# NSFOCUS ADS M

# User Guide

**Version: V4.5R89F03 (2017-05-17)**

# Contents

# Figures

# Tables

# Preface

## Scope

This document describes all functions and usage of ADS NX3-M 600A/1600A/1600E (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.

## Audience

This document is intended for the following users:

- System administrator
- Network administrator
- Users who wish to know main techniques and usage of this product

This document assumes that you have a basic knowledge of the following areas:

- Linux and Windows operating systems
- TCP/IP protocols
- Network security

## 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 Traffic Monitoring | Describes in detail the traffic and attacks monitored by the managed devices. |
| 4 Logs | Describes how to view device logs. |
| 5 Region Management | Describes how to configure device regions and region IP groups. |
| 6 Device Management | Describes device management, policy configuration, and abnormal traffic detection. |
| 7 Web-based System Management | Describes system management and maintenance. |
| 8 Console-based System Management | Describes menus of the console management interface. |
| A Parameters | Describes parameters of policy templates. |

| Chapter | Overview |
|---|---|
| B Default Parameters | Introduces default settings of ADS M. |

# 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. |

# Customer Support

Email: support@nsfocusglobal.com

Portal: https://nsfocus.desk.com/

Contacts:

- 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

# 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 deliver these files to ADS devices.

# 2 Web-based Manager

## 2.1 Login

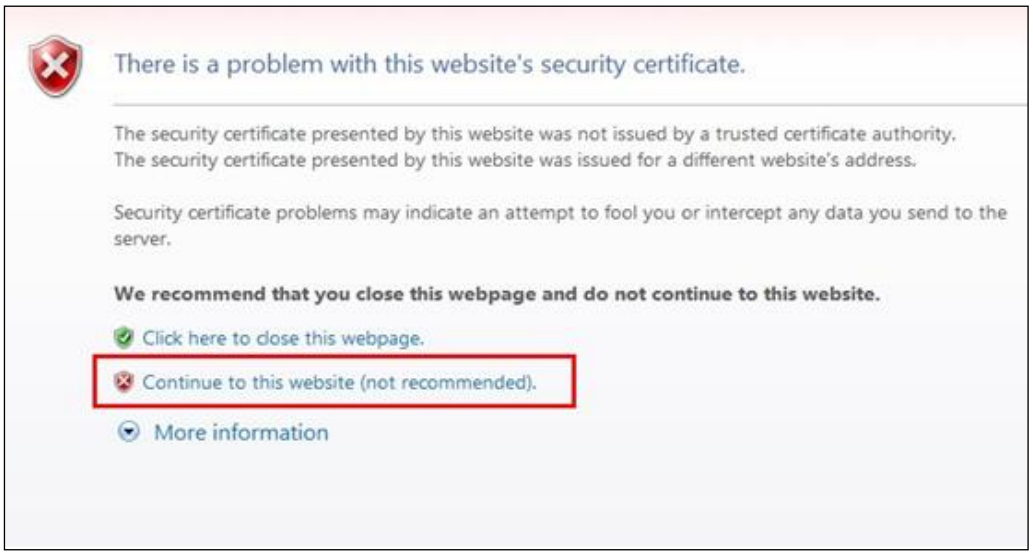
To log in to the web-based manager of ADS M, perform the following steps:

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

**Step 2** Open a browser (for example, Microsoft Internet Explorer) 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.

A security alert page appears, as shown in Figure 2-1.

Figure 2-1 Security alert page




**Step 3** Click **Continue to this website (not recommended)** to accept the channel secured by the ADS M certificate.

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

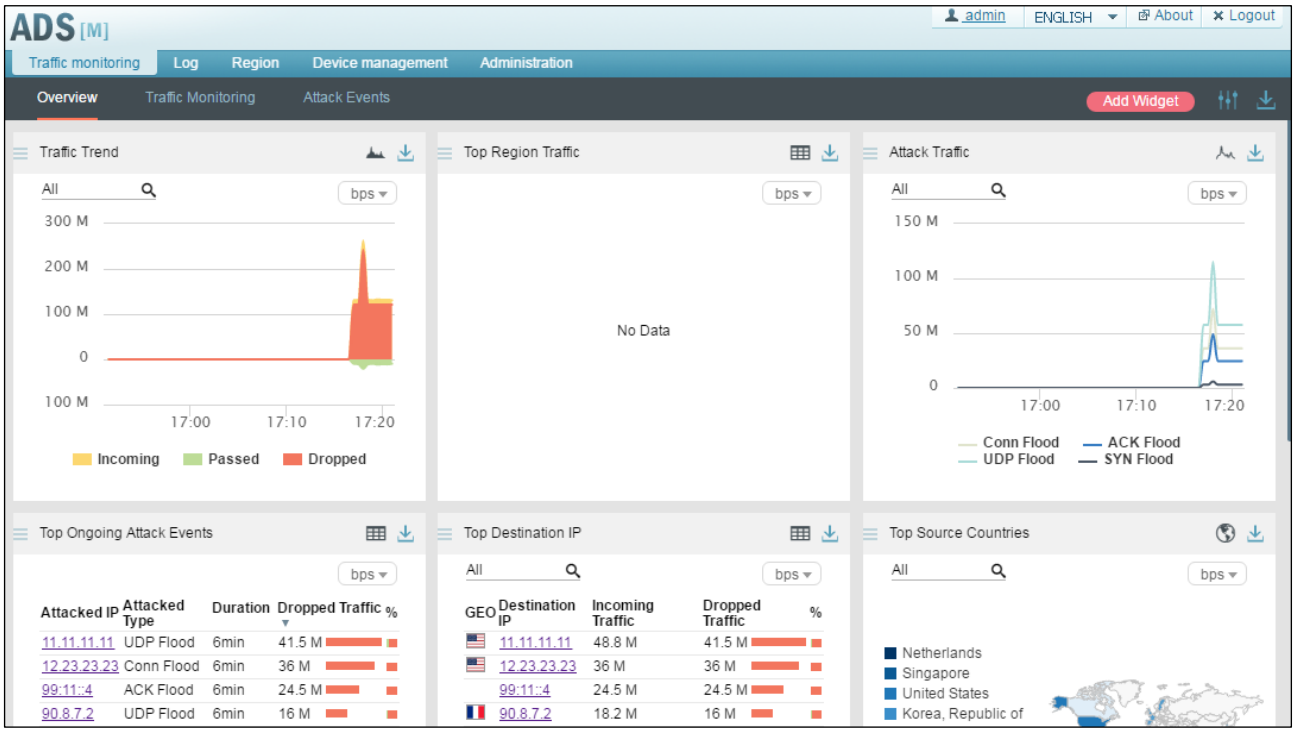
Figure 2-2 Login page of the web-based manager


**Step 4** Type the correct user name and password and 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 V4.5R89F03, 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 *NSFOCUS ADS M Installation Guide*.<br>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 2-3.

Figure 2-3 Homepage




**----End**

| | |
|---|---|
| Caution | • The browser you use must support JavaScript, cookies, and frames.<br>• 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.<br>• You must change the password immediately after the first login.<br>• The system will return to the login page if you remain inactive on a page other than the three 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 module** no matter how long you stay inactive on this page.<br>• For the first login, you must import a valid license before using the system. For details, see section 7.1.2 License Management. |

# 2.2 Layout

Figure 2-4 shows the layout of the web-based manager.

Figure 2-4 Layout of the web-based manager

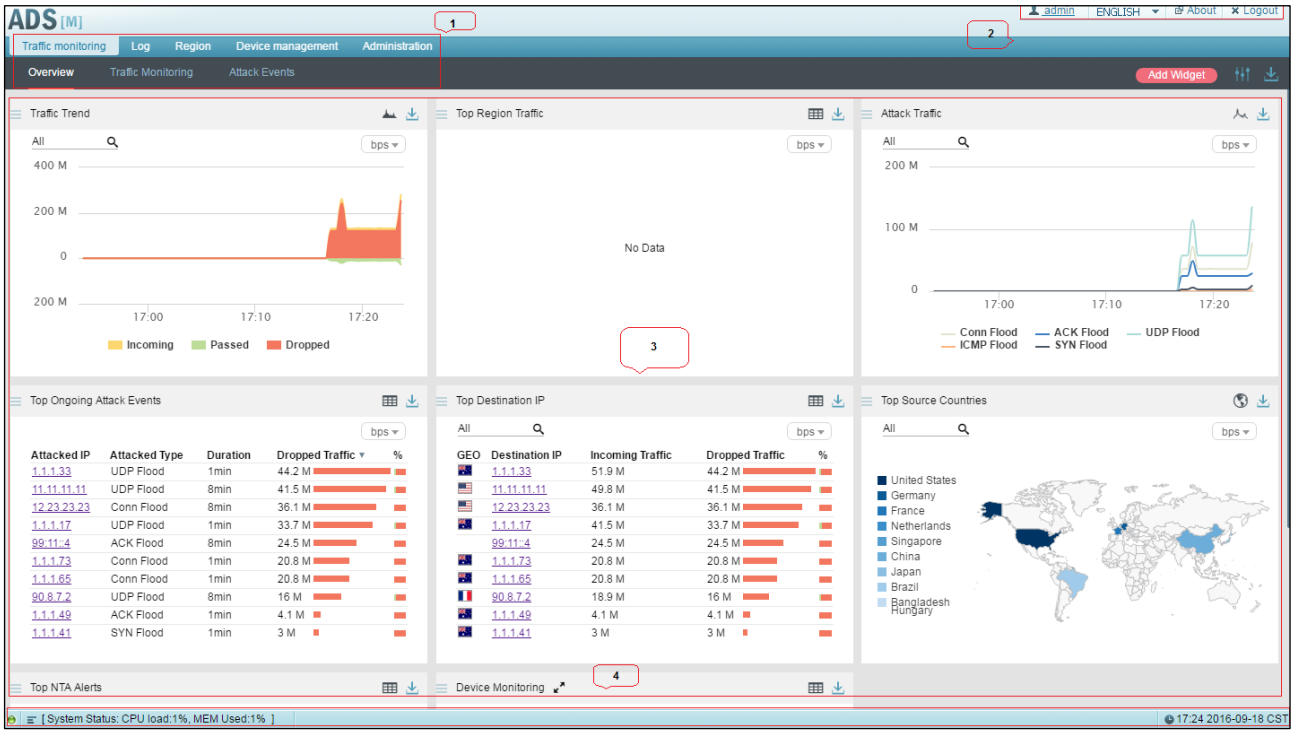



Table 2-1 describes areas of the web-based manager.

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.<br>• admin : enables you to modify your information. See section 7.2.1 User Management for details.<br>• ENGLISH : switches between languages. See section 7.1.1 Basic Settings for details.<br>• About : displays product information of ADS M devices.<br>• 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 current system time, 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 2-2, move the cursor to the **Language** button in the lower-right corner. Then all languages available are automatically displayed, as shown in Figure 2-5. Click the desired language. The interface language is now changed to the one that you selected.

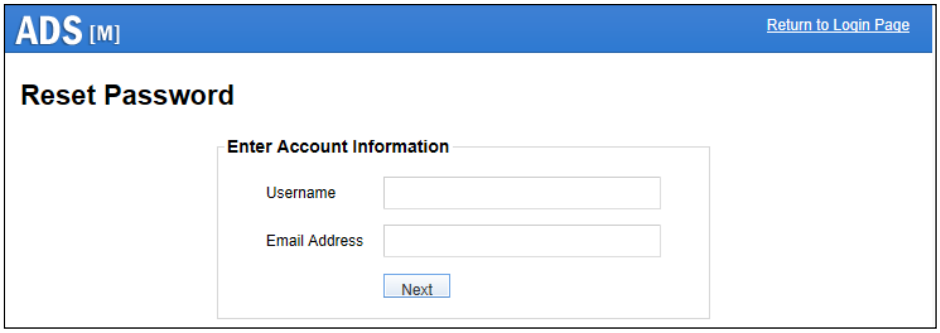
Figure 2-5 Language options


## Resetting the Password

On the login page shown in Figure 2-2, click **Forgot Password** in the lower-right corner. On the **Reset Password** page shown in Figure 2-6, 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 7.2.2 Security Settings.<br>• 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.<br>• The password resetting function also requires a Simple Mail Transfer Protocol (SMTP) server. For details, see section 7.3.5 SMTP Server Configuration. |

Figure 2-6 Password resetting page



# 3 Traffic Monitoring

Traffic monitoring provides the following information:

| Section | Description |
|---|---|
| Overview | Displays monitoring information regarding four types of traffic, six types of attack events, and status information of the managed devices (NTA and ADS). |
| Traffic Monitoring | Displays traffic monitoring information of specified IP addresses, protection groups, regions, region IP groups, and ADS. |
| Attack Events | Displays attack monitoring information of specified IP addresses, protection groups, regions, region IP groups, and ADS. |

## 3.1 Overview

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

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

Table 3-1 describes in detail the monitoring information on the **Overview** page.

Table 3-1 Monitoring information displayed on the Overview page

| Category | Monitoring Information | Description |
|---|---|---|
| Traffic monitoring | 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 | 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 ADS in the last 30 minutes as well as details about each type of traffic. |
| | Traffic trend | Displays the trends of traffic received, dropped, and forwarded by ADS in the last 30 minutes. |

| Category | Monitoring Information | Description |
|---|---|---|
| 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. |

### 3.1.1 Adding a Panel

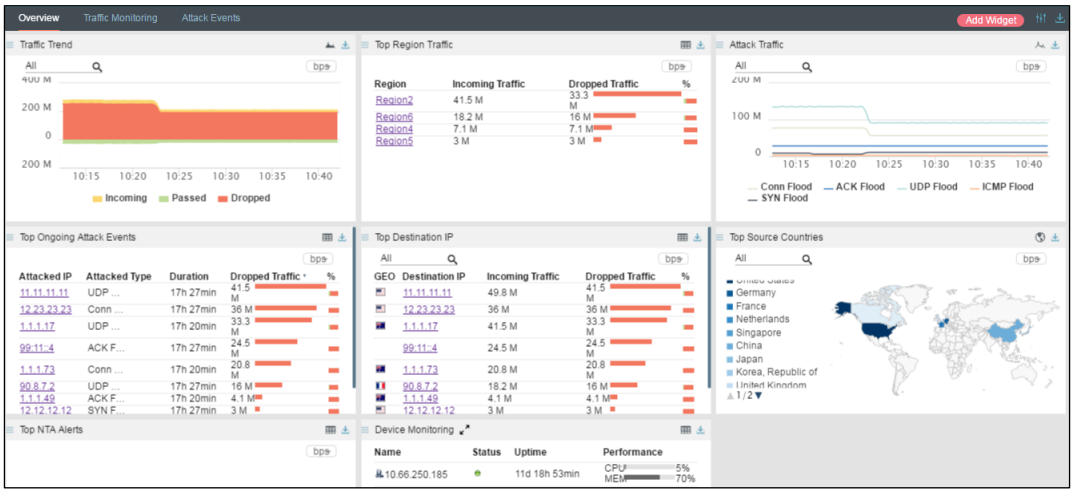
The **Overview** page presents the following 11 panels by default:

- Traffic Trend
- Protocol Analysis
- Top Destination IP
- Top Region Traffic
- Top Source Countries
- Attack Traffic
- Top NTA Alerts
- Top Ongoing Attack Events
- Top 10 Source IP
- Attack Type Distribution
- Device Monitoring

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

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

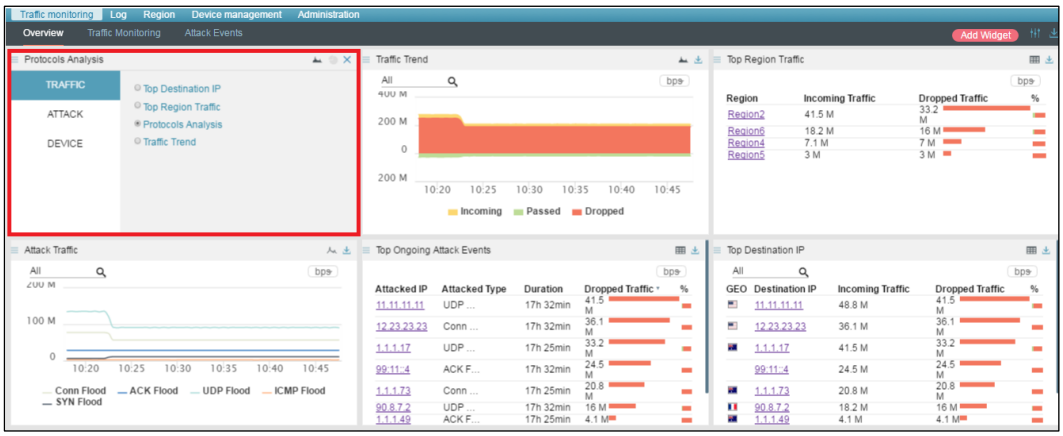
Figure 3-1 Overview page




**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 3-2, for you to choose a panel to display on the **Overview** page.

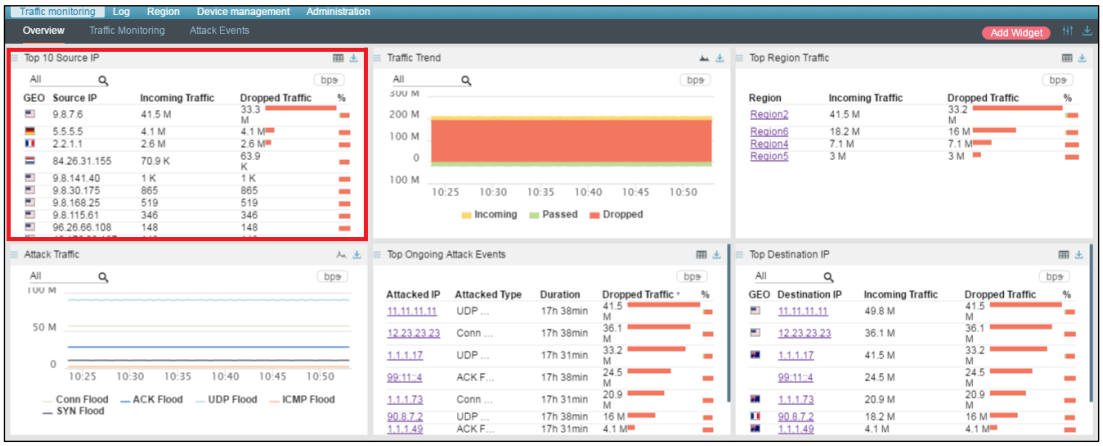
Figure 3-2 Adding a panel




**Step 3** In the box, select a category from the left pane and then click a panel from the right pane.

Then the new panel appears in the **Overview** page. For example, if you select **ATTACK** and **Top 10 Source IP**, the new panel appears in the upper-left corner, as shown in Figure 3-3.

Figure 3-3 Viewing the new panel




**----End**

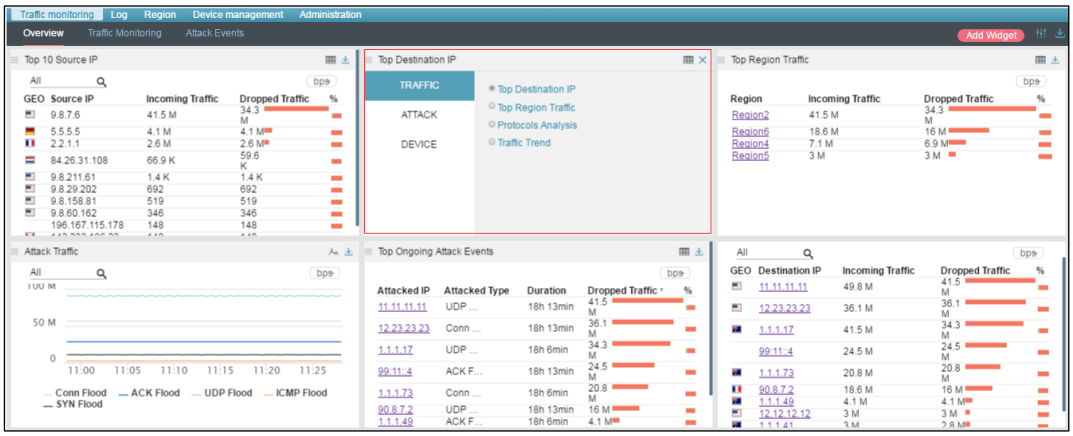
## 3.1.2 Changing a Panel

You can change a panel by performing the following steps:

**Step 1** On the page shown in Figure 3-1, click in the upper-left corner of a panel, for example, **Top Destination IP**.

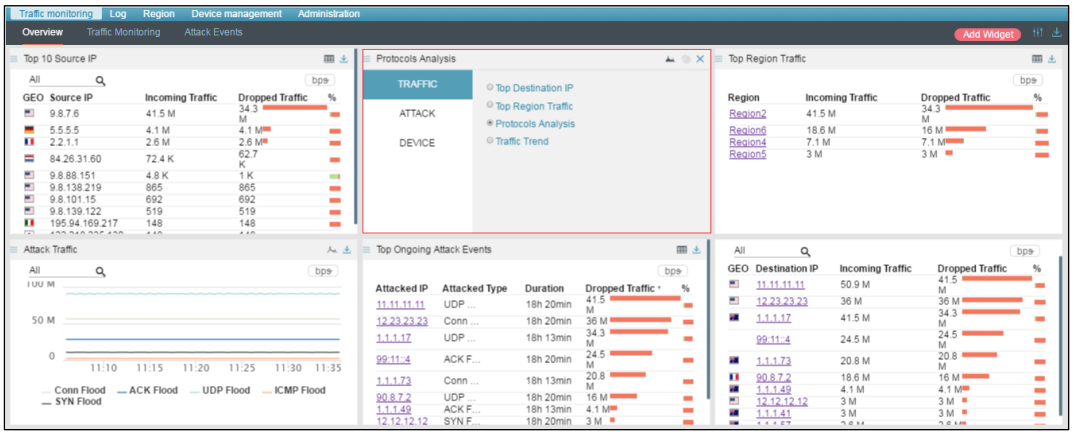
Then the panel reverses, as shown in Figure 3-4.

Figure 3-4 Reversed panel



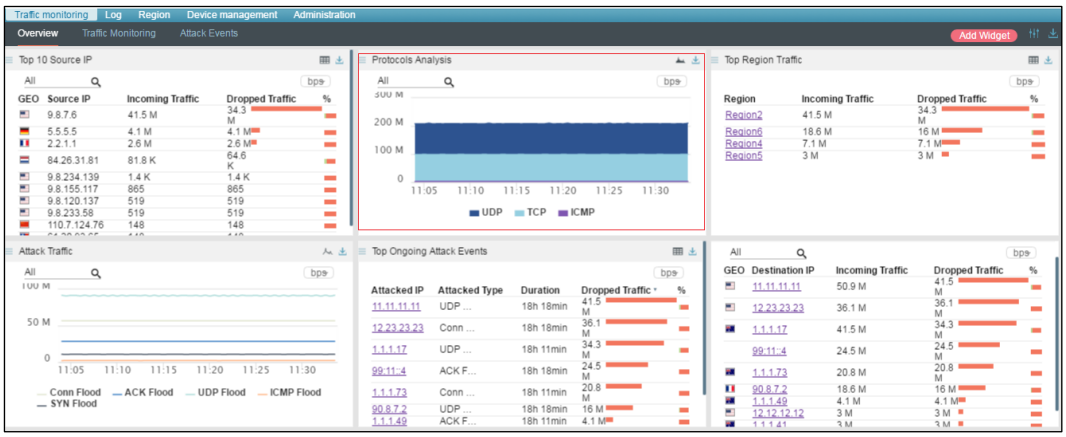

**Step 2** Specify another panel to display, for example, **Protocols Analysis** under **Traffic**, as shown in Figure 3-5.

Figure 3-5 Specifying another panel to display




After you click the panel name, the box reverses to display the selected panel, as shown in Figure 3-6.

Figure 3-6 New panel displayed




**----End**

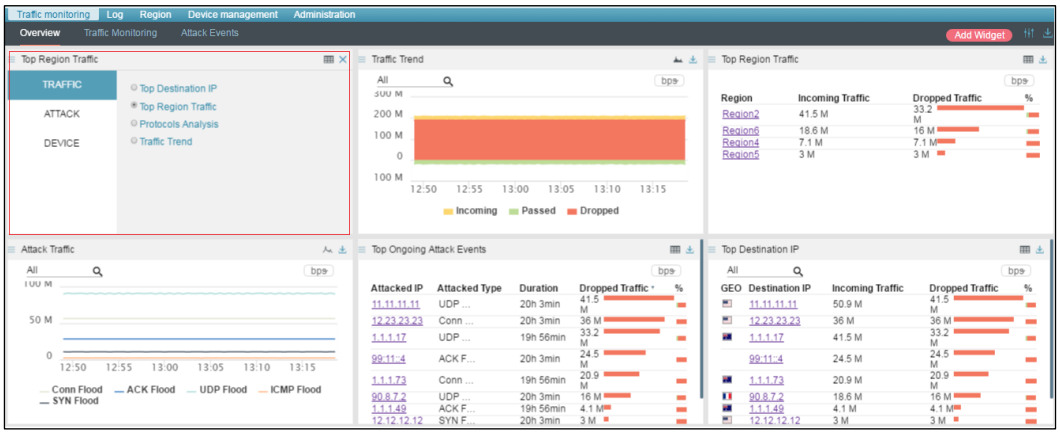
## 3.1.3 Deleting a Panel

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

**Step 1** On the page shown in Figure 3-1, click in the upper-left corner of the unnecessary panel.

Then the panel reverses, as shown in Figure 3-7.

Figure 3-7 Reversed panel




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

Then the panel is deleted.

**----End**

## 3.1.4 Configuring a List of Email Addresses

You can configure a list of email addresses to receive reports from ADS M in a scheduled manner. After that, you can add, delete, edit, enable, and disable email addresses.

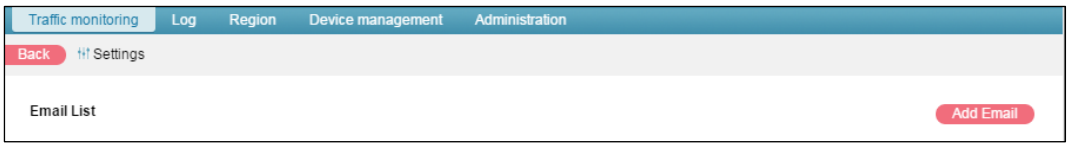
### Adding Email Addresses

To enable the function of sending reports via email, you must first configure an SMTP server. For how to configure an SMTP server, see section 7.3.5 SMTP Server Configuration.

To add email addresses, follow these steps:

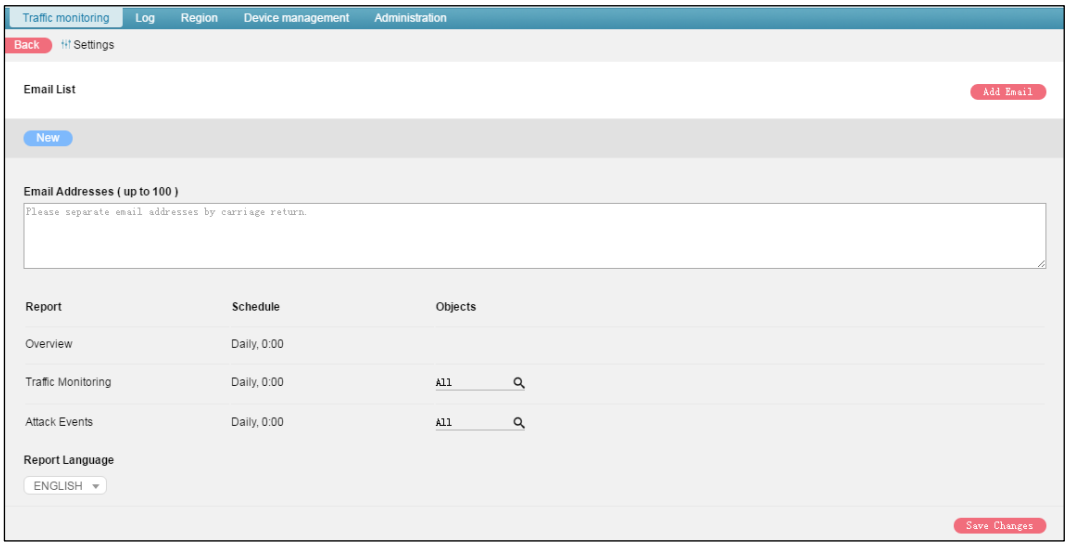
**Step 1** Click in the upper-right corner of the page.

Figure 3-8 Email configuration page




**Step 2** Click **Add Email**.

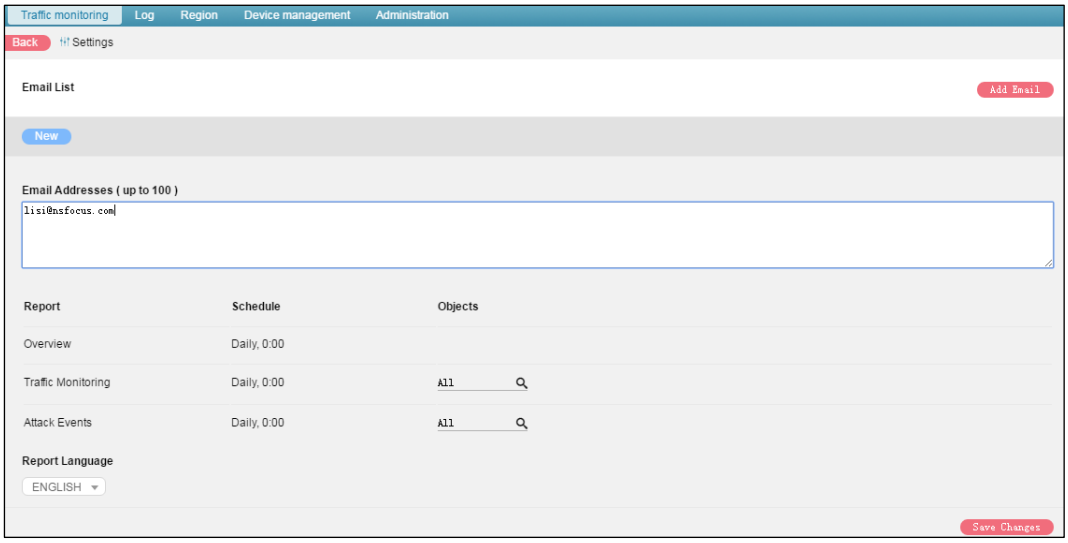
Figure 3-9 Page for configuring email parameters




**Step 3** Specify email addresses to receive reports by email.

Type email addresses in the **Email Addresses** text box. Multiple email addresses must be separated with carriage returns, as shown in Figure 3-10.

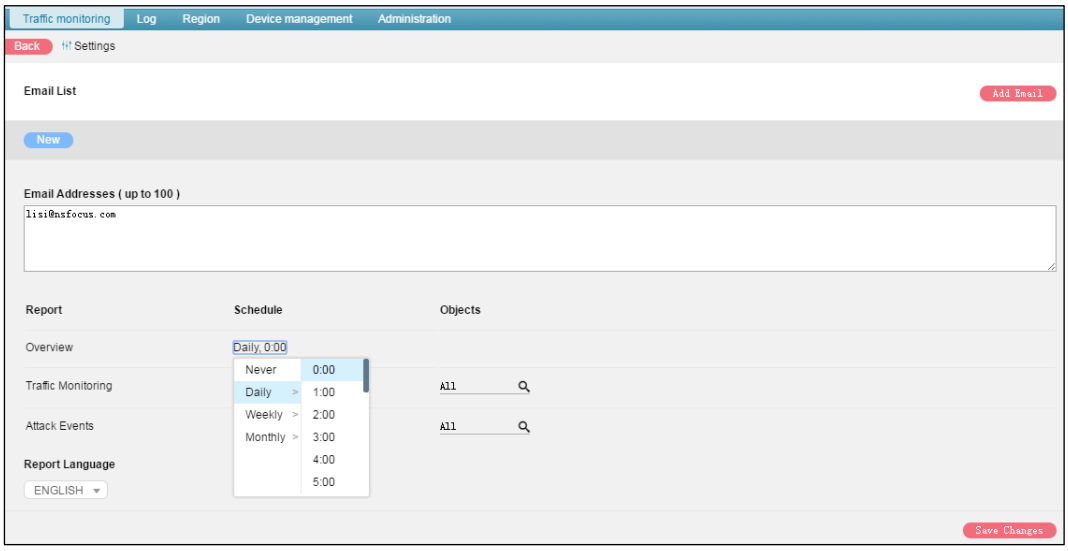
Figure 3-10 Specifying email addresses




**Step 4** Schedule and specify the type of reports to be sent.

Under **Schedule**, you can specify which type of reports to be sent, and set how often and when these reports are to be sent, as shown in Figure 3-11.

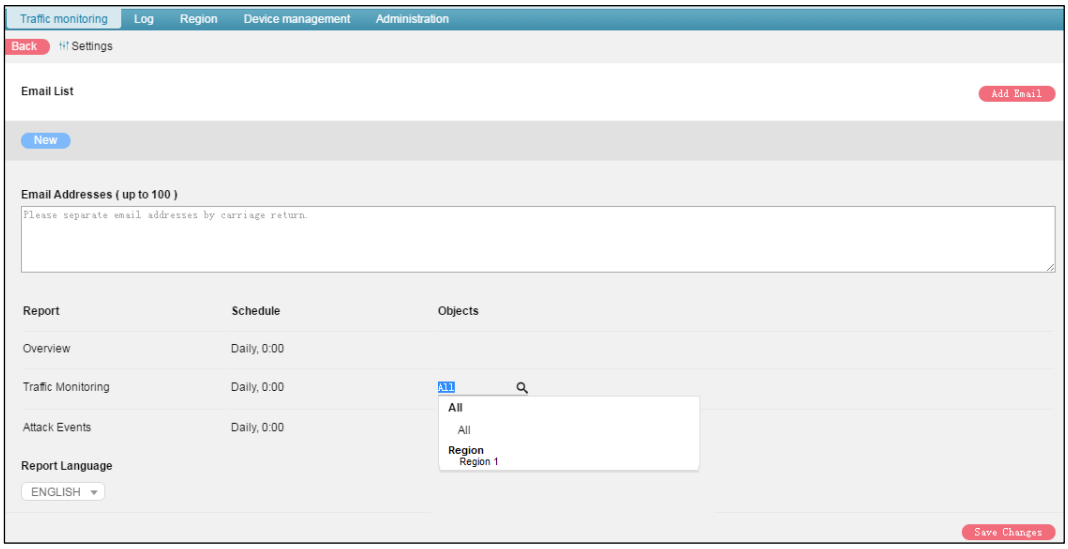
Figure 3-11 Configuring report sending parameters




**Step 5** Specify an object whose data will be reported.

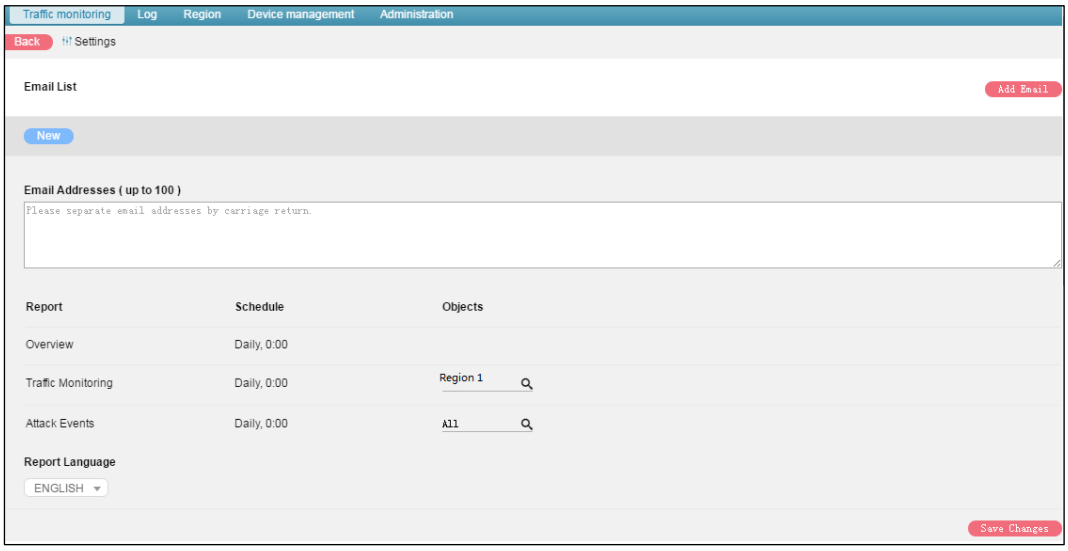
For traffic monitoring reports and attack event reports, data of all objects is collected by default. If you want reports to provide data regarding only a specific object, you must type a character string under **Objects** and then press **Enter**. The system then displays objects containing the typed character string, as shown in Figure 3-12.

Figure 3-12 Specifying an object whose data will be reported




After you select an object, it will be displayed under **Objects**, as shown in Figure 3-13.

Figure 3-13 Object selected

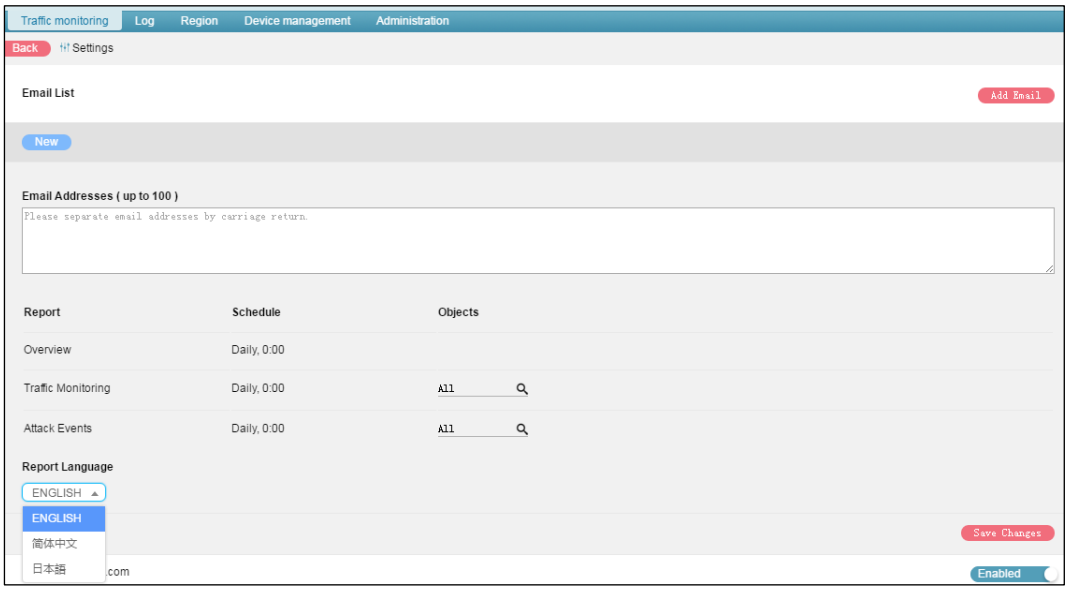



**Step 6** Specify a language for reports.

Move the cursor to the upper-right corner to select a language, as shown in Figure 2-5. Click the desired language. The UI language is now changed to the one that you selected.

Click the **Report Language** drop-down list and select a language for reports.

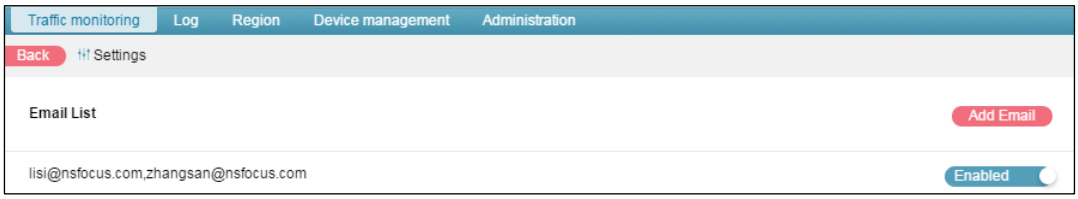
Figure 3-14 Specifying a language for reports




**Step 7** Click **Save Changes** to commit the settings.

The newly added email addresses are displayed under **Email List** and are enabled by default, as shown in Figure 3-15.

Figure 3-15 List of email addresses




**Step 8** Click **Back** to return to the **Overview** page.

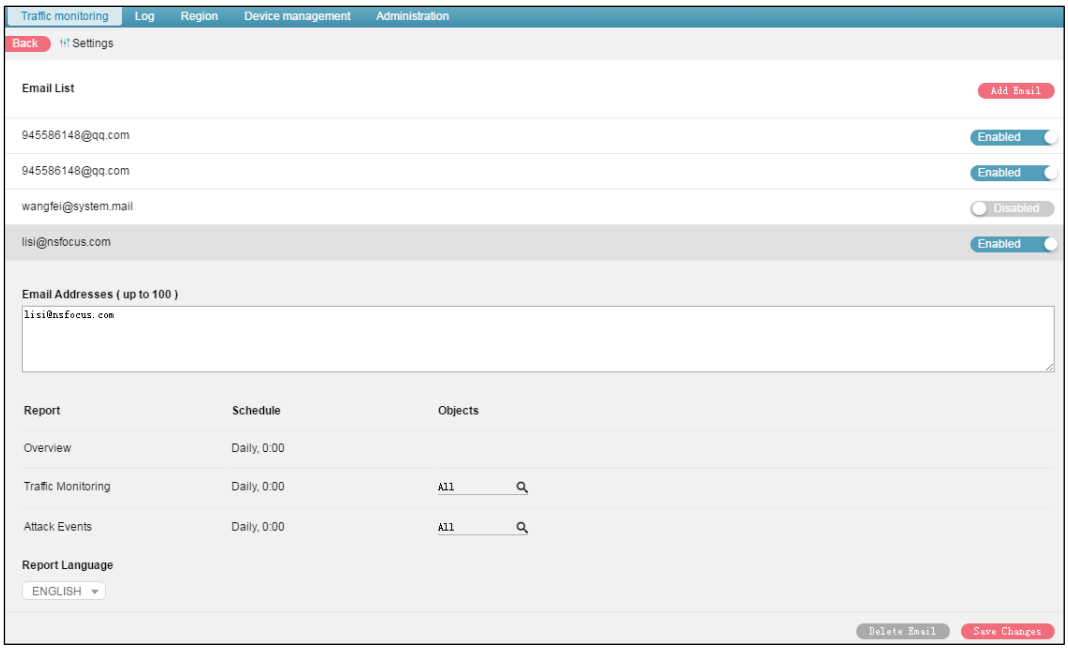
**----End**

## Editing Email Settings

**Step 1** In the list of email addresses shown in Figure 3-15, click an email address.

More information is displayed below, as shown in Figure 3-16, allowing you to modify email settings.

Figure 3-16 Email editing page




**Step 2** Modify parameters and click **Save Changes**.

**Step 3** Click **Back** to return to the **Overview** page.

**----End**

## Deleting Email Settings

**Step 1** In the list of email addresses shown in Figure 3-15, click an email address.

More information is displayed below, as shown in Figure 3-16, allowing you to modify email settings.

**Step 2** Click **Delete Email** to clear the list of email addresses.

**Step 3** Click **Back** to return to the **Overview** page.

**----End**

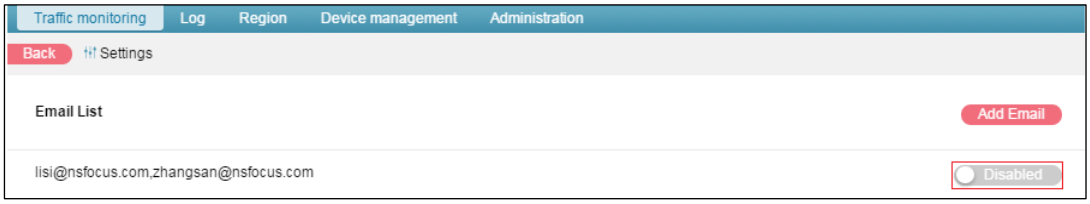
## Enabling/Disabling Email Addresses

Only enabled email addresses can receive reports.

### Disabling Email Addresses

In the list of email addresses shown in Figure 3-15, click **Enabled** and the related email addresses are disabled, as shown in Figure 3-17.

Figure 3-17 Email addresses disabled




### Enabling Email Addresses

After email addresses are disabled, click **Disabled** and they are enabled again.

Click **Back** to return to the **Overview** page.

## 3.1.5 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:

**Step 1** On the page shown in Figure 3-1, 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 data of this panel is exported as a report.
- Click in the upper-right corner of the page and then all data displayed on this page is exported as an integrated report.

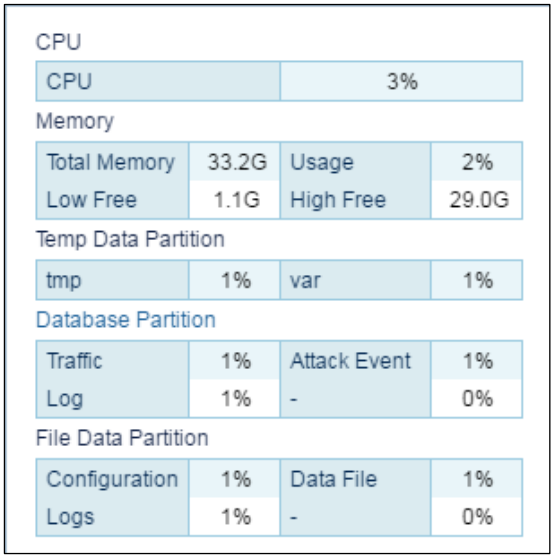
## 3.1.6 Viewing the System Status Bar

The system status bar at the bottom of the web-based manager displays the system service status ( indicates that the device operates properly), system status (CPU usage and memory usage), and system time, as shown in Figure 3-18.

Figure 3-18 System status bar


Clicking system status information in the status bar shows details such as CPU usage, memory usage, temporary data partition, database partition, and file data partition, as shown in Figure 3-19. Clicking system status information in the status bar again will hide it.

Figure 3-19 Detailed system status information



CPU

| | |
|---|---|
| CPU | 3% |

Memory

| | | | |
|---|---|---|---|
| Total Memory | 33.2G | Usage | 2% |
| Low Free | 1.1G | High Free | 29.0G |

Temp Data Partition

| | | | |
|---|---|---|---|
| tmp | 1% | var | 1% |

Database Partition

| | | | |
|---|---|---|---|
| Traffic | 1% | Attack Event | 1% |
| Log | 1% | - | 0% |

File Data Partition

| | | | |
|---|---|---|---|
| Configuration | 1% | Data File | 1% |
| Logs | 1% | - | 0% |

## 3.1.7 Generating Sound Alerts

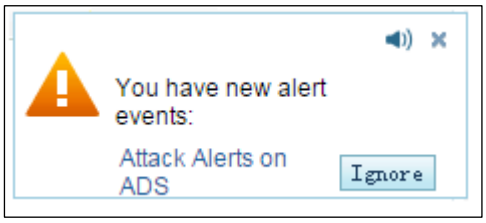
After sound alerting is enabled, the system makes a sound and displays an alert reminder box, as shown in Figure 3-20, when either of the following conditions is met:

- 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 3-20 Sound alert



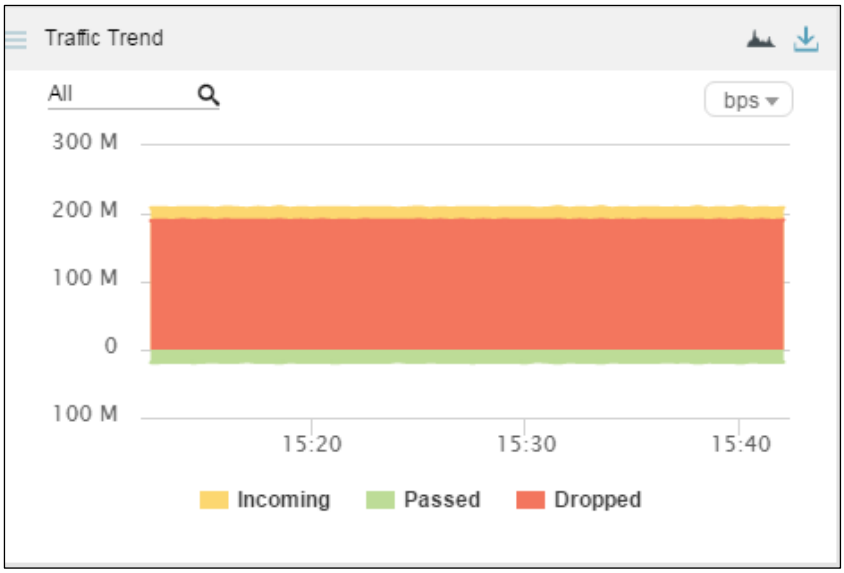

For how to disable sound alerting, see section 7.1.1 Basic Settings.

## 3.1.8 Viewing Traffic Trends

The **Traffic Trend** panel shows trends of traffic received, forwarded, and dropped by ADS in the last 30 minutes, as shown in Figure 3-21.

Data on this panel refreshes every 30 seconds.

Figure 3-21 Traffic Trend panel




### 3.1.8.1 Understanding Data on the Panel

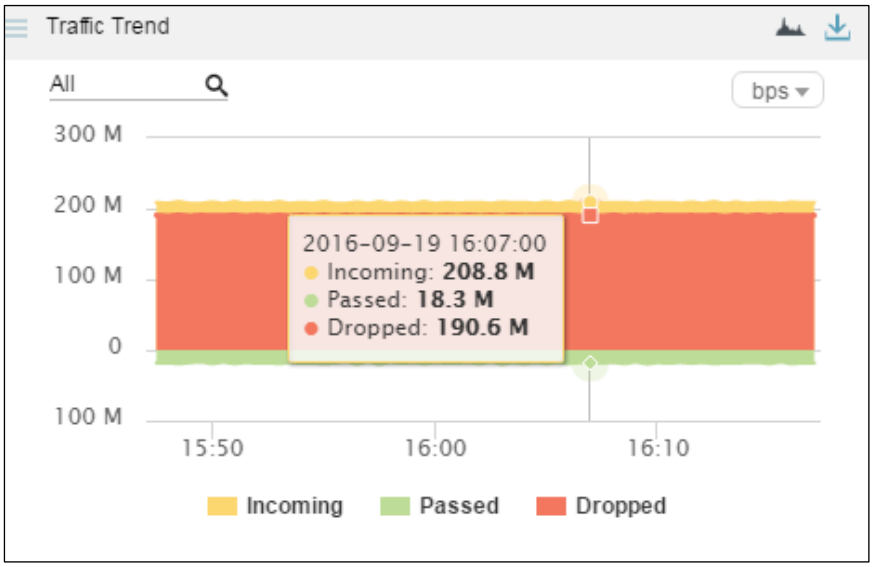
In the **Traffic Trend** graph,

- 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.

### 3.1.8.2 Viewing Traffic at a Random Point of Time

Pointing to a random point in the **Traffic Trend** graph displays the specific time and values of incoming traffic, forwarded traffic, and dropped traffic, as shown in Figure 3-22.

Figure 3-22 Detailed traffic information at a specific point of time



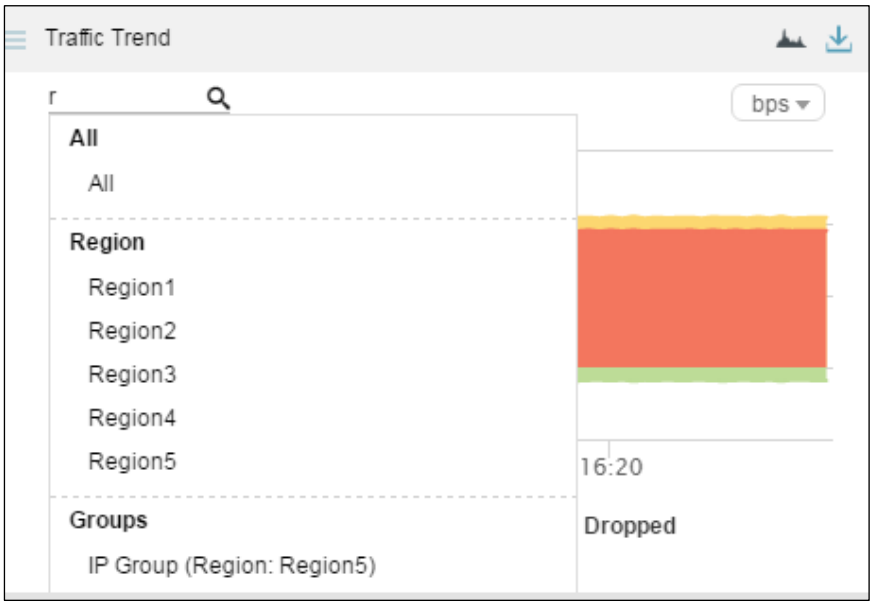

### 3.1.8.3 Viewing Traffic of a Specified Object

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

**Step 1** On the page shown in Figure 3-22, type a character string and then press **Enter**.

The system displays all objects containing the typed character string.

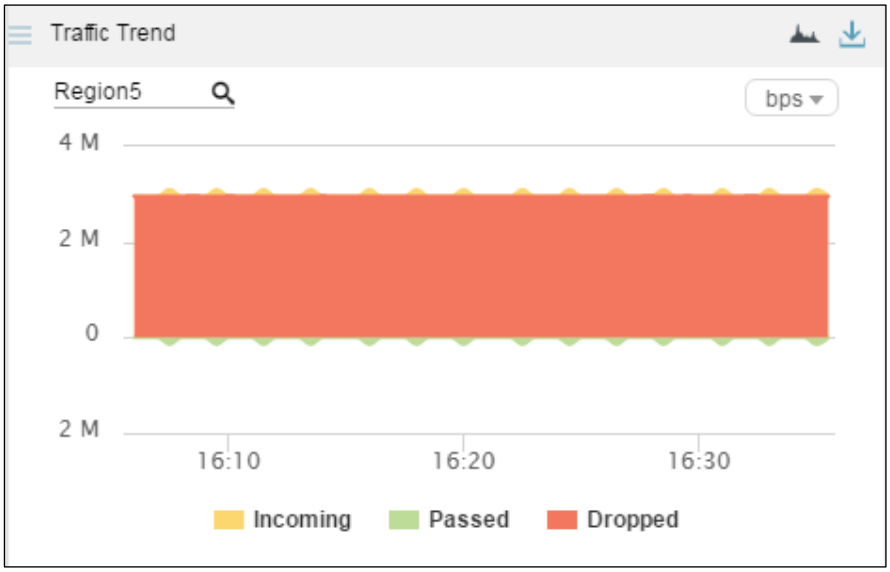
Figure 3-23 Searching for an object




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

Traffic trends of the specified object are displayed, as shown in Figure 3-24.

Figure 3-24 Real-time traffic trends of a specified object

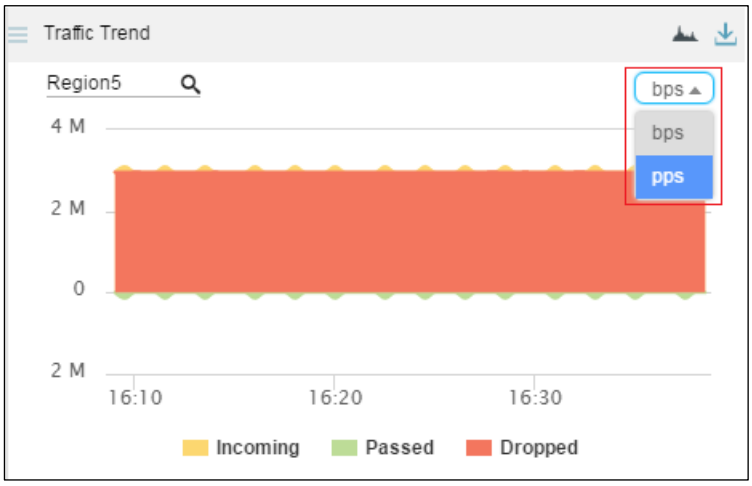



**----End**

## 3.1.8.4 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 **Traffic Trend** panel to display traffic data in pps, as shown in Figure 3-25.

Figure 3-25 Switching the traffic unit




### 3.1.8.5 Downloading a Report

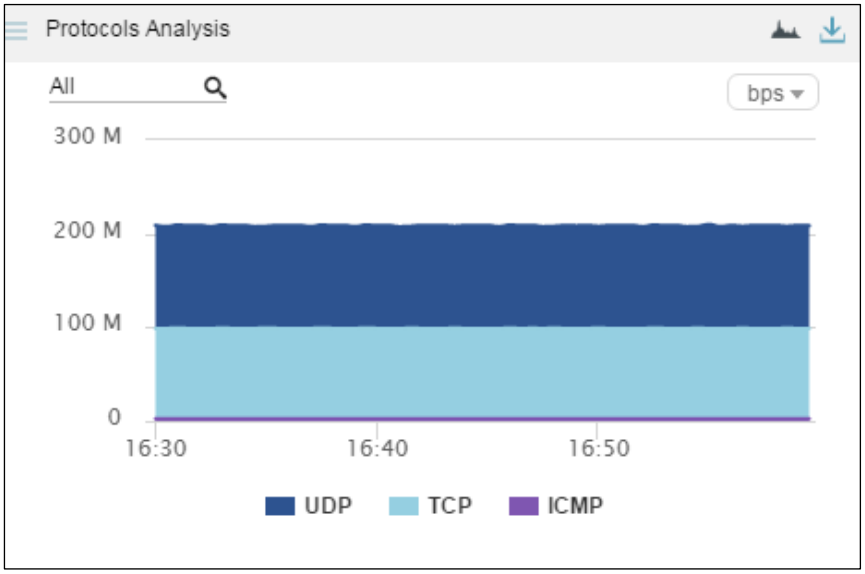
Click in the upper-right corner of the **Traffic Trend** panel and then data of this panel will be exported as a report. For details, see section 3.1.5 Downloading a Report.

## 3.1.9 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, as shown in Figure 3-26.

Data on this panel refreshes every 30 seconds.

Figure 3-26 Protocols Analysis panel



### 3.1.9.1 Understanding Data on the Panel

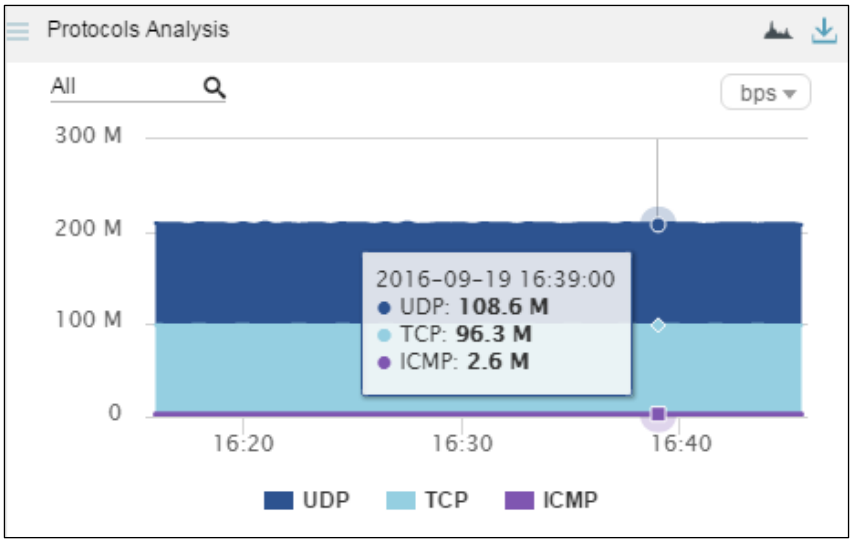
In the **Protocols Analysis** graph,

- 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.

### 3.1.9.2 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 3-27.

Figure 3-27 Viewing traffic of different protocols at a specific point of time



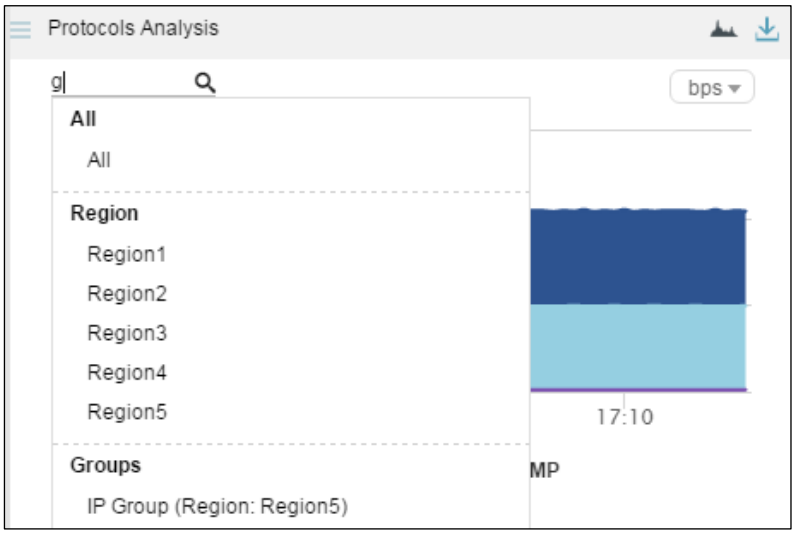

### 3.1.9.3 Viewing Traffic of a Specified Object

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 3-27, type a character string and then press **Enter**.

The system displays all objects containing the typed character string, as shown in Figure 3-28.

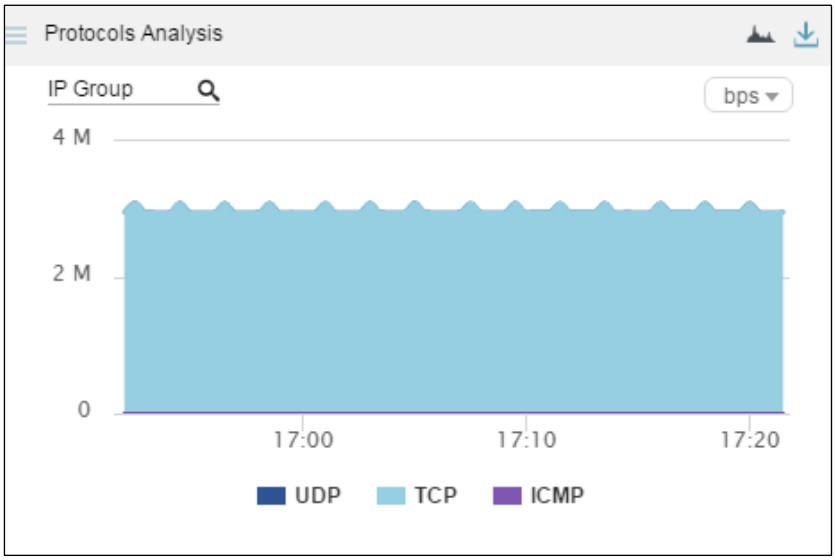
Figure 3-28 Searching for an object




**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 3-29.

Figure 3-29 Real-time traffic trends of a specified object

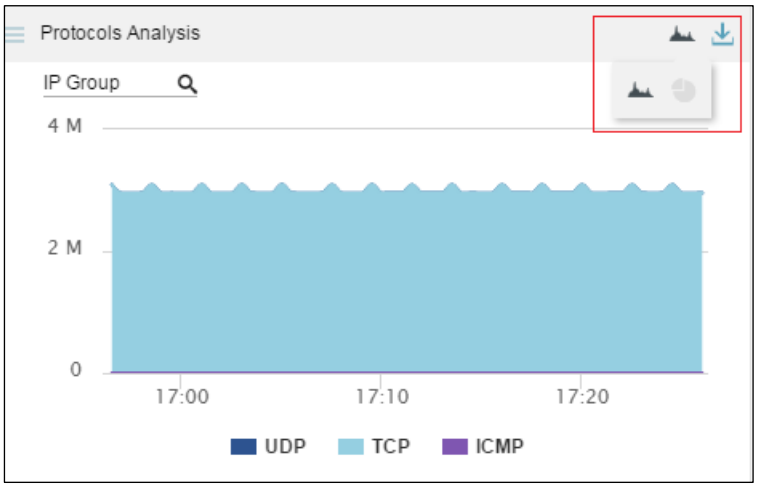



**----End**

## 3.1.9.4 Switching the Display Mode

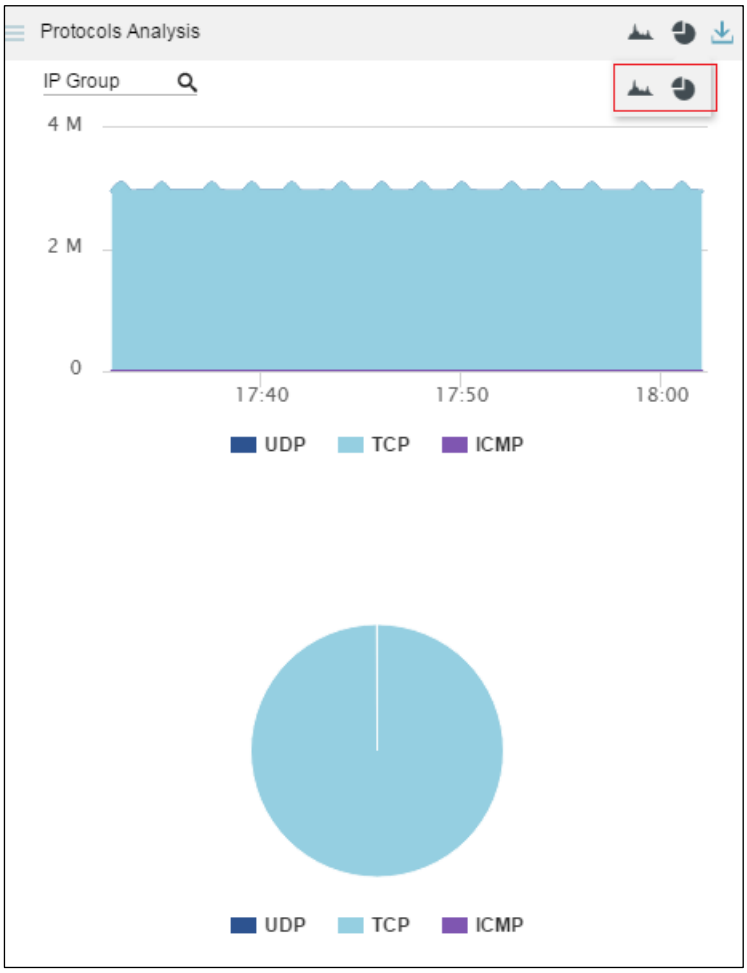
By default, protocol-specific traffic data is presented in an area graph. You can click and/or to display real-time traffic data in an area graph and/or pie chart, as shown in Figure 3-30.

Figure 3-30 Switching the display mode



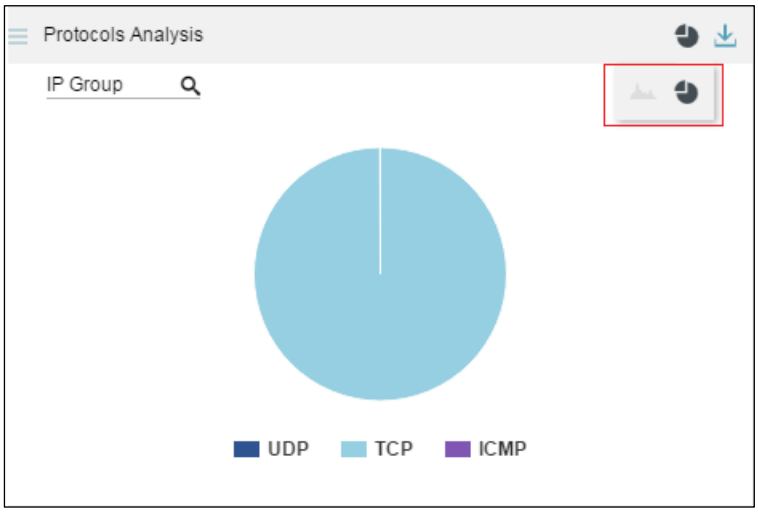

In Figure 3-30, appears normal, while appears dimmed. Therefore, data is presented only in an area graph. After you click , this icon turns . In this case, traffic data is presented in both an area graph and pie chart, as shown in Figure 3-31.

Figure 3-31 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 3-32.

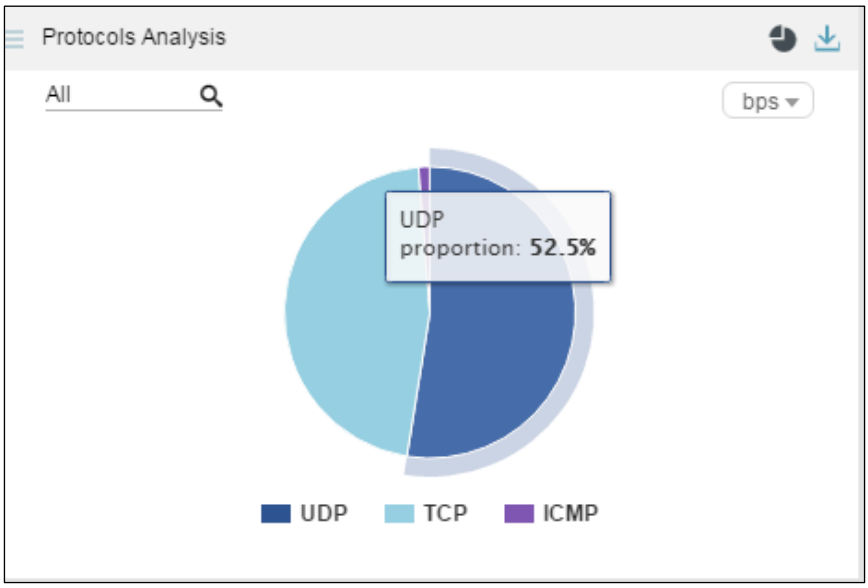
Figure 3-32 Display of traffic data in a pie chart




### 3.1.9.5 Viewing the Percentage of Protocol-Specific Traffic

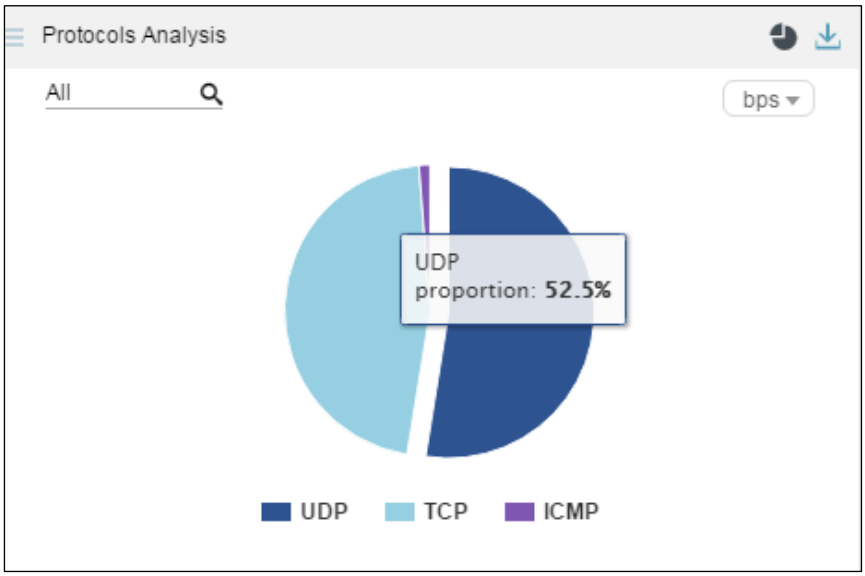
Pointing to a random point in the pie chart displays the protocol name and the percentage of protocol-specific traffic to the total traffic, as shown in Figure 3-33.

Figure 3-33 Percentage of protocol-specific traffic




Clicking in this area separates this area from other areas, as shown in Figure 3-34.

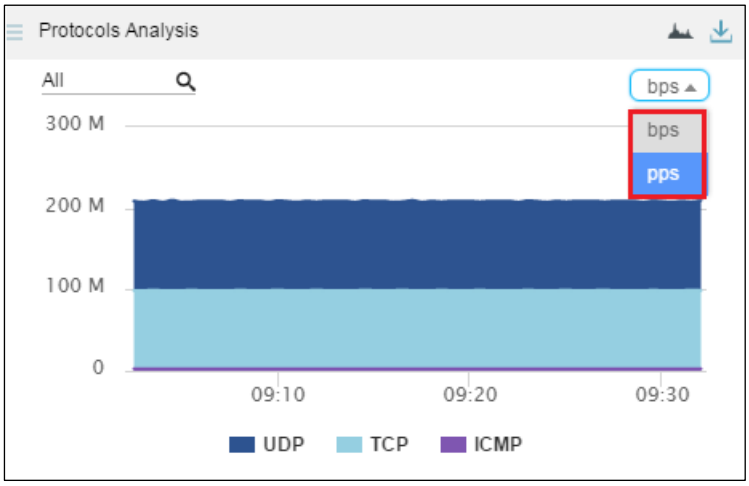
Figure 3-34 Area representing traffic of a protocol separated from other areas




## 3.1.9.6 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, as shown in Figure 3-35.

Figure 3-35 Switching the traffic unit




## 3.1.9.7 Downloading a Report

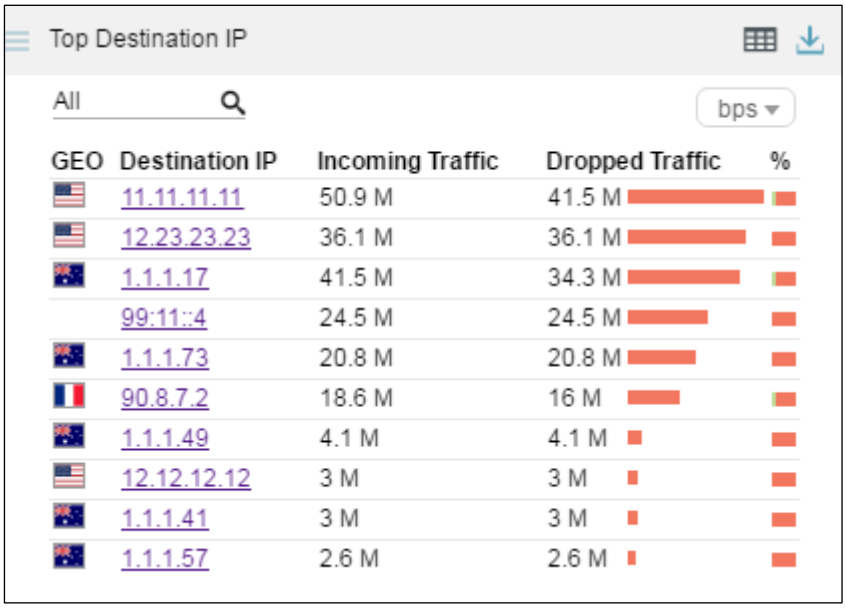
Click in the upper-right corner of the **Protocols Analysis** panel and then data of this panel will be exported as a report. For details, see section 3.1.5 Downloading a Report.

## 3.1.10 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, as shown in Figure 3-36.

Data on this panel refreshes every 30 seconds.

Figure 3-36 Top Destination IP panel

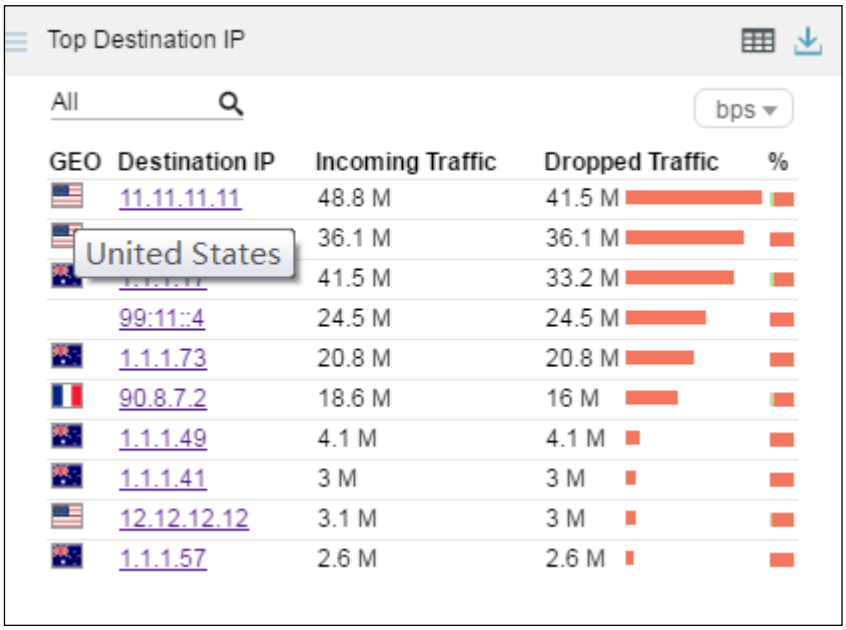



### 3.1.10.1 Understanding Data on the Panel

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

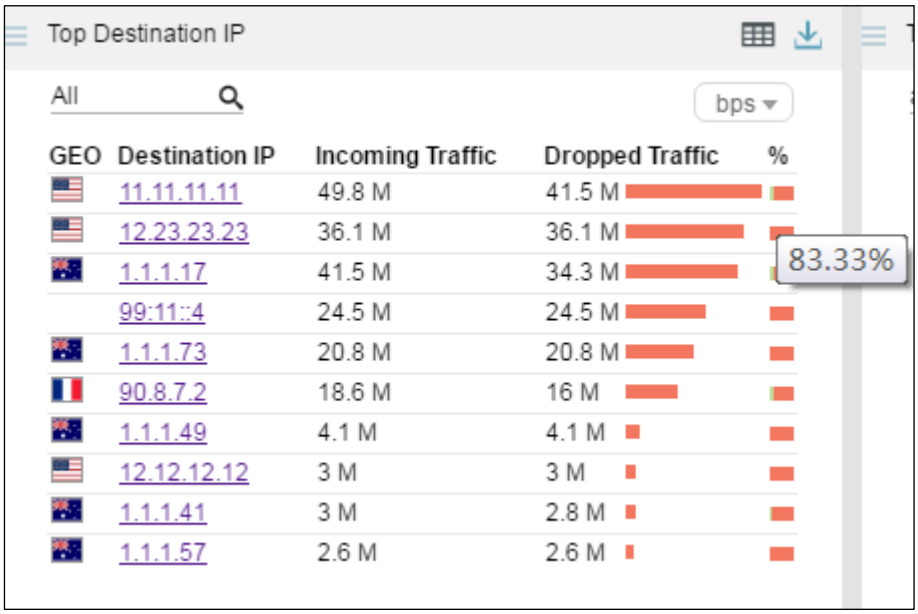
- **GEO**: shows the national flag icons. Pointing to a national flag displays the corresponding country name, as shown in Figure 3-37.

Figure 3-37 Display of the country name




- **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 3.1.10.2 Viewing Comprehensive Traffic Information of a Specified Object.
- **Incoming 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 3-38, the percentage of dropped traffic for 11.11.11.11 is 83.33%.

Figure 3-38 Percentage of dropped traffic to incoming traffic



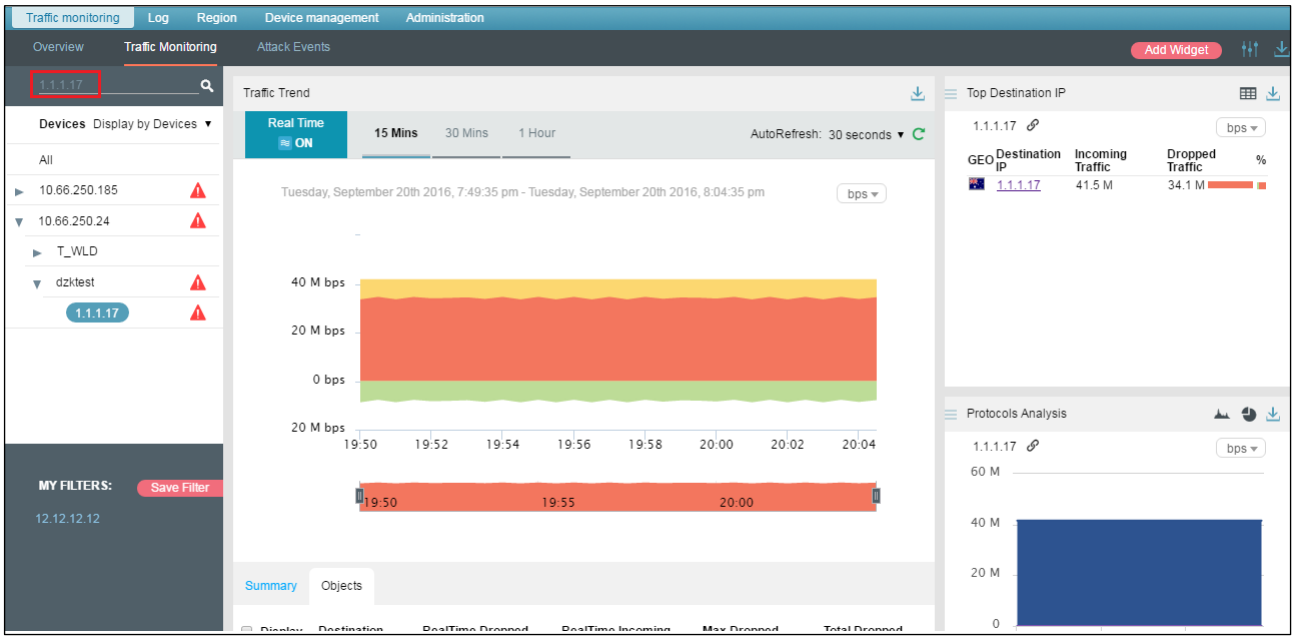

### 3.1.10.2 Viewing Comprehensive Traffic Information of a Specified Object

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 3-38, click an IP address, for example, 1.1.1.17.

The **Traffic Monitoring** page is displayed, with the IP address in question already in the search box, as shown in Figure 3-39.

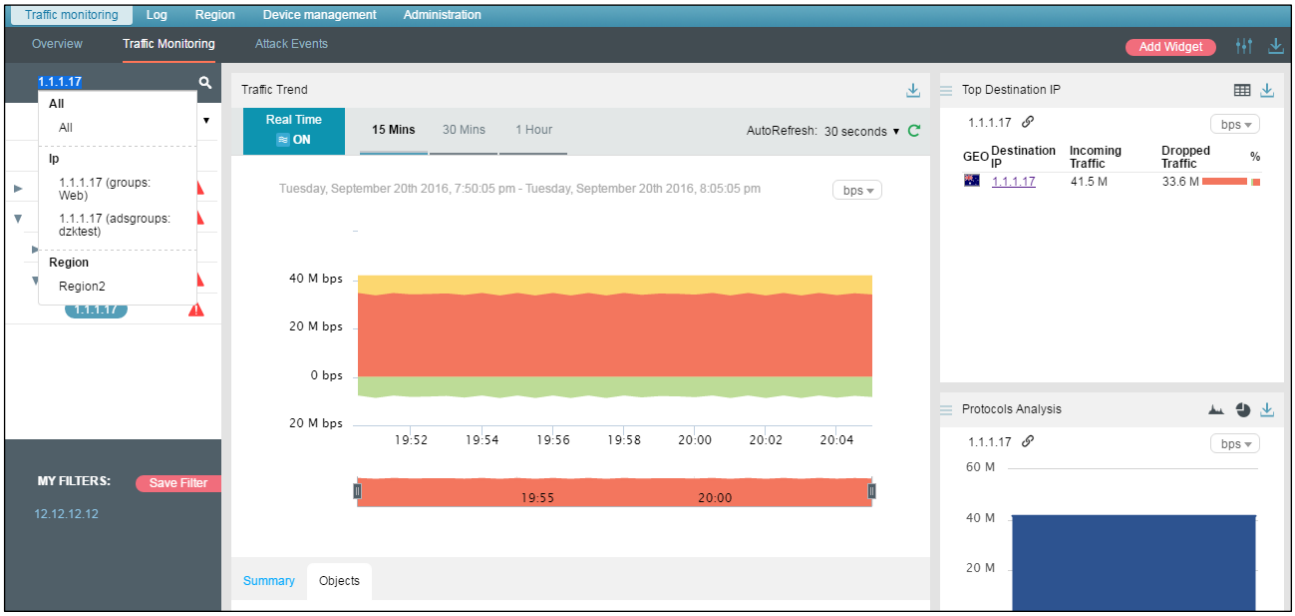
Figure 3-39 Traffic of a specific IP address




**Step 2** Click in the search box.

The system displays all objects containing the current IP address, as shown in Figure 3-40.

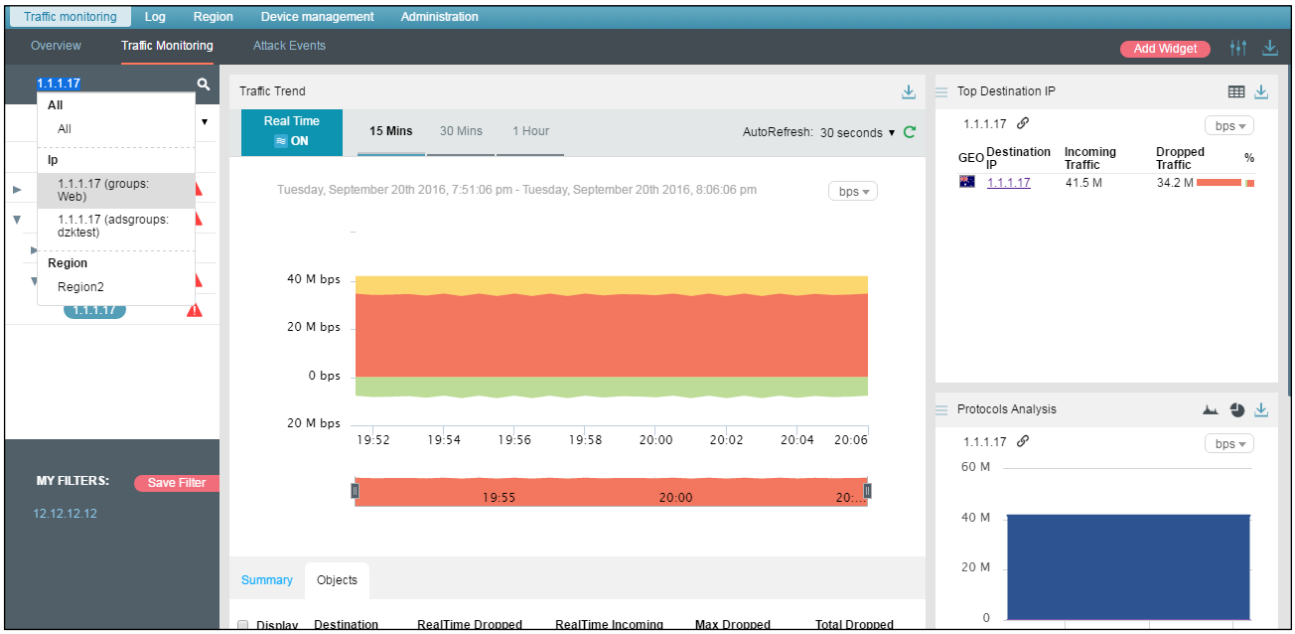
Figure 3-40 Searching for objects containing the current IP address




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

Comprehensive traffic information of the specified object is displayed, as shown in Figure 3-41.

Figure 3-41 Viewing traffic information of a specified object



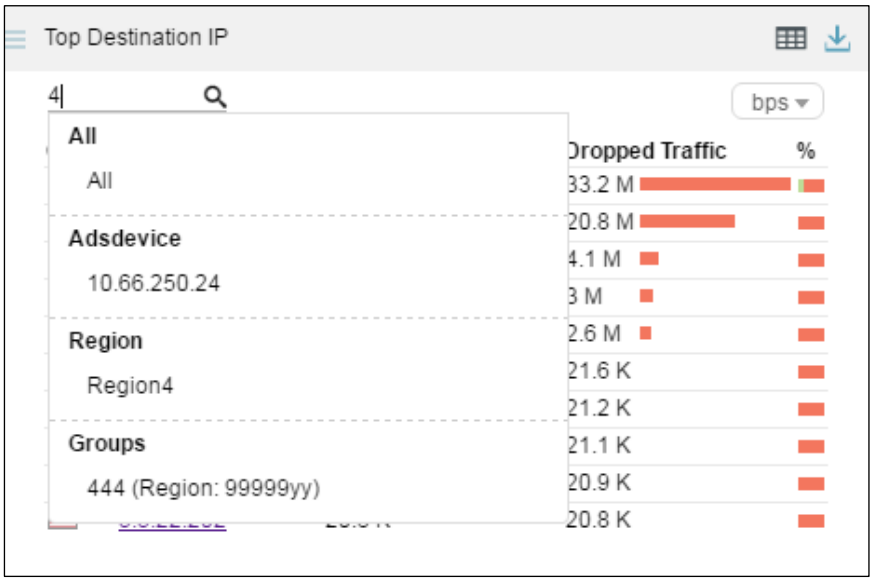

## 3.1.10.3 Viewing Top Destination IP Addresses of a Specified Object

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 3-36, type a character string and then press **Enter**.

The system automatically displays all objects containing the typed character string, as shown in Figure 3-42.

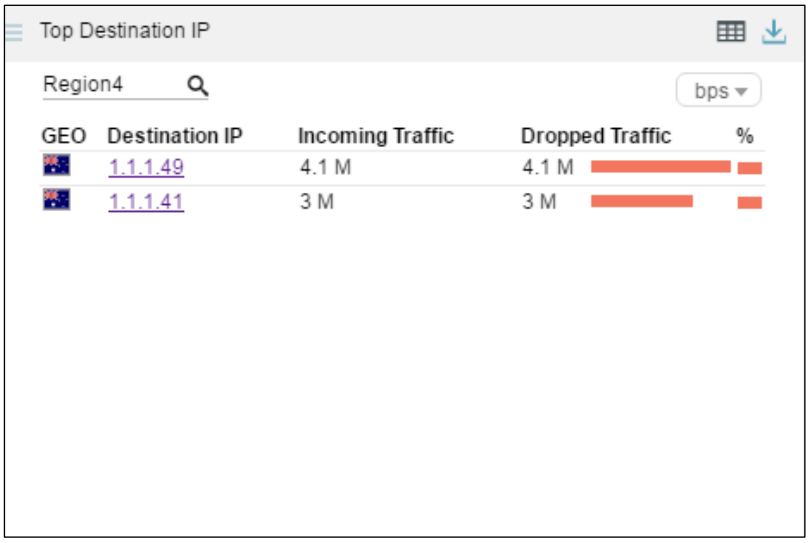
Figure 3-42 Searching for an object




**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 3-43 Top destination IP addresses associated with a specified object




**----End**

## 3.1.10.4 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.

### 3.1.10.5 Downloading a Report

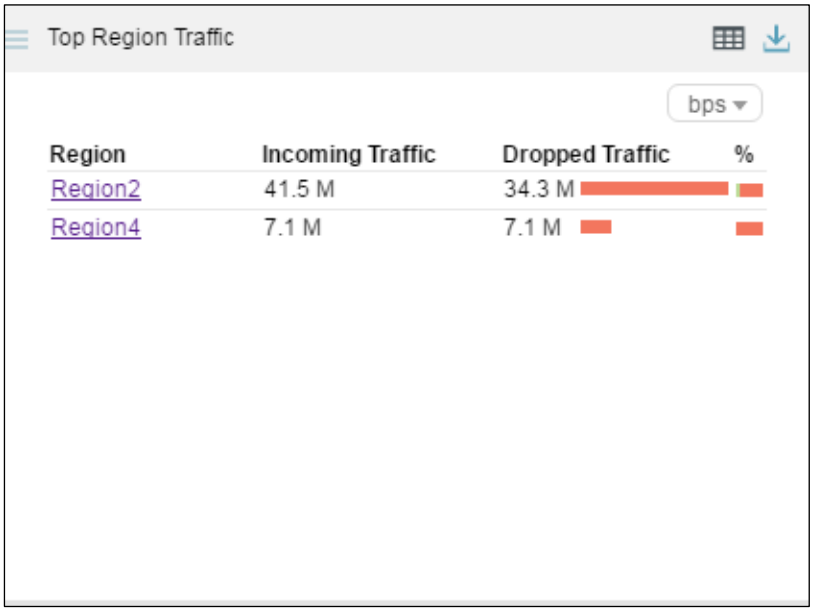
Click in the upper-right corner of the **Top Destination IP** panel and then data of this panel will be exported as a report. For details, see section 3.1.5 Downloading a Report.

## 3.1.11 Viewing Traffic of Top Regions

The **Top Region Traffic** panel presents in real time top 10 regions with the largest traffic dropped by ADS in the last 30 seconds, as shown in Figure 3-44, letting users know which regions see the largest traffic or are most severely attacked.

Data on this panel refreshes every 30 seconds.

Figure 3-44 Top Region Traffic panel

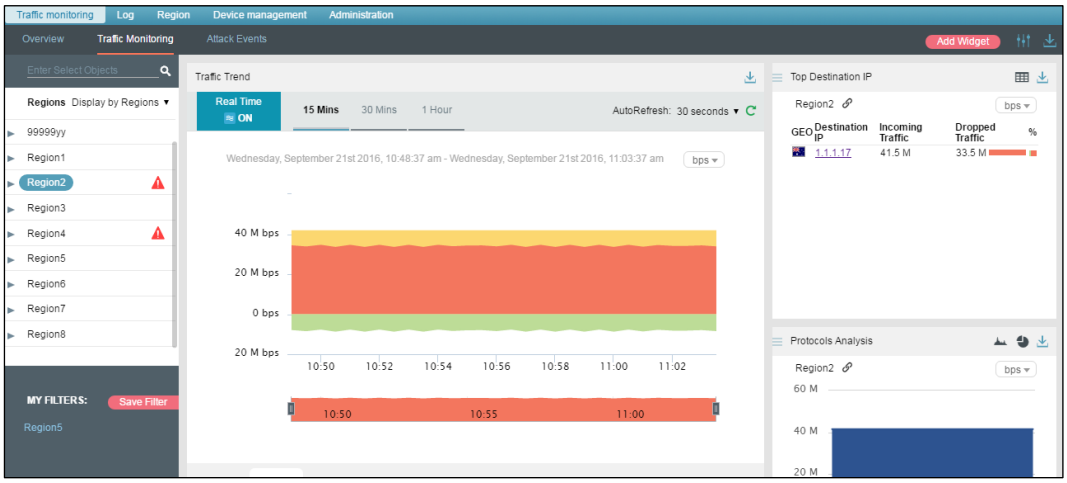



### 3.1.11.1 Understanding Data on the Panel

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

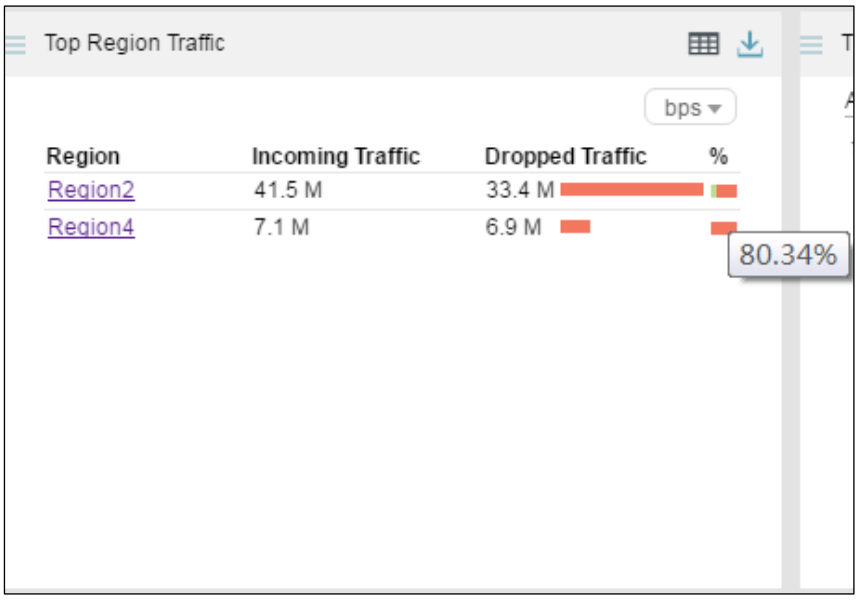
- **Region**: region for which traffic is dropped by ADS. Clicking a region name, for example, **Region2**, opens the **Traffic Monitoring** tab page, where you can view more details about traffic destined for this region, as shown in Figure 3-45.

Figure 3-45 Traffic of a specific region




- **Incoming 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 3-46, the percentage of dropped traffic for Region2 is 80.34%.

Figure 3-46 Percentage of dropped traffic for a specific region



### 3.1.11.2 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.

### 3.1.11.3 Downloading a Report

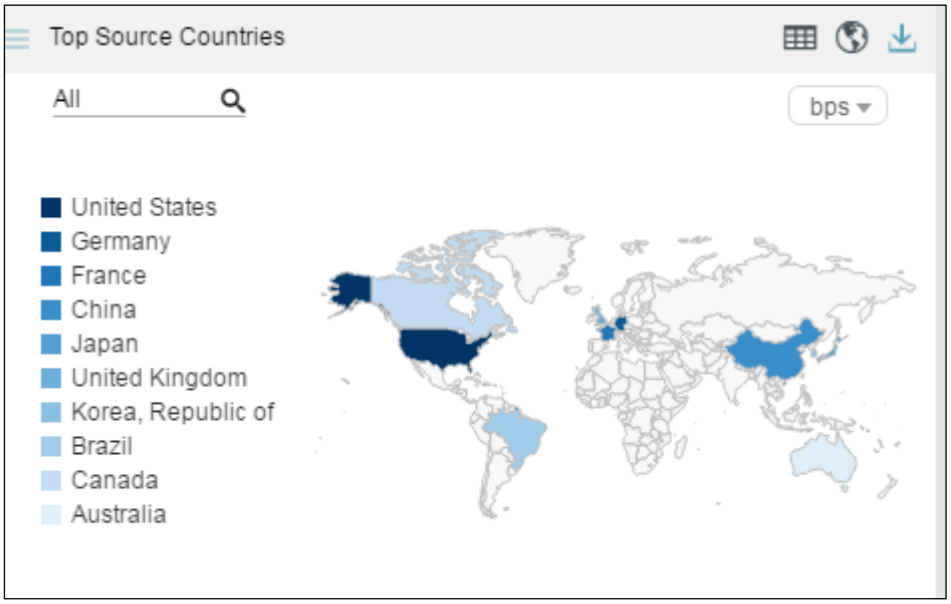
Click in the upper-right corner of the **Top Region Traffic** panel and then data of this panel will be exported as a report. For details, see section 3.1.5 Downloading a Report.

## 3.1.12 Viewing Traffic of Top Source Countries

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, as shown in Figure 3-47.

Data on this panel refreshes every 30 seconds.

Figure 3-47 Top Source Countries panel

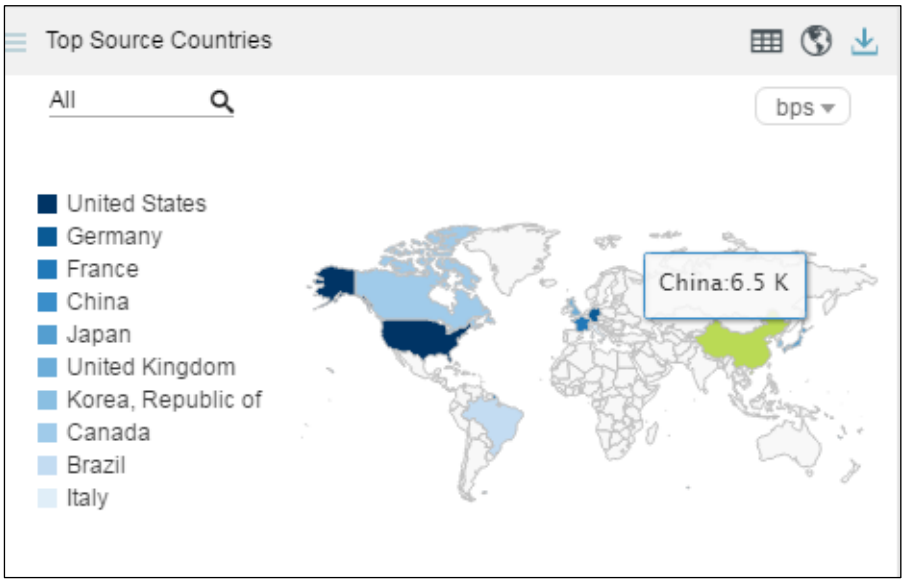



### 3.1.12.1 Understanding Data Displayed in a Map

Top 10 source countries 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 are indicated in a map with the same colors.

Pointing to the area of a top 10 country changes its color to green and displays the country name and the value of traffic dropped by ADS, as shown in Figure 3-48.

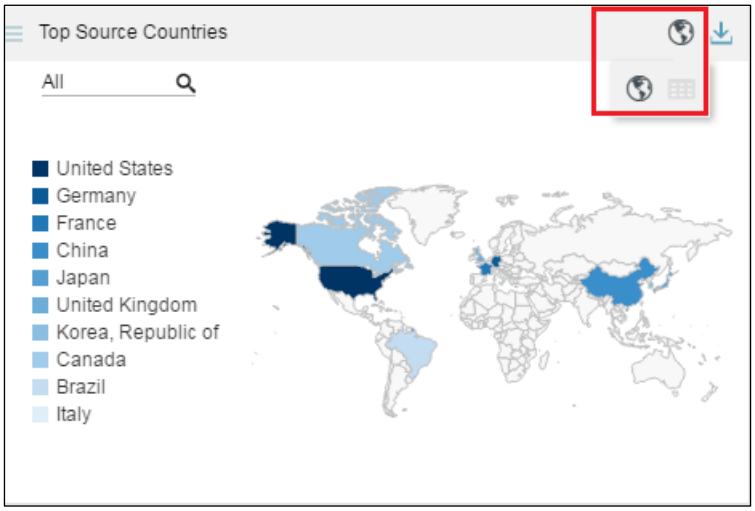
Figure 3-48 Display of the value of attack traffic from a country




## 3.1.12.2 Switching the Display Mode

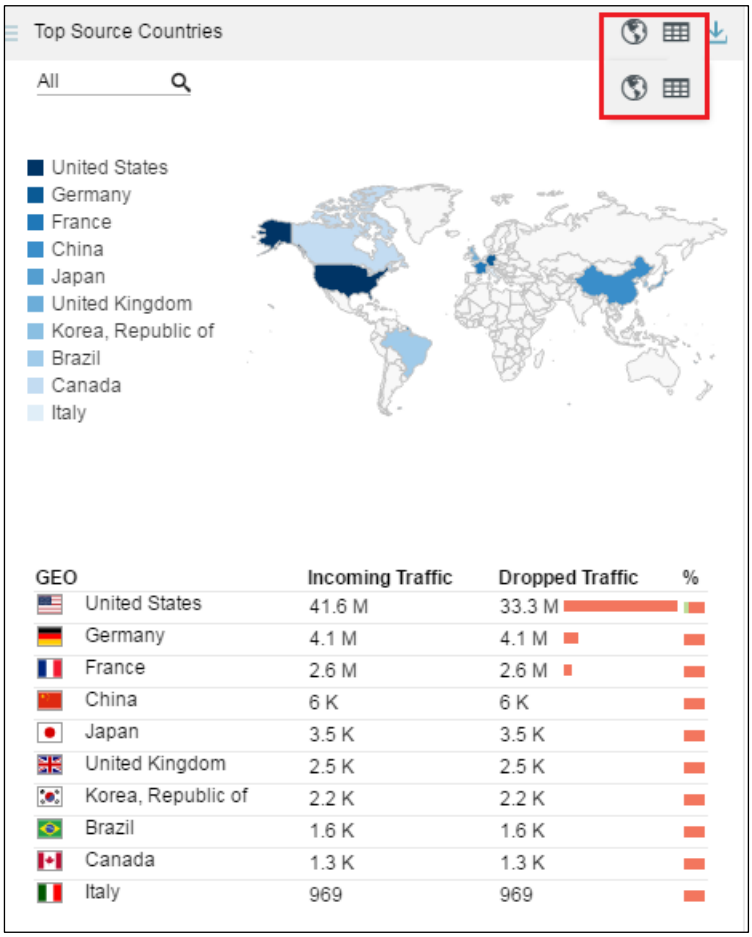
By default, traffic of top 10 source countries is presented in a map of the world. You can click in the upper-right corner of the **Top Source Countries** panel to choose a display mode (list or map) or both modes, as shown in Figure 3-49.

Figure 3-49 Switching the display mode



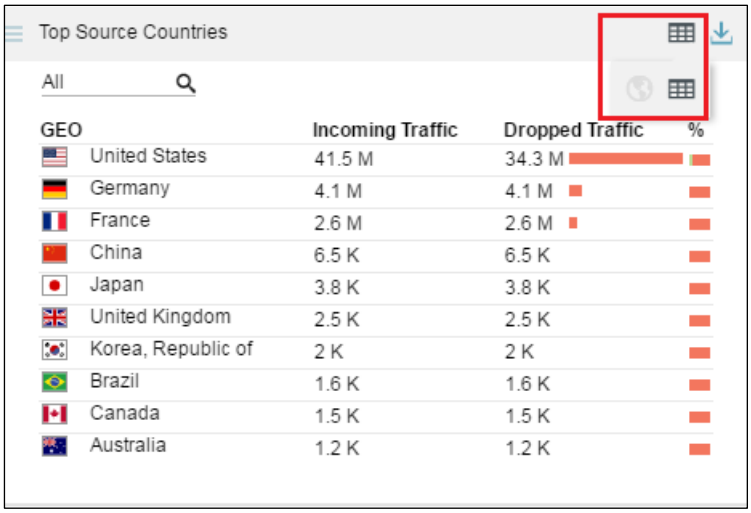

In Figure 3-49, appears normal, while appears dimmed. Therefore, data is presented only in a map. After you click , this icon turns . In this case, traffic data is presented in both a map and a list, as shown in Figure 3-50.

Figure 3-50 Display of traffic data in both a map and a list




Clicking makes this icon dimmed and hides the map, as shown in Figure 3-51.

Figure 3-51 Display of traffic data only in a list

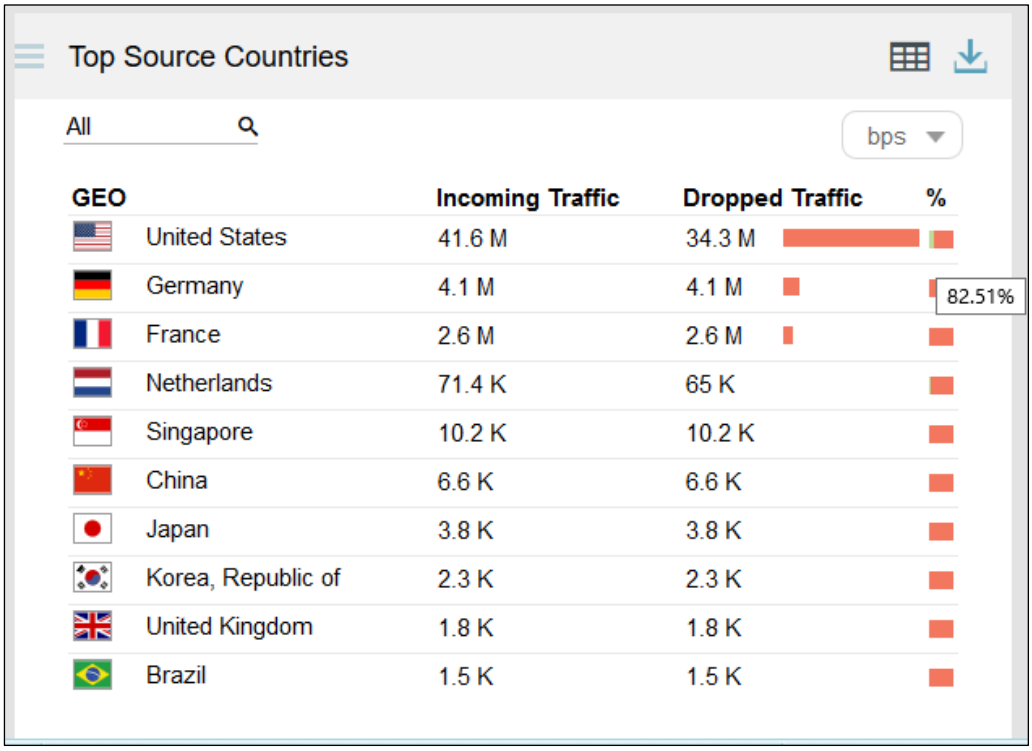


### 3.1.12.3 Viewing the List of Top Source Countries

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 3-37.
- **Incoming 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 3-52, the percentage of dropped traffic for United States is 82.51%.

Figure 3-52 Percentage of dropped traffic of a source country



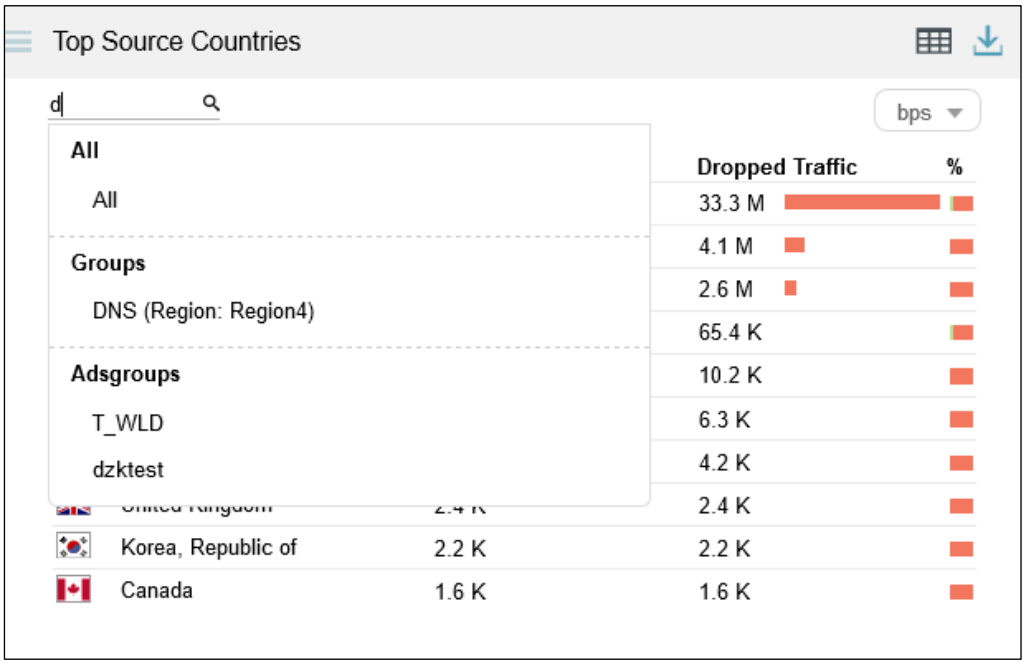

| GEO | Incoming Traffic | Dropped Traffic | % |
|---|---|---|---|
| United States | 41.6 M | 34.3 M | |
| Germany | 4.1 M | 4.1 M | |
| France | 2.6 M | 2.6 M | |
| Netherlands | 71.4 K | 65 K | |
| Singapore | 10.2 K | 10.2 K | |
| China | 6.6 K | 6.6 K | |
| Japan | 3.8 K | 3.8 K | |
| Korea, Republic of | 2.3 K | 2.3 K | |
| United Kingdom | 1.8 K | 1.8 K | |
| Brazil | 1.5 K | 1.5 K | |

### 3.1.12.4 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.

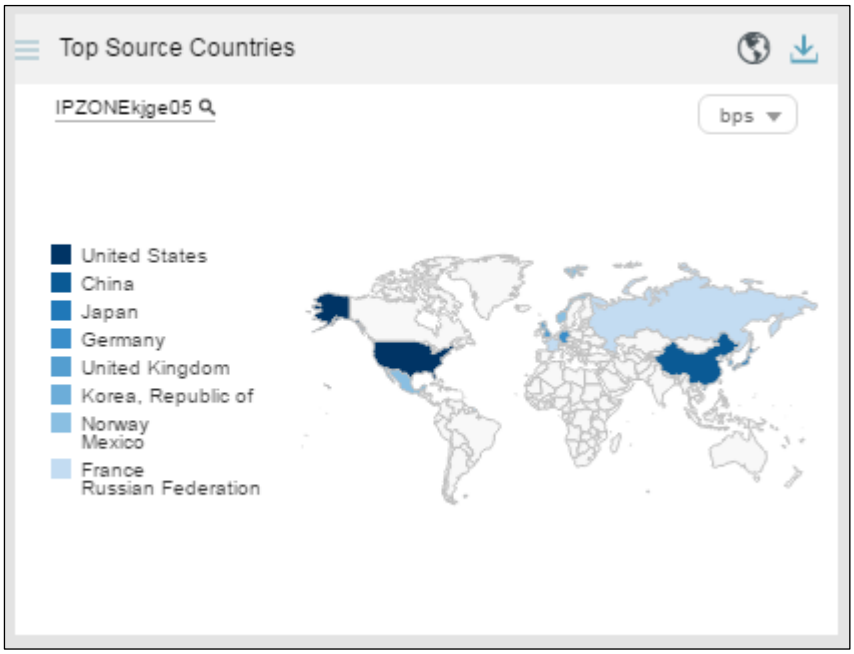
On the page shown in Figure 3-53, after you type a character string, the system displays all objects containing the typed character string.

Figure 3-53 Searching for a specific object




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

Figure 3-54 Traffic of top source countries associated with a specific object



### 3.1.12.5 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.

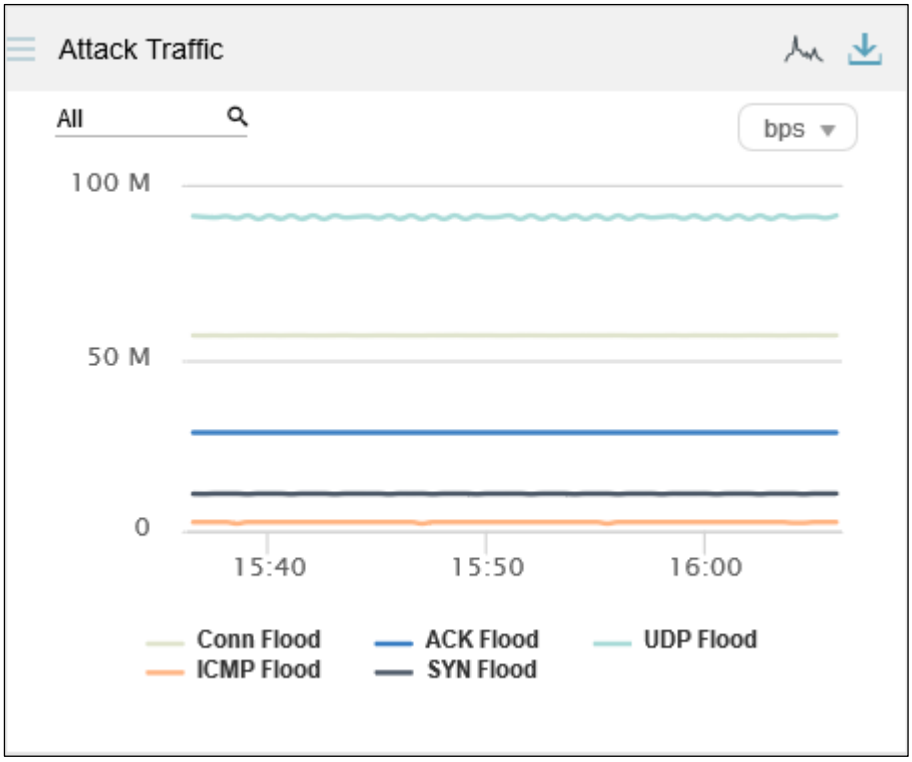
### 3.1.12.6 Downloading a Report

Click in the upper-right corner of the **Top Source Countries** panel and then data of this panel will be exported as a report. For details, see section 3.1.5 Downloading a Report.

## 3.1.13 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.

Figure 3-55 Attack traffic




### 3.1.13.1 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.

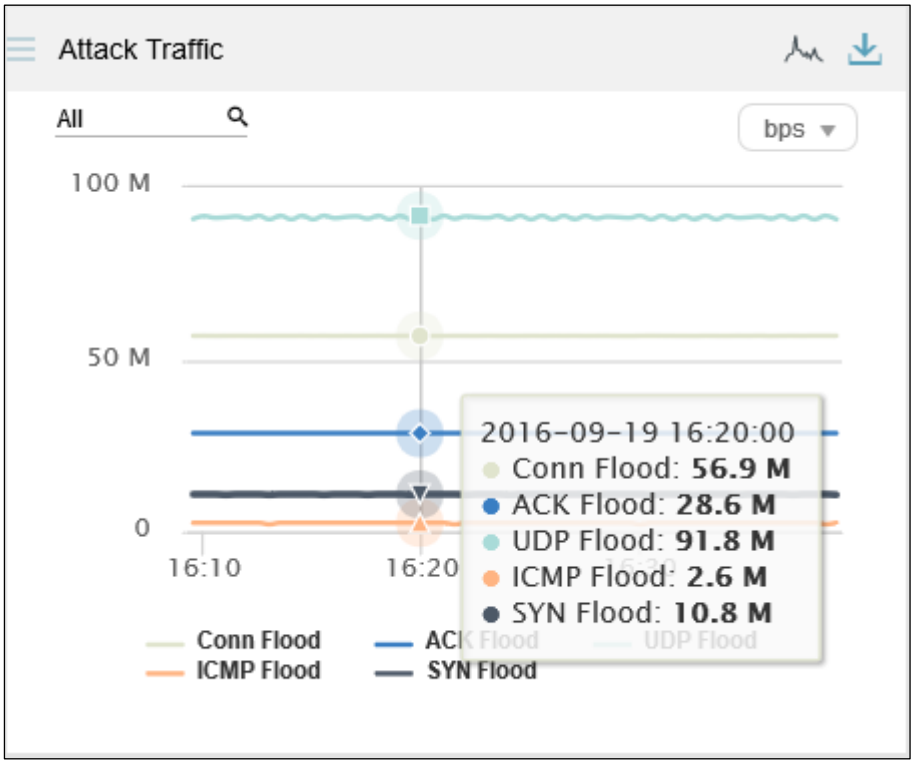
Table 3-2 Mappings between attack types and curve colors

| Attack Type | Curve Color |
|---|---|
| ICMP flood attack | ICMP Flood |
| UDP flood attack | UDP Flood |
| Connection flood attack | Conn Flood |
| Others | Others |
| ACK flood attack | ACK Flood |
| SYN flood attack | SYN Flood |

## 3.1.13.2 Viewing Traffic at a Point of Time

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

Figure 3-56 Viewing traffic at a specific point of time



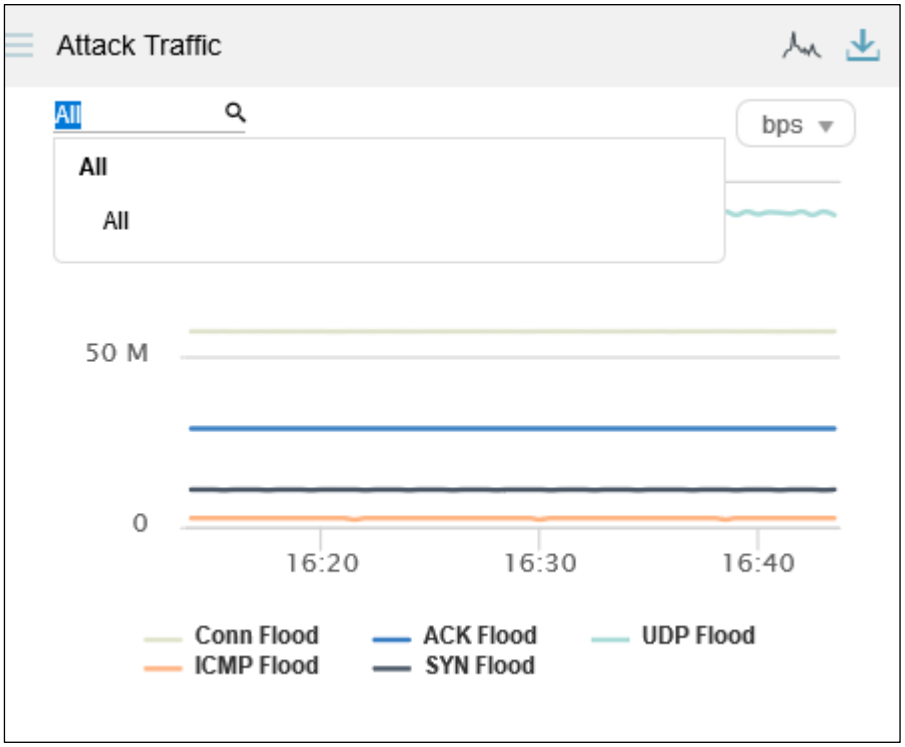

## 3.1.13.3 Viewing Attack Traffic of a Specified Object

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 3-56, type a character string.

The system displays all objects containing the typed character string.

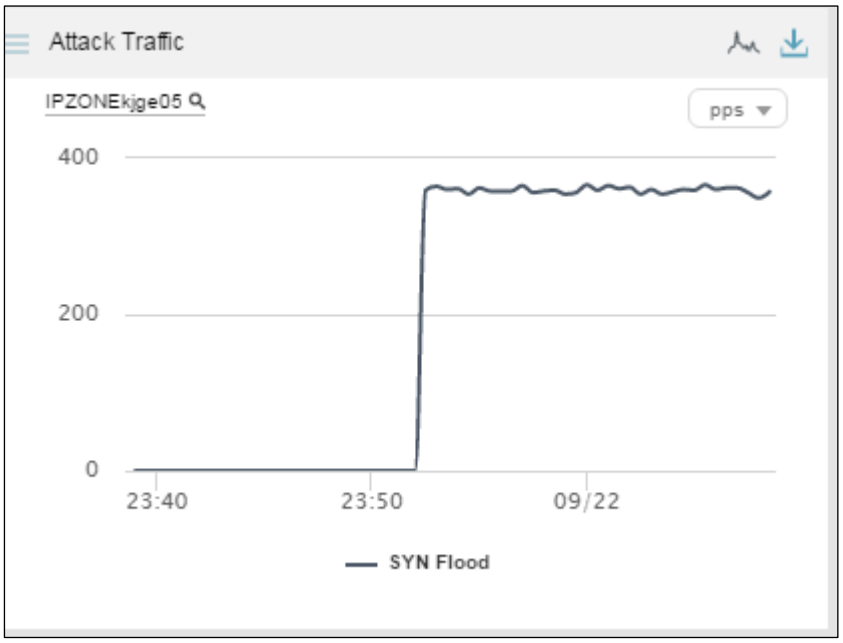
Figure 3-57 Searching for an object




**Step 2** Click a desired object.

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

Figure 3-58 Viewing the attack traffic trend of a specified object



**----End**

### 3.1.13.4 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.

### 3.1.13.5 Downloading a Report

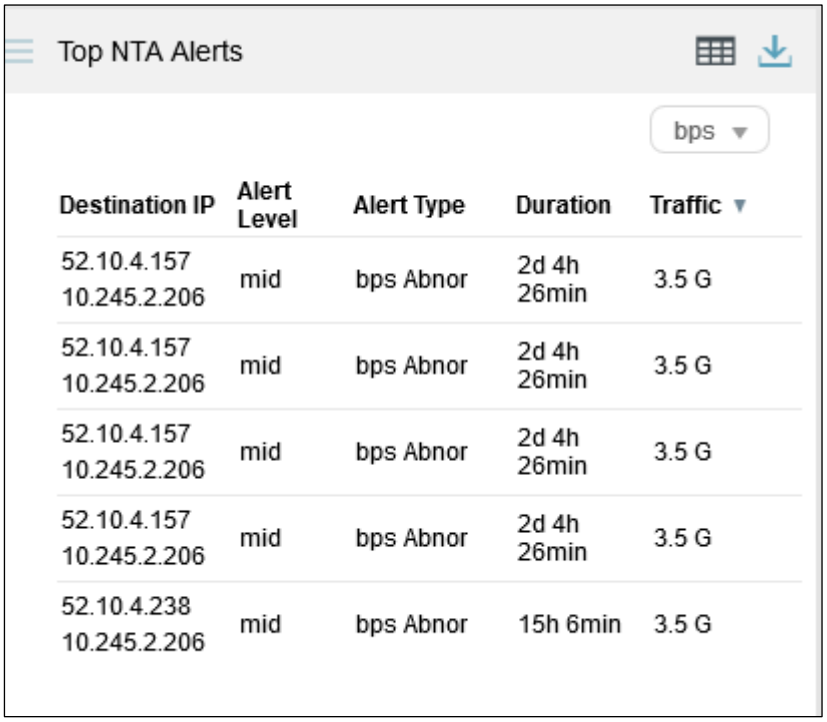
Click in the upper-right corner of the **Attack Traffic** panel and then data of this panel will be exported as a report. For details, see section 3.1.5 Downloading a Report.

## 3.1.14 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 3-59 Top alerts reported by NTA




### 3.1.14.1 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**, **Medium**, or **Low**. The alert level is determined by the deviation of the actual traffic value from the specified threshold. As

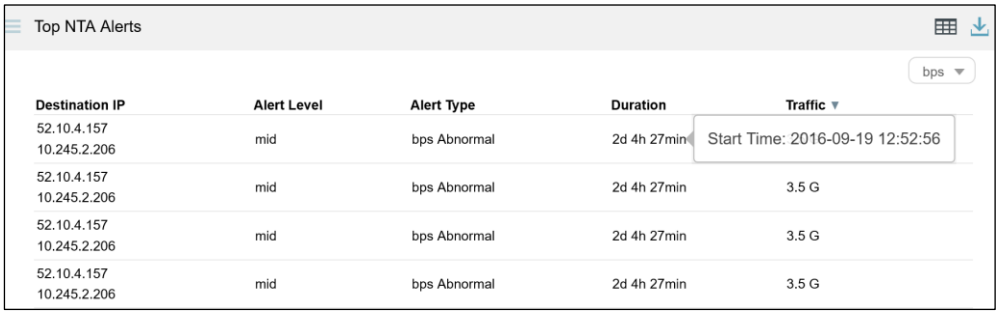
thresholds vary with NTA devices, alert levels of these devices are determined by different deviations.

- **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 NTS, see section "Alert Parameters" in the *NSFOCUS NTA User Guide*. |

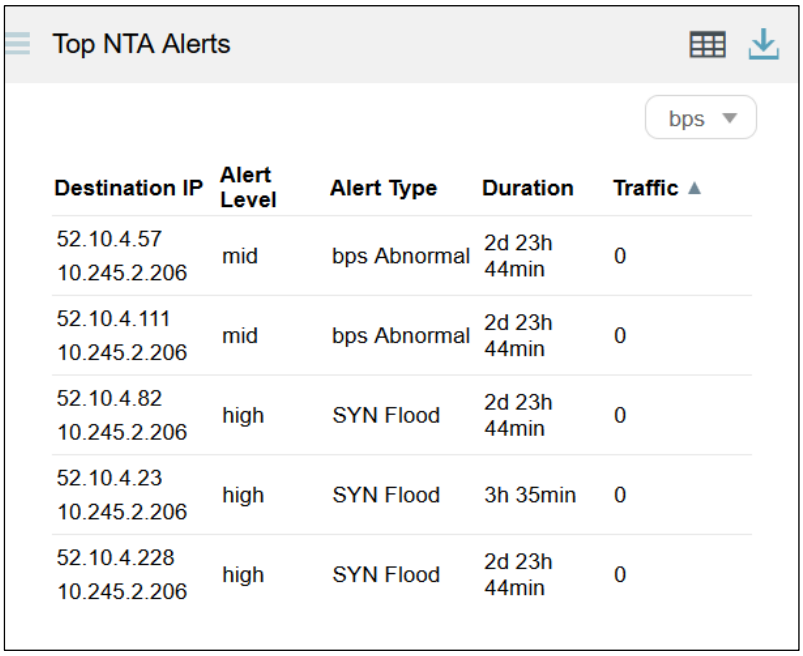
- **Duration**: shows the duration of the alert from the start time to current time. Pointing to a specific duration displays the start time of the attack against the destination IP address, as shown in Figure 3-60.

Figure 3-60 Start time of an alert reported by NTA




- **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 3-61 Top alerts reported by NTA in terms of smallest traffic




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

### 3.1.14.2 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.

### 3.1.14.3 Downloading a Report

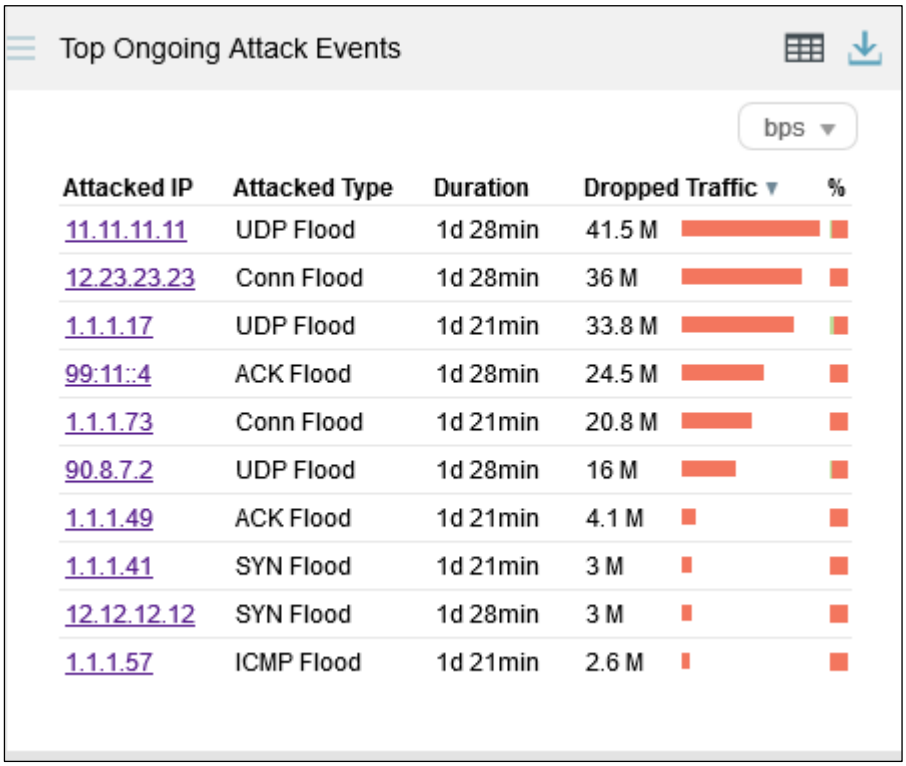
Click in the upper-right corner of the **Top NTA Alerts** panel and then data of this panel will be exported as a report. For details, see section 3.1.5 Downloading a Report.

## 3.1.15 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.

Figure 3-62 Top ongoing attack events



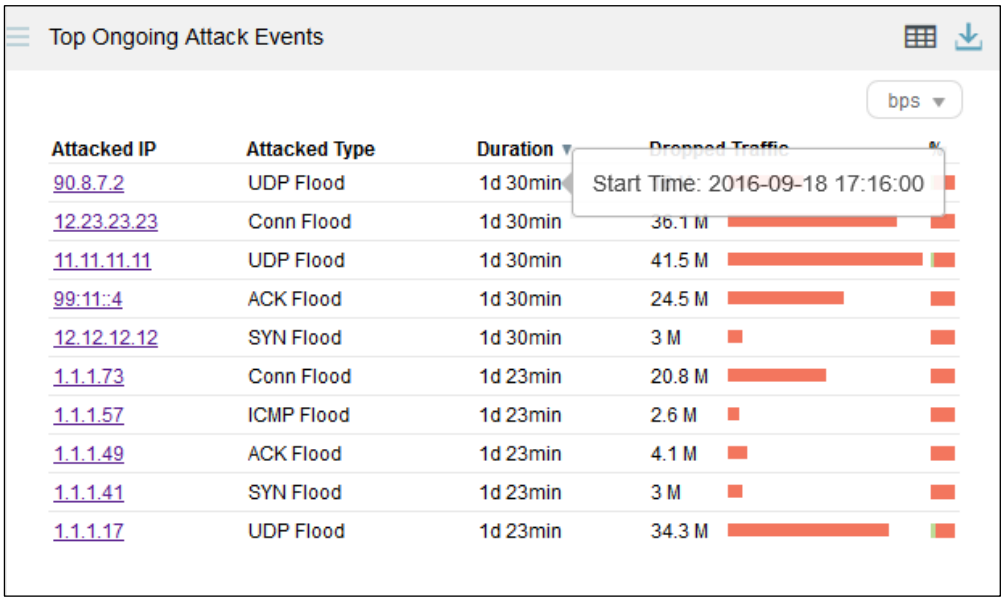

| Attacked IP | Attacked Type | Duration | Dropped Traffic | % |
|---|---|---|---|---|
| 11.11.11.11 | UDP Flood | 1d 28min | 41.5 M | |
| 12.23.23.23 | Conn Flood | 1d 28min | 36 M | |
| 1.1.1.17 | UDP Flood | 1d 21min | 33.8 M | |
| 99:11::4 | ACK Flood | 1d 28min | 24.5 M | |
| 1.1.1.73 | Conn Flood | 1d 21min | 20.8 M | |
| 90.8.7.2 | UDP Flood | 1d 28min | 16 M | |
| 1.1.1.49 | ACK Flood | 1d 21min | 4.1 M | |
| 1.1.1.41 | SYN Flood | 1d 21min | 3 M | |
| 12.12.12.12 | SYN Flood | 1d 28min | 3 M | |
| 1.1.1.57 | ICMP Flood | 1d 21min | 2.6 M | |

### 3.1.15.1 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.

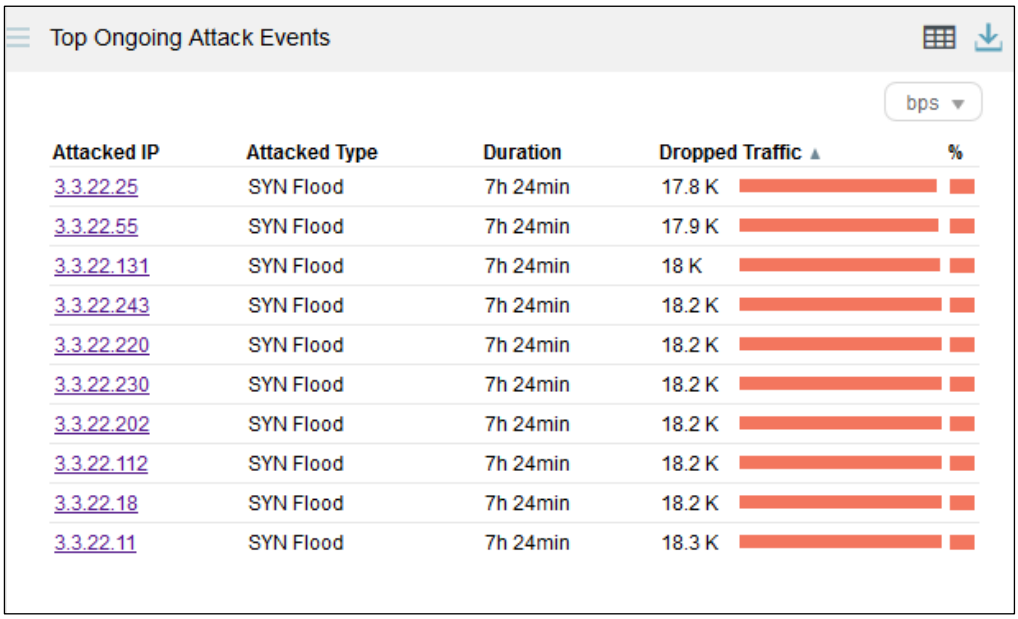
- **Attacked IP**: shows the attacked IP address. Clicking an IP address, you can view its detailed attack event information on an individual page. For details, see section 3.1.15.2 Viewing Attack Events Specific to an IP Address.
- **Attack Type**: shows the specific attack type.
- **Duration**: shows 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 3-63.

Figure 3-63 Start time of an ongoing attack event




- **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.

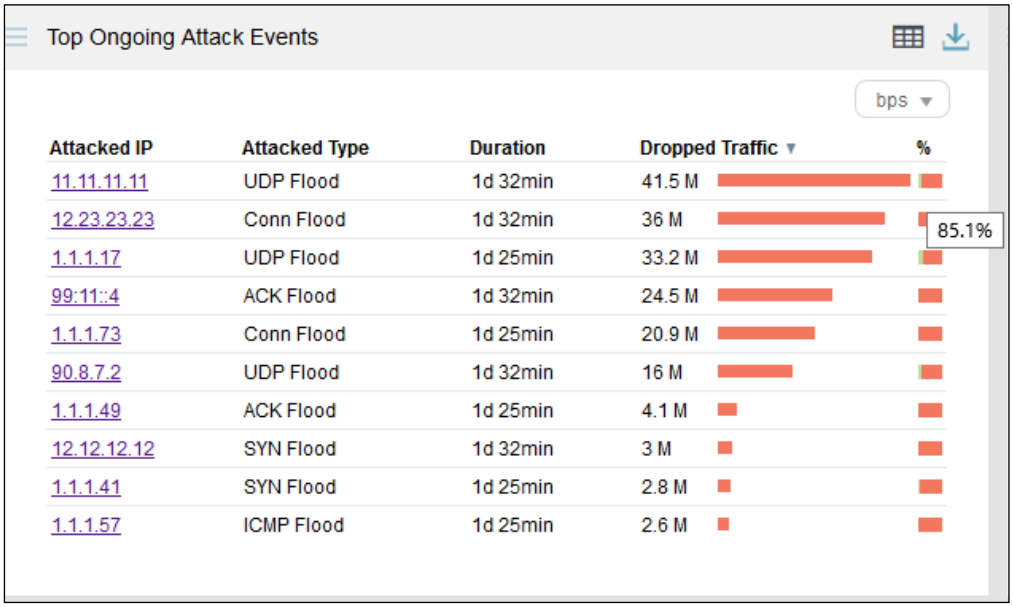
Figure 3-64 Top ongoing attack events by total minimum dropped traffic




- **%**: 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 3-65, the percentage of dropped traffic for 11.11.11.11 is 85.1%.

Figure 3-65 Percentage of forwarded traffic in an ongoing attack event




| Attacked IP | Attacked Type | Duration | Dropped Traffic | % |
|---|---|---|---|---|
| 11.11.11.11 | UDP Flood | 1d 32min | 41.5 M | |
| 12.23.23.23 | Conn Flood | 1d 32min | 36 M | |
| 1.1.1.17 | UDP Flood | 1d 25min | 33.2 M | |
| 99:11::4 | ACK Flood | 1d 32min | 24.5 M | |
| 1.1.1.73 | Conn Flood | 1d 25min | 20.9 M | |
| 90.8.7.2 | UDP Flood | 1d 32min | 16 M | |
| 1.1.1.49 | ACK Flood | 1d 25min | 4.1 M | |
| 12.12.12.12 | SYN Flood | 1d 32min | 3 M | |
| 1.1.1.41 | SYN Flood | 1d 25min | 2.8 M | |
| 1.1.1.57 | ICMP Flood | 1d 25min | 2.6 M | |

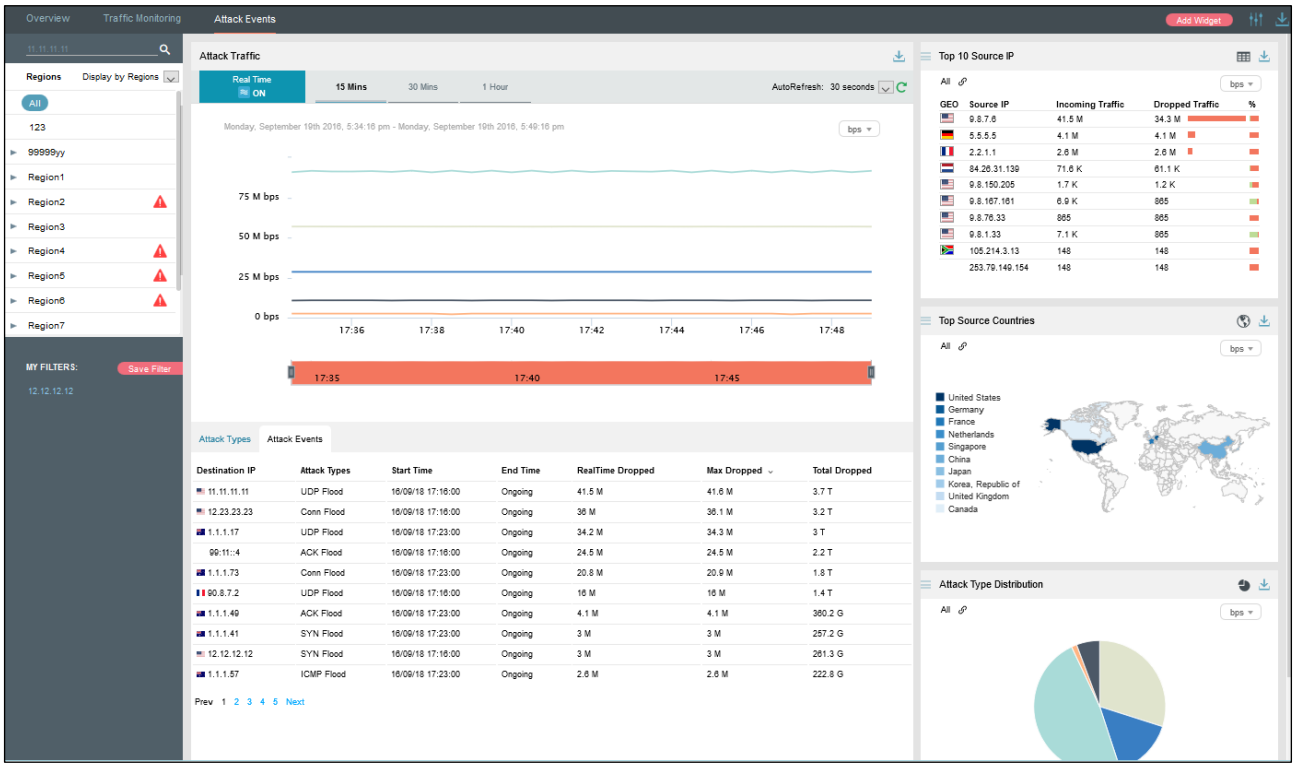
## 3.1.15.2 Viewing Attack Events Specific to an IP Address

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 3-65, click an IP address, for example, 11.11.11.11.

The **Attack Events** page is displayed, with the IP address in question already in the search box in the left, as shown in Figure 3-66.

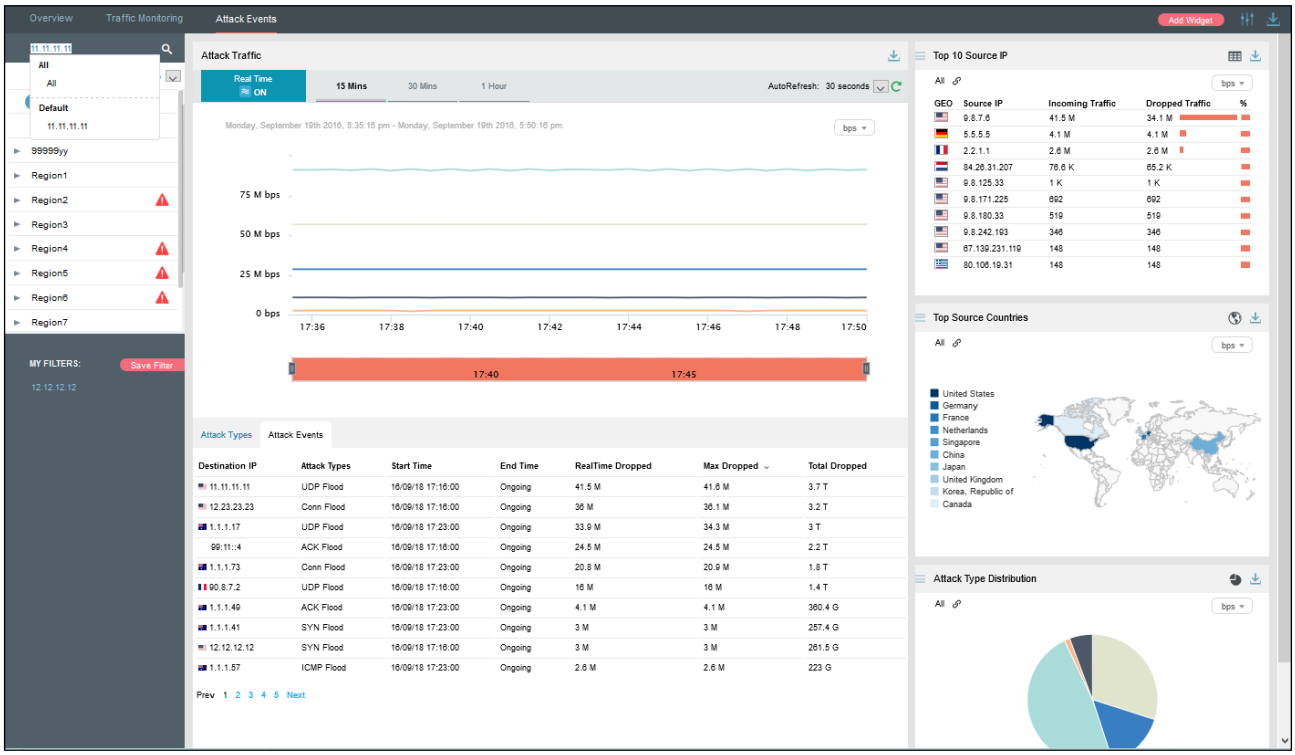
Figure 3-66 Attack traffic targeting an IP address




**Step 2** Click in the search box.

The system displays all objects containing the current IP address.

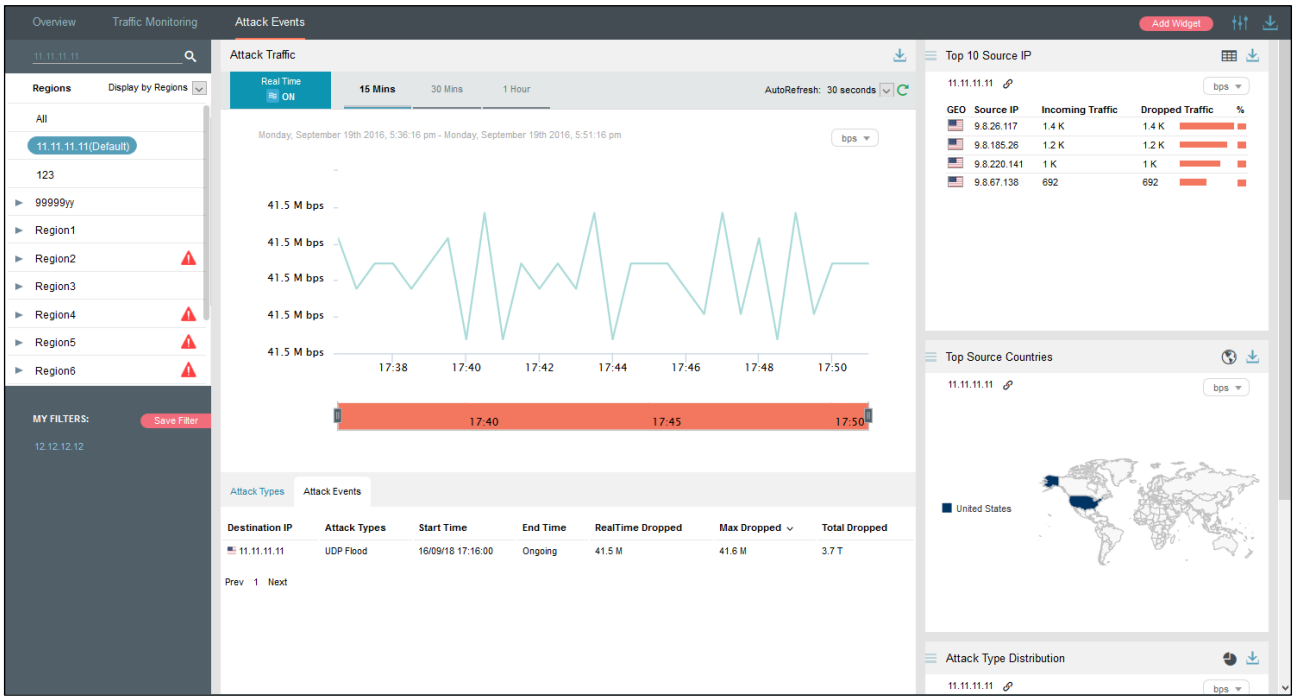
Figure 3-67 Searching for an IP address object




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

The attack event information of this IP address is displayed.

Figure 3-68 Viewing attack event information of an IP address




## 3.1.15.3 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.

## 3.1.15.4 Downloading a Report

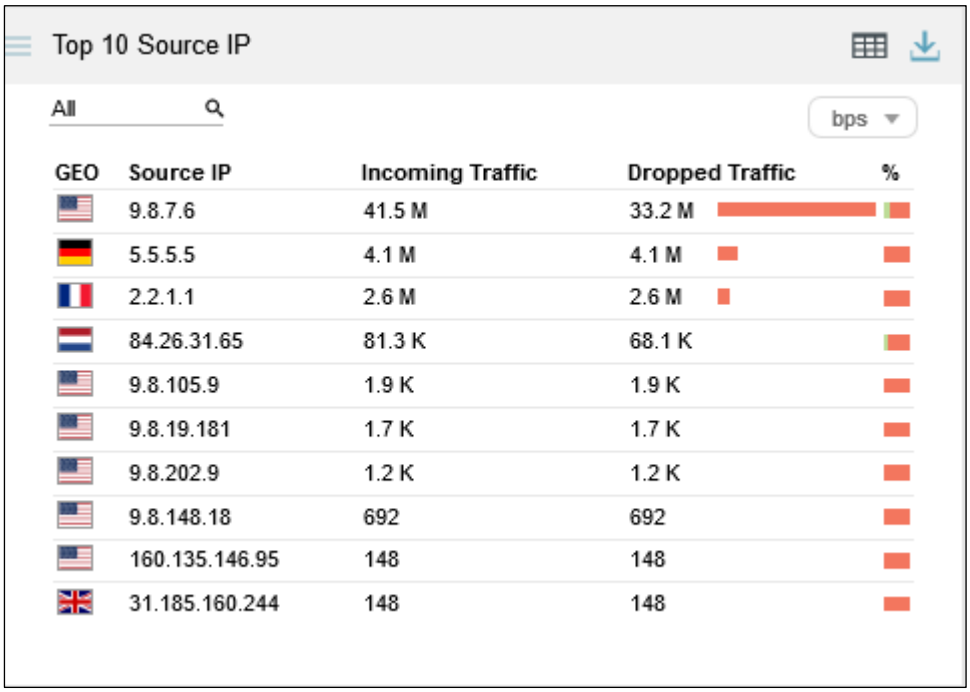
Click  in the upper-right corner of the **Top Ongoing Attack Events** panel and then data of this panel will be exported as a report. For details, see section 3.1.5 Downloading a Report.

# 3.1.16 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.

Figure 3-69 Top 10 source IP addresses

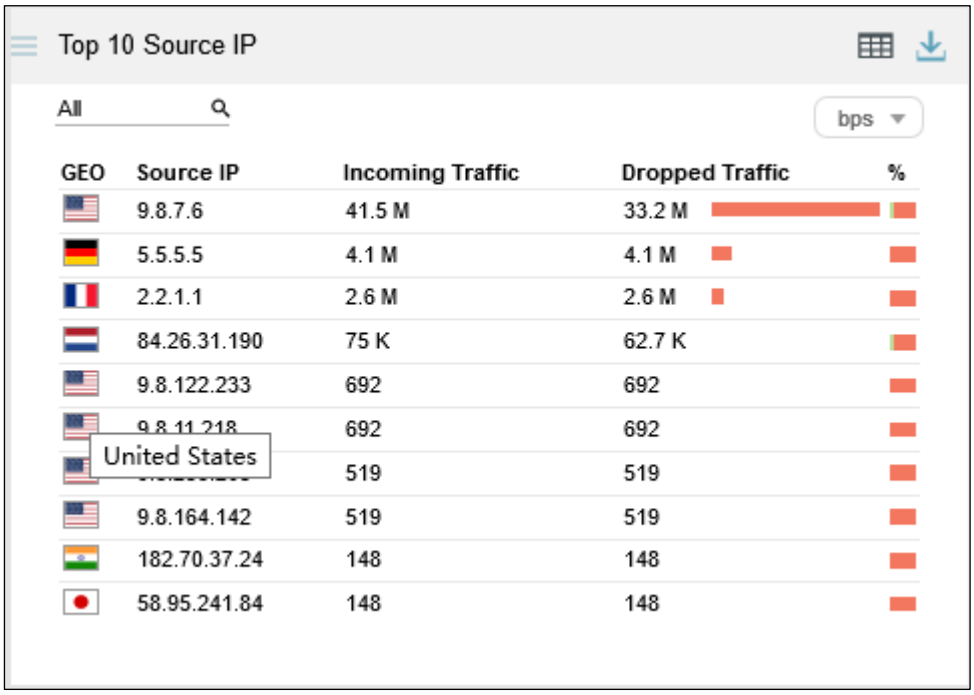



### 3.1.16.1 Understanding Data on the Panel

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

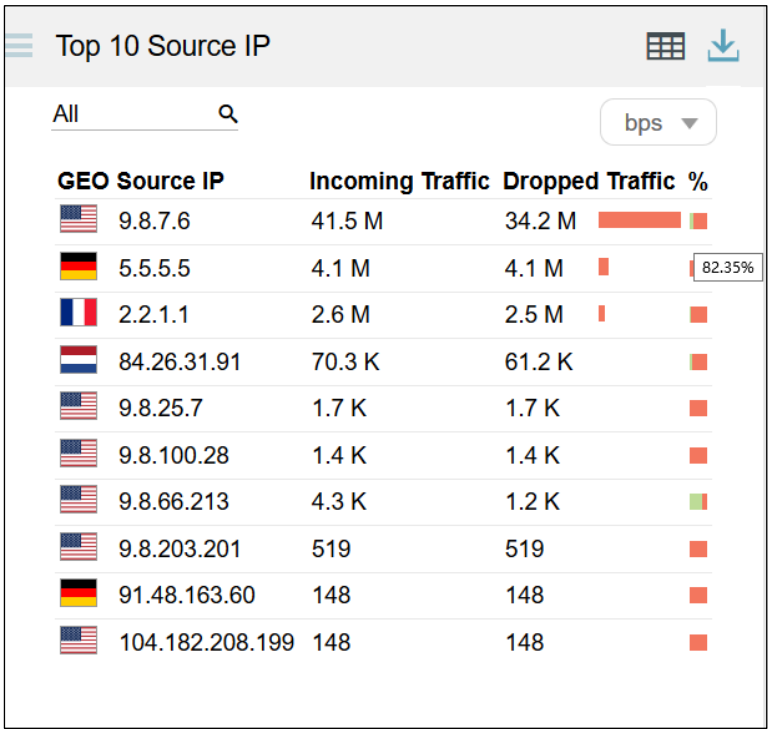
- **GEO**: shows the national flag icons. Pointing to an icon displays the country name, as shown in Figure 3-70.

Figure 3-70 Display of the country name




- **Source IP**: shows source IP addresses.
- **Incoming 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 3-71, the percentage of dropped traffic for 9.8.7.6 is 82.35%.

Figure 3-71 Percentage of dropped traffic of a source IP address



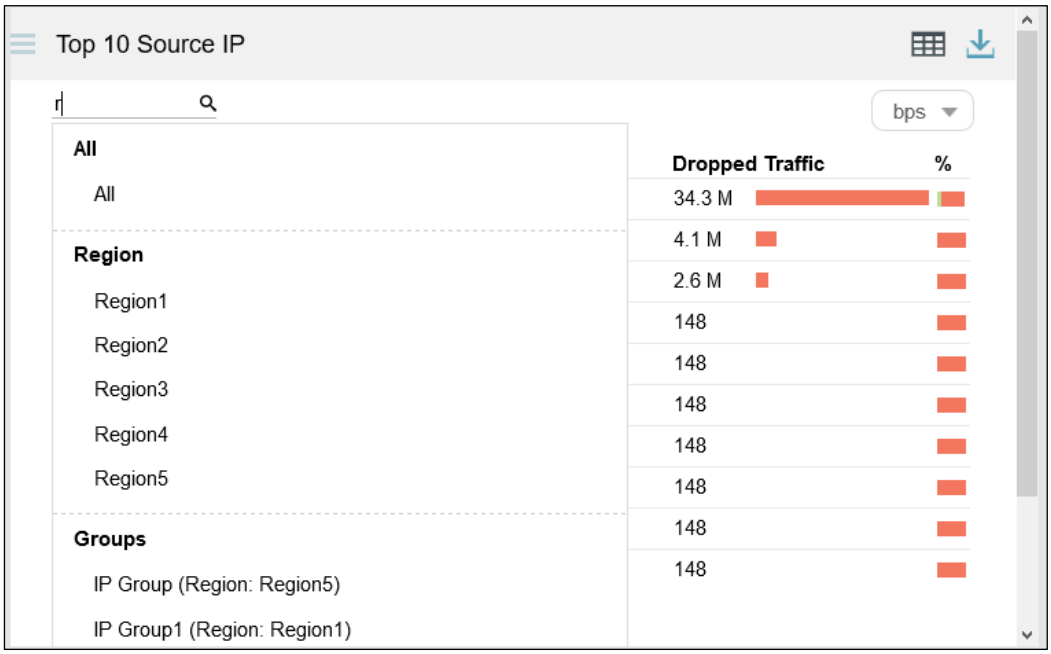

## 3.1.16.2 Viewing Traffic of a Specific Object

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 3-71, type a character string and then press **Enter**.

The system displays all objects containing the typed character string.

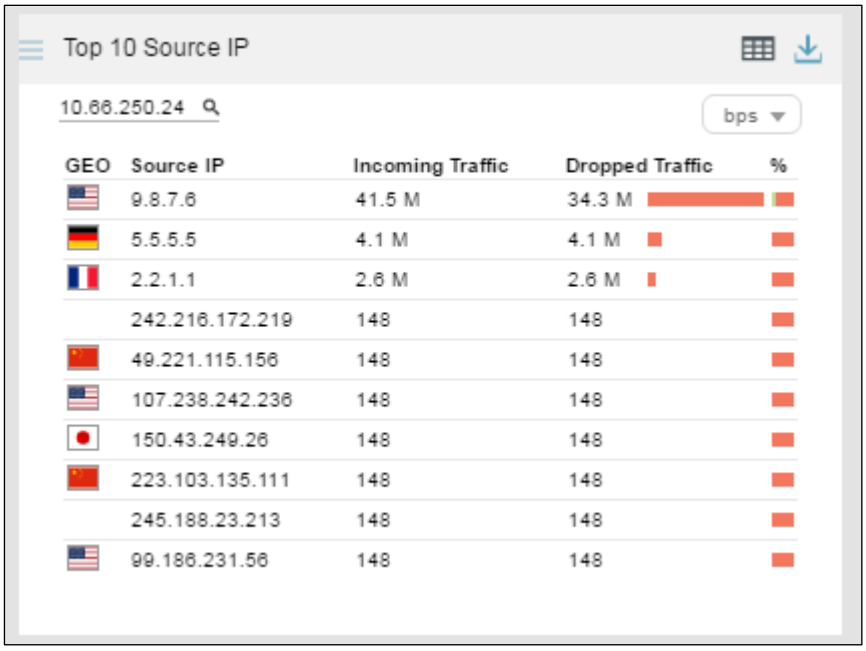
Figure 3-72 Searching for an object




**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 3-73 Viewing traffic of top 10 source IP addresses associated with a specific object



### 3.1.16.3 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 10 Source IP** panel to display traffic data in pps.

### 3.1.16.4 Downloading a Report

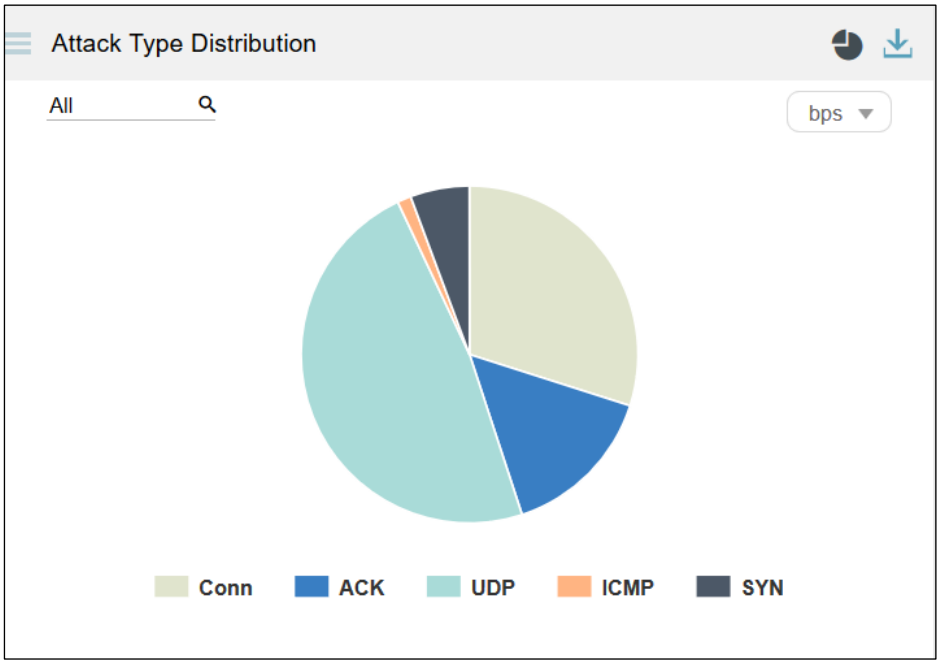
Click in the upper-right corner of the **Top 10 Source IP** panel and then data of this panel will be exported as a report. For details, see section 3.1.5 Downloading a Report.

## 3.1.17 Attack Type Distribution

The **Attack Type Distribution** panel shows the percentage of traffic of each attack type to the total traffic detected by ADS, as shown in Figure 3-74.

Data on this panel refreshes every 30 seconds.

Figure 3-74 Area representing traffic of an attack type separated from other areas




### 3.1.17.1 Understanding Data on the Panel

All attack types are displayed in a pie chart, with each indicated by a different color.

Table 3-3 Mappings between attack types and colors

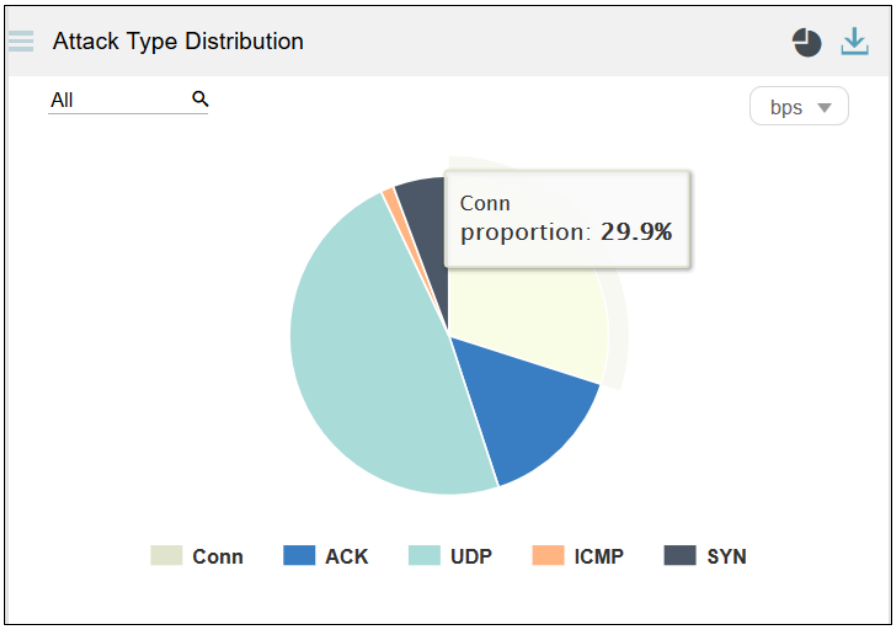
| Attack Type | Color |
|---|---|
| Connection flood attack | Conn |
| ACK flood attack | ACK |
| UDP flood attack | UDP |

| Attack Type | Color |
|---|---|
| ICMP flood attack | ICMP |
| SYN flood attack | SYN |

### 3.1.17.2 Viewing the Percentage of Traffic of an Attack Type

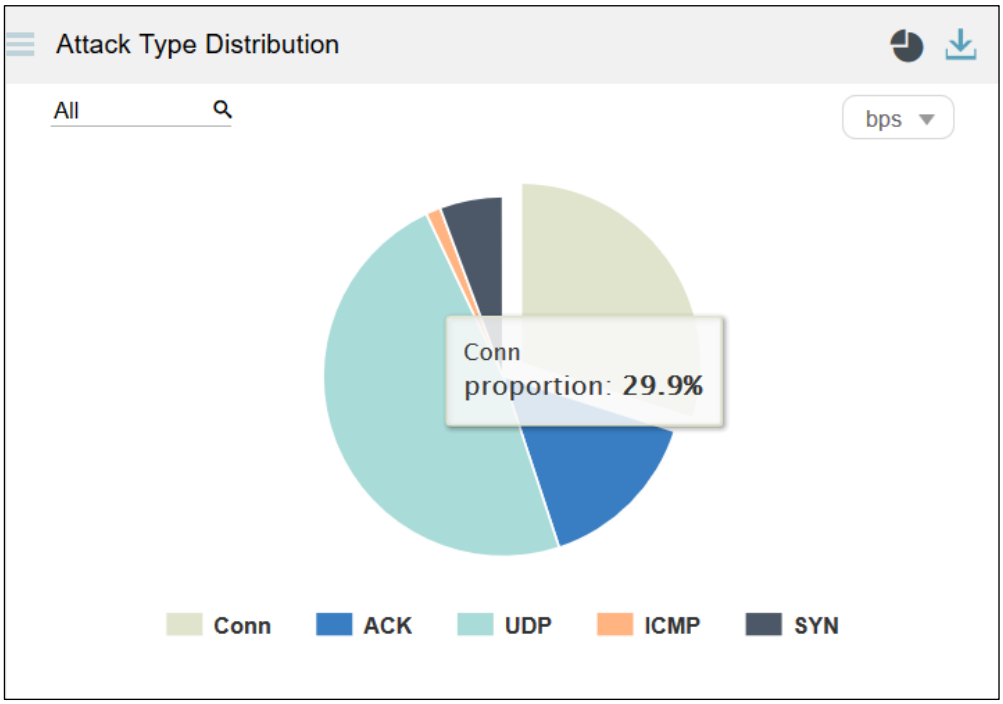
Pointing to the area of a specific attack type displays the percentage of traffic of this attack type to the total traffic, as shown in Figure 3-75.

Figure 3-75 Viewing the percentage of traffic of an attack type




Clicking in this area separates this area from other areas, as shown in Figure 3-76.

Figure 3-76 Separating the area of an attack type from other areas



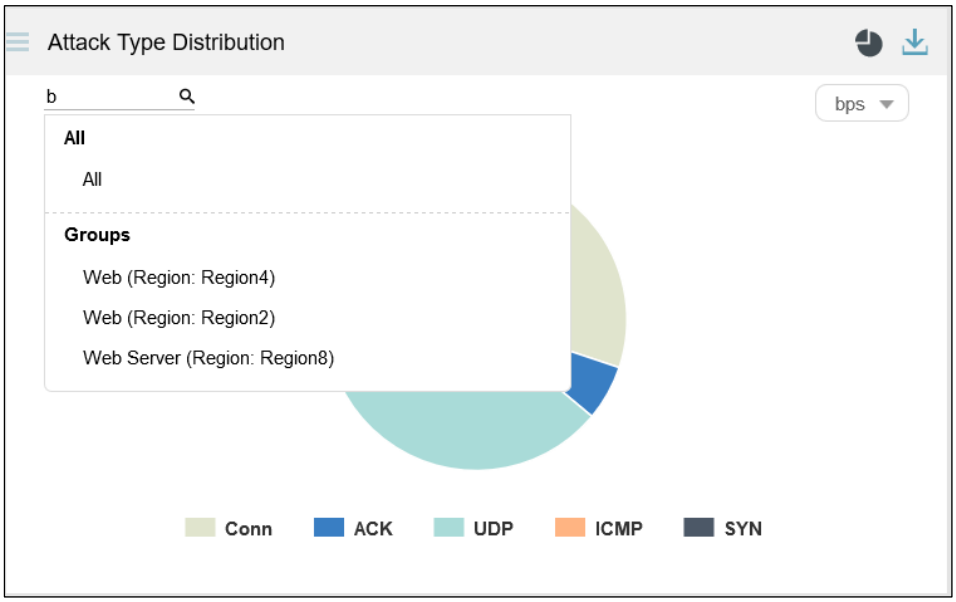

### 3.1.17.3 Viewing Attack Type Distribution of a Specified Object

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 3-74, type a character string.

The system displays all objects containing the typed character string.

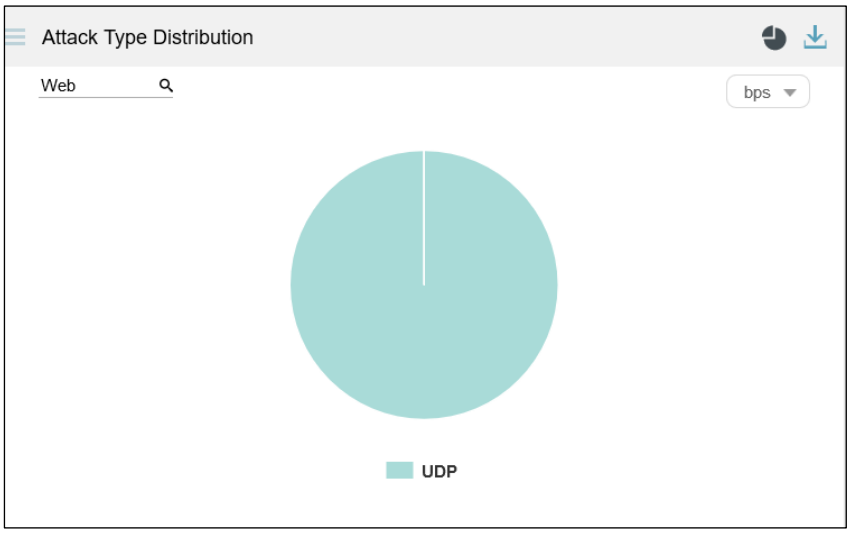
Figure 3-77 Searching for an object




**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 3-78 Viewing the attack type distribution of a specified object




## 3.1.17.4 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 Type Distribution** panel to display traffic data in pps.

### 3.1.17.5 Downloading a Report

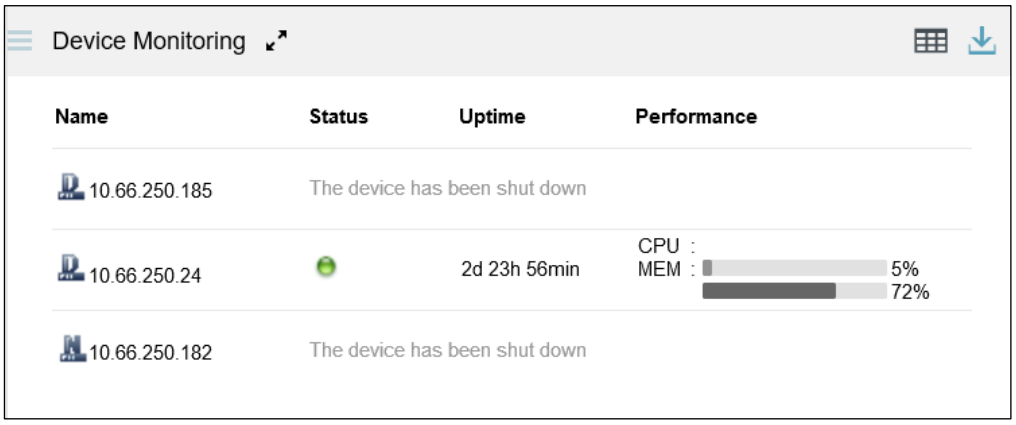
Click in the upper-right corner of the **Attack Type Distribution** panel and then data of this panel will be exported as a report. For details, see section 3.1.5 Downloading a Report.

## 3.1.18 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 3-79.

Data on this panel refreshes every 30 seconds.

Figure 3-79 Device monitoring information

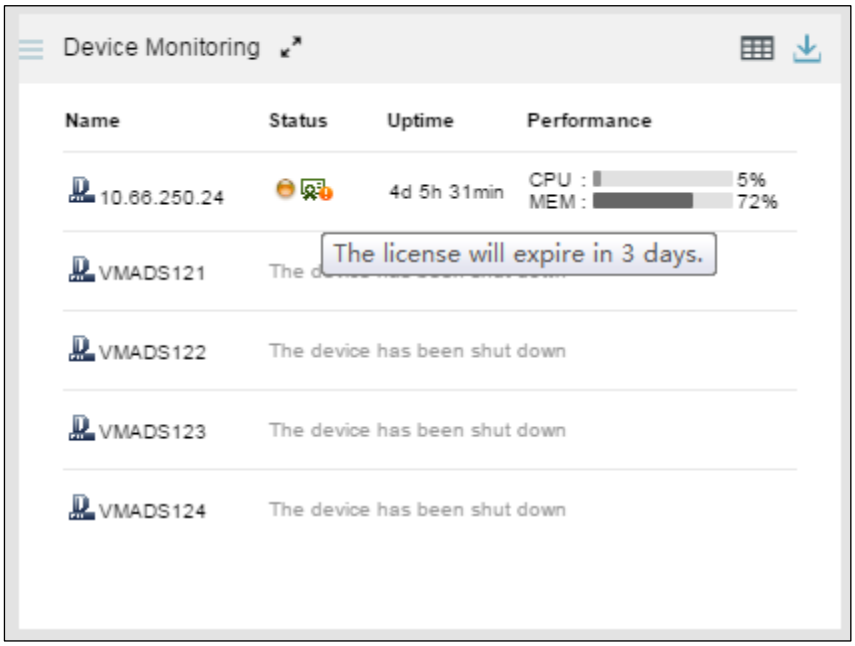



### 3.1.18.1 Understanding Data on the Panel

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 3-80 License expiration reminder

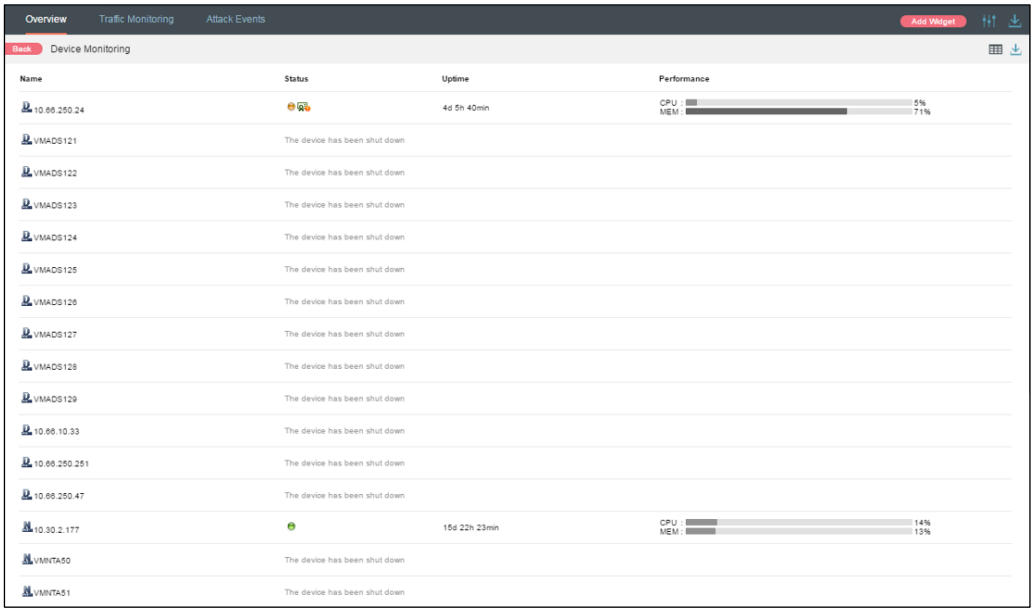



- **Uptime**: shows how long the system has been running continuously. The uptime is available only for online devices.
- **System Status**: shows the CPU/memory usage. Such information is available only to online devices.

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

You can click  to switch to the full screen mode.

Figure 3-81 Device monitoring information in full screen mode



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

#### 3.1.18.2 Downloading a Report

Click in the upper-right corner of the **Device Monitoring** panel and then data of this panel will be exported as a report. For details, see section 3.1.5 Downloading a Report.

## 3.2 Traffic Monitoring

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

- View real-time and historical traffic trends of all objects or a specified region, region 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 traffic monitoring information of such an IP address, you need to expressly indicate the IP address before the system displays such information.

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

### 3.2.1 Viewing Real-Time Traffic Monitoring Information

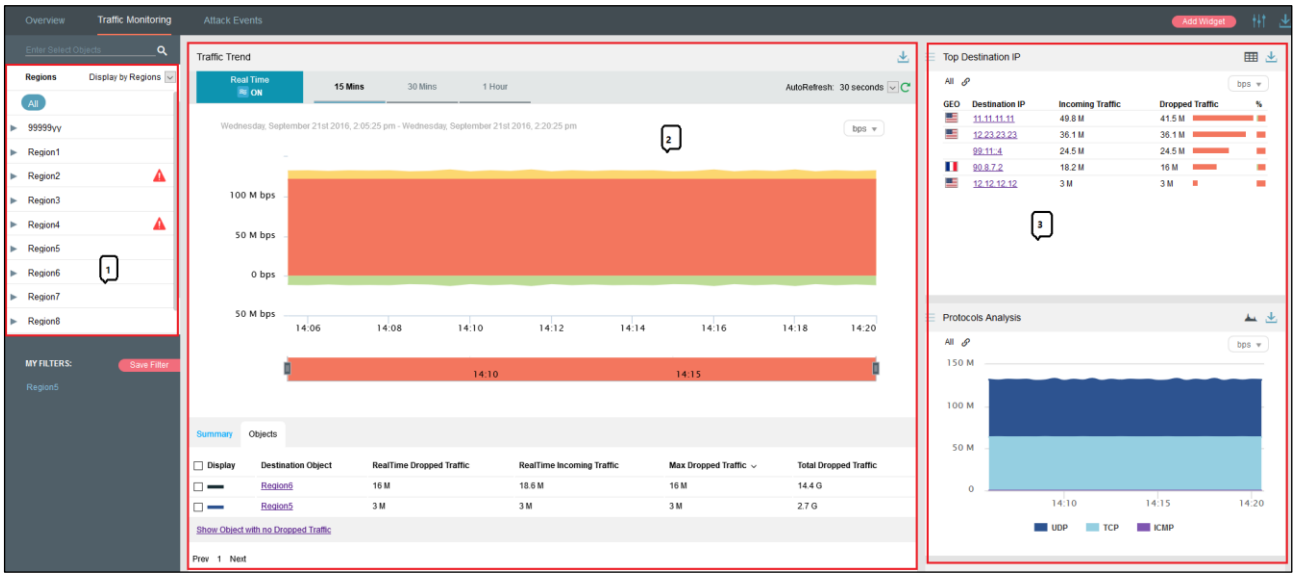
To view real-time traffic monitoring information, perform the following steps:

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

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

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

Figure 3-82 Traffic monitoring information of all objects




① List of objects ② Traffic trend ③ Panels

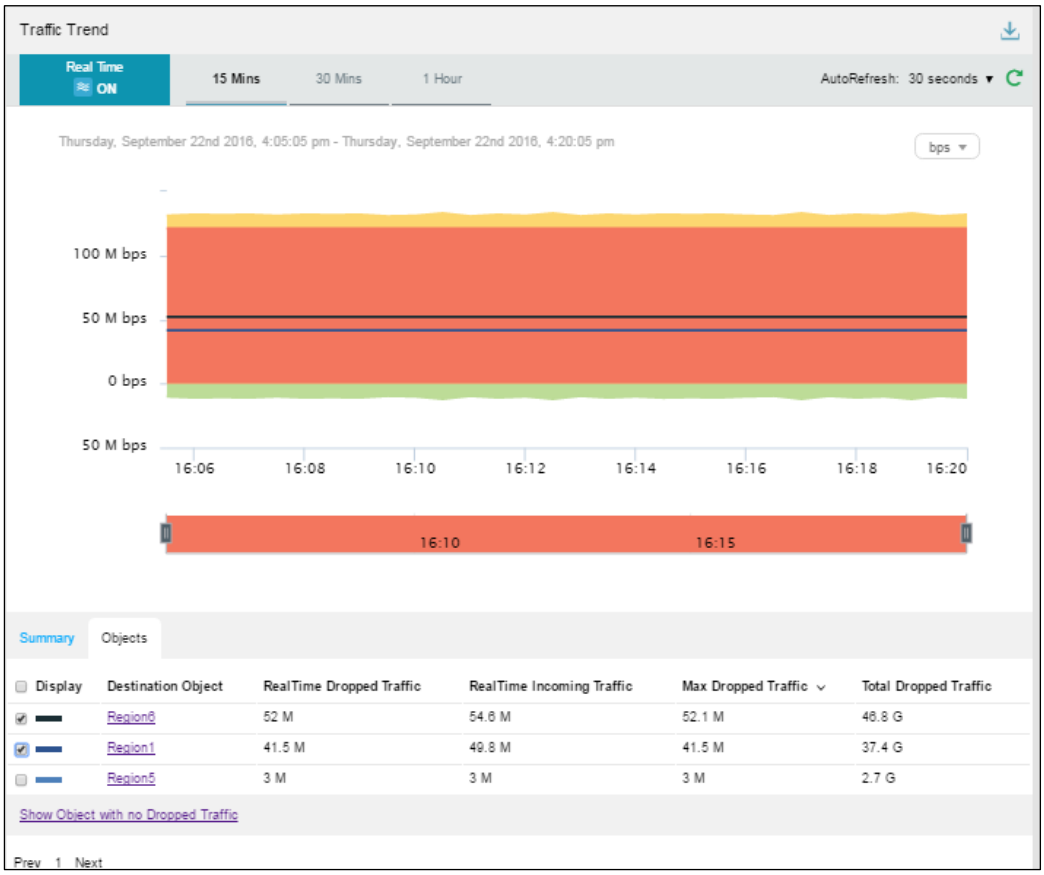
In the **Traffic Trend** panel, the **Objects** tab page ranks regions in descending order of traffic dropped by ADS.

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

| Parameter | Description |
|---|---|
| Display | Indicates the volume of dropped traffic with a color that shades from dark blue to light blue. |
| Destination Object | Indicates the traffic monitoring object. |
| RealTime Dropped Traffic | Indicates the traffic dropped by ADS for the object. The traffic unit is bps or pps. |
| RealTime Incoming Traffic | Indicates the real-time incoming traffic of the object. The traffic unit is bps or pps. |
| Max Dropped Traffic | Indicates the maximum traffic dropped by ADS for the object in the statistical period. The traffic unit is bps or pps. |
| Total Dropped Traffic | Indicates the total traffic dropped by ADS for the object in the statistical period. The traffic unit is bit. |

**Step 2** On the **Objects** tab page shown in Figure 3-82, select one or more objects to view traffic dropped by ADS for them.

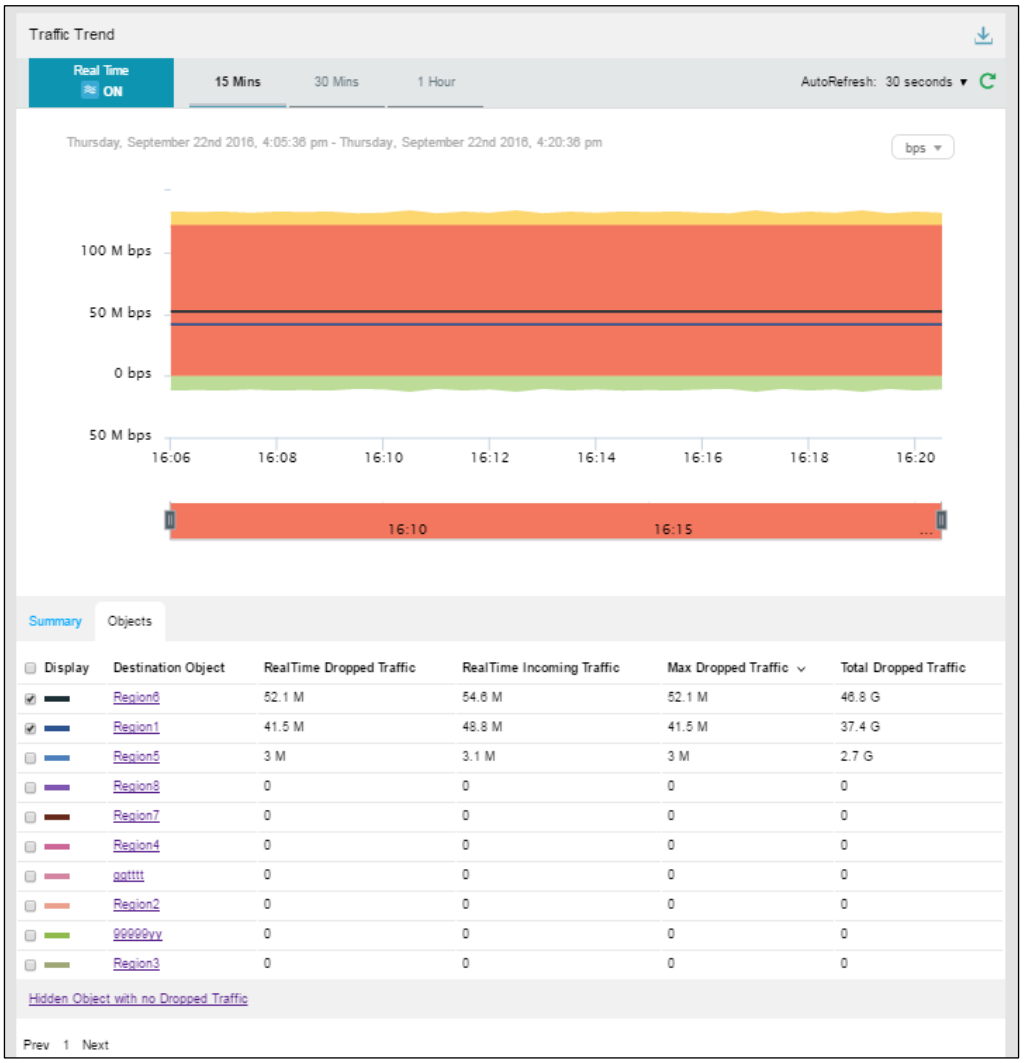
Figure 3-83 Viewing real-time traffic trend graph of a specified object




**Step 3** By default, only the objects with traffic dropped by ADS are displayed. Click the **Show Object with no Dropped Traffic** link to show all objects, as shown in Figure 3-84.

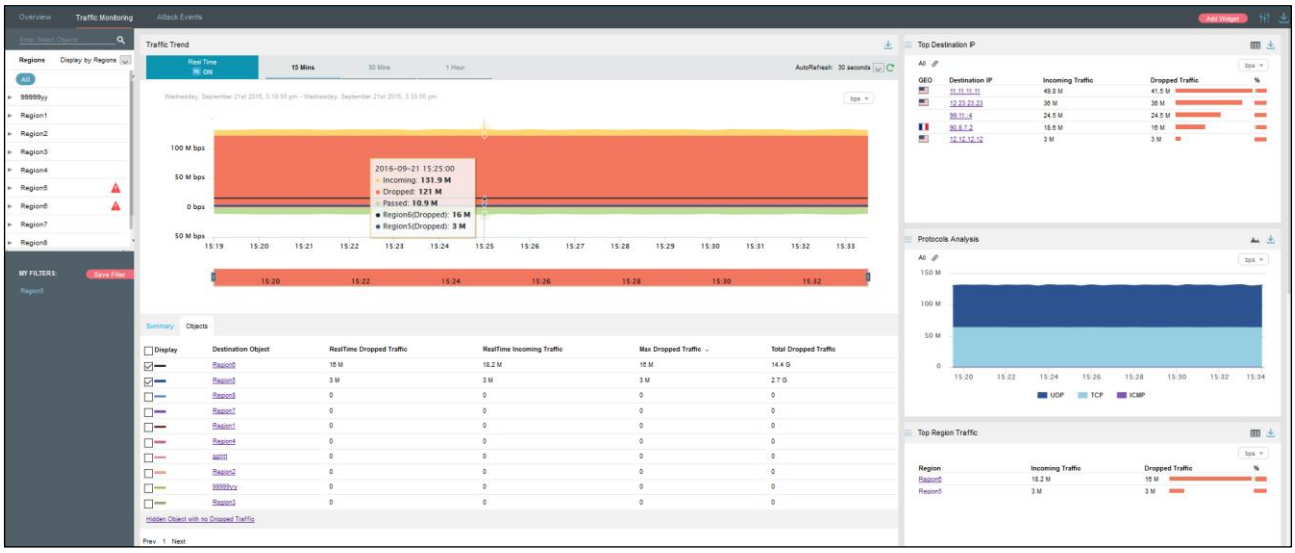
Clicking the **Hidden Object with no Dropped Traffic** link displays only objects with traffic dropped by ADS, but hides objects with no traffic dropped.

Figure 3-84 Real-time traffic trend graph of all objects



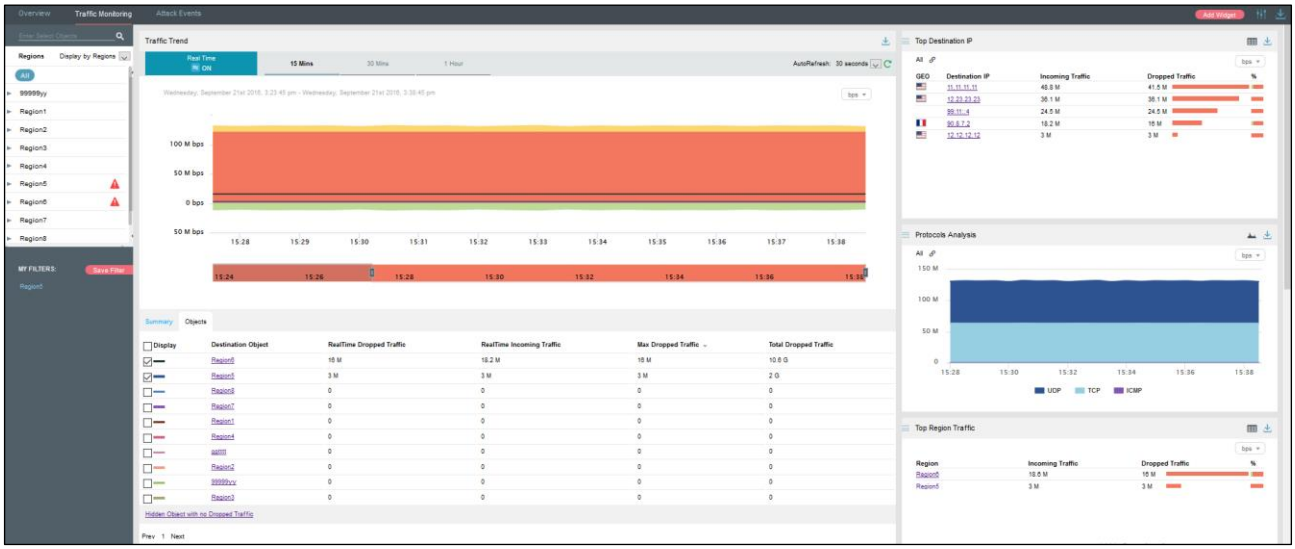

**Step 4** Point to a random point in the traffic trend graph to display the specific time, total traffic received, forwarded, and dropped by ADS for specified objects, as shown in Figure 3-85.

Figure 3-85 Traffic monitoring information at a specific time




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

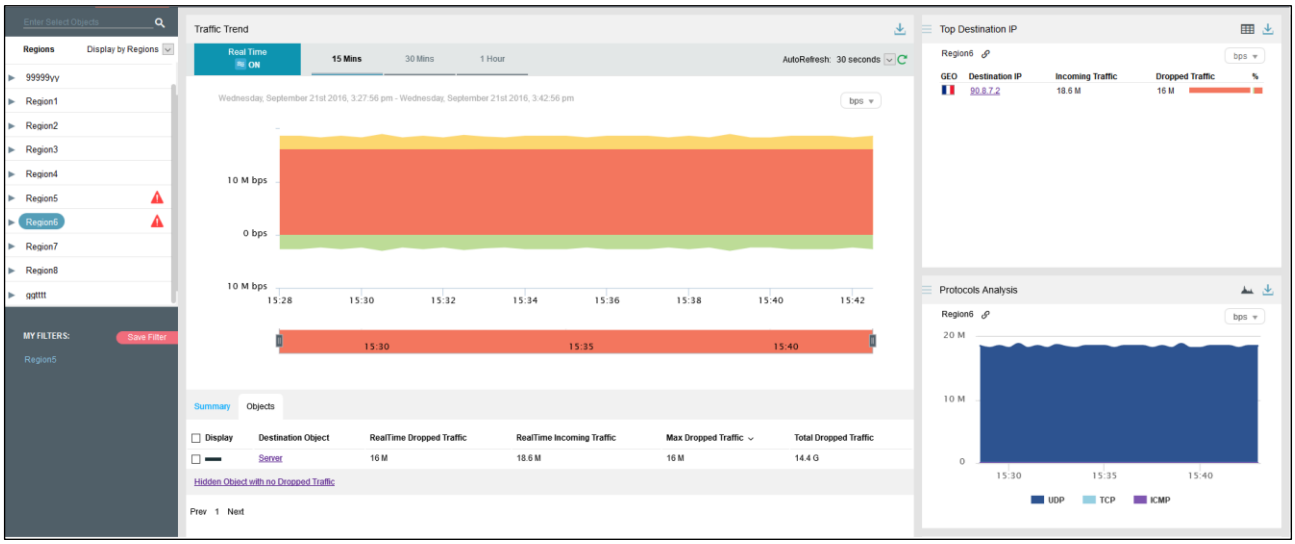
Figure 3-86 Viewing finer-granularity traffic monitoring information




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

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

Figure 3-87 Traffic monitoring information of a specific region




**Step 7** On the page shown in Figure 3-820, click **Summary**.

The average and total are displayed for dropped traffic, outgoing traffic, and incoming traffic in the statistical period.

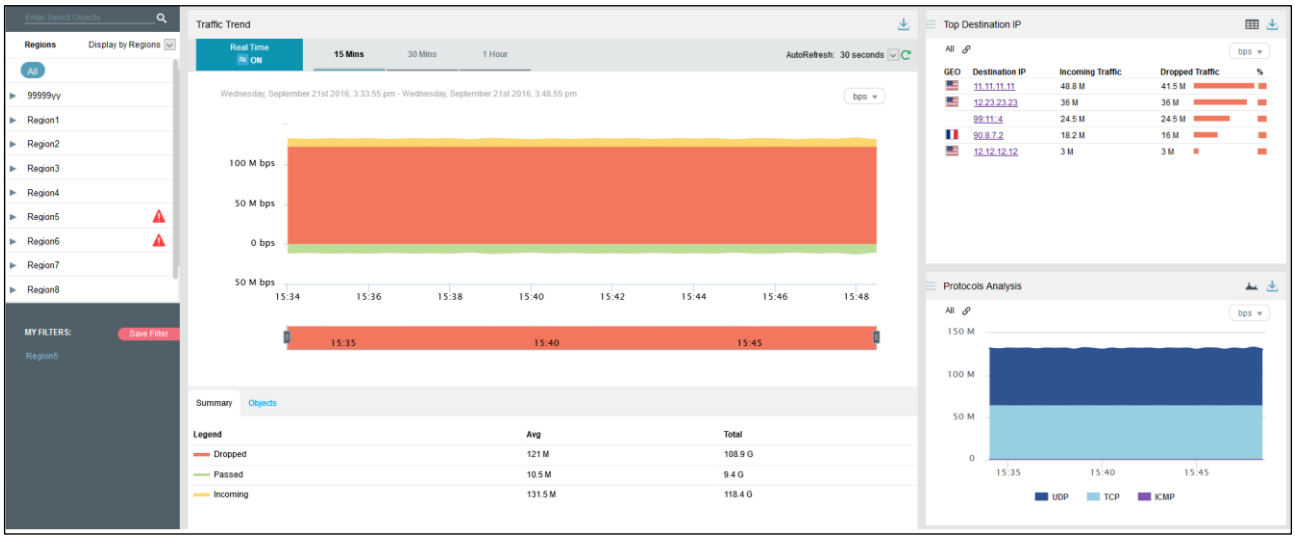
Clicking the bar or text in the **Legend** column hides or displays the corresponding traffic in the traffic trend graph. By default, all three types of traffic are displayed. A dimmed legend indicates that this type of traffic is hidden.

Table 3-5 describes parameters on the **Summary** tab page.

Table 3-5 Real-time traffic trend – Parameters on the Summary tab page

| Parameter | Description |
|---|---|
| Legend | Legends for dropped traffic, outgoing traffic, and incoming traffic. |
| Avg | Average of the dropped traffic, ongoing traffic, or incoming traffic. The traffic unit is bps or pps. |
| Total | Total value of the dropped traffic, ongoing traffic, or incoming traffic. The traffic unit is bit. |

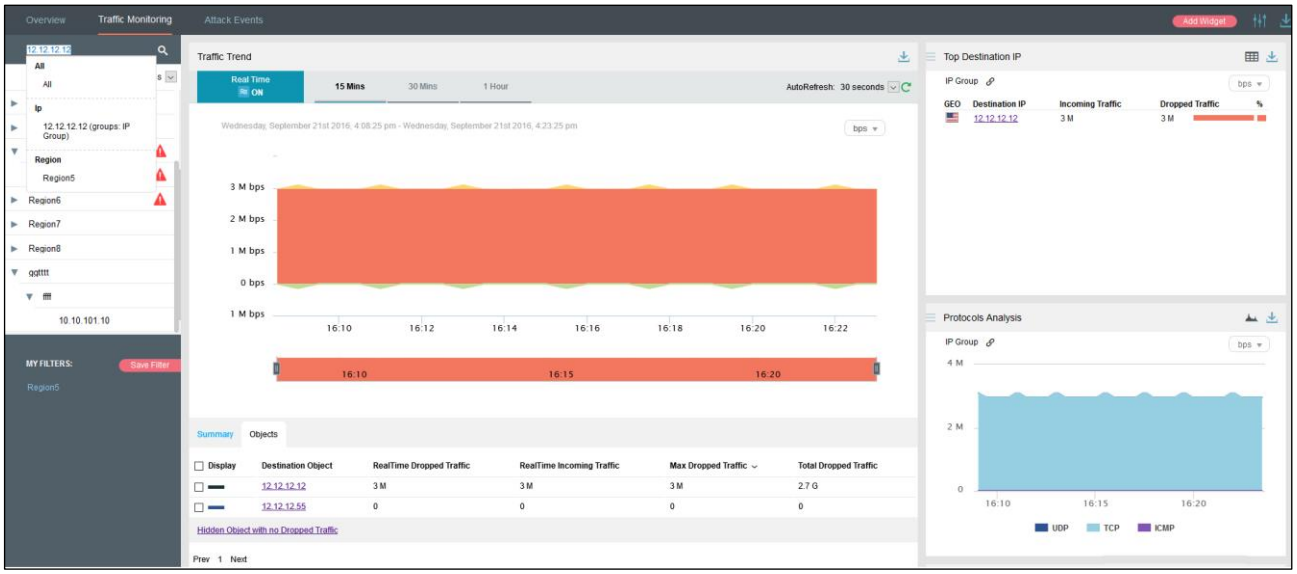
Figure 3-88 Summary of real-time traffic monitoring




**Step 8** Click an IP address in the **Destination Object** column on the **Objects** tab page.

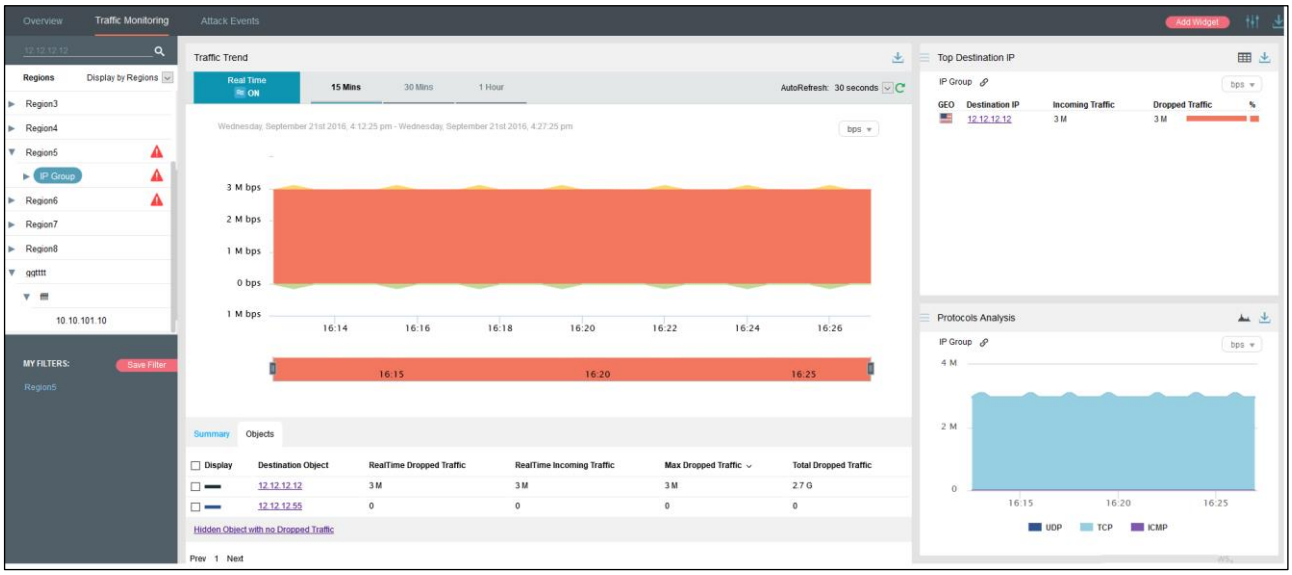
Then the search bar in the upper-right corner of the **Traffic Monitoring** page shows the region to which the IP address in question belongs.

Figure 3-89 Searching for information associated with an IP address




The **Traffic Trend**, **Top Destination IP**, and **Protocols Analysis** panels concerning the IP address are displayed, as shown in Figure 3-90.

Figure 3-90 Real-time traffic monitoring of an IP address

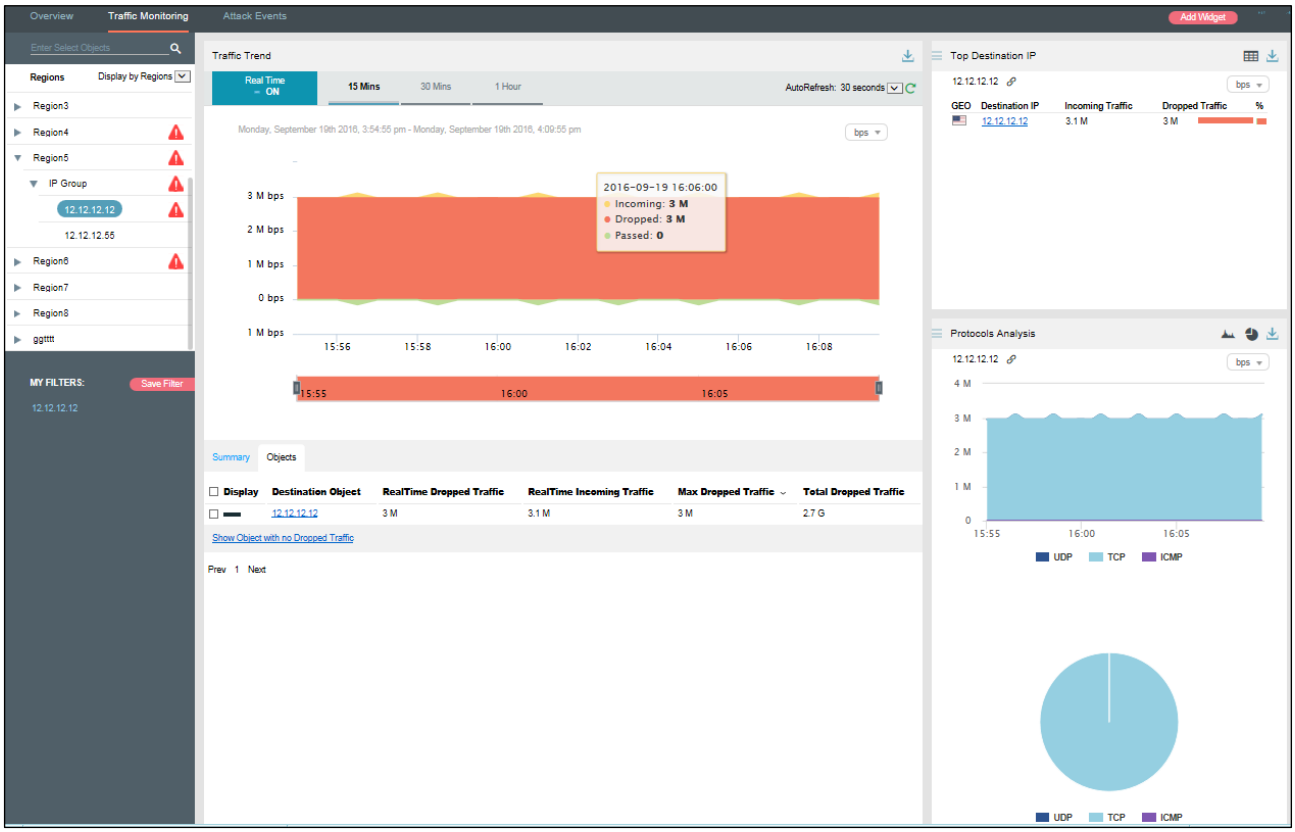



**----End**

## 3.2.2 Viewing Region-Specific Traffic Monitoring Information

On the page shown in Figure 3-82, 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 **Region5** > **IP Group** > **12.12.12.12** to view traffic monitoring information of IP address **12.12.12.12**.

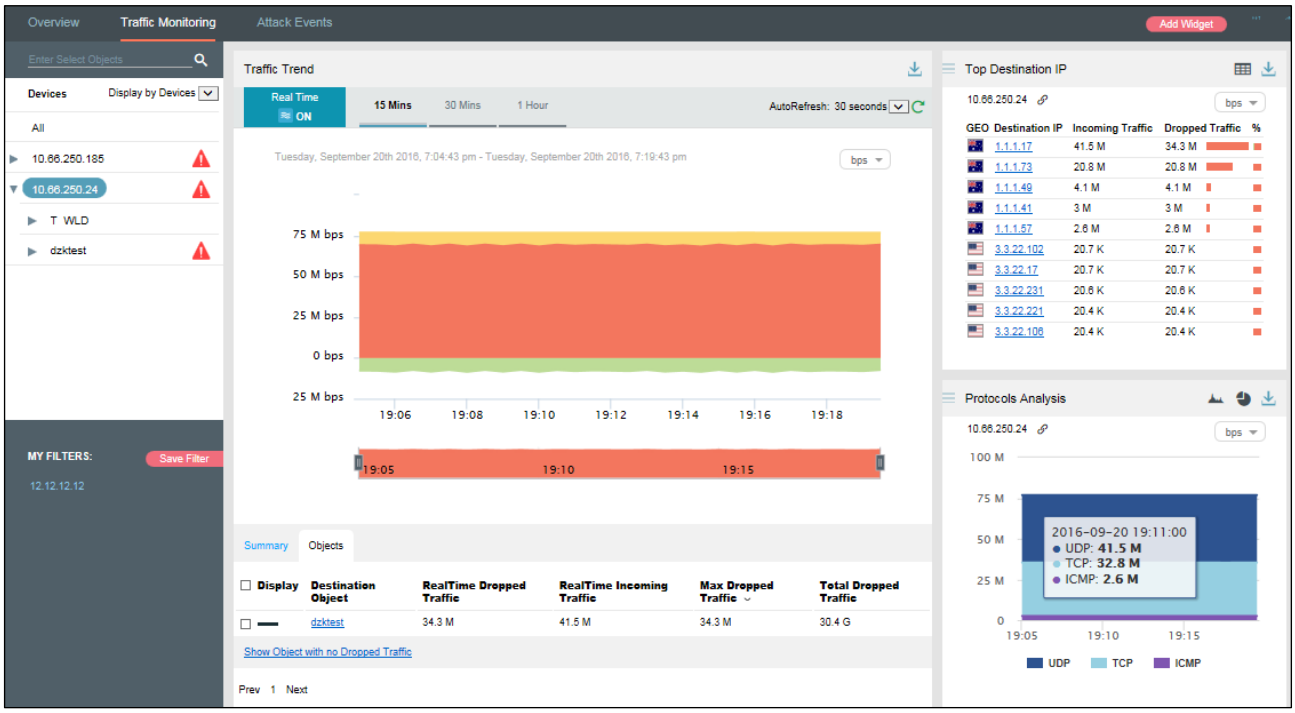
Figure 3-91 Traffic Monitoring page




## 3.2.3 Viewing Device-Specific Traffic Monitoring Information

On the page shown in Figure 3-82, you can select **Display by Devices** from the drop-down list in the left pane and then select a device to view real-time traffic monitoring information of an ADS device, ADS-protected group, and specific IP addresses under a protection group. You can view historical and real-time traffic trends and panels of a selected ADS, ADS-protected group, and IP address under a protection group. For example, you can choose **10.66.250.24 > dzktest** to view traffic monitoring information of group **dzktest** protected by device 10.66.250.45.

Figure 3-92 Device-specific traffic monitoring information



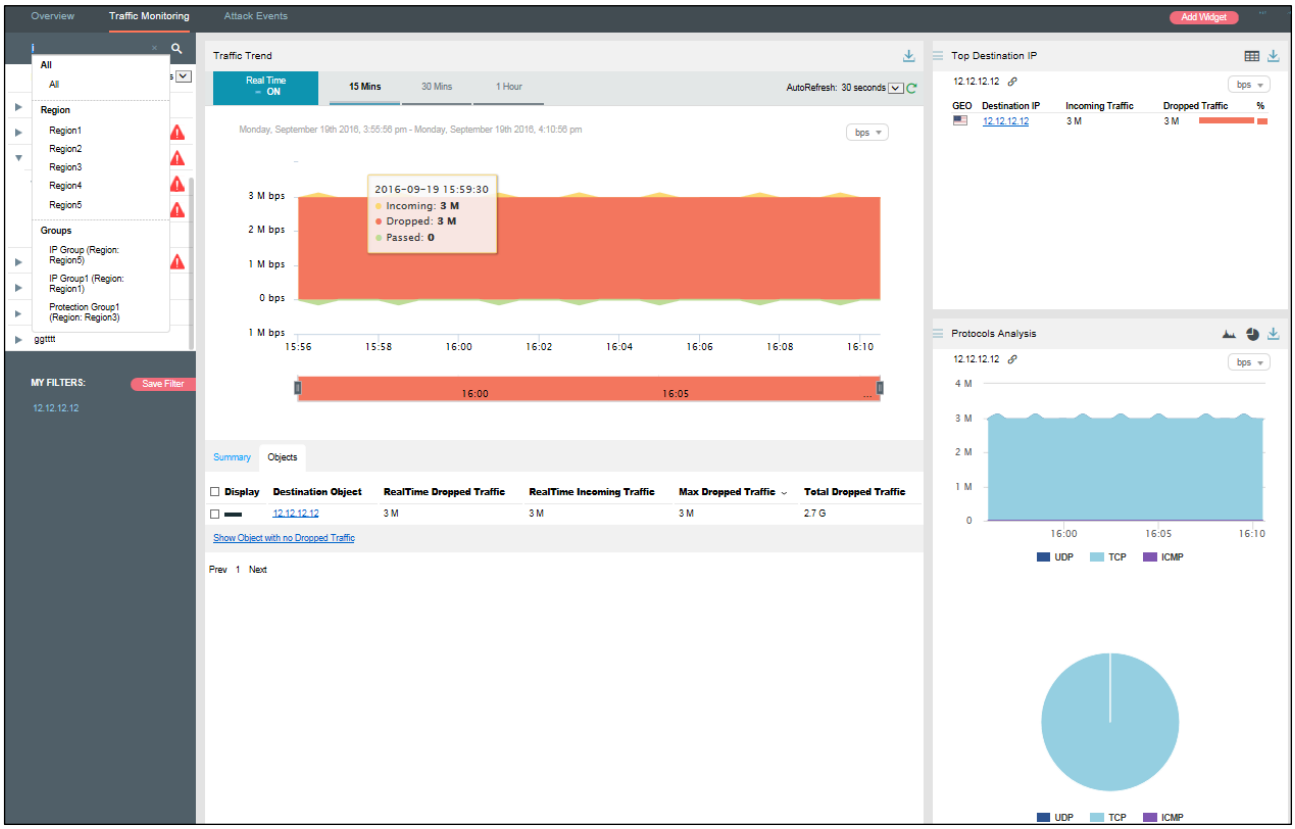

## 3.2.4 Viewing Object-Specific Traffic Monitoring Information

By default, the **Traffic Monitoring** tab page displays traffic trends of all ADS devices monitored by ADS M. You can view the real-time 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 3-82, type a character string and then press **Enter**.

The system displays all objects containing the typed character string.

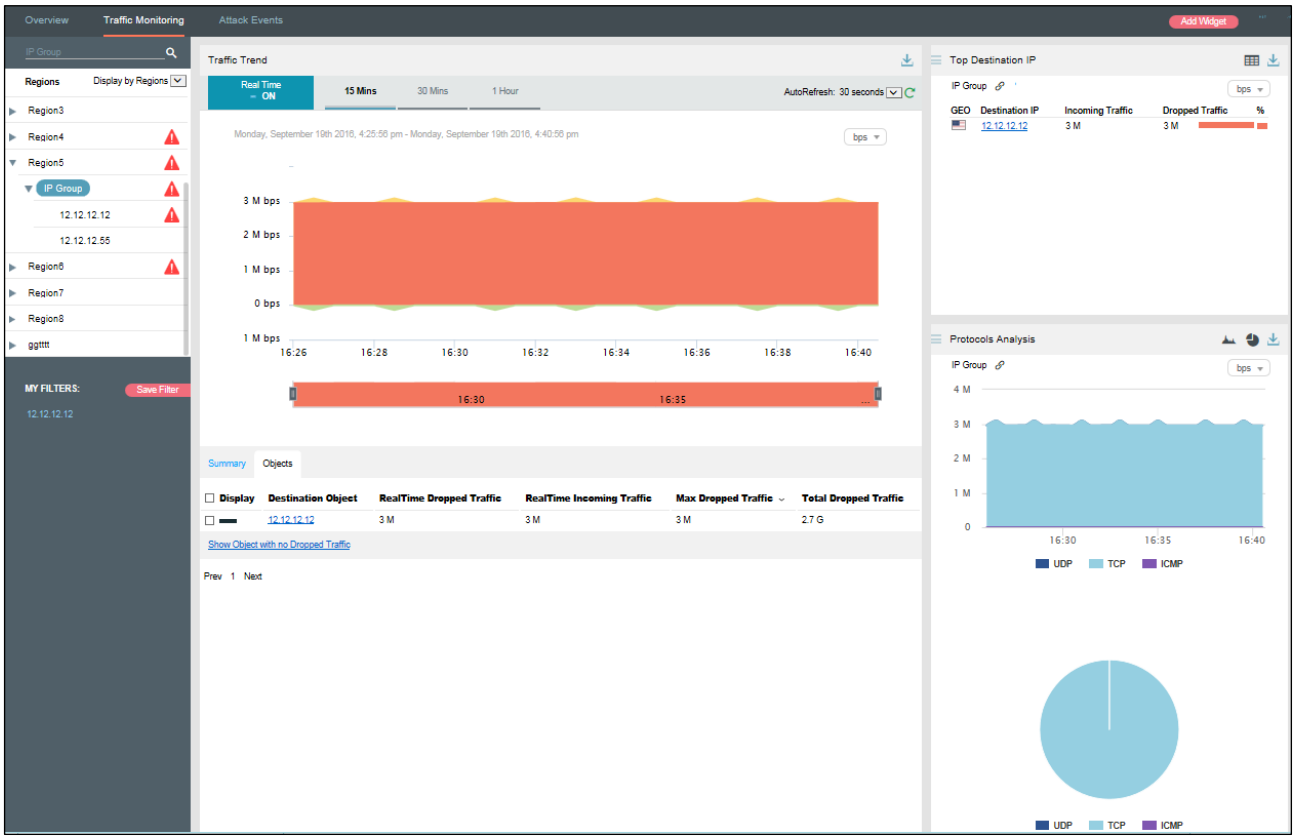
Figure 3-93 Searching for a traffic monitoring object




**Step 2** Select an object to be queried, such as **IP Group (Group: Regions)**, and then press **Enter**.

The traffic monitoring information of the selected object is displayed.

Figure 3-94 Viewing traffic monitoring information of a specified object




**----End**

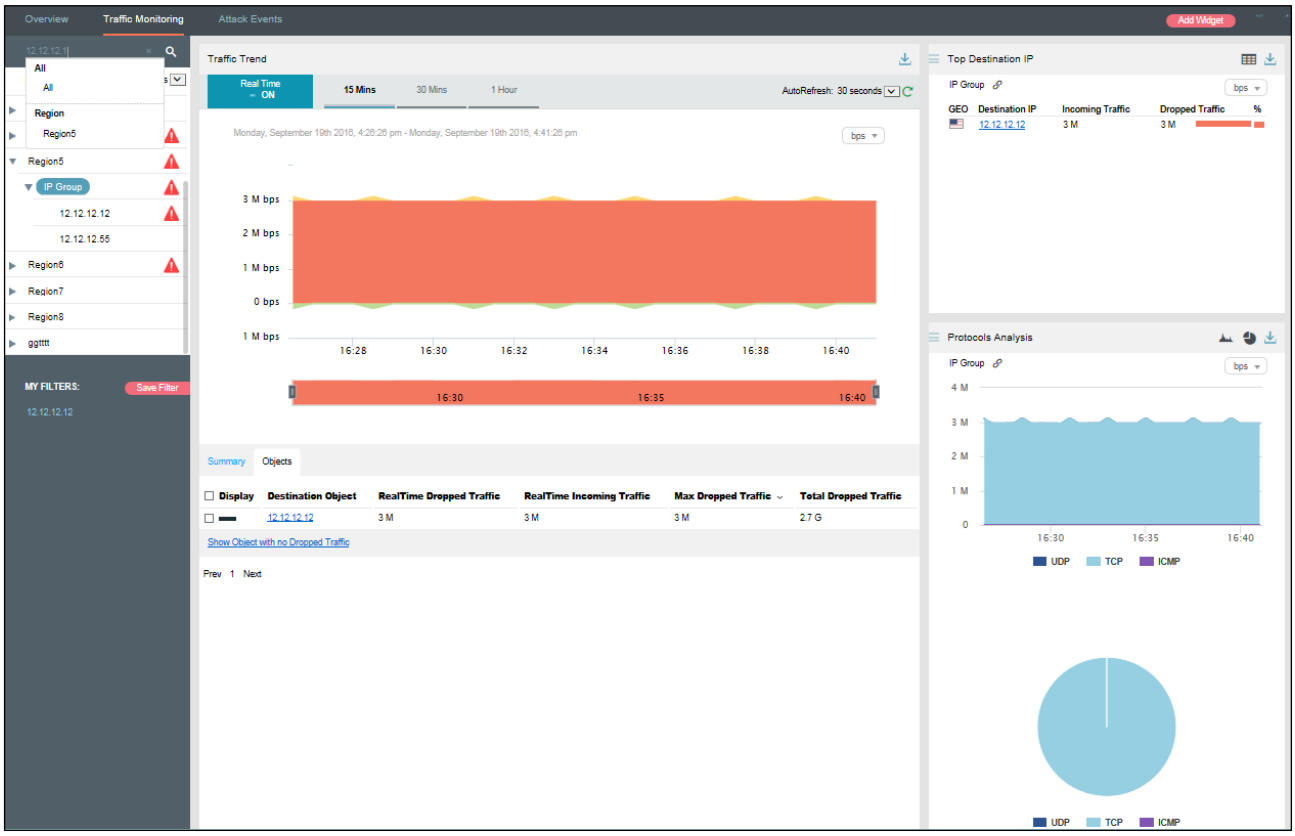
## 3.2.5 Viewing Traffic Monitoring Information of an IP Address in the Default Protection Group

IP addresses under the default protection group do not belong to any regions or ADS-protected groups. To view traffic 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 3-82, type an IP address (such as 12.12.12.12) and then press **Enter**.

The system displays all objects containing this IP address.

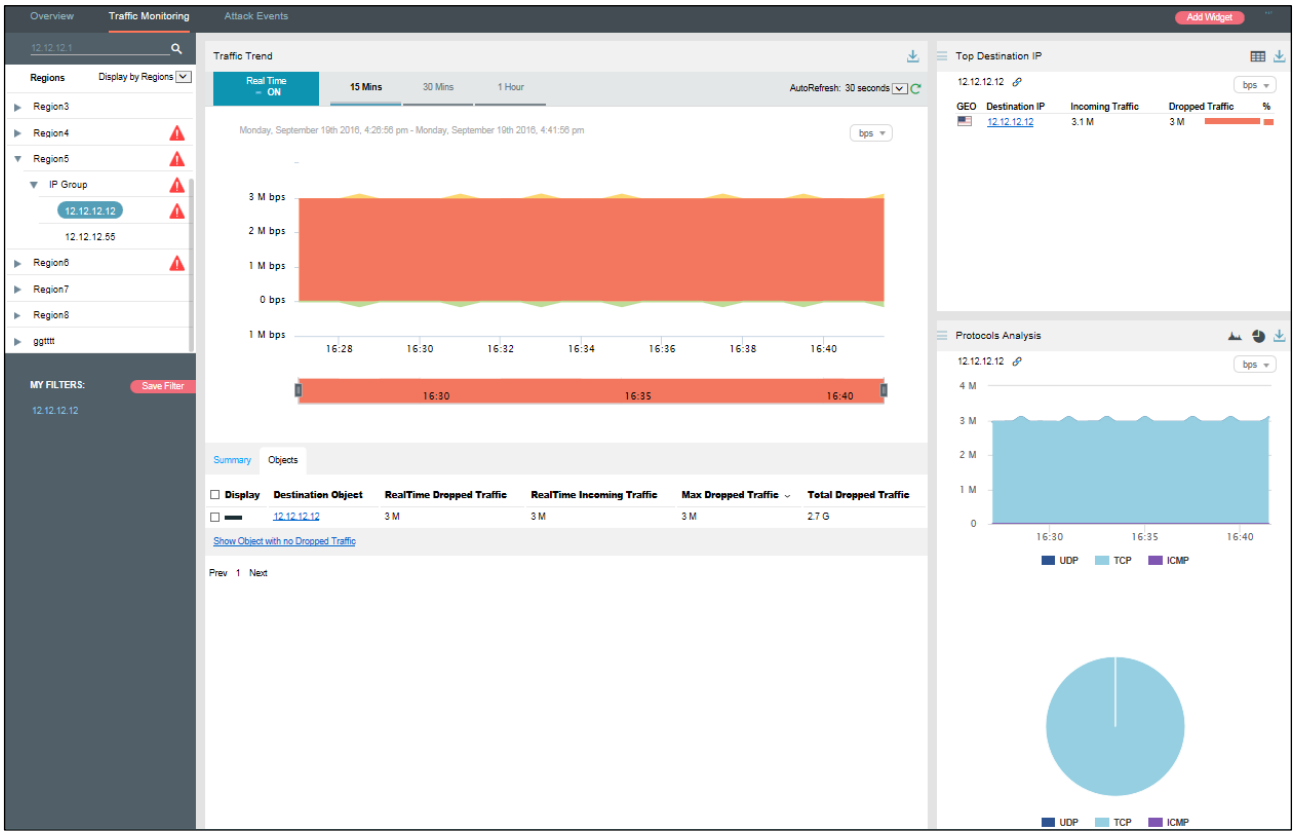
Figure 3-95 Searching for a traffic monitoring object




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

The traffic monitoring information of this IP address is displayed.

Figure 3-96 Traffic monitoring information of an IP address in the default protection group




**----End**

## 3.2.6 Viewing Historical Traffic Trends

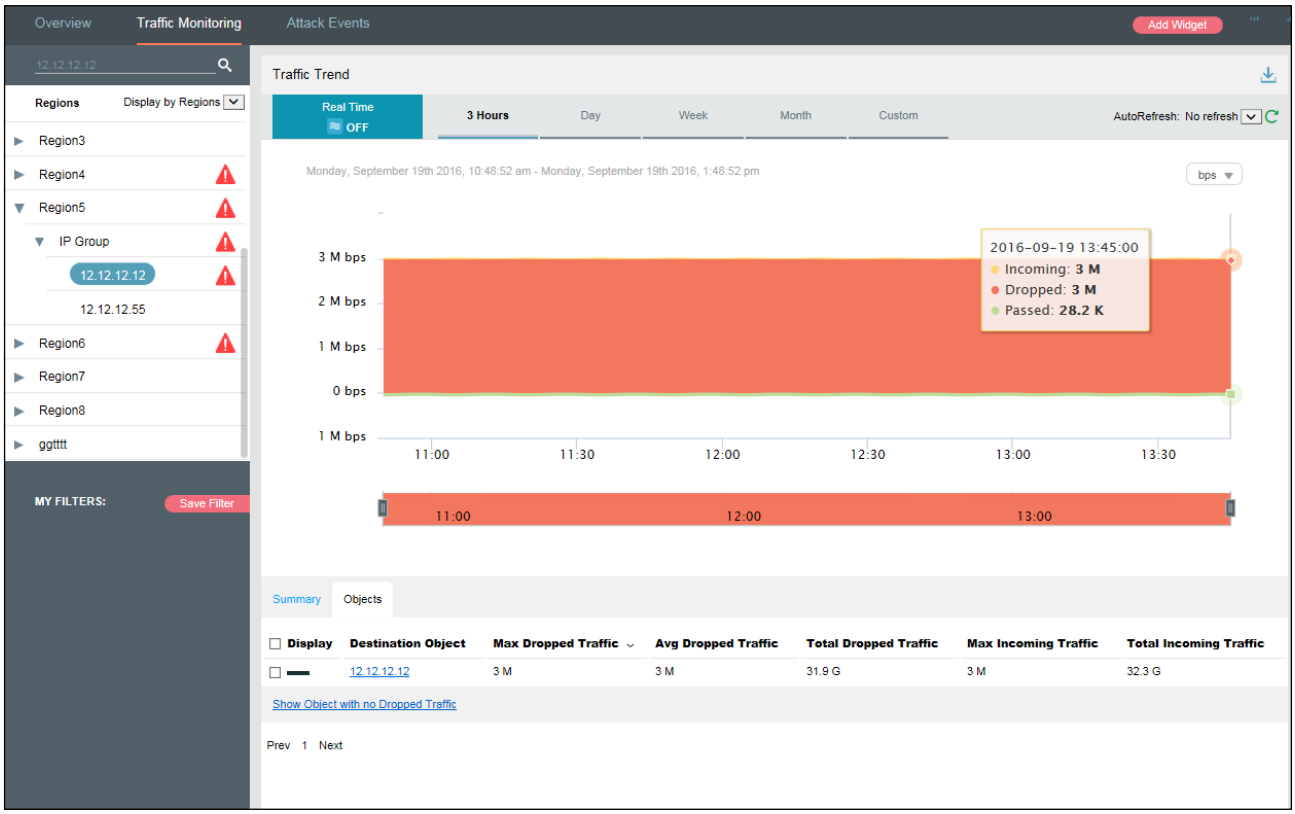
To view historical traffic trends, follow these steps:

**Step 1** On the page shown in Figure 3-82, clicking **ON** for **Real Time** in the **Traffic Trend** 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, traffic trend graphs and panels with the icon display historical data

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

Figure 3-97 Historical traffic trend graph – object




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

Table 3-6 Historical traffic trend – parameters in the object list

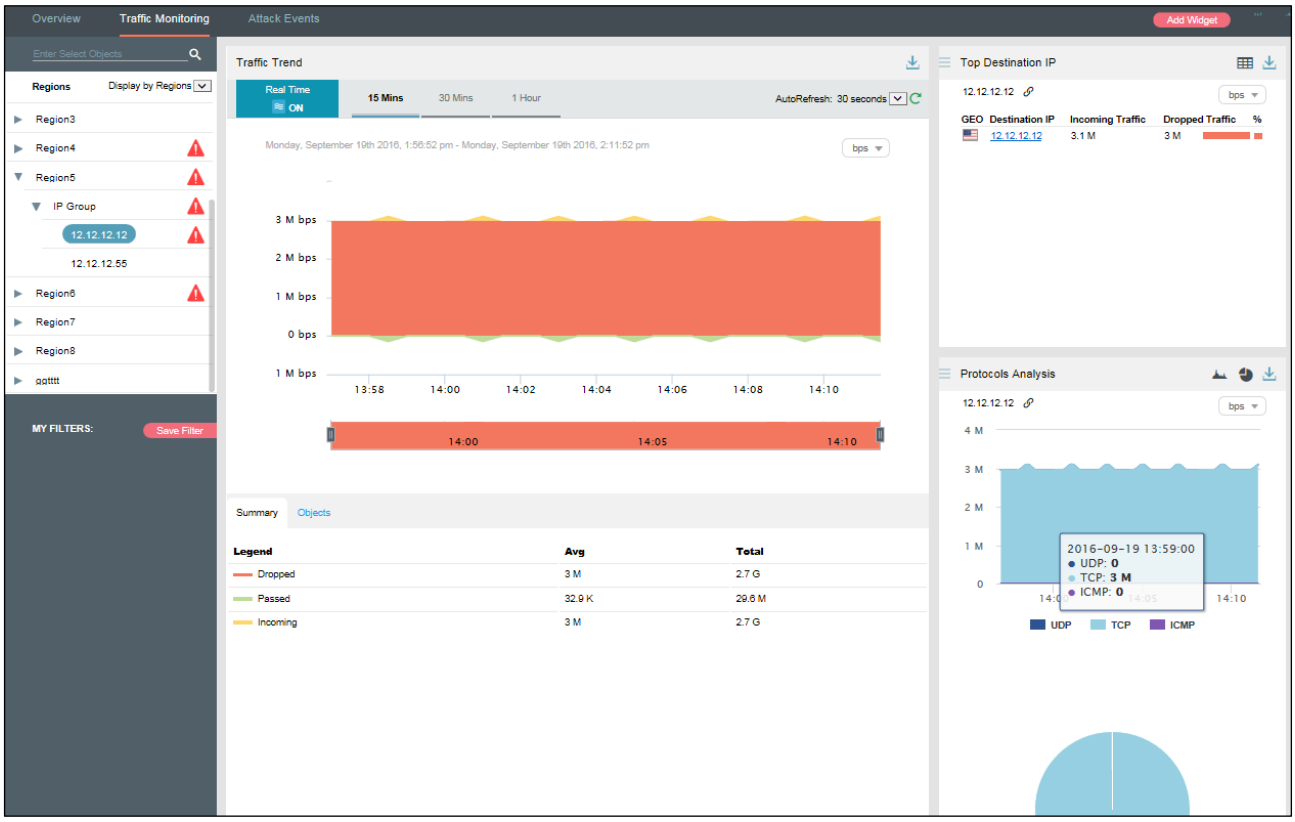
| Parameter | Description |
|---|---|
| Display | Indicates the volume of dropped traffic with a color that shades from dark blue to light blue. |
| Destination Object | Indicates the traffic monitoring object. |
| Max Dropped Traffic | Indicates the maximum traffic dropped by ADS for the object in the statistical period. The traffic unit is bps or pps. |
| Avg Dropped Traffic | Indicates the average traffic dropped by ADS for the object in the statistical period. The traffic unit is bps or pps. |
| Total Dropped Traffic | Indicates the total traffic dropped by ADS for the object in the statistical period. The traffic unit is bit. |
| Max Incoming Traffic | Indicates the maximum traffic received by ADS for the object in the statistical period. The traffic unit is bps or pps. |
| Total Incoming Traffic | Indicates the total traffic received by ADS for the object in the statistical period. The unit is bit. |

**Step 2** On the page shown in Figure 3-97, click **Summary**.

The summary of the historical 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 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.

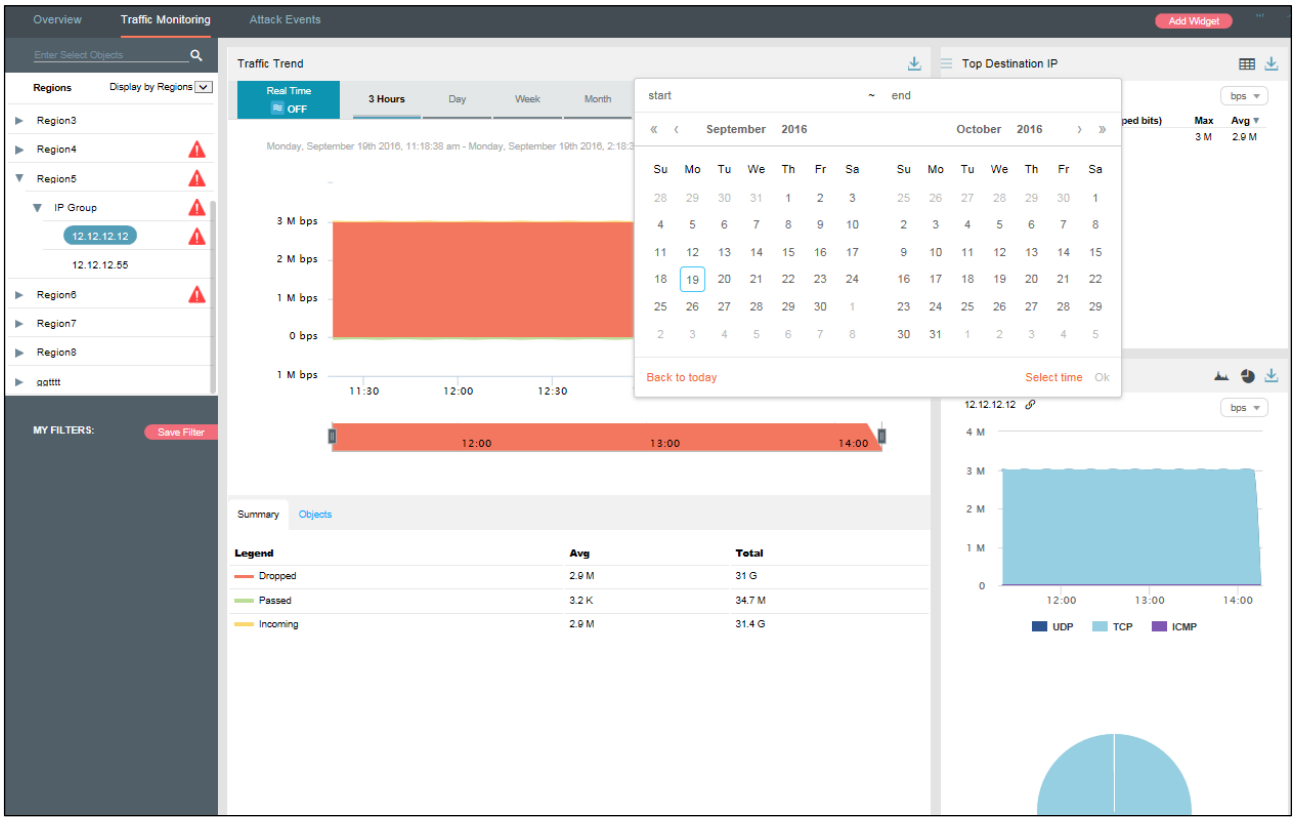
Figure 3-98 Historical traffic trend graph – overview




**Step 3** On the page shown in Figure 3-97**, click Custom.**

You can select the start time and end time of the traffic trend graph as required. The unit is the day.

Figure 3-99 Custom traffic trend graph




**----End**

## 3.2.7 Switching the Traffic Unit

By default, traffic is expressed in bps in the traffic trend graph. On the page shown in Figure 3-82, you can select **pps** from the drop-down list in the upper-right corner of the **Traffic Trend** panel to display traffic data in pps.

## 3.2.8 Refreshing the Traffic Trend Graph

By default, the traffic trend graph automatically refreshes every 30 seconds in real time mode. On the page shown in Figure 3-82, you can select **Not fresh** from the **AutoFresh** drop-down list in the upper-right corner of the **Traffic Trend** panel. In this case, the traffic trend graph can be refreshed only by clicking .

By default, the traffic trend graph does not automatically refresh in historical mode. On the page shown in Figure 3-82, you can select **5 minute** from the **AutoFresh** drop-down list in the upper-right corner of the **Traffic Trend** panel. In this case, the traffic trend graph will refresh every 5 minutes.

## 3.2.9 Downloading a Traffic Trend Report

On the page shown in Figure 3-82, you can click in the upper-right corner to export the current data of the traffic trend graph as a report. For details, see 3.1.5 Downloading a Report.

## 3.2.10 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 monitoring information of the object specified by the filter.

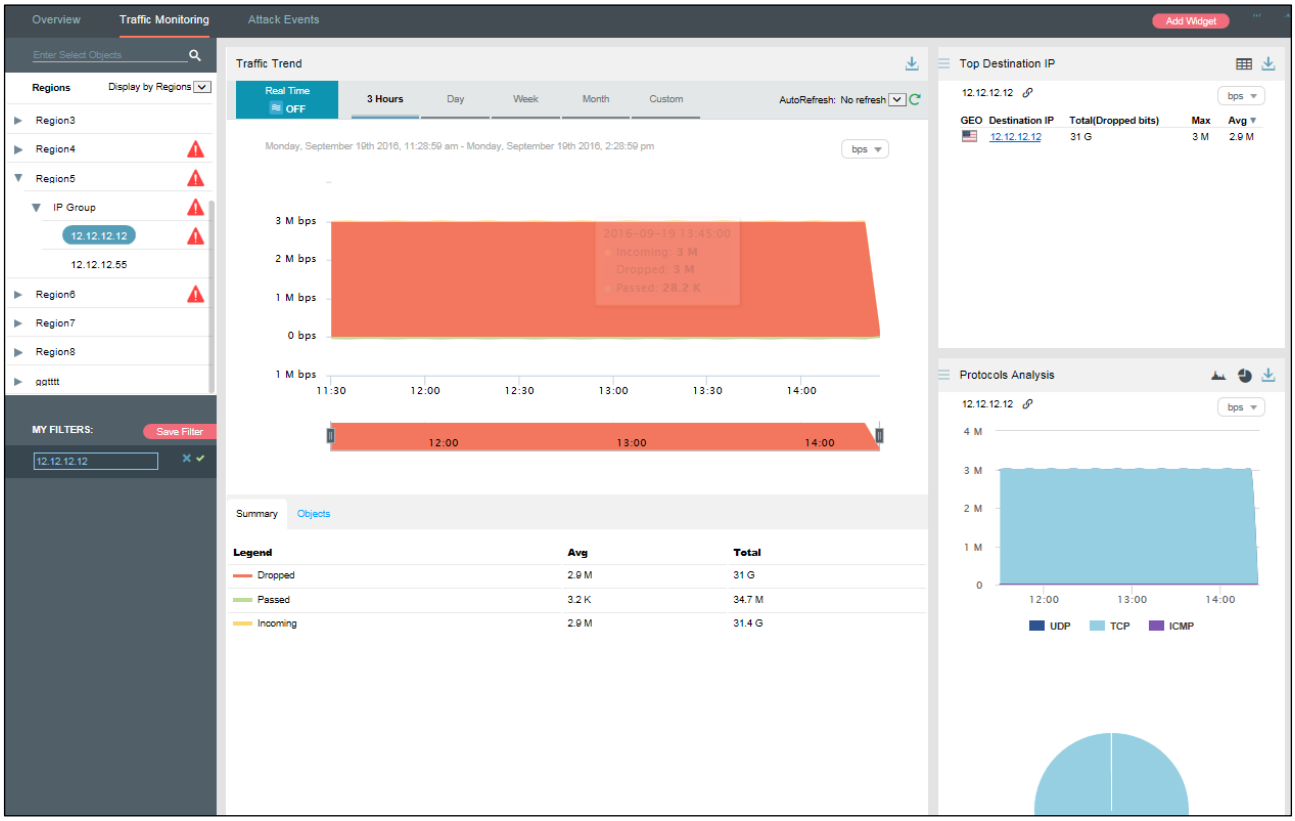
Any queried objects, such as a region, region IP group, ADS device, ADS-protected group, or IP address can be configured as a filter. But **All** and **Default IP (Default)** cannot be configured as a filter. You can configure multiple filters.

### 3.2.10.1 Configuring a Filter

To configure a filter, follow these steps:

**Step 1** On the page shown in Figure 3-82, select an object from the left pane, such as 12.12.12.12, and then click **Save Filter**.

Figure 3-100 Adding a filter



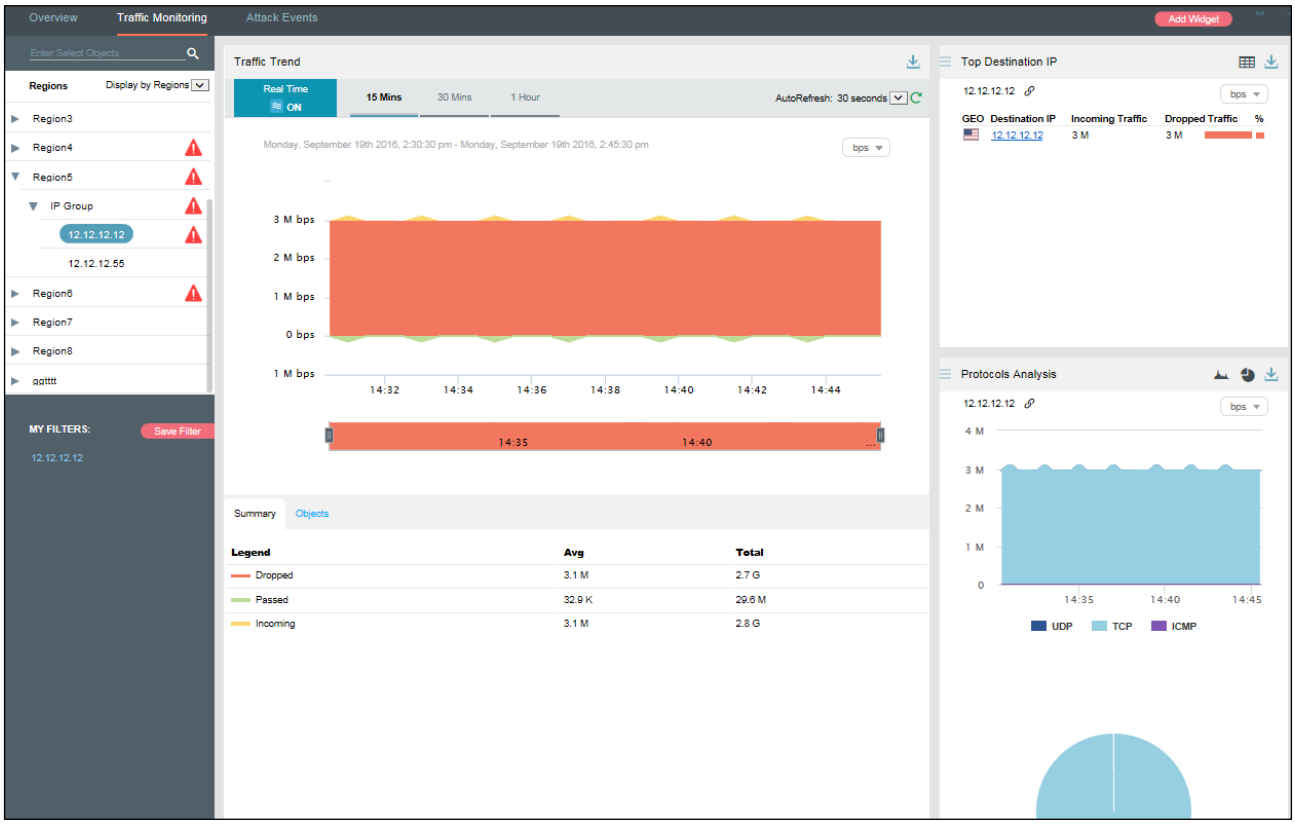

**Step 2** Type the filter name.

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 **12.12.12.12** in the filter list to view its traffic information.

Figure 3-101 Viewing a filter




**----End**

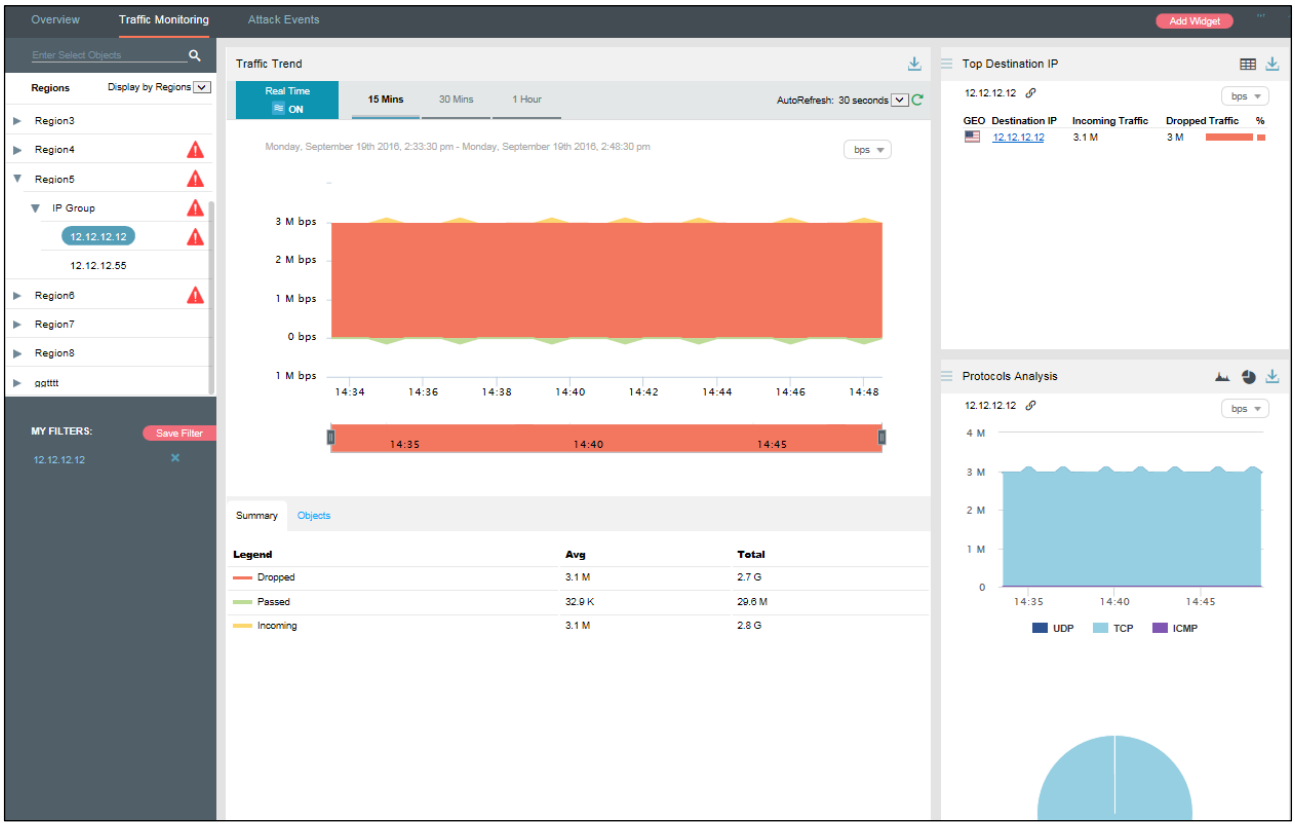
## 3.2.10.2 Deleting a Filter

To delete a filter, follow these steps:

**Step 1** On the page shown in Figure 3-101, point to a filter name

The icon  appears.

Figure 3-102 Deleting a filter




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

Then this filter is deleted.

**----End**

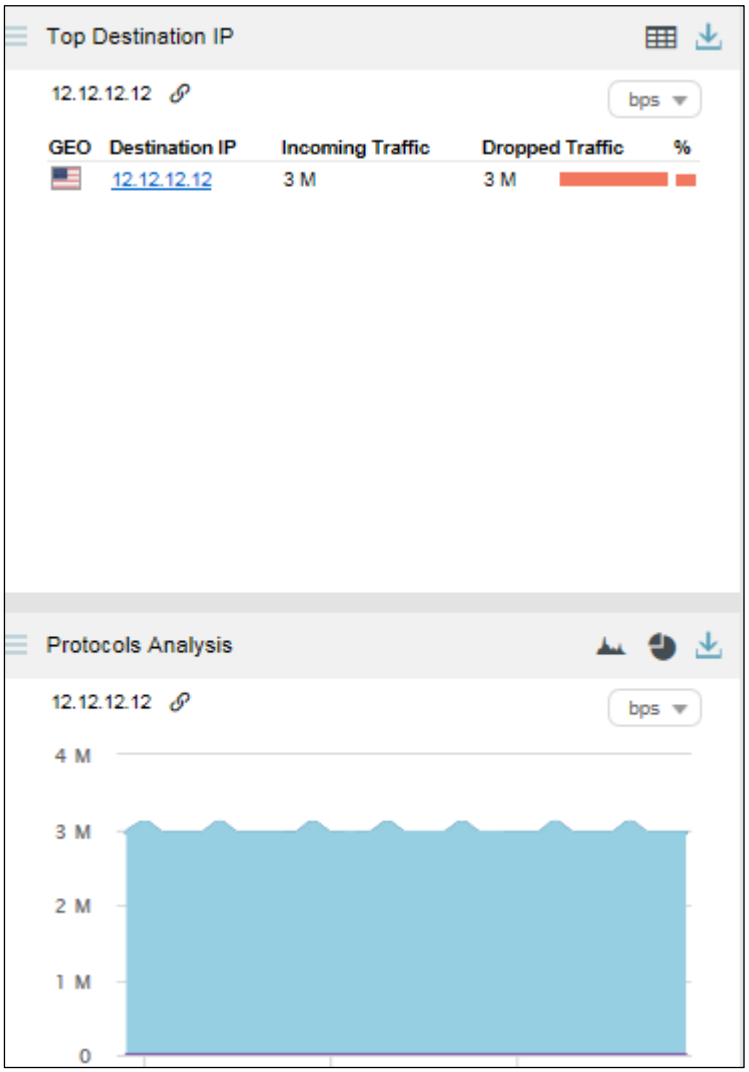
## 3.2.11 Managing Panels

By default, **Top Destination IP** and **Protocols Analysis** panels are displayed under **Traffic monitoring** > **Traffic Monitoring**, as shown in Figure 3-103.

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 3.1 Overview.

Figure 3-103 Default panels on the Traffic Monitoring page




## 3.3 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.

### 3.3.1 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.

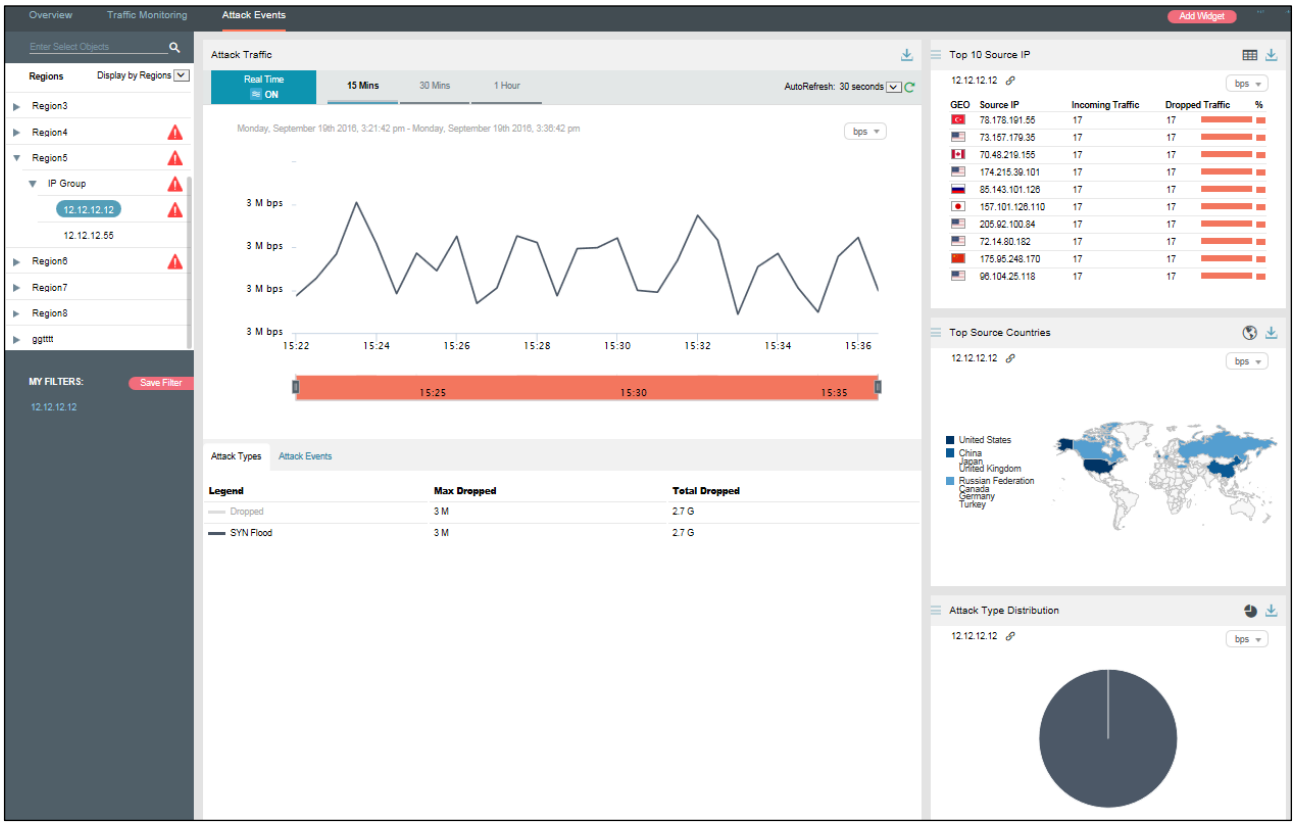
In the **Attack Types** panel, attack type names and information of dropped traffic are displayed.

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 3-7 Attack type parameters

| Parameter | Description |
|---|---|
| Legend | Indicates the volume of attack traffic with a color that shades from dark blue to light blue. |
| Max Dropped | Indicates the maximum traffic dropped by ADS for the object in the statistical period. The traffic unit is bps or pps. |
| Total Dropped | Indicates the total traffic dropped by ADS for the object in the statistical period. The traffic unit is bit. |

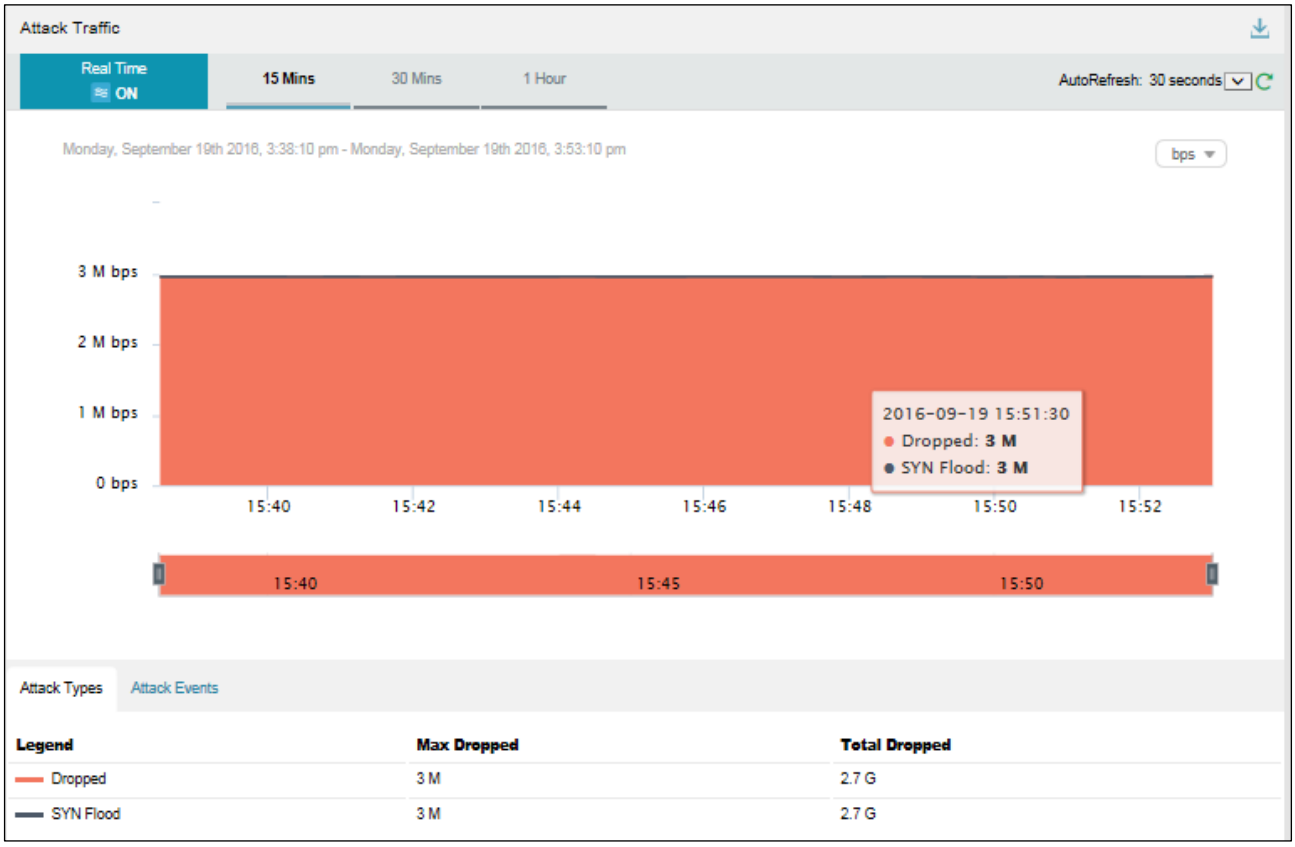
Figure 3-104 Attack Events page – Attack Types panel




**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.

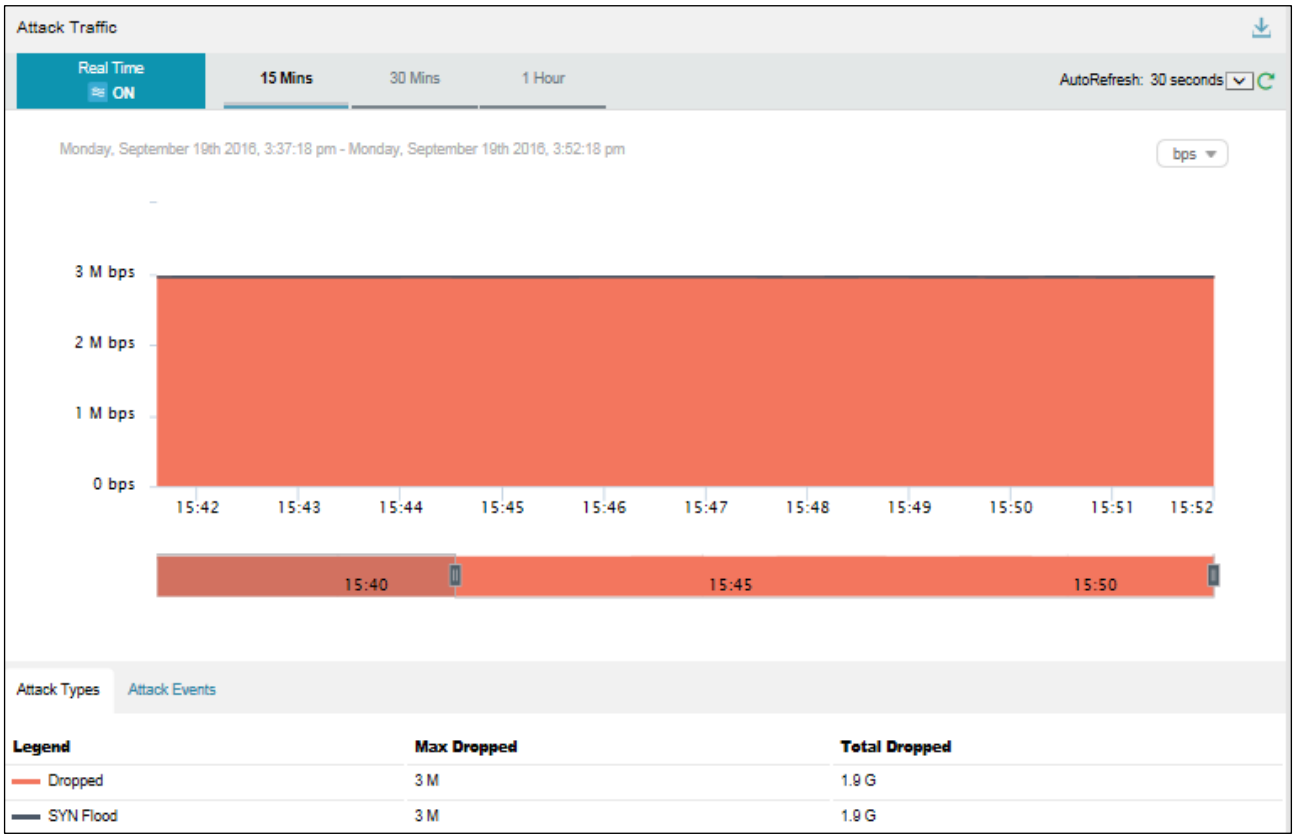
Figure 3-105 Attack traffic monitoring information of a specific time




**Step 3** Below the attack traffic trend graph, drag .

A finer-granularity traffic trend is displayed.

Figure 3-106 Finer-granularity traffic monitoring information




**Step 4** On the page shown in Figure 3-104, click **Attack Events** below the attack traffic trend graph.

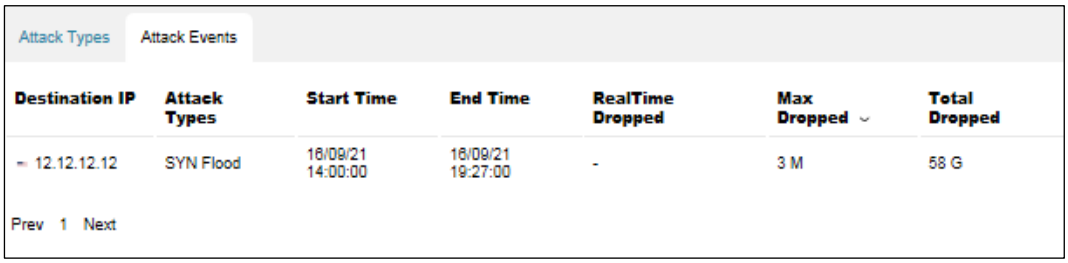
The ongoing attack events and their details are displayed.

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

Table 3-8 Attack event parameters

| Parameter | Description |
|---|---|
| Destination IP | Indicates 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 dropped by ADS for the object. The traffic unit is bps or pps. |
| Max Dropped | Indicates the maximum traffic dropped by ADS for the object. The traffic unit is bps or pps. |
| Total Dropped | Indicates the total traffic dropped by ADS for the object. The traffic unit is bit. |

Figure 3-107 Attack traffic – attack events

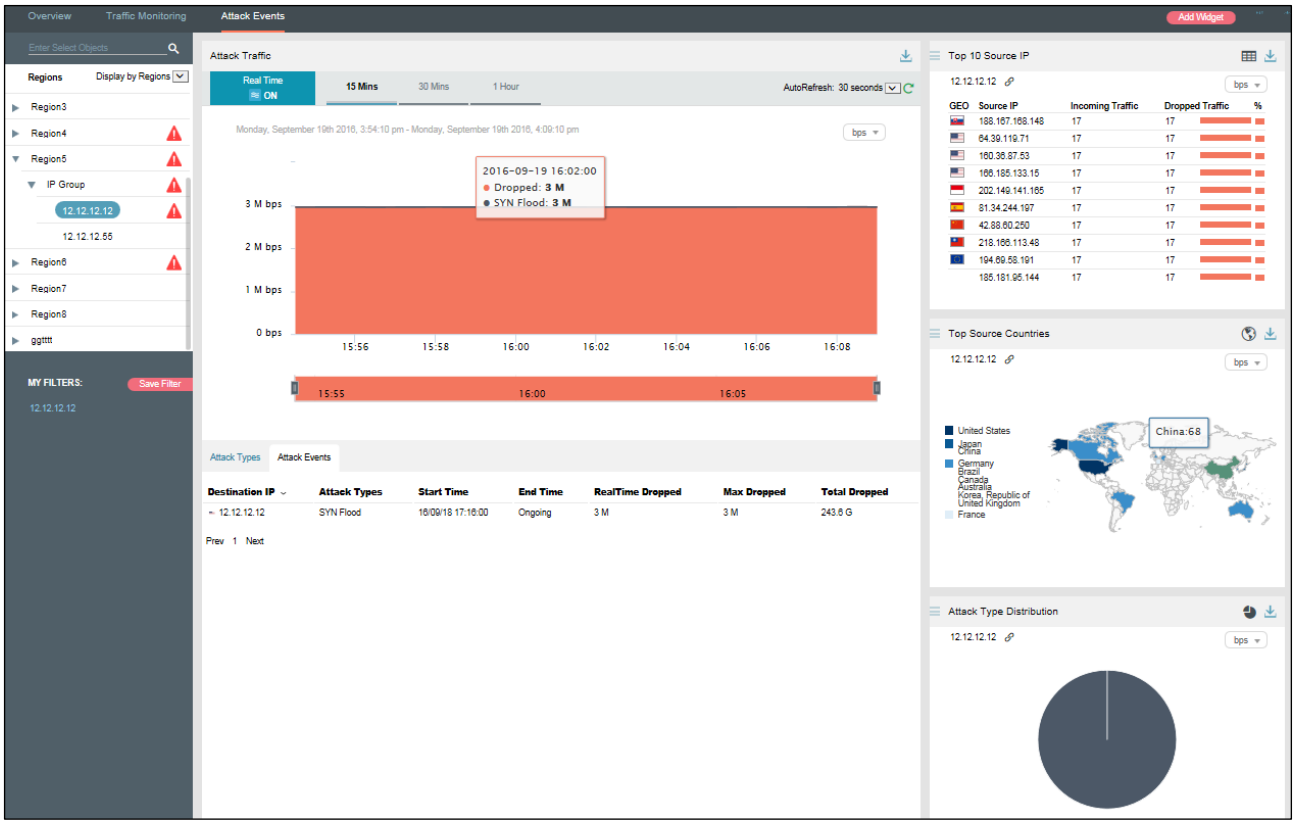



**----End**

## 3.3.2 Viewing Region-Specific Attack Events

On the page shown in Figure 3-104, 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 **Region5 > IP Group > 12.12.12.12**, you can view attack events of IP address 12.12.12.12.

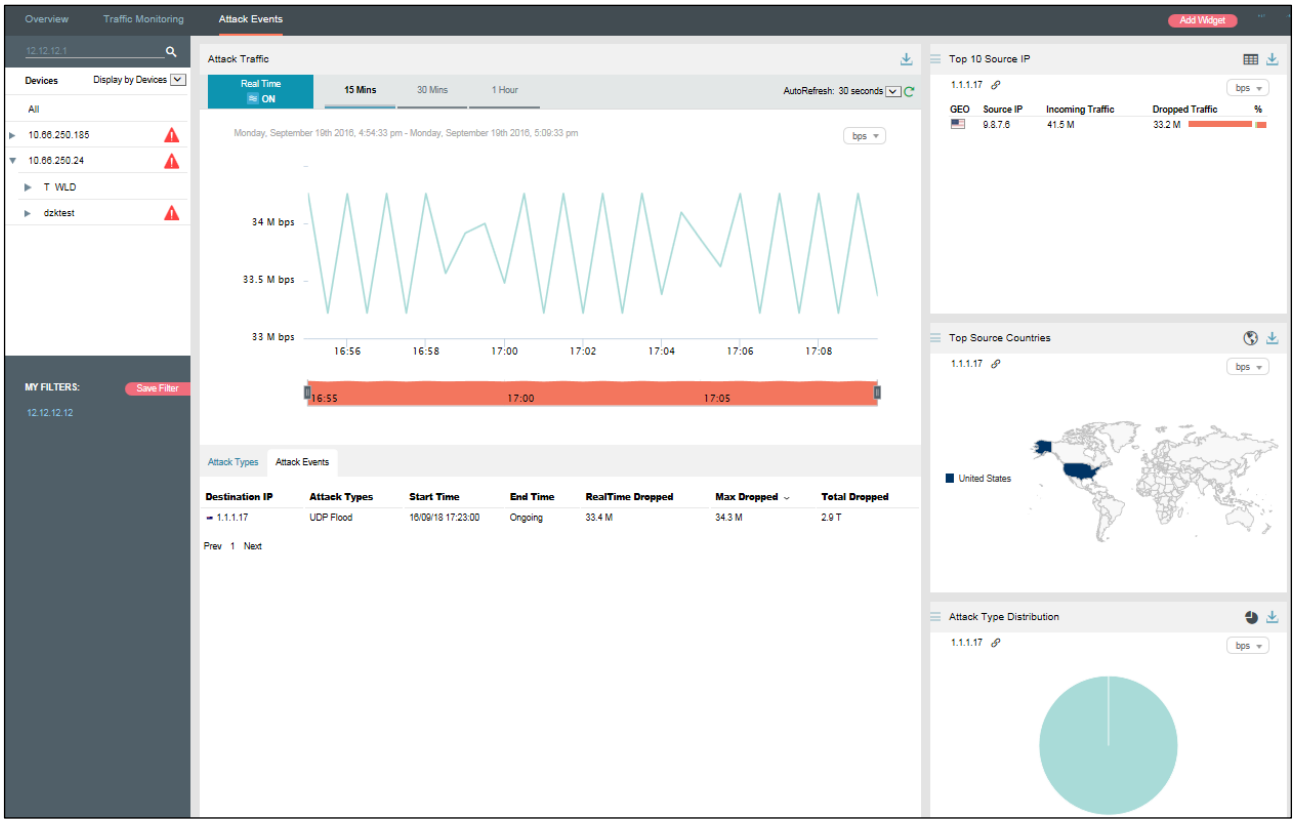
Figure 3-108 Region-specific attack events



## 3.3.3 Viewing Device-Specific Attack Events

On the page shown in Figure 3-104, 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 **10.66.250.24** > **dzktest** to view attack event information of group **dzktest** under device 10.66.250.45.

Figure 3-109 Device-specific attack events



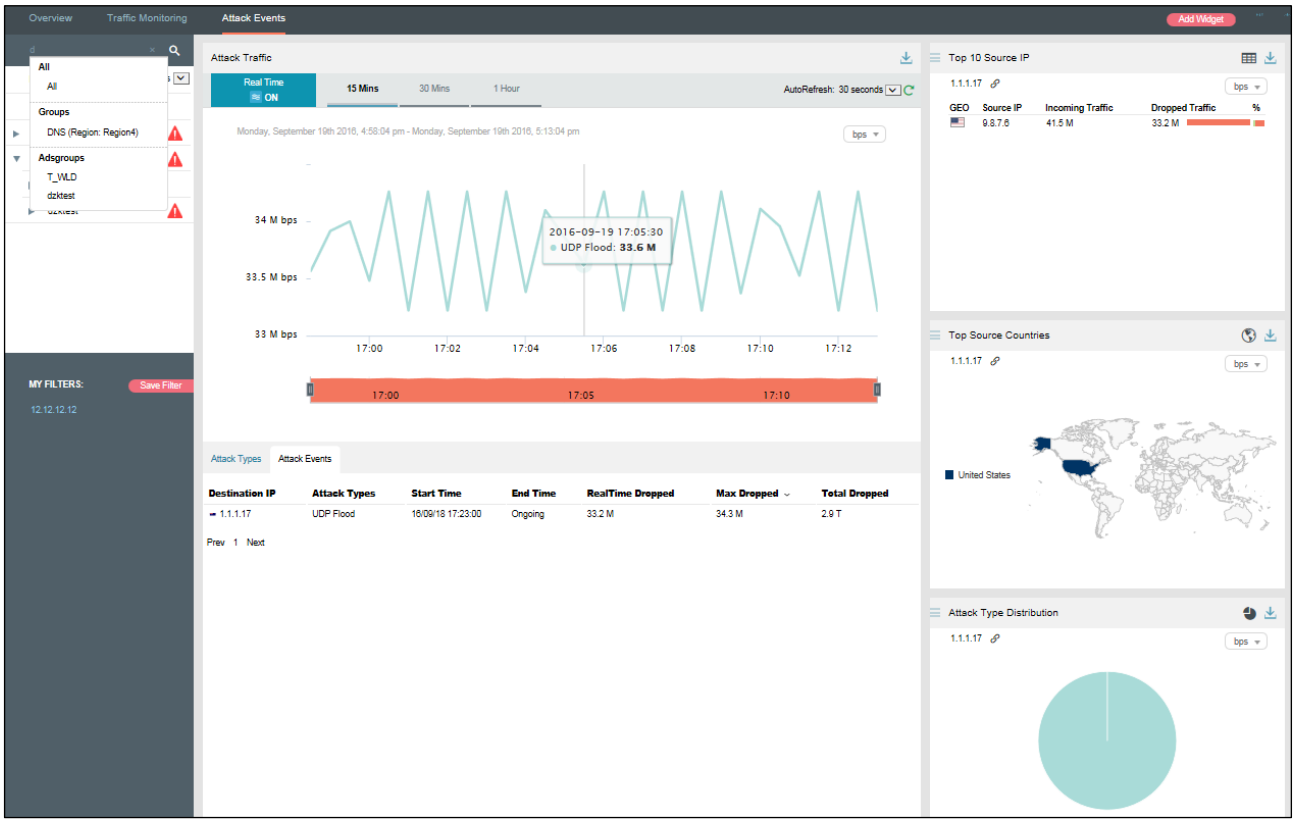

## 3.3.4 Viewing Object-Specific Attack Events

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, region IP group, ADS device, ADS-protected group, or IP address.

**Step 1** On the page shown in Figure 3-104, type a character string and then press **Enter**.

The system displays all objects containing the typed character string.

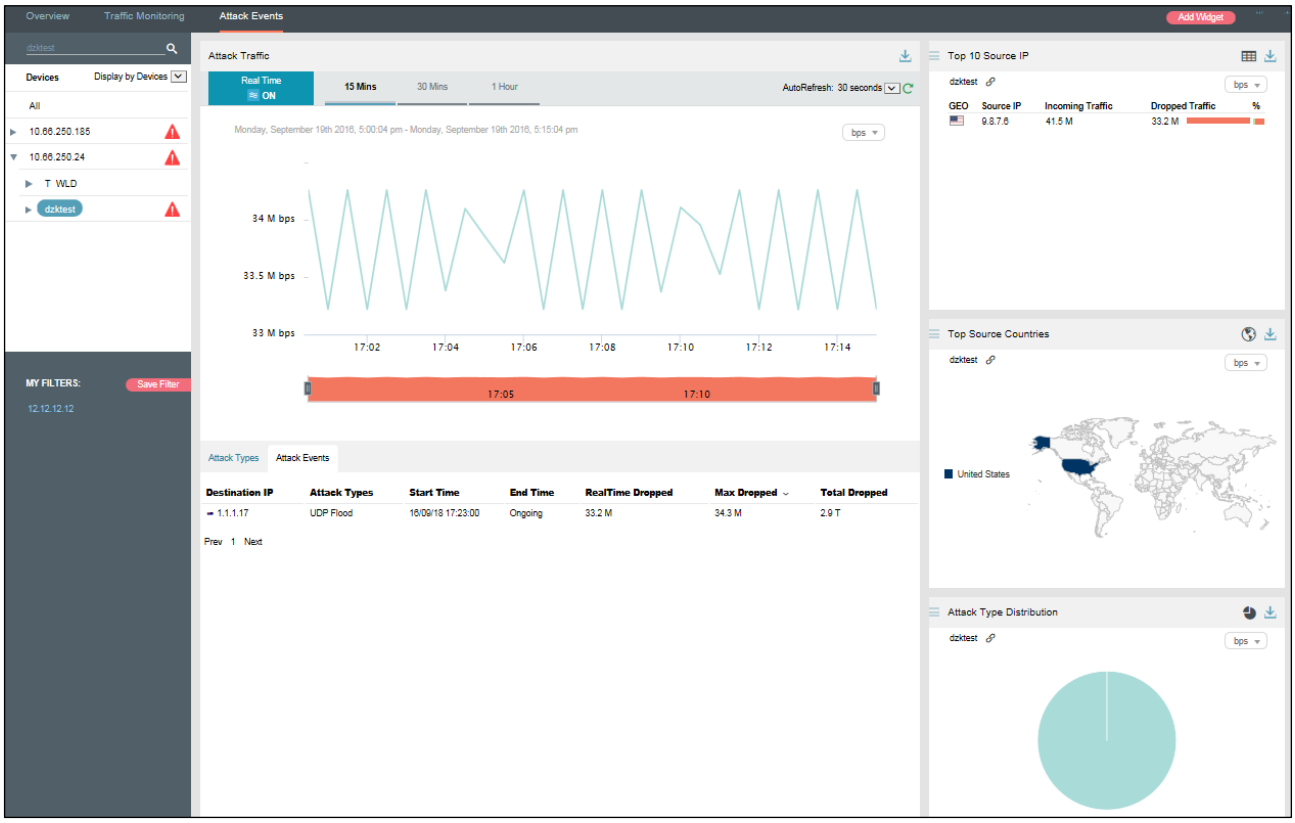
Figure 3-110 Searching for attack event objects




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

Traffic monitoring information of the selected object is displayed.

Figure 3-111 Object-specific attack event information




**----End**

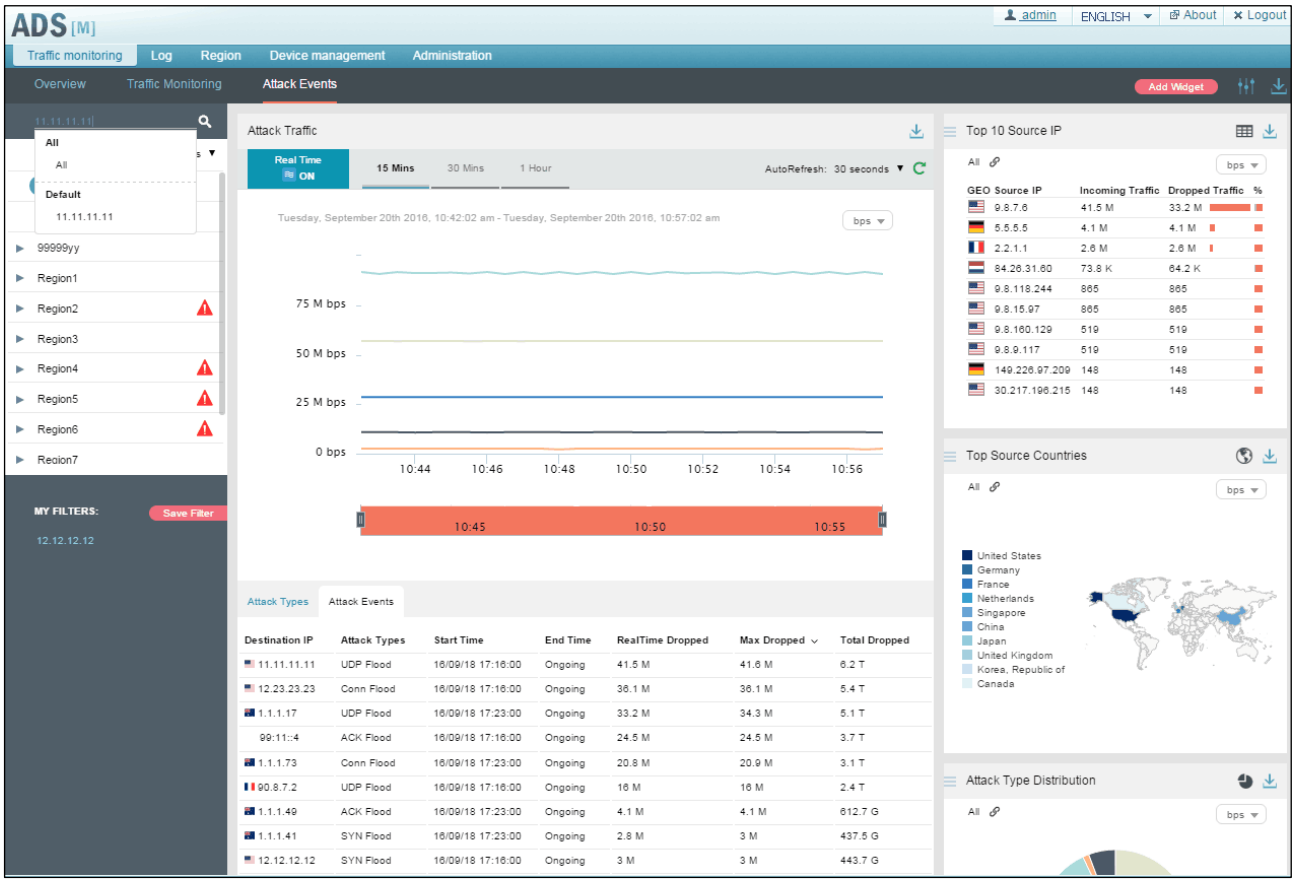
## 3.3.5 Viewing Attack Event Information of an IP Address in the Default Protection Group

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 3-104, type an IP address (such as 11.11.11.11) and then press **Enter**.

The system displays all objects containing this IP address.

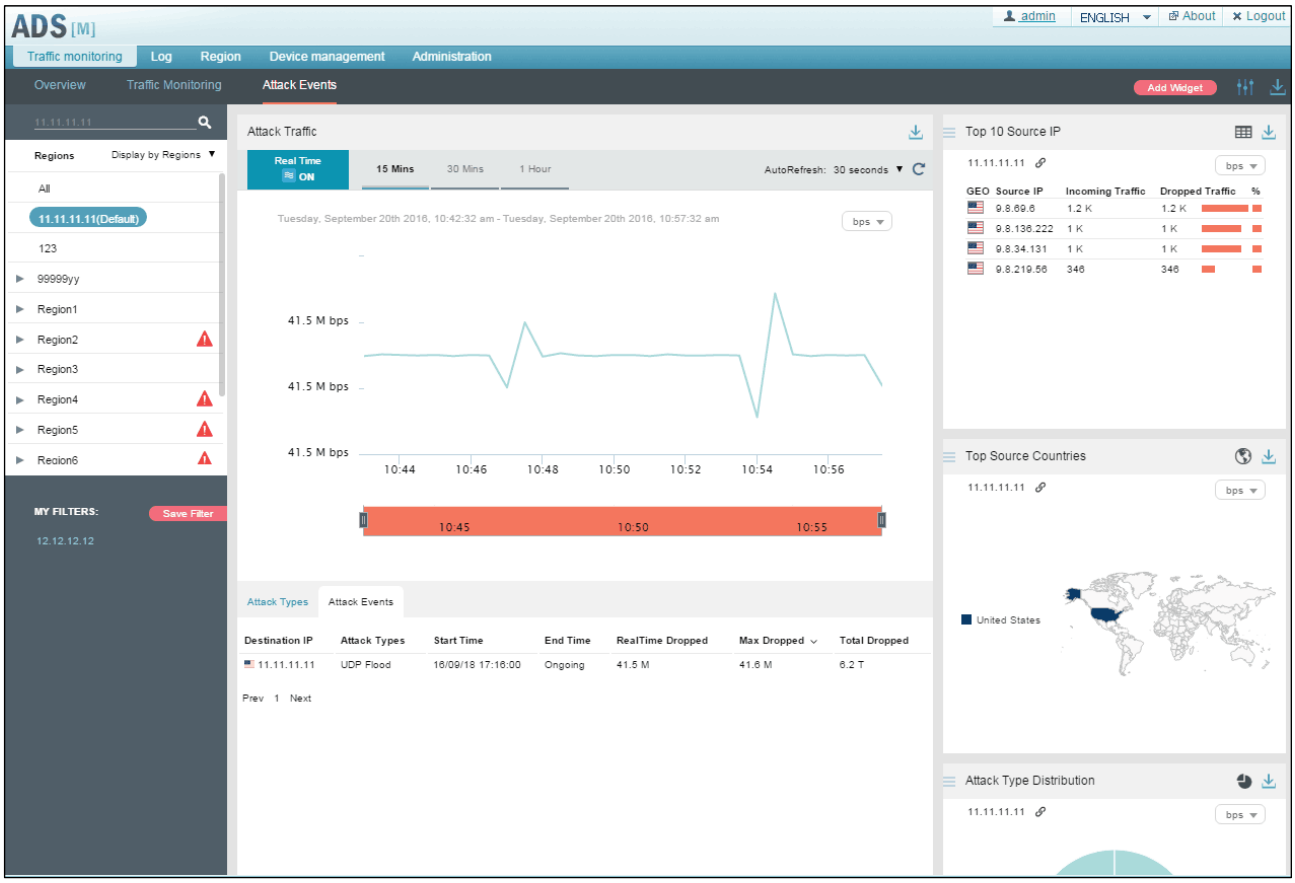
Figure 3-112 Searching for attack event objects




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

Traffic monitoring information of this IP address is displayed.

Figure 3-113 Attack event information of an IP address in the default protection group




**----End**

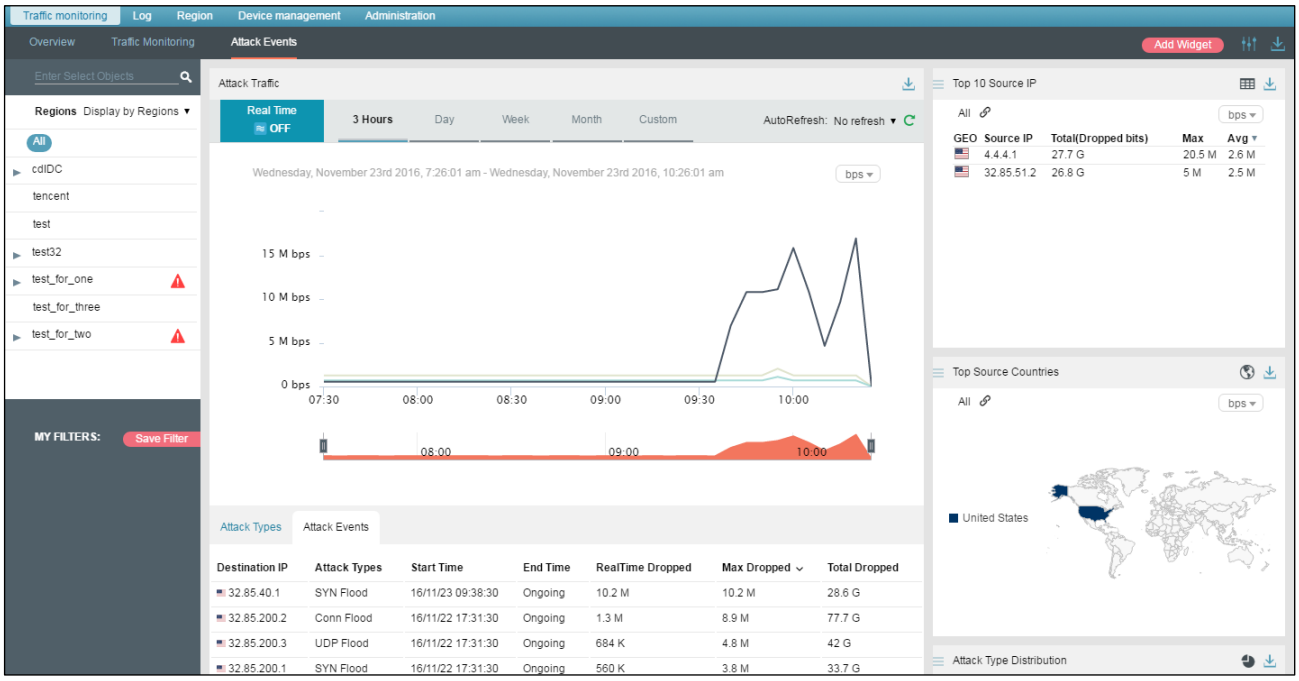
## 3.3.6 Viewing Attack Events in Historical Mode

On the page shown in Figure 3-104, clicking **ON** for **Real Time** in the **Attack 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, 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.

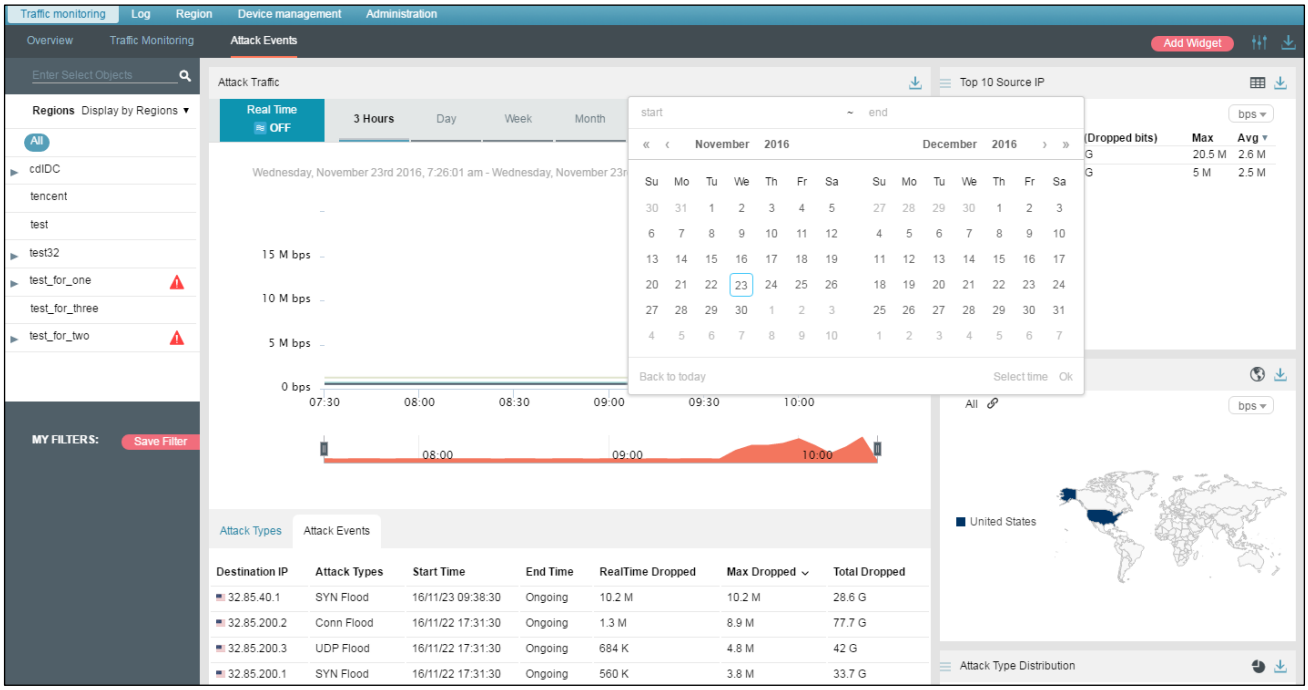
Figure 3-114 Historical attack traffic trend




On the page shown in Figure 3-114, click **Custom** above the traffic trend graph.

You can select the start time and end time of the attack traffic trend graph as required. The unit is the day.

Figure 3-115 Customization of the attack traffic trend graph



## 3.3.7 Switching the Traffic Unit

By default, traffic is expressed in bps in attack traffic trend graphs. On the page shown in Figure 3-104, 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.

## 3.3.8 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 3-104, you can select **Not fresh** from the **AutoFresh** drop-down list in the upper-right corner of the **Attack Traffic** 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 3-104, you can select **5 minute** from the **AutoFresh** drop-down list in the upper-right corner of the **Attack Traffic** panel. In this case, the attack traffic trend graph will automatically refresh every 5 minutes.

## 3.3.9 Downloading an Attack Traffic Trend Report

On the page shown in Figure 3-104, you can click in the upper-right corner to export the current data of the attack traffic trend graph as a report. For details, see section 3.1.5 Downloading a Report.

## 3.3.10 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.

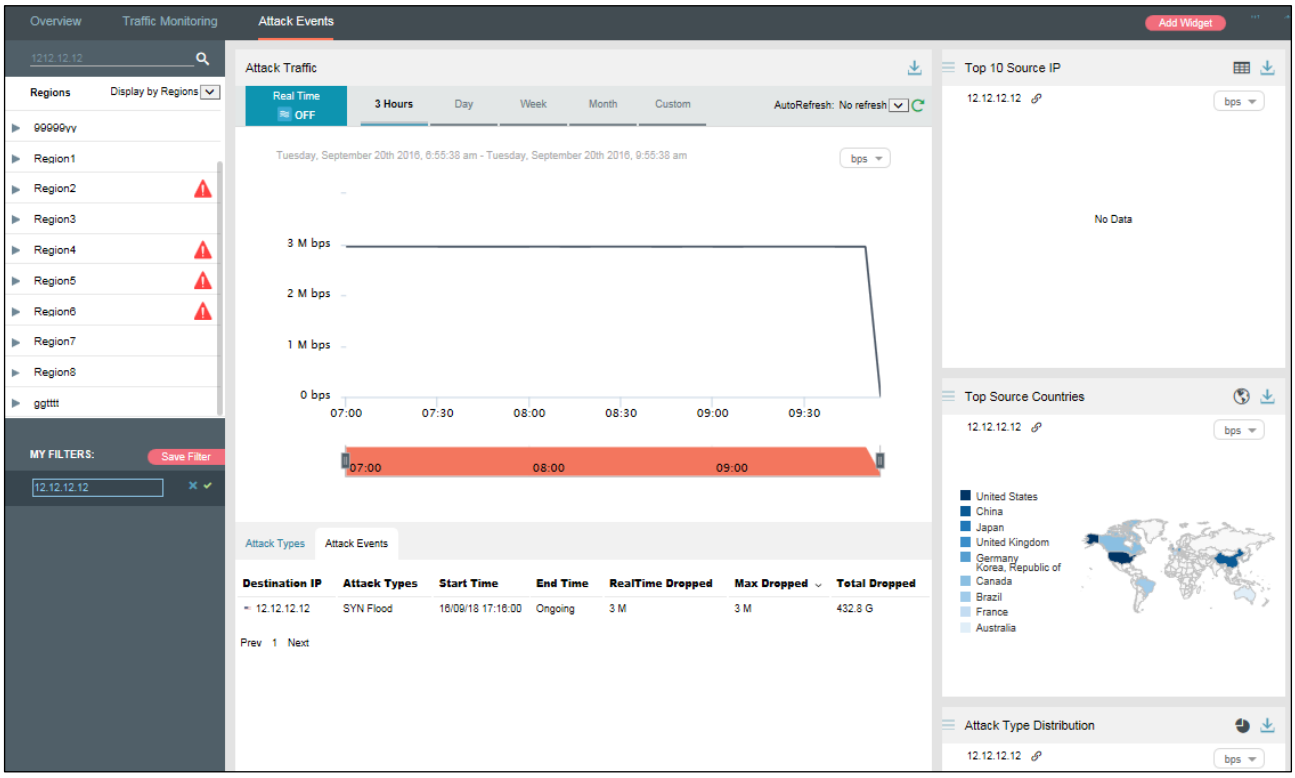
Any queried objects, such as a region, region IP group, ADS device, ADS-protected group, or IP address can be configured as a filter. But **All** and **Default IP (Default)** cannot be configured as a filter. You can configure multiple filters.

### 3.3.10.1 Configuring a Filter

To configure a filter, follow these steps:

**Step 1** On the page shown in Figure 3-104, select an object from the left pane, such as 12.12.12.12, and then click **Save Filter**.

Figure 3-116 Adding a filter



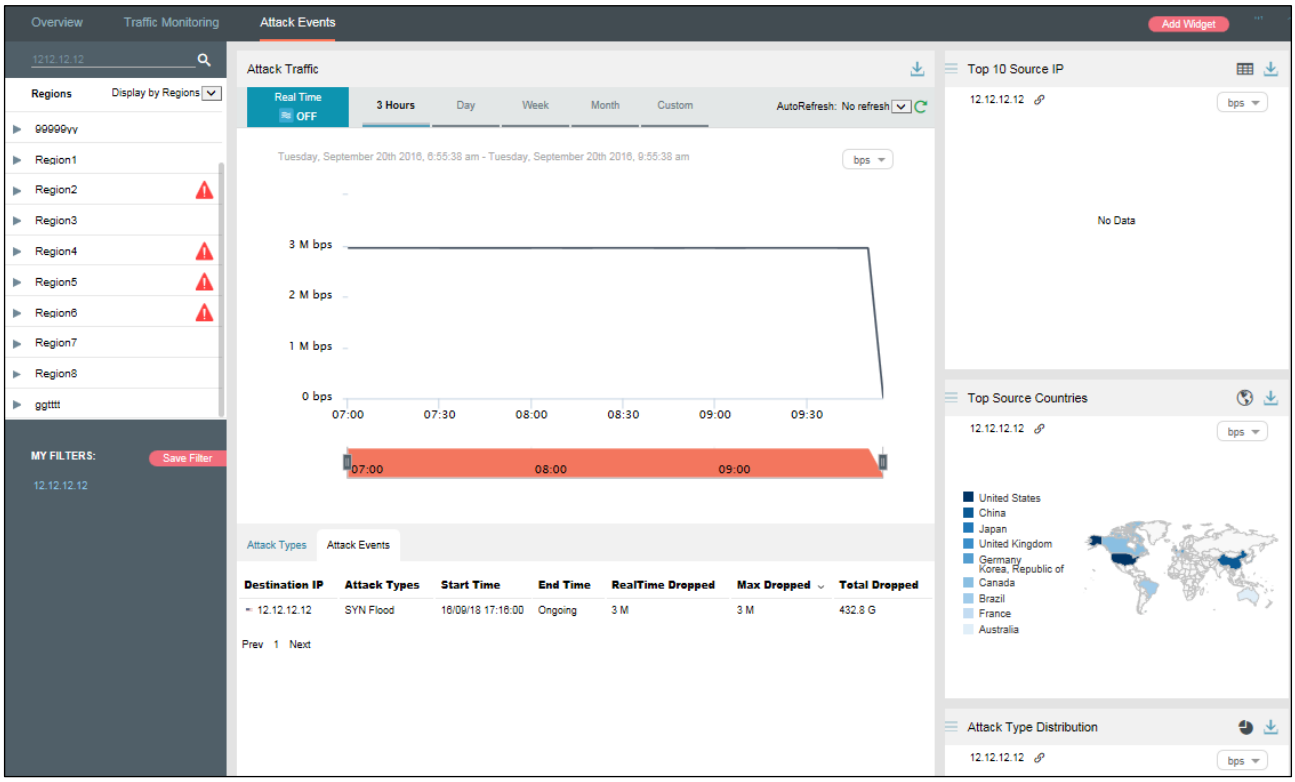

**Step 2** Type the filter name.

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 then click **Confirm** in the dialog box that appears.

**Step 4** Click **12.12.12.12** in the filter list to view its attack traffic information.

Figure 3-117 Viewing a filter




**----End**

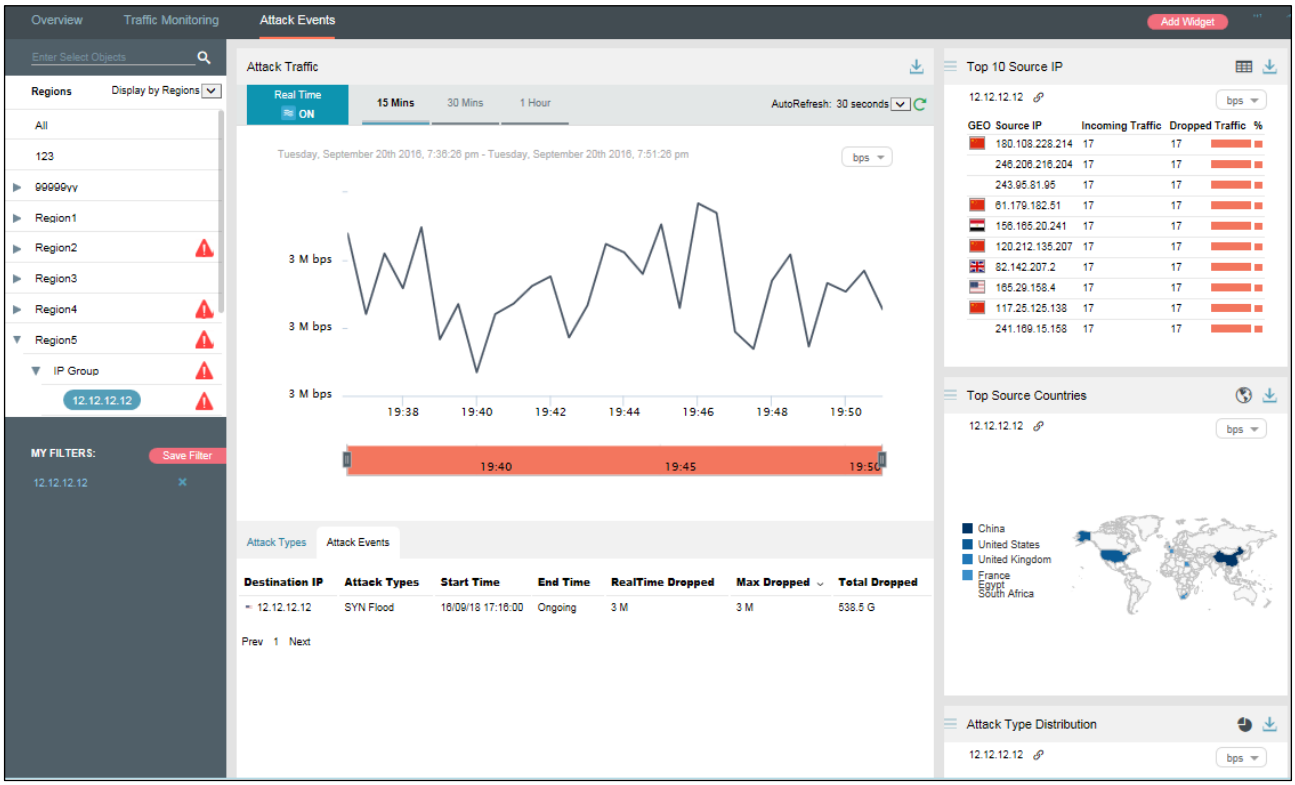
## 3.3.10.2 Deleting a Filter

To delete a filter, follow these steps:

**Step 1** On the page shown in Figure 3-117, point to a filter name

The icon  appears.

Figure 3-118 Deleting a filter




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

Then this filter is deleted.

**----End**

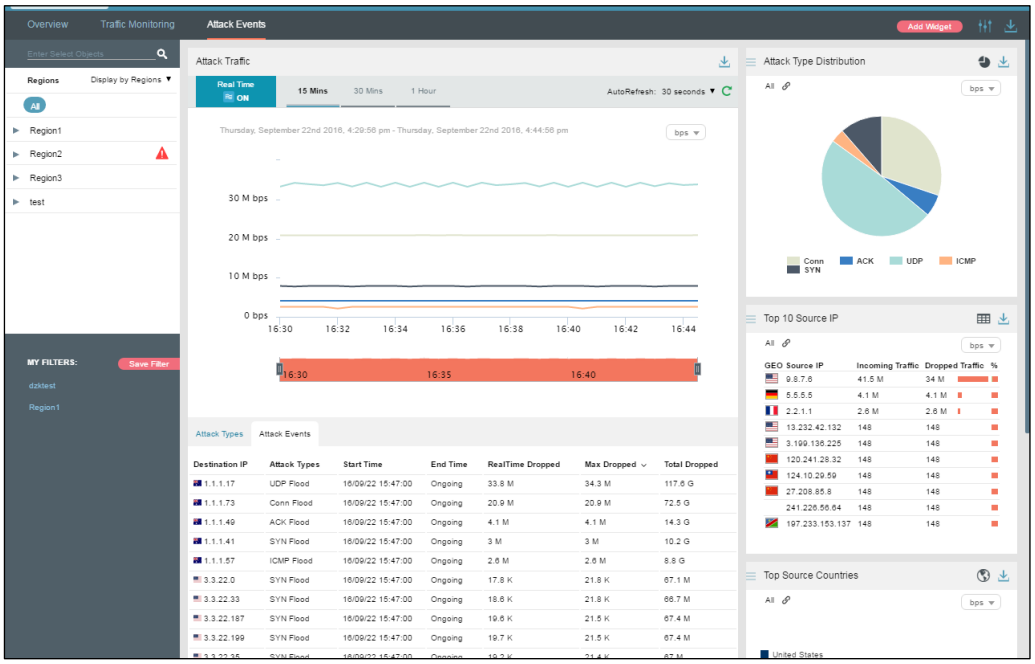
## 3.3.11 Managing Panels

By default, **Top 10 Source IP, Top Source Countries, and Attack Type Distribution** are displayed under **Traffic monitoring** > **Attack Events**, as shown in Figure 3-119.

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 3.1 Overview.

Figure 3-119 Default panels on the Attack Events page



# 4 Logs

Device logs include attack summary logs, login logs, operation logs, link status logs, performance logs, diversion logs, running alert log, HA logs, traffic alert logs, and cloud authentication logs. 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

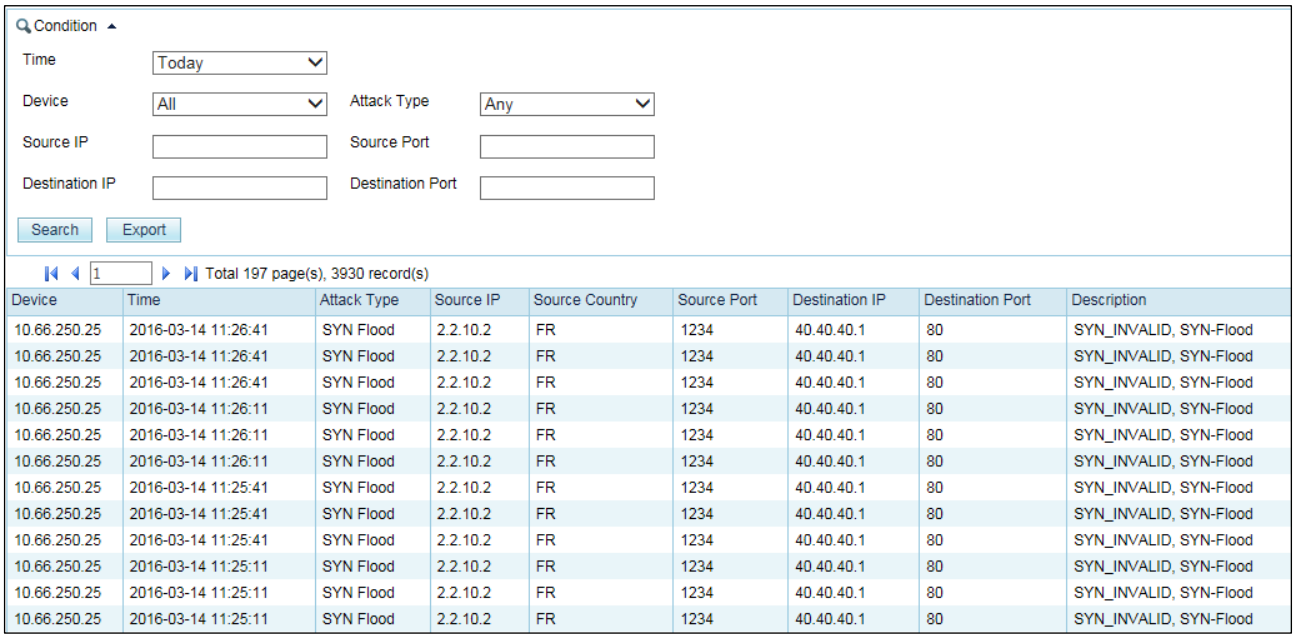
  After setting log export conditions, click **Export** to save logs to the local host.

## 4.1 Attack Summary Log

Choose **Log** > **Attack Summary Log**. The **Attack Summary Log** page appears, as shown in Figure 4-1.

You can set specific conditions to query or export logs of attacks detected and defended against by all devices in the device list.

Figure 4-1 Attack summary logs




| Device | Time | Attack Type | Source IP | Source Country | Source Port | Destination IP | Destination Port | Description |
|---|---|---|---|---|---|---|---|---|
| 10.66.250.25 | 2016-03-14 11:26:41 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |
| 10.66.250.25 | 2016-03-14 11:26:41 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |
| 10.66.250.25 | 2016-03-14 11:26:41 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |
| 10.66.250.25 | 2016-03-14 11:26:11 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |
| 10.66.250.25 | 2016-03-14 11:26:11 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |
| 10.66.250.25 | 2016-03-14 11:26:11 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |
| 10.66.250.25 | 2016-03-14 11:25:41 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |
| 10.66.250.25 | 2016-03-14 11:25:41 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |
| 10.66.250.25 | 2016-03-14 11:25:41 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |
| 10.66.250.25 | 2016-03-14 11:25:11 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |
| 10.66.250.25 | 2016-03-14 11:25:11 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |
| 10.66.250.25 | 2016-03-14 11:25:11 | SYN Flood | 2.2.10.2 | FR | 1234 | 40.40.40.1 | 80 | SYN_INVALID, SYN-Flood |

Table 4-1 describes parameters of attack summary logs.

Table 4-1 Parameters of attack summary logs

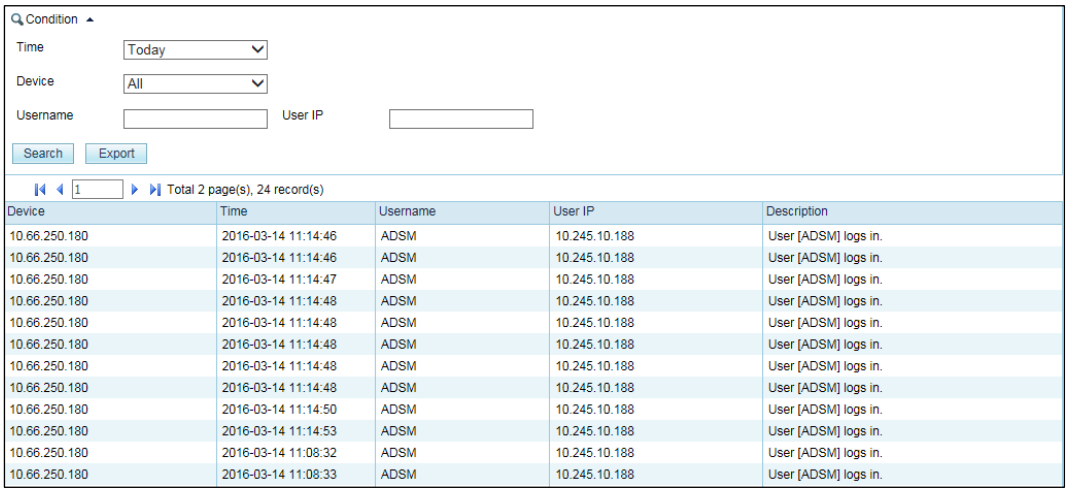
| Parameter | Description |
|---|---|
| Time | Specifies the query time range.<br>The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range. |
| Device | Specifies the device whose logs are queried.<br>**All** indicates that logs on all devices are queried. |
| Attack Type | Specifies the attack type of logs to be queried.<br>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. |

# 4.2 Login Log

Choose **Log** > **Login Log**. The **Login Log** page appears, as shown in Figure 4-2.

You can set specific conditions to query or export login logs of all devices in the device list.

Figure 4-2 Login logs




| Device | Time | Username | User IP | Description |
|---|---|---|---|---|
| 10.66.250.180 | 2016-03-14 11:14:46 | ADSM | 10.245.10.188 | User [ADSM] logs in. |
| 10.66.250.180 | 2016-03-14 11:14:46 | ADSM | 10.245.10.188 | User [ADSM] logs in. |
| 10.66.250.180 | 2016-03-14 11:14:47 | ADSM | 10.245.10.188 | User [ADSM] logs in. |
| 10.66.250.180 | 2016-03-14 11:14:48 | ADSM | 10.245.10.188 | User [ADSM] logs in. |
| 10.66.250.180 | 2016-03-14 11:14:48 | ADSM | 10.245.10.188 | User [ADSM] logs in. |
| 10.66.250.180 | 2016-03-14 11:14:48 | ADSM | 10.245.10.188 | User [ADSM] logs in. |
| 10.66.250.180 | 2016-03-14 11:14:48 | ADSM | 10.245.10.188 | User [ADSM] logs in. |
| 10.66.250.180 | 2016-03-14 11:14:48 | ADSM | 10.245.10.188 | User [ADSM] logs in. |
| 10.66.250.180 | 2016-03-14 11:14:50 | ADSM | 10.245.10.188 | User [ADSM] logs in. |
| 10.66.250.180 | 2016-03-14 11:14:53 | ADSM | 10.245.10.188 | User [ADSM] logs in. |
| 10.66.250.180 | 2016-03-14 11:08:32 | ADSM | 10.245.10.188 | User [ADSM] logs in. |
| 10.66.250.180 | 2016-03-14 11:08:33 | ADSM | 10.245.10.188 | User [ADSM] logs in. |

Table 4-2 describes parameters of login logs.

Table 4-2 Parameters of login logs

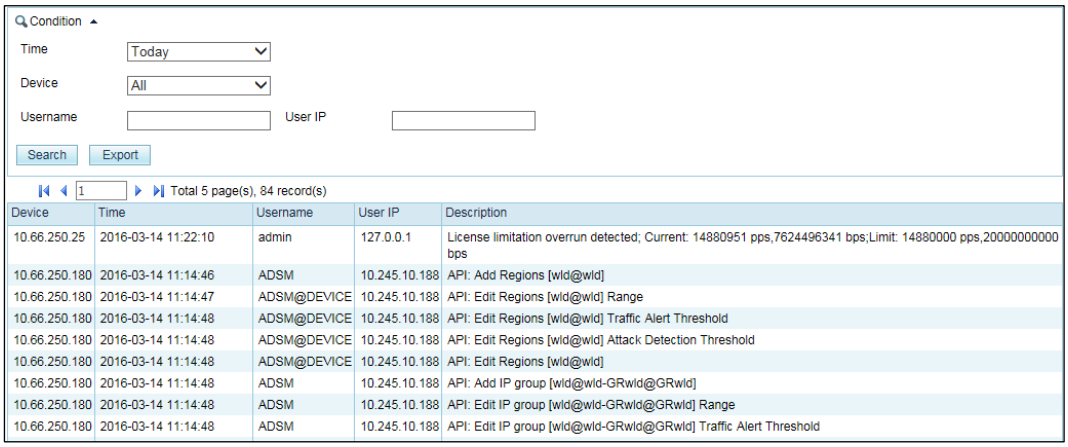
| Parameter | Description |
|---|---|
| Time | Specifies the query time range.<br>The default value is **Today**, indicating that logs of the current day are queried. Also, you can query logs on a specified date, of a month, or in a specified time range. **Custom** indicates that you can query logs in a specified time range. |
| Device | Specifies the device whose logs are queried.<br>**All** indicates that logs on all devices are queried. |
| Username | Specifies the login user name.<br>The full user name is required because fuzzy query is not allowed here. |
| User IP | Specifies the IP address of the user device.<br>The full IP address is required because fuzzy query is not allowed here. |

# 4.3 Operation Log

Choose **Log** > **Operation Log**. The **Operation Log** page appears, as shown in Figure 4-3.

You can set specific conditions to query or export operation logs of all devices in the device list.

Figure 4-3 Operation logs




| Device | Time | Username | User IP | Description |
|---|---|---|---|---|
| 10.66.250.25 | 2016-03-14 11:22:10 | admin | 127.0.0.1 | License limitation overrun detected; Current: 14880951 pps,7624496341 bps;Limit: 14880000 pps,20000000000 bps |
| 10.66.250.180 | 2016-03-14 11:14:46 | ADSM | 10.245.10.188 | API: Add Regions [wld@wld] |
| 10.66.250.180 | 2016-03-14 11:14:47 | ADSM@DEVICE | 10.245.10.188 | API: Edit Regions [wld@wld] Range |
| 10.66.250.180 | 2016-03-14 11:14:48 | ADSM@DEVICE | 10.245.10.188 | API: Edit Regions [wld@wld] Traffic Alert Threshold |
| 10.66.250.180 | 2016-03-14 11:14:48 | ADSM@DEVICE | 10.245.10.188 | API: Edit Regions [wld@wld] Attack Detection Threshold |
| 10.66.250.180 | 2016-03-14 11:14:48 | ADSM@DEVICE | 10.245.10.188 | API: Edit Regions [wld@wld] |
| 10.66.250.180 | 2016-03-14 11:14:48 | ADSM | 10.245.10.188 | API: Add IP group [wld@wld-GRwld@GRwld] |
| 10.66.250.180 | 2016-03-14 11:14:48 | ADSM | 10.245.10.188 | API: Edit IP group [wld@wld-GRwld@GRwld] Range |
| 10.66.250.180 | 2016-03-14 11:14:48 | ADSM | 10.245.10.188 | API: Edit IP group [wld@wld-GRwld@GRwld] Traffic Alert Threshold |

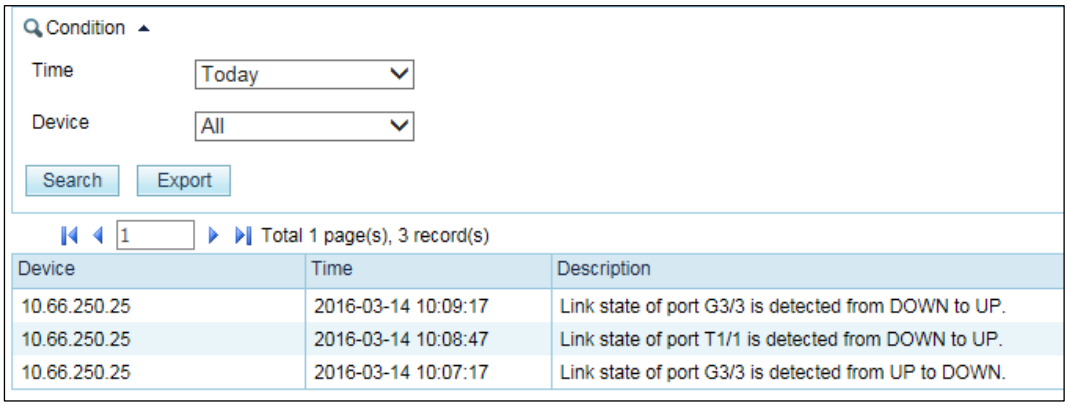
# 4.4 Link Status Log

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**. The **Link Status Log** page appears, as shown in Figure 4-4.

You can set specific conditions to query or export all link status logs of all devices in the device list.

Figure 4-4 Link status logs




| Device | Time | Description |
|---|---|---|
| 10.66.250.25 | 2016-03-14 10:09:17 | Link state of port G3/3 is detected from DOWN to UP. |
| 10.66.250.25 | 2016-03-14 10:08:47 | Link state of port T1/1 is detected from DOWN to UP. |
| 10.66.250.25 | 2016-03-14 10:07:17 | Link state of port G3/3 is detected from UP to DOWN. |

# 4.5 Diversion Log

Traffic diversion is logged only after you configure ADS diversion parameters.

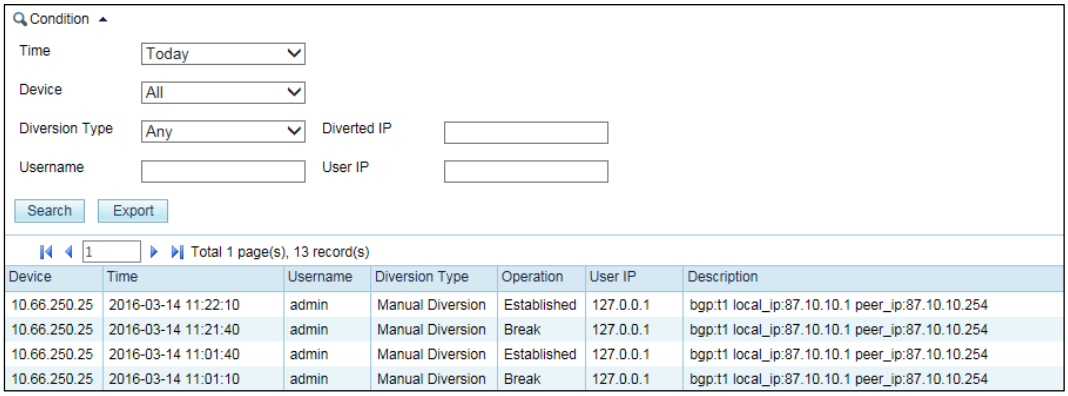
Choose **Log** > **Diversion Log**. The **Diversion Log** page appears, as shown in Figure 4-5.

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

Figure 4-5 Diversion logs




| Device | Time | Username | Diversion Type | Operation | User IP | Description |
|---|---|---|---|---|---|---|
| 10.66.250.25 | 2016-03-14 11:22:10 | admin | Manual Diversion | Established | 127.0.0.1 | bgp:t1 local_ip:87.10.10.1 peer_ip:87.10.10.254 |
| 10.66.250.25 | 2016-03-14 11:21:40 | admin | Manual Diversion | Break | 127.0.0.1 | bgp:t1 local_ip:87.10.10.1 peer_ip:87.10.10.254 |
| 10.66.250.25 | 2016-03-14 11:01:40 | admin | Manual Diversion | Established | 127.0.0.1 | bgp:t1 local_ip:87.10.10.1 peer_ip:87.10.10.254 |
| 10.66.250.25 | 2016-03-14 11:01:10 | admin | Manual Diversion | Break | 127.0.0.1 | bgp:t1 local_ip:87.10.10.1 peer_ip:87.10.10.254 |

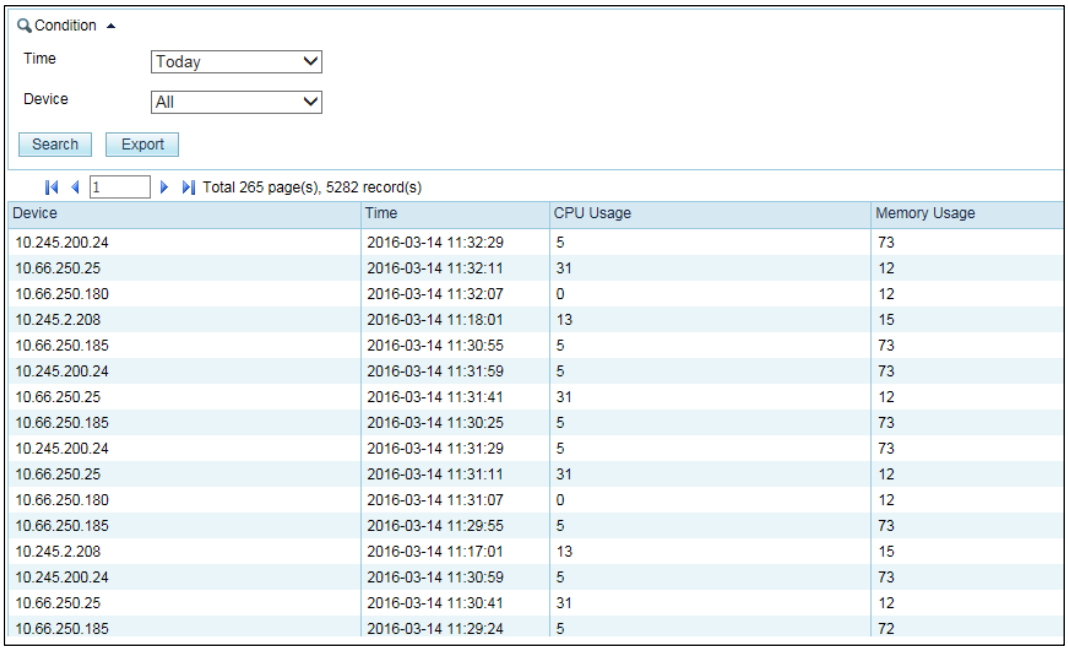
# 4.6 Performance Log

Choose **Log** > **Performance Log**. The **Performance Log** page appears, as shown in Figure 4-6.

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

Figure 4-6 Performance logs



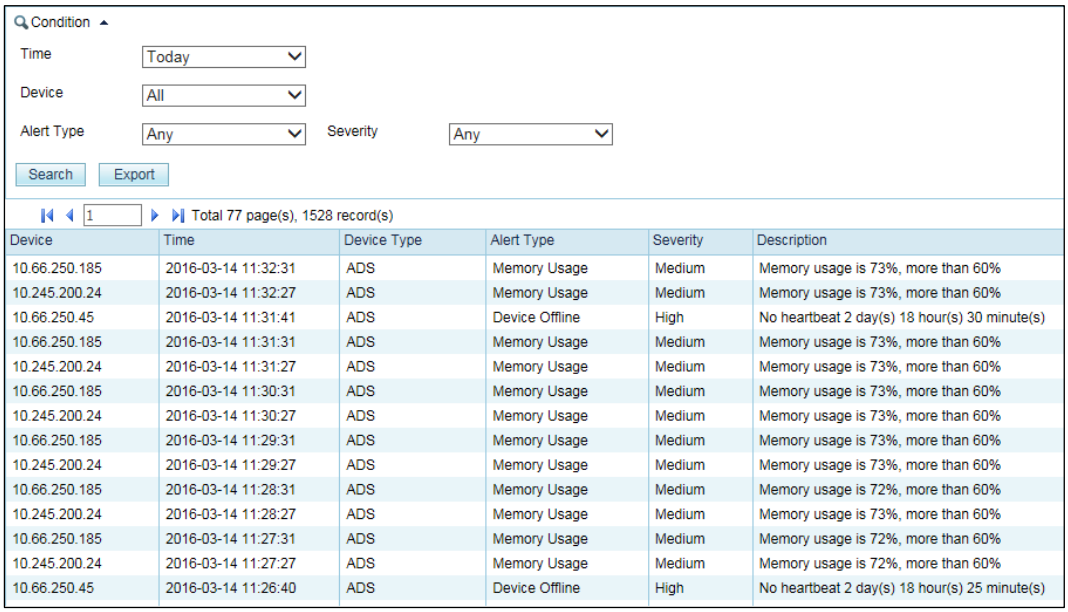

| Device | Time | CPU Usage | Memory Usage |
|---|---|---|---|
| 10.245.200.24 | 2016-03-14 11:32:29 | 5 | 73 |
| 10.66.250.25 | 2016-03-14 11:32:11 | 31 | 12 |
| 10.66.250.180 | 2016-03-14 11:32:07 | 0 | 12 |
| 10.245.2.208 | 2016-03-14 11:18:01 | 13 | 15 |
| 10.66.250.185 | 2016-03-14 11:30:55 | 5 | 73 |
| 10.245.200.24 | 2016-03-14 11:31:59 | 5 | 73 |
| 10.66.250.25 | 2016-03-14 11:31:41 | 31 | 12 |
| 10.66.250.185 | 2016-03-14 11:30:25 | 5 | 73 |
| 10.245.200.24 | 2016-03-14 11:31:29 | 5 | 73 |
| 10.66.250.25 | 2016-03-14 11:31:11 | 31 | 12 |
| 10.66.250.180 | 2016-03-14 11:31:07 | 0 | 12 |
| 10.66.250.185 | 2016-03-14 11:29:55 | 5 | 73 |
| 10.245.2.208 | 2016-03-14 11:17:01 | 13 | 15 |
| 10.245.200.24 | 2016-03-14 11:30:59 | 5 | 73 |
| 10.66.250.25 | 2016-03-14 11:30:41 | 31 | 12 |
| 10.66.250.185 | 2016-03-14 11:29:24 | 5 | 72 |

# 4.7 Performance Alert Log

Choose **Log** > **Performance Alert Log**. The **Performance Alert Log** page appears, as shown in Figure 4-7. 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:

- Alert ID
- Generation time
- Device type
- Alert type
- Severity
- Description

Figure 4-7 Performance alert logs




| Device | Time | Device Type | Alert Type | Severity | Description |
|---|---|---|---|---|---|
| 10.66.250.185 | 2016-03-14 11:32:31 | ADS | Memory Usage | Medium | Memory usage is 73%, more than 60% |
| 10.245.200.24 | 2016-03-14 11:32:27 | ADS | Memory Usage | Medium | Memory usage is 73%, more than 60% |
| 10.66.250.45 | 2016-03-14 11:31:41 | ADS | Device Offline | High | No heartbeat 2 day(s) 18 hour(s) 30 minute(s) |
| 10.66.250.185 | 2016-03-14 11:31:31 | ADS | Memory Usage | Medium | Memory usage is 73%, more than 60% |
| 10.245.200.24 | 2016-03-14 11:31:27 | ADS | Memory Usage | Medium | Memory usage is 73%, more than 60% |
| 10.66.250.185 | 2016-03-14 11:30:31 | ADS | Memory Usage | Medium | Memory usage is 73%, more than 60% |
| 10.245.200.24 | 2016-03-14 11:30:27 | ADS | Memory Usage | Medium | Memory usage is 73%, more than 60% |
| 10.66.250.185 | 2016-03-14 11:29:31 | ADS | Memory Usage | Medium | Memory usage is 73%, more than 60% |
| 10.245.200.24 | 2016-03-14 11:29:27 | ADS | Memory Usage | Medium | Memory usage is 73%, more than 60% |
| 10.66.250.185 | 2016-03-14 11:28:31 | ADS | Memory Usage | Medium | Memory usage is 72%, more than 60% |
| 10.245.200.24 | 2016-03-14 11:28:27 | ADS | Memory Usage | Medium | Memory usage is 73%, more than 60% |
| 10.66.250.185 | 2016-03-14 11:27:31 | ADS | Memory Usage | Medium | Memory usage is 72%, more than 60% |
| 10.245.200.24 | 2016-03-14 11:27:27 | ADS | Memory Usage | Medium | Memory usage is 72%, more than 60% |
| 10.66.250.45 | 2016-03-14 11:26:40 | ADS | Device Offline | High | No heartbeat 2 day(s) 18 hour(s) 25 minute(s) |

Table 4-3 describes parameters of performance alert logs.

Table 4-3 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**, **Device Offline**, or **HA Alert**. **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. |

# 4.8 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**. The **HA Log** page appears, as shown in Figure 4-8.

Figure 4-8 HA logs

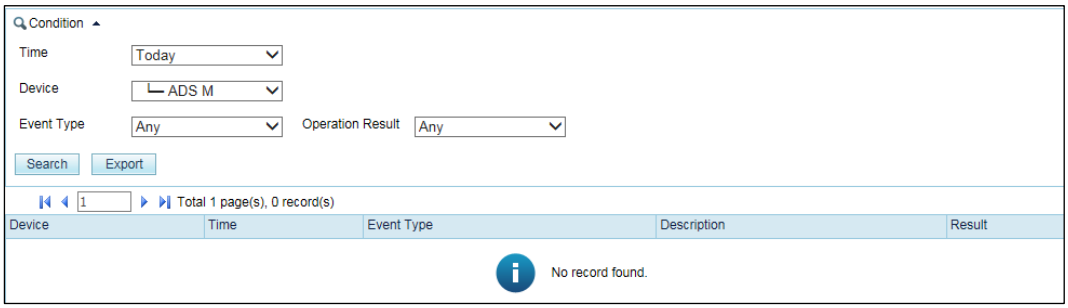



Table 4-4 describes parameters of HA logs.

Table 4-4 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:<br>• **Succeeded**: indicates that all logs about succeeded operations are queried.<br>• **Failed**: indicates that all logs about failed operations are queried.<br>• **Any**: indicates that logs with any results are queried. |

# 4.9 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 7.1.1 Basic Settings.

Choose **Log** > **Traffic Alert Log**. The **Traffic Alert Log** page appears, as shown in Figure 4-9.

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 (such as start time, end time, or duration)
- Description

  The description is usually instantaneous traffic in the unit of pps and bps when the alert is generated. 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.

Figure 4-9 Traffic alert logs

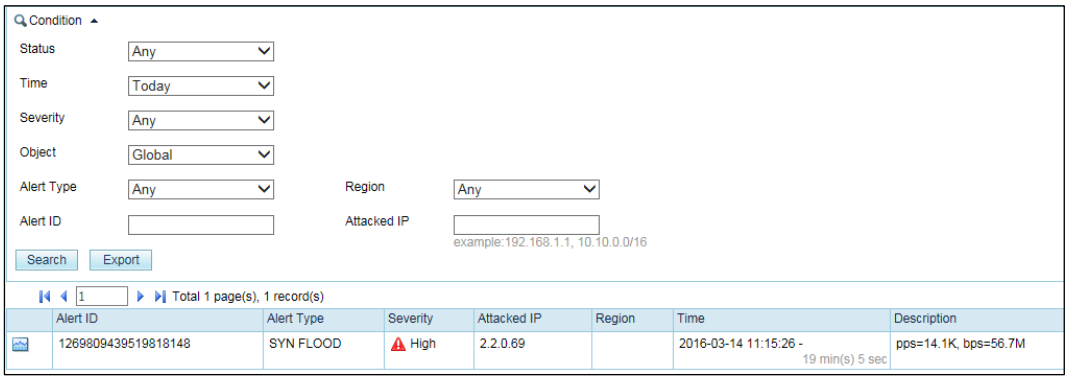



Table 4-5 describes parameters of traffic alert logs.

Table 4-5 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:<br>• **Ongoing**: indicates alerts that are occurring.<br>• **Ended**: indicates alerts that are over.<br>• **Any**: indicates all generated alerts. |
| Time | Specifies the query time range.<br>The default value is **Today**, that is, logs of the current day are queried. In addition, you can query logs monthly, on a specified day, or in a custom period. For **Custom**, you need to set the start time and end time. |
| Severity | Specifies the alert severity, which can be set to **High**, **Medium**, and **Low**.<br>**Any** indicates that alerts of all severities are queried. |
| Object | • **Global** indicates that alerts generated by all NTA devices are queried.<br>• **By device** indicates that alerts generated by an NTA device are queried. |
| Device (Optional) | 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 6.1.3 Configuring an NTA Device. |
| Alert Type | Specifies the type of alert events that can be reported by NTA devices to ADS M.<br>For the setting of this option, see section 6.2 Configuring NTA Diversion Settings. **Any** indicates that alerts of all types are queried. |
| Region | Specifies the region where alerts are queried.<br>New regions on ADS M are also displayed here. For region configuration, see section 5.3 Configuring a Region. **Any** indicates that alerts in all regions are queried. |

| Parameter | Description |
|---|---|
| Alert ID | Specifies the alert ID.<br>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. |

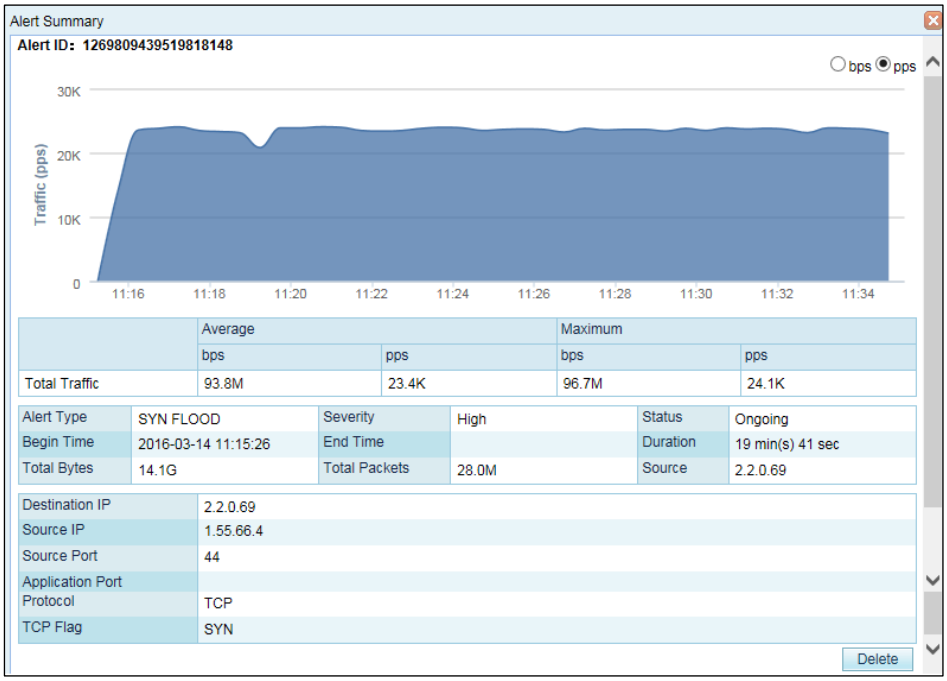
Click in the query results to open the **Alert Summary** page, as shown in Figure 4-10. This page displays detailed information of this alert, including:

- 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. Please perform this operation with caution. |

Figure 4-10 Alert summary



# 4.10 Cloud Authentication Logs

The **Cloud Authentication Logs** page is available only when an ADS M virtual machine is used. For how to configure cloud authentication, see section 7.1.2 License Management.

Choose **Log > Cloud Authentication Logs**. The **Cloud Authentication Logs** page appears.

Figure 4-11 Cloud Authentication Logs page

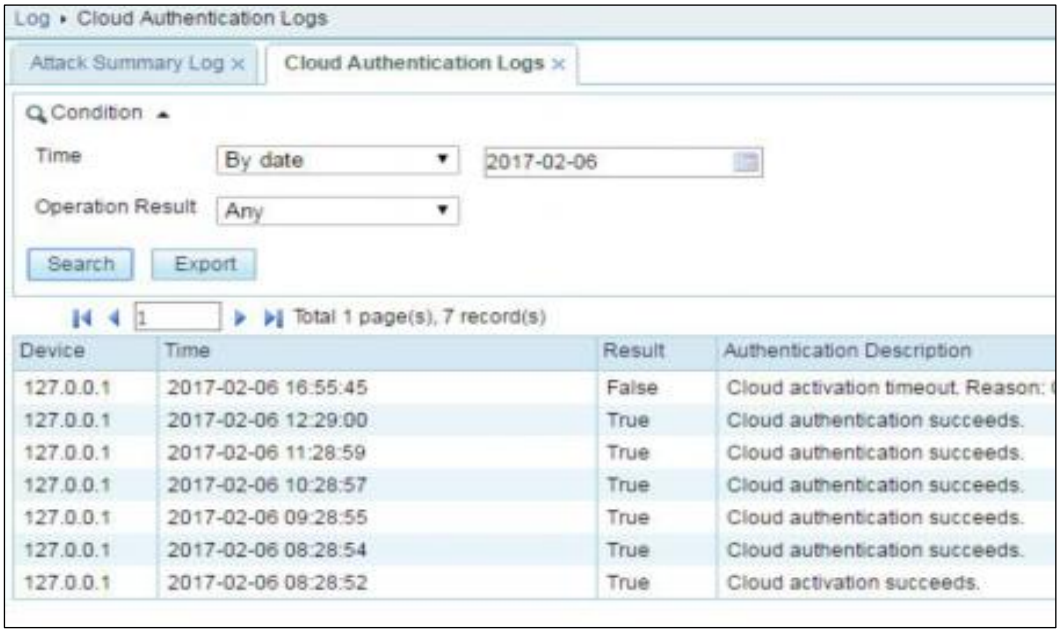



Table 4-6 describes parameters for querying cloud authentication logs.

Table 4-6 Parameters for querying 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. Other options include **By Date**, **By Month**, and **Custom**. **Custom** indicates that you can query logs in a specified time range. |
| Operation Result | • **Successful** indicates that logs of successful activation or authentication are queried.<br>• **Failed** indicates that logs of failed authentication are queried.<br>• **Any** indicates that all logs are queried. |

# 5 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.

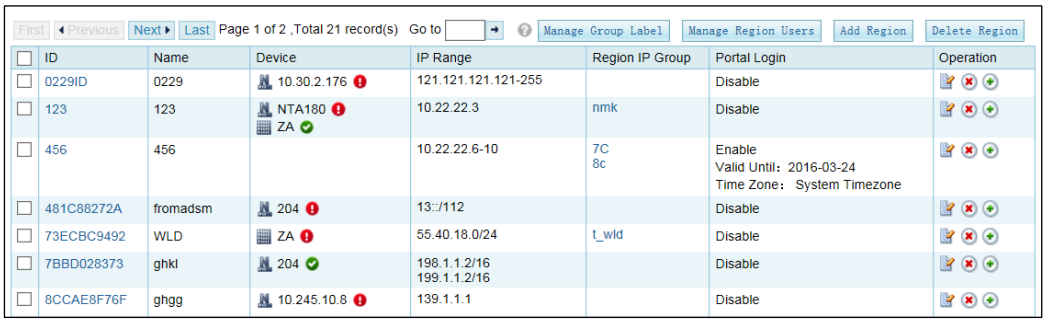
## 5.1 Managing Group Labels

ADS M supports grouped management of regions. A group label identifies one or more regions, facilitating region classification.

Choose **Region** > **Region Management**.

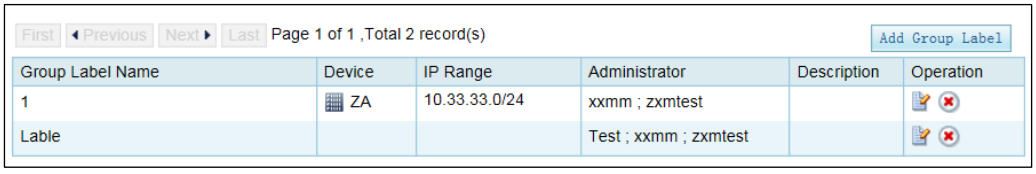
The **Region List** page appears, as shown in Figure 5-1.

Figure 5-1 Region list




Click **Manage Group Label**. The group label management page appears, as shown in Figure 5-2.

Figure 5-2 Group label management page



You can create, edit, and delete a group label.

## 5.1.1 Creating a Group Label

Click **Add Group Label** on the page shown in Figure 5-2. The dialog box for creating a group label appears, as shown in Figure 5-3.

Figure 5-3 Creating a group label

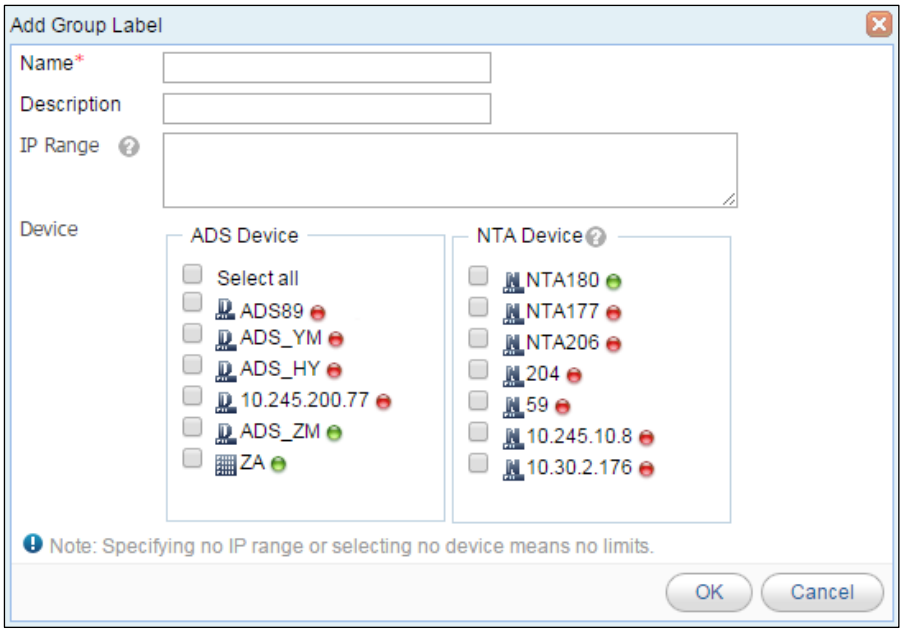



Table 5-1 describes parameters for creating a group label.

Table 5-1 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.<br>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 devices that are managed by ADS M are available for you to select. |

## 5.1.2 Editing a Group Label

In the group label list, click in the **Operation** column to edit a group label.

### 5.1.3 Deleting a Group Label

In the group label list, click in the **Operation** column to delete a group label.

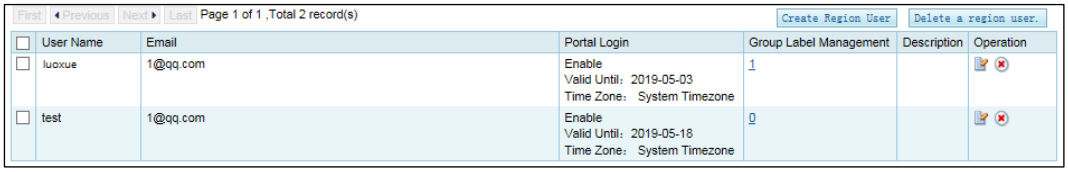
| | |
|---|---|
| Caution | Deleting a group label will delete the region that references this label and all IP groups in the region. Also, this operation will make it impossible for a region user to log in to the enabled Portal system. |

## 5.2 Managing Region Managers

A region manager for whom the Portal is enabled can create or edit regions on the Portal.

On the **Region List** page shown in Figure 5-4, click **Manage Region Users** in the upper-right corner. The list of region managers appears.

Figure 5-4 List of region managers




A system administrator can create, edit, or delete region managers.

### 5.2.1 Creating a Region Manager

On the **Manage Region Users** page shown in Figure 5-4, 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 *NSFOCUS ADS Portal User Guide*.

Figure 5-5 Creating a region manager

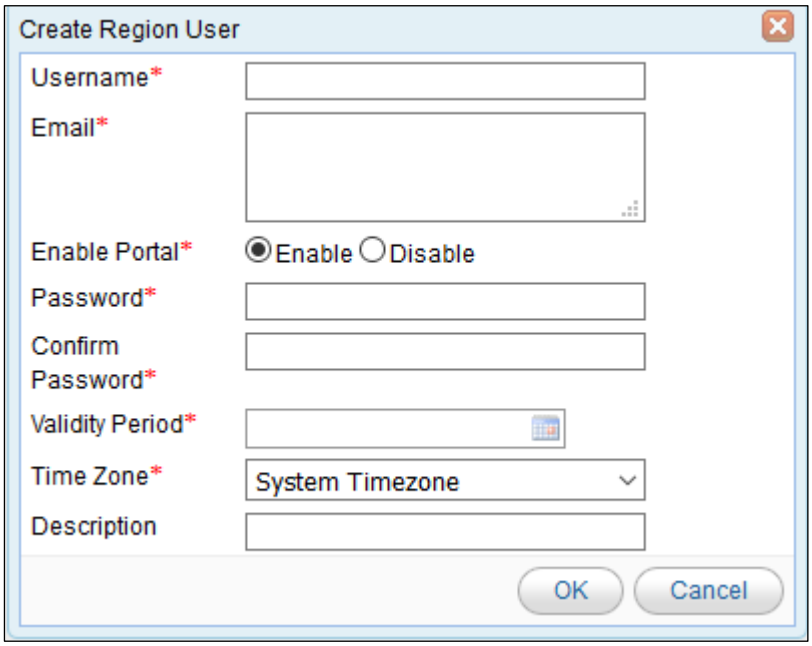



Table 5-2 describes parameters for creating a region manager.

Table 5-2 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. |
| Description | Brief description of this region manager. |

## 5.2.2 Configuring Permissions of a Region Manager

On the **Manage Region Users** page shown in Figure 5-4, you can click a figure in the **Group Label Management** column of the region manager list to configure permissions of a region manager.

Figure 5-6 Configuring permissions of a region manager

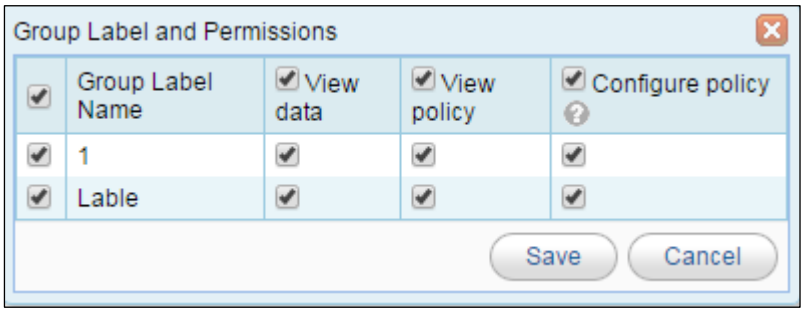



Table 5-3 describes parameters for configuring permissions of a region manager.

Table 5-3 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. |

### 5.2.3 Editing a Region Manager

On the region manager list, click in the **Operation** column to edit settings of a region manager.

### 5.2.4 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 managers.

## 5.3 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 7.1.1 Basic Settings):

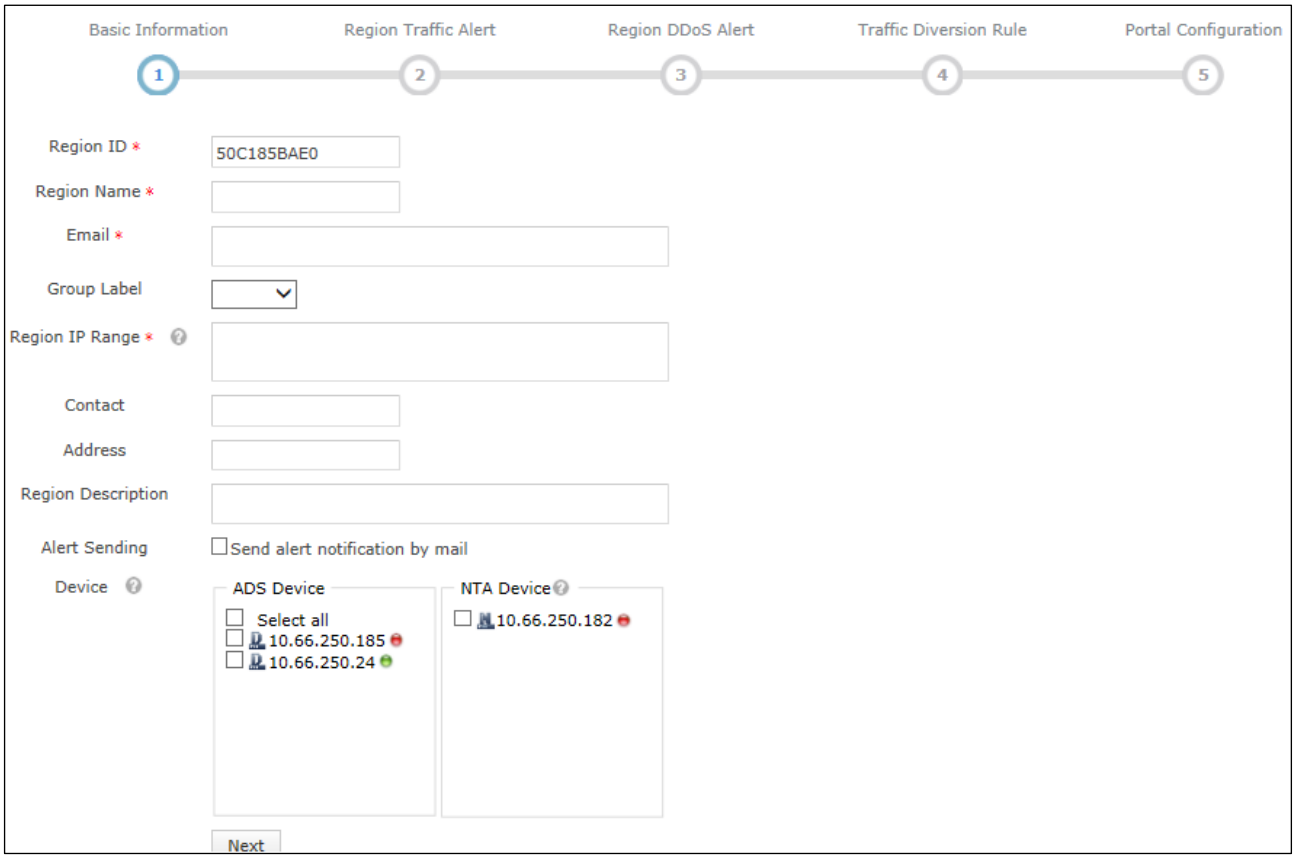
- For the detection mode of **NTA**, you need to configure basic information, region traffic alert parameters, region DDoS alert parameters, and traffic diversion rules.
- For the detection mode of **None** or **Local**, you need to configure only basic information.

## 5.3.1 Creating a Region

For ADS M whose detection mode is set to **NTA**, perform the following steps to create a region:

**Step 1** Click **Add Region** in the upper-right corner of the **Region List** page.

Figure 5-7 Configuring basic information of a region




**Step 2** Configure basic information.

Table 5-4 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 (;). |

| Parameter | Description |
|---|---|
| | Note<br>Only the first 10 email address will be delivered to NTA devices.<br>After **Send alert notification by mail** is selected, ADS M will periodically send region alerts to the email address of the contact person.<br>For details about scheduling the sending of region alerts , see section 7.3.4 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.<br>Note<br>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.<br>Both IPv4 and IPv6 addresses are accepted. You can type one or more IP addresses, IP subnets, and IP segments, with each in a separate line. A maximum of 4096 entries are allowed.<br>• IPv4 address format: 192.168.0.1, 192.168.0.1/24, or 192.168.0.1–254<br>• IPv6 address format: 2001::1-fffe, 2001::1-fffe/126, or 2001::1<br>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.<br>Note<br>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.<br>For details about scheduling the sending of region alerts or reports, see section 7.3.4 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. |

**Step 3** Configure region traffic alert parameters.

After configuring basic information, click **Next** to open the **Region Traffic Alert** page.

Figure 5-8 Configuring region traffic alert parameters

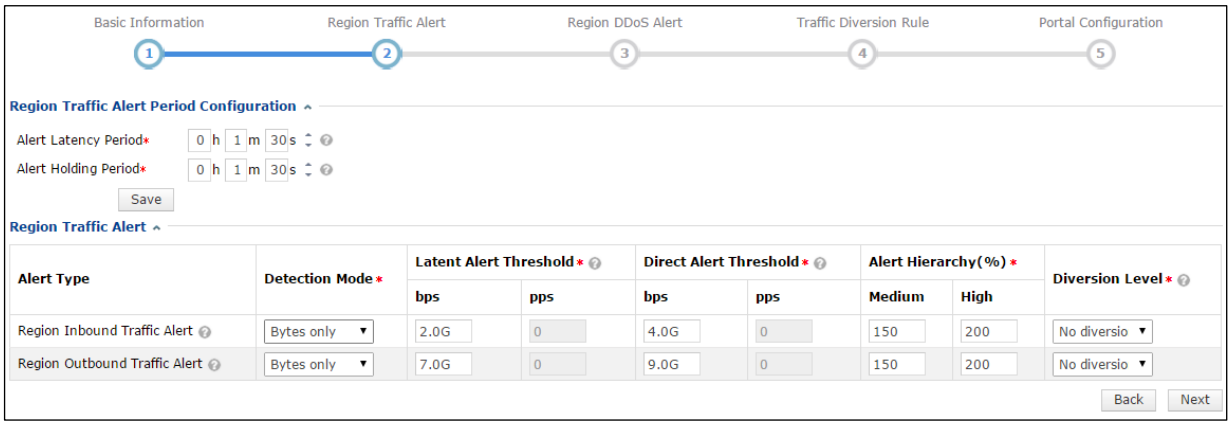



Table 5-5 describes region traffic alert parameters.

Table 5-5 Region traffic alert parameters

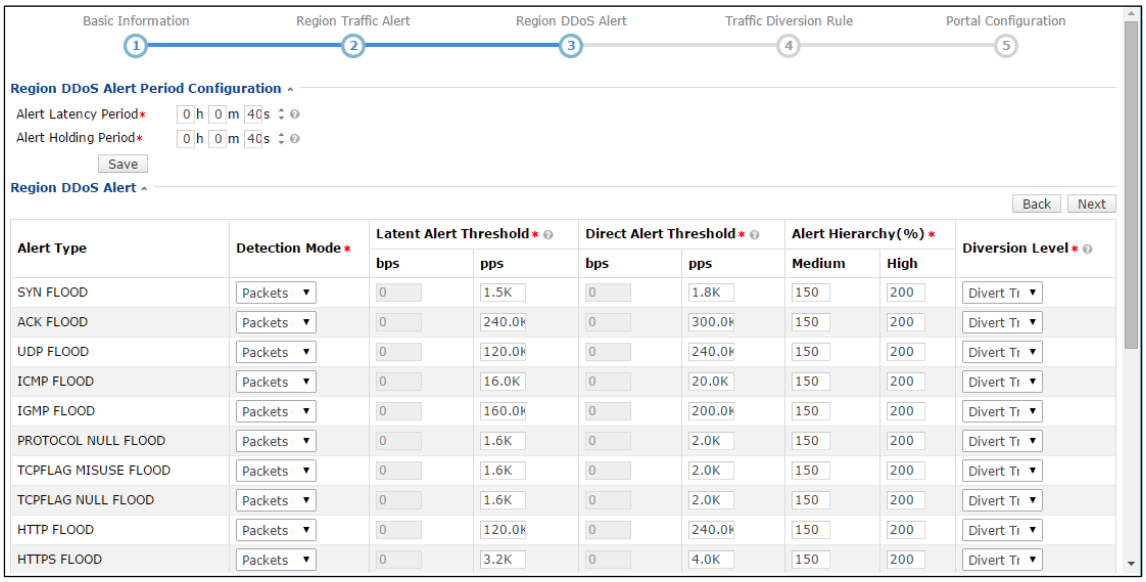
| Parameter | Description |
|---|---|
| Alert Latency Period | Specifies the maximum duration NTA must wait to generate an alert for the traffic between the value of **Latent Alert Threshold** and that of **Direct Alert Threshold**. The value ranges are 0–23 for the hour (**h**), 0–59 for the minute (**m**), and 0–59 for the second (**s**). |
| 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**), 0–59 for the minute (**m**), and 0–59 for the second (**s**). |
| Alert Type | Specifies the type of region traffic alerts, which can be either of the following:<br>• **Region Inbound Traffic Alert**: checks the total inbound traffic of the region.<br>• **Region Outbound Traffic Alert**: checks the total outbound traffic of the region. |
| Detection Mode | Specifies a detection mode, which can be **Not detect**, **Packets only**, **Bytes only**, **Both packets and bytes**, and **Either packets or bytes**. |
| Latent Alert Threshold | Specifies the threshold that triggers NTA to enter the latent period. If the traffic stays below the direct alert threshold but above the latent alert threshold for a certain period (which is called "latency period" and can be configured under **Global Alert Settings** > **Alert Parameters**), the system generates an alert. For details, see section 6.3.3.2 Alert Parameters.<br>The proper use of the latent alert threshold can reduce false positives due to traffic jitter. |
| Alert Hierarchy | Specifies the hierarchy of traffic alerts and DDoS alerts. |
| Direct Alert Threshold | Specifies the threshold that triggers NTA to generate an alert. |
| Diversion Level | Specifies the level of traffic diversion conducted after a region traffic alert is triggered.<br>There are three diversion levels (low, medium, and high), corresponding to three alert levels (low, medium, and high) that can be configured under **Global Alert Settings** > **Alert Parameters**. For details, see section 6.3.3.2 Alert |

| Parameter | Description |
|---|---|
| | Parameters. |

**Step 4** Configure region DDoS alert parameters.

After configuring region traffic alert parameters, click **Next** to open the **Region DDoS Alert** page.

Figure 5-9 Configuring region DDoS alert parameters




For the description of parameters on this page, see Table 5-5.

**Step 5** Configure region traffic diversion rules.

After configuring region alert hierarchy parameters, click **Next** to open the **Traffic Diversion Rule** page.

Figure 5-10 Configuring traffic diversion rules

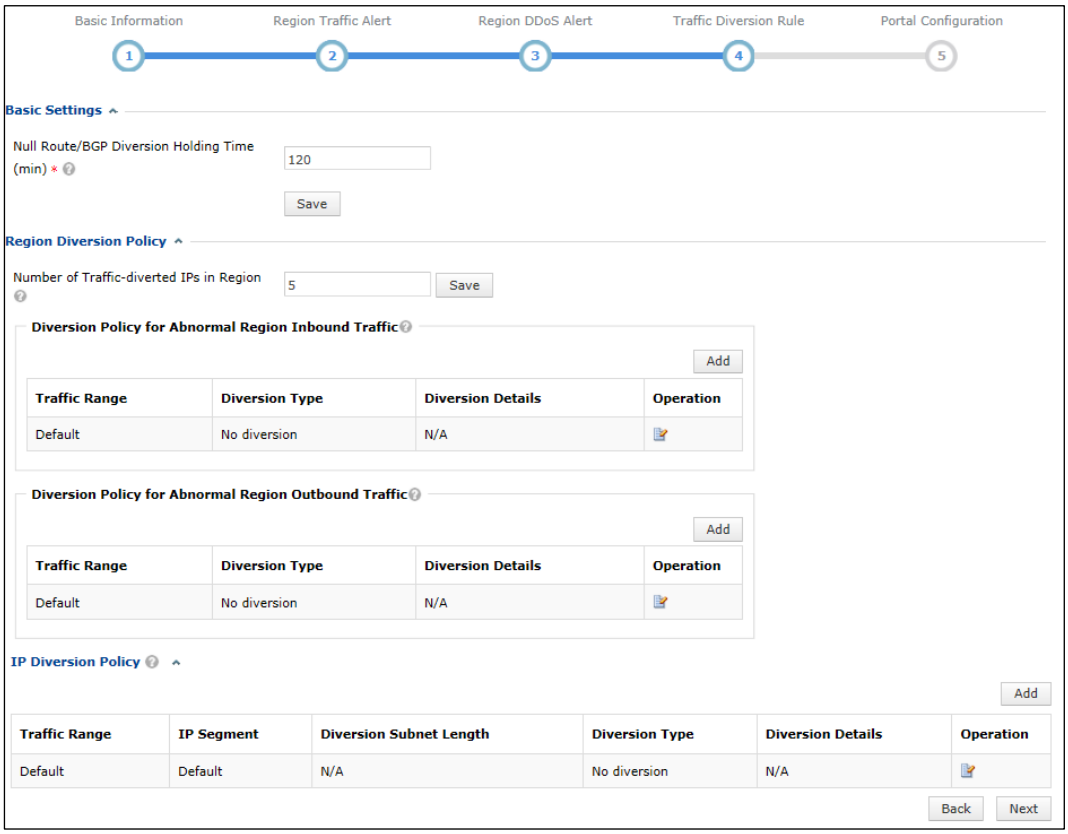



Table 5-6 describes parameters for configuring traffic diversion rules.

Table 5-6 Parameters for configuring traffic diversion rules

| Parameter | | Description |
|---|---|---|
| Basic Settings | Null Route/BGP Diversion Holding Time (min) | After sending a "Null route/BGP diversion" notification to a device, NTA will start a countdown to the revocation of the involved route. Once the diversion holding time expires, NTA revokes the route. |
| Region Diversion Policy | Number of 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 200.<br>When **Diversion Policy for Abnormal Region Inbound/Outbound Traffic** is triggered, NTA can perform null route 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.<br>• 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**.<br>• When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set.<br>Note |

| Parameter | | Description |
|---|---|---|
| | | The diversion policy for a region has a lower priority than that for an IP group.<br>• You can click **Add** and create new diversion policies. |
| | 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.<br>• 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**.<br>• When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set.<br>Note<br>The diversion policy for a region has a lower priority than that for an IP group.<br>• 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.<br>• 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**.<br>• When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set.<br>• You can click **Add** and create new diversion policies. |

**Step 6** Configuring the Portal.

After configuring traffic diversion rules, click **Next** to open the **Portal Configuration** page.

Figure 5-11 Configuring the Portal

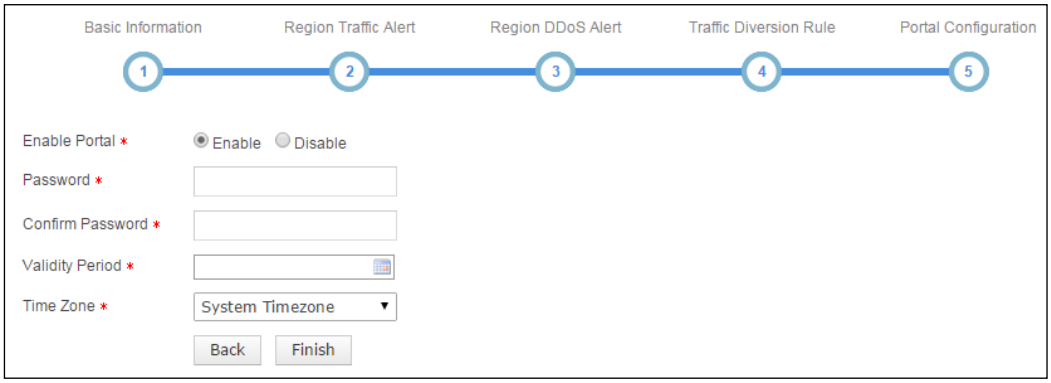



Table 5-7 describes the parameters for configuring the Portal.

Table 5-7 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.<br>Note<br>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.<br>Note<br>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. |

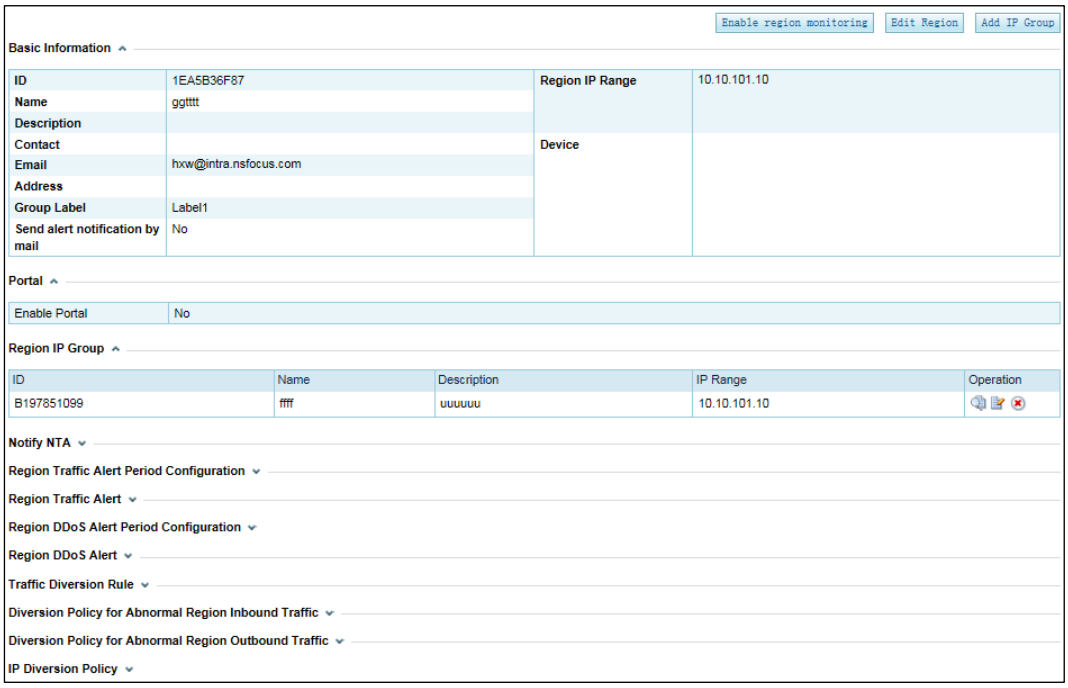
**Step 7** After configuring traffic diversion rules, click **Finish**.

**----End**

## 5.3.2 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 5-12. Then details of the selected region appear.

Figure 5-12 Details of a region




## 5.3.3 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. |

## 5.3.4 Deleting a Region

On the region list, click in the **Operation** column to delete a region.

| | |
|---|---|
| Caution | • Deleting a region stops you from continuing to view the opened monitoring page, configuration page, or other pages related to this region.<br>• 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. |

# 5.4 Configuring a Region IP Group

You can add a region 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 7.1.1 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.

## 5.4.1 Adding a Region IP Group

### 5.4.1.1 NTA Detection Mode

**Step 1** On the **Region List** page shown in Figure 5-1, 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 5-12.

Figure 5-13 Adding an IP group in NTA detection mode


**Step 2** Configure basic information of the IP group.

Table 5-8 Parameters for configuring basic information of an IP group

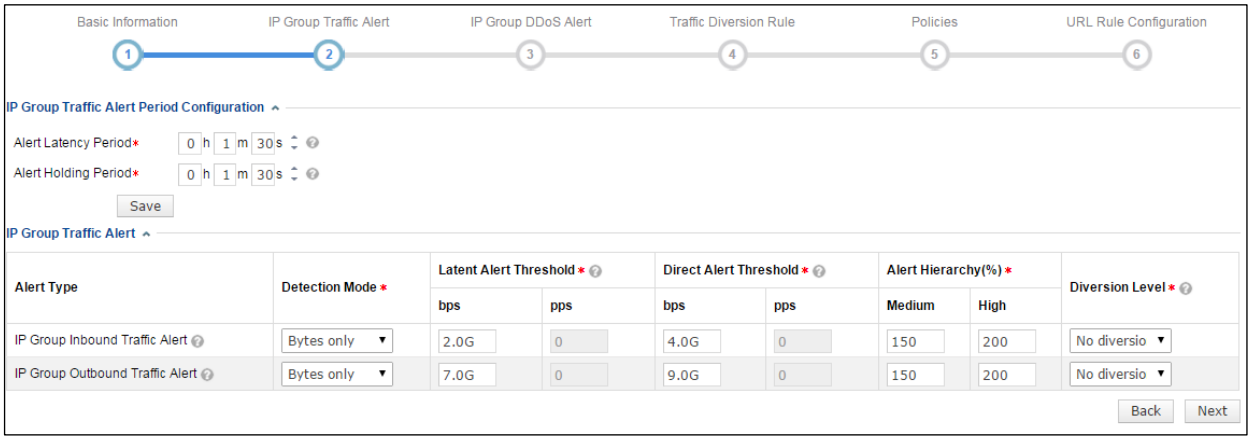
| Parameter | Description |
|---|---|
| IP Group ID | Uniquely identifies an IP group. It is automatically generated by the system and can be manually changed (note that you cannot change it when editing an IP group and it cannot be the same as an existing one) when you add an IP group. The IP group 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.<br>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 |

| Parameter | Description |
|---|---|
| | add up to 1024 entries.<br>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.<br>When you type IP addresses, the IP range of the region to which the IP group belongs is dynamically displayed below the text box.<br>**Note**<br>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. |
| 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.

Figure 5-14 Configuring IP group traffic alert parameters

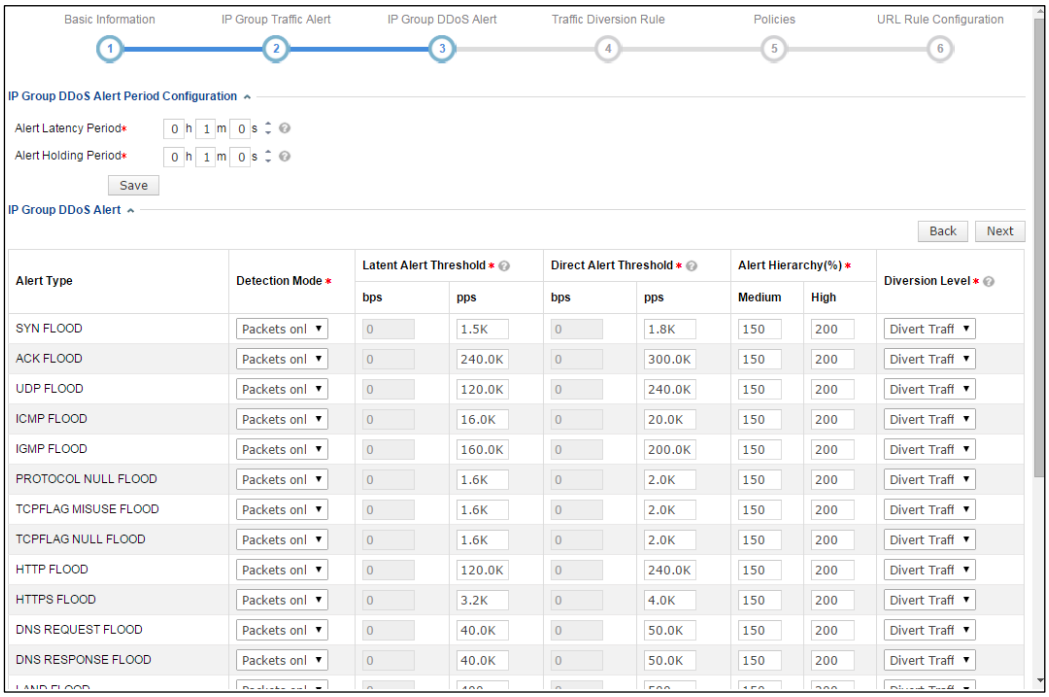



Parameter configuration here is the similar to that for a region. For the description of parameters, see Table 5-5.

**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.

Figure 5-15 Configuring IP group DDoS alert parameters




For the description of parameters on this page, see Table 5-5.

**Step 5** Configure IP group traffic diversion rules.

After configuring IP group alert hierarchy parameters, click **Next** to open the **Traffic Diversion Rule** page.

Figure 5-16 Configuring IP group traffic diversion rules

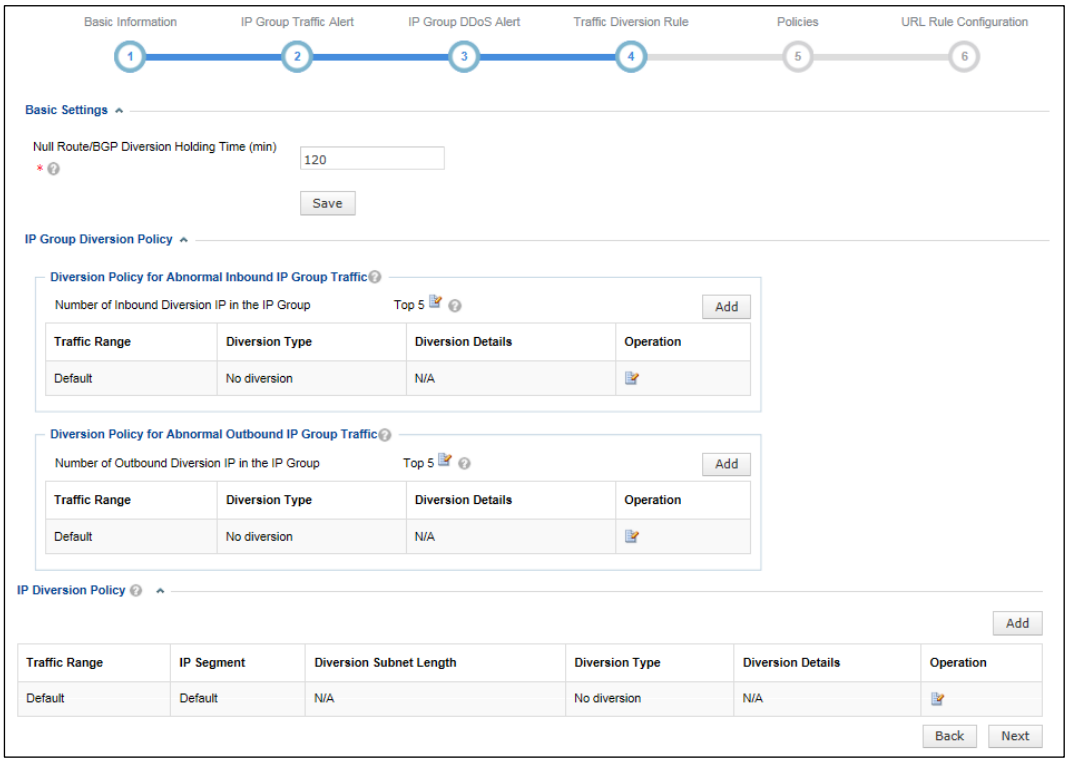



Table 5-9 describes parameters for configuring traffic diversion rules for an IP group.

Table 5-9 Parameters for configuring diversion rules for an IP group

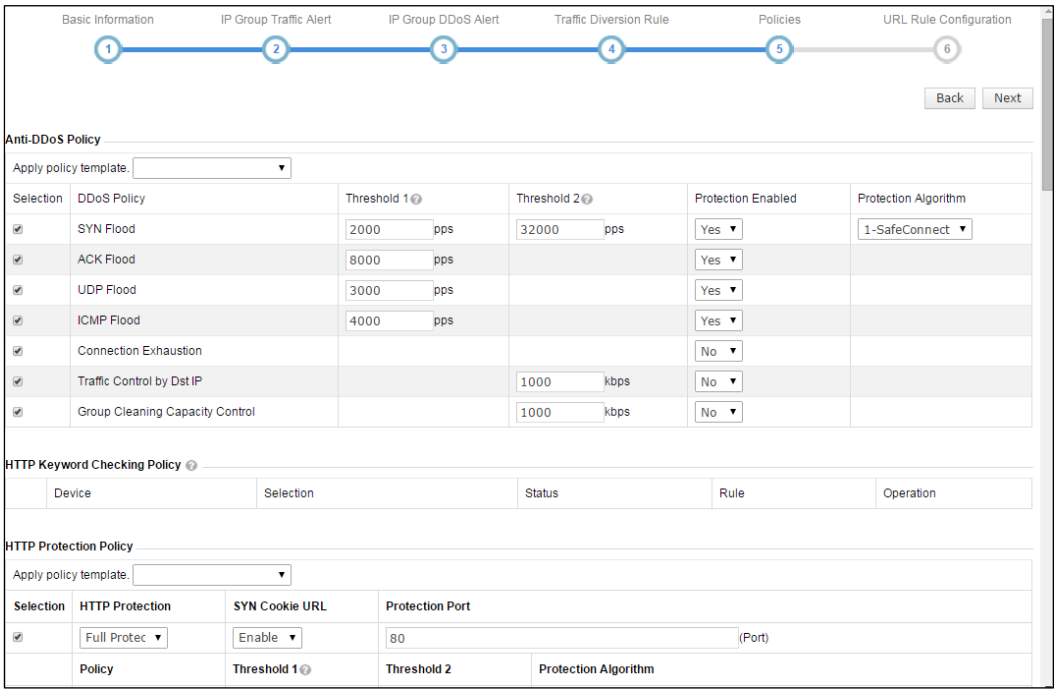
| Parameter | | Description |
|---|---|---|
| Basic Settings | Null Route/BGP Diversion Holding Time (min) | After sending a "Null route/BGP diversion" notification to a device, NTA will start a countdown to the revocation of the involved route. Once the diversion holding time expires, NTA revokes the route. |
| IP Group Diversion Policy | 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.<br>• 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**.<br>• When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set.<br>**Note**<br>The diversion policy for a region has a lower priority than that for an IP group.<br>• When the **Diversion Policy for Abnormal Inbound IP Group Traffic** is triggered, NTA can perform null route diversion for the top N IP addresses or all IP addresses (**Any**) in an IP group. N stands for a variable ranging from 1 to 200. The system sorts top N IP addresses every 5 minutes. |

| Parameter | | Description |
|---|---|---|
| | | • You can click **Add** and add new diversion policies. |
| | 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.<br>• 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**.<br>• When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set.<br>Note<br>The diversion policy for a region has a lower priority than that for an IP group.<br>• When **Diversion Policy for Abnormal Region Outbound Traffic** is triggered, NTA can perform null route diversion for top N IP addresses. N stands for a variable ranging from 1 to 200. The system sorts top N IP addresses every 5 minutes.<br>• You can click **Add** and add new diversion policies. |
| IP Diversion Policy | | Specifies the diversion policy for IP addresses in a region when the DDoS alert is triggered.<br>• **IP Diversion Policy** can be triggered together with the **Diversion Policy for Abnormal Inbound Region Traffic** and **Diversion Policy for Abnormal Outbound Region Traffic**.<br>• When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set.<br>• You can click **Add** and add new diversion policies. |

**Step 6** Configure IP group protection policies.

After configuring traffic diversion rules, click **Next** to open the **Policies** page.

Figure 5-17 Configuring IP group protection policies

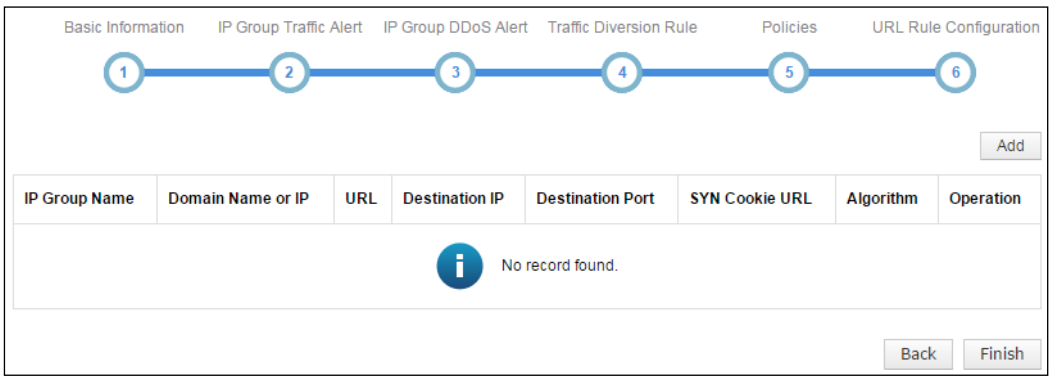



To edit protection policies, you can directly modify default settings or use policy templates. The method of configuring policies on ADS M is the same as that for policies on ADS devices. For details, see *NSFOCUS ADS User Guide*.

**Step 7** Configure URL rules.

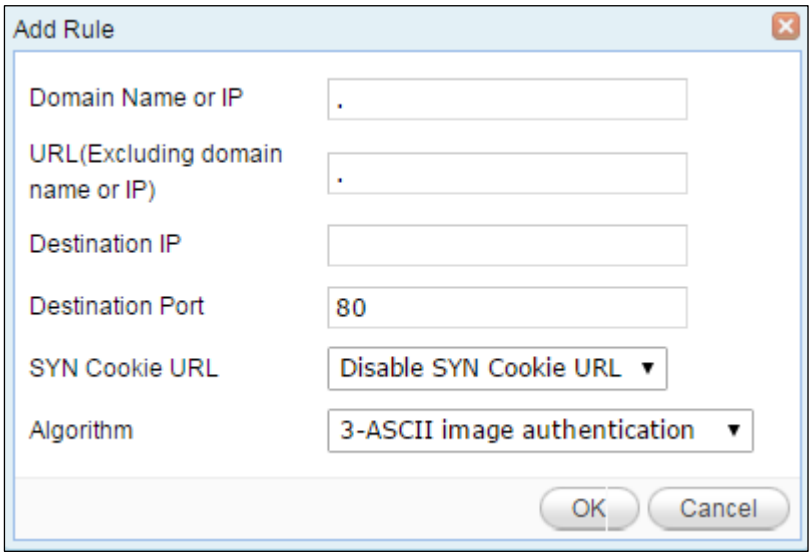
After configuring policies, click **Next** to open the **URL Rule Configuration** page.

Figure 5-18 Configuring a URL rule




a. Click **Add**.

Figure 5-19 Adding a URL rule




b. In the **Add Rule** dialog box, configure URL rule parameters.

Table 5-10 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 | Algorithm of the URL rule. Nine algorithms are available for you to select. |

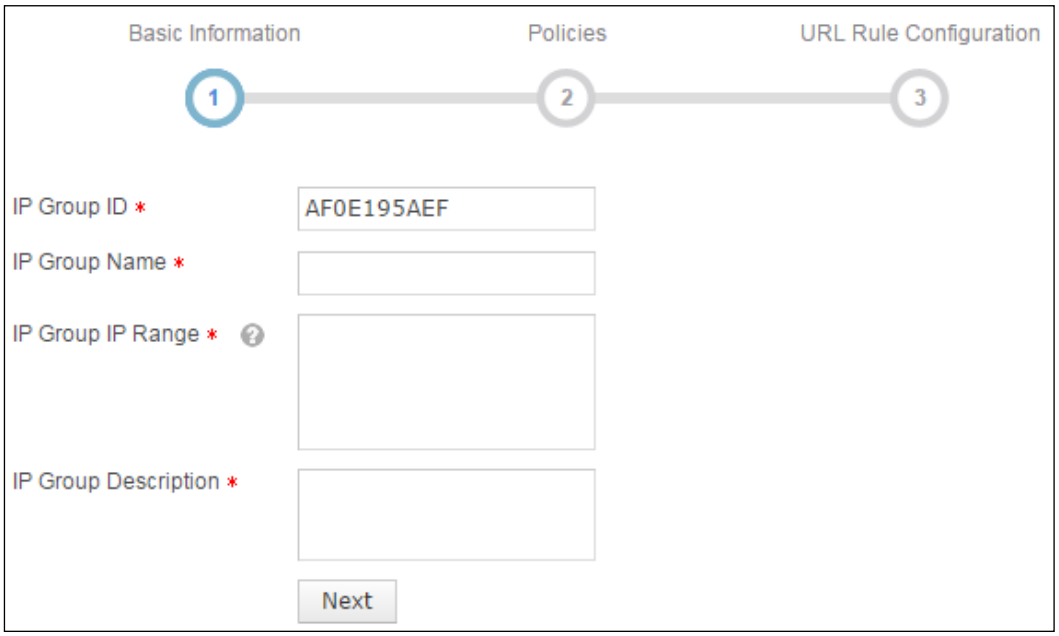
**Step 8** After configuring the URL rule, click **Finish**.

**----End**

### 5.4.1.2 "None" Detection Mode

**Step 1** Click **Add IP Group** on the page shown in Figure 5-12.

Figure 5-20 Adding an IP group in "None" detection mode



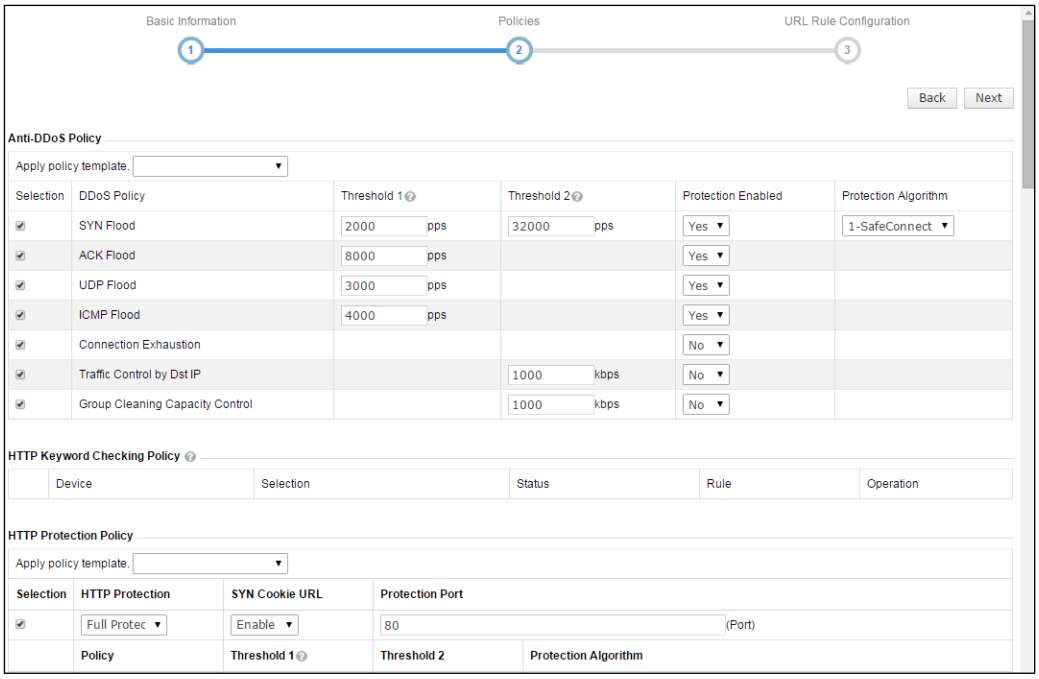

**Step 2** Configure basic information for adding an IP group.

For the description of parameters for configuring basic information, see Table 5-8.

**Step 3** Configure IP group protection policies.

After configuring basic information, click **Next** to open the **Policies** page.

Figure 5-21 Configuring IP group protection policies in "None" detection mode

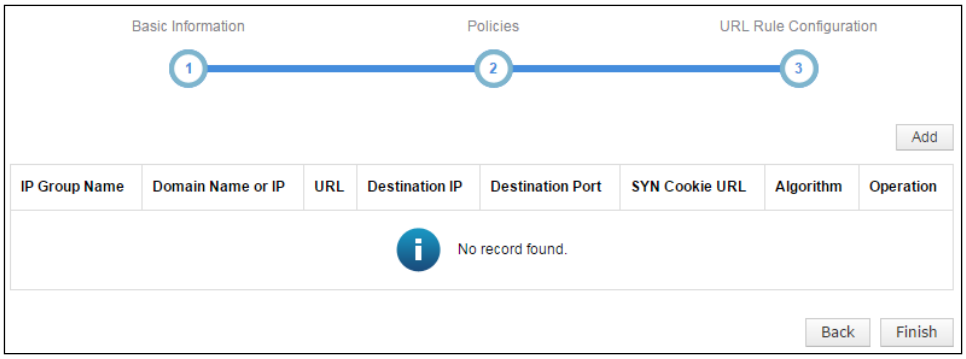


To edit protection policies, you can directly modify default settings or use policy templates. The method of configuring policies on ADS M is the same as that for policies on ADS devices. For details, see *NSFOCUS ADS User Guide*.

**Step 4** Configure URL rules.

After configuring policies, click **Next** to open the **URL Rule Configuration** page.

Figure 5-22 Configuring URL rules in "None" detection mode




For details about configuring a URL rule, see Step 7 in section 5.4.1.1.

**Step 5** After configuring the URL rule, click **Finish**.

**----End**

## 5.4.2 Modifying a Region IP Group

On the region IP group list, click in the row of a region IP group to modify parameters (except the IP group ID) of the region IP group.

| | |
|---|---|
| Note | For region 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. |

## 5.4.3 Deleting a Region IP Group

On the region IP group list, click in the row of a region IP group to delete the IP group.

| | |
|---|---|
| Caution | • Deleting a region IP group stops you from continuing to view the opened monitoring page, configuration page, or other pages related to this group.<br>• 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. |

### 5.4.4 Viewing Configuration Information of a Region IP Group

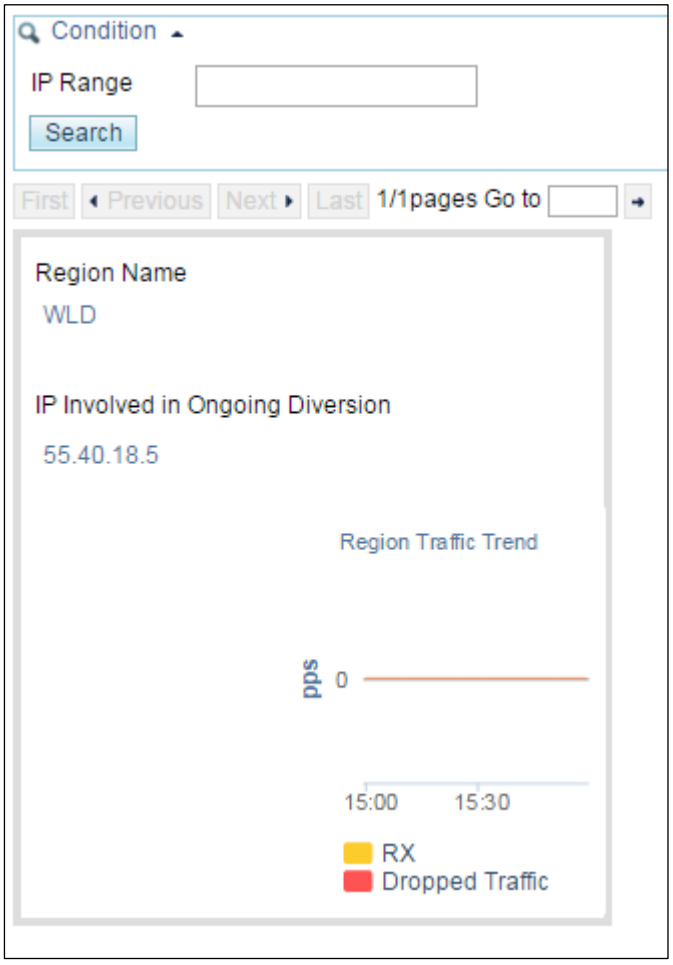
On the region IP group list, click in the row of a region IP group to view the configuration information of the IP group.

## 5.5 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 5-23 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."

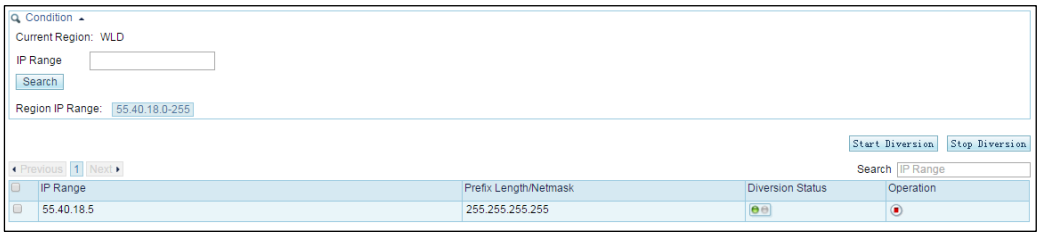
Figure 5-23 Region traffic diversion



## 5.5.1 Viewing the Region Under Traffic Diversion

You can click the region name on the page shown in Figure 5-23 to view the IP address range of this region and the IP address under traffic diversion, as shown in Figure 5-24. Note that only the IP addresses within this region in question can be retrieved.

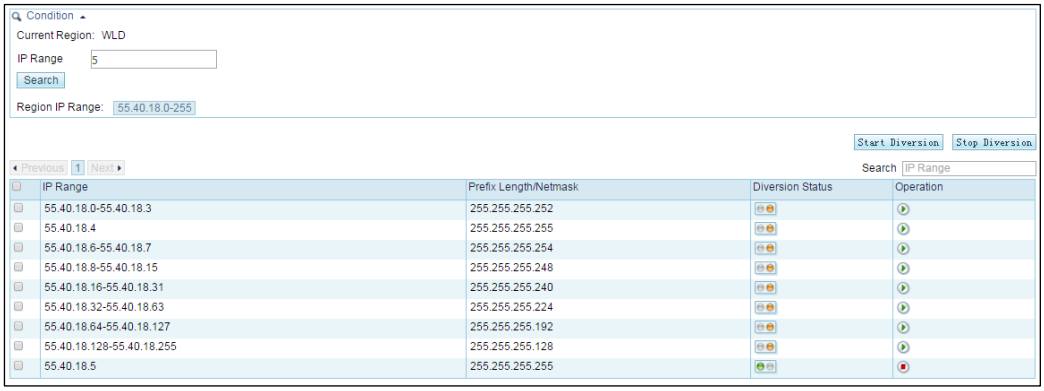
Figure 5-24 Viewing the region under traffic diversion




## 5.5.2 Configuring IP Addresses for Diversion

On the page shown in Figure 5-24, 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 5-25 Searching for IP addresses whose traffic can be diverted




- 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. |

# 6 Device Management

The Device Management module allows you to configure related parameters and protection policies in a centralized way for all devices under ADS M.

## 6.1 Managing Devices

This section 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.

### 6.1.1 Configuring an ADS Device

To configure an ADS device, perform the following steps:

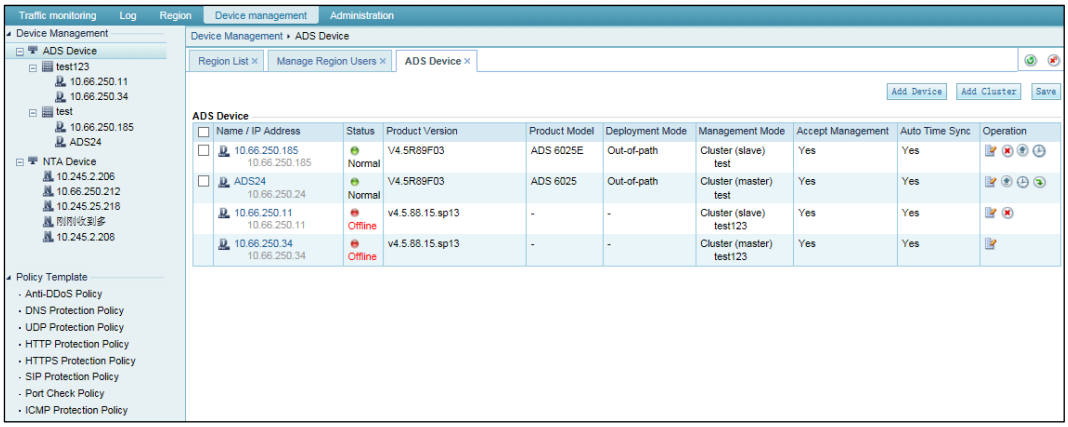
**Step 1** Click **Device Management** > **ADS Device**.

The **ADS Device** page appears, as shown in Figure 6-1.

The ADS device list consists of ADS devices and clusters. Initially, the device list is empty and you need to add devices or clusters manually.

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 6-1 ADS Device page



**Step 2** Click a device to edit its policy settings.

**----End**

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 *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 tree structure of monitoring objects.

## Adding an ADS Device

To add an ADS device, perform the following steps:

**Step 1** Click **Add Device** in the upper-right corner of the **ADS Device** page shown in Figure 6-1.

The dialog box for adding an ADS device appears, as shown in Figure 6-2.

Figure 6-2 Adding an ADS device

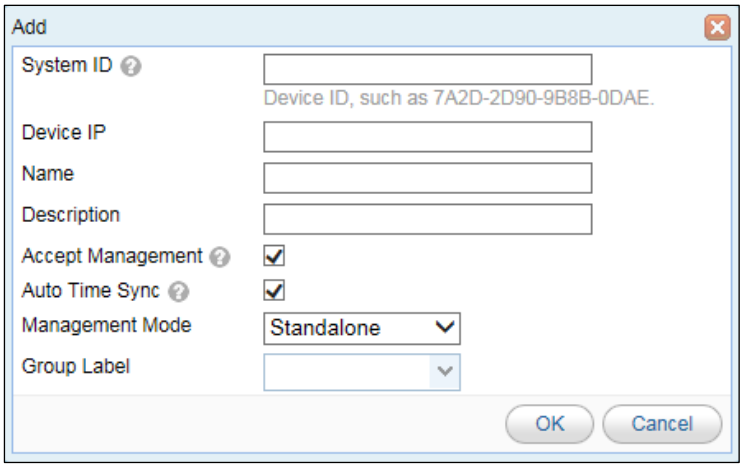



Table 6-1 describes parameters of an ADS device.

Table 6-1 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. |
| Accept Management | Controls whether this device is subject to the management of ADS M. By default, this option is selected. |

| Parameter | Description |
|---|---|
| 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**. After an ADS device is successfully added, ADS M automatically obtains the ADS deployment mode such as in-path or out-of-path mode. |
| Group Label | Specifies the label of the group to which the device belongs. The device tree in the left part displays devices by groups. |

**Step 2** Set the parameters in the dialog box, and click **OK.**

**----End**

## Modifying ADS Device Settings

On the **ADS Device page**, click in the **row of** an ADS device to modify information about the device, except device ID.

## Deleting an ADS Device

On the **ADS Device page**, click in the **row of** an ADS device to delete the device. Once an ADS device is deleted, it is no longer subject to management of ADS M nor will it upload the device information to ADS M.

| | |
|---|---|
| Caution | Once a device is deleted, you cannot continue to view opened monitoring page, configuration page, or other pages that relate to this device. In a cluster, the master device cannot be deleted except that the cluster has only one device. |

## 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 turns orange, notifying you of time inconsistency.<br>• Inconsistent system time between two devices may impair the accuracy of statistical reports and device logs.<br>• You are advised to ensure consistent time between ADS devices and the ADS M device through the NTP service. |

### 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 6-1 to save the settings of selected devices.

| | |
|---|---|
| Caution | Pay attention to the followings when saving the configuration:<br>• Time synchronization and configuration saving can be performed on online ADS devices only.<br>• 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. |

## 6.1.2 Configuring an ADS Cluster

ADS cluster (that is, device group) facilitates centralized management and configuration of multiple ADS devices. In ADS cluster mode, after the administrator configures 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.

### Adding an ADS Cluster

To add an ADS cluster, perform the following steps:

**Step 1** Click **Add Cluster** in the upper-right corner of the **ADS Device page**.

The **ADS Cluster** dialog box appears, as shown in Figure 6-3.

Figure 6-3 Adding an ADS cluster

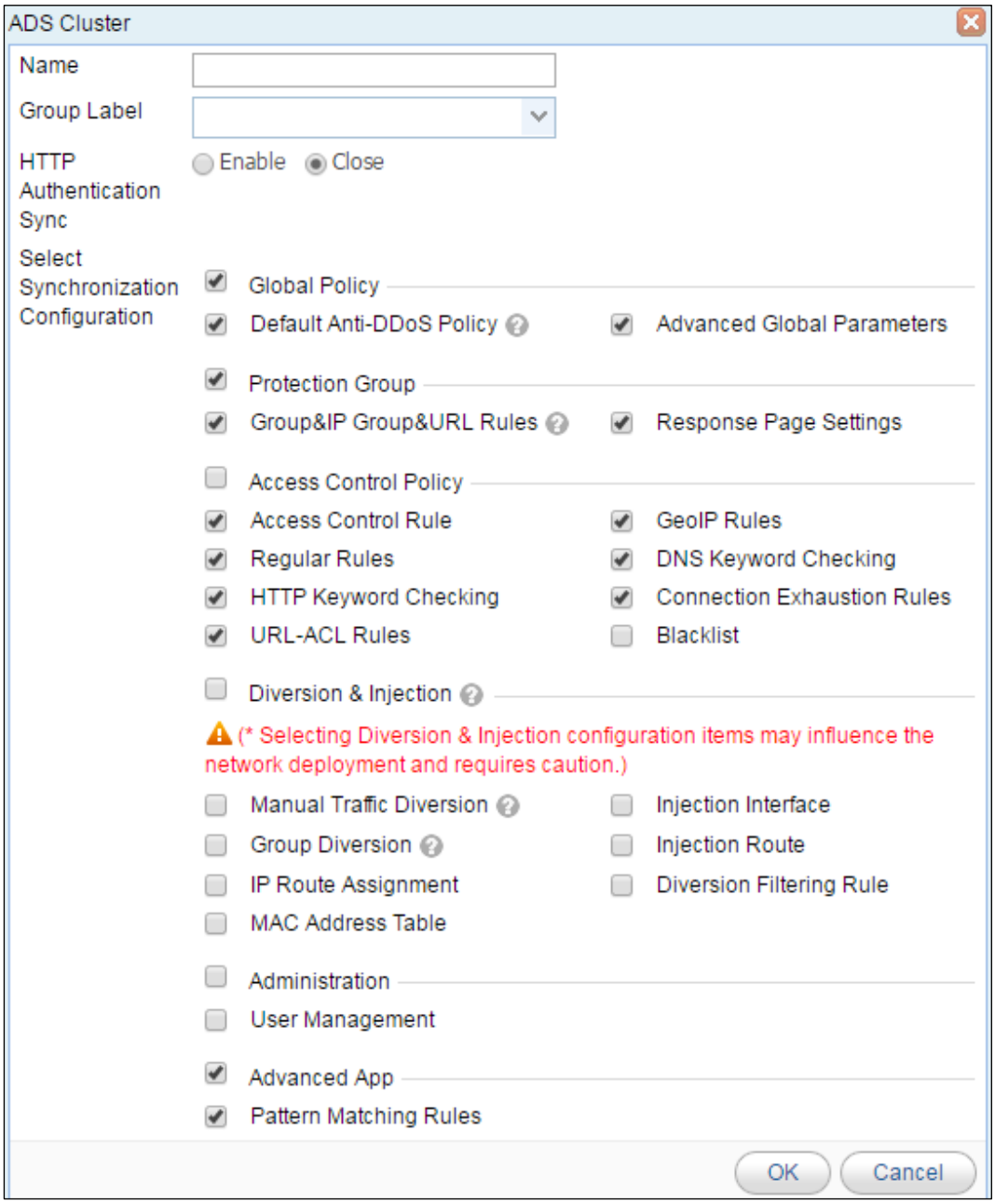



Table 6-2 describes parameters of an ADS cluster.

Table 6-2 ADS cluster parameters

| Parameter | Description |
|---|---|
| Name | Specifies the ADS cluster name.<br>It must be 1 to 20 characters long and cannot contain angle brackets (<, or >), quotation marks (" or '), or slashes (/).<br>The ADS cluster name is mandatory and must be unique. |

| Parameter | | Description |
|---|---|---|
| Group Label | | Specifies the group label for an ADS cluster<br>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.<br>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. |

| | |
|---|---|
| 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 click **OK**.

Then, the new ADS cluster is displayed on the treelike device list.

**----End**

## Adding an ADS Device to a Cluster

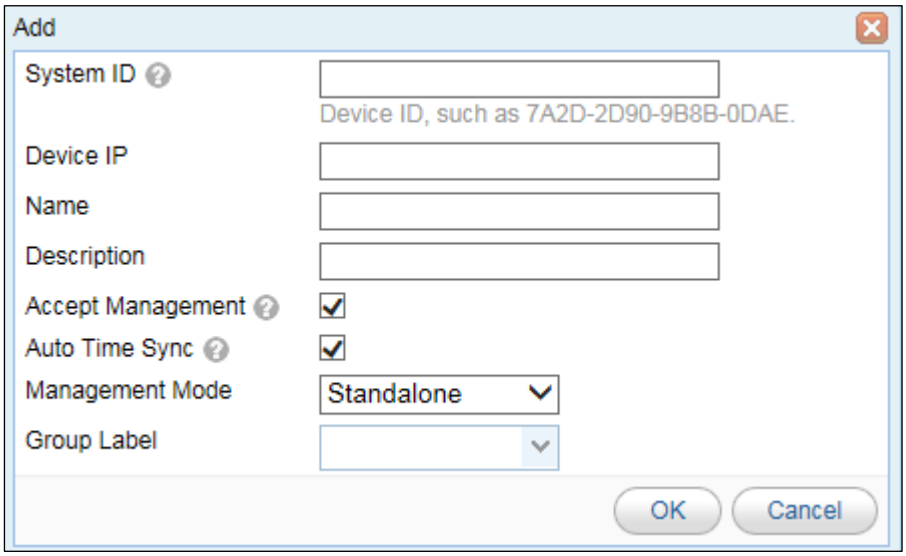
To configure an ADS device in a cluster, perform the following steps:

**Step 1** Click a cluster name on the left tree device list.

The ADS cluster configuration page appears.

**Step 2** Click **Add Device**.

Figure 6-4 Adding an ADS device to the cluster



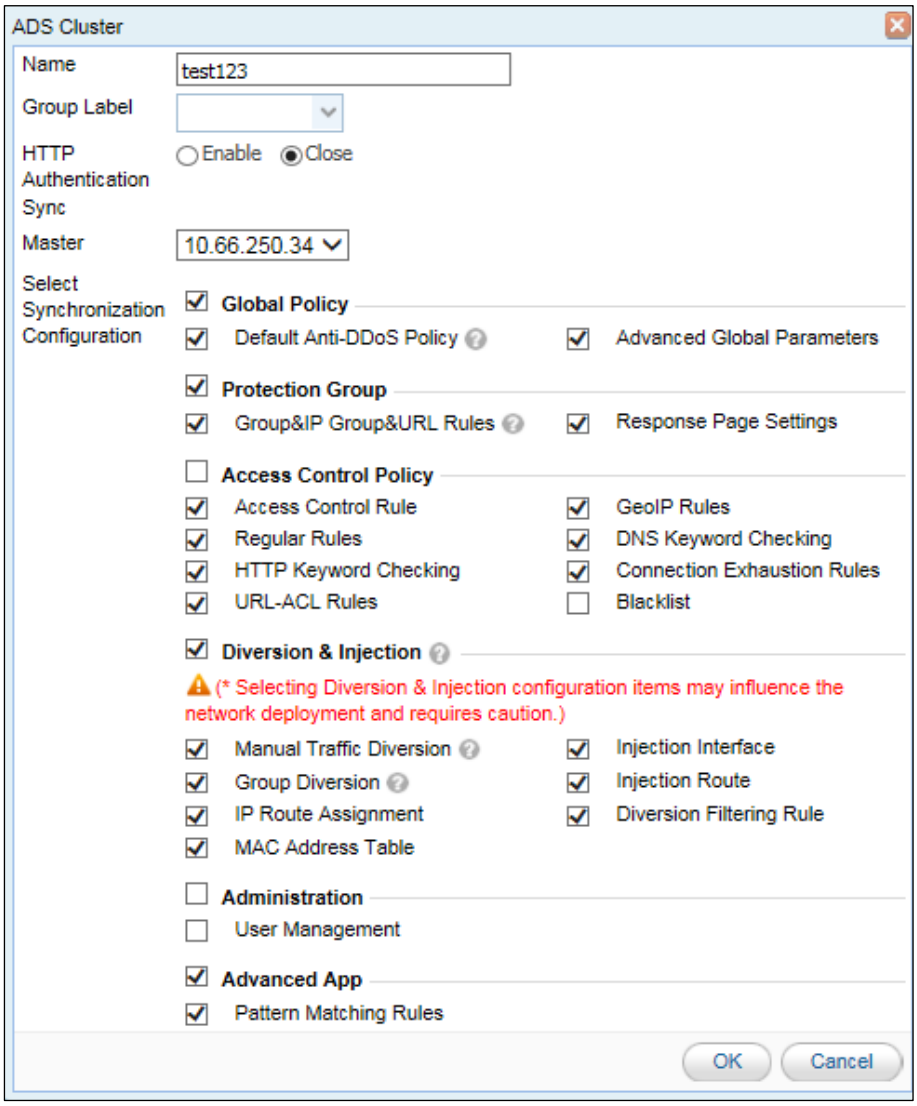

**Step 3** Set parameters in the dialog box and click **OK**.

**----End**

## Modifying an ADS Cluster

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 6-5.

Figure 6-5 Modifying an ADS cluster




| | |
|---|---|
| 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.<br>• 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. |

## Deleting an ADS Cluster

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.<br>• In a cluster, the master device cannot be deleted except that the cluster has only one device. |

## 6.1.3 Configuring an NTA Device

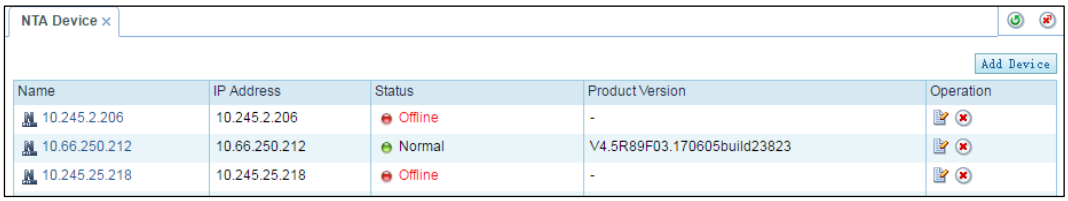
To configure an NTA device, perform the following steps:

**Step 1** Click **NTA Device** under **Device Management**.

The **NTA Device** page appears, as shown in Figure 6-6. 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 6-6 NTA Device page




**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 *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.

**----End**

### Adding an NTA Device

To add an NTA device, perform the following steps:

**Step 1** Click **Add Device** in the upper-right corner of the **NTA Device** page.

A dialog box for adding an NTA device is displayed. See Figure 6-7.

Figure 6-7 Adding an NTA device


Table 6-3 describes parameters of an NTA device.

Table 6-3 NTA device parameters

| Parameter | Description |
|---|---|
| System ID | Specifies the system ID of an NTA device.<br>This parameter is mandatory. |
| Device IP | Specifies the IP address of an NTA device.<br>Either an IPv4 or IPv6 address is acceptable. This parameter is mandatory. |
| Name | Specifies the name of an NTA device.<br>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 V4.5R89F03.<br>It must be the same as the authorization key configured on the web-based manager (**Administration > Third-Party Interface > Management Mode**) of NTA.<br>**Note**<br>NTA V4.5.61.2 does not require the management password. |
| Description | Specifies the brief description of an NTA device, for example, device usage. |

**Step 2** Set parameters in the dialog box and click **OK**.

**----End**

## Modifying NTA Device Settings

On the **NTA Device** page, click in the row of an NTA device to modify the information about the device. Note that the device ID cannot be edited.

### Deleting an NTA Device

On the **NTA Device** page, click in the row of an NTA device to delete the device. After an NTA device is deleted, it is no longer subject to management of ADS M, nor will it upload the 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. |

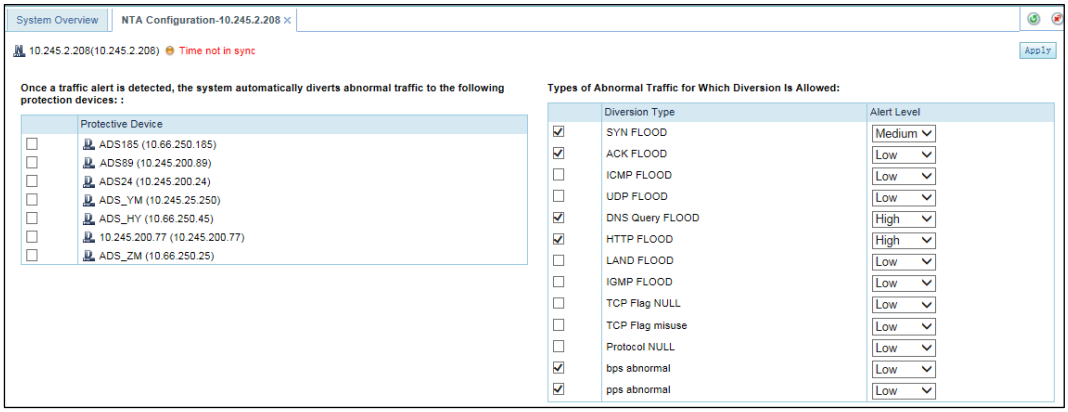
After adding an NTA device, you need to configure traffic diversion settings before the interaction between ADS and NTA devices. For details, see sections 6.2 Configuring NTA Diversion Settings or 6.3 Configuring an NTA Device.

## 6.2 Configuring NTA Diversion Settings

This section describes how to configure traffic diversion settings of ADS devices and abnormal traffic types that can be diverted on NTA V4.5.61.2. For diversion settings on NTA V4.5R89F03, see section 6.3.4 Configuring Global Diversion Settings.

On the left treelike NTA device list, click an NTA device to open the device configuration page. By default, the current diversion configuration of this device is displayed. See Figure 6-8.

Figure 6-8 Diversion configuration on an NTA device



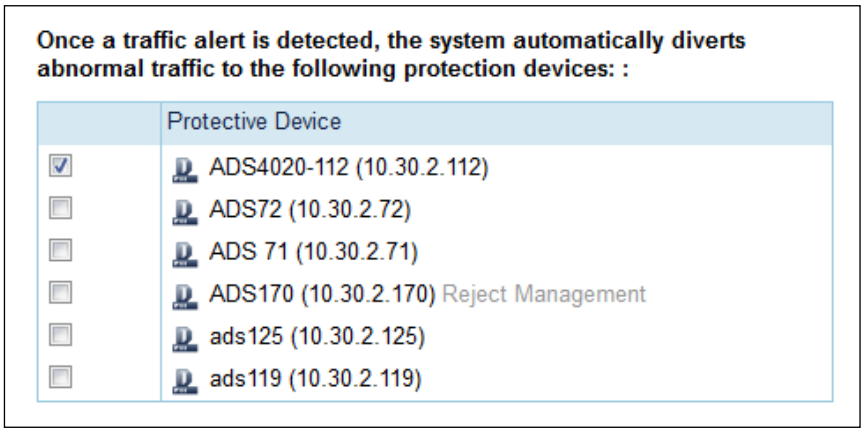

### Configuring Traffic Diversion

On ADS M, you can configure an ADS device for traffic diversion and the type of traffic to be diverted. The detailed procedure is as follows:

**Step 1** Configure an ADS device to which the abnormal traffic is diverted.

As shown in Figure 6-9, select an ADS device (for example, 10.30.2.112). The ADS devices listed as follows are devices on the **ADS Device** page.

Figure 6-9 Configuring an ADS device for traffic diversion

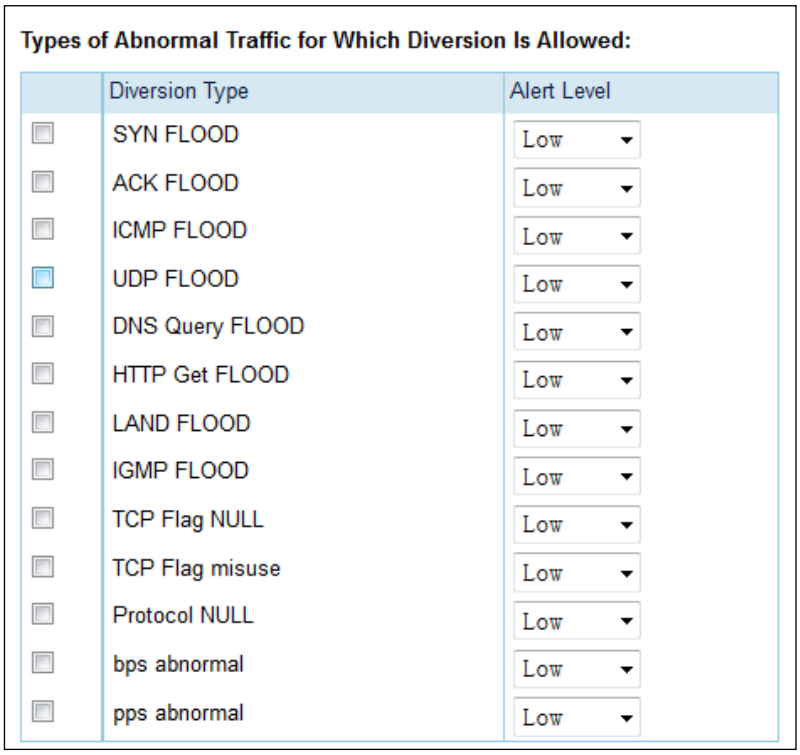



| | |
|---|---|
| Note | • ADS M fails to deliver the configuration information to an ADS device that is not subordinate to it. That is, the setting of the **Probe IP Address** option will not be changed on the ADS device.<br>• Once detecting an abnormal traffic alert, the NTA device delivers a diversion notification to a specific ADS device that will filter out the abnormal traffic and then re-inject it to the network.<br>• If the configured ADS device is not managed by ADS M, you need to configure this device to work under ADS M. For details, see section 6.1.1 Configuring an ADS Device. |

**Step 2** Configure the type of traffic to be diverted.

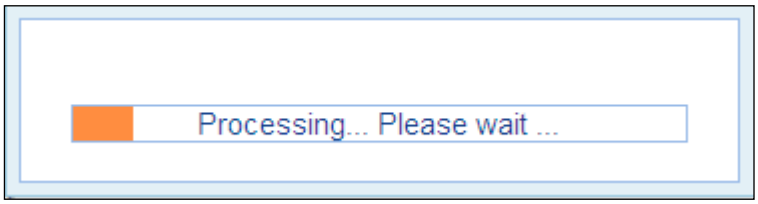
As shown in Figure 6-10, select the abnormal traffic type and the alert level.

Figure 6-10 Configuring the type of traffic to be diverted



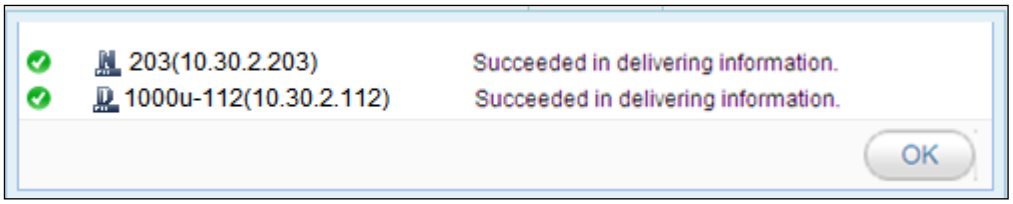

**Step 3** Click **Apply** on the page shown in Figure 6-8 to allow ADS M to deliver the configuration information to the ADS device and NTA device. See Figure 6-11.

Figure 6-11 Delivering the configuration information




After the configuration information is successfully delivered to the ADS device and NTA device, the following dialog box is displayed.

Figure 6-12 Information successfully delivered




**Step 4** Click **OK** to complete the configuration.

The delivered information will overwrite the original information saved on devices.

**----End**

## Verifying Traffic Diversion Configuration

After the traffic diversion configuration is successfully delivered to NTA, verify the configuration on the ADS device and NTA device.

- Verify the configuration on the ADS device as follows:

  Choose **Diversion & Injection** > **General Settings** > **Running Mode** to open the **Running Mode** page, where **Accept Probe Notification** is **Yes** and **Probe IP Address** is **10.30.2.203** (IP address of the NTA device). See Figure 6-13.

Figure 6-13 Running Mode page

Running Mode

**Off-Path Mode Settings**

| Item | Value |
|---|---|
| Running Mode | Diversion |
| Port Mode | Default |
| Accept Probe Notification | Yes |
| Probe IP Address | 10.30.2.203 |
| Probe Running Mode | netflow |
| Arbor Interaction | No |
| Arbor IP Address | |
| Arbor Port | 514 |
| GenieATM Interaction | No |
| GenieATM IP Address | |
| GenieATM Port | 514 |
| | |
| Enable Injection MPLS Label Learning | No |

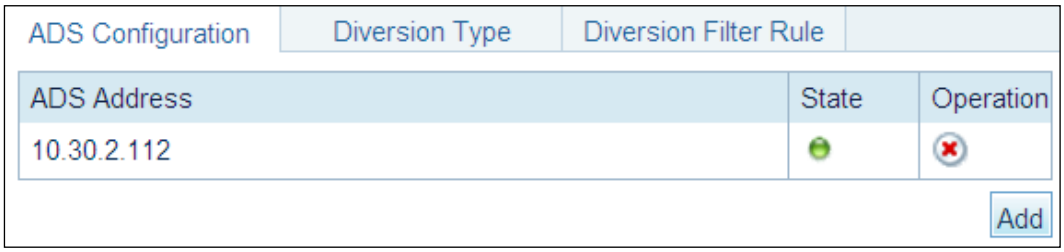
Edit

- Verify the configuration on the NTA device as follows:

**Step 1** Choose **Configuration** > **Traffic Diversion** > **ADS Diversion** > **ADS Configuration** to open the **ADS Configuration** page shown in Figure 6-14.

You can view the ADS device (IP address: 10.30.2.112) on the page.

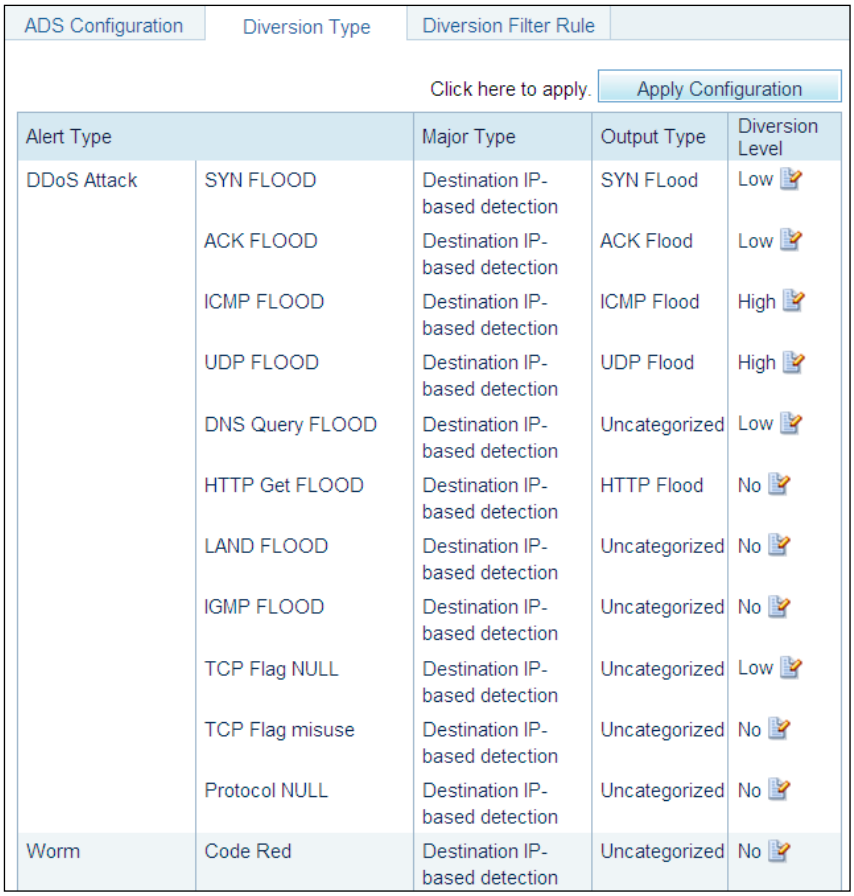
Figure 6-14 ADS Configuration page on the NTA device




**Step 2** Click **Diversion Type** on the page in Figure 6-14 to configure the traffic diversion type, as shown in Figure 6-15.

This page displays the type of traffic to be diverted and diversion event level configured on ADS M.

Figure 6-15 Diversion Type page on the NTA device




| Alert Type | | Major Type | Output Type | Diversion Level |
|---|---|---|---|---|
| DDoS Attack | SYN FLOOD | Destination IP-based detection | SYN FLood | Low |
| | ACK FLOOD | Destination IP-based detection | ACK Flood | Low |
| | ICMP FLOOD | Destination IP-based detection | ICMP Flood | High |
| | UDP FLOOD | Destination IP-based detection | UDP Flood | High |
| | DNS Query FLOOD | Destination IP-based detection | Uncategorized | Low |
| | HTTP Get FLOOD | Destination IP-based detection | HTTP Flood | No |
| | LAND FLOOD | Destination IP-based detection | Uncategorized | No |
| | IGMP FLOOD | Destination IP-based detection | Uncategorized | No |
| | TCP Flag NULL | Destination IP-based detection | Uncategorized | Low |
| | TCP Flag misuse | Destination IP-based detection | Uncategorized | No |
| | Protocol NULL | Destination IP-based detection | Uncategorized | No |
| Worm | Code Red | Destination IP-based detection | Uncategorized | No |

**----End**

## Refreshing Configuration Information on the NTA Device

On the page shown in Figure 6-8, click **Refresh** to synchronize the configured ADS device and traffic diversion type on the NTA device to the current page.

| | |
|---|---|
| Note | Only ADS devices that are added on ADS M can be displayed on the list of protection devices. If the ADS device that is configured on the NTA device is not added to the ADS device list on ADS M, the ADS device is not displayed. |

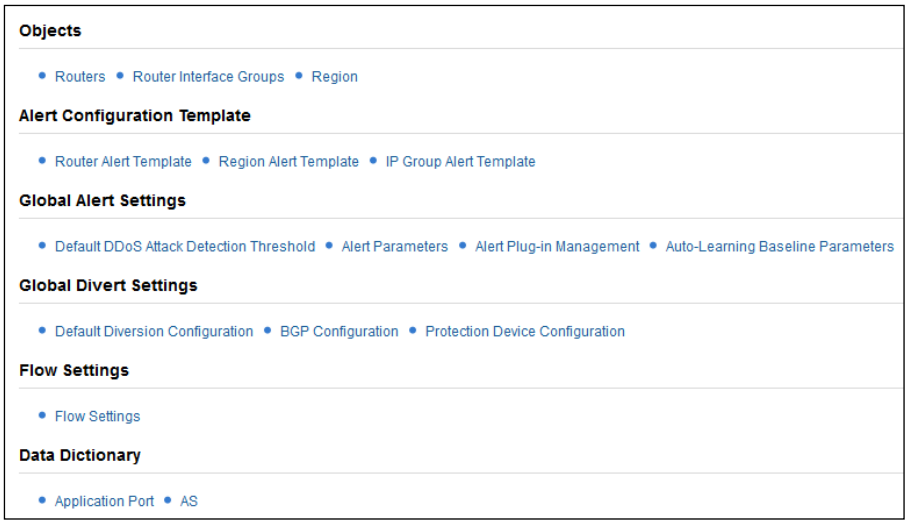
## 6.3 Configuring an NTA Device

On ADS M, the NTA V4.5R89F03 configuration involves the following aspects:

- Configuring Monitoring Objects
- Configuring Alert Configuration Templates
- Configuring Global Alert Settings
- Configuring Global Diversion Settings
- Configuring Flow Collection and Forwarding
- Configuring a Data Dictionary

On the left treelike NTA device list, click a device to open the configuration page. See Figure 6-16.

Figure 6-16 NTA configuration page




This section describes how to configure core settings of NTA on ADS M.

### 6.3.1 Configuring Monitoring Objects

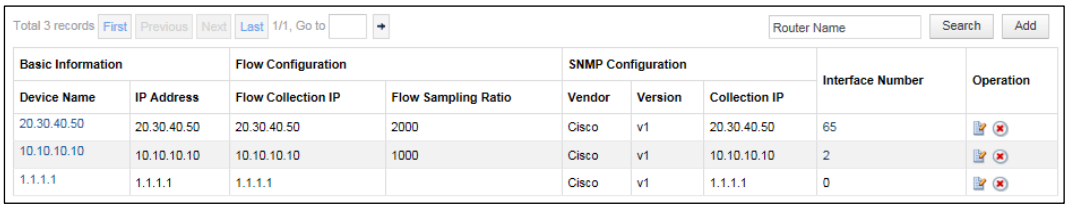
This section describes how to configure objects monitored by NTA, including routers, router interface groups, and regions.

#### 6.3.1.1 Router

By default, NTA does not monitor any devices. If you want NTA to monitor a device, you need to add this device manually.

Click **Routers** under **Objects** on the NTA configuration page shown in Figure 6-16. The router configuration page appears, as shown in Figure 6-17. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Objects** > **Routers** to this page.

Figure 6-17 Router configuration page




Router configuration involves the following tasks:

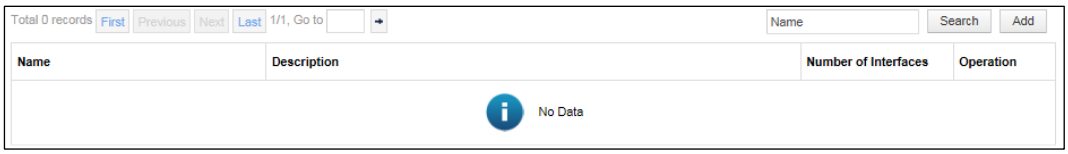
- Configuring router parameters
- Configuring router interfaces

For detailed configuration operations, see *NSFOCUS NTA User Guide*.

### 6.3.1.2 Router Interface Group

Click **Router Interface Groups** under **Objects** on the NTA configuration page shown in Figure 6-16. The router interface group configuration page appears, as shown in Figure 6-18. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Objects** > **Router Interface Groups** to open this page.

Figure 6-18 Router interface group configuration page

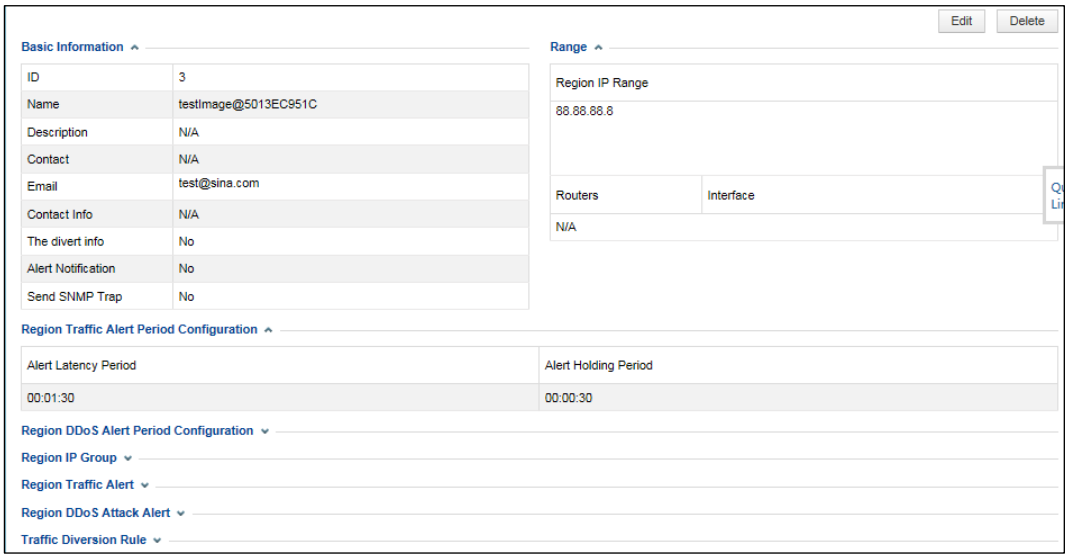



You can add, edit, delete and search for router interfaces as well as add interfaces to interface groups. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

### 6.3.1.3 Region

Click **Region** under **Objects** on the NTA configuration page shown in Figure 6-16. The region configuration page appears, as shown in Figure 6-19. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Objects** > **Region** to open this page.

Figure 6-19 Region configuration page




You can add, edit, delete, and search for regions as well as add IP groups to regions. Region configuration involves the configuration of the following:

- Basic information: configuration of such basic information as the region name and contact person and whether to send a diversion notification, alert notification, or SNMP trap message.
- Range: configuration of IP address ranges or router interfaces to be included in the region.
- Region traffic alert period: configuration of latency period and holding period of alerts for abnormal traffic.
- Region DDoS alert period configuration: configuration of latency period and holding period of alerts for DDoS attacks.
- IP Group: configuration of an IP group for businesses of the same property in the region and configuration of a traffic detection policy for this IP group.
- Region traffic alert: involves the following:
  - Inbound traffic alert policy: configuration of a policy for monitoring the inbound traffic of the entire region so that an alert can be generated when a threshold is exceeded. In addition, you can specify the diversion level to enable diversion of the corresponding inbound traffic.
  - Outbound traffic alert policy: configuration of a policy for monitoring the outbound traffic of the entire region so that an alert can be generated when a threshold is exceeded. In addition, you can specify the diversion level to enable diversion of the corresponding outbound traffic.
- Region DDoS alert: configuration of DDoS attack detection policies for all IP addresses in the region. After an attack is detected, NTA generates an alert if the traffic rate exceeds the threshold. When the alert level reaches the diversion level, the attack traffic will be diverted according to the diversion policy. If you do not configure DDoS attack alert settings, DDoS attacks will be monitored according to default thresholds.
- Traffic diversion rule: involves the following:
  - Inbound traffic diversion policy: configuration of different diversion policies for inbound traffic of different levels to implement abnormal traffic detection for the

entire region. When the specified policy is hit, null route diversion will be conducted for top n IP addresses in the region. In other words, traffic to these IP addresses will be diverted to a null route.

- Outbound traffic diversion policy: configuration of different diversion policies for outbound traffic of different levels to implement abnormal traffic detection for the entire region. When the specified policy is hit, null route diversion will be conducted for top n IP addresses in the region. In other words, traffic from these IP addresses will be diverted to a null route.
- IP diversion policy: configuration of a traffic diversion policy for devices encountering DDoS attacks.

For detailed configuration operations, see *NSFOCUS NTA User Guide*.

## 6.3.2 Configuring Alert Configuration Templates

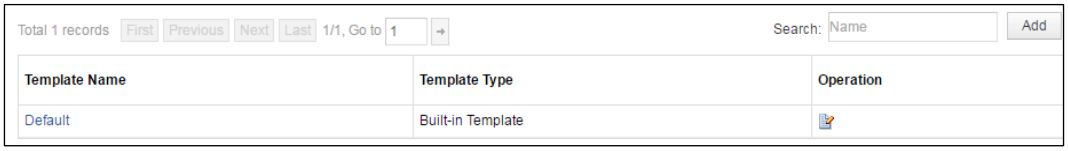
The Alert Configuration Template module allows you to configure common alert templates as required. When configuring a policy, you can directly use a template to define alert parameters. NTA supports the following alert templates:

- Router Alert Template
- Region Alert Template
- IP Group Alert Template

### 6.3.2.1 Router Alert Template

Click **Router Alert Template** under **Alert Configuration Template** on the page shown in Figure 6-16. The router alert template configuration page appears, as shown in Figure 6-20. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Alert Configuration Template** > **Router Alert Template** to open this page.

Figure 6-20 Router alert template configuration page




You can add, edit, and delete router alert templates. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

### 6.3.2.2 Region Alert Template

Click **Region Alert Template** under **Alert Configuration Template** on the page shown in Figure 6-16. The region alert template configuration page appears, as shown in Figure 6-21. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Alert Configuration Template** > **Region Alert Template** to open this page.

Figure 6-21 Region alert template configuration page


You can add, edit, and delete region alert templates. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

### 6.3.2.3 IP Group Alert Template

Click **IP Group Alert Template** under **Alert Configuration Template** on the page shown in Figure 6-16. The IP group alert template configuration page appears, as shown in Figure 6-22. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Alert Configuration Template > IP Group Alert Template** to open this page.

Figure 6-22 IP group alert template configuration page


You can add, edit, and delete IP group alert templates. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

## 6.3.3 Configuring Global Alert Settings

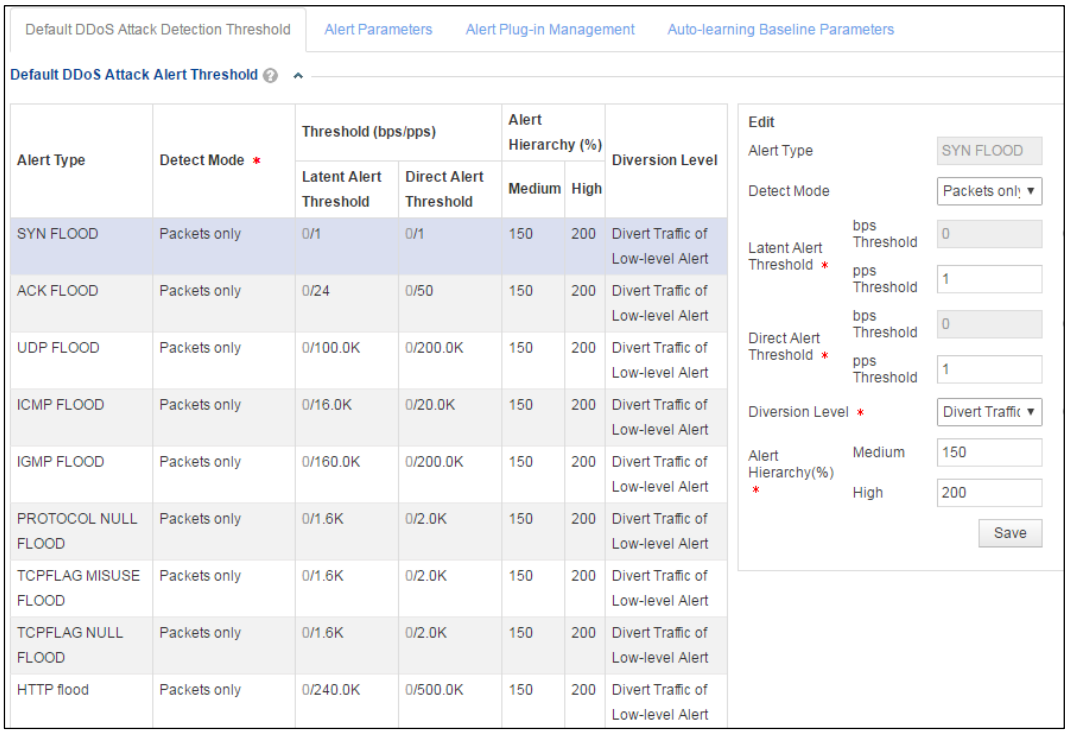
The Global Alert Settings module allows you to configure the following:

- Default DDoS Attack Detection Threshold
- Alert Parameters
- Alert Plug-in Management
- Auto-Learning Baseline Parameters

### 6.3.3.1 Default DDoS Attack Detection Threshold

Click **Default DDoS Attack Detection Threshold** under **Global Alert Settings** on the NTA configuration page shown in Figure 6-16. The page for configuring default DDoS attack detection thresholds appears, as shown in Figure 6-23. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Global Alert Settings > Default DDoS Attack Detection Threshold** to open this page.

Figure 6-23 Default DDoS Attack Detection Threshold page



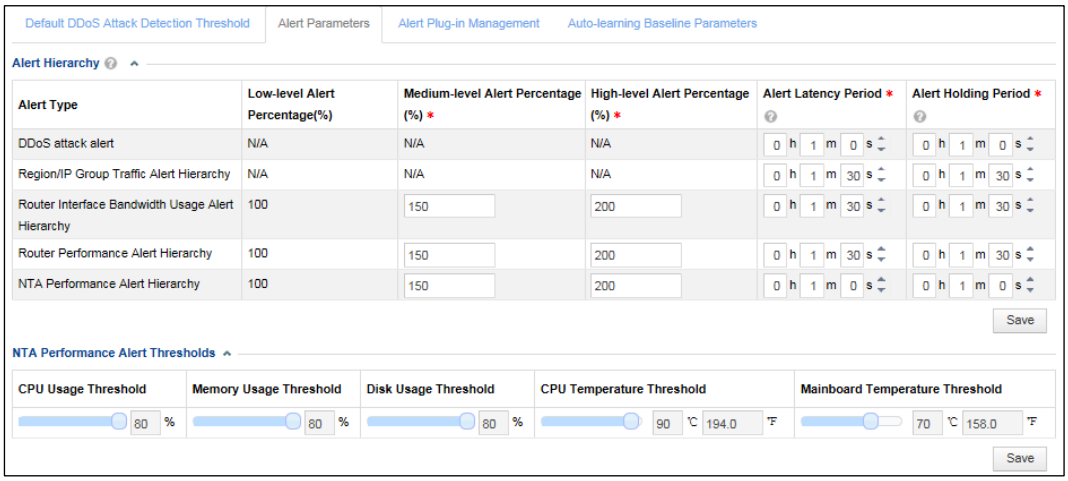

This page shows built-in attack types. For each attack type, you can modify the detection mode, latent alert threshold, direct alert threshold, and diversion level.

For detailed configuration operations, see *NSFOCUS NTA User Guide*.

## 6.3.3.2 Alert Parameters

Click **Alert Parameters** under **Global Alert Settings** on the page shown in Figure 6-16. The alert parameter configuration page appears, as shown in Figure 6-24. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Global Alert Settings** > **Alert Parameters** to open this page.

Figure 6-24 Alert parameter configuration page

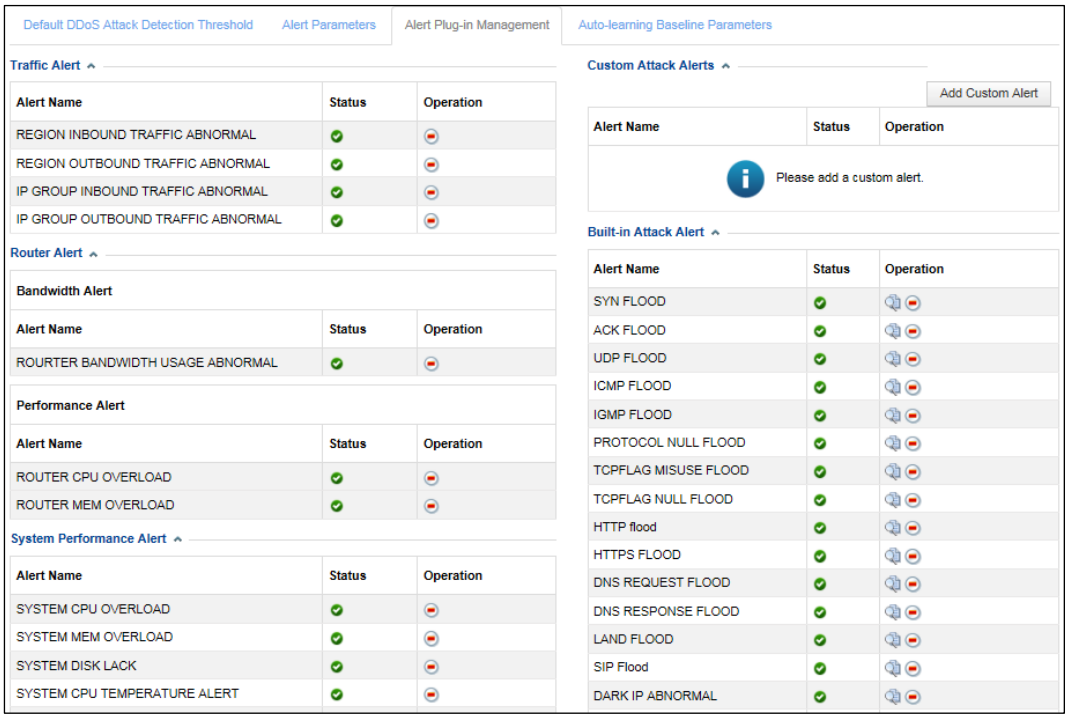



This page shows alert hierarchy policies. In the hierarchy, alert levels are defined by reference to the alert latency threshold. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

## 6.3.3.3 Alert Plug-in Management

Click **Alert Plug-in Management** under **Global Alert Settings** on the page shown in Figure 6-16. The **Alert Plug-in Management** page appears, as shown in Figure 6-25. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Global Alert Settings > Alert Plug-in Management** to open this page.

Figure 6-25 Alert Plug-in Management page



NTA has the following alert plug-ins:

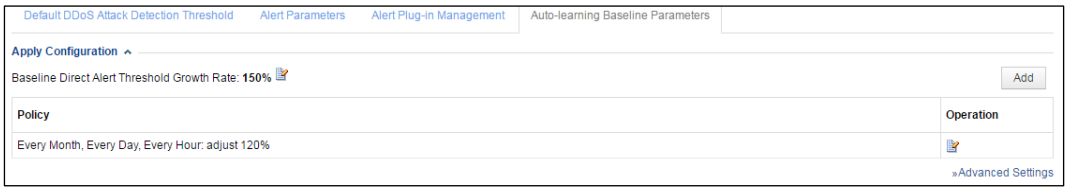
- Traffic alert plug-in: checks whether inbound and outbound traffic of a region or an IP group is abnormal.
- Router alert plug-in: checks whether the router interface usage and performance are abnormal.
- System performance alert plug-in: checks whether the NTA system performance (including the CPU usage, memory usage, and disk space usage) is abnormal.
- Attack alert plug-ins, classified into the following:
  - Custom attack alert plug-in: contains user-defined attack signatures.
  - Built-in attack alert plug-in: contains common attack signatures.

Each type of plug-in contains child plug-ins. You can enable or disable a child plug-in. After a child plug-in is disabled, the corresponding detection policy will not take effect. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

### 6.3.3.4 Auto-Learning Baseline Parameters

Click **Auto-learning Baseline Parameters** under **Global Alert Settings** on the page shown in Figure 6-16. The page for configuring auto-learning baseline parameters appears, as shown in Figure 6-26. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Global Alert Settings > Auto-learning Baseline Parameters** to open this page.

Figure 6-26 Auto-learning Baseline Parameters page




You can add, edit, delete, and sort auto-learning baseline parameters. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

## 6.3.4 Configuring Global Diversion Settings

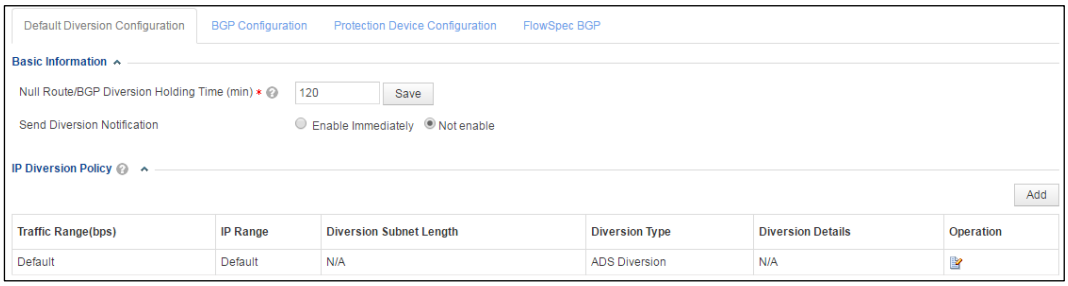
The Global Divert Settings module allows you to configure the following:

- Default Diversion Configuration: configuration of a default policy for diverting attack traffic that does not match any policies
- BGP Configuration: configuration of BGP diversion and null route diversion parameters
- Protection Device Configuration: configuration of ADS or a third-party protection device

### 6.3.4.1 Default Diversion Configuration

Click **Default Diversion Configuration** under **Global Divert Settings** on the page shown in Figure 6-16. The default diversion configuration page appears, as shown in Figure 6-27. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Global Divert Settings > Default Diversion Configuration** to open this page.

Figure 6-27 Default Diversion Configuration page

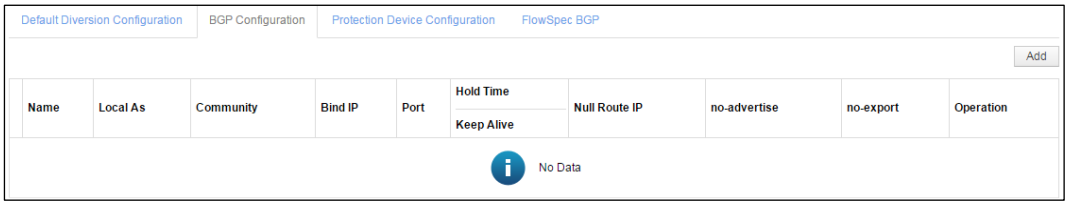



You can add, edit, delete, and sort diversion policies. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

## 6.3.4.2 BGP Configuration

Click **BGP Configuration** under **Global Divert Settings** on the page shown in Figure 6-16. The BGP configuration page appears, as shown in Figure 6-28. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Global Divert Settings** > **BGP Configuration** to open this page.

Figure 6-28 BGP Configuration page




You can create, edit, and delete BGP sessions as well as view the session application and the list of IP addresses for diversion via BGP sessions. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

## 6.3.4.3 Protection Device Configuration

Click **Protection Device Configuration** under **Global Divert Settings** on the page shown in Figure 6-16. The protection device configuration page appears, as shown in Figure 6-29. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Global Divert Settings** > **Protection Device Configuration** to open this page.

Figure 6-29 Protection Device Configuration page

A protection device is either an ADS or a third-party protection device. You can add, edit, and delete protection devices as well as view the usage of third-party devices. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

## 6.3.5 Configuring Flow Collection and Forwarding

Click **Flow Settings** on the NTA configuration page shown in Figure 6-16. The Flow collection and forwarding configuration page appears, as shown in Figure 6-30. Alternatively, you can right-click an NTA device on the left treelike device list and select **Flow Settings** to open this page.

Figure 6-30 Flow collection and forwarding configuration page

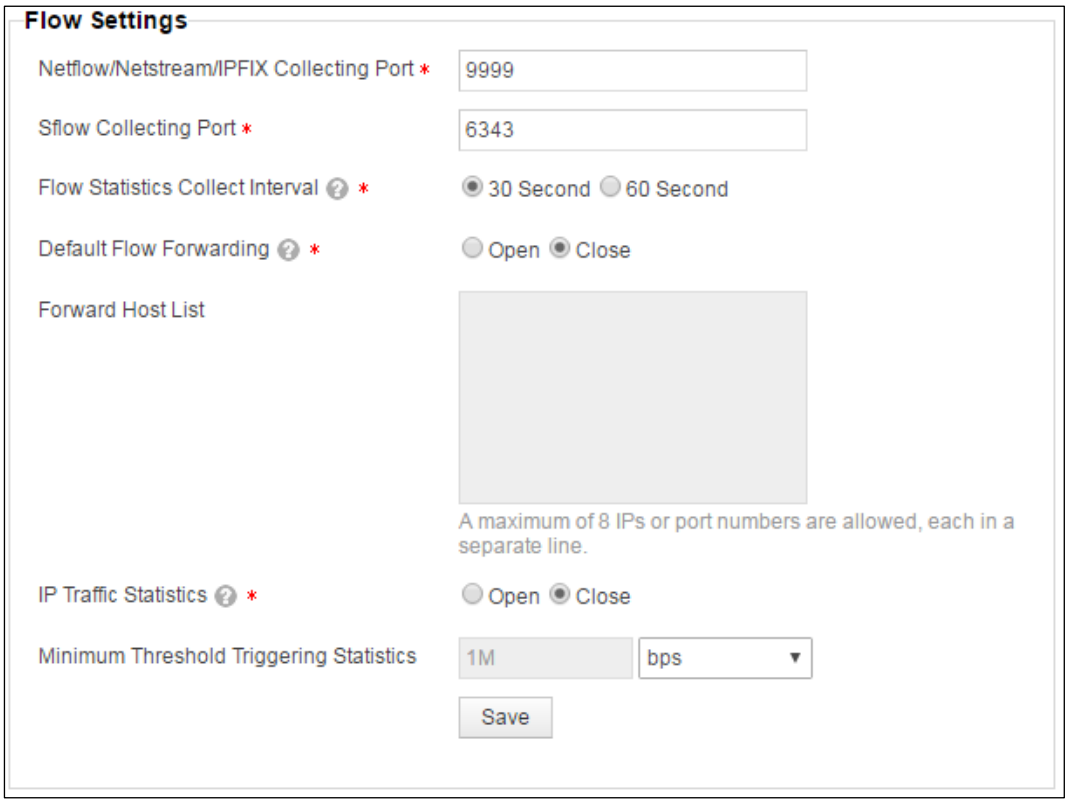



Table 6-4 describes parameters for Flow data collection and forwarding.

Table 6-4 Parameters of Flow data collection and forwarding

| Parameter | Description |
|---|---|
| Net flow/Netstream/IPFIX Collecting Port | Specifies the number of port on which NetFlow packets, NetStream packets, and IPFIX packets are collected.<br>The default value is **9999**. |
| Sflow Collecting Port | Specifies the number of port on which sFlow packets are collected.<br>The default value is **6343**. |
| Flow Statistics Collect Interval | Specifies the interval at which Flow statistics are collected, which can be **30 Second** or **60 Second**. |

| Parameter | Description |
|---|---|
| Default Flow Forwarding | Controls whether NTA forwards the received Flow data. By default, the Flow data is not forwarded. When this parameter is set to **Open**, you must specify the **Forward Host List**. |
| Forward Host List | Specifies the destination IP address and port number for Flow data forwarding. This parameter is required only when **Default Flow Forwarding** is set to **Open**. |
| IP Traffic Statistics | Controls whether NTA collects statistics on IP traffic. By default, statistics on IP traffic are not collected. When this parameter is set to **Open**, you must set **Minimum Threshold Triggering Statistics**. |
| Minimum Threshold Triggering Statistics | Specifies the threshold of IP traffic within a statistical period, above which the statistical result of IP traffic will be displayed on NTA's web-based manager. |

For detailed configuration operations, see *NSFOCUS NTA User Guide*.

## 6.3.6 Configuring a Data Dictionary

The Data Dictionary module allows you to define common applications and Autonomous Systems (ASs), whose information will be intuitively displayed on the web-based manager. A data dictionary consists of either of the following:

- Application Port
- AS

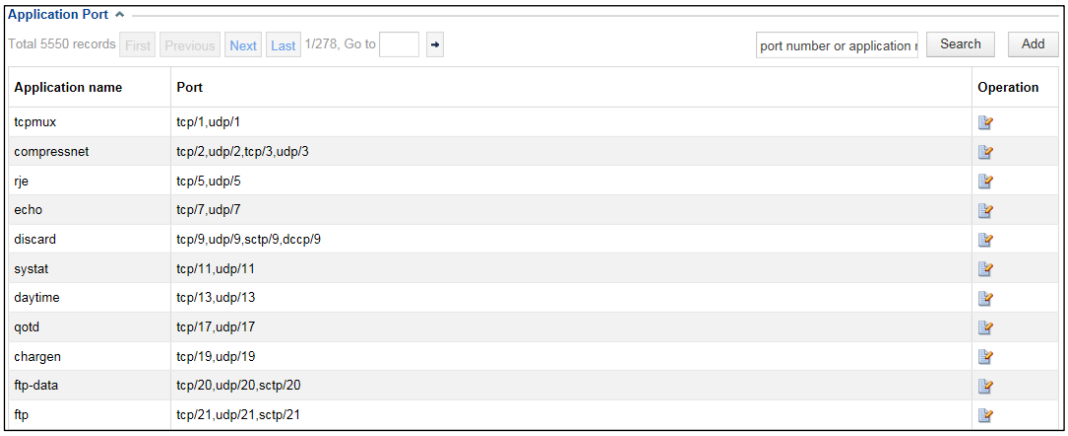
### 6.3.6.1 Application Port

Click **Application Port** under **Data Dictionary** on the page shown in Figure 6-16. The application port configuration page appears, as shown in Figure 6-31. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Data Dictionary > Application Port** to open this page.

After an application is defined with both the protocol name and port number, the application name will be displayed in the **Top5 Applications Traffic** chart of a router or region under **Monitor > Routers** or **Monitor > Regions** on the web-based manager of NTA. An application can be either of the following:

- Built-in application: can be edited, but cannot be deleted.
- Custom application: can be added, modified, and deleted.

Figure 6-31 Application port configuration page




| Application name | Port | Operation |
|---|---|---|
| tcpmux | tcp/1,udp/1 | |
| compressnet | tcp/2,udp/2,tcp/3,udp/3 | |
| rje | tcp/5,udp/5 | |
| echo | tcp/7,udp/7 | |
| discard | tcp/9,udp/9,sctp/9,dccp/9 | |
| systat | tcp/11,udp/11 | |
| daytime | tcp/13,udp/13 | |
| qotd | tcp/17,udp/17 | |
| chargen | tcp/19,udp/19 | |
| ftp-data | tcp/20,udp/20,sctp/20 | |
| ftp | tcp/21,udp/21,sctp/21 | |

You can add, edit, delete, and search for application ports. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

### 6.3.6.2 AS

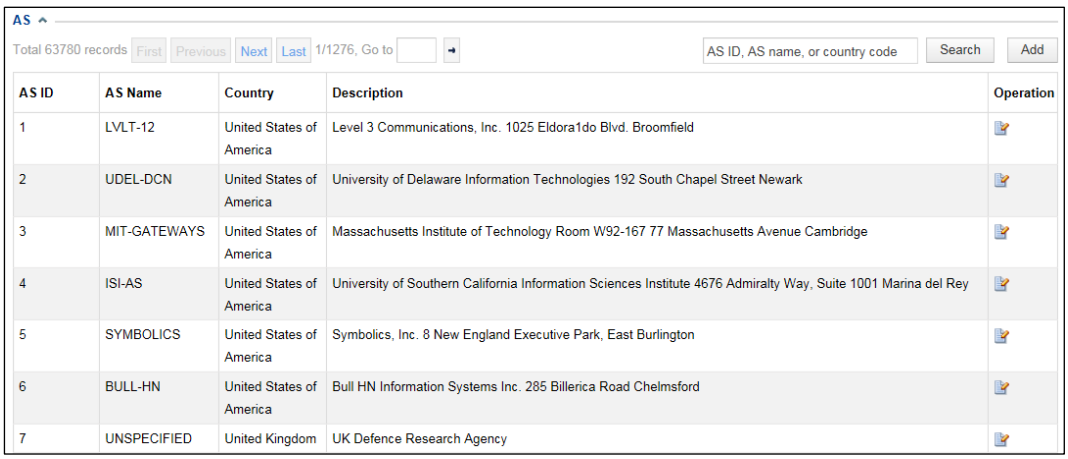
Click **AS** under **Data Dictionary** on the page shown in Figure 6-16. The AS configuration page appears, as shown in Figure 6-32. Alternatively, you can right-click an NTA device on the left treelike device list and choose **Data Dictionary > AS** to open this page.

An AS is a network consisting of mutually connected routing devices that use the same routing protocol. After a common AS is defined as an organization, the organization name will be displayed in the **Top5 AS Traffic** chart **of a region or** router under **Monitor > Regions** or **Monitor > Routers** on the web-based manager of NTA.

An AS can be either of the following:

- Built-in AS: can be edited, but cannot be deleted.
- Custom AS: can be added, modified, and deleted.

Figure 6-32 AS configuration page




| AS ID | AS Name | Country | Description | Operation |
|---|---|---|---|---|
| 1 | LVLT-12 | United States of America | Level 3 Communications, Inc. 1025 Eldora1do Blvd. Broomfield | |
| 2 | UDEL-DCN | United States of America | University of Delaware Information Technologies 192 South Chapel Street Newark | |
| 3 | MIT-GATEWAYS | United States of America | Massachusetts Institute of Technology Room W92-167 77 Massachusetts Avenue Cambridge | |
| 4 | ISI-AS | United States of America | University of Southern California Information Sciences Institute 4676 Admiralty Way, Suite 1001 Marina del Rey | |
| 5 | SYMBOLICS | United States of America | Symbolics, Inc. 8 New England Executive Park, East Burlington | |
| 6 | BULL-HN | United States of America | Bull HN Information Systems Inc. 285 Billerica Road Chelmsford | |
| 7 | UNSPECIFIED | United Kingdom | UK Defence Research Agency | |

You can add, edit, delete, and search for ASs. For detailed configuration operations, see *NSFOCUS NTA User Guide*.

## 6.4 Configuring ADS Protection Policies

This section describes how to configure ADS settings on the ADS M, including:

- ADS protection policies
- Protection groups
- Access control policy
- Diversion and injection
- System management
- Advanced applications

In the web-based manager of ADS M, the contents of ADS policy pages are directly obtained from ADS devices. Since ADS functions vary with diversions and deployment modes, the contents of the policy pages are subject to ADS versions and deployment modes.

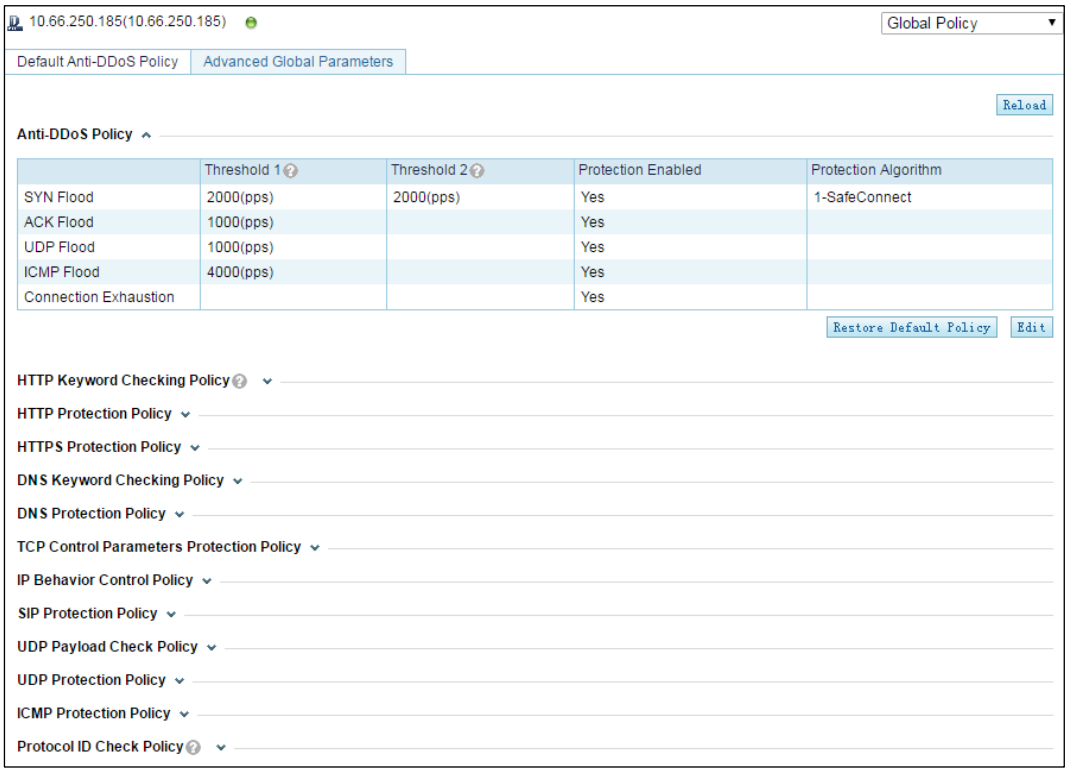
| | |
|---|---|
| Note | After configuration information of an ADS device is updated, changes may not be displayed on ADS M immediately. In this case, you can click **Reload** to synchronize the latest configuration of the ADS device to ADS M. |

### 6.4.1 Configuring Global Policies

On the left treelike device list, click an ADS device to open the device's policy configuration page. By default, the page displays the global policies configured and used on the ADS device, as shown in Figure 6-33.

For an ADS device later than V4.5.88.15, you can right-click a device on the left treelike device list and choose **Global Policy > Default Anti-DDoS Policy** to open the page shown in Figure 6-33.

Figure 6-33 Global policies




## Editing Default Anti-DDoS Policies

You can edit or restore the default anti-DDoS policies on this page. For detailed operations, see *NSFOCUS ADS User Guide*.

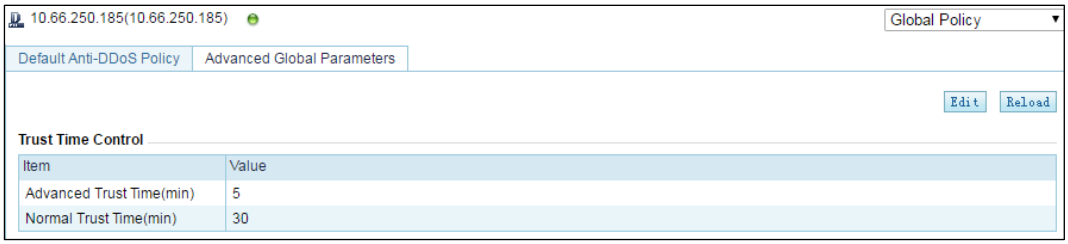
## Editing Advanced Global Parameters

You can configure the trust time of source IP addresses for policies in a centralized way on ADS devices.

**Step 1** On the page shown in Figure 6-33, click the **Advanced Global Parameters** tab.

The page for setting the trust time for source IP addresses appears, as shown in Figure 6-34.

Figure 6-34 Advanced Global Parameters page




**Step 2** Click **Edit** to edit the trust time.

Table 6-5 Advanced parameters

| Parameter | Description |
|---|---|
| Advanced Trust Time(min) | Time during which a source IP address authenticated with the advanced algorithm stays in the trust list. The value ranges from 1 to 3600, with **5** as the default. |
| Normal Trust Time(min) | Time during which a source IP address authenticated with the common algorithm stays in the trust list. The value ranges from 1 to 3600, with **30** as the default. |

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

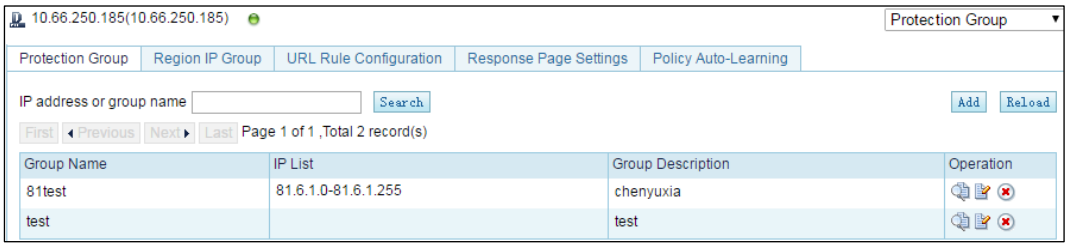
**----End**

## 6.4.2 Configuring Protection Groups and Related Parameters

In the upper-right corner of the page shown in Figure 6-33, choose **Protection Group** from the drop-down list to open the page for protection group configuration and related settings of an ADS. By default, the protection group configuration page appears, as shown in Figure 6-35.

For an ADS device later than V4.5.88.15, you can right-click a device on the left treelike device list and choose **Protection Group** > **Protection Group** to open the page shown in Figure 6-35.

Figure 6-35 Protection groups




On this page, you can configure the following:

- Protection groups

  The listed protection groups are those on the selected ADS device. You can view, edit, create, delete, and reload protection groups.
- Region IP groups

  The listed IP groups are those dispatched from ADS M to the selected ADS device. You can view and reload region IP groups.
- URL protection rules

  You can edit, create, delete, and reload URL protection rules.
- Response page settings

  You can edit, create, delete, and reload response page settings.
- Policy auto-learning

You can start and stop policy auto-learning, generate groups, and reload auto-learning settings.

For detailed configuration operations, see *NSFOCUS ADS User Guide*. When adding a global protection group, you can select one out of several common protection policies templates, as shown in Figure 6-36.

Figure 6-36 Selecting a common protection policy template

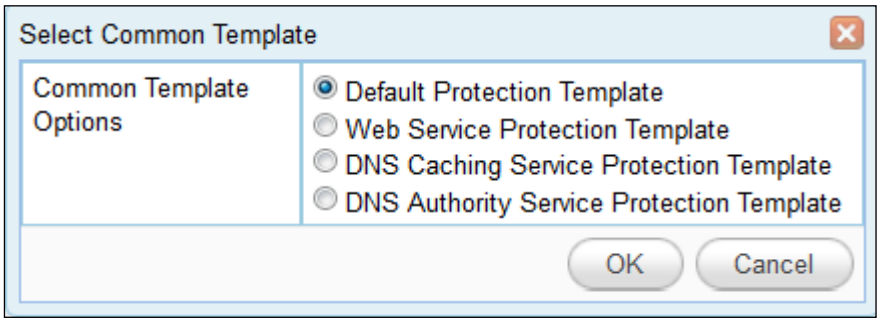



Table 6-6 describes the differences between these templates.

Table 6-6 Template differences

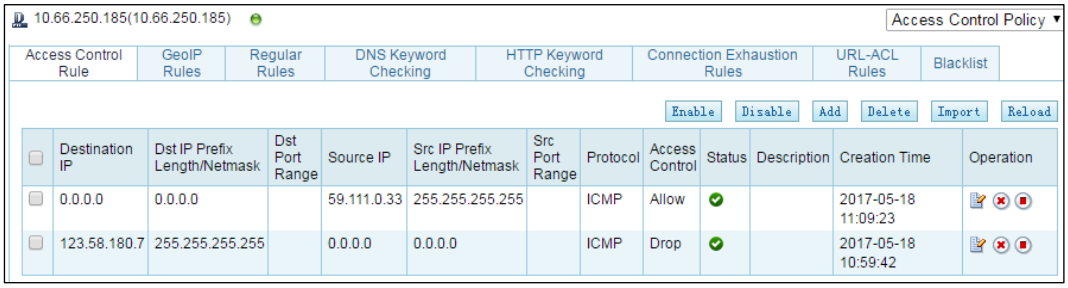
| Template Name | Description |
|---|---|
| Default Protection Template | Protection template that uses system default policies. |
| Web Service Protection Template | Difference from the default protection template:<br>• Policies related to UDP flood are disabled by default.<br>• Policies related to DNS are disabled by default.<br>• The SIP protection policy is disabled by default.<br>• URL authentication is used by default in the HTTP Get flood protection policy. |
| DNS Caching Service Protection Template | Difference from the default protection template:<br>• The HTTP protection policy is disabled by default.<br>• Algorithm 2 is enabled by default in the DNS protection policy.<br>• The SIP protection policy is disabled by default. |
| DNS Authority Service Protection Template | Difference from the default protection template:<br>• The HTTP protection policy is disabled by default.<br>• Algorithm 3 is enabled by default in the DNS protection policy.<br>• The ACK flood protection policy is disabled by default.<br>• The SIP protection policy is disabled by default. |

## 6.4.3 Configuring Access Control Policy

In the upper-right corner of the page shown in Figure 6-33, choose **Access Control Policy** from the drop-down list to open the page for configuring access control policies of an ADS. By default, access control rules on the ADS are displayed. See Figure 6-37.

For an ADS device later than V4.5.88.15, you can right-click a device on the left treelike device list and choose **Access Control Policy** > **Access Control Rule** to open the page shown in Figure 6-37.

Figure 6-37 Access control policies




On this page, the administrator can configure the following:

- Access control rules

  You can create, edit, delete, enable, disable, import, and reload access control rules.
- GeoIP rules

You can create, edit, delete, enable, disable, and reload GeoIP rules.

- Regular expression rules

  You can create, edit, delete, and reload regular expression rules.
- DNS keyword check

  You can create, edit, delete, and reload DNS keywords.
- HTTP keyword check

  You can create, edit, delete, and reload HTTP keywords.
- Connection exhaustion rules

  You can create, edit, delete, and reload connection exhaustion rules.
- URL-ACL rules

  You can edit, create, delete, and reload URL-ACL rules.
- Blacklist

  You can create, view, delete, clear, search for, enable, disable, import, and export blacklists.

For detailed configuration operations, see *NSFOCUS ADS User Guide*.

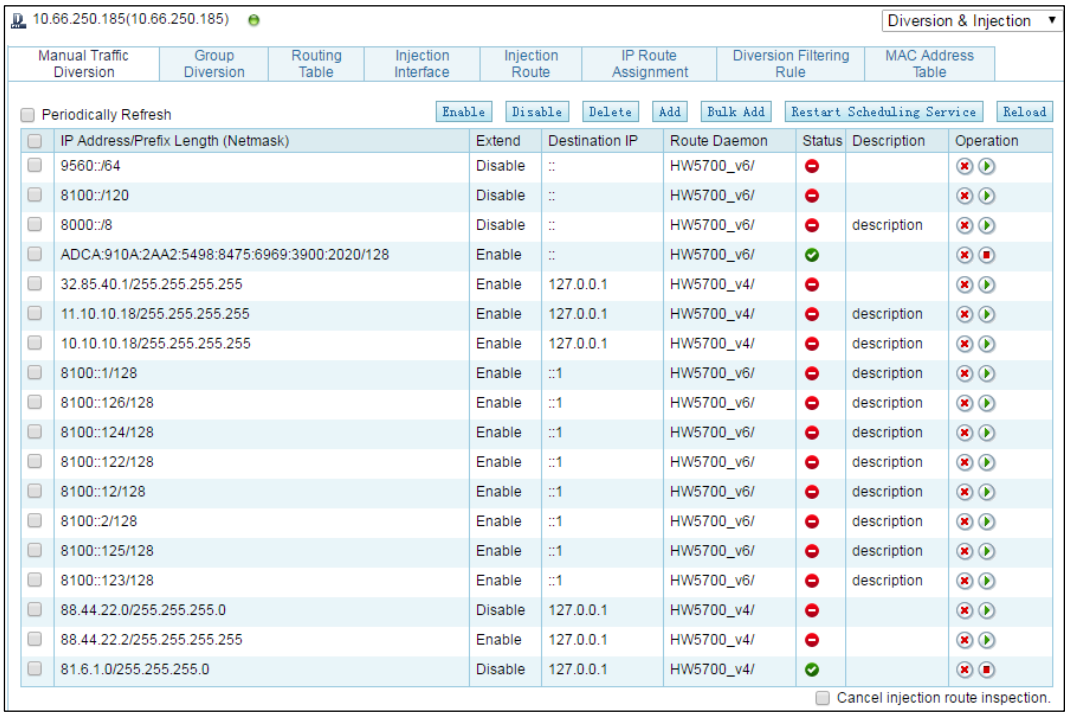
## 6.4.4 Configuring Diversion and Injection

In the upper-right corner of the page shown in Figure 6-33, choose **Diversion & Injection** from the drop-down list to open the page for configuring diversion and injection of an ADS. By default, manual diversion rules on the ADS are displayed. See Figure 6-38.

For an ADS device later than V4.5.88.15, you can right-click the device on the left treelike device list and choose **Diversion & Injection > Manual Traffic Diversion** to open the page shown in Figure 6-38.

For ADS V4.5R89F03 deployed in in-path mode, **Diversion & Injection** is not displayed in the drop-down box in the upper-right of the page shown in Figure 6-38.

Figure 6-38 Manual diversion rules




| IP Address/Prefix Length (Netmask) | Extend | Destination IP | Route Daemon | Status | Description | Operation |
|---|---|---|---|---|---|---|
| 9560::/64 | Disable | :: | HW5700_v6/ | | | |
| 8100::/120 | Disable | :: | HW5700_v6/ | | | |
| 8000::/8 | Disable | :: | HW5700_v6/ | | description | |
| ADCA:910A:2AA2:5498:8475:6969:3900:2020/128 | Enable | :: | HW5700_v6/ | | | |
| 32.85.40.1/255.255.255.255 | Enable | 127.0.0.1 | HW5700_v4/ | | | |
| 11.10.10.18/255.255.255.255 | Enable | 127.0.0.1 | HW5700_v4/ | | description | |
| 10.10.10.18/255.255.255.255 | Enable | 127.0.0.1 | HW5700_v4/ | | description | |
| 8100::1/128 | Enable | ::1 | HW5700_v6/ | | description | |
| 8100::126/128 | Enable | ::1 | HW5700_v6/ | | description | |
| 8100::124/128 | Enable | ::1 | HW5700_v6/ | | description | |
| 8100::122/128 | Enable | ::1 | HW5700_v6/ | | description | |
| 8100::12/128 | Enable | ::1 | HW5700_v6/ | | description | |
| 8100::2/128 | Enable | ::1 | HW5700_v6/ | | description | |
| 8100::125/128 | Enable | ::1 | HW5700_v6/ | | description | |
| 8100::123/128 | Enable | ::1 | HW5700_v6/ | | description | |
| 88.44.22.0/255.255.255.0 | Disable | 127.0.0.1 | HW5700_v4/ | | | |
| 88.44.22.2/255.255.255.255 | Enable | 127.0.0.1 | HW5700_v4/ | | | |
| 81.6.1.0/255.255.255.0 | Disable | 127.0.0.1 | HW5700_v4/ | | | |

On this page, you can configure the following:

- Manual traffic diversion

  You can add, bulk add, delete (one or more), enable (one or more), disable (one or more), and reload manual diversion routes, restart the scheduling service, periodically refresh routes, and cancel injection route inspection.
- Group diversion

  You can add, delete (one or more), enable, disable, and reload group diversions.
- Diversion routing table

  You can query diversion routing information of specified IP addresses and reload the routing table.
- Injection interface

  You can edit, add, delete (one or more), and reload injection interfaces.
- Injection route

  You can edit, add, delete (one or more), enable (one or more), disable (one or more), view, import, and reload injection routes, edit advanced configurations, learn MAC addresses, and reset the link switch count.
- IP route assignment

  You can edit, add, delete, and reload IP route assignment.

- Diversion filtering rules

  You can edit, add, delete, enable, disable, move up, move down, and reload diversion filtering rules, and enable diversion filtering rules by default.

- MAC address table

  You can add, edit, delete, and reload MAC addresses as well as set invalid MAC addresses.

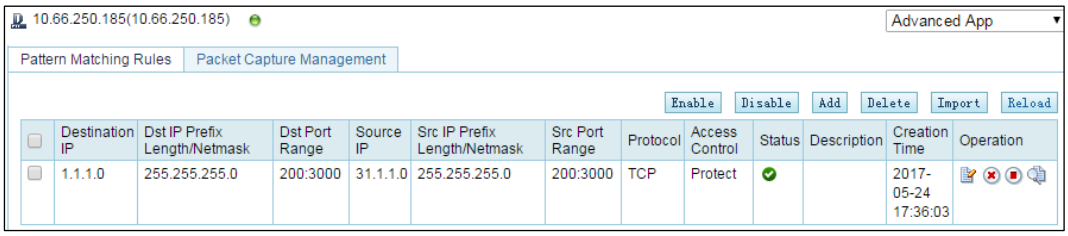
For detailed configuration operations, see *NSFOCUS ADS User Guide*.

## 6.4.5 Configuring System Management

In the upper-right corner of the page shown in Figure 6-33, choose **Administration** from the drop-down list to open the system management configuration page of an ADS. By default, user information on the ADS is displayed. See Figure 6-39.

For an ADS device later than V4.5.88.15, you can right-click a device on the left treelike device list and choose **Administration** > **Packet Matching Rules** to open the page shown in Figure 6-39.

Figure 6-39 Packet Matching Rules page




On this page, you can configure the following:

- User management

  You can edit the super user, change the password of the CLI user, enable/disable the CLI user, create and delete other system user, and reload user management configurations.

- Configuration file import and export

  You can configure the import and export of user configuration files.

- HA configuration

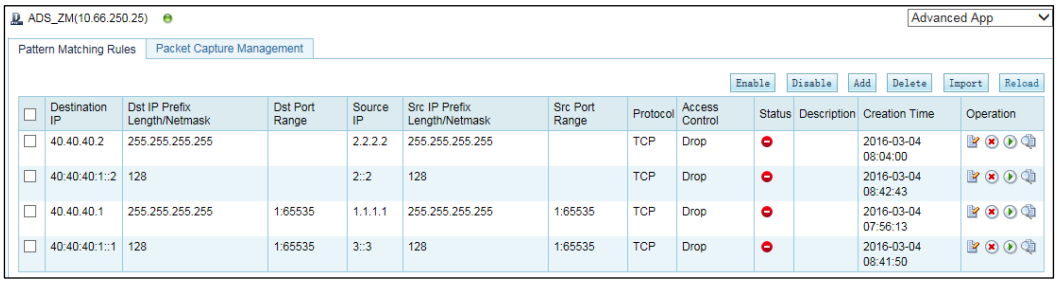
  You can configure the HA function.

For detailed configuration operations, see *NSFOCUS ADS User Guide*.

## 6.4.6 Configuring Advanced Applications

In the upper-right corner of the page shown in Figure 6-33, choose **Advanced App** from the drop-down list to open the page for configuring advanced applications of an ADS. By default, the pattern matching rules on the ADS are displayed. See Figure 6-40.

Figure 6-40 Advanced applications




| Destination IP | Dst IP Prefix Length/Netmask | Dst Port Range | Source IP | Src IP Prefix Length/Netmask | Src Port Range | Protocol | Access Control | Status | Description | Creation Time | Operation |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 40.40.40.2 | 255.255.255.255 | | 2.2.2.2 | 255.255.255.255 | | TCP | Drop | | | 2016-03-04 08:04:00 | |
| 40:40:40:1::2 | 128 | | 2::2 | 128 | | TCP | Drop | | | 2016-03-04 08:42:43 | |
| 40.40.40.1 | 255.255.255.255 | 1:65535 | 1.1.1.1 | 255.255.255.255 | 1:65535 | TCP | Drop | | | 2016-03-04 07:56:13 | |
| 40:40:40:1::1 | 128 | 1:65535 | 3::3 | 128 | 1:65535 | TCP | Drop | | | 2016-03-04 08:41:50 | |

On this page, you can configure the following:

- Pattern matching rule

  You can view, edit, add, delete (one or more), enable (one or more), disable (one or more), import, and reload pattern matching rules.

- Packet capture management

  Packet capture tasks can be created manually or automatically. You can view, download, or delete packet capture files. The files for automatic packet capture tasks can be viewed on line.

For detailed configuration operations, see *NSFOCUS ADS User Guide*.

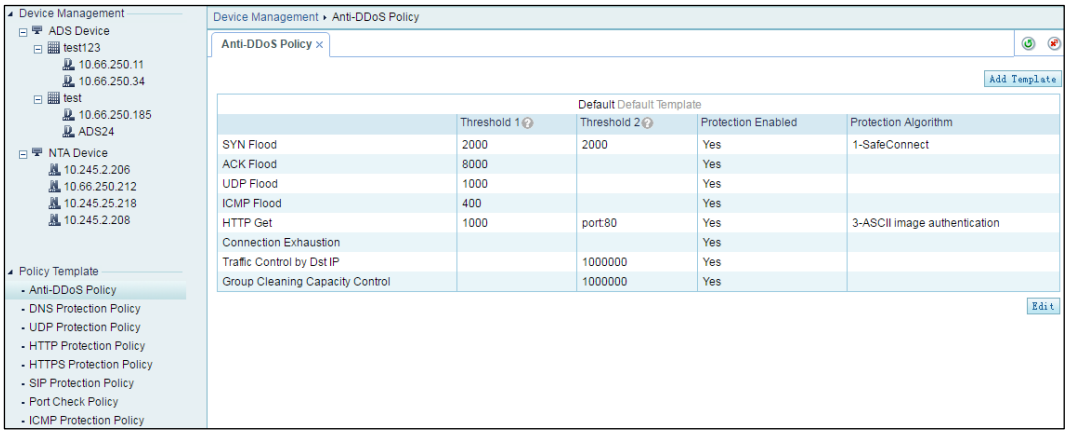
# 6.5 Configuring Protection Policy Templates

The protection policies of ADS are used to detect and prevent DDoS attacks on devices in centralized management mode. Policy templates tailor prevention policies for different users, making it easier for users to modify policy parameters. A policy template can be assigned to multiple ADS devices.

**Step 1** Choose **Device Management** > **Policy Template** > **Anti-DDoS Policy**.

The page for configuring anti-DDoS policy templates appears, as shown in Figure 6-41.

Figure 6-41 Anti-DDoS policy templates




| | 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 | port:80 | Yes | 3-ASCII image authentication |
| Connection Exhaustion | | | Yes | |
| Traffic Control by Dst IP | | 1000000 | Yes | |
| Group Cleaning Capacity Control | | 1000000 | Yes | |

You can edit templates for the following policies:

- Anti-DDoS policies
- DNS protection policy
- UDP protection policy
- HTTP protection policy
- HTTPS protection policy
- SIP protection policy
- Port check policy
- ICMP protection policy

For detailed configuration operations, see *NSFOCUS ADS User Guide*.

| | |
|---|---|
| Note | By default, a new protection group and region IP group adopt the default anti-DDoS policy template. For details about anti-DDoS policy parameters, see appendix A Parameters. |

# 7 Web-based System Management

This chapter describes routine ADS M system management and maintenance operations on the web-based manager.

## 7.1 Local Settings

This section describes basic configuration of ADS M, including basic system parameters, license management, system upgrade, data storage, network configuration, DNS server configuration, HA configuration, and running alert configuration.

### 7.1.1 Basic Settings

As shown in Figure 7-1, 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 7-1 Basic system information

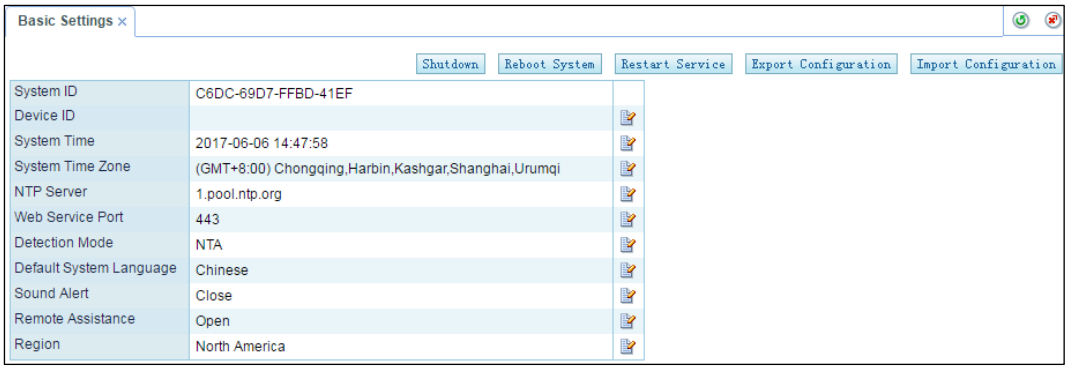



Table 7-1 describes detailed system information.

Table 7-1 Basic system information

| Parameter | Description |
|---|---|
| System ID | Specifies the ADS M hardware ID. |
| Device ID | Specifies the name of ADS M. |

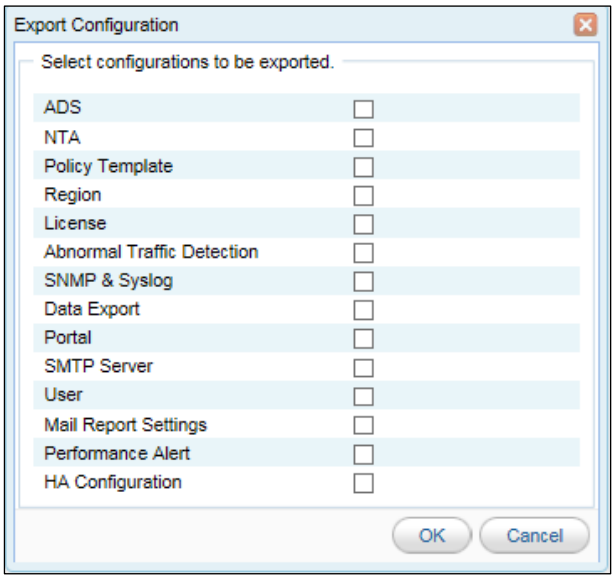
| Parameter | Description |
|---|---|
| System Time | Specifies the current system time in format of 2012-09-27 17:07:07.<br>Changing the system time may cause a loss of certain data. Please handle with caution. |
| System Time Zone | Specifies the time zone of the system time.<br>When daylight saving time (DST) is used, the page will prompts a message, indicating that the clock is automatically adjusted based on the DST. |
| NTP Server | Specifies the IP address of the server with which ADS M synchronizes time. |
| Web Service Port | Specifies the 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.<br>Note<br>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 | Species the detection mode adopted by the system.<br>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 | Specifies the default language used by the system to save audit logs.<br>The web-based manager supports both **Chinese** and **English**. The default language is **English**.<br>The changed default language takes effect only after the system restart. |
| Sound Alert | Controls whether to enable sound alerting.<br>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 3.1.7 Generating Sound Alerts. |
| Remote Assistance | By default, remote assistance is disabled. Selecting **Open** allows NSFOCUS technical personnel to log in to the system in the background for remote assistance. Selecting **Close** disables this function.<br>SSH is used for remote login, running on port 50022. |

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 Services** 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 7-2. Click **OK** to save the configuration file to a specified target path.

Figure 7-2 Exporting configurations

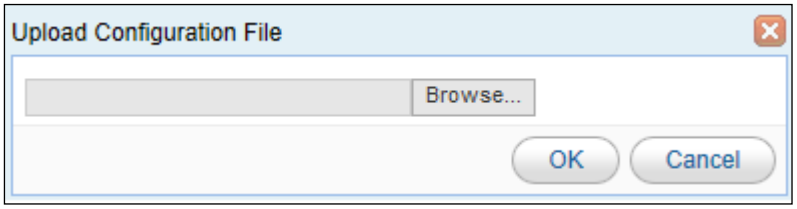



| | |
|---|---|
| Note | The configuration files will be exported as an encrypted package which is not editable and can be used for backup or imported to the device. |

- Import a configuration file

  Click **Import Configuration** and upload a file in the **Upload Configuration File** dialog box shown in Figure 7-3 to overwrite the original configuration file. This operation reconfigures ADS devices, NTA devices, and policy templates.

Figure 7-3 Upload Configuration File dialog box




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

## 7.1.2 License Management

After an ADS M is installed, you need to import a license before using it. On the **License** page, click **Browse** 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 7-4.

Figure 7-4 License page

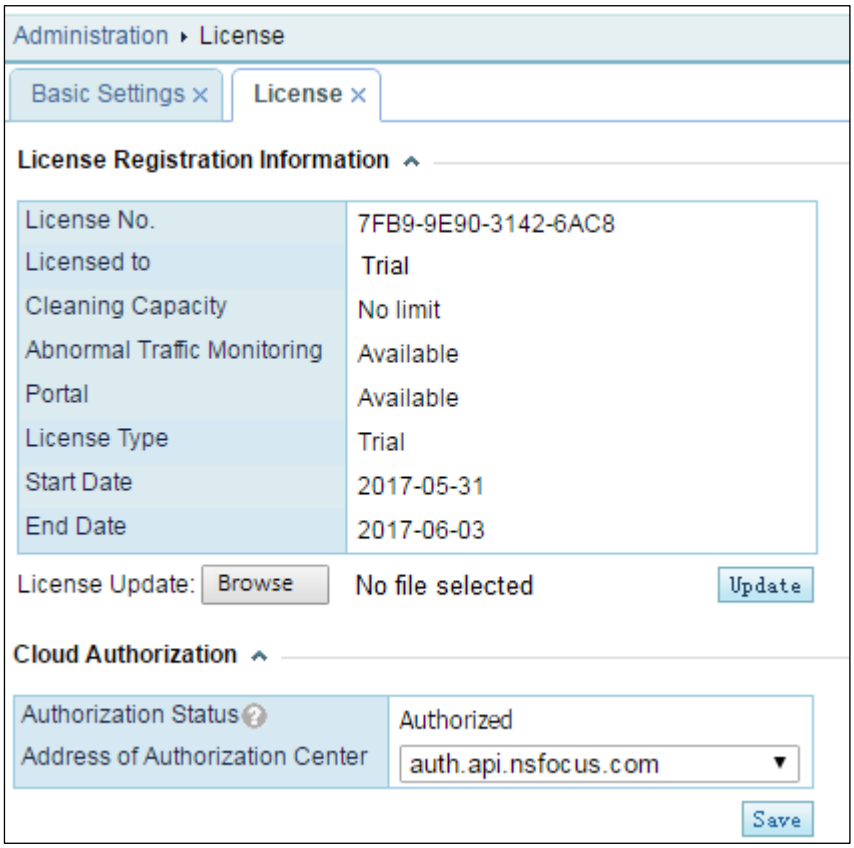



Table 7-2 describes license parameters.

Table 7-2 License parameters

| Parameter | Description |
|---|---|
| License No. | Specifies the license number of the current ADS M. |
| Licensed to | Specifies the customer host that is authorized to use this system. |
| Number of Monitored Devices | Specifies the maximum number of ADS devices that can be monitored by the current ADS M. |
| Abnormal Traffic Monitoring | Allows abnormal traffic detection. |
| Portal | Allows portal. |
| License Type | Specifies the license type, which can be **Trial** and **Paid**. |
| Start Date | Specifies the start date of the license validity, which is usually the production date of the current license. |

| Parameter | Description |
|---|---|
| End Date | Specifies the 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. |
| Authorization Status | Note:<br>The cloud authentication function is available only when an ADS M virtual machine is used. Meanwhile, an ADS M virtual machine can be used only after it is connected to the cloud authentication center.<br>After you configure the address of the cloud authorization center, the virtual machine starts automatically sends authentication requests to the cloud.<br>• If the address is correct and connection is established, the status is **Authorized**.<br>• If you enter a wrong authorization center address when the authorization status is **Authorized**, the authorization status changes to **Offline**, and you can still use the web-based manager temporarily.<br>• After the **Offline** status remains for more than 7 days, the status changes to **Unauthorized**, and you cannot use the web-based manager.<br>During its operation, the virtual machine periodically sends authentication requests to the cloud. Please keep the connection between the virtual machine and the cloud. |
| Address of Authorization Center | URL of the cloud authorization server.<br>• For use on the Chinese mainland, choose **auth.api.nsfocus.com**.<br>• For use in other countries and regions, choose **auth.nsfocusglobal.com**. |

| | |
|---|---|
| Note | Once the license expires, please update it or contact technical support personnel of NSFOCUS for a new license. |

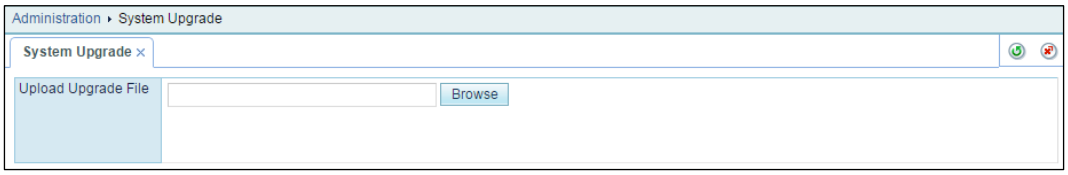
## 7.1.3 System Upgrade

To upgrade ADS M, perform the following steps:

**Step 1** Contact technical support personnel of NSFOCUS for upgrade packages of ADS M. Make sure that the package applies to your product.

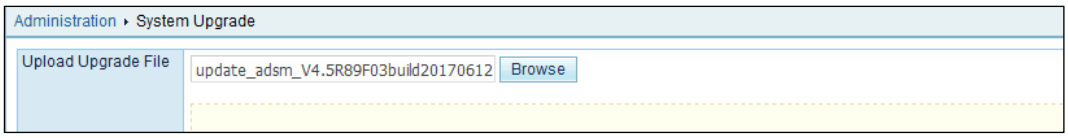
**Step 2** Choose **Administration** > **System Upgrade**.

Figure 7-5 System Upgrade page




**Step 3** Click **Browse** to select an upgrade package file.

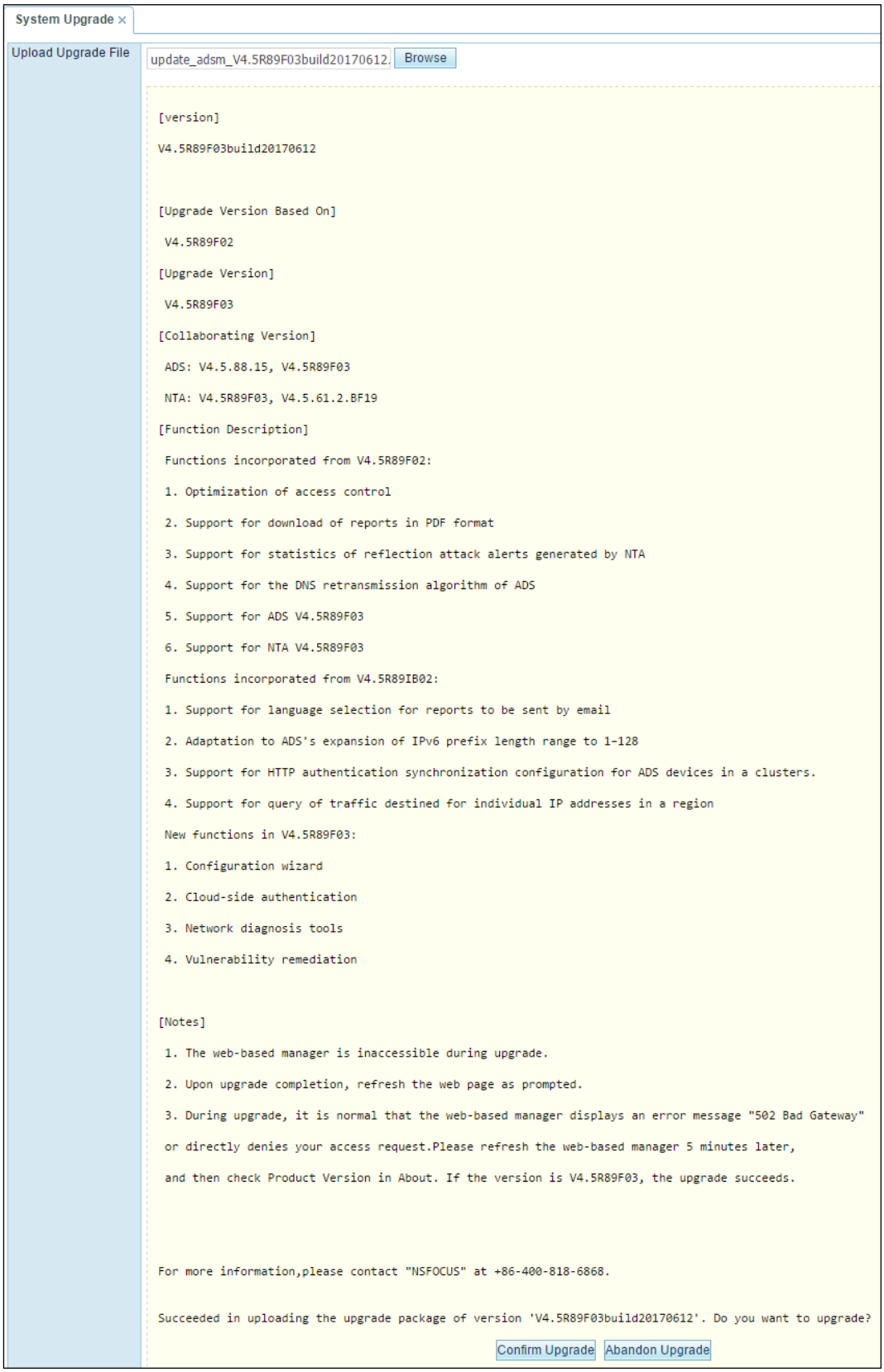
Figure 7-6 Selecting an upgrade file




**Step 4** Click **Upload**.

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

Figure 7-7 Upgrade confirmation



**Step 5** After upgrade, click **OK** when the system prompts that the system service will be rebooted.

**Step 6** Click **Confirm Upgrade** to start the upgrade.

A progress bar is displayed to indicate the upgrade progress. After upgrade, click **OK** when the system prompts that the system service will be rebooted.

**Step 7** Refresh the **System Upgrade** page.

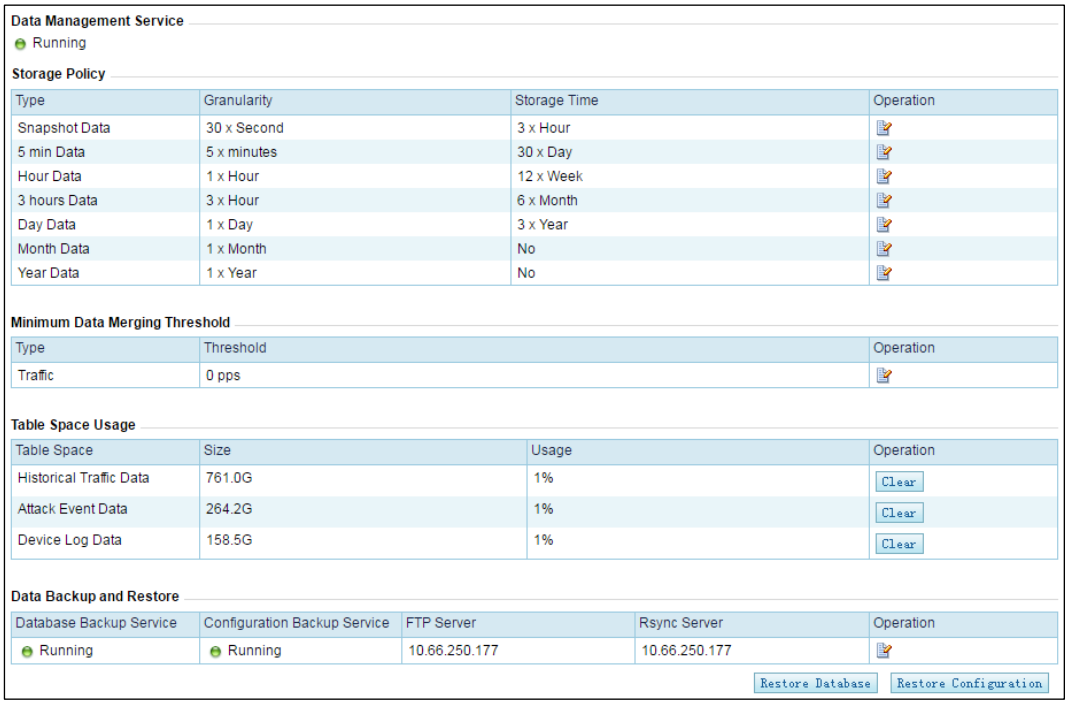
**Step 8** Click **About** in the upper-right corner of the web-based manager, to view the product version information to determine whether the system upgrade succeeded.

**----End**

## 7.1.4 Data Storage

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

Figure 7-8 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 | |

Restore Database  Restore Configuration

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

- View the data management service status.

  You can view the operating status of the data management service.
- Edit data storage policies.

  On the **Data Storage** page, 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 on the data storage time. In addition, the system automatically clears out-of-date data. |

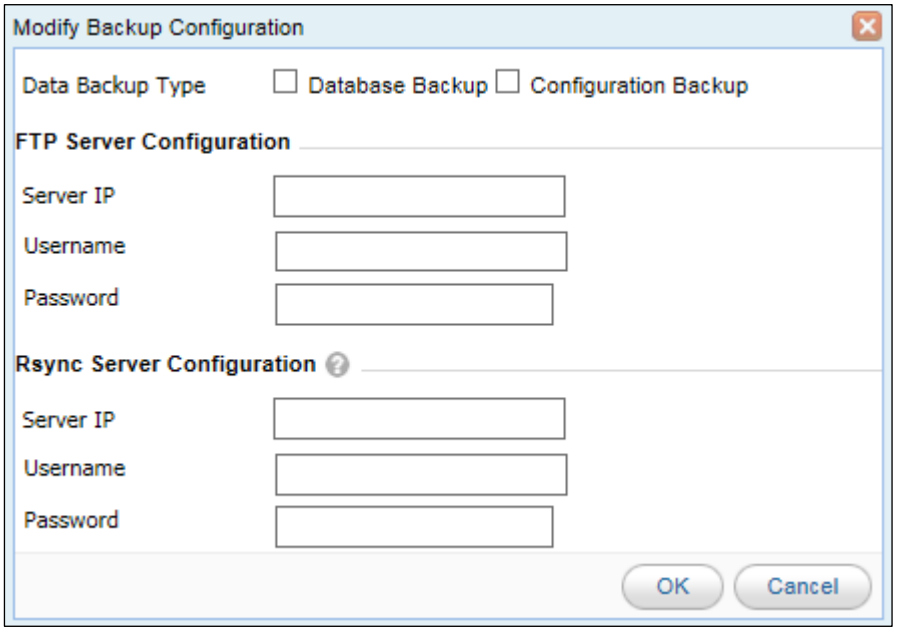
- Edit the minimum data merging threshold.

  Click in the **Operation** column to edit the minimum data merging threshold.
- View the table space usage.

  You can view the space occupied by historical traffic data, attack event data, and device log data as well and space usage.
- Manage data backup and restoration.
  - Modify the backup configuration.

    Under **Data Backup and Restore**, click in the **Operation** column to edit the backup configuration in the dialog box shown in Figure 7-9.

Figure 7-9 Modifying the backup configuration




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.

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

– Apply the backup file for restoration.

  Under **Data Backup and Restore**, click **Restore Configuration** below the table to retrieve 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.

## 7.1.5 Network Configuration

ADS M supports both IPv4 and IPv6 protocols. The following sections describe the IPv4 and IPv6 configurations.

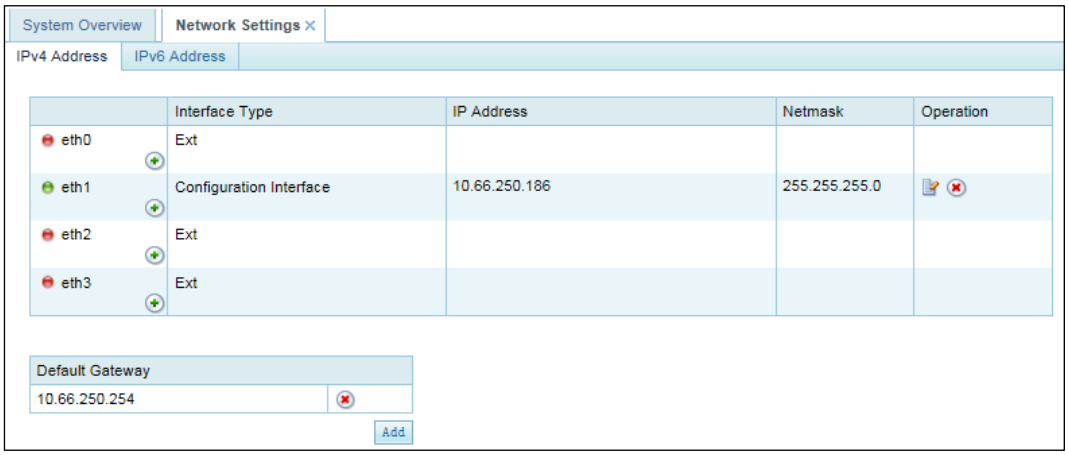
### 7.1.5.1 Configuring IPv4 Address

#### ADS NX3-M600A/M1600A

ADS M provides multiple interfaces, as shown in Figure 7-10. eth1 acts as a management interface of ADS M. It is used to configure the IP address, subnet mask, and default network gateway of ADS M. Other interfaces are extended interfaces. indicates interfaces are connected to the network. indicates that interfaces are disconnected from the network. Each interface can be configured with two IP addresses. Initially, default parameters are displayed. You need to configure the IPv4 address and subnet mask of the NIC. 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 denied access to the web-based manager of ADS M. |

Figure 7-10 IPv4 network configuration page




On the interface list shown in Figure 7-10, click to configure the IP address and other parameters of an interface, as shown in Figure 7-11.

Figure 7-11 Configuring an interface in IPv4 mode

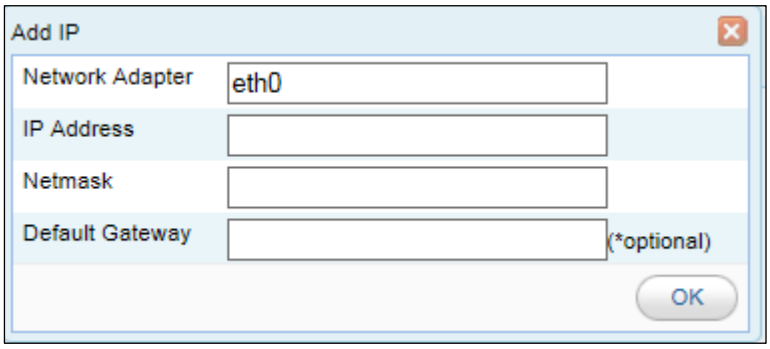



Table 7-3 describes parameters for configuring an interface in IPv4 mode.

Table 7-3 Parameters for configuring an interface in IPv4 mode

| Parameter | Description |
|---|---|
| Network Adapter | Specifies the management interface or expansion interface of ADS M. |
| IP Address | Specifies the IP address of ADS M. Only IPv4 addresses are allowed here. |
| Netmask | Specifies the netmask of the IPv4 address of ADS M. |
| Default Gateway | Specifies the IP address of the network gateway of the subnet that involves ADS M. |

| | |
|---|---|
| Tip | After you change the IP address of the management interface, the current windows may be unavailable. In this case, re-log in to the system. |

## ADS NX3-M1600E

ADS NX3-M1600E differs greatly from ADS NX3-M600A/M1600A in the front panel.

Figure 7-12 Front panel of ADS NX3-M1600E

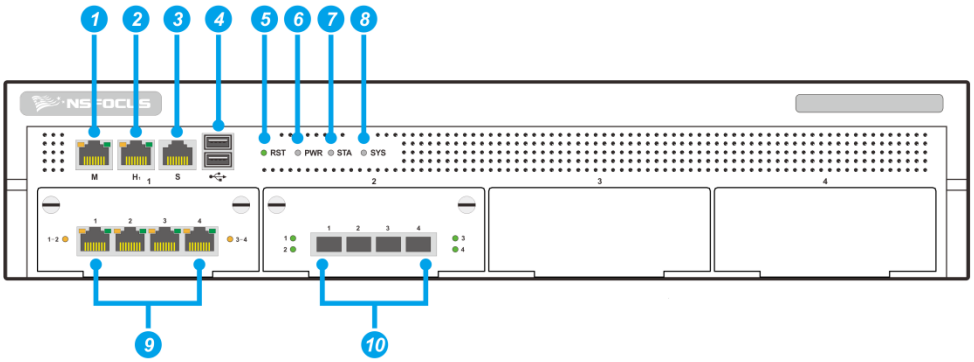


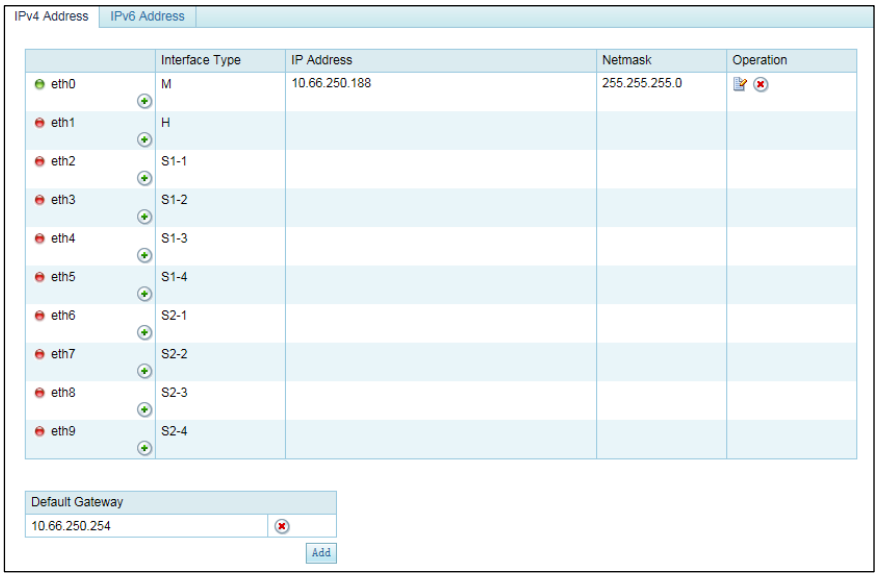

Table 7-4 describes the interfaces on the front panel of ADS NX3-M1600E.

Table 7-4 Front panel of ADS NX3-M1600E

| | | | |
|---|---|---|---|
| ① Management interface: M | ② Management interface: H | ③ – | ④ – |
| ⑤ – | ⑥ – | ⑦ – | ⑧ – |
| ⑨ Working port: GE electrical (RJ-45)<br>Electrical interfaces are, from left to right, indicated by **S1-1**, **S1-2**, **S1-3**, and **S1-4**. | ⑩ Working port: GE optical (SFP)<br>Optical interfaces are, from left to right, indicated by **S2-1**, **S2-2**, **S2-3**, **and S2-4**. | – | – |

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

Figure 7-13 ADS NX3-M1600E – IPv4 address configuration




The interface LED in the left column table indicates the network connection status of the 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 indicate roles of interfaces, interfaces M and H are recommended for configuration and management purposes and other interfaces 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 of the NIC.

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 not access the web-based manager of ADS-M. |

On the interface list in Figure 7-13, click to configure the IPv4 address and other parameters of an interface, as shown in Figure 7-14.

Figure 7-14 ADS NX3-M1600E – Configuring an interface in IPv4 mode

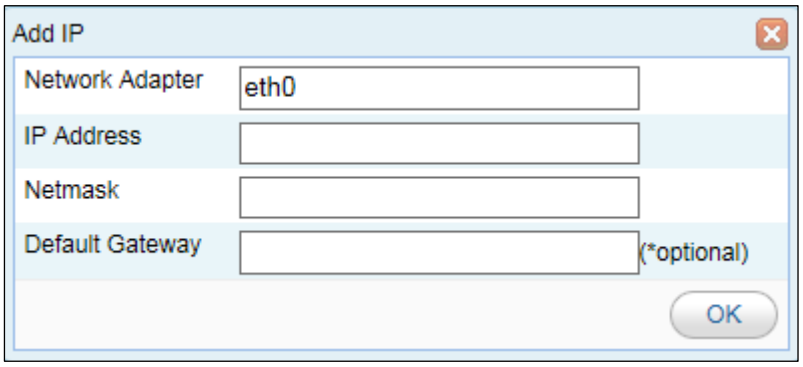



Table 7-5 describes IPv4 network parameters.

Table 7-5 Parameters for configuring an interface in IPv4 mode

| Parameter | Description |
|---|---|
| Network Adapter | Specifies the management interface or expansion interface of ADS M. |
| IP Address | Specifies the IP address of ADS M. Only IPv4 addresses are allowed here. |
| Netmask | Specifies the subnet mask of the IPv4 address of ADS-M. |
| Default Gateway | Specifies the IP address of the network gateway of the subnet that involves ADS M. |

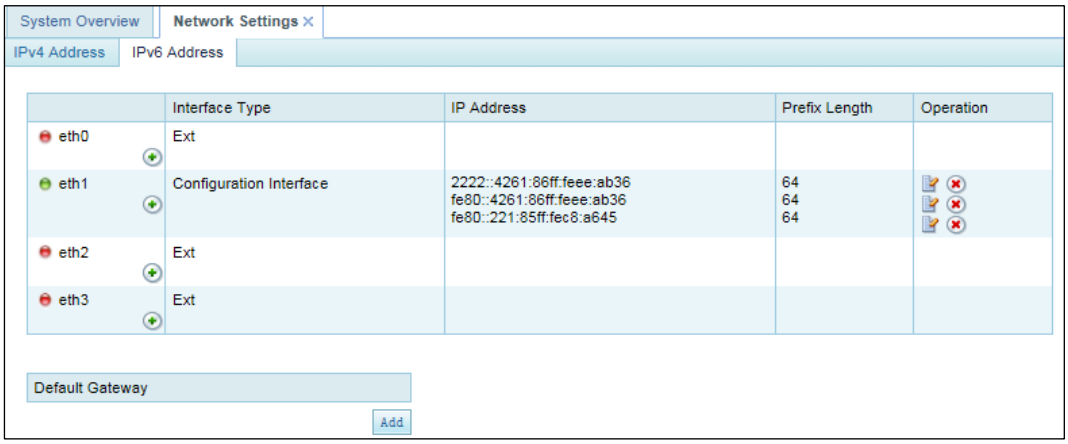
| | |
|---|---|
| Tip | After you change the IP address of the management interface, the current windows may be unavailable. In this case, re-log in to the system. |

## 7.1.5.2 Configuring IPv6 Address

### ADS NX3-M600A/M1600A

On the **Network Configuration** page shown in Figure 7-10, click **IPv6 Address** to open the IPv6 a configuration page. See Figure 7-15.

Figure 7-15 IPv6 network configuration page




On the interface list shown in Figure 7-15, click to configure the IPv6 address and other parameters of an interface in the dialog box as shown in Figure 7-16.

Figure 7-16 Configuring an interface in IPv6 mode

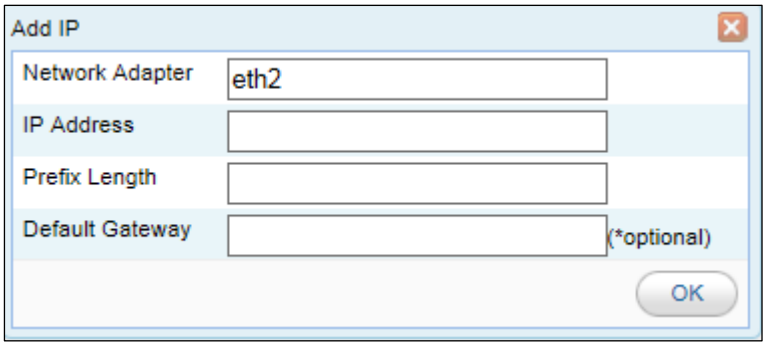



Table 7-6 describes parameters for configuring an interface in IPv6 mode.

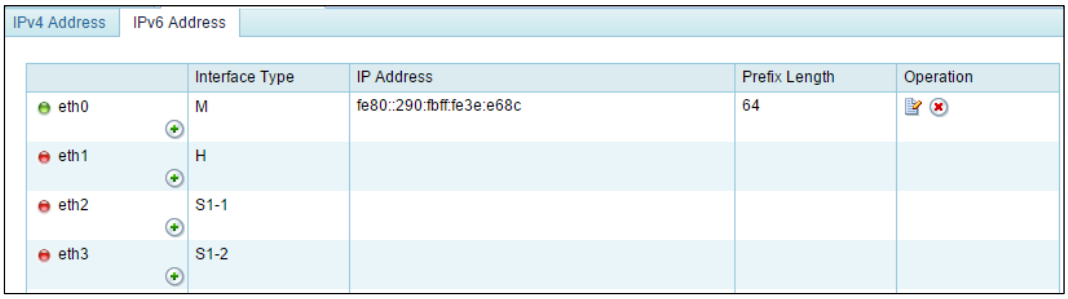
Table 7-6 Parameters for configuring an interface in IPv6 mode

| Parameter | Description |
|---|---|
| Network Adapter | Specifies the management interface or extended interface of ADS M. |
| IP Address | Specifies the IP address of ADS M. Only IPv6 addresses are allowed here. |
| Prefix Length | Specifies the prefix length of the configured IPv6 address. |
| Default Gateway | Specifies the IP address of the network gateway of the subnet that involves ADS M. |

## ADS NX3-M1600E

On the **Network Settings** page in Figure 7-10, click **IPv6 Address** to open the IPv6 address configuration page, as shown in Figure 7-17.

Figure 7-17 IPv6 address configuration




On the interface list in Figure 7-17, click to configure the IPv6 address and other parameters of an interface, as shown in Figure 7-18.

Figure 7-18 Configuring an interface in IPv6 mode

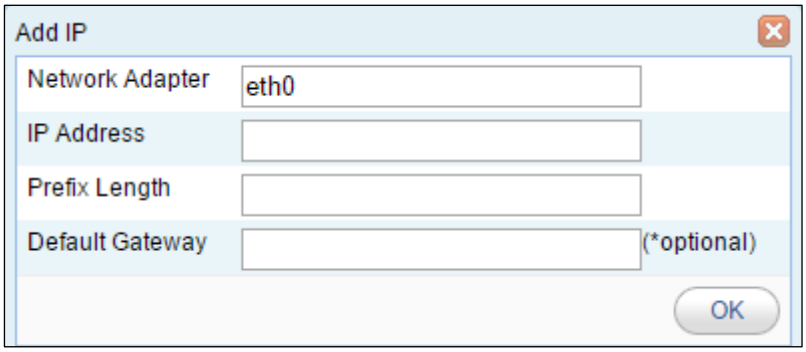



Table 7-7 describes IPv6 network parameters.

Table 7-7 Parameters for configuring an interface in IPv6 mode

| Parameter | Description |
|---|---|
| Network Adapter | Specifies the management interface or expansion interface of ADS M. |
| IP Address | Specifies the IP address of ADS M. Only IPv4 addresses are allowed here. |
| Prefix Length | Prefix length of the IPv6 address. |
| Default Gateway | Specifies the IP address of the network gateway of the subnet that involves ADS M. |

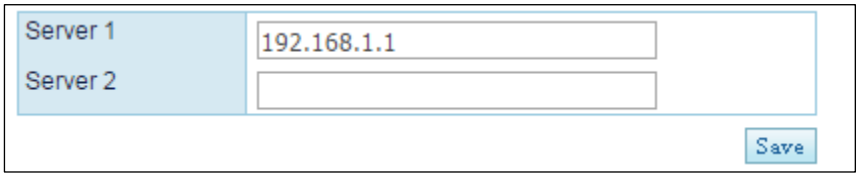
| | |
|---|---|
| Tip | After you change the IP address of the management interface, the current windows may be unavailable. In this case, re-log in to the system from a new explorer window. |

## 7.1.6 DNS Server

As an essential and fundamental service, the DNS service is used to determine the mapping between host domain names and IP addresses. ADS M allows you configure the DNS server for it.

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, as shown in Figure 7-19.

Figure 7-19 DNS Server page

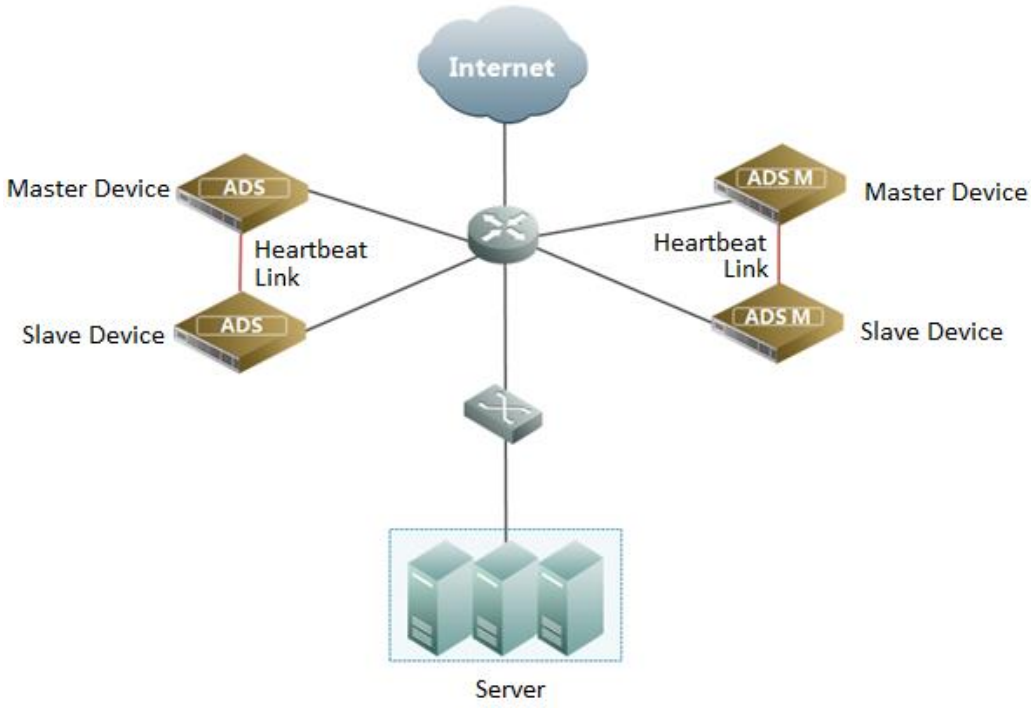



## 7.1.7 Configuring HA

Currently, ADS M supports the dual-system hot backup function, with one ADS M functions as the master device and another ADS M 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 that services are provided properly.

Routes need to 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 7-20 shows the topology for HA briefly.

Figure 7-20 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 8.3.2 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.

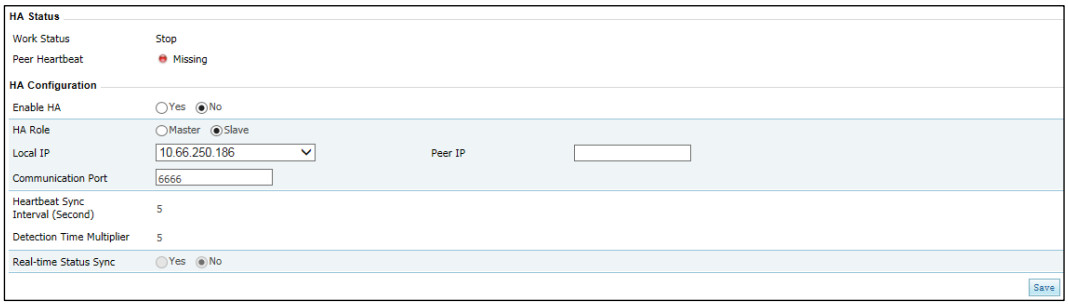
  Routes must be reachable between heartbeat interfaces of master and slave devices.
- Configure other communication interfaces.

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**.

The **HA Configuration** page appears, as shown in Figure 7-21.

Figure 7-21 HA Configuration page




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

Table 7-8 describes HA parameters.

Table 7-8 HA parameters

| Parameter | Description |
|---|---|
| Enable HA | Determines whether to enable the HA function.<br>• **Yes** indicates that HA function is enabled.<br>• **No** indicates that the HA function is disabled. |
| HA Role | Role played by this device in dual-system hot backup mode.<br>• **master**: indicates that this device functions as the master device and starts to handle user services immediately after HA is enabled, until a failover.<br>• **slave**: indicates that this device functions as the slave device. After HA is enabled, the slave device stays in the backup state without handling user services, until a failover. |
| 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.<br>Note<br>Routes must be reachable between heartbeat interfaces of master and slave devices. |
| Communication Port | Port used by the device for communication with the peer.<br>Note<br>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.<br>Note |

| Parameter | Description |
|---|---|
| | 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 | Multiples 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.<br>After an HA connection is established between the master and slave devices, the detection time multiplier 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.<br>**Real-Time Status Sync** should be enabled on both the master and slave devices, and so that the two devices could synchronize files. After an HA connection is established between the master and slave devices, the real-time status synchronization setting on the slave device will automatically synchronized to that on the master device. |

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

**Step 4** Click **OK** 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 7-21. 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.

## 7.1.8 Performance Alert Configuration

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

- **Global Configuration** area specifies the alert thresholds for the CPU and memory usage of ADS M itself and all devices under ADS M.

- **ADS Alert Configuration** area specifies the alert thresholds for the CPU and memory usage of all ADS devices under ADS M.
- **NTA Alert Configuration** area specifies the alert thresholds for the CPU and memory usage of all NTA devices under ADS M. After configuring alert thresholds, you can view the status of CPU and memory usage alerts in **Monitoring > System Overview > Device Monitoring**. For details, see section 3.1.6 Viewing the System Status Bar.

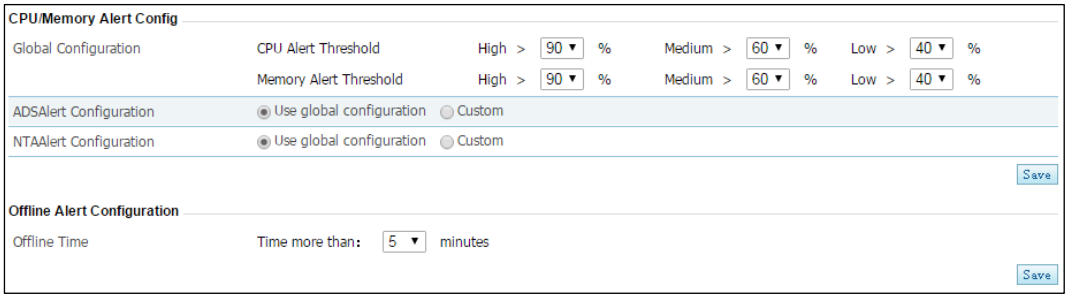
Under **Offline Alert Configuration**, you can set the time threshold for triggering device offline alerts. When a device under ADS M remains offline for a period longer than specified, a device offline alert is generated and sent via Syslog or email (syslog server and email settings should be completed in advance). For related configuration, see sections 7.3.2 Syslog and 7.3.4 Mail Alert Settings.

To configure performance alerts, perform the following steps:

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

The **Performance Alert Configuration** page appears, as shown in Figure 7-22.

Figure 7-22 Performance Alert Configuration page




**Step 2** Set CPU and memory alert thresholds and the offline alert parameter.

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

**----End**

# 7.2 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.

## 7.2.1 User Management

As shown in Figure 7-23, the **User Management** page displays all current users. Initially, only the default user **admin** is displayed.

Figure 7-23 User Management page

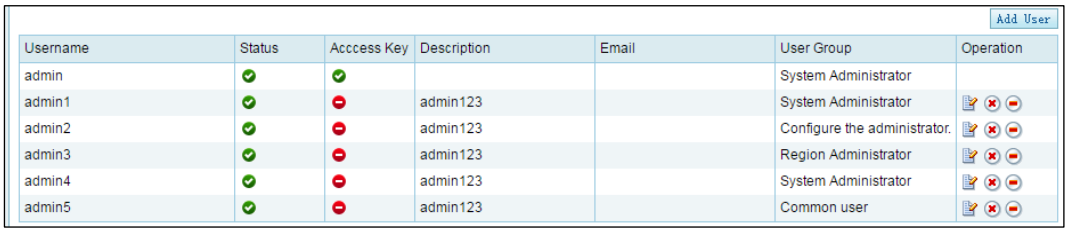



Table 7-9 describes ADS M user groups and their respective privileges.

Table 7-9 ADS M user groups and their respective privileges

| User Group | Privileges |
|---|---|
| System administrator | Has all system management privileges. |
| Configuration administrator | Has privileges of managing device configurations and viewing system monitoring information, reports, logs, and region information, without system management privileges. |
| Region administrator | Has privileges of configuring regions, viewing system monitoring information, reports, and logs, and viewing device configurations, without system management privileges. |
| Common user | Has privileges of viewing information of all modules, except the system management module. |

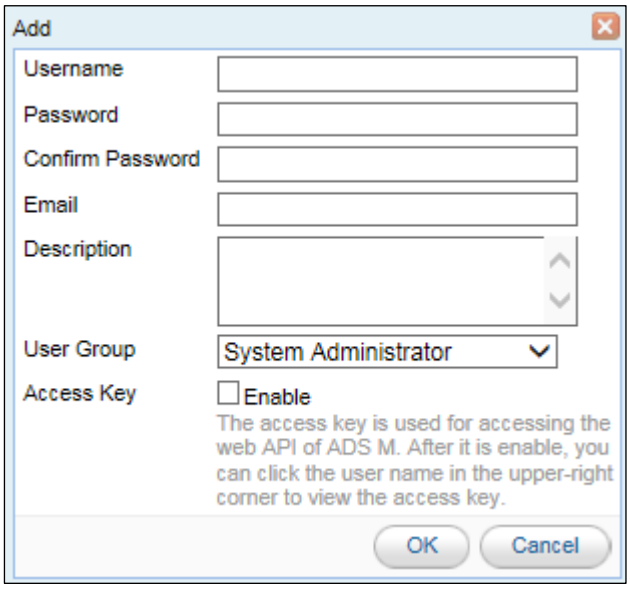
## Creating a User

Only the user **admin** can create system administrators. Only system administrators can create configuration administrators, region administrators, and common users.

To create a user, perform the following steps:

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

Figure 7-24 Creating a user




**Step 2** Set parameters in the dialog box and click **OK**.

Table 7-10 Parameters for creating a user

| Parameter | Description |
|---|---|
| Username | Specifies the user name.<br>The user name must be 4 to 20 characters and cannot contain invalid characters such as tab character, carriage return, \0, space, vertical bar (\|), slash (/), angle bracket (<, or >), quotation mark (" or '), and semicolon (;). |
| Password | Specifies the password.<br>The minimum length and strength of the password can be configured under **Administration** > **User and Audit** > **Security Settings**. |
| Confirm Password | Password confirmation.<br>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 privileges. |
| Access Key | Used for accessing the web API of ADS M. For details about configuration of the web API, please contact technical support personnel of NSFOCUS. |

**----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 to edit information of a 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. |

## 7.2.2 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 7-25.

Figure 7-25 Security settings

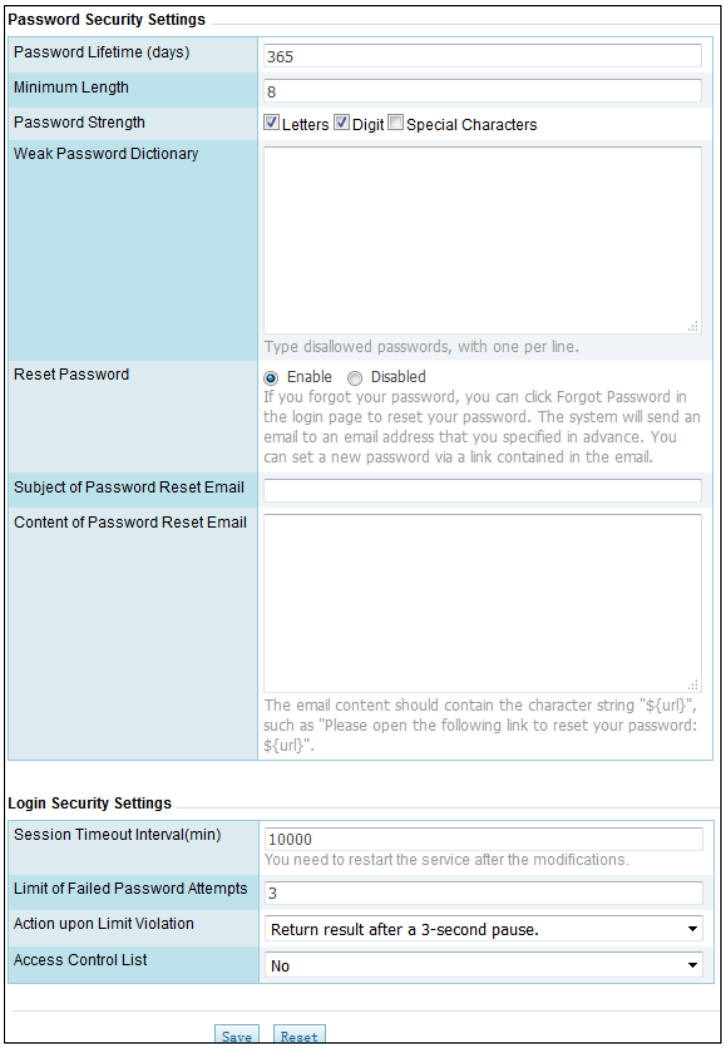



Table 7-11 describes parameters of security settings.

Table 7-11 Parameters of security settings

| Parameter | Description |
|---|---|
| Password Lifetime (days) | Specifies the password validity.<br>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.<br>The value is an integer ranging from 8 to 99, with **8** as the default. |
| Password Strength | Specifies the complexity of a password.<br>By default, the password must contain letters and digits. Also, you can define that 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.<br>Each weak password should be in a separate line. |

| Parameter | Description |
|---|---|
| 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.<br>This can be defined by users. |
| Content of Password Reset Email | Specifies the content of the email message notifying password resetting.<br>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.<br>Values include **Return result after 3-second pause** and **Lock client IP for 20 minutes**. |
| Access Control List | Specifies whether to allow a client to access the system. It has the following values:<br>• **No**: indicates any clients can access to the system.<br>• **Permit access from the following IP addresses**: indicates that only clients with IP addresses included in the text box below can access the system.<br>• **Deny access from the 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. Please contact the administrator to check access control settings." on the login page.<br>Note<br>After the access control list is successfully modified, you are advised to wait at least 3 minutes for the settings to take effect. |

## 7.2.3 Authentication Configuration

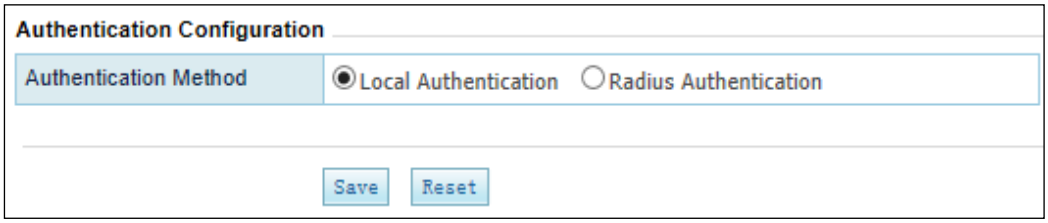
ADS M supports local authentication and third-party Radius server authentication for user authentication.

| | |
|---|---|
| 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**.<br>• When third-party Radius server authentication is used, users must add the user name and password configured on the third-party Radius server to ADS M and use such user name and password to access ADS M. |

To configure an authentication method, perform these steps:

**Step 1** Choose **Administration** > **User and Audit** > **Authentication Configuration**.

Figure 7-26 Authentication Configuration page




**Step 2** Select an authentication method, which can be **Local Authentication** or **Radius Authentication**.

**Step 3** (Optional) When **Authentication Method** is set to **Radius Authentication, set Radius server parameters in the dialog box shown in** Figure 7-27**.**

Figure 7-27 Configuring the Radius server

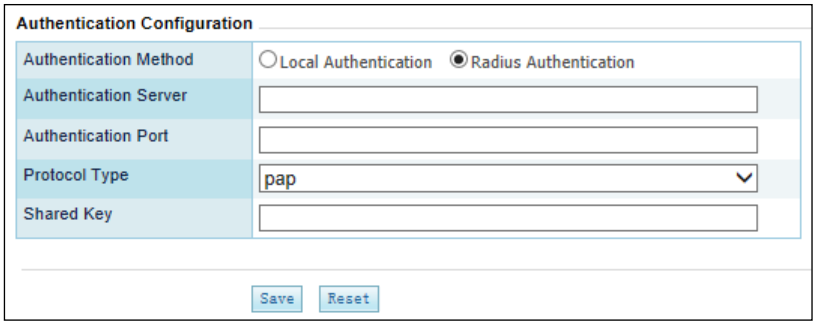



Table 7-12 describes parameters for configuring the Radius server.

Table 7-12 Parameters for configuring the Radius server

| Parameter | Description |
|---|---|
| Authentication Server | Specifies the IP address of the third-party Radius server. |
| Authentication Port | Specifies the port of the third-party Radius server that is used for data communication. |
| Protocol Type | Specifies the protocol used for authenticating the third-party Radius server, which can be **pap**, **chap**, **spap**, **mschapv1**, or **mschapv2**. |
| Shared Key | Specifies the key shared between ADS M and the third-party Radius server. |

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

**----End**

## 7.2.4 Audit Logs

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 Logs** to open the **Audit Logs** page, as shown in Figure 7-28. 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 7-28 Audit logs

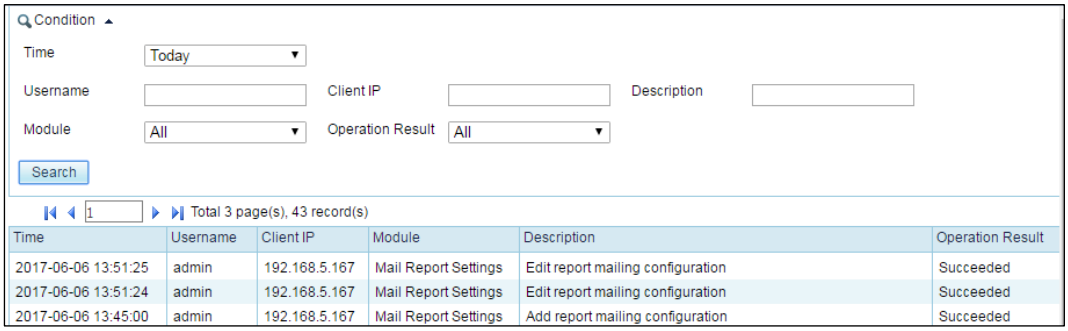



Table 7-13 describes audit log parameters.

Table 7-13 Audit log parameters

| Parameter | Description |
|---|---|
| Time | Specifies the query time range.<br>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.<br>The full user name is required because fuzzy query is not allowed here. |
| Client IP | Specifies the IP address of the user device.<br>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.<br>**All** indicates that all operation result logs are displayed. |

# 7.3 Third-Party Interface

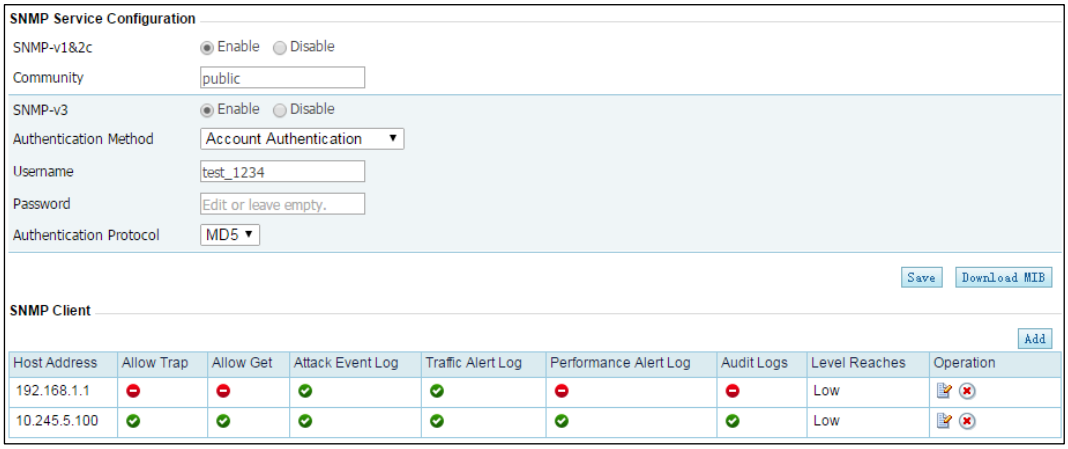
ADS M exchanges data with external systems via SNMP and syslog interfaces. The third-party interface configuration includes configuration of an SNMP server, syslog server, SMTP server, and other servers.

# 7.3.1 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 7-29.

Figure 7-29 SNMP configuration




## Downloading a MIB File

Click **Download MIB** in the upper-right corner of the page shown in Figure 7-29. 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 7-14 describes parameters for configuring an SNMP server.

Table 7-14 Parameters for configuring an SNMP server

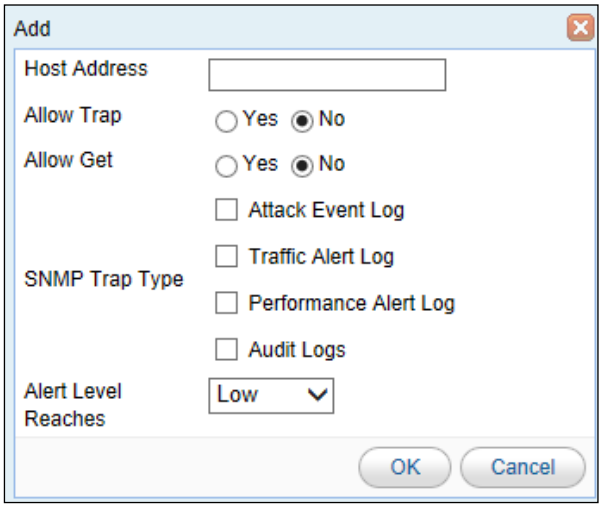
| Parameter | Description |
|---|---|
| SNMP-v1&2c | Controls whether SNMPv1 and SNMPv2c are enabled for management. |
| Community | Specifies the community supported by the SNMP agent. This parameter is required when **SNMP-v1&2c** is set to **Enable**. |
| SNMP-v3 | Controls whether SNMPv3 is enabled for management.<br>Note<br>When both **SNMP-v1&2c** and **SNMP-v3 are set to Enable, ADS M uses SNMP-v3 for authentication.** |

| Parameter | Description |
|---|---|
| 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.<br>This parameter is required when **Authentication Method** is set to **Account Authentication or Private key Authentication.** |
| Authentication Protocol | Specifies the protocol used for user authentication via SNMPv3, which can be **MD5** or **SHA**.<br>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.<br>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.<br>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 7-29.

Figure 7-30 Adding an SNMP client




**Step 2** Configure parameters in the dialog box.

Table 7-15 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 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 Logs**. |
| Alert Level Reaches | Specifies which level of alert messages will be filtered, which can be **Low**, **Medium**, or **High**. |

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

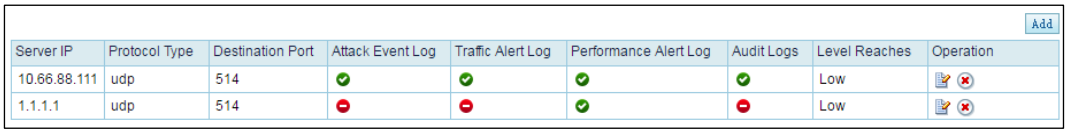
**----End**

## 7.3.2 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, as shown in Figure 7-31.

Figure 7-31 Syslog configuration




### Adding a Syslog Server

On the **Syslog Configuration** page shown in Figure 7-31, click **Add** to add a syslog server, as shown in Figure 7-32.

Figure 7-32 Adding a syslog server

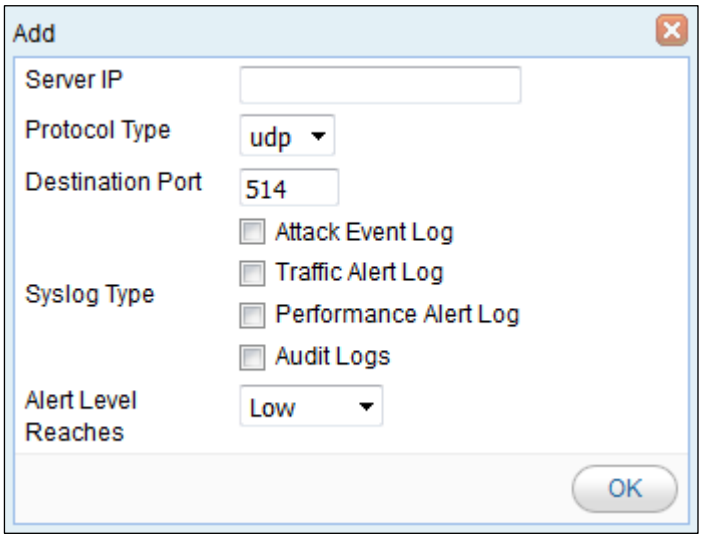



Table 7-16 describes syslog server parameters.

Table 7-16 Syslog server parameters

| Parameter | Description |
|---|---|
| Server IP | Specifies the IP address of the syslog server. |
| Protocol Type | Specifies the protocol used for data transmission.<br>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.<br>Values are **Attack Event Log**, **Traffic Alert Log**, **Performance Alert Log**, and **Audit Logs**. **Traffic Alert Log** is available only when ADS M works in NTA detection mode. |

## Editing a Syslog Server

On the **Syslog Configuration** page shown in Figure 7-31, click in the **Operation** column of a syslog server to edit all its parameters, except **Server IP**.

## Deleting a Syslog Server

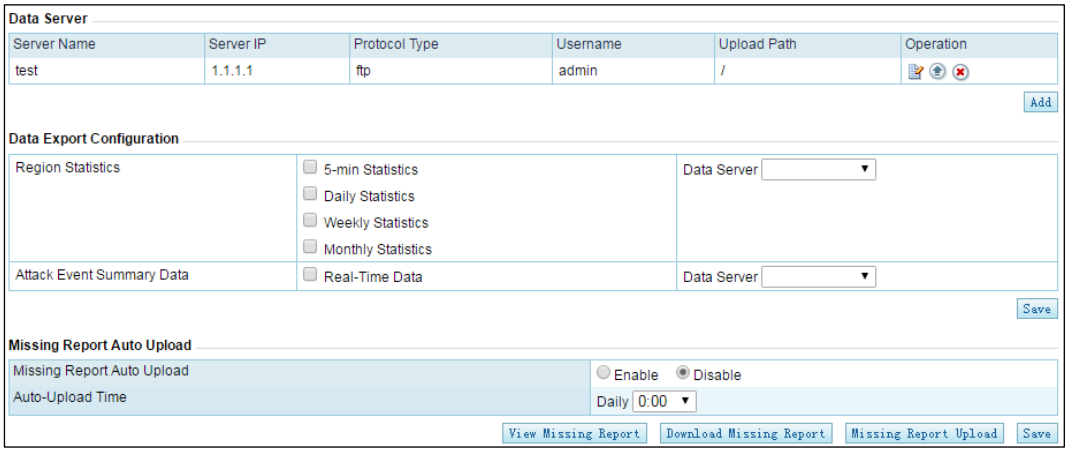
On the **Syslog Configuration** page shown in Figure 7-31, click in the **Operation** column of a syslog server to delete it.

# 7.3.3 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 7-33.

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

Figure 7-33 Data export




## Adding a Data Server

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

On the **Data Export** page shown in Figure 7-33, click **Add** to add a data server for remote backup, as shown in Figure 7-34.

Figure 7-34 Adding a data server

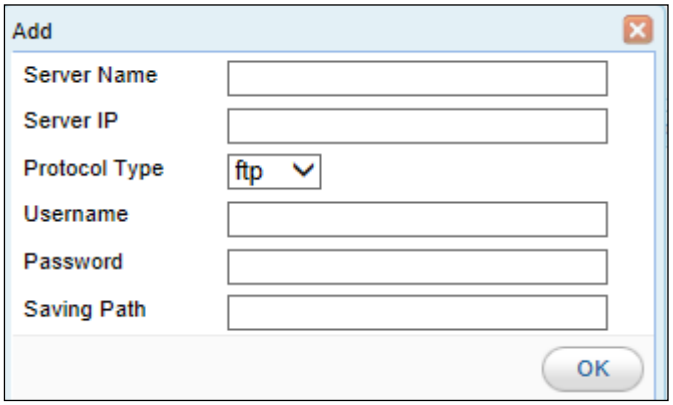



Table 7-17 describes parameters for adding a data server.

Table 7-17 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**. |

| Parameter | Description |
|---|---|
| | 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. |

### Editing a Data Server

On the **Data Export** page in Figure 7-33, click in the **Operation** column to edit settings of a data server.

### Deleting a Data Server

On the **Data Export** page in Figure 7-33, click in the **Operation** column to delete a data server.

### Uploading Data to a Data Server

On the **Data Export** page in Figure 7-33, click in the **Operation** column to test whether files can be uploaded to a remote data server.

### Configuring Data Export

On the **Data Export** page in Figure 7-33, you can select the type of data to be exported and the server to which the data is uploaded. Click **OK** to complete the configuration.

### Configuring Missing Report Upload

In the **Missing Report Auto Upload** area of the **Data Export** page shown in Figure 7-33, set **Missing Report Auto Upload to Enable**, specify the upload time, and click **Save** to save the settings.

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.

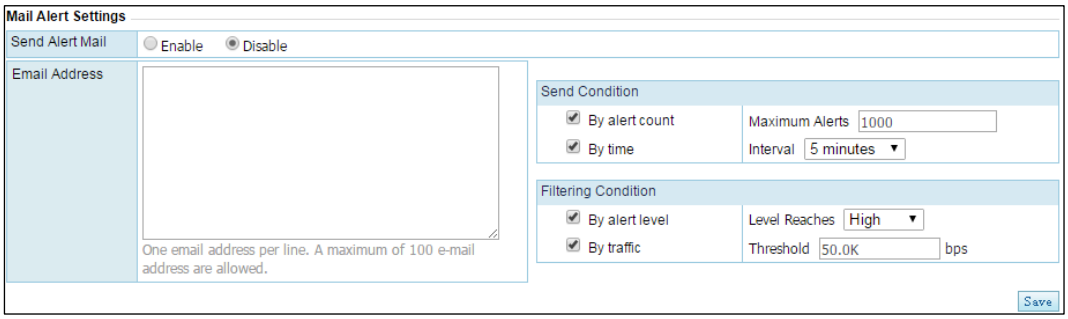
## 7.3.4 Mail Alert Settings

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**.

Figure 7-35 Mail alert settings




**Step 2** Set **Send Alert Mail** to **Enable**.

**Step 3** Specify email addresses that receive alert mails, and set mail sending and filtering conditions for alert mails.

| | |
|---|---|
| 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 4** Click **Save** to complete the configuration.

**----End**

## 7.3.5 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 7-36 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**.

Figure 7-36 SMTP server configuration

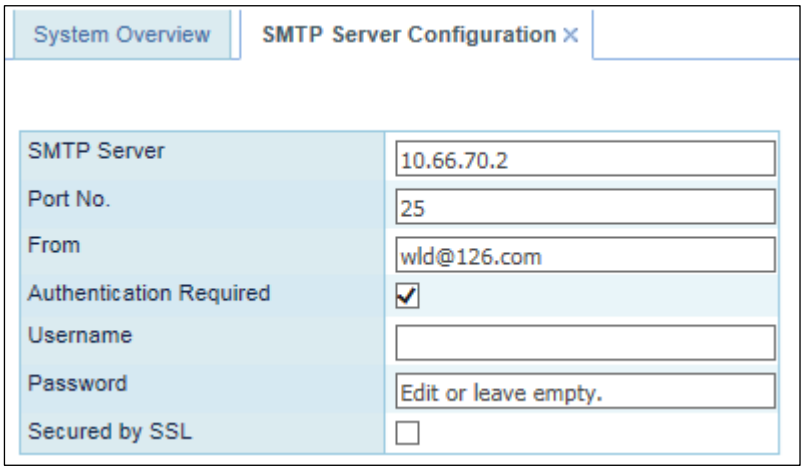



Table 7-18 lists parameters for configuring an SMTP server.

Table 7-18 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.<br>This parameter is required only when **Authentication Required** is selected. |
| Password | Specifies the password of the account from which emails are sent.<br>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. |

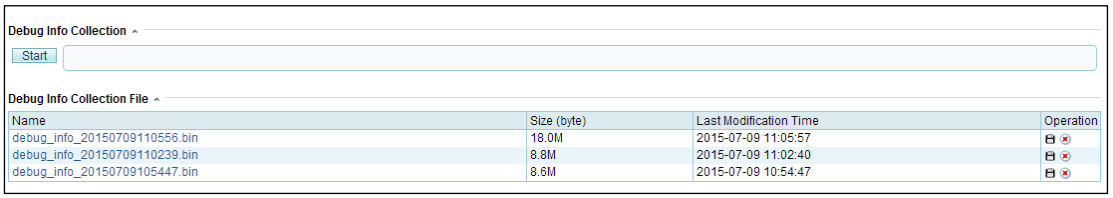
# 7.4 Debug Information Collection

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 technical support personnel of NSFOCUS 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 7-37.

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 7-37 Debug information collection



# 8 Console-based System Management

## 8.1 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.

## 8.2 Login to the Console

For details about console login, refer to section 4.1 "Login to the Console" in the *NSFOCUS ADS M Installation Guide*.

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.

## 8.3 Console Configuration

After a successful login, the main menu is displayed, as shown in Figure 8-1. 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 8.3.6 Changing the Console Password.

Figure 8-1 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
      r)  Restart system services
      b)  Reboot
      h)  Shutdown
      x)  Logout
========================================
Input your selection:
```

## 8.3.1 Checking System Status

On the main menu, type **s** and press **Enter** to view the system status. As shown in Figure 8-2, 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 8-2 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...
```

## 8.3.2 Configuring Network Settings

On the main menu, type **1** and press **Enter** to access the network setting menu, as shown in Figure 8-3. On this menu, you can type **0** and press **Enter** to return to the main menu.

Figure 8-3 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 8-4. The following screen displays network settings of the current system interface.

Figure 8-4 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 8-5.

Figure 8-5 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 8-6.

Figure 8-6 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 8-7.

Figure 8-7 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 8-8.

Figure 8-8 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 8-9.

Figure 8-9 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 **6** 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 8-10.

Figure 8-10 Configuring the DNS server

```
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
> 6
Please input 1-2 domain server ip address:
>
```

### Restore 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 8-11.

Figure 8-11 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]
>
```

## 8.3.3 Setting System Time

On the main menu, type **2** and press **Enter** to set the current system date and time, as shown in Figure 8-12. 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 8-12 Console management – Setting system time

```
datetime set:
current date is 2012-03-19 15:08:48
input the new date:
```

## 8.3.4 Setting the System Time Zone

On the main menu, type **3** and press **Enter** to set the system time zone, as shown in Figure 8-13. Select the time zone as prompted, and press **Enter** to save the setting. Then press any key to return to the main menu.

Figure 8-13 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.
#?
```

## 8.3.5 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 8-14. 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 8-14 Console management – Setting system language

```
Select the default locale
 0) Simple Chinese(zh_CN)
 1) English(en_US)
>
```

## 8.3.6 Changing the Console Password

On the main menu, type **5** and press **Enter** to change the console login password, as shown in Figure 8-15. 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 8-15 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. |

## 8.3.7 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 8-16. 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 8-16 Console management – resetting the administrator's password

```
Are you sure to reset web admin's password?[Y/n]
```

## 8.3.8 Restoring Factory Settings

On the main menu, type **7** and press **Enter** to restore factory settings, as shown in Figure 8-17 On this menu, you can type **0** and press **Enter** to return to the main menu.

Figure 8-17 Restoring factory settings

```
  1)  network settings
  2)  system config
  3)  database & data files
  4)  license file
  0)  return
> 4
```

### 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.

### Database Restoration

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.

## 8.3.9 Restoring the Database

On the main menu, type **8** and press **Enter** to restore the backup database to ADS M.

| | |
|---|---|
| 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**. |

## 8.3.10 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.

## 8.3.11 Restarting System Services

On the main menu, type **r** and press **Enter** to restart system services.

## 8.3.12 Rebooting the System

On the main menu, type **b** and press **Enter** to reboot the system.

## 8.3.13 Shutting Down the System

On the main menu, type **h** and press **Enter** to shut down the system.

## 8.3.14 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 15,000,000 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

For ADS NX3-M600A/M1600A:

| | |
|---|---|
| **Management Interface** | 1.1.1.1 |
| **Subnet Mask** | 255.255.255.0 |

For ADS NX3-M1600E:

| | |
|---|---|
| **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 |

## B.5 Default Account of the Web Administrator

| | |
|---|---|
| **Baud Rate** | 115200 |
| **Data Bits** | 8 |