# NSFOCUS ADS Portal

# User Guide

**Version: V4.5R90F05 (2023-11-16)**

**Confidentiality: RESTRICTED**

**■ Statement**

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

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

**■ Disclaimer**

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

- Data loss and system availability reduction caused by the negligence or misconduct of the system O&M or management personnel, for example, they do not handle alerts that affect system stability and availability in a timely manner.
- Data loss and system availability reduction caused by the fact that the traffic exceeds the planned hardware capacity.
- Data loss and system availability reduction or unavailability caused by natural disasters (including but not limited to floods, fires, and earthquakes) or environmental factors (including but not limited to network disconnection and power outage).

# Contents

# Preface

## Scope

This document describes functions of and methods of installing, deploying, and using NSFOCUS Anti-DDoS System User Portal ("ADS Portal" for short).

This document is provided for reference only. It may slightly differ from the actual product due to version upgrade or other reasons.

## Organization

| Chapter | Description |
|---|---|
| 1 Introduction | Briefly describes ADS Portal. |
| 2 Portal Configuration | Describes how to install and configure ADS Portal. |
| 3 Getting Started | Describes the login method and layout of the web-based manager of ADS Portal. |
| 4 Region Management | Describes how to view and configure regions on ADS Portal. |
| 5 Region Traffic Diversion | Describes how to configure traffic diversion for IP addresses in a region. |
| 6 System Overview | Describes monitoring information on the home page of the web-based manager of ADS Portal. |
| 7 Reports | Describes how to view various reports generated by ADS Portal. |
| A Default Parameters | Describes the default network settings of ADS Portal. |

## Change History

| Version | Description |
|---|---|
| V4.5R90F05 | • Added functions: connection anomaly detection configuration and exception IP address of IP groups.<br>• Optimized functions: login security settings and DDoS alert rules. |
| V4.5R90F04 | • Updated the structure based on the new template.<br>• Modified access policies and alert parameters. |

# 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. |
|   | Reminds users to take note. |
|   | Indicates a tip to make your operations easier. |
|   | Indicates a situation in which you might perform an action that could result in equipment damage or loss of data. |
|   | Indicates a situation in which you might perform an action that could result in bodily injury. |
| **A > B** | Indicates selection of menu options. |

# Technical Support

### Hardware and Software Support

Email: support@nsfocusglobal.com

### Cloud Mitigation Support

Email: cloud-support@nsfocusglobal.com

Phone:

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

# Documentation Feedback

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

- Email: info-support@nsfocus.com

# 1 Introduction

ADS M is used to exercise centralized management over ADS devices deployed in cluster mode and to generate reports. An ADS M device can monitor traffic and operating status of multiple ADS devices simultaneously. It collects traffic information and attack alerts from ADS devices and then displays such information on the web-based manager.

ADS M supports region-based management. The monitoring information about traffic and alerts in a region, by default, is available only to users who have access to ADS M, but unavailable to the customer's hosts in the region. To enable the customer's hosts in a region to obtain the monitoring information of their own network, the ADS M administrator can create ADS Portal accounts for region managers and users in different regions and deploy ADS Portal for the regions. A region can have only one Portal account, with the region ID as its user name.

ADS Portal provides a channel for the customer's hosts to obtain information from ADS M about traffic and alerts generated in their region. Through this channel, the monitoring information regarding a region obtained by ADS M can be displayed on the web-based manager of ADS Portal.

| | |
|---|---|
| Note | Whether ADS M supports the Portal system is controlled by the license. The Portal system is available only when a valid license supporting the Portal module is imported for ADS M. |

# 2 Portal Configuration

## 2.1 Creating a Portal Account

The ADS M administrator can create Portal accounts via the web-based manager of ADS M. The administrator can create Portal accounts for both new and existing regions and region managers. For details about regions managed by ADS M, see the *NSFOCUS ADS M User Guide*.

The following sections describe how to create a Portal account for a new region and region manager and for an existing region and region manager.

### 2.1.1 Creating a Portal Account for a New Region

To create a region and create a Portal account for it, follow these steps:

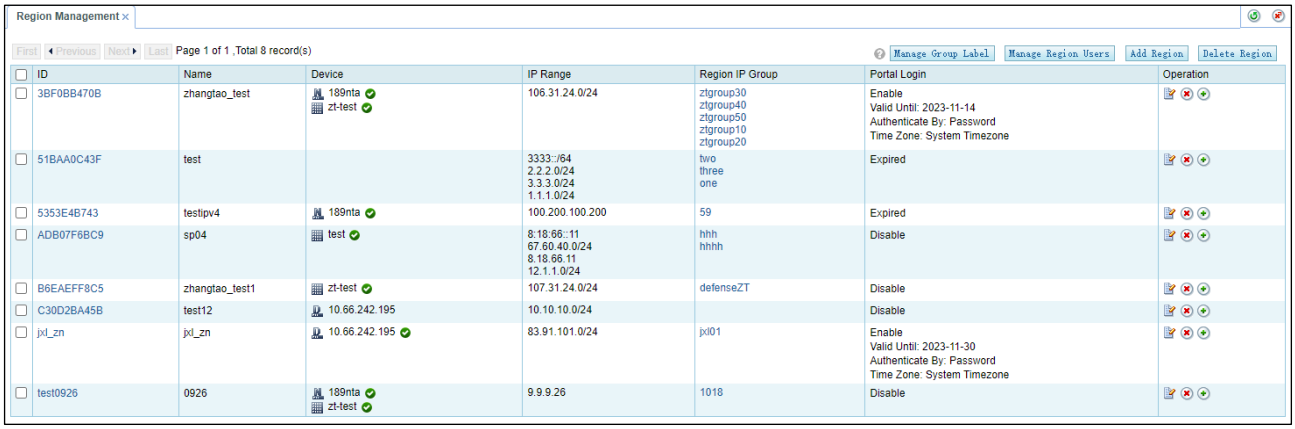
**Step 1** Log in to the web-based manager of ADS M.

For how to log in to ADS M, see the *NSFOCUS ADS M User Guide*.

**Step 2** Choose **Region > Region Management**.

The **Region Management** page appears, as shown in Figure 2-1.

Figure 2-1 Region Management page of ADS M




**Step 3** Click **Add Region**.

**Step 4** Configure basic information, traffic alerts, DDoS attack alerts, and traffic diversion rules for the region step by step.

For details, see the *NSFOCUS ADS M User Guide*.

**Step 5** After traffic diversion rules are configured, click **Next**.

The **Portal Configuration** page appears, as shown in Figure 2-2.

Figure 2-2 Portal configuration page

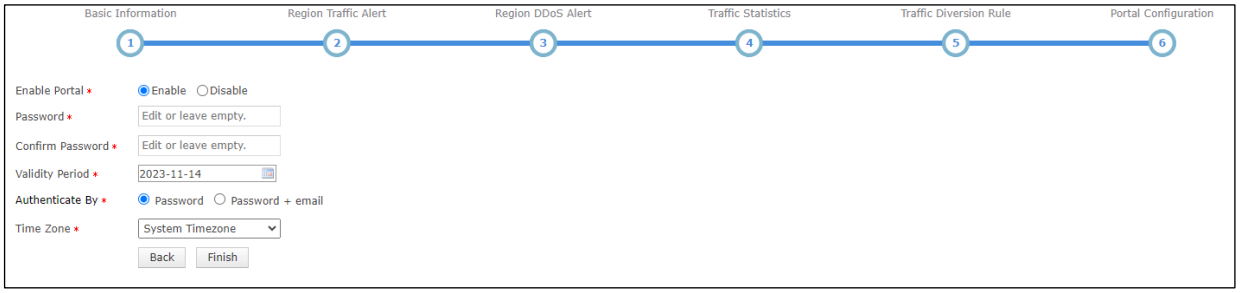



Table 2-1 describes Portal configuration parameters.

Table 2-1 Portal configuration parameters

| 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, which can be viewed under **Administration > User and Audit > Security Settings > Password Security Settings**. |
| 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. |
| Authenticate By | Specifies the authentication method for login to the Portal, which can be **Password** or **Password + email**.<br>• **Password**: The account can log in to the Portal after typing the correct user name and password.<br>• **Password + email**: The account can log in to the Portal after typing the correct user name, password, and the verification code provided via email. |
| 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. The setting takes effect immediately if you change the time zone |

| Parameter | Description |
| --- | --- |
| | on the Portal. For how to change the time zone on the Portal, see section 3.3 Editing Portal Information. |

**Step 6** Configure parameters and click **Finish**.

A new region is added and a Portal account is created for it.

**----End**

## 2.1.2 Creating a Portal Account for an Existing Region

To create a Portal account for an existing region, follow these steps:

**Step 1** Log in to the web-based manager of ADS M.

For the login method, see the *NSFOCUS ADS M User Guide*.

**Step 2** Choose **Region > Region Management**.

The **Region Management** page appears, as shown in Figure 2-1.

**Step 3** Click  in the **Operation** column of a region for which you want to create a Portal account.

**Step 4** Click the step number of **Portal Configuration**.

The Portal configuration page appears, as shown in Figure 2-2.

**Step 5** Enable the Portal and configure Portal account parameters.

For the description of Portal account parameters, see Table 2-1.

**Step 6** Click **Finish**.

A Portal account is now created for the region.

**----End**

## 2.1.3 Creating a Portal Account for a New Region Manager

To create a Portal account for a new region manager, follow these steps:

**Step 1** Log in to the web-based manager of ADS M.

For the login method, see the *NSFOCUS ADS M User Guide*.

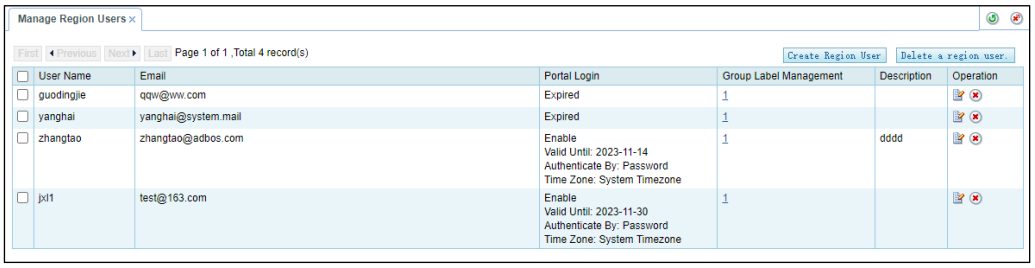
**Step 2** Choose **Region > Region Management.**

The **Region Management** page appears, as shown in Figure 2-1.

**Step 3** Click **Manage Region Users**.

The **Manage Region Users** page appears, as shown in Figure 2-3.

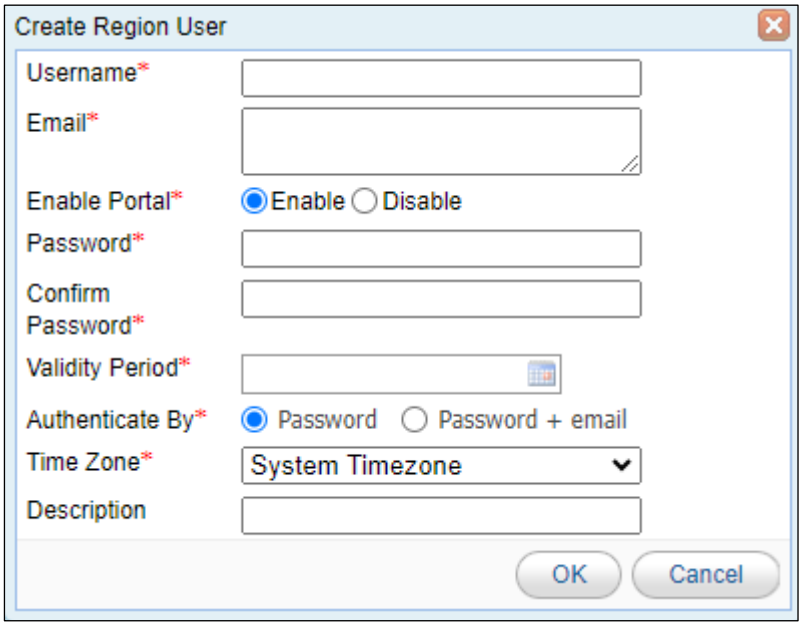
Figure 2-3 Manage Region Users page




**Step 4** Click **Create Region User**.

Information about the Portal account is displayed only after you configure a group label and enable the Portal, as shown in Figure 2-4.

Figure 2-4 Adding a region manager




**Step 5** After enabling the Portal, configure Portal account parameters.

**Username** of the region manager is the user name of the Portal account.

For the description of Portal account parameters, see Table 2-1.

**Step 6** Click **OK**.

A Portal account is now created for the new region manager.

**Step 7** Assign a group label to this region manager.

On the **Manage Region Users** page shown in Figure 2-3, you can click the figure in the **Group Label Management** column to configure permissions for this region manager

A region manager can log in to ADS Portal only when the Portal is enabled for the related account and a group label and appropriate permissions are granted to this account.

| | |
|---|---|
| Note | A Portal account created for a new region manager has the permissions configured in the **Group Label and Permissions** dialog box. A Portal account created in any other way has no such permissions. |

**----End**

## 2.1.4 Creating a Portal Account for an Existing Region Manager

To create a Portal account for an existing region manager, follow these steps:

**Step 1** Log in to the web-based manager of ADS M.

For the login method, see the *NSFOCUS ADS M User Guide*.

**Step 2** Choose **Region** > **Region Management**.

The **Region Management** page appears, as shown in Figure 2-1.

**Step 3** Click **Manage Region Users**.

The **Manage Region Users** page appears, as shown in Figure 2-3.

**Step 4** Click  in the **Operation** column of an existing region manager.

**Step 5** In the **Edit Region User** dialog box, configure the group label, enable the Portal, and configure Portal account parameters.

**Username** of the region manager is the user name of the Portal account.

For the description of Portal account parameters, see Table 2-1.

**Step 6** Click **OK**.

A Portal account is now created for the existing region manager.

**Step 7** Assign a group label to this region manager.

For details, see section 2.1.3 Creating a Portal Account for a New Region Manager.

**----End**

# 2.2 Sending Email Alerts

After email alert sending is enabled, ADS M sends region alert messages to one or more email addresses specified during region configuration.

**Step 1** Log in to the web-based manager of ADS M.

For the login method, see the *NSFOCUS ADS M User Guide*.

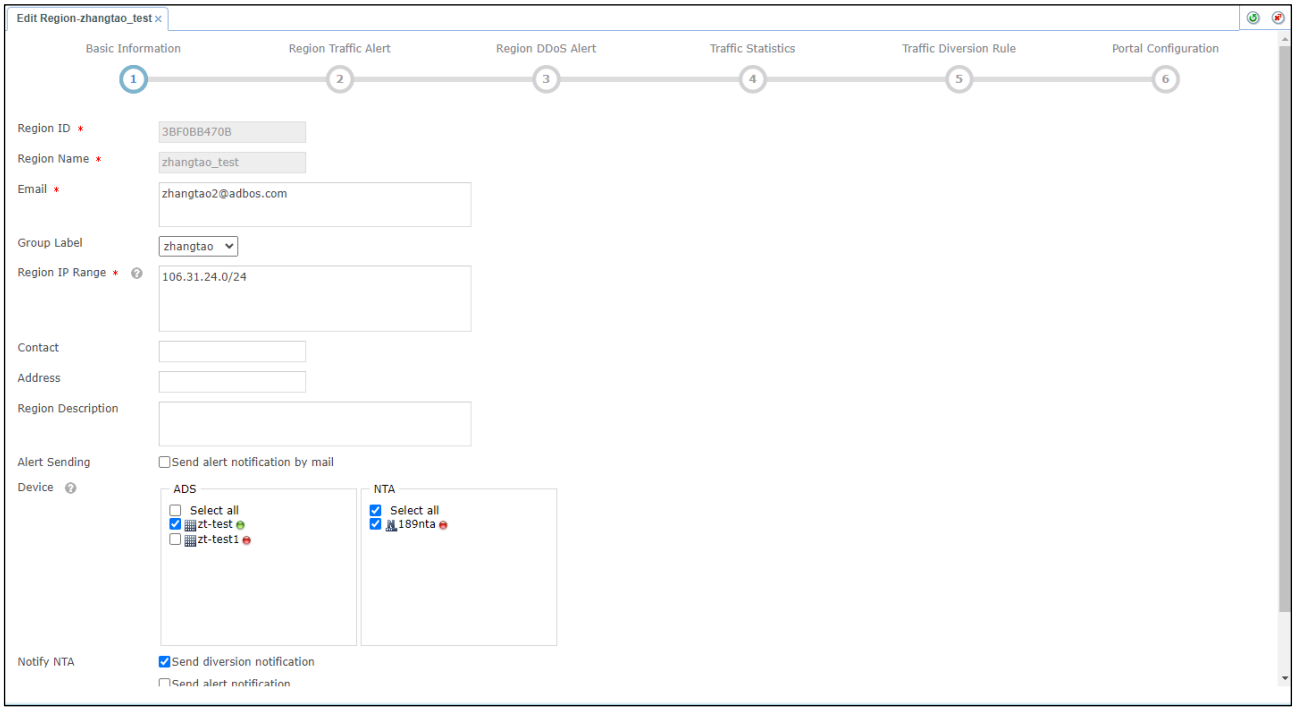
**Step 2** Enable the function of sending email alerts.

a. Click the **Region** menu.

The **Region Management** page appears, as shown in Figure 2-1.

b. When adding or editing a region, select **Send alert notification by mail**, select NTA devices, and configure **Notify NTA**, as shown in Figure 2-5.

Figure 2-5 Enabling the function of sending email alerts

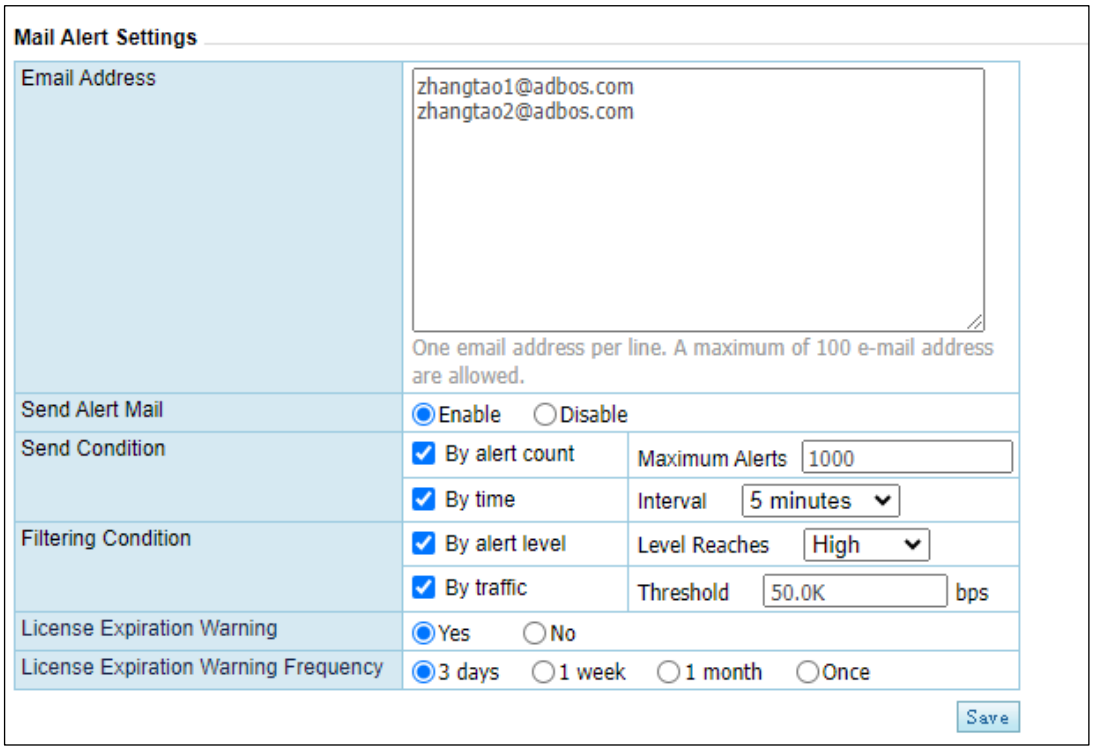



**Step 3** Configure email alert sending parameters.

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

The **Mail Alert Settings** page appears, as shown in Figure 2-6.

Figure 2-6 Configuring mail alert settings




b. Select **Enable** for **Send Alert Mail**.

c. Set **Email Address**, **Send Condition**, and **Filtering Condition**.

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

**----End**

# 2.3 Importing the Portal Virtual Machine

For the initial Portal deployment, you need to import the image file (Portal.vmx) of the Portal virtual machine.

| | |
|---|---|
| Note | Before importing the image file, you need to install the virtual machine environment. VMware Player V4. 0 or later is recommended. |

To import the image file of the Portal virtual machine, follow these steps:

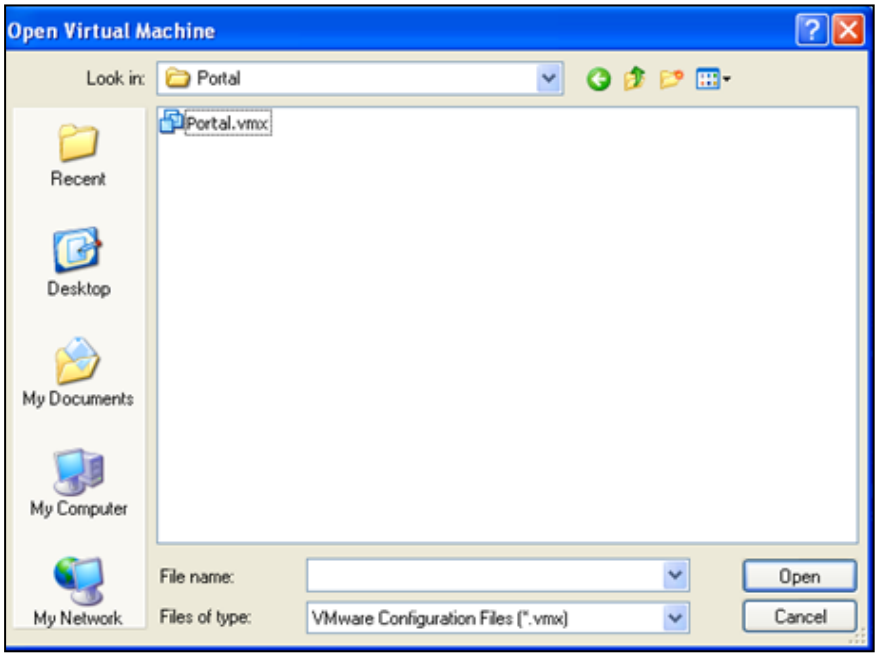
**Step 1** Open VMware Player.

Figure 2-7 Home page of VMware Player


**Step 2** Select **Open a Virtual Machine**.

In the dialog box that appears, locate the image file, **Portal.vmx.**

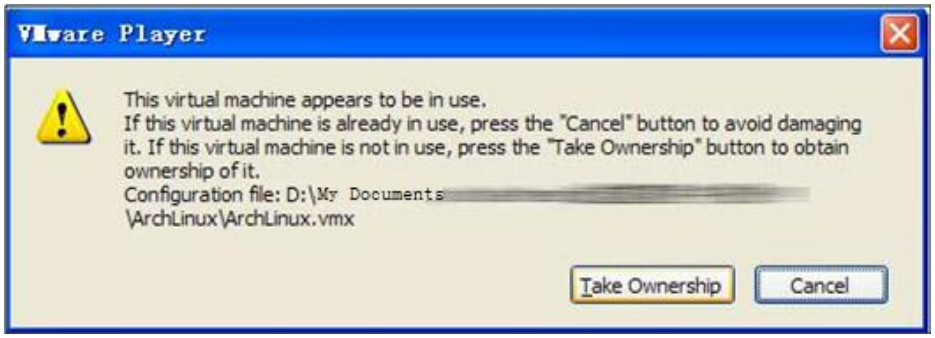
Figure 2-8 Selecting a virtual machine image file




**Step 3** Click **Open**.

**Step 4** In the alert dialog box that appears, click **Take Ownership**.

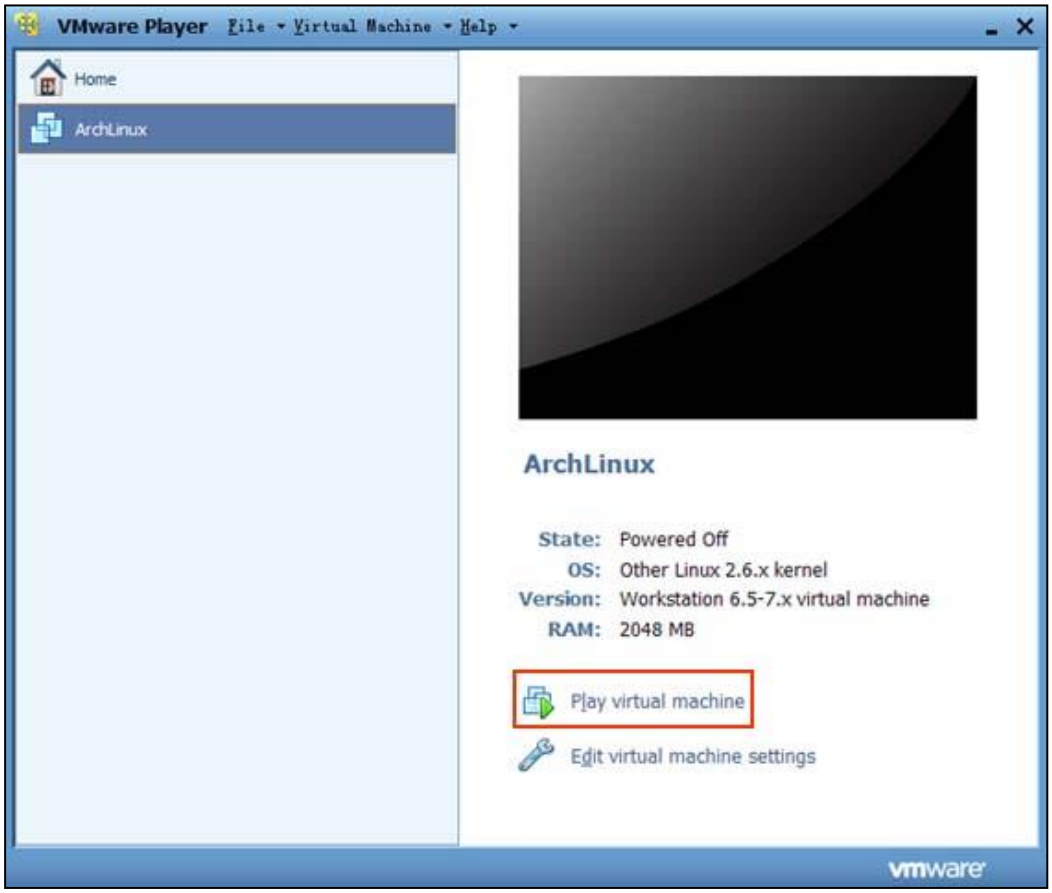
Figure 2-9 Alert message of VMware Player




After the image file is successfully imported, a page appears, as shown in Figure 2-10. At this time, the virtual machine is shut down.

**Step 5** Click **Play virtual machine** to start the virtual machine.

Figure 2-10 Image file imported successfully




**Step 6** Select **I copied it** and click **OK** in the **ArchLinux – VMware Player** dialog box in the process of playing the virtual machine.

Figure 2-11 Virtual machine alert message

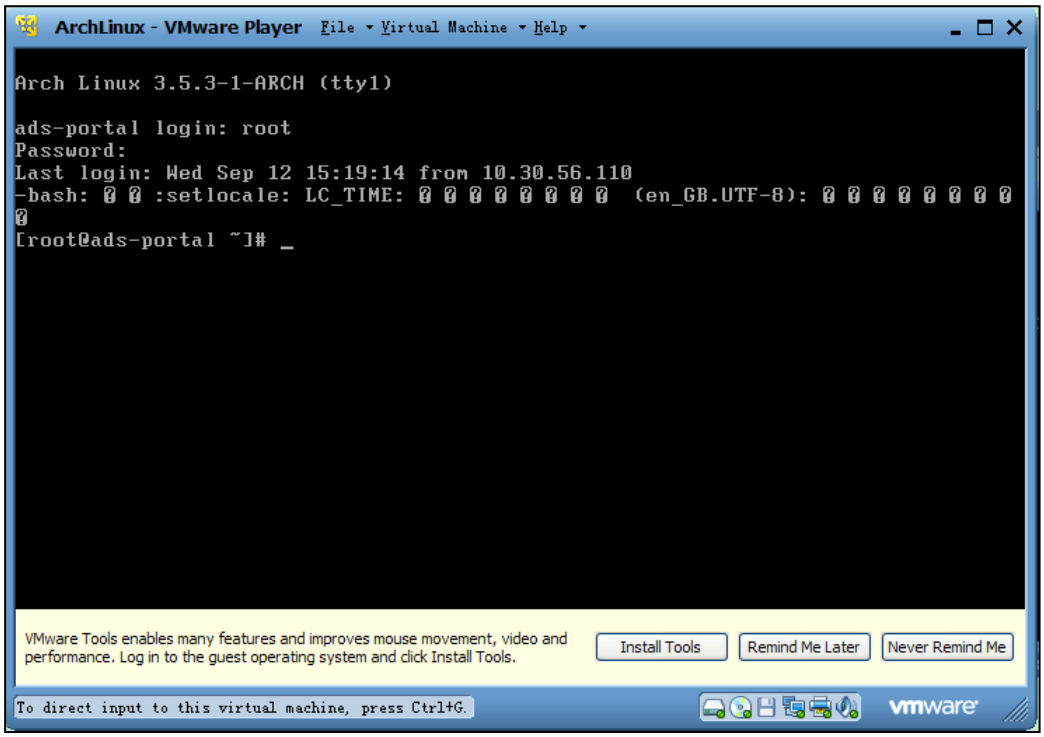

After the virtual machine is started, a window appears, as shown in Figure 2-12, requiring you to log in.

**Step 7** Type the user name and password.

After logging in to the Portal background, set the IP address of the Portal host and the SSH port.

| | |
|---|---|
| Note | • The default login user name of the Portal background is **root** and the default password is **nsfocus**. You must change the password immediately after the first login to avoid information disclosure.<br>• For the default network settings of the virtual machine, see appendix *A* Default Parameters. You can modify the settings as required. |

Figure 2-12 Login to the ADS Portal background




**----End**

# 2.4 Managing the Portal

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

- ADS Portal account

  A region can have only one Portal account, with the region ID as its user name. For details about regions, see the corresponding description in the *NSFOCUS ADS M User Guide*.
- Portal deployment

The ADS M administrator configures and deploys the Portal to set up an information channel between ADS M and the customer's hosts in a region. Therefore, region monitoring information obtained by ADS M can be displayed on the graphic user interface (GUI) of ADS Portal.

After login to the web-based manager of ADS M, you can perform the following operations regarding the Portal:

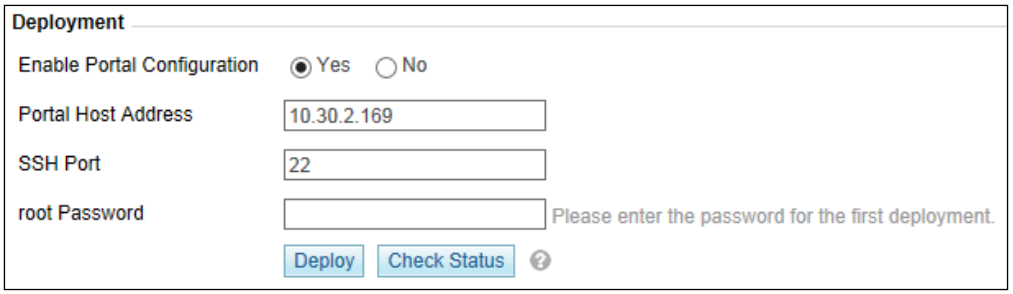
- Deploying the Portal
- Configuring Portal Authentication Parameters
- Replacing the Logo
- Replacing the SSL Certificate
- Configuring Login Security Parameters

## 2.4.1 Deploying the Portal

To deploy the Portal, follow these steps:

**Step 1** Choose **Administration** > **Third-Party Interface** > **Portal Configuration**.

Figure 2-13 Deployment area on the Portal Configuration page




**Step 2** Enable Portal configuration.

Select **Yes** for **Enable Portal Configuration**.

**Step 3** Configure Portal parameters.

Table 2-2 describes Portal parameters.

Table 2-2 Portal parameters

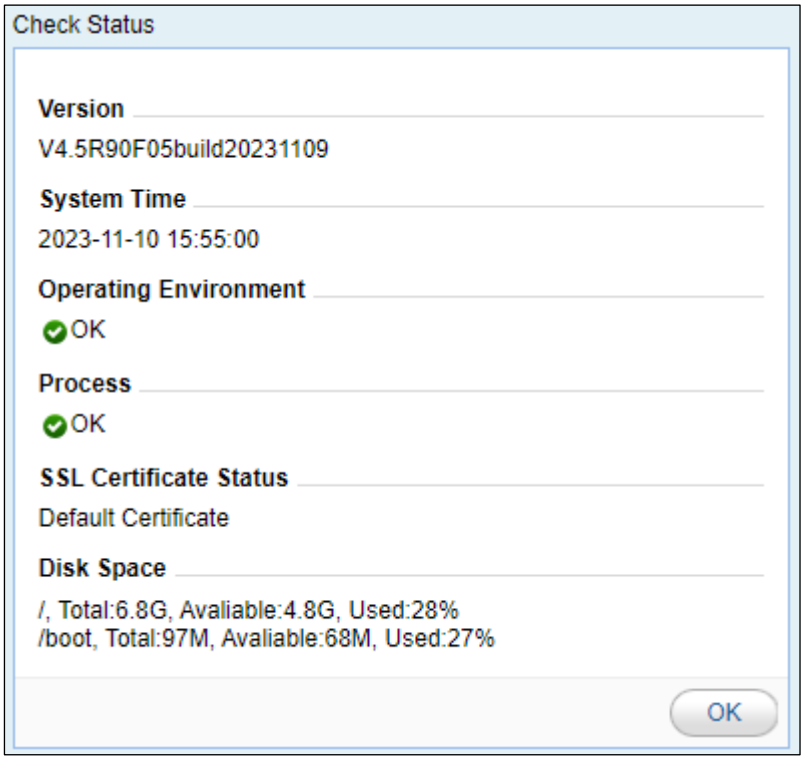
| Parameter | Description |
|---|---|
| Portal Host Address | Specifies the IP address of the host on which the Portal virtual machine is installed. The customer can log in to the Portal system using this IP address.<br>Both IPv4 and IPv6 addresses are allowed here. |
| SSH Port | Specifies the SSH port for the communication between the customer's hosts and the Portal host. |
| root Password | Specifies the password used by the user **root** to log in to the Portal virtual machine. For the **root** password and how to configure the Portal virtual machine, see section 2.3 Importing the Portal Virtual Machine.<br>The **root** password is required only for the first Portal deployment and can |

| Parameter | Description |
|---|---|
| | be left empty for subsequent deployments. |

**Step 4** Click **Deploy** to save the configuration and deploy the Portal.

**Step 5** (Optional) Click **Check Status** to check the status of the Portal host.

Figure 2-14 Portal status




**----End**

| | |
|---|---|
| Note | You can configure the authentication method, choose whether to replace the logo, and configure login security settings only after deploying the Portal. |

## 2.4.2 Configuring Portal Authentication Parameters

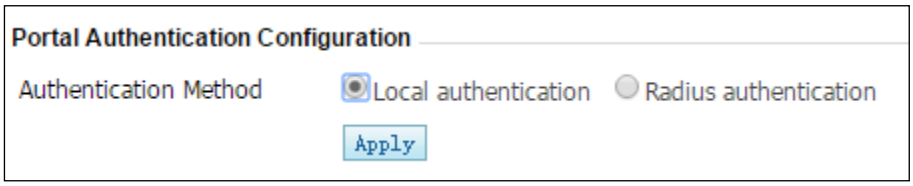
Portal users can be authenticated locally or by a third-party Radius server.

To configure Portal authentication parameters, follow these steps:

**Step 1** Choose **Administration** > **Third-Party Interface** > **Portal Configuration**.

Figure 2-15 shows the Portal Authentication Configuration area.

Figure 2-15 Portal deployed




**Step 2** Select a Portal authentication method.

Options include **Local authentication** and **Radius authentication**.

**Step 3** (Optional) When **Authentication Method** is set to **Radius authentication**, set Radius server parameters, as shown in Figure 2-16.

Figure 2-16 Radius server configuration

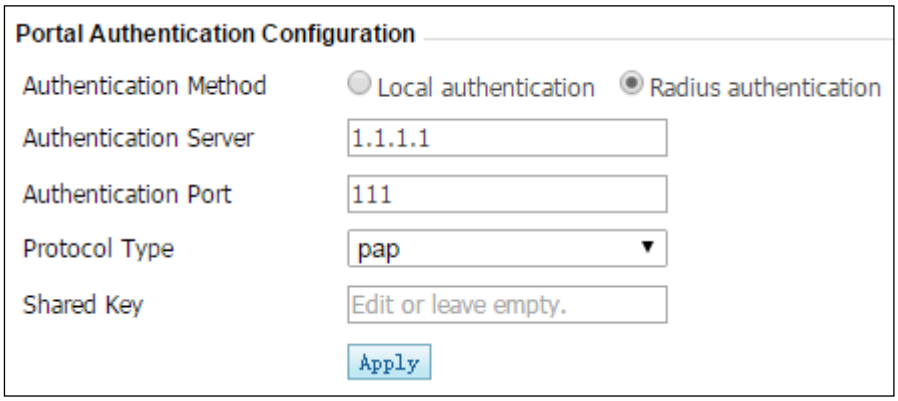



Table 2-3 describes parameters for configuring the Radius server.

Table 2-3 Parameters for configuring the Radius server

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

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

**----End**

## 2.4.3 Replacing the Logo

The logo on the login page, home page, **Reset Password** page, and report page can be customized.

To replace the logo, follow these steps:

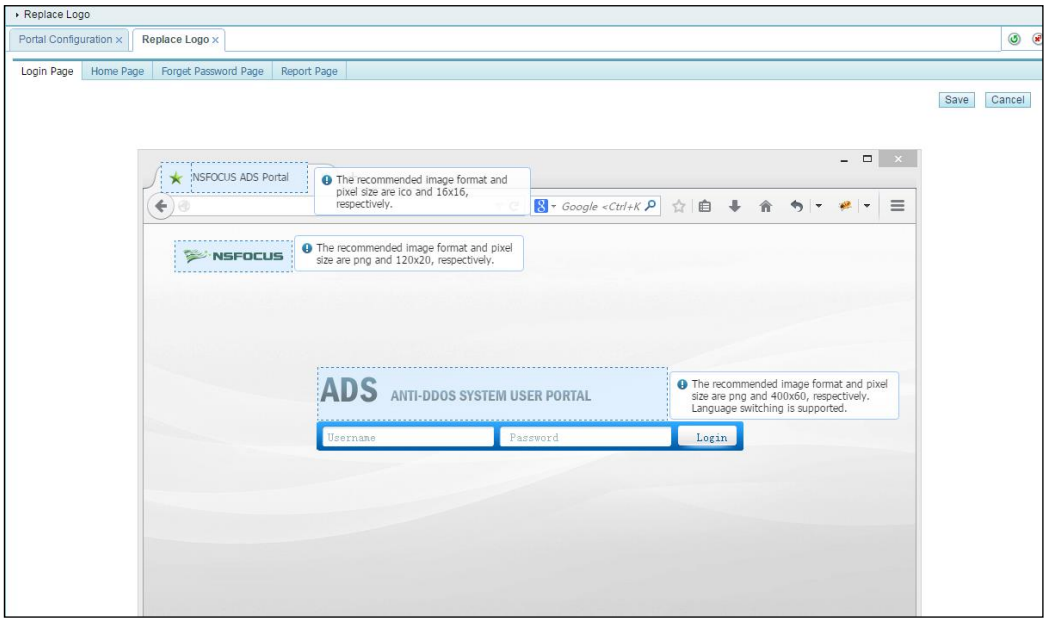
**Step 1** Choose **Administration** > **Third-Party Interface** > **Portal Configuration**.

Figure 2-17 shows the **Logo Replacement** area.

Figure 2-17 Logo Replacement area


**Step 2** Click **Replace Logo** and replace the logo on the Portal login page, home page, **Reset Password** page, or report page.

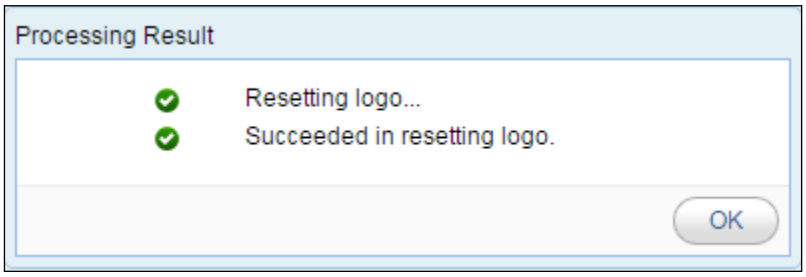
Figure 2-18 Replacing the login page logo




In addition to the logo, you can also change the GUI titles.

**Step 3** Click **Reset Logo** to restore factory defaults for the logo on and titles of the login page, home page, **Reset Password** page, and report page.

Figure 2-19 Resetting the logo and title




**----End**

## 2.4.4 Replacing the SSL Certificate

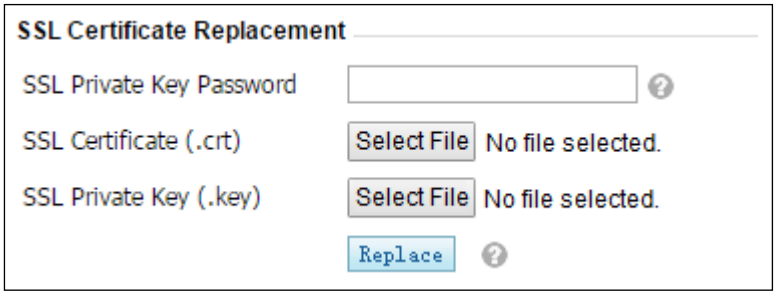
The system has a built-in SSL certificate, which can be replaced.

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

**Step 1** Choose **Administration** > **Third-Party Interface** > **Portal Configuration**.

Figure 2-20 shows the **SSL Certificate Replacement** area.

Figure 2-20 SSL Certificate Replacement area




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

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

**Step 4** Browse to the SSL private key file and then click **Open**.

**Step 5** Click **Replace** to complete the operation.

The system then automatically restarts the web service of the Portal.

**----End**

## 2.4.5 Configuring Login Security Parameters

To configure login security parameters, follow these steps:

**Step 1** Choose **Administration** > **Third-Party Interface** > **Portal Configuration**.

Figure 2-21 shows the **Login Security Settings** area.

Figure 2-21 Login Security Settings area


**Step 2** Set the session timeout interval and click **Apply**.

The system then automatically restarts the web service of the Portal.

**Step 3** If you remain inactive for a period longer than the value specified here, the system automatically logs you out.

**----End**

# 3 Getting Started

## 3.1 Login

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

**Step 1** Make sure that the host has been connected to ADS M.

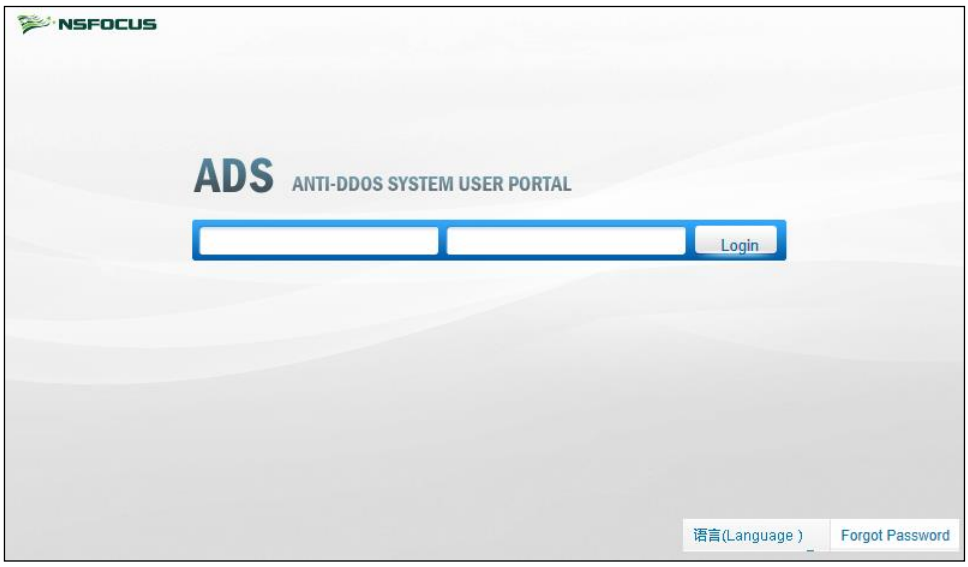
**Step 2** Open the browser (Chrome is used here) and access ADS Portal in HTTPS mode by typing the server IP address, such as https://192.168.1.100, and pressing **Enter**.

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

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

The login page appears, as shown in Figure 3-1.

Figure 3-1 Web login page of ADS Portal

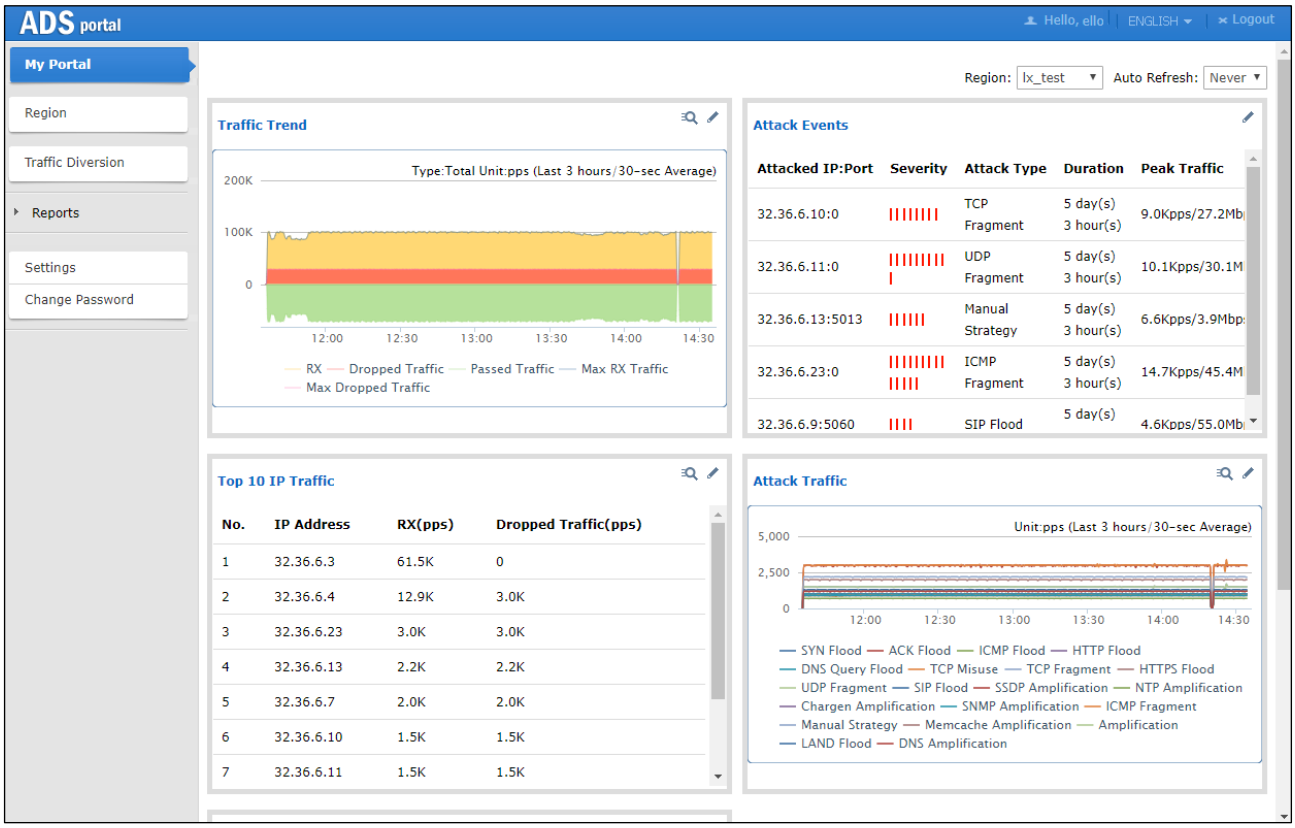



**Step 4** Type the user name and password and then click **Login** or press **Enter**.

A page shown in Figure 3-2 appears, indicating that you have successfully logged in to the system.

| | |
|---|---|
| Note | You can ask the system administrator of ADS M or the region administrator for the user name and initial password of the Portal account. |

Figure 3-2 Home page of the web-based manager




**----End**

| | |
|---|---|
| Note | • The browser you use must support JavaScript, cookies, and frames.<br>• You are advised to use the latest version of Chrome, Firefox, or Edge and set the display resolution to 1280 x 700 or higher.<br>• You must change the initial password immediately after the first login.<br>• If you are authenticated by password + email, you need to type a correct password and verification code provided via email. The user account will be locked after several failed verification code attempts. |

# 3.2 Page Layout

Figure 3-3 shows the layout of the web-based manager of ADS Portal.

Figure 3-3 Layout of the web-based manager

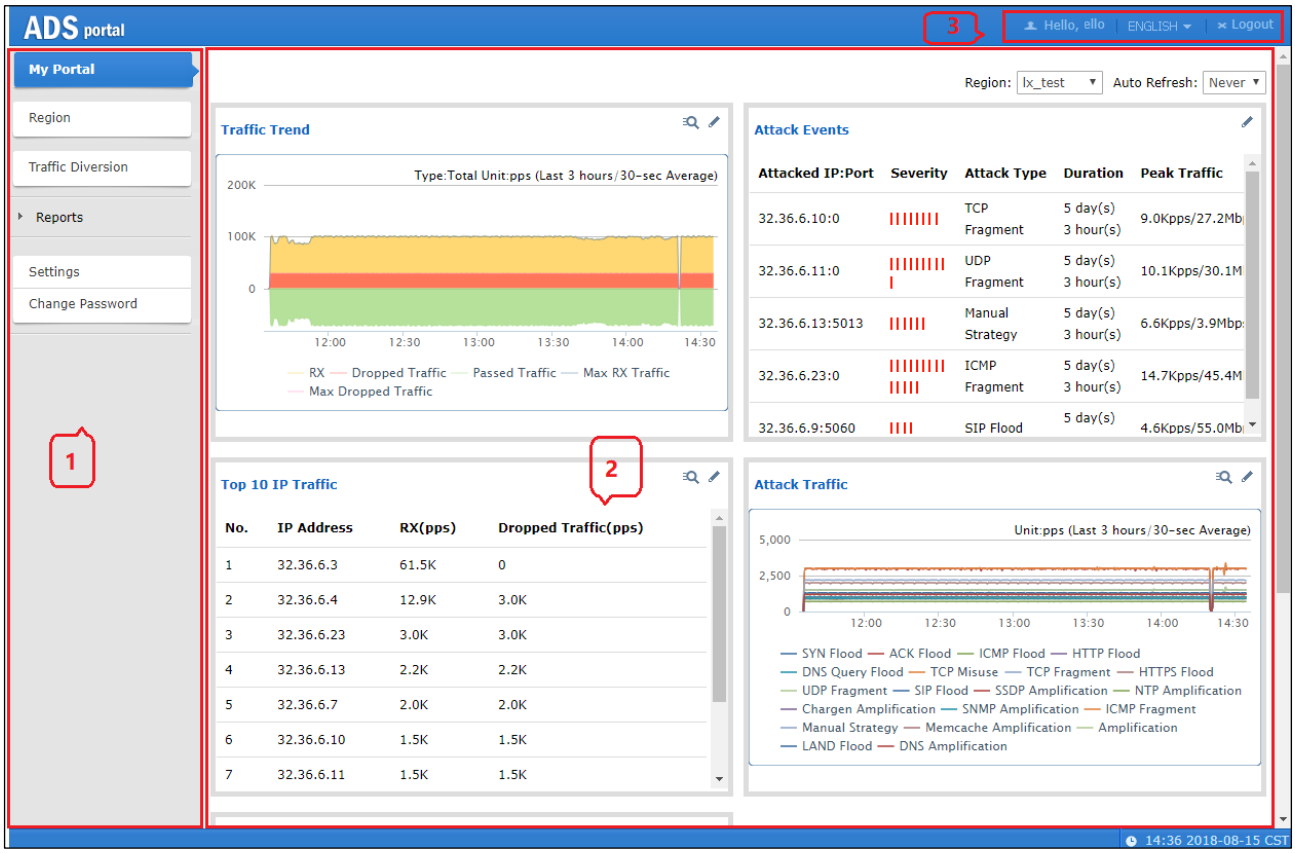



Table 3-1 describes the layout of the web-based manager.

Table 3-1 Webpage layout

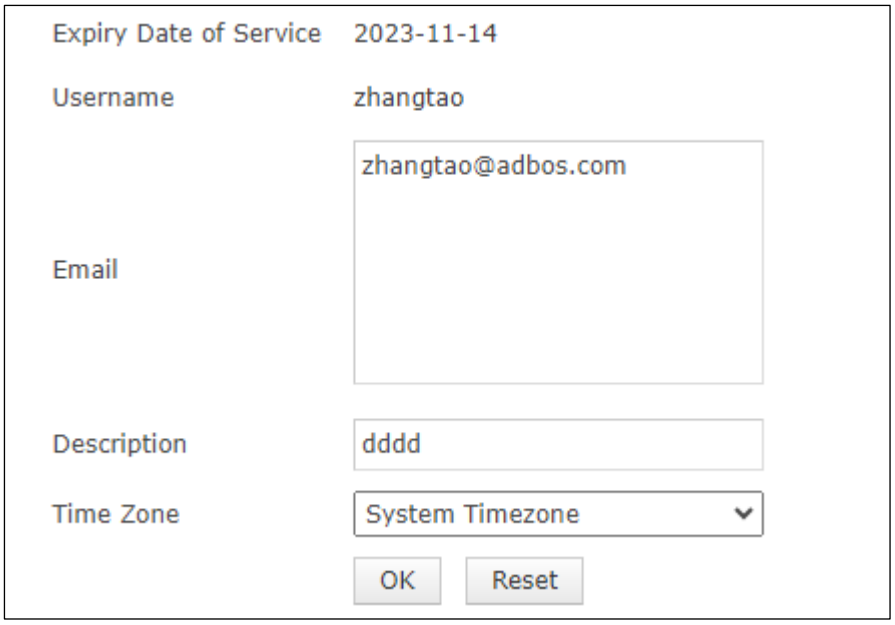
| No. | Area | Description |
|---|---|---|
| 1 | Menu bar | Main menus of the system. |
| 2 | Work area | Area where you can perform configurations and operations and view data. |
| 3 | Quick access bar | Provides buttons for quick access to certain functions of the system.<br>• ENGLISH: switches between simplified Chinese and English.<br>• Logout: logs you out of ADS Portal.<br>Note<br>Changes to user information takes effect within one minute and is synchronized to region configurations of ADS M. For details about region configuration on ADS M, see the corresponding description in the *NSFOCUS ADS M User Guide*. |

## 3.3 Editing Portal Information

On the page shown in Figure 3-3, click the **Settings** menu. A user logging in with a region ID can change only the time zone. A user logging in as a region manager can also change the email address and description.

The Portal information page appears, as shown in Figure 3-4.

Figure 3-4 Portal information page




Edit Portal information and then click **OK** to save the changes.

## 3.4 Changing the Password of a Portal Account

On the page shown in Figure 3-3, click the **Change Password** menu.

Change the password of the Portal account and then click **OK** to save the change.

## 3.5 Resetting the Password of a Portal Account

You can reset the password of a Portal account only after the ADS M system user **admin** selects **Enable** for **Reset Password** under **Administration > User and Audit > Security Settings > Password Security Settings**. Otherwise, the system will prompt you that "The password cannot be reset. Please contact the administrator" after you click **Forgot Password**.

On the login page shown in Figure 3-1, click **Forgot Password** in the lower-right corner.

Type the user name and email address, and then click **Next**. The system will send the new password to the registered email address.

| | |
|---|---|
| Note | You must enter a valid email address; otherwise, the password cannot be reset. When you set a password for the Portal account, the password strength must be consistent with that specified under **Administration > User and Audit > Security Settings** on ADS M. |

# 4 Region Management

A user can log in to the web-based manager of the Portal as a region manager or with a region ID. In either case, the user can manage regions, but the permissions vary with the type of the login account.

## 4.1 Management of Regions by a Region Manager

Permissions of a region manager are assigned when a global label is allocated to him or her. Different region managers have different permissions.

If you log in to the Portal as a region manager with full permissions and click **Region** in the left pane of the page shown in Figure 3-3, the region management page appears, as shown in Figure 4-1.

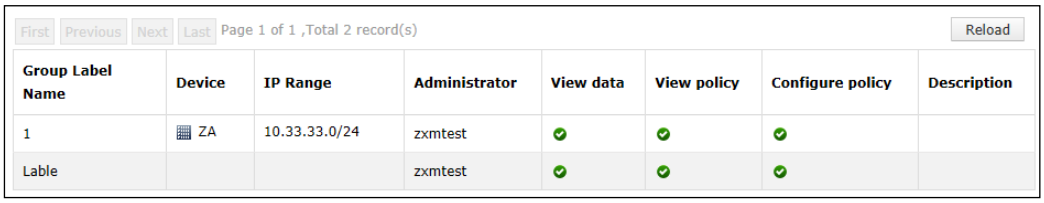
Figure 4-1 Region list


### 4.1.1 Viewing the Group Label

On the page shown in Figure 4-1, click **View Group Label**. Then the group label assigned to the current region manager and his or her privileges are displayed, as shown in Figure 4-2.

To change the group label, you must perform related operations on the web-based manager of ADS M. For details, see the *NSFOCUS ADS M User Guide*.

Figure 4-2 Viewing the group label



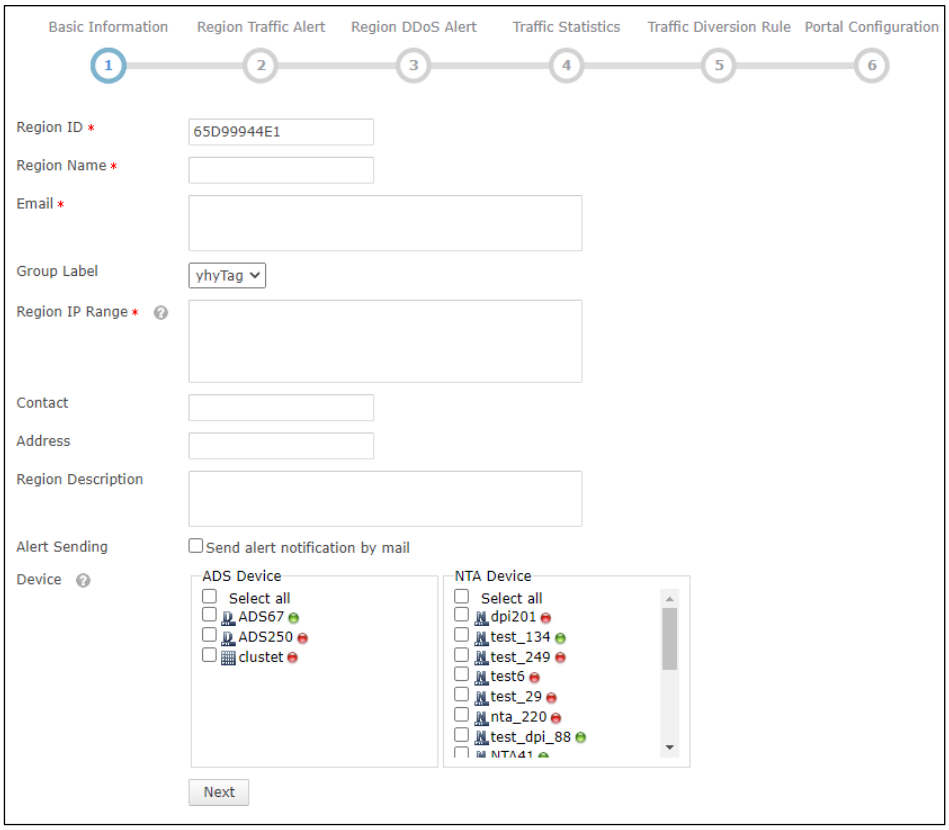

## 4.1.2 Creating a Region

You can also create, edit, and delete a region on the web-based manager of ADS M. For details, see the *NSFOCUS ADS M User Guide*.

To create a region, follow these steps:

**Step 1** In the upper-right corner of the page shown in Figure 4-1, click **Add Region**.

Figure 4-3 Configuring basic information of the region




**Step 2** Configure basic information of the new region.

Table 4-1 describes parameters for configuring basic information of a region.

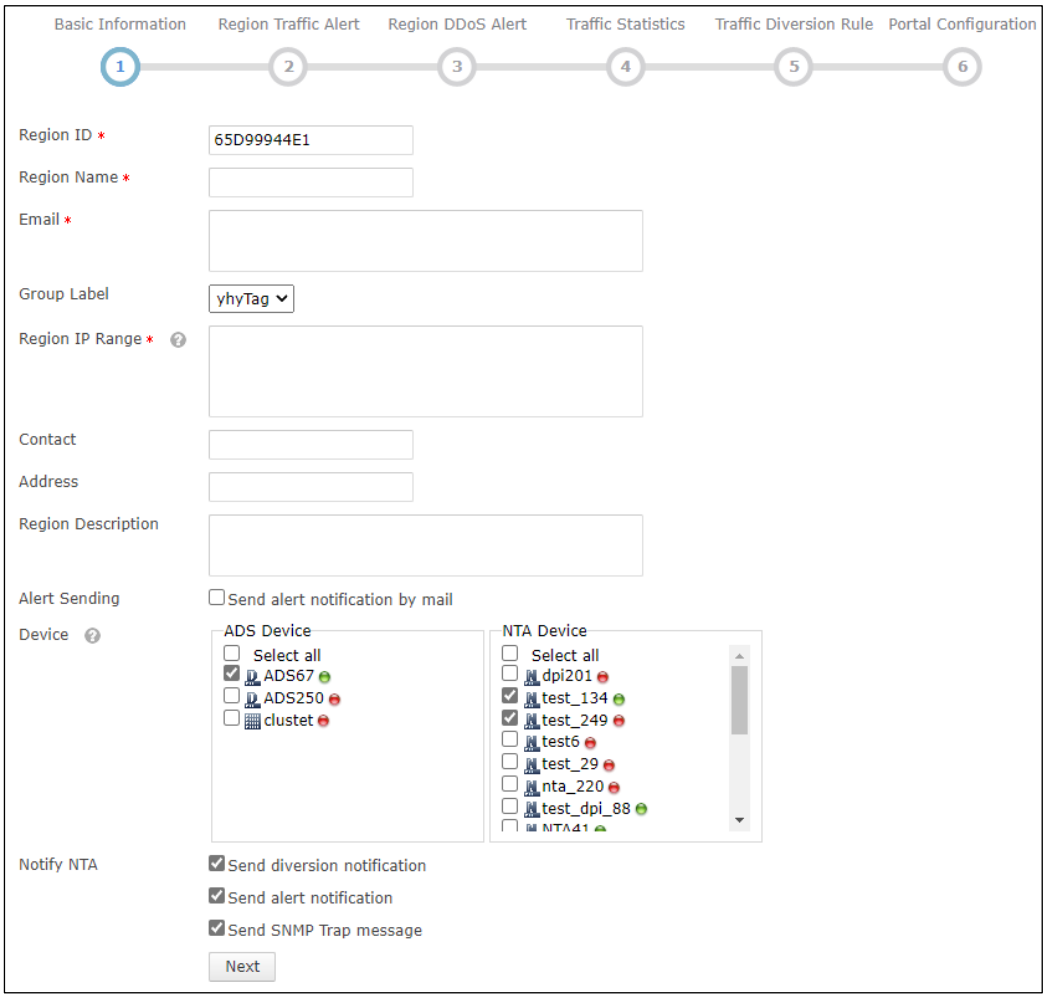
Table 4-1 Parameters for configuring basic information of a region

| 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 one) when you create a region. The region ID should be a string of 1 to 100 characters, consisting of letters, digits, and/or underscores. |
| Region Name | Name of the region, which should be a string of 1 to 50 characters, consisting of 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 (;).<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 2.2 Sending Email Alerts. |
| Group Label | Group label of the region. |
| 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 address ranges, 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 112–128. |
| 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 alerts regarding a host in the region. |
| Device | Specifies ADS and NTA devices for the region. Only devices that are managed by ADS M are available for you to select.<br>For NTA, you can select devices of either the DPI or DFI type, but cannot use both types at the same time. |

**Step 3** Configure what to be notified to NTA.

In Figure 4-3, after selecting one or multiple NTA devices, you can specify types of notifications to be sent to NTA via email.

Figure 4-4 Configuring what to be notified to NTA




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

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

b. Configure parameters on this page.

Table 4-2 Region traffic alert parameters

| Parameter | Description |
|---|---|
| Alert Latency Period | Specifies the maximum duration NTA must wait to generate an alert for the traffic between the value of **Latent Alert Threshold** and that of **Direct Alert Threshold**. The value ranges are 0–23 for the hour (**h**) and 0–59 for the minute (**m**). For the second (**s**), you can click ▲ or ▼ to set it to **0s** or **30s**. |
| Alert Holding Period | Specifies the time when an alert persists after the traffic rate falls below the value of **Direct Alert Threshold**, which indicates that the attack ends. This parameter is valid only for latent alerts. The value ranges are 0–23 for the hour (**h**) and 0–59 for the minute (**m**). For the second (**s**), you can click ▲ or ▼ to set it to **0s** or **30s**. |
| Alert Type | Specifies the type of region traffic alerts, which can be either of the following: |

| Parameter | Description |
|---|---|
| | • **Region Inbound Traffic Alert**: checks the total inbound traffic of the region.<br>• **Region Outbound Traffic Alert**: checks the total outbound traffic of the region. |
| Detection Mode | Specifies the type of traffic based on which an alert is generated. It has the following values:<br>• **Not detect**: indicates that NTA does not check whether inbound or outbound traffic is abnormal.<br>• **Packets only**: indicates that an alert is generated when the traffic rate in pps is found to exceed the threshold.<br>• **Bytes only**: indicates that an alert is generated when the traffic rate in bps is found to exceed the threshold.<br>• **Both packets and bytes**: indicates that an alert is generated when the traffic rate in pps and that in bps are both found to exceed the thresholds.<br>• **Either packets or bytes**: indicates that an alert is generated when either the traffic rate in pps or that in bps is found to exceed the threshold. |
| Latent Alert Threshold | Specifies the traffic rate threshold in bps or pps that triggers NTA to generate an alert only after the traffic rate stays at this level for some time.<br>• **bps**: indicates a threshold in bps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **Not detect** or **Packets only** for **Detection Mode**.<br>• **pps**: indicates a threshold in pps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **Not detect** or **Bytes only** for **Detection Mode**.<br>Note<br>The latent alert threshold must be lower than the direct alert threshold. |
| Direct Alert Threshold | Specifies the traffic rate threshold in bps or pps that triggers NTA to generate an immediate alert.<br>• **bps**: indicates a threshold in bps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **Not detect** or **Packets only** for **Detection Mode**.<br>• **pps**: indicates a threshold in pps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **Not detect** or **Bytes only** for **Detection Mode**.<br>Note<br>Note that the direct alert threshold must be greater than the latent alert threshold. |
| Alert Hierarchy(%) | Specifies how to classify alert levels. **Latent Alert Threshold** is a basis for classifying alert levels and needs to be configured in advance. Alert levels are classified according to the ratio of actual traffic to the **Latent Alert Threshold** value:<br>• **Low**: specifies the lowest ratio for triggering a low-level alert. The value is always **100**. When the actual ratio falls between the smallest ratio for |

| Parameter | Description |
|---|---|
| | triggering a lower-level alert and the smallest ratio for triggering a medium-level alert, NTA generates a low-level alert.<br>• **Medium**: specifies the ratio for triggering a medium-level alert. The default value is **150** and the maximum value is **10000**. When the actual ratio falls between the smallest ratio triggering a medium-level alert and the smallest ratio for triggering a high-level alert, NTA generates a medium-level alert.<br>• **High**: specifies the ratio for triggering a high-level alert. The default value is **200** and the maximum value is **10000**. When the actual ratio is greater than the smallest ratio for triggering a high-level alert, NTA generates a high-level alert.<br>If **Alert Hierarchy** is not configured, NTA will detect traffic and send alerts according to the global alert hierarchy. |
| Diversion Level | Specifies the alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted.<br>• **No diversion**: indicates that no traffic diversion will take place.<br>• **Divert Traffic of Low-level Alert**: indicates that a low-level alert or higher will trigger traffic diversion.<br>• **Divert Traffic of Medium-level Alert**: indicates that a medium-level alert or higher will trigger traffic diversion.<br>• **Divert Traffic of High-level Alert**: indicates that only a high-level alert can trigger traffic diversion. |
| Carpet Bombing Detection | Controls whether to enable the carpet bombing detection function. By default, this function is disabled.<br>After you select **Open**, NTA will check traffic for carpet bombing attacks. Carpet bombing is a kind of DDoS attack that targets a large number of IP addresses. |
| TopN | Specifies the number of top IP addresses with the largest inbound traffic for the carpet bombing detection.<br>Value range: 3–300.The value **3** indicates that the proportion of aggregate inbound traffic to the top 3 IP addresses to the total traffic will be compared with the number specified for **Threshold Percentage**. If the former is less than the latter, a carpet bombing alert is generated. |
| Threshold Percentage | Specifies the percentage of aggregate inbound traffic to top n IP addresses to the total traffic.<br>Value range: 1–100.The value **1** indicates that if the percentage of aggregate inbound traffic to top n IP addresses to the total traffic is less than 1, a carpet bombing alert is generated. |

**Step 5** Configure region DDoS alert parameters.

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

b. Configure parameters on this page.

- **Region DDoS Alert Period Configuration**: Configure **Alert Latency Period** and **Alert Holding Period**. For specific configuration, see Table 4-2.
- **Region DDoS Alert**: Respectively configure Inbound Check Configuration and Outbound Check Configuration.

- **Inbound Check Configuration**: supports **Fixed Threshold Configuration**, **Constituent Proportion Configuration**, and **Connection Anomaly Detection Configuration**.

  For details about parameter description of the former, see Table 4-2.

  To configure a constituent proportion alert policy, enable the function in the **Status Control** area, and configure alert parameters. If the traffic exceeds both **Min Trigger Threshold** and **Proportion for Direct Alerts**, the system directly generates an alert. For the configurations of other parameters, see Table 4-2.

  **Connection Anomaly Detection Configuration** checks whether the IP segments covered by the region have more abnormal connections than the specified threshold. For detailed parameters, see Table 4-3.

- **Outbound Check Configuration**: Configure **Constituent Proportion Configuration** after enabling this function.

Table 4-3 DDoS attack alert parameters (abnormal connections)

| Parameter | Description |
|---|---|
| Detect Mode | Specifies a basis for DDoS detection and alerting. Options include **Not detect** and **Abnormal Connections**.<br>The **Latent Alert Threshold** and **Direct Alert Threshold** parameters can be configured after this parameter is set to **Abnormal Connections**. |
| Latent Alert Threshold | Specifies a threshold for the number of connections to an IP address in the statistical period (usually 30 seconds). When the number of connections exceeds this threshold, but is below the direct alert threshold, NTA does not generate an alert until the number of connections stays above this threshold for some time (alert latency period).<br>Value range: 1–65535. The latent alert threshold must be smaller than the direct alert threshold. |
| Direct Alert Threshold | Specifies a threshold for the number of connections to an IP address in the statistical period (usually 30 seconds) that will trigger NTA to generate an alert.<br>Value range: 1–65535. The direct alert threshold must be larger than the latent alert threshold. |
| Alert Level | Specifies how to classify alert levels for the low-and-slow attack detection against each IP address in the region.<br>• **Medium**: specifies the lowest proportion to trigger a medium-level alert. The default value is **150**, indicating that when the number of connections is higher than 1.5 times the **Latent Alert Threshold** but lower than the lowest proportion triggering a high-level alert, NTA generates a medium-level alert.<br>• **High:** specifies the lowest proportion to trigger a high-level alert. The default value is **200**, indicating that when the number of connections is higher than 2 times the **Latent Alert Threshold,** NTA generates a high-level alert.<br>Value range: 100–10000. The value specified for **High** should be larger than that for **Medium**. |
| Diversion Level | • Specifies an alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted.<br>• **No diversion**: generates alerts only, with no traffic diversion to take place.<br>• **Divert Traffic of Low-level Alert**: indicates that a low-level alert or higher will trigger traffic diversion.<br>• **Divert Traffic of Medium-level Alert**: indicates that a medium-level alert or higher will trigger traffic diversion. |

| Parameter | Description |
| --- | --- |
| | • **Divert Traffic of High-level Alert**: indicates that only a high-level alert can trigger traffic diversion. |

**Step 6** Configure the region traffic statistics function.

You can specify statistical items of traffic for the region and click **Save**. After that, click **Next** to configure region traffic diversion rules.

**Step 7** Configure region traffic diversion rules.

Configure traffic diversion parameters on the **Traffic Diversion Rule** page after you configure the traffic statistics function and click **Next**.

Table 4-4 describes parameters for configuring traffic diversion rules.

Table 4-4 Parameters for configuring traffic diversion rules

| Parameter | | Description |
| --- | --- | --- |
| Region Diversion Policy | Number of Inbound-Traffic diverted IPs in Region | Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 300.<br>When **Diversion Policy for Abnormal Region Inbound Traffic** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses. |
| | Diversion Policy for Abnormal Region Inbound Traffic | Specifies the diversion policy for inbound traffic of top N IP addresses when the inbound traffic alert is triggered.<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>  <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. |
| | Number of Outbound-Traffic diverted IPs in Region | Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 100.<br>When **Diversion Policy for Abnormal Region Outbound Traffic** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses. |
| | Diversion Policy for Abnormal Region Outbound Traffic | Specifies the diversion policy for outbound traffic of top N IP addresses when the outbound traffic alert is triggered.<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**. |

| Parameter | | Description |
|---|---|---|
| | | • 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. The traffic (in bps or pps) or abnormal connections to a specific IP address reach the threshold, diversion takes place.<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 8** Configure the Portal.

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

b. Configure parameters on this page.

Table 4-5 describes the parameters for configuring the Portal.

Table 4-5 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. |
| Confirm Password | Requires you to type the password again. The password you typed here must be the same as that you typed for **Password**. |
| Validity Period | Specifies how long the Portal account will be valid for use. After the validity period expires, this Portal account will be invalid. |
| Authenticate By | Specifies the authentication method for login to the Portal, which can be **Password** or **Password + email**.<br>• **Password**: The account can log in to the Portal after typing the correct user name and password.<br>• **Password + email**: The account can log in to the Portal after typing the correct user name, password, and the verification code provided via email. |
| Time Zone | Specifies the time zone that the Portal account belongs to. |

**Step 9** Click **Finish** to save the settings.

A new region is thus added.

**----End**

## 4.1.3 Editing a Region

In the region list shown in Figure 4-1, click in the **Operation** column of a region to open the page for editing the region. Edit settings of the region step by step.

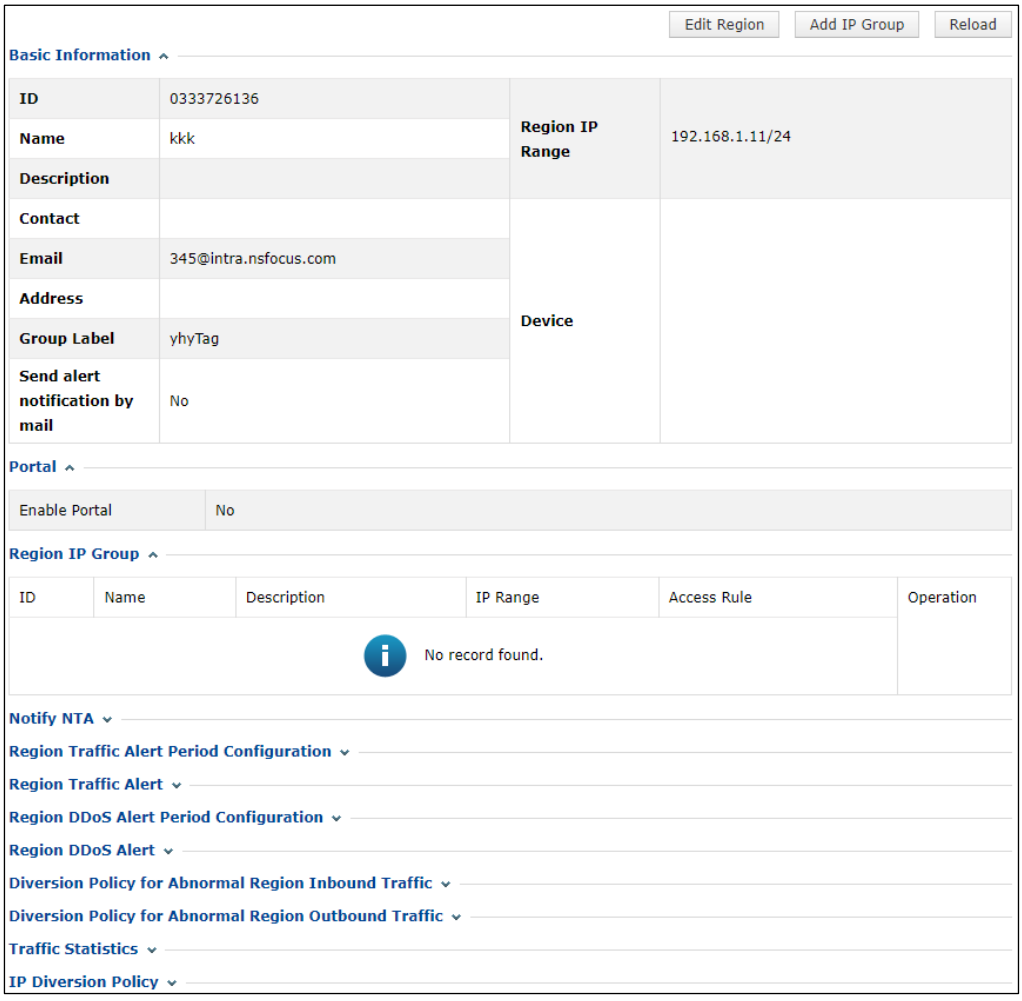
## 4.1.4 Deleting a Region

In the region list shown in Figure 4-1, click in the **Operation** column of a region to delete this region.

## 4.1.5 Viewing Region Settings

In the region list shown in Figure 4-1, click a region ID to view the settings of this region.

Figure 4-5 Viewing region settings



## 4.1.6 Creating an IP Group

To create an IP group, follow these steps:

**Step 1** In the list shown in Figure 4-1, click  in the **Operation** column of a region.

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

Table 4-6 describes parameters for configuring basic information of an IP group.

Table 4-6 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 create an IP group. The IP group ID should be a string of 1 to 50 characters, consisting of 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 letters, digits, and/or underscores. |
| Included IPs | IP address range monitored and protected by ADS M.<br>• You can type one or more IP addresses, IP subnets, and IP address ranges, with each in a separate line. A maximum of 1024 entries are allowed.<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. |
| Exception IPs | Specifies the IP addresses, IP subnets, or IP segments excluded from the IP range of the protection group. The exceptions configured here will not be protected by the policies for this IP group.<br>The format is the same as that for **Included IPs**. |
| IP Group Description | Brief description of the IP group. |
| Notify NTA | Controls whether to send diversion notifications, alert notifications, or SNMP trap messages to NTA. |

**Step 3** Configure IP group traffic alert parameters.

a. After configuring basic information, click **Next** to open the **IP Group Traffic Alert** page.

b. Configure parameters on this page.

Parameter configuration here is similar to that for a region. For the description of parameters, see Table 4-2.

**Step 4** Configure IP group DDoS alert parameters.

a. After configuring IP group traffic alert parameters, click **Next** to open the **IP Group DDoS Attack Alert** page.

b. Configure parameters on this page.

- **IP Group DDoS Alert Period Configuration**: Configure **Alert Latency Period** and **Alert Holding Period**. For specific configuration, see Table 4-2.
- **IP Group DDoS Alert**: Respectively configure **Inbound Check Configuration** and **Outbound Check Configuration**.
  - **Inbound Check Configuration**: Configure **Fixed Threshold Configuration**, and **Constituent Proportion Configuration**, and **Connection Anomaly Detection Configuration**.

    For details about parameter description of the former, see Table 4-2.

    To configure a constituent proportion alert policy, enable the function in the **Status Control** area, and configure alert parameters. If the traffic exceeds both **Min Trigger Threshold** and **Proportion for Direct Alerts**, the system directly generates an alert. For the configurations of other parameters, see Table 4-2.

    For the configuration of an abnormal connection alert policy, see Table 4-3.
  - **Outbound Check Configuration**: Configure **Constituent Proportion Configuration** after enabling this function.

**Step 5** Configure the IP group traffic statistics function.

You can specify statistical items of traffic for the IP group and click **Save**. After that, click **Next** to configure IP group traffic diversion rules.

**Step 6** Configure IP group traffic diversion rules.

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

b. Configure parameters on this page.

Table 4-7 describes parameters for configuring traffic diversion rules for an IP group.

Table 4-7 Parameters for configuring diversion rules for an IP group

| Parameter | | Description |
|---|---|---|
| IP Group Diversion Policy | Number of Inbound Diversion IP in the IP Group | Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 300.<br>When **Diversion Policy for Abnormal Inbound IP Group Traffic** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses or all IP addresses (**Any**) in an IP group. |
| | Diversion Policy for Abnormal Inbound IP Group Traffic | Specifies the diversion policy for inbound traffic of top N IP addresses or all IP addresses (**Any**) in an IP group when the inbound traffic alert is triggered.<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. |

| Parameter | | Description |
|---|---|---|
| | | Note<br>The diversion policy for a region has a lower priority than that for an IP group.<br>• You can click **Add** to add new diversion policies. |
| | Number of Outbound Diversion IP in the IP Group | Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 100.<br>When **Diversion Policy for Abnormal Outbound IP Group Traffic** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses. |
| | Diversion Policy for Abnormal Outbound IP Group Traffic | Specifies the diversion policy for outbound traffic of top N IP addresses in an IP group when the outbound traffic alert is triggered.<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>• You can click **Add** to add new diversion policies. |
| IP Diversion Policy | | Specifies the diversion policy for IP addresses in an IP group when the DDoS alert is triggered.<br>• **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** to add new diversion policies. |

**Step 7** Configure IP group protection policies.

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

b. Configure parameters on this page.

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

**Step 8** Configure the IP group access policies.

After configuring the protection policies, click **Next** to open the **Access Policy** page and configure the access policies.

The configurations of access control rule, blocklist ("blacklist" on UI), NTI, and GeoIP rules are essentially same as those on ADS. For details, see the *NSFOCUS ADS User Guide*.

**Step 9** Configure a URL rule.

a. After configuring the access rule, click **Next** to open the **URL Rule Configuration** page.

b. Click **Add**.

c. In the **Add Rule** dialog box, configure URL rule parameters.
Table 4-8 describes parameters for adding a rule.

Table 4-8 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 as required. |
| Destination Port | Port of the server. |
| SYN Cookie URL | Controls whether to enable **SYN Cookie URL**. |
| Algorithm | Protection mode and policy adopted for packets matching URL protection rules. Protection modes include **Unified protection** and **Precision protection**. Nine algorithms are available for you to select. |

**Step 10** Click **Finish**.

In the **Region IP Group** list on the page shown in Figure 4-5, click an IP group ID to view the settings of this IP group.

| | |
|---|---|
| Note | An IP group that is included in a smart protection group cannot be viewed or modified. |

**----End**

## 4.1.7 Modifying an IP Group

An IP group can be modified by using either of the following methods:

Method 1: In the **Region IP Group** list on the page shown in Figure 4-5, click in the **Operation** column of an IP group to open the page for editing the IP group. Edit the settings of the IP group step by step.

Method 2: In the region list shown in Figure 4-1, click the name of an IP group to open the page for editing the IP group. Edit the settings of the IP group step by step.

| | |
|---|---|
| Note | • You can modify all parameters except **IP Group ID** and **IP Group Name**.<br>• An IP group that is included in a smart protection group cannot be modified. |

### 4.1.8 Deleting an IP Group

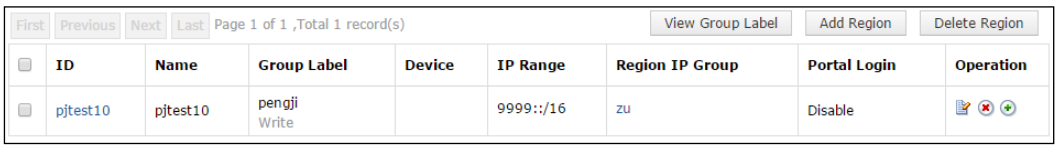
In the **Region IP Group** list on the page shown in Figure 4-5, click in the **Operation** column of an IP group to delete this group.

## 4.2 Management of a Region by a User Logging In with a Region ID

A user logging in to the Portal with a region ID can only edit basic information of the region and view settings of the region and settings of IP groups in this region.

On the page shown in Figure 3-3, click **Region**.

Figure 4-6 Region page

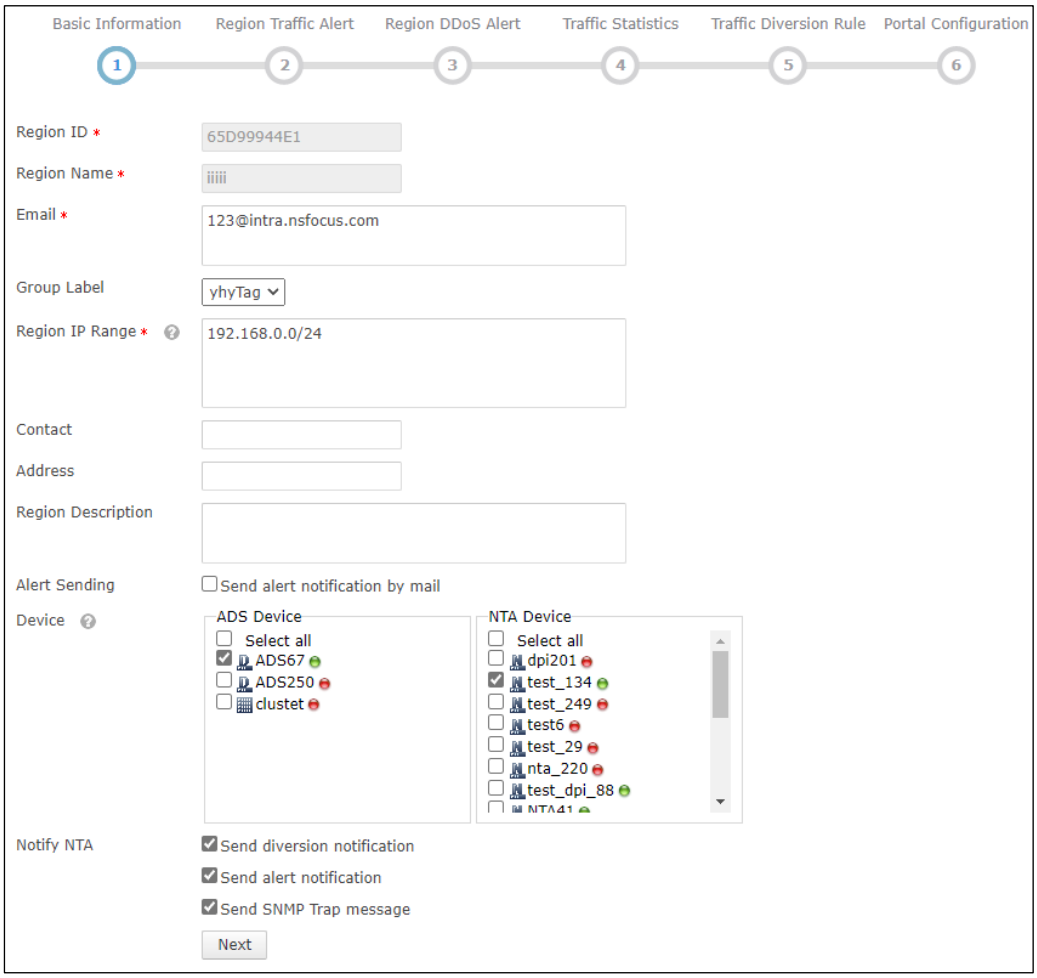



### 4.2.1 Editing Basic Information of a Region

On the page shown in Figure 4-6, click in the **Operation** column of a region.

A user logging in with a region ID can only modify the email address, contact person, contact address, region description, and alert and report sending method. After editing basic information, click **Save**.

Figure 4-7 Editing basic information of a region

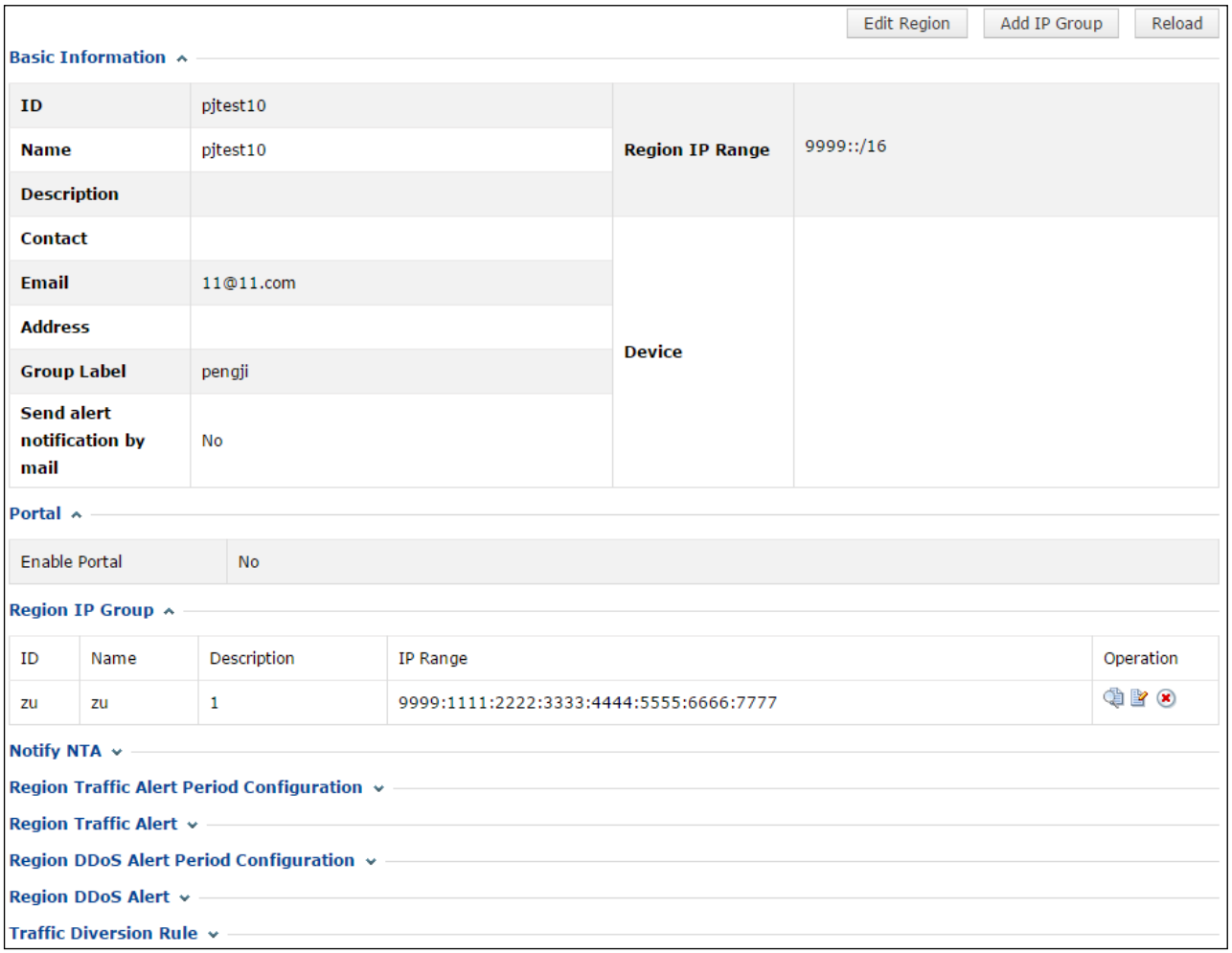



## 4.2.2 Viewing Region Settings

On the page shown in Figure 4-6, click the region ID to open the page for editing the region.

A user logging in with a region ID can only modify the email address, contact person, contact address, region description, and alert and report sending method. After editing basic information, click **Save**.

Figure 4-8 Viewing region settings

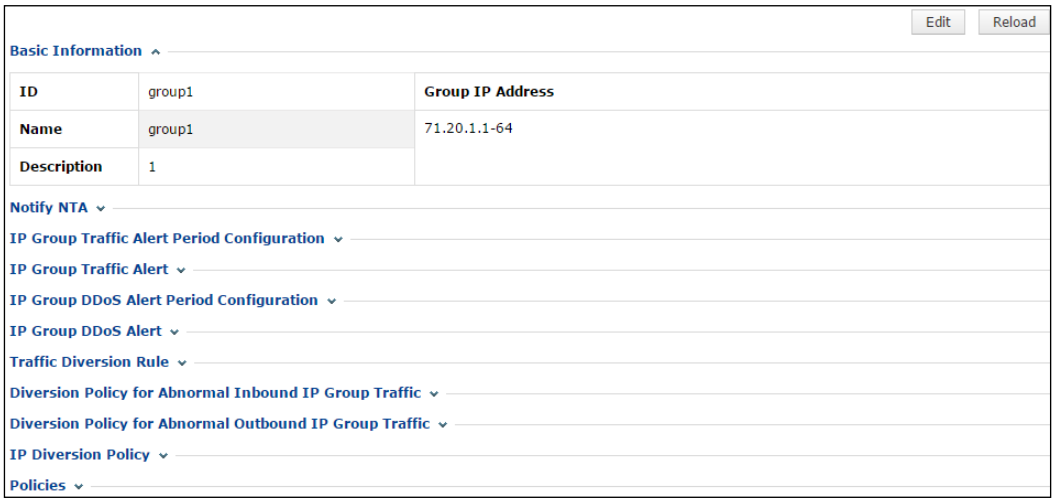



## 4.2.3 Viewing IP Group Settings

On the page shown in Figure 4-8, click in the **Operation** column of an IP group in the Region IP Group area to view its settings.

A user logging in with a region ID can only modify the email address, contact person, contact address, region description, and alert and report sending method. After editing basic information, click **Save**.

Figure 4-9 Viewing IP group settings



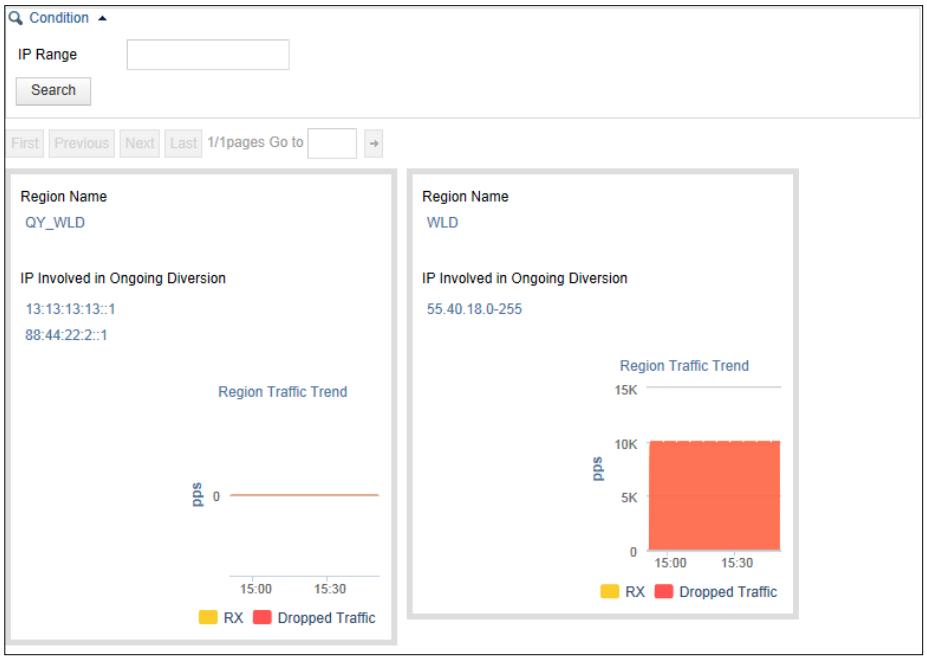
# 5 Region Traffic Diversion

You can log in to the web-based manager of ADS Portal as a region manager or with a region ID. As long as these accounts are granted appropriate permissions, you can perform operations regarding service traffic.

You can check the ongoing traffic diversion and IP addresses whose traffic can be diverted in manageable regions, and also manually divert traffic related to these IP addresses.

On the page shown in Figure 3-3, click **Traffic Diversion**. The page that appears displays IP addresses involved in traffic diversion and the traffic trend of the region to which these IP addresses belong, as shown in Figure 5-1. If no traffic diversion is happening currently, the system displays "No region is involved in traffic diversion."

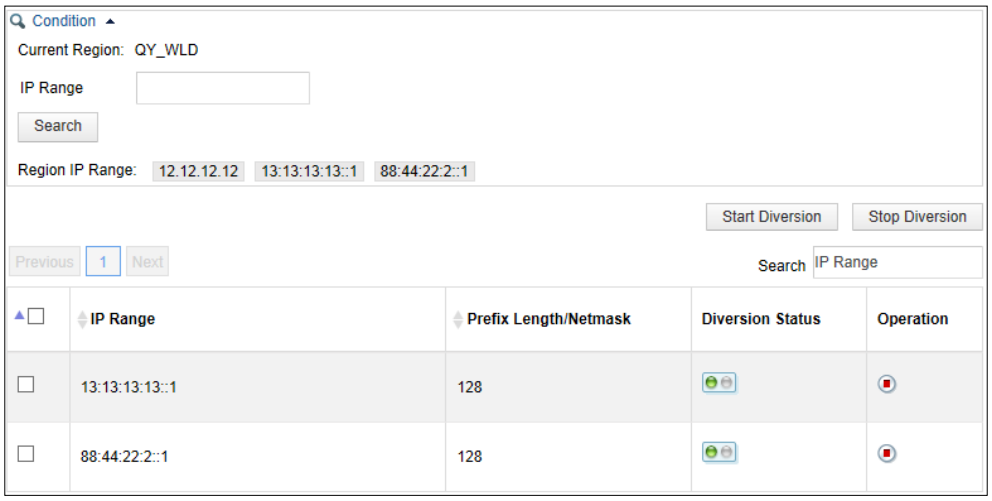
Figure 5-1 Traffic Diversion page




## 5.1 Viewing a Region Involved in Traffic Diversion

You can click the region name on the page shown in Figure 5-1 to view IP address ranges covered by this region and IP addresses involved in ongoing traffic diversion, as shown in Figure 5-2. Note that only the IP addresses covered by this region in question can be retrieved.

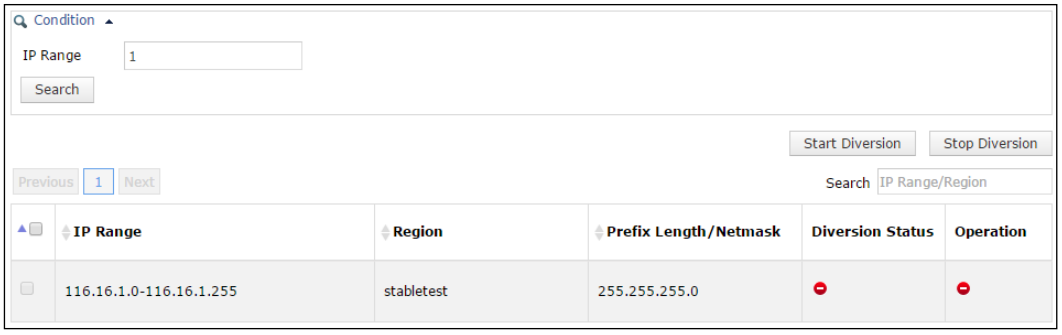
Figure 5-2 Viewing a region involved in traffic diversion




# 5.2 Configuring IP Addresses for Diversion

On the page shown in Figure 5-1, you can type an IP address range for query. Associated query is supported. For example, if you type **1**, all IP addresses starting with this digit will be displayed, as shown in Figure 5-3.

Figure 5-3 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. In this case, you can click in the **Operation** column to stop the diversion.
- : Traffic diversion is supported, but no traffic is being diverted. In this case, you can click in the **Operation** column to start 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 IP addresses on this page, make sure that the following items are properly configured for these IP addresses on ADS: routing daemon, IP route assignment, injection route, injection interface, and diversion filtering rules. |

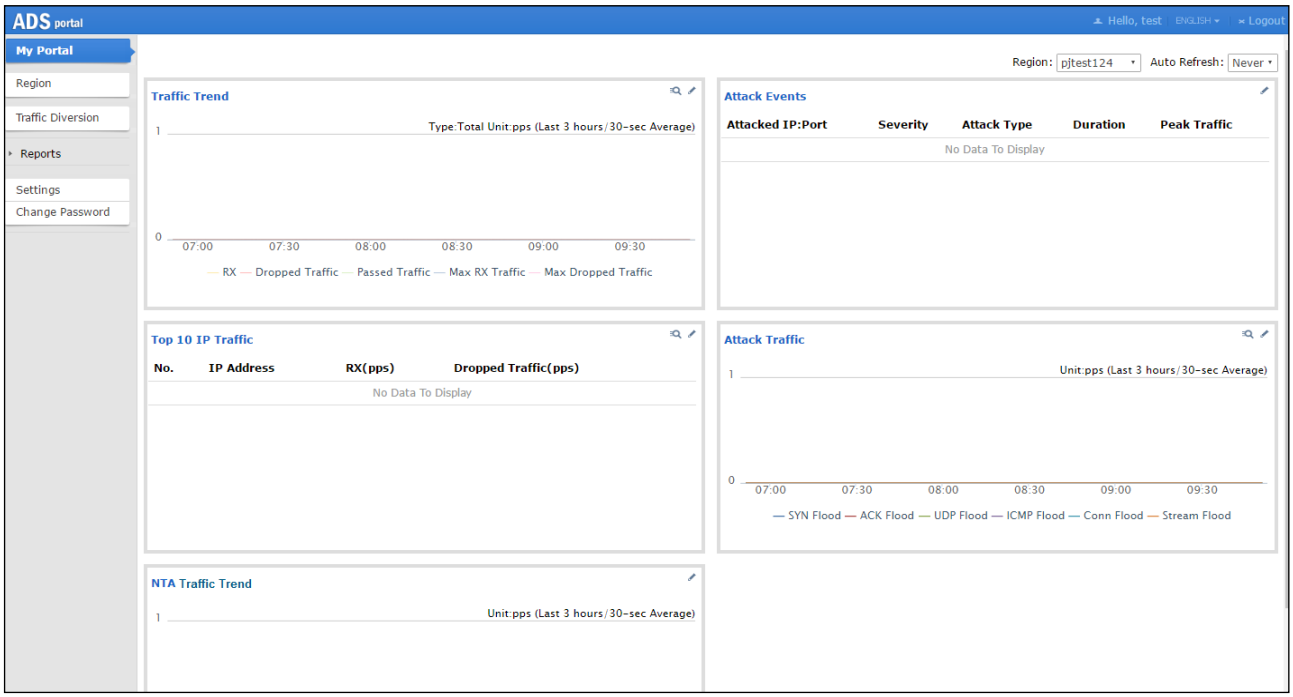
# 6 System Overview

After you log in to the web-based manager of ADS Portal successfully or click **My Portal**, the **System Overview** page appears by default. This page displays real-time information about traffic and attack events detected by ADS devices. On this page, you can view the traffic trend, current attack events, top 10 IP addresses with the heaviest traffic, and distribution of traffic by attack type detected by ADS devices.

If you log in to the Portal as a region manager, the **Region** drop-down list displays all regions created by the region manager. If you log in with a region ID, the **Region** drop-down list displays only the current region.

In the upper-right corner of this page, you can select **1 min**, **5 min**, or **Never** from the **Auto Refresh** drop-down list to make the system automatically refresh the monitoring page every 1 or 5 minutes, or to disable the auto refresh function.

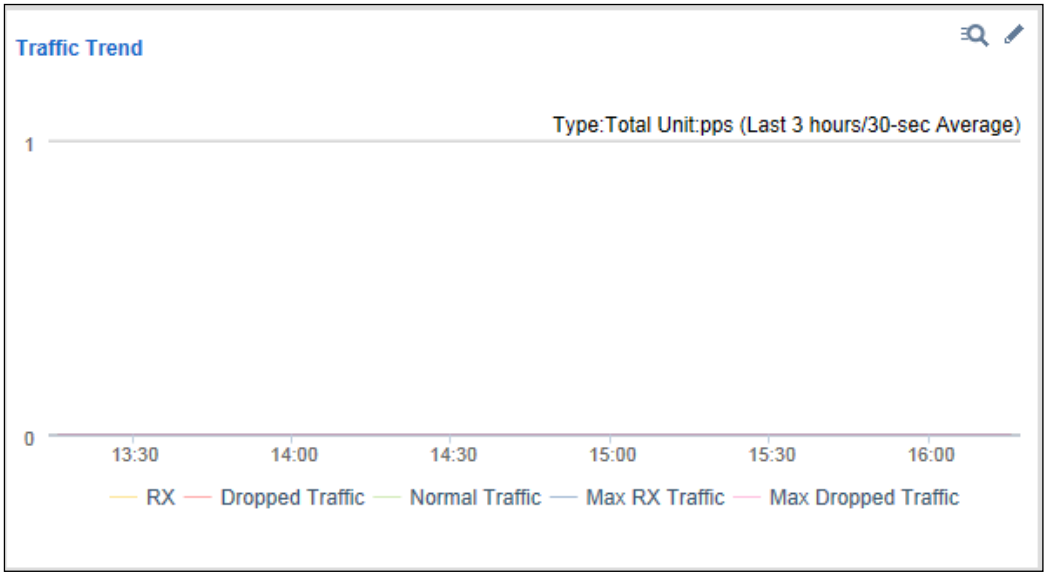
Figure 6-1 My Portal page




# 6.1 Viewing Traffic Trends

The Traffic Trend graph displays the trends of received traffic, dropped traffic, and normal traffic in the last 3 hours or 24 hours on ADS, as shown in Figure 6-2.

Figure 6-2 Traffic trends



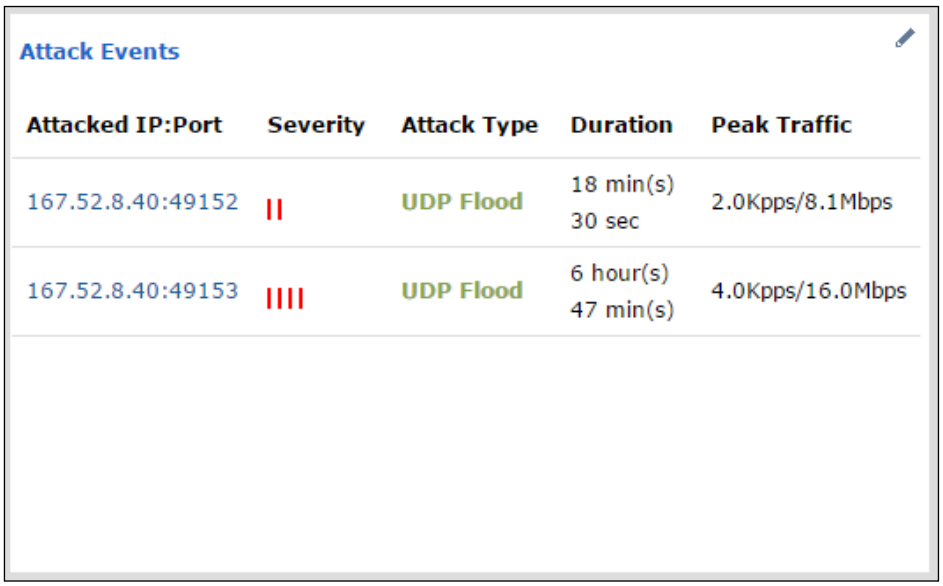

- Clicking in the upper-right corner of the graph opens the traffic trend report page.

- Clicking in the upper-right corner of the graph allows you to edit graph parameters in the dialog box that appears.
  - **Type**: specifies what type of traffic the traffic trend graph will display. Options include **TCP**, **UDP**, **ICMP**, and **Total**.
  - **Unit**: specifies whether the graph displays traffic in pps or bps.
  - **Time**: specifies whether the traffic trend graph displays traffic in the last 3 hours or 24 hours.
- Clicking **RX**, **Dropped Traffic**, **Normal Traffic**, **Max RX Traffic**, or **Max Dropped Traffic** below the graph hides the trend curve of such traffic.

## 6.2 Viewing Attack Events

The Attack Events list displays ongoing attack events or those in the last 24 hours, as shown in Figure 6-3. **Severity** is calculated based on the severity measurement threshold and the severity scale interval.

Figure 6-3 Attack events

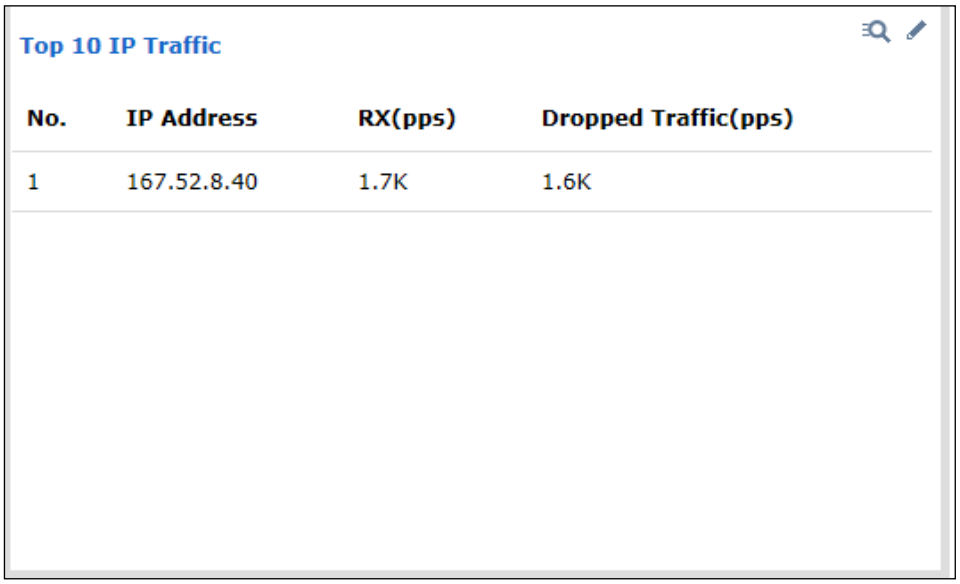



- Clicking an entry under **Attacked IP:Port** opens the attack event report of this IP address.
- Clicking in the upper-right corner of the list allows you to edit list parameters in the dialog box that appears.
  - **Time**: specifies whether the list displays ongoing attack events or those in the last 24 hours.
  - **Severity Measurement Threshold**: specifies the lower limit in pps for the system to measure the severity of an event. The severity is calculated only when the maximum traffic exceeds this threshold.
  - **Scale Interval for Severity Measurement**: specifies the scale interval against which the severity of an event is raised. Each interval corresponds to one level and the highest severity level is level 20.

# 6.3 Viewing Top 10 IP Addresses

As shown in Figure 6-4, the Top 10 IP Traffic graph lists top 10 IP addresses in a region protected by ADS with the heaviest average traffic in a specified period. From this list, you can find out which IP address receives the heaviest traffic or has been attacked most severely.

Figure 6-4 Top 10 IP addresses

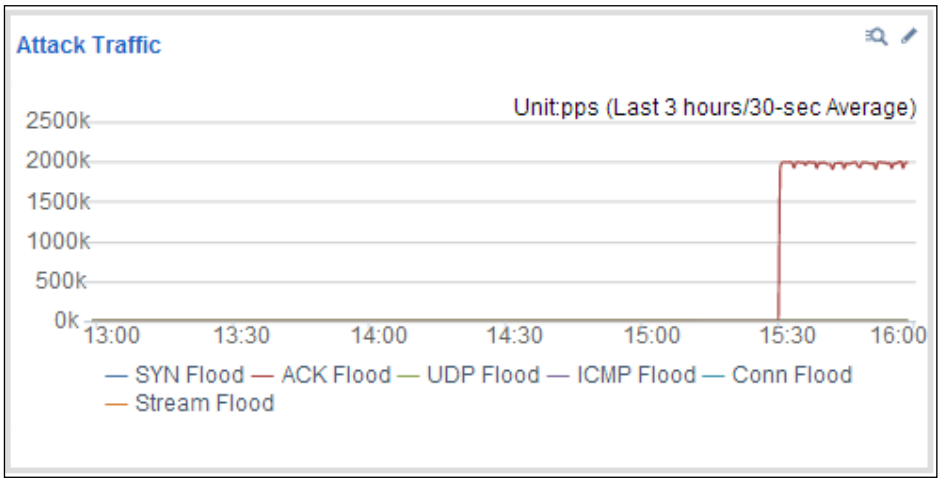



- Clicking in the upper-right corner of the list opens the top N IP address report page (the **TOP** value is **IP**).
- Clicking in the upper-right corner of the list allows you to edit list parameters in the dialog box that appears.
  - **Time**: specifies whether the list displays top 10 IP addresses with the heaviest traffic in the last 15 minutes or 1 hour.
  - **Type**: specifies whether to rank IP addresses by received traffic or dropped traffic.
  - **Unit**: specifies whether to display traffic in packets, bits, pps, or bps.

# 6.4 Viewing Attack Traffic of Different Types

The Attack Traffic graph displays attack traffic of different types in the last 3 hours or 24 hours, as shown in Figure 6-5.

Figure 6-5 Attack traffic of different types

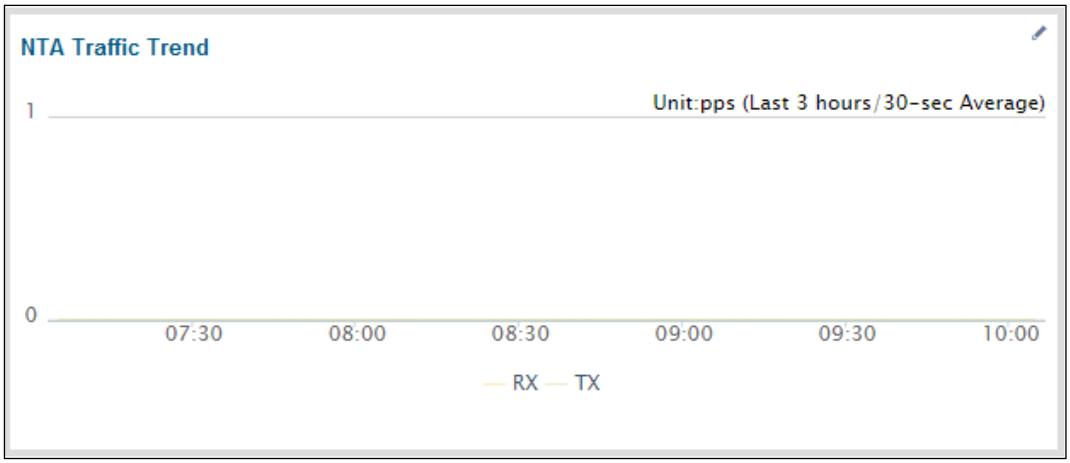



- Clicking in the upper-right corner of the graph opens the top N attack type report page (the **TOP** value is **Attack Type**).
- Clicking in the upper-right corner of the graph allows you to edit graph parameters in the dialog box that appears.
  - **Unit**: specifies whether the graph displays traffic in pps or bps.
  - **Time**: specifies whether the graph displays traffic in the last 3 hours or 24 hours.
- Clicking an attack type below the graph hides the traffic curve of this type in the graph.

# 6.5 Viewing the Trend of Traffic on NTA

The NTA Traffic Trend graph displays the trend of received traffic and dropped traffic in the last 3 hours or 24 hours on NTA, as shown in Figure 6-6.

Figure 6-6 Trend of traffic on NTA



- Clicking  in the upper-right corner of the graph allows you to edit graph parameters in the dialog box that appears.
  - **Unit**: specifies whether the graph displays traffic in pps or bps.
  - **Time**: specifies whether the traffic trend graph displays traffic in the last 3 hours or 24 hours.
- Clicking **RX** or **TX** below the graph hides the trend curve of such traffic.

# 7 Reports

Reports are a vital part of ADS M products. After login to ADS Portal using a Portal account, you can view historical traffic and attack data collected and delivered by ADS M on the web-based manager. Based on such data, you can further analyze network status.

If you log in as a region manager, you can query reports of the manageable regions under a group label only when this account is granted the permission for viewing data of this group label.

Reports include the attack event report, traffic trend report, top N traffic report, integrated report, and attack summary report.

## 7.1 Operations on Reports

After setting report query conditions, you can view reports online or export reports that have been generated.

- Querying a report

  Set query conditions (such as IP address, time, and attack type) and click **Search**. Then a report matching the conditions will be generated.

- Exporting a report

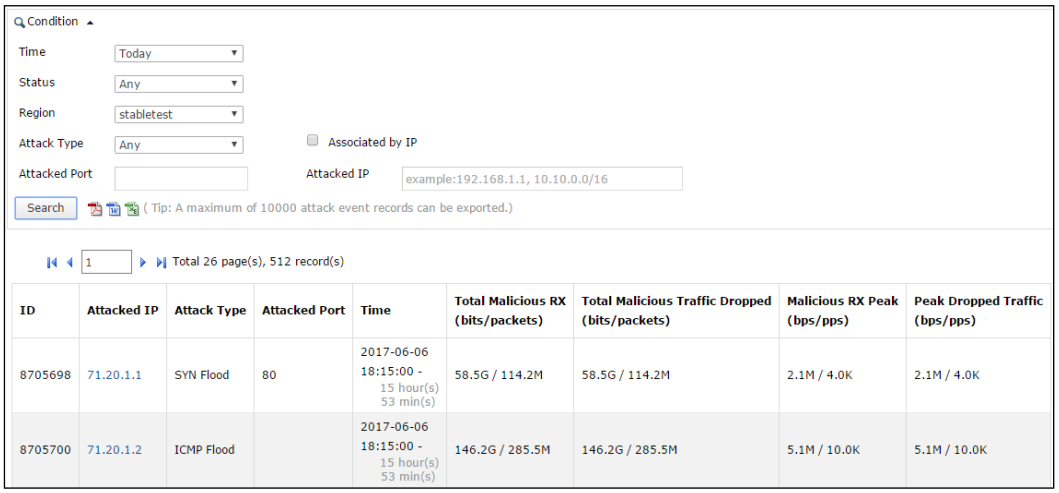
  After a report is generated, click  ,  , or  to save it as a PDF, Word, or HTML document to the local hard disk.

  You can export a maximum of 10,000 records to a report.

## 7.2 Attack Event Report

An attack event report collects data about attack events in a specified period. The statistics include the following information: attacked IP address, attacked port, attack type, attack time, total received traffic, total dropped traffic, peak received traffic, and peak dropped traffic, as shown in Figure 7-1.

Figure 7-1 Attack event report




| | |
|---|---|
| Note | Clicking an attacked IP address in the query result opens the attack summary report of this attacked IP address. For details, see section 7.6 Attack Summary Report. |

Table 7-1 describes parameters for querying an attack event report.

Table 7-1 Parameters for querying an attack event report

| Parameter | Description |
|---|---|
| Time | Specifies the time of attack events the report will cover. The default value is **Today**, indicating that the report will cover attack events occurring on the current day. Other options include **By Date**, **By Month**, and **Custom**. **Custom** indicates that you can specify a time frame by entering the start time and end time in the calendar text boxes. |
| Status | Status of attack events, which can be **Ended** or **Ongoing**. The option **Any** indicates that the report covers attack events of any status. |
| Region | Specifies the region in which attack events are detected. If you log in to the Portal as a region manager, the drop-down list displays all regions created by the region manager. If you log in with a region ID, the drop-down list displays only the current region. |
| Attack Type | Type of attack events such as **SYN Flood** or **ACK Flood**. |
| Associated by IP | Controls whether to combine all attack information of an IP address in an attack event for display.<br>If this option is selected, **Attack Type** and **Attacked Port** are unavailable. |
| Attacked Port | Port of the device under attack. |
| Attacked IP | IP address of the device under attack. |

| | |
|---|---|
| Tip | You can export a maximum of 10, 000 entries in a report. In case large amounts of data are involved, it is recommended that you export the data in different reports by specifying different periods of time. |

# 7.3 Traffic Trend Report

A traffic trend report collects statistics on the traffic (of one or more protocols) received and dropped by ADS devices in a specified period, and presents the traffic statistics in tables and graphs, in bps and pps respectively. Figure 7-2 shows a traffic trend report.

Figure 7-2 Traffic trend report

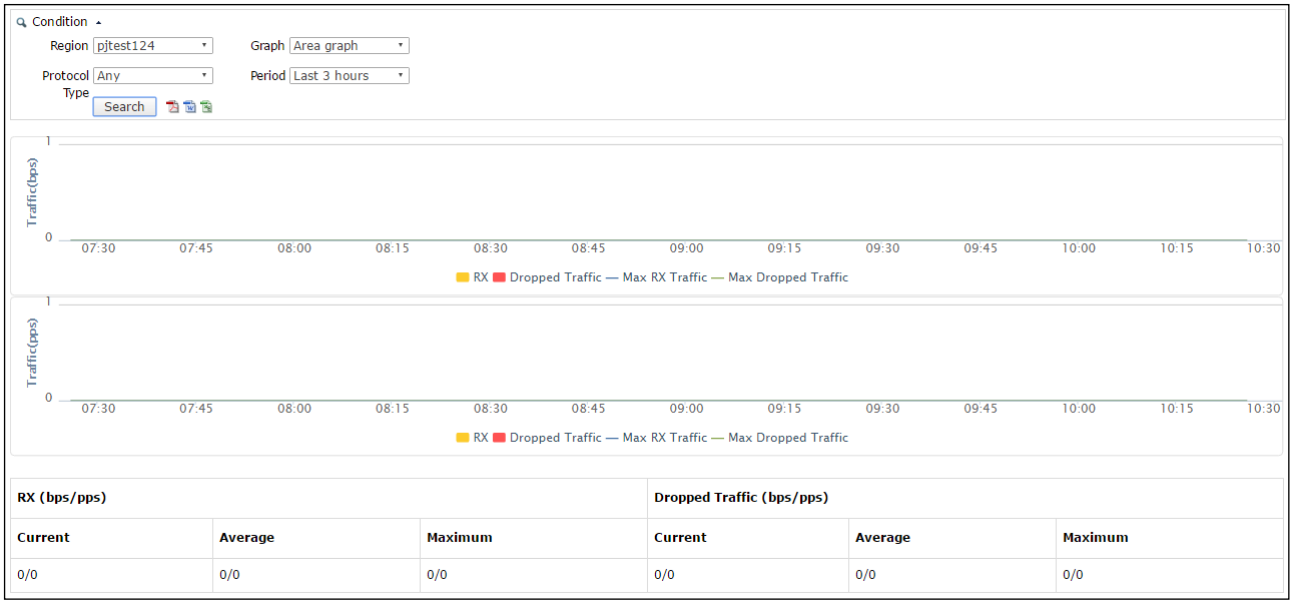



Table 7-2 describes parameters for querying a traffic trend report.

Table 7-2 Parameters for querying a traffic trend report

| Parameter | Description |
|---|---|
| Region | Specifies the region whose traffic statistics will be displayed. If you log in to the Portal as a region manager, the drop-down list displays all regions created by the region manager. If you log in with a region ID, the drop-down list displays only the current region. |
| Graph | Display type of the graph, which can be **Line graph** or **Area graph**. |
| Protocol Type | Specifies the protocol type of traffic covered by the report. Options include **TCP**, **UDP**, and **ICMP** and **Any**. **Any** indicates that traffic data of all protocol types will be collected. |
| Period | Specifies the generation time of traffic the report will cover. The default value is **Last 3 hours**, indicating that the system collects data in the last 3 hours. Values also include **Day**, **Week**, **Month**, and **Year**. |

| Parameter | Description |
| --- | --- |
| | • **Day**: indicates that traffic data of a specified date (0:00 to 24:00) will be collected.<br>• **Week**: indicates that traffic data of the week (starting from Monday) covering the specified date will be collected.<br>• **Month**: indicates that traffic data of a specified calendar month will be collected.<br>• **Year**: indicates that traffic data of a specified calendar year will be collected. |

# 7.4 Top N Traffic Report

A top N traffic report collects one of the following types of data in a specified period: top 10 addresses, top 10 protocols in terms of received and dropped traffic, and top 10 attack types. The report presents traffic statistics in graphs and tables in bps and pps respectively, as shown in Figure 7-3.

Figure 7-3 Top 10 IP address report

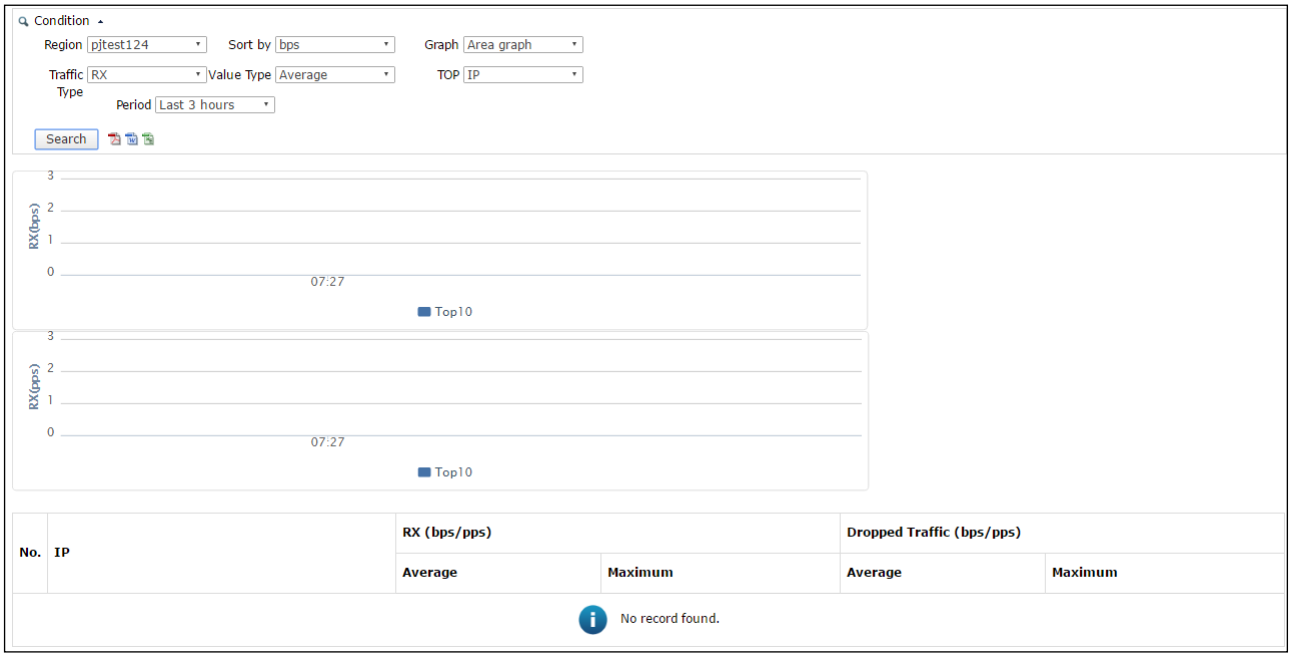



Table 7-3 describes parameters for querying a top N traffic report.

Table 7-3 Parameters for querying a top N traffic report

| Parameter | Description |
| --- | --- |
| Region | Specifies the region whose traffic ranking statistics will be displayed. If you log in to the Portal as a region manager, the drop-down list displays all regions created by the region manager. If you log in with a region ID, the drop-down list displays only the current region. |

| Parameter | Description |
|---|---|
| Sort by | Specifies the unit to measure the top 10 traffic. The options include **bps** and **pps**. |
| Graph | Specifies the statistical graph types:<br>• **Area graph**: available only when **Value Type** is set to **Average**.<br>• **Line graph**: always available. |
| Traffic Type | Specifies the traffic type.<br>• **RX**: indicates that only data of received traffic will be collected.<br>• **Dropped Traffic**: indicates that data of traffic dropped after attacks are detected will be collected. |
| Value Type | Type of traffic data to be displayed, which can be **Average** or **Maximum**. |
| TOP | Specifies the basis for ranking traffic. Here, traffic can be ranked by IP address, protocol, attack type, or source country/region. |
| Period | Specifies the generation time of traffic the report will cover. The default value is **Last 3 hours**, indicating that the system collects data in the last 3 hours. Values also include **Day**, **Week**, **Month**, **Year**, and **Custom**.<br>• **Day**: indicates that traffic data of a specified date (0:00 to 24:00) will be collected.<br>• **Week**: indicates that traffic data of the week (starting from Monday) covering the specified date will be collected.<br>• **Month**: indicates that traffic data of a specified calendar month will be collected.<br>• **Year**: indicates that traffic data of a specified calendar year will be collected.<br>• **Custom**: indicates that the traffic data of a specified period will be collected. |

## 7.5 Integrated Report

An integrated report collects overall traffic data in the region of the current user in a specified period. It contains traffic overview, traffic statistics, attack statistics, and protocol statistics, presented with graphs and tables, as shown in Figure 7-4.

Figure 7-4 Integrated report

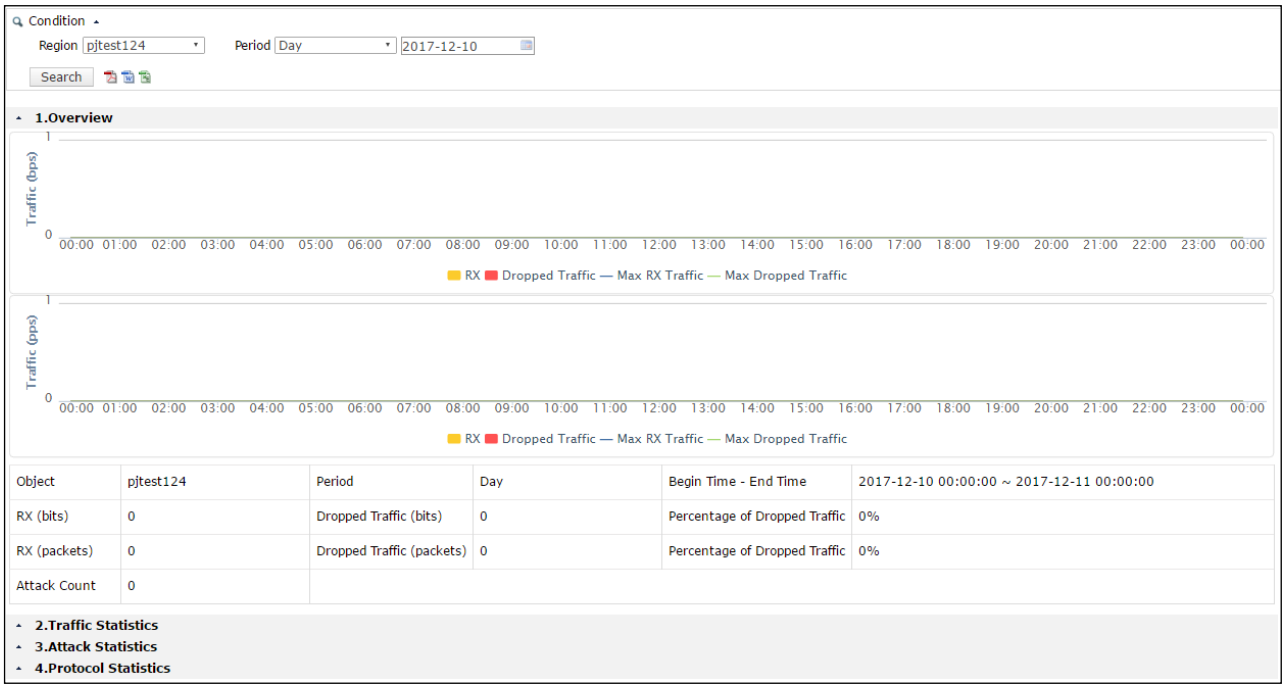



Table 7-4 describes parameters for querying an integrated report.

Table 7-4 Parameters for querying an integrated report

| Parameter | Description |
|---|---|
| Region | Specifies the region whose integrated statistics will be displayed. If you log in to the Portal as a region manager, the drop-down list displays all regions created by the region manager. If you log in with a region ID, the drop-down list displays only the current region. |
| Period | Specifies the generation time of traffic the report will cover. Options include **Day**, **Week**, **Month**, and **Year**.<br>• **Day**: indicates that traffic data of a specified date (0:00 to 24:00) will be collected.<br>• **Week**: indicates that traffic data of the week (starting from Monday) covering the specified date will be collected.<br>• **Month**: indicates that traffic data of a specified calendar month will be collected.<br>• **Year**: indicates that traffic data of a specified calendar year will be collected. |

# 7.6 Attack Summary Report

An attack summary report collects data about various attack events in a specified period, targeting a specified IP address under monitoring, as shown in Figure 7-5.

Figure 7-5 Attack summary report

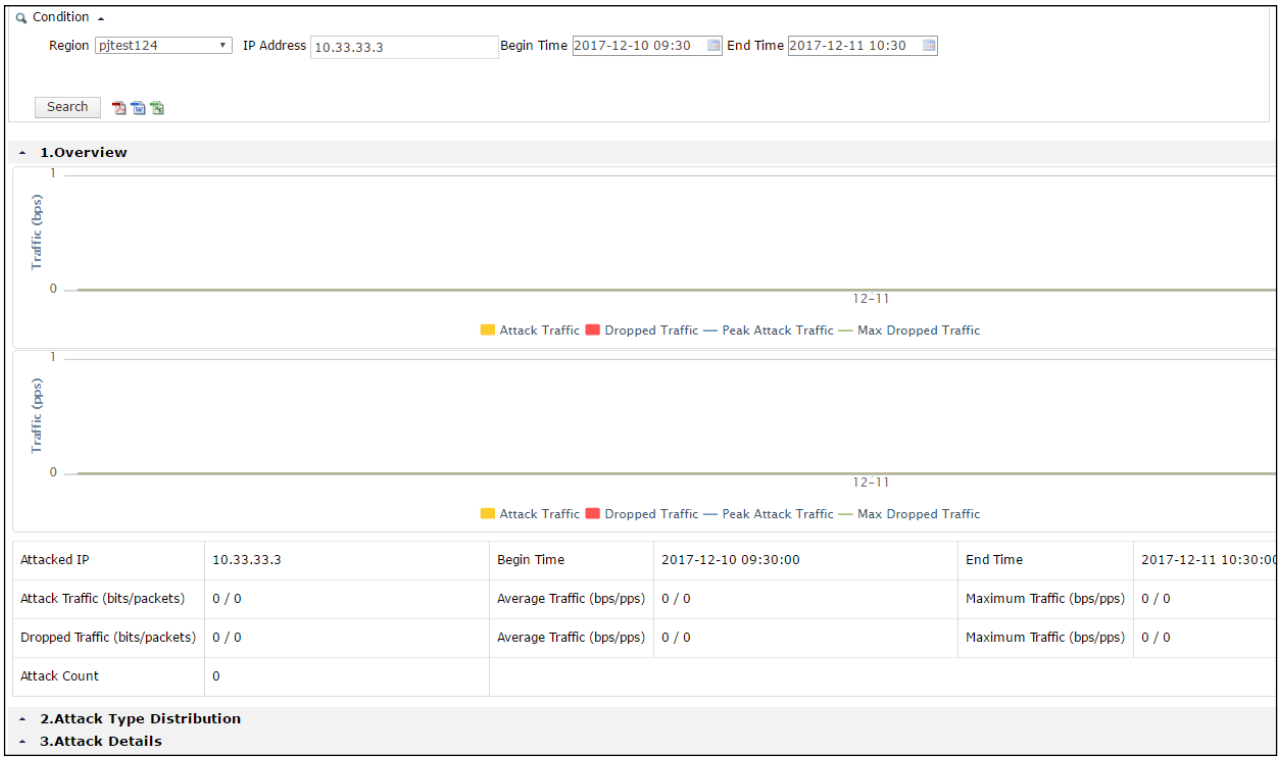



Table 7-5 describes parameters for querying an attack summary report.

Table 7-5 Parameters for querying an attack event report

| Parameter | Description |
|---|---|
| Region | Specifies the region whose attack summary statistics will be displayed. If you log in to the Portal as a region manager, the drop-down list displays all regions created by the region manager. If you log in with a region ID, the drop-down list displays only the current region. |
| IP Address | Specifies an IP address for you to learn how much it is attacked. |
| Start Time | Specifies the start time of attacks targeting the specified IP address. |
| End Time | Specifies the end time of attacks targeting the specified IP address. |

# A Default Parameters

The default network settings of the virtual machine are as follows:

| | |
|---|---|
| **IP Address** | 192.168.1.100 |
| **Subnet Mask** | 255.255.255.0 |
| **Default Gateway** | 192.168.1.1 |
| **DNS Server** | 192.168.1.1 |
| **NTP Server** | 192.168.1.1 |