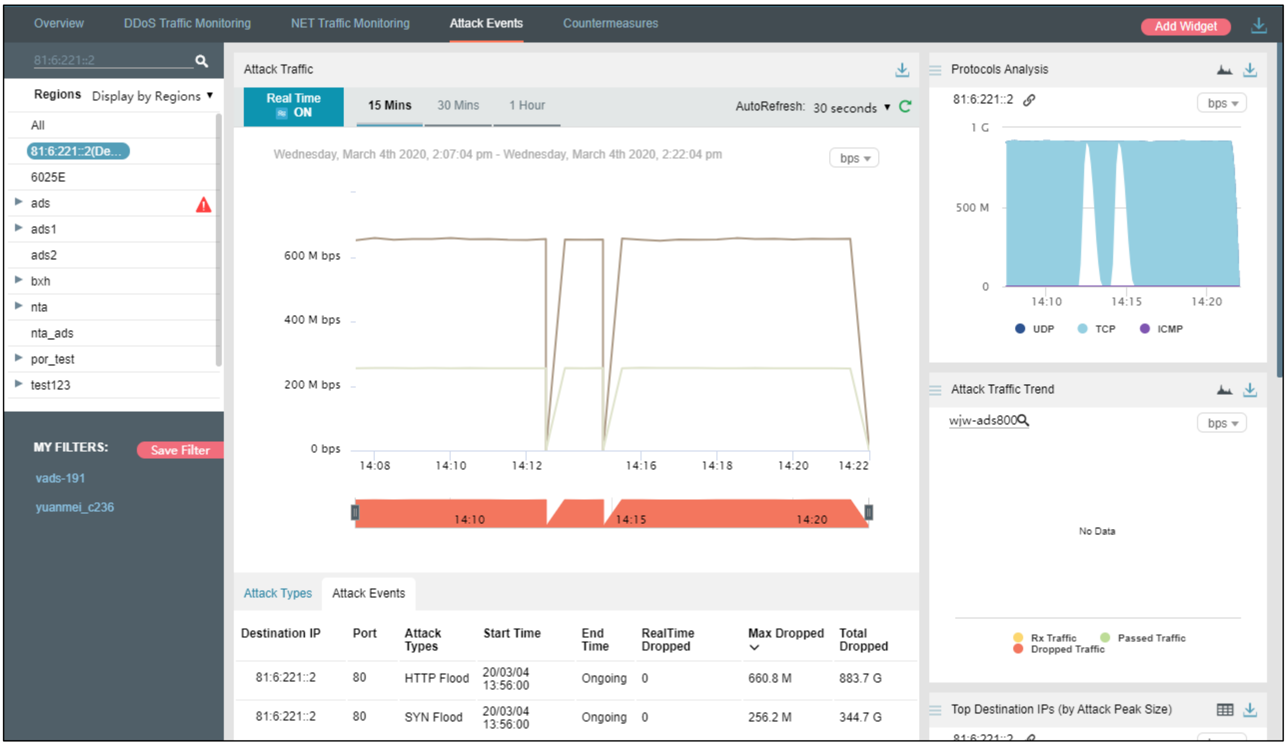


Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:221::2	80	HTTP Flood	20/03/04 13:56:00	Ongoing	0	660.8 M	883.7 G

Step 2 Select the object to be queried and then press **Enter**.

Traffic monitoring information of this IP address is displayed, as shown in Figure 4-111.

Figure 4-111 Attack event information of an IP address in the default protection group



Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:221::2	80	HTTP Flood	20/03/04 13:56:00	Ongoing	0	660.8 M	883.7 G
81:6:221::2	80	SYN Flood	20/03/04 13:56:00	Ongoing	0	256.2 M	344.7 G

----End

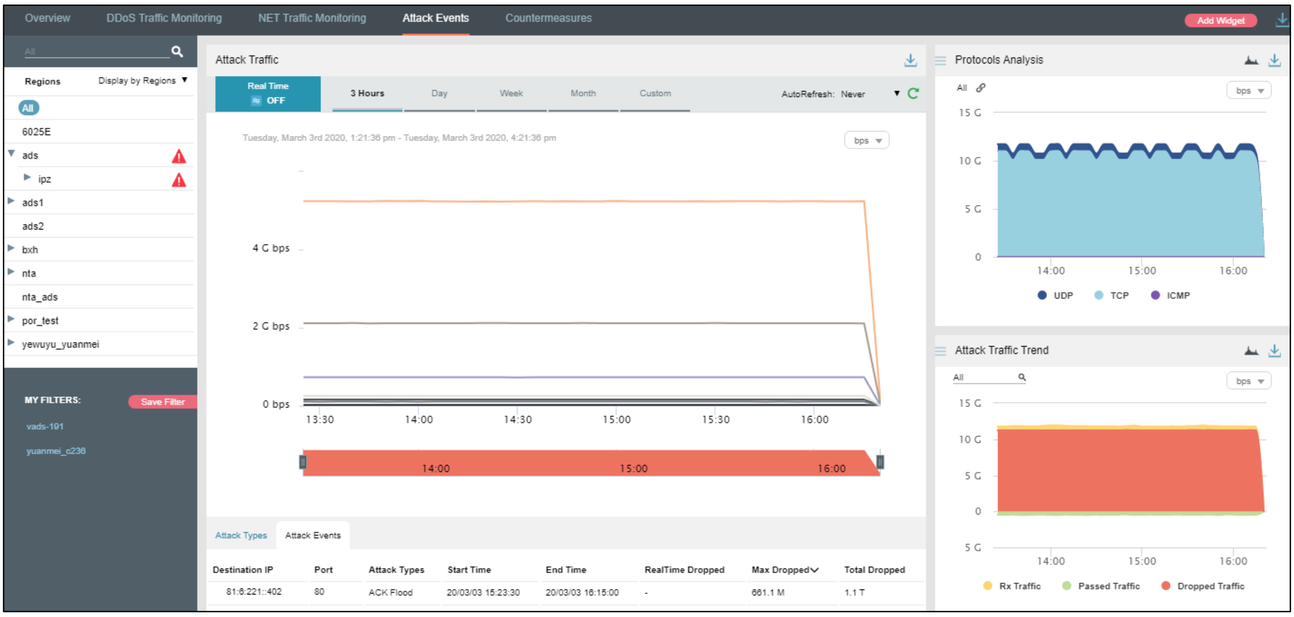
4.4.6 Viewing Attack Events in Historical Mode

On the page shown in Figure 4-102, clicking **ON** for **Real Time** in the **Attack Traffic** area disables the real-time mode and enables the historical mode. Clicking **OFF** for **Real Time** enables the real-time mode again.

In historical mode, attack traffic trend graphs and panels with the icon 🔗 display historical data.

By default, the attack traffic trend graph displays attack traffic data in the last 3 hours. Clicking **Day**, **Week**, **Month**, or **Custom** displays attack traffic trend graphs in the last day, week, month, or a custom period.

Figure 4-112 Historical attack traffic trend

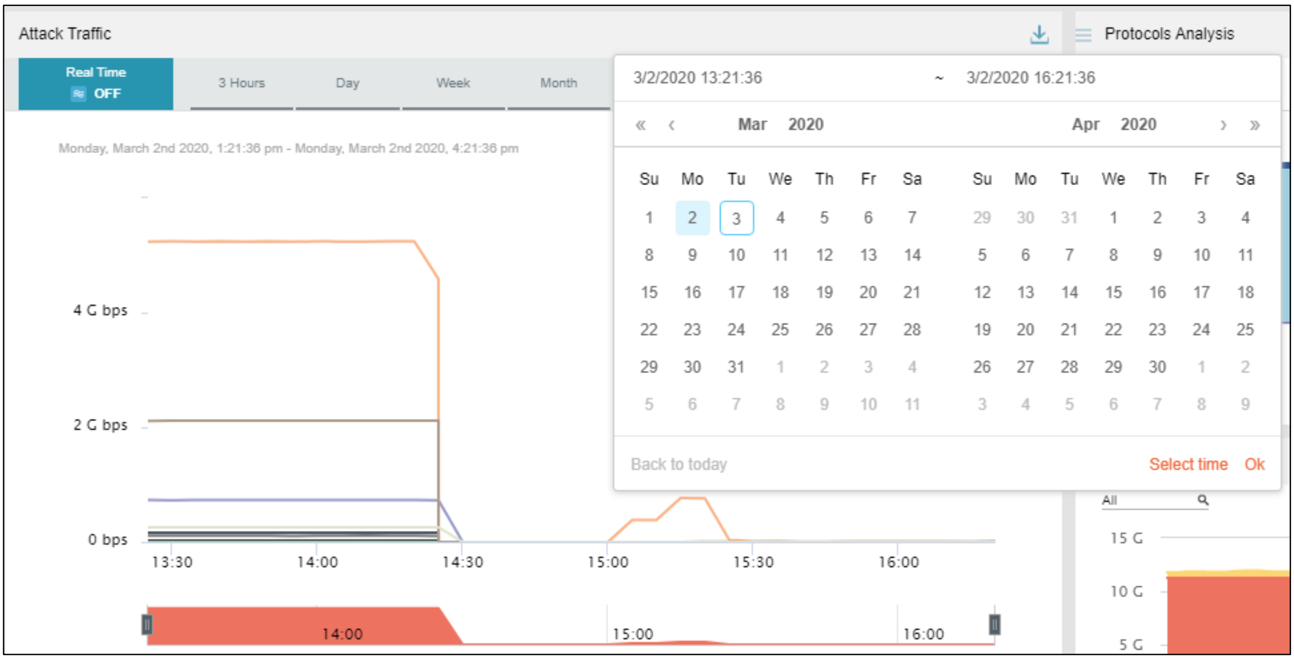


Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:221::402	80	ACK Flood	20/03/03 15:23:30	20/03/03 16:15:00	-	661.1 M	1.1 T

On the page shown in Figure 4-112, click **Custom** above the attack traffic graph.

You can select the start time and end time of the attack traffic graph as required, as shown in Figure 4-113. The unit is the day.

Figure 4-113 Customization of the attack traffic trend graph



3/2/2020 13:21:36 ~ 3/2/2020 16:21:36

Mar 2020

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

Apr 2020

Su	Mo	Tu	We	Th	Fr	Sa
29	30	31	1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	1	2
3	4	5	6	7	8	9

4.4.7 Switching the Traffic Unit

By default, traffic is expressed in bps in attack traffic trend graphs. On the page shown in Figure 4-102, you can select **pps** from the drop-down list in the upper-right corner of the **Attack Traffic** area to display traffic data in pps.

4.4.8 Refreshing the Attack Traffic Trend Graph

By default, the attack traffic trend graph automatically refreshes every 30 seconds in real time mode. On the page shown in Figure 4-102, you can select **Never** from the **AutoRefresh** drop-down list in the upper-right corner of the **Attack Traffic** area. In this case, the attack traffic trend graph does not refresh unless you click ↻.

By default, the attack traffic trend graph does not automatically refresh in historical mode. On the page shown in Figure 4-102, you can select **Every 5 min** from the **AutoRefresh** drop-down list in the upper-right corner of the **Attack Traffic** area. In this case, the attack traffic trend graph will automatically refresh every 5 minutes.

4.4.9 Downloading an Attack Traffic Trend Report

On the page shown in Figure 4-102, you can click ⤓ in the upper-right corner and then click HTML or PDF to export the current data of the attack traffic trend graph as an HTML or PDF report. For details, see section 4.1.4 Downloading a Report.

4.4.10 Managing Filters

Filters are provided for users to define objects of their concern, so that they can find detected attack events more conveniently. After being created, filters are displayed in the filter list. You can click a filter to view attack event information of the object specified by the filter.

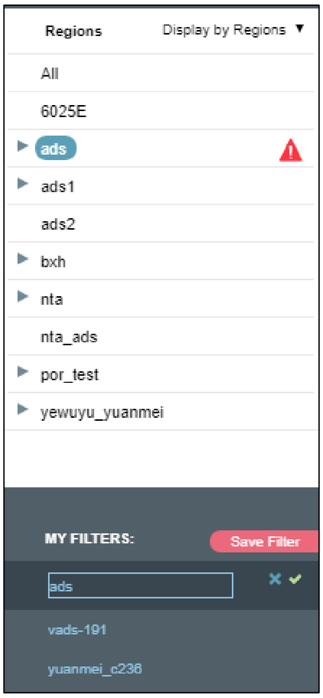
Any queried objects, such as a region, region IP group, ADS device, ADS-protected group, or IP address can be configured as a filter. But **All** and **Default** cannot be configured as a filter. You can configure multiple filters.

4.4.10.1 Configuring a Filter

To configure a filter, follow these steps:

Step 1 On the page shown in Figure 4-102, select an object from the left pane, such as **ads**, and then click **Save Filter**.

Figure 4-114 Creating a filter



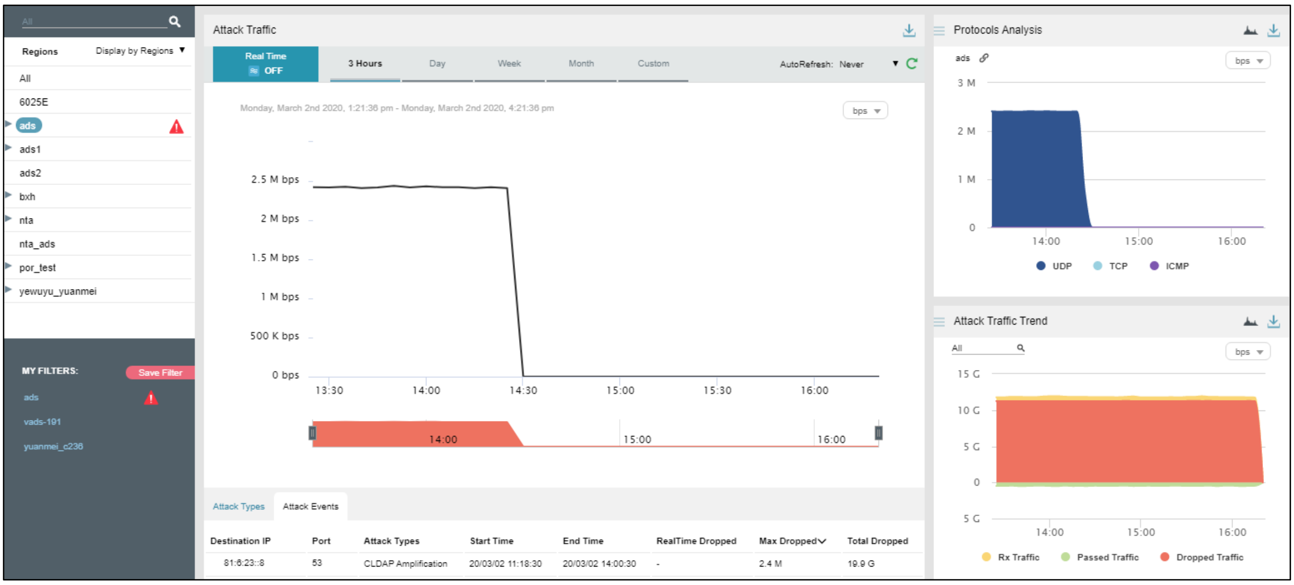
Step 2 Type the filter name.

By default, the object name is displayed as the filter name. You can use the default name or type a new one.

Step 3 Click ✓ and then click **Confirm** in the dialog box that appears.

Step 4 Click **ads** in the filter list to view its attack traffic information.

Figure 4-115 Viewing a filter



Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:23::8	53	CLDAP Amplification	20/03/02 11:18:30	20/03/02 14:00:30	-	2.4 M	19.9 G

----End

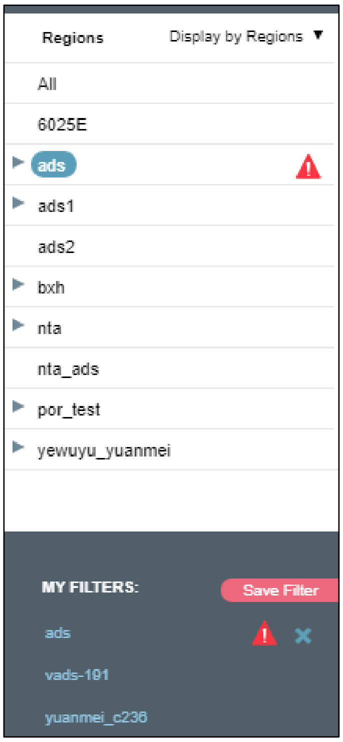
4.4.10.2 Deleting a Filter

To delete a filter, follow these steps:

Step 1 On the page shown in Figure 4-115, point to a filter name

The icon ✖ appears, as shown in Figure 4-116.

Figure 4-116 Deleting a filter



Step 2 Click ✖ and then **Confirm** in the dialog box that appears.

----End

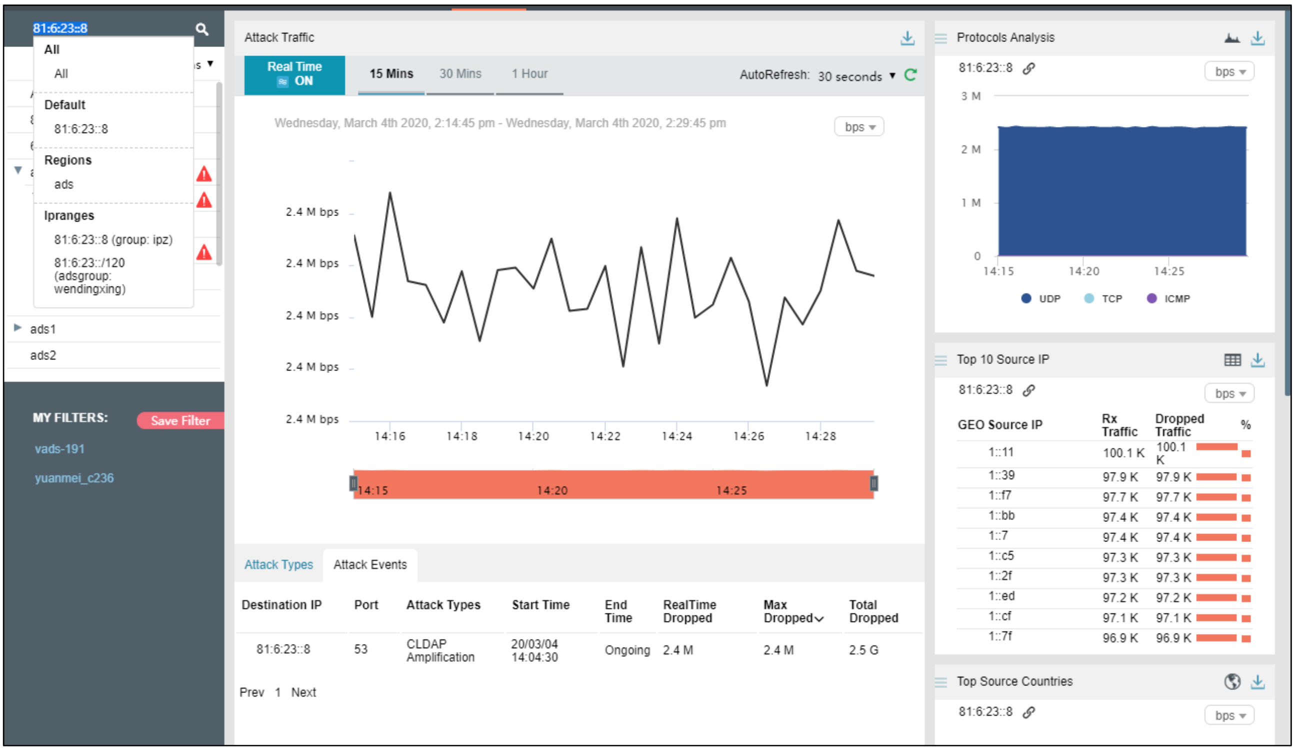
4.4.11 Managing Panels

By default, **Top 10 Source IP**, **Top Source Countries**, and **Attack Type Distribution** are displayed under **Traffic Monitoring > Attack Events**, as shown in Figure 4-117.

A panel with the icon 🔗 indicates that when the selected object and statistical period change, the object and statistical period of this panel will change accordingly. A panel without the icon 🔗 indicates the opposite.

You can add panels as required. For how to add, edit, and delete panels, see section 4.1 Overview.

Figure 4-117 Default panels on the Attack Events page



Destination IP	Port	Attack Types	Start Time	End Time	RealTime Dropped	Max Dropped	Total Dropped
81:6:23::8	53	CLDAP Amplification	20/03/04 14:04:30	Ongoing	2.4 M	2.4 M	2.5 G

GEO Source IP	Rx Traffic	Dropped Traffic	%
1::11	100.1 K	100.1 K	
1::39	97.9 K	97.9 K	
1::f7	97.7 K	97.7 K	
1::bb	97.4 K	97.4 K	
1::7	97.4 K	97.4 K	
1::c5	97.3 K	97.3 K	
1::2f	97.3 K	97.3 K	
1::ed	97.2 K	97.2 K	
1::cf	97.1 K	97.1 K	
1::7f	96.9 K	96.9 K	

4.5 Countermeasures

Under **Traffic Monitoring > Countermeasures**, you can do as follows:

- View real-time and historical dropped traffic of all objects or a specified region, region IP group, ADS device, ADS-protected group, or IP address.
- View or add panels.
- Configure filters.

By default, when **Display by Regions** is selected, dropped traffic information of all monitored regions is displayed in real-time mode.

4.5.1 Viewing Real-Time Dropped Traffic

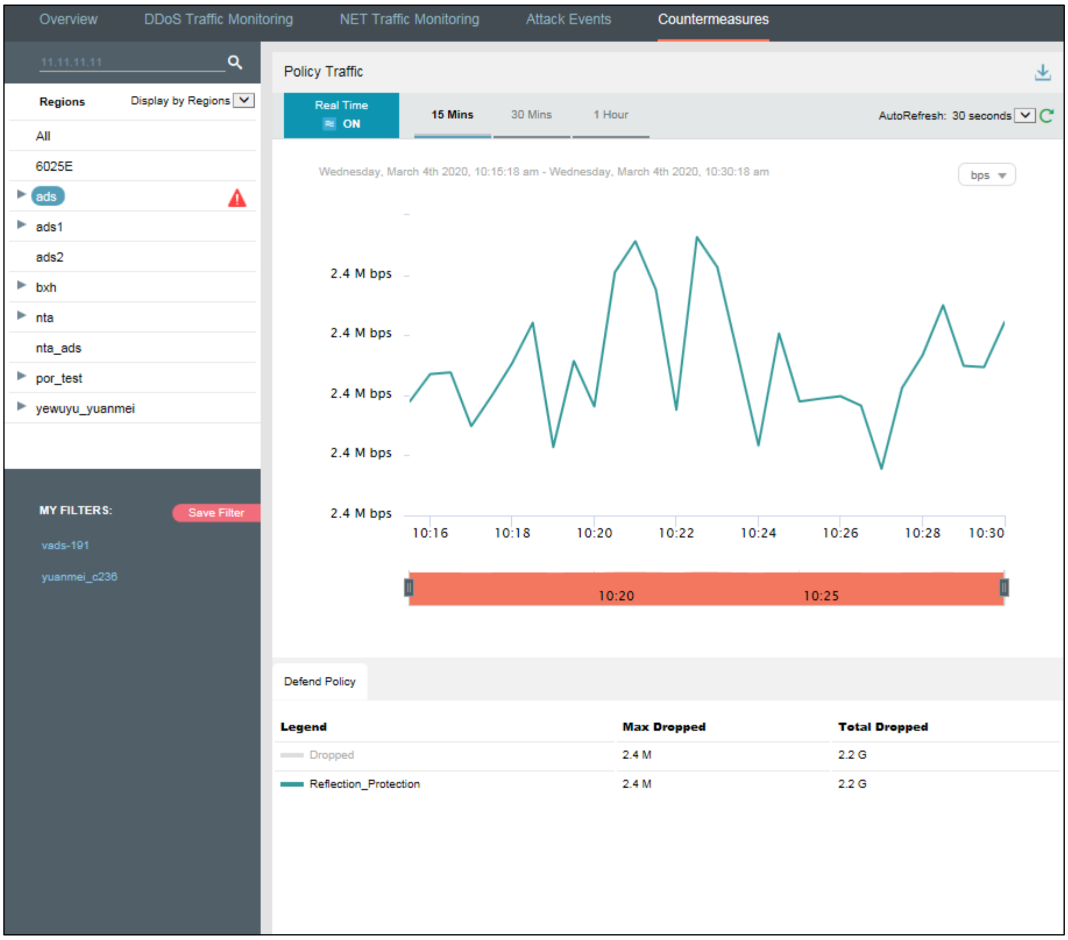
To view real-time dropped traffic information, follow these steps:

Choose **Traffic Monitoring > Countermeasures**.

By default, in the **Policy Traffic** panel, dropped traffic of all monitored objects is displayed, including the traffic trend and traffic distribution by protection policy, as shown in Figure 4-118.

In real-time mode, the dropped traffic trend graph in the last 15 minutes is displayed by default. You can click **30 Mins** or **1 Hour** to view the traffic graph in the last 30 minutes or last hour.

Figure 4-118 Dropped traffic information of all objects



Wednesday, March 4th 2020, 10:15:18 am - Wednesday, March 4th 2020, 10:30:18 am

Legend	Max Dropped	Total Dropped
Dropped	2.4 M	2.2 G
Reflection_Protection	2.4 M	2.2 G

The protection policy list ranks the types of dropped traffic in descending order of volume. For the description of parameters, see Table 4-12.

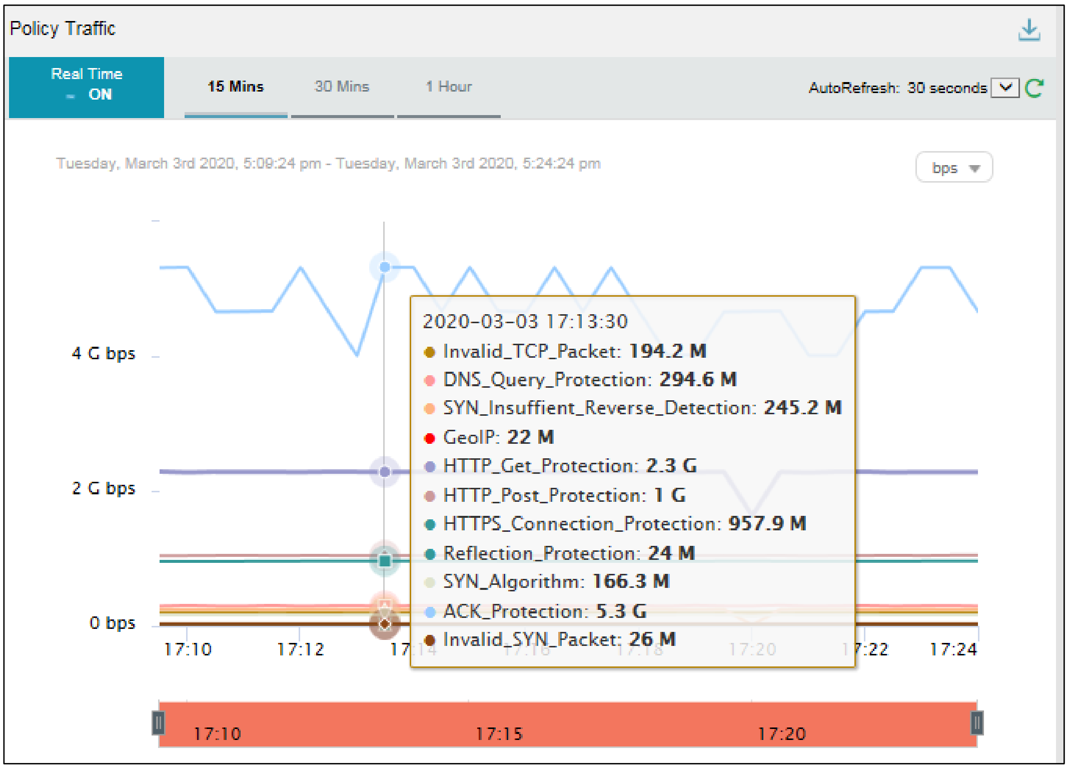
Clicking the bar or text in the **Legend** column hides or displays this type of dropped traffic in the trend graph. By default, all types of dropped traffic are displayed. A dimmed color indicates that this type of traffic is not displayed. Otherwise, the traffic is displayed.

Table 4-12 Parameters displayed in the Defend Policy panel

Parameter	Description
Legend	Indicates the type of dropped traffic to be displayed in the trend graph.
Max Dropped	Indicates the maximum traffic dropped by ADS for the current object in the statistical period. The traffic is ranked in descending order of volume and expressed in bps or pps.
Total Dropped	Indicates the total traffic dropped by ADS for all objects in the statistical period. The unit is bps or pps.

Step 2 Point to a random point in the dropped traffic trend graph to view detailed information about the dropped traffic, including the time, traffic type, and volume.

Figure 4-119 Viewing dropped traffic at a specific time



2020-03-03 17:13:30
- Invalid_TCP_Packet: 194.2 M
- DNS_Query_Protection: 294.6 M
- SYN_Insuffient_Reverse_Detection: 245.2 M
- GeoIP: 22 M
- HTTP_Get_Protection: 2.3 G
- HTTP_Post_Protection: 1 G
- HTTPS_Connection_Protection: 957.9 M
- Reflection_Protection: 24 M
- SYN_Algorithm: 166.3 M
- ACK_Protection: 5.3 G
- Invalid_SYN_Packet: 26 M

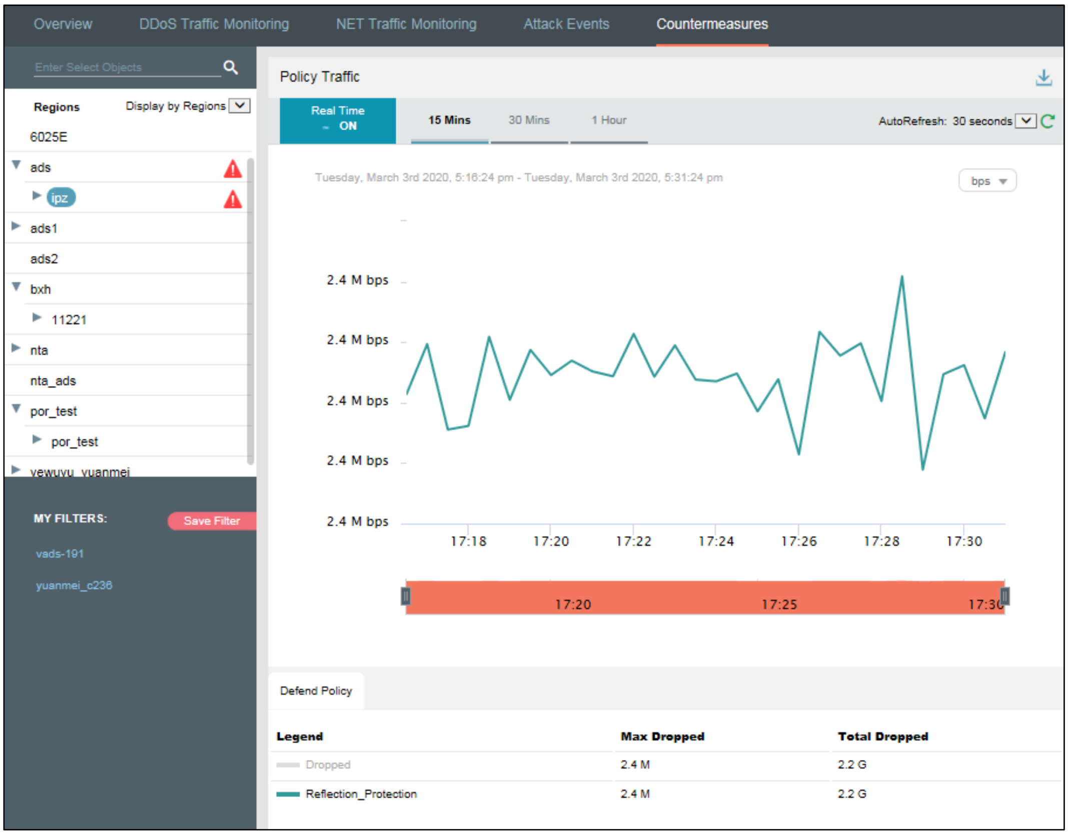
Step 3 Below the dropped attack traffic trend graph, drag ▮ to view a finer-granularity traffic trend.

----End

4.5.2 Viewing Region-Specific Dropped Traffic

On the page shown in Figure 4-118, clicking a region in the left pane displays dropped traffic information of the region and of all IP groups and IP addresses in this region. You can further view historical and real-time dropped traffic trends and panels of a selected region or a specific IP group or IP address in this region. For example, clicking **ipz** displays the trend graph of the traffic dropped by ADS for the region ipz. See Figure 4-120.

Figure 4-120 Dropped traffic trend graph of a specified region



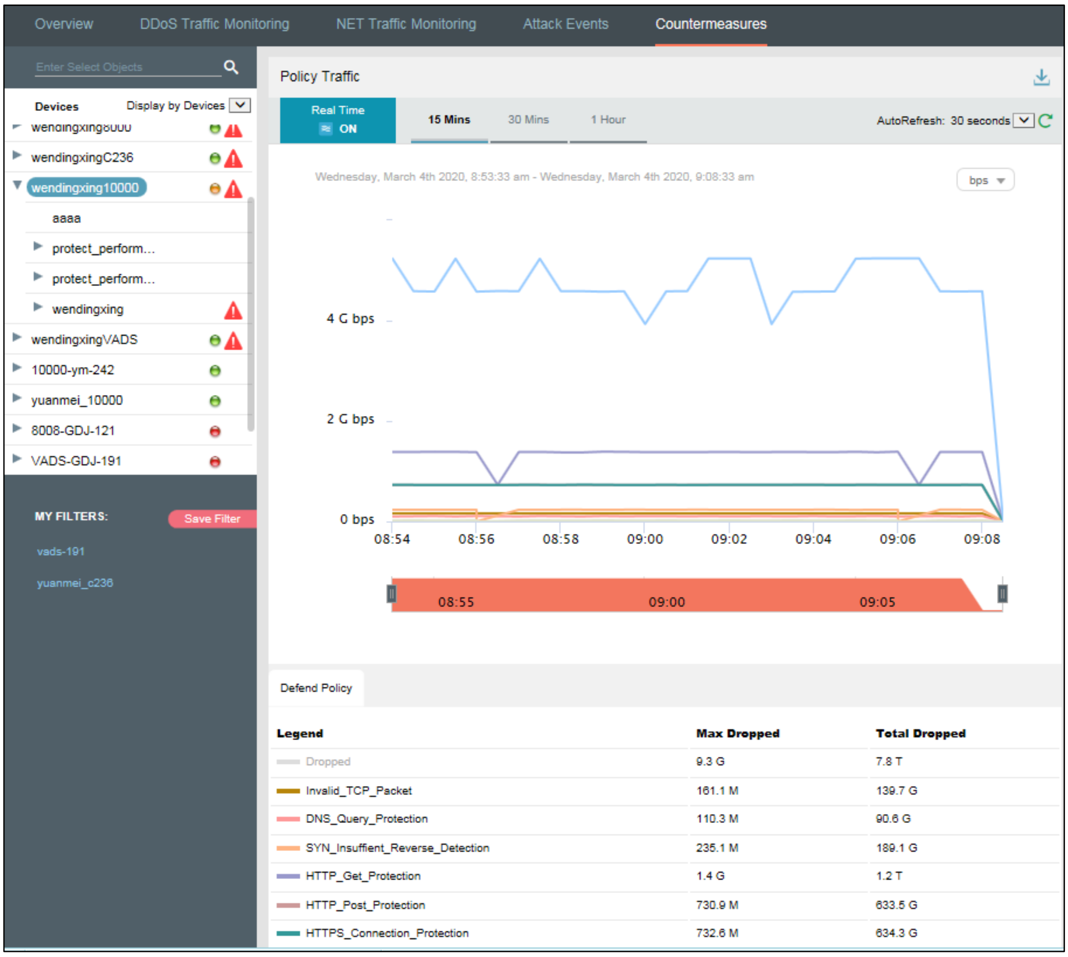
Tuesday, March 3rd 2020, 5:16:24 pm - Tuesday, March 3rd 2020, 5:31:24 pm

Legend	Max Dropped	Total Dropped
Dropped	2.4 M	2.2 G
Reflection_Protection	2.4 M	2.2 G

4.5.3 Viewing Device-Specific Dropped Traffic

On the page shown in Figure 4-118, you can select **Display by Devices** from the drop-down list in the left pane and then select an ADS device to view real-time dropped traffic information of this device, ADS-protected group, and specific IP addresses under a protection group. You can view the dropped traffic trend of a selected ADS, ADS-protected group, or a specific IP address under a protection group. For example, clicking **wendingxing10000** displays the trend of the traffic dropped by ADS for this group. See Figure 4-121.

Figure 4-121 Dropped traffic trend graph of a specified device



Legend	Max Dropped	Total Dropped
Dropped	9.3 G	7.8 T
Invalid_TCP_Packet	161.1 M	139.7 G
DNS_Query_Protection	110.3 M	90.6 G
SYN_Insuffient_Reverse_Detection	235.1 M	189.1 G
HTTP_Get_Protection	1.4 G	1.2 T
HTTP_Post_Protection	730.9 M	633.5 G
HTTPS_Connection_Protection	732.6 M	634.3 G

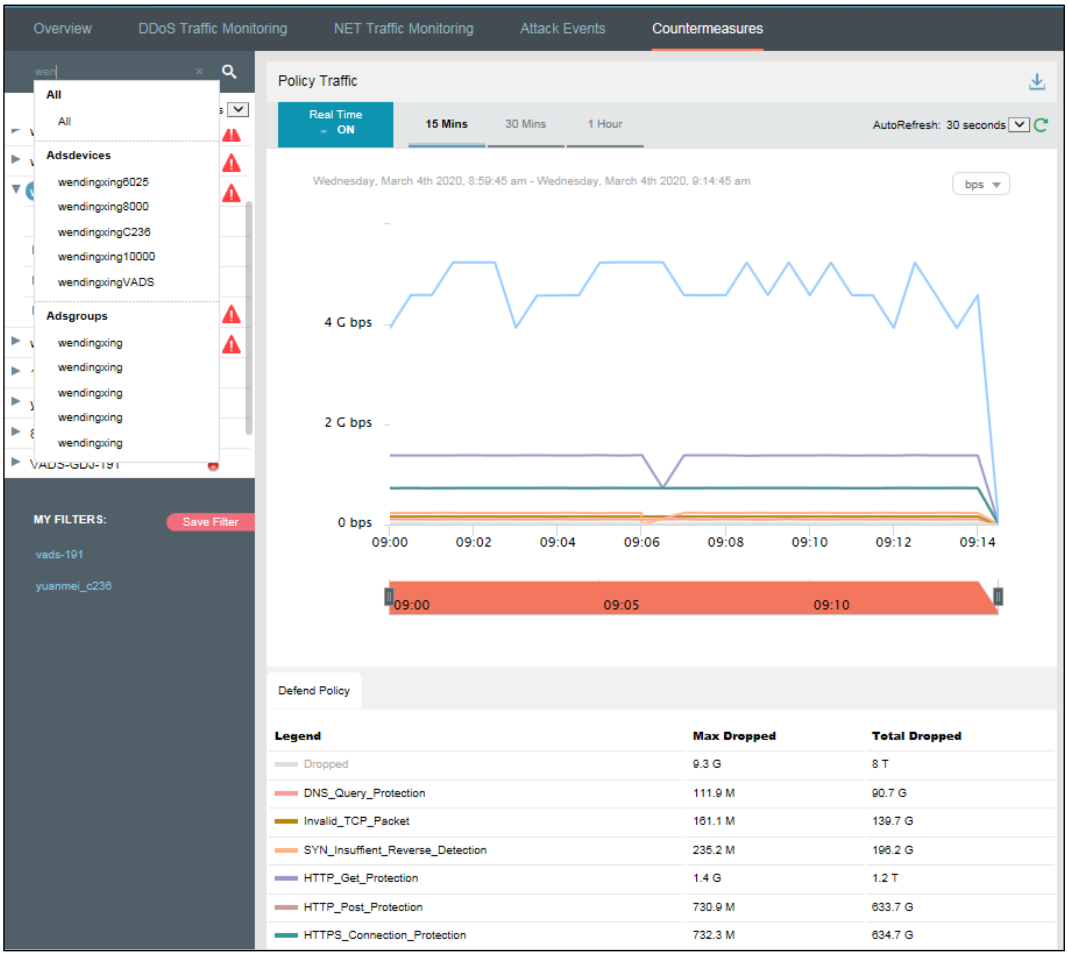
4.5.4 Viewing Object-Specific Dropped Traffic

By default, the **Countermeasures** tab page displays the trend of traffic dropped by all ADS devices under the monitoring of ADS M. You can view the real-time dropped traffic trends of a specified region, region IP group, ADS device, ADS-protected group, or IP address.

Step 1 On the page shown in Figure 4-118, type a character string and then press **Enter**.

The system displays all objects containing the typed character string.

Figure 4-122 Searching for monitored objects by character string

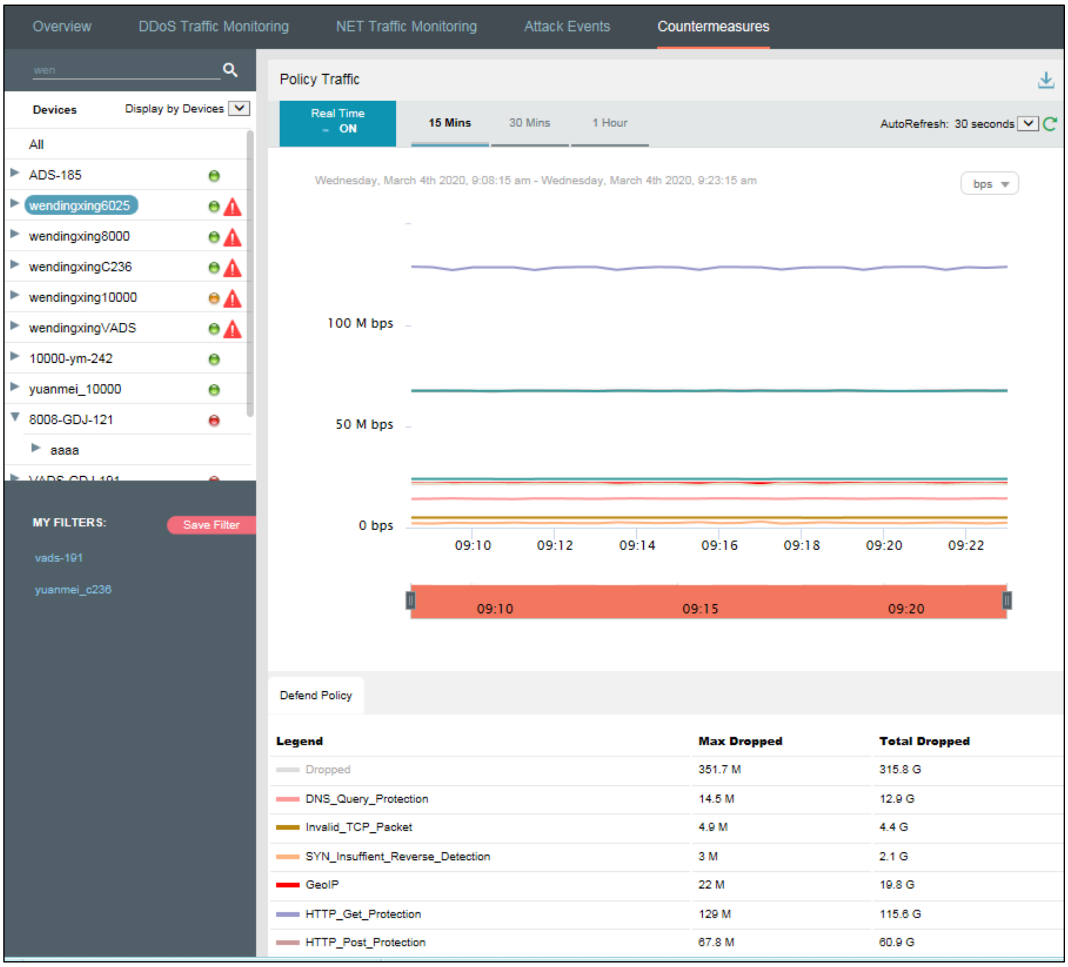


Legend	Max Dropped	Total Dropped
Dropped	9.3 G	8 T
DNS_Query_Protection	111.9 M	90.7 G
Invalid_TCP_Packet	161.1 M	139.7 G
SYN_Insuffient_Reverse_Detection	235.2 M	196.2 G
HTTP_Get_Protection	1.4 G	1.2 T
HTTP_Post_Protection	730.9 M	633.7 G
HTTPS_Connection_Protection	732.3 M	634.7 G

Step 2 Select an object to be queried, such as wendingxing6025, and then press **Enter**.

The dropped traffic of the selected object is displayed, as shown in Figure 4-123.

Figure 4-123 Viewing dropped traffic of a specified object



Legend	Max Dropped	Total Dropped
Dropped	351.7 M	315.8 G
DNS_Query_Protection	14.5 M	12.9 G
Invalid_TCP_Packet	4.9 M	4.4 G
SYN_Insuffient_Reverse_Detection	3 M	2.1 G
GeoIP	22 M	19.8 G
HTTP_Get_Protection	129 M	115.6 G
HTTP_Post_Protection	67.8 M	60.9 G

----End

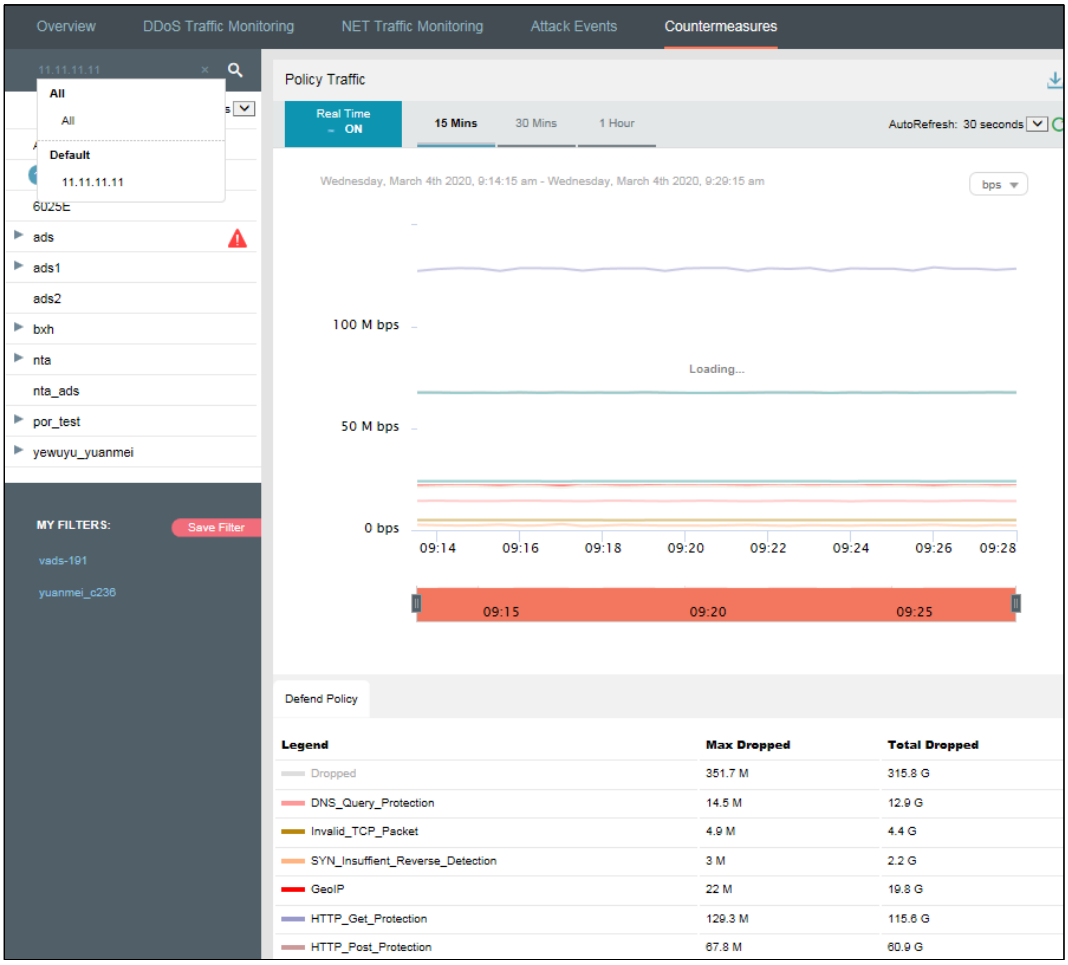
4.5.5 Viewing Dropped Traffic of an IP Address in the Default Protection Group

IP addresses under the default protection group do not belong to any regions or ADS-protected groups. To view dropped traffic information of such an IP address, you need to expressly indicate the IP address before the system displays such information.

Step 1 On the page shown in Figure 4-118, type an IP address (such as 11.11.11.11) and then press **Enter**.

The system displays all objects containing this IP address, as shown in Figure 4-124.

Figure 4-124 Searching for monitored objects by IP address

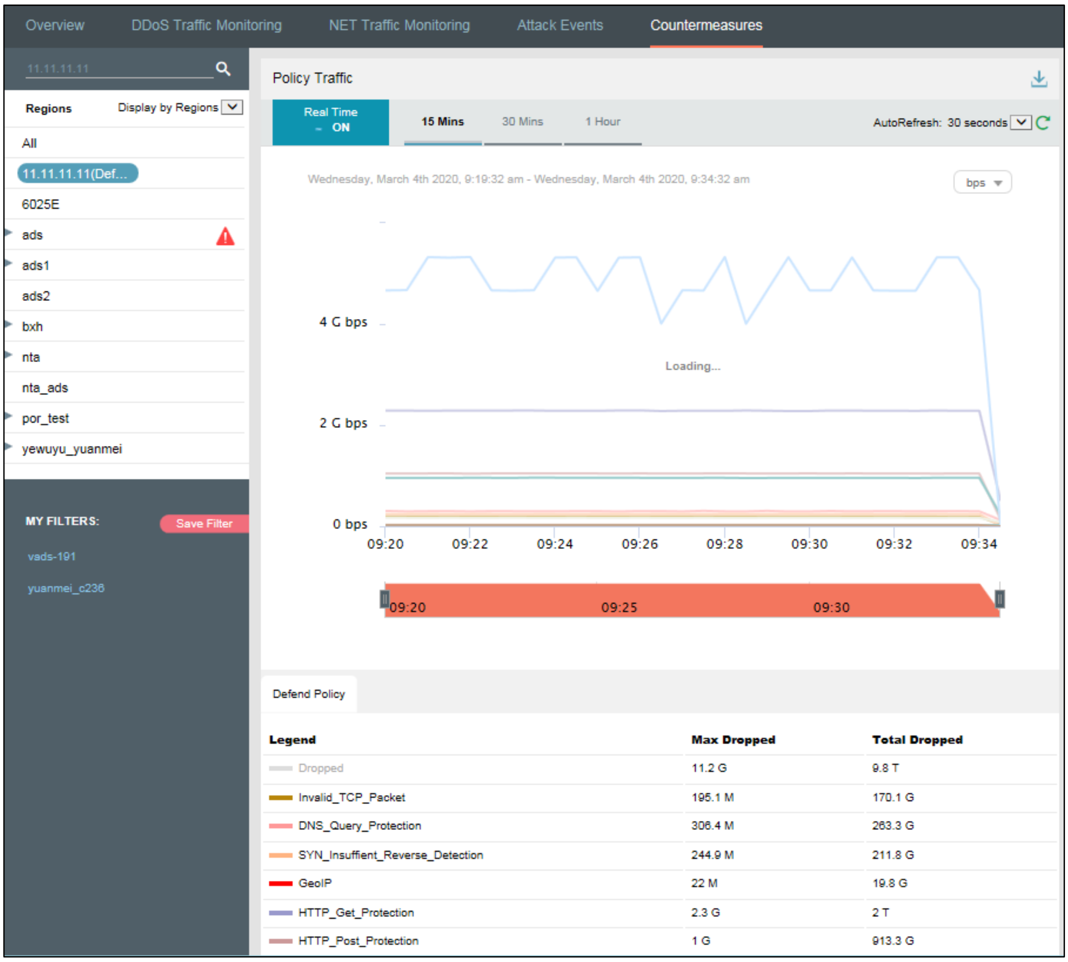


Legend	Max Dropped	Total Dropped
Dropped	351.7 M	315.8 G
DNS_Query_Protection	14.5 M	12.9 G
Invalid_TCP_Packet	4.9 M	4.4 G
SYN_Insuffient_Reverse_Detection	3 M	2.2 G
GeoIP	22 M	19.8 G
HTTP_Get_Protection	129.3 M	115.6 G
HTTP_Post_Protection	67.8 M	60.9 G

Step 2 Select the object to be queried and then press **Enter**.

The dropped traffic information of this IP address is displayed, as shown in Figure 4-125.

Figure 4-125 Viewing dropped traffic information of an IP address in the default protection group



Legend	Max Dropped	Total Dropped
Dropped	11.2 G	9.8 T
Invalid_TCP_Packet	195.1 M	170.1 G
DNS_Query_Protection	306.4 M	263.3 G
SYN_Insuffient_Reverse_Detection	244.9 M	211.8 G
GeoIP	22 M	19.8 G
HTTP_Get_Protection	2.3 G	2 T
HTTP_Post_Protection	1 G	913.3 G

----End

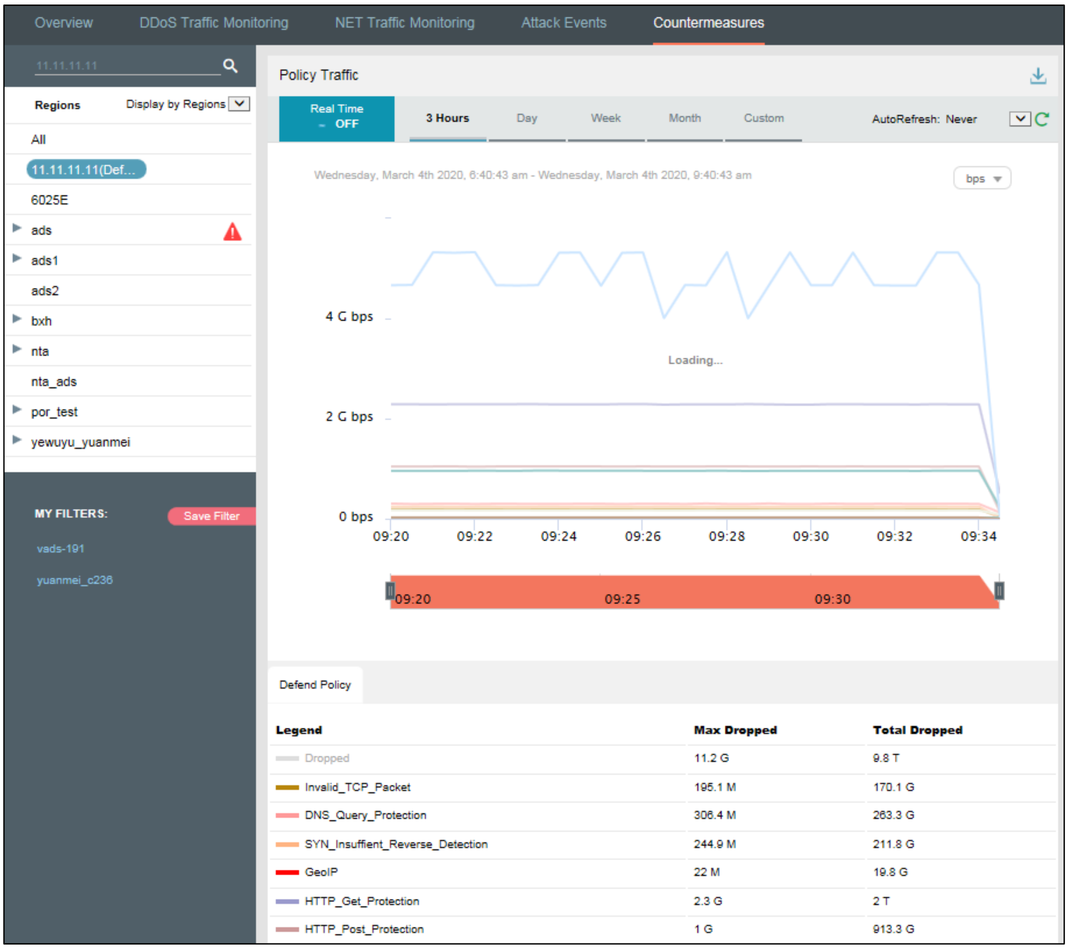
4.5.6 Viewing Historical Dropped Traffic

On the page shown in Figure 4-118, clicking **ON** for **Real Time** in the **Policy Traffic** panel disables the real-time mode and enables the historical mode. Clicking **OFF** for **Real Time** enables the real-time mode again.

In historical mode, dropped traffic trend graphs and panels with the icon 🔗 display historical data.

By default, the trend graph displays dropped traffic in the last 3 hours. Clicking **Day**, **Week**, **Month**, or **Custom** displays dropped traffic trend graphs in the last day, week, month, or a custom period.

Figure 4-126 Viewing historical dropped traffic trend

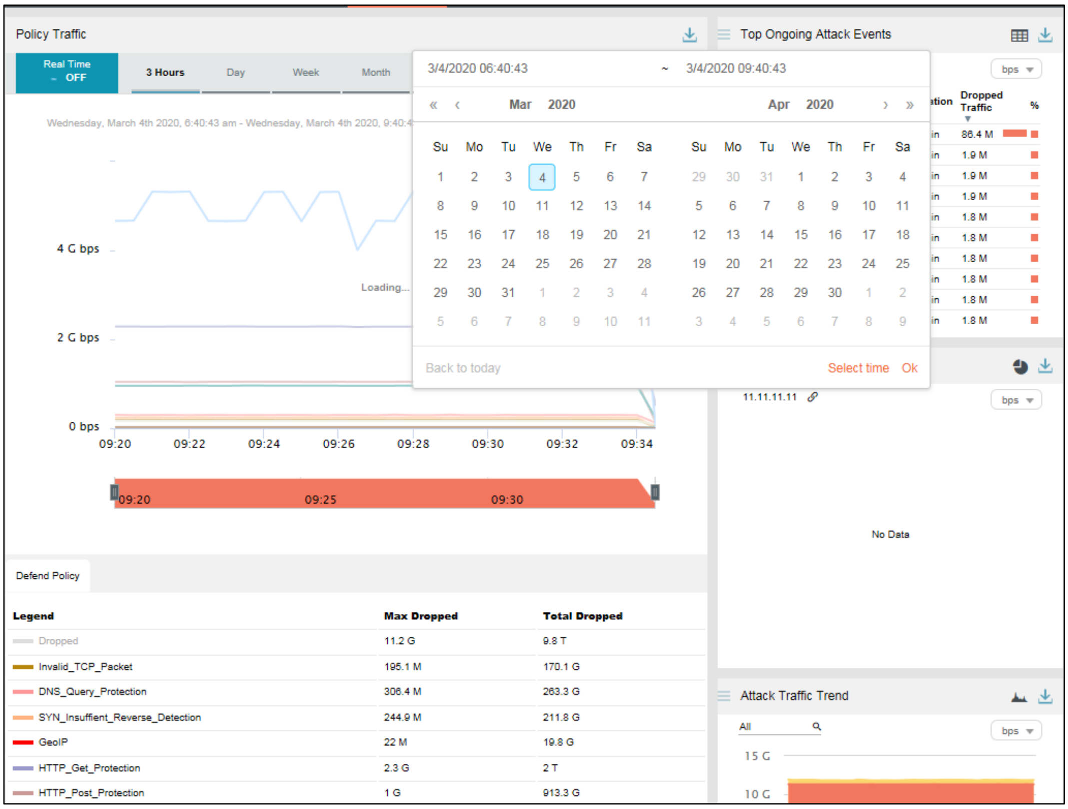


Legend	Max Dropped	Total Dropped
Dropped	11.2 G	9.8 T
Invalid_TCP_Packet	195.1 M	170.1 G
DNS_Query_Protection	306.4 M	263.3 G
SYN_Insuffient_Reverse_Detection	244.9 M	211.8 G
GeoIP	22 M	19.8 G
HTTP_Get_Protection	2.3 G	2 T
HTTP_Post_Protection	1 G	913.3 G

On the page shown in Figure 4-126, click **Custom**.

You can select the start time and end time of the dropped traffic trend graph as required. The unit is the day.

Figure 4-127 Custom dropped traffic trend graph



Defend Policy

Legend	Max Dropped	Total Dropped
Dropped	11.2 G	9.8 T
Invalid_TCP_Packet	195.1 M	170.1 G
DNS_Query_Protection	306.4 M	263.3 G
SYN_Insuffient_Reverse_Detection	244.9 M	211.8 G
GeoIP	22 M	19.8 G
HTTP_Get_Protection	2.3 G	2 T
HTTP_Post_Protection	1 G	913.3 G

4.5.7 Switching the Traffic Unit

By default, traffic is expressed in bps in the dropped traffic trend graph. On the page shown in Figure 4-118, you can select **pps** from the drop-down list in the upper-right corner of the **Policy Traffic** panel to display traffic data in pps.

4.5.8 Refreshing the Dropped Traffic Trend Graph

By default, the dropped traffic trend graph is automatically refreshed every 30 seconds in real-time mode. On the page shown in Figure 4-118, you can select **Never** from the **AutoFresh** drop-down list in the upper-right corner of the **Policy Traffic** panel. In this case, the trend graph can be refreshed only by manual clicking ⟳.

By default, the dropped traffic trend graph does not automatically refresh in historical mode. On the page shown in Figure 4-118, you can select **Every 5 min** from the **AutoFresh** drop-down list in the upper-right corner of the **Policy Traffic** panel. In this case, the trend graph will refresh every 5 minutes.

4.5.9 Downloading a Dropped Traffic Trend Report

On the page shown in Figure 4-118, you can click ⤓ in the upper-right corner of the **Policy Traffic** panel and then click HTML or PDF to download the traffic report in HTML or PDF format to a local disk drive. For details, see in section 4.1.4 Downloading a Report.

4.5.10 **Managing Filters**

Filters are provided for users to define objects of their concern, so that they can find monitored objects more conveniently. After being created, filters are displayed in the filter list. You can click a filter to view dropped traffic information of the object specified by the filter.

Any queried objects, such as a region, region IP group, ADS device, ADS-protected group, or IP address, can be configured as a filter. But **All** and **Default IP (Default)** cannot be configured as a filter. You can configure multiple filters.

The procedures for configuring and deleting a filter here are the same as those for creating and deleting a filter on the **Attack Events** tab page. For details, see section 4.4.10 Managing Filters.

5 Reports

You can view the following types of reports on ADS M:

- Built-in reports: include network traffic reports and DDoS attack reports.
- Custom reports: refer to the reports customized by users.

This chapter mainly covers:

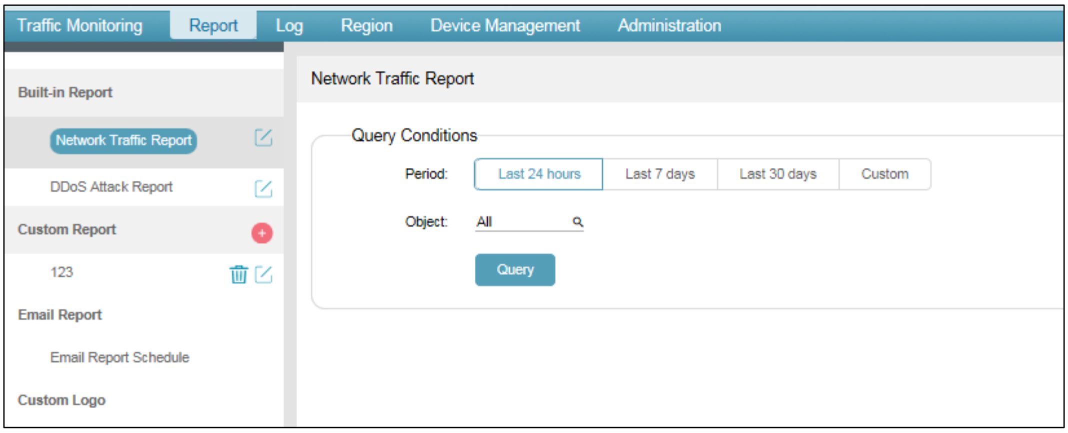
Section	Description
Built-in Report	Describes how to query and view built-in reports.
Custom Report	Describes how to create and manage custom reports.
Email Report	Describes how to configure ADS M to send reports via email.
Custom Logo	Describes how to customizes the report logo.

5.1 Built-in Report

You can query built-in reports and edit the logo image displayed in built-in reports.

Choose **Report > Built-in Report > Network Traffic Report**.

Figure 5-1 Network Traffic Report page



Querying a Report

After selecting a report type, you can query such type of reports in a specified period, which can be set to **Last 24 hours**, **Last 7 days**, **Last 30 days**, and **Custom**.

After setting **Period** and **Object**, click **Query**.

Reports meeting query conditions are displayed.

Editing a Report

You can edit the logo displayed in built-in reports. The procedure is as follows:

Step 1 Click ✎ next to **Network Traffic Report**.

The **Edit** dialog box appears.

Step 2 Point to the logo image.

Step 3 Click ▣ to view the big logo image.

Step 4 Select a logo image and then click **Confirm** to save the setting.

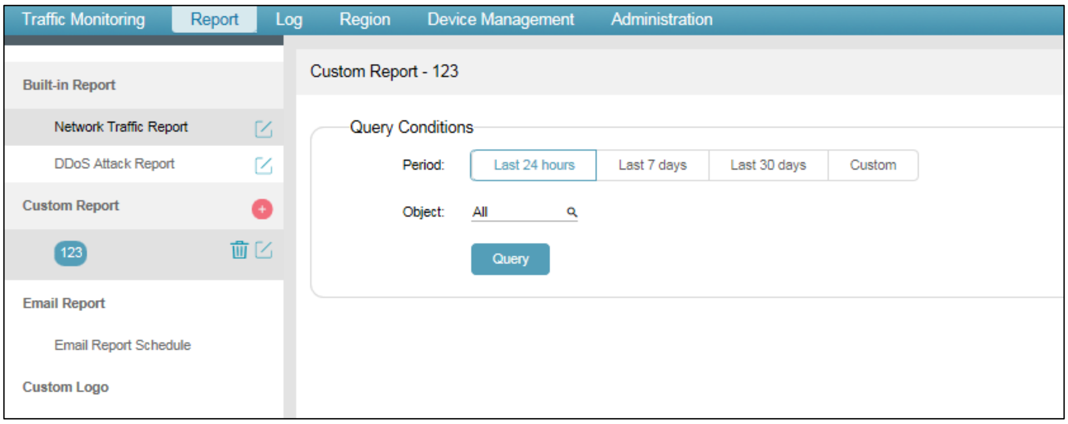
----End

5.2 Custom Report

You can create, query, edit, and delete custom reports.

Choose **Report > Custom Report**.

Figure 5-2 Custom Report page



Custom Report - 123

Query Conditions

Period: Last 24 hours | Last 7 days | Last 30 days | Custom

Object: All

Query

Creating a Custom Report

To create a custom report, follow these steps:

Step 1 Click ⊕ next to **Custom Report**.

Step 2 In the **Create** dialog box, set the parameters.

- Set the report name.
- Select report contents.
- Select a report logo.

Step 3 Click **Confirm** to save the settings.

----End

Querying a Custom Report

After selecting a custom report type, you can query such type of reports in a specified period, which can be set to **Last 24 hours**, **Last 7days**, **Last 30 days**, and **Custom**.

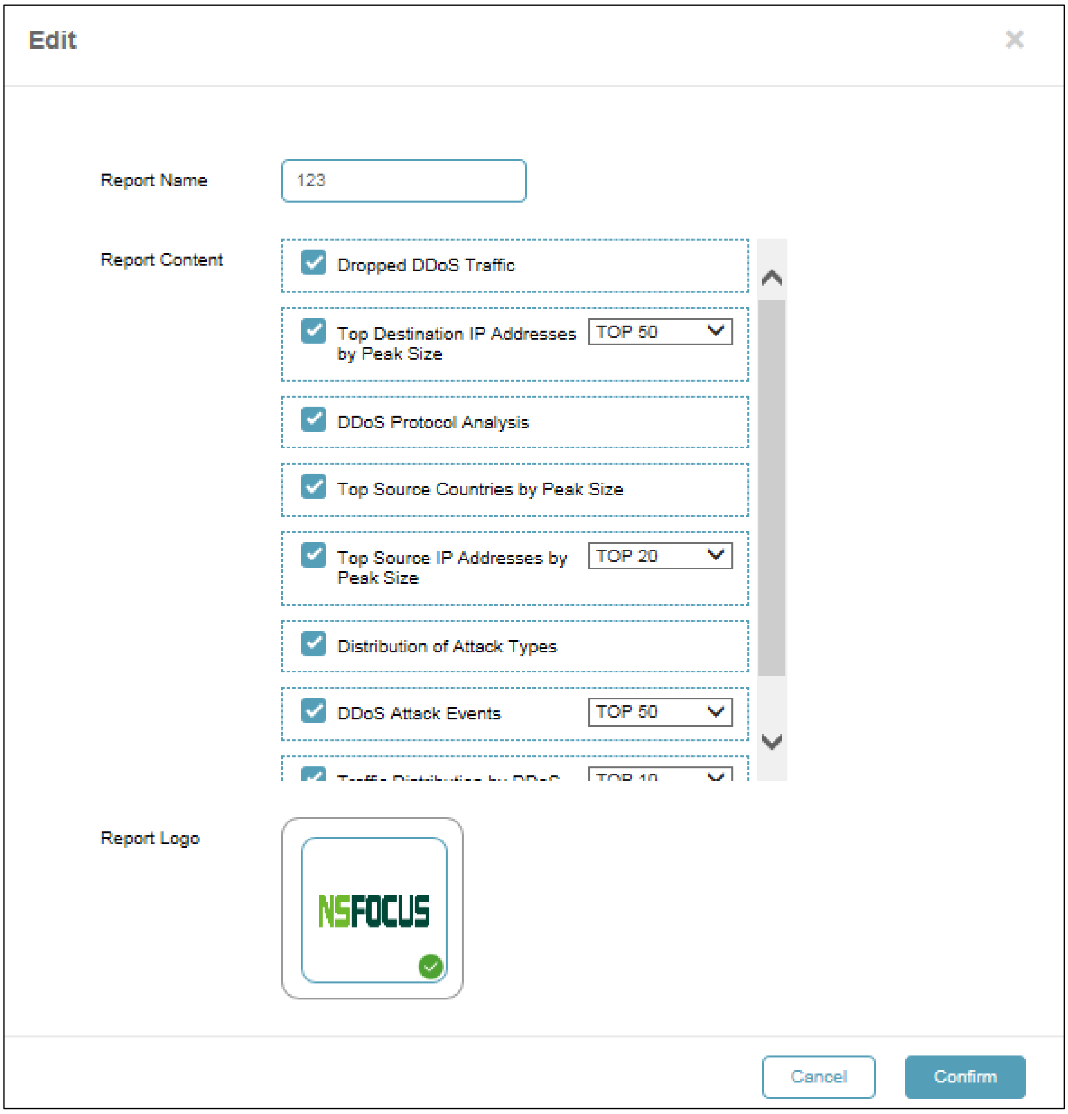
After setting **Period** and **Object**, click **Query**.

Reports meeting query conditions are displayed.

Editing a Custom Report

You can edit the name, module, and logo of custom reports. Clicking ✎ next to a custom report displays the dialog box shown in Figure 5-3.

Figure 5-3 Editing a custom report



Report Name: 123

Report Content:

- ☑ Dropped DDoS Traffic
- ☑ Top Destination IP Addresses by Peak Size — TOP 50
- ☑ DDoS Protocol Analysis
- ☑ Top Source Countries by Peak Size
- ☑ Top Source IP Addresses by Peak Size — TOP 20
- ☑ Distribution of Attack Types
- ☑ DDoS Attack Events — TOP 50
- ☑ Traffic Distribution by DDoS — TOP 10

Report Logo: NSFOCUS

After editing the report name, report contents, and report log, click **Confirm** to save the settings.

Deleting a Custom Report

You can click 🗑 next to a custom report and then click **Confirm** in the confirmation dialog box to delete this custom report.

5.3 Email Report

Note

Before configuring an email report, you must configure the SMTP server under **Administration** > **Third-Party Interface** > **SMTP Server Configuration**. For details, see section 3.3.5 SMTP Server Configuration.

Configuring an email report sending schedule includes configuration of **Email Address**, **Report**, **Report Language**, and **Report Type**.

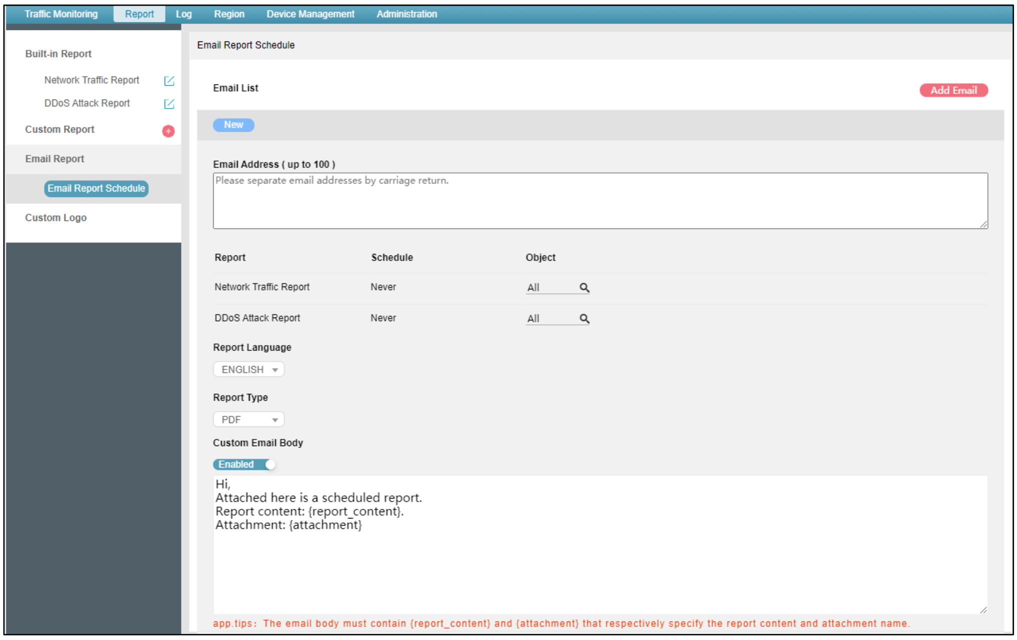
You can create, edit, enable/disable, and delete email report sending schedules.

Creating an Email Report Sending Schedule

Step 1 Choose **Report** > **Email Report** > **Email Report Schedule**.

Step 2 Click **Add Email**.

Figure 5-4 Creating an email report sending schedule



Email Address (up to 100)

Please separate email addresses by carriage return.

Report	Schedule	Object
Network Traffic Report	Never	All
DDoS Attack Report	Never	All

Report Language

ENGLISH

Report Type

PDF

Custom Email Body

Enabled

Hi,
Attached here is a scheduled report.
Report content: {report_content}.
Attachment: {attachment}

app.tips: The email body must contain {report_content} and {attachment} that respectively specify the report content and attachment name.

Step 3 Configure parameters.

Table 5-1 Parameters for configuring an email report sending schedule

Parameter	Description
Email Address	Specifies the email addresses to which reports will be sent.
Report	You can set **Schedule** and **Object** to specify how reports will be sent.

Parameter	Description
	- **Schedule**: specifies the interval at which reports are sent. Options include **Daily**, **Weekly**, **Monthly**, and **Never**. - **Object**: For traffic monitoring reports and attack event reports, data of all objects is collected by default. If you want reports to provide data regarding only a specific object, you must specify this object by doing as follows: Type a string under **Object** and then select the desired one from the objects containing the string.
Report Language	Specifies the language of reports to be sent, which can be English and Simplified Chinese.
Report Type	Specifies the format of reports to be sent, which can be **PDF**, **HTML**, and **WORD**.
Custom Email Body	Controls whether to type the email body text.

Step 4 Click **Save Changes** to save the settings.

The newly created email sending schedule will be displayed in the email list and is enabled by default.

----End

Editing an Email Report Sending Schedule

On the **Email Report Schedule** page, clicking an email address in the email list expands the email report sending schedule. You can edit parameters as required (for parameter description, see Table 5-1) and then click **Save Changes** to save the settings.

Enabling/Disabling an Email Report Sending Schedule

On the **Email Report Schedule** page, you can click Disabled / Enabled in the row of an email address to enable/disable this email report sending schedule.

Deleting an Email Report Sending Schedule

On the **Email Report Schedule** page, clicking an email address in the email list expands the email report sending schedule. You can click **Delete Email** to delete this email report sending schedule.

5.4 Custom Logo

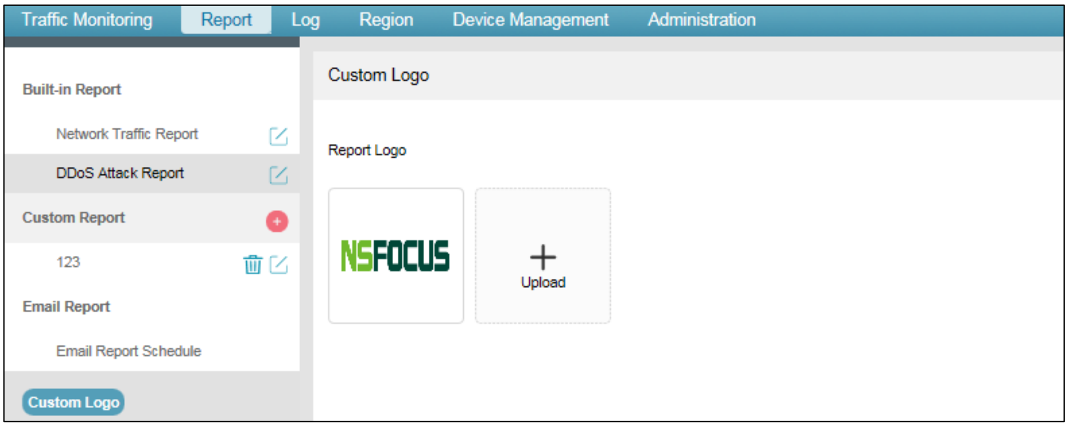
You can upload, view, and delete custom logos.

Uploading a Custom Logo

You can upload a logo image for use in the generated reports.

Step 1 Choose **Report** > **Custom Logo**.

Figure 5-5 Custom Logo page



Step 2 Click and then select the logo image to be uploaded.

----End

Viewing a Custom Logo

Pointing to the logo image displays the icon . You can click to view the big logo image.

Deleting a Custom Logo

You can delete uploaded logo images but not the built-in one.

Pointing to a custom logo displays . You can click and then **Confirm** in the confirmation dialog box to delete this custom logo.

6 Logs

Device logs can be queried and exported. You can set query conditions to view logs online and export logs.

- Querying logs

  After setting query conditions, click **Search** to generate desired logs.
- Exporting logs

  After setting log export conditions, click **Export** to save logs to the local disk drive.

This chapter mainly covers:

Section	Description
Attack Summary Log	Describes how to query and export attack summary logs.
Login Log	Describes how to query and export login logs.
Operation Log	Describes how to query and export operation logs.
Link Status Log	Describes how to query and export link status logs.
Diversion Log	Describes how to query and export diversion logs.
Performance Log	Describes how to query and export performance logs.
Performance Alert Log	Describes how to query and export performance alert logs.
HA Log	Describes how to query and export HA logs.
Traffic Alert Log	Describes how to query and export traffic alert logs.
Cloud Authentication Log	Describes how to query and export cloud authentication logs.
FlowSpec Diversion Log	Describes how to query and export FlowSpec diversionlogs.
NTA Running Log	Describes how to query and export NTA running logs.
ADS Authorization Log	Describes how to query and ADS authorization logs.
Local Authentication Log	Describes how to query and export local authentication logs.
ADS Web API Log	Describes how to query and export web API logs.

6.1 Attack Summary Log

Choose **Log** > **Attack Summary Log** to open the **Attack Summary Log** page.

You can set specific conditions to query or export logs of attacks detected and defended against by all devices in the device list.

Table 6-1 describes parameters of attack summary logs.

Table 6-1 Parameters of attack summary logs

Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Device	Specifies the device whose logs are queried. **All** indicates that logs on all devices are queried.
Attack Type	Specifies the attack type of logs to be queried. If you cannot determine what the attack type is, select **Any**.
Source IP	Specifies the IP address of the attack source.
Source Port	Specifies the port where attacks occur.
Destination IP	Specifies the IP address that suffers attacks.
Destination Port	Specifies the port that suffers attacks.

6.2 Login Log

Choose **Log** > **Login Log** to open the **Login Log** page.

You can set specific conditions to query or export login logs of all devices in the device list.

Table 6-2 describes parameters of login logs.

Table 6-2 Parameters of login logs

Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Device	Specifies the device whose logs are queried. **All** indicates that logs on all devices are queried.
Username	Specifies the login user name. The full user name is required because fuzzy query is not allowed here.
User IP	Specifies the IP address of the user device. The full IP address is required because fuzzy query is not allowed here.

6.3 Operation Log

Choose **Log** > **Operation Log** to open the **Operation Log** page.

You can set specific conditions to query or export operation logs of all devices in the device list.

6.4 Link Status Log

Link status logs refer to connection and disconnection state logs at the interface of ADS M, that is, the records of states from Up to Down or from Down to Up.

Choose **Log** > **Link Status Log** to open the **Link Status Log** page.

You can set specific conditions to query or export all link status logs of all devices in the device list.

6.5 Diversion Log

Traffic diversion is logged only after you configure ADS diversion parameters.

Choose **Log** > **Diversion Log** to open the **Diversion Log** page.

You can set specific conditions to query or export all diversion information of all devices in the device list. The log information includes:

- Automatic diversion information
- Manual diversion information
- Diversion information generated during hierarchical coordination of ADS devices

6.6 Performance Log

Choose **Log** > **Performance Log** to open the **Performance Log** page.

You can set specific conditions to query or export all performance logs of all devices in the device list. The log information includes:

- Device name
- Generation time
- CPU usage
- Memory usage

6.7 Performance Alert Log

Choose **Log > Performance Alert Log** to open the **Performance Alert Log** page.

You can set specific conditions to query or export performance alert logs reported by ADS M and managed ADS and NTA devices. The alerts include CPU usage alerts, memory usage alerts, ADS/NTA device offline alerts, and ADS M's HA alerts. The log information includes:

- Device IP
- Generation time
- Device type
- Alert type
- Severity
- Description

Note	If **NTP Exception Log** is set to **Open** under **Administration > Local Settings > Performance Alert Config of Managed Devices**, NTP exception logs are also displayed here.

Table 6-3 describes parameters of performance alert logs.

Table 6-3 Parameters of performance alert logs

Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Device	Device whose logs are queried. **All** indicates that logs on all devices are queried.
Alert Type	Alert type, which could be **Any**, **CPU usage**, **Memory usage**, **Disk usage**, **Device offline**, **HA alert**, **Data backup**, **CPU temperature**, **Mainboard temperature**, and **Fan status**. **Any** indicates that alerts of all types are queried.
Severity	Alert severity, which could be **Any**, **High**, **Medium**, or **Low**. **Any** indicates that alerts of all severities are queried.

6.8 HA Log

When the master and slave devices synchronize information such as configuration files and engine exceptions, ADS M will record such synchronization in HA logs, for further analysis and conclusion.

Choose **Log > HA Log** to open the **HA Log** page.

Table 6-4 describes parameters of HA logs.

Table 6-4 Parameters of HA logs

Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Device	Type of devices, which can be **ADS M** or **ADS**, indicating that HA logs on ADS M or ADS devices will be displayed.
Event Type	HA event type, which could be **Any**, **HA Start**, **HA Stop**, **Synchronize Configuration File**, **Update HA Configuration**, or **Exception**. **Any** indicates that logs of all event types are queried.
Operation Result	Operation result, which could be one of the following: • **Succeeded**: indicates that all logs about succeeded operations are queried. • **Failed**: indicates that all logs about failed operations are queried. • **Any**: indicates that logs with any results are queried.

6.9 Traffic Alert Log

The **Traffic Alert Log** page can be displayed only when **Detection Mode** is set to **NTA** on the **Basic Settings** page. For the configuration of the detection mode, see section 3.1.1 Basic Settings.

Choose **Log** > **Traffic Alert Log** to open the **Traffic Alert Log** page.

You can set specific conditions to query or export all traffic alert logs of all NTA devices. The log information includes:

- Alert ID
- Alert type
- Severity
- Attacked IP address
- Region
- Attack time (including the start time, end time, and duration)
- Description

  The description is usually instantaneous traffic in the unit of pps and bps when the alert is generated. If the alert persists, the description information will be updated accordingly. If the traffic of the attacked IP address is being diverted or filtered, words such as being diverted or being filtered will be displayed in the **Description** column.

Table 6-5 describes parameters of traffic alert logs.

Table 6-5 Parameters of traffic alert logs

Parameter	Description
Status	Specifies the status of alerts to be queried, which can be set to one of the following:

Parameter	Description
	• **Ongoing**: indicates alerts that are occurring. • **Ended**: indicates alerts that are over. • **Any**: indicates all generated alerts.
Time	Specifies the query time range. The default value is **Today**, that is, logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range.. **Custom** indicates that you can query logs in a specified time range.
Severity	Specifies the alert severity, which can be set to **High**, **Medium**, and **Low**. **Any** indicates that alerts of all severities are queried.
Object	• **Global**: indicates that alerts generated by all NTA devices are queried. • **By device**: indicates that alerts generated by an NTA device are queried.
Device	This option is available only when **Object** is set to **By device**. NTA devices added on ADS M will be displayed here. For NTA configuration, see section 9.3 Managing NTA Devices.
Alert Type	Specifies the type of alert events that can be reported by NTA devices to ADS M. **Any** indicates that alerts of all types are queried.
Region	Specifies the region where alerts are queried. New regions on ADS M are also displayed here. For region configuration, see section 7.3 Configuring a Region. **Any** indicates that alerts in all regions are queried.
Alert ID	Specifies the alert ID. The alert ID is reported by the NTA device to ADS M. This alert ID is the same as that on the NTA.
Attacked IP	Specifies the IP address that suffers attacks.

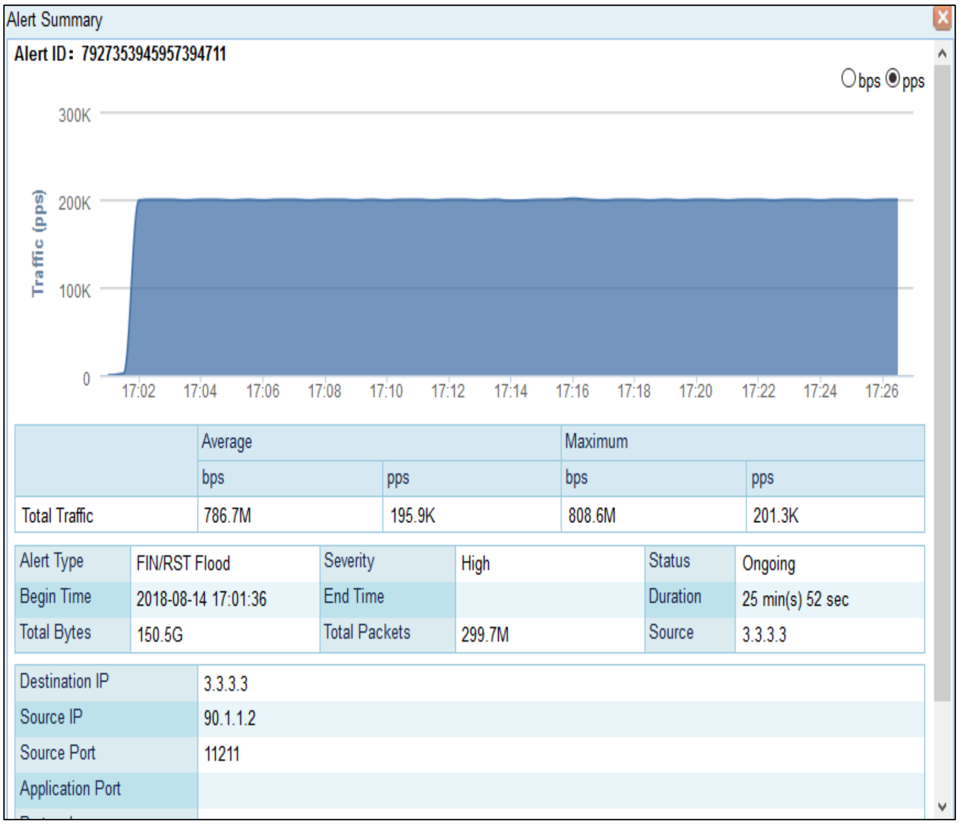
Click 📈 in the query results to open the **Alert Summary** page, as shown in Figure 6-1. This page displays detailed information of this alert, including:

- Traffic trend graph
- Average total traffic
- Maximum total traffic
- Other alert information

If the query time range is over three hours, the system displays the traffic trend only in three hours. You can select **bps** or **pps** to view the trend of abnormal traffic in pps or bps or click **Delete** in the lower-right corner of this page to delete this alert record.

⚠ Caution	After you click **Delete**, the alert record is deleted from the database, and cannot be restored. Perform this operation with caution.

Figure 6-1 Alert summary



Alert Summary

Alert ID: 7927353945957394711

○bps ●pps

	Average		Maximum	
	bps	pps	bps	pps
Total Traffic	786.7M	195.9K	808.6M	201.3K

Alert Type	FIN/RST Flood	Severity	High	Status	Ongoing
Begin Time	2018-08-14 17:01:36	End Time		Duration	25 min(s) 52 sec
Total Bytes	150.5G	Total Packets	299.7M	Source	3.3.3.3

Destination IP	3.3.3.3
Source IP	90.1.1.2
Source Port	11211
Application Port	

6.10 Cloud Authentication Log

The **Cloud Authentication Logs** page is available only when an ADS M virtual machine is used. For how to configure cloud authentication, see section 3.1.2 License.

Choose **Log > Cloud Authentication Log**s to open the **Cloud Authentication Logs** page appears.

Table 6-6 describes parameters of cloud authentication logs.

Table 6-6 Parameters of cloud authentication logs

Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Operation Result	Operation result, which could be one of the following: • **Successful**: indicates that logs of successful activation or authentication are queried. • **Failed**: indicates that logs of failed authentication are queried. • **Any**: indicates that all logs are queried.

6.11 FlowSpec Diversion Log

Choose **Log** > **FlowSpec Diversion Log** to open the **FlowSpec Diversion Log** page. You can set specific conditions to query or export all traffic FlowSpec diversion logs of devices managed by ADS M. The log information includes:

- Device
- Generation time
- Diversion event name
- Alert ID
- Region/IP group
- Protocol
- Source network segment
- Source port
- Destination network segment
- Destination port
- Details

Table 6-7 describes parameters of FlowSpec diversion logs.

Table 6-7 Parameters of FlowSpec diversion logs

Parameter	Description
Device	Device whose logs are queried. **Any** indicates that logs on all devices are queried.
Date	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Operation Result	Operation result, which could be one of the following: • **Succeeded**: indicates that all logs about succeeded cloud activation or authentication operations are queried. • **Failed**: indicates that all logs about failed cloud activation or authentication operations are queried. • **Any**: indicates that logs with any results are queried.
Alert ID	Specifies the alert ID.
Name	Name of the diversion event to be queried.
Destination IP	Destination IP address of the diversion to be queried.

6.12 NTA Running Log

Choose **Log > NTA Running Log** to open the **NTA Running Log** page.

You can set specific conditions to query or export all running logs of all NTA devices. The log information includes:

- Device IP

- Generation time
- Source
- Description

Table 6-8 describes parameters of NTA running logs.

Table 6-8 Parameters of NTA running logs

Parameter	**Description**
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Device	Device whose logs are queried. **All** indicates that logs on all devices are queried.
Source	Specifies the log source. **Any** indicates that logs from any sources are queried.
Description	Description of keywords of the logs to be queried.

6.13 ADS Authorization Log

Choose **Log > ADS Authorization Log** to open the **ADS Authorization Log** page.

You can set specific conditions to query or export all logs for cloud authorization and local authorization of ADS devices subject to management of ADS M. The log information includes:

- Device IP
- Generation time
- Type
- Status
- Description

Table 6-9 describes parameters of ADS authorization logs.

Table 6-9 Parameters of ADS authorization logs

Parameter	**Description**
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range.
Device	Device whose logs are queried. **All** indicates that logs on all devices are queried.
Status	Specifies the authorization status to be queried. **Any** indicates that all authorization logs are queried.
Description	Description of keywords of the logs to be queried.

6.14 Local Authentication Log

The **Local Authentication Log** page is available only when ADS-M-VM is used. For how to configure local authentication, see section 3.1.2 License. Choose **Log > Local Authentication Log** to open the **Local Authentication Log** page.

Table 6-10 describes parameters for querying logs for local authentication.

Table 6-10 Parameters for querying logs for local authentication

Parameter	Description
Time	Specifies the query time range. The default value is **Today**, indicating that logs of the current day are queried. Other options include **By date**, **By month**, and **Custom**. **Custom** indicates that you can query logs in a specified time range.
Operation Result	Results of local authentication. • **Succeeded**: indicates that logs about successful local activation or authentication are queried. • **Failed**: indicates that logs for failed local authentication are queried. • **Any**: indicates that all logs for local authentication are queried.

6.15 ADS Web API Log

ADS M can receive, save, and display ADS's web API logs.

Choose **Log > ADS Web API Log**. You can set specific conditions to query or export all logs generated by third-party management platforms calling ADS's web APIs to perform operations.

7 Region Management

A region is a collection of one or more ADS-protected hosts that work at the same geographical region or have some characteristics in common. Traffic of hosts in a region is displayed as a whole. Region management enables the administrator to perform corresponding deployment and management tailored to different requirements.

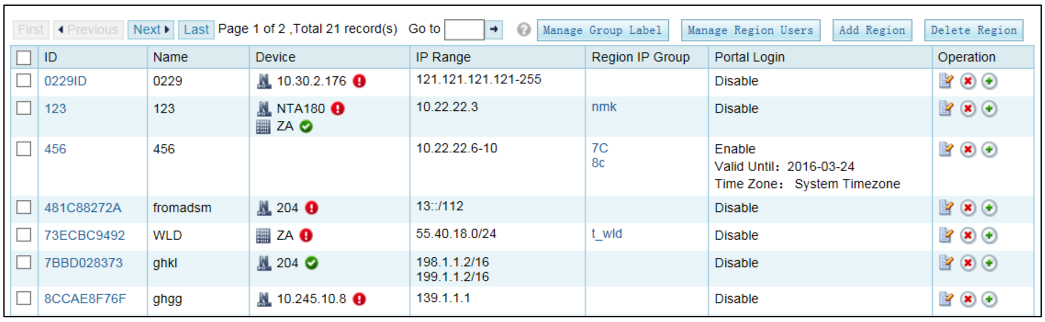
Section	Description
Managing Group Labels	Describes how to add, edit, and modify group labels.
Managing Region Managers	Describes how to manage region managers and configure their permissions.
Configuring a Region	Describes how to configure a region.
Configuring a Regional IP Group	Describes how to configure a regional IP group.
Configuring an NTA Global Policy	Describes how to configure a diversion allowlist.
Configuring Traffic Diversion for a Region	Describes how to check the region whose traffic is diverted and configure to divert the traffic of certain IP addresses.
Configuring an ADS Protection Policy Template	Describes how to configure an ADS protection policy template.
Configuring an NTA Policy Template	Describes how to configure an NTA policy template.

7.1 Managing Group Labels

ADS M supports grouped management of regions. A group label identifies one or more regions, facilitating region classification.

Choose **Region** > **Region Management**.

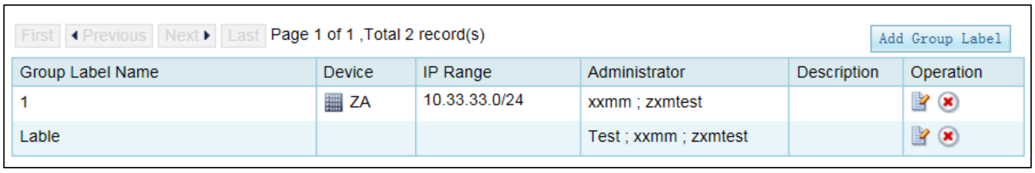
Figure 7-1 Region list



□	ID	Name	Device	IP Range	Region IP Group	Portal Login	Operation
□	0229ID	0229	10.30.2.176	121.121.121.121-255		Disable	
□	123	123	NTA180 ZA	10.22.22.3	nmk	Disable	
□	456	456		10.22.22.6-10	7C 8c	Enable Valid Until：2016-03-24 Time Zone： System Timezone	
□	481C88272A	fromadsm	204	13::/112		Disable	
□	73ECBC9492	WLD	ZA	55.40.18.0/24	t_wld	Disable	
□	7BBD028373	ghkl	204	198.1.1.2/16 199.1.1.2/16		Disable	
□	8CCAE8F76F	ghgg	10.245.10.8	139.1.1.1		Disable	

Click **Manage Group Label**.

Figure 7-2 Group label management page



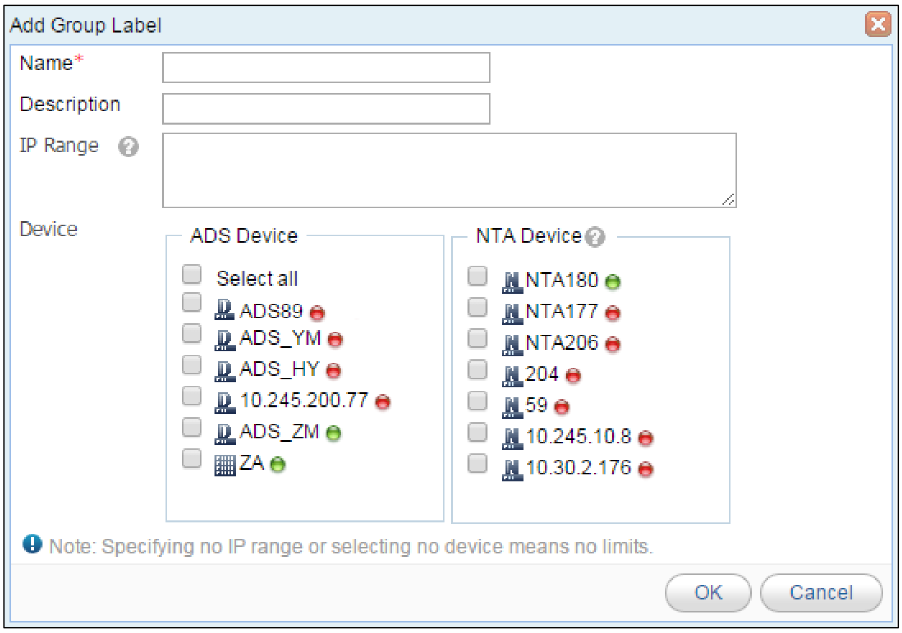
Group Label Name	Device	IP Range	Administrator	Description	Operation
1	ZA	10.33.33.0/24	xxmm ; zxmtest		
Lable			Test ; xxmm ; zxmtest		

You can create, edit, and delete a group label.

7.1.1 Creating a Group Label

Click **Add Group Label** on the page shown in Figure 7-2.

Figure 7-3 Creating a group label



Add Group Label

Name*

Description

IP Range

Device

ADS Device

□ Select all
□ ADS89
□ ADS_YM
□ ADS_HY
□ 10.245.200.77
□ ADS_ZM
□ ZA

NTA Device

□ NTA180
□ NTA177
□ NTA206
□ 204
□ 59
□ 10.245.10.8
□ 10.30.2.176

Note: Specifying no IP range or selecting no device means no limits.

Table 7-1 describes parameters for creating a group label.

Table 7-1 Parameters for creating a group label

Parameter	Description
Name	Name of the group label, which cannot be the same as an existing one or the name of a region.
Description	Brief description of the group label.
IP Range	IP address range under this group label. Both IPv4 and IPv6 addresses are accepted. You can type one or more IP addresses, IP address ranges, and IP segments, with each in a separate line. A maximum of 4096 entries are allowed.
Device	ADS and NTA devices that are assigned this group label. Only the devices that are managed by ADS M are available for you to select.

7.1.2 Editing a Group Label

In the group label list shown in Figure 7-1, click 📝 in the **Operation** column to edit a group label.

7.1.3 Deleting a Group Label

In the group label list shown in Figure 7-1, click ⊗ in the **Operation** column to delete a group label.

Caution

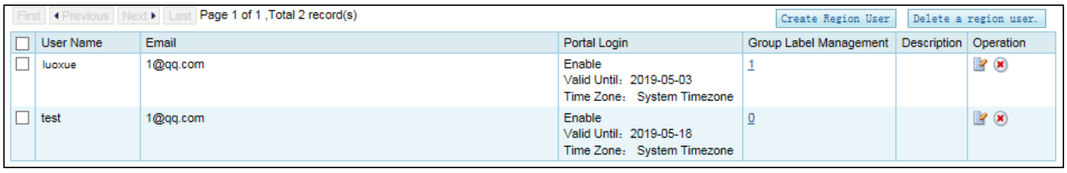
Deleting a group label will delete the region that references this label and all IP groups in the region. Also, this operation will make it impossible for a region user to log in to the enabled Portal system.

7.2 Managing Region Managers

A region manager for whom the Portal is enabled can create or edit regions on the Portal.

In the group label list shown in Figure 7-1, click **Manage Region Users** in the upper-right corner. The list of region managers appears.

Figure 7-4 List of region managers



Page 1 of 1 ,Total 2 record(s)

□	User Name	Email	Portal Login	Group Label Management	Description	Operation
□	luoxue	1@qq.com	Enable Valid Until：2019-05-03 Time Zone： System Timezone	1		📝 ⊗
□	test	1@qq.com	Enable Valid Until：2019-05-18 Time Zone： System Timezone	0		📝 ⊗

You can create, edit, or delete region managers.

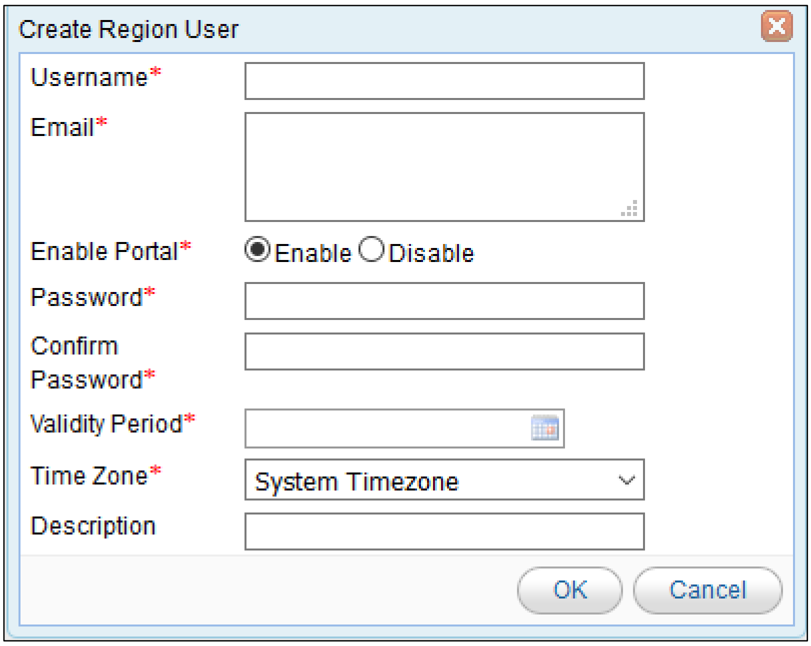
7.2.1 Creating a Region Manager

On the **Manage Region Users** page shown in Figure 7-4, click **Create Region User** in the upper-right corner to create a region manager.

As long as the Portal is enabled (under **Administration > Third-Party Interface > Portal Configuration**), Portal-related settings appear when you create or edit a manager for this region. You can determine whether to enable the Portal for this manager. If the Portal is enabled, you also need to set the Portal login password, validity period, and time zone.

Only the region manager with Portal enabled and assigned a group label can log in to the Portal client for region management. For details about the Portal, see the *NSFOCUS ADS Portal User Guide*.

Figure 7-5 Creating a region manager



Create Region User

Username*

Email*

Enable Portal* ● Enable ○ Disable

Password*

Confirm Password*

Validity Period*

Time Zone* System Timezone

Description

Table 7-2 describes parameters for creating a region manager.

Table 7-2 Parameters for creating a region manager

Parameter	Description
Username	Account name of this region manager. It cannot be the same as an existing region manager account name or region ID.
Email	Email address of this region manager.
Enable Portal	Controls whether to enable Portal to allow access to the Portal.
Password	Specifies the password for login to the web-based manager of the Portal. Note The password strength must be consistent with that specified in ADS M.

Parameter	Description
Confirm Password	Requires you to type the password again. The password you typed here must be the same as that you typed for **Password**.
Validity Period	Specifies how long the Portal account will be valid for use. After the validity period expires, this Portal account will be invalid.
Time Zone	Specifies the time zone that the Portal account belongs to. Note The time zone configured here takes effect on Portal only after the Portal user log in again.
Description	Brief description of this region manager.

7.2.2 Configuring Permissions of a Region Manager

On the **Manage Region Users** page shown in Figure 7-4, you can click a number in the **Group Label Management** column of the region manager list to configure permissions of a region manager.

Table 7-3 describes parameters for configuring permissions of a region manager.

Table 7-3 Parameters for configuring permissions of a region manager

Parameter	Description
Group Label Name	Group label under which the region manager can manage settings of devices.
View data	Permission of viewing data of devices under the specified group label.
View policy	Permission of viewing policies applied to devices under the specified group label.
Configure policy	Permission of configuring policies for devices under the specified group label. Note Selecting this parameter will cause "View data" and "View policy" to be automatically selected.

7.2.3 Editing a Region Manager

On the region manager list, click 📝 in the **Operation** column to edit settings of a region manager.

7.2.4 Deleting a Region Manager

- On the region manager list, click ✖ in the **Operation** column to delete a manager.
- On the region manager list, select one or more region managers and click **Delete a region user** to delete the selected manager(s).

7.3 Configuring a Region

This section details the configuration method of all regions managed by ADS M, including how to create, modify and delete a region.

The method of configuring IP groups varies with the detection mode of ADS M (for the configuration of the detection mode, see section 3.1.1 Basic Settings):

- For the detection mode of **NTA**, you need to configure basic information, region traffic alert parameters, region DDoS alert parameters, and traffic diversion rules.
- For the detection mode of **None** or **Local**, you need to configure only basic information.

7.3.1 Creating a Region

For ADS M whose detection mode is set to **NTA**, follow these steps to create a region:

Step 1 On the **Region List** page shown in Figure 7-1, click **Add Region** in the upper-right corner.

The traffic statistics function is unavailable if an NTA device of the DPI type is selected on the **Basic Information** page.

Step 2 Configure basic information.

Table 7-4 Parameters for configuring basic information

Parameter	Description
Region ID	Uniquely identifies a region. It is automatically generated by the system and can be manually changed (note that you cannot change it when editing a region and it cannot be the same as an existing region ID or region user name) when you add a region. The region ID should be a string of 1 to 100 characters, consisting of English letters, digits, and/or underscores.
Region Name	Name of the region, which should be a string of 1 to 50 characters, consisting of English letters, digits, and/or underscores. The new region name cannot be the same as an existing one or the group label.
Email	Email address of the contact person of the region. You can type multiple email addresses, separated with the semicolon (;). Note Only the first 10 email addresses will be delivered to NTA devices. After **Send alert notification by mail** is selected, ADS M will periodically send region alerts to the email address of the contact person. For details about scheduling the sending of region alerts , see section 3.3.4 Mail Alert Settings.
Group Label	Specifies the label of the group to which the region belongs. Regions are displayed in hierarchical mode in the region tree in the left pane. Note You can also drag a region to a specific group label in the region tree in the left pane.
Region IP Range	Specifies the IP address range in the region monitored and protected by ADS M. Both IPv4 and IPv6 addresses are accepted. You can type one or more IP addresses,

Parameter	Description
	IP subnets, and IP segments, with each in a separate line. A maximum of 4096 entries are allowed. • IPv4 address format: 192.168.0.1, 192.168.0.1/24, or 192.168.0.1–254 • IPv6 address format: 2001::1-fffe, 2001::1-fffe/126, or 2001::1 An IP subnet can be a class B or class C IP subnet, containing up to 65,536 IP addresses. The prefix length of IPv4 addresses can be 16–32 and that of IPv6 addresses can be 1–128. Note For the addition of a region, ADS M does not support defining of the region based on router interfaces currently.
Contact	Contact person of the region.
Address	Fixed-line phone or mobile phone number of the contact person.
Region Description	Briefly describes service information of the region.
Alert Sending	Specifies the method of sending host alerts regarding the region. For details about scheduling the sending of region alerts or reports, see section 3.3.4 Mail Alert Settings.
Device	Specifies ADS and NTA devices for the region. Only devices that are managed by ADS M are available for you to select. Region information cannot be dispatched to ADS V4.5R89 or NTA V4.5R89. For NTA, you can select devices of either the DPI or DFI type, but cannot use both types at the same time. If no DPI devices are selected during the region creation, you cannot select this type of device when you edit the region.
NTA Region Alert Template	Specifies the region alert template to be used by NTA. For details, see section 7.8 Configuring an NTA Policy Template.

Step 3 Configure region traffic alert parameters.

After configuring basic information, click **Next** to open the **Region Traffic Alert** page.

Table 7-5 describes region traffic alert parameters.

Table 7-5 Region traffic alert parameters

Parameter	Description
Alert Latency Period	Specifies the maximum duration NTA must wait to generate an alert for the traffic between the value of **Latent Alert Threshold** and that of **Direct Alert Threshold**. The value ranges are 0–23 for the hour (**h**) and 0–59 for the minute (**m**). For the second (**s**), you can click ▲ or ▼ to set it to **0s** or **30s**.
Alert Holding Period	Specifies the time when an alert persists after the traffic rate falls below the value of **Direct Alert Threshold**, which indicates that the attack ends. This parameter is valid only for latent alerts. The value ranges are 0–23 for the hour (**h**) and 0–59 for the minute (**m**). For the second (**s**), you can click ▲ or ▼ to set it to **0s** or **30s**.
Alert Type	Specifies the type of region traffic alerts, which can be either of the following:

Parameter	Description
	• **Region Inbound Traffic Alert**: checks the total inbound traffic of the region. • **Region Outbound Traffic Alert**: checks the total outbound traffic of the region.
Detection Mode	Specifies the type of traffic based on which an alert is generated. It has the following values: • **Not detect**: indicates that NTA does not check whether inbound or outbound traffic is abnormal. • **Packets only**: indicates that an alert is generated when the traffic rate in pps is found to exceed the threshold. • **Bytes only**: indicates that an alert is generated when the traffic rate in bps is found to exceed the threshold. • **Both packets and bytes**: indicates that an alert is generated when the traffic rate in pps and that in bps are both found to exceed the thresholds. • **Either packets or bytes**: indicates that an alert is generated when either the traffic rate in pps or that in bps is found to exceed the threshold.
Latent Alert Threshold	Specifies the traffic rate threshold in bps or pps that triggers NTA to generate an alert only after the traffic rate stays at this level for some time. • **bps**: indicates a threshold in bps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **Not detect** or **Packets only** for **Detection Mode**. • **pps**: indicates a threshold in pps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **Not detect** or **Bytes only** for **Detection Mode**. Note The latent alert threshold must be lower than the direct alert threshold.
Direct Alert Threshold	Specifies the traffic rate threshold in bps or pps that triggers NTA to generate an immediate alert. • **bps**: indicates a threshold in bps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **Not detect** or **Packets only** for **Detection Mode**. • **pps**: indicates a threshold in pps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **Not detect** or **Bytes only** for **Detection Mode**. Note Note that the direct alert threshold must be greater than the latent alert threshold.
Alert Hierarchy(%)	Specifies how to classify alert levels. **Latent Alert Threshold** is a basis for classifying alert levels and needs to be configured in advance. Alert levels are classified according to the ratio of actual traffic to the **Latent Alert Threshold** value:

Parameter	Description
	• **Low**: specifies the lowest ratio for triggering a low-level alert. The value is always **100**. When the actual ratio falls between the smallest ratio for triggering a lower-level alert and the smallest ratio for triggering a medium-level alert, NTA generates a low-level alert. • **Medium**: specifies the ratio for triggering a medium-level alert. The default value is **150** and the maximum value is **10000**. When the actual ratio falls between the smallest ratio triggering a medium-level alert and the smallest ratio for triggering a high-level alert, NTA generates a medium-level alert. • **High**: specifies the ratio for triggering a high-level alert. The default value is **200** and the maximum value is **10000**. When the actual ratio is greater than the smallest ratio for triggering a high-level alert, NTA generates a high-level alert. If **Alert Hierarchy** is not configured, NTA will detect traffic and send alerts according to the global alert hierarchy.
Diversion Level	Specifies the alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted. • **No diversion**: indicates that no traffic diversion will take place. • **Divert Traffic of Low-level Alert**: indicates that a low-level alert or higher will trigger traffic diversion. • **Divert Traffic of Medium-level Alert**: indicates that a medium-level alert or higher will trigger traffic diversion. • **Divert Traffic of High-level Alert**: indicates that only a high-level alert can trigger traffic diversion.

Step 4 Configure region DDoS alert parameters.

After configuring region traffic alert parameters, click **Next** to open the **Region DDoS Alert** page.

- **Region DDoS Alert Period Configuration**: Configure **Alert Latency Period** and **Alert Holding Period**. For specific configuration, see Table 7-5.
- **Region DDoS Alert**: Respectively configure **Inbound Check Configuration** and **Outbound Check Configuration**.
  - **Inbound Check Configuration**: Configure **Fixed Threshold Configuration** or **Constituent Proportion Configuration**. For details about parameter description of the former, see Table 7-5. To configure a constituent proportion, enable the function in the **Status Control** area, and configure alert parameters. If the traffic exceeds both **Min Trigger Threshold** and **Proportion for Direct Alerts**, the system directly generates an alert. For the configurations of other parameters, see Table 7-5.
  - **Outbound Check Configuration**: Configure **Constituent Proportion Configuration** after enabling this function.

Step 5 Configure the region traffic statistics function.

You can specify statistical items of traffic for the region and click **Save**. After that, click **Next** to configure region traffic diversion rules.

Step 6 Configure region traffic diversion rules.

Configure traffic diversion parameters on the **Traffic Diversion Rule** page after you configure the traffic statistics function and click **Next**.

Table 7-6 describes parameters for configuring traffic diversion rules.

Table 7-6 Parameters for configuring traffic diversion rules

Parameter		Description
Region Diversion Policy	Number of Inbound-Traffic diverted IPs in Region	Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 300. When **Diversion Policy for Abnormal Region Inbound Traffic** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses.
	Diversion Policy for Abnormal Region Inbound Traffic	Specifies the diversion policy for inbound traffic of top N IP addresses when the inbound traffic alert is triggered. • The **Diversion Policy for Abnormal Region Inbound Traffic** can be triggered together with the **Diversion Policy for Abnormal Outbound Region Traffic** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. Note The diversion policy for a region has a lower priority than that for an IP group. • You can click **Add** and create new diversion policies.
	Number of Outbound-Traffic diverted IPs in Region	Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 100. When **Diversion Policy for Abnormal Region Outbound Traffic** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses.
	Diversion Policy for Abnormal Region Outbound Traffic	Specifies the diversion policy for outbound traffic of top N IP addresses when the outbound traffic alert is triggered. • The **Diversion Policy for Abnormal Region Outbound Traffic** can be triggered together with the **Diversion Policy for Abnormal Region Inbound Traffic** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. Note The diversion policy for a region has a lower priority than that for an IP group. • You can click **Add** and create new diversion policies.
IP Diversion Policy		Specifies the diversion policy for IP addresses in a specific IP group when the DDoS alert is triggered. • The **IP Diversion Policy** can be triggered together with the **Diversion Policy for Abnormal Inbound IP Group Traffic** and **Diversion Policy for Abnormal Outbound IP Group Traffic**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. • You can click **Add** and create new diversion policies.

Step 7 Configuring the Portal.

After configuring traffic diversion rules, click **Next** to open the **Portal Configuration** page.

Table 7-7 describes the parameters for configuring the Portal.

Table 7-7 Parameters for configuring the Portal

Parameter	Description
Enable Portal	Controls whether to allow access to the Portal.
Password	Specifies the password for login to the web-based manager of the Portal. Note The password strength must be consistent with that specified in ADS M.
Confirm Password	Requires you to type the password again. The password you typed here must be the same as that you typed for **Password**.
Validity Period	Specifies how long the Portal account will be available. After the validity period expires, this Portal account will be invalid.
Time Zone	Specifies the time zone that the Portal account belongs to. Note The time zone configured on ADS M for the region takes effect and is displayed on the Portal only after the Portal user logs out and then logs in again. If a user directly configures the time zone on the Portal, the configuration takes effect immediately.

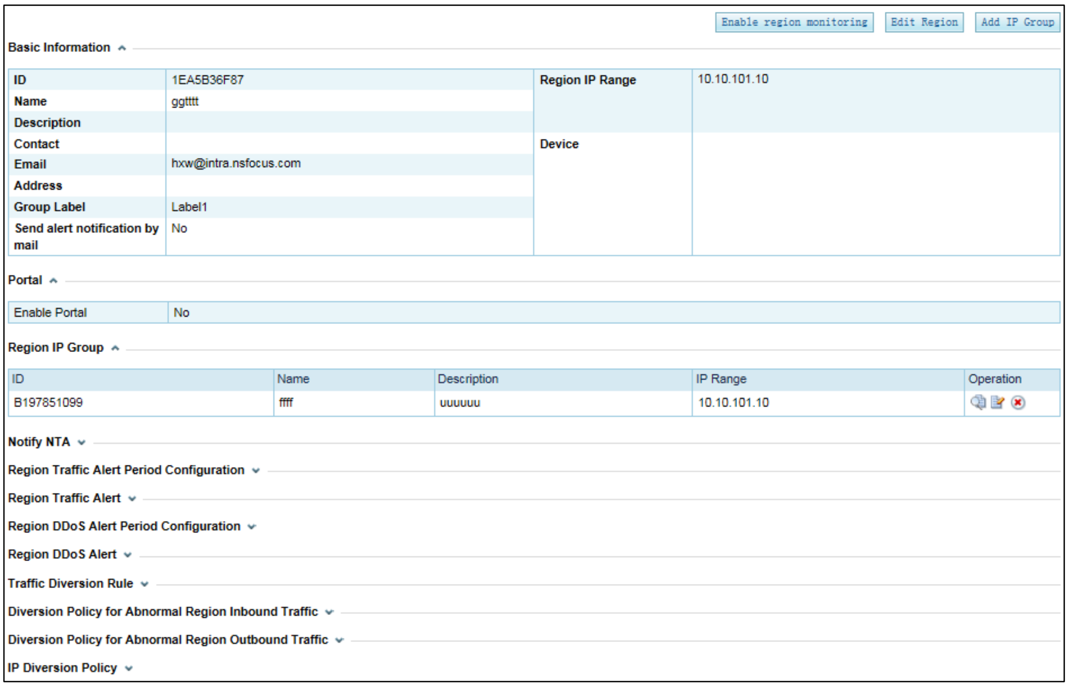
Step 8 After configuring traffic diversion rules, click **Finish**.

----End

7.3.2 Viewing Details of a Region

Choose **Region > Region Management** and select a region from the left region tree or click the ID of a region on the **Region List** page, as shown in Figure 7-6. Then details of the selected region appear.

Figure 7-6 Details of a region



Basic Information

ID	1EA5B36F87	Region IP Range	10.10.101.10
Name	ggtttt		
Description			
Contact		Device	
Email	hxw@intra.nsfocus.com		
Address			
Group Label	Label1		
Send alert notification by mail	No		

Portal

Enable Portal	No

Region IP Group

ID	Name	Description	IP Range	Operation
B197851099	ffff	uuuuuu	10.10.101.10	

Notify NTA

Region Traffic Alert Period Configuration

Region Traffic Alert

Region DDoS Alert Period Configuration

Region DDoS Alert

Traffic Diversion Rule

Diversion Policy for Abnormal Region Inbound Traffic

Diversion Policy for Abnormal Region Outbound Traffic

IP Diversion Policy

7.3.3 Editing a Region

On the region list, click 📝 in the **Operation** column to modify settings of a region. Alternatively, click a region ID on the region list and then click **Edit Region** to open the region editing page.

Note

- For a region dispatched by ADS M to NTA, it can be modified only on ADS M. Modifications made on NTA cannot be synchronized to ADS M.
- A region that has an IP group under intelligent protection cannot be edited.
- When editing basic region information, you can select or deselect NTA devices of current types, but cannot add devices of other types.

7.3.4 Deleting a Region

On the region list, click ☒ in the **Operation** column to delete a region. Or click **Delete Region** in the upper-right corner of the region list to delete the specified regions.

Caution

- Deleting a region stops you from continuing to view the opened monitoring page, configuration page, or other pages related to this region.
- If NTA devices are offline when you delete a region or the management password is different for ADS M and NTA devices, the deletion of this region removes the region only from ADS M rather than from NTA devices.
- A region that has an IP group under intelligent protection cannot be deleted.

7.4 Configuring a Regional IP Group

You can add a regional IP group for an existing region.

The method of configuring IP groups varies with the detection mode of ADS M (for the configuration of the detection mode, see section 3.1.1 Basic Settings):

- For the detection mode of **NTA**, you need to configure basic information, IP group traffic alert parameters, IP group DDoS alert parameters, IP group alert hierarchy parameters, traffic diversion rules, protection policies, and URL rule.
- For the detection mode of **None**, you need to configure basic information, protection policies, and URL rule.

7.4.1 Adding a Regional IP Group

7.4.1.1 NTA Detection Mode

Step 1 On the **Region List** page shown in Figure 7-1, click ⊕ in the **Operation** column to add an IP group for a region.

Alternatively, you can click **Add IP Group** on the page shown in Figure 7-6.

Step 2 Configure basic information of the IP group.

Table 7-8 Parameters for configuring basic information of an IP group

Parameter	Description
IP Group ID	Uniquely identifies an IP group. It is automatically generated by the system and can be manually changed (note that you cannot change it when editing an IP group and it cannot be the same as an existing one) when you add an IP group. The IP group ID should be a string of 1 to 50 characters, consisting of English letters, digits, and/or underscores.
IP Group Name	Name of the IP group, which should be a string of 1 to 50 characters, consisting of English letters, digits, and/or underscores.
IP Group IP Range	IP address range monitored and protected by ADS M. The IP address range can include one or more IP addresses, IP subnets, and IP segments. Each IP address or IP segment should be in a separate line. You can add up to 1024 entries. IP addresses in an IP group must be covered by the IP address range of the region. Otherwise, the system prompts you to change the range. Different IP groups in a region must contain different IP addresses. Otherwise, the system prompts you to change the range. When you type IP addresses, the IP range of the region to which the IP group belongs is dynamically displayed below the text box. Note A region can have a maximum of 64 IP groups, each of which can contain a maximum of 1024 entries.
IP Group Description	Brief description of the IP group. A maximum of 80 characters are allowed, including letters, digits, underscores, and hyphens only.
NTA IP Group Alert Template	Alert template of the IP group.

Parameter	Description
Notify NTA	Controls whether to send NTA diversion notifications, alert notifications, or SNMP trap messages.

Step 3 Configure IP group traffic alert parameters.

After configuring basic information, click **Next** to open the **IP Group Traffic Alert** page.

Parameter configuration here is the similar to that for a region. For the description of parameters, see Table 7-5.

Step 4 Configure IP group DDoS alert parameters.

After configuring IP group traffic alert parameters, click **Next** to open the **IP Group DDoS Alert** page.

- **IP Group DDoS Alert Period Configuration**: Configure **Alert Latency Period** and **Alert Holding Period**. For specific configuration, see Table 7-5.
- **IP Group DDoS Alert**: Respectively configure **Inbound Check Configuration** and **Outbound Check Configuration**.
  - **Inbound Check Configuration**: Configure **Fixed Threshold Configuration** and **Constituent Proportion Configuration**. For details about parameter description of the former, see Table 7-5. To configure a constituent proportion, enable the function in the **Status Control** area, and configure alert parameters. If the traffic exceeds both **Min Trigger Threshold** and **Proportion for Direct Alerts**, the system directly generates an alert. For the configurations of other parameters, see Table 7-5.
  - **Outbound Check Configuration**: Configure **Constituent Proportion Configuration** after enabling this function.

Step 5 Configure IP group traffic statistics.

After configuring IP group DDoS alter parameters, click **Next** to select the traffic data to collect.

Step 6 Configure IP group traffic diversion rules.

After configuring IP group traffic statistics parameters, click **Next** to open the **Traffic Diversion Rule** page.

Table 7-9 describes parameters for configuring traffic diversion rules for an IP group.

Table 7-9 Parameters for configuring diversion rules for an IP group

Parameter		Description
IP Group Diversion Policy	Number of Inbound Diversion IP in the IP Group	Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 300. When **Diversion Policy for Abnormal Inbound IP Group Traffic** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses or all IP addresses (**Any**) in an IP group.
	Diversion Policy for Abnormal Inbound IP Group Traffic	Specifies the diversion policy for inbound traffic of top N IP addresses or all IP addresses (**Any**) in an IP group when the inbound traffic alert is triggered.

Parameter		Description
		• The **Diversion Policy for Abnormal Inbound IP Group Traffic** can be triggered together with the **Diversion Policy for Abnormal Outbound IP Group Traffic** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. Note The diversion policy for a region has a lower priority than that for an IP group. • You can click **Add** to add new diversion policies.
	Number of Outbound Diversion IP in the IP Group	Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 100. When **Diversion Policy for Abnormal Outbound IP Group Traffic** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses.
	Diversion Policy for Abnormal Outbound IP Group Traffic	Specifies the diversion policy for outbound traffic of top N IP addresses in an IP group when the outbound traffic alert is triggered. • The **Diversion Policy for Abnormal Inbound IP Group Traffic** can be triggered together with the **Diversion Policy for Abnormal Outbound IP Group Traffic** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. Note The diversion policy for a region has a lower priority than that for an IP group. • You can click **Add** to add new diversion policies.
IP Diversion Policy		Specifies the diversion policy for IP addresses in a IP group when the DDoS alert is triggered. • **IP Diversion Policy** can be triggered together with the **Diversion Policy for Abnormal Inbound IP Group Traffic** and **Diversion Policy for Abnormal Outbound IP Group Traffic**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. • You can click **Add** to add new diversion policies.

Step 7 Configure IP group protection policies.

After configuring traffic diversion rules, click **Next** to open the **Policies** page.

To edit protection policies, you can directly modify default settings or use policy templates. The method of configuring policies on ADS M is the same as that for policies on ADS devices. For details, see the *NSFOCUS ADS User Guide*.

Step 8 Configure the IP group access policies.

After configuring the protection policies, click **Next** to open the **Access Policy** page and configure the access policies.

The configurations of access control rule, blocklist ("blacklist" on UI), NTI, and GeoIP rules are virtually the same as those on ADS. For details, see the *NSFOCUS ADS User Guide*.

Step 9 Configure URL rules.

After configuring the access rule, click **Next** to open the **URL Rule Configuration** page.

a. Click **Add**.

b. In the **Add Rule** dialog box, configure URL rule parameters.

Table 7-10 URL rule parameters

Parameter	Description
Domain Name or IP	Domain name or IP address of the server. The dot (.) indicates that this rule is valid for all domain names or IP addresses.
URL(Excluding domain name or IP)	Specifies the URL of a page on the server, with the domain name or IP address excluded. The dot (.) indicates that this rule is valid for all URLs.
Destination IP	IP address of the server. You can type an IPv4 or IPv6 address according to the actual network deployment.
Destination Port	Port of the server.
SYN Cookie URL	Controls whether to enable **SYN Cookie URL**.
Algorithm	Protection mode and policy adopted for packets matching URL protection rules. Protection modes include **Unified protection** and **Precision protection**. Nine algorithms are available for you to select.

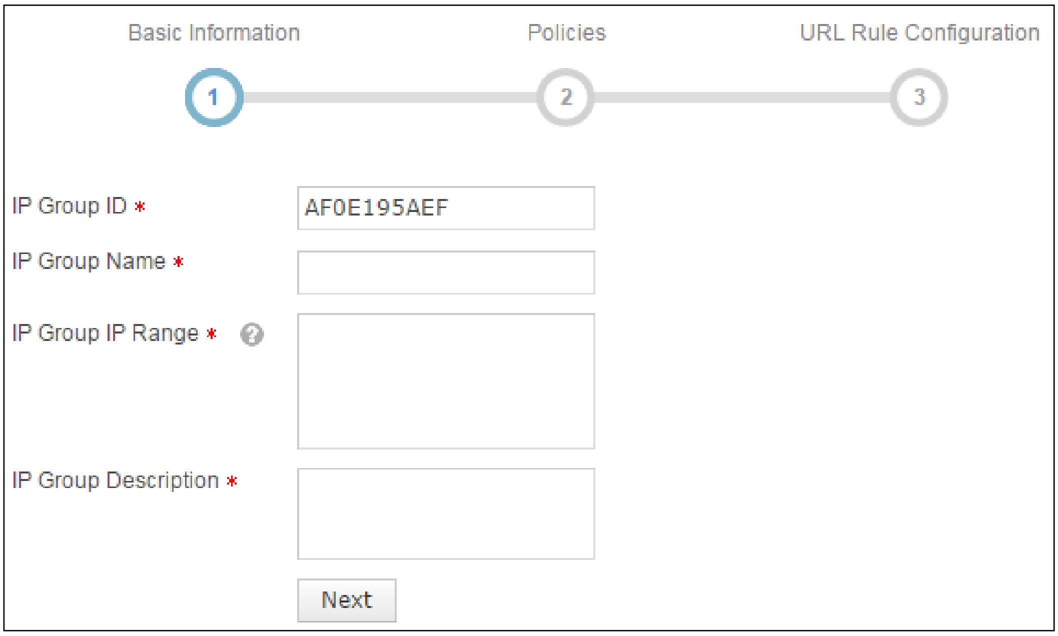
Step 10 After configuring the URL rule, click **OK**.

----End

7.4.1.2 "None" Detection Mode

Step 1 Click **Add IP Group** on the page shown in Figure 7-6.

Figure 7-7 Adding an IP group in "None" detection mode



IP Group ID * AF0E195AEF

IP Group Name *

IP Group IP Range *

IP Group Description *

Step 2 Configure basic information for adding an IP group.

For the description of parameters for configuring basic information, see Table 7-8.

Step 3 Configure IP group protection policies.

After configuring basic information, click **Next** to open the **Policies** page.

To edit protection policies, you can directly modify default settings or use policy templates. The method of configuring policies on ADS M is the same as that for policies on ADS devices. For details, see the *NSFOCUS ADS User Guide*.

Step 4 Configure the IP group access policies.

After configuring the protection policies, click **Next** to open the **Access Policy** page and configure the access policies.

The configurations of access control rule, blocklist ("blacklist" on UI), NTI, and GeoIP rules are virtually the same as those on ADS. For details, see the *NSFOCUS ADS User Guide*.

Step 5 Configure URL rules.

After configuring policies, click **Next** to open the **URL Rule Configuration** page.

For how to configure a URL rule, see Step 9 in section 7.4.1.1 NTA Detection Mode.

Step 6 After configuring the URL rule, click **Finish**.

----End

7.4.2 Modifying a Regional IP Group

On the regional IP group list, click 📝 in the **Operation** column of a regional IP group to modify parameters (except the IP group ID) of the regional IP group.

Note

- For regional IP groups dispatched by ADS M to ADS or NTA, they can be modified only from ADS M, but not on ADS or NTA. Even if you modify such IP groups on ADS or NTA, the modifications cannot be synchronized to ADS M.
- An IP group under intelligent protection cannot be edited.

7.4.3 Deleting a Regional IP Group

On the regional IP group list, click ✖ in the **Operation** column of a regional IP group to delete the IP group.

Caution

- Deleting a regional IP group stops you from continuing to view the opened monitoring page, configuration page, or other pages related to this group.
- If ADS or NTA devices are offline when you delete an IP group, the management password is different for ADS M and NTA devices, or the IP group is undergoing traffic diversion, the deletion of this IP group removes the group only from ADS M rather than from ADS or NTA devices.
- An IP group under intelligent protection cannot be deleted.

7.4.4 Viewing Configuration Information of a Regional IP Group

On the regional IP group list, click 🔍 in the **Operation** column of a regional IP group to view the configuration information of the IP group.

7.4.5 Configuring the Access Policies for a Regional IP Group

The access policies include access control rules, blocklist ("blacklist" on UI), NTI, and GeoIP rules.

- Access control rules: control traffic passing through the controlled device.
- Blocklist: filters source IP addresses of packets.
- GeoIP rules: control traffic from certain IP addresses based on geographic locations.
- NTI: controls whether to enable the NTI-based protection algorithm and the actions taken against packets matching the algorithm.

On the regional IP group list, click the respective rule in the **Access Policy** column to configure the access policies. For specific configuration, see the *NSFOCUS ADS User Guide*.

7.5 Configuring an NTA Global Policy

The NTA global policy refers to a diversion allowlist ("whitelist" on UI). After you add a specified IP address and IP range to the allowlist, traffic destined for it will not be diverted again.

Choose **Region** > **NTA Global Policy** > **Diversion Whitelist**. Click **Add** and configure parameters in the dialog box that appears. Table 7-11 describes parameters for configuring a diversion allowlist.

A diversion allowlist, after being created, can be queried, edited, and deleted.

Table 7-11 Parameters for configuring a diversion allowlist

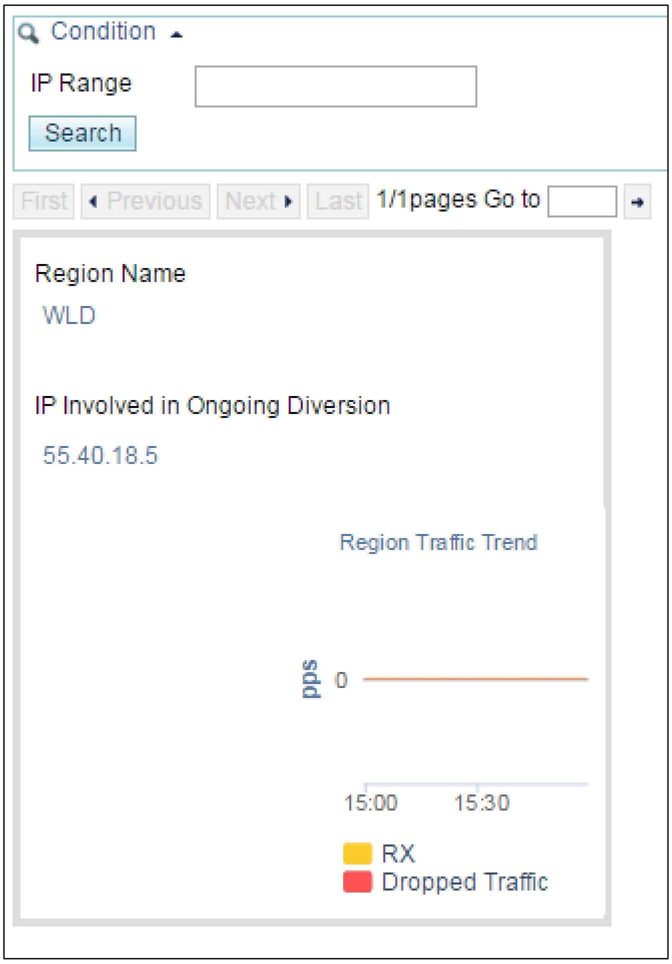
Parameter	Description
Name	Name of the diversion allowlist.
IP Range	Specifies the IP range that will not be diverted. Type one IP address, IP subnet, or IP segement per line, such as **192.168.1.0/24** or **192.168.1.0–200**.
Device	Specifies the devices that will not divert traffic destined for the allowed IP addresses.
Enable	Controls whether to enable the diversion allowlist. After it is enabled, traffic destined for allowed IP addresses will not be diverted.
Description	Other brief information of the diversion allowlist.

7.6 Configuring Traffic Diversion for a Region

You can check the ongoing traffic diversion and IP addresses whose traffic can be diverted in the region, and also manually divert the traffic of certain IP addresses.

Choose **Region > Traffic Diversion**. The page shown in Figure 7-8 displays the IP address under traffic diversion and the traffic trend of the region to which this IP address belongs. If no traffic diversion is happening currently, the system displays "No region is involved in traffic diversion."

Figure 7-8 Region traffic diversion



Region Name

WLD

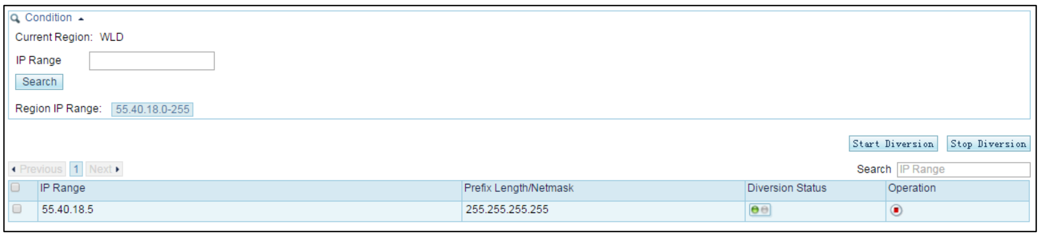
IP Involved in Ongoing Diversion

55.40.18.5

7.6.1 Viewing the Region Under Traffic Diversion

You can click the region name on the page shown in Figure 7-8 to view the IP address range of this region and the IP address under traffic diversion, as shown in Figure 7-9. Note that only the IP addresses within this region in question can be retrieved.

Figure 7-9 Viewing the region under traffic diversion



Current Region: WLD

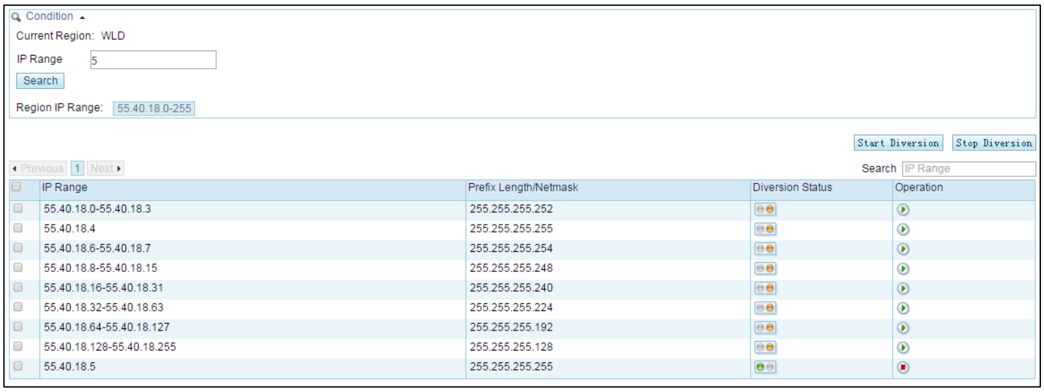
Region IP Range: 55.40.18.0-255

□	IP Range	Prefix Length/Netmask	Diversion Status	Operation
□	55.40.18.5	255.255.255.255	●	●

7.6.2 Configuring IP Addresses for Diversion

On the page shown in Figure 7-9, you can type an IP address range for query. Fuzzy query is supported. For example, if you type **5**, all IP addresses starting with this digit will be displayed.

Figure 7-10 Searching for IP addresses whose traffic can be diverted



Condition

Current Region: WLD

IP Range: 5

Search

Region IP Range: 55.40.18.0-255

□	IP Range	Prefix Length/Netmask	Diversion Status	Operation
□	55.40.18.0-55.40.18.3	255.255.255.252	○●	▶
□	55.40.18.4	255.255.255.255	○●	▶
□	55.40.18.6-55.40.18.7	255.255.255.254	○●	▶
□	55.40.18.8-55.40.18.15	255.255.255.248	○●	▶
□	55.40.18.16-55.40.18.31	255.255.255.240	○●	▶
□	55.40.18.32-55.40.18.63	255.255.255.224	○●	▶
□	55.40.18.64-55.40.18.127	255.255.255.192	○●	▶
□	55.40.18.128-55.40.18.255	255.255.255.128	○●	▶
□	55.40.18.5	255.255.255.255	●○	■

- Icons in the **Diversion Status** column are described as follows:
  - ⛔ : Traffic diversion is not supported.
  - ●○: Traffic diversion is ongoing.
  - ○● : Traffic diversion is supported, but no traffic is being diverted.
- Icons in the **Operation** column are described as follows:
  - ▶: starts traffic diversion.
  - ■ : stops traffic diversion.

Also, you can select multiple IP addresses and click **Start Diversion** to start traffic diversion for them, or click **Stop Diversion** to stop traffic diversion.

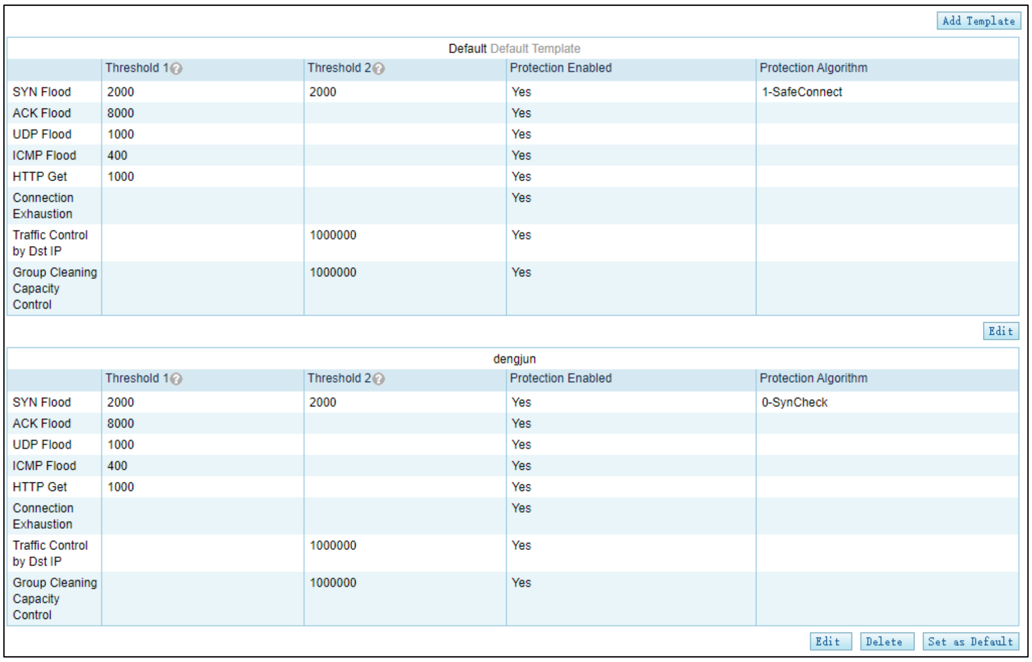
Note	To ensure successful traffic diversion, before starting diversion for an IP address on this page, make sure that the following items are properly configured for this IP address: routing daemon, IP route assignment, injection route, injection interface, and diversion filtering rule.

7.7 Configuring an ADS Protection Policy Template

The protection policies of ADS are used to detect and prevent DDoS attacks on ADS devices under centralized management. ADS M provides various policy templates and allows users to configure their own according to their particular business needs. A policy template can be assigned to multiple ADS devices.

Choose **Region > Policy Template > Anti-DDoS Policy**.

Figure 7-11 Anti-DDoS policy template



Default Default Template

	Threshold 1	Threshold 2	Protection Enabled	Protection Algorithm
SYN Flood	2000	2000	Yes	1-SafeConnect
ACK Flood	8000		Yes	
UDP Flood	1000		Yes	
ICMP Flood	400		Yes	
HTTP Get	1000		Yes	
Connection Exhaustion			Yes	
Traffic Control by Dst IP		1000000	Yes	
Group Cleaning Capacity Control		1000000	Yes	

dengjun

	Threshold 1	Threshold 2	Protection Enabled	Protection Algorithm
SYN Flood	2000	2000	Yes	0-SynCheck
ACK Flood	8000		Yes	
UDP Flood	1000		Yes	
ICMP Flood	400		Yes	
HTTP Get	1000		Yes	
Connection Exhaustion			Yes	
Traffic Control by Dst IP		1000000	Yes	
Group Cleaning Capacity Control		1000000	Yes	

You can edit the following policy templates:

- Anti-DDoS policy
- DNS protection policy
- UDP protection policy
- HTTP protection policy
- SIP protection policy
- Port check policy
- ICMP protection policy

For detailed configuration operations, see the *NSFOCUS ADS User Guide*.

Note	By default, a new protection group and regional IP group adopt the default anti-DDoS policy template. For details about anti-DDoS policy parameters, see appendix A Parameters.

7.8 Configuring an NTA Policy Template

NTA policy templates refer to the templates used by NTA devices managed by ADS M to generate alerts. NTA policy templates can be divided into region alert templates and IP group alert templates. An alert template can be assigned to multiple NTA devices.

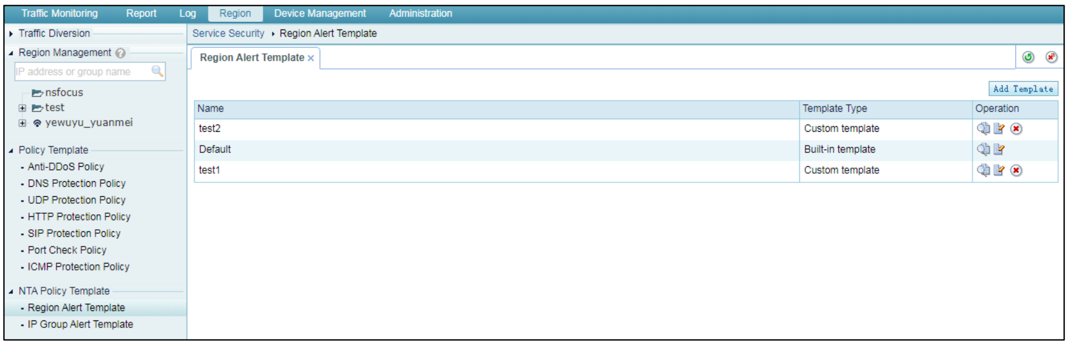
7.8.1 Configuring a Region Alert Template

After a region alert template is configured, you can directly reference it when creating a region.

To configure a region alert template, follow these steps:

Step 1 Choose **Region** > **NTA Policy Template** > **Region Alert Template**.

Figure 7-12 Region Alert Template page



Name	Template Type	Operation
test2	Custom template	
Default	Built-in template	
test1	Custom template	

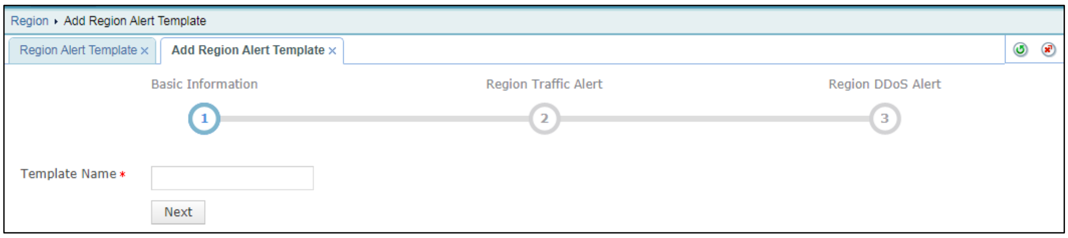
In the template list, the **Template Type** column shows the type of the template. **Default** indicates a built-in template. Other templates are custom ones. In the **Operation** column, you can click 📝 to modify parameter settings and ✖ to delete a custom template.

Step 2 Add a template.

a. Click **Add Template**. The page for adding a template appears, as shown in Figure 7-13.

You can define basic information, region traffic alert policies, and region DDoS attack alert policies.

Figure 7-13 Configuring a region alert template

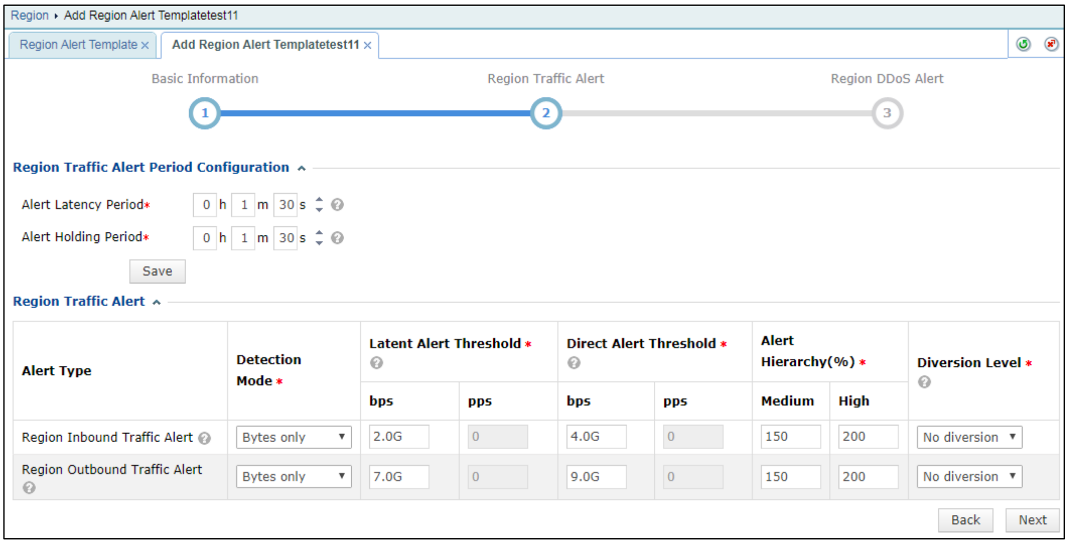


Template Name *

b. Enter a name and then click **Next**.

Step 3 Configure region traffic alert parameters.

Figure 7-14 Configuring region traffic alert policies



Region ▸ Add Region Alert Templatetest11

Region Alert Template × | Add Region Alert Templatetest11 ×

Region Traffic Alert Period Configuration

Alert Latency Period* 0 h 1 m 30 s

Alert Holding Period* 0 h 1 m 30 s

Save

Region Traffic Alert

Alert Type	Detection Mode *	Latent Alert Threshold *		Direct Alert Threshold *		Alert Hierarchy(%) *		Diversion Level *
		bps	pps	bps	pps	Medium	High	
Region Inbound Traffic Alert	Bytes only	2.0G	0	4.0G	0	150	200	No diversion
Region Outbound Traffic Alert	Bytes only	7.0G	0	9.0G	0	150	200	No diversion

Back Next

Table 7-12 Parameters for configuring traffic alert policies

Parameter	Description
Alert Latency Period	Specifies the maximum duration NTA must wait to generate an alert for the traffic between the value of **Latent Alert Threshold** and that of **Direct Alert Threshold**. This period is the alert latency period. The value ranges are 0–23 for the hour (**h**) and 0–59 for the minute (**m**). For the second (**s**), you can click ▲ or ▼ to set it to **0s** or **30s**
Alert Holding Period	Specifies the time when an alert persists after the traffic rate falls below the value of **Direct Alert Threshold**, which indicates that the attack ends. This parameter is valid only for latent alerts. The value ranges are 0–23 for the hour (**h**) and 0–59 for the minute (**m**). For the second (**s**), you can click ▲ or ▼ to set it to **0s** or **30s**.
Detection Mode	Specifies the type of traffic based on which an alert is generated. It has the following values: • **Not detect**: indicates that NTA does not check whether inbound or outbound traffic is abnormal. • **Packets only**: indicates that an alert is generated when the traffic rate in pps is found to exceed the threshold. • **Bytes only**: indicates that an alert is generated when the traffic rate in bps is found to exceed the threshold. • **Both packets and bytes**: indicates that an alert is generated when the traffic rate in pps and that in bps are both found to exceed the thresholds. • **Either packets or bytes**: indicates that an alert is generated when either the traffic rate in pps or that in bps is found to exceed the threshold.
Latent Alert Threshold	Specifies the traffic rate threshold in bps or pps that triggers NTA to generate an alert only after the traffic rate stays at this level for some time.

Parameter	Description
	• **bps**: indicates a threshold in bps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **Not detect** or **Packets only** for **Detection Mode**. • **pps**: indicates a threshold in pps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **Not detect** or **Bytes only** for **Detection Mode**. Note The latent alert threshold must be lower than the direct alert threshold.
Direct Alert Threshold	Specifies the traffic rate threshold in bps or pps that triggers NTA to generate an immediate alert. • **bps**: indicates a threshold in bps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **Not detect** or **Packets only** for **Detection Mode**. • **pps**: indicates a threshold in pps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **Not detect** or **Bytes only** for **Detection Mode**. Note The direct alert threshold must be greater than the latent alert threshold.
Alert Hierarchy(%)	Specifies how to classify alert levels. **Latent Alert Threshold** is a basis for classifying alert levels and needs to be configured in advance. Alert levels are classified according to the ratio of actual traffic to the **Latent Alert Threshold** value: • **Low**: specifies the lowest ratio for triggering a low-level alert. The value is always **100**. When the actual ratio falls between the smallest ratio for triggering a lower-level alert and the smallest ratio for triggering a medium-level alert, NTA generates a low-level alert. • **Medium**: specifies the ratio for triggering a medium-level alert. The default value is **150** and the maximum value is **10000**. When the actual ratio falls between the smallest ratio triggering a medium-level alert and the smallest ratio for triggering a high-level alert, NTA generates a medium-level alert. • **High**: specifies the ratio for triggering a high-level alert. The default value is **200** and the maximum value is **10000**. When the actual ratio is greater than the smallest ratio for triggering a high-level alert, NTA generates a high-level alert. If **Alert Hierarchy** is not configured, NTA will detect traffic and send alerts according to the global alert hierarchy.
Diversion Level	Specifies the alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted. • **No diversion**: indicates that no traffic diversion will take place. • **Divert Traffic of Low-level Alert**: indicates that a low-level alert or higher will trigger traffic diversion. • **Divert Traffic of Medium-level Alert**: indicates that a medium-level alert or higher will trigger traffic diversion. • **Divert Traffic of High-level Alert**: indicates that only a high-level alert can trigger traffic diversion.

After configuring traffic alert policies, click **Next**.

Step 4 Configure region DDoS attack alert parameters.

After configuring region traffic alert parameters, click **Next** to open the **Region DDoS Alert** page.

- **Region DDoS Alert Period Configuration**: Configure **Alert Latency Period** and **Alert Holding Period**. For specific configuration, see Table 7-12.
- **Region DDoS Alert**: Respectively configure **Inbound Check Configuration** and **Outbound Check Configuration**.
  - **Inbound Check Configuration**: Configure **Fixed Threshold Configuration** and **Constituent Proportion Configuration**. For details about parameter description of the former, see Table 7-12. To configure a constituent proportion, enable the function in the **Status Control** area, and configure alert parameters. If the traffic exceeds both **Min Trigger Threshold** and **Proportion for Direct Alerts**, the system directly generates an alert. For the configurations of other parameters, see Table 7-12.
  - **Outbound Check Configuration**: Configure **Constituent Proportion Configuration** after enabling this function.

Step 5 Click **Finish** to commit the settings.

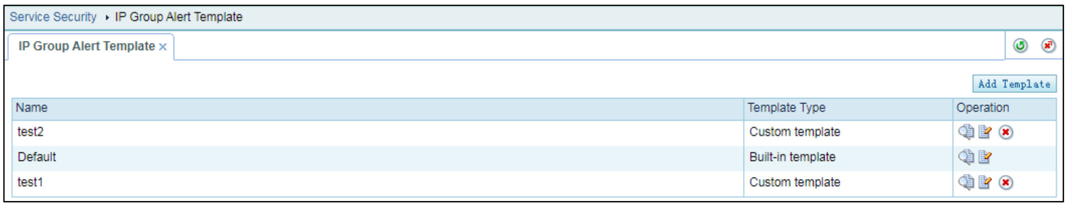
----End

7.8.2 IP Group Alert Template

After an IP group alert template is configured, you can directly reference it when creating an IP group.

Choose **Region > NTA Policy Template > IP Group Alert Template**.

Figure 7-15 IP Group Alert Template page



Service Security ‣ IP Group Alert Template
IP Group Alert Template ×
Add Template

Name	Template Type	Operation
test2	Custom template	⎘ ✎ ✖
Default	Built-in template	⎘ ✎
test1	Custom template	⎘ ✎ ✖

In the template list, the **Template Type** column shows the type of the template. **Default** indicates a built-in template. Other templates are custom ones. In the **Operation** column, you can click ✎ to modify parameter settings and ✖ to delete a custom template.

You can click **Add Template** to create a template. The procedure for configuring an IP group alert template is the same as that for configuring a region alert template. For details, see section 7.8.1 Configuring a Region Alert Template.

8 Smart Protection

After learning traffic of the network environment of a protection group, ADS M establishes a smart protection model to achieve real-time DDoS protection through smart detection. You can create multiple smart protection groups to address various business requirements.

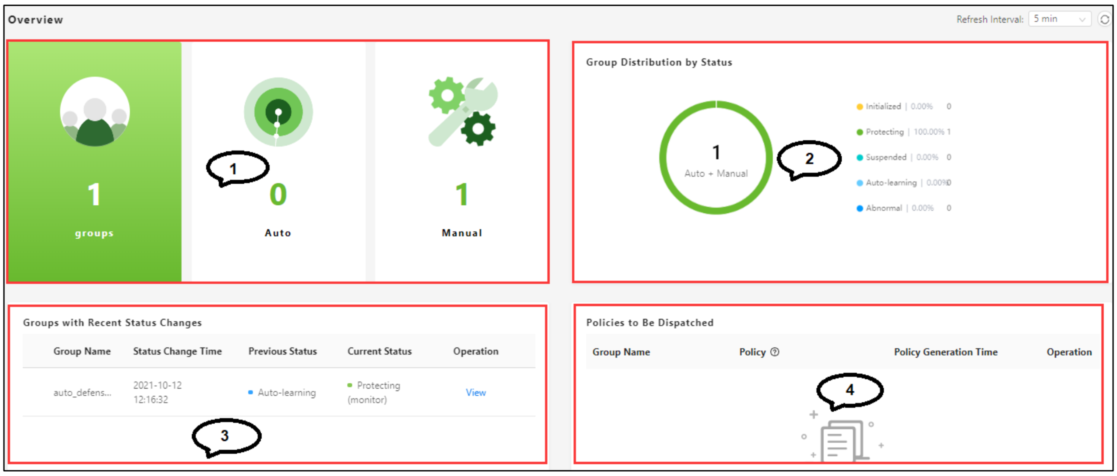
This chapter mainly covers:

Section	Description
Protection Overview	Describes the webpage layout of the protection overview.
Protection Group Management	Describes how to manage a protection group, including the creating and dispatching of a policy.
Logs	Describes how to view mitigation logs, running logs, and audit logs.

8.1 Protection Overview

On the system login page shown in Figure 2-1, select **Smart Anti-DDoS System**, type the correct user name and password, and click **Login** or press **Enter** to open the smart protection overview page.

Figure 8-1 Smart protection overview



Group Name	Status Change Time	Previous Status	Current Status	Operation
auto_defens...	2021-10-12 12:16:32	Auto-learning	Protecting (monitor)	View

Group Name	Policy	Policy Generation Time	Operation

Table 8-1 describes four areas on the smart protection overview page.

Table 8-1 Smart protection information

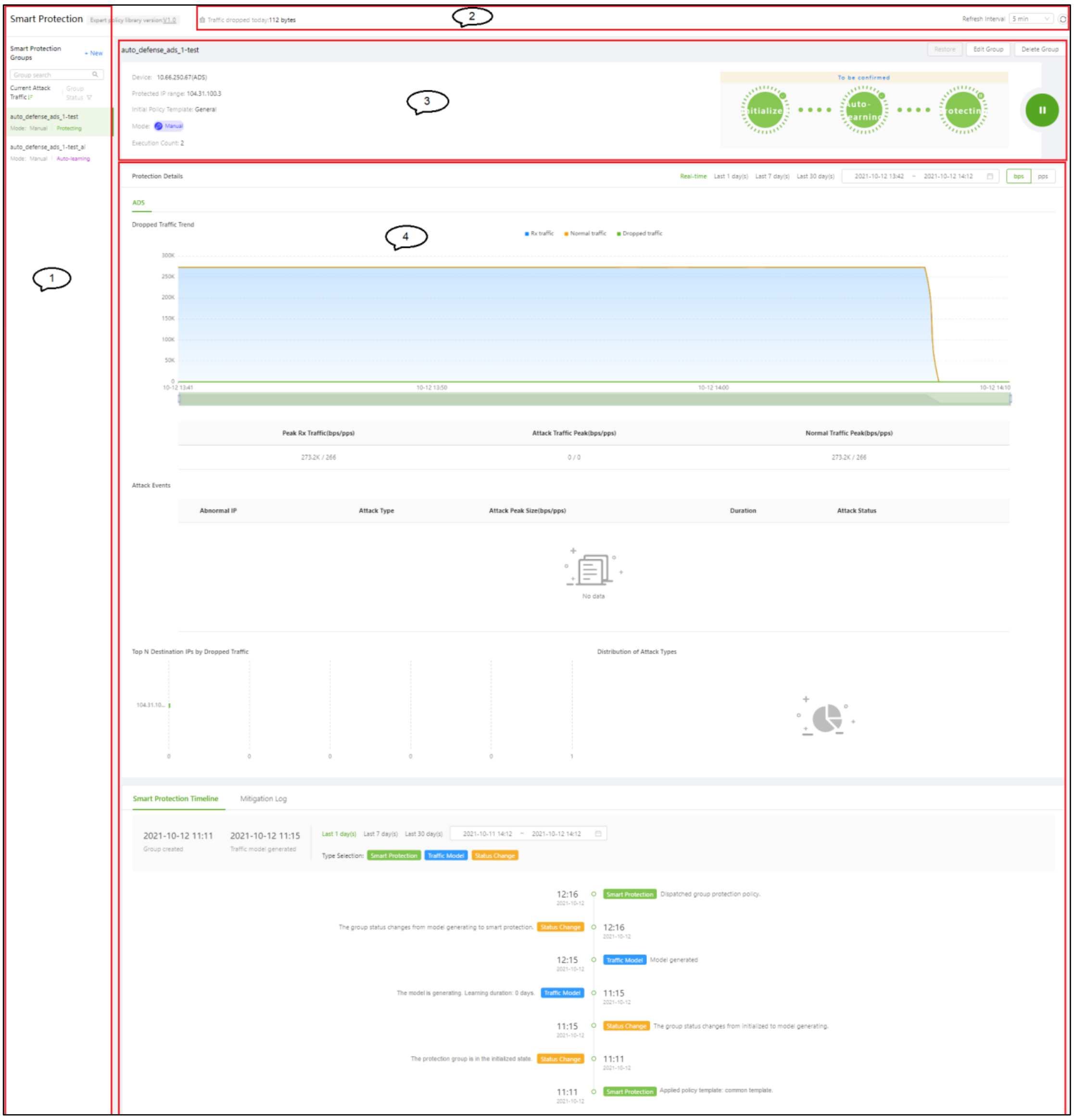
No.	Area Name	Description
1	Protection group information	Presents the total number of protection groups, the number of groups created automatically, and the number of groups created manually.
2	Group distribution by status	Presents the total number of protection groups and the percentage of groups in each state that can be initialized, auto-learning, protecting, suspended, or abnormal.
3	Groups with recent status changes	Presents the names of protection groups with recent status changes, previous status, current status, and status change time. You can click **View** in the **Operation** column to open the monitoring information page of this protection group.
4	Policies to be dispatched	Presents the name of protection group to which the policies are dispatched, policies to be dispatched, and policy generation time. You can click **View** in the **Operation** column to open the monitoring information page of this protection group.

8.2 Protection Group Management

8.2.1 Viewing Monitoring Information of a Smart Protection Group

After a smart protection group is created, you can choose the **Protection Groups** menu to view information about existing protection groups.

Figure 8-2 Protection group information



Traffic dropped today:112 bytes

auto_defense_ads_1-test
Mode: Manual | Protecting

auto_defense_ads_1-test_al
Mode: Manual | Auto-learning

auto_defense_ads_1-test

Device: 10.66.250.67(ADS)

Protected IP range: 104.31.100.3

Initial Policy Template: General

Mode: Manual

Execution Count: 2

2021-10-12 13:42 ~ 2021-10-12 14:12

Peak Rx Traffic(bps/pps)	Attack Traffic Peak(bps/pps)	Normal Traffic Peak(bps/pps)
273.2K / 266	0 / 0	273.2K / 266

Attack Events

Abnormal IP	Attack Type	Attack Peak Size(bps/pps)	Duration	Attack Status

2021-10-12 11:11 Group created

2021-10-12 11:15 Traffic model generated

2021-10-11 14:12 ~ 2021-10-12 14:12

12:16 2021-10-12 Smart Protection Dispatched group protection policy.

The group status changes from model generating to smart protection. Status Change 12:16 2021-10-12

12:15 2021-10-12 Traffic Model Model generated

The model is generating. Learning duration: 0 days. Traffic Model 11:15 2021-10-12

11:15 2021-10-12 Status Change The group status changes from initialized to model generating.

The protection group is in the initialized state. Status Change 11:11 2021-10-12

11:11 2021-10-12 Smart Protection Applied policy template: common template.

Table 8-2 describes four areas on the smart protection group page.

Table 8-2 Smart protection information

No.	Area Name	Description
1	Existing smart protection groups	This area allows you to view and manage all existing smart protection groups:

No.	Area Name	Description
		• Click + or **New** in the upper-right corner of the area to create a new smart protection group. • Type a protection group name and click 🔍 in the search box or press **Enter** to search for a specific protection group. Fuzzy search is supported. • Click ⊗ in the search box to present all protection groups. • By default, protection groups are listed in the descending order of attack traffic. Pointing to **Current Attack Traffic**, you can list protection groups in the descending order of attack traffic or current traffic by selecting **Current attack traffic (descending)** or **Current normal traffic (descending)**. • By default, protection groups under all states are listed. You can click **Group Status** and select **Initialized**, **Auto-learning**, **Protecting**, **Suspended**, or **Abnormal** from the drop-down box and click **OK** to present protection groups of the selected state. • Click a protection group to view its basic information, protection details, smart protection timeline, and mitigation logs in the right pane of the page.
2	Traffic dropped for the protection group	This area presents the total traffic (byte) dropped for all protection groups. You can specify the refresh interval as follows: • Select **5 min** or **1 min** to refresh the page every 5 or 1 minute. • Select **Never** to turn off the auto refresh function. In this case, you can refresh the page only by manually clicking ↻.
3	Protection group basics	This area presents basics of the specific protection group: • **Device**: information of ADS that protects the protection group. • **Protected IP range**: IP address range of the protection group. • **Initial Policy Template**: policy template used initially. The value here is **General**, indicating that the general policy template is used. • **Mode**: protection group mode, which can be **Auto** or **Manual**. • Protection group state: protection group state, which can be **Initialized**, **Auto-learning**, **Protecting**, **Suspended**, or **Abnormal**. • **Execution Count**: number of times policies are dispatched. In the upper-right corner of the area, you can edit or restore protection group settings or delete the protection group by clicking the corresponding button. Protection groups of different states support different operations.
4	Protection details	This area presents the attack traffic trend in an area graph and attack types in a pie chart.

No.	Area Name	Description
		• Hovering the mouse over the dropped traffic trend, you can view the received traffic, normal traffic, and dropped traffic at a specific time spot. • The attack event table displays the abnormal IP address, attack type, attack peak size, attack duration, and attack state. • Hovering the mouse over the graph of top N destination IP addresses, you can view top destination IP addresses by dropped traffic and the maximum dropped traffic. • Hovering the mouse over the pie chart of attack type distribution, you can view the current attack types and the percentage of each type. • The area graph of dropped traffic trend shows real-time protection by default. You can click **Last 1 day(s)**, **Last 7 day(s)**, or **Last 30 day(s)** to view the protection details of this protection group during the period. • You can click in the time frame box and specify the start time and end time to view protection details in the specified period. • You can click **bps** or **pps** to view protection details of traffic in bps or pps.
5	Smart protection timeline	The **Smart Protection Timeline** tab page presents the smart protection timeline of a specific protection group, including when a protection group is created, when a traffic model is generated, when protection policies and rules are dispatched. • By default, smart protection dynamics in the last one day are displayed. You can click **Last 7 day(s)** or **Last 30 day(s)** to view dynamics of smart protection during the period. • You can click in the time frame box and specify the start time and end time to view smart protection details in the specified period. • By default, the timeline shows information about smart protection, traffic model, and status changes. You can click the corresponding type to show or hide its information. An uncolored type is hidden from the timeline. • You can click **More** below the timeline to view more dynamics of smart protection. You can click the **Mitigation Log** tab to view mitigation logs of this protection group in a specified period. • By default, mitigation logs in the last one day are displayed. You can click **Last 7 day(s)** or **Last 30 day(s)** to view logs during the period. • You can click in the time frame box and specify the start time and end time to view mitigation logs in the specified period. • By default, all mitigation logs in the specified period are displayed. You can select **Dispatch failed** or **Dispatch successful** from the **Status** drop-down box to view the corresponding logs.

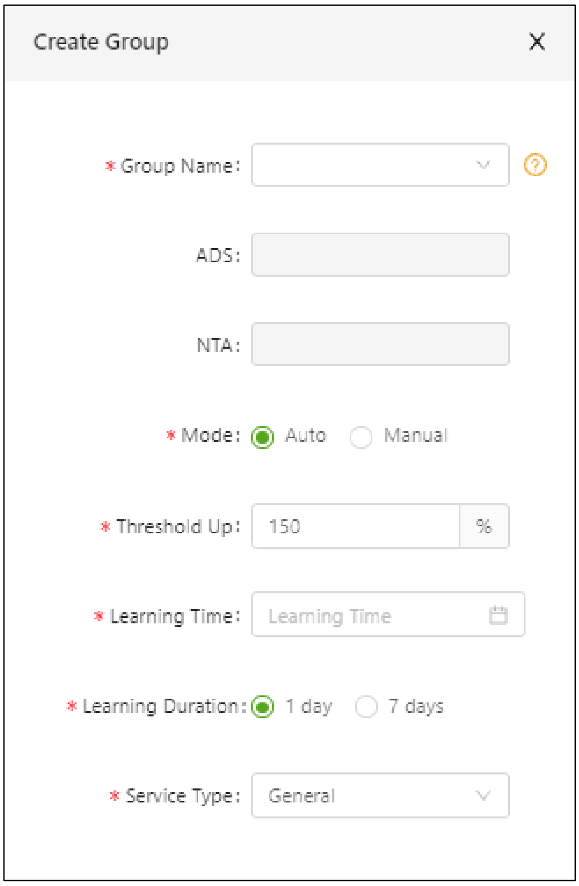
8.2.2 Creating a Smart Protection Group

The system supports a maximum of 15 smart protection groups.

To create a smart protection group, follow these steps:

Step 1 Click **New** in the left pane of the page shown in Figure 8-2.

Figure 8-3 Creating a smart protection group



Create Group

* Group Name:

ADS:

NTA:

* Mode: ● Auto ○ Manual

* Threshold Up: 150 %

* Learning Time: Learning Time

* Learning Duration: ● 1 day ○ 7 days

* Service Type: General

Step 2 Configure parameters in the dialog box.

Table 8-3 Parameters for creating a smart protection group

Parameter	**Description**
Group Name	Region IP group that is added as a smart protection group. IP groups can be listed in the drop-down box only when the region to which the IP group belongs is protected by a single ADS device or ADS cluster.
Protection Device (ADS)	Device that protects the selected region IP group. After an IP group is selected as a smart protection group, the system automatically identifies protection devices without manual configuration.
Protection Device (NTA)	Device that protects the selected region IP group. After an IP group is selected as a smart protection group, the system automatically identifies protection devices without manual configuration.
Mode	Protection group mode, which can be manual or automatic.
Threshold Up	Growth rate of the auto-learning baseline threshold. The traffic threshold for a smart protection group is the auto-learning baseline threshold increased by a certain percentage. The growth rate range is 100–500, with 150 as default.
Learning Time	Time for auto-learning of the smart protection group. Only after learning the network traffic for a period of time can ADS M generate a protection model.

Parameter	Description
	You can determine when the auto-learning starts. The longer ADS M learns network traffic, the better its protection effect is.
Learning Duration	Duration of auto-learning of the smart protection group. Only after learning the network traffic for a period of time can ADS M generate a protection model. • **1 day**: After learning network traffic for one day, ADS M starts smart protection for the protection group. • **7 days**: After learning network traffic for seven days, ADS M starts smart protection for the protection group. The longer ADS M learns network traffic, the better its protection effect is.
Service Type	Service type whose smart protection template is used. Options include: • **General**: uses the smart protection template of anti-DDoS policies. • **Authoritative DNS server**: uses the smart protection template of the DNS authorization policy. • **DNS cache server**: uses the smart protection template of the DNS cache protection policy. • **HTTP**: uses the smart protection template of HTTP protection policies. • **TCP download**: uses the smart protection template of the TCP download protection policy. • **TCP games**: uses the smart protection template of the TCP games protection policy. • **UDP applications**: uses the smart protection template of the UDP protection policy.

Step 3 Click **Save** to commit the settings.

Step 4 Upon creation of the smart protection group, ADS M starts to learn its traffic.

The smart protection group can be in one of the following states:

- Initialized: The new smart protection group is under initialization.
- Auto-learning: After the smart protection group is initialized, ADS M starts to learn its traffic. The protection group is in auto-learning state when ADS M either learns or re-learns its traffic. Protection groups in this state can only be edited or deleted.
- Protecting (monitoring): When auto-learning is finished, ADS M gets a complete set of baseline data and starts to monitor the traffic of the protection group. Protection groups in this state can be suspended, deleted, or re-learned.
- Protecting (attack defense): When an attack is detected, the protection group is put under smart protection; when the attack is dealt with, the protection groups is subject to monitoring. Protection groups in this state can only be suspended or deleted.
- When in protection (attack defense) state, ADS M provides the following types of smart protection for protection groups: fragment attack protection (only IPv4), UDP packet protection by packet length, reflection attack protection, DNS keyword checking, HTTP keyword checking, payload detection and protection, rate limitation of trusted IP addresses, pattern matching, and access control (only IPv4).
- Suspended: Smart protection groups can be suspended only when under protection. Protection groups support the following operations: protection resumption, re-learning, policy dispatch, one-click policy restoration, and group editing and deletion.
- Abnormal: A smart protection group will be in the abnormal state when the detection or protection device gets offline or auto-learning fails.

----End

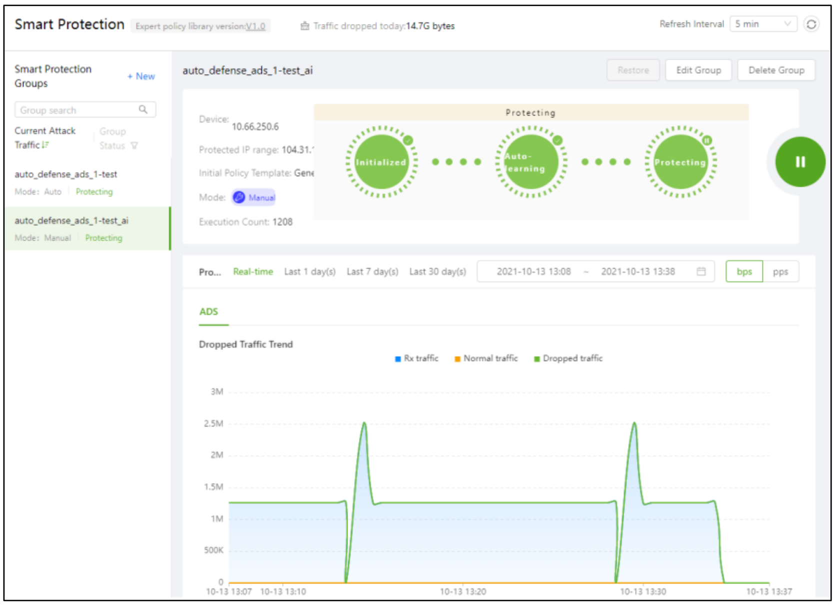
8.2.3 Suspending Protection for a Smart Protection Group

Only smart protection groups under protection can be suspended.

Click in the upper-right corner of the page shown in Figure 8-2 to suspend protection for the protection group.

For a suspended protection group, you can resume protection, restore policy configurations, or edit and delete the group.

Figure 8-4 Suspending protection for a protection group



Smart Protection Expert policy library version:V1.0 Traffic dropped today:14.7G bytes Refresh Interval 5 min

Smart Protection Groups

auto_defense_ads_1-test
Mode: Auto | Protecting

auto_defense_ads_1-test_ai
Mode: Manual | Protecting

auto_defense_ads_1-test_ai

Device: 10.66.250.6

Protected IP range: 104.31.

Initial Policy Template: Gene

Mode: Manual

Execution Count: 1208

2021-10-13 13:08 ~ 2021-10-13 13:38

8.2.4 Restoring Protection for a Smart Protection Group

The protection restoration is available only to smart protection groups with suspended protection.

Click in the protection group basics area to suspend the protection for the protection group.

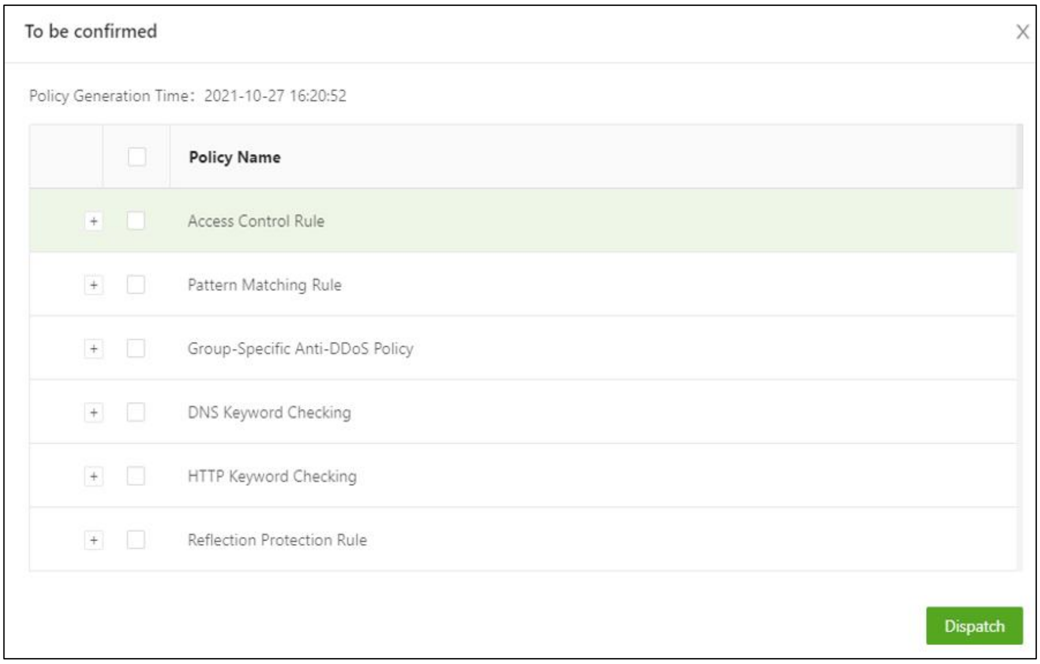
A protection group, whether in the monitoring or attack defense state, returns to the protection state upon protection resumption.

8.2.5 Dispatching Policies (Manual Mode)

For a protection group in manual mode, you need to dispatch policies manually.

You can click **To be confirmed** in the upper-right corner of the page shown in Figure 8-4 to open the policy dispatch configuration page.

Figure 8-5 Dispatching policies



To be confirmed

Policy Generation Time：2021-10-27 16:20:52

	□	Policy Name
+	□	Access Control Rule
+	□	Pattern Matching Rule
+	□	Group-Specific Anti-DDoS Policy
+	□	DNS Keyword Checking
+	□	HTTP Keyword Checking
+	□	Reflection Protection Rule

Step 2 Select policies and click **Dispatch** to dispatch them to the protection group.

----End

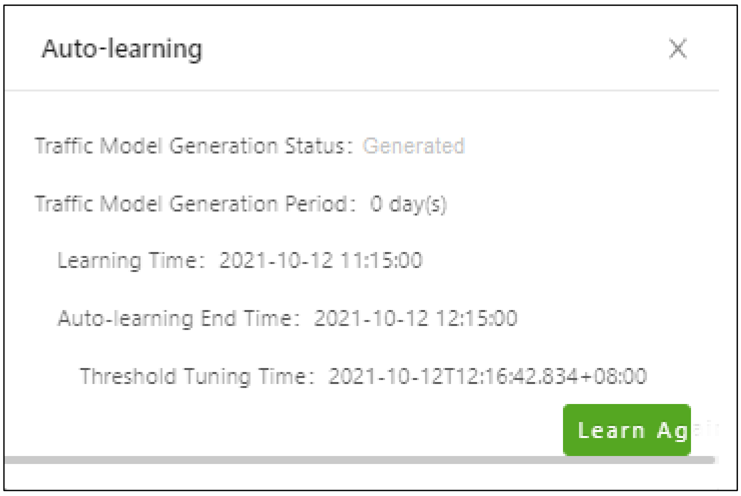
8.2.6 **Re-learning Traffic**

Traffic re-learning is available only to smart protection groups with ongoing or suspended protection.

To configure the traffic re-learning function, follow these steps:

Step 1 Click auto-learning in the upper-right part of the smart protection group page shown in Figure 8-4.

Figure 8-6 Starting re-learning



Auto-learning

Traffic Model Generation Status: Generated

Traffic Model Generation Period: 0 day(s)

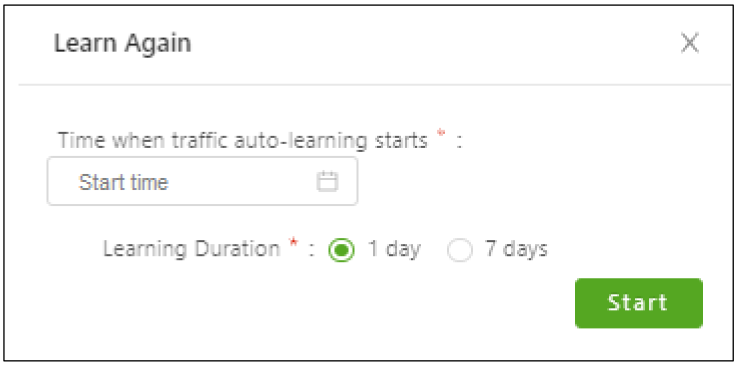
Learning Time: 2021-10-12 11:15:00

Auto-learning End Time: 2021-10-12 12:15:00

Threshold Tuning Time: 2021-10-12T12:16:42.834+08:00

Step 2 Click **Learn Again** to configure the traffic re-learning function.

Figure 8-7 Re-learning traffic



Learn Again

Time when traffic auto-learning starts * :

Start time

Learning Duration * : ● 1 day ○ 7 days

Step 3 Configure the re-learning start time and learning duration.

Step 4 Click **Start**.

Then ADS M starts learning the normal traffic model.

After the auto-learning is completed, the smart protection group will be automatically put in protection.

----End

8.2.7 Editing a Smart Protection Group

If the smart protection effect is less satisfactory, you can edit policies of smart protection groups and dispatch protection policies. Then the smart protection system will protect protection groups according to the dispatched policies.

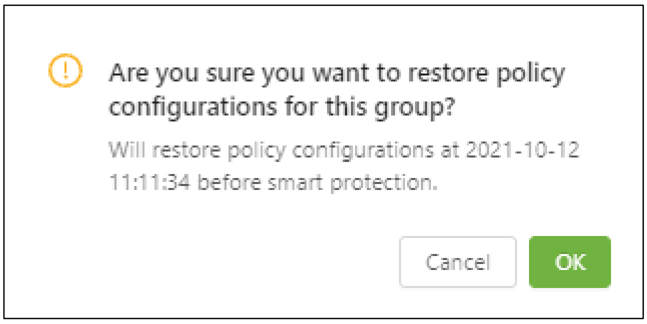
You can click **Edit Group** in the upper-right corner of the page shown in Figure 8-4 to edit policies of the smart protection group.

8.2.8 Restoring Policies upon One Click

One-click policy restoration is available only to smart protection groups in the protection suspension state.
To configure one-click policy restoration, follow these steps:

Step 1 Click **Restore** in the upper-right corner of the page shown in Figure 8-4.

Figure 8-8 Restoring policies upon one click



Are you sure you want to restore policy configurations for this group?

Will restore policy configurations at 2021-10-12 11:11:34 before smart protection.

Step 2 Click **OK**.

Then policies of the smart protection group will be restored to those used before the protection group is created.

After policies are restored, the smart protection group is still in the protection suspension state.

----End

8.2.9 Deleting a Smart Protection Group

Smart protection groups can be deleted regardless of the protection state.

You can click **Delete Group** in the upper-right corner of the page shown in Figure 8-2 and click **OK** in the confirmation dialog box to delete a smart protection group.

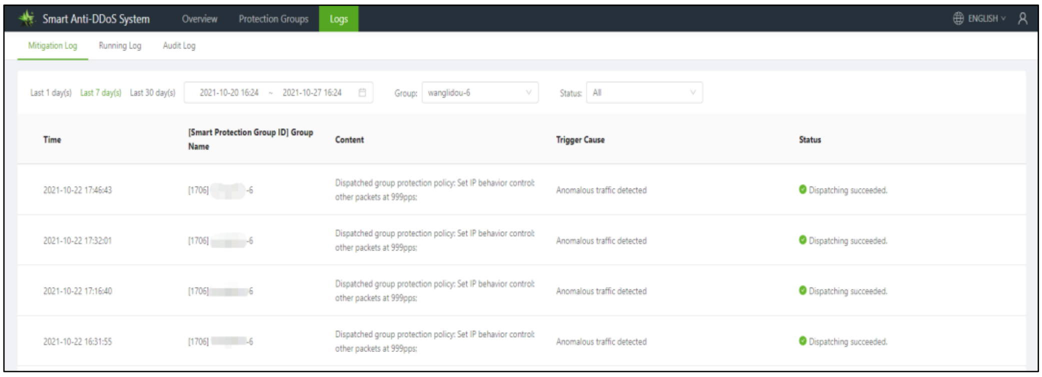
8.3 Logs

In the smart protection system, you can view mitigation logs, running logs, and audit logs.

8.3.1 Mitigation Log

Choose **Logs > Mitigation Log**. The **Mitigation Log** page presents attack mitigation logs. You can specify the log query time and select the protection group and its state to view desired logs.

Figure 8-9 Mitigation logs



2021-10-20 16:24 ~ 2021-10-27 16:24

Group: wanglidou-6

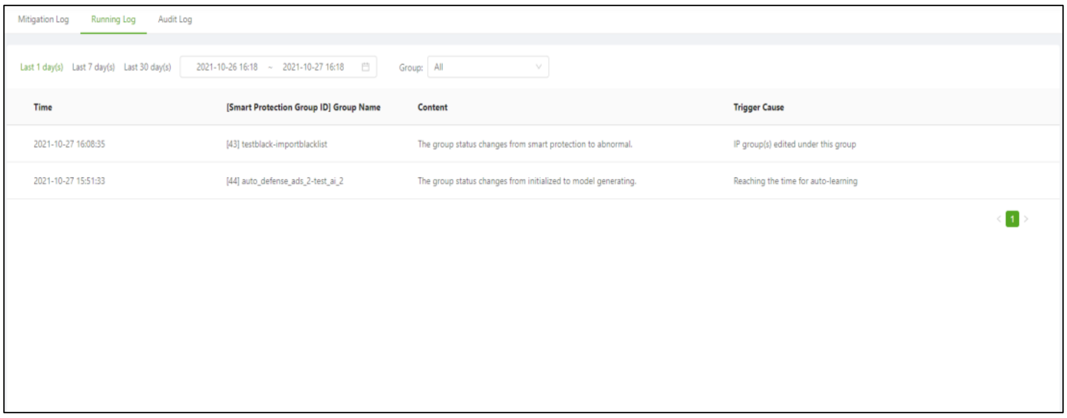
Status: All

Time	[Smart Protection Group ID] Group Name	Content	Trigger Cause	Status
2021-10-22 17:46:43	[1706] [redacted]-6	Dispatched group protection policy: Set IP behavior control: other packets at 999pps;	Anomalous traffic detected	● Dispatching succeeded.
2021-10-22 17:32:01	[1706] [redacted]-6	Dispatched group protection policy: Set IP behavior control: other packets at 999pps;	Anomalous traffic detected	● Dispatching succeeded.
2021-10-22 17:16:40	[1706] [redacted]6	Dispatched group protection policy: Set IP behavior control: other packets at 999pps;	Anomalous traffic detected	● Dispatching succeeded.
2021-10-22 16:31:55	[1706] [redacted]-6	Dispatched group protection policy: Set IP behavior control: other packets at 999pps;	Anomalous traffic detected	● Dispatching succeeded.

8.3.2 Running Log

On the page shown in Figure 8-9, select the **Running Log** tab to view protection status change logs of smart protection groups. You can specify the log query time and select a protection group to view desired logs.

Figure 8-10 Running logs



2021-10-26 16:18 ~ 2021-10-27 16:18

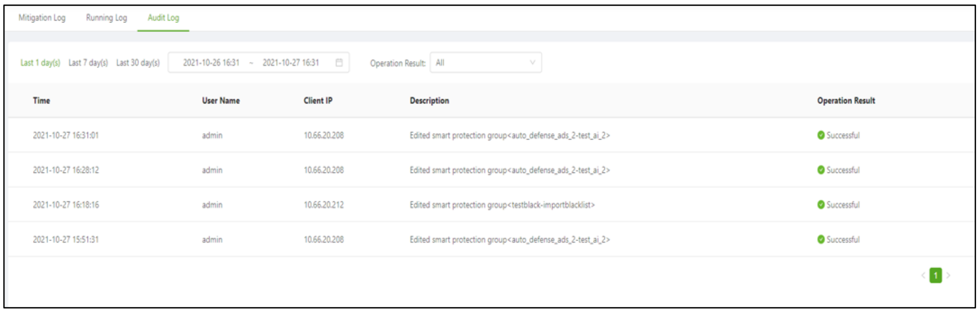
Group: All

Time	[Smart Protection Group ID] Group Name	Content	Trigger Cause
2021-10-27 16:08:35	[43] testblack-importblacklist	The group status changes from smart protection to abnormal.	IP group(s) edited under this group
2021-10-27 15:51:33	[44] auto_defense_ads_2-test_ai_2	The group status changes from initialized to model generating.	Reaching the time for auto-learning

8.3.3 Audit Log

On the page shown in Figure 8-9, select the **Audit Log** tab to view audit logs of smart protection groups. You can specify the log query time and select the operation result to view desired logs.

Figure 8-11 Audit logs



Time	User Name	Client IP	Description	Operation Result
2021-10-27 16:31:01	admin	10.66.20.208	Edited smart protection group<auto_defense_ads_2-test_ai_2>	✓ Successful
2021-10-27 16:28:12	admin	10.66.20.208	Edited smart protection group<auto_defense_ads_2-test_ai_2>	✓ Successful
2021-10-27 16:18:16	admin	10.66.20.212	Edited smart protection group<testblack-importblacklist>	✓ Successful
2021-10-27 15:51:31	admin	10.66.20.208	Edited smart protection group<auto_defense_ads_2-test_ai_2>	✓ Successful

9 Device Management

This chapter describes in detail the configuration methods of devices under ADS M, including how to add, modify and delete an ADS device, ADS cluster, and NTA device.

This chapter mainly covers:

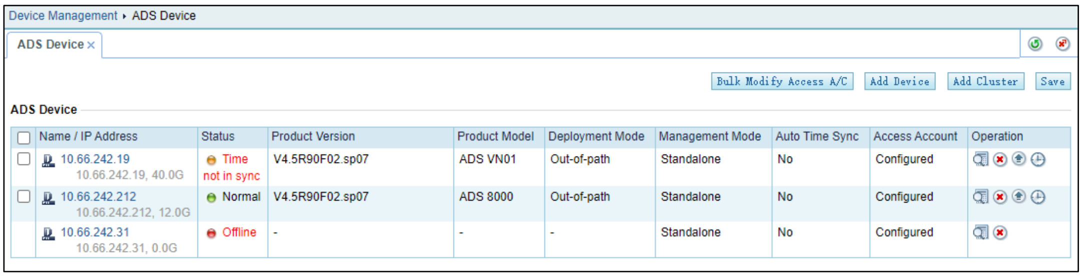
Section	Description
Managing ADS Devices	Describes how to configure and manage ADS devices.
Managing ADS Clusters	Describes how to configure and manage ADS clusters.
Managing NTA Devices	Describes how to configure and manage NTA devices.

9.1 Managing ADS Devices

Click **Device Management > ADS Device**.

The **ADS Device** page appears, as shown in Figure 9-1.

Figure 9-1 ADS Device page



ADS Device

□	Name / IP Address	Status	Product Version	Product Model	Deployment Mode	Management Mode	Auto Time Sync	Access Account	Operation
□	10.66.242.19 10.66.242.19, 40.0G	Time not in sync	V4.5R90F02.sp07	ADS VN01	Out-of-path	Standalone	No	Configured	
□	10.66.242.212 10.66.242.212, 12.0G	Normal	V4.5R90F02.sp07	ADS 8000	Out-of-path	Standalone	No	Configured	
	10.66.242.31 10.66.242.31, 0.0G	Offline	-	-	-	Standalone	No	Configured	

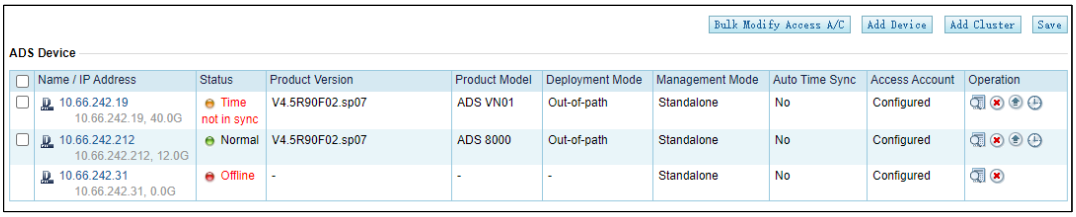
The ADS device list consists of ADS devices and clusters, as shown in Figure 9-2. Initially, the device list is empty and you need to add devices or clusters manually. Clicking a device name opens the page for configuring protection policies.

Note

Pages for configuring protection policies on ADS are accessible only when **Managed Device Access** is set to **Open**. For details, see section 3.1.1 Basic Settings.

When ADS is in the packet forwarding state, the state is also indicated in the **Device Monitoring** area on the **System Overview** page. If the license of ADS is about to expire in less than seven days, the system displays a message indicating that the license will expire in X days. When the license validity period is displayed as 0 days, the system displays a message indicating that the license is invalid or expires.

Figure 9-2 ADS devices



ADS Device

□	Name / IP Address	Status	Product Version	Product Model	Deployment Mode	Management Mode	Auto Time Sync	Access Account	Operation
□	10.66.242.19 10.66.242.19, 40.0G	● Time not in sync	V4.5R90F02.sp07	ADS VN01	Out-of-path	Standalone	No	Configured	
□	10.66.242.212 10.66.242.212, 12.0G	● Normal	V4.5R90F02.sp07	ADS 8000	Out-of-path	Standalone	No	Configured	
	10.66.242.31 10.66.242.31, 0.0G	● Offline	-	-	-	Standalone	No	Configured	

Prior to adding an ADS device, you need to log in to the web-based manager of this device to verify that this device is subordinate to ADS M (**System** > **Local Settings** > **Management Mode**) and type the IP address of ADS M. For details, see the *NSFOCUS ADS User Guide***.**

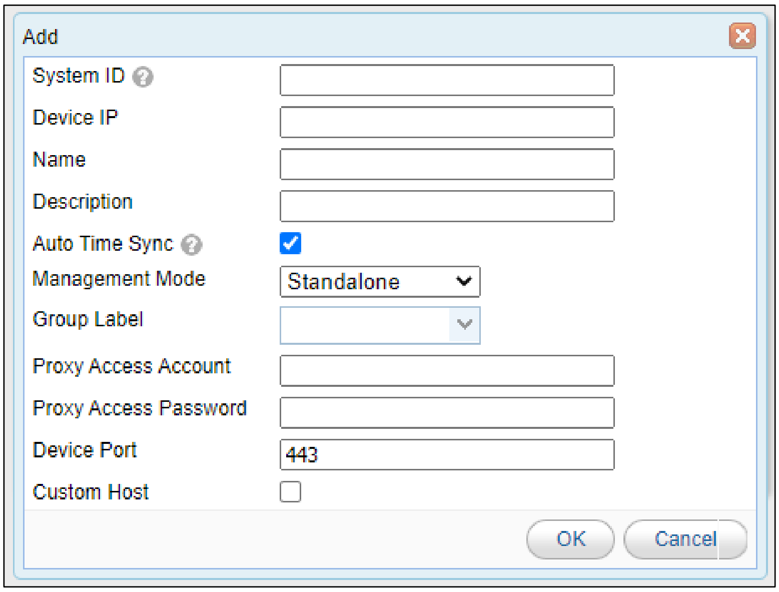
After you complete the configuration and properly connect the two devices, this ADS device is subordinate to ADS M and appears in the treelike structure of monitoring objects.

9.1.1 Adding an ADS Device

To add an ADS device, follow these steps:

Step 1 Click **Add Device** in the upper-right corner of the **ADS Device** page shown in Figure 9-1.

Figure 9-3 Adding an ADS device



Add

System ID

Device IP

Name

Description

Auto Time Sync ☑

Management Mode: Standalone

Group Label

Proxy Access Account

Proxy Access Password

Device Port: 443

Custom Host □

Table 9-1 describes parameters of an ADS device.

Table 9-1 Parameters of an ADS device

Parameter	Description
System ID	Specifies the system ID of the ADS device. It is required.
Device IP	Specifies the IP address of the device. Either an IPv4 or IPv6 address is accepted. It is required.
Name	Specifies the device name. It must be 1 to 20 characters long and cannot contain invalid characters such as angle brackets (<, or >), quotation marks (" or '), and slashes (/). The device name is mandatory and must be unique.
Description	Specifies the brief description of this ADS device such as the use of the device.
Auto Time Sync	Controls whether to automatically synchronize the system time of the device with that of ADS M. By default, this option is selected.
Management Mode	Specifies the device management mode, which can be **Standalone** or **Cluster**. • **Standalone**: indicates that the ADS device is independently deployed and does not belong to any cluster. • **Cluster**: indicates that the ADS device is a member of a cluster and accepts centralized management of ADS M.
Cluster	Specifies the cluster to which the ADS device belongs. This parameter is required when **Management Mode** is set to **Cluster**.
Group Label	Specifies the label of the group to which the device belongs. The device tree in the left part displays devices by groups. This parameter is required when **Management Mode** is set to **Standalone**.
Proxy Access Account	Specifies the account of the proxy ADS device. After the proxy access account and password are configured, ADS M can directly log in to the corresponding ADS device.

Parameter	Description
Proxy Access Password	Specifies the password of the proxy ADS device. After the proxy access account and password are configured, ADS M can directly log in to the corresponding ADS device.
Login Mode	• **Use the same account & password as the master device**: indicates that ADS M uses the same account and password as those of the master device to access the ADS device. • **Use different account & password**: indicates that ADS M uses the proxy access account and password specified here to access the ADS device. This parameter is required when **Management Mode** is set to **Cluster**.
Device Port	Specifies the port of the device. The default value is **443**.
Custom Host	Specifies the ADS proxy's host name.

Step 2 Set the parameters in the dialog box, and click **OK.**

----End

9.1.2 Editing ADS Device Settings

On the **ADS Device** page, click ✎ in the **Operation** column of an ADS device to modify information about the device, except device ID.

9.1.3 Deleting an ADS Device

On the **ADS Device** page, click ✖ in the **Operation** column of an ADS device to delete the device. Once an ADS device is deleted, it is no longer subject to management of ADS M and so will not upload its device information to ADS M.

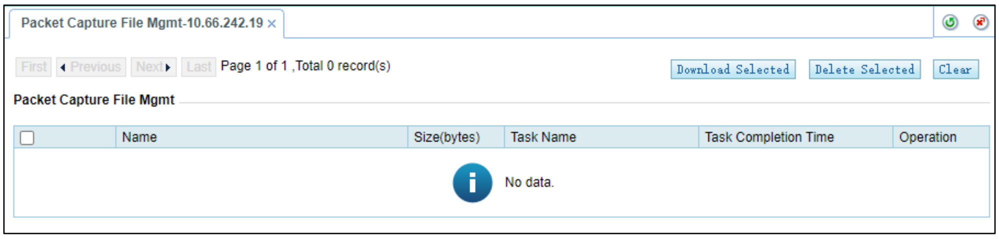
⚠ Caution	Once a device is deleted, you cannot continue to view monitoring pages, configuration pages, and other pages related to this device even if these pages were previously opened. In a cluster, the master device cannot be deleted unless the cluster has only one device.

9.1.4 Managing Packet Capture Files

You can download, delete, or clear packet capture files of ADS. The detailed procedure is as follows:

Step 1 On the **ADS Device** page shown in Figure 9-4, click 🗐 in the **Operation** column of an ADS device to open its packet capture file page.

Figure 9-4 Packet capture file management page



Packet Capture File Mgmt-10.66.242.19 ×

First ◂ Previous Next ▸ Last Page 1 of 1 ,Total 0 record(s)

Download Selected | Delete Selected | Clear

Packet Capture File Mgmt

□	Name	Size(bytes)	Task Name	Task Completion Time	Operation

No data.

Step 2 Download packet capture files.

Bulk download: Select more than one checkbox in the leftmost column and click **Download Selected** to download these files to a local disk drive.

Download one by one: Click 💾 in the **Operation** column of a packet capture file to download it to a local disk drive.

Step 3 Delete packet capture files.

Bulk delete: Select more than one checkbox in the leftmost column and click **Delete Selected** and click **OK** in the confirmation dialog box to delete these files.

Delete one by one: Click ✖ in the **Operation** column of a packet capture file to delete it.

Step 4 Clear packet capture files.

Click **Clear** and then click **OK** in the confirmation dialog box to clear all packet capture files.

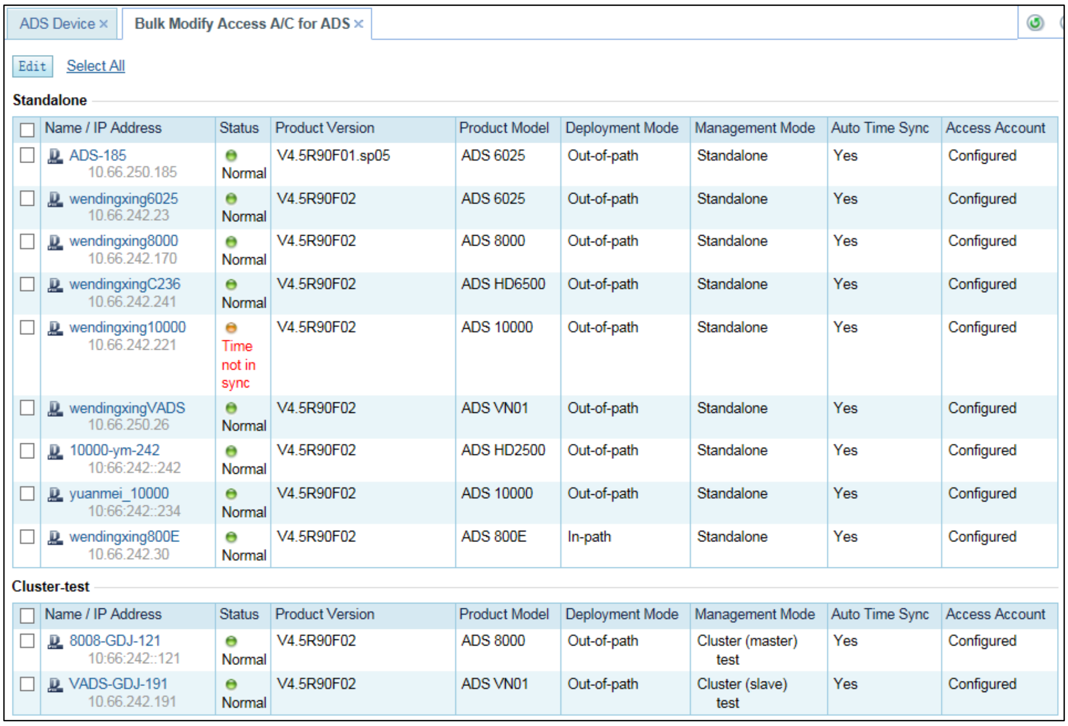
----End

9.1.5 Modifying Access Accounts in Batches

You can modify access account passwords in batches by following these steps:

Step 1 In the ADS device list shown in Figure 9-1, click **Bulk Modify Access A/C**.

Figure 9-5 Modifying access accounts in batches



Standalone

□	Name / IP Address	Status	Product Version	Product Model	Deployment Mode	Management Mode	Auto Time Sync	Access Account
□	ADS-185 10.66.250.185	● Normal	V4.5R90F01.sp05	ADS 6025	Out-of-path	Standalone	Yes	Configured
□	wendingxing6025 10.66.242.23	● Normal	V4.5R90F02	ADS 6025	Out-of-path	Standalone	Yes	Configured
□	wendingxing8000 10.66.242.170	● Normal	V4.5R90F02	ADS 8000	Out-of-path	Standalone	Yes	Configured
□	wendingxingC236 10.66.242.241	● Normal	V4.5R90F02	ADS HD6500	Out-of-path	Standalone	Yes	Configured
□	wendingxing10000 10.66.242.221	● Time not in sync	V4.5R90F02	ADS 10000	Out-of-path	Standalone	Yes	Configured
□	wendingxingVADS 10.66.250.26	● Normal	V4.5R90F02	ADS VN01	Out-of-path	Standalone	Yes	Configured
□	10000-ym-242 10:66:242::242	● Normal	V4.5R90F02	ADS HD2500	Out-of-path	Standalone	Yes	Configured
□	yuanmei_10000 10:66:242::234	● Normal	V4.5R90F02	ADS 10000	Out-of-path	Standalone	Yes	Configured
□	wendingxing800E 10.66.242.30	● Normal	V4.5R90F02	ADS 800E	In-path	Standalone	Yes	Configured

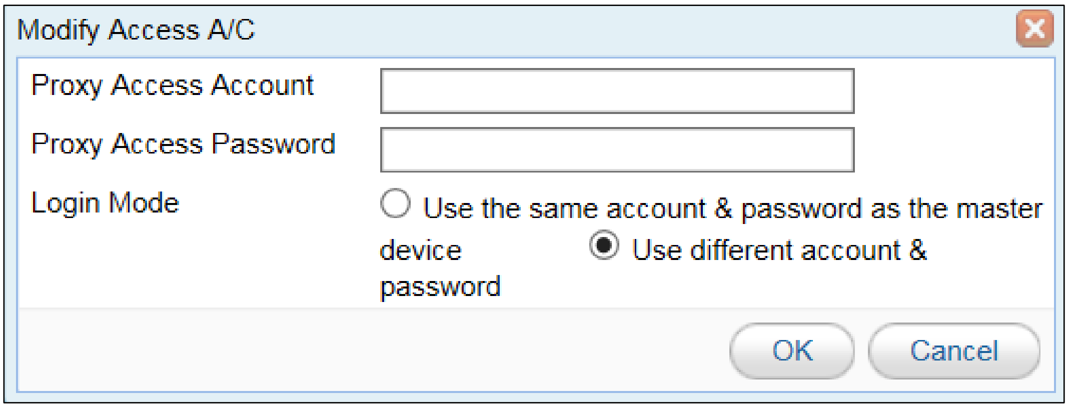
Cluster-test

□	Name / IP Address	Status	Product Version	Product Model	Deployment Mode	Management Mode	Auto Time Sync	Access Account
□	8008-GDJ-121 10:66:242::121	● Normal	V4.5R90F02	ADS 8000	Out-of-path	Cluster (master) test	Yes	Configured
□	VADS-GDJ-191 10.66.242.191	● Normal	V4.5R90F02	ADS VN01	Out-of-path	Cluster (slave) test	Yes	Configured

Step 2 Click multiple check boxes and then click **Edit**.

You can click **Select All** to select all devices and then configure parameters.

Figure 9-6 Modifying access accounts



Modify Access A/C

Proxy Access Account:

Proxy Access Password:

Login Mode: ○ Use the same account & password as the master device ● Use different account & password

Step 3 Click **OK** to save the settings.

----End

9.1.6 Synchronizing Time

On the **ADS Device** page, click 🕓 in the row of an ADS device to synchronize system time between the device and ADS M.

Note

- If system time is inconsistent between an ADS device and ADS M, the status icon of the device is displayed as , notifying you of time inconsistency. Inconsistent system time between two devices may impair the accuracy of statistical reports and device logs.
- You are advised to ensure consistent time between ADS devices and ADS M through the NTP service.

9.1.7 Manually Synchronizing Configurations

Only the master device has the manual synchronization function.

In the ADS device list shown in Figure 9-1, click in the **Operation** column to synchronize the settings of the master device to slave devices.

9.1.8 Saving the Configuration

After the ADS device configuration is complete, click in the row of an ADS device save the settings. You can click **Save** in the upper-right corner of the page shown in Figure 9-1 to save the settings of selected devices.

Caution

Pay attention to the followings when saving the configuration:

- Time synchronization and configuration saving can be performed on online ADS devices only.
- If you save the configuration, the configuration information is still valid after the ADS device is restarted; if you do not write to the firmware, the ADS device is restored to the state before it is edited once the device is restarted.

9.1.9 Configuring an ADS Device

After an ADS device is added, you can click its name/IP address to access its web-based manager for configuration. For how to configure an ADS device, see the *NSFOCUS ADS User Guide*.

9.2 Managing ADS Clusters

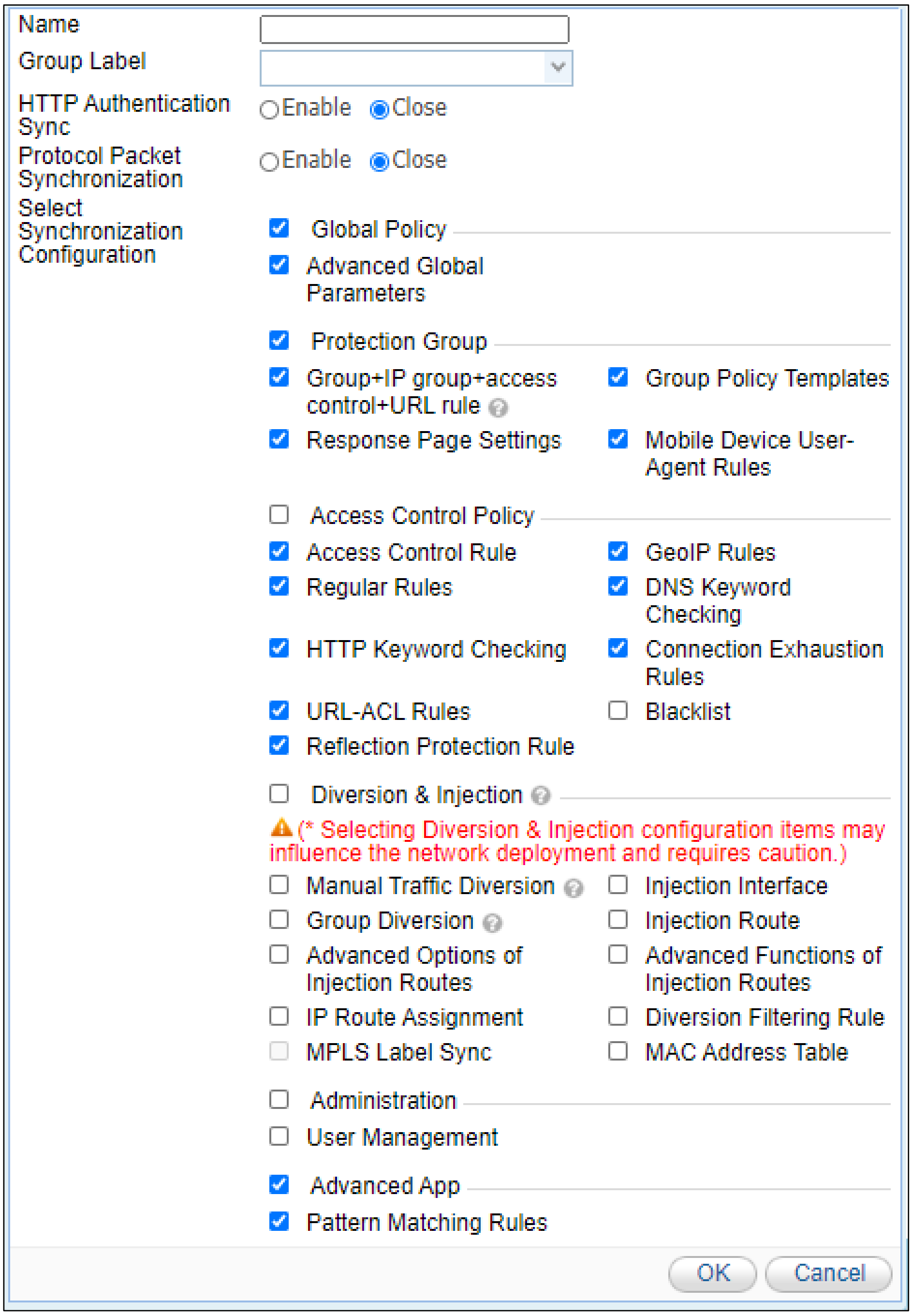
ADS cluster (that is, device group) facilitates centralized management and configuration of multiple ADS devices. In ADS cluster mode, after you configure protection parameters of the master device, slave devices automatically synchronize the configurations of protection groups configured on the master device. You can determine which configuration items need to be synchronized.

9.2.1 Adding an ADS Cluster

To add an ADS cluster, follow these steps:

Step 1 Click **Add Cluster** in the upper-right corner of the **ADS Device** page shown in Figure 9-1.

Figure 9-7 Adding an ADS cluster



Name

Group Label

HTTP Authentication Sync ○Enable ●Close

Protocol Packet Synchronization ○Enable ●Close

Select Synchronization Configuration

☑ Global Policy
☑ Advanced Global Parameters

☑ Protection Group
☑ Group+IP group+access control+URL rule ☑ Group Policy Templates
☑ Response Page Settings ☑ Mobile Device User-Agent Rules

□ Access Control Policy
☑ Access Control Rule ☑ GeoIP Rules
☑ Regular Rules ☑ DNS Keyword Checking
☑ HTTP Keyword Checking ☑ Connection Exhaustion Rules
☑ URL-ACL Rules □ Blacklist
☑ Reflection Protection Rule

□ Diversion & Injection
⚠(* Selecting Diversion & Injection configuration items may influence the network deployment and requires caution.)
□ Manual Traffic Diversion □ Injection Interface
□ Group Diversion □ Injection Route
□ Advanced Options of Injection Routes □ Advanced Functions of Injection Routes
□ IP Route Assignment □ Diversion Filtering Rule
□ MPLS Label Sync □ MAC Address Table

□ Administration
□ User Management

☑ Advanced App
☑ Pattern Matching Rules

Table 9-2 describes parameters of an ADS cluster.

Table 9-2 ADS cluster parameters

Parameter	Description
Name	Specifies the ADS cluster name. It must be 1 to 20 characters long and cannot contain angle brackets (<, or >), quotation marks (" or '), or slashes (/).

Parameter		Description
		The ADS cluster name is mandatory and must be unique.
Group Label		Specifies the group label for an ADS cluster The device tree in the left part displays ADS clusters by groups.
HTTP Authentication Sync		Controls whether to enable HTTP authentication synchronization.
Select Synchronization Configuration	Global Policy	Lists global settings that can be synchronized.
	Protection Group	Lists protection group settings that can be synchronized
	Access Control Policy	Lists access control rules that can be synchronized.
	Diversion & Injection	Lists diversion and injection settings that can be synchronized. Synchronizing such items may influence the network deployment. Therefore, handle with care.
	Administration	Controls whether to synchronize user settings.
	Advanced App	Controls whether to synchronize pattern matching rules and NTI.

Note

Currently, packet capture can be conducted in a centralized way in an ADS cluster. In other words, when packets are captured on the master device in a cluster, the system prompts whether to capture packets on slave devices.

Step 2 Set parameters in the dialog box and then click **OK**.

Then, the new ADS cluster is displayed on the treelike device list.

----End

9.2.2 Configuring a Cluster Blocklist

The cluster blocklist is used to temporarily or permanently block specified IP addresses. After the blocklist function is enabled, ADS devices in the cluster will block packets from IP addresses on the blocklist permanently or for a specified period, depending on the configuration.

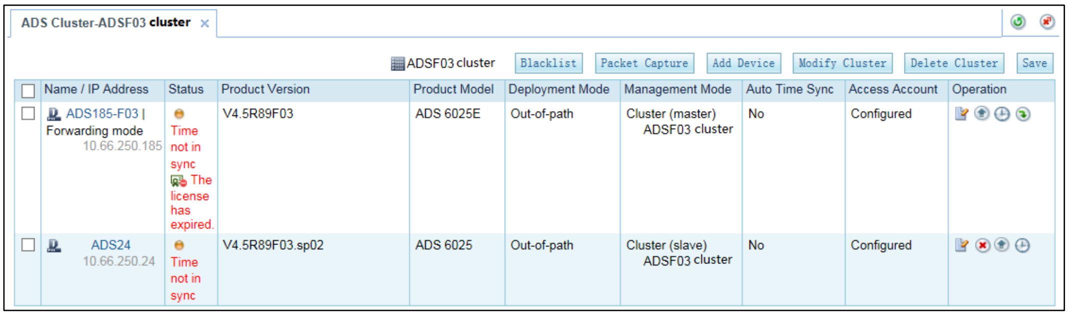
You must manually add IP addresses to the blocklist or import a blocklist file.

Note

To use the cluster blocklist, you must select the **Blacklist** check box under **Select Synchronization Configuration** when creating an ADS cluster.

After adding an ADS cluster, click its name on the treelike device list in the left pane to open the ADS cluster configuration page.

Figure 9-8 Configuring an ADS cluster



□	Name / IP Address	Status	Product Version	Product Model	Deployment Mode	Management Mode	Auto Time Sync	Access Account	Operation
□	ADS185-F03 | Forwarding mode 10.66.250.185	Time not in sync The license has expired.	V4.5R89F03	ADS 6025E	Out-of-path	Cluster (master) ADSF03 cluster	No	Configured	
□	ADS24 10.66.250.24	Time not in sync	V4.5R89F03.sp02	ADS 6025	Out-of-path	Cluster (slave) ADSF03 cluster	No	Configured	

Click **Blacklist** in the upper-right of the page to open the blocklist configuration page.

The blocklist is configured in the same way as that on ADS. For details, see the *NSFOCUS ADS User Guide*.

9.2.3 Configuring a Cluster GeoIP Library

The GeoIP library provides mappings between IP addresses and countries/regions. After importing a GeoIP library and configuring a GeoIP rule, you enable ADS to control traffic from certain IP addresses based on geographic locations.

Note	To use the cluster GeoIP library, you must select the **GeoIP Rules** check box under **Select Synchronization Configuration** when creating an ADS cluster.

After adding an ADS cluster, click its name on the treelike device list in the left pane to open the ADS cluster configuration page.

Click **Cluster GeoIP Library** in the upper-right corner of the page to open the **GeoIP Library Information** page. Click **Choose File**, select a file to be imported, and click **Import**. After the GeoIP library is imported, its version and update time will be displayed on the **GeoIP Library Information** page.

The GeoIP library supports both IPv4 and IPv6 addresses. When importing a GeoIP library, you must select the file type, which must be **.zip**. The file to be imported cannot exceed 20 MB.

9.2.4 Cluster Packet Capture

Cluster packet capture is to capture network packets from master and slave devices according to the configured conditions. Packets can be captured manually and automatically.

9.2.4.1 Configuring Manual Packet Capture

Creating a Manual Packet Capture Task

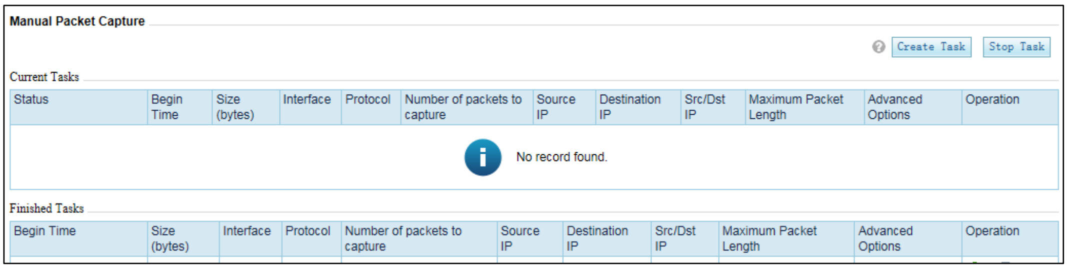
To create a manual packet capture task, follow these steps:

Step 1 On the page shown in Figure 9-8, click **Packet Capture**.

The packet capture configuration page appears. Figure 9-9 shows the **Manual Packet Capture** area.

In the upper part of the **Manual Packet Capture** area, the status of packet capture tasks is displayed. When the packet capture task is in progress, **Status** is displayed as **Ongoing**. When the packet capture task is manually stopped, **Status** is displayed as **Stopped**.

Figure 9-9 Manual Packet Capture area



Manual Packet Capture

Current Tasks

Status	Begin Time	Size (bytes)	Interface	Protocol	Number of packets to capture	Source IP	Destination IP	Src/Dst IP	Maximum Packet Length	Advanced Options	Operation

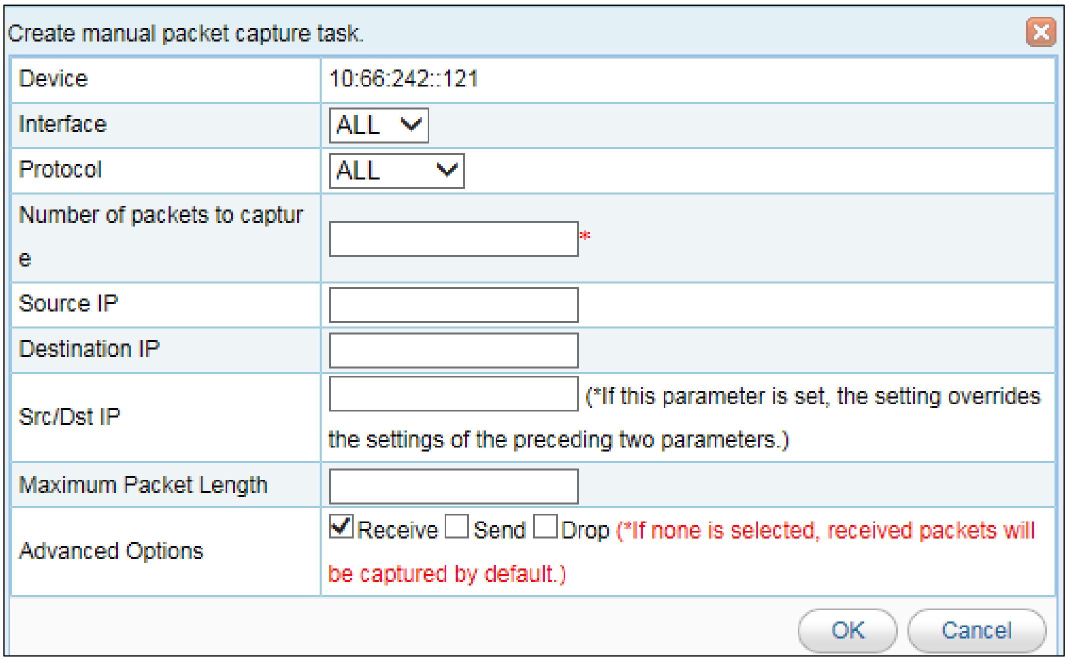
No record found.

Finished Tasks

Begin Time	Size (bytes)	Interface	Protocol	Number of packets to capture	Source IP	Destination IP	Src/Dst IP	Maximum Packet Length	Advanced Options	Operation

Step 2 Click Create Task.

Figure 9-10 Creating a manual packet capture task



Create manual packet capture task.

Device	10:66:242::121
Interface	ALL
Protocol	ALL
Number of packets to captur e	*
Source IP	
Destination IP	
Src/Dst IP	(*If this parameter is set, the setting overrides the settings of the preceding two parameters.)
Maximum Packet Length	
Advanced Options	☑ Receive □ Send □ Drop (*If none is selected, received packets will be captured by default.)

Step 3 Configure manual packet capture parameters.

Table 9-3 Parameters for creating a manual packet capture task

Parameter	Description
Device	Device object of this task, which cannot be modified.
Interface	Interface on which packets are captured for this task. **ALL** indicates that packets on

Parameter	Description
	all interfaces are captured.
Protocol	Specifies a protocol. Packets using the specified protocol will be captured. The value can be **ALL** , **TCP**, **UDP**, **ICMP**, or **ICMPv6**, with **ALL** as the default value.
Number of packets to capture	Number of the packets to be captured. The value ranges from 1 to 30000.
Source IP	Specifies the source IP address of this task. This parameter is optional. Leaving this parameter empty indicates that packets from any IP address will be captured. Note The source IP address can be an IPv4 or IPv6 address.
Destination IP	Specifies the destination IP address of this task. This parameter is optional. Leaving this parameter empty indicates that packets to any IP address will be captured. Note The destination IP address can be an IPv4 or IPv6 address.
Src/Dst IP	Specifies the source or destination IP address of this task. This parameter is optional. If you set this parameter, ignore **Source IP** and **Destination IP**. Note Both IPv4 and IPv6 addresses are allowed.
Maximum Packet Length	Specifies the maximum length of the packets to be captured. The value ranges from 64 to 1518.
Advanced Options	This parameter is optional. Options include **Receive**, **Send**, and **Drop**. • **Receive**: indicates that ADS captures received packets. • **Send**: indicates that ADS captures packets that are sent. • **Drop**: indicates that ADS captures dropped packets. If none is selected, received packets will be captured by default.

Step 4 Click **OK**.

The new manual packet task starts immediately after being created and the status is displayed in the current task list.

----End

Stopping a Manual Packet Capture Task

You can stop a manual packet capture task in either of the following ways:

- Method 1: In the current task list shown in Figure 9-9, click ⊖ in the **Operation** column of a manual packet capture task to stop this task immediately.
- Method 2: In Figure 9-9, click **Stop Task** in the upper-right corner of the page to immediately stop manual packet capture tasks that are in progress.

Downloading a Master's Manual Packet Capture File

In the current task list shown in Figure 9-9, click ⬇ in the **Operation** column of a manual packet capture task to download the master's manual packet capture file to a local disk drive.

Download a Cluster Manual Packet Capture File

In the current task list shown in Figure 9-9, click 💾 in the **Operation** column of a manual packet capture task to download the cluster's (including both master and slave devices') manual packet capture file to a local disk drive.

Duplicating a Manual Packet Capture Task

To duplicate a manual packet capture task, follow these steps:

Step 1 In the current task list shown in Figure 9-9, click ⧉ in the **Operation** column of a manual packet capture task to copy this task and edit its parameters.

Step 2 After editing parameters, click **OK** to start this manual packet capture task immediately.

----End

Deleting a Manual Packet Capture Task

In the completed task list shown in Figure 9-9, click ⊗ in the **Operation** column of a manual packet capture task and then click **OK** in the confirmation dialog box to delete this task.

9.2.4.2 Configuring Automatic Packet Capture

Creating an Automatic Packet Capture Task

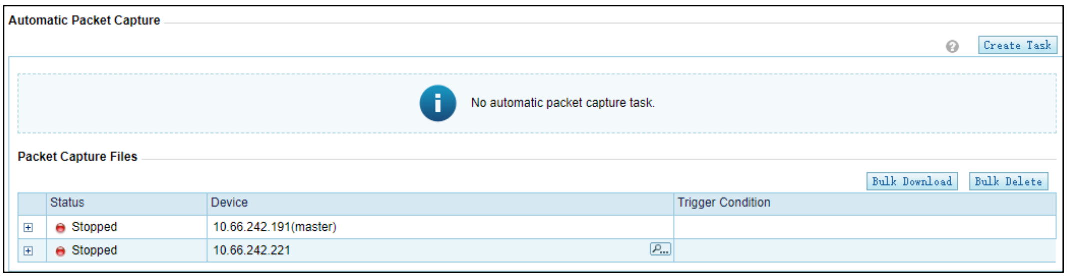
To configure an automatic packet capture task, follow these steps:

Step 1 In Figure 9-8, click **Packet Capture**.

The packet capture configuration page appears. Figure 9-11 shows the **Automatic Packet Capture** area.

In the upper part of the **Automatic Packet Capture** area, the status of packet capture tasks is displayed. When the packet capture task is in progress, **Status** is displayed as **Ongoing**. When the packet capture task is manually stopped, **Status** is displayed as **Stopped**.

Figure 9-11 Automatic Packet Capture area



Automatic Packet Capture

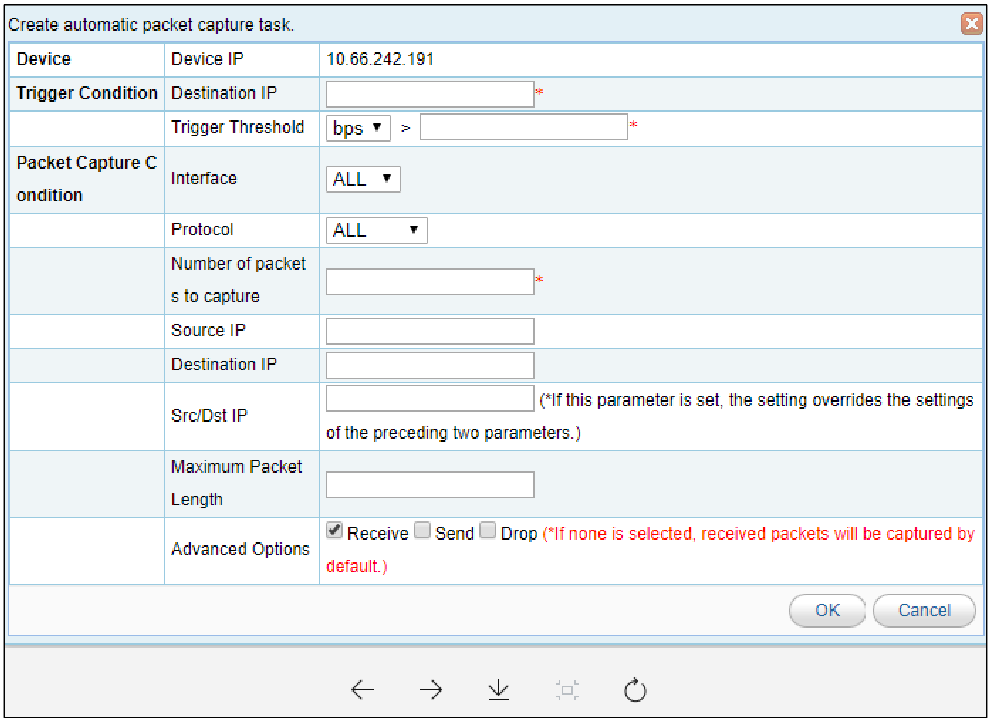
No automatic packet capture task.

Packet Capture Files

	Status	Device	Trigger Condition
⊞	● Stopped	10.66.242.191(master)	
⊞	● Stopped	10.66.242.221	

Step 2 Click Create Task.

Figure 9-12 Creating an automatic packet capture task



Create automatic packet capture task.

Device	Device IP	10.66.242.191
Trigger Condition	Destination IP	*
	Trigger Threshold	bps ▼ > *
Packet Capture Condition	Interface	ALL ▼
	Protocol	ALL ▼
	Number of packets to capture	*
	Source IP	
	Destination IP	
	Src/Dst IP	(*If this parameter is set, the setting overrides the settings of the preceding two parameters.)
	Maximum Packet Length	
	Advanced Options	☑ Receive □ Send □ Drop (*If none is selected, received packets will be captured by default.)

Table 9-4 describes some parameters for creating an automatic packet capture task. For details, see Table 9-3.

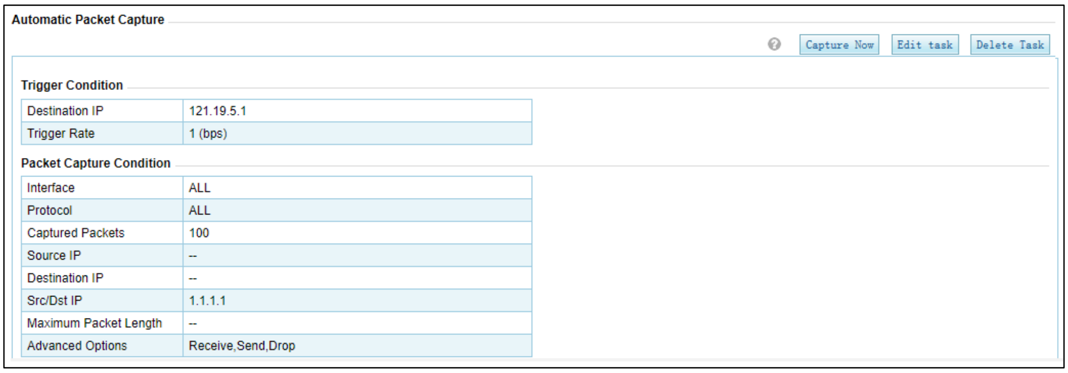
Table 9-4 Parameters for creating an automatic packet capture task

Parameter	Description
Device IP	Device object of this task, which cannot be modified.
Destination IP	Specifies the destination IP address for this packet capture task.
Triggering Threshold	Specifies the number of packets received by the destination IP address per second that will trigger automatic packet capture. The value range is 1–4294967295 pps or 1–42949672960 bps.

Step 3 Click **OK** to complete the configuration.

The newly created automatic packet capture task will be displayed in the **Automatic Packet Capture** area shown in Figure 9-13 and it starts only when the specified conditions are triggered.

Figure 9-13 Newly created automatic packet capture task



Trigger Condition

Destination IP	121.19.5.1
Trigger Rate	1 (bps)

Packet Capture Condition

Interface	ALL
Protocol	ALL
Captured Packets	100
Source IP	--
Destination IP	--
Src/Dst IP	1.1.1.1
Maximum Packet Length	--
Advanced Options	Receive,Send,Drop

----End

Stopping an Automatic Packet Capture Task

After an automatic packet capture task is created, click **Stop Task** in the upper-right of the **Automatic Packet Capture** area shown in Figure 9-13 to stop this task immediately.

After the automatic packet capture task is stopped, **Status** is displayed as **Stopped**.

Starting an Automatic Packet Capture Task

Stopped automatic packet capture tasks can be manually started.

In the **Automatic Packet Capture** area shown in Figure 9-13, click **Capture Now** in the upper-right corner to start the automatic packet capture task immediately.

When the packet capture task is in progress, **Status** is displayed as **Ongoing**.

Editing an Automatic Packet Capture Task

To edit an automatic packet capture task, follow these steps:

Step 1 In the **Automatic Packet Capture** area shown in Figure 9-13, click **Edit Task** in the upper-right corner.

Step 2 After editing parameters, click **OK** to save the settings.

----End

Deleting Automatic Packet Capture Files

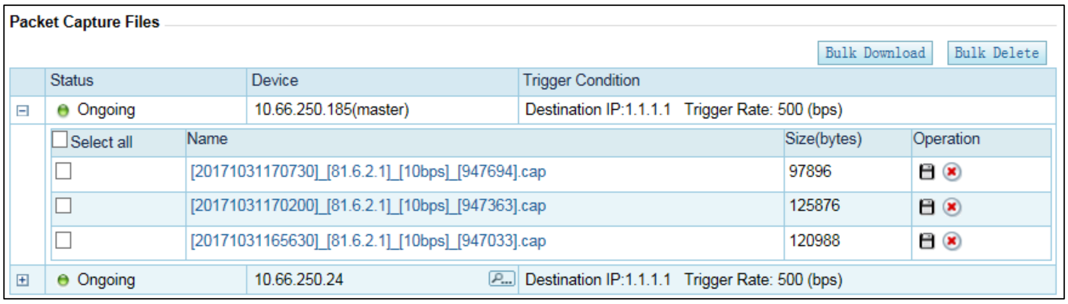
You can delete automatic packet capture files one by one or in batches.

Deleting Automatic Packet Capture Files One by One

To delete an automatic packet capture file, follow these steps:

Step 1 In the **Packet Capture Files** area shown in Figure 9-11, click ⊞ to expand the automatic packet capture file list.

Figure 9-14 Packet capture files



Packet Capture Files

	Status	Device	Trigger Condition
⊟	● Ongoing	10.66.250.185(master)	Destination IP:1.1.1.1 Trigger Rate: 500 (bps)

□ Select all	Name	Size(bytes)	Operation
□	[20171031170730]_[81.6.2.1]_[10bps]_[947694].cap	97896	💾 ⊗
□	[20171031170200]_[81.6.2.1]_[10bps]_[947363].cap	125876	💾 ⊗
□	[20171031165630]_[81.6.2.1]_[10bps]_[947033].cap	120988	💾 ⊗

	Status	Device	Trigger Condition
⊞	● Ongoing	10.66.250.24	Destination IP:1.1.1.1 Trigger Rate: 500 (bps)

Step 2 Click ⊗ in the **Operation** column of a packet capture file and then click **OK** in the confirmation dialog box.

----End

Deleting Automatic Packet Capture Files in Batches

Step 1 In Figure 9-14, select the check box(es) of one or more automatic packet capture files and then click **Bulk Delete**.

Step 2 Click **OK** in the confirmation dialog box.

----End

Viewing an Automatic Packet Capture File

In Figure 9-14, click the name of an automatic packet capture file to view its details.

Downloading an Automatic Packet Capture File

You can download automatic packet capture files one by one or in batches.

Downloading Automatic Packet Capture Files One by One

In Figure 9-14, click 💾 in the **Operation** column of an automatic packet capture file to download this file to a local disk drive.

Downloading Automatic Packet Capture Files in Batches

In Figure 9-14, select the check box(es) of one or more automatic packet capture files and then click **Bulk Download** to download the selected file(s) to a local disk drive.

9.2.5 Configuring a Cluster Threat Intelligence Policy

The system supports threat intelligence-based security checks, helping users better identify and detect various cyber threats. For high-risk IP addresses, ADS automatically lists them on the blocklist and blocks packets from these addresses.

Note

To use the cluster threat intelligence, you must select the **NTI** check box under **Select Synchronization Configuration** when creating an ADS cluster.

After adding an ADS cluster, click its name on the treelike device list in the left pane to open the ADS cluster configuration page.

Click **Cluster Threat Intelligence** in the upper-right of the page to redirect to the **NTI Configuration** page on the web-based manager of ADS.

For details about how to configure the threat intelligence, see the *NSFOCUS ADS User Guide*.

9.2.6 Adding an ADS Device to the Cluster

In Figure 9-8, click **Add Device** to add an ADS device to the cluster.

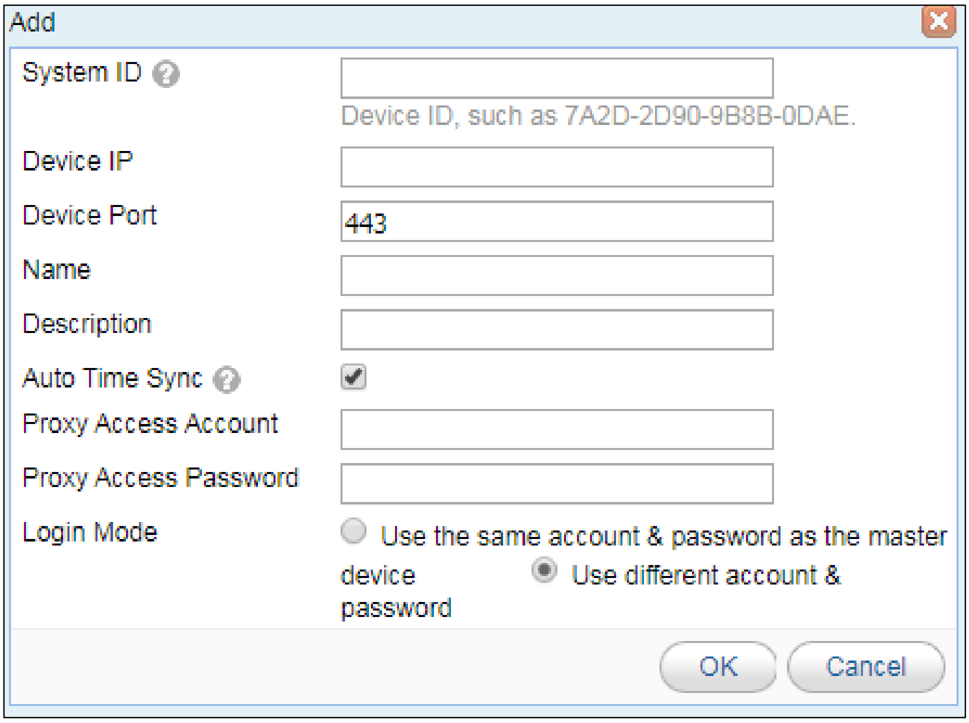
For description of parameters for adding an ADS device, see Table 9-1.

In addition to adding a device, you can perform the following operations on the cluster configuration page:

- Editing a device
- Deleting a device
- Synchronizing time
- Manually synchronizing configurations
- Saving the configuration

For details, see section 9.1 Managing ADS Devices.

Figure 9-15 Adding an device to the cluster


Add

System ID

Device ID, such as 7A2D-2D90-9B8B-0DAE.

Device IP

Device Port: 443

Name

Description

Auto Time Sync: ☑

Proxy Access Account

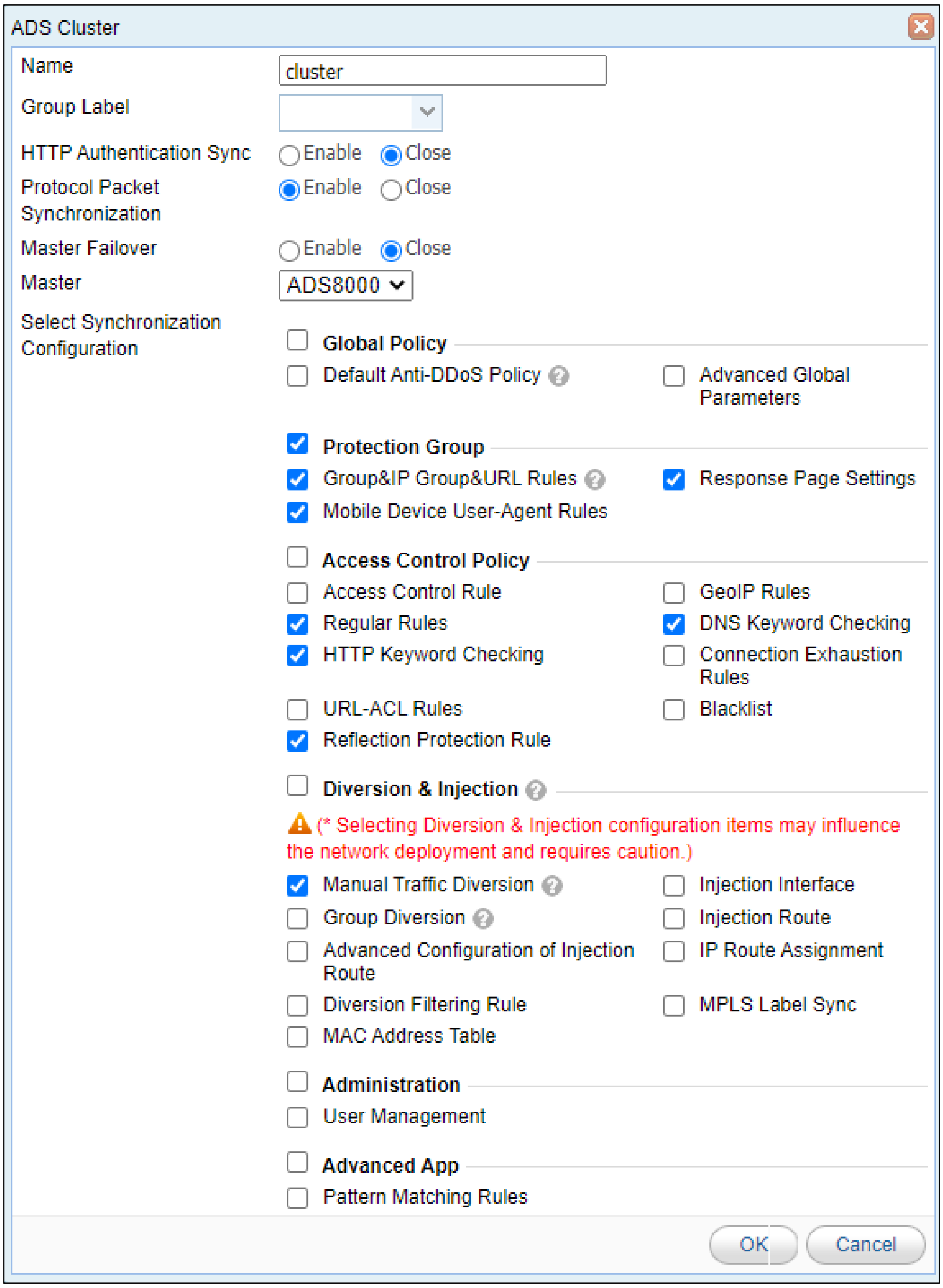
Proxy Access Password

Login Mode: ○ Use the same account & password as the master device ● Use different account & password

9.2.7 Modifying a Cluster

In Figure 9-8, click an ADS cluster name on the left treelike device list and then click **Modify Cluster** on the ADS cluster configuration page to modify settings of this cluster. See Figure 9-16.

Figure 9-16 Modifying an ADS cluster



ADS Cluster

Name: cluster

Group Label:

HTTP Authentication Sync: ○ Enable ● Close

Protocol Packet Synchronization: ● Enable ○ Close

Master Failover: ○ Enable ● Close

Master: ADS8000

Select Synchronization Configuration

□ **Global Policy**

□ Default Anti-DDoS Policy
□ Advanced Global Parameters

☑ **Protection Group**

☑ Group&IP Group&URL Rules
☑ Response Page Settings
☑ Mobile Device User-Agent Rules

□ **Access Control Policy**

□ Access Control Rule
□ GeoIP Rules
☑ Regular Rules
☑ DNS Keyword Checking
☑ HTTP Keyword Checking
□ Connection Exhaustion Rules
□ URL-ACL Rules
□ Blacklist
☑ Reflection Protection Rule

□ **Diversion & Injection**

⚠ (* Selecting Diversion & Injection configuration items may influence the network deployment and requires caution.)

☑ Manual Traffic Diversion
□ Injection Interface
□ Group Diversion
□ Injection Route
□ Advanced Configuration of Injection Route
□ IP Route Assignment
□ Diversion Filtering Rule
□ MPLS Label Sync
□ MAC Address Table

□ **Administration**

□ User Management

□ **Advanced App**

□ Pattern Matching Rules

Note

- When a cluster includes one or more ADS devices, you can configure a master device and edit its settings. A cluster can have only one master device.
- ADS clusters without a master device are not displayed on the device list under **Region**. You cannot perform any operations on devices in such clusters.

9.2.8 Deleting a Cluster

In Figure 9-8, click an ADS cluster name on the left treelike device list and then click **Delete Cluster** on the ADS cluster configuration page to delete the cluster. As an ADS cluster is deleted, ADS devices in this cluster will not be deleted but automatically switch to the standalone mode.

Caution	- Once an ADS cluster is deleted, you cannot continue to view opened monitoring page, configuration page, or other pages that relate to this cluster. - In a cluster, the master device cannot be deleted except that the cluster has only one device.

9.2.9 Saving the Configuration

In Figure 9-8, select the check box(es) of one or more devices and then click **Save** in the upper-right corner to save the configuration of the selected device(s).

Caution	Note the following when saving the configuration: - Time synchronization and configuration saving can be performed only on online ADS devices. - If you save the configuration, the configuration information remains valid after the ADS device is restarted; if you do not save the configuration, the ADS device is restored to the state before it is edited once the device is restarted.

9.3 Managing NTA Devices

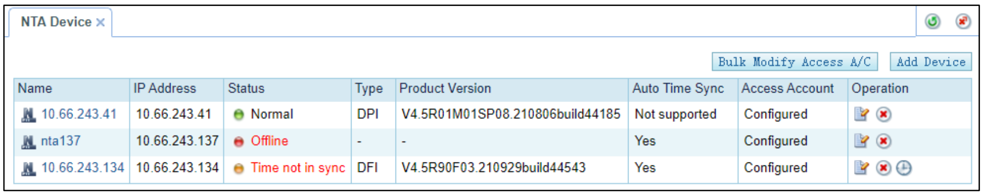
To configure an NTA device, follow these steps:

Step 1 Choose **Device Management > Device Management**. Click **NTA Device** under **Device Management**.

The **NTA Device** page appears, as shown in Figure 9-17. Initially, the device list is empty and you need to add a device manually.

If the license of NTA is about to expire in less than seven days, the system displays a message indicating that the license will expire in X days. When the license validity period is displayed as 0 days, the system displays a message indicating that the license is invalid or expires.

Figure 9-17 NTA Device page



Name	IP Address	Status	Type	Product Version	Auto Time Sync	Access Account	Operation
10.66.243.41	10.66.243.41	● Normal	DPI	V4.5R01M01SP08.210806build44185	Not supported	Configured	
nta137	10.66.243.137	● Offline	-	-	Yes	Configured	
10.66.243.134	10.66.243.134	● Time not in sync	DFI	V4.5R90F03.210929build44543	Yes	Configured	

Step 2 Click a device to reconfigure its settings.

Prior to adding an NTA device, you need to log in to the web-based manager of this **device to** verify that this device is subordinate to ADS M (**Administration > Third-Party Interface > Management Mode**) and type the IP address of ADS M**.** For details, see the *NSFOCUS NTA User Guide*. After you complete the configuration and properly connect the two devices, this NTA device is subordinate to ADS M and appears in the tree structure of monitoring objects.

The **NTA Device** page lists the name, IP address, status, type, product version, automatic time synchronization, access account, and supported operations of the NTA devices.

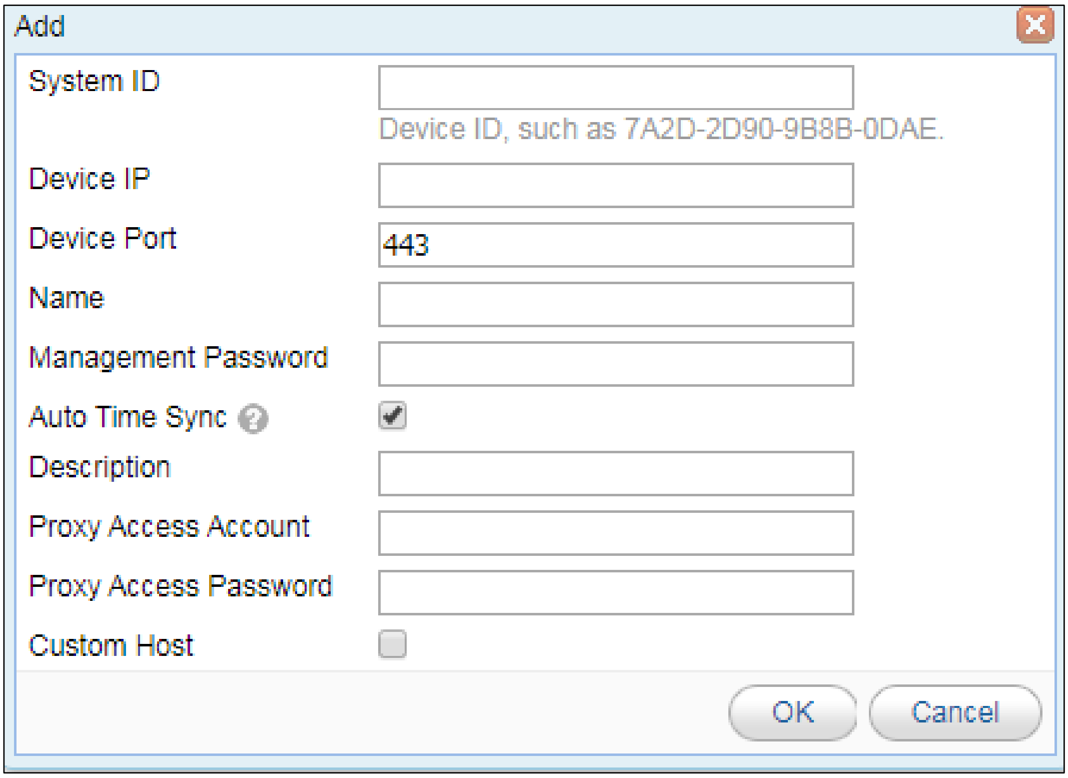
----End

9.3.1 Adding an NTA Device

To add an NTA device, follow these steps:

Step 1 Click **Add Device** in the upper-right corner of the **NTA Device** page.

Figure 9-18 Adding an NTA device



Add

System ID	Device ID, such as 7A2D-2D90-9B8B-0DAE.
Device IP	
Device Port	443
Name	
Management Password	
Auto Time Sync	☑
Description	
Proxy Access Account	
Proxy Access Password	
Custom Host	□

Table 9-5 describes parameters of an NTA device.

Table 9-5 NTA device parameters

Parameter	Description
System ID	Specifies the system ID of an NTA device. This parameter is mandatory.

Parameter	Description
Device IP	Specifies the IP address of an NTA device. Either an IPv4 or IPv6 address is acceptable. This parameter is mandatory.
Device Port	Specifies the port of the device. The default value is **443**.
Name	Specifies the name of an NTA device. The name should be 1 to 20 characters long and cannot contain angle brackets (<, or >), quotation marks (" or '), or slashes (/). A new name cannot duplicate that of an existing device. This parameter is mandatory.
Management Password	Specifies the management password of NTA V4.5R90F00. It must be the same as the authorization key configured on the web-based manager (**Administration** > **Third-Party Interface** > **Management Mode**) of NTA. Note NTA V4.5.61.2 does not require the management password.
Auto Time Sync	After it is selected, time on NTA will be in synchronization with that on ADS M.
Description	Specifies the brief description of an NTA device, for example, device usage.
Proxy Access Account	Specifies the account of the proxy NTA device. After the proxy access account and password are configured, ADS M can directly log in to the corresponding NTA device.
Proxy Access Password	Specifies the password of the proxy NTA device. After the proxy access account and password are configured, ADS M can directly log in to the corresponding NTA device.
Custom Host	Specifies the NTA proxy's host name.

Step 2 Set parameters in the dialog box and click **OK**.

----End

9.3.2 Modifying NTA Device Settings

On the **NTA Device** page, click 📝 in the row of an NTA device to modify the information about this device. Note that the device ID or device IP cannot be edited.

9.3.3 Deleting an NTA Device

On the **NTA Device** page, click ✖ in the row of an NTA device to delete this device. After an NTA device is deleted, it is no longer subject to management of ADS M, nor will it upload information to ADS M.

Note	Once an NTA device is deleted, you cannot continue to view the opened monitoring page, configuration page, or other pages that relate to this device.

After adding an NTA device, you need to configure traffic diversion settings before the interaction between ADS and NTA devices. For details, see the *NSFOCUS NTA User Guide*.

9.3.4 Modifying Access Accounts in Batches

You can modify NTA access account passwords in batches in the same way as ADS access accounts. For details, see section 9.1.5 Modifying Access Accounts in Batches.

9.3.5 Configuring an NTA Device

After an NTA device is added, you can click its name to access its web-based manager for configuration. For how to configure an NTA device, see the *NSFOCUS NTA User Guide*.

Note	The web-based manager of NTA is accessible only when **Managed Device Access** is set to **Open**. For details, see section 3.1.1 Basic Settings.

10 Console-based System Management

This chapter mainly covers:

Section	Description
Overview	Describes the introduction of the console.
Login to the Console	Describes how to log in to the console.
Console Configuration	Describes how to configure the console.

10.1 Overview

Using console port connections, you can access the console management interface to perform operations such as restoration of initial configuration, status detection, and system restoration, which cannot be conducted on the web-based manager.

10.2 Login to the Console

Before logging in to the console, prepare the following:

- One PC
- One serial cable shipped with the device
- Terminal software that can connect to the console port (for example, the HyperTerminal software that comes with the Windows operating system)
- Connection of ADS M to the PC with the serial cable

To log in to ADS M via the console port, follow these steps:

Step 1 Use terminal software to connect to the ADS M console via a serial port.

For serial communication parameters, see appendix B Default Parameters.

Step 2 Type the default user name and password of the console administrator.

If the user name and password are correct, you will successfully log in to the console.

----End

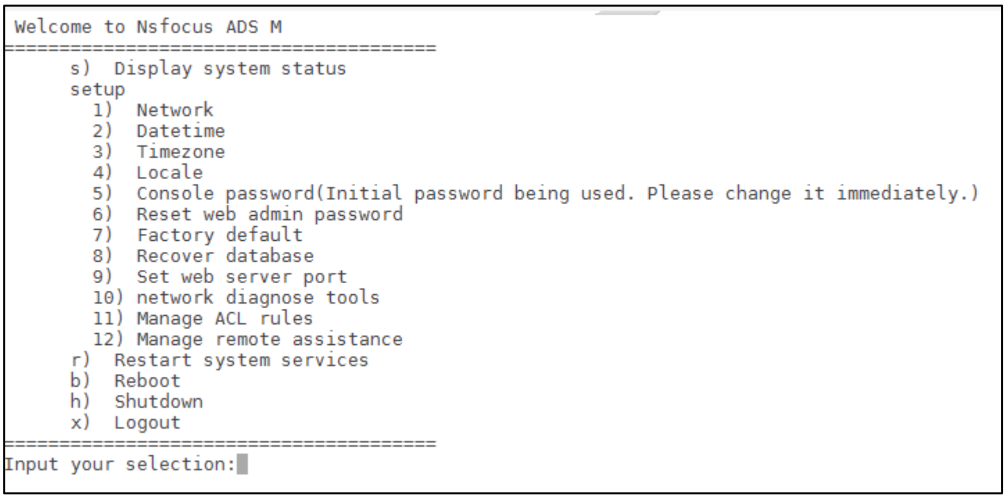
After login, if you remain inactive on the console within 20 minutes, the system logs you out of the console unconditionally. To continue your operation, you must log in again.

10.3 Console Configuration

After a successful login, the main menu is displayed, as shown in Figure 10-1. Type a sequence number as prompted and press **Enter** to open a menu.

If you log in to the console with the default password, the system reminds you to change the password. You are advised to change a new password. For how to change the password, see section 10.3.6 Changing the Console Password.

Figure 10-1 Main menu of the console

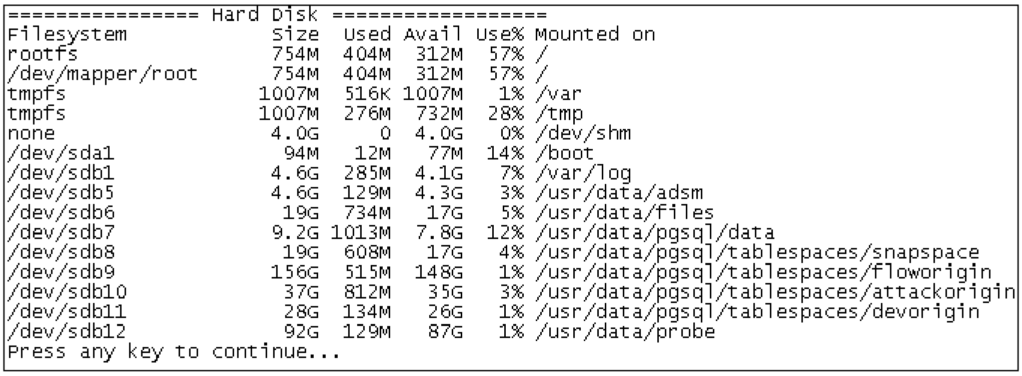


```
 Welcome to Nsfocus ADS M
======================================
      s)  Display system status
      setup
        1)  Network
        2)  Datetime
        3)  Timezone
        4)  Locale
        5)  Console password(Initial password being used. Please change it immediately.)
        6)  Reset web admin password
        7)  Factory default
        8)  Recover database
        9)  Set web server port
        10) network diagnose tools
        11) Manage ACL rules
        12) Manage remote assistance
      r)  Restart system services
      b)  Reboot
      h)  Shutdown
      x)  Logout
======================================
Input your selection:
```

10.3.1 Checking System Status

On the main menu, type **s** and press **Enter** to view the system status. As shown in Figure 10-2, the displayed screen shows the hard disk mount status, system status, network status, and route status, from which you can determine the system operating condition.

Figure 10-2 Checking system status

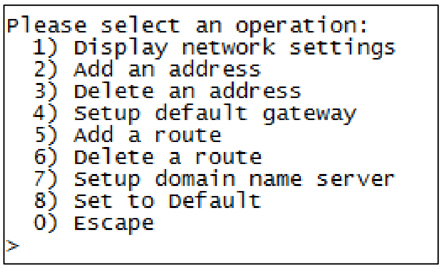


```
================ Hard Disk ==================
Filesystem            Size  Used Avail Use% Mounted on
rootfs                754M  404M  312M  57% /
/dev/mapper/root      754M  404M  312M  57% /
tmpfs                1007M  516K 1007M   1% /var
tmpfs                1007M  276M  732M  28% /tmp
none                  4.0G     0  4.0G   0% /dev/shm
/dev/sda1              94M   12M   77M  14% /boot
/dev/sdb1             4.6G  285M  4.1G   7% /var/log
/dev/sdb5             4.6G  129M  4.3G   3% /usr/data/adsm
/dev/sdb6              19G  734M   17G   5% /usr/data/files
/dev/sdb7             9.2G 1013M  7.8G  12% /usr/data/pgsql/data
/dev/sdb8              19G  608M   17G   4% /usr/data/pgsql/tablespaces/snapspace
/dev/sdb9             156G  515M  148G   1% /usr/data/pgsql/tablespaces/floworigin
/dev/sdb10             37G  812M   35G   3% /usr/data/pgsql/tablespaces/attackorigin
/dev/sdb11             28G  134M   26G   1% /usr/data/pgsql/tablespaces/devorigin
/dev/sdb12             92G  129M   87G   1% /usr/data/probe
Press any key to continue...
```

10.3.2 Configuring Network Settings

On the main menu, type **1** and press **Enter** to access the network setting menu, as shown in Figure 10-3. On this menu, you can type **0** and press **Enter** to return to the main menu.

Figure 10-3 Network setting menu

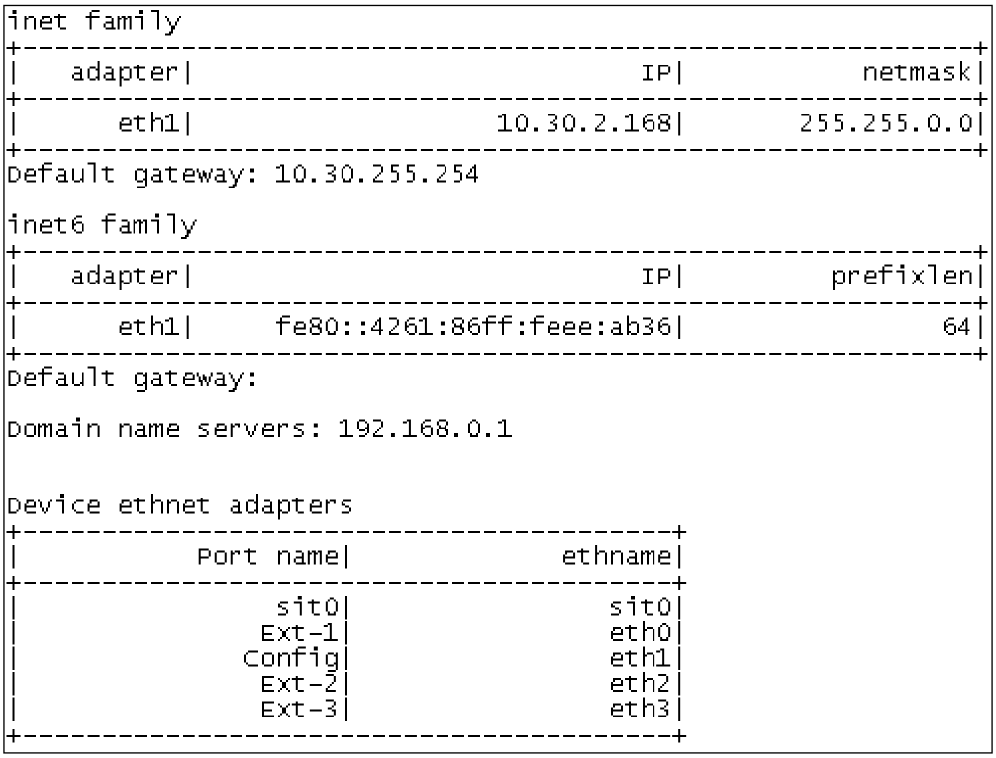


```
Please select an operation:
  1) Display network settings
  2) Add an address
  3) Delete an address
  4) Setup default gateway
  5) Add a route
  6) Delete a route
  7) Setup domain name server
  8) Set to Default
  0) Escape
>
```

Viewing Network Settings

On the network setting menu, type **1** and press **Enter** to view network settings, as shown in Figure 10-4. The following screen displays network settings of the current system interface.

Figure 10-4 Viewing network settings

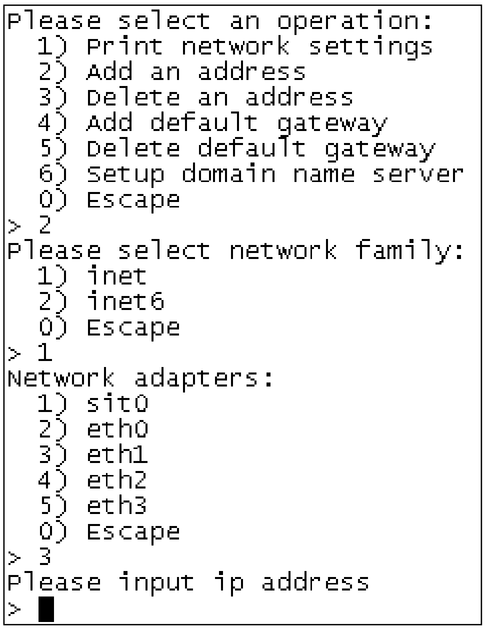


```
inet family
+------------------------------------------------------------+
|   adapter|                            IP|           netmask|
+------------------------------------------------------------+
|      eth1|                   10.30.2.168|       255.255.0.0|
+------------------------------------------------------------+
Default gateway: 10.30.255.254

inet6 family
+------------------------------------------------------------+
|   adapter|                            IP|         prefixlen|
+------------------------------------------------------------+
|      eth1|     fe80::4261:86ff:feee:ab36|                64|
+------------------------------------------------------------+
Default gateway:

Domain name servers: 192.168.0.1


Device ethnet adapters
+-----------------------------------------+
|           Port name|             ethname|
+-----------------------------------------+
|                sit0|                sit0|
|               Ext-1|                eth0|
|              Config|                eth1|
|               Ext-2|                eth2|
|               Ext-3|                eth3|
+-----------------------------------------+
```

Adding an IP Address

On the network setting menu, type **2** and press **Enter** to configure an IP address of the system management interface. Type the IP address and subnet mask of the network interface, and press **Enter**. Then the system displays the settings and return to the network setting menu, as shown in Figure 10-5.

Figure 10-5 Adding an IP address

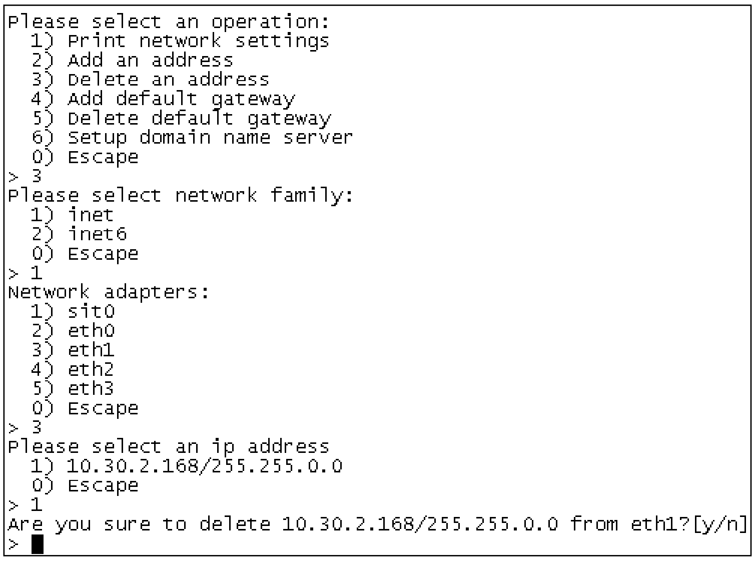


```
Please select an operation:
  1) Print network settings
  2) Add an address
  3) Delete an address
  4) Add default gateway
  5) Delete default gateway
  6) Setup domain name server
  0) Escape
> 2
Please select network family:
  1) inet
  2) inet6
  0) Escape
> 1
Network adapters:
  1) sit0
  2) eth0
  3) eth1
  4) eth2
  5) eth3
  0) Escape
> 3
Please input ip address
> 
```

Deleting an IP Address

On the network setting menu, type **3** and press **Enter** to delete an IP address. Select the IP address to be deleted, type **y** and press **Enter** to delete it and return to the network setting menu, as shown in Figure 10-6.

Figure 10-6 Deleting an IP address

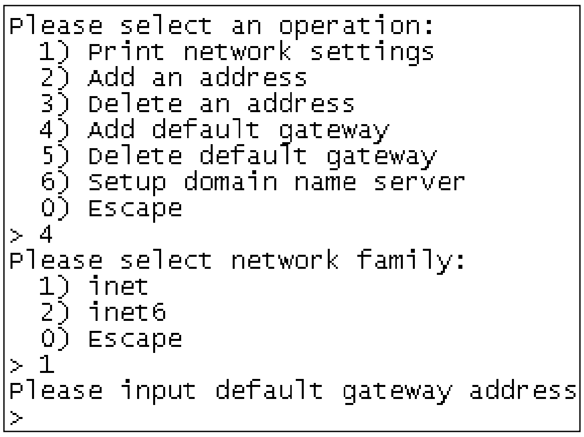


```
Please select an operation:
  1) Print network settings
  2) Add an address
  3) Delete an address
  4) Add default gateway
  5) Delete default gateway
  6) Setup domain name server
  0) Escape
> 3
Please select network family:
  1) inet
  2) inet6
  0) Escape
> 1
Network adapters:
  1) sit0
  2) eth0
  3) eth1
  4) eth2
  5) eth3
  0) Escape
> 3
Please select an ip address
  1) 10.30.2.168/255.255.0.0
  0) Escape
> 1
Are you sure to delete 10.30.2.168/255.255.0.0 from eth1?[y/n]
> 
```

Adding a Default Gateway

On the network setting menu, type **4** and press **Enter** to add a default gateway. Type the IP address of the gateway as prompted, and press **Enter**. Then the system displays the settings and return to the network setting menu, as shown in Figure 10-7.

Figure 10-7 Adding a default gateway

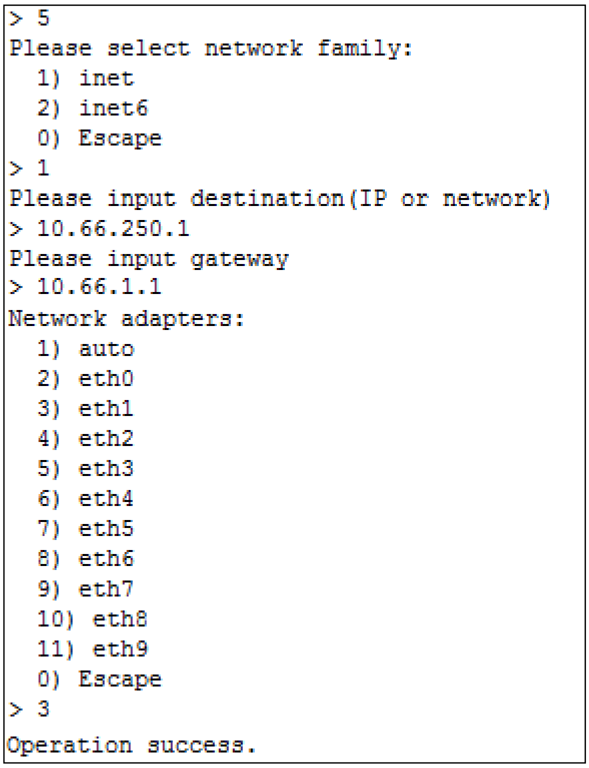


```
Please select an operation:
  1) Print network settings
  2) Add an address
  3) Delete an address
  4) Add default gateway
  5) Delete default gateway
  6) Setup domain name server
  0) Escape
> 4
Please select network family:
  1) inet
  2) inet6
  0) Escape
> 1
Please input default gateway address
>
```

Adding a Route

On the networking menu, type **5** and press **Enter** to add a route. Type the IP address and gateway address as prompted, select an interface, and press **Enter**. Then the system displays the configured route and returns to the networking menu, as shown in Figure 10-8.

Figure 10-8 Adding a route

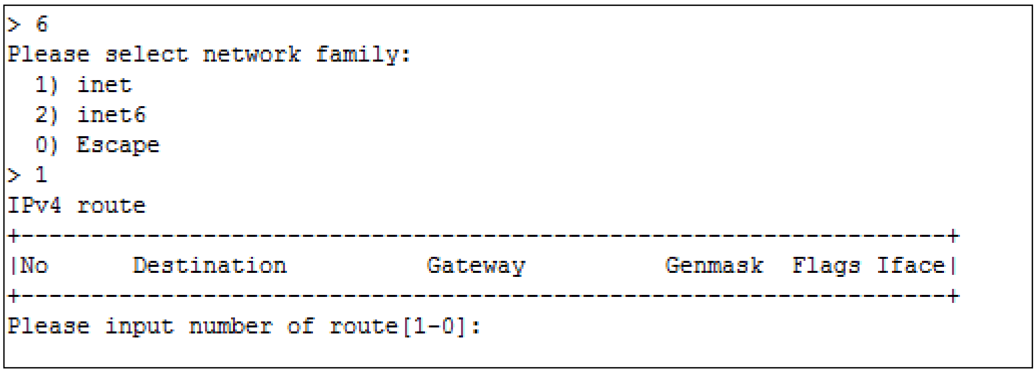


```
> 5
Please select network family:
  1) inet
  2) inet6
  0) Escape
> 1
Please input destination(IP or network)
> 10.66.250.1
Please input gateway
> 10.66.1.1
Network adapters:
  1) auto
  2) eth0
  3) eth1
  4) eth2
  5) eth3
  6) eth4
  7) eth5
  8) eth6
  9) eth7
  10) eth8
  11) eth9
  0) Escape
> 3
Operation success.
```

Deleting a Route

On the network setting menu, type **6** and press **Enter** to delete a route. Select a desired route, type **y** and press **Enter** to delete it and return to the network setting menu, as shown in Figure 10-9.

Figure 10-9 Deleting a route

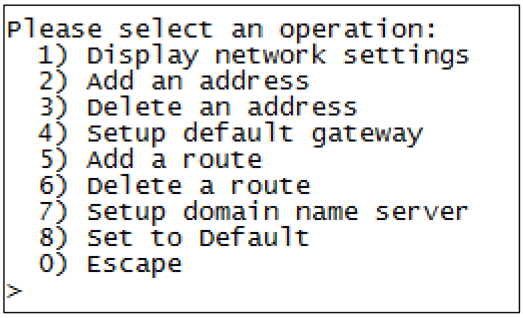


```
> 6
Please select network family:
  1) inet
  2) inet6
  0) Escape
> 1
IPv4 route
+--------------------------------------------------------------------+
|No      Destination          Gateway           Genmask  Flags Iface|
+--------------------------------------------------------------------+
Please input number of route[1-0]:
```

Configuring a DNS Server

On the network setting menu, type **7** and press **Enter** to configure a DNS server. Type the IP address of the DNS as prompted, and press **Enter** to save the setting and return to the network setting menu, as shown in Figure 10-10.

Figure 10-10 Configuring the DNS server

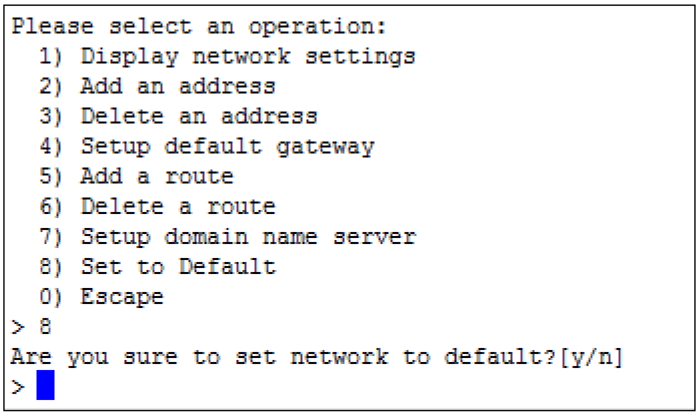


```
Please select an operation:
  1) Display network settings
  2) Add an address
  3) Delete an address
  4) Setup default gateway
  5) Add a route
  6) Delete a route
  7) Setup domain name server
  8) Set to Default
  0) Escape
>
```

Restoring Default Network Settings

On the network setting menu, type **8** and press **Enter** to enter the network restore menu. Type **y** and press **Enter**. Then the system will reset all network settings to factory settings and returns to the networking menu, as shown in Figure 10-11.

Figure 10-11 Restoring default network settings

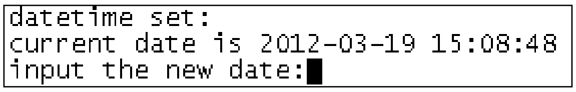


```
Please select an operation:
  1) Display network settings
  2) Add an address
  3) Delete an address
  4) Setup default gateway
  5) Add a route
  6) Delete a route
  7) Setup domain name server
  8) Set to Default
  0) Escape
> 8
Are you sure to set network to default?[y/n]
> 
```

10.3.3 Setting System Time

On the main menu, type **2** and press **Enter** to set the current system date and time, as shown in Figure 10-12. Type system date and time, such as 2012-03-19 15:18:55, and press **Enter** to save the settings. Then press any key to return to the main menu.

Figure 10-12 Console management – Setting system time

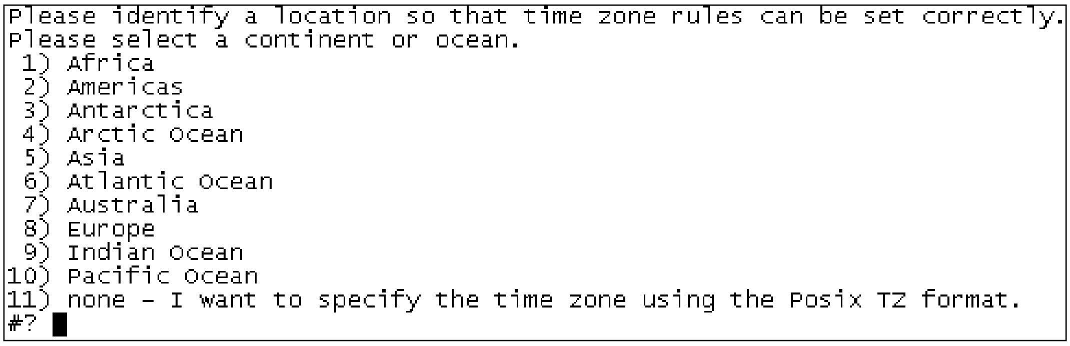


```
datetime set:
current date is 2012-03-19 15:08:48
input the new date:
```

10.3.4 Setting the System Time Zone

On the main menu, type **3** and press **Enter** to set the system time zone, as shown in Figure 10-13. Select the time zone as prompted, and press **Enter** to save the setting. Then press any key to return to the main menu.

Figure 10-13 Console management – setting system time zone

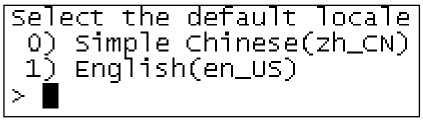


```
Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
 1) Africa
 2) Americas
 3) Antarctica
 4) Arctic Ocean
 5) Asia
 6) Atlantic Ocean
 7) Australia
 8) Europe
 9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#? 
```

10.3.5 Setting the System Language

On the main menu, type **4** and press **Enter** to set the language of the web-based manager, as shown in Figure 10-14. You can select Simplified Chinese or English, and press **Enter** to save the setting. Then press any key to return to the main menu.

Figure 10-14 Console management – Setting system language

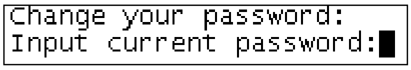


```
Select the default locale
 0) Simple Chinese(zh_CN)
 1) English(en_US)
> 
```

10.3.6 Changing the Console Password

On the main menu, type **5** and press **Enter** to change the console login password, as shown in Figure 10-15. First type the current password, then the new password, and press **Enter**. The new password must contain a minimum of 6 characters. The system will display a message notifying whether the password is changed.

Figure 10-15 Console management – changing console password



```
Change your password:
Input current password:
```

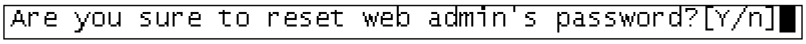
Note

As prompted, the console password must be at least six characters long. See appendix B Default Parameters for the initial account of the console.

10.3.7 Resetting the Web Administrator's Password

On the main menu, type **6** and press **Enter** to open the menu for resetting the password used by the administrator **admin** to log in to the web-based manager, as shown in Figure 10-16. First type **y** and press **Enter** to restore the initial password used by the administrator **admin** for login to the web-based manager. The system will display a message notifying whether the initial password is restored.

Figure 10-16 Console management – resetting the administrator's password

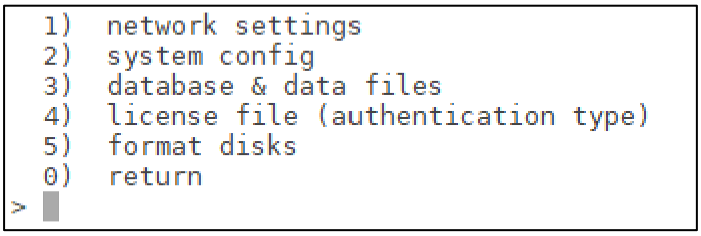


```
Are you sure to reset web admin's password?[Y/n]
```

10.3.8 Restoring Factory Settings

On the main menu, type **7** and press **Enter** to restore factory settings, as shown in Figure 10-17 On this menu, you can type **0** and press **Enter** to return to the main menu.

Figure 10-17 Restoring factory settings



```
  1)  network settings
  2)  system config
  3)  database & data files
  4)  license file (authentication type)
  5)  format disks
  0)  return
>
```

Restoring Network Settings

On the factory setting restoration menu, type **1** and press **Enter** to restore network settings. Type **y** and press **Enter** to restore initial network settings. This operation restores the IP address, subnet mask, and gateway address of a network interface to the initial state. System reboot is not required after restoration.

Restoring System Settings

On the factory setting restoration menu, type **2** and press **Enter** to conduct system restoration. Type **y** and press **Enter** to restore initial system settings, including the password. After restoration, the system is rebooted automatically.

Restoring the Database

On the factory setting restoration menu, type **3** and press **Enter** to conduct database restoration. Type **y** and press **Enter** to clear the system database.

Note	System log reports are cleared as you clear the database. Therefore, back up vital data before this operation.

Deleting the License

On the factory setting restoration menu, type **4** and press **Enter** to open the page of deleting the license. Type **y** and press **Enter** to delete the imported license.

Formatting the Hard Disk

On the factory setting restoration menu, type **5** and press **Enter** to open the page for formatting the hard disk. Type **y** and press **Enter** to format the hard disk. After the hard disk is formatted, all data is deleted.

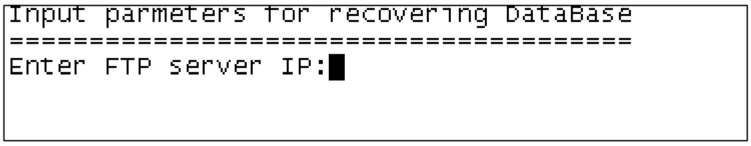
Initializing the System

On the factory setting restoration menu, type **6** and press **Enter** to open the page for initializing the system. Type **y** and press **Enter** to initialize all the system settings.

10.3.9 Restoring the Database

On the main menu, type **8** and press **Enter** to restore the backup database to ADS M.

Figure 10-18 Restoring the backup database



```
Input parmeters for recovering DataBase
=======================================
Enter FTP server IP:
```

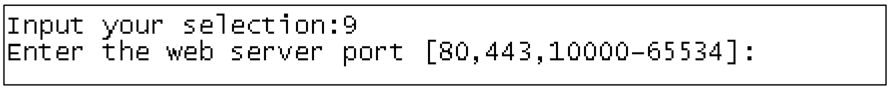
Type the IP address, user name, and password of the FTP server, and press **Enter**. Then the backup database is restored to the ADS M system.

Note	You can successfully restore the backup only after database backup is configured in the **Data Backup and Restore** area under **Administration** > **Local Settings** > **Data Storage**.

10.3.10 Setting the Web Service Port

On the main menu, type **9** and press **Enter** to set the port via which you can log in to ADS M. The port number can be **80**, **443**, or an integer ranging from 10000 to 65534. Assume that the IP address of ADS M is https://192.168.1.100. If the port number is changed to **80**, you need to type https://192.168.1.100:80 in the address bar of the browser.

Figure 10-19 Setting the web service port

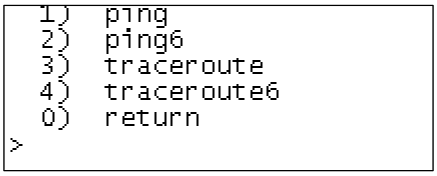


```
Input your selection:9
Enter the web server port [80,443,10000-65534]:
```

10.3.11 Using Network Diagnosis Tools

On the main menu, type **10** and press **Enter** to open the network diagnosis menu. On the menu shown in Figure 10-20, you can type **0** and press **Enter** to return to the main menu.

Figure 10-20 Network diagnosis tools

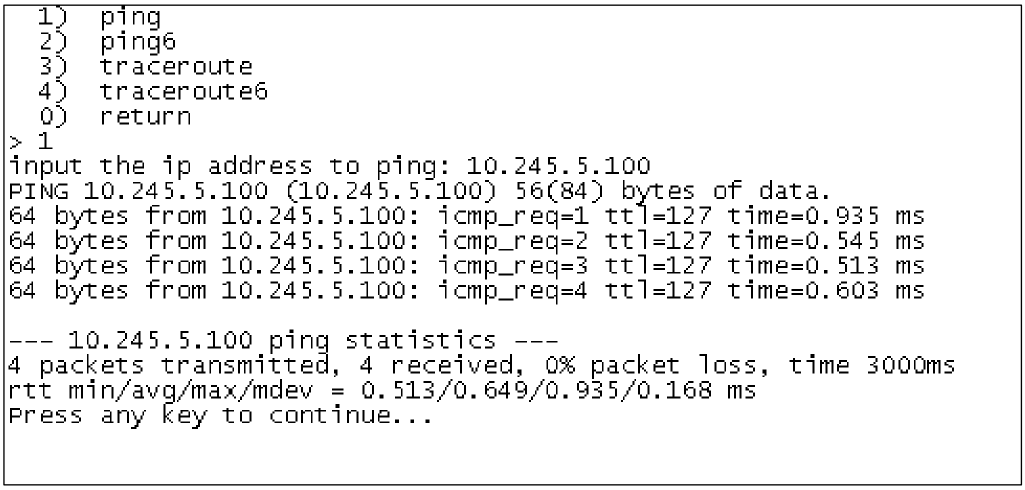


```
  1)  ping
  2)  ping6
  3)  traceroute
  4)  traceroute6
  0)  return
>
```

Pinging an IPv4 Address

On the network diagnosis tool menu, type **1**, press **Enter**, and type an IPv4 address. Then the ping result is displayed below, as shown in Figure 10-21.

Figure 10-21 Pinging an IPv4 address



```
  1)  ping
  2)  ping6
  3)  traceroute
  4)  traceroute6
  0)  return
> 1
input the ip address to ping: 10.245.5.100
PING 10.245.5.100 (10.245.5.100) 56(84) bytes of data.
64 bytes from 10.245.5.100: icmp_req=1 ttl=127 time=0.935 ms
64 bytes from 10.245.5.100: icmp_req=2 ttl=127 time=0.545 ms
64 bytes from 10.245.5.100: icmp_req=3 ttl=127 time=0.513 ms
64 bytes from 10.245.5.100: icmp_req=4 ttl=127 time=0.603 ms

--- 10.245.5.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3000ms
rtt min/avg/max/mdev = 0.513/0.649/0.935/0.168 ms
Press any key to continue...
```

Pinging an IPv6 Address

On the network diagnosis tool menu, type **2**, press **Enter**, and type an IPv6 address. Then the ping result is displayed below.

Tracing an IPv4 Address

On the network diagnosis tool menu, type **3**, press **Enter**, and type an IPv4 address. Then the traceroute result is displayed below.

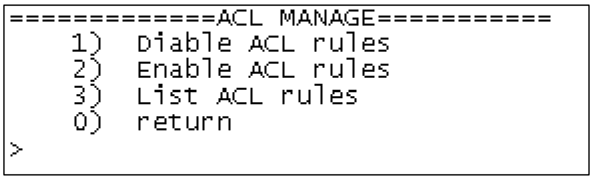
Tracing an IPv6 Address

On the network diagnosis tool menu, type **4**, press **Enter**, and type an IPv6 address. Then the traceroute result is displayed below.

10.3.12 Performing Access Control for the Management Interface

On the main menu, type **11** and press **Enter** to open the menu for configuring management interface access control. On the menu shown in Figure 10-22, you can type **0** and press **Enter** to return to the main menu.

Figure 10-22 Management interface access control menu



```
=============ACL MANAGE===========
    1)  Diable ACL rules
    2)  Enable ACL rules
    3)  List ACL rules
    0)  return
>
```

Disabling Management Interface Access Control

On the management interface access control menu, type **1** and press **Enter** to disable the function. After that, any IP addresses can access ADS M.

Enabling Management Interface Access Control

On the management interface access control menu, type **2** and press **Enter** to enable the function.

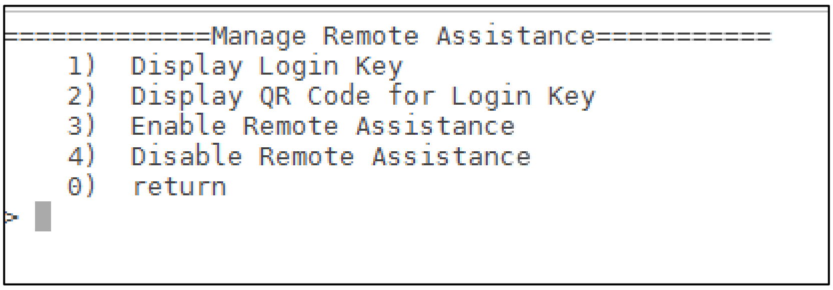
Viewing the Access Control List

On the management interface access control menu, type **3** and press **Enter** to list the access control rules configured for the management interface.

10.3.13 Managing Remote Assistance

On the main menu, type **12** and press **Enter** to open the remote assistance configuration window, as shown in Figure 10-23. You can type **0** and press **Enter** to return to the main menu.

Figure 10-23 Managing remote assistance



```
=============Manage Remote Assistance===========
    1)  Display Login Key
    2)  Display QR Code for Login Key
    3)  Enable Remote Assistance
    4)  Disable Remote Assistance
    0)  return
>
```

Viewing the Login Key

In the window shown in Figure 10-23, type **1** and press **Enter**. Then the login key is displayed.

Viewing the QR Code for the Login Key

In the window shown in Figure 10-23, type **2** and press **Enter**. Then the QR code of the login key is displayed.

Enabling Remote Assistance

In the window shown in Figure 10-23, type **3** and press **Enter**. In the subsequent window that appears, type up to IP addresses for remote access and press **Enter**. Then NSFOCUS technical support can remotely diagnose ADS M from these IP addresses.

Disabling Remote Assistance

In the window shown in Figure 10-23, type **4** and press **Enter**. Then the remote assistance function is disabled.

10.3.14 Restarting System Services

On the main menu, type **r** and press **Enter** to restart system services.

10.3.15 Rebooting the System

On the main menu, type **b** and press **Enter** to reboot the system.

10.3.16 Shutting Down the System

On the main menu, type **h** and press **Enter** to shut down the system.

10.3.17 Exiting the System

On the main menu, type **x** and press **Enter** to log out of the console management interface.

A Parameters

A.1 Anti-DDoS Policy

- SYN Flood

  Threshold 1: The SYN traffic rate at which SYN flood protection is triggered. If the rate (pps) of SYN traffic to a destination exceeds the specified value, SYN flood protection is triggered.

  Threshold 2: The rate at which ADS sends reverse detection packets in response to SYN packets, after SYN flood protection is triggered. A greater value means a better protection effect and a higher load on ADS M.

  You are advised to set threshold 1 to 80% of the maximum traffic carried by the user server and threshold 2 to **15000000** pps.

- ACK Flood

  Threshold 1: The ACK traffic rate at which ACK flood protection is triggered. If the rate (pps) of ACK traffic to a destination exceeds the specified value, ACK flood protection is triggered. Under most application environments, you are advised use the default value.

- UDP Flood

  Threshold 1: The UDP traffic rate at which UDP flood protection is triggered. If the rate (pps) of UDP traffic to a destination exceeds the specified value, UDP flood protection is triggered. Under most application environments, you are advised use the default value.

- ICMP Flood

  Threshold 1: The ICMP traffic rate at which ICMP flood protection is triggered. If the rate (pps) of ICMP traffic to a destination exceeds the specified value, ICMP flood protection is triggered. Under most application environments, you are advised use the default value.

- Connection Exhaustion Prevention

  Currently, ADS M provides only the option of whether to enable connection exhaustion protection in the anti-DDoS policy. Further configurations need to be performed on the web-based manager of ADS.

A.2 UDP Policy Parameters

- Drop UDP Fragment

  Selecting **Drop UDP Fragment** indicates that ADS M drops received UDP fragments.

- Max UDP Packet Length

ADS M drops UDP packets with the length over the specified value. RFC specifies that the default maximum length of UDP packets is 65535.

- Bandwidth Coefficient of Source IP

  It limits the number of UDP packets transmitted from each source IP address per second.

A.3 Diversion Filtering Rules

- Allow Diversion by Default

  A checkmark in the **Allow Diversion by Default** checkbox indicates that the diversion filtering rule applied by ADS M to protected hosts allows diversion by default.

- IP Address/Netmask

  IP address/subnet mask of the diversion filtering rule.

- Allow Diversion

  A checkmark in the **Diversion** checkbox indicates that the traffic of the IP address/subnet mask can be diverted.

- Enable Diversion Filtering Rules

  Selecting the **Enable** checkbox indicates that the manual diversion policy takes effect on ADS M.

B Default Parameters

B.1 Default Parameters of the Communication Interface

Management Interface	192.168.1.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.1

B.2 Default Account of the Web Administrator

User Name	admin
Password	nsfocus

B.3 Default Account of the Console Administrator

User Name	admin
Password	nsfocus

B.4 Communication Parameters of the Console Port

Baud Rate	115200
Data Bits	8