NSFOCUS ADS Portal

User Guide

Version: V4.5R90F06 (2024-12-31)

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

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
V4.5R90F06	• Added functions: DNS subdomain allowlist auto-learning and carpet bombing protection. • Optimized functions: region DDoS alerts
V4.5R90F05SP03	Optimized functions: protection policies and access policies of IP groups, traffic diversion, and importing portal to the virtual platform.
V4.5R90F05	• Added functions: connection anomaly detection configuration and exception IP address of IP groups. • Optimized functions: login security settings and DDoS alert rules.
V4.5R90F04	• Updated the structure based on the new template. • 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:

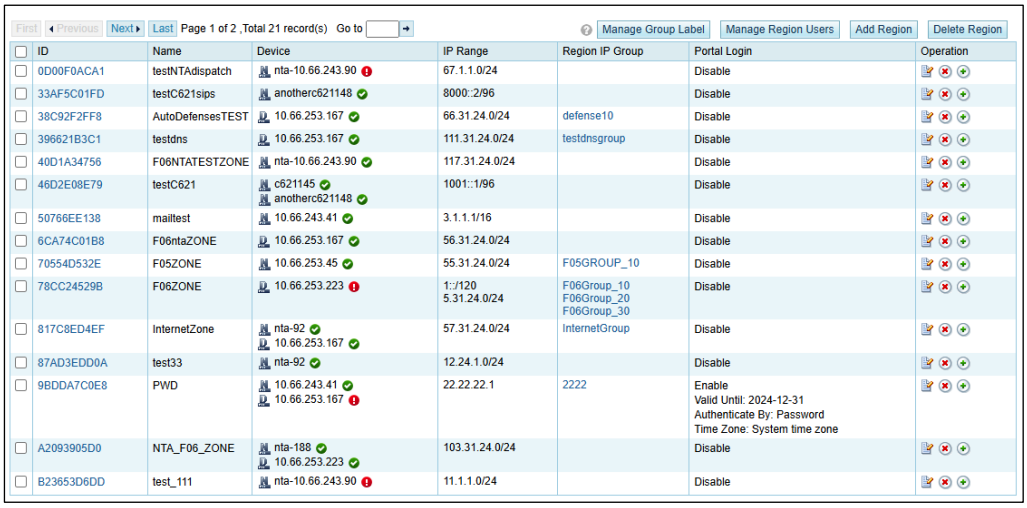
Step 1 Log in to the web-based manager of ADS M.

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, traffic diversion rules, and carpet bombing protection 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** page appears, as shown in Figure 2-2.

Figure 2-2 Portal configuration page

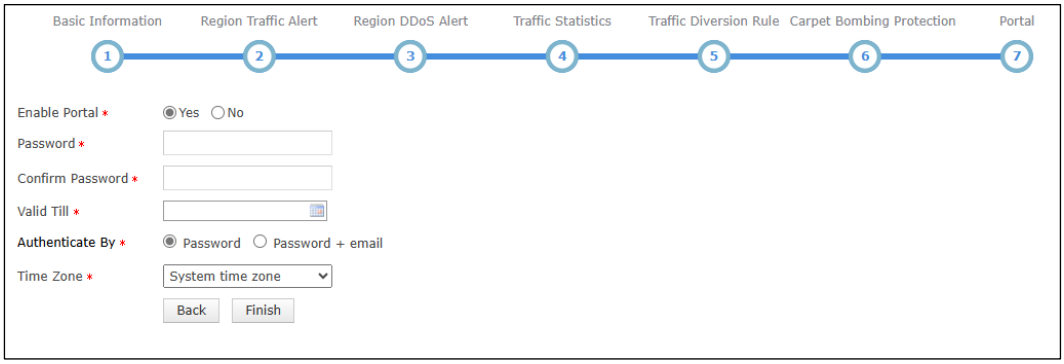


Table 2-1 describes Portal configuration parameters.

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. Note • The password strength must be consistent with that specified in ADS M, which can be viewed under **System > 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**.
Valid Till	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**. • **Password**: The account can log in to the Portal after typing the correct user name and password. • **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. Note

Parameter	Description
	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 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**.

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*.

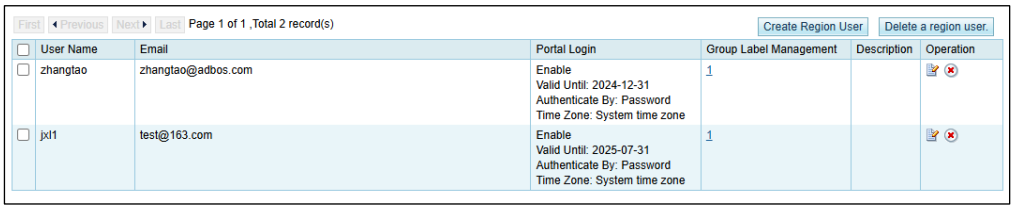
Step 2 Choose **Region** > **Region Management.**

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.

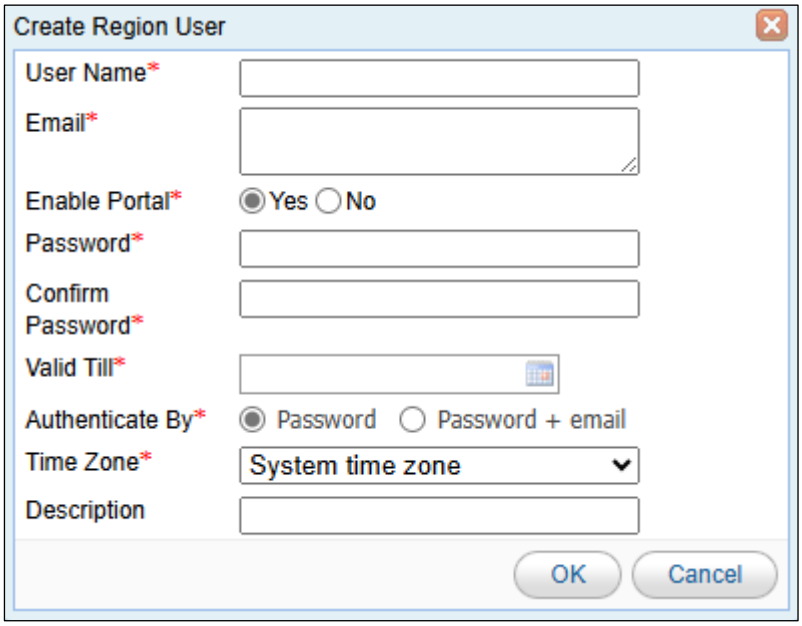
Figure 2-3 Manage Region Users page



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.

User Name 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 number 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.

User Name 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*.

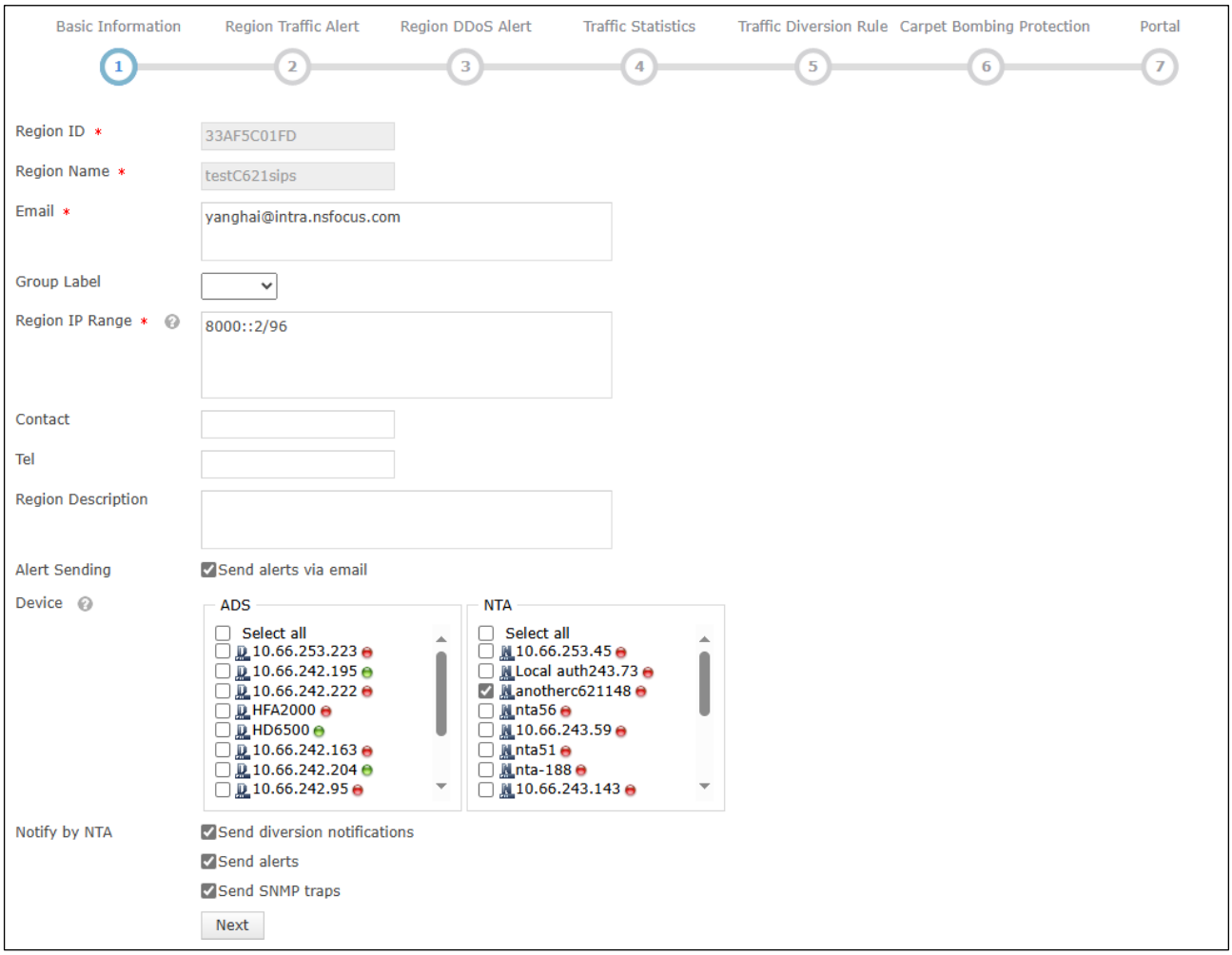
Step 2 Enable the function of sending email alerts.

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 alerts via email**, select NTA devices, and configure **Notify by NTA**, as shown in Figure 2-5.

Figure 2-5 Enabling the function of sending email alerts

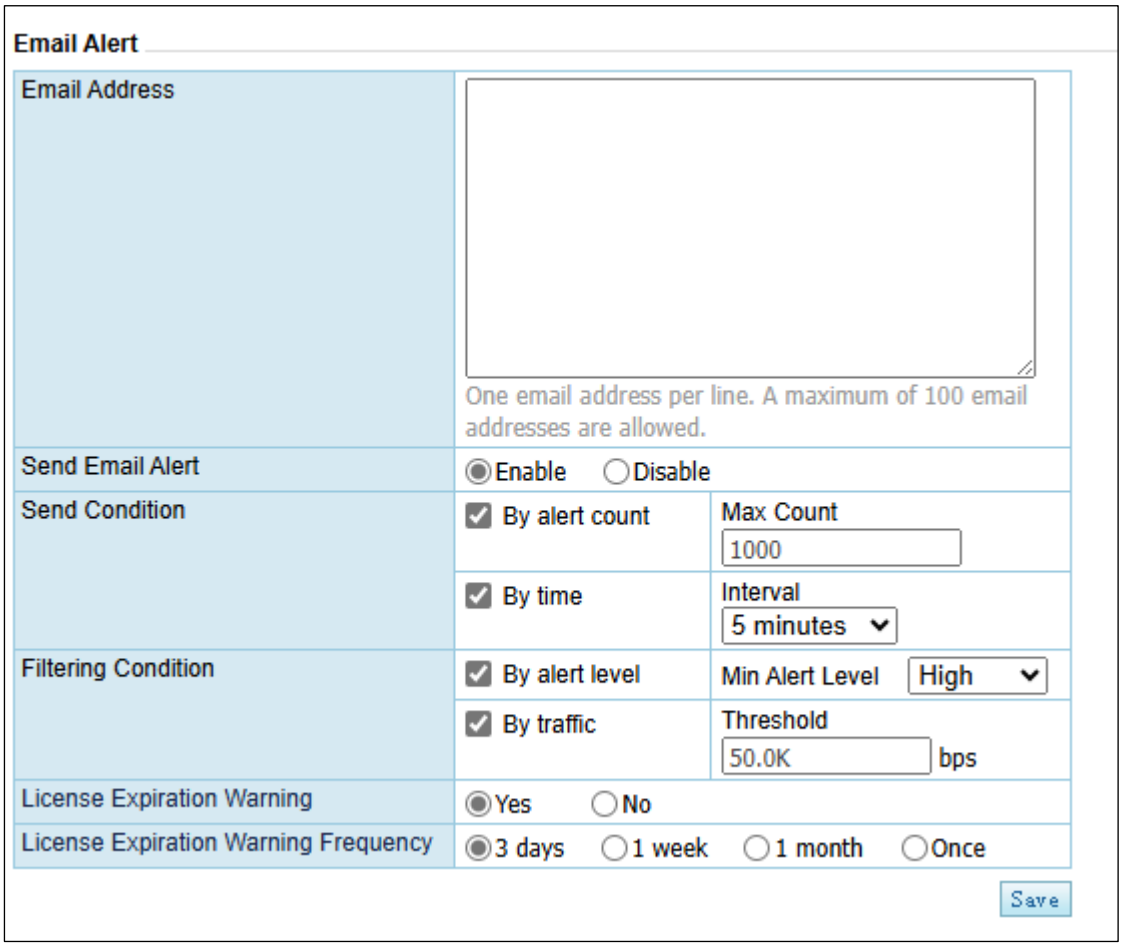


Step 3 Configure email alert sending parameters.

a. Choose **System > Third-Party Interface > Email Alert**.

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

Figure 2-6 Configuring email 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 to the Virtual Machine

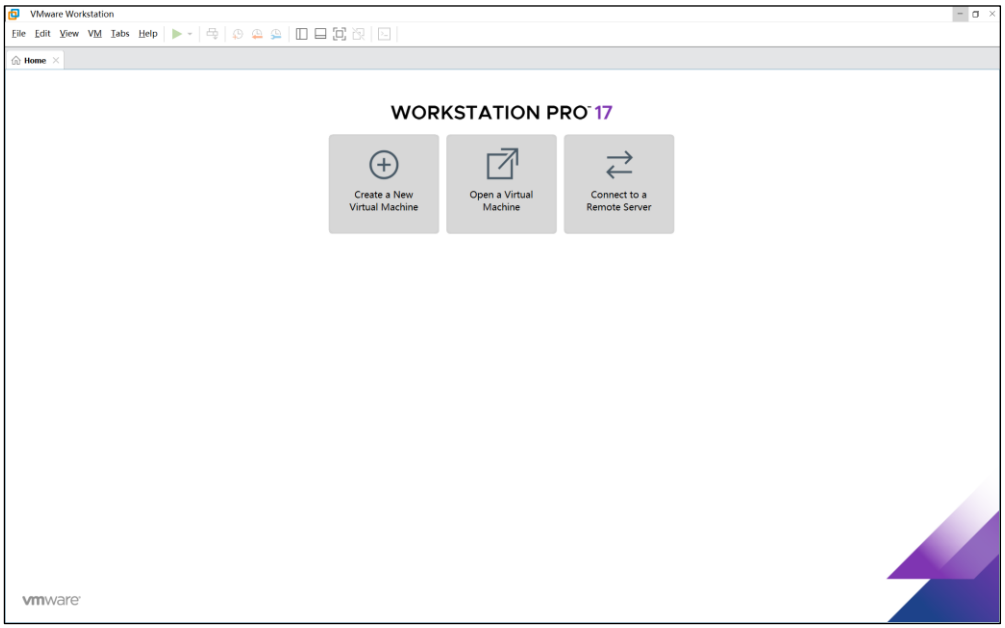
For the initial Portal deployment, you need to import the Portal image file (Portal.ova) to a virtual machine.

Note	• Before importing the image file, you need to install the virtual machine environment. Workstation Pro 17.0 or later, and VMware EXSi 6.7 or later is recommended. This section describles how to import the Portal image file to Workstation Pro 17.5.2. • The V4.5R90F05SP03 Portal image file only adapts to ADS M V4.5R90F05SP03 or later versions.

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

Step 1 Open VMware Workstation Pro 17.5.2.

Figure 2-7 Home page of VMware Player



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

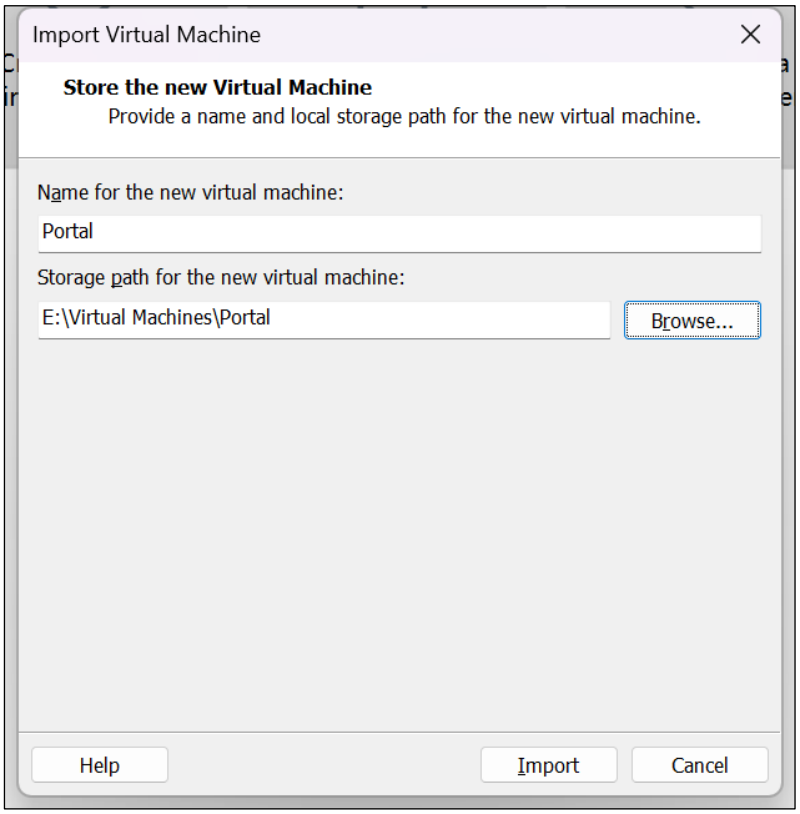
In the dialog box that appears, locate the image file, **Portal.ova.**

Figure 2-8 Selecting a virtual machine image file

Step 3 Click **Open**.

Step 4 Set a name and storage for the new virtual machine.

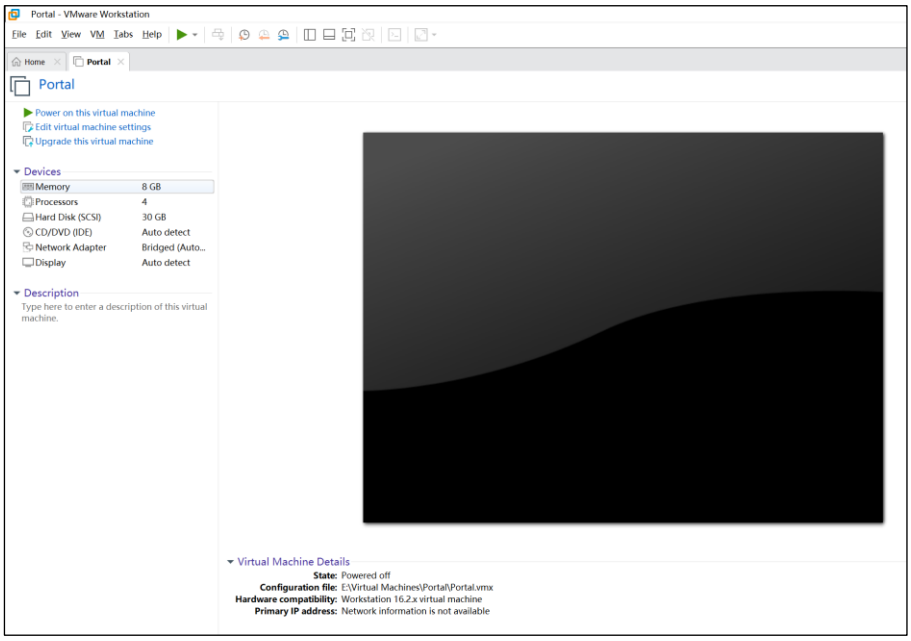
Figure 2-9 Setting a name and storage



Step 5 Click **Import**

After the image file is successfully imported, a page appears, as shown in Figure 2-10.

Figure 2-10 Image file imported successfully



At this time, the virtual machine is shut down.

Step 6 Click **Power on this virtual machine** to start the virtual machine.

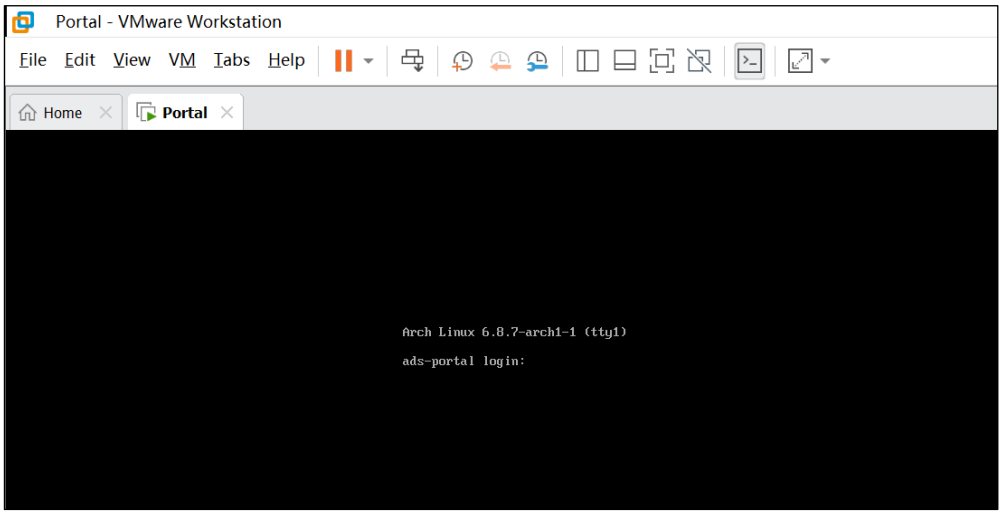
After the virtual machine is started, a window appears, as shown in Figure 2-11, requiring you to log in.

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. • For the default network settings of the virtual machine, see appendix *A* Default Parameters. You can modify the settings as required.

Figure 2-11 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:

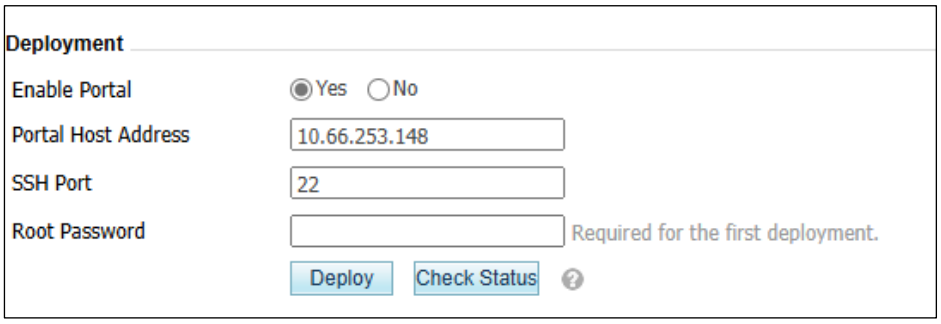
- Deploying the Portal
- Configuring Portal Authentication Parameters
- Replacing the Logo
- Replacing the SSL Certificate
- Configuring Login Security Parameters

2.4.1 Deploying the Portal

To deploy the Portal, follow these steps:

Step 1 Choose **System** > **Third-Party Interface** > **Portal**.

Figure 2-12 Deployment area on the Portal Configuration page



Step 2 Enable Portal configuration.

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

Step 3 Configure Portal parameters.

Table 2-2 describes Portal parameters.

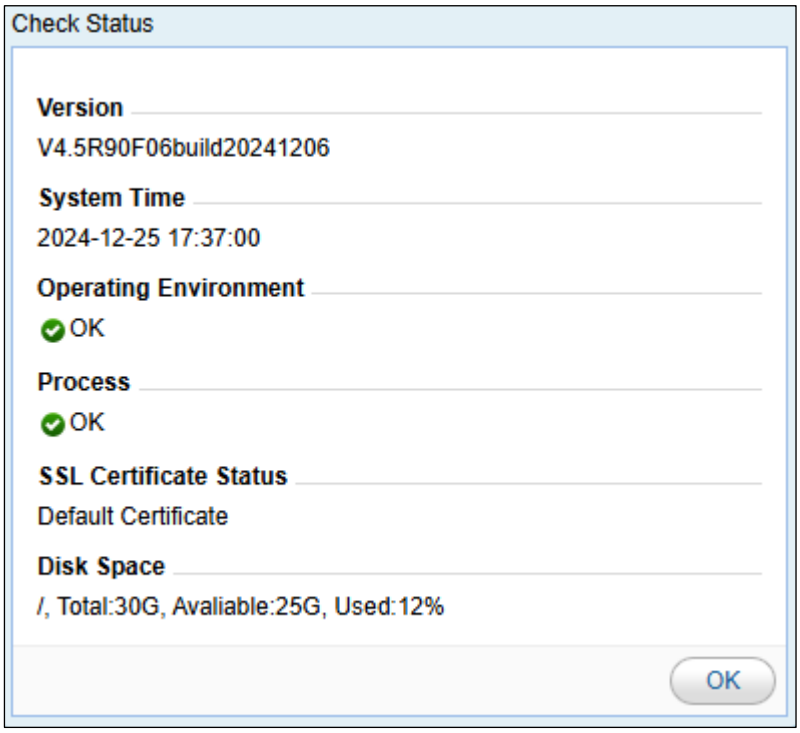
Table 2-2 Portal parameters

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. 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 to the Virtual Machine. The **root** password is required only for the first Portal deployment and can 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 2-13 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

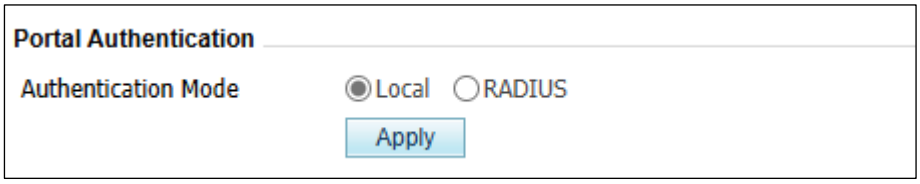
Portal users can be authenticated locally or by a third-party RADIUS server.

To configure Portal authentication parameters, follow these steps:

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

Figure 2-14 shows the Portal Authentication Configuration area.

Figure 2-14 Portal deployed



Step 2 Select a Portal authentication method.

Options include **Local** and **RADIUS**.

Step 3 (Optional) When **Authentication Method** is set to **RADIUS**, set RADIUS server parameters, as shown in Figure 2-15.

Figure 2-15 RADIUS server configuration

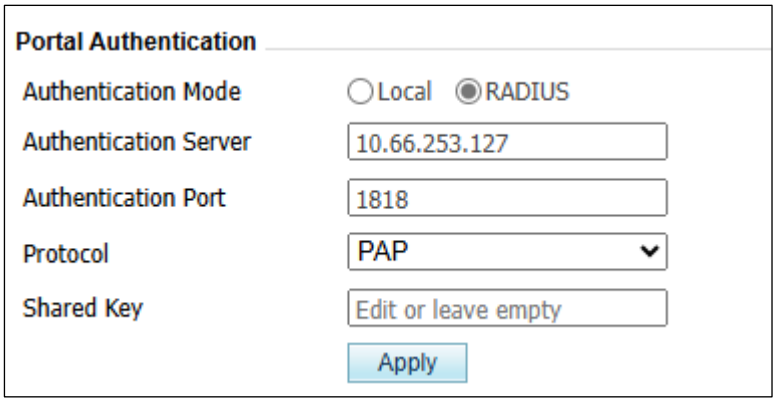


Table 2-3 describes parameters for configuring the RADIUS server.

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 authentication protocol used to secure a connection to the RADIUS server, which can be **PAP**, **CHAP**, **SPAP**, **MSCHAPv1**, or **MSCHAPv1**.
Shared Key	Specifies a text string used to encrypt the connection to the third-party RADIUS server. At most 64 characters can be specified.

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

----End

2.4.3 Replacing the Logo

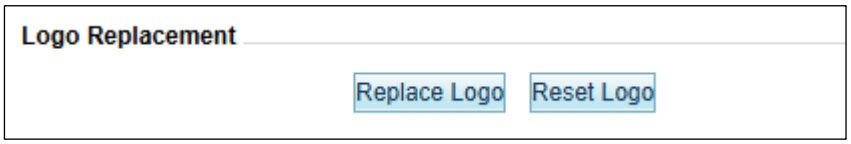
The logo on the login page, home page, **Reset Password** page, and report page can be customized.

To replace the logo, follow these steps:

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

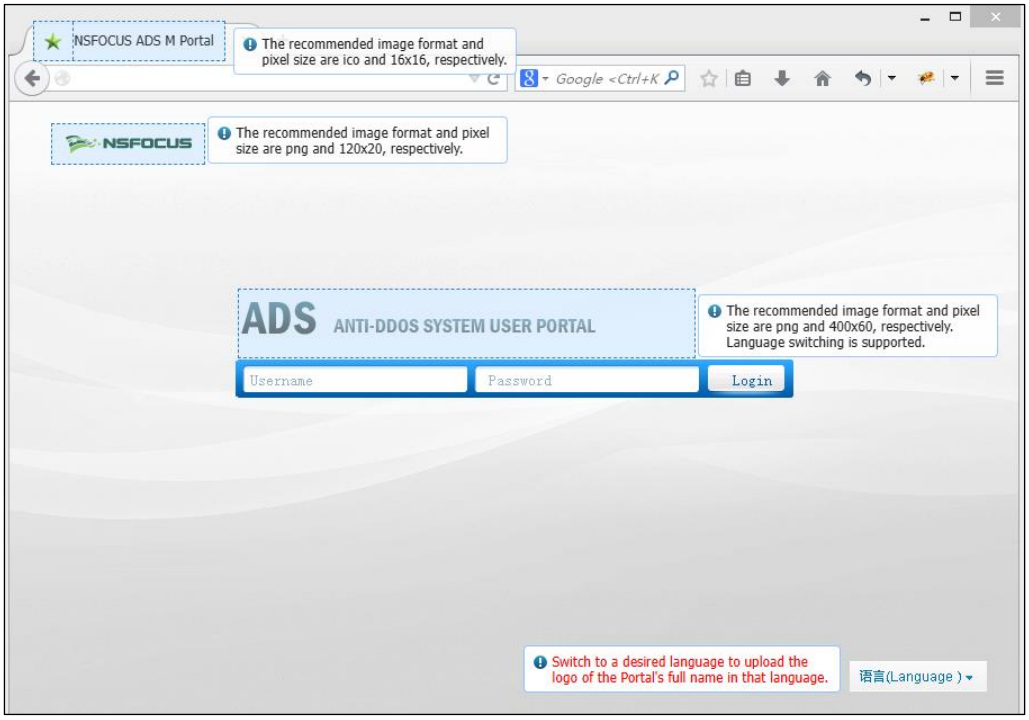
Figure 2-16 shows the **Logo Replacement** area.

Figure 2-16 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.

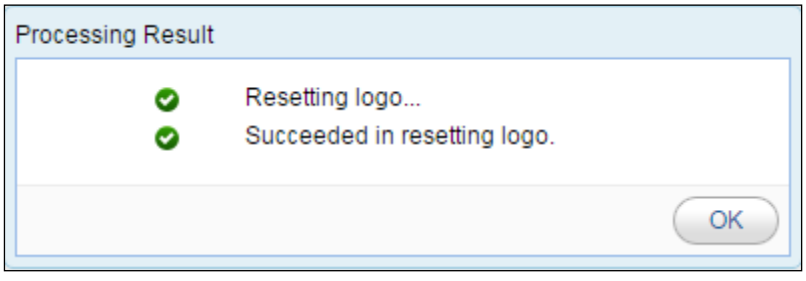
Figure 2-17 Replacing the login page logo



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 2-18 Resetting the logo and title



----End

2.4.4 Replacing the SSL Certificate

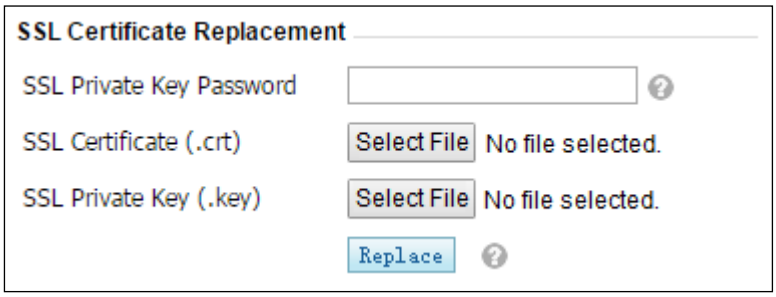
The system has a built-in SSL certificate, which can be replaced.

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

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

Figure 2-19 shows the **SSL Certificate Replacement** area.

Figure 2-19 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

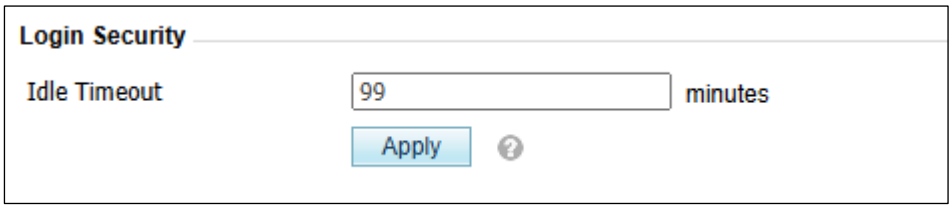
2.4.5 Configuring Login Security Parameters

To configure login security parameters, follow these steps:

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

Figure 2-20 shows the **Login Security** area.

Figure 2-20 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.

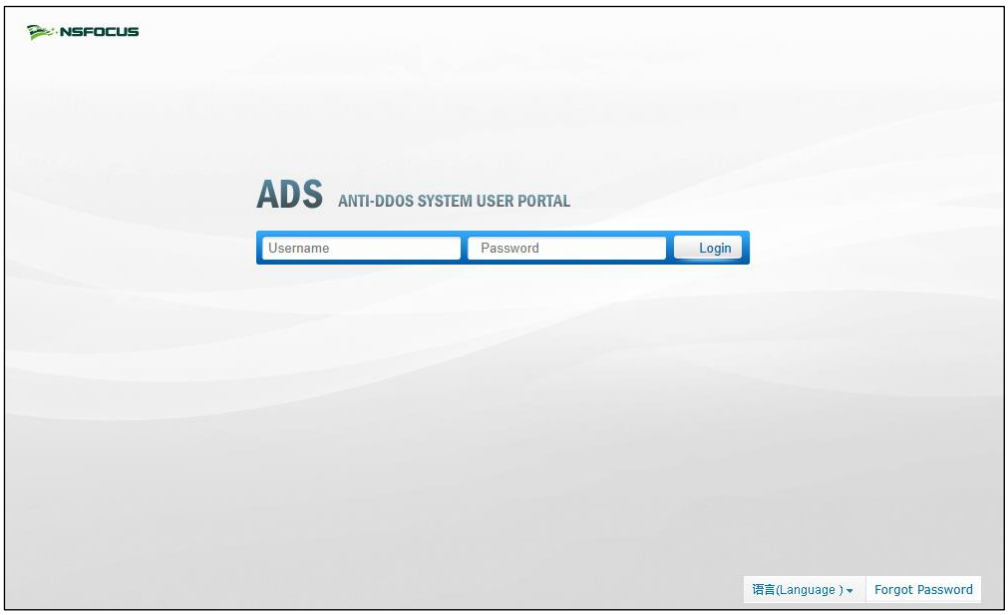
Step 2 Open the browser (Chrome is used here) and access ADS Portal in HTTPS mode by typing the server IP address, such as https://192.168.1.100, and pressing **Enter**.

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

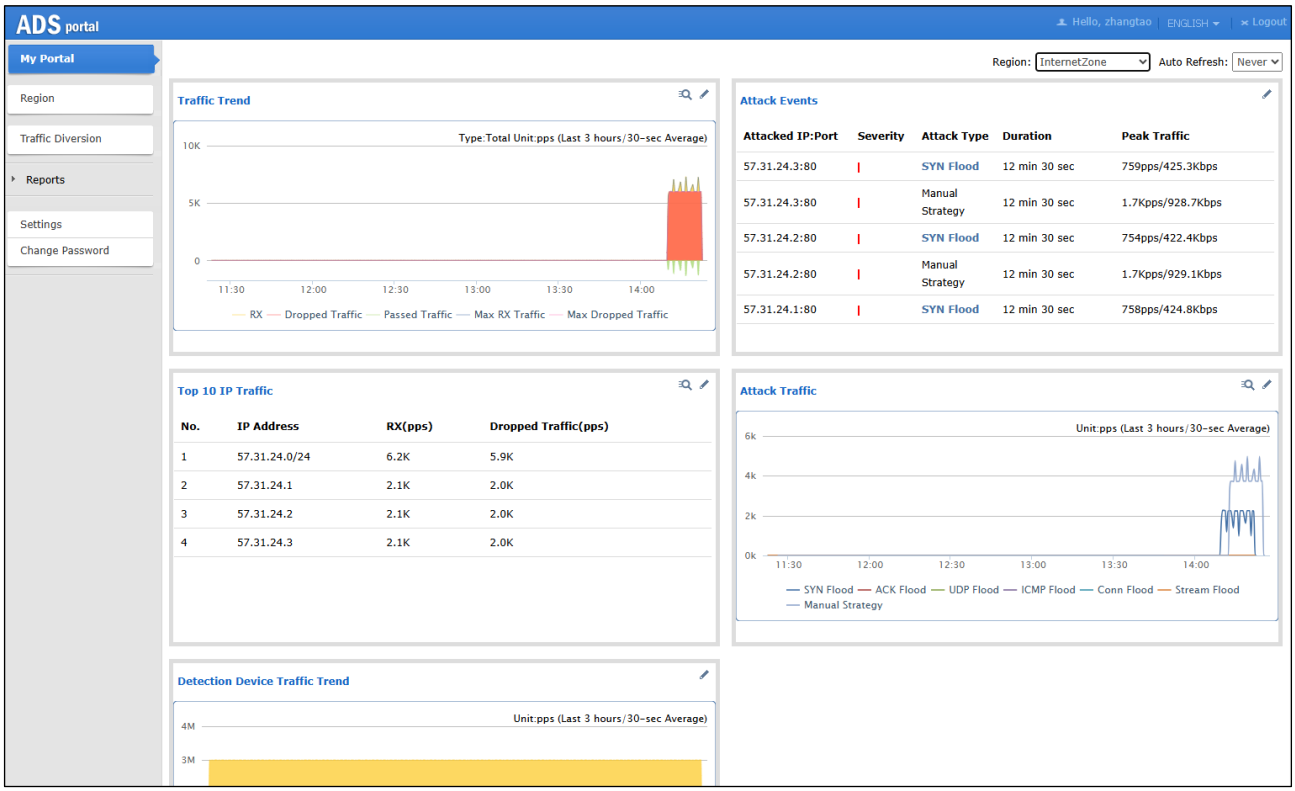


Step 4 Type the user name and password and then click **Login** or press **Enter**.

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. • You are advised to use the latest version of Chrome, Firefox, or Edge and set the display resolution to 1280 x 700 or higher. • You must change the initial password immediately after the first login. • 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. • The system will return to the login page if you remain inactive for a period specified by **Idle Timeout**. In this case, you need to log in again to continue using the system. For details, see section 2.4.5 Configuring Login Security Parameters.

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

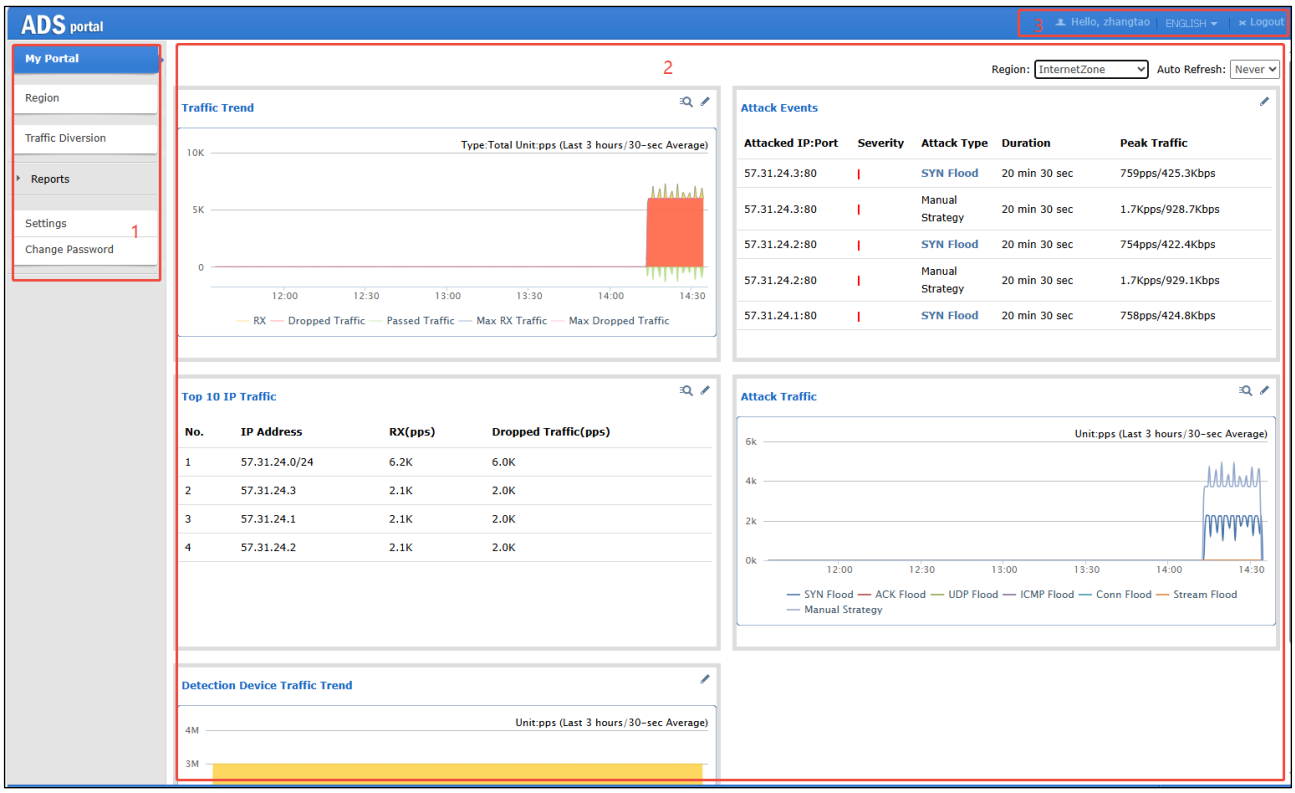


Table 3-1 describes the layout of the web-based manager.

Table 3-1 Webpage layout

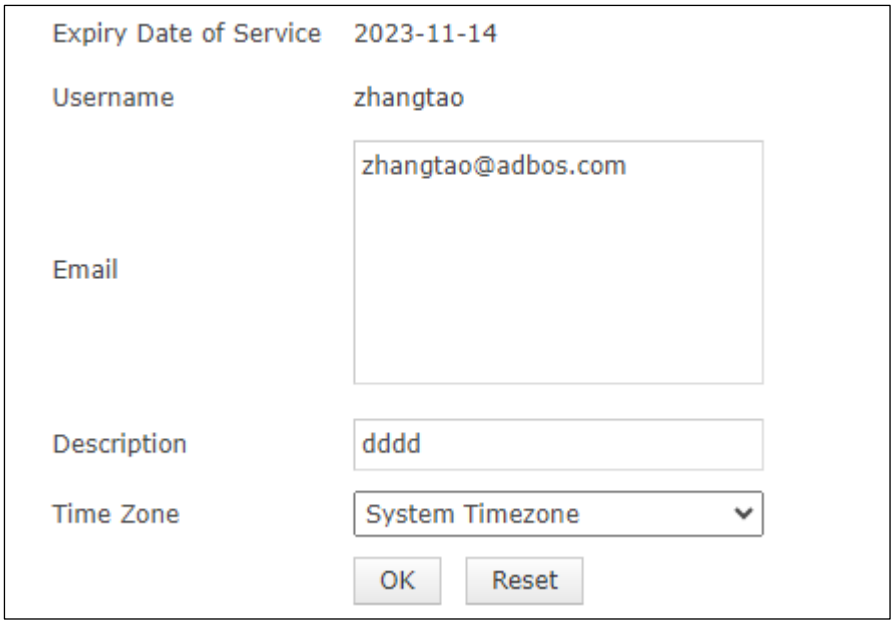
No.	Area	Description
1	Menu bar	Main menus of the system.
2	Work area	Area where you can perform configurations and operations and view data.
3	Quick access bar	Provides buttons for quick access to certain functions of the system. • ENGLISH: switches between simplified Chinese and English. • Logout: logs you out of ADS Portal. Note 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 **System > 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 **System > 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.

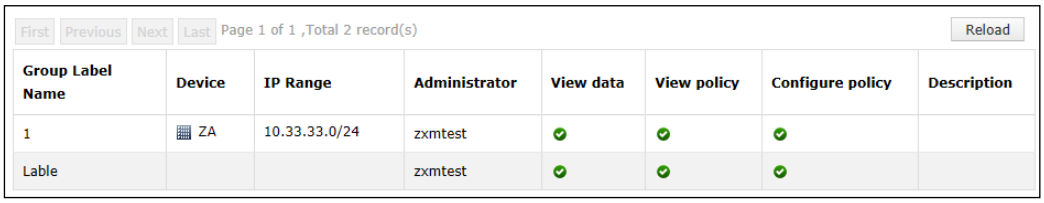
Figure 4-1 Region list

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



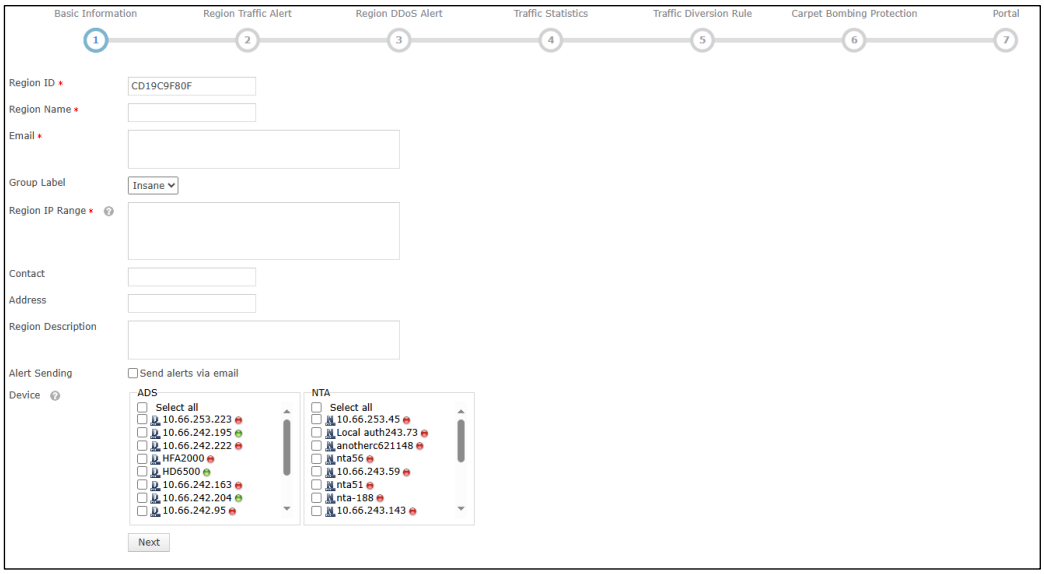
4.1.2 Creating a Region

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

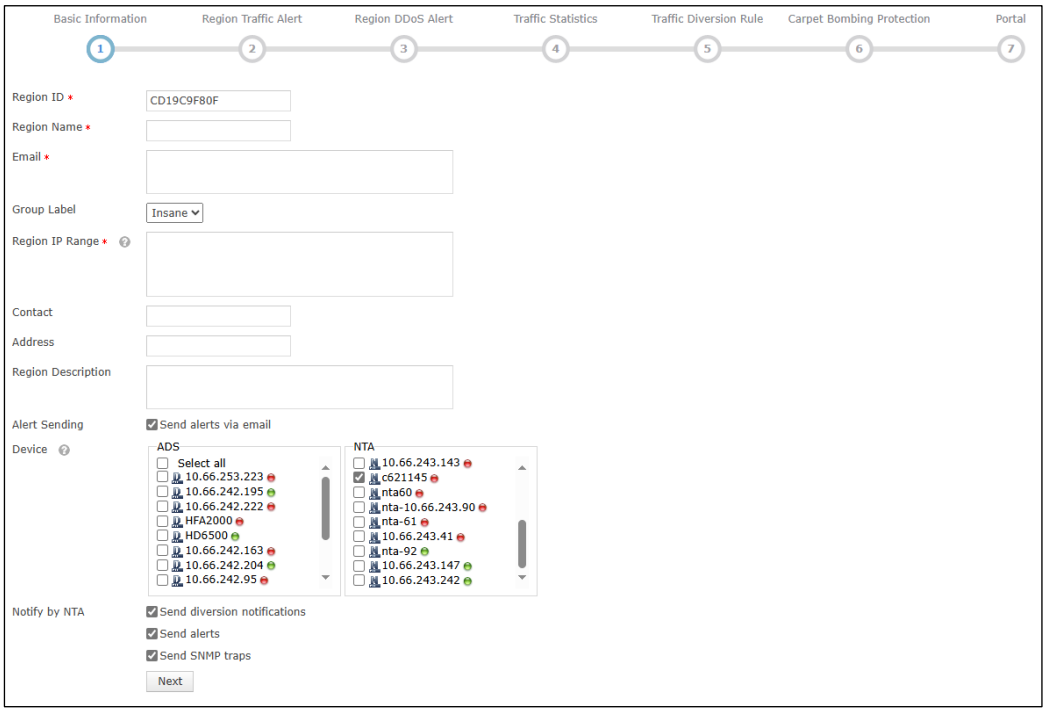
Parameter	Description
Region ID	Uniquely identifies a region. It is automatically generated by the system and can be manually changed (note that you cannot change it when editing a region and it cannot be the same as an existing one) when you create a region. The region ID should be a string of 1 to 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

Parameter	Description
	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 (;).
Group Label	Group label of the region.
Region IP Range	Specifies the IP address range in the region monitored and protected by ADS M. Both IPv4 and IPv6 addresses are accepted. You can type one or more IP addresses, IP subnets, and IP address ranges, with each in a separate line. A maximum of 4096 entries are allowed. • IPv4 address format: 192.168.0.1, 192.168.0.1/24, or 192.168.0.1–254 • IPv6 address format: 2001::1-fffe, 2001::1-fffe/126, or 2001::1 An IP subnet can be a class B or class C IP subnet, containing up to 65,536 IP addresses. The prefix length of IPv4 addresses can be 16–32 and that of IPv6 addresses can be 112–128.
Contact	Contact person of the region.
Tel	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. After **Send alerts via email** is selected, ADS M will periodically send region alerts to the email address of the contact person. For details about scheduling the sending of region alerts, see section 2.2 Sending Email Alerts.
Device	Specifies ADS and NTA devices for the region. Only devices that are managed by ADS M are available for you to select. 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: • **Region Inbound Traffic Abnormal**: checks the total inbound traffic of the region. • **Region Outbound Traffic Abnormal**: checks the total outbound traffic of the region.
Detection Mode	Specifies the type of traffic based on which an alert is generated. It has the following values: • **Not detect**: indicates that NTA does not check whether inbound or outbound traffic is abnormal.

Parameter	Description
	• **Packets only**: indicates that an alert is generated when the traffic rate in pps is found to exceed the threshold. • **Bytes only**: indicates that an alert is generated when the traffic rate in bps is found to exceed the threshold. • **Both packets and bytes**: indicates that an alert is generated when the traffic rate in pps and that in bps are both found to exceed the thresholds. • **Either packets or bytes**: indicates that an alert is generated when either the traffic rate in pps or that in bps is found to exceed the threshold.
Latent Alert Threshold	Specifies the traffic rate threshold in bps or pps that triggers NTA to generate an alert only after the traffic rate stays at this level for some time. • **bps**: indicates a threshold in bps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **Not detect** or **Packets only** for **Detection Mode**. • **pps**: indicates a threshold in pps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **Not detect** or **Bytes only** for **Detection Mode**. Note The latent alert threshold must be lower than the direct alert threshold.
Direct Alert Threshold	Specifies the traffic rate threshold in bps or pps that triggers NTA to generate an immediate alert. • **bps**: indicates a threshold in bps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **Not detect** or **Packets only** for **Detection Mode**. • **pps**: indicates a threshold in pps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **Not detect** or **Bytes only** for **Detection Mode**. Note Note that the direct alert threshold must be greater than the latent alert threshold.
Alert Hierarchy (%)	Specifies how to classify alert levels. **Latent Alert Threshold** is a basis for classifying alert levels and needs to be configured in advance. Alert levels are classified according to the ratio of actual traffic to the **Latent Alert Threshold** value: • **Low**: specifies the lowest ratio for triggering a low-level alert. The value is always **100**. When the actual ratio falls between the smallest ratio for triggering a lower-level alert and the smallest ratio for triggering a medium-level alert, NTA generates a low-level alert. • **Medium**: specifies the ratio for triggering a medium-level alert. The default value is **150** and the maximum value is **10000**. When the actual ratio falls between the smallest ratio triggering a medium-level alert and the smallest ratio for triggering a high-level alert, NTA generates a medium-level alert. • **High**: specifies the ratio for triggering a high-level alert. The default value is **200** and the maximum value is **10000**. When the actual ratio is greater

Parameter	Description
	than the smallest ratio for triggering a high-level alert, NTA generates a high-level alert. If **Alert Hierarchy** is not configured, NTA will detect traffic and send alerts according to the global alert hierarchy.
Diversion Level	Specifies the alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted. • **No diversion**: indicates that no traffic diversion will take place. • **Low**: indicates that a low-level alert or higher will trigger traffic diversion. • **Medium**: indicates that a medium-level alert or higher will trigger traffic diversion. • **High**: 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. After you select **On**, NTA will check traffic for carpet bombing attacks. Carpet bombing is a kind of DDoS attack that targets a large number of IP addresses.
Top N	Specifies the number of top IP addresses with the largest inbound traffic for the carpet bombing detection. 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. 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 Attack Alert for a Network Segment**: After it is enabled, IP addresses in the region will be aggregated by the specified netmask/prefix length to a CIDR block to detect attack traffic. When the aggregate inbound traffic of the CIDR block in a detection period that matches an attack signature exceeds the specified threshold, a network segment-specific DDoS attack alert will be generated. The default IPv4 netmask is **24**, and the default IPv6 prefix is **120**.

Note	The region's IP address range must be in CIDR notation to enable network segment-based detection.

- **Region DDoS Attack Alert for an IP Address**: Respectively configure **Inbound Detection Configuration** and **Outbound Detection Configuration**.
  - **Inbound Detection 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 Detection Configuration**: Configure **Constituent Proportion Configuration** after enabling this function.

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

Parameter	Description
Detection Mode	Specifies a basis for DDoS detection and alerting. Options include **Not detect** and **Abnormal Connections**. 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). 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. 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. • **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. • **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. Value range: 100–10000. The value specified for **High** should be larger than that for **Medium**.

Parameter	Description
Diversion Level	Specifies an alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted. • **No diversion**: generates alerts only, with no traffic diversion to take place. • **Low**: indicates that a low-level alert or higher will trigger traffic diversion. • **Medium**: indicates that a medium-level alert or higher will trigger traffic diversion. • **High**: 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. 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	Top N IPs for Inbound Traffic Diversion	Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 300. When **Region Policy for Abnormal Inbound Traffic Diversion** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses.
	Region Policy for Abnormal Inbound Traffic Diversion	Specifies the diversion policy for inbound traffic of top N IP addresses when the inbound traffic alert is triggered. • The **Region Policy for Abnormal Inbound Traffic Diversion** can be triggered together with the **Region Policy for Abnormal Outbound Traffic Diversion** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. Note • The diversion policy for a region has a lower priority than that for an IP group. • You can click **Add** and create new diversion policies.
	Top N IPs for Outbound Traffic Diversion	Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 100. When **Region Policy for Abnormal Outbound Traffic Diversion** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses.
	Region Policy for	Specifies the diversion policy for outbound traffic of top N IP

Parameter		Description
	Abnormal Outbound Traffic Diversion	addresses when the outbound traffic alert is triggered. • The **Region Policy for Abnormal Outbound Traffic Diversion** can be triggered together with the **Region Policy for Abnormal Inbound Traffic Diversion** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. Note The diversion policy for a region has a lower priority than that for an IP group. • You can click **Add** and create new diversion policies.
IP Diversion Policy		Specifies the diversion policy for IP addresses in a specific IP group when the DDoS alert is triggered. • The **IP Diversion Policy** can be triggered together with the **Region Policy for Abnormal Inbound Traffic Diversion** and **Region Policy for Abnormal Outbound Traffic Diversion**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. • You can click **Add** and create new IP-specific diversion policies.
Network Segment-specific Diversion Policy		Specifies the diversion policy for a global CIDR block when the network segment-based DDoS alert is triggered. • The **Network Segment-specific Diversion Policy** can be triggered together with the **Region Policy for Abnormal Inbound Traffic Diversion** and **Region Policy for Abnormal Outbound Traffic Diversion**. • You can click **Add** and create new network segment-specific diversion policies

Step 8 Click **Next** to configure a carpet bombing protection rule.

Carpet bombing is a kind of DDoS attack that targets a large number of IP addresses. It generates massive attack traffic in a short time, which easily paralyzes the entire equipment room. A carpet bombing protection rule can be configured on the basis of DDoS policy and behavior.

Table 4-5 Parameters of carpet bombing protection

Parameter	Description
Enable	Controls whether to enable the carpet bombing protection function. • **Yes**: enables the carpet bombing protection function. • **No**: disables the carpet bombing protection function.
IP Aggregation	Specifies how to aggregate IP addresses using the IPv4 netmask or IPv6 prefix length. The **IPv4 Netmask** is fixed to **24** and the **IPv6 Prefix Length** is fixed to **120**. The value here cannot be edited.
DDoS Policy-based Carpet	The protection thresholds here work for network segments defined with a subnet mask or prefix length. If the total number of packets of a certain type to a network segment

Bombing Protection	exceeds the related threshold, the network segment will be protected with the related policy, which is the one configured for the protection group to which the destination IP address belongs.	
	DDoS Policy	Displays different types of packets and the traffic control by destination segment.
	Threshold 1	Threshold for the rate of traffic to a network segment. When the rate (pps) of such traffic exceeds the specified value, the network segment will be protected with the related policy. • **SYN Flood**: The value range is 0–48000000. • **ACK Flood**: The value range is 0–240000000. • **UDP Flood**: The value range is 0–48000000. • **ICMP Flood**: The value range is 0–48000000. • **HTTP Get Flood**: The value range is 0–48000000. • **HTTP Post Flood**: The value range is 0–48000000. • **HTTPS Flood**: The value range is 0–48000000. • **Traffic Control by Dst Segment**: The value range is 0–8000000, in kbps.
	Enable	Controls whether to enable the protection of the current type.
Behavior-based Carpet Bombing Protection	**Destination IPs** here refers to the number of IP addresses to be protected. The system counts the number of visits of a source IP address to destination IP addresses and determines whether the source IP address is abnormal. For the identified attack source, the system can add it to the blocklist or limit its rate, or do both.	
	Enable	Controls whether to enable the behavior-based carpet bombing protection.
	Action	Specifies the action taken against a source IP address that triggers the carpet bombing protection rule. Options include **Add to blocklist**, **Limit rate**, and **Limit rate & add to blocklist**.
	Period	Specifies a period of time when the number of visits to destination IP addresses is counted. Value range: 1–600, in seconds.
	Parameters of **Limit rate** policy	When a source IP address accesses more IP addresses than the value of **Destination IPs** within the statistical period and this anomaly persists for the specified number of **Consecutive Abnormal Cycles, the device limits its traffic.** • **Destination IPs**: maximum allowed number of destination IP addresses accessed by a single source IP address in the statistical period. Value range: 1–10000. • **Consecutive Abnormal Cycles**: number of consecutive cycles where a source IP address accesses the specified number of destination IP addresses. The device deems such a source IP address to be abnormal. Value range: 1–10. • **Per Source IP Rate Limit**: maximum traffic rate allowed for a source IP address. Excess packets will be dropped. Value range: 0–524280 in pps or 0–1073741824 in bps. • **Rate Limit Duration**: specifies how long rate limiting is implemented against a source IP address. When the duration expires, rate limiting stops. Value range: 1–3600, in minutes.
	Parameters of **Add to**	When a source IP address accesses more IP addresses than the value of **Destination IPs** within the statistical period and this anomaly persists for the specified number of **Consecutive Abnormal Cycles,** the device

	blocklist policy	adds it to the blocklist. • **Destination IPs**: maximum allowed number of destination IP addresses accessed by a single source IP address in the statistical period. Value range: 1–10000. • **Consecutive Abnormal Cycles**: number of consecutive cycles where a source IP address accesses the specified number of destination IP addresses. The device deems such a source IP address to be abnormal. Value range: 1–10.
Description	Brief information about the carpet bombing protection rule, which is less than 256 characters.	

Step 9 Configure the Portal.

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

b. Configure parameters on this page.

Table 4-6 describes the parameters for configuring the Portal.

Table 4-6 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**.
Valid Till	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**. • **Password**: The account can log in to the Portal after typing the correct user name and password. • **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 10 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.

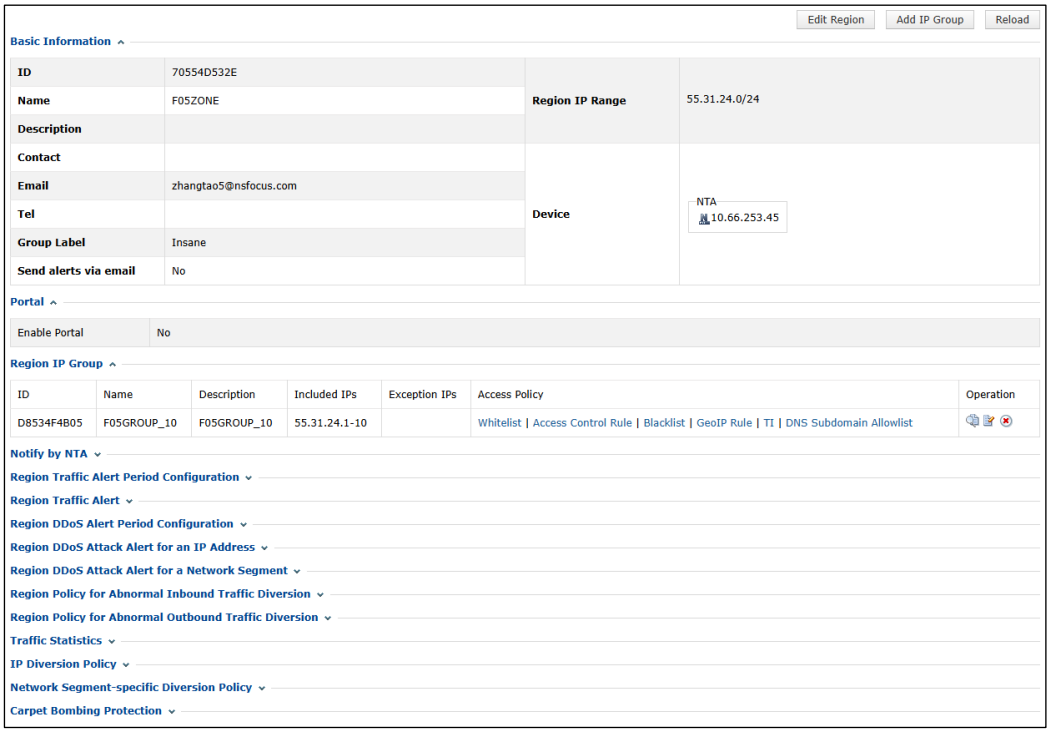
4.1.4 Deleting a Region

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. Or click **Add IP Group** on the region setting page as shown in Figure 4-5.

Step 2 Configure basic information of the new IP group.

Table 4-7 describes parameters for configuring basic information of an IP group.

Table 4-7 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

Parameter	Description
	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. • 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. • IP addresses in an IP group must be covered by the IP address range of the region. Otherwise, the system prompts you to change the range. Different IP groups in a region must contain different IP addresses. Otherwise, the system prompts you to change the range. • When you type IP addresses, the IP range of the region to which the IP group belongs is dynamically displayed below the text box. Note A region can have a maximum of 64 IP groups, each of which can contain a maximum of 1024 entries.
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. The format is the same as that for **Included IPs**.
IP Group Description	Brief description of the IP group.
Notify by 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 Attack Alert for an IP Address**: Respectively configure **Inbound Detection Configuration** and **Outbound Detection Configuration**.
  - **Inbound Detection Configuration**: Configure **Fixed Threshold Configuration**, and **Constituent Proportion 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 Detection 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. 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 4-8 describes parameters for configuring traffic diversion rules for an IP group.

Table 4-8 Parameters for configuring diversion rules for an IP group

Parameter		Description
IP Group Diversion Policy	Top N IPs for Inbound Traffic Diversion	Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 300. When **IP Group Policy for Abnormal Inbound Traffic Diversion** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses or all IP addresses (**Any**) in an IP group.
	IP Group Policy for Abnormal Inbound Traffic Diversion	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. • The **IP Group Policy for Abnormal Inbound Traffic Diversion** can be triggered together with the **IP Group Policy for Abnormal Outbound Traffic Diversion** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. Note The diversion policy for a region has a lower priority than that for an IP group. • You can click **Add** to add new diversion policies.
	Top N IPs for Outbound Traffic Diversion	Specifies the number of top IP addresses for which traffic diversion is conducted. The system sorts top N IP addresses every 5 minutes. N stands for a variable ranging from 1 to 100. When **IP Group Policy for Abnormal Outbound Traffic Diversion** is triggered, NTA can perform null-route or BGP diversion for top N IP addresses.
	IP Group Policy for Abnormal Outbound Traffic Diversion	Specifies the diversion policy for outbound traffic of top N IP addresses in an IP group when the outbound traffic alert is triggered.

Parameter		Description
		• The **IP Group Policy for Abnormal Inbound Traffic Diversion** can be triggered together with the **IP Group Policy for Abnormal Outbound Traffic Diversion** and **IP Diversion Policy**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. Note The diversion policy for a region has a lower priority than that for an IP group. • You can click **Add** to add new diversion policies.
IP Diversion Policy		Specifies the diversion policy for IP addresses in a IP group when the DDoS alert is triggered. • **IP Diversion Policy** can be triggered together with the **IP Group Policy for Abnormal Inbound Traffic Diversion** and **IP Group Policy for Abnormal Outbound Traffic Diversion**. • When there are multiple diversion policies, the one on top has the highest priority. Policy priorities can be manually set. • You can click **Add** to add new diversion policies.

Step 7 Configure IP group protection policies.

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.

Setting a Group-specific Allowlist

Specify whether to enable the allowlist ("whitelist" on the UI) and the proxy monitoring.

Setting a Group-specific Access Control Rule

Click **Add** to create an access control rule. Table 4-1 describes parameters for creating an access control rule.

Table 4-9 Parameters for creating an access control rule

Parameter	Description
Protocol Type	Protocol that a packet uses. Values can be **TCP**, **UDP**, **ICMP**, **ICMPv6**, and **ALL**. **ALL** means all the four protocols.

Parameter	Description
Enable	Controls whether to enable the access control rule. • **Yes**: enables the rule. • **No**: disables the rule.
Dst IP	IP address of the server to be protected. You can type an IPv4 or IPv6 address according to the actual network deployment. The value **0.0.0.0** or **::** indicates all destination IP addresses.
Dst IP Prefix Length/Netmask	Netmask of the destination IP address.
Dst Port	Server port to be protected. This parameter is available only when **Protocol** is set to **TCP** or **UDP**. You can specify a port ranging from 0 to 65535.
Src IP	Client IP address to be protected. You can type an IPv4 or IPv6 address according to the actual network deployment.
Src IP Prefix Length/Netmask	Netmask of the client IP address.
Src Port	Source port to be protected against. This parameter is available only when **Protocol** is set to **TCP** or **UDP**. You can specify a port ranging from 0 to 65535. If this parameter is not specified, the device enables the access control policy for all connections of the source IP address.
Access Policy	Action performed by the device on packets with specified signatures. It has the following options: • **Accept**: allows such packets to pass through. • **Drop**: drops the packets once they are detected.
Description	Description of the new rule, which can contain a maximum of 256 characters.
Creation Time	Time automatically generated by the system on the creation of the new rule. It cannot be edited.

Setting a Group-specific Blocklist

Specify whether to enable the blocklist ("blacklist" on the UI), block time, and whether to enable proxy monitoring.

Setting a Group-specific GeoIP Rule

Click **Add** to configure a group-specific GeoIP rule. You need to choose whether to enable the group-specific rule, and specify the source location, access control rule, and description.

Setting a Group-specific TI

Specify whether to enable the TI protection and specify the policies taken against traffic whose source/destination IP address has a match in the intelligence database. Options include **Block** and **Traffic Control by Dst IP**.

Setting a Group-specific DNS Subdomain Allowlist

Specify whether to enable the DNS subdomain allowlist and configure its parameters. This group-specific DNS subdomain allowlist works only when the global DNS subdomain allowlist is disabled.

Table 4-10 Parameters of DNS subdomain allowlist auto-learning

Parameter		Description
DNS Subdomain Allowlist Configuration	Enable	Controls whether to enable the DNS subdomain allowlist function.
	Primary Domain	Only DNS requests matching a primary domain name are further matched against the subdomain allowlist. Enter each primary domain name in a separate line. At most three can be configured. Leaving this field empty indicates that all DNS requests will be checked against this policy. A primary domain name should meet the following requirements: • The domain name consists of letters, digits, dots, hyphens, and/or underscores. • Each label of the primary domain name ranges from 1 to 63 characters, and the primary domain name cannot exceed 128 characters. • The primary domain name should contain at least one label. • A label cannot start or end with a hyphen, nor have consecutive hyphens
	Action for Unmatched DNS Requests	Controls DNS requests matching the primary domain list but not the subdomain list. Options include **Default**, **Limit rate**, and **Drop**. If the subdomain list is empty, this action does not work. Before setting an action, configure a valid DNS subdomain allowlist for the group first.
Subdomain Allowlist Auto-Learning	Enable	Controls whether to enable the auto-learning function of the subdomain allowlist. After the DNS subdomain allowlist and its auto-learning function are both enabled, the system can automatically learn and identify requests from normal DNS subdomains, and filters out requests from malicious subdomains. This improves protection effectiveness and reduces false positives.
	Auto-learning Type	Packet type on which DNS subdomain auto-learning will be based. Options include **DNS query** and **DNS response**. • **DNS query** is applicable to diversion and in-path modes.

			– In diversion mode, ADS will automatically learn subdomain names from DNS queries over all interfaces. – In in-path mode, ADS will automatically learn subdomain names only from DNS queries over the IN interface. • **DNS response** is applicable to the in-path mode. In this mode, ADS will automatically learn subdomain names from DNS responses received by the OUT interface. For ADS in in-path mode, the preferred option is **DNS response**. Note If **DNS response** is selected, **Action for Unmatched DNS Requests** cannot be set to **Drop**.
	Min Source IPs		This parameter is required when **DNS query** is selected for **Auto-learning Type**. Minimum number of source IP addresses that request the same subdomain names. The value range is 2–256, with **3** as the default.
	Period		This parameter is required when **DNS query** is selected for **Auto-learning Type**. Period of time when the number of source IP addresses that request the same domain name is counted. The value range is 1–3600 seconds, with **30** as the default. When the number reaches the threshold specified with **Min Source IPs** in the statistical period, the requested subdomain name is added to the allowlist.
	Constraints	Max Domain Levels	Maximum number of levels allowed for domain name. When the number reaches the threshold, the domain name will not be added to the allowlist. The value range is 0–16, with **0** as the default. The value **0** indicates no limit.
		Uppercase Restriction	Controls whether to allow the subdomain name to contain uppercase letters. The value **Yes** indicates subdomain names containing uppercase letters will not be added to the allowlist.
	Auto Allowlist Duration		Validity period of subdomain names in the allowlist. After this period, the subdomain names will be removed from the allowlist. The value range is 0–8000000 minutes, with **120** as the default. The value **0** indicates permanently valid.

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** dialog box, configure URL rule parameters.

Table 4-11 describes parameters for adding a rule.

Table 4-11 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 (without 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.
Dst 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**. • An IP group that is included in a smart protection group cannot be modified.

4.1.8 Deleting an IP Group

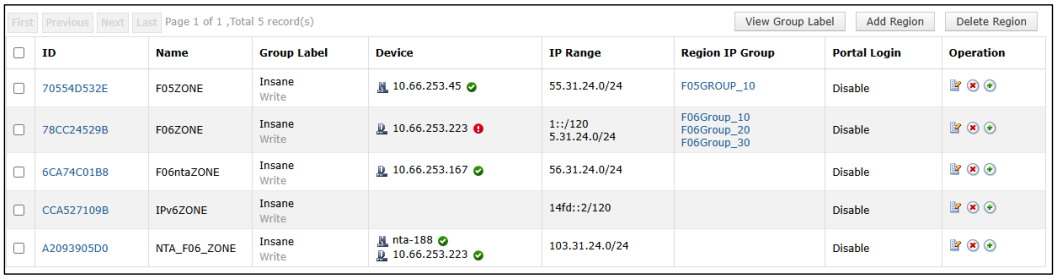
In the **Region IP Group** list on the page shown in Figure 4-5, click  in the **Operation** column of an IP group to delete this group.

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

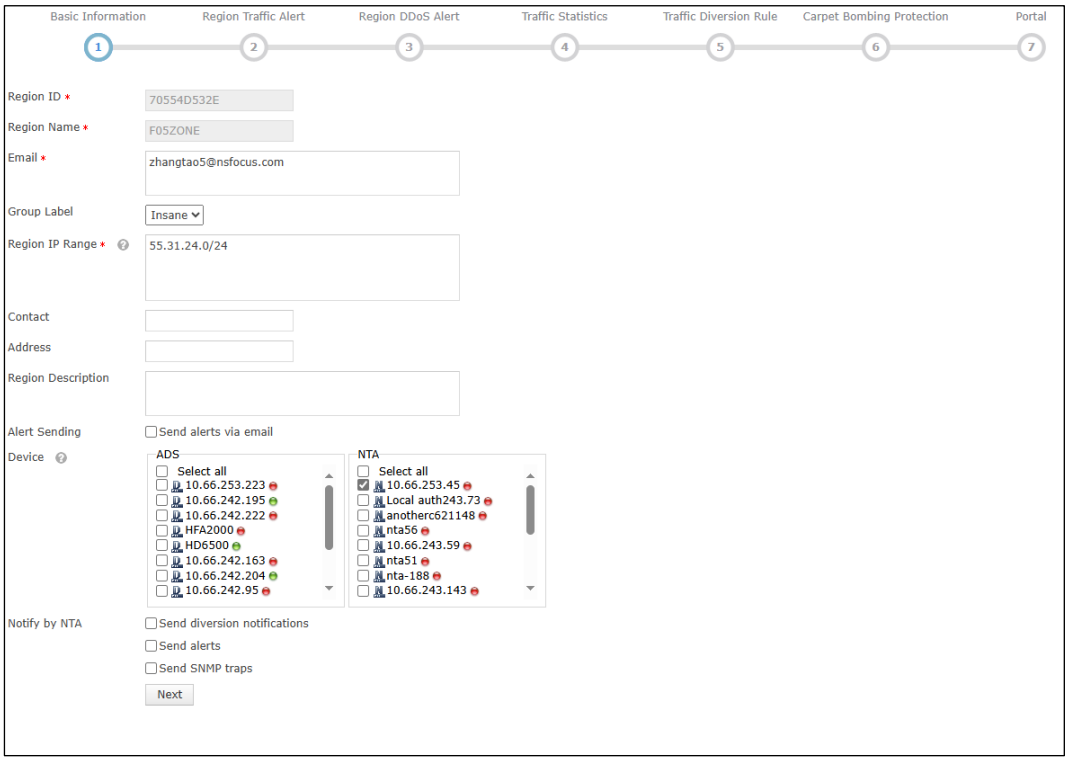


4.2.1 Editing Basic Information of a Region

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

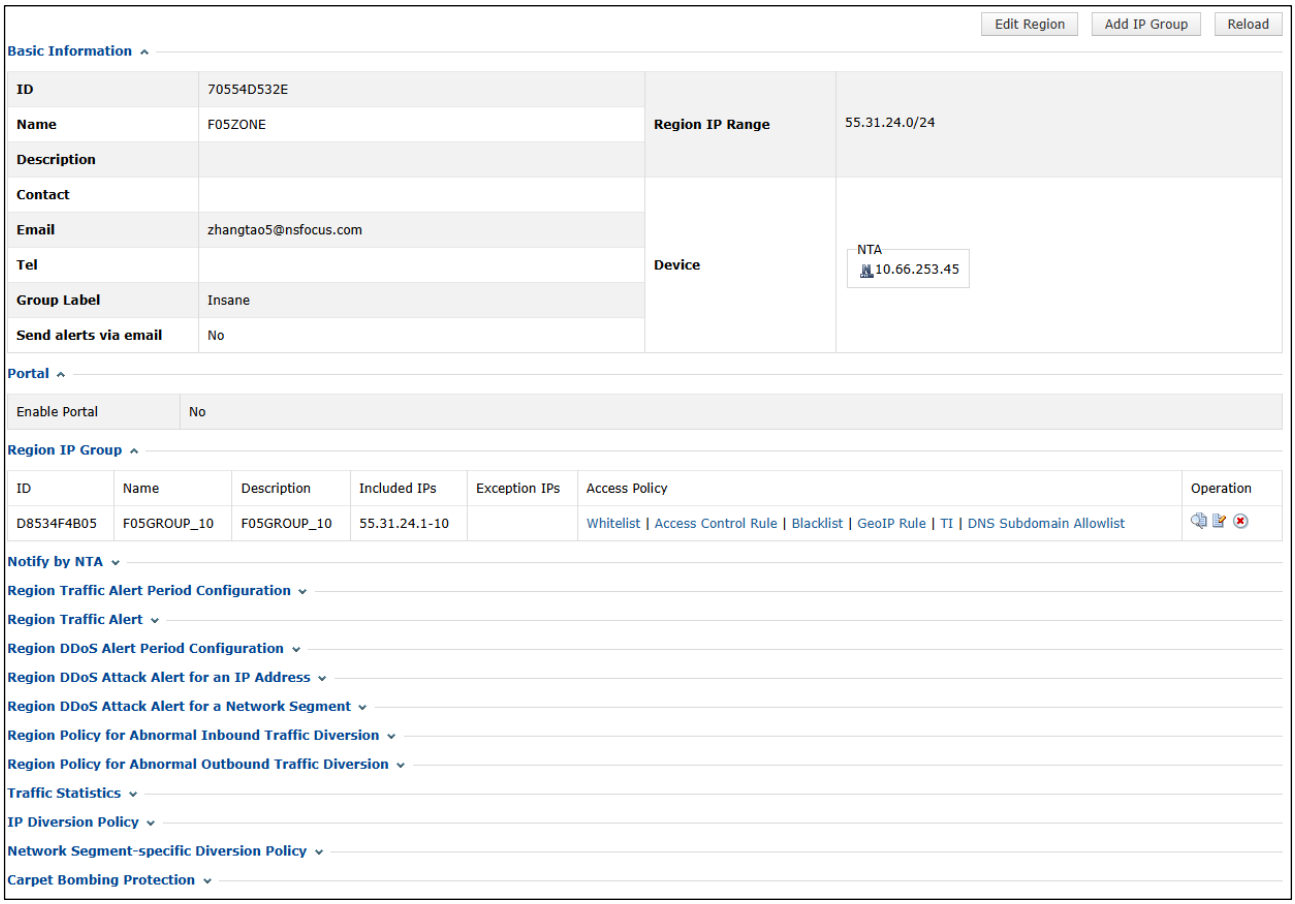


4.2.2 Viewing Region Settings

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

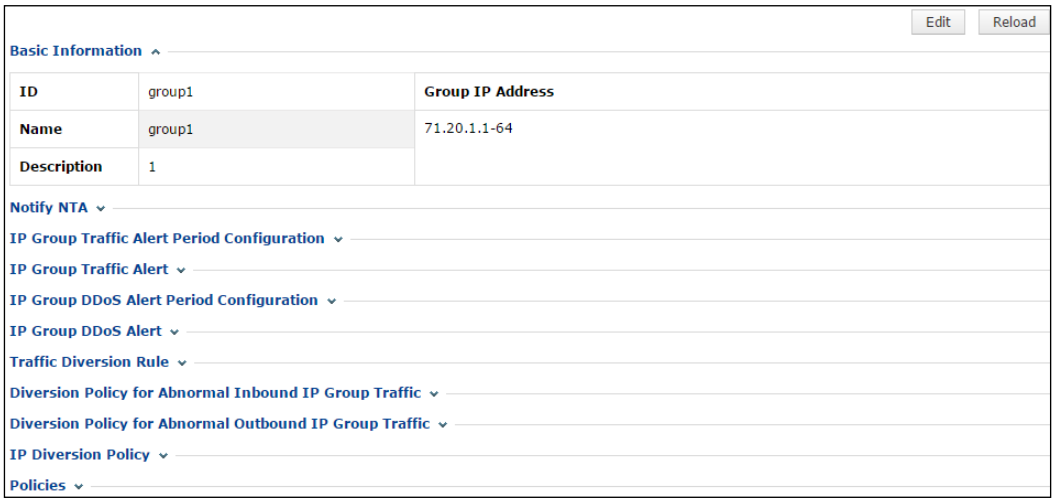


4.2.3 Viewing IP Group Settings

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



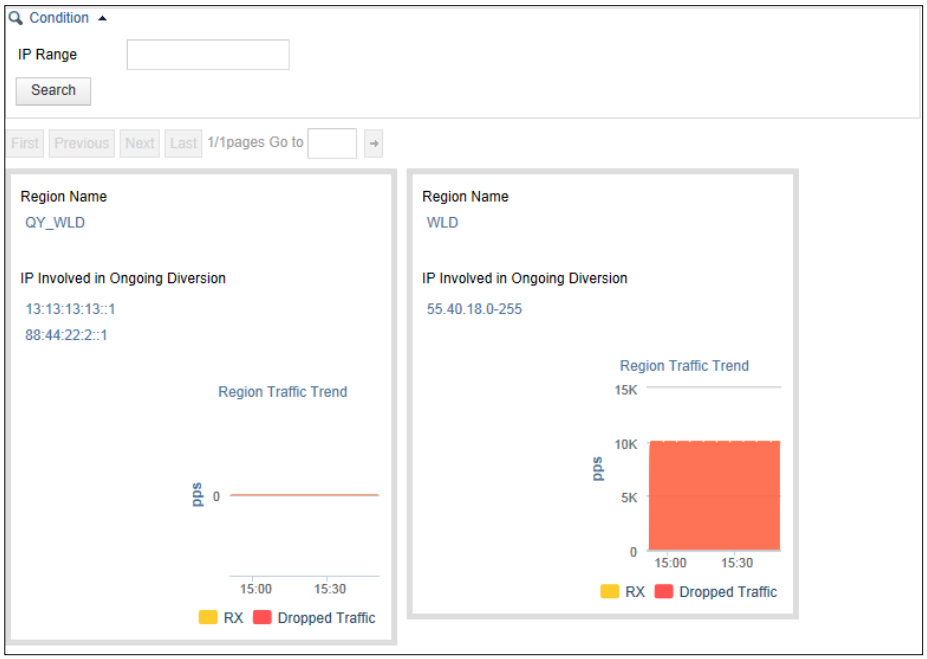
5 Region Traffic Diversion

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."

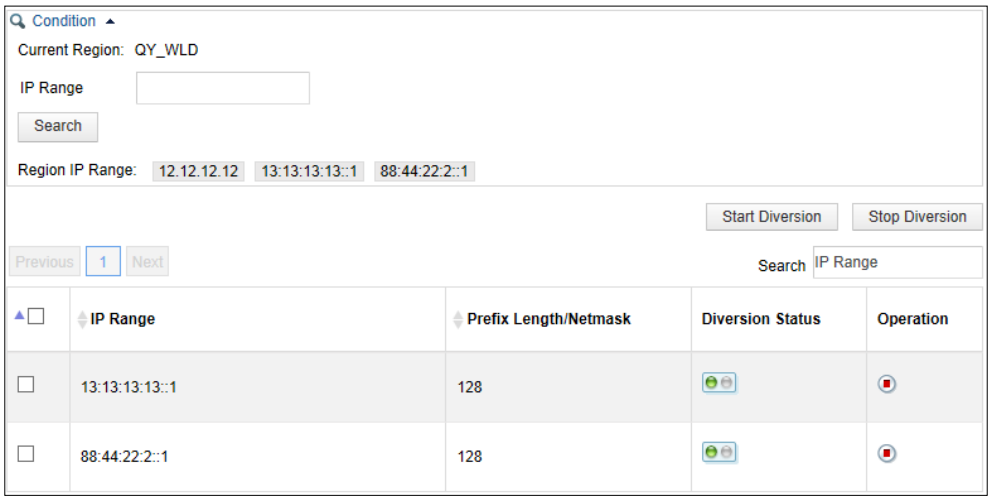
Figure 5-1 Traffic Diversion page



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.

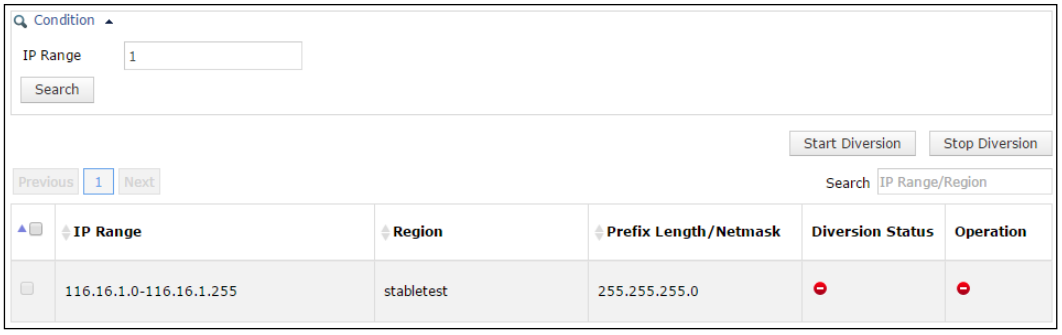
Figure 5-2 Viewing a region involved in traffic diversion



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.

Note	Icons in the **Operation** column are available only when **Route Source** is **Probe**.

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.

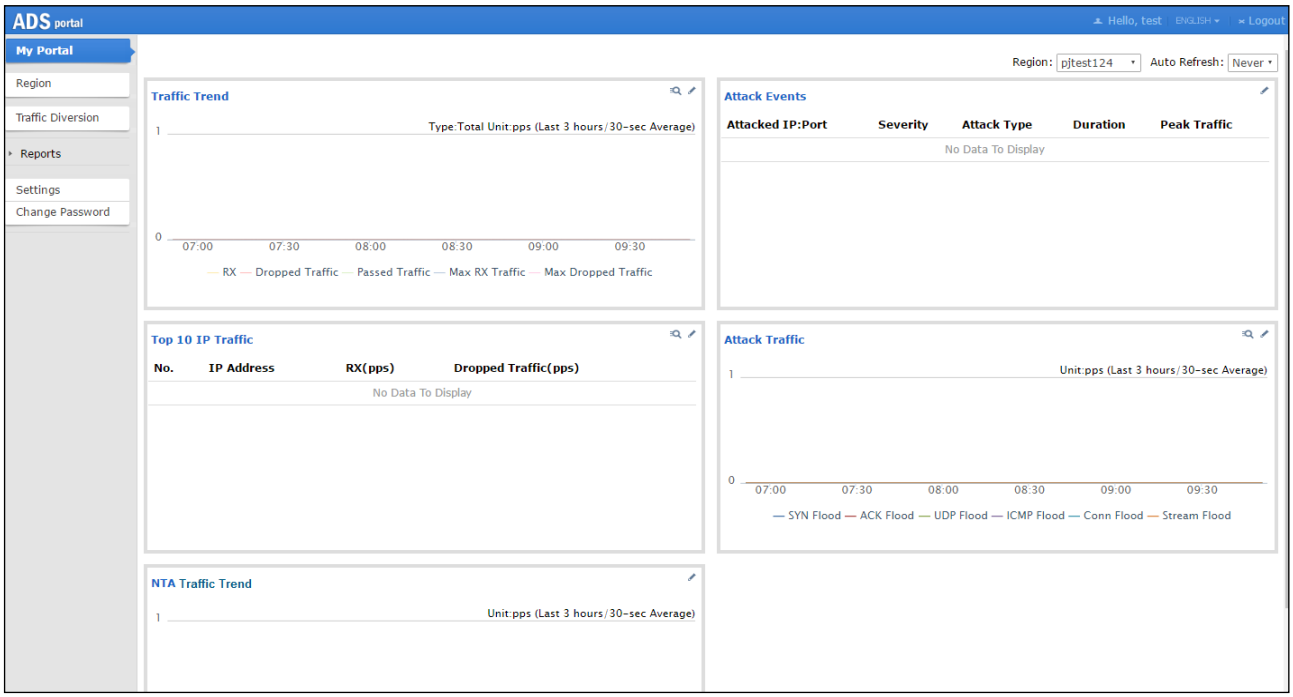
6 System Overview

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.

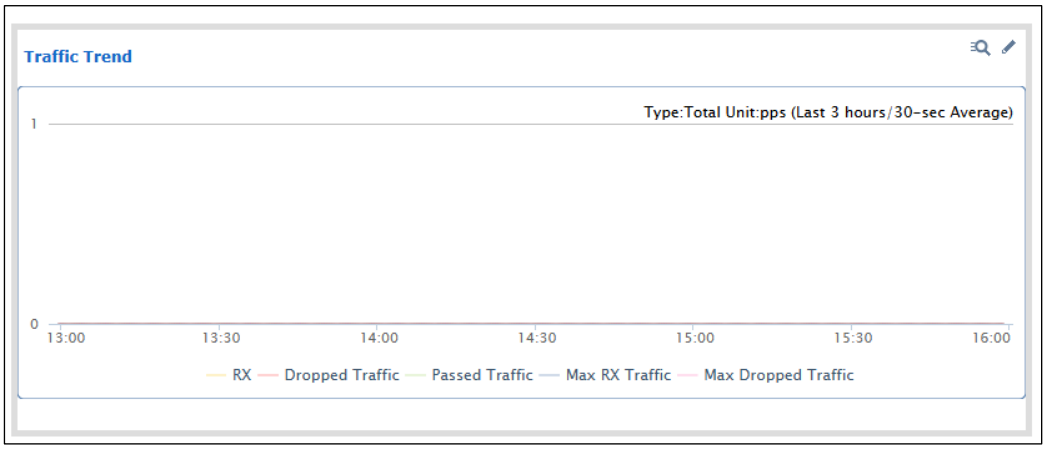
Figure 6-1 My Portal page



6.1 Viewing Traffic Trends

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

Figure 6-2 Traffic trends



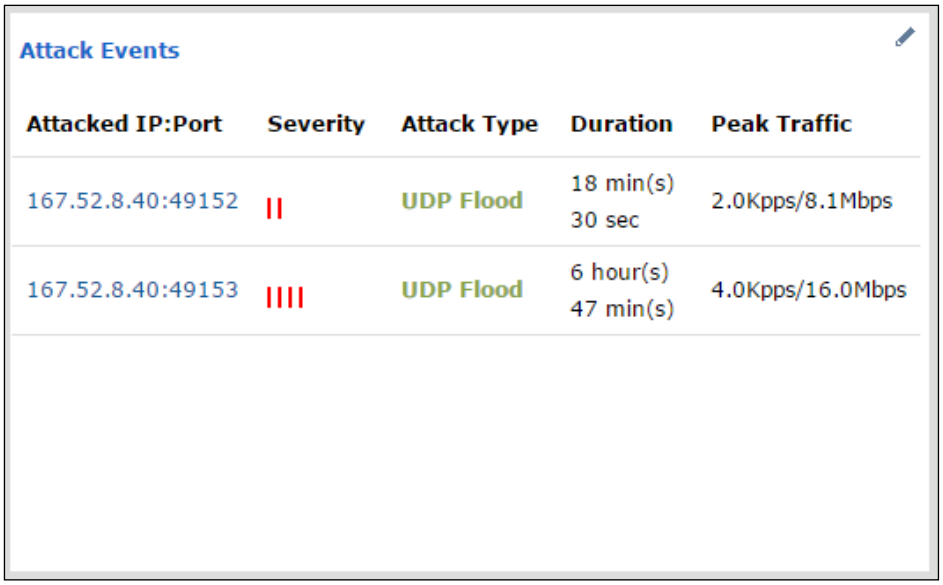
- Clicking in the upper-right corner of the graph opens the traffic trend report page.
- Clicking in the upper-right corner of the graph allows you to edit graph parameters in the dialog box that appears.

  - **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**, **Passed 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

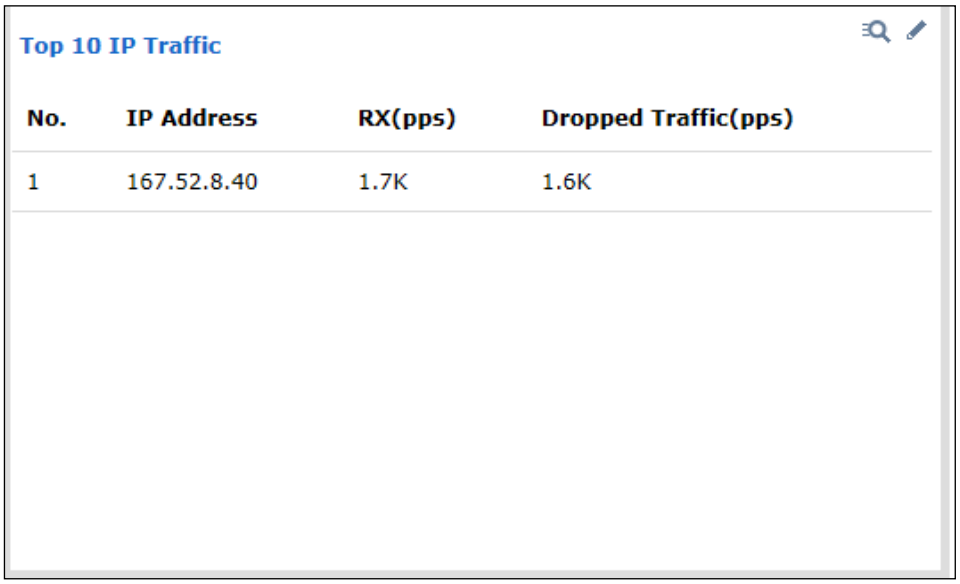


- Clicking an entry under **Attacked IP:Port** opens the attack event report of this IP address.
- Clicking in the upper-right corner of the list allows you to edit list parameters in the dialog box that appears.
  - **Time**: specifies whether the list displays ongoing attack events or those in the 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

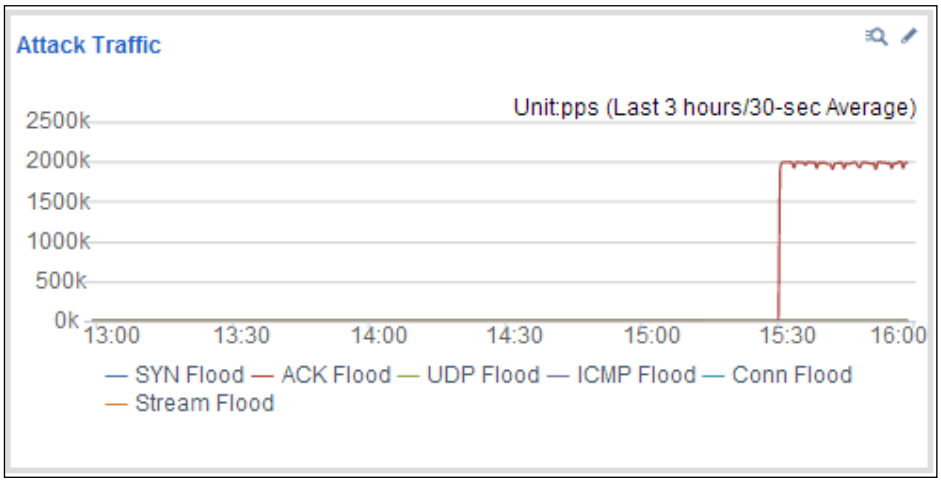


- Clicking in the upper-right corner of the list opens the top N IP address report page (the **TOP** value is **IP**).
- Clicking in the upper-right corner of the list allows you to edit list parameters in the dialog box that appears.
  - **Time**: specifies whether the list displays top 10 IP addresses 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

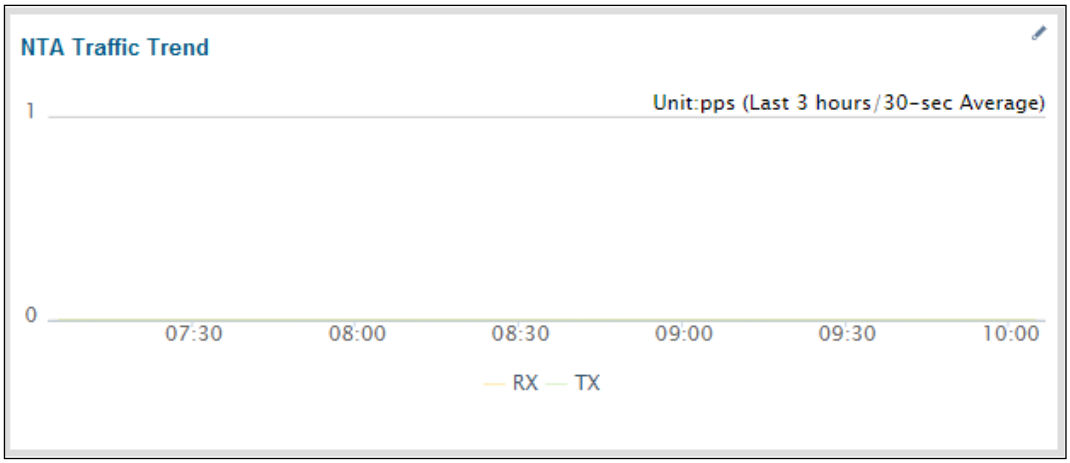


- Clicking in the upper-right corner of the graph opens the top N attack type report page (the **TOP** value is **Attack Type**).
- Clicking in the upper-right corner of the graph allows you to edit graph parameters in the dialog box that appears.
  - **Unit**: specifies whether the graph displays traffic 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 region, 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.

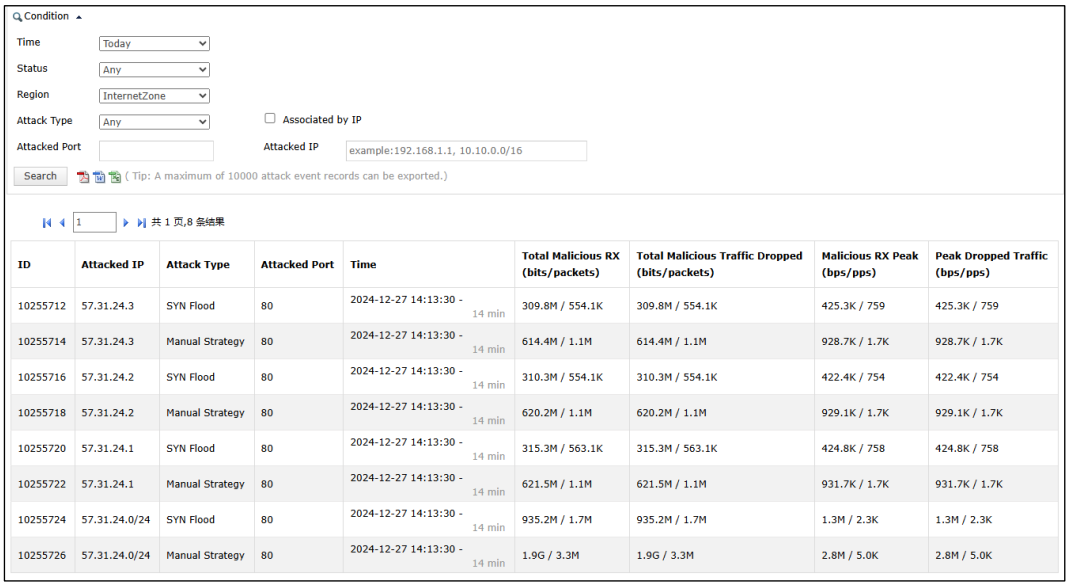
  You can export a maximum of 10,000 records to a report.

7.2 Attack Event Report

An attack event report collects data about attack events in a specified period.

Choose **Reports > Attack Event Report**. 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



ID	Attacked IP	Attack Type	Attacked Port	Time	Total Malicious RX (bits/packets)	Total Malicious Traffic Dropped (bits/packets)	Malicious RX Peak (bps/pps)	Peak Dropped Traffic (bps/pps)
10255712	57.31.24.3	SYN Flood	80	2024-12-27 14:13:30 - 14 min	309.8M / 554.1K	309.8M / 554.1K	425.3K / 759	425.3K / 759
10255714	57.31.24.3	Manual Strategy	80	2024-12-27 14:13:30 - 14 min	614.4M / 1.1M	614.4M / 1.1M	928.7K / 1.7K	928.7K / 1.7K
10255716	57.31.24.2	SYN Flood	80	2024-12-27 14:13:30 - 14 min	310.3M / 554.1K	310.3M / 554.1K	422.4K / 754	422.4K / 754
10255718	57.31.24.2	Manual Strategy	80	2024-12-27 14:13:30 - 14 min	620.2M / 1.1M	620.2M / 1.1M	929.1K / 1.7K	929.1K / 1.7K
10255720	57.31.24.1	SYN Flood	80	2024-12-27 14:13:30 - 14 min	315.3M / 563.1K	315.3M / 563.1K	424.8K / 758	424.8K / 758
10255722	57.31.24.1	Manual Strategy	80	2024-12-27 14:13:30 - 14 min	621.5M / 1.1M	621.5M / 1.1M	931.7K / 1.7K	931.7K / 1.7K
10255724	57.31.24.0/24	SYN Flood	80	2024-12-27 14:13:30 - 14 min	935.2M / 1.7M	935.2M / 1.7M	1.3M / 2.3K	1.3M / 2.3K
10255726	57.31.24.0/24	Manual Strategy	80	2024-12-27 14:13:30 - 14 min	1.9G / 3.3M	1.9G / 3.3M	2.8M / 5.0K	2.8M / 5.0K

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. 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.

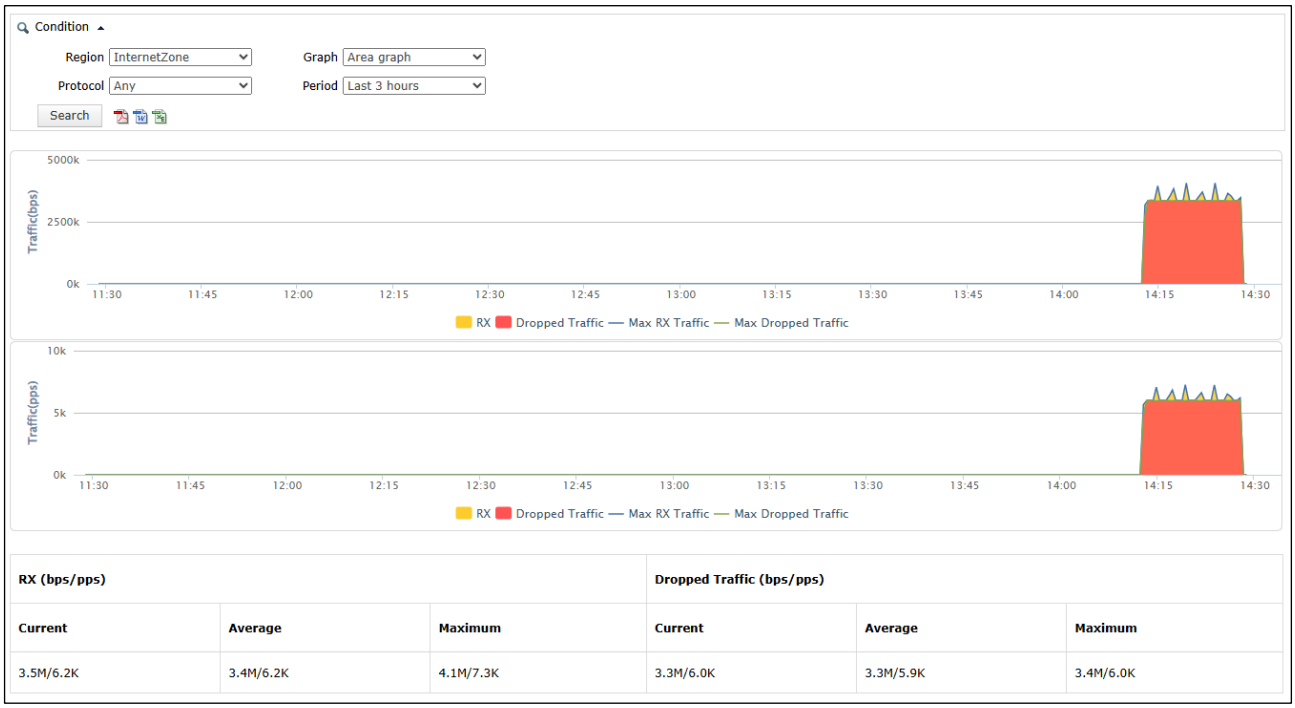
Tip	You can export a maximum of 10, 000 entries in a report. In case large amounts of data are involved, it is recommended that you export the data in different reports by specifying different periods of time.

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.

Choose **Reports > Traffic Trend Report**. Figure 7-2 shows a traffic trend report.

Figure 7-2 Traffic trend report



RX (bps/pps)			Dropped Traffic (bps/pps)		
Current	Average	Maximum	Current	Average	Maximum
3.5M/6.2K	3.4M/6.2K	4.1M/7.3K	3.3M/6.0K	3.3M/5.9K	3.4M/6.0K

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**.

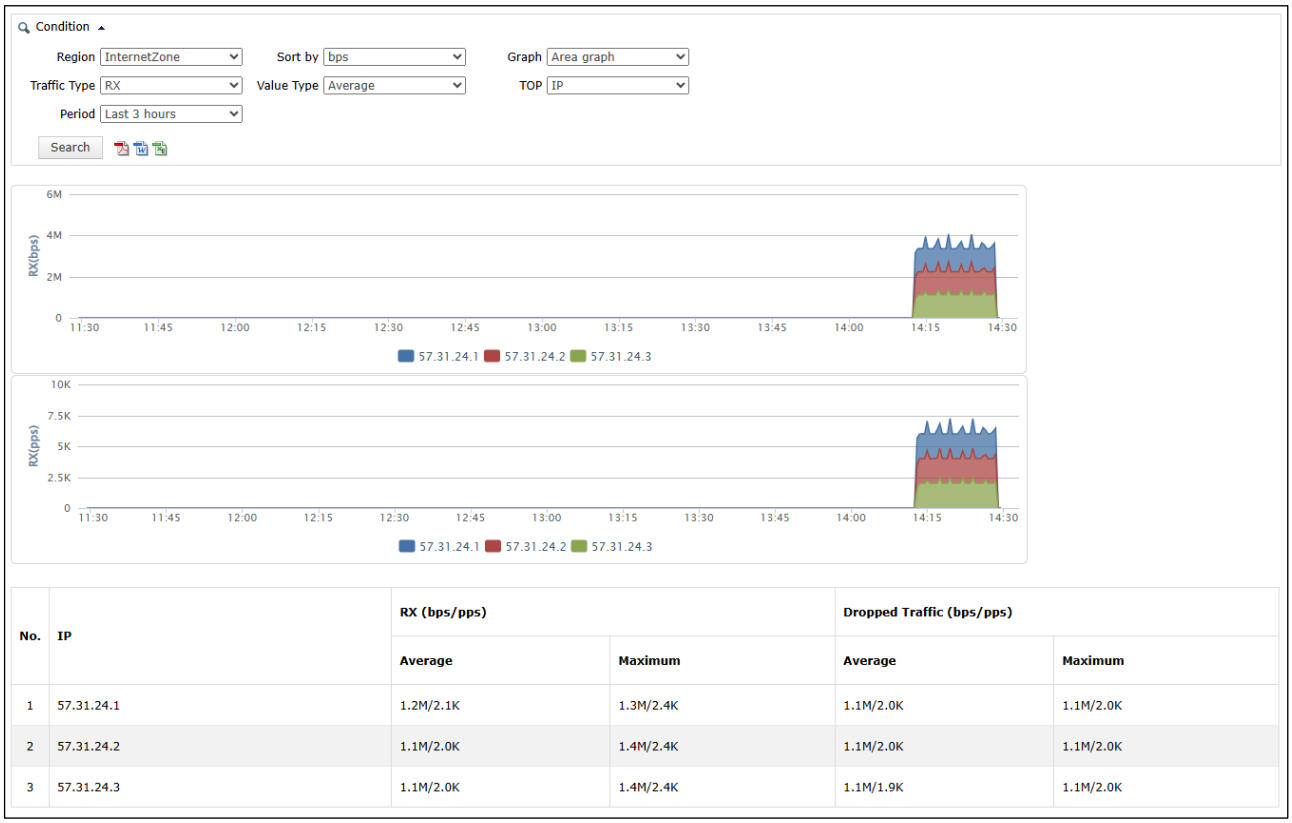
Parameter	Description
Protocol Type	Specifies the protocol type of traffic covered by the report. Options include **TCP**, **UDP**, and **ICMP** and **Any**. **Any** indicates that traffic data of all protocol types will be collected.
Period	Specifies the generation time of traffic the report will cover. 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**. • **Day**: indicates that traffic data of a specified date (0:00 to 24:00) will be collected. • **Week**: indicates that traffic data of the week (starting from Monday) covering the specified date will be collected. • **Month**: indicates that traffic data of a specified calendar month will be collected. • **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.

Choose **Reports > Top N Traffic Report**. 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



No.	IP	RX (bps/pps)		Dropped Traffic (bps/pps)	
		Average	Maximum	Average	Maximum
1	57.31.24.1	1.2M/2.1K	1.3M/2.4K	1.1M/2.0K	1.1M/2.0K
2	57.31.24.2	1.1M/2.0K	1.4M/2.4K	1.1M/2.0K	1.1M/2.0K
3	57.31.24.3	1.1M/2.0K	1.4M/2.4K	1.1M/1.9K	1.1M/2.0K

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.
Sort by	Specifies the unit to measure the top 10 traffic. The options include **bps** and **pps**.
Graph	Specifies the statistical graph types: • **Area graph**: available only when **Value Type** is set to **Average**. • **Line graph**: always available.
Traffic Type	Specifies the traffic type. • **RX**: indicates that only data of received traffic will be collected. • **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.

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

Choose **Reports > Integrated Report**. This report 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

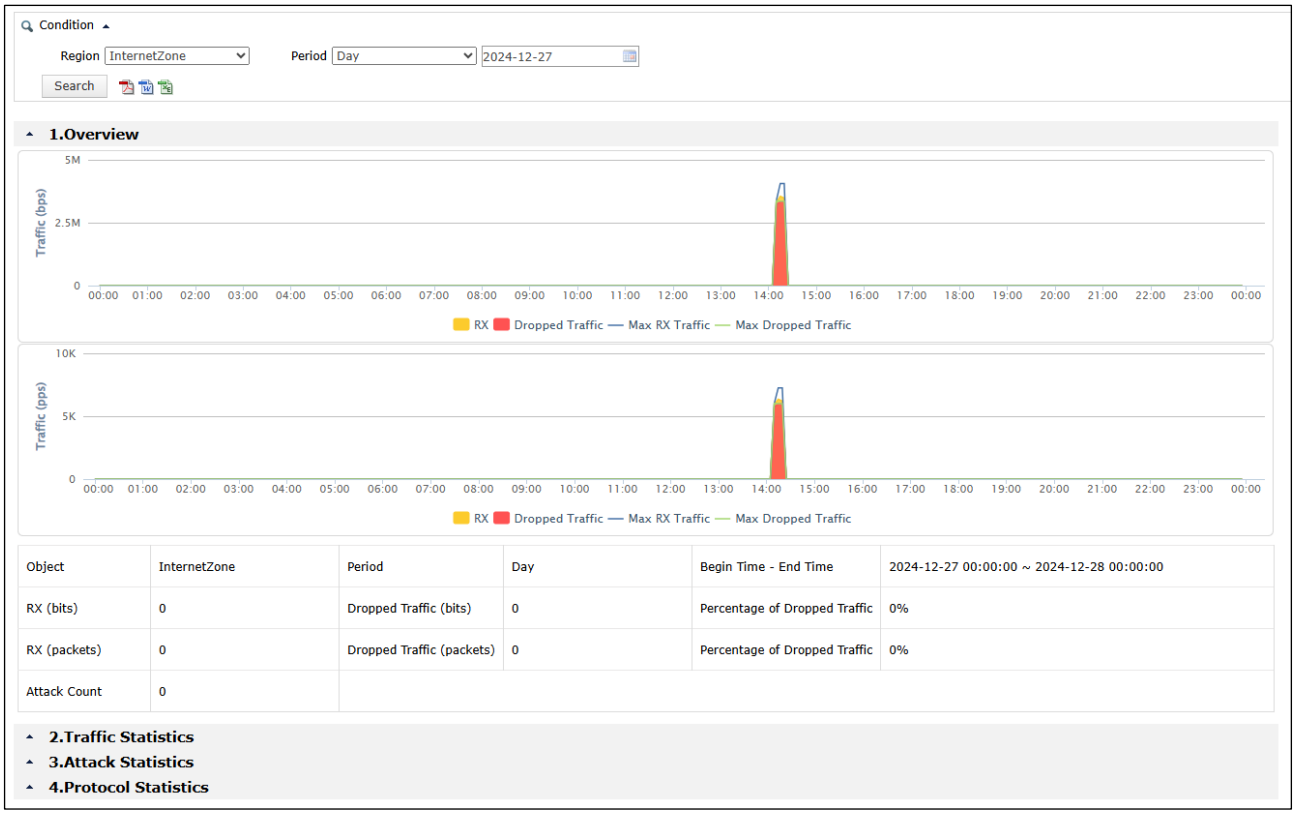


Table 7-4 describes parameters for querying an integrated report.

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**. • **Day**: indicates that traffic data of a specified date (0:00 to 24:00) will be collected. • **Week**: indicates that traffic data of the week (starting from Monday) covering the specified date will be collected. • **Month**: indicates that traffic data of a specified calendar month will be collected. • **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.

Choose **Reports > Attack Summary Report**, as shown in Figure 7-5.

Figure 7-5 Attack summary report

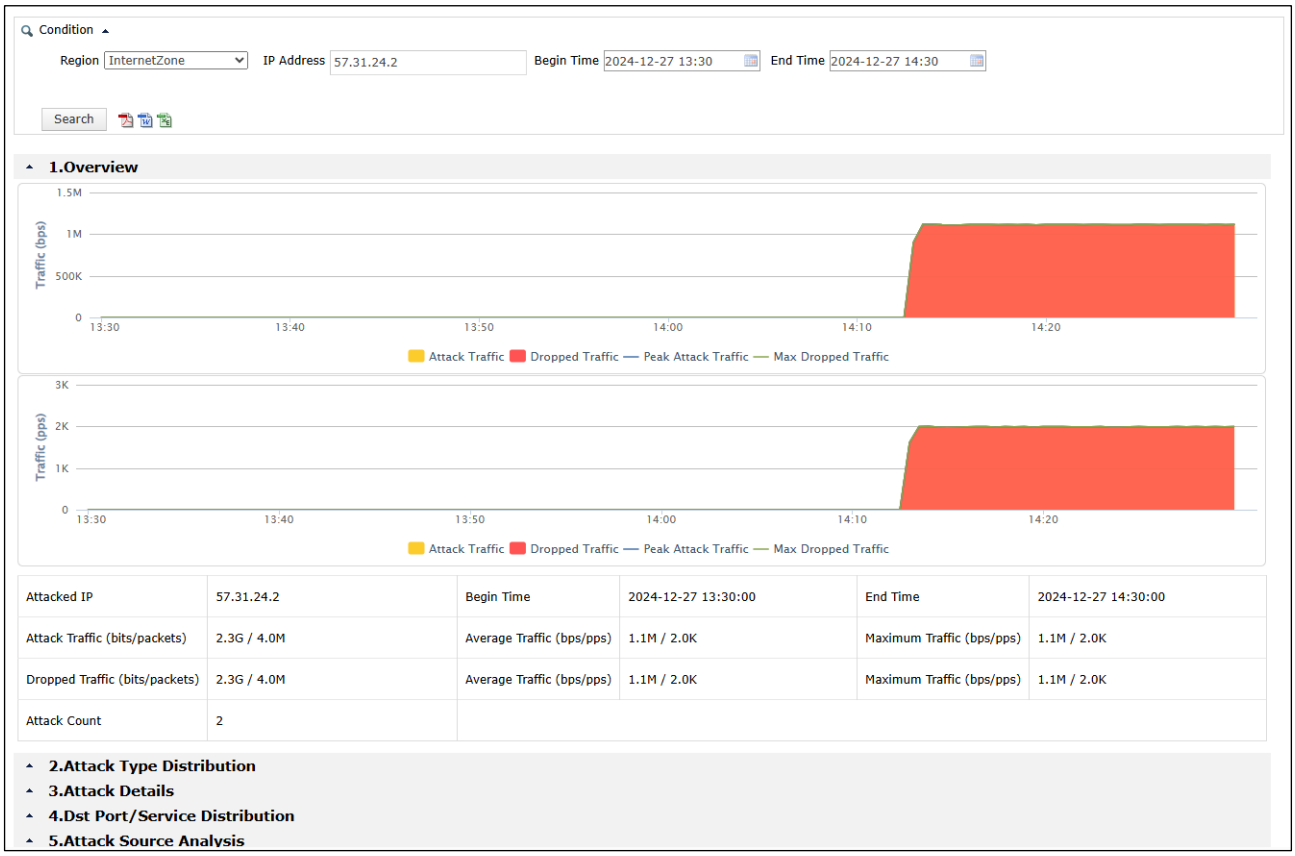


Table 7-5 describes parameters for querying an attack summary report.

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