NSFOCUS NIPS
User Guide

Version: V5.6R11F00SP04 (2022-02-28)

Confidentiality: RESTRICTED

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 Dashboard	Describes information that you can obtain from the Dashboard module.
3 Alert	Describes how to view alert events.
4 Traffic	Describes how to configure bandwidth management policies or traffic analysis policies.
5 Log	Describes how and what to view about various logs and reports.
6 Policies	Describes how to configure protection policies.
7 Objects	Describes how to configure objects.
8 Network	Describes configurations related to network connections.
9 System	Describes common operations and methods for system maintenance.
10 Audit Log	Describes how to view the audit logs.

Chapter	Description
A Console-based Management	Describes how to log in to and manage NIPS via the console user interface.
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

Hardware and Software Support

Email: support@nsfocusglobal.com

Cloud Mitigation Support

Email: cloud-support@nsfocusglobal.com

Phone:

- USA: +1-844-673-6287 or +1-844-NSFOCUS
- UK: +44 808 164 0673 or +44 808 164 0NSF
- Australia: +61 2 8599 0673 or +61 2 8599 0NSF
- Netherlands: +31 85 208 2673 or +31 85 208 2NSF

- Brazil: +55 13 4042 1673 or +55 13 4042 1NSF
- Japan: +81 3-4510-8673 or +81 3-4510-8NSF
- Singapore: +65 3158 3757
- Hong Kong: +852 5803 2673 or +852 5803 2NSF
- Middle East: +973 1619 7607

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. This type of products fill in the gaps of traditional firewalls and intrusion detection productions and provide dynamic, in-depth, and proactive security protection, offering a new intrusion prevention solution for enterprises.

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

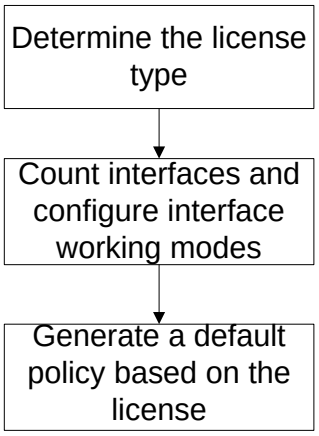
1.1 Product Characteristics

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 profiles. Based on the imported license, NIPS can automatically configure interfaces, select an appropriate profile, 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.

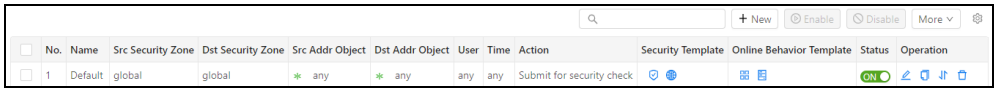
Figure 1-1 Go-live procedure of NIPS



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 in which **Src Addr Object**, **Dst Addr Object**, **User**, and **Time** all set to **any**, rule profile set to **default**, and web security profile set to **Web security – injection attack protection profile**. By default, this policy is enabled, 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 Major 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 to damage and 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 download, online games, online videos, and network streaming media.

- 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 IE and Firefox 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 Web Users

The web-based manager of NIPS has two types of user: operator and auditor. The **admin** operator and **auditor** auditor are default accounts. The **admin** operator has privileges of managing and configuring administrators and their privileges (see Roles for details). Table 1-1 describes privileges of operators and auditors.

Table 1-1 Privileges of operators and auditors

User		Privilege
Operator	**admin** (default)	Has all permissions except managing auditors (but can enable the default auditor account **auditor**) and viewing system logs.

User		Privilege
	New operator (read/write) (Created by **admin**)	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 password of his or her own account and viewing system logs.

1.3.1.2 Login to the Web-based Manager

By default, NIPS is accessed via HTTPS port 443. You can change the HTTPS port on the **Engine Configuration** page under **System > System Setting**.

Note	• Before login, check whether the options of blocking pop-ups and disabling JavaScript are selected in the browser. If yes, cancel the selections. • You are advised to use IE 11.0, Firefox 76.0, Chrome 83.0, or Edge 84.0, or later browser and set the browser resolution to 1024x768 or higher.

This section uses a Chrome browser as an example to describe how to log in to the web-based manager of NIPS.

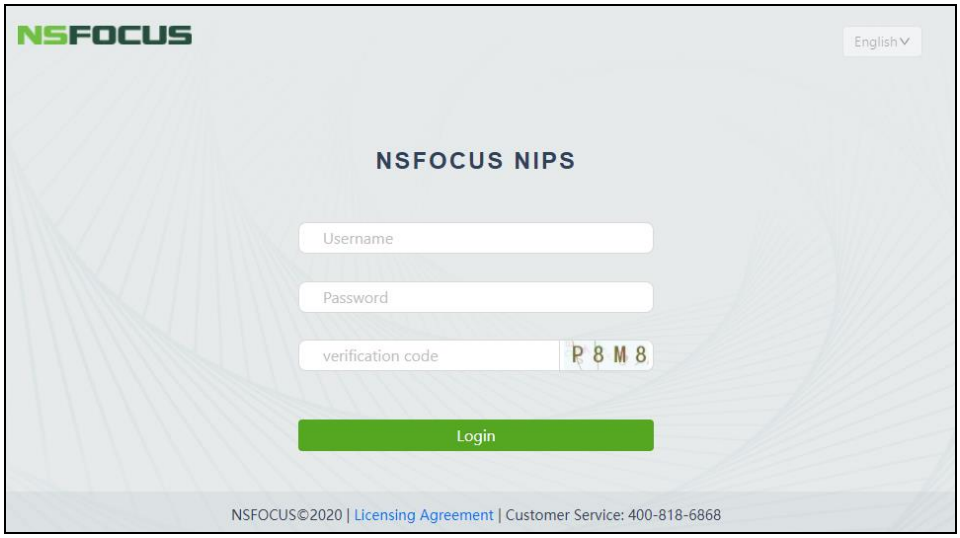
Step 1 Make sure that the client communicates properly with NIPS (open port 443 if the traffic needs to go through a firewall).

Step 2 Open the Chrome browser and connect to the management IP address of NIPS over HTTPS, for example, enter **https://192.168.1.1** in the address bar, and press **Enter**.

A security alert appears.

Step 3 Click **Advanced** and then **Proceed to xxxx (unsafe)**.

Figure 1-3 Login page



Step 4 Enter a valid user name and password.

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

Step 5 Click **Login**.

----End

Note	• 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 username; (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 1-4 shows the general layout of the page.

Figure 1-4 Web page layout

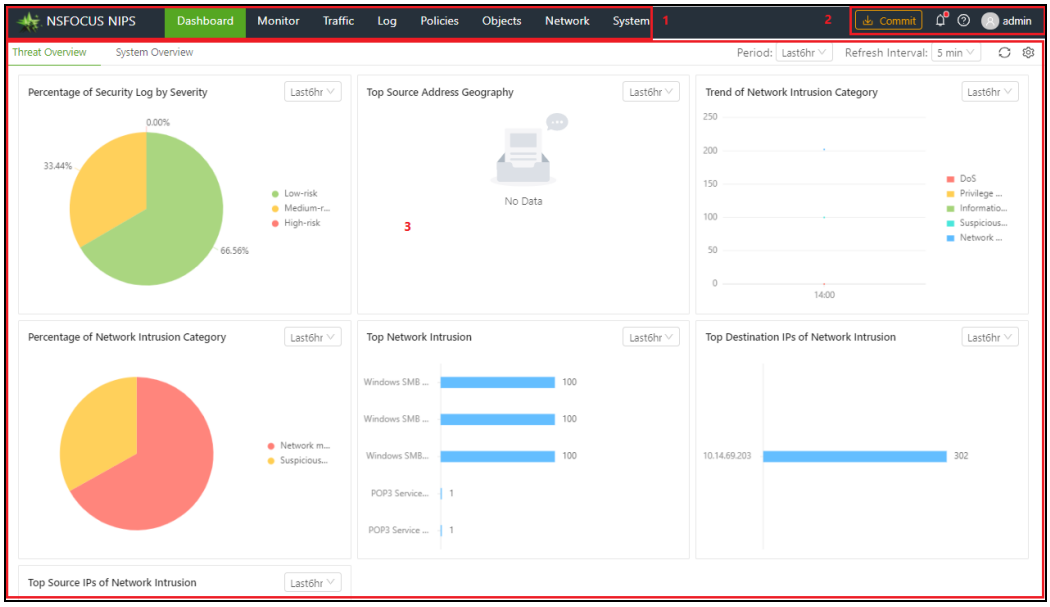


Table 1-2 describes the page layout.

Table 1-2 Page layout description

No.	Area	Description
1	Navigation bar	Area where menus and related submenus are provided to help you locate system functions.
2	Quick access bar	Area providing the following common icons of the system: • : applies configurations. • : message center. • : allows you to view related device information and online help and switch the system language. • admin: modifies the password of the current account, locks the current session, and logs you out of the web-based manager. Note • For security concern, you are advised to click admin and **Log Out** to log out of the web-based manager. • Clicking **Lock Session** directly logs you out of the web-based manager. In this case, when you log in again, you will be redirected back to the page that you are on before logout.
3	Work area	Area where you can perform configurations and operations and view data.

Note	The menus and work areas vary with user permissions.

1.3.1.4 Common Buttons and Their Functions

Table 1-3 describes common icons/buttons and their functions.

Table 1-3 Common icons/buttons and their functions

Icon/Button	Description
	Edits the current item.
	Deletes the current item. Note • Predefined items, such as the "any" subnet, cannot be deleted. • Referenced items cannot be deleted.
	Retrieves object settings.
	Starts an operation.
	Stops an ongoing operation.
	Moves up/down a policy in a list.
	Configures parameters.
	Refreshes the page.
+	Creates an object.
/	Enables or disables a policy.
	Copies the current item.
	Exports a log or report as an HTML, Word, or Excel file.
	Previews a report.
	Prints logs or a report.

Tip	Pointing to an icon 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 **Commit** in the quick access bar to make the security policy take effect.
- Choose **System > System Control** and then click **Deploy Policies**.

1.3.2 Console-based Management

The default console user of NIPS is **conadmin**, with **conadmin** as the default password. 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. For details, see A Console-based Management.

2 Dashboard

The Dashboard module, accessible only to system administrators, presents threat status information and system status information through the use of tables and graphs.

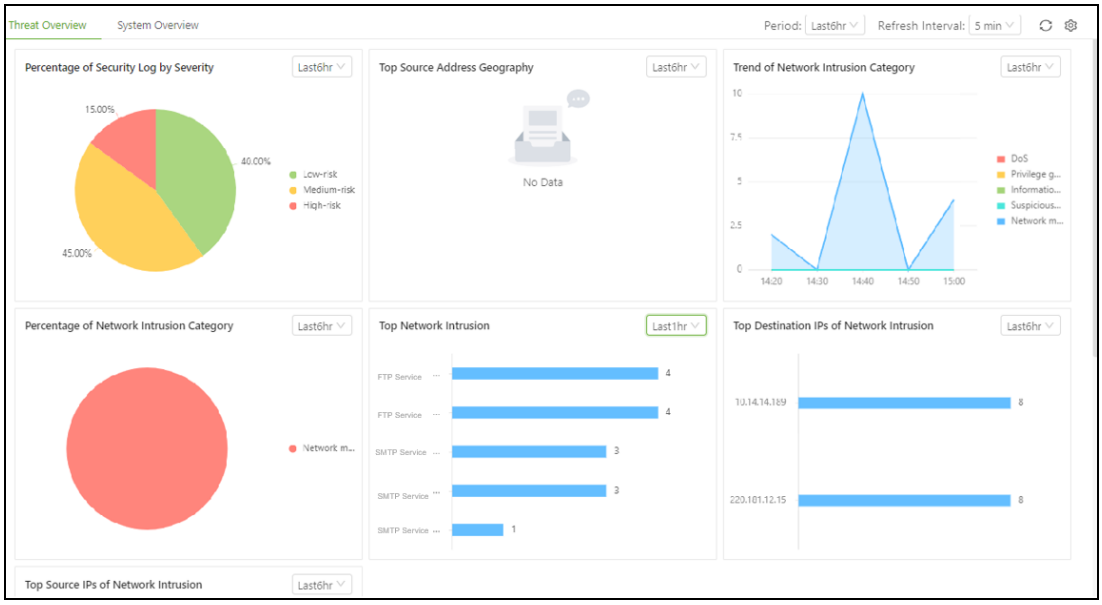
This chapter contains the following sections:

Section	Description
Threat Overview	Presents the threat status information and how to view the information.
System Overview	Presents the system status information and how to view the information.

2.1 Threat Overview

Choose **Dashboard**. The **Threat Overview** page appears, as shown in Figure 2-1.

Figure 2-1 Threat overview



The **Threat Overview** page presents configurable threat status information. You can click ⚙ in the upper-right corner of the page to view component configurations on the page:

- A component in green indicates that it is displayed on the page.
- A component in gray indicates that it is hidden from on the page.

By default, top 5 statistics are displayed. You can change to top 10.

You can click **Reset** to restore the default settings.

Figure 2-2 Component configuration

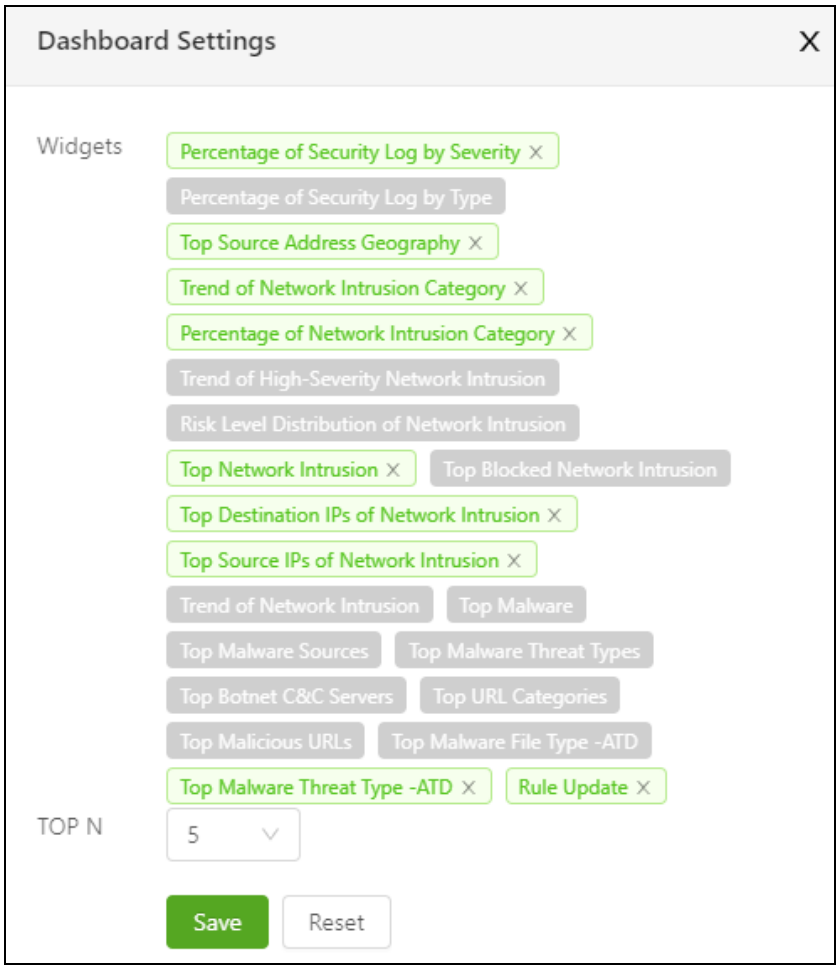


Table 2-1 describes components available on the threat overview page.

Table 2-1 Threat status components

Threat Type	Threat Status	Description
Malicious File	Top Malware	This component presents top N malicious files within the specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the histogram displays the name of a specific malicious file and its number of occurrences at a particular time point.
	Top Malware Sources	This component presents top N source IP addresses of malicious files within a specified statistical period which can be **Last 1 hr**, **Last 6**

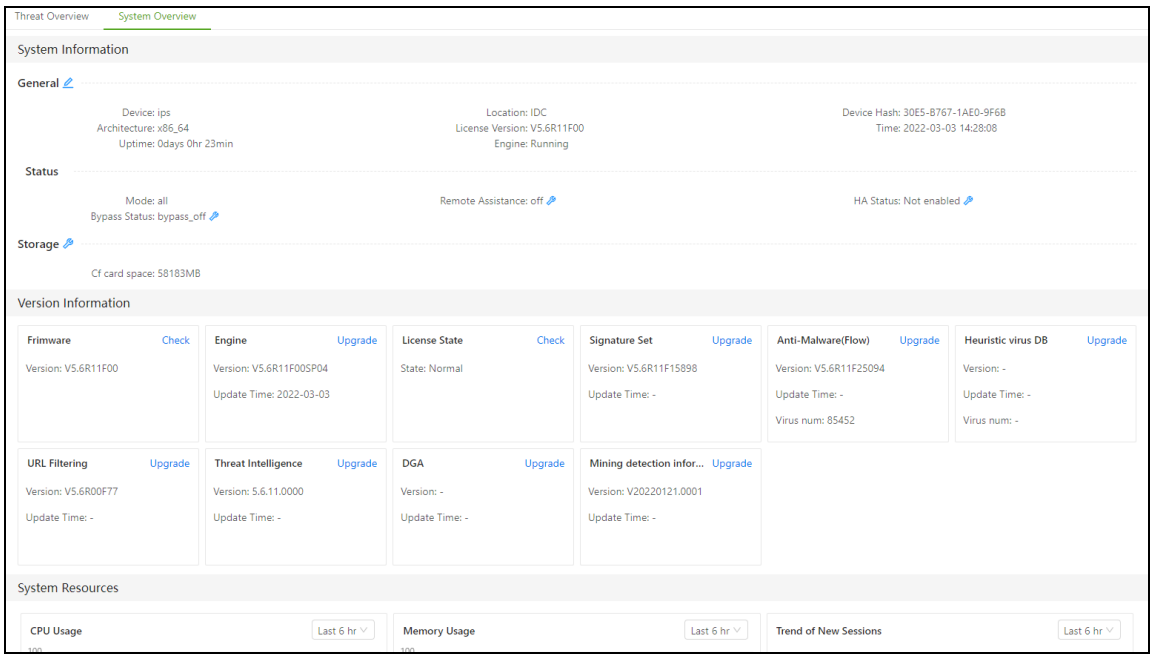
Threat Type	Threat Status	Description
		hr, **Last 12 hr**, or **Last 24 hr**. Pointing to the histogram displays a specific source IP address and its number of occurrences at a particular time point.
	Top Malware Threat Type	This component presents top N types of threat imposed by malicious files within a specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the histogram displays the specific type of threat imposed by malicious files and the number of threat of this type at a particular time point.
Intrusion Event	Trend of Network Intrusion Category	This component presents the trend of intrusion events by type within a specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the histogram displays attack types and the number of attacks of each type at a particular time point.
	Percentage of Network Intrusion Category	This component presents the intrusion attack type distribution within a specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the pie chart displays a specific attack type and the number of attacks of this type at a particular time point.
	Trend of High-Severity Network Intrusion	This component presents the trend of high-risk intrusion events within a specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the trend graph displays the number of high-risk intrusion events occurring at a particular time point.
	Risk Level Distribution of Network Intrusion	This component presents the distribution of high, medium, and low-risk intrusion events within a specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the pie chart displays the number of network intrusion events of corresponding risk levels at a particular time point.
	Top Network Intrusion	This component presents top N intrusion events occurring within a specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the histogram shows the name and count of intrusion events occurring at a particular time point.
	Top Blocked Network Intrusion	This component presents top N intrusion events blocked within a specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the histogram shows the name and count of intrusion events blocked at a particular time point.
	Top Destination IPs of Network Intrusion	This component presents top N destination IP addresses of intrusion events occurring within a statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to a histogram displays a specific destination IP address and the number of attacks it suffered at a particular time point.
	Top Source IPs of Network Intrusion	This component presents top N source IP addresses of intrusion events occurring within a statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to a histogram displays the specific source IP address and the number of attacks it launched at a particular time point.

Threat Type	Threat Status	Description
	Trend of Network Intrusion	This component presents the intrusion event trend within a statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the trend graph displays the number of intrusion events occurring at a particular time point.
Security Log	Top Source Address Geography	Presents the geographical distribution of security logs generated within the specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the geographical distribution graph displays a specific source IP address and its longitude, latitude, and number of security events at a particular time point.
	Percentage of Security Log by Severity	This component presents the distribution of security logs by risk level within the specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the pie chart displays the number of security events of a risk level at a particular time point.
	Percentage of Security Log by Type	This component presents the distribution of security logs by type within the specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the graph shows the security log type and the number of security events of this type at a particular time point.
Advanced Malicious Sample	Top Malware File Type	This component presents top N file types of advanced malicious samples within the specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the histogram shows the specific type of advanced malicious sample files and the number of files of this type at a particular time point.
	Top Malware Threat Types	This component presents top N types of alert generated for advanced malicious samples within the specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the histograph shows the specific type of threats imposed by advanced malicious samples and the number of threats of this type at a particular time point.
Top Botnet C&C Servers		This component presents top N C&C servers within the specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the histogram displays a specific C&C server and its count at a particular time point.
Top URL Categories		This component presents top N URL categories within the specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the histogram displays a specific URL category and its count at a particular time point.
Top Malicious URLs		This component presents top N malicious URLs and the number of hits on each URL within the specified statistical period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**.
Rule Update		This component presents the latest rule base update package information at the update website.

2.2 System Overview

Choose **Dashboard** > **System Overview**. The **System Overview** page appears.

Figure 2-3 System overview



The system status information includes system information, version information, monitoring information and device interface information.

Table 2-2 describes system status details.

Table 2-2 System status information

Information Category	System Status	Description
System information	General	This area presents basic system information, including the device description, device location, hash value, CPU architecture, license version, system time, system runtime, and engine status. You can click to edit the device description, device location, and system time.
	Status	This area presents system status information, including the working mode, remote assistance, HA status, and bypass status. You can click following the remote assistance, HA status, and bypass status to edit the related information.
	Storage	This area presents resource information, including information about the CF card space, log space, and backup space. You can click following each resource item to perform configurations on the corresponding pages.
Version Information		This area presents version information, including the firmware version, engine version, license status, signature sets, flow-based

Information Category	System Status	Description
		anti-malware database, heuristic anti-malware database, URL category database, NTI, DGA, and mining detection information pack version and update time. You can click **Upgrade** following an item to update the related information.
System Resources	CPU usage	This panel presents the CPU usage trend during a selected period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the trend graph shows the CPU usage of the management plane and the data plane at a specific time point.
	Memory usage	This panel presents the memory usage trend during a selected period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to the trend graph shows the memory usage at a specific time point.
	Trend of new sessions	This area presents the trend of new sessions during a selected period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to a trend graph shows the number of new sessions at a specific time point.
	Trend of concurrent sessions	This area presents the trend of concurrent sessions during a selected period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to a trend graph shows the number of new sessions at a specific time point.
	Traffic	This area presents the trend of traffic sent and received by a specific interface during a selected period which can be **Last 1 hr**, **Last 6 hr**, **Last 12 hr**, or **Last 24 hr**. Pointing to a trend graph shows traffic sent or received at a specific time point. You can determine whether to show the transmitted traffic and received traffic on the trend graph by clicking the related legend.
	Hardware monitoring information	This area presents the following information: • Fan state: presents the status of system fans and the CPU fan. • Power state: presents the status of the power supply. • Voltage state: presents the voltage status. • Temperature state: presents the motherboard temperature, power supply temperature, and CPU temperature. Note Hardware monitoring information varies with hardware platforms.
Device interface information		This area presents device interface information, including the interface name, interface status (indicates the interface is enabled and indicates the opposite), and information type, and medium type.

3 Alert

The Monitor module presents various real-time alerts. It contains the following sections:

Section	Description
Related Configurations	Describes general configurations on various alert pages.
Network Intrusion	Describes how to query intrusion prevention alerts.
Malicious Files	Describes how to query alerts for malicious files.
Web Security	Describes how to view web security alerts.
Advanced Threats	Describes how to view alerts for advanced threats.
C&C Communications	Describes how to view alerts for C&C communications.
Online Behavior	Describes how to query alerts for online behaviors.
Server Exception	Describes how to view server anomaly alerts.
Global Blacklist	Describes how to view global blacklist alerts.
DNS Safety	Describes how to view DNS sinkhole and DNS blacklist alerts.
DoS Protection	Describes how to view DoS alerts.

3.1 Related Configurations

Operations on pages under the Monitor module are almost the same. This section describes these common operations.

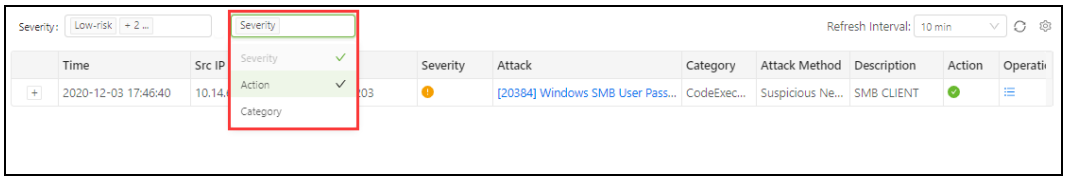
Filtering Logs

Default filtering conditions are displayed in the upper-left corner of the page.

Figure 3-1 Default filtering conditions

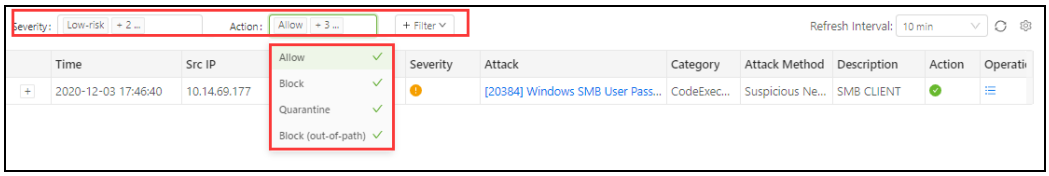
You can click **Filter** to set filtering conditions to filter logs.

Figure 3-2 Setting filtering conditions



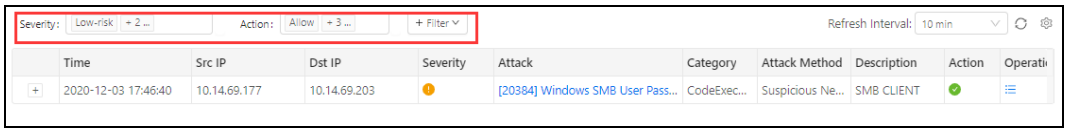
Selected filtering conditions will be displayed above the log table.

Figure 3-3 Setting filtering conditions



After filtering conditions are set, alert information retrieved based the conditions is displayed in the alert log table.

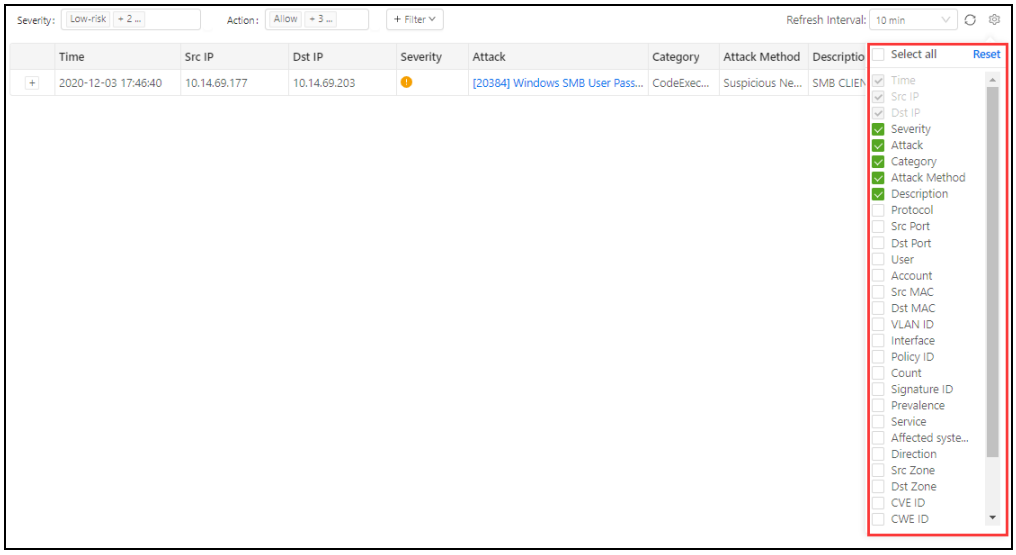
Figure 3-4 Alert logs retrieved based on the specified filtering conditions



Setting Alert Content Columns

On the alert event page, you can click ⚙ in the upper-right corner of the page to determine which columns to show.

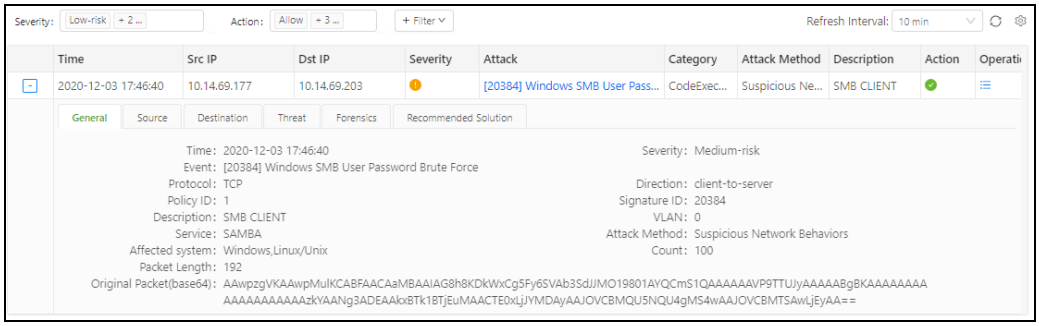
Figure 3-5 Setting alert content columns



Viewing Alert Event Details

You can click + preceding an alert event to view alert details below the event.

Figure 3-6 Viewing alert event details



You can click different page tabs to view different information. Different types of alert correspond to different alert information.

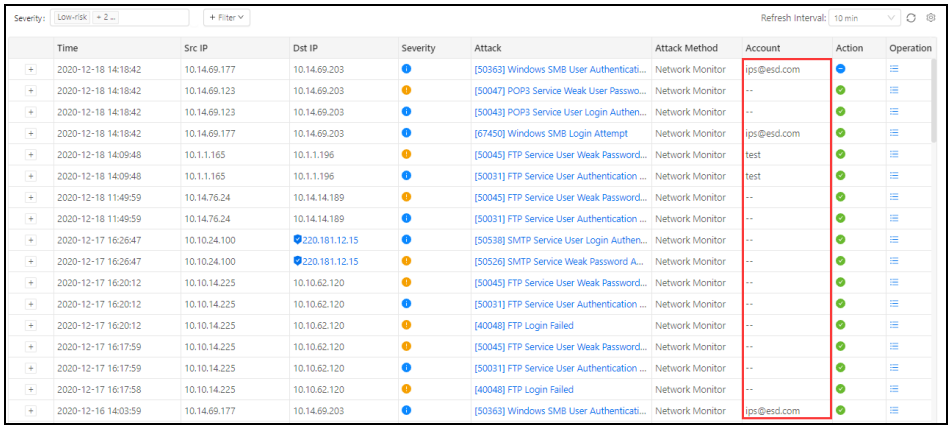
Viewing Information About Authenticated Users

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

Viewing Information About Associated Accounts

If an event matches an intelligent user identification policy (for configuration of such a policy, see Users in AD, the latest two associated accounts are displayed under **Account**.

Figure 3-7 Viewing associated user accounts



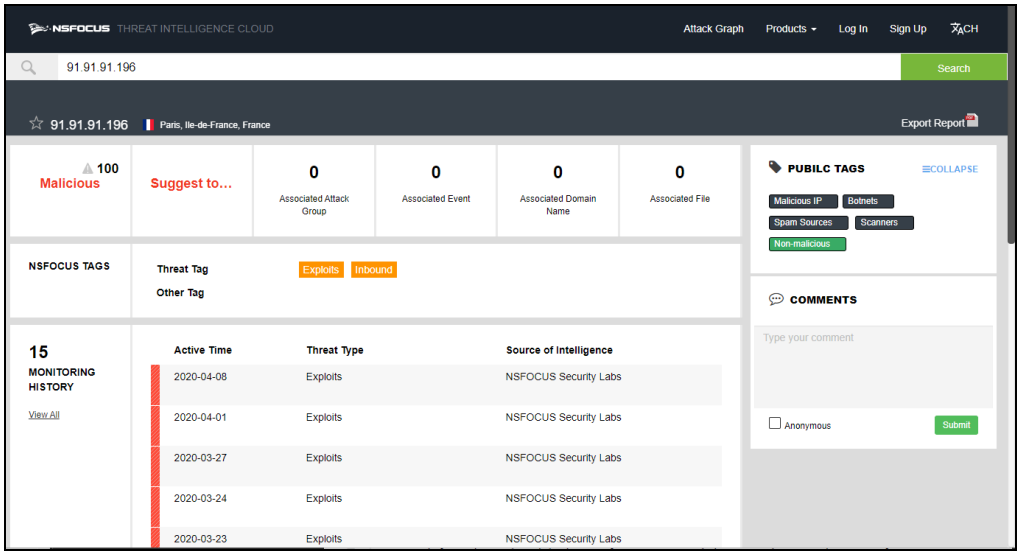
Time	Src IP	Dst IP	Severity	Attack	Attack Method	Account	Action	Operation
2020-12-18 14:18:42	10.14.69.177	10.14.69.203		[50363] Windows SMB User Authenticati...	Network Monitor	ips@esd.com		
2020-12-18 14:18:42	10.14.69.123	10.14.69.203		[50047] POP3 Service Weak User Passwo...	Network Monitor	--		
2020-12-18 14:18:42	10.14.69.123	10.14.69.203		[50043] POP3 Service User Login Authen...	Network Monitor	--		
2020-12-18 14:18:42	10.14.69.177	10.14.69.203		[67450] Windows SMB Login Attempt	Network Monitor	ips@esd.com		
2020-12-18 14:09:48	10.1.1.165	10.1.1.196		[50045] FTP Service User Weak Password...	Network Monitor	test		
2020-12-18 14:09:48	10.1.1.165	10.1.1.196		[50031] FTP Service User Authentication ...	Network Monitor	test		
2020-12-18 11:49:59	10.14.76.24	10.14.14.189		[50045] FTP Service User Weak Password...	Network Monitor	--		
2020-12-18 11:49:59	10.14.76.24	10.14.14.189		[50031] FTP Service User Authentication ...	Network Monitor	--		
2020-12-17 16:26:47	10.10.24.100	220.181.12.15		[50538] SMTP Service User Login Authen...	Network Monitor	--		
2020-12-17 16:26:47	10.10.24.100	220.181.12.15		[50526] SMTP Service Weak Password A...	Network Monitor	--		
2020-12-17 16:20:12	10.10.14.225	10.10.62.120		[50045] FTP Service User Weak Password...	Network Monitor	--		
2020-12-17 16:20:12	10.10.14.225	10.10.62.120		[50031] FTP Service User Authentication ...	Network Monitor	--		
2020-12-17 16:20:12	10.10.14.225	10.10.62.120		[40048] FTP Login Failed	Network Monitor	--		
2020-12-17 16:17:59	10.10.14.225	10.10.62.120		[50045] FTP Service User Weak Password...	Network Monitor	--		
2020-12-17 16:17:59	10.10.14.225	10.10.62.120		[50031] FTP Service User Authentication ...	Network Monitor	--		
2020-12-17 16:17:58	10.10.14.225	10.10.62.120		[40048] FTP Login Failed	Network Monitor	--		
2020-12-16 14:03:59	10.14.69.177	10.14.69.203		[50363] Windows SMB User Authenticati...	Network Monitor	ips@esd.com		

Viewing Details of a Public IP Address

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 117.50.109.22 .

You can click the source or destination IP address or click the submenu under **Threat intelligence forensics** in the **Operation** column to directly connect to NSFOCUS NTI to obtain details of the public IP address.

Figure 3-8 Viewing details of a public IP address



Refreshing Data

You can refresh data in either of the following ways on alert pages:

- Automatically refresh data.

  Specify the automatic refresh interval in the **Refresh Interval** text box so that the system can automatically refresh data at the specified interval.

- Manually refresh data.

  Click to refresh data manually on the current page.

3.2 Network Intrusion

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

3.2.1 Network Intrusion

Network intrusion events can be generated only after network intrusion profiles are configured and referenced in security policies.

NIPS displays the latest 100 network intrusion events. For each event, you can view the time, description, source and destination IP addresses, user, and details.

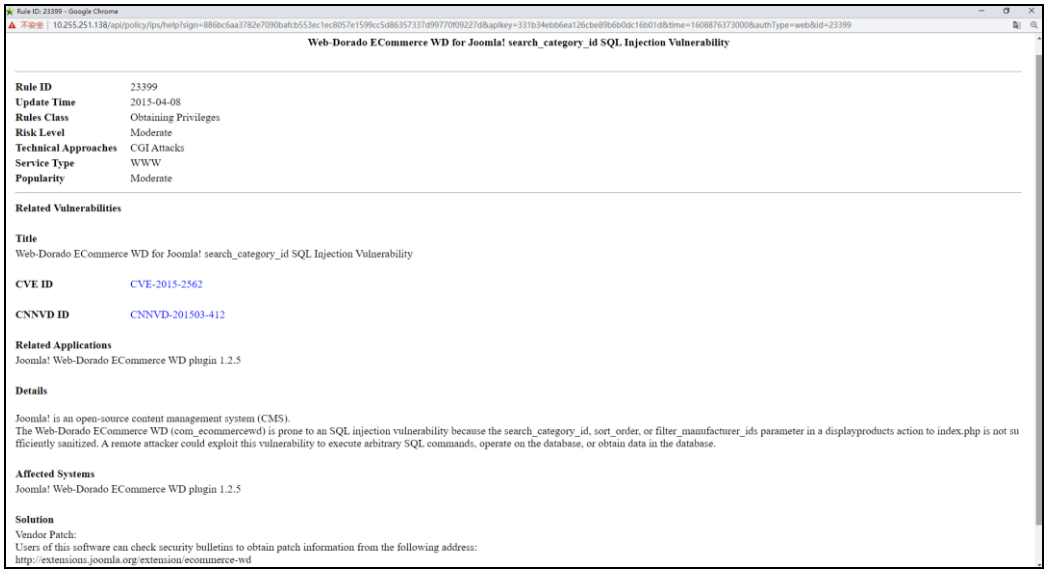
Choose **Monitor > Network Intrusion > Network Intrusion**. In the network intrusion event list shown in Figure 3-9, the icon in the **Action** column indicates that traffic related to this event was allowed to pass through, while indicates that such traffic was blocked.

Figure 3-9 List of intrusion detection events

Viewing Details of a Network Intrusion Event

Clicking an event name displays the detailed analysis of and solution for this event, as shown in Figure 3-10.

Figure 3-10 Network intrusion event analysis



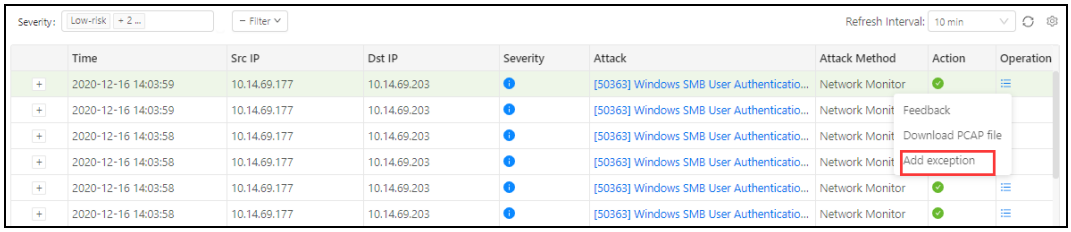
Clicking a blue link, such as the vulnerability title, NSFOCUS ID, or BUGTRAQ ID, directs you to the detailed vulnerability information page of the NSFOCUS website.

Adding an Exception

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

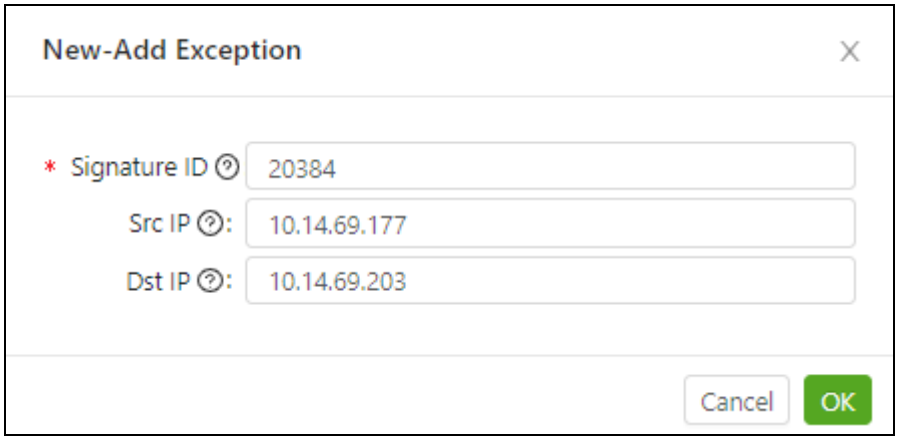
Step 1 For a network intrusion event, point to in the **Operation** column and click **Add exception**.

Figure 3-11 List of exception rules



The **New-Add Exception** dialog box appears, as shown in Figure 3-12.

Figure 3-12 Adding a rule to exception



Step 2 Configure parameters.

Table 3-1 Parameters for configuring an exception rule

Parameter	Description
Signature ID	ID of the exception rule. This ID must be the same as the ID of the related intrusion prevention rule.
Src 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.
Dst IP	Specifies the destination IP address or IP segment, that is, the valid range of destination 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 3 Click **OK**.

You can view and cancel this exception rule under **Objects** > **Network Intrusion** > **Exceptions**.

Step 4 Click **Commit** to make the settings take effect.

----End

Downloading a PCAP File

If the packet capture option is selected in a rule referenced by a policy that the current event matches, you can point to in the **Operation** column and see that the **Download PCAP file** option is available. You can click this option to download the packet capture file of the event for analysis and debugging.

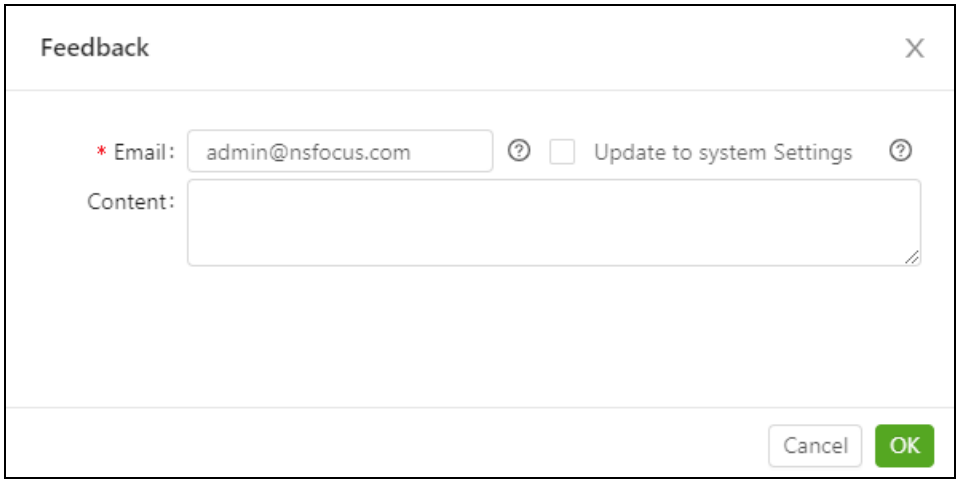
Feeding Back a False Positive

If you determine that a security event is a false positive, you can point to in the **Operation** column and click **Feedback** to inform NSFOCUS rule group.

Step 1 Point to in the **Operation** column and click **Feedback** to report false positives to NSFOCUS rule group.

The **Feedback** dialog box appears.

Figure 3-13 Typing feedback information



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

Table 3-2 Parameters for reporting feedback

Parameter	Description
Email	Specifies the email address for receiving feedback replies from the vendor. 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 the email address typed here and uses it as the default email address for sending feedback information to the vendor. For how to configure the email address, see Users.
Content	Brief feedback information.

Step 3 Click **OK**.

The system sends false positives as configured. After the false positive is successfully sent, a message indicating sending success appears.

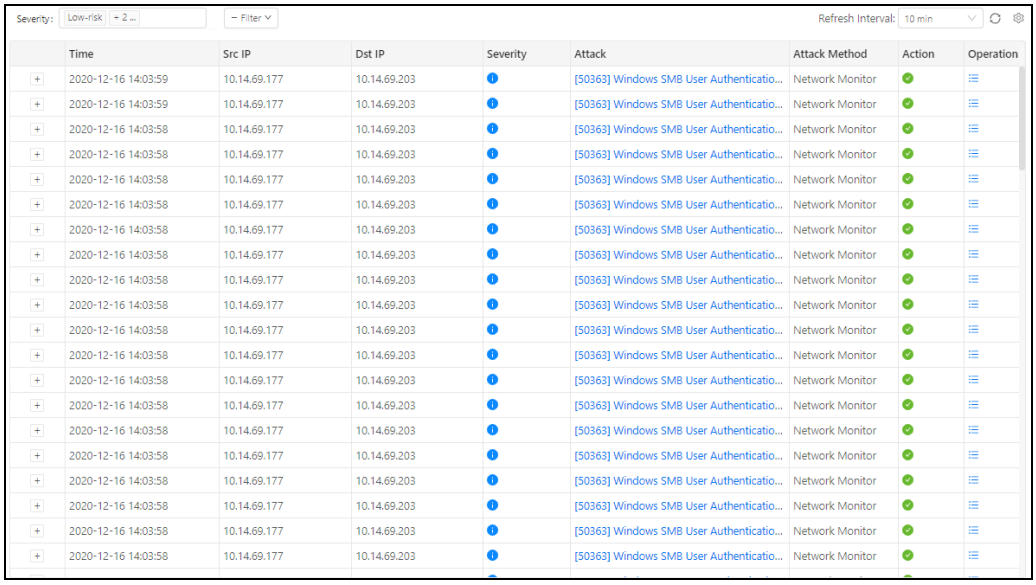
----End

3.2.2 Network Monitoring

The **Network Monitor** page shows the latest 100 network monitoring alert events.

Choose **Monitor > Network Intrusion > Network Monitor**. In the monitoring event list shown in Figure 3-14, the icon in the **Action** column indicates that traffic related to this event was allowed to pass through, while indicates that such traffic was blocked.

Figure 3-14 Viewing monitoring events



Feeding Back a False Positive

If you determine that a security event is a false positive, you can point to in the **Operation** column and click **Feedback** to inform NSFOCUS rule group. For details, see Feeding Back a False Positive.

Downloading a PCAP File

If the packet capture option is selected in a rule referenced by a policy that the current event matches, you can point to in the **Operation** column and see that the **Download PCAP file** option is available. You can click this option to download the packet capture file of the event for analysis and debugging.

Adding an Exception

If you do not want NIPS to detect real-time alert events against a certain rule, you can add this rule as an exception. For details, see Adding an Exception.

Obtaining Threat Intelligence for Forensics

If the source or destination IP address of a security event is a public IP address, you can get details of the IP address.

You can point to in the **Operation** column and click an item under **Threat intelligence forensics** to view traceback details on NTI.

Viewing Event Information

Click the content in the **Event Name** column to view details of the rule matching the event.

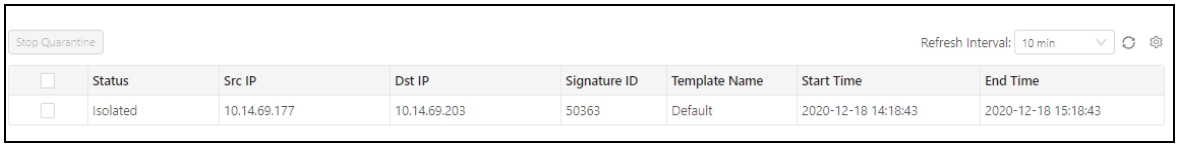
3.2.3 Quarantine List

If a security policy references an intrusion prevention profile that involves a rule with the quarantine option selected, when an attack triggers this rule, NIPS quarantines the communications between the source IP address and destination IP address of this attack.

The quarantine list displays the quarantined source and destination IP addresses, signature ID, and quarantine start and end time, as shown in Figure 3-15.

Choose **Monitor > Network Intrusion > Quarantine List**.

Figure 3-15 Quarantine list



- Click the link text **Stop quarantine** in the **Status** column to disable the quarantine.
- Click the signature ID to view details of the rule that triggers the quarantine.

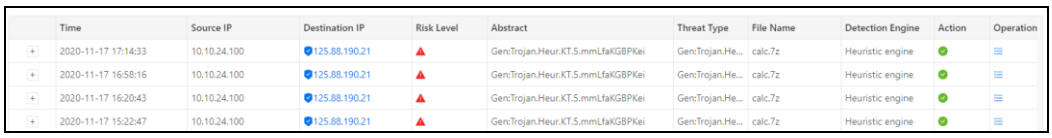
3.3 Malicious Files

Malicious file alerts can be generated only after malicious file profiles are configured and referenced in security policies.

The malicious file alert list presents the latest 100 alerts. For each alert, you can view the alert time, alert content, source IP address, and destination IP address.

Choose **Monitor > Malware**. The **Malware** page presents the list of alerts for malicious files.

Figure 3-16 Malicious file alerts



The **Severity** column shows the risk level of an alert.

In the **Action** column, the icon indicates that traffic related to this event was allowed to pass through, while indicates that such traffic was blocked.

Adding an Entry to Whitelist

For a malicious file alert, if an engine other than **Flow-based engine** is shown in the **Engine** column, you can add a malicious file to the file sample whitelist.

You can point to in the **Operation** column and then click **Add to whitelist** to add the MD5 value of the malicious file to the file sample whitelist. Then, this file is taken as a legitimate one and will no longer be subject to detections for suspicious files. For details about the file sample whitelist, see File Whitelist.

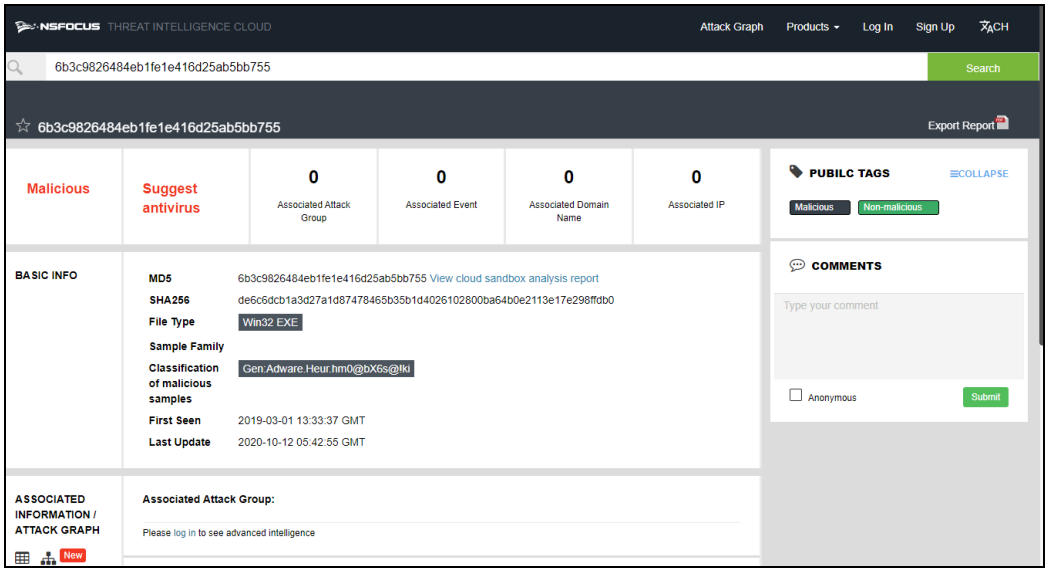
Obtaining Threat Intelligence for Forensics

For a malicious file alert, if an engine other than **Flow-based engine** is shown in the **Engine** column, you can get information about the malicious file.

For this purpose, you can point to in the **Operation** column and click one of the following items under **Threat intelligence forensics** to view traceback details on NTI:

- **Source IP**: source IP address of the malicious file.
- **Destination IP**: destination IP address of the malicious file.
- **Malicious file**: malicious file information retrieved based on its MD5 value.

Figure 3-17 Traceback information of malicious files



3.4 Web Security

The web security alert module involves malicious URLs and injection attacks.

3.4.1 Malicious URL

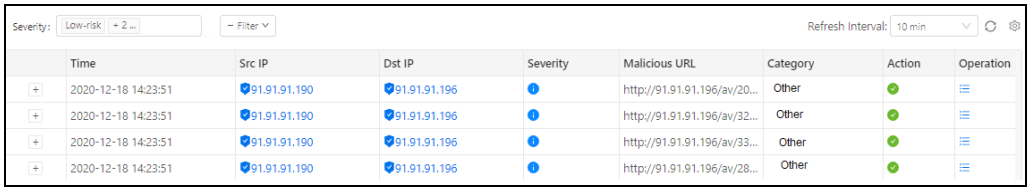
Malicious URL alerts can be reported only after you perform either of the following operations:

- Enable malicious URL protection (disabled by default) in a web security profile referenced in a security policy. Also, enable collaboration with NTI on the NTI configuration page.
- Choose **Objects** > **Malware** > **Settings** and select **Alert for Malware URL**. If a malicious file is sent via HTTP, an alert will be reported, indicating that this HTTP URL is a malicious one.

The malicious URL alert list presents the latest 100 alerts. For each alert, you can view the alert time, alert content, source IP address, and destination IP address.

Choose **Monitor** > **Web Security** > **Malicious URL**. In the **Action** column, the icon indicates that traffic related to this event was allowed to pass through, while indicates that such traffic was blocked.

Figure 3-18 Malicious URL access events



Adding an Entry to Whitelist

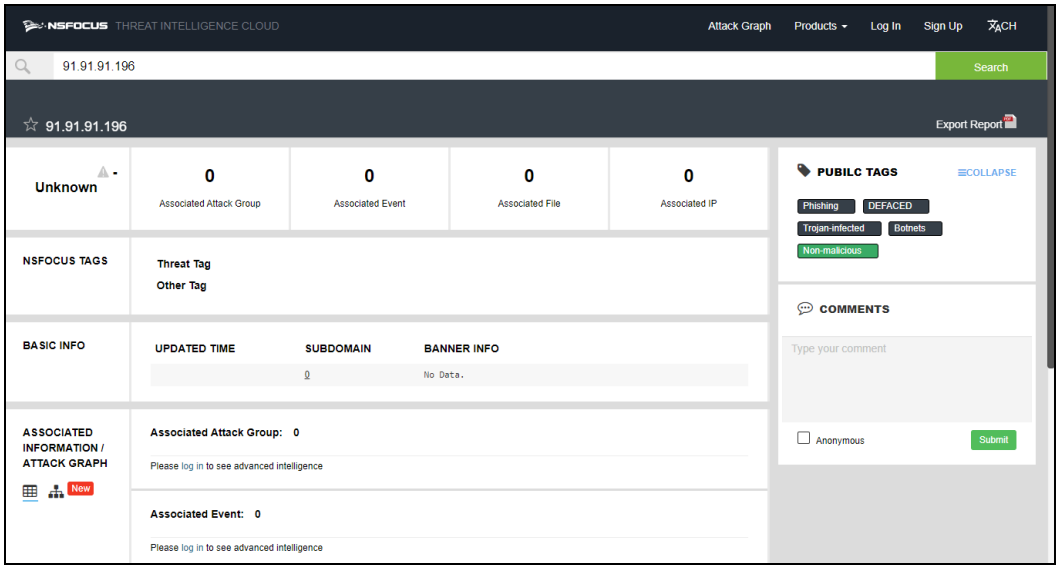
You can point to in the **Operation** column and click **Add to whitelist** to add the URL to the URL whitelist. Then this URL is considered as a legitimate one and will not be subject to subsequent URL detections. For details, see URL Whitelist.

Obtaining Threat Intelligence for Forensics

You can get details of this malicious URL, including the source IP address, destination IP address, and domain name.

For this purpose, you can point to in the **Operation** column and click **Domain name** under **Threat intelligence forensics** to view the domain name of the malicious URL.

Figure 3-19 Malicious domain name of a URL



3.4.2 Injection Attack

Injection attack alerts can be generated only after SQL injection detection is enabled in web security profiles referenced in security policies.

The injection attack alert list presents the latest 100 injection attack alerts. For each alert, you can view the time, source IP address, destination IP address, URL, and category of the attack event.

Choose **Monitor** > **Web Security** > **Injection Attack**. In the **Action** column, the icon indicates that traffic related to this event was allowed to pass through, while indicates that such traffic was blocked.

Figure 3-20 Injection attack events

Obtaining Threat Intelligence for Forensics

If the source or destination IP address of an alert event is a public IP address, you can get event details, including the time, source IP address, and destination IP address of the event.

You can click the IP address in the **Source IP** or **Destination IP** column or point to the icon in the **Operation** column and click an item under **Threat intelligence forensics** to view details of an injection attack.

3.5 Advanced Threats

If parameters for collaboration with the sandbox are configured, NIPS will send malicious file samples to the sandbox for detection and trigger an alert. In this case, if the callback monitoring function is enabled in a security policy, you can view the callback monitoring list and callback block events.

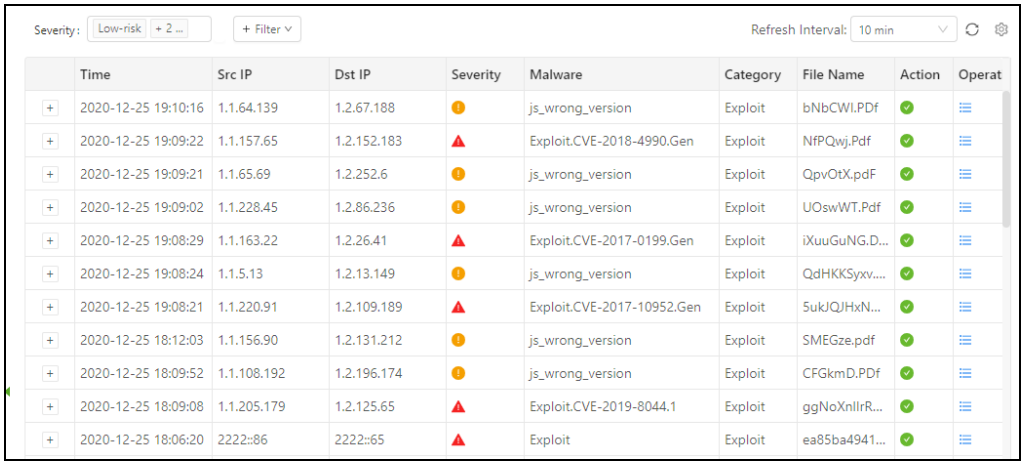
The **Advanced Threat** menu involves the following submenus: **Malware Sample**, **Callback Monitoring**, and **Callback Blocked**.

3.5.1 Advanced Malicious Samples

The system can display the latest 100 advanced malicious sample alerts.

Choose **Monitor** > **Advanced Threat** > **Malware Sample**.

Figure 3-21 Alerts of advanced malicious samples



Time	Src IP	Dst IP	Severity	Malware	Category	File Name	Action	Operat
2020-12-25 19:10:16	1.1.64.139	1.2.67.188		js_wrong_version	Exploit	bNbCWI.PDf		
2020-12-25 19:09:22	1.1.157.65	1.2.152.183		Exploit.CVE-2018-4990.Gen	Exploit	NfPQwj.Pdf		
2020-12-25 19:09:21	1.1.65.69	1.2.252.6		js_wrong_version	Exploit	QpvOtX.pdF		
2020-12-25 19:09:02	1.1.228.45	1.2.86.236		js_wrong_version	Exploit	UOswWT.Pdf		
2020-12-25 19:08:29	1.1.163.22	1.2.26.41		Exploit.CVE-2017-0199.Gen	Exploit	iXuuGuNG.D...		
2020-12-25 19:08:24	1.1.5.13	1.2.13.149		js_wrong_version	Exploit	QdHKKSyxv....		
2020-12-25 19:08:21	1.1.220.91	1.2.109.189		Exploit.CVE-2017-10952.Gen	Exploit	5ukJQJHxN...		
2020-12-25 18:12:03	1.1.156.90	1.2.131.212		js_wrong_version	Exploit	SMEGze.pdf		
2020-12-25 18:09:52	1.1.108.192	1.2.196.174		js_wrong_version	Exploit	CFGkmD.PDf		
2020-12-25 18:09:08	1.1.205.179	1.2.125.65		Exploit.CVE-2019-8044.1	Exploit	ggNoXnlIrR...		
2020-12-25 18:06:20	2222::86	2222::65		Exploit	Exploit	ea85ba4941...		

For each alert, you can view the time, source IP address, destination IP address, risk level, abstract, threat type, file name, and action of the alert.

Obtaining Threat Intelligence for Forensics

If the source or destination IP address of an alert event is a public IP address, you can get event details, including the time, source IP address, destination IP address of the event.

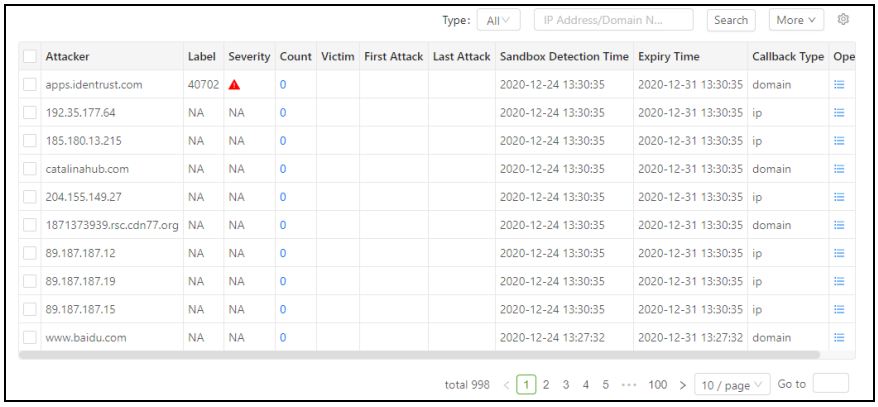
You can click the IP address in the **Source IP** or **Destination IP** column or point to the icon in the **Operation** column and then click an item under **Threat intelligence forensics** to view details of an advanced malicious sample.

3.5.2 Callback Monitoring List

NIPS supports the malware callback monitoring function. During the analysis of an advanced malicious sample, the sandbox, when detecting the sample's callback behavior, will record the address and domain name initiating callback in the callback monitoring list. You can add the IP addresses or domain names on the callback monitoring list to the blacklist or whitelist. Those added to the whitelist will be no longer subject to monitoring. If one of those added to the blacklist is hit, a callback event will be triggered.

Choose **Monitor > Advanced Threat > Callback Monitoring**.

Figure 3-22 Callback monitoring list



Attacker	Label	Severity	Count	Victim	First Attack	Last Attack	Sandbox Detection Time	Expiry Time	Callback Type	Ope
apps.identrust.com	40702	▲	0				2020-12-24 13:30:35	2020-12-31 13:30:35	domain	
192.35.177.64	NA	NA	0				2020-12-24 13:30:35	2020-12-31 13:30:35	ip	
185.180.13.215	NA	NA	0				2020-12-24 13:30:35	2020-12-31 13:30:35	ip	
catalinahub.com	NA	NA	0				2020-12-24 13:30:35	2020-12-31 13:30:35	domain	
204.155.149.27	NA	NA	0				2020-12-24 13:30:35	2020-12-31 13:30:35	ip	
1871373939.rsc.cdn77.org	NA	NA	0				2020-12-24 13:30:35	2020-12-31 13:30:35	domain	
89.187.187.12	NA	NA	0				2020-12-24 13:30:35	2020-12-31 13:30:35	ip	
89.187.187.19	NA	NA	0				2020-12-24 13:30:35	2020-12-31 13:30:35	ip	
89.187.187.15	NA	NA	0				2020-12-24 13:30:35	2020-12-31 13:30:35	ip	
www.baidu.com	NA	NA	0				2020-12-24 13:27:32	2020-12-31 13:27:32	domain	

Adding an Entry to the Blacklist

You can move whitelisted entries to the blacklist in either of the following ways:

- Move one by one: Point to in the **Operation** column and click **Add to blacklist** to move an entry to the blacklist for callback monitoring.
- Move all at once: Point to **More** and click **Blacklist all** to move whitelisted entries to the blacklist all at once.
- Move in bulk: Select one or more entries and point to **More** and click **Blacklist selected** to move selected entries to the blacklist.

Adding an Entry to the Whitelist

You can move blacklisted entries to the whitelist in either of the following ways:

- Move one by one: Point to in the **Operation** column and click **Add to blacklist** to move an entry to the blacklist for callback monitoring.
- Move all at once: Point to **More** and click **Whitelist all** to move blacklisted entries to the whitelist all at once.
- Move in bulk: Select one or more entries and point to **More** and click **Whitelist selected** to move selected entries to the whitelist.

Obtaining Threat Intelligence for Forensics

If the source or destination IP address of an alert event is a public IP address, you can get event details, including the time, source IP address, and destination IP address of the event.

You can click the IP address in the **Callback Address** column or point to the icon in the **Operation** column and then click an item under **Threat intelligence forensics** to view traceback details, for example, clicking **Callback address trace** to view details of a callback address on NTI.

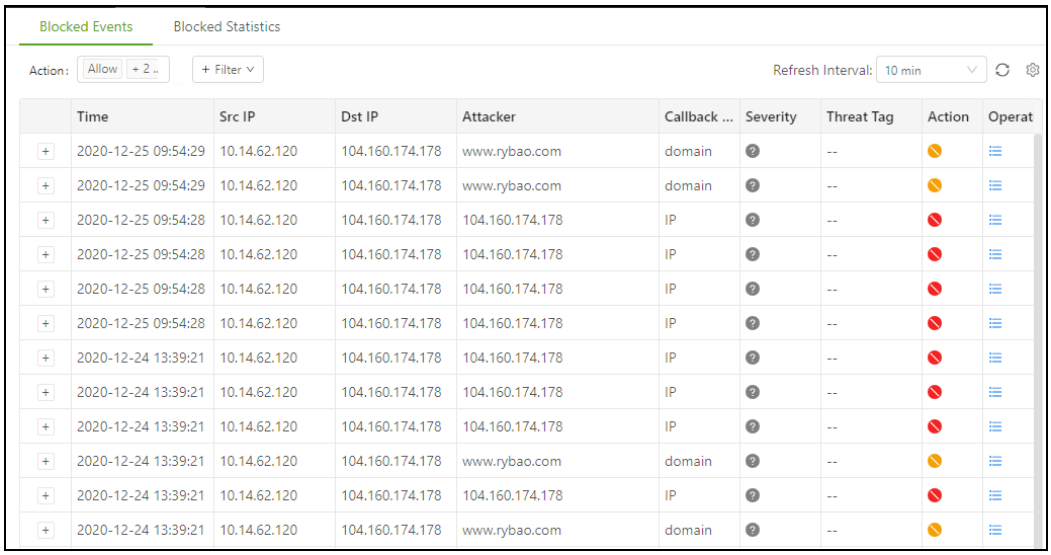
3.5.3 Callback Block Events

Choose **Monitor** > **Advanced Threat** > **Callback Blocked** to view the list of all callback block events and block event statistics.

3.5.3.1 Callback Block Events

Choose **Monitor > Advanced Threat > Callback Blocked**.

Figure 3-23 Callback block events



Time	Src IP	Dst IP	Attacker	Callback ...	Severity	Threat Tag	Action	Operat
2020-12-25 09:54:29	10.14.62.120	104.160.174.178	www.rybao.com	domain		--		
2020-12-25 09:54:29	10.14.62.120	104.160.174.178	www.rybao.com	domain		--		
2020-12-25 09:54:28	10.14.62.120	104.160.174.178	104.160.174.178	IP		--		
2020-12-25 09:54:28	10.14.62.120	104.160.174.178	104.160.174.178	IP		--		
2020-12-25 09:54:28	10.14.62.120	104.160.174.178	104.160.174.178	IP		--		
2020-12-25 09:54:28	10.14.62.120	104.160.174.178	104.160.174.178	IP		--		
2020-12-24 13:39:21	10.14.62.120	104.160.174.178	104.160.174.178	IP		--		
2020-12-24 13:39:21	10.14.62.120	104.160.174.178	104.160.174.178	IP		--		
2020-12-24 13:39:21	10.14.62.120	104.160.174.178	104.160.174.178	IP		--		
2020-12-24 13:39:21	10.14.62.120	104.160.174.178	www.rybao.com	domain		--		
2020-12-24 13:39:21	10.14.62.120	104.160.174.178	104.160.174.178	IP		--		
2020-12-24 13:39:21	10.14.62.120	104.160.174.178	www.rybao.com	domain		--		

Obtaining Threat Intelligence for Forensics

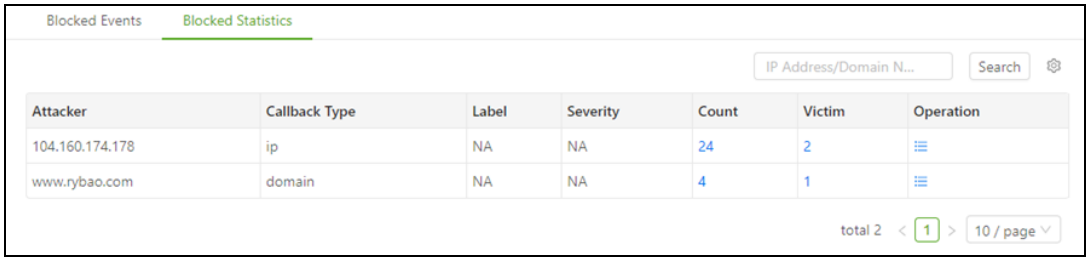
If the source or destination IP address of an alert event is a public IP address, you can get details of the two IP addresses of this event.

For this purpose, you can point to in the **Operation** column and click an item under **Threat intelligence forensics** to view event details, for example, clicking **Callback address trace** to view details of a blocked callback address on NTI.

3.5.3.2 Block Statistics

Choose **Monitor > Advanced Threat > Callback Blocked > Blocked Statistics**.

Figure 3-24 Callback block statistics



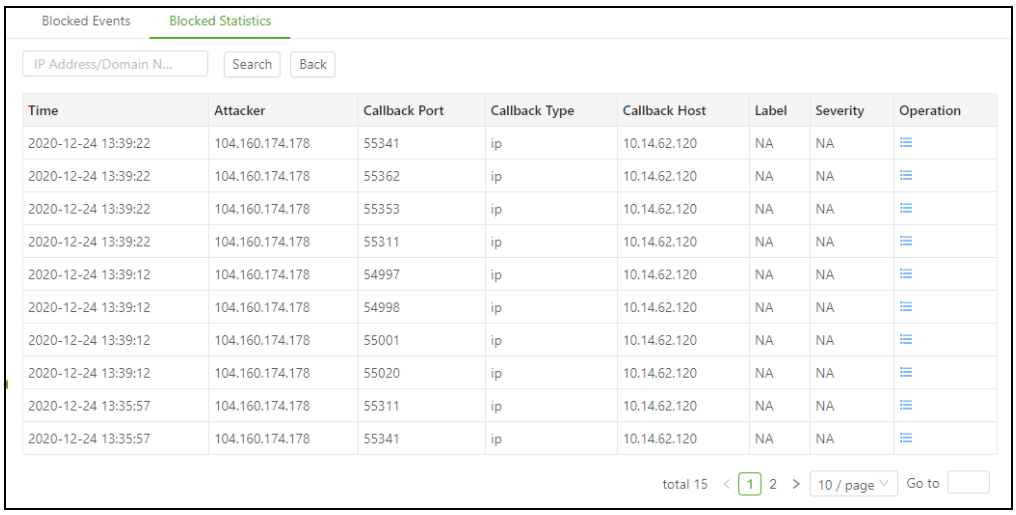
Attacker	Callback Type	Label	Severity	Count	Victim	Operation
104.160.174.178	ip	NA	NA	24	2	
www.rybao.com	domain	NA	NA	4	1	

You can view callback block statistics and traceback details of blocked callback hosts.

Viewing Block Statistics

On the page shown in Figure 3-25, you can click a figure in the **Count** column to view block details.

Figure 3-25 Viewing callback block statistics



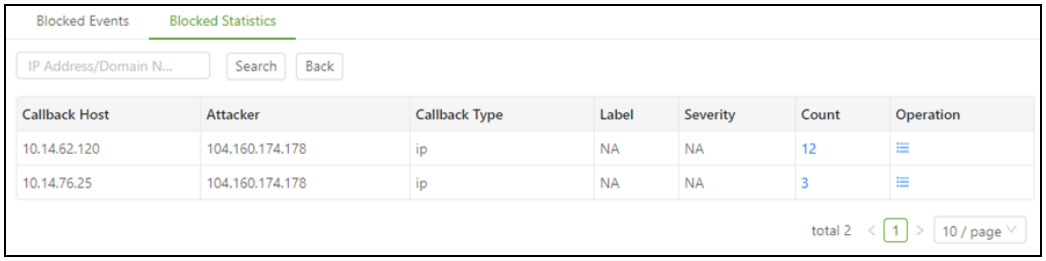
Time	Attacker	Callback Port	Callback Type	Callback Host	Label	Severity	Operation
2020-12-24 13:39:22	104.160.174.178	55341	ip	10.14.62.120	NA	NA	
2020-12-24 13:39:22	104.160.174.178	55362	ip	10.14.62.120	NA	NA	
2020-12-24 13:39:22	104.160.174.178	55353	ip	10.14.62.120	NA	NA	
2020-12-24 13:39:22	104.160.174.178	55311	ip	10.14.62.120	NA	NA	
2020-12-24 13:39:12	104.160.174.178	54997	ip	10.14.62.120	NA	NA	
2020-12-24 13:39:12	104.160.174.178	54998	ip	10.14.62.120	NA	NA	
2020-12-24 13:39:12	104.160.174.178	55001	ip	10.14.62.120	NA	NA	
2020-12-24 13:39:12	104.160.174.178	55020	ip	10.14.62.120	NA	NA	
2020-12-24 13:35:57	104.160.174.178	55311	ip	10.14.62.120	NA	NA	
2020-12-24 13:35:57	104.160.174.178	55341	ip	10.14.62.120	NA	NA	

You can type an IP address, domain name or URL in the text box in the upper-left corner of the page and click **Search** to view desired callback block statistics.

Viewing Callback Host Information

On the page shown in Figure 3-26, you can click a figure in the **Victim** column to view information about blocked callback hosts.

Figure 3-26 Viewing callback host information



Callback Host	Attacker	Callback Type	Label	Severity	Count	Operation
10.14.62.120	104.160.174.178	ip	NA	NA	12	
10.14.76.25	104.160.174.178	ip	NA	NA	3	

Obtaining Threat Intelligence for Forensics

You can point to in the **Operation** column and click **Callback address traceback** under **Threat intelligence forensics** to view details of a blocked callback address on NTI.

3.6 C&C Communications

C&C communication alerts can be generated only after C&C communication profiles are configured and referenced in security policies.

NIPS displays the latest 100 C&C communication events. For each event, you can view the time, source and destination IP addresses, event category, description, and user.

Choose **Monitor** > **C&C Communication**. In the **Action** column, the icon ✓ indicates that traffic related to this event was allowed to pass through, while ⊘ indicates that such traffic was blocked.

Figure 3-27 C&C communication events

Action: Allow + 2 ..

Refresh Interval: 10 min

	Time	Src IP	Dst IP	Domain/Host	Event	Engine	Action	Operati
+	2020-12-25 17:13:56	192.168.1.4	10.14.62.120	arcdesign.info	Botnet	Threat intelli...	⊘	☰
+	2020-12-25 17:13:56	192.168.1.4	10.14.62.120	arcdesign.info	Botnet	Threat intelli...	⊘	☰
+	2020-12-25 17:13:56	192.168.1.4	10.14.62.120	arcdesign.info	Botnet	Threat intelli...	⊘	☰
+	2020-12-25 17:13:56	192.168.1.4	10.14.62.120	arcdesign.info	Botnet	Threat intelli...	⊘	☰
+	2020-12-25 17:13:56	192.168.1.4	10.14.62.120	arcdesign.info	Botnet	Threat intelli...	⊘	☰
+	2020-12-25 17:13:56	192.168.1.4	10.14.62.120	arcdesign.info	Botnet	Threat intelli...	⊘	☰
+	2020-12-25 17:13:55	192.168.1.4	10.14.62.120	arcdesign.info	Botnet	Threat intelli...	⊘	☰
+	2020-12-25 17:13:55	192.168.1.4	10.14.62.120	arcdesign.info	Botnet	Threat intelli...	⊘	☰
+	2020-12-25 10:12:57	192.168.1.4	10.14.62.120	arcdesign.info	Botnet	Threat intelli...	⊘	☰
+	2020-12-25 10:12:57	192.168.1.4	10.14.62.120	arcdesign.info	Botnet	Threat intelli...	⊘	☰
+	2020-12-25 10:12:57	192.168.1.4	10.14.62.120	arcdesign.info	Botnet	Threat intelli...	⊘	☰

Adding an Entry to the Whitelist

You can point to ☰ in the **Operation** column and click **Add to whitelist** to add the C&C address to the whitelist. Then this address is considered as a legitimate one and will not be subject to subsequent C&C detections. For details, see C&C Whitelist.

Obtaining Threat Intelligence for Forensics

You can point to ☰ in the **Operation** column and click an item under **Threat intelligence forensics** to view traceback details, for example, clicking **C&C** to view details of the C&C attack.

3.7 Online Behavior

The **Network Behavior** menu involves three submenus: **Application Control**, **URL Filtering**, and **Data Loss Prevention**.

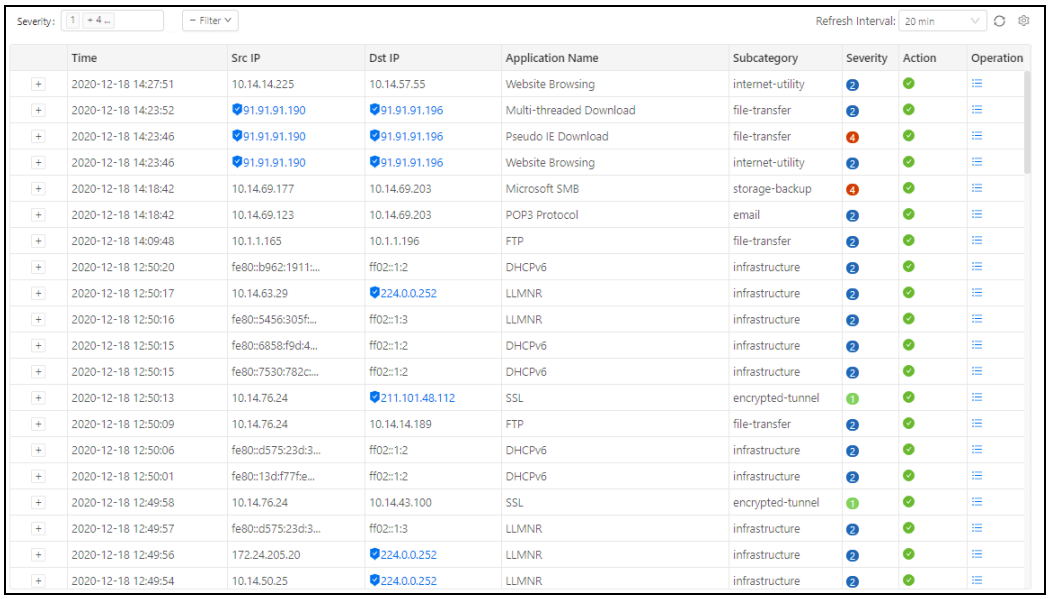
3.7.1 Application Control

Application control alerts can be generated only after application control profiles are referenced in online behavior profiles used in security policies.

NIPS can present the latest 100 application control events. For each event, you can view the time, source IP address, destination IP address, application name, application subcategory, and risk level.

Choose **Monitor > Network Behavior > Application Control**. In the application control event list, the icon in the **Action** column indicates that traffic related to this event was allowed to pass through, while indicates that such traffic was blocked.

Figure 3-28 Application control events



Severity: 1 + 4 ... Filter Refresh Interval: 20 min

	Time	Src IP	Dst IP	Application Name	Subcategory	Severity	Action	Operation
+	2020-12-18 14:27:51	10.14.14.225	10.14.57.55	Website Browsing	internet-utility	2		
+	2020-12-18 14:23:52	91.91.91.190	91.91.91.196	Multi-threaded Download	file-transfer	2		
+	2020-12-18 14:23:46	91.91.91.190	91.91.91.196	Pseudo IE Download	file-transfer	4		
+	2020-12-18 14:23:46	91.91.91.190	91.91.91.196	Website Browsing	internet-utility	2		
+	2020-12-18 14:18:42	10.14.69.177	10.14.69.203	Microsoft SMB	storage-backup	4		
+	2020-12-18 14:18:42	10.14.69.123	10.14.69.203	POP3 Protocol	email	2		
+	2020-12-18 14:09:48	10.1.1.165	10.1.1.196	FTP	file-transfer	2		
+	2020-12-18 12:50:20	fe80::b962:1911:...	ff02::1:2	DHCPv6	infrastructure	2		
+	2020-12-18 12:50:17	10.14.63.29	224.0.0.252	LLMNR	infrastructure	2		
+	2020-12-18 12:50:16	fe80::5456:305f:...	ff02::1:3	LLMNR	infrastructure	2		
+	2020-12-18 12:50:15	fe80::6858:f9d:4...	ff02::1:2	DHCPv6	infrastructure	2		
+	2020-12-18 12:50:15	fe80::7530:782c:...	ff02::1:2	DHCPv6	infrastructure	2		
+	2020-12-18 12:50:13	10.14.76.24	211.101.48.112	SSL	encrypted-tunnel	1		
+	2020-12-18 12:50:09	10.14.76.24	10.14.14.189	FTP	file-transfer	2		
+	2020-12-18 12:50:06	fe80::d575:23d:3...	ff02::1:2	DHCPv6	infrastructure	2		
+	2020-12-18 12:50:01	fe80::13d:f77f:e...	ff02::1:2	DHCPv6	infrastructure	2		
+	2020-12-18 12:49:58	10.14.76.24	10.14.43.100	SSL	encrypted-tunnel	1		
+	2020-12-18 12:49:57	fe80::d575:23d:3...	ff02::1:3	LLMNR	infrastructure	2		
+	2020-12-18 12:49:56	172.24.205.20	224.0.0.252	LLMNR	infrastructure	2		
+	2020-12-18 12:49:54	10.14.50.25	224.0.0.252	LLMNR	infrastructure	2		

If the source or destination IP address of an event is a public IP address, you can click the specific IP address in the **Source IP** or **Destination IP** column and click an item under **Threat intelligence forensics** to view details of the source or destination IP address of the event.

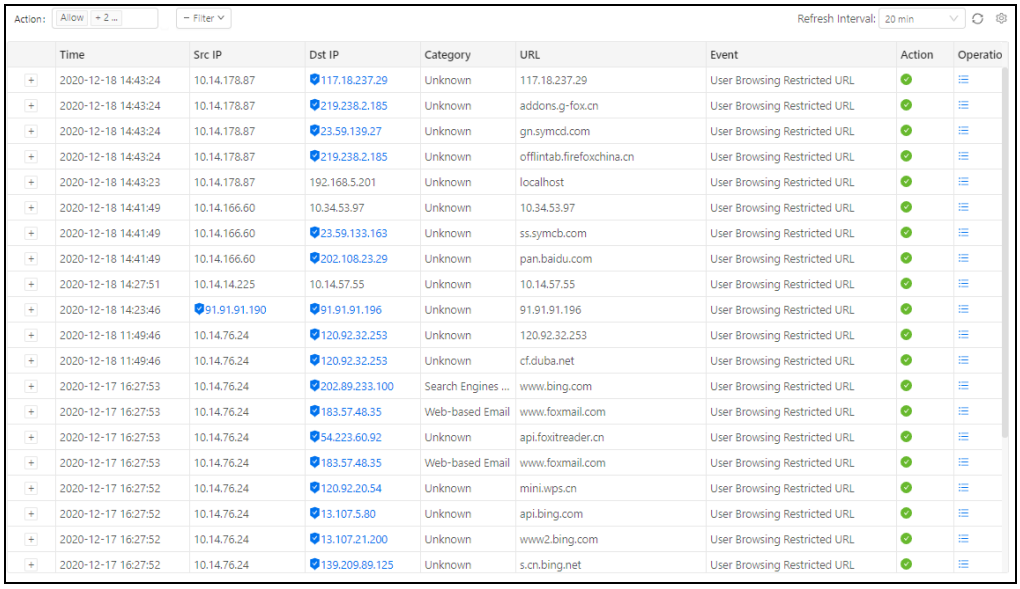
3.7.2 URL Categorization

URL categorization alerts can be generated only after URL categorization profiles are referenced in online behavior profiles used in security policies.

NIPS displays the latest 100 URL categorization events. For each event, you can view the time, source and destination IP addresses, URL category, and specific website URL.

Choose **Monitor > Network Behavior > URL Filtering**. In the URL categorization event list, the icon in the **Action** column of an event indicates that traffic related to this event was allowed to pass through, while indicates that such traffic was blocked.

Figure 3-29 URL categorization events



Action: Allow + 2 ... − Filter Refresh Interval: 20 min

	Time	Src IP	Dst IP	Category	URL	Event	Action	Operatio
+	2020-12-18 14:43:24	10.14.178.87	117.18.237.29	Unknown	117.18.237.29	User Browsing Restricted URL		
+	2020-12-18 14:43:24	10.14.178.87	219.238.2.185	Unknown	addons.g-fox.cn	User Browsing Restricted URL		
+	2020-12-18 14:43:24	10.14.178.87	23.59.139.27	Unknown	gn.symcd.com	User Browsing Restricted URL		
+	2020-12-18 14:43:24	10.14.178.87	219.238.2.185	Unknown	offlintab.firefoxchina.cn	User Browsing Restricted URL		
+	2020-12-18 14:43:23	10.14.178.87	192.168.5.201	Unknown	localhost	User Browsing Restricted URL		
+	2020-12-18 14:41:49	10.14.166.60	10.34.53.97	Unknown	10.34.53.97	User Browsing Restricted URL		
+	2020-12-18 14:41:49	10.14.166.60	23.59.133.163	Unknown	ss.symcb.com	User Browsing Restricted URL		
+	2020-12-18 14:41:49	10.14.166.60	202.108.23.29	Unknown	pan.baidu.com	User Browsing Restricted URL		
+	2020-12-18 14:27:51	10.14.14.225	10.14.57.55	Unknown	10.14.57.55	User Browsing Restricted URL		
+	2020-12-18 14:23:46	91.91.91.190	91.91.91.196	Unknown	91.91.91.196	User Browsing Restricted URL		
+	2020-12-18 11:49:46	10.14.76.24	120.92.32.253	Unknown	120.92.32.253	User Browsing Restricted URL		
+	2020-12-18 11:49:46	10.14.76.24	120.92.32.253	Unknown	cf.duba.net	User Browsing Restricted URL		
+	2020-12-17 16:27:53	10.14.76.24	202.89.233.100	Search Engines ...	www.bing.com	User Browsing Restricted URL		
+	2020-12-17 16:27:53	10.14.76.24	183.57.48.35	Web-based Email	www.foxmail.com	User Browsing Restricted URL		
+	2020-12-17 16:27:53	10.14.76.24	54.223.60.92	Unknown	api.foxitreader.cn	User Browsing Restricted URL		
+	2020-12-17 16:27:53	10.14.76.24	183.57.48.35	Web-based Email	www.foxmail.com	User Browsing Restricted URL		
+	2020-12-17 16:27:52	10.14.76.24	120.92.20.54	Unknown	mini.wps.cn	User Browsing Restricted URL		
+	2020-12-17 16:27:52	10.14.76.24	13.107.5.80	Unknown	api.bing.com	User Browsing Restricted URL		
+	2020-12-17 16:27:52	10.14.76.24	13.107.21.200	Unknown	www2.bing.com	User Browsing Restricted URL		
+	2020-12-17 16:27:52	10.14.76.24	139.209.89.125	Unknown	s.cn.bing.net	User Browsing Restricted URL		

If the source or destination IP address of an event is a public IP address, you can click the specific IP address in the **Source IP** or **Destination IP** column and click an item under **Threat intelligence forensics** to view details of the source or destination IP address of the event.

3.7.3 Data Loss Prevention

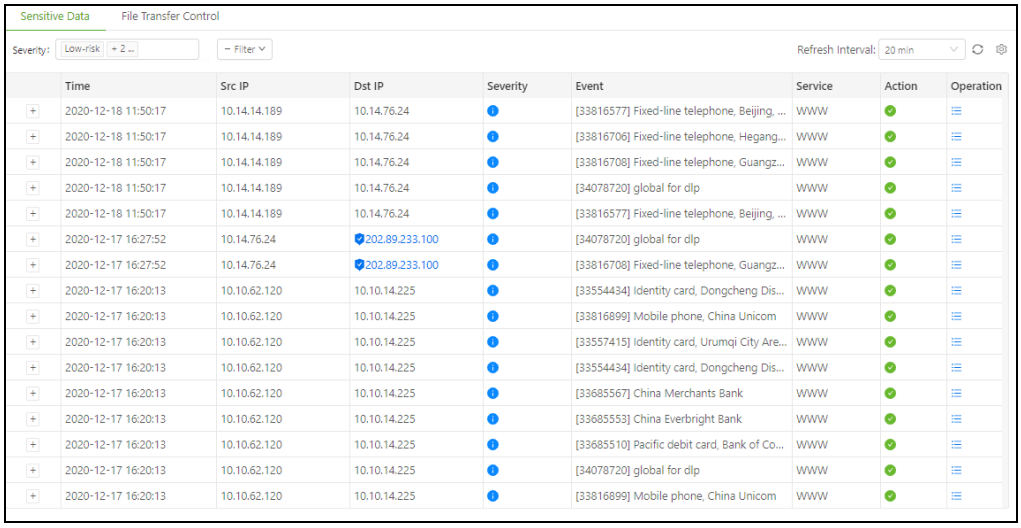
The **Data Loss Protection** menu involves two pages: **Sensitive Data** and **File Transfer Control**. Data loss prevention alerts can be generated only after data loss prevention profiles are configured and referenced by online behavior profiles used in security policies.

3.7.3.1 Sensitive Data

NIPS displays the latest 100 data loss prevention events. For each event, you can view the time, source and destination IP addresses, risk level, event description, and service.

Choose **Monitor > Network Behavior > Data Loss Prevention > Sensitive Data**. In the data loss prevention event list, the icon in the **Action** column of an event indicates that traffic related to this event was allowed to pass through, while indicates that such traffic was blocked.

Figure 3-30 Data loss prevention events



Time	Src IP	Dst IP	Severity	Event	Service	Action	Operation
2020-12-18 11:50:17	10.14.14.189	10.14.76.24		[33816577] Fixed-line telephone, Beijing, ...	WWW		
2020-12-18 11:50:17	10.14.14.189	10.14.76.24		[33816706] Fixed-line telephone, Hegang...	WWW		
2020-12-18 11:50:17	10.14.14.189	10.14.76.24		[33816708] Fixed-line telephone, Guangz...	WWW		
2020-12-18 11:50:17	10.14.14.189	10.14.76.24		[34078720] global for dlp	WWW		
2020-12-18 11:50:17	10.14.14.189	10.14.76.24		[33816577] Fixed-line telephone, Beijing, ...	WWW		
2020-12-17 16:27:52	10.14.76.24	202.89.233.100		[34078720] global for dlp	WWW		
2020-12-17 16:27:52	10.14.76.24	202.89.233.100		[33816708] Fixed-line telephone, Guangz...	WWW		
2020-12-17 16:20:13	10.10.62.120	10.10.14.225		[33554434] Identity card, Dongcheng Dis...	WWW		
2020-12-17 16:20:13	10.10.62.120	10.10.14.225		[33816899] Mobile phone, China Unicom	WWW		
2020-12-17 16:20:13	10.10.62.120	10.10.14.225		[33557415] Identity card, Urumqi City Are...	WWW		
2020-12-17 16:20:13	10.10.62.120	10.10.14.225		[33554434] Identity card, Dongcheng Dis...	WWW		
2020-12-17 16:20:13	10.10.62.120	10.10.14.225		[33685567] China Merchants Bank	WWW		
2020-12-17 16:20:13	10.10.62.120	10.10.14.225		[33685553] China Everbright Bank	WWW		
2020-12-17 16:20:13	10.10.62.120	10.10.14.225		[33685510] Pacific debit card, Bank of Co...	WWW		
2020-12-17 16:20:13	10.10.62.120	10.10.14.225		[34078720] global for dlp	WWW		
2020-12-17 16:20:13	10.10.62.120	10.10.14.225		[33816899] Mobile phone, China Unicom	WWW		

If the source or destination IP address of an event is a public IP address, you can click the specific IP address in the **Source IP** or **Destination IP** column and click an item under **Threat intelligence forensics** to view details of the source or destination IP address of the event.

3.7.3.2 File Transfer Control

NIPS displays the latest 100 file transfer events. For each event, you can view the time, source and destination IP addresses, risk level, event description, service, and event details.

Choose **Monitor > Network Behavior > Data Loss Prevention > File Transfer Control**. In the file transfer control event list, the icon in the **Action** column of an event indicates that traffic related to this event was allowed to pass through, while indicates that such traffic was blocked.

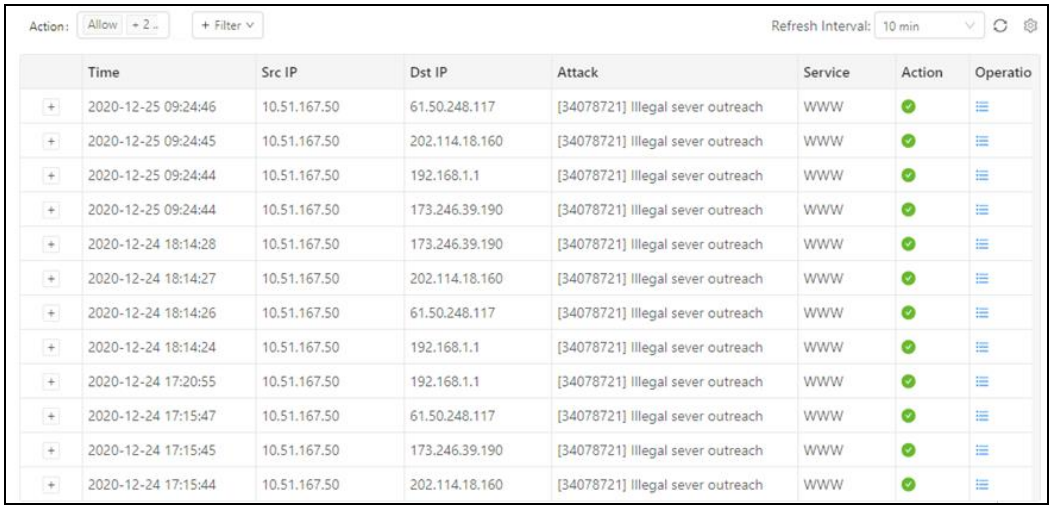
You can click the specific IP address in the **Source IP** or **Destination IP** column or click an item under **Threat intelligence forensics** to view details of the source or destination IP address of the event.

3.8 Server Exception

NIPS can monitor server outreach behaviors only after server outreach policies are configured. Server exception alerts will be generated once illegitimate server outreach behaviors are detected.

Choose **Monitor > Server Exception**.

Figure 3-31 Server exception alerts



Action: Allow + 2 ... + Filter Refresh Interval: 10 min

	Time	Src IP	Dst IP	Attack	Service	Action	Operatio
+	2020-12-25 09:24:46	10.51.167.50	61.50.248.117	[34078721] Illegal sever outreach	WWW		
+	2020-12-25 09:24:45	10.51.167.50	202.114.18.160	[34078721] Illegal sever outreach	WWW		
+	2020-12-25 09:24:44	10.51.167.50	192.168.1.1	[34078721] Illegal sever outreach	WWW		
+	2020-12-25 09:24:44	10.51.167.50	173.246.39.190	[34078721] Illegal sever outreach	WWW		
+	2020-12-24 18:14:28	10.51.167.50	173.246.39.190	[34078721] Illegal sever outreach	WWW		
+	2020-12-24 18:14:27	10.51.167.50	202.114.18.160	[34078721] Illegal sever outreach	WWW		
+	2020-12-24 18:14:26	10.51.167.50	61.50.248.117	[34078721] Illegal sever outreach	WWW		
+	2020-12-24 18:14:24	10.51.167.50	192.168.1.1	[34078721] Illegal sever outreach	WWW		
+	2020-12-24 17:20:55	10.51.167.50	192.168.1.1	[34078721] Illegal sever outreach	WWW		
+	2020-12-24 17:15:47	10.51.167.50	61.50.248.117	[34078721] Illegal sever outreach	WWW		
+	2020-12-24 17:15:45	10.51.167.50	173.246.39.190	[34078721] Illegal sever outreach	WWW		
+	2020-12-24 17:15:44	10.51.167.50	202.114.18.160	[34078721] Illegal sever outreach	WWW		

In the server exception alert list, the icon in the **Action** column of an event indicates that traffic related to this event was allowed to pass through, while indicates that such traffic was blocked.

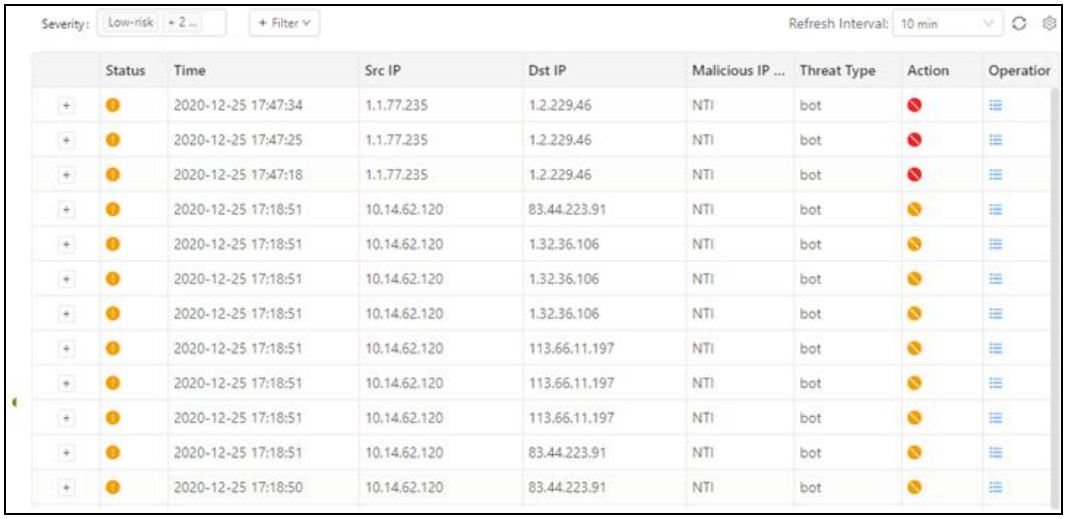
If the source or destination IP address of an event is a public IP address, you can click the specific IP address in the **Source IP** or **Destination IP** column and click an item under **Threat intelligence forensics** to view details of the source or destination IP address of the event.

3.9 Global Blacklist

If the IP address of a website hits an entry in the global IP blacklist, an IP blacklist alert is generated, and the system directly blocks its connection.

Choose **Monitor** > **Global Blacklist** > **IP Blacklist**.

Figure 3-32 IP blacklist



Status	Time	Src IP	Dst IP	Malicious IP ...	Threat Type	Action	Operatior
	2020-12-25 17:47:34	1.1.77.235	1.2.229.46	NTI	bot		
	2020-12-25 17:47:25	1.1.77.235	1.2.229.46	NTI	bot		
	2020-12-25 17:47:18	1.1.77.235	1.2.229.46	NTI	bot		
	2020-12-25 17:18:51	10.14.62.120	83.44.223.91	NTI	bot		
	2020-12-25 17:18:51	10.14.62.120	1.32.36.106	NTI	bot		
	2020-12-25 17:18:51	10.14.62.120	1.32.36.106	NTI	bot		
	2020-12-25 17:18:51	10.14.62.120	1.32.36.106	NTI	bot		
	2020-12-25 17:18:51	10.14.62.120	113.66.11.197	NTI	bot		
	2020-12-25 17:18:51	10.14.62.120	113.66.11.197	NTI	bot		
	2020-12-25 17:18:51	10.14.62.120	113.66.11.197	NTI	bot		
	2020-12-25 17:18:51	10.14.62.120	83.44.223.91	NTI	bot		
	2020-12-25 17:18:50	10.14.62.120	83.44.223.91	NTI	bot		

Obtaining Threat Intelligence for Forensics

You can point to in the **Operation** column and click an item under **Threat intelligence forensics** to view details of the source IP address, destination IP address, or malicious IP address of a global blacklist alert event.

Feeding Back a False Positive

If you determine that a security event is a false positive, you can point to in the **Operation** column and click **Feedback** to inform NSFOCUS rule group. For details, see Feeding Back a False Positive.

3.10 DNS Safety

The **DNS Safety** menu includes two submenus: **DNS Sinkhole** and **DNS Blacklist.**

3.10.1 DNS Sinkhole

Choose **Monitor** > **DNS Safety** > **DNS Sinkhole** to view records of events triggering DNS sinkholing policies. Click **Add to blacklist** in the **Operation** column of an event to add the domain name to the blacklist. A DNS sinkhole alert will be generated when this domain name is matched.

Figure 3-33 DNS sinkhole

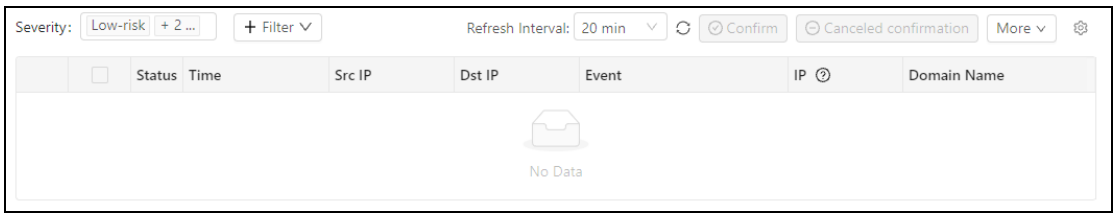
Src IP	Dst IP	Abnormal Domain Name	SinkHole IP	Count	Last Time	Operation
10.0.2.15	10.0.2.2	www.baidu.com	10.8.15.215	193	2021-08-26 13:42:08	Add to blacklist
10.66.35.26	119.6.6.6	www.qq.com	1.1.1.1	3	2021-07-31 16:20:54	Add to blacklist

3.10.2 DNS Blacklist

If the domain name of a website hits an entry in the DNS blacklist, a DNS backlist alert is generated.

Choose **Monitor** > **DNS Safety** > **DNS Blacklist.**

Figure 3-34 DNS backlist



Obtaining Threat Intelligence for Forensics

You can point to in the **Operation** column and click an item under **Threat intelligence forensics** to view details of the source IP address or destination IP address of a DNS blacklist alert event.

Feeding Back a False Positive

If you determine that a security event is a false positive, you can point to in the **Operation** column and click **Feedback** to inform NSFOCUS rule group. For details, see Feeding Back a False Positive.

If the IP address or domain name of a website hits an entry in the global blacklist, the system will directly block connections to the website. Global blacklists include the IP blacklist and domain name blacklist.

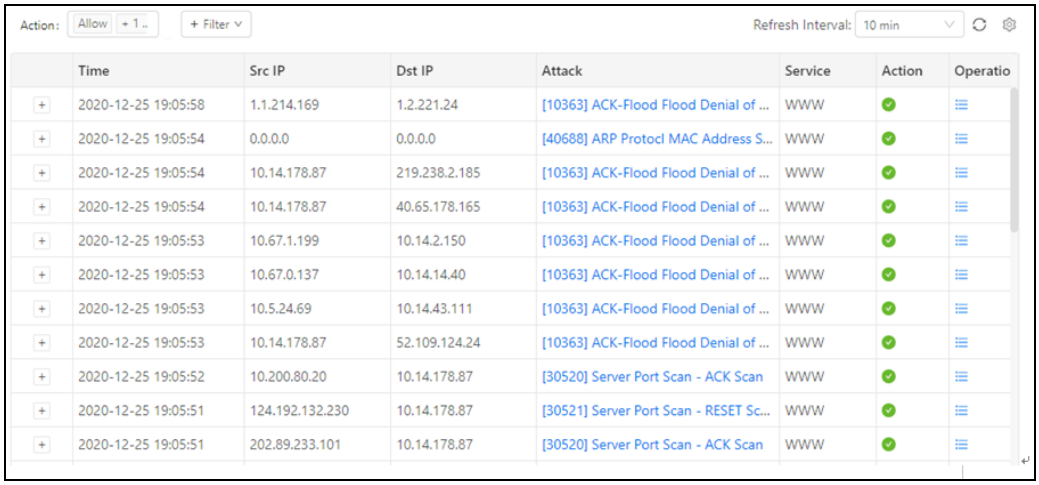
3.11 DoS Protection

DoS protection alerts can be generated only after DoS protection policies are enabled and configured.

NIPS displays the latest 100 DoS protection events. For each event, you can view the time, source and destination IP addresses, event name, service, and action.

Choose **Monitor** > **DoS Protection**. In the DoS alert list, the icon in the **Action** column of an event indicates that traffic related to this event was allowed to pass through, while indicates that such traffic was subject to a limited rate.

Figure 3-35 DoS protection alerts



Time	Src IP	Dst IP	Attack	Service	Action	Operatio
2020-12-25 19:05:58	1.1.214.169	1.2.221.24	[10363] ACK-Flood Flood Denial of ...	WWW		
2020-12-25 19:05:54	0.0.0.0	0.0.0.0	[40688] ARP Protocl MAC Address S...	WWW		
2020-12-25 19:05:54	10.14.178.87	219.238.2.185	[10363] ACK-Flood Flood Denial of ...	WWW		
2020-12-25 19:05:54	10.14.178.87	40.65.178.165	[10363] ACK-Flood Flood Denial of ...	WWW		
2020-12-25 19:05:53	10.67.1.199	10.14.2.150	[10363] ACK-Flood Flood Denial of ...	WWW		
2020-12-25 19:05:53	10.67.0.137	10.14.14.40	[10363] ACK-Flood Flood Denial of ...	WWW		
2020-12-25 19:05:53	10.5.24.69	10.14.43.111	[10363] ACK-Flood Flood Denial of ...	WWW		
2020-12-25 19:05:53	10.14.178.87	52.109.124.24	[10363] ACK-Flood Flood Denial of ...	WWW		
2020-12-25 19:05:52	10.200.80.20	10.14.178.87	[30520] Server Port Scan - ACK Scan	WWW		
2020-12-25 19:05:51	124.192.132.230	10.14.178.87	[30521] Server Port Scan - RESET Sc...	WWW		
2020-12-25 19:05:51	202.89.233.101	10.14.178.87	[30520] Server Port Scan - ACK Scan	WWW		

Obtaining Threat Intelligence for Forensics

If the source or destination IP address of a security event is a public IP address, you can point to in the **Operation** column of an event and click an item under **Threat intelligence forensics** to view details of the source IP address or destination IP address of this event.

Viewing Event Information

Click the content in the **Attack** column to view details of the rule matching the event.

4 Traffic

This chapter describes traffic configurations. It contains the following sections:

Section	Description
Bandwidth Management	Describes how to configure a bandwidth management policy.
Traffic Analysis	Describes how to configure a traffic analysis policy.
NetFlow Configuration	Describes how to configure NetFlow settings.

4.1 Bandwidth Management

Bandwidth 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.

Bandwidth management configurations involve two parts:

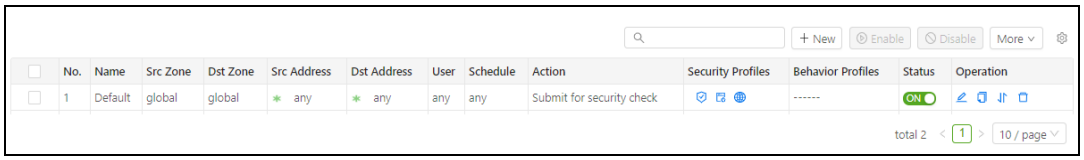
- Policy
- Bandwidth Management Profile

4.1.1 Policy

You can query, create, edit, delete, sort, duplicate, enable, or disable bandwidth management policies. The following describes how to create a policy.

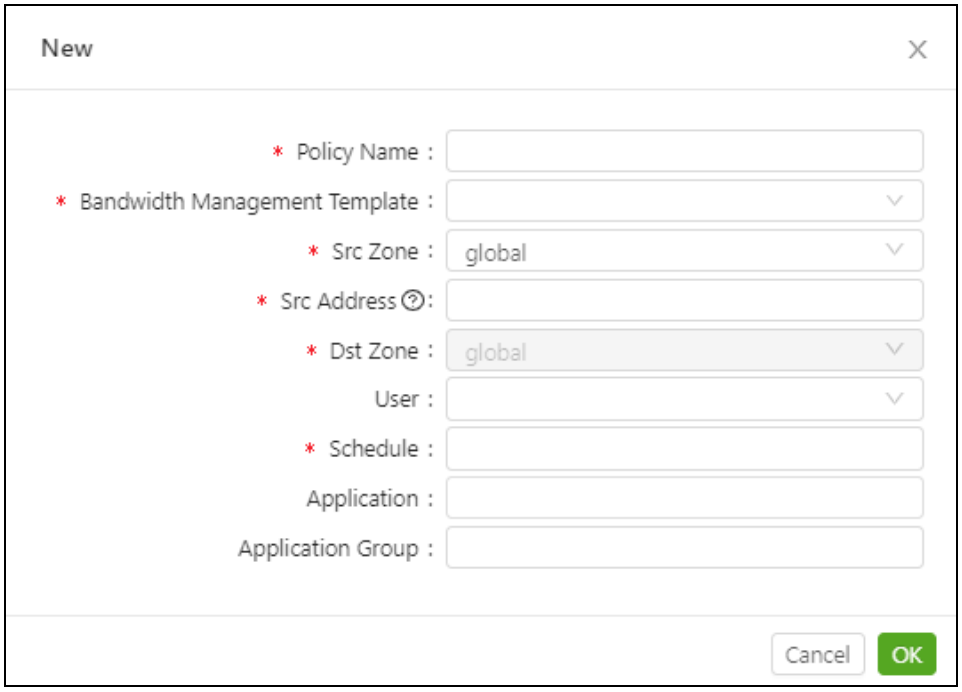
Step 1 Choose **Traffic** > **Bandwidth Management** > **Policies**.

Figure 4-1 Bandwidth management policies



Step 2 Click **New** to create a bandwidth management policy.

Figure 4-2 Creating a bandwidth management policy



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

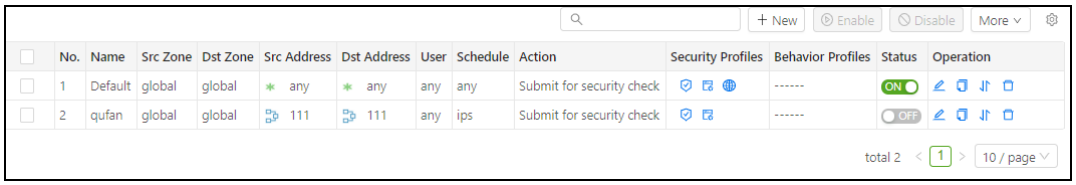
Table 4-1 Parameters for creating a bandwidth management policy

Parameter	Description
Policy Name	Specifies the name of the bandwidth management policy.
Bandwidth Management Template	Specifies the bandwidth management profile referenced in this policy.
Src/Dst Zone	Specifies a security zone. Packets from or to the specified security zone match this bandwidth management policy. **global** indicates that packets from or to any security zones will be checked against this policy. The destination security zone automatically refreshes with a matching value each time you select a source security zone.
Src Address	Specifies the source IP address object of uplink traffic. **any** cannot be selected as the source address object.
User	Specifies user objects of this policy.
Schedule	Specifies the period when this policy is valid.
Application	Specifies applications to which this policy will apply.
Application Group	Specifies application groups to which this policy will apply. If neither applications nor application groups are selected, the traffic control is performed only based on IP addresses.

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

The new bandwidth management policy is as shown in Figure 4-3.

Figure 4-3 Bandwidth management policies



Step 5 Click **Commit** in the quick access bar to make the security policy take effect.

----End

4.1.2 Bandwidth Management Profile

Choose **Traffic** > **Bandwidth Management** > **Bandwidth Management Template**. A traffic line with the maximum uplink/downlink bandwidth being 100 Mbps is configured on NIPS by default.

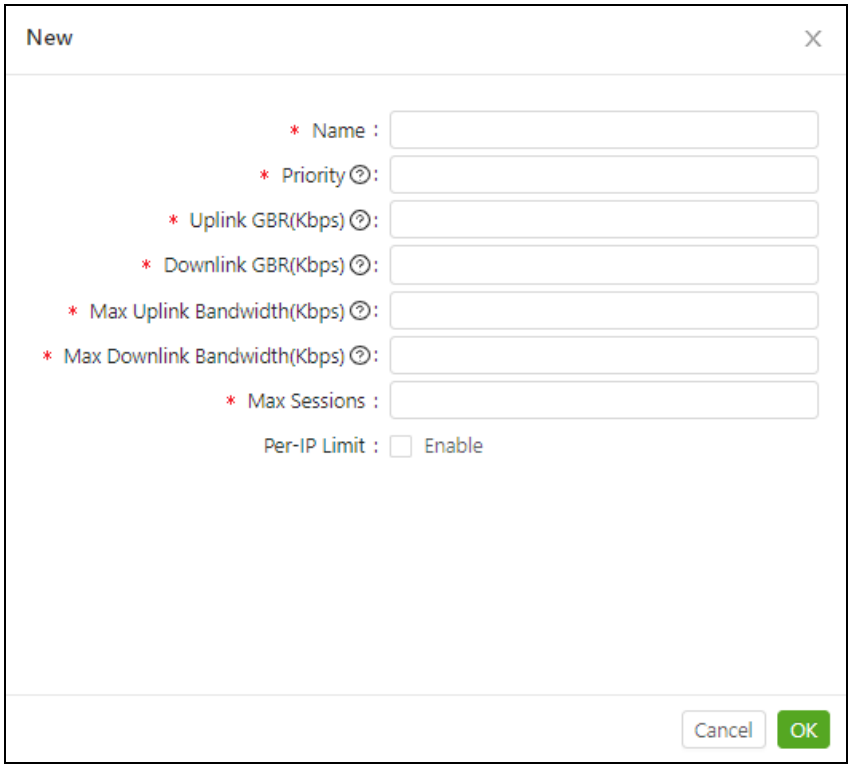
Figure 4-4 Bandwidth management profiles

You can create, edit or delete bandwidth management profiles or traffic lines. The following describes how to create a bandwidth management policy and how to create a traffic line.

Creating a Bandwidth Management Profile

Step 1 On the page shown in Figure 4-5, click + in the **Operation** column of this traffic line to create a bandwidth management profile for this line.

Figure 4-5 Creating a bandwidth management profile



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

Table 4-2 Parameters for creating a bandwidth management profile

Parameter	Description
Name	Specifies the name of the bandwidth management profile. The name must be unique and cannot contain 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. **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. **Note** The total downlink traffic must be greater than the sum of downlink GBRs of traffic channels involved in all policies.

Parameter		Description
Max Uplink Bandwidth(Kbps)		Specifies the maximum bandwidth for (unit: kbps) for outgoing traffic.
Max Downlink Bandwidth(Kbps)		Specifies the maximum bandwidth for (unit: kbps) for incoming traffic.
Max Sessions		Specifies the maximum number of TCP sessions allowed by the traffic channel.
Per-IP Limit	Enable	If you select **Per-IP Limit**, NIPS controls traffic from each IP address included in source address objects. If you do not select it, NIPS controls traffic for source address objects on the whole.
	Max Uplink Bandwidth (Kbps)	Specifies the maximum uplink bandwidth for each IP address.
	Max Downlink Bandwidth (Kbps)	Specifies the maximum downlink bandwidth for each IP address.
	Max Sessions	Specifies the maximum number of TCP sessions allowed for each IP address.

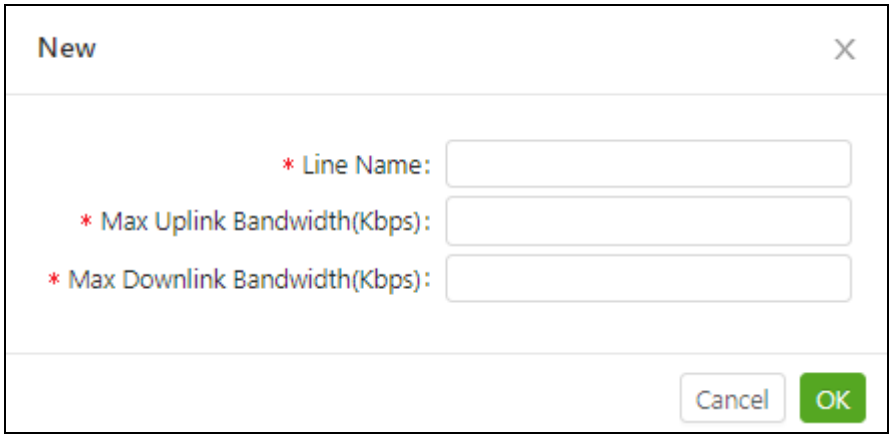
Step 3 Click **OK** to save the settings.

----End

Creating a Traffic Line

Step 1 On the page shown in Figure 4-4, click **Create Line**.

Figure 4-6 Creating a traffic line



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

Table 4-3 Parameters for creating a traffic line

Parameter	Description
Line Name	Specifies the line name. The name must be unique and cannot contain the following special characters:

Parameter	Description
	% \ ` < > ' & "
Max Uplink Bandwidth(Kbps)	Specifies the maximum bandwidth for outgoing traffic. The unit is kbps.
Max Downlink Bandwidth(Kbps)	Specifies the maximum bandwidth for incoming traffic. The unit is kbps.

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

----End

4.2 Traffic Analysis

Traffic analysis policies are used to analyze network traffic data. After analysis, NIPS presents the handled traffic destined to applications and IP addresses on the web-based manager.

Traffic analysis configurations involve the following parts:

- Policy
- Application Analysis
- IP Analysis
- Traffic Integrity Distribution

4.2.1 Policy

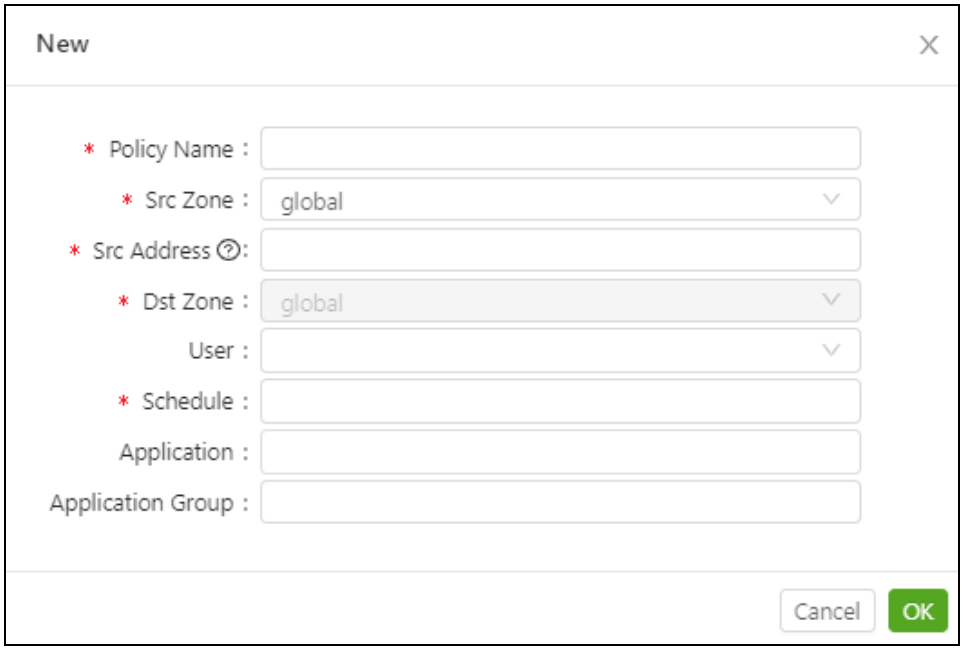
You can query, create, edit, delete, sort, duplicate, enable, or disable traffic analysis policies. To create a traffic analysis policy, follow these steps:

Step 1 Choose **Traffic** > **Traffic Analysis** > **Policies**.

Figure 4-7 Traffic analysis policy

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

Figure 4-8 Creating a traffic analysis policy



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

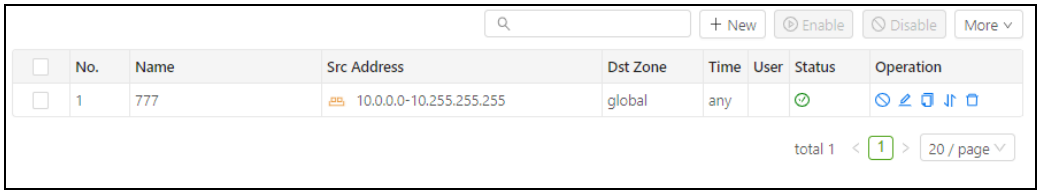
Table 4-4 Parameters for creating a new traffic analysis policy

Parameter	Description
Policy Name	Specifies the policy name.
Src/Dst Zone	Specifies a security zone. Packets from or to the specified security zone match this policy. **global** indicates that packets from or to any security zones will be checked against this policy. The destination security zone automatically refreshes with a matching value each time you select a source security zone.
Src Address	Src Address should not be any when Src Zone is set to global, Direct-A, Direct-B, Direct-C, Direct-D, or Direct-E.
Schedule	Specifies a period during which this policy is valid.
User	Specifies user objects of this policy.
Application	Specifies application objects to which this policy applies.
Application Group	Specifies application group objects to which this policy applies.

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

The new policy is shown in Figure 4-9.

Figure 4-9 Policy list



Step 5 Click **Commit** in the quick access bar to make the security policy take effect.

----End

4.2.2 Application Analysis

Choose **Traffic** > **Traffic Analysis** > **Application Analysis**. The **Application Analysis** page shows statistics of application traffic matching traffic analysis policies. You can perform the following operations on application analysis data:

- Automatically refresh data.

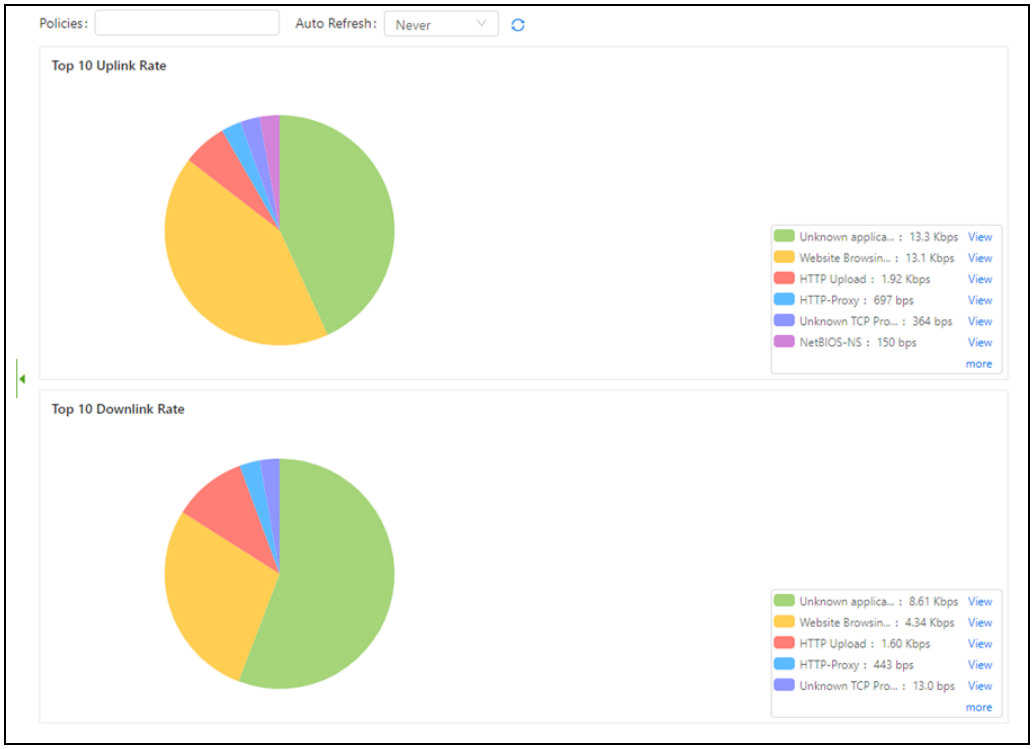
  Set the automatic refresh interval and click . Then the system will automatically refresh application analysis data at the specified interval.

- Manually refresh data.

  Click to refresh application analysis data manually on the current page.

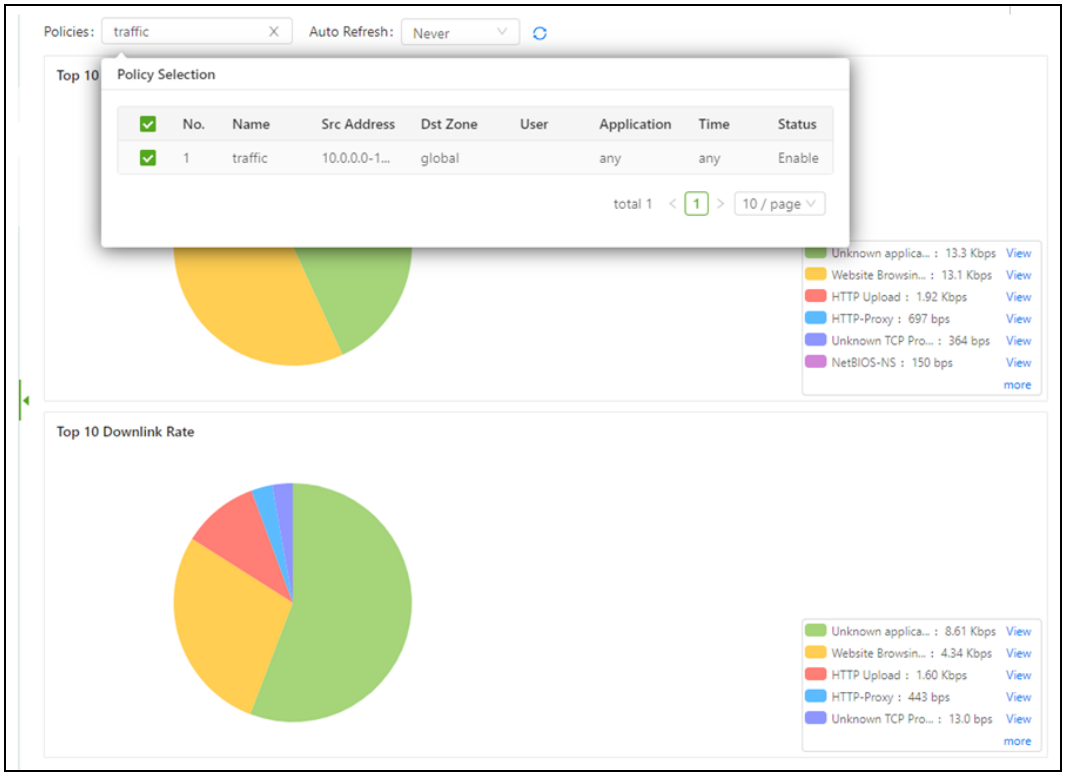
  By default, this page shows top 10 uplink rates and top 10 downlink rates of application traffic matching each traffic analysis policy. Alternatively, you can select one or more policies to view statistics of traffic matching the policies.

Figure 4-10 Viewing overall application analysis data



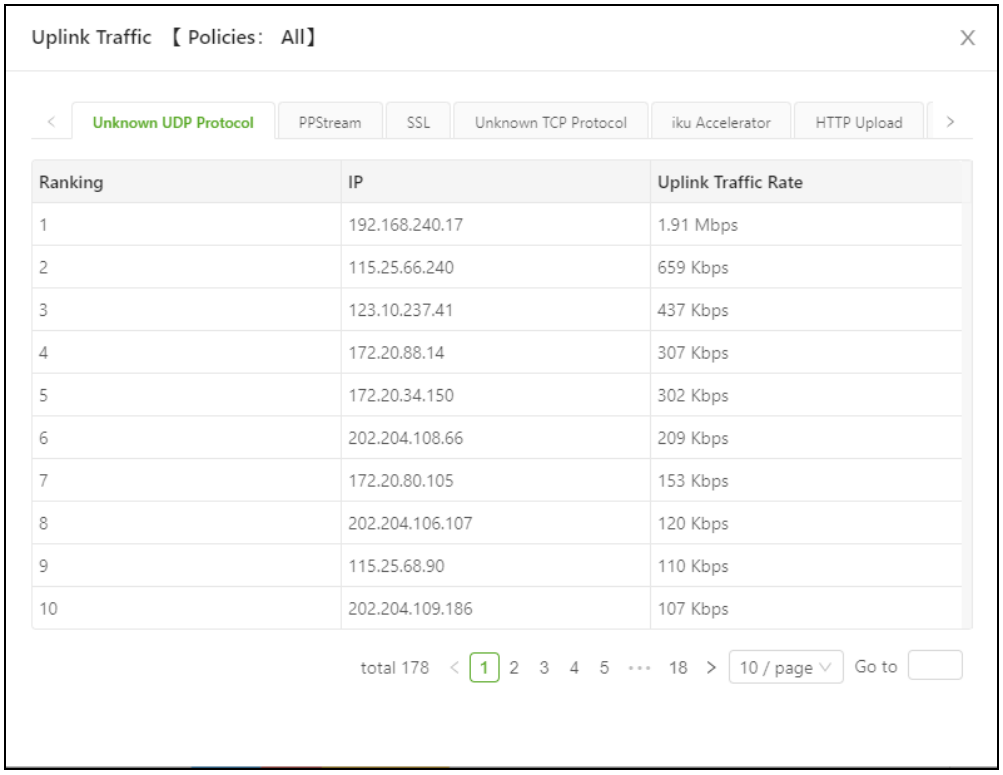
Click in the **Policies** text box, select a policy, and click the refresh icon to view analysis data of applications covered by this policy.

Figure 4-11 Viewing analysis data of applications covered by a specific policy



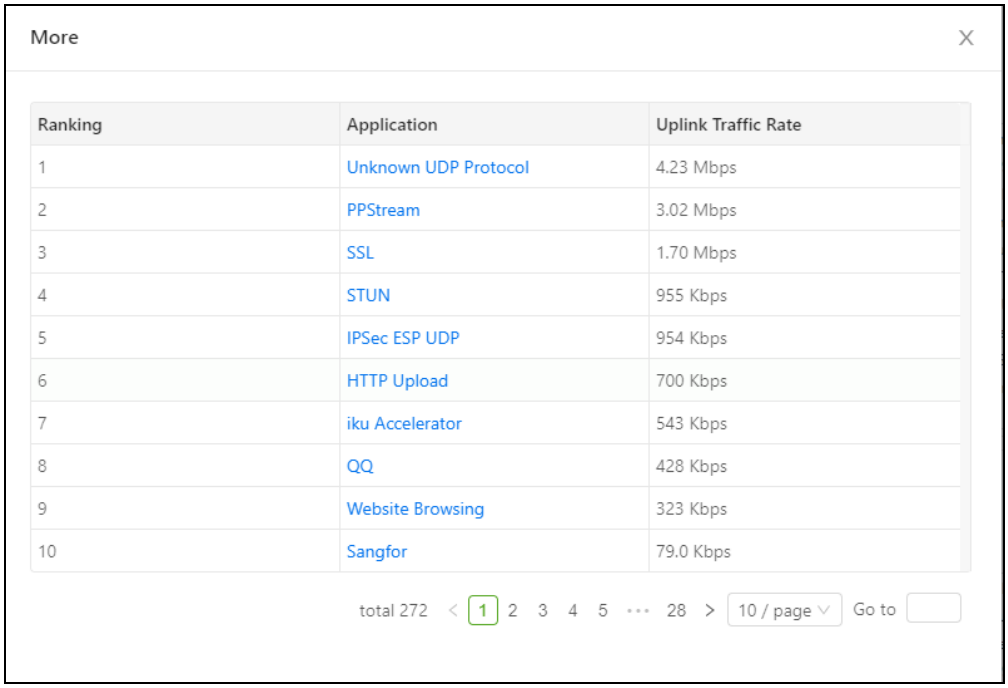
On the page shown in Figure 4-10, click **View** to the right of the application name to view rankings of the uplink or downlink traffic rates of the application covered by the selected policy.

Figure 4-12 Viewing uplink traffic



Click **more** below the list in the **Uplink Rate Top10** or **Downlink Rate Top10** panel shown in Figure 4-10 to view more application traffic monitoring information.

Figure 4-13 Viewing more application traffic monitoring information



4.2.3 IP Analysis

Choose **Traffic > Traffic Analysis > IP Analysis**. The **IP Analysis** page shows statistics of IP traffic matching traffic analysis policies. You can perform the following operations on IP traffic analysis data:

- Automatically refresh data.

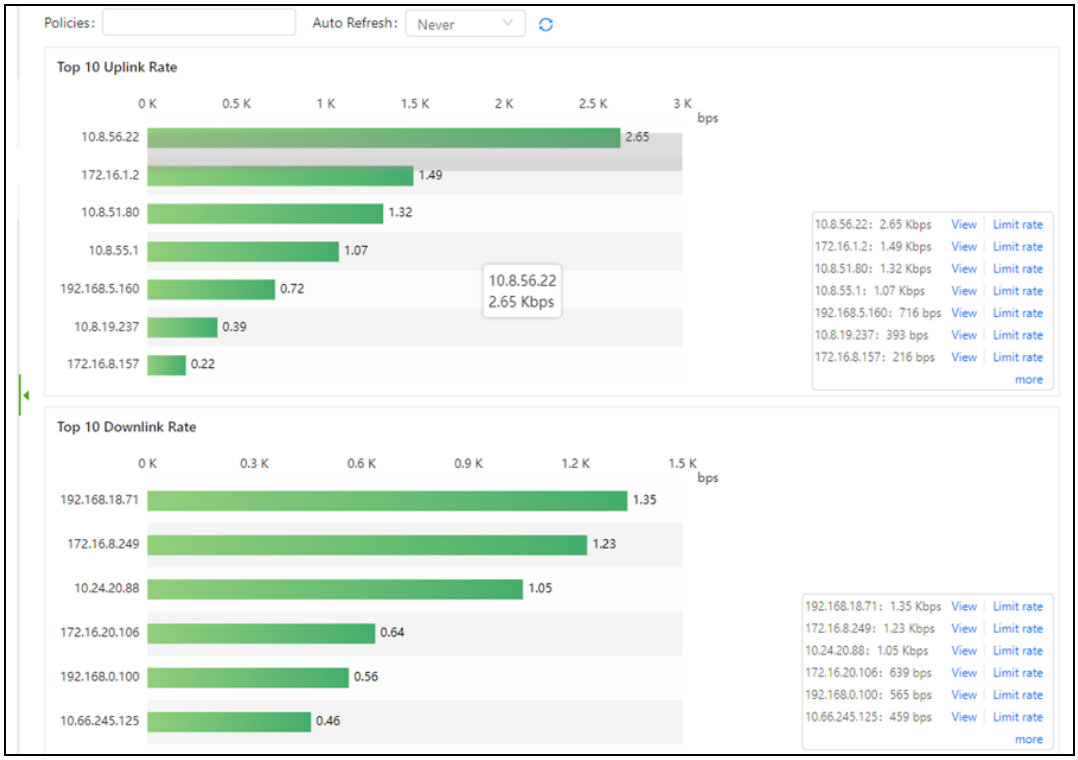
  Set the automatic refresh interval and click . Then the system will automatically refresh IP traffic analysis data at the specified interval.

- Manually refresh data.

  Click to refresh IP traffic analysis data manually on the current page.

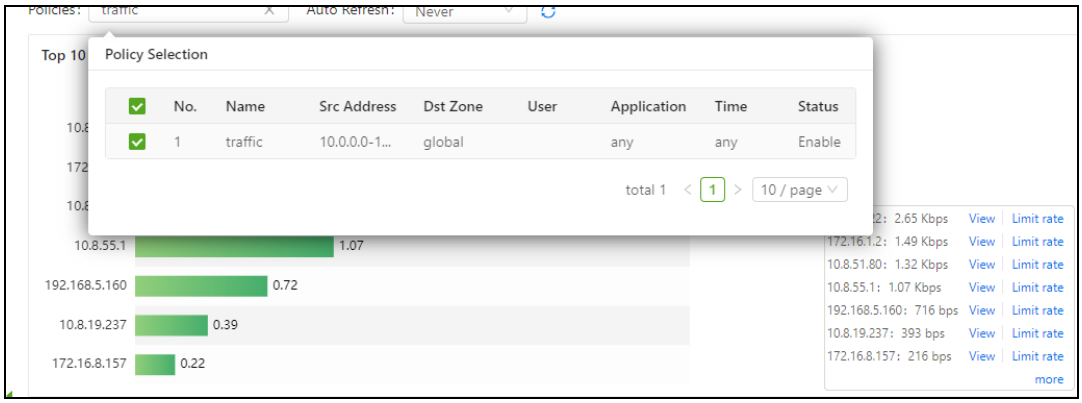
  By default, this page shows top 10 uplink rates and top 10 downlink rates of IP traffic matching each traffic analysis policy. Alternatively, you can select one or more policies to view statistics of traffic matching the policies.

Figure 4-14 Viewing overall IP traffic analysis data



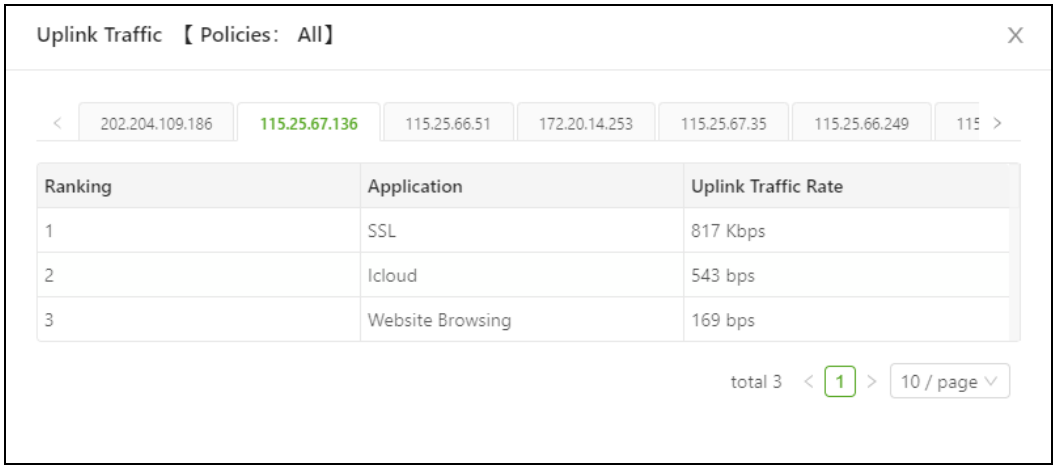
You can select a specific traffic analysis policy to view traffic analysis data of IP addresses covered by this policy.

Figure 4-15 Viewing traffic analysis data of IP addresses covered by a specific policy



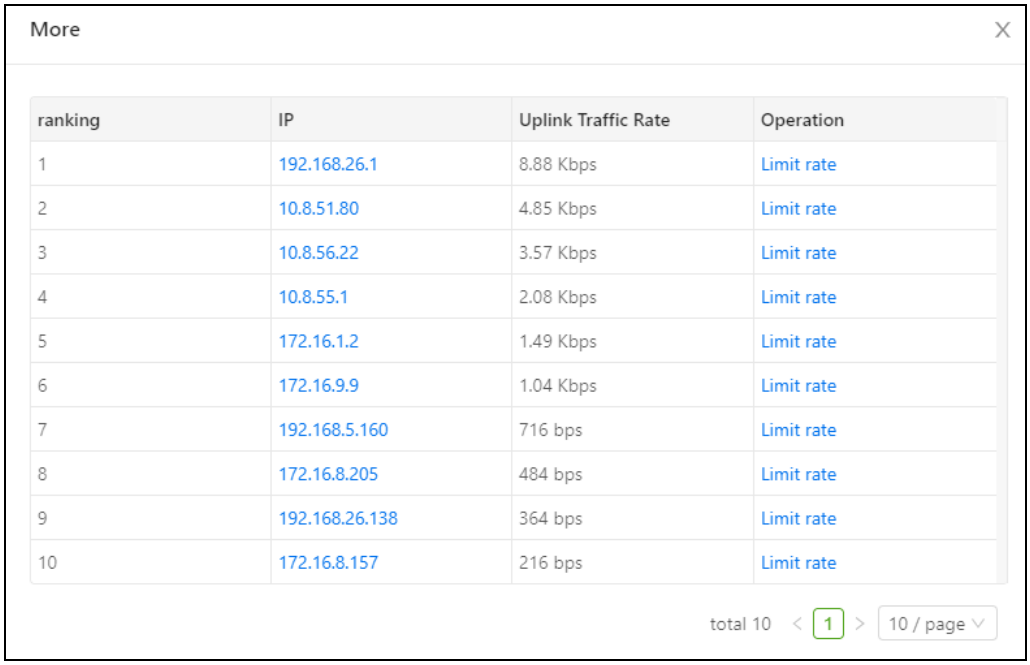
On the page shown in Figure 4-14, click **View** to the right of an IP address to view rankings of the uplink or downlink traffic rates of the IP address covered by the selected policy.

Figure 4-16 Viewing uplink traffic



Click **more** below the list in the **Uplink Rate Top10** or **Downlink Rate Top10** panel shown in Figure 4-14 to view more traffic monitoring information of IP sessions.

Figure 4-17 Viewing more traffic monitoring information of IP sessions

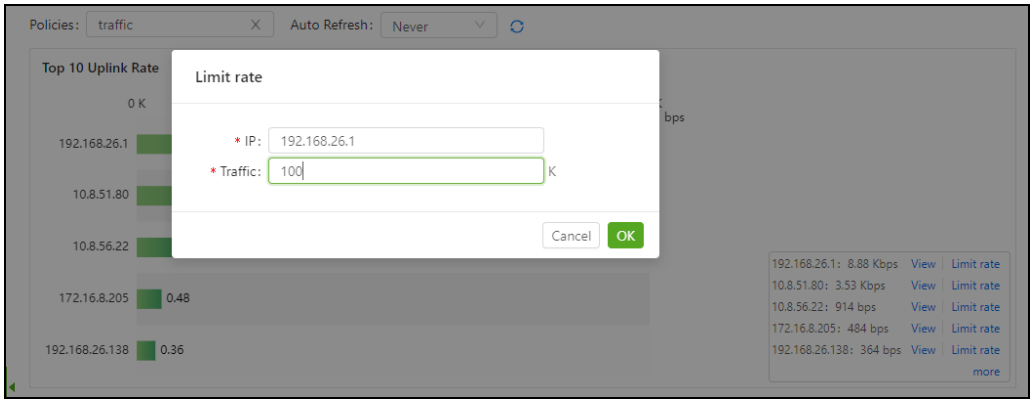


One-Click Rate Limit

The one-click rate limit function allows you to configure a bandwidth management policy on the **Bandwidth Management** page for managing IP-specific traffic.

Step 1 On the page shown in Figure 4-17 or Figure 4-14, click **Limit rate** to the right of a specific IP address.

Figure 4-18 Limiting the traffic rate of a specific IP address



Step 2 Set **Traffic** to the maximum traffic allowed for the IP address.

Step 3 Click **OK**. After parameters are properly specified, the system will automatically perform the following operations:

- Creates a bandwidth management policy for this source IP address.
- Automatically checks whether a line with the same name exists on NIPS. If yes, the system directly references such line. If not, the system adds a new line, which will be referenced in the bandwidth management policy. For details about traffic management policies and lines, see Bandwidth Management.
- Adds a new bandwidth management profile named **speedlimit***** as shown in Figure 4-19. This profile object will be referenced in bandwidth management policies, as shown in Figure 4-20.

Figure 4-19 Automatically added bandwidth management profile

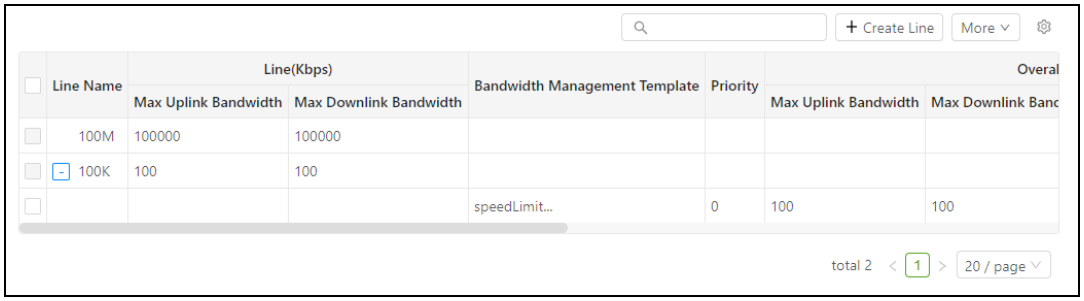
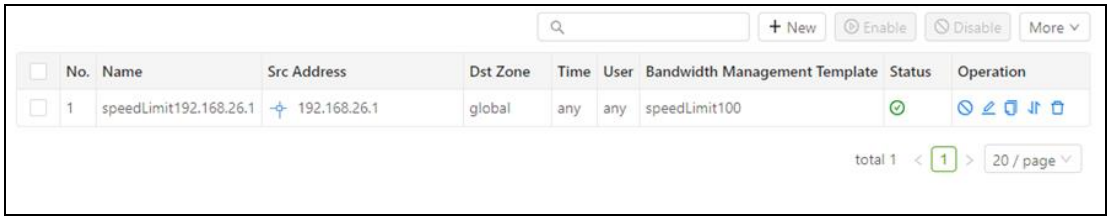


Figure 4-20 Automatically added bandwidth management policy



----End

4.2.4 Traffic Integrity Distribution

The traffic integrity distribution module consists of traffic integrity statistics, packet loss trend, and session monitoring.

4.2.4.1 Traffic Integrity Statistics

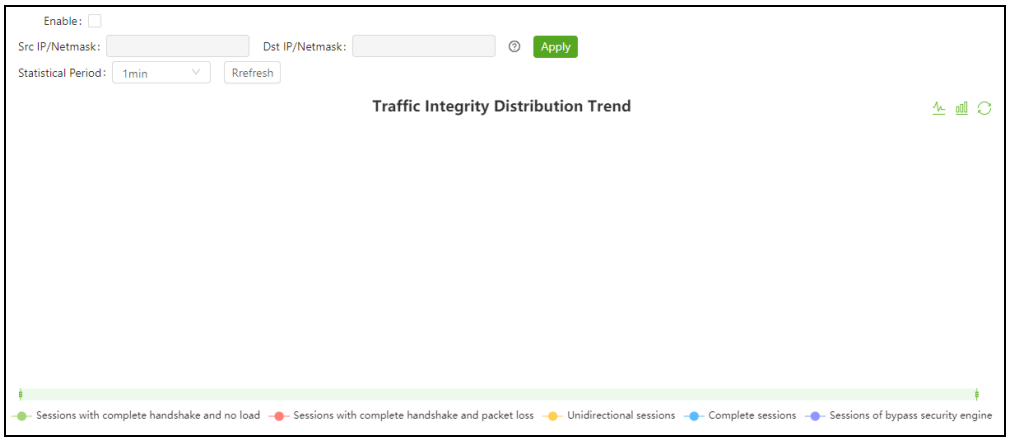
The application traffic integrity statistics function collects statistics on the total number, proportion, and trend of six types of sessions: Sessions with an incomplete three-way handshake, sessions with complete handshake and packet loss, unidirectional sessions, complete sessions, sessions of bypass security engine, and sessions with a complete handshake complete but no load. This function is disabled by default as it may affect the system performance when enabled.

After the application traffic integrity statistics function and packet loss statistics function are enabled, you can view the integrity distribution trend graph, packet loss trend graph, and session monitoring within the statistical period.

Step 1 Choose **Traffic > Traffic Analysis > Traffic Integrity Distribution**.

The **Traffic Integrity Statistics** page appears.

Figure 4-21 Traffic integrity distribution trend



Step 2 Select the **Enable** checkbox to enable the traffic integrity statistics function.

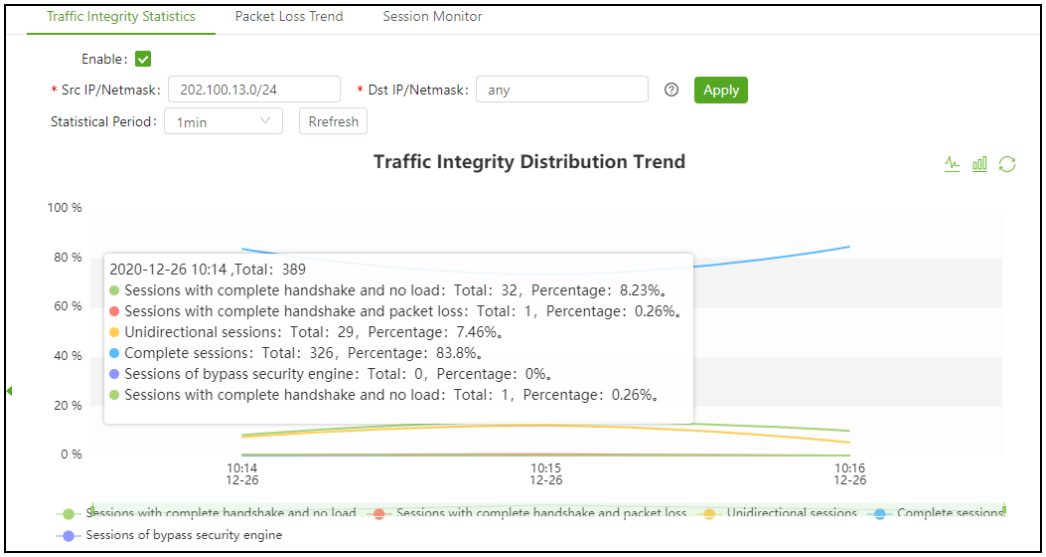
Step 3 Configure **Src IP/Netmask** and **Dst IP/Netmask**.

- The two parameters cannot be both **any**.
- You can type multiple IP addresses, separated by the comma (,).
- The netmask value range is 24–32 for IPv4 or 96–128 for IPv6, for example, 1.1.1.1/24 or 2002::1510:20691/96.

Step 4 Click **Apply** to enable integrity statistics.

Then you can view the statistics.

Figure 4-22 Viewing integrity statistics



Step 5 (Optional) Modify the statistical period.

The statistical period is 1 minute by default which can be changed to 5 or 10 minutes. After the parameter modification, you can click **Refresh** to commit the setting.

Step 6 (Optional) Switch to the histogram.

By default, the line chart is displayed. You can click to switch to the histogram or to switch back to the original chart.

----End

Traffic Integrity Distribution Trend

As shown Figure 4-21, the **Traffic Integrity Distribution Trend** area shows the distribution trend graph of different types of session. Pointing to a curve shows the total number of all sessions and each type of session at a specific time point. The traffic integrity distribution can be shown as a line chart or histogram, as shown in Figure 4-23 and Figure 4-24.

Figure 4-23 Application traffic integrity trend – line chart

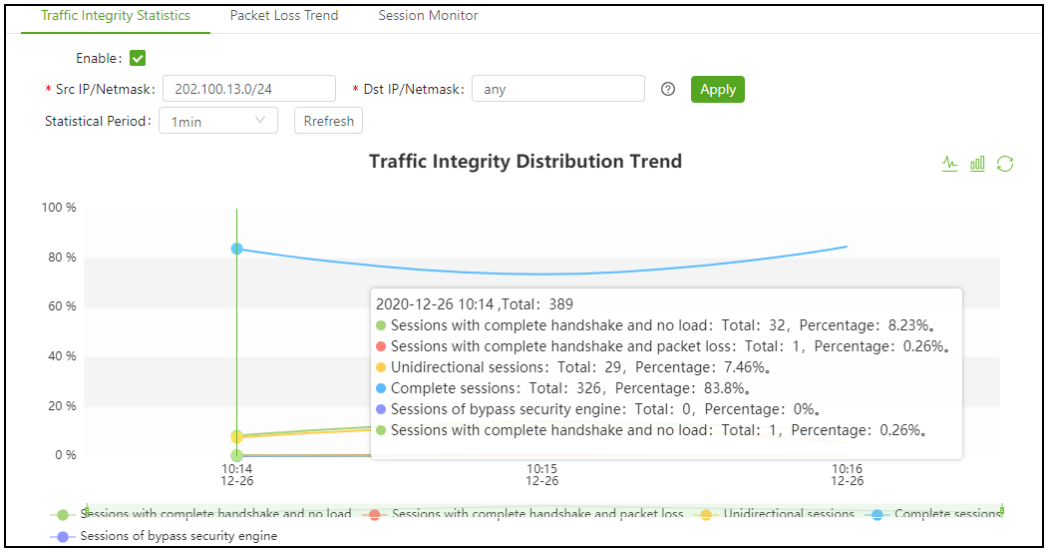
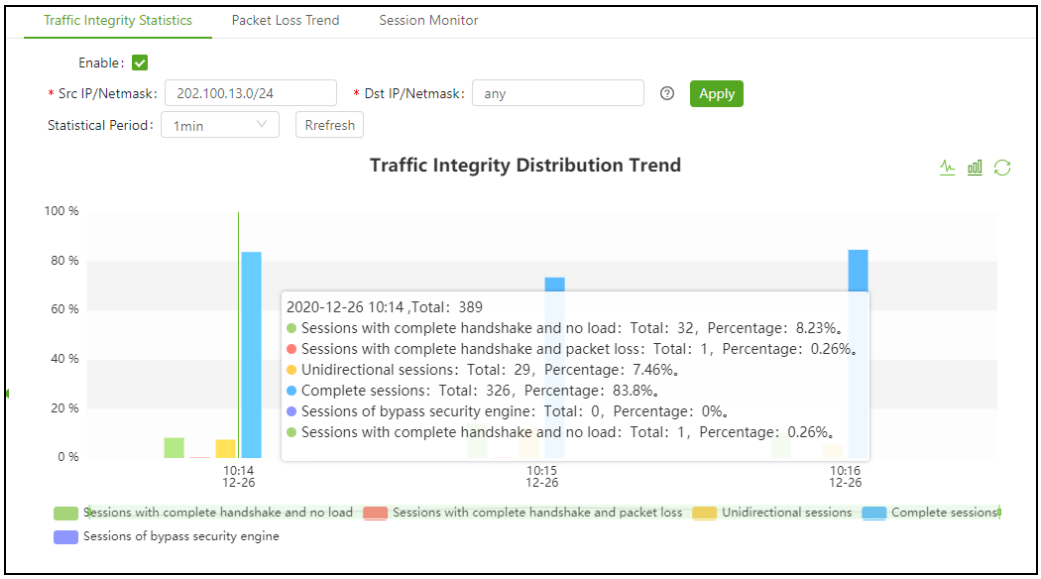


Figure 4-24 Application traffic integrity trend – histogram



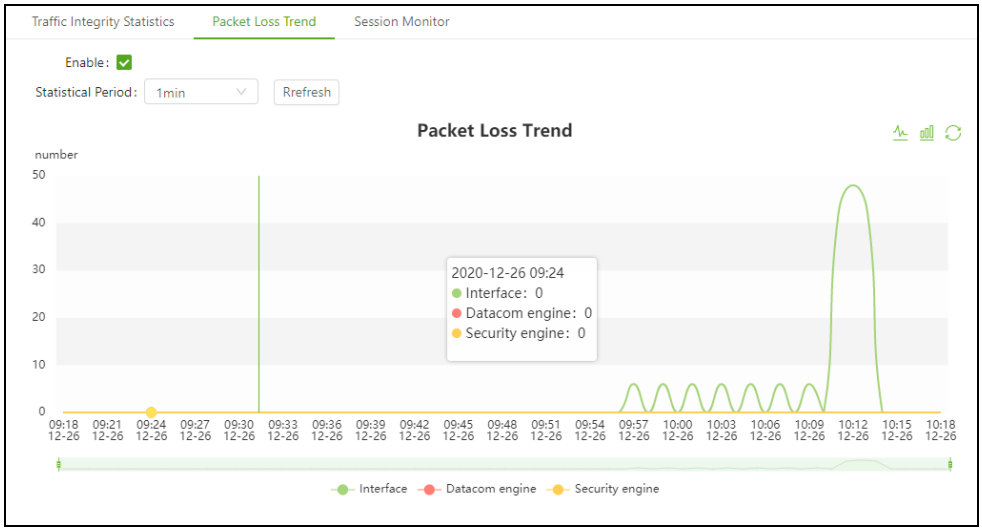
4.2.4.2 Packet Loss Trend

On the **Packet Loss Trend** page, you can enable the packet loss statistics function to view the packet loss trend within a statistical period (1 minute by default).

Step 1 Choose **Traffic > Traffic Analysis > Traffic Integrity Distribution**.

The **Packet Loss Trend** page appears.

Figure 4-25 Packet loss trend



Step 2 Select the **Enable** checkbox to view the packet loss trend.

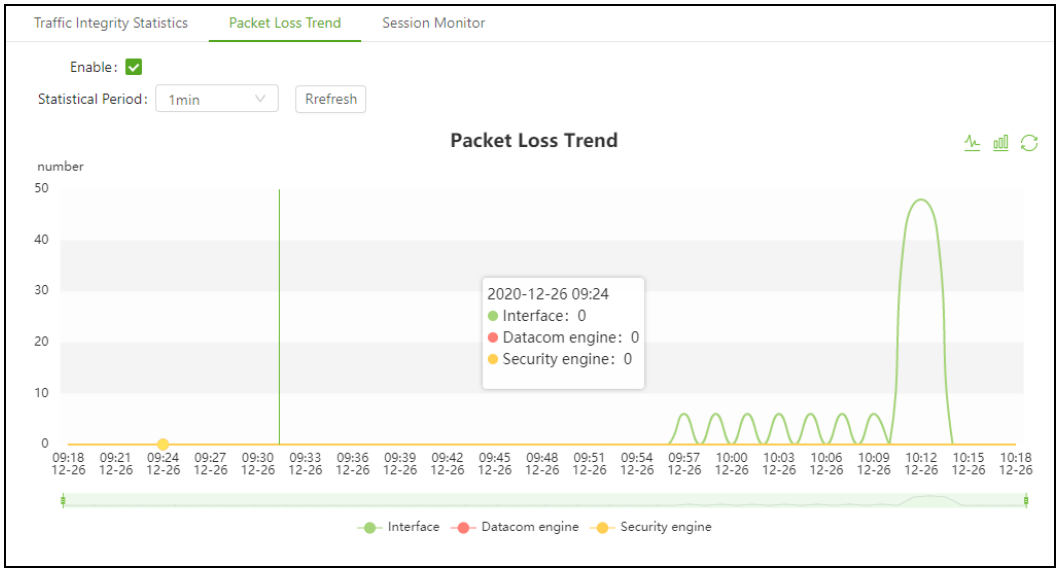
Step 3 Set the statistical period.

The statistical period is 1 minute by default which can be changed to 5 or 10 minutes.

Step 4 Click **Refresh** to view statistics.

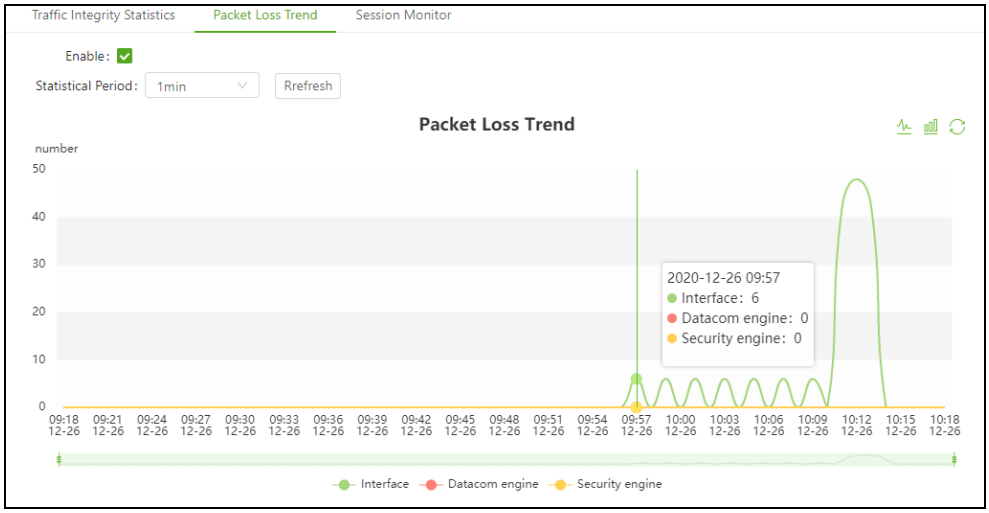
By default, the packet loss trend is shown as a line chart.

Figure 4-26 Packet loss trend



On the line chart, the packet loss trend is displayed in different colored curves for interfaces and the data communication engine and security engine. Pointing to a curve shows the total number of sessions of all types and each type at a specific time point.

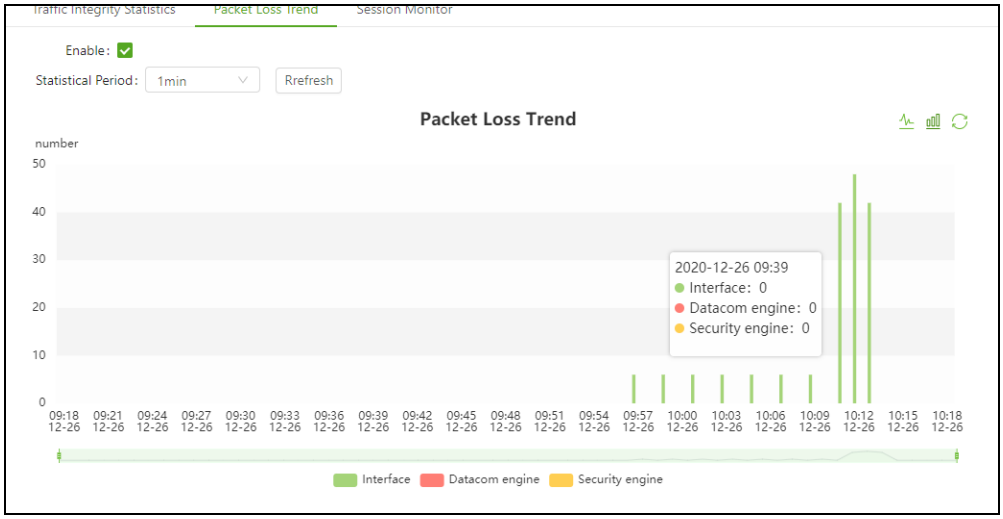
Figure 4-27 Viewing the packet loss trend at a specific time point



Step 5 Switch the display mode.

Click to switch to the histogram.

Figure 4-28 Viewing the packet loss trend - histogram



----End

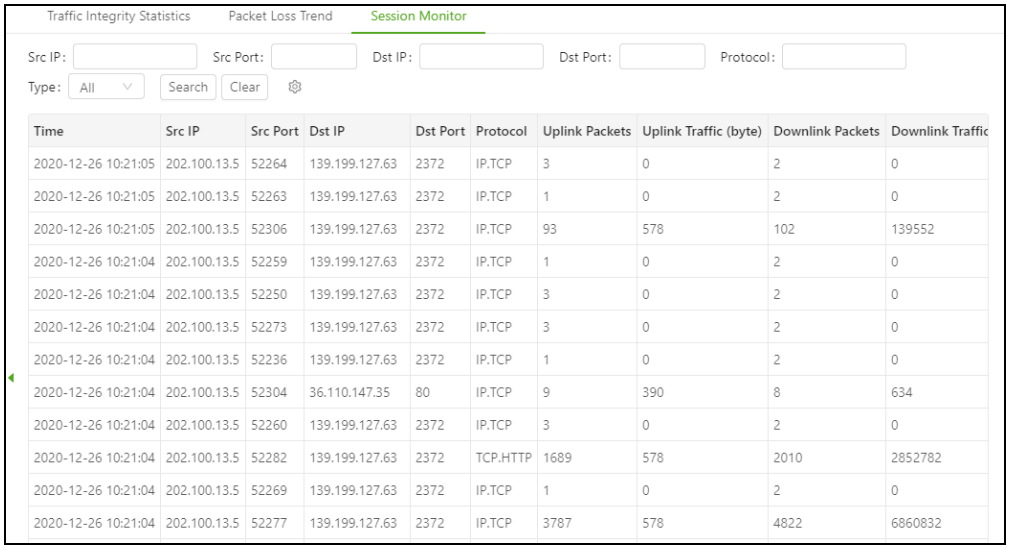
4.2.4.3 Session Monitoring

On the **Session Monitor** page, you can view session details amid application traffic integrity statistics.

Step 1 Choose **Traffic > Traffic Analysis > Session Monitor**.

The **Session Monitor** page appears.

Figure 4-29 Session monitoring



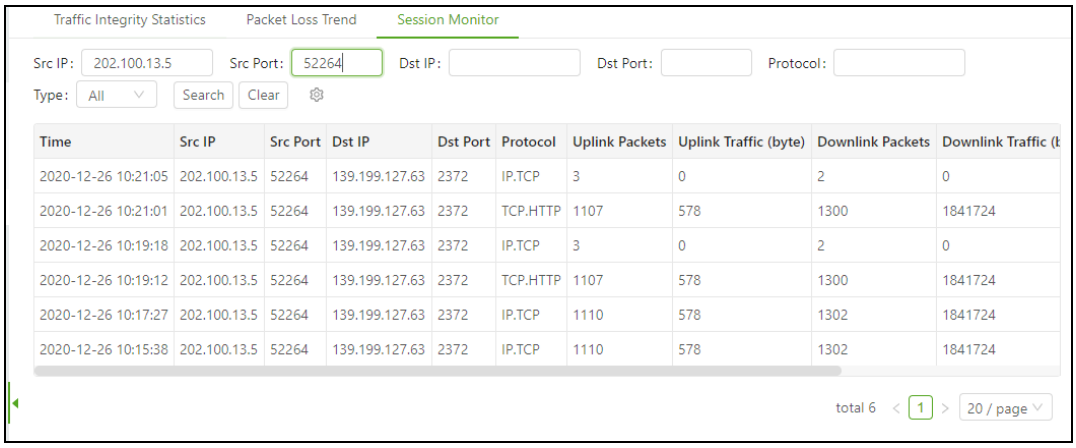
Time	Src IP	Src Port	Dst IP	Dst Port	Protocol	Uplink Packets	Uplink Traffic (byte)	Downlink Packets	Downlink Traffic
2020-12-26 10:21:05	202.100.13.5	52264	139.199.127.63	2372	IP.TCP	3	0	2	0
2020-12-26 10:21:05	202.100.13.5	52263	139.199.127.63	2372	IP.TCP	1	0	2	0
2020-12-26 10:21:05	202.100.13.5	52306	139.199.127.63	2372	IP.TCP	93	578	102	139552
2020-12-26 10:21:04	202.100.13.5	52259	139.199.127.63	2372	IP.TCP	1	0	2	0
2020-12-26 10:21:04	202.100.13.5	52250	139.199.127.63	2372	IP.TCP	3	0	2	0
2020-12-26 10:21:04	202.100.13.5	52273	139.199.127.63	2372	IP.TCP	3	0	2	0
2020-12-26 10:21:04	202.100.13.5	52236	139.199.127.63	2372	IP.TCP	1	0	2	0
2020-12-26 10:21:04	202.100.13.5	52304	36.110.147.35	80	IP.TCP	9	390	8	634
2020-12-26 10:21:04	202.100.13.5	52260	139.199.127.63	2372	IP.TCP	3	0	2	0
2020-12-26 10:21:04	202.100.13.5	52282	139.199.127.63	2372	TCP.HTTP	1689	578	2010	2852782
2020-12-26 10:21:04	202.100.13.5	52269	139.199.127.63	2372	IP.TCP	1	0	2	0
2020-12-26 10:21:04	202.100.13.5	52277	139.199.127.63	2372	IP.TCP	3787	578	4822	6860832

This page presents the latest 1000 entries of session monitoring data.

Step 2 Filter session monitoring information.

You can specify the source IP address, destination IP address, source port, destination port, protocol, and type and then click **Search** to find desired session monitoring information.

Figure 4-30 Querying session information based on a source IP address



Time	Src IP	Src Port	Dst IP	Dst Port	Protocol	Uplink Packets	Uplink Traffic (byte)	Downlink Packets	Downlink Traffic (b
2020-12-26 10:21:05	202.100.13.5	52264	139.199.127.63	2372	IP.TCP	3	0	2	0
2020-12-26 10:21:01	202.100.13.5	52264	139.199.127.63	2372	TCP.HTTP	1107	578	1300	1841724
2020-12-26 10:19:18	202.100.13.5	52264	139.199.127.63	2372	IP.TCP	3	0	2	0
2020-12-26 10:19:12	202.100.13.5	52264	139.199.127.63	2372	TCP.HTTP	1107	578	1300	1841724
2020-12-26 10:17:27	202.100.13.5	52264	139.199.127.63	2372	IP.TCP	1110	578	1302	1841724
2020-12-26 10:15:38	202.100.13.5	52264	139.199.127.63	2372	IP.TCP	1110	578	1302	1841724

Step 3 Click **Clear** to clear query results.

----End

4.3 NetFlow Configuration

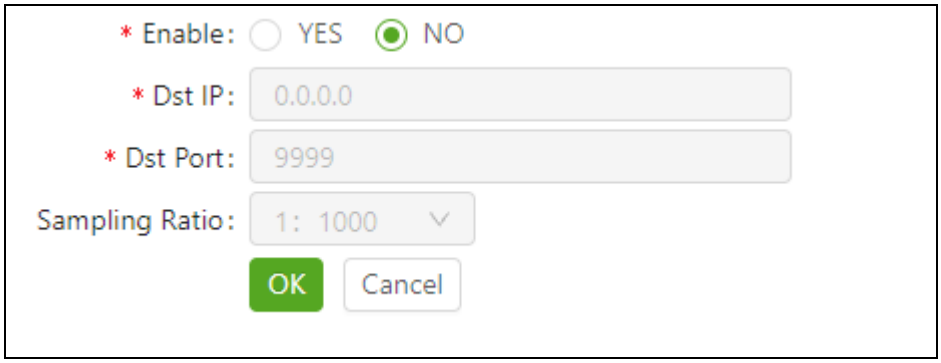
When collaborating with NSFOCUS Network Traffic Analyst (NTA), NIPS can identify DDoS attacks more effectively. When NIPS and NTA are deployed for this purpose, the

switch may not support NetFlow. In this case, you must configure NetFlow on NIPS by performing the following steps:

Step 1 Choose **Traffic** > **NetFlow**.

On the **NetFlow** page, the NetFlow feature is disabled by default.

Figure 4-31 Netflow



Step 2 Select **Yes** for **Enable**.

Figure 4-32 Enabling NetFlow

Step 3 Configure parameters.

Table 4-5 NetFlow parameters

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

Parameter	Description
Sampling Ratio	Specifies the likelihood of packets being encapsulated into NetFlow packets. By default, the sampling ratio is **1: 1000**, indicating that one out of 1000 packets will be encapsulated into NetFlow packets. The sampling ratio can be **1:10000**, **1:1000**, **1:100**, **1:1**, or a desired custom value.

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

Step 5 Click **Commit** in the quick access bar to make the security policy take effect.

----End

5 Log

The log module allows you to configure report profiles for generating reports in addition to querying security logs, online behavior logs, O&M logs, malicious file archive logs, and data maintenance logs.

This chapter contains the following sections:

Section	Description
Security Log	Describes how to query and manage security logs.
Network Behavior	Describes how to query and manage online behavior logs.
O&M Log	Describes how to query and manage operating logs and hardware logs.
Malware Archive	Describes how to manage archived malicious files and how to send them externally.
Data Maintenance	Describes how to maintain configurations, back up logs, and view the backup history.
Report	Describes how to manage report profiles and report files.

For security logs, online behavior logs, and O&M logs, the following basic operations can be performed in a similar way.

Setting Log Fields to Be Displayed

You can determine which log fields are displayed by clicking ⚙ to the upper right of the log table.

Filtering Logs

At the top of the log page, you can specify both default and optional log filtering conditions to query logs.

- Default filtering conditions: **Time**, **Severity**, **Action**, and **Signature ID**.
- You can click **Filter** to select a filtering condition from the drop-down list to add it to the log query area. More than one condition can be added.

Then you can click **Search** to query desired logs which will be shown in the log table.

Viewing Logs

- Click + preceding a log to view log details, including but not limited to basic information, source information, destination information, threat information, attack forensics, and handling suggestions.
- Click the source or destination IP address to view detailed threat intelligence of the address on NTI. If the source or destination IP address is an external one, it is indicated in blue and preceded by .
- Click the event name to open the event details dialog box where you can view event details and click the vulnerability title, NSFOCUS ID, CVE ID, or other blue links to view vulnerability details.

Exporting Logs

Click **Export** and select a file export format to export all listed logs and save them to a local disk drive.

Confirming Events

After viewing an event log, you can confirm this event. Upon confirmation, the event status is changed to **Confirmed**.

- Point to in the **Operation** column of an event log and click **Confirm** to complete log confirmation.
- Select multiple logs from the log table and click **Confirm** to confirm the selected logs.
- Point to **More** and click **Confirm all** to confirm all logs in the log table.

Also, you can cancel confirmation of events that are confirmed in the same way as they are confirmed.

Deleting Logs

- Point to in the **Operation** column of a log and click **Delete** to delete the log.
- Select multiple logs, point to **More**, and click **Delete selected** to delete the selected logs.
- Point to **More** and click **Delete all** to delete all logs in the table.

5.1 Security Log

The security log module involves ten types of log, including network intrusion logs, malicious file logs, web security logs, and advanced threat logs.

5.1.1 Network Intrusion

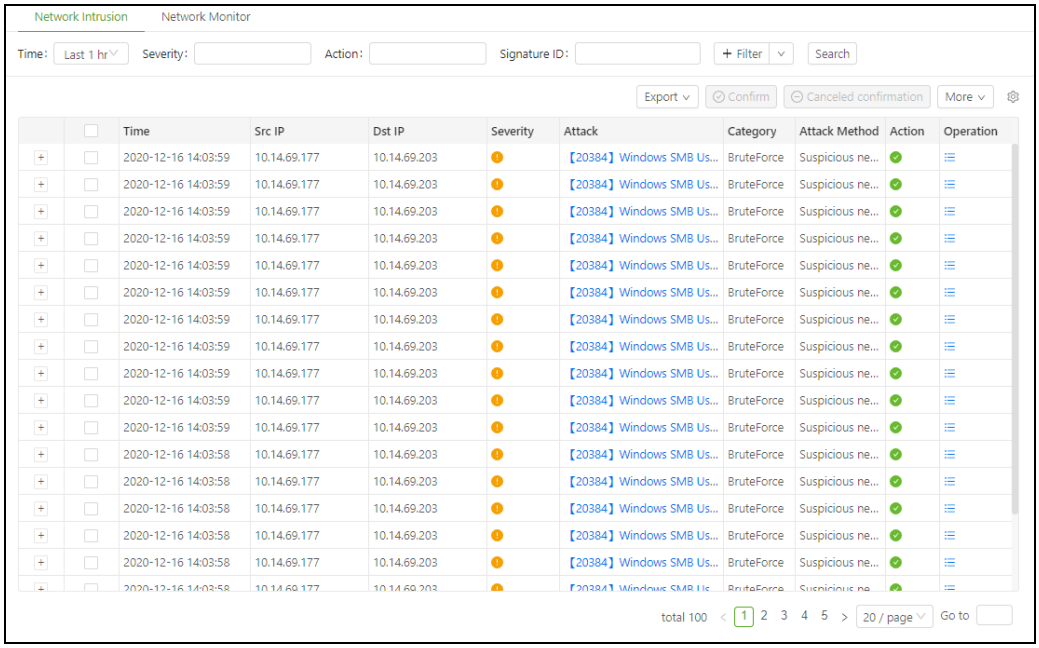
The network intrusion module involves intrusion events and monitoring events.

5.1.1.1 Intrusion Event

Intrusion event logs can be generated only after intrusion event profiles are configured and referenced in global security policies.

Choose **Log > Security Log > Network Intrusion**. The **Network Intrusion** page shows network intrusion logs.

Figure 5-1 Intrusion events



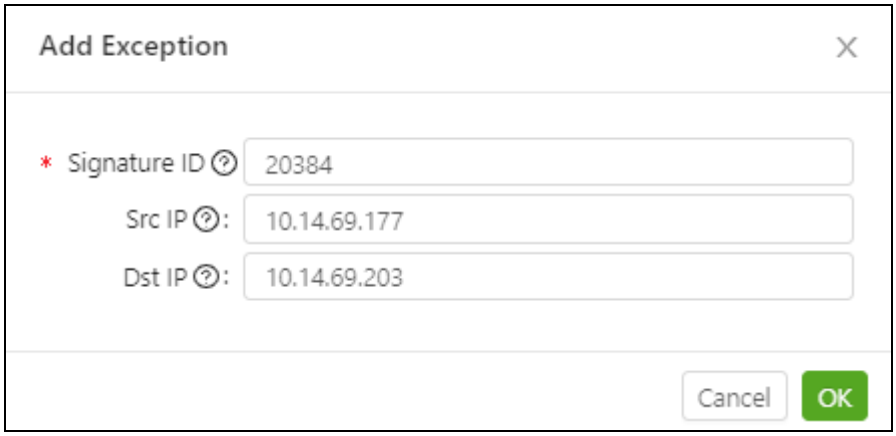
Besides basic operations, you can perform the operations specific to intrusion events: adding an exception, downloading a PCAP file, and feeding back to the vendor.

Adding an Exception

If you do not want NIPS to check intrusion events against a certain rule, you can add this rule as an exception.

Step 1 Point to in the **Operation** column of an intrusion event and click **Add exception**.

Figure 5-2 Adding a rule to exception



Step 2 Configure parameters in **Add Exception** dialog box.

Table 5-1 Parameters for configuring an exception rule

Parameter	Description
Signature ID	ID of rule added as an exception. This ID must be the ID of an existing rule.
Src 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/IPv6 address or segment. Typing **0.0.0.0** or leaving the field empty indicates no limit.
Dst IP	Specifies the destination IP address or IP segment, that is, the valid range of destination 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/IPv6 address or segment. Typing **0.0.0.0** or leaving the field empty indicates no limit.

Step 3 Click **OK**.

You can view and cancel this exception rule under **Objects** > **Network Intrusion** > **Exceptions**.

Step 4 Click **Commit** in the quick access bar to make the security policy take effect.

----End

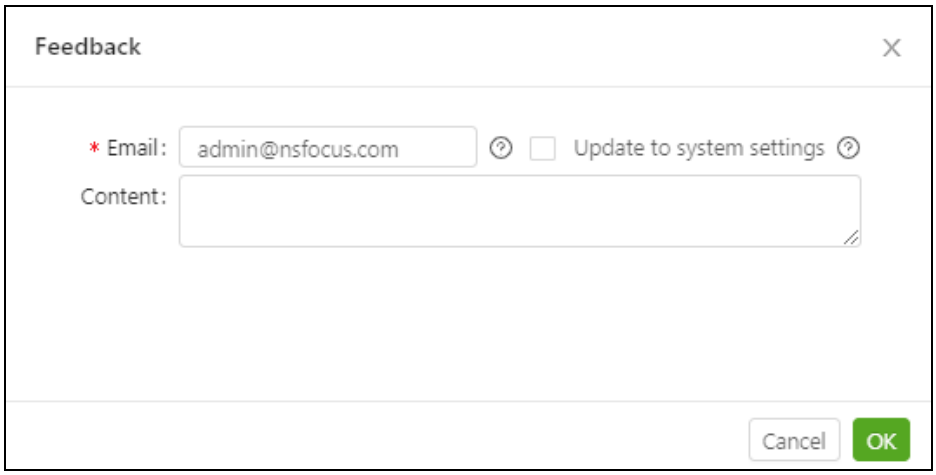
Downloading a PCAP File

If the packet capture option is selected in a rule referenced in a security policy profile triggering an event, you can point to in the **Operation** column of the event log and then click **Download PCAP file** to download the packet capture file of this event for analysis and debugging.

Feeding Back to the Vendor

If you consider an intrusion log as a false positive, you can point to in the **Operation** column of the log, click **Feedback**, and type feedback information to inform NSFOCUS rule group.

Figure 5-3 Typing feedback information



- **Email**: specifies the email address for receiving feedback replies from the vendor. 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 the email address typed here and uses it as the default email address for sending feedback information to the vendor. For details on email address configuration, see Mail Server.
- **Content**: brief feedback to the vendor.

Click **OK**. The system sends false positives as configured. After the false positive is successfully sent, a message indicating feedback success appears.

5.1.1.2 Monitoring Event

Monitoring event logs can be generated only after network intrusion profiles are configured and referenced in global security policies.

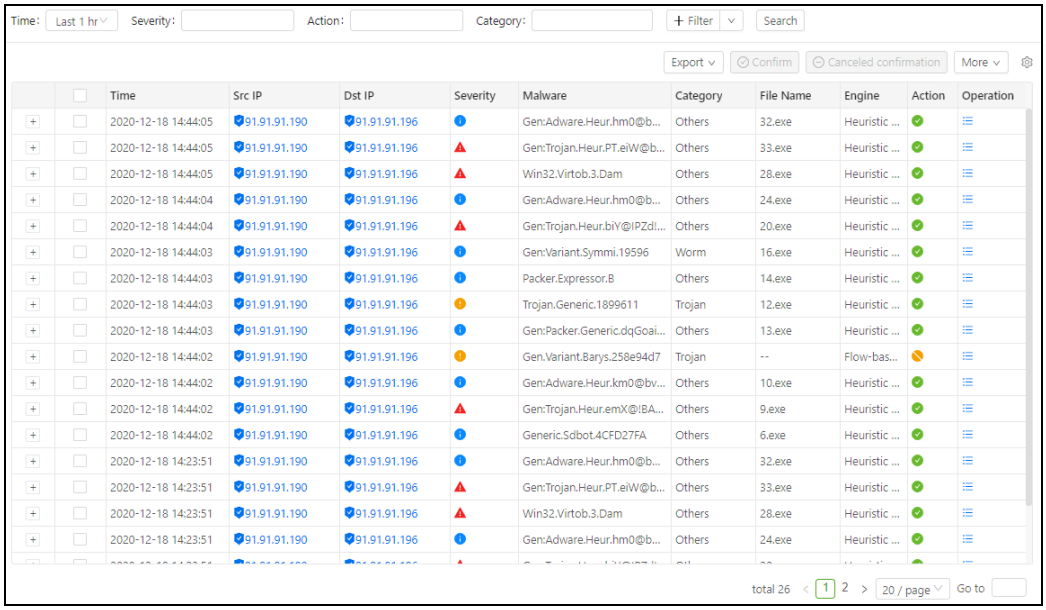
Choose **Log** > **Security Log** > **Network Intrusion** > **Network Monitor**. On the **Network Monitor** page, you can manage monitoring event logs in the same way as intrusion event logs.

5.1.2 Malious File

Malicious file logs can be generated only after malicious file profiles are configured and referenced in global security policies.

Choose **Log** > **Security Log** > **Malware**. The malware log page shows malicious file logs.

Figure 5-4 Malicious file logs



In addition to basic operations, you can point to in the **Operation** column of a log to add the file to the whitelist.

Adding an Entry to the Whitelist

If an engine other than the flow-based antivirus engine is used as the detection engine in a malicious file profile referenced in a global security policy triggering a malicious file log, you can add the malicious file to the file sample whitelist.

You can point to in the **Operation** column and then click **Add to whitelist** to add the malicious file to the file sample whitelist. Then, this file will be deemed a legitimate file and no longer subject to detections for suspicious files. For details about the file sample whitelist, see File Whitelist.

5.1.3 Web Security

Web security logs consist of malicious URL logs and injection attack logs.

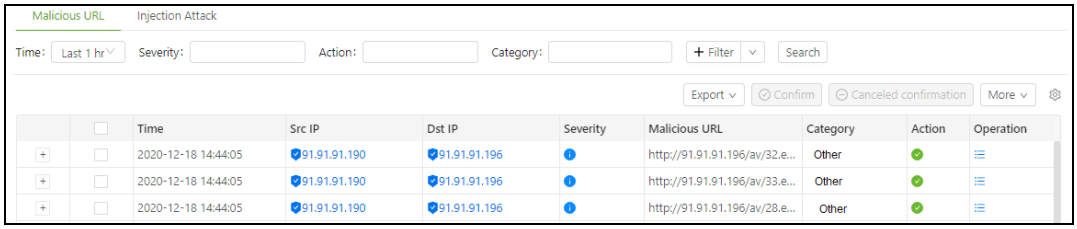
5.1.3.1 Malicious URL

Malicious URL logs can be generated only after malicious URL detection is enabled in web security profiles that are referenced in global security policies.

Choose **Log** > **Security Log** > **Web Security**.

The **Malicious URL** page lists malicious URL logs.

Figure 5-5 Malicious URL logs



In addition to basic operations, you can feed back false positives to the vendor and add URLs to the whitelist.

Feeding Back to the Vendor

If you consider a malicious URL log as a false positive, you can point to in the **Operation** column of the log, click **Feedback**, and type feedback information to inform NSFOCUS rule group.

For details on feedback parameters, see Feeding Back to the Vendor.

Adding an Entry to the Whitelist

You can add URLs indicated in logs to the whitelist only after malicious URL detection is enabled in web security profiles referenced in global security policies triggering malicious URL logs.

For details, see Adding an Entry to the Whitelist.

5.1.3.2 Injection Attack

Injection attack logs can be generated only after SQL injection detection is enabled in web security profiles that are referenced in global security policies.

Choose **Log > Security Log > Web Security > Injection Attack**. The **Injection Attack** page shows injection attack logs. Injection attack logs are operated in the same way as malicious URL logs. For details, see Malicious URL.

5.1.4 Advanced Threat

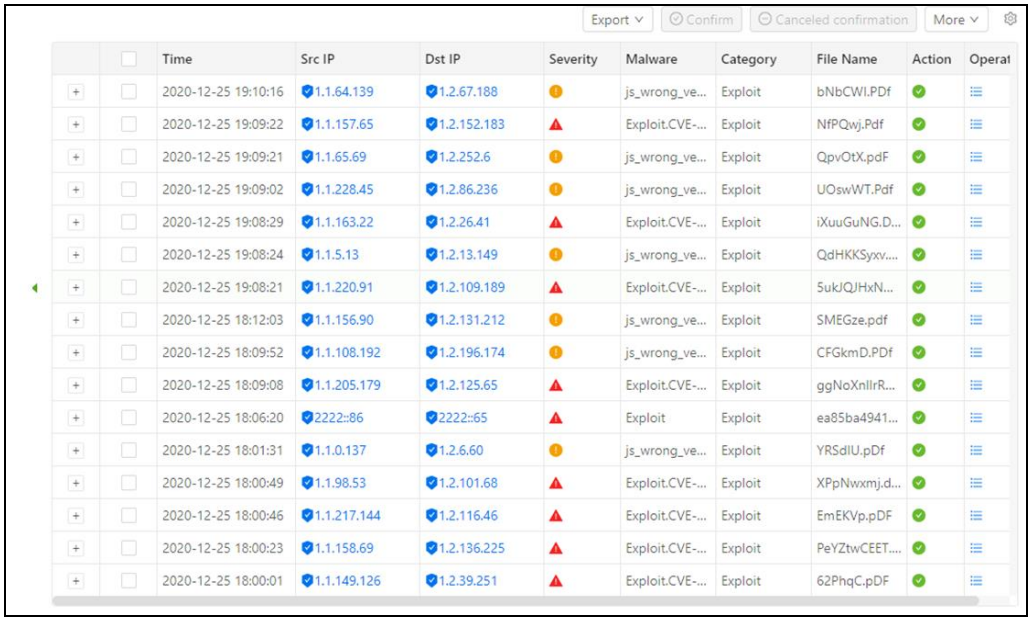
The advanced threat module encompasses advanced malicious sample logs and callback block event logs.

5.1.4.1 Advanced Malicious Sample

Collaborate with TAC or a cloud-side sandbox, NIPS can obtain the latest advanced malicious sample detection logs.

Choose **Log > Security Log > Advanced Threat > Malware Sample**. The **Malware Sample** page shows advanced malicious sample detection logs.

Figure 5-6 Advanced malicious sample detection logs



Export | Confirm | Canceled confirmation | More

Time	Src IP	Dst IP	Severity	Malware	Category	File Name	Action	Operat
2020-12-25 19:10:16	1.1.64.139	1.2.67.188		js_wrong_ve...	Exploit	bNbCWI.PDf		
2020-12-25 19:09:22	1.1.157.65	1.2.152.183		Exploit.CVE-...	Exploit	NfPQwj.Pdf		
2020-12-25 19:09:21	1.1.65.69	1.2.252.6		js_wrong_ve...	Exploit	QpvOtX.pdF		
2020-12-25 19:09:02	1.1.228.45	1.2.86.236		js_wrong_ve...	Exploit	UOswWT.Pdf		
2020-12-25 19:08:29	1.1.163.22	1.2.26.41		Exploit.CVE-...	Exploit	iXuuGuNG.D...		
2020-12-25 19:08:24	1.1.5.13	1.2.13.149		js_wrong_ve...	Exploit	QdHKKSyxv....		
2020-12-25 19:08:21	1.1.220.91	1.2.109.189		Exploit.CVE-...	Exploit	5ukJQJHxN...		
2020-12-25 18:12:03	1.1.156.90	1.2.131.212		js_wrong_ve...	Exploit	SMEGze.pdf		
2020-12-25 18:09:52	1.1.108.192	1.2.196.174		js_wrong_ve...	Exploit	CFGkmD.PDf		
2020-12-25 18:09:08	1.1.205.179	1.2.125.65		Exploit.CVE-...	Exploit	ggNoXnlIrR...		
2020-12-25 18:06:20	2222::86	2222::65		Exploit	Exploit	ea85ba4941...		
2020-12-25 18:01:31	1.1.0.137	1.2.6.60		js_wrong_ve...	Exploit	YRSdIU.pDf		
2020-12-25 18:00:49	1.1.98.53	1.2.101.68		Exploit.CVE-...	Exploit	XPpNwxmj.d...		
2020-12-25 18:00:46	1.1.217.144	1.2.116.46		Exploit.CVE-...	Exploit	EmEKVp.pDF		
2020-12-25 18:00:23	1.1.158.69	1.2.136.225		Exploit.CVE-...	Exploit	PeYZtwCEET....		
2020-12-25 18:00:01	1.1.149.126	1.2.39.251		Exploit.CVE-...	Exploit	62PhqC.pDF		

For operations on advanced malicious sample logs, see basic operations in Log.

5.1.4.2 Callback Block Event

Collaborating with TAC or a cloud-side sandbox, NIPS can obtain the latest callback block event logs.

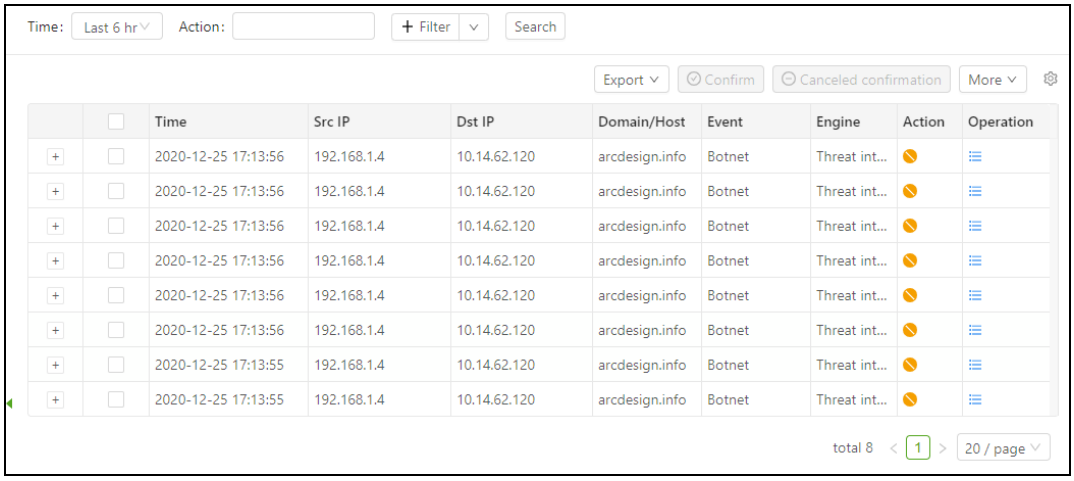
Choose **Log > Security Log > Advanced Threat > Blocked Events**. The **Blocked Events** page displays callback block event logs. Operations on callback block event logs can be performed in a similar way as advanced malicious sample detection logs. For details see Advanced Malicious Sample.

5.1.5 C&C Communication

C&C communication logs can be generated only after C&C communication profiles are configured and referenced in global security policies.

Choose **Log > Security Log > C&C Communication**. The **C&C Communication** page shows C&C communication logs.

Figure 5-7 C&C communication logs



In addition to basic operations, you can feed back false positives to the vendor and add the address of a C&C server to the whitelist.

Adding an Entry to the Whitelist

You can add the address of a C&C server to the whitelist only after the whitelist function is enabled in C&C communication profiles in global security policies.

The domain name or IP address of the C&C server, once being added to the whitelist, will be taken as a legitimate one and on longer be subject to subsequent C&C detection. For details, see Adding an Entry to the Whitelist.

Feeding Back to the Vendor

If you consider a C&C communication log as a false positive, you can point to in the **Operation** column of the log, click **Feedback**, and type feedback information to inform NSFOCUS rule group.

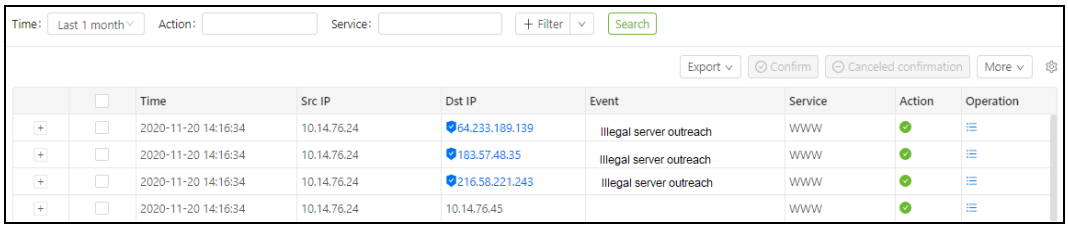
For details on feedback parameters, see Feeding Back to the Vendor.

5.1.6 Server Exception

Server exception logs can be generated only after server outreach policies are configured.

Choose **Log** > **Security Log** > **Server Exception**. The **Server Exception** page shows server exception logs.

Figure 5-8 Server exception logs



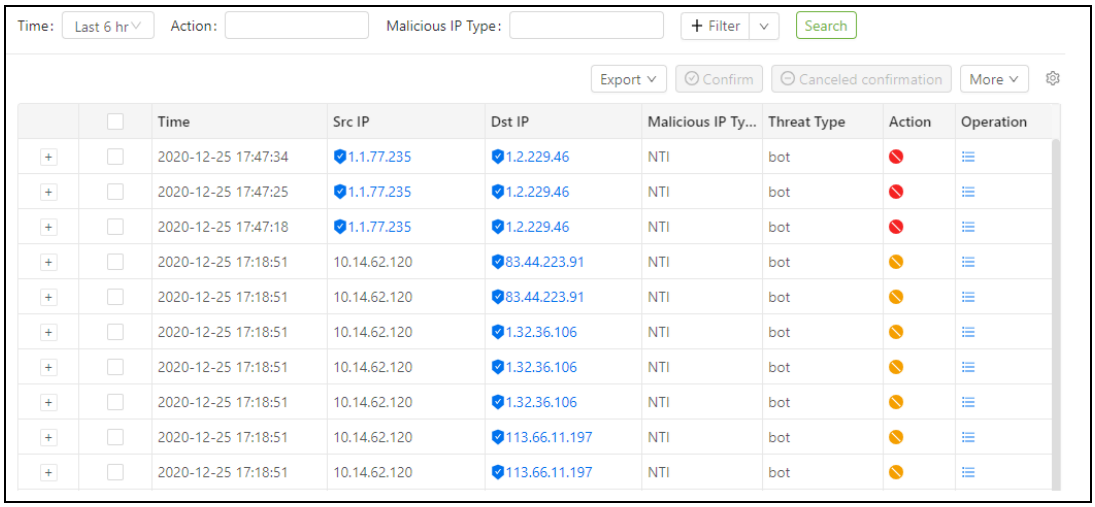
For operations on server exception logs, see basic operations in Log.

5.1.7 Global Blacklist

If the IP address of a website matches an entry in the global IP blacklist, an IP blacklist log is generated, and the system directly blocks connections to the website.

Choose **Log** > **Security Log** > **Global Blacklist** > **IP Blacklist**. The **IP Blacklist** page shows IP blacklist logs.

Figure 5-9 IP blacklist logs



Time	Src IP	Dst IP	Malicious IP Ty...	Threat Type	Action	Operation
2020-12-25 17:47:34	1.1.77.235	1.2.229.46	NTI	bot		
2020-12-25 17:47:25	1.1.77.235	1.2.229.46	NTI	bot		
2020-12-25 17:47:18	1.1.77.235	1.2.229.46	NTI	bot		
2020-12-25 17:18:51	10.14.62.120	83.44.223.91	NTI	bot		
2020-12-25 17:18:51	10.14.62.120	83.44.223.91	NTI	bot		
2020-12-25 17:18:51	10.14.62.120	1.32.36.106	NTI	bot		
2020-12-25 17:18:51	10.14.62.120	1.32.36.106	NTI	bot		
2020-12-25 17:18:51	10.14.62.120	1.32.36.106	NTI	bot		
2020-12-25 17:18:51	10.14.62.120	113.66.11.197	NTI	bot		
2020-12-25 17:18:51	10.14.62.120	113.66.11.197	NTI	bot		

For operations on IP blacklist logs, see basic operations in Log.

5.1.8 DNS Safety

If the domain name of a website hits an entry in the DNS blacklist, a domain name blacklist log is generated, and the system directly blocks connections to the website.

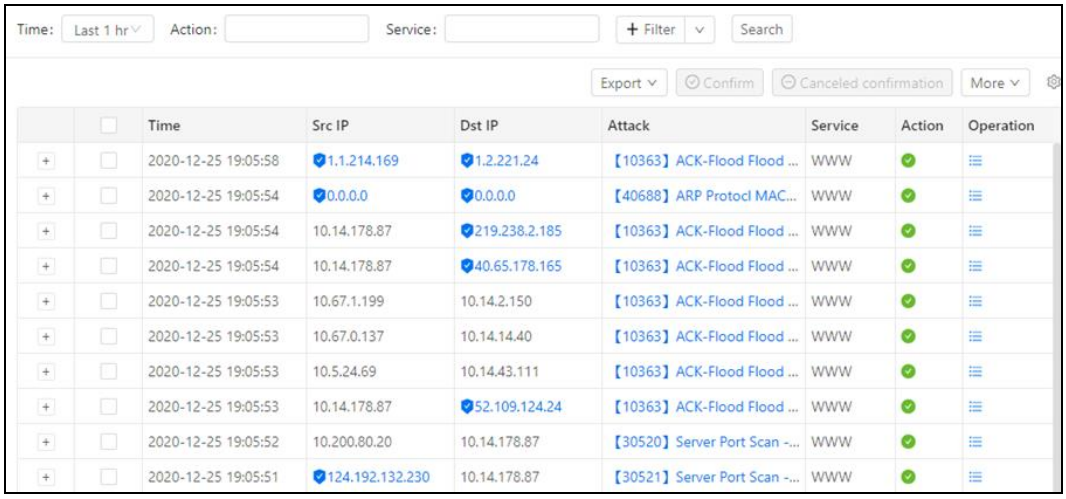
Choose **Log** > **Security Log** > **DNS Safety** > **DNS Blacklist**. The **DNS Blacklist** page displays domain name blacklist logs. DNS blacklist logs are operated in the same way as IP blacklist logs. For details, see Global Blacklist.

5.1.9 DoS Protection

DoS protection logs can be generated only after DoS protection policies are configured and enabled.

Choose **Log** > **Security Log** > **DoS Protection**. The **DoS Protection** page displays DoS protection logs.

Figure 5-10 DoS protection logs



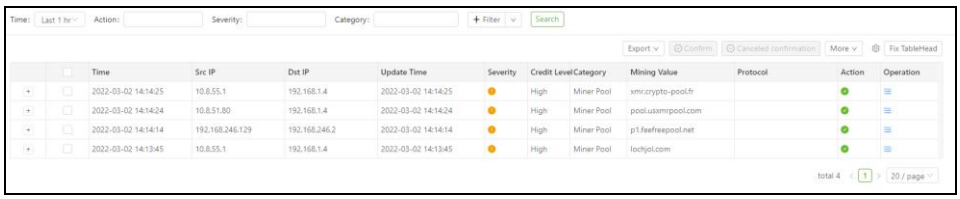
For operations on DoS protection logs, see basic operations in Log.

5.1.10 Mining

Mining logs can be generated only after mining protection policies are configured and enabled.

Choose **Log > Security Log > Mining**. The **Mining** page displays mining logs.

Figure 5-11 Mining page



For operations on DoS protection logs, see basic operations in Log.

5.2 Network Behavior

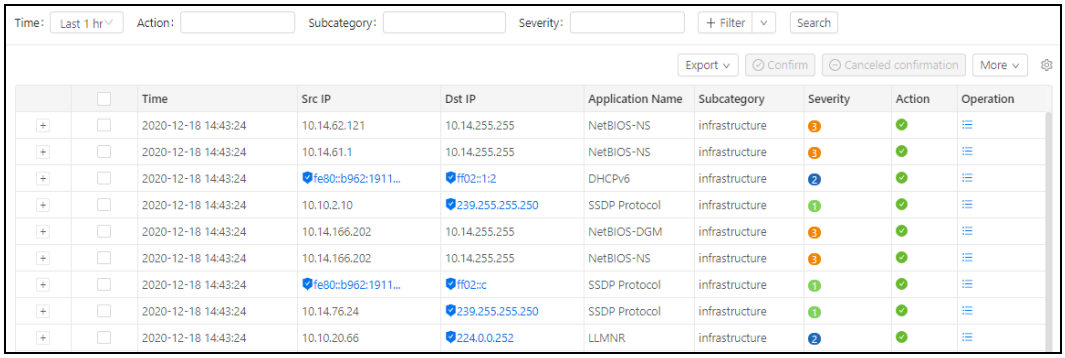
Online behavior logs include application control logs, URL categorization logs, and data loss prevention logs.

5.2.1 Application Control

Application control logs can be generated only after application control profiles are configured and referenced in online behavior profiles used in global security policies.

Choose **Log > Network Behavior > Application Control**. The **Application Control** page shows application control logs.

Figure 5-12 Application control logs



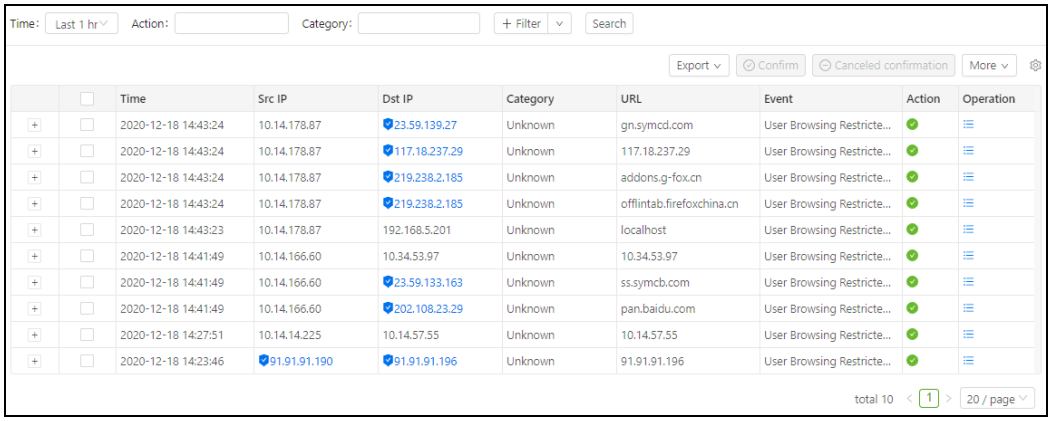
For operations on application control logs, see basic operations in Log.

5.2.1 URL Categorization

URL categorization logs can be generated only after URL categorization profiles are configured and referenced in online behavior profiles used in global security policies.

Choose **Log > Network Behavior > URL Filtering**. The **URL Filtering** page shows URL categorization logs.

Figure 5-13 URL categorization logs



For operations on URL categorization logs, see basic operations in Log.

5.2.2 Data Loss Prevention

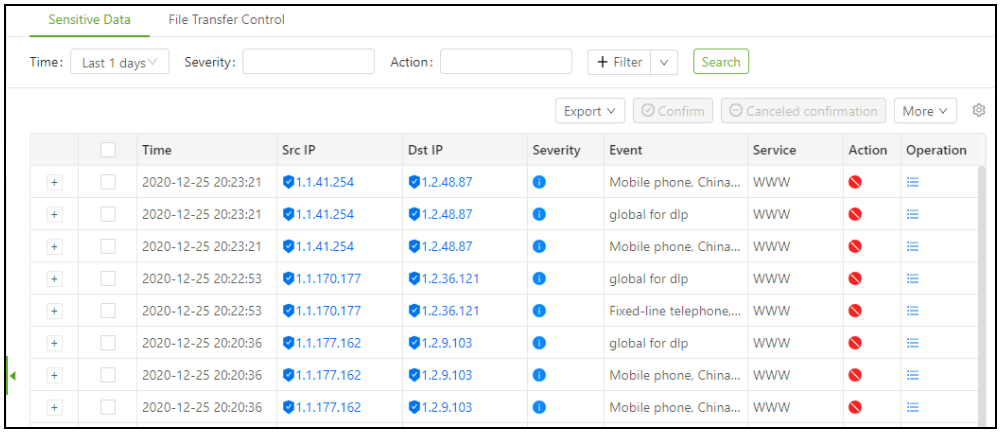
Data loss prevention logs include sensitive data protection logs and file transfer control logs.

Data loss prevention logs can be generated only after data loss prevention profiles are configured and referenced in online behavior profiles used in global security policies.

5.2.2.1 Sensitive Data

Choose **Monitor > Network Behavior > Data Loss Prevention > Sensitive Data**. The **Sensitive Data** page shows sensitive data protection logs.

Figure 5-14 Sensitive data protection logs



For operations on sensitive data protection logs, see basic operations in Log.

5.2.2.2 File Transfer Control

Choose **Log > Network Behavior > Data Loss Prevention > File Transfer Control**. The **File Transfer Control** page shows file transfer control logs. File transfer controls logs are operated in the same way as sensitive data protection logs. For details, see Sensitive Data.

5.3 O&M Log

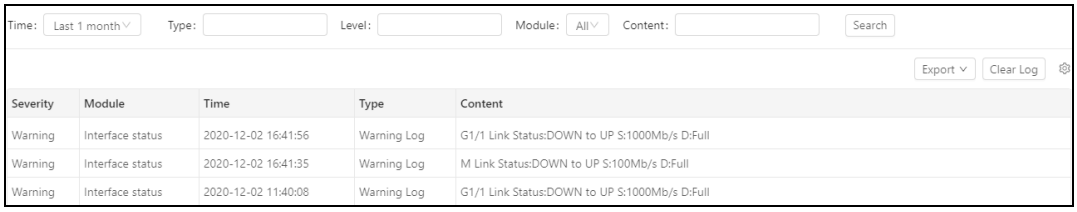
O&M logs include running logs and hardware logs.

5.3.1 Running Log

Running logs record the interface status, HA status, system running status, and bypass status.

Choose **Log > O&M Log > Running Log**. The **Running Log** page shows running logs.

Figure 5-15 Running log



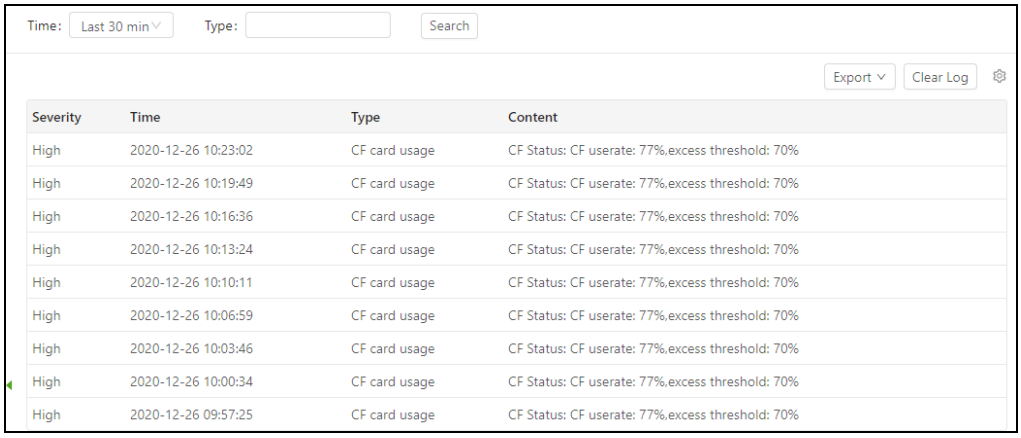
Besides basic operations, you can click **Clear Log** to delete all running logs.

5.3.2 Hardware Log

Hardware logs record the temperature and usage of the CPU, motherboard, and power supply of the device.

Choose **Log > O&M Log > Hardware Log**. The **Hardware Log** page shows hardware logs.

Figure 5-16 Hardware logs



Severity	Time	Type	Content
High	2020-12-26 10:23:02	CF card usage	CF Status: CF userate: 77%,excess threshold: 70%
High	2020-12-26 10:19:49	CF card usage	CF Status: CF userate: 77%,excess threshold: 70%
High	2020-12-26 10:16:36	CF card usage	CF Status: CF userate: 77%,excess threshold: 70%
High	2020-12-26 10:13:24	CF card usage	CF Status: CF userate: 77%,excess threshold: 70%
High	2020-12-26 10:10:11	CF card usage	CF Status: CF userate: 77%,excess threshold: 70%
High	2020-12-26 10:06:59	CF card usage	CF Status: CF userate: 77%,excess threshold: 70%
High	2020-12-26 10:03:46	CF card usage	CF Status: CF userate: 77%,excess threshold: 70%
High	2020-12-26 10:00:34	CF card usage	CF Status: CF userate: 77%,excess threshold: 70%
High	2020-12-26 09:57:25	CF card usage	CF Status: CF userate: 77%,excess threshold: 70%

Besides basic operations, you can click **Clear Log** to delete all hardware logs.

5.4 Malware Archive

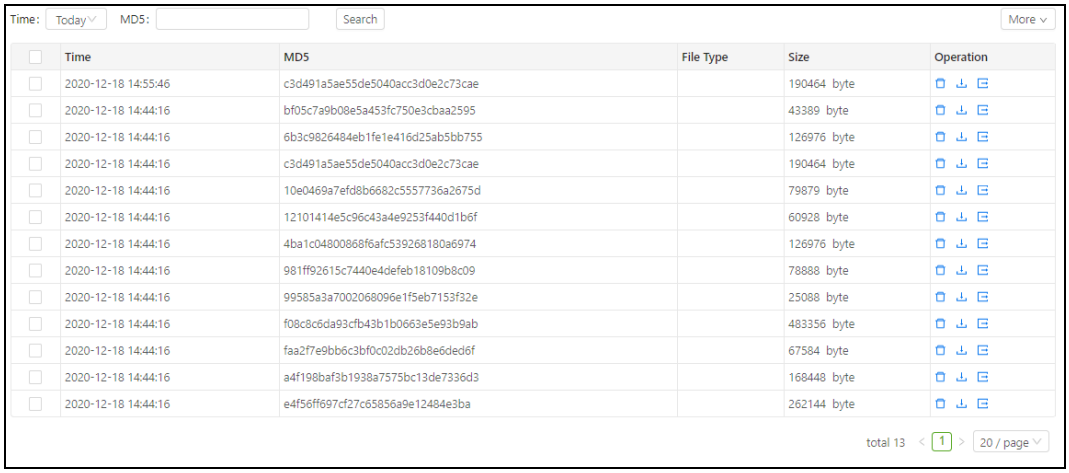
The malware archive module lists archived malicious files and server settings. Currently, this function is available only to NIPS with a hard disk.

5.4.1 Archived Malicious Files

If the malicious file forensics function is enabled under **Objects** > **Malware** > **Settings**, malicious file samples will be stored in a local disk drive.

Choose **Log** > **Malware Archive** > **Archived Malware**. The **Archived Malware** page shows archived malicious files.

Figure 5-17 Archived malicious files



Time	MD5	File Type	Size	Operation
2020-12-18 14:55:46	c3d491a5ae55de5040acc3d0e2c73cae		190464 byte	
2020-12-18 14:44:16	bf05c7a9b08e5a453fc750e3cbaa2595		43389 byte	
2020-12-18 14:44:16	6b3c9826484eb1fe1e416d25ab5bb755		126976 byte	
2020-12-18 14:44:16	c3d491a5ae55de5040acc3d0e2c73cae		190464 byte	
2020-12-18 14:44:16	10e0469a7efd8b6682c5557736a2675d		79879 byte	
2020-12-18 14:44:16	12101414e5c96c43a4e9253f440d1b6f		60928 byte	
2020-12-18 14:44:16	4ba1c04800868f6afc539268180a6974		126976 byte	
2020-12-18 14:44:16	981ff92615c7440e4defeb18109b8c09		78888 byte	
2020-12-18 14:44:16	99585a3a7002068096e1f5eb7153f32e		25088 byte	
2020-12-18 14:44:16	f08c8c6da93cfb43b1b0663e5e93b9ab		483356 byte	
2020-12-18 14:44:16	faa2f7e9bb6c3bf0c02db26b8e6ded6f		67584 byte	
2020-12-18 14:44:16	a4f198baf3b1938a7575bc13de7336d3		168448 byte	
2020-12-18 14:44:16	e4f56ff697cf27c65856a9e12484e3ba		262144 byte	

- Delete malicious files.
  - Click in the **Operation** column of a malicious file to delete the file.

- Select multiple malicious files, point to **More**, and click **Delete selected** to delete the selected files.
- Point to **More** and click **Delete all** to delete all malicious files in the table.

- Export malicious files.
  - Click in the **Operation** column of a malicious file to export it to a local disk drive.
  - Select multiple files, point to **More**, and click **Export selected** to export malicious files to a local disk drive.
- Perform forensics on NTI.

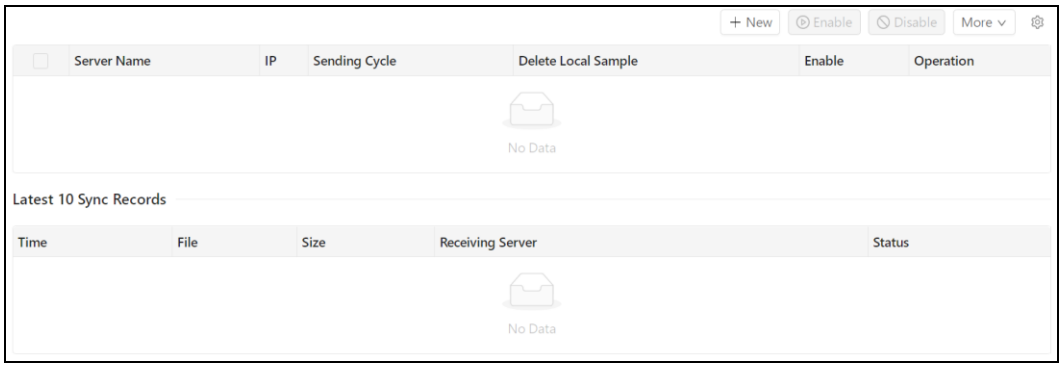
  Click in the **Operation** column of a malicious file to perform forensics on NTI.

5.4.2 Server Settings

NIPS can send archived malicious files to third parties. On the **Server Settings** page, you can configure the parameters of third-party servers and view the latest 10 sync records.

Step 1 Choose **Log** > **Malware Archive** > **Server Settings**.

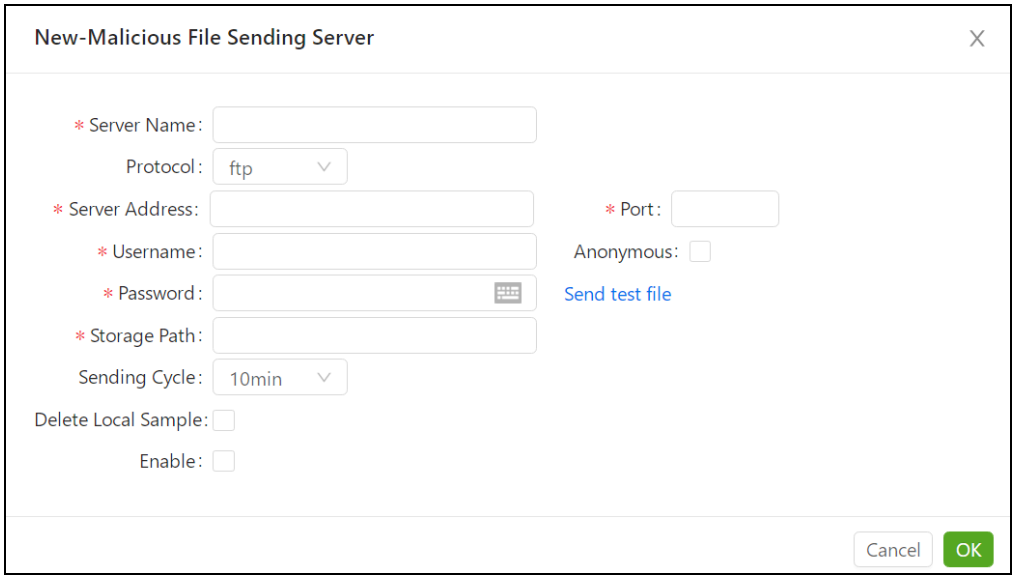
Figure 5-18 Server settings



You can add an external server to receive archived malicious files from NIPS. The following describes how to add such a server.

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

Figure 5-19 Adding an external server to receive archived malicious files



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

Table 5-2 Parameters for adding an external server to receive archived malicious files

Parameter	Description
Server Name	Name of the server.
Protocol	Protocol used by the server.
Server Address/Port	Specifies the IP address/port number used by the server to provide services.
Username/Password	Specifies the user name/password for access to the server.
Storage Path	Specifies the path to store archived malicious files on a third-party server.
Sending Cycle	Specifies the interval of sending archived malicious files to the server.
Delete Local Sample	Controls whether to delete local samples.
Enable	Controls whether to enable the server. The server can receive malicious files only after it is enabled.

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

----End

5.5 Data Maintenance

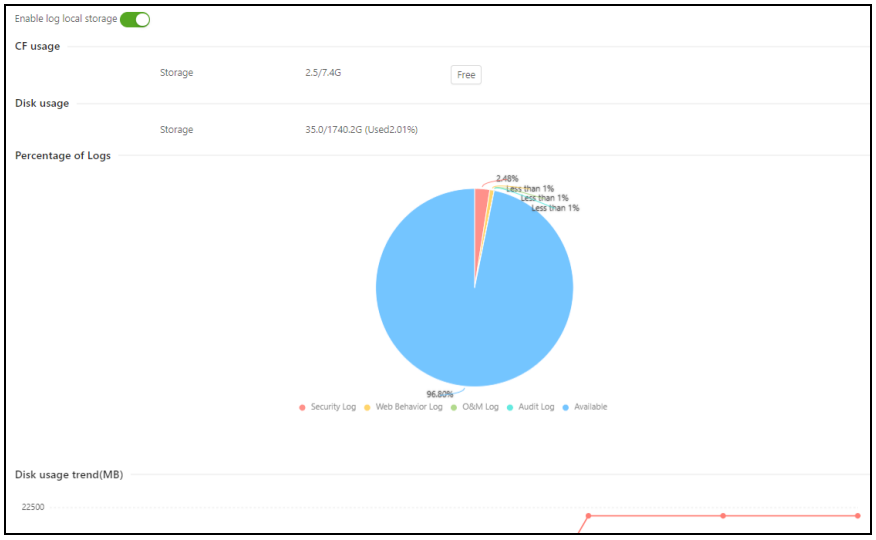
The data maintenance modules involve maintenance configuration, log backup, and backup history.

5.5.1 Maintenance Configuration

After maintenance configuration is enabled, you can view the CF card usage, usage of the entire hard disk, log distribution, and current log storage disk usage and its trend in the last seven days.

Choose **Log** > **Data Maintenance** > **General**.

Figure 5-20 Maintenance configuration



- CF card usage

  This area shows the CF card usage and you can click **Free** to clear data stored on the CF card.

- Hard disk usage

  This area shows the usage of the hard disk.

- Log storage disk usage

  This area shows the usage of the log storage disk and the percentage of each type of logs stored in the disk. You can perform the following operations:

  – Point to the pie chart to view log types and percentage of each type.

  – Click a legend below the pie chart to show or hide the corresponding log type on the pie chart.

- Trend of log storage disk usage in the last seven days

  This area shows the trend of log storage disk usage in the last seven days.

  Pointing to the trend graph shows the usage of the log storage disk at a specific time point.

5.5.2 Log Backup

After log backup is enabled, you can determine how logs are backed up and output.

Choose **Log** > **Data Maintenance** > **Setting**.

Figure 5-21 Log backup

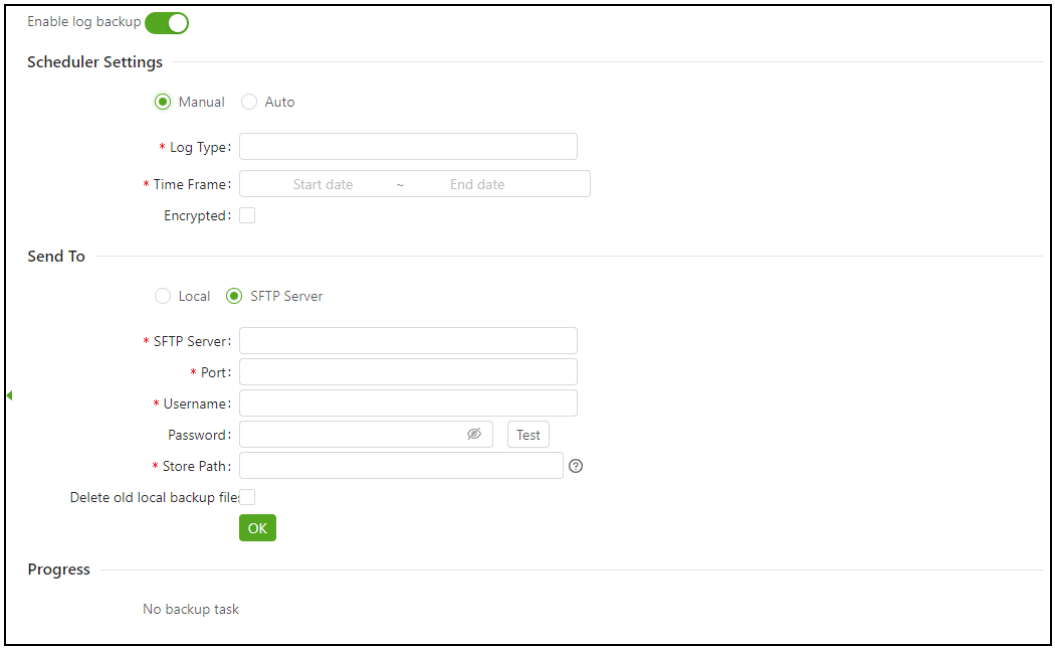


Table 5-3 shows parameters for configuring the log backup method and output method.

Table 5-3 Parameters for configuring the log backup method and output method

Parameter		Description
Backup method	Backup method	Logs can be backed up automatically or manually: • **Auto**: specify log types to be backed up, set the backup time, and click **OK**. • **Manual**: specify the log types to be backed up, set the backup time and frequency, and click **OK**.
	Log Type	Specifies the log types to be backed up.
	Recurrence	Specifies the backup frequency. This parameter is required only when **Manual** is selected as the backup method. You can select the backup cycle from the drop-down list.
	Time	Specifies the backup time. This parameter is required only when **Manual** is selected as the backup method.
	Time Frame	Specifies a time frame. Logs generated in this period will be backed up.
	Encrypted	Controls whether to encrypt data to be backed up.
Output method	Output method	Controls whether logs are backed up in a local disk drive or sent to the SFTP server.
	SFTP Server/Port	Specifies the IP address/port number used by the SFTP server to receive logs from NIPS.
	Username/Password	Specifies the user name/password for access to the SFTP server.
	Store Path	Specifies the log storage path on the SFTP server.

Parameter		Description
	Delete old local backup files when success	Controls whether to delete local backup files after backup.

After the preceding parameters are configured, you can click **Test** to test the connection between NIPS and SFTP to make sure that the log backup succeeds.

5.5.3 Backup History

The backup history is a string of records of backup done as configured. By default, the latest 50 backup records are displayed.

Choose **Log > Data Maintenance >History**.

Figure 5-22 Backup history

Name	Size	Type	Mode	Time	State
alert_cycle_backup_1...	612.77MB	Network Intrusion	Manual	2020-12-02 09:43:20	Success
alert_immediately_ba...	13.44MB	Network Intrusion	Auto	2020-12-01 11:26:29	Success
alert_immediately_ba...	13.44MB	Network Intrusion	Auto	2020-12-01 11:18:02	Success
alert_immediately_ba...	13.44MB	Network Intrusion	Auto	2020-12-01 11:17:12	Success
alert_cycle_backup_1...	580.36MB	Network Intrusion	Manual	2020-12-01 09:43:31	Success
alert_immediately_ba...	10.00KB	Network Intrusion	Auto	2020-11-30 11:21:27	Success
alert_immediately_ba...	10.00KB	Network Intrusion	Auto	2020-11-30 10:09:11	Success
alert_immediately_ba...	1.38GB	Network Intrusion	Auto	2020-11-28 11:45:01	Success
alert_immediately_ba...	10.00KB	Network Intrusion	Auto	2020-11-28 11:44:17	Success
alert_immediately_ba...	30.00KB	Network Intrusion	Auto	2020-11-27 15:40:02	Success

< 1 2 3 4 >

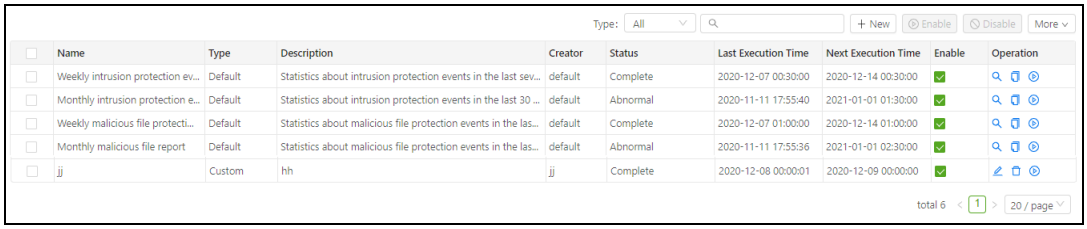
5.6 Report

NIPS generates reports by using report profiles.

5.6.1 Report Profile

Choose **Log > Report > Report Template**. NIPS comes with monthly and weekly general report profiles.

Figure 5-23 Report profiles

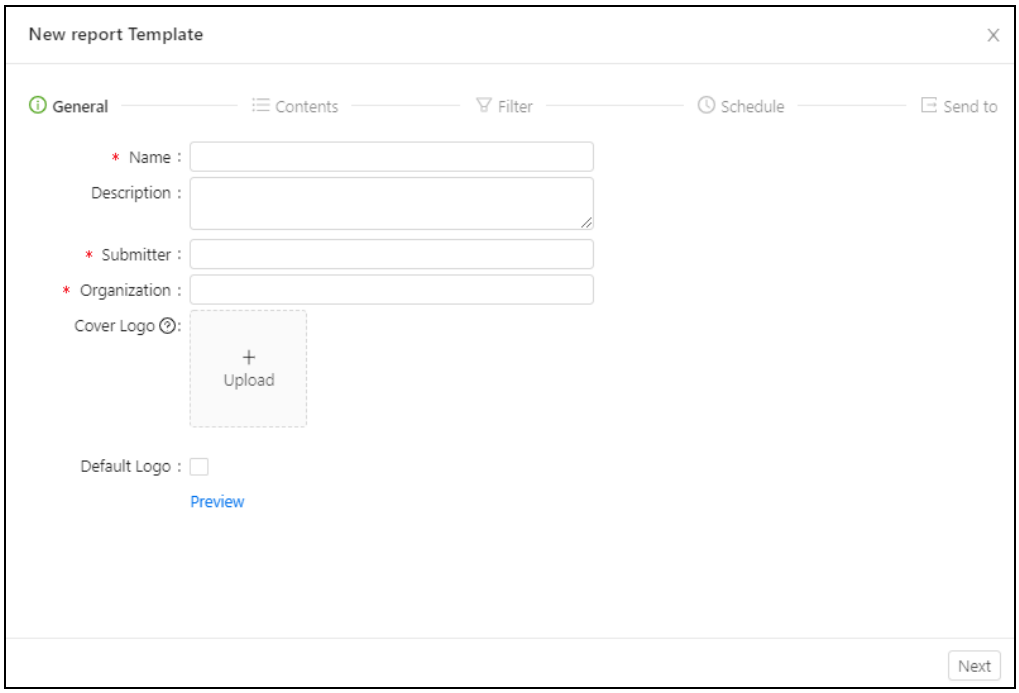


Creating a Report Profile

To create a custom report profile, follow these steps:

Step 1 Click **New**.

Figure 5-24 Creating a new report profile



Step 2 Configure basic parameters.

Table 5-4 Basic parameters for configuring a report profile

Parameter	Description
Name	Name of the custom report profile.
Description	Description of the report profile.
Submitter	Report submitter.
Department	Organization that submits the report.

Parameter	Description
Cover Logo	Logo used on the cover. Click **Upload** to upload a logo image. After a logo is uploaded, you can click **Preview** to preview it. Note • Image format: png/jpg/jpeg • Image size: less than 1 MB. • Recommended image scale: 3:2
Default Logo	If this option is selected, the built-in logo is used.

Step 3 Configure report contents.

a. Click **Next** to open the report content configuration page.

b. Select the built-in report content profile **default** or click + to create a new profile.

c. For a new report content profile, type the profile name and select items included in the profile. Then the selected items will be displayed in the **Selected Items** box. Click ✓ beside the **Name** text box to save this new profile. Then the name of the new profile is displayed in the **Template** text box.

Note	You can click , , , or beside the **Template** text box to edit, rename, copy, or delete a report content profile.

Step 4 Configure a filter.

a. Click **Next** to open the filter configuration page.

b. Select a filter profile or click + to create a filter profile.

c. Type the filter profile name and set filtering conditions in the right box.

d. Click ✓ beside the **Name** text box to save this new profile. Then the name of the new profile is displayed in the **Filter Template** text box.

Step 5 Configure the report task schedule.

a. Click **Next** to open the report task schedule configuration page.

b. Set schedule parameters.

- Report generation method: **Schedule** and **Subscribe**.
- **Recurrence**: report generation cycle.
- **Execute Day/Time**: report generation time.
- **Time Frame**: statistical period of logs.

Step 6 Configure the output method.

a. Click **Next** to open the report output configuration page.

b. Configure report output parameters.

- Report format: PDF, HTML, WORD, EXCEL. PDF and WORD are default formats.
- **Send to Email**: If you select this option, you need to select an existing email profile or click + to create a new one.
- **Send to FTP Server**: If you select this option, you need to select an existing FTP profile or click + to create a new one by specifying the IP address and port used by the FTP server to receive reports, user name and password for access of the FTP server, as well as the report storage path on the FTP server.

Step 7 Click **Save** to save the settings.

----End

Other Operations

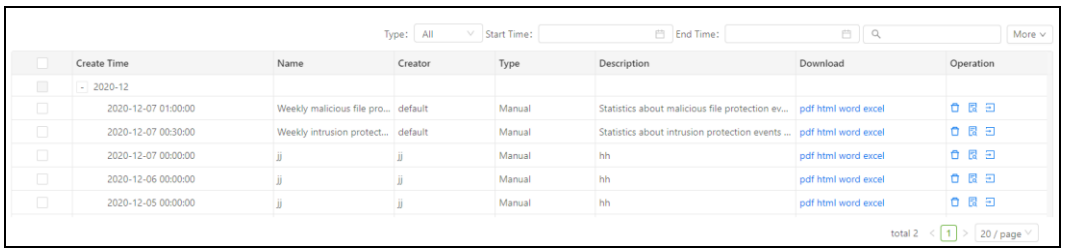
- View: Click in the **Operation** column of a built-in report profile to view details of this profile.
- Edit: Click in the **Operation** column of a custom report to edit a profile.
- Derive: Click in the **Operation** column of a built-in report profile to create a derived profile.
- Enable/Disable: Enable or disable profiles one by one or in bulk.
- Delete: Delete a profile. Only profiles that are not in use can be deleted. For details see Log.
- View: View settings of report profile.
- Generate: Click in the **Operation** column to generate a report. You can view the new report under **Log** > **Report** > **Report File**.

5.6.2 Report File

Choose **Log** > **Report** > **Report File**.

The **Report File** page presents report files generated based on report profiles.

Figure 5-25 Report files



Besides basic operations, you can perform the following operations on report files.

Previewing a Report

Click in the **Operation** column of a report file to preview it.

Downloading a Report

Click **pdf**, **html**, **word**, or **excel** in the **Download** column to download the report to a local disk drive for future reference and analysis.

Sending Reports

Reports can be sent in one of the following ways:

- Click in the **Operation** column of a report file to send the report as configured.
- Select multiple report files, point to **More**, and click **Send selected** to send the reports as configured.
- Point to **More** and click **Send all** to send all reports as configured.

6 Policies

This chapter contains the following sections:

Section	Description
Security Policy	Describes how to manage integrated security policies.
DoS Protection	Describes how to configure various DoS protection policies.
Server Outreach	Describes how to configure a server outreach policy and server outreach learning settings.
Sandbox Collaboration	Describes how to configure the device to collaborate with sandboxes and how to view detection statistics.
Threat Intelligence	Describes how to configure the device to collaborate with threat intelligence platforms and how to view hit statistics and query intelligence.
Global Blacklist/Whitelist	Describes how to manage and configure the global blacklist and whitelist.
DNS Safety	Describes how to manage and configure the DNS blacklist, whitelist, and sinkhole policy.
IP/MAC Binding	Describes how to manage IP/MAC bindings.
Collaboration with Firewalls	Describes how to configure the device to collaborate with NSFOCUS NF.
User Management	Describes how to manage users.
Geodatabase	Describes how to query an IP address in the public IP geodatabase and how to manage the private IP geodatabase.
Mining Protection	Describes how to configure a mining protection policy.

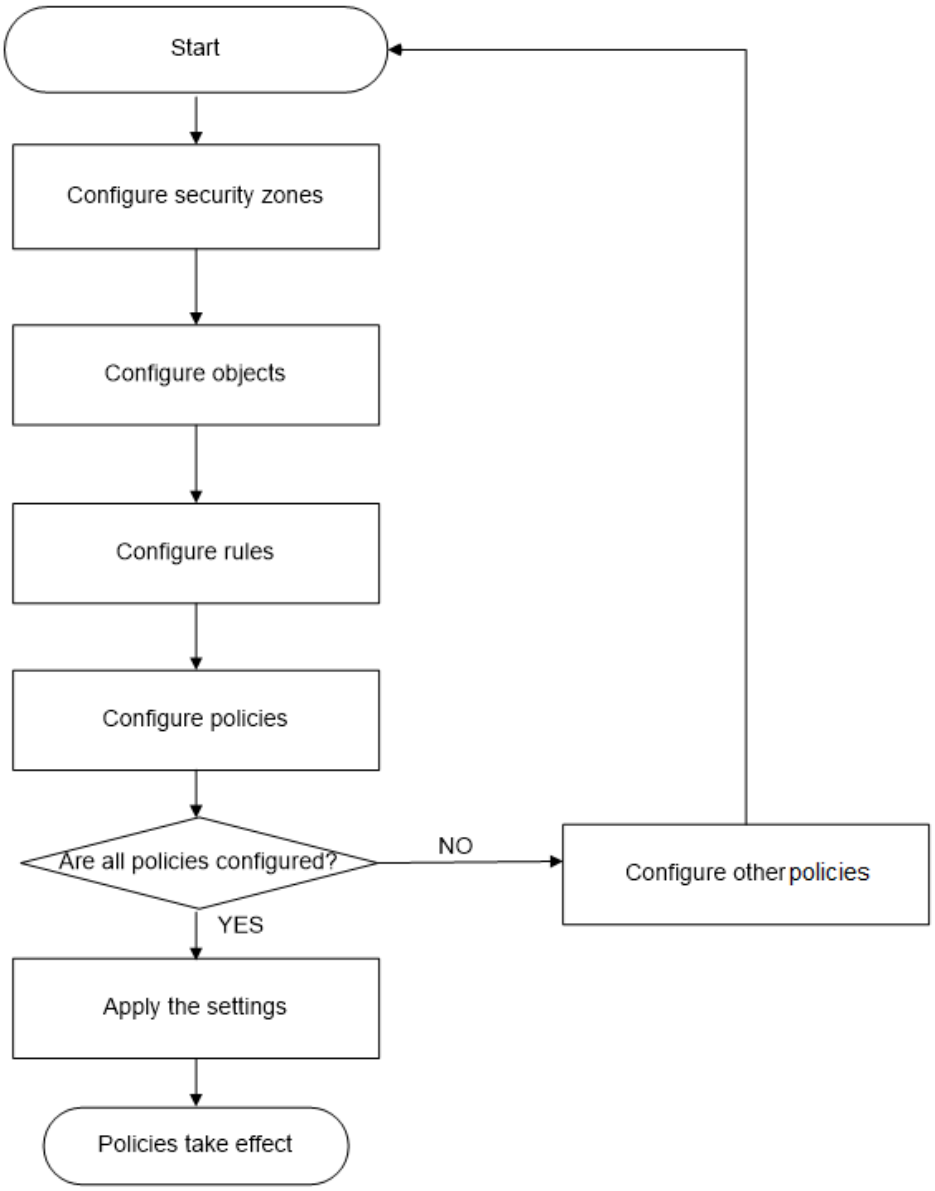
6.1 Security Policy

You can configure integrated policies by setting security zones, objects, security profiles, and online behavior profiles. NIPS will check traffic flowing through it against these policies for intrusions, malicious files, C&C communication, web threats, application-layer threats, and data breaches and for identification of URL categories. In this manner, the intranet is effectively secured.

NIPS comes with intrusion prevention profiles and web security profiles. Therefore, without much user intervention, NIPS can go live to deliver some degree of protection.

Figure 6-1 shows the procedure for configuring policies.

Figure 6-1 Policy configuration process



6.1.1 Security Policy Management

Security policy management involves policy creation and other operations.

Creating a Security Policy

To create a security policy, follow these steps:

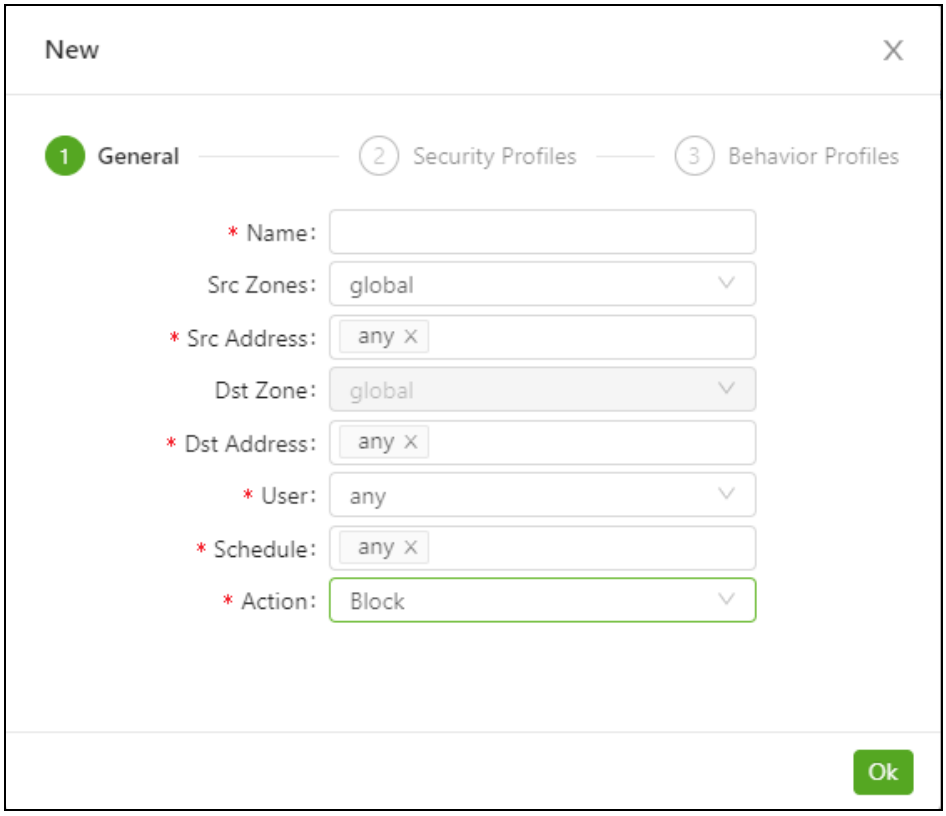
Step 1 Choose **Policies** > **Security Policy** > **Policies**.

The **Policies** page lists existing policies.

Click ⚙ and you can configure which fields to be displayed in the list.

Step 2 Click **New**.

Figure 6-2 Creating a security policy



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

Table 6-1 General parameters

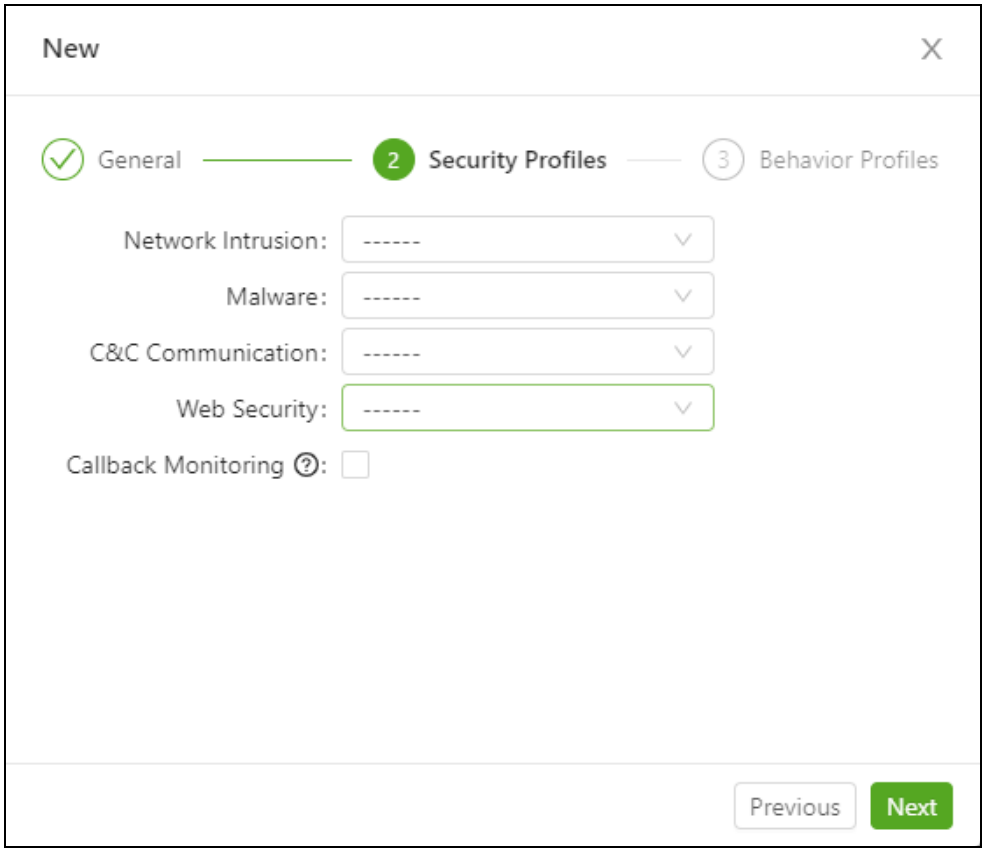
Parameter	Description
Name	Name of the security policy.
Src Zone	Specifies a security zone, packets from which will be matched against this security policy.
Src Addr	Specifies source addresses, packets from which will be matched against this security policy. The value **any** indicates that packets from any IP addresses will be sent to NIPS for checking.
Dst Zone	Indicates a security zone, packets to which will be matched against this security policy. **Note** The destination security zone automatically refreshes with a matching value each time you select a source security zone.

Parameter	Description
Dst Addr	Specifies destination addresses, packets to which will be matched against this security policy. The value **any** indicates that packets to any IP addresses will be sent to NIPS for checking.
User	Specifies the type of users to which this security policy will be applied. It has the following values: • **any**: indicates any users. • **Trusted user**: indicates online users. For details about online users, see Online Users. • **Untrusted user**: indicates other users than online users.
Schedule	Specifies time periods when this security policy takes effect. The value **any** indicates that this security policy is always valid.
Action	Specifies an action to be taken against matching packets. It has the following values: • **Block**: disallows matching packets from passing through NIPS. • **Allow**: allows matching packets to pass through NIPS. • **Submit for security check**: submits matching packets for checks against security templates and online behavior templates.

Step 4 Configure security templates.

a. Click **Next** to open the **Security Profiles** dialog box.

Figure 6-3 Dialog box for configuring security profiles



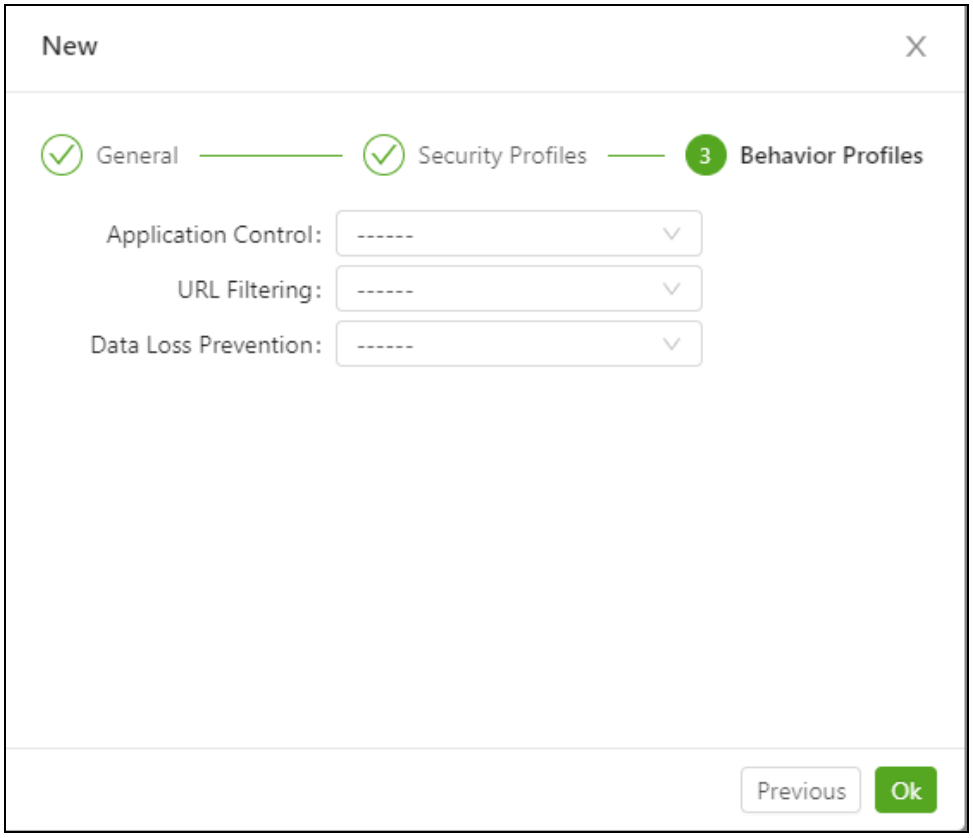
b. Configure security profiles.

- Select a template respectively from the drop-down lists of **Network Intrusion**, **Malware**, **C&C Communication**, and **Web Security**. If existing templates do not meet your requirements, click **New** to create one.
- **Callback Monitoring**: After this is enabled, when collaborating with sandboxes, the device will receive information from sandboxes about any suspicious callbacks found in advanced malicious file samples and monitor traffic for such callbacks.

Step 5 Configure online behavior profiles.

a. Click **Next** to open the **Behavior Profiles** dialog box.

Figure 6-4 Dialog box for configuring online behavior profiles



b. Configure online behavior profiles.

Select a profile respectively from the drop-down lists of **Application Control**, **URL Filtering**, and **Data Loss Prevention**. If existing profiles do not meet your requirements, click **New** to create one.

Step 6 Click **OK** to save the policy as a new one.

Step 7 Click **Commit** in the quick access bar to make the security policy take effect.

After a policy is created, the icon flashes intermittently. Click this icon and then click **OK** in the **Warning** dialog box to apply the configuration. After that, the new policy takes effect.

----End

Understanding the Policy Priority

The policy matching sequence of packets passing through NIPS is as follows:

1. Determine which policy to match according to basic information of packets, including the source security zone, source address object, destination security zone, and destination address object.
2. The sequence of security policies being matched depends on the strictness of rules. For example, if both policy 1 and policy 2 reference rule 1000, whose action is set to **Alert** for the former and to **Block** for the latter, then policy 2 is matched. If the action is the same for both policies, they will be matched in sequence.

Managing Security Policies

Besides creating security policies, you can also perform the following operations:

- Enabling/Disabling policies
  - Policies are enabled by default after being created. You can click ON or OFF in the **Status** column of a policy to disable or enable it.
  - Select multiple policies and click **Enable** or **Disable** in the upper-right corner of the page to enable or disable policies in batches.
  - Point to **More** in the upper-right corner of the page and click **Enable all** or **Disable all** to enable or disable all policies.
- Editing a policy: Click in the **Operation** column of a policy and then edit parameters. For the parameter description, see Table 6-1.
- Duplicating a policy: Click in the **Operation** column of a policy to rapidly create a similar policy.
- Moving a policy: Click in the **Operation** column of a policy and type a policy number as prompted to move the current policy to the row above that policy.

Note	The policy location in the list may determine the order in which policies are matched. Therefore, perform the operation with caution.

- Deleting policies
  - Click in the **Operation** column of a policy to delete the policy.
  - Select multiple policies, point to **More** in the upper-right corner of the page, and click **Delete selected** to delete policies in batches.
  - Point to **More** in the upper-right corner of the page and click **Delete all** to clear policies.
- Importing/Exporting policies
  - Point to **More** in the upper-right corner of the page and click **Export** to export all policies to a local disk drive.
  - Point to **More** in the upper-right corner of the page, click **Import**, and select a local policy file to import policies to NIPS.

Note	After making changes to policies, you must click **Commit** in the quick access bar to make such changes take effect.

6.1.2 Security Policy Settings

Choose **Policies** > **Security Policy** > **Settings**.

On the **Settings** page, you can configure the following settings:

- **Global Action**: specifies a global action for all security policies. Its priority is higher than actions specified in profiles. This configuration is usually used for go-live commissioning.
- **X-Forward-For support**: controls whether to check the X-Forward-For header. After such support is enabled, NIPS can, through the X-Forwarded-For header, identify the real IP address of a client connecting to the web server via an HTTP proxy or load balancing.
- **Drop Packet with Bad Checksum**: controls whether to drop packets with incorrect IP checksums. After this function is enabled, NIPS will drop packets with incorrect IP checksums.

6.2 DoS Protection

DoS attacks usually target computers' network bandwidths 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 a built-in DoS protection module, NIPS can detect and defend against DoS attacks. With DoS protection policies, NIPS can protect specified network objects against the following types of attacks:

- Flood
- Port scan
- Ping sweep
- ARP spoofing
- Application-layer flood

6.2.1 Flood

In flood attacks, attackers initiate a large number of fake requests to the destination host. The destination host exhausts its resources to process these fake requests and so cannot process requests from authorized users, thus a denial of service.

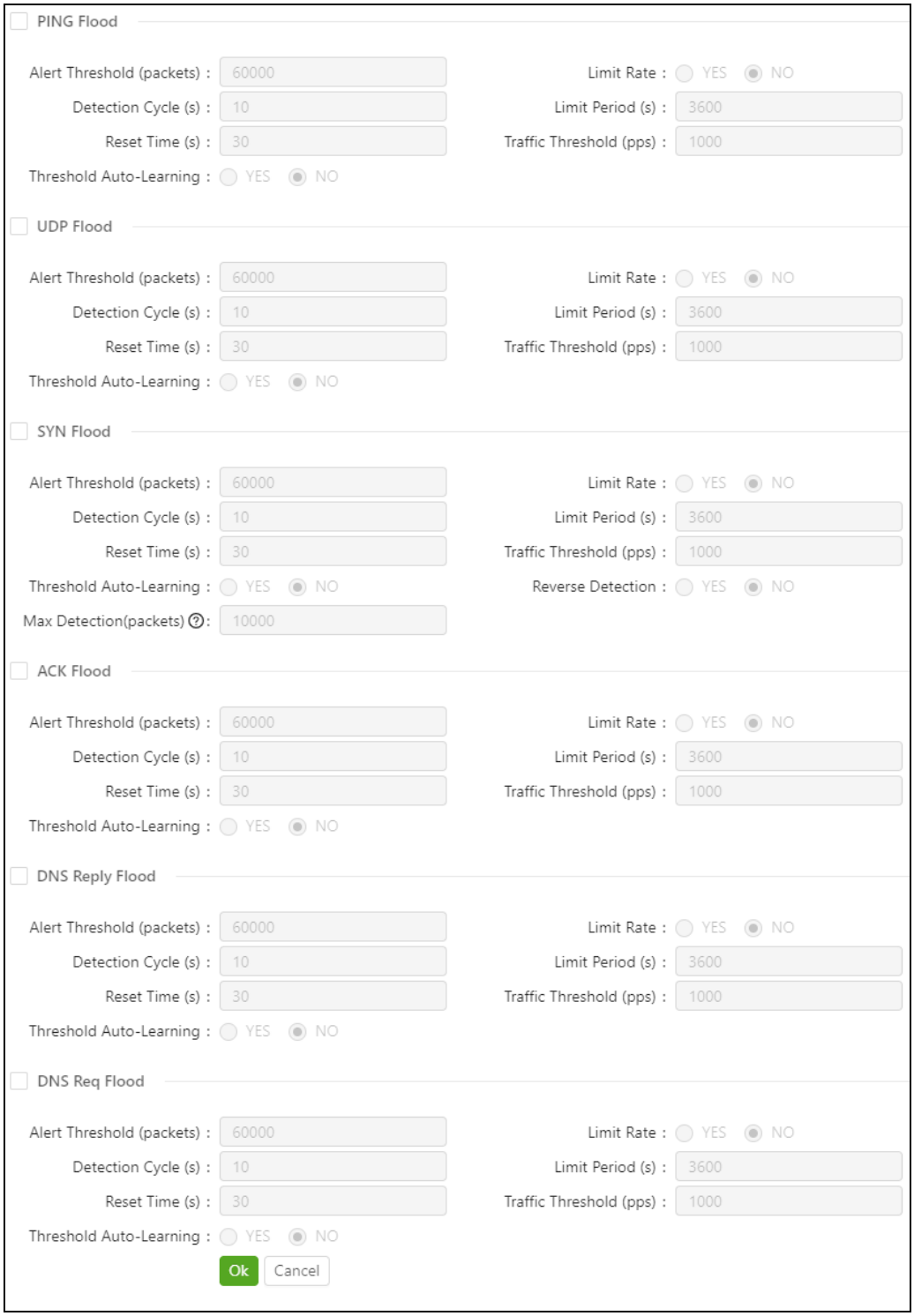
Currently, common flood attacks include the following types:

- Ping flood
- UDP flood
- SYN flood
- DNS reply flood
- ACK flood
- DNS request flood

With flood protection policies, NIPS can defend against the preceding flood attacks. To configure flood protection policies, follow these steps:

Step 1 Choose **Policies** > **DoS Protection > Flood**.

Figure 6-5 Page for configuring flood protection policies



Step 2 Select check boxes on the left of flood attack types against which NIPS will defend, and set parameters.

Table 6-2 Parameters for configuring flood protection policies

Parameter	Description
Alert Threshold (packets)	Specifies the packet number threshold. When detecting that the number of packets sent to a host reaches or exceeds this threshold, NIPS deems that a flood attack occurs and generates alerts.
Detection Cycle (s)	Specifies the period of time for NIPS to detect flood attacks. The interval is expressed in seconds.
Reset Time (s)	Specifies the interval at which the system clears the detection data and starts a new round of detection. The interval is expressed in seconds.
Threshold Auto-Learning	Controls whether NIPS automatically sets the alert threshold. After this function is enabled, NIPS learns traffic during the specified detection cycle and then automatically sets the alert threshold based on the learned traffic information.
Limit Rate	Controls whether automatic protection is enabled when NIPS detects flood attacks. If this function is set to **YES**, NIPS limits the traffic rate and generates an alert when detecting a flood attack. If this parameter is set to **NO**, NIPS only generates an alert when detecting a flood attack.
Limit Period (s)	Specifies the traffic limit period. After the protection time expires, NIPS starts a new round of detection. The period is expressed in seconds.
Traffic Threshold (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 (packets)	Specifies the maximum number of reverse detection packets to be sent in a second.

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

Step 4 Click Commit in the quick access bar to make the settings take effect.

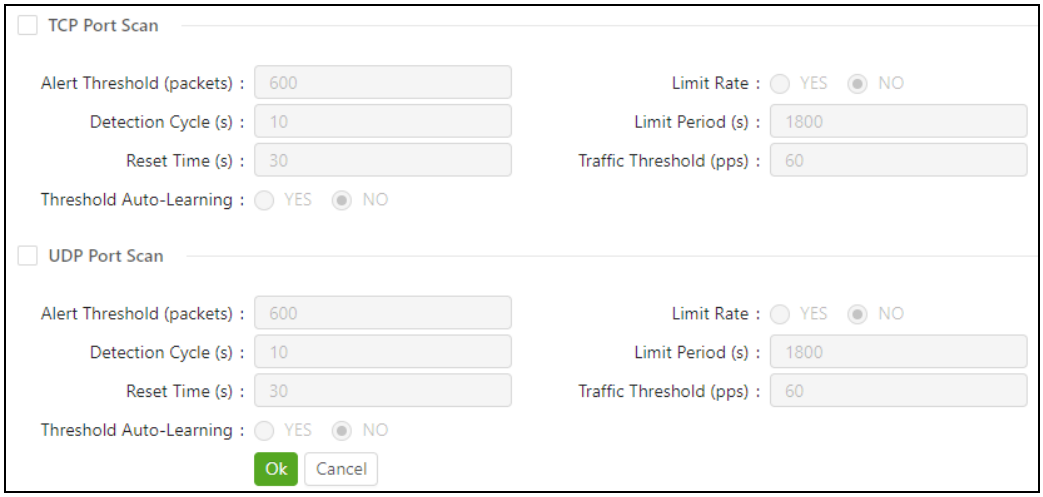
----End

6.2.2 Port Scan

In port scan attacks, attackers scan TCP or UDP ports on destination hosts to identify services running on the host for further intrusion. With port scan protection policies, NIPS can effectively protect against scanning of TCP or UDP ports. To configure port scan protection policies, follow these steps:

Step 1 Choose **Policies** > **DoS Protection** > **Port Scan**.

Figure 6-6 Page for configuring port scan protection



Step 2 Select check boxes on the left of port scan attack types against which NIPS will defend, and configure parameters.

For the description of parameters, see Table 6-2.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

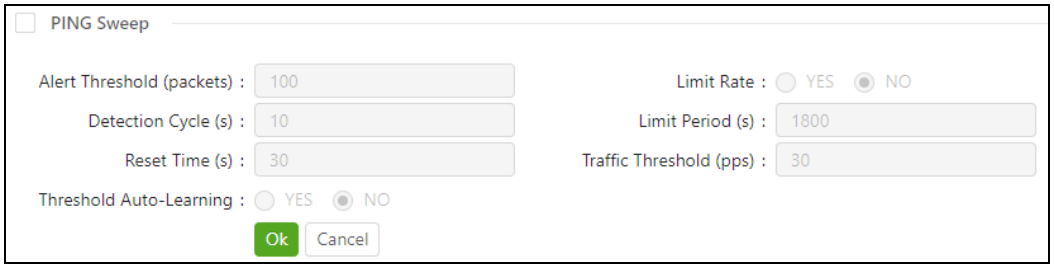
----End

6.2.3 Ping Sweep

Usually, an attacker, via ping sweep (ping scanning), detects active hosts on a network to find out the services and potential vulnerabilities in the target system for further intrusion. With a ping sweep protection policy, NIPS can defend against ping sweep attacks. To configure a ping sweep protection policy, follow these steps:

Step 1 Choose **Policies** > **DoS Protection** > **Ping Sweep**.

Figure 6-7 Page for configuring ping sweep protection



Step 2 Select the check box on the left of **PING Sweep** and configure parameters.

For the description of parameters, see Table 6-2.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

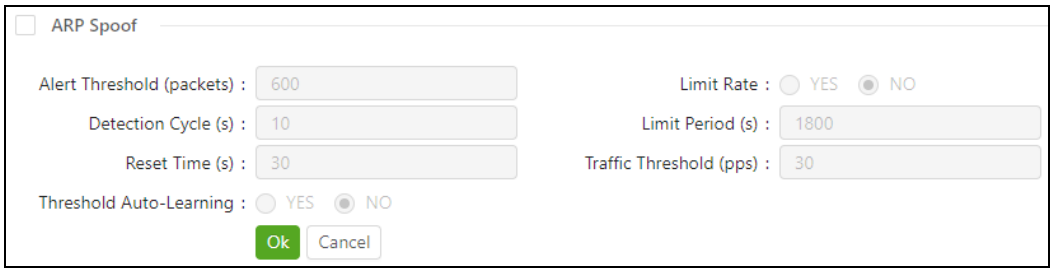
----End

6.2.4 ARP Spoofing

An ARP spoofing attack is conducted by sending falsified Address Resolution Protocol (ARP) messages via spoofed 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 user names and passwords of game accounts, online bank accounts, and file access accounts. With an ARP spoofing protection policy, NIPS can defend against ARP spoofing attacks. To configure an ARP spoofing protection policy, follow these steps:

Step 1 Choose **Policies** > **DoS Protection** > **ARP Spoofing**.

Figure 6-8 Page for configuring ARP spoofing protection



Step 2 Select the check box on the left of **ARP Spoof** and configure parameters.

For the description of parameters, see Table 6-2.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

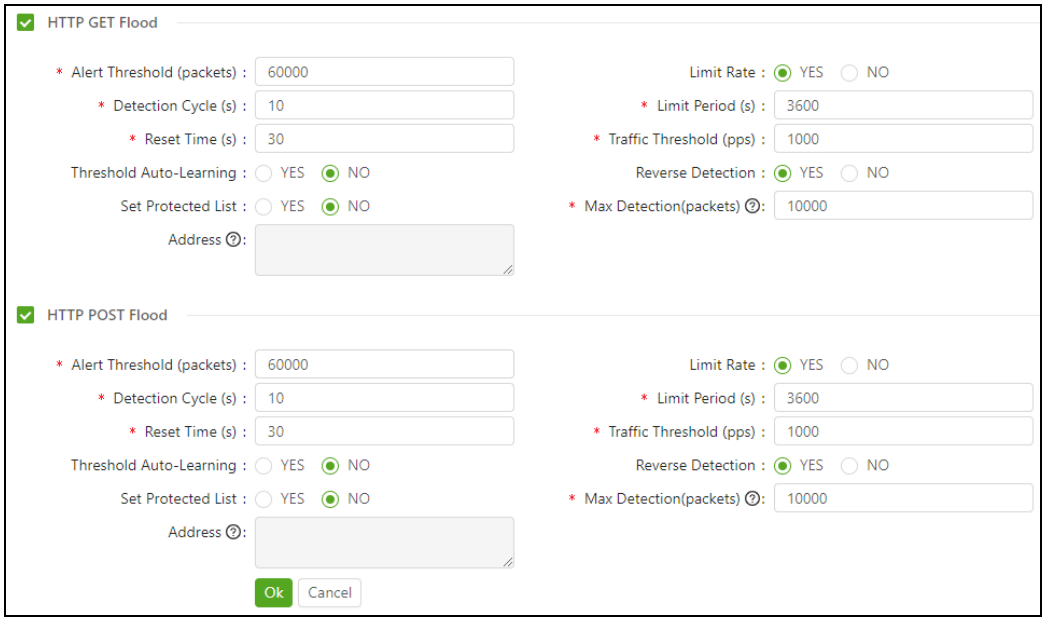
6.2.5 Application-Layer Flood

After configuring an application-layer flood 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 **Policies** > **DoS Protection** > **Application-Layer Flood**.

Figure 6-9 Page for configuring application-layer flood protection



Step 2 Select check boxes on the left of flood attack types against which NIPS will defend, and set parameters.

Most parameters have the same meanings as those for configuring protection policies on the **Flood** page. For the description of these parameters, see Table 6-2. The other parameter is 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.
- If you select this parameter to **NO**, NIPS will check all packets passing through it for HTTP DoS attacks.

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

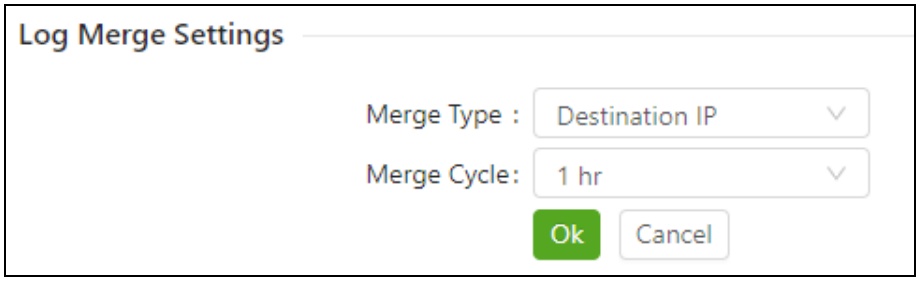
Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

6.2.6 Other Settings

Choose **Policies** > **DoS Protection** > **Settings**.

Figure 6-10 Page for configuring log merge settings



- **Merge Type**: Options include **Destination IP** and **Disable**.
- **Merge Cycle**: Options include **10 min**, **30 min**, **1 hr**, and **Custom**.

6.3 Server Outreach

The Server Outreach module allows you to configure server outreach policies and server outreach learning settings.

6.3.1 Policies

Server outreach policies identify outreach behaviors of servers in particular circumstances. You can specify legitimate outreach behaviors by setting the allowed destination, protocol, and port. All outreach behaviors other than the defined legitimate ones are considered illegitimate, and will be handled according to the server outreach protection policy. NIPS supports a maximum of 1000 server outreach policies.

You can configure a server outreach policy in either of the following ways:

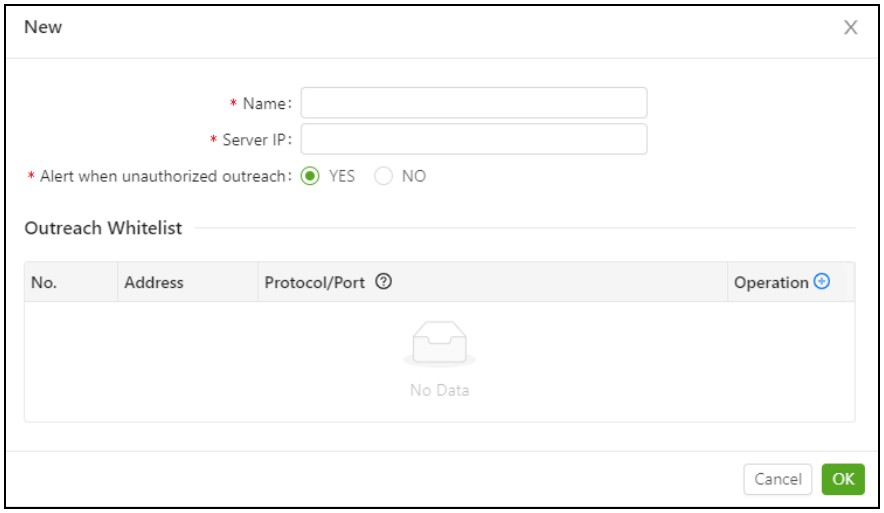
Common Configuration

The regular method of configuring a server outreach policy is as follows:

Step 1 Choose **Policies** > **Server Outreach** > **Policies**.

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

Figure 6-11 Creating a server outreach policy



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

Table 6-3 Parameters for configuring a server outreach policy

Parameter	Description
Name	Name of the server outreach policy.
Server IP	Specifies the IP address of the server protected by the policy.
Alert when unauthorized outreach	Control whether to report an alert when unauthorized outreach behaviors are detected.
Outreach Whitelist	Defines legitimate server outreach behaviors. Clicking displays parameters for defining legitimate outreach behaviors. For the description of parameters in this area, see Table 6-4.

Table 6-4 Parameters for defining legitimate server outreach behaviors

Parameter	Description
Address	Specifies an IP address to which the server is allowed to connect.
tcp/Port	Specifies a TCP port (associated with the specified destination IP address) to which the server is allowed to connect.
udp/Port	Specifies a UDP port (associated with the specified destination IP address) to which the server is allowed to connect.
icmp	Controls whether the server is allowed to access the ICMP service of the specified destination IP address.

Step 4 In the **Outreach Whitelist** area, click and configure parameters. After configuration, click to save the configuration.

You can click X or 🗑 to cancel or delete the configuration.

Step 5 Click **OK** to save the policy as a new one.

Step 6 Click **Commit** in the quick access bar to make the settings take effect.

----End

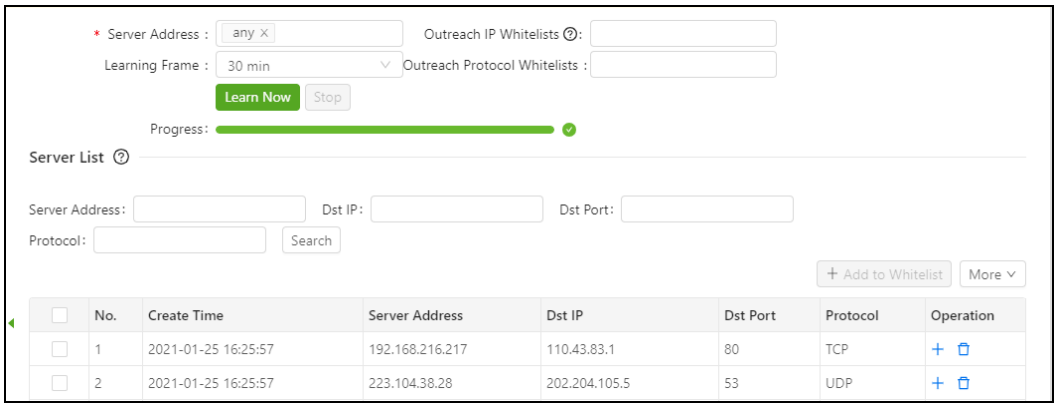
Quick Configuration

Based on server outreach behaviors automatically learned by NIPS, you can quickly create a server outreach protection policy as follows:

Step 1 Choose **Policies** > **Server Outreach** > **Auto Learning**.

The lower part of the page is **Server List**, which displays server outreach information learned by NIPS, as shown in Figure 6-12.

Figure 6-12 Server outreach learning page



Step 2 Quickly configure a server outreach protection policy.

a. Select one or more entries from the server list.

b. Click **Add to Whitelist** to set them as legitimate ones. This way, one or more server outreach policies are created. Alternatively, point to **More** and click **Add all to whitelist**. This way, all entries in the list are added as server outreach policies.

Step 3 (Optional) Choose **Policies** > **Server Outreach** > **Policies** to view new policies created.

----End

6.3.2 Auto Learning

NIPS can automatically learn server outreach behaviors. After auto-learning is configured, NIPS captures outreach data from specified servers and learns destination ports and corresponding services from such 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 auto-learning of server outreach behaviors, follow these steps:

Step 1 Choose **Policies** > **Server Outreach** > **Auto Learning**.

The upper part of the page provides auto-learning configuration parameters and the lower part provides an outreach behavior list (**Server List**).

Step 2 Configure auto-learning parameters.

Table 6-5 Auto-learning parameters

Parameter	Description
Server Address	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 are configured under **Objects** > **Addresses**. Alternatively, click **New** to configure a network object. For details about network objects, see IP/Netmask.
Learning Frame	Specifies the period when NIPS learns the server's outreach behavior data. Options include **30 min**, **1 hr**, **12 hr**, **1 day**, and **1 week**.
Outreach IP Whitelists	Specifies IP addresses to be included in the whitelist. NIPS does not perform server outreach learning for packets exchanged between the server and IP addresses included in the whitelist. Note **Outreach IP Whitelists** and **Outreach Protocol Whitelists** form an AND relationship. That is to say, only packets that meet both conditions are exempt from auto-learning.
Outreach Protocol Whitelists	Specifies protocols to be included in the whitelist. NIPS does not perform server outreach learning for packets exchanged between the server and whitelisted IP addresses by using protocols specified here. Note **Outreach IP Whitelists** and **Outreach Protocol Whitelists** form an AND relationship. That is to say, only packets that meet both conditions are exempt from server exception learning.

Step 3 Click **Learn Now** to start learning immediately.

The progress bar shows the percentage of the server's outreach behavior data that has been learnt.

Step 4 (Optional) Click **Stop** to suspend the learning.

----End

6.4 Sandbox Collaboration

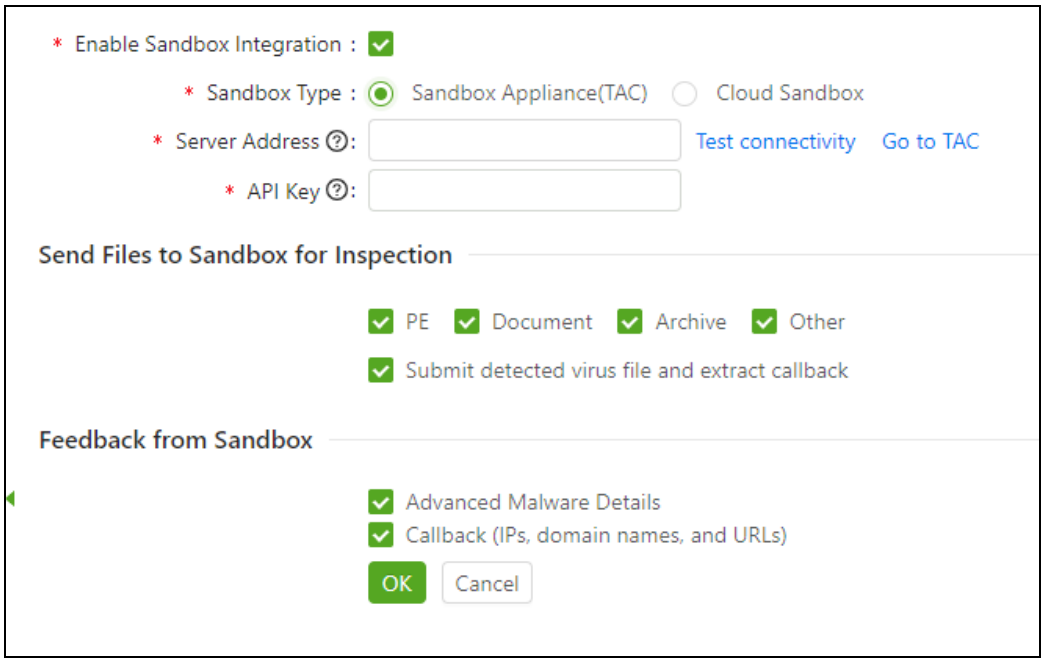
NIPS can collaborate with sandboxes.

6.4.1 Settings

After enabling collaboration with sandboxes, you need to further configure some parameters so that sandboxes can detect advanced malicious samples and malware callbacks and return detection results as configured.

Step 1 Choose **Policies** > **Sandbox Collaboration** > **Settings**.

Figure 6-13 Configuring collaboration with sandboxes



Step 2 Configure parameters.

Table 6-6 Parameters for configuring collaboration with sandboxes

Parameter	Description
Sandbox Type	Specifies the type of sandboxes that NIPS will collaborate with. Options include Sandbox Appliance (TAC) and Cloud Sandbox.
Server Address	Specifies the IP address of the selected sandbox. After typing the IP address, you can click **Test connectivity** to check whether NIPS can connect to the sandbox. If the connection is properly established, the system prompts that "Connected to TAC." In this case, you can click **Go to TAC** to open the login page of NSFOCUS Threat Analysis Center (TAC).
API Key	Specifies a key for authentication of the interface via which NIPS collaborates with NSFOCUS TAC. The API key is configured under **Policies** > **Collaborative Defense** > **API Key** on the web-based manager of NSFOCUS TAC. **Note** If **Cloud sandbox** is selected, NIPS automatically fills in the API key provided that the license covers the cloud sandbox module.
Send Files to Sandbox for Inspection	Specifies types of files to be submitted for the sandbox's inspection. File types include **PE**, **Document**, **Archive**, and **Others**. You can also choose whether to submit detected virus files and extract callback information.

Parameter	Description
Feedback from Sandbox	Specifies which type of information to return: • Whether to return advanced malicious sample details • Whether to return sample callback information, including IP addresses, domain names, and URLs

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

6.4.2 Statistics

The **Statistics** page displays detection results returned by the collaborative sandbox.

Choose **Policies** > **Sandbox Collaboration** > **Statistics**.

Figure 6-14 Statistics page

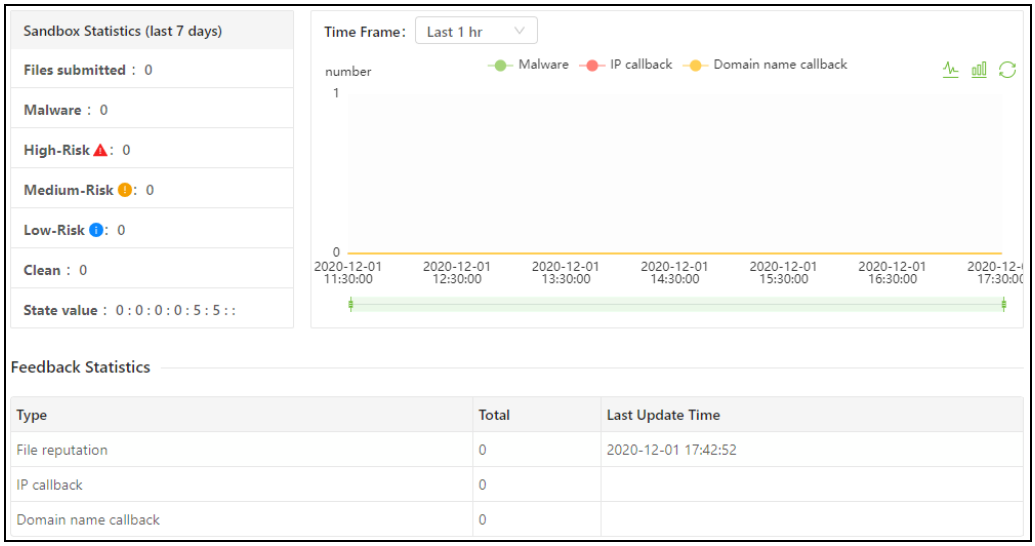


Table 6-7 describes statistical items.

Table 6-7 Sandbox detection statistics

Statistical Item	Description
Sandbox Statistics (last 7 days)	The last 7-day statistics include the total number of checked files, number of malicious files, number of high-/medium-/low-risk files, number of threat-free files, and state value.
Threat trends within a specified period	The periods you can specify include **Last 1 hr**, **Last 24 hr**, **Last 1 week**, and **Last 1 month**. Threat trends include the file reputation trend, IP callback trend, and domain name callback trend.

Statistical Item	Description
	Hovering over the trend chart displays detection data at that specific point of time. In the legend area, you can click a symbol (representing file reputation, IP callback, or domain name callback) to display or not to display the related trend. • Clicking or displays the trend in a line chart or bar chart. • Clicking restores all display settings to default values.
Feedback Statistics	Feedback statistics include the total quantities of different types of statistics (file reputation, IP callback, and domain name callback) and the last update time.

6.5 Threat Intelligence

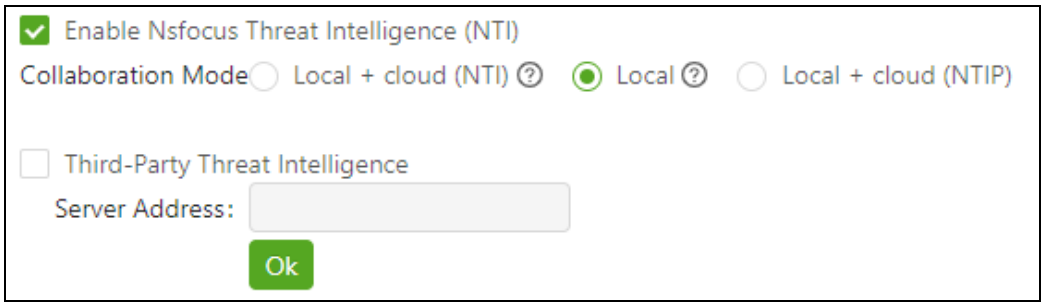
NIPS can collaborate with NSFOCUS Threat Intelligence center (NTI) to protect against malicious URLs, malicious IP addresses, and C&C communication based on intelligence.

6.5.1 Settings

To configure NIPS to collaborate with a threat intelligence system, follow these steps:

Step 1 Choose **Policies** > **Threat Intelligence** > **Settings**.

Figure 6-15 Page for configuring collaboration with a threat intelligence system



Step 2 Select an intelligence system and configure related parameters.

- Table 6-8 describes parameters for collaboration with NTI.

Table 6-8 Parameters for configuring collaboration with NTI

Parameter	Description
Collaboration Mode	NIPS supports the following collaboration modes: • **Local + cloud (NTI)**: This is the online mode, where the cloud is used as a complement to the local detection capability. In this mode, NIPS should submit objects to the cloud for detection of threats. • **Local**: This is the offline mode, where NIPS performs local detection based on intelligence obtained regularly from the offline intelligence

Parameter	Description
	database of NTI. • **Local + cloud (NTIP)**: In this mode, NIPS collaborates with NTIP, which serves as a complement to the local detection capability. When detecting no threat in objects locally, NIPS submits them to NTIP for further checks.
Local + cloud (NTI)	Specifies the IP address of NTI. After typing the IP address, you can click **Test connectivity** to check whether NIPS can connect to NTI. If you select **Auto sync latest intelligence to device**, all latest intelligence in NTI will be automatically synchronized to NIPS. Note The server address of NTI is automatically displayed and cannot be changed.
Local + cloud (NTIP)	Specifies the IP address of NTIP. • After typing the IP address, you can click **Test connectivity** to check whether NIPS can connect to NTIP. • **NTIP key**: specifies the user key, which is automatically generated on NTIP during user management.

- If you choose to use third-party intelligence, type the server address of the intelligence system.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

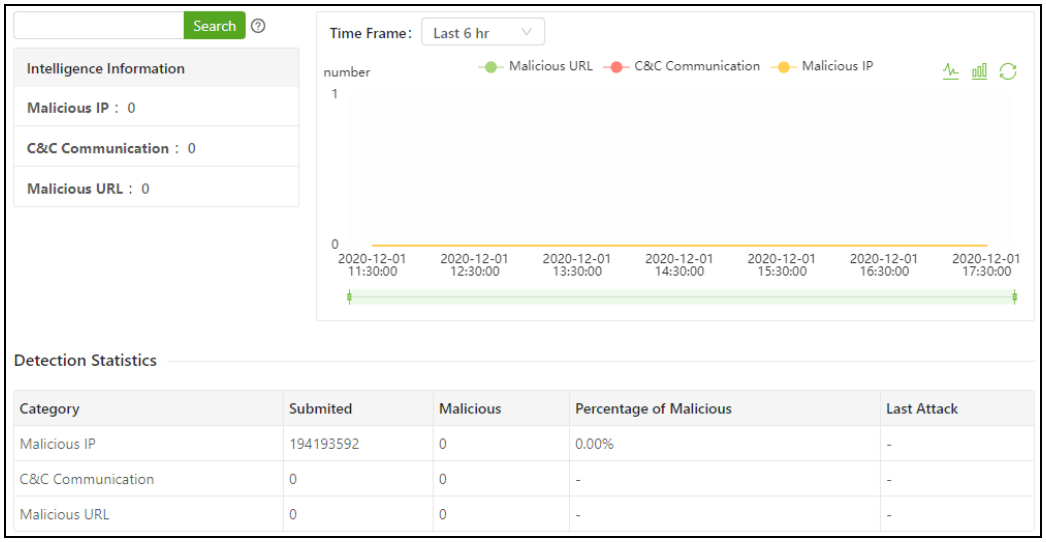
----End

6.5.2 Hits Statistics

The **Statistics** page displays statistics about events detected based on intelligence.

Choose **Policies > Threat Intelligence > Statistics**.

Figure 6-16 Statistics page



In the upper-left corner, type a URL (such as https://nsfocusglobal.com/), IPv4/IPv6 address, file MD5, or file hash in the text box and click **Search**. The system will return exact match results.

Table 6-9 describes statistical items.

Table 6-9 Hits statistics

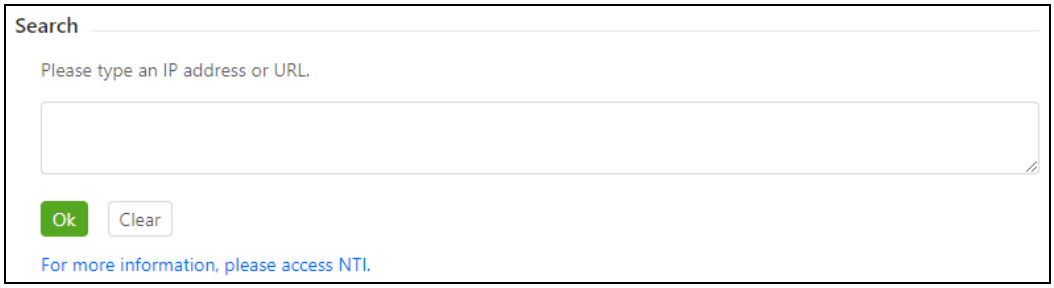
Statistical Item	Description
Intelligence Information	Intelligence information presents the number of malicious samples, including malicious IP addresses, C&C communication, and malicious URLs.
Threat trends within a specified period	The periods you can specify include **Last 6 hr**, **Last 24 hr**, **Last 1 week**, and **Last 1 month**. The trend chart shows trends of malicious URLs, malicious IP addresses, and C&C communication detected based on intelligence. Hovering over a trend curve displays hits data at a specific point of time. In the legend area, you can click a symbol (representing malicious URL, C&C communication, or malicious IP address) to display or not to display the related trend. • Clicking or displays the trend in a line chart or bar chart. • Clicking restores all display settings to default values.
Detection Statistics	Statistics in this area include the total number of samples, number of malicious samples (malicious URLs, malicious IP addresses, and C&C communication), proportion of malicious samples, and the last attack time.

6.5.3 Intelligence Query

NIPS, after collaborating with NTI, allows you to query intelligence on NTI.

Choose **Policies** > **Threat Intelligence** > **Search**.

Figure 6-17 Intelligence query page



Type an IP address or URL and click **OK**. You will be redirected to the NTI page, where detailed intelligence about the keyword is provided.

Alternatively, you can type multiple IP addresses or URLs separated by a comma. In this case, after you click **OK**, keywords are displayed below for you to click to obtain their detailed intelligence on NTI pages.

Besides, you can click the link text of "For more information, please access NTI" to directly query intelligence on NTI.

6.6 Global Blacklist/Whitelist

NIPS deems traffic of IP addresses in the global blacklist to be dangerous by default, thus blocking such traffic. As for traffic of whitelisted IP addresses, NIPS deems such traffic legitimate by default without any detection.

6.6.1 Blacklist

You can add known malicious IP addresses to the global blacklist. Then, when detecting traffic of these IP addresses, NIPS directly blocks it.

Manual Addition

Manually added blacklist entries can be edited, imported/exported, deleted, and disabled. The following sections describe how to create and disable blacklist entries.

Adding an IP Address to the Blacklist

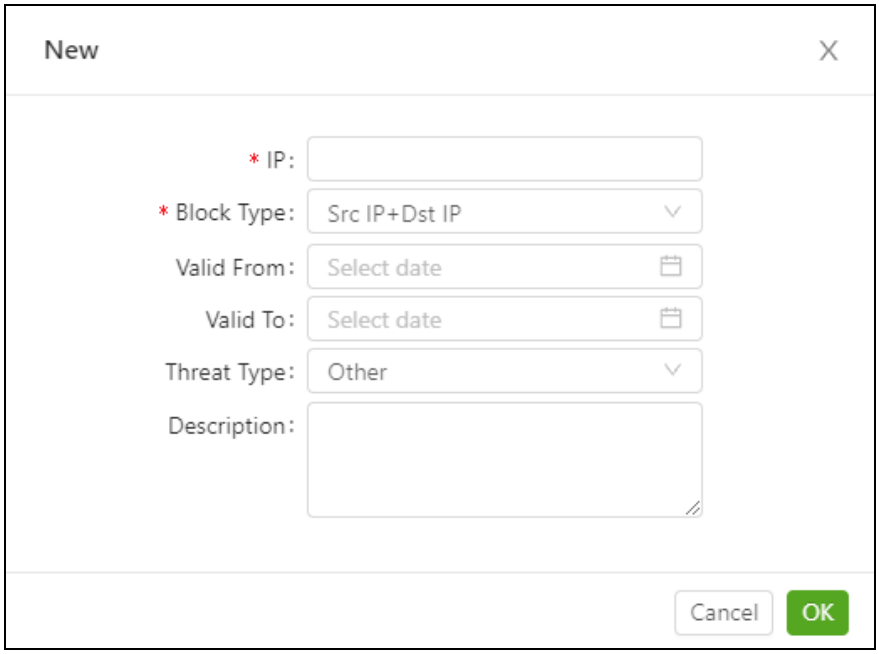
To manually add an IP address to the blacklist, follow these steps:

Step 1 Choose **Policies** > **Global Black/Whitelist** > **Blacklist**.

By default, the **Custom** page appears.

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

Figure 6-18 Dialog box for adding an entry to the blacklist



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

Table 6-10 Blacklist parameters

Parameter	Description
IP/Block Type	Specifies the IP address to be added to the blacklist, and the block type.
Valid From	Start date of the validity period of the blacklist entry. You should click Select date to select a date.
Valid To	End date of the validity period of the blacklist entry. You should click Select date to select a date.
Threat Type	Threat type of the specified IP address, which should be selected from the drop-down list.
Description	Description of the blacklist entry.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

Disabling Blacklist Entries

A disabled blacklist entry will cease to be effective. You can disable blacklist entries as follows:

- Click ON in the **Status** column of an entry to disable this entry.

- Select multiple entries and click **Disable** in the upper-right corner of the page to disable the selected ones.
- Point to **More** in the upper-right corner of the page and click **Disable all** to disable all entries.

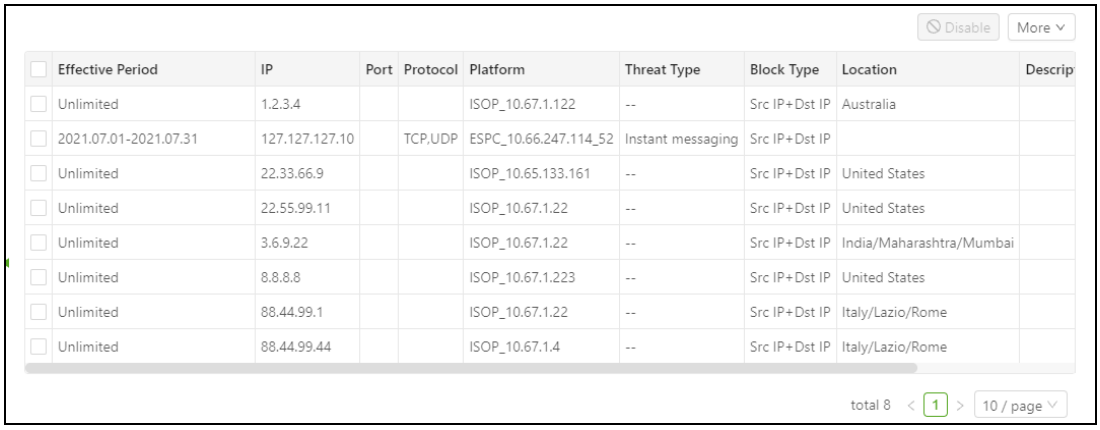
Disabled entries are no longer listed on the **Custom** page. You can view and manage them on the **Forbidden** page.

Third-Party Blacklist

NIPS can automatically add IP addresses blocked by a third-party platform to the blacklist. You can disable such blacklisted IP addresses.

Choose **Policies** > **Global Black/Whitelist** > **Blacklist** > **Third-Party Blacklist**.

Figure 6-19 Third-Party Blacklist page



The list shows blacklist details.

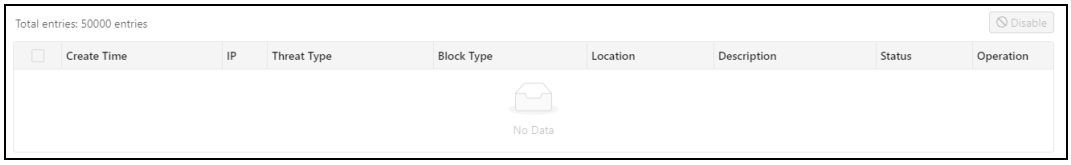
For how to disable blacklist entries, see Disabling Blacklist Entries.

Malicious IP Database

The malicious IP database here refers to the IP reputation library in NTI. NIPS can automatically add malicious IP addresses in this database to the blacklist. You can disable such blacklist entries.

Choose **Policies** > **Global Black/Whitelist** > **Blacklist** > **Malicious IP (NTI)**.

Figure 6-20 Malicious IP (NTI) page



The list shows blacklist details.

For how to disable blacklist entries, see Disabling Blacklist Entries.

Forbidden List

The forbidden list shows disabled blacklist entries manually added or obtained from the third-party blacklist or malicious IP database.

Choose **Policies** > **Global Black/Whitelist** > **Blacklist** > **Forbidden**.

On this page, you can enable and delete blacklist entries that have been disabled.

To enable disabled blacklist entries, you can use one of the following methods:

- Click OFF in the **Status** column of an entry to enable this entry.
- Select multiple entries and click **Enable** in the upper-right corner of the page to enable the selected ones.
- Point to **More** in the upper-right corner of the page and click **Enable all** to enable all entries.

Disabled blacklist entries, after being enabled, return to their original pages.

6.6.2 Whitelist

You can only manually add IP addresses to the global whitelist.

Whitelist

The **Whitelist** page lists predefined entries and manually added ones. Manually added whitelist entries can be edited and deleted. The following sections describe how to manually add an IP address to the whitelist and how to disable whitelist entries.

Adding an IP Address to the Whitelist

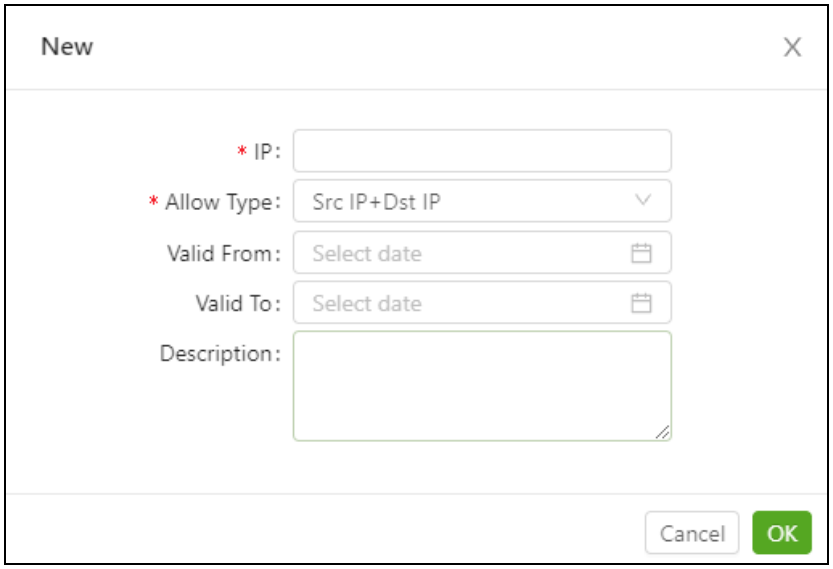
To manually add an entry to the whitelist, follow these steps:

Step 1 Choose **Policies** > **Global Black/Whitelist** > **Whitelist**.

By default, the **Whitelist** page appears.

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

Figure 6-21 Dialog box for adding an entry to the whitelist



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

Table 6-11 Whitelist parameters

Parameter	Description
IP/Allow Type	Specifies an IP address to be added to the whitelist, and the allow type.
Valid From	Start date of the validity period of the whitelist entry. You should click Select date to select a date.
Valid To	End date of the validity period of the whitelist entry. You should click Select date to select a date.
Description	Description of the whitelist entry.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

Manually added whitelist entries should be enabled before taking effect. For details, see "Enable custom whitelist."

----End

Disabling Whitelist Entries

Built-in and manually added whitelist entries can both be disabled. A disabled whitelist entry will cease to be effective. You can disable whitelist entries as follows:

- Click ON in the **Status** column of an entry to disable this entry.
- Select multiple entries and click **Disable** in the upper-right corner of the page to disable the selected entries.

- Point to **More** in the upper-right corner of the page and click **Disable all** to disable all entries.

Disabled entries are no longer listed on the **Whitelist Entries** page. You can view and manage them on the **Forbidden** page.

Forbidden List

The **Forbidden** page shows whitelist entries that have been disabled.

Choose **Policies** > **Global Black/Whitelist** > **Whitelist** > **Forbidden**.

On this page, you can enable and delete whitelist entries that have been disabled.

To enable disabled whitelist entries, you can use one of the following methods:

- Click OFF in the **Status** column of an entry to enable this entry.
- Select multiple entries and click **Enable** in the upper-right corner of the page to enable the selected entries.
- Point to **More** in the upper-right corner of the page and click **Enable all** to enable all entries.

Disabled whitelist entries, after being enabled, return to the **Whitelist** page.

6.6.3 Settings

Choose **Policies** > **Global Black/Whitelist** > **Settings**.

Figure 6-22 Blacklist/Whitelist configuration page

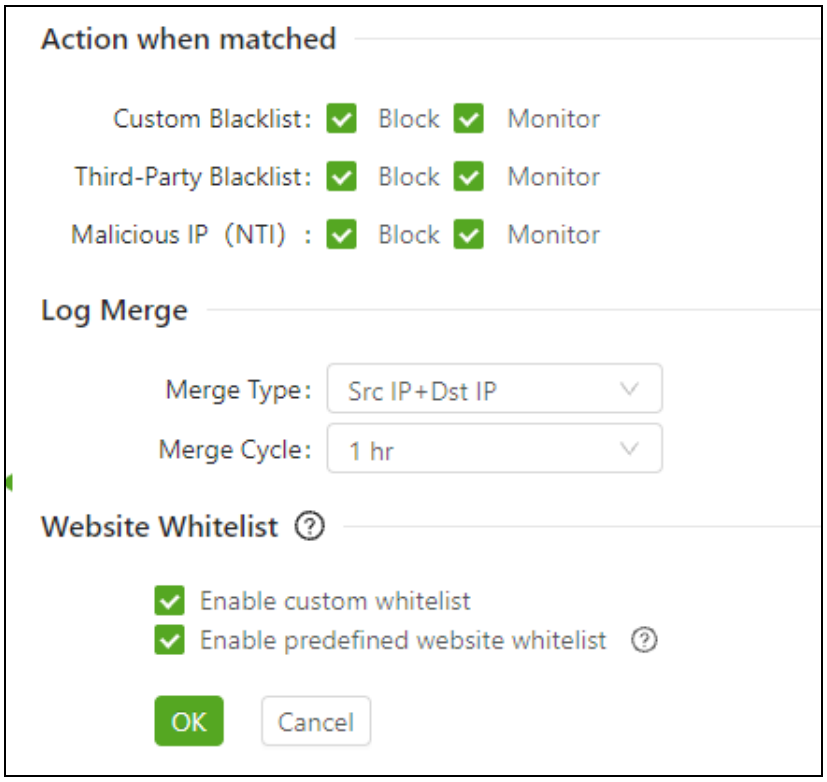


Table 6-12 describes parameters on this page.

Table 6-12 Global blacklist/whitelist configuration parameters

Parameter	Description
Action when matched	**Custom blacklist**: specifies how NIPS handles traffic of blacklisted IP addresses. Options include **Block** and **Monitor**.
	Third-party blacklist: specifies how NIPS handles traffic of platform-blocked IP addresses. Options include **Block** and **Monitor**.
	Malicious IP (NTI): specifies how NIPS handles traffic of IP addresses in the malicious IP database. Options include **Block** and **Monitor**.
Log Merge	**Merge Type**: specifies how logs of events involving blacklisted IP addresses are merged. You can select an option from the drop-down list.
	Merge Cycle: specifies the interval at which logs involving blacklisted IP addresses are merged. You can select an interval from the drop-down list.
Website Whitelist	**Enable custom whitelist**: controls whether to enable the custom whitelist. After this is enabled, whitelisted entries manually added will take effect. In this case, NIPS will allow traffic of whitelisted IP addresses to pass, without subjecting them to any security checks and online behavior controls.
	Enable predefined website whitelist: controls whether to enable the website whitelist. After this is enabled, for enterprises' Internet edge protection scenarios, NIPS will deem popular websites to be trusted ones and add them to the whitelist, thus improving the gateway performance by minimizing detection of innocuous traffic.

6.7 DNS Safety

NIPS deems traffic to domain names in the DNS blacklist to be dangerous by default, thus blocking such traffic. As for traffic to whitelisted domain names, NIPS deems such traffic legitimate by default without any detection.

6.7.1 Blacklist

You can add known malicious domain names to the DNS blacklist. Then, when detecting traffic to these domain names, NIPS directly blocks it.

Manual Addition

Manually added blacklist entries can be edited, imported/exported, deleted, and disabled. The following sections describe how to create and disable blacklist entries.

Adding a Domain Name to the Blacklist

To manually add a domain name to the blacklist, follow these steps:

Step 1 Choose **Policies** > **DNS Safety** > **Blacklist**.

By default, the **Custom** page appears.

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

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

Table 6-13 Blacklist parameters

Parameter	Description
Domain Name	Specifies the domain name to be added to the blacklist.
Valid From	Start date of the validity period of the blacklist entry. You should click Select date to select a date.
Valid To	End date of the validity period of the blacklist entry. You should click Select date to select a date.
Threat Type	Threat type of the specified domain name, which should be selected from the drop-down list.
Description	Description of the blacklist entry.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

Disabling Blacklist Entries

A disabled blacklist entry will cease to be effective. You can disable blacklist entries as follows:

- Click ON in the **Status** column of an entry to disable this entry.
- Select multiple entries and click **Disable** in the upper-right corner of the page to disable the selected ones.
- Point to **More** in the upper-right corner of the page and click **Disable all** to disable all entries.

Disabled entries are no longer listed on the **Custom** page. You can view and manage them on the **Forbidden** page.

DNS Blacklist

The DNS blacklist refers to the built-in blacklist database. If a domain name is found to be included in the DNS blacklist, NIPS blocks it and generates an alert.

Choose **Policies** > **DNS Safety** > **Blacklist** > **DNS Blacklist**.

The list shows blacklist details.

For how to disable blacklist entries, see Disabling Blacklist Entries.

Sinkhole Domain

NIPS can automatically add a sinkhole domain name to the blacklist. You can disable such blacklist entries.

Choose **Policies** > **DNS Safety** > **Blacklist** > **Sinkhole Domain**.

The list shows blacklist details.

For how to disable blacklist entries, see Disabling Blacklist Entries.

Forbidden List

The forbidden list shows manually added blacklist entries that have been disabled and those disabled on the **DNS Blacklist** or **Sinkhole Domain** tab page.

Choose **Policies** > **DNS Safety** > **Blacklist** > **Forbidden**.

On this page, you can enable and delete blacklist entries that have been disabled.

To enable disabled blacklist entries, you can use one of the following methods:

- Click OFF in the **Status** column of an entry to enable this entry.
- Select multiple entries and click **Enable** in the upper-right corner of the page to enable the selected ones.
- Point to **More** in the upper-right corner of the page and click **Enable all** to enable all entries.

Disabled blacklist entries, after being enabled, return to their original pages.

6.7.2 Whitelist

You can only manually add domain names to the DNS whitelist.

Whitelist

The **Whitelist** page lists predefined entries and manually added ones. Manually added whitelist entries can be edited and deleted. The following sections describe how to manually add a domain name to the whitelist and how to disable whitelist entries.

Adding a Domain Name to the Whitelist

To manually add an entry to the whitelist, follow these steps:

Step 1 Choose **Policies** > **DNS Safety** > **Whitelist**.

By default, the **Whitelist** page appears.

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

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

Table 6-14 Whitelist parameters

Parameter	Description
Domain Name	Specifies the domain name to be added to the whitelist.
Valid From	Start date of the validity period of the whitelist entry. You should click Select date to select a date.
Valid To	End date of the validity period of the whitelist entry. You should click

Parameter	Description
	Select date to select a date.
Description	Description of the whitelist entry.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

Manually added whitelist entries should be enabled before taking effect. For details, see "Enable custom whitelist."

----End

Disabling Whitelist Entries

Built-in and manually added whitelist entries can both be disabled. A disabled whitelist entry will cease to be effective. You can disable whitelist entries as follows:

- Click ON in the **Status** column of an entry to disable this entry.
- Select multiple entries and click **Disable** in the upper-right corner of the page to disable the selected entries.
- Point to **More** in the upper-right corner of the page and click **Disable all** to disable all entries.

Disabled entries are no longer listed on the **Whitelist** page. You can view and manage them on the **Forbidden** page.

Forbidden List

The **Forbidden** page shows whitelist entries that have been disabled.

Choose **Policies** > **DNS Safety** > **Whitelist** > **Forbidden**.

On this page, you can enable and delete whitelist entries that have been disabled.

To enable whitelist entries, you can use one of the following methods:

- Click OFF in the **Status** column of an entry to enable this entry.
- Select multiple entries and click **Enable** in the upper-right corner of the page to enable the selected entries.
- Point to **More** in the upper-right corner of the page and click **Enable all** to enable all entries.

Disabled whitelist entries, after being enabled, return to the **Whitelist** page.

6.7.3 Sinkhole Configuration

NIPS detects the traffic from and to the sinkhole server, and performs DNS sinkholing, records logs, or generates alerts against the detection result depending on the configured policy.

To add a sinkhole policy, follow these steps:

Step 1 Choose **Policies** > **DNS Safety** > **Sinkhole Configuration**.

The **Sinkhole Configuration** page lists all existing sinkhole policies.

You can click the icon to set the fields to be displayed in the list.

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

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

Table 6-15 Sinkhole parameters

Parameter	Description
Domain	Domain name of the website susceptible to attacks.
Sinkhole IP	IP address of the sinkhole server.
Description	Description of the sinkhole policy.

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

Step 5 On the **Sinkhole Configuration** page, click next to **Enable Sinkhole**.

Step 6 Click **Commit** in the quick access bar to make the settings take effect.

----End

6.7.4 Settings

Choose **Policies** > **DNS Safety** > **Settings**.

Figure 6-23 Blacklist/Whitelist configuration page

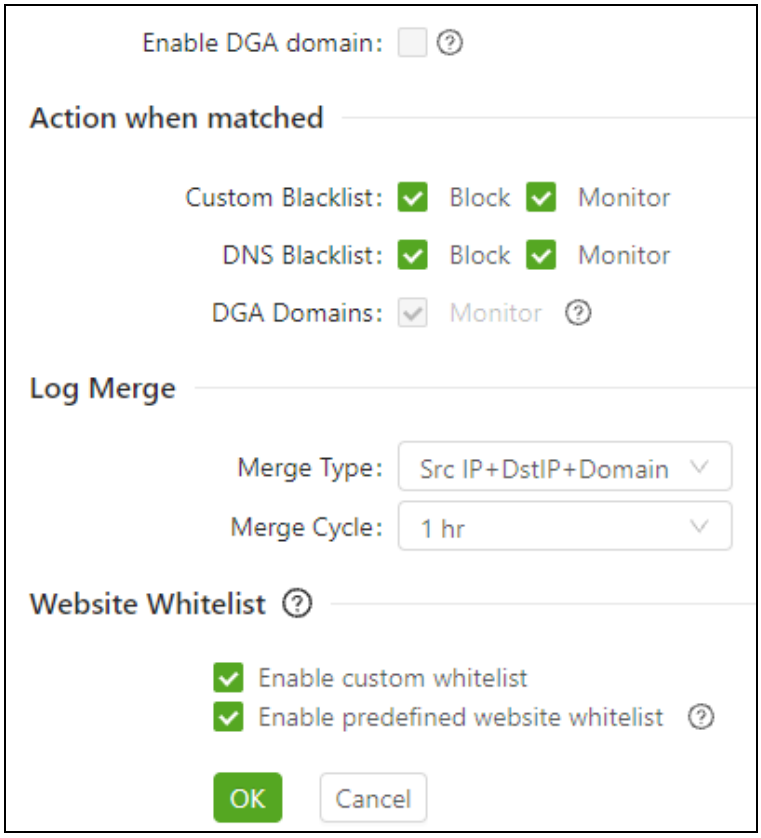


Table 6-16 describes parameters on this page.

Table 6-16 DNS blacklist/whitelist configuration parameters

Parameter	Description
Enable DGA domain	Controls whether to enable DGA domain detection. If it is enabled, the DNS requests and responses passing through NIPS will be detected for DGA domains according to machine learning algorithms. If a DGA domain is identified, NIPS blocks it and generates alerts based on the configurations.
Action when matched	**Custom blacklist**: specifies how NIPS handles traffic of manually added blacklisted domains. Options include **Block** and **Monitor**.
	DNS blacklist: specifies how NIPS handles traffic of DNS blacklisted domains in the database. Options include **Block** and **Monitor**. In addition, NIPS performs DNS sinkholing on the blacklisted domains.
	DGA domains: specifies how NIPS handles traffic of DGA domains. The option includes **Monitor**. In addition, NIPS performs DNS sinkholing on the blacklisted DGA domains.
Log Merge	**Merge Type**: specifies how logs of events involving blacklisted domains are merged. You can select an option from the drop-down list.
	Merge Cycle: specifies the interval at which logs involving blacklisted domains are merged. You can select an interval from the drop-down list.
Website Whitelist	**Enable custom whitelist**: controls whether to enable the custom whitelist. After this is enabled, whitelisted entries manually added will take effect. In this case,

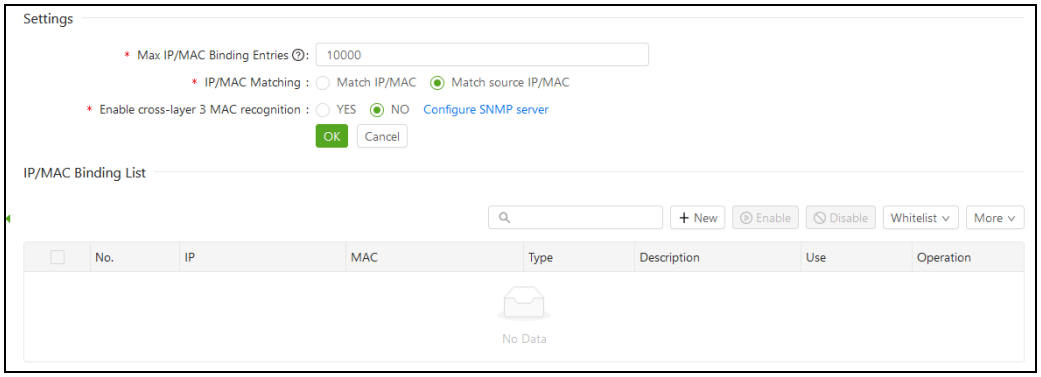
Parameter	Description
	NIPS will allow traffic to whitelisted domains to pass, without subjecting them to any security checks and online behavior controls.
	Enable predefined website whitelist: controls whether to enable the website whitelist. After this is enabled, for enterprises' Internet edge protection scenarios, NIPS will deem popular websites to be trusted ones and add them to the whitelist, thus improving the gateway performance by minimizing detection of innocuous traffic.

6.8 IP/MAC Binding

Binding IP addresses to MAC addresses prevents unauthorized hosts from accessing a network using the IP address of an authorized host, thereby effectively avoiding IP address spoofing.

Choose **Policies** > **IP/MAC Binding**.

Figure 6-24 IP/MAC Binding page



You can configure IP/MAC binding parameters and the IP/MAC binding list, including creating, editing, deleting, importing, and searching for IP/MAC binding entries.

Configuring IP/MAC Binding Parameters

In the **Settings** area, you can configure IP/MAC binding parameters shown in Table 6-17 and click **OK** to commit the settings.

Table 6-17 IP/MAC binding parameters

Parameter		Description
Max IP/MAC Binding Entries		Specifies the maximum number of IP/MAC entries allowed. The value range is 1–10000.
IP/MAC Matching	Match IP/MAC	Checks whether the source or destination addresses of a packet match entries included in IP/MAC binding list. • A packet will be passed through if there is a match for both the source IP address and MAC address. • A packet will be passed through if there is a match for both the

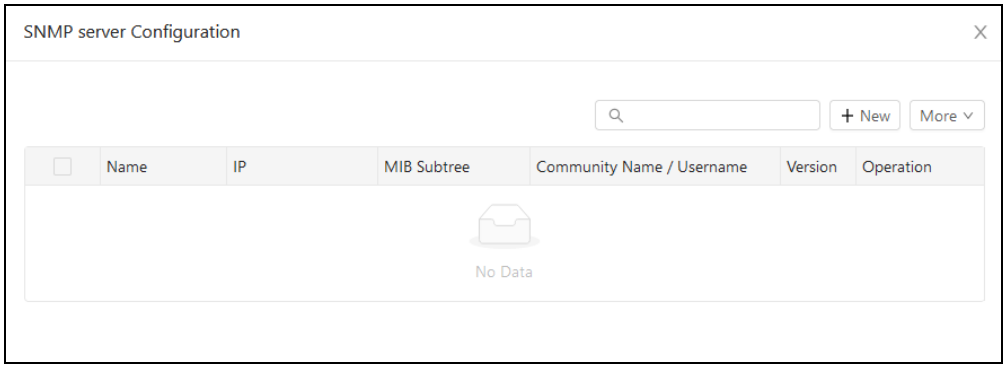
Parameter		Description
		destination IP address and MAC address. • No match: The packets will be discarded.
	Match source IP/MAC	Checks whether the source IP address and source MAC address of a packet match entries included in IP/MAC binding list. • If the IP/MAC binding list is empty, packets will not be checked against list. • If the IP/MAC binding list is not empty, ✓ a packet will be discarded if there is a match for its source IP address but not for its MAC address. ✓ a packet will be passed through if no match is found for its source IP address, regardless of whether there is a match for its MAC address.
Cross-layer MAC Recognition	Enable cross-layer 3 MAC recognition	Select yes to enable the cross-layer 3 MAC recognition. After it's enabled, NIPS recognizes MAC addresses of intranet users in a cross-layer 3 environment as follows: NIPS regularly obtains the ARP table on the layer 3 switch via SNMP, in order to get IP/MAC bindings of all PCs on the intranet Note The SNMP service must be enabled on the layer 3 switch before cross-layer 3 MAC recognition works properly.
	SNMP Server Access Timeout	Specifies the maximum interval for NIPS to wait for an ARP reply from the layer 3 switch. If receiving no reply during the specified period, NIPS does not make the next query until the interval specified with SNMP Server Access Interval expires.
	SNMP Server Access Interval	Specifies how long NIPS has to wait before sending the next ARP request to the layer 3 switch.

Configuring an SNMP Server

If there is more than one layer 3 switch on 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.

Step 1 On the **IP/MAC Binding** page, click **Configure SNMP server** to configure a layer 3 switch.

Figure 6-25 Configuring an SNMP server



Step 2 Click **New** in the upper-right corner of the dialog box to configure an SNMP server.

Figure 6-26 Configuring an SNMP server

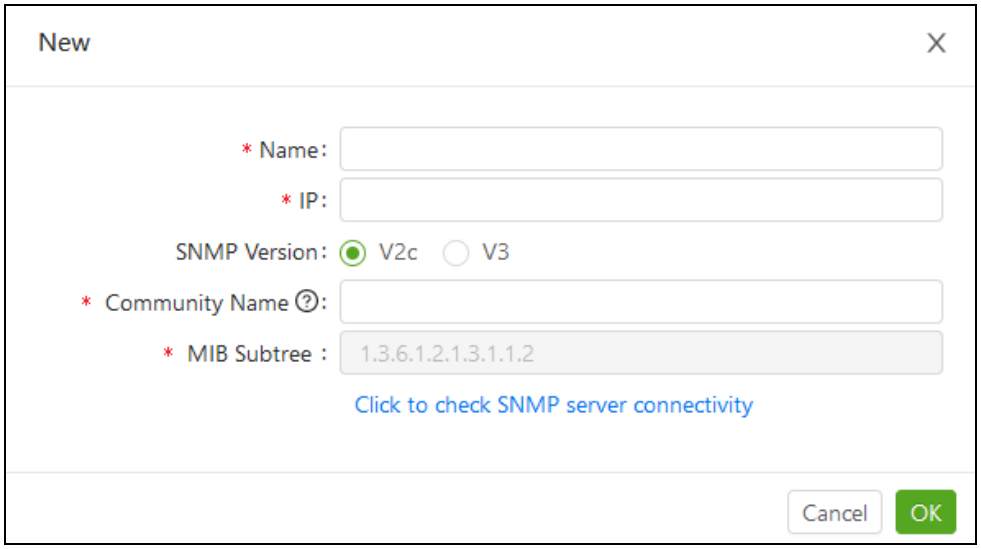


Table 6-18 shows the parameters for configuring an SNMP server.

Table 6-18 Parameters for configuring an SNMP server

Parameter	Description
Name	String that uniquely identifies the layer 3 switch.
IP	IP address of the switch's nearest port to NIPS.
SNMP Version	SNMP version supported by the layer 3 switch. The SNMP version must be V2c or V3; otherwise, cross-layer 3 MAC recognition cannot be implemented.
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.

Step 3 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, "The connection succeeded" is displayed; otherwise, "The connection failed" is displayed.

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

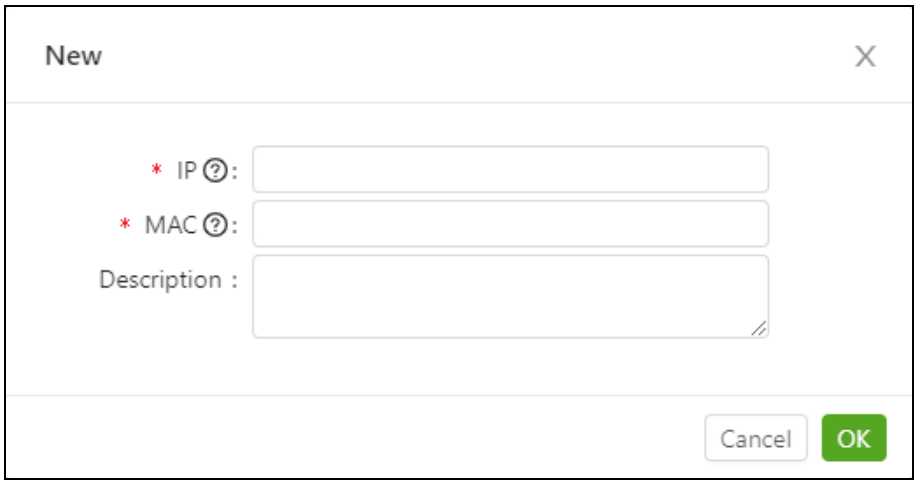
----End

Creating an IP/MAC Binding Entry

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

Step 1 Click **New** in the **IP/MAC Binding List** area.

Figure 6-27 Dialog box for creating an IP/MAC binding entry



Step 2 Type the IP address and MAC address in the **New** dialog box.

Note	When creating an IP/MAC binding entry, note the following: • The new IP/MAC pair cannot be the same as an existing IP address or MAC address in the binding list. • The new IP address cannot be the same as the IP address of NIPS's gateway.

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

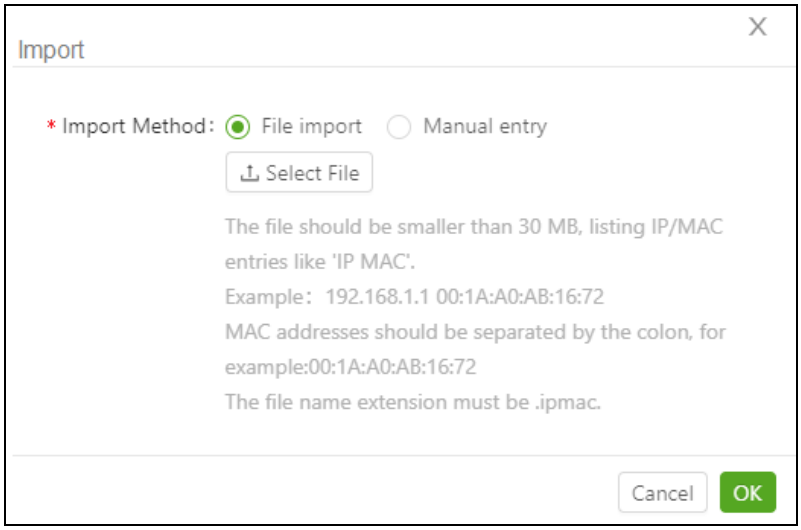
----End

Importing IP/MAC Binding Entries

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

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

Figure 6-28 Importing a file of IP/MAC binding entries



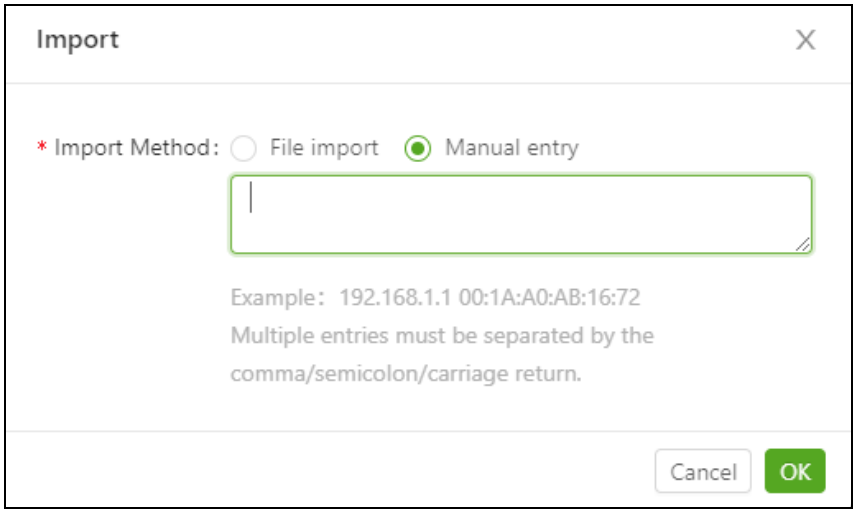
Select **File import** for **Import Method**, click **Select File** to select a local file, and then click **OK** to import the file. Such a file must meet the following conditions:

- The file should list IP/MAC pairs in the format of "IP address MAC address". That is to say, the IP address and MAC address must be separated by a space. In each MAC address, octets must be separated by a colon, like 00:1A:A0:AB:16:72.
- The file name extension must be .ipmac.

Note	When importing IP/MAC binding entries, note the following: • The IP address and MAC address in each IP/MAC binding entry cannot be the same as those included in existing entries. • The IP address in each IP/MAC binding entry cannot be the same as the IP address of NIPS's network gateway.

- **Manual entry**: Select **Manual entry**, type one or more IP/MAC binding entries, and click **OK**.

Figure 6-29 Manually entering IP/MAC binding entries



Each IP/MAC binding entry must be in the format of "IP address MAC address". That is to say, the IP address and MAC address must be separated by a space. In each MAC address, octets must be separated by a colon, like 00:1A:A0:AB:16:72.

Multiple IP/MAC binding entries must be separated by a carriage return, with each in a separate line.

Performing Other Operations on IP/MAC Entries

NIPS also allows you to perform the following operations on IP/MAC binding entries:

- Editing an IP/MAC binding entry

  Click in the **Operation** column of an IP/MAC binding entry to edit it.
- Deleting IP/MAC binding entries

  You can use one of the following methods to delete IP/MAC binding entries:

  – Click in the **Operation** column of an IP/MAC binding entry to delete it.

  – Select multiple IP/MAC binding entries, point to **More**, and click **Delete selected** to delete entries in batches.

  – Point to **More** and click **Delete all** to clear the IP/MAC binding list.
- Enabling/Disabling IP/MAC binding entries

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

  – To disable an IP/MAC binding entry, clear the check box in the **Use** column. To enable it, reselect the check box.

  – Select multiple IP/MAC binding entries, click **Enable** or **Disable** to enable or disable entries in batches.

  – Point to **More** and click **Enable all** or **Disable all** to enable or disable all entries.

6.9 Collaboration with Firewalls

NIPS can collaborate with NSFOCUS Next-Generation Firewall (NF).

To configure such collaboration, follow these steps:

Step 1 Choose **Policies** > **Firewall Collaboration**.

Figure 6-30 Firewall Collaboration page

Step 2 Configure parameters.

Table 6-19 Parameters for configuring NIPS to collaborate with firewalls

Parameter		Description
NSFOCUS NF	Enable	If NSFOCUS NF is deployed on the network, you can choose to enable NIPS's collaboration with the firewall. Note It is not enough to enable such collaboration on NIPS. You also need to enable it on NSFOCUS NF.
	Firewall IP	After enabling collaboration with NSFOCUS NF, you need to type the IP address of the firewall. You can type multiple IP addresses, separated by a comma, like 192.168.1.3,192.168.1.5.
	Password	Specifies a password for NIPS to collaborate with NSFOCUS NF.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

6.10 User Management

User management involves user authentication, authentication policy management, user identification, intelligent account identification, and viewing of online users, authentication logs, and authentication status.

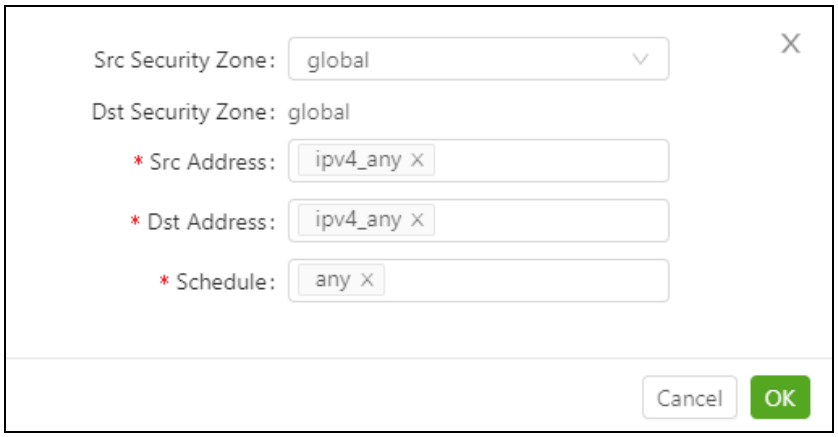
6.10.1 Authentication Policy

NIPS authenticates a user when packets of the user match an authentication policy. For how to configure user authentication, see Authentication Settings. This section describes how to create an authentication policy.

Step 1 Choose **Policies** > **User & Authentication** > **Policies**.

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

Figure 6-31 Dialog box for creating an authentication policy



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

Table 6-20 Parameters for configuring an authentication policy

Parameter	Description
Src Security Zone	Specifies a security zone. Users sending packets from the specified security zone need authentication. **global** indicates that users sending packets from any security zones need authentication.
Dst Security Zone	Specifies a security zone. Users sending packets to the specified security zone need authentication. **global** indicates that users sending packets to any security zones need authentication. **Note** The destination security zone automatically refreshes with a matching value each time you select a source security zone.
Src Address	Specifies a source address or more to which this policy will apply. The value **any** indicates that users sending packets from any IP address need authentication.
Dst Address	Specifies a destination address or more to which this policy will apply. The value **any** indicates that users sending packets to any IP address need authentication.
Schedule	Specifies a period when this policy is valid.

Parameter	Description
	The value **any** indicates that this policy is always valid.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

6.10.2 Users in AD

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:

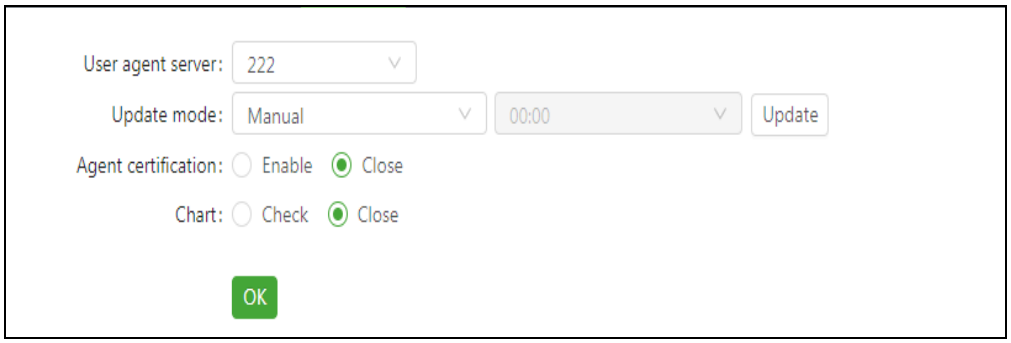
Step 1 Choose **Policies** > **User & Authentication** > **Users in AD**.

By default, the user agent server is off.

Step 2 Select a server for AD domain authentication.

Related parameters are displayed, as shown in Figure 6-32.

Figure 6-32 Users in AD page



Step 3 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 at that time regularly.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

Step 6 (Optional) Click **Update** to immediately synchronize the user list on the AD domain server to NIPS.

Step 7 (Optional) Click **Check** for **Chart** to view users displayed in the tree structure.

----End

6.10.3 Authentication Settings

NIPS can authenticate users locally or via a third-party server, which can be any of the following:

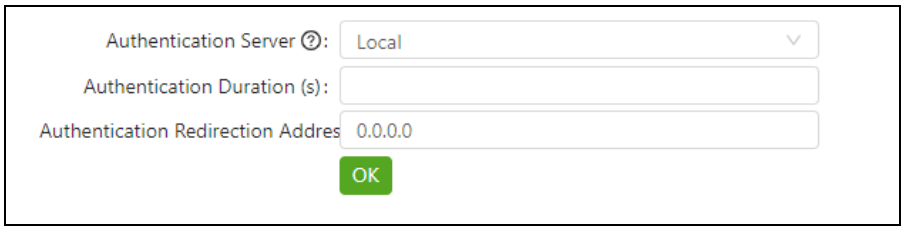
- AD domain authentication server
- RADIUS authentication server
- LDAP authentication server

For how to configure an authentication server, see Authentication Server.

To configure user authentication, follow these steps:

Step 1 Choose **Policies** > **User & Authentication** > **Authentication Settings**.

Figure 6-33 Authentication Settings page



Step 2 Configure parameters.

Table 6-21 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 Backup.
Authentication Duration (s)	Time that authentication lasts.
Authentication Redirection Address	Specifies the IP address of a page to which NIPS redirects a client for 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 **OK** to save the settings.

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

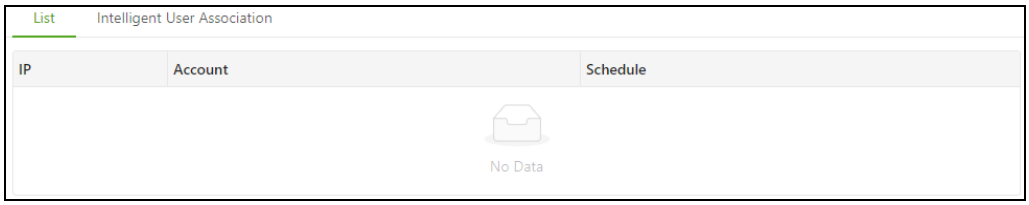
6.10.4 Intelligent Account Identification

NIPS supports intelligent account identification, which will be available after you configure intelligent user association conditions.

6.10.4.1 List

The **List** page lists users on all IP addresses identified by NIPS, as shown in Figure 6-34.

Figure 6-34 List of users associated with IP addresses



6.10.4.2 Intelligent User Association

NIPS provides the intelligent user association function. After this function is enabled, NIPS can identify users on 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.

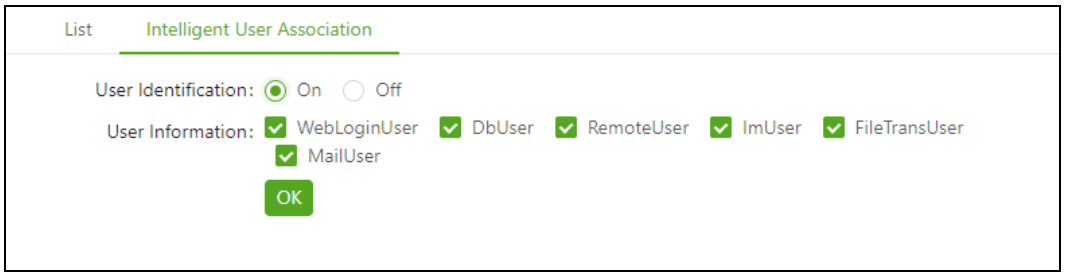
After intelligence user association is enabled, you can view associated users of IP addresses on the List page.

To configure intelligent user association, follow these steps:

Step 1 Choose **Policies** > **User & Authentication** > **Related Account** > **Intelligent User Association**.

Step 2 Click **On** for **User Identification** and select user types.

Figure 6-35 Intelligent User Association page



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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

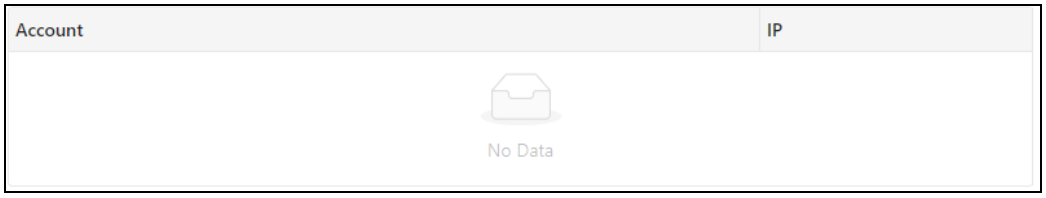
----End

6.10.5 Online Users

NIPS can display current online users in real time, including the login account and IP address.

Choose **Policies** > **User & Authentication** > **Online Users**.

Figure 6-36 List of online users

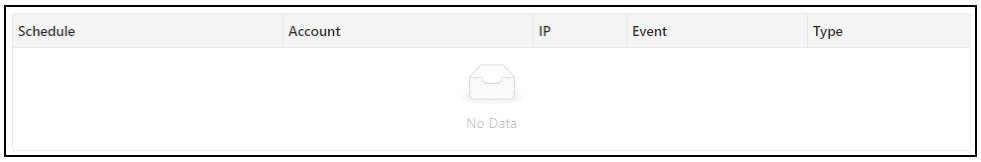


6.10.6 Authentication Log

The authentication log is a record of user authentication by NIPS. Authentication logs help you manage authentication methods used for network communication.

Choose **Policies** > **User & Authentication** > **Logs**.

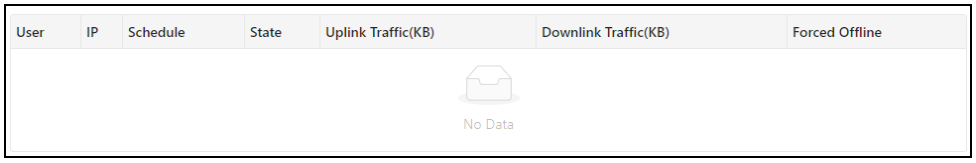
Figure 6-37 Authentication Log page



6.10.7 Authentication Status

Choose **Policies** > **User & Authentication** > **Authentication Status**.

Figure 6-38 Authentication status log



Selecting the check box in the **Forced Offline** column of an online user gets this user offline.

6.11 Geodatabase

NIPS comes with geodatabases, which are automatically loaded at startup.

After an alert is triggered, NIPS queries the source IP address and destination IP address in the public IP database and private IP database respectively.

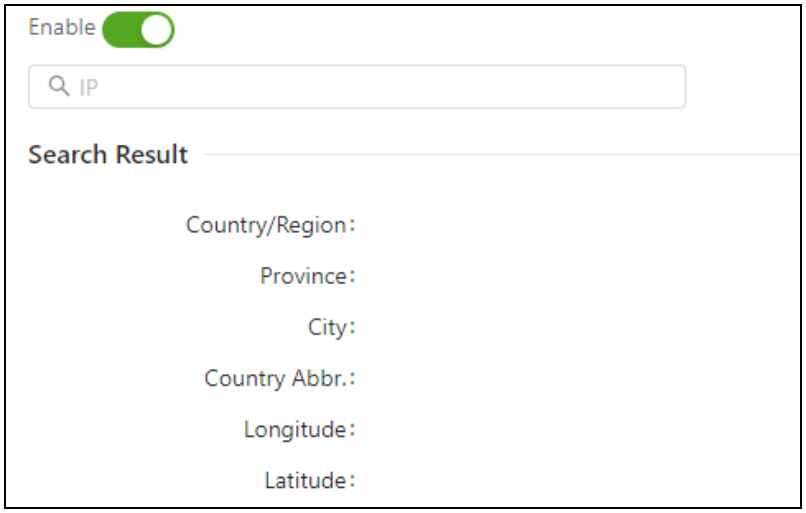
- If the source/destination IP address can be queried in the public IP database, the system returns its geographical location, which is then displayed in the related log.
- If the source/destination IP address can be queried in the private IP database, the system returns "Reserved", which is then displayed as the geographical location in the related log.
- If the source/destination IP address is a public one, which, however, is not queried in the public IP database, the system returns "None" and the log database records the location as "NULL".

6.11.1 Public IP Geodatabase

After the public IP database is enabled, you can query public IP addresses and the database will return their detailed geographical information, including the country/region, province, city, abbreviation, longitude, and latitude.

Choose **Policies** > **Regions** > **Public IP**.

Figure 6-39 Public IP geodatabase



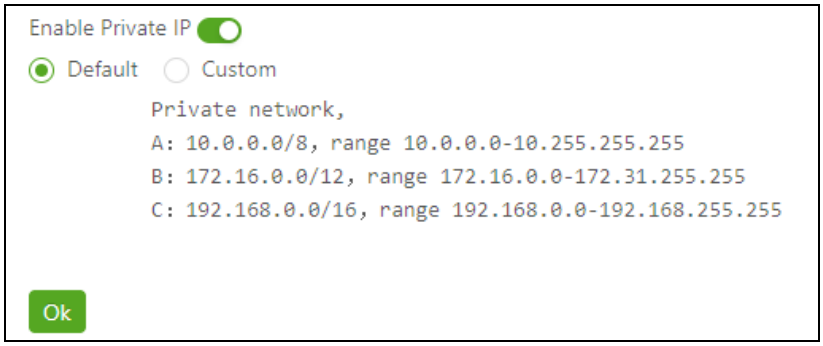
Type an IP address and press **Enter**. Then the geographical information of this IP address is listed below.

6.11.2 Private IP Geodatabase

After private segment identification is enabled, you can further select **Default** or **Custom**.

Choose **Policies** > **Regions** > **Private IP**.

Figure 6-40 Private IP geodatabase



- Select **Default** and click **OK**.
- Select **Custom**, type the IP address database that you want to customize, and click **OK**.

  In the database, IP addresses should be separated by a carriage return, with each in a separate line. You can type individual IP addresses, IP segments, and IP address/netmask, like 202.168.1.1, 202.168.1.1-202.168.1.155, and 202.168.1.0/24.

6.12 Mining Protection

This policy is used to detect the mining protocol in the traffic and analyze the webpage mining. Additionally, NIPS supports linkage with NTI to detect the access to DNS miner pool.

To configure the policy, follow these steps:

Step 1 Choose **Policies** > **Mining Protection**.

Figure 6-41 Mining Protection page

Step 2 Configure parameters.

Table 6-22 Parameters for configuring a mining protection policy

Parameter		Description
Mining Protection	Enable	Controls whether to enable the mining protection policy.
	Reporting Cycle	After enabling the mining protection policy, you need to specify the logging time after a mining protocol is detected. You can type an integer in the range of 0–3600, in seconds. Typing **0** means the log will be immediately reported.

Parameter		Description
	Block Threshold	Specifies a threshold for blocking. If the value specified here is equal to or smaller than the confidence value of the mining log, traffic will be blocked. You can type an integer in the range of 0–100.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

7 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 define objects before configuring policies. These objects include the signature, address, service, application, schedule, and sensitive data.

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. This makes policy management simpler and more flexible. For how to configure policies, see Policies.

This chapter describes object configuration on NIPS, containing the following sections:

Section	Description
Service	Describes how to configure service-related objects.
Application	Describes how to configure application-related objects.
Schedule	Describes how to configure schedule-related objects.
Address	Describes how to configure address-related objects.
Network Intrusion	Describes how to configure intrusion-related objects.
Malware	Describes how to configure malicious file-related objects.
Web Security	Describes how to configure web security-related objects.
C&C Communication	Describes how to configure C&C communication-related objects.
Callback Monitoring	Describes how to configure the callback monitoring blacklist and whitelist.
URL Filtering	Describes how to configure URL filter-related objects.
Application Control	Describes how to configure application management-related objects.
Data Loss Prevention	Describes how to configure DLP-related objects.

7.1 Service

Service-related objects are used to describe system services, custom services, service groups, and timeout periods.

7.1.1 Predefined Service

NIPS comes with predefined services. Based on these services, NIPS can automatically identify common protocols, such as TCP and UDP, and protocols on non-fixed ports.

To query system services, do as follows:

Choose **Objects** > **Service** > **Predefined**.

Figure 7-1 Predefined services

ID	Name	Protocol	Option	Description
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
310010	ssh[t]	tcp	Source Port:any:Destination Port:22	SSH Remote Login Proto...
310011	telnet[t]	tcp	Source Port:any:Destination Port:23	
310012	smtp[t]	tcp	Source Port:any:Destination Port:25	Simple Mail Transfer Pro...
310013	time[t]	tcp	Source Port:any:Destination Port:37	
310014	time[u]	udp	Source Port:any:Destination Port:37	
310015	nameserver[t]	tcp	Source Port:any:Destination Port:42	Host Name Server

The **Predefined** page lists all predefined services on NIPS. You can only view and reference these services, but cannot create, edit, or delete them.

7.1.2 Custom Service

You can configure custom services, that is, custom service ports, as required. The procedure is as follows:

Step 1 Choose **Objects** > **Service** > **Custom**.

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

Note that the **New** dialog box for configuring a TCP or UDP service object is different from that for an IP service object.

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

Table 7-1 Parameters for configuring a custom service object

Parameter	Description
Protocol	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** must be specified. When **Protocol** is set to **IP**, **Type** must be specified.
Name	Name of the custom service.

Parameter	Description
	The name must be unique and cannot contain the following special characters: % \ ` < > ' & "
Source Port	Source port used by the service object. This parameter must be specified only when **Protocol** is set to **TCP** or **UDP**. You can specify multiple ports or ranges of ports whose number ranges from 0 to 65535.
Destination Port	Destination port used by this service. This parameter must be specified only when **Protocol** is set to **TCP** or **UDP**. You can specify multiple ports or ranges of ports whose number ranges from 0 to 65535.
Type	IP protocol ID, such as **1** that indicates ICMP and **2** that indicates IGMP. The value range is 0–255. This parameter must be specified when **Protocol** is set to **IP**.
Description	Brief description of the custom service.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

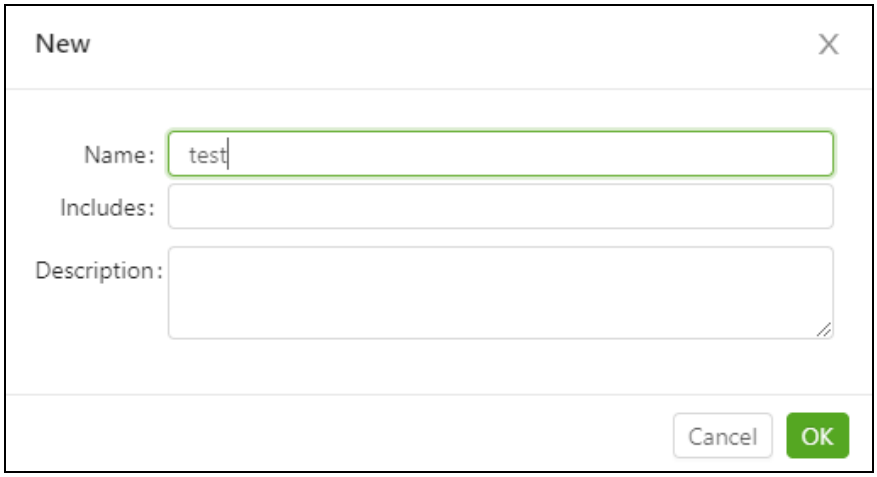
7.1.3 Service Group

A service group here refers to a logical collection of predefined services, custom services, and existing service groups. To configure a service group, follow these steps:

Step 1 Choose **Objects** > **Service** > **Groups**.

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

Figure 7-2 Configuring a group object



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

Table 7-2 Parameters for configuring a group object

Parameter	Description
Name	Name of the service group. The name must be unique and cannot contain the following special characters: % \ ` < > ' & "
Includes	Specifies objects to be contained in the service group.
Description	Brief description of the service group.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.1.4 Service Timeout

Timeouts for communication can be specified for most protocols. You can specify a service timeout object as required.

To configure a service timeout period, follow these steps:

Step 1 Choose **Objects** > **Service** > **Service Timeout**.

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

Figure 7-3 Configuring a service timeout object

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

Table 7-3 Parameters for configuring a service timeout period

Parameter	Description
Name	Specifies the type of the protocol used for communication. Note

Parameter	Description
	The timeout period for each protocol type can be configured only once.
Timeout	Specifies the timeout period (in seconds) for communication. The default value is **0**, indicating 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. The setting of this field depends on the actual interval required between two consecutive data flows of a protocol. A longer interval requires a larger value.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.2 Application

Application-related objects are used to describe various applications such as Kuwo Player. The system comes with predefined applications. Also, you can configure custom applications and filters to filter packets destined for applications specified in application management policies.

This section describes how to view predefined system applications, create a custom application, and configure an application group and a filter.

7.2.1 Predefined Application

NIPS comes with predefined applications. You can only reference and view them, but cannot create, edit, or delete them.

To query a predefined application, follow these steps:

Step 1 Choose **Objects** > **Application** > **Predefined**.

Step 2 Click the plus sign (+) beside the object name to shows its details.

Figure 7-4 Application page

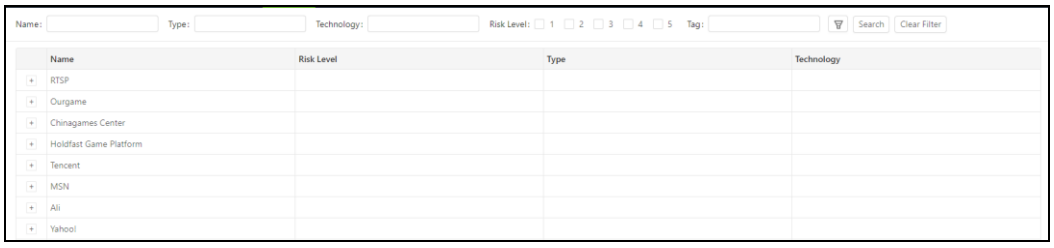


Table 7-4 describes parameters in the application list.

Table 7-4 Predefined application list parameters

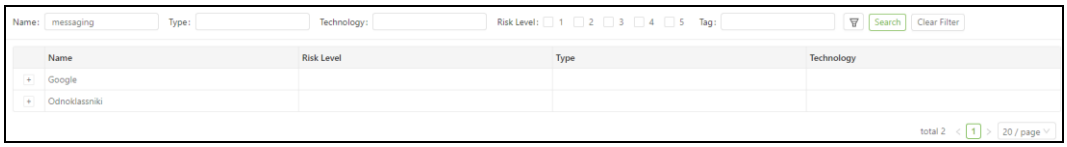
Parameter	Description
Name	Name of a predefined application.
Risk Level	Risk level of a predefined application. The value is an integer ranging from 1 to 5, and a larger value indicates a higher risk level.
Type	Type of a predefined application.
Technology	Technology on which a predefined application is based. The value can be **browser-based**, **client-server**, **network-protocol**, **peer-to-peer**, or **unknown**.

Step 3 Type an object name in the **Name** text box and click **Search**.

Related objects are listed below.

You can also specify the type and technology to view related application objects.

Figure 7-5 Query result

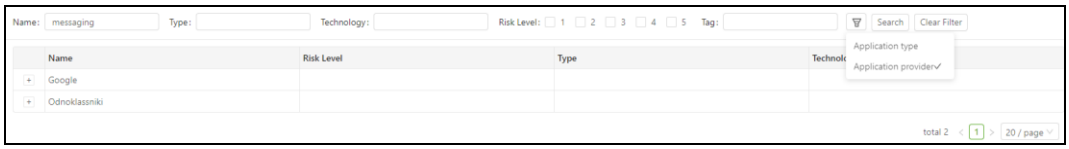


NIPS lists applications by application type by default.

Step 4 Point to and click **Application provider**.

Applications are then listed by application provider, as shown in Figure 7-6.

Figure 7-6 Searching for predefined applications



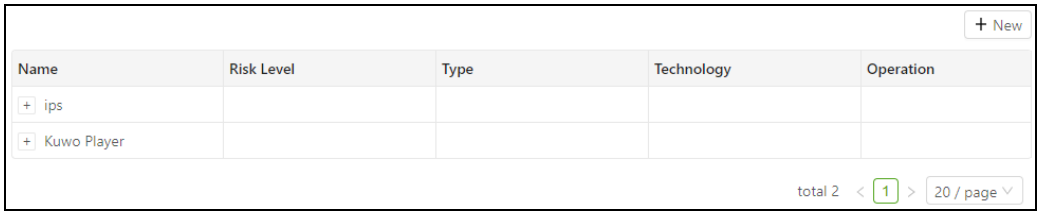
----End

7.2.2 Custom Application

In addition to predefined applications, you can configure custom applications. To configure a custom application, follow these steps:

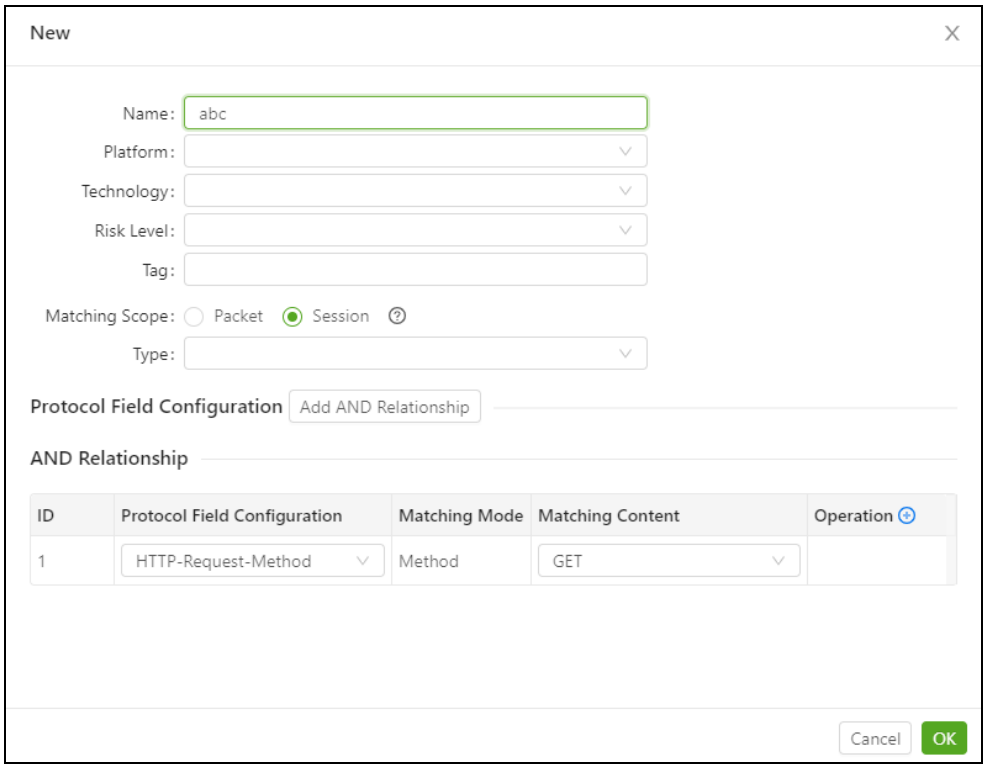
Step 1 Choose **Objects** > **Application** > **Custom**.

Figure 7-7 Custom application page



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

Figure 7-8 Configuring a custom application



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

Table 7-5 Parameters for configuring a custom application

Parameter	Description
Name	Name of the application.
Platform	Specifies a platform on which the application runs.
Technology	Specifies a technology on which the application is based. The value can be **browser-based**, **client-server**, **network-protocol**, **peer-to-peer**, or **unknown**.
Risk Level	Specifies a risk level for 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 level of an application, see Calculating the Risk Level of an Application.

Parameter	Description
Tag	Specifies a tag for the application. The value can be Unknown, Evasive, Excessive Bandwidth, Prone to Misuse, Transfers Files, Tunnels Other Apps, Used by Malware, Vulnerability, Widely used, and Mobile.
Matching Scope	Specifies the matching scope, which can be either of the following: **Packet**: indicates that matching and logical determination are conducted based on individual packets. A packet is the minimum transmission unit on a packet-switched network. The coverage of packet matching is smaller than that of session matching. **Session**: indicates that matching and logical determination are conducted based on individual sessions. A session is an uninterrupted request-response sequence between a client and a server.
Type	Specifies the type of the application.

Step 4 Configure protocol fields.

For how to configure protocol fields, see Step 4 in Advanced Signature.

Step 5 Click **OK** to save the settings.

Step 6 Click **Commit** in the quick access bar to make the settings take effect.

----End

Calculating the Risk Level of an Application

The risk level of an application is calculated based on all its tags. From the perspective of severity, tags are categorized into three types:

- High-level risk: indicates that an application is vulnerable or can be easily exploited by malware, thus probably causing a severe impact on hosts or the entire network.
- Medium-level risk: indicates that an application involves data transfers or uses other applications as pipelines, thus potentially imposing an impact on the network.
- Low-level risk: indicates that an application is widely used but does not impose any impact on network security.

Table 7-6 lists tags and their corresponding risk levels.

Table 7-6 Risk level of tags

No.	Tag	Risk Level
1	Unknown	Low
2	Evasive	Medium
3	Excessive Bandwidth	Low
4	Prone to Misuse	Low
5	Transfer Files	Medium
6	Tunnels Other Apps	Medium
7	Used by Malware	High

No.	Tag	Risk Level
8	Vulnerability	High
9	Widely used	Low
10	Mobile	Low

7.2.3 Application Group

NIPS provides the group function for you to pick out desired data among massive amounts of data. You can configure groups to filter data handled by NIPS based on specific conditions.

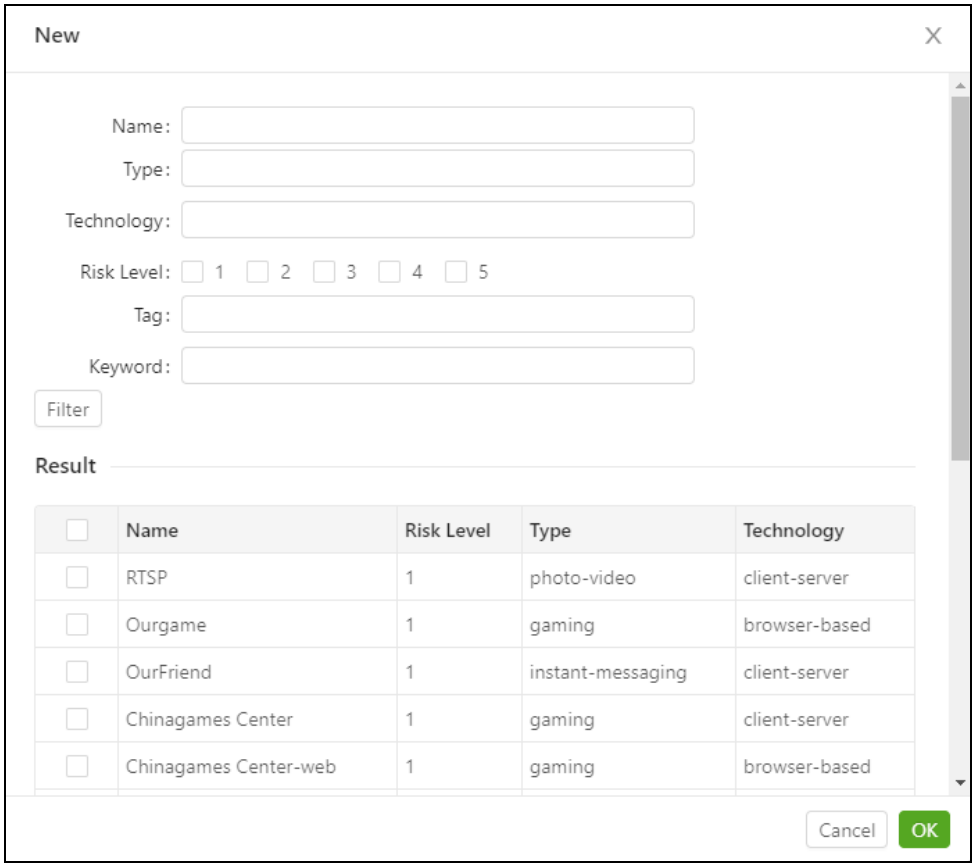
Note	A filter filters applications based on application types and tags, while groups provide better flexibility by allowing you to group applications based on keywords.

An application group can achieve the intended filtering effect only after being applied to application management policies or bandwidth management policies. This section describes how to create an application group. The procedure is as follows:

Step 1 Choose **Objects** > **Application** > **Groups**.

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

Figure 7-9 Creating an application group



Step 3 Type the name of the new group.

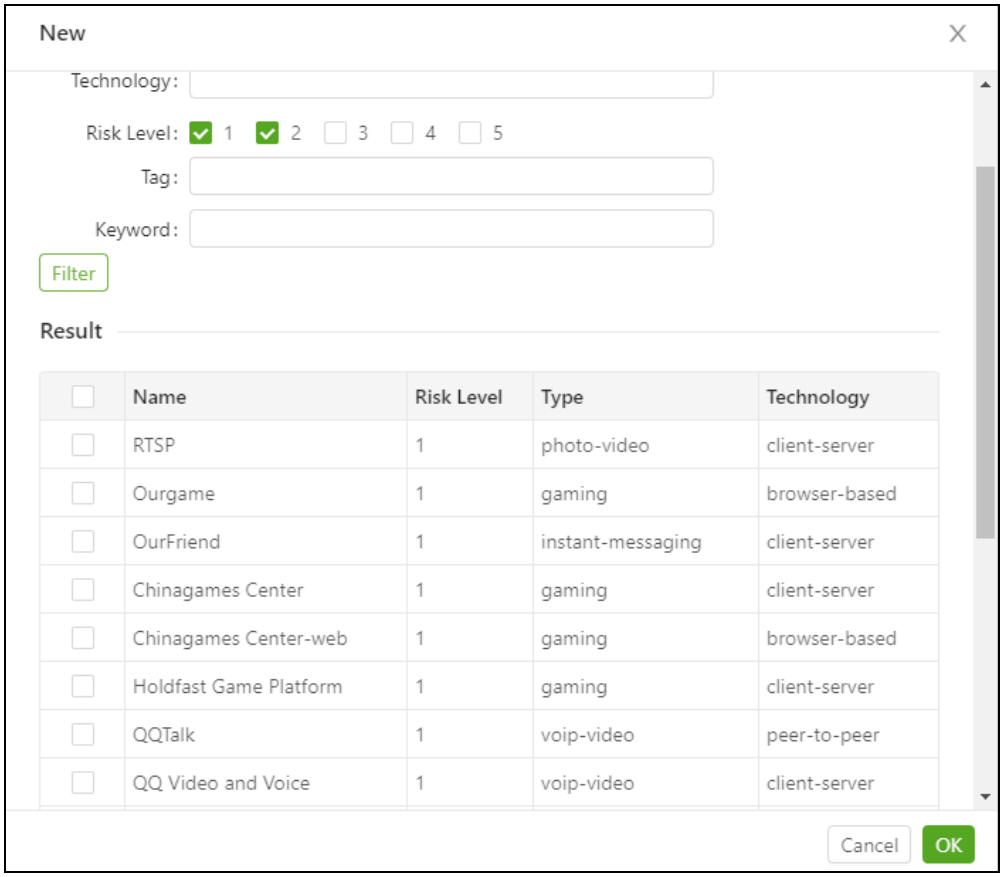
Step 4 Configure other parameters.

Table 7-7 Parameters for grouping applications

Parameter	Description
Type	Specifies the types of applications to be grouped.
Technology	Specifies the technologies by which applications to be grouped are implemented.
Risk Level	Specifies the risk levels of applications to be grouped.
Tag	Specifies the tags of applications to be grouped.
Keyword	Specifies keywords for a fuzzy search for applications.

Step 5 Click **Filter** to view all applications that meet the filtering conditions.

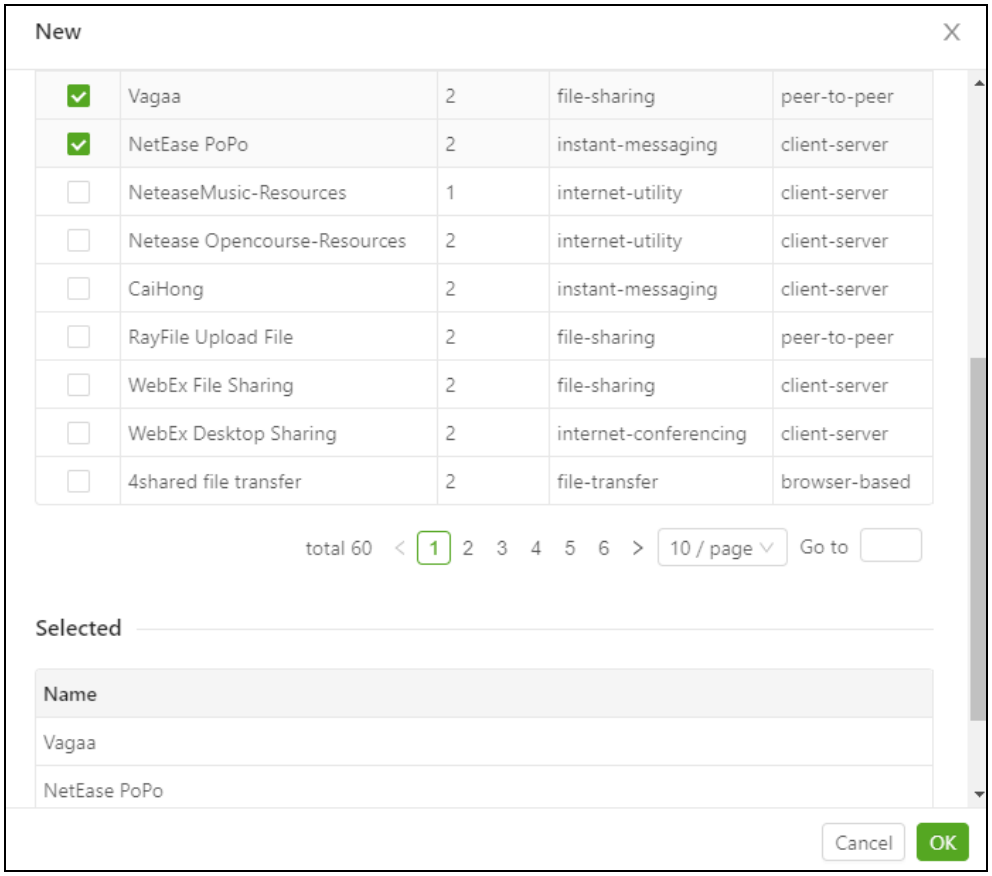
Figure 7-10 Viewing filtering results



Step 6 Select applications to be grouped together.

Select the check box beside the application name. Then the selected applications are listed in the **Selected** area, as shown in Figure 7-11.

Figure 7-11 Viewing selected applications



Clearing the check box in the **Result** list deletes this application from the **Selected** list.

Step 7 Click **OK** to save the settings.

Step 8 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.2.4 Filter

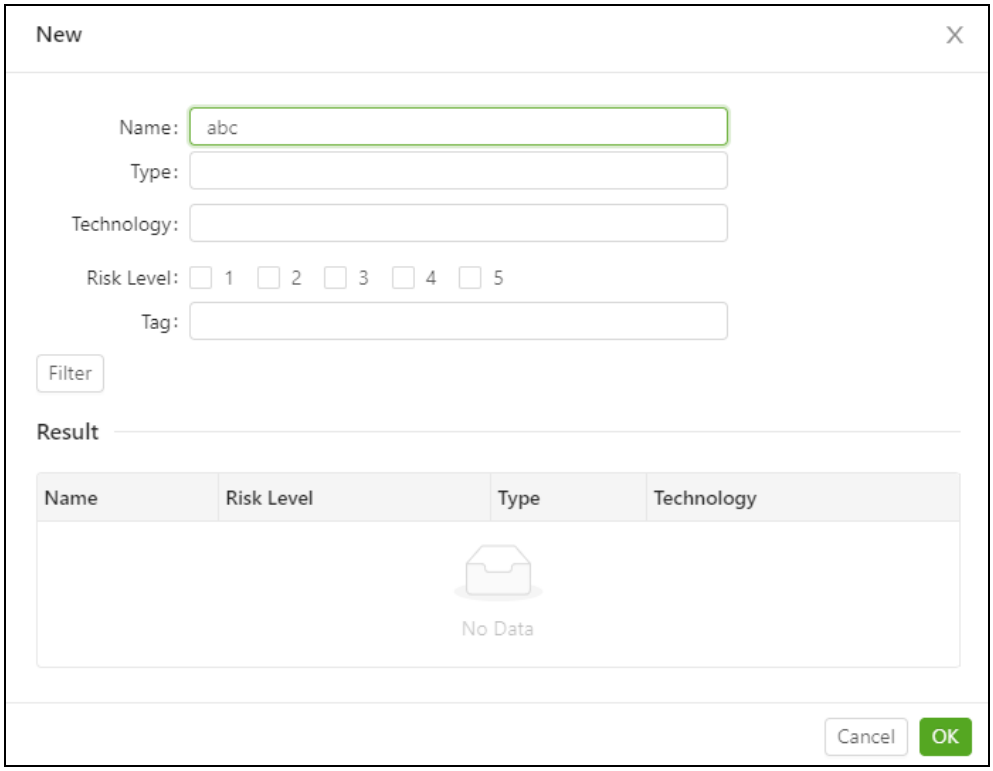
NIPS provides the filter function for you to pick out desired data among massive amounts of data. You can configure filters to filter data handled by NIPS based on specific conditions.

Filters can take effect only after being applied to application management policies. This section describes how to create a filter. The procedure is as follows:

Step 1 Choose **Objects** > **Application** > **Filters**.

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

Figure 7-12 Creating a filter



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

Table 7-8 Parameters for creating a filter

Parameter	Description
Name	Specifies the name of the filter.
Type	Specifies the types of applications to be filtered.
Technology	Specifies the technologies by which applications to be filtered are implemented.
Risk Level	Specifies the risk levels of applications to be filtered.
Tag	Specifies the tags of applications to be filtered.

Step 4 Click **Filter** to find all objects that meet the filtering conditions.

Step 5 Click **OK** to save the settings.

Step 6 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.3 Schedule

Schedule-related objects represent time ranges. They include custom schedules and schedule groups. This section describes how to configure a custom schedule and a schedule group.

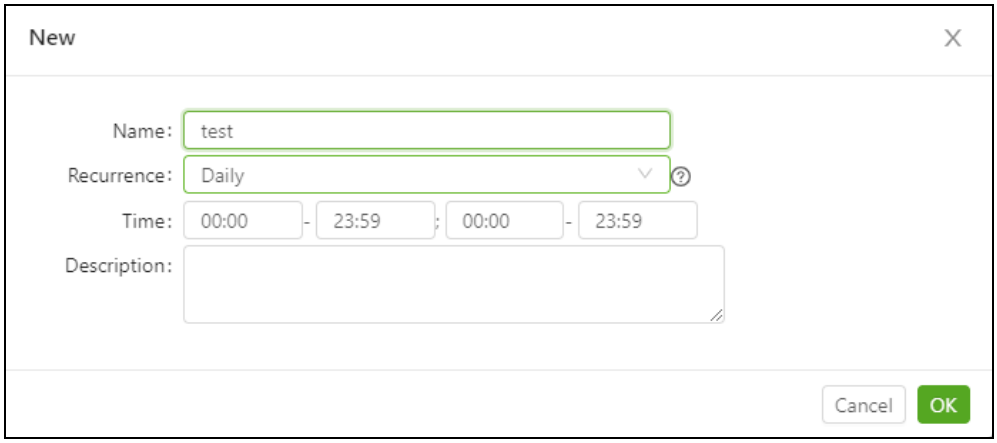
7.3.1 Custom Schedule

Each schedule contains two time periods, which you can customize as required. To configure a custom schedule, follow these steps:

Step 1 Choose **Objects** > **Schedule** > **Custom**.

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

Figure 7-13 Configuring a custom schedule



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

Table 7-9 Parameters for configuring a custom schedule

Parameter	Description
Name	Name of the custom schedule. The name must be unique and cannot contain the following special characters: % \ ` < > ' & "
Recurrence	Specifies how the schedule recurs, which can be **Daily**, **Weekday** (Monday to Friday), **Weekly**, or **Monthly**.
Time	Time periods contained in the object. You can configure two time periods. If only one time period is needed, you should set the second time period to **00:00-00:00**. If **Type** is set to **Monthly**, you also need to specify a date.
Description	Brief description of the custom schedule.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.3.2 Schedule Group

A schedule group here refers to a logical collection of custom schedules and existing schedule groups. To create a schedule group, follow these steps:

Step 1 Choose **Objects** > **Schedule** > **Groups**.

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

Figure 7-14 Configuring a schedule group

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

Table 7-10 Parameters for configuring a schedule group

Parameter	Description
Name	Name of the schedule group. The name must be unique and cannot contain the following special characters: % \ ` < > ' & "
Includes	Specifies schedules and existing schedule groups to be contained in this group.
Description	Brief description of the schedule group.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.4 Address

Address-related objects are used to describe network devices and network groups. Currently, NIPS supports the following address-related objects:

- IP/netmask

- IP node
- MAC address
- IP pool
- Group

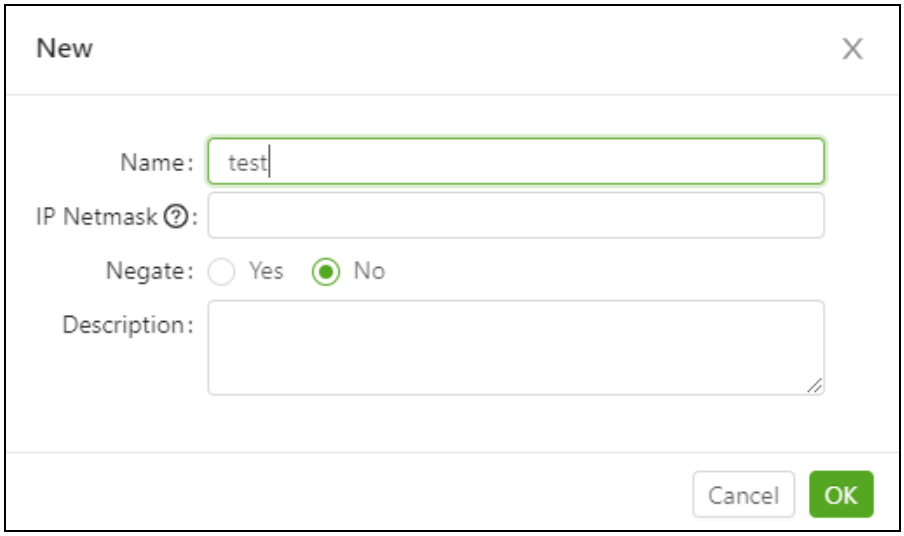
7.4.1 IP/Netmask

An IP/netmask specifies a network segment, that is, an IPv4 or IPv6 subnet. To configure a subnet, follow these steps:

Step 1 Choose **Objects** > **Addresses** > **IP Netmask**.

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

Figure 7-15 Configuring a subnet



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

Table 7-11 Parameters for configuring a subnet

Parameter	Description
Name	Name of the subnet. The name must be unique and cannot contain the following special characters: % \ ` < > ' & "
IP Netmask	Specifies the IPv4 or IPv6 address and netmask.
Negate	Controls whether to reverse the IP address setting. It has the following values: • **Yes**: indicates that other segments than the specified one will be taken as the object. • **No**: indicates that the specified segment will be taken as the object.
Description	Brief description of the subnet.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.4.2 IP Node

An IP node refers to a host specified with an IPv4 or IPv6 address. To configure an IP node, follow these steps:

Step 1 Choose **Objects** > **Addresses** > **IP Nodes**.

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

Figure 7-16 Configuring an IP node

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

Table 7-12 Parameters for configuring an IP node

Parameter	Description
Name	Name of the IP node. The name must be unique and cannot contain the following special characters: % \ ` < > ' & "
IP	Specifies the IP address of the node, which can be an IPv4 address (such as 192.168.1.1) or IPv6 address (such as fe80::250:56ff:fec0:8).
Negate	Controls whether to reverse the IP address setting. It has the following values: • **Yes**: indicates that other IP addresses than the specified one will be taken as the object. • **No**: indicates that the specified IP address is used as the object.
Description	Brief description of the IP node.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

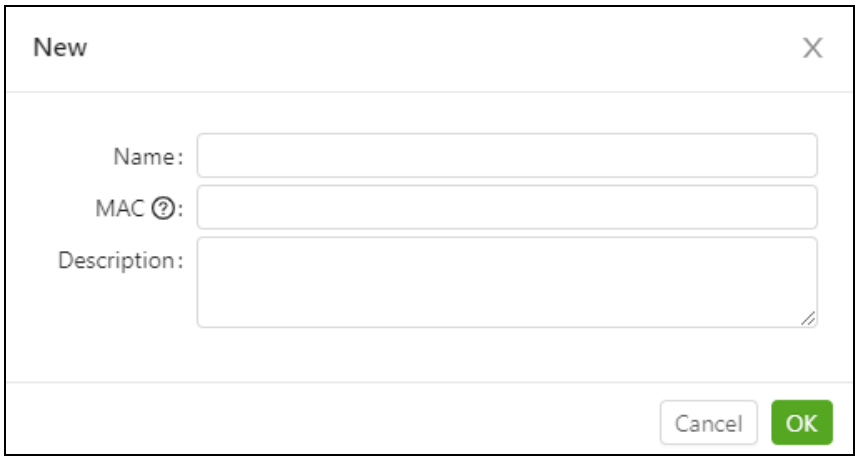
7.4.3 MAC Address

An individual MAC address is taken as an object. To configure such an object, follow these steps:

Step 1 Choose **Objects** > **Addresses** > **MAC Address**.

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

Figure 7-17 Configuring a MAC address



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

Table 7-13 Parameters for configuring a MAC address

Parameter	Description
Name	Name of the MAC address. The name must be unique and cannot contain the following special characters: % \ ` < > ' & "
MAC	Specifies a MAC address. 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.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

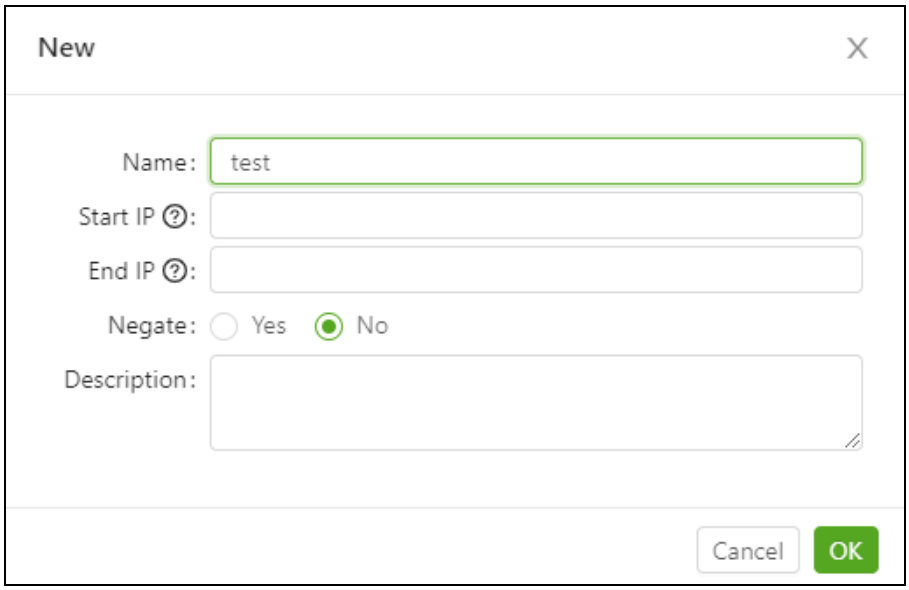
7.4.4 IP Pool

An IP pool is a range of consecutive IPv4 or IPv6 addresses that identify hosts. To configure such an object, follow these steps:

Step 1 Choose **Objects** > **Addresses** > **IP Pools**.

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

Figure 7-18 Configuring an IP pool



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

Table 7-14 Parameters for configuring an IP pool

Parameter	Description
Name	Name of the IP pool. The name must be unique and cannot contain the following special characters: % \ ` < > ' & "
Start IP	Specifies the first IPv4 or IPv6 address in the IP pool. Note The start IP address and end IP address must be of the same protocol version, that is, both are IPv4 or IPv6 addresses.
End IP	Specifies the last IPv4 or IPv6 address in the IP pool. Note The start IP address and end IP address must be of the same protocol version, that is, both are IPv4 or IPv6 addresses. Besides, the end IP address must be greater than the start IP address.

Parameter	Description
Negate	Controls whether to reverse the IP address settings. It has the following values: • **Yes**: indicates that other IP address ranges than the specified one will be taken as the object. • **No**: indicates that the specified IP address range will be taken as the object.
Description	Brief description of the IP pool.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

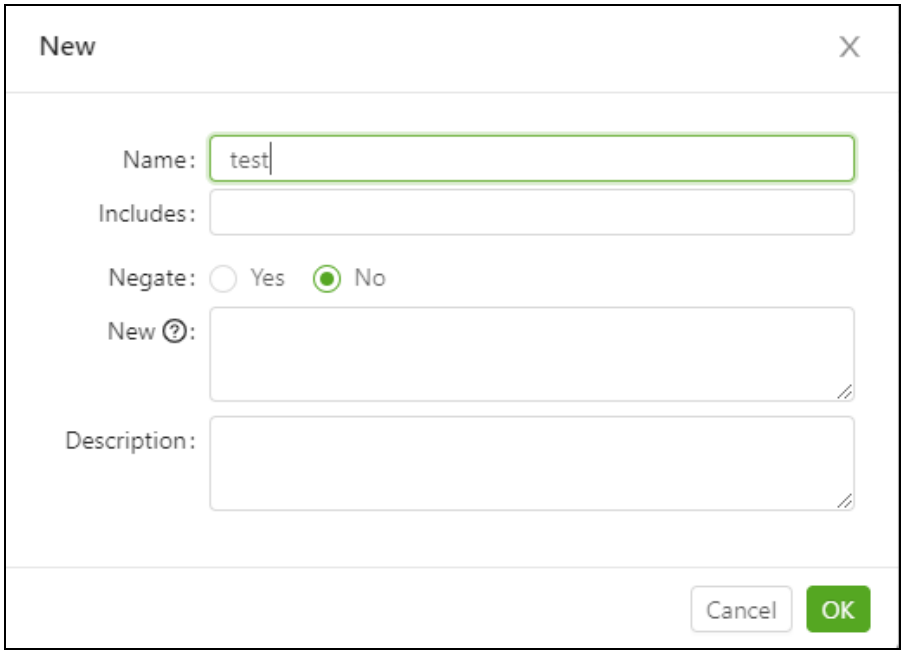
7.4.5 Address Group

An address group here refers to a logical collection of subnets, nodes, MAC addresses, IP pools, and existing groups. To configure such an object, follow these steps:

Step 1 Choose **Objects** > **Addresses** > **Groups**.

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

Figure 7-19 Configuring an address group



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

Table 7-15 Parameters for configuring an address group

Parameter	Description
Name	Name of the address group. The name must be unique and cannot contain the following special characters: % \ ` < > ' & "
Includes	Specifies objects to be contained in this address group.
Negate	Controls whether to reverse the object settings. It has the following values: • **Yes**: indicates that other objects than the specified ones will be taken as the group object. • **No**: indicates that the specified objects will be taken as the group object.
New	Specifies new address-related objects, including subnets, nodes, MAC addresses, and IP pools. Multiple objects are separated by a carriage return, with each in a separate line. New objects are named in the format of "group name_object name".
Description	Brief description of the address group.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.5 Network Intrusion

The Network Intrusion module consists of the following:

- Signature set profiles, including predefined ones and custom ones
- Custom signature
- Signature search
- Exceptions
- Settings

7.5.1 Signature Set Profile

NIPS provides multiple signature set profiles applicable to typical user environments, increasing the ease of use during policy configuration. Such profiles are divided into the following:

- Predefined profiles

  Predefined profiles are subdivided into built-in ones and derived ones. Built-in profiles are pre-configured profiles, which can only be viewed and referenced in policies, but cannot be edited. Derived profiles are created based on built-in profiles, and can be, to some extent, modified as required (for example, you can modify action settings (alert, block, and quarantine), and add or delete signatures).

- Custom profiles

  A custom profile is created by adding or deleting signatures in signature sets or modifying action settings (alert, block, and quarantine) as required.

7.5.1.1 Predefined Profile

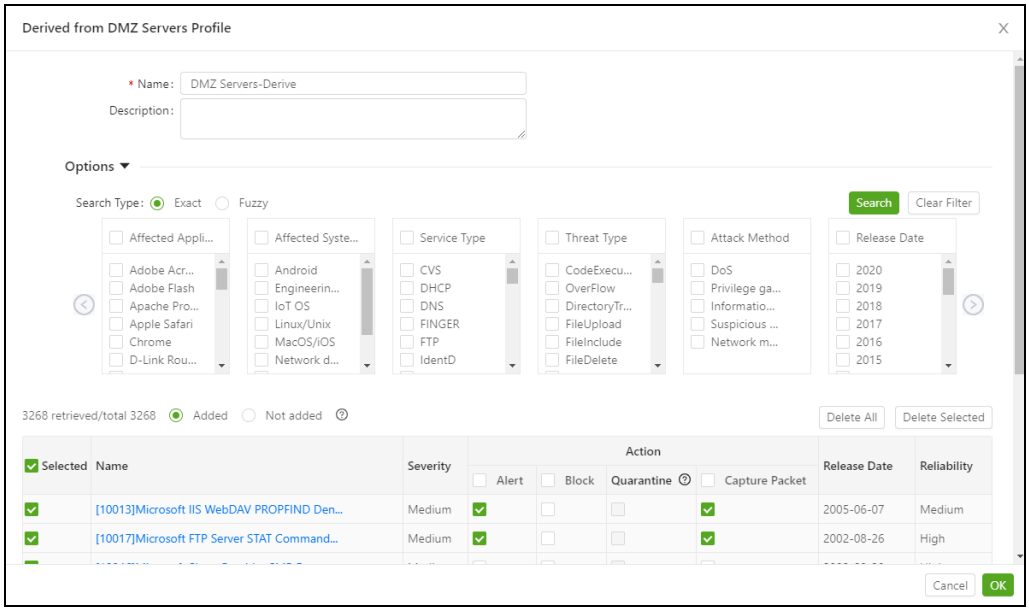
For typical scenarios, the NIPS system combines signatures in the signature database in different ways to form typical built-in profiles. These built-in signature set profiles, which are produced based on NSFOCUS's years of experience in intrusion detection and technical engineers' onsite experience, can fit in with most network deployment environments. Therefore, you are advised to use built-in signature set profiles when configuring intrusion detection policies.

You can create derived profiles based on built-in profiles. The procedure is as follows:

Step 1 Choose **Objects** > **Network Intrusion** > **Signature Set Profiles** > **Predefined Profiles**.

Step 2 Click in the **Operation** column of a built-in profile.

Figure 7-20 Configuring a derived template



Step 3 Configure parameters in the dialog box.

Table 7-16 Parameters for configuring a derived profile

Parameter	Description
Name	Name of the derived profile. By default, the profile name is in the format of "*name of the original template*-Derive".
Description	Brief description of the derived profile.
Event	Specifies intrusion events to be included in the derived profile. You can modify action settings (**Alert**, **Block**, **Quarantine**, and **Capture Packet**) for each event and delete rules. **Note** • When the protection mode is enabled in a policy, selection of **Quarantine** will isolate the IP address that triggers the related rule in the specified time.

Parameter	Description
	• You can download PCAP files on alert or log pages.

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

The newly configured derived template is displayed in the **Derived Profiles** list.

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.5.1.2 Custom Profile

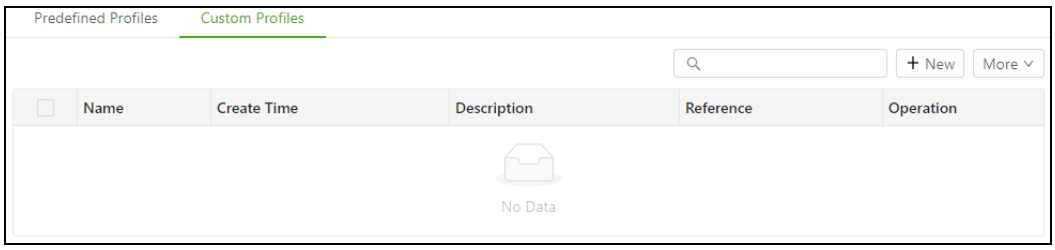
Custom profiles are a supplement to predefined profiles. They are configured by administrators for use in special deployment environments.

Creating a Custom Profile

To configure a custom profile, follow these steps:

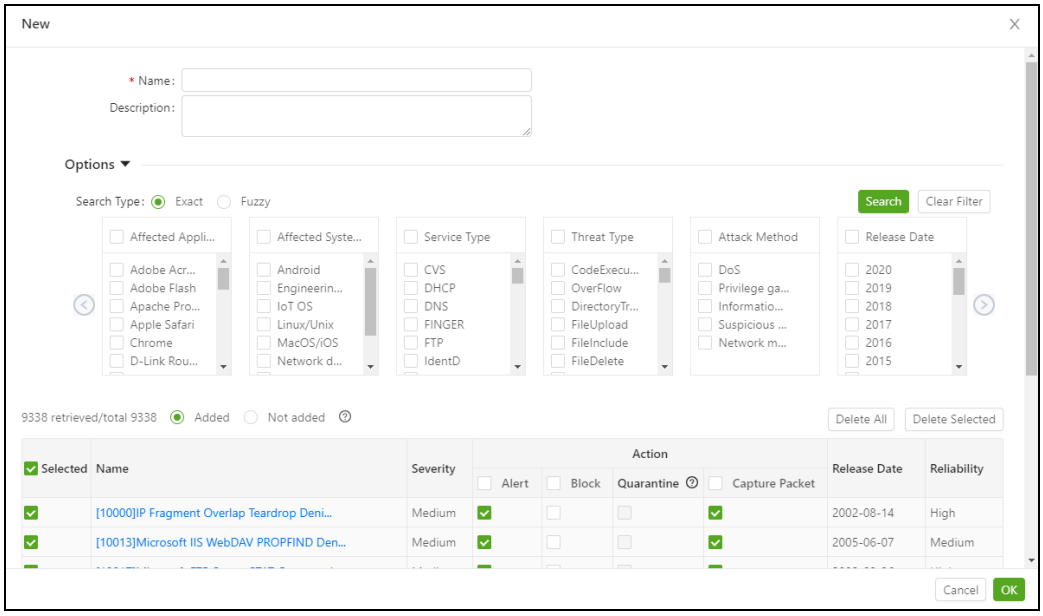
Step 1 Choose **Objects** > **Network Intrusion** > **Signature Set Profiles** > **Custom Profiles**.

Figure 7-21 Custom Profiles page



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

Figure 7-22 Custom Template page



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

Table 7-17 Parameters for configuring a custom rule template

Parameter	Description
Name	Name of the custom profile.
Description	Brief description of the custom profile.
Event	Specifies intrusion events to be included in the custom profile and actions (**Alert**, **Block**, **Quarantine**, and **Capture Packet**) for each intrusion event. **Note** • When the protection mode is enabled in a policy, selection of **Quarantine** will isolate the IP address that triggers the related rule in the specified time. • You can locate an event through the **Rule Query** module. For details, see Signature Search. • You can download PCAP files on alert or log pages.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

Importing or Exporting a Custom Profile

On the **Custom Profiles** page, select the desired custom profiles and click **More** > **Import** or **More** > **Export** to import or export them.

- Parameters including the reference, name, and action, will be imported or exported.
- The password for decompressing the exported file is Yo(+5r74.

7.5.2 Custom Signature

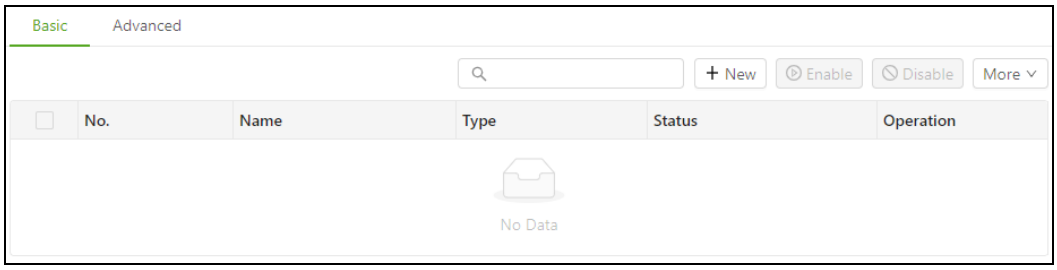
As a supplement to the predefined signature database, custom signatures are configured for various network protocols. The custom signature ID starts from 80001. Signatures with an ID greater than 80000 in the signature database are custom ones. Custom signatures are divided into basic ones and advanced ones. The procedures for configuring these two types of custom signatures are described respectively in the following sections.

7.5.2.1 Basic Signature

Basic signatures are subdivided into three types by network protocol: IP signature, UDP signature, and TCP signature. This section describes how to configure each type of basic signature respectively.

Choose **Objects** > **Network Intrusion** > **Custom Signature** > **Basic**.

Figure 7-23 Basic page

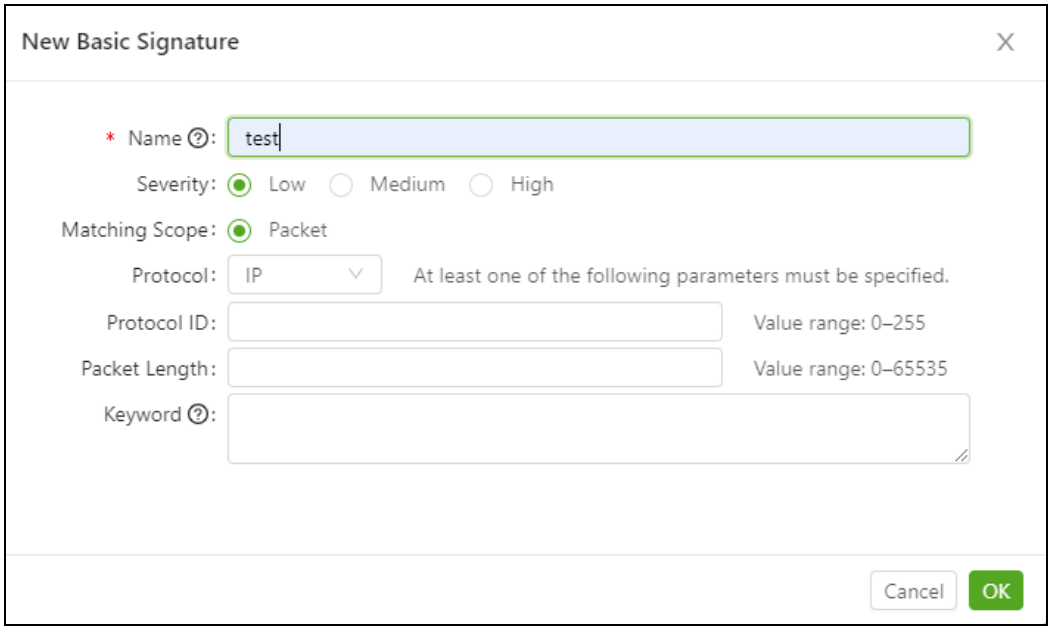


IP Signature

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

The **New Basic Signature** dialog box appears, with **IP** as the default protocol, as shown in Figure 7-24.

Figure 7-24 Configuring a custom IP signature



Step 2 Configure IP signature parameters in the dialog box.

Table 7-18 Parameters for configuring an IP signature

Parameter	Description
Name	Unique name of the IP signature. The name cannot contain the following special characters: \ % ` ^ < > { } ' & " :
Severity	Specifies the risk level of the IP signature, which can be **Low**, **Medium**, or **High**.
Matching Scope	By default, the system supports only packet matching. Packet matching means that NIPS matches individual packets with a rule composed of one or more signatures and determines accordingly whether an attack exists.
Protocol	Protocol type. To create a basic rule for the IP protocol, you must select **IP**, which is the default value.
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. • If **Protocol ID** is set to **6** (TCP), the value of **Packet Length** is 20 plus the payload length of an IP packet. • If **Protocol ID** is set to **17** (UDP), the value of **Packet Length** is 8 plus the length of packet payload.
Keyword	Specifies the keyword to search for in the payload of an IP packet. Note

Parameter	Description
	Keywords can be specified in regular and non-regular 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.

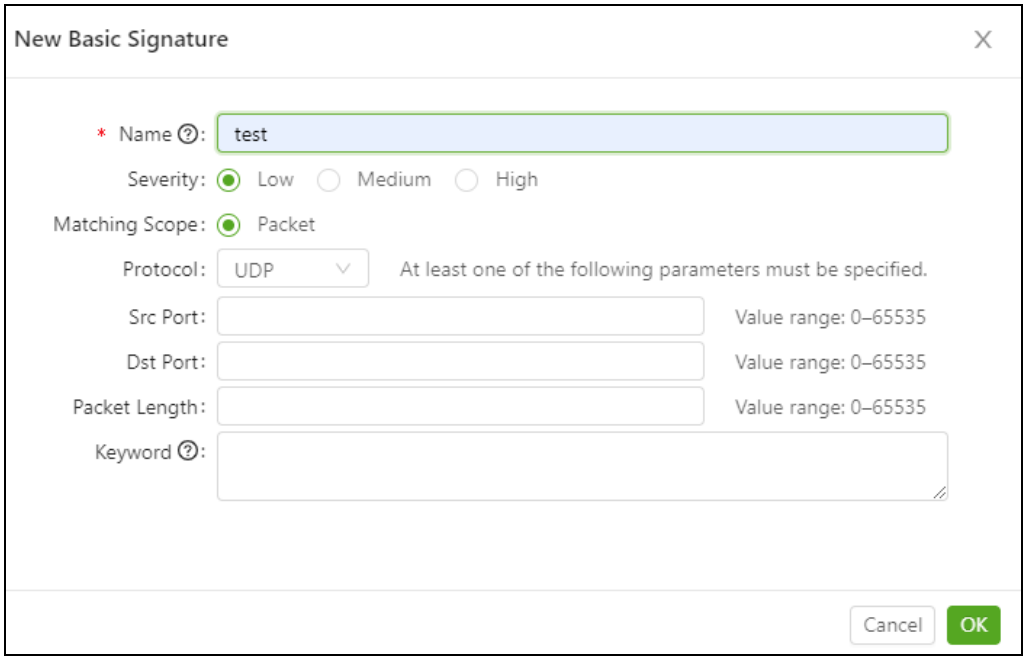
Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

UDP Signature

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

Figure 7-25 Configuring a custom UDP signature



Step 2 In the **New Basic Signature** dialog box, select **UDP** for **Protocol** and configure other parameters.

Table 7-19 Parameters for configuring a UDP signature

Parameter	Description
Name	Unique name of the UDP signature. The name cannot contain the following special characters: % \ ` < > ' & "
Severity	Specifies the risk level of the UDP signature, which can be **Low**, **Medium**, or **High**.

Parameter	Description
Matching Scope	By default, the system supports only packet matching. Packet matching means that NIPS matches individual packets with a rule composed of one or more signatures and determines accordingly whether an attack exists.
Protocol	Specifies the protocol type. Here, this parameter should be set to **UDP**.
Src/Dst 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 3 Click **OK** to save the settings.

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

TCP Signature

The procedure for configuring a TCP signature is similar to that for configuring a UDP signature. For details, see UDP Signature.

7.5.2.2 Advanced Signature

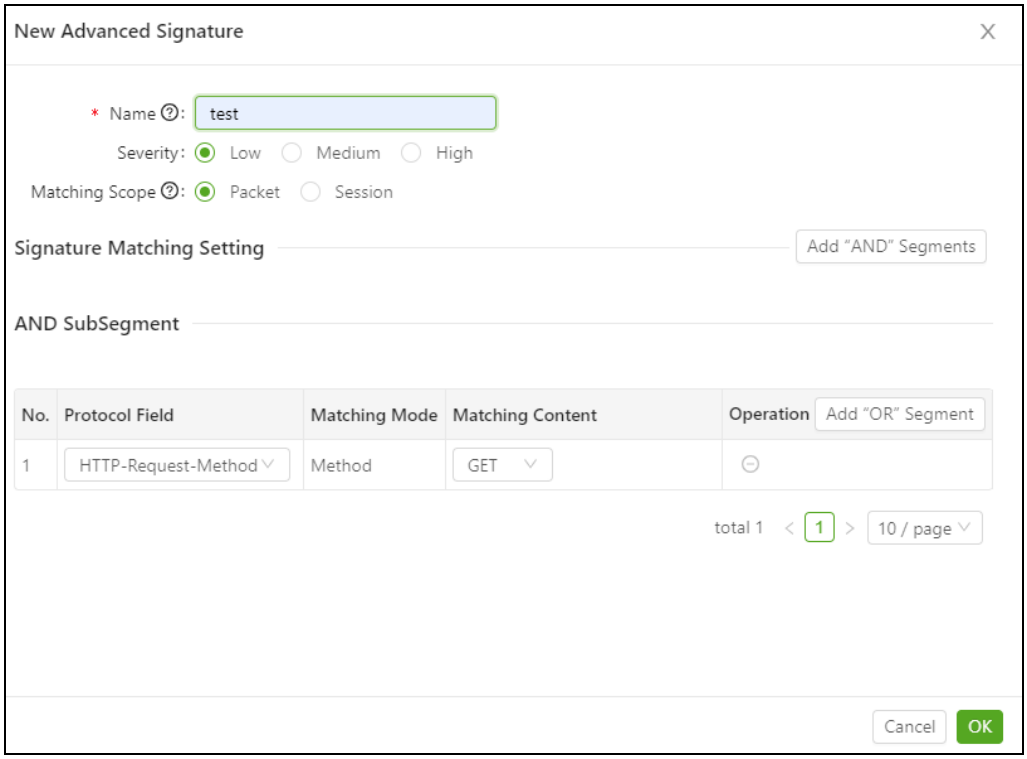
An advanced signature is a combination of fields in such protocols as HTTP, FTP, SMTP, POP3, QQ, and File with the AND or OR relationship. To configure an advanced signature, follow these steps:

Step 1 Choose **Objects** > **Network Intrusion** > **Custom Signature** > **Advanced**.

Figure 7-26 Advanced page

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

Figure 7-27 Configuring an advanced rule



Step 3 Configure basic parameters in the **New Advanced Signature** dialog box.

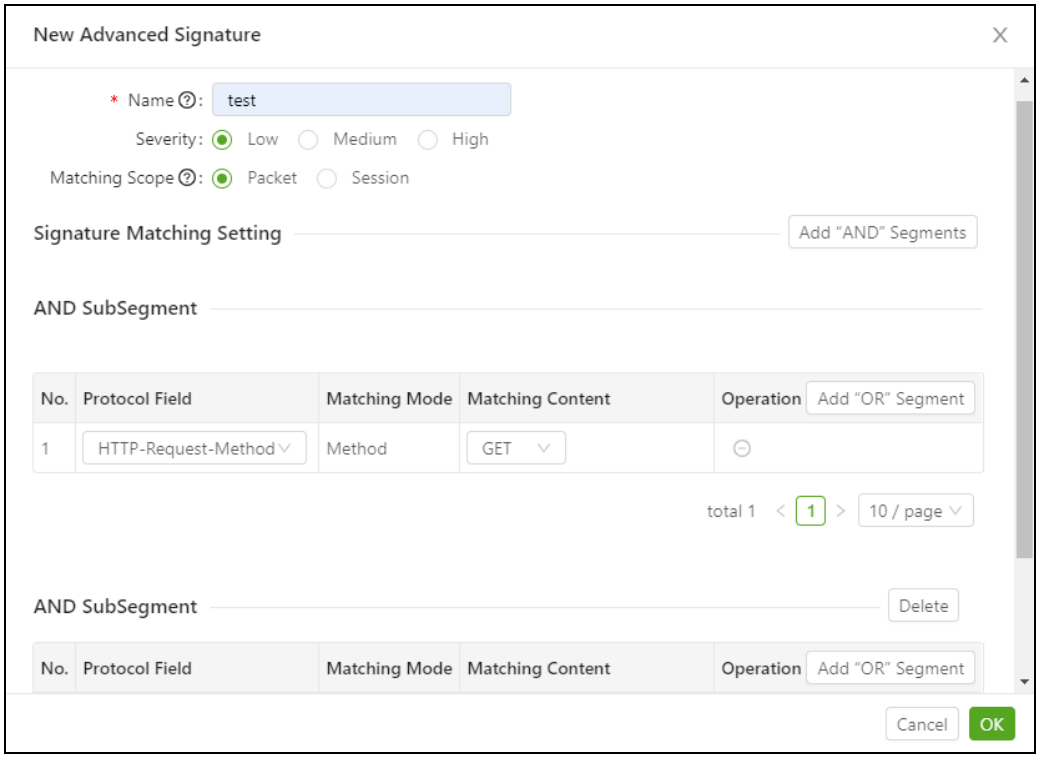
Table 7-20 Parameters for configuring an advanced signature

Parameter	Description
Name	Unique name of the advanced signature. The name cannot contain the following special characters: % \ ` < > ' & "
Severity	Risk level of the advanced signature, which can be **Low**, **Medium**, or **High**.
Matching Scope	Specifies the matching scope, which can be either of the following: • **Packet**: indicates that NIPS matches individual packets 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 packet matching is smaller than that of session matching. • **Session**: indicates that NIPS matches individual sessions 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 a server.

Step 4 Configure AND segments.

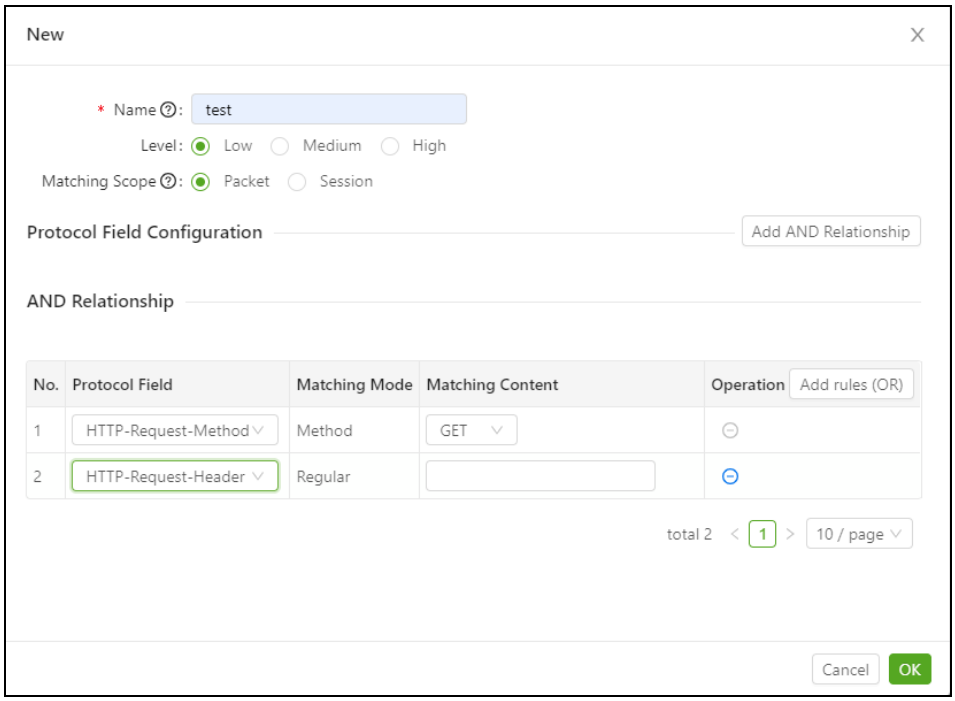
a. Click **Add "AND" Segments**.

Figure 7-28 Adding an AND segment



b. Click **Add "OR" Segment** in the **Operation** column.

Figure 7-29 Adding a protocol field of the OR relationship



c. Configure **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 are explained in Table 7-21.

Table 7-21 Signature matching setting parameters

Matching Mode		Matching Content
Method	HTTP request methods	Specifies the request method of the HTTP protocol. It has the following values: • **GET**: indicates received data. • **POST**: indicates transmitted data.
	FTP/POP3 request methods	Specifies the request method of the FTP or POP3 protocol, which can be **USER**, **PASS**, or **LIST**.
	SMTP request methods	Specifies the request method of the SMTP protocol, which can be **MAIL**, **DATA**, or **RCPT**.
Regular		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.

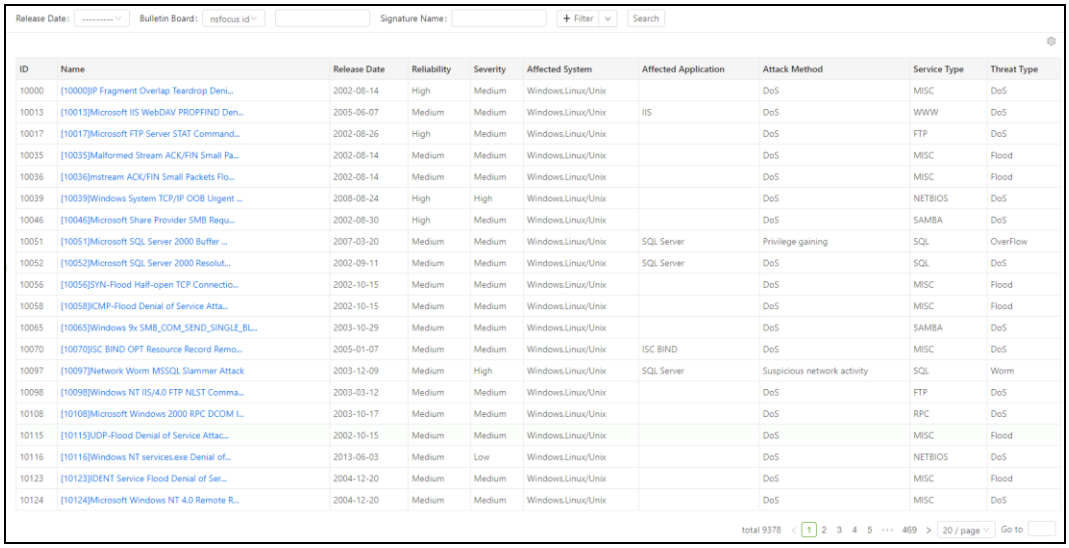
Step 6 Restart the engine to make the settings take effect.

----End

7.5.3 Signature Search

Choose **Objects** > **Network Intrusion** > **Signature Search**. The **Signature Search** page displays details of signatures in the signature database, as shown in Figure 7-30.

Figure 7-30 Signature Search page



You can query signatures by release date, bulletin type, bulletin ID, and signature name.

In addition, you can narrow down the search scope to get more accurate results by configuring advanced options.

Clicking **Filter** shows advanced options, as shown in Figure 7-31.

Figure 7-31 Advanced options

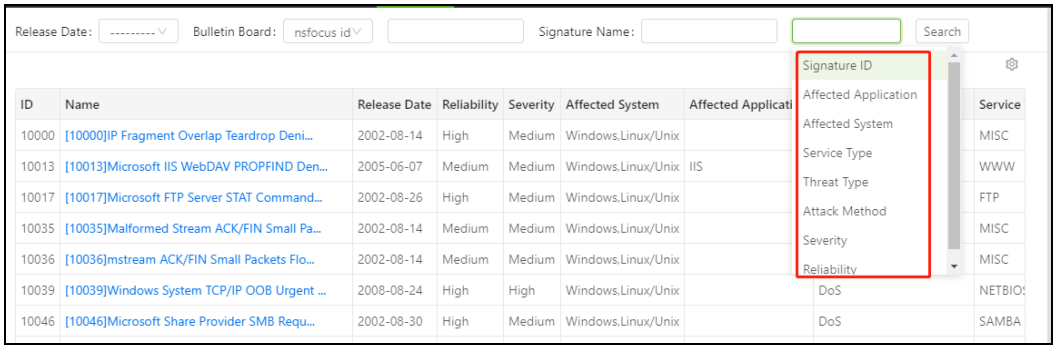


Table 7-22 describes these advanced options and basic query parameters.

Table 7-22 Advanced options

Parameter	Description
Signature ID	Specifies a signature ID to query related signatures.
Affected Application	Specifies applications affected by intrusion events to query related signatures.
Affected System	Specifies operating systems affected by intrusion events to query related signatures.
Service Type	Specifies service types affected by intrusion events to query related signatures.

Parameter	Description
Threat Type	Specifies threat types of intrusion events to query related signatures.
Attack Method	Specifies attack methods of intrusion events to query related signatures.
Severity	Specifies risk levels of intrusion events to query related signatures.
Reliability	Specifies reliability levels of intrusion events to query related signatures.
Signature Name	Specifies a signature name to query related signatures.
Bulletin Board	Specifies a bulletin type: • **nsfocus id**: retrieves signatures in NSFOCUS's IPS signature database. • **cve id**: retrieves vulnerabilities in the Common Vulnerabilities and Exposures (CVE) database. • **cnnvd id**: retrieves vulnerabilities in the China National Vulnerability Database (CNNVD). • **bugtraq id**: retrieves vulnerabilities disclosed in the BUGTRAQ mailing list.

7.5.4 Exception

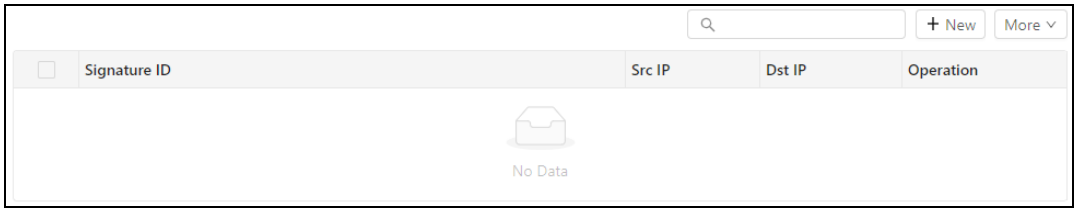
If you know that an intrusion event triggers an intrusion prevention alert and are sure that this event does not threaten or have a severe impact on the current network environment, you can add this intrusion event to the exception list. When creating such an exception, you can set the coverage by specifying the source and destination IP addresses.

After an intrusion event is added to the exception list, NIPS will not generate any alert for or block it. For how to create an exception, see Adding an Exception. The procedures for viewing and deleting an exception are described respectively in the following sections.

Viewing an Exception

Step 1 Choose **Objects** > **Network Intrusion** > **Exceptions**.

Figure 7-32 Exceptions page



Step 2 Click the ID of a signature to view its details.

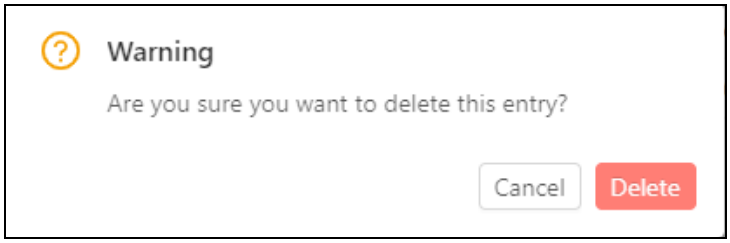
----End

Deleting an Exception

Step 1 Click in the **Operation** column of an exception.

A confirmation dialog box appears, as shown in Figure 7-33.

Figure 7-33 Confirmation dialog box



Step 2 Click **Delete** to delete the exception.

Step 3 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.5.5 Other Settings

For intrusion prevention, you can configure the following:

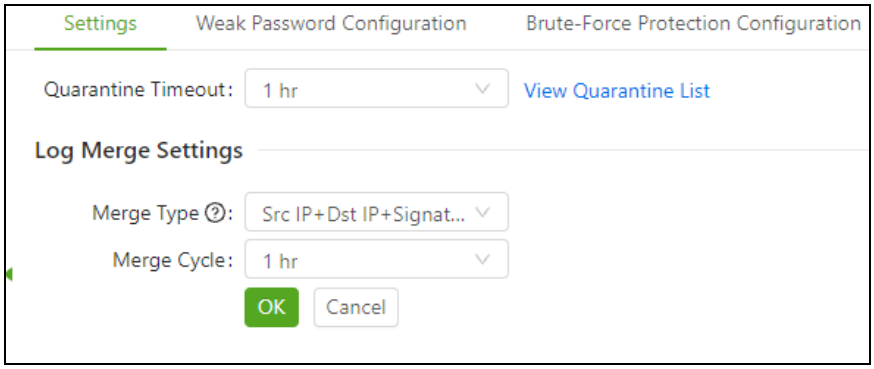
- Common parameters
- Weak password detection parameters
- Brute-force protection parameters

7.5.5.1 Common Parameters

On the **Settings** tab page, you can configure the quarantine timeout and log merge parameters. The procedure is as follows:

Step 1 Choose **Objects** > **Network Intrusion** > **Settings** > **Settings**.

Figure 7-34 Settings tab page



Step 2 Configure parameters.

Table 7-23 Common parameters

Parameter	Description
Quarantine Timeout	Specifies how long traffic between the source and destination IP addresses of an intrusion event will be blocked. You can click **View Quarantine List** to view the quarantined IP addresses under **Monitor** > **Network Intrusion** > **Quarantine**

Parameter	Description
	List.
Merge Type	Controls whether to enable log merge. If it is enabled, multiple logs conforming to a specified condition will be merged as one log in the log merge cycle. It has the following values: **Disable**: does not merge logs. **Src IP+Signature ID**: merges logs of events involving the same source IP address and the same signature as one. **Dst IP+Signature ID**: merges logs of events involving the same destination IP address and the same signature as one. **Src IP+Dst IP+Signature ID**: merges logs of events involving the same source and destination IP addresses and the same signature as one.
Merge Cycle	Specifies the interval at which logs are merged. This can be set when log merge is enabled.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

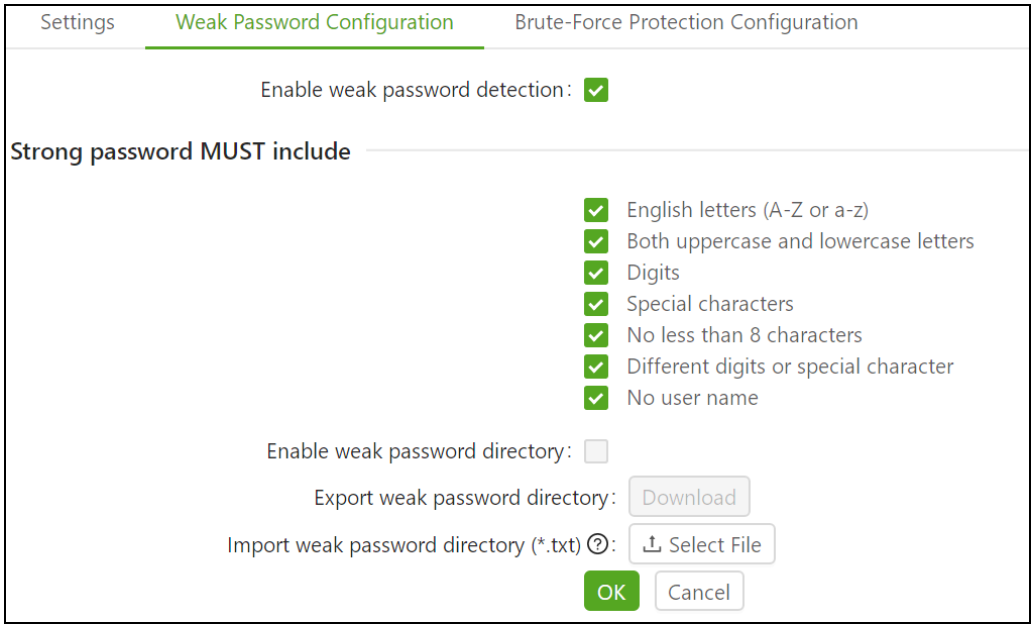
----End

7.5.5.2 Weak Password Configuration

On the **Weak Password Configuration** page, you can enable or disable weak password detection. After this function is enabled, NIPS will detect weak passwords based on the built-in weak password check rule. If the custom weak password dictionary is enabled, NIPS allows users to detect weak passwords based on their custom weak password dictionaries created as required.

Step 1 Choose **Objects** > **Network Intrusion** > **Settings** > **Weak Password Configuration**.

Figure 7-35 Weak Password Configuration tab page



Step 2 Configure parameters.

Table 7-24 Weak password detection parameters

Parameter	Description
Enable weak password detection	Controls whether to enable the weak password detection function.
Strong password MUST include	Specifies conditions that a password must meet to avoid being detected as a weak one.
Enable weak password dictionary	Controls whether to enable custom weak password dictionaries. After enabling this, you can click **Select File** and import a custom weak password dictionary. You can also click **Download** to export the custom weak password dictionary from NIPS to a local disk drive for backup.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

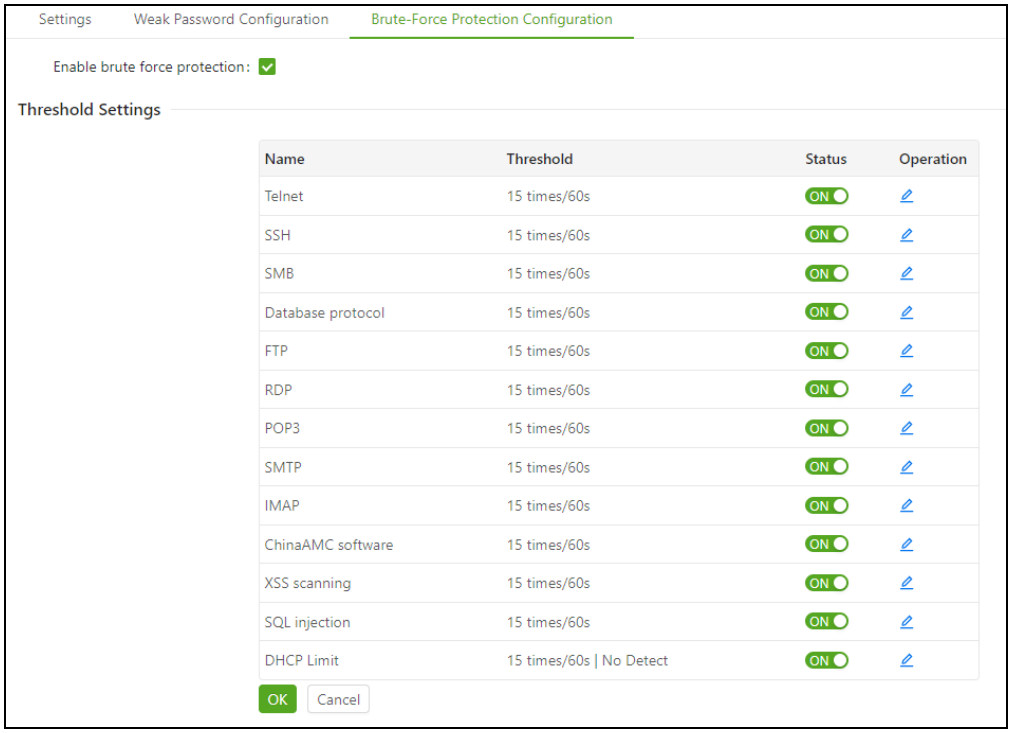
----End

7.5.5.3 Brute-Force Protection Configuration

You can choose to enable brute-force protection configuration. After that, you can configure a threshold for triggering this type of detection.

Step 1 Choose **Objects** > **Network Intrusion** > **Settings** > **Brute-Force Protection Configuration**.

Figure 7-36 Brute-Force Protection Configuration tab page



Step 2 Configure parameters.

Table 7-25 Brute-force protection configuration parameters

Parameter	Description
Enable brute force protection	Controls whether to enable brute force protection. It is enabled by default. You can disable it by clearing the check box.
Threshold Settings	Specifies the maximum number of consecutive failed login attempts via various protocols during the statistical period. For the **DHCP Limit**, the detection level and detection block will also be considered. When the actual number of failed login attempts reaches this threshold, NIPS deems it a brute force event.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.6 Malware

The Malware module consists of the following:

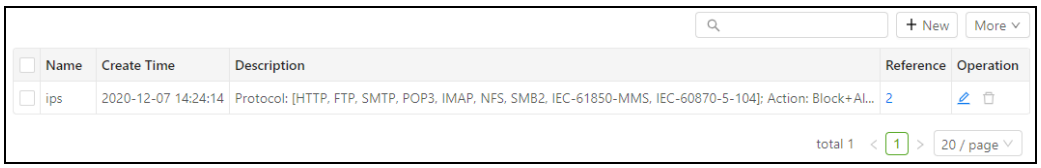
- Profile
- Blacklist
- Whitelist

- Other settings

7.6.1 Profile

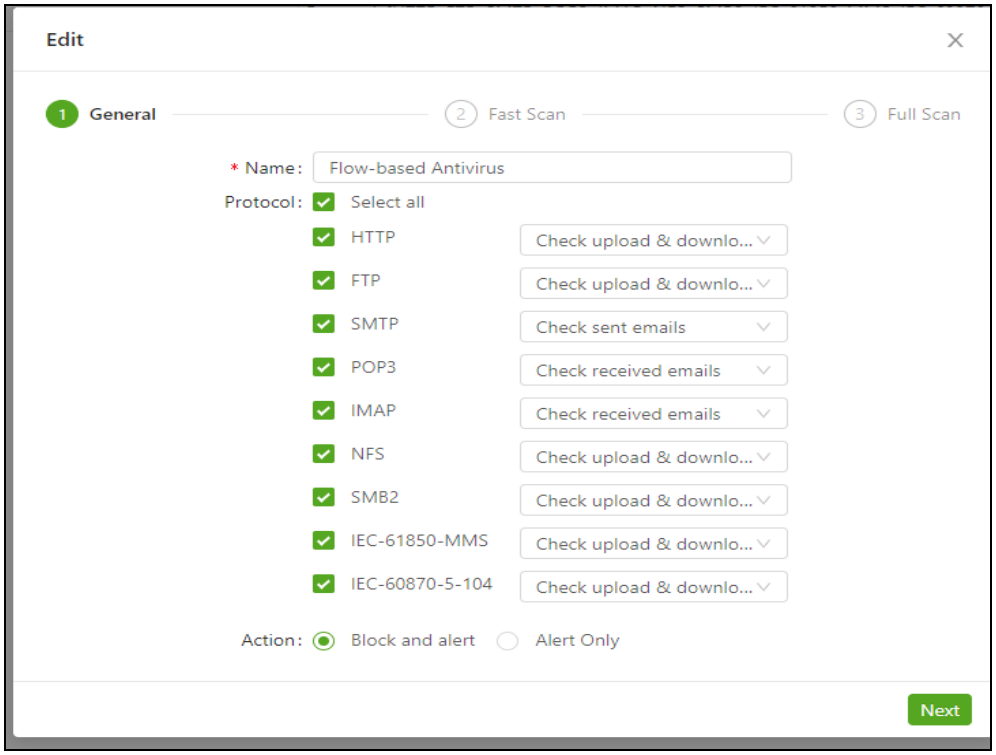
Step 1 Choose **Objects** > **Malware** > **Profile**.

Figure 7-37 Malware profiles



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

Figure 7-38 Configuring a malware detection profile



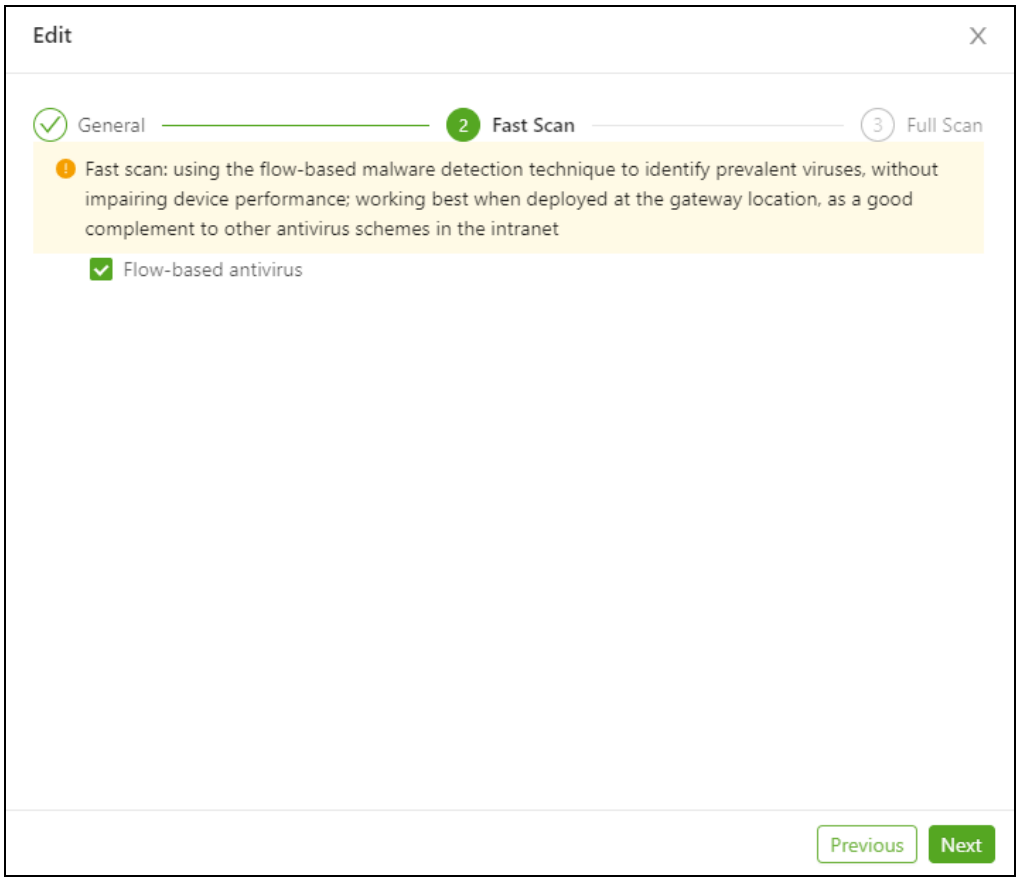
Step 3 Configure basic information in the **New malware profile** dialog box.

Table 7-26 Basic parameters of the malware detection profile

Parameter	Description
Name	Name of the profile.
Protocol	Specifies the protocol to be scanned and the related detection mode.
Action	Specifies an action to be taken upon detection of matching malware.

Step 4 Click **Next** to open the **Fast Scan** page.

Figure 7-39 Fast scan parameters

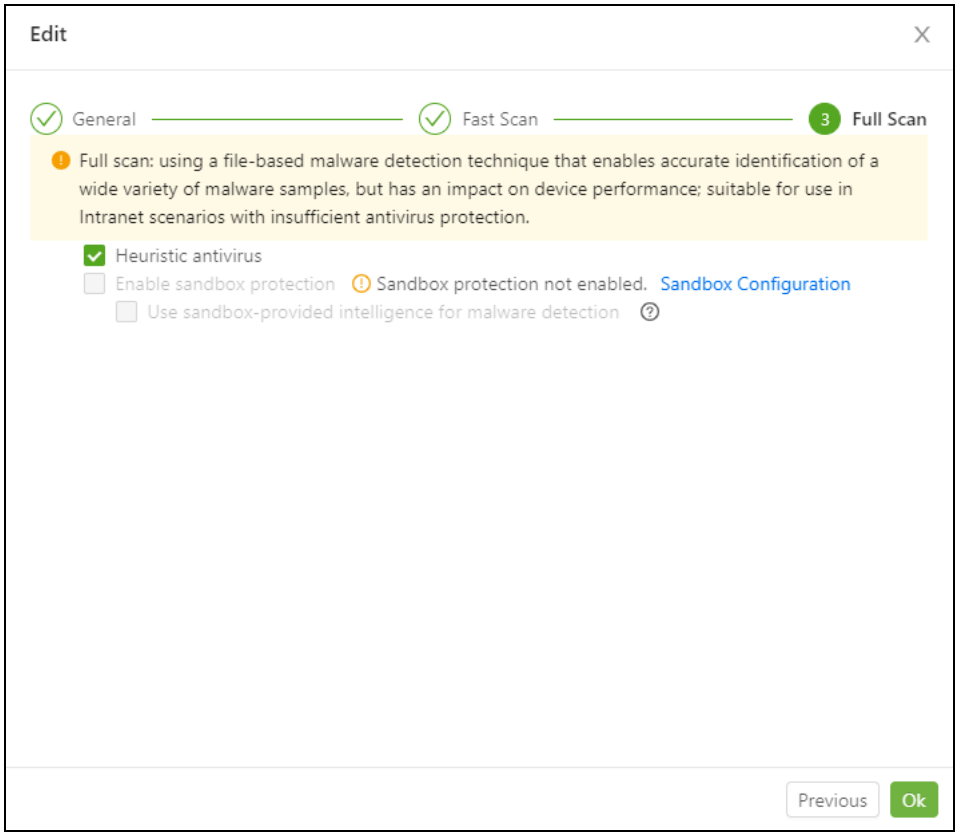


Step 5 Choose whether to enable flow-based antivirus.

After this is enabled, NIPS will check packets for viruses without reassembling packets into files.

Step 6 Click **Next** to open the **Full Scan** page.

Figure 7-40 Full scan parameters



Step 7 Configure the following full scan parameters:

- **Heuristic antivirus**: After this is enabled, NIPS will reassemble files before checking whether they are malicious.

Note	This function can work only after the heuristic virus signature database has been imported. For details, see Manual Import.

- **Enable sandbox protection**: This is disabled by default. If you enable it and select the check box of **Use sandbox-provided intelligence for malware detection**, NIPS will generate an alert when detecting a malware sample that matches a rule configured on NSFOCUS Threat Analysis Center (TAC).

Step 8 Click **OK** to save the settings.

Step 9 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.6.2 File Blacklist

Files on the blacklist are directly blocked, without being subject to further malicious file detection.

To add a file to the blacklist, follow these steps:

Step 1 Choose **Objects** > **Malware** > **Blacklist**.

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

Figure 7-41 Adding a file to the blacklist

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

Table 7-27 File blacklist parameters

Parameter	Description
File MD5	Specifies the MD5 value of a file that you want to add to the blacklist.
File Name	Specifies the name of a file that you want to add to the blacklist.
Description	Brief description of the file.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.6.3 File Whitelist

Files on the whitelist are not subject to malicious file detection, but are still submitted to other modules for further security checks.

To add a file to the whitelist, follow these steps:

Step 1 Choose **Objects** > **Malware** > **Whitelist**.

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

Figure 7-42 Adding a file to the whitelist

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

Table 7-28 File whitelist parameters

Parameter	Description
File MD5	Specifies the MD5 value of a file that you want to add to the whitelist.
File Name	Specifies the name of a file that you want to add to the whitelist.
Description	Brief description of the file.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

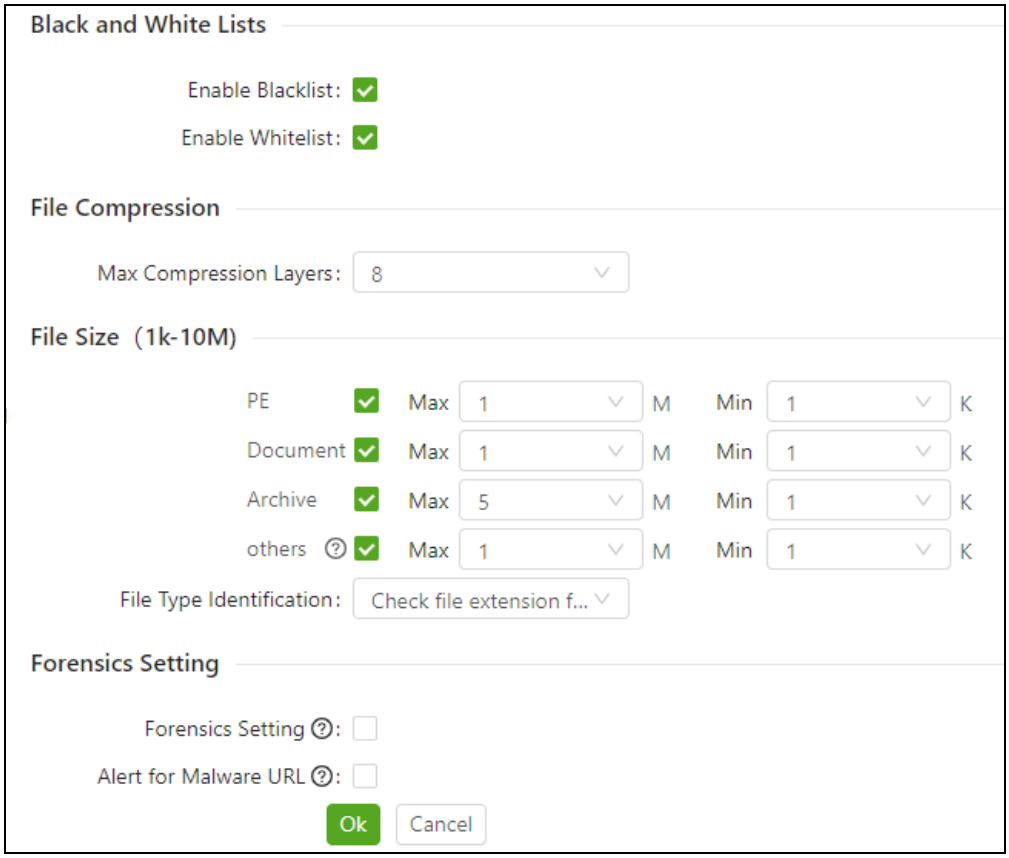
----End

7.6.4 Other Settings

To configure other parameters, follow these steps:

Step 1 Choose **Objects** > **Malware** > **Settings**.

Figure 7-43 Other settings regarding malware



Step 2 Configure parameters.

Table 7-29 Other parameters regarding malware detection

Parameter		Description
Black and White Lists		Controls whether to enable blacklist- and whitelist-based malware detection.
Max Compression Layers		Specifies the maximum number of layers to be decompressed for security checks.
File Size	PE/Document/Archive/others	Specifies the maximum and minimum sizes of various files.
	File Type Identification	Specifies the file check priority, which can be any of the following: • Check file header first • Check file extension first • Check file header & file extension
Forensics Setting	Forensics Setting	Specifies whether to store malware samples locally. This parameter is available only when NIPS comes with a hard drive.
	Alert for Malicious File URL	Specifies whether to record the URL from which a malware sample is transmitted and display this URL under **Monitor** > **Web Security** > **Malicious URL**.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.7 Web Security

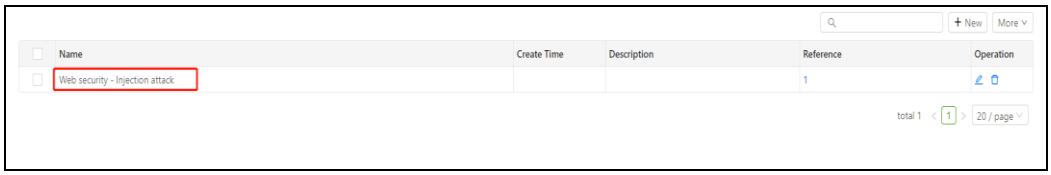
The Web Security module consists of the following:

- Profile
- URL blacklist
- URL whitelist
- SQL injection whitelist
- Other settings

7.7.1 Profile

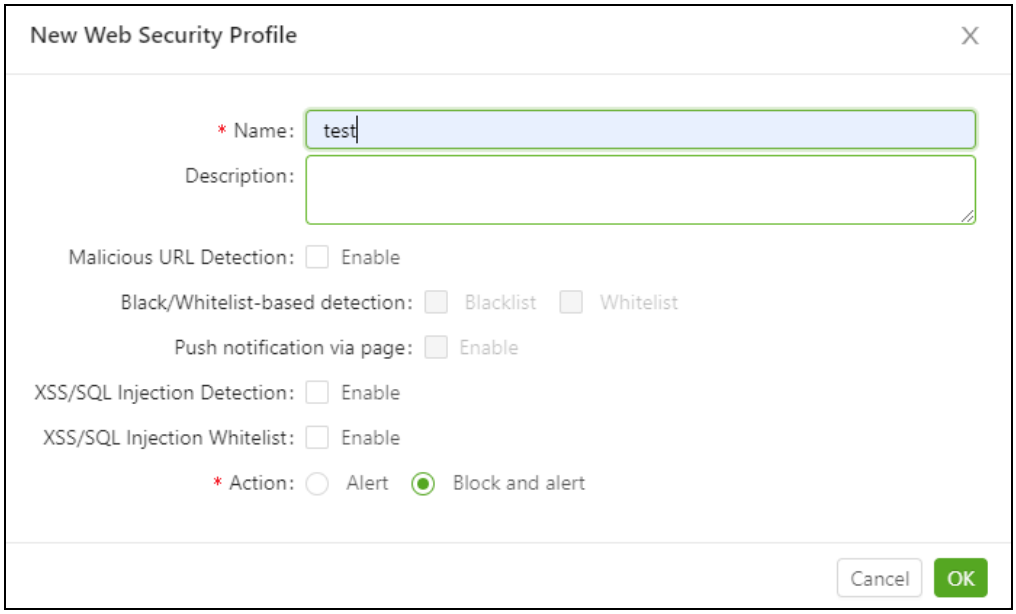
Step 1 Choose **Objects** > **Web Security** > **Profile**.

Figure 7-44 Web security profiles



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

Figure 7-45 Creating a web security profile



Step 3 Configure parameters in the **New Web Security Profile** dialog box.

Table 7-30 Web security profile parameters

Parameter	Description
Name	Name of the profile.
Description	Brief description of the profile.
Malicious URL Detection	Controls whether to enable malicious URL detection.
Black/Whitelist-based detection	Controls whether to enable blacklist-/whitelist-based detection. This is available when you enable malicious URL detection.
Push notification via page	Controls whether to push notifications via a page. This is available when you enable malicious URL detection.
XSS/SQL Injection Detection	Controls whether to enable detection of cross-site scripting (XSS) and SQL injection.
XSS/SQL Injection Whitelist	Controls whether to enable the XSS and SQL injection whitelist.
Action	Specifies an action to be taken upon detection of a web threat.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

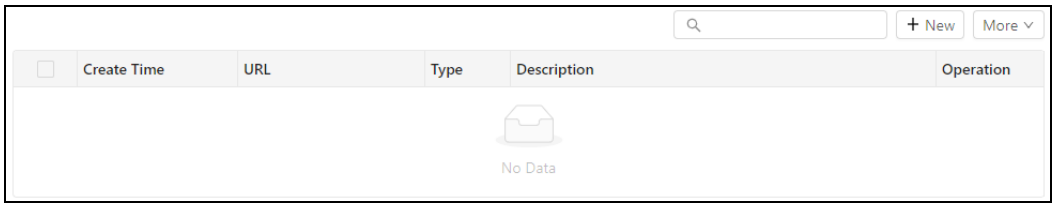
----End

7.7.2 URL Blacklist

Requests for access to a URL on the blacklist are directly blocked, without being subject to any further web security checks.

Step 1 Choose **Objects** > **Web Security** > **URL Blacklist**.

Figure 7-46 URL Blacklist page



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

Figure 7-47 Adding a URL to the blacklist

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

Table 7-31 URL blacklist parameters

Parameter	Description
URL	Specifies a URL that you want to add to the blacklist. The URL should start with a protocol like **http**, **https**, or **ftp**.
Description	Brief description of the URL.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

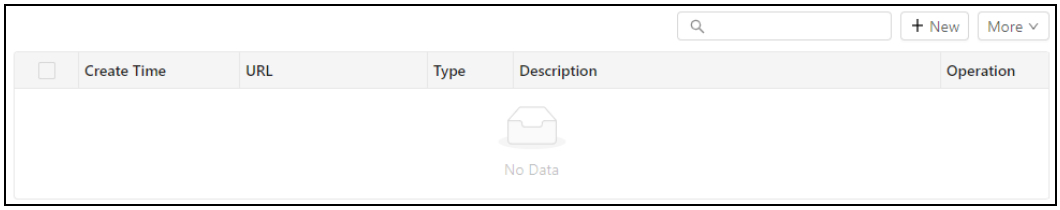
----End

7.7.3 URL Whitelist

Requests for access to a URL on the whitelist are allowed to pass, but are still submitted to other modules for further security checks.

Step 1 Choose **Objects** > **Web Security** > **URL Whitelist**.

Figure 7-48 URL Whitelist page



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

Figure 7-49 Adding a URL to the whitelist

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

Table 7-32 URL whitelist parameters

Parameter	Description
URL	Specifies a URL that you want to add to the whitelist. The URL should start with a protocol like **http**, **https**, or **ftp**.
Description	Brief description of the URL.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.7.4 SQL Injection Whitelist

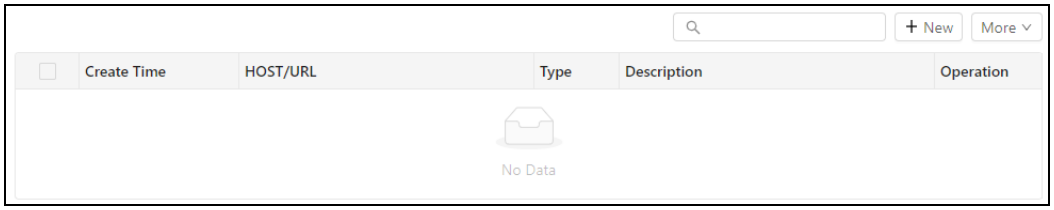
The SQL injection whitelist is a part of NIPS's core function of network intrusion. This section describes how to add a host name or URL to the SQL injection whitelist.

If a network intrusion policy references the "[29001]WEB Service Remote SQL Injection Suspicious Behavior" rule, which is expected not to work for certain servers, you can add the URLs of these servers to the SQL injection whitelist.

To add a host name or URL to the SQL injection whitelist, follow these steps:

Step 1 Choose **Objects** > **Web Security** > **SQL Injection Whitelist**.

Figure 7-50 SQL Injection Whitelist page



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

Figure 7-51 Adding a URL to the SQL injection whitelist

Step 3 Type the host name or URL of the server that you want to exclude from SQL injection protection.

Note	The host name and domain name of a URL should be separated by a slash (/), for example, www.google.cn/zh-CN.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

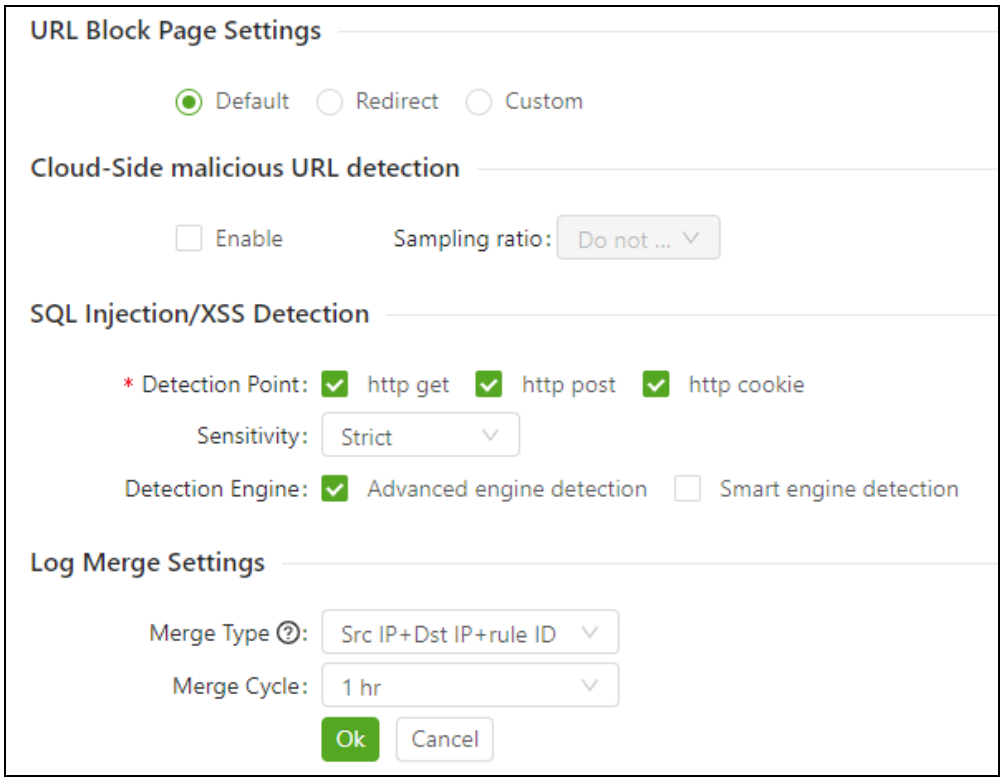
----End

7.7.5 Other Settings

To configure other parameters, follow these steps:

Step 1 Choose **Objects** > **Web Security** > **Settings**.

Figure 7-52 Other settings regarding web security



Step 2 Configure parameters.

Table 7-33 Web security configuration parameters

Parameter		Description
URL Block Page Settings		• **Default**: uses the default notification push page. • **Redirect**: redirects users to a new address. In this case, you should set the redirect address. Only domain names in a format like www.nsfocus.com are supported. • **Custom**: allows you to set the title, content, and copyright statement for a custom notification page.
Cloud-side malicious URL detection		Controls whether to enable cloud-side detection of malicious URLs. If this is enabled, you need to further set whether to enable sampling and, if yes, the sampling ratio.
SQL Injection/XSS	Detection Point	Specifies objects to check for SQL injection and XSS, including HTTP GET, HTTP POST, and HTTP cookies. You can select multiple options. In this case, when any one of them has a match, the

Parameter		Description
Detection		detection engine generates an alert.
	Sensitivity	Specifies how sensible the detection engine is to detect SQL injection or XSS. It has the following values: • Strict • Normal
	Detection Engine	Specifies detection modes, which include: • Advanced engine detection • Smart engine detection
Log Merge Settings	Merge Type	Specifies whether to enable log merge and, if yes, the merge type. Options include the following: • **Disable**: does not merge web security logs. In this case, multiple alerts may be generated throughout an attack. • **Src IP+rule ID**: merges logs of events involving the same source IP address and the same signature as one. • **Dst IP+rule ID**: merges logs of events involving the same destination IP address and the same signature as one. • **Src IP+Dst IP+rule ID**: merges logs of events involving the same source and destination IP addresses and the same signature as one.
	Merge Cycle	Specifies the interval at which logs are merged.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.8 C&C Communication

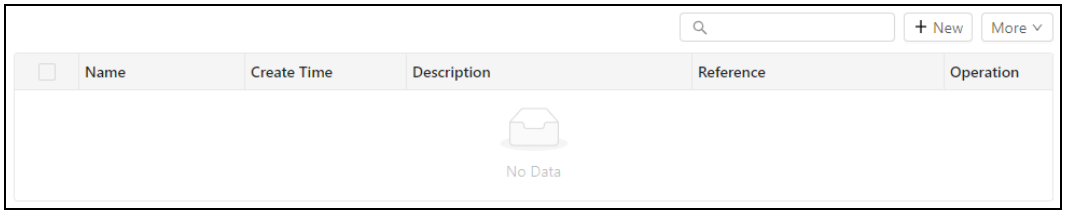
The C&C Communication module consists of the following:

- Profiles
- C&C blacklist
- C&C whitelist
- Other settings

7.8.1 Profile

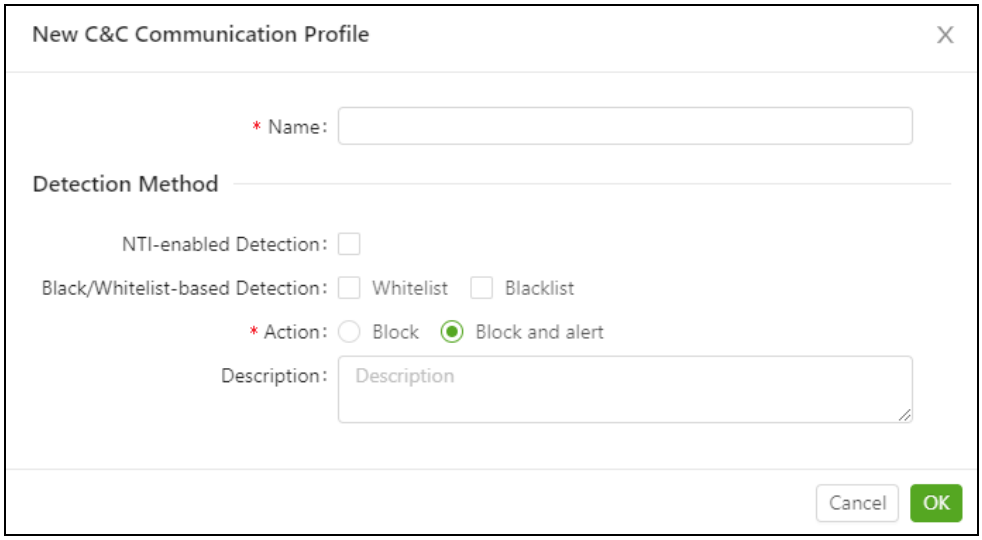
Step 1 Choose **Objects** > **C&C Communication** > **Profile**.

Figure 7-53 C&C communication profile page



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

Figure 7-54 Creating a C&C communication profile



Step 3 Configure parameters in the **New C&C Communication Profile** dialog box.

Table 7-34 Parameters for configuring a C&C communication profile

Parameter	Description
Name	Name of the profile.
NTI-enabled Detection	Controls whether to enable NTI-driven detection.
Black/Whitelist-based Detection	Controls whether to enable blacklist- and/or whitelist-based detection.
Action	Specifies an action to be taken for matching packets, which can be either of the following: • **Block**: After a detection mechanism is enabled, if C&C communication is detected, the system will block subsequent traffic, without generating any alerts. • **Block and alert**: After a detection mechanism is enabled, if C&C communication is detected, the system will generate alerts and block subsequent traffic.

Parameter	Description
Description	Brief description of the profile.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

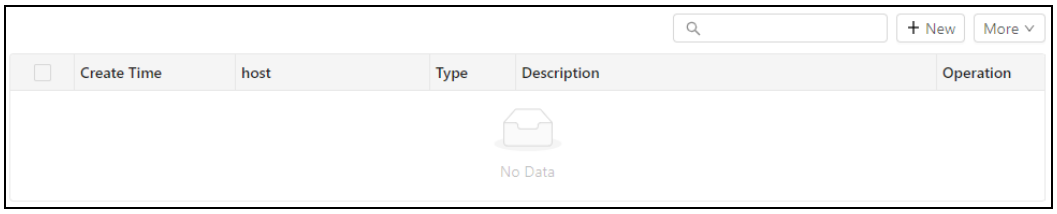
7.8.2 C&C Blacklist

Requests for access to an address on the C&C blacklist are directly blocked, without being subject to any further C&C attack checks.

To add a C&C address to the blacklist, follow these steps:

Step 1 Choose **Objects** > **C&C Communication** > **C&C Blacklist**.

Figure 7-55 C&C blacklist page



For a manually added C&C address, **Manual addition** is displayed in the **Type** column.

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

Figure 7-56 Adding a C&C address to the blacklist

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

Table 7-35 C&C blacklist parameters

Parameter	Description
Host	Specifies a host that you want to add to the C&C blacklist. You can type an IPv4/IPv6 address or a domain name.
Description	Brief description of the C&C address.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

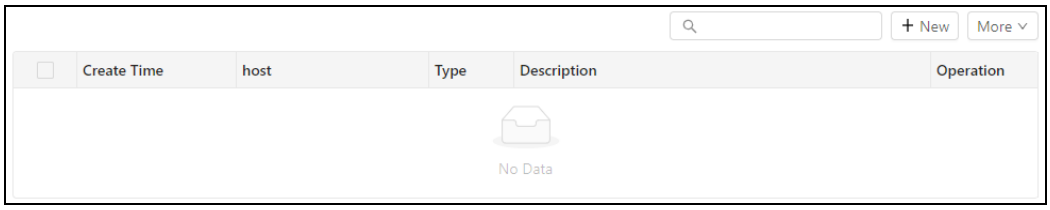
7.8.3 C&C Whitelist

Requests for access to an address on the C&C whitelist are allowed to pass, but are still submitted to other modules for further security checks.

To add an address to the C&C whitelist, follow these steps:

Step 1 Choose **Objects** > **C&C Communication** > **C&C Whitelist**.

Figure 7-57 C&C whitelist page



For a C&C address added from a log or alert message, **One-click addition** is displayed in the **Type** column. If it is manually added here, **Manual addition** is displayed in the **Type** column.

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

Figure 7-58 Adding a C&C address to the whitelist

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

Table 7-36 C&C whitelist parameters

Parameter	Description
Host	Specifies a host that you want to add to the C&C whitelist. You can type an IPv4/IPv6 address or a domain name.
Description	Brief description of the C&C address.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

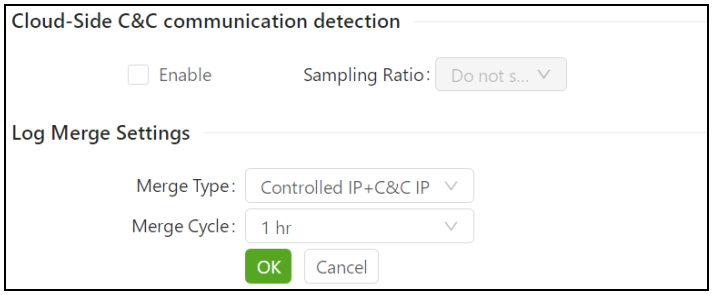
----End

7.8.4 Other Settings

You can enable cloud-side detection of C&C communication and configure log merge settings. The procedure is as follows:

Step 1 Choose **Objects** > **C&C Communication** > **Settings**.

Figure 7-59 Other settings regarding C&C communication



Step 2 Configure parameters.

Table 7-37 C&C communication detection and logging parameters

Parameter	Description
Enable	Controls whether to enable cloud-side detection. If you select the **Enable** check box, traffic will be sent to the cloud for detection of C&C communication against policies that reference a C&C communication profile. When detecting an address matching the cloud-side C&C address list, the system generates an alert. After enabling this function, you need to further specify whether to enable sampling and, if yes, set the sampling ratio. If you do not select the **Enable** check box, traffic will not be sent to the cloud for detection of C&C communication.
Merge Type	Specifies whether to enable log merge and, if yes, the merge type. Options include the following: • **Disable**: does not merge logs. In this case, multiple alerts may be generated throughout an attack. • **Controlled IP**: merges logs of events involving the same controlled IP address as one. • **Controlled IP**: merges logs of events involving the same C&C IP address as one. • **Controlled IP+C&C IP**: merges logs of events involving the same controlled IP address and C&C IP address as one.
Merge Cycle	Specifies the interval at which logs are merged.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.9 Callback Monitoring

NIPS supports the malicious software callback monitoring function. If a sandbox, through analysis, finds that an advanced malicious sample engages in network callback, the system records the callback IP address or domain name to the callback monitoring list (**Monitor > Advanced Threat > Callback Monitoring**). The user can then add this IP address or domain name to the blacklist or whitelist. In the former case, when detecting the IP address or domain name again in subsequent traffic monitoring, the system logs a callback event. In the latter case, the system will no longer monitor the IP address or domain name for callback events.

The Callback Monitoring module consists of the following:

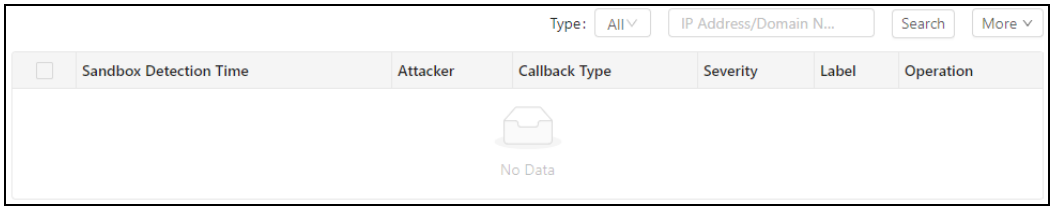
- Blacklist
- Whitelist

Note	Callback monitoring information returned by the sandbox is saved on NIPS, which monitors and alerts callbacks accordingly. Even if NIPS is disconnected from the sandbox, the saved callback monitoring list remains unchanged.

7.9.1 Blacklist

Choose **Objects** > **Callback Monitoring** > **Blacklist**.

Figure 7-60 Callback monitoring blacklist page



By default, all entries are listed. You can select **IP** or **Domain Name** from the **Type** drop-down list to display only entries of the specified type.

Type an IP address or domain name and click **Search** to check whether it has been added to the blacklist.

Adding an Entry to the Whitelist

You can move blacklist entries to the whitelist in one of the following ways:

- Move one by one: Point to in the **Operation** column of an entry and click **Add to whitelist** to move this entry to the callback monitoring whitelist.
- Move all: Point to **More** and click **Whitelist all** to move all entries in the blacklist to the whitelist.
- Move multiple: Select one or more entries, point to **More**, and click **Whitelist selected** to move the selected entries to the whitelist.

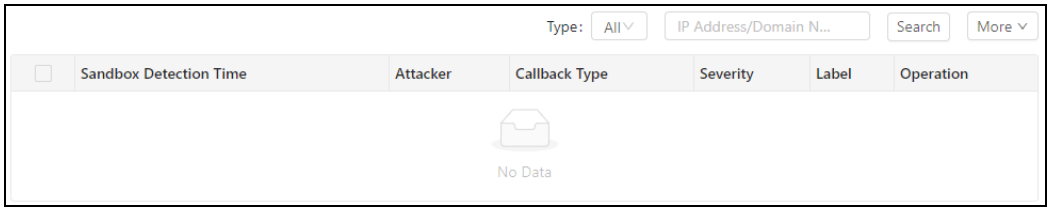
NTI-based Traceback

For a blacklist entry, point to in the **Operation** column of an entry and click **NTI traceback**. Then you are redirected to the related page of NTI, where you can view detailed traceback information.

7.9.2 Whitelist

Choose **Objects** > **Callback Monitoring** > **Whitelist**.

Figure 7-61 Callback monitoring whitelist page



By default, all entries are listed. You can select **IP** or **Domain Name** from the **Type** drop-down list to display only entries of the specified type.

Type an IP address or domain name and click **Search** to check whether it has been added to the whitelist.

Adding an Entry to the Blacklist

You can move whitelist entries to the blacklist in one of the following ways:

- Move one by one: Point to in the **Operation** column of an entry and click **Add to blacklist** to move this entry to the callback monitoring blacklist.
- Move all: Point to **More** and click **Blacklist all** to move all entries in the whitelist to the blacklist.
- Move multiple: Select one or more entries, point to **More**, and click **Blacklist selected** to move the selected entries to the blacklist.

7.10 URL Filtering

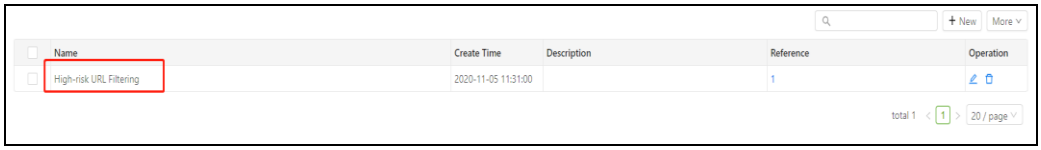
The URL Filtering module consists of the following:

- Profile
- Custom
- Category search
- Other settings

7.10.1 Profile

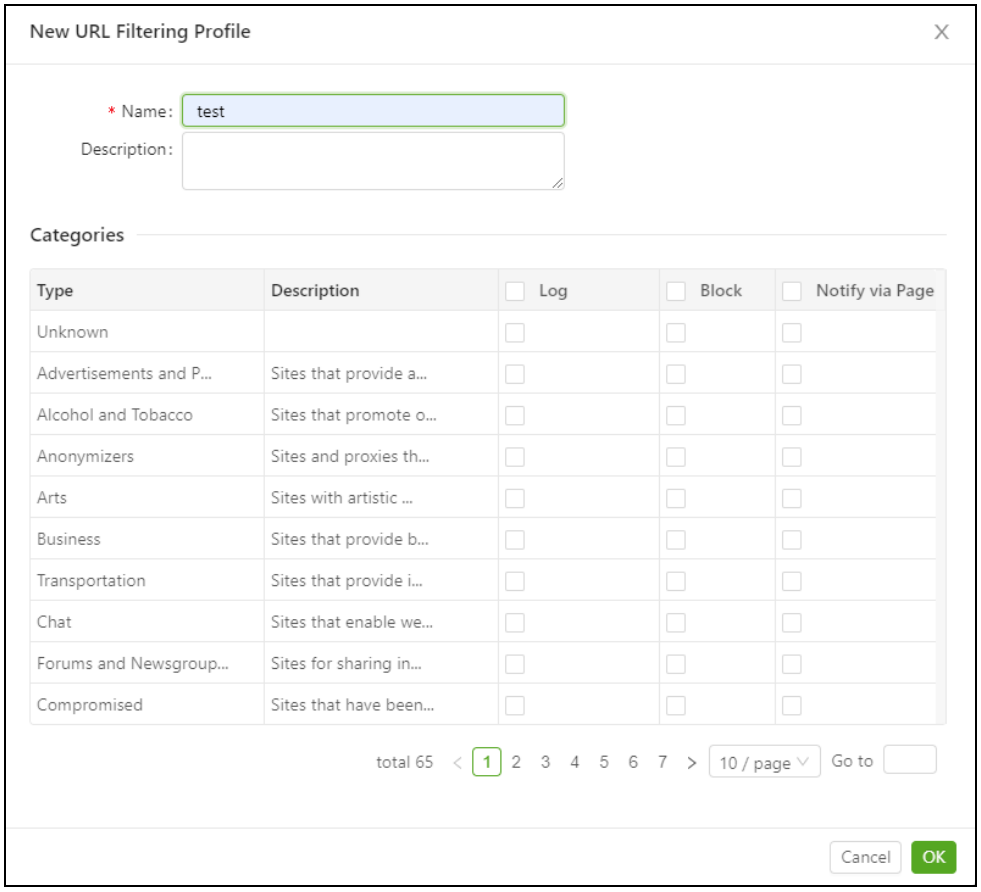
Step 1 Choose **Objects** > **URL Filtering** > **Profile**.

Figure 7-62 URL filtering profile page



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

Figure 7-63 Creating a URL filtering profile



Step 3 Configure parameters in the **New URL Filtering Profile** dialog box.

Table 7-38 Parameters for configuring a URL filtering profile

Parameter	Description
Name	Name of the profile.
Description	Brief description of the profile.
Rules	Specifies actions for each URL category. Options include **Log**, **Block**, and **Notify via Page**.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

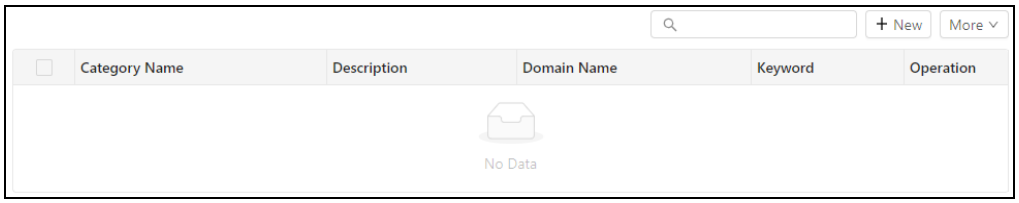
7.10.2 Custom URL Category

When you need to add some websites for filtering, you can create custom URL categories.

To configure a custom category, follow these steps:

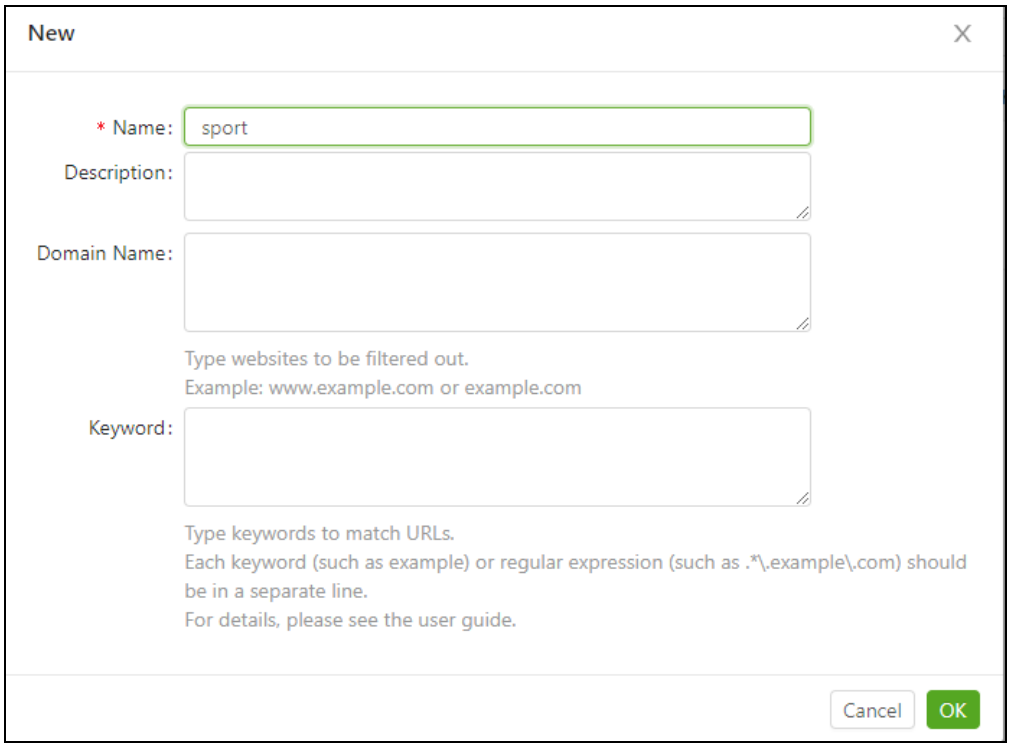
Step 1 Choose **Objects** > **URL Filtering** > **Custom**.

Figure 7-64 Custom page



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

Figure 7-65 Creating a URL category



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

Table 7-39 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 the carriage return.

Note	Once a URL is included in a custom category, it no longer exists in the predefined URL category database.

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

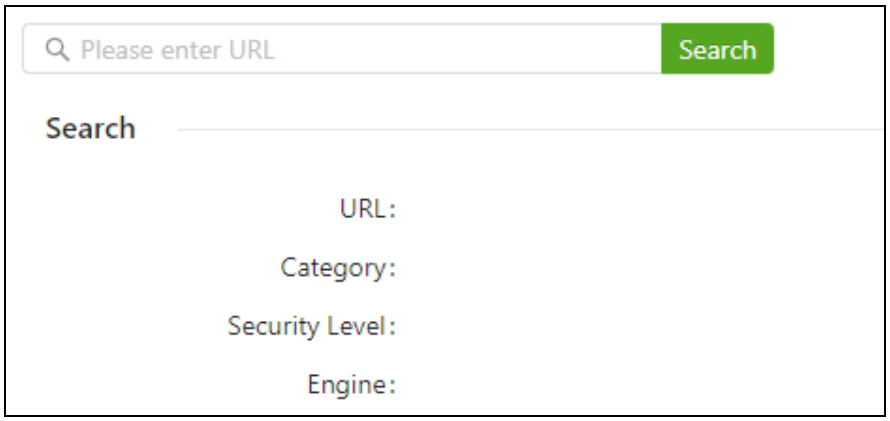
----End

7.10.3 Category Search

NIPS caches a small number of URL categories locally. With the URL search feature, you can quickly find the category to which a URL belongs. 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 that are categorized as **Other**, you can create custom categories for them. For how to create a URL category, see Custom URL Category. To query a URL, follow these steps:

Step 1 Choose **Objects** > **URL Filtering** > **Category Search**.

Figure 7-66 Category Search page



Step 2 Type a URL and click **Search**.

The system displays the category to which the URL belongs, as shown in Figure 7-67.

Figure 7-67 URL query result

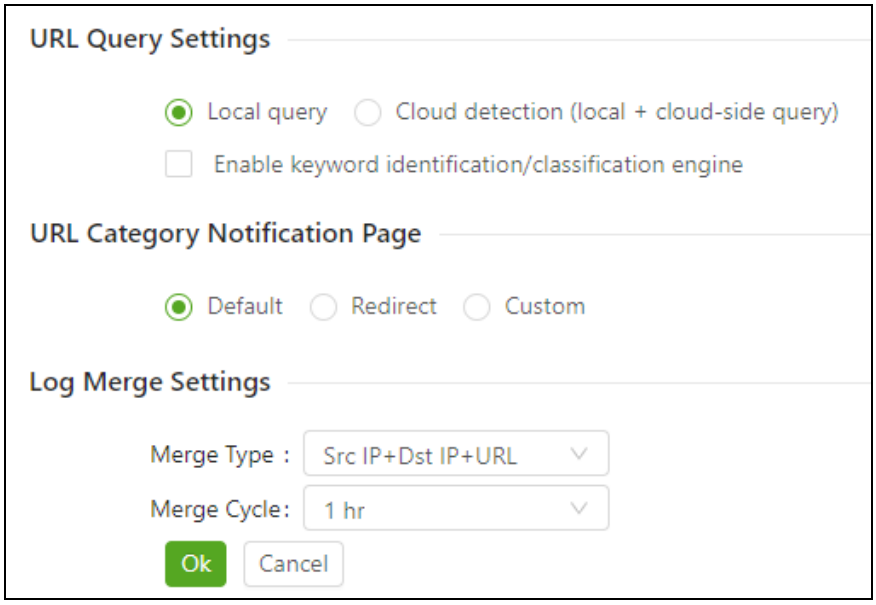
----End

7.10.4 Other Settings

You can configure the URL query mode and log merge settings. The procedure is as follows:

Step 1 Choose **Objects** > **URL Filtering** > **Settings**.

Figure 7-68 Other settings regarding URL filtering



Step 2 Configure parameters.

Table 7-40 URL query and log merge configuration parameters

Parameter	Description
URL Query Settings	Select a URL classification mode. • **Local query**: indicates that URL categories, including predefined URL

Parameter		Description
		categories and custom URL categories, will be obtained from the local NIPS. • **Cloud detection (local + cloud-side query)**: indicates that URL categories, including predefined URL categories, custom URL categories, and URL categories on servers, will be obtained from the local NIPS and online server.
URL Category Notification Page		Specifies a notification push page. Options include the following: • **Default**: uses the default notification push page. • **Redirect**: redirects users to a new address. In this case, you should set the redirect address. Only domain names in a format like www.nsfocus.com are supported. • **Custom**: allows you to set the title, content, and copyright statement for a custom notification page.
Log Merge Settings	Merge Type	Specifies whether to enable log merge and, if yes, the merge type. Option include the following: • **Disable**: does not merge logs. In this case, multiple alerts may be generated throughout an attack. • **Src IP+URL**: merges logs of events involving the same source IP address and the same URL as one. • **Dst IP+URL**: merges logs of events involving the same destination IP address and the same URL as one. • **Src IP+Dst IP+URL**: merges logs of events involving the same source and destination IP addresses and the same URL as one.
	Merge Cycle	Specifies the interval at which logs are merged.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.11 Application Control

The Application Control module consists of the following:

- Profile
- Other Settings

7.11.1 Profile

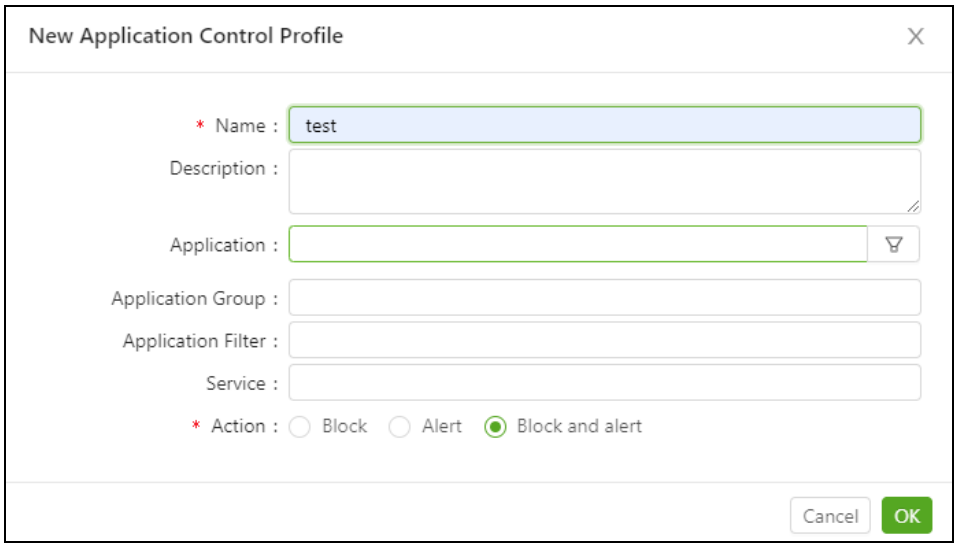
To create an application control profile, follow these steps:

Step 1 Choose **Objects** > **Application Control** > **Profile**.

Figure 7-69 Application control profile page

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

Figure 7-70 Creating an application control profile



Step 3 Configure parameters in the **New Application Control Profile** dialog box.

Table 7-41 Parameters for configuring an application control profile

Parameter	Description
Name	Name of the profile.
Description	Brief description of the profile.
Application	Specifies applications to be covered by the profile.
Application Group	Specifies application groups to be covered by the profile.
Application Filter	Specifies application filters.
Service	Specifies services.
Action	Specifies an action to be taken against matching traffic. Options include **Block**, **Alert**, and **Block and alert**.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

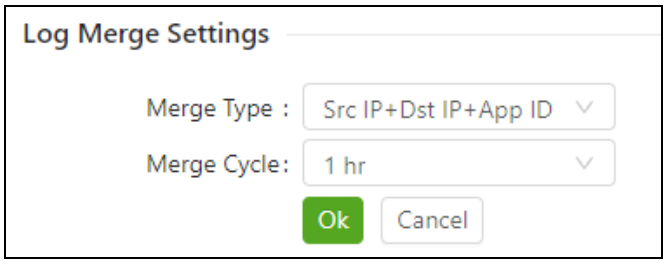
----End

7.11.2 Other Settings

You can configure application control log merge settings. The procedure is as follows:

Step 1 Choose **Objects** > **Application Control** > **Settings**.

Figure 7-71 Other settings regarding application control



Step 2 Configure parameters.

Table 7-42 Application control log merge parameters

Parameter	Description
Merge Type	Specifies whether to enable log merge and, if yes, the merge type. Option include the following: • **Disable**: does not merge logs. In this case, multiple alerts may be generated throughout an attack. • **Src IP+App ID**: merges logs of events involving the same source IP address and the same application as one. • **Dst IP+App ID**: merges logs of events involving the same destination IP address and the same application as one. • **Src IP+Dst IP+App ID**: merges logs of events with the same source and destination IP addresses and the same application as one.
Merge Cycle	Specifies the interval at which logs are merged.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.12 Data Loss Prevention

The Data Loss Prevention (DLP) module consists of the following:

- Profile
- Sensitive Data

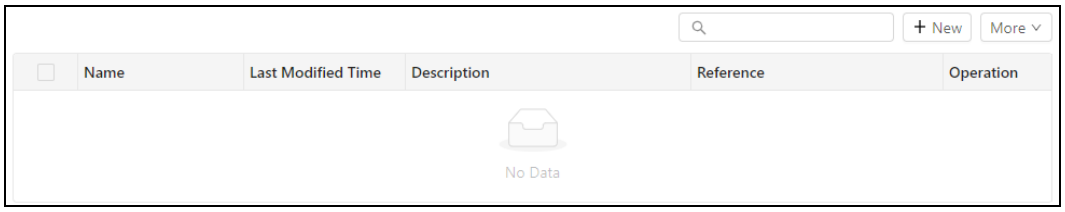
- Other settings

7.12.1 Profile

To create a DLP profile, follow these steps:

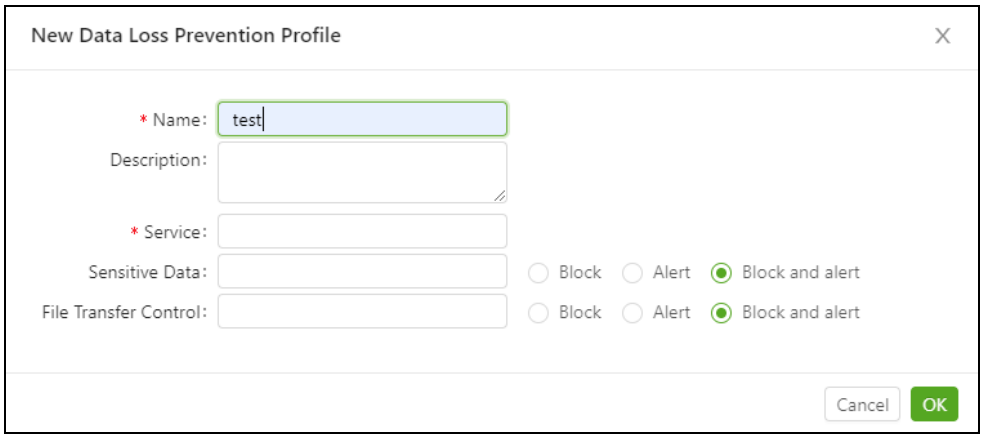
Step 1 Choose **Objects** > **Data Loss Prevention** > **Profile**.

Figure 7-72 DLP profile page



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

Figure 7-73 Creating a DLP profile



Step 3 Configure parameters in the **New Data Loss Prevention Profile** dialog box.

Table 7-43 Parameters for configuring a DLP profile

Parameter	Description
Name	Name of the profile.
Description	Brief description of the profile.
Service	Specifies services to be covered by the profile.
Sensitive Data	Specifies sensitive data to be covered by the profile and an action to be taken upon detection of a data breach.
File Transfer Control	Specifies file types to be covered by the profile and an action to be taken upon detection of a data breach.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

7.12.2 Sensitive Data

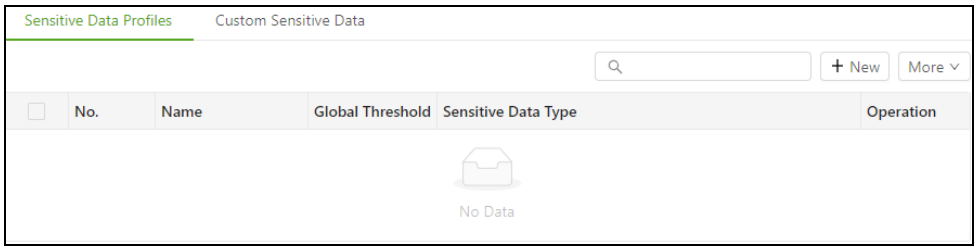
Sensitive data can be divided into predefined sensitive data and custom sensitive data.

7.12.2.1 Sensitive Data Profile

Configuring sensitive data objects can protect internal sensitive data, such as identity (ID) card numbers, bank card numbers, and telephone numbers, from being disclosed. To configure a sensitive data profile, follow these steps:

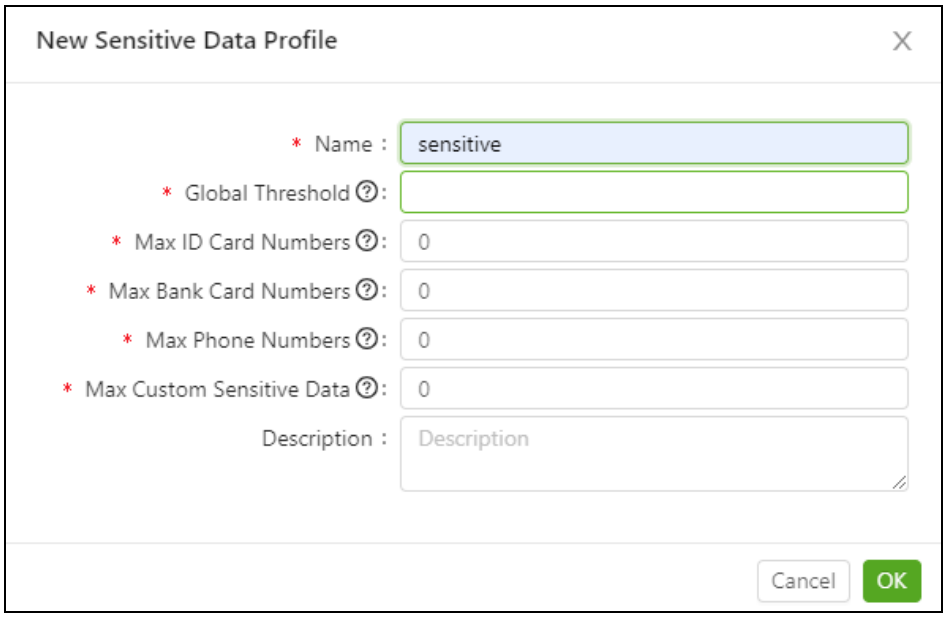
Step 1 Choose **Objects** > **Data Loss Prevention** > **Sensitive Data** > **Sensitive Data Profiles**.

Figure 7-74 Sensitive data profile page



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

Figure 7-75 Creating a sensitive data profile



Step 3 Configure parameters in the **New Sensitive Data Profile** dialog box.

Table 7-44 Parameters for creating a sensitive data profile

Parameter	Description
Name	Name of the profile. The name must be unique and cannot contain the following special characters: % \ ` < > ' & "
Global Threshold	Specifies a global threshold for the quantity of sensitive data in a session, which must be greater than the threshold for each type of sensitive data. The value range is 1–65535. When the total number of sensitive data entries (including ID card numbers, bank card numbers, and telephone numbers) in a session exceeds the global threshold, a global sensitive data alert is generated.
Max ID Card Numbers	Specifies the maximum number of ID card numbers in a session, which must be smaller than the global threshold.
Max Bank Card Numbers	Specifies the maximum number of bank card numbers in a session, which must be smaller than the global threshold.
Max Phone Numbers	Specifies the maximum number of telephone numbers in a session, which must be smaller than the global threshold.
Max Custom Sensitive Data	Specifies the maximum number of data entries of a custom type in a session. When the actual number exceeds the threshold, a related alert is triggered. The value **0** indicates that NIPS will not detect custom sensitive data. For how to configure custom sensitive data types, see Custom Sensitive Data.
Description	Brief description of the profile.

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

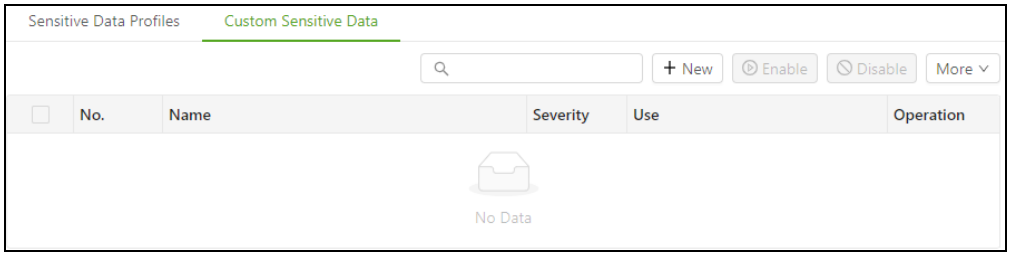
----End

7.12.2.2 Custom Sensitive Data

To configure a custom sensitive data type, follow these steps:

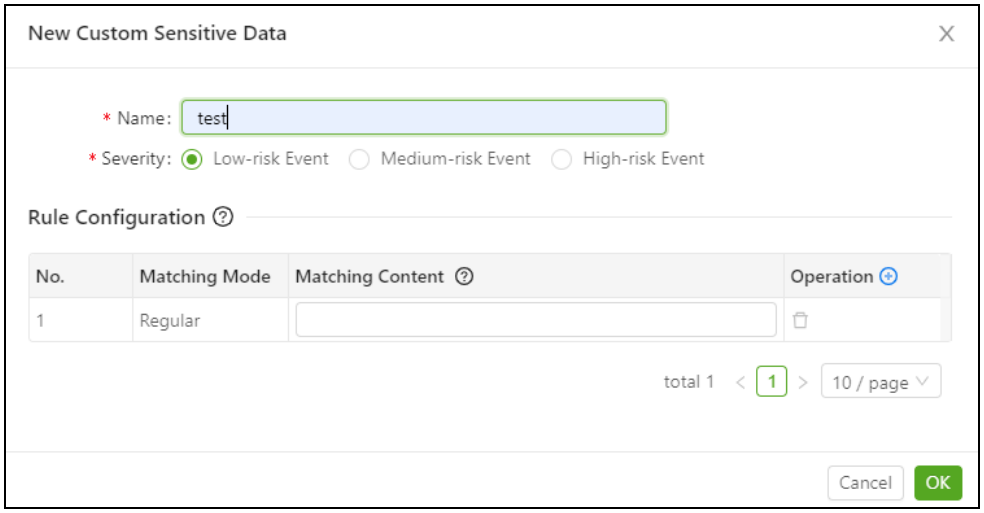
Step 1 Choose **Objects** > **Data Loss Prevention** > **Sensitive Data** > **Custom Sensitive Data**.

Figure 7-76 Custom Sensitive Data page



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

Figure 7-77 Creating a custom sensitive data type



Step 3 Configure parameters in the **New Custom Sensitive Data** dialog box.

Table 7-45 Parameters for creating a custom sensitive data type

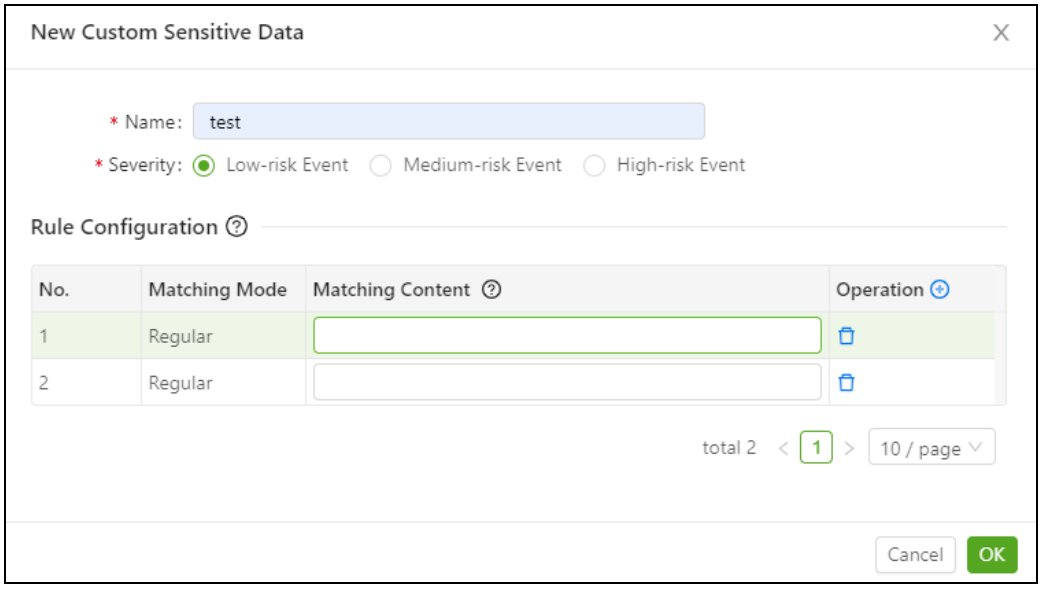
Parameter	Description
Name	Name of the custom sensitive data type. The name must be unique and cannot contain the following special characters: % \ ` < > ' & "
Severity	Risk level of the custom sensitive data type.

Step 4 Configure rules.

Note	Custom rules slow down the engine's efficiency. Therefore, you are advised to verify each rule you create to make it count.

a. Click ⊕ in the **Operation** column to add an OR segment.

Figure 7-78 Adding an OR segment



b. Type the matching content.

Follow this format when typing the matching content: (^|[^\d])436742\d{10}([^\d]|$), which represents 16 digits, with the first six being 436742.

Step 5 Click **OK** to save the settings.

Step 6 Click **Commit** in the quick access bar to make the settings take effect.

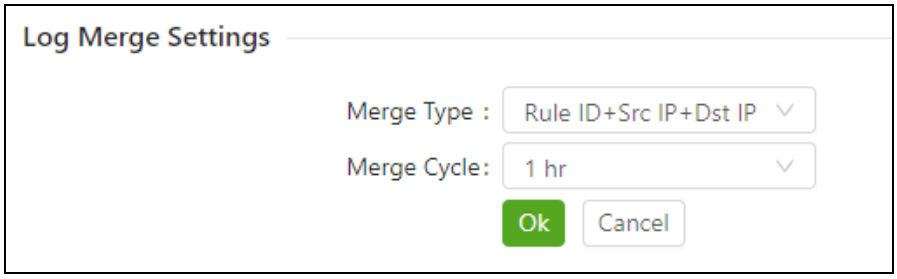
----End

7.12.3 Other Settings

To configure log merge parameters for DLP events, follow these steps:

Step 1 Choose **Objects** > **Data Loss Prevention** > **Settings**.

Figure 7-79 Other settings regarding DLP



Step 2 Configure parameters.

Table 7-46 Log merge parameters

Parameter	Description
Merge Type	Specifies whether to enable log merge and, if yes, the merge type. Options include the following: • **Disable**: does not merge logs. In this case, multiple alerts may be generated throughout an attack. • **Rule ID+Src IP**: merges logs of events involving the same rule and the same source IP address as one. • **Rule ID+Dst IP**: merges logs of events involving the same rule and the same destination IP address as one. • **Rule ID+Src IP+Dst IP**: merges logs of events involving the same rule and the same source and destination IP addresses as one.
Merge Cycle	Specifies the interval at which logs are merged.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

8 Network

This chapter contains the following sections:

Section	Description
Interfaces	Describes how to configure NIPS interfaces.
HA	Describes how to configure high availability parameters.
Bypass	Describes how to configure bypass parameters.
Security Zones	Describes how to create security zones.
SNMP	Describes how to configure SNMP parameters.
DNS	Describes how to configure DNS server addresses.
Exchange	Describes data exchange protocols and how to configure such a protocol.
Route	Describes how to configure routing.
DHCP	Describes how to configure DHCP relayS.
Authentication Server	Describes how to configure authentication server parameters.
Mail Server	Describes how to configure mail server parameters.

8.1 Interfaces

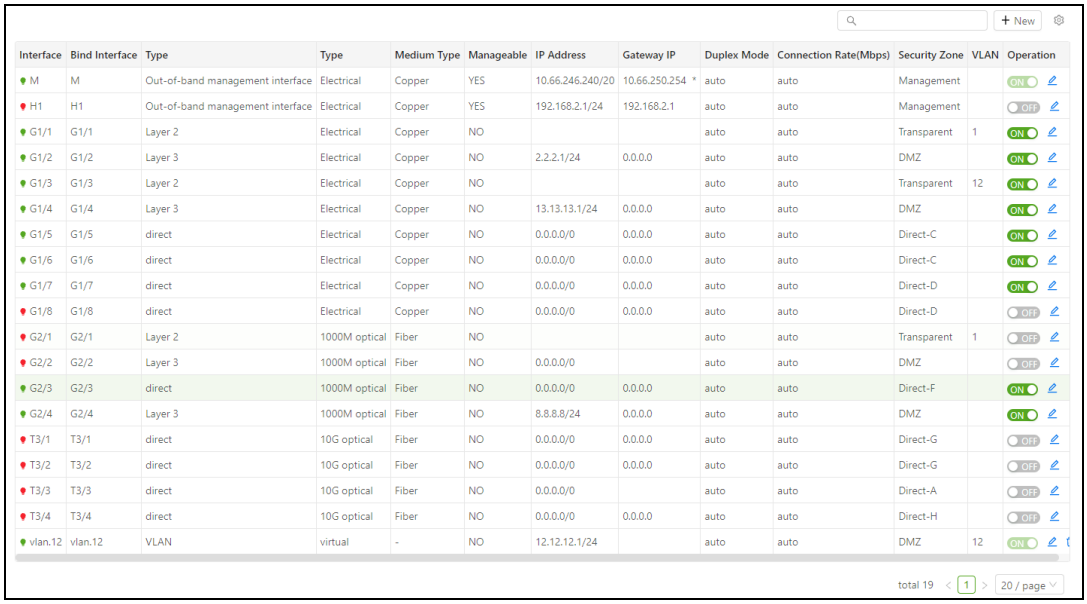
An interface is a shared boundary or connection between devices for data exchange. The Interface module consists of the following:

- Interface setting: property settings of NIPS interfaces.
- Response ports configuration

8.1.1 Interface Setting

Choose **Network** > **Interfaces** > **Setting**.

Figure 8-1 Interface list



Interface	Bind Interface	Type	Type	Medium Type	Manageable	IP Address	Gateway IP	Duplex Mode	Connection Rate(Mbps)	Security Zone	VLAN	Operation
M	M	Out-of-band management interface	Electrical	Copper	YES	10.66.246.240/20	10.66.250.254 *	auto	auto	Management		ON
H1	H1	Out-of-band management interface	Electrical	Copper	YES	192.168.2.1/24	192.168.2.1	auto	auto	Management		OFF
G1/1	G1/1	Layer 2	Electrical	Copper	NO			auto	auto	Transparent	1	ON
G1/2	G1/2	Layer 3	Electrical	Copper	NO	2.2.2.1/24	0.0.0.0	auto	auto	DMZ		ON
G1/3	G1/3	Layer 2	Electrical	Copper	NO			auto	auto	Transparent	12	ON
G1/4	G1/4	Layer 3	Electrical	Copper	NO	13.13.13.1/24	0.0.0.0	auto	auto	DMZ		ON
G1/5	G1/5	direct	Electrical	Copper	NO	0.0.0.0/0	0.0.0.0	auto	auto	Direct-C		ON
G1/6	G1/6	direct	Electrical	Copper	NO	0.0.0.0/0	0.0.0.0	auto	auto	Direct-C		ON
G1/7	G1/7	direct	Electrical	Copper	NO	0.0.0.0/0	0.0.0.0	auto	auto	Direct-D		ON
G1/8	G1/8	direct	Electrical	Copper	NO	0.0.0.0/0	0.0.0.0	auto	auto	Direct-D		OFF
G2/1	G2/1	Layer 2	1000M optical	Fiber	NO			auto	auto	Transparent	1	OFF
G2/2	G2/2	Layer 3	1000M optical	Fiber	NO	0.0.0.0/0		auto	auto	DMZ		OFF
G2/3	G2/3	direct	1000M optical	Fiber	NO	0.0.0.0/0	0.0.0.0	auto	auto	Direct-F		ON
G2/4	G2/4	Layer 3	1000M optical	Fiber	NO	8.8.8.8/24	0.0.0.0	auto	auto	DMZ		ON
T3/1	T3/1	direct	10G optical	Fiber	NO	0.0.0.0/0	0.0.0.0	auto	auto	Direct-G		OFF
T3/2	T3/2	direct	10G optical	Fiber	NO	0.0.0.0/0	0.0.0.0	auto	auto	Direct-G		OFF
T3/3	T3/3	direct	10G optical	Fiber	NO	0.0.0.0/0		auto	auto	Direct-A		OFF
T3/4	T3/4	direct	10G optical	Fiber	NO	0.0.0.0/0	0.0.0.0	auto	auto	Direct-H		OFF
vlan.12	vlan.12	VLAN	virtual	-	NO	12.12.12.1/24		auto	auto	DMZ	12	ON

On NIPS, physical interfaces include out-of-band management interfaces and Ethernet 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

The loopback interface is a layer 3 logical interface and does not need to be bound to any physical interfaces. Therefore, its link status is immune to external factors. An administrator can learn about the device status from the link status of the loopback interface. In addition, the loopback interface can be used for the following purposes:

- 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

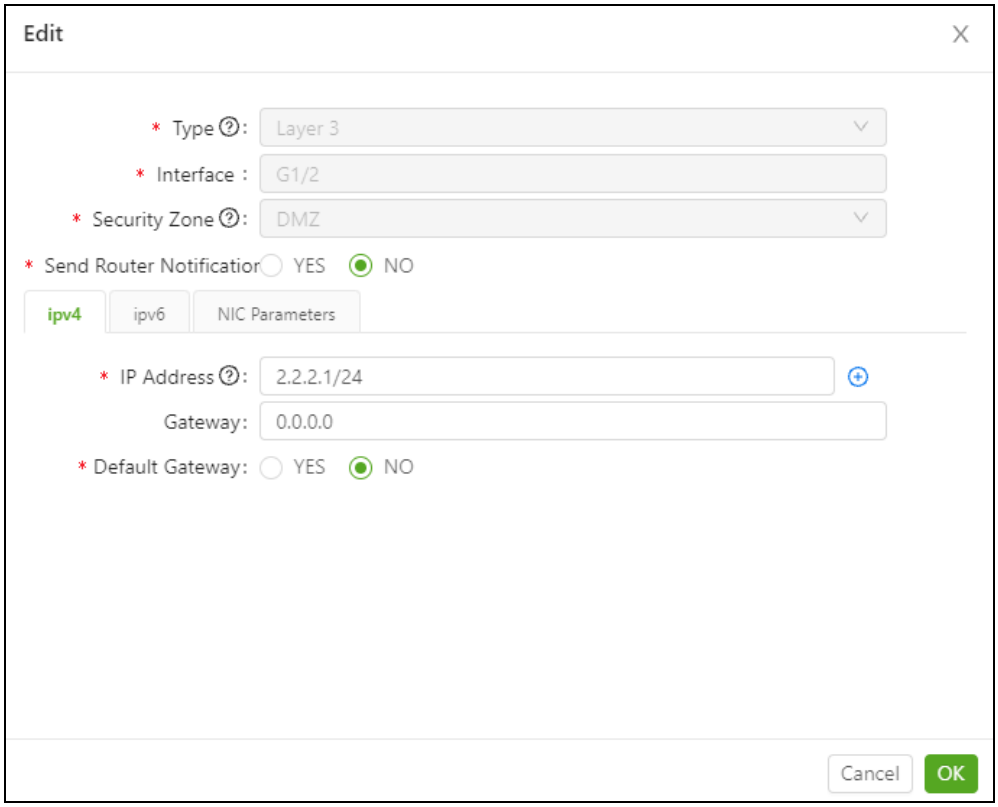
  VLAN interfaces are layer 3 logical interfaces created based on layer 2 physical interfaces.

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

8.1.1.1 Modifying Interface Configurations

Step 1 In the interface list, click in the **Operation** column of an interface and then configure parameters in the **Edit** dialog box.

Figure 8-2 Configuring an Interface



Ethernet working interfaces are divided into the following:

- Unconfigured

  Such interfaces are not configured.
- In-band management interface

  A service interface acts as a management interface.
- Layer 2 interface

  Layer 2 interfaces do not have IP addresses, and can be used only for forwarding Ethernet frames. Generally, layer 2 interfaces connect to a layer 2 switch.
- Layer 3 interface

  IP addresses can be assigned to layer 3 interfaces, which are used 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, NIPS can monitor traffic.
- Direct interface

  Such an interface connects two interfaces in the same security zone for data communication. These two interfaces respectively work as an IN and OUT interface.
- Aggregation member interface

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

For the detailed description of parameters, see Table 8-1.

Note	• You must configure security zones in advance. For details, see section 8.4 Security Zones. • 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.

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

Table 8-1 Interface parameters

Parameter		Description
Security Zone		Select a security zone for the interface. Note The security zone cannot be changed in the following circumstances: • When the interface is interface M or H. • When the license is abnormal. • When the interface is referenced in an asymmetric routing policy. • When the interface is referenced in external bypass or block configuration. • When the interface is referenced in bonding.
Manageable		Specifies whether the interface is a management interface.
IPv4	IP Address	Specifies the IPv4 address of the interface. You can configure up to three IPv4 addresses. Click the icon ⊕ to add an IPv4 address.
	Gateway	Specifies the IPv4 gateway so that the interface is accessible on the network.
	Default Gateway	Specifies whether the gateway is a default one.
IPv6	Configuration Mode	Specifies how to configure the IPv6 address, which can be **Automatic** or **Manual**.
	Address	When **Configuration Mode** is set to **Manual**, the address must be configured in IPv6 format. After the IPv6 address is configured, you need to restart the service by clicking **Reload Service** under **System** > **System Control**.
	Gateway	When **Configuration Mode** is set to **Manual**, the IPv6 gateway must be configured so that the interface is accessible on the network.
	Default Gateway	Specifies whether the gateway is a default one.
NIC Parameters	Duplex Mode	Specifies the duplex mode of the interface, which can be any of the following: • **Auto**: transmits data according to the actual duplex mode. • **Half**: transmits data in just one direction (either sends or receives data)

Parameter		Description
		at a time. • **Full**: provides communication in both directions (sends and receives data) and allows this to happen simultaneously.
	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 1700 bytes. The default value is **1500**.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

Enabling/Disabling an Ethernet Interface

All Ethernet interfaces are in either enabled or disabled state. Disabled interfaces do not send or receive packets. The OFF icon in the **Operation** column of an interface indicates that the interface is disabled. You can click this icon to enable it. Then the icon turns to ON. Clicking this icon will disable 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**.

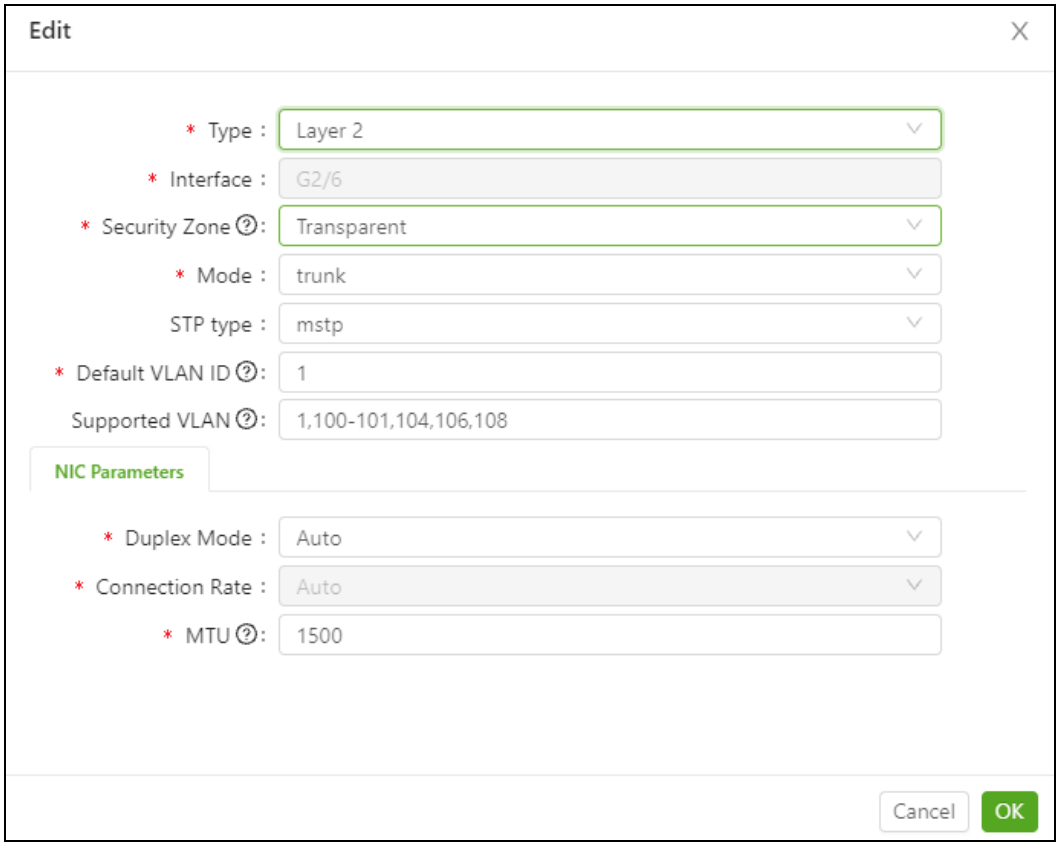
  – If yes, NIPS checks whether the trunk interface allows VLAN data to pass through, which depends on whether the packet's VLAN ID belongs to the range specified in **Supported VLAN**. If yes, NIPS forwards the packet. Otherwise, NIPS drops the packet.

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 8-1, click in the **Operation** column of an interface and then set **Interface Type** to **Layer 2** in the **Edit** dialog box.

Figure 8-3 Configuring a layer 2 interface



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

Table 8-2 Parameters for configuring a layer 2 interface

Parameter	Description
Type	Specifies the type of the interface, which should be set to **Layer 2**.
Interface	Indicates the default interface name, which cannot be edited.
Security Zone	Specifies the working mode of the security zone to which the interface belongs. 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

Parameter	Description
	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**. It specifies VLAN IDs that are allowed to pass through the interface. Multiple VLAN IDs should be separated by comma (,) and consecutive VLAN IDs should be separated by a hyphen (-). For example, you can configure "1,2,4" and "2-5".
NIC Parametes	
Duplex Mode	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 3 Click **OK** to complete the configuration.

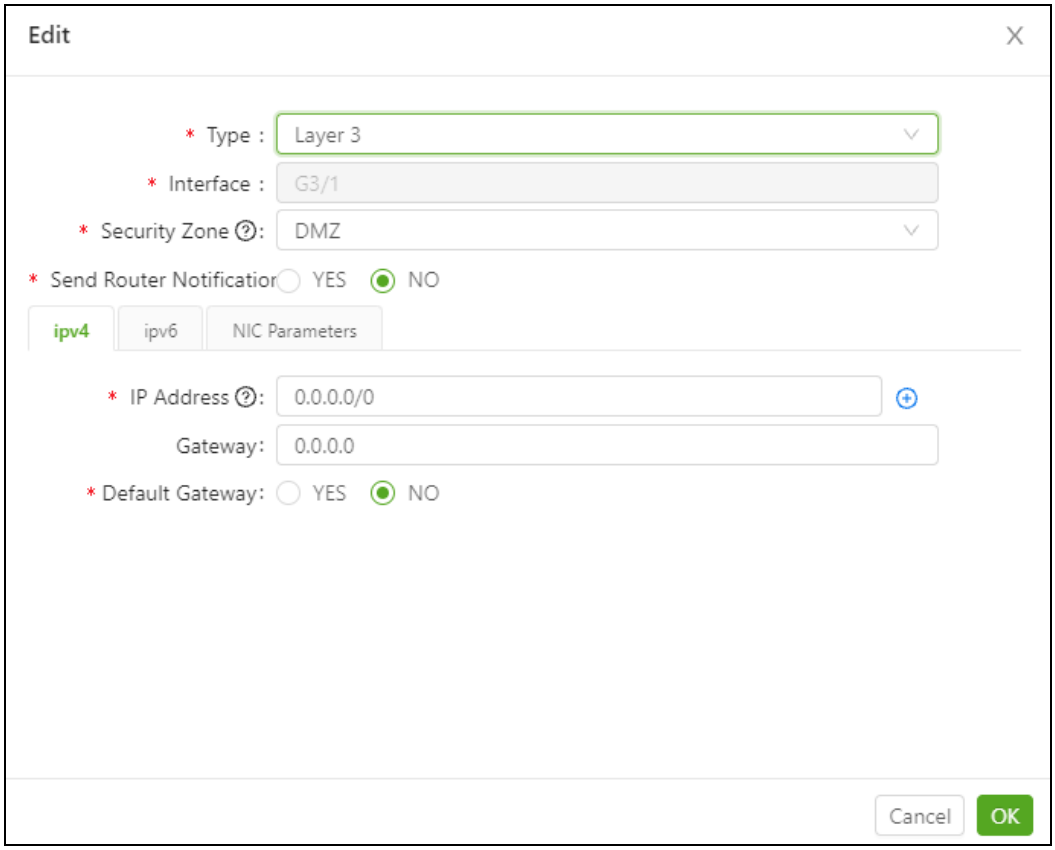
Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

Configuring a Layer 3 Interface

Step 1 On the page shown in Figure 8-1, click in the **Operation** column of an interface and then set **Type** to **Layer** 3 in the **Edit** dialog box.

Figure 8-4 Configuring a layer 3 interface



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

Table 8-3 Parameters for configuring a layer 3 interface

Parameter		Description
Type		Specifies the type of the interface, which should be set to **Layer 3**.
Interface		Indicates the default interface name, which cannot be edited.
Security Zone		Specifies the working mode of the security zone to which the interface belongs. 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.
Send Router Notification		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, this parameter should be set to **Yes.**
IPv4	IP Address	Specifies the IPv4 address of the interface. You can configure up to three IPv4 addresses. Click the icon ⊕ to add an IPv4 address.
	Gateway	Specifies the IPv4 gateway so that the interface is accessible on the network.
	Default Gateway	Specifies whether the gateway is a default one.
IPv6	Configurati	Specifies how to configure the IPv6 address, which can be **Automatic** or

Parameter		Description
	on Mode	**Manual**.
	Address	When **Configuration Mode** is set to **Manual**, the address must be configured in IPv6 format. After the IPv6 address is configured, you need to restart the service by clicking **Reload Service** under **System** > **System Control**.
	Gateway	When **Configuration Mode** is set to **Manual**, the IPv6 gateway must be configured so that the interface is accessible on the network.
	Default Gateway	Specifies whether the gateway is a default one.
NIC Parameters	Duplex Mode	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 1700 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.
	MAC	Specifies the MAC address of the interface. Only unicast MAC addresses can be configured. Only MAC addresses that are manually configured are displayed here.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

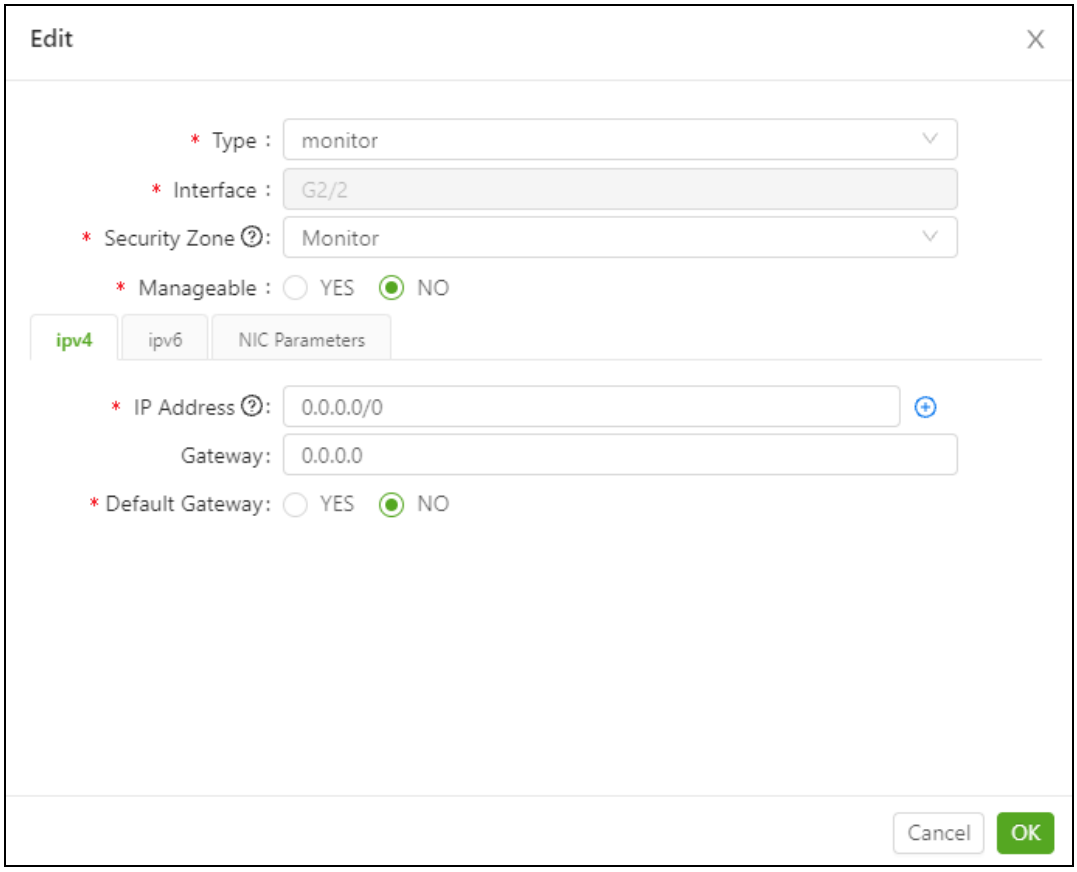
----End

Configuring 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 for user's analysis. For details about playback test, see section 9.8.2 Packet Playback.

Step 1 On the page shown in Figure 8-1, click in the **Operation** column of an interface and then set **Type** to monitor in the **Edit** dialog box.

Figure 8-5 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 2 Click **OK** to complete the configuration.

Step 3 Click **Commit** in the quick access bar to make the settings take effect.

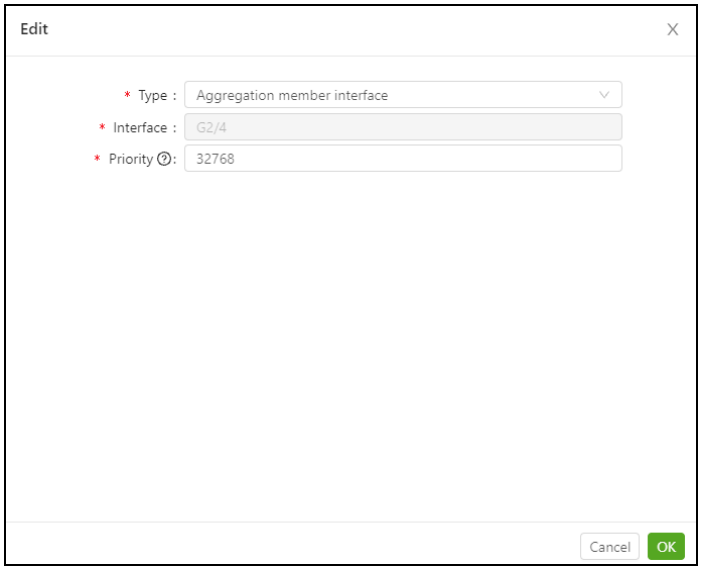
----End

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 8.1.1.2 Creating an Aggregation Interface.

Step 1 On the page shown in Figure 8-1, click in the **Operation** column of an interface and then set **Type** to **Aggregation member interface** in the **Edit** dialog box.

Figure 8-6 Configuring an aggregation member interface



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

Table 8-4 Parameters for configuring an aggregation member interface

Parameter	Description
Type	Specifies the type of the interface, which should be set to **Aggregation member interface**.
Interface	Indicates the default interface name, which cannot be edited.
Priority	Specifies the priority of the Link Aggregation Control Protocol (LACP). The priority must be an integer in the range of 0–65535. The priority is valid for dynamic binding but not for manual binding.

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

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

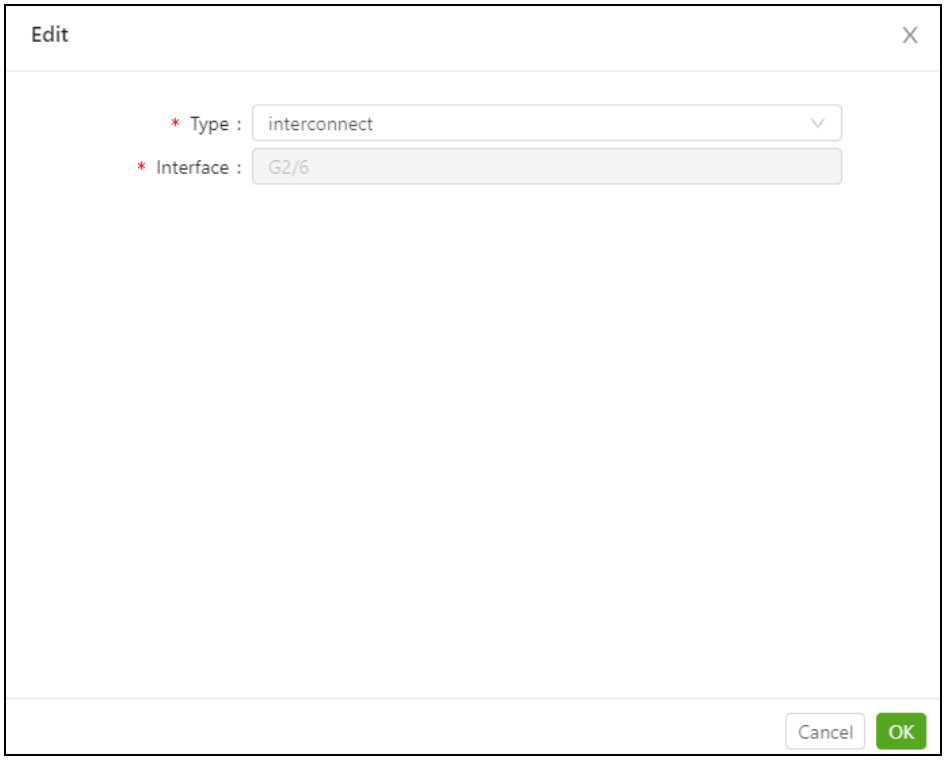
Configuring a Device Interconnection Interface

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 interface is configured, you can specify this interface for asymmetric routing support. For details, see section 8.2.3 Asymmetric Routing.

Step 1 On the page shown in Figure 8-1, click in the **Operation** column of an interface and then set **Type** to **interconnect** in the **Edit** dialog box.

Figure 8-7 Configuring a device interconnection interface



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

Step 3 Click **Commit** in the quick access bar to make the settings take effect.

----End

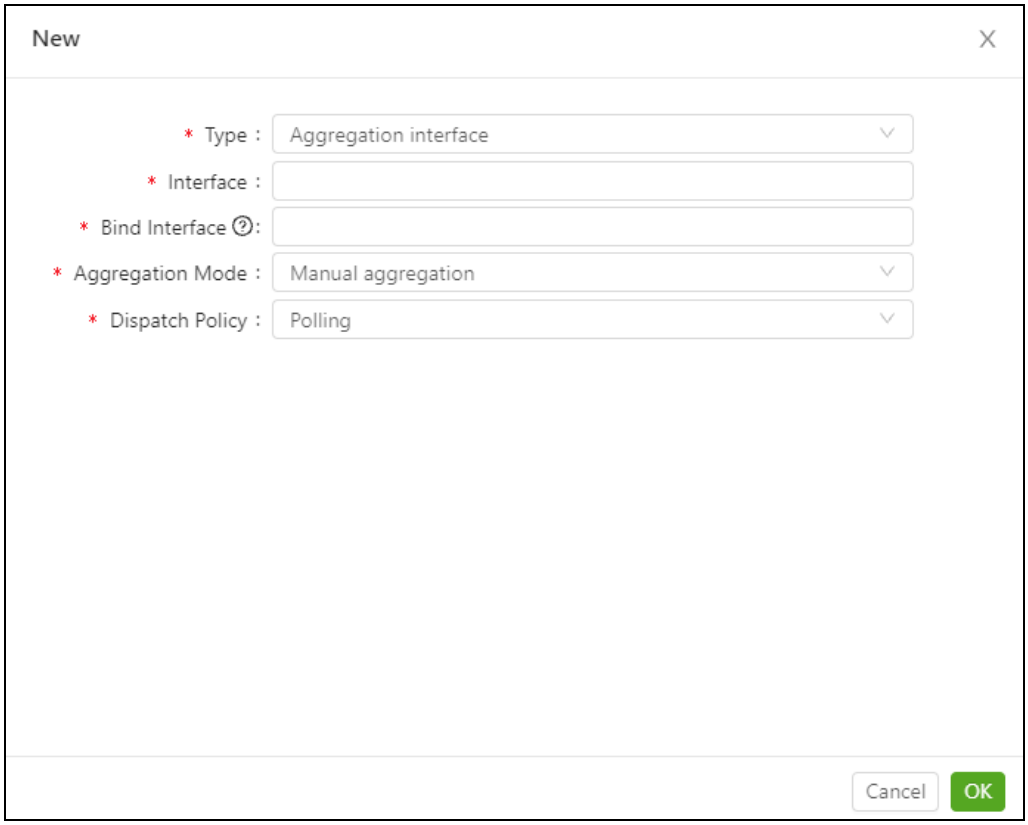
8.1.1.2 Creating an Aggregation Interface

NIPS supports manually aggregating two or three interfaces in the same security zone and dispatching data packets based on different dispatch policies to achieve load balancing.

To create an aggregation interface, follow these steps:

Step 1 On the page shown in Figure 8-1, click **New** in the upper-right corner of the page and then set **Type** to **Aggregation interface** in the **New** dialog box.

Figure 8-8 Creating an aggregation interface



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

Table 8-5 Parameters for configuring an aggregation interface

Parameter	Description
Interface Type	Specifies the type of the interface, which should be set to **Aggregation interface.**
Interface	Specifies the name of the aggregation interface.
Bind Interface	Specifies the aggregation member interface which can be selected from the existing aggregation member interfaces. The duplex modd, connection rate, and security zone 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.
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: • **Src MAC**: indicates that packets with the same source MAC address are sent from the same interface. Otherwise, they are sent from different interfaces.

Parameter	Description
	• **Dst 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.

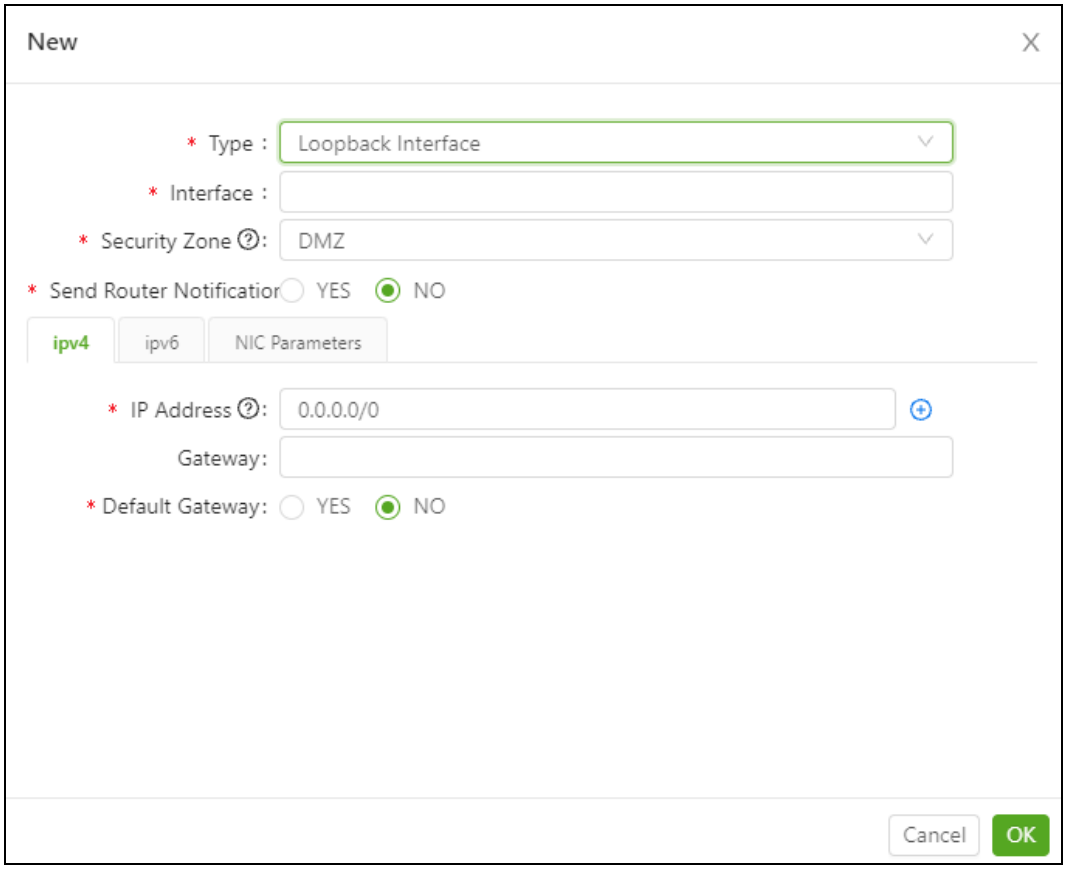
Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.1.1.3 Creating a Loopback Interface

Step 1 On the page shown in Figure 8-1, click **New** in the upper-right corner of the page and then set **Type** to **Loopback interface** in the **New** dialog box.

Figure 8-9 Creating a loopback interface



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

For **Interface**, type the interface name you want to customize.

Other parameters are the same as those for configuring a layer 3 Ethernet interface. For details, see Table 8-3.

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

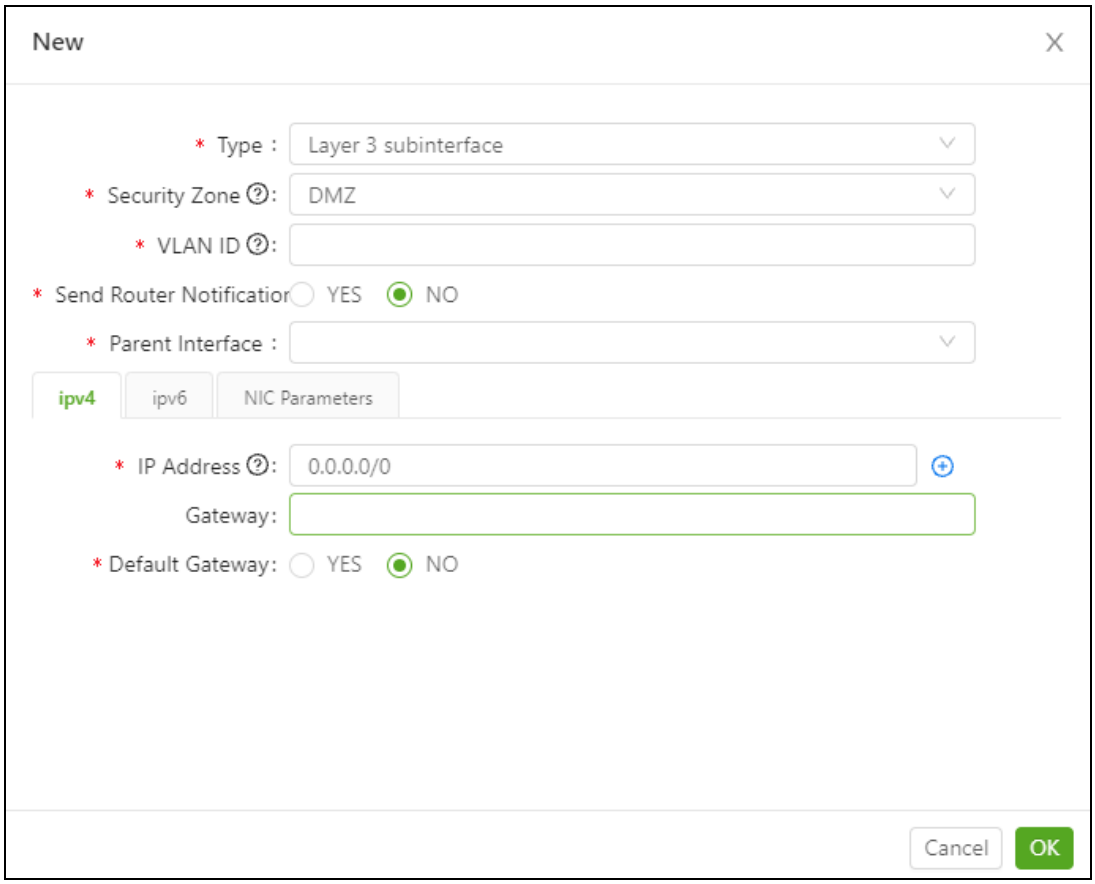
Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.1.1.4 Creating a Layer 3 Subinterface

Step 1 On the page shown in Figure 8-1, click **New** in the upper-right corner of the page and then set **Type** to **Layer 3 subinterface** in the **New** dialog box.

Figure 8-10 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 Table 8-3.

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

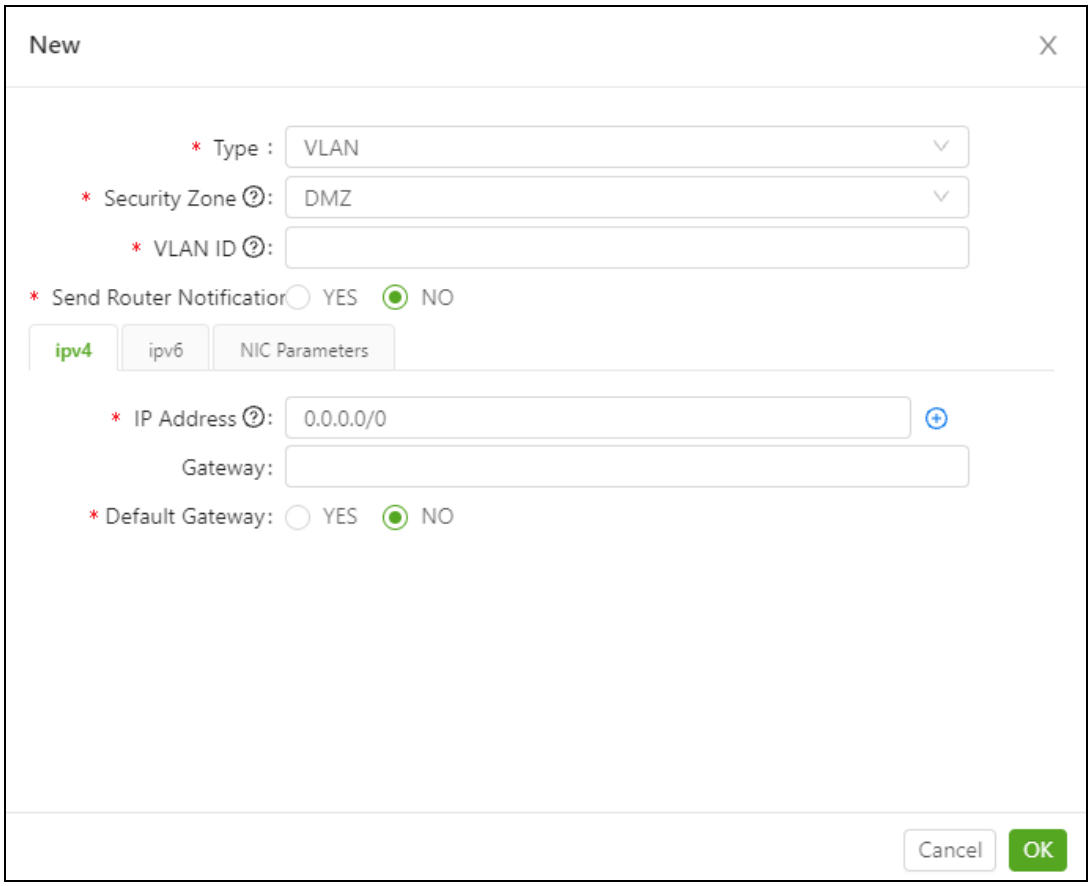
Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.1.1.5 Creating a VLAN Interface

Step 1 On the page shown in Figure 8-1, click **New** in the upper-right corner of the page and then set **Interface Type** to **VLAN** in the **New** dialog box.

Figure 8-11 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 Table 8-3.

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

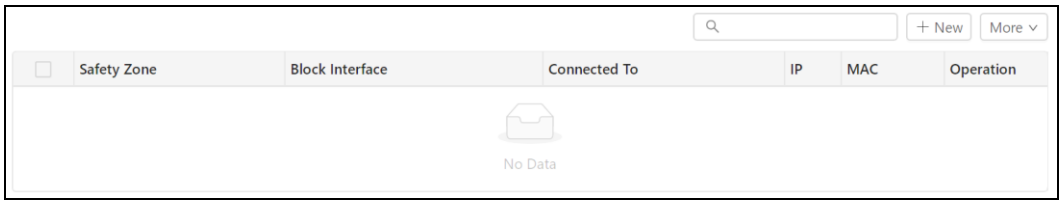
Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.1.2 Response Port Configuration

Step 1 Choose **Network** > **Interfaces** > **Response Ports**.

Figure 8-12 Response ports



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

Figure 8-13 Creating a response port

Step 3 Configure parameters of a response port.

Table 8-6 Parameters of a response port

Parameter	Description
Name	Specifies a security zone, which can only be **Monitor** here. The security zone must be associated with an interface first.
Block Interface	Specifies a previously configured response interface.
Connected To	Specifies a network to connect to, which can be **Switch** or **Router**.
MAC Address	Specifies a MAC address.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.2 HA

During data communication, any kind of software or hardware error may cause improper network connection or network interruption, which in turn will cause data transmission failure. To avoid communication interruption resulting from single points of failure, NIPS provides the high availability (HA) function to enhance network reliability.

The HA module consists of the following:

- Basic configuration
- Direct connect configuration
- Asymmetric routing
- VRRP configuration
- Layer 2 configuration

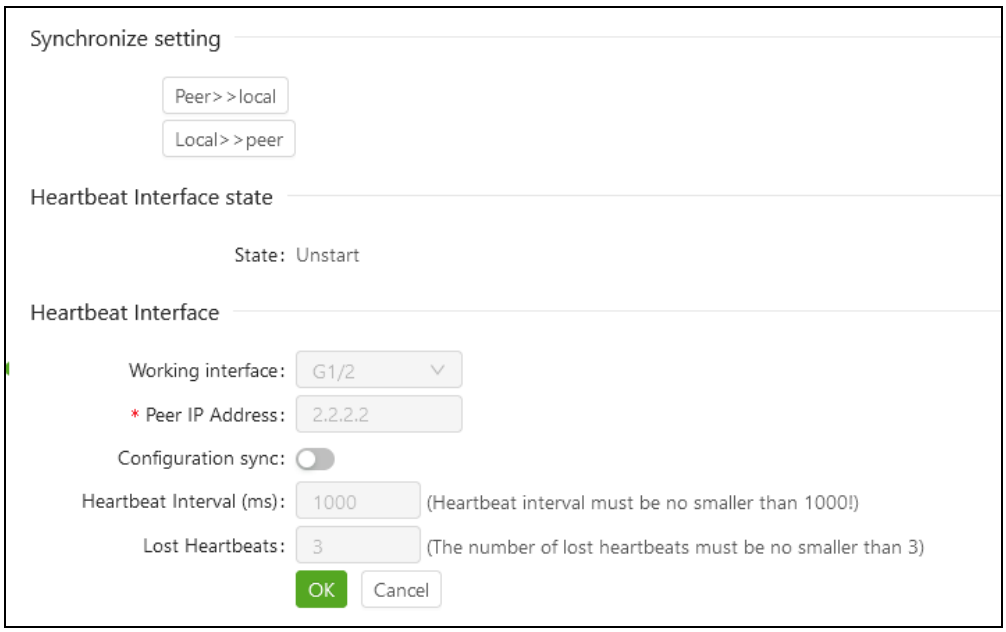
8.2.1 Basic Configuration

Two devices are connected via a management interface (heartbeat interface) for transmitting heartbeat information, and synchronizing configuration files and session information.

To configure the HA function, follow these steps:

Step 1 Choose **Network** > **HA** > **Basic Configuration**.

Figure 8-14 Basic HA parameters



Step 2 Configure parameters in the **Heartbeat Interface** area.

Table 8-7 Basic HA parameters

Parameter	Description
Working Interface	Heartbeat interface on the local device. On an NIPS device, the interface M, H1, or the layer 3 interface can be used as a heartbeat interface. The heartbeat interface cannot be used to handle service traffic.
Peer IP Address	IP address of the heartbeat interface on the peer device.
Configuration Sync	Controls whether to enable automatic synchronization. You can click the icon on the right side of **Configuration Sync** to enable the function. Then, click **Commit** in the quick access bar to make the settings take effect.
Heartbeat Interval (ms)	Specifies the interval at which the local device sends a heartbeat message to the peer device. The minimum value is **1000** ms. The value of this parameter must be the same for the local device and the peer device.
Lost Heartbeats	Specifies a threshold for the number of times the local device fails to receive heartbeat messages from the peer device. When this threshold is reached, the local device deems 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 **Activated**, while that of the peer device is displayed as **Unknown**.

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

----End

Manual Synchronization Configuration

- Click **Peer** >> **local** to synchronize the configurations on the peer device to the local device.
- Click **Local** >> **peer** to synchronize the configurations on the local device to the peer device.

8.2.2 Direct Connect Configuration

Direct HA of NIPS supports only the active/standby mode. After direct HA is enabled, the master device is working and responsible for forwarding packets, while the slave device is in standby 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 to detect whether the peer host is active.

To configure direct HA, follow these steps:

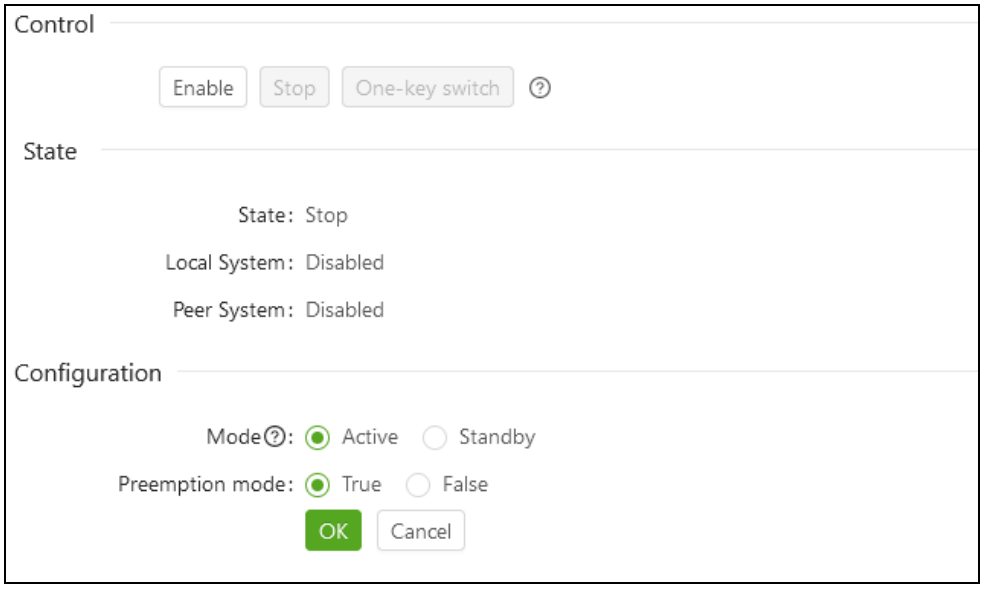
Step 1 Configure basic parameters of HA.

For details, see Basic Configuration.

Step 2 Configure direct HA parameters.

a. Choose **Network** > **HA** > **Direct Connect Configuration**.

Figure 8-15 Direct HA configuration parameters



b. Configure parameters.

Table 8-8 Direct HA configuration parameters

Parameter	Description
State	Indicates the working status of the local device, which can be **Running** or **Stop**. • **Running**: After direct HA is successfully enabled, the working status of the local device is displayed as **Running**. • **Stop**: When direct HA is stopped or not enabled, the working status of the local device is displayed as **Stop**.
Local/Peer System	Indicates the status of the local system, which can be **Activated**, **Unactivated**, or **Disabled**. Indicates the status of the peer system, which can be **Activated**, **Unactivated**, **Disabled**, or **Unknown**. • After direct HA is successfully enabled, if the local device is a master 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 direct HA is successfully enabled, if the local device is a slave in standby mode and can properly communicate with the heartbeat interface of the master device, the local system status is displayed as **Unactivated** and the peer system status as **Activated**. • After direct 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 direct HA is disabled, both the local system status and peer system status are displayed as **Off**.

Parameter	Description
Mode	Direct HA supports only the active/standby mode. • **Active**: The local device, after direct HA is enabled, works in active mode and is responsible for forwarding packets until the failover. • **Standby**: The local device, after direct HA is enabled, works in standby mode without forwarding data until the failover.
Preemption Mode	Controls whether to enable the preemption mode. • **True**: 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. • **False**: 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 the direct HA function.

a. Click **Enable** in the **Control** area.

b. In the confirmation dialog box, click **OK**.

----End

8.2.3 Asymmetric Routing

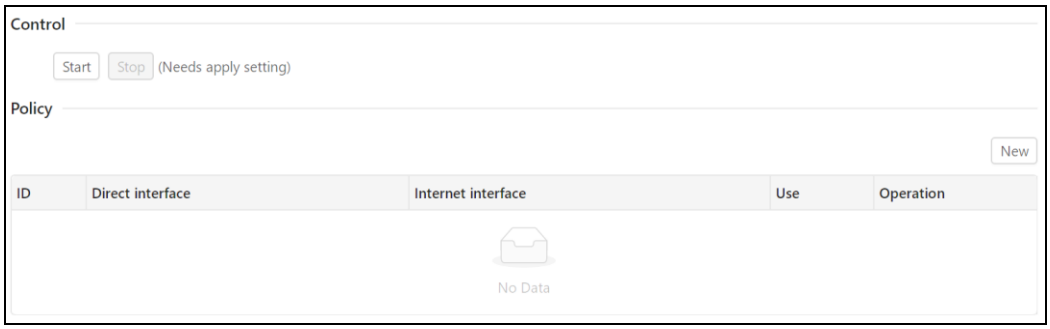
After asymmetric routing (ASR) support is enabled, NIPS devices in the ASR support group exchange packet transmission information. Based on such information, a transmitted packet can take a different path when it returns to the source. This allows the establishment of a complete data transmission session. In this manner, deep packet inspection (DPI) is conducted, with the data transmission path unchanged.

You can query, create, edit, and delete ARS policies.

To create an ASR policy, follow these steps:

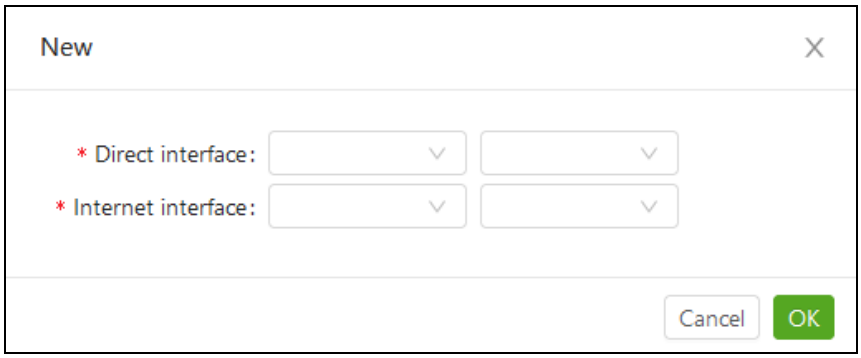
Step 1 Choose **Network** > **HA** > **Asymmetric Routing**.

Figure 8-16 Asymmetric routing configuration page



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

Figure 8-17 Creating an ASR policy



Step 3 In the dialog box, set the parameters.

Table 8-9 Parameters for configuring an ARS policy

Parameter	Description
Direct 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.
Internet interface	A pair of interfaces for forwarding connection information on the device.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.2.4 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.

In layer 3 HA mode, each device can be configured with multiple VRRP backup groups. In addition, interfaces with the same virtual router ID (VRID) on two devices will back up each other. 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.

You can configure layer 3 HA and edit and delete layer 3 HA lines.

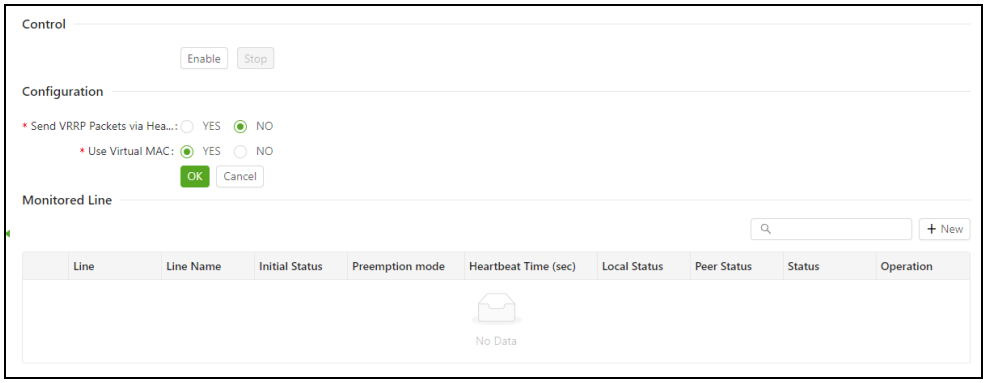
To configure layer 3 HA, follow these steps:

Step 1 Set public parameters of HA.

For details, see section Basic Configuration.

Step 2 Choose **Network > HA Settings > VRRP Configuration**.

Figure 8-18 VRRP Configuration page



Step 3 Configure VRRP configurations in the **Configuration** area.

Table 8-10 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 are sent through VRRP member interfaces. If you select **Yes**, VRRP packets are sent through the heartbeat interface.
Use Virtual MAC	Controls whether to use a virtual MAC address for sending VRRP packets. The default value is **Yes**, indicating that VRRP packets are sent by using a virtual MAC address, onto which IP addresses of virtual routers in a VRRP group are mapped. It is recommended that the default value be used.

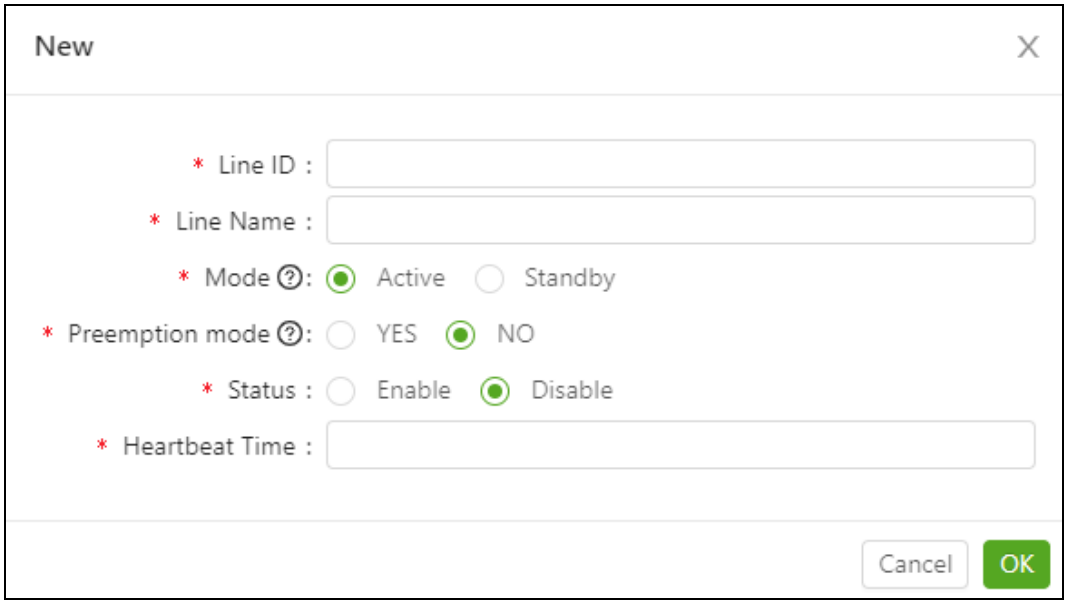
After parameters are set, click **OK** to save the settings.

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.

a. Click **New** in the upper-right corner of the **Monitored Line** area.

Figure 8-19 Creating a monitoring line



b. In the **New** dialog box, configure parameters.

Table 8-11 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.
Mode	Working mode of the new line. Layer 3 HA supports the active/active mode and active/standby mode. • **Active**: forwards packets until the failover after layer 3 HA is enabled. • **Standby**: remains in the standby state and does not forward data until the failover after layer 3 HA is enabled.
Preemption mode	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

Parameter	Description
	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.

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

Step 5 Configure interfaces for this line.

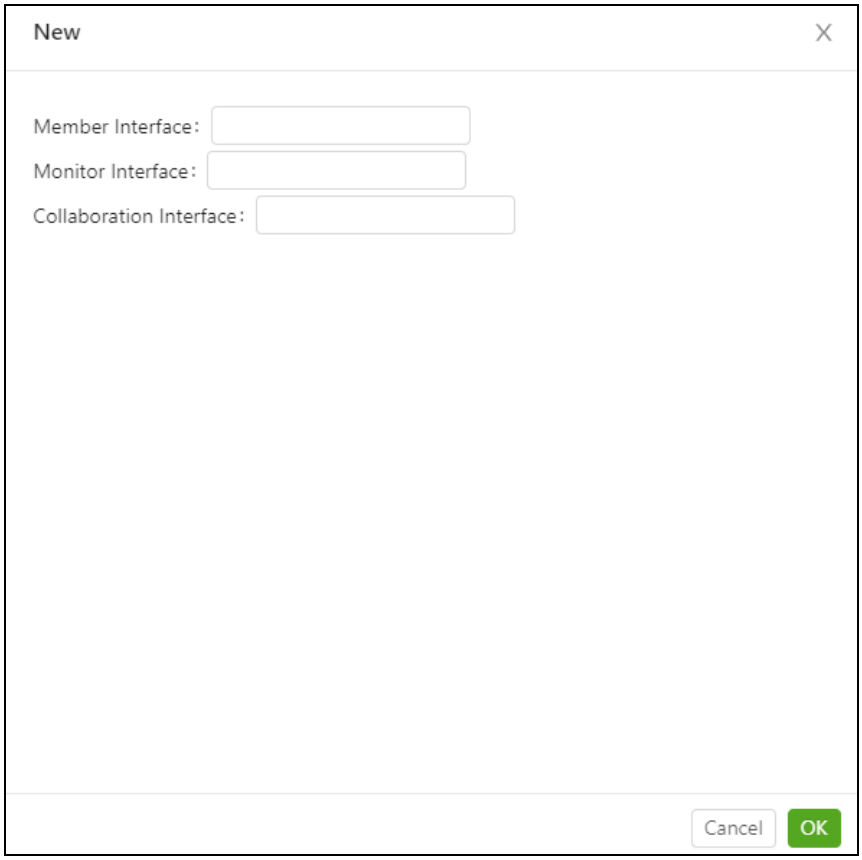
Interfaces of a monitoring line are divided into the following:

- **Member Interface**: As VRRP instances, such interfaces can be configured with virtual IP addresses. When one interface of the master line is down, the other interface in this line releases the virtual IP address 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 either of the monitoring interfaces 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.

Figure 8-20 Creating line interfaces



b. Configure parameters.

Table 8-12 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. The value is an integer ranging from 1 to 254. • 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.
	Priority	Specifies the priority of the layer 3 interface in the VRRP group. The value is an integer ranging from 1 to 254. A VRRP group selects 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

Parameter		Description
		slave device replaces it as the gateway, ensuring the continuous communication of the host with external networks. In each VRRP group, the device with a higher priority works as the master device to forward data, while that with a lower priority as the slave device working in monitoring mode.
	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	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 integer ranging from 0 to 254, is 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.

a. Click **Enable** in the **Control** area.

b. In the confirmation dialog box, click **OK**.

----End

8.2.5 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 back up 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 fewer 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.

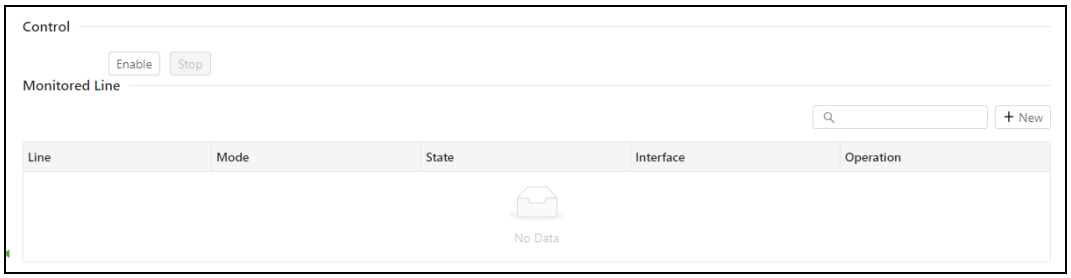
You can configure layer 2 HA parameters and enable or disable this function. To configure layer 2 HA, follow these steps:

Step 1 Set public parameters of HA.

For details, see section Basic Configuration.

Step 2 Choose **Network > HA Settings > Layer 2 Config**.

Figure 8-21 Layer 2 Config page



Step 3 Create a monitoring line.

Note	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 8-22 Creating a monitoring line

b. In the **New** dialog box, configure parameters.

Table 8-13 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. Layer 2 Ethernet interfaces or aggregation interfaces are supported. **Note** STP cannot be enabled on member interfaces for layer 2 HA.
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 **Enable** in the **Control** area.

b. In the confirmation dialog box, click **OK**.

----End

8.3 Bypass

The Bypass module consists of the following:

- External bypass
- Internal bypass
- Forcible internal bypass

Note	The internal bypass function works only when NIPS comes with a bypass card.

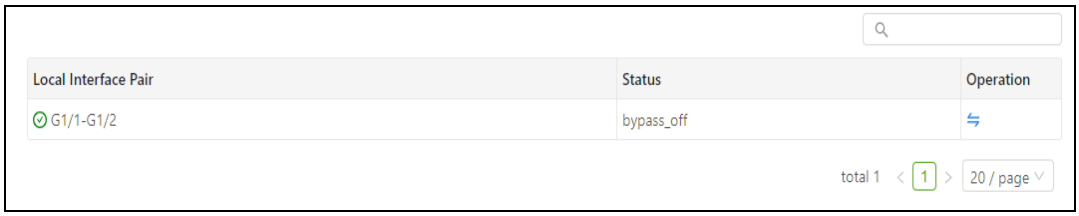
8.3.1 Internal Bypass

Internal 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.

Note	An NIPS device with a bypass card allows you to configure internal bypass on the web-based manager.

Step 1 Choose **Network** > **Bypass** > **Internal Bypass**.

Figure 8-23 Internal Bypass page



Step 2 View the **Status** column in the list for the status of the internal bypass, which has the following two values:

- **bypass_off**: The interface pair is in the normal state, and packets over the interface pair will be forwarded after being checked.
- **bypass_on**: The interface pair is in the bypass state, and packets over the interface pair will be forwarded without being checked.

Step 3 Click ⇆ in the **Operation** column to change the status of the related bypass interface pair.

Note	When the internal bypass status is changed, whether automatically or manually, the bypass indicator color changes as follows: • 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.

----End

8.3.2 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 and 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.

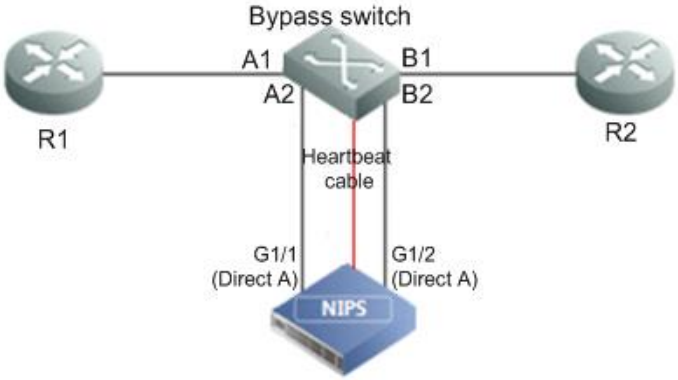
Take the topology in Figure 8-24 as an example. In this example, NIPS works properly and the bypass switch is in normal state. The route for traffic from R1 is as follows:

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 8-24 Topology for the collaboration between NIPS and the bypass switch



Note	After the external bypass feature is enabled, make sure that the out-of-band management interface of NIPS can properly communicate with the external bypass switch. For how to install and use the external bypass switch, refer to the *NSFOCUS Bypass Switch User Guide*.

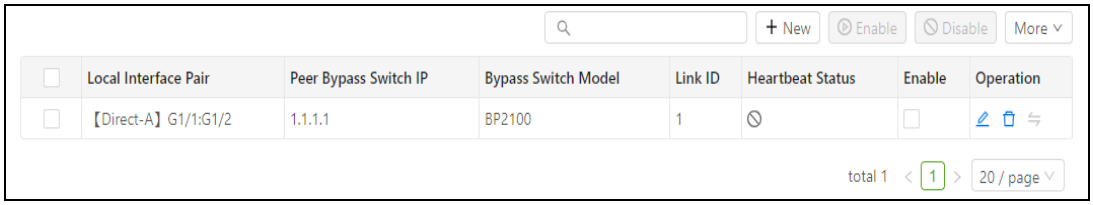
As **admin**, you can configure bypass interface pairs, including creating, deleting, modifying, enabling, and disabling such pairs, and manually switch the bypass status. The following sections describe how to create an external bypass interface pair and to manually switch the bypass status.

Creating an External Bypass Interface Pair

The procedure is as follows:

Step 1 Choose **Network** > **Bypass** > **External Bypass**.

Figure 8-25 External Bypass page



Step 2 In the upper-right corner of the page, click **New**.

Figure 8-26 Creating a bypass interface pair

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

Table 8-14 Parameters for configuring external bypass

Parameter	Description
Bypass Switch Model	Specifies a bypass switch model.
Peer Bypass Switch IP	Specifies the IP address of the bypass switch.
Password	Specifies the password for login to the bypass switch. This parameter is available only when you select **BP2100** for **Bypass Switch Model**.
Local Interface Pair	Specifies a pair of interfaces for NIPS to collaborate with the bypass switch.
Bypass Link ID	Specifies a link as required.

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

----End

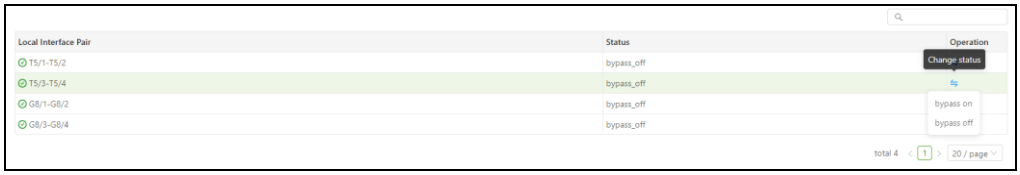
Manually Switching the Bypass Status

As **admin**, you can manually switch the current link to the bypass switch or switch back to NIPS.

The procedure is as follows:

Step 1 On the **External Bypass** page, point to ⇆ in the **Operation** column of a bypass interface pair to display status switching commands.

Figure 8-27 Manually switching the bypass status



Step 2 Select **bypass_off** or **bypass_on**.

- **bypass_off**: This is the default status of external bypass interface pairs. In this case, packets pass through and are handled by NIPS before being forwarded to the destination.
- **bypass_on**: When an external bypass interface pair is in this state, packets are forwarded to the specified bypass switch without passing through NIPS.

----End

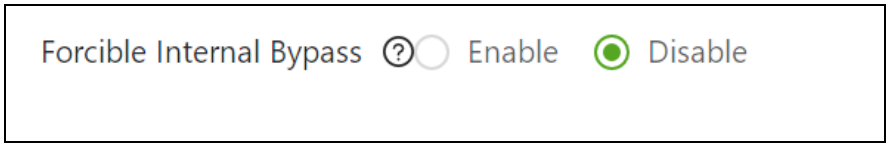
Note	Manual or automatic switching of the status of an external bypass will change bypass indicator status: • If the status is switched to **bypass-on**, the bypass indicator turns red. • If the status is switched to **bypass_off**, the bypass indicator turns green.

8.3.3 Forcible Internal Bypass

When **Forcible Internal Bypass** is enabled, NIPS will be forced to enter the bypass state. **Disable** indicates the opposite.

Step 1 Choose **Network** > **Bypass** > **Forcible Internal Bypass**.

Figure 8-28 Forcible internal bypass



Step 2 Select **Enable**, and you can enable the forcible internal bypass function.

At this time, all bypass cards will enter the bypass mode without affecting the work of non-bypass cards. In order to give priority to traffic continuity, the direct connect link traffic on bypass cards will be directly forwarded, without undergoing security inspection.

----End

8.4 Security Zones

A security zone is a collection of interfaces of the same type. Table 8-15 lists security zone types supported by NIPS.

Table 8-15 Security zone types

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.
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.
management	Security zone of the management type. Interfaces in such a security zone can be used for out-of-band or in-band management.
global	Default security zone, which cannot be edited and contains all security zones.
response	The system sends response packets via interfaces in such a security zone.

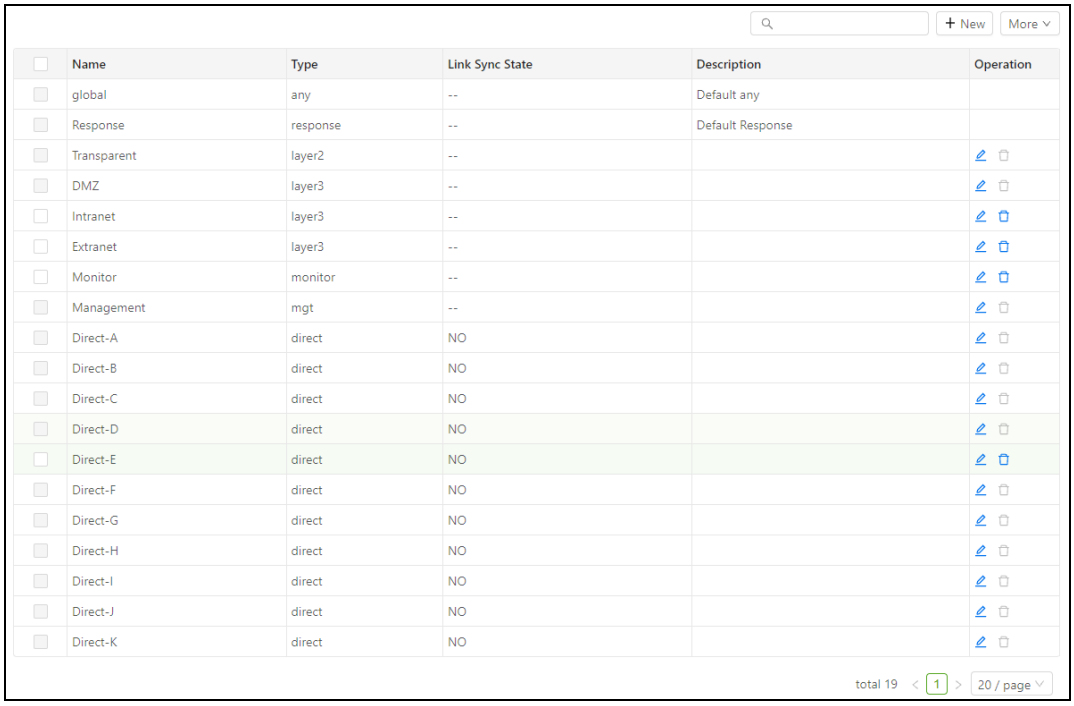
You can search for, create, edit, and delete security zones. In practice, you can move interfaces to other security zones except for the following interfaces.

Tip	Security zones cannot be changed for interfaces in the following cases: • Interfaces M and H1 • 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. • Non-Gigabit Intel NIC interface • Interfaces configured with routing policies • Interfaces configured with subinterfaces or referenced inpolicies.

To create a security zone, follow these steps:

Step 1 Choose **Network** > **Zones**.

Figure 8-29 Security zone list



Name	Type	Link Sync State	Description	Operation
global	any	--	Default any	
Response	response	--	Default Response	
Transparent	layer2	--		
DMZ	layer3	--		
Intranet	layer3	--		
Extranet	layer3	--		
Monitor	monitor	--		
Management	mgt	--		
Direct-A	direct	NO		
Direct-B	direct	NO		
Direct-C	direct	NO		
Direct-D	direct	NO		
Direct-E	direct	NO		
Direct-F	direct	NO		
Direct-G	direct	NO		
Direct-H	direct	NO		
Direct-I	direct	NO		
Direct-J	direct	NO		
Direct-K	direct	NO		

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

Figure 8-30 Creating a security zone

Step 3 Configure security zone parameters.

Table 8-16 Security zone parameters

Parameter	Description
Name	Unique name of the security zone. It is case-sensitive and cannot contain the following special characters: / % \ { } `

Parameter	Description
	^ < > ' & " :
Type	Specifies the work type of the security zone.
Description	Descriptive information of the security zone.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.5 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 SNMP v3, and is compatible with SNMP v1 and SNMP v2c. When conducting network query on NIPS via SNMP v1 or SNMP v2c, 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 SNMP v3, 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.

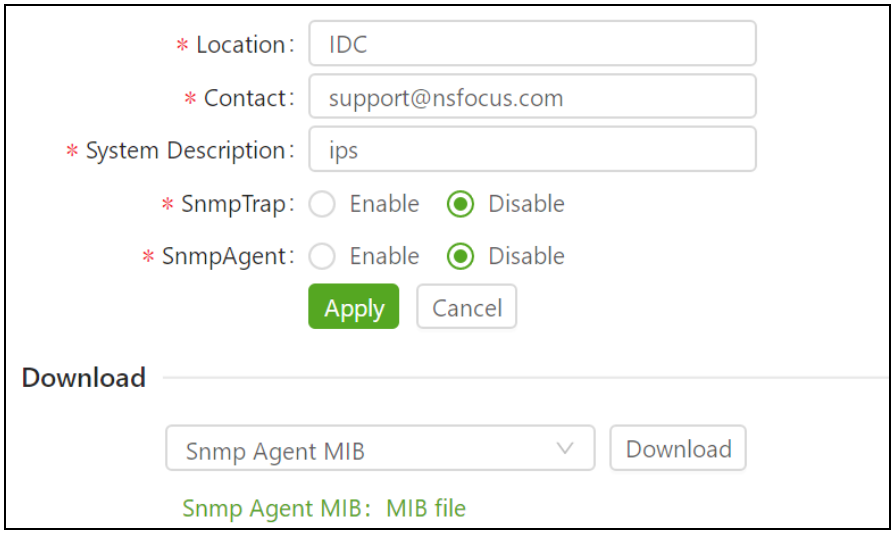
NIPS supports mainstream SNMP management software, such as MIB Browser and Solarwinds.

8.5.1 System Setting Information

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

Step 1 Choose **Network > SNMP > Setting**.

Figure 8-31 SNMP setting page



Step 2 Configure parameters.

Table 8-17 SNMP setting parameters

Parameter	Description
Location	Specifies the location of NIPS in the network environment.
Contact	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, settings configured in Trap take effect.
SnmpAgent	Controls whether to enable NIPS to accept management from the SNMP manager. After it is enabled, settings configured in Agent Access Control take effect.

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

----End

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

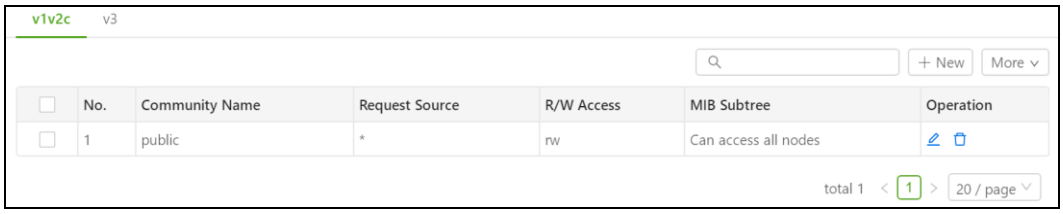
8.5.2 Agent Access Control

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 System Setting Information.

To configure agent access control parameters, follow these steps:

Step 1 Choose **Network** > **SNMP** > **Agent**.

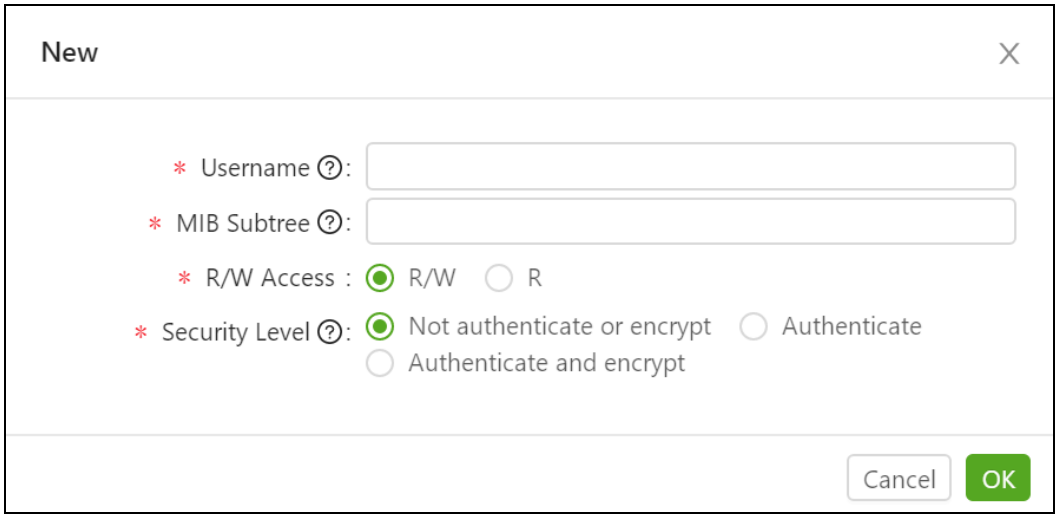
Figure 8-32 SNMP Agent page



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

Figure 8-33 Configuring agent access control – SNMP v1 and v2c

Figure 8-34 Configuring agent access control – SNMP v3



Step 3 Configure parameters.

Table 8-18 Parameters for configuring agent access control (SNMP v1 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 OID. **1** indicates access permissions to all nodes. You can type other values such as **1.3.6.1.4.1.19849.2**.
R/W Access	Specifies the SNMP manager's permissions to the MIB subtree on NIPS, which can be **R/W** or **R**.

Table 8-19 Parameters for configuring agent access control (SNMP v3)

Parameter	Description
Username	Specifies the SNMP v3 user name.
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**.
R/W Access	Specifies the SNMP manager's permissions to the MIB subtree on NIPS, which can be **R/W** or **R**.
Security Level	Specifies the minimum security level for a user's access, which can be **Not authenticate or encrypt**, **Authenticate**, or **Authenticate and encrypt**.
Authentication	Specifies the protocol used for authentication, which can be **MD5** or **SHA**.

Parameter	Description
Protocol	
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.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.5.3 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 System Setting Information. To configure SNMP trap parameters, follow these steps:

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

Figure 8-35 SNMP Trap

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

Figure 8-36 Configuring SNMP v1/v2c trap

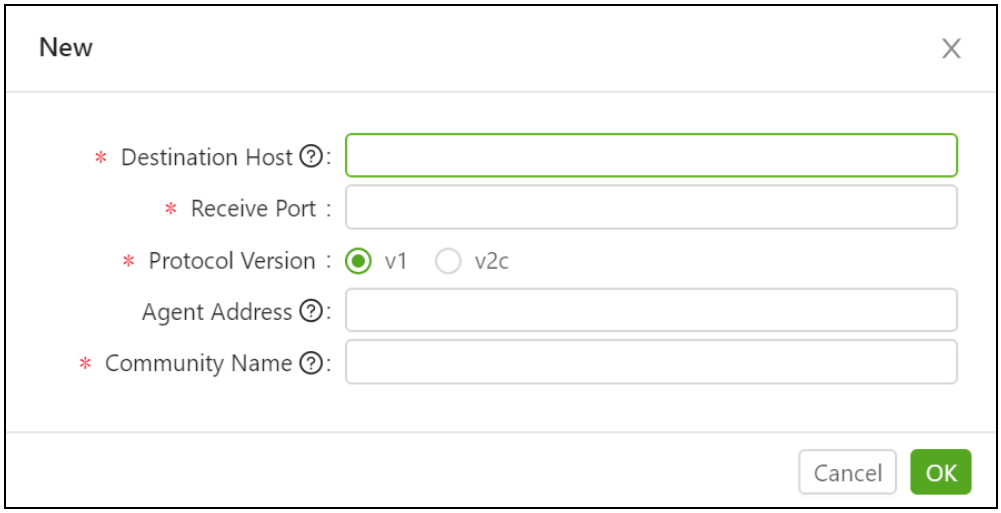
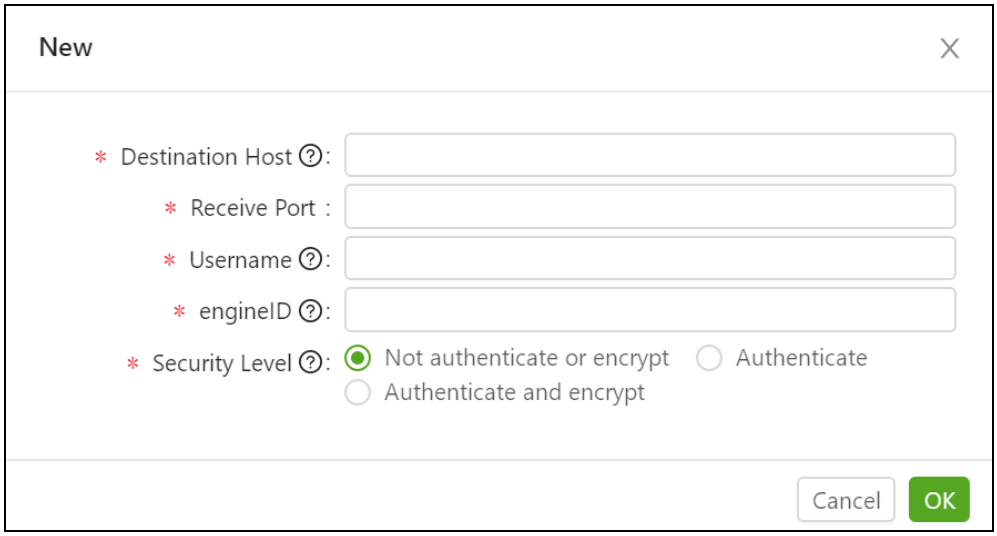


Figure 8-37 Configuring SNMP v3 trap



Step 3 Configure SNMP trap parameters.

Table 8-20 Parameters for configuring SNMP v1/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::**.
Receive 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 8-21 Parameters for configuring SNMP v3 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::**.
Receive Port	Specifies the port for receiving SNMP trap alerts.
Username	Specifies the SNMP v3 user name.
engineID	Specifies the ID of the SNMP engine. The ID is a 16-bit string of hexadecimal characters, for example, 0x8000000001020304.
Security Level	Specifies the minimum security level for a user's access, which can be **Not authenticate or encrypt**, **Authenticate**, or **Authenticate and encrypt**.
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.

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

----End

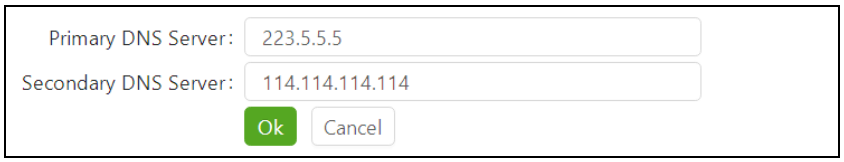
8.6 DNS

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**.

Figure 8-38 Configuring DNS servers



Step 2 Specify IP addresses of the DNS servers.

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

----End

8.7 Exchange

NIPS provides the following layer 2 exchange functions:

- MAC table: allows you to configure rules for forwarding layer 2 packets based on VLAN IDs and MAC addresses.
- RSTP: allows you to configure the Rapid Spanning Tree Protocol (RSTP) on NIPS.
- MSTP: allows you to configure the Multiple Spanning Tree Protocol (MSTP) on NIPS.

8.7.1 MAC Table

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 either of 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 passes 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.

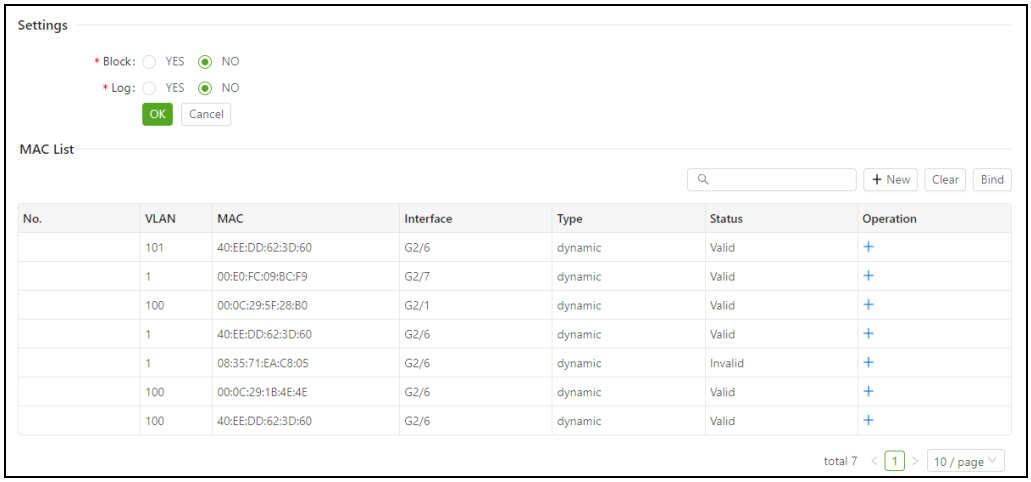
  - If yes, NIPS will forward the packets via the interface configured in the static MAC entry.
  - If no, NIPS will block or forward the packets as configured in the policy.

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 8-39 MAC table



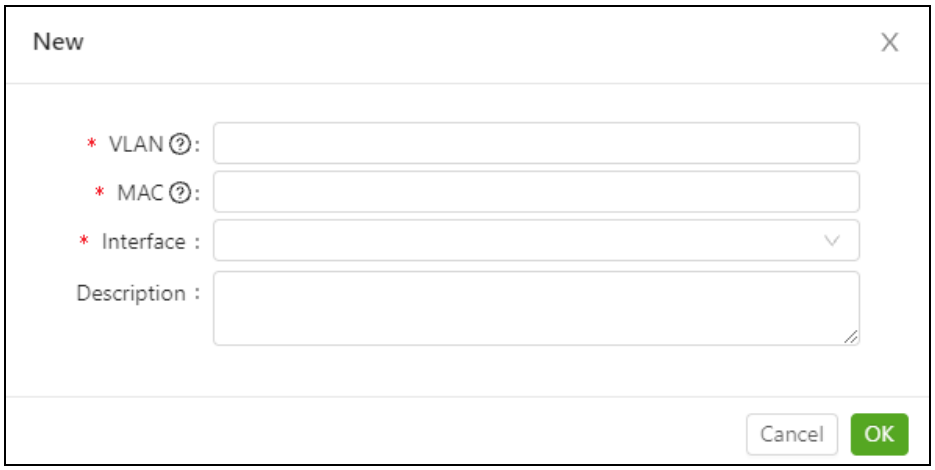
Step 2 Configure parameters.

- **Block**: controls whether NIPS blocks packets that do not match a static MAC entry.
- **Log**: controls whether NIPS logs the situation where packets match the VLAN and MAC address of a staic MAC entry but are fowarded through another interface.

Step 3 Create a static MAC entry.

a. Click **New** in the upper-right of the MAC list.

Figure 8-40 Creating a VLAN/MAC binding



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

Table 8-22 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

Parameter	Description
	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 8.8.3 ARP Table.

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.7.2 RSTP Configuration

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

8.7.2.1 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 when 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.

The 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 designated port, 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.

8.7.2.2 Configuring RSTP

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:

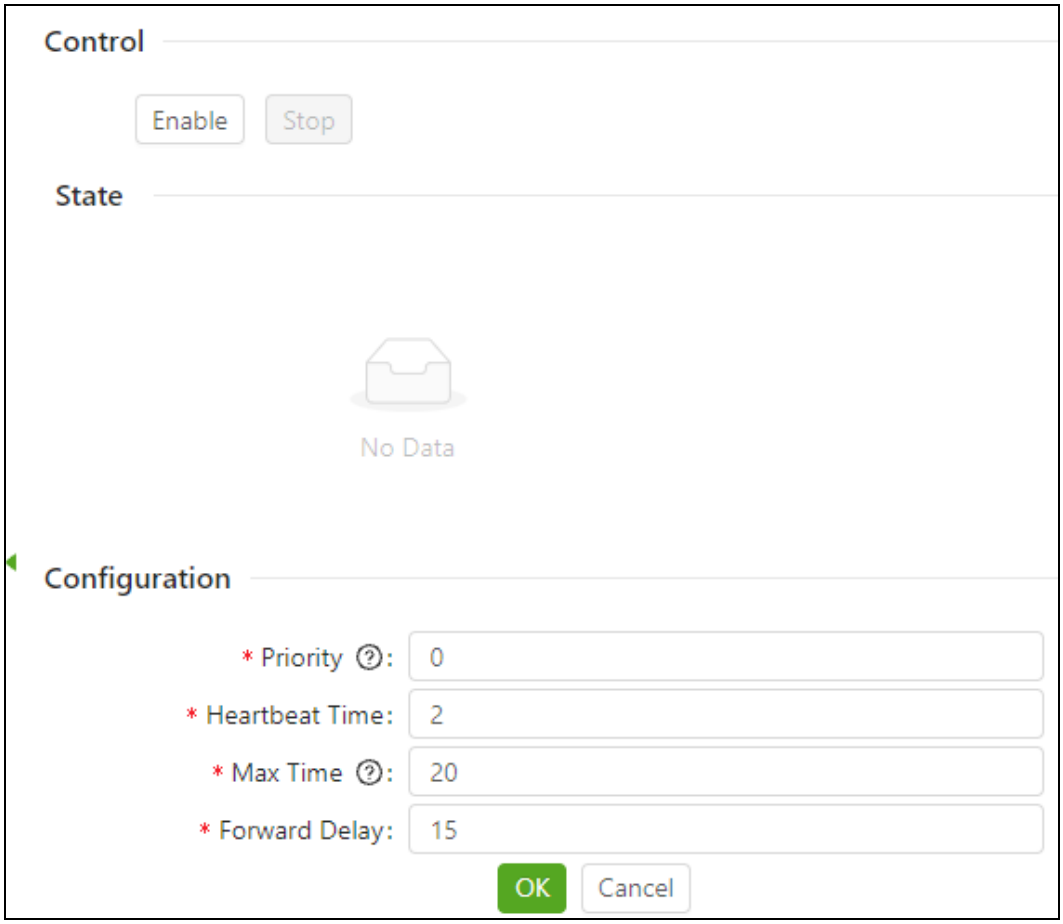
Step 1 Configure interfaces and enable the RSTP function on them.

On NIPS, configure at least one 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 8-41 RSTP page



b. Configure parameters.

Table 8-23 RSTP configuration parameters

Parameter	Description
State	Specifies 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 addresses and can send, receive, and handle configuration messages. • **Forwarding**: The port can forward data, learn addresses, and send, receive, and handle configuration messages.
Priority	Specifies the RSTP priority. It must be an integer multiple of 4096. The value range is

Parameter	Description
	0–61440.
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 Time	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. The maximum time must be smaller than 2 x (Forward Delay – 1), and no smaller than 2 x (Heartbeat Time + 1)
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 8-41, click **Enable** in the **Control** area and click **OK** in the confirmation dialog box.

Step 4 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.7.3 MSTP Configuration

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, and 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.

8.7.3.1 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 (STIs) 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.

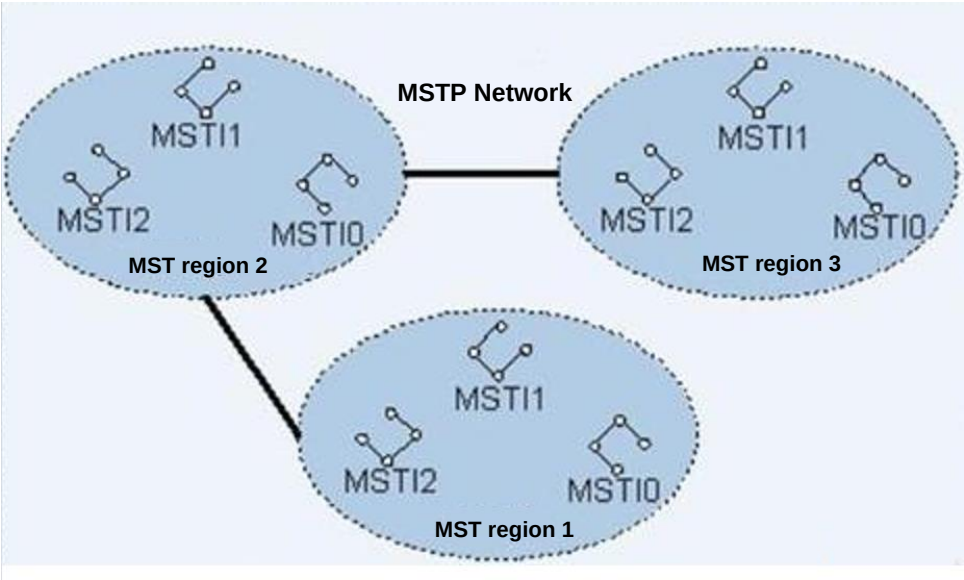
On the whole, an MSTP network has three tiers:

- 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 8-42 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.
- They 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 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. Common Spanning Tree

Common Spanning Tree (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

Internal Spanning Tree (IST) is a spanning tree within an MST region. The IST and CST constitute the CIST of the entire switching 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. Common and Internal Spanning Tree

Common and Internal Spanning Tree (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 several 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 on the network may receive configuration information with a higher priority. This may cause the current root bridge to lose its status, 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.

8.7.3.2 Configuring MSTP

The MSTP configuration roadmap 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.

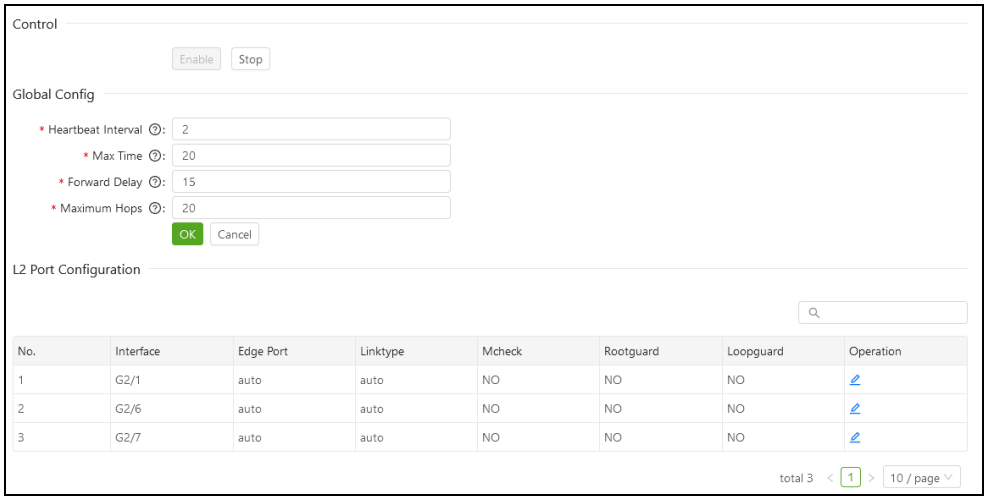
To configure the MSTP function, follow these steps:

Step 1 Configure interfaces.

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.

Step 2 Choose **Network** > **Exchange** > **MSTP**.

Figure 8-43 MSTP page



Step 3 Configure global parameters.

Table 8-24 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.
Max Time	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. The value ranges from 1 to 40, with **20** 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 exceeding 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.

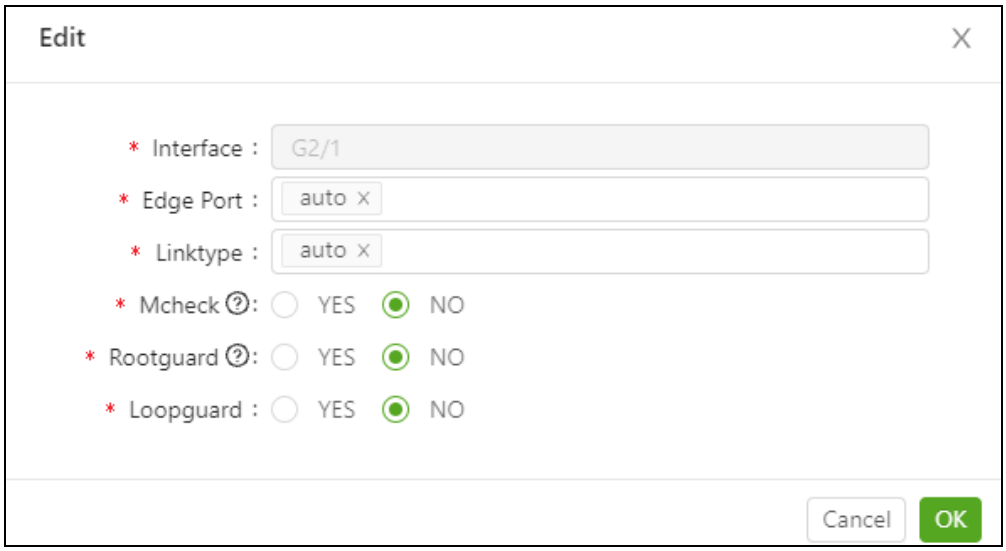
Click **OK** to save the settings.

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 8-44 Configuring layer 2 port parameters



b. Configure parameters.

Table 8-25 Parameters related to a layer 2 port

Parameter	Description
Edge Port	Controls whether this interface is an edge port. This interface is regarded as an edge 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 shared type. **auto** is the default value. • **point-to-point**: indicates that the interface link is in of the point-to-point type. • **shared**: indicates that the interface link is of the shared 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-compatible 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

Parameter	Description
	operates in the STP-compatible mode. In 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 8-45 Initial instance configuration

Caution	For instance 0, **Instance Name** indicates the MST region to which it belongs; for other instances, **Instance Name** has no practical meaning.

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 8-46 Creating an MST instance.

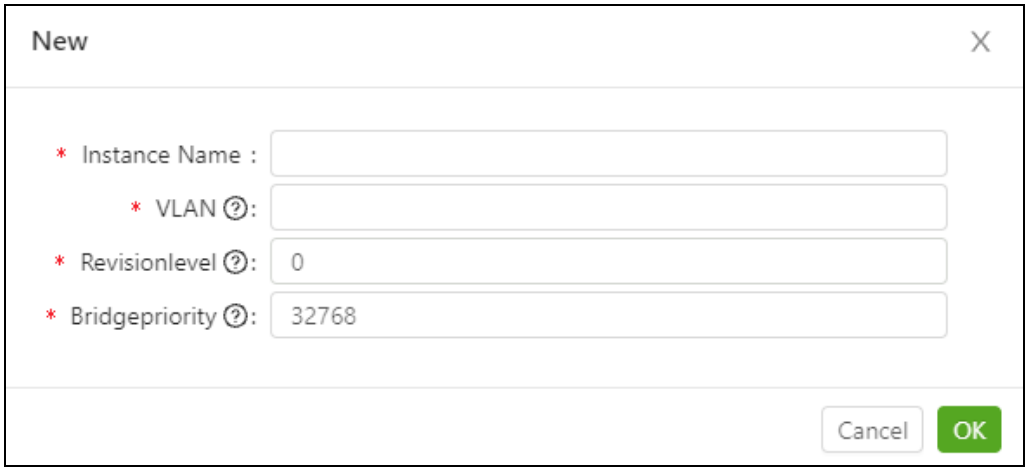


Table 8-26 describes parameters for creating an MST instance.

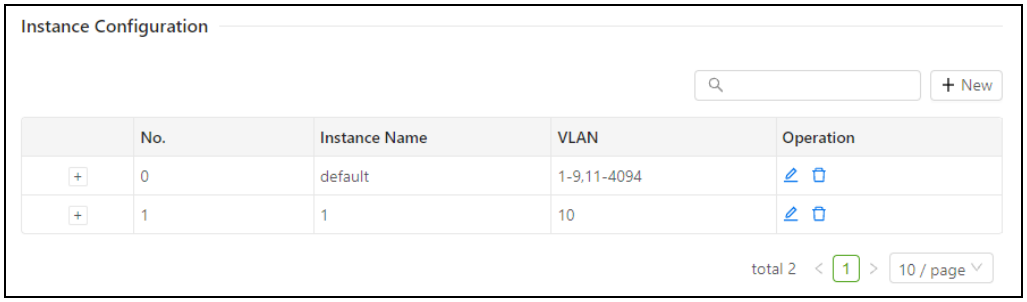
Table 8-26 Parameters for creating an MST instance

Parameter	Description
Instance Name	For instances other 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 of the VLAN mapped to this instance. The value can be integers or a specific range. Multiple VLAN IDs are separated by the comma (,), for example, 1,3-100. One VLAN can map to only one instance. After a VLAN ID is assigned to a new instance, it no longer maps to instance 0.
Revisionlevel	Revision level of an MST region. The value is an integer in the range of 0–65535. 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 an integer in 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 8-47.

Figure 8-47 Instance list after a new instance is created

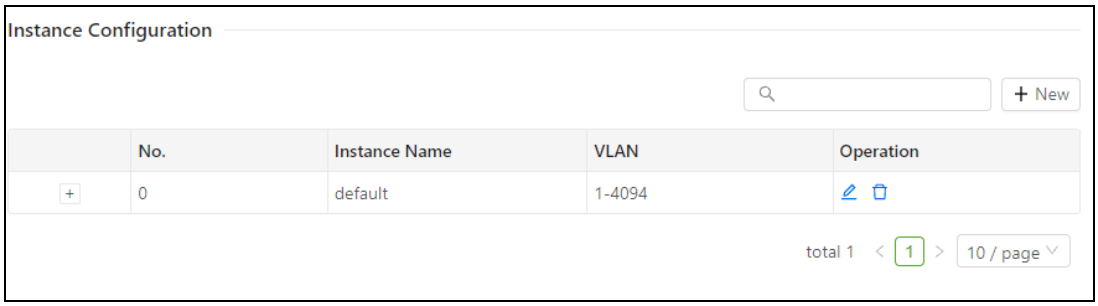


c. Delete an instance.

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 8-47 is deleted, the VLAN assigned to it is remapped to instance 0.

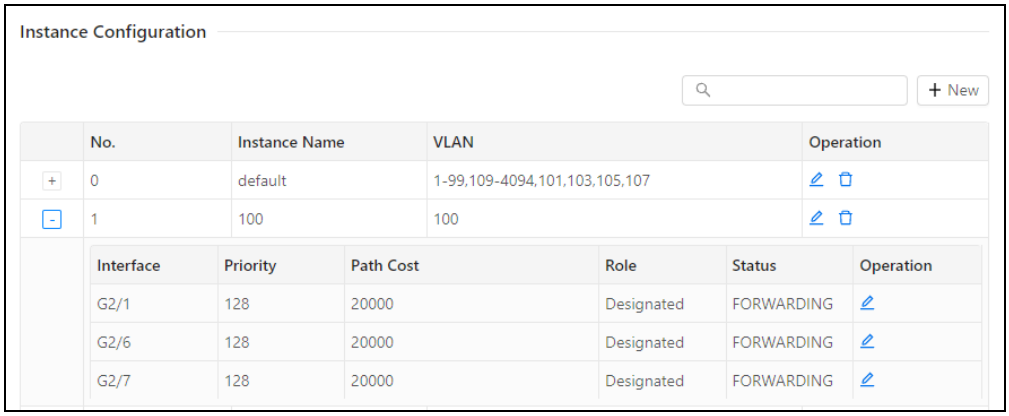
Figure 8-48 Instance list after an instance is deleted



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 8-49 Viewing layer 2 interfaces configured for an instance



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

Figure 8-50 Editing MSTP parameter settings of an interface

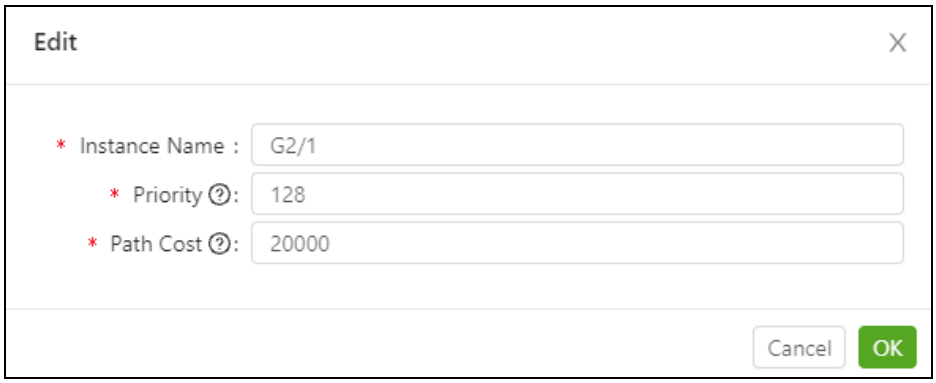


Table 8-27 describes MSTP parameters of an interface.

Table 8-27 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 8-43, click **Enable** and then click **OK** in the confirmation dialog box.

Step 7 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.8 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, priority, 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. 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

Priority

It is an integer from 1 to 65535. A route with a smaller priority value is more reliable. The priority allows a router to select the best path as follows: When receiving information about several matching routes of different protocols, the router will check their prioritities, select the route with the smallest value as the trustworthy one, and insert it into the router's routing table for packet forwarding.

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. **Minimum priority value**: If the routes have the same subnet mask, the router selects the route with the smallest priority value.

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

8.8.1 Static Route

A static route is a route manually configured by the administrator. Such routes are used for small-scale networks that do not frequently change. As static routes are not 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, search for, import, export, delete, and clear static routes.

To create a static route, follow these steps:

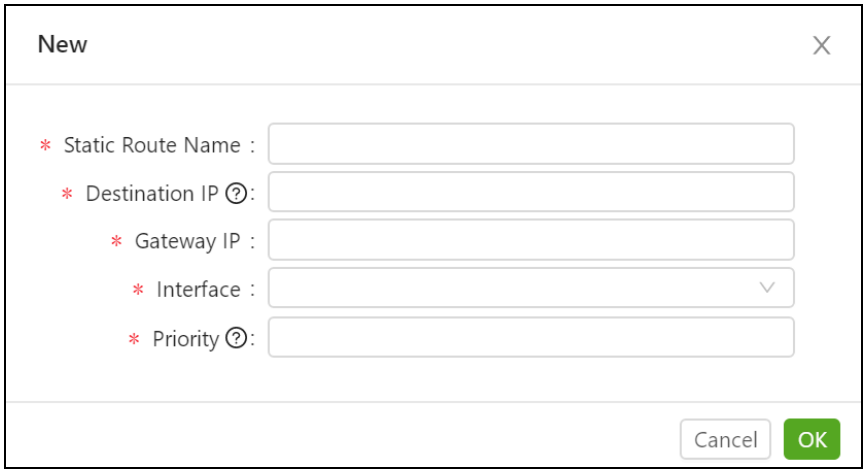
Step 1 Choose **Network** > **Route** > **Static Route**.

The static route page appears, as shown in Figure 8-51.

Figure 8-51 Static route page

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

Figure 8-52 Creating a static route



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

Table 8-28 Parameters for configuring a static route

Parameter	Description
Static Route Name	Specifies the name of the static route, which cannot contain 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 ingress IP address of the next-hop device.
Interface	Specifies the egress interface of the static route.
Priority	Specifies the priority of the static route. The value range is 1–65535. A smaller value indicates a higher priority.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.8.2 Policy Routing

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.

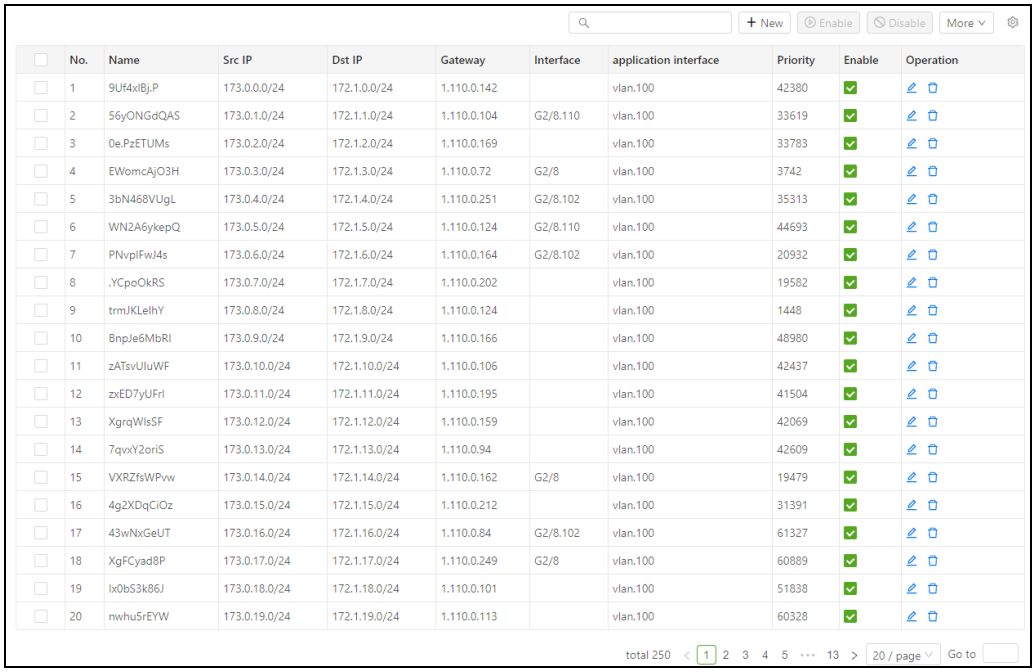
PBR routes takes precedence over other routes. That is to say, NIPS matches the received packets against PBR routes first. If no matching PBR route is found, NIPS searches for a static route for packet forwarding.

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**.

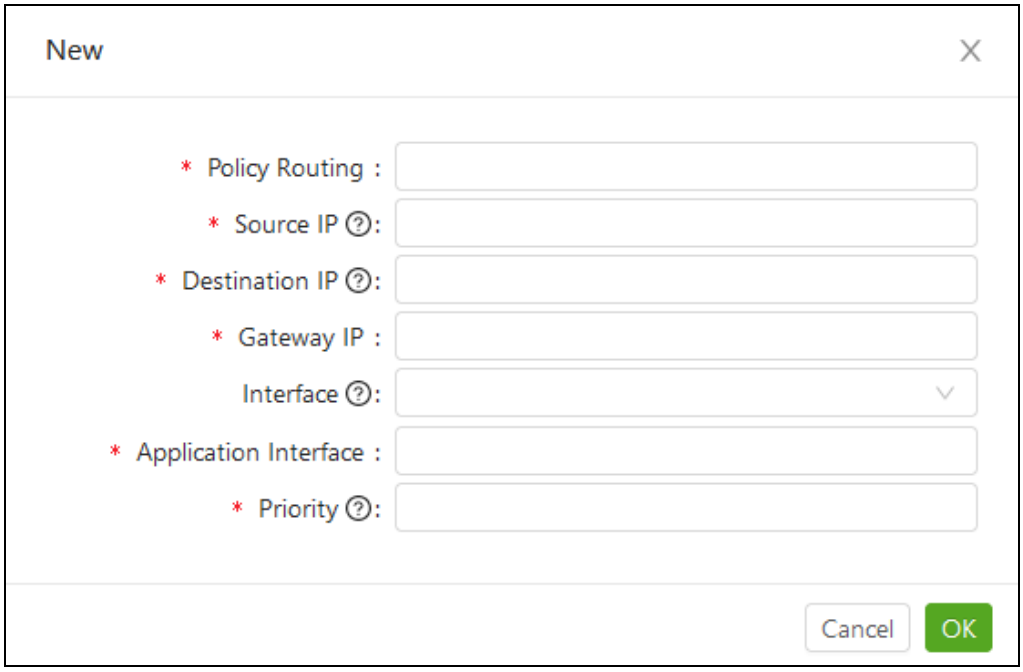
Figure 8-53 Policy-based routing page



No.	Name	Src IP	Dst IP	Gateway	Interface	application interface	Priority	Enable	Operation
1	9Uf4xlBj.P	173.0.0.0/24	172.1.0.0/24	1.110.0.142		vlan.100	42380	✓	
2	56yONGdQAS	173.0.1.0/24	172.1.1.0/24	1.110.0.104	G2/8.110	vlan.100	33619	✓	
3	0e.PzETUMs	173.0.2.0/24	172.1.2.0/24	1.110.0.169		vlan.100	33783	✓	
4	EWomcAjO3H	173.0.3.0/24	172.1.3.0/24	1.110.0.72	G2/8	vlan.100	3742	✓	
5	3bN468VUgL	173.0.4.0/24	172.1.4.0/24	1.110.0.251	G2/8.102	vlan.100	35313	✓	
6	WN2A6ykepQ	173.0.5.0/24	172.1.5.0/24	1.110.0.124	G2/8.110	vlan.100	44693	✓	
7	PNvplFwJ4s	173.0.6.0/24	172.1.6.0/24	1.110.0.164	G2/8.102	vlan.100	20932	✓	
8	.YCpoOkRS	173.0.7.0/24	172.1.7.0/24	1.110.0.202		vlan.100	19582	✓	
9	trmJKLelhY	173.0.8.0/24	172.1.8.0/24	1.110.0.124		vlan.100	1448	✓	
10	BnpJe6MbRI	173.0.9.0/24	172.1.9.0/24	1.110.0.166		vlan.100	48980	✓	
11	zATsvUIuWF	173.0.10.0/24	172.1.10.0/24	1.110.0.106		vlan.100	42437	✓	
12	zxED7yUFrl	173.0.11.0/24	172.1.11.0/24	1.110.0.195		vlan.100	41504	✓	
13	XgrqWlsSF	173.0.12.0/24	172.1.12.0/24	1.110.0.159		vlan.100	42069	✓	
14	7qvxY2oriS	173.0.13.0/24	172.1.13.0/24	1.110.0.94		vlan.100	42609	✓	
15	VXRZfsWPvw	173.0.14.0/24	172.1.14.0/24	1.110.0.162	G2/8	vlan.100	19479	✓	
16	4g2XDqCiOz	173.0.15.0/24	172.1.15.0/24	1.110.0.212		vlan.100	31391	✓	
17	43wNxGeUT	173.0.16.0/24	172.1.16.0/24	1.110.0.84	G2/8.102	vlan.100	61327	✓	
18	XgFCyad8P	173.0.17.0/24	172.1.17.0/24	1.110.0.249	G2/8	vlan.100	60889	✓	
19	lx0bS3k86J	173.0.18.0/24	172.1.18.0/24	1.110.0.101		vlan.100	51838	✓	
20	nwhu5rEYW	173.0.19.0/24	172.1.19.0/24	1.110.0.113		vlan.100	60328	✓	

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

Figure 8-54 Creating a policy-based route



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

Table 8-29 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.
Interface	Specifies the outbound interface from which packets are sent. It can be a layer 3 interface. The security zone of the interface available with routing policies must work in layer 3 or management mode.
Application Interface	Specifies the interface to which the policy-based routing applies.
Priority	Specifies the priority of the policy-based routing. The value range is 1–65535. A smaller value indicates a higher priority.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

8.8.3 ARP Table

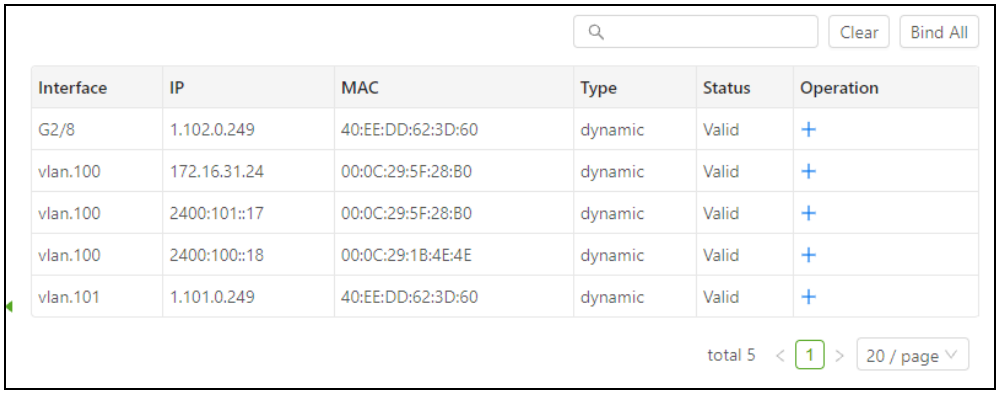
Address Resolution Protocol (ARP) is a protocol for resolution of IP addresses on the network layer into MAC addresses on the data link layer. The ARP table records one-to-one mappings between IP addresses and MAC addresses, offering guidance for layer 3 packet forwarding.

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.

Viewing ARP Entries

To view ARP entries learned by NIPS, choose **Network** > **Route** > **ARP Table**.

Figure 8-55 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.

Searching for ARP Entries

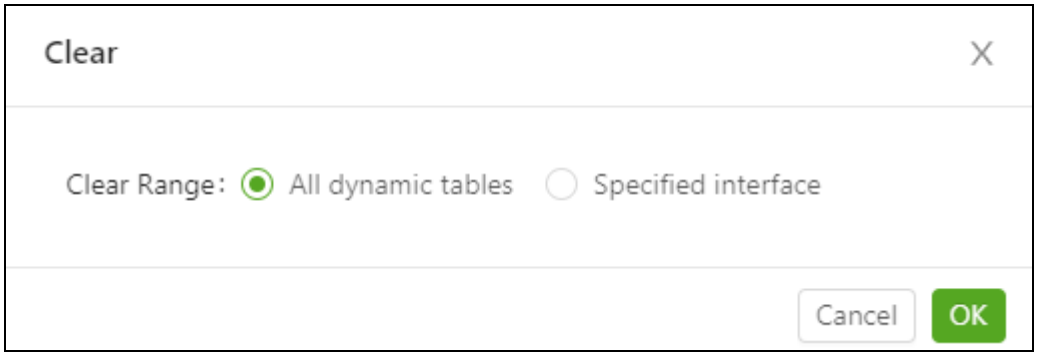
If these are many ARP entries in the ARP table shown in Figure 8-55, you can search for desired entries according to the IP address, MAC address, type, or status of entries.

In the upper right of the ARP table shown in Figure 8-55, you can type a specific search condition in the text box, and click 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 8-55, 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 8-56 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 **Policy** > **IP/MAC Binding**. For details, see section 6.8 IP/MAC Binding.

On the ARP table shown in Figure 8-55, you can click + in the **Operation** table to configure an ARP entry as an IP/MAC binding entry.

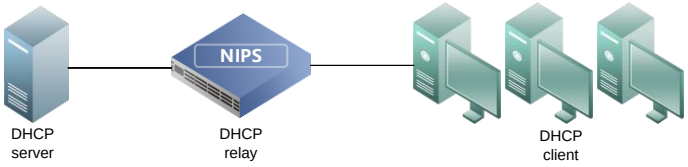
Also, you can click **Bind All** in the upper right of the ARP table to configure all qualified dynamic ARP entries as IP/MAC binding entries.

8.9 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 forward such information to DHCP clients in any security zones.

Figure 8-57 shows the topology when NIPS works as a DHCP relay agent.

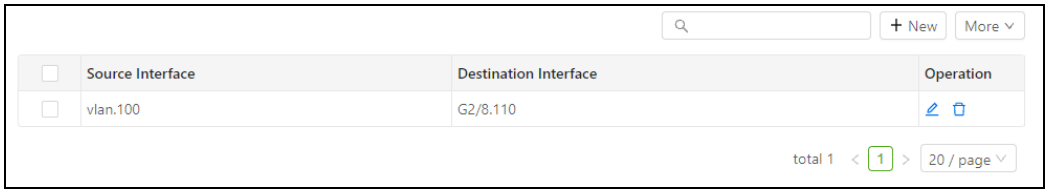
Figure 8-57 Topology in which NIPS acts as a DHCP relay



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**.

Figure 8-58 DHCP relay list



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

Figure 8-59 Creating a DHCP relay

Step 3 Configure parameters.

Table 8-30 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 Click **Commit** in the quick access bar to make the settings take effect.

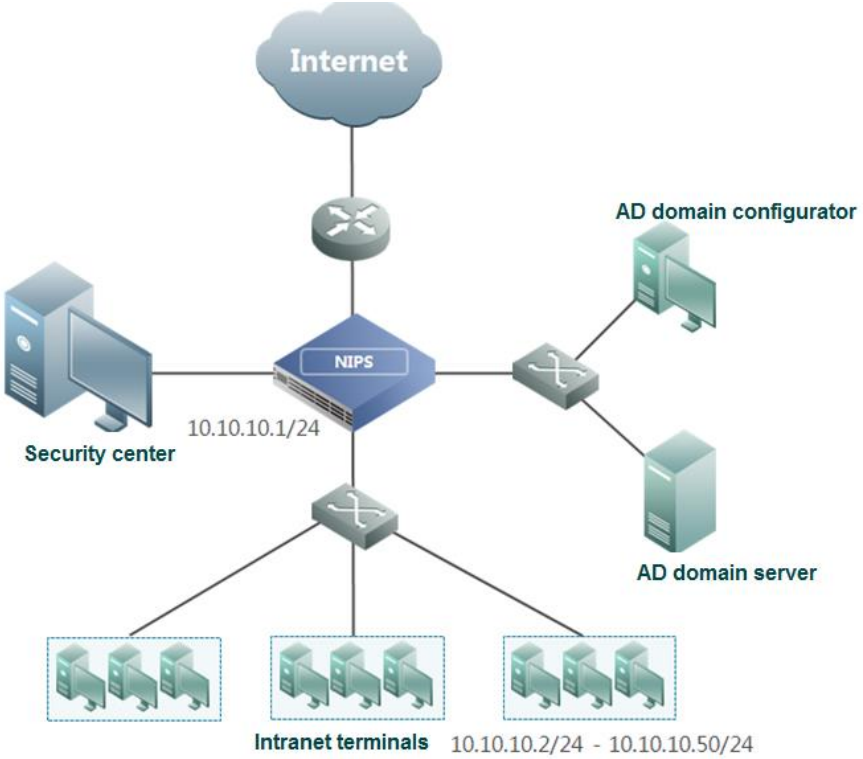
----End

8.10 Authentication Server

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 8-60 shows the network topology for this type of authentication.

Figure 8-60 Network topology for AD domain authentication



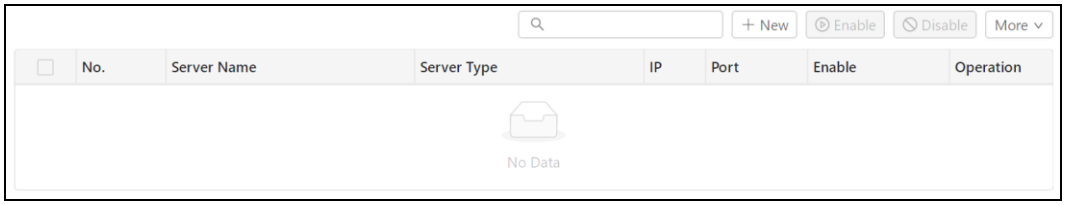
To use AD domain authentication, you must have configured the AD domain configurator to manage user information obtained from the domain controller. For details, see B AD Domain Configurator Management. Then configure the following on NIPS:

- AD domain server
- Method of updating the user list on the AD domain server (see Users in AD).

To configure authentication servers on NIPS, follow these steps:

Step 1 Log in as **admin** and choose **Network** > **Authentication Server**.

Figure 8-61 Server configuration page



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

Parameters in the **New** dialog box vary with the type of authentication servers. Figure 8-62 shows the dialog box for configuring an AD domain server. Figure 8-63 shows the dialog box for configuring a Radius server. Figure 8-64 shows the dialog box for configuring an LDAP server.

Figure 8-62 Configuring an AD domain server

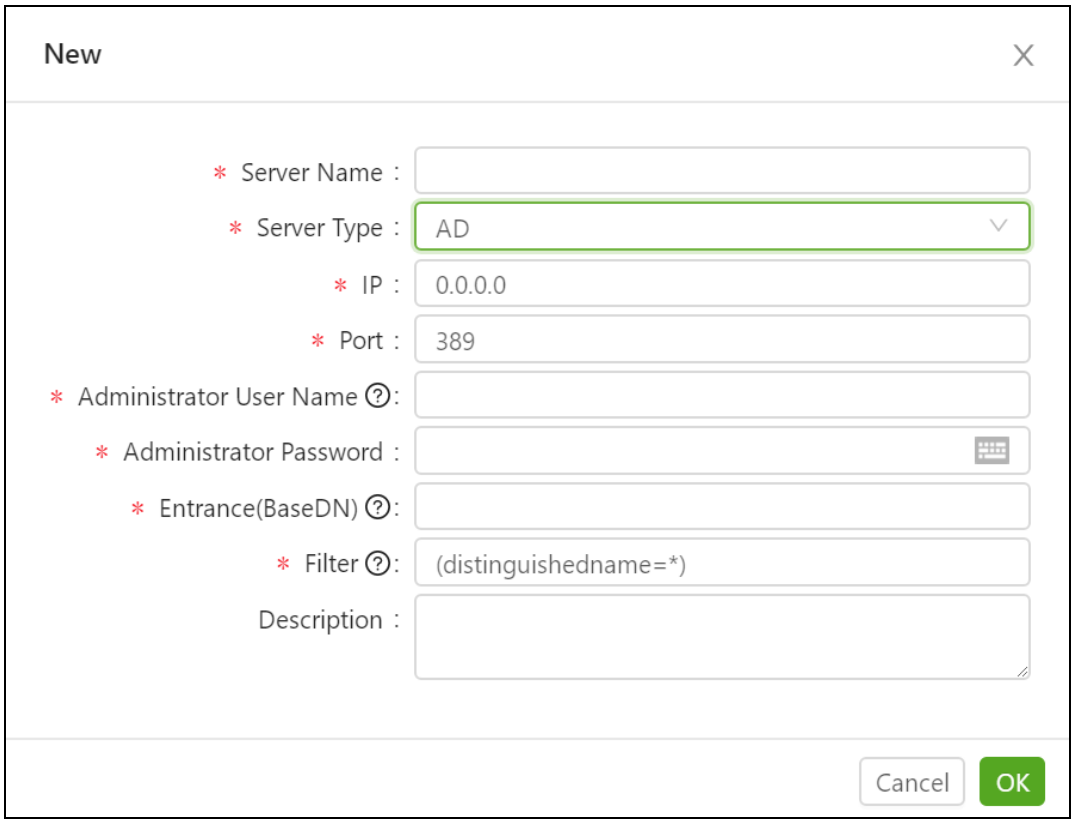


Figure 8-63 Configuring a Radius server

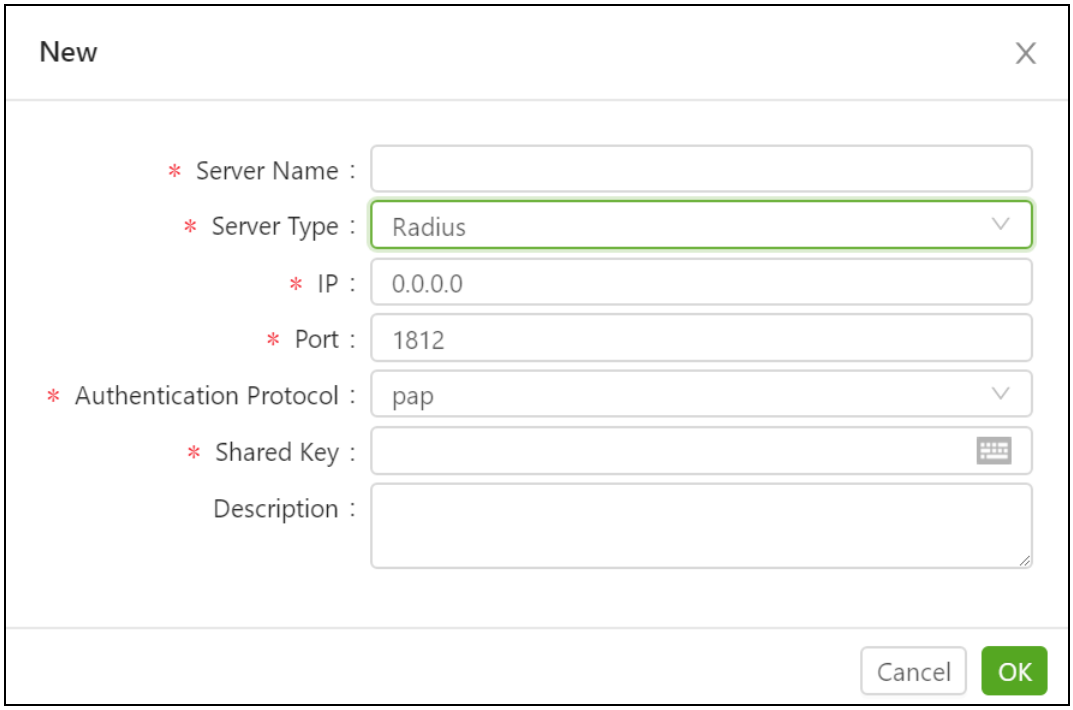
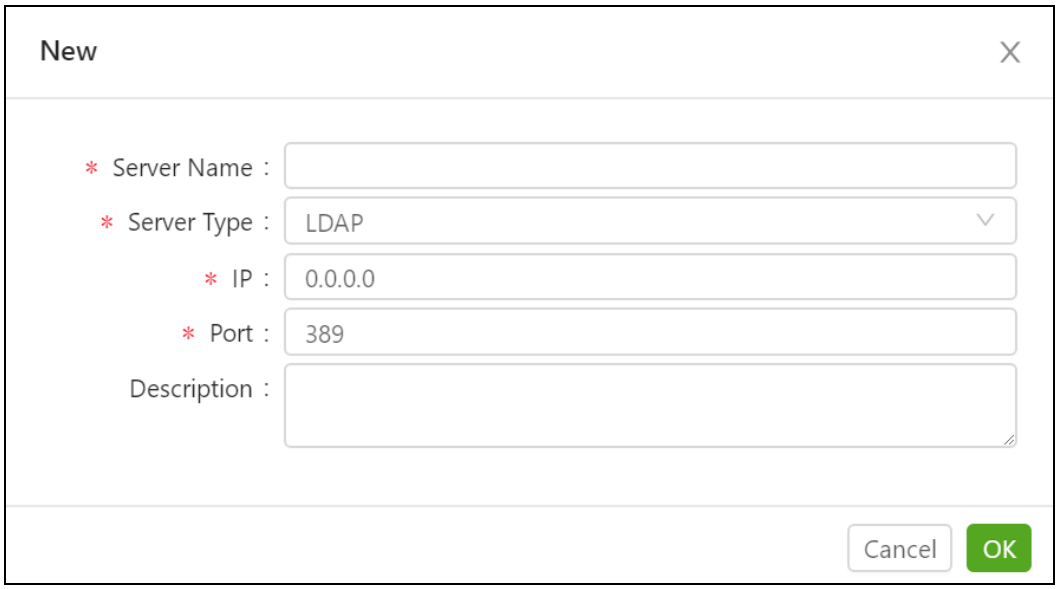


Figure 8-64 Configuring an LDAP server



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

Table 8-31 Parameters for configuring authentication servers

Parameter	Description
Server Name	Specifies the name of the authentication server.

Parameter	Description
	The server name must be unique. It is a string that cannot contain 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. • **LDAP**: indicates a server for LDAP authentication.
IP/Port	Specifies the IP address and port of an authentication server.
Administrator User Name/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.
Entrance (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 Protocol	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.
Shared Key	Specifies the shared key that serves as a password between the Radius server and a Radius client. Note • The shared key 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.

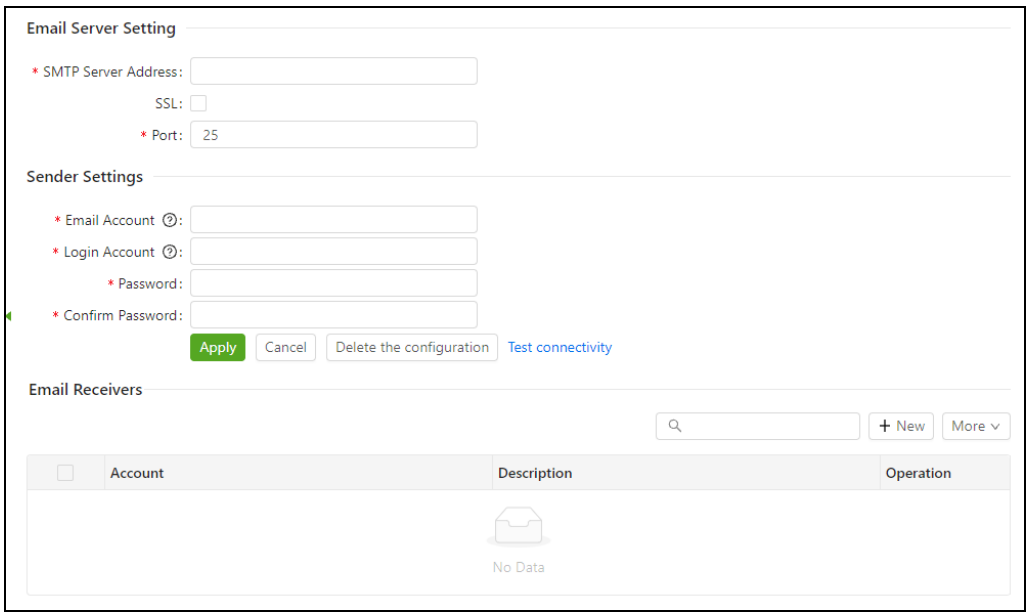
Step 4 Click **OK** to save the settings.

----End

8.11 Mail Server

Step 1 Choose **Network** > **Mail Server**.

Figure 8-65 Email server



Step 2 Configure mail server parameters, including the server address, whether to use the SSL protocol to send a mail, and the number of the sending port.

Step 3 Configure sender settings, including the email account, the login account, and password (which needs to be typed again for confirmation).

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

Step 5 Configure at least one receiver below **Email Receivers**.

a. Click **New** in the **Email Receivers** area.

Figure 8-66 Configuring an email receiver

b. Configure the receiver's account and add necessary information to the **Description** area.

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

----End

9 System

This chapter contains the following sections:

Section	Description
System Setting	Describes how to configure system parameters.
Alert Rules	Describes how to set alert rules.
Users and Roles	Describes how to set the Admin account.
Updating	Describes how to configure update parameters.
Backup and Restore	Describes how to configure file backup and restoration parameters.
Central Manager	Describes how to configure parameters for collaboration with ESPC, LAS, BSA, ISOP, ESP-H, syslog, and kafka.
Service Subscription	Describes how to configure the parameters on license management and device care services.
Troubleshooting	Describes how to use various diagnosis tools.
System Control	Describes how to perform system controls, including restart, system closeup, and application configuration.

9.1 System Setting

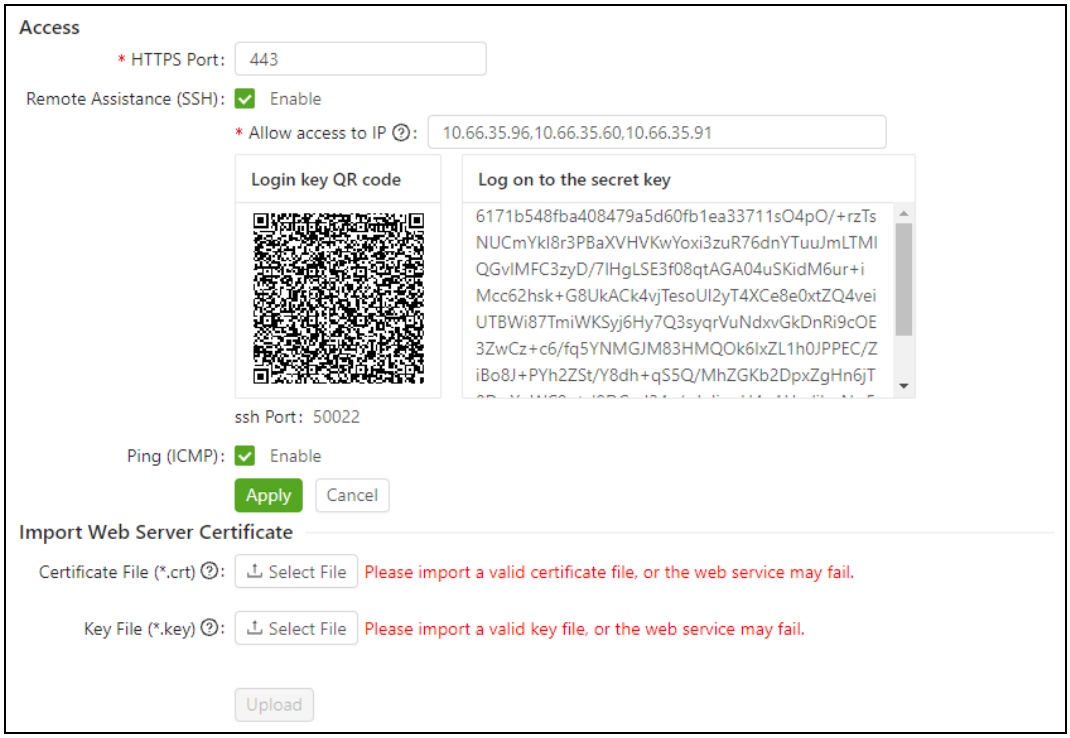
System setting mainly includes engine configuration, NTP server configuration, and configuration of special parameters.

9.1.1 Configuring the Engine

To configure engine parameters, follow these steps:

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

Figure 9-1 Configuring the engine



Step 2 In the dialog box, configure administrative access parameters.

Table 9-1 Engine configuration parameters

Parameter	Description
HTTPS Port	NIPS provides the administrator with the port number of HTTPS services. The default port is **443**, which can be changed.
Remote Assistance (SSH)	Controls whether to enable remote assistance and specifies the IP addresses that are allowed to access NIPS for remote assistance. Up to three IP addresses can be configured. After this is enabled, the remote assistance information, including login key QR code, log on to the secret key, and ssh port, will be provided.
Ping (ICMP)	Controls whether to enable NIPS to respond to ICMP requests. After this is enabled, NIPS responds to ICMP requests, which makes it convenient for an administrator to debug the device. After this is disabled, NIPS does not respond to ICMP requests.

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

----End

Importing a Web Server Certificate

A web server certificate includes the following:

- Certificate file: is a .crt file that cannot exceed 1 MB.

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

Step 1 Click **Select File** and select the certificate file and key file stored on the local device.

Caution	The certificate file and key file to be imported must be valid; otherwise, a web service error would occur.

Step 2 Click **Upload**.

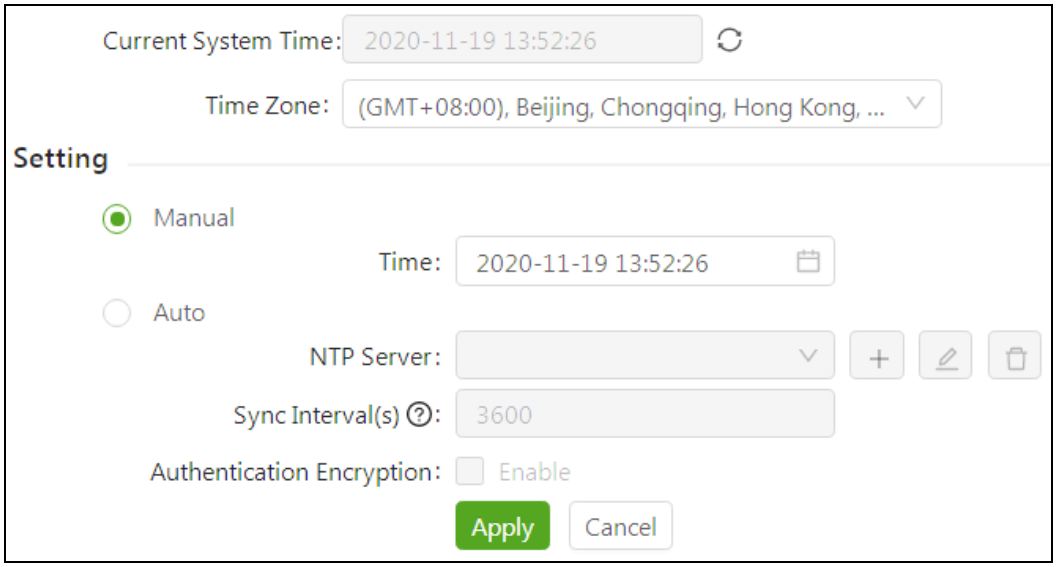
----End

9.1.2 Configuring the NTP Server

To configure an NTP server, follow these steps:

Step 1 Choose **System** > **System Setting** > **NTP Server**.

Figure 9-2 Configuring the NTP server



Step 2 Configure parameters of the NTP server.

Table 9-2 NTP server configuration parameters

Parameter		Description
Current System Time		Indicates the date and time of the current NIPS device.
Time Zone		Specifies the time zone of the current NIPS device.
Manual	Time	Specifies the date and time after **Manual** is selected.
Auto	NTP Server	After **Auto** is selected, you must select the pre-configured NTP server from the drop-down list and make sure that the engine

Parameter		Description
		management interface can communicate with the time synchronization server. Click + on the right of the drop-down list to add a new NTP server with the following parameters: **Server Address**: specifies the IP address of the NTP server. **Server Name**: specifies the name of the NTP server. **Encryption File**: is a .key file that cannot exceed 1 MB.
	Sync Interval(s)	Specifies the interval for NIPS to automatically synchronize the time with the NTP server after **Auto** is selected. The value is expressed in seconds. The interval is no smaller than 60s.
	Authentication Encryption	This parameter is available only when **Auto** is selected. If authentication is enabled on the NTP server, NTP encryption should be turned on here.

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

Step 4 Go to **System** > **System Control** and click **Reboot System** to make the settings take effect.

----End

9.1.3 Configuring Special Parameters

Choose **System** > **System Setting** > **Advanced** to configure special parameters.

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.

9.2 Alert Rules

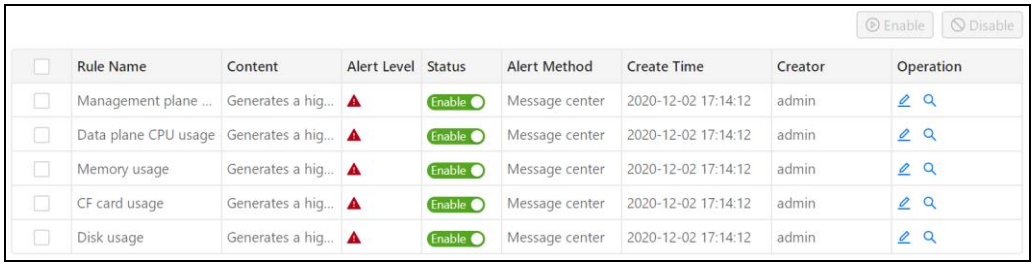
Alert rules are created for either device resource or device status.

9.2.1 Alert Rules for Device Resources

Alert rules for device resources are used to monitor management plane CPU usage, data plane CPU usage, memory usage, CF card usage, and disk usage of NIPS. After the usage exceeds the threshold in a rule, an alert is triggered and an alert log is pushed to the message center.

Step 1 Choose **System** > **Alert Rules** > **Device Resource**.

Figure 9-3 Alert rules for device resources



You can see the contents of the alert rules for various resources on the list, as described in Table 9-3.

Step 2 Click in the **Operation** column to view details.

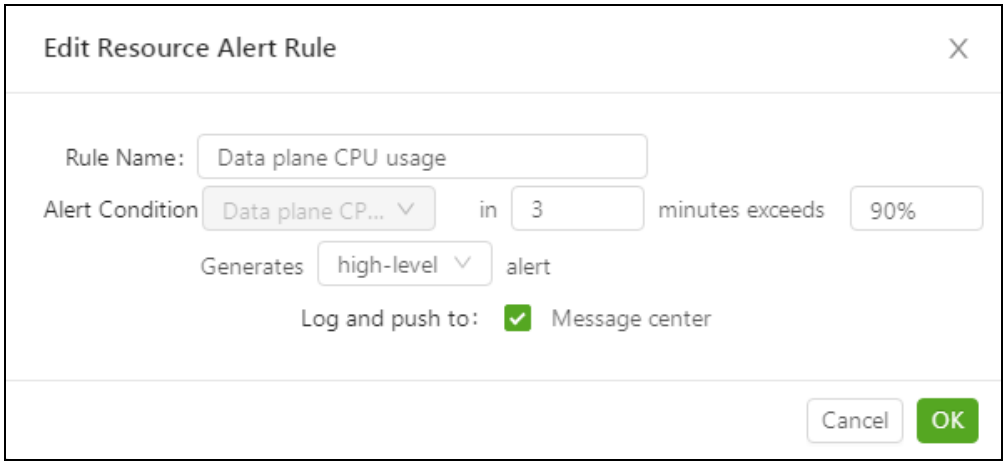
Table 9-3 Description of alert rules for device resources

Rule Name	Description
Management plane CPU usage	Monitors the management plane CPU usage. If the usage exceeds the threshold (the default value is **90%**) within a duration (the default value is **3** minutes), an alert with a designated level (The default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
Data plane CPU usage	Monitors the data plane CPU usage. If the usage exceeds the threshold (the default value is **90%**) within a duration (the default value is **3** minutes), an alert with a designated level (the default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
Memory usage	Monitors the memory usage. If the usage exceeds the threshold (the default value is **90%**) within a duration (the default value is **3** minutes), an alert with a designated level (the default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
CF card usage	Monitors the CF card usage. If the usage exceeds the threshold (the default value is **70%**) within a duration (the default value is **3** minutes), an alert with a designated level (the default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
Disk usage	Monitors the disk usage. If the usage exceeds the threshold (the default value is **70%**) within a duration (the default value is **3** minutes), an alert with a designated level (the default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.

Step 3 Edit an alert rule.

Click in the **Operation** column to modify the parameters of the rule.

Figure 9-4 Editing the parameters of an alert rule



Step 4 Enable/Disable a rule.

A rule does not take effect before being enabled. The **Status** column shows whether the rule has taken effect via the following icons:

- Enable indicates that the rule is enabled. Click it and then click **Disable** in the dialog box to disable the rule.
- Disable indicates that the rule is disabled. Click it and then click **Enable** in the dialog box to enable the rule.

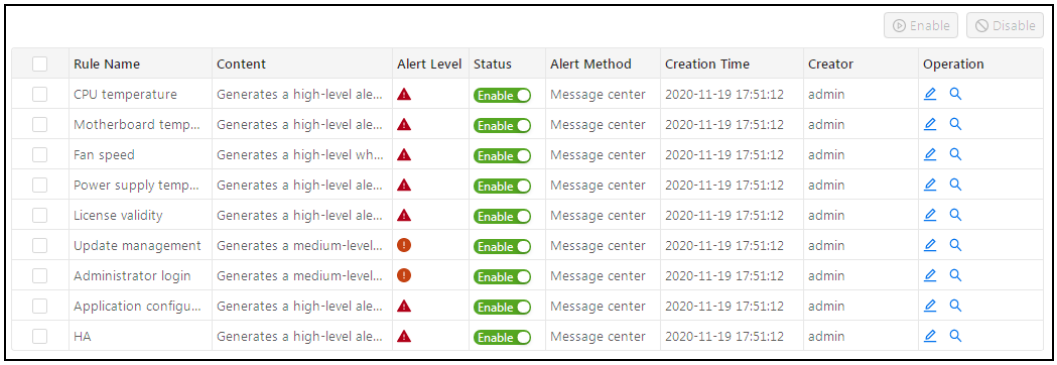
----End

9.2.2 Alert Rules for Device Status

Alert rules for device status are used to monitor the CPU temperature, motherboard temperature, fan speed, power supply temperature, license validity, update management, administrator login, application configuration, and high availability (HA) modules of NIPS. Once a rule is hit, an alert is triggered and an alert log is pushed to the message center.

Step 1 Choose **System** > **Alert Rules** > **Device Status**.

Figure 9-5 Alert rules for device status



Enable Disable

Rule Name	Content	Alert Level	Status	Alert Method	Creation Time	Creator	Operation
CPU temperature	Generates a high-level ale...		Enable	Message center	2020-11-19 17:51:12	admin	
Motherboard temp...	Generates a high-level ale...		Enable	Message center	2020-11-19 17:51:12	admin	
Fan speed	Generates a high-level wh...		Enable	Message center	2020-11-19 17:51:12	admin	
Power supply temp...	Generates a high-level ale...		Enable	Message center	2020-11-19 17:51:12	admin	
License validity	Generates a high-level ale...		Enable	Message center	2020-11-19 17:51:12	admin	
Update management	Generates a medium-level...		Enable	Message center	2020-11-19 17:51:12	admin	
Administrator login	Generates a medium-level...		Enable	Message center	2020-11-19 17:51:12	admin	
Application configu...	Generates a high-level ale...		Enable	Message center	2020-11-19 17:51:12	admin	
HA	Generates a high-level ale...		Enable	Message center	2020-11-19 17:51:12	admin	

You can see the contents of the alert rules on the list, as described in Table 9-4.

Step 2 Click in the **Operation** column to view details.

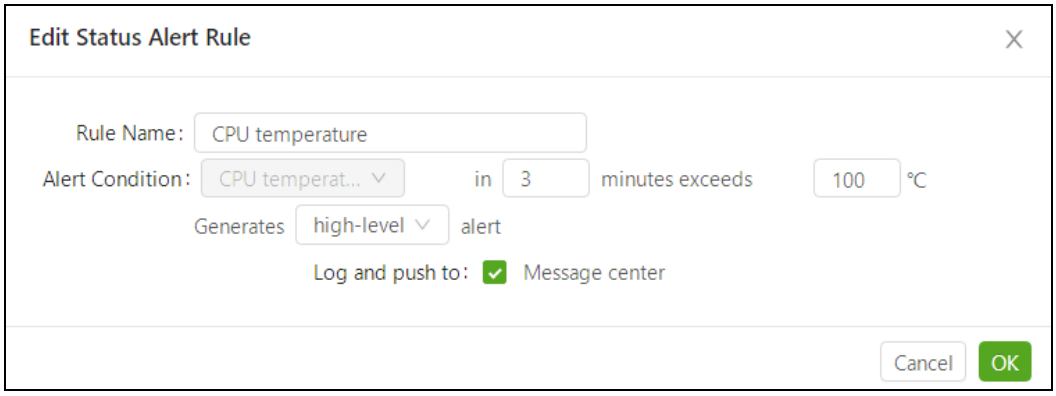
Table 9-4 Description of alert rules for device status

Rule Name	Description
CPU temperature	Monitors the CPU temperature. If the temperature exceeds the threshold (the default value is **98.8ºC**) within a duration (the default value is **3** minutes), an alert with a designated level (the default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
Motherboard temperature	Monitors the motherboard temperature. If the temperature exceeds the threshold (the default value is **70ºC**) within a duration (the default value is **3** minutes), an alert with a designated level (the default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
Fan speed	Monitors the fan speed. If the usage exceeds the threshold (the default value is **4.8** *1000 r/min) within a duration (the default value is **3** minutes), an alert with a designated level (the default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
Power supply temperature	Monitors the power supply temperature. If the usage exceeds the threshold (the default upper limit is **+45ºC** and lower limit is **0ºC**) within a duration (the default value is **3** minutes), an alert with a designated level (the default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
License validity	Monitors the validity of the licenses in various modules. If a license is invalid, an alert with a designated level (the default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
Update management	Monitors the system update status, which has the following values: update success, update failure, and update package installation. It a status change is detected, an alert with a designated level (the default value is **medium-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
Administrator login	Monitors the status of administrator login. If the administrator logs in to the device, an alert with a designated level (the default value is **medium-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
Application configuration	Monitors application configuration. If the administrator configures an application, an alert with a designated level (the default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.
HA	Monitors the status of HA modules. If the active device is switched to the standby device, an alert with a designated level (the default value is **high-level**) is generated. Besides, you can make settings on whether to push the alert information to the message center.

Step 3 Edit an alert rule.

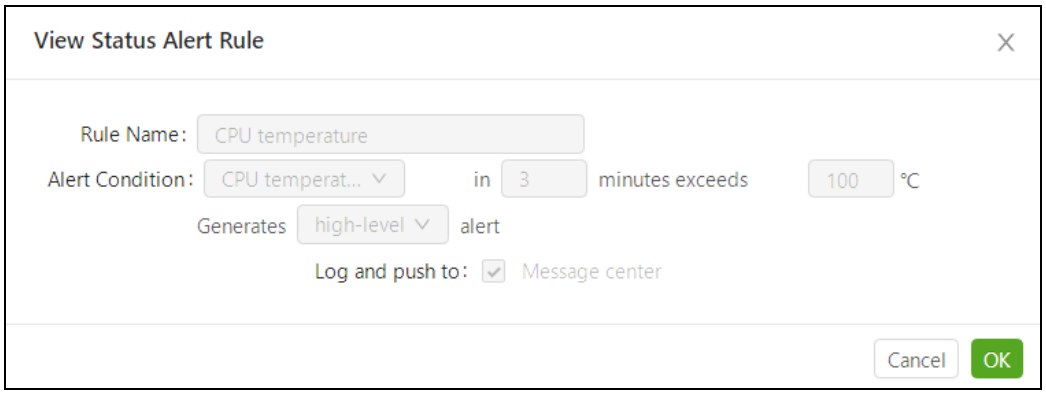
Click in the **Operation** column to modify the parameters of the rule.

Figure 9-6 Editing the parameters of an alert rule



Step 4 Click in the **Operation** column to view the parameters of such a rule.

Figure 9-7 Viewing the parameters of a status alert rule



Step 5 Enable/Disable a rule.

A rule cannot take effect before being enabled. The **Status** column shows whether the rule has taken effect via the following icons:

- Enable indicates that the rule is enabled. Click it and then click **Disable** in the dialog box to disable the rule.
- Disable indicates that the rule is disabled. Click it and then click **Enable** in the dialog box to enable the rule.

----End

9.3 Users and Roles

Under **System** > **Users and Roles**, you can manage local authenticated users and rules and set login parameters.

9.3.1 Users

NIPS has two default accounts: default operator **admin** and default auditor **auditor**. **auditor** is not enabled by default and can only be enabled by **admin**. **admin** and **auditor** can create operator accounts and auditor accounts respectively. 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 add, 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.

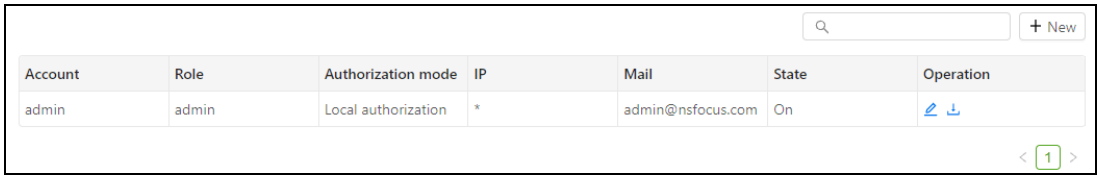
9.3.1.1 Enabling the Default Auditor Account

The default auditor (**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** > **Users and Roles** > **Users**.

Figure 9-8 User configuration



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

Figure 9-9 Setting the initial password for the default auditor account

Step 3 Set the initial password.

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.

----End

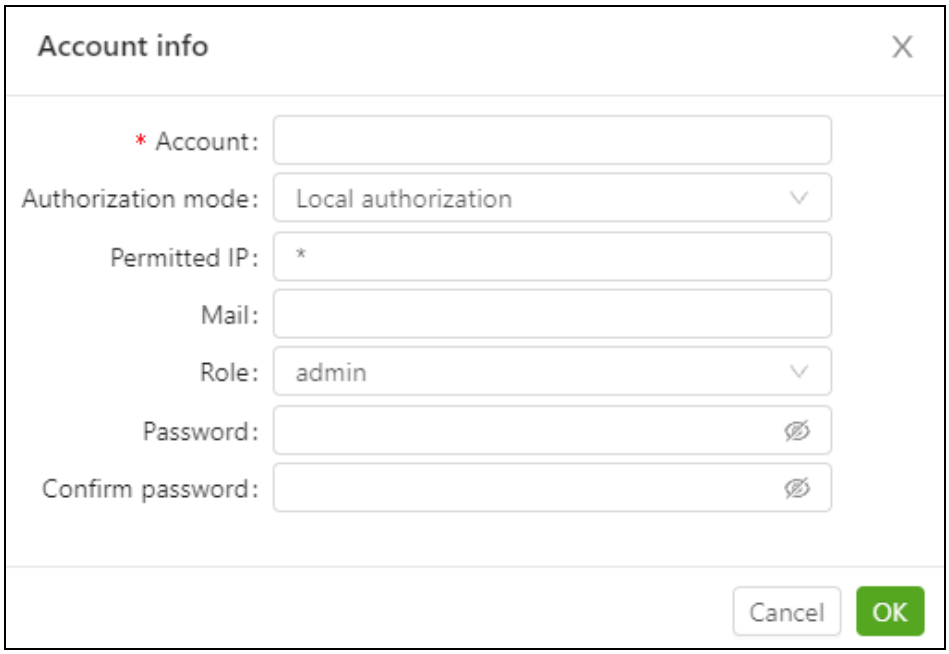
9.3.1.2 Creating a User Account

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** > **Users and Roles** > **Users**.

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

Figure 9-10 Creating an account



Step 3 Configure parameters in the **Account info** dialog box.

Table 9-5 Parameters for creating an 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 being successfully created.
Authorization mode	Specifies an authentication mode, which can be one of the following: • **Local authorization**: Default settings are used. • **Radius authorization**: The Radius authorization server must be specified. For details, see Authentication Server. • **Ldap authorization**: The LDAP authorization server must be specified. For details, see Authentication Server. • **Local authorization and license**: After password authorization, the account needs to pass certificate authorization. Only after a correct user certificate is imported can the account pass the authorization. After **Enable** is selected, you need to download a certificate. For details, see Exporting a Certificate.
Permitted IP	Specifies the IP address that can be used by this new account for login. You can type an IP address, an IP range, or multiple IP addresses. The default value is *****, indicating that the operator can log in to NIPS from any IP

Parameter	Description
	address.
Mail	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. For how to configure a role, see Roles.
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 Access Settings.
Confirm password	Requires you to reenter the password for confirmation.

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

9.3.1.3 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 A.2.3 Using Maintenance Tools.
- You can change the password via the web-based manager. Specifically, point to in the quick access bar, click **Change Password**, and change the current password.

9.3.1.4 Deleting an Account

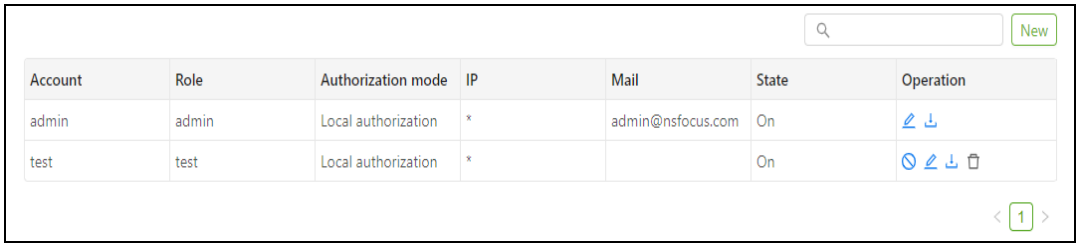
Only the default operator account (**admin**) and auditor account (**auditor**) can delete accounts that they have created respectively. They cannot delete default system accounts.

9.3.1.5 Exporting a Certificate

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

Step 1 Choose **System > Users and Roles > Users**.

Figure 9-11 Exporting a certificate



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

Step 2 Click in the **Operation** column of an account to export the certificate to the default download path.

----End

9.3.2 Roles

Besides default accounts **admin** and **auditor**, new roles can be configured by **admin**, who should also grant permissions to these roles.

Step 1 Choose **System** > **Users and Roles** > **Roles**.

Figure 9-12 Roles page

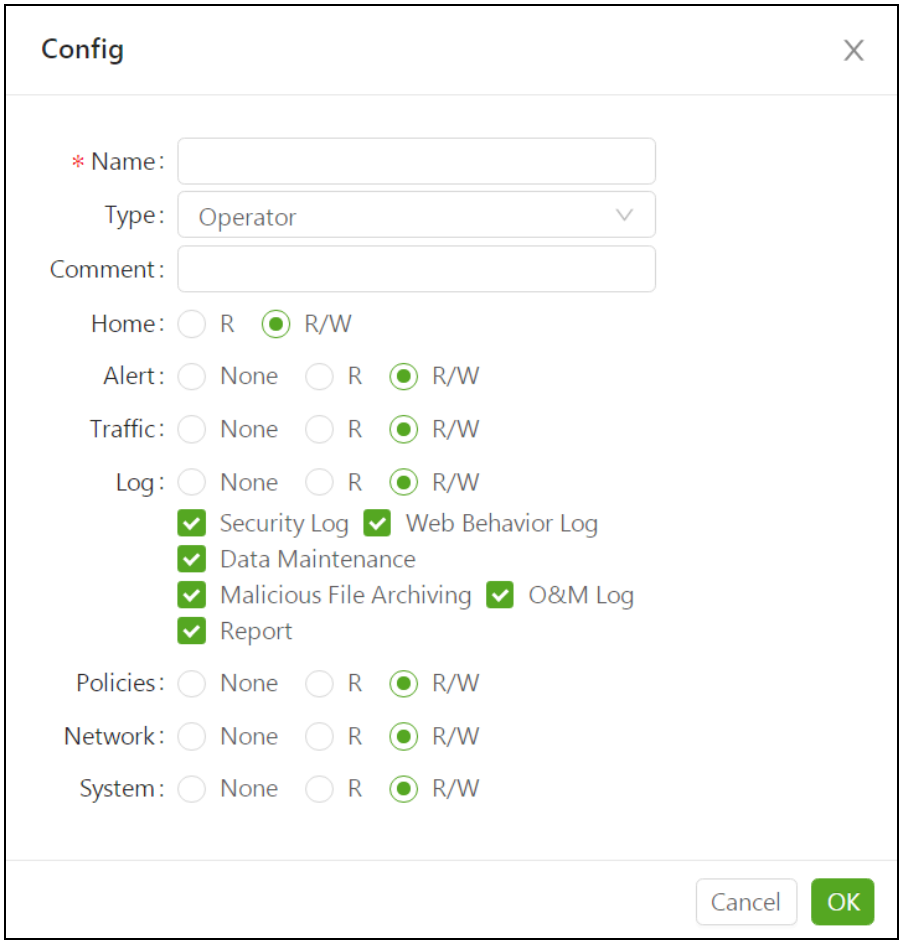
Step 2 View the role list.

You can see all roles in the list below and the permissions of the roles in the **Permission** column.

Step 3 Create a role.

a. Click **New** to create a role.

Figure 9-13 Creating a role



b. Grant permissions to this role.

For each module, select permissions, which can be any of the following:

- **None**: The module is unavailable for this role.
- **R**: The role can only view configurations of the module.
- **R/W**: The role can modify configurations of the module.

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

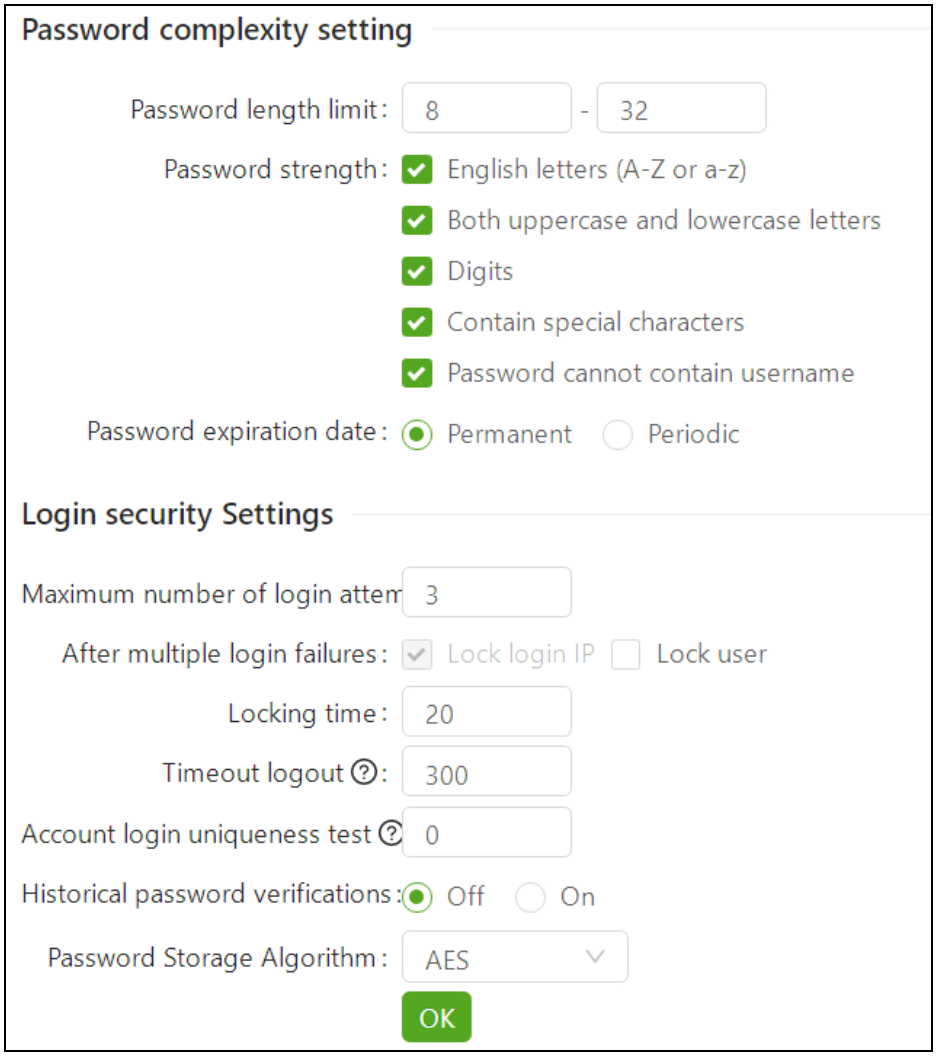
----End

9.3.3 Access Settings

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

Step 1 Choose **System > Users and Roles > Access Settings**.

Figure 9-14 Access Settings page



Step 2 Configure parameters.

Table 9-6 Parameters for access settings

Parameter		Description
Password Complexity Setting	Password length limit	Specifies the length limit of the password used by the user who logs in to a local NIPS device. The value range is 8–32.
	Password strength	Specifies the password strength requirements. After multiple password strength requirements are selected, the password must meet multiple conditions at the same time.
	Password expiration date	• **Permanent**: indicates that the password expiration days are not limited. • **Periodic**: 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.
Login Security	Maximum number of login attempts	Specifies the maximum number of consecutive login attempts by a user with a wrong user name or password. After the maximum

Parameter		Description
Settings		number is exceeded, the account will be locked for a certain period of time to restrict the user's login. The default value is **3**, and the maximum value that you can set is **8**.
	After multiple login failures	Action after login failures. Specifies whether to lock an account when the number of consecutive login failures reaches the threshold specified with **Lock login IP**. 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 **Locking time** expires. • Account locking will be recorded in an audit log. The auditor can view such logs after logging in to the system.
	Locking time	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 **Lock login IP**. The default value is **20** minutes.
	Timeout logout	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 The maximum value is **600**. It is recommended that the value be at least **60**. Too short a period will cause frequent system timeouts.
	Account login uniqueness test	Specifies the maximum number of concurrent login sessions per user account. The default value is **0**, indicating no limit to such a number. The value range is 0–10.
	Historical password verifications	The default value is **Off**. If **On** is selected, you need to set a value in the text box below to specify the number of unique new passwords that must be associated with a user account before an old password can be reused.
	Password Storage Algorithm	Specifies the way to secure the storage of the user's login password, which can be **AES**, **SM2**, or **SM4**.

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

----End

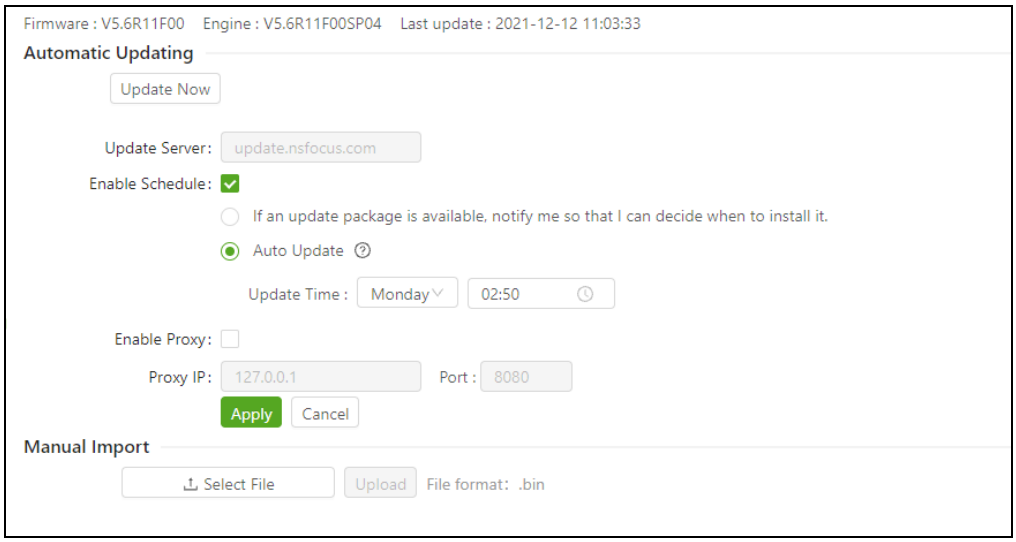
9.4 Updating

You can update system software and various databases, and view the update history.

9.4.1 Updating System Software

Choose **System** > **Updating** > **System Software**.

Figure 9-15 Updating system software



Automatic Updating

If NIPS can connect to the Internet, you can update the device online. NIPS can be updated online in the following four ways:

- Remote scheduled update
- Remote instant update
- Remote update via a proxy
- Remote manual update

Note	• The prerequisite for any of the online updating ways is that NIPS can connect to 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 DNS. • The DNS server IP address should be excluded from interface configurations; otherwise, an IP address conflict would occur and the update would fail.

Step 1 Specify the IP address of the update server.

Step 2 Select **Enable Schedule**.

Then NIPS will automatically detect whether there is a new update package available. When a new update package is detected, system software will be automatically updated at the time set by the administrator.

Step 3 Configure parameters.

Table 9-7 Parameters for configuring online update

Parameter		Description
Update Server		Specifies the network address of the system update package. The default value is **update.nsfocus.com**, which cannot be modified.
Enable Schedule	Auto Update	Controls whether NIPS automatically checks the latest update package and updates the system at the specified time. **Update Time**: specifies the time when NIPS automatically updates the system. After **Auto Update** is selected, NIPS can automatically update the system daily or at any hour on any day from Monday through Sunday, depending on your configuration. 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.
	If an update package is available, notify me so that I can decide when to install it.	If this is selected, the system will automatically check updates and notify users when detecting new update packages.
Enable Proxy	Enable Proxy	Specifies whether to enable a proxy server for automatic updating.
	Proxy IP	IP address of the proxy server.
	Port	Port number of the proxy server.

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

Step 5 Choose **System > System Control** and then click **Deploy Policies**.

----End

Instant Update

You can also update the device instantly when necessary.

To update the device instantly, follow these steps:

Step 1 Choose **System > Updating > System Software**.

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

For the description of parameters, see Table 9-7.

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

----End

Manual Import

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

To update the device instantly, follow these steps:

Step 1 Choose **System** > **Updating** > **System Software**.

Step 2 Click **Select File**, select the file, and click **Open**.

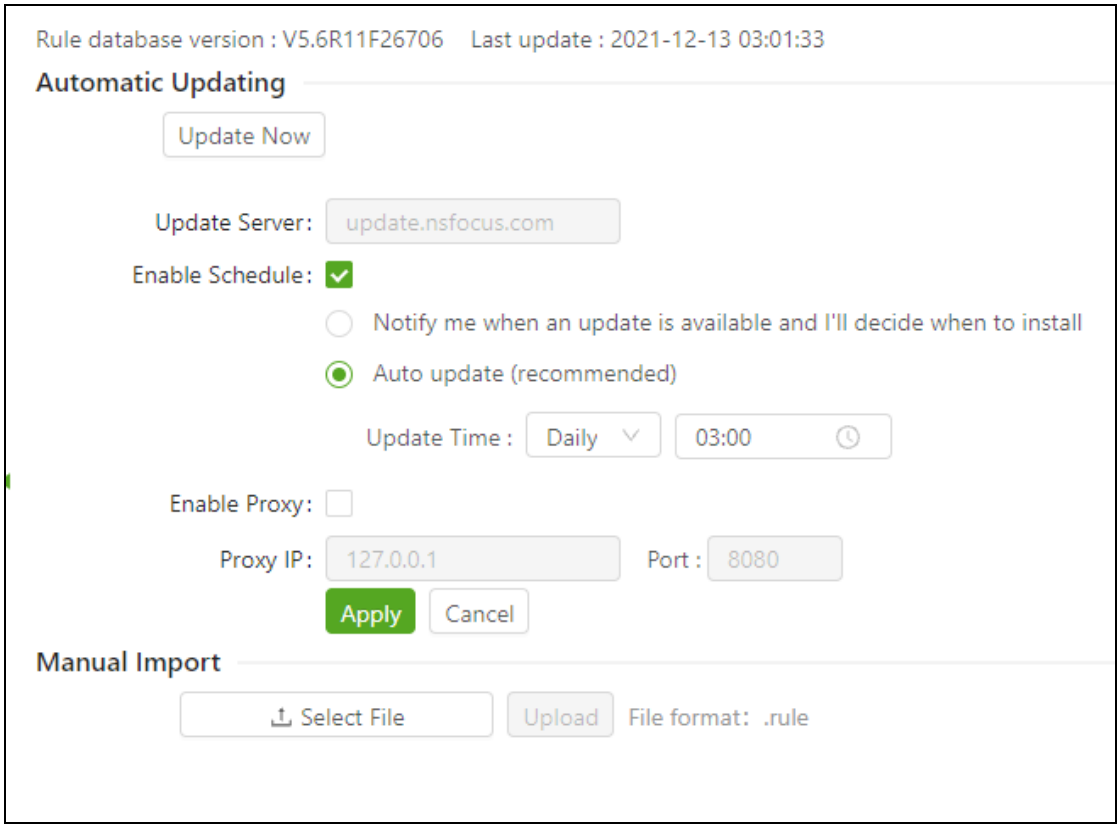
Step 3 Click **Upload** to update the device immediately.

----End

9.4.2 Updating Signature Sets

Choose **System** > **Updating** > **Signature Sets**.

Figure 9-16 Updating signature sets



For details, see Updating System Software.

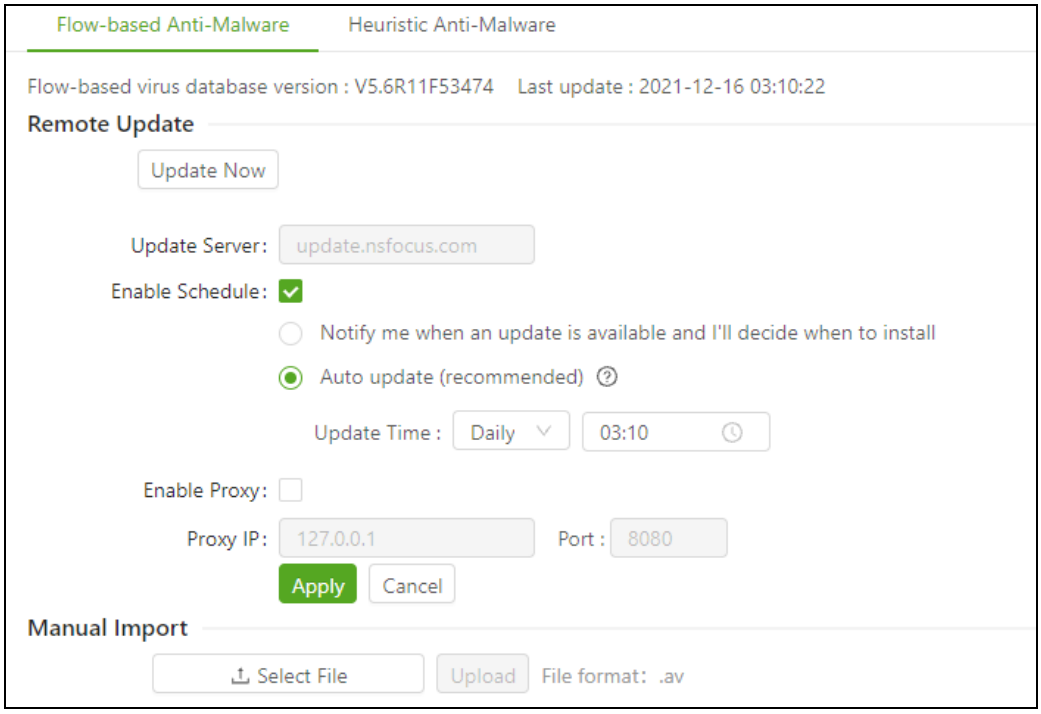
9.4.3 Updating Anti-Malware Databases

Anti-malware databases include flow-based anti-malware and heuristic anti-malware databases.

9.4.3.1 Updating the Flow-based Anti-Malware Database

Choose **System** > **Updating** > **Anti-Malware** > **Flow-based Anti-Malware**.

Figure 9-17 Updating the flow-based anti-malware database

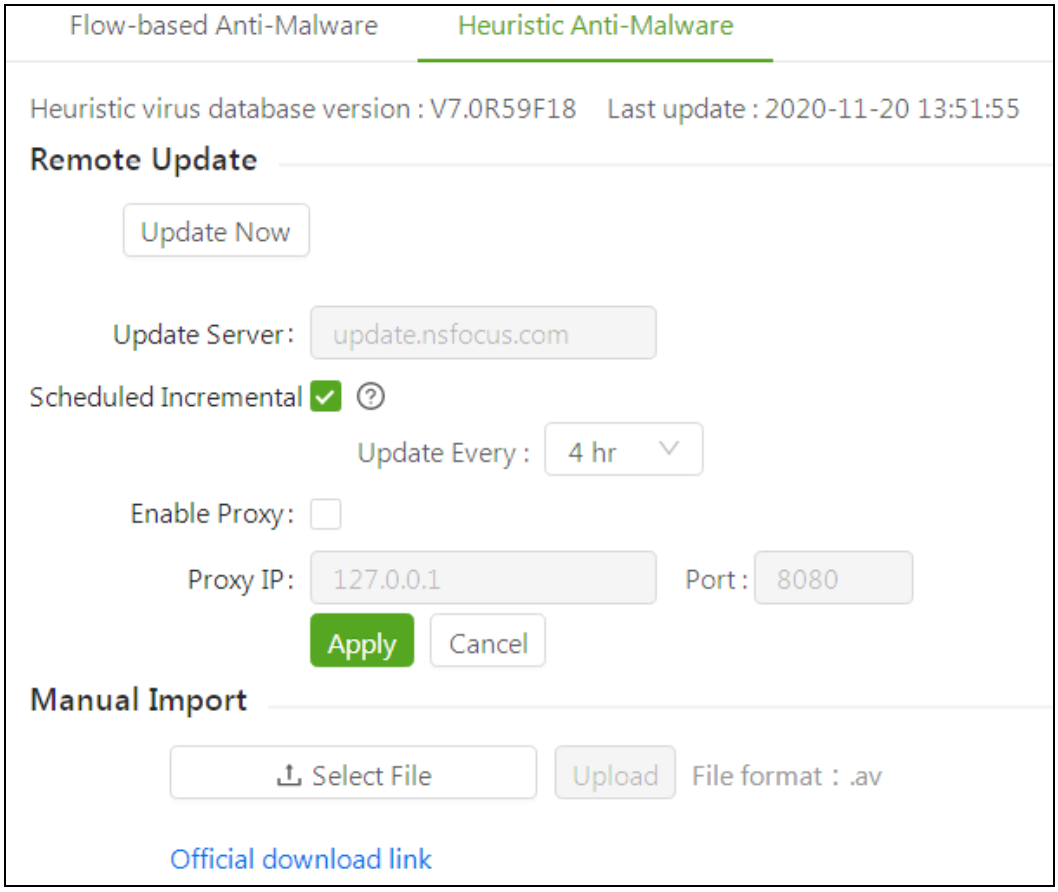


For details, see Updating System Software.

9.4.3.2 Updating the Heuristic Anti-Malware Database

Step 1 Choose **System** > **Updating** > **Anti-Malware** > **Heuristic Anti-Malware**.

Figure 9-18 Updating the heuristic anti-malware database



Step 2 Update the anti-malware database online.

For details, see Updating System Software.

For local updating, see Downloading the File for Updating the Heuristic Anti-Malware Database.

----End

Downloading the File for Updating the Heuristic Anti-Malware Database

Step 1 Click **Official download link** in Figure 9-18 to switch to the **Software Update** page of NSFOCUS.

Step 2 Click **NSFOCUS Threat Analysis Center (TAC)**.

Step 3 Choose the latest version (for example, v2.0.2).

Step 4 Click **Anti-Malware Database Update Package 7.0.0**.

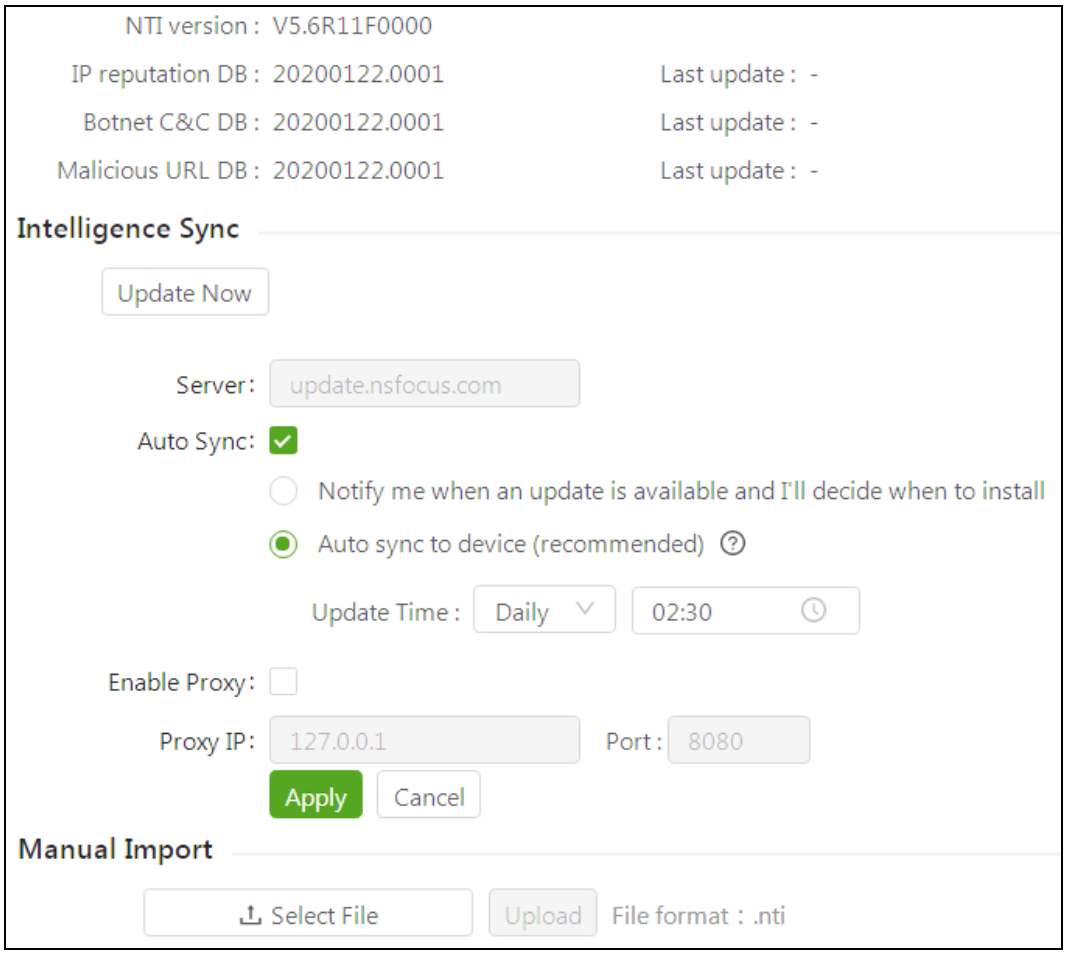
Step 5 Click the name link to download an anti-malware database to a local disk drive.

----End

9.4.4 Updating Threat Intelligence Databases

Choose **System** > **Updating** > **Threat Intelligence**.

Figure 9-19 Updating threat intelligence databases

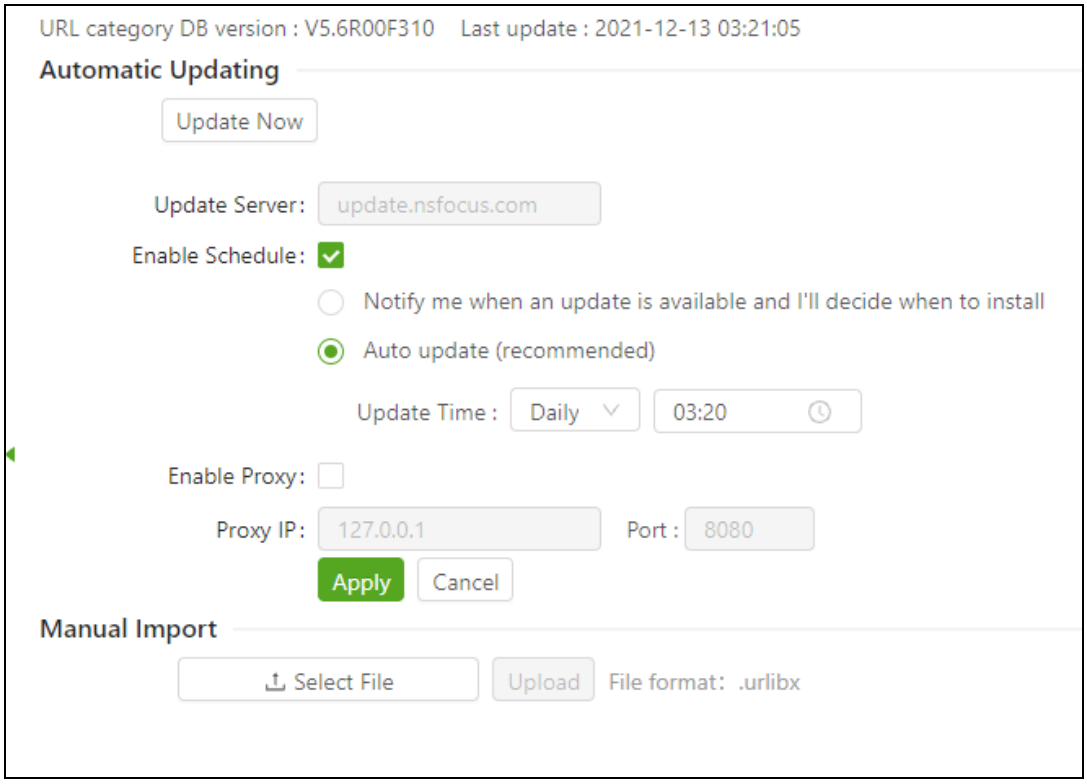


You can see information about the current version of the threat intelligence databases in the upper part of the page. For update details, see Updating System Software.

9.4.5 Updating the URL Category Database

Choose **System** > **Updating** > **URL Category**.

Figure 9-20 Updating the URL category database

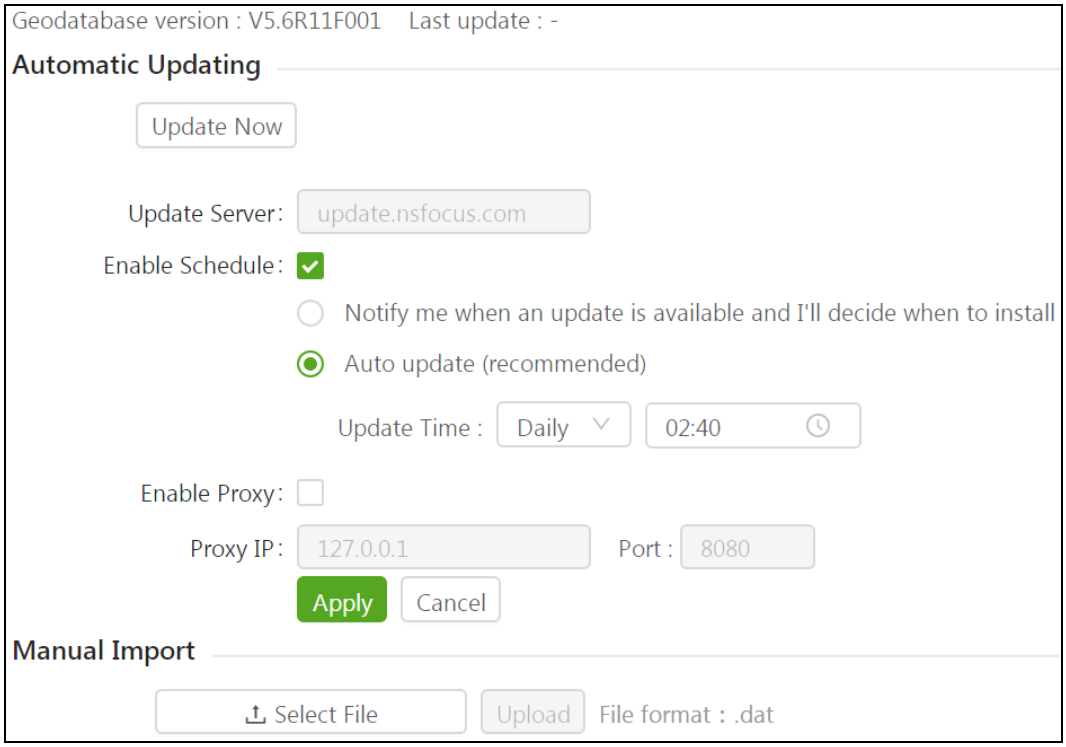


You can see information about the current version of the URL category database in the upper part of the page. For update details, see Updating System Software.

9.4.6 Updating the Geodatabase

Choose **System** > **Updating** > **Regions**.

Figure 9-21 Updating the geodatabase

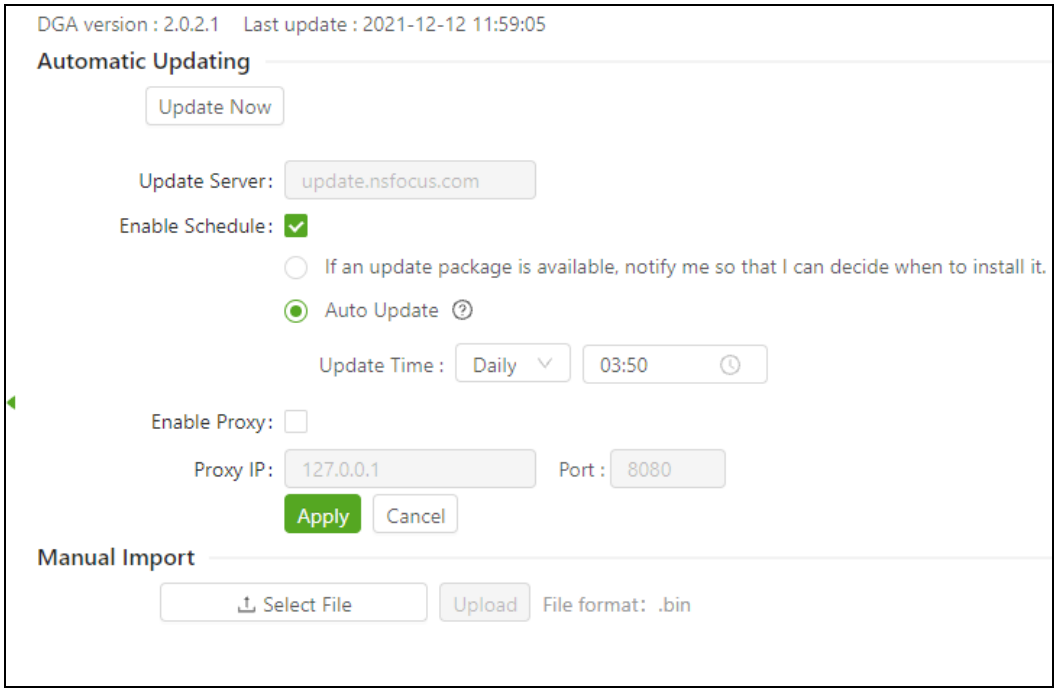


You can see information about the current version of the geodatabase in the upper part of the page. For update details, see Updating System Software.

9.4.7 Updating DGA

Choose **System** > **Updating** > **DGA Upgrade**.

Figure 9-22 DGA upgrade

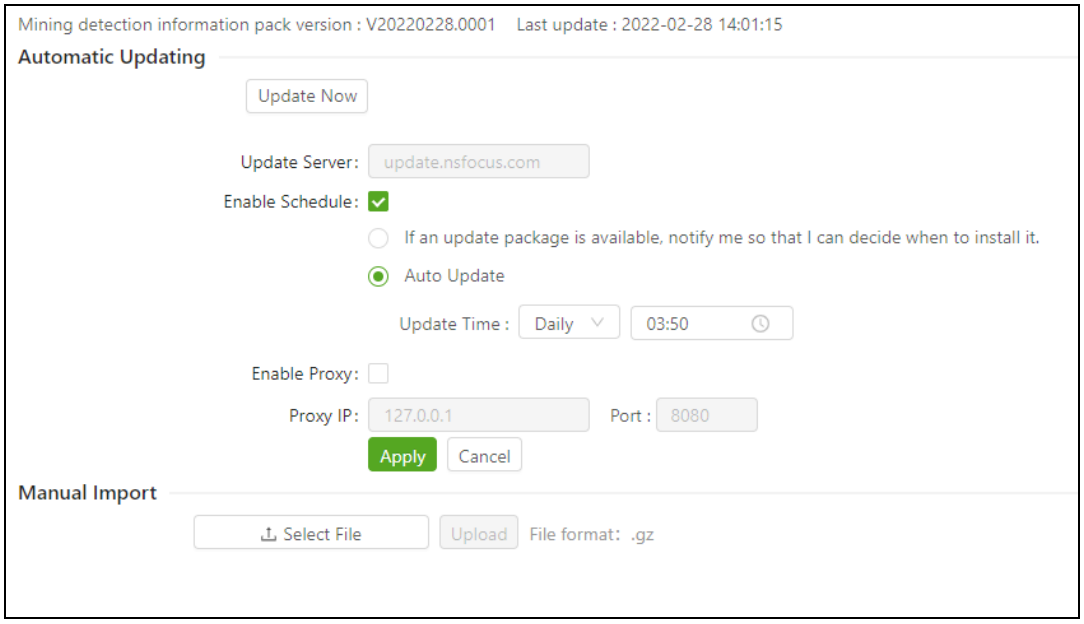


You can see information about the current DGA version in the upper part of the page. For update details, see Updating System Software.

9.4.8 Updating the Mining Detection Information Pack

Choose **System > Updating > Mining Detection Upgrade**.

Figure 9-23 Updating the mining detection information pack

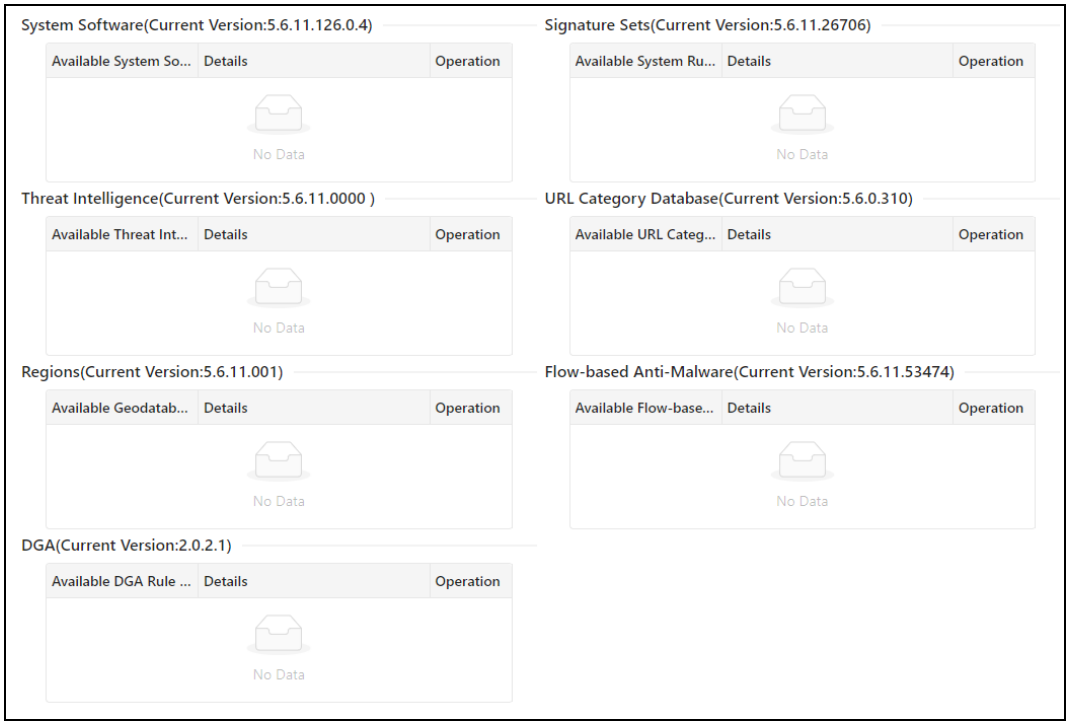


You can see information about the current version of the mining detection information pack in the upper part of the page. For update details, see Updating System Software.

9.4.9 Manual Deploy

Choose **System** > **Updating** > **Manual Deploy**.

Figure 9-24 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:

a. Click **Click to update**.

b. Click in the **Operation** column to 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.

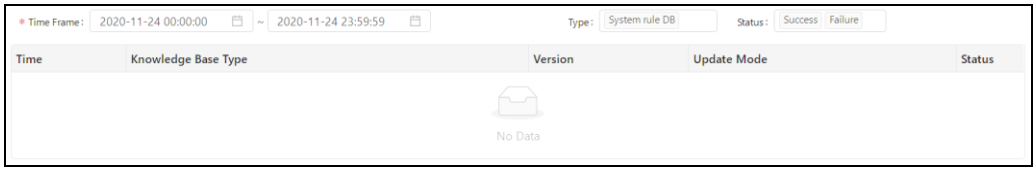
- To save an update package, perform the following step:

Click to save the current upgrade package to a local disk drive.

9.4.10 Update History

Choose **System** > **Updating** > **Update History** to view the update history of the system software and various databases.

Figure 9-25 Viewing the update history



You can set filtration conditions by time frame, type, and status to view specific update history information.

9.5 Backup and Restore

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

9.5.1 Backup

Currently, NIPS allows you to back up the following files:

- All configuration files
- Engine parameter file
- Interface parameter file
- Custom rule file
- Local authentication file
- Object configuration file
- Rule configuration file
- License file

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

Step 1 Choose **System** > **Restore Settings** > **Backup**.

Figure 9-26 Backing up a file

Step 2 Select **Engine parameter file** from the drop-down list.

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

----End

9.5.2 Restore

Currently, NIPS allows you to restore configurations from the following backup files:

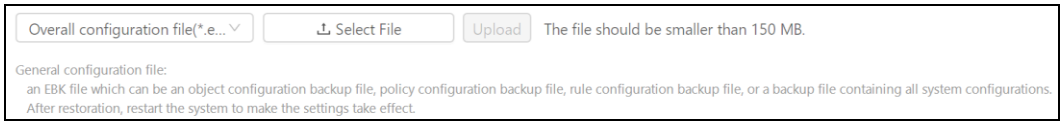
- Overall configuration file (*.ebk)
- Engine parameter file (*.ebk)
- Interface parameter file (*.ebk)
- Custom rule base (*.ebk)
- Local authentication file (*.list)
- Object configuration file (*.ebk)
- Rule configuration file (*.ebk)

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

To restore a backup file, follow these steps:

Step 1 Choose **System** > **Restore Settings** > **Restore**.

Figure 9-27 Restoring a file



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

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

----End

9.5.3 Configuration Restore

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 a restore point for the general configuration file

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 a 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.

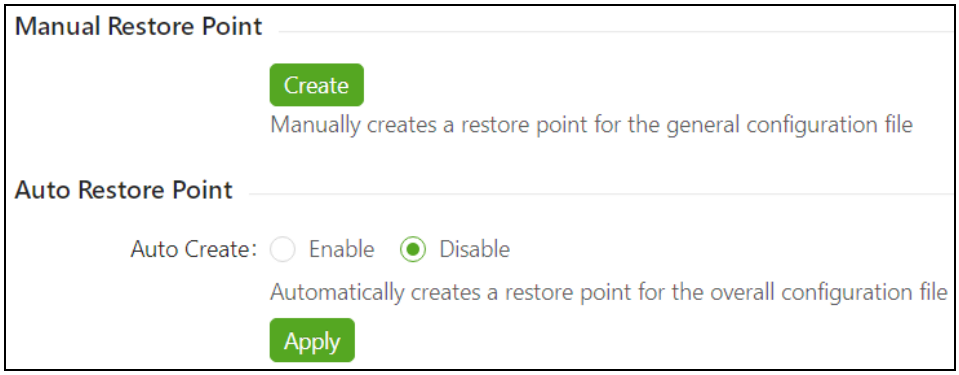
Manual Restore Point

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** > **Restore Settings** > **Configuration Restore**.

Figure 9-28 shows the **Manual Restore Point** area.

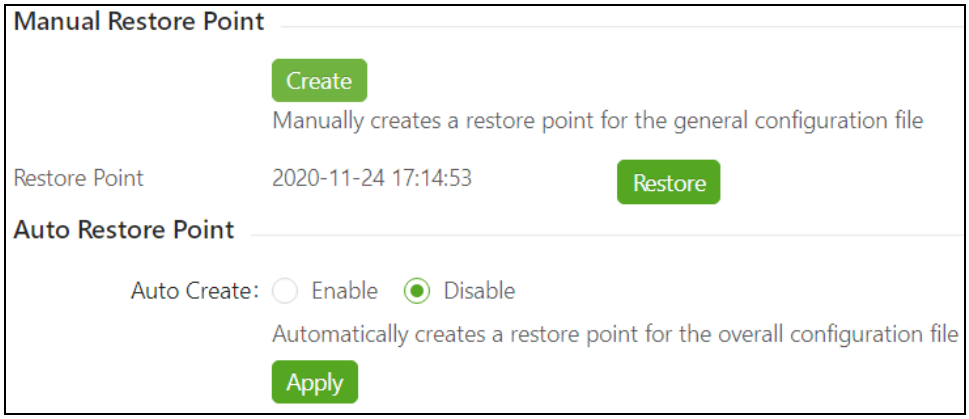
Figure 9-28 Manual Restore Point area



Step 2 Click **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.

Figure 9-29 Manual restore point created



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

----End

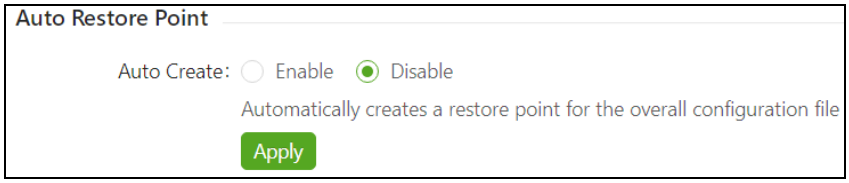
Auto Restore Point

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

Step 1 Choose **System** > **Restore Settings** > **Configuration Restore**.

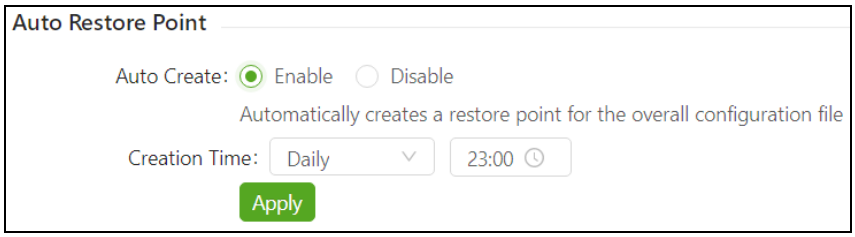
Figure 9-30 shows the **Auto Restore Point** area.

Figure 9-30 Auto Restore Point area



Step 2 Select **Enable** for **Auto Create** to enable NIPS to automatically create a restore point.

Figure 9-31 Enabling the Auto Restore function



Step 3 Specify the restore point creation time.

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

Step 4 Click **Apply** to save 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

9.6 Central Manager

The Central Manager module allows you to configure parameters to make NIPS collaborate with the other platforms or servers.

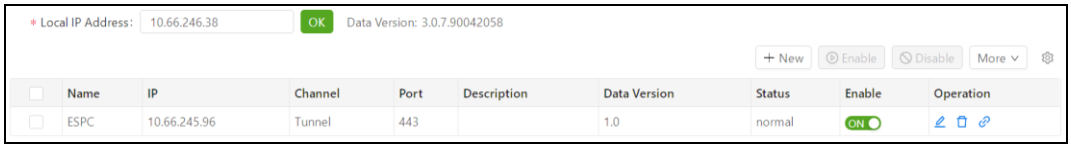
9.6.1 ESPC

NIPS can be registered on NSFOCUS ESPC only after you configure related parameters on the **Central Manager** page. You can establish, delete, enable, or disable connections. The following section just describes how to establish a connection.

To establish a connection, follow these steps:

Step 1 Choose **System** > **Central Manager** > **ESPC** to establish a connection between NIPS and NSFOCUS ESPC.

Figure 9-32 ESPC page



If the connection is correct, the **Status** column displays "Normal", indicating that NIPS has been connected to NSFOCUS ESPC.

Click ⚙ on the upper right of the table to specify what to display. Only the selected columns can be seen in the list.

Step 2 Configure the local IP address.

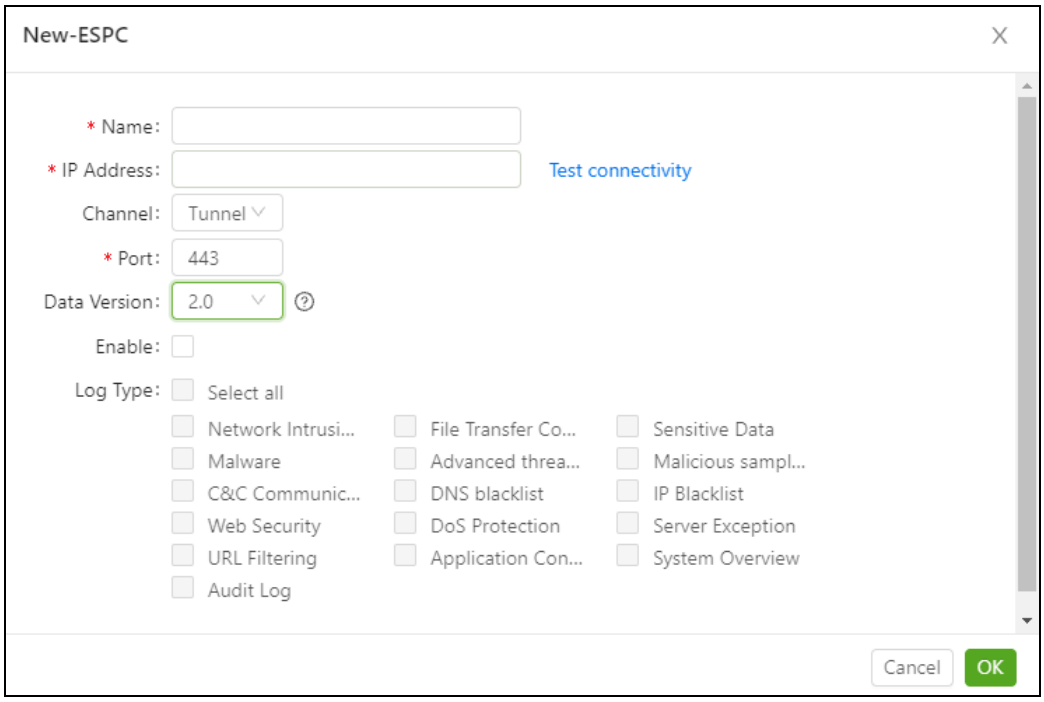
Before configuring NIPS to connect to NSFOCUS ESPC and other settings, you need to configure the local IP address of NIPS, which is usually the IP address of an interface with the management function or that of a management interface.

By default, NIPS automatically detects the IP address that can connect to the Internet and automatically connects to NSFOCUS ESPC. After successful connection, NIPS 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 will no longer detect any IP address for access to the Internet.

Step 3 Click **New** to establish a connection with NSFOCUS ESPC by configuring an IP address, port parameter, and other parameters.

Figure 9-33 Establishing a connection with NSFOCUS ESPC



Step 4 Configure parameters.

Table 9-8 Parameter for connecting to NSFOCUS ESPC

Parameter	Description
Name	Connection name.
IP Address	IP address of NSFOCUS ESPC that NIPS will connect to. Click **Test connectivity** to check whether NIPS properly connects to NSFOCUS ESPC.
Channel	Specifies the mode (**Tunnel** or **Encrypted**) for connection between NIPS and NSFOCUS ESPC. The setting on NIPS should be the same as that on NSFOCUS ESPC. By default, the connection mode is **Tunnel**.
Port	Specifies the port for NSFOCUS ESPC to receive various data from the NIPS engine.
Data Version	Supports versions 1.0 and 2.0. • **1.0**: uploads all logs and data of NIPS V5.6R10F02 or earlier versions. • **2.0**: uploads the selected logs and data of NIPS V5.6R11F00 or later versions
Enable	Select the **Enable** check box to enable the NIPS engine to connect to NSFOCUS ESPC.

Step 5 Click **OK** to make the settings take effect.

----End

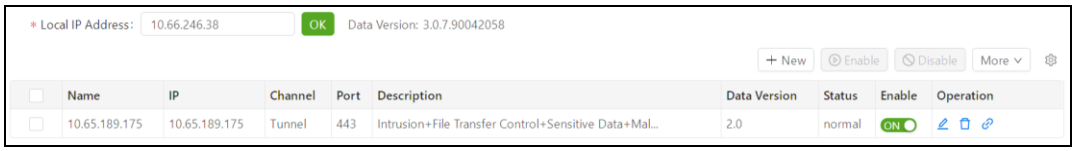
9.6.2 LAS

You can configure NSFOCUS LAS to receive various logs from NIPS. After configuration, NIPS can send related log data to NSFOCUS LAS. You can establish, delete, enable, or disable connections. The following section just describes how to establish a connection.

To establish a connection with NSFOCUS LAS, follow these steps:

Step 1 Choose **System** > **Central Manager** > **LAS**.

Figure 9-34 LAS page



If the connection is correct, the **Status** column displays "Connected", indicating that NIPS has been connected to NSFOCUS LAS.

Click on the upper right of the table to specify what to display. Only the selected columns can be seen in the list.

Step 2 Configure the local IP address.

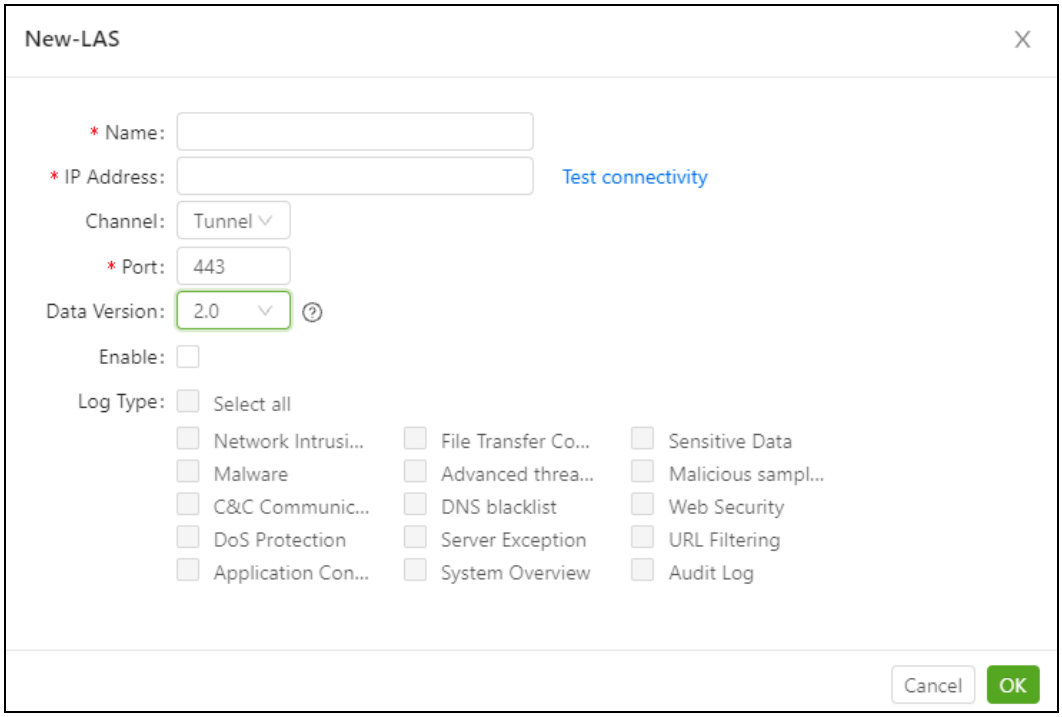
Before configuring NIPS to connect to NSFOCUS LAS and other settings, you need to configure the local IP address of NIPS, which is usually the IP address of an interface with the management function or that of a management interface.

You can change the local IP address and then click **OK**. After the change, the device will no longer detect any IP address for access to the Internet.

Step 3 Click **New**.

A dialog box appears, as shown in Figure 9-35.

Figure 9-35 Establishing a connection with NSFOCUS LAS



Step 4 Configure parameters.

Table 9-9 Parameter for connecting to NSFOCUS LAS

Parameter	Description
Name	Connection name.
IP Address	IP address of NSFOCUS LAS that NIPS will connect to. Click **Test connectivity** to check whether NIPS properly connects to NSFOCUS LAS.
Channel	Specifies the mode (**Tunnel** or **Encrypted**) for connection between NIPS and NSFOCUS LAS. The setting on NIPS should be the same as that on NSFOCUS LAS. By default, the connection mode is **Tunnel**.
Port	Specifies the port for NSFOCUS LAS to receive various data from the NIPS engine.
Data Version	Supports versions 1.0 and 2.0. • **1.0**: uploads all logs and data of NIPS V5.6R10F02 or earlier versions. • **2.0**: uploads the selected logs and data of NIPS V5.6R11F00 or later versions
Enable	Select the **Enable** check box to enable the NIPS engine to connect to NSFOCUS LAS.

Step 5 Click **OK** to make the settings take effect.

----End

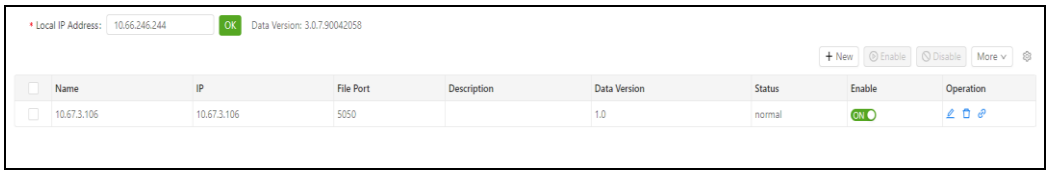
9.6.3 BSA

You can configure NSFOCUS BSA to receive various data from NIPS. After configuration, NIPS can send related data to NSFOCUS BSA. You can establish, delete, enable, or disable connections. The following section just describes how to establish a connection.

To establish a connection with NSFOCUS BSA, follow these steps:

Step 1 Choose **System** > **Central Manager** > **BSA**.

Figure 9-36 BSA page



If the connection is correct, the **Status** column displays "Normal", indicating that NIPS has been connected to NSFOCUS BSA.

Click ⚙ on the upper right of the table to determine the columns that are to be displayed. Only the selected columns can be seen in the list.

Step 2 Configure the local IP address.

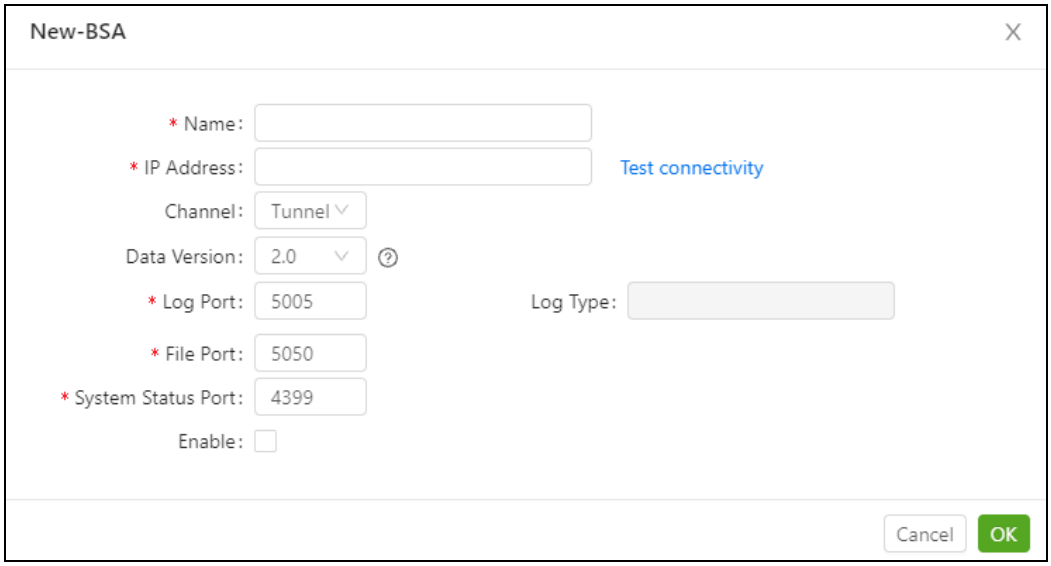
Before configuring NIPS to connect to NSFOCUS BSA and other settings, you need to configure the local IP address of NIPS, which is usually the IP address of an interface with the management function or that of a management interface.

You can change the local IP address and then click **OK**. After the change, the device will no longer detect any IP address for access to the Internet.

Step 3 Click **New**.

A dialog box appears, as shown in Figure 9-37.

Figure 9-37 Establishing a connection with NSFOCUS BSA



Step 4 Configure parameters.

Table 9-10 Parameters for configuring NIPS to connect to NSFOCUS BSA

Parameter	Description
Name	Connection name.
IP Address	IP address of NSFOCUS BSA that NIPS will connect to. Click **Test connectivity** to check whether NIPS properly connects to NSFOCUS BSA.
Channel	Specifies the mode (**Tunnel** or **Encrypted**) for connection between NIPS and NSFOCUS BSA. The setting on NIPS should be the same as that on NSFOCUS BSA. By default, the connection mode is **Tunnel**.
Data Version	Supports versions 1.0 and 2.0. • **1.0**: uploads all logs and data of NIPS V5.6R10F02 or earlier versions. • **2.0**: uploads the selected logs and data of NIPS V5.6R11F00 or later versions
Log Port	Specifies the port for NSFOCUS BSA to receive security logs (JSON) from the NIPS engine.
File Port	Specifies the port for NSFOCUS BSA to receive files from the NIPS engine. The default value is **5050**.
System Status Port	Specifies the port for NSFOCUS BSA to receive status logs from the NIPS engine. The default value is **4399**. **Note** You can set the port to **0**. In this case, no status log will be sent to NSFOCUS BSA.
Enable	Select the **Enable** check box to enable the NIPS engine to connect to NSFOCUS BSA.

Step 5 Click **OK** to make the settings take effect.

----End

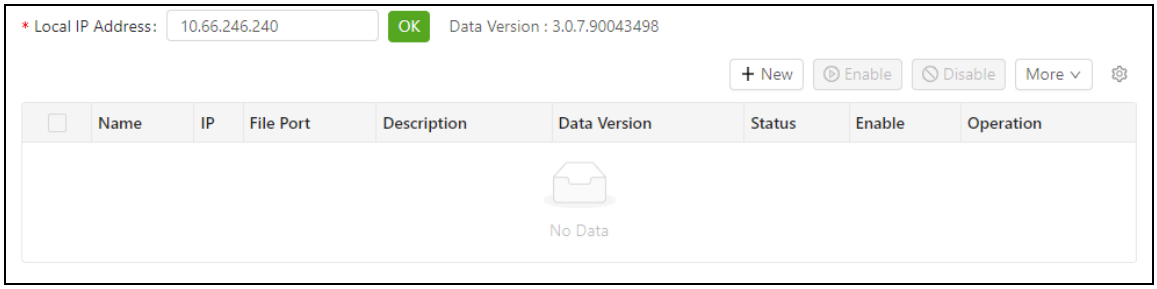
9.6.4 ISOP

You can configure NSFOCUS ISOP to receive various data from NIPS. After configuration, NIPS can send related data to NSFOCUS ISOP. You can establish, delete, enable, or disable connections. The following section just describes how to establish a connection.

To establish a connection with NSFOCUS ISOP, follow these steps:

Step 1 Choose **System** > **Central Manager** > **ISOP**.

Figure 9-38 ISOP page



If the connection is correct, the **Status** column displays "Normal", indicating that NIPS has been connected to NSFOCUS ISOP.

Click ⚙ on the upper right of the table to determine the columns that are to be displayed. Only the selected columns can be seen in the list.

Step 2 Configure the local IP address.

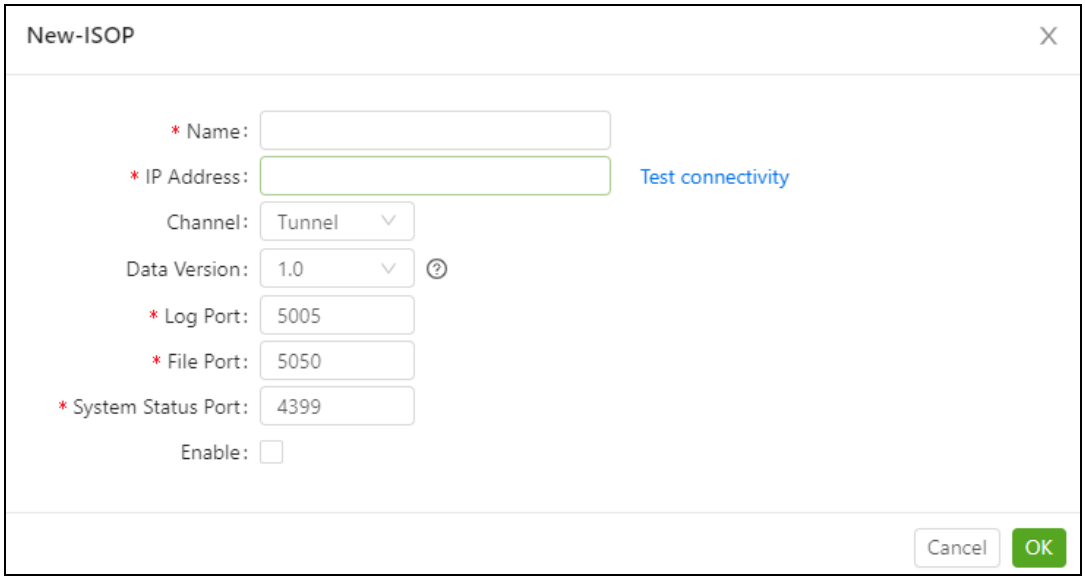
Before configuring NIPS to connect to NSFOCUS ISOP and other settings, you need to configure the local IP address of NIPS, which is usually the IP address of an interface with the management function or that of a management interface.

You can change the local IP address and then click **OK**. After the change, the device will no longer detect any IP address for access to the Internet.

Step 3 Click **New**.

A dialog box appears, as shown in Figure 9-39.

Figure 9-39 Establishing a connection with NSFOCUS ISOP



Step 4 Configure parameters.

Table 9-11 Parameters for configuring NIPS to connect to NSFOCUS ISOP

Parameter	Description
Name	Connection name.
IP Address	IP address of NSFOCUS ISOP that NIPS will connect to. Click **Test connectivity** to check whether NIPS properly connects to NSFOCUS ISOP.
Channel	Specifies the mode (**Tunnel** or **Encrypted**) for connection between NIPS and NSFOCUS ISOP. The setting on NIPS should be the same as that on NSFOCUS ISOP. By default, the connection mode is **Tunnel**.
Data Version	Supports versions 1.0 and 2.0. • **1.0**: uploads all logs and data of NIPS V5.6R10F02 or earlier versions. • **2.0**: uploads the selected logs and data of NIPS V5.6R11F00 or later versions
Log Port	Specifies the port for NSFOCUS ISOP to receive security logs (JSON) from the NIPS engine.
File Port	Specifies the port for NSFOCUS ISOP to receive files from the NIPS engine. The default value is **5050**.
System Status Port	Specifies the port for NSFOCUS ISOP to receive status logs from the NIPS engine. The default value is **4399**. **Note** You can set the port to **0**. In this case, no status log will be sent to NSFOCUS ISOP.
Enable	Select the **Enable** check box to enable the NIPS engine to connect to NSFOCUS ISOP.

Step 5 Click **OK** to make the settings take effect.

----End

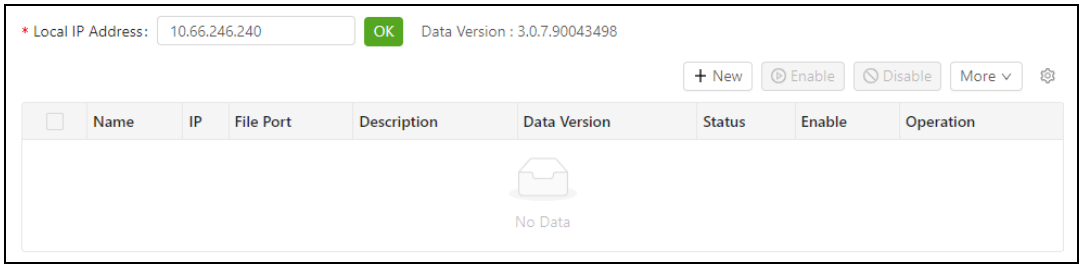
9.6.5 ESP-H

You can configure NSFOCUS ESP-H to receive various data from NIPS. After configuration, NIPS can send related data to NSFOCUS ESP-H. You can establish, delete, enable, or disable connections. The following section just describes how to establish a connection.

To establish a connection with NSFOCUS ESP-H, follow these steps:

Step 1 Choose **System** > **Central Manager** > **ESP-H**.

Figure 9-40 ESP-H page



If the connection is correct, the **Status** column displays "Normal", indicating that NIPS has been connected to NSFOCUS ESP-H.

Click ⚙ on the upper right of the table to determine the columns that are to be displayed. Only the selected columns can be seen in the list.

Step 2 Configure the local IP address.

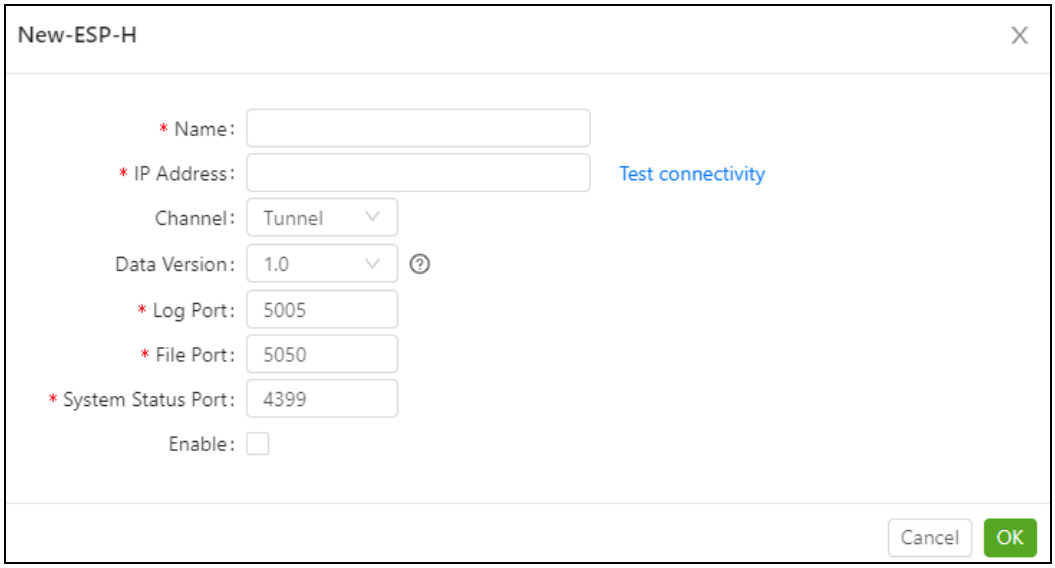
Before configuring NIPS to connect to NSFOCUS ESP-H and other settings, you need to configure the local IP address of NIPS, which is usually the IP address of an interface with the management function or that of a management interface.

You can change the local IP address and then click **OK**. After the change, the device will no longer detect any IP address for access to the Internet.

Step 3 Click **New**.

A dialog box appears, as shown in Figure 9-41.

Figure 9-41 Establishing a connection with NSFOCUS ESP-H



Step 4 Configure parameters.

Table 9-12 Parameters for configuring NIPS to connect to NSFOCUS ESP-H

Parameter	Description
Name	Connection name.
IP Address	IP address of NSFOCUS ESP-H that NIPS will connect to. Click **Test connectivity** to check whether NIPS properly connects to NSFOCUS ESP-H.
Channel	Specifies the mode (**Tunnel** or **Encrypted**) for connection between NIPS and NSFOCUS ESP-H. The setting on NIPS should be the same as that on NSFOCUS ESP-H. By default, the connection mode is **Tunnel**.
Data Version	Supports versions 1.0 and 2.0. • **1.0**: uploads all logs and data of NIPS V5.6R10F02 or earlier versions. • **2.0**: uploads the selected logs and data of NIPS V5.6R11F00 or later versions
Log Port	Specifies the port for NSFOCUS ESP-H to receive security logs (JSON) from the NIPS engine.
File Port	Specifies the port for NSFOCUS ESP-H to receive files from the NIPS engine. The default value is **5050**.
System Status Port	Specifies the port for NSFOCUS ESP-H to receive status logs from the NIPS engine. The default value is **4399**. **Note** You can set the port to **0**. In this case, no status log will be sent to NSFOCUS ESP-H.
Enable	Select the **Enable** check box to enable the NIPS engine to connect to NSFOCUS ESP-H.

Step 5 Click **OK** to make the settings take effect.

----End

9.6.6 SYSLOG

Syslog-related configurations include:

- **Server Settings**: specifies parameters of the syslog server.
- **Log Template**: allows you to customize log templates and edit formats of logs sent to the syslog server.

9.6.6.1 Server Settings

The local storage space of NIPS is limited. To save more logs, you can configure NIPS to send logs to the syslog server for storage.

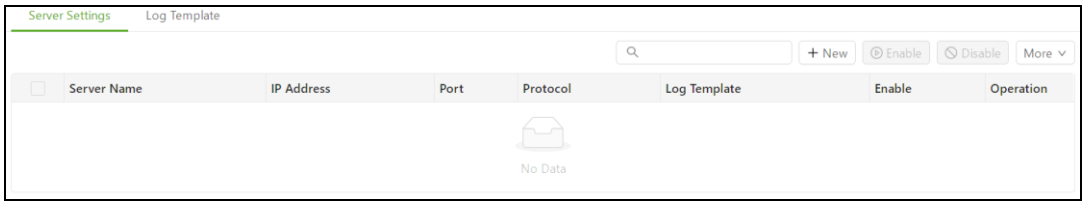
You can add, edit, delete, or search for a syslog server on NIPS. The following section describes how to add and search for a syslog server.

Adding a Syslog Server

NIPS supports five syslog servers at most. To configure a syslog server on NIPS, follow these steps:

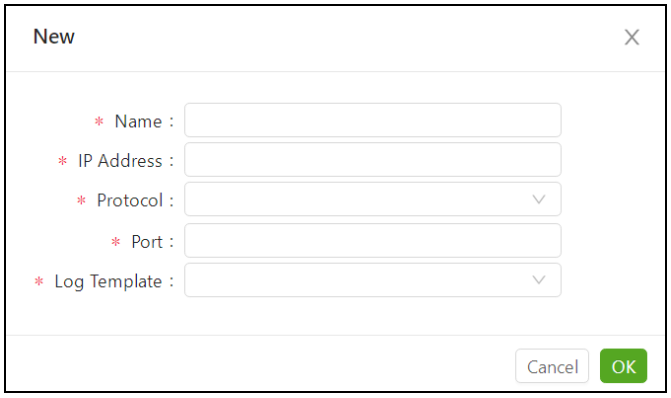
Step 1 Choose **System** > **Central Manager** > **SYSLOG** > **Server Settings**.

Figure 9-42 Server Settings page



Step 2 Click **New** to add a syslog server.

Figure 9-43 Adding a syslog server



Step 3 Set parameters.

Table 9-13 Parameters for configuring a syslog server

Parameter	Description
Name	Name of the new syslog server.
IP Address	IP address of the new syslog server.
Protocol	Specifies the type of the transport-layer protocol used by the syslog server. It has two values: TCP and UDP.
Port	Port of the syslog server.
Log Template	Can be selected from the drop-down list. The built-in template of the system is **default + UTF-8**. If you select a custom template, you can edit the format of log messages sent to the syslog server. For details, see Log Template.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

Searching for a Syslog Server

On the **Server Settings** page shown in Figure 9-42, you can search for a syslog server by typing the name, IP address, port number, or log template of the syslog server in the text box and click the button .

Then the desired syslog server (if any) will be displayed in the table.

9.6.6.2 Log Template

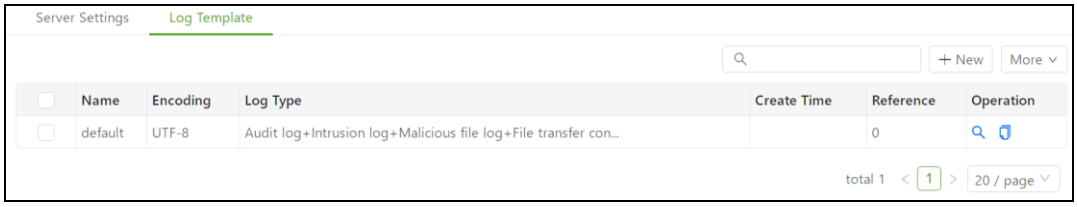
Log Template defines formats of logs sent to a syslog server. Log templates include **default** (the built-in template of the system) and custom log templates. The built-in template only allows you to view its contents. Custom log templates mean that you can configure the connector, separator, and encoding method and customize the event classification and formats of the logs sent to the syslog server.

You can create, copy, edit, or delete custom templates. Besides, you can only view and copy the built-in template. You can also import templates into or export templates from NIPS.

The following section describes how to create a log template.

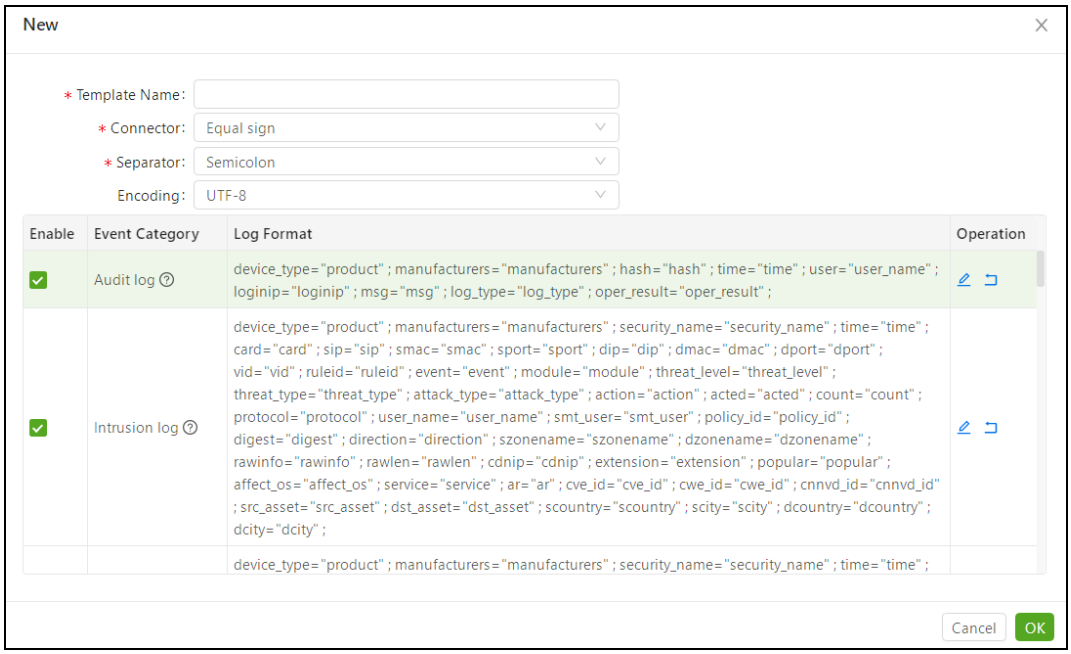
Step 1 Choose **System** > **Central Manager** > **SYSLOG** > **Log Template**.

Figure 9-44 Log template



Step 2 Click **New**.

Figure 9-45 Creating a new custom template

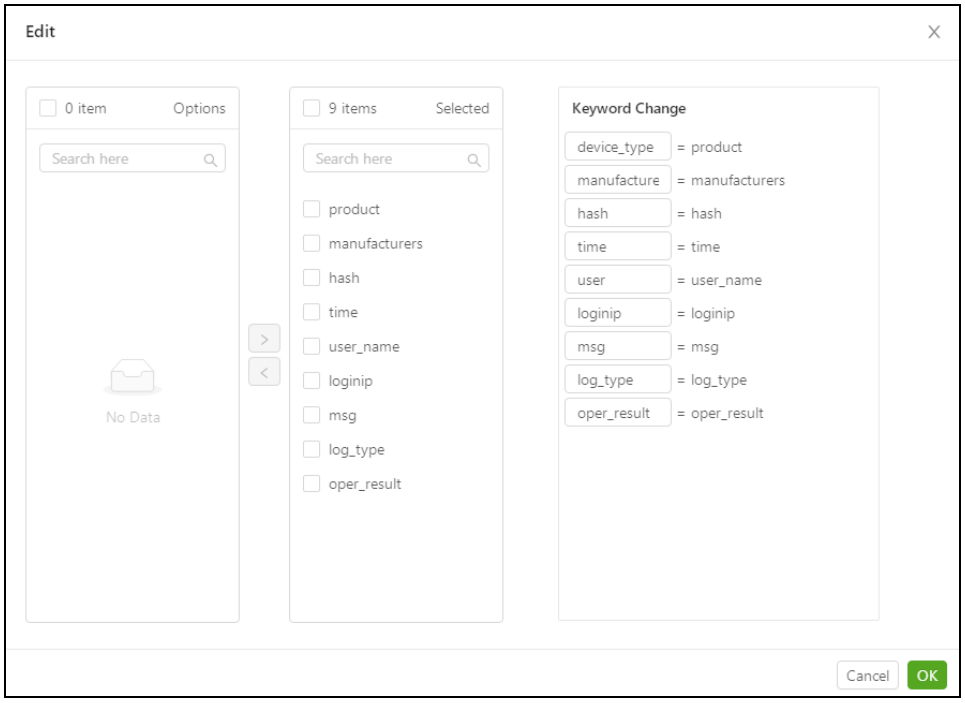


Step 3 Set parameters.

Table 9-14 Parameters for configuring a log template

Parameter		Description
Template Name		Name of the custom template.
Connector		Connector that connects the variable name and its value in the **Log Format** column in the log type table.
Separator		Separator that separates two variables in the **Log Format** column in the log type table.
Encoding		Specifies how a log is encoded.
Log Configuration	Enable	Specifies whether to enable an event.
	Event Category	Specifies event categories.
	Log Format	Specifies formats of logs sent to a syslog server.
	Operation	Click the icon to define log formats of various events, as shown in Figure 9-46. Click the icon to restore the log formats to default values.

Figure 9-46 Editing a log template



- In the **Options** area, you can see the names of variables that can be added. Select the desired variables and click > to add them to the **Selected** list. Then, you can see the selected variables below **Keyword Change**.
- Below **Selected** are the selected fields. By ticking ☐ before each field and clicking <, you can move the selected fields to the **Options** list.
- Below **Keyword Change** are the selected keywords. You can only change the keyword strings on the left of the equal sign.

Step 4 Click **OK** to return to the previous page.

----End

9.6.7 KAFKA

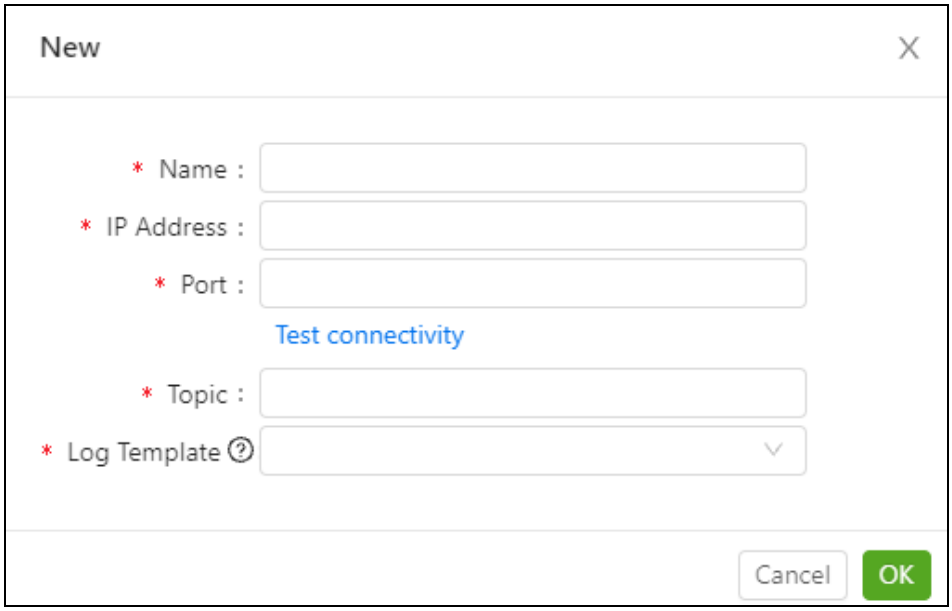
NIPS supports reporting logs to a third-party platform via Kafka.

Up to five Kafka servers can be configured. To configure a Kafka server, follow these steps:

Step 1 Choose **System** > **Central Manager** > **KAFKA**.

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

Figure 9-47 Adding a kafka server



Step 3 Set parameters.

Table 9-15 Parameters for configuring a Kafka server

Parameter	Description
Name	Name of the new Kafka server.
IP Address	IP address of the new Kafka server.
Port	Port of the Kafka server.
Topic	Topic to which the Kafka message belongs.
Log Template	Can be selected from the drop-down list.

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

Step 5 Click **Commit** in the quick access bar to make the settings take effect.

----End

9.7 Service Subscription

This section describes the functions concerning license and care service.

9.7.1 License

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 requires users to pay a specified amount of money for the use of the device. It is mainly used for controlling upgrade services during the authorized time period.

  – After the authorized update period for the engine software expires, the update page automatically disappears. In this case, neither the engine software nor various libraries can be updated.

  – If the authorized update period for the engine software is still valid and those for other databases (system rule database, virus database, threat intelligence databases, URL category databases, and geodatabases) expire, the expiring databases cannot be upgraded.

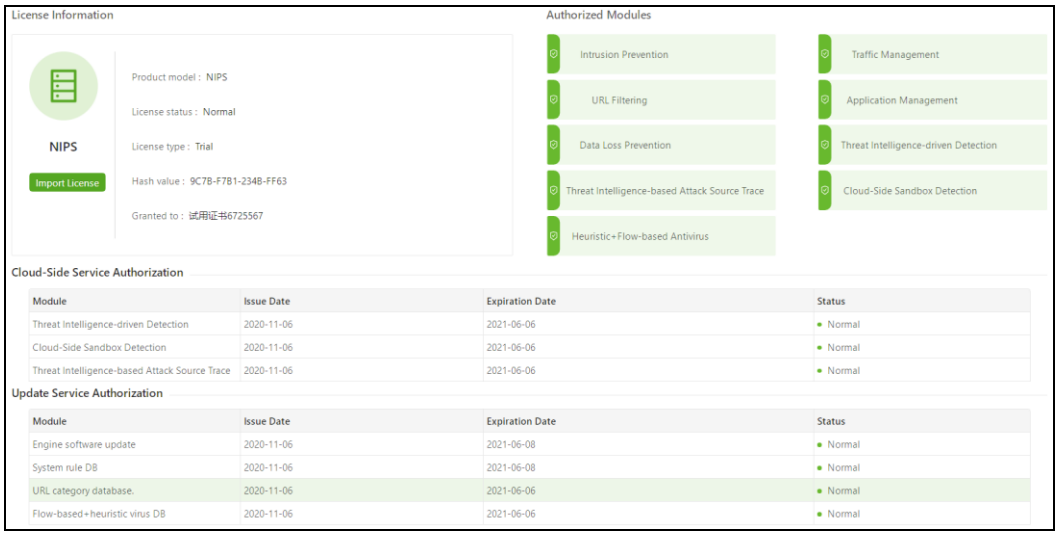
  After a paid license expires, other databases of earlier versions remain valid, users can still use the security detection function and view logs.

Viewing License Status

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

Step 1 Choose **System > Service Subscription > License**.

Figure 9-48 Viewing license information



Step 2 View license information.

Table 9-16 Parameters on the License page

Parameter		Description
License Information	Product model	Indicates the product model covered by this license.
	License status	Indicates the license status. **Normal** indicates that a valid license has been imported and the system can be used. **Expired** indicates that the

Parameter		Description
		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. • **Paid**: After this type of license expires, users can still use NIPS, but cannot update it.
	Hash value	Device hash.
	Granted to	Indicates users that are entitled to use this NIPS.
Authorized Modules		Include the modules that have been authorized and have not been authorized. Authorized modules can be used even if the upgrade service expires. However, the working of modules depends heavily on various databases. If these databases cannot be updated due to the expiration of the update service, these modules will be unable to function properly. Unauthorized modules cannot function properly.
Cloud-side Service Authorization		Indicates the issue date, expiration date, and status of the upgrade service authorized by NSFOCUS Cloud for the following purchased modules: • **Threat Intelligence-driven Detection**: indicates the authorized service period and status of the threat intelligence module. • **Cloud-Side Sandbox Detection**: indicates the authorized service period and status of the cloud-side sandbox detection module. • **Threat Intelligence-based Attack Source Trace**: indicates the authorized service period and status of the cloud-side NTI connection. 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.
Update Service Authorization		Indicates the issue date, expiration date, and status of the update service authorized for the purchased modules. If the current system time is beyond the authorized service period, the system cannot update services, but databases of earlier versions remain valid. Within the authorized period specified with **Issue Date** and **Expiration Date**, the databases or software can be properly updated. • **Engine software update**: indicates the authorized service period and status of the device engine. • **System rule DB**: indicates the authorized service period and status of network intrusion rules, application rules, and sensitive data rules. • **URL category database**: indicates the authorized service period and status of URL category rules. • **Flow-based+heuristic virus DB**: indicates the authorized service period and status of flow-based and heuristic virus databases. Note

Parameter	Description
	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.

----End

Importing a License

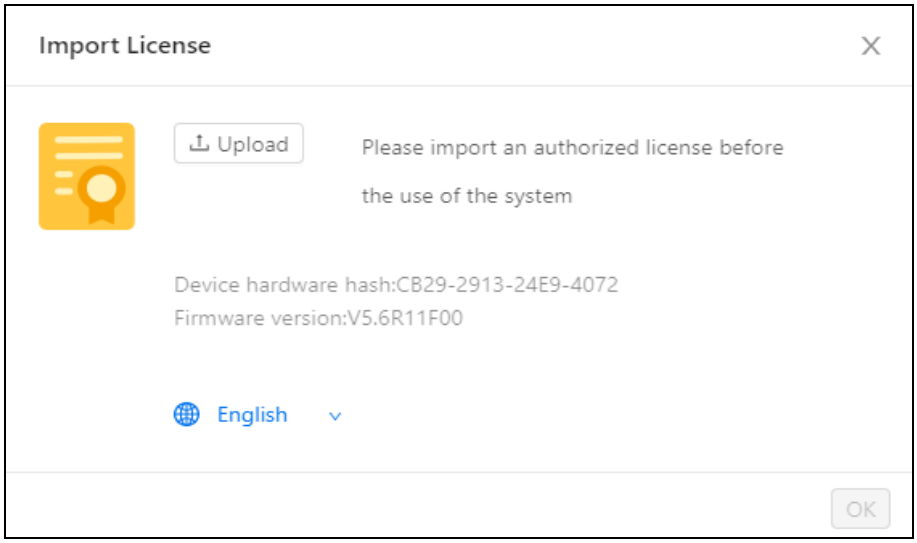
During the first login, you must import a license; otherwise, you cannot use NIPS.

To import a license, follow these steps:

Step 1 Choose **System** > **Service Subscription** > **License**.

Step 2 Click **Import License**.

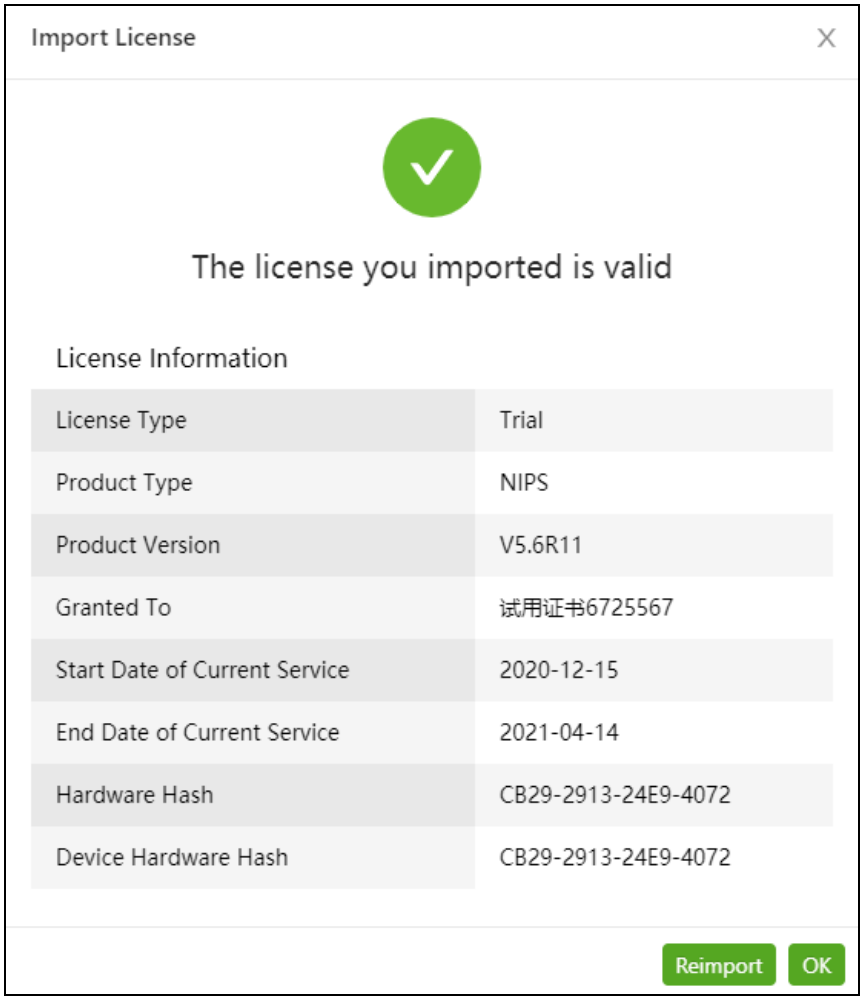
Figure 9-49 Importing a license



Step 3 Click **Upload**, select the license file (*.lic), and click **OK**.

A dialog box appears, as shown in Figure 9-50, asking you to confirm your operation.

Figure 9-50 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 **Reimport** and repeat the preceding steps.

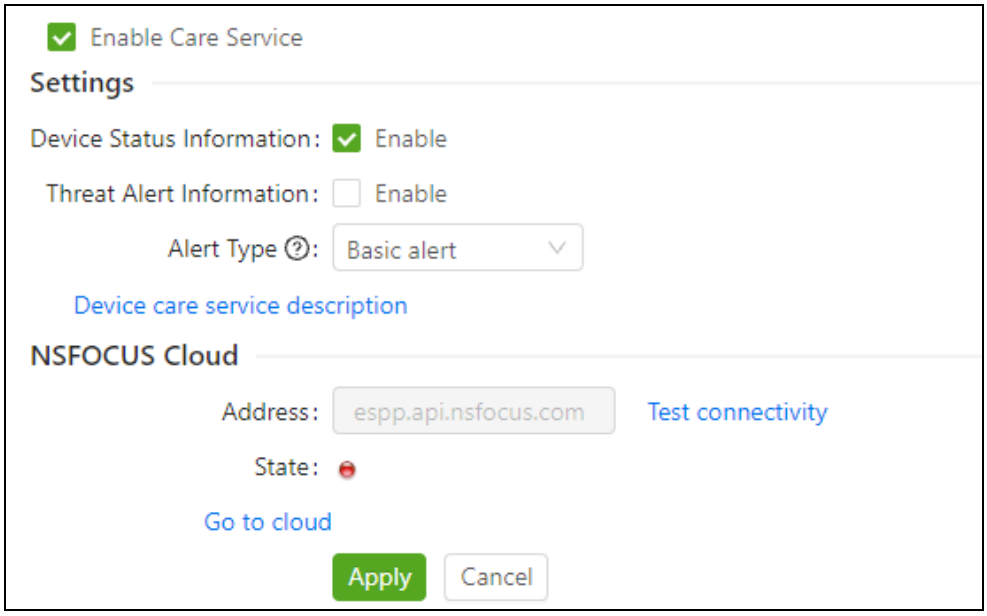
----End

9.7.2 Care Service

After the device care service is enabled, NIPS sends alert messages generated on it to NSFOCUS Security Manager (a mobile app) in real time and informs the emergency response team of any faults detected in real time. The device care service is enabled on NIPS by default.

Step 1 Choose **System** > **Service Subscription** > **Care Service**.

Figure 9-51 Care service



Step 2 Test the reachability of NSFOCUS Cloud.

Click the text link **Test connectivity** to test whether NIPS can be properly connected to NSFOCUS Cloud.

Step 3 In the area shown in Figure 9-51, select the **Enable Care Service** check box to enable the device care service.

Step 4 Check the connection state.

After the care service is enabled, as long as you ensure the connectivity between NIPS and NSFOCUS Cloud, NIPS will be automatically connected to NSFOCUS Cloud. You can check the connection state via the status icon. State: indicates that NIPS is connected to NSFOCUS Cloud., as shown in Figure 9-52.

Step 5 Set the alert type to determine which fields are included in security event logs that are to be uploaded to NSFOCUS Cloud.

Alert Type has the following values:

- **Basic alert**: uploads logs as is. This is the default setting.
- **Custom alert**: allows you to specify which fields of logs to upload.

Step 6 Click **Apply** to make the setting take effect.

Step 7 View device information via either of the following methods:

- Log in to NSFOCUS Cloud: Click the link text **Go to cloud** to open the login page (Figure 9-52) of NSFOCUS Cloud. After login, you can view device information. You can use one of the following accounts to log in to NSFOCUS Cloud:
  - **New account**: Sign up a new account, which can manage multiple devices.
  - **Existing account**: Use an existing account, which can manage multiple devices.
  - **Default account**: 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.

----End

9.8 Troubleshooting

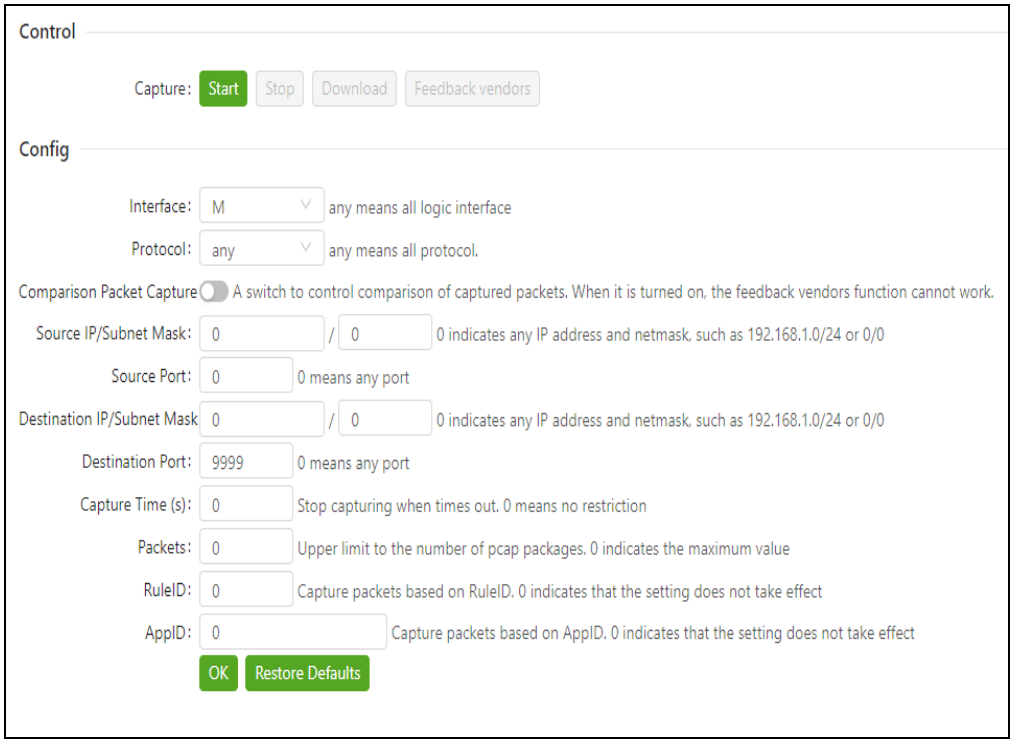
Under **System** > **Troubleshooting**, you can view such information as network connections and network interface card (NIC) status. For example, when an exception occurs, you can use the ping or traceroute tool to perform diagnosis and view related information.

9.8.1 Packet Capturing

NIPS allows users to capture packets directly from device interfaces for analysis and debugging of problems with network deployment. To capture packets, follow these steps:

Step 1 Choose **System** > **Troubleshooting** > **Packet Capturing**.

Figure 9-52 Packet capturing



Step 2 Configure packet capturing parameters.

Table 9-17 Parameters for configuring a packet capturing 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.

Parameter	Description
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 compare captured packets. 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 **OK** 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 capturing process, you can click **Stop** to terminate the ongoing task.

Step 6 Click **Download** to download the packet capturing file to a local disk drive for analysis.

Step 7 Click **Feedback vendors** to send the packet capturing file to NSFOCUS Cloud.

----End

9.8.2 Packet Playback

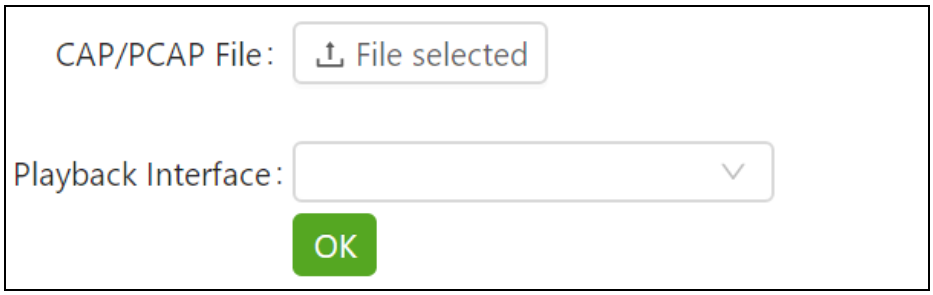
NIPS provides the function of reading packet capture files through the monitoring interface. Users can analyze network data based on these files.

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. For details about the configuration method, see Interface Setting.

To perform a playback test, follow these steps:

Step 1 Choose **System** > **Troubleshooting** > **Packet Playback**.

Figure 9-53 Packet playback



Step 2 Click **File selected**, 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** and check the playback data.

----End

9.8.3 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 promptly and conveniently.

- Hardware inspection objects

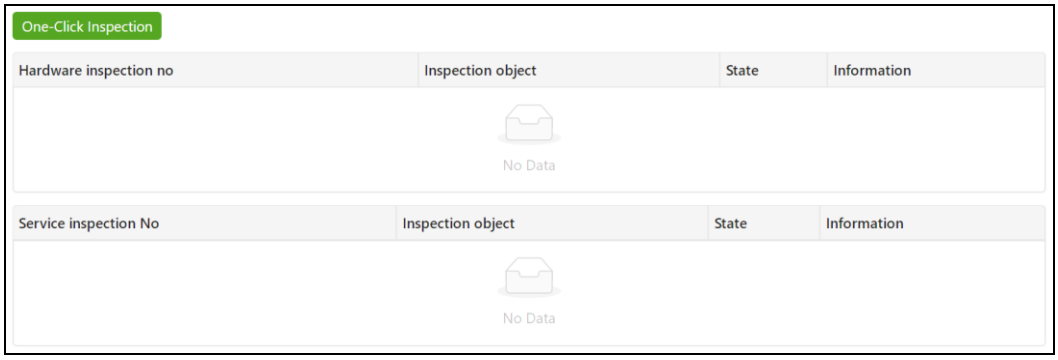
  CPU, memory, disk drives, management interfaces, and working interfaces
- Service inspection objects

  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** > **Troubleshooting** > **One-Click Inspection**.

Figure 9-54 One-click inspection

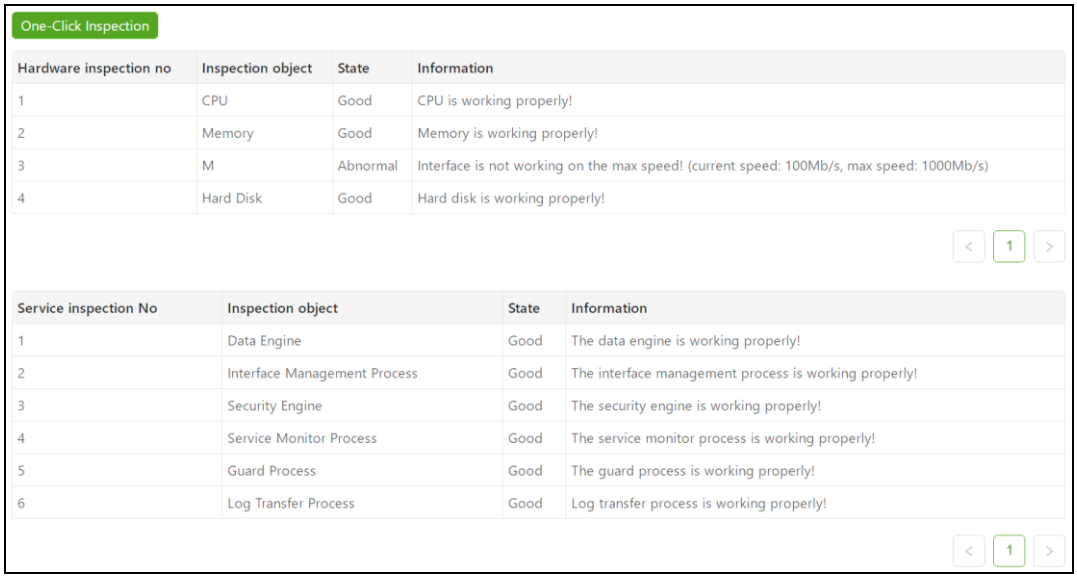


Step 2 Click **One-Click Inspection**.

The system starts inspecting hardware and services.

The inspection will take some time. Please wait patiently. Figure 9-55 shows the inspection result. Hardware components or services in abnormal state are displayed in red. The **Information** column provides details about the cause of such anomalies.

Figure 9-55 Inspection result



One-Click Inspection

Hardware inspection no	Inspection object	State	Information
1	CPU	Good	CPU is working properly!
2	Memory	Good	Memory is working properly!
3	M	Abnormal	Interface is not working on the max speed! (current speed: 100Mb/s, max speed: 1000Mb/s)
4	Hard Disk	Good	Hard disk is working properly!

Service inspection No	Inspection object	State	Information
1	Data Engine	Good	The data engine is working properly!
2	Interface Management Process	Good	The interface management process is working properly!
3	Security Engine	Good	The security engine is working properly!
4	Service Monitor Process	Good	The service monitor process is working properly!
5	Guard Process	Good	The guard process is working properly!
6	Log Transfer Process	Good	Log transfer process is working properly!

----End

9.8.4 Remote Diagnosis

Choose **System** > **Troubleshooting** > **Remote Diagnosis**. Then you can turn on the **Remote Diagnosis** 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.

9.8.5 Network Tools

Network tools include Ping and Traceroute.

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 9-56.

Figure 9-56 Ping result

Traceroute

Traceroute is used to check 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 9-57

Figure 9-57 Traceroute result

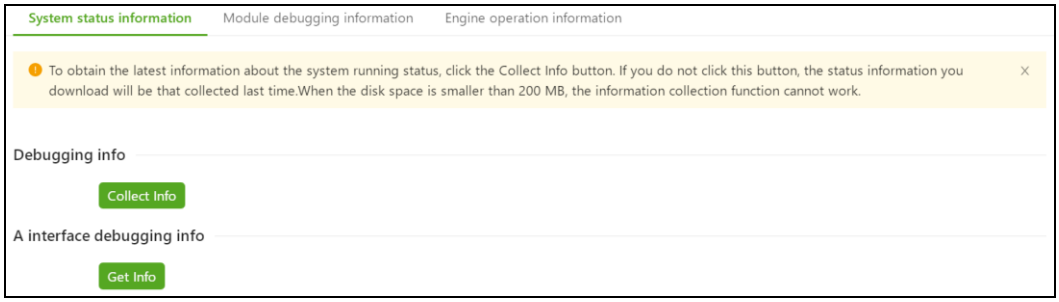
9.8.6 Diagnostics Trace

NIPS allows you to collect the latest information about its running status, which helps locate problems quickly and effectively.

System Status Information

Choose **System** > **Troubleshooting** > **Diagnostics Trace** > **System status information**.

Figure 9-58 System status information

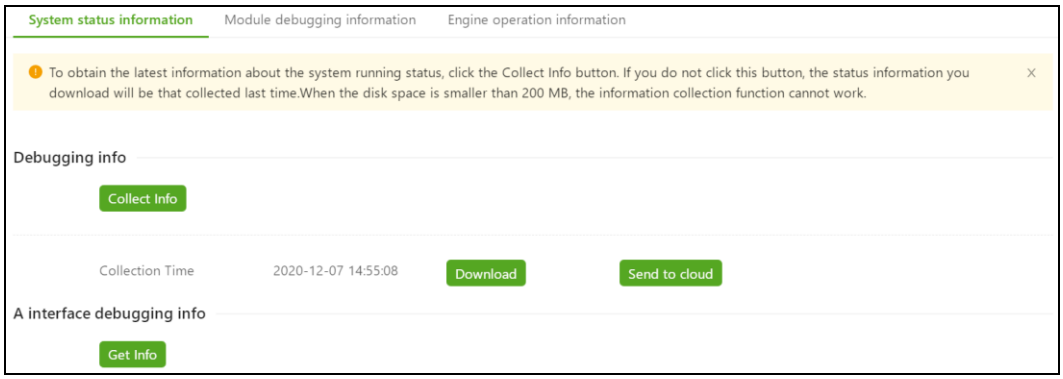


Collecting System Status Information

Step 1 Click **Collect Info**.

NIPS starts collecting the latest information about the system running status. The page then displays the time when system running status information is collected, as shown in Figure 9-59.

Figure 9-59 System status information collection



Step 2 Click **Download** to download the system running status information to a local disk drive for future reference and analysis.

Step 3 Click **Send to cloud** to send the collected information about the device running status to NSFOCUS Cloud.

----End

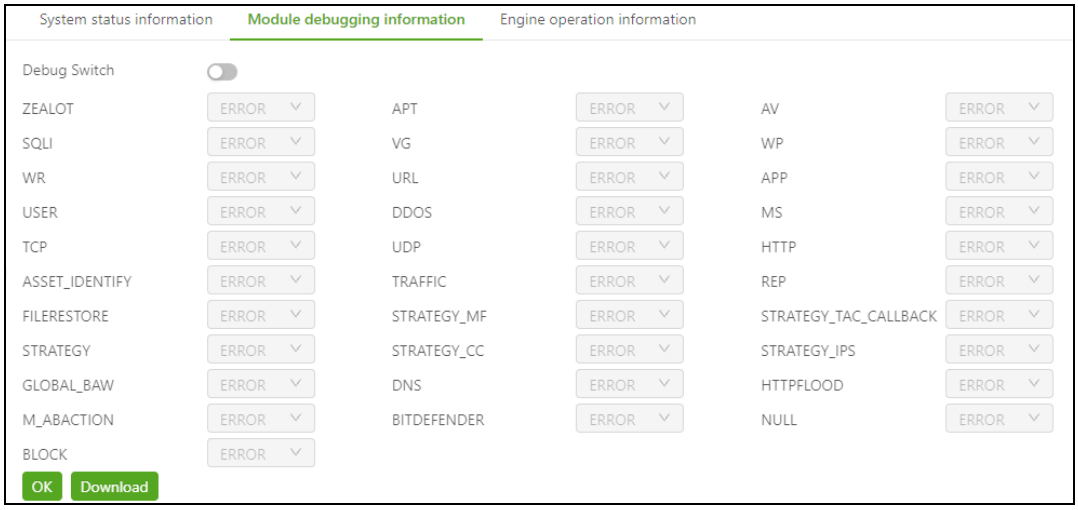
An Interface Debugging Information

When the connection of NIPS to NSFOCUS Cloud, ESPC, or BSA becomes faulty, you can click **Get Info** to save debugging information to a local hard drive for technical support personnel's analysis of the fault.

Module Debugging Information

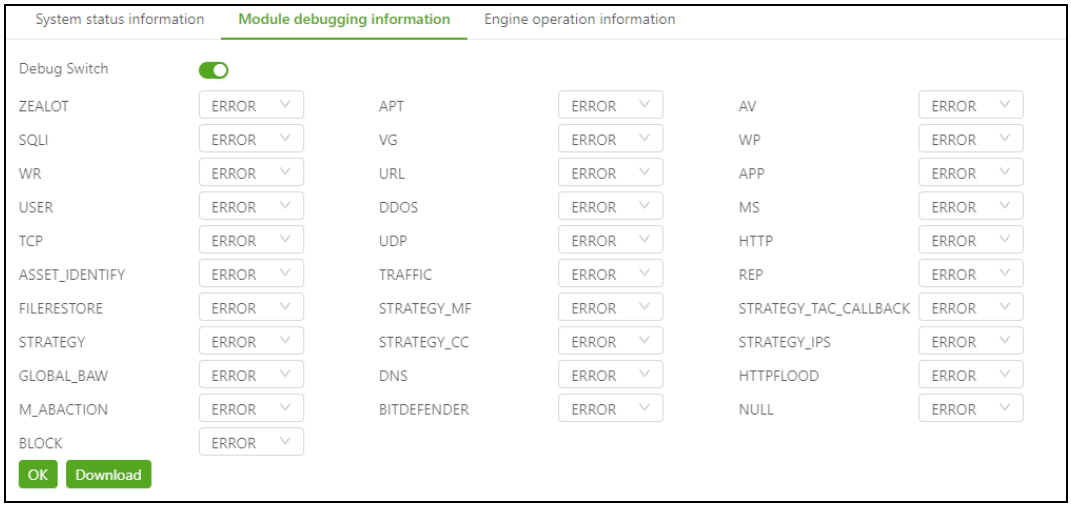
Step 1 Choose **System > Troubleshooting > Diagnostics Trace > Module debugging information**.

Figure 9-60 Module debugging information



Step 2 Click on the right of **Debug Switch** to enable the debugging function.

Figure 9-61 Turning on the debug switch



Step 3 Set debugging parameters of various modules.

Step 4 Click **OK** to return to the previous page.

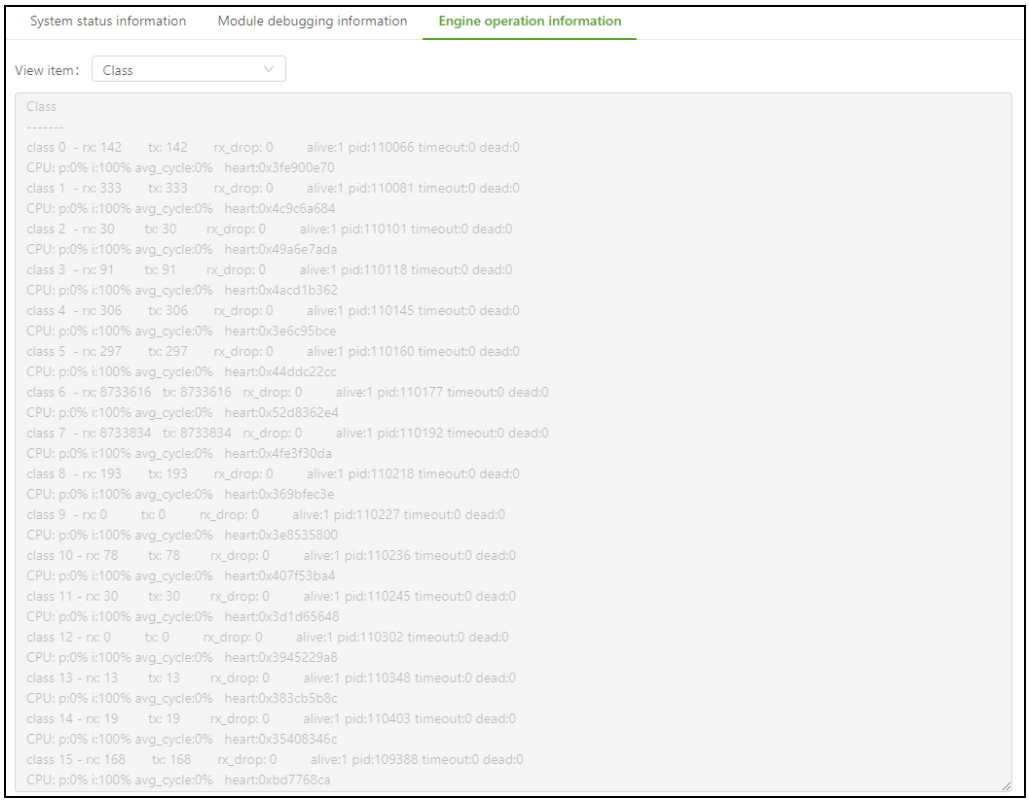
Step 5 Click **Download** to save debugging information to a local hard drive.

----End

Engine Operation Information

Step 1 Choose **System** > **Troubleshooting** > **Diagnostics Trace** > **Engine operation information**.

Figure 9-62 Engine operation information



Step 2 Select an item from the **View item** drop-down list to check information in the below table.

----End

9.8.7 Network Connections

You can view the network status, including the system's network connections and routing table.

System Network Connection

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

- The **System network connection** page displays network connection information, including the protocol and port, as shown in Figure 9-63.

Figure 9-63 System network connection

System network connection | System routing table

```
CF card capacity  8GB

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 0.0.0.0:62026           0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:5355            0.0.0.0:*               LISTEN
tcp        0      0 10.14.4.233:10002       0.0.0.0:*               LISTEN
tcp        0      0 0.0.0.0:695             0.0.0.0:*               LISTEN
tcp        0      0 10.14.4.233:5050        0.0.0.0:*               LISTEN
tcp        0      0 10.14.4.233:6092        221.122.179.2:5050      ESTABLISHED
tcp        0      0 10.14.4.233:50022       10.14.76.25:58605       ESTABLISHED
tcp        0      0 10.14.4.233:50022       10.8.12.4:65015         ESTABLISHED
```

- 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.

System Routing Table

Choose **System > Troubleshooting > Network Connections > System routing table** to view real-time routing information on the current device.

Figure 9-64 System routing table

System network connection | System routing table

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.14.255.254   0.0.0.0         UG    0      0        0 M
10.14.0.0       0.0.0.0         255.255.0.0     U     0      0        0 M
192.168.2.0     0.0.0.0         255.255.255.0   U     0      0        0 H1
Kernel IPv6 routing table
Destination                     Next Hop                   Flag Met Ref Use If
localhost/128                   [::]                       Un   0   1     9 lo
fe80::a35:71ff:fe11:4783/128    [::]                       Un   0   1     3 lo
fe80::a35:71ff:fe11:4784/128    [::]                       Un   0   1     3 lo
fe80::a35:71ff:fe11:4785/128    [::]                       Un   0   1     3 lo
fe80::a35:71ff:fe11:4786/128    [::]                       Un   0   1     3 lo
ff00::/8                        [::]                       U    256 0     0 G1/1
ff00::/8                        [::]                       U    256 0     0 G1/2
ff00::/8                        [::]                       U    256 0     0 G1/3
```

9.8.8 Hardware

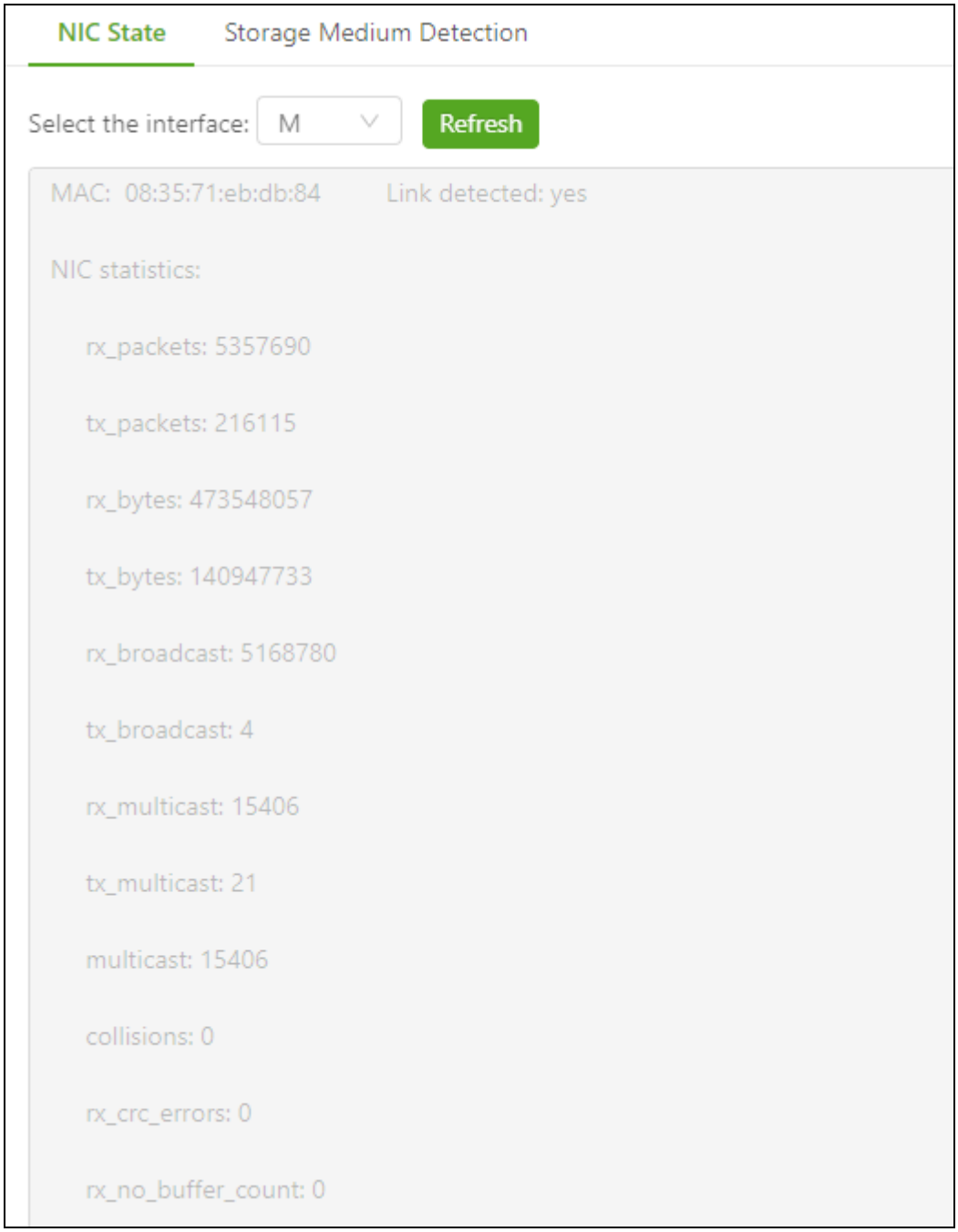
Under the **Hardware** module, you can view the NIC state and check the storage medium.

NIC State

The **NIC State** page displays NIC status information. Users can determine whether a network exception is caused by a NIC fault from information on this page.

Choose **System > Troubleshooting > Hardware > NIC State**.

Figure 9-65 NIC State



Select an interface from the drop-down list and then click **Refresh** to view the status of the specified interface.

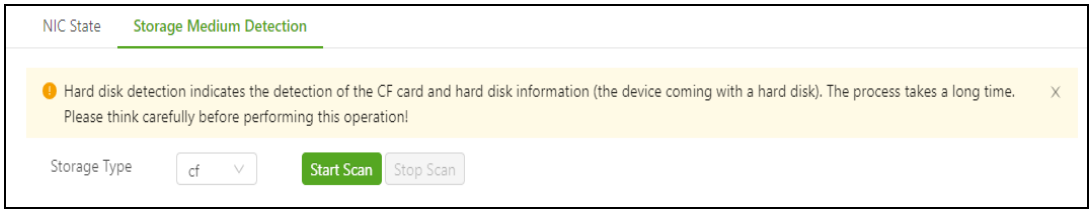
Storage Medium Detection

The **Storage Medium Detection** tab page allows you to check CF card information. If the device has a hard disk, NIPS can also check hard disk information.

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

Step 1 Choose **System** > **Troubleshooting** > **Hardware** > **Storage Medium Detection**.

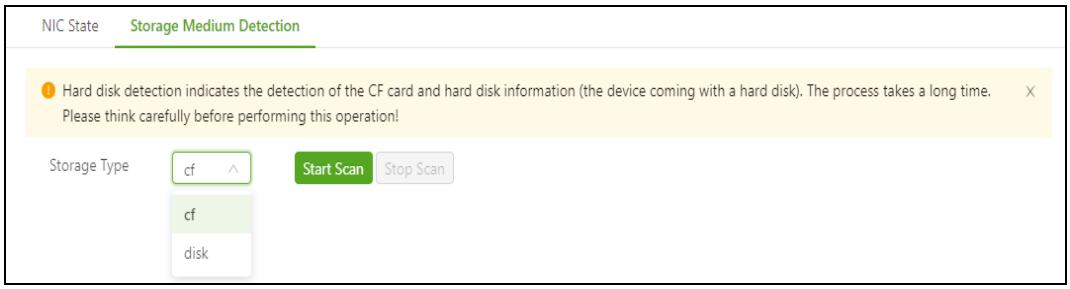
Figure 9-66 Storage medium detection information



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

- If the device does not have a hard disk, only **cf** 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 9-67 Hard disk maintenance page – device with a hard disk



Step 3 Click **Start Scan**.

The hardware detection result is displayed.

----End

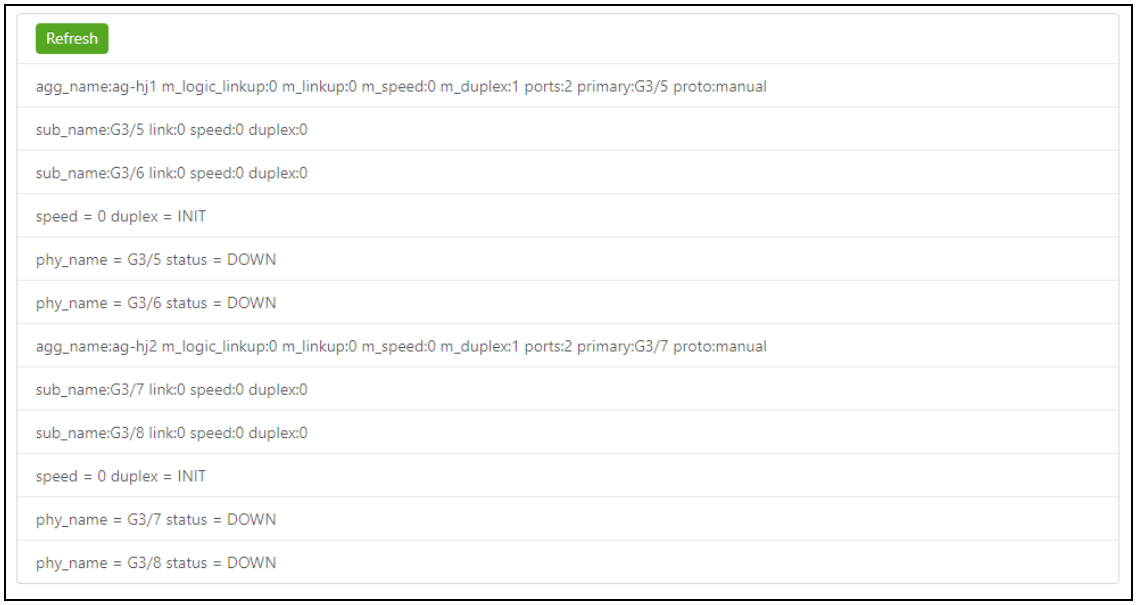
9.8.9 Aggregation Status

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 8.1.1.2 Creating an Aggregation Interface.

Step 1 Choose **System** > **Troubleshooting** > **Aggregation**.

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

Figure 9-68 Aggregation status



Step 2 (Optional) Click **Refresh** to manually refresh the aggregation status.

----End

9.8.10 Forwarding Information

The **Forwarding Information** page is used to check whether specified switch information exists, query real-time route information, and check whether layer-2 loops exist, and view and how to view all route information.

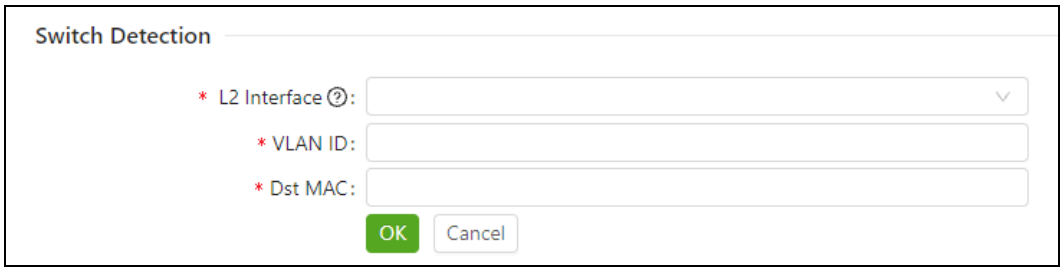
Switch Detection

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** > **Troubleshooting** > **Forwarding Information**.

Figure 9-69 Switch Detection area



Step 2 Configure parameters.

Table 9-18 Parameters for enabling the switch detection function

Parameter	Description
L2 Interface	Specifies the layer 2 interface that connects to the destination host.
VLAN ID	Specifies the ID of the VLAN that the destination host belongs to.
Dst MAC	Specifies the MAC address of the destination host.

Step 3 Click **OK** to check whether the MAC address information of the specified layer 2 switch already exists.

----End

Route Detection

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

Step 1 Choose **System** > **Troubleshooting** > **Forwarding Information**.

Figure 9-70 Querying information about the specified route

Step 2 Set source and destination IP addresses.

Step 3 Click **OK**.

----End

Layer 2 Loop Detection

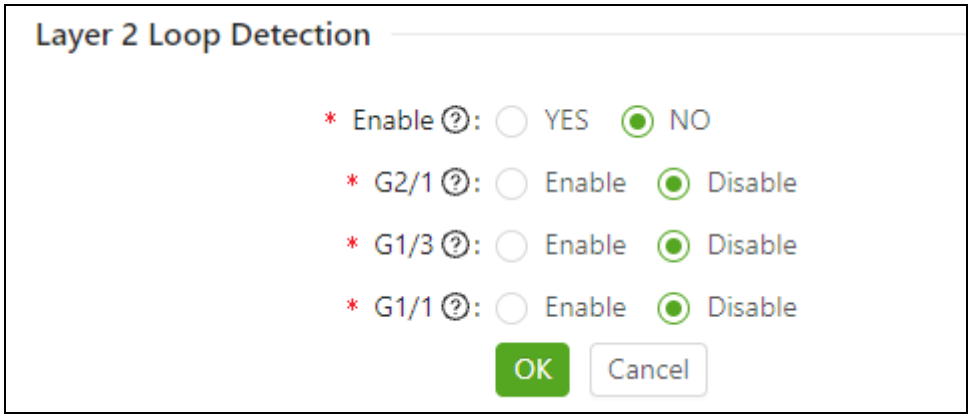
The layer 2 loop detection tool is used to check whether a loop exists on the layer 2 link.

Note	When the layer 2 loop testing function is enabled for a specific interface, the system logs the detected layer 2 loop information in running logs. For how to view running logs, see section 5.3.1 Running Log.

To enable the layer 2 loop testing function, follow these steps:

Step 1 Choose **System** > **Troubleshooting** > **Forwarding Information**.

Figure 9-71 Layer 2 Loop Detection area



Step 2 Configure parameters.

a. Select **Yes** for **Enable** 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 **Enable**.

c. Click **OK**.

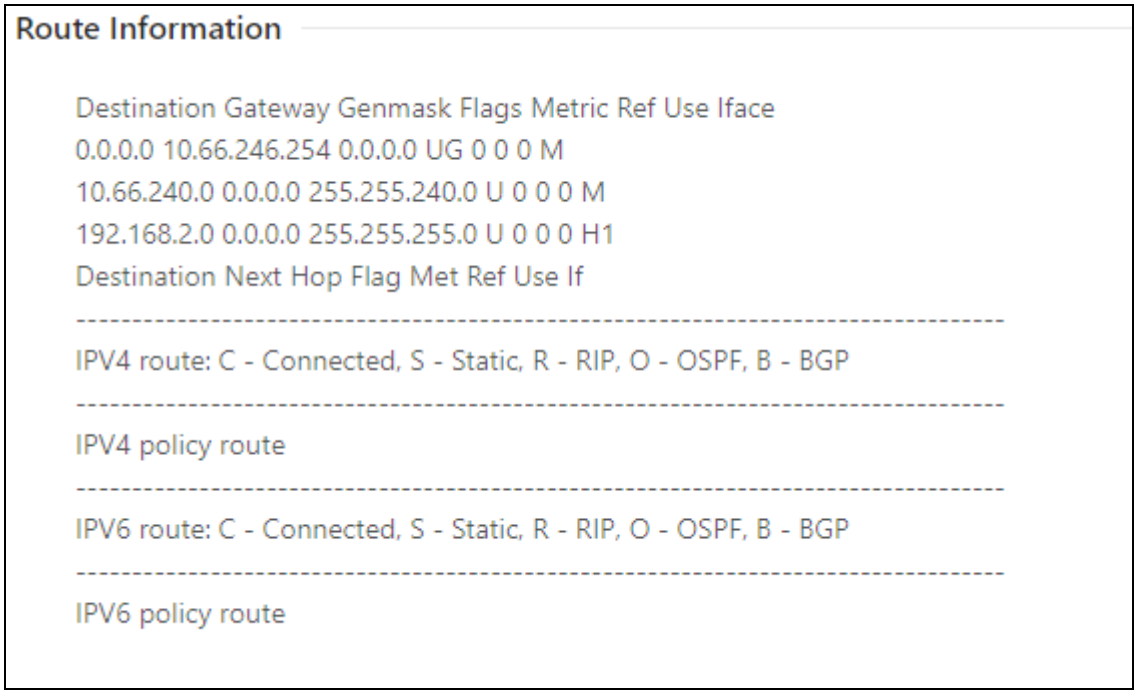
----End

Route Information

This tool is used for obtaining route information in real time.

Choose **System** > **Troubleshooting** > **Forwarding Information** to view the route information

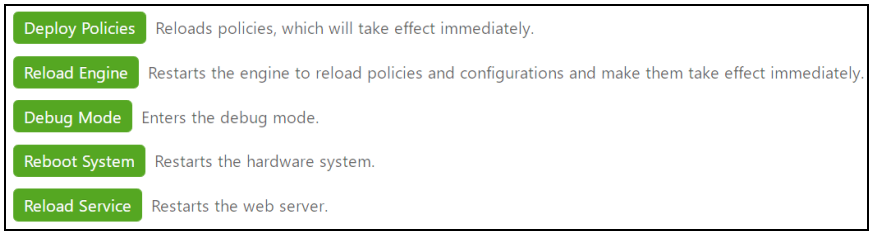
Figure 9-72 Route information



9.9 System Control

Choose **System > System Control**.

Figure 9-73 System control



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

- Click **Deploy Policies**.

  Click **Deploy Policies** to reload all policies and engine settings, except interface settings, and make them take effect immediately. The policies here include security policies, DoS protection policies, server outreach policies, sandbox collaboration policies, threat intelligence policies, global black/whitelist policies, IP/MAC binding policies, user management policies, bandwidth management policies, traffic analysis policies, and geodatabases.

- Click **Reload Engine**.

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

- Click **Debug Mode**.

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

- Click **Reboot System**.

  Click **Reboot System** to restart the hardware system of NIPS.

- Click **Reload Service**.

Click **Reload Service** to restart the web server.

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

10 Audit Log

Only the **auditor** user has the privilege of viewing audit logs.

Audit logs include login logs, operation logs, system running logs, and upgrade logs.

Log in to the system as **auditor**, and choose **Log** > **Audit Log**. Set the query conditions and click **Search** to view audit logs that meet query conditions.

A 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 user interface.

A.1 Log In to the Console User Interface

The following section describes how a console user accesses the console user interface of NIPS.

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

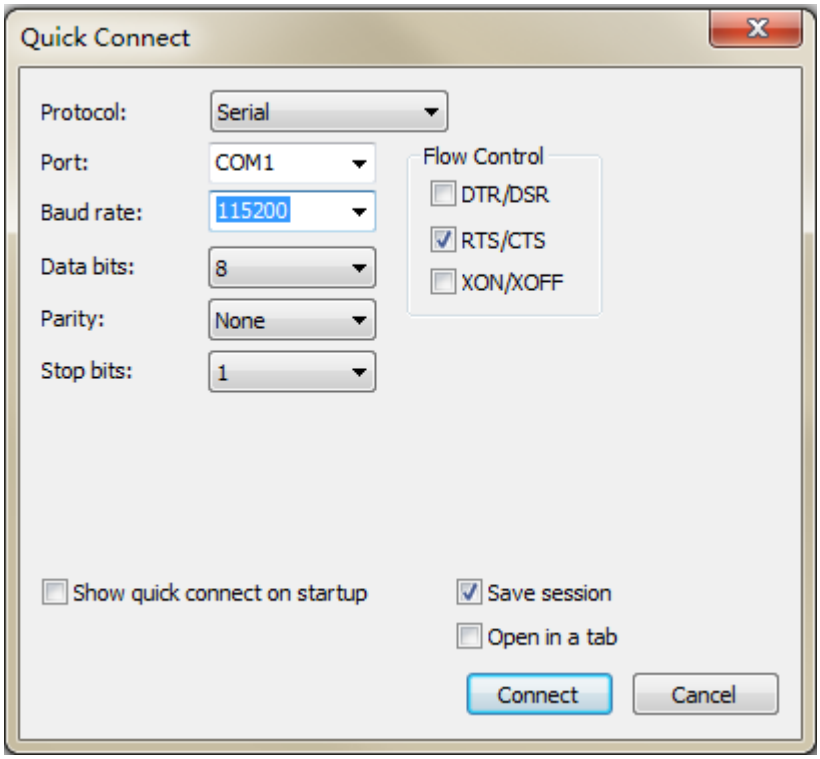
The following takes SecureCRT as an example to describe how to log in to the console user interface of NIPS:

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

Step 2 Configure quick 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 A-1.

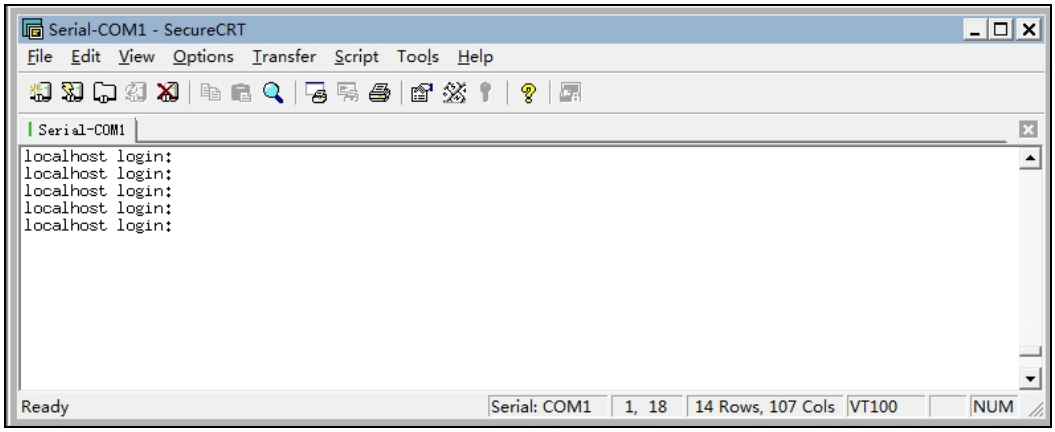
Figure A-1 Configuring a quick connection



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

The console login page appears.

Figure A-2 Console login window



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 A-3 shows the language selection page.

Figure A-3 Selecting a language

```
+--- Select Menu Language ---+
|+-------------------------+|
||1.中文                    ||
||2.English                ||
||                         ||
|+-------------------------+|
|+-------------------------+|
||Select this for using     ||
||English later            ||
||                         ||
||                         ||
||                         ||
||                         ||
|+-------------------------+|
+----------------------------+
```

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 A-4 Main menu for console-based management

```
|+-------------------------------------------------------------------------+
||1.Check system information                                               |
||2.Diagnostic Tools                                                       |
||3.Maintenance Tools                                                      |
||4.System initialization                                                  |
||5.Restart the system                                                     |
||6.Shutdown the system                                                    |
||0.Exit                                                                   |
||                                                                         |
||                                                                         |
||                                                                         |
|+-------------------------------------------------------------------------+
|+-------------------------------------------------------------------------+
||Check system information, which helps you to check system configuration  |
||and status.                                                              |
||                                                                         |
||                                                                         |
||                                                                         |
||                                                                         |
||                                                                         |
|+-------------------------------------------------------------------------+
```

----End

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

Table A-1 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 an operation.
Enter	Confirms an operation.
Tab	Switches between an input box, the **OK** button, and the **Cancel** button.
BackSpace	Deletes the character to the left of the cursor.

A.2 Configuration Parameters

The following sections describe how to configure relevant parameters after logging in to the console user interface.

A.2.1 Viewing System Information

You can perform the following operations:

- Viewing interface configuration

  Views information about all network interfaces of the system, including interface names, IP addresses, management IP addresses, gateway, 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 Interfaces.)
- Viewing license information

  You can view the engine license of NIPS, including the license status, license type, date of issuance, and expiry date.
- Setting the IP address of the management interface

  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 A-5 Viewing system information

```
+---------------------- (Com Program Version 5.6.1187) ------------------------+
|+------------------------- Check system information -------------------------+|
||+-------------------------------------------------------------------------+||
|||1.Show interface configuration                                            |||
|||2.Show certificate information                                            |||
|||3.Set Interface Ip Address                                                |||
|||4.Start Important Process                                                 |||
|||5.Set Device Clock                                                        |||
|||6.Set Device TimeZone                                                     |||
|||7.Set Login Timeout                                                       |||
|||8.Produce Hardware ID                                                     |||
||+-v(Down)---------------------------------------------------------------+||
||+-------------------------------------------------------------------------+||
|||Show present interface ip and manageable ip,zone etc                      |||
|||                                                                          |||
|||                                                                          |||
|||                                                                          |||
|||                                                                          |||
|||                                                                          |||
||+-------------------------------------------------------------------------+||
|+-----------------------------------------------------------------------------+|
+-------------------------------------------------------------------------------+
```

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 License.

A.2.2 Using Diagnostic Tools

As shown in Figure A-6, 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 A-6 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 Troubleshooting.

A.2.3 Using Maintenance Tools

As shown in Figure A-7, you can 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.
- Resetting web system users

  You can reset system administrator information that has 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.
- Cleaning up 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 after pressing **Enter** and entering the submenu.

- 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.

- Resetting interfaces

  You can reset interface counts and change the up/down status of the interfaces with caution.

- Returning to the previous menu

  After performing the desired operations, you can return to the previous menu.

Figure A-7 Maintenance tools

```
+---------------------- (Com Program Version 5.6.18569) ----------------------+
|+---------------------------- Maintenance Tools ----------------------------+|
||+-----------------------------------------------------------------------+||
|||1.Set Administrator password                                            |||
|||2.Reset Web System User                                                 |||
|||3.Clean up temporary files                                              |||
|||4.Close Remote Assist                                                   |||
|||5.Forbid Ping(Icmp)                                                     |||
|||6.Open Force Hardware Bypass                                            |||
|||7.Interface reset                                                       |||
|||0.Exit to previous menu                                                 |||
||+-----------------------------------------------------------------------+||
||+-----------------------------------------------------------------------+||
|||Set Administrator password for serial port log in.Not more than 32 byte. |||
|||                                                                        |||
|||                                                                        |||
|||                                                                        |||
|||                                                                        |||
|||                                                                        |||
||+-----------------------------------------------------------------------+||
|+-------------------------------------------------------------------------+|
+---------------------------------------------------------------------------+
```

A.2.4 Initializing System Settings

As shown in Figure A-8, 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

  Restoring 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 A-8 System initialization

```
+---------------------- (Com Program Version 5.6.18569) ----------------------+
|+------------------------- 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.

A.2.5 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 A-9 Restarting the system

```
+---------------------- (Com Program Version 5.6.18569) ----------------------+
|+-------------------------------------------------------------------------+|
||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                                                   ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
|+-------------------------------------------------------------------------+|
+-----------------------------------------------------------------------------+
```

A.2.6 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 A-10 Shutting down the system

```
+---------------------- (Com Program Version 5.6.18569) ----------------------+
|+-------------------------------------------------------------------------+|
||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                                                  ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
||                                                                          ||
|+-------------------------------------------------------------------------+|
+-----------------------------------------------------------------------------+
```

A.2.7 Exiting the Configuration Interface

After completing all settings, you can point to **0** and press **Enter** to exit the configuration interface of NIPS.

Figure A-11 Exiting the system

```
+---------------------- (Com Program Version 5.6.18569) ----------------------+
|+-------------------------------------------------------------------------+|
||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.

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

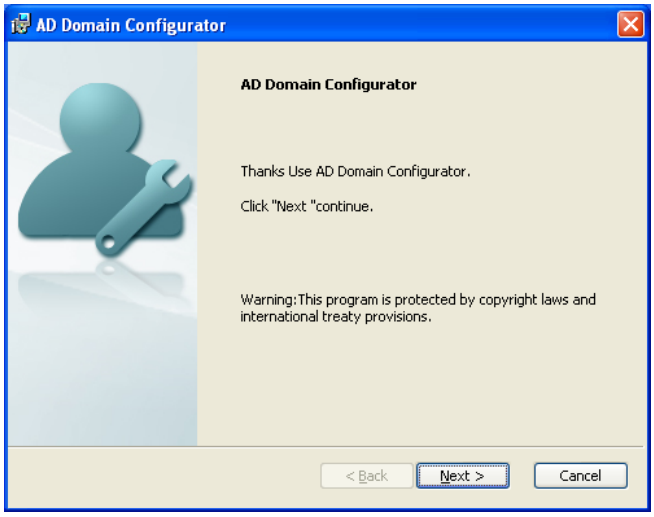
Before installing the AD domain configurator, make the following preparations:

- 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, perform the following steps:

Step 1 Double-click **setup.exe** to start the installation wizard, as shown in Figure B-1.

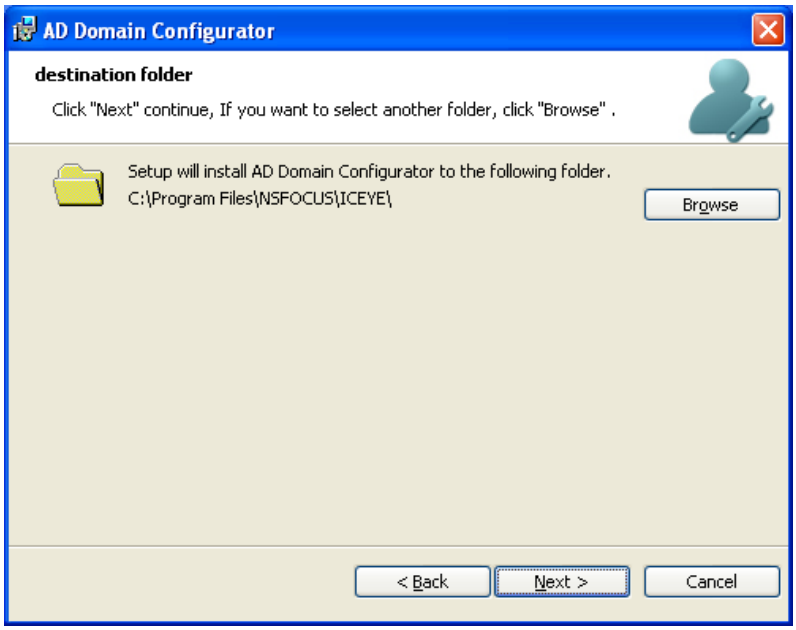
Figure B-1 Starting the installation wizard



Step 2 Click **Next** and select an installation path.

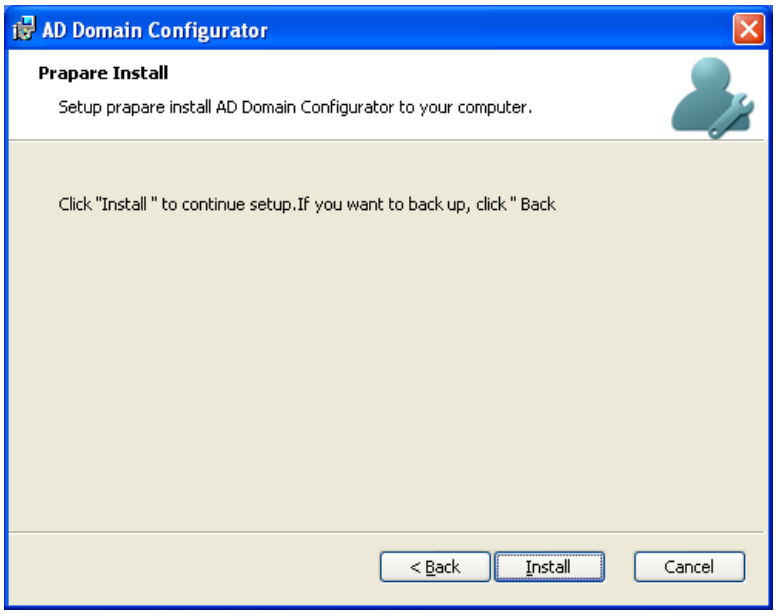
Figure B-2 shows that the default installation path is selected.

Figure B-2 Selecting an installation path



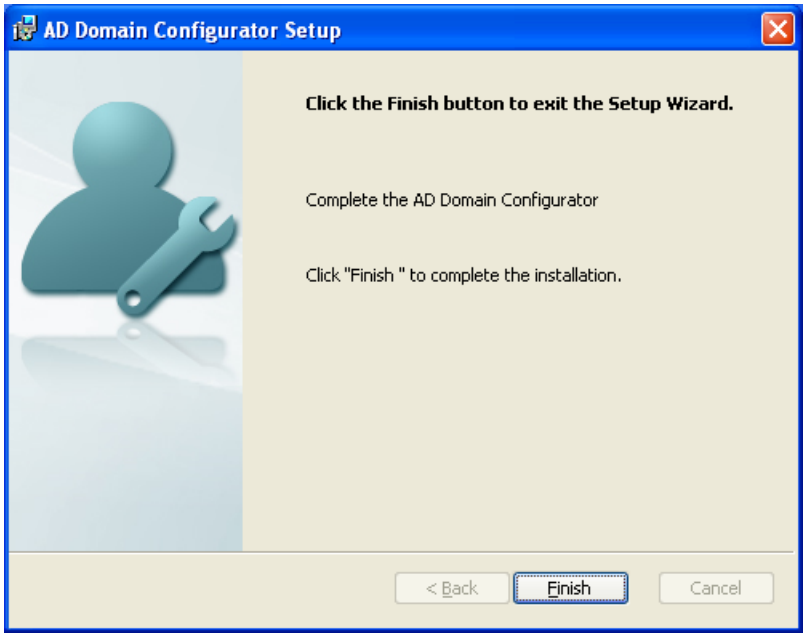
Step 3 Click **Next** to install the software. In the dialog box shown in Figure B-3, click **Install**.

Figure B-3 Starting installation



Step 4 After the installation is complete, click **Finish**.

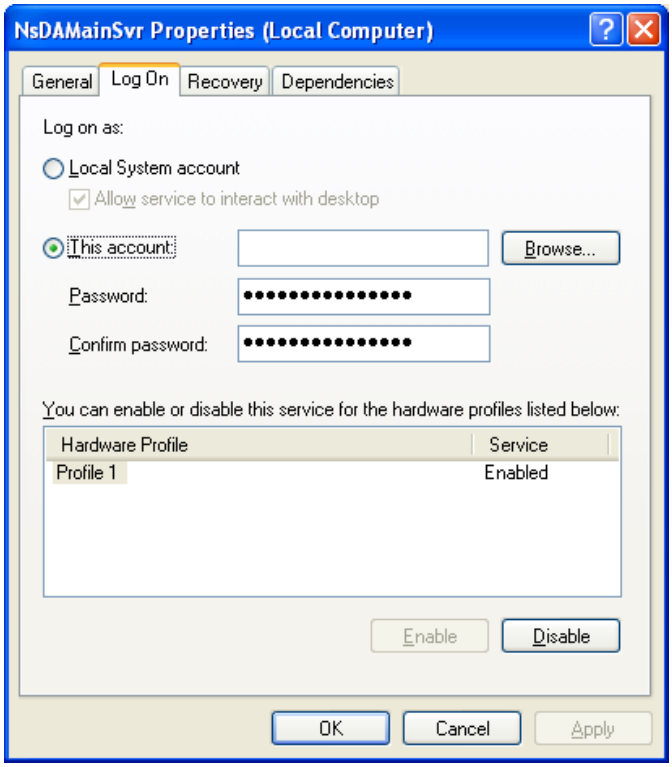
Figure B-4 Completing installation



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.

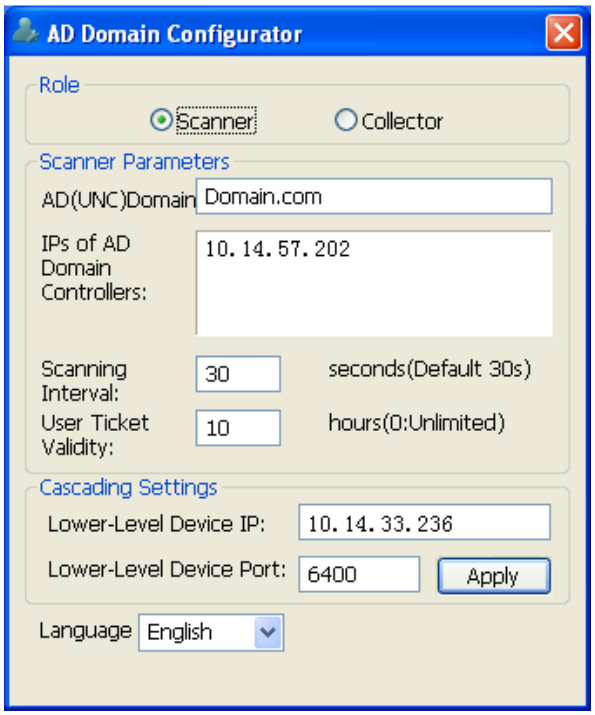
- Collector

  A collector regularly combines and filters user lists received from the scanner and sends them to NIPS.

The configuration procedure is as follows:

Step 1 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 2 Configure parameters in the 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 logged-in users.
User Ticket Validity	Specifies the validity period of user authentication. The default value is **10** hours.
Lower-Level Device IP	Specifies P 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

Default parameters include default interface settings, default administrator accounts, and communication parameters of the console port.

C.1 Default Interface Settings

IP	M: 192.168.1.1 H1: 192.168.2.1 (whether H1 interface 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.)
Netmask	255.255.255.0

C.2 Default Administrator Accounts

	Web Operator	Web Auditor	Console Administrator	ESPC Administrator	BSA Administrator
User Name	admin	auditor	conadmin	admin	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