NSFOCUS NTA

User Guide

Version: V4.5R90F06 (2024-12-26)

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 main functions and usage of the web-based manager of NSFOCUS Network Traffic Analyzer ("NTA" 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 Product Overview	Describes the characteristics, major functions, typical deployment modes, and configuration process of NTA.
2 Initial Configuration	Describes the initial configurations to be completed before the initial login to NTA.
3 Login Management	Describes how to log in to and manage NTA.
4 Administration	Describes how to configure basic settings, network connections, and interfaces to third-party software, how to use diagnosis and analysis tools, and how to manage data and user accounts, import the license, and upgrade the system.
5 Configuration	Describes how to configure monitoring objects, alert templates, global alert parameters, global diversion settings, traffic statistics, the data dictionary, and allowlists.
6 Log Management	Describes how and what to view about various logs.
7 Report Management	Describes how and what to view about various reports generated in real time.
8 Alert Management	Describes how to view alert statistics and details of each log.
9 Monitoring	Describes how to view monitoring information, including regions, IP groups, routers, router interface groups, diversion routing tables, local interfaces, and local status of NTA.
A Abbreviations	Describes acronyms and abbreviations used in this document.
B Default Parameters	Describes default settings of NTA.
C IPv4/IPv6 Support	Describes NTA's module-specific IPv4/IPv6 support.

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.

Convention	Description
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.

Change History

Version	Description
V4.5R90F06	• New functions: network segment-based DDoS detection and network segment-specific diversion policy. • Optimized functions: alert allowlist, NTP server, DDoS attack report, user management, security setting, RADIUS authentication, and license.
V4.5R90F05	• New functions: HTTP slow attack detection, carpet bombing detection, online help, and password + email authentication. • Optimized functions: packet capture, license expiration warning, access control, and alert plugins.
V4.5R90F04SP02	First issue.

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
- Netherlands Toll: +31 85 208 2673 or +31 85 208 2NSF

- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757
- Middle East: +973 1619 7607
- Hong Kong, China: +852 5803 2673 or +852 5803 2NSF
- Macao, China: +853 6825 8594
- Chinese mainland: +86 10 5387 5981

Documentation Feedback

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

Email: info-support@nsfocus.com

1 Product Overview

With the rapid development of Internet technologies, networks are growing in size at an unprecedentedly fast pace, giving rise to more and more applications. The diversity of network applications greatly enriches Internet users' experience. On the other hand, networks are becoming increasingly complex, posing severe challenges to operation and maintenance (O&M) personnel.

On the other side of the fence, cyberattack costs have plummeted thanks to readily accessible attack tools and techniques. As a result, distributed denial-of-service (DDoS) attacks are increasing in both the frequency and destructiveness. These attacks will consume a lot of network resources, potentially causing such severe consequences as mission-critical business being disrupted or the quality of service (QoS) of networks being significantly degraded.

This chapter contains the following sections:

Section	Description
Product Characteristics	Describes outstanding characteristics of NTA.
Typical Deployment	Describes typical deployment modes of NTA.
Configuration Process	Describes the recommended process for configuring NTA.

1.1 Product Characteristics

To address the preceding problems in complex networks, NSFOCUS developed Network Traffic Analyzer (NTA) based on its years of network analysis experience and insight into cybersecurity gained from the research on attacks and defenses. NTA provides an intelligent means of management, enabling network O&M personnel to grasp the real-time network status and immediately discover anomalies and threats. This will help reduce the O&M workload and create a steady and efficient network environment.

NTA is a traffic analysis and detection product based on flow or port monitoring/optical splitting techniques. Oriented towards carrier and data center markets, the product provides real-time monitoring of networks and alerting on attacks and other exceptions. This way, it can well secure customers' network environments.

1.2 Typical Deployment

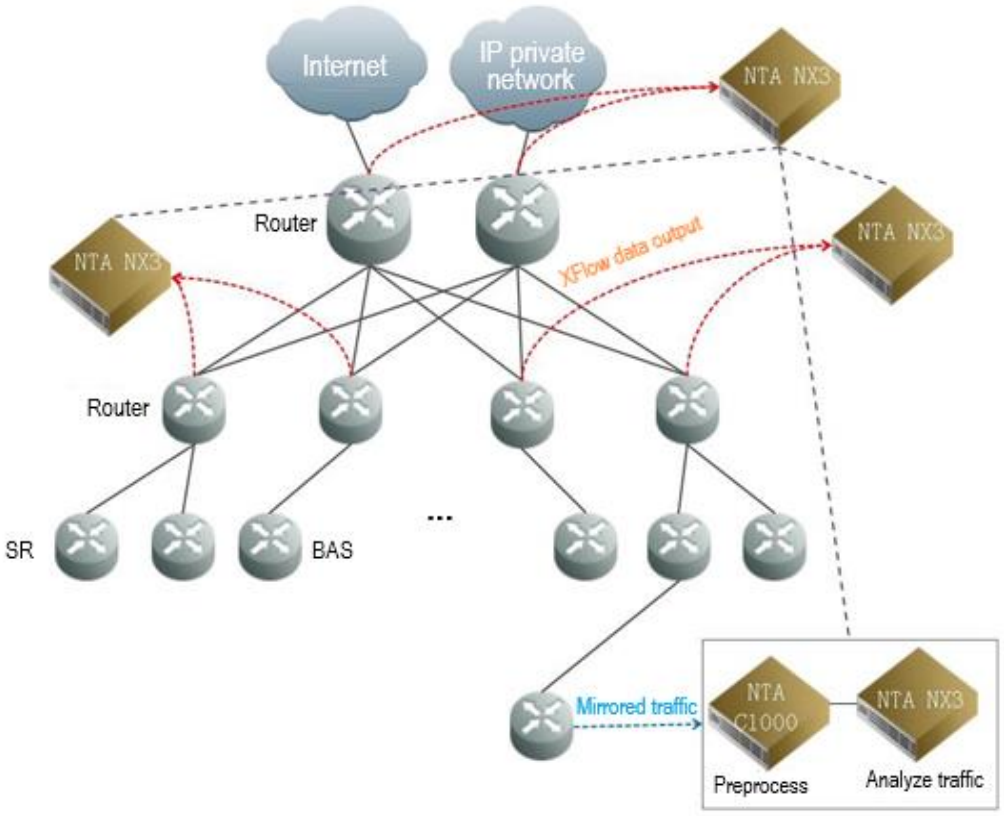
This section describes how to deploy NTA in DFI mode and DPI mode.

1.2.1 Deploying NTA in DFI Mode

When deployed on telecom carriers' metropolitan area networks (MANs) and various private networks, NTA receives flows from core routers for overall statistics and analysis of network traffic. When it comes to networks of large industries and campus networks of large enterprises, O&M personnel need to learn about traffic of egress networks and subnets. For this purpose, an NTA C series device can be deployed to receive mirrored network traffic from each access router and then convert it to NetFlow data for thorough analysis.

Figure 1-1 shows the typical deployment topology of NTA on a carrier's MAN or a large industry's private network.

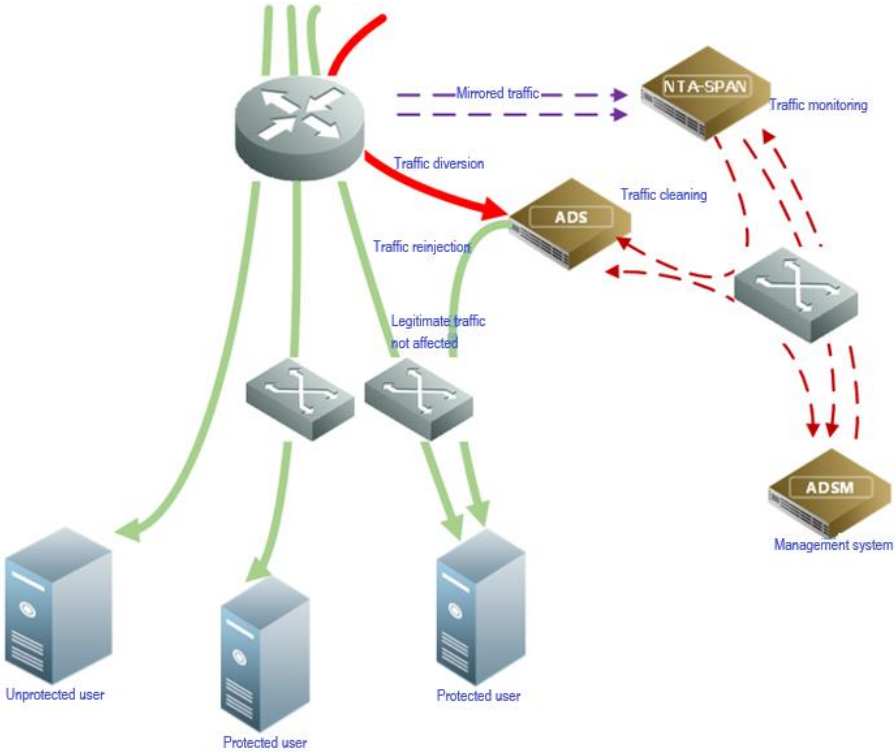
Figure 1-1 Typical deployment topology of NTA in DFI mode



1.2.2 Deploying NTA in DPI Mode

NTA in DPI mode is usually deployed with a scrubbing device cluster to protect MANs and private networks, as shown in Figure 1-2.

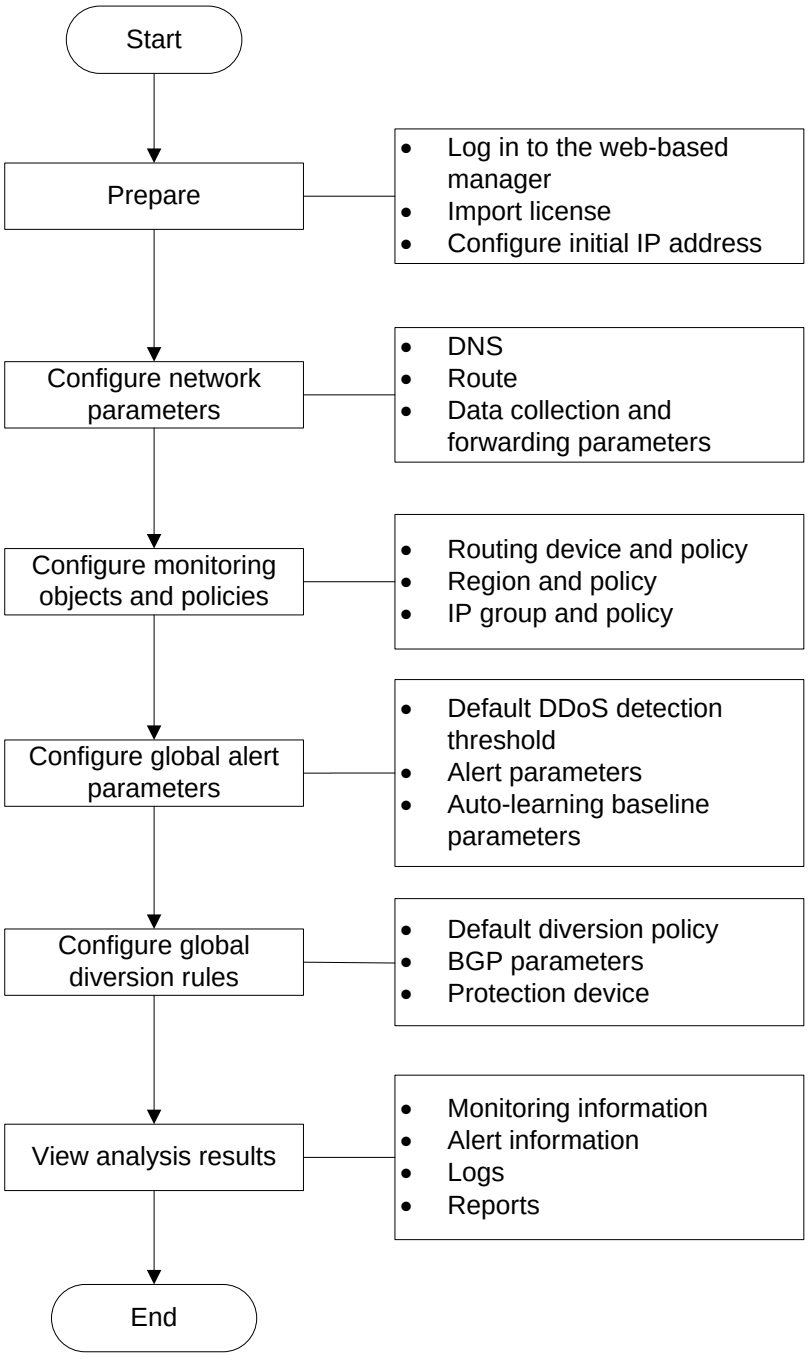
Figure 1-2 Typical deployment topology of NTA in DPI mode



1.3 Configuration Process

Figure 1-3 shows the configuration process of NTA.

Figure 1-3 NTA configuration flow chart



2 Initial Configuration

To use the web-based manager, you must perform initial configuration upon your first login.

This chapter contains the following sections:

Section	Description
Logging In to the Console	Describes how to log in to the console by using a tool.
Configuring the Management IP Address	Describes how to configure the IP address and subnet mask of the management interface of NTA.
Logging In to the Web-based Manager	Describes how to log in to and perform initial configuration on the web-based manager of NTA.
Importing a License	Describes how to import a license.

2.1 Logging In to the Console

For initial use, you need to log in to the console to change the IP address of the management interface.

Before logging in to the console, prepare the following:

- One PC
- One serial cable shipped in the accessory kit
- Terminal software that can connect to the console port, such as SecureCRT.
- NTA connected to the PC with the serial cable

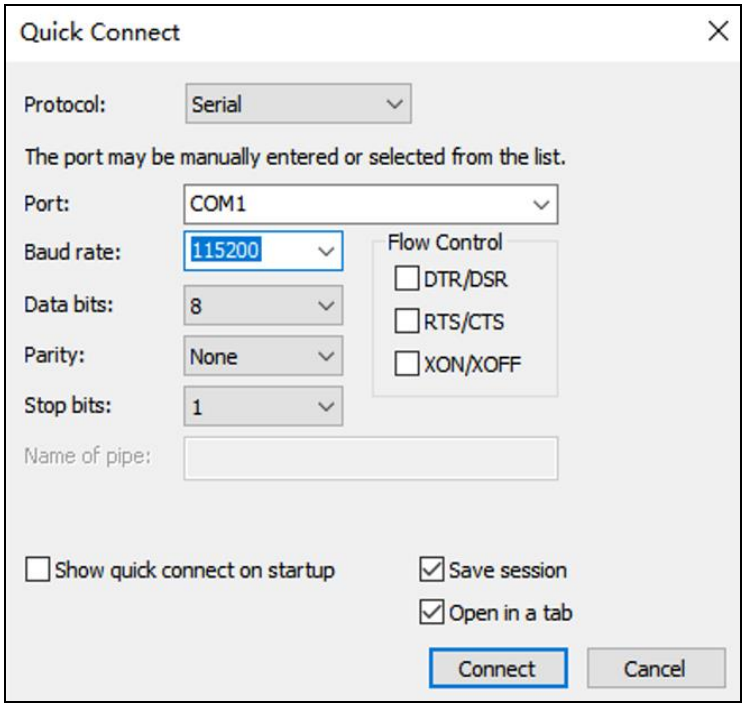
The following takes SecureCRT as an example to describe how to log in to the console user interface of NTA:

Step 1 Click **SecureCRT.exe** to open SecureCRT.

Step 2 Configure quick connection parameters.

Set **Protocol** to **Serial**, **Port** to **COM1**, **Baud rate** to **115200**, and **Data bits** to **8**, and leave other parameters at their default settings.

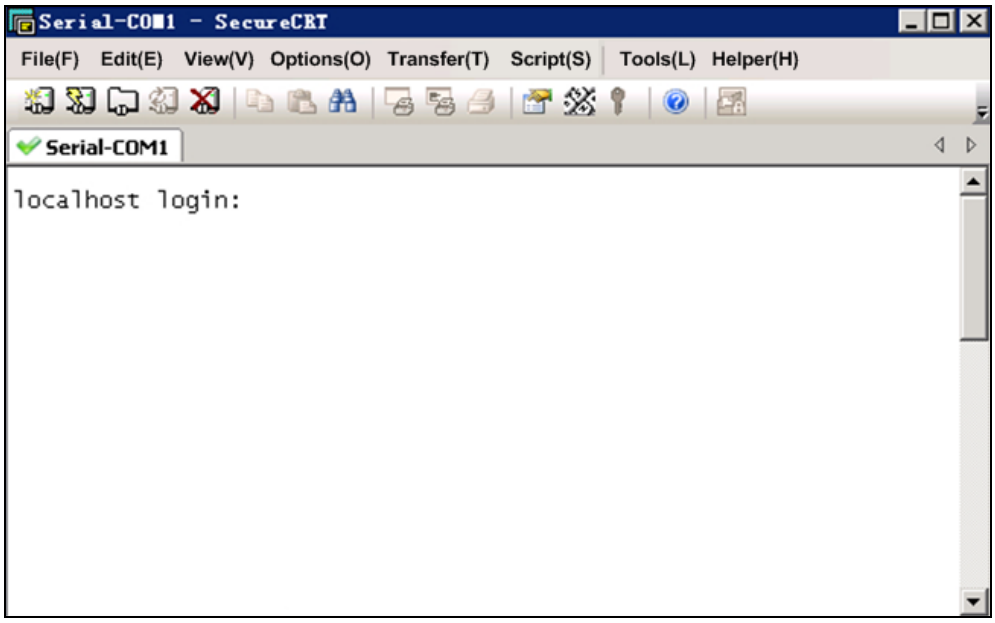
Figure 2-1 Configuring a quick connection



Step 3 Click **Connect**.

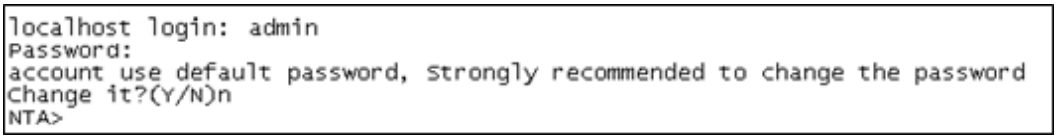
The console login window appears.

Figure 2-2 Login window



Step 4 Type the default user name and password (both are **admin**) to log in to the console.

Figure 2-3 Logging in to the console



Step 5 Change the login password.

Press **Y** and type the new password. The password should consist of at least digits and English letters.

Step 6 Access the unprivileged mode.

For login to NTA via the console port, you are permitted unprivileged access by default, as shown in Figure 2-4. In this mode, you can use only some of the commands.

Figure 2-4 Commands available in unprivileged mode

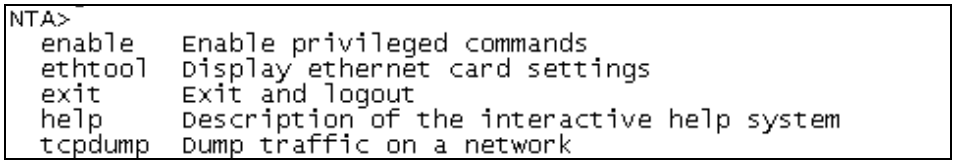


Table 2-1 lists the commands available in unprivileged mode.

Table 2-1 Commands available in unprivileged mode

Command	Description
enable	Enables the privileged mode.
ethtool	Queries and configures Ethernet card settings.
tcpdump	Prints contents of network packets for fast network diagnosis.
help	Displays help information about the use of command lines.
exit	Exits the console user interface.

----End

On the console-based manager, you can only perform operations with the keyboard. Table 2-2 describes meanings of the frequently used keys.

Table 2-2 Meanings of keys for console-based management

Key	Meaning
↑	(1) Switches to the input box. (2) Moves up.
↓	(1) Switches to **OK**. (2) Moves down.
←	(1) Switches to **OK**. (2) Moves left.

Key	Meaning
→	(1) Switches to **Cancel**. (2) Moves right.
Esc	Cancels an operation.
Enter	Confirms an operation.
Tab	Switches between an input box, the **OK** button, and the **Cancel** button.
BackSpace	Deletes the character to the left of the cursor.

2.2 Configuring the Management IP Address

After successful login to the console user interface, you can configure the IPv4 address, subnet mask, and default gateway address for the management interface, as shown in Figure 2-5 and Figure 2-6. After the configuration is complete, you can log in to the web-based manager.

Figure 2-5 Configuring the IP address of the management interface

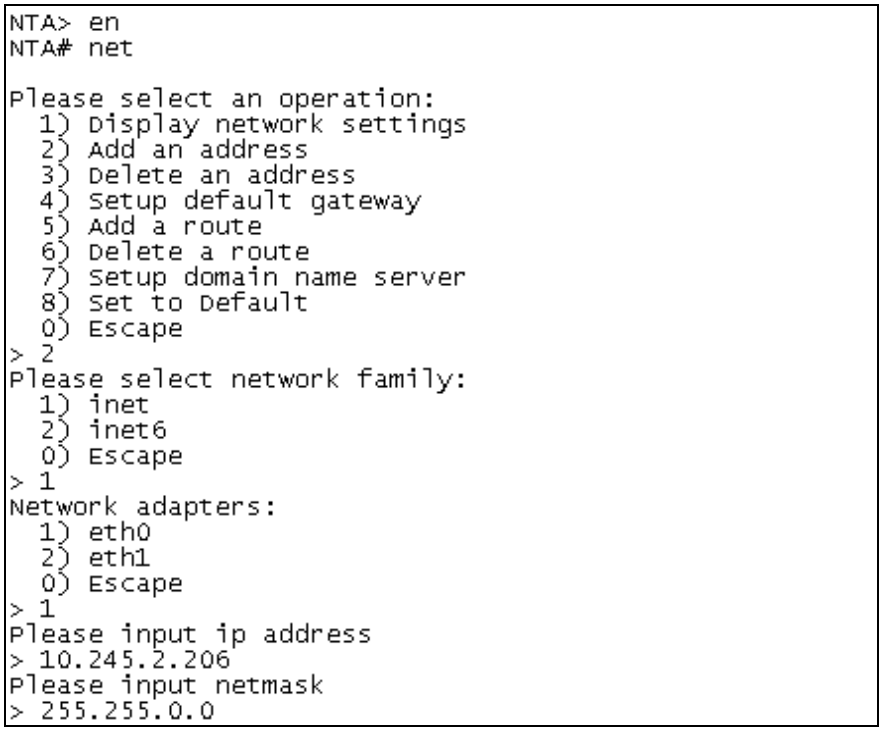


Figure 2-6 Configuring the network gateway of the management interface

```
NTA> en
NTA# net

Please select an operation:
  1) Display network settings
  2) Add an address
  3) Delete an address
  4) Setup default gateway
  5) Add a route
  6) Delete a route
  7) Setup domain name server
  8) Set to Default
  0) Escape
> 4
Please select network family:
  1) inet
  2) inet6
  0) Escape
> 1
Please input default gateway address
> 10.245.255.254
Operation success.
```

2.3 Logging In to the Web-based Manager

Note	• Before login, check whether the options of blocking pop-ups and disabling JavaScript are selected in the browser. If yes, cancel the selections. • You are advised to use the latest Firefox or Chrome browser and set the screen resolution to 1024x768 or higher.

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

Step 1 Make sure that the client communicates properly with NTA (open port 443 if the traffic needs to go through a firewall).

Step 2 Open a browser (Chrome is used here) and connect to the management IP address of NTA over HTTPS, for example, type **https://192.168.1.1** in the address bar.

After you press **Enter**, a security alert appears.

Step 3 Click **Advanced** and then **Proceed to** *IP address* **(unsafe)** to accept the channel secured by the NTA certificate.

The login page shown in Figure 2-7 appears.

Figure 2-7 Login page

Step 4 Type the initial user name and password (both are **admin**), and then click **Log In**.

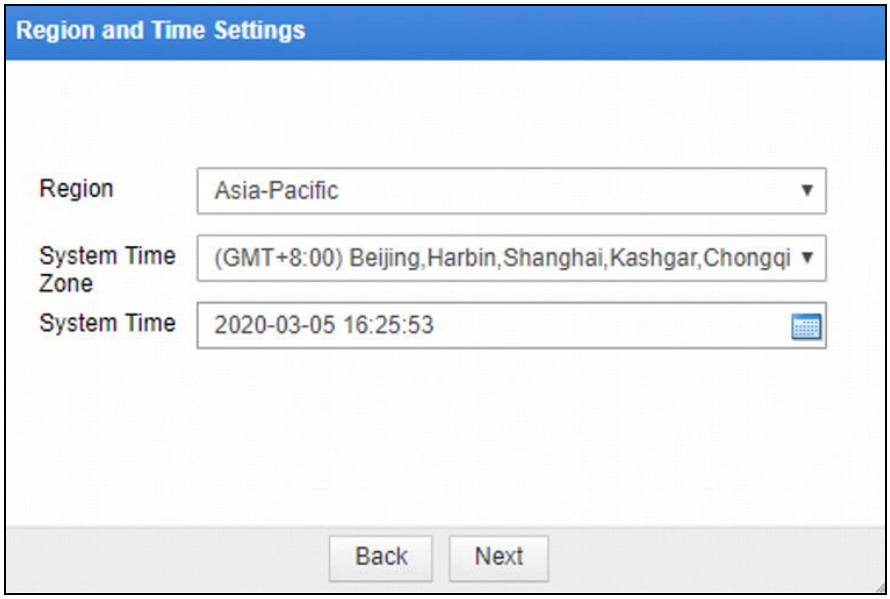
A dialog box shown in Figure 2-8 appears, asking you to select a system language.

Note	• During the first login to NTA that has just been upgraded to V4.5R90F00 or later, you need to set the locality, system time zone, and system time. • 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.

Figure 2-8 Setting the system language

Step 5 Select a language. After the system directs you to the page shown in Figure 2-9, set the locality of the device, time zone, and system time. Then click **Next**.

Figure 2-9 Setting the country/region and time zone



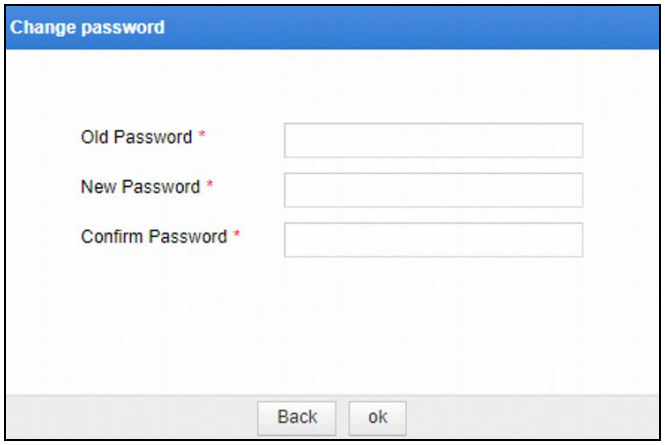
Step 6 Change the initial password.

The page for changing the initial password appears.

The new password must be a string of no less than eight characters and contain at least two of the following character types: English letters, digits, and special characters.

Note	On first login, you are required to change the initial password before performing other operations.

Figure 2-10 Changing the initial password



Step 7 After changing the initial password, click **Submit** to make the settings take effect.

Then you successfully log in to the web-based manager.

----End

2.4 Importing a License

After logging in to an NTA device, you must import a license before using it.

To import a license, perform the following steps:

Step 1 Choose **Administration** > **License**.

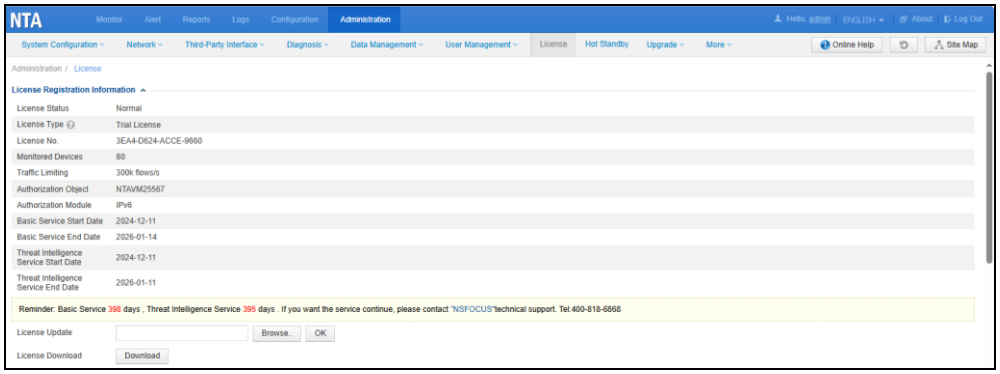
Step 2 Browse to the NTA license file and click **Open**.

Note	To get the NTA license file, please contact NSFOCUS technical support.

Step 3 Click **OK** to import the license.

For details about authorization and authentication, see section 4.7 License.

Figure 2-11 License imported successfully



----End

3 Login Management

This chapter describes three login management modes of NTA, containing the following sections:

Section	Description
Web-based Manager	Describes management through the web-based manager, whose intuitive human-machine interfaces (HMIs) provide all necessary management functions.
Console User Interface	Describes how to configure and manage NTA using command lines via the console.
SSH	Describes how to manage NTA from a remote management client supporting the Secure Shell protocol (SSH).

Note	All NSFOCUS products support web-based management and console-based management, but some may not support management via SSH or other means.

3.1 Web-based Manager

The web-based manager of NTA provides intuitive interfaces for users to manage and configure NTA. The following sections describe the users, login method, and page layout of, and common operations on the web-based manager.

3.1.1 Users

The web-based manager of NTA has different types of user roles: system administrator, configuration administrator, auditor, common user, and custom user. All these roles can log in to the web-based manager. Table 3-1 lists their specific permissions.

For initial user names and passwords, see appendix B.1.3 Default Administrator Accounts.

Table 3-1 Permissions of different roles

Role	Permission
Super administrator (**admin**)	Has the highest permissions and can create user accounts, change account passwords, and perform other configurations.

Role	Permission
System administrator	Has almost the same permissions as **admin**. Specifically, this role can create and manage configuration administrator, auditor, common user, and custom user accounts, but cannot modify information of **admin** and system administrator accounts.
Configuration administrator	Has permissions of configuring business-related settings, such as routers, regions, and policies. Unlike a system administrator, a configuration administrator cannot perform the following operations: • Manage the NTA system, that is, access the Administration module. • View audit logs. • Configure NTI and allowlists.
Auditor	Can only view the local monitoring status and audit logs.
Common user	Unlike a system administrator, a common user cannot perform the following operations: • View routing tables, local interface list, and machine status in the Monitor module. • View audit logs in the Logs module. • Configure any settings in the Configuration module. • Configure any settings in the Administration module.
Custom user	**admin** or a system administrator can grant a custom user access to one or more of the following modules: • Administration: excluding user management and alert allowlist management • Configuration • Logs • Reports • Alert • Monitor

3.1.2 Login

Before logging in to the web-based manager, you must make sure that NTA can properly connect to the network. For details about the login method, see section 2.3 Logging In to the Web-based Manager.

Upon your first login, import a license for proper use of the system. For how to import a license, see section 2.4 Importing a License.

3.1.3 Page Layout

The page layout is the same for all functional modules, as shown in Figure 3-1.

Note	The menus and work area vary with user roles.

Figure 3-1 Page layout

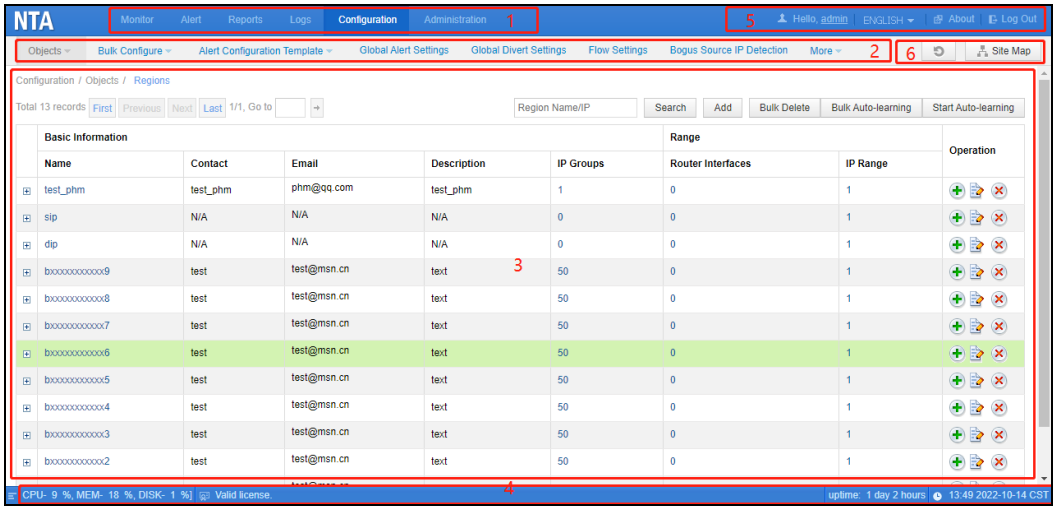


Table 3-2 describes the page layout.

Table 3-2 Page layout

No.	Area	Description
1	Level-1 menu bar	Area of level-1 function menus. Clicking a menu name displays its level-2 functional menu in area 2.
2	Level-2/3 menu bar	Area of level-2 function menus. Pointing to a level-2 menu name displays its level-3 menu (if any).
3	Work area	Area where you can perform configurations and operations and view data.
4	Real-time system status bar	The status bar shows the following information (for more details, see section 9.10 Local Status): • CPU- 3 %, MEM- 6 %, DISK- 1 %]: real-time resource usage of the system. • Valid license.: authorization status of the system. • uptime: 1 day 2 hours: uninterrupted operating hours of the system. • 11:14 2023-09-26 CST: current time and time zone of the system.
5	Quick access bar	The quick access bar provides the following buttons: • Hello, admin : allows you to modify the password, authentiction mode, and other information of the current account. If the web API is enabled, you can also view the access key. Clicking updates the key. Then third-party users must use the new key to access NTA. Clicking to the right of **API Download** saves the API description file to a local disk drive. • ENGLISH: switches the language. Currently, Simplified Chinese

No.	Area	Description
		and English are supported. • About: allows you to view the product version, technical support contacts, end-user license agreement, and other information of NTA. • Log Out: logs you out of the web-based manager.
6	System tool bar	• Clicking Online Help displays online help information of NTA. • Clicking manually refreshes the current page. • **Site Map** lists all level-1 and level-2 menus of NTA. Clicking one level-2 menu name directly opens its page. What menus are shown on the site map depends on permissions of the current user. For details, see section 3.1.1 Users.

3.2 Console User Interface

Through a console port, you can access the console user interface of NTA, which provides certain functions such as initial system configuration, status detection, and restoration of the initial configurations. Functions that cannot be managed on the web-based manager can be managed via the console.

- For the communication parameters of and initial user name and password for access to the console user interface, see appendixes B.1.3 Default Administrator Accounts and B.2 Communication Parameters of the Console Port.
- For how to log in to and perform operations in the console user interface, see section 2.1 Logging In to the Console.

3.3 SSH

In addition to the web-based manager and console, NTA can be remotely managed via software that supports SSH, such as secureCRT or PuTTY.

You should type the correct user name, password, and port number for SSH login. For the first use, you will be forced to change the default password.

Note	• To implement SSH-based management, make sure that the SSH service has been enabled on the system. For details, see section 4.1.1.2 Configuring Remote Management. • For the initial user name and password of the SSH management account, see appendix B.1.3 Default Administrator Accounts.

4 Administration

This chapter describes common operations and methods for system maintenance, containing the following sections:

Section	Description
System Configuration	Describes how to configure the system theme, remote assistance, and basic parameters and import an SSL certificate.
Network Configuration	Describes how to configure a physical interface, static route, DNS server, and bond parameters.
Third-Party Interface	Describes how to configure interfaces for interworking with third-party platforms.
Diagnosis	Describes how to use tools to diagnose NTA and network faults.
Data Management	Describes how to configure automatic disk cleaning and view the usage of each data partition.
User Management	Describes how to configure user accounts, security settings, authentication settings, web API allowlist, and HTTP host allowlist.
License	Describes how to import a license and view the authorization status.
Hot Standby	Describes how to configure the hot standby function based on VRRP.
System Upgrade	Describes how to upgrade the system software, detection rule library, and threat intelligence database.
Access Control	Describes how to configure access control.

4.1 System Configuration

System configuration consists of basic configuration, website customizaton, SSL certificate import, and remote assistance.

4.1.1 Basic Configuration

This section describes how to configure the system time and default language and how to enable or disable services in the system. You can directly shut down the system and restart the system, engines, and web service on the **Basic Information** page.

Choose **Administration > System Configuration > Basic Information**. On the **Basic Information** page, you can configure basic, remote management, and web port management

settings, enable or disable system services, import and export configurations, restart the engines, web service, and system, and shut down the system.

4.1.1.1 Configuring Basic Information

In the **Basic Information** area, click  to edit basic parameters of the system. Table 4-1 describes these basic parameters.

Table 4-1 Parameters for configuring basic information

Parameter	Description
Hardware ID	Indicates the unique identifier of the system, which cannot be edited.
System Time	Specifies the current system time of the built-in clock. You can click  to change the time according to your geographical location.
System Mode	Shows the system mode of the current device. • vNTA: The system mode cannot be edited. • NX3-HD2100/HD2200/HD3000/NX5-HD3500: The system can be switched between the DFI and DPI modes. For the difference between the two modes, see section 4.1.1.4 Configuring System Engines.
System Time Zone	Specifies the time zone of the built-in clock. You can click  to change the time zone according to your geographical location.
NTP Server	Specifies the domain name of the current NTP server. The NTP server can synchronize system clocks to ensure that the time on all devices on the network is the same. You can click  to change the NTP server. You can configure a primary and secondary NTP servers. The time of the secondary server will be used only when the synchronization with the primary NTP server fails.
Clock Source	Specifies the reference clock source for time synchronization of NTA, which can be **NTP Server** or **ADS M**.
Region	• For the selection of **Chinese mainland**, the default NTI server address is **nti.nsfocus.com**. • For the selection of other regions, the default NTI server address is **nti.nsfocusglobal.com**.
Default Language	Specifies the default language of logs. The web-based manager supports Simplified Chinese and English. The default language is **English**. You can click  to change the default language of the system. The change can take effect only after you restart the system.
Device Description	Provides descriptive information of the device to make it easier to identify the device.

4.1.1.2 Configuring Remote Management

NTA can be remotely managed via SSH. You can control whether to enable the SSH service and specify the port number of the SSH service.

Changing the SSH Service Port

The **Remote Management** table shows the current port (**50022** by default) on NTA to provide the SSH service. You can click in the **Operation** column to change the port. After that, the system automatically restarts the SSH service to make the change take effect immediately.

Stopping/Starting the SSH Service

In the **Remote Management** table, you can stop or start the SSH service, depending on the current status of the service:

- The status indicators indicate that the service has been started. To stop the service, click in the **Operation** column. After that, you cannot remotely log in to and configure the current device via SSH.
- The status indicators indicate that the service has been disabled. To start the service, click in the **Operation** column.

4.1.1.3 Configuring the Web Management Port

The **Web Port Management** table shows the current port (**443** by default) used for access to the web-based manager of NTA. You can click in the **Operation** column to change the port. After that, the system automatically restarts the web service.

4.1.1.4 Configuring System Engines

You can view whether a service runs properly, but cannot enable/disable it in the **System Engine** area.

- NTA in DPI mode provides traffic collection, distribution, analysis, and detection, alert management, configuration management, auto-learning, diversion control, and NTP services.
- NTA in DFI mode provides traffic collection, analysis, and detection, alert management, configuration management, SNMP collection, auto-learning, diversion control, and NTP services.

The following indicators or information may be displayed in the **Status** column:

- : indicate that the service has been started.
- : indicate that the service has been disabled.
- **No service**: indicates that the service is currently unavailable.

For how to restart these engines, see section 4.1.1.9 Restarting Engines.

4.1.1.5 Exporting Configurations

Click **System Operation** in the upper-right corner of the page and choose **Export Config**. Then the **Export** dialog box appears, listing configurations that can be exported (clicking shows **Service Configuration** contents). Click **Yes** for configurations that you want to export and then click **Export** to export the selected configurations to a specified directory.

4.1.1.6 Importing Configurations

Click **System Operation** in the upper-right corner of the page and choose **Import Config**. Browse to the configuration file and click **Import**.

Note	• The imported configuration file can take effect only when its NTA version is the same as the current one. • Before configuration import, make sure that the configuration file contains all required parameters; otherwise, file parsing would fail. • The imported configuration file will overwrite the current settings of the system and the engines will automatically restart in the process. Therefore, traffic auto-learning and alerting will also stop functioning.

4.1.1.7 Restarting the System

Click **System Operation** in the upper-right corner of the page and choose **Reboot** to restart the hardware system of NTA from the web-based manager.

4.1.1.8 Shutting Down the System

Click **System Operation** in the upper-right corner of the page and choose **Shutdown** to shut down the hardware system of NTA from the web-based manager.

4.1.1.9 Restarting Engines

Click **System Operation** in the upper-right corner of the page and choose **Restart Engine** to restart all engines of NTA.

4.1.1.10 Restarting the Web Service

After modifying system settings, generally, you are prompted to restart the web server to commit the changes. In this case, click **System Operation** in the upper-right corner of the page and choose **Restart web server** to restart the web service of NTA.

4.1.2 Website Customization

On the **Website Customization** page, you can upload an image as the logo above the title in reports, including traffic reports and DDoS attack reports.

Choose **Administration > System Configuration > Website Customization**, browse to the desired image (for the image format and size, see online tips), and click **OK**. You can preview the logo online.

4.1.3 SSL Certificate Import

Choose **Administration > System Configuration > SSL Certificate Import**, browse to an SSL certificate and configure parameters, and click **OK**. Table 4-2 describes these parameters.

Table 4-2 SSL certificate import parameters

Parameter	Description
Status	Shows the status of the current SSL certificate in the system: • : indicates that the current SSL certificate works properly. • : indicates that the current SSL certificate has expired or no SSL certificate has been installed.

Parameter	Description
SSL Certificate (.crt)	Allows you to import an SSL certificate, which must be a .crt file.
SSL Private Key (.key)	Allows you to import an SSL private key, which must be a .key file.
Private Key Password	Specifies a password for the imported private key.

Note	After the SSL certificate is successfully submitted, an error may be prompted on the page. In this case, refresh the page and allow using the new certificate.

4.1.4 Remote Assistance

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

Choose **Administration > System Configuration > Remote Assistance**. By default, this function is disabled. After manually enabling it, you need to configure related parameters. Then send the generated QR code and key to NSFOCUS technical support for them to remotely log in to the device for troubleshooting when necessary. Table 4-3 describes remote assistance parameters.

Table 4-3 Remote assistance parameters

Parameter	Description
Allowed IP Address	Specifies IP addresses that are allowed remote access to NTA. You can type at most three IP addresses, separated by the comma (,).
Port	Specifies a port for remote access. Leaving it empty indicates any ports. The value range is 1024–65535, excluding 50022 and 22022.

4.2 Network Configuration

The Network module allows you to configure parameters for NTA to connect to other network devices and the Internet.

4.2.1 Configuring a Local Interface

You can configure the IP address of the network interface on NTA. NTA supports IPv4/IPv6 dual stack. As a dual-stack node, NTA allows you to configure both IPv4 and IPv6 addresses. It uses the IPv4 protocol stack for communication with IPv4 nodes and the IPv6 protocol stack for communication with IPv6 nodes. For an interface connecting to a dual-stack network, you must configure both IPv4 and IPv6 addresses.

Note	The dual-stack technology is an effective IPv4-to-IPv6 transition technology. Dual-stack network nodes support both IPv4 and IPv6 protocol stacks. A source node chooses a protocol stack according to the protocol supported by the destination node and a network device does so according to the protocol type of packets when processing and forwarding packets.

Step 1 Choose **Administration > Network > Local Interface**.

Table 4-4 describes parameters on this page.

Table 4-4 Interface attributes

Parameter	Description
Interface Identifier	Indicates the type of an interface, which can be either of the following: • **H** or **M**: configuration interface • *Sa-b*: the bth interface on the ath expansion board, such as **S1-2**
Interface Name	Indicates the name of each physical interface of NTA.
MAC Address	Indicates the MAC address of the physical interface.
Bandwidth	Indicates the maximum physical bandwidth of each interface. When the network connection of an interface is down, its bandwidth is displayed as **Unknown**.
Interface Status	Indicates the status of each interface: • indicates that the network connection of the interface is up. • indicates that the network connection of the interface is down.

Step 2 Configure interface attributes.

a. Click on the left of the interface name.
b. Click **Add** in the IPv4 or IPv6 address area.
c. Type an IPv4 address and subnet mask or IPv6 address and prefix length.
d. Click **OK**.

Step 3 (Optional) Click or in the **Operation** column of an IP address to edit its description or delete it.

----End

4.2.2 Configuring a Route

NTA forwards packets through a static route and default gateway. For this purpose, you must configure a static route and default gateway in advance.

The procedure is as follows:

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

Step 2 Configure a default gateway.

a. A default gateway is the node that NTA uses to forward packets when an IP address does not match any other routes in the routing table.

b. Type an IPv4 or IPv6 address in the **Default Gateway** field and then click **Save**.

Step 3 Configure a static route.

a. Click **Add** and configure parameters in the dialog box. Table 4-5 describes these parameters.

b. Click **OK** to save the settings.

Table 4-5 Parameters for configuring a static route

Parameter	Description
Destination	Specifies the destination address or network of IP packets. You can type an IPv4 address and its subnet mask for an IPv4 route or an IPv6 address and its prefix for an IPv6 route. Note If you want to configure a static route for a network segment, you need to convert the subnet mask into a subnet length, such as 10.20.0.0/24.
Gateway or Next-hop	Specifies the gateway for the static route, usually, the local IP address of the next-hop device.
Interface	Specifies the egress interface of the static route.

----End

4.2.3 Configuring a DNS Server

As an essential and fundamental service on the Internet, the Domain Name System (DNS) service is used to determine the mapping between domain names and IP addresses. As a DNS client, NTA can request the domain name resolution service from a specified DNS server.

Choose **Administration** > **Network** > **DNS Server**, type an IPv4 or IPv6 address, and click **Save**.

You can configure a primary and secondary DNS servers. The secondary server will be used only when the primary DNS server malfunctions.

4.2.4 Configuring a Bond

NIC bonding is a method of grouping two or more physical NICs into a single virtual NIC. This is useful in scenarios that see high throughputs while requiring high network stability.

Choose **Administration > Network > Bond Configuration**, click **Add**, select two interfaces, and click **Save**.

Note	• Currently, only two NICs can be selected for bonding. • If an interface has been configured with an IP address, you should delete this configuration before adding it to a bond. For details, see section 4.2.1 Configuring a Local Interface. • NTA in DPI mode does not support this function.

4.3 Third-Party Interface

The Third-Party Interface module allows you to configure interfaces for communication with other devices.

This section covers the following topics:

- Email Service: describes how to configure a Simple Mail Transfer Protocol (SMTP) server to send alert messages by email.
- SNMP Service: describes how to configure NTA to be managed via SNMP.
- Syslog Service: describes how to configure NTA to dump logs and alerts to a third-party syslog server.
- SFTP Service: describes how NTA dumps status information to a third-party SFTP server.
- Cloud Platform: describes how to configure NTA to collaborate with NSFOCUS ESPP for reports of the latest threats to the latter.
- Third-Party Cloud Platform: describes how to configure NTA to report the latest threats to the configured third-party cloud platform.
- Cloud Cleaning Platform: describes how to configure NTA to report latest threats to the NSFOCUS cloud cleaning platform.
- BSA Configuration: describes how to configure NTA to collaborate with BSA.
- Management Mode: describes how to configure NTA to be managed by ADS M.
- NTA-ATM: describes how to configure NTA to collaborate with NTA-ATM.

4.3.1 Email Service

To configure the email service, you must perform the following tasks:

- Configuring Mail Settings: Configure parameters for sending logs, alerts, and scheduled reports by email.
- Configuring the Email Template: Configure the header and content of the alert email template.
- Configuring an SMTP Server: Configure an SMTP server for sending email messages.

4.3.1.1 Configuring Mail Settings

This involves the following sub-tasks:

- Email alert configuration: configuration of email addresses to which alerts and global diversion notifications will be sent
- Log sending configuration: configuration of log sending conditions and alert filtering conditions
- Scheduled alerting configuration: configuration of parameters for generating and sending alerts in a scheduled manner

The procedure is as follows:

Choose **Administration** > **Third-Party Interface** > **Email Service**. On the **Mail Configuration** page that appears by default, configure email alert and log sending parameters, and click **Save**.

Table 4-6 describes log sending parameters.

Table 4-6 Log sending parameters

Parameter	Description
To	Specifies email addresses that will receive alerts, logs, and global diversion notifications. A maximum of 100 email addresses are allowed, each in a separate line.
Send log mails	Controls whether to enable the function of sending logs that meet specified conditions.
Sending Method	Specifies how log contents are sent. It has the following options: • **Sent in the body**: indicates that logs are sent in the body of the email message. • **Sent in attachment**: indicates that logs are sent in the attachment of the email message. • **Sent in both the body and attachment**: indicates that logs are sent in both the body and attachment of the email message.
Sending Condition	Specifies at least one condition to trigger log emailing: • **By log count**: Logs are sent to the specified email addresses when the number of logs generated reaches the specified value of **Items Count**, which is **200** by default. • **By time**: Logs are sent at an interval to the specified email addresses. The interval can be **5 min**, **15 min**, **30 min** (default), **1 hr**, **3 hr**, **6 hr**, **12 hr**, or **1 day**.
Log Type Filtering	Specifies types of logs to be sent to the specified email addresses: • This is disabled by default, indicating that any type of logs will be sent. • After enabling this, you need to further specify log types (**Alert Log**, **Running Log**, **Diversion Log**, and **Audit Log**) to be sent.
Alert Filtering	Specifies conditions to trigger alert emailing: • **By alert level**: Only alerts of the specified level or above will be sent by email. For example, when **Medium** is specified, alerts of only medium- and high-level risks will be sent. • **By trigger traffic**: Alerts are sent to the specified email addresses only when the traffic reaches the specified threshold in bps.

4.3.1.2 Configuring the Email Template

The email template is used to configure the format of alert messages sent by email. NTA comes with a default email template, which can be modified as required.

Choose **Administration** > **Third-Party Interface** > **Email Service** > **Email Template**, configure parameters (those in blue are editable), and click **Save**.

You can click **Restore Default** to restore settings of the default email template.

Table 4-7 Email template parameters

Parameter	Description
Email subject	Header that applies to all email messages sent by NTA, which is **NTA Log E-mail** by default

Parameter	Description
First line of the email body	Salutation, which is **Hello** by default
Last line of the email body	Contact information
Signature	Sender information

4.3.1.3 Configuring an SMTP Server

An SMTP server can be used for sending alerts by email.

Choose **Administration** > **Third-Party Interface** > **Email Service** > **SMTP Server**, configure parameters, and click **Save**. Table 4-8 describes parameters for configuring an SMTP server.

After configuring an SMTP server, you can click **Send Test Mail** to check whether parameters are correctly configured.

Table 4-8 Parameters for configuring an SMTP server

Parameter	Description
SMTP Server Address	Specifies the IPv4 or IPv6 address or domain name of the server for sending email messages.
Port	Specifies the port number of the SMTP server for sending email messages. The default port is **25**. • When **Secure by SSL** is selected, this value automatically changes to **465**. • When **STARTTLS** is selected, this value automatically changes to **587**.
From	Specifies the email address from which logs are sent.
Authentication Method	Specifies the authentication method, which can be one of the following: • **Secure by SSL**: encrypts SMTP sessions via SSL. • **STARTTLS**: encrypts communication traffic via StartTLS. • **Identity Authentication**: authenticates the sender account based on the user name and password. When this is selected, you can also select **Secure by SSL** or **STARTTLS.**
Username/Password	Specifies the user name and password for sending email messages. The user name is usually the local part of the email address.

When SMTP server settings are being edited, you are not allowed to send a test mail. The **Send Test Mail** button is available only after you complete the editing and save the changes.

4.3.2 SNMP Service

The Simple Network Management Protocol (SNMP) service is used to configure related parameters for NTA to accept management by third-party SNMP software (network management station, NMS). SNMP configuration involves the following sub-tasks:

- Enable and configure the SNMP service on NTA.
- Download the MIB library from NTA and import it to NMSs.
- Configure trusted NMSs.

To configure the SNMP service, follow these steps:

Step 1 Choose **Administration > Third-Party Interface > SNMP Service**.

Step 2 Configure the SNMP service.

NTA can be managed and monitored through SNMPv1, SNMPv2c, or SNMPv3.

a. Configure SNMPv1/v2c parameters.
   - By default, SNMPv1/v2c-based traffic monitoring is enabled on NTA. You can enable or disable this function as required.
   - After SNMPv1/v2c is enabled, you must configure **Community**. The community string configured here must be the same as the read-only community string on the NMS; otherwise, NTA could not communicate with NMS. The default value is **public**.
   - After completing the configuration, click **Save** to commit the settings.

b. Configure SNMPv3 parameters.
   - By default, SNMPv3-based traffic monitoring is disabled on NTA. You can enable or disable this function as required.
   - SNMPv3 supports three authentication methods: **No authentication**, **Account authentication**, and **Private key authentication**. The default value is **No authentication**. For the description of these authentication methods, see Table 4-9.
   - After completing the configuration, click **Save** to commit the settings.

Table 4-9 SNMPv3 authentication methods

Authentication Method	Description
No authentication	Indicates that no authentication is performed. In this case, you need to configure only the user name. For details, see the description of **Private key authentication**.
Account authentication	Indicates that authentication based on HMAC-MD5 or HMAC-SHA is adopted. In this case, the encryption function is unavailable. you need to select an authentication protocol and type the user name and password for this method. For details, see the description of **Private key authentication**.
Private key authentication	Indicates that private key-based authentication is adopted. In this case, data is also encrypted with the Data Encryption Standard (DES) algorithm for transmission, ensuring the privacy of data. For this selection, you need to configure the following parameters: • **Username**: SNMP user name. • **Password**: password for generating the authentication key. • **Authentication Protocol**: specifies an authentication protocol, which can be **MD5** or **SHA**.

Authentication Method	Description
	• **Private Key Protocol**: specifies a private key protocol, which can be **DES** or **AES**. • **Private Key Password**: password for generating a private key for encryption and decryption protocols.

Step 3 Download the MIB library.

a. Click **Download MIB Library** and **Download SNMP Description Document** to download the corresponding document to a local disk drive.

b. To manage and monitor NTA, you must download the MIB library from NTA and then import it to NMS configured in step 4.

Step 4 Configure a trusted NMS.

After the SNMP service is enabled on NTA, it does not mean that NTA will accept management from all NMSs. Actually, NTA accepts management only from trusted NMSs. For this purpose, you need to configure a list of trusted NMSs to:

- Put NTA under management of these NMSs.
- Allow or not allow NTA to send trap messages to a specified NMS.
- Allow or not allow NTA to accept GET requests from a specified NMS.

Note	You also need to import the MIB library of NTA to NMSs so that NMSs can obtain NTA's basic information via the GET method and receive trap messages from NTA.

Click **Add**, configure NMS parameters, and click **OK**.

Table 4-10 describes NMS parameters.

Table 4-10 Parameters for configuring a trusted NMS

Parameter	Description
Host IP	Specifies the IP address of the trusted NMS.
Port	Specifies the port of the trusted NMS. The value range is 1–65535.
Allow Get	Controls whether to allow this NMS to obtain product information and performance information, such as CPU usage, memory usage, and disk usage, of NTA by using the GET method. If you need to use the OID value of NTA, contact NSFOCUS technical support.
Allow Trap	Controls whether NTA automatically sends trap messages to NMS. After this is enabled, NTA automatically sends a trap message when a log is generated.
Trap Type	Specifies the types of logs that NTA automatically sends to the NMS via trap messages. Options include **Alert Log**, **Running Log**, **Diversion Log**, **Audit Log**, and **System Uptime**. This parameter can be configured only when the Allow Trap check box is selected.

Parameter	Description
	After this parameter is configured, NTA will automatically send a trap message when a log of a specified type is generated.  Note You need to specify data sources after **Alert Log** is selected. The data source can be **Global** and/or **Region/IP Group**. **Global** indicates alerts involving destination IP addresses not belonging to any region or IP group.

----End

4.3.3 Syslog Service

On NTA, certain logs can be dumped to a syslog server. For this purpose, you must configure a syslog server and specify the types of logs to be dumped in advance.

Choose **Administration > Third-Party Interface > Syslog Service** and click **Download Syslog Description Document** to download the corresponding document to a local disk drive for reference in the case of adding a syslog server. Click **Add** and configure parameters.

Table 4-11 describes syslog server parameters.

Table 4-11 Parameters for configuring a syslog server

Parameter	Description
Server Address	Specifies the IP address of the syslog server.
Protocol	Specifies the protocol type that the syslog server uses to provide the service, which can be **udp** or **tcp**.
Destination Port	Specifies a port for the syslog server to receive logs. The default port is **514**.
Syslog Type	Specifies the types of logs to be dumped to the syslog server. You must select at least one type.
Alert Level	Specifies which levels of alert will be sent to the syslog server. This field can be configured only when **Syslog Type** is set to **Alert Logs**.
User-defined Field	Specifies the custom contents to be sent to the syslog server.

4.3.4 SFTP Service

After the SFTP service is configured and enabled, the background program of NTA will automatically send status information to the specified SFTP server.

Choose **Administration > Third-Party Interface > SFTP Service** and configure parameters.

Table 4-12 describes SFTP service parameters.

Table 4-12 Parameters for configuring the SFTP service

Parameter	Description
Enable	Determines whether to enable the SFTP service. You can configure its parameters only after enabling the service.
Server Address	Specifies the IP address of the SFTP server. Only IPv4 addresses are allowed here.
Port	Specifies the port used by the SFTP server to receive status information.
Username/Password	Specifies the user name and password used for login to the SFTP server. This account must have the read/write access to the SFTP server.
Upload Path	Specifies the directory on the SFTP server where the received status information is stored. If the root directory is used to save logs, type /.

4.3.5 Cloud Platform

After the cloud platform is enabled and NSFOCUS ESPP is configured, the background program of NTA will automatically upload log files (including alerts and performance information) to ESPP as long as NTA can properly connect to the latter. Upon detection of a problem with NTA, ESPP immediately notifies the technical support personnel, thereby guaranteeing the security of customers' networks.

Choose **Administration > Third-Party Interface > Cloud Platform**. When NTA properly connects to a cloud platform, the indicator on the right of the IP address is green; otherwise, it is red. Configure cloud platform parameters.

Table 4-13 describes cloud platform parameters.

Table 4-13 Parameters for configuring a cloud platform

Parameter	Description
Enable	Controls whether to enable NTA to connect to ESPP.
ESPP Address *X*	Specifies the IP address or domain name of ESPP that can properly communicate with NTA. For the IP address of ESPP, contact NSFOCUS technical support.

4.3.6 Third-Party Cloud Platform

After the third-party cloud platform is configured and enabled, the background program of NTA will automatically uploads log files (including alert and performance information) and traffic data to the third-party cloud platform as long as NTA properly connects to this platform.

Choose Administration > Third-Party Interface > Third-Party Cloud Platform and click **Download Third-Party Cloud Platform User Guide** to download the corresponding document to a local disk drive for reference in the case of adding a third-party cloud platform. Click **Add** and configure parameters.

Table 4-14 describes third-party cloud platform parameters.

After such a platform is added, it can be modified and deleted.

Table 4-14 Parameters for configuring a third-party cloud platform

Parameter	Description
Enable	Controls whether to enable NTA to connect to the third-party cloud platform.
Upload Protocol	Specifies the protocol for uploading data. Options include **HTTP** and **HTTPS**.
Upload Path	Specifies the URL of the third-party cloud platform.
Data Type	Specifies the types of data to be uploaded to the third-party cloud platform.
Data Source	Specifies data sources of DDoS alerts. It has the following values: • **Global**: uploads DDoS alerts from all possible sources. • **Region/IP Group**: uploads DDoS alerts only from regions and IP groups. Note Use of global sources may overload the third-party system with too much data.
Description	Brief description of the third-party cloud platform.

4.3.7 Cloud Cleaning Platform

After the cloud cleaning platform is configured and enabled, the background program of NTA will automatically uploads log files (including alert and performance information) and traffic data to the cloud cleaning platform as long as NTA properly connects to this platform.

Choose **Administration > Third-Party Interface > Cloud Cleaning Platform**, click **Add**, and configure parameters.

Table 4-15 describes cloud cleaning platform parameters.

After such a platform is added, it can be modified and deleted.

Table 4-15 Parameters for configuring a cloud cleaning platform

Parameter	Description
Enable	Controls whether to enable NTA to connect to the cloud cleaning platform.
IP	Specifies the IP address of the cloud cleaning platform that can properly communicate with NTA. For the IP address of the cloud cleaning platform, contact NSFOCUS technical support.
Port	Specifies the port used by the cloud cleaning platform to connect to NTA. The value range is 1–65535. For the port of the cloud cleaning platform, contact NSFOCUS technical support.
Send Syslog	Controls whether to send logs via syslog. This function is disabled by default. After enabling this, you need to further specify the destination port. Currently, syslog messages can be sent only via UDP.
Description	Brief description of the cloud cleaning platform.

4.3.8 BSA Configuration

After NSFOCUS Big Data Security Analytics Platform (BSA) is configured and enabled, the background program of NTA will automatically uploads log files (including alert and performance information) to BSA as long as NTA properly connects to BSA.

Choose **Administration > Third-Party Interface > BSA Configuration** and configure parameters.

Table 4-16 describes BSA parameters.

Table 4-16 BSA configuration parameter

Parameter	Description
Enable	Controls whether to enable NTA to connect to BSA.
BSA Address X	Specifies the IP address of BSA that can properly communicate with NTA. For the IP address of BSA, contact NSFOCUS technical support.
File Port	Port for transmitting files to NTA.
Log Port	Port for transmitting logs to NTA.
translocalhost	When BSA works in a NAT environment, this parameter is set to **127.0.0.1**; otherwise, it is set to the IP address that BSA uses to collaborate with NTA.

4.3.9 Management Mode

When used for abnormal traffic detection, NTA can be managed by NSFOCUS ADS M to provide real-time traffic monitoring for traffic cleaning objects.

- At most five ADS M devices of V4.5R90F06 can be added.
- The management password specified must be the same for all ADS M devices.

Choose **Administration > Third-Party Interface > Management Mode**, click **Add**, and configure parameters.

Table 4-17 describes ADS M parameters.

After an ADS M device is added, it can be modified and deleted.

Table 4-17 Parameters for configuring ADS M

Parameter	Description
Enable device	Controls whether to enable NTA to connect to ADS M. Initially, this is disabled. You need to click **Yes** to enable this function.
ADS M Address	Specifies the IP address of ADS M, which can be an IPv4 or IPv6 address.
Port	Specifies the port used by ADS M to connect NTA.

Parameter	Description
Management Password	Specifies a password for authentication of ADS M. This password must be the same on both sides.

4.3.10 NTA-ATM

NTA-ATM stands for NSFOCUS Network Traffic Analyzer–Attack Trend Monitoring System. NTA can collaborate with NTA-ATM, which obtains data from NTA in an unsolicited manner to inform administrators of the attack situation in the network, making security O&M easy and convenient. For this purpose, you need to configure parameters on both NTA and NTA-ATM. Here only the method of configuring related parameters on NTA is described. For the configuration method on NTA-ATM, see the *NSFOCUS NTA-ATM User Guide*.

Choose **Administration > Third-Party Interface > NTA-ATM** and configure synchronization parameters.

Table 4-18 describes parameters for synchronizing data to NTA-ATM.

Table 4-18 Parameters for configuring synchronization with NTA-ATM

Parameter	Description
Synchronization Mode	Specifies the synchronization mode. It has the following values: • **Scheduled**: indicates that data is synchronized between NTA and NTA-ATM every 5 minutes. • **Real-time**: indicates that data is synchronized between NTA and NTA-ATM every 30 seconds.
NTA-ATM Address *X*	Specifies the IP address of NTA-ATM that can properly communicate with NTA. At most three IP addresses can be configured. For the IP address of NTA-ATM, contact NSFOCUS technical support.
File Port	Specifies a port for transmission of files to NTA-ATM for real-time synchronization.
Log Port	Specifies a port for transmission of logs to NTA-ATM for real-time synchronization.
translocalhost	When NTA-ATM works in a NAT environment, this parameter should be set to **127.0.0.1**; otherwise, it should be the IP address of NTA-ATM.

4.4 Diagnosis

NTA provides basic diagnostic tools for users to troubleshoot network faults.

Choose **Administration > Diagnosis > ping/traceroute/snmpwalk/pcap/tcpdump/telnet/fault diagnosis**. You can select an appropriate tool to check the network connectivity between the system and the destination. Table 4-19 describes how to use these tools.

Table 4-19 Diagnostic tools

Tool	Parameter	Usage
ping	• **ping**: Type the IPv4 address of the destination. • **ping6**: Type the IPv6 address of the destination and select the corresponding network interface.	Checks the connectivity between the system and the destination host, the response time, and whether domain names are correctly resolved.
traceroute	• **traceroute**: Type the IPv4 address of the destination. • **traceroute6**: Type the IPv6 address of the destination and select the corresponding network interface.	Displays the path that a packet takes to the destination host and the time when it reaches each node.
snmpwalk (DFI mode)	Select a router and specify the object identifier (OID), which can be **Device Name**, **Device Description**, or **Custom**.	Obtains values of MIB objects on a router.
pcap (DPI mode)	Click **Packet Capture** and configure parameters to capture matching packets and save related data as .cap files. For the description of parameters, see Table 4-20. After a packet capture task is completed, you can download and delete its related file. Packet capture files of ongoing tasks cannot be deleted.	Intercepts and analyzes packets being transmitted over a network as defined by a user. The user can check the status of and troubleshoot NICs based on such analysis.
tcpdump (DFI mode)	Click **Packet Capture** and configure parameters to capture matching packets and save related data as .cap files. For the description of parameters, see Table 4-21. After a packet capture task is completed, you can download and delete its related file. Packet capture files of ongoing tasks cannot be deleted.	Intercepts and analyzes packets being transmitted over a network as defined by a user.
telnet	• **IP Address**: Type an IPv4 or IPv6 address. • **Port**: Type the port number corresponding to the specified IP address.	When NTA collaborates with or sends data to other devices, Telnet is used to check whether the peer port is reachable, checking whether a firewall is configured or whether a certain service is disabled on the peer device.
fault diagnosis	Click **Start Collecting** to collect fault information. The progress and details of fault collection will be displayed on the page. After the task is complete, you can download and delete the related file.  NTA can store up to three fault information files. If three files already exist in the system, newly collected information files will overwrite the earliest file.	NTA allows one-click fault collection and upload of encrypted fault information. NSFOCUS technical support can locate and troubleshoot faults according to the collected data.

Table 4-20 PCAP parameters

Parameter		Description
Service	Type	Specifies the type of packets to be captured. Options include **All**, **TCP**, **UDP**, **ICMP**, and **ICMPv6**.
	Max Packet Count	Maximum number of packets to be captured, ranging from 1 to 30000.
	Source IP	Specifies the source IPv4 or IPv6 address of packets to be captured.
	Destination IP	Specifies the destination IPv4 or IPv6 address of packets to be captured.
	Source/Destination IP	Specifies the source or destination IP address of packets to be captured. After this is specified, the preceding two values are ignored.
	Interface	Specifies an enabled network interface from which packets will be captured.
	Sampling Rate	Specifies the ratio of matched packets to captured packets. Value range: 1–65535. For example, the value **1000** indicates that one in 1000 packets is captured. The default value is **1**, indicating no sampling. When the traffic bursts, the packet sampling ratio allows the device to capture packets in a longer period.
System	Protocol	Specifies the protocol of packets to be captured. Options include **All**, **TCP**, **UDP**, and **ICMP**.
	Port	Specifies the transport-layer port from which packets will be captured. The value range is 0–65535. The value **0** indicates no limit.
	Max Packet Count	Maximum number of packets to be captured, ranging from 1 to 10000.
	Host IP	Specifies the destination IPv4 or IPv6 address of packets to be captured. Leaving it empty indicates any IP addresses.
	Interface	Specifies an enabled network interface from which packets will be captured.

Table 4-21 Tcpdump parameters

Parameter		Description
Pattern 1	Type	Specifies the type of packets to be captured. Options include **All**, **Netflow**, **NetStream**, **IPFIX**, **sFlow**, **SNMP**, and **BGP**.
	Device	Specifies a device from which packets will be captured. The value **Any** indicates that the system will automatically select a device to capture packets from it. For how to configure such a device, see section 5.1.1.1 Configuring a Router.
	Max Packet Count	Maximum number of packets to be captured, ranging from 1 to 10000.
	Interface	Specifies an enabled network interface from which packets will be captured.
Pattern 2	Protocol	Specifies the protocol of packets to be captured. Options include **All**, **TCP**, **UDP**, and **ICMP**.
	Port	Specifies the transport-layer port from which packets will be captured. The

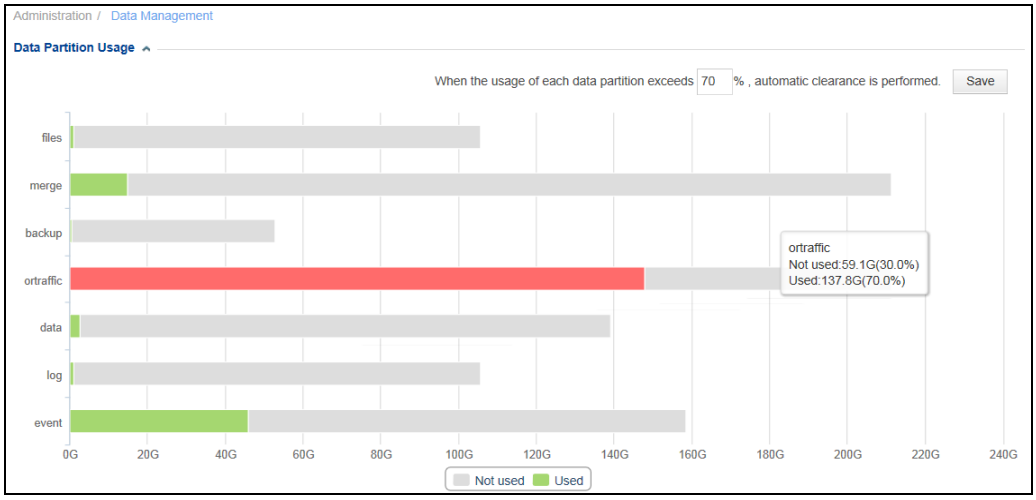
Parameter		Description
		value range is 0–65535. The value **0** indicates no limit.
	Max Packet Count	Maximum number of packets to be captured, ranging from 1 to 10000.
	Host IP	Specifies the destination IPv4 or IPv6 address of packets to be captured. Leaving it empty indicates any IP addresses.
	Interface	Specifies an enabled network interface from which packets will be captured.

4.5 Data Management

The Data Management module allows you to learn the usage of data partitions in the NTA system in real time. You can specify a threshold for the partition usage. When the actual partition usage exceeds the threshold, NTA automatically cleans the disk. This effectively prevents data loss caused by insufficient disk space.

Choose **Administration > Data Management > Data Partition**. The **Data Partition** page displays the usage of all partitions, as shown in Figure 4-1.

Figure 4-1 Data Partition Usage page



Setting the Automatic Disk Cleaning Threshold

At the upper right of the page, you can set a threshold (**70%** by default) for the partition usage. When the actual usage exceeds the threshold, the bar in the chart turns red and the system automatically cleans expired data.

Viewing the Partition Usage

The used space and available space of all data partitions are both displayed by default. If the usage of a data partition is represented by a red bar, it indicates that the usage has exceeded the threshold. Clicking a legend item hides or displays usage statistics of that type. Hovering

the mouse over a bar of the graph shows specific figures concerning usage of the corresponding data partition.

4.6 User Management

In the User Management module, you can manage accounts and set login parameters.

4.6.1 Managing User Accounts

Choose **Administration > User Management > Account Configuration**. The account list contains the default account **admin**, which can create and manage other accounts.

Creating an Account

Click **Add** and configure parameters.

Table 4-22 describes parameters for configuring an account.

Table 4-22 Parameters for configuring an account

Parameter	Description
Username	User name of the new account, which must be a string of 4 to 20 English letters, digits, underscores, and/or hyphens (-).
Password/Confirm Password	Password of the new account, the minimum length of which depends on the **Minimum Length** value specified under **Administration > User Management > Security Configuration**. You need to type the password twice to ensure its correctness.
Email	Valid email address. It is an optional parameter.
Description	Brief description of the new account. It is an optional parameter.
User Group	Specifies a group to which the new account will belong to control the user permissions. Options include **System administrator**, **Configuration administrator**, **Auditor**, **Common user**, and **Custom-permission user**. The user **admin** can create any type of accounts, but a common system administrator can create only configuration administrators, auditors, and common users.
Access Key	Controls whether to enable the key for third-party access to NTA through the web API. After this is enabled, the user accessing the web-based manager of NTA with the new account can view the specific key after clicking Hello in the quick access bar.
Authenticate By	Specifies the login authentication method, which can be **Password** or **Password and email**. Password: The new account can log in to NTA after typing the correct user name and password. Password and email: The new account can log in to NTA after typing the correct user name, password, and the verification code provided via email. Note For the Password and email authentication, you need to type a correct email address.

Editing an Account

You can edit the default user (**admin**) and custom users.

Click  in the **Operation** column of a user to edit the user's account information. Only **admin** can edit user accounts and other users can only change their own passwords. Changing the password will refresh the enabled access key.

Rename the default user (**admin**) with caution. If you forget the new name, you have to restore it along with its password to the default through the console. For details, see section 2.1 Logging In to the Console.

Deleting an Account

In the account list, click  in the **Operation** column of an account to delete this account. The default account **admin** cannot be deleted. In addition, only the default account admin can delete an account.

Disabling an Account

The default account cannot be disabled. Only newly created accounts can be disabled, which must be performed by a system administrator. After being disabled, an account cannot be used for login to the web-based manager of NTA.

In the account list, click  in the **Operation** column of an account to disable this account.

Enabling an Account

After disabling an account, **admin** can reenable it so that this account can be used for login to the web-based manager of NTA again.

In the account list, click  in the **Operation** column of an account to enable this account.

4.6.2 Configuring Security Settings

Security settings ensure the security of local accounts through login authentication. However, local security settings do not take effect for RADIUS, TACACS+, and LDAP authentication., whose settings on the corresponding servers prevail.

Choose **Administration** > **User Management** > **Security Configuration** and configure parameters.

Table 4-23 describes security configuration parameters.

Table 4-23 Security configuration parameters

Parameter	Description
Idle Timeout	Specifies the time for NTA to keep the session alive in the absence of any operation before logging you out to ensure account security. The default value is **10** minutes.
Limit of Failed Password Attempts	Specifies the maximum number of consecutive login failures that are allowed before a specified action is taken against the account.

Parameter	Description
	The value is an integer in the range of 3–20, with **3** as the default value.
Action After Limit Is Exceeded	Specifies an action taken against the account after the **Limit of Failed Password Attempts** is exceeded. It has the following values: • **Return result after 3s**: returns error information. This is the default action. • **Lock client IP**: locks the IP address of the client for a specified period before allowing users to log in again from this IP address. The lockout time is 1–60, in minutes, with 20 as the default. • **Lock account**: locks the account for a specified period before allowing users to log in again with this account. The lockout time is 1–60, in minutes, with **20** as the default.
Use Verification Code	Controls whether to use verification codes to authenticate user login. • **Yes**: enables use of verification codes so that a user can successfully log in to NTA only after typing a correct verification code. • **No**: disables use of verification codes for login authentication.
Email Verification Code Timeout	Specifies the allowed maximum period during which the email verification code is effective. The value range is 1–60, in minutes, with 1 as the default. After this period, the verification code expires. You need to obtain a new one via email and use it for the login to NTA.
Web Access Control List	Specifies IP addresses from which users are or are not allowed to access NTA. It has the following values: • **No Limit**: no limit to source IP addresses. • **Allow Access from the Following IP Addresses**: allows user access to NTA from the specified IP addresses. • **Block Access from the Following IP Addresses**: denies user access to NTA from the specified IP addresses. The default value is **No Limit**.
Validity	Specifies a period for a login password to remain valid before the system pops up a dialog box for you to change the password. The value range is 0–365, with **365** as the default value and **0** indicating no limit.
Minimum Length	Specifies the minimum length of a login password. The default value is **8**.
Strength	Specifies the complexity of a login password. It has the following values: • **All**: no requirement for the setting of passwords. This is the default value. • **Necessary parts**: specifies what types of characters must be contained in a password. You can select **Uppercase letter**, **Lowercase letter**, **Digit**, and/or **Special Characters**.
Password Dictionary	Specifies character strings that cannot be used as passwords. It is empty by default.

4.6.3 Configuring Authentication

Accounts can be authenticated based on a local database or a third-party authentication server, including RADIUS, TACACS+, and LDAP authentication servers.

Note	No matter which authentication method is used, you need to configure a user account on NTA. When RADIUS, TACACS+, or LDAP authentication is selected, the account created on NTA must have the same user name and password as those specified on the authentication server. For account configuration, see section 4.6.1 Managing User Accounts.

Choose **Administration** > **User Management** > **Authentication Configuration** and configure authentication parameters.

Table 4-24 describes authentication parameters.

Table 4-24 Authentication parameters

Parameter		Description
Authentication Method		Specifies an authentication mode, which can be **Local**, **RADIUS**, **TACACS+**, or **LDAP**. Local authentication is the default authentication method. If this is selected, no other parameter needs to be configured.
RADIUS	Authentication Server	Specifies the IP address of the RADIUS server.
	Authentication Port	Specifies the port that the RADIUS server uses to provide authentication.
	Protocol	Specifies the protocol used for authentication, which can be any of the following: • **pap**: Password Authentication Protocol • **chap**: Challenge Handshake Authentication Protocol • **spap**: Shiva Password Authentication Protocol • **mschapv1**: Microsoft Challenge Handshake Authentication Protocol version 1 • **mschapv2**: Microsoft Challenge Handshake Authentication Protocol version 2
	Shared Key	Specifies the password provided for NTA authentication for its access to the RADIUS server. NTA and the RADIUS server can receive packets from each other and respond accordingly only when the key configured here is the same as that on the RADIUS server.
	Authentication Hold-in Time	Specifies the time for NTA to keep attempting to connect to the RADIUS server. The value range is 5–60 seconds.
	Use backup Radius server	Controls whether to enable the secondary RADIUS server for authentication. If it is enabled, the secondary RADIUS server provides services when the primary server fails to handle authentication requests. To make the secondary RADIUS server take effect, you need to configure its parameters in the same way as that of the primary server.
TACACS+	Authentication Server	Specifies the IP address of the TACACS+ server.
	Authentication Port	Specifies the port that the TACACS+ server uses to provide authentication. The default value is **49**.
	Protocol	Specifies the protocol used for authentication, which can be **ascii**, **pap**,

Parameter		Description
		or **chap**.
	Shared Key	Specifies the password provided for NTA authentication for its access to the TACACS+ server. NTA and the TACACS+ server can receive packets from each other and respond accordingly only when the key configured here is the same as that on the TACACS+ server.
	Authentication Hold-in Time	Specifies the time for NTA to keep attempting to connect to the TACACS+ server. The value range is 5–60 seconds.
LDAP	Authentication Server	Specifies the IP address of the LDAP authentication server.
	Authentication Port	Specifies the port that the LDAP server uses to provide authentication. The default value is **389**.
	Protocol	Specifies the protocol used for authentication, which can be **clear**, **ssl**, or **tls**.
	User Property	Specifies an LDAP attribute for user authentication. Values can be any of the following, depending on the operating system: • Linux LDAP: **uid**, **cn**, or **displayName** • Windows LDAP: **sAMAccountName** or **displayName**
	Base DN	Specifies the base domain name for LDAP authentication in the format of cn=xx,dc=xx1,dc=xx2.
	Username/Password	Specifies the user name and password for LDAP authentication.

4.6.4 Configuring the Web API Allowlist

Third-party users can access NTA through the web API. If the web API allowlist is disabled, any IP addresses can be used for login to NTA with an access key. After the allowlist is enabled, only IP addresses on the allowlist can be used for login to NTA with an access key.

Choose **Administration > User Management > Web API Allowlist** and configure parameters.

Table 4-25 describes parameters for configuring the web API allowlist.

Table 4-25 Parameters for configuring the web API allowlist

Parameter	Description
Allowlist	After the allowlist is enabled, only specified IP addresses can access the web API of NTA.
IP Address	IP addresses to be allowed, which can be individual IPv4 or IPv6 addresses, IP segments, and/or IP address ranges, with each in a separate line.

4.6.5 Configuring the HTTP Host Allowlist

The HTTP host allowlist is disabled by default. After it is enabled, no HTTP host-related vulnerability will be reported regarding the system.

Note	The HTTP host allowlist applies to all management interfaces of an HTTP host by default. Therefore, after this function is enabled, you should add IP addresses of all interfaces used for web management to the allowlist; otherwise, the system would be unavailable for access.

Choose **Administration > User Management > HTTP Host Allowlist**, enable the allowlist, and configure parameters.

Table 4-26 describes HTTP host allowlist parameters.

Table 4-26 Parameters for configuring the HTTP host allowlist

Parameter	Description
HTTP Host	Specifies IP addresses and/or domain names of HTTP hosts to be added to the allowlist. At most 10 IP addresses and/or domain names can be typed. After adding or deleting entries, click **Save** to commit the settings.

4.7 License

After an NTA device is installed, you must import the license before using it. Information about the license will be automatically displayed after the license is imported.

Choose **Administration > License**. On the **License** page, you can perform product authorization, download the license, and view the registered authorization information.

Product Authorization

Virtual NTA (vNTA) supports cloud-based authentication and local authentication. The hardware edition of NTA does not support these two types of authentication.

Local Authentication

Below **License Registration Information**, click **Browse**, select a license file from a local disk drive, and click **OK** to import the license.

Note	• To get a license file, contact NSFOCUS technical support. • You are advised not to include special characters or Chinese characters in the license file name.

Cloud-based Authentication

In the authentication and authorization area, type the address of the authorization center and click **OK**. If the authorization is successful, the authorization status is displayed as "Authorized".

Viewing Registered Authorization Information

After a license is imported, authorization information registered under the license is displayed by default. Table 4-27 describes such authorization information.

Table 4-27 Registered authorization information

Parameter	Description
License Status	Status of the current license.
License Type	Type of the current license, which may be any of the following: • **Trial**: free license for trial use • **Temporary Sales**: license for devices for which a purchase contract has been signed but the full payment is not made • **Subscription**: license for devices that have been purchased with full payment • **Perpetual Sales**: license in effect after payment
License No.	Unique number of the current license.
Monitored Devices	Number of devices monitored by the current NTA.
Traffic Limiting	Maximum traffic that the current NTA can detect.
Authorization Object	Object to which the current license is authorized.
Authorization Module	Module authorized by the current license.
Basic Service Start Date	Start date of the basic service covered by the current license, that is, the authorized upgrade service.
Basic Service End Date	End date of the basic service covered by the current license, that is, the authorized upgrade service. When the license expires: • Trial/Temporary Sales/Subscription: NTA can no longer be upgraded and all system services stop, ceasing to provide any protection. • Perpetual Sales: NTA still provides protection, but can no longer be upgraded.
Threat Intelligence Service Start Date	Start date of the threat intelligence service, if NSFOCUS Threat Intelligence (NTI) is covered by the current license.
Threat Intelligence Service End Date	End date of the threat intelligence service, if NTI is covered by the current license.
Reminder	Number of days before the basic service and threat intelligence service covered by the current license, that is, the authorized upgrade service, expires.

Downloading a License

You can click **Download** to download a license that has been imported to a local disk drive.

License Expiration Warning

After license expiration warning is configured, you will receive alert emails before and after the license expires. Table 4-28 describes parameters for configuring license expiration warning.

Table 4-28 Parameters of license expiration warning

Parameter	Description
License Expiration Warning	Controls whether to enable the license expiration warning function. If you select **On**, alert emails will be sent to users before and after the license expires.
License Expiration Warning Frequency	How often a license expiration warning is sent by email. Options include **3 days**, **1 week**, **1 month**, and Only **once**.
License Expiration Reminder Object	Specifies the email address or user account to receive license expiration warming emails. Type email addresses in the text box or click  to add user accounts. Up to five email addresses or user accounts are allowed, with one per line.  When adding a user account, ensure its email address has been correctly configured for receiving license expiration warning emails.

4.8 Hot Standby

NTA in DPI mode does not support this function.

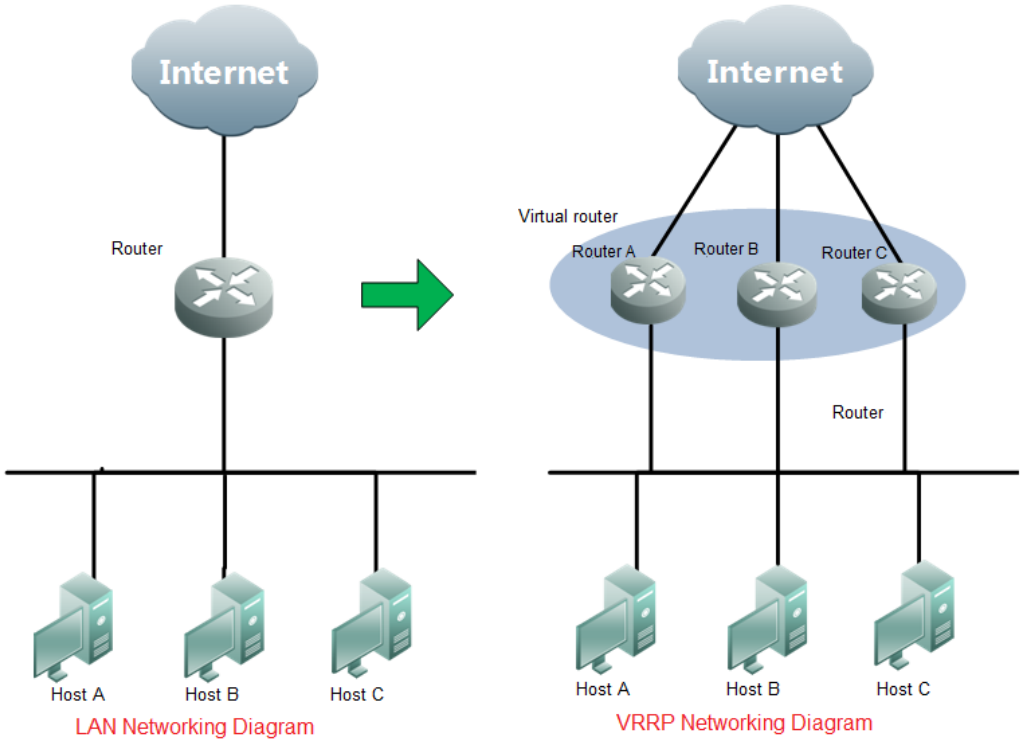
During data communication, any kind of software or hardware error may cause improper network connection or network interruption, which in turn will cause data transmission failure. The VRRP-based hot standby function provided by NTA can effectively prevent data communication interruptions caused by single point of failures (SPOFs) and enhance network reliability.

4.8.1 Getting to Know VRRP

Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) is a redundancy protocol used to resolve network interruptions caused by gateway faults. As shown in Figure 4-2, several routers on a local area network (LAN) are grouped together to form a VRRP backup group. A backup group, which consists of a master router and multiple backup routers, functions as a virtual router.

Figure 4-2 VRRP networking diagram



Router A, router B, and router C constitute a virtual router. This virtual router has its own IP address and hosts on the LAN take it as their default gateway. Router A, router B, or router C, whichever has the highest priority, works as the master router assuming the responsibility of a gateway. The other two work as backup routers. When the master router becomes faulty, the backup ones automatically forward packets in lieu of the former, thereby ensuring the continuity and reliability of network communication.

VRRP Backup Group

A VRRP group has the following characteristics:

- Has the unique virtual router identifier (VRID).
- Has its own virtual IP address: Hosts on a LAN know only the IP address of the virtual router, with no need to distinguish the master router from backup routers.
- The master router and backup routers in the backup group each has its own IP address.
- The election mechanism of VRRP decides which router in the group assumes the forwarding responsibility. Hosts on a LAN need to only take the virtual router as the default gateway.

VRRP Advertisement Interval Timer

The master router in a VRRP backup group sends periodic VRRP advertisement messages, notifying other routers in the group that it is working properly.

Users can adjust the interval for the master router to send advertisement messages by setting a VRRP timer. A backup router, if failing to receive any VRRP advertisement message over a

period of three intervals, takes itself as the master router and sends VRRP advertisement messages, thereby starting reelection of the master router.

Working Mode of Routers in a Backup Group

Routers in a backup group work in either of the following modes:

- Non-preemption: In this mode, a backup router, even if it is configured with a higher priority, will not become the master one as long as the master router functions properly.
- Preemption: In this mode, the backup router sends VRRP advertisement messages when finding that it has a higher priority than the current master router. This leads to the reelection of the master router within the group to replace the original master one. Accordingly, the original master router will become a backup router.

4.8.2 Configuring Hot Standby

NTA supports the hot standby function implemented by only two NTA devices working in active/standby mode. One NTA works in active mode, handling all services and sending configurations to the standby device for backup. The other works in standby mode, not handling services and for backup purposes only.

Before enabling high availability (HA), you need to first specify the master and backup NTA devices and configure a VRRP backup group on the master device. Interfaces on the two devices with the same VRID back up each other. Interfaces on the master device in the VRRP backup group are all master ones and those on the backup device are all backup ones.

After the hot standby function is enabled, the master NTA synchronizes configuration information in real time to the backup device to ensure consistent configurations between the two. Configuration information that can be synchronized includes the following:

- Monitoring object settings
- Alert configuration templates
- Global alert settings
- Global diversion settings
- Flow collection and forwarding settings
- Data dictionary settings
- Basic system settings
- Third-party interface settings
- User management settings
- Auto-learning baseline thresholds

An active/standby switchover is triggered when any of the following occurs on the master device:

- Any interface in the VRRP group is down.
- The system restarts.
- The system engine is down.
- The system is power off.

To configure the hot standby function, follow these steps:

Step 1 Choose **Administration > Hot Standby** and configure peer parameters.

Table 4-29 describes peer configuration parameters.

Table 4-29 Hot standby parameters (peer device)

Parameter	Description
Management IP address of the peer NTA device	IP address of the peer device. In this case, the IP address of interface M is preferable.
Use peer as master	If the current NTA is a backup device, select this check box; otherwise, leave it empty. After the HA role of NTA is specified, all roles in the VRRP group are the same as the HA role of the device: • When the current NTA is a master, all interfaces on it are master ones. • When the current NTA is a backup device, all interfaces on it are backup ones.

Step 2 Click **Verify** to check whether the current NTA properly connects to the peer NTA, whether their time zone configurations are the same, and whether their software versions are the same.

You can continue configuring related parameters only after the current NTA passes the verification.

Step 3 Enable the hot standby function.

Click **Enable** to enable the function or click **Disable** to disable the function.

Step 4 Configure related parameters.

a. Check the role of the current device.

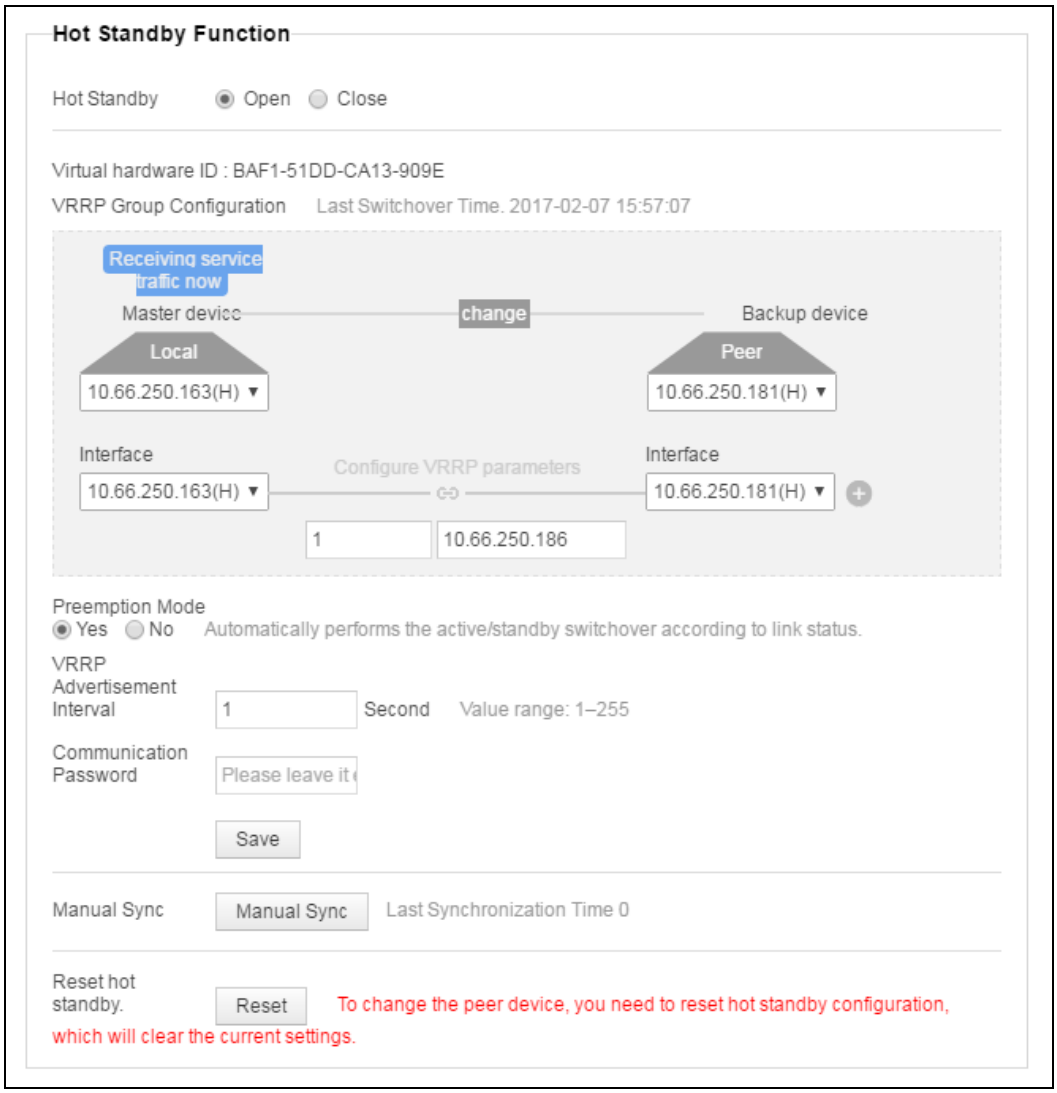
In the upper part of the page, the roles of the current and peer devices in the backup group are displayed.

b. Configure VRRP backup groups. At most five can be configured. Table 4-30 describes VRRP back group configuration parameters.

Table 4-30 Hot standby parameters (VRRP backup group)

Parameter	Description
Interface	Interfaces that back up each other. The two interfaces in a group must have IP addresses on the same segment; otherwise, VRRP multicast packets for configuration synchronization cannot be received.
Configure VRRP parameters	In the left text box, specify a VRID to uniquely identify the VRRP group. The value must be an integer in the range of 1–255. Note the following when configuring a VRID: • It is recommended that the same VRID be assigned to corresponding interfaces on the master and backup devices, such as the M interface on the master device and the M interface on the backup device, so that they belong to the same VRRP group and can back up each other. • The VRID of interfaces in the same VRRP group must be the same. • Different interfaces on a device cannot be configured with the same VRID, that is, cannot be in the same VRRP group. In the right text box, configure the virtual IP address of the VRRP backup group. This IP address must be on the same network segment as the IP addresses of the two interfaces in the group and different from the IP address of any interface. You can click  to add a VRRP group or  to delete one.

Figure 4-3 Configuring hot standby parameters



c. Configure the preemption mode.
   - If you click **Yes** for **Preemption Mode**, when the fault on the master device is fixed, this device preempts to become the master, forwarding data again.
   - If you click **No** for **Preemption Mode**, when the fault on the master device is fixed, this device does not preempt to become the master. In this case, services are not handed over back to it. That is to say, the original backup device still works in active state to forward data.

d. Configure a communication password.

   A communication password facilitates secure configuration synchronization. It must be a string of 8–20 characters. To configure such a password, you need to log in from a virtual IP address or log in to a master or backup device with the **admin** account, and then type the password on the **Hot Standby Function** page.

For an NTA device with the hot standby function, after it is upgraded to V4.5R89F01CN or later, you must configure a communication password before properly using this function.

e. Configure synchronization settings.

NTA supports manual and automatic synchronization of all configurations on the master device to the backup device. This can take place only after you properly configure VRRP group parameters.

By default, when configurations on the master device change, such changes are synchronized to the backup device.

- When the current device is the master, the system administrator can click **Manual Sync** to synchronize configurations on this device to the backup.
- When the current device is the backup, the **Manual Sync** button is unavailable.

f. Configure the VRRP advertisement interval.

The VRRP advertisement interval indicates the interval at which the device sends a heartbeat message in multicast mode to notify its own status. The default value is recommended. If the backup line interface fails to receive any multicast packet from the master line interface after the specified interval, the system deems that the master line is down. In this case, the backup line turns to active and begins to forward data.

The VRRP advertisement interval configured on the local device must be the same as that on the peer device.

Step 5 Click **Save** to commit the settings.

Step 6 (Optional) If you need to reconfigure parameters, click **Reset** to clear the current settings.

----End

4.9 System Upgrade

In the Upgrade module, you can perform the following operations:

- Upgrading System Software
- Upgrading Detection Rules
- Upgrading Threat Intelligence

4.9.1 Upgrading System Software

The system software of NTA can only be manually upgraded. The procedure is as follows:

Step 1 Contact NSFOCUS technical support for the NTA upgrade package. Make sure that the package matches the current device.

Step 2 Choose **Administration** > **Upgrade** > **System Software Upgrade**, click **Browse**, select the upgrade package, and then click **Open**.

Step 3 Click **Upload**.

After the upgrade package is uploaded, the system displays the upgrade confirmation dialog box.

Step 4 Click **Confirm Upgrade** to start the upgrade immediately.

During the upgrade, NTA displays the progress. After the upgrade is complete, NTA automatically returns to the previous page.

Note	During the upgrade, you need to wait patiently until a message indicating successful upgrade appears.

The system automatically restarts after the message prompting the upgrade success.

Step 5 Log in to the system and view the firmware version and upgrade date in the **Upgrade History** list to check whether the upgrade succeeded.

Step 6 View upgrade notes.

a. Click  in the **Operation** column to view upgrade notes. The "-" sign in the **Operation** column indicates that it is the original software version.

b. Click **Close** to return to the **System Upgrade** page.

----End

4.9.2 Upgrading Detection Rules

Choose **Administration** > **Upgrade** > **Detection Rule Upgrade**. You can upgrade NTA's detection rule library locally and remotely.

Local Upgrade

Before the upgrade, contact NSFOCUS technical support for the latest upgrade package of the detection rule library.

In the **Local Upgrade** area, click **Browse**, select the upgrade package, and then click **Open**. Click **Upload** to start the upgrade. If the upgrade is successful, a related record is shown in the **Upgrade History** list and the new rule library version is shown in the upper-left corner of the page.

Remote Upgrade

In the **Auto Sync** area, configure automatic synchronization parameters and click **Save**. You can also click **Upgrade Now** to immediately upgrade the rule library. Table 4-31 describes remote upgrade parameters.

Table 4-31 Remote upgrade parameters

Parameter	Description
Server Address	Specifies the remote upgrade server address, which is **update.nsfocus.com** by default.
Enable Auto Sync	Controls whether to enable automatic synchronization. After this is enabled, the rule library will be automatically synchronized.
Upgrade Time	Specifies a time for the rule library to automatically upgrade. Options include **Every day**, **Every week**, and **Every month**, followed by specific time or days for you to choose.

4.9.3 Upgrading Threat Intelligence

Choose **Administration > Upgrade > Threat Intelligence Upgrade**. The threat intelligence database can be upgraded locally and remotely with the same methods for the rule library. For details, see section 4.9.2 Upgrading Detection Rules.

4.10 Access Control

NTA supports access control. In other words, it can allow or deny access from one or more external IP addresses.

Choose **Administration > Access Control**. The access control function is disabled by default. To enable this function and configure an access control rule, follow these steps:

Step 1 Click **Enable** and then **Save** to enable access control.

By default, all external IP addresses are allowed to access the device.

Caution	During the configuration, the local IP address may fail to be added to the allowlist or may be deleted by mistake, making it impossible to log in to the web-based manager and background. To restore the settings, do as follows: Log in to the console user interface and run the **NTA# iptables off** command to disable the access control function.

Step 2 On the **Access Control** page, click **Add** to add external IP addresses.

Table 4-32 describes access control parameters.

Table 4-32 Parameters for configuring an access control rule

Parameter		Description
Default rule		Global access control rule: • **Deny external access**: forbids all external IP addresses to access the current NTA. • **Allow external access**: allows all external IP addresses to access the current NTA.
Custom rule	Source IP	External source IPv4 or IPv6 address.
	Prefix Length/Subnet Mask	Subnet mask of the IPv4 address or the prefix length of the IPv6 address. The subnet mask of IPv4 addresses ranges from 24 to 32 and the prefix length of IPv6 addresses ranges from 96 to 128.
	Access Control	Specifies an access control action: • **Allow**: allows the specified external IP address to access the current NTA. • **Forbid**: forbids the specified external IP address to access the current NTA.

Custom access control rules can be edited, deleted, and re-sorted.

Note	Rules in the list are matched one by one from top to bottom. You can click  or  to move a rule up or down.

----End

5 Configuration

This chapter presents core configurations of NTA, containing the following sections:

Section	Description
Objects	Describes how to configure objects monitored by NTA, including routers, router interface groups, and regions.
Bulk Configuration	Describes how to configure regions and IP groups in bulk and how to start bulk auto-learning.
Alert Templates	Describes how to configure a router alert template, region alert template, and IP group alert template.
Global Alert Settings	Describes how to configure global alert settings, including default DDoS attack detection thresholds, global alert parameters, alert plug-in management, auto-learning parameters, traffic statistics, and fast alert parameters.
Global Diversion Settings	Describes how to configure default diversion policies, a BGP route for routing notification, a protection device, and FlowSpec BGP.
Flow Data Collection and Forwarding	Describes how to configure flow data collection and forwarding.
Detection of Bogus Source IP Addresses	Describes how to configure a rule for bogus source IP address detection.
NTI	Describes how to configure NTA to collaborate with NSFOCUS Threat Intelligence center (NTI).
Data Dictionary	Describes how to configure an application port and AS object.
Allowlist	Describes how to configure the alert allowlist and diversion allowlist.

5.1 Objects

The Objects module allows you to configure the following objects for NTA to monitor:

- Router
- Router Interface Group
- Region

5.1.1 Router

NTA in DPI mode does not support router monitoring.

NTA can monitor data packets sent through a router. It can also monitor the CPU and memory usage as well as traffic on interfaces of the router on which the SNMP function is enabled.

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

Router configuration involves the following tasks:

- Configuring a Router
- Configuring Router Interfaces

5.1.1.1 Configuring a Router

NTA can detect and analyze traffic through a router. It can also monitor the resource usage and interface bandwidth usage of the router. For this purpose, you need to configure the router first, which involves the following:

- Basic information configuration: configuration of the device name, its IP address, and which alert template to use
- SNMP configuration: configuration of parameters for receiving data from the router via SNMP
- Router alert configuration: configuration of the interface bandwidth usage and performance alert thresholds

NTA monitors traffic through routers for attacks according to default DDoS attack alert thresholds. For details, see section 5.4.1 Default DDoS Attack Detection Thresholds.

To configure a router, follow these steps:

Step 1 Choose **Configuration > Objects > Routers**.

Initially, the router list is empty.

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

Table 5-1 describes basic parameters of a router.

Table 5-1 Basic parameters of a router

Parameter	Description
IP Address	IPv4 or IPv6 address of the router to be monitored. This parameter is mandatory.
Device Name	Name of the router (characters like < > ' " \ are not allowed in a device name). It is the IP address by default.
Capture Flow Packets	Specifies whether to collect flows from the router. If you select **Yes**, proceed to step 3. If you select **No**, proceed to step 4.
Router Alert Template	Specifies an alert template to configure alert parameters for this router. The drop-down list displays the existing alert templates. You can also select **Custom** and configure alert parameters on the **Router Alert Configuration** page. For how to configure a router alert template, see section 5.3 Alert Templates.

Step 3 (Optional) Configure flow collection parameters.

Table 5-2 describes flow collection parameters.

Table 5-2 Flow collection parameters

Parameter	Description
Flow Collection IP	IP address used by the router to send flow data to NTA.
Flow Version	Specifies the flow protocol type and version number. If **Flow Version** is set to **Flexible NetFlow**, the flow protocol type can be NetFlow V5, NetFlow V9, or IPFIX.
Sampling Rate Adaption	Controls whether to enable sampling rate adaption for sFlow (**sFlow_v4** and **sFlow_v5)**.
Flow Sampling Rate	Indicates the rate of packets to be sampled to all the packets passing through the router, which must be the same as that configured on the router. The maximum value is **65535**. When **sFlow_v4** or **sFlow_v5** is selected for **Flow Version** and sampling rate adaption is enabled, this field is unavailable.
Flow Forwarding Configuration	Specifies whether to forward collected flow data to other IP addresses. It has the following values: • **Use Default Configuration**: uses global default settings. For details, see section 5.6 Flow Data Collection and Forwarding. • **Not Forward**: does not forward received flow data. • **Custom**: specifies IPv4 or IPv6 addresses and port numbers to which flow data will be forwarded. You can type up to eight destination addresses, with each in a separate line.

Step 4 Configure SNMP parameters.

Table 5-3 describes these parameters.

If SNMP collection is not configured here, only interface index information can be viewed from the interface list, but not other information such as the interface name, IP address, description, and bandwidth.

Note that NTA can query information of a router only after parameters related to the SNMP server have been configured on the router.

Table 5-3 SNMP configuration parameters

Parameter	Description
SNMP Collection	Controls whether to enable NTA to collect data from the router via SNMP. By default, it is not enabled.
SNMP Collection IP	Specifies the IPv4 or IPv6 address from which SNMP information will be collected. The IP address here may be different from the source address of flow data. If you do not specify any IP address here, NTA uses the IP address of the router to collect SNMP information.
Vendor	Specifies the vendor of the router. Whether the CPU and memory OIDs will be

Parameter	Description
	collected and what algorithm will be adopted depend on the vendor.
SNMP Version	Specifies the SNMP version. Currently, NTA supports data collection via SNMPv1, v2c, and v3.
Context	Indicates the context of the router. This parameter is optional. It is available only when **v3** is selected for **SNMP Version**.
Community	Specifies the community string for access to the router's statistics. This parameter is available for SNMPv1 and SNMPv2c.
Username/Password	Specifies the user name and password of the SNMP service user. This parameter is available for SNMPv3.
Security Level	Specifies the authentication method. SNMPv3 supports three authentication methods: **No authentication**, **Account authentication**, and **Private key authentication**. The default value is **No authentication**. Parameters vary with the authentication method. This parameter is available for SNMPv3.
Authentication Protocol	Specifies the authentication protocol, which can be **MD5** or **SHA**. This parameter is available when SNMPv3 is selected and the authentication method is **Account authentication** or **Private key authentication**.
Private Key Encryption Protocol	Specifies an encryption protocol. Currently, NTA supports DES and AES symmetric-key algorithms. This parameter is available when SNMPv3 is selected and the authentication method is **Private key authentication**.
Private Key Password	Specifies the password for generating the authentication key. This parameter is available when SNMPv3 is selected and the authentication method is **Private key authentication**.
Custom OID	Controls whether to enable custom OIDs. After selecting the **Enable** check box, you need to further configure related parameters.
CPU Usage OID	This is available only after custom OIDs are enabled. Specifies an OID for the CPU usage. After this is specified, the system directly uses it instead of obtaining the related OID from the attached OID document.
Memory Usage Computation Method	Specifies a method of calculating the memory usage OID, which can be either of the following: • **Usage OID**: calculates the memory usage based on the specified memory usage OID. For this method, you should specify an OID for the memory usage. • **Numerical OID**: calculates the memory usage based on multiple memory usage OIDs. For this method, you should configure at least two of the following: **Total Memory OID**, **OID of Used Memory**, and **OID of Idle Memory**.
Memory Usage OID	This parameter must be configured when custom OIDs are enabled and **Usage OID** is selected as the memory usage calculation method. Specifies an OID for the memory usage. After this is specified, the system directly uses it to calculate the memory usage instead of obtaining the related OID from the attached OID document.
Total Memory OID	This parameter must be configured when custom OIDs are enabled and **Numerical OID** is selected as the memory usage calculation method. Specifies an OID for the total memory space. After this is specified, the system directly uses it to calculate the total memory space instead of obtaining the related OID from the attached OID document.
OID of Used Memory	This parameter must be configured when custom OIDs are enabled and

Parameter	Description
	Numerical OID is selected as the memory usage calculation method. Specifies an OID for the used memory space. After this is specified, the system directly uses it to calculate the used memory space instead of obtaining the related OID from the attached OID document.
OID of Idle Memory	This parameter must be configured when custom OIDs are enabled and **Numerical OID** is selected as the memory usage calculation method. Specifies an OID for the idle memory space. After this is specified, the system directly uses it to calculate the idle memory space instead of obtaining the related OID from the attached OID document.

Step 5 Configure router alert parameters.

If a router alert template is selected during the configuration of basic router information, the default settings of the template are displayed on this page. You can modify these default settings.

NTA supports alerting for abnormal bandwidth, CPU usage, and memory usage as well as SNMP data collection anomalies and flow data collection anomalies.

Table 5-4 describes router alert parameters.

Table 5-4 Router alert parameters

Parameter	Description
Alert or not	Controls whether to enable the alerting function.
Latent Alert Threshold	Specifies the bandwidth, CPU, or memory usage threshold that triggers NTA to generate an alert only after the usage stays at this level for some time (depending on **Alert Latency Period** under **Configuration > Global Alert Settings > Alert Parameters**). For the setting of **Alert Latency Period**, see section 5.4.3 Alert Parameters.
Direct Alert Threshold	Specifies the bandwidth, CPU, or memory usage threshold that triggers NTA to generate an immediate alert.
Alert Threshold	Specifies the threshold for the SNMP or flow data acquisition interruption duration, which triggers NTA to generate an immediate alert.

Step 6 Configure traffic statistics parameters.

On the **Traffic Statistics** page, select statistical items of traffic.

Step 7 Click **Save and Complete** to commit the settings and return to the **Routers** page.

In the router list, you can view brief information of the router monitored by NTA.

Table 5-5 describes parameters in this list.

Table 5-5 Monitored router information

Parameter	Description
Device Name	Name of the router.

Parameter	Description
IP Address	IP address that identifies the router.
Vendor	Vendor of the router.
Version	Version of the SNMP protocol.
Collection IP	IP address from which SNMP information will be collected.
Interface Number	Number of router interfaces obtained via SNMP. Clicking the number shows basic settings, interface bandwidth usage, and inbound and outbound traffic statistics of all monitored interfaces on the router.
Operation	You can edit and delete a router by clicking or .

----End

5.1.1.2 Configuring Router Interfaces

You can configure router interfaces as required, including:

- Enabling or disabling the monitoring function: After it is enabled for a router interface, NTA can monitor the traffic and bandwidth usage of this interface.
- Specifying the interface type: An interface connecting a router and the Internet is called an uplink interface, and an interface connecting a router and the server is called a downlink interface.
- Adding an interface to a router interface group: After a router interface group is configured, NTA can monitor the overall traffic of the group.

To configure router interfaces, follow these steps:

Step 1 Choose **Configuration > Objects > Routers** and click the interface number of a router to open its interface list page.

Table 5-6 describes parameters in the interface list.

Table 5-6 Parameters in the interface list

Parameter	Description
Interface Index	Indicates the interface index, which is obtained from flow data.
Name	Indicates the interface name, which is obtained via SNMP. If SNMP collection is not enabled during router configuration, nothing is displayed here.
SNMP Status	Indicates whether SNMP is enabled to monitor traffic and bandwidth usage of the interface. • indicates that SNMP is enabled. • indicates that SNMP is disabled. In this case, NTA cannot obtain traffic and bandwidth usage of the interface.
Flow Statistics Status	Indicates whether flow statistics are enabled. • indicates that this function is enabled. • indicates that this function is disabled. In this case, NTA does not collect flow data of the interface.

Parameter	Description
IP Address	Indicates the IP address of the interface, which is obtained via SNMP. If SNMP collection is not enabled during router configuration, or SNMP collection is enabled but no IP address is configured for this interface, nothing is displayed here.
Description	Indicates brief information about the interface, which is obtained via SNMP. If SNMP collection is not enabled during router configuration, nothing is displayed here.
Bandwidth	Indicates the bandwidth configuration of the interface, which is obtained via SNMP. If SNMP collection is not enabled during router configuration, **N/A** is displayed here.
Type	Indicates the interface type, which can be **Downlink Interface**, **Uplink Interface**, or **Interconnection**.
SNMP Monitoring	Enables or disables SNMP interface traffic monitoring. NTA can monitor the traffic and bandwidth usage of the interface only after this is enabled.
Flow Operation	Enables or disables flow statistics on the interface. NTA can collect flow data of this interface only after this is enabled.

Step 2 Enable or disable SNMP-based monitoring.

The **SNMP Status** column shows whether SNMP is enabled for monitoring traffic and bandwidth usage of an interface.

- The icon indicates that SNMP-based monitoring is enabled. In this case, you can click in the **SNMP Monitoring** column to disable this function.
- The icon indicates that SNMP-based monitoring is disabled. In this case, you can click in the **SNMP Monitoring** column to enable this function.

Select one or more interfaces and then choose corresponding commands from the **Monitor** drop-down list to monitor or cancel monitoring of the specified interfaces. You can also choose **Monitor All** or **No Monitor** to monitor or cancel monitoring of all interfaces.

Step 3 Enable or disable flow statistics.

The **Flow Statistics Status** column shows whether flow statistics are enabled.

- The icon indicates that this function is enabled. In this case, you can click in the **Flow Operation** column to disable this function.
- The icon indicates that this function is enabled. In this case, you can click in the **Flow Operation** column to enable this function.

Select one or more interfaces and then choose corresponding commands from the **Monitor** drop-down list to monitor or cancel flow statistics on the specified interfaces. You can also choose **Monitor All** or **No Monitor** to monitor or cancel flow statistics on all interfaces.

Step 4 Specify the interface type.

a. In the interface list, select one or more interfaces. Pointing to the question mark following **Configure Interface Type** displays the router interface topology.

b. Select one or more interfaces and click **Configure Interface Type**. You can configure the specified interfaces as uplink, downlink, or interconnection interfaces. To distinguish

between inbound and outbound traffic, you are advised to specify the interface type of a router as follows:

- The interface for connecting to the Internet is an uplink interface.
- The interface for connecting to the server is a downlink interface.
- Interfaces for connecting to other routers are interconnection interfaces.

Step 5 Add interfaces to a router interface group.

Select interfaces from the interface list and click **Add**.

- If router interface groups are available, select one from the drop-down list. Then the selected interfaces are added to this group.
- If no router interface group is available or existing ones are not appropriate for the purpose, choose **Add Interface Group** to create a new group, to which the selected interfaces will be added. For the creation of a router interface group, see section 5.1.2 Router Interface Group.

Step 6 Query interfaces.

You can set query conditions to find the desired interfaces. If you want to query interfaces based on the bandwidth, make sure that such information can be obtained.

Step 7 Switch to another router.

Select another router from the **Select Router** drop-down list to open the editing page of the specified router.

----End

5.1.2 Router Interface Group

NTA in DPI mode does not support router interface group configuration.

A router interface group is a set of interfaces on a router, used to define the network boundary. After configuration, you can monitor the overall traffic of this interface group.

To configure a router interface group, follow these steps:

Step 1 Choose **Configuration > Objects > Router Interface Groups**.

Initially, the router interface group list is empty.

Step 2 Click **Add**, type the group name and description, and click **OK**.

The new group does not contain any interface. Therefore, Number of Interfaces is displayed as **0**.

Step 3 Specify interfaces to be included in the interface group.

When there are a large number of interfaces, you can set query conditions to display only those that you are interested in.

a. Click  in the **Operation** column to open the **Interface List** page.

b. Select one or more interfaces and click **Add** to add them to the group.

Step 4 View interfaces included in an interface group.

Click  next to the number of interfaces to display all interfaces in the group. You can delete interfaces from the group.

----End

5.1.3 Region

A region is a collection of a user's or a company's businesses. On NTA, you can define a region based on IP address ranges or router interfaces to implement region-based centralized monitoring of traffic. You can further define an IP group for businesses of the same property in the region and define a traffic detection policy for this IP group.

Region configuration involves the following:

- Configuring Basic Information: configuration of such basic information as the region name and contact person
- Configuring the IP Range: configuration of IP address ranges or router interfaces to be included in the region (DFI mode), or configuration of IP address ranges to be included in the region (DPI mode)
- Configuring Traffic Alert Policies: configuration of monitoring policies for both inbound and outbound traffic of the region, including traffic alert policies, alert hierarchy policies, and alert diversion policies
- Configuring DDoS Attack Detection Policies: configuration of DDoS attack detection policies for all IP addresses and certain network segments in the region, including attack detection policies, alert hierarchy policies, and alert diversion policies
- Configuring Traffic Statistics: configuration of traffic statistics parameters for the region, such as top IP addresses, top applications, and top protocols
- Configuring Traffic Diversion Rules: configuration of separate policies for diverting abnormal inbound and outbound traffic of the region, and policies for diverting traffic destined for devices encountering DDoS attacks
- Configuring an IP Group and Related Policies: configuration of an IP group for businesses of the same property in the region and configuration of a traffic detection policy for this IP group

Note	• Regional traffic is monitored against traffic alert thresholds and traffic diversion rules. Traffic diversion can take place only when the traffic rate reaches the threshold and the traffic meets the diversion condition. • The policy for an IP group comes before the policy for its region when NTA implements abnormal traffic detection. When neither is hit, NTA will conduct abnormal traffic detection based on default policies.

You can configure regions one by one or in batches. This section describes how to configure a single region. For details about how to configure regions in batches, see section 5.2.1 Bulk Configuring Regions.

To configure a single region, follow these steps:

Step 1 Choose **Configuration > Objects > Regions**.

Basic information of all regions is displayed. Table 5-7 describes parameters in this list.

Table 5-7 Parameters in the region list

Parameter		Description
Name		Name of the region.
Contact		Name of the contact person for the region.
Email		Email address of the contact person. A maximum of 10 email addresses are allowed, with each in a separate line.
Description		Region description.
IP Groups		Number of IP groups in the region. Clicking the number displays all included IP groups. Clicking on the left of the region name displays the same information.
Range	Router Interfaces	Indicates the number of router interfaces in the region. This information is unavailable on NTA in DPI mode.
	IP Range	Indicates the number of IP address ranges in the region. Pointing to the number displays details about the address ranges.
Operation		Operations that can be performed for the region: • : adds an IP group. • : modifies region settings. • : deletes the region.

Step 2 Create a region.

Click **Add** and complete configuration of the following settings in six steps as instructed by the configuration wizard:

- Basic information
- Range
- Regional traffic alert
- Regional DDoS attack alert
- Traffic statistics
- Traffic diversion rule

You can just configure basic information. To configure other settings of such a region, click in the **Operation** column and configure parameters as required.

Step 3 View and modify region settings.

Clicking the region name displays all settings of the region on one page.

After clicking **Edit**, you can modify its settings. You can also click in the **Operation** column of the region and then modify the settings.

During the edit process, you can click the configuration step name to quickly navigate to the desired page for parameter modification.

Step 4 (Optional) Delete regions.

Regions can be deleted one by one or in bulk.

----End

5.1.3.1 Configuring Basic Information

Table 5-8 describes parameters for configuring basic information of a region.

Table 5-8 Parameters for configuring basic information of a region

Parameter	Description
Region name	Specifies the name of the region to be monitored. This parameter is mandatory.
Email	Specifies the email address of the contact person. A maximum of 10 email addresses are allowed, with each in a separate line.
Contact	Specifies the name of the contact person for the region.
Address	Specifies the correspondence address of the contact person.
Region Description	Describes the region. A maximum of 50 characters are allowed.
Region Alert Template	Specifies an alert template to configure alert parameters for this region. The drop-down list displays the existing alert templates. For the configuration of a region alert template, see section 5.3.2 Region Alert Template.
Send Diversion Notification	If you select **Yes**, NTA sends a diversion notification email to the designated email address of the contact when the diversion targeting a region or IP groups within a region starts and ends.
Send Alert Notification	If you select Yes, when an alert related to a region or IP groups within a region starts and ends, NTA sends an email to the designated email address of the contact, including the destination IP address and the region or IP group to which the IP address belongs.
Send SNMP Trap	If you select Yes, NTA sends alerts and diversion logs about a region to the SNMP server.

5.1.3.2 Configuring the IP Range

A region is a collection of the customer's businesses. You can define a region based on IP address ranges or interfaces. NTA in DPI mode does not support defining a region based on interfaces.

IP Address Ranges

If you are clear about the IP addresses used by the customer, you can define this region based on IP address ranges. Moreover, you can define IP groups to subdivide the businesses and define different policies for these IP groups.

After **IP Range** is selected, you must enter IPv4 and/or IPv6 address ranges in the following formats:

- Range specified by a start IP address and an end IP address like 10.10.10.2-10.10.10.23 or 10.10.10.2-23.
- IP/mask: IPv4 address with a netmask ranging from 15 to 32 or IPv6 address with a prefix length ranging from 1 to 128.
- Specific IPv4 or IPv6 address.

When a configured IP address conflicts with an existing one in a region, the system prompts a message indicating the region name and IP address or IP segment.

Interfaces

NTA in DPI mode does not support defining a region based on interfaces.

A region can be defined based on interfaces, which must all be uplink or downlink ones. A region cannot contain both uplink and downlink interfaces.

You can click **Select Router Interface** to select another router and its uplink or downlink interfaces.

5.1.3.3 Configuring Traffic Alert Policies

NTA can separately monitor the inbound and outbound traffic of a region after you configure traffic alert policies for the region. The traffic alert policies include the following:

- Traffic detection policies: check the inbound and outbound traffic of the entire region so that an alert can be generated when a threshold is exceeded.
- Alert hierarchy policies: set the alert hierarchy.
- Traffic diversion policies: specify which levels of alerts will trigger traffic diversion. If an alert reaches the diversion-triggering level, NTA will divert traffic as specified by the corresponding diversion policy.

When detecting abnormal traffic, NTA generates an alert of an appropriate level according to the alert hierarchy policy, and diverts traffic according to the diversion policy.

Traffic Alert Period Configuration

In the **Region Traffic Alert Period Configuration** area, you can configure **Alert Latency Period** and **Alert Holding Period** for alerts triggered on abnormal traffic. For parameter description, see Table 5-23.

Traffic Alert Configuration

In the **Region Traffic Alert** area, you can configure alert policies for inbound traffic and outbound traffic.

When you click an alert type, the **Edit** area shows the alert type's parameters for you to edit.

Table 5-9 describes the parameters for configuring traffic alert policies.

Table 5-9 Parameters for configuring traffic alert policies

Parameter	Description
Detect Mode	Specifies a measurement basis for abnormal traffic detection and alerting: • **No detection**: indicates that NTA does not check whether inbound or outbound traffic is abnormal. • **Packets only**: indicates that NTA checks whether traffic exceeds the pps threshold and, if yes, generates an alert. • **Bytes only**: indicates that NTA checks whether traffic exceeds the bps threshold and, if yes, generates an alert. • **Both packets and bytes**: indicates that NTA checks whether traffic exceeds

Parameter	Description
	both the pps and bps thresholds and, if yes, generates an alert. • **Either packets or bytes**: indicates that NTA checks whether traffic exceeds either he pps or bps threshold and, if yes, generates an alert.
Latent Alert Threshold	Specifies a traffic threshold in bps or pps that triggers NTA to generate an alert only after the traffic rate stays above this level for some time.  The latent alert threshold must be lower than the direct alert threshold. • **bps Threshold**: specifies a threshold in bps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: specifies a threshold in pps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
Direct Alert Threshold	Specifies a traffic threshold in bps or pps that triggers NTA to generate an immediate alert.  The direct alert threshold should be greater than the latent alert threshold. • **bps Threshold**: specifies a threshold in bps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: specifies a threshold in pps that triggers NTA to generate an immediate alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
Carpet Bombing Detection	Controls whether to enable the carpet bombing detection function. By default, this function is disabled. After you select Yes, NTA will check traffic for carpet bombing attacks. Carpet bombing is a kind of DDoS attack that targets a large number of IP addresses.
TopN	Specifies the number of top IP addresses with the largest inbound traffic for the carpet bombing detection. 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.
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 proportion of actual traffic to the **Latent Alert Threshold** value: • **Low**: specifies the lowest proportion to trigger a low-level alert. The value is fixed to 100%. When the actual proportion is higher than the lowest

Parameter	Description
	proportion triggering a lower-level alert but lower than the lowest proportion triggering a medium-level alert, NTA generates a low-level alert. • **Medium**: specifies the lowest proportion to trigger a medium-level alert. The default value is **150**, and the maximum value is 10000. When the actual proportion is higher than the lowest proportion triggering a medium-level alert 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**, and the maximum value is 10000. When the actual proportion is higher than the lowest proportion triggering a high-level alert, NTA always generates a high-level alert. If the region alert hierarchy is not configured, NTA will detect traffic and send alerts according to the global alert hierarchy. For details, see section 5.4.3 Alert Parameters.
Diversion Level	Specifies an alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted. For the definition of alert levels, see section 5.4.3 Alert Parameters. • **No Diversion**: indicates that no traffic diversion will take place. • **Divert Traffic of Low-level Alert**: indicates that a low-level alert or higher will trigger traffic diversion. • **Divert Traffic of Medium-level Alert**: indicates that a medium-level alert or higher will trigger traffic diversion. • **Divert Traffic of High-level Alert**: indicates that only a high-level alert can trigger traffic diversion.

5.1.3.4 Configuring DDoS Attack Detection Policies

NTA can detect DDoS attacks for each IP address in the region, and network segments in the region aggregated by the specified netmask/prefix length. You can configure the following detection, alert, and diversion policies for various attack types:

- DDoS attack detection policies: check the traffic of each IP address and network segments aggregated by the specified netmask/prefix length. If attack signatures are matched, NTA generates alerts.
- Alert hierarchy policies: set the alert hierarchy.
- Traffic diversion policies: specify which levels of alerts will trigger traffic diversion. If an alert reaches the diversion-triggering level, NTA will divert traffic as specified by the corresponding diversion rule.

DDoS attack alert configuration consists of fixed threshold-based alert configuration and constituent proportion-triggered alert configuration.

DDoS Alert Period Configuration

In the **Region DDoS Alert Period Configuration** area, you can configure **Alert Latency Period** and **Alert Holding Period** for alerts triggered on DDoS attacks. For parameter description, see Table 5-23.

DDoS Attack Alert for a Network Segment

This DDoS attack alert only detects the inbound traffic of the targeted network segment. This function is disabled by default. To use it, set **Region** for **Detection Type** under **Configuration > Global Alert Settings > Network Segment-based DDoS Detection**, and select **Open** for **Status** in the **Region DDoS Attack Alert for a Network Segment** area.

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-based DDoS attack alert will be generated.

To enable network segment-based detection, the region's IP address range (see IP Address Ranges) specified must meet the following requirements:

- The IP address range must be in CIDR notation, and the difference between netmasks/prefix lengths configured is less than or equal to eight.
- At most 256 IP segments can be configured.

- **IPv4 Netmask**: Aggregate the region's IP address ranges to a network segment using the IPv4 netmask. The value range is 16–30, with **24** as the default. The value must be greater than or equal to the maximum IPv4 CIDR length configured for the region's IP address range, but less than or equal to the minimum IPv4 CIDR length plus 8.
- **IPv6 Prefix Length**: Aggregate the region's IP address ranges to a network segment using the IPv6 prefix length. The value range is 64–126, with **120** as the default. The value must be greater than or equal to the maximum IPv6 CIDR length configured for the region's IP address range, but less than or equal to the minimum IPv6 CIDR plus 8.

Table 5-10 Parameters of network segment-based DDoS attack alerts

Parameter	Description
Alert Type	Type of DDoS attack alerts. Currently, 27 types of attacks can be alerted, which cannot be edited.
Detect Mode	Specifies a measurement basis for the network segment-based DDoS detection and alerting. The default value is **No detection**. • **No detection**: indicates that NTA does not check whether the inbound traffic exceeds pps and bps thresholds. • **Packets only**: indicates that NTA checks whether the inbound traffic exceeds the pps threshold and, if yes, generates an alert. • **Bytes only**: indicates that NTA checks whether the inbound traffic exceeds the bps threshold and, if yes, generates an alert. • **Both packets and bytes**: indicates that NTA checks whether the inbound traffic exceeds both the pps and bps thresholds and, if yes, generates an alert. • **Either packets or bytes**: indicates that NTA checks whether the inbound traffic exceeds either the pps or bps threshold and, if yes, generates an alert.
Latent Alert Threshold	Specifies a threshold for the aggregate inbound traffic of a network segment in a detection period that matches an attack signature. When traffic exceeds this threshold, but is below the direct alert threshold, NTA

Parameter	Description
	does not generate an alert until the traffic rate stays above this threshold for some time (alert latency period).  Caution • The latency alert threshold must be lower than the direct alert threshold. • The format is number + K/M/G, such as 800M or 100K. • **bps Threshold**: specifies a threshold in bps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: specifies a threshold in pps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
Direct Alert Threshold	Specifies a threshold for the aggregate inbound traffic of a network segment in a detection period that matches an attack signature. When traffic exceeds this threshold, NTA immediately generates an alert.  Caution • The direct alert threshold should be greater than the latency alert threshold. • The format is number + K/M/G, such as 800M or 100K. • **bps Threshold**: specifies a threshold in bps that triggers NTA to immediately generate an alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: specifies a threshold in pps that triggers NTA to immediately generate an alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
Diversion Level	Specifies an alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted. For the definition of alert levels, see section 5.4.3 Alert Parameters. • **Not Diversion**: generates alerts only, with no traffic diversion to take place. • **Divert Traffic of Low-level Alert**: indicates that a low-level alert or higher will trigger traffic diversion. • **Divert Traffic of Medium-level Alert**: indicates that a medium-level alert or higher will trigger traffic diversion. • **Divert Traffic of High-level Alert**: indicates that only a high-level alert can trigger traffic diversion.
Alert Hierarchy (%)	Specifies the hierarchical structure of network segment-based DDoS attack alerts and traffic anomaly alerts generated for each network segment under detection. • **Medium**: specifies the lowest proportion to trigger a medium-level alert. The default value is **150**, and the maximum value is 10000. When the actual proportion is higher than the lowest proportion triggering a medium-level alert but lower than the lowest proportion

Parameter	Description
	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**, and the maximum value is 10000. When the actual proportion is higher than the lowest proportion triggering a high-level alert, NTA always generates a high-level alert.

DDoS Attack Alert Configuration

The **Region DDoS Attack Alert** area displays all attack types that can be detected by NTA, including built-in attack types and custom ones. For adding custom attack types, see section 5.4.4 Alert Plug-in Management. Here, you can configure inbound and outbound detection to detect anomalous traffic to destination IP addresses and anomalous traffic from source IP addresses.

- Inbound detection configuration
  - Fixed Threshold Configuration: checks whether the size of a type of traffic exceeds the specified threshold.
  - Constituent Proportion Configuration: checks the proportion of a type of traffic to the total traffic.
  - Connection Anomaly Detection Configuration: checks whether the IP segments covered by the region have more abnormal connections than the specified threshold.
- Outbound detection configuration

  Only constituent proportion configuration is supported.

Note	Only NTA in DPI mode supports the connection anomaly detection.

When you click an alert type, the **Edit** area shows its parameters for you to edit.

Table 5-11 describes parameters for configuring fixed threshold-based alerting. Table 5-12 describes parameters for configuring constituent proportion-triggered alerting. Table 5-13 describes parameters for configuring connection anomaly-triggered alerting.

Table 5-11 DDoS attack alert parameters (fixed thresholds)

Parameter	Description
Alert Type	Alert type. More than 20 types of attacks can be alerted.
Detect Mode	Specifies a measurement basis for DDoS detection and alerting: • **No detection**: indicates that NTA does not check whether traffic exceeds pps and bps thresholds. • **Packets only**: indicates that NTA checks whether traffic exceeds the pps threshold and, if yes, generates an alert. • **Bytes only**: indicates that NTA checks whether traffic exceeds the bps

Parameter	Description
	threshold and, if yes, generates an alert. • **Both packets and bytes**: indicates that NTA checks whether traffic exceeds both the pps and bps thresholds and, if yes, generates an alert. • **Either packets or bytes**: indicates that NTA checks whether traffic exceeds either he pps or bps threshold and, if yes, generates an alert.
Latent Alert Threshold	Specifies a threshold for the aggregate inbound or outbound traffic of an IP address in a detection period that matches an attack signature. When traffic exceeds this threshold, but is below the direct alert threshold, NTA does not generate an alert until the traffic rate stays above this threshold for some time (alert latency period). For the setting of **Alert Latency Period**, see section 5.4.3 Alert Parameters. Note The latent alert threshold must be lower than the direct alert threshold. The format is number + K/M/G, such as 800M or 100K. • **bps Threshold**: specifies a threshold in bps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: specifies a threshold in pps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
Direct Alert Threshold	Specifies a threshold for the aggregate inbound or outbound traffic of an IP address in a detection period that matches an attack signature. When traffic exceeds this threshold, NTA immediately generates an alert. Note The direct alert threshold must be greater than the latent alert threshold. The format is number + K/M/G, such as 800M or 100K. • **bps Threshold**: specifies a threshold in bps that triggers NTA to immediately generate an alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: specifies a threshold in pps that triggers NTA to immediately generate an alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
Diversion Level	Specifies an alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted. For the definition of alert levels, see section 5.4.3 Alert Parameters. • **No Diversion**: generates alerts only, with no traffic diversion to take place. • **Divert Traffic of Low-level Alert**: indicates that a low-level alert or higher will trigger traffic diversion. • **Divert Traffic of Medium-level Alert**: indicates that a medium-level alert or higher will trigger traffic diversion. • **Divert Traffic of High-level Alert**: indicates that only a high-level alert can trigger traffic diversion.
Alert Hierarchy (%)	NTA supports the hierarchical structure of DDoS attack alerts and traffic anomaly alerts generated for each IP address. • **Low**: specifies the lowest proportion to trigger a low-level alert. The value is

Parameter	Description
	fixed to 100%. When the actual proportion is higher than the lowest proportion triggering a lower-level alert but lower than the lowest proportion triggering a medium-level alert, NTA generates a low-level alert. • **Medium**: specifies the lowest proportion to trigger a medium-level alert. The default value is **150**, and the maximum value is 10000. When the actual proportion is higher than the lowest proportion triggering a medium-level alert 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**, and the maximum value is 10000. When the actual proportion is higher than the lowest proportion triggering a high-level alert, NTA always generates a high-level alert.

Table 5-12 DDoS attack alert parameters (constituent proportions)

Parameter	Description
Status	Controls whether to enable the constituent proportion function. The following parameters can be configured only after you enable the function.
Alert Type	Alert type, which can be **SYN Flood**, **ACK Flood**, **UDP Flood**, **ICMP Flood**, **DNS Query Flood**, or **Other Protocol Abnormal**. Alerts other than the first five types fall into **Other Protocol Abnormal**.
Detect Mode	Specifies a basis for DDoS detection and alerting: • **No detection**: indicates that NTA does not check whether a type of traffic in bps and pps exceeds the specified constituent proportions. • **Packet proportion only**: indicates that NTA checks whether the proportion of a traffic type in pps exceeds the specified value and, if yes, generates an alert. • **Byte proportion only**: indicates that NTA checks whether the proportion of a traffic type in bps exceeds the specified value and, if yes, generates an alert. • **Both packet proportion and byte proportion**: indicates that NTA checks whether the proportions of a traffic type in both pps and bps exceed the specified values and, if yes, generates an alert. • **Either packet proportion or byte proportion**: indicates that NTA checks whether the proportion of a traffic type in either pps or bps exceeds the specified value and, if yes, generates an alert.
Proportion for Latent Alerts (%)	Specifies the proportion of a type of traffic in the aggregate to the total traffic received or transmitted by an IP address in a detection period that matches an attack signature. When a type of traffic exceeds this proportion, but is below the proportion for direct alerts, NTA does not generate an alert until the traffic proportion stays above this value for some time (alert latency period). For the definition of alert levels, see section 5.4.3 Alert Parameters.  Note The proportion for latent alerts must be lower than that for direct alerts. • **bps Proportion**: specifies a proportion of a traffic type in bps (above the minimum trigger threshold) that triggers NTA to stay latent for some time

Parameter	Description
	before generating an alert. This parameter is unavailable when you select **No detect** or **Packet proportion only** for **Detect Mode**. • **pps Proportion**: specifies a proportion of a traffic type in pps (above the minimum trigger threshold) that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detect** or **Byte proportion only** for **Detect Mode**.
Proportion for Direct Alerts (%)	Specifies the proportion of a type of traffic in the aggregate to the total traffic received or transmitted by an IP address in a detection period that matches an attack signature. When this proportion is exceeded, NTA immediately generates an alert. Note The proportion for direct alerts should be greater than that for latent alerts. • **bps Proportion**: specifies a proportion of a traffic type in bps (above the minimum trigger threshold) that triggers NTA to immediately generate an alert. This parameter is unavailable when you select **No detect** or **Packet proportion only** for **Detect Mode**. • **pps Proportion**: specifies a proportion of a traffic type in pps (above the minimum trigger threshold) that triggers NTA to immediately generate an alert. This parameter is unavailable when you select **No detect** or **Byte proportion only** for **Detect Mode**.
Min Trigger Threshold (bps/pps)	Specifies the aggregate amount of traffic received or transmitted by an IP address in a detection period that matches an attack signature. It is one of the conditions triggering alerts. • **bps Threshold**: When a type of traffic in bps reaches this threshold and its proportion also reaches the related threshold, NTA generates an alert. This parameter is unavailable when you select **No detect** or **Packet proportion only** for **Detect Mode**. • **pps Threshold**: When a type of traffic in pps reaches this threshold and its proportion also reaches the related threshold, NTA generates an alert. This parameter is unavailable when you select **No detect** or **Byte proportion only** for **Detect Mode**.
Alert Level (%)	NTA supports the hierarchical structure of DDoS attack alerts and traffic anomaly alerts generated for each IP address. • **Low**: When the actual proportion of a traffic type is between 100% and 150% of the proportion for latent alerts, NTA generates a low-level alert. • **Medium**: When the actual proportion of a traffic type is between 150% and 200% of the proportion for latent alerts, NTA generates a medium-level alert. • **High**: When the actual proportion of a traffic type is more than 200% of the proportion for latent alerts, NTA generates a high-level alert.

Table 5-13 DDoS attack alert parameters (abnormal connections)

Parameter	Description
Alert Type	Currently, connection anomaly detection works only for HTTP slow attack. This parameter cannot be modified.

Parameter	Description
Detect Mode	Specifies a basis for DDoS detection and alerting. Options include No detection and Number of Connections. The Latent Alert Threshold and Direct Alert Threshold parameters can be configured after this parameter is set to Number of 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). For the setting of **Alert Latency Period**, see section 5.4.3 Alert Parameters. 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.
Diversion Level	Specifies an alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted. For the definition of alert levels, see section 5.4.3 Alert Parameters. • **Not Diversion**: generates alerts only, with no traffic diversion to take place. • **Divert Traffic of Low-level Alert**: indicates that a low-level alert or higher will trigger traffic diversion. • **Divert Traffic of Medium-level Alert**: indicates that a medium-level alert or higher will trigger traffic diversion. • **Divert Traffic of High-level Alert**: indicates that only a high-level alert can trigger traffic diversion.
Alert Hierarchy	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.

5.1.3.5 Configuring Traffic Statistics

Traffic statistics include top source IP addresses, top applications, top protocols, top TCP flags, top ports, top interfaces (DFI mode), top autonomous systems (ASs) (DFI mode), top prefixes (DFI mode), top differentiated services code points (DSCPs), top countries/regions, and top packet lengths. You can select one or more of the preceding items to include related data in traffic statistics.

5.1.3.6 Configuring Traffic Diversion Rules

You can configure the following diversion policies to handle abnormal traffic and attack traffic of a region:

- Region-specific diversion policy

  When the inbound or outbound traffic of a region becomes so abnormal as to trigger an alert that requires traffic diversion, NTA will divert traffic to or from top IP addresses in the region according to the diversion policy configured here.

- IP address-specific diversion policy

  When traffic to or from an IP address in a region becomes so abnormal as to trigger a DDoS attack alert that requires traffic diversion, NTA will divert such traffic according to the diversion policy configured here.

- Network segment-specific diversion policy

  When traffic destined for a CIDR block in the region becomes so abnormal as to trigger a network segment-specific DDoS attack alert that reaches the diversion level, NTA will divert such traffic according to the diversion policy configured here.

Note	If no IP address-specific or network segment-specific diversion policy is configured here, no traffic of an IP address or a CIDR block that triggers the policy will be diverted.

Configuring the Number of Top IP Addresses

After you specify **Number of Traffic-diverted IPs in Region**, traffic of that number of addresses in the region will be diverted to a null route after the region's inbound or outbound traffic is so abnormal as to trigger the related diversion policy. The default value of **Number of Traffic-diverted IPs in Region** is **5**. You can click  and then change the value to any integer no greater than 300.

Creating a Region-specific Diversion Policy

A region-specific diversion policy specifies how to divert a region's inbound or outbound traffic within a range.

Click **Add** in the upper-right corner of the **Region Diversion Policy** area and configure a diversion policy. Table 5-14 describes parameters for configuring a region-specific diversion policy.

A region-specific diversion policy, after being created, can be edited, deleted, and re-sorted.

Table 5-14 Parameters for configuring a region-specific diversion policy

Parameter	Description
Policy Type	Specifies whether the policy is for abnormal inbound or outbound traffic.
Detection Type	Specifies a traffic unit, which can be **bps** or **pps**.
Traffic Range	Specifies a traffic range. When traffic of a region triggers a traffic anomaly alert and is within the specified range, it will be diverted.

Parameter	Description
	The value is in the format of "number + K/M/G", containing at most two decimal places. The maximum value is 1000G. • ≥: Traffic equal to or greater than the specified value is diverted. • **to**: Traffic between the specified two values, such as 800M and 1000M, is diverted.
Diversion Type	Specifies a diversion type. It has the following values: • **No Diversion**: indicates that NTA will not divert abnormal traffic. • **BGP Diversion**: indicates that NTA will divert abnormal traffic to a third-party cleaning device. • **Null-Route Diversion**: indicates that NTA will drop abnormal traffic by diverting it to a null route.
Protection Device	Third-party cleaning device for BGP diversion. This must be specified when **BGP Diversion** is selected for **Diversion Type**. For how to configure a third-party cleaning device, see section 5.5.3 Protection Device Configuration.
Null Route IP	Destination IP address of the null route. This must be specified when **Null-Route Diversion** is selected for **Diversion Type**. For how to configure a null route IP address, see section 5.5.2 BGP Configuration.
Diversion Holding Time	Specifies how long a diversion route will remain valid. This must be specified when **BGP Diversion** or **Null-Route Diversion** is selected for **Diversion Type**. After sending a "BGP/Null-Route Diversion" notification to a device, NTA will start a countdown for the diversion. Once the diversion holding time expires, NTA revokes the diversion. **0** indicates immediate revocation of the diversion.

Creating an IP Address-specific Diversion Policy

You can configure IP address-specific policies to enable traffic diversion to be triggered by a DDoS attack alert. For different IP address ranges in a region, you can configure different diversion policies.

Click **Add** in the upper-right corner of the **IP Diversion Policy** area and configure a diversion policy. Table 5-15 describes parameters for configuring an IP address-specific diversion policy.

An IP address-specific diversion policy, after being created, can be edited, deleted, and re-sorted.

Table 5-15 Parameters for configuring an IP address-specific diversion policy

Parameter	Description
Detection Type	Specifies the traffic unit, which can be **bps**, **pps**, or **Abnormal connections**.
Traffic Range	This parameter is available only when Detection Type is set to bps or pps. Specifies a traffic range. When traffic of an IP address triggers a DDoS alert and is within the specified range, it will be diverted. The value is in the format of "number + K/M/G", containing at most two decimal

Parameter	Description
	places. The maximum value is 1000G. • ≥: Traffic equal to or greater than the specified value is diverted. • **to**: Traffic between the specified two values, such as 800M and 1000M, is diverted.
Abnormal Connections	This parameter is available only when **Detection Type** is set to **abnormal connections**. Specifics a threshold range for the number of abnormal connections that triggers an IP address-specific diversion policy. This configuration is applicable to **HTTP Slow Attack** alert. When an IP address has the specified number of abnormal connections that triggers the HTTP Slow Attack alert and is within the range specified here, its traffic will be diverted. You can type an integer in the range of 1–65535, in either format as follows. • ≥: The number of abnormal connections is equal to or greater than the specified value, such as ≥ 500**.** • **to**: The number of abnormal connections is between the specified two values, such as 400 to 500.
IP Range	Specifies an IP address or IP segment for which the traffic to be diverted is destined. It has the following values: • **Default**: indicates the diversion policy when no IP address or IP segment is matched. • **Custom**: indicates the diversion policy when the specified IP address segment is matched.
Diversion Type	Specifies a diversion type. It has the following values: • **No Diversion**: indicates that NTA will not divert attack traffic. • **Scrubbing Device Diversion**: indicates that the router forwards the traffic to the scrubbing device for cleaning upon receiving a routing notification from the scrubbing device which is notified by NTA of abnormal traffic. For how to specify such a scrubbing device for this purpose, see section 5.5.3 Protection Device Configuration. • **FlowSpec Diversion**: indicates that NTA will use FlowSpec to automatically divert traffic when detecting abnormal traffic. • **BGP Diversion**: indicates that NTA sends a BGP routing notification to the router for traffic diversion. For this purpose, you need to select a configured third-party router. For details, see section 5.5.3 Protection Device Configuration. For how to configure BGP parameters for sending routing notifications, see section 5.5.2 BGP Configuration. • **Null-Route Diversion**: indicates that NTA will drop attack traffic by diverting it to a null route.
IPv4 Diversion Netmask Length	This parameter is available when **Diversion Type** is set to **BGP Diversion**, **FlowSpec Diversion**, or **Null-Route Diversion**. The diversion netmask length is used to control the route netmask sent by NTA. The value ranges from 15 to 32, with **32** as the default value. For example, the value **32** indicates that NTA sends only one host route for diversion; the value **24** indicates that NTA sends an IP segment with a 24-bit netmask for diversion.
IPv6 Diversion Netmask Length	Specifies the diversion prefix length of the IPv6 address. This parameter is available when **Diversion Type** is set to **BGP Diversion**, **FlowSpec Diversion**, or **Null-Route Diversion**.

Parameter	Description
	The value ranges from 1 to 128, with **128** as the default value.
Null Route IP	Destination IP address of the null route. This must be specified when **Null-Route Diversion** is selected for **Diversion Type**. For how to configure a null route IP address, see section 5.5.2 BGP Configuration.
Action	This parameter is available only when **Diversion Type** is set to **FlowSpec Diversion**. • **accept**: indicates that NTA will instruct the router to accept traffic by sending a routing notification to the latter based on the FlowSpec BGP neighbor configuration. • **discard**: indicates that NTA will instruct the router to drop traffic by sending a routing notification to the latter based on the FlowSpec BGP neighbor configuration. • **rate_limit**: indicates that NTA will instruct the router to limit the traffic rate by sending a routing notification to the latter based on the FlowSpec BGP neighbor configuration. • **redirect**: indicates that NTA will instruct the router to redirect traffic by sending a routing notification to the latter based on the FlowSpec BGP neighbor configuration. • **traffic_marking**: indicates that NTA will instruct the router to mark traffic by sending a routing notification to the latter based on the FlowSpec BGP neighbor configuration.
Protective Device	Destination cleaning device for BGP diversion. This must be specified when **BGP Diversion** is selected for **Diversion Type**. A third-party device will be selected from the drop-down box for traffic cleaning. For how to configure a third-party cleaning device, see section 5.5.3 Protection Device Configuration.
FlowSpec BGP	This parameter is available only when **Diversion Type** is set to **FlowSpec Diversion**. Specifies a BGP neighbor.
Diversion Holding Time	Specifies how long a diversion route will remain valid. This must be specified when **Null-Route**, **BGP Diversion**, **Scrubbing Device Diversion**, **or FlowSpec Diversion** is selected for **Diversion Type**. After sending a "Null-Route/BGP/Scrubbing Device/FlowSpec Diversion" notification to a device, NTA will start a countdown for the diversion. Once the diversion holding time expires, NTA revokes the diversion. **0** indicates immediate revocation of the diversion.
Enable Double Diversion	Controls whether to enable double diversion. Double diversion indicates that two diversion actions can be configured for a diversion rule. For the two diversion types, the IP range is the same, but the IPv4 or IPv6 diversion prefix length can be different. For example, configure BGP1 and BGP2 diversion for a diversion policy, with the same IP range, but different prefix lengths, /24 and /32 respectively.

Creating a Network Segment-specific Diversion Policy

You can configure a network segment-specific diversion policy to divert traffic destined for a CIDR block in the region when a network segment-specific DDoS alert is triggered. For different traffic ranges, you can configure different diversion policies.

This policy can be triggered together with the **Diversion Policy for Abnormal Region Inbound Traffic** and **Diversion Policy for Abnormal Region Outbound Traffic**.

Click **Add** in the upper-right corner of the **Network Segment-specific Diversion Policy** area and configure a diversion policy. Table 5-16 describes parameters for configuring a network segment-specific diversion policy.

A network segment-specific diversion policy, after being created, can be edited, deleted, and resorted.

Table 5-16 Parameters for configuring a network segment-specific diversion policy

Parameter	Description
Detection Type	Specifies the traffic unit, which can be **bps** or **pps**.
Traffic Range	Specifies the traffic range of a network segment-specific diversion policy. When traffic to a CIDR block triggers a network segment-based DDoS alert and is within the specified range, it will be diverted. The value is in the format of "number + K/M/G", containing at most two decimal places. The maximum value is **1000G**. Two formats are available: • ≥: Traffic equal to or greater than the specified value, such as ≥ 800M, is diverted. • **to**: Traffic between the specified two values, such as **800M** and **1000M**, is diverted.
Diversion Type	Specifies a diversion type. It has the following values: • **No Diversion**: indicates that NTA will not divert attack traffic. • **Scrubbing Device Diversion**: indicates that the router forwards the traffic to the scrubbing device for cleaning upon receiving a routing notification from the scrubbing device which is notified by NTA of abnormal traffic. For how to specify such a scrubbing device for this purpose, see section 5.5.3 Protection Device Configuration. • **BGP Diversion**: indicates that NTA sends a BGP routing notification to the router for traffic diversion. For this purpose, you need to select a configured third-party router. For details, see section 5.5.3 Protection Device Configuration. For how to configure BGP parameters for sending routing notifications, see section 5.5.2 BGP Configuration. • **Null-Route Diversion**: indicates that NTA will drop attack traffic by diverting it to a null route.
IPv4 Diversion Netmask Length	This parameter is available when **Diversion Type** is set to **BGP Diversion** or **Null-Route Diversion**. The diversion netmask length is used to control the route netmask sent by NTA. The value range is 15–32, with **32** as the default. For example, the value **32** indicates that NTA sends only one host route for diversion; the value **24** indicates that NTA sends a 24-bit netmask for diversion. The value must be greater than or equal to the netmask length configured for DDoS detection, but less than or equal to this netmask plus 8. For how to configure the netmask for DDoS detection, see DDoS Attack Alert for a Network Segment.
IPv6 Diversion Netmask Length	This parameter is available when **Diversion Type** is set to **BGP Diversion** or **Null-Route Diversion**. Specifies the diversion prefix length of the IPv6 network segment. The value range is 1–128, with **128** as the default.

Parameter	Description
	The value must be greater than or equal to the prefix length configured for DDoS detection, but less than or equal to this length plus 8. For how to configure the prefix length for DDoS detection, see DDoS Attack Alert for a Network Segment.
Null Route IP	Destination IP address of the null route. This must be specified when **Null-Route Diversion** is selected for **Diversion Type**. For how to configure a null route IP address, see section 5.5.2 BGP Configuration.
Diversion holding time	Specifies how long a diversion route will remain valid. This must be specified when **Null-Route Diversion**, **BGP Diversion**, or **Scrubbing Device Diversion**, is selected for **Diversion Type**. After sending a diversion notification to a device, NTA will start a countdown for the diversion. Once the diversion holding time expires, NTA revokes the diversion. The value **0** indicates immediate revocation of the diversion.
Enable Double Diversion	Controls whether to enable double diversion. Double diversion indicates that two diversion actions can be configured for a diversion rule. For the two different diversion types, the IPv4 or IPv6 diversion prefix length can also be different.

Changing the Policy Priority

When multiple diversion policies are available, they are displayed in descending order of priority. When diverting traffic, NTA does so based on the diversion policy of the highest priority.

- Click  in the **Operation** column to raise the priority.
- Click  in the **Operation** column to lower the priority.

5.1.3.7 Configuring an IP Group and Related Policies

A region may contain different types of business. For example, a region may contain a web IP group, a game IP group, and a DNS IP group. For more accurate traffic detection, you can define an IP group for each of these businesses and configure detection and diversion rules for each IP group.

IP group configuration involves the following tasks:

- Configuring an IP Group and Related Policies
- Configuring the Auto-Learning Baseline: configuration of the function of dynamically learning DDoS attack traffic for determining baseline thresholds for an IP group

Configuring an IP Group and Related Policies

Configuration methods of IP groups and related policies are similar to those for regions. For details, see section 5.1.3 Region.

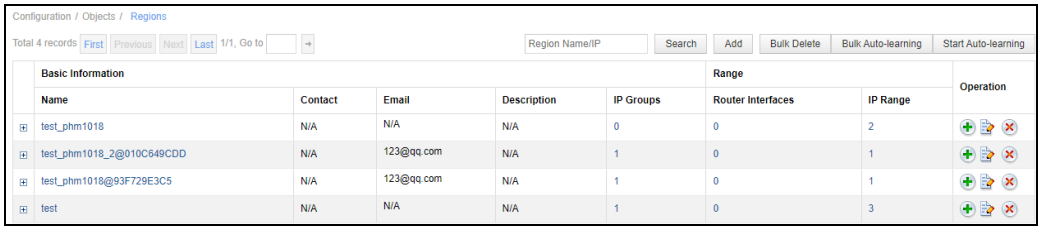
Note	If an IP address belongs to both an IP group and a region, the priority of traffic diversion policies is IP group policy > region policy > default policy. That is to say, NTA first checks traffic against the policy for the IP group and will handle the traffic accordingly if that policy is hit; otherwise, NTA uses the policy for the region and then the default policy to detect abnormal traffic.

You can configure IP groups one by one or in batches. This section describes how to configure a single IP group. For details about how to configure IP groups in batches, see section 5.2.2 Bulk Configuring IP Groups.

To create a single IP group, follow these steps:

Step 1 Choose **Configuration > Objects > Regions**.

Figure 5-1 Region list



Step 2 Click  in the **Operation** column to create an IP group.

To create an IP group, you must complete the following tasks:

a. Configure basic information such as the IP group name and notification parameters. Table 5-17 describes parameters for configuring an IP group.

Table 5-17 Parameters for configuring basic information of an IP group

Parameter	Description
IP Group Name	Name of the IP group to be monitored. This parameter is mandatory.
Description	Necessary description of the IP group. A maximum of 500 characters are allowed.
IP Group Alert Template	Specifies an alert template for this IP group. The drop-down list displays existing alert templates. For the configuration of an IP group alert template, see section 5.3.3 IP Group Alert Template.
Send Diversion Notification	Controls whether to notify the related region's contact person of the diversion by email. If you select **Yes**, when an automatic diversion for an IP address in the IP group starts and ends, NTA will send a notification to the contact email address specified during creation of the region to which the IP group belongs.
Send Alert Notification	Controls whether to notify the contact person of the related region of generated alerts by email. If you select **Yes**, when an alert related to an IP address in the IP group is generated, NTA will send a notification to the contact email address specified during creation of the region to which the IP group belongs.
Send SNMP Trap	Controls whether to send alerts and diversion logs of this IP group to the SNMP server. If you select **Yes**, NTA will send alerts and diversion logs related to the IP group to the SNMP server.

b. Configure IP addresses to be included in and excluded from the IP group.

- **Included IPs**: IP addresses to be included in the IP group for protection.
- **Exception IPs**: IP addresses excluded from the IP group because they need special or no protection.

  IP address ranges in an IP group cannot be beyond the IP address range of the region. You can enter IPv4 and/or IPv6 addresses in the following formats:

  - Range specified by a start IP address and an end IP address like 10.10.10.2-10.10.10.23 or 10.10.10.2-23
  - IP/mask: IPv4 address with a netmask ranging from 15 to 32 or IPv6 address with a prefix length ranging from 1 to 128.
  - Specific IPv4 or IPv6 address.

  When a configured IP address conflicts with an existing IP group in a region, the system prompts a message indicating the IP group name and IP address or IP segment.

c. Configure abnormal traffic alert policies.

For the configuration method and description of parameters, see section 5.1.3.3 Configuring Traffic Alert Policies.

d. Configure DDoS attack detection policies for each IP address or some network segments, including:

- Alert thresholds
- Alert hierarchy
- Diversion policy

- For IP segments in the IP group, you can enable the network segment-based detection after setting **IP Group** for **Detection Type** under **Configuration > Global Alert Settings > Network Segment-based DDoS Detection** and selecting **Open** for **Status** in the **IP Group DDoS Attack Alert for a Network Segment** area.

IP addresses in the IP group 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-based alert policy will be triggered. For the configurations and parameters, see DDoS Attack Alert for a Network Segment.

Note	To enable an IP group segment-based DDoS detection, the IP group's IP address range specified must meet the following requirements: • The IP address range must be in CIDR notation, and the difference between netmasks/prefix lengths configured is less than or equal to eight. • No exception IP address is configured for the IP group.

- For DDoS attack detection for each IP address, you can set related thresholds using either of the following methods: Choose **Inbound Detection Configuration > Fixed Threshold Configuration**, set fixed thresholds, and click **Save**.
  - For the configuration method and description of parameters, see section 5.1.3.4 Configuring DDoS Attack Detection Policies
  - Choose **Inbound Detection Configuration > Auto-learning Threshold Configuration** and configure NTA to dynamically adjust thresholds. For the description of related parameters, see Configuring the Auto-Learning Baseline.

e. Choose **Inbound Detection Configuration > Detection Rule Library Configuration** and configure the application mode and detection rules.

- **Application Mode**: **Manual** by default. In automatic mode, NTA will apply configuration changes to all detection rules in the current rule library. In manual mode, NTA will apply configuration changes only to new rules added later in the rule library. For the description of automatic application parameters, see Table 5-9.
- Detection rule: For the manual application mode, you need to select detection rules. Click **Add rule** and create an application layer, transport layer, or IP layer rule, or a custom rule.

f. Choose **Inbound/Outbound Detection Configuration** > **Constituent Proportion Configuration** and set the constituent proportions. For the description of constituent proportion configuration parameters, see Table 5-12.

g. Configure traffic statistics. For details, see section5.1.3.5 Configuring Traffic Statistics.

h. Configure diversion policies, including:

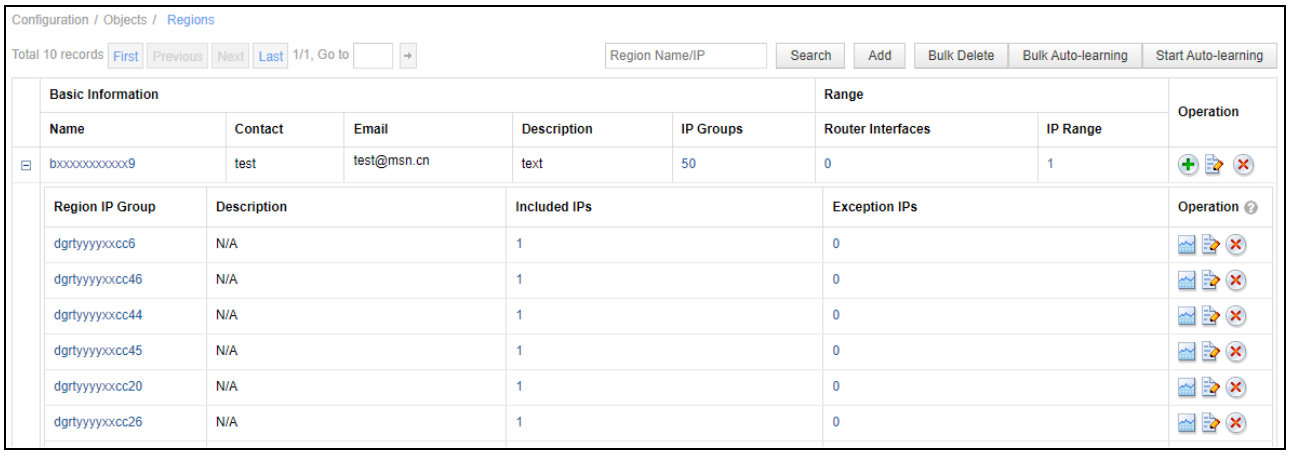
- Policies for diverting abnormal traffic received or sent by the IP group
- Policies for diverting DDoS attack traffic destined for a specific device

  For the description of related parameters, see section 5.1.3.6 Configuring Traffic Diversion Rules.

Step 3 View IP groups.

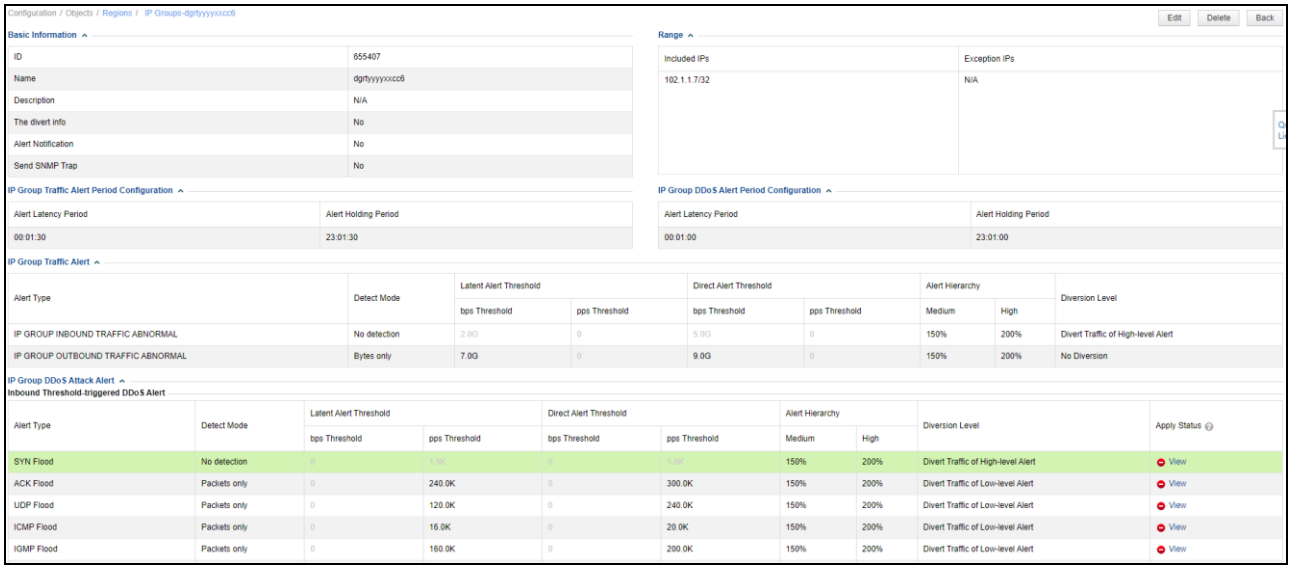
a. Click ⊞ on the left of a region name. All the existing IP groups in this region are then displayed, as shown in Figure 5-2.

Figure 5-2 IP groups included in a region



b. Click the name of an IP group. All settings of this IP group are then displayed, as shown in Figure 5-3.

Figure 5-3 Settings of an IP group



c. To modify the settings, click **Edit** in the upper-right corner. To delete this IP group, click **Delete**.

d. To return to the **Regions** page, click **Back**.

----End

Configuring the Auto-Learning Baseline

DDoS attack alerting is implemented based on alert thresholds. A too high threshold tends to cause false negatives. A too low threshold tends to cause a large number of false positives. Therefore, it is especially important to set proper thresholds. An IP group is a collection of IP addresses for similar businesses. In normal situations, the traffic of an IP group remains stable in the volume and characteristics. Therefore, NTA can automatically learn, record, and analyze network traffic of this IP group and then automatically generates proper thresholds for detecting various DDoS attacks. A baseline is the upper limit of traffic in normal situations. NTA determines such an upper limit after learning traffic over some time and uses it as an attack alert threshold. This process is called traffic auto-learning.

If traffic auto-learning has been configured, NTA dynamically adjusts DDoS attack alert thresholds according to auto-learning results. NTA can calculate thresholds at an interval specified by **Time Granularity** (see section 5.4.5 Auto-learning Baseline Parameters) based on traffic learned in a day or seven days and then dynamically adjust these thresholds.

Traffic auto-learning is performed in three steps:

- After traffic auto-learning starts, NTA learns live traffic and, based on the actual traffic trend, generates latent alert thresholds using an appropriate algorithm.
- Based on global traffic auto-learning parameters, NTA generates direct alert thresholds and then raises the thresholds according to the auto-learning policy. For the configuration of global traffic auto-learning parameters, see section 5.4.5 Auto-learning Baseline Parameters.
- Apply thresholds to the IP group in either of the following ways:
  - Direct application

– Manual application: Edit thresholds before manually applying them.

NTA can detect DDoS attacks according to dynamic thresholds only after these thresholds are applied.

Traffic auto-learning configuration includes starting learning, stopping learning, editing learning results, and applying baseline thresholds.

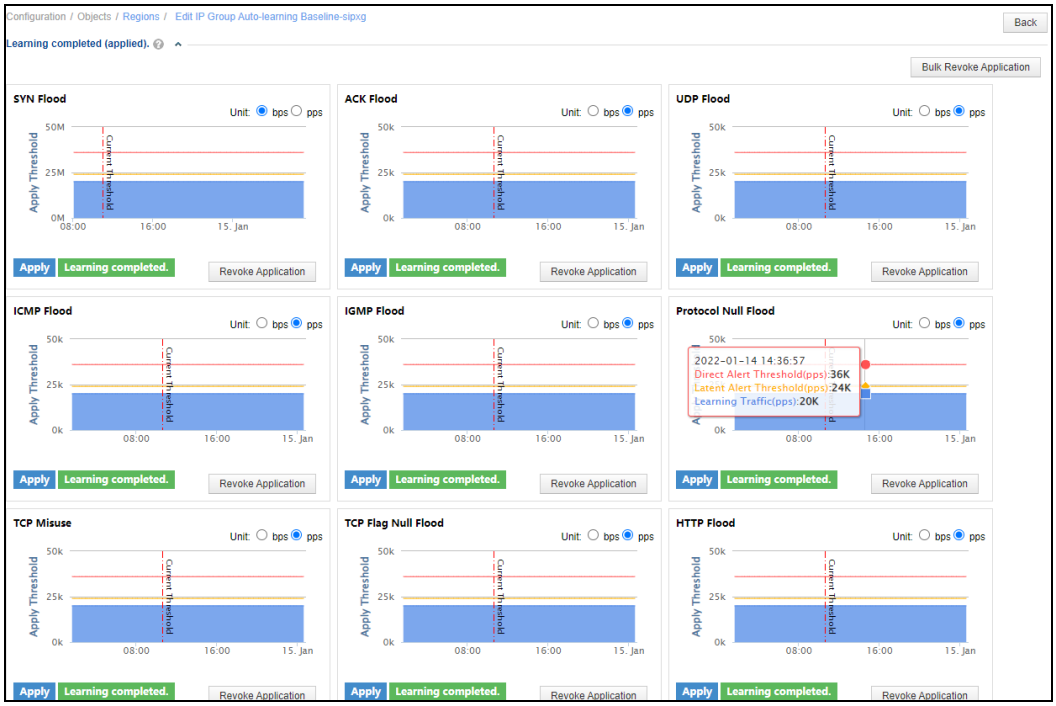
The procedure is as follows:

Step 1 Choose **Configuration > Objects > Regions**.

Click ⊞ on the left of a region name. All the existing IP groups in this region are then displayed.

Step 2 Click  in the **Operation** column to open the **Edit IP Group Auto-learning Baseline** page.

Figure 5-4 Edit IP Group Auto-learning Baseline page



By default, the page displays the traffic learning status for all DDoS attacks, which can be:

- **Not learned**: indicates that traffic learning has not started. For a new IP group, the traffic learning status for all attack types is **Not learned**.
- **Learning**: indicates that the learning process is ongoing.
- **Learning failed**: indicates that traffic learning failed due to system exceptions.
- **Learning completed**: indicates that traffic learning has been completed.

For each attack type, you can start, stop, and resume learning.

Step 3 Start learning.

a. Click **Start Learning** in the area of a certain attack type and configure parameters in the dialog box that appears. Alternatively, you can click **Bulk Learn** to start learning for all attack types that are in the **Not learned** state. Click **OK** to commit the settings. Then NTA starts learning and the status changes to **Learning**, as shown in Figure 5-5.

Table 5-18 describes parameters for configuring traffic auto-learning.

Table 5-18 Parameters for configuring traffic auto-learning

Parameter	Description
Learning Duration	Specifies the duration from when learning starts till it ends.
After learning is completed	Specifies when baseline thresholds are applied. • **Apply immediately**: indicates that baseline thresholds are applied for DDoS attack detection immediately after traffic auto-learning is completed. • **Not apply**: indicates that fixed thresholds are still used after traffic auto-learning is completed. In this case, you need to perform manual operations to make the baseline thresholds take effect. For details, see Step 6. Note In practice, thresholds are raised according to related global settings. For details, see section 5.4.5 Auto-learning Baseline Parameters.
Minimum bps	Specifies the lower limit for the traffic rate in bps. When the actual traffic rate is lower than the minimum bps specified here, NTA uses the latter for baseline threshold calculation.
Minimum pps	Specifies the lower limit for the traffic rate in pps. When the actual traffic rate is lower than the minimum pps specified here, NTA uses the latter for baseline threshold calculation.

Figure 5-5 Auto-learning in progress

Step 4 When the learning is complete, click **OK** to commit the learned information.

a. When the specified learning duration expires, NTA automatically stops learning.

b. You can also manually stop learning. To do so, click **Stop Learning** for a certain attack type. Alternatively, click **Bulk Stop** to stop learning for all attack types that are in the **Learning** state.

c. Handle learning results in either of the following ways:

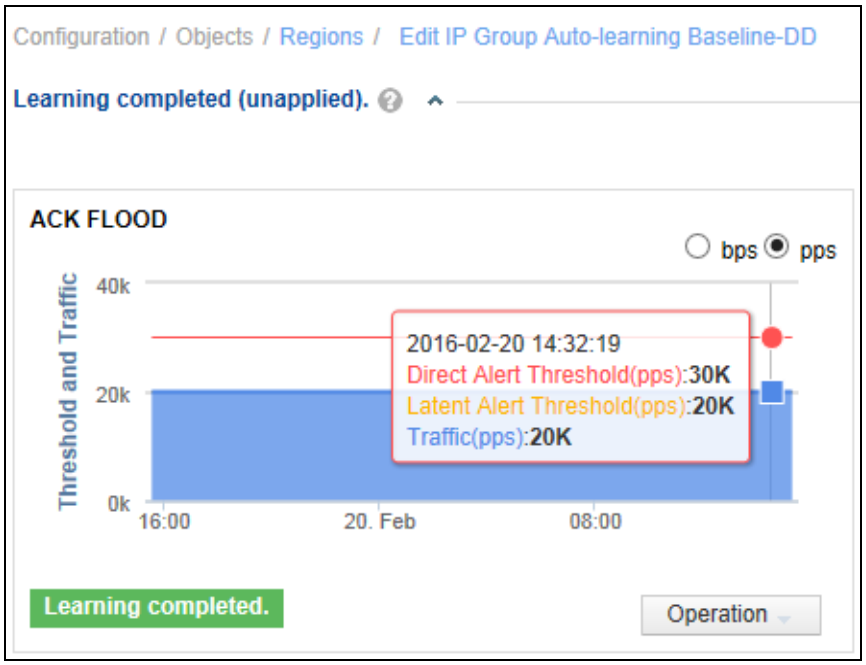
- **Save learning result**: indicates that the learning result will be saved. In this case, when at least one value is determined based on the learning result, NTA deems the learning to be successful.
- **Drop learning result**: indicates that the learning result will not be saved. In this case, the learning status changes to **Learning failed**.

Step 5 Edit baseline data.

Learning results are displayed in the **Learning completed** area. From the curves, you can view the direct alert threshold, latent alert threshold, and traffic trend during the learning period. Pointing to a specific position on a curve displays threshold and traffic values at that specific point of time.

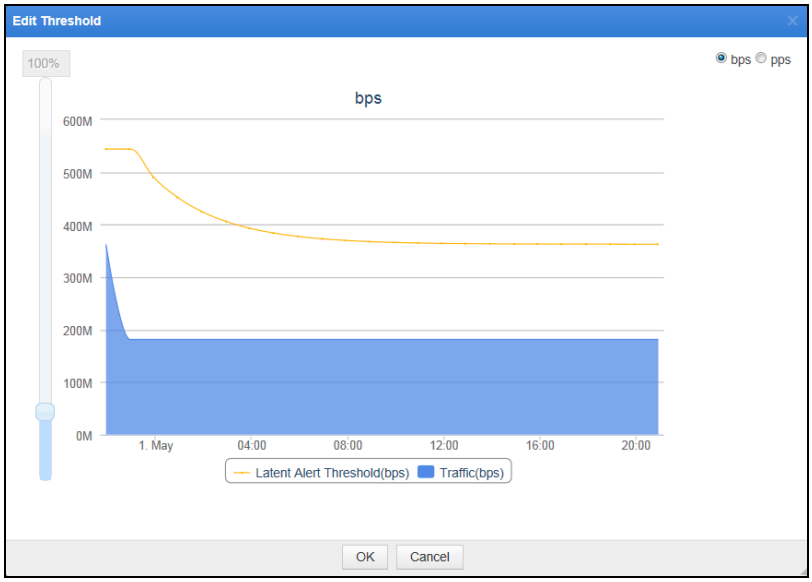
a. If **Not apply** is selected during auto-learning configuration, the learning result is displayed, as shown in Figure 5-6.

Figure 5-6 Baseline data obtained through auto-learning



b. Click **Operation** and then choose **Edit** from the drop-down menu. You can adjust only the latent alert threshold, as shown in Figure 5-7.

Figure 5-7 Edit Threshold page



A scroll bar is available on the left for you to increase or decrease the thresholds as a whole. You can also drag any point on the curve up or down to increase or decrease the value at that point of time.

c. After the adjustment, click **OK**.

Step 6 Apply baseline thresholds.

If you select **Not apply** for the learning result, you can later manually apply the threshold to the IP group for the related attack type.

a. Click **Operation** on the page shown in Figure 5-6 and then choose **Apply** from the drop-down menu. Then the learning result is applied for attack detection.

b. Click **Bulk Operation** and then choose **Apply** from the drop-down menu. Then you can make unapplied baseline thresholds take effect immediately.

Step 7 (Optional) Re-learn baseline thresholds.

Click **Operation** on the page shown in Figure 5-6 and then choose **Re-learn** from the drop-down menu.

----End

5.2 Bulk Configuration

This section describes how to configure regions and IP groups in batches.

5.2.1 Bulk Configuring Regions

Choose **Configuration** > **Bulk Configure** > **Regions**. You can click **Add** repeatedly to add multiple regions. After the configuration, click **Save**.

Table 5-19 describes parameters for configuring a region.

Table 5-19 Region configuration parameters

Parameter	Description
Region Name	Name of the new region. This parameter is mandatory.
IP Range	IP addresses, IP subnets, and IP segments covered by the region. This parameter is mandatory.
Region Alert Template	Alert template for the region.

5.2.2 Bulk Configuring IP Groups

IP groups can be configured one by one or in bulk. For how to configure an IP group, see Configuring an IP Group and Related Policies. The following describes how to configure IP groups in bulk.

Choose **Configuration** > **Bulk Configure** > **IP Groups**. Click **Add** repeatedly to add multiple IP groups. After the configuration, click **Save**.

Table 5-20 describes parameters for configuring an IP group.

Table 5-20 IP group configuration parameters

Parameter	Description
Region Name	Region to which the IP group belongs.
IP Group Name	Name of the new IP group. This parameter is mandatory.
Included IPs	IP addresses, IP subnets, and IP segments to be included in the IP group for protection. This parameter is mandatory.
Exception IPs	IP addresses excluded from the current IP group because they need special or no protection.
IP Group Alert Template	Alert template for the IP group.

5.2.3 Bulk Configuring Auto-Learning

To configure auto-learning in batches for multiple regions, follow these steps:

Step 1 Choose **Configuration** > **Objects** > **Regions**.

Step 2 Click **Bulk Auto-learning** in the upper-right corner of the page.

Check boxes appear in the leftmost column.

Step 3 Select one or more regions, click **Bulk Auto-learning** again, and configure parameters.

For the description of parameters, see Table 5-18.

Step 4 Click **OK** to commit the settings.

Then NTA begins to automatically learn traffic of these regions.

----End

5.2.4 One-Click Auto-Learning

The one-click auto-learning function can instruct the engine to automatically learn traffic from IP groups in all regions based on the traffic auto-learning parameters, helping improve configuration efficiency. For details, see section 5.2.3 Bulk Configuring Auto-Learning.

Note	• One-click auto-learning is invalid for IP groups in Learning failed, Learning completed, or Applied state. • One-click auto-learning can cover up to 60 IP groups each time.

5.3 Alert Templates

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

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

5.3.1 Router Alert Template

NTA in DPI mode does not support this function.

A router alert template is used to define bandwidth usage alert and performance alert parameters. After being configured, a router alert template can be referenced for adding a router, thereby simplifying parameter configuration.

Choose **Configuration** > **Alert Configuration Template** > **Router Alert Template**. Initially, the page lists only the default template. Click **Add** and configure bandwidth usage alert, CPU usage alert, memory usage alert, and data collection anomaly alert (SNMP data collection and flow data collection) policies as well as traffic statistics in a template. Table 5-21 describes parameters for defining such a template.

After being created, a template can be edited and deleted. The default template cannot be deleted.

Table 5-21 Parameters for configuring a router alert template

Parameter	Description
Template Name	Specifies the name of the template to be created.
Alert or not	Controls whether to enable alerting. An alerting policy can take effect only after this function is enabled.
Latent Alert Threshold	Specifies the bandwidth, CPU, or memory usage threshold that triggers NTA to generate an alert only after the usage stays at this level for some time.
Direct Alert Threshold	Specifies the bandwidth, CPU, or memory usage threshold that triggers NTA to generate an immediate alert.

Parameter	Description
	Note The direct alert threshold must be greater than the latent alert threshold.
Alert Threshold	Specifies the threshold for data collection interruption duration. When data collection is interrupted for a period longer than the value configured here, NTA immediately generates an alert.
Traffic Statistics	Specifies statistical items of traffic.

5.3.2 Region Alert Template

A region alert template is used to define traffic alert parameters, DDoS attack alert parameters, traffic statistics, and traffic diversion rules. After being configured, a region alert template can be referenced for adding a region, thereby simplifying parameter configuration.

To configure a region alert template, follow these steps:

Step 1 Choose **Configuration** > **Alert Configuration Template** > **Region Alert Template**.

Initially, the page lists only the built-in template.

Step 2 Click **Add**.

The page for adding a template appears.

Step 3 Configure basic information.

Type the template name and click **Next**.

Step 4 Configure region traffic alert parameters.

For the configuration method and description of parameters, see section 5.1.3.3 Configuring Traffic Alert Policies.

Step 5 Configure region DDoS attack alert parameters.

For the configuration method and description of parameters, see section 5.1.3.4 Configuring DDoS Attack Detection Policies.

Step 6 Configure traffic statistics.

For the configuration method and description of parameters, see section 5.1.3.5 Configuring Traffic Statistics.

Step 7 Configure traffic diversion rules.

For the configuration method and description of parameters, see section 5.1.3.6 Configuring Traffic Diversion Rules.

Step 8 Click **Complete** to commit the settings.

Step 9 (Optional) View and edit templates.

a. In the template list, click  in the **Operation** column to modify parameter settings.

b. In the template list, click a template name to view all its settings. A shortcut link is available on this page for you to quickly navigate to the desired area.

Step 10 Apply the template.

In the template list, click  in the **Operation** column of the edited template and apply it to the specified regions.

----End

Note	The built-in region alert template cannot be deleted.

5.3.3 IP Group Alert Template

An IP group alert template is used to define traffic alert parameters, DDoS attack alert parameters, traffic statistics, and traffic diversion rules. After being configured, an IP group alert template can be referenced for adding an IP group, thereby simplifying parameter configuration.

Choose **Configuration > Alert Configuration Template > IP Group Alert Template**. Initially, the page lists only the built-in template. The configuration method is similar to that for region alert templates. For details, see section 5.3.2 Region Alert Template.

5.4 Global Alert Settings

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

- Default DDoS Attack Detection Thresholds
- Network Segment-based DDoS Detection
- Alert Parameters
- Alert Plug-in Management
- Auto-learning Baseline Parameters
- Traffic Statistics
- Fast Alert

5.4.1 Default DDoS Attack Detection Thresholds

If a destination IP address does not belong to any IP group or region, NTA determines whether the IP address is the target of a DDoS attack based on default DDoS attack detection thresholds. You can view and modify these default settings on the **Default DDoS Attack Alert Threshold** page. The priority of default DDoS attack detection is lower than that of regions and IP group protection policies.

Choose **Configuration > Global Alert Settings > Default DDoS Attack Detection Threshold**. The **Default DDoS Attack Alert Threshold** page displays default detection modes and parameters for all built-in DDoS attack types. Click an attack alert type in the left widget and then you can modify its parameters in the right widget. For the description of these parameters, see Table 5-11. After the modification, click **Save** to commit the changes.

5.4.2 Network Segment-based DDoS Detection

This detection determines whether a CIDR block aggregated by the configured network/prefix length is attacked. If the aggregate traffic destined for a CIDR block that matches an attack signature exceeds the global threshold, a network segment-based DDoS alert will be generated.

Choose **Configuration > Global Alert Settings > Network Segment-based DDoS Detection** and configure parameters. Table 5-22 describes parameters for configuring a network segment-based DDoS detection policy.

Table 5-22 Parameters for configuring a network segment-based DDoS detection policy

Parameter		Description
Basic Settings	Detection Type	Specifies a network segment to be detected. Options include the following: • **No detection**: detects no DDoS attacks for network segments. • **Global**: detects DDoS attacks across the entire set of IP addresses protected by the device. If this is selected, even if a matched IP address belongs to a region/IP group, its traffic is still counted in global DDoS detection statistics. • **Region**: detects DDoS attacks on the IP address range covered by a region. If this is selected, even if a matched IP address belongs to an IP group, its traffic is still counted in the DDoS detection statistics of the region to which the IP group belongs. • **IP group**: detects DDoS attacks on the IP address range covered by an IP group. If this is selected, only traffic of IP addresses in an IP group is counted in DDoS detection statistics of that IP group.
Netmask/Prefix Length Settings	This parameter is available only when **Global** is selected for **Detection Type**.	
	IPv4 Netmask	Specifies the IPv4 netmask length. The value range is 16–30, with **24** as the default.
	IPv6 Prefix Length	Specifies the IPv6 prefix length. The value range is 64–126, with **120** as the default.
Global Network Segment-based DDoS Detection Thresholds	Specifies parameters for a global network segment-based DDoS detection policy.	
	Alert Type	Type of DDoS attack alerts. Currently, 27 types of attacks can be alerted, which cannot be edited.
	Detect Mode	Specifies a measurement basis for the network segment-based DDoS detection and alerting. The default value is **No detection**. • **No detection**: indicates that NTA does not check whether the inbound traffic exceeds pps and bps thresholds. • **Packets only**: indicates that NTA checks whether the inbound traffic exceeds the pps threshold and, if yes, generates an alert. • **Bytes only**: indicates that NTA checks whether the inbound traffic exceeds the bps threshold and, if yes, generates an alert. • **Both packets and bytes**: indicates that NTA checks whether the inbound traffic exceeds both the pps and bps thresholds and, if yes, generates an alert. • **Either packets or bytes**: indicates that NTA checks whether the inbound traffic exceeds either the pps or bps threshold and, if yes,

		generates an alert.
	Latent Alert Threshold	Specifies a global threshold for the aggregate inbound traffic of a network segment in a detection period that matches an attack signature. When traffic exceeds this threshold, but is below the direct alert threshold, NTA does not generate an alert until the traffic rate stays above this threshold for some time (alert latency period).  **Caution** • The latency alert threshold must be lower than the direct alert threshold. • The format is number + K/M/G, such as 800M or 100K. • **bps Threshold**: specifies a threshold in bps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: specifies a threshold in pps that triggers NTA to stay latent for some time before generating an alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
	Direct Alert Threshold	Specifies a global threshold for the aggregate inbound traffic of a network segment in a detection period that matches an attack signature. When traffic exceeds this threshold, NTA immediately generates an alert.  **Caution** • The direct alert threshold should be greater than the latency alert threshold. • The format is number + K/M/G, such as 800M or 100K. • **bps Threshold**: specifies a threshold in bps that triggers NTA to immediately generate an alert. This parameter is unavailable when you select **No detection** or **Packets only** for **Detect Mode**. • **pps Threshold**: specifies a threshold in pps that triggers NTA to immediately generate an alert. This parameter is unavailable when you select **No detection** or **Bytes only** for **Detect Mode**.
	Diversion Level	Specifies an alert level for traffic diversion. When an alert of the specified level or above is generated, traffic will be diverted. For the definition of alert levels, see section 5.4.3 Alert Parameters. • **Not Diversion**: generates alerts only, with no traffic diversion to take place. • **Divert Traffic of Low-level Alert**: indicates that a low-level alert or higher will trigger traffic diversion. • **Divert Traffic of Medium-level Alert**: indicates that a medium-level alert or higher will trigger traffic diversion. • **Divert Traffic of High-level Alert**: indicates that only a high-level alert can trigger traffic diversion.
	Alert Hierarchy (%)	Specifies the hierarchical structure of DDoS attack alerts and traffic anomaly alerts generated for each network segment under detection. • **Medium**: specifies the lowest proportion to trigger a medium-level alert. The default value is **150**, and the maximum value is 10000. When the actual proportion is higher than the lowest proportion triggering a

		medium-level alert 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**, and the maximum value is 10000. When the actual proportion is higher than the lowest proportion triggering a high-level alert, NTA always generates a high-level alert.

5.4.3 Alert Parameters

When detecting a DDoS attack, abnormal traffic, abnormal router interface usage and performance, or NTA system exception, NTA generates an alert. Alerts are classified into low, medium, and high levels based on the deviation from the threshold.

On the **Alert Parameters** page, you can define the alert classification policy, alert latency period, and alert holding period.

Choose **Configuration > Global Alert Settings > Alert Parameters**. The page displays default alert parameters (see Table 5-23). Alert levels on this page are defined based on the traffic in a detection period specified for the latent alert threshold. Alert levels are classified according to the proportion of actual traffic to the **Latent Alert Threshold** value. Table 5-23 describes parameters for defining global alerts.

Table 5-23 Global alert parameters

Parameter	Description
Low-level Alert Percentage(%)	Specifies the lowest proportion that triggers a low-level alert: • **DDoS attack alert**: cannot be edited. • **Region/IP group Traffic Alert Hierarchy**: cannot be edited. • **Threat Intelligence Alert Hierarchy**: cannot be edited. • **Router Interface Bandwidth Usage Alert Hierarchy**: The default value is **100**, which indicates 100% of the latent alert threshold and cannot be edited. When the actual traffic is more than 100% of the latent alert threshold but less than the lowest proportion for triggering a medium-level alert, a low-level alert is triggered. NTA supports this only when in DFI mode. • **Router Performance Alert Hierarchy**: same as the description of **Router Interface Bandwidth Usage Alert Hierarchy**. NTA supports this only when in DFI mode. • **Device Performance Alert Hierarchy**: same as the description of **Router Interface Bandwidth Usage Alert Hierarchy**.
Medium-level Alert Percentage(%)	Specifies the lowest proportion that triggers a medium-level alert: • **DDoS attack alert**: cannot be edited. • **Region/IP group Traffic Alert Hierarchy**: cannot be edited. • **Threat Intelligence Alert Hierarchy**: cannot be edited. • **Router Interface Bandwidth Usage Alert Hierarchy**: The default value is **150** and the maximum value is **10000**. When the actual traffic is more than 150% of the latent alert threshold but less than the lowest proportion for triggering a high-level alert, a medium-level alert is triggered. NTA supports this only when in DFI mode.

Parameter	Description
	• **Router Performance Alert Hierarchy**: same as the description of **Router Interface Bandwidth Usage Alert Hierarchy**. NTA supports this only when in DFI mode. • **Device Performance Alert Hierarchy**: same as the description of **Router Interface Bandwidth Usage Alert Hierarchy**.
High-level Alert Percentage(%)	Specifies the lowest proportion that triggers a high-level alert: • **DDoS attack alert**: cannot be edited. • **Region/IP group Traffic Alert Hierarchy**: cannot be edited. • **Threat Intelligence Alert Hierarchy**: cannot be edited. • **Router Interface Bandwidth Usage Alert Hierarchy**: The default value is **200** and the maximum value is **10000**. When the actual traffic is more than 200% of the latent alert threshold, a high-level alert is triggered. NTA supports this only when in DFI mode. • **Router Performance Alert Hierarchy**: same as the description of **Router Interface Bandwidth Usage Alert Hierarchy**. NTA supports this only when in DFI mode. • Device Performance Alert Hierarchy: same as the description of Router Interface Bandwidth Usage Alert Hierarchy.
Alert Latency Period	Specifies the time when NTA stays latent before generating an alert for traffic that remains at a specified level for some time. This is conducive to reduction of false positives. For example, if you want NTA to generate an alert when the traffic stays above 1 Gbps for at least 60 seconds, you can set the latent alert threshold to **1** Gbps and the alert latency period to **60** seconds. • **h**: ranges from 0 to 23. • **m**: ranges from 0 to 59. • **s**: The value can only be **0** or **30**.
Alert Holding Period	Specifies the time when an alert persists after the traffic rate falls below the threshold, which indicates that the attack ends. This is conducive to reduction of repeated alerts on the same event. For example, the alert holding period is set to **60** seconds. When the alerted traffic falls below the alert threshold, NTA starts a 60-second countdown. If the traffic stays below the alert threshold throughout this period, the alert is cleared when the countdown ends. • **h**: ranges from 0 to 23. • **m**: ranges from 0 to 59. • **s**: The value can only be **0** or **30**.
NTA Performance Alert Thresholds	Specifies thresholds of NTA's CPU, memory, and disk usage, and CPU/motherboard temperature. When any usage or temperature exceeds the related threshold set here, an alert is triggered.

5.4.4 Alert Plug-in Management

NTA has the following alert plug-ins:

- Traffic alert plug-in: checks whether inbound and outbound traffic of a region or an IP group is abnormal. For details, see section 5.4.4.1 Managing the Traffic Alert Plug-In.
- Router alert plug-in: checks whether the router interface usage and performance are abnormal. For details, see section 5.4.4.2 Managing the Router Alert Plug-In.
- System performance alert plug-in: checks whether NTA performance is abnormal. For details, see section 5.4.4.3 Managing the System Performance Alert Plug-In.
- Detection rule library plug-in: provides common detection rules. For details, see section 5.4.4.4 Managing the Detection Rule Library Plug-In.
- Attack alert plug-ins, classified into the following:
  - Custom attack alert plug-in: contains user-defined attack signatures. For details, see section 5.4.4.5 Managing the Custom Attack Alert Plug-In.
  - Built-in attack alert plug-in: contains common attack signatures. For details, see section 5.4.4.6 Managing the Built-in Attack Alert Plug-In.

Choose **Configuration > Global Alert Settings > Alert Plug-in Management**. Each type of plug-in contains one or more child plug-ins, which are enabled by default.

5.4.4.1 Managing the Traffic Alert Plug-In

The traffic alert plug-in consists of four child alert plug-ins for inbound/outbound traffic of regions and IP groups respectively. Clicking or in the **Operation** column enables or disables a child plug-in. After a child plug-in is disabled, the related detection policy loses effect.

5.4.4.2 Managing the Router Alert Plug-In

NTA in DPI mode does not support this function.

The router alert plug-in consists of child alert plug-ins for bandwidth usage, CPU usage, memory usage, SNMP data collection anomaly, and flow data collection anomaly of a router. Clicking or in the **Operation** column enables or disables a child plug-in. After a child plug-in is disabled, the related detection policy loses effect.

5.4.4.3 Managing the System Performance Alert Plug-In

The system performance alert plug-in consists of child alert plug-ins for CPU usage, memory usage, hard disk usage, CPU temperature, motherboard temperature, and fan status of NTA. Clicking or in the **Operation** column enables or disables a child plug-in. After a child plug-in is disabled, the related detection policy loses effect.

5.4.4.4 Managing the Detection Rule Library Plug-In

This plug-in provides information about the built-in detection rule library, including the library version number and the number of detection rules in the library.

5.4.4.5 Managing the Custom Attack Alert Plug-In

Click **Add Custom Alert** and configure parameters (Table 5-24). Then click **OK** to return to the custom alert plug-in list. Click in the **Operation** column and configure parameters (0). Then click **Save** to commit the settings.

A custom attack alert plug-in, after being created, can be enabled, disabled, edited, and deleted. Also, you can click to view its rule.

Table 5-24 Parameters for creating a custom attack alert plug-in

Parameter	Description
Alert Name	Name of the custom attack alert plug-in, which should be a string of up to 20 characters.
Alert ID	ID of the custom attack alert plug-in, which should be in the range of 129–200.
Alert Description	Description of the custom attack alert plug-in.
Enable Now	Controls whether to enable the custom attack alert plug-in immediately.

Table 5-25 Parameters for configuring attack signatures of a custom attack alert plug-in

Parameter	Description
Basic Feature Attribute	Basic attributes include **Protocol Field**, **Application Name**, **Source/Destination Port**, **Source/Destination AS** (unavailable in DPI mode), **Source/Destination Group ID**, **Inbound/Outbound Interface Index** (unavailable in DPI mode), **Bytes/flow**, **Packets/flow**, **Source/Destination IPv4 Range**, **Source/Destination IPv6 Range**, and **Average Packet Length**.
TCP Flag	Allows arbitrary combinations of TCP flags.
Equivalent Attribute	Specifies attributes that have the same value on both the source and destination sides. You can select arbitrary attributes for this purpose, for example, **IP** (indicating the source and destination IP addresses are the same) and **Port** (indicating the source and destination ports are the same).

5.4.4.6 Managing the Built-in Attack Alert Plug-In

The built-in attack alert plug-in consists of more than 20 child alert plug-ins, which can be enabled and disabled and whose rules can be viewed. Among these child plug-ins, the UDP flood alert plug-in allows you to enable or disable UDP reflection attack detection.

- **Enable**: When detecting a UDP reflection attack, NTA triggers a reflection attack alert rather than the UDP flood alert.
- **Disable**: NTA only checks for non-reflection UDP flood attacks.

5.4.5 Auto-learning Baseline Parameters

Traffic auto-learning is a process whereby NTA automatically learns live traffic and determines proper thresholds, which can be adapted to different scenarios. Here is a description of how global parameters are configured for an IP group. For specific learning policies, see Configuring the Auto-Learning Baseline.

Choose **Configuration > Global Alert Settings > Auto-learning Baseline Parameters**. By default, the page lists the built-in auto-learning baseline policy, which cannot be re-sorted or deleted.

Configuring Auto-learning Baseline Parameters

On the **Auto-learning Baseline Parameters** page, you can configure the direct alert threshold growth rate, auto-learning policy (click **Add** and configure parameters), and time granularity

(click **Advanced Settings** and type a value). After configuration, click **OK** to commit the settings. Table 5-26 describes auto-learning baseline parameters.

Table 5-26 Auto-learning baseline parameters

Parameter		Description
Baseline Direct Alert Threshold Growth Rate		The auto-learning result is the basis of determining the latent alert threshold. The direct alert threshold is the product of the latent alert threshold multiplied by the value specified here. The value range is 120–1000, with **150** as the default indicating 150%.
Policy	Time Adjustment Multiple	• On particular days, traffic may rise sharply. You can specify days during which the latent alert threshold and direct alert threshold will be automatically raised to reduce false positives. • A traffic auto-learning policy specifies when and how much the growth rate needs to be adjusted. After a latent alert threshold is raised, the direct alert threshold is raised accordingly.
Advanced Settings		Specifies the interval from when the threshold is calculated till it is applied for DDoS attack detection. The default value is **60** minutes. The time granularity has a direct impact on the overall NTA performance and may cause unpredictable performance problems. Therefore, you are advised not to change the default value.

Re-sorting the Auto-learning Baseline Policies

The default policy is always at the bottom of the list. Other policies are sorted in the reverse order of creation time by default.

The latest policy stands at the top of the list, with the highest priority. You can click  or  to move a policy up or down.

5.4.6 Traffic Statistics

Choose **Configuration > Global Alert Settings > Traffic Statistics** and configure statistical items. For details, see section 5.1.3.5 Configuring Traffic Statistics.

5.4.7 Fast Alert

This function is available only in DPI mode.

Choose **Configuration > Global Alert Settings > Fast Alert**, enable or disable the function, and click **Save**.

- After the fast alert function is enabled, the detection cycle can be as fast as only several seconds. NTA generates an alert as soon as the traffic reaches twice the direct alert threshold.
- After the fast alert function is disabled, the detection cycle changes to 30 seconds.

Note	Fast alerting does not work for constituent proportion detection.

5.5 Global Diversion Settings

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

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

5.5.1 Default Diversion Configuration

You can configure a default diversion policy to divert DDoS attack traffic that does not match any policies. The default diversion policy includes an IP diversion policy and a network segment-specific diversion policy.

Choose **Configuration** > **Global Divert Settings** > **Default Diversion Configuration**. The page lists the built-in global diversion policy by default, which cannot be re-sorted or deleted.

Configuring a Global Default Diversion Policy

Configure global default diversion policies. Table 5-27 describes these parameters.

Table 5-27 Global default diversion parameters

Parameter		Description
Send Diversion Notification		Specifies whether to send diversion notifications when the diversion starts and ends. After you click **Enable Now**, the setting takes effect immediately. After this is enabled, NTA sends diversion notification emails to the designated receiving email address when automatic diversion starts and ends for an IP address not in any region or IP group. For how to configure a receiving email address, see section 4.3.1.1 Configuring Mail Settings.
IP Diversion Policy	You can click **Add** and configure different diversion policies for DDoS attack traffic of different levels and IP address ranges.	
	Detection Type	Unit of measure, which can be **bps** or **pps**.
	Traffic Range	Specifies a traffic range. When traffic of an IP address within the specified IP range triggers a DDoS alert and is within the specified range, it will be diverted. The value is in the format of "number + K/M/G", containing at most two decimal places. The maximum value is 1000G. • ≥: Traffic equal to or greater than the specified value is diverted. • **to**: Traffic between the specified two values, such as **800M** and **1000M**,

Parameter		Description
		is diverted.
	IP Range	Specifies a single IP address or an IP address range covered by the policy. For example, when traffic from an IP address triggers a DDoS alert and both the traffic and the IP address are within the specified ranges, NTA initiates traffic diversion.
	Diversion type	Specifies a diversion type. For details, see Table 5-15.
	Enable Double Diversion	After this is enabled, two diversion policies will work for an attacked IP address so that traffic will be diverted to two BGP neighbors.
Network segment-specific diversion policy	Specifies the diversion policy for a global CIDR block when the network segment-based DDoS alert is triggered. You can click **Add** and configure different diversion policies for DDoS attack traffic of different levels.	
	Detection Type	Specifies the traffic unit, which can be **bps** or **pps**.
	Traffic Range	Specifies the traffic range of a network segment-specific diversion policy. When the inbound traffic of a CIDR block triggers a network segment-based DDoS alert and is within the specified range, it will be diverted. The value is in the format of "number + K/M/G", containing at most two decimal places. The maximum value is **1000G**. Two formats are available: • ≥: Traffic equal to or greater than the specified value, such as **≥ 800M**, is diverted. • **to**: Traffic between the specified two values, such as **800M** and **1000M**, is diverted.
	Diversion Type	Specifies the type of traffic diversion. For details, see Table 5-16.
	Enable Double Diversion	Controls whether to enable double diversion. Double diversion indicates that two diversion actions can be configured for a diversion rule, meaning the diversion type must be different.

Re-sorting Global Diversion Policies

The built-in policy is always at the bottom of the list. Other policies are sorted in the reverse order of creation time by default. The traffic is matched against diversion policies one by one from top to bottom. Once a policy is hit, the traffic is diverted accordingly.

The latest policy stands at the top of the list, with the highest priority. You can click or to move a policy up or down.

5.5.2 BGP Configuration

To implement null route or BGP diversion, NTA must establish iBGP neighborship with a router. Only in this way can NTA advertise route update notifications for diversion of attack traffic to a null route IP address for dropping or a third-party device for cleaning. This module allows you to configure parameters for establishing a BGP session.

Choose **Configuration > Global Divert Settings > BGP Configuration**.

Initially, the BGP configuration list is empty.

Configuring a Global BGP Diversion Policy

Click **Add** in the upper-right corner of the **BGP Configuration** page and configure parameters.

Table 5-28 describes BGP session parameters.

Table 5-28 BGP session parameters

Parameter	Description
Name	Specifies a string that identifies the entry.
Local AS	Specifies the local AS number, which must be the same as that of the BGP neighbor; otherwise, neighborship cannot be established.
Local Port	Specifies the source port for data exchange with BGP neighbors. Generally, it is port 179.
Bind IP	Specifies the local IP address used by NTA to establish the BGP neighborship. When two NTA devices constitute a master/backup pair for HA and the local device is a master one, you must select a virtual IP address.
Management Port	Specifies the management port of the local route analysis module. The default value is recommended.
Keep Alive	Specifies the interval for sending keepalive messages to a BGP neighbor to ensure that the link with the neighbor is operating. The default value is **60** seconds.
Hold Time	Specifies the maximum time BGP waits between successive messages before closing the connection. Generally, it is 180 seconds.
Maximum Routing Entries	Specifies the maximum number of routing entries that NTA can send in a session based on this BGP entry. This can prevent router performance from deteriorating because of NTA sending too many BGP messages.
Community	Specifies how the BGP-speaking router treats this route. A maximum of five community strings are allowed, with each one in a separate line. • **no-advertise**: If this parameter is set to **YES**, it indicates that this route is not advertised to any BGP peers. • **no-export**: If this parameter is set to **YES**, it indicates that this route is not advertised to other ASs. • Parameters other than **no-advertise** and **no-export** should be typed in the text box to the right of **Community** in the format of xxx:xxx.
Null Route IP	Specifies the destination IP address for null route diversion. Traffic reaching the null route IP address will be dropped. This parameter is required only when the BGP session is used in null-route diversion. Note • If traffic triggers null-route diversion, NTA uses the BGP protocol to set the next hop of the traffic to the null route IP address, sends a BGP Update message to the neighbor router, and diverts traffic to the BGP neighbor router. • Since a static route is configured on the router to direct all traffic destined for the null-route IP address to null, all traffic destined for the null route IP address will be dropped by the router.
Route Neighbor	Specifies one or more BGP neighbors by configuring the following parameters:

Parameter	Description
	• Name: name of the router that establishes the BGP neighborship with NTA. • **Neighbor IP**: IP address of the router that establishes the BGP neighborship with NTA. • **Remote AS**: remote autonomous system number of the router that establishes the BGP neighborship with NTA. • **Last-Hop IP**: IP address of the router that is the last hop of the route from the router to NTA. • **Encryption**: controls whether to encrypt BGP connections. Selecting this option indicates that communication between NTA and the BGP neighbor will be encrypted and requires you to enter a password in the adjacent text box.
Third-party Protection Device	Specifies a third-party device for traffic cleaning. For how to configure a third-party protection device, see section 5.5.3 Protection Device Configuration. This parameter is required only when the BGP session is used in BGP diversion. Note • If traffic triggers BGP diversion, NTA uses the BGP protocol to set the next hop of the traffic to a third-party protection device, sends a BGP Update message to the neighbor router, and diverts traffic to the BGP neighbor router. • Since a static route destined for the third-party device is configured on the router, traffic reaching the neighboring router will be diverted to the third-party device.

Modifying a BGP Entry

In the BGP session list, click  in the **Operation** column and modify parameters. If the current BGP entry is being used in a session, modifying its parameters will cause the BGP service to restart and the diversion to end. In this case, you need to confirm your operation in the prompt box.

Deleting a BGP Entry

In the BGP session list, click  in the **Operation** column. If the current BGP entry is being used in a session, deleting it will cause the related diversion policy to be reset. In this case, you need to confirm your operation in the prompt box.

Viewing the Referencing of an Entry

In the BGP session list, click  in the **Operation** column to view which regions or IP groups have referenced this session.

- **Name** indicates the name of the object that references this BGP session.
- **Type** indicates the type of the object that references this BGP session. It has the following values:
  - **Region**: indicates that the entry is referenced by a region.
  - **IP group**: indicates that the entry is referenced by an IP group.

- **Manual diversion**: indicates that the related BGP session is triggered by manual diversion.
- **Global diversion**: indicates that the object that references the session is not defined.

Viewing Routing Entries

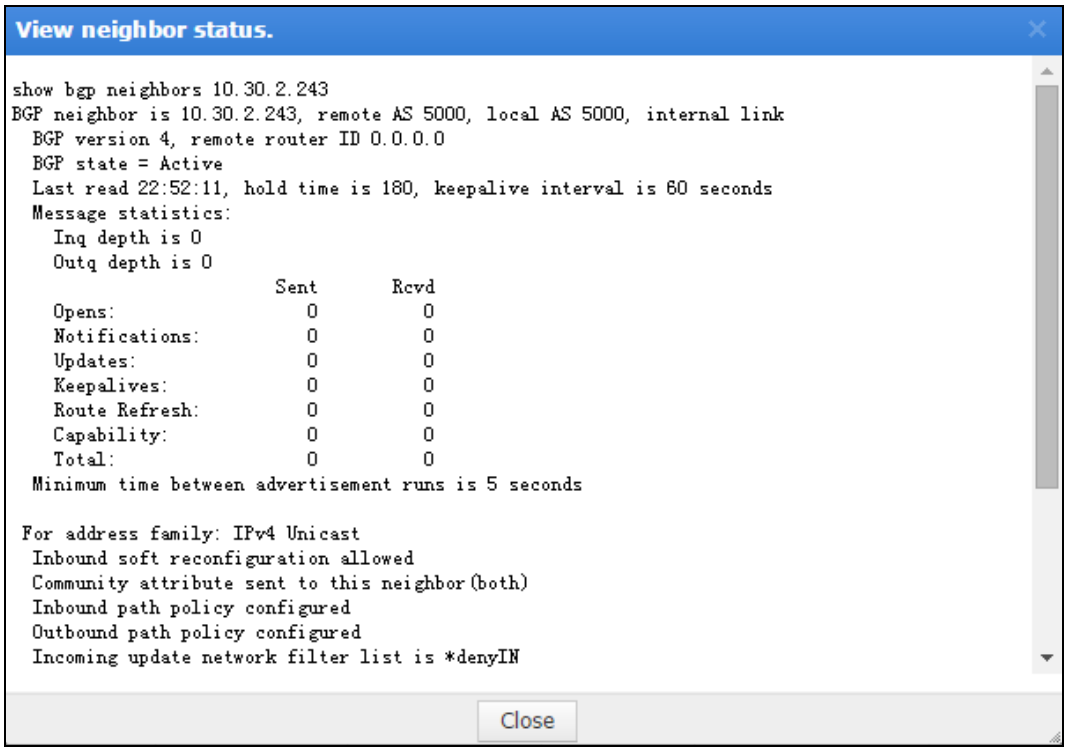
In the BGP session list, click  in the **Operation** column to view IP addresses whose traffic is diverted through this BGP entry.

To cancel diversion of traffic destined for an IP address, click  in the **Operation** column. To delete multiple routes in batches, select the desired ones and click **Revocate routing entries**.

Querying the BGP Neighbor Status

In the BGP session list, click  on the left of the BGP entry name to display the BGP neighbor. Clicking View online status, you can view the BGP neighbor status, as shown in Figure 5-8.

Figure 5-8 BGP neighbor status query result



5.5.3 Protection Device Configuration

When detecting abnormal traffic, NTA can have such traffic diverted to a scrubbing device. Alternatively, it can have the traffic diverted to a third-party protection device after sending a BGP routing notification to this device.

A protection device is either a scrubbing device or a third-party protection device:

- For the scrubbing device, NTA checks whether the device is online. indicates that the device is online and indicates the opposite.
- For a third-party device, click in the **Operation** column to view its status. **Name** indicates the name of an object that uses this device. **Type** indicates the type of the object that uses this device, which can only be **BGP**. NTA does not check its status, which is always displayed as **N/A**.

Choose **Configuration > Global Divert Settings > Protection Device Configuration**, click **Add**, and configure parameters.

A protection device, after being added, can be modified and deleted.

Table 5-29 Protection device parameters

Parameter	Description
Device Type	• **Scrubbing Device**: indicates NSFOCUS Anti-DDoS System. The management IP address of the current NTA should be added on the scrubbing device side. • **Third-party**: indicates a protection device from another security vendor than NSFOCUS.
Device Name	Name of the device.
IP Address	IP address of the device.

5.5.4 BGP FlowSpec Configuration

NTA supports the BGP flow specification (FlowSpec). To implement BGP FlowSpec, you must configure parameters for establishing a BGP FlowSpec session.

Choose **Configuration > Global Divert Settings > FlowSpec BGP**, click **Add**, and configure parameters.

After creating a FlowSpec BGP session, you can edit and delete it and view which regions or IP groups have referenced it, routing entries, and routing neighbor status. For more details, see section 5.5.2 BGP Configuration.

Table 5-30 BGP FlowSpec configuration parameters

Parameter	Description
Name	Specifies a string that identifies the entry.
Local AS	Specifies the local AS number, which must be the same as that of the BGP FlowSpec neighbor; otherwise, neighborship cannot be established.
Local Port	Specifies the source port for data exchange with BGP FlowSpec neighbors. Generally, it is port 179.
Bind IP	Specifies the local IP address used by NTA to establish the BGP FlowSpec neighborship. When two NTA devices constitute a master/backup pair for HA and the local device is a master one, you need to select a virtual IP address.
Hold Time	Specifies the maximum time BGP FlowSpec waits between successive messages before closing the connection. Generally, it is 180 seconds.

Parameter	Description
Maximum Routing Entries	Specifies the maximum number of routing entries that NTA can send in a session based on this BGP FlowSpec entry. This can prevent router performance from deteriorating because of NTA sending too many BGP FlowSpec messages.
Community	Specifies how the BGP FlowSpec-speaking router treats this BGP FlowSpec routing message. A maximum of five community strings are allowed, with each one in a separate line. • **no-advertise**: The value of **YES** indicates that information about this route is not advertised to any BGP FlowSpec peers. • **no-export**: The value of **YES** indicates that information about this route is not advertised to other ASs. • Parameters other than **no-advertise** and **no-export** should be typed in the text box to the right of **Community** in the format of xxx:xxx.
Route Neighbor	Specifies one or more neighbors by configuring the following parameters: • **Name**: name of the router that establishes the BGP FlowSpec neighborship with NTA. • **Remote AS**: number of the external AS. • **Neighbor IP**: IP address of the router that establishes the BGP FlowSpec neighborship with NTA. • **Encryption**: controls whether to encrypt BGP FlowSpec connections. Selecting this option indicates that communication between NTA and the BGP FlowSpec neighbor will be encrypted. In this case, you must set a password in the adjacent text box.

5.6 Flow Data Collection and Forwarding

NTA in DPI mode does not support this function.

NTA analyzes traffic and detects exceptions based on flow data sent by a device. The Flow Settings module allows you to configure default settings for Flow data collection and forwarding, including the port receiving Flow data and whether to forward Flow data as it is. During router configuration, you can specify Flow data collection and forwarding settings for each router or use default settings configured here. For details about the former method, see section 5.1.1.1 Configuring a Router.

Choose **Configuration > Flow Settings** and configure parameters.

Table 5-31 Flow collection and forwarding parameters

Parameter	Description
Netflow/Netstream/IPFIX Collecting Port	The default port number is **9999**.
Sflow Collecting Port	The default port number is **6343**.
Flow Statistics Collect Interval	Specifies the interval at which Flow statistics are collected, which can be **30s** or **60s**.
Statistical Mode	Specifies a statistical mode. This parameter must be specified when **60s** is selected for **Flow**

Parameter	Description
	Statistics Collect Interval. • **Partial**: collects flow data within the 60-second statistical interval. When the cache period of flows is longer than 60 seconds, you are advised to select this option. • **All**: collects all flow data within the cache period. When the cache period of flows is shorter than or equal to 60 seconds, you are advised to select this option.
Default Flow Forwarding	Controls whether NTA forwards the received Flow data. By default, the Flow data is not forwarded. When this parameter is set to **Open**, you must specify **Forward Host List**.
Forward Host List	Specifies the destination IP address and port number for flow data forwarding. This parameter is required only when **Default Flow Forwarding** is set to **Open**. At most eight hosts can be specified.

5.7 Detection of Bogus Source IP Addresses

NTA in DPI mode does not support this function.

If bogus source IP addresses are configured for router interfaces, NTA can discover and present these IP addresses and determine which interfaces they belong to.

Choose **Configuration > Bogus Source IP Detection**, click **Add**, and configure parameters.

After creating a bogus source IP detection rule, you can click the plus sign (+) beside the device name to display information about the included router interfaces, which can be edited and deleted.

Table 5-32 Parameters for configuring a bogus source IP address detection rule

Parameter	Description
Enable	Controls whether to enable the new rule. This rule can take effect only after it is enabled.
Router Name	Router name to be checked against this rule.
Router Interfaces	Router interface name to be checked against this rule.
IP Range	Router interfaces' IP address range to be checked against this rule.
Description	Brief information of this rule.

5.8 NTI

NTA can collaborate with NSFOCUS Threat Intelligence (NTI). When an alert is generated, users can search for associated information available on NTI to learn details about the attack source, such as the geographical information, port information, associated domain names, ASN, and security information.

Note	• To use the NTI collaboration function, you must select the NTI module when creating an NTA license. After the license (whether trial or paid) expires, the NTI query function becomes unavailable. • You can search for IP addresses via NTI for a maximum of 1000 times every day.

Choose **Configuration > Threat Intelligence** and configure parameters.

Table 5-33 Parameters for configuring NTA to collaborate with NTI

Parameter	Description
Compromised Host/Cryptominer Detection	Controls whether to enable compromised host/cryptominer detection.
C&C Communication Detection	Controls whether to enable C&C communication detection.
DDoS Botnet Traceback	Controls whether to enable DDoS botnet traceback.
Collaboration Mode	Specifies an intelligence database that NTA will collaborate with, which can be either of the following: • **NTI (cloud)**: This option requires you to further configure the server address and whether to share threat intelligence. • **Local intelligence database**: This requires no further configuration.
IP Address	Specifies the attack source IP address to be queried. Only IPv4 addresses are supported. Type an IP address and click **Search** to view threat intelligence concerning this IP address.

5.9 Data Dictionary

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

- Application Ports
- Autonomous Systems

5.9.1 Application Ports

After an application is defined with both the protocol name and port number, the application name will be displayed in the **Top5 Applications Traffic** chart of a router or region under **Monitor > Routers** or **Monitor > Regions**.

An application can be either of the following:

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

Choose **Configuration > Data Dictionary > Application Port**. The page lists all built-in applications by default. Click **Add** and configure parameters.

Table 5-34 Parameters for adding an application

Parameter	Description
Application name	Name of the application.
Protocol/Port	Specifies the protocols and port numbers of the application. Format: protocol/port number like tcp/455. Multiple entries should be separated by the comma (,), such as tcp/455,udp/456. Up to 10 entries are allowed.

5.9.2 Autonomous Systems

NTA in DPI mode does not support this function.

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

An AS can be either of the following:

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

Choose **Configuration > Data Dictionary > AS**. The page lists built-in ASs by default. Click **Add** and configure parameters.

Table 5-35 Parameters for adding an AS

Parameter	Description
AS ID	Specifies the ID of the AS, which must be an integer greater than 64511. This parameter is mandatory.
AS Name	Specifies the AS name to be displayed in the **Top5 AS Traffic** chart of a region or router under **Monitor > Regions** or **Monitor > Routers**. This parameter is mandatory.
Country	Specifies the country/region where the AS is located.
Description	Briefly describes the AS.

5.10 Allowlist

On NTA, you can configure the alert allowlist and diversion allowlist. Note that the allowlist does not work for network segment-specific alerts.

5.10.1 Alert Allowlist

After the alert allowlist is enabled, NTA will generate no alert for IP addresses on the allowlist. If this is not enabled, NTA will generate alerts for any possible IP addresses.

Choose **Configuration > Allowlist > Alert Allowlist**, configure alert allowlist parameters, and click **Save**.

select the **Enable** check box, type individual IPv4/IPv6 addresses, IP prefixes, and/or IP address ranges, with each in a separate line, and click **Save**.

Table 5-36 Parameters of an alert allowlist

Parameter	Description
Allowlist	Controls whether to enable the alert allowlist function.
Validity Period	Specifies how long the alert allowlist remains valid. The validity period can be configured only after the allowlist is enabled. After clicking **Enable** for **Validity Period**, specify the start date and end date of the alert allowlist. The default validity period is 1 day. No alerts will be generated for specified IP addresses in the specified period.
IP Address	Specifies the IP address to be added to the alert allowlist. Type IPv4 addresses, IPv6 addresses, IP subnets, or IP segments, with each in a separate line.

5.10.2 Diversion Allowlist

After the diversion allowlist is enabled, NTA will not divert traffic for IP addresses on the allowlist or network segments containing such IP addresses. The diversion allowlist can be dispatched via the web-based manager and web API.

Choose **Configuration > Allowlist > Diversion Allowlist**, select the **Enable** check box, type individual IPv4/IPv6 addresses, IP prefixes, and/or IP address ranges, with each in a separate line, and click **Save**. The allowlist can contain a maximum of 1000 entries.

6 Log Management

This chapter describes how to view and manage logs generated by NTA, containing the following sections:

Section	Description
Log Query Notes	Describes things to note during log query.
Diversion Log	Describes how to query and understand diversion logs.
Audit Log	Describes how to query and understand audit logs.
Running Log	Describes how to query and understand running logs.
FlowSpec Diversion Log	Describes how to query and understand FlowSpec logs.

6.1 Log Query Notes

The query method varies with the log type. Note the following when querying logs:

- Multiple query conditions are of the AND relationship.
- The **Statistical Time** parameter is available for all logs, which indicates the period during which logs are generated. It has the following values:
  - **Last 24 hr**: indicates the duration from current time of the previous day to the current time. This is the default value.
  - **Yesterday**: indicates the duration from 00:00:00 to 23:59 yesterday.
  - **This week**: indicates the duration from 00:01 on Monday to the current time.
  - **This month**: indicates the time period from 00:01 on the first day of the month to current time.
  - **Custom**: specifies a duration.
- After the query result is returned, you can click  to export the result as a CSV file.
- When there are more than 10,000 logs, the export function stops working, with an error message prompted by the system.

6.2 Diversion Log

Choose **Logs > Diversion Log**, set query conditions, and click **Search**. The system will return all logs concerning traffic diversion by NSFOCUS scrubbing device and third-party protection devices.

Table 6-1 describes parameters of the diversion log.

Table 6-1 Parameters of the diversion log

Parameter	Description
Time	Indicates the period during which logs are generated.
Diversion Network Segment	Indicates the network segment from which traffic is diverted.
Triggering Threshold	Indicates the actual traffic (in bps and pps) or the number of abnormal connections that triggers the diversion.
Diversion Mode	Indicates the diversion mode, which can be one of the following: • **Auto IP diversion**: indicates that traffic to a specific IP address is diverted when DDoS attack traffic is detected. • **Auto group diversion**: indicates that traffic to an IP group is diverted due to traffic anomaly. • **Manual IP diversion**: indicates that traffic to an IP address or IP segment is diverted when hitting a manual traffic diversion rule or when you revoke an auto IP diversion route. • **Manual group diversion**: indicates that traffic to an IP group is diverted when traffic anomaly occurs or when you revoke diversion. • **Network segment-specific diversion**: indicates that traffic to a segment is diverted when segment-specific DDoS attack traffic is detected.
Alert ID	Indicates the ID of the alert triggering the diversion event. Clicking this alert ID, you can view alert details.
Trigger Strategy	Indicates the name of policy which triggers diversion.
Region/IP Group	Indicates the region or IP group that the diverted IP address belongs to. If this IP address does not belong to any region or IP group, **Default Diversion Policy** is displayed.
Diversion Type	Indicates the diversion type, which can be one of the following: • **Scrubbing Device Diversion**: indicates that traffic is diverted to the scrubbing devices. • Null-Route Diversion: indicates that traffic is diverted to a null route IP address using the Border Gateway Protocol (BGP). In this case, BGP next-hop IP address is the null route IP address. • **BGP Diversion**: indicates that traffic is diverted to a protection device using BGP. In this case, the IP address of the protection device is the BGP next-hop IP address.
Destination/BGP Next-Hop	Indicates the destination of traffic diversion, which can be the the scrubbing device or BGP next-hop IP address
Operation	Indicates the operation, which can be one of the following: • **Add diversion request success**: indicates that NTA's diversion request is

Parameter	Description
	successfully added on a router or the scrubbing device. • **Delete diversion request success**: indicates that NTA's diversion request is successfully deleted from a router or the scrubbing device. • **Add diversion request failed**: indicates that NTA's diversion request fails to be added on a router or the scrubbing device. • **Delete diversion request failed**: indicates that NTA's diversion request fails to be deleted from a router or the scrubbing device.

6.3 Audit Log

Choose **Logs > Audit Log**, set query conditions, and click **Search**. The system will return all logs concerning users' configurations.

Table 6-2 describes parameters of the audit log.

Table 6-2 Parameters of the audit log

Parameter	Description
Time	Indicates when the system is configured.
Username	Indicates the user name you use for configuring NTA.
Client IP	Indicates the IP address of your computer on which you configure NTA.
Module	Indicates the modules you have configured.
Description	Indicates brief description about the event.
Operation Result	Indicates whether configuration is successful.

6.4 Running Log

Choose **Logs > Running Log**, set query conditions, and click **Search**. The system will return all logs concerning the running of NTA and BGP neighborship status changes.

Table 6-3 describes parameters of the running log.

Table 6-3 Parameters of the running log

Parameter	Description
Statistical Time	Specifies the period when running logs are generated.
Source	Indicates the module which generates running logs, which can be: • **All**: no limitation on the source of logs • **System Engine**: generates logs about the running of NTA. • BGP Service: generates logs about BGP status changes. • FlowSpec BGP: generates logs about the status changes of NTA's BGP neighbor during FlowSpec diversion.

Parameter	Description
	• **NTPD Log**: generates logs about the status changes of the NTPD service. Such logs are generated when NTA and the NTP clock source have a time difference of 1000 seconds. • **Interface Link Status**: generates interface link status logs. Such logs are generated when the status of an interface changes from up to down or from down to up.
Description	Indicates brief description about the event.

6.5 FlowSpec Diversion Log

Choose **Logs > FlowSpec Diversion Log**, set query conditions, and click **Search**. The system will return all logs concerning all events of traffic diversion via FlowSpec.

Table 6-4 describes parameters of the FlowSpec diversion log.

Table 6-4 Parameters of the FlowSpec diversion log

Parameter	Description
Name	Number of the FlowSpec diversion event.
Alert ID	ID of the alert corresponding to this event.
Region/IP Group	Region or IP group to which the IP address with diverted traffic belongs. If this IP address does not belong to any region or IP group, **Default Diversion Policy** is displayed.
Protocol	Protocol used for exchanging routing information during diversion of traffic via FlowSpec.
Source Network Segment	Source IP address of traffic diverted via FlowSpec.
Source Port	Source port of traffic diverted via FlowSpec.
Destination Network Segment	Destination IP address of traffic diverted via FlowSpec.
Destination Port	Destination port of traffic diverted via FlowSpec.
Start Time	Time when traffic diversion starts.
Packet Length	Length of diverted packets.
Action	Action taken on the diverted traffic.
FlowSpec BGP	Name of the BGP FlowSpec entry.
Diversion Mode	Mode of diversion, which can be automatic FlowSpec diversion or manual FlowSpec diversion.
Operation Type	Indicates the operation, which can be one of the following: • **Add diversion success**: indicates that NTA's diversion request is successfully added on a router. • **Delete diversion success**: indicates that NTA's diversion request is successfully deleted from a router. • **Add diversion failure**: indicates that NTA's diversion request fails to be

Parameter	Description
	added on a router. • **Delete diversion failure**: indicates that NTA's diversion request fails to be deleted from a router.
Details	Brief description of the message.

7 Report Management

NTA has a flexible report system, which can generate various reports based on the combination of different conditions. The system provides real-time and historical reports, allowing viewing of reports for the last 1/7/30 days, by day/week/month, or for a custom period. In other words, NTA provides not only real-time monitoring reports but also historical reports for future reference and forensics. This chapter describes how to generate, view, and manage reports in real time.

This chapter contains the following sections:

Section	Description
Traffic Report	Describes how to generate traffic reports.
DDoS Attack Report	Describes how to generate DDoS attack reports.
Bogus Source IP Report	Describes how to generate bogus source IP reports.
Traffic Comparison Report	Describes how to generate traffic comparison reports.
Email Sending Configuration	Describes how to configure scheduled sending of reports via email.
Report Export	Describes how to export reports.

7.1 Traffic Report

Choose **Reports** > **Traffic Report** and set query conditions to generate a traffic report of the specified time frame. Open the report preview page and hover the mouse at a random point in a graph to view statistical data at a specific point of time.

Table 7-1 describes conditions for generating a traffic report.

Table 7-1 Conditions for generating a traffic report

Parameter	Description
Statistical Time	Specifies a statistical period. It has the following values: • **Last 24 hr**: indicates the period from the current time yesterday to now. • **Last 7 days**: indicates the period from the current time 7 days ago to now. • **Last 30 days**: indicates the period from the current time 30 days ago to now. • **By day**: specifies a date to display traffic data of that day. NTA cannot generate

Parameter	Description
	reports of the current day. • **By week**: specifies a date to display traffic data of the week containing that day. NTA cannot generate reports of the current week. • **By month**: specifies a month to display traffic data of that month. NTA cannot generate reports of the current month. • **Custom**: specifies a custom period.
Object	Specifies the statistical object. It has the following values: • **Regions**: specifies a region whose traffic statistics will be reported. • **IP Groups**: specifies an IP group whose traffic statistics will be reported. • **Routers**: specifies a router whose traffic statistics will be reported. • **Router Interfaces**: specifies a router interface whose traffic statistics will be reported. • **Router Interface Groups**: specifies a router interface group whose traffic statistics will be reported.
Condition	Specifies one or more dimensions in which statistics are collected. It has the following values: • IP • Application name • Protocol • Packet length • DSCP • AS • Prefix • Country/Region For example, if you select **IP**, the report will cover statistics about top IP addresses by traffic.
Sorting Order	Specifies the unit of the traffic rate for sorting top items, which can be bps or pps. A single traffic report can display traffic data expressed in both pps and bps.
TOP	Specifies the number of top items in the report. Values include **5**, **10**, **20**, **50**, and **100**.

7.2 DDoS Attack Report

Choose **Reports > DDoS Attack Report** and set query conditions to generate a DDoS attack report of the specified time frame. Open the report preview page and hover the mouse at a random point in a graph to view statistical data at a specific point of time.

Table 7-2 Conditions for generating a DDoS attack report

Parameter	Description
Statistical Time	Specifies a statistical period. It has the following values: • **Last 24 hr**: indicates the period from the current time yesterday to now.

Parameter	Description
	• **Last 7 days**: indicates the period from the current time 7 days ago to now. • **Last 30 days**: indicates the period from the current time 30 days ago to now. • **By day**: specifies a date to display DDoS attack data of that day. NTA cannot generate reports of the current day. • **By week**: specifies a date to display DDoS attack data of the week containing that day. NTA cannot generate reports of the current week. • **By month**: specifies a month to display DDoS attack data of that month. NTA cannot generate reports of the current month. • **Custom**: specifies a custom period.
Object	Indicates the statistical object. It has the following values: • **Global**: indicates that DDoS attack data of all IP addresses that are not in any regions or IP groups will be reported. • **Regions**: specifies a region whose DDoS attack data will be reported. • **IP Groups**: specifies an IP group whose DDoS attack data will be reported. • **IP Address/IP Segment**: specifies an IPv4 address or segment whose DDoS attack data will be reported.
Consolidated Report	Specifies the types of statistical content contained in the report. Options available vary with the selected object: • When **Object** is **Global**, **Regions**, or **IP Groups**, the report can contain attack target statistics, attack alert statistics, attack traffic statistics, and/or attack source statistics. • When **Object** is **IP Address/IP Segment**, the report can contain attack alert statistics, attack traffic statistics, and/or attack source statistics.
Allowlist IP	Specifies the destination IP address that is not displayed in the report. Only a single IP address can be typed. The relevant attack data of the destination IP address is filtered out and is not included in the report.
TOP	Specifies the number of top items in the report. Values include **5**, **10**, **20**, **50**, and **100**.
Unit	Specifies the unit of the traffic rate for sorting top items, which can be bps or pps.
Attack Type	Specifies a type of DDoS attacks whose statistics will be covered by the report. **All** indicates all types of DDoS attacks.
Alert Level	Specifies an alert level of DDoS attacks whose statistics will be covered by the report. **All** indicates all alert levels.

7.3 Bogus Source IP Report

NTA in DPI mode does not support this function.

Choose **Reports > Bogus Source IP Report** and set query conditions to generate a bogus source IP report of the specified time frame. Open the report preview page and hover the mouse at a random point in a graph to view statistical data at a specific point of time.

Table 7-3 Parameters for generating a bogus source IP report

Parameter	Description
Statistical Time	Specifies a statistical period. It has the following values: • **Last 24 hr**: indicates the period from the current time yesterday to now. • **Last 7 days**: indicates the period from the current time 7 days ago to now. • **Last 30 days**: indicates the period from the current time 30 days ago to now. • **By day**: specifies a date to display traffic data of the specified bogus source IP address on that day. NTA cannot generate reports of the current day. • **By week**: specifies a date to display traffic data of the specified bogus source IP address in the week containing that day. NTA cannot generate reports of the current week. • **By month**: specifies a month to display traffic data of the specified bogus source IP address in that month. NTA cannot generate reports of the current month. • **Custom**: specifies a custom period.
Bogus Source IP	Bogus source IP address to be queried.
Destination IP/Port	Destination IP address/port to be queried.
Routers	Router to be queried.

7.4 Traffic Comparison Report

Through a traffic comparison report, you can discover abnormal traffic in time. This report can contain either of the following types of contents:

- A comparative analysis is made around traffic of the same statistical object (routers, router interfaces, router interface groups, regions, or IP groups) in different periods.
- A comparative analysis is made around traffic of different statistical objects (routers, router interfaces, router interface groups, regions, or IP groups) in the same period.

Choose **Reports > Traffic Comparison Report** and set query conditions to generate a traffic comparison report of the specified time frame. Open the report preview page and hover the mouse at a random point in a graph to view statistical data at a specific point of time.

Table 7-4 Parameters for generating a traffic comparison report

Parameter	Description
Object Type	Specifies whose traffic will be compared, the same object or different objects.
Statistical Time	Specifies a statistical period. A report on the same object has the following values: • **By day**: specifies dates to display traffic data of the statistical object on different days. At most five dates can be selected. NTA cannot generate reports of the current day. • **By week**: specifies dates to display traffic data of the statistical object in different weeks containing those days. At most five weeks can be selected. NTA cannot generate reports of the current week. • **By month**: specifies months to display traffic data of the statistical object in

Parameter	Description
	those months. At most five months can be selected. NTA cannot generate reports of the current month. A report on different objects has the following values: • **Last 24 hr**: indicates the period from the current time yesterday to now. • **Last 7 days**: indicates the period from the current time 7 days ago to now. • **Last 30 days**: indicates the period from the current time 30 days ago to now. • **By day**: specifies a date to display traffic data of the specified objects on that day. NTA cannot generate reports of the current day. • **By week**: specifies a date to display traffic data of the specified objects in the week containing that day. NTA cannot generate reports of the current week. · **By month**: specifies a month to display traffic data of the specified objects in that month. NTA cannot generate reports of the current month. • **Custom**: specifies a custom period.
Object	• Same object: specifies a region, IP group, router, router interface, or router interface group. For their descriptions, see Table 7-1. • Different objects: specifies two or more regions, IP groups, routers, router interfaces, or router interface groups. For their descriptions, see Table 7-1.
Statistics Value Type	Maximum value or average value for statistics.

7.5 Email Sending Configuration

You can configure email sending settings to send reports to a designated email address. To configure email sending settings, follow these steps:

Choose **Reports > Email Sending Configuration**, click **Add**, and configure parameters. Then reports will be sent to the specified email addresses.

An email sending policy, after being created, can be edited and deleted.

Table 7-5 Parameters for configuring an email sending policy

Parameter	Description
To	Email addresses to receive reports. A maximum of 20 email addresses can be typed, with each in a separate line.
Language	Language of reports, which can be **Simplified Chinese** or **English**.
Report Format	File format, which can be **PDF**, **XML**, or **CSV**. Bogus source IP reports cannot be exported as XML files.
Enable	Enabling this policy indicates that reports will be sent accordingly.
Sending Time	Specifies how frequently reports are sent. Options include **Daily**, **Weekly**, and **Monthly**.
Description	Brief description of the policy.
Report Type	Specifies one or more types of reports, including the following:

Parameter	Description
	• Traffic report. For details, see section 7.1 Traffic Report. • DDoS attack report. For details, see section 7.2 DDoS Attack Report. • Bogus source IP report. For details, see section 7.3 Bogus Source IP Report.

7.6 Report Export

On the report preview page, click  ,  , or  and configure report export parameters of the PDF, XML, or CSV format. Table 7-6 describes report export parameters.

Table 7-6 Report export parameters

Parameter	Description
Export Format	Format of the report to be exported: • Traffic/DDoS attack/Traffic comparison report: can be exported as a PDF, XML, or CSV file. • Bogus source IP report: can only be exported as a CSV file.
Report Name	Report title displayed on the preview page by default, which can be edited.
Made by	**NSFOCUS** by default, which can be changed to the name of the person generating the report and will be displayed in the exported report
Submitted by	Name of the person submitting the report. It will be displayed in the exported report.
Report Description	Brief description of the report.

8 Alert Management

This chapter contains the following sections:

Section	Description
Overview	Describes how to view overall alert statistics, basic information about a specific type of alerts, and alert details.
Alert Query	Describes how to set conditions to query alerts.

8.1 Overview

This section describes how to view overall alert statistics, basic information about a specific type of alerts, and alert details. It involves the following:

- Overall Alert Statistics: information about all alerts
- Information About Specified Alerts:
  - Information about the alerted traffic
  - Top 5 information, covering source IP addresses, ports, protocols, and TCP flags

8.1.1 Overall Alert Statistics

Choose **Alert > Overview**. This page displays alert distribution information and the alert list, as shown in Figure 8-1.

Figure 8-1 Overview of alerts

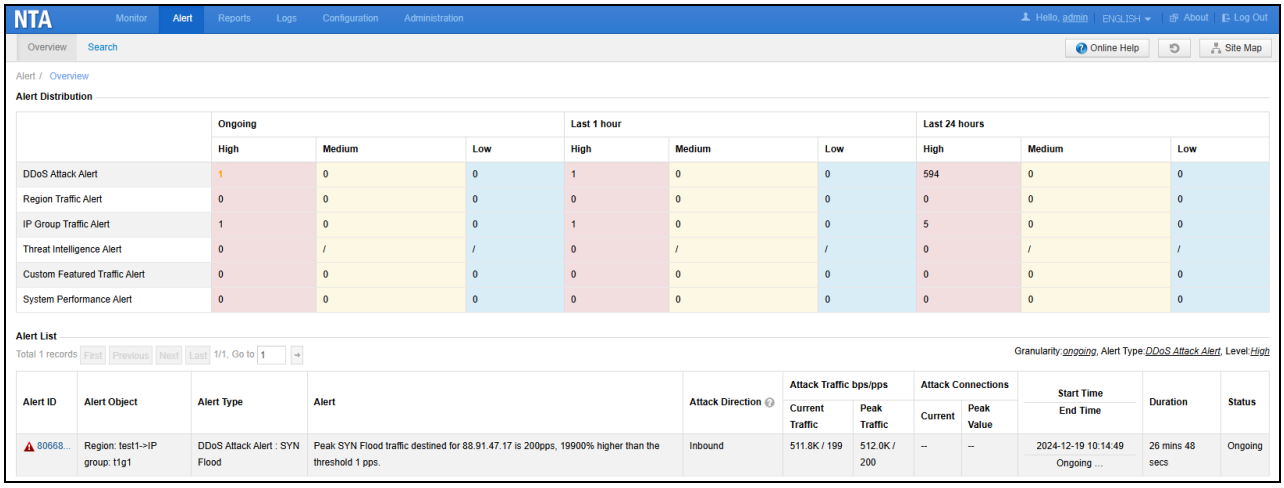


Table 8-1 describes parameters on the **Overview** page.

Table 8-1 Parameters on the Overview page

Parameter		Description
Alert Distribution		Displays statistical information about alerts of all types, including ongoing alerts, alerts ending in the past hour, and alerts ending in the past 24 hours of various severity levels (high, medium, and low). The slash (/) indicates no corresponding alert has been detected. Clicking the number of alerts at a specific level shows related alert information in the **Alert List** below and changes the number to an orange one in bold.
Alert List		• Displays ongoing DDoS attack alerts with a high level of severity by default. • Clicking a number in the alert distribution table shows related alert information here.
Alert List	Alert ID/Severity	• **Alert ID**: uniquely identifies an alert. For a DDoS attack alert, region traffic alert, IP group traffic alert, or custom featured traffic alert, you can click the alert ID to view more information and download the related report. For details, see section 8.1.2 Information About Specified Alerts. • Severity: indicates the severity level of an alert with one of the following symbols according to the global alert configuration (see section 5.4.3 Alert Parameters): - : low-level alert - : medium-level alert - : high-level alert
	Alert Object	Object that triggers the alert, which may be a router, region, or IP group. If such an object cannot be found, **Default DDoS Attack Alert** is displayed here.
	Alert Type	Indicates the type of the alert, which can be any of the following:

Parameter			Description
			• **DDoS Attack Alert**: alert triggered by a DDoS attack. The specific type of DDoS attacks is also displayed, like **DDoS Attack Alert: SYN FLOOD**. • **Region Traffic Alert:** alert triggered by abnormal inbound or outbound traffic of a region. • **IP Group Traffic Alert**: alert triggered by abnormal traffic received or sent by an IP group. • **Threat Intelligence Alert**: alert triggered by an IP group asset matching a threat intelligence database rule. • **Custom Featured Traffic Alert**: alert triggered by traffic that contains custom attack signatures. • **Router Interface Bandwidth Alert**: alert triggered by abnormal interface bandwidth usage of a router. This type of alerts is unavailable on NTA in DPI mode. • **Router Performance Alert**: alert triggered by abnormal CPU or memory usage of a router. This type of alerts is unavailable on NTA in DPI mode. • **System Performance Alert**: alert triggered by abnormal CPU or memory usage of NTA.
	Alert		Details about the alert.
	Alert Direction		Indicates the attack direction, which can be outbound or inbound. To use this function, you need to configure the IP address of the asset to be protected to belong to a region or IP group. • When the target IP address does not belong to a region or IP group, the direction is displayed as "Outbound". • When the target IP address belongs to a region or IP group, the actual direction of abnormal traffic is displayed.
	Attack Traffic	Current Traffic	Current traffic in bps and pps. For an alert that has ended or an alert that was triggered by the number of abnormal connections, -/- is displayed.
		Peak Traffic	Peak traffic in bps and pps flowing during the alert.
	Attack Connections	Current	Current number of abnormal connections.
		Peak Value	Maximum number of abnormal connections throughout the alert period.
	Start Time		Time when the alert starts.
	End Time		Time when the alert ends. If the alert has not ended, **Ongoing** is displayed.
	Duration		Duration of the alert from the start time to current time.
	Status		Status of the alert, which can be **Ongoing** or **Ended**.

8.1.2 Information About Specified Alerts

Choose **Alert > Overview**. In **Alert List**, click an alert ID to view details about this alert, including:

- **Basic information**: includes basic alert information and traffic details.
- **Top 5 information**: Top 5 information varies with alert types. It usually covers IP addresses, ports, protocols, TCP flags, packet lengths, DSCPs, and countries/regions.

8.1.2.1 Basic Information

For the following types of alerts, you can click an alert ID in the alert list to view alert details:

- DDoS attack alert
- Region traffic alert
- IP group traffic alert
- Custom featured traffic alert

Viewing Alert Details

Figure 8-2 and Figure 8-3 shows the alert detail page. Table 8-2 describes parameters on this page.

Figure 8-2 Page displaying traffic details about an alert

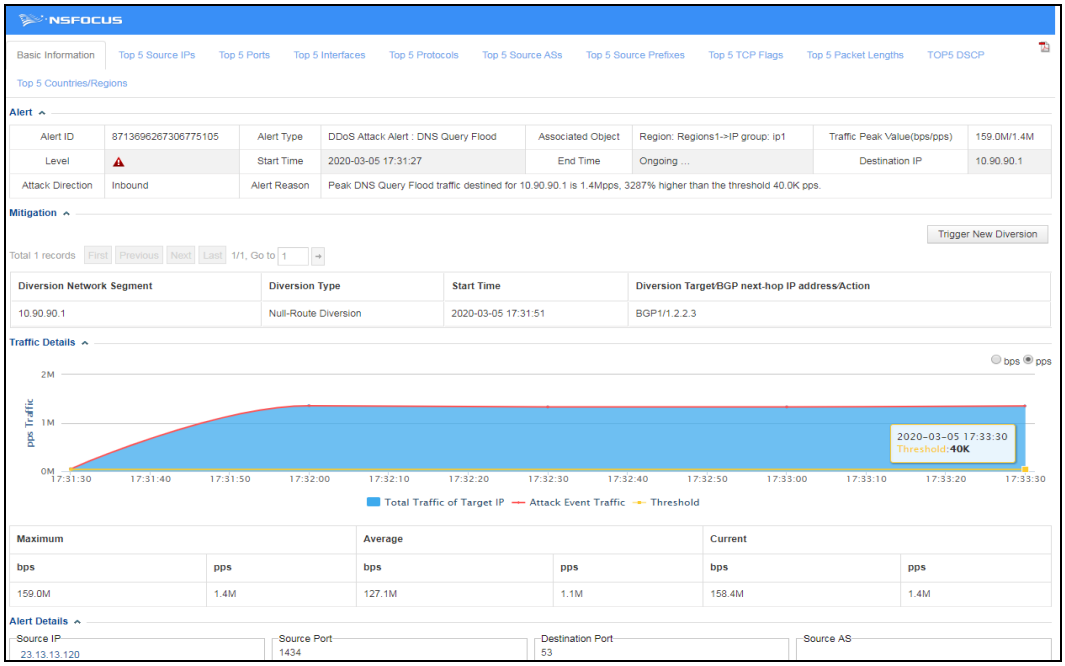


Figure 8-3 Page displaying connection details about an alert

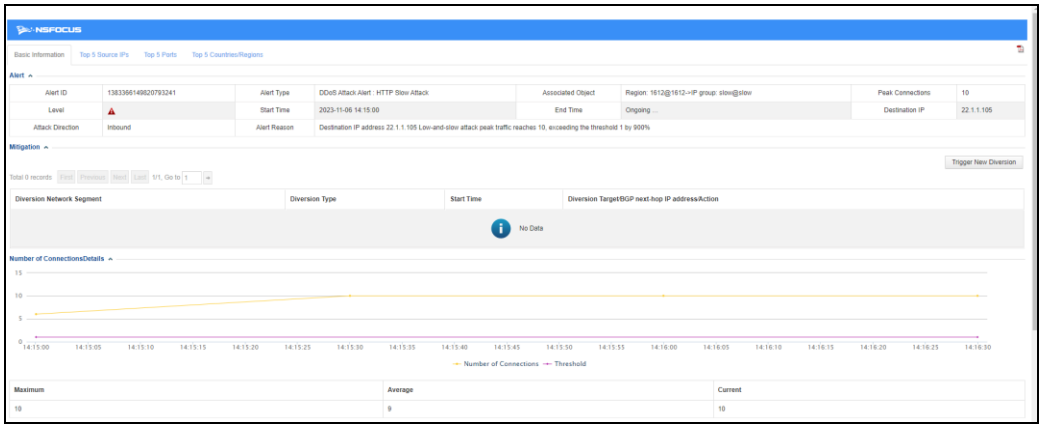


Table 8-2 Basic alert parameters

Parameter	Description
Alert	See Table 8-1.
Mitigation	Information about the diversion triggered by the alert. **Trigger New Diversion** is displayed only when the alert status is "Ongoing". • Empty list: indicates that the alert has not triggered diversion. To manually start diversion, click **Trigger New Diversion**, configure manual diversion parameters, and click **OK** to commit the settings. For the description of parameters, see Table 9-10. • List with diversion information: Click **Trigger New Diversion**, configure manual diversion parameters, and click **OK**. The system prompts that "The manual diversion already exists. You can view it in the diversion routing table."
Traffic Details	Displays overall traffic information of the alert source (for a DDoS attack, the alert source is also the attack target) throughout the alert duration. For an ongoing alert, traffic information till the current moment is displayed. For a DDoS attack alert, the area graph shows three curves by default. You can click **bps** or **pps** to display traffic measured accordingly. • **Total Traffic of Target IP**: indicates the trend curve of total traffic to the target IP address throughout the event that triggers the alert. • **Attack Event Traffic**: indicates the trend curve of attack traffic to the target IP address throughout the event that triggers the alert. • **Threshold**: attack traffic threshold (bps/pps). If the threshold is a fixed value, a straight line is displayed. If the threshold is based on auto-learning baselines, a curve is displayed, indicating that it changes over time. Clicking a legend item hides or displays statistics of that type. Hovering the mouse over the graph shows specific figures. The table below the graph shows the maximum, average, and current traffic of the attack triggering the current alert. Note The area graph of abnormal traffic alerts shows only two curves: **Attack**

Parameter	Description
	Event Traffic and **Threshold**.
Number of Connections Details	Displays the number of abnormal connections to the alert target under the low-and-slow attack in a line chart. • **Number of Connections**: displays the trend curve of the number of abnormal connections to the target IP address has throughout the event that triggers the alert. • **Threshold**: indicates the threshold for low-and-slow attack detection, which is displayed in a straight line. Clicking a legend item hides or displays statistics of that type. Hovering the mouse over the graph shows specific figures. The table below the graph shows the maximum, average, and current numbers of abnormal connections triggering the current alert.
Alert Feature	The following signature information is displayed: • **Source IP**: source IP address contributing the largest proportion of traffic or abnormal connections and the related proportion in the alert period. • **Source Port**: source port contributing the largest proportion of traffic or abnormal connections and the related proportion in the alert period. • **Destination IP**: destination IP address receiving the largest proportion of traffic or abnormal connections and the related proportion in the alert period. • **Destination Port**: destination port receiving the largest proportion of traffic or abnormal connections and the related proportion in the alert period. • **Protocol**: protocol contributing the largest proportion of traffic and the related proportion in the alert period. The protocol displayed here can be **TCP**, **UDP**, **ICMP**, or **OTHERS**. • **TCP Flag**: TCP flag with the largest proportion of traffic and the related proportion in the alert period. • **Packet Length**: most common packet length and the related proportion of traffic in the alert period. • **Source Country/Region**: source country/region contributing the largest proportion of traffic or abnormal connections and the related proportion in the alert period. The country/region information is represented with both the text and national flag.
Alert Details	Details of an event triggering the alert. Details of a DDoS attack event are slightly different from those of an abnormal traffic event. Clicking the source IP address shows its details, including the security, basic, port, associated domain, and ASN information.  Note • If application ports are defined in the data dictionary, the alert detail list shows the object name. For how to configure the data dictionary, see section 5.9 Data Dictionary. • To view details about a source IP address, you need to configure NTA to collaborate with NTI in advance. For details, see section 5.8 NTI.

Exporting an Alert Report

On the page shown in Figure 8-2, click in the upper-right corner and configure parameters in the **Export** dialog box to export the report as a PDF file.

Table 8-3 Parameters for exporting a report

Parameter	Description
Content to Export	Specifies the content to export. Options vary with alert types.
Top 5 Items Sorting Dimension	Specifies how top 5 items are sorted, which can be Maximum, Current, or Average.
Report Name	Specifies the report name.
Made by	Specifies the person generating this report. The default value is **NSFOCUS**. This information will be presented in the exported report.
Submitted by	Specifies the person submitting the exported report. This information will be presented in the exported report.
Report Description	Brief description of this report.

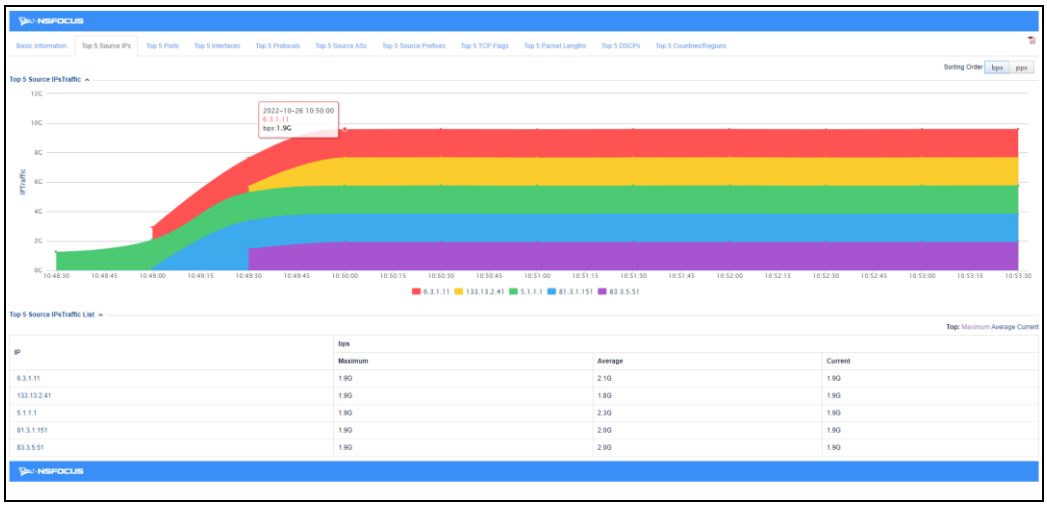
8.1.2.2 Top 5 Information

Top 5 information varies with alert types. It usually covers source IP addresses, ports, interfaces, protocols, source ASs, source prefixes, TCP flags, packet lengths, DSCPs, and countries/regions.

Take top 5 source IP addresses of a DDoS attack alert.

Choose **Alert > Overview**. In **Alert List**, click a specific alert ID and then click the **Top 5 Source IPs** tab. This page displays top 5 source IP addresses with the most traffic, as shown in Figure 8-4.

Figure 8-4 Top 5 source IP addresses of DDoS attack alerts



Note	For the HTTP Slow Attack alert, this page displays top 5 source IP addresses with the most abnormal connections.

Table 8-4 Parameters on the Top 5 Source IPs page

Parameter	Description
Top 5 Source IPs by Traffic	Displays traffic trends of top 5 source IP addresses in an area graph. Clicking a legend item hides or displays statistics of an IP address. Hovering the mouse over the graph shows specific figures.
Top 5 Source IPs by Traffic List	Lists top 5 source IP addresses with maximum, average, and current traffic rates. By default, top 5 source IP addresses are ranked by maximum traffic. You can click **Average** or **Current** to rank top 5 source IP addresses by average traffic or current traffic.
Sorting Order	By default, **bps** is used to measure the traffic for source IP address ranking. You can click **pps** to measure the traffic in pps.

8.2 Alert Query

You can set conditions to query desired alerts.

Choose **Alert > Search** and set query conditions. For the description of related parameters, see Table 8-5.

In the alert list, click an alert ID to view its details. For details, see section 8.1.2 Information About Specified Alerts. Clicking  , you can export the alert report as a CSV file. For how to configure report export parameters, see section 7.6 Report Export.

Table 8-5 Parameters for querying alerts

Parameter	Description
Alert Status	Status of alerts to be queried, which can be one of the following: • **Ongoing**: indicates ongoing alerts. • **End**: indicates ended alerts. • **All**: indicates all alerts
Statistical Time	Specifies a statistical period when **Alert Status** is set to **End** or **All**. The value can be any of the following: • **Last 24 hr**: indicates the duration from current time of the previous day to the current time. This is the default value. • **Last 7 days**: indicates the duration from current time 7 days before to the current time. • **Last 30 days**: indicates the duration from current time 30 days before to the current time. • **By day**: specifies a date to query alerts of that day from 00:00 to 23:59.

Parameter	Description
	• **By week**: specifies a date to query alerts of the week containing that day. • **By month**: specifies a month to query alerts of that month from 00:00 on the first day to 23:59 on the last day of the month. • **Custom**: specifies a custom period.
Alert Type	Allows you to select an alert type from the drop-down list: • **All**: indicates alerts of all types. • **DDoS Attack Alert**: indicates alerts triggered by DDoS attacks. • **Region Traffic Alert:** indicates alerts triggered by abnormal inbound or outbound traffic of a region. • **IP Group Traffic Alert**: indicates alerts triggered by abnormal traffic received or sent by an IP group. • **Threat Intelligence Alert**: indicates alerts triggered by an IP group asset matching the threat intelligence database. • **Custom Featured Traffic Alert**: indicates alerts triggered by traffic that contains custom attack signatures. • **Router Interface Bandwidth Alert**: indicates alerts triggered by abnormal interface bandwidth usage of a router. This is unavailable on NTA in DPI mode. • **Router Performance Alert**: indicates alerts triggered by abnormal CPU or memory usage of a router. This is unavailable on NTA in DPI mode. • **Router Data Acquisition Abnormal Alert**: indicates alerts triggered by a router failing to collect data (that is, failing to report flow and SNMP data to NTA). This is unavailable on NTA in DPI mode. • **Device Performance Alert**: indicates alerts triggered by abnormal CPU or memory usage of NTA.
Alert Level	Specifies an alert level (**High**, **Medium**, or **Low**). **All** indicates alerts of all levels.
Alert ID	Specifies an alert ID. Leaving it empty indicates any alerts.
Alert Object	Indicates objects whose alerts will be queried. Clicking in the text box will display all available alert objects, including: • Fuzzy query is supported. That is, after you type part of an object name, the system shows all object names containing your input. You can specify multiple objects, which are of the OR relationship. • If no object is selected, all alerts that meet other conditions are displayed.
Destination IP	This is unavailable for router interface bandwidth alerts, router performance alerts, router data collection anomaly alerts, and device performance alerts. Specifies a destination IP address or IP segment to query related alerts. Both IPv4 and IPv6 are supported.
Routers/Interface	This is unavailable for device performance alerts. specifies a router and router interface to query related alerts.
Attack Direction	This is available for DDoS attack alerts, threat intelligence alerts, custom featured traffic alerts, and device performance alerts. Specifies an attack direction, which can be **Outbound** or **Inbound**. • When the destination IP address does not belong to any region or IP group, select **Outbound**. • When the destination IP address belongs to a region or IP group, select the

Parameter	Description
	direction according to the actual situation.
Alert Peak Value	Specifies a peak traffic range by selecting ≥, ≤, or **to** and typing specific numbers. The peak value can be expressed in bps or pps.  Note When **Alert Type** is set to DDoS Attack Alert > HTTP Slow Attack, this item specifies the number range of connections. You can select ≥, ≤, or to and type a specific number or two numbers to query alerts with the specified attack connections.

9 Monitoring

This chapter contains the following sections:

Section	Description
View Management	Describes how to manage views on monitoring pages.
Overall Monitoring Statistics	Describes how to view statistics about traffic of and attacks against routers, regions, and IP groups monitored by NTA.
Regions	Describes how to view alert and traffic statistics of all regions, detailed monitoring information of each region, and detailed monitoring information of specific IP addresses.
Routers	Describes how to view performance and traffic statistics of routers monitored by NTA and monitoring information of each router.
Router Interface Groups	Describes how to view traffic statistics of router interface groups monitored by NTA and detailed monitoring information of each router interface group.
IP Addresses	Describes how to view traffic statistics of specific IP addresses.
Diversion Routing Table	Describes how to view dynamically added routing tables for IP address- and group-specific diversion, and how to configure routes for manual traffic diversion.
Traffic Auto-learning	Describes how to check the traffic auto-learning results of IP groups.
Local Interfaces	Describes how to view traffic statistics of all interfaces on NTA.
Local Status	Describes how to view NTA's system status, basic information, system services, and local interface status.

9.1 View Management

NTA provides monitoring views, each consisting of several widgets, to present monitoring statistics to users. These views are displayed on monitoring pages under **Monitor**.

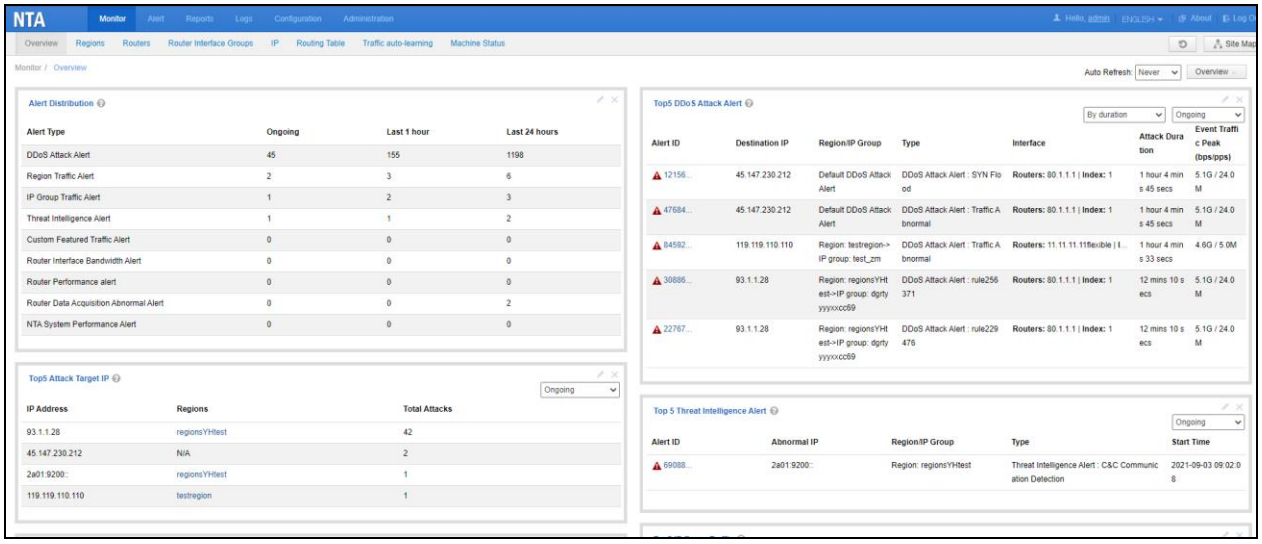
Uses can customize monitoring views as required by doing the following:

- Adding a View
- Editing a View
- Deleting a View

- Setting a View as Default

Choose **Monitor > Overview**. The default view (**Overview**) is displayed by default, as shown in Figure 9-1. Using the **Overview** page under **Monitor** as an example, this section describes how to manage and configure views.

Figure 9-1 Monitoring overview

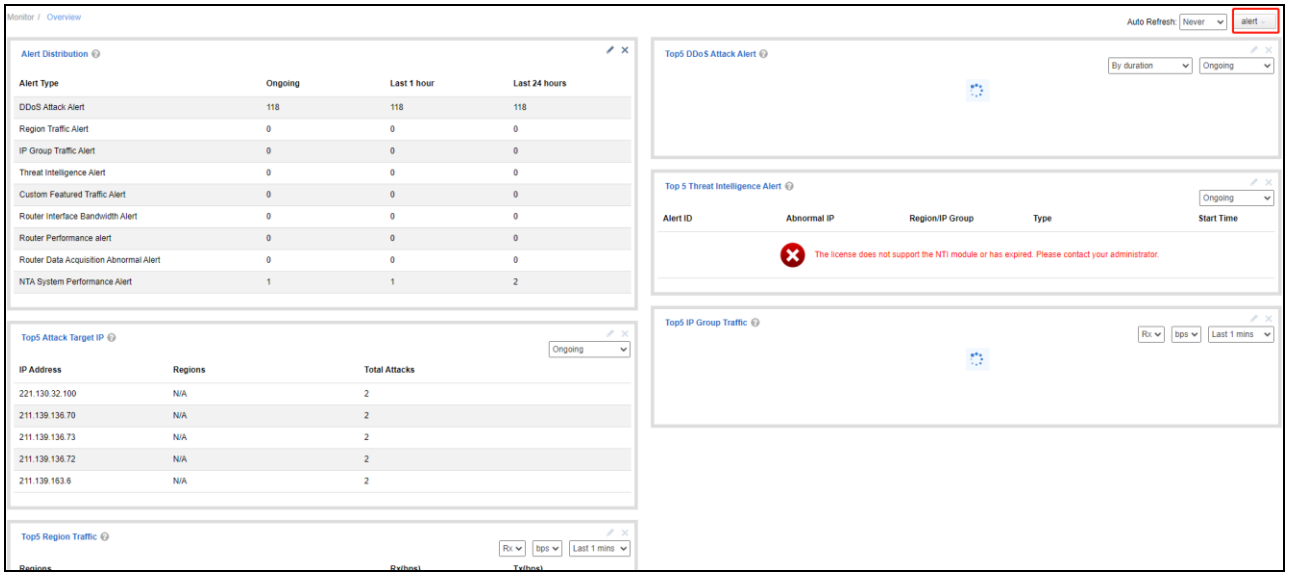


9.1.1 Adding a View

In the upper-right corner of the **Overview** page, click the button showing the view name (**Overview** in this example), and click **Add View** on the dropped-down list. In the dialog box that appears, type the view name and click **OK**. Then the new view appears on the **Overview** page, as shown in Figure 9-2.

The new view contains all widgets by default. You can click ✕ in the upper-right corner of a widget to delete it or ✎ to edit it.

Figure 9-2 New view named alert



9.1.2 Editing a View

You can change the view name, delete a widget, add a widget, or move a widget.

Changing the View Name

In the upper-right corner of the **Overview** page, click the button showing the view name, and click **Edit View** on the dropped-down list. Change the view name and click **OK**.

Deleting a Widget

To delete a widget from a view, click ✕ in the upper-right corner of the widget and then OK in the confirmation dialog box that pops up. Then the widget disappears from the view.

Adding a Widget

In the upper-right corner of the **Overview** page, click **Overview** and select **Add Pane** in the dropped-down list. Select a desired widget to add to the view and click **OK**.

Moving a Widget

To move a widget, hold the mouse on the widget name and drag it to the desired position.

Editing Widget Properties

Click ✎ in the upper-right corner of the widget. Change its title and frame color and click **OK**.

9.1.3 Deleting a View

Click the view name button (**Overview** by default), select Delete View from the drop-down list, and click OK in the confirmation dialog box that pops up.

9.1.4 Switching to a Desired View

To switch to a desired view, click the view name button in the upper-right corner of the page, and click the desired view. Then the **Overview** page displays the desired view.

9.1.5 Setting a View as Default

When the **Overview** page is opened, it automatically displays the default view, which can be changed.

To set a view as default, switch to the view, click the view name in the upper-right corner of the page, and click **As Default View**. The next time the **Overview** page is opened, it automatically displays the new default view.

9.2 Overall Monitoring Statistics

Choose **Monitor** > **Overview**. On the page, you can view overall monitoring statistics about traffic of and attacks against routers, regions, interfaces, and IP groups monitored by NTA.

Note	By default, the **Overview** page contains only one view named **Overview**. You can add new views and configure and manage them as required. For details, see section 9.1 View Management.

Viewing Overall Monitoring Statistics

NTA supports a maximum of seven monitoring widgets, which are described in Table 9-1.

Table 9-1 describes the widgets in details.

Table 9-1 Overall monitoring widgets

Widget Name	Description
Top 5 Attack Target IP	Displays top 5 IP addresses encountering most attacks. By default, the widget displays top 5 target IP addresses under ongoing attacks (Ongoing). Alternatively, you can configure the widget to display top 5 IP addresses under attacks ending in the past hour (**End(Last 1 hour)**) or past 24 hours (**End(**Last 24 hour)). You can click a region name to view more specific monitoring information. For details, see section 9.3 Regions.
Alert Distribution	Statistical information about alerts of all types, including ongoing alerts, alerts ending in the past hour, and those ending in the past 24 hours. For details, see section 8.1 Overview.
Top 5 DDoS Attack Alert	Displays top 5 DDoS attack alerts. • By default, alerts are sorted by attack duration. Alternatively, you can configure the widget to sort them by peak traffic in bps or pps or by peak connections in DDoS attacks. • By default, the widget displays top 5 alerts for ongoing DDoS attacks

Widget Name	Description
	(**Ongoing**). Alternatively, you can configure the widget to display top 5 alerts for DDoS attacks ending in the past hour (**End(Last 1 hour)**) or past 24 hours **(End(Last 24 hours)**). You can also click the ID of a listed alert to view its details. For details, see section 8.1.2 Information About Specified Alerts.
Top 5 Region Traffic	Displays top 5 regions by traffic received or transmitted within a specified interval. By default, regions are sorted by received (Rx) traffic in bps within the past minute. Alternatively, you can configure the widget to sort regions by received (Rx) or transmitted (Tx) traffic in bps or pps within the past minute (**Last 1 mins**), hour (**Last 1 hour**), or 24 hours (**Last 24 hours**). You can click a region's name to view its specific monitoring information. For details, see section 9.3 Regions.
Top 5 IP Group Traffic	Displays top 5 IP groups by traffic received or transmitted within a specified interval. By default, IP groups are sorted by received (Rx) traffic in bps within the past minute. Alternatively, you can configure the widget to sort IP groups by received (Rx) or transmitted (Tx) traffic in bps or pps within the past minute (Last 1 mins), hour (Last 1 hour), or 24 hours (Last 24 hours). You can click a region name to view more specific monitoring information. For details, see section 9.3 Regions.
Top 5 Interface Traffic (unavailable on NTA in DPI mode)	Displays top 5 interfaces by traffic received or transmitted within a specified interval. By default, interfaces are sorted by received (Rx) traffic in bps within the past minute. Alternatively, you can configure the widget to sort interfaces by received (Rx) or transmitted (Tx) traffic in bps or pps within the past minute (Last 1 mins), hour (Last 1 hour), or 24 hours (Last 24 hours). You can click an interface's name to view its specific monitoring information. For details, see section 9.4 Routers.
Top 5 Interface Group Traffic (unavailable on NTA in DPI mode)	Displays top 5 interface groups by traffic received or transmitted within a specified interval. By default, interface groups are sorted by received (Rx) traffic in bps within the past minute. Alternatively, you can configure the widget to sort interfaces by received (Rx) or transmitted (Tx) traffic in bps or pps within the past minute (**Last 1 mins**), hour (**Last 1 hour**), or 24 hours (**Last 24 hours**). You can click an interface group's name to view its specific monitoring information. For details, see section 9.5 Router Interface Groups.

Refreshing Monitoring Information

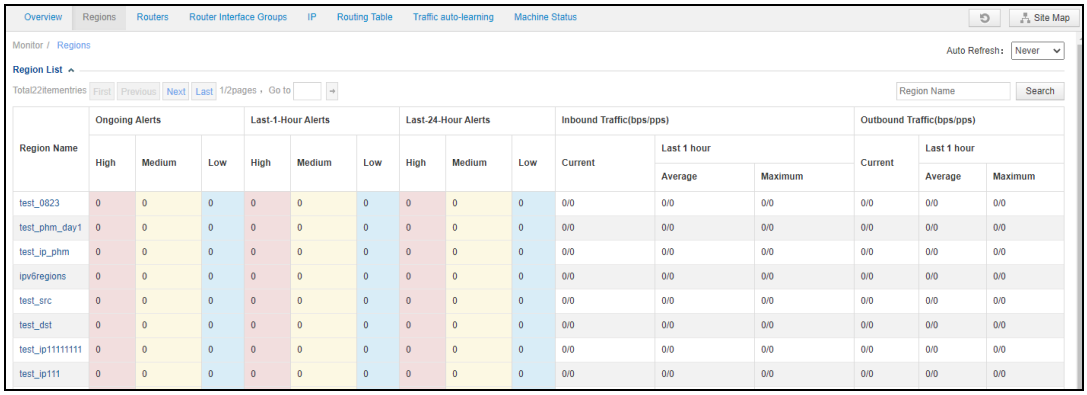
The default setting for **Auto Refresh** is **Never**, indicating that the system does not automatically refresh the page to obtain the latest monitoring information. Alternatively, you can set **Auto Refresh** to **30 sec**, **1 min**, or **5 mins**.

Note that the **Auto Refresh** setting is automatically restored to **Never** after the user exits or manually refreshes the page.

9.3 Regions

Choose **Monitor > Regions**. The page displays alert and traffic statistics of all regions by default. Alert statistics cover all high-, medium-, and low-level alerts that are ongoing, ending in the past hour, and ending in the past 24 hours. Traffic statistics cover the maximum and average traffic that each region receives and transmits currently and in the past hour.

Figure 9-3 Alert and traffic statistics of regions



Viewing Monitoring Information of a Specific Region

On the **Regions** page, click a region name to open this region's monitoring page, where all types of statistics are displayed. For the description of parameters on this page, see Table 9-2.

You can click **View other regions** in the upper-right corner of the current page to return to the previous page.

When the page is opened, it automatically displays the default monitoring view, which is initially the **default** view. Click **default** and choose commands from the drop-down list to manage views and add a widget.

Clicking a legend item hides or displays statistics of a type. Pointing to the region traffic trend graph displays the traffic data of the current node.

Note	By default, the region monitoring page contains only one view named **default**. You can add new views and configure and manage them as required. For details, see section 9.1 View Management.

Table 9-2 Region monitoring information

Parameter		Description
Basic Information of the Region		Displays the region ID, region name, contact person, and email address.
Region Monitor	Top 5 IP Traffic	Displays top 5 IP addresses in the region by traffic received or transmitted within a specified interval.

Parameter		Description
		The default interval is **5** minutes. You can click in the upper-right corner of the widget to change the title, frame color, and monitoring start and end time. By default, the system displays statistics about received traffic expressed in bps. You can configure NTA to sort IP addresses by received (Rx) or transmitted (Tx) traffic in bps or pps.
	Top 5 IP Group Traffic	Displays top 5 IP groups in the region by traffic received or transmitted within a specified interval. The default interval is **5** minutes. You can click in the upper-right corner of the widget to change the title, frame color, and monitoring start and end time. By default, the system displays statistics about received traffic expressed in bps. You can configure NTA to sort IP groups by received (Rx) or transmitted (Tx) traffic in bps or pps.
	Top 5 AS Traffic (unavailable on NTA in DPI mode)	Displays top 5 ASs in the region by traffic received or transmitted within a specified interval. If organization names corresponding to ASs are defined in the data dictionary, such organization names are displayed here. The default interval is **5** minutes. You can click in the upper-right corner of the widget to change the title, frame color, and monitoring start and end time. By default, the system displays statistics about received traffic expressed in bps. You can configure NTA to sort ASs by received (Rx) or transmitted (Tx) traffic in bps or pps.
	Ongoing Alert Events	Displays statistics about ongoing alerts, including alert IDs, levels, regions/IP groups to which alerts belong, alert types, and alert durations. You can click the ID of an alert to view and download more specific monitoring information about the alert. For details, see section 8.1.2 Information About Specified Alerts.
	Top 5 Application Traffic	Displays top 5 applications in the region by traffic received or transmitted within a specified interval in a histogram. The default interval is **5** minutes. You can click in the upper-right corner of the widget to change the title, frame color, direction, and monitoring start and end time. By default, the system displays statistics about received traffic expressed in bps. You can configure NTA to sort applications by received (Rx) or transmitted (Tx) traffic in bps or pps.
	Region Traffic Trend	Displays the trend of average or maximum traffic of a region within a specified interval in an area graph. Traffic statistics of the region are collected every 5 minutes. You can click in the upper-right corner of the widget to change the title, frame color, and monitoring start and end time. By default, the system displays statistics about the region's average traffic expressed in bps. You can configure NTA to display statistics by the maximum or average traffic in bps or pps.
	Top5 Protocol Traffic	Displays top 5 protocols in the region by traffic received or transmitted within a specified interval in a histogram. The default interval is **5** minutes. You can click in the upper-right corner of the widget to change the title, frame color, and monitoring start and end time. By default, the system displays statistics about received traffic expressed in bps. You can configure NTA to display statistics by received (Rx) or transmitted (Tx) traffic in bps or pps.

Parameter		Description
	Top 5 Packet Length Traffic	Displays top 5 packet lengths of all packets received and transmitted by a region within a specified interval in a histogram. The default interval is **5** minutes. You can click in the upper-right corner of the widget to change the title, frame color, direction, and monitoring start and end time. By default, the system displays statistics about received traffic expressed in bps. You can configure NTA to display statistics by received (Rx) or transmitted (Tx) traffic in bps or pps.
	Top 5 DSCP Traffic	Displays top 5 DSCPs in the region by traffic received or transmitted within a specified interval. The default interval is **5** minutes. You can click in the upper-right corner of the widget to change the title, frame color, direction, and monitoring start and end time. By default, the system displays statistics about received traffic expressed in bps. You can configure NTA to display statistics by received (Rx) or transmitted (Tx) traffic in bps or pps.
	Top 5 Prefix Traffic (unavailable on NTA in DPI mode)	Displays top 5 prefixes in the region by traffic received or transmitted within a specified interval. The default interval is **5** minutes. You can click in the upper-right corner of the widget to change the title, frame color, direction, and monitoring start and end time. By default, the system displays statistics about received traffic expressed in bps. You can configure NTA to display statistics by received (Rx) or transmitted (Tx) traffic in bps or pps.
	Top 5 Country/Region Traffic	Displays top 5 countries/regions in the region by traffic received or transmitted within a specified interval. The default interval is **5** minutes. You can click in the upper-right corner of the widget to change the title, frame color, direction, and monitoring start and end time. By default, the system displays statistics about received traffic expressed in bps. You can configure NTA to display statistics by received (Rx) or transmitted (Tx) traffic in bps or pps.

Refreshing Monitoring Information

The default setting for **Auto Refresh** is **Never**. To refresh monitoring information on the page, see Refreshing Monitoring Information.

9.4 Routers

NTA in DPI mode does not support this function.

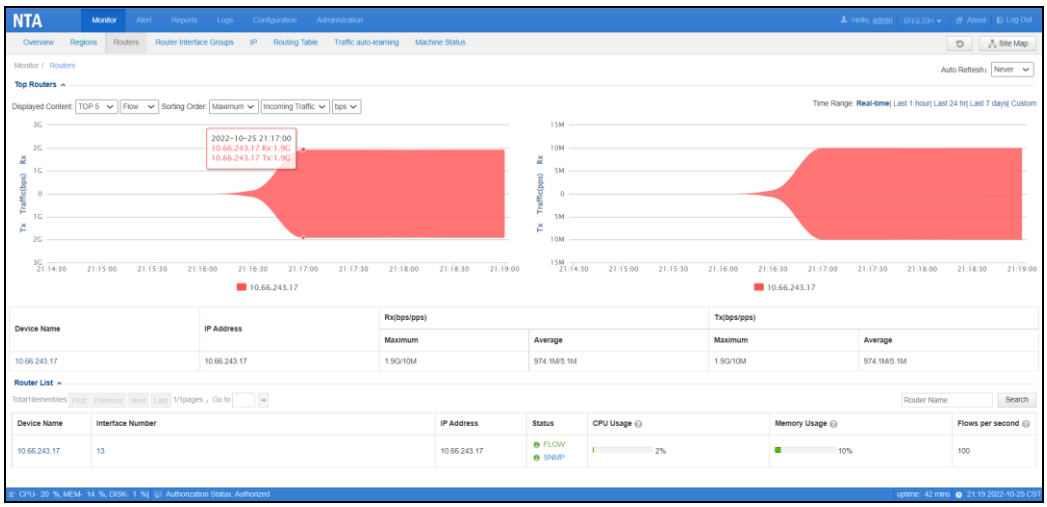
Choose **Monitor > Routers**. The **Routers** page displays performance and traffic statistics of all NTA-monitored routers. On this page, you can perform the following:

- Viewing Overall Statistics of Routers
- Viewing Monitoring Information of Interfaces on a Specific Router

9.4.1 Viewing Overall Statistics of Routers

The router monitoring page displays top routers with the most traffic and a list of routers, as shown in Figure 9-4.

Figure 9-4 Router monitoring



Viewing Top Routers with the Most Traffic

The **Top Routers** area shows curves indicating traffic statistics (see Table 9-3) of top routers with the most traffic.

Table 9-3 Information in the Top Routers area

Parameter		Description
Filter	**Displayed Content**	Specifies the content to be displayed. By default, traffic curves of top 5 routers with the most traffic and flow data are displayed. You can configure NTA to display the curves of top 5, top 10, or top 20 routers with the most flow or SNMP traffic.
	Sorting Order	Specifies how routers are sorted, by maximum or average traffic, by inbound or outbound traffic, and by pps or bps. By default, routers are sorted by the maximum inbound traffic in bps.
	Time Range	Specifies the period in which traffic statistics are collected. The value can be **Real-time**, **Last 1 hour**, **Last Day**, **Last 7 days**, or **Custom**.
Router traffic trend graph		Displays traffic trends of routers in bps and pps in area graphs.
Router List		Lists routers, including the device name, IP address, maximum/average inbound traffic, and maximum/average outbound traffic. Clicking the device name displays statistics of this device. For the subsequent operations, see Viewing Statistics of a Specified Router.

Viewing Statistics of All Routers Under Monitoring

The **Router List** area lists statistics of all routers.

Table 9-4 describes parameters of performance and traffic statistics of NTA-monitored routers.

Table 9-4 Parameters of performance and traffic statistics

Parameter	Description
Device Name	Name of the router. Clicking the device name displays statistics of this device. For the subsequent operations, see Viewing Statistics of a Specified Router.
Interface Number	Number of router interfaces obtained via SNMP or flow data. Clicking a number in the **Interface Number** column displays information about all monitored interfaces of the router, including basic settings, interface bandwidth usage, and inbound and outbound traffic.
IP Address	IP address that identifies the router.
Status	Indicates whether the device is receiving flow and SNMP data. • : receiving data • : not receiving data
CPU Usage	CPU usage of the router. To obtain the CPU usage of a monitoring object, when configuring a monitoring object under **Configuration** > **Objects**, you need to enable and configure SNMP collection, and enable **CPU Usage Alert** during the **Router Alert Configuration** phase. Otherwise, data related to the CPU usage of the monitoring object cannot be obtained, and the CPU usage is displayed as **N/A**. For the specific configuration methods, see sections 5.1.1.1 Configuring a Router and 5.3.1 Router Alert Template.
Memory Usage	Memory usage of the router. To obtain memory usage of a monitoring object, when configuring a monitoring object under **Configuration** > **Objects**, you need to enable and configure SNMP collection, and enable **Memory Usage Alert** during the **Router Alert Configuration** phase. Otherwise, data related to the memory usage of the monitoring object cannot be obtained, and the memory usage is displayed as **N/A**. For the specific configuration methods, see sections 5.1.1.1 Configuring a Router and 5.3.1 Router Alert Template.
Flows per second	Number of flows received by a router per second. To obtain flow data of a monitoring object, when configuring a monitoring object under **Configuration** > **Objects**, you need to enable and configure flow collection. Otherwise, flow data cannot be obtained or an error is displayed for flow obtaining. In this case, **N/A** is displayed in the list. For the specific configuration methods, see sections 5.1.1.1 Configuring a Router and 5.3.1 Router Alert Template.

Viewing Statistics of a Specified Router

Click the name of a desired router in the **Device Name** column. A page appears, showing basic information and monitoring information of the router.

To switch to the monitoring page of another router, expand the drop-down box next to the **Auto Refresh** drop-down box and click the name of the desired router.

In the **Device Basics** area, clicking opens the interface list of the router. For subsequent operations, see section 9.4.2 Viewing Monitoring Information of Interfaces on a Specific Router.

Refreshing Monitoring Information

The default setting for **Auto Refresh** is **Never**. To refresh monitoring information on the page, see Refreshing Monitoring Information.

9.4.2 Viewing Monitoring Information of Interfaces on a Specific Router

In the router list, click the number in the **Interface Number** column to view information of all monitored interfaces of the router, including basic settings, interface bandwidth usage, and inbound and outbound traffic.

Figure 9-5 Page showing interface monitoring information

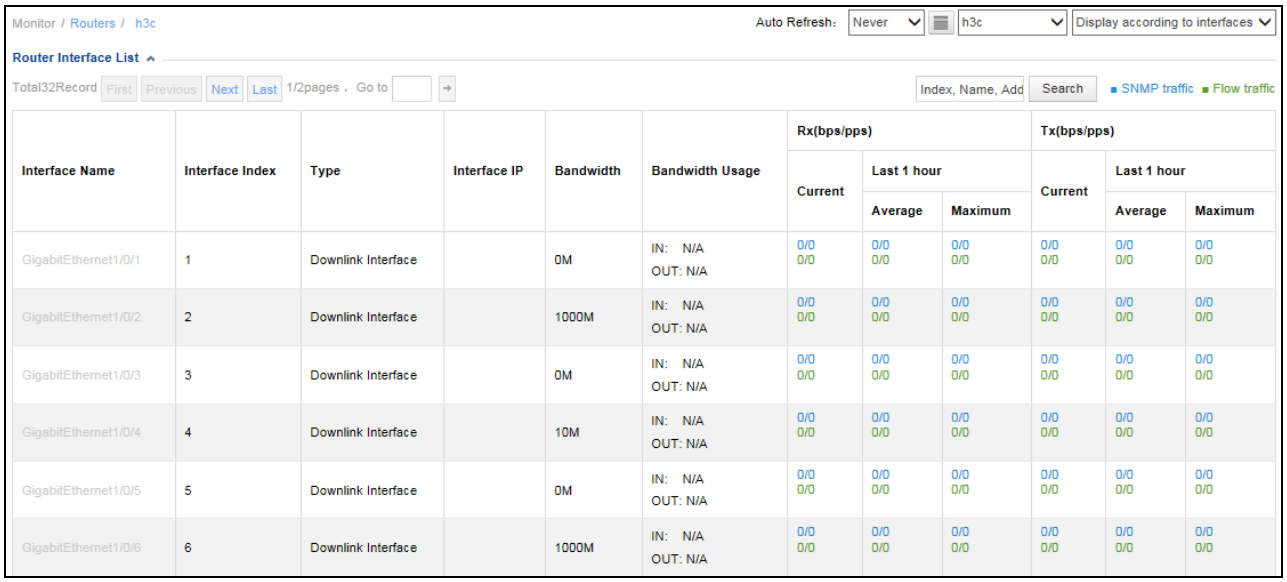


Table 9-5 describes parameters in the router interface list.

Table 9-5 Parameters in the router interface list

Parameter	Description
Favorite status	• ☆: indicates that the interface is not a favorite one. • ★: indicates that the interface is a favorite one.
Interface Name	Interface name that NTA obtains from the router via SNMP. If SNMP collection is disabled on the router or exceptions occur during SNMP data transmission, the interface index will be displayed as the interface name. The interface name will turn blue from gray only when SNMP monitoring is enabled on the interface of the router. For how to enable SNMP monitoring, see section 5.1.1.2 Configuring Router Interfaces. Clicking an interface name shows basic information and monitoring statistics of

Parameter	Description
	the interface. For the description of related parameters, see Table 9-2.
Interface Index	Interface index that NTA obtains from the router via flow data.
Type	Type of the interface, which may be an uplink or downlink interface.
Interface IP	Interface IP address that NTA obtains from the router via SNMP. If SNMP collection is disabled on the router or SNMP collection is enabled but no IP address is configured for the interface, nothing is displayed here.
Description	Brief description of the interface.
Bandwidth	Interface bandwidth that NTA obtains from the router via SNMP. If SNMP collection is disabled on the router or exceptions occur during SNMP data transmission, **N/A** is displayed.
Bandwidth Usage	Interface bandwidth usage that NTA obtains from the router via SNMP. If SNMP collection is disabled on the router, exceptions occur during SNMP data transmission, or if SNMP collection is enabled but monitoring is disabled for the interface, **N/A** is displayed.
Rx (bps/pps)	Information about traffic received over the interface, including current traffic and average and maximum traffic in the past hour. Numbers in blue indicate SNMP traffic, and those in green indicate flow traffic.
Tx (bps/pps)	Information about traffic transmitted over the interface, including current traffic and average and maximum traffic in the past hour. Numbers in blue indicate SNMP traffic, and those in green indicate flow traffic.

9.5 Router Interface Groups

NTA in DPI mode does not support this function.

Choose **Monitor > Router Interface Groups**. The **Router Interface Groups** page shows traffic statistics of all NTA-monitored router interface groups and detailed monitoring information of each router interface group, as shown in Figure 9-6. The methods of viewing monitoring interface of router interface groups are similar to those for routers. For details, see section 9.4 Routers.

Figure 9-6 Monitoring information of router interface groups

9.6 IP Addresses

You can view traffic statistics of a specified IP address on the **IP** page. Note that traffic statistics collected during the period when IP traffic statistics are disabled cannot be retrieved.

This function is disabled by default. It can be enabled only by **admin** in the console user interface.

Choose **Monitor > IP**, set query conditions, and click **Search**. Two graphs are displayed, showing the trends of the received (Rx) and transmitted (Tx) traffic of the specified IP address, respectively. The statistical granularity varies with the time range. For the description of query parameters, see Table 9-6.

The default setting for Auto Refresh is Never. For how to refresh the page, see Refreshing Monitoring Information.

Table 9-6 Traffic monitoring parameters of a specific IP address

Parameter	Description
Time Range	Specifies a time range, which can be **Last 1 hour**, **Last 24 hr**, **Last 7 days**, **Last 30 days**, or **Custom**. The default time range is **Last 1 hour**. For the selection of **Custom**, you need to further specify the start time and end time.
IP Address	Specify an address, which must belong to a region. Both IPv4 and IPv6 are supported.

9.7 Diversion Routing Table

Diversion routes on NTA are classified into the following types:

- IP Diversion — routes for diverting DDoS attack traffic destined for individual IP addresses, which are displayed dynamically.
- FlowSpec Diversion — routes for diverting DDoS attack traffic via FlowSpec, which are displayed dynamically.
- Group Diversion — routes for diverting abnormal inbound or outbound group traffic, which are displayed dynamically.
- Manual Diversion — static route that is manually added by users for forced diversion.
- Manual FlowSpec Diversion — static route that is manually added by users for forced diversion via FlowSpec.

9.7.1 IP Diversion

When a single IP address is under DDoS attacks, NTA diverts the attack traffic according to configured policies. During the diversion, the route for the diversion is displayed on the **IP Diversion** page under **Monitor > Routing Table**. After the diversion is complete, the route will be automatically removed from the page. You can also manually delete an IP diversion route.

Choose **Monitor > Routing Table > IP Diversion**. If there are many routes, you can locate specific routes by clicking **Search** and setting query conditions. Routes listed here include diversion routes of regions and IP groups as well as the default diversion route.

Table 9-7 describes parameters in the IP diversion route list.

Table 9-7 Parameters of IP diversion routes

Parameter	Description
Diversion IP Range	IP address and its subnet mask whose traffic is diverted.

Parameter	Description
Region/IP Group	Region or IP group to which the IP address with diverted traffic belongs. If such an IP address does not belong to any region or IP group, **Default Diversion Policy** is displayed.
Current Alert	Number of ongoing alerts. Hovering the mouse over the number displays alert causes.
Trigger Strategy	Type of the alert that triggers the diversion.
Triggering Threshold	Threshold for actual traffic (in bps and pps) or abnormal connections that triggers the diversion.
Current	Current attack traffic (in bps and pps) or current abnormal connections.
Diversion Mode	Mode of the IP diversion, which can be either of the following: • **Auto IP diversion**: indicates that traffic to a specific IP address is diverted when DDoS attack traffic is detected. • **Manual IP diversion**: indicates that traffic of an IP address or IP segment is diverted when hitting a manual traffic diversion rule or when you revoke an auto IP diversion route.
Diversion Type	Type of the IP diversion, which can be one of the following: • **Scrubbing Device Diversion**: indicates that traffic is diverted to the scrubbing devices. • **Null-Route Diversion**: indicates that traffic is diverted to a null-route IP address using the Border Gateway Protocol (BGP). In this case, BGP next-hop IP address is the null-route IP address. • **BGP Diversion**: indicates that traffic is diverted to a protection device using BGP. In this case, the IP address of the protection device is the BGP next-hop IP address.
Diversion Target/BGP next-hop IP address	• **Diversion Target**: indicates the destination to which traffic is diverted. It displays information about the scrubbing device or BGP session. • **BGP next-hop IP address**: information displayed only when **Diversion Type** is **BGP Diversion** or **Null-Route Diversion**. • When **Diversion Type** is **BGP Diversion**, the BGP next-hop IP address is the IP address of the protection device. • When **Diversion Type** is **Null-Route Diversion**, the BGP next-hop IP address is the null-route IP address of the diversion.
Start Time	Time when traffic diversion starts.
Diversion Holding Time (Min)	Time during which diversion is conducted. This parameter takes effect only when **Diversion Type** is **Null-Route Diversion** or **BGP Diversion**. NTA starts a countdown immediately after sending a null-route/BGP diversion route, and automatically revokes the diversion when the diversion holding time reaches **0**.
Processing Status	Indicates whether NTA successfully processes a diversion request. Note that "Processed" does not mean that the router or the scrubbing device successfully sends a diversion route. In fact, "Processed" only means that NTA successfully sends a diversion request.
Remarks	Necessary supplementary information about the route. If there are remarks,  is displayed, and you can view such information by hovering the mouse over  . If there are no remarks, **N/A** is displayed.

Parameter	Description
	You can click in the **Operation** column to add and edit remarks.
Operation	• Click to add and edit remarks. • Click to manually revoke the diversion route. You can also select the check boxes of multiple routes and click **Bulk Withdraw Diversion** in the upper-right corner of the page to delete these routes in one go. After the revocation, the route(s) will be automatically removed. You can view the related logs among the ones whose **Diversion Mode** is **Manual IP Diversion** under **Logs > Diversion Log**.

9.7.2 FlowSpec Diversion

Choose **Monitor > Routing Table > FlowSpec Diversion**. On this tab page, you can query active diversion routes for traffic diversion via FlowSpec. Such a route will be automatically deleted after the diversion is complete. You can also manually delete a FlowSpec diversion route.

Table 9-8 describes parameters of FlowSpec diversion routes.

Table 9-8 FlowSpec diversion route parameters

Parameter	Description
Name	Number of the FlowSpec diversion route.
Alert ID	ID of the alert corresponding to this diversion event.
Region/IP Group	Region or IP group to which the IP address with diverted traffic belongs. If this IP address does not belong to any region or IP group, **Default Diversion Policy** is displayed.
Protocol	Protocol used for exchanging routing information during diversion of traffic via FlowSpec.
Source IP	Source IP address of traffic diverted via FlowSpec.
Source Port	Source port of traffic diverted via FlowSpec.
Destination IP	Destination IP address of traffic diverted via FlowSpec.
Destination Port	Destination port of traffic diverted via FlowSpec.
Start Time	Time when FlowSpec diversion starts.
Diversion Holding Time (Min)	Time during which diversion is conducted. This parameter takes effect only when **Diversion Type** is **Null-Route Diversion** or **FlowSpec BGP Diversion**. NTA starts a countdown immediately after sending a null-route/BGP FlowSpec diversion route, and automatically revokes the diversion when the diversion holding time reaches **0**.
Packet Length	Length of diverted packets.
Action	Action taken on the diverted traffic.
FlowSpec BGP	Name of the BGP FlowSpec session.
Processing Status	Indicates whether NTA successfully processes a diversion request. Note that "Processed" does not mean that the router or the scrubbing device

Parameter	Description
	successfully sends a diversion route. In fact, "Processed" only means that NTA successfully sends a diversion request.
Operation	• You can click  to add and edit remarks. • You can click  to manually revoke the diversion route. You can also select the check boxes of multiple routes and click **Bulk Withdraw Diversion** in the upper-right corner of the page to delete these routes in one go. After the revocation, the route(s) will be automatically removed.

9.7.3 Group Diversion

Group diversion routes are used for diversion of abnormal traffic received or transmitted by regions and IP groups. Group diversion routes are displayed dynamically. That is, a group diversion route is displayed when abnormal traffic received or transmitted by a region or IP group is diverted according to configured policies, and removed automatically when the diversion is completed.

Choose **Monitor > Routing Table > Group Diversion**. If there are many routes, you can locate specific routes by clicking **Search** and setting query conditions. After diversion is complete, the related route is automatically deleted.

Table 9-9 describes parameters of group diversion routes.

Table 9-9 Parameters of group diversion routes

Parameter	Description
Diversion IP Range	IP address and its subnet mask whose traffic is diverted.
Region/IP Group	Region or IP group to which the IP address with diverted traffic belongs. If such an IP address does not belong to any region or IP group, **Default Diversion Policy** is displayed.
Current Alert	Number of ongoing alerts. Hovering the mouse over the number displays alert causes.
Trigger Strategy	Type of the alert that triggers the diversion.
Trigger Traffic	Rate and unit of the traffic that triggers the diversion.
Current Attack Traffic	Current attack traffic.
Diversion Mode/Diversion Type	• **Diversion Mode**: Mode of group diversion, which can only be **Auto Diversion**. • **Diversion Type**: type of group diversion, which can be one of the following: - **Scrubbing Device Diversion**: indicates that traffic is diverted to the scrubbing devices. - **Null-Route Diversion**: indicates that traffic is diverted to a null-route IP address using BGP. In this case, the BGP next-hop IP address is the null-route IP address. - **BGP Diversion**: indicates that traffic is diverted to a protection device using BGP. In this case, the IP address of the protection device is the BGP next-hop IP address.

Parameter	Description
Diversion Target/BGP next-hop IP address	• **Diversion Target**: indicates the destination to which traffic is diverted. It displays information about the scrubbing device or BGP session. • **BGP next-hop IP address**: information displayed only when **Diversion Type** is **BGP Diversion** or **Null-Route Diversion**. - When **Diversion Type** is **BGP Diversion**, the BGP next-hop IP address is the IP address of the protection device of the diversion. - When **Diversion Type** is **Null-Route Diversion**, the BGP next-hop IP address is the null-route IP address of the diversion.
Start Time	Time when traffic diversion starts.
Diversion Holding Time (Min)	Time during which diversion is conducted. This parameter takes effect only when **Diversion Type** is **Null-Route Diversion** or **BGP Diversion**. NTA starts a countdown immediately after sending a null-route/BGP diversion route, and automatically revokes the diversion when the holding time reaches **0**.
Processing Status	Indicates whether NTA successfully processes a diversion request. Note that "Processed" does not mean that the router or the scrubbing device successfully sends a diversion route. In fact, "Processed" only means that NTA successfully sends a diversion request.
Remark	Necessary supplementary information about the route. If there are remarks,  is displayed, and you can view such information by hovering the mouse over  . If there are no remarks, **N/A** is displayed. You can click  in the **Operation** column to add and edit remarks.
Operation	• Click  to add and edit remarks. • Click  to manually revoke the diversion route. You can also select the check boxes of multiple routes and click **Bulk Withdraw Diversion** in the upper-right corner of the page to delete these routes in one go. After the revocation, the route(s) will be automatically removed.

9.7.4 Manual Diversion

Manual diversion routes refer to static routes that are manually added by users for forced diversion.

Choose **Monitor > Routing Table > Manual Traffic Diversion**, click **Add** in the upper-right corner of the page, and configure a manual diversion route.

A manual diversion route, after being created, can be edited, deleted, and dispatched to a network for traffic diversion.

Table 9-10 Parameters for adding a manual diversion route

Parameter	Description
Diversion IP	IP address whose traffic is to be diverted.
Diversion Subnet Length	Subnet length of the IP address or IP segment whose traffic is to be diverted. This parameter appears and needs to be specified when **Diversion Type** is set to **Null-Route Diversion** or **BGP Diversion**.

Parameter	Description
Diversion Duration(Min)	Specifies manual diversion duration. It has the following values: • **Unlimited**: specifies that the diversion will last till you manually revoke it. For how to revoke diversion, see section 9.7.1 IP Diversion or 9.7.2 FlowSpec Diversion. • **Custom**: specifies a duration in minutes. When the duration expires, NTA automatically revokes the diversion.  For scrubbing device diversion, after receiving a diversion revocation request from NTA, the scrubbing device does not immediately revoke diversion. In fact, the scrubbing device revoking diversion has nothing to do with whether NTA sends a diversion revocation request. The scrubbing device checks for DDoS attacks on its own. If detecting a DDoS attack, the scrubbing device continues to divert traffic. If detecting no DDoS attack, the scrubbing device revokes diversion after a 5-minute countdown.
Diversion Mode	Type of diversion, which can be one of the following: • **Scrubbing Device Diversion**: indicates that NTA diverts attack traffic to the scrubbing device. For how to specify such a scrubbing device for this purpose, see section 5.5.3 Protection Device Configuration. • **BGP Diversion**: indicates that NTA sends a BGP routing notification to the router for traffic diversion. For this purpose, you need to select a configured third-party router. For details, see section 5.5.3 Protection Device Configuration. For details about how to configure BGP parameters for sending routing notifications, see section 5.5.2 BGP Configuration. • **Null-Route Diversion**: indicates that NTA drops attack traffic by diverting it to a null route. When Null-Route Diversion is selected, Null Route IP appears. You need to select a null-route IP address for the parameter. For details, see section 5.5.2 BGP Configuration.
Null Route IP	For null route diversion, you should specify a null route IP address. For how to configure a null route IP address, see section 5.5.2 BGP Configuration.

9.7.5 Manual FlowSpec Diversion

Manual FlowSpec diversion routes refer to static routes that are manually added by users for forced diversion via FlowSpec.

Choose **Monitor > Routing Table > FlowSpec Manual Traffic Diversion**, click **Add**, and configure a manual FlowSpec diversion route.

A manual FlowSpec diversion route, after being created, can be edited, deleted, and dispatched to a network for traffic diversion.

Table 9-11 Parameters for configuring a manual FlowSpec diversion route

Parameter	Description
Address Type	Specifies an IP address type for manual FlowSpec diversion routes.

Parameter	Description
Name	Number of the manual FlowSpec diversion route.
Diversion Duration(Min)	Specifies the diversion duration, which can be either of the following: • **Unlimited**: indicates no limitation on the diversion duration. • **Custom time**: allows you to set a diversion duration in minutes. After a value is specified, NTA will start a countdown when the diversion begins. When the specified duration expires, the diversion automatically stops.
Protocol	Specifies one or more protocols of traffic to be checked. This field is available only when you select **IPV4** for **Address Type**.
Source IP/Port	Specifies the source IP address, subnet mask, and source port of traffic to be diverted via FlowSpec. Only one source IP address and port can be configured.
Destination IP/Port	Specifies the destination IP address, subnet mask, and destination port of traffic to be diverted via FlowSpec. Only one destination IP address and port can be configured.
DSCP	Specifies a DSCP value. The value range is 0–63. This field is available only when you select **IPV4** for **Address Type**.
Flow Label	Specifies a flow label. This field is available only when you select **IPV6** for **Address Type**.
Next Header	Specifies one or more protocols of the next packet header. Options include **udp** and **tcp**. This field is available only when you select **IPV6** for **Address Type**.
Tcp Flags	Specifies one or more TCP flag bits. Options include **FIN**, **SYN**, **RST**, **PSH**, **ACK**, and **URG**.
Icmp Type	Specifies one or more ICMP types.
Icmp Code	Specifies one or more ICMP codes.
Fragment	Specifies one or more fragment types. This field is available only when you select **IPV4** for **Address Type**.
Packet Length	Specifies the length of packets to be diverted to be equal to, greater than, or smaller than a value or within a range. The value range is 1–65535.
Action	Specifies an action to be taken by NTA on packets that match the preceding settings. Some actions require custom values, as indicated in online tips.
FlowSpec BGP	Specifies a BGP FlowSpec entry from the existing ones. For how to configure a FlowSpec BGP entry, see section 5.5.4 BGP FlowSpec Configuration.

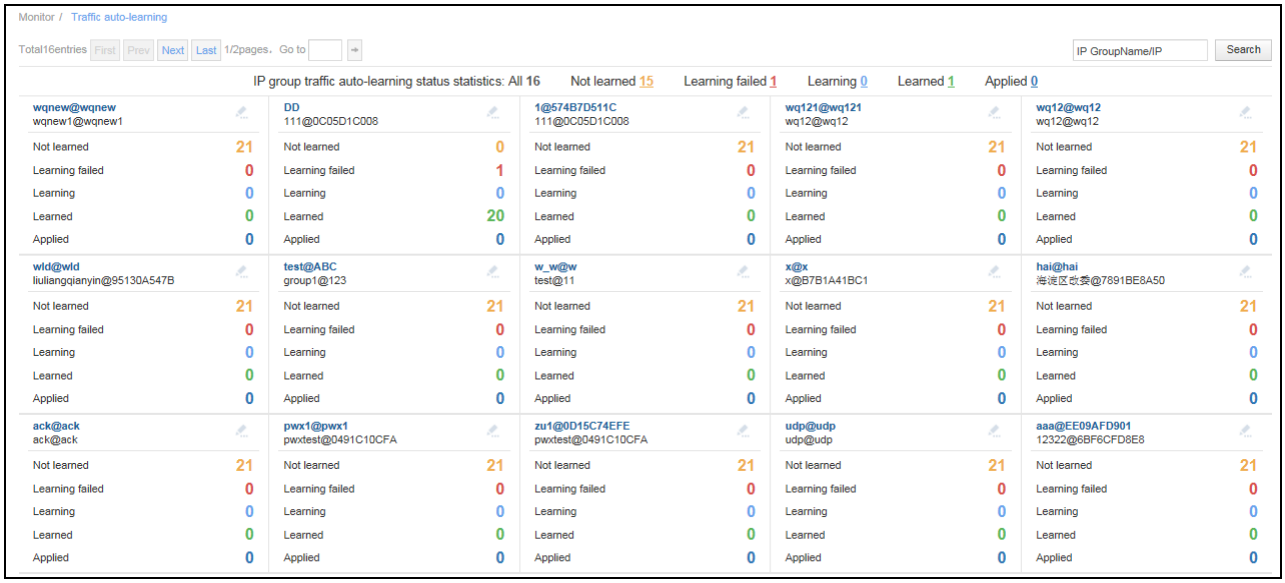
9.8 Traffic Auto-learning

For an IP group with baseline auto-learning enabled, its traffic auto-learning status (such as **Learning**, **Learning failed**, or **Learned**) and learning results can be viewed on the **Traffic auto-learning** page.

Choose Monitor > Traffic auto-learning. This page presents the traffic auto-learning information of all IP groups with baseline auto-learning enabled, as shown in Figure 9-7. You

can type an IP group name and click **Search** to view this group's auto-learning information. Fuzzy search is supported.

Figure 9-7 Monitoring of traffic auto-learning results



Viewing Traffic Auto-learning Information of IP Groups by Learning Status

IP group statistics by auto-learning status are listed at the top of the page shown in Figure 9-7.

Pointing to a number following the status, the mouse pointer turns to the hand shape from the angled arrow. Clicking the number shows statistics of IP groups in this specific learning state. For example, clicking the number next to **Learning** displays traffic auto-learning information of all IP groups in the Learning state.

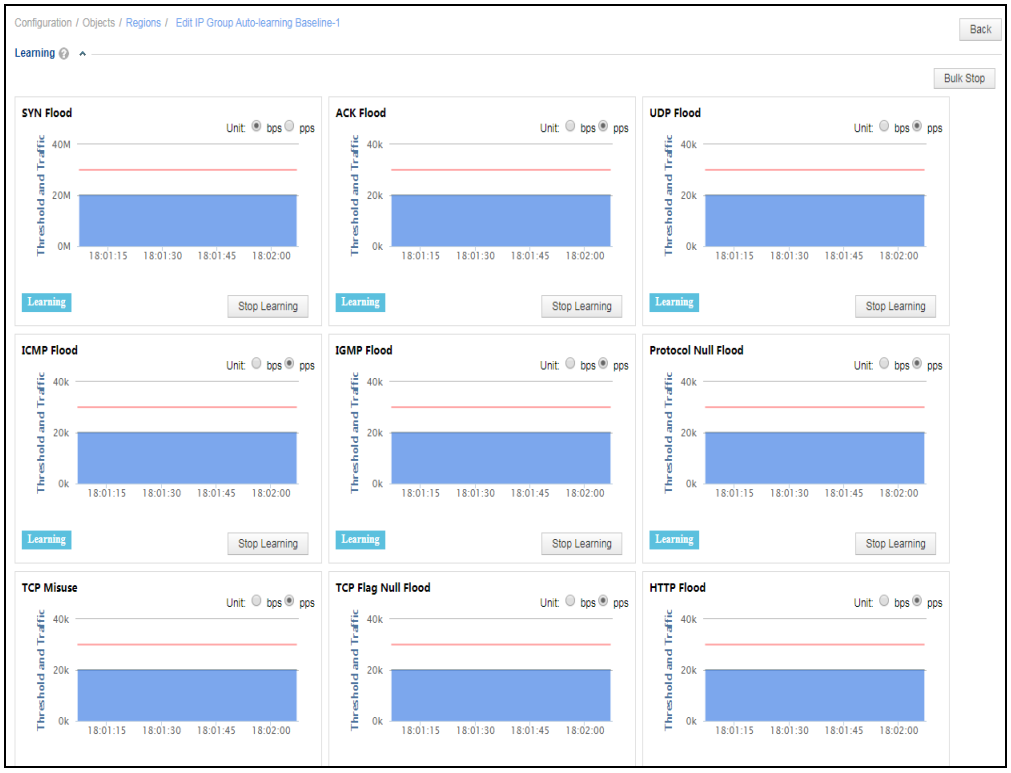
Viewing DDoS Attack Alerts of an IP Group

On the page shown in Figure 9-7, point to an IP group and you can view DDoS attack alerts of this IP group.

Viewing the Auto-learning Baseline Configuration of an IP Group

On the page shown in Figure 9-7, can click to view learning baseline configuration of an IP group, as shown in Figure 9-8. For details, see Configuring the Auto-Learning Baseline in section .5.1.3.7 Configuring an IP Group and Related Policies.

Figure 9-8 Editing auto-learning baseline settings of an IP group



9.9 Local Interfaces

NTA in DFI mode does not support this function.

Choose **Monitor > Local Interface**. The **Local Interface** page shows traffic trends of interfaces on NTA in the upper part and lists these interfaces in the lower part, as shown in Figure 9-9. You can set query conditions to view only interested traffic statistics.

Figure 9-9 Traffic statistics of local interfaces

Table 9-12 describes parameters in the traffic list.

Table 9-12 Parameters in the traffic list

Parameter	Description
Interface Name	Interface name.
Description	Brief description of the interface.
Interface IP	IP address of the interface. Note If an interface has multiple IP addresses, only the first IP address and its traffic information are displayed.
Rx(bps/pps)	Traffic received by the interface, in bps and pps.
Tx(bps/pps)	Traffic transmitted by the interface, in bps and pps.

9.10 Local Status

Choose **Monitor > Machine Status**. The **Machine Status** page displays the system status, basic information, system service, and interface status of the current NTA, as shown in Figure 9-10.

Figure 9-10 Machine Status page (DPI mode)

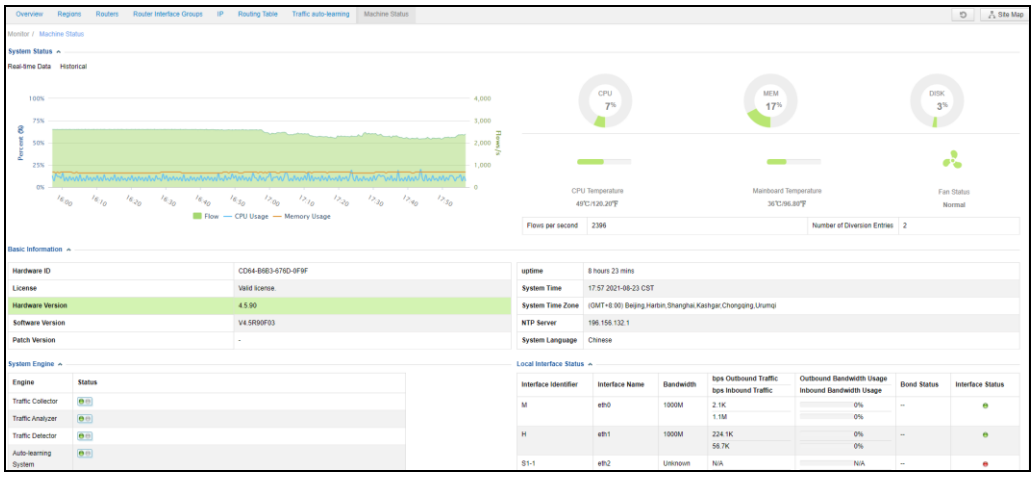


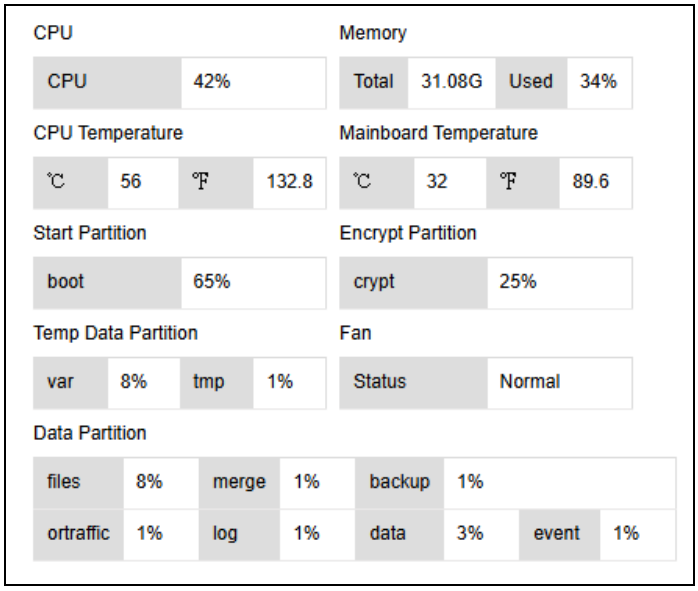
Table 9-13 Parameters on the Machine Status page

Parameter	Description
System Status	The **Real-time Data** page provides the following real-time data: • Trends of service traffic, memory usage, and CPU usage changes in the past 2 hours and the change trend of packets received per second on average in the past 30 seconds.

Parameter		Description
		• Current CPU, memory, and disk usage. • **Flows per second**: number of packets received per second on average in the past 30 seconds (available only on NTA in DFI mode). • **Real-time service traffic**: available only on NTA in DPI mode. • **Number of Diversion Entries**: number of IP addresses whose traffic is being diverted. Click **Historical** and specify a time frame to query historical system status data of that period. Clicking a legend item hides or displays statistics of the corresponding category. Hovering the mouse over the graph shows specific figures.
Basic Information	Hardware ID	Unique hardware ID of the current NTA.
	Product Logo	Product model of the current NTA.
	License	License status of the current NTA. For how to import a license, see section 4.7 License.
	Firmware Version	Firmware version of the current NTA.
	Software Version	Software version of the current NTA.
	Patch Version	Version of the patch that was last installed on NTA, if NTA has been upgraded by installing patch files.
	Uptime	Length of time from when NTA is switched on till the current moment.
	System Time	Time of NTA's internal clock. You can adapt it to your own geographical location. For details, see section 4.1.1.1 Configuring Basic Information.
	System Time Zone	Time zone of NTA's internal clock. You can adapt it to your own geographical location. For details, see section 4.1.1.1 Configuring Basic Information.
	NTP Server	NTP server used for system time synchronization. You can adapt it to your own network environment. For details, see section 4.1.1.1 Configuring Basic Information.
	System Language	Default language used by the web-based manager of the current NTA. You can change the system language. For details, see section 4.1.1.1 Configuring Basic Information.
System Engine		Whether all service engines of the current NTA have been enabled.
Local Interface Status		Traffic information of all physical interfaces on the current NTA. For the description of parameters, see Table 4-4.
Status bar	The status bar at the bottom of the page indicates the status of the current NTA.	
	CPU/memory/disk usage/authorization status	• Clicking the left part of the status bar CPU usage, memory usasge, disk usage, memeory temperature, motherboard temperature, start partition, encryption partition, temporary data partition, and data partition usage, as shown in Figure 9-11. • Clicking the authorization status in the left part of the status bar opens the **License** page, where you can view detailed information

Parameter		Description
		of the current license. For details, see section 4.7 License.
	Uptime/current time	In the right part of the status bar, you can view the uptime and system time of the current NTA.

Figure 9-11 Real-time usage information of the system



A Abbreviations

Abbreviation	Full Spelling
AS	autonomous system
ADS M	NSFOCUS Anti-DDoS System Management
BGP	Border Gateway Protocol
bps	bits per second
pps	packets per second
DDoS	distributed denial of service
DNS	Domain Name System
HTTP	Hyper Text Transfer Protocol
IDC	Internet data venter
IP	Internet Protocol
SSH	Secure Shell
NTP	Network Time Protocol
NTA	Network Traffic Analyzer
ESPC	Enterprise Security Planning Customer
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
URL	Uniform Resource Locator
PAP	Password Authentication Protocol
CHAP	Challenge Handshake Authentication Protocol
Spap	Shiva Password Authentication Protocol
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol

B Default Parameters

B.1 Default Network Settings

B.1.1 Default Settings of Local Interfaces

eth0 (M interface)	192.168.1.100/255.255.255.0
Other Interfaces	No IP address configured

B.1.2 Default Route Settings

IPv4 Default Gateway	192.168.1.1
IPv6 Default Gateway	None

B.1.3 Default Administrator Accounts

Role	User Name	Password	SSH Port
Web administrator	admin	admin	/
Console administrator	admin	admin	/
SSH administrator	conadmin	k@eT!23i	50022

B.2 Communication Parameters of the Console Port

Baud Rate	115200
Data Bits	8

B.3 Flow Collecting and Forwarding

NetFlow/NetStream/IPFIX Collecting Port	9999
sFlow Collecting Port	6343

C IPv4/IPv6 Support

The following table lists NTA's support for IPv4 and IPv6.

Function		IPv4	IPv6
Web login	Web login	√	√
Third-party interface	Email	√	√
	SNMP	√	√
	Syslog	√	√
	Cloud platform	√	×
	Third-party cloud platform	√	√
	BSA	√	×
	Cloud cleaning	√	×
	Management mode	√	√
	ATM	√	×
	NTI	√	×
Network interface configuration	Interface configuration IPv6	√	√
	Route	√	√
	DNS server	√	√
System configuration	NTP server	√	√
Diagnosis tools	ping	√	√
	traceroute	√	√
	telnet	√	√
User management	ACL	√	√
	Web API allowlist	√	√
	RADIUS authentication	√	×

Function		IPv4	IPv6
	TACAS Authentication	√	×
	LDAP Authentication	√	×
Hot standby	HA	√	√
Core business	Detection alerts	√	√
	Alert allowlist	√	√
	Diversion	√	√
	Flow settings	√	√
	Routers	√	√
	Regions	√	√
	IP groups	√	√
	Protection device configuration	√	√
	BGP configuration	√	√
Reports	Reports	√	√