NSFOCUS NIPS
User Guide

Version: V5.6R10F02 (2017-03-27)

Contents

Figures

Tables

Preface

Scope

This document describes major functions and usage of the web-based manager and console user interface of NSFOCUS Network Intrusion Prevention System ("NIPS" for short).

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

Audience

This document is intended for the following users:

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

This document assumes that you have knowledge in the following areas:

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

Organization

Chapter	Description
1 Product Overview	Describes NIPS's characteristics and major functions, and methods of managing NIPS.
2 Home	Describes information that you can obtain from the Home module.
3 Alert Center	Describes how to view alert events on NIPS.
4 System	Describes common operations and methods for system maintenance.
5 Network	Describes configurations related to network connection.
6 Objects	Describes how to configure system objects.
7 Policies	Describes how to configure system policies.
8 Logs and Reports	Describes how and what to view about various logs and reports.
9 Console-based Management	Describes how to log in to and manage NIPS via the console user interface.

Chapter	Description
A Acronyms and Abbreviations	Describes acronyms and abbreviations used in this document.
B AD Domain Configurator Management	Describes how to install and configure the Active Directory (AD) domain configurator.
C Default Parameters	Describes default settings of NIPS.

Conventions

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

Customer Support

Email: support@nsfocusglobal.com

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

Contact:

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

- Hong Kong +852 5803 2673 or +852 5803 2NSF
- Middle East: +973 1619 7607

1 Product Overview

Security issues are getting increasingly complicated in recent years. Customers are vexed by various security threats, especially mixed ones, such as worms, viruses, spyware, distributed denial-of-service (DDoS) attacks, spam, and network resource abuse (P2P download, instant messaging (IM), online games, videos ...). Enterprises' information networks are at the risk of severe damage.

NIPS is a next-generation network security product developed by NSFOCUS. As a networked product, it is designed to accurately monitor abnormal network traffic and block all kinds of attack traffic, especially threats at the application layer, in real time instead of alerting upon detection of malicious traffic. Superior to conventional firewalls and intrusion detection systems (IDSs), NIPS is a brand-new solution that provides dynamic, in-depth, and proactive intrusion prevention for enterprise networks.

This chapter contains the following sections:

Section	Description
Product Characteristics	Describes outstanding characteristics of NIPS.
Main Functions	Describes major functions of NIPS.
Management Modes	Describes methods for managing NIPS.

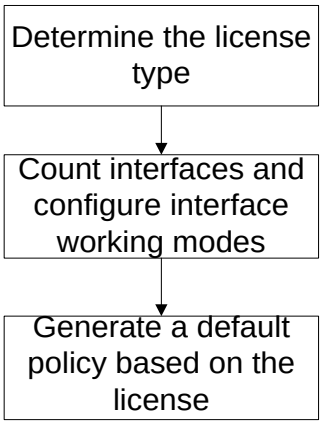
1.1 Product Characteristics

Compared with other vendors' intrusion prevention devices, NIPS can work immediately out of the box thanks to its zero-configuration networking (zeroconf) function. This function is available thanks to NIPS's mature built-in security policy templates. Based on the imported license, NIPS can automatically configure interfaces, select an appropriate template, add a default security policy, and enable the protection mode.

Common intrusion prevention devices can be used only after users perform complicated configuration procedures. This poses an obstacle to those who have never used a security device. To streamline the configuration procedure and improve the ease of use, NIPS is embedded with diverse scenario models, making it plug-and-play and usable without manual operator intervention.

Figure 1-1 shows the basic procedure for NIPS to go through before going live.

Figure 1-1 Go-live procedure of NIPS



Note	After the correct license is imported, NIPS automatically configures two adjacent network interfaces as a pair of interfaces working in direct mode.

Generally, after the go-live procedure is complete, NIPS automatically generates a default security policy, as shown in Figure 1-2.

Figure 1-2 Default security policy generated after the go-live procedure

NIPS's zeroconf function is convenient, making NIPS easy to use. However, it cannot cover all scenarios to meet special configuration needs. In practice, a network may require hybrid deployment and a customer may want to use two nonadjacent interfaces as a pair to work in direct mode. Therefore, NIPS must allow users to modify interface and security policy configurations as required.

When implementing the zeroconf function, NIPS checks the current configurations. If it finds user-defined configurations or the system not in initial state, it will not automatically configure interfaces and security policies.

1.2 Main Functions

NIPS integrates cutting-edge intrusion prevention technologies into its advanced system structure. It is a next-generation intrusion prevention engine that takes in-depth, all-round protocol analysis as the basis and protocol identification, protocol anomaly detection, and association analysis as the core. It provides users with the following functions:

- Network protection

  NIPS provides real-time and proactive network protection. It also supports traffic management, effectively identifying potential abnormal traffic and preventing DoS attacks.
- Application protection

  NIPS provides protection for the application layer. For operating systems, applications, and databases, it filters out malicious traffic and attack packets through in-depth content detection, so as to prevent the existing vulnerabilities from being exploited and to protect operating systems and applications from damage and breakdown.
- Content management

  NIPS provides content management over intranet resources, effectively detecting and blocking spyware (including trojan backdoor, malware, and adware), as well as monitoring and blocking IM, P2P downloads, online games, and online videos.
- Antivirus

  NIPS can detect and remove nearly 1 million viruses (trojan, worms, macro viruses, and script viruses) related to various protocols, including HTTP, SMPT, POP3, and FTP. Moreover, it can effectively control, detect, and block multithreading and in-depth file compressing behaviors.

1.3 Management Modes

NIPS can be managed in either of the following ways:

- Web-based management

  This is a method implemented through the web-based manager, whose intuitive human-machine interfaces provide all necessary management functions. NIPS supports Internet Explorer, Firefox, and Chrome browsers.
- Console-based management

  This is a method implemented through the command line interface (CLI) for basic operations.

1.3.1 Web-based Management

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

1.3.1.1 Roles and Permissions

The web-based manager of NIPS has three types of roles:

- Operator

An operator has permissions of managing and configuring the web-based manager. **admin** is the default system operator account.

- Auditor

  An audit administrator has permissions of viewing system logs. **auditor** is the default auditor account.

- Maintainer (**supervisor**)

  A maintainer has the same permissions as an operator for managing and configuring the web-based manager, but cannot restart the device or engine, or manage accounts.

On NIPS, different roles have different permissions, as shown in Table 1-1.

Table 1-1 Privileges of different roles

Role		Permissions
Operator	**admin** (default)	Has all permissions except managing auditors (but can enable the default auditor account **auditor**) and viewing system logs.
	New operator (created by **admin** and has read and write permissions)	Has all permissions except managing other users and viewing system logs.
	New operator (created by **admin** and has the read permission)	Has permissions of changing the current account's password and viewing pages he or she has permissions to operate; cannot write to or update system files.
Auditor	**auditor** (default)	Has permissions of managing auditor accounts and viewing system logs after being enabled by **admin**.
	New auditor (created by **auditor**)	Has permissions of changing the current account's password and viewing system logs.
Maintainer (**supervisor**)		Has all permissions except managing auditors viewing system logs, restarting the device or engine, and managing accounts.

1.3.1.2 Login to the Web-based Manager

This section takes an Internet Explorer browser as an example to describe how to log in to the web-based manager of NIPS.

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

Step 2 Open the Internet Explorer browser and connect to NIPS in HTTPS mode by typing the management IP address of NIPS, for example, **https://192.168.1.1**, in the address bar.

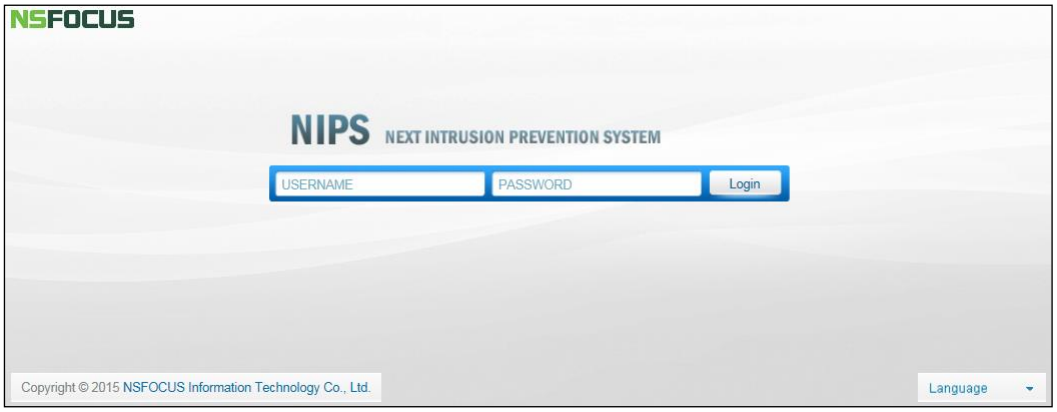
A security alert appears after you press **Enter**, as shown in Figure 1-3.

Figure 1-3 Security alert page

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

The NIPS login page appears, as shown in Figure 1-4.

Figure 1-4 Login page



Step 4 Type a valid user name and password.

For the first login, type the user name (**admin**) and password (**admin**) for the default operator.

Step 5 Click **Login**.

----End

Note	• Before login, check whether **Block pop-ups** is selected or JavaScript is disabled in the browser. If yes, uncheck the selection. • You are advised to use the latest Firefox or Internet Explorer 8.0 or later browser and set the browser resolution to 1024 x 768 or higher. • The default user name and password are both **admin**, which are used during the first login. You must change the password immediately after the first login. • The system will return to the login page if you remain inactive for over 5 minutes. In this case, you need to log in again to continue using the system. • The possible cause for a login failure may be (1) incorrect user name; (2) incorrect password; (3) upper/lower case confusion; or (4) account disabled or deleted.

1.3.1.3 Page Layout of the Web-based Manager

The user **admin** accesses the system after successful login. Figure 1-5 shows the general layout of the page.

Figure 1-5 Page layout of the web-based manager

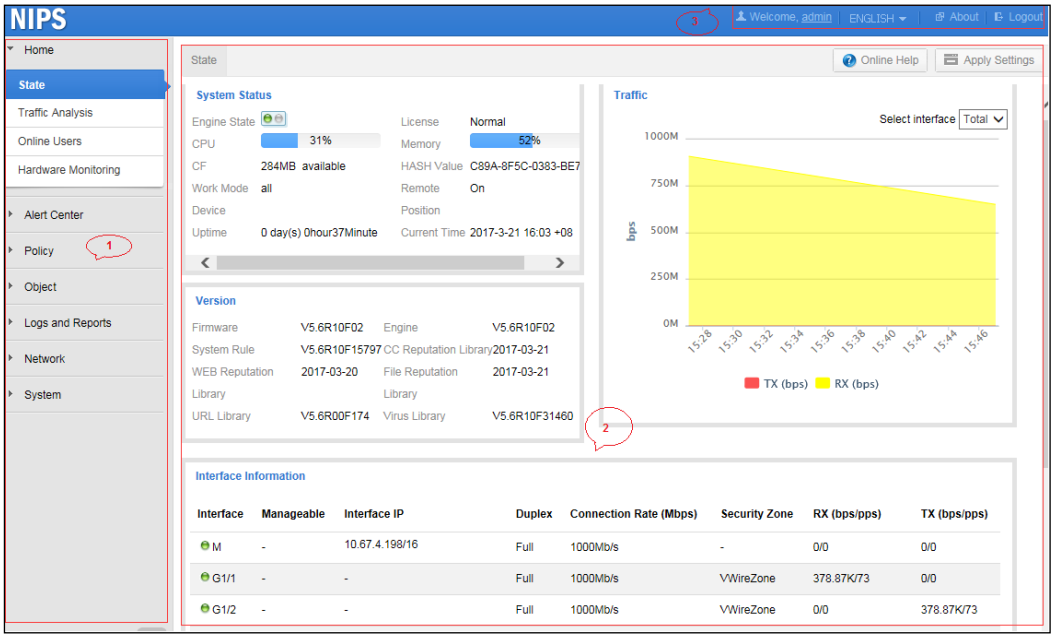


Table 1-2 describes the page layout.

Table 1-2 Page layout

No.	Area	Description
1	Navigation bar	Area where menus and related submenus are provided to help you locate system functions.
2	Work area	Area where you can perform configurations and operations and view data. Clicking Online Help displays online help information of NIPS.

No.	Area	Description
3	Quick access bar	Area providing the following common buttons of the system: • Welcome, admin: changes the password of the current account. • ENGLISH: switches the language. • About: presents information about NIPS. • Logout: logs you out of the web-based manager. Note For the sake of security, you are advised to click Logout to log out of the system.

Note	The menus and work area vary with user permissions.

1.3.1.4 Common Buttons and Their Functions

Table 1-3 describes common buttons and their functions.

Table 1-3 Common buttons and their functions

Button	Function
	Edits the current item.
	Deletes the current item. Note Predefined items, such as the "any" subnet, cannot be deleted. Referenced items cannot be deleted.
	Starts an operation.
	Stops an ongoing operation.
	Moves up/down a policy in a list.
/	Enables/Disables a policy.
	Copies the current item.
/ /	Exports a log or report as an HTML, Word, or Excel file.
	Prints logs or a report.
Search	Returns the query result according to the conditions a user has specified.

Tip	Pointing to a button displays the description of what the button does.

In addition to the common operations listed in Table 1-3, there is another important operation: apply settings.

On NIPS, settings can take effect only after being committed in either of the following ways:

- Click **Apply Settings** in the upper-right corner of the page.
- Choose **System** > **System Control** and then click **Apply Settings**.

1.3.2 Console-based Management

Through a console port, you can access the console user interface of NIPS, 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. The following sections describe how a console user accesses the console user interface of NIPS over a serial connection.

1.3.2.1 Console User

The default console user of NIPS is **conadmin**, with **conadmin** as the default password.

1.3.2.2 Login to the Console

Before logging in to NIPS using a serial connection, prepare the following:

- One PC
- One serial cable shipped in the accessory kit
- Terminal software that can connect to the console port
- NIPS connected to the PC with the serial cable

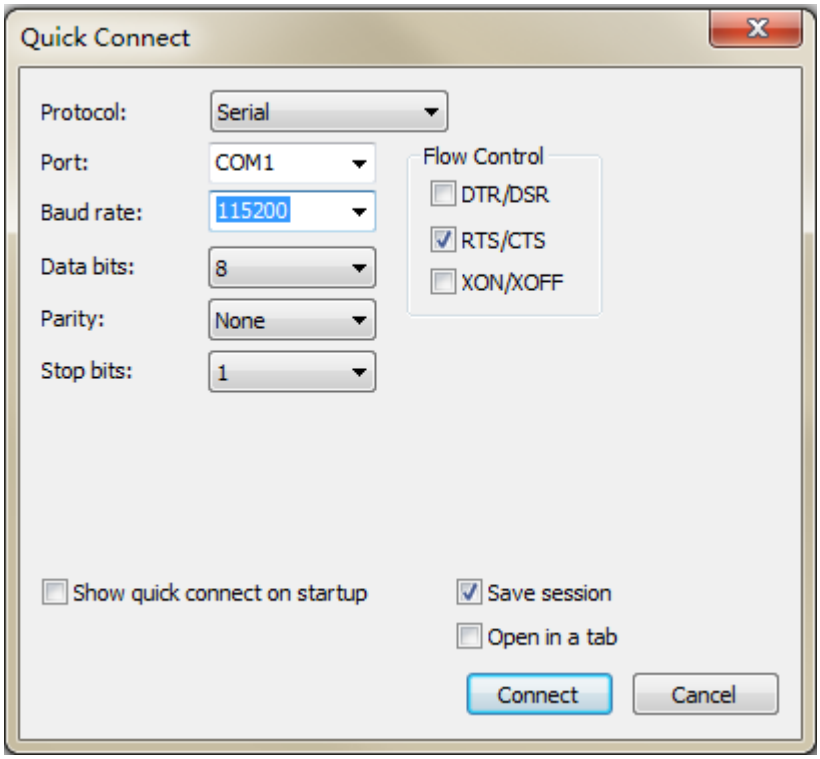
The following takes SecureCRT as an example to describe how to log in to the console user interface of NIPS:

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

Step 2 Configure fast connection parameters.

Set **Protocol** to **Serial**, **Baud Rate** to **115200**, and **Data Bits** to **8**, and leave other parameters at their default settings, as shown in Figure 1-6.

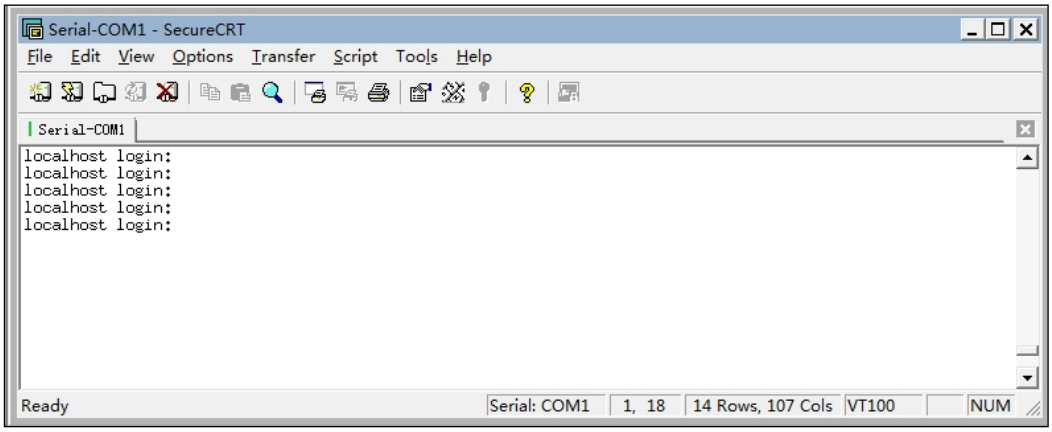
Figure 1-6 Configuring quick connection



Step 3 Click **Connect** and then press **Enter**.

The console login page appears, as shown in Figure 1-7.

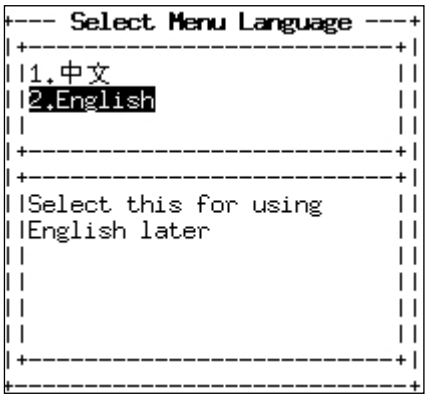
Figure 1-7 Console login page



Step 4 Type the user name and password (both are **conadmin** by default) of the console administrator.

You can successfully access NIPS if the user name and password are correct. Figure 1-8 shows the language selection page.

Figure 1-8 Selecting a language

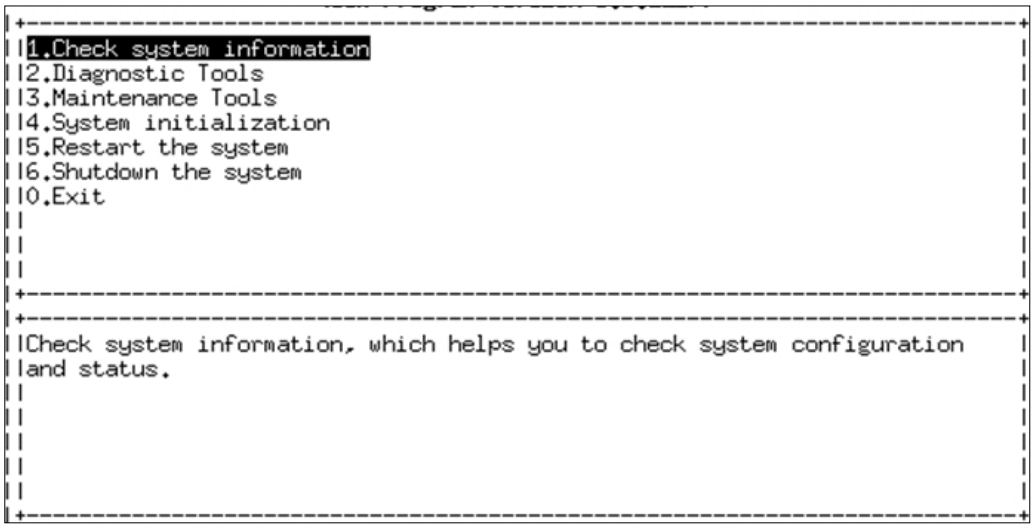


Tip	You can set the terminal type to **VT100** after connection to achieve the optimal display effect.

Step 5 Select **2. English** and press **Enter**.

The menu in English appears.

Figure 1-9 Main menu for console-based management



----End

In the console user interface, you can only perform operations with the keyboard. Table 1-4 describes the meanings of the frequently used keys.

Table 1-4 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.
→	(1) Switches to **Cancel**; (2) Moves right.
Esc	Cancels a setting.
Enter	Confirms a setting.
Tab	Switches between the input box, **OK**, and **Cancel**.
BackSpace	Deletes the character to the left of the cursor.

For how to manage NIPS through menus in the console user interface and the meanings of menu commands, see chapter 9 Console-based Management.

.

2 Home

The Home module allows you to view the basic status, traffic analysis data, and online users. This chapter contains the following sections:

Section	Description
State	Describes how to view the system status, traffic in the past 24 hours, version information, and interface information.
Traffic Analysis	Describes how to view traffic analysis data.
Online Users	Describes how to view information about online users.
Hardware Monitoring	Describes how to view hardware monitoring data.

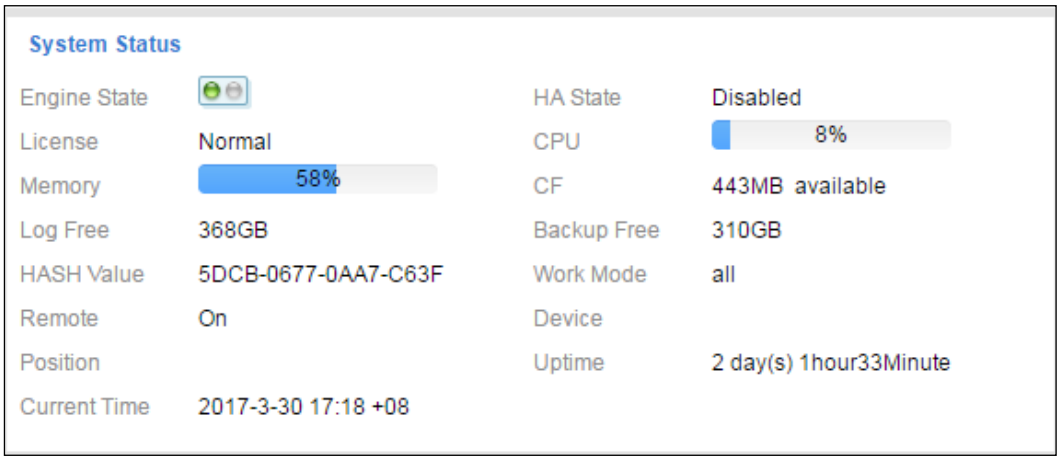
2.1 State

By default, the system displays the **State** page the first time you access NIPS. On this page, you can view the system status, traffic in the past 24 hours, version information, and interface information.

System Status

The **System Status** area displays basic information of NIPS, as shown in Figure 2-1.

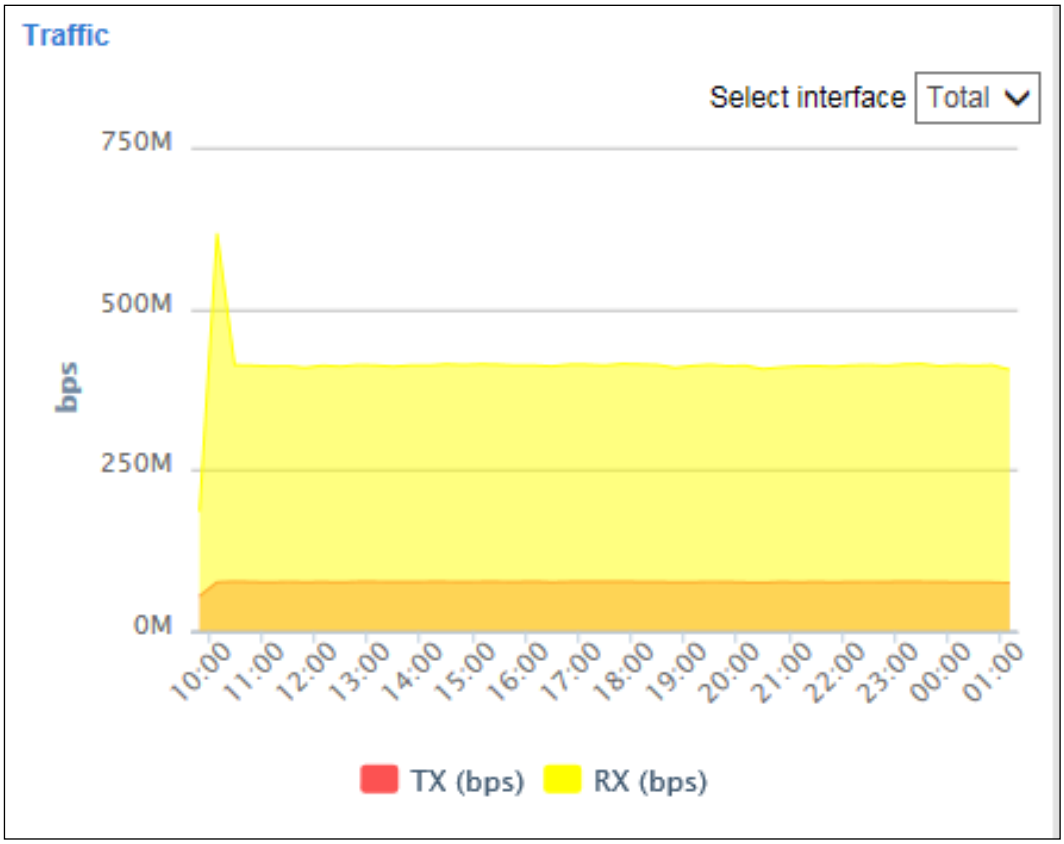
Figure 2-1 System status



Traffic Monitoring

The **Traffic** area displays the inbound and outbound traffic monitored by NIPS in the last 24 hours, as shown in Figure 2-2.

Figure 2-2 Traffic monitoring



By default, the system displays the total traffic of all interfaces. You can select an interface from the **Select interface** drop-down list in the upper-right corner of the **Traffic** area to view traffic received and transmitted by this interface in the past 24 hours.

Version Information

The **Version** area displays the firmware version and engine version of NIPS, and versions of rule libraries available on NIPS.

Figure 2-3 Version information

Interface Information

The **Interface Information** area displays basic information and traffic rates of each interface. Interface information varies with NIPS models.

- Figure 2-4 shows interface information of NX5-T9010A and NX5-T9020A.

Figure 2-4 Interface information of NX5-T9010A and NX5-T9020A

Interface Information

Interface	Interface Type	Medium Type	Manageable	Interface IP	Duplex	Connection Rate (Mbps)	Security Zone	RX (bps/pps)	TX (bps/pps)
M	Electrical	Copper	Yes	10.67.4.10/16	Full	1000Mb/s	Management	0/0	0/0
H1	Electrical	Copper	Yes	192.168.2.1/24	-	-	Management	0/0	0/0
T1/1	10G optical	Fiber	Yes	0.0.0.0/0	-	-	Monitor	0/0	0/0
T1/2	10G optical	Fiber	Yes	0.0.0.0/0	-	-	Direct-A	0/0	0/0
G2/1	Electrical	Copper	Yes	0.0.0.0/0	Full	100Mb/s	Direct-B	26.76K/22	192/0
G2/2	Electrical	Copper	Yes	0.0.0.0/0	Full	1000Mb/s	Direct-B	192/0	27.46K/22
G2/3	Electrical	Copper	Yes	0.0.0.0/0	-	-	Direct-C	0/0	0/0

- Figure 2-5 shows interface information of NIPS of other models.

Figure 2-5 Interface information of NIPS of other models

Interface Information

Interface	Manageable	Interface IP	Duplex	Connection Rate (Mbps)	Security Zone	RX (bps/pps)	TX (bps/pps)
M	-	10.67.4.162/16	Full	100Mb/s	-	0/0	0/0
H1	-	192.168.2.1/24	-	-	-	0/0	0/0
G1/1	-	-	-	-	VWireZone	55.95K/29	0/0
G1/2	-	-	-	-	VWireZone	0/0	55.95K/29
G1/3	-	-	-	-	VWireZone	0/0	0/0
G1/4	-	-	-	-	VWireZone	0/0	0/0
G2/1	-	-	-	-	VWireZone	0/0	0/0

All interfaces on the current device are displayed here. The green indicator indicates that an interface is Up and the red indicates that an interface is Down. The number of interfaces varies with device models.

- **Interface Type** indicates the type of the interface, which can be **Electrical**, **10G optical**, and **1000M optical**.
- **Medium Type** indicates the type of the cable to which the interface connects, which can be **Fiber** or **Copper**.

2.2 Traffic Analysis

The **Traffic Analysis** module consists of three tab pages: **TCP/UDP Traffic**, **Application Traffic**, **IP Traffic**, and **IP Session**. On each page, you can perform the following operations:

- Automatically refreshing data

  Select the **Auto Refresh** check box and set the refresh interval. Then, the system automatically refreshes traffic analysis data at the specified interval.
- Manually refreshing data

  Click **Manual Refresh** to refresh traffic analysis data manually on the current page.

The following sections detail operations on each page.

2.2.1 TCP/UDP Traffic

Choose **Home** > **Traffic Analysis** > **TCP/UDP Traffic**. The **TCP/UDP Traffic** page displays the total traffic passing through NIPS, historical application information, and the number of application sessions.

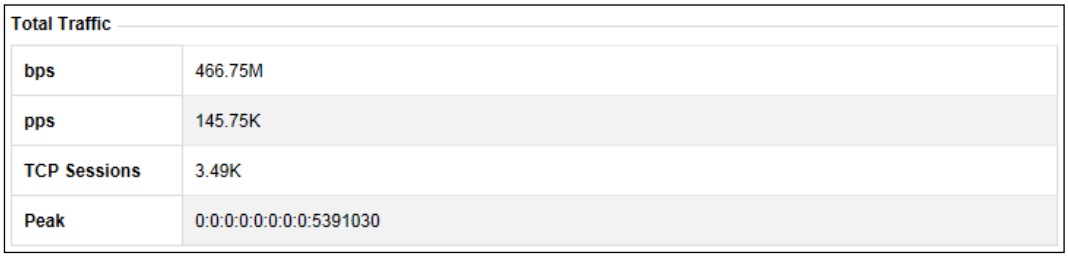
In the **Application History** and **Application Session Number** areas, you can specify the statistical granularity and application based on which data is displayed:

- **Display Granularity**: Select **hour**, **day(s)**, or **Week** to display the historical application information or the number of application sessions in the past 1 hour, 1 day, or 1 week.
- **Select the application**: Specify an application or all applications to display their historical information or the number of their sessions.

Total Traffic

The **Total Traffic** area lists the total traffic passing through all interfaces of NIPS, as shown in Figure 2-6.

Figure 2-6 Total traffic



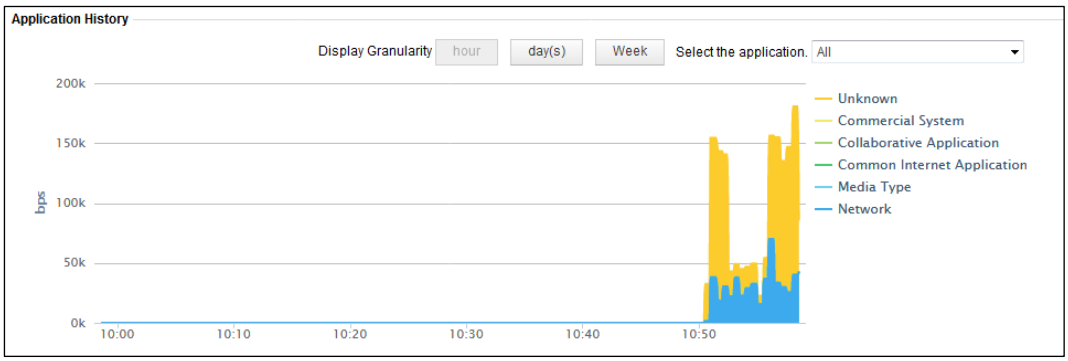
Total Traffic

bps	466.75M
pps	145.75K
TCP Sessions	3.49K
Peak	0:0:0:0:0:0:0:0:5391030

Application History

The **Application History** area displays historical traffic information of the specified applications, as shown in Figure 2-7.

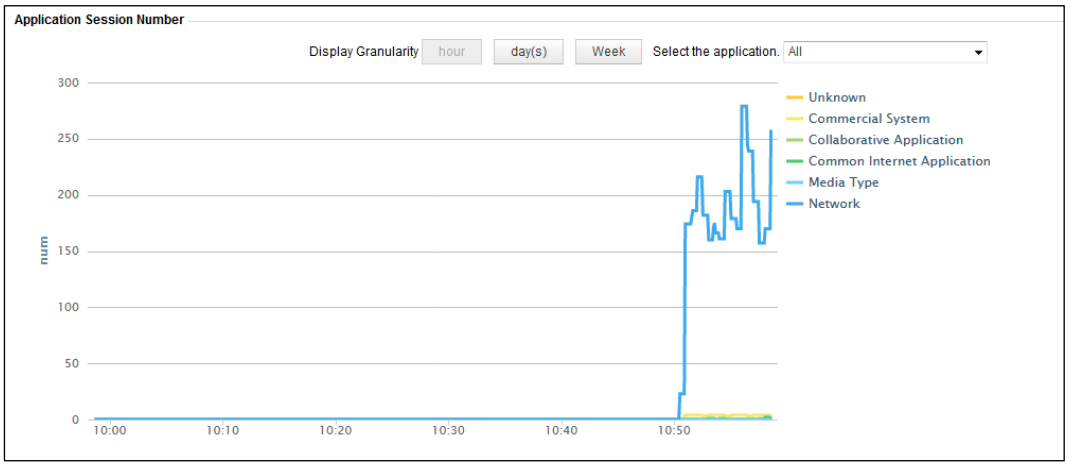
Figure 2-7 Historical traffic information of applications



Number of Application Sessions

The **Application Session Number** area displays historical information about the number of sessions related to the specified applications, as shown in Figure 2-8.

Figure 2-8 Historical session information of applications



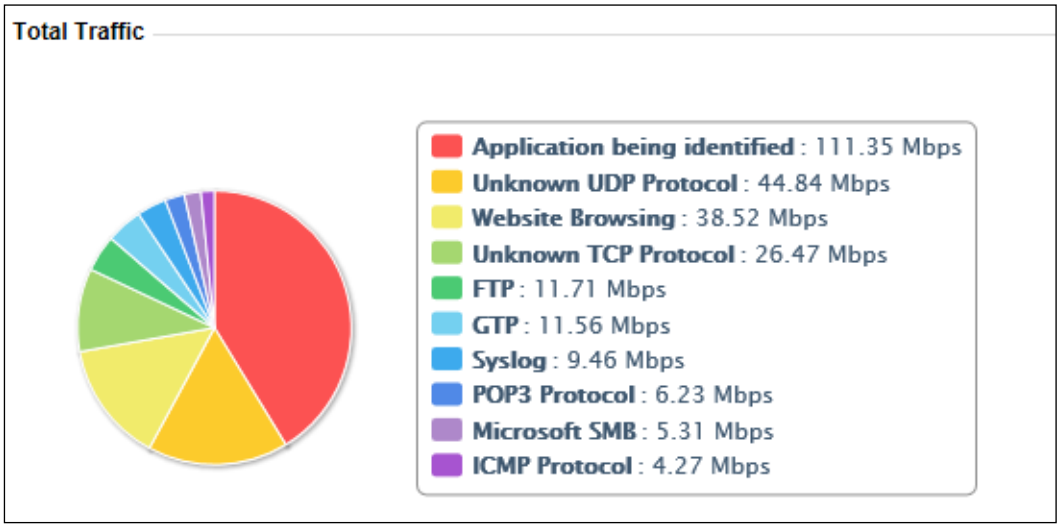
2.2.2 Application Traffic

Choose **Home** > **Traffic Analysis** > **Application Traffic**. The **Application Traffic** page displays the total traffic, top 10 uplink traffic rates, and top 10 downlink traffic rates.

Total Traffic

The **Total Traffic** area displays the percentages of traffic related to various applications to the total traffic, as shown in Figure 2-9.

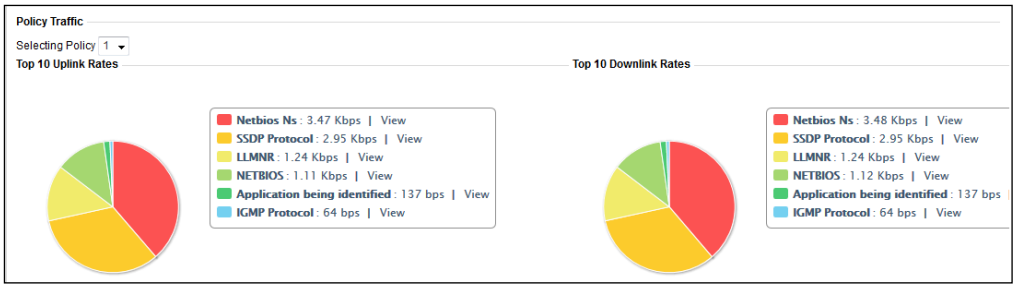
Figure 2-9 Percentages of traffic related to various applications



Policy-based Traffic

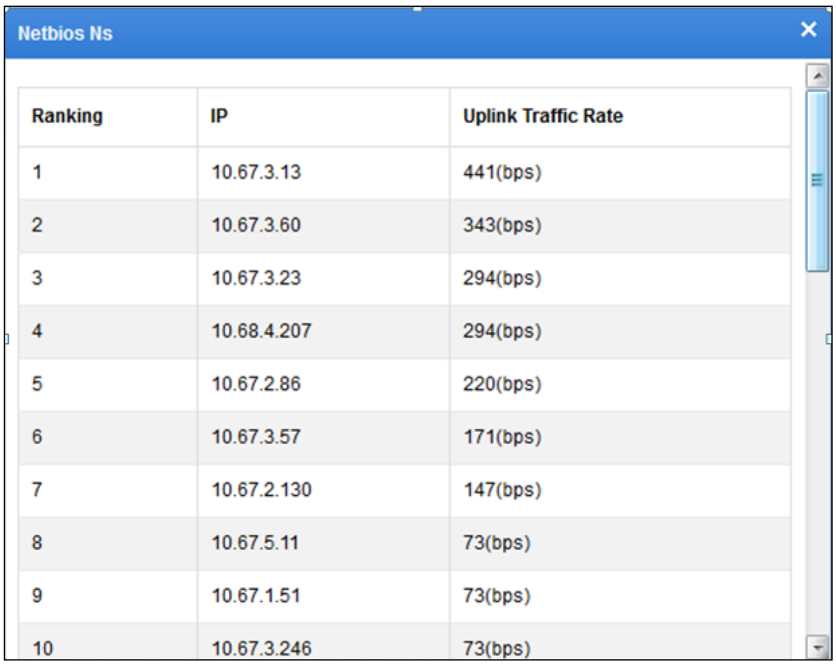
The **Policy Traffic** area displays top 10 uplink and top 10 downlink traffic rates related to various applications covered by the specified traffic management policy, as shown in Figure 2-10.

Figure 2-10 Traffic rates related to various applications covered by the specified traffic management policy



On the page shown in Figure 2-10, click **View** on the right of the application name to view rankings of the uplink or downlink traffic rates of the application covered by the selected policy. See Figure 2-11.

Figure 2-11 Uplink or downlink traffic rate rankings



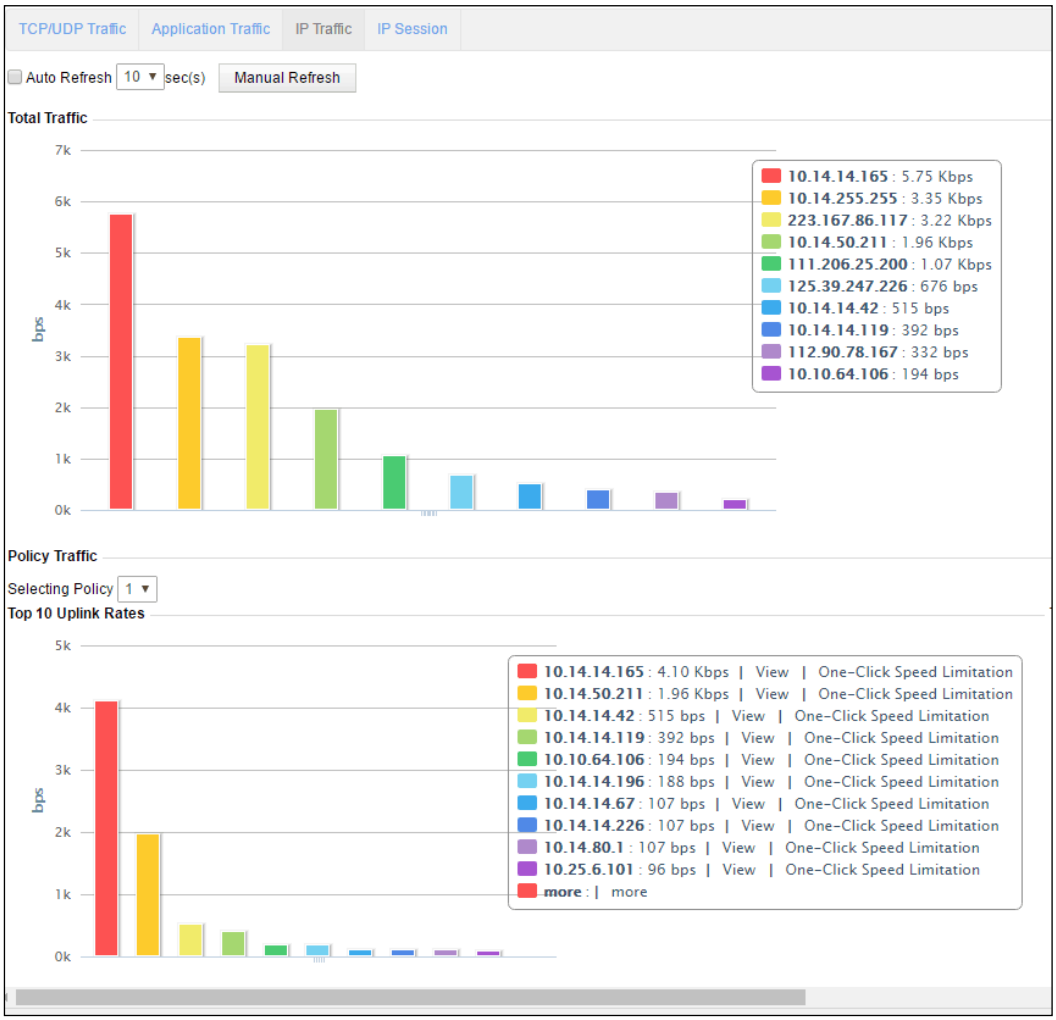
Netbios Ns

Ranking	IP	Uplink Traffic Rate
1	10.67.3.13	441(bps)
2	10.67.3.60	343(bps)
3	10.67.3.23	294(bps)
4	10.68.4.207	294(bps)
5	10.67.2.86	220(bps)
6	10.67.3.57	171(bps)
7	10.67.2.130	147(bps)
8	10.67.5.11	73(bps)
9	10.67.1.51	73(bps)
10	10.67.3.246	73(bps)

2.2.3 IP Traffic

Choose **Home** > **Traffic Analysis** > **IP Traffic**. The **IP Traffic** page displays the total IP traffic, top 10 uplink and downlink traffic rates hitting the specified traffic management policy, and the uplink and downlink traffic in the past week, as shown in Figure 2-12.

Figure 2-12 IP traffic monitoring



In the **Policy Traffic** area, you can click **more** to view traffic information of a maximum of top 256 IP addresses.

Figure 2-13 Viewing more policy traffic monitoring information

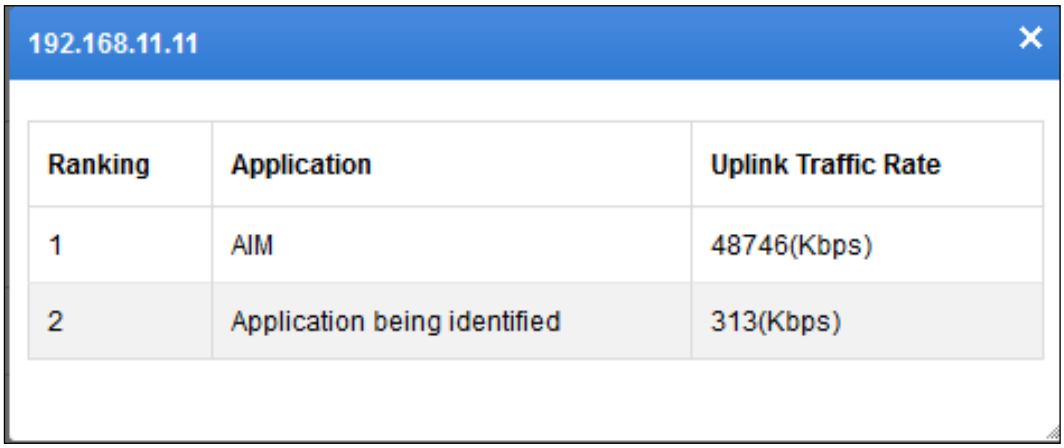
more

Ranking	Name	Traffic Rate	Operation
1	10.14.14.165	5.58(Kbps)	One-Click Speed Limitation
2	10.14.50.211	1.82(Kbps)	One-Click Speed Limitation
3	10.14.14.119	1.3(Kbps)	One-Click Speed Limitation
4	10.10.18.2	513(bps)	One-Click Speed Limitation
5	10.10.20.20	483(bps)	One-Click Speed Limitation
6	10.10.22.222	436(bps)	One-Click Speed Limitation
7	10.14.14.42	368(bps)	One-Click Speed Limitation
8	10.10.2.37	293(bps)	One-Click Speed Limitation
9	10.14.59.66	229(bps)	One-Click Speed Limitation
10	10.14.61.1	171(bps)	One-Click Speed Limitation

Viewing Application Traffic Information of a Specific IP Address

In the **Policy Traffic** area shown in Figure 2-12, you can click **View** to the right of an IP address to view traffic monitoring information of each application on this IP address.

Figure 2-14 Viewing traffic monitoring information of each application on an IP address



Ranking	Application	Uplink Traffic Rate
1	AIM	48746(Kbps)
2	Application being identified	313(Kbps)

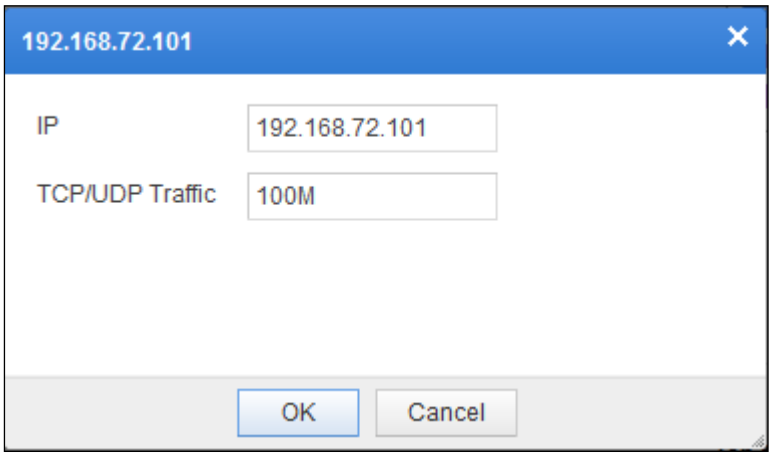
One-Click Speed Limitation

The one-click speed limitation function is used to configure a traffic management policy on the **IP Traffic** page for managing IP-specific traffic.

Step 1 In the **Policy Traffic** area shown in Figure 2-12 or the policy traffic monitoring information list shown in Figure 2-13, click **One-Click Speed Limitation** to the right of an IP address.

The dialog box for configuring a traffic management policy appears, as shown in Figure 2-15.

Figure 2-15 Configuring a traffic management policy



Step 2 In the dialog box, configure parameters.

IP cannot be edited. **Traffic** specifies the traffic limit with **100M** as the default value.

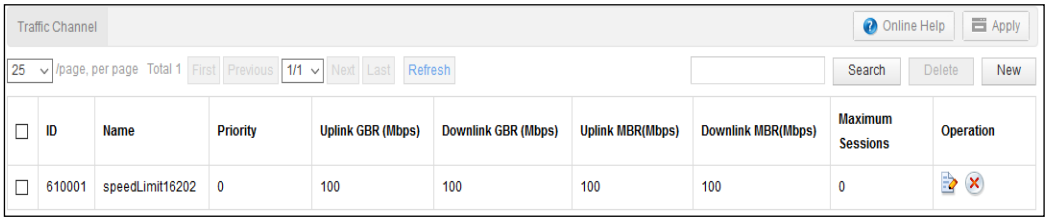
Step 3 Click **OK**.

After correct configuration, the system automatically performs the following operations:

- Adding a traffic management policy for this source IP address.

- Automatically checking whether an existing line with the same name exist on NIPS. If yes, the system directly references such line. If not, the system adds a new line and references it in the traffic management policy. For details about traffic management policies and lines, see section 7.9.1 Application Management Policy.
- Automatically adding a traffic channel object and referencing it in the traffic management policy. The name of the new traffic channel object is **speedLimit16202**, as shown in Figure 2-16. For details about traffic channel objects, see section 6.7 Configuring a Traffic Channel Object.

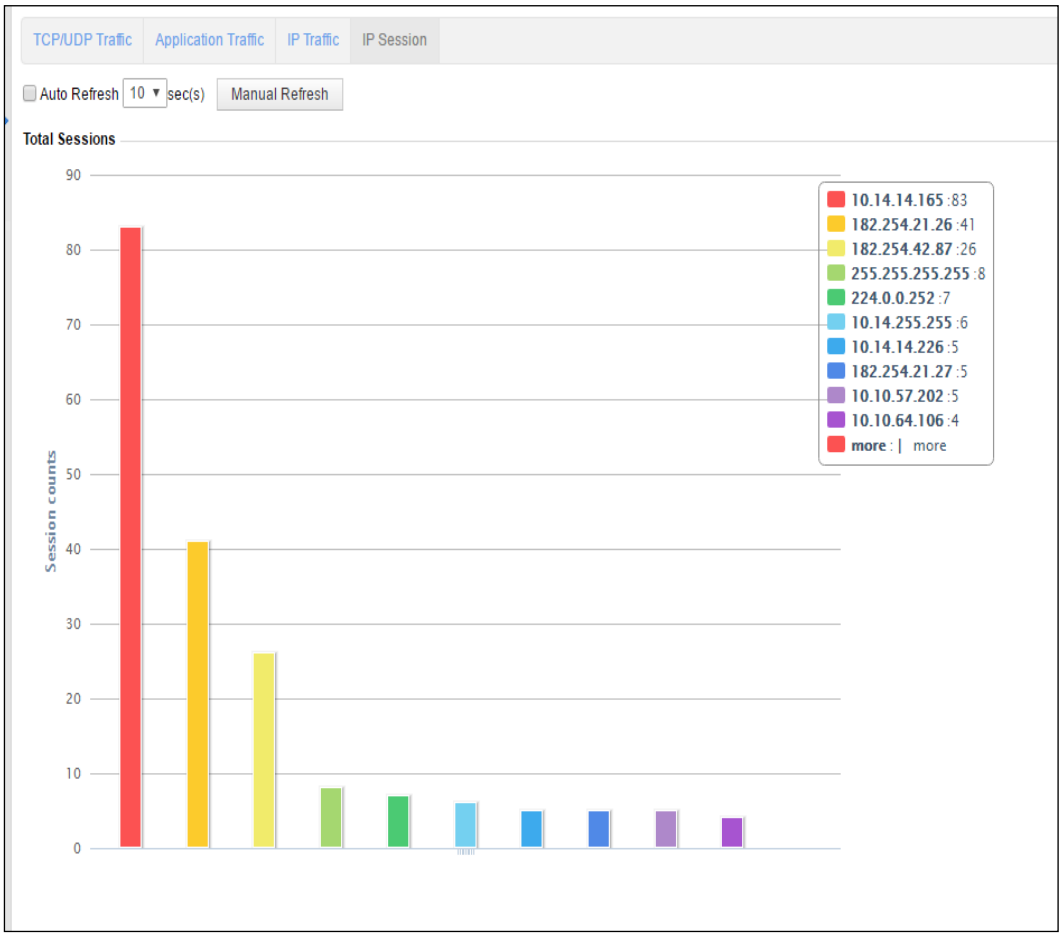
Figure 2-16 Automatically added traffic channel object



2.2.4 IP Session

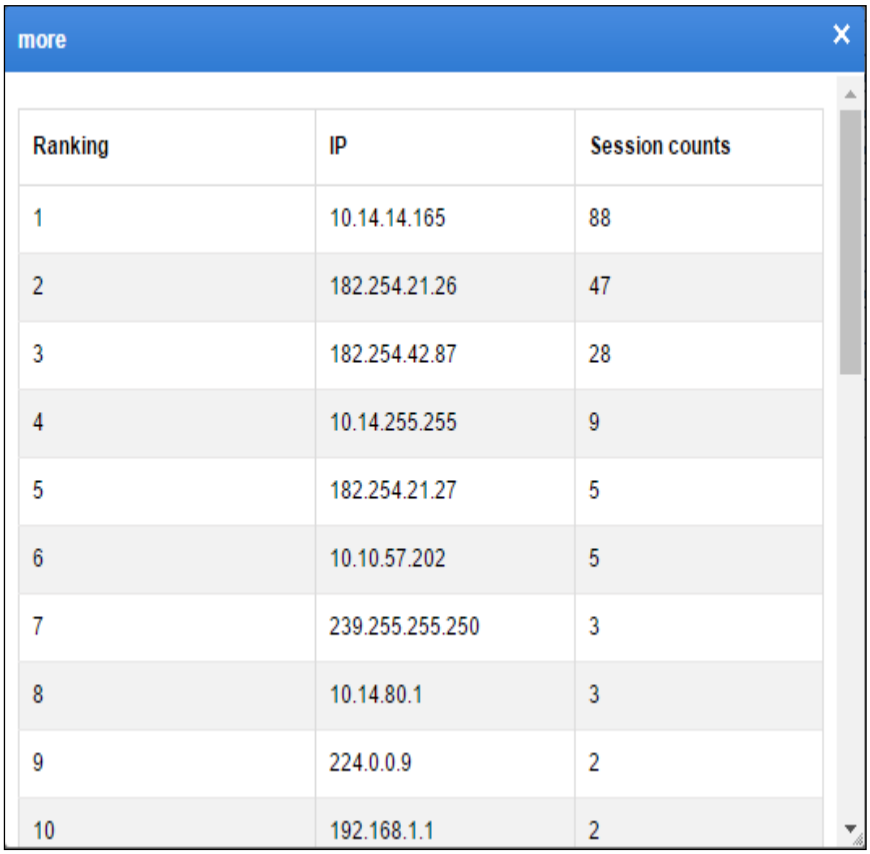
Choose **Home** > **Traffic Analysis** > **IP Session**. The **IP Session** page displays top 10 sessions established by NIPS, as shown in Figure 2-17.

Figure 2-17 IP Session page



You can click **more** to view a maximum of top 256 IP sessions.

Figure 2-18 Viewing top 256 IP sessions



more

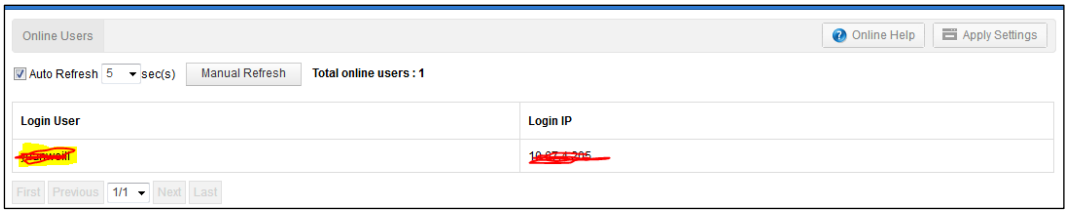
Ranking	IP	Session counts
1	10.14.14.165	88
2	182.254.21.26	47
3	182.254.42.87	28
4	10.14.255.255	9
5	182.254.21.27	5
6	10.10.57.202	5
7	239.255.255.250	3
8	10.14.80.1	3
9	224.0.0.9	2
10	192.168.1.1	2

2.3 Online Users

NIPS can display current online users in real time, including login IP addresses and user names.

Step 1 Choose **Home** > **Online Users**.

Figure 2-19 List of online users



Step 2 Refresh the user list.

a. On the **Online Users** page, select the **Auto Refresh** check box and set the refresh interval.

Then the system automatically refreshes information about online users at the specified interval.

b. Click **Manual Refresh** to refresh information about online users manually on the current page.

----End

2.4 Hardware Monitoring

Under **Home** > **Hardware Monitoring**, you can view the following information:

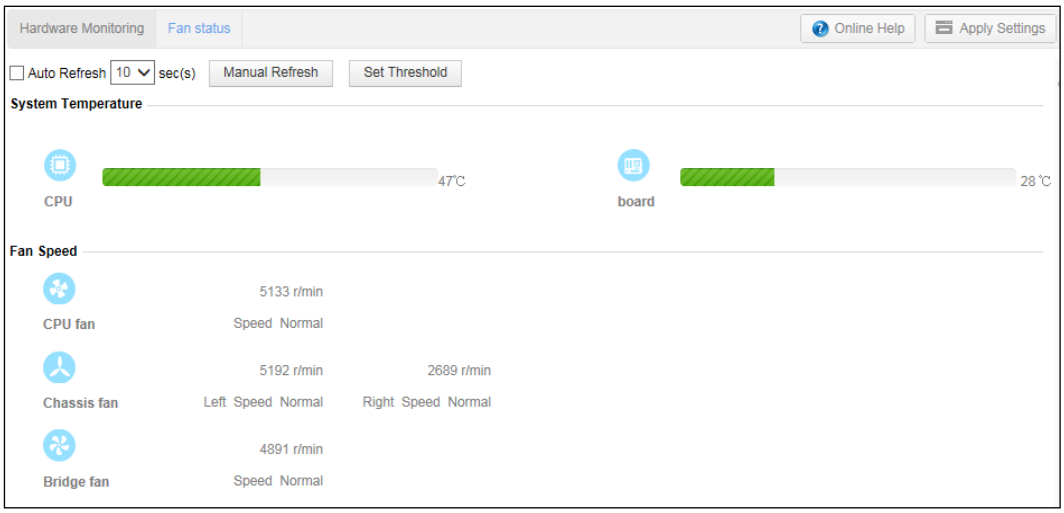
- Hardware monitoring: You can view hardware information of NIPS, including the mainboard temperature, CPU temperature, fan speed, power temperature, voltage, and fault status.
- Fan status: You can view status information of all fans on NIPS.

Note	NIPS devices of the following models do not show the status of fans: • NIPS NX3-N300 • NIPS NX3-N2000A, NX3-N3000A, NX5-N4000A, NX5-N6000A, NX5-N8000A, NX5-T9010A, or NX5-T020A, whose serial number contains the letter P, for example, 16-24-P-0223

2.4.1 Hardware Monitoring

Choose **Home** > **Hardware Monitoring** > **Hardware Monitoring**. On the **Hardware Monitoring** page, you can view real-time hardware monitoring information, including the mainboard temperature, CPU temperature, CF usage, hard disk usage, fan speed, power temperature, voltage, and fault status.

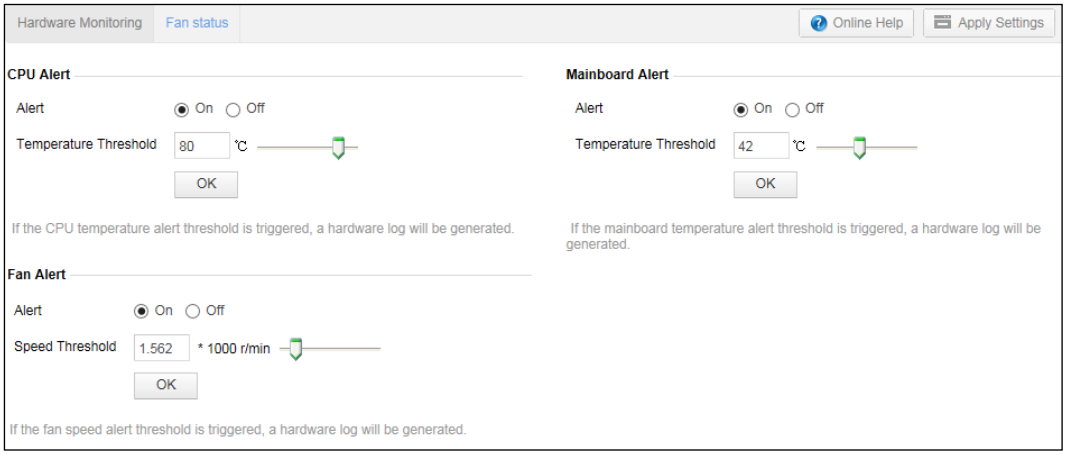
Figure 2-20 Hardware monitoring information



Note	• If NIPS has a CF card, but not a hard disk, hard disk monitoring information will not be displayed. • **Power Supply Status** is available only for NIPS devices of the following models, whose serial numbers contain the letter P (for example, 16-24-P-0223): NX3-N2000A, NX3-N3000A, NX5-N4000A, NX5-N6000A, NX5-N8000A, NX5-T9010A, and NX5-T9020A.

- On the **Hardware Monitoring** page, select the **Auto Refresh** check box and set the refresh interval. Then the system automatically refreshes information about hardware monitoring at the specified interval.
- Click **Manual Refresh** to refresh information about hardware monitoring manually on the current page.
- Click **Set Threshold** to configure alert thresholds for each hardware item. For details, see section 4.3.5 Configuring Hardware Monitoring.

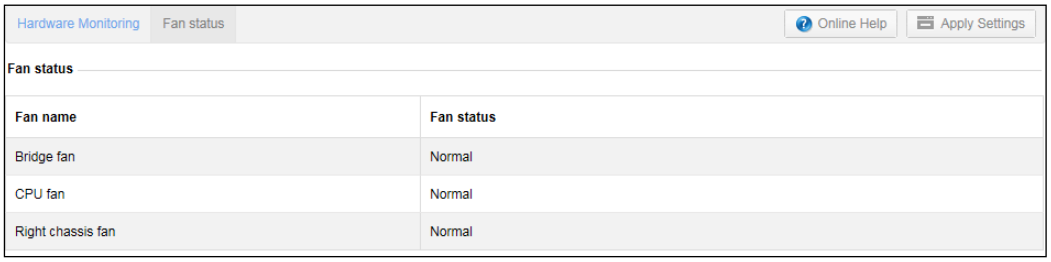
Figure 2-21 Configuring alert thresholds



2.4.2 Fan Status

Choose **Home** > **Hardware Monitoring** > **Fan Status**. On the **Fan Status** page, you can view information about all fans on NIPS.

Figure 2-22 Fan Status page



After the fan alert is enabled, when the fan speed is lower than the specified threshold (for how to configure the threshold, see section 4.3.5 Configuring Hardware **Monitoring**), the

system assumes that the fan is abnormal and then records a hardware log with the type of "Fan status log". For how to view hardware logs, see section 8.1.4.4 Hardware Logs.

3 Alert Center

From the alert center, you can view the latest 200 alert messages of various events or the latest 20 alert messages of a specific event type. This chapter contains the following sections:

Section	Description
Common Operations	Describes how to view alert messages.
All Events	Describes how to view the latest 200 alert messages of various events.
Intrusion Prevention Event	Describes how to view the latest 20 alert messages on intrusion prevention events.
Data Leak Event	Describes how to view the latest 20 alert messages on data leak events.
Reputation-related Event	Describes how to view the latest 20 alert messages on reputation-related events.
URL Category Event	Describes how to view the latest 20 alert messages on access to various URLs.
Antivirus Event	Describes how to view the latest 20 alert messages on antivirus events.

3.1 Common Operations

Operations on the **All** page and pages of various events are almost the same. This section describes these common operations.

Viewing Event Details

If you select the **Show Details** check box in the upper-right corner of the page, event details are displayed for each alert, as shown in Figure 3-1.

Figure 3-1 Alert page with event details displayed

Viewing Domain Names

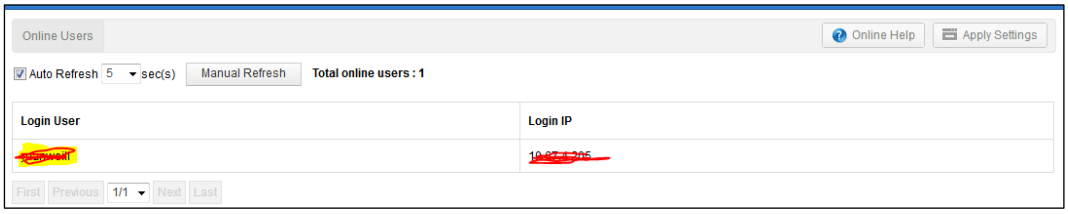
If you select the **Show domain name** check box in the upper-right corner of the page, domain names are displayed for each alert, as shown in Figure 3-2.

Figure 3-2 Alert page with domain names displayed

Viewing Information about Authenticated Users

If an event matches an authentication policy (for configuration of such a policy, see section 7.8.4 Authentication Policy), the authenticated user name is displayed under **Authenticated User**.

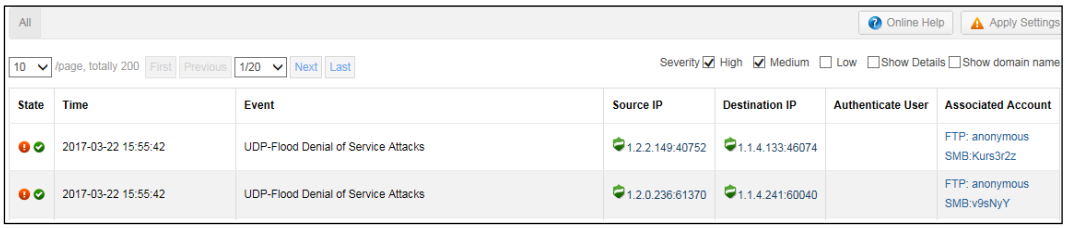
Figure 3-3 Alert page with authenticated user information displayed



Viewing Associated Users

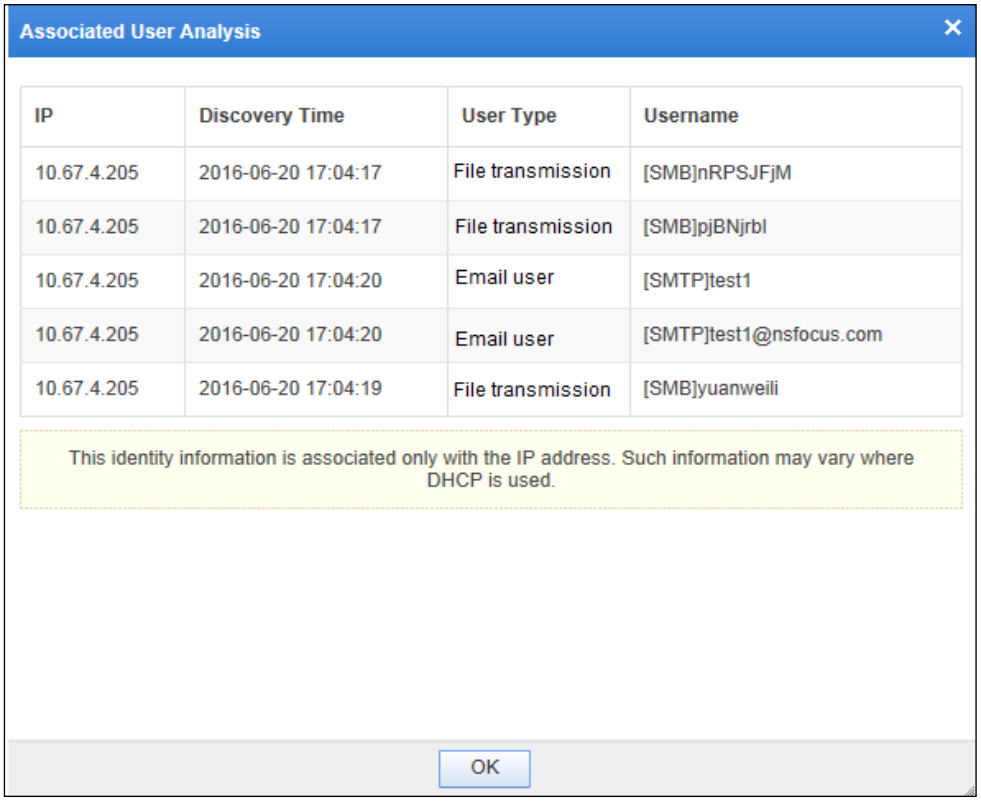
If an event matches an intelligent user identification policy (for configuration of such a policy, see section 7.8.5 Intelligent User Association), the latest two associated accounts are displayed under **Associated Account**.

Figure 3-4 Alert page with associated account information displayed



Click the account name under **Associated account**. A dialog box appears, showing information about all users intelligently identified, as shown in Figure 3-5.

Figure 3-5 Information about associated users



Viewing Details of Public IP Addresses

If the source or destination IP address of an event is a public IP address, appears before the IP address, which is displayed in blue, like 124.239.223.30:80 .

Clicking this IP address, you are directly connected to Seer, NSFOCUS Threat Intelligence Center, where details of this IP address are displayed.

In addition, you can perform the following operations on pages of specific event types:

Refreshing Data

Data on these pages can be refreshed as follows:

- Automatically refresh data.

  Select the **Auto Refresh** check box and set the refresh interval. Then, the system automatically refreshes data on the current page at the specified interval.
- Manually refresh data.

  Click **Manual Refresh** to refresh data manually on the current page.

3.2 All Events

The **All** page displays the latest 200 events, including 100 reputation-related events and 100 other events (intrusion prevention, data leak, URL access, and antivirus events). You can query events by severity.

Choose **Alert Center** > **All**. The **All** page appears, as shown in Figure 3-1.

This page displays high- and medium-level events by default. You can specify one or more severity levels to view only events of the specified levels, as shown in Figure 3-6.

Figure 3-6 All page with high- and medium-level events displayed

3.3 Intrusion Prevention Event

The **IPS Event** module allows you to view basic information and details of intrusion prevention events, add exceptions, view the list of isolated IP addresses, and disable the isolation.

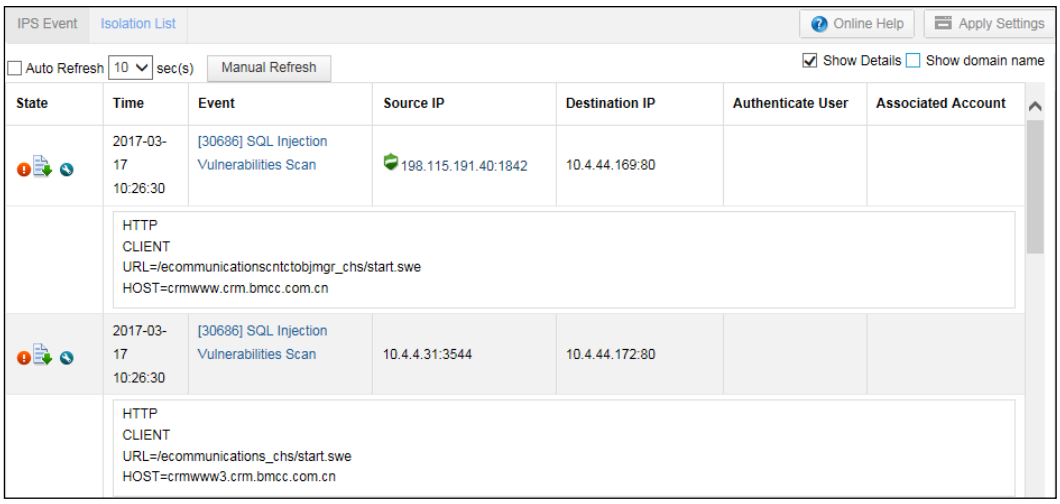
3.3.1 List of Intrusion Prevention Events

Intrusion prevention events are displayed only after you configure the corresponding rule template and the template is then referenced in the intrusion prevention policy. For details about intrusion protection policies, see section 7.2.1 Intrusion Prevention Policies.

NIPS displays the latest 20 intrusion prevention events. For each event, you can view the status, time, description, source and destination IP addresses, user, and details.

Choose **Alert Center > IPS Event > IPS Event**.

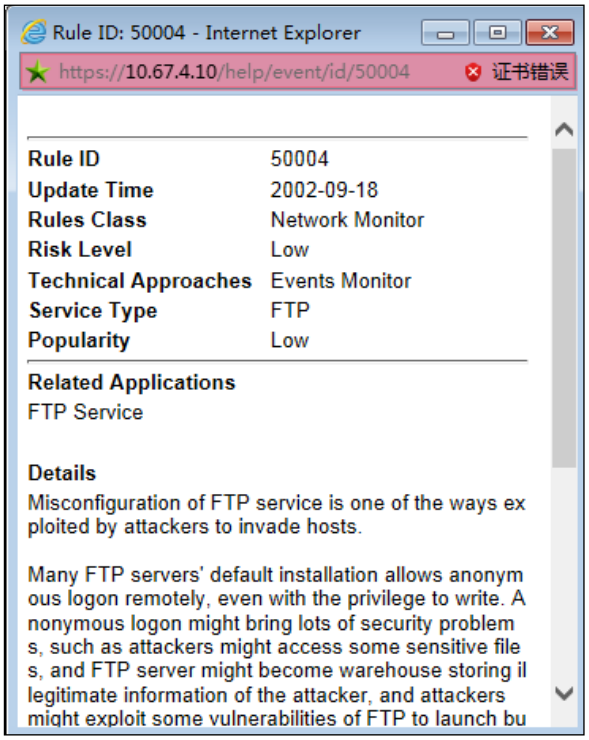
Figure 3-7 List of intrusion prevention events



Viewing Details of an Intrusion Prevention Event

Clicking an event name displays the detailed analysis of and solution for this event, as shown in Figure 3-8.

Figure 3-8 Intrusion prevention event analysis



Clicking a blue link, such as the vulnerability title, NSFOCUS ID, or BUGTRAQ ID, directs you to the detailed vulnerability information page of the NSFOCUS website.

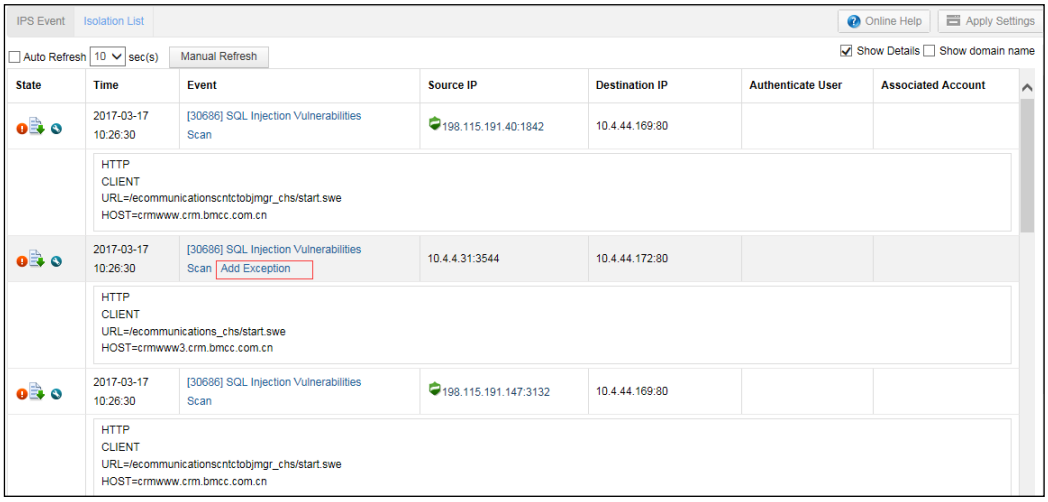
Adding an Exception

If you do not want NIPS to detect and alert events in real time against a certain rule, you can add this rule as an exception.

Step 1 Point to an event.

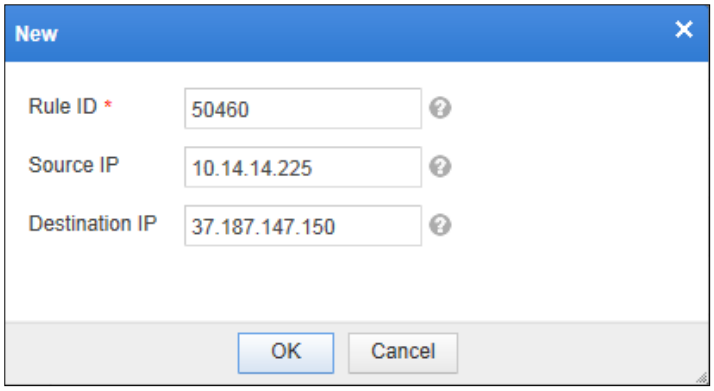
Add Exception appears after the event name, as shown in Figure 3-9.

Figure 3-9 Adding an exception



Step 2 Click **Add Exception**.

Figure 3-10 Configuring exception parameters



Step 3 Configure parameters in the **New** dialog box.

Table 3-1 Parameters for configuring a rule as an exception

Parameter	Description
Rule ID	ID of the exception rule. This ID must be the same as the ID of the related intrusion prevention rule.
Source IP	Specifies the source IP address or IP segment, that is, the valid range of IP addresses to be covered by this exception rule. Only packets from the specified source IP address or IP segment are allowed to go through. You should type an IPv4 address or IPv4 segment, for example, 192.168.1.0/24. Typing 0.0.0.0 or leaving the field empty indicates no limit.
Destination IP	Specifies the destination IP address or IP segment, that is, the valid range of IP addresses to be covered by this exception rule. Only packets to the specified destination IP address or IP segment are allowed to go through. You should type an IPv4 address or IPv4 segment, for example, 192.168.1.0/24. Typing 0.0.0.0 or leaving the field empty indicates no limit.

Step 4 Click **OK**.

You can view and cancel this exception rule under **Object** > **Rule** > **Exception Rule**.

Step 5 Apply the settings.

----End

Downloading a PCAP File

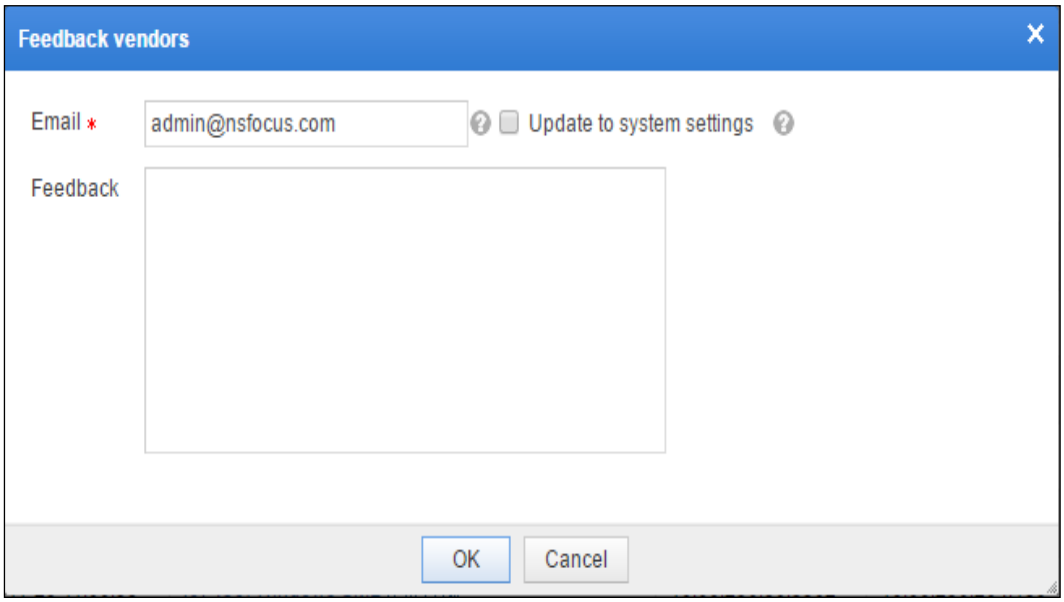
If the **Packet Capture** check box is selected in the policy that the current event hits, appears in the **State** column. You can click this icon to download the packet capture file of this event for analysis and debugging.

Reporting a False Positive

If you determine that a security event is a false positive, you can click in the **State** column to inform NSFOCUS rule team.

If the administrator's email address has been correctly configured, after you click , the system displays a message, as shown in Figure 3-11.

Figure 3-11 Message confirming the success of reporting the false positive



- **Email Address**: specifies the email address for receiving feedback information. By default, the current logged-in administrator's email address is displayed.
- **Update to System Settings**: After this option is selected, the system sets the current logged-in user's email address to this email address and uses it as the default email address for sending feedback information. For how to configure the email address, see section 4.5.1 Managing Accounts.
- **Feedback Content**: presents the brief description of feedback information.

After you click **OK**, the system sends the false positive as configured. After the false positive is successfully sent, a message indicating sending success appears.

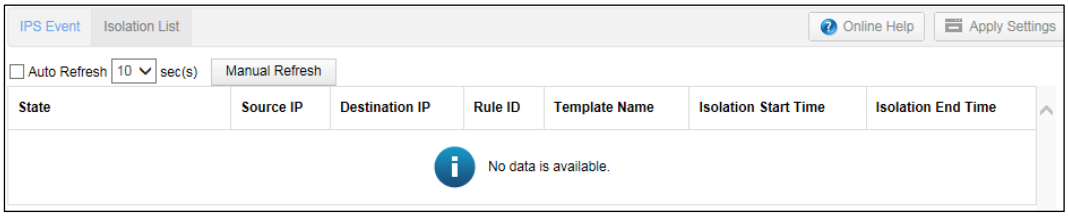
3.3.2 Isolation List

An intrusion prevention policy may reference a rule template that includes rules for which the **Isolation** check box is selected. If this policy is enabled and triggered by certain attack behaviors, NIPS will isolate traffic between the source and destination IP addresses related to such attack behaviors.

The isolation list displays the isolated source and destination IP addresses, rule ID, and isolation start and end time, as shown in Figure 3-12.

Choose **Alert Center** > **IPS Event** > **Isolation List**.

Figure 3-12 Isolation list



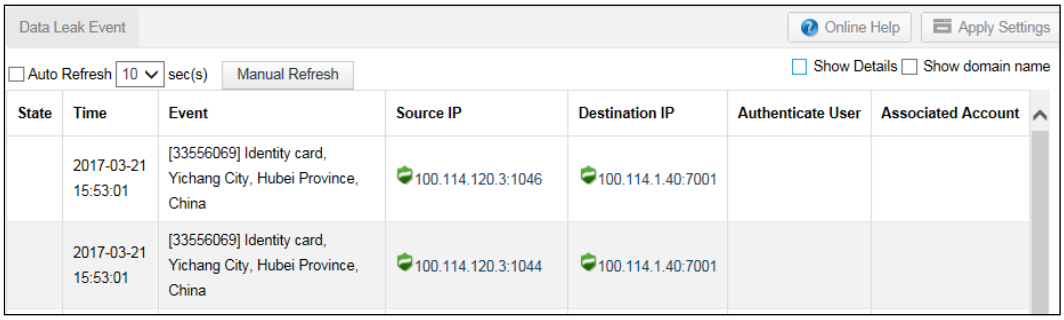
- Click the link text **End Isolation** in the **State** column to disable the isolation.
- Click the rule ID to view details of the rule that triggers the isolation.

3.4 Data Leak Event

NIPS displays the latest 20 data leak events. For each event, you can view the status, time, description, source and destination IP addresses, user, and details.

Choose **Alert Center** > **Data Leak Event**. in the **State** column indicates that related traffic is blocked. If is not displayed, related traffic is allowed to pass.

Figure 3-13 List of data leak events

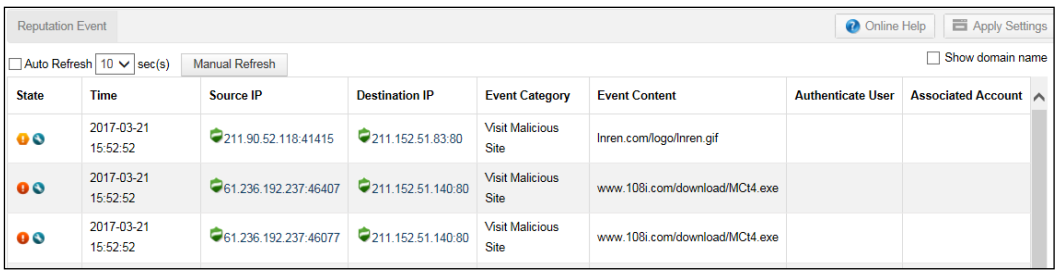


3.5 Reputation-related Event

NIPS displays the latest 20 reputation events. For each event, you can view the status, time, source and destination IP addresses, event category, description, and user.

Choose **Alert Center** > **Reputation Event**. in the **State** column indicates that related traffic is blocked. If is not displayed, related traffic is allowed to pass.

Figure 3-14 List of reputation events



If you determine that a reputation-related event is a false positive, you can click in the **State** column to send this information to the cloud. For details, see "Reporting a False Positive" in section 3.3.1 List of Intrusion Prevention Events.

For an alert event whose **Event Category** is displayed as **Visit Malicious File**, you can click in the **State** column to add the MD5 value of this file to the whitelist. Then NIPS will no

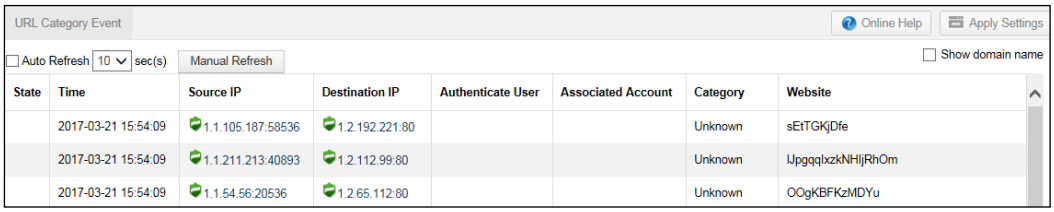
longer check the reputation of this file. For details about the file whitelist, see Configuring the File Whitelist in section 7.4.4 File Reputation.

3.6 URL Category Event

NIPS displays the latest 20 URL access events. For each event, you can view the status, time, source and destination IP addresses, user, URL category, and website name.

Choose **Alert Center** > **URL Category Event**. in the **State** column indicates that related traffic is blocked. If is not displayed, related traffic is allowed to pass.

Figure 3-15 List of URL access events



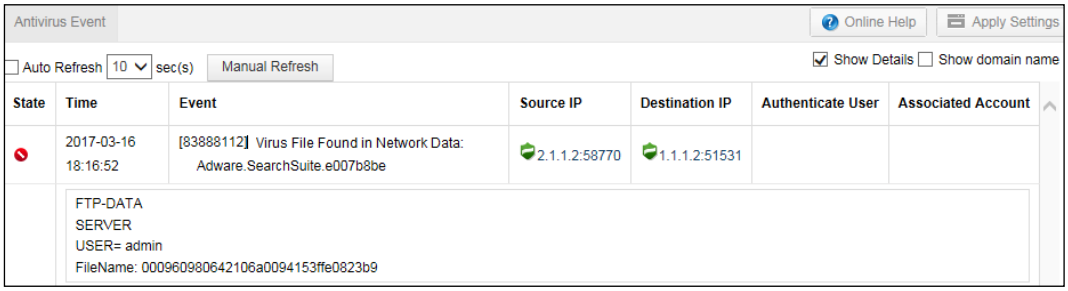
3.7 Antivirus Event

NIPS displays the latest 20 antivirus events. For each event, you can view the status, time, description, source and destination IP addresses, and user.

Note	Antivirus events can be displayed only after antivirus templates are configured and referenced in security policies. For details about antivirus policies, see section 7.6 Configuring URL Category Filtering Policies.

Choose **Alert Center** > **Antivirus Event**. in the **State** column indicates that related traffic is blocked. If is not displayed, related traffic is allowed to pass.

Figure 3-16 Antivirus events



4 System

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

Section	Description
System Update	Describes how to update the system online and offline.
Backup and Restoration	Describes how to back up and restore parameter files, rule files, and configuration files.
System Configuration	Describes how to configure engine parameters and special parameters.
Security Center	Describes how to connect NIPS to NSFOCUS ESPC.
Account Management	Describes how to manage system accounts.
Diagnosis Tools	Describes built-in diagnostic tools and methods for using these tools.
License Management	Describes how to import the license and view license information.
System Control	Describes how to perform system control such as rebooting the engine and restarting the system.

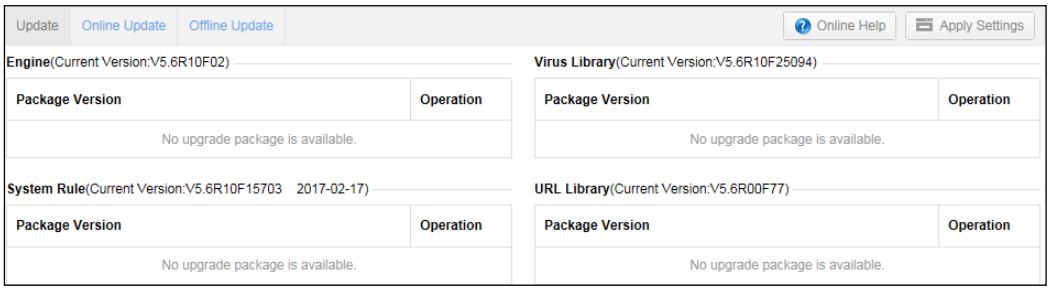
4.1 System Update

You can update the engine, system rule libraries (intrusion signature library, application signature library, and data leak library), virus library, and URL library. The following details how to view the current system status and update the system online and offline.

4.1.1 Viewing Version Information of NIPS

Choose **System** > **System Update** > **Update**. On the **Update** page, you can view the versions of the system engine, system rule library, virus library, and URL library, as shown in Figure 4-1.

Figure 4-1 System version information



- To update the device, follow these steps:

  If online update is permitted, when detecting that an update is available, NIPS prompts you to update the device:

  – Click **Click to update**.

  – Update the device.

  The system records only the latest version number. Click in the **Operation** column. Then the device is updated to the latest version.

- To save an update package, click in the **Operation** column to save it to a local disk drive.

4.1.2 Updating the System Online

If NIPS can connect to the Internet, you can update the device online. Online updates can be performed in a scheduled or instant manner.

Note	• A prerequisite for both types of updates is that NIPS can access the Internet. You need to configure a proper DNS server IP address on the DNS client so that NIPS can access the NSFOCUS home page for update. For details, see section 5.6 DNS. • The DNS server IP address should be excluded from interface configurations; otherwise, an IP address conflict would occur and the update would fail.

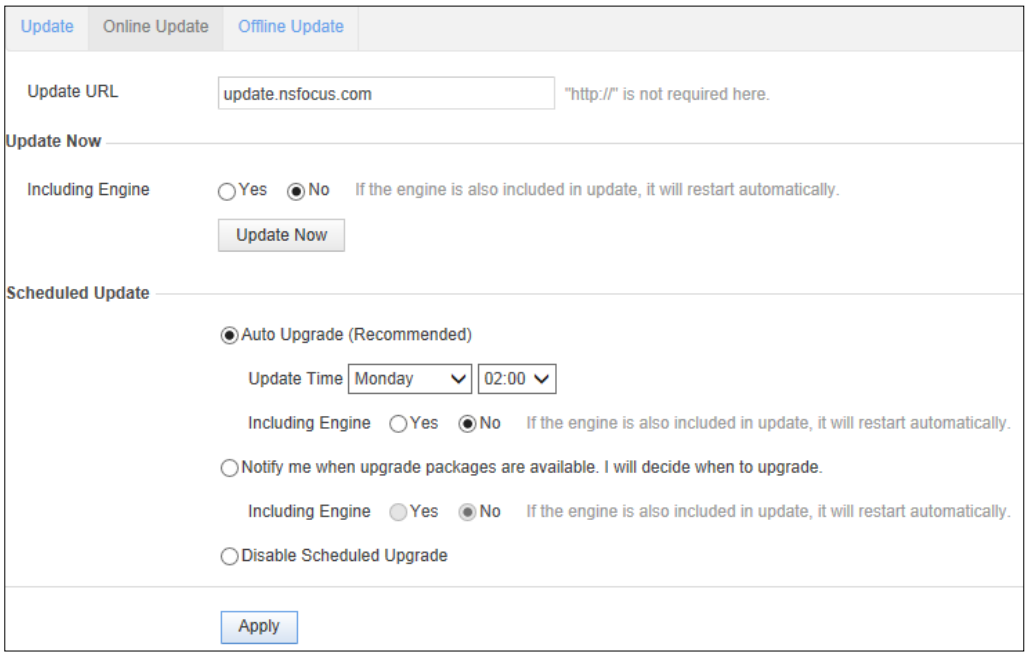
4.1.2.1 Scheduled Update

If scheduled update is enabled, the system automatically checks new updates. When detecting a new one, the system updates the engine and all rule libraries at the specified time.
The whole update process requires no manual intervention.

To configure scheduled update, follow these steps:

Step 1 Choose **System** > **System Update** > **Online Update**.

Figure 4-2 Online Update page



Step 2 Configure parameters.

Table 4-1 Parameters for configuring online update

Parameter	Description
Update URL	Specifies the URL where the latest update is available. Generally, this URL directs you to the official website of NSFOCUS. The value of this parameter must be a URL without "http://", and the default value is **update.nsfocus.com**.
Auto Upgrade (Recommended)	Controls whether NIPS automatically checks the latest update and updates the system at the specified time. • **Update Time**: specifies the time when NIPS automatically updates the system. After **Auto upgrade (recommended)** is selected, NIPS can automatically update the system at any hour on **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**, or **Sunday**. • **Including Engine**: controls whether the engine will be updated together with the system. **Note** You are advised to specify an off hour to update the system. The engine will automatically restart during its update, resulting in temporary service interruption.
Notify me when upgrade packages are available. I will decide when to upgrade.	If this is selected, the system will automatically check updates and notify users when detecting new update packages. You can also decide whether the engine will be updated together with the system by selecting or deselecting **Including Engine**.

Parameter	Description
Disable Scheduled Upgrade	Controls whether to disable the scheduled update function.

Step 3 Click **Apply Settings** to save the settings.

Step 4 Apply the settings.

----End

4.1.2.2 Instant Update

You can also update the device instantly as required.

To update the device instantly, follow these steps:

Step 1 Choose **System** > **System Update** > **Online Update**.

Step 2 Enter the URL where the latest update is available and configure online update parameters.

For the description of parameters, see Table 4-1.

Step 3 Click **Update Now** to update the device instantly.

----End

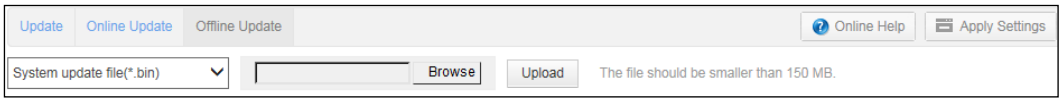
4.1.3 Updating the System Offline

If NIPS cannot connect to the official website of NSFOCUS, you can update the device by importing the update file.

To update the device offline, follow these steps:

Step 1 Choose **System** > **System Update** > **Offline Update**.

Figure 4-3 Offline Update page



Step 2 Select the file type.

Table 4-2 Update file types

Parameter	Description
System update file(*.bin)	After this type of file is imported, the system determines whether to automatically reboot the engine based on the file content.
System rule(*.rule)	The system rule library contains the intrusion signatures, application signatures, data leak signatures, help file, and description file. After this type of file is imported, the engine automatically loads the file, which will take effect immediately.
Virus Library Upgrade File	After this type of file is imported, the system determines whether to

Parameter	Description
(*.av)	automatically reboot the engine based on the file content.
URL Library(*.urlibx)	After this type of file is imported, the engine automatically loads the file, which will take effect immediately.
Reputation Library(*.tar.gz)	You need to contact engineering personnel of NSFOCUS for download of the reputation library.

Step 3 Click **Browse**, select the file, and click **Open**.

Step 4 Click **Upload** to update the device immediately.

----End

4.2 Backup and Restoration

This section describes how to back up and restore parameter files, rule files, configuration files, and documents, and how to restore system configurations.

4.2.1 Backing Up a File

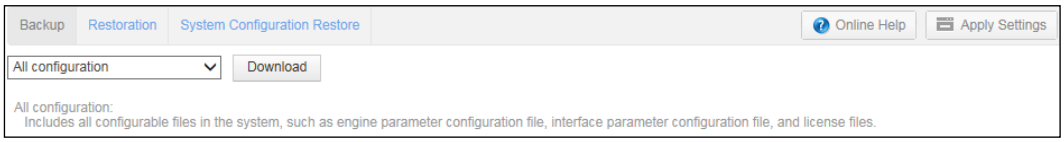
Currently, NIPS can back up the following files:

- All configuration files
- Engine parameter file
- Interface parameter file
- Custom rules
- Local authentication file
- Streaming media server list file
- Object configuration file
- Rule configuration file
- Intrusion prevention policy file
- SNMP agent MIB file
- SNMP trap document
- Syslog-related file
- License file
- Weak password dictionary

The following takes an engine parameter file as an example to describe how to back up various files:

Step 1 Choose **System** > **Backup and Restoration** > **Backup**.

Figure 4-4 Backup page



Step 2 On the **Backup** page, select **Engine parameter file** from the drop-down list.

Step 3 Click **Download** to download the file to a local disk drive.

----End

4.2.2 Restoring a Backup File

Currently, NIPS can restore the following files that have been backed up:

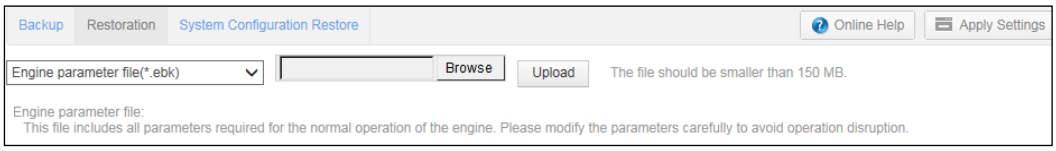
- Engine parameter file (*.ebk)
- Interface parameter file (*.ebk)
- Custom rules (*.xml)
- Local authentication file (*.list)
- Streaming media server list file (*.conf)
- Configuration file (*.ebk)
- Weak password dictionary (*.txt)

Only backed-up files can be used for restoration. The same backup file can be used between NIPS devices of the same software version on the same hardware platform.

To restore a file, follow these steps:

Step 1 Choose **System** > **Backup and Restoration** > **Restoration**.

Figure 4-5 Restoration page



Step 2 Click **Browse**, select the desired file, and click **Open**.

Step 3 Click **Upload** to complete the restoration.

----End

4.2.3 Restoring System Configurations

You can restore NIPS system configurations to the state at the restore point created on NIPS. The restore point can be created in either of the following ways:

- Manually creating the restore point

  You can back up the current system configuration files of NIPS whenever required.

- Automatically creating the restore point

  You can configure NIPS to automatically back up all configuration files at the specified time.

To reduce NIPS disk usage, the system saves only configurations backed up at the manual restore point and auto restore point most recently created.

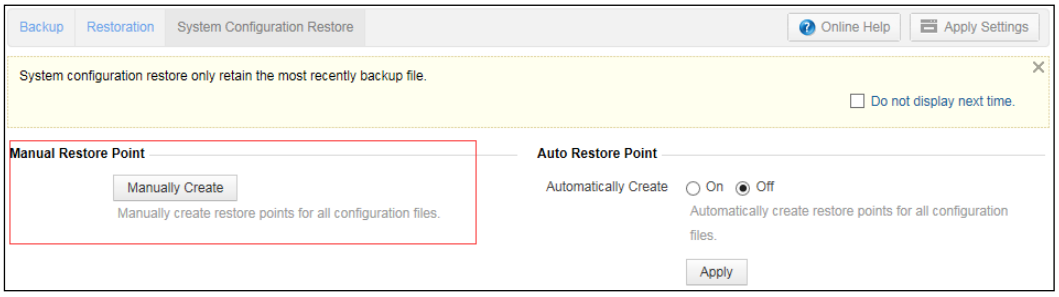
4.2.3.1 Manual Restore Point

When system configurations undergo a major change, you are advised to immediately create a restore point manually. The procedure is as follows:

Step 1 Choose **System** > **Backup and Restoration** > **System Configuration Restore**.

Figure 4-6 shows the **Manual Restore Point** area.

Figure 4-6 Manual Restore Point area



Step 2 Click **Manually Create** to manually create a restore point.

The backup will take some time. You must wait patiently for the process to complete. After a restore point is manually created, restore point information will appear or be refreshed.

Step 3 Click **Restore** to restore system configurations of NIPS to the state at the restore point.

----End

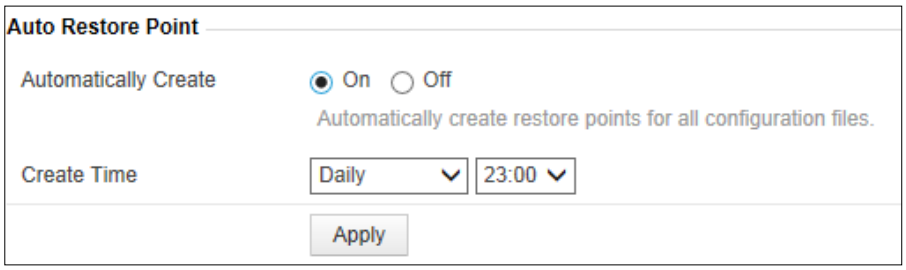
4.2.3.2 Auto Restore Point

To configure NIPS to automatically create restore points, follow these steps:

Step 1 Choose **System** > **Backup and Restoration** > **System Configuration Restore**.

Figure 4-7 shows the **Auto Restore Point** area.

Figure 4-7 Auto Restore Point area



Step 2 Select **On** for **Automatically Create** to enable NIPS to automatically create restore points.

Step 3 Specify the restore point creation time.

You can select **Daily** or specify a weekday, Saturday, or Sunday.

Step 4 Apply the settings.

NIPS will automatically create restore points at the specified time and restore point information will appear or be refreshed.

Step 5 Click **Restore** to restore system configurations of NIPS to the state at the restore point.

----End

4.3 System Configuration

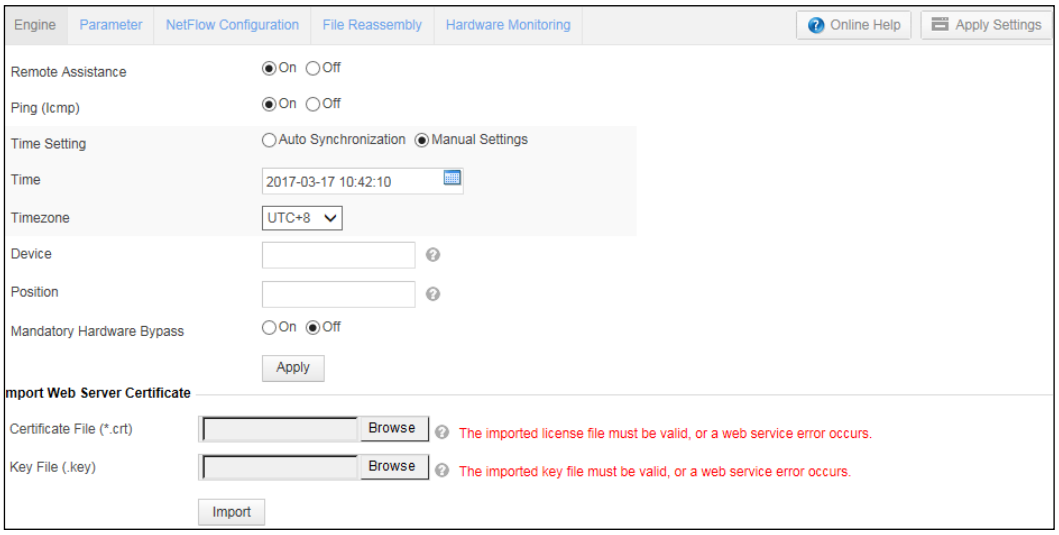
This section describes how to set system-related parameters, including engine parameters, special parameters, NetFlow, file reassembly, and hardware monitoring.

4.3.1 Configuring the Engine

To configure engine parameters, follow these steps:

Step 1 Choose **System** > **System Configuration** > **Engine**.

Figure 4-8 Engine configuration



Step 2 Configure engine parameters.

Table 4-3 Engine configuration parameters

Parameter	Description
Remote Assi	Controls whether to enable remote assistance. • **On**: enables remote assistance through port 50022. • **Off**: disables remote assistance. Remote assistance can be used only by NSFOCUS engineers for network commissioning.
Ping(Icmp)	Controls whether to enable NIPS to respond to ICMP requests. It has the following values: • **On**: indicates that NIPS responds to ICMP requests, which makes it convenient for an administrator to debug the device. • **Off**: indicates that NIPS does not respond to ICMP requests.
Time Setting	Specifies the method of synchronizing the time on NIPS with the time synchronization server. Its values include **Auto Synchronization** and **Manual Settings**. After this parameter is set, the setting can take effect only after the engine is restarted.
Time Synchronization Server	Specifies the IP address of the time synchronization server after **Auto Synchronization** is selected. Note that the engine management interface must be able to properly communicate with the time synchronization server.
Synchronization Interval (sec)	Specifies the interval for NIPS to automatically synchronize the time with the time synchronization server after **Auto Synchronization** is selected. The value is expressed in seconds.
Time	Specifies the date and time after **Manual Settings** is selected.
Timezone	Specifies the time zone of the device.
Device	Specifies NIPS's device name that is displayed on its home page.

Parameter	Description
Position	Specifies the location of NIPS.
Mandatory Hardware Bypass	Controls whether NIPS is forced to enter the bypass state. **On** indicates that NIPS will be forced to enter the bypass state. **Off** indicates the opposite. The mandatory hardware bypass state, after being changed, takes effect only after system restart.

Step 3 Apply the settings.

----End

Importing a Web Server Certificate

A web server certificate includes the following:

- License file: is a .crt file that cannot exceed 1 MB.
- Key file: is a .key file that cannot exceed 1 MB.

To import a web server certificate, follow these steps:

Step 1 Click **Browse** and then select a license file and key file from the local disk drive.

Note	The license file and key file to be imported must be valid, or a web service error occurs.

Step 2 Click **Import**.

----End

4.3.2 Configuring Special Parameters

You can configure special parameters under **System** > **System Configuration** > **Parameter**.

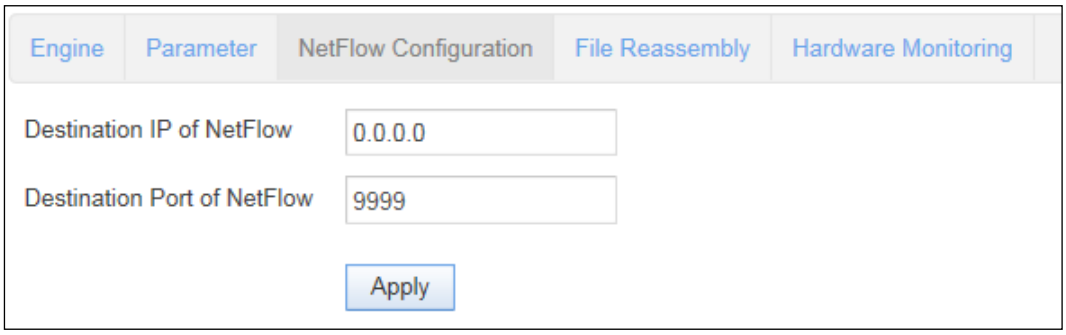
Special parameters are provided to adapt NIPS to special network environments. In normal conditions, users do not need to make changes to them. Modifying settings of special parameters may cause system or network exceptions. You are advised to ask technical personnel of NSFOCUS for help when you need to modify these parameters.

4.3.3 Configuring NetFlow

When collaborating with NSFOCUS Network Traffic Analyst (NTA), NIPS can identify DDoS attacks more effectively. However, if the switch does not support NetFlow, you must configure NetFlow on NIPS by performing the following steps:

Step 1 Choose **System** > **System Configuration** > **NetFlow Configuration**.

Figure 4-9 NetFlow configuration



Step 2 Configure NetFlow parameters.

Table 4-4 NetFlow configuration parameters

Parameter	Description
Destination IP of NetFlow	Specifies the destination IP address to which NetFlow data will be sent, that is, the IP address of NTA.
Destination Port of NetFlow	Specifies the destination port corresponding to the specified destination IP address, that is, the port corresponding to the IP address of NTA.

Step 3 Click **Apply Settings** to save the settings.

----End

4.3.4 Configuring File Reassembly

NIPS supports reassembly of files transmitted. This function is associated with the file reputation switch and the TAC collaboration module. That is to say, if file reputation or advanced threat protection is enabled, the file reassembly function is automatically turned on.

Note	NIPS devices of the NX3-N300A model does not support the file reassembly function. Therefore, the **File Reassembly** page is absent on the web-based manager.

After this function is enabled, NIPS can reassemble files transferred via HTTP, FTP, POP3, SMTP, or IMAP. The following file types are supported:

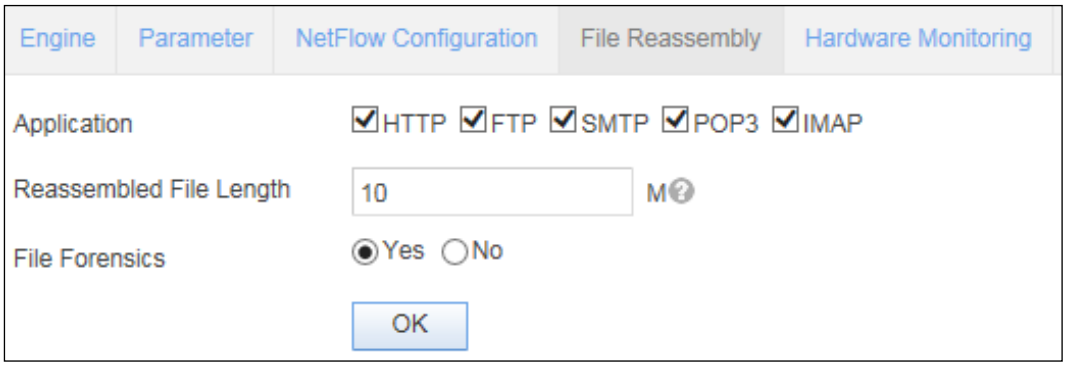
- MS Office (.doc, .xls, .ppt, .docx, .xlsx, and .pptx)
- Executables (.exe, .dll, .com, .scr, .pif, and .bat)
- PDF files (.pdf)
- Flash files (.swf)
- Java programs (.class and .jar)
- Web files (.html, .xml, and .js)
- Compressed files (.zip, .rar, .gzip, .gz, .tar, .7z, and .bz2)

Note	• Enabling the file reassembly function will degrade the performance of NIPS. • The current version does not support reassembly of files transferred via an encrypted channel.

To configure file reassembly, follow these steps:

Step 1 Choose **System** > **System Configuration** > **File Reassembly**.

Figure 4-10 File Reassembly page



Step 2 Configure parameters.

Table 4-5 File reassembly parameters

Parameter	Description
Application	Specifies protocols via which files are transferred. NIPS will reassemble files transferred via the specified protocols.
Reassembled File Length	Specifies the maximum length of files that can be reassembled by NIPS. Files whose size is larger than the value specified here will not be reassembled, matched, alerted, or blocked. The default value is **10** MB and the maximum value is 100 MB.
File Forensics	Controls whether to turn on the file forensics function. After **File Forensics** is set to **Yes**, NIPS will upload file samples to ESPC.

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

Step 4 Apply the settings.

----End

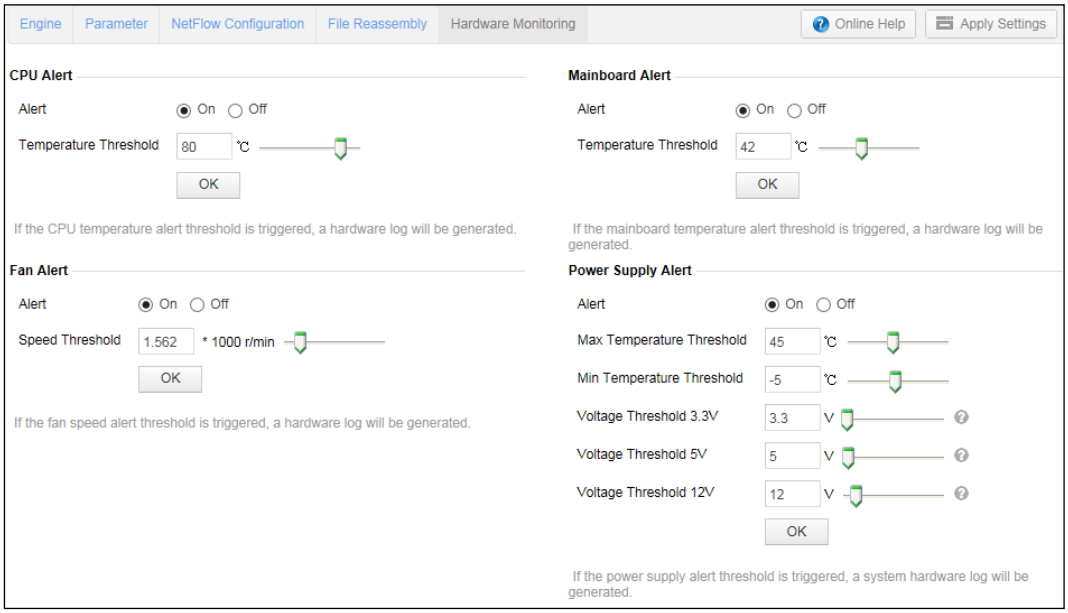
4.3.5 Configuring Hardware Monitoring

To configure hardware monitoring, follow these steps:

Step 1 Choose **System** > **System Configuration** > **Hardware Monitoring**.

The **Hardware Monitoring** page appears, on which you can configure hardware alert thresholds.

Figure 4-11 Configuring alert thresholds



Note	If NIPS has a CF card, but not a hard disk, the **Disk Alert** and **Auto Backup** areas are unavailable. The **Power Supply Alert** area is available only for NIPS devices of the following models, whose serial numbers contain the letter P (for example, 16-24-P-0223): NX3-N2000A, NX3-N3000A, NX5-N4000A, NX5-N6000A, NX5-N8000A, NX5-T9010A, and NX5-T9020A..

Step 2 Modify parameters and then click **OK** in the respective areas to commit the settings.

- **CPU Alert**: If the CPU alert function is enabled, when the CPU temperature exceeds the specified threshold, NIPS records a hardware log with the type of "CPU temperature log".
- **Mainboard Alert**: If the mainboard alert function is enabled, when the mainboard temperature exceeds the specified threshold, NIPS records a hardware log with the type of "Mainboard temperature log".
- **Fan Alert**: If the fan alert function is enabled, when the fan speed is lower than the specified threshold, NIPS records a hardware log with the type of "Fan status log".
- **Power Supply Alert**: If the power supply alert function is enabled, you need to respectively configure temperature thresholds and voltage thresholds.
  - **Temperature Threshold**: If the power temperature not in the range from the specified threshold lower limit to upper limit, the system assumes that the power supply is faulty. In this case, NIPS records a hardware log with the type of "Power temperature log".
  - **Voltage Threshold**: The voltage must fall within a plus or minus 5% of the specified threshold. If the voltage fluctuates beyond the range, the system assumes that the

power is faulty. In this case, NIPS records a hardware log with the type of "Power voltage log".

For how to view hardware logs, see section 8.1.4.4 Hardware Logs.

Step 3 Apply the settings.

----End

4.4 Security Center

NIPS can collaborate with NSFOCUS Cloud, Enterprise Security Planning Customer (ESPC), and Big Data Security Analytics (BSA).

- NSFOCUS Cloud

  NIPS sends alert messages generated on it to NSFOCUS cloud in real time and informs the emergency response team of faults in real time.

- NSFOCUS ESPC

  ESPC is a centralized management platform for NSFOCUS products. Thanks to the following features, it can greatly improve management efficiency:

  - Unified monitoring of multiple products
  - Configuration of policies in a centralized manner
  - Comprehensive management of reports

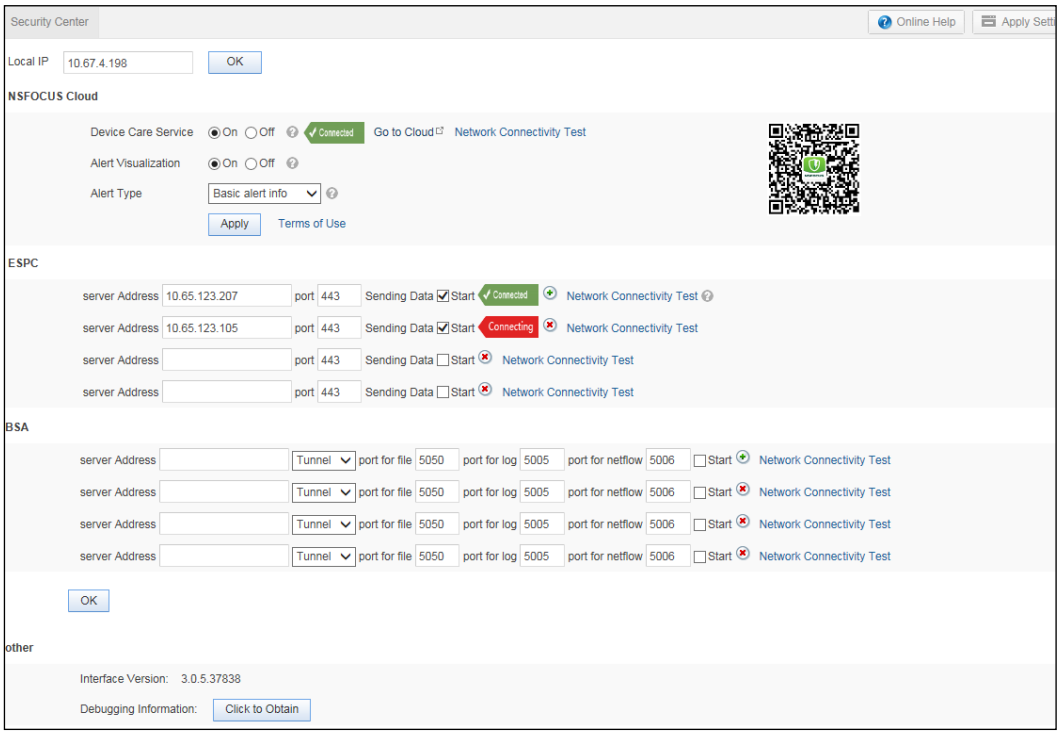
- NSFOCUS BSA

  BSA is a big data analysis platform for NSFOCUS products and third-party applications that meet certain conditions. Used to analyze security threat trends and provide support for customers' decision-making, BSA incorporates the functions of data collection and storage, indexing, query, report customization, real-time alerting, and basic analysis.

To connect NIPS to the security center, follow these steps:

Step 1 Choose **System** > **Security Center**.

Figure 4-12 Security Center page



Step 2 Configure **Local IP**.

Before configuring NIPS to connect to NFOCUS Cloud, ESPC, and BSA and configuring other settings, you need to configure the local IP address of NIPS, which is usually the IP address of an interface with the management function or that of a management interface.

Step 3 In the **NSFOCUS Cloud** area, configure parameters.

Table 4-6 Parameters for connecting NIPS to NSFOCUS Cloud

Parameter		Description
Local IP		By default, NIPS automatically detects the IP address of the interface that can connect to the Internet and automatically connects to NSFOCUS Cloud. After successful connection, NIPS automatically configures the IP address of this interface for Internet access as the local IP address. You can change the local IP address and then click **OK**. After the change, the device does not automatically detect any IP address that can connect to the Internet.
NSFOCUS Cloud	Device Care Service	Specifies whether to enable the device care service. The device care service is enabled by default. After it is turned on, NIPS automatically connects to NSFOCUS Cloud as long as the latter is reachable. Before the connection is established, Connecting is displayed. After the connection is established, Connected is displayed. Clicking **Go to Cloud** displays the NSFOCUS Cloud page, as shown in Figure 4-12. You can view device information by registering a new account or using an existing account or the

Parameter		Description
		default account. After logging in to NSFOCUS Cloud with a new or existing account, you can manage multiple devices. If you want to use the default account, click **Sign Up Later**. Then you can log in to NSFOCUS Cloud with the default account bundled with NIPS. In this case, you can view information about the current device and can manage only this device. Note After collaboration parameters are set, you can click **Network Connectivity Test** to check whether NIPS can properly connect to NSFOCUS Cloud. You can scan the QR code to download the app of NSFOCUS security manager. It can keep you updated on your device running status and service security status. For how to connect to NSFOCUS Cloud, refer to the online help information under **Products & Services > Device Care Service** on the NSFOCUS Cloud website (https://cloud.nsfocus.com/).
	Alert Visualization	Controls whether NIPS sends security event logs to the NSFOCUS cloud. By default, alert visualization is enabled.
	Alert Type	Specifies what fields of security event logs on NIPS to upload to ESPP. This field is available when **Alert Visualization** is turned on. **Basic alert info**: uploads all fields. This is the default setting. **Custom alert info:** allows you to select fields to upload.
ESPC	Server Address	Specifies the IP address of ESPC. NIPS can connect to a maximum of four ESPCs.
	Port	Specifies the port used by ESPC to exchange data with the NIPS engine.
	Sending Data	Controls whether to start connecting NIPS to ESPC. Selecting the **Start** check box enables NIPS to connect to ESPC. Note After collaboration parameters are set, you can click **Network Connectivity Test** to check whether NIPS can properly connect to ESPC. If the icon Connected is displayed, the connection has been established.
BSA	Server Address	Specifies the IP address of BSA. You can select the mode (**Tunnel** or **Encryption**) for connection between NIPS and BSA from the drop-down list to the right of **Server Address**. The configuration should be the same as that on NIPS. By default, the connection mode is **Tunnel**. You can click + or × to add or delete a BSA that connects to the NIPS engine.

Parameter		Description
	port for file	Specifies the port used by BSA to send files to the NIPS engine.
	port for log	Specifies the port used by BSA to send security logs (JSON) to the NIPS engine.
	port for netflow	Specifies the port used by BSA to send traffic logs (NetFlow) to the NIPS engine.
	Start	Controls whether to start connecting NIPS to BSA. Selecting the **Start** check box enables NIPS to connect to BSA. Note After collaboration parameters are set, you can click **Network Connectivity Test** to check whether NIPS can properly connect to BSA. If the icon Connected is displayed, the connection has been established.
Other	Interface Version	Indicates the version of the NPAI interface.
	Debugging Information	Status information of NIPS's collaboration with other devices through the NPAI interface. You can click **Click to Obtain** to save debugging information to a local disk drive.

Step 4 Apply the settings.

----End

4.5 Account Management

Under **System** > **Account Management**, you can manage accounts and set login parameters.

4.5.1 Managing Accounts

NIPS has three default accounts: operator **admin,** auditor **auditor,** and maintainer **supervisor**. **auditor** is not enabled by default and can only be enabled by **admin**. **admin** and **auditor** can create operator accounts and auditor accounts respectively. The default maintainer **supervisor** has any other permissions of admin, than permissions of restarting the device and engine and managing accounts. For details about their permissions, see Table 1-1.

- When you log in to NIPS with the **admin** account, the account list displays only operator accounts and the default auditor account. You can enable the default auditor account and create, modify, and delete operator accounts.
- When you log in to NIPS with the **auditor** account, the account list displays only auditor accounts. You can create, modify, and delete auditor accounts.
- When you log in to NIPS with the **supervisor** account, you cannot configure accounts.

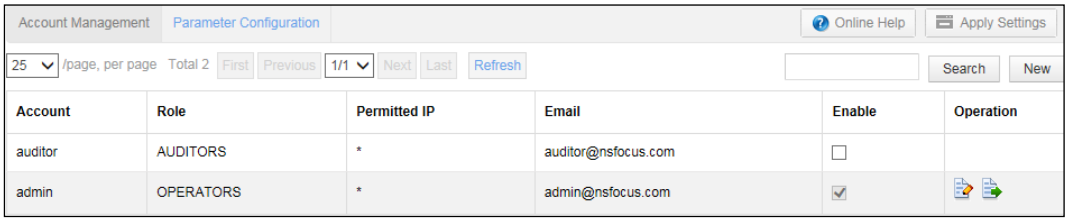
4.5.1.1 Enabling the Default Auditor Account

The default auditor account (**auditor**) can only be enabled by the default operator (**admin**). The default auditor account cannot be disabled after being enabled.

To enable the default auditor account, follow these steps:

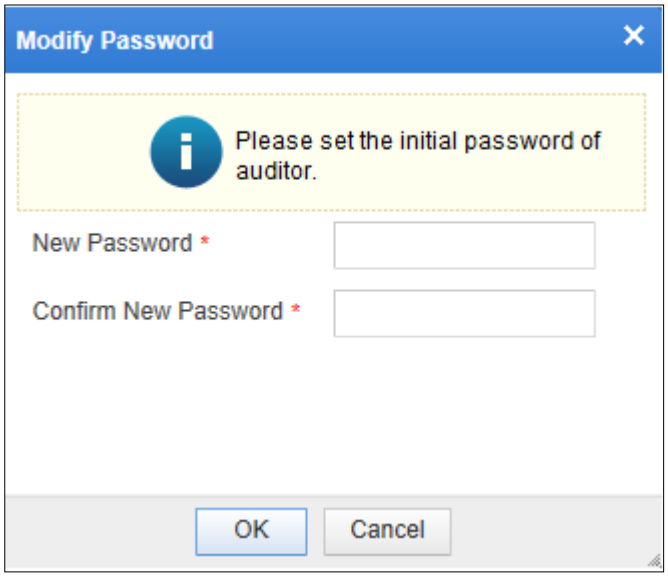
Step 1 Log in to NIPS with the **admin** account and choose **System** > **Account Management** > **Account Management**.

Figure 4-13 Account list



Step 2 Select the **Enable** check box of the auditor account.

Figure 4-14 Setting the initial password of the default auditor account



Step 3 In the **Modify Password** dialog box, set the initial password of the default auditor account.

Step 4 Click **OK** to complete the configuration and enable the default auditor account.

After being enabled, the default auditor account (**auditor**) disappears from the account list shown in Figure 4-15.

----End

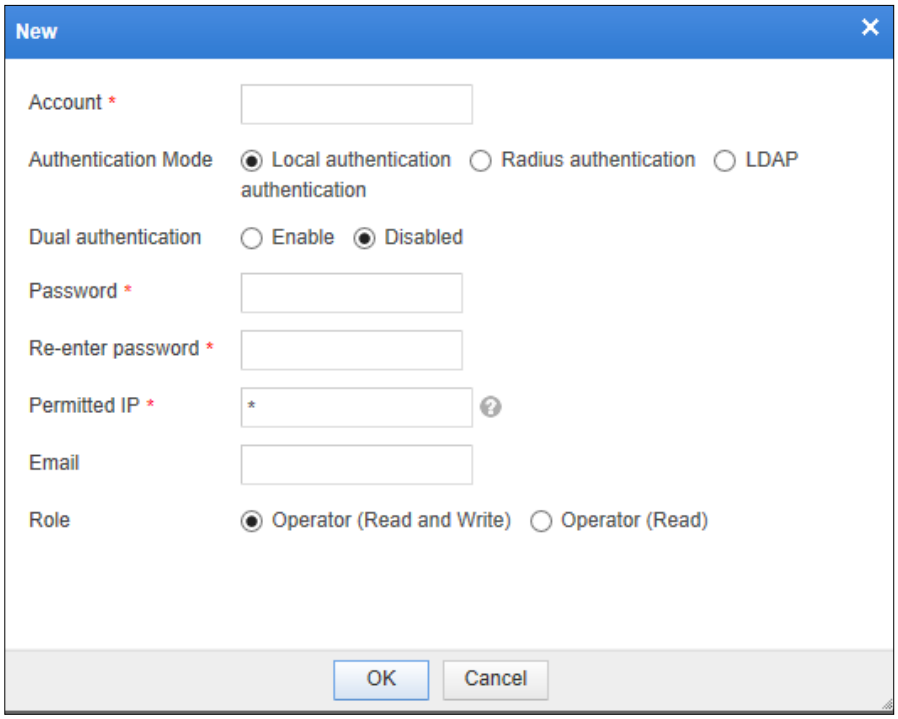
4.5.1.2 Creating an Account

Only the default operator and auditor accounts can create accounts. The following takes the default operator account (**admin**) as an example to describe how to create an account:

Step 1 Choose **System** > **Account Management** > **Account Management**.

Step 2 Click **New** in the upper-right corner.

Figure 4-15 Creating an account



Step 3 Configure parameters in the **New** dialog box.

Table 4-7 Parameters for creating an operator account

Parameter	Description
Account	Specifies the account name. It is a string of 4 to 20 characters, including English letters, digits, hyphens, and underscores. An account name must start with a letter. The account name cannot be changed after the account is successfully created.
Authentication Mode	Specifies the authentication mode for this account. It has the following values: • **Local authentication**: Use the default settings. • **Radius authentication**: The Radius authentication server, port, method, and shared key must also be specified. For details, see section 4.5.2 Configuring Parameters. • **LDAP authentication**: An LDAP authentication server must be configured. For details, see section 4.5.2 Configuring Parameters.
Dual authentication	Controls whether to enable certificate-based authentication for this account at the same time. After **Dual authentication** is set to **Enable**, both password authentication and certificate-based authentication are enabled for this account.

Parameter	Description
	That is, this account is authenticated only after an incorrect certificate is imported. After **Dual authentication** is set to **Enable**, you need to download a certificate. For details, see section 4.5.1.5 Exporting a Certificate.
Password	Specifies the login password, which cannot be the same as the account name and whose length and complexity must comply with the specifications described in section 4.5.2 Configuring Parameters.
Re-enter password	Requires you to reenter the password for confirmation.
Permitted IP	Specifies the IP address that can be used by this new account for login. You can type an IP address, a network segment, or multiple IP addresses. The default value is *****, indicating that the operator can log in to NIPS from any IP address.
Email	Specifies the valid email address of the operator who uses this new account.
Role	Specifies the role of this account. Different roles have different permissions. The value can be **Operator (Read and Write)** or **Operator (Read)**.

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

Note	By default, all new accounts are enabled. Only enabled accounts can be used for login.

----End

4.5.1.3 Modifying an Account

Log in to NIPS with the default account **admin** or **auditor**. Clicking in the **Operation** column opens the **Edit** dialog box.

- With a default system account, you can modify information of accounts that you have created except the account name.
- New operators or auditors can modify their own account information except the account name.
- If you forget the new password for a default system account, you can reset the password on the console user interface of the engine. For details, see section 9.3 Using Maintenance Tools.
- You can modify information of the current account on the home page of NIPS. For details, see section 1.3.1.3 Page Layout of the Web-based Manager.
- After you log in to NIPS with the **supervisor** account, you can only modify the password of the current account by clicking the user name in the upper-right corner of the page and then configuring parameters in the dialog box that appears.

4.5.1.4 Deleting an Account

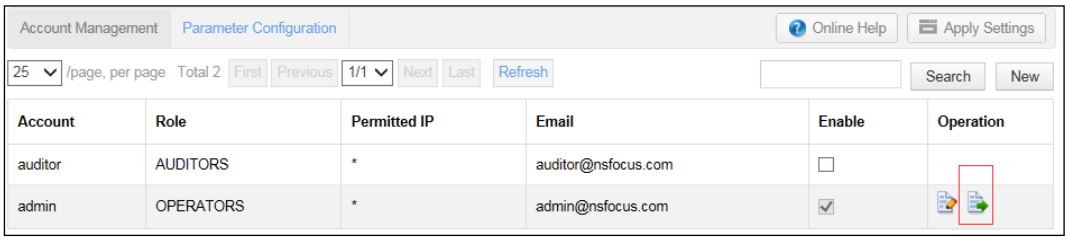
Only the default operator account (**admin**) and auditor account (**auditor**) can delete accounts that they have created respectively. They cannot delete default system accounts.

4.5.1.5 Exporting a Certificate

When creating an account, if you enable dual authentication, the account will be authenticated first by password and then by certificate. In this case you need to export a certificate for the account to log in to the system.

Step 1 Choose System > Account Management > Account Management.

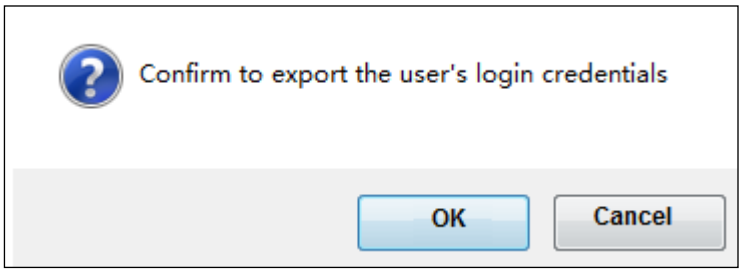
Figure 4-16 Downloading a certificate



The **auditor** account does not support dual authentication. Therefore, you cannot export a certificate for the **auditor** account.

Step 2 Click  in the **Operation** column of an account.

Figure 4-17 Confirming the export of a certificate



Step 3 Click **OK** in the confirmation dialog box.

You can select a path and file name for the certificate to be exported.

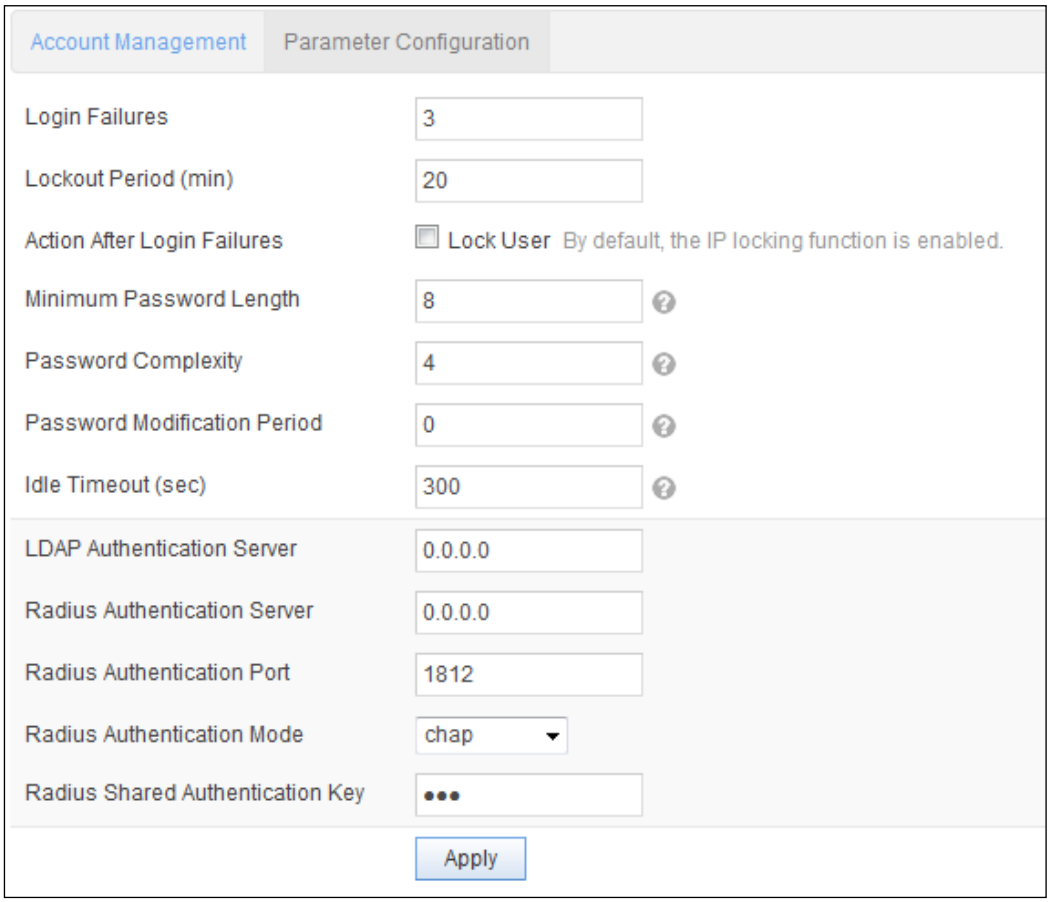
----End

4.5.2 Configuring Parameters

The **Parameter Configuration** page is used for setting parameters for logging in to NIPS and parameters for connecting to third-party authentication servers. To configure these parameters, follow these steps:

Step 1 Choose **System** > **Account Management** > **Parameter Configuration**.

Figure 4-18 Account parameter configuration



Step 2 Configure parameters.

Table 4-8 Account login configuration parameters

Parameter	Description
Login Failures	Specifies the number of allowed consecutive login failures. The default value and the maximum value you can set are both **3**.
Lockout Period (min)	Specifies a period during which a user has to wait before being allowed to log in again after the number of consecutive login failures reaches the threshold specified with **Login Failures**. The default value is **20** minutes.
Action After Login Failures	Specifies whether to lock an account when the number of consecutive login failures reaches the threshold specified with **Login Failures**. If the **Lock User** check box is selected, the account will be locked out even if the user logs in from another IP address. **Note** • By default, the IP lockout function is enabled. A locked-out account can retry only after the account lockout period specified with **Lockout Period (min)** expires. • Account locking will be recorded in an audit log. The auditor can view such logs after logging in to the system.

Parameter	Description
Minimum Password Length	Specifies the minimum length of passwords for users to log in to NIPS. The value range is 8–32 characters, with **8** as the default.
Password Complexity	Specifies the password complexity, that is, how many of the following must be included in passwords: • Digit • Uppercase letter • Lowercase letter • Symbol The value range is 1–4, with **4** as the default.
Password Modification Period	Specifies the number of days a password can be used. When a password remains in use for a period longer than the value specified here, the system will force users to change it. The default value is **0**, indicating no limit to the number of days a password is used.
Idle Timeout (sec)	Specifies the period during which a user can stay idle before being logged out. When the idle period expires, NIPS automatically returns to the login page and the user has to log in again before performing other operations. The default value is **300**. The value **0** indicates that users will not be automatically logged out regardless of how long they are idle. Note It is recommended that you set this parameter to a value smaller than 600.
LDAP Authentication Server	Specifies the IP address of the LDAP authentication server.
Radius Authentication Server	Specifies the IP address of the Radius authentication server.
Radius Authentication Port	Specifies the port on which the Radius authentication server listens for authentication requests. The default Radius authentication port is **1812**.
Radius Authentication Mode	Specifies the authentication mode of the Radius authentication server, which can be **pap**, **spap**, **chap**, **mschapv1**, **mschapv2**, or **eap_md5**.
Radius Shared Authentication Key	Specifies the shared key that serves as a password between the Radius server and a Radius client. Note The shared secret configured on NIPS must be the same as that configured on the Radius server; otherwise, NIPS cannot communicate with the Radius server.

Step 3 Apply the settings.

----End

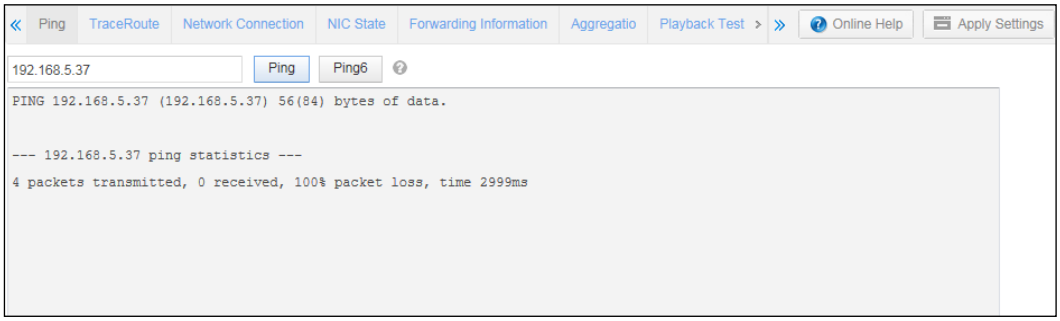
4.6 Diagnosis Tools

Under **System** > **Diagnostic Tools**, you can use diagnostic tools to view such information as network connections and network interface card (NIC) status. For example, when an exception occurs, you can use the ping or traceroute tool to perform diagnosis and view related information.

4.6.1 Ping

Ping is used to check whether a host is alive or reachable over the current network. NIPS provides the function of pinging both IPv4 and IPv6 addresses, as shown in Figure 4-19.

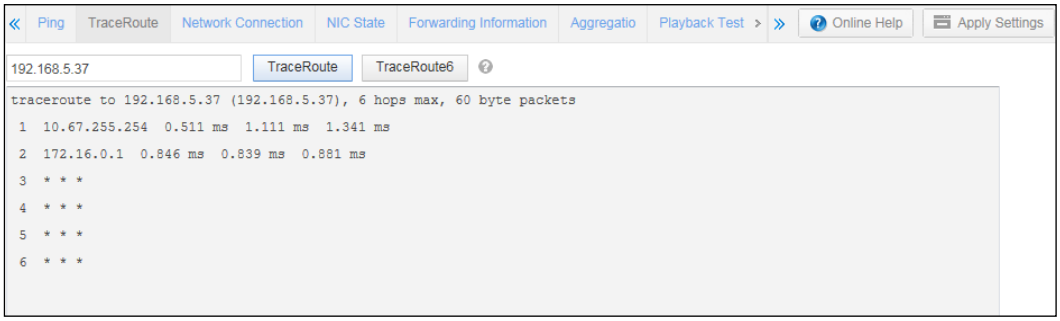
Figure 4-19 Ping result



4.6.2 Traceroute

Traceroute is a network diagnostic tool for checking the route (path) taken by packets across an IP network. The traceroute tool on NIPS supports both IPv4 and IPv6 addresses, as shown in Figure 4-20.

Figure 4-20 Traceroute result



4.6.3 Network Connection

You can check the network connections and server status. In addition, you can clear session information in the system.

- The **Network Connection** page displays network connection information, including the protocol and port, as shown in Figure 4-21.

Figure 4-21 Network connections

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:50022           0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:8081          0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:695             0.0.0.0:*               LISTEN
tcp        0      0 10.67.4.124:50022       10.67.5.1:53191         ESTABLISHED
tcp        0      0 10.67.4.124:37427       216.163.188.45:80       CLOSE_WAIT
tcp        1      0 10.67.4.124:35898       216.163.188.45:80       CLOSE_WAIT
tcp        0      0 10.67.4.124:50022       10.67.4.22:58800        ESTABLISHED
tcp        1      0 10.67.4.124:51706       103.5.198.219:80        CLOSE_WAIT
tcp        0      0 10.67.4.124:50022       10.67.4.22:58785        ESTABLISHED
tcp        1      0 10.67.4.124:56085       103.5.198.219:80        CLOSE_WAIT
tcp6       0      0 :::50022                :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
tcp6       0      0 10.67.4.124:443         10.67.1.9:60095         TIME_WAIT
tcp6       0      0 10.67.4.124:443         10.67.1.9:60133         ESTABLISHED
udp        0      0 127.0.0.1:50002         0.0.0.0:*
udp   116920      0 127.0.0.1:50003         0.0.0.0:*
udp        0      0 127.0.0.1:50004         0.0.0.0:*
udp        0      0 127.0.0.1:50005         0.0.0.0:*
udp        0      0 0.0.0.0:60358           0.0.0.0:*
udp        0      0 127.0.0.1:1040          0.0.0.0:*
udp        0      0 127.0.0.1:1041          0.0.0.0:*
udp        0      0 127.0.0.1:1042          0.0.0.0:*
udp        0      0 127.0.0.1:1050          0.0.0.0:*
udp        0      0 127.0.0.1:1051          0.0.0.0:*
udp        0      0 127.0.0.1:1061          0.0.0.0:*
udp        0      0 127.0.0.1:1150          0.0.0.0:*
udp        0      0 127.0.0.1:30015         0.0.0.0:*
udp        0      0 127.0.0.1:20016         0.0.0.0:*
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ACC ]     STREAM     LISTENING     8711     /var/run/nsconfig.socket
unix  2      [ ACC ]     STREAM     LISTENING     1102     /var/run/acpid.socket
unix  2      [ ]         DGRAM                    52309    /var/tmp/updater.socket
unix  2      [ ]         DGRAM                    1719     /var/plat_srv.socket
unix  2      [ ]         DGRAM                    8147     /var/tmp/guard.socket
unix  2      [ ]         DGRAM                    3171
unix  2      [ ]         DGRAM                    3166
unix  2      [ ]         DGRAM                    3159
```

- The **Network Connection** page also displays server status information, as shown in Figure 4-22.

Figure 4-22 Server status

```
class 4  - rx: 71866533  rx_drop: 0         alive:1 pid:20475 timeout:5 dead:5
   cpu: p:1% i:99% avg_cycle:0%   heart:0x10ff4fdc4
Server
------
r: 26% t: 34% p: 16% i: 24%
heart: 0x53880df0c  avg_cycle:229174
Packet Pools:
------
pktmbuf_pool:13824/65536
MP_Client_0_RX:0/4095MP_Client_1_RX:0/4095MP_Client_2_RX:0/4095MP_Client_3_RX:0/4095MP_Client_4_RX:0/4095
virtual_ring:0/4095
ipflow info:
------
realtime total flow count: 1044146
                      tcp: 1009218
                      udp: 34928
flow created: 32526338
drop count: 96367968
turbo boost: 692107
flowmbuf_pool:4430
packets cache:close
```

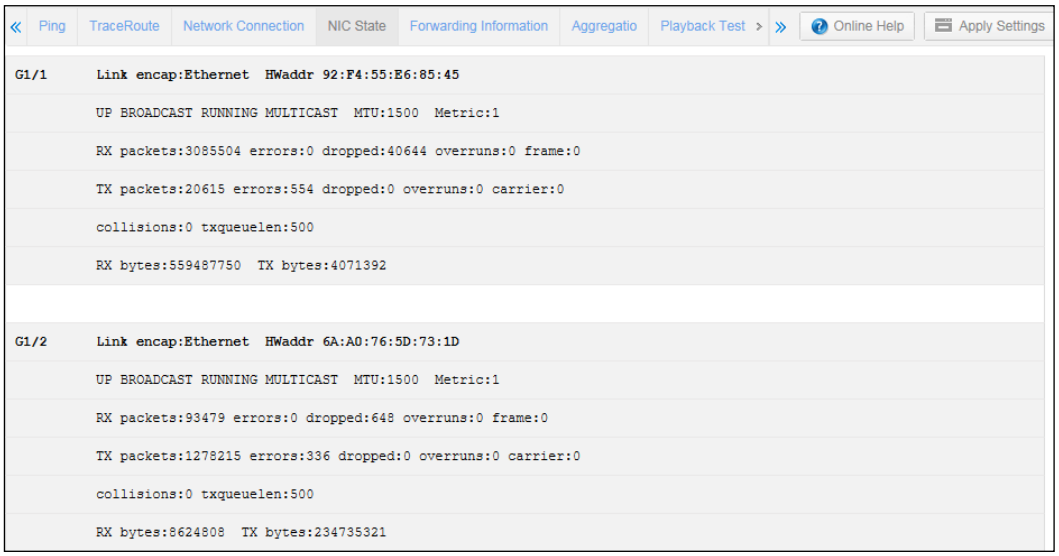
Clear Session Table Clearing the session table will cause temporary network interruption.

- Clicking **Clear Session Table** will clear all session information and restart the engine. This operation would result in temporary network interruption. Therefore, perform this operation with caution.

4.6.4 NIC State

The **NIC State** page displays NIC status information, as shown in Figure 4-23. Users can determine whether a network exception is caused by a NIC fault from information on this page.

Figure 4-23 NIC status



4.6.5 Aggregation Status

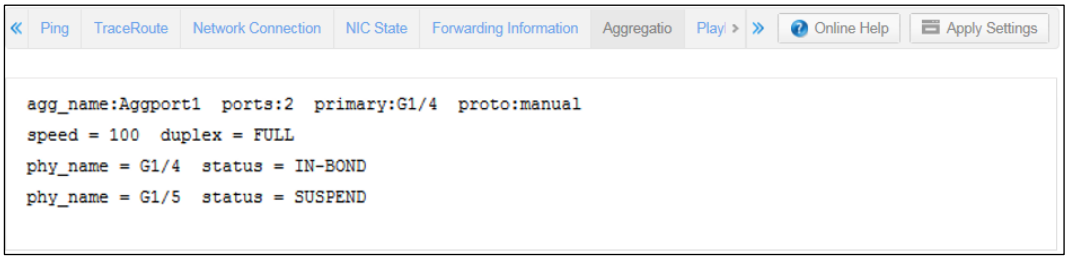
NIPS adopts IEEE 802.3ad for link aggregation, allowing the operator to bind multiple Ethernet interfaces that are configured as member interfaces to the specified aggregation interface. Aggregation interfaces can increase the bandwidth and improve fault tolerance. You can view the status of the aggregation link. For how to configure an aggregation interface, see section 5.1.2.3 Creating an Aggregation Interface.

Step 1 Choose **System** > **Diagnostic Tools** > **Aggregation**.

The aggregation mode can be manual aggregation or dynamic aggregation. The aggregation status information varies with the aggregation mode.

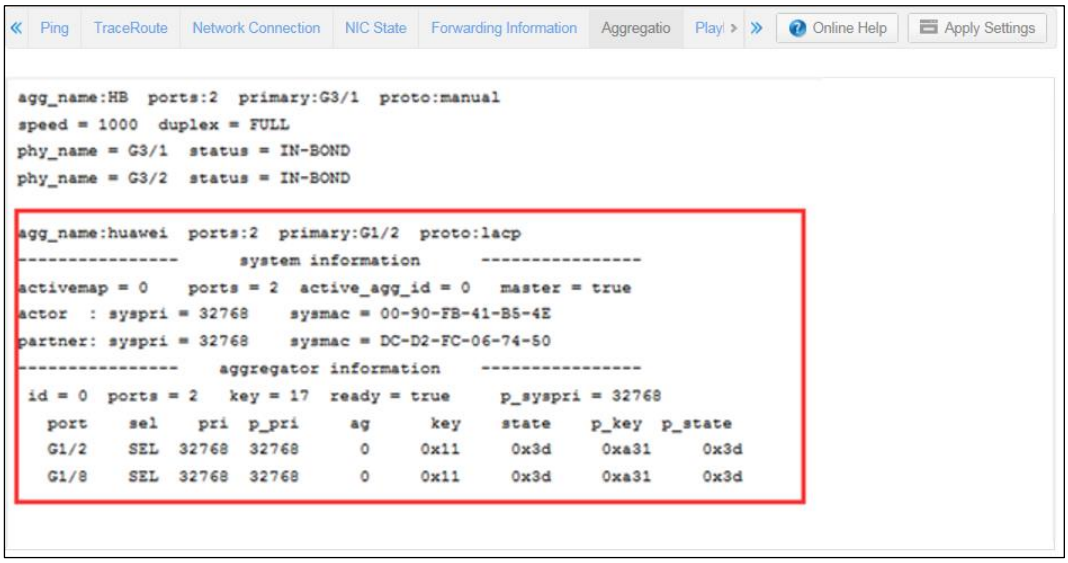
- Figure 4-24 shows the link aggregation status in manual aggregation mode.

Figure 4-24 Aggregation status in manual aggregation mode



- Figure 4-25 shows the link aggregation status in dynamic aggregation mode.

Figure 4-25 Aggregation status in dynamic aggregation mode



----End

4.6.6 Forwarding Information

NIPS NX5-T9010A and NX5-T9020A have the **Route Information** tab page that displays only real-time route information.

Other models have the **Forwarding Information** tab page for users to check whether specified switch information, route information, and layer-2 loops already exist and how to view all route information.

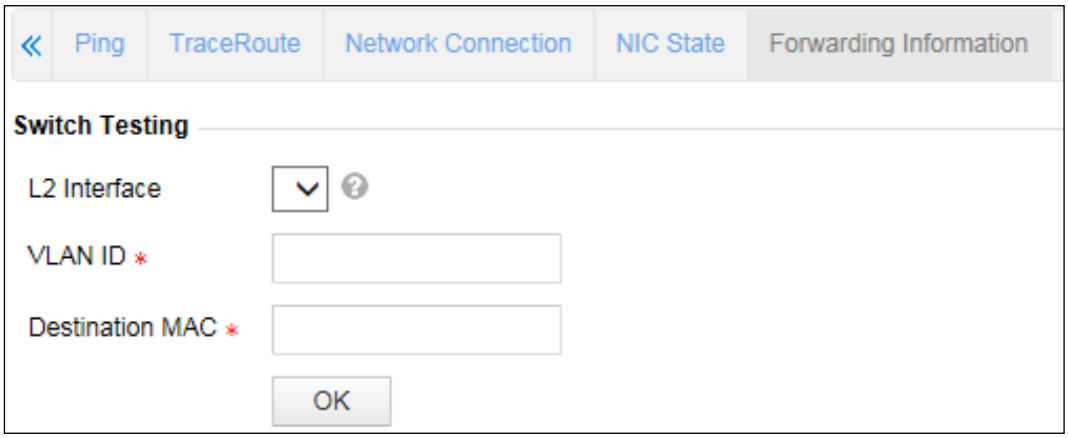
4.6.6.1 Switch Detection

You can use the switch detection tool to check whether the MAC address information of the specified layer 2 switch already exists.

To use the switch detection tool, perform the following steps:

Step 1 Choose System > Diagnostic Tools > Forwarding Information.

Figure 4-26 Switch Testing area



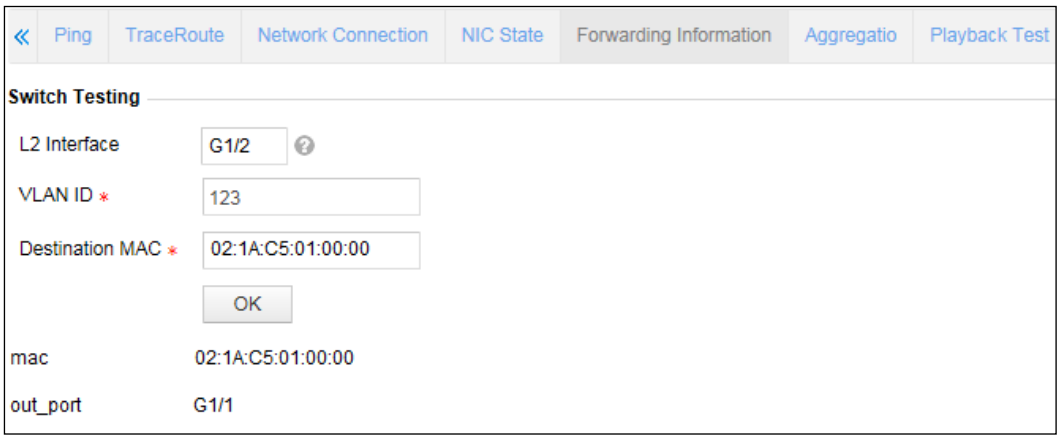
Step 2 Configure parameters.

Table 4-9 Parameters for enabling the switch detection function

Parameter	Description
Layer 2 Interface	Specifies the layer 2 interface that connects to the target host.
VLAN ID	Specifies the ID of the VLAN that the target host belongs to.
Destination MAC	Specifies the MAC address of the target host.

Step 1 Click **OK** to check whether the MAC address information of the specified layer 2 switch already exists.

Figure 4-27 Switch detection result



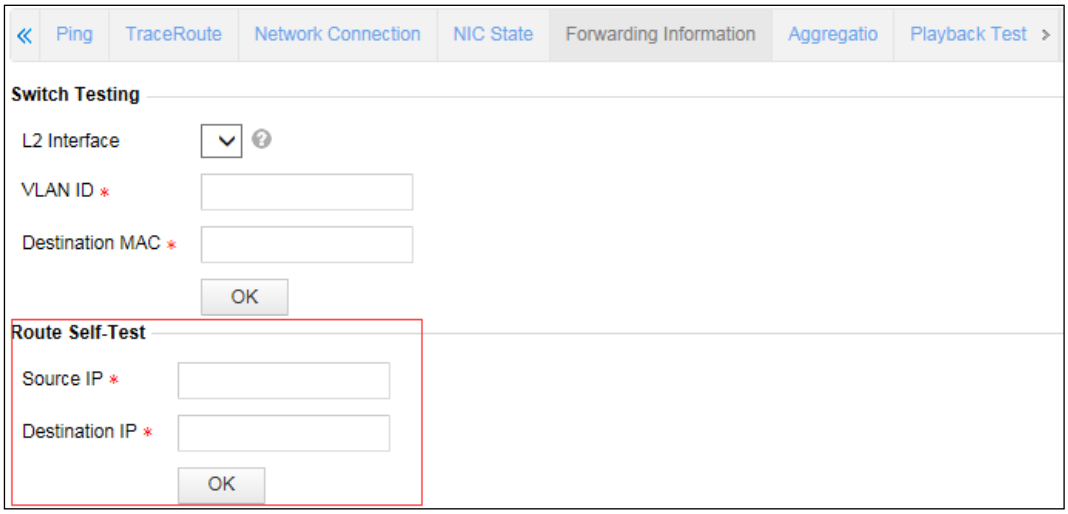
----End

4.6.6.2 Route Detection

The route detection tool is used to check whether the specified route information already exists.

Step 1 Choose **System** > **Diagnostic Tools** > **Forwarding Information**.

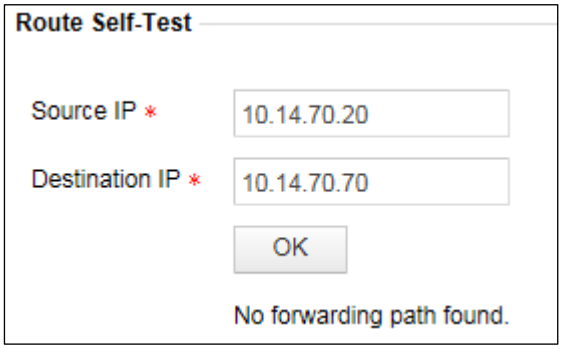
Figure 4-28 Viewing information about the specified route



Step 2 Set source and destination IP addresses.

Step 3 Click **OK**.

Figure 4-29 Viewing information about the specified route



----End

4.6.6.3 Layer 2 Loop Detection

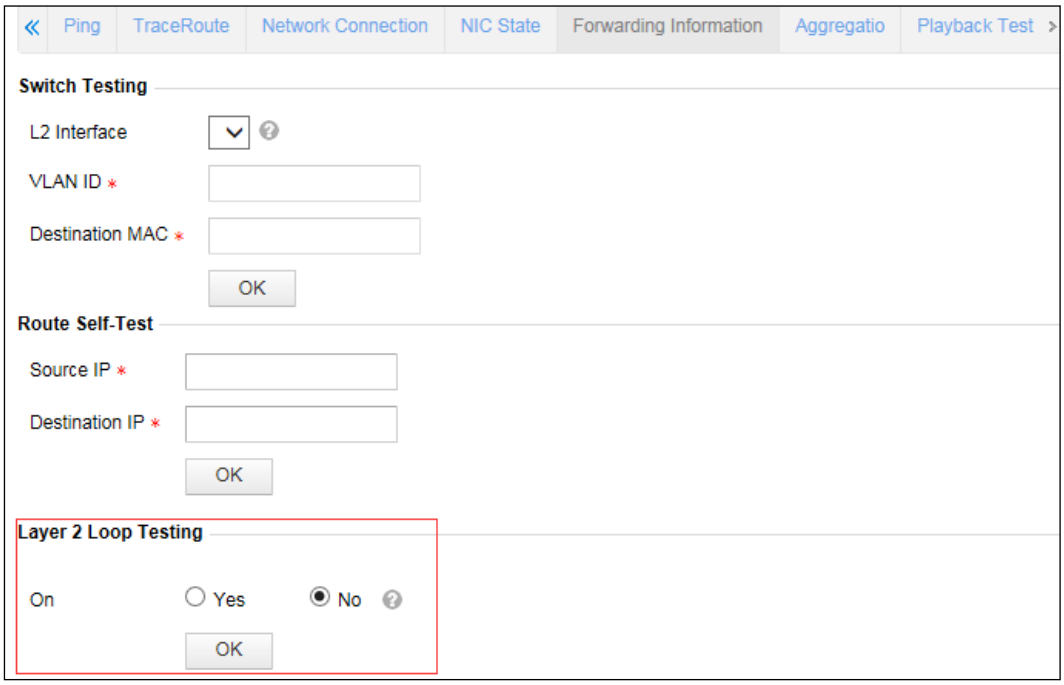
The layer 2 loop detection tool is used to check whether a loop exists on the layer 2 link.

Note	When the layer 2 loop testing function is enabled for a specific interface, the system logs the detected layer2 loop information in running logs. For how to view running logs, see section 8.1.4.3 Running Logs.

For how to enable the layer 2 loop testing function, follow these steps:

Step 1 Choose **System** > **Diagnostic Tools** > **Forwarding Information**.

Figure 4-30 Layer 2 Loop Testing area



Step 2 Configure parameters.

a. Select **Yes** for **On** to enable the layer 2 loop detection function.

b. Enable or disable the layer 2 loop detection function for a specific interface.

All layer 2 interfaces are displayed. By default, the layer 2 loop detection function is disabled. You enable the layer 2 loop detection function for a specific interface by selecting **Yes** for **On**.

c. Click **OK**.

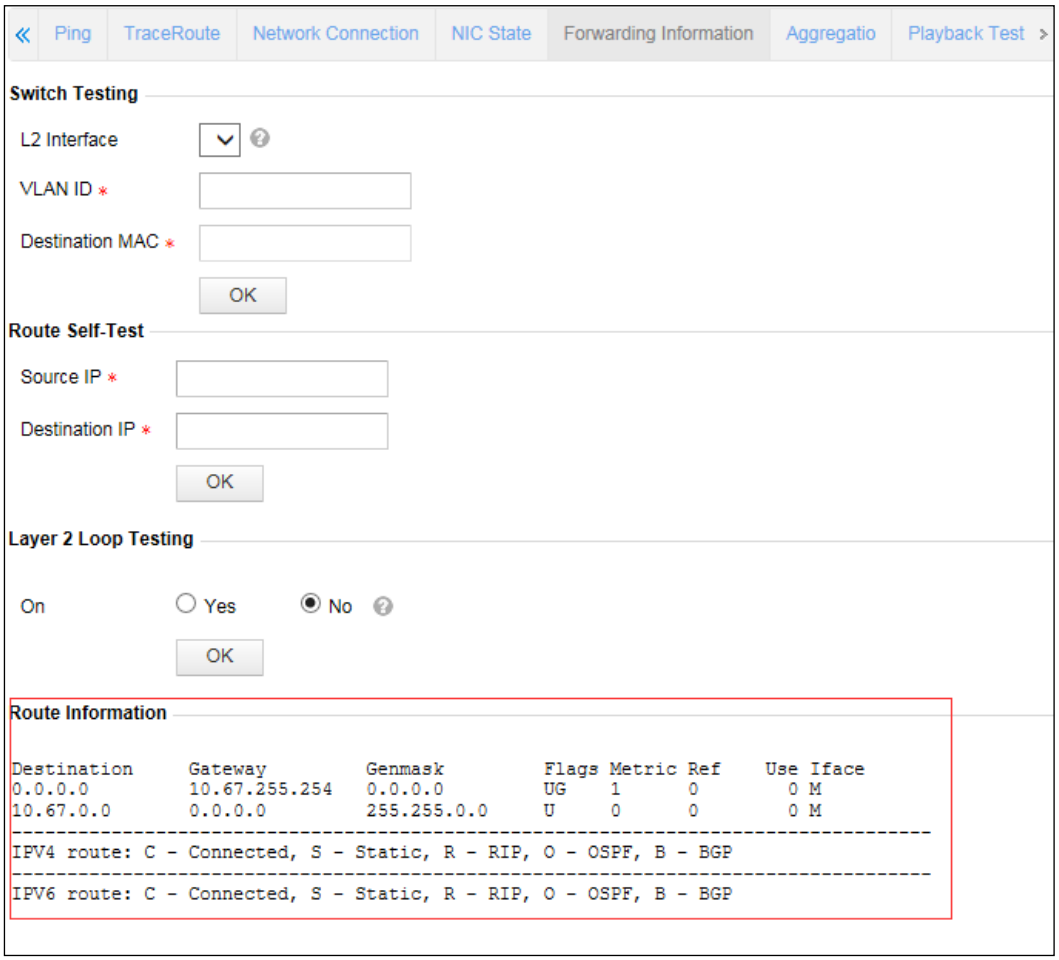
----End

4.6.6.4 Route Information

This tool is used for obtaining route information in real time. The route information varies with hardware platforms.

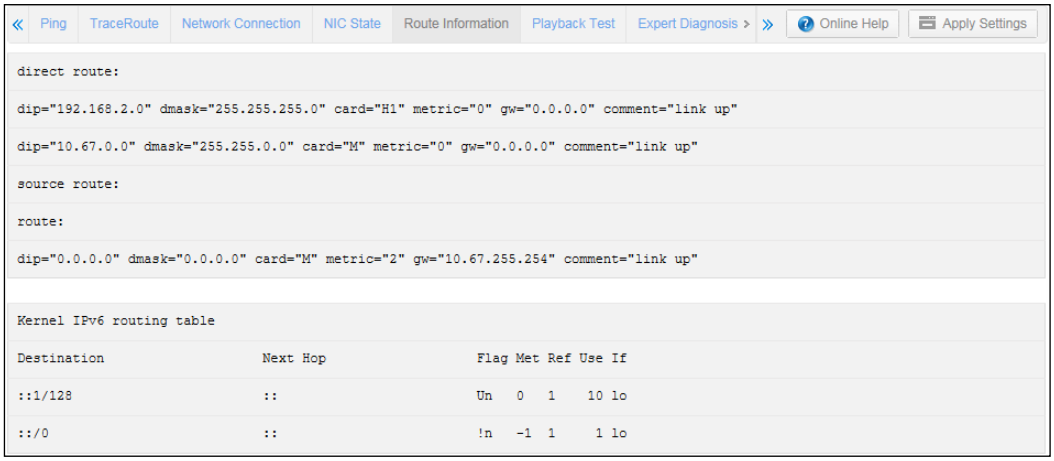
- For NIPS devices other than NIPS NX5-T9010A and NX5-T9020A, choose **System** > **Diagnostic Tools** > **Forwarding Information** to view real-time route information.

Figure 4-31 Real-time route information



- For NIPS NX5-T9010A and NX5-T9020A, choose **System** > **Diagnostic Tools** > **Route Information** to view real-time route information.

Figure 4-32 Route information



4.6.7 Playback Test

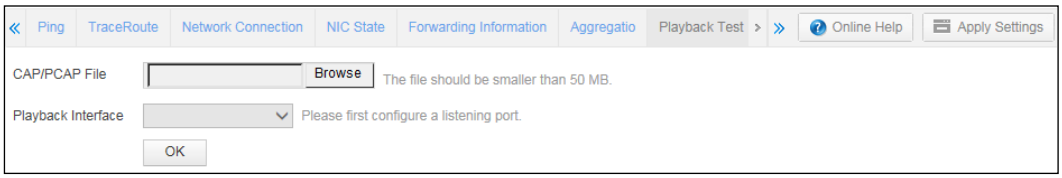
NIPS provides the function of reading packet capture files through the listening interface. Users can analyze network data based on these files.

Note	• Only interfaces in security zones of the Monitor type can be used to play back data. • If no monitoring interface is available, you must configure one first.

To perform a playback test, follow these steps:

Step 1 Choose **System** > **Diagnostic Tools** > **PlaybackTest**.

Figure 4-33 Playback test



Step 2 Click **Browse**, select a CAP/PCAP file, and click **Open**.

Step 3 From the **Playback Interface** drop-down list, select a monitoring interface to which data will flow during the playback test.

Step 4 Click **OK**.

----End

4.6.8 Expert Diagnosis

When NIPS is faulty and requires remote assistance, technical support engineers of NSFOCUS can remotely log in to the faulty NIPS via SSH and perform troubleshooting in the background.

The IP address and port of an SSH server, which is deployed on the Internet, are available in the NIPS background. After expert diagnosis is started, technical support engineers of NSFOCUS can connect to the SSH server from an SSH client and log in to the mapped device for troubleshooting in the background.

- If the faulty NIPS can access the Internet, you can use the expert diagnosis function provided by this device.
  - If the faulty device can access the SSH server, the device will map the SSH port on it to the SSH server.
  - If the faulty device cannot access the SSH server, but a host that is reachable from the device can access the SSH server, run **PortGo.exe** on this host and configure related settings. After that, the SSH port on the device can be mapped to the SSH server.
- If the faulty device cannot access the Internet, the expert diagnosis function is unavailable.

Note	• **PortGo.exe** is provided and used by site engineers. Therefore, it is not delivered with NIPS. • Currently, a host for technical support can connect to multiple NIPS devices. However, multiple hosts for technical support cannot connect to the same NIPS simultaneously.

To enable the expert diagnosis function, follow these steps:

Step 1 Choose **System** > **Diagnostic Tools** > **Expert Diagnosis**.

Figure 4-34 Expert diagnosis

Step 2 Click **Start** to start the expert diagnosis function.

----End

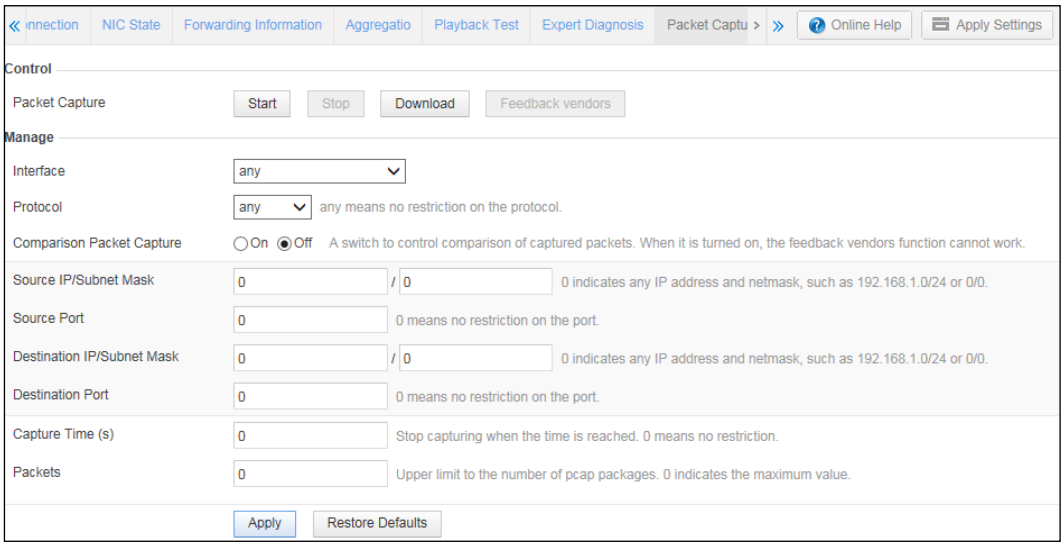
4.6.9 Packet Capture

NIPS allows users to capture packets directly from device interfaces for analyzing and debugging problems with network deployment.

To capture packets, follow these steps:

Step 1 Choose **System** > **Diagnostic Tools** > **Packet Capture**.

Figure 4-35 Packet capture



Step 2 Configure parameters.

Table 4-10 Parameters for configuring a packet capture task

Parameter	Description
Interface	Specifies an interface on which packets are captured. The default value is **any**, indicating that packets are captured on all interfaces other than management interfaces.
Protocol	Specifies a protocol so that packets transmitted through this protocol will be captured. This parameter can be set to **any**, **IP**, **TCP**, **UDP**, **ICMP**, **IPv6**, or **ICMPv6**. The default value is **any**, indicating packets of all these protocols will be captured.
Comparison Packet Capture	Controls whether to enable the comparative packet capture function. It is disabled by default. • **On**: saves inbound packets and outbound packets in two files, which will then be compressed and bundled into a single folder. • **Off**: saves inbound and outbound packets in a single file and then compresses it.
Source IP/Subnet Mask	Specifies the source IP address and subnet mask so that packets from this IP segment will be captured. This parameter is optional. Leaving this parameter empty indicates that packets from any IP addresses will be captured.
Source Port	Specifies a port so that packets from this port will be captured. The value **0** indicates that packets from any ports will be captured.
Destination IP/Subnet Mask	Specifies the destination IP address and subnet mask so that packets destined for this IP segment will be captured. This parameter is optional. Leaving this parameter empty indicates that packets destined for any IP address will be captured.
Destination Port	Specifies a port so that packets to this port will be captured. The value **0** indicates that packets to any ports will be captured.
Capture Time (s)	Specifies the duration of this packet capture task. Packet capture will stop when the specified length of time elapses. The value **0** indicates no limit to the time.
Packets	Specifies the maximum number of PCAP packets to be captured. Packet capture will stop when the number of packets reaches this value. The value **0** indicates no limit to the number of packets.
ruleid	Specifies a rule ID on which packet capture will be based. The value **0** indicates that this parameter does not take effect.
appid	Specifies an application ID on which packet capture will be based. The value **0** indicates that this parameter does not take effect.

Step 3 Click **Apply Settings** to save the settings.

Step 4 Click **Start** to start capturing packets.

Step 5 (Optional) Stop the packet capture task.

- The packet capture task will automatically stop when the **Capture Time** value is reached.
- The packet capture task will automatically stop when the **Packets** value is reached.
- During the packet capture process, you can click **Stop** to terminate the ongoing task.

Step 6 (Optional) Click **Download** to download the packet capture file to a local disk drive for analysis.

Step 7 (Optional) Click **False Positive** to send the packet capture file to ESPP.

----End

4.6.10 One-Click Inspection

NIPS allows you to inspect the hardware and services by clicking only one button. In this manner, you can learn the status and information of all hardware components and services quickly and conveniently.

- Hardware inspection objects

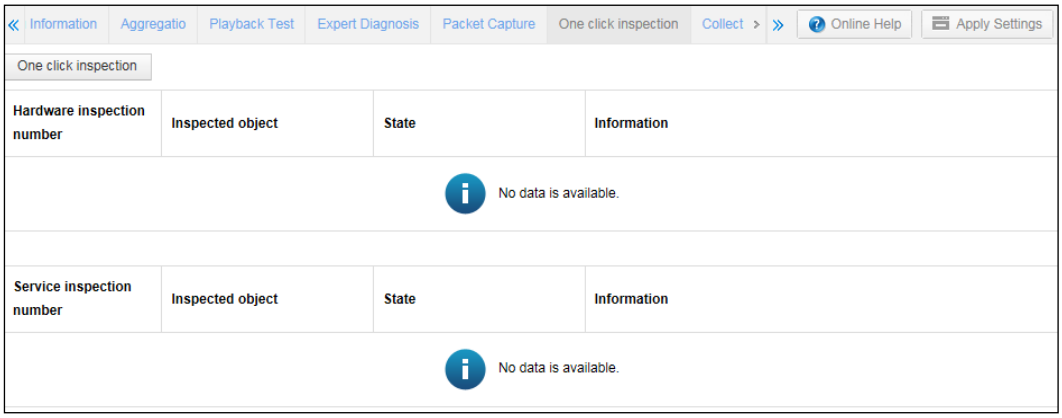
  CPU, memory, disk drives, management interfaces, and working interfaces
- Service inspection objects

  Datacom engine, security engine, service monitoring process, daemon (Guard), process for transmitting system status logs, process for transmitting security logs, and process for transmitting application logs

To inspect hardware and services, follow these steps:

Step 1 Choose **System** > **Diagnostic Tools** > **One click inspection**.

Figure 4-36 One-click inspection

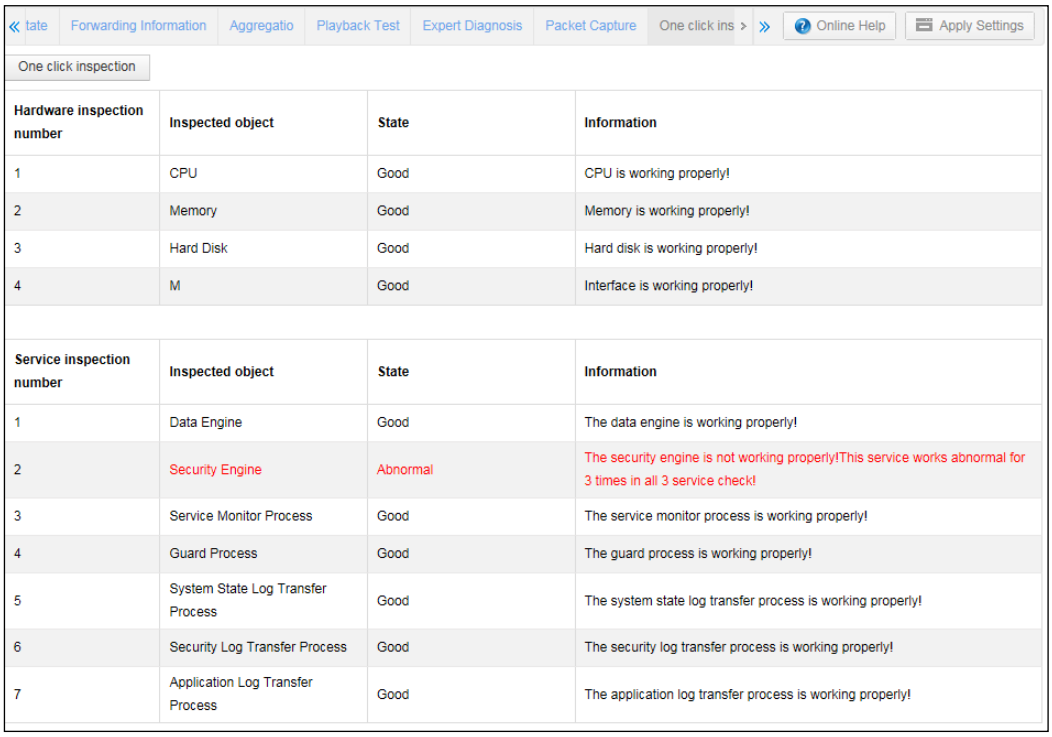


Step 2 Click **One click inspection**.

The system starts inspecting hardware and services.

The inspection will take some time. Please wait patiently. Figure 4-37 shows the inspection result.

Figure 4-37 Inspection result



Hardware inspection number	Inspected object	State	Information
1	CPU	Good	CPU is working properly!
2	Memory	Good	Memory is working properly!
3	Hard Disk	Good	Hard disk is working properly!
4	M	Good	Interface is working properly!

Service inspection number	Inspected object	State	Information
1	Data Engine	Good	The data engine is working properly!
2	Security Engine	Abnormal	The security engine is not working properly!This service works abnormal for 3 times in all 3 service check!
3	Service Monitor Process	Good	The service monitor process is working properly!
4	Guard Process	Good	The guard process is working properly!
5	System State Log Transfer Process	Good	The system state log transfer process is working properly!
6	Security Log Transfer Process	Good	The security log transfer process is working properly!
7	Application Log Transfer Process	Good	The application log transfer process is working properly!

Hardware components or services in abnormal state are displayed in red. The **Information** column provides details about the cause of such anomalies.

----End

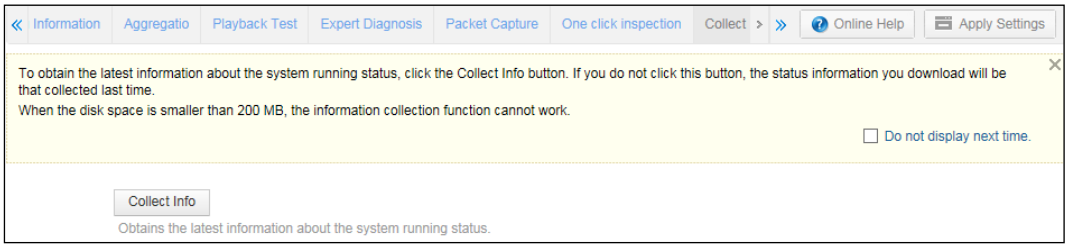
4.6.11 Information Collection

NIPS allows you to collect the latest information about its running status, including packet loss information and bypass-related logs.

To collect information about the system running status, follow these steps:

Step 1 Choose **System > Diagnostic Tools > Collect Info**.

Figure 4-38 Information collection

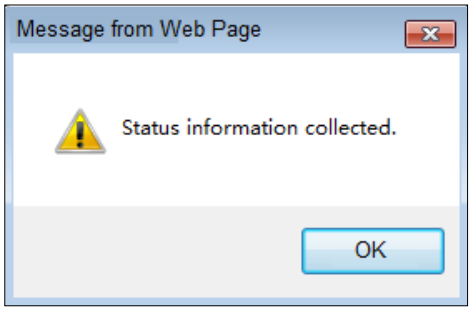


Step 2 Click **Collect Info**.

NIPS starts collecting the latest information about the system running status.

After such information is collected, the system displays a message, as shown in Figure 4-39.

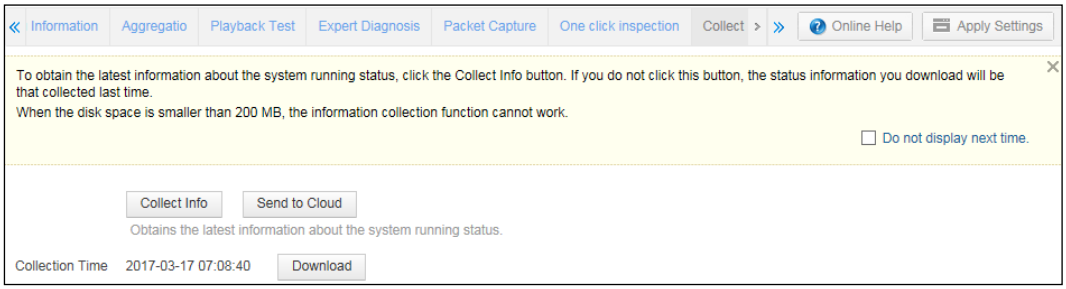
Figure 4-39 Message indicating the successful collection



Step 3 Click **OK**.

The page then displays the time when system running status information is collected, as shown in Figure 4-40.

Figure 4-40 Display of collection time



Step 4 Click **Download** to download the system running status information to a local disk drive for future reference and analysis.

Step 5 Click **Send to Cloud** to send the collected information about the device running status to ESPP.

----End

4.6.12 Debugging Information

Choose **System** > **Diagnostic Tools** > **Debugging Info**. On the **Debugging Info** page, you can turn on the debug switch and then specify which level of messages to be logged by each functional module. You can download debug logs to a local disk drive.

This function can be used only by NSFOCUS engineers for network debugging. Users are advised to ignore it.

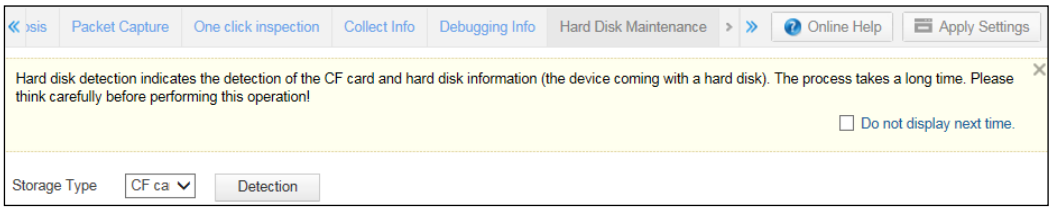
4.6.13 Hard Disk Maintenance

The **Hard Disk Maintenance** tab page allows you to check CF card information. If the device has a hard disk, NIPS can also check hard disk information.

Note	It takes a long time to check hard disk maintenance information. Please use this function with caution.

Step 1 Choose System > Diagnostic Tools > Hard Disk Maintenance.

Figure 4-41 Hard Disk Maintenance page



Step 2 Select a hardware type from the drop-down list for **Storage Type**.

- If the device does not have a hard disk, only **CF card** is available in the drop-down list.
- If the device has a hard disk, **CF card** and **Hard disk** are available in the drop-down list.

Figure 4-42 Hard Disk Maintenance page – device with a hard disk

Step 3 Click **Detection**.

The hardware detection result is displayed.

----End

4.7 License Management

NIPS licenses are classified into two types:

- Trial license

  A trial license is usually used for pre-sales tests. Based on the update time of the engine software, after a trial license expires, users cannot log in to the web-based manager of NIPS to continue using the security detection function.

- Paid license

  A paid license is mainly used for controlling upgrade services during the authorized time period.

- After the engine software update expires, the update page automatically disappears. In this case, neither the engine software nor various libraries can be updated.
- When the engine software is still valid, other libraries (such as the system rule library, URL category library, and virus database) cannot be updated after they expire.

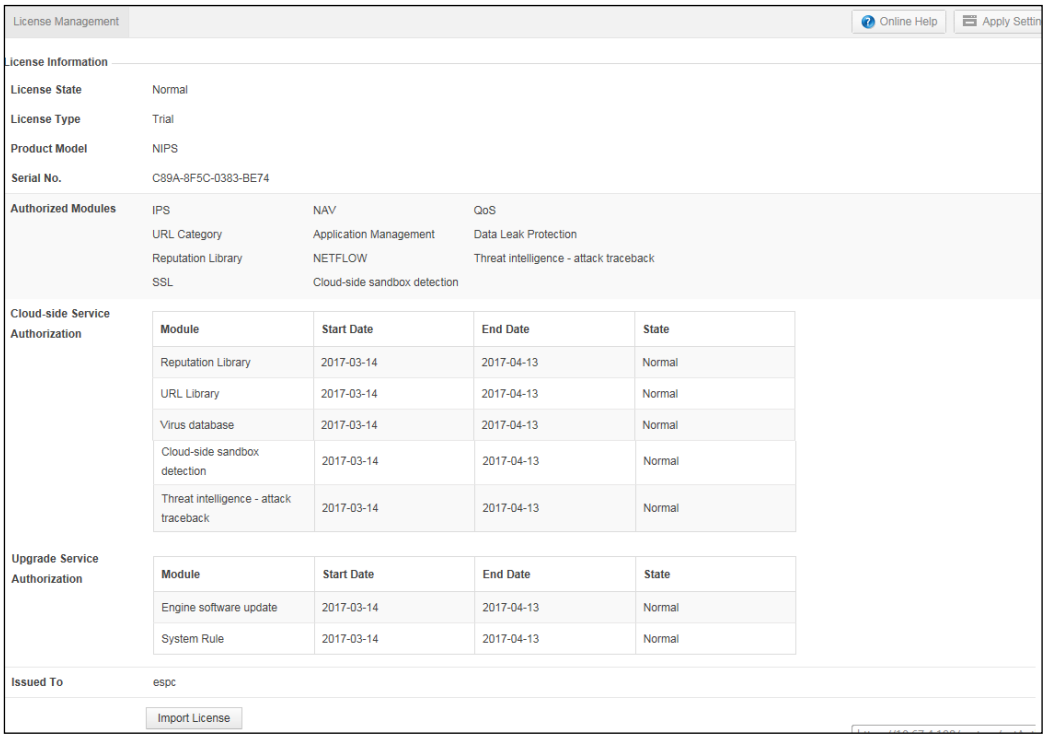
  After a paid license expires, other libraries of earlier versions remain valid, users can still use the security detection function and view logs.

4.7.1 Viewing License Status

The **License Management** page displays functional modules provided by NIPS and the period when NIPS can be used.

Step 1 Choose **System > License Management**.

Figure 4-43 License status



Step 2 View license information.

Table 4-11 Parameters on the License Management page

Parameter	Description
License State	Indicates the license status. • **Normal**: indicates that a valid license has been imported and the system can be used. • **Expired**: indicates that the license has expired.
License Type	Indicates the type of the license imported in NIPS. It has the following values: • **Trial**: After this type of license expires, users cannot continue to use NIPS.

Parameter	Description
	• **Paid**: After this type of license expires, users can still use NIPS, but cannot update it.
Product Model	Indicates the product model covered by this license.
Serial No.	Serial number of the license.
Authorized Modules	Indicates functional modules provided by NIPS according to this license. Authorized modules can be used even if the upgrade service expires. However, the working of modules depends heavily on various libraries. If these libraries cannot be updated due to the expiration of the upgrade service, modular functions will be affected.
Upgrade Service Authorization	Indicates the start date, end date, and status of the upgrade service authorized for the purchased modules. Indicates the start date and end date of the upgrade service authorization time during which NIPS can upgrade various libraries and software. Within the authorized period specified with **Start Date** and **End Date**, the upgrade service authorization time during which NIPS can be properly updated. • **Engine software update**: indicates the authorized service period and status of the device engine. • **System Rule**: the authorized service period and status of intrusion prevention rules, application rules, and sensitive data rules. • **URL Library**: indicates the authorized service period and status of URL category rules. • **Virus database**: indicates the authorized service period and status of the virus database. If the current system time is beyond the authorized service period, the system cannot update services, but libraries of earlier versions remain valid. Note Within 30 days before the license expires, NIPS displays a notification, prompting users to update the license. After the license expires, NIPS notifies users of the expiration.
Unauthorized Modules	Indicates functional modules provided by NIPS but not covered by this license.
Issued To	Indicates users that are entitled to use this NIPS.

----End

4.7.2 Importing the License

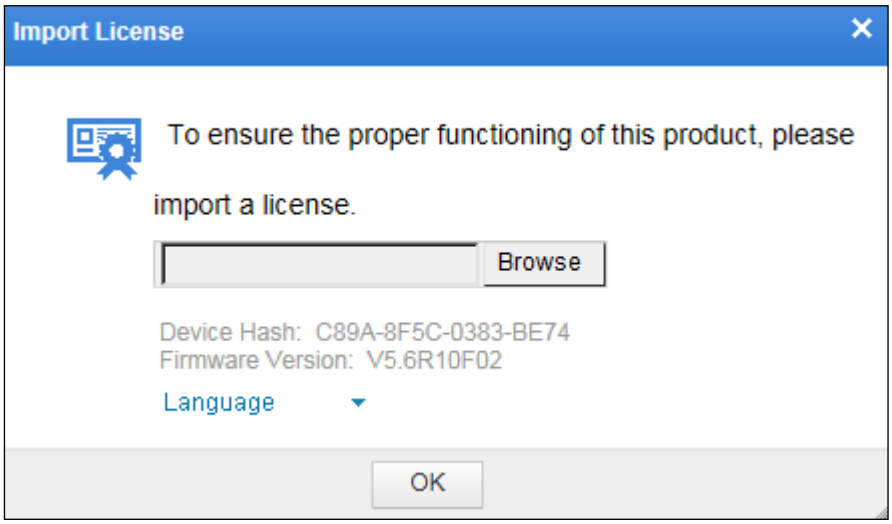
During the first login, you must import the license; otherwise, you cannot use NIPS.

To import the license, follow these steps:

Step 1 Choose **System** > **License Management**.

Step 2 Click **Import License**.

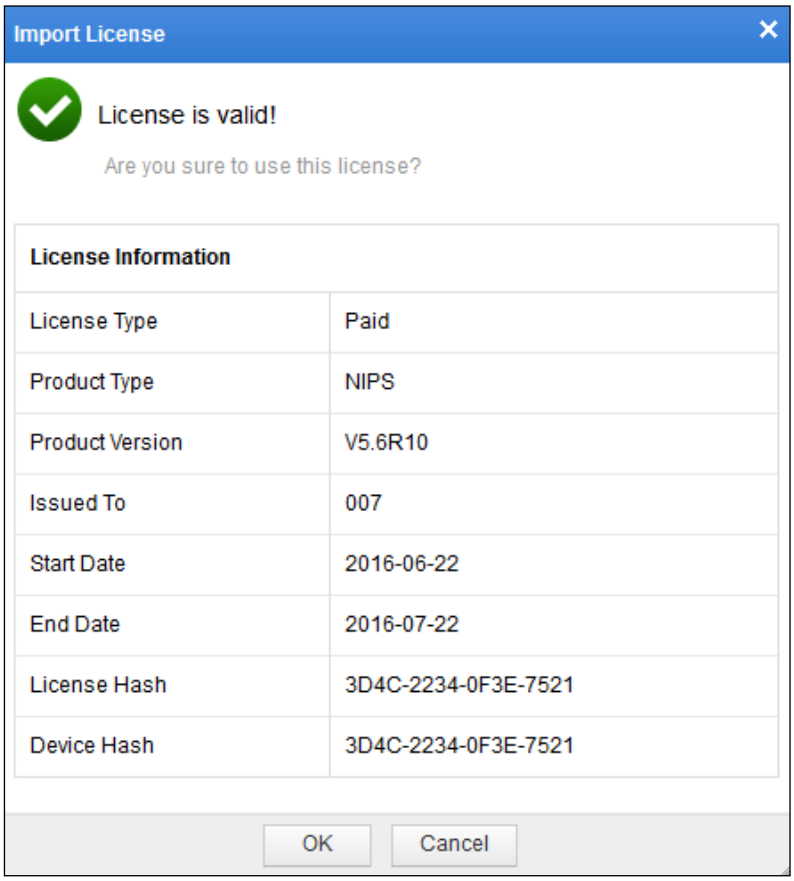
Figure 4-44 Importing the license



Step 3 Click **Browse**, select the license file (*.lic), and click **Open**.

A dialog box appears, as shown in Figure 4-45, asking you to confirm your operation.

Figure 4-45 Dialog box for confirming license import



Step 4 Determine whether to import the license.

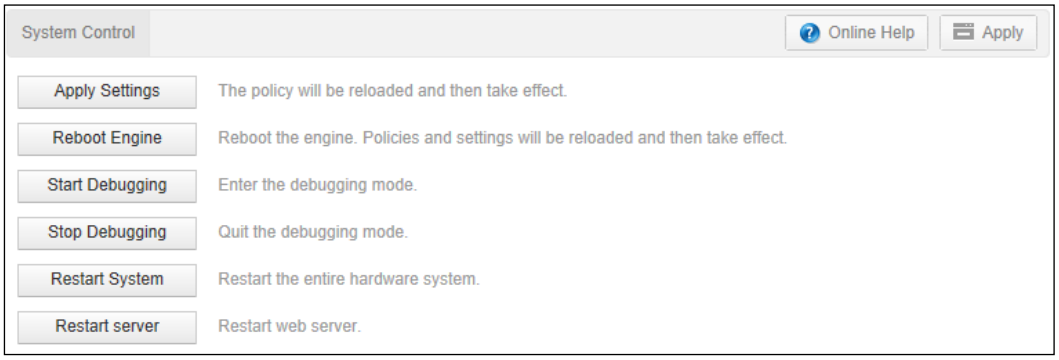
- If license information is correct, click **OK** to complete the import. The license then takes effect immediately.
- If license information is incorrect, click **Cancel** and repeat the preceding steps.

----End

4.8 System Control

Choose **System** > **System Control**.

Figure 4-46 System control



On the **System Control** page, you can perform the following system control operations:

- Apply settings.

  Click **Apply Settings** to reload all policies and engine settings, except interface settings, and make them take effect immediately. Policies reloaded include intrusion prevention policies, data leak protection policies, web reputation policies, URL category filtering policies, antivirus policies, user management policies, traffic management policies, and application management policies.
- Reboot the engine.

  Click **Reboot Engine** to restart the engine. All policies and engine settings, including interface settings, will be reloaded and take effect immediately.
- Start debugging.

  Click **Start Debugging** to start network debugging. This operation can be performed only by technical support engineers of NSFOCUS for network debugging.
- Stop debugging.

  Click **Stop Debugging** to stop network debugging. This operation can be performed only by technical support engineers of NSFOCUS during network debugging.
- Restart the system.

  Click **Restart System** to restart the hardware system of NIPS.
- Restart services.

  Click **Restart server** to restart the web server.

Caution	After the system is restarted, all report data is cleared, and the system starts collecting new statistics.

5 Network

The Network module enables you to configure network connectivity information such as interfaces, security zones, and routes within the network. This chapter describes the Network module from the following aspects:

Section	Description
Interface	Describes how to configure NIPS interfaces.
Security Zone	Describes how to configure security zones.
Virtual Wire	Describes the virtual wire and how to configure a virtual wire.
Switch	Describes data exchange protocols and how to configure such a protocol.
DHCP	Describes how to configure NIPS as a DHCP server and DHCP relay.
DNS	Describes how to configure the domain name system.
IP/MAC Binding	Describes how to configure IP-to-MAC binding.
Route	Describes how to configure static routes.
Network Management	Describes how to configure NIPS as an SNMP agent and to send trap messages, and how to configure basic functions of SNMP and the syslog server.
High Availability	Describes how to configure the high availability feature.
Others	Describes how to configure NIPS to work in external bypass or built-in bypass mode.

Note	NIPS NX5-T9010A and NX5-T9020A do not support the following functions: • Virtual wire configuration · Switch configuration • DHCP configuration • Policy-based route configuration · ARP table configuration • Logical interface configuration • Manageable attribute configuration

5.1 Interface

An interface is a shared boundary or connection between devices for data exchange. This section describes interface types, interface attribute, and interface configuration.

5.1.1 Interface Types

Interfaces of NIPS are divided physical interfaces and logical interfaces.

Note	NIPS NX5-T9010A and NX5-T9020A have only physical interfaces.

Physical Interfaces

On NIPS, physical interfaces include the following:

- Out-of-band management interface

  The out-of-band management interface is used for device management. It only transmits management and control information, but not forwards service traffic. Separating the management traffic from service traffic enhances the security of device management and guarantees the stability of the management bandwidth.

  NIPS provides out-of-band management interfaces M and H1. Out-of-band management interfaces enable the administrator to manage the NIPS device via HTTPS and SSH and access such interfaces from other devices by using the ping command.
- Ethernet interface

  The names of Ethernet interfaces are predefined, including G interfaces (Gigabit interfaces, such as G1/1 and G1/2), and T interfaces (10 Gb interfaces such as T1/1 and T1/2).

Logical Interface

Logical interfaces are created based on Ethernet interfaces, including the following:

- Aggregation interface

  NIPS adopts IEEE 802.3ad for link aggregation, allowing the administrator to bind multiple Ethernet interfaces that are configured as member interfaces to the specified aggregation interface. Aggregation interfaces can increase the bandwidth and improve fault tolerance.
- Loopback interface

  Loopback interfaces are layer 3 logical interfaces and do not need to be bound to any physical interface. Therefore, the link status of loopback interfaces is not impacted by any factors. The administrator can learn about the device status according to link status of the loopback interface. In addition, loopback interfaces can be applied to the following scenarios:

  - The administrator can manage the NIPS device through the IP address of the loopback interface.

- The loopback interface can be used as a virtual IP address in a Network Address Translation (NAT) policy.

- Layer 3 subinterface

  When a layer 3 Ethernet interface needs to identify VLAN packets, you need to configure layer 3 subinterfaces based on this layer 3 Ethernet interface. Therefore, packets from different VLANs can be forwarded through different subinterfaces.

  A maximum of 512 subinterfaces can be configured for a layer 3 interface. Whether a subinterface is up or down depends on its parent interface.

- VLAN interface

  VLAN interfaces are layer 3 logical interfaces created based on layer 2 physical interfaces.

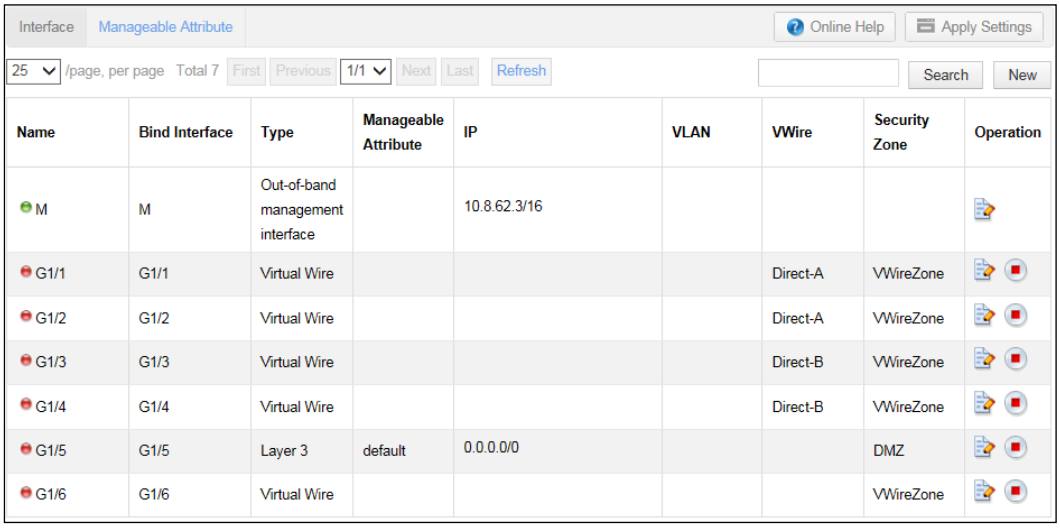
  For layer 2 Ethernet interfaces, the administrator can define a VLAN interface for forwarding data between different VLANs.

5.1.2 Interface Configuration

NIPS devices of all models have physical interfaces. The administrator can edit physical interface settings. All NIPS devices except NX5-T9010A and NX5-T9020A support logical interfaces. The administrator can create and edit logical interfaces.

Choose **Network** > **Interface**. The **Interface** page varies with models of NIPS devices.Figure 5-1 shows the **Interface** page of device models other than NX5-T9010A and NX5-T9020A.

Figure 5-1 Interface page of device models other than NX5-T9010A and NX5-T9020A



Name	Bind Interface	Type	Manageable Attribute	IP	VLAN	VWire	Security Zone	Operation
M	M	Out-of-band management interface		10.8.62.3/16				
G1/1	G1/1	Virtual Wire				Direct-A	VWireZone	
G1/2	G1/2	Virtual Wire				Direct-A	VWireZone	
G1/3	G1/3	Virtual Wire				Direct-B	VWireZone	
G1/4	G1/4	Virtual Wire				Direct-B	VWireZone	
G1/5	G1/5	Layer 3	default	0.0.0.0/0			DMZ	
G1/6	G1/6	Virtual Wire					VWireZone	

- Figure 5-2 shows the **Interface** page of NX5-T9010A and NX5-T9020A.

Figure 5-2 Interface page of NX5-T9010A and NX5-T9020A

Interface | Online Help | Apply Settings

Interface	Interface Type	Medium Type	Manageable	Interface IP	Subnet Mask	Gateway IP	Duplex	Connection Rate (Mbps)	Security Zone	Operation
M	Electrical	Copper	Yes	10.67.4.10	255.255.0.0	192.168.1.1	auto	auto	Management	
H1	Electrical	Copper	Yes	192.168.2.1	255.255.255.0	192.168.2.1	auto	auto	Management	
G1/1	Electrical	Copper	Yes	0.0.0.0	0.0.0.0	0.0.0.0	auto	auto	Direct-A	
G1/2	Electrical	Copper	Yes	0.0.0.0	0.0.0.0	0.0.0.0	auto	auto	Direct-A	
G1/3	Electrical	Copper	Yes	0.0.0.0	0.0.0.0	0.0.0.0	auto	auto	Direct-B	
G1/4	Electrical	Copper	Yes	0.0.0.0	0.0.0.0	0.0.0.0	auto	auto	Direct-B	
G2/1	1000M optical	Fiber	Yes	111.111.1.2	255.255.0.0	0.0.0.0	auto	auto	Management	
G2/2	1000M optical	Fiber	Yes	0.0.0.0	0.0.0.0	0.0.0.0	auto	auto	Direct-C	
G2/3	1000M optical	Fiber	Yes	0.0.0.0	0.0.0.0	0.0.0.0	auto	auto	Direct-D	
G2/4	1000M optical	Fiber	Yes	0.0.0.0	0.0.0.0	0.0.0.0	auto	auto	Direct-D	
T3/1	10G optical	Fiber	Yes	0.0.0.0	0.0.0.0	0.0.0.0	auto	auto	Direct-E	
T3/2	10G optical	Fiber	Yes	0.0.0.0	0.0.0.0	0.0.0.0	auto	auto	Direct-E	

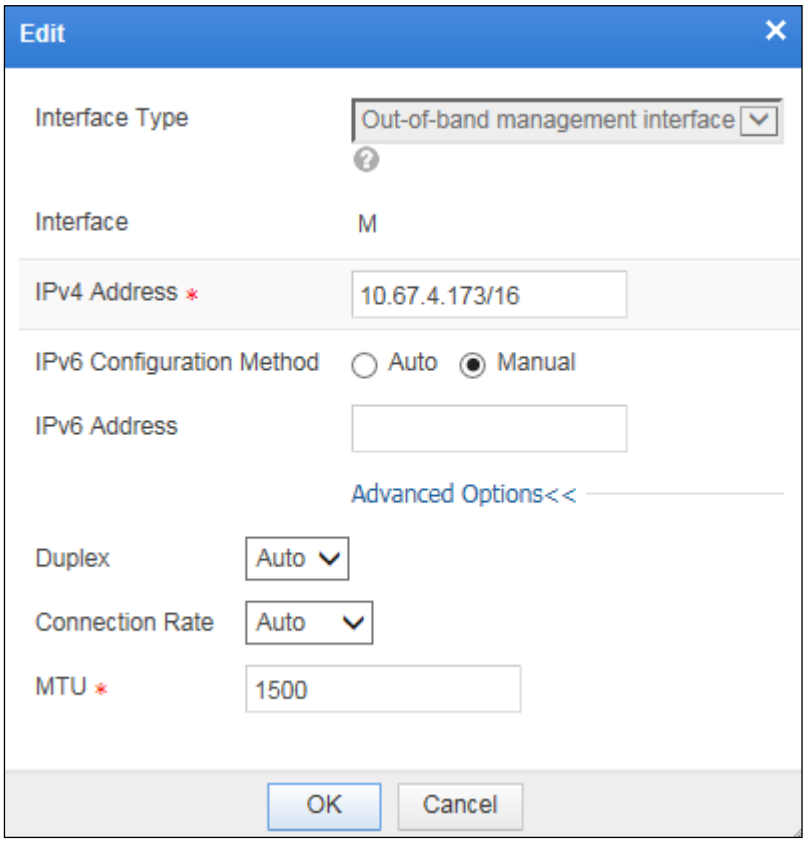
The following describes how to configure interfaces on NIPS.

5.1.2.1 Editing an Out-of-Band Management Interface

Step 1 On the page shown in Figure 5-1, click in the **Operation** column of interface M.Parameters displayed in the **Edit** dialog box vary with device models.

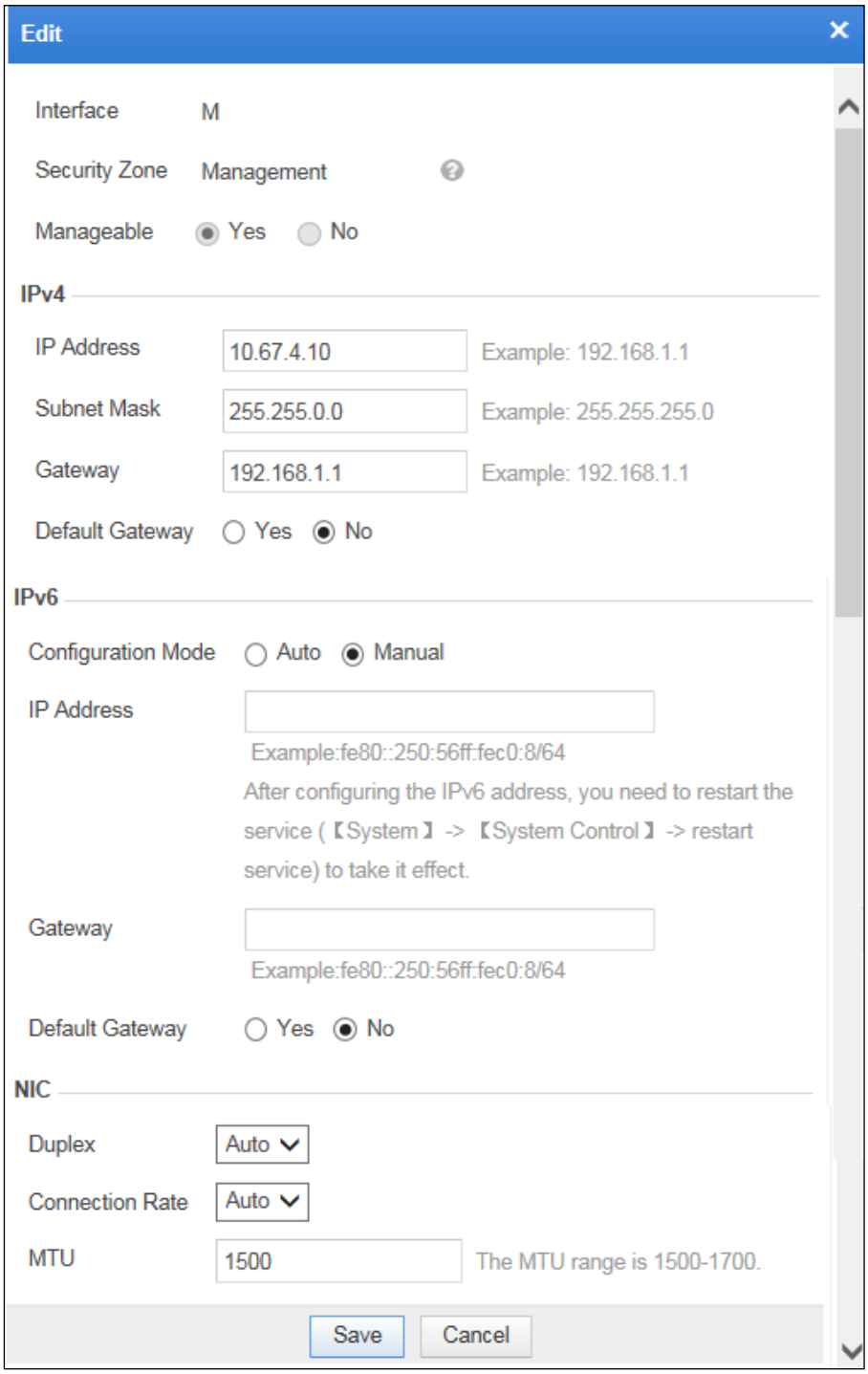
- Figure 5-3 shows the **Edit** dialog box for configuring an out-of-band management interface on device models other than NX5-T9010A and NX5-T9020A.

Figure 5-3 Configuring interface M for device models other than NX5-T9010A and NX5-T9020A



- Figure 5-4 shows the **Edit** dialog box for configuring an out-of-band management interface on NX5-T9010A and NX5-T9020A.

Figure 5-4 Configuring interface M for NX5-T9010A and NX5-T9020A



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

Table 5-1 Parameters for configuring interface M

Parameter	Description
IPv4 Address	Specifies the IP address of the out-of-band management interface. The format should be IP address/netmask length. Note For NX5-T9010A and NX5-T9020A, you can also configure the IPv4 gateway, so that interface M is accessible on the network.
IPv6 Address	Specifies the IPv6 address of the out-of-band management interface, which can be automatically obtained or manually configured. Note For NX5-T9010A and NX5-T9020A, you can also configure the IPv6 gateway, so that interface M is accessible on the network.
Duplex	Specifies the duplex mode of the interface, which can be **Full**, **Half**, or **Auto**. **Full**: transmits data in two directions (sends and receives data) at a time. **Half**: transmits data in just one direction (either sends or receives data) at a time. **Auto**: transmits data according to the actual duplex mode.
Connection Rate	Specifies the data transmission rate, which can be **10M**, **100M**, **1000M**, or **Auto**. **Auto** indicates that NIPS automatically adjusts the data transmission rate of the interface.
MTU	Specifies the maximum transmission unit, which should be in the range of 128 to 1600 bytes. The default value is **1500**. The MTU of the layer 3 interface applies only to packets of the egress interface. That is, when the packet length is greater than the MTU of the layer 3 interface, fragmentation will be performed on the egress interface. Note When the IPv6 address is used, the minimum value of MTU is 1280.

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

Step 2 Apply the settings.

----End

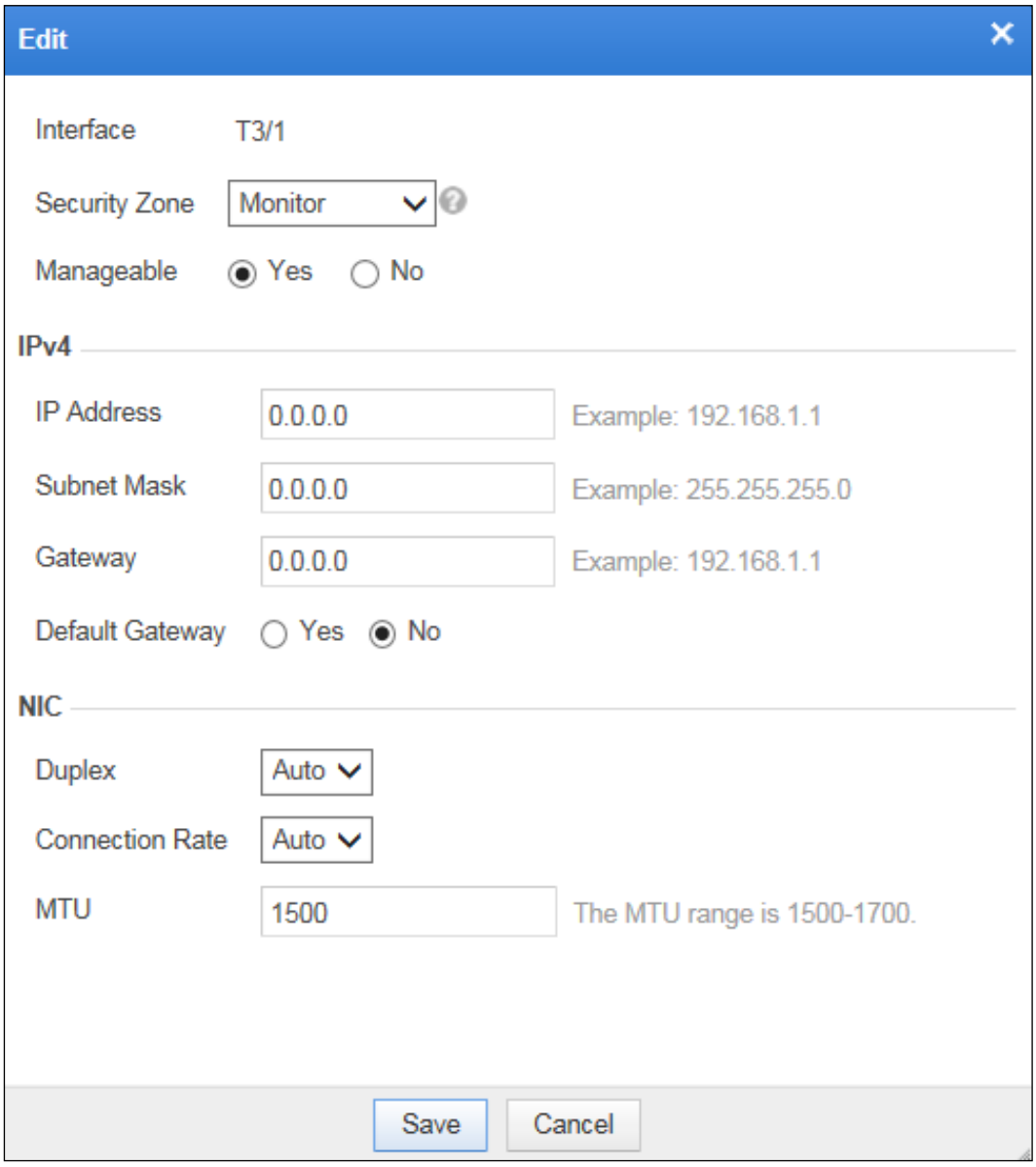
5.1.2.2 Editing an Ethernet Interface

In the interface list, click in the **Operation** column of an Ethernet interface and then configure parameters in the **Edit** dialog box.

Ethernet interface configuration varies with device models.

- Figure 5-5 shows the dialog box for editing an Ethernet interface for NX5-T9010A and NX5-T9020A.

Figure 5-5 Dialog box for editing an Ethernet interface for NX5-T9010A and NX5-T9020A



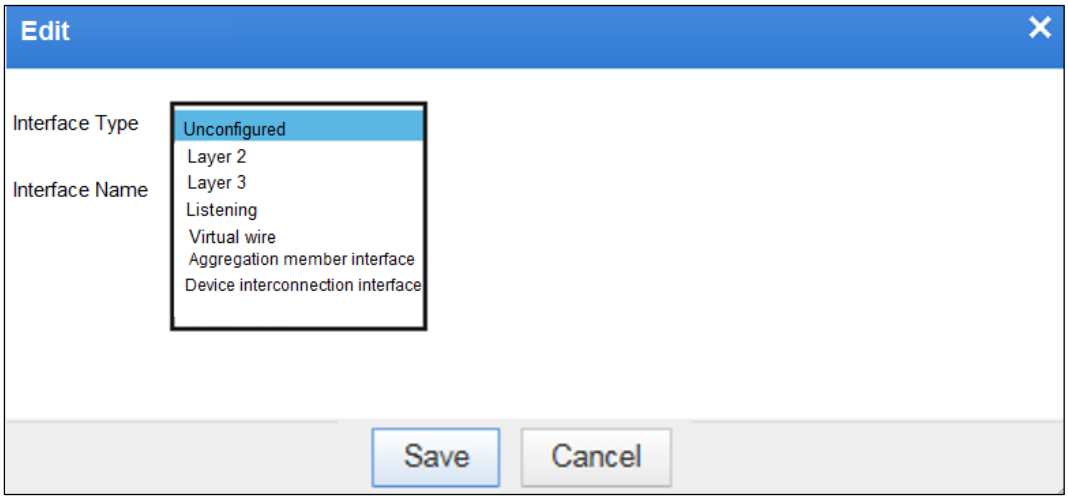
The interface type depends on the security zone that the interface belongs to.

- If **Security Zone** is set to **Monitor**, the Ethernet interface is a monitoring interface which connects to the switch for traffic monitoring.
- If **Security Zone** is set to **Direct**, the Ethernet interface is a direct interface which connects two interfaces in the same security zone for data communication. These two interfaces respectively work as an IN and OUT interface.
- If **Security Zone** is set to **Interconnect**, the Ethernet interface is a device interconnection interface. For how to configure a device interconnection interface, see Configuring a Device Interconnection Interface.
- If **Security Zone** is set to **Management**, the Ethernet interface is a management interface. For the description of M interface parameters, see Table 5-2.

Note	• You must configure security zones in advance. For details, see section 5.2 Security Zone. • You need to configure **IP Address** and **Gateway** only when **Manageable** is set to **Yes**. In this case, this Ethernet interface can be used as a management interface. When **Manageable** is set to **No**, leave parameters at their default values.

- For device models other than NX5-T9010A and NX5-T9020A: By default, the Ethernet interface type is **Unconfigured**. Figure 5-6 shows the dialog box for editing an Ethernet interface for device models other than NX5-T9010A and NX5-T9020A.

Figure 5-6 Dialog box for editing an Ethernet interface for device models other than NX5-T9010A and NX5-T9020A



For device models other than NX5-T9010A and NX5-T9020A, Ethernet working interfaces are divided into the following:

- Layer 2 interfaceLayer 2 interfaces do not have IP addresses. Layer 2 interfaces can be used only for forwarding Ethernet frames. Generally, layer 2 interfaces connect to a layer 2 switch.
- Layer 3 interfaceIP addresses can be assigned to layer 3 interfaces. Layer 3 interfaces can be used unnecessary for data transmission based on static and dynamic routing protocols. Generally, layer 3 interfaces connect to a layer 3 switch or router.
- Listening interface

  After the listening interface is configured and connects to the listening port of a switch, traffic monitoring can be performed.
- Virtual wire interface

  After a pair of Ethernet interfaces are configured as virtual wire interfaces, these two interfaces can be connected as a virtual channel for data communication. For how to configure the virtual wire, see section 5.3 Virtual Wire.
- Aggregation member interface

  After multiple interfaces are configured as aggregation member interfaces, they can be aggregated as one interface. For how to configure aggregation interfaces, see section 5.1.2.3 Creating an Aggregation Interface.

- Device interconnection interface

  Device interconnection interfaces are used in the scenario where an asymmetric routing is configured to divert traffic to the host, thereby guaranteeing the integrity of sessions.

All Ethernet interface can be enabled or disabled. Disabled interfaces do not send or receive packets. The icon in the **Operation** column of an interface indicates that the interface has been enabled. You can click this icon to disable it. Then the icon turns to . Clicking this icon will enable the interface again.

Configuring a Layer 2 Interface

Layer 2 interfaces of NIPS can work in the following modes:

- Access mode

  The interface working in access mode is used to connect to terminal users and can belong only to one VLAN. That is, such interface only allows packets from one VLAN to pass through.

- Trunk mode

  The interface working in trunk mode is used to connect switching devices. That is, such interface allows packets form multiple VLANs to pass through.

  After receiving a packet via the trunk interface, it checks whether the packet contains VLAN information.

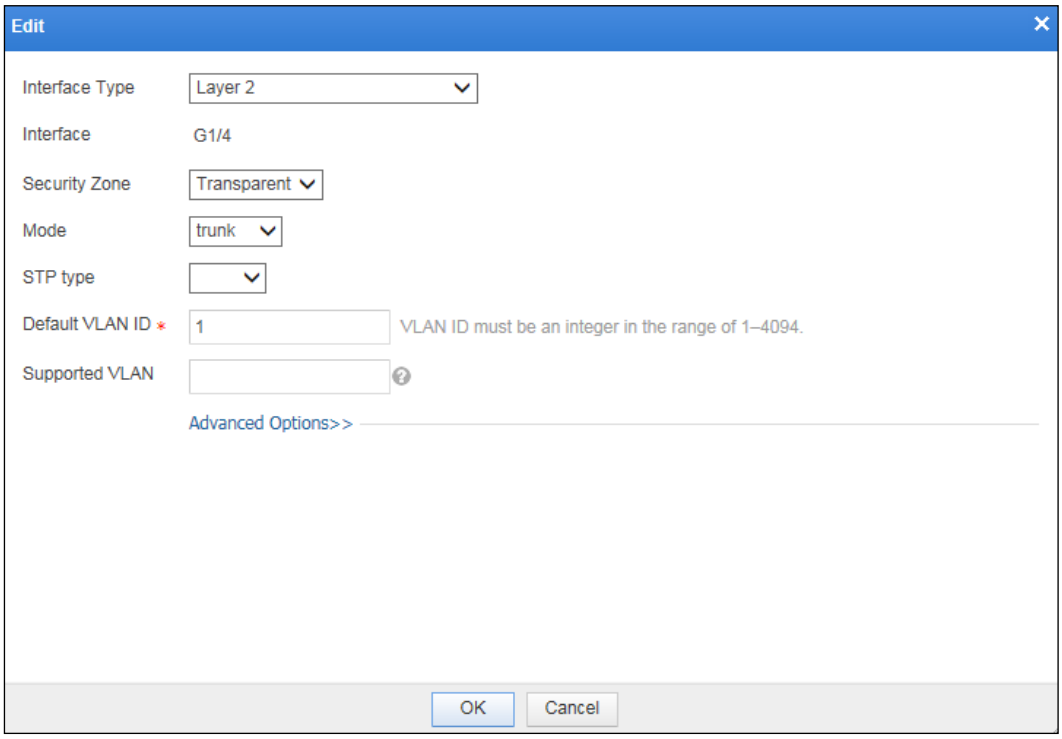
  - If no, NIPS forwards the packet using the configured **Default VLAN ID**.
  - If yes, NIPS checks whether the trunk interface allows VLAN data to pass through, which depends on whether the packet's VLAN ID belongs to the range specified in **Supported VLAN**. If yes, NIPS forwards the packet. Otherwise, NIPS drops the packet.

Before sending packets via the trunk interface, NIPS compares VLAN tag contained in the packets to be sent with the configured **Default VLAN ID**. If they are the same, NIPS removes the VLAN tag and then sends the packets. If they are different, NIPS directly forwards the packets.

To configure a layer 2 Ethernet interface, follow these steps:

Step 1 On the page shown in Figure 5-1, click in the **Operation** column of an interface and then set **Interface Type** to **Layer 2** in the **Edit** dialog box.

Figure 5-7 Configuring a layer 2 interface



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

Table 5-2 Parameters for configuring a layer 2 interface

Parameter	Description
Interface Type	Specifies the type of the interface, which should be set to **Layer 2**.
Interface Name	Indicates the default interface name, which cannot be edited.
Security Zone	Specifies the working mode of the security zone which the interface belongs to. A layer 2 interface can work only in a layer 2 security zone. You can select a layer 2 security zone from the drop-down list.
Mode	Specifies the work mode of the interface, which can be **access** or **trunk**.
STP type	Specifies the type of the Spanning Tree Protocol (STP) for the forwarding port. If STP is not used, you do not need to configure this parameter. • **rstp**: indicates that the Rapid Spanning Tree Protocol (RSTP) is used. • **mstp**: indicates that Multi Spanning Tree Protocol (MSTP) is used.
Default VLAN ID	This parameter is available only when **Mode** is set to **trunk**. When the interface receives packets with no VLAN tag, the system will automatically add the default VLAN tag. When the interface sends a packet with a VLAN tag, if the VLAN ID is the same as that of the default one, the system will send the packet after removing its VLAN tag.
Supported VLAN	This parameter is available only when **Mode** is set to **trunk**. Specifies VLAN IDs that are allowed. Multiple VLAN IDs should be separated by comma (,) and consecutive VLAN IDs

Parameter	Description
	should be separated by a hyphen (-). For example, you can configure "1,2,4" and "2-5".

Step 3 Configure advanced parameters.

Figure 5-8 Advanced Options area

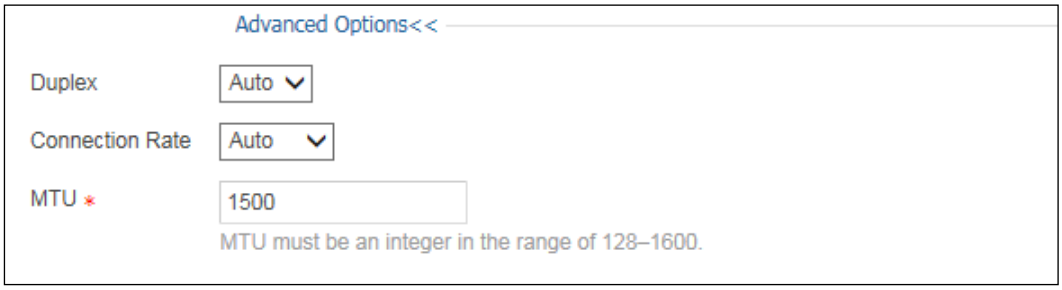


Table 5-3 Advanced parameters for configuring a layer 2 interface

Parameter	Description
Duplex	Specifies the duplex mode of the interface, which can be **Full**, **Half**, or **Auto**. • **Full**: transmits data in two directions (sends and receives data) at a time. • **Half**: transmits data in just one direction (either sends or receives data) at a time. • **Auto**: transmits data according to the actual duplex mode.
Connection Rate	Specifies the data transmission rate, which can be **10M**, **100M**, **1000M**, or **Auto**. **Auto** indicates that NIPS automatically adjusts the data transmission rate of the interface.
MTU	Specifies the maximum transmission unit, which should be in the range of 128 to 1600 bytes. The default value is **1500**. The MTU of the layer 2 interface applies only to packets of the egress interface. That is, when the packet length is greater than the MTU of the layer 2 interface, fragmentation will be performed on the egress interface.

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

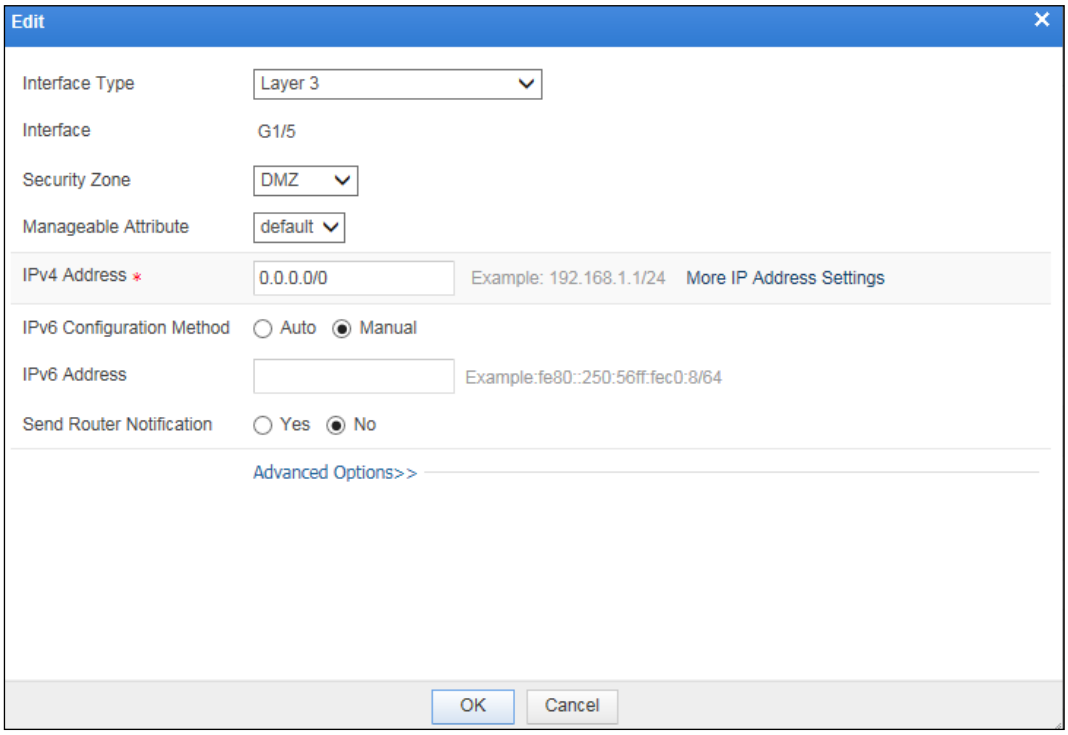
Step 4 Apply the settings.

----End

Configuring a Layer 3 Interface

Step 1 On the page shown in Figure 5-1, click in the **Operation** column of an interface and then set **Interface Type** to **Layer 3** in the **Edit** dialog box.

Figure 5-9 Configuring a layer 3 interface



Step 5 Configure parameters in the **Edit** dialog box.

Table 5-4 Parameters for configuring a layer 3 interface

Parameter	Description
Interface Type	Specifies the type of the interface, which should be set to **Layer 3**.
Interface Name	Indicates the default interface name, which cannot be edited.
Security Zone	Specifies the working mode of the security zone which the interface belongs to. A layer 3 interface can work only in a layer 3 security zone. You can select a layer 3 security zone from the drop-down list.
Manageable Attribute	You can leave it at the default value: **default**.
IPv4 Address	Specifies the IPv4 address of the interface. You can configure multiple IPv4 addresses for a layer 3 interface. Clicking **More IP Address Settings** displays the dialog box for configuring multiple IP addresses. **Note** The interface supports a maximum of 32 IP addresses. You cannot configure multiple addresses when **IPv4 Address** is set to **0.0.0.0/***.
IPv6 Configuration Method	Specifies how to configure the IPv6 address, which can be **Auto obtain** or **Manual configuration**. The default value is **Manual configuration**.
IPv6 Address	This parameter is available only when **IPv6 Configuration Method** is set to **Manual configuration**.

Parameter	Description
Send Router Advertisement	Controls whether to periodically send neighbors a router advertisement packet that announces its availability. If the interface needs to assign IP addresses to the device it connects, **Send Router Advertisement** should be set to **Yes**.

Step 2 Configure advanced parameters.

Figure 5-10 Advanced Options area

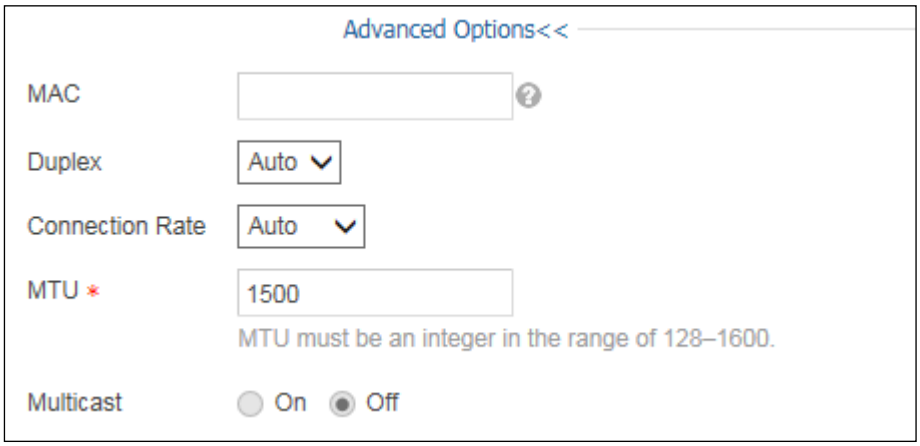


Table 5-5 Advanced parameters for configuring a layer 3 interface

Parameter	Description
MAC	Specifies the MAC address of the interface. Only MAC addresses that are manually configured are displayed here.
Duplex	Specifies the duplex mode of the interface, which can be **Full**, **Half**, or **Auto**. • **Full**: transmits data in two directions (sends and receives data) at a time. • **Half**: transmits data in just one direction (either sends or receives data) at a time. • **Auto**: transmits data according to the actual duplex mode.
Connection Rate	Specifies the data transmission rate, which can be **10M**, **100M**, **1000M**, or **Auto**. **Auto** indicates that NIPS automatically adjusts the data transmission rate of the interface.
MTU	Specifies the maximum transmission unit, which should be in the range of 128 to 1600 bytes. The default value is **1500**. The MTU of the layer 2 interface applies only to packets of the egress interface. That is, when the packet length is greater than the MTU of the layer 2 interface, fragment reassembly will be performed on the egress interface.
Multicast	Controls whether to enable the multicast packet forward function. By default, **Multicast** is set to **Off**. After multicast is enabled, it applies only to the primary IP address though multiple IPv4 addresses are configured.

Step 6 Click **OK** to complete the configuration.

Step 3 Apply the settings.

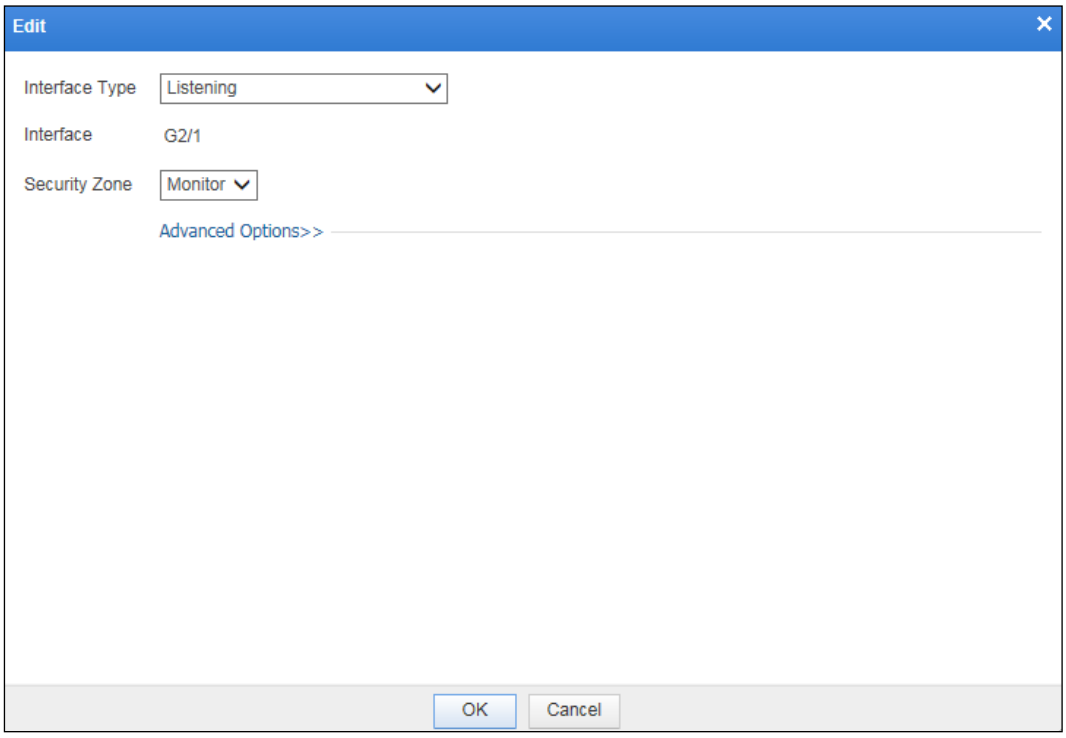
----End

Configure a Listening Interface

After the listening interface is configured and connects to the listening port of the switch, traffic monitoring can be performed. After reading the packet capture file through a listening interface, NIPS can play back the data in a playback test, helping users analyze network data. For details about playback test, see section 4.6.7 Playback Test.

Step 1 On the page shown in Figure 5-1, click in the **Operation** column of an interface and then set **Interface Type** to **Listening** in the **Edit** dialog box.

Figure 5-11 Configure a listening interface



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

Note	A listening interface can work only in a "monitor" security zone. You can select a "Monitor" zone from the drop-down list of **Security Zone**.

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

Step 2 Apply the settings.

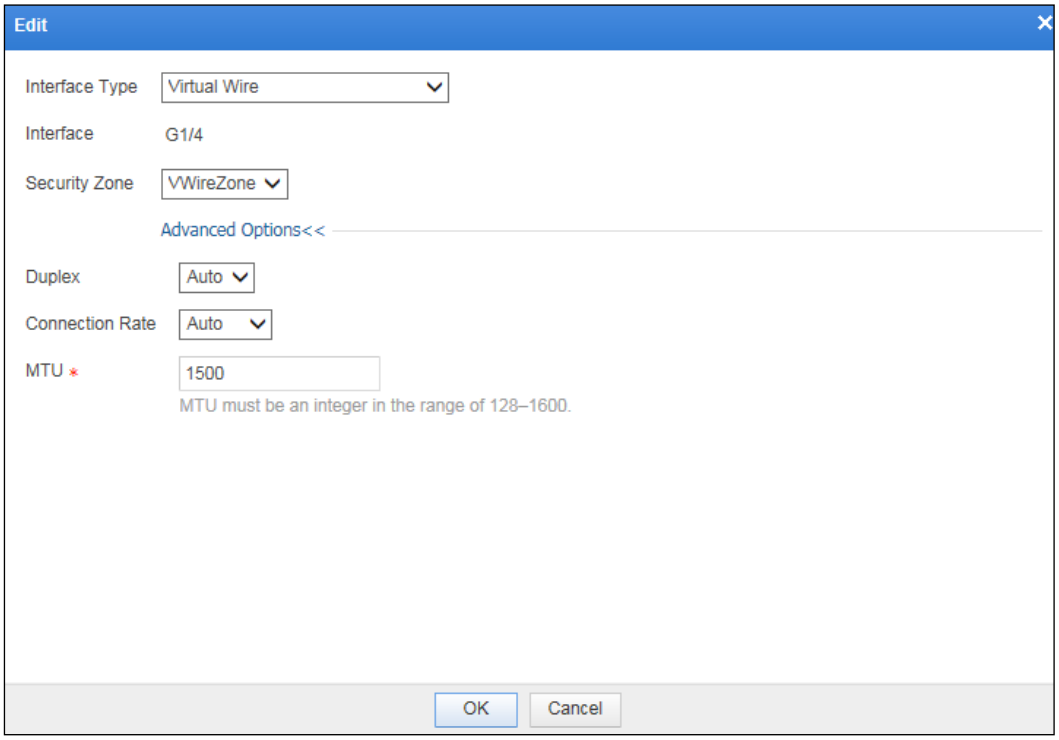
----End

Configuring a Virtual Wire Interface

After a pair of Ethernet interfaces are configured as virtual wire interfaces, these two interfaces can be connected as a virtual channel for data communication. Before configuring a virtual wire interface, you need to create a virtual wire first. For how to configure a virtual wire, see section 5.3 Virtual Wire.

Step 1 On the page shown in Figure 5-1, click in the **Operation** column of an interface and then set **Interface Type** to **Virtual Wire** in the **Edit** dialog box.

Figure 5-12 Configuring a virtual wire interface



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

Table 5-6 Parameters for configuring a virtual wire interface

Parameter	Description
Interface Type	Specifies the type of the interface, which should be set to **Virtual Wire**.
Interface Name	Indicates the default interface name, which cannot be edited.
Security Zone	A virtual wire interface can work only in a virtual wire security zone. You can select a v-wire zone from the drop-down list of **Security Zone**.
Duplex	Specifies the duplex mode of the interface, which can be **Full**, **Half**, or **Auto**. • **Full**: transmits data in two directions (sends and receives data) at a time. • **Half**: transmits data in just one direction (either sends or receives data) at a time. **Auto**: transmits data according to the actual duplex mode.
Connection Rate	Specifies the data transmission rate, which can be **10M**, **100M**, **1000M**, or **Auto**. **Auto**

Parameter	Description
	indicates that NIPS automatically adjusts the data transmission rate of the interface.
MTU	Specifies the maximum transmission unit, which should be in the range of 128 to 1600 bytes. The default value is **1500**. The MTU of the layer 2 interface applies only to packets of the egress interface. That is, when the packet length is greater than the MTU of the layer 2 interface, fragment reassembly will be performed on the egress interface.

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

Step 4 Apply the settings.

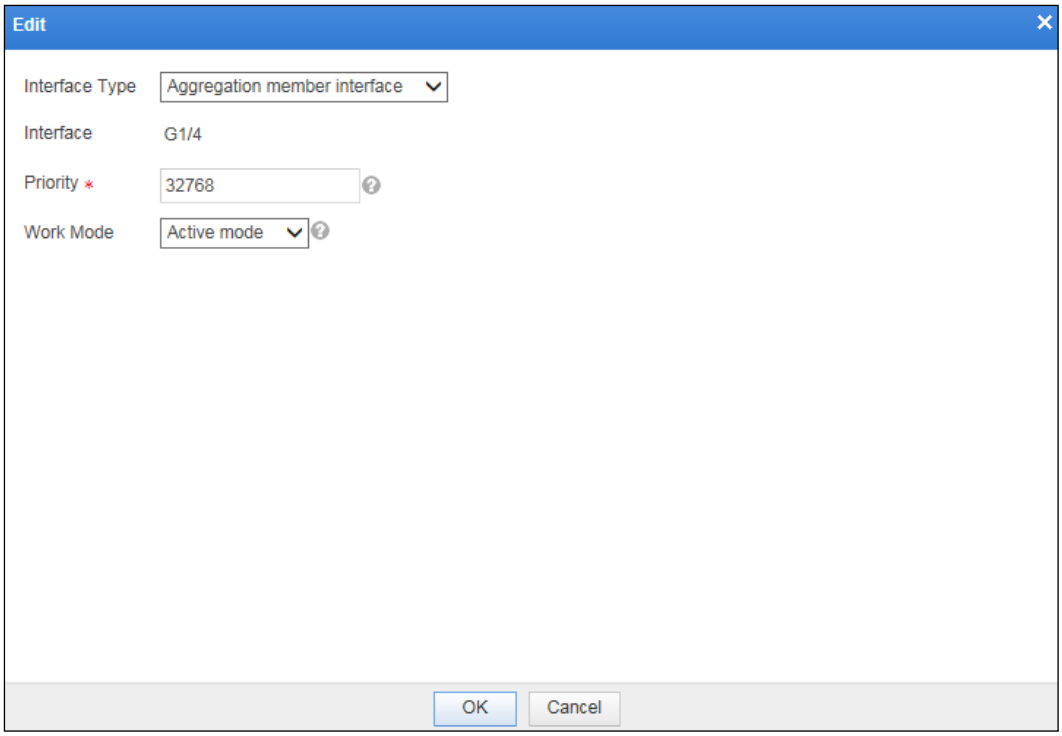
----End

Configuring an Aggregation Member Interface

After multiple interfaces are configured as aggregation member interfaces, such aggregation member interfaces can be aggregated as one interface. For how to configure aggregation interfaces, see section 5.1.2.3 Creating an Aggregation Interface.

Step 1 On the page shown in Figure 5-1, click in the **Operation** column of an interface and then set **Interface Type** to **Aggregation member interface** in the **Edit** dialog box.

Figure 5-13 Configuring an aggregation member interface



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

Table 5-7 Parameters for configuring an aggregation member interface

Parameter	Description
Interface Type	Specifies the type of the interface, which should be set to **Aggregation member interface**.
Interface Name	Indicates the default interface name, which cannot be edited.
Priority	Specifies the priority of the Link Aggregation Control Protocol (LACP). The value range is 0–65535. The priority is valid for dynamic binding but not for manual binding.
Work Mode	Specifies the work mode of the interface, which can be **Active mode** and **Passive mode**.

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

Step 4 Apply the settings.

----End

Configuring a Device Interconnection Interface

After device interconnection interfaces are configured, if two NIPS devices communicate with each other via a device interconnection interface for HA purposes (if configured), the response data can be returned through the original link.

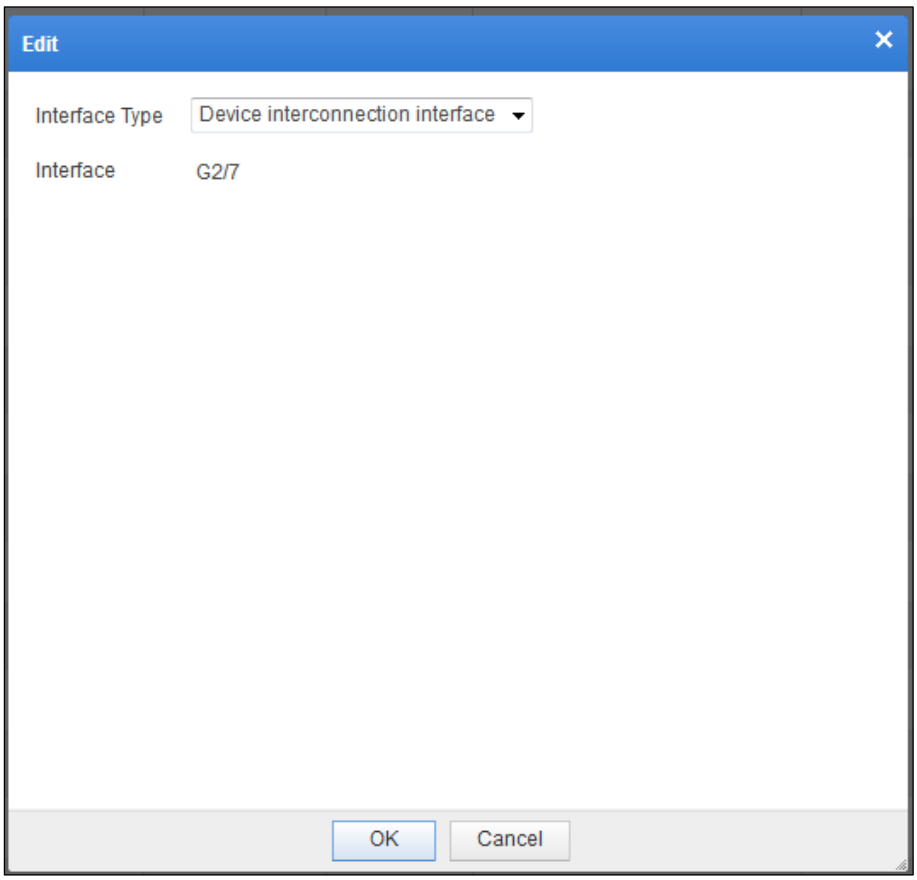
Note	After a device interconnection interfaces is configured, you can specify this interface for asymmetric routing support. For details, see section 5.10.6 Asymmetric Routing Support.

Step 1 On the page shown in Figure 5-1, click  in the **Operation** column of an interface.

The dialog box for configuring a device interconnection interface varies with device models.

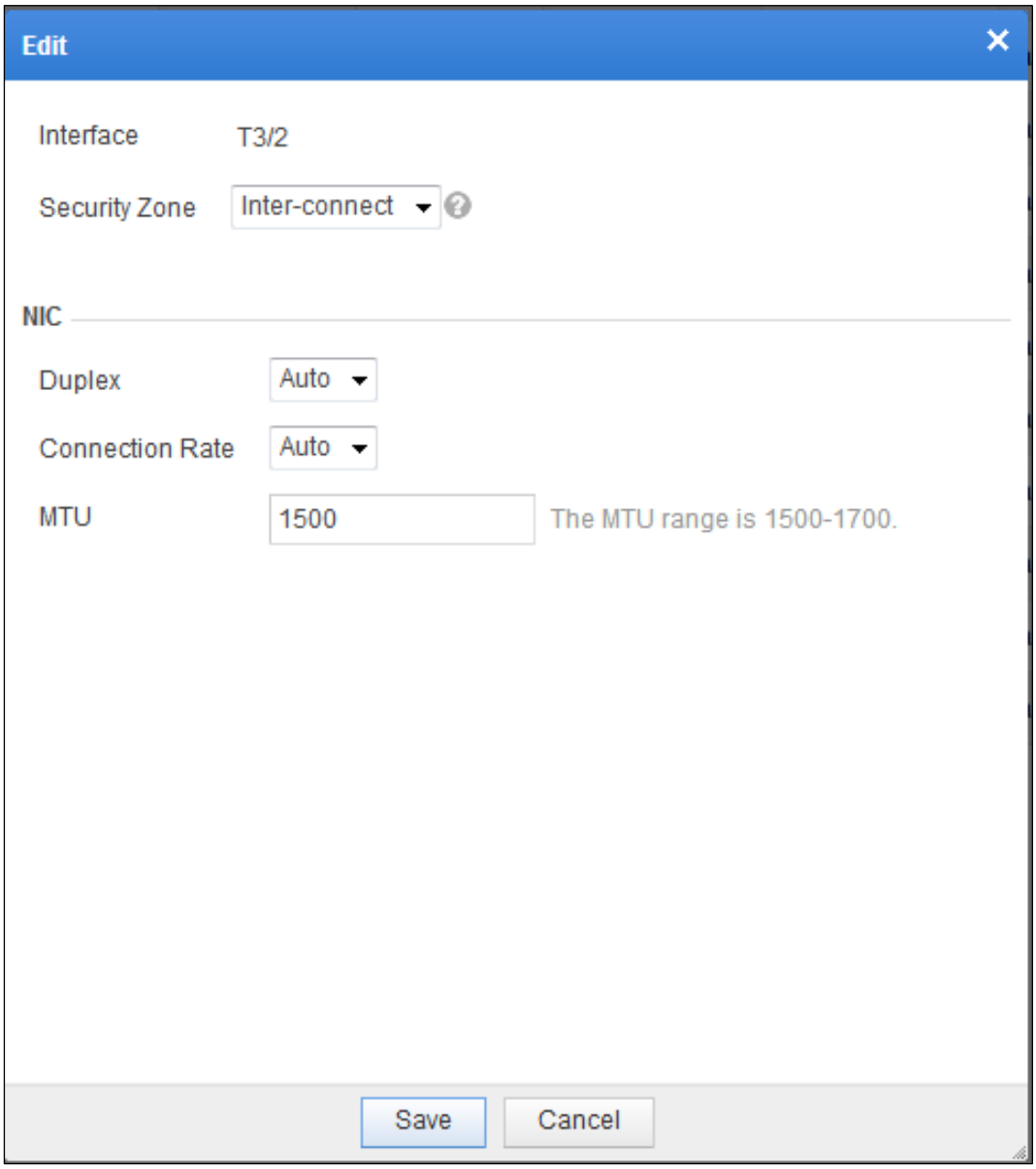
- Figure 5-14 shows the dialog box for configuring a device interconnection interface on device models other than NX5-T9010A and NX5-T9020A.

Figure 5-14 Configuring a device interconnection interface on device models other than NX5-T9010A and NX5-T9020A



- Figure 5-15 shows the dialog box for configuring a device interconnection interface on NX5-T9010A and NX5-T9020A. You must configure **Security Zone** to **Inter-connect** in advance. (For details, see section 5.2 Security Zone.)

Figure 5-15 Configuring a device interconnection interface on NX5-T9010A and NX5-T9020A



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

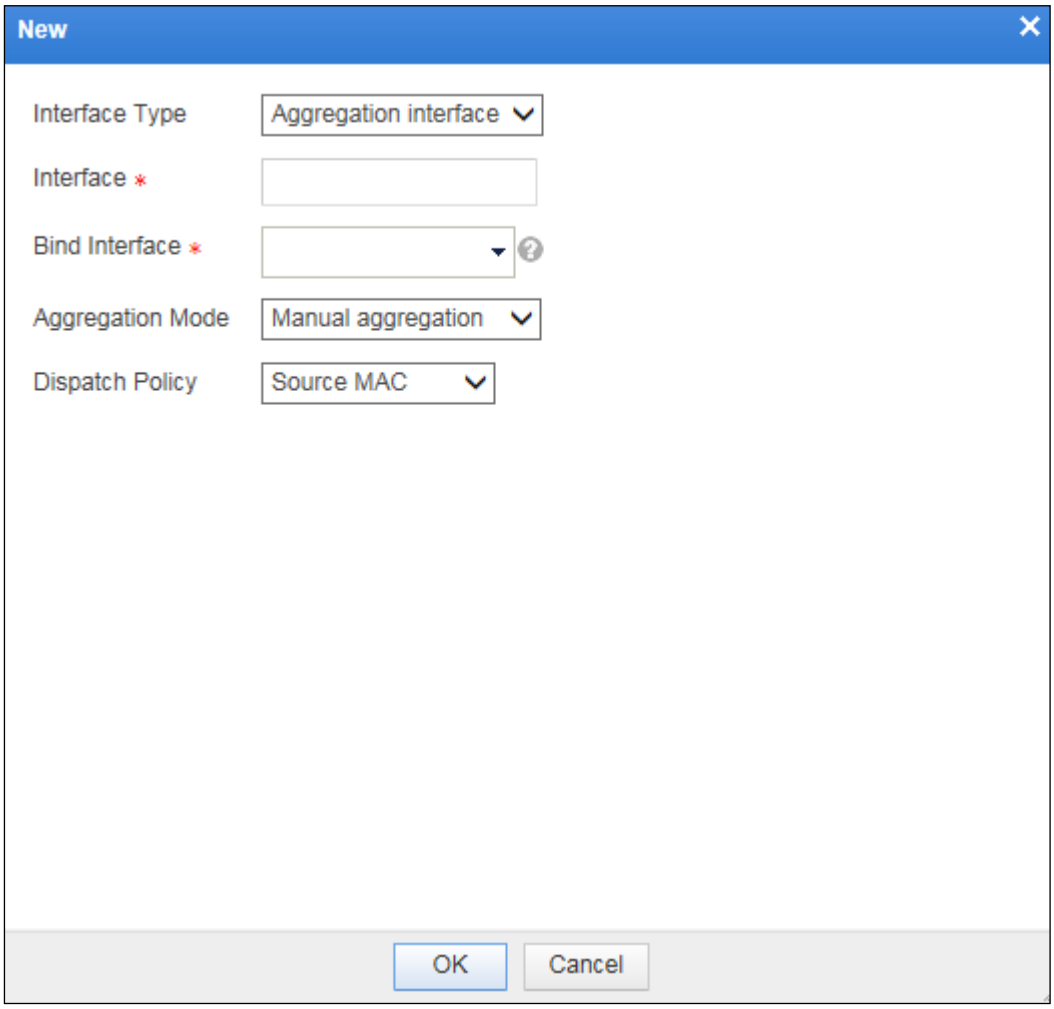
Step 3 Apply the settings.

----End

5.1.2.3 Creating an Aggregation Interface

Step 1 On the page shown in Figure 5-1, click **New** in the upper-right corner of the page and then set **Interface Type** to **Aggregation interface** in the **New** dialog box.

Figure 5-16 Creating an aggregation interface



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

Table 5-8 Parameters for configuring an aggregation interface

Parameter	Description
Interface Type	Specifies the type of the interface, which should be set to **Aggregation interface**.
Interface Name	Specifies the name of the aggregation interface, which should be a string of 1 to 15 characters, including letters, digits, underscores (_), slashes (/), and dots (.).
Bind Interface	Specifies the aggregation member interface which can be selected from the existing aggregation member interfaces. The duplex mode and connection rate of the bound interfaces must be the same.
Aggregation Mode	Specifies the mode of aggregation, which can be **Manual aggregation** or **Dynamic aggregation**. • When **Aggregation Mode** is set to **Manual aggregation**, the number of aggregation member interfaces can be 2 to 8. • When **Aggregation Mode** is set to **Dynamic aggregation**, the number of aggregation member interfaces can be 2 to 32.

Parameter	Description
Dispatch Policy	Specifies the dispatch policy of the aggregation interface. When there are multiple aggregation members in the aggregation group, the configured policy will dispatch packets for better load balancing. The options include the following: • **Source MAC**: indicates that packets with the same source MAC address are sent from the same interface. Otherwise, they are sent from different interfaces. • **Destination MAC**: indicates that packets with the same destination MAC address are sent from the same interface. Otherwise, they are sent from different interfaces. • **Polling**: indicates that packets are sent from interfaces one by one. • **Layer 2**: indicates that the interface for sending packets depends on the source and destination MAC addresses of the packet. • **Layer 2+3**: indicates that the interface for sending packets depends on layer 2 and layer 3 information in packet headers. • **Layer 3+4**: indicates that the interface for sending packets depends on layer 3 and layer 4 information in packet headers.

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

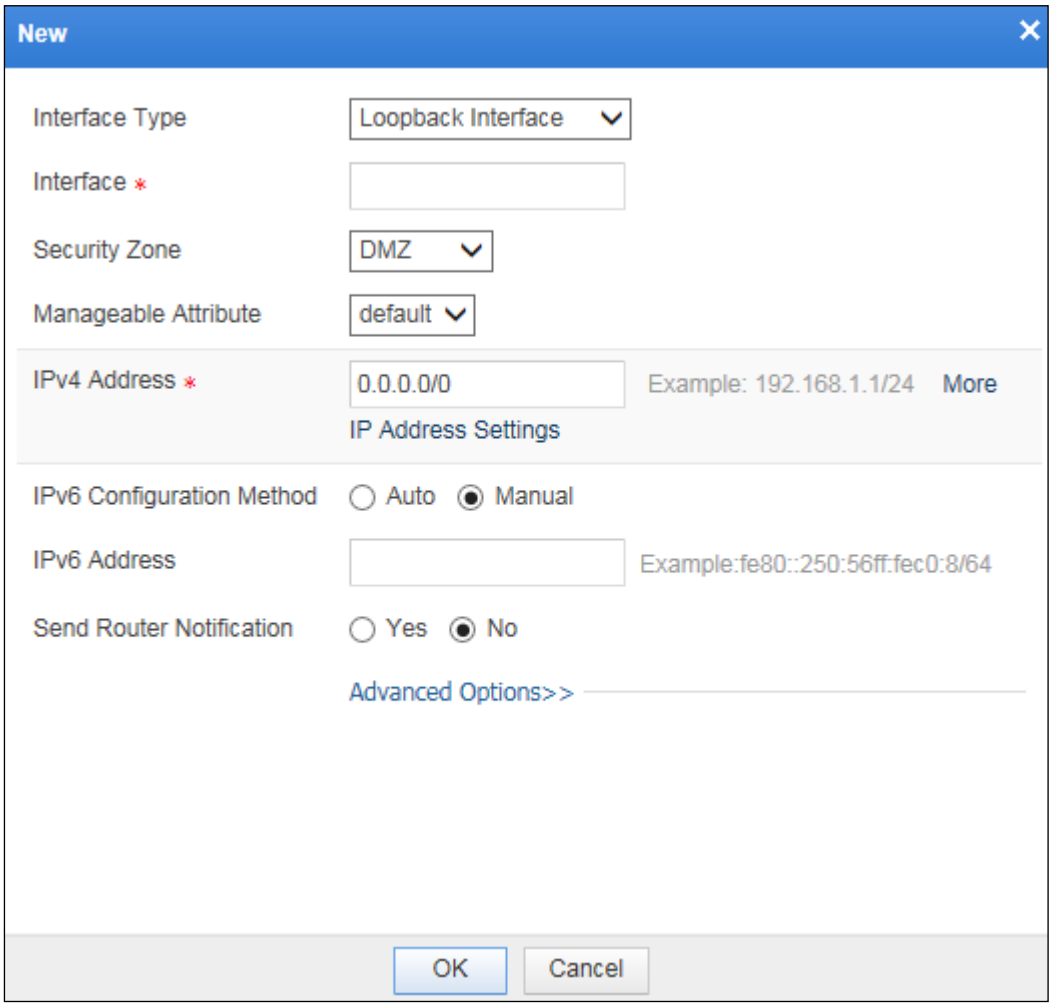
Step 4 Apply the settings.

----End

5.1.2.4 Creating a Loopback Interface

Step 1 On the page shown in Figure 5-1, click **New** in the upper-right corner of the page and then set **Interface Type** to **Loopback interface** in the **New** dialog box.

Figure 5-17 Creating a loopback interface



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

The name of a loopback interface should be a string of 1 to 15 characters, including letters, digits, underscores (_), slashes (/), and dots (.).

Other parameters are the same as those for configuring a layer 3 Ethernet interface. For details, see Figure 5-4 and Table 5-5.

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

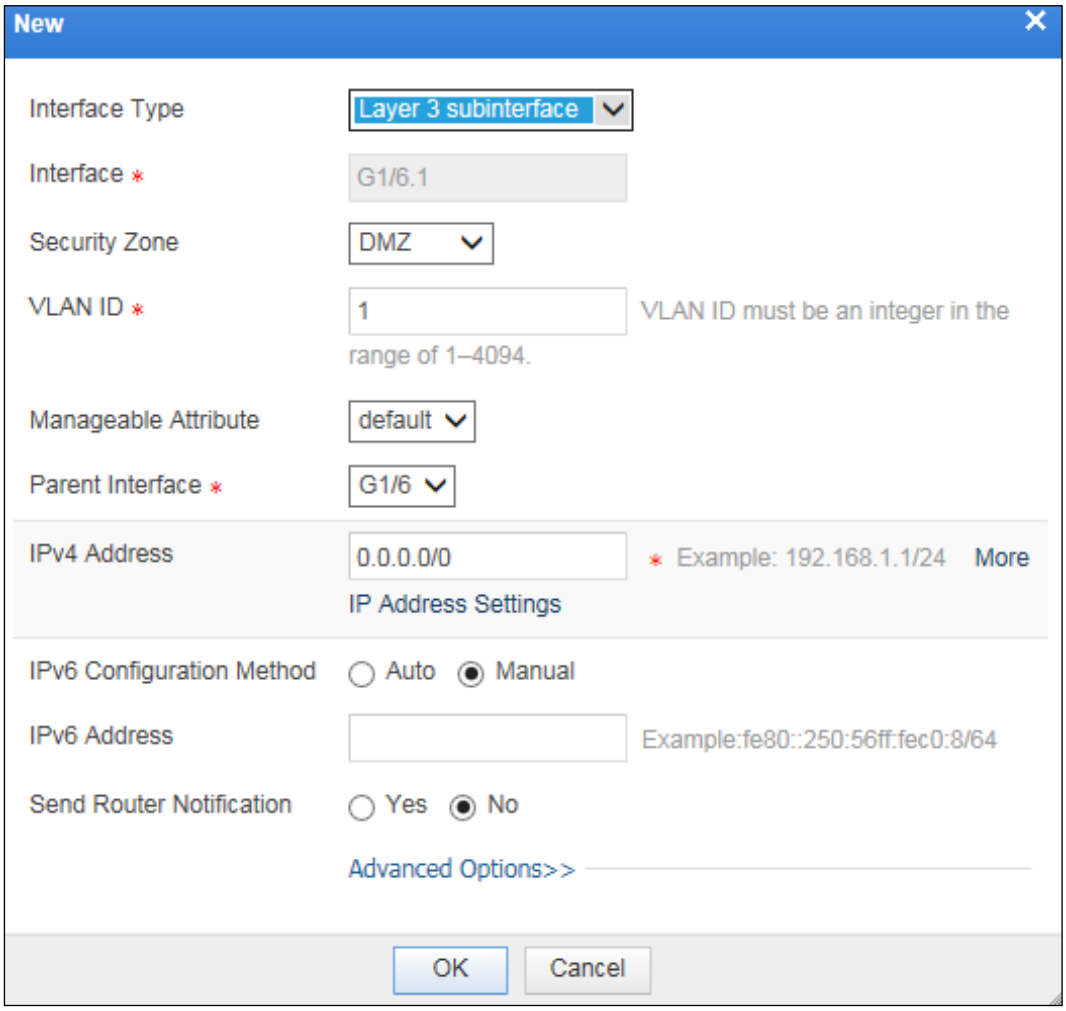
Step 4 Apply the settings.

----End

5.1.2.5 Creating a Layer 3 Subinterface

Step 1 On the page shown in Figure 5-1, click **New** in the upper-right corner of the page and then set **Interface Type** to **Layer 3 subinterface** in the **New** dialog box.

Figure 5-18 Creating a layer 3 subinterface



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

Layer 3 subinterfaces are created based on layer 3 Ethernet interfaces. The name of such a subinterface is a combination of the parent interface name and VLAN ID specified for the subinterface like "parent interface name.+VLAN ID". For example, if **VLAN ID** is set to **100** and the parent interface is G1/1, the name of the newly configured layer 3 subinterface will be G1/1.100.

Other parameters are the same as that for configuring a layer 3 Ethernet interface. For details, see Figure 5-4 and Table 5-5.

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

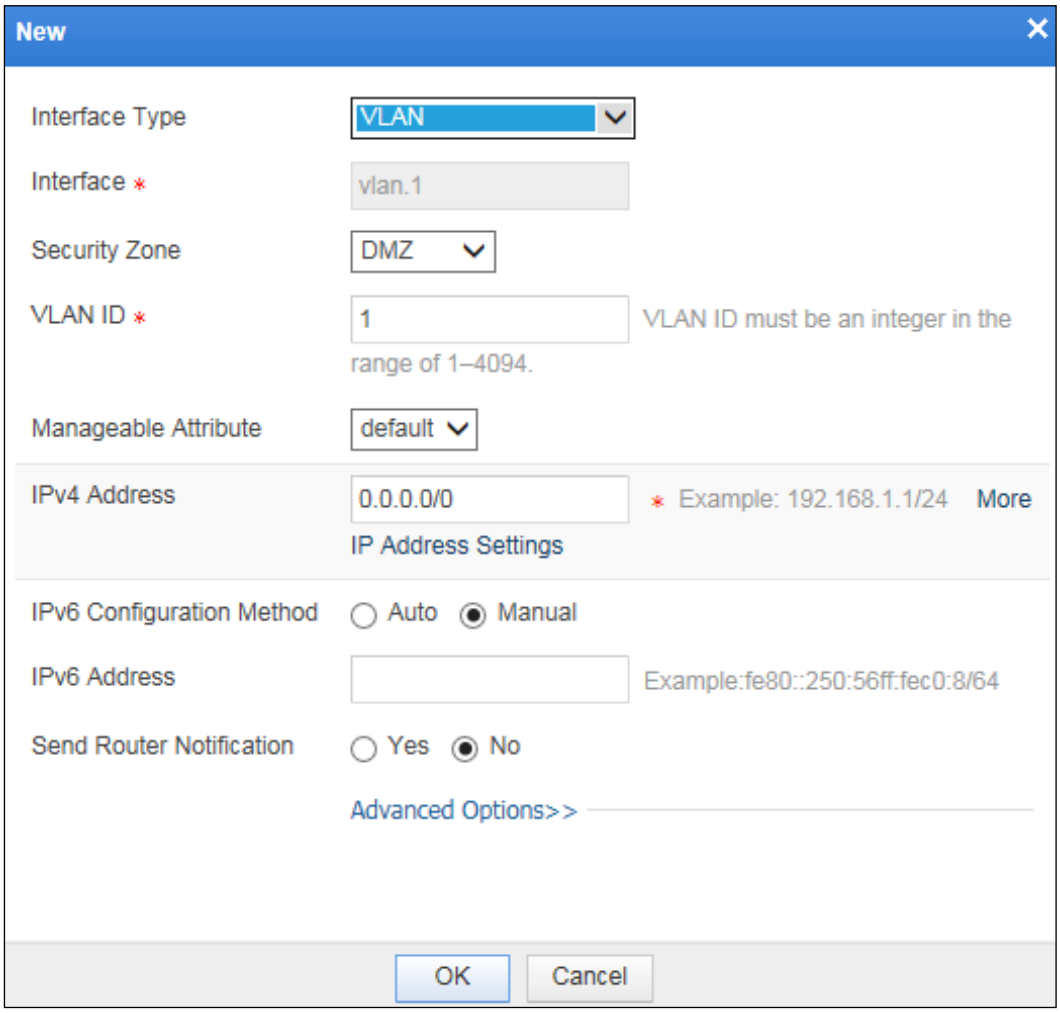
Step 4 Apply the settings.

----End

5.1.2.6 Creating a VLAN Interface

Step 1 On the page shown in Figure 5-1, click **New** in the upper-right corner of the page and then set **Interface Type** to **VLAN** in the **New** dialog box.

Figure 5-19 Creating a VLAN interface



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

VLAN interfaces are layer 3 logical interfaces created based on layer 2 physical interfaces. You need to specify a VLAN ID for them so that VLANs can communicate with each other at layer 3 via VLAN interfaces.

After you specify a VLAN ID, the interface name is automatically generated in the form of "vlan.+ VLAN ID". For example, if **VLAN ID** is set to **20**, the name of the VLAN interface will be vlan.20.

Other parameters are the same as those for configuring a layer 3 Ethernet interface. For details, see Figure 5-4 and Table 5-5.

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

Step 4 Apply the settings.

----End

5.1.3 Manageable Attribute

The management attribute of the interface can be used to configure the management privileges for NIPS interfaces, including the following:

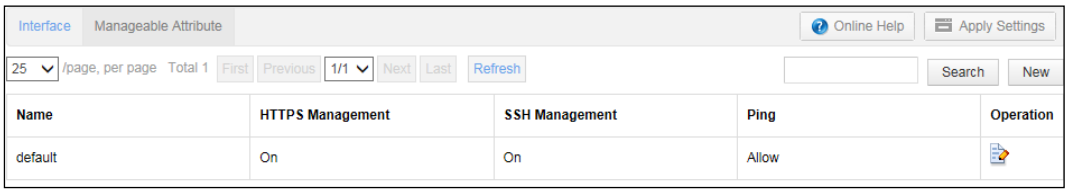
- **HTTPS Management**: controls whether to allow device management from a remote host via HTTPS.
- **SSH Management**: controls whether to allow device management from a remote host via SSH.
- **Ping**: controls whether to allow sending ping response packets.

You can define different manageable attribute objects as required. Management attribute objects can be directly referenced for interface configuration. NIPS allows or denies device management depending on the configuration.

Note	NIPS NX5-T9010A and NX5-T9020A do not support the management attribute.

Step 1 Choose **Network** > **Interface** > **Manageable Attribute**.

Figure 5-20 Manageable Attribute page

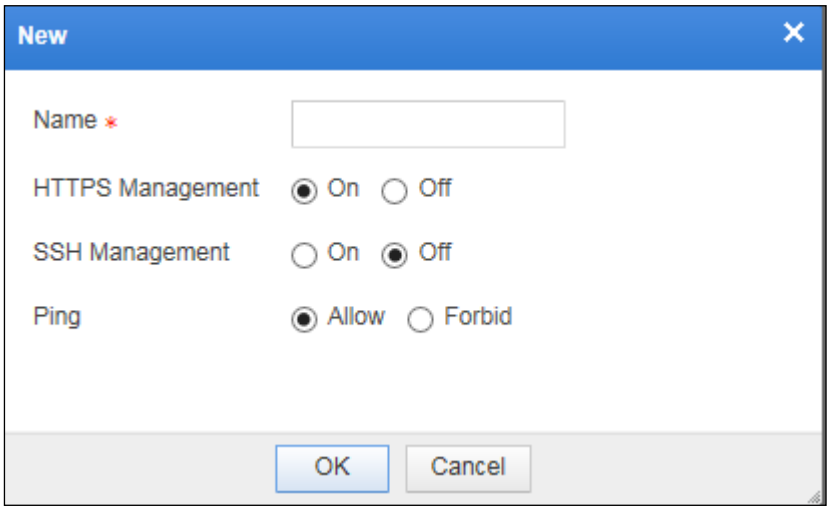


The factory settings of NIPS contains a built-in management attribute object (**default**), for which **HTTPS Management** and **SSH Management** are set to **On** and **Ping** is set to **Allow**.

Step 2 Create a management attribute object.

a. Click **New** in the upper-right corner of the **Manageable Attribute** page.

Figure 5-21 Creating a management attribute object



b. In the dialog box, configure parameters.

c. Click **OK** to complete the configuration.

Step 3 Edit a management attribute object.

Click in the **Operation** column, modify parameters in the displayed dialog box, and then click **OK**.

Step 4 Delete a manageable attribute.

Click in the **Operation** column of a custom manageable attribute and then click **OK** in the confirmation dialog box.

Step 5 Apply the settings.

----End

5.2 Security Zone

A security zone is a collection of interfaces of the same type. Supported security zone types vary with device models.

Table 5-9 lists security zone types supported by device models other than NX5-T9010A and NX5-T9020A.

Table 5-9 Security zone types supported by device models other than NX5-T9010A and NX5-T9020A

Type	Description
layer2	Security zone of the transparent type. Interfaces in such a security zone work in layer 2 switch mode.
-layer3	Security zone of the route type. Interfaces in such a security zone work in route mode. Only layer 3 interfaces work in this mode.

Type	Description
monitor	Security zone of the monitoring type. Interfaces in such a security zone monitor data transmission.
vwire	Security zone of the direct connection type. Interfaces in such a security zone work in v-wire mode.
mgt	Security zone of the management type. Interfaces in such a security zone are working interfaces that can be used for out-of-band management.
global	Default security zone, which cannot be edited and contains all security zones.

Table 5-10 lists security zone types supported by device models other than NX5-T9010A and NX5-T9020A.

Table 5-10 Security zone types supported by NX5-T9010A and NX5-T9020A

Type	Description
monitor	Security zone of the monitoring type. Interfaces in such a security zone monitor data transmission.
direct	Security zone of the direct connection type. Interfaces in such a security zone work in direct mode.
interconnect	Security zone of the device interconnection type. Interfaces in such a security zone work in interconnection mode.
mgt	Security zone of the management type. Interfaces in such a security zone can be used for out-of-band management.
global	Default security zone, which cannot be edited and contains all security zones.

You can search for, create, edit, and delete security zones. In practice, you can move interfaces to other security zones except for the following interfaces.

Note	Security zone cannot be changed for interfaces in the following cases: • Interfaces M and H1 • Non-Gigabit Intel NIC interface • Interfaces configured with routing policies • The license status is abnormal, for example, it has not been imported. In this case, you cannot move any interfaces out of their security zones. • Interfaces configured with subinterfaces or policies.

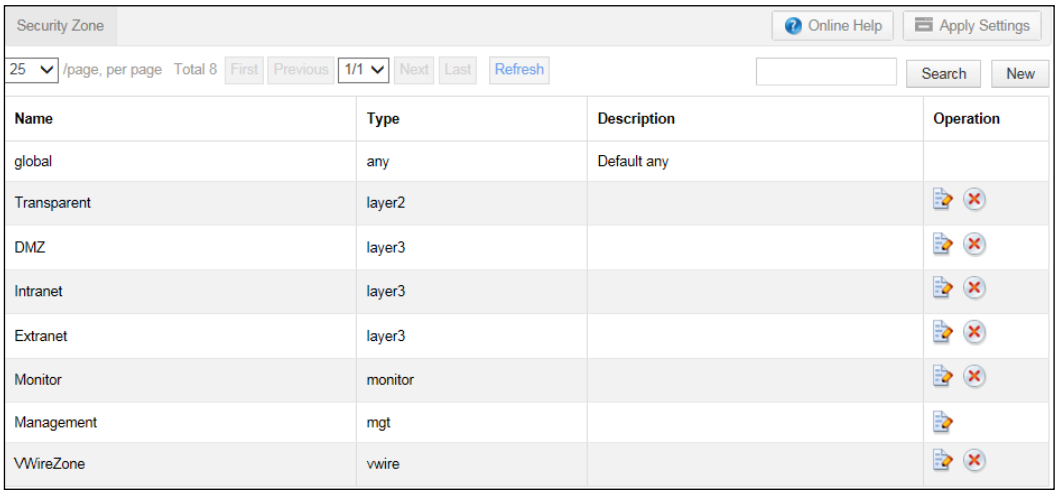
To create a security zone, follow these steps:

Step 1 Choose **Network** > **Security Zone**.

Note that the "global" zone cannot be edited or deleted, and the "Management" zone cannot be deleted. The **Security Zone** page varies with device models.

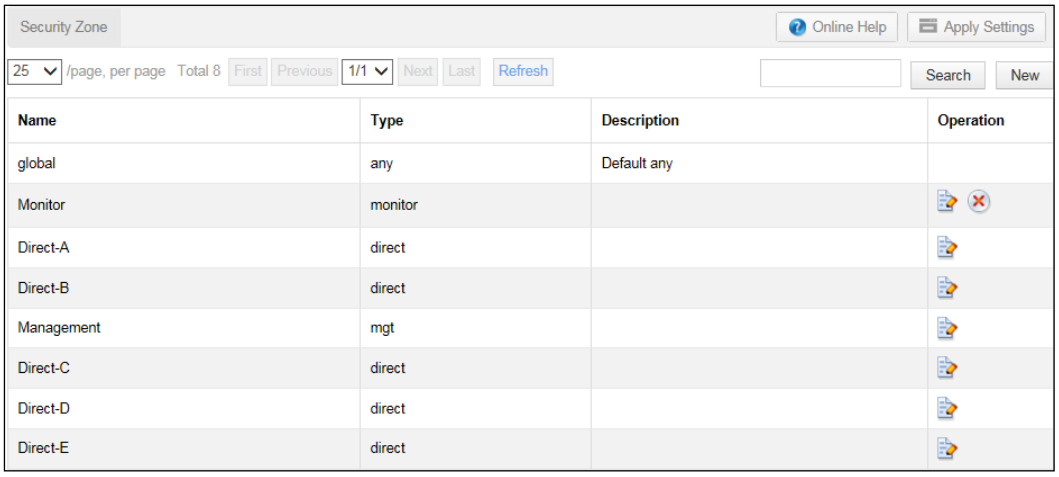
- Figure 5-22 shows the **Security Zone** page of device models other than NX5-T9010A and NX5-T9020A.

Figure 5-22 Security Zone page of device models other than NX5-T9010A and NX5-T9020A



- Figure 5-23 shows the **Security Zone** page of NX5-T9010A and NX5-T9020A.

Figure 5-23 Security Zone page of NX5-T9010A and NX5-T9020A

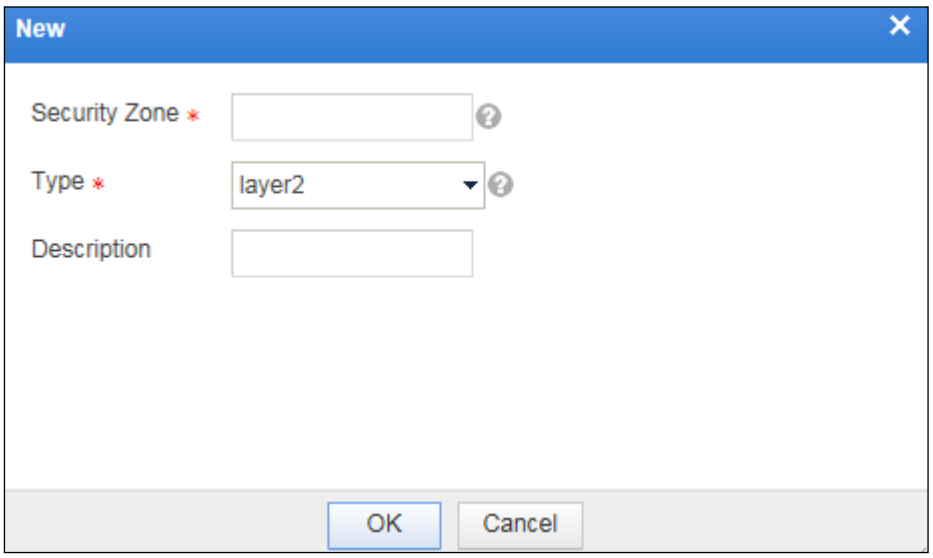


Step 2 Click **New** in the upper-right corner.

The **New** dialog box for creating a security zone varies with device models.

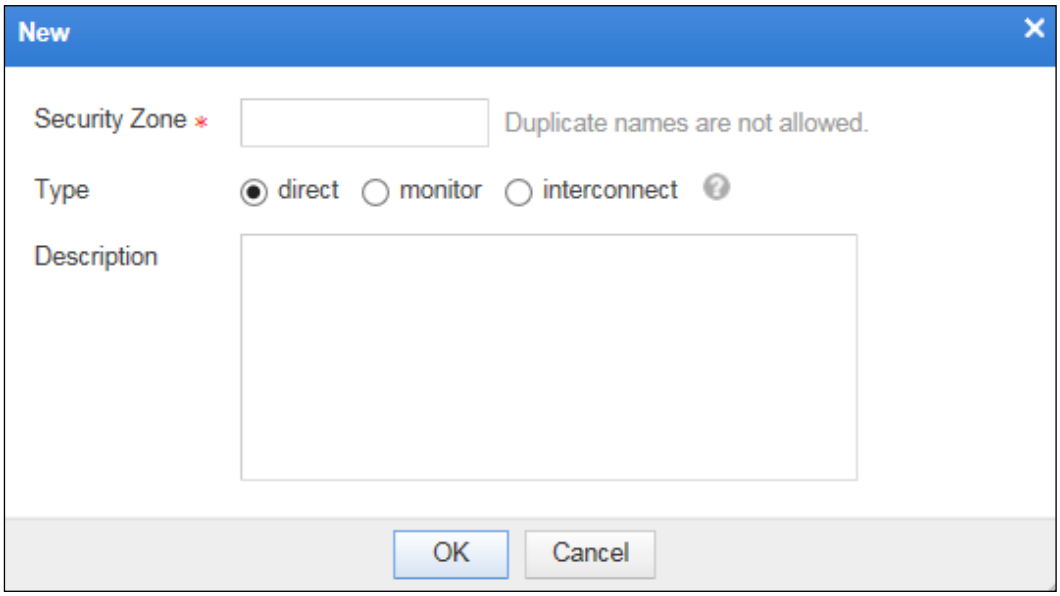
- Figure 5-24 shows the dialog box for creating a security zone on device models other than NX5-T9010A and NX5-T9020A.

Figure 5-24 Creating a security zone on device models other than NX5-T9010A and NX5-T9020A



- Figure 5-25 shows the dialog box for creating a security zone on device models other than NX5-T9010A and NX5-T9020A.

Figure 5-25 Creating a security zone on NX5-T9010A and NX5-T9020A



Step 3 Configure parameters in the **New** dialog box.

Table 5-11 Security zone configuration parameters

Parameter	Description
Security Zone	Name of the security zone.

Parameter	Description
	It is case-sensitive and cannot contain spaces and the following special characters: / % \ { } ` @ ^ < > ' & " : The security name must be unique.
Type	Security zone type.
Description	Descriptive information of the security zone.

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

Step 5 Apply the settings.

----End

5.3 Virtual Wire

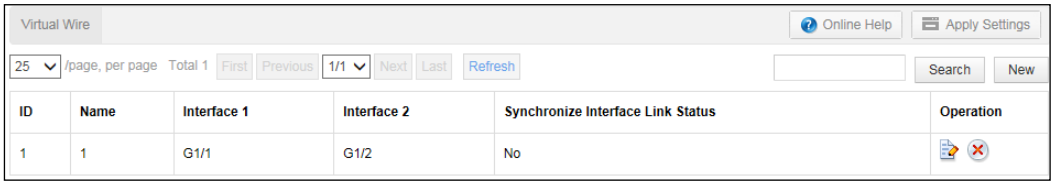
In virtual wire mode, NIPS is used as a virtual wire, which has a pair of interfaces.

Note	NIPS NX5-T9010A and NX5-T9020A do not support the virtual wire function.

You can search for, create, edit, and delete virtual wires. To create a virtual wire, follow these steps:

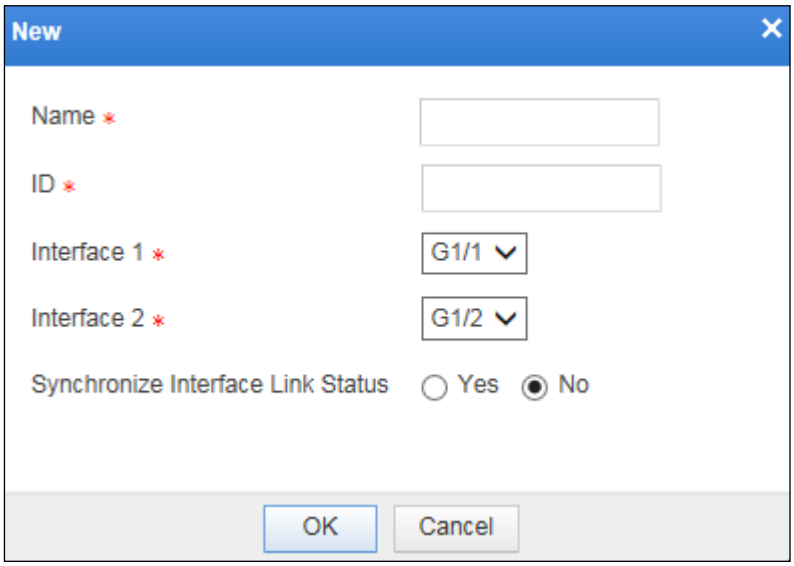
Step 1 Choose **Network** > **Virtual Wire**.

Figure 5-26 Virtual Wire page



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

Figure 5-27 Configuring a virtual wire



Step 3 In the dialog box, configure parameters.

Table 5-12 Parameters for creating a virtual wire

Parameter	Description
Name	Unique name of the virtual wire. The name cannot contain the following special characters: % \ ` < > ' & "
ID	ID of the virtual wire.
Interface 1/2	Specifies the two working interfaces of the virtual wire. The interface type must be v-wire.
Synchronize Interface Link Status	Controls whether to synchronize the interface link status. • **Yes**: indicates that when one interface is down, the other interface is also down. • **No**: indicates that when one interface is down, the other interface keeps its original status.

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

Step 5 Apply the settings.

----End

5.4 Switch

NIPS provides the following layer 2 switch functions:

- MAC table: configures rules for forwarding layer 2 packets based on VLAN IDs and MAC addresses.
- RSTP: configures parameters for creating rapid spanning trees with other switches.
- MSTP: configures parameters for creating multiple spanning trees with other switches.

Note	NIPS NX5-T9010A and NX5-T9020A do not support the switch function.

5.4.1 MAC Table Configuration

The MAC table is used to configure rules for forwarding layer 2 packets. Via static MAC entries, a device for which a VLAN and a MAC address are specified can access the network through a given interface. If the device uses another interface, instead of the given one, to access the network, the device will no longer be able to obtain MAC entries through dynamic learning. If a device without a MAC entry accesses the network through an interface, a dynamic MAC entry is automatically established for the device through its dynamic learning.

Entries in a MAC table can be divided as follows:

- Dynamic MAC entries:

  Dynamic MAC entries refer to the MAC entries that NIPS dynamically learns from the received layer 2 packets. Dynamic MAC entries can be in the following states in the MAC table:

  - Valid: If any packets that match a dynamic MAC entry pass through NIPS in 300 seconds, the state of this dynamic MAC entry is displayed as "valid".
  - Invalid: If no packet that matches a dynamic MAC entry pass through NIPS in 300 seconds, the state of this dynamic MAC entry is displayed as "invalid".
- Static MAC entries:

  Static MAC entries refer to the MAC forwarding entries added by the administrator or the dynamic MAC forwarding entries bound by the administrator. Static MAC entries are used to configure rules for forwarding layer 2 packets.

  When forwarding layer 2 packets, NIPS checks whether such packets hit any static entries in the MAC table based on the VLAN ID and MAC address of the packets.

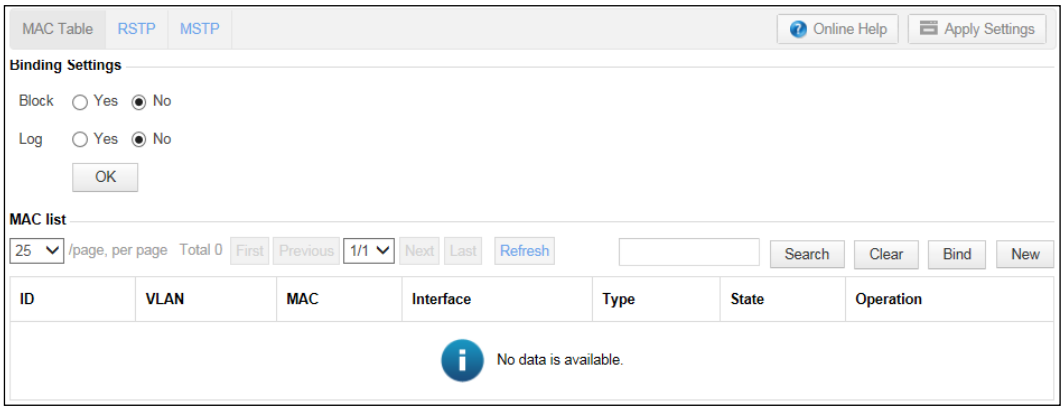
  - If yes, NIPS will forward the packets via the interface configured in the static MAC entry.
  - If no, NIPS will block or forward the packets as configured in the policy.

To configure a MAC table, follow these steps:

Step 1 Choose **Network > Exchange > MAC Table**.

The **MAC Table** page appears, displaying VLAN/MAC bindings that are discovered by NIPS and added manually.

Figure 5-28 MAC table



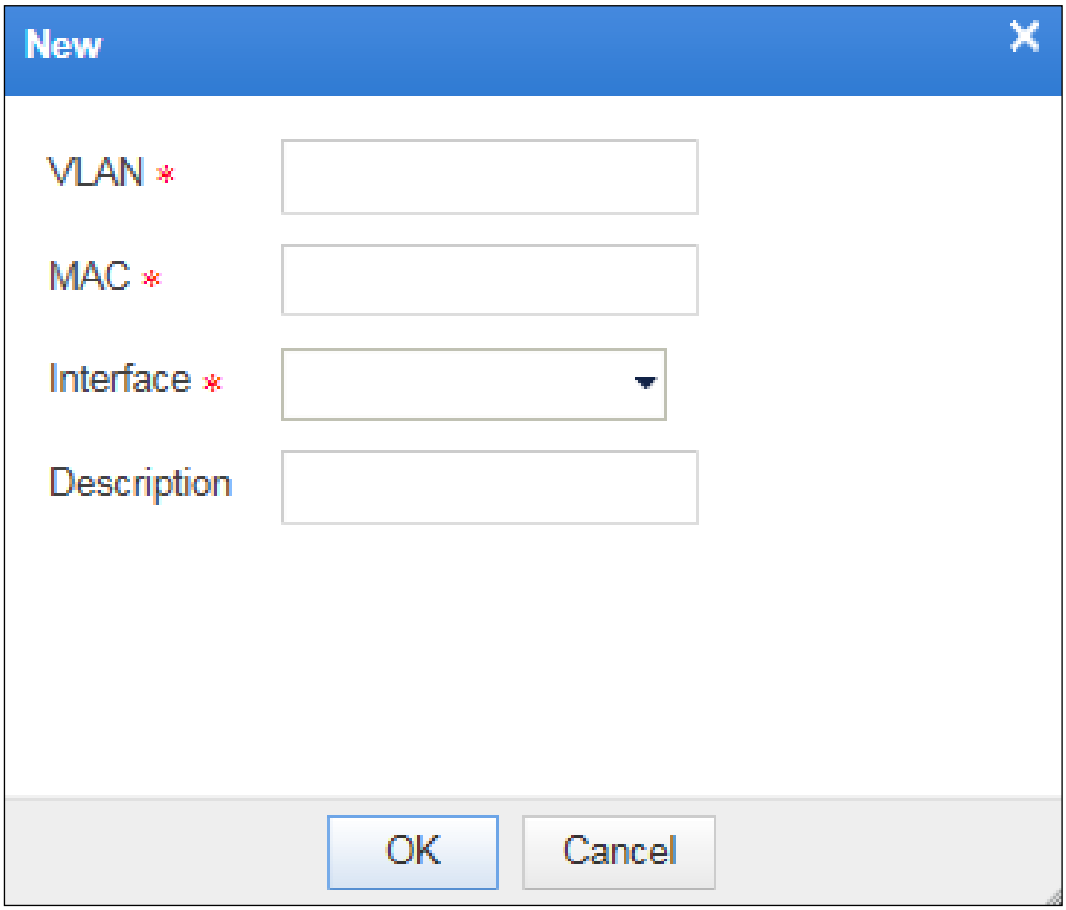
Step 2 Configure parameters.

- **Block**: controls whether NIPS blocks packets that do not match a static MAC entry.
- **Log**: controls whether NIPS logs the situation where packets hitting a static MAC entry.

Step 3 Create a static MAC entry.

a. On the page shown in Figure 5-28, click **New** in the upper-right of the MAC list.

Figure 5-29 Creating a VLAN/MAC binding



b. Configure parameters in the **New** dialog box.

Table 5-13 Parameters for configuring a static VLAN/MAC binding

Parameter	Description
VLAN	Specifies the destination VLAN ID of the packet. For an interface working in access mode, select the ID of the VLAN to which the interface belongs; for an interface working in trunk mode, select a VLAN ID within the corresponding range.
MAC	Specifies the destination MAC address of the packet.
Interface	Specifies a layer 2 interface. The packets whose VLAN ID and MAC address match the configured conditions will be forwarded through this interface. **The interface here must be an interface within a layer 2 security zone.**
Description	Brief description of the VLAN-MAC binding. This parameter is optional.

c. Click **OK** to complete the configuration.

Step 4 (Optional) Perform other operations.

You can also edit, delete, enable, disable, search for, clear, and confirm in batches VLAN/MAC bindings in the same way as IP/MAC bindings in the ARP table. For details, see section 5.8.3 ARP Table.

Step 5 Apply the settings.

----End

5.4.2 RSTP Configuration

The following describes the working principle of the Rapid Spanning Tree Protocol (RSTP) and the spanning tree configuration.

5.4.2.1 Working Principle

RSTP is a layer 2 protocol that prevents layer 2 loops by blocking certain redundant links in a network. Compared with the Spanning Tree Protocol (STP), RSTP provides a faster convergence if a LAN link fails.

RSTP provides five types of ports: root port, designated port, backup port, alternate port, and disabled port. Port states include Discarding, Learning, and Forwarding.

Spanning Tree Algorithm (STA) determines the port role through Bridge Protocol Data Unit (BPDU) and prioritizes the ports based on BPDU packets saved on the port. After the STA becomes stable after a period of time, the designated port and root port enter the forwarding state. Subsequently, network bridges will send STP BPDU packets periodically from the specified interface, so as to maintain the link state. If the network topology changes, the spanning tree will be regenerated and the port state will change accordingly.

5.4.2.2 RSTP Configuration

The RSTP configuration roadmap is as follows:

1. Configure layer 2 interfaces and enable the RSTP function on them.
2. Configure RSTP parameters.
3. Enable RSTP.

The procedure is as follows:

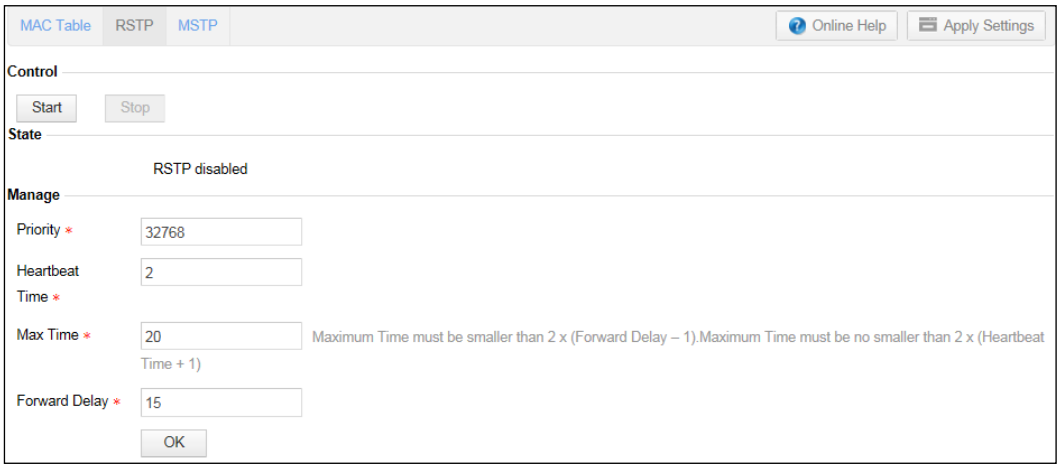
Step 1 Configure interfaces and enable the RSTP function on them.

On NIPS, configure at least a pair of layer 2 interfaces with RSTP as their STP type to forward data and generate the spanning tree.

Step 2 Configure RSTP.

a. Choose **Network** > **Exchange** > **RSTP**.

Figure 5-30 RSTP page



b. Configure parameters.

Table 5-14 RSTP configuration parameters

Parameter	Description
State	RSTP interfaces and their status. The RSTP interface status can be as follows: • **Discarding**: The port can neither learn addresses nor forward data. • **Learning**: The port starts learning address and can send, receive, and handle configuration messages. • **Forwarding**: The port can forward data, learn addresses, and send, receive, and handle configuration messages.
Priority	RSTP priority. It must be an integer multiple of 4096. The default value is **32768**.
Heartbeat Time	Specifies the interval of sending hello packets. Hello packets are sent to check whether links between devices are in the normal state. The interval refers to how often NIPS sends hello packets. The value is an integer in the range of 1–10 in seconds, with **2** as the default.
Max Age	Specifies the maximum interval allowed to receive packets. If the specified interval expires, the system drops the received packets. The default value is **20** seconds.
Forward Delay	Specifies the time taken by NIPS to change from the learning state to the forwarding state. The default value is **15** seconds.

Note	Enabling RSTP will make parameters under **Configuration** unavailable. These parameters can be edited only after RSTP is disabled.

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

Step 3 Enable RSTP.

On the page shown in Figure 5-30, click **Start** on the **RSTP** page and click **OK** in the confirmation dialog box.

Step 4 Apply the settings.

----End

5.4.3 MSTP

Multiple Spanning Tree Protocol (MSTP) is a new spanning tree protocol defined in the IEEE802.1s standard. It enables STP to work with VLANs. In simple terms, STP and RSTP are based on ports, PVST+ is based on VLANs, while MSTP is based on instances. While maintaining RSTP's advantage of rapid port migration, MSTP solves the issue in RSTP that different VLANs in RSTP mode must be on the same tree.

The following describes the working principle of MSTP and the spanning tree configuration.

5.4.3.1 Working Principle

MSTP stands for Multiple Spanning Tree Protocol. Here, Multiple Spanning Tree has two meanings:

- A switching network can be divided into multiple spanning tree instances based on VLANs.
- Each spanning tree instance can contain multiple VLANs.

For PVST and PVST+ of Cisco, the entire switching network can also be divided into multiple spanning tree instances based on VLANs, but each instance can contain only one VLAN. Compared with PVST and PVST+, MSTP is more appropriate to large networks because it can divide a large network into spanning tree instances in a more flexible way to meet actual requirements.

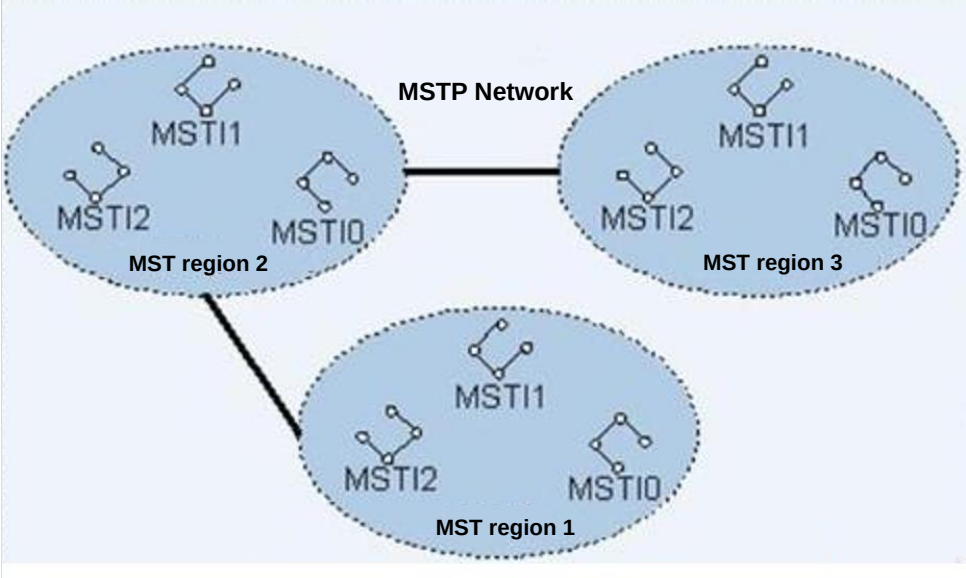
On the whole, an MSTP network has three tiers:

- MSTP network
- Multiple spanning tree (MST) region
- Multiple spanning tree instance (MSTI)

The three tires constitute an inclusion relationship. Specifically, an MSTP network contains MST regions and MSTIs; an MST region contains MSTIs.

In an MSTP network, network segments with different configurations are divided into different MST regions in which multiple independent spanning trees can be built. All MST regions are connected via one spanning tree (i.e., common spanning tree (CST)) to ensure that all such regions are fully connected but no loops exist.

Figure 5-31 Hierarchy of an MSTP network



The following are basic concepts in MSTP.

1. MST Region

An MST region consists of multiple switches in a switching network and the network segments among them. Such devices have the following characteristics:

- MSTP is enabled.
- The share the same domain name, VLAN-spanning tree mapping configuration, and MSTP revision level configuration.
- They are connected via physical links.

A local area network (LAN) can have multiple MST regions that are physically connected to each other in a direct or indirect way. With MSTP configuration commands, you can assign multiple switches to the same MST region.

2. MST Instance

An MST instance is a spanning tree within an MST region. Within an MST region, multiple spanning trees can be generated via MSTP, which are independent of each other. Each spanning tree, called as an MST instance, maps to a VLAN.

3. VLAN Mapping Table

The VLAN mapping table is an attribute of an MST region. The table is used to describe the mapping between VLANs and MST instances. For example, a VLAN mapping table of an MST region contains the following mappings: VLAN 1 is mapped to spanning tree instance 1; VLAN 2 is mapped to spanning tree instance 2; other VLANs are mapped to the Common and Internal Spanning Tree (CIST).

MSTP implements load balancing according to the VLAN mapping table.

4. CST

CST assumes one spanning tree for connecting all MST regions in a switching network. If each MST region is viewed as a switch, the CST is a spanning tree generated through calculations by these switches via STP and RSTP.

5. Internal Spanning Tree (IST)

IST is a spanning tree within an MST region. The IST and CST constitute the CIST of the entire switch network. IST is a segment of the CIST in an MST region, and is a special MSTI with the MSTI ID being 0. CIST has a segment in each MST region, and such segment is IST in each MST region.

6. CIST

CIST is one spanning tree to connect all switches in a switching network. It consists of the IST in each MST region and CST that interconnects MST regions.

7. Single Spanning Tree

Single Spanning Tree (SST) exists in the following situations:

- Switches running STP or RSTP belong to the same spanning tree.
- The only switch in an MST region is an SST.

8. Regional Root

A regional root is the root of IST and MSTIs within a region. Within an MST region, spanning trees with different topologies have different regional roots.

9. Common Root Bridge

The common root bridge is the CIST root.

10. Port Role

MSTP calculation involves these port roles: root port, designated port, master port, alternate port, backup port, region edge port, and edge port. A port can play different roles in different MSTIs.

- Root port: a port on a non-root switch, providing the minimum-cost path to the root switch. The root port is responsible for forwarding data to the root bridge. The root switch has only designated ports, but not have a root port.
- Designated port: a port responsible for forwarding BPDU packets to downstream network segments or switches. All ports used by switches to connect to downstream switches are designated ports. Such ports exist on both the root switch and non-root switches.
- Master port: a port that connects an MST region to the common root bridge. It is on the shortest path from the current region to the common root bridge.
- Region edge port: a port located on the edge of an MST region. It is used to connect the MST region to another MST region or an SST-enabled region. During MSTP calculations, the role of a region edge port plays in an MSTI is consistent with the role it plays in the CIST instance. That is to say, if a region edge port plays the role of master port (connecting the region to the common root bridge) in the CIST instance, it also plays the same role in all MSTIs of the region.
- Alternate port: a standby port of the master port. When the master port is blocked, the alternate port will become the new master port.
- Backup port: A loop exists when two ports on one switch connect to the same device. In this case, a port will be blocked. The blocked port is a backup port.

- Edge port: a port located on the edge of the entire MST region. Generally, it is directly connected to a user terminal device (for example, a PC), instead of being connected to any switches. Such a port is not involved in MSTP calculations.

11. Root Port Protection

In the case of misconfiguration or malicious attack by maintenance personnel, the legitimate root bridge device in the network may receive configuration information with a higher priority. This may cause the current root bridge to lose the status as the root bridge device, resulting in wrong changes to the network topology.

MSTP provides the root port protection function that can prevent the above situation. This function protects the root switching device. For a port protected by this function, its roles in all instances can only be designated ports. Once such a port receives configuration information with a higher priority, that is, this port is about to be elected as a non-designated port, this port enters the monitoring state and no longer forwards packets. If no higher-priority configuration information is received within a long enough period, the port will return to the previous normal state.

5.4.3.2 Configuring a Spanning Tree

The spanning tree configuration guideline is as follows:

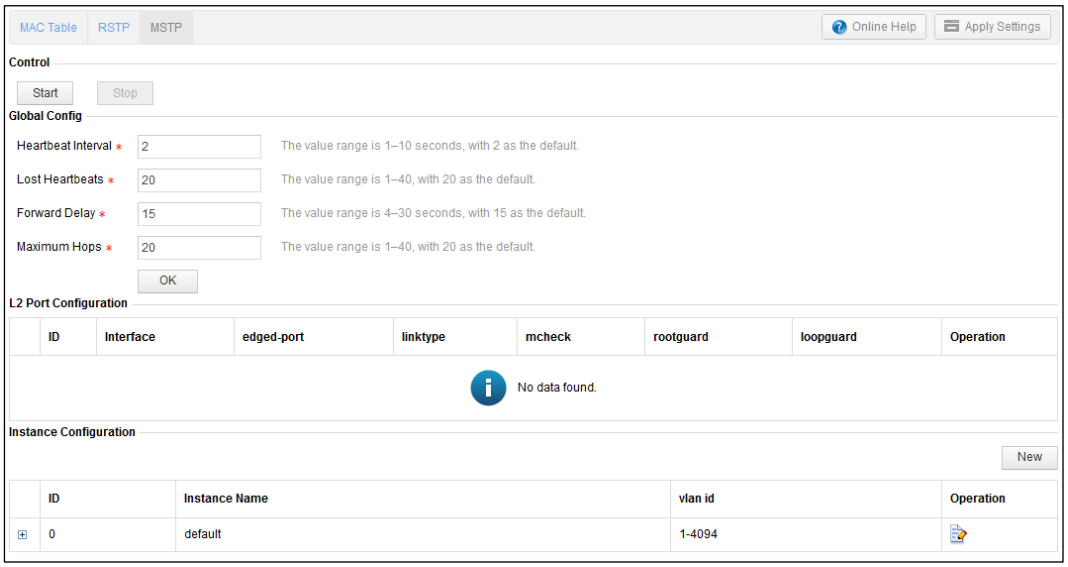
- Configure a layer 2 interface, set its **STP Type** to **MSTP**, and configure its mode and VLAN.
- Set MSTP global parameters.
- Configure layer 2 port parameters.
- Configure mappings between MSTIs and VLANs.
- Enable MSTP.

To configure a spanning tree, follow these steps:

Step 1 Configure interfaces.

Step 2 On NIPS, configure at least a pair of layer 2 interfaces with MSTP as their STP type to forward data and generate spanning trees. For details, see Configuring a Layer 2 Interface in section 5.1.2.2 Editing an Ethernet Interface. Choose **Network** > **Exchange** > **MSTP**.

Figure 5-32 MSTP page



Step 3 Configure global parameters.

Table 5-15 Global parameters of MSTP

Parameter	Description
Heartbeat Interval	Specifies the interval of sending a Hello packet. Hello packets are sent to check whether links between devices are in the normal state. The value is an integer in the range of 1–10 in seconds, with **2** as the default.
Forward Delay	Specifies how long it takes the device to switch from the learning state to the forwarding state. The value is an integer in the range of 4–30 in seconds, with **15** as the default.
Maximum Hops	Specifies the maximum hops of an MST region. Each time a configuration message forwarded from the root bridge passes through a device, the number of hops of this message is decreased by one. NIPS will drop the received configuration message with the number of hops decreased to zero. In this way, devices out of the reach of the maximum number of hops are excluded from spanning tree calculations, thereby limiting the size of the MST region. The value is an integer in the range of 1–40, with **20** as the default. **Note** A greater number of hops in an MST region indicates a larger MST region. Only the maximum number of hops set on the regional root device can limit the size of the MST region.

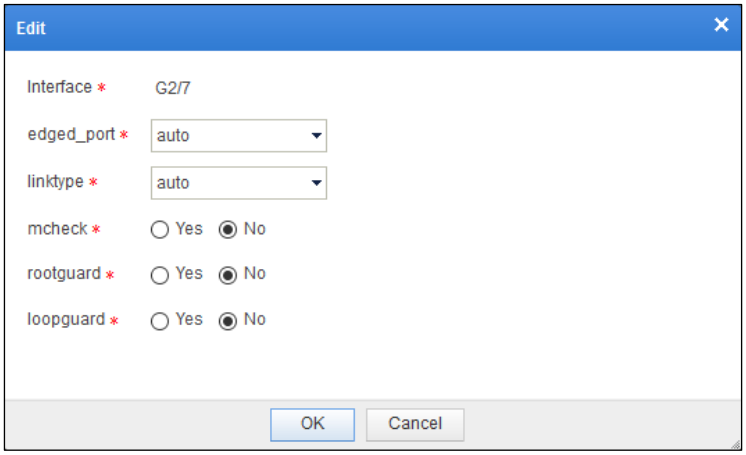
Click **OK** to save the settings.

Step 4 Configure parameters of layer 2 ports.

Under **L2 Port Configuration**, the list shows all layer 2 interfaces with MSTP enabled.

a. Click in the **Operation** column of an interface.

Figure 5-33 Configuring layer 2 port parameters



b. Configure parameters.

Table 5-16 Parameters related to a layer 2 port

Parameter	Description
Edged-port	Controls whether this interface is an edged port. This interface is regarded as an edged port if it is directly connected to a user terminal, instead of being connected to another network bridge device or a shared link.
Linktype	Specifies the link type of this interface, which can be one of the following: • **Auto**: indicates that the interface link is in automatic mode. That is to say, when the interface works in full duplex mode, the link is of the point-to-point type; when the interface works in half duplex mode, the link is of the sharing type. **auto** is the default value. • **point-to-point**: indicates that the interface link is in of the point-to-point type. • **Share**: indicates that the interface link is of the sharing type. **Note** • The parameter setting depends on actual conditions of physical links. For example, if you set a link of an interface to the point-to-point type, but the physical link is not of this type, a temporary loop may occur. Therefore, you are advised to use the default value **auto**. • The parameter setting is valid for the CIST and all MSTIs.
Mcheck	Controls whether to check the existence of an STP-enabled network bridge in the network segment connecting to this interface. If such a network bridge exists, this interface will be switched to STP-consistent mode. When the network is in stable conditions, though the STP-enabled network bridge is removed from the network segment, the interface connecting to the bridge still operates in the STP-compatible mode. In

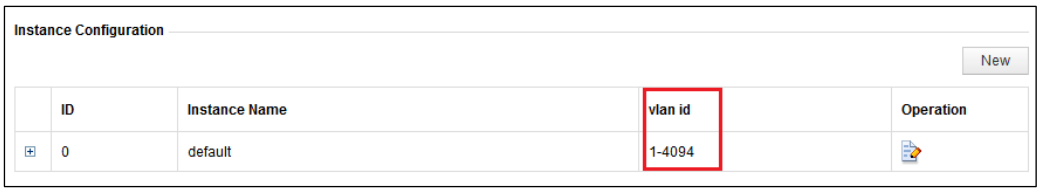
Parameter	Description
	this case, you can set this parameter to force this port to migrate to the MSTP mode and then determine whether to enable the interface to operate in MSTP mode or STP-compatible mode based on the type of the received packets.
Rootguard	Controls whether to enable the root bridge protection function to prevent the root bridge device from losing its status due to misconfiguration or malicious attacks. After this function is enabled, the port can only play the role of designate port on all instances. Once such a port receives configuration information with a higher priority, that is, the interface is about to be set to a non-designated port, this system gets the interface to enter the monitoring state so that it no longer forwards packets. If no higher-priority configuration message is received within a long enough period, the interface will return to the previous normal state. By default, the root protection function is disabled.
Loopguard	Controls whether to enable the loop protection function for the interface. Link congestion or a unidirectional link failure may cause a loop on the switching network. The loop protection function of MSTP is intended to prevent this kind of loop. After this function is enabled, the root port keeps playing its due role and the blocked port keeps discarding packets, preventing loops from forming. By default, the loop protection function is disabled.

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

Step 5 Configure an MST instance.

By default an MST region only has instance 0 (CIST) to which all VLANs are mapped.

Figure 5-34 Initial instance configuration



Caution	For instance 0, **Instance Name** indicates the MST region to which it belongs; for other instances, **Instance Name** indicates the name of the instance.

b. Create an MST instance.

Within an MST region, you can create multiple MST instances and assign different VLANs to them.

Click **New** in the upper-right corner of the page.

Figure 5-35 Creating an MST instance.

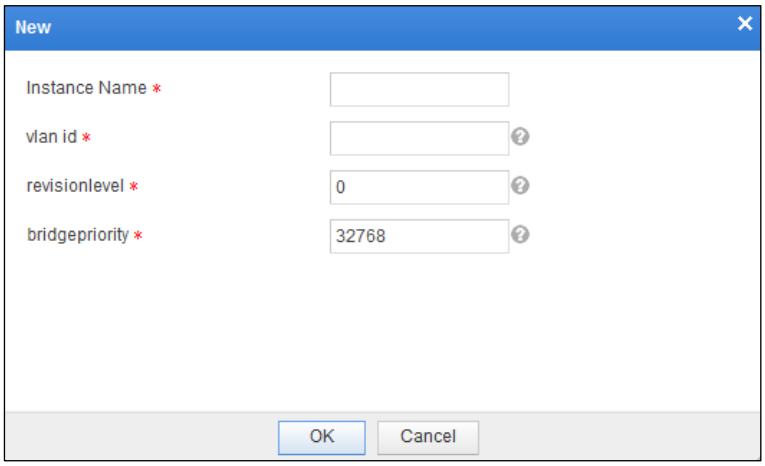


Table 5-17 describes parameters for creating an MST instance.

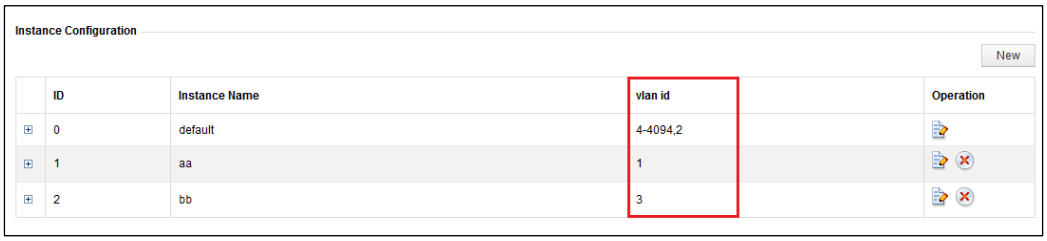
Table 5-17 Parameters for creating an MST instance

Parameter	Description
Instance Name	For other instances than instance 0, this parameter indicates the name of the instance. It has little meaning, and therefore no requirement is placed on its setting.
vlan id	ID of the VLAN mapped to this instance. The value can be one or more integers or a specific range within the range of 0–4094. Multiple VLAN IDs are separated by the comma (,). **One VLAN can map to only one instance. After a VLAN ID is assigned to a new instance, it is no longer mapped to instance 0.**
revisionlevel	Revision level of an MST region. All MST instances within a region should have the same revision level. The default value is **0**.
bridgepriority	Priority of the MST instance. The network bridge priority plays an importance role in selecting the root bridge of a spanning tree. Different MST instances can have different priorities. A smaller value indicates a higher priority. The value should be within the range of 0–61440 and a multiple of 4096, with **32768** as the default.

Click **OK** to save the settings.

The VLAN assigned to the new instance no long maps to instance 0, as shown in Figure 5-36.

Figure 5-36 Instance list after a new instance is created



c. Delete an instance.

Click in the **Operation** column of an instance and click **OK** in the confirmation dialog box.

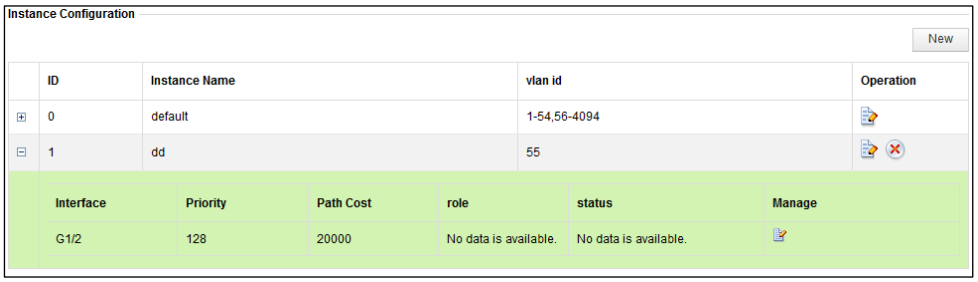
After an instance is deleted, the VLAN assigned to it is mapped to instance 0 again. For example, after instance 1 in Figure 5-36 is deleted, the VLAN assigned to it is remapped to instance 0.

Figure 5-37 Instance list after an instance is deleted

d. View interfaces involved in an instance.

Click to the left of an instance ID to check information about layer 2 interfaces configured for this instance.

Figure 5-38 Viewing layer 2 interfaces configured for an instance



Click in the **Operation** column to modify settings of an interface.

Figure 5-39 Editing MSTP parameter settings of an interface

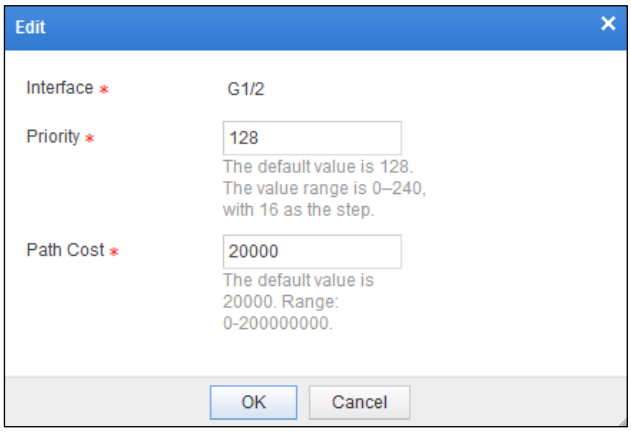


Figure 5-40 describes MSTP parameters of an interface.

Table 5-18 MSTP parameters of an interface

Parameter	Description
Priority	Specifies the priority of the interface in the current MST instance. The priority of this interface determines its role in an MST instance, which can be a designated port, root port, standby root port, or standby designated port. A standby root port and standby designated port discard packets, instead of forwarding them. A designated port and root generally forward packets. A smaller value indicates a higher priority.
Path Cost	Path cost of this layer 2 interface in the current MST instance. After proper path costs are set for interfaces, traffic of different VLANs can be forwarded along different physical links, achieving VLAN-based load balancing.

Click **OK** to save the settings.

Step 6 Enable MSTP.

On the page shown in Figure 5-32, click **Start** and then click **OK** in confirmation dialog box to restart the system engine.

Step 7 Apply the settings.

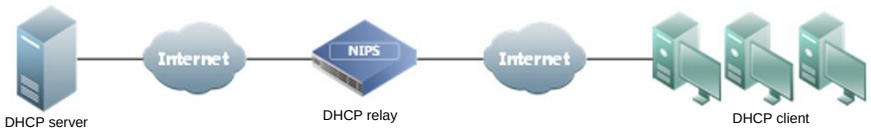
----End

5.5 DHCP

NIPS provides the DHCP relay service to users. A layer 3 interface on NIPS can be configured as a DHCP relay to receive DHCP information from the DHCP server and forwards such information to DHCP clients in any security zones.

Figure 5-40 shows the topology when NIPS works as a DHCP relay agent.

Figure 5-40 Topology in which NIPS acts as a DHCP relay



Note	NIPS NX5-T9010A and NX5-T9020A do not support the DHCP function.

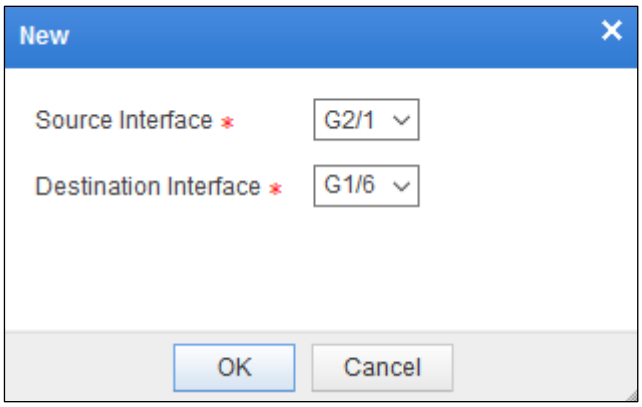
On NIPS, you can create, edit, search for, and delete DHCP relays. To create a DHCP relay, follow these steps:

Step 1 Choose **Network** > **DHCP** > **DHCP Relay**.

Figure 5-41 DHCP relay list

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

Figure 5-42 Creating a DHCP relay



Step 3 Configure parameters.

Table 5-19 Parameters for creating a DHCP relay

Parameter	Description
Source Interface	Specifies the interface that connects to DHCP clients. The interface can be a layer 3 Ethernet interface, layer 3 subinterface, or VLAN interface.
Destination Interface	Specifies the interface that connects to the DHCP server. The interface can be a layer 3 Ethernet interface, layer 3 subinterface, or VLAN interface.

Caution	**Source Interface** and **Destination Interface** cannot be set to the same interface.

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

Step 5 Apply the settings.

----End

5.6 DNS

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, NIPS can request the domain name translation service from a specified DNS server.

To configure DNS servers, follow these steps:

Step 1 Choose **Network** > **DNS** > **DNS Server Configuration**.

Figure 5-43 Configuring DNS servers

Step 2 Specify IP addresses of the DNS servers.

Step 3 Apply the settings.

----End

5.7 IP/MAC Binding

This module involves the configuration of static IP/MAC binding rules and cross-layer 3 IP/MAC binding rules to prevent unauthorized hosts from accessing a network using the IP address of an authorized host, thereby effectively avoiding IP address spoofing.

- NIPS NX5-T9010A and NX5-T9020A support the configuration of static IP/MAC bindings only.
- NIPS of other models:
  - Support static IP/MAC bindings.
  - Can obtain ARP entries from layer 3 switches via SNMP and check layer 3 IP/MAC bindings based on the entries.
  - Support the whitelist configuration. Whitelisted IP addresses or MAC addresses are free from checks.

This section describes how to configure IP/MAC binding rules.

5.7.1 Configuring IP/MAC Binding Entries

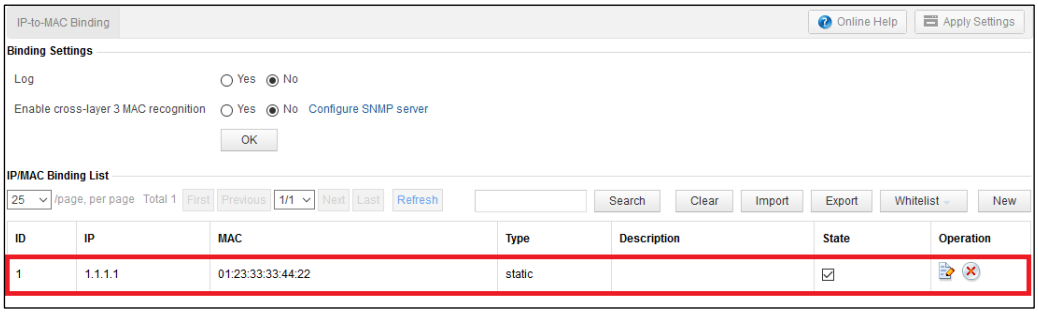
After static IP/MAC bindings are set, NIPS checks IP/MAC binding of packets according to the setting of **ipmac_strict** under **System > System Configuration > Parameter**.

- If **ipmac_strict** is set to **Yes**, NIPS only forwards packets whose source IP addresses and MAC addresses or destination IP addresses and MAC addresses exactly match static IP/MAC binding entries.
- If **ipmac_strict** is set to **No**, NIPS searches the static IP/MAC binding table for the source IP address of packets. Here are two situations:
  - If the source IP address is found but the bound MAC address is different from that of the packet, NIPS discards the packet.
  - If the source IP address is not found, NIPS forwards the packet.

To create an IP/MAC binding entry, follow these steps:

Step 1 Choose **Network > IP-to-MAC Binding**.

Figure 5-44 IP-to-MAC Binding page



Static IP/MAC binding entries are at the top of the IP/MAC binding list. Such entries have the following characteristics:

- Each static IP/MAC binding entry has a number. However, dynamic IP/MAC binding entries have no such numbers.

- **Type** is **static**.
- The **State** column shows whether static IP/MAC binding entries are enabled. Only enabled static entries can be used for IP/MAC binding checks. For how to enable or disable a static IP/MAC binding entry, see Enabling or Disabling a Static IP/MAC Binding Entry.
- Static IP/MAC binding entries can be edited. For details, see Editing a Static IP/MAC Binding Entry.
- Static IP/MAC binding entries can be deleted. For details, see Deleting a Static IP/MAC Binding Entry.

Step 2 Create a static IP/MAC binding entry.

You can create a static IP/MAC binding entry in one of the following ways:

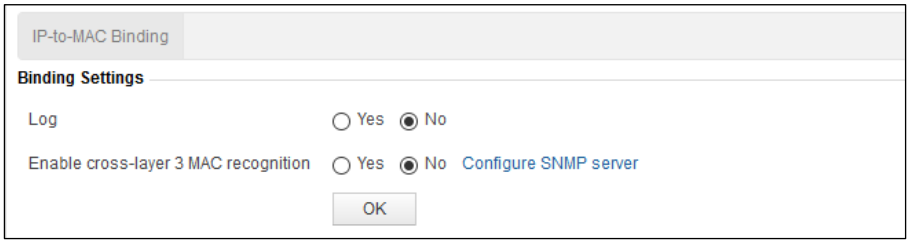
- Click **New** to the upper right of the IP/MAC binding list. For details, see Creating a Static IP/MAC Binding Entry.
- Bind a dynamic ARP entry in the ARP table. For details, see Binding ARP Entries.
- Confirm a dynamic (cross-layer 3) IP/MAC binding entry in the IP/MAC binding table. For details, see Confirming a Dynamic (Cross-Layer 3) IP/MAC Binding Entry.
- Import a file that contains static IP/MAC binding entries. For details, see Importing Static IP/MAC Binding Entries in Batches.

Step 3 Configure whether to record logs.

Based on static IP/MAC binding entries, NIPS performs IP/MAC binding checks for packets. If packets match no entries, NIPS blocks these packets.

On the page shown in Figure 5-45, **Log** under **Binding Settings** controls whether to generate an application management log for such a block event.

Figure 5-45 Log configuration



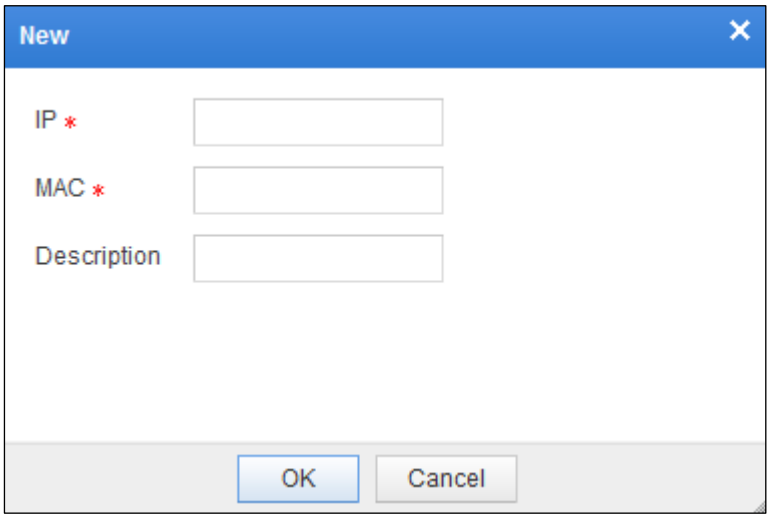
Step 4 Click **OK** to commit the settings.

----End

Creating a Static IP/MAC Binding Entry

Click **New** to the upper right of the IP/MAC binding list. In the **New** dialog box that appears, specify an IP address and MAC address and click **OK** to create a static IP/MAC binding entry.

Figure 5-46 Creating a static IP/MAC binding entry



Tip	• The specified IP address and MAC address cannot be the same as those included in existing IP/MAC binding entries. • The specified IP address cannot be the same as the IP address of NIPS's network gateway.

Confirming a Dynamic (Cross-Layer 3) IP/MAC Binding Entry

When cross-layer 3 MAC recognition is enabled, you can create a static IP/MAC binding entry by confirming a dynamic (cross-layer 3) entry in the IP/MAC binding list.

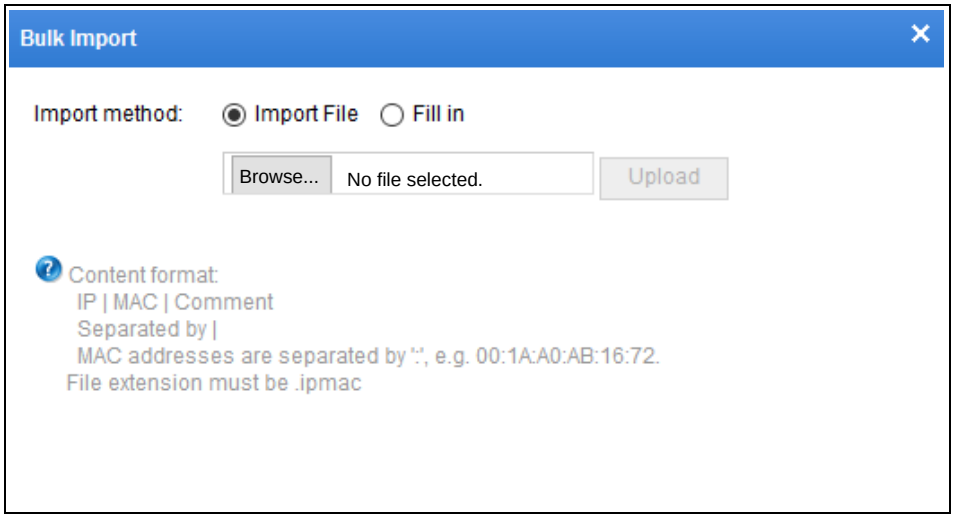
On the IP/MAC binding list shown in Figure 5-44, click in the **Operation** column of an entry with **Type** being **dynamic (cross-layer 3)** to configure the dynamic entry as a static one.

Importing Static IP/MAC Binding Entries in Batches

To the upper right of the IP/MAC binding list, click **Import** to import a file that contains multiple static IP/MAC bindings or manually type multiple bindings.

- File import: import static IP/MAC binding entries from a file.

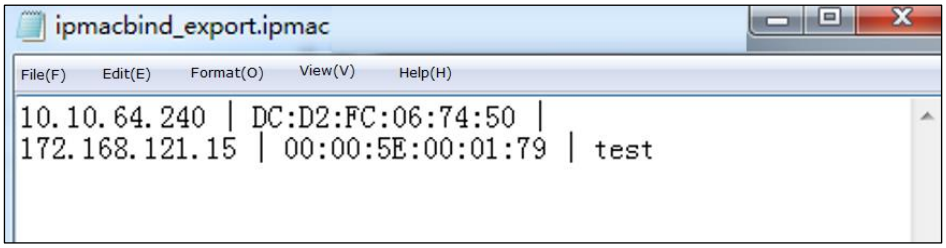
Figure 5-47 Importing static IP/MAC binding entries from a file



Select **Import File** for **Import method**, click **Browse** to select a local file that contains properly configured static ARP entries, and then click **Upload** to import the file. Such a file must meet the following conditions:

- The file must contain properly configured IP/MAC binding entries that are in the format of IP|MAC|description. That is, the IP address, MAC address, and description are separated by the vertical bar (|). In each MAC address, items are separated by the colon (:), for example, 00:1A:A0:AB:16:72. Note that even if there is no descriptive information in an IP/MAC binding entry, the MAC address must also be followed by a vertical bar (|). See Figure 5-48.
- The file name extension must be .ipmac.

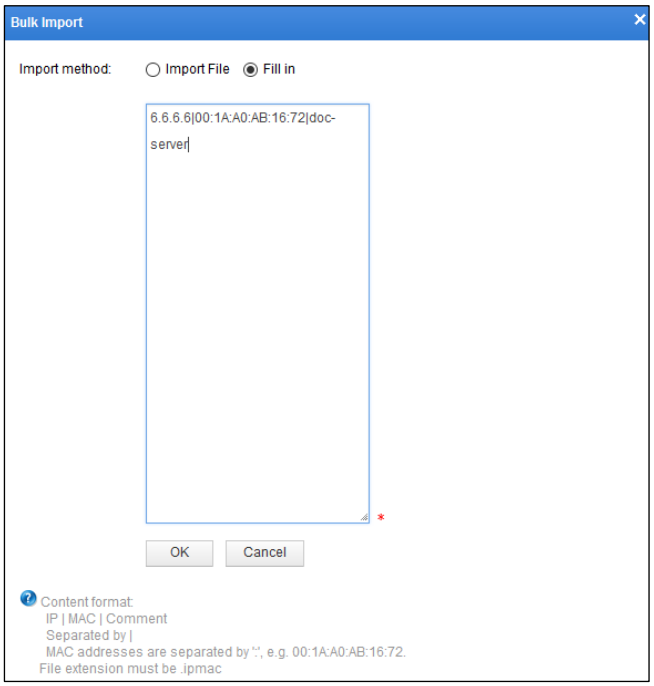
Figure 5-48 A file that contains static IP/MAC binding entries



Tip	• The IP address and MAC address in each IP/MAC binding entry to import cannot be the same as those in existing entries. • The IP address in each IP/MAC binding entry to import must not be the same as the IP address of NIPS's network gateway.

- Manual typing: Select **Fill in** for **Import Method**, type one or more static IP/MAC binding entries, and click **OK**.

Figure 5-49 Manually typing static IP/MAC binding entries



Each typed IP/MAC binding entry must be in the format of IP|MAC|description. That is, the IP address, MAC address, and description are separated by the vertical bar (|). In each MAC address, items are separated by the colon (:), for example, 00:1A:A0:AB:16:72. Note that even if there is no descriptive information in an entry, the MAC address must also be followed by a vertical bar (|).

Multiple static IP/MAC binding entries are separated by carriage returns, with each in a separate line.

Exporting Static IP/MAC Binding Entries

For IP/MAC binding entries with **Type** being **static**, you can click **Export** to export all these entries to a file for backup. Later, you can import static IP/MAC binding entries from the file to NIPS. For details, see Importing Static IP/MAC Binding Entries in Batches.

Editing a Static IP/MAC Binding Entry

You can click in the **Operation** column to edit an IP/MAC binding entry with **Type** being **static**.

Deleting a Static IP/MAC Binding Entry

You can click in the **Operation** column to edit an IP/MAC binding entry with **Type** being **static**.

Enabling or Disabling a Static IP/MAC Binding Entry

Static IP/MAC binding entries are enabled by default. Only enabled static entries can be used for IP/MAC binding checks.

To disable such a binding entry, deselect the check box in the **Status** column. To enable it, reselect the check box.

5.7.2 Configuring Cross-Layer 3 MAC Recognition

Based on the list of static IP/MAC bindings, IP/MAC binding checks can effectively prevent IP address embezzlement. However, when a user deploys a layer 3 switch in front of NIPS that connects to the Internet, after packets pass through the switch, the source MAC address of those packets is changed to that of the outbound interface of the switch. This makes impossible for NIPS to obtain the user's real MAC address, thus unable to conduct IP/MAC binding checks.

To solve this issue, NIPS V5.6R10F02 supports cross-layer 3-switch recognition of the MAC address of an intranet user. NIPS regularly obtains the ARP table on the layer 3 switch via SNMP, in order to get IP/MAC bindings of all PCs in the intranet. After that, the NIPS administrator sets cross-layer 3 dynamic IP/MAC binding entries as static entries before NIPS performs cross-layer 3 IP/MAC binding checks.

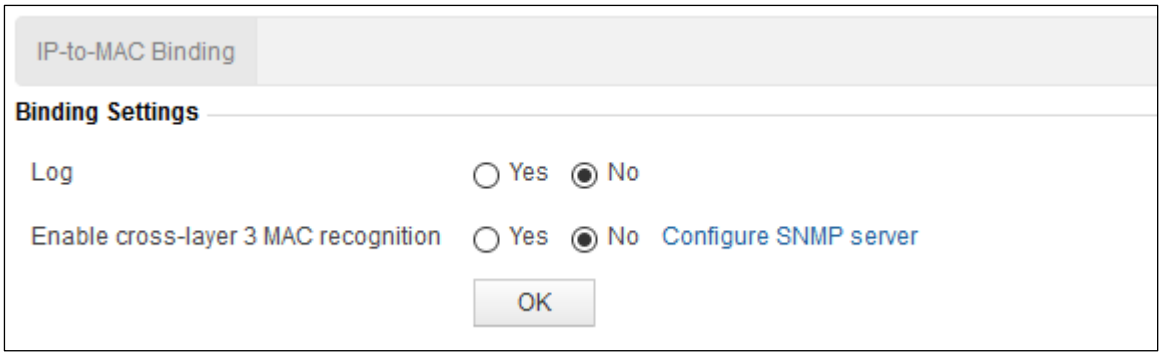
Note	The SNMP service must be enabled on the layer 3 switch before cross-layer 3 MAC recognition.

To configure the cross-layer 3 MAC recognition function, follow these steps:

Step 1 Choose **Network > IP-to-MAC Binding**.

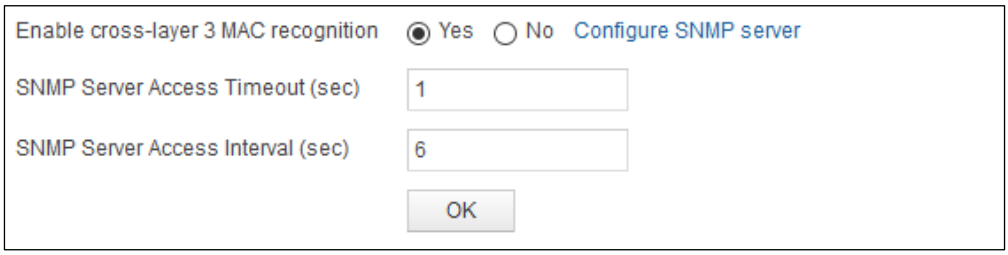
The cross-layer 3 MAC recognition function is disabled by default.

Figure 5-50 Configuring cross-layer 3 MAC recognition



Step 2 Set **Enable cross-layer 3 MAC recognition** to **Yes**.

Figure 5-51 Configuring parameters for cross-layer 3 IP/MAC binding



Step 3 Configure parameters for NIPS to make an SNMP query from the layer 3 switch that acts as an SNMP server.

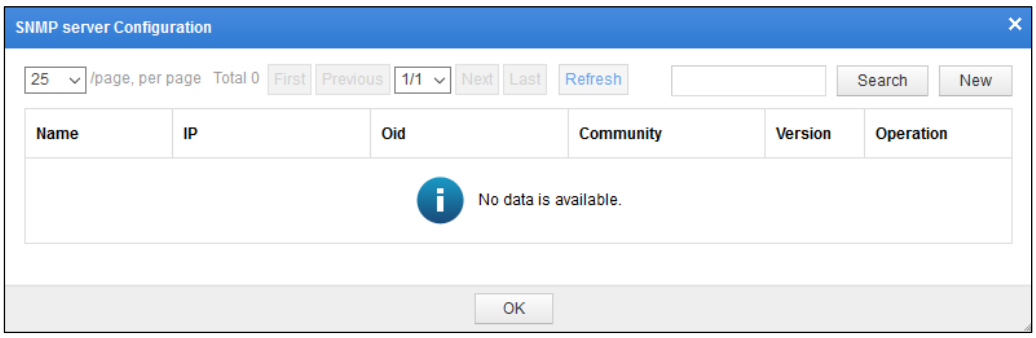
SNMP Server Access Timeout (sec): specifies the maximum interval for NIPS to wait for an ARP reply from the layer 3 switch. If no reply is received during the specified period, NIPS cannot the next request until the interval specified with **SNMP Server Access Interval (sec)** expires.
SNMP Server Access Interval (sec): specifies how long NIPS has to wait before sending the next ARP request to the layer 3 switch.

Step 4 Configure an SNMP server.

Note that if there is more than one layer 3 switch in the intranet, you need to configure multiple SNMP servers on NIPS so that the device can obtain ARP tables from all these switches through SNMP queries.

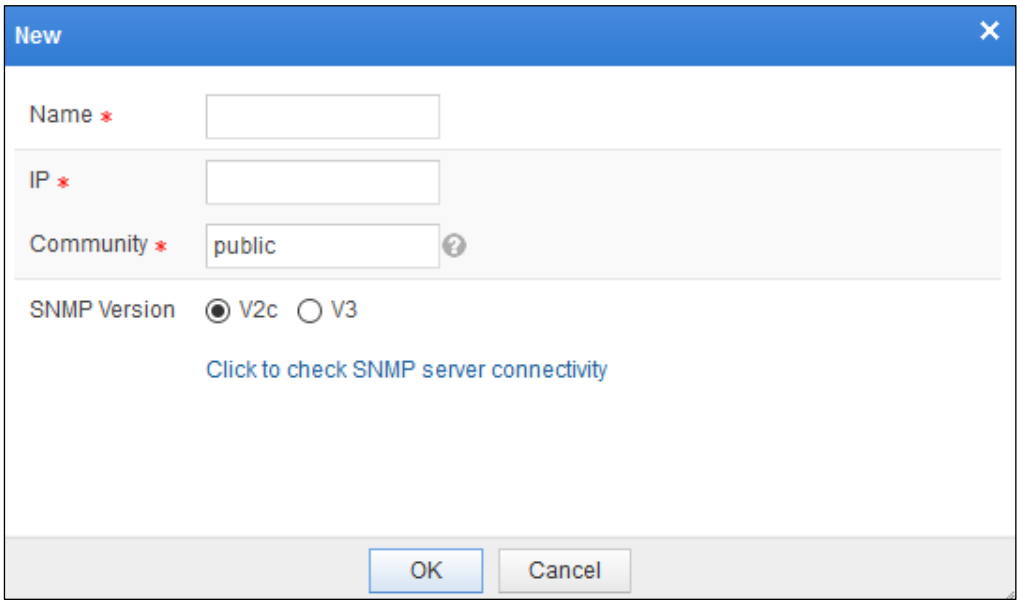
a. Click **Configure SNMP Server** to configure a layer 3 switch.

Figure 5-52 Configuring an SNMP server



b. Click **New** in the upper-right corner of the page to configure an SNMP server

Figure 5-53 Configuring an SNMP server



c. Configure parameters in the **New** dialog box.

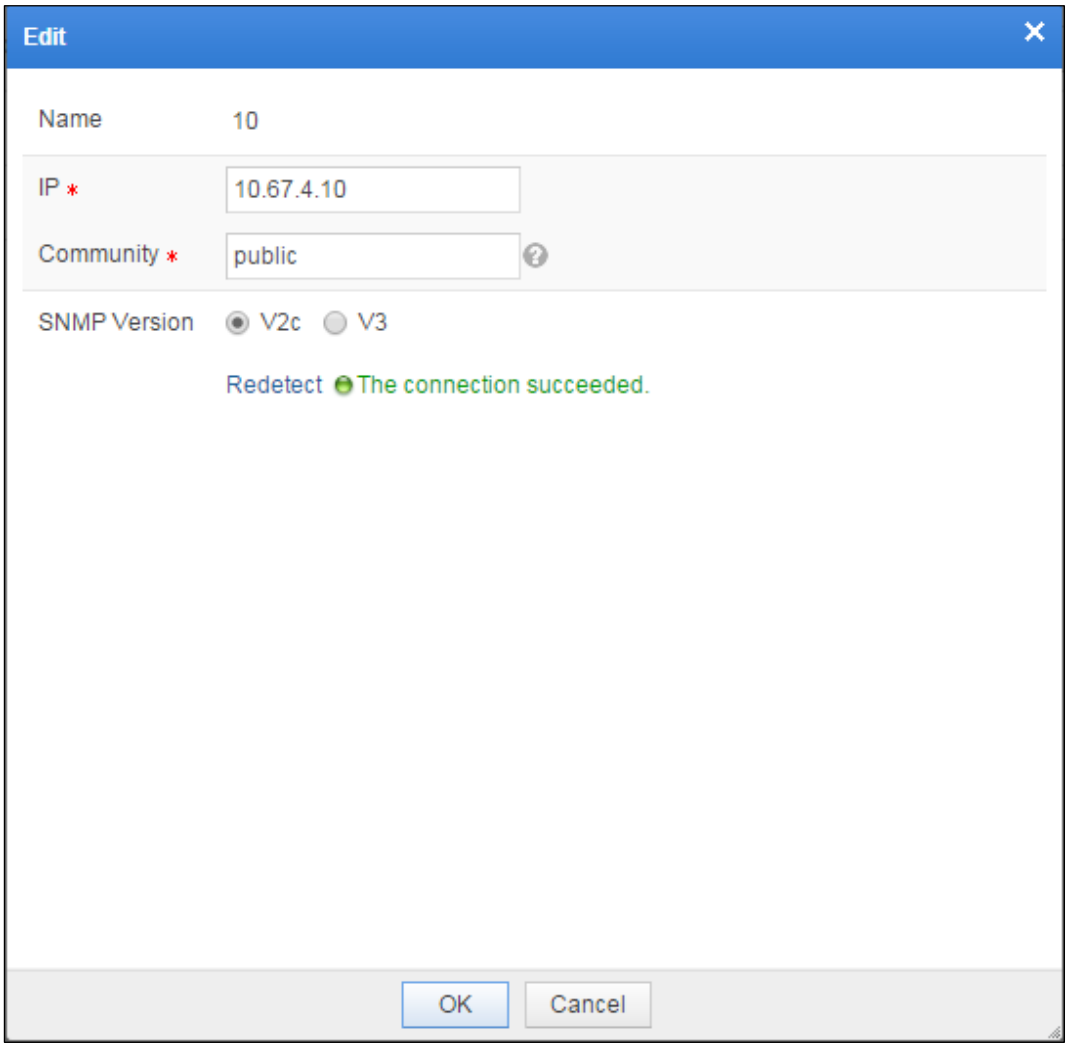
Table 5-20 Parameters for configuring an SNMP server

Parameter	Description
Name	Name of the layer 3 switch, which is the switch identity.
IP	IP address of the switch's nearest port to NIPS.
Community	Community used by NIPS to communicate with the layer 3 switch via SNMP. NIPS and the layer 3 switch must use the same community for communication; otherwise, SNMP query packets from NIPS will be discarded by the switch.
SNMP Version	SNMP version supported by the layer 3 switch. The SNMP version must be V2C or V3, otherwise cross-layer 3 MAC recognition is not supported.

d. Check the status of the connection between NIPS and the SNMP server.

Click **Click to check SNMP server connectivity** to check whether NIPS can connect to the layer 3 switch. If the connection succeeds, **Connection succeeded** appears; otherwise, **Connection failed** is displayed.

Figure 5-54 Checking the status of the connection to the SNMP server



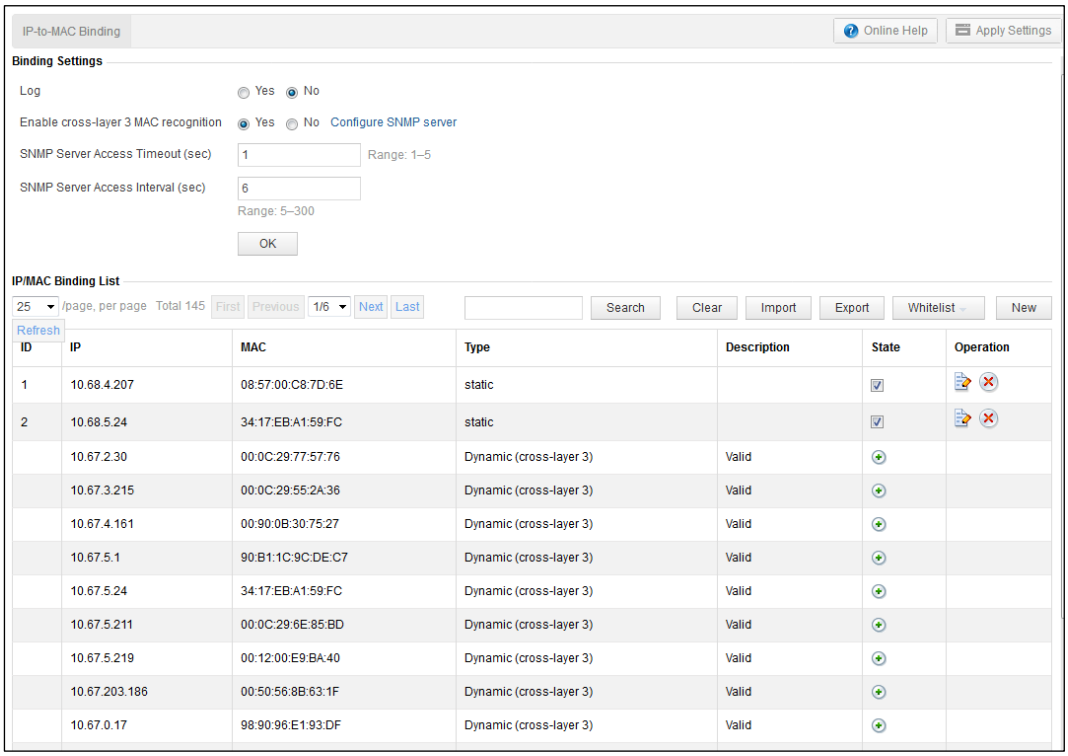
e. Click **OK** to complete the configuration.

Step 5 Apply the settings.

Step 6 Check ARP entries obtained from the layer 3 switch.

ARP entries obtained from the layer 3 switch are of the **dynamic (cross-layer 3)** type.

Figure 5-55 Checking ARP entries obtained from the layer 3 switch



Step 7 Add static IP/MAC binding entries.

Dynamic (cross-layer 3) ARP entries can be used for cross-layer 3 IP/MAC binding checks only after they are added as static IP/MAC binding entries. For details, see Confirming a Dynamic (Cross-Layer 3) IP/MAC Binding Entry.

----End

5.7.3 Configuring the Whitelist

During IP/MAC binding checks, NIPS forwards packets destined for IP addresses or MAC addresses included in the whitelist, without any checks. Therefore, the whitelist has the highest priority during IP/MAC binding checks.

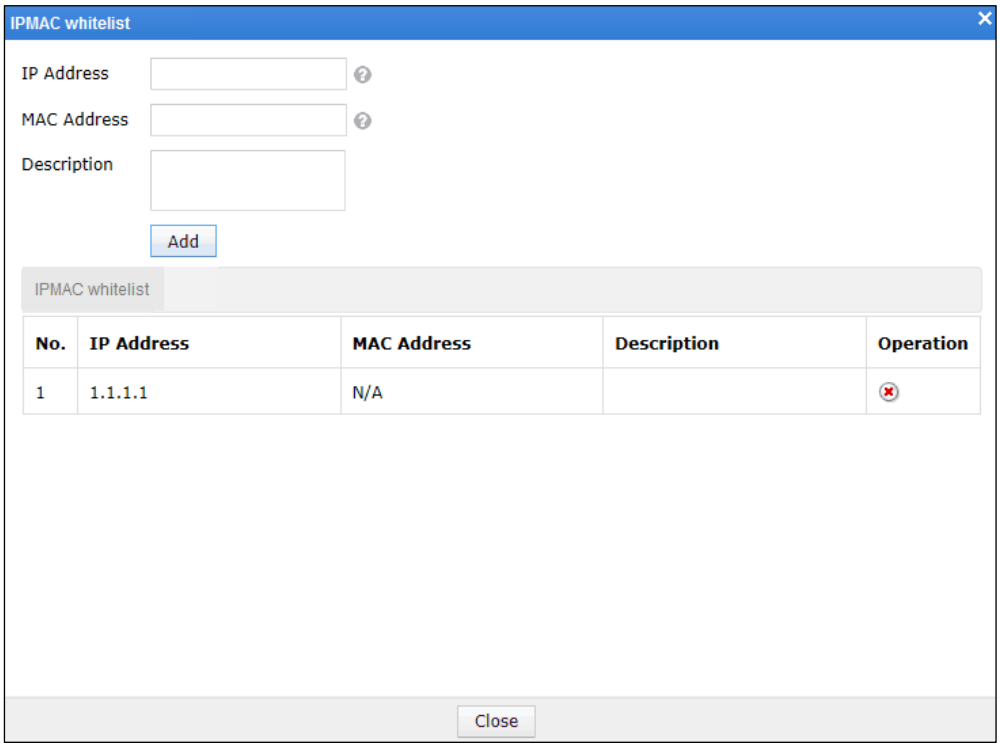
You can create, view, import, export, and delete whitelist entries.

Adding/Viewing Whitelist Entries

Step 1 Choose **Network** > **IP-to-MAC Binding**.

Step 2 Click **Whitelist** to the upper right of the IP/MAC binding list and select **Create/View**.

Figure 5-56 Adding/viewing whitelist entries



The IP/MAC whitelist below shows all whitelisted IP addresses and MAC addresses.

Step 3 Type an IP address or MAC address and then click **Add** to add it to the whitelist.

----End

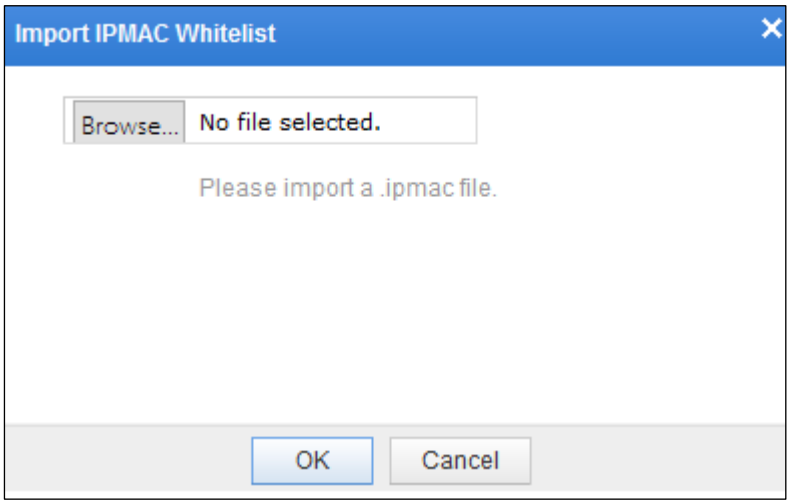
Deleting a Whitelist Entry

On the page shown in Figure 5-56, click in the **Operation** column to delete a whitelist entry.

Importing Whitelist Entries in Batches

Click **Whitelist** to the upper right of the IP/MAC binding list and select **Import Whitelist** to import a file that contains multiple whitelist entries.

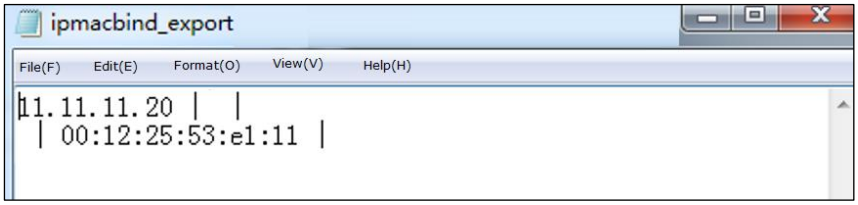
Figure 5-57 Importing a file that contains whitelist entries



Click **Browse** to select a local file that contains whitelist entries and then click **OK** to import the file. Such a file must meet the following conditions:

- The file must contain IP/MAC binding entries in the format of IP|MAC|description. That is to say, the IP address, MAC address, and description are separated by the vertical bar (|). For each entry, either an IP address or MAC address must be contained. In each MAC address, items are separated by the colon (:), for example, 00:1A:A0:AB:16:72.
- The file name extension must be .ipmac.

Figure 5-58 File that contains whitelisted IP addresses and MAC addresses



Tip	The file to import cannot contain whitelisted IP addresses or MAC addresses that already exist on NIPS. Otherwise, the file import fails.

Exporting the Whitelist

To the upper right of the IP/MAC binding list, click **Whitelist** and select **Export Whitelist** to export all whitelist entries to a file for backup. Later, you can import this file to NIPS.

5.8 Route

Routing refers to the process of selecting the best paths from a routing table for transmitting packets across networks from a source IP address to a destination IP address. The routing occurs at the network layer. As packets at the network layer are IP packets, the routing is also called IP routing.

Packets may pass through one or more intermediate nodes during routing. Routers are major intermediate nodes on the Internet. Like a transfer station on the Internet, a router directs IP packets to the next-hop device.

Route-related concepts also include routing table, administrative distance, metric, and route matching.

Routing Table

A routing device is used to direct packets passing through it to the next-hop routing device or destination host. For this purpose, each routing device maintains the information required for packet forwarding. Such information constitutes a routing table. A routing table can be generated by the system (using dynamic routes) or configured by the administrator (using static routes). Generally, a routing table contains the following information:

- Destination IP address of packets
- Next-hop routing device or IP addresses that are directly connected to the network
- Other supplementary information for packet forwarding

Administrative Distance

Administrative distance (AD) defines the priority of various routes. It is an integer from 0 to 255. The lower the AD is, the more reliable the route is. By virtue of AD, a router selects the best path as follows: When receiving information about several matching routes of different protocols, the router will check their ADs, select the route with the lowest AD as the trustworthy one, and insert it into the router's routing table for packet forwarding.

Metric

You can set the metric to achieve a reasonable traffic distribution among multiple links in load balancing mode. A link with a lower metric is more trustworthy and also assigned a larger traffic. For example, the metrics of two equal-cost routes are respectively 1 and 2. The traffic weights of the two links in load balancing mode are calculated as follows:

Traffic weight of the link with the metric of 1: 2/1=2 Traffic weight of the link with the metric of 2: 2/2=1 You can see that the traffic weight of the link with metric of 1 is double that of the link with metric of 2.

For a reasonable traffic distribution, you can set an appropriate traffic weight for each link to the next-hop routing devices. In this case, when one link to the next-hop routing device fails, the traffic can be transmitted along other links, ensuring continuous network availability.

Route Matching

The route matching principles are as follows:

1. Policy-based routes have the highest priority, static routes come second, and ARP translation comes last.

2. **Longest mask matching**: If the destination IP address is involved in multiple networks, the route with the longest subnet mask is preferred.

3. **Lowest administrative distance**: If the routes have the same subnet mask, the router selects the route with the lowest AD.

Note	If a static route has the same AD as that of a dynamic route, the AD of the static route is considered to be the default value **1**.

NIPS provides the layer 3 routing function and supports three types of routes: static routes, policy-based routes, and ARP table.

Note	NIPS NX5-T9010A and NX5-T9020A do not support policy-based routing or ARP table.

5.8.1 Static Route

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

Default routes are a special type of static routes, with 0.0.0.0/0 as the destination IP address. The routing device uses a default route to forward packets for which no matching route is found in the routing table. If no default route is configured, the routing device will drop such packets.

Currently, NIPS supports both IPv4 and IPv6 static routes. Similar to IPv4 static routes, IPv6 static routes are suitable for IPv6 networks with a simple structure. The major difference lies in the destination address and next-hop address. That is, IPv6 static routes use IPv6 addresses, while IPv4 static routes use IPv4 addresses.

Note	• When configuring an IPv4 static route, you can configure a default route by specifying 0.0.0.0 as the destination address and 0.0.0.0 as the subnet mask. If the destination address of IPv4 packets fails to match any route in the routing table, these packets are forwarded via the default IPv4 route. • When configuring an IPv6 static route, you can configure a default route by specifying ::/0 (the prefix length is 0) as the destination address. If the destination address of IPv6 packets fails to match any route in the routing table, these packets are forwarded via the default IPv6 route.

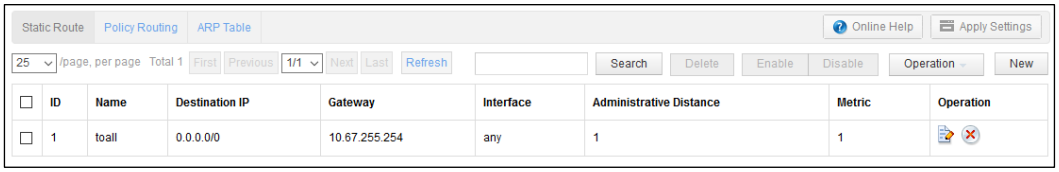
On NIPS, you can create, edit, enable, disable, search for, import, export, delete, and clear static routes.

To create a static route, follow these steps:

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

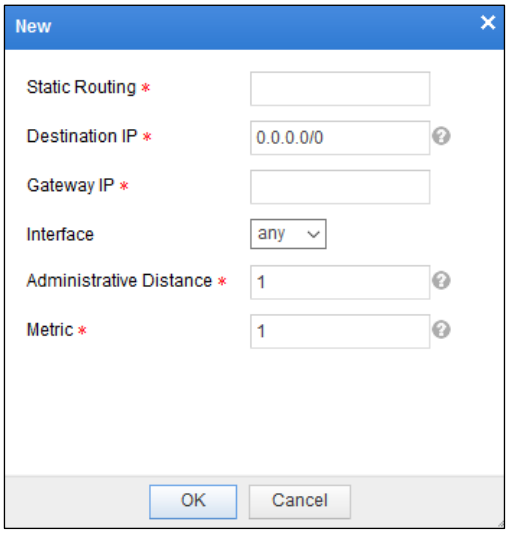
The **Static Route** page appears, as shown in Figure 5-59.

Figure 5-59 List of static routes



Step 2 Click **New** in the upper-right corner.

Figure 5-60 Creating a static route



Step 3 Configure parameters in the **New** dialog box.

Table 5-21 Parameters for configuring a static route

Parameter	Description
Static Routing	Specifies the name of the static route, which cannot contain spaces and the following special characters: / % \ { } ` @ ^ < > ' & " :
Destination IP	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 the destination IP address is 0.0.0.0/0 or ::/0, it indicates that this route is a default one based on which NIPS sends/forwards packets if no route matches the destination IP address of such packets in the routing table.
Gateway IP	Specifies the gateway for the static route, usually, the local IP address of the next-hop device.

Parameter	Description
Interface	Specifies the egress interface of the static route.
Administrative Distance	Specifies the priority of the static route, which is an integer from 1 to 255. A smaller value indicates a higher priority. Setting the route priority aims at achieving load balancing among links with the same administrative distance to the destination.
Metric	Specifies the session weight of the static route for achieving load balancing among multiple links. The value range is 1–65535. The weight is the proportion of sessions distributed to each next-hop routing device. A higher weight indicates a larger proportion of sessions.

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

Step 5 Apply the settings.

----End

5.8.2 Policy-based Route

Policy-based routing (PBR) is a routing mechanism based on user-defined policies. PBR routes need to be manually configured by the administrator. Unlike destination-based static routes, PBR routes give you flexible means of routing packets based on the source IP address, destination IP address, and service of packets.

PBR routes takes precedence over other routes. That is to say, NIPS matches the received packets against PBR routes first. If no matching PBR route is found, NIPS searches for a static route for packet forwarding.

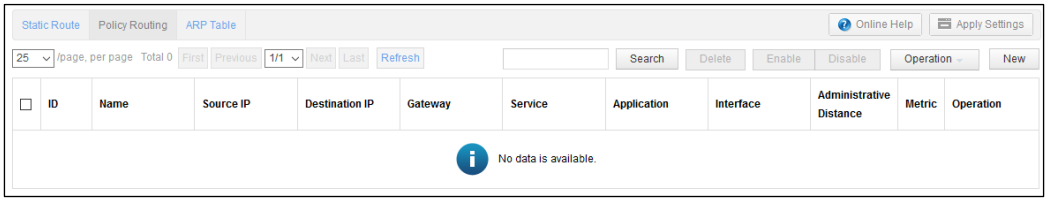
Note	NIPS NX5-T9010A and NX5-T9020A do not support policy-based routing.

You can create, edit, search for, enable, disable, import, export, delete, and clear policy-based routes.

To configure a policy-based route, perform the following steps:

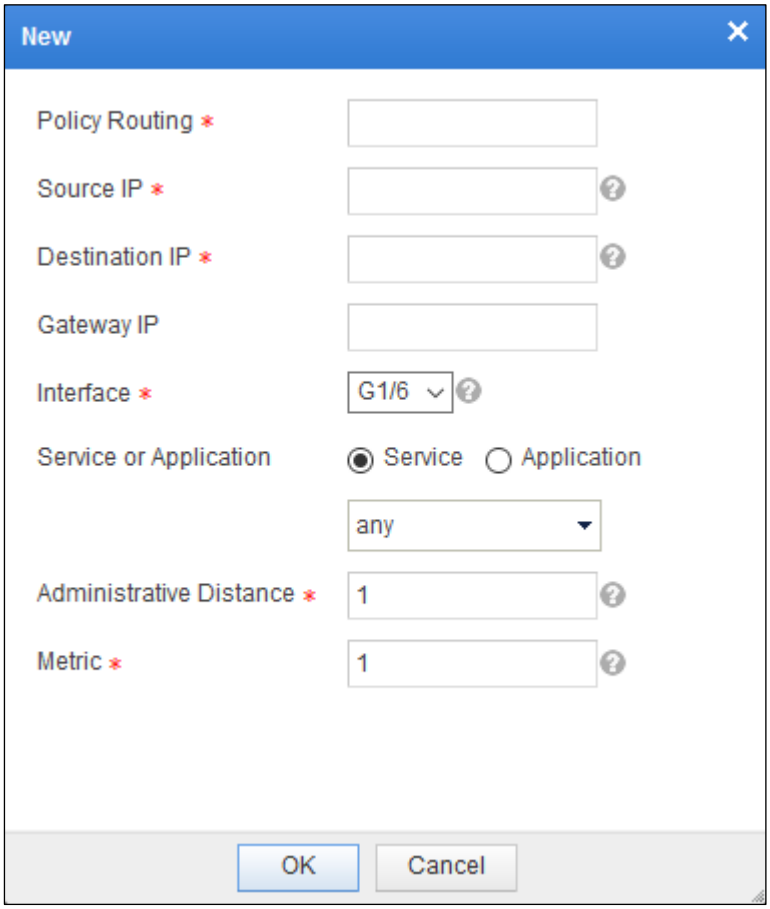
Step 1 Choose **Network** > **Route** > **Policy Routing**.

Figure 5-61 Policy-based routing page



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

Figure 5-62 Creating a policy-based route



Step 3 In the **New** dialog box, configure parameters.

Table 5-22 Parameters for configuring a policy-based route

Parameter	Description
Policy Routing	Name of the new policy-based route.
Source IP	Specifies the IP address of the source host or the source network segment from which packets are sent. The address format is "IP address/subnet mask length".
Destination IP	Specifies the IP address of the destination host or the destination network segment to which packets will be sent. The address format is "IP address/subnet mask length".
Gateway IP	Specifies the next-hop IP address of the outbound interface.
Service or Application	Specifies the service or application based on which packets are routed.

Parameter	Description
	• **Service**: Packets are routed based on services at the transport layer. You can select services from the drop-down box. **any** indicates that any service matches this route. • **Application**: Packets are routed based on various applications. You can select one or more applications from the drop-down box.
Interface	Specifies the outbound interface from which packets are sent. It can be a layer 3 interface.
Administrative Distance	Specifies the priority of the policy-based route, which is an integer from 1 to 255. A smaller value indicates a higher priority. Setting the route priority aims at achieving load balancing among routes with the same administrative distance to the destination.
Metric	Specifies the session weight of the route for achieving load balancing among multiple links. The value range is 1–65535. The weight is the proportion of sessions distributed to each next-hop routing device. A higher weight indicates a larger proportion of sessions.

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

Step 5 Apply the settings.

----End

5.8.3 ARP Table

Address Resolution Protocol (ARP) is a protocol for resolution of IP addresses on the network layer into MAC addresses on the data link layer. The ARP table records one-to-one mappings between IP addresses and MAC addresses, offering guidance for layer 3 packet forwarding.

With ARP, NIPS resolves a destination IP address of a packet into a destination MAC address and adds the address mapping as a dynamic ARP entry. Such an ARP entry offers a guidance for the forwarding of packets with the same destination IP address. Also, you can bind the IP address and MAC address within an ARP entry to create an IP/MAC binding entry.

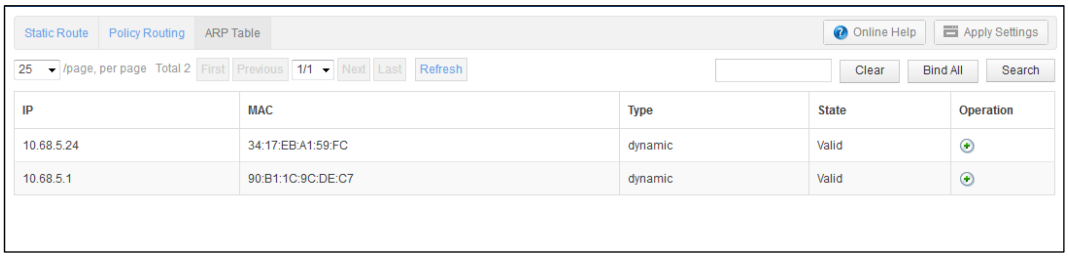
Note	NIPS NX5-T9010A and NX5-T9020A do not support the ARP table configuration.

Viewing ARP Entries

To view ARP entries learned by NIPS, follow these steps:

Step 1 Choose **Network** > **Route** > **ARP Table**.

Figure 5-63 ARP Table page



The **ARP Table** page presents dynamic ARP entries automatically generated and maintained by NIPS according to ARP packets. Such entries are updated in a dynamic way and can age as well.

Dynamic IP/MAC bindings can be in the following states in the ARP table:

- Valid: Real and valid IP/MAC bindings.
- Being resolved: The IP address is being resolved into a MAC address.
- Invalid: The IP address fails to be resolved into a MAC address. The resolution will start again when the next packet destined for the IP address is received by NIPS.

Search for ARP Entries

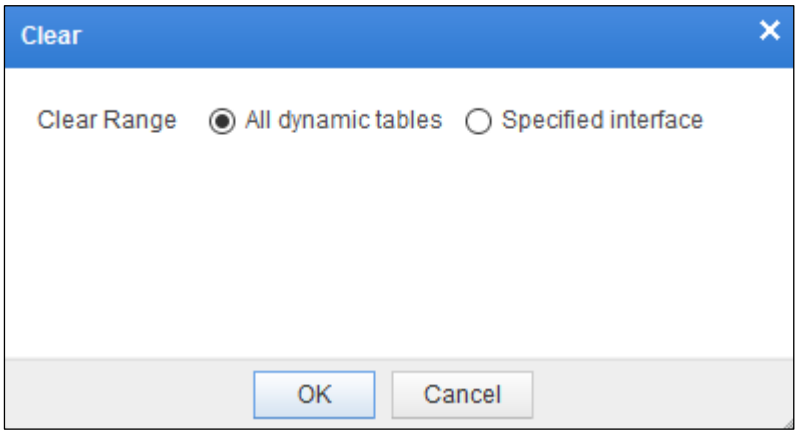
If these are many ARP entries in the ARP table shown in Figure 5-63, you can search for desired entries according to the IP address, MAC address, type, or status of entries.

In the upper right of the ARP table shown in Figure 5-63, you can type a specific search condition in the text box, and click **Search** to search for desired ARP entries. Also, you can click ✖ in this text box to clear the search condition. After that, all IP/MAC bindings are listed.

Clearing ARP Entries

In the upper right of the ARP table shown in Figure 5-63, you can click **Clear** to clear all dynamic ARP entries or those of a specified interface (a layer 3 interface, subinterface, or VLAN interface).

Figure 5-64 Clearing IP/MAC bindings



Then click **OK** to clear ARP entries of the selected type.

Binding ARP Entries

You can bind valid and invalid dynamic ARP entries in the ARP table to create static IP/MAC binding entries. IP/MAC binding entries created in this way can be viewed only under **Network > IP-to-MAC Binding**. For details, see section 5.7 IP/MAC Binding.

On the ARP table shown in Figure 5-63, you can click in the **Operation** table to configure an ARP entry as an IP/MAC binding entry.

Also, you can click **Bind All** in the upper right of the ARP table to configure all qualified dynamic ARP entries as IP/MAC binding entries.

5.9 Network Management

Network management configuration involves SNMP and the syslog server.

5.9.1 SNMP

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

NIPS supports SNMPv3, and is compatible with SNMPv1 and SNMPv2. When conducting network query on NIPS via SNMPv1 or SMNPv2, you only need to configure the community string. However, the transferred authentication and management data is not encrypted and no identification mechanism is available for data receiving and sending, exposing the network to security risks. When conducting network query on NIPS via SNMPv3, the transmitted messages are encrypted with the DES or AES symmetric-key algorithm. In addition, the key is configured for user identification on NIPS, enhancing the security of SNMP management on NIPS.

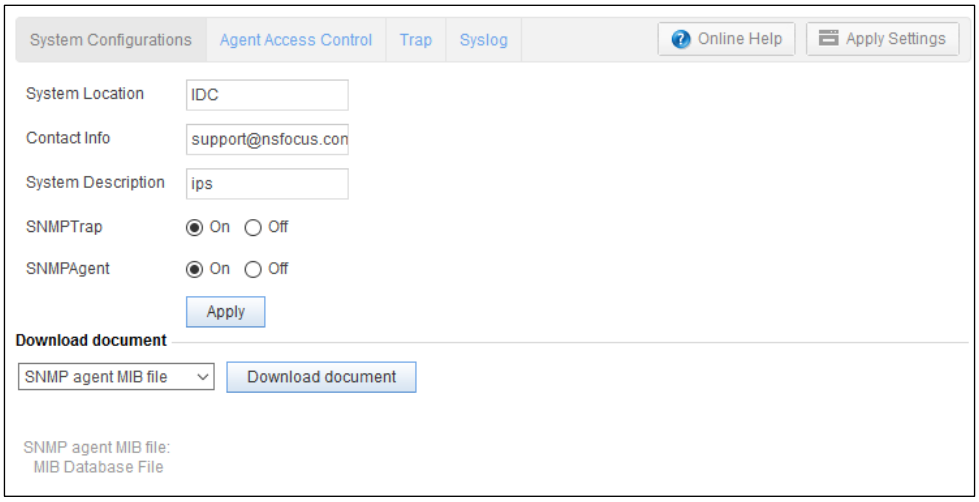
NIPS supports mainstream SNMP management software, such as MIB Browser and Solarwinds.

5.9.1.1 System Configuration Information

NIPS supports SNMP management only after being properly configured. To configure NIPS to support SNMP management, follow these steps:

Step 1 Choose **Network** > **Network Configuration** > **System Configurations**.

Figure 5-65 System configuration



Step 2 Configure parameters.

Table 5-23 SNMP system configuration parameters

Parameter	Description
System Location	Specifies the location of NIPS in the network environment.
Contact Info	Specifies the contact method of the person in charge of NIPS. It can be a telephone number or an email address. By default, the email address of NSFOCUS customer service is displayed.
System Description	Brief description of NIPS.
SNMPTrap	Controls whether to enable NIPS to proactively send alerts to the SNMP host. After it is enabled, the setting configured in section 5.9.1.3 Trap takes effect.
SNMPAgent	Controls whether to enable NIPS to accept management from the SNMP manager. After it is enabled, the setting configured in section 5.9.1.2 Agent Access Control takes effect.

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

----End

NIPS supports download of SNMP agent MIB files and SNMP trap-related documents. In the **Download document** area, select a file from the drop-down list and then click **Download document** to download this file to the specified local directory.

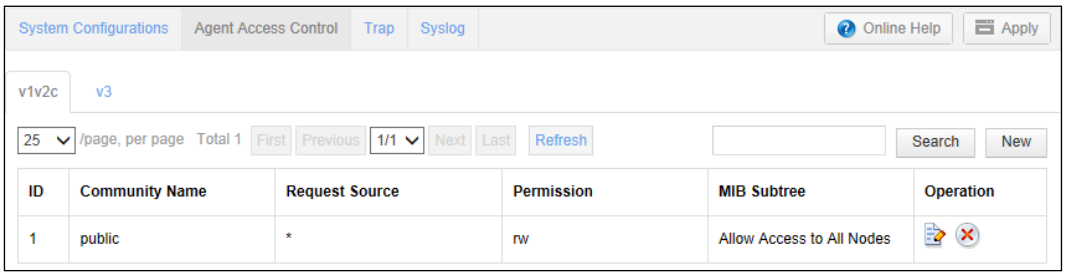
5.9.1.2 Agent Access Control

The SNMP manager performs SNMP management and generates SNMP alerts only after the SNMP agent service is enabled and agent access control parameters are properly configured. For how to enable the SNMP agent service, see section 5.9.1.1 System Configuration Information.

To configure agent access control parameters, follow these steps:

Step 1 Choose **Network** > **Network Configuration** > **Agent Access Control**.

Figure 5-66 Agent Access Control page



Step 2 Click **New** in the upper-right corner.

Figure 5-67 Configuring agent access control – SNMPv1 and v2c

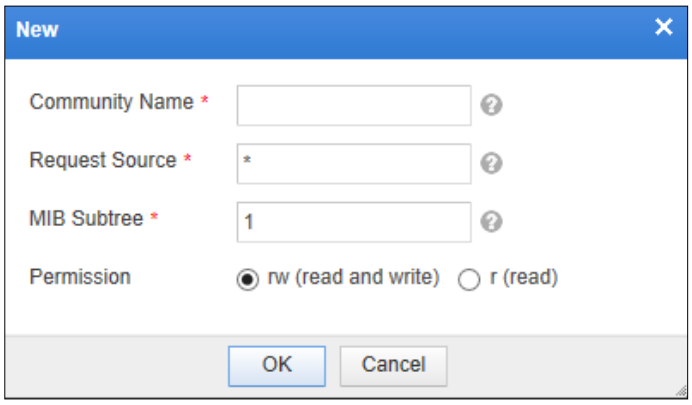
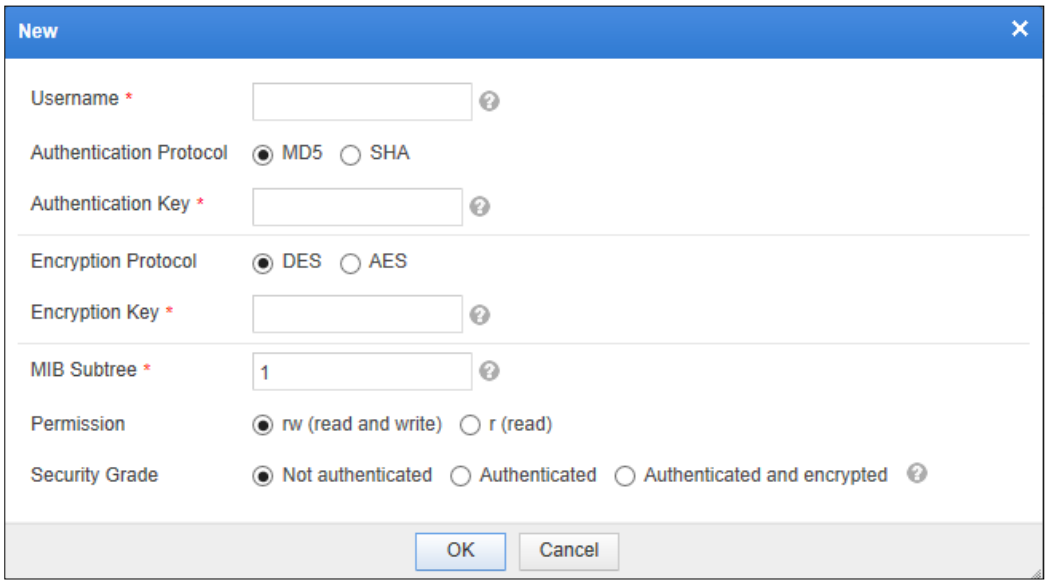


Figure 5-68 Configuring agent access control – SNMPv3



Step 3 Configure parameters in the **New** dialog box.

Table 5-24 Parameters for configuring agent access control (SNMPv1 and v2c)

Parameter	Description
Community Name	Specifies the community string used by NIPS for accessing the SNMP manager after the SNMP agent is enabled on NIPS.
Request Source	Specifies the source IP address of the SNMP manager.
MIB Subtree	Specifies the SNMP manager's permissions to access the MIB subtree on NIPS. The access permissions are controlled by means of the object identifier (OID). **1** indicates access permissions to all nodes. You can type other values such as 1.3.6.1.4.1.19849.2.
Permission	Specifies the SNMP manager's permissions to the MIB subtree on NIPS, which can be **rw (read and write)** or **r (read)**.

Table 5-25 Parameters for configuring agent access control (SNMPv3)

Parameter	Description
Username	Specifies the SNMPv3 user name.
Authentication Protocol	Specifies the protocol used for authentication, which can be **MD5** or **SHA**.
Authentication Key	Specifies the key used for authentication.
Encryption Protocol	Specifies the encryption algorithm used for transmitting messages, which can be **DES** or **AES**.
Encryption Key	Specifies the key used for encryption.

Parameter	Description
MIB Subtree	Specifies the SNMP manager's permissions to access the MIB subtree on NIPS. The access permissions are controlled by means of OID. **1** indicates access permissions to all nodes. You can type other values such as 1.3.6.1.4.1.19849.2.
Permission	Specifies the SNMP manager's permissions to the MIB subtree on NIPS, which can be **rw (read and write)** or **r (read)**.
Security Grade	Specifies the minimum security level for a user's access, which can be **Not authenticated**, **Authenticated**, or **Authenticated and encrypted**.

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

Step 5 Apply the settings.

----End

5.9.1.3 Trap

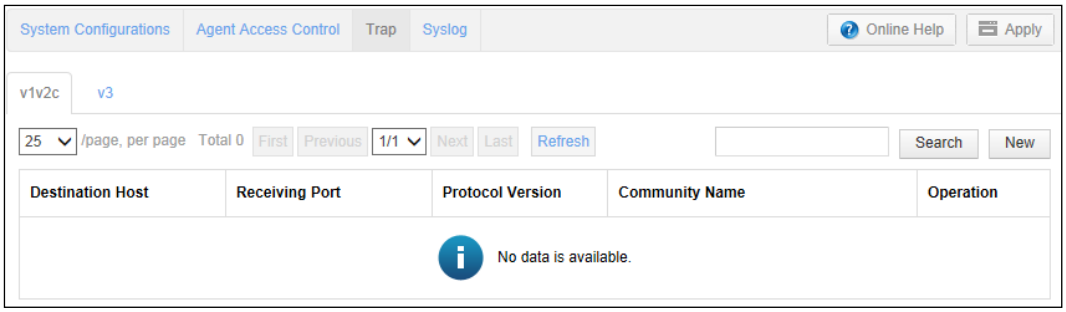
Trap is a message for proactive reporting. As an SNMP agent, NIPS can send messages about its own situations to the SNMP manager proactively, instead of being requested to do so.

NIPS can send information about its status to the SNMP manager only after the SNMP trap service is enabled and related parameters are properly configured.

For how to enable the SNMP trap service, see section 5.9.1.1 System Configuration Information. To configure SNMP trap parameters, follow these steps:

Step 1 Choose **Network** > **Network Configuration** > **Trap**.

Figure 5-69 SNMP Trap page



Step 2 Click **New** in the upper-right corner.

Figure 5-70 Configuring SNMPv1/v2c trap

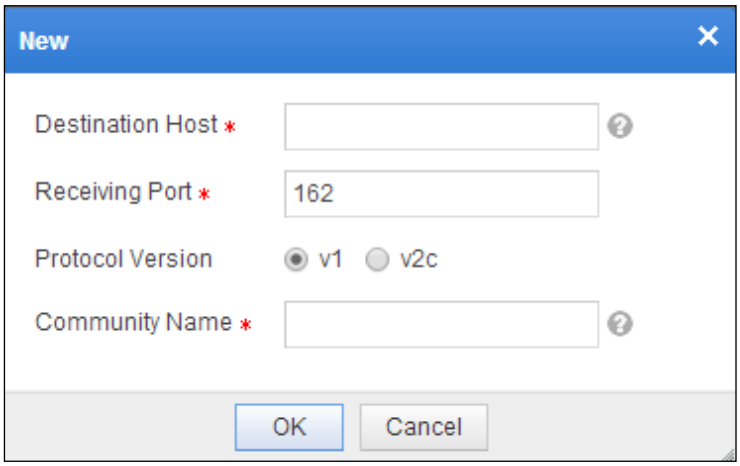
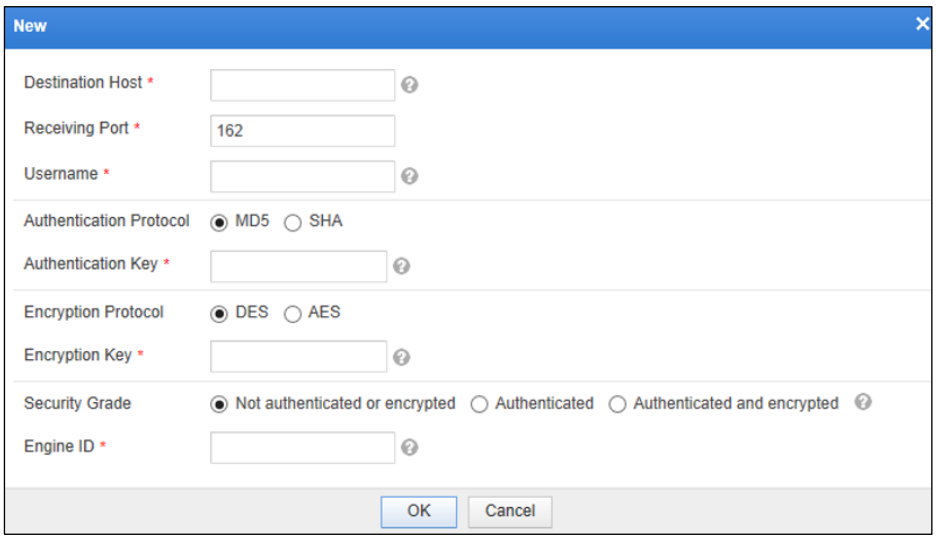


Figure 5-71 Configuring SNMPv3 trap



Step 3 Configure SNMP trap parameters.

Table 5-26 Parameters for configuring SNMPv1/v2c trap

Parameter	Description
Destination Host	Specifies the host that receives the SNMP trap alerts sent by NIPS. You can type an IPv4 or IPv6 address, for example, 192.168.1.0 or 2001:abcd:123:1::.
Receiving Port	Specifies the port for receiving SNMP trap alerts.
Protocol Version	Specifies the version of the SNMP protocol, which can be **v1** or **v2c**.
Community Name	Specifies the community string of the host for receiving SNMP trap alerts.

Table 5-27 Parameters for configuring SNMPV3 trap

Parameter	Description
Destination Host	Specifies the host that receives the SNMP trap alerts sent by NIPS. You can type an IPv4 or IPv6 address, for example, 192.168.1.0 or 2001:abcd:123:1::.
Receiving Port	Specifies the port for receiving SNMP trap alerts.
Username	Specifies the SNMPv3 user name.
Authentication Protocol	Specifies the protocol used for authentication, which can be **MD5** or **SHA**.
Authentication Key	Specifies the key used for authentication.
Encryption Protocol	Specifies the encryption algorithm used for transmitting messages, which can be **DES** or **AES**.
Encryption Key	Specifies the key used for encryption.
Security Grade	Specifies the minimum security level for a user's access, which can be **Not authenticated**, **Authenticated**, or **Authenticated and encrypted**.
Engine ID	Specifies the ID of the SNMP engine. The ID is a string of 16 hexadecimal digits, for example, 0x8000000001020304.

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

----End

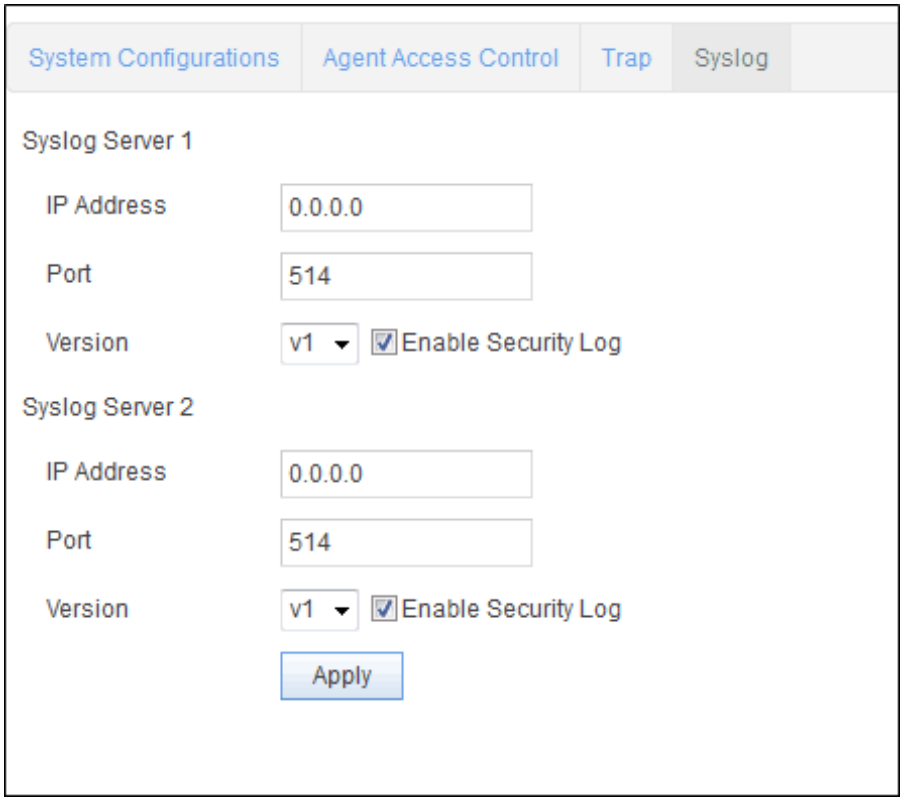
5.9.2 Syslog

The local storage space of NIPS is limited. To save more logs, you need to configure NIPS to send logs to the syslog server for storage.

To configure the syslog server on NIPS, follow these steps:

Step 1 Choose **Network > Network Configuration > Syslog**.

Figure 5-72 Configuring the syslog server



Step 2 Specify the IP address, port, and version (**v1** or **v2**) of the syslog server.

You can configure two syslog servers, which can be of the v1 or v2 version. The v2 version supports more diversified and detailed logs. You can choose whether to send security logs to syslog servers.

Step 3 Click **Apply**.

Step 4 Apply the settings**.**

----End

5.10 High Availability

During data communication, any kind of software and hardware error may cause a network connection interruption, which, in turn, leads to a data transmission failure. To avoid communication interruption resulting from single points of failure, NIPS provides the high availability (HA) function to enhance network reliability.

Note	NIPS NX5-T9010A and NX5-T9020A do not support the following HA functions: • VRRP • Layer 2 HA

5.10.1 Basic Concepts

NIPS's HA function is implemented by means of virtual wire (v-wire), Virtual Router Redundancy Protocol (VRRP, in layer 3), and asymmetric routing support (ARS) between two devices.

- V-wire HA

  V-wire HA involves configuration of a virtual wire. This HA mode is required when the device uses security zones of the v-wire type. NIPS's v-wire HA supports only the active/standby mode.

- VRRP

  VRRP is a protocol for implementing fault tolerance. Multiple physical routers are simulated to form a virtual router by means of interactive VRRP multicast packets to communicate with hosts on the network. When the master router in a VRRP group fails, the slave router will automatically take over the work from the master one, thereby ensuring the continuity and reliability of communication.

- Layer 2 HA

  HA configuration in transparent mode.

- Asymmetric routing support

  After asymmetric routing (ASR) support is configured, NIPS devices in the ASR support group exchange packet transmission information. Based on such information, a transmitted packet can take a different path when it returns to the source. This allows the establishment of a complete data transmission session. In this manner, deep packet inspection (DPI) is conducted, with the data transmission path unchanged.

HA can work in the following modes:

- Active/standby mode

  The active/standby mode involves two devices: one serves as the master, and the other as the slave. The master device handles all traffic and sends session and configuration information to the slave device for backup; the latter is responsible only for backup, without handling any traffic. When the master device fails, the slave device will take over all traffic handled by the master device. This ensures that newly initiated sessions can be successfully established and the current ongoing sessions will not be interrupted.

- Active/active mode

  In active/active mode, both devices are active ones and handle traffic simultaneously. Also, the two devices serve as each other's backup, mutually keeping a copy of their session information and configuration files. Once one device fails, the other will take over all traffic. This ensures that newly initiated sessions can be set up properly and the current ongoing sessions are not disconnected.

- Preemption mode

  In preemption mode, if the master device fails, the traffic is switched to the slave device. After the fault is fixed, the master device will take traffic back from the slave device. At this time, the master device becomes active, while the slave device returns to the inactive state.

- Non-preemption mode

  In non-preemption mode, if the master device fails, the slave device takes over the traffic. After the fault is fixed, the master device does not take back the traffic until the slave device fails.

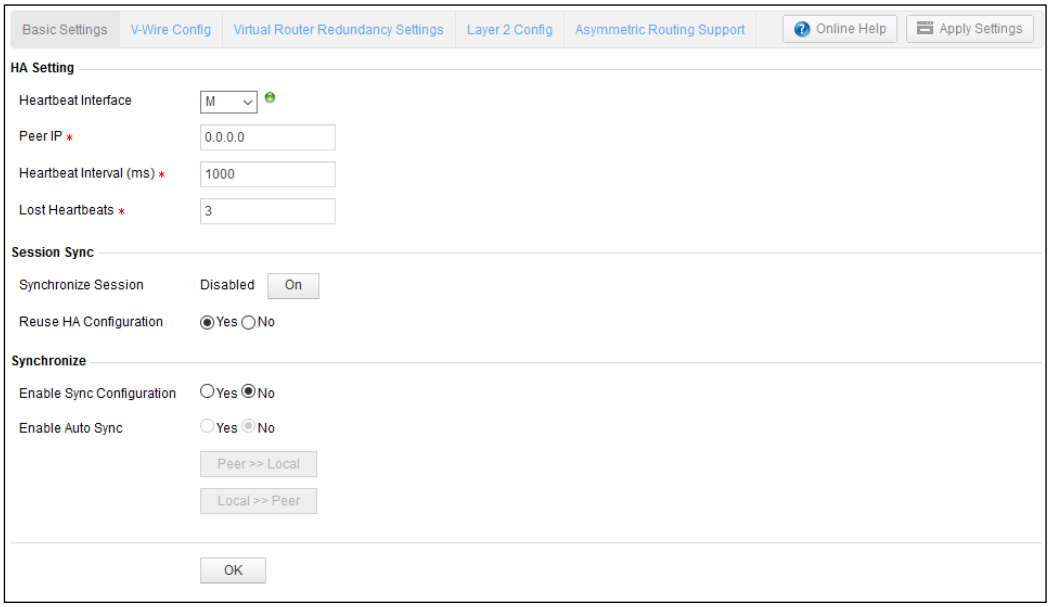
5.10.2 Basic Configuration

The master and slave devices are connected with a management interface (heartbeat interface), which is used to send and receive heartbeat messages and synchronize configuration files and session information.

To configure the HA function, follow these steps:

Step 1 Choose **Network** > **HA Settings** > **Basic Settings**.

Figure 5-73 Configuring basic settings



Step 2 Configure parameters.

Table 5-28 Basic HA parameters

Parameter		Description
HA Setting	Heartbeat Interface	Heartbeat interface on the local device. The heartbeat interface can be interface M or H1 or layer 3 working interfaces. The heartbeat interface cannot be used to handle traffic. The icon beside the heartbeat interface indicates that this interface is up. If the icon is , the interface is down. Note The heartbeat interface and the peer IP address are unavailable in any of the following cases: • Both HA and session synchronization are enabled. • HA is enabled, while session synchronization is not. • HA is disabled, while session synchronization is enabled.
	Peer IP	IP address of the heartbeat interface on the peer device.
	Heartbeat Interval	Specifies the interval at which the local device sends a heartbeat

Parameter		Description
	(ms)	message to the peer device. The minimum value is 1000 ms. The value of this parameter must be the same for the master device and the slave device.
	Lost Heartbeats	Specifies the number of consecutive heartbeat messages that are not received from the peer device before the local device assumes that the peer device is down. In this case, if the local device is a master one, its status remains unchanged, while the status of the peer device is displayed as **Unknown**. If the local device is a slave one, its status changes to active for forwarding packets. At this time, the status of the local device turns to active, while that of the peer device is displayed as **Unknown**.
Session Sync	Synchronize Session	Controls whether to synchronize sessions via the heartbeat interface or another interface.
	Reuse HA Configuration	If you select **Yes**, sessions will be synchronized through the heartbeat interface. If you select **No**, you need to further configure the interface for session synchronization and the peer IP address. **Sync Interface**: specifies an interface for session synchronization. This parameter appears only when session synchronization is enabled and you select **No** for **Reuse HA Configuration**. **Peer IP**: specifies the IP address of the peer interface through which sessions will be synchronized. This parameter appears only when session synchronization is enabled and you select **No** for **Reuse HA Configuration**.
Synchronize		NIPS supports both manual and automatic synchronization of all configurations. This can be configured only when you properly configure the heartbeat interface and peer IP address. By default, synchronization configuration is disabled. You can click **Yes** for **Enable Auto Sync** to enable it and then determine whether to synchronize configurations automatically or manually. Automatic synchronization: You can select **Yes** for **Enable Auto Sync** to enable automatic configuration synchronization and click **Apply Settings** in the upper-right corner of the page to commit the setting. Manual synchronization: You can click **Peer >> Local** to synchronize the settings on the peer device to the local device or click **Local >> Peer** to synchronize the settings on the local device to the peer device.

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

----End

5.10.3 Virtual Wire Configuration

Virtual wire configuration refers to configuration of the v-wire HA function. This type of HA is required when the device uses security zones of the v-wire type. NIPS's v-wire HA supports only the active/standby mode.

After v-wire HA is enabled, the master device is working and responsible for forwarding packets, while the slave device is in backup state and ready to take over traffic handled by the master device. The master device and slave device send heartbeat messages regularly to each other about the number of available virtual wires.

Note	The **V-Wire Config** page is replaced by the **Direct HA Settings** page on NIPS NX5-T9010A and NX—T9020A.

To configure v-wire HA, perform the following steps:

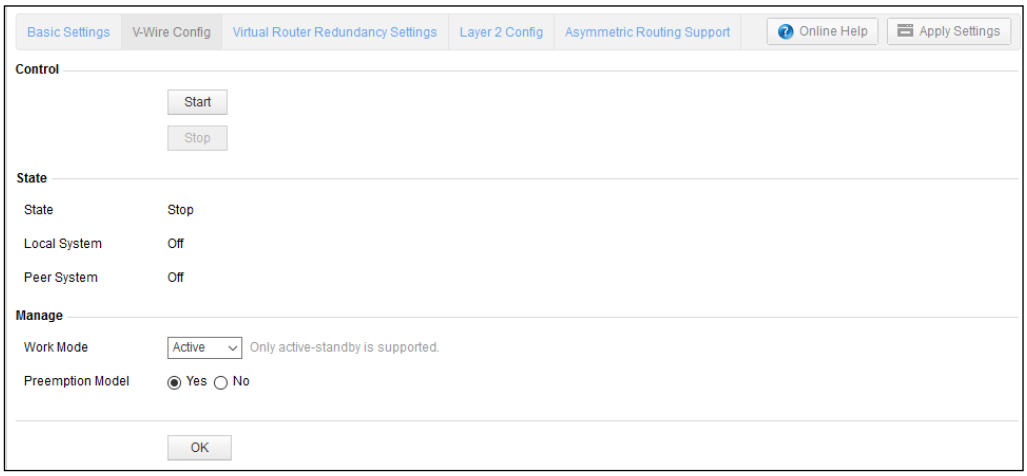
Step 1 Set public parameters of HA.

For details, see section 5.10.2 Basic Configuration.

Step 2 Configure v-wire HA.

a. Choose **Network > HA Settings > V-Wire Config**.

Figure 5-74 V-Wire Config page



b. Configure parameters.

Table 5-29 Parameters for configuring v-wire HA

Parameter	Description
State	Indicates the working status of the local device, which can be **Running** or **Stop**. • **Running**: This is displayed after v-wire HA is successfully enabled. • **Stop**: This is displayed when v-wire HA stops working or is disabled.
Local System/Peer System	• **Local System** indicates the status of the local system, which can be **Activated**, **Unactivated**, or **Off**. • **Peer System** indicates the status of the peer system, which can be **Activated**, **Unactivated**, **Off**, or **Unknown**. ➢ After v-wire HA is successfully enabled, if the local device is in active mode and can properly communicate with the heartbeat interface of the slave device, the local system status is displayed as **Activated** and the peer system status as **Unactivated**. ➢ After v-wire HA is successfully enabled, if the local device is in standby mode and can properly communicate with the heartbeat interface of the master

Parameter	Description
	device, the local system status is displayed as **Unactivated** and the peer system status as **Activated**. ➢ After v-wire HA is successfully enabled, if the local device cannot communicate properly with the heartbeat interface of the peer device, the local system status is displayed as **Activated** and the peer system status as **Unknown**. ➢ If v-wire HA is disabled, both the local system status and peer system status are displayed as **Off**.
Work Mode	V-wire HA supports only the active/standby mode. • **Master**: After v-wire HA is enabled, the local device works in active mode and is responsible for forwarding packets until the failover. • **Slave**: After v-wire HA is enabled, the local device works in standby mode without forwarding data until the failover.
Preemption Mode	Controls whether to enable the preemption mode. • **Yes**: If the master device fails and traffic is switched to the slave device, when the master device is back to normal, it turns to active mode again and traffic is switched back to it for forwarding. • **No**: If the master device fails and traffic is switched to the slave device, when the master device is back to normal, traffic is not switched back to this device and is still forwarded by the slave device that works in active mode.

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

Step 3 Enable v-wire HA.

d. Click **Start** in the **Control** area.

e. In the confirmation dialog box, click **OK**.

----End

5.10.4 VRRP Configuration

Virtual router redundancy is configured to implement layer 3 HA. This type of HA is used when the device uses layer 3 security zones. NIPS's layer 3 HA supports the active/standby mode and active/active mode.

In layer 3 HA mode, each device can be configured with multiple VRRP backup groups. In addition, the configuration of interfaces with the same virtual router ID (VRID) is backed up between two devices. In each VRRP group, the device with a higher priority works as the master device, while that with a lower priority as the slave device.

Note	NIPS NX5-T9010A and NX5-T9020A do not support VRRP.

You can configure layer 3 HA and edit and delete layer 3 HA lines.

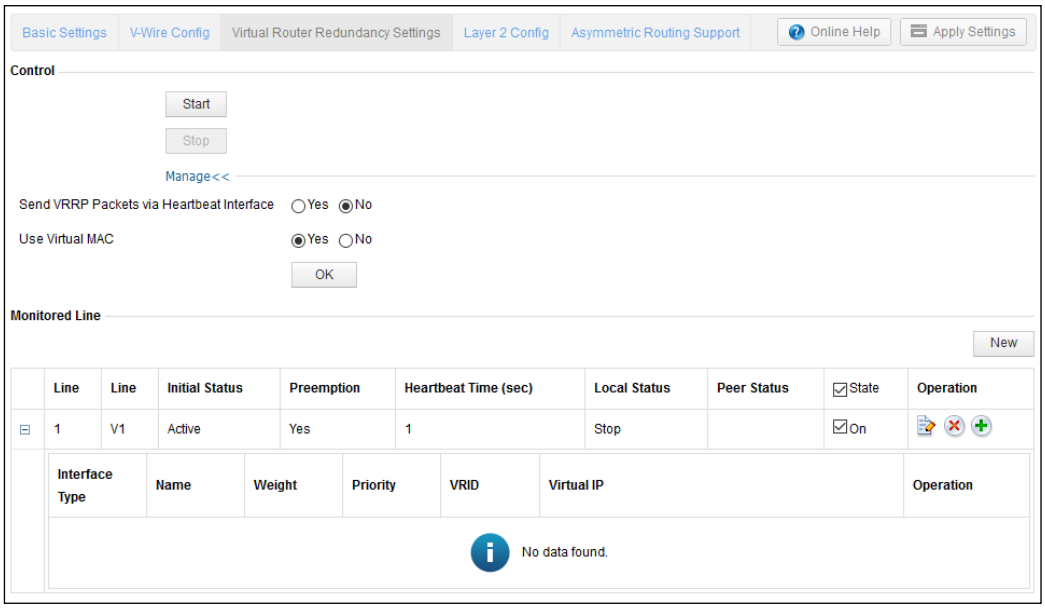
To configure layer 3 HA, perform the following steps:

Step 1 Set public parameters of HA.

For details, see section 5.10.2 Basic Configuration.

Step 2 Choose **Network** > **HA Settings** > **Virtual Router Redundancy Settings**.

Figure 5-75 Virtual Router Redundancy Settings page



Step 3 Configure VRRP parameters.

Parameter	Description
Send VRRP Packets via Heartbeat Interface	Controls whether to send VRRP packets through the heartbeat interface. The default value is **No**, indicating that VRRP packets through VRRP member interfaces. If you select **Yes**, VRRP packets are sent through the heartbeat interface. If HA is configured on NIPS which connects to a router, you must select **No**; otherwise, VRRP packets cannot be sent.
Use Virtual MAC	Controls whether to use MAC addresses for sending VRRP packets. The default value is **Yes**, indicating that MAC addresses are used for sending VRRP packets. It is recommended that the default value be used.

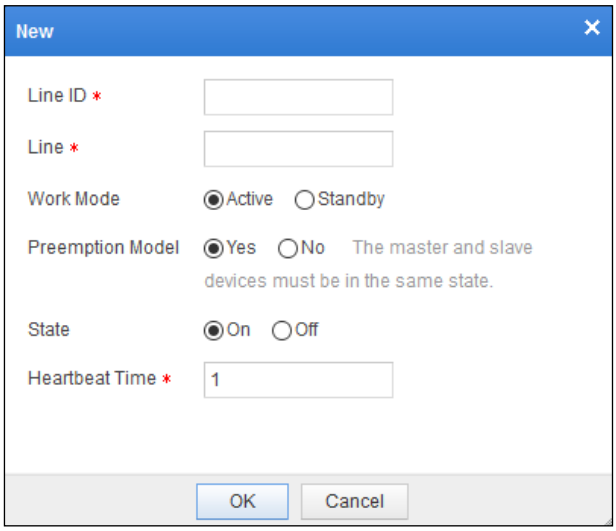
After parameter settings, click **OK** to save the settings.

Step 4 Create a monitoring line.

Generally, a line consists of a pair of interfaces (IN and OUT indicated in packets), which belong to different VRRP groups. Each VRRP group contains interfaces to be backed up between two devices. These interfaces have the same virtual IP address.

b. Click **New** in the upper-right corner of the **Monitored Line** area.

Figure 5-76 Creating a monitoring line



c. In the **New** dialog box, configure parameters.

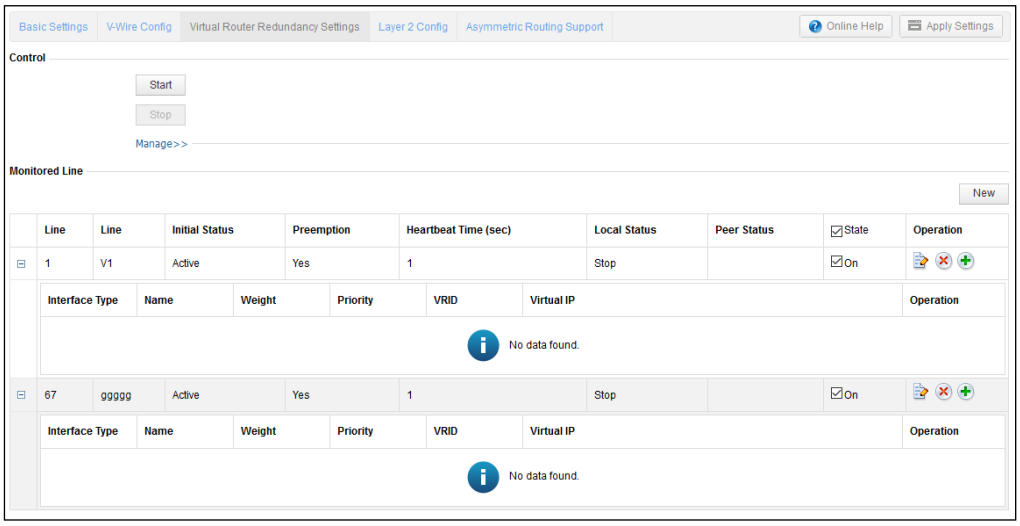
Table 5-30 Parameters for configuring a monitoring line

Parameter	Description
Line ID	Uniquely identifies a line, which must be an integer in the range of 1–255. The line ID configured on the local device must be the same as that on the peer device.
Line	Name of the new line, which must be a string of letters and digits. It is case-sensitive.
Work Mode	Working mode of the new line. Layer 3 HA supports the active/active mode and active/standby mode. • **Master**: forwards packets until the failover after layer 3 HA is enabled. • **Slave**: remains in the standby state and does not forward data until the failover after layer 3 HA is enabled.
Preemption Model	Controls whether to enable the preemption mode. • **Yes**: If the master line fails and traffic is switched to the slave line, when the master line is back to normal, it turns to active mode again and traffic is switched back to it for forwarding. • **No**: If the master line fails and traffic is switched to the slave line, when the master line is back to normal, traffic is not switched back to this line and is still forwarded by the slave line that works in active mode.
Status	Specifies the working status of the new line. The settings can take effect only when the line is enabled.
Heartbeat Time	Specifies 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 slave line interface fails to receive any multicast packet from the master line interface after [3 x heartbeat time + (255 – priority of the slave line interface)/256] seconds, the system deems that the master line is down. In this case, the slave line turns to active and begins to forward data. The heartbeat time configured on the local line must be the same as that on the peer line.

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

Now the new line is displayed in the **Monitor Line** list.

Figure 5-77 New line displayed



Step 5 Configure interfaces for this line.

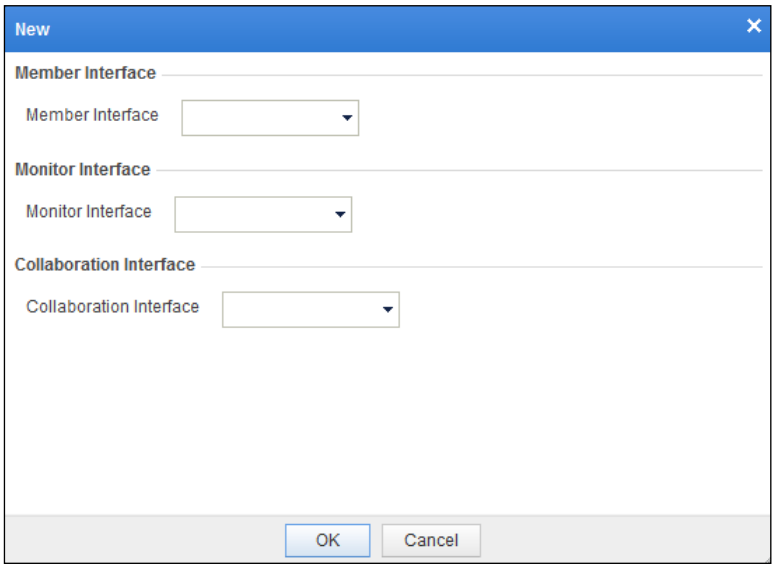
Interfaces of a monitoring line are divided into the following:

- **Member Interface**: As VRRP instances, such interfaces can be configured with virtual IP addresses. When an interface of the master line is down, other interfaces in this line release virtual IP addresses and at the same time traffic is taken over by the slave line.
- **Monitor Interface**: used by VRRP to monitor line status. You cannot specify a member interface as the monitoring interface. When any one of the monitoring interface is down, an active/standby switchover will be performed.
- **Collaboration Interface**: When VRRP performs an active/standby switchover, the status of such interfaces changes accordingly: The collaboration interface on the active line goes Up, while that on the standby line goes Down. You cannot specify a member interface as the collaboration interface.

a. Click in the **Operation** column of a line.

The **New** dialog box appears, as shown in Figure 5-78.

Figure 5-78 Creating line interfaces



b. Configure parameters.

Table 5-31 Parameters for configuring line interfaces

Parameter		Description
Member Interface	Interface	Member interface, which must be a layer-3 interface because only layer 3 interfaces can be configured with virtual IP addresses. Other parameters are available only after you select one or more interfaces.
	VRID	Virtual router ID, uniquely identifying a VRRP group. Usually, corresponding interfaces on the master and slave devices, such as the G1/1 interface on the master device and the G1/1 interface on the slave device, are assigned the same VRID. In this manner, they belong to one 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. The value is an integer ranging from 1 to 255.
	Priority	Specifies the priority of the layer-3 interface in the VRRP group. A VRRP group elects the device with the highest interface priority as the master device to work as a gateway for forwarding data. Other devices serve as slave devices working in monitoring mode. Once the master device fails, a slave device replaces it as the gateway, ensuring the continuous communication of the host with external networks. The value is an integer ranging from 1 to 254.
	Virtual IP	Specifies the virtual IP address of the VRRP group. A VRRP group can be configured with a maximum of 20 virtual IP addresses separated by commas, for example, 192.168.1.1/24,192.168.2.1/24.
	Weight	Weight of the member interface. When all member interfaces of master and slave lines are down, the line with the larger sum of weight values turns to active, while the line with the smaller sum turns to standby. The value is an integer ranging

Parameter		Description
		from 0 to 254. When an interface failure occurs on both master and slave devices, neither device can work and all networks will be interrupted. To avoid such issue, the link weight mechanism is introduced: A weight, which is an integers ranging from 0 to 254, are set for each interface on each link of NIPS. When both master and slave NIPSs fail, the interface weight sums of VRRP groups will be calculated. The device with a larger weight sum turns to active, while the device with a smaller sum turns to standby. If the master and slave NIPSs have the same weight sum, the interface priority sums are calculated for both devices. The device with a larger priority sum turns to active, while the device with a smaller sum turns to standby.
Monitor Interface	Interface	Specifies a monitoring interface, which must be on the device to which the line belongs and cannot be a member interface. Generally, this interface does not work for any lines. That is to say, HA is not enabled on this interface. When the monitoring interface is down, the current VRRP line turns to standby. The **Weight** parameter is available only after you select one or more interfaces.
	Weight	Weight of the monitoring interface. When all monitoring interfaces of master and slave lines are down, the line with the larger sum of weight values turns to active, while the line with the smaller sum turns to standby. The value is an integer ranging from 0 to 254.
Collaboration Interface		Specifies a collaboration interface. When VRRP implements an active/standby switchover, the collaboration interface on the active line goes Up, while that on the standby line goes Down.

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

Step 6 Enable layer 3 HA.

d. Click **Start** in the **Control** area.

e. In the confirmation dialog box, click **OK**.

----End

5.10.5 Layer 2 HA Configuration

NIPS supports the HA function in transparent mode. With layer 2 HA, NIPS can provide link redundancy backup when using layer 2 security zones.

In layer 2 HA mode, each NIPS can have multiple monitoring lines and member interfaces with the same line ID between two devices serve as backups of each other. Layer 2 HA only supports active/standby mode. A device's working mode will be specified when a monitoring line is created.

After layer 2 HA is enabled, the system monitors the status of member interfaces on monitoring lines and counts the number of healthy interfaces on both the master device and slave interface.

- If both devices have the same number of healthy interfaces, the master/slave relationship is determined by the working mode of devices.
- If the master device has less healthy interfaces than the slave device, an active/standby switchover will be performed.

- If the master device has more healthy interfaces than the slave device, the active/standby status of devices remains the same.

Note	NIPS NX5-T9010A and NX5-T9020A do not support layer 2 HA.

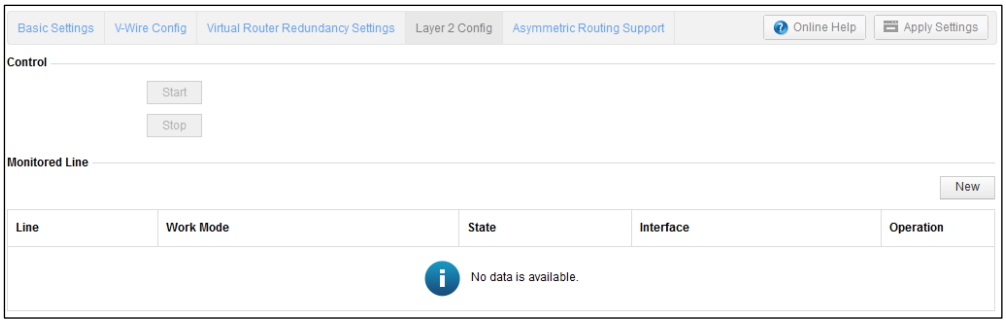
You can configure layer 2 HA parameters and enable or disable this function. To configure layer 2 HA, follow these steps:

Step 1 Set public parameters of HA.

For details, see section 4.7.1 Basic Configuration.

Step 2 Choose **Network > HA Settings > Layer 2 Config**.

Figure 5-79 Layer 2 Config page

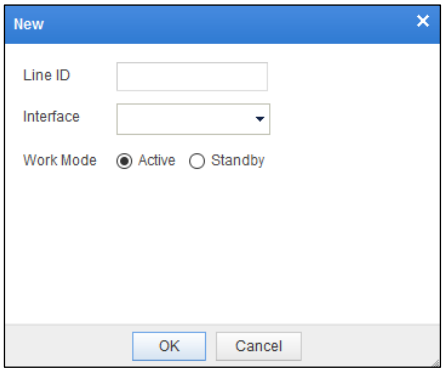


Step 3 Create a monitoring line.

A monitoring line can be created, modified, and deleted only when layer 2 HA is stopped.

a. Click **New** in the upper-right corner of the **Monitored Line** area.

Figure 5-80 Creating a monitoring line



b. In the **New** dialog box, configure parameters.

Table 5-32 Parameters for configuring a monitoring line

Parameter	Description
Line ID	Uniquely identifies a line, which must be an integer in the range of 1–255. The line ID configured on the local device must be the same as that on the peer device.
Interface	Member interfaces involved in this line. Here, layer 2 Ethernet interfaces or aggregation interfaces are supported. Note STP cannot be enabled on member interfaces for layer 2 HA.
Work Mode	Layer 2 HA supports only the active/standby mode. • **Active**: forwards packets until the failover after layer 2 HA is enabled. • **Standby**: remains in the standby state and does not forward data until the failover after layer 2 HA is enabled.

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

Step 4 Enable layer 2 HA.

a. Click **Start** in the **Control** area.

b. In the confirmation dialog box, click **OK**.

----End

5.10.6 Asymmetric Routing Support

All NIPS models support asymmetric routing (ASR) but differ in the configuration of this function.

- Other models than NX5-T9010A and NX5-T9020A

  ASR can be deployed on two NIPSs only when they are deployed in point-to-point v-wire mode.

- NX5-T9010A and NX5-T9020A

  ASR can be deployed on two NIPSs only when they are deployed in direct mode.

You can query, create, edit, and delete ARS policies.

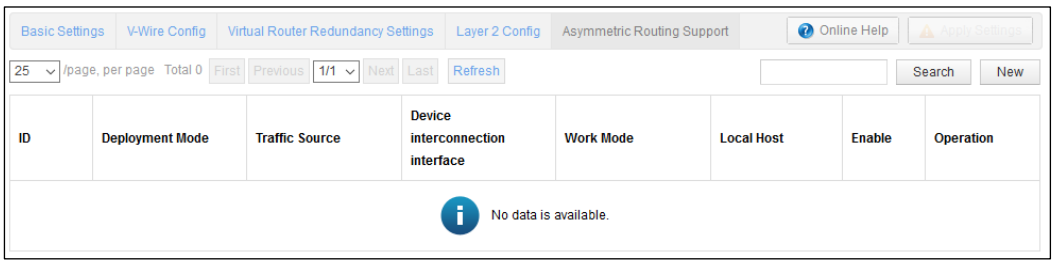
To create an ASR support policy, follow these steps:

Step 1 Choose **Network > HA Settings > Asymmetric Routing Support**.

The ASR configuration page varies with models of NIPS devices.

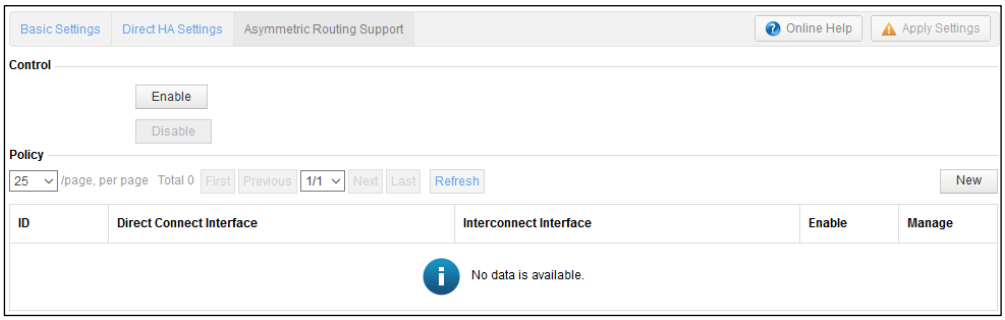
- Figure 5-81 shows the ASR configuration page of other NIPS models than NX5-T9010A and NX5-T9020A.

Figure 5-81 Asymmetric Routing Support page of other models than NX5-T9010A and NX5-T9020A



- Figure 5-82 shows the ASR configuration page of NIPS NX5-T9010A and NX5-T9020A.

Figure 5-82 Creating an ASR policy on NIPS NX5-T9010A and NX5-T9020A



Step 2 Click **New** in the upper-right corner.

The ASR policy creation page varies with models of NIPS devices.

- Figure 5-83 shows the ASR policy creation page of other NIPS models than NX5-T9010A and NX5-T9020A.

Figure 5-83 Creating an ASR policy on other NIPS models than NX5-T9010A and NX5-T9020A

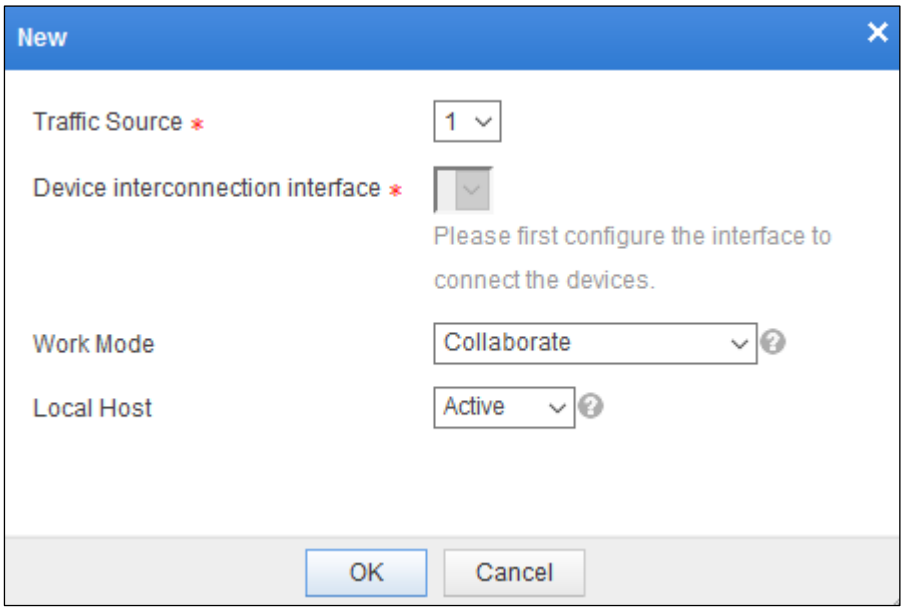


Table 5-33 describes parameters in the **New** dialog box.

Table 5-33 Parameters for creating an ARS policy on other NIPS models than NX5-T9010A and NX5-T9020A

Parameter	Description
Traffic Source	Specifies the source of data traffic. You can only select from among virtual wires.
Device interconnection interface	Interface used for forwarding interconnection information on devices. Prior to this parameter setting, you need to first set **Interface Type** to **Device interconnection interface** under **Configuring Device Interconnection Interface** in section 5.1 Interface.
Work Mode	• **Handle by master device**: indicates that only the master device will check whether to allow forwarding received data traffic. • **Collaborate**: indicates that both the master and slave devices will check whether to allow forwarding received data traffic. In addition, the system determines whether the master or slave device will be used to forward data traffic based on NIPS's load check algorithm and then sends traffic to the selected device. **The working mode of the two interconnected devices must be the same.**
Local Host	• When **Handle by master device** is selected for **Work Mode**: **Active**: specifies that the local host acts as the active device. For data traffic from the standby device, the active device sends the check result to the standby device. For data traffic from other devices, the active device forwards the data traffic that is allowed to pass. **Standby**: specifies that the local host acts as the standby device. Then the local host sends received data traffic to the active device. After receiving the check result from the active device, the standby device forwards the data traffic as indicated in the check result. • When **Collaborate** is selected for **Work Mode**: **Active**: specifies that the local host acts as the active device. The local host forwards data traffic that is allowed to pass and ought to be forwarded by the active device

Parameter	Description
	according to the load check algorithm. **Standby**: specifies that local host acts as the standby device. Then the local host forwards data traffic that is allowed to pass and ought to be forwarded by the standby device according to the load check algorithm. **Of the two interconnected devices, one must serve as the master device and the other as the slave device.**

- Figure 5-84 shows the ASR policy creation page of NIPS NX5-T9010A and NX5-T9020A.

Figure 5-84 Creating an ASR policy

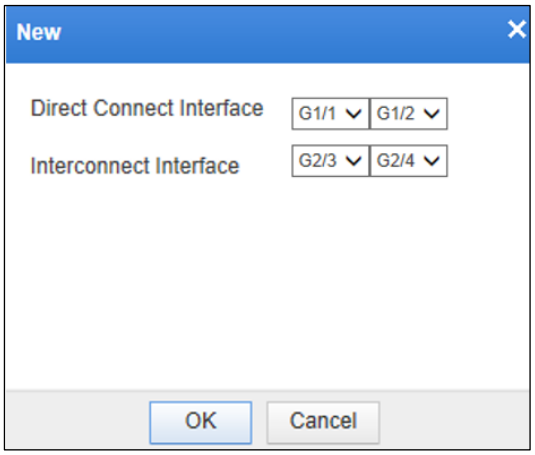


Table 5-34 describes parameters in the **New** dialog box.

Table 5-34 Parameters for creating an ASR policy for NIPS NX5-T9010A and NX5-T9020A

Parameter	Description
Direct Connect Interface	A pair of direct interfaces serving as sources of traffic. The two interfaces must belong to the same security zone of the direct type.
Interconnect Interface	A pair of interfaces for forwarding connection information on the device. The two interfaces must belong the same security zone of the Interconnect type.

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

Step 3 Apply the settings.

----End

5.11 Others

This section covers the following topics:

- Configuring External Bypass
- Configuring Built-in Bypass

The built-in bypass function works only when NIPS comes with a bypass card.

5.11.1 Configuring External Bypass

Usually, NIPS is deployed in an important location on the network to provide comprehensive protection for the intranet. Once NIPS fails, serious problems, such as network interruption, will occur.

To prevent NIPS from turning into a single point of failure in the event of failures such as power failure or system breakdown, we can configure NIPS to collaborate with an external bypass switch. In this manner, the traffic can bypass the faulty gateway or link, thereby ensuring uninterrupted communication.

After NIPS is powered off, its heartbeat interface or working interface fails, or a working interface cannot properly send or receive packets, the collaborative bypass switch turns to the bypass state automatically and forwards the traffic to the next-hop device while bypassing NIPS, ensuring proper network connections. After the preceding problem is resolved, the bypass switch turns to the normal state and forwards the traffic to NIPS, which then receives, handles, and forwards the traffic.

Note	• When a direct interface on fails, the other direct interface does not fail. • NIPS NX5-T9010A and NX5-T9020A have no direct interfaces, but provide v-wire interfaces to play the same role as direct interfaces.

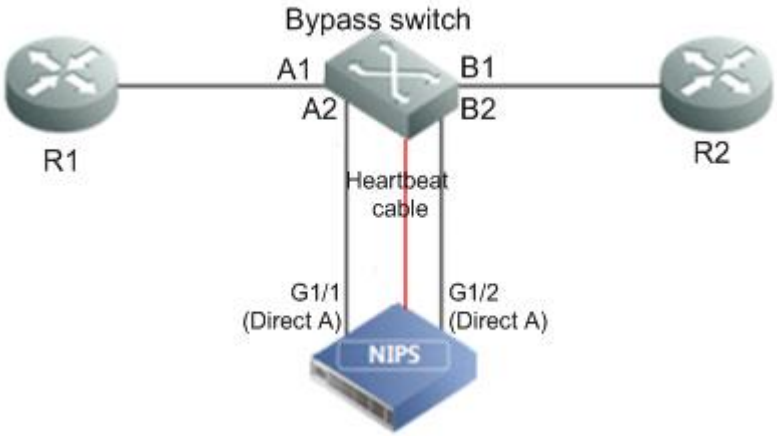
Take the topology in Figure 5-85 as an example. In this example, NIPS works properly and the bypass switch is in normal state. The route for traffic from R1 is as follows:

R1 → Interface A1 on the bypass switch → Interface A2 on the bypass switch → Interface G1/1 on NIPS → Interface G1/2 on NIPS → Interface B2 on the bypass switch → Interface B1 on the bypass switch → R2

When NIPS is powered off or its heartbeat interface fails, the bypass switch turns to the bypass state and forwards the traffic by bypassing NIPS. In this case, the route for traffic from R1 is as follows:

R1 → Interface A1 on the bypass switch → Interface B1 on the bypass switch → R2

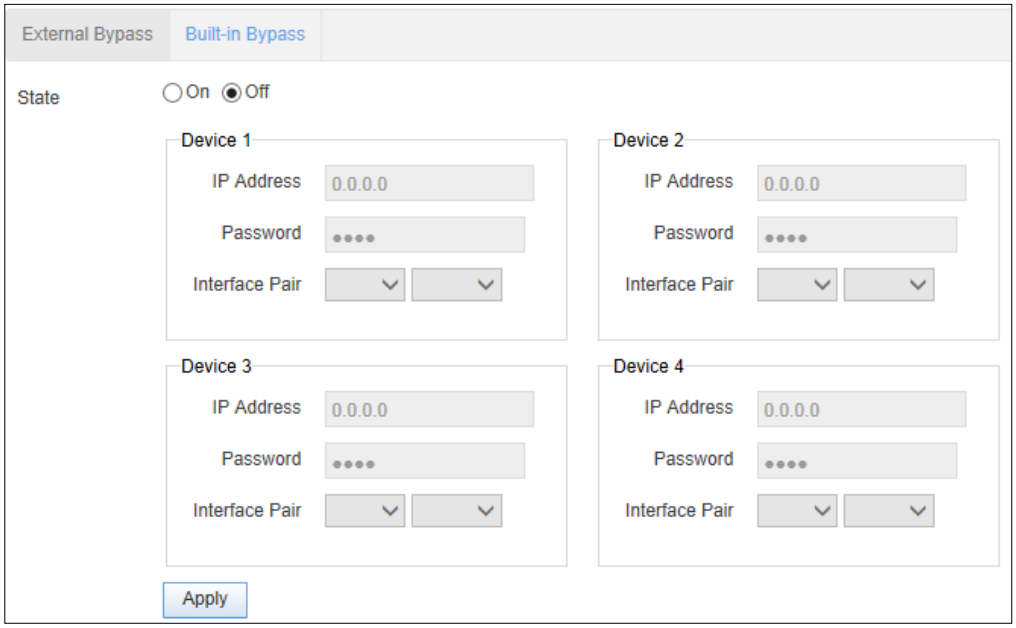
Figure 5-85 Topology for the collaboration between NIPS and the bypass switch



To configure the external bypass feature, follow these steps:

Step 1 Choose **Network** > **Others** > **External Bypass**.

Figure 5-86 Configuring external bypass



Step 2 Click **On** for **State** to enable the external bypass feature.

Step 3 Configure parameters.

Table 5-35 Parameters for configuring external bypass

Parameter	Description
State	Controls whether to enable the external bypass feature.

Parameter	Description
	Note After the external bypass feature is enabled, make sure that the out-of-band management interface of NIPS communicates with the external bypass switch properly. For how to install and use external bypass switches, refer to the *NSFOCUS Bypass Switch User Guide*.
IP Address	IP address of device 1/2/3/4.
Password	Specifies the password for login to a bypass switch.
Interface Pair	Specifies a pair of interfaces for NIPS to collaborate with the bypass switch.

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

----End

5.11.2 Configuring Built-in Bypass

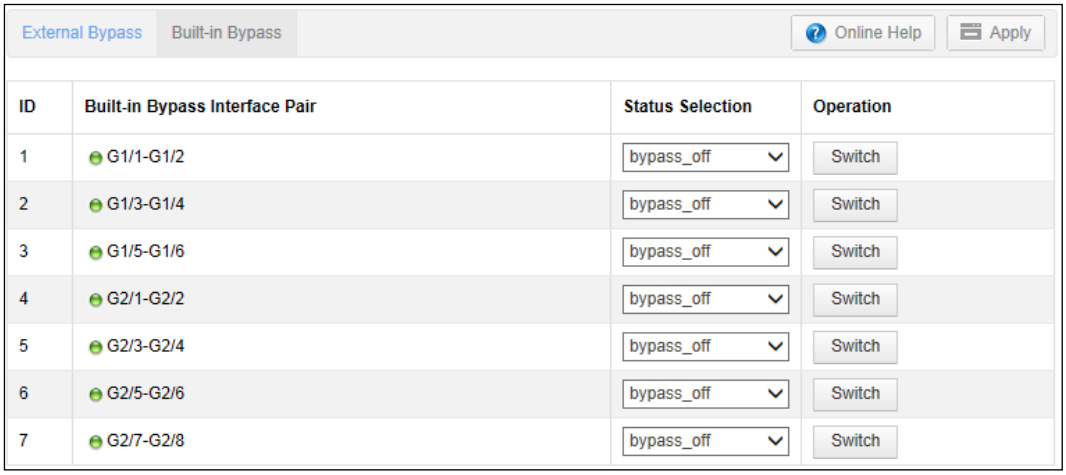
Built-in bypass refers to the use of network interfaces of NIPS to implement the bypass feature. The purpose is to ensure physical connections when NIPS is faulty.

An NIPS device with a bypass card allows you to configure built-in bypass on the web-based manager.

To configure built-in bypass, follow these steps:

Step 1 Choose **Network** > **Others** > **Built-in Bypass**.

Figure 5-87 Built-in bypass interface pairs



Step 2 Select a status from the **Status Selection** drop-down list for an interface pair.

Options include **bypass_off** and **bypass_on**.

- When a built-in bypass interface pair is switched to the **bypass_off** status, the interface pair enters the normal state, and packets over the interface pair will be forwarded after being checked.
- When a built-in bypass interface pair is switched to the **bypass_on** status, the interface pair enters the bypass state, and packets over the interface pair will be forwarded without being checked.

Note	Manual or automatic switching of bypass status will change bypass indicator status: • If the status is switched to **bypass_on**, the bypass indicator turns red. • If the status is switched to **bypass_off**, the bypass indicator turns green.

Step 3 Click **Switch** in the **Operation** column to change the status of the related bypass interface pair.

----End

6 Objects

An object refers to a collection of items with the same characteristics. The items may be IP addresses, rules, and services. An alias is assigned to each object as the object name.

On NIPS, all policies are configured based on objects. Therefore, you must configure objects before configuring policies. You can define such objects as the rule, network, service, application, time, sensitive data, and traffic channel.

The concept of object greatly simplifies the management of NIPS. When an object changes, you only need to modify properties of this object, instead of modifying all policies referencing this object. For how to configure policies, see chapter 7 Policies.

This chapter describes system objects on NIPS, containing the following sections:

Section	Description
Configuring Rules	Describes how to configure a rule.
Configuring Network Objects	Describes how to configure a network object.
Configuring Service Objects	Describes how to configure a service.
Configuring Application Objects	Describes how to configure an application.
Configuring Time Objects	Describes how to configure the time.
Configuring Sensitive Data Object	Describes how to configure sensitive data.
Configuring a Traffic Channel Object	Describes how to configure a traffic channel.
Clearing Asset Trees	Describes how to view and configure asset trees dispatched by ESPC.

6.1 Configuring Rules

The rule object is used to describe NIPS customers' topologies, actual requirements, protection objects, and application environments.

The rule object on NIPS consists of the following:

- Rule template

  NIPS provides multiple typical user-environment templates, increasing the ease of use when you configure IPS policies. Rule templates are divided into the following:

  - System rule templates

System rule templates are subdivided into built-in templates and derived templates. Built-in templates are preconfigured templates, which cannot be edited and can only be viewed and referenced for configuring new policies. Based on default templates, derived templates can be, to some extent, modified as required (for example, you can modify the action (**Alert**, **Block**, and **Isolate**) settings, but you cannot create or delete a rule).

– User rule templates

You can add or delete rules in a rule base or modify the action (such as **Alert** and **Block**) setting as required to generate user rule templates.

- Rules

  Rules are the basic element of a rule template. NIPS comes with built-in intrusion prevention rules, based on which you can customize rules as required. Also, you can create exception rules.

In addition to the preceding rule objects, NIPS also supports rule query.

6.1.1 System Rule Templates

For typical application scenarios, the NIPS system combines rules in the intrusion prevention rule base to form ten typical built-in rule templates, as listed in Table 6-1.

Table 6-1 Built-in rule templates

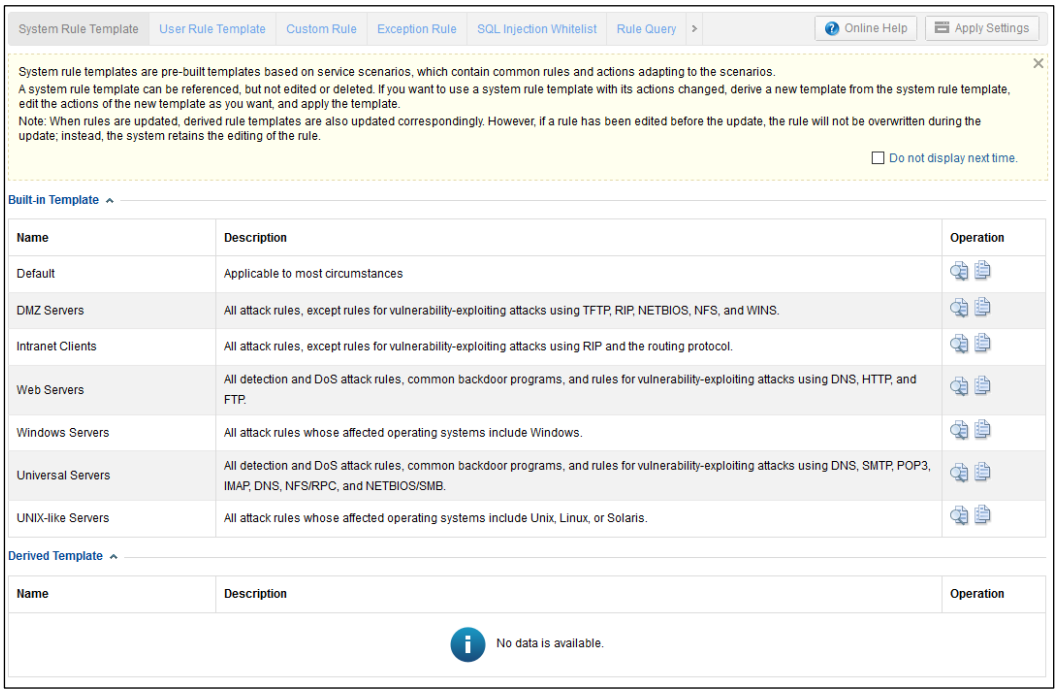
Template	Description
Default	Applicable to most environments.
DMZ Servers	Rules for all attack types except attacks that exploit vulnerabilities in TFTP, RIP, NETBIOS, NFS, and WINS.
Intranet Clients	Rules for all attack types except attacks that exploit vulnerabilities in RIP and routing protocols.
Web Servers	Probe rules, DoS rules, common backdoor programs, and rules for vulnerability exploitation attacks related to DNS, HTTP, and FTP.
Window Servers	Rules for all attacks that exploit vulnerabilities in the Windows operating system.
Universal Servers	Probe rules, DoS rules, common backdoor programs, and rules for vulnerability exploitation attacks relating to DNS, SMTP, POP3, IMAP, DNS, NFS/RPC, and NETBIOS/SMB.
UNIX-like Servers	Rules for all attacks that exploit vulnerabilities in the UNIX, Linux, and Solaris operating systems.

Based on our years of experience in intrusion prevention and technical engineers' onsite experience, the ten typical built-in rule templates in NIPS can fit in with most network deployment environments. Therefore, you are advised to use built-in rule templates when configuring intrusion prevention policies.

In addition to built-in templates, system rule templates also contain derived templates. To configure a derived template, follow these steps:

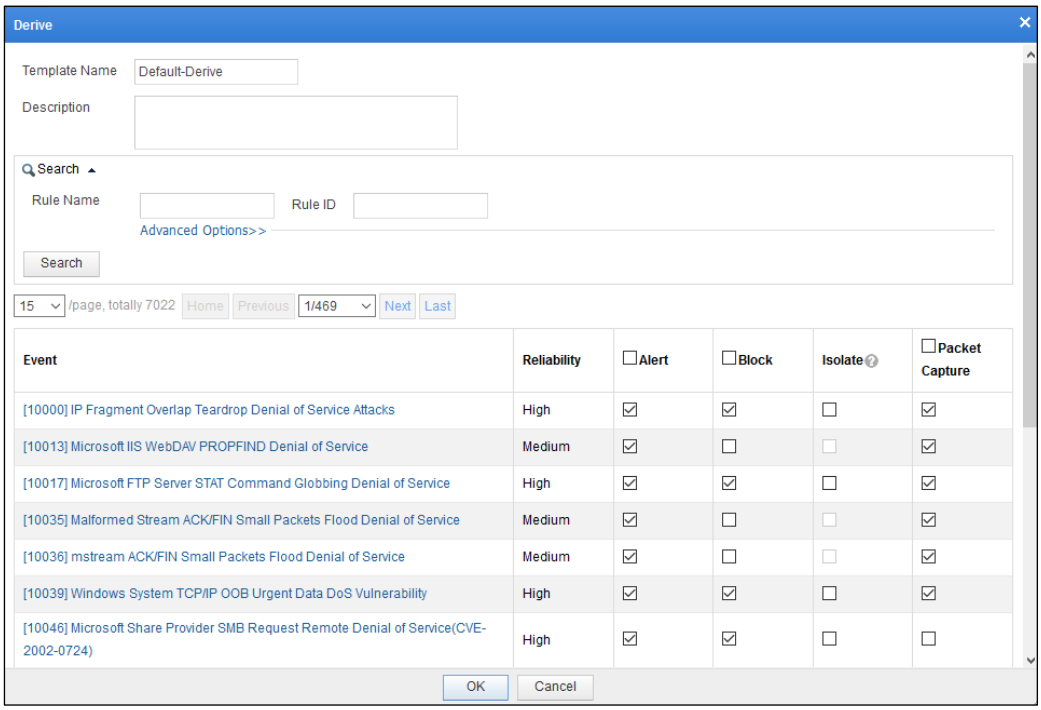
Step 1 Choose **Object** > **Rule** > **System Rule Template**.

Figure 6-1 System rule templates



Step 2 Click  in the **Operation** column of a built-in template.

Figure 6-2 Configuring a derived template



Step 3 Configure parameters in the **Derive** dialog box.

Table 6-2 Parameters for configuring a derived template

Parameter	Description
Template Name	Specifies the name of the derived template. By default, the template name is in the format of "name of the built-in template" + "Derive".
Description	Brief description of the derived template.
Event	Specifies the intrusion prevention events to be include in the derived template. Here, you can only modify the action setting for each intrusion prevention event, which can be **Alert**, **Block**, **Isolate**, or **Packet Capture**. Note • When the protection mode is enabled, selection of **Isolate** will isolate rule-triggering attack IP addresses in the specified period of time. • If the **Packet Capture** check box is selected, a **Download Original PCAP** button will appear on ESPC. In this case, original packets contain complete data. Otherwise, no such button appears on ESPC. In this case, original packets contain no data.

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

The newly configured derived template is displayed in the **Derived Template** area.

Step 5 Apply the settings.

----End

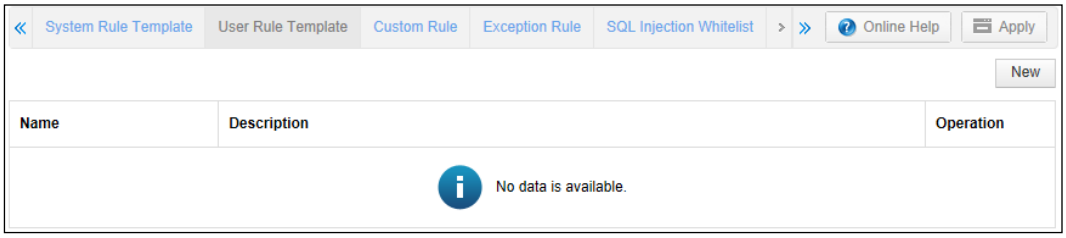
6.1.2 User Rule Templates

User rule templates are a supplement to system rule templates. You can configure them as required.

To configure a user rule template, follow these steps:

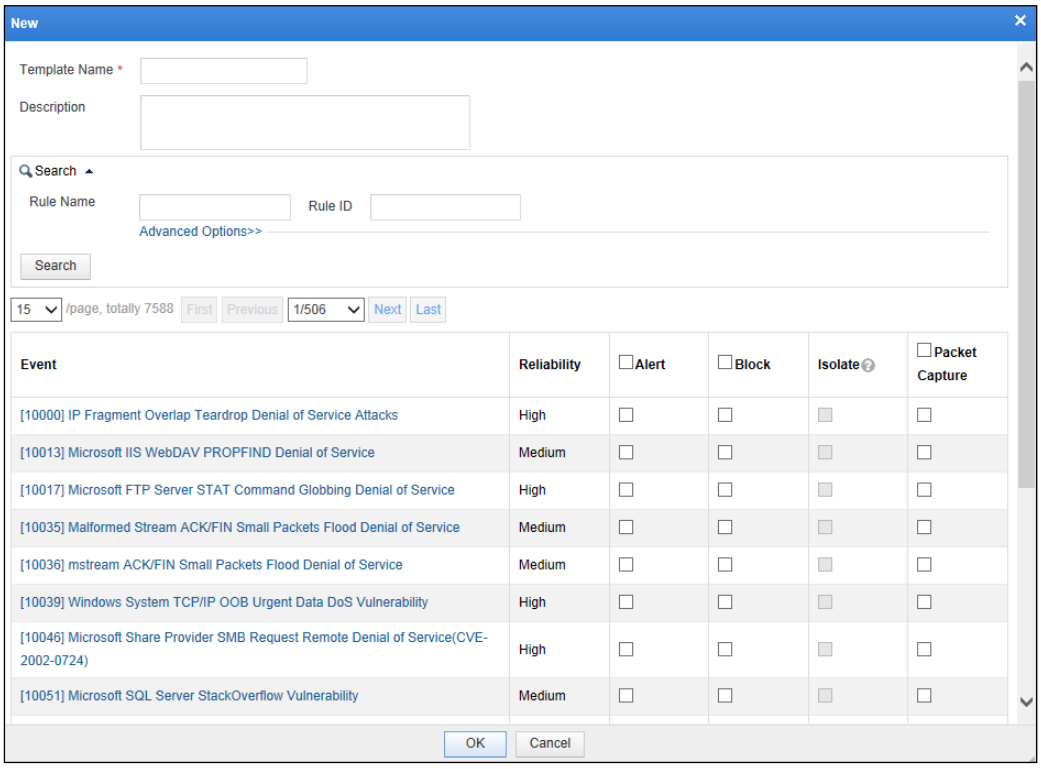
Step 1 Choose **Object > Rule > User Rule Template**.

Figure 6-3 User rule templates



Step 2 Click **New** in the upper-right corner.

Figure 6-4 Configuring a user rule template



Step 3 Configure parameters in the **New** dialog box.

Table 6-3 Parameters for configuring a user rule template

Parameter	Description
Template Name	Specifies the name of the user rule template.
Description	Brief description of the user rule template.
Event	Specifies the intrusion prevention events to be included in the user rule template and action for each intrusion prevention event, which can be **Alert**, **Block**, **Isolate**, or **Packet Capture**. Note • When the protection mode is enabled, selection of **Isolate** will isolate rule-triggering attack IP addresses in the specified period of time. • You can locate an event through the **Rule Query** module. For details, see section 6.1.6 Rule Query. • If the **Packet Capture** check box is selected, a **Download Original PCAP** button will appear on ESPC. In this case, original packets contain complete data. Otherwise, no such button appears on ESPC. In this case, original packets contain no data.

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

Step 5 Apply the settings.

----End

6.1.3 Custom Rules

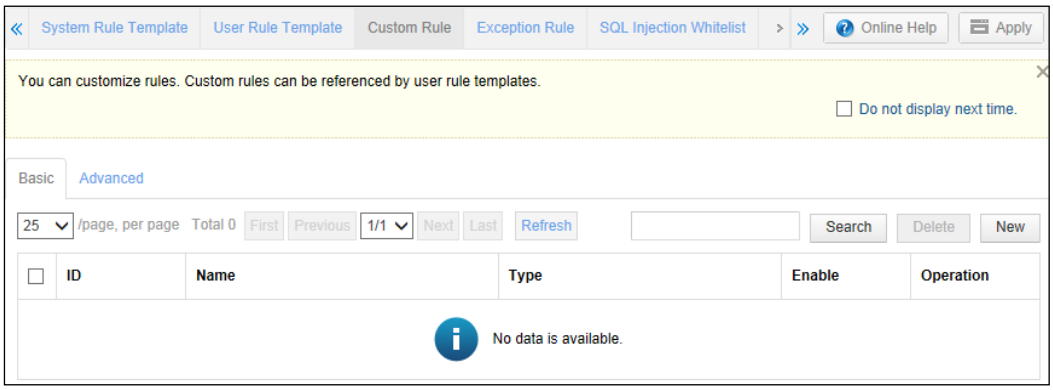
As a supplement to the predefined intrusion prevention rule base, custom rules are configured for various network protocols. IDs of custom rules start from 80001. That is to say, a rule with an ID larger than 80000 is a custom one. Custom rules are divided into basic rules and advanced rules. The procedures for configuring these two types of custom rules are described respectively in the following sections.

6.1.3.1 Basic Rules

Basic rules are subdivided into four types by network protocols: IP rules, UDP rules, TCP rules, and ICMP rules. This section describes how to configure each type of basic rules respectively.

Choose **Object** > **Rule** > **Custom Rule** > **Basic**.

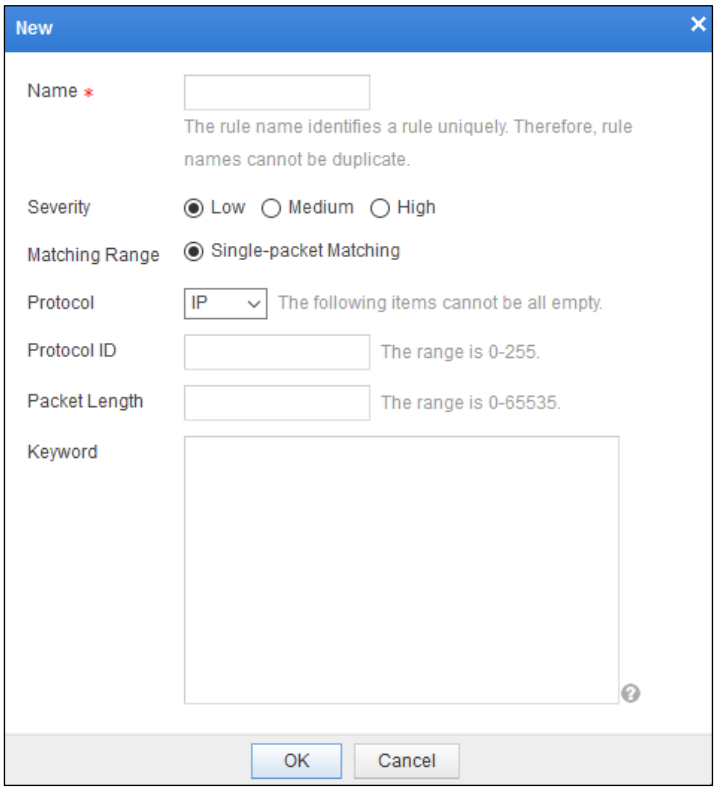
Figure 6-5 Basic rules



IP Rule

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

Figure 6-6 Configuring an IP rule



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

Table 6-4 Parameters for configuring an IP rule

Parameter	Description
Name	Specifies the name of the IP rule, which is the unique identifier of this IP rule on NIPS. The IP rule name cannot contain spaces and the following special characters: \ % ` @ ^ < > { } ' & " :
Severity	Specifies the risk level of the IP rule, which can be **Low**, **Medium**, or **High**.
Matching Range	Specifies the matching range, which can only be **Single-packet Matching** by default. Single-packet matching means that NIPS matches a single packet with a rule composed of one or more signatures and determines accordingly whether an attack exists.
Protocol	Specifies the protocol type. Here you should select **IP**.
Protocol ID	Specifies the ID of the upper-layer protocol of the IP protocol. The value must be an integer ranging from 0 to 255. For example, the value **6** indicates that the upper-layer protocol is the TCP protocol and **17** indicates the UDP protocol.
Packet Length	Specifies the length of the IP packet, which must be an integer ranging from 0 to 65535.

Parameter	Description
	• If **Protocol ID** is set to **6**, the value of **Packet Length** is 20 plus the payload length of an IP packet. • If **Protocol ID** is set to **17**, the value of **Packet Length** is 8 plus the length of packet payload.
Keyword	Specifies the keyword to search for in the payload of IP packets. **Note** Keywords can be specified in regular and irregular expressions. When regular expressions are used, keywords must start with "regex_." For example, the keyword "regex_\d\d" matches two integers. If a keyword starts with "case_", which is a non-regular expression, the keyword is case-sensitive.

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

Step 4 Apply the settings.

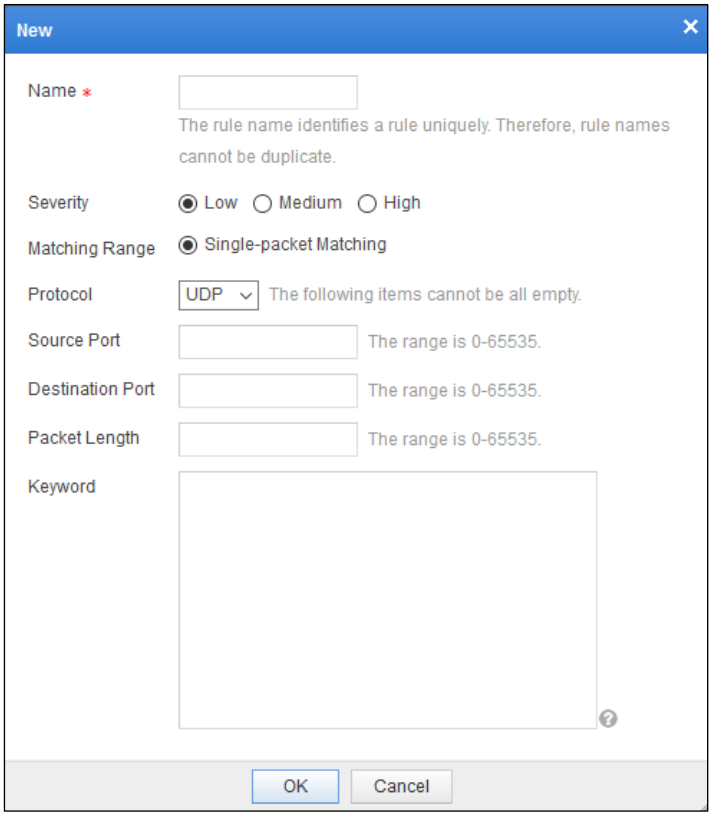
----End

UDP Rule

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

Step 2 In the **New** dialog box, set **Protocol** to **UDP**.

Figure 6-7 Configuring a UDP rule



Step 3 Configure other parameters in the **New** dialog box.

Table 6-5 Parameters for configuring a UDP rule

Parameter	Description
Name	Specifies the name of the UDP rule, which is the unique identifier of this UDP rule on NIPS. The name cannot contain the following special characters: % \ ` < > ' & "
Severity	Specifies the risk level of the UDP rule, which can be **Low**, **Medium**, or **High**
Matching Range	Specifies the matching range, which can only be **Single-packet Matching** by default. Single-packet matching means that NIPS matches a single packet with a rule composed of one or more signatures and determines accordingly whether an attack exists.
Protocol	Specifies the protocol type. Here you should select **UDP**.
Source/Destination Port	Specifies the source or destination port of UDP packets.
Packet Length	Specifies the payload length of UDP packets.
Keyword	Specifies the keyword to search for in the payload of UDP packets.

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

Step 5 Apply the settings.

----End

TCP Rule

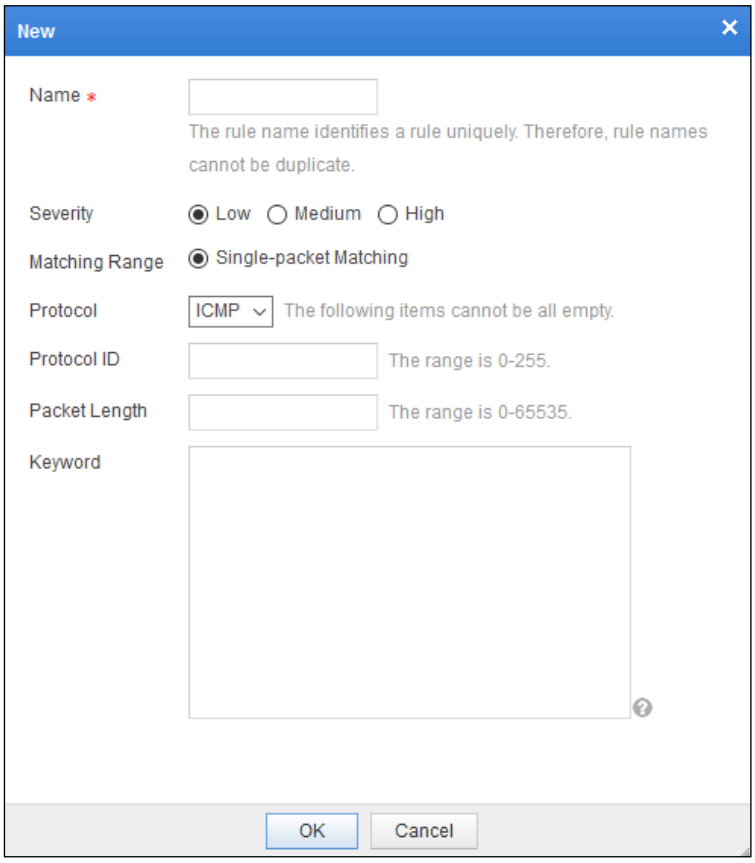
The procedure for configuring a TCP rule is similar to that for configuring a UDP rule. For details, see UDP Rule.

ICMP Rule

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

Step 2 In the **New** dialog box, set **Protocol** to **ICMP**.

Figure 6-8 Configuring an ICMP rule



Step 3 Configure other parameters in the **New** dialog box.

Table 6-6 Parameters for configuring an ICMP rule

Parameter	Description
Name	Specifies the name of the ICMP rule, which is the unique identifier of this ICMP rule on NIPS. The name cannot contain the following special characters: % \ ` < > ' & "
Severity	Specifies the risk level of the ICMP rule, which can be **Low**, **Medium**, or **High**.
Matching Range	Specifies the matching range, which can only be **Single-packet Matching** by default. Single-packet matching means that NIPS matches a single packet with a rule composed of one or more signatures and determines accordingly whether an attack exists.
Protocol	Specifies the protocol type. Here you should select **ICMP**.
Protocol ID	Specifies the protocol ID corresponding to ICMP packets. The value must be an integer ranging from 0 to 255. For example, the value **8** indicates the ping response type, and the value **3** indicates the network unreachability error.
Packet Length	Specifies the payload length of the ICMP packet.

Parameter	Description
Keyword	Specifies the keyword to search for in the payload of an ICMP packet.

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

Step 5 Apply the settings.

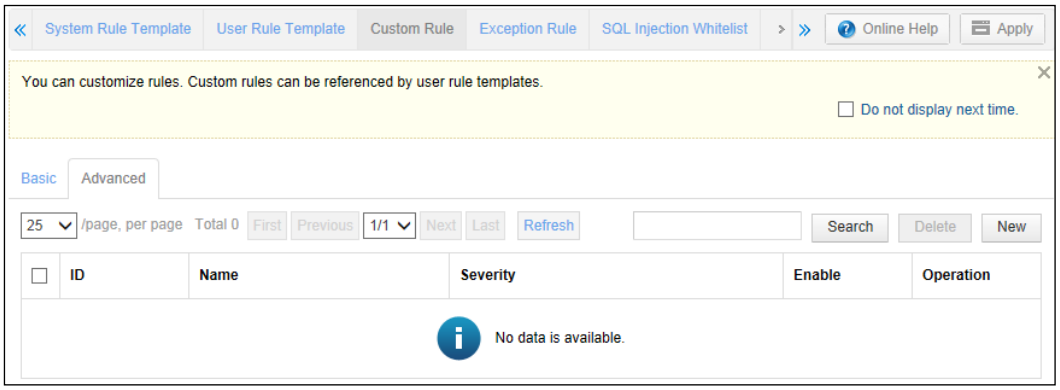
----End

6.1.3.2 Advanced Rules

An advanced rule is a combination of fields in such protocols as HTTP, FTP, SMTP, POP3, QQ, and File with the AND or OR relationship. To configure an advanced rule, follow these steps:

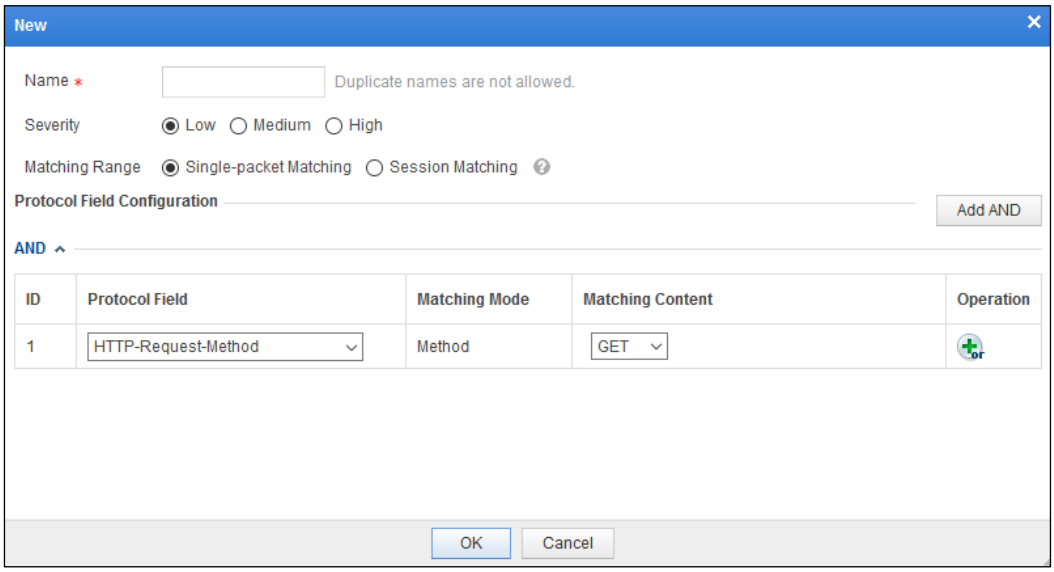
Step 1 Choose **Object** > **Rule** > **Custom Rule** > **Advanced**.

Figure 6-9 Advanced rules



Step 2 Click **New** in the upper-right corner.

Figure 6-10 Configuring an advanced rule



Step 3 Configure parameters in the **New** dialog box.

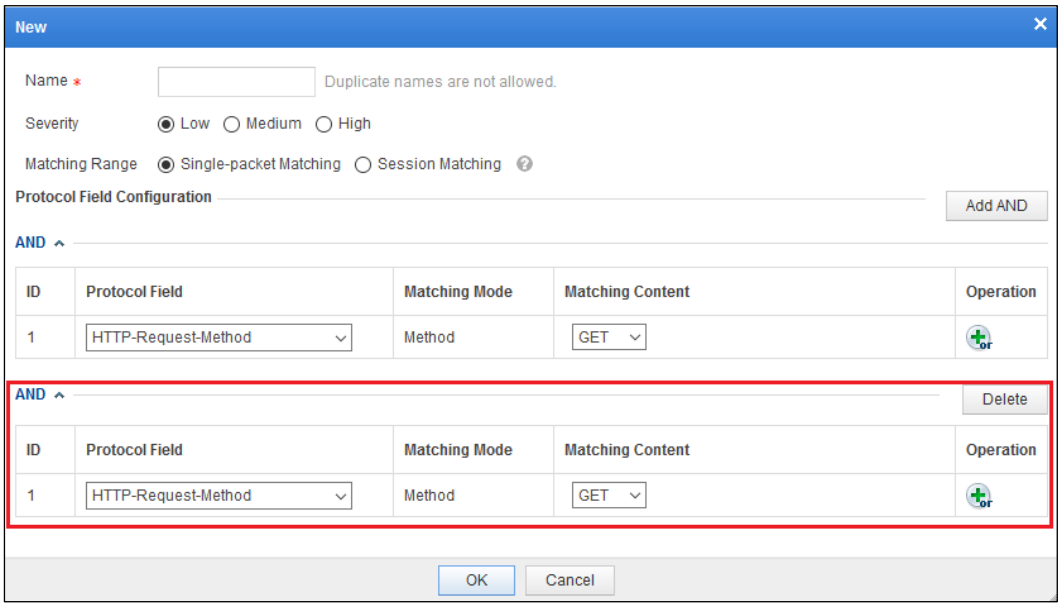
Table 6-7 Parameters for configuring an advanced rule

Parameter	Description
Name	Specifies the name of the advanced rule, which is the unique identifier of this advanced rule on NIPS. The name cannot contain the following special characters: % \ ` < > ' & "
Severity	Specifies the risk level of the advanced rule, which can be **Low**, **Medium**, or **High**.
Matching Range	Specifies the matching range, which can be **Single-packet Matching** or **Session Matching**. • Single-packet matching means that NIPS matches a single packet with a rule composed of one or more signatures and determines accordingly whether an attack exists. A packet is the minimum transmission unit on a packet-switched network. The coverage of single-packet matching is smaller than that of session matching. • Session matching means that NIPS matches a single session with a rule composed of one or more signatures and determines accordingly whether an attack exists. A session is an uninterrupted request-response sequence between a client and server.

Step 4 Configure protocol fields.

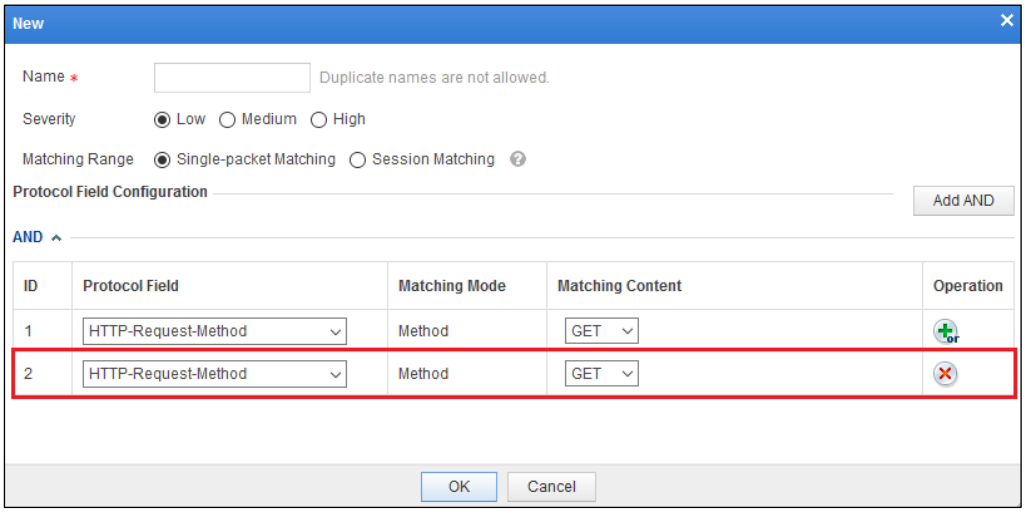
a. Click **Add AND** to add an AND relationship.

Figure 6-11 Adding an ADD relationship



b. Click in the **Operation** column to add an OR relationship.

Figure 6-12 Adding an OR relationship



c. Configure the **Protocol Field**, **Matching Mode**, and **Matching Content**.

Select a protocol field from the drop-down list, and then configure **Matching Content**. A protocol field can be matched by method, regular expression, numerical value, or string, which is explained in Table 6-8.

Table 6-8 Parameters for configuring a protocol field

Matching Mode		Matching Content
Method	HTTP request	Specifies the request type of the HTTP protocol. It has the following values: • **GET**: indicates received packets. • **POST**: indicates sent packets.
	FTP/POP3 request	Specifies the request type of the FTP or POP3 protocol. It has the following values: • **USER** • **PASS** • **LIST**
	SMTP request	Specifies the request type of the SMTP protocol. It has the following values: • **MAIL** • **DATA** • **RCPT**
Regular Express		Specifies a regular expression.
Value		Specifies the matching length in the format of an integer following "=", ">", or "<", or in the format of a range following **in-range**.
String		Specifies a string of decimal or hexadecimal characters. Examples: • \x61\x62\x63\x64\x65 • abcde • abc\x64e

Step 5 Click **OK** to save the settings.

Step 6 Apply the settings.

----End

6.1.4 Exception Rules

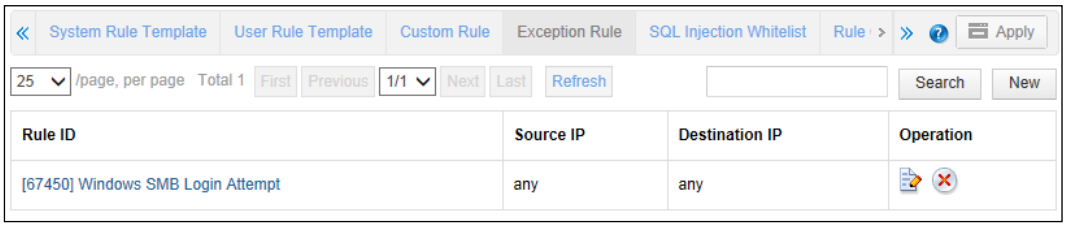
If you know that an intrusion prevention event triggers an intrusion prevention alert and confirm that this event will not threat or have a severe impact on the current network environment, you can add this intrusion prevention event as an exception rule. When adding such a rule, you can set the valid range covered by this rule by specifying the source and destination IP addresses.

After an intrusion prevention event is added as an exception rule, NIPS will not generate an alert for or block it and the exception rule will be no longer displayed under **Home > IPS Event**. For how to add an exception rule, see Adding an Exception in section 3.3.1 List of Intrusion Prevention Events. The procedures for querying and deleting an exception rule are described respectively in the following sections.

Viewing an Exception Rule

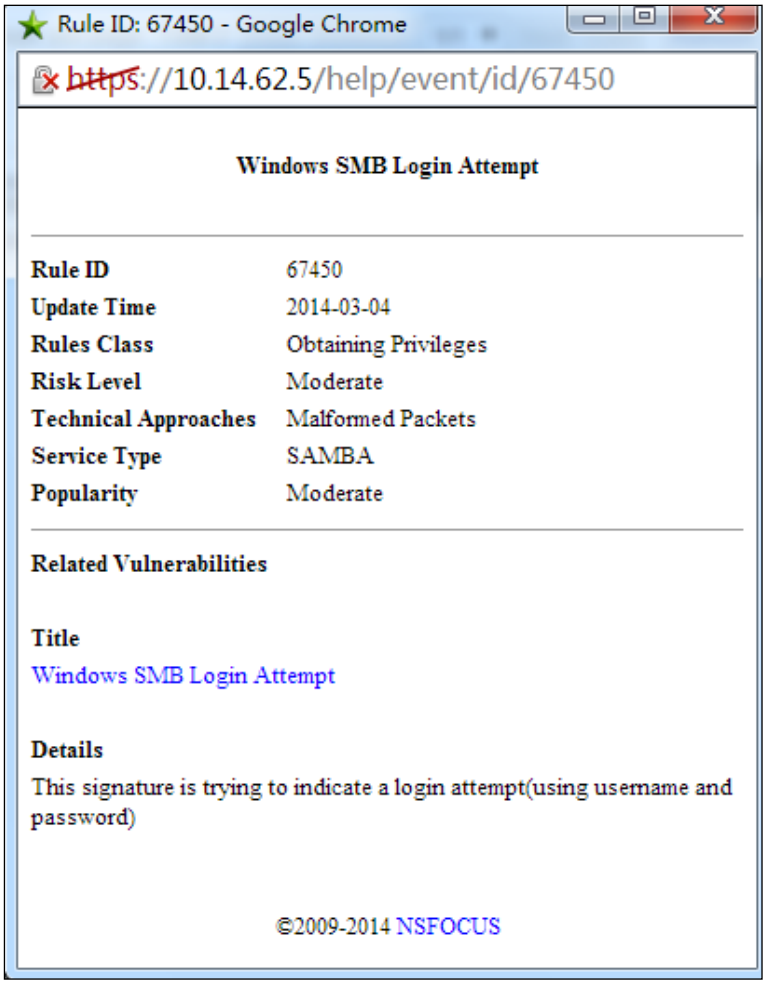
Step 1 Choose **Object > Rule > Exception Rule**.

Figure 6-13 Exception rules



Step 2 Click the rule ID to view detailed information.

Figure 6-14 Detailed information about the rule



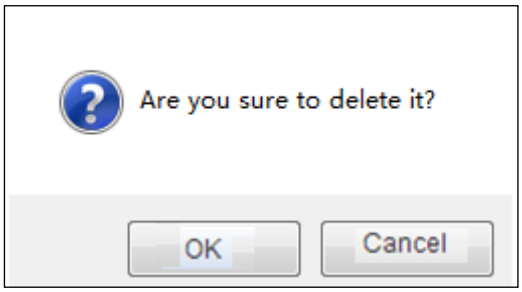
----End

Deleting an Exception Rule

Step 1 Click in the **Operation** column of an exception rule.

A confirmation dialog box appears, as shown in Figure 6-15.

Figure 6-15 Confirmation dialog box



Step 2 Click **OK** to delete the exception rule.

Step 3 Apply the settings.

----End

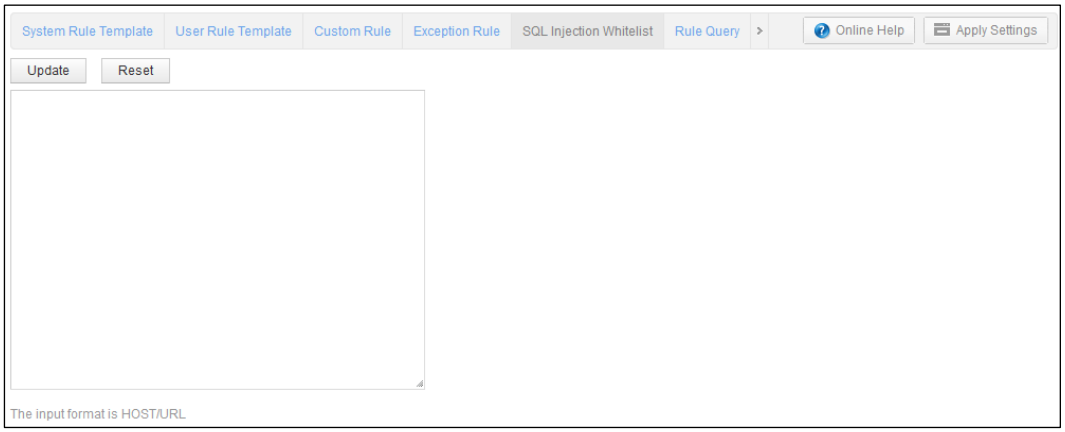
6.1.5 SQL Injection Whitelist

The SQL injection whitelist is a core function of NIPS in terms of intrusion prevention. This section describes how to configure a whitelist.

If the objects to which an intrusion prevention policy applies include "[29001]WEB Service Remote SQL Injection Suspicious Behavior" and this policy is expected to ignore some servers, add the URLs of these servers to the SQL injection whitelist.

Step 1 Choose **Object**> **Rule** > **SQL Injection Whitelist**.

Figure 6-16 SQL injection whitelist



Step 2 Enter URLs of servers that will not be protected against SQL injection.

Note	• The host name and domain name of a URL should be separated with a slash (/), for example, www.google.cn/zh-CN. • Each URL should be entered in a separate line.

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

If necessary, click **Reset** to undo the configuration.

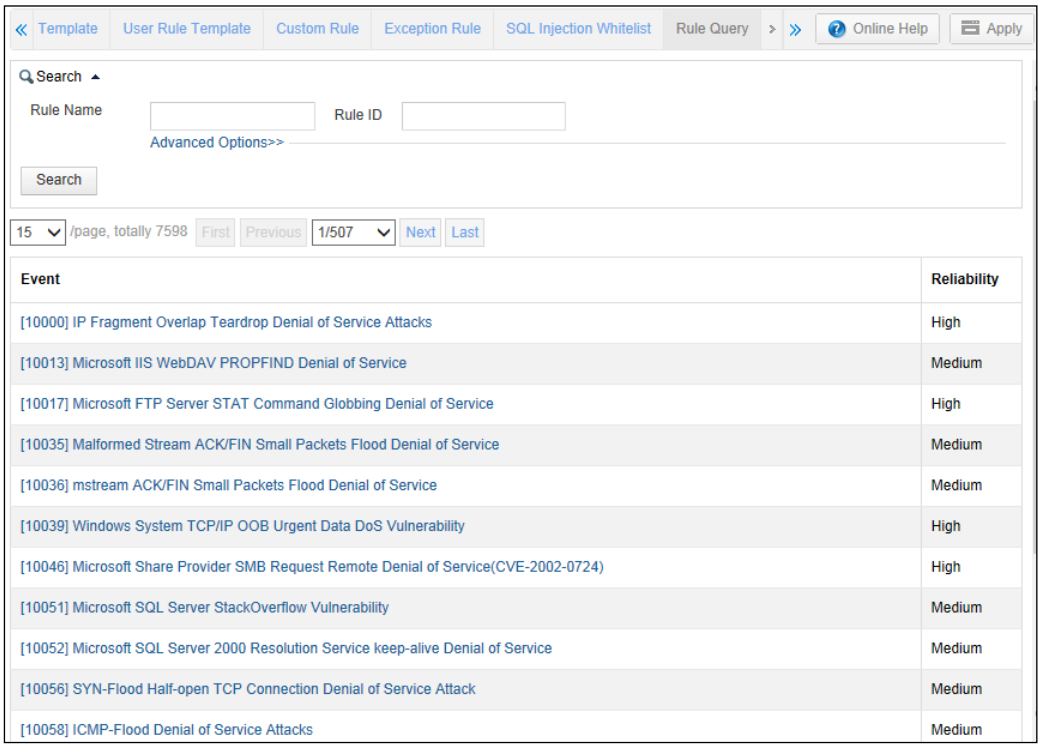
Step 4 Apply the settings.

----End

6.1.6 Rule Query

Step 1 Choose **Object** > **Rule** > **Rule Query**.

Figure 6-17 Rule query



You can search for intrusion prevention rules from the rule base in either of the following ways:

- By rule ID
- By rule name

In addition, you can narrow down the search scope to achieve more accurate results by configuring **Advanced Options**.

Step 2 Click **Advanced Options**.

The **Advanced Options** area appears, as shown in Figure 6-18.

Figure 6-18 Advanced Options area

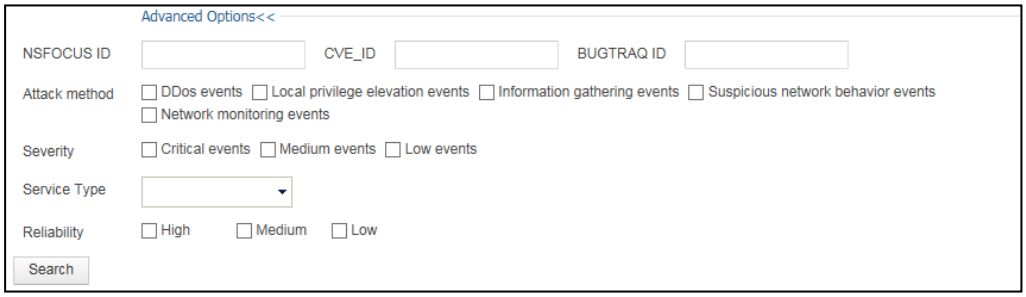


Table 6-9 describes advanced parameters.

Table 6-9 Advanced parameters

Parameter	Description
NSFOCUS_ID	Specifies the NSFOCUS ID of intrusion prevention rules to search for.
CVE_ID	Specifies the CVE ID of intrusion prevention rules to search for.
BUGTRAQ_ID	Specifies the BUGTRAQ ID of intrusion prevention rules to search for.
Attack Method	Specifies the attack method of intrusion prevention rules to search for.
Severity	Specifies the risk level of intrusion prevention rules to search for.
Service Type	Specifies the service type of intrusion prevention rules to search for.
Reliability	Specifies the reliability of intrusion prevention rules to search for.

----End

6.2 Configuring Network Objects

Network objects are used to describe network devices or device groups. Currently, NIPS supports the following network objects:

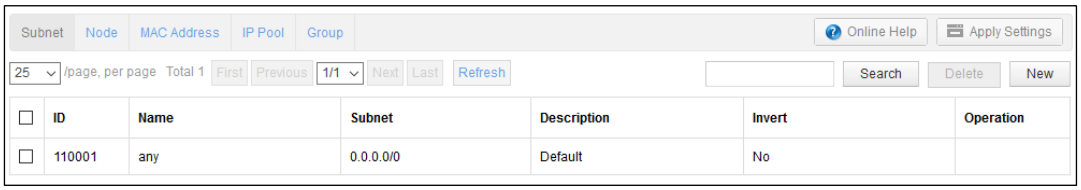
- Subnet
- Node
- MAC address
- IP address pool
- Group

6.2.1 Subnet

A subnet object is a network segment, that is, an IPv4 or IPv6 subnet specified by an IP address and subnet mask. To configure a subnet object, follow these steps:

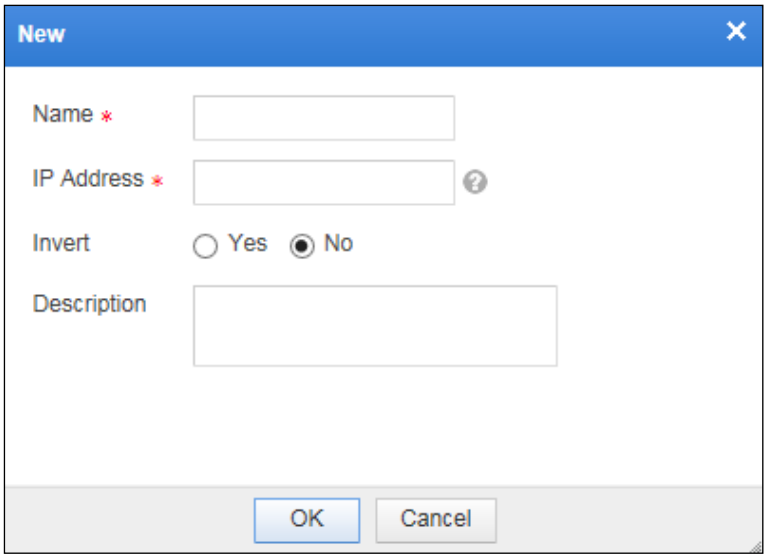
Step 1 Choose **Object** > **Network** > **Subnet**.

Figure 6-19 Subnet object list



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

Figure 6-20 Configuring a subnet object



Step 3 Configure parameters in the **New** dialog box.

Table 6-10 Parameters for configuring a subnet object

Parameter	Description
Name	Specifies the name of the subnet object. The name must be unique in the system and cannot contain spaces and the following special characters: / % \ ` @ ^ < > { } ' & " :
IP Address	Specifies the IP address and subnet mask of an IPv4 or IPv6 subnet.
Invert	Controls whether the specified network segment or the other network segments than the specified one are configured as the subnet object. • **Yes**: indicates that the other network segments than the specified one are used as the subnet object. • **No**: indicates that the specified network segment is used as the subnet object.
Description	Brief description of the subnet object.

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

Step 5 Apply the settings.

----End

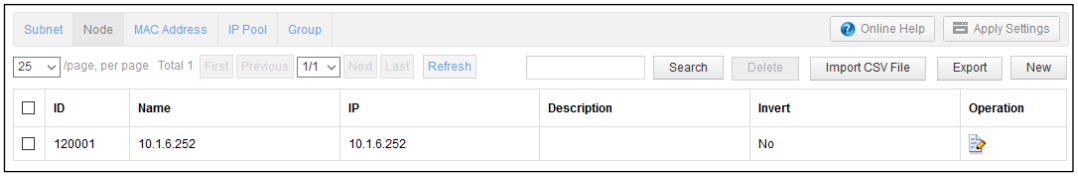
6.2.2 Node

A node object refers to a host specified by an IPv4 or IPv6 address. You can add a node object in either of the following ways.

6.2.2.1 Configuring a Node Object

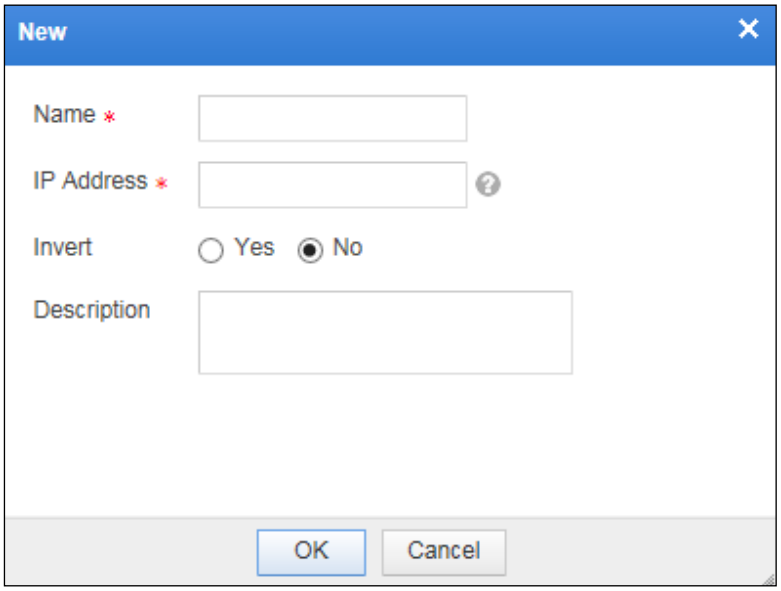
Step 1 Choose **Object** > **Network** > **Node**.

Figure 6-21 Node object list



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

Figure 6-22 Configuring a node object



Step 3 Configure parameters in the **New** dialog box.

Table 6-11 Parameters for configuring a node object

Parameter	Description
Name	Specifies the name of the node object. The name must be unique in the system and cannot contain spaces and the

Parameter	Description
	following special characters: / % \ ` @ ^ < > { } ' & " :
IP Address	Specifies the IP address of the node object, which can be an IPv4 address (such as 192.168.1.1) or IPv6 address (such as fe80::250:56ff:fec0:8).
Invert	Controls whether the specified IP address or other IP addresses than the specified one are used as the node object. • **Yes**: indicates that the other IP addresses than the specified one are used as the node object. • **No**: indicates that the specified IP address is used as the node object.
Description	Brief description of the node object.

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

Step 5 Apply the settings.

----End

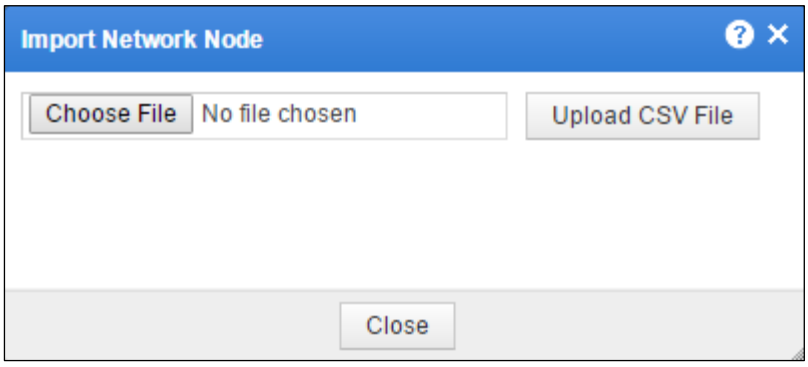
6.2.2.2 Importing a Node Object

Before importing a CSV file, you need to obtain the CSV file from a third-party device or create one that contains information about a large number of nodes.

Caution	Note the following when creating a CSV file: • The name and IP address of a node cannot be empty. • The name is the unique identity of a node. • Both IPv4 (such as 192.168.1.1) and IPv6 (such as fe80::250:56ff:fec0:8/64) are accepted. • The node description is optional. A node description, if any, cannot the following characters: < > / \ ' ` Example: • a node only with the name and IP address: nsfocus1,1.1.1.1 • a node with complete information: nsfocus3,2.2.2.2,Nsfocus

Step 1 On the **Node** page, click **Import CSV File**.

Figure 6-23 Import Network Node dialog box



Step 2 Click **Browse** and select the CVS file.

Step 3 Click **Upload CSV File**.

----End

6.2.2.3 Exporting a Node Object

You can export node objects in the list as a CSV file for backup. The procedure is as follows:

Step 1 On the page shown in Figure 6-21, click **Export**.

Step 2 In the dialog box that appears, click **Save**.

By default, the system exports the object to the **node.csv** file in the download directory of the host.

You can also click the drop-down arrow next to **Save** and choose **Save As** to export this node to another file or directory.

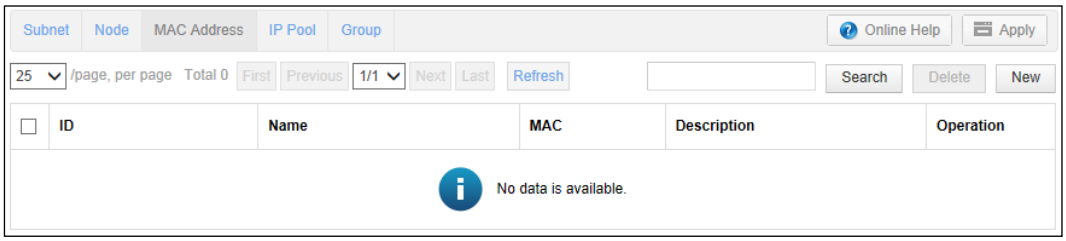
----End

6.2.3 MAC Address

An MAC address object refers to a single MAC address. To configure an MAC address object, follow these steps:

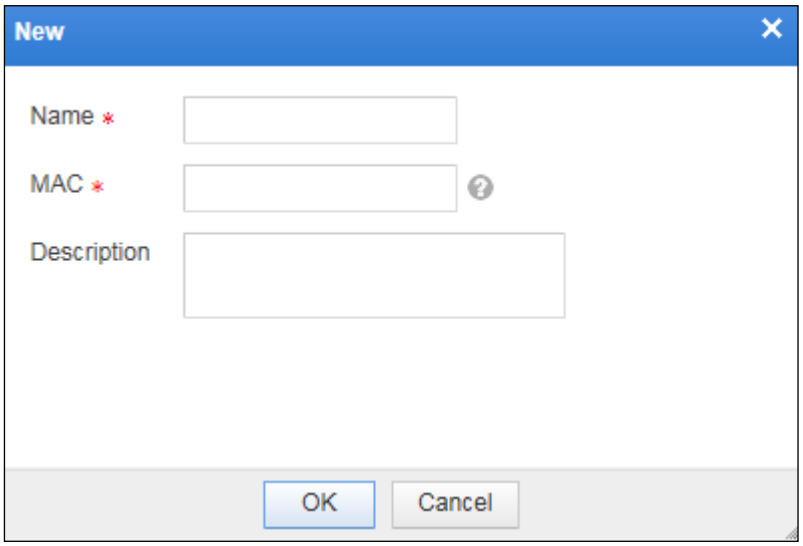
Step 1 Choose **Object** > **Network** > **MAC Address**.

Figure 6-24 MAC address object list



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

Figure 6-25 Configuring an MAC address object



Step 3 Configure parameters in the **New** dialog box.

Table 6-12 Parameters for configuring an MAC address object

Parameter	Description
Name	Specifies the name of the MAC address object. The name must be unique in the system and cannot contain spaces and the following special characters: / % \ ` @ ^ < > { } ' & " :
MAC	Specifies the MAC address of the object. The format of this value is "XX-XX-XX-XX-XX-XX" or "XX:XX:XX:XX:XX:XX", in which *X* is a hexadecimal character.
Description	Brief description of the MAC address object.

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

Step 5 Apply the settings.

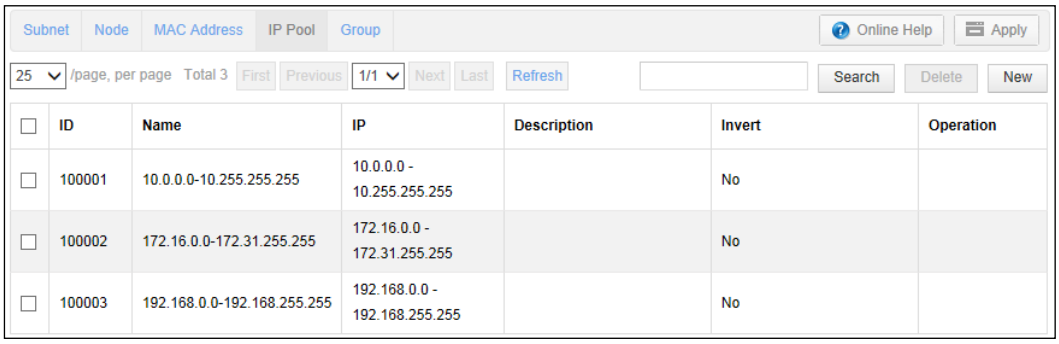
----End

6.2.4 IP Address Pool

An IP address pool is a range of consecutive IPv4 or IPv6 addresses that identify hosts. To configure an IP address pool object, follow these steps:

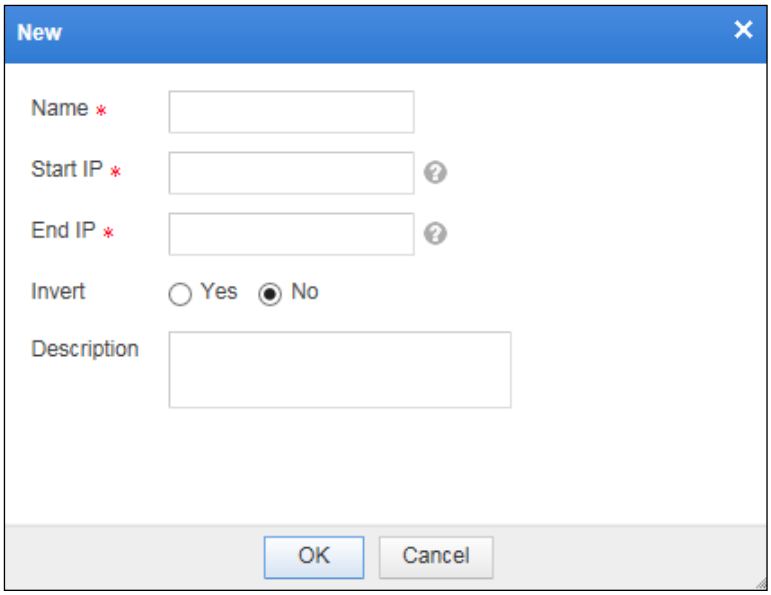
Step 1 Choose **Object** > **Network** > **IP Pool**.

Figure 6-26 IP address pool objects



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

Figure 6-27 Configuring an IP pool object



Step 3 Configure parameters in the **New** dialog box.

Table 6-13 Parameters for creating an IP address pool object

Parameter	Description
Name	Specifies the name of the IP address pool object. The name must be unique in the system and cannot contain spaces and the following special characters: / % \ ` @ ^ < > { } ' & " :
Start IP	Specifies the IP address pool's start IP address, which can be an IPv4 or IPv6 address. The version of the start IP address must be the same as that of the end IP address.
End IP	Specifies the IP address pool's end IP address, which can be an IPv4 or IPv6

Parameter	Description
	address. The version of the end IP address must be the same as that of the start IP address, and must be greater than the start IP address.
Invert	Controls whether the specified IP address range or other ranges than the specified one are used as the IP address pool object. • **Yes**: indicates that the other IP address ranges than the specified one are used as the IP address pool object. • **No**: indicates that the specified IP address range is used as the IP address pool object.
Description	Brief description of the IP address pool object.

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

Step 5 Apply the settings.

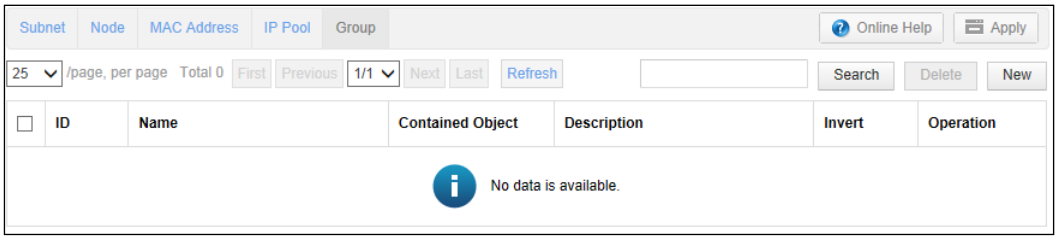
----End

6.2.5 Network Group

A network group object refers to a logical collection of network objects, node objects, MAC address objects, IP address pool objects, and existing group objects. To configure a network group object, follow these steps:

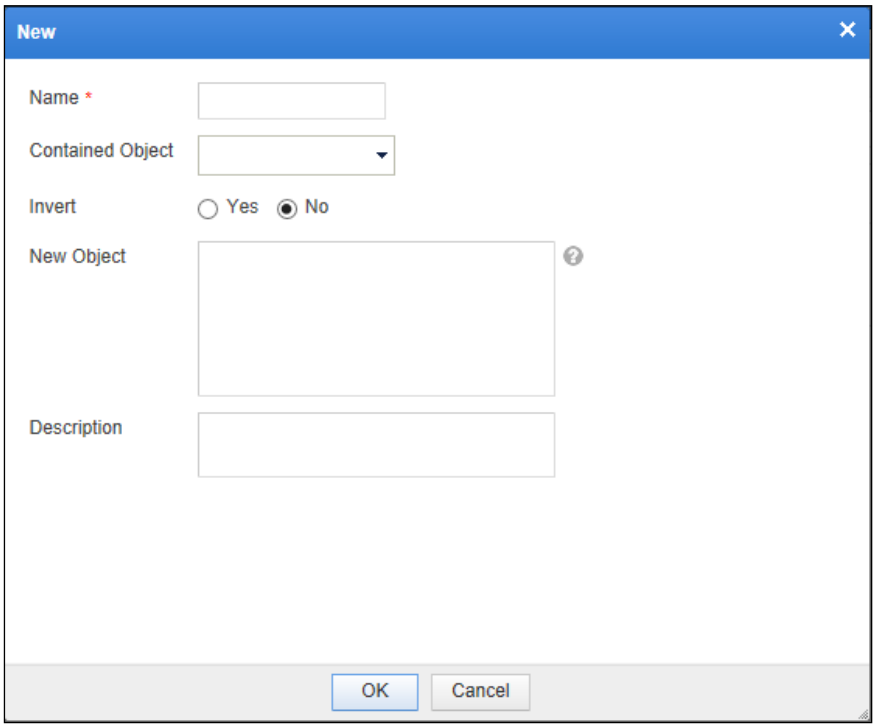
Step 1 Choose **Object** > **Network** > **Group**.

Figure 6-28 Network group object list



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

Figure 6-29 Configuring a network group object



Step 3 Configure parameters in the **New** dialog box.

Table 6-14 Parameters for configuring a network group object

Parameter	Description
Name	Specifies the name of the network group object. The name must be unique in the system and cannot contain spaces and the following special characters: / % \ ` @ ^ < > { } ' & " :
Contained Object	Specifies the objects that can be contained in the network group.
Invert	Controls whether the selected network objects or other network objects in the drop-down list than the selected ones are contained in the network group object. • **Yes**: indicates that the other network objects than the selected ones are contained in the network group object. • **No**: indicates that the selected network objects are contained in the network group object.
New Object	New network objects, including subnets, nodes, MAC addresses, and IP pools. Multiple objects must be separated by carriage returns, that is, each object takes up a separate line. New objects are named in the format of "group name_object name".
Description	Brief description of the network group object.

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

Step 5 Apply the settings.

----End

6.3 Configuring Service Objects

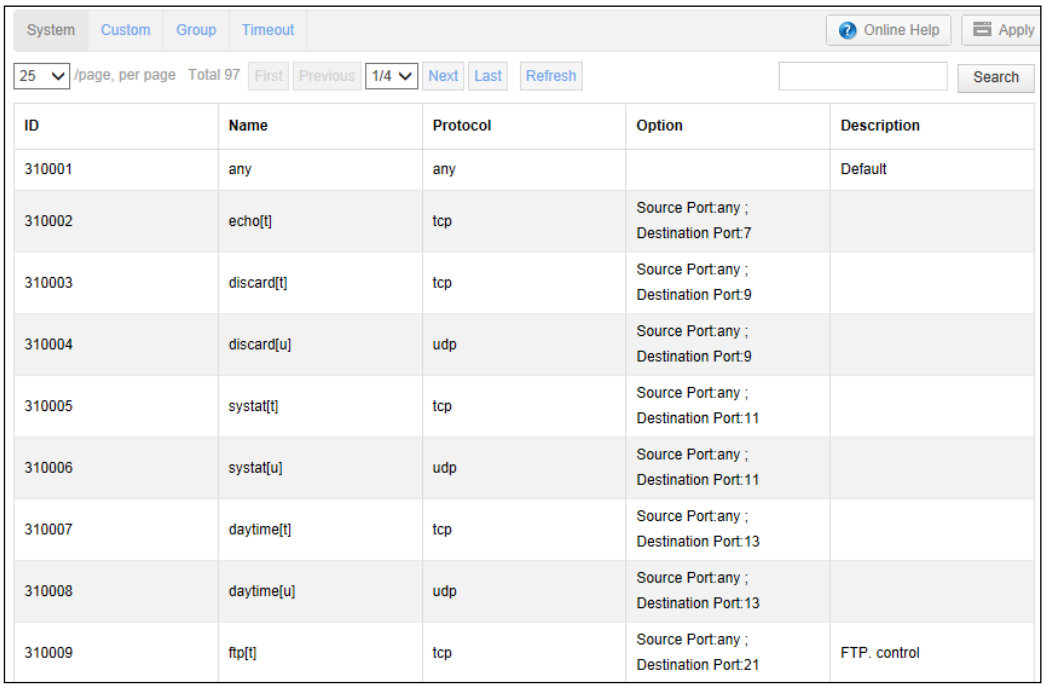
Service objects are used to describe system services, custom services, service groups, and timeout objects.

6.3.1 System Service

System service objects are pre-defined services on NIPS. Such objects support automatic protocol recognition and recognition of protocols on non-fixed ports. Common protocols, such as FTP and BitTorrent, can be recognized.

Choose **Object** > **Service** > **System**.

Figure 6-30 System service object list



ID	Name	Protocol	Option	Description
310001	any	any		Default
310002	echo[t]	tcp	Source Port:any ; Destination Port:7	
310003	discard[t]	tcp	Source Port:any ; Destination Port:9	
310004	discard[u]	udp	Source Port:any ; Destination Port:9	
310005	systat[t]	tcp	Source Port:any ; Destination Port:11	
310006	systat[u]	udp	Source Port:any ; Destination Port:11	
310007	daytime[t]	tcp	Source Port:any ; Destination Port:13	
310008	daytime[u]	udp	Source Port:any ; Destination Port:13	
310009	ftp[t]	tcp	Source Port:any ; Destination Port:21	FTP. control

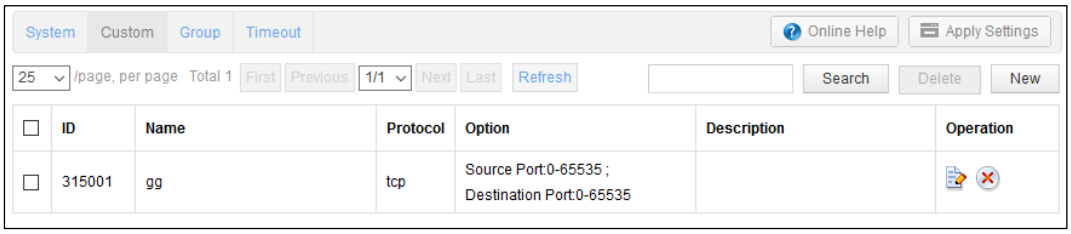
The **System** page lists all pre-defined service objects on NIPS. You can only view and reference these objects, but cannot create, edit, or delete them.

6.3.2 Custom Service

You can configure custom service objects (custom service ports) as required. To configure a custom service object, follow these steps:

Step 1 Choose **Object** > **Service** > **Custom**.

Figure 6-31 Custom service list



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

Figure 6-32 shows the **New** dialog box for configuring a TCP or UDP service object. Figure 6-33 shows the **New** dialog box for configuring an IP service object.

Figure 6-32 Configuring a TCP or UDP service object

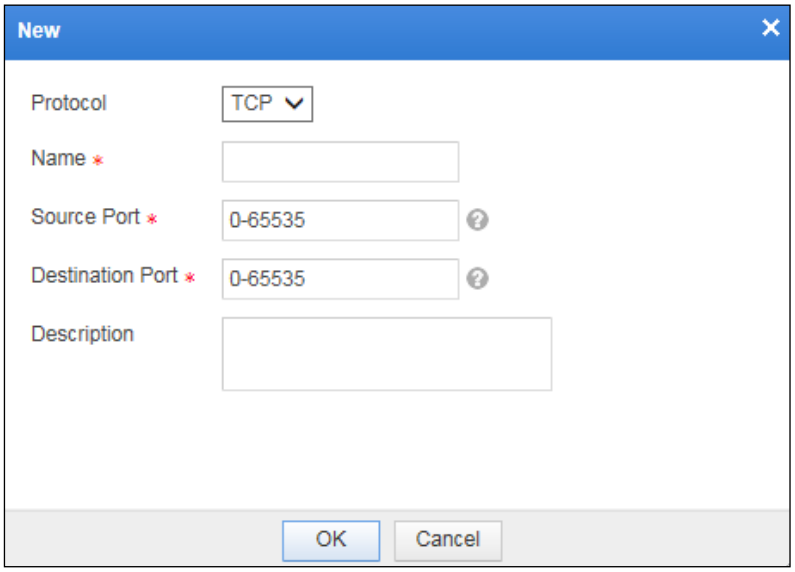
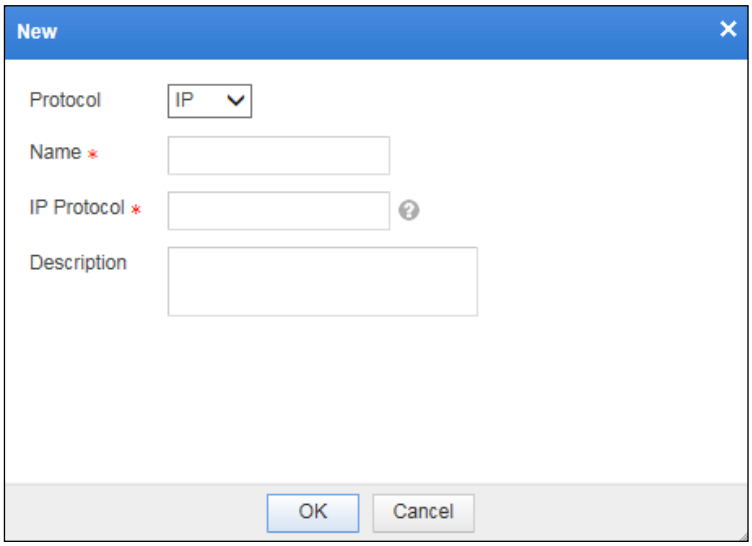


Figure 6-33 Configuring an IP service object



Step 3 Configure parameters in the **New** dialog box.

Table 6-15 Parameters for configuring a custom service object

Parameter	Description
Protocol	Specifies the protocol type, which can be **TCP**, **UDP**, or **IP**. Different protocols require different parameters. When **Protocol** is set to **TCP** or **UDP**, **Source Port** and **Destination Port** need to be specified. When **Protocol** is set to **IP**, **IP Protocol** needs to be specified.
Name	Specifies the name of the service object. The name must be unique in the system and cannot contain spaces and the following special characters: / % \ ` @ ^ < > { } ' & " :
Source Port	Specifies the source port of the service object. This parameter needs to be specified only when **Protocol** is set to **TCP** or **UDP**. You can specify multiple ports or port ranges within the range of 0 to 65535.
Destination Port	Specifies the destination port of the service object. This parameter needs to be specified only when **Protocol** is set to **TCP** or **UDP**. You can specify multiple ports or port ranges within the range of 0 to 65535.
IP Protocol	Specifies the IP protocol ID. For example, **1** indicates ICMP and **2** indicates IGMP. The value range is 0–255. This parameter needs to be specified only when **Protocol** is set to **IP**.
Description	Brief description of the service object.

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

Step 5 Apply the settings.

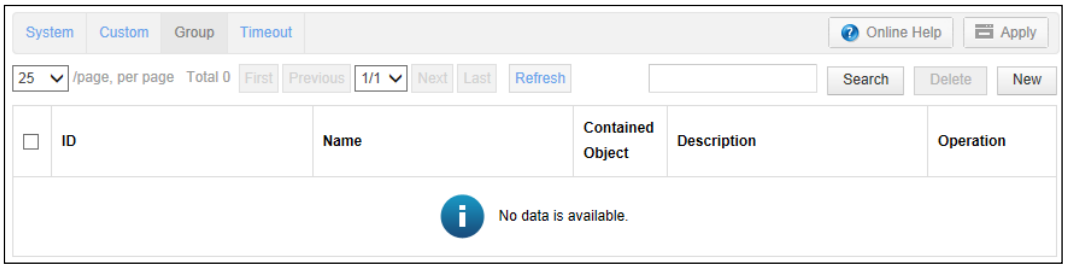
----End

6.3.3 Service Group

A service group object here refers to a logical collection of system service objects, custom service objects, and existing service group objects. To configure a service group object, follow these steps:

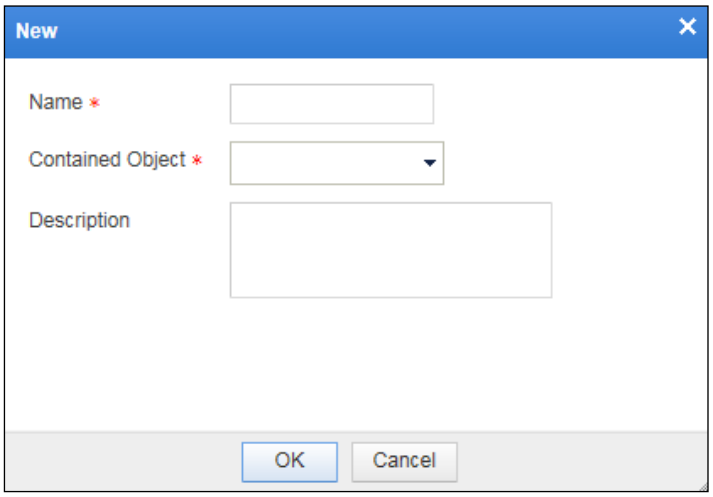
Step 1 Choose **Object** > **Service** > **Group**.

Figure 6-34 Custom service group list



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

Figure 6-35 Creating a service group object



Step 3 Configure parameters in the **New** dialog box.

Table 6-16 Parameters for configuring a service group object

Parameter	Description
Name	Specifies the name of the service group object. The name must be unique in the system and cannot contain spaces and the following special characters: / % \ ` @ ^ < > { } ' & " :
Contained Object	Specifies the objects contained in the service group.
Description	Brief description of the service group object.

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

Step 5 Apply the settings.

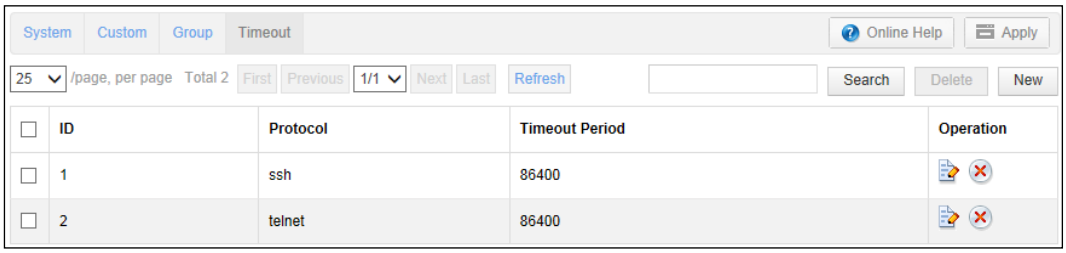
----End

6.3.4 Service Timeout

Time lengths for protocol communication can be specified for most protocols. You can specify a service timeout period as required. To configure a service timeout period, follow these steps:

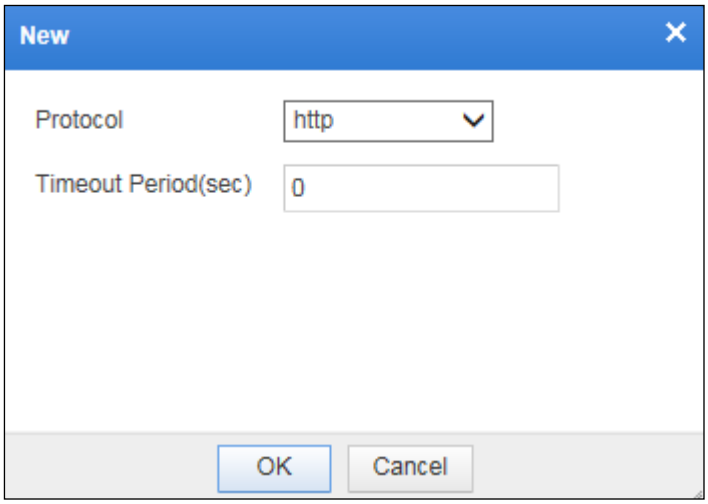
Step 1 Choose **Object** > **Service** > **Timeout**.

Figure 6-36 Service timeout period list



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

Figure 6-37 Configuring a service timeout period



Step 3 Configure parameters in the **New** dialog box.

Table 6-17 Parameters for configuring a service timeout period

Parameter	Description
Protocol	Specifies the type of the protocol used for communication.

Parameter	Description
	Note The timeout period for each protocol type can be configured only once.
Timeout Period(sec)	Specifies the timeout period for communication. The default value is **0**, which indicates that the communication will never time out. Note The timeout period refers to the allowed maximum interval between two consecutive data flows of the protocol. The service persists as long as the interval between two consecutive data flows is within the specified timeout period. If a long interval is required between two consecutive data flows of a protocol, you are advised to specify a long timeout period.

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

Step 5 Apply the settings.

----End

6.4 Configuring Application Objects

Application objects are used to describe various application technologies such as Kuwo player. The system is embedded with default application objects. Also, you can configure custom application objects and filters to filter packets by specifying application objects for application management policies.

This section describes how to view system application objects, create a custom application object, and configure a filter.

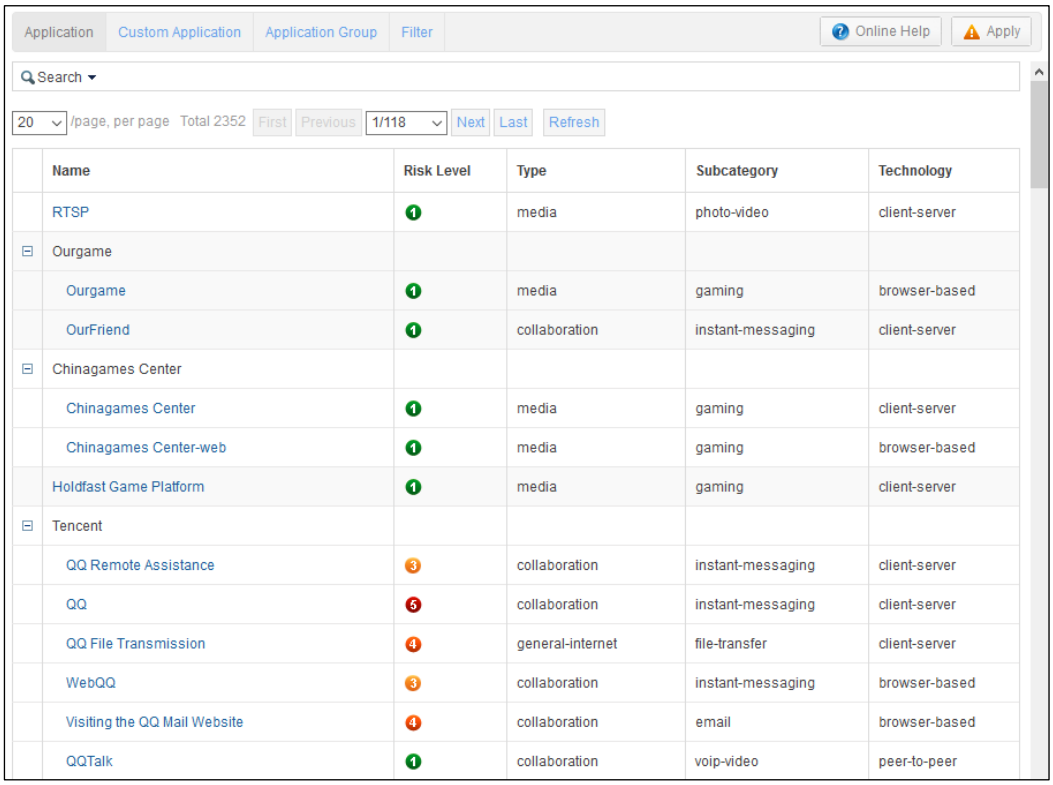
6.4.1 System Application

The NIPS system comes with system application objects. You can only reference and view them, but cannot create, edit, or delete them.

Step 1 Choose **Object** > **Application** > **Application**.

Click the name of a system application object to view details about this object.

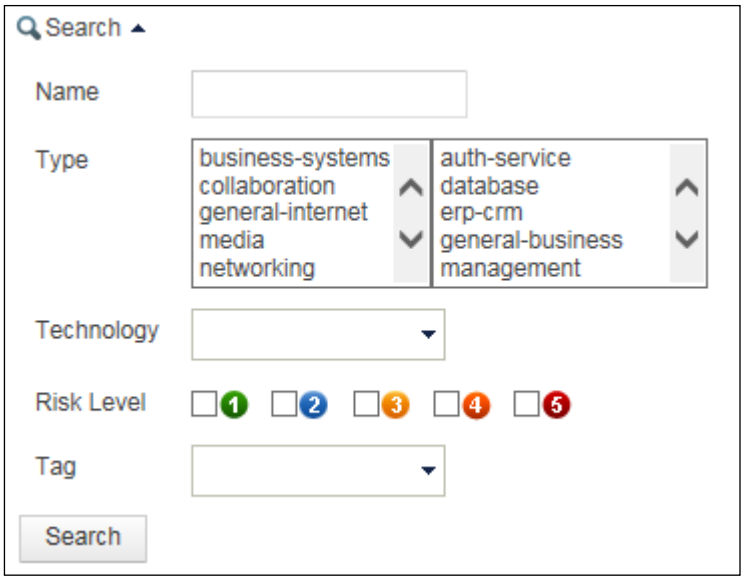
Figure 6-38 System application list



Name	Risk Level	Type	Subcategory	Technology
RTSP	1	media	photo-video	client-server
Ourgame				
Ourgame	1	media	gaming	browser-based
OurFriend	1	collaboration	instant-messaging	client-server
Chinagames Center				
Chinagames Center	1	media	gaming	client-server
Chinagames Center-web	1	media	gaming	browser-based
Holdfast Game Platform	1	media	gaming	client-server
Tencent				
QQ Remote Assistance	3	collaboration	instant-messaging	client-server
QQ	5	collaboration	instant-messaging	client-server
QQ File Transmission	4	general-internet	file-transfer	client-server
WebQQ	3	collaboration	instant-messaging	browser-based
Visiting the QQ Mail Website	4	collaboration	email	browser-based
QQTalk	1	collaboration	voip-video	peer-to-peer

Step 2 Click **Search** to search for desired system application objects.

Figure 6-39 Searching for system applications



Step 3 Configure parameters in the **Search** area.

Table 6-18 Parameters for querying system applications

Parameter	Description
Name	Specifies the name of the system application object.
Type	Specifies the type and subtype to which a system application object belongs.
Technology	Specifies the technology on which the system application object is based. The value can be **browser-based**, **client-server**, **network-protocol**, **peer-to-peer**, or **unknown**.
Risk Level	Specifies the risk level of the system application object. The value is an integer ranging from 1 to 5, and a larger value indicates a higher risk level.
Tag	Specifies the tag of the system application object. The value can be **Evasive**, **Excessive Bandwidth**, **Prone to Misuse**, **Transfers Files**, **Tunnels Other Apps**, **Used by Malware**, **Vulnerability**, or **Widely used**.

Step 4 Click **Search**.

System application objects that meet the conditions are displayed.

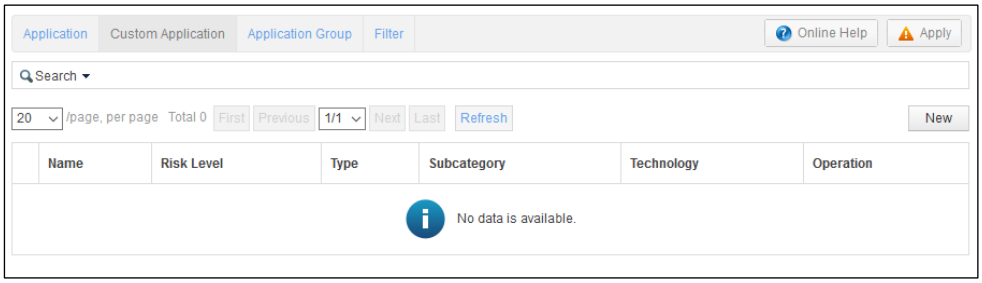
----End

6.4.2 Custom Application

In addition to system applications, you can configure custom application objects. To configure a custom application object, follow these steps:

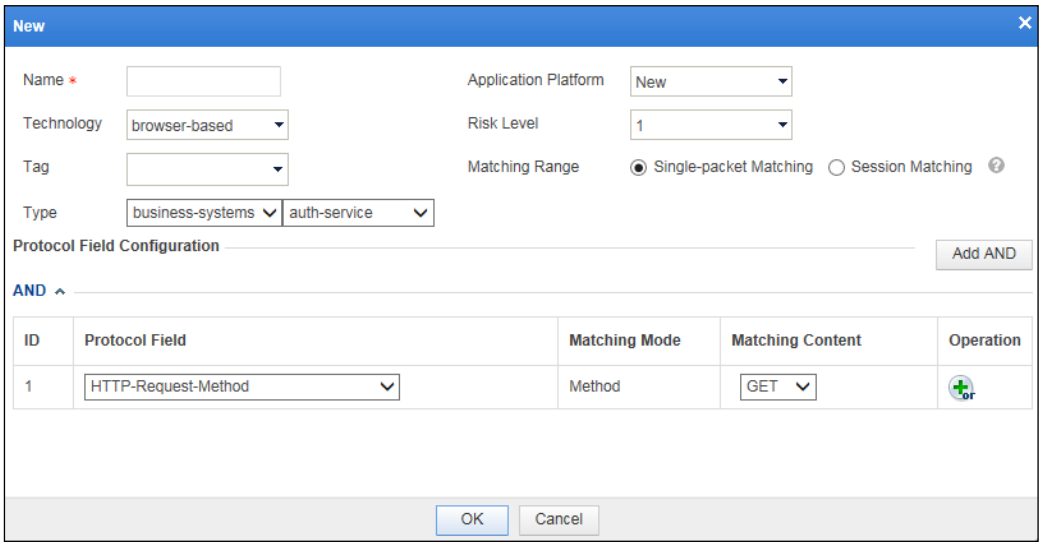
Step 1 Choose **Object** > **Application** > **Custom Application**.

Figure 6-40 Custom application object list



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

Figure 6-41 Configuring an application object



Step 3 Configure parameters in the **New** dialog box.

Table 6-19 Parameters for configuring an application object

Parameter	Description
Name	Specifies the name of the application object.
Application Platform	Specifies the platform on which the application object runs. If **Application Platform** is set to **New**, the name of the platform on which the application runs is the same as the name of the application.
Technology	Specifies the technology on which the system application object is based. The value can be **browser-based**, **client-server**, **network-protocol**, **peer-to-peer**, or **unknown**.
Risk Level	Specifies the risk level of the application. The value is an integer ranging from 1 to 5, and a larger value indicates a higher risk level. For how to evaluate the risk levels of application objects, see Calculating the Risk Level of an Application Object.
Tag	Specifies the tag of the application object. The value can be **Evasive**, **Excessive Bandwidth, Prone to Misuse**, **Transfers Files**, **Tunnels Other Apps**, **Used by Malware**, **Vulnerability**, and **Widely used**.
Matching Range	Specifies the matching range, which can be **Single-packet Matching** or **Session Matching**. • Single-packet matching means that NIPS matches a single packet with a rule and determines accordingly whether an attack exists. A packet is the minimum transmission unit on a packet-switched network. The coverage of single-packet matching is smaller than that of session matching. • Session matching means that NIPS matches a single session with a rule and determines accordingly whether an attack exists. A session is an uninterrupted request-response sequence between a client and server.
Type	Specifies the type of the custom application object.

Step 4 Configure protocol fields.

For how to configure protocol fields, see Step 4 in section 6.1.3.2 Advanced Rules.

Step 5 Click **OK** to save the settings.

Step 6 Apply the settings.

----End

Calculating the Risk Level of an Application Object

The risk level of an application object is calculated based on all tags of this object. From the perspective of risk level, tags are categorized into three types:

- High-level risk: indicates an application that tends to impose a severe impact on hosts or the entire network.
- Medium-level risk: indicates an application that will potentially impose an impact on the network.
- Low-level risk: indicates an application that is widely used but will not impose an impact on network security.

Table 6-20 lists the risk level of tags.

Table 6-20 Risk level of tags

No.	Tag	Description	Severity
1	evasive	Evasive	Medium
2	exband	Bandwidth consuming	Low
3	misuse	Prone to misuse	Low
4	transfer	Transferring files	Medium
5	tunnel	Using other applications as tunnels	Medium
6	malware	Used by malware	High
7	vulner	Vulnerable	High
8	widely	Widely used	Low

Tags are weighed based on the risk level. The risk value of an application is calculated using the following tag-based formulas:

$$a(x,y) = \begin{cases} 1, & x \in y \\ 0, & x \notin y \end{cases}$$

$$f(x,y) = \begin{cases} 10 \times a(x,y), x = \text{"}evasive\text{"} \\ 1 \times a(x,y), x = \text{"exband"} \\ 1 \times a(x,y), x = \text{misuse"} \\ 10 \times a(x,y), x = \text{"transfer"} \\ 10 \times a(x,y), x = \text{"tunnel"} \\ g(x,y) \times a(x,y), x = \text{"malware"} \\ 19 \times a(x,y), x = \text{"vulner"} \\ 1 \times a(x,y), x = \text{"widely"} \end{cases}$$

$$g(x,y) = \begin{cases} 19, & x = \text{"malware", } a(\text{"vulner"}, y) = 0 \\ 10, & x = \text{"}malware\text{"}, a(\text{"}vulner\text{"}, y) = 1 \end{cases}$$

$$h(x) = \lfloor \left(\sum_{k=\text{"evasive"}}^{\text{"widely"}} f(k,x) \Big/ 10 \right)$$

$$risk = \begin{cases} 5, & h(x) > 5 \\ h(x), & 0 < h(x) \leq 5 \\ 1, & h(x) = 0 \end{cases}$$

The following is an example of calculating the risk value of an application object:

x ={ "exband","malware","vulner","widely" }

h(x) = L((0 + f("exband",x) + 0 + 0 + 0 + f("malware",x) + f("vulner",x) + f("widely",x)) / 10)

h(x) = L((1*a("exband",x) + g("malware",x) * a("malware",x) + f("vulner",x) + f("widely",x)) / 10)

h(x) = L((1 + 10*1 + 19 + 1)/10)

h(x) = L(31/10)

h(x) = 3

0 < h(x) <= 5

risk = h(x) = 3

6.4.3 Application Group

NIPS provides the application group function for you to pick out desired data among massive amounts of data. You can configure application group to filter data handled by NIPS based on specific conditions.

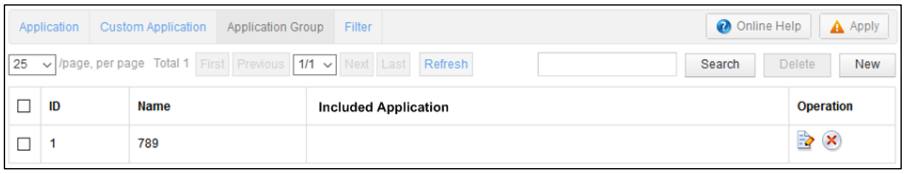
Note	Filters filter applications based on application type and tag, while application groups screen applications in a more flexible way by allowing users to pick out applications in terms of keywords in addition to the preceding conditions.

You can achieve the intended filtering effect with application groups only after applying them to application management policies and traffic management policies. For how to configure application management policies, see section 7.9 Configuring Application Management Policies. For how to configure traffic management policies, see section 7.10 Configuring Traffic Management Policies. To create an application group, follow these steps:

Step 1 Choose **Object** > **Application** > **Application Group**.

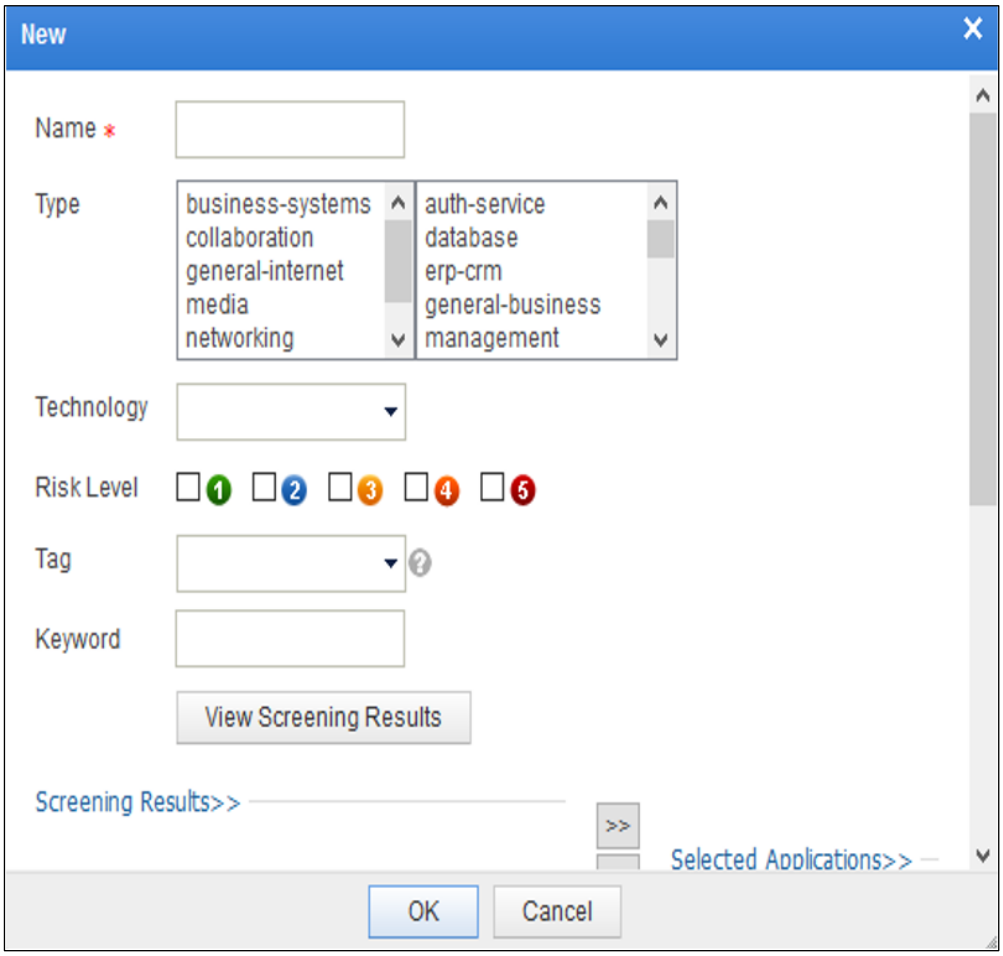
The **Application Group** page lists all current application group objects.

Figure 6-42 Application group list



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

Figure 6-43 Creating an application group object



Step 3 Set **Name** to the name of the new application group.

Step 4 Configure filtering parameters.

Table 6-21 Parameters for filtering applications by an application group

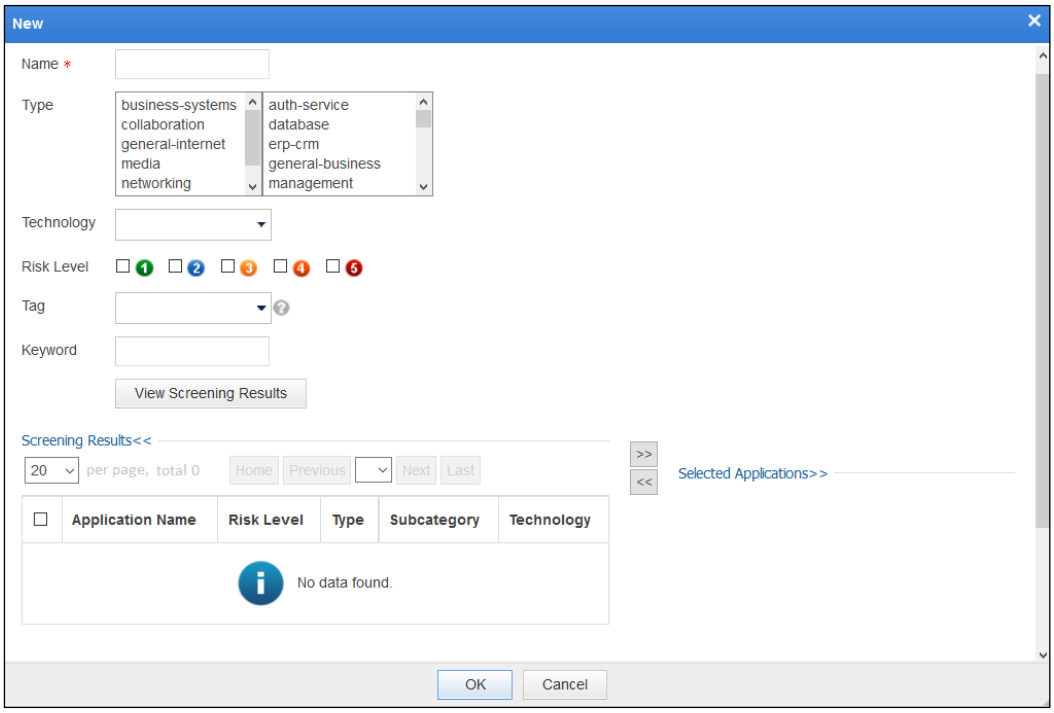
Parameter	Description
Type	Specifies the type and subtype of the application objects to be filtered by the application group.
Technology	Specifies the technologies by which the application objects to be filtered by the application group are implemented.
Risk Level	Specifies the risk levels of the application objects to be filtered by the application group.
Tag	Specifies the tags of the application objects to be filtered by the application group.
Keyword	Specifies the keywords based on which fuzzy search of applications are performed.

Step 5 Click **View Screening Results** to view all application objects that meet the filtering conditions.

Step 6 Select application objects to be included in the application group.

Select application objects and click >>. Then the selected applications will be added to the right list.

Figure 6-44 Viewing selected applications

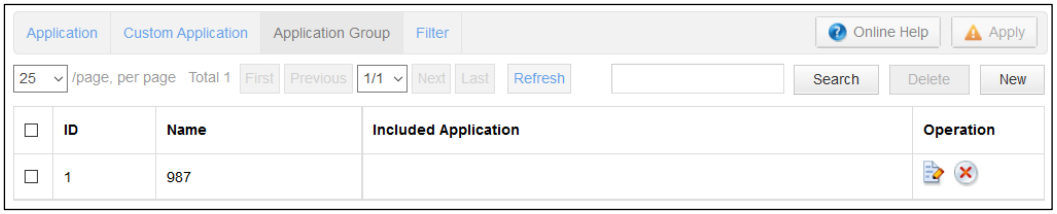


You can click << to remove the selected applications from the right list.

Step 7 Click **OK** to save the settings.

The new application group is displayed on the **Application Group** page.

Figure 6-45 Viewing the new application group



Step 8 Apply the settings.

----End

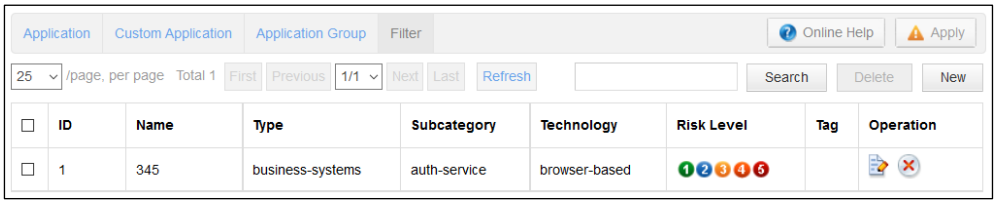
6.4.4 Filter

NIPS provides the filter function for you to pick out desired data among massive amounts of data. You can configure filters to filter data handled by NIPS based on specific conditions.

Filters can take effect only after being applied to application management policies. For how to configure application management policies, see section 7.9 Configuring Application Management Policies. This section describes how to create a filter.

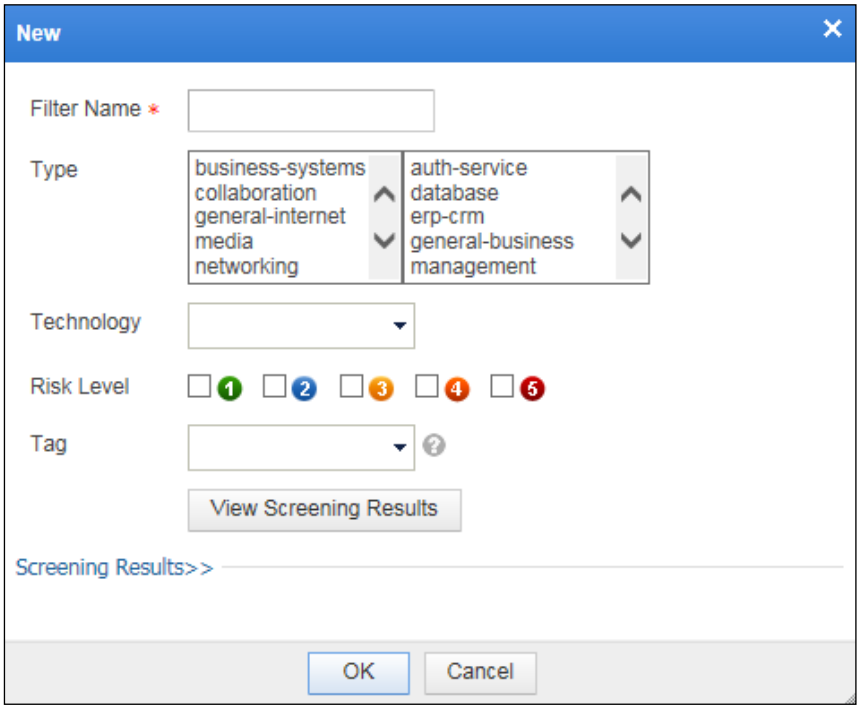
Step 1 Choose **Object** > **Application** > **Filter**.

Figure 6-46 Filter list



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

Figure 6-47 Creating a filter



Step 3 Configure parameters in the **New** dialog box.

Table 6-22 Parameters for creating a filter

Parameter	Description
Filter Name	Specifies the name of the filter.
Type	Specifies the type and subtype of the application objects to be filtered by the filter.
Technology	Specifies the technologies by which the application objects to be filtered by the filter are implemented.
Risk Level	Specifies the risk levels of the application objects to be filtered by the filter.
Tag	Specifies the tags of the application objects to be filtered by the filter.

After setting filtering parameters, you can click **View Screening Results** to view all application objects that meet the filtering conditions.

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

Step 5 Apply the settings.

----End

6.5 Configuring Time Objects

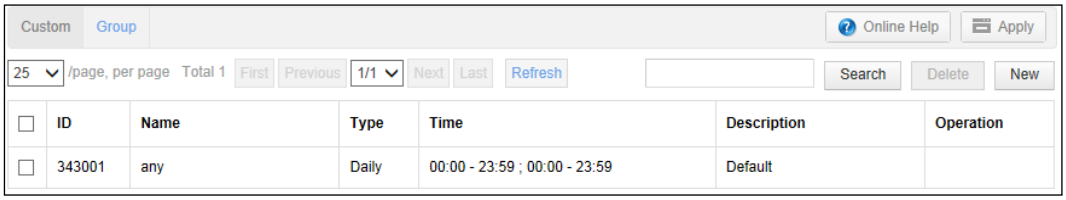
Time objects are used to describe time ranges. Time objects include custom time objects and time group objects. This section describes how to configure a custom time object and a time group object.

6.5.1 Custom Time

Each custom time object contains two time periods. You can configure custom time objects as required. To configure a time object, follow these steps:

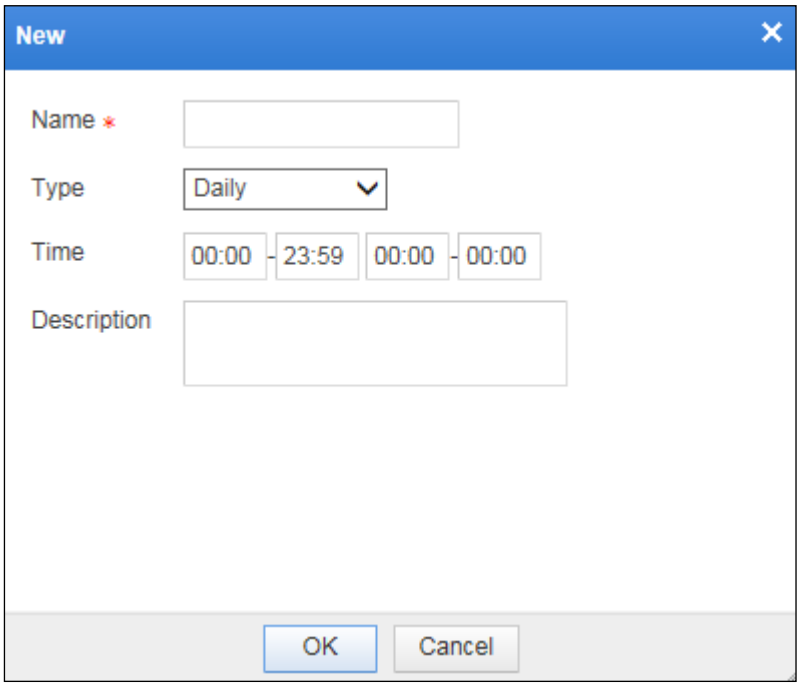
Step 1 Choose **Object** > **Time** > **Custom**.

Figure 6-48 Custom time object list



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

Figure 6-49 Configuring a time object



Step 3 Configure parameters in the **New** dialog box.

Table 6-23 Parameters for configuring a time object

Parameter	Description
Name	Specifies the name of the time object. The name must be unique in the system and cannot contain spaces and the following special characters: \ % ` @ ^ < > { } ' & " :
Type	Specifies the type of the time object. This parameter can be set to **Daily**, **Each workday** (Monday to Friday), **Weekly**, or **Monthly**.
Time	Specifies the two time periods contained in the time object. If only one time period is needed, leave the second time period at the default value **00:00-00:00**. If **Type** is set to **Monthly**, specify **Date** also.
Description	Brief description of the time object.

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

Step 5 Apply the settings.

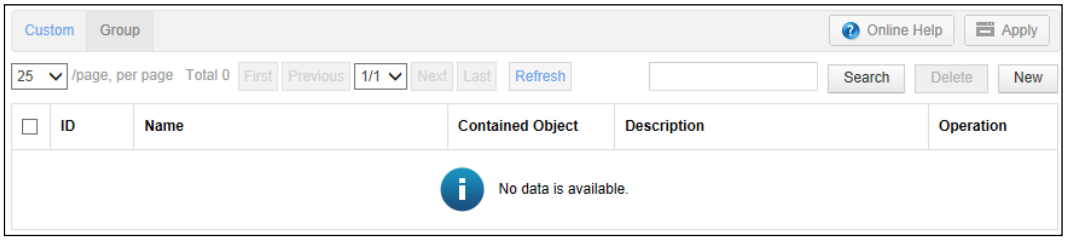
----End

6.5.2 Time Group

A time group refers to a logical collection of custom time objects and existing time groups. To configure a time group object, follow these steps:

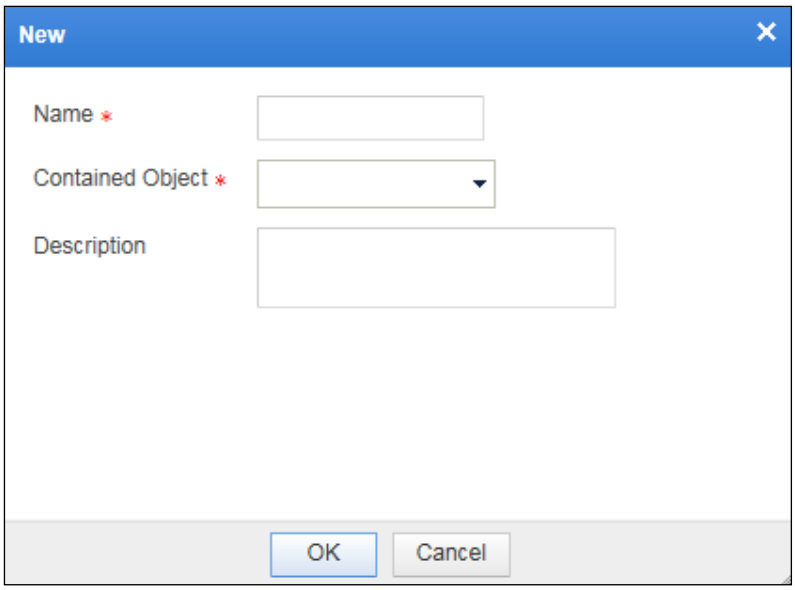
Step 1 Choose **Object** > **Time** > **Group**.

Figure 6-50 Time group list



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

Figure 6-51 Configuring a time group



Step 3 Configure parameters in the **New** dialog box.

Table 6-24 Parameters for configuring a time group object

Parameter	Description
Name	Specifies the name of the time group object. The name must be unique in the system and cannot contain spaces and the following special characters: / % \ ` @ ^ < > { } ' & " :
Contained Object	Specifies objects contained in the time group.
Description	Brief description of the time group object.

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

Step 5 Apply the settings.

----End

6.6 Configuring Sensitive Data Objects

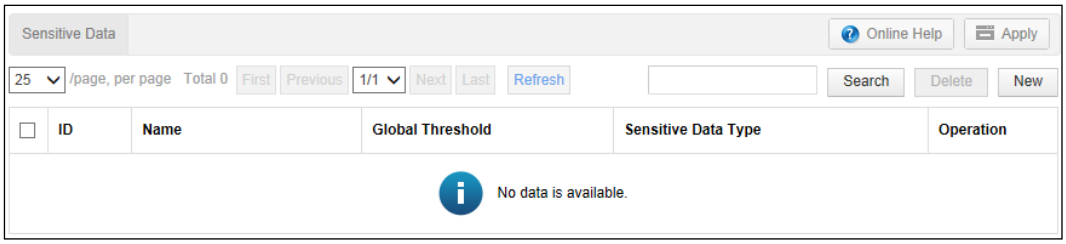
Sensitive data objects can be divided into system sensitive data objects and custom sensitive data objects.

6.6.1 System Sensitive Data Objects

Built-in sensitive data objects can protect internal sensitive data such as identity card numbers, bank card numbers, and telephone numbers, from being disclosed. To configure a sensitive data object, follow these steps:

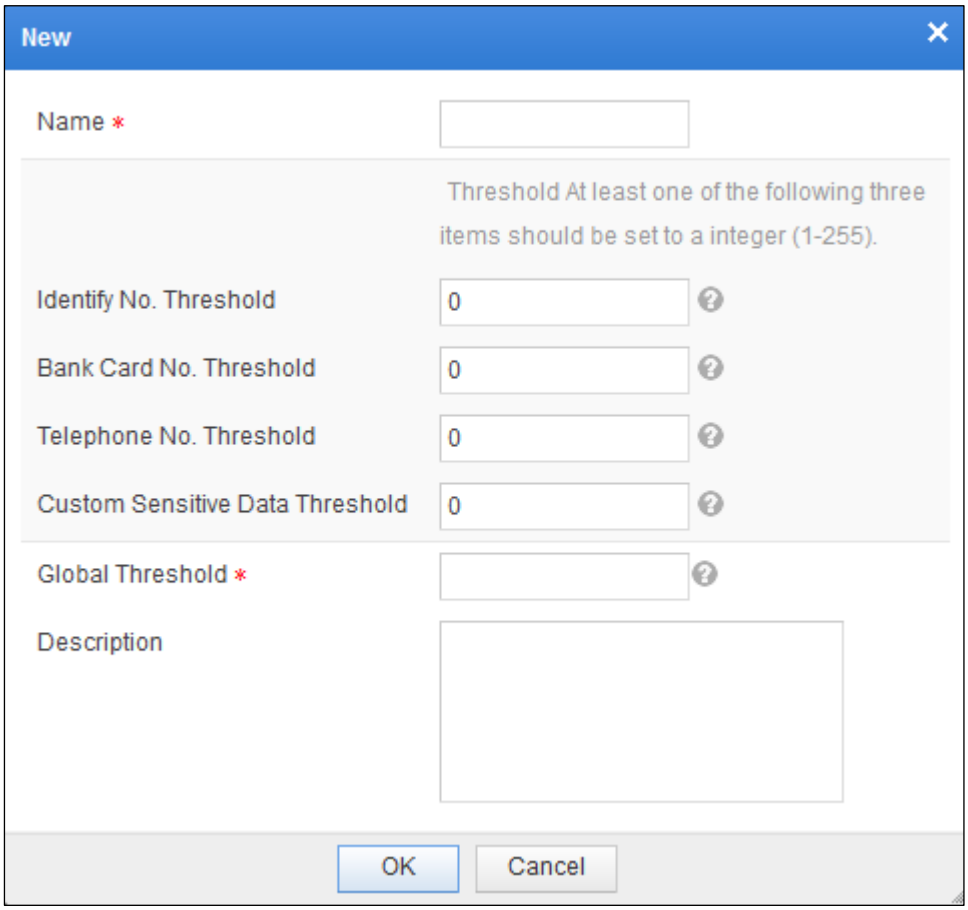
Step 1 Choose **Object** > **Sensitive Data** > **Sensitive Data**.

Figure 6-52 List of system sensitive data objects



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

Figure 6-53 Configuring a system sensitive data object



Step 3 Configure parameters in the **New** dialog box.

Table 6-25 Parameters for configuring a system sensitive data object

Parameter	Description
Name	Specifies the name of a system sensitive data object. The name must be unique in the system and cannot contain spaces and the following special characters: \ % ` @ ^ < > { } ' & " :
Identify No. Threshold	Specifies the number of occurrences of identity card numbers, which must be smaller than the global threshold.
Bank Card No. Threshold	Specifies the number of occurrences of bank card numbers, which must be smaller than the global threshold.
Telephone No. Threshold	Specifies the number of occurrences of telephone numbers, which must be smaller than the global threshold.
Custom Sensitive Data Threshold	Specifies the number of occurrences of a type of sensitive data, above which an alert of this type will be triggered.
Global Threshold	Specifies the number of occurrences of sensitive data, which must be greater than the threshold of each type of sensitive data. The value must be an integer ranging from 0 to 65535.

Parameter	Description
	When the total number of occurrence of sensitive data (including identity card numbers, bank card numbers, and telephone numbers) exceeds the global threshold, a global sensitive data alert will be generated.
Description	Brief description of the sensitive data object.

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

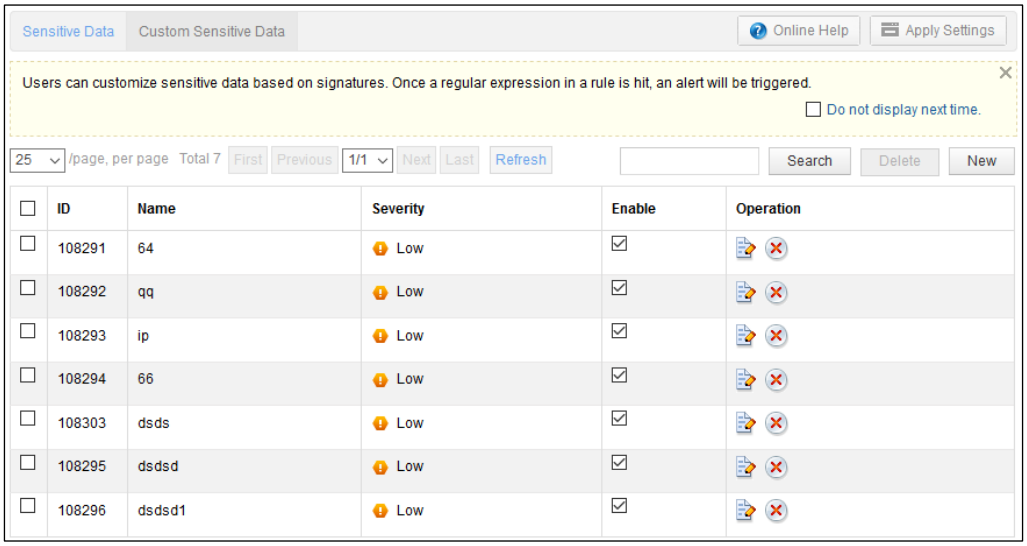
----End

6.6.2 Custom Sensitive Data Objects

To configure a custom sensitive data object, follow these steps:

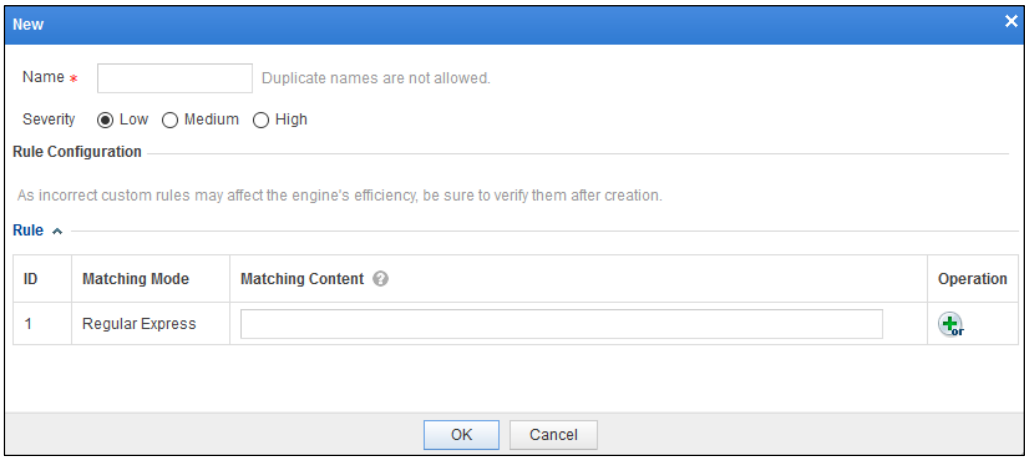
Step 1 Choose **Object** > **Sensitive Data** > **Custom Sensitive Data**.

Figure 6-54 List of custom sensitive data objects



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

Figure 6-55 Creating a custom sensitive data object



Step 3 Configure parameters in the **New** dialog box.

Table 6-26 Parameters for creating a custom sensitive data object

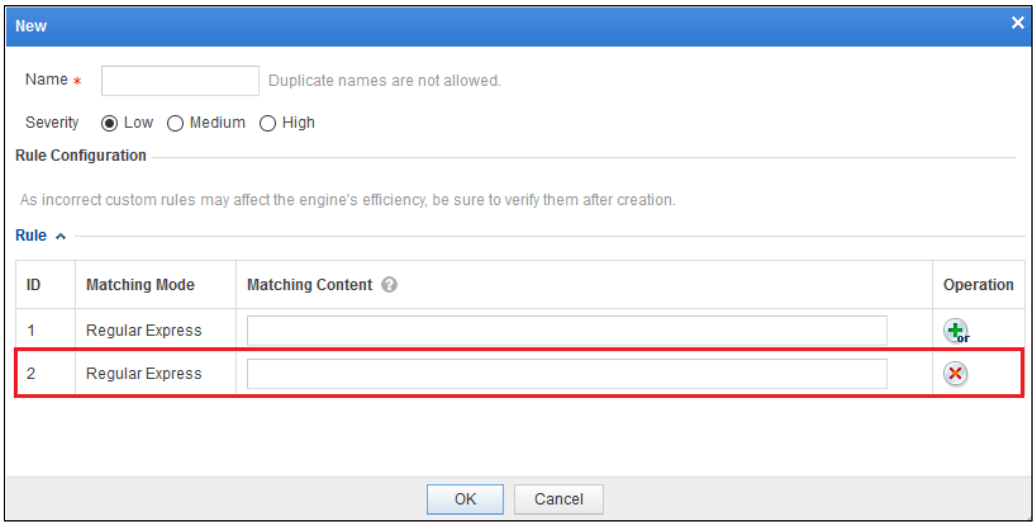
Parameter	Description
Name	Specifies the name of a custom sensitive data object. The name must be unique in the system and cannot contain spaces and the following special characters: \ % ` @ ^ < > { } ' & " :
Severity	Specifies the severity of a custom sensitive data object.

Step 4 Configure rules.

Caution	As incorrect custom rules may affect the engine's efficiency, verify the validity of a rule after creating it.

a. Click in the **Operation** column to add a regular expression for the OR relationship.

Figure 6-56 Adding a regular expression for matching in the OR relationship



b. Add the matching content.

Add the matching content by following the template, (^|[^\d])436742\d{10}([^\d]|$). This template represents 16 digits, with the first six being 436742.

Step 5 Click **OK** to save the settings.

Step 6 Apply the settings.

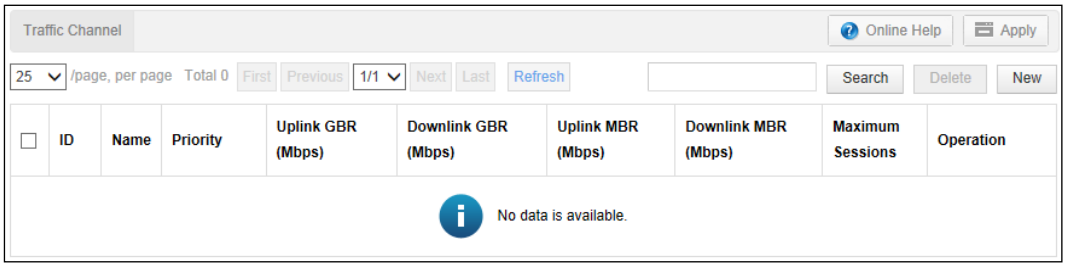
----End

6.7 Configuring a Traffic Channel Object

Traffic channel objects are used by traffic channel management policies, thereby facilitating traffic management over different channels. To configure a traffic channel object, follow these steps:

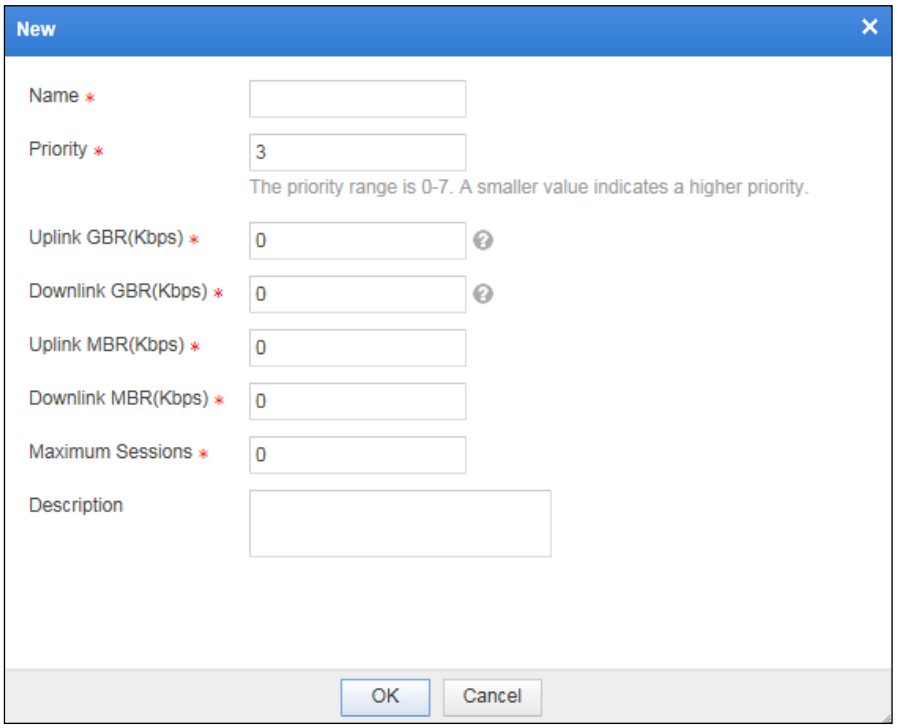
Step 1 Choose **Object** > **Traffic Channel**.

Figure 6-57 Traffic channel list



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

Figure 6-58 Configuring a traffic channel



Step 3 Configure parameters in the **New** dialog box.

Table 6-27 Parameters for configuring a traffic channel object

Parameter	Description
Name	Specifies the name of the traffic channel object. The name must be unique in the system and cannot contain spaces and the following special characters: \ % ` @ ^ < > { } ' & " :
Priority	Specifies the priority of the traffic channel object. This parameter can be set to an integer ranging from 0 to 7. A smaller value indicates a higher priority.
Uplink GBR(Kbps)	Specifies the minimum bit rate (unit: kbps) for outgoing traffic. The default value is **0**, indicating that there is no bit rate limit. Note The total uplink traffic must be greater than the sum of uplink GBRs of traffic channels involved in all policies.
Downlink GBR(Kbps)	Specifies the minimum bit rate (unit: kbps) for incoming traffic. The default value is **0**, indicating that there is no bit rate limit. Note The total downlink traffic must be greater than the sum of downlink GBRs of traffic channels involved in all policies.
Uplink MBR(Kbps)	Specifies the maximum bit rate (unit: kbps) for outgoing traffic. The default

Parameter	Description
	value is **0**, indicating that there is no bit rate limit.
Downlink MBR(Kbps)	Specifies the maximum bit rate (unit: kbps) for incoming traffic. The default value is **0**, indicating that there is no bit rate limit.
Maximum Sessions	Specifies the maximum number of TCP sessions allowed by the traffic channel. The default value is **0**, indicating that there is no limit to the number of TCP sessions.
Description	Brief description of the traffic channel object.

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

----End

6.8 Clearing Asset Trees

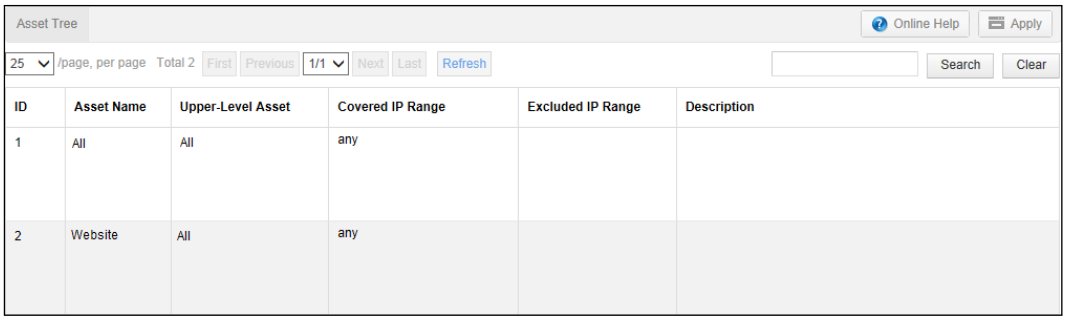
After NIPS successfully connects to ESPC, ESPC can dispatch asset trees to NIPS.

Note	After receiving asset trees from ESPC, NIPS identifies assets indicated with IP addresses in asset trees according to the configured asset identification policy (see section 7.9.2 Asset Identification Policy) and displays the identified assets on the asset details page (see section 8.1.6 Viewing Asset Details).

Step 1 Choose **Object > Asset Tree.**

The asset trees dispatched by ESPC are displayed on the **Asset Tree** page, as shown in Figure 6-59.

Figure 6-59 Asset tree list



Step 2 Clear asset trees.

Click **Clear** in the upper-right corner to clear all asset trees dispatched by ESPC.

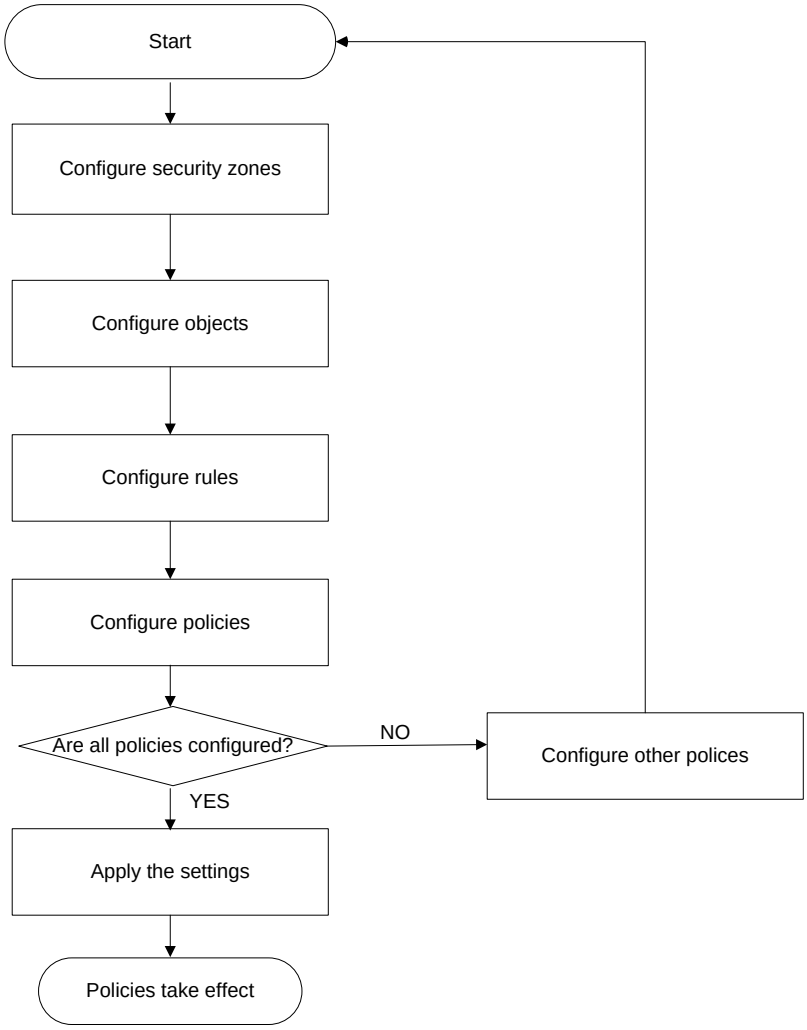
----End

7 Policies

Policies serve as a basis for NIPS to perform intrusion prevention for networks. With eight types of policies, NIPS matches the traffic passing through with rules, thereby protecting the network against various intrusion events and ensuring the intranet security.

Figure 7-1 shows the procedure for configuring policies.

Figure 7-1 Procedure for configuring policies



Caution	After configuring policies, you must apply the settings.

This chapter describes how to configure policies. It has the following sections:

Section	Description
Common Operations	Describes common operations on various policies on NIPS.
Configuring Intrusion Prevention Policies	Describes how to configure intrusion prevention policies and DoS prevention policies.
Configuring Data Leak Protection Policies	Describes how to configure data leak prevention policies.
Configuring Reputation Policies	Describes how to configure botnet prevention policies and reputation policies.
Configuring Advanced Threat Protection	Describes how to configure advanced threat protection.
Configuring URL Category Filtering Policies	Describes how to configure URL category filtering policies.
Configuring Antivirus Policies	Describes how to configure antivirus policies.
Configuring User Management Policies	Describes how to configure user management policies.
Configuring Application Management Policies	Describes how to configure application management policies.
Configuring Traffic Management Policies	Describes how to configure traffic management policies.

7.1 Common Operations

Common operations on NIPS policies include deleting, enabling/disabling, moving and duplicating. This section describes how to perform these common operations.

Moving a Policy

You can move up or down any of the following policies:

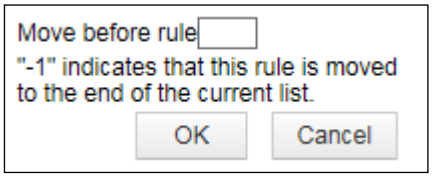
- Intrusion prevention policy
- Sensitive data protection policy
- File identification policy
- URL category policy
- Antivirus policy
- User management policy
- Application management policy
- Traffic management policy

When multiple policies are available in a policy list, NIPS matches packets with these policies according to the sequence in the list. Therefore, you need to place strict policies before loose policies, so as to improve NIPS's efficiency for processing packets.

To move an IPS policy, follow these steps:

Step 1 Click in the row of a policy.

Figure 7-2 Moving a policy



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

Step 3 Apply the setting.

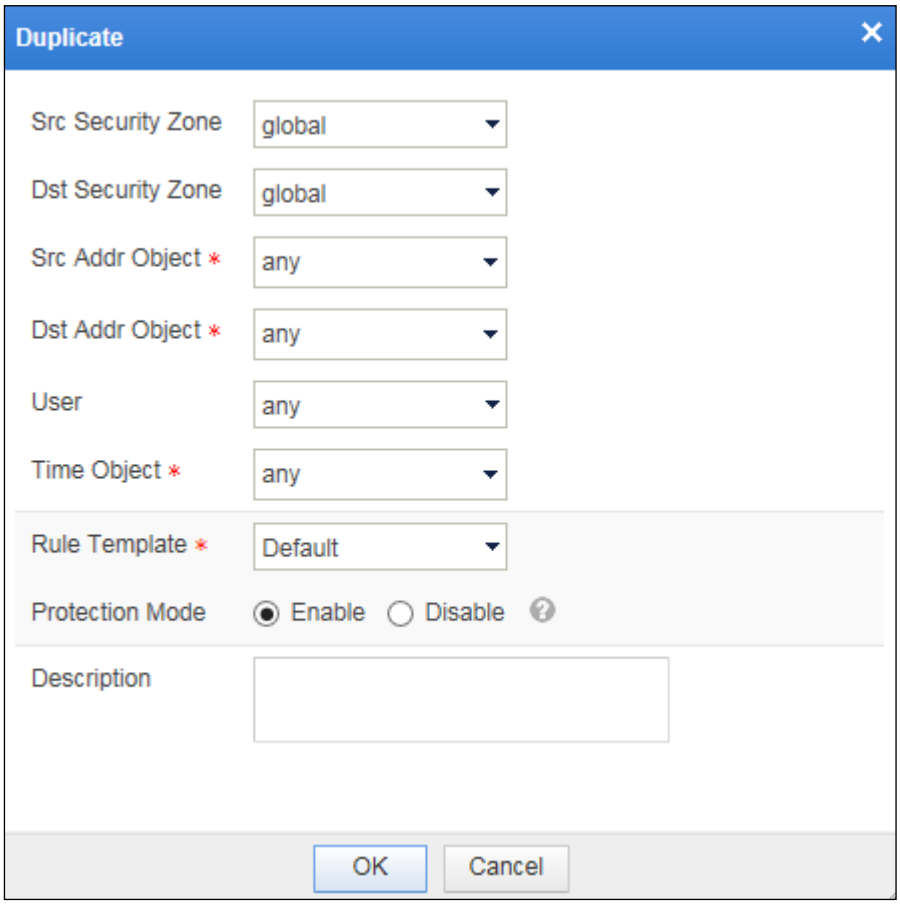
----End

Duplicating a Policy

If you want to configure a new policy which is similar to the existing one, you can duplicate the existing policy and modify it as required.

Step 1 Click in the row of a policy.

Figure 7-3 Duplicating a policy



Step 2 Modify parameters as required and click OK to save the settings.

Step 3 Apply the settings.

----End

Deleting Policies

You can delete policies one by one or in batches as follows:

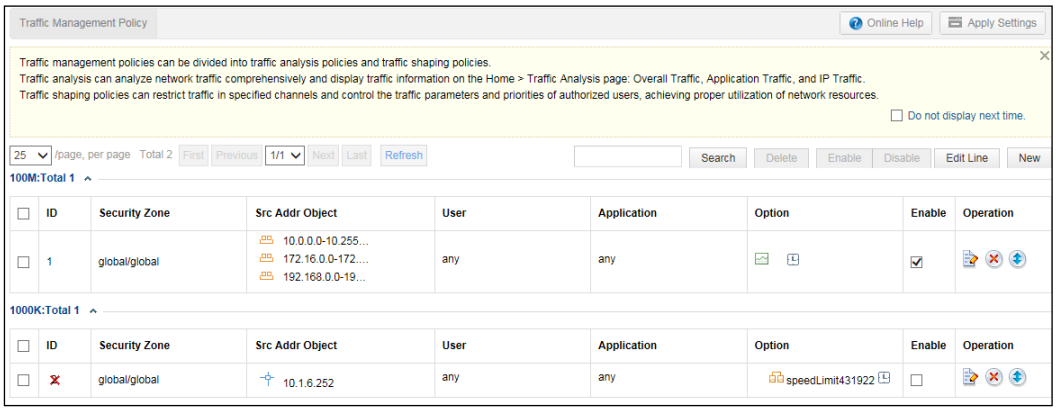
- Delete one policy.
  - Click ⊗ in the **Operation** column of a policy and then **OK** in the confirmation dialog box.
  - Select one policy, click **Delete** to the upper right of the list, and then click **OK** in the confirmation dialog box.
- Delete policies in batches.

  Select policies, click **Delete** to the upper right of the list, and then click **OK** in the confirmation dialog box.

Enabling/Disabling Policies

Only enabled policies can take effect. The **ID** column shows whether policies are enabled. A red cross ( ) on the number indicates that this policy is disabled. A policy whose number is free of this red cross is enabled. By default, a security policy is enabled after being created.

Figure 7-4 Policy list



You can enable/disable policies one by one or in batches as follows:

- Enable/Disable policies in batches.

  Select policies, click the **Enable** or **Disable** button to the upper right of the list, and then click **OK** in the confirmation dialog box.
- Enable/Disable one policy.
  - Select a policy, click the **Enable** or **Disable** button to the upper right of the list, and then click **OK** in the confirmation dialog box.
  - Select or deselect the **Enable** check box of a policy.

7.2 Configuring Intrusion Prevention Policies

This section covers the following topics:

- Intrusion Prevention Policies
- DoS Prevention Policies
- DNS Configuration

7.2.1 Intrusion Prevention Policies

Using intrusion prevention policies, NIPS can proactively defend against known and unknown attacks and block hacker attacks in real time. The hacker attacks include the following:

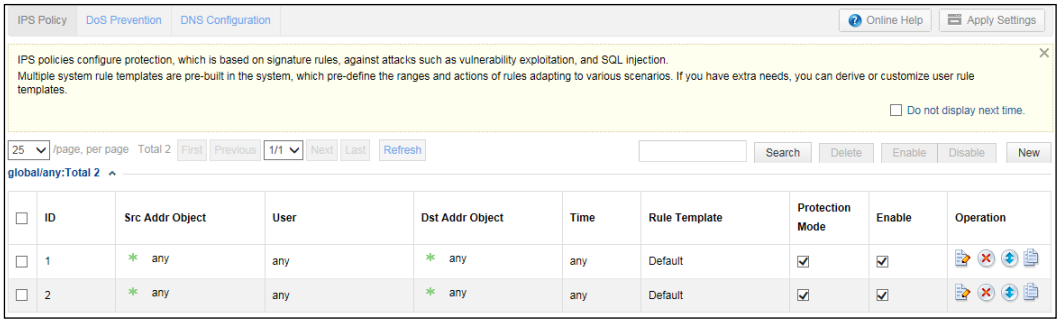
- Buffer overflow
- SQL injection
- Brute-force guessing
- DoS

- Scanning
- Unauthorized access
- Worm
- Botnet

To configure an intrusion prevention policy, follow these steps:

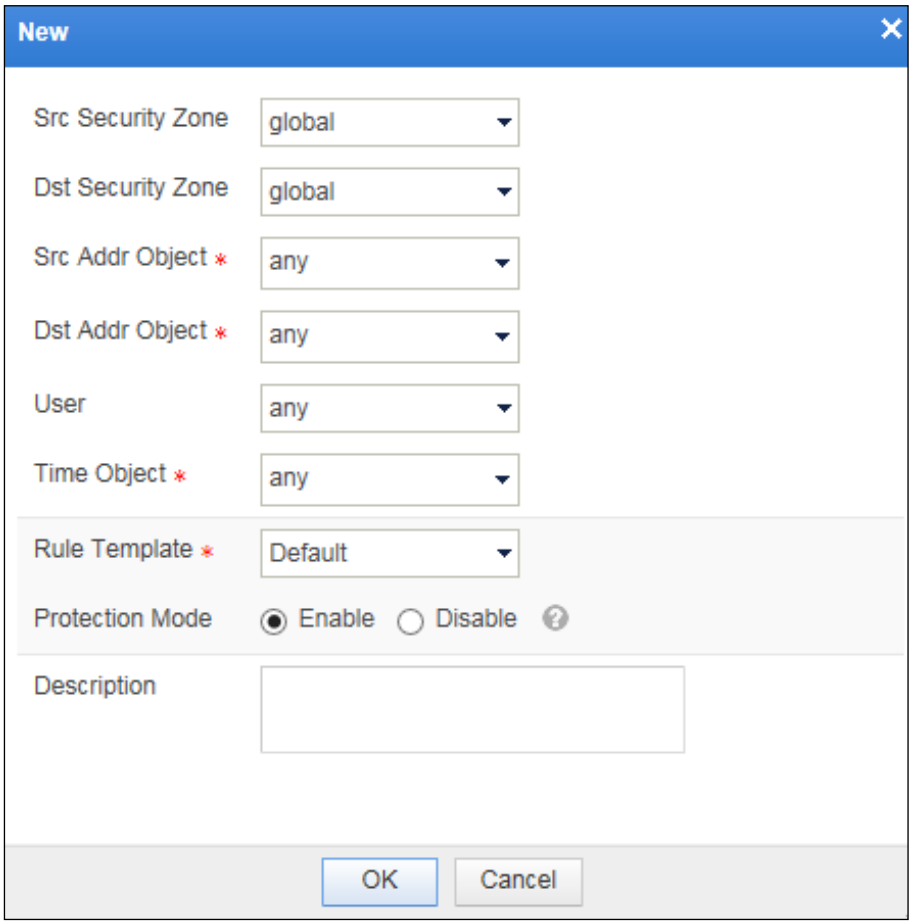
Step 1 Choose **Policy** > **IPS** > **IPS Policy**.

Figure 7-5 Intrusion prevention policy list



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

Figure 7-6 Configuring an intrusion prevention policy



Step 3 Configure parameters in the **New** dialog box.

Table 7-1 Parameters for configuring an intrusion prevention policy

Parameter	Description
Src Security Zone	Specifies a source security zone. Packets from the specified security zone will be checked against intrusion prevention policy.
Dst Security Zone	Specifies a destination security zone. Packets to the specified security zone will be checked against intrusion prevention policy. **Note** For NIPS NX5-T9010A and NX5-T9020A, the source security zone and destination security zone must be the same for an intrusion prevention policy. After you select the source security zone, the destination security zone changes automatically.
Src Addr Object	Specifies one or more source addresses to which the intrusion prevention policy will apply. **any** indicates that packets from any IP addresses will be checked against this policy.

Parameter	Description
Dst Addr Object	Specifies one or more destination addresses to which the intrusion prevention policy will apply. **any** indicates that packets to any IP addresses will be checked against this policy.
User	Specifies users to which the intrusion prevention policy will apply. Four types of users are available: • **any**: indicates any users. • **Trusted user**: indicates online users. For details about online users, see section 2.3 Online Users. • **Untrusted user**: indicates other users than online users. • **Custom user**: indicates users selected from the user list obtained from the AD domain configurator. For details about the AD domain configurator, see appendix B AD Domain Configurator Management.
Time Object	Specifies the period when the intrusion prevention policy takes effect. **any** indicates that this policy is valid at any time.
Rule Template	Specifies the rule template to be referenced by the policy. For details about rule templates, see section 6.1 Configuring Rules.
Protection Mode	Controls whether to enable the protection mode. By default, it is enabled. After the protection mode is enabled, NIPS blocks attack sessions or isolates attack IP addresses when the blocking or isolation rule in the rule template is triggered. After the protection mode is disabled, NIPS only generates alert logs.
Description	Brief description of the intrusion prevention policy.

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

Step 5 Apply the settings.

----End

7.2.2 DoS Prevention Policies

The most common DoS attacks target computers' network bandwidth or connectivity. Bandwidth attacks flood a network with such a high volume of traffic that all available network resources are consumed, leading to a denial of service. Connectivity attacks flood a computer with such a high volume of connection requests that all available operating system resources are consumed, causing the computer to stop processing legitimate user requests.

With the built-in DoS prevention module, NIPS can detect and defend against common DoS attacks. With DoS prevention policies, you can configure NIPS to protect specific network objects against the following types of attacks:

- Flood attacks
- Port scanning attacks
- Ping sweep attacks
- ARP spoof attacks
- Application-layer attacks

7.2.2.1 Flood Prevention Policies

In flood attacks, attackers initiate a large number of fake requests to the target host. The target host exhausts its resources to process these fake requests and therefore fails to process requests from authorized users, causing a denial of service. Currently, common flood attacks include the following:

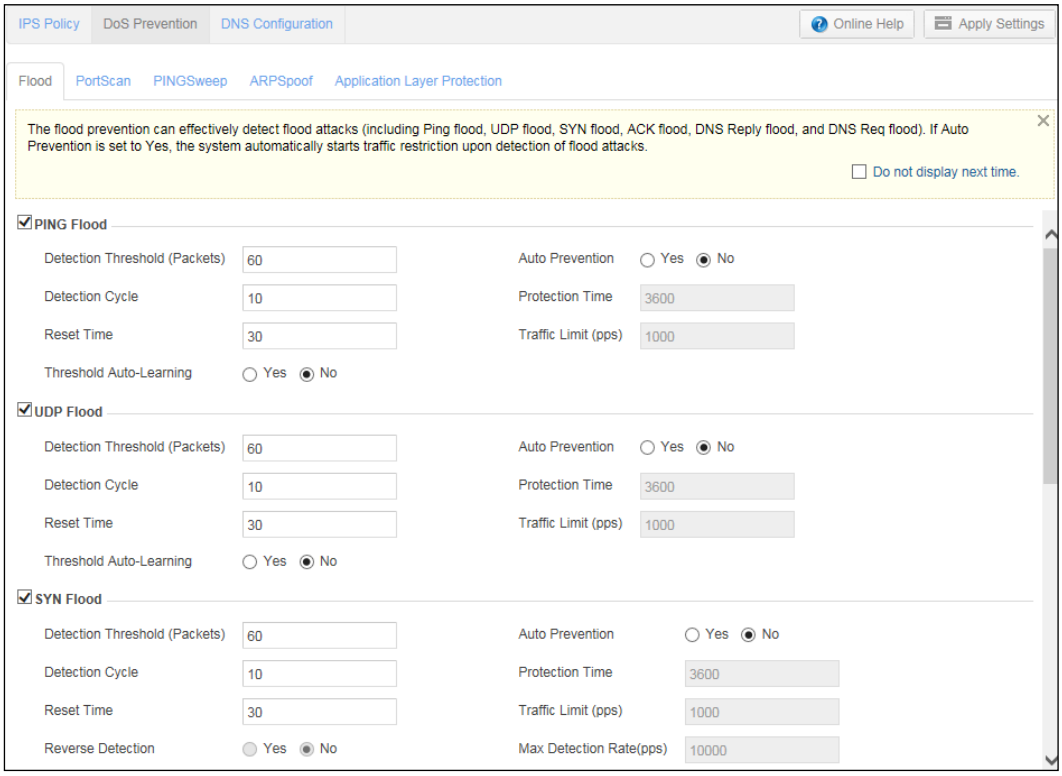
- Ping flood attacks
- UDP flood attacks
- SYN flood attacks
- DNS reply flood attacks
- ACK flood attacks
- DNS request flood attacks

With flood prevention policies, NIPS can defend against the preceding flood attacks.

To configure flood prevention policies, follow these steps:

Step 1 Choose **Policy** > **IPS** > **DoS Prevention** > **Flood**.

Figure 7-7 Flood prevention



Step 2 Select the check boxes to the left of flood attack types against which NIPS needs to defend, and set the parameters.

Table 7-2 Parameters for configuring a flood prevention policy

Parameter	Description
Detection Threshold (Packets)	Specifies the packet number threshold. When detecting that the number of packets sent to a host reaches or exceeds this threshold, NIPS considers that a flood attack occurs.
Detection Cycle	Specifies the period of time for NIPS to detect flood attacks. The interval is expressed in seconds.
Reset Time	Specifies the interval at which the system clears the detection data and starts a new round of detection. The interval is expressed in seconds.
Auto Prevention	Controls whether to enable the auto prevention mode. • If this parameter is set to **Yes**, NIPS limits traffic and generates an alert when a flood attack is detected. • If this parameter is set to **No**, NIPS only generates an alert when a flood attack is detected.
Protection Time	Specifies the traffic limit period. After the protection time expires, NIPS starts a new round of detection. The interval is expressed in seconds.
Traffic Limit (pps)	Specifies the maximum packet transmission rate allowed during the traffic limit period.
Reverse Detection	Controls whether to send reverse detection packets when a DDoS attack is detected. Reverse detection aims to check whether the source IP address is used by a real user. If so, NIPS adds this IP address to the whitelist and allows packets from this IP address to pass through.
Max Detection Rate(pps)	Specifies the maximum number of reverse detection packets to be sent per second.
Threshold Auto-Learning	Controls whether NIPS automatically learns the detection threshold during the specified detection cycle. After this function is enabled, NIPS learns the detection threshold and then automatically sets **Detection Threshold** to the learned value.

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

Step 4 Apply the settings.

----End

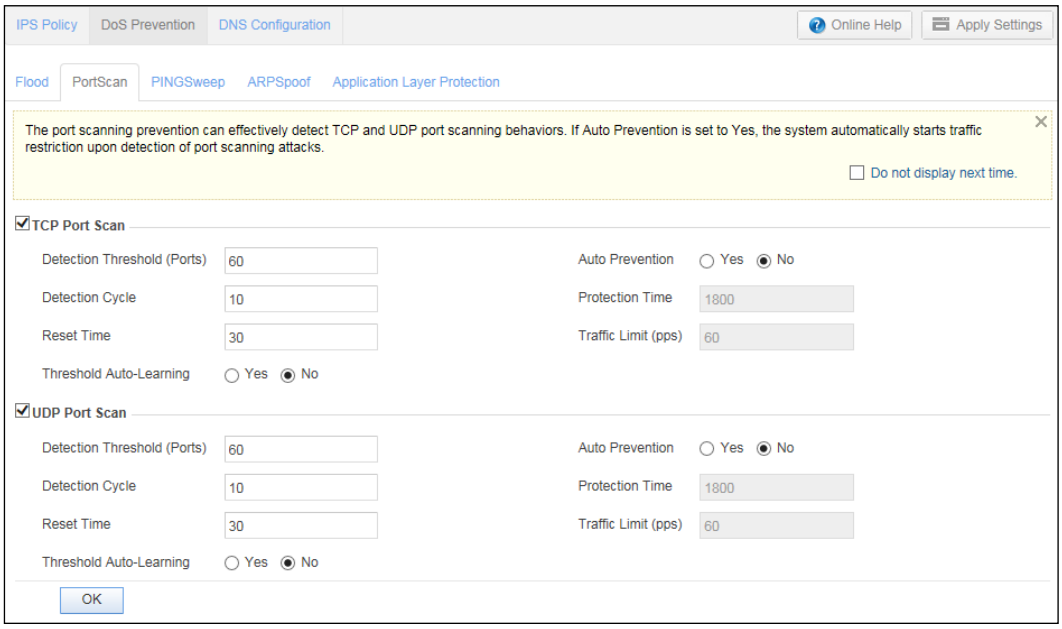
7.2.2.2 Port Scanning Prevention Policies

In port scanning attacks, the attackers scan TCP or UDP ports on the target host to identify services running on the host for further intrusion. With port scanning prevention policies, NIPS can prevent scanning of TCP or UDP ports.

To configure a port scanning prevention policy, follow these steps:

Step 1 Choose **Policy** > **IPS** > **DoS Prevention** > **PortScan**.

Figure 7-8 Port scanning prevention



Step 2 Select the check boxes to the left of port scanning attack types against which NIPS needs to defend, and set the parameters.

For the description of parameters, see Table 7-2.

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

Step 4 Apply the settings.

----End

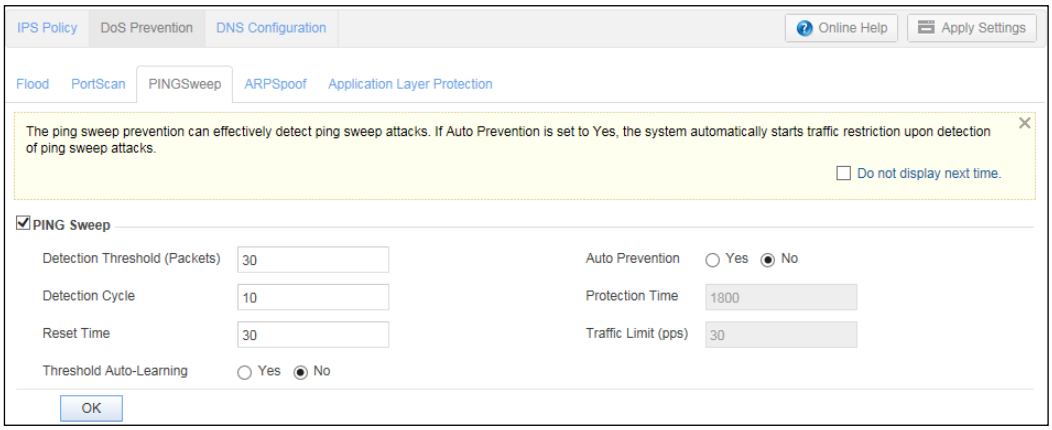
7.2.2.3 Ping Sweep Prevention Policy

Usually, an attacker, via ping sweep (ping scanning), detects active hosts on the network to learn the services and potential vulnerabilities on target hosts for further intrusion into the hosts. With the ping sweep prevention policy, NIPS can defend against ping sweep attacks.

To configure a ping sweep prevention policy, follow these steps:

Step 1 Choose **Policy** > **IPS** > **DoS Prevention** > **PINGSweep**.

Figure 7-9 Ping sweep prevention



Step 2 Select the check box to the left of **PING Sweep** and set the parameters.

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

Step 4 Apply the settings.

----End

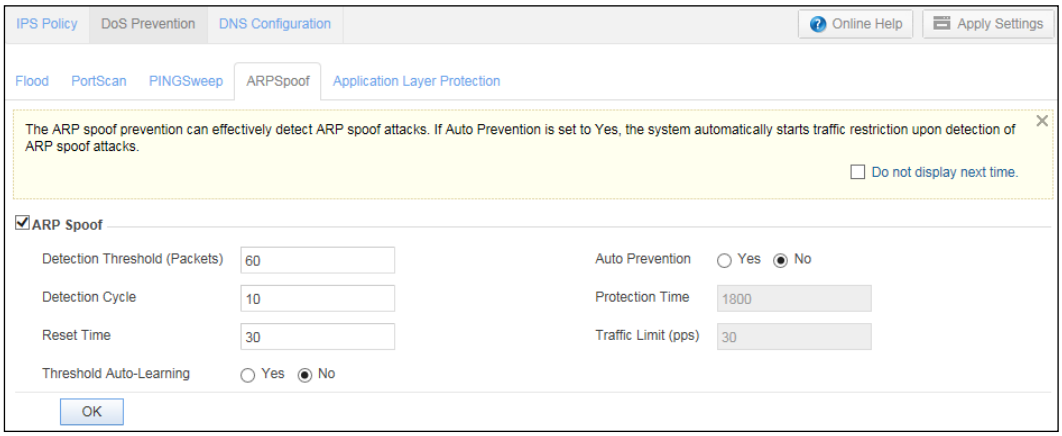
7.2.2.4 ARP Spoof Prevention Policy

In an ARP spoofing attack, the attacker implements ARP spoofing via forged IP addresses and MAC addresses. This kind of attacks causes network instability, and even network interruption. In addition, attackers can further launch man-in-the-middle attacks to steal the user names and passwords of game accounts, online bank accounts, and file access accounts. With the ARP spoof prevention policy, NIPS can defend against ARP spoofing attacks.

To configure an ARP spoof policy, follow these steps:

Step 1 Choose **Policy** > **IPS** > **DoS Prevention** > **ARPSpoof**.

Figure 7-10 ARP spoofing protection



Step 2 Select the check box to the left of **ARP Spoof** and set parameters.

For the description of parameters, see Table 7-2.

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

Step 4 Apply the settings.

----End

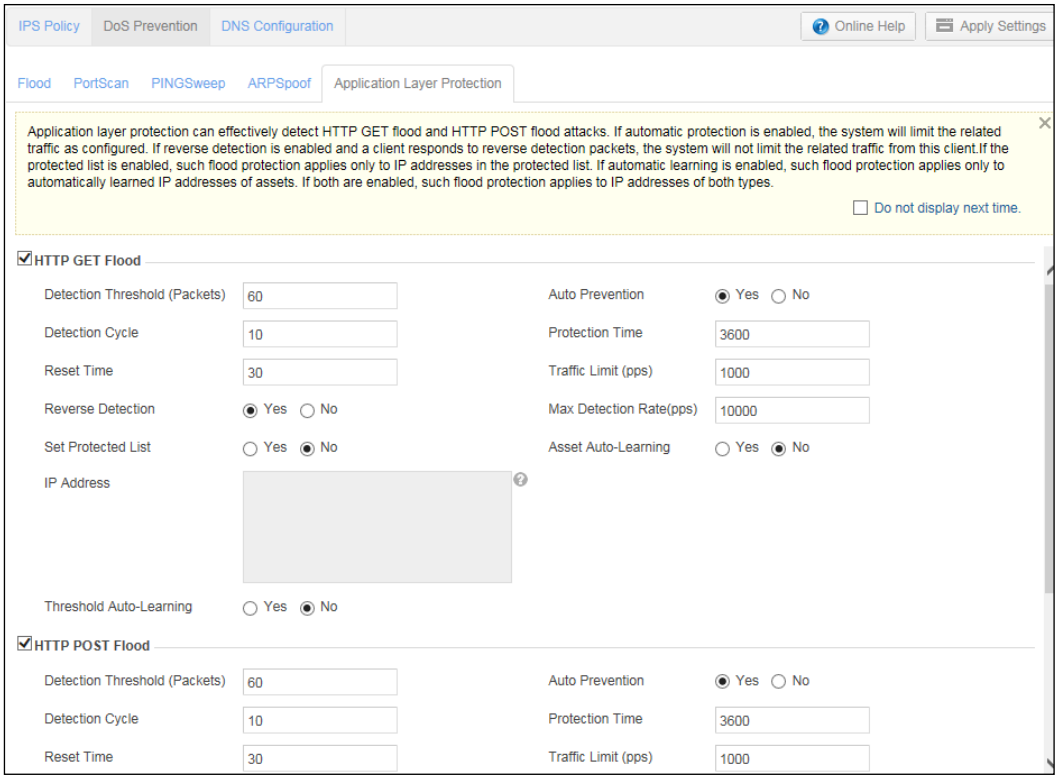
7.2.2.5 Application-Layer Protection Policy

After configuring an application-layer protection policy, NIPS can effectively detect HTTP GET flood and HTTP POST flood attacks. In addition, if automatic protection is enabled, the system will automatically limit the traffic.

To configure an application-layer protection policy, follow these steps:

Step 1 Choose **Policy** > **IPS** > **DoS Prevention** > **Application Layer Protection**.

Figure 7-11 Application-layer protection



Step 2 Select the check boxes to the left of flood attack types against which NIPS needs to defend, and set the parameters.

Most parameters have the same meanings as those for configuring protection policies on the **Flood** tab page. For the description of these parameters, see Table 7-2. Other parameters are described as follows:

- **Set Protected List**: controls whether to enable the protected list. If yes, you need to further specify IP addresses in the box below. Then NIPS will implement protection for these IP addresses.

- **Asset Auto-Learning**: controls whether to enable the automatic learning function. If yes, NIPS will implement protection for the assets automatically learned.

If you select **No** for both parameters, NIPS will check all packets for HTTP DoS attacks that pass through NIPS.

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

Step 4 Apply the settings.

----End

7.2.3 DNS Configuration

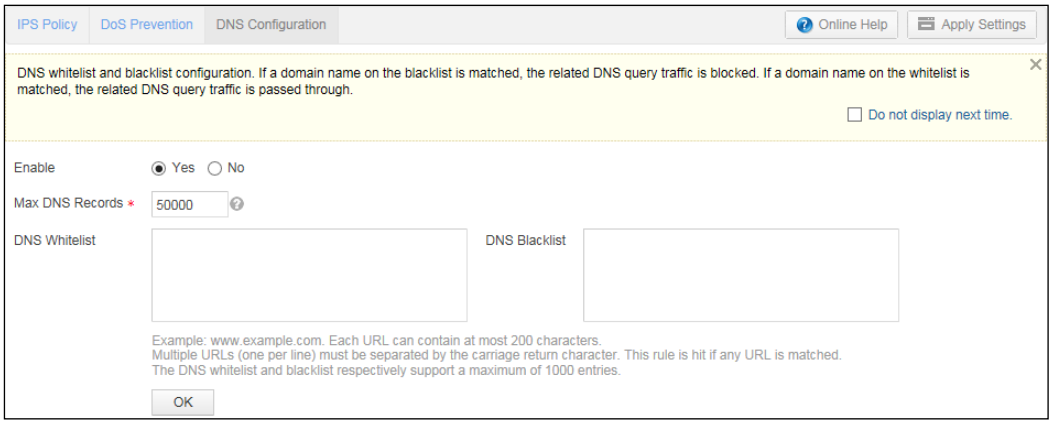
With the DNS blacklist and whitelist, NIPS can handle DNS query packets quickly.

- DNS blacklist: NIPS blocks DNS query packets matching URLs in the blacklist, without further checks.
- DNS whitelist: NIPS passes DNS query packets matching URLs in the whitelist, without further checks.

This section describes how to configure the DNS blacklist and whitelist.

Step 1 Choose **Policy** > **IPS** > **DNS Configuration** to configure the DNS whitelist and blacklist.

Figure 7-12 DNS Configuration page



Step 2 Select **Yes** for **Enable** to enable the DNS blacklist and whitelist.

Step 3 Configure parameters.

Table 7-3 Parameters for configuring the DNS blacklist and whitelist

Parameter	Description	
Max DNS Records	Specifies the number of entries included in the DNS blacklist and whitelist. The value should be an integer no greater than 50000.	
DNS Whitelist	Specifies URLs included in the DNS whitelist.	Note The URL format should be HOST, such as www.example.com.
DNS Blacklist	Specifies URLs included in the DNS	

Parameter	Description	
	blacklist.	Each URL takes one line. Multiple URLs should be separated by carriage returns. You can separately configure a maximum of 1000 entries in the DNS whitelist and blacklist.

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

Step 5 Apply the settings.

----End

7.3 Configuring Data Leak Protection Policies

The data leak protection module protects intranet security by means of:

- Sensitive Data Protection Policy
- File Identification Policy
- Server Exception Protection Policy

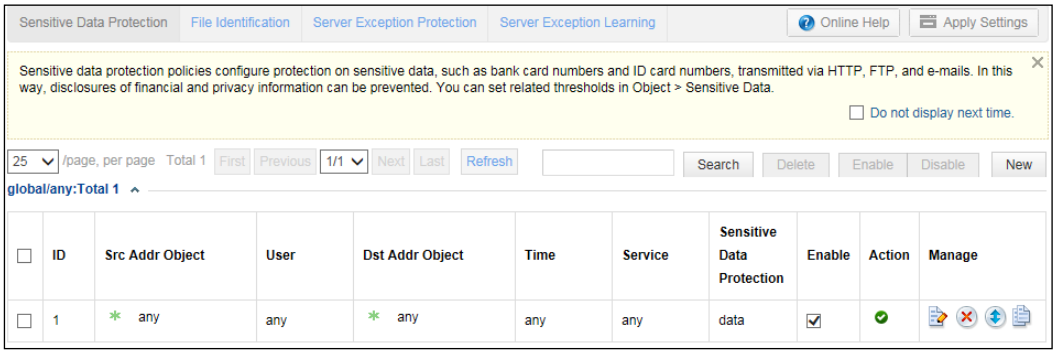
7.3.1 Sensitive Data Protection Policy

Sensitive data protection policies are used to identify data traffic in certain circumstances to prevent the leakage of internal sensitive data (such as telephone numbers, identity card numbers, and bank card numbers), thereby guaranteeing the information security on the intranet.

To configure a sensitive data protection policy, follow these steps:

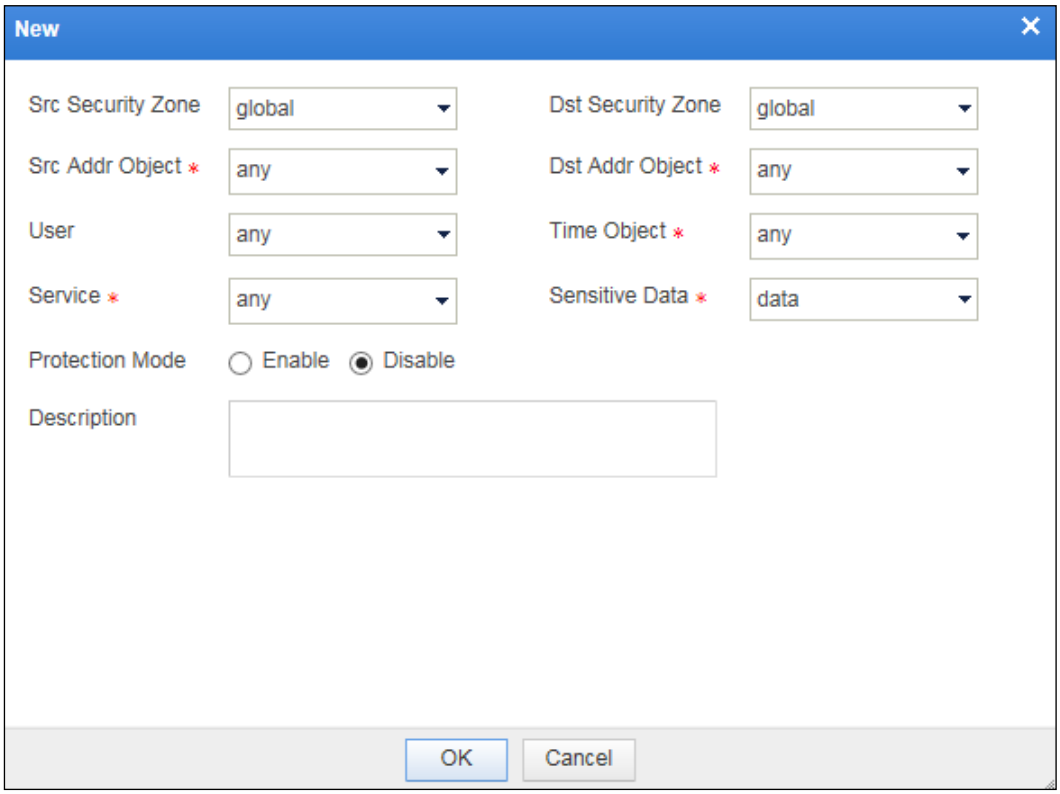
Step 1 Choose **Policy** > **Data Leak Protection** > **Sensitive Data Protection**.

Figure 7-13 Sensitive data protection policy list



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

Figure 7-14 Configuring a sensitive data protection policy



Step 3 Configure parameters in the **New** dialog box.

Table 7-4 Parameters for configuring a sensitive data protection policy

Parameter	Description
Src Security Zone	Specifies a source security zone. Packets from the specified security zone will be checked against the sensitive data protection policy. **global** indicates that packets from any security zones will be checked against this policy. **Note** For NIPS NX5-T9010A and NX5-T9020A, the source security zone and destination security zone must be the same for a sensitive data protection policy. After you select the source security zone, the destination security zone changes automatically.
Dst Security Zone	Specifies a destination security zone. Packets to the specified security zone will be checked against the sensitive data protection policy.. **global** indicates that packets to any security zones will be checked against this policy.
Src Addr Object	Specifies one or more source addresses to which the sensitive data protection policy will apply. **any** indicates that packets from any IP addresses will be checked against this policy.
Dst Addr Object	Specifies one or more destination addresses to which the sensitive data protection

Parameter	Description
	policy will apply. **any** indicates that packets to any IP addresses will be checked against this policy.
User	Specifies users to which the sensitive data protection policy will apply. Four types of users are available: • **any**: indicates any users. • **Trusted user**: indicates online users. For details about online users, see section 2.3 Online Users. • **Untrusted user**: indicates other users than online users. • **Custom user**: indicates users selected from the user list obtained from the AD domain configurator. For details about the AD domain configurator, see appendix B AD Domain Configurator Management.
Time Object	Specifies the period when this sensitive data protection policy takes effect. **any** indicates that this policy is valid at any time.
Service	Specifies services to which this policy will apply. It has such values as **any**, **HTTP**, **FTP**, and **EMAIL**. **any** indicates that this policy applies to any services.
Sensitive Data	Specifies the sensitive data to be protected by this policy.
Protection Mode	Controls whether to enable the protection mode. By default, it is disabled. After the protection mode is enabled, NIPS will block packets hitting this policy.
Description	Brief description of the sensitive data protection policy.

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

Step 5 Apply the settings.

----End

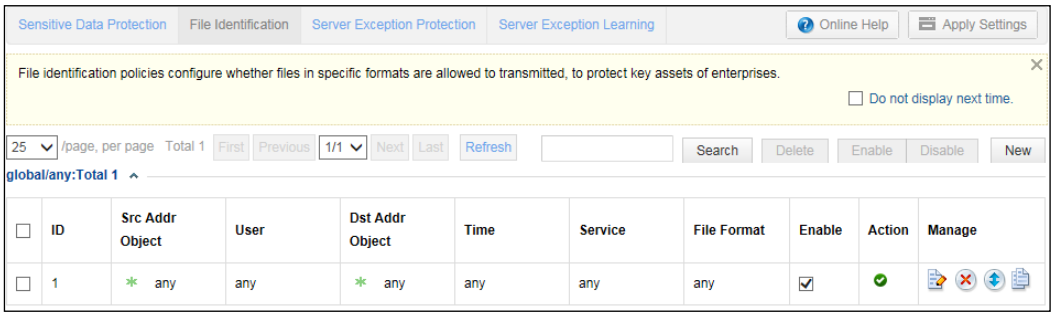
7.3.2 File Identification Policy

File identification policies are used to identify file formats of data traffic in certain circumstances, thereby guaranteeing the information security on the intranet.

To configure a file identification policy, follow these steps:

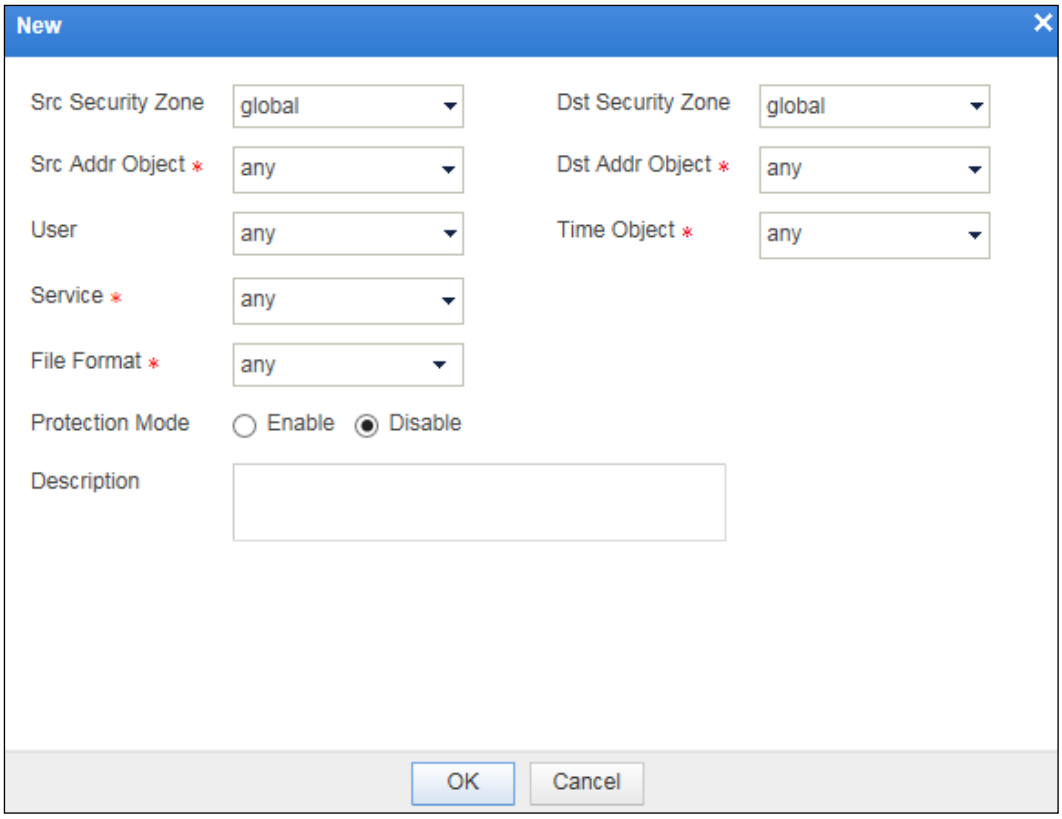
Step 1 Choose **Policy** > **Data Leak Protection** > **File Identification**.

Figure 7-15 File identification policy list



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

Figure 7-16 Configuring a file identification policy



Step 3 Configure parameters in the **New** dialog box.

Table 7-5 Parameters for configuring a file identification policy

Parameter	Description
Src Security Zone	Specifies a source security zone. Packets from the specified security zone will be checked against the file identification policy. **global** indicates that packets from any security zones will be checked against this policy.

Parameter	Description
Dst Security Zone	Specifies a destination security zone. Packets to the specified security zone will be checked against the file identification policy. **global** indicates that packets to any security zones will be checked against this policy.
Src Addr Object	Specifies one or more source addresses to which the file identification policy will apply. **any** indicates that packets from any IP addresses will be checked against this policy.
Dst Addr Object	Specifies one or more destination addresses to which the file identification policy will apply. **any** indicates that packets to any IP addresses will be checked against this policy.
User	Specifies users to which the file identification policy will apply. Four types of users are available: • **any**: indicates any users. • **Trusted user**: indicates online users. For details about online users, see section 2.3 Online Users. • **Untrusted user**: indicates other users than online users. • **Custom user**: indicates users selected from the user list obtained from the AD domain configurator. For details about the AD domain configurator, see appendix B AD Domain Configurator Management.
Time Object	Specifies the period when this policy takes effect. **any** indicates that this policy is valid at any time.
Service	Specifies services to which this policy will apply. It has such values as **any**, **HTTP**, **FTP**, and **EMAIL**. **any** indicates that this policy applies to any services.
File Format	Specifies file formats to be identified by this policy. **any** indicates that this file identification policy applies to all file formats.
Protection Mode	Controls whether to enable the protection mode. By default, it is disabled. After the protection mode is enabled, NIPS will block packets hitting this policy.
Description	Brief description of the file identification policy.

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

Step 5 Apply the settings.

----End

7.3.3 Server Exception Protection Policy

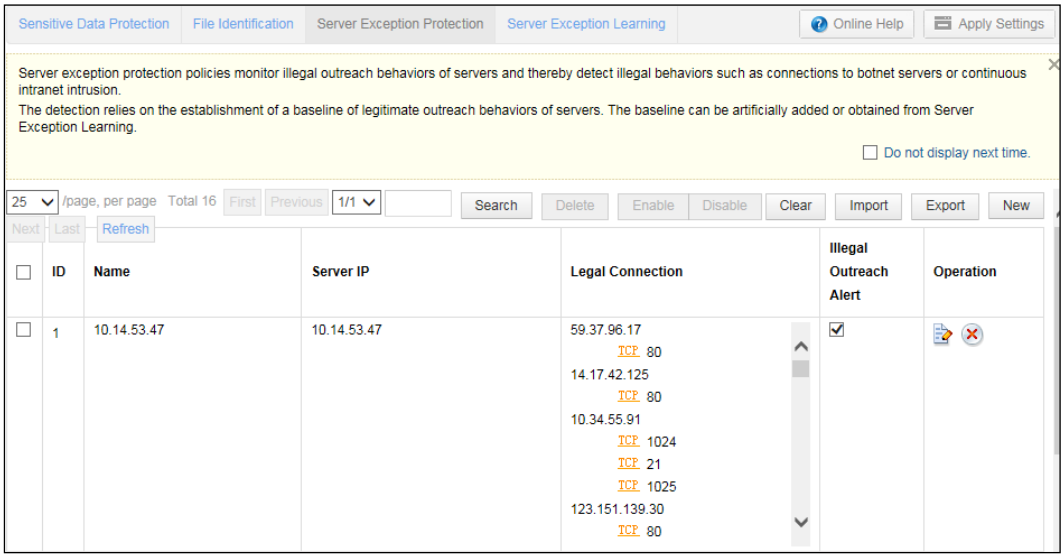
Server exception protection policies identify outreach behaviors of servers in certain circumstances. You can specify legitimate outreach behaviors by setting the allowed outreach IP address, protocol, and port. All outreach behaviors other than the defined legitimate ones are considered illegitimate, and will be handled according to the server exception protection policy. NIPS can provide protection against outreach behaviors of a maximum of 1000 servers.

You can configure a server exception policy in either of the following ways:

7.3.3.1 Common Configuration

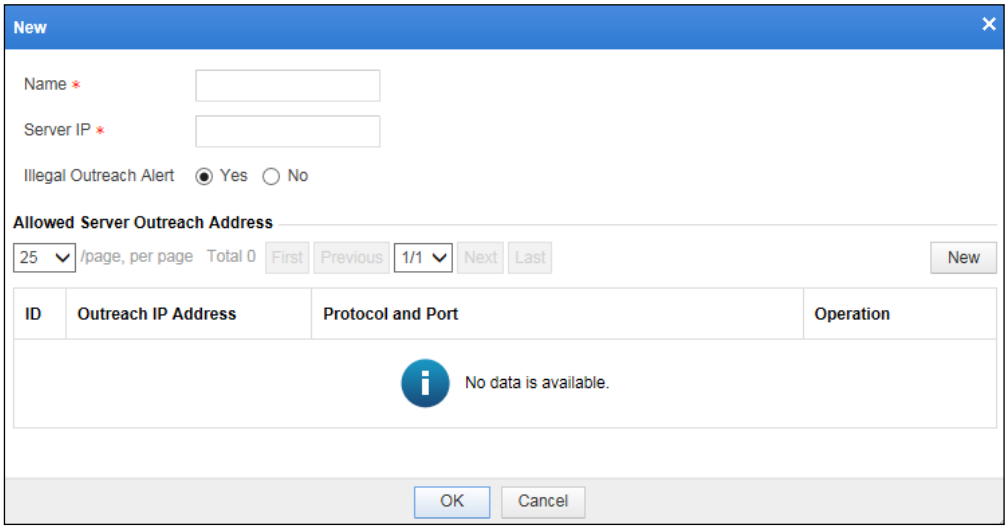
Step 1 Choose **Policy** > **Data Leak Protection** > **Server Exception Protection**.

Figure 7-17 Server exception protection policy list



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

Figure 7-18 Configuring a server exception protection policy



Step 3 Configure parameters in the **New** dialog box.

Table 7-6 Parameters for configuring a server exception protection policy

Parameter	Description
Name	Specifies the name of the server exception protection policy.
Server IP	Specifies the IP address of the server protected by the policy.
Illegal Outreach Alert	Control whether to report an alert when illegitimate outreach behaviors are detected.
Allowed Server Outreach Address	Defines legitimate server outreach behaviors. Click **New**, define the allowed IP address, protocol, and port, and click **OK** to commit the settings.

Figure 7-19 Defining legitimate server outreach behaviors

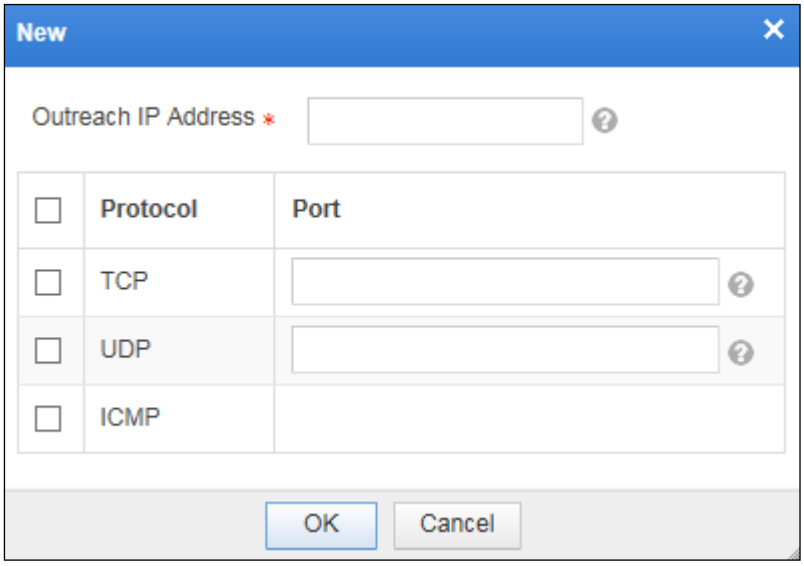


Table 7-7 Parameters for defining legitimate server outreach behaviors

Parameter	Description
Outreach IP Address	Specifies an IP address to which the server is allowed to connect.
TCP/Port	Specifies the TCP port which the specified IP address opens to the server.
UDP/Port	Specifies the UDP port which the specified IP address opens to the server.
ICMP	Controls whether the specified IP address provides the ICMP service to the server.

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

Step 5 Apply the settings.

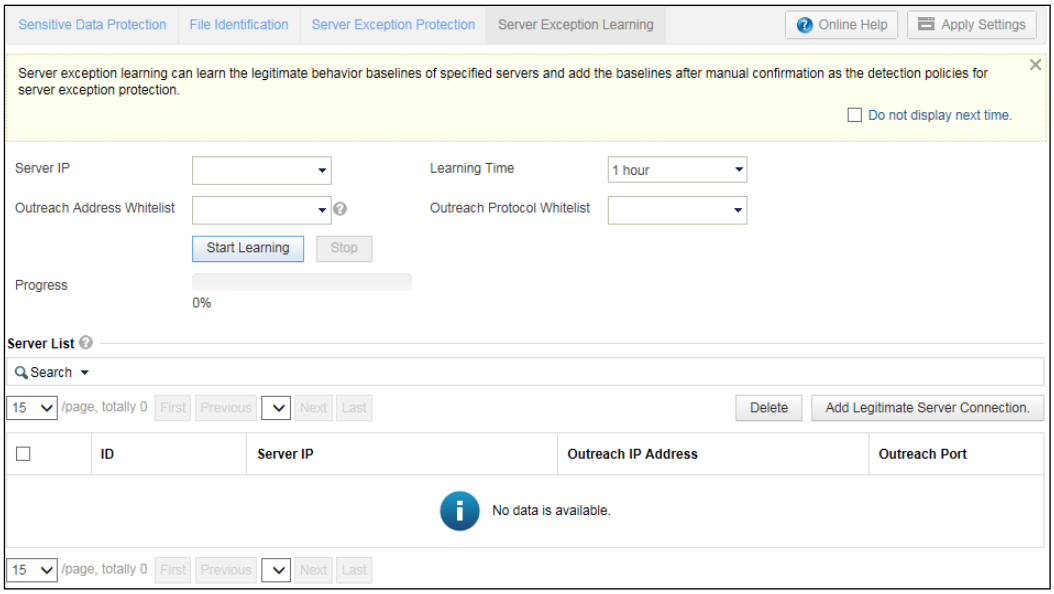
----End

7.3.3.2 Quick Configuration

Based on the outreach information learned by NIPS, you can quickly configure server exception protection policies.

Step 1 Choose **Policy** > **Data Leak Protection** > **Server Exception Learning**.

Figure 7-20 Server exception learning



Step 2 Quickly configure a server exception protection policy.

a. Select one or more server outreach behaviors from the server list.

b. Click **Add Legitimate Server Connection**, and set **Server IP**, **Outreach IP Address**, and **Outreach Port** for legitimate server connections.

Step 3 View the newly configured server exception protection policies on the **Server Exception Protection** page, as shown in Figure 7-17.

----End

7.3.4 Server Exception Learning

After server exception learning is configured, NIPS captures outreach data from specified servers and learns the port and service information from the unsolicited outreach data. NIPS identifies all network behaviors of servers by means of auto-learning. You can identify illegitimate outreach behaviors according to learning results.

To configure server exception learning, follow these steps:

Step 1 Choose **Policy** > **Data Leak Protection** > **Server Exception Learning**.

Step 2 Configure parameters.

Table 7-8 Parameters for configuring server exception learning

Parameter	Description
Server IP	Specifies the IP address of a server on which NIPS will perform auto-learning. You can select server IP addresses from the drop-down list, which is configured under **Object** > **Network**. Alternatively, you can click **New** to configure a network object. For details about network objects, see section 6.2 Configuring Network Objects.
Learning Time	Specifies the period when NIPS learns the servers' unsolicited outreach behavior data. It has such values as **1 hour**, **12 hours**, **1 day**, and **1 week.**
Outreach Address Whitelist	Specifies the outreach IP address whitelist. NIPS does not perform server exception learning for packets exchanged between the server and IP addresses included in the whitelist. Note **Outreach Address Whitelist** and **Outreach Protocol Whitelist** form an AND relationship. That is to say, only packets that meet both conditions are exempt from server exception learning.
Outreach Protocol Whitelist	Specifies the outreach protocol whitelist. NIPS does not perform server exception auto-learning for packets exchanged between the server and outreach IP addresses by using protocols included in the whitelist. Note **Outreach Address Whitelist** and **Outreach Protocol Whitelist** form an AND relationship. That is to say, only packets that meet both conditions are exempt from server exception learning.

Step 3 Click **Start Learning**.

You can view the progress through the progress bar and the percentage.

Step 4 (Optional) Click **Stop** to suspend the learning.

----End

7.4 Configuring Reputation Policies

NIPS's reputation protection involves the reputation library source, botnet prevention, and protection for web reputation and file reputation.

Note

- To make sure that the reputation protection function works properly, NIPS must properly connect to the reputation cloud. Otherwise, NIPS must connect to ESPC.
- NIPS devices of the NX3-N300A model does not support file disassembly and file reputation detection functions. Therefore, the file reputation configuration area is absent on the web-based manager of NIPS on such a platform.

7.4.1 Reputation Library Source

NIPS checks reputation based on the reputation library to protect against botnets, malicious websites, and dangerous files in real time.

You can select a reputation library source according to the particular network conditions:

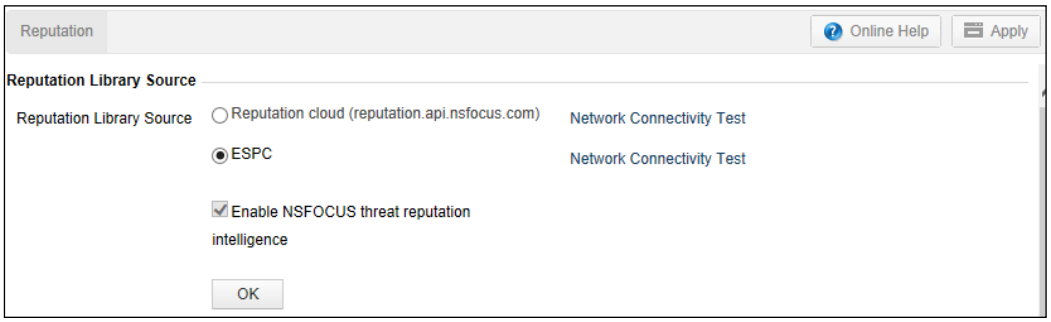
- When NIPS cannot access the extranet: Select **ESPC** to enable NIPS to collaborate with ESPC on the intranet. In this case, ESPC can obtain the reputation library by collaborating with the reputation cloud on the extranet or with TAC. Then ESPC dispatches the obtained reputation library to NIPS regularly. NIPS can also check ESPC for the latest reputation library for real-time protection against botnets, malicious websites, and dangerous files.
- When NIPS can access the extranet: Select **Reputation cloud** to enable NIPS to collaborate with NSFOCUS reputation cloud. In this case, the reputation cloud dispatches the reputation library regularly to NIPS. NIPS can also check the reputation cloud for the latest reputation library for real-time protection against botnets, malicious websites, and dangerous files.

Note	The Reputation module can work properly and NSFOCUS threat intelligence is available (for proper use of the reputation library obtained from the reputation cloud or ESPC) only when the license covers Reputation Library. For how to view the license, see section 4.7.1 Viewing License Status.

To configure the reputation library source, follow these steps:

Step 1 Choose **Policy** > **Reputation**.

Figure 7-21 Reputation library source



Step 2 Select a reputation library source, which can be **Reputation cloud** or **ESPC**.

Enable NSFOCUS threat reputation intelligence cannot be configured. The check box is selected by default if the license covers Reputation Library. The default reputation library source is **Reputation cloud**.

After the reputation library source is selected, you can click **Network Connectivity Test** to check whether NIPS can properly connect to the reputation library. The system will prompt whether the connection is properly established.

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

Step 4 Apply the settings.

----End

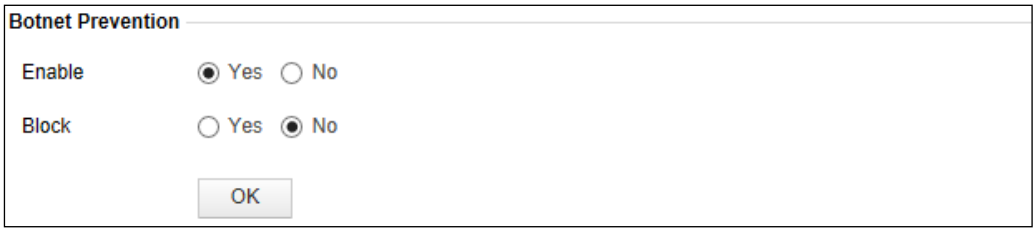
7.4.2 Botnet Prevention

A botnet is to intrude the host and plant zombie programs. It spreads by means of remote attacks, weak password scanning, email attachments, and malicious files. Embedding a trojan into web pages is the main spreading method.

With a built-in advanced botnet detection engine and real-time botnet cloud rules, NIPS provides all-round protection against botnets. The all-round protection means that zombie programs cannot be planted into networks. In the case when a host is infected, the zombie program cannot be exploited to launch attacks and disclose data.

Step 1 Choose **Policy** > **Reputation**.

Figure 7-22 Botnet Prevention area



Step 2 Select **Yes** or **No** to enable or disable botnet detection.

Step 3 Select **Yes** or **No** to block or allow botnet connections.

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

Step 5 Apply the settings.

----End

7.4.3 Web Reputation

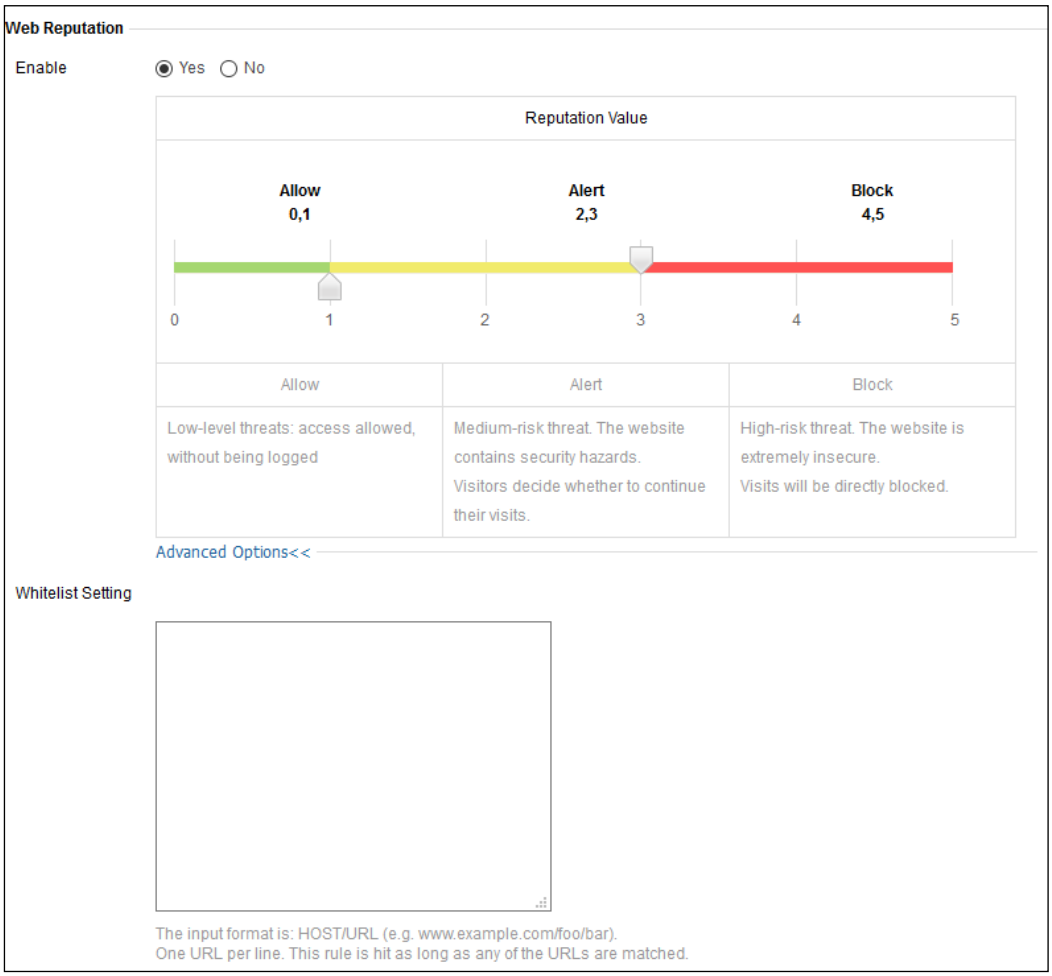
In addition to the built-in malicious website library, NIPS also allows you to flexibly set reputation values based on the malicious website library to realize website filtering. On an intranet protected by NIPS, when the access to the Trojan-infected website occurs, NIPS will take measures in real time to effectively defend enterprise intranets against web security threats, prevent privacy invasion, and protect enterprises' confidential information. The measures include the following:

- Alert
- Block
- Alert and block

To configure web reputation, follow these steps:

Step 1 Choose **Policy** > **Reputation**.

Figure 7-23 Web Reputation area



Step 2 Click **Yes** to enable web reputation.

Step 3 Configure the web reputation policy.

a. Move the upper cursor to set the reputation value for websites to be alerted or blocked.

b. Move the lower cursor to set reputation values for websites to which visits are allowed.

Table 7-9 Reputation values of a web reputation policy example

Reputation Value	Description
0	Indicates that the website poses low-risk threats. Visits to the website are allowed, without logs generated.
1	
2	Indicates that the website poses medium-risk threats. Visits to the website are allowed and reputation logs are recorded, with **Action** being **Allow** and **Event Type** being **Visit Malicious Site**. Alerts are displayed under **Alert Center** > **Reputation Event**.
3	
4	Indicates that the website poses high-risk threats. Visits to the website are blocked

Reputation Value	Description
5	and reputation logs are recorded, with **Action** being **Block** and **Event Type** being **Visit Malicious Site**. Alerts are displayed under **Alert Center** > **Reputation Event**.

You can set a web reputation policy by reference to reputation values of websites.

Table 7-10 Reputation values of a website

Reputation Value	Description
0	Indicates that a website has only a few adverse records, for example, a small number of low-risk behaviors.
1	Indicates that a website has a small number of adverse records, for example, frequent low-risk behaviors.
2	Indicates that a website has adverse records at an average level, for example, a small number of medium-risk behaviors or a great number of low-risk behaviors.
3	Indicates that a website has adverse records at a medium level, for example, frequent medium-risk behaviors.
4	Indicates that a website has serious adverse records, for example, a small number of high-risk behaviors or a great number of medium-risk behaviors.
5	Indicates that a website has extremely serious adverse records, for example, frequent high-risk behaviors.

Step 4 Click **Advanced Options** to set the website whitelist.

Step 5 In the dialog box that prompts engine restart, click **OK** to save the settings.

Step 6 Apply the settings.

----End

7.4.4 File Reputation

NIPS obtains the file reputation value by calculating the MD5 value of the reassembled file and mapping the MD5 value to reputation values stored in the reputation library. Then NIPS generates an alert or blocks the file as configured, thereby effectively preventing the transmission of suspicious files on the intranet and protecting the network security.

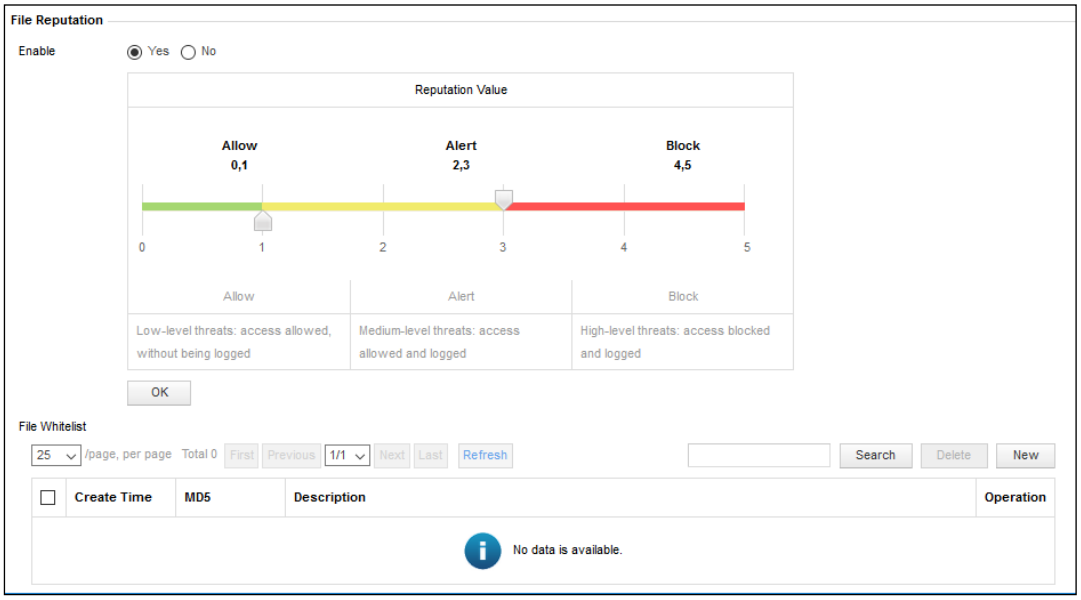
Note	• NIPS only compares the MD5 value with the hash value of the external restored file, but not the internal of decompressed files or packet files. • The file reputation function is available only after file reassembly is enabled. For how to enable file assembly, see section 4.3.3 Configuring NetFlow.

This section describes how to configure the file reputation policy and file whitelist that is a list of MD5 values of files.

Configuring the File Reputation Detection Policy

Step 1 Choose **Policy** > **Reputation**.

Figure 7-24 File Reputation area



Step 2 Click **Yes** to enable file reputation.

Step 3 Configure the file reputation policy.

a. Move the upper cursor to set the reputation value for files to be alerted or blocked.

b. Move the lower cursor to set the reputation value for allowed files.

Table 7-11 Reputation values of a file reputation policy example

Reputation Value	Description
0	Low-level suspicious. Visits are allowed but not logged.
1	
2	
3	Medium-level suspicious. Visits are allowed and reputation logs are recorded, with **Action** being **Allow** and **Event Type** being **Visit Dangerous File**. Alerts are displayed under **Alert Center** > **Reputation Event**.
4	High-level suspicious. Visits are disallowed and reputation logs are recorded, with **Action** being **Block** and **Event Type** being **Visit Dangerous File**. Alerts are displayed under **Alert Center** > **Reputation Event**.
5	

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

Step 5 Apply the settings.

----End

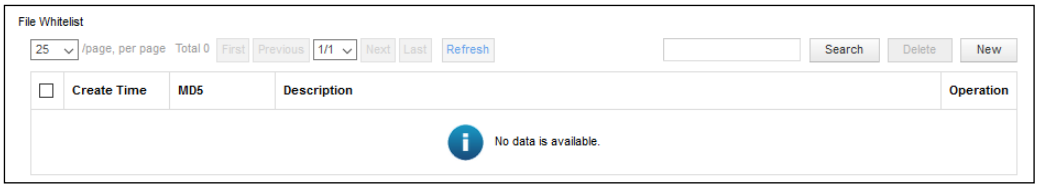
Configuring the File Whitelist

The file whitelist contains MD5 values of files for which reputation detection is unnecessary.

Step 1 Choose **Policy** > **Reputation**.

Figure 7-25 shows the file whitelist area.

Figure 7-25 File whitelist

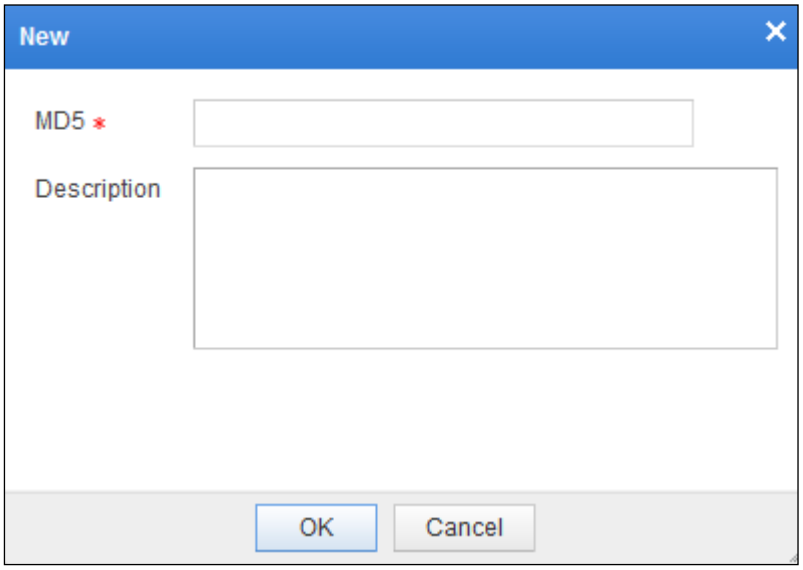


You can click  or  in the **Operation** column to edit or delete a whitelist entry.

Also, you can select multiple entries and click **Delete** to delete them.

Step 2 Click **New** to add a new whitelist entry.

Figure 7-26 Adding a file whitelist entry



Step 3 Type an MD5 value and its descriptive information.

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

Step 5 Apply the settings.

----End

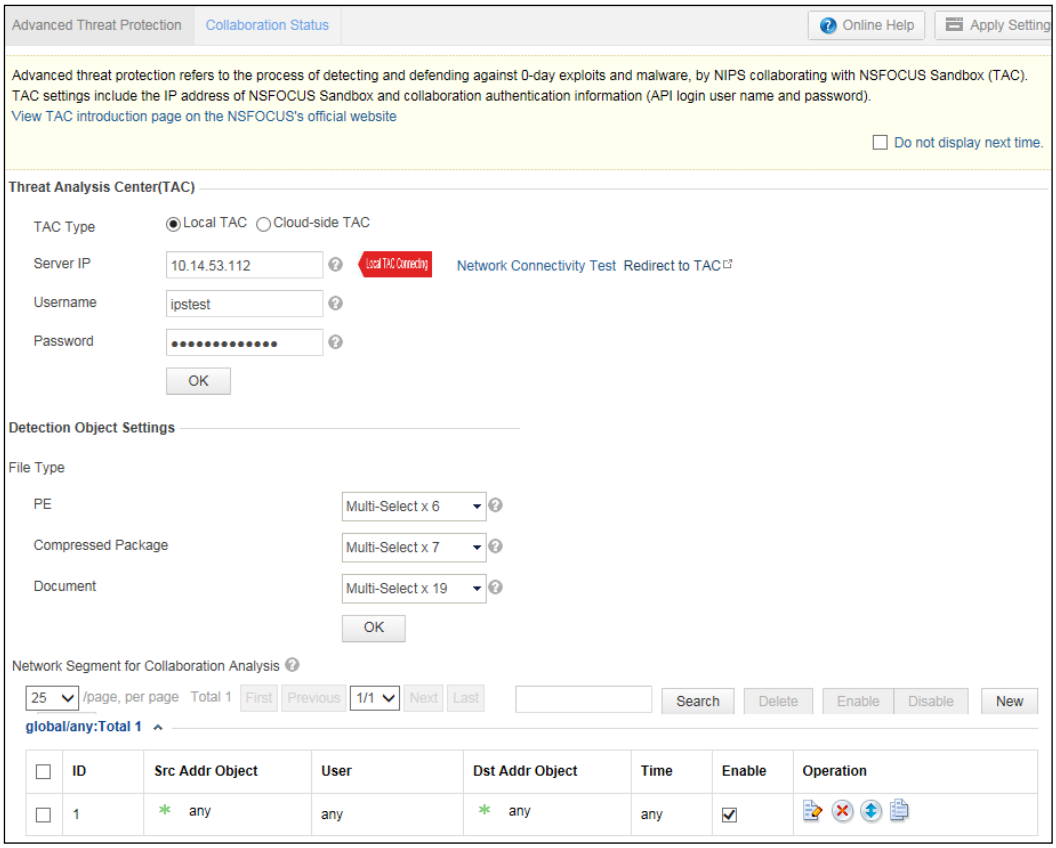
7.5 Configuring Advanced Threat Protection Policies

The advanced threat protection module involves parameter configuration for collaboration with NSFOCUS TAC and collaboration analysis results.

7.5.1 Advanced Threat Protection

Step 1 Choose **Policy** > **Advanced Threat Protection** > **Advanced Threat Protection**.

Figure 7-27 Advanced threat protection



Step 2 Configure parameters for collaboration between NIPS and TAC.

- Parameters for collaboration with TAC:
  - **Local TAC**: specifies **Server IP** (IP address of local TAC) and **Username** and **Password** for collaboration authentication.
- Cloud-side TAC: specifies the IP address of the cloud-side TAC.
- **Detection objects**: specifies the types to files to be sent to TAC for detection. Only files of the specified types will be sent to TAC for detection.
- Packet filtering rules: specifies packet filtering rules. Only packets that match one of enabled rules will be sent to TAC for detection.

Note	If no packet filtering rule is set, the collaboration function is disabled.

----End

The following sections describe how to configure parameters for collaboration.

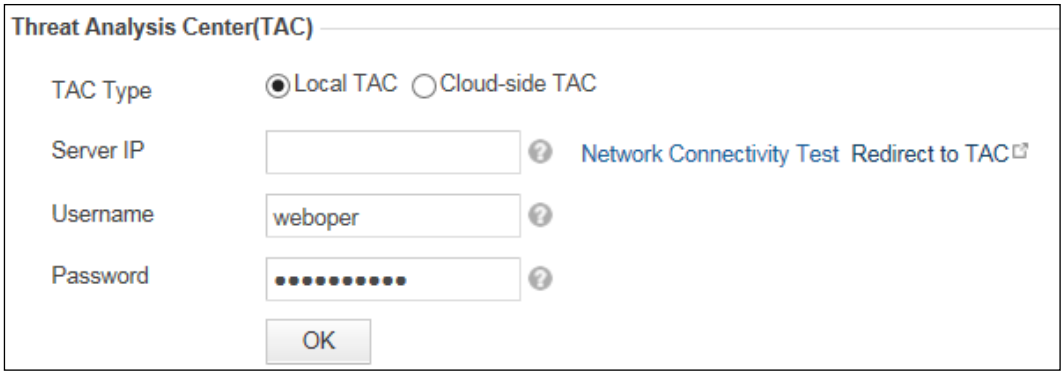
7.5.1.1 Configuring Parameters for Collaboration with TAC

NIPS can collaborate with local TAC and cloud-side TAC.

Configuration Parameters for Collaboration with Local TAC

Step 1 In the **Threat Analysis Center(TAC)** area, select **Local TAC** for **TAC Type**.

Figure 7-28 Configuring parameters for collaboration with local TAC



Step 2 Configure parameters for collaboration with local TAC.

Table 7-12 Parameters for collaboration with TAC

Parameter	Description
Server IP	IP address of TAC.
User Name	Account of the API for collaboration with TAC.
Password	Password of the API for collaboration with TAC.

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

Step 4 Test the connection between NIPS and TAC.

After configuring collaboration parameters, you can click **Network Connectivity Test** to check whether NIPS can properly connect to TAC. If the connection succeeds, 

is displayed to the right of the **Server IP** text box.

You can click **Redirect to TAC** to the right of the **Password** text box to log in to TAC.

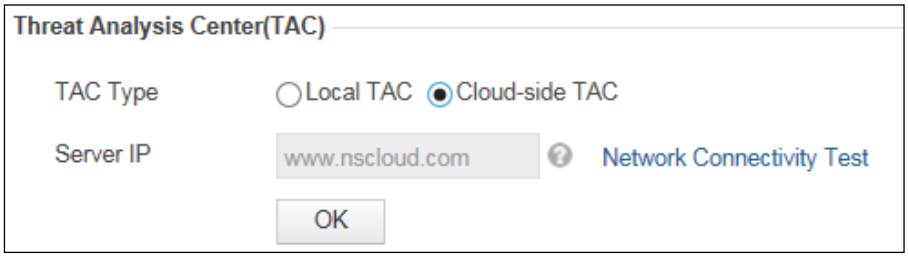
Step 5 Apply the settings.

----End

Configuring Parameters for Collaboration with Cloud-side TAC

Step 1 In the **Threat Analysis Center(TAC)** area, select **Cloud-side TAC** for **TAC Type**.

Figure 7-29 Configuring parameters for collaboration with cloud-side TAC



Step 2 Set the IP address of the cloud-side TAC server, which is www.nscloud.com by default. Then click **Network Connectivity Test** to check whether NIPS can properly connect to the cloud-side TAC.

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

Step 4 Apply the settings.

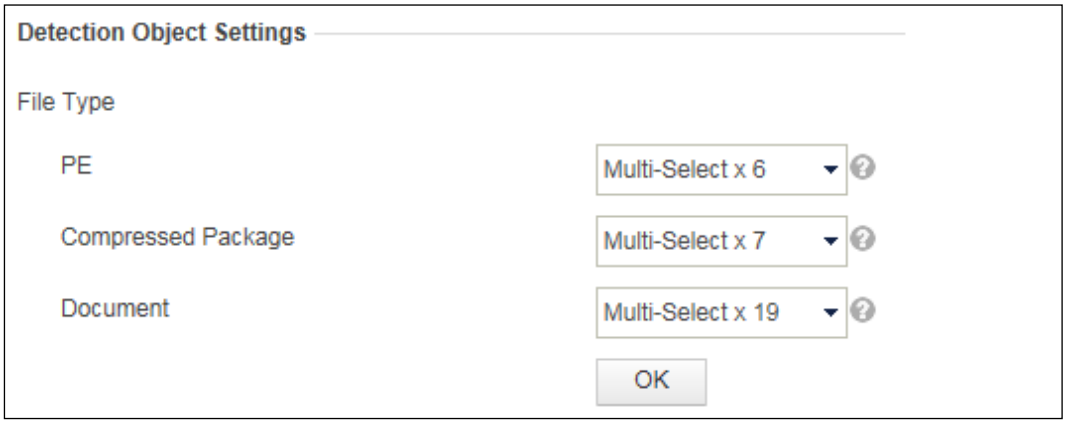
----End

7.5.1.2 Configuring Detection Objects

In the **Detection Object Configuration** area, set the types of files sent to TAC for detection.

Step 1 Open the **Advanced Threat Protection** page.

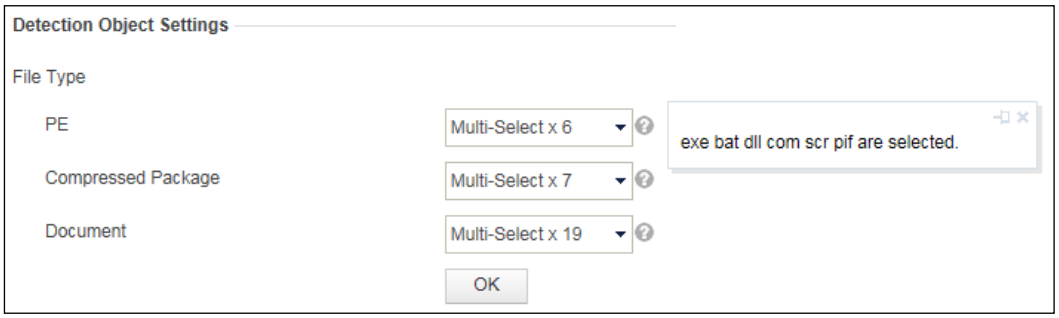
Figure 7-30 Configuring detection objects



Step 2 Set file types: **PE**, **Compressed Package**, and **Document**.

Pointing to to the right of each text box, you can see the selected file types.

Figure 7-31 Checking the selected file types



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

Step 4 Apply the settings.

----End

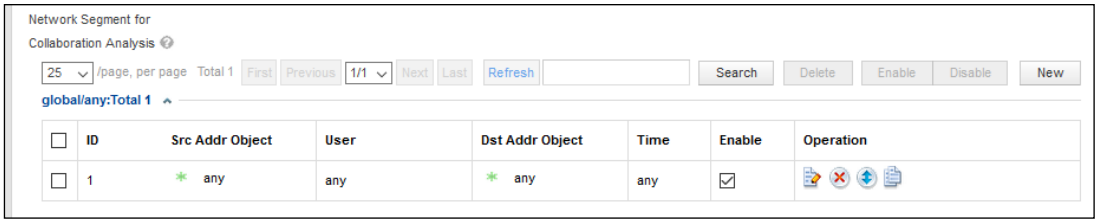
7.5.1.3 Configuring a Network Segment for Collaborative Analysis

In the **Network Segment for Collaboration Analysis** area, you can configure parameters to make NIPS forward only certain files to TAC for detection. If no rule is set here, the collaboration is disabled automatically.

Step 1 Open the **Advanced Threat Protection** page.

Figure 7-32 shows the **Network Segment for Collaboration Analysis** area.

Figure 7-32 Packet filtering rules for collaboration with TAC



You can search for, enable, disable, edit, move, or delete packet filtering rules. For details, see section 7.1 Common Operations. To add a network segment for collaboration analysis, follow these steps:

Step 1 Click **New** to create a packet filtering rule.

Figure 7-33 Creating a packet filtering rule

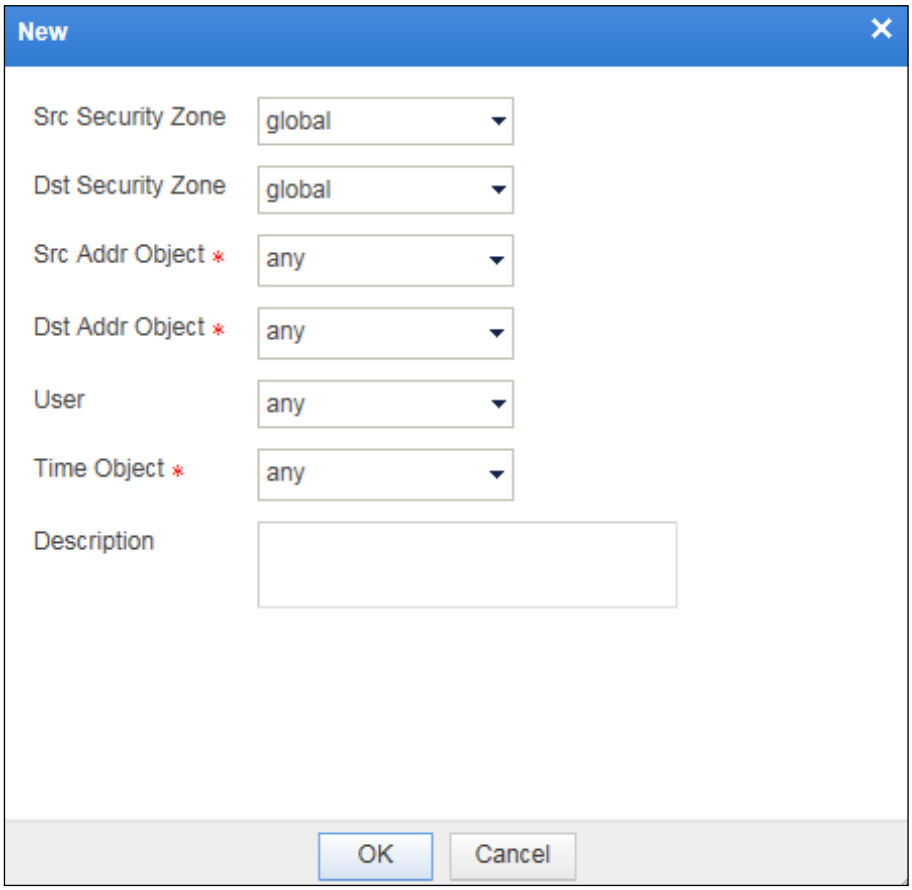


Table 7-13 describes parameters for creating a packet filtering rule.

Table 7-13 Parameters of a packet filtering rule

Parameter	Description
Src Security Zone	Specifies a source security zone. Packets from the specified security zone will be checked against the packet filtering rule. **global** indicates that packets from any security zones will be sent to TAC to check against the packet filtering rule.
Dst Security Zone	Specifies a destination security zone. Packets to the specified security zone will be checked against the packet filtering rule. **global** indicates that packets to any security zones will be sent to TAC to check against the packet filtering rule. **Note** For NIPS NX5-T9010A and NX5-T9020A, the source security zone and destination security zone must be the same for the packet filtering rule. After you specify a source security zone, the destination security zone changes automatically.
Src Addr Object	Specifies a source address object. Packets from IP addresses of the specified source address object match the packet filtering rule.

Parameter	Description
	any indicates that packets from any IP addresses will be sent to TAC for detection.
Dst Addr Object	Specifies a destination address object. Packets to IP addresses of the specified source address object match the packet filtering rule. **any** indicates that packets destined for any IP addresses will be sent to TAC for detection.
User	Specifies users that match the packet filtering rule. Four types of users are available: • **any**: indicates any users. • **Trusted user**: indicates online users. For details about online users, see section 2.3 Online Users. • **Untrusted user**: indicates other users than online users. • **Custom user**: indicates users selected from the user list obtained from the AD domain configurator. For details about the AD domain configurator, see appendix B AD Domain Configurator Management.
Time Object	Specifies the time that matches the packet filtering rule. **any** indicates that packets arriving at NIPS at any time will be sent to TAC for detection.
Description	Brief description of packets sent to TAC for detection.

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

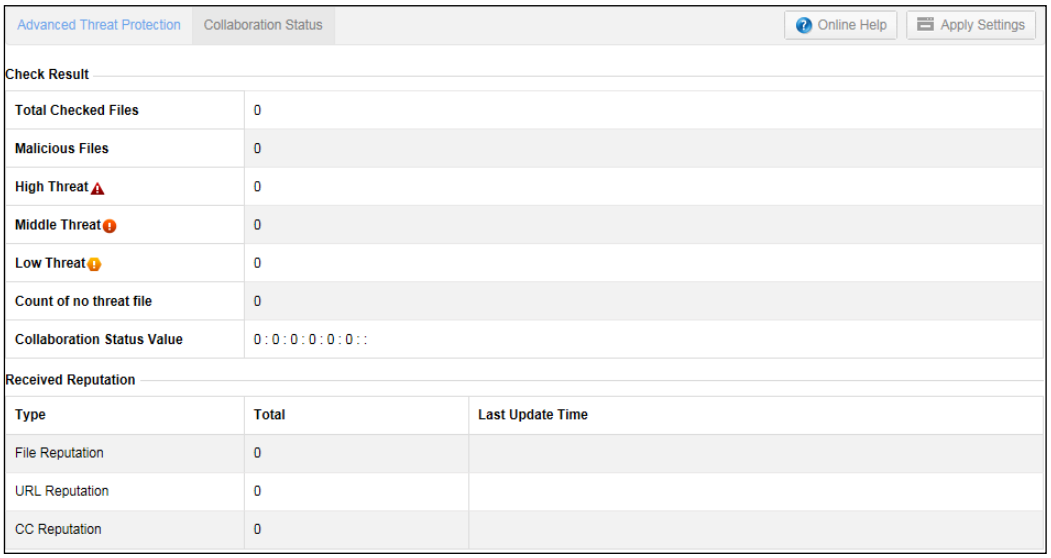
Step 3 Apply the settings.

----End

7.5.2 Collaboration Analysis Results

Choose **Policy** > **Advanced Threat Protection** > **Collaboration Status**. On the page that appears, you can check the file detection results and reputation data received by NIPS from TAC.

Figure 7-34 Viewing the collaboration analysis results



- Detection results: file detection results received by NIPS from TAC
  - **Total Checked Files**
  - **Malicious files**: including the number of high-risk files, number of medium-risk files, and number of low-risk files.
  - **Count of no threat files**
- Received reputation data
  - **File Reputation**: number of reputation values of dangerous files received from TAC
  - **URL Reputation**: number of reputation values of malicious websites received from TAC
  - **CC Reputation**: number of botnet reputation values received from TAC

7.6 Configuring URL Category Filtering Policies

URL category filtering is a web page filtering function. With URL category filtering policies, NIPS can filter HTTP request packets based on the following:

- Source/Destination IP address
- User
- Time
- Website

NIPS can obtain URL categories by means of the following:

- Built-in categories: NIPS caches certain system categories locally. Each system category contains websites that will be filtered.
- Categories obtained from cloud servers: NIPS can obtain URL category rules from the cloud servers.
- Custom URL categories: URL categories created by administrators.

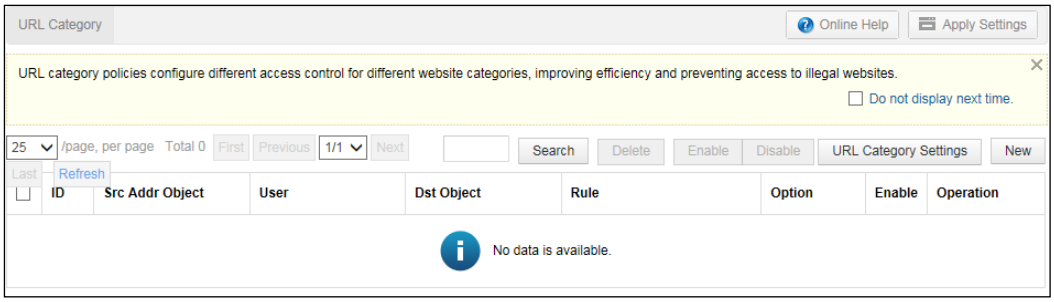
This section describes how to configure the URL category mode, and create and test URL categories.

7.6.1 URL Category Mode

The URL category mode determines the URL categories that can be managed in the URL category policy.

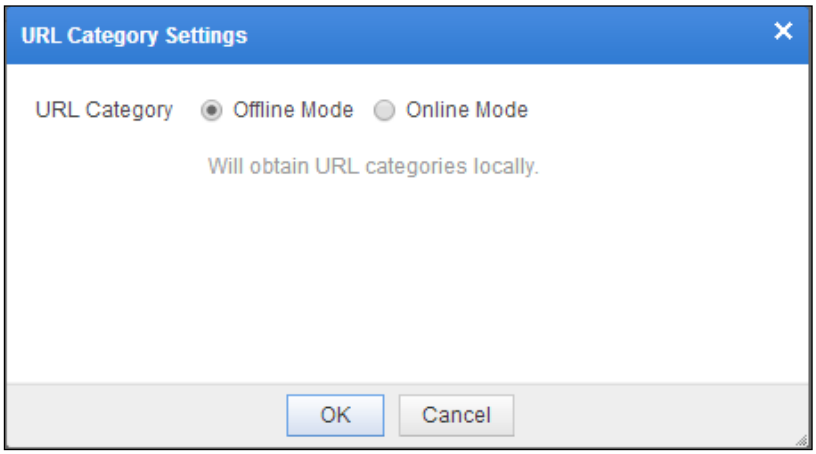
Step 1 Choose **Policy** > **URL Category**.

Figure 7-35 URL Category page



Step 2 Click **URL Category Settings**.

Figure 7-36 URL Category Settings dialog box



Step 3 Select a URL category mode.

- **Offline Mode**: indicates that URL categories, including built-in URL categories and custom URL categories, will be obtained from the local NIPS.
- **Online Mode**: indicates that URL categories, including built-in URL categories, custom URL categories, and URL categories configured on local and online servers, will be obtained from the local NIPS and online servers.

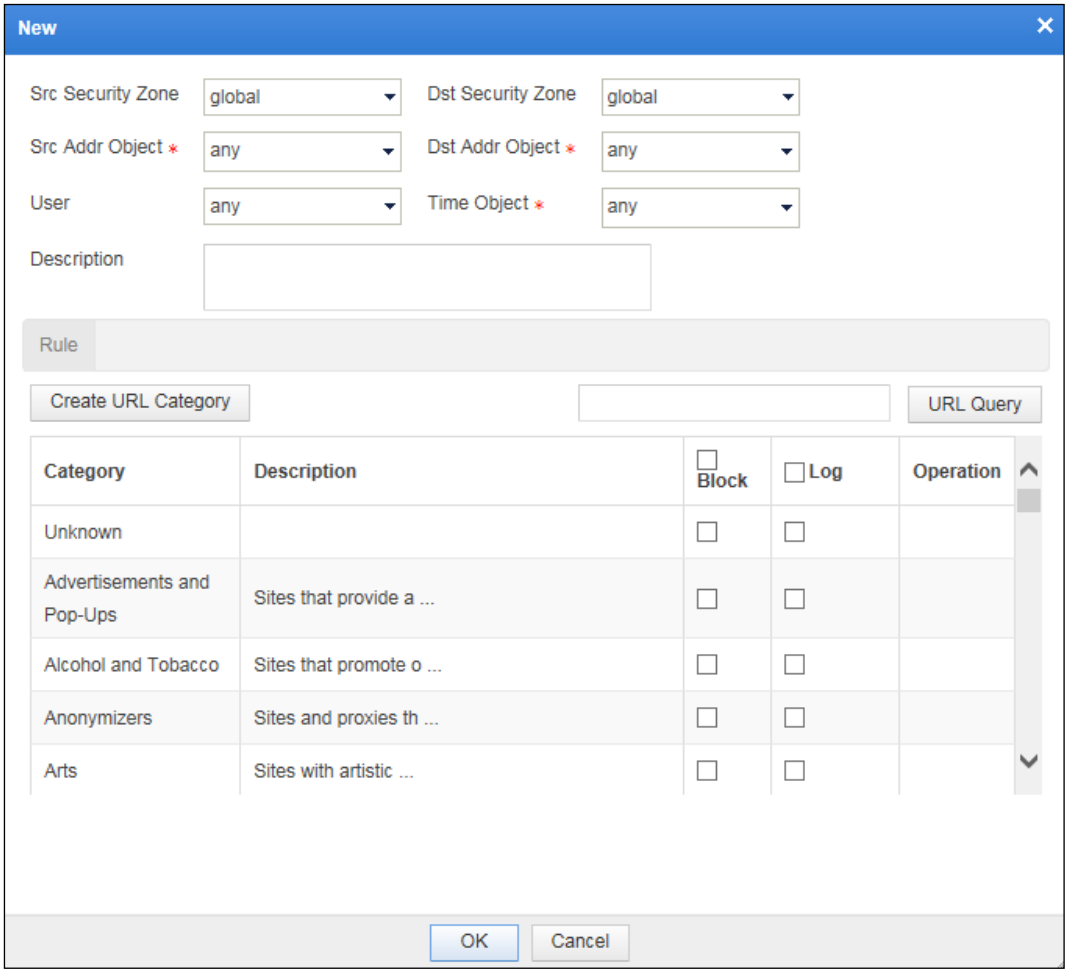
Step 4 Click **OK** to save the settings.

----End

7.6.2 URL Category Policy

Step 1 On the **URL Category** page shown in Figure 7-35, click **New**.

Figure 7-37 Creating a URL category policy



Step 2 Configure parameters.

Table 7-14 Parameters for configuring a URL category policy

Parameter	Description
Src Security Zone	Specifies a source security zone. Packets from the specified security zone will be checked against this URL filtering policy. **global** indicates that packets from any security zones will be checked against this policy.
Dst Security Zone	Specifies a destination security zone. Packets to the specified security zone will be checked against this URL category policy. **global** indicates that packets to any security zones will be checked against this policy.

Parameter	Description
	Note For NIPS NX5-T9010A and NX5-T9020A, the source security zone and destination security zone must be the same for a URL filtering policy. After you select the source security zone, the destination security zone changes automatically.
Src Addr Object	Specifies one or more source address objects to which the URL category policy will apply. **any** indicates that packets to any IP addresses will be checked against this policy.
Dst Addr Object	Specifies one or more destination address objects to which the URL category policy will apply. **any** indicates that packets to any IP addresses will be checked against this policy.
User	Specifies users to which the URL category filtering policy will apply. Four types of users are available: • **any**: indicates any users. • **Trusted user**: indicates online users. For details about online users, see section 2.3 Online Users. • **Untrusted user**: indicates IP addresses other than IP addresses of trusted users. • **Custom user**: indicates users selected from the user list obtained from the AD domain configurator. For details about the AD domain configurator, see appendix B AD Domain Configurator Management.
Time Object	Specifies time periods when this URL category policy takes effect. **any** indicates that this policy is valid all any time.
Description	Brief description of the URL category policy.
Rule	Specifies URL categories contained in the URL category policy and corresponding processing methods. The processing method has two values: **Block** and **Log**.

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

Step 4 Apply the settings.

----End

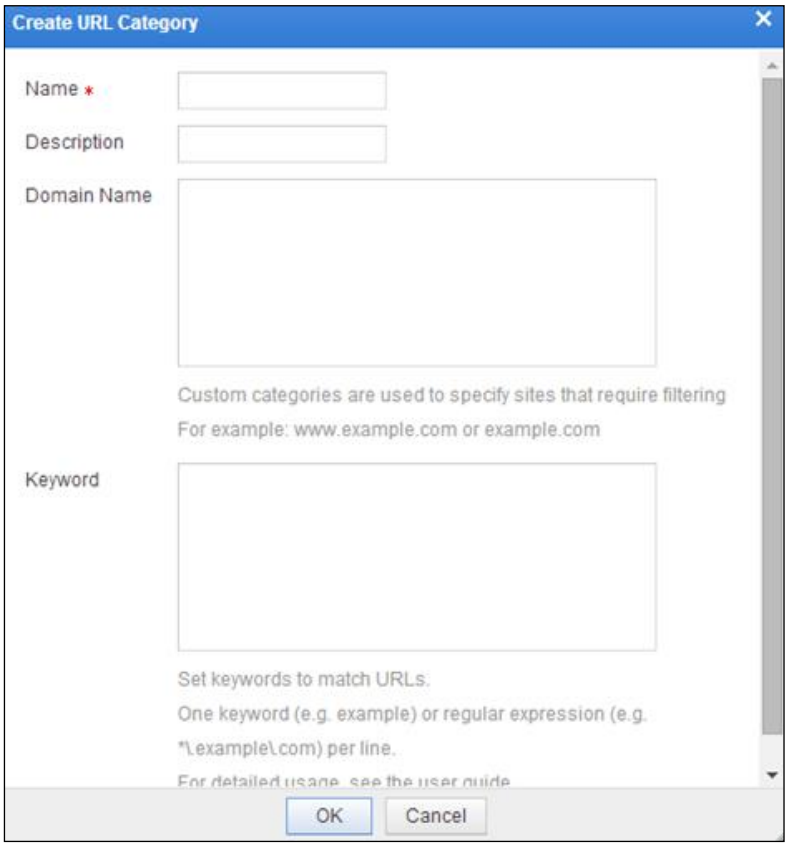
7.6.3 Custom URL Category

When it is necessary to add some websites for filtering, NIPS allows you to create custom URL categories.

To configure a custom category, follow these steps:

Step 1 In the dialog box shown in Figure 7-37, click **Create URL Category**.

Figure 7-38 Creating a URL category



Step 2 Configure parameters in the **Create URL Category** dialog box.

Table 7-15 Parameters for configuring a URL category

Parameter	Description
Name	Specifies the name of the URL category.
Description	Brief description of the URL category.
Domain Name	Specifies domain names of websites to be included in the URL category.
Keyword	Specifies the keyword or regular expression to match by the domain name. Multiple keywords or regular expressions are separated by carriage returns.

Note	Once a URL is specified in the custom categories, it no longer exists in system categories of the URL library.

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

----End

7.6.4 URL Category Query

NIPS caches parts of URL categories locally. With the URL category query feature, you can quickly find out the category to which a URL belongs in the URL library. If the category cannot be found in the local cache, NIPS checks it from the cloud server and displays the result on the web-based manager. For URLs which are categorized as **Unknown**, you can categorize them as required. For how to customize URL categories, see section 7.6.3 Custom URL Category.

To query the category of a URL, follow these steps:

Step 1 In the dialog box shown in Figure 7-37, enter a desired URL (www.youku.com for example) in the text box on the left of **URL Test**.

Figure 7-39 URL Test text box

Step 2 Click **URL Query**.

Figure 7-40 URL category query result

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

----End

7.7 Configuring Antivirus Policies

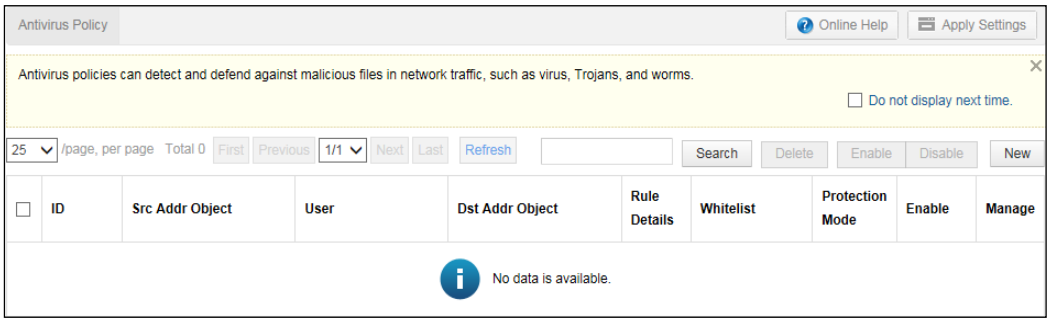
In addition to the built-in malicious virus database, NIPS also brings third-party virus database, Bitdefender, with a total number of 100,000 viruses.

Antivirus policies enable NIPS to provide protection against viruses. You can set a virus whitelist to allow certain special virus files to pass. You can configure, edit, delete, move, or copy policies on NIPS.

To configure an antivirus policy, follow these steps:

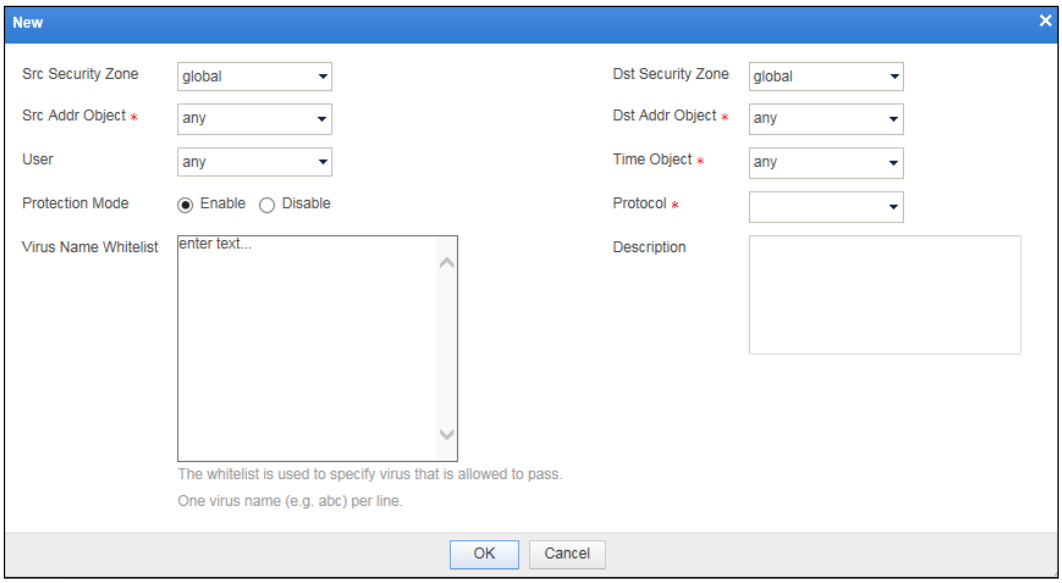
Step 1 Choose **Policy** > **Antivirus**.

Figure 7-41 Antivirus Policy page



Step 2 Click **New** in the upper-right corner.

Figure 7-42 Creating an antivirus policy



Step 3 Configure parameters in the **New** dialog box.

Table 7-16 Parameters for configuring an antivirus policy

Parameter	Description
Src Security Zone	Specifies a source security zone. Packets from the specified security zone will be checked against this antivirus policy. **global** indicates that packets from any security zones will be checked against this policy.
Dst Security Zone	Specifies destination a security zone. Packets to the specified security zone will be checked against this antivirus policy. **global** indicates that packets from any security zones will be matched with this policy. Note

Parameter	Description
	For NIPS NX5-T9010A and NX5-T9020A, the source security zone and destination security zone must be the same for an antivirus policy. After you specify a source security zone, the destination security zone changes automatically.
Protocol	Specifies protocols to which this policy will apply. It has such values as **http**, **ftp**, **smtp**, **pop3**, and **imap**.
Src Addr Object	Specifies one or more source address objects to which the antivirus policy will apply. **any** indicates that packets from any IP addresses will be matched with this policy.
Dst Addr Object	Specifies one or more destination address objects to which the antivirus policy will apply. **any** indicates that packets to any IP addresses will be matched with this policy.
User	Specifies users to which the antivirus policy will apply. Four types of users are available: • **any**: indicates any users. • **Trusted user**: indicates online users. For details about online users, see section 2.3 Online Users. • **Untrusted user**: indicates users other than trusted users. • **Custom user**: indicates users selected from the user list obtained from the AD domain configurator. For details about the AD domain configurator, see appendix B AD Domain Configurator Management.
Time Object	Specifies time periods when this antivirus policy is valid. **any** indicates that this policy is valid all the time.
Protection Mode	Controls whether to enable the protection mode. By default, it is enabled. If the protection mode is enabled, the system will block packets matching this antivirus policy. If the protection mode is disabled, the system only reports alert logs, but not block packets.
Virus Name Whitelist	Specifies virus names in the whitelist which will not be scanned by the antivirus engine. Multiple virus names are separated by spaces.
Description	Brief description of the antivirus policy.

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

Step 5 Apply the settings.

----End

7.8 Configuring User Management Policies

NIPS can authenticate users locally or via a third-party server. Authentication via a third-party server includes:

- AD domain authentication
- Radius authentication

- EPS authentication
- LDAP authentication

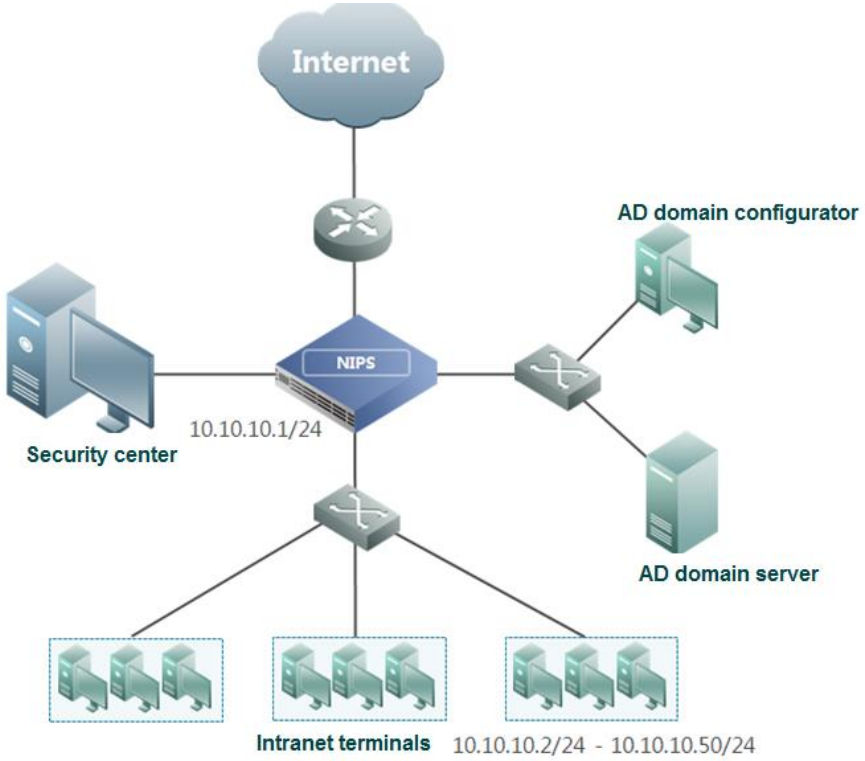
This section describes how to configure a third-party authentication server, user authentication mode, user identification policy, user authentication policy, and an intelligent user association policy.

7.8.1 Server Configuration

The following describes how to configure authentication servers on NIPS.

In AD domain authentication, intranet users are managed by the AD domain server. NIPS regularly obtains online users' information (including the IP address of each online user) from the AD domain configurator. Figure 7-43 shows the network topology for this type of authentication.

Figure 7-43 Network topology for AD domain authentication



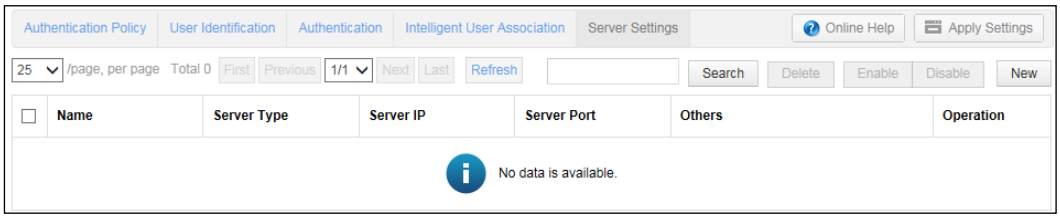
To use AD domain authentication, you must have configured the AD domain configurator to manage user information obtained from the domain controller. For details, see appendix B AD Domain Configurator Management. Then configure the following on NIPS:

- AD domain server
- Method of updating the user list on the AD domain server (see section 7.8.3 User Identification)

To configure authentication servers on NIPS, follow these steps:

Step 1 Log in as **admin** and choose **Policy** > **User Management** > **Server Settings**.

Figure 7-44 Server Settings page



Step 2 Click **New** in the upper-right corner.

Parameters in the **New** dialog box vary with the type of authentication servers. Figure 7-45 shows the **New** dialog box for configuring an AD domain server. Figure 7-46 shows the **New** dialog box for configuring a Radius server. Figure 7-47 shows the **New** dialog box for configuring an EPS server. Figure 7-48 shows the **New** dialog box for configuring an LDAP server.

Figure 7-45 **C**onfiguring an AD domain server

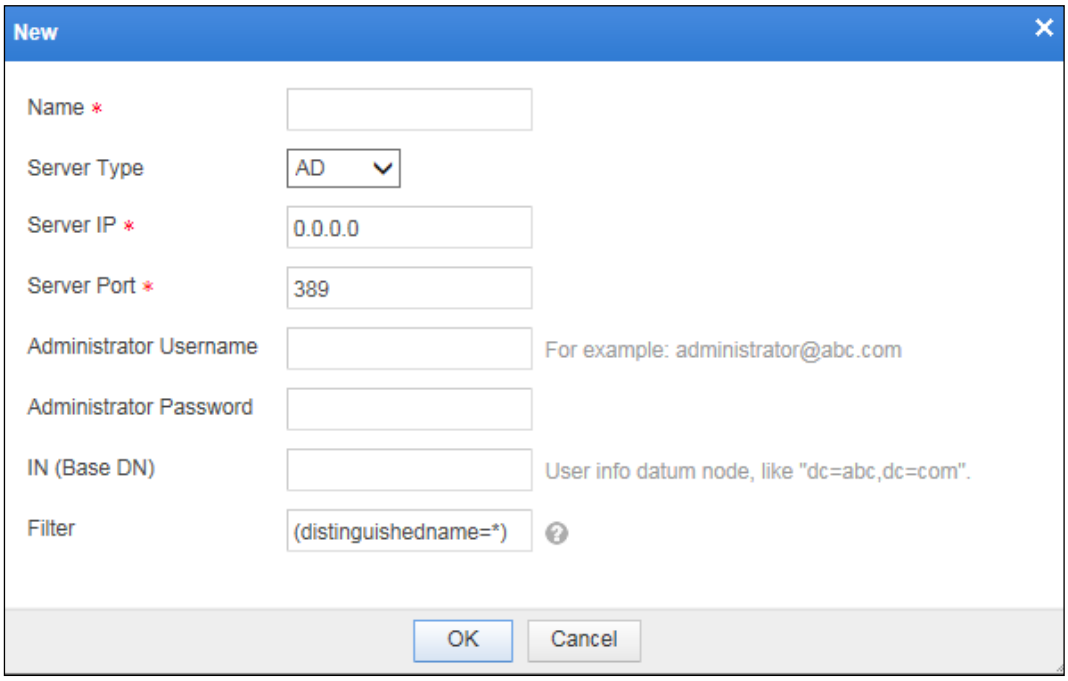


Figure 7-46 **C**onfiguring a Radius server

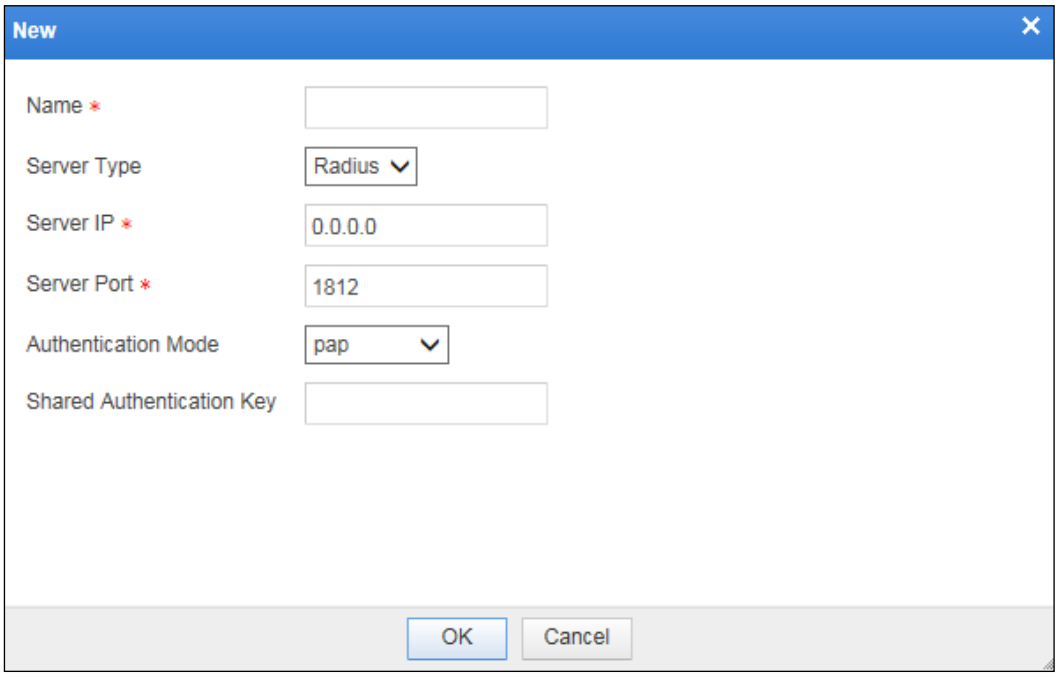


Figure 7-47 Configuring an EPS server

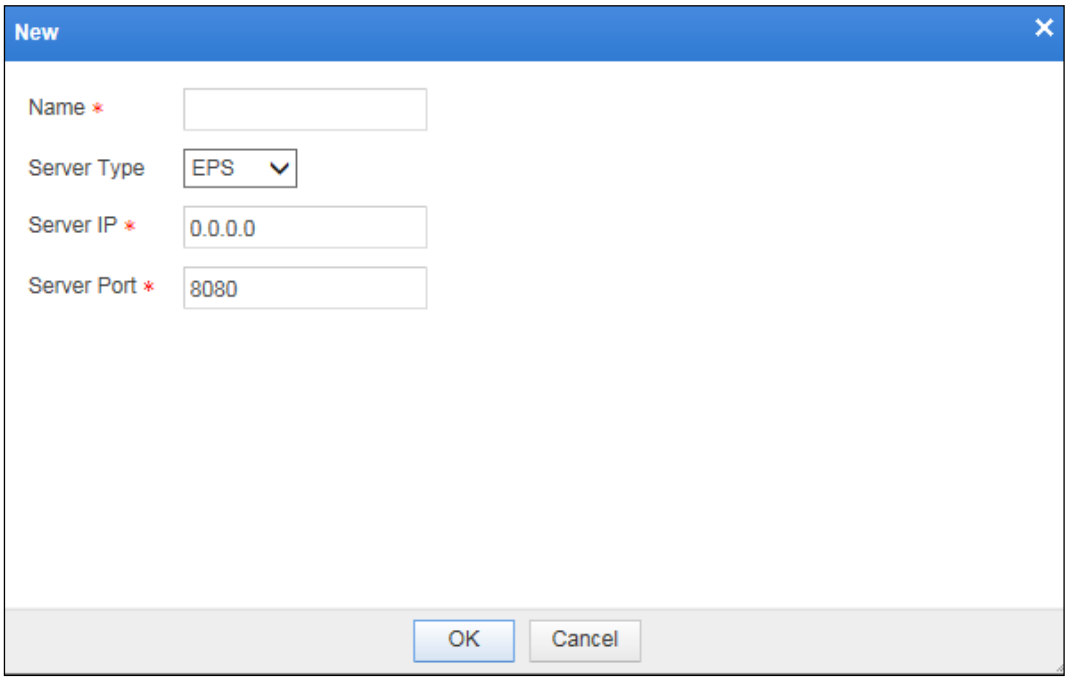
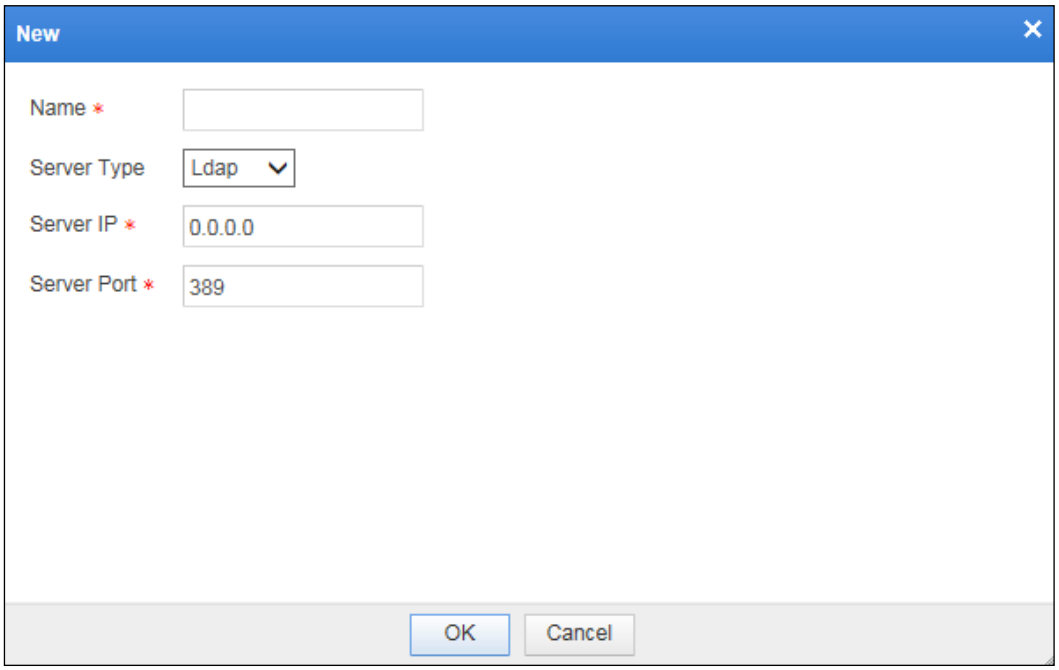


Figure 7-48 Configuring an LDAP server



Step 3 Configure authentication server parameters.

Table 7-17 Parameters for configuring authentication servers

Parameter	Description
Name	Specifies the name of an authentication server. The server name must be unique. It is a character string that cannot contain spaces and the following characters: / % \ { } ` ^ < > ' & " :
Server Type	Specifies the type of an authentication server, which can be one of the following: • **AD**: indicates a server for AD domain authentication. • **Radius**: indicates a server for Radius authentication. • **EPS**: indicates authentication with NSFOCUS EPS that collaborates with NIPS. After collaboration with EPS is enabled, the client automatically switches to the authentication page of EPS for authentication after the agent is downloaded. **Note** • A management interface or a working interface with the management function must be used for collaboration between NIPS and EPS. • For details about EPS, contact technical support engineers of NSFOCUS. • **Ldap**: indicates a server for LDAP authentication.
Server IP Address/Port	Specifies the IP address and port of the new authentication server or

Parameter	Description
	collaborative server.
Administrator Username/Password	Specifies the user name and password for login to the AD domain server. Note These two parameters are available only for AD domain servers.
IN (Base DN)	Specifies where to load user information. Note This parameter is available only for AD domain authentication.
Filter	Specifies the filter. The default value is **(distinguishedname=*)**, indicating that all user lists can be obtained. For details about more advanced usage, refer to the search syntax related to LDAP search filters. Note This parameter is available only for AD domain authentication.
Authentication Mode	Specifies the authentication mode of the Radius authentication server, which can be **pap**, **spap**, **chap**, **mschapv1**, **mschapv2**, or **eap_md5**. Note This parameter is available only for Radius authentication.
Authentication Shared Key	Specifies the shared key that serves as a password between the Radius server and a Radius client. Note • The shared secret configured on NIPS must be the same as that configured on the Radius server; otherwise, NIPS cannot communicate with the Radius server. • This parameter is available only for Radius authentication.

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

----End

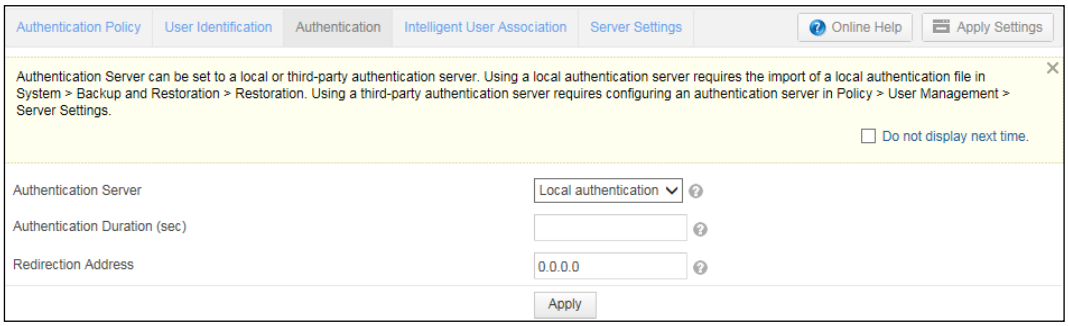
7.8.2 User Authentication

After the user authentication configuration is complete, the engine automatically restarts.

To configure user authentication, follow these steps:

Step 1 Choose **Policy** > **User Management** > **Authentication**.

Figure 7-49 Authentication page



Step 2 Configure user authentication parameters.

Table 7-18 User authentication parameters

Parameter	Description
Authentication Server	Specifies an authentication server, which can be a local server or a third-party server. Before enabling local authentication, you must import the local authentication file. For details, see section 4.2.2 Restoring a Backup File.
Authentication Duration (sec)	Time that authentication lasts. If **Server Type** is set to **EPS**, the value of this parameter must be greater than the authentication interval configured on EPS.
Redirect Address	Specifies the IP address of a page to which NIPS redirects a client during authentication. **Note** This IP address must be the IP address of NIPS's management interface or working interface with the management function. In addition, this IP address must be reachable from the client over the network.

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

----End

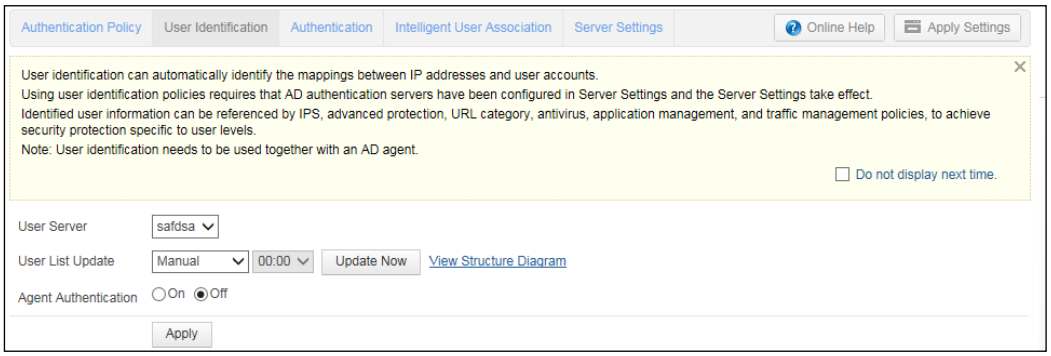
7.8.3 User Identification

Currently, NIPS supports user identification with the AD domain server. The user list can be automatically or manually updated, depending on the user identification setting. To configure user identification, follow these steps:

Step 1 Choose **Policy** > **User Management** > **User Identification**.

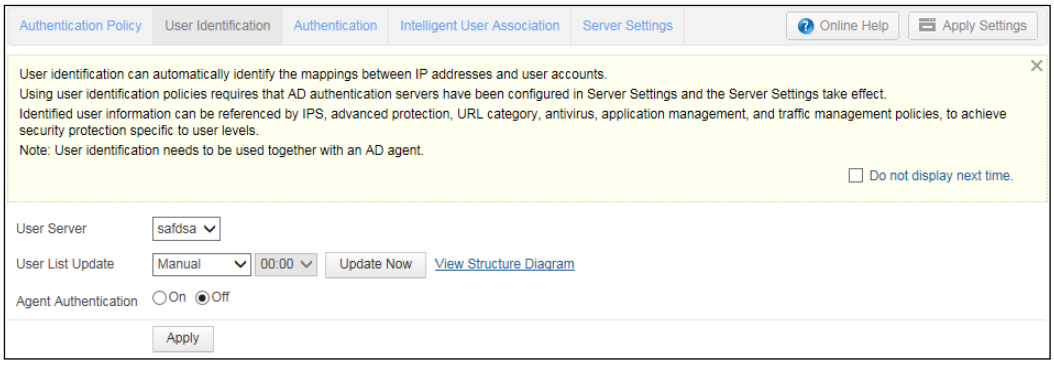
By default, **User Server** is **Off**, as shown in Figure 7-50.

Figure 7-50 User Identification page on which User Server is Off



Select a server for AD domain authentication. Figure 7-51 shows the page after such a server is selected.

Figure 7-51 User Identification page on which a server is selected



Step 2 Specify the user list update method (manual or automatic).

- The value **Manual** indicates that you need to update the user list manually.
- For the selection of other values, you need to configure the specific time so that NIPS can automatically update user information regularly.

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

Step 4 Apply the settings.

Step 5 (Optional) Click **Update Now** to immediately synchronize the user list on the AD domain server to NIPS.

Step 6 (Optional) Click **View Structure Diagram** to view users displayed in the tree structure.

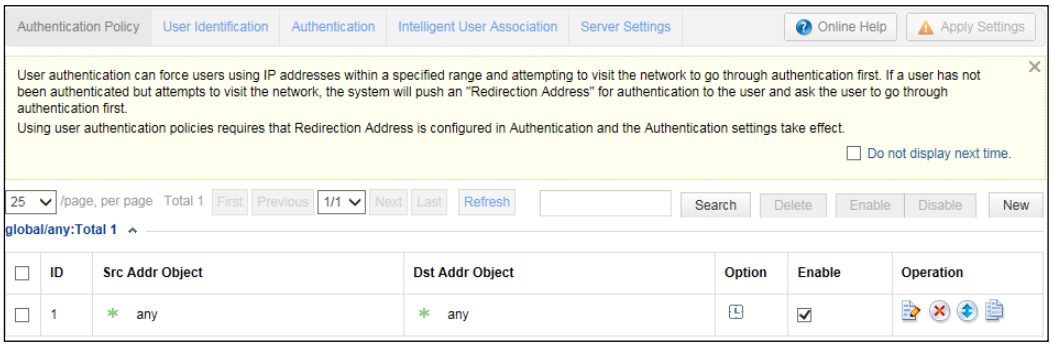
----End

7.8.4 Authentication Policy

NIPS authenticates a user when packets of the user match an authentication policy. For how to configure user authentication, see section 7.8.2 User Authentication. This section describes how to create an authentication policy.

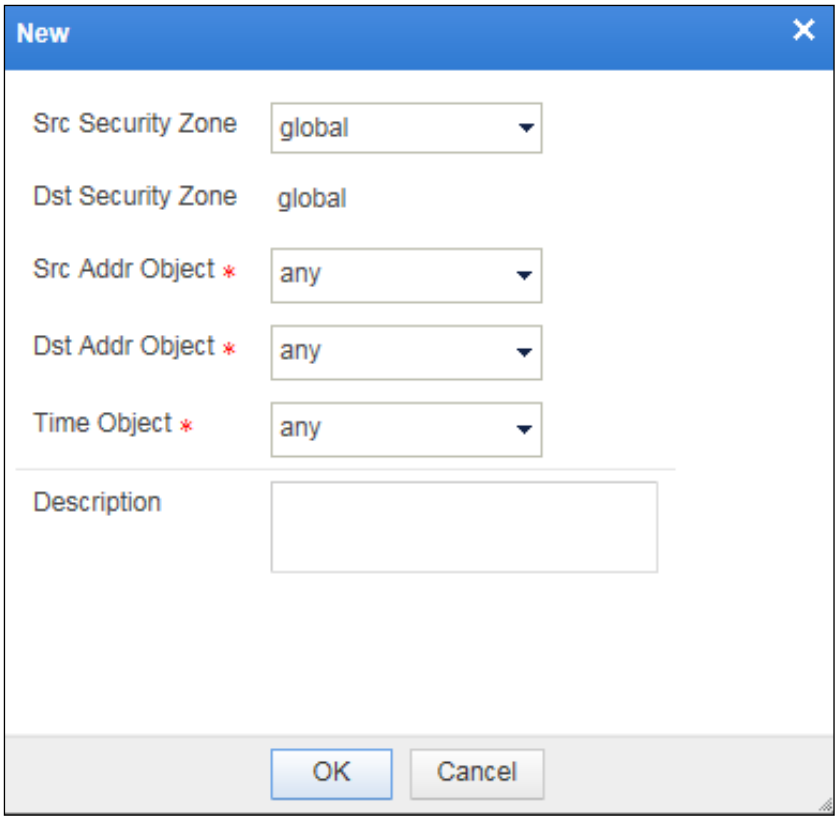
Step 1 Choose **Policy** > **User Management** > **Authentication Policy**.

Figure 7-52 Authentication Policy page



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

Figure 7-53 Creating an authentication policy



Step 3 Configure parameters in the **New** dialog box.

Table 7-19 Parameters for creating an authentication policy

Parameter	Description
Src Security Zone	Specifies a source security zone. Packets from the specified security zone will be checked against this authentication policy. **global** indicates that packets from any security zones will be checked against this

Parameter	Description
	policy.
Dst Security Zone	Specifies destination a security zone. .Packets to the specified security zone will be checked against this authentication policy. **global** indicates that packets from any security zones will be checked against this policy. Note For NIPS NX5-T9010A and NX5-T9020A, the source security zone and destination security zone must be the same for an authentication policy. After you specify a source security zone, the destination security zone changes automatically.
Src Addr Object	Specifies a source address or more to which this policy will apply. **any** indicates that packets to any IP addresses will be checked against this policy.
Dst Addr Object	Specifies a destination address or more to which this policy will apply. **any** indicates that packets to any IP addresses will be checked against this policy.
Time Object	Specifies a period when this policy is valid. **any** indicates that this policy is valid all any time.
Description	Brief description of this policy.

Step 7 Click **OK** to save the settings.

Step 8 Apply the settings.

----End

7.8.5 Intelligent User Association

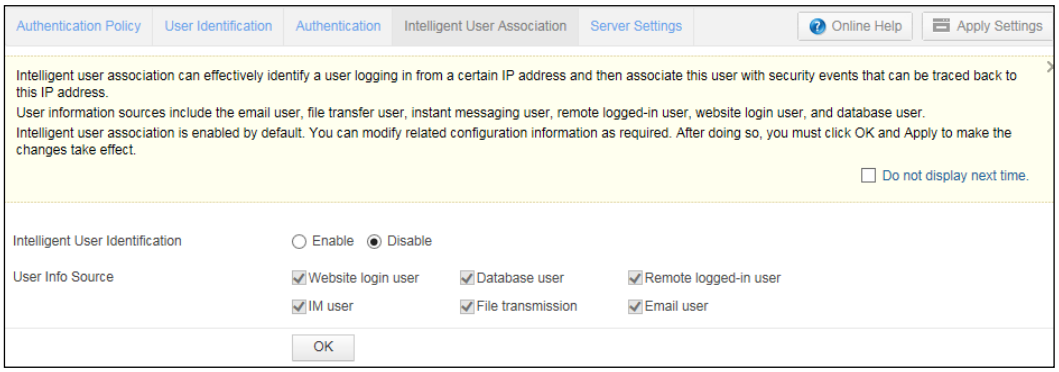
NIPS provides the intelligent user association function. After this function is enabled, NIPS can identify users of all IP addresses and perform a correlative analysis between various security events and identified users. By default, this function is disabled. After being enabled, this function applies to all types of users by default.

If intelligent user identification is enabled, the latest two associated user names are displayed in the **Associated account** column of various security events. Clicking a user name displays all accounts associated with the IP address. For details, see "Viewing Associated Users" in section 3.1 Common Operations.

To configure intelligent user association, follow these steps:

Step 1 Choose **Policy** > **User Management > Intelligent User Association**.

Figure 7-54 Intelligent User Association page



Step 2 Click **Enable** for **Intelligent User Identification** and select user types.

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

Step 4 Apply the settings.

----End

7.9 Configuring Application Management Policies

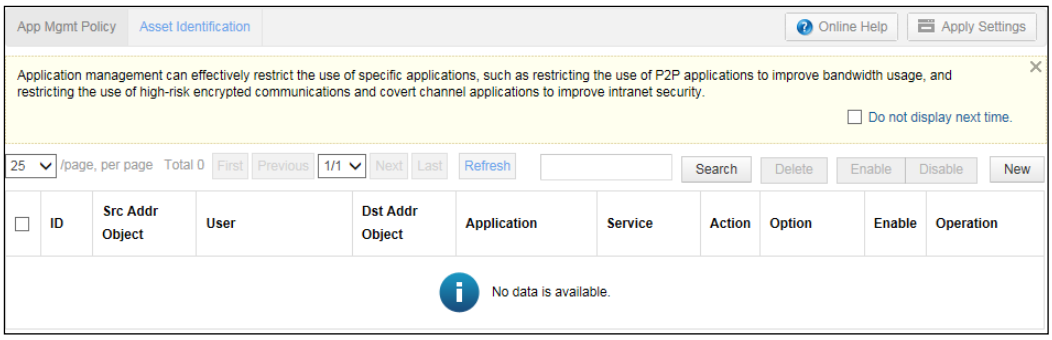
7.9.1 Application Management Policy

With application management policies, NIPS can exert application- or service-based control over packets passing through it. The control actions include allowing to pass through, blocking, forwarding, and logging related events.

This section describes how to create an application management policy. The procedure is as follows:

Step 1 Choose **Policy** > **Application Management**.

Figure 7-55 App Mgmt Policy page

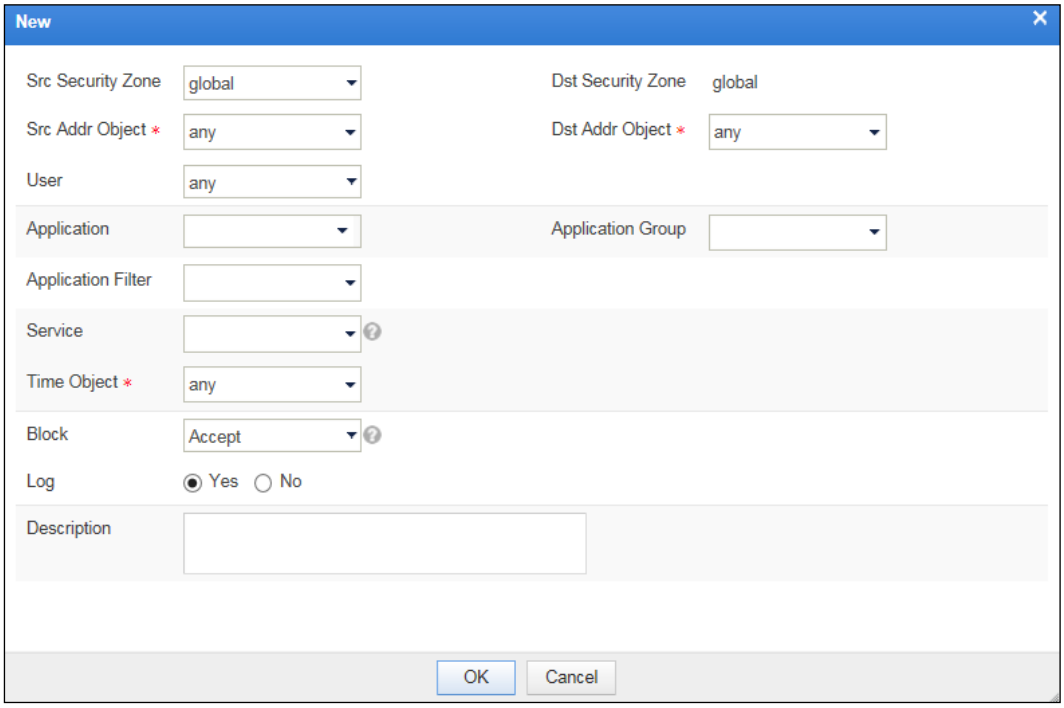


Step 2 Click **New** in the upper-right corner of the page.

The dialog box displayed for creating an application management policy varies with device models.

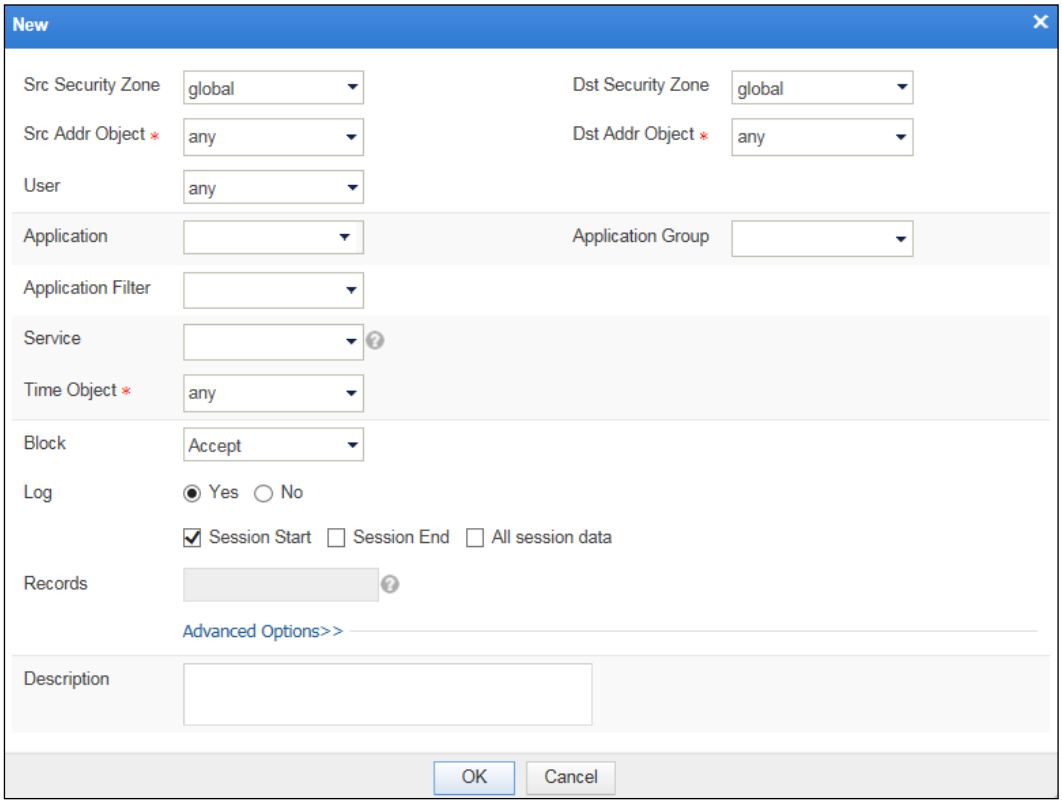
- Figure 7-56 shows the dialog box for creating an application management policy on NX5-T9010A and NX5-T9020A.

Figure 7-56 Creating an application management policy on NX5-T9010A and NX5-T9020A



- Figure 7-57 shows the dialog box for creating an application management policy of device models other than NX5-T9010A and NX5-T9020A.

Figure 7-57 Creating an application management policy of device models other than NX5-T9010A and NX5-T9020A



Step 3 Configure parameters in the **New** dialog box.

Table 7-20 Parameters for configuring an application management policy

Parameter	Description
Src Security Zone	Specifies a source security zone. Packets from the specified security zone will be checked against this application management policy. **global** indicates that packets from any security zones will be checked against this policy.
Dst Security Zone	Specifies a destination security zone. Packets to the specified security zone will be checked against this application management policy. **global** indicates that packets from any security zones will be checked against this policy. **Note** For NIPS NX5-T9010A and NX5-T9020A, the source security zone and destination security zone must be the same for an application management policy. After you specify a source security zone, the destination security zone changes automatically.
Src Addr Object	Specifies a source address or more to which this policy will apply. **any** indicates that packets from any IP addresses will be checked against this policy.

Parameter	Description
Dst Addr Object	Specifies a destination address or more to which this policy will apply. **any** indicates that packets to any IP addresses will be checked against this policy.
User	Specifies users to which this policy will apply. Four types of users are available: • **any**: indicates any users. • **Trusted user**: indicates online users. For details about online users, see section 2.3 Online Users. • **Untrusted user**: indicates IP addresses other than IP addresses of trusted users. • **Custom user**: indicates users selected from the user list obtained from the AD domain configurator. For details about the AD domain configurator, see appendix B AD Domain Configurator Management.
Application	Specifies applications to which this policy will apply. For details about how to configure application objects, see sections 6.4.1 System Application and 6.4.2 Custom Application. Note At least one of **Application**, **Application Filter**, **Application Group** and **Service** must be specified.
Application Group	Specifies the application group object to which this policy will apply. For details on how to configure an application group, see section 6.4.3 Application Group. Note At least one of **Application**, **Application Filter**, **Application Group**, and **Service** must be specified.
Application Filter	Specifies an application filter or more to pick out applications that will be checked against this policy. For how to configure application objects, see section 6.4.4 Filter. Note At least one of **Application**, **Application Filter**, **Application Group** and **Service** must be specified.
Service	Specifies service objects to which this policy will apply. Note At least one of **Application**, **Application Filter**, **Application Group** and **Service** must be specified.
Time Object	Specifies the period when this policy takes effect. **any** indicates that this policy is valid all any time.
Block	Controls how to handle packets that hit this policy. • **Block**: NIPS blocks matching packets without checking them against other policies.

Parameter	Description
	• **Accept**: NIPS allows matching packets to pass the check by this policy, but continues to check them against other policies. • **Forward**: NIPS directly forwards matching packets, without any further checks. Note This parameter can be set to **Forward** only when **Service** is set to a service at layer 4 to 6 (namely, the transport layer, session layer, and presentation layer), and **Application**, **Application Group**, and **Filter** are left empty.
Log	Controls whether to log related events. • If **Log** is set to **Yes**, logs are recorded when packets match this policy. For NX5-T9010A and NX5-T9020A, you can only set **Log** to **Yes** or **No**. • For other models other than NX5-T9010A and NX5-T9020A, if **Log** is set to **Yes**, you also need to configure the logging method by selecting **Session Started**, **Session Ended**, and/or **All session data**. When you select **All session data**, you also need to set the maximum number of entries. Note that logging all session data will generate a large number of logs and will affect the performance of NIPS.
Description	Brief description of this policy

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

Step 5 Apply the settings.

----End

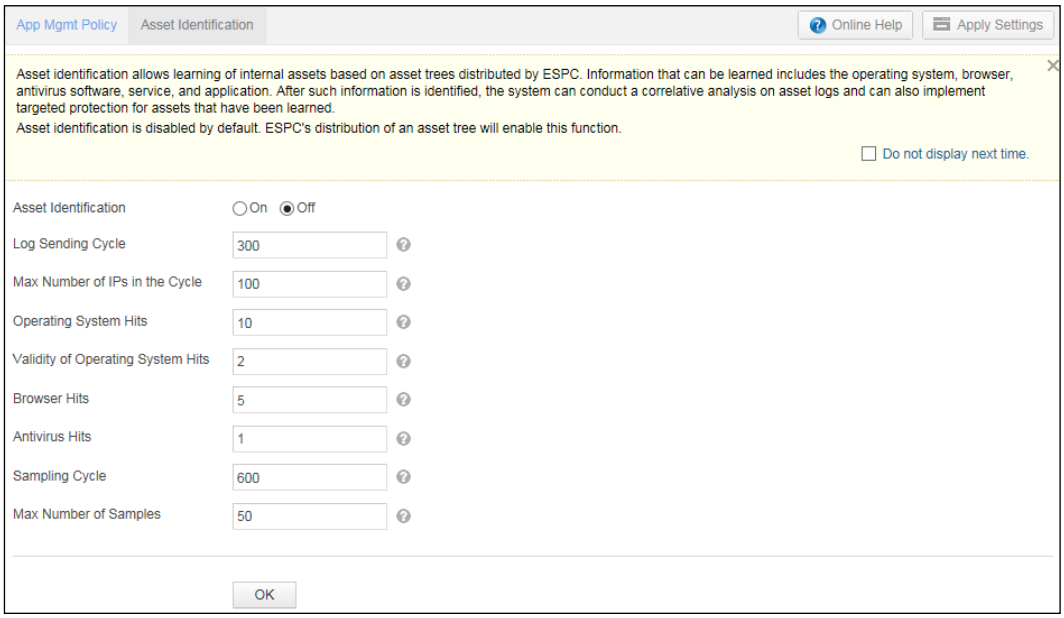
7.9.2 Asset Identification Policy

When NIPS properly collaborates with ESPC, after receiving asset trees (see section 6.8 Clearing Asset Trees) from ESPC, NIPS identifies assets indicated with IP addresses in asset trees according to the configured asset identification policy and displays the identified assets on the asset details page (see section 8.1.6 Viewing Asset Details).

To create an asset identification policy, follow these steps:

Step 1 Choose **Policy** > **Application Management** > **Asset Identification**.

Figure 7-58 Asset Identification page



Step 2 Configure parameters.

Table 7-21 Parameters for configuring an asset identification policy

Parameter	Description
Asset Identification	Controls whether to enable asset identification. By default, this function is disabled. **Note** After receiving an asset identification policy from ESPC, NIPS automatically turns on asset identification.
Log Sending Cycle	Cycle for sending asset-related logs. The value range is 0–3600 seconds.
Max Number of IPs in the Cycle	Specifies the maximum number of IP addresses sent in a log sending cycle.
Operating System Hits	A log is sent to ESPC and BSA when an operating system is identified for the number of times specified here within a log sending cycle. The value range is 0–255.
Validity of Operating System Hits	When the number of consecutive log sending times for an operating system reaches the value specified here, NIPS deems the operating system to be a trusted asset and will not attempt to identify it again.
Browser Hits	A log is sent when a browser is identified for the number of times specified here within a log sending cycle. The value range is 0–255.
Antivirus Hits	A log is sent when a piece of antivirus software is identified for the number of times specified here within a log sending cycle. The value range is 0–255.
Sampling Cycle	Cycle for sampling each attribute of an asset. The value range is 0–3600 seconds.
Max Number of Samples	Specifies the maximum number of times each attribute of an asset is sampled

Parameter	Description
	in a sampling cycle. The value range is 0–3600.

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

Step 4 Apply the settings.

----End

7.10 Configuring Traffic Management Policies

Traffic management policies are used to restrict channel traffic and control traffic licenses and priorities of authorized users. They can ensure the proper use of network resources and more reasonable proportions and distributions of different types of traffic. In addition, together with the minimum guaranteed bit rate, maximum guaranteed bit rate, and session restriction, traffic management policies guarantee the bandwidth for key sessions.

NIPS's traffic management policies can be divided into traffic control policies and traffic analysis policies.

The roadmap for configuring a traffic management policy is as follows:

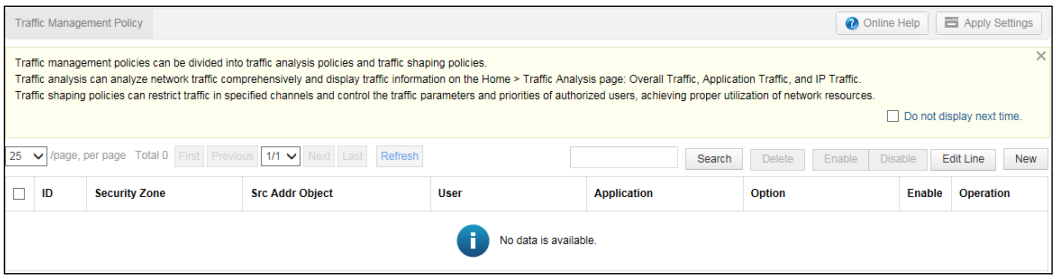
- Configure a traffic channel (see section 6.7 Configuring a Traffic Channel Object for details).
- Configure a line.
- Create a traffic management policy.
- Apply configuration.

7.10.1 Traffic Control Policy

To create a traffic control policy, follow these steps:

Step 1 Choose **Policy** > **Traffic**.

Figure 7-59 Traffic Management Policy page



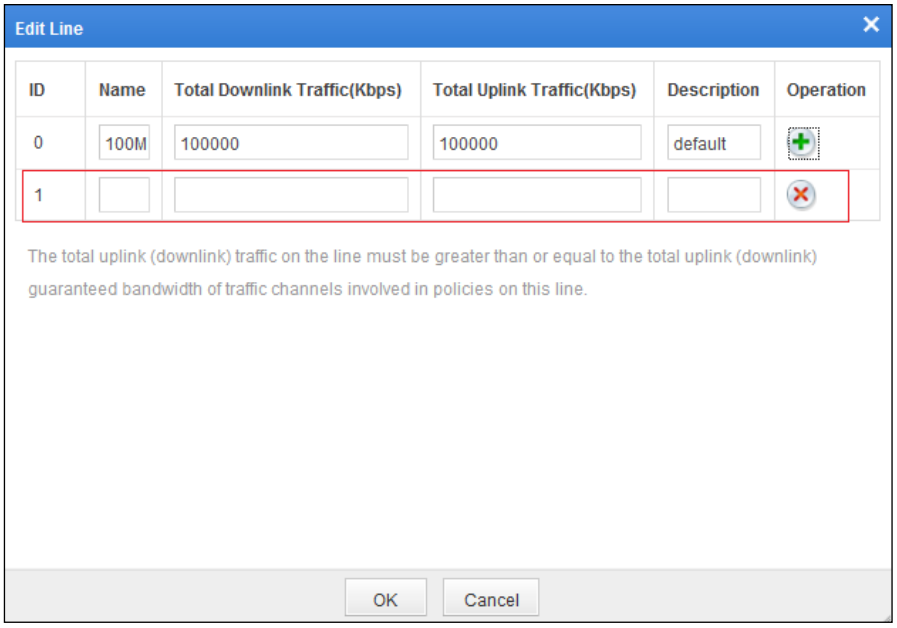
If you move to an object name and hover for a while, details of this object are displayed.

Step 2 (Optional) Create a line.

Alternatively, you can use default lines.

a. Click **Edit Line** in the upper-right corner of the tab page.

Figure 7-60 Creating a line



b. Click to add a line.

c. Configure parameters for this line.

Table 7-22 Parameters for creating a line

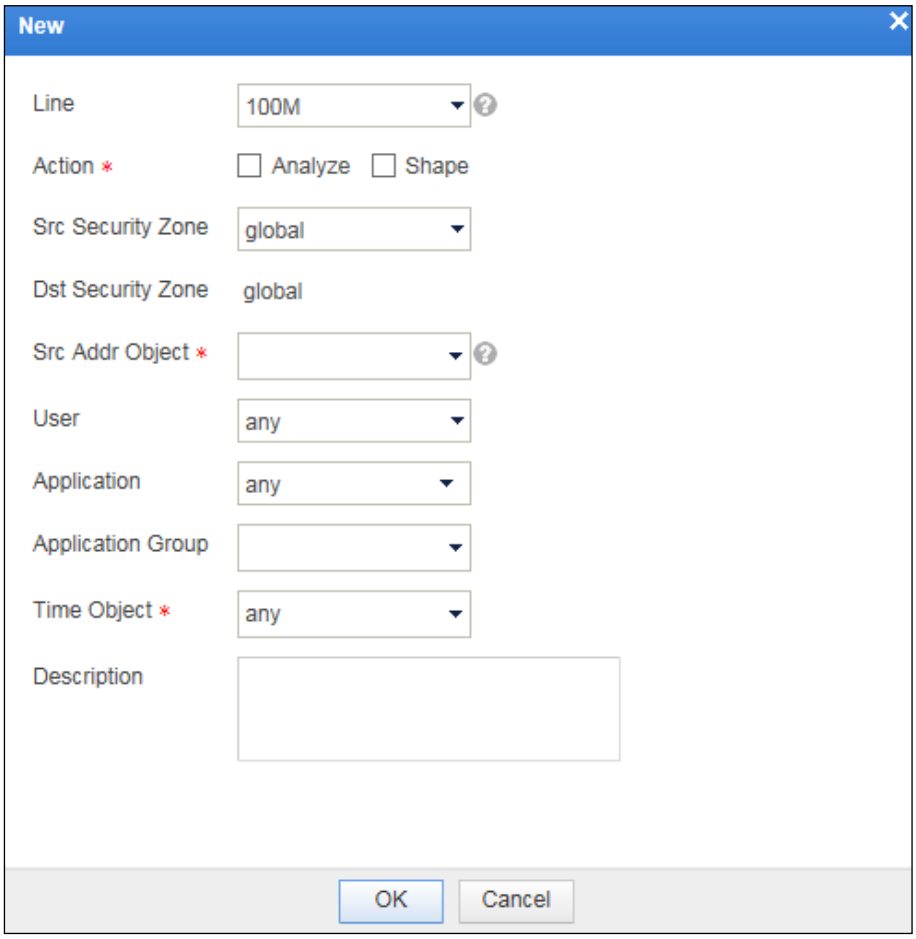
Parameter	Description
Name	Name of the new line.
Total Uplink Traffic(Kbps)	The total uplink traffic must be greater than the sum of uplink GBRs of traffic channels involved in all policies.
Total Downlink Traffic(Kbps)	The total downlink traffic must be greater than the sum of downlink GBRs of traffic channels involved in all policies.
Description	Brief description of the new line.

d. Click **OK** to save the settings and return to the list of traffic management policies.

Step 3 Create a traffic control policy.

a. Click **New** in the upper-right corner of the **Traffic Management Policy** page.

Figure 7-61 Creating a traffic control policy



b. Configure parameters in the **New** dialog box.

Table 7-23 Parameters for creating a traffic control policy

Parameter	Description
Line	Specifies a line to which this policy applies.
Action	Specifies the policy type. To create a traffic control policy, you must select **Shape**. • **Analyze**: indicates that NIPS uses this new policy to analyze traffic of services used by source address objects. • **Shape**: limits the traffic rate on a specified channel.
Traffic Channel	Specifies a traffic channel to which this policy will apply.
Src Security Zone	Specifies a source security zone. Packets from the specified security zone will be checked against this traffic control policy. **global** indicates that packets from any security zones will be checked against this policy.
Dst Security Zone	Specifies a destination security zone. Packets from the specified security zone will be checked against this traffic control policy. **global** indicates that packets to any security zones will be checked against this

Parameter	Description
	policy. Note For NIPS NX5-T9010A and NX5-T9020A, the source security zone and destination security zone must be the same for a traffic control policy. After you specify a source security zone, the destination security zone changes automatically.
Src Addr Object	Specifies an address object that generate uplink traffic. Note • **Src Addr Object** should not be any when **Security Zone** is set to **global**, **Direct-A**, or **Direct-B (or Vwire in certain device models)**. • **Per IP** is available only for a traffic control policy (when Shape is selected for Action). If you select Per IP, NIPS controls traffic for each IP address included in source address objects. If you do not select it, NIPS controls traffic for source address objects on the whole.
User	Specifies user objects of this policy.
Application	Specifies applications to which this policy will apply.
Application Group	Specifies the application group to which this policy will apply
Time Objects	Specifies the period when this policy is valid.
Description	Brief description of this policy.

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

Step 4 Apply the settings.

----End

7.10.2 Traffic Analysis Policy

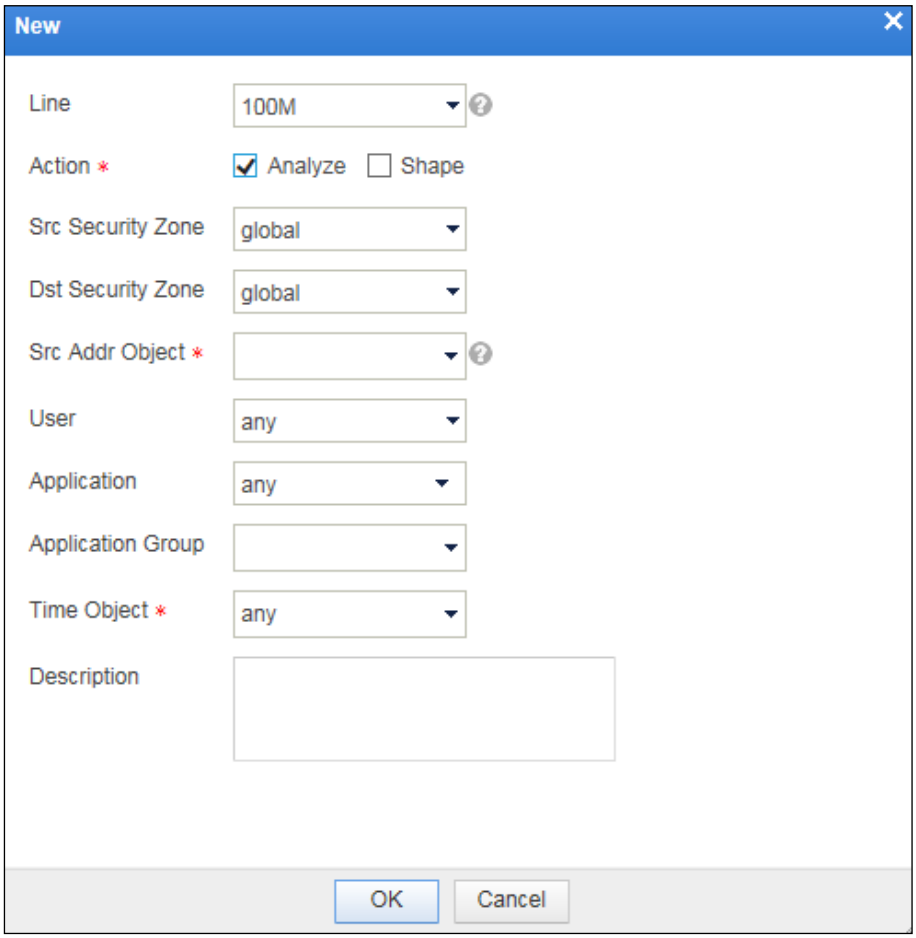
A traffic analysis policy is used to analyze network traffic data. You can search for, create, edit, delete, and sort traffic analysis policies. To create a traffic analysis policy, follow these steps:

Step 1 Perform Step 1 and Step 2 in section 7.10.1 Traffic Control Policy.

Step 2 Create a traffic analysis policy.

a. Click **New** in the upper-right corner of the **Traffic Management Policy** page.

Figure 7-62 Creating a traffic analysis policy



b. Configure parameters in the **New** dialog box.

For the description of parameters, see Table 7-23.

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

Step 3 Apply the settings.

----End

8 Logs and Reports

This chapter covers the following sections:

Section	Description
Logs	Describes how to handle and view various logs.
Reports	Describes how to handle and view various reports.

8.1 Logs

This section covers the following topics:

- Handling Logs
- Viewing Logs

You can query various logs of NIPS based on different query conditions. From logs, you can detect traces of attackers, view real-time network status, and adjust the prevention policy promptly to achieve more efficient security protection for the network or server.

NIPS can store up to 10,000 latest logs and display 1000 latest logs at most. Logs will be cleared after the device is restarted.

8.1.1 Handling Logs

You can perform the following operations on logs:

- Querying logs

  You can query logs based on conditions such as the time, action, protocol, port, and address. Query conditions vary with log types.
- Exporting logs

  After querying logs, you can export query results for further statistical analysis. On the log page, you can click , , or to save logs as an HTML, Word, or Excel file to a local disk drive.
- Clearing logs

  In the upper-right corner of the log list, you can click **Clear Log** to delete all log data. The data deleted in this way cannot be restored. Therefore, you are advised to download logs before clearing data.
- Printing logs

On the log list page, you can click to print the current logs. Make sure that the printer is properly connected before printing a report.

- Viewing Logs

  You can analyze various events based on related logs.

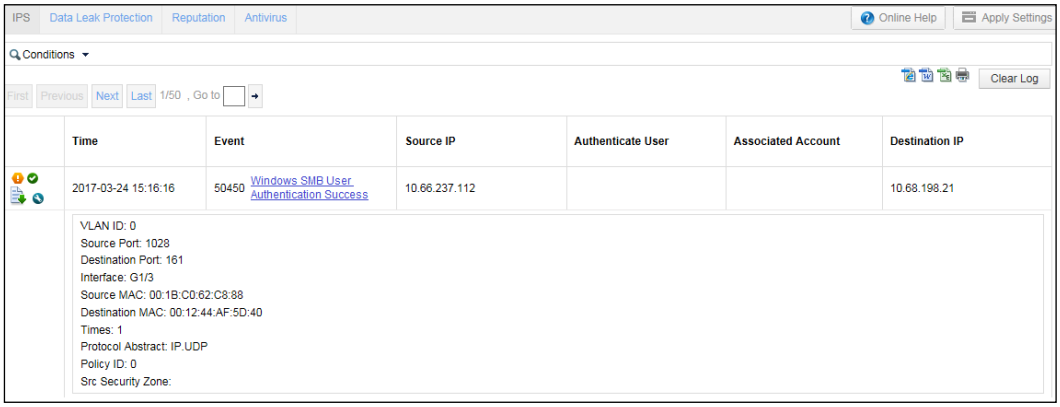
Note	• In all security logs and web behavior logs, you can view associated users (if any). For details, see Viewing Associated Users in section 3.1 Common Operations. • In all security logs and URL category logs, you can view details of public IP addresses involved. For details, see "Viewing Details of Public IP Addresses" in section 3.1 Common Operations.

8.1.2 Viewing Security Logs

8.1.2.1 Intrusion Prevention Logs

Choose **Logs and Reports** > **Security Log** > **IPS**. Set query conditions and click **Search**. Then intrusion prevention logs are displayed.

Figure 8-1 Page for querying intrusion prevention logs

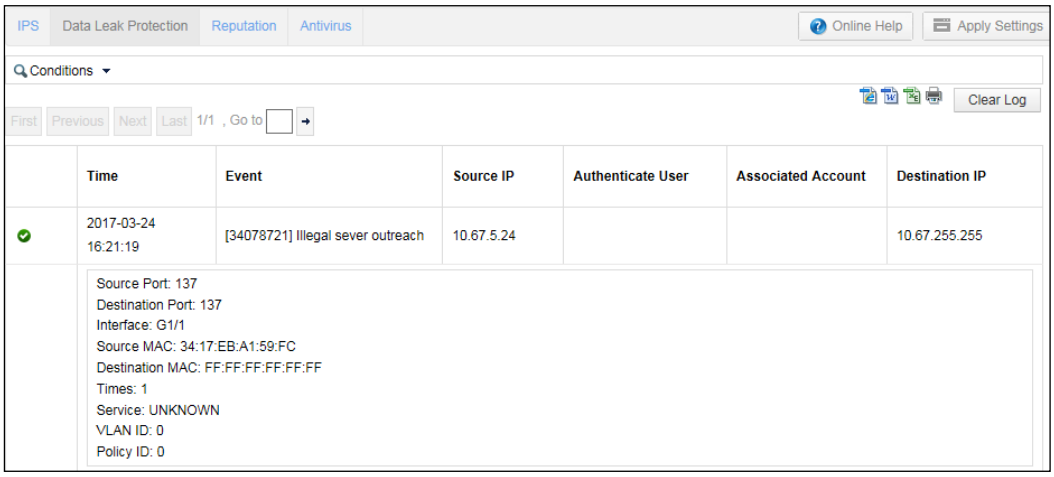


On this page, you can download PCAP files and report a false positive and view event details. For details, see section 3.3.1 List of Intrusion Prevention Events.

8.1.2.2 Data Leak Protection Logs

Choose **Logs and Reports** > **Security Log** > **Data Leak Protection**. Set query conditions and click **Search**. Then data leak protection logs are displayed.

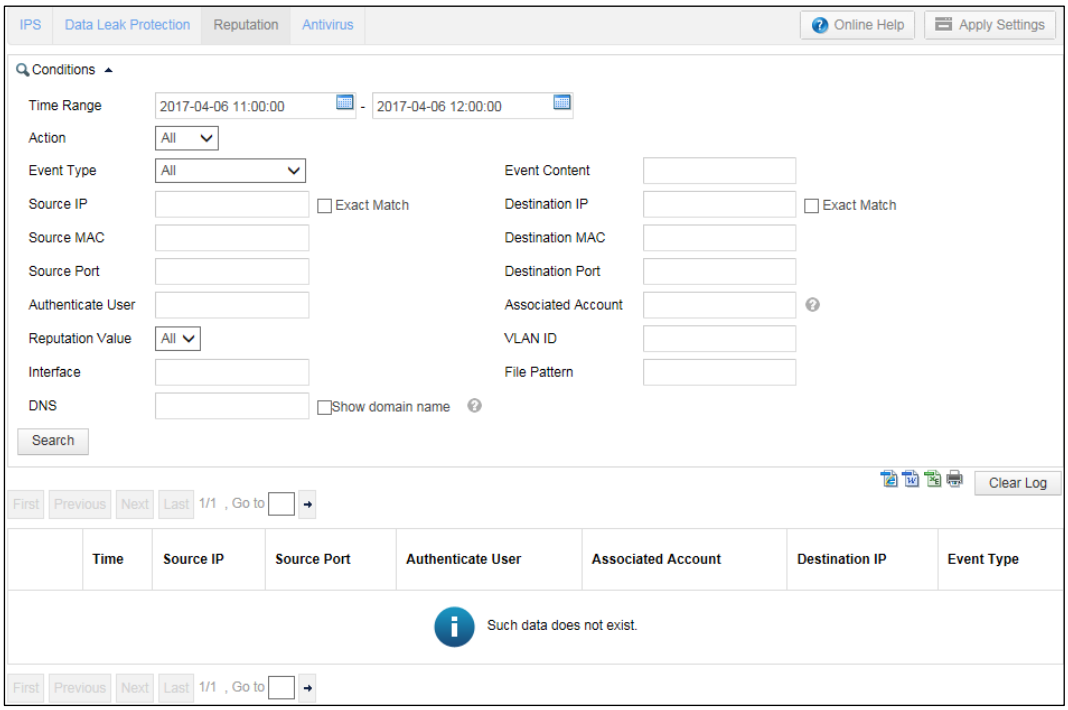
Figure 8-2 Page for querying data leak protection logs



8.1.2.3 Reputation Logs

Choose **Logs and Reports** > **Security Log** > **Reputation**. Set query conditions and click **Search**. Then reputation logs are displayed.

Figure 8-3 Page for querying reputation logs



- **Reporting a false positive**

  If you determine that a reputation event is a false positive, you can click in the leftmost column to send the information to the cloud. For details, see "Reporting a False Positive" in section 3.3.1 List of Intrusion Prevention Events.

- **Viewing a report on malicious files**

  For a reputation log with **Visit Dangerous File (Advanced Threat Protection)** shown in its **Event Type** column, you can click in the leftmost column to check the report on malicious files on the web-based manager of TAC. If the web-based manager of TAC does not open, clicking opens the TAC login page on which you can type the user name and password and then check the report. If the web-based manager of TAC opens, clicking opens the report on TAC.

- **Downloading a malicious file analysis report**

  For a reputation log with **Visit Dangerous File (Advanced Threat Protection)** in the **Event Type** column, you can click in the leftmost column to download the malicious file analysis report to a specified directory.

- Adding a file MD5 value to the file whitelist

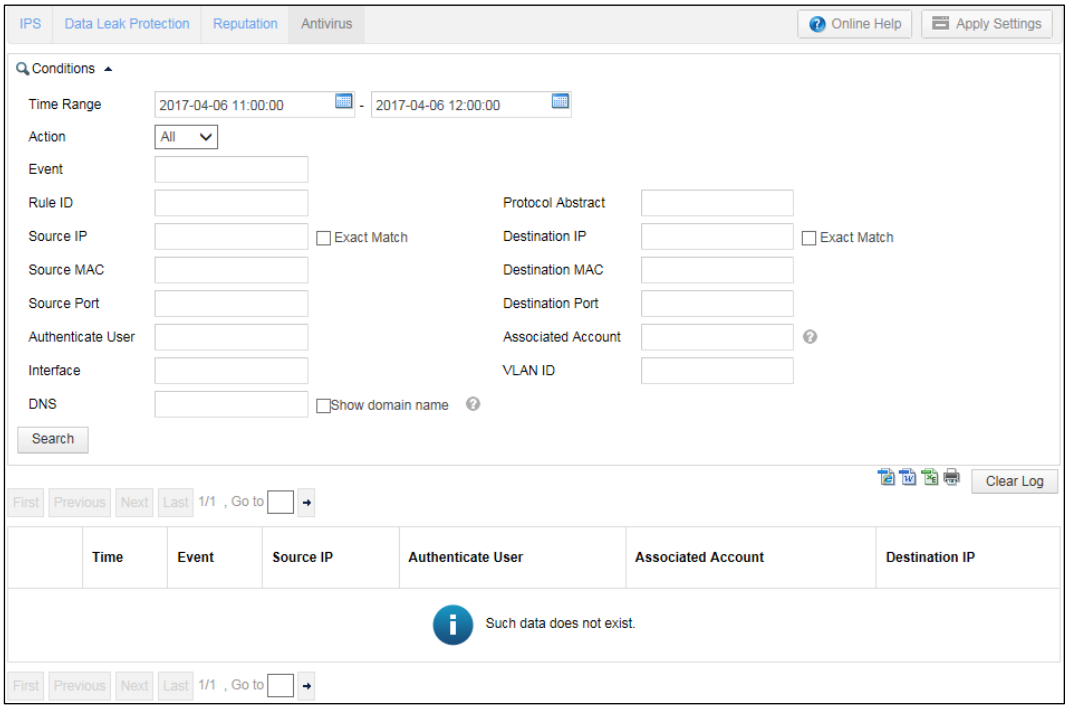
  For a reputation log with **Event Type** being **Visit Dangerous File**, you can click **Add to File Whitelist** in log details to add the MD5 value of the file in question to the file whitelist. Then this file will be free from file reputation detection. For details about the file whitelist, see Configuring the File Whitelist.

8.1.2.4 Antivirus Logs

Antivirus logs let you know the source address, destination address, and protocol abstract of virus-infected messages.

Choose **Logs and Reports** > **Security Log** > **Antivirus**. Set query conditions and click **Search**. Then antivirus logs are displayed.

Figure 8-4 Page for querying antivirus logs

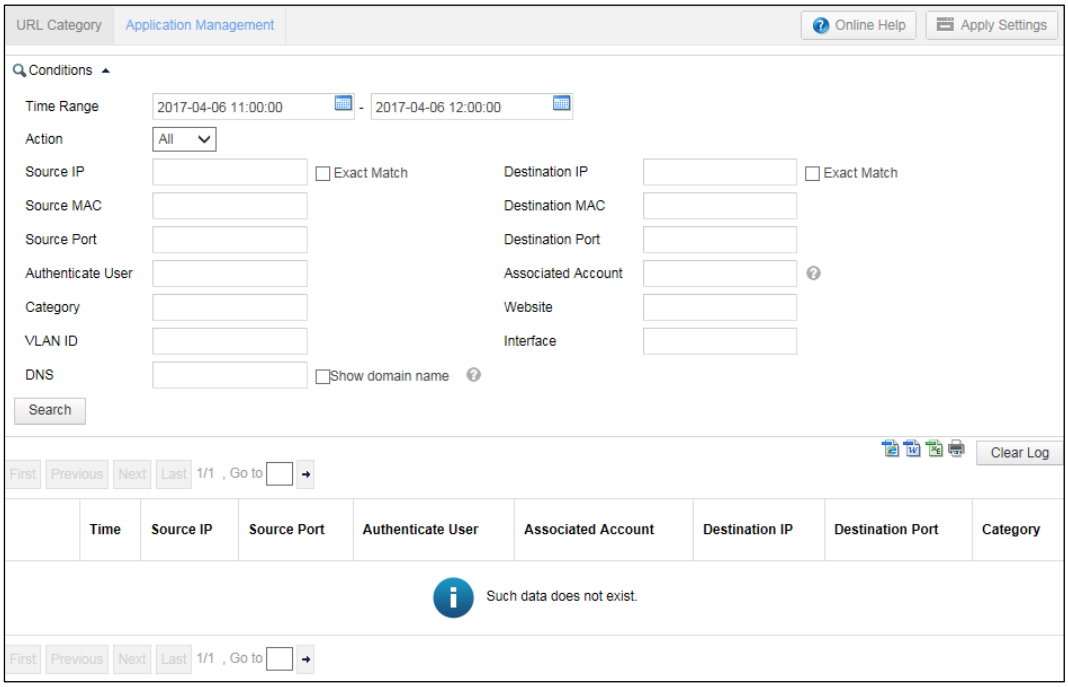


8.1.3 Viewing Web Behavior Logs

8.1.3.1 URL Category Logs

Choose **Logs and Reports** > **Web Behavior Log** > **URL Category**. Set query conditions and click **Search**. Then URL category logs are displayed.

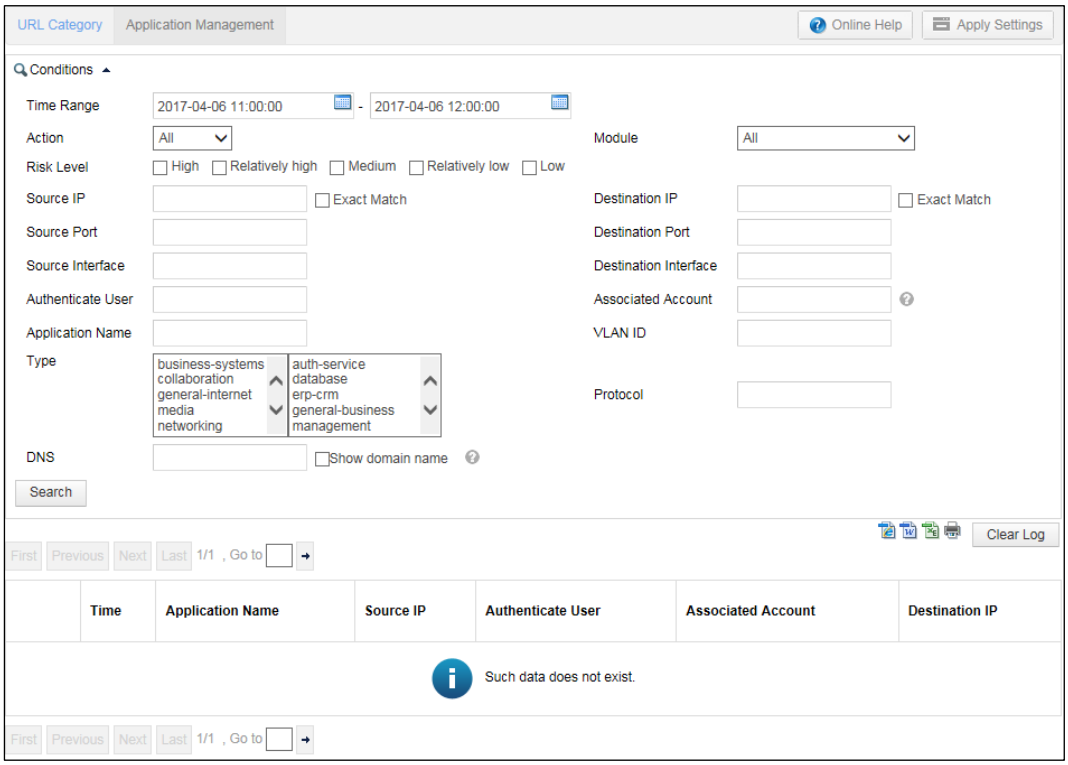
Figure 8-5 Page for querying URL category logs



8.1.3.2 Application Management Logs

Choose **Logs and Reports** > **Web Behavior Log** > **Application Management**. Set query conditions and click **Search**. Then application management logs are displayed.

Figure 8-6 Page for querying application management logs



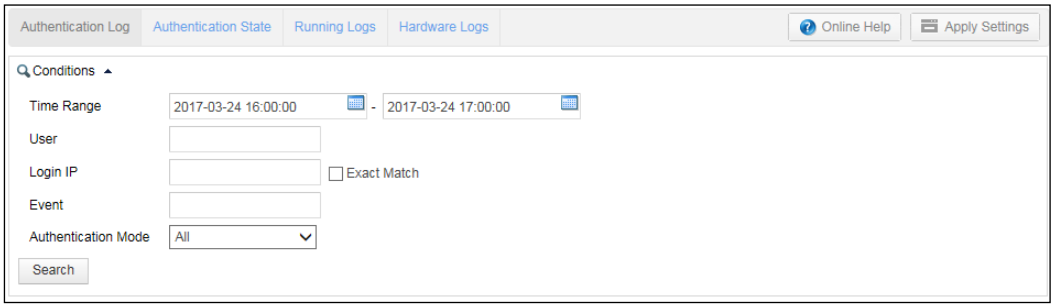
8.1.4 Viewing O&M Logs

8.1.4.1 Authentication Logs

Authentication logs help you manage authentication methods used for network communication.

Choose **Logs and Reports** > **O&M Log** > **Authentication Log**. Set query conditions and click **Search**. Then authentication logs are displayed.

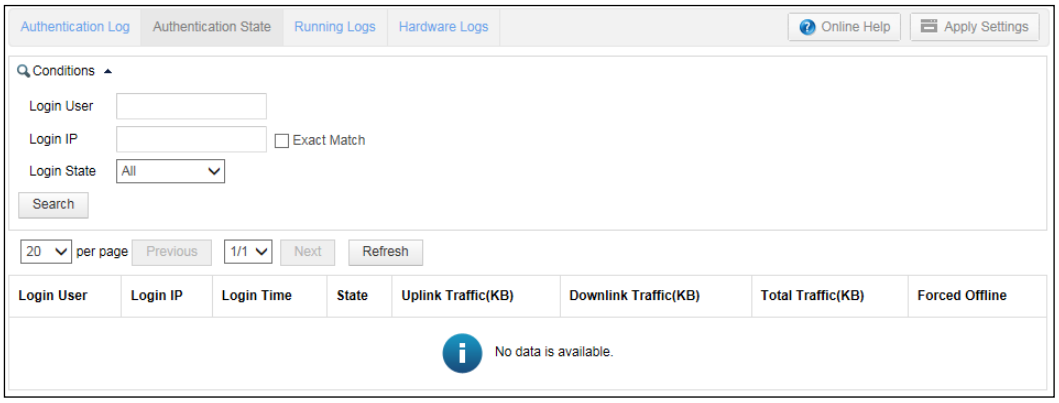
Figure 8-7 Page for querying authentication logs



8.1.4.2 Authentication State Logs

Choose **Logs and Reports** > **O&M Log** > **Authentication State**. Set query conditions and click **Search**. Then authentication state logs are displayed.

Figure 8-8 Page for querying authentication state logs

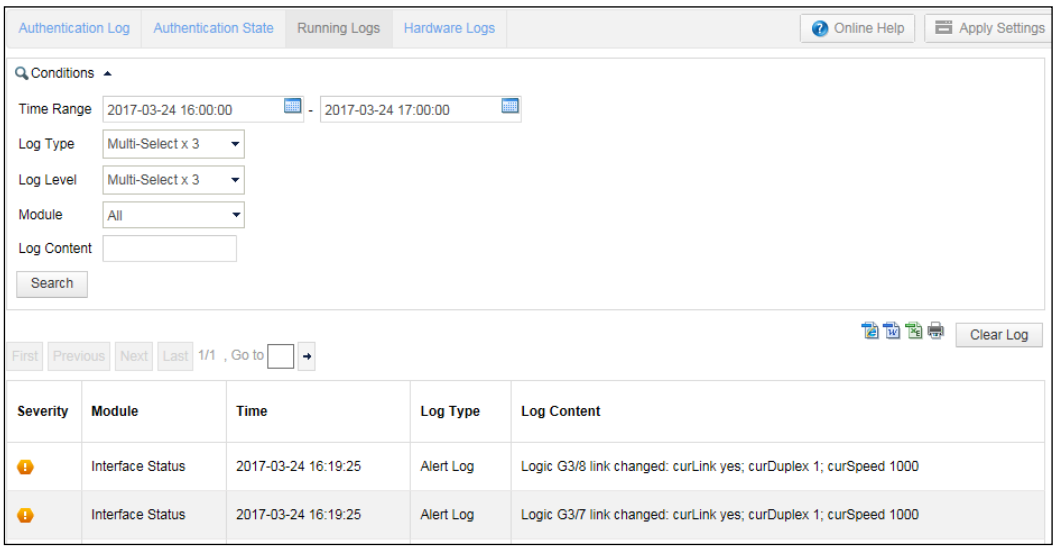


8.1.4.3 Running Logs

On the **Running Logs** page, you can view interface status logs, HA logs, system logs, and bypass logs of different types (warning, running, and debugging) at different levels (normal, warning, and critical).

Choose **Logs and Reports** > **O&M Log** > **Running Logs**. Set query conditions and click **Search**. Then running logs are displayed.

Figure 8-9 Page for querying running logs



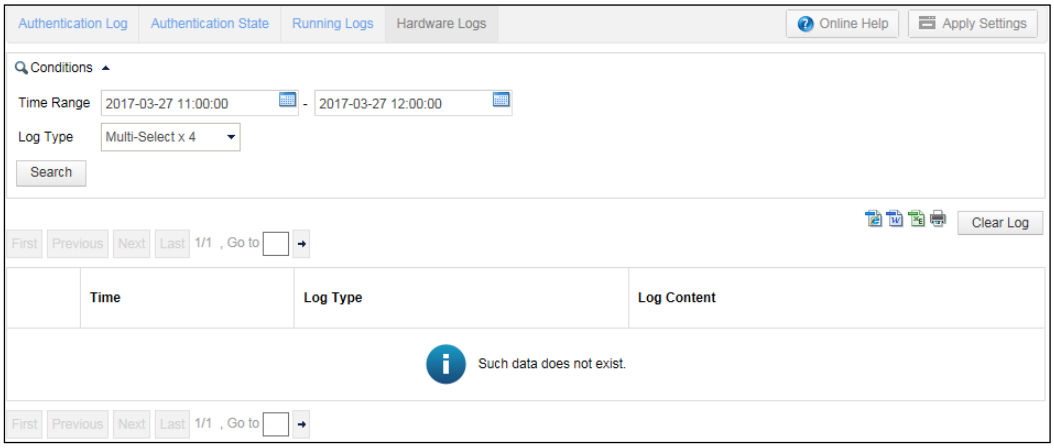
8.1.4.4 Hardware Logs

On the **Hardware Logs** page, you can view various alerts of the NIPS hardware.

Note	Alerts are logged on the **Hardware Logs** page only when the monitoring alert functions are enabled on the **Hardware Monitoring** page and device hardware such as the CPU, fan, mainboard, or power supply fails. For details on hardware alert thresholds, see section 4.3.5 Configuring Hardware Monitoring.

Choose **Logs and Reports** > **O&M Log** > **Hardware Logs**. On the page that appears, set query conditions and click **Search**. Then the desired hardware logs are displayed.

Figure 8-10 Hardware logs

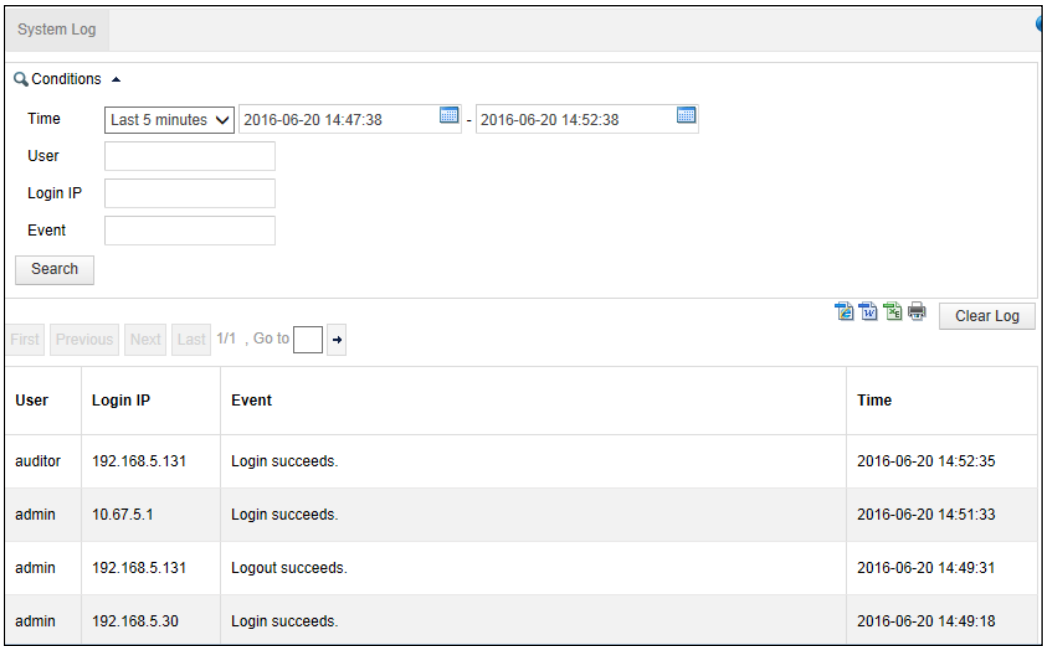


8.1.5 Viewing System Logs

Only an auditor can view system logs. System logs include login logs, system operation logs, and system startup logs. For how to enable the default auditor account, see section 4.5.1.1 Enabling the Default Auditor Account.

Choose **Log** > **System Log**. Set query conditions and click **Search**. Then system logs are displayed.

Figure 8-11 Page for querying system logs

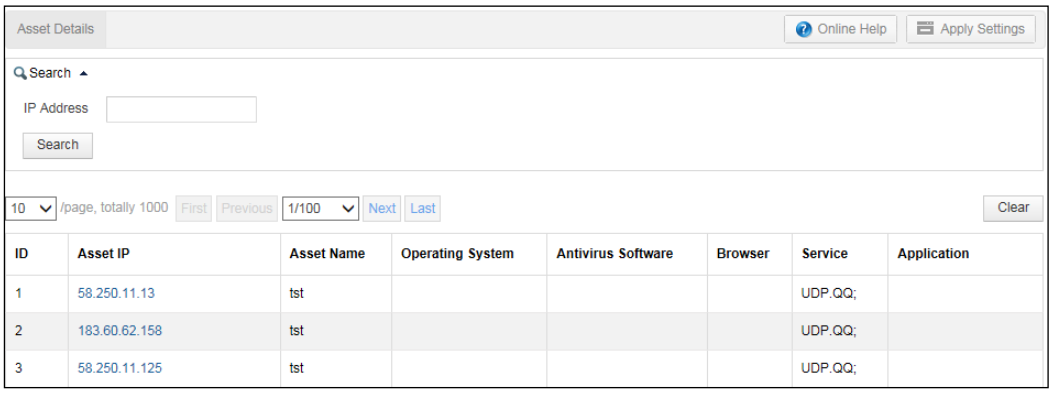


8.1.6 Viewing Asset Details

If ESPC properly collaborates with NIPS, after you configure an asset identification policy and enable asset identification on ESPC, ESPC dispatches this policy to managed devices. After receiving the policy, NIPS automatically turns on asset identification. When traffic passes through NIPS, NIPS identifies the assets within the configured asset scope and generates related logs. Asset details are logs related to each asset, including such information as the operating system, browser, antivirus software, and open services and applications.

Step 1 Choose **Logs and Reports** > **Asset Details**.

Figure 8-12 Page for querying asset details

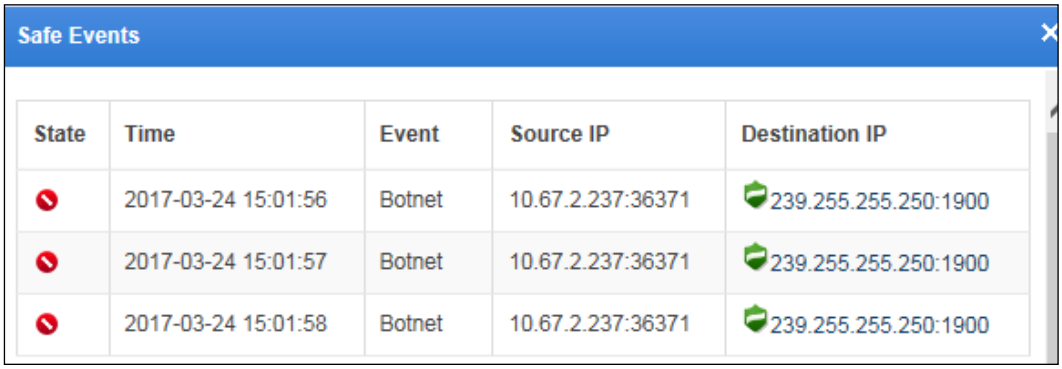


Step 2 Type an IP address and click **Search**.

Then asset identification logs are displayed.

Step 3 Click the IP address to display security events associated with this IP address.

Figure 8-13 Query result



Safe Events

State	Time	Event	Source IP	Destination IP
	2017-03-24 15:01:56	Botnet	10.67.2.237:36371	239.255.255.250:1900
	2017-03-24 15:01:57	Botnet	10.67.2.237:36371	239.255.255.250:1900
	2017-03-24 15:01:58	Botnet	10.67.2.237:36371	239.255.255.250:1900

----End

You can click Clear to the upper right of the asset table to empty the table.

8.1.7 Log Configuration

The administrator can save and back up NIPS logs.

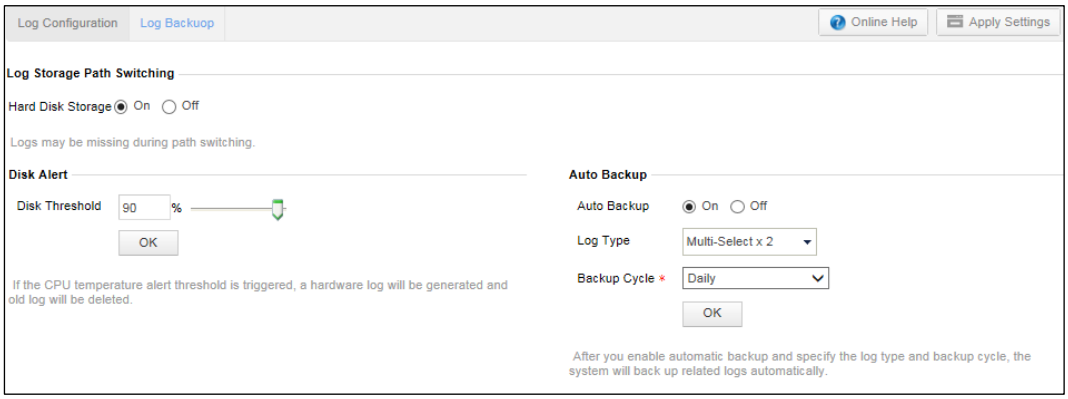
Note	The **Log Configuration** page is available only when NIPS has a hard disk.

8.1.7.1 Log Configuration

The **Log Configuration** page contains three areas: **Log Storage Path Switching** area, **Disk Alert** area, and **Auto Backup** area.

Step 1 Choose **Logs and Reports** > **Log Configuration** > **Log Configuration**.

Figure 8-14 Log Configuration page



Step 2 Configure parameters in the **Log Storage Path Switching**, **Disk Alert**, and **Auto Backup** areas.

- **Log Storage Path Switching** area

  Enable or disable the hard disk storage function. After **Hard Disk** Storage is set to **On**, logs will be saved in the hard disk.

Note	Logs may be lost during log storage path switching. Therefore, perform this operation with caution.

- **Disk Alert** area

  Set **Disk Threshold**. If the specified threshold is exceeded, a hardware log will be generated and old logs will be deleted.

- **Auto Backup** area

  Enable or disable the auto backup function. After **Auto Backup** is set to **On**, you need to configure **Log Type** and **Backup Cycle**.

  – If you select **Daily** for **Backup Cycle**, the system backs up logs at 00:00 every day.

  – If you select **Weekly** for **Backup Cycle**, the system backs up logs at 00:00 on a specified day every week.

  – If you select **Monthly** for **Backup Cycle**, the system backs up logs at 00:00 on a specified day every month.

  You can view logs that are backed up under **Logs and Reports** > **Log Configuration** > **Log Backup**.

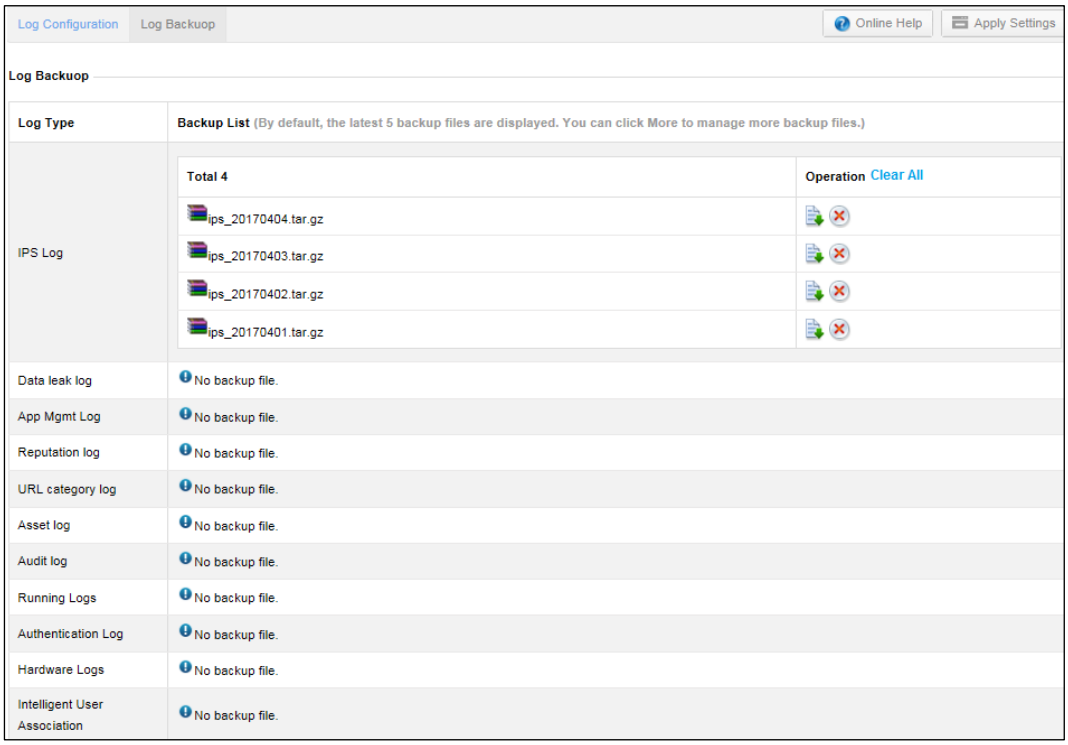
----End

8.1.7.2 Log Backup

You can view logs that the system backs up as configured.

Step 1 Choose **Logs and Reports** > **Log Configuration** > **Log Backup**.

Figure 8-15 Log Backup page



Step 2 Click in the **Operation** column of a log to download this log to a local disk drive.

Step 3 (Optional) Click in the **Operation** column of a log to delete this log. Alternatively, click **Clear All** to delete logs of all types.

----End

8.2 Reports

This section covers the following topics:

- Handling Reports
- Report Details

8.2.1 Handling Reports

You can perform the following operations on reports:

- Querying a report

  You can query a report based on conditions such as the report type (daily, weekly, monthly, or annual) and interface name.

- Exporting a report

  After querying a report, you can export query results for further statistical analysis. On the report page, you can click , , or to save the report as an HTML, Word, or Excel file to a local disk drive.

- Printing a report

  On the report page, you can click to print the current report. Make sure that the printer is properly connected before printing a report.

8.2.2 Report Details

On the page of each report type, you can query the related report based on query conditions. Table 8-1 describes these reports.

Table 8-1 Contents of different types of reports

Type	Content
Intrusion prevention report	Contains top 10 source and destination addresses involved in all intrusion events and those involved in blocked events, top 10 intrusion events, and top 10 blocked events.
Data leak protection report	Contains the overview of all advanced threats, top 10 source and destination IP addresses involved in sever exception events, distribution of sensitive data events, top 10 source and destination IP addresses involved in sensitive data events and those involved in blocked events, distribution of file type events in file identification, top 10 source and destination IP addresses involved in file identification and those involved in blocked events.
Application management report	Contains top 10 source and destination IP addresses, top 10 users, and top 10 applications involved in all application management events and those involved in blocked events.
Reputation report	Contains the following information: • Reputation overview: presents the number and percentage of each type of events and actions taken upon these events. • Malicious website: presents top 10 source IP addresses, top 10 domain names, and top 10 websites (in terms of user visits) involved in all events and those involved in blocked events. • Botnet: presents top 10 source IP addresses, top 10 botnet servers, and top 10 websites involved in all events and those involved in blocked events. • Dangerous file: presents top 10 source IP addresses, top 10 dangerous file names, and top 10 websites (in terms of user visits) involved in all events and those involved in blocked events.
URL category report	Contains top 10 source and destination IP addresses, top 10 URL categories, and top 10 websites involved in all events and those involved in blocked events.
Antivirus report	Presents top 10 source and destination addresses (all events and blocked events respectively), and top 10 viruses.

9 Console-based Management

Via the console port, the console administrator (**conadmin**) can access the console user interface of NIPS and perform basic operations, such as initial system configurations, status detection, and restoration of initial configurations. When failing to log in to the web-based manager or perform certain management via the web-based manager, you can manage NIPS via the console.

This chapter contains the following sections:

Section	Description
Viewing System Information	Describes how to view system software, hardware, and other basic information.
Using Diagnostic Tools	Describes how to use network diagnostic tools in the console user interface.
Using Maintenance Tools	Describes how to maintain the system via the console port.
Initializing System Settings	Describes how to restore factory defaults.
Restarting the System	Describes how to restart system hardware.
Shutting Down the System	Describes how to shut down system hardware.
Exiting the Configuration Interface	Describes how to exit the console user interface.

9.1 Viewing System Information

As shown in Figure 9-1, the console user interface allows you to perform the following operations as a console administrator:

- Viewing interface configuration

  Views information about all network interfaces of the system, including interface names, IP addresses, management IP addresses, and security zones to which the interfaces belong. (The settings of network interfaces can be modified only on the web-based manager. For details, see section Manageable attribute configuration.)
- Viewing license information

  You can view the engine license of NIPS, including the license status, license type, date of issuance, and expiry date.
- Setting interface IP addresses

You can configure the IP address for management interface M or H1 so that you can log in to the web-based manager for device management.

- Setting the interface gateway

  You can set the IP address of the next-hop device.

- Restarting key processes

  You can start key processes to enable the device to work properly.

- Setting the system clock

  You can set the system clock for use in communication and logging.

- Setting the time zone

  You can set the time zone for the system when the engine is located in other time zones than the default one (**UTC+8**, which can be changed in the range of –12 to +12).

- Setting the timeout

  You can set the timeout period. After login to the console user interface, if you remain inactive until the specified timeout expires, the system logs you out automatically by taking you to the login page.

- Viewing the hardware ID

  You can view the hardware ID, which is a unique ID of each engine required for producing the related license.

- Viewing the product status value

  The product status value is provided for engineering personnel of NSFOCUS for internal use. It changes on a daily basis.

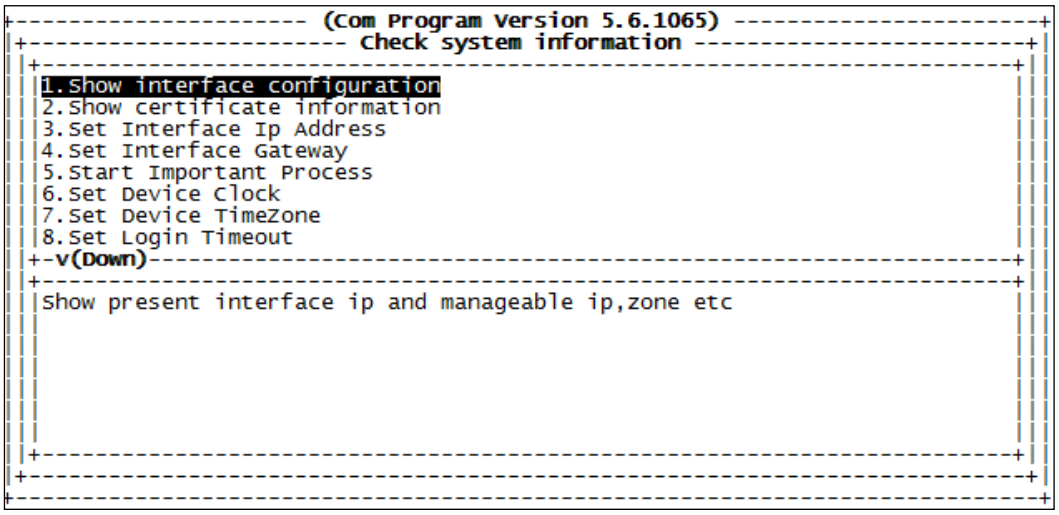
- Viewing version information

  You can view information about the current engine and firmware versions.

- Returning to the previous menu

  After performing the desired operations, you can return to the previous menu.

Figure 9-1 Viewing system information



Note	No license is available on NIPS when it leaves the factory. You can import the related license via the web-based manager. For how to import the license, see section 4.7.2 Importing the License.

9.2 Using Diagnostic Tools

As shown in Figure 9-2, the console user interface provides some diagnostic tools under UNIX. You can use them to check the network status and solve problems in system installation.

You can perform the following operations:

- Pinging destination IP addresses

  You can check whether a destination IP address is reachable over the network using the ping command.
- Tracing routes

  You can view the status of the route between the engine and the specified IP address.
- Checking network status

  You can view the current network connectivity of the engine.
- Viewing route information

  You can view the current routing table on the engine.
- Viewing NIC information

  You can view the NIC information of the engine.
- Returning to the previous menu

  After performing the desired operations, you can return to the previous menu.

Figure 9-2 Diagnostic tools

```
+---------------------------- Diagnostic Tools ----------------------------+
|+-------------------------------------------------------------------------+|
||1.Ping                                                                   ||
||2.Trace route                                                            ||
||3.Network Status                                                         ||
||4.show route information                                                 ||
||5.network interface card information                                      ||
||0.Exit to previous menu                                                  ||
||                                                                         ||
||                                                                         ||
|+-------------------------------------------------------------------------+|
|+-------------------------------------------------------------------------+|
||Check network communication status with specified IP address host.       ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
||                                                                         ||
|+-------------------------------------------------------------------------+|
+-----------------------------------------------------------------------------+
```

Note	You can also use these diagnostic tools on the web-based manager of NIPS. For details, see section 4.6 Diagnosis Tools.

9.3 Using Maintenance Tools

As shown in Figure 9-3, the **Maintenance Tools** menu allows you to perform the following operations:

- Setting the administrator password

  You can set a password for the **conadmin** account. You must keep this password in mind; otherwise, you cannot configure the system via the console port and must contact technical support engineers of NSFOCUS for password resetting.

- Setting the password for the CLI administrator

  You can set a password for the **shell** account for login to the command-line interface (CLI). You must keep this password in mind; otherwise, you cannot configure dynamic routes via the CLI and must contact technical support engineers of NSFOCUS for password resetting.

- Resetting web users

  You can reset system administrators that have been configured on the web-based manager. In this way, the passwords for the two default administrator accounts (**admin** and **auditor**) will be reset and all information of custom administrators will be deleted.

- Clearing temporary files

  You can clear temporary files generated during engine running. Generally, you are not advised to do so. After temporary files are cleared, if the web-based manager cannot work properly or other exceptions occur, you must restart the NIPS system.

- Disabling/Enabling remote assistance

  By default, remote assistance is disabled. You can enable it by pressing **Enter**. If you want to disable it, press **Enter** again.

- Disabling/Enabling ping (ICMP)

  By default, ping (ICMP) is enabled. You can disable it by pressing **Enter**. If you want to enable it, press **Enter** again.

- Disabling forced hardware bypass

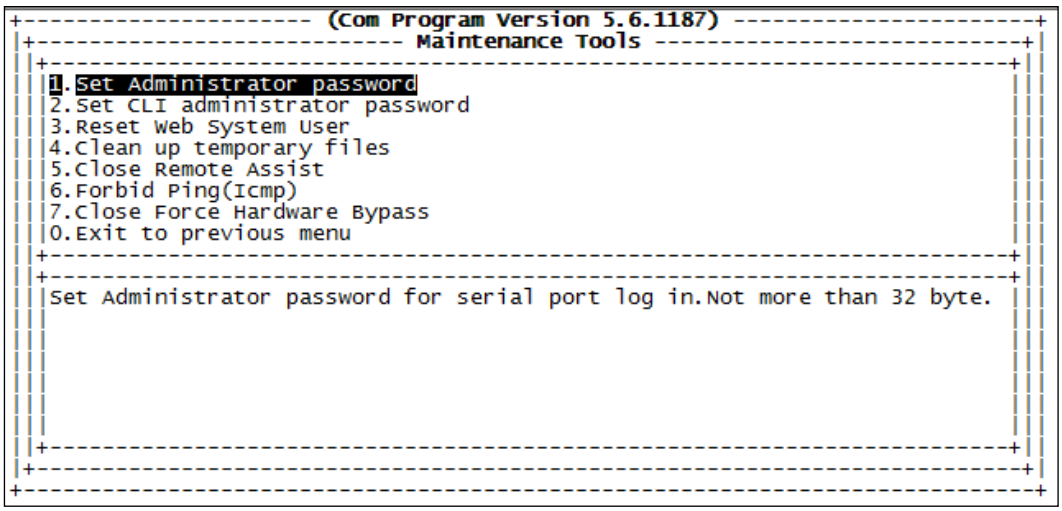
  You can disable mandatory hardware bypass (the setting takes effect after system restart) only for NIPS devices that are powered on. After disabling this function, you must save the current settings. You cannot enable mandatory hardware bypass again after disabling it.

Note	• This setting takes effect only for NIPS devices that are powered on. If an NIPS device is powered off, your operation of disabling its mandatory hardware bypass function will not work. • To disable the mandatory hardware bypass function of an NIPS device that is powered off, you must perform the operation in BIOS mode.

- Returning to the previous menu.

After performing the desired operations, you can return to the previous menu.

Figure 9-3 Maintenance tools



9.4 Initializing System Settings

As shown in Figure 9-4, the **System Initialization** interface allows you to restore all program files or data, including passwords and settings, to their initial state. You can perform the following operations:

- Initializing settings

  You can initialize all settings (except the system clock and object configuration files) to factory defaults. This operation will delete the hardware license. Before initialization, make sure that a duplicate of the license has been saved. After initialization, you must restart the browser.
- Restoring the system

  Restoring the system will restore all programs and settings to their factory defaults.
- Formatting the hard disk

  Formatting the hard disk will clear all data on the hard disk.
- Returning to the previous menu

  After performing the desired operations, you can return to the previous menu.

Figure 9-4 System initialization

```
+---------------------- (Com Program Version 5.6.1065) ----------------------+
|+-------------------------- System initialization --------------------------+|
||+-----------------------------------------------------------------------+||
|||1.ReInit Config                                                         |||
|||2.Restore System                                                        |||
|||3.Format Disk of Data Partition                                         |||
|||4.Format Disk of Backup Partition                                       |||
|||0.Exit to previous menu                                                 |||
|||                                                                        |||
|||                                                                        |||
||+-----------------------------------------------------------------------+||
||+-----------------------------------------------------------------------+||
|||ReInit Config, All Config Paramater will be set to factory version.     |||
|||System time will not change                                             |||
|||CERTIFICATE WILL BE DELETED!                                            |||
|||Please backup your certificate before this operation!                   |||
|||Please restart your browser after configuration restored                |||
|||                                                                        |||
|||                                                                        |||
||+-----------------------------------------------------------------------+||
|+-------------------------------------------------------------------------+|
+-----------------------------------------------------------------------------+
```

Note	After initializing settings, you must restart the system to make the settings take effect.

9.5 Restarting the System

After you select **5**, a message is displayed. If you select **Yes**, the NIPS system is restarted; if you select **No**, you return to the current menu.

Figure 9-5 Restarting the system

```
+---------------------- (Com Program Version 5.6.1187) ----------------------+
|+-----------------------------------------------------------------------+|
||1.Check system information                                              ||
||2.Diagnostic Tools                                                      ||
||3.Maintenance Tools                                                     ||
||4.System initialization                                                 ||
||5.Restart the system                                                    ||
||6.Shutdown the system                                                   ||
||0.Exit                                                                  ||
||              +-------------------- Reboot --------------------+        ||
||              |Are you sure REBOOT system?                     |        ||
||              +------------------------------------------------+        ||
|+-------------|              < Yes >       < No >               |-------------+|
|+-------------+------------------------------------------------+-------------+|
||Restart hardware system                                                 ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
|+-----------------------------------------------------------------------+|
+-------------------------------------------------------------------------+
```

9.6 Shutting Down the System

After you select **6**, a message is displayed. If you select **Yes**, the NIPS system is shut down without being powered off; if you select **No**, you return to the current menu.

Figure 9-6 Shutting down the system

```
+---------------------- (Com Program Version 5.6.1187) ----------------------+
|+-----------------------------------------------------------------------+|
||1.Check system information                                              ||
||2.Diagnostic Tools                                                      ||
||3.Maintenance Tools                                                     ||
||4.System initialization                                                 ||
||5.Restart the system                                                    ||
||6.Shutdown the system                                                   ||
||0.Exit                                                                  ||
||              +-------------------- Shutdown --------------------+      ||
||              |Are you sure SHUTDOWN system?                   |        ||
||              +------------------------------------------------+        ||
|+-------------|              < Yes >       < No >               |-------------+|
|+-------------+------------------------------------------------+-------------+|
||Shutdown hardware system                                                ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
|+-----------------------------------------------------------------------+|
+-------------------------------------------------------------------------+
```

9.7 Exiting the Configuration Interface

After completing all settings, you can point to **0** and press **Enter** to exit the configuration interface of NIPS.

Figure 9-7 Exiting the system

```
+---------------------- (Com Program Version 5.6.1187) ----------------------+
|+-----------------------------------------------------------------------+|
||1.Check system information                                              ||
||2.Diagnostic Tools                                                      ||
||3.Maintenance Tools                                                     ||
||4.System initialization                                                 ||
||5.Restart the system                                                    ||
||6.Shutdown the system                                                   ||
||0.Exit                                                                  ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
|+-----------------------------------------------------------------------+|
|+-----------------------------------------------------------------------+|
||Exit this menu and logout                                               ||
||The system will inquire if you will save it and put it in operation    ||
||If save needed and you are using remote asist,Please reboot system.     ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
||                                                                        ||
|+-----------------------------------------------------------------------+|
+-------------------------------------------------------------------------+
```

After you exit the console user interface, the configuration interface automatically logs you out, saves all settings, and makes them take effect. To modify the settings, you need to log in to the console user interface again.

A Acronyms and Abbreviations

Acronym/Abbreviation	Full Spelling
ARP	Address Resolution Protocol
CSRF	Cross-site Request Forgery
CGI	Common Gateway Interface
CSS/XSS	Cross Site Scripting
DDoS	Distributed Denial of Service
DNS	Domain Name System
HA	High Availability
HTTP	Hyper Text Transfer Protocol
IDC	Internet Data Center
IP	Internet Protocol
MAC	Media Access Control
NIPS	Network Intrusion Prevention System
ESPC	Enterprise Security Planning Customer
SSL	Secure Sockets Layer
SQL	Structured Query Language
URL	Uniform Resource Locator

B AD Domain Configurator Management

If the AD domain server is configured on NIPS and the AD domain configurator (that is, user management configuration tool) is installed and properly configured on the AD domain server or the ESPC host, NIPS can obtain information about logged-in users in the AD domain via the AD domain configurator.

B. 1 Installing the AD Domain Configurator

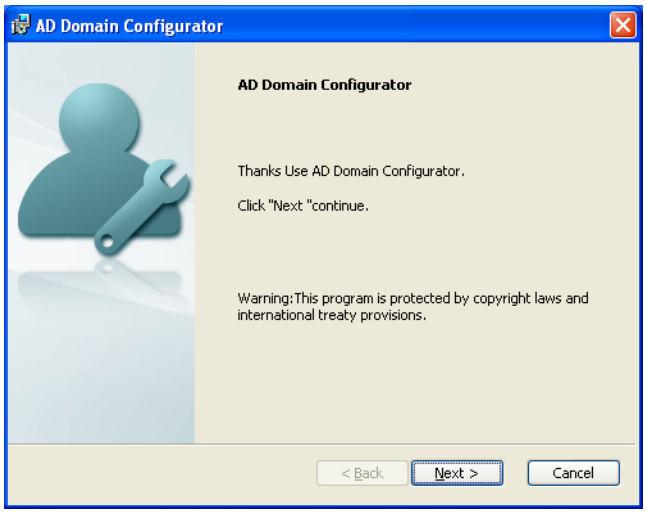
Before installing the AD domain configurator, make the following preparations:

- Prepare an AD domain member PC or server.
- Create a user on the AD domain server and assign log access permissions to this user. Create a user on the AD domain server and assign log access permissions to this user.
- Contact technical support engineers of NSFOCUS to obtain the software. To get the license file, please contact technical support engineers of NSFOCUS.

To install an AD domain configurator, follow these steps:

Step 1 Double-click **setup.exe** to start the installation wizard, as shown in Figure B-1.

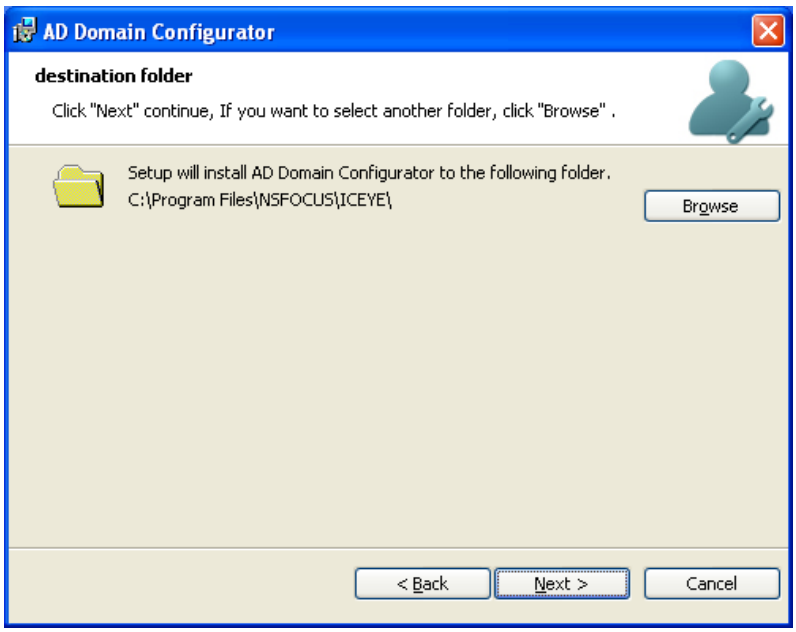
Figure B-1 Starting the installation wizard



Step 4 Click **Next** and select an installation path.

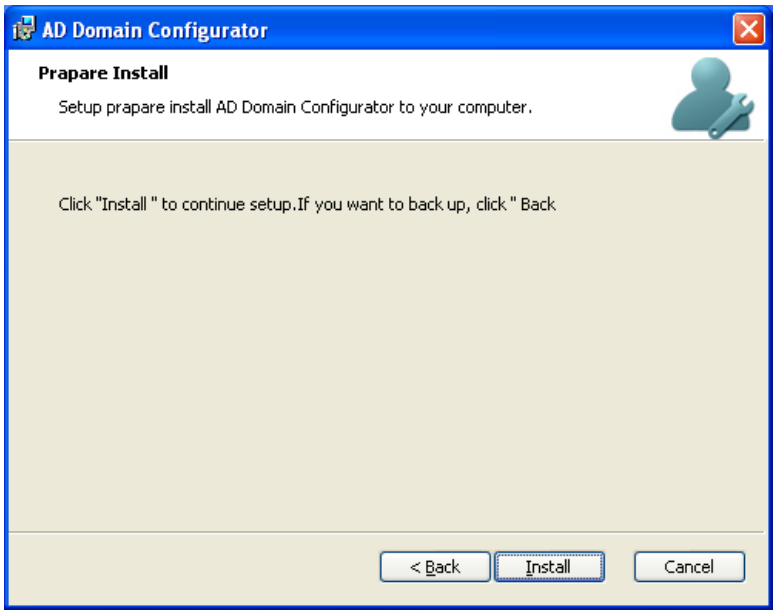
Figure B-2 shows that a default installation path is selected.

Figure B-2 Selecting an installation path



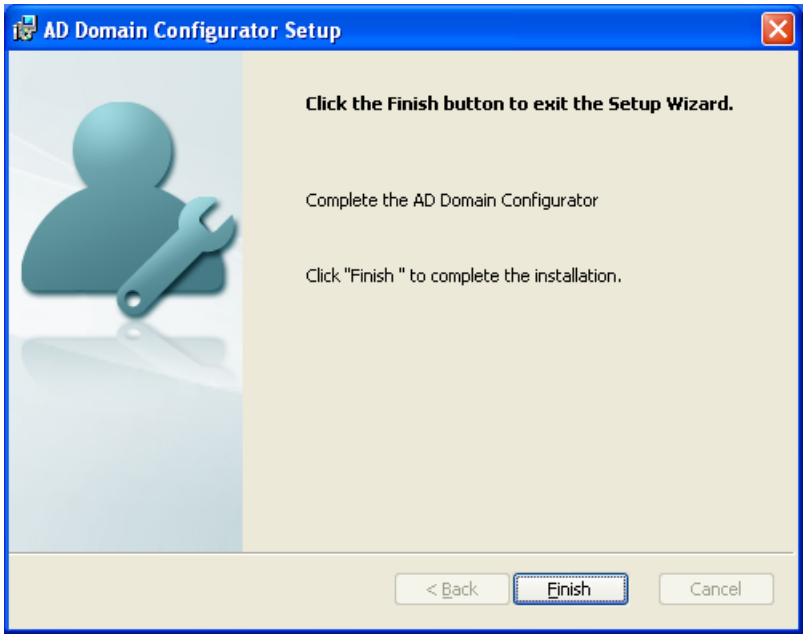
Step 5 Click **Next** to install the software. In the dialog box shown in Figure B-3, click **Install**.

Figure B-3 Starting installation



Step 6 After the installation is complete, click **Finish**.

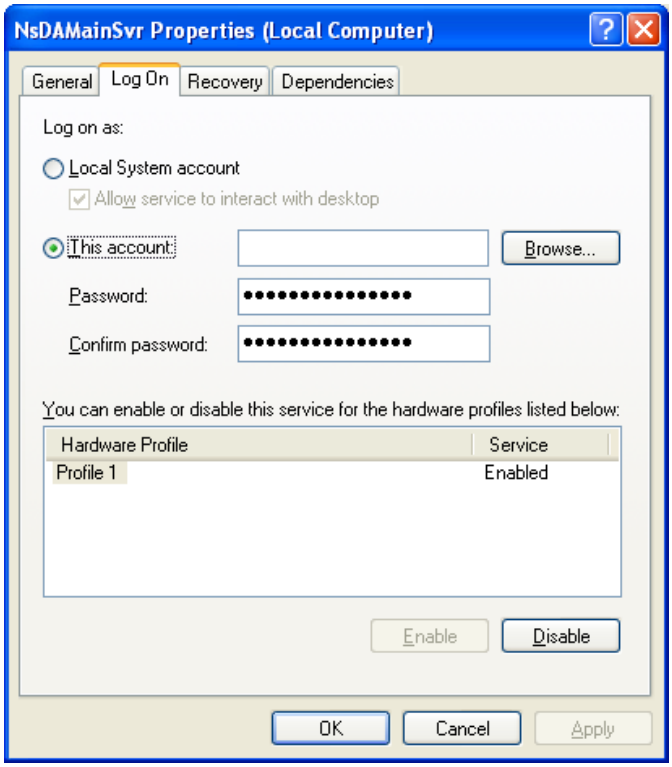
Figure B-4 Completing installation



a. After installing the AD domain configurator, configure the NsDomainSvr service. Choose **Control Panel > Performance and Maintenance > Administrative Tools > Services**.

b. Configure an account created before installing the AD domain configurator as the account for initiating the NsDomainSvr service.

Figure B-5 Configuring the NsDomainSvr service



----End

B. 2 Configuring the AD Domain Configurator

An AD domain configurator can work as either of the following:

- Scanner

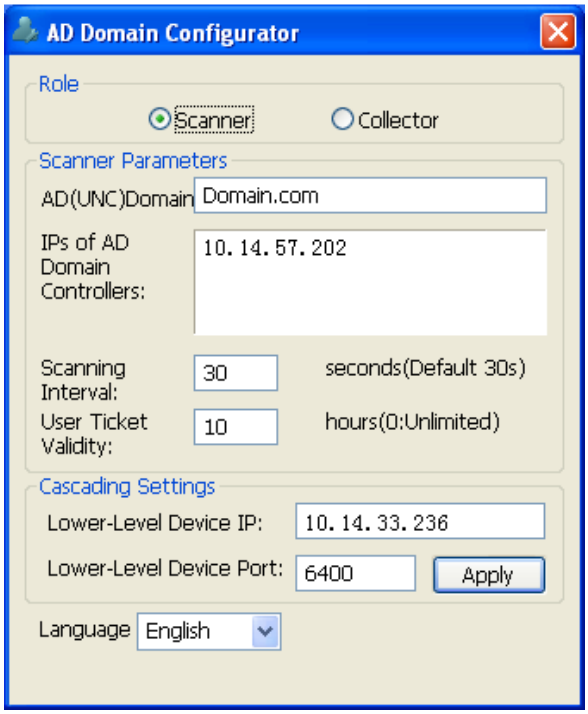
  A scanner regularly scans the list of logged-in users from security logs recorded on the AD domain server within a specified period and then sends the obtained user list to the NIPS using the specified method. If scanners are multiplexed, these scanners can also send collected logs to the specified collector.

- Collector

  A collector regularly combines and filters user lists received from the scanner and sends them to NIPS.

Step 2 After the AD domain configurator is successfully installed and configured, double-click the shortcut icon on the desktop to open the login dialog box.

Figure B-6 Configuring the AD domain configurator



Step 7 Configure parameters in the **New** dialog box.

Table B-1 Parameters for configuring the AD domain configurator

Parameter	Description
AD(UNC)Domain	Domain name of the AD server.
IPs of AD Domain Controllers	Specifies the list of IP addresses to be scanned, with one address in each line. This parameter is valid only when the AD domain configurator works as a scanner. Multiple IP addresses should be separated by carriage returns, with one in each line.
Scanning Interval	Specifies the interval for scanning or collecting information about

Parameter	Description
	logged-in users.
User Ticket Validity	Specifies the validity period of user authentication. The default value is **10** hours.
Lowe-Level Device IP	Specifies the IP addresses of NIPS devices, with each in a separate line. Multiple IP addresses should be separated by carriage returns, with one in each line.
Lower-Level Device Port	Specifies the communication port of NIPS. The default value is **6400**.

----End

C Default Parameters

C. 1 Default Interface Settings

IP Address	• M: 192.168.1.1 • H1: 192.168.2.1 (whether interface H1 exists depends on the hardware platform) • G1/1: 0.0.0.0 • G1/2: 0.0.0.0 • … (For working interfaces not for management purposes, their initial IP addresses are all 0.0.0.0.)
Subnet Mask	255.255.255.0

C. 2 Default Administrators

	Web Operator	Web Auditor	Web Maintainer	Console Administrator	ESPC Administrator
User Name	admin	auditor	supervisor	conadmin	admin
Password		No default password (the password is set when **admin** enables this account)			

C. 3 Communication Parameters of the Console Port

Baud Rate	115200
Data Bits	8

C. 4 Default CLI Administrator Account

User Name	shell
Password	