MAIPU

MPSec MSG4000 Series Firewall

User Manual

Version 1.0

Contents

1 System Management

1.1 Device Management

1.1.1 Local Settings

Set Device Name

The device name is used to identify the device.

Step 1. Select "System > Device Management > Local Settings".

Step 2. Set the device name.

The device name supports Chinese characters, letters, numbers, @, underscore "_", hyphen "-", and dot ".", ranging from 1 to 63 characters.

The modified device name can be found in "Home> System Information".

Step 3. After the settings are complete, click “Apply”.

Set System Time

The system time is the time of the firewall system. If the NTP function is enabled, you do not need to manually modify the system time.

Step 1. Select "System > Device Management > Local Settings".

Step 2. Set the system time.

- Method 1: Click "Native Synchronization", and after the prompt is successful, the system time of the firewall will be synchronized with the current time of the management host used by the administrator immediately. The content of the "Time" text box is changed to the time when the synchronization with the machine is performed.
- Method 2: Manually modify the time and time zone. After modifying the time in the "Time" text box, click "Apply" to change the system time to the set time.

Set DNS

The purpose of setting DNS is to allow the firewall to perform domain name resolution when accessing domain names. For example, when the user configures a domain name address or specifies the feature database upgrade server as domain name, the firewall needs to use DNS. The firewall supports one primary and two secondary DNS servers.

Step 1. Select "System > Device Management > Local Settings".

Step 2. Set the preferred DNS and alternative DNS server addresses.

- Preferred DNS server

  If the DNS server address is provided by the operator, it is recommended to match the egress link operator. If the egress link is Beijing Unicom, the DNS server is recommended to fill in the DNS of Beijing Unicom.

- Alternative DNS server

  An alternative DNS server is enabled when the primary DNS server does not respond.

Step 3. After the settings are complete, click “Apply”.

Set NTP

Set the firewall as an NTP client to synchronize time with an NTP time server. It will take effect only after the NTP service is enabled.

Step 1. Select "System > Device Management > Local Settings".

Step 2. Enable NTP.

Step 3. The NTP service will take effect only after "Enable" is selected.

Step 4. Set the server address or name, and set whether to be the master server.

Step 5. Users can fill in no more than three server addresses or names.

Step 6. Configure the time policy.

When the network is busy, in order to reduce resource waste and ensure the efficiency of time synchronization with the NTP server, the user is required to fill in the time policy when configuring time synchronization.

Parameter	Description
Minimum search time	When the network is normal, the time search time for time synchronization with the NTP server is subject to the configuration of the minimum search time. The unit is 2^n second. The specified range is 3-10, which must be less than or equal to the maximum search time. For example, the user sets the minimum search time to 3. When the network is normal, the device requests the NTP server for time synchronization every 2^3 seconds (that is, 8 seconds).
Maximum search time	When the network is busy, the time search time for time synchronization with the NTP server will be offset to the specified value of the maximum search time by a certain algorithm. The unit is 2^n second. The specified range is 3 to 10. For example, if the user sets the maximum search time to 10, when the network is busy, the time interval for the device to

Parameter	Description
	send query requests to the NTP server will offset to 2^{10} seconds as the delay caused by the busy network increases, until the time interval of the query request increases to 2^{10} second (that is, 1024 seconds). When the network returns to normal, the time interval will be restored to the minimum search time.

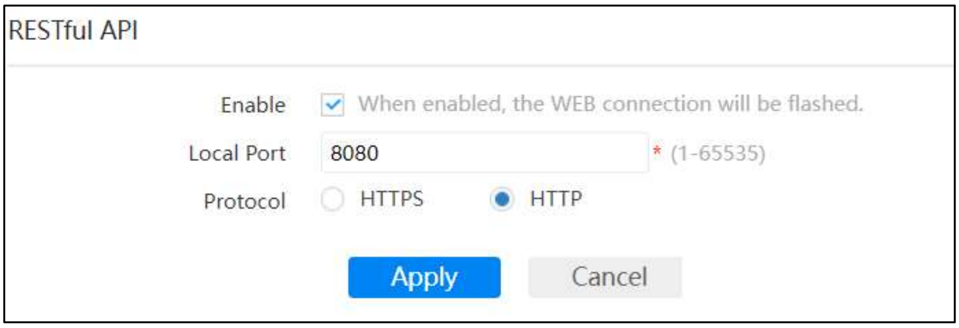
Step 7. After the configuration is complete, click “Apply”.

Set RESTful APIs

The RESTful API is a northbound API interface for third-party clients to call the firewall. By using the RESTful API, third- party clients can manage the configuration of the firewall.

Step 1. Select "System > Device Management > Local Settings".

Step 2. Configure local ports and protocols.



RESTful API

Enable ☑ When enabled, the WEB connection will be flashed.

Local Port 8080 * (1-65535)

Protocol ○ HTTPS ● HTTP

Step 3. Check the “Enable” checkbox. Enable the RESTful API to allow third-party clients to communicate with the firewall.

Step 4. After the configuration is complete, click “Apply”.

1.1.2 Administration Host

The firewall allows users to set the IP address and MAC address of user terminals that can log in and manage the firewall through trusted hosts and trusted MAC addresses, and trust the terminal security management system and SNMP server that actively communicate with the firewall. The administration port is used to set the port number of the login service.

Notes

The configuration of the trusted host and trusted MAC is valid for HTTP, HTTPS, TELNET, SSH and SNMP login methods. The users who log in through the console are not subject to this limitation.

Add Trusted Host

The trusted host function is used to set the IP address of the host that can log in to the firewall and the management services that can be used. After this function is enabled, only hosts within the IP range of trusted hosts can log in to the firewall. This feature is enabled by default. After this function is disabled, the host IPs that log in to the firewall will no longer be restricted, and all IPs can manage the firewall.

The default trusted host IP address of the firewall is 10.0.0.44. When logging in to the firewall for the first time, the user must configure the IP address of the administration host as 10.0.0.44.

Step 1. Select "System > Device Management > Administration Host".

Step 2. On the “Trusted Hosts” page, click “Add”.

Step 3. Set the IP addresses of trusted hosts and allowed services.

Parameter	**Description**
IP address	The IP address range of trusted hosts. Supports IPv4 addresses, IPv4 address ranges, IPv6 addresses, and IPv6 address ranges. For example: 10.10.1.2 represents an IPv4 host; 10.10.1.2-10.10.1.10, representing the IPv4 host address range, all hosts in this range are included; 11::11, representing an IPv6 host; 11::11-11::22, representing the IPv6 host range, all hosts in this range are included.
Description	Add the description for the administration host.
Service	Specifies the service corresponding to the trusted host. Services are divided into: • Device management Trusted hosts are used to log in to manage firewall devices. • SNMP When the firewall device is managed centrally through the smart management and analysis system, it is necessary to set the smart management and analysis system as a trusted host and select the SNMP service. The firewall device sends monitoring data information such as CPU usage rate and memory usage rate to the smart management analysis system through SNMP. • RESTful API The trusted host is a third-party client that manages the firewall through the RESTful API.

Step 4. After the configuration is complete, click “OK”.

Step 5. Check “Enable”.

The firewall enables the trusted host function by default. To disable this function, uncheck "Enable", then the configuration of trusted hosts will not take effect, and all hosts can manage the firewall.

Add Trusted MAC

Users can not only limit the range of hosts that can manage the firewall by IP address, but also limit the range of hosts that can manage the firewall by specifying MAC addresses.

This function is disabled by default. This function must be enabled to take effect. After the trusted MAC is enabled, the MAC address of the login device must be a trusted MAC to manage the firewall.

Step 1. Select "System > Device Management > Administration Host".

Step 2. Click “Trusted MAC”.

Step 3. Click “Add”.

Step 4. Set the MAC address of the trusted host.

The MAC address format is AA:AA:AA:AA:AA:AA, and up to 64 trusted MAC addresses can be added.

Step 5. After the configuration is complete, click “OK”.

The configured trusted MAC addresses are displayed in the trusted MAC address list. You can "Modify " and "Delete " the added MAC address.

Step 6. Select "Enable" to enable the trusted MAC function.

By default, this function is not enabled. This function takes effect only after it is enabled.

Set administration port

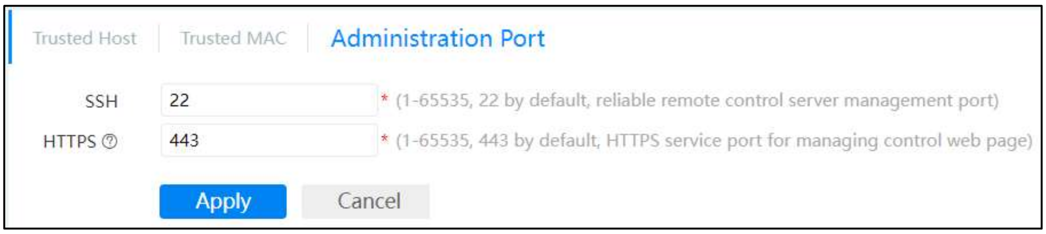
Set the port to manage the firewall via Telnet, SSH, HTTP or HTTPS.

Step 1. Select "System > Device Management > Administration Host".

Step 2. Click “Administration Port”.

Step 3. View or modify administration ports.

The default login protocol is the default well-known port. Users can modify the management port. Please make sure that the management ports set at both ends of the communication protocol are the same.



SSH 22 * (1-65535, 22 by default, reliable remote control server management port)

HTTPS ⓘ 443 * (1-65535, 443 by default, HTTPS service port for managing control web page)

Step 4. After modification, click “Apply”.

1.1.3 Administration User

The administration user is used to perform operations such as business configuration, log audit, and account security management on the firewall. By setting different roles for different levels of administrator accounts, limit the authorities of administration users, so as to grant the least authority to the administrator user and improve the security of the firewall itself.

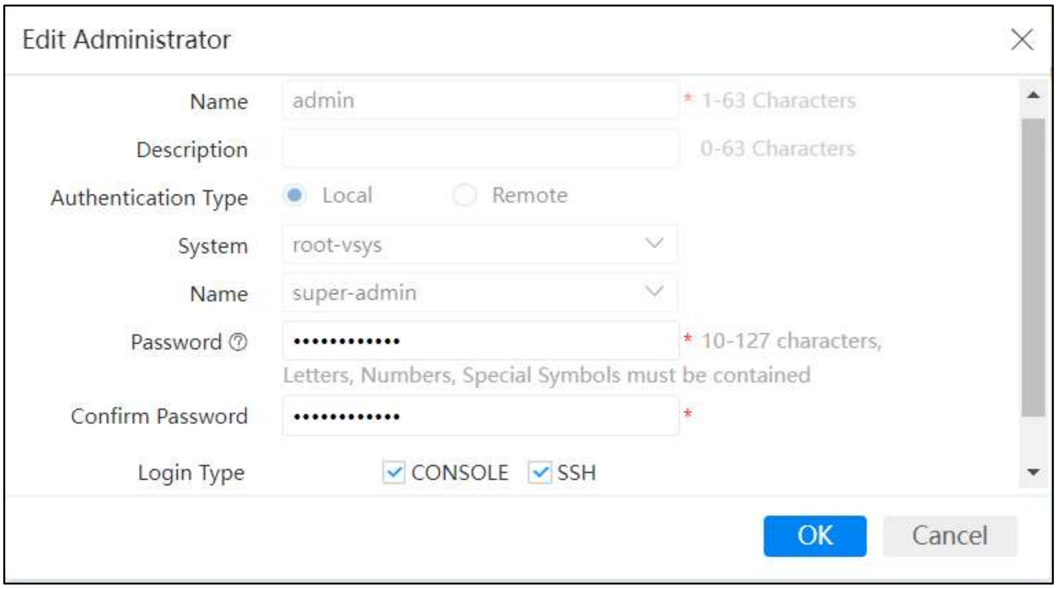
Notes

The administrator password must be changed regularly to ensure the security of the administrator account.

Default Administrator

By default, there is a super administrator named admin in the firewall, and the password of this administrator is **maipu@ 1993.** This administrator cannot be deleted.

The properties of the default administrator admin are shown in the figure below. The name, description, authentication type, system, and role of the default administrator cannot be modified. Only password and login type can be modified.



Edit Administrator

Name: admin * 1-63 Characters

Description: 0-63 Characters

Authentication Type: ● Local ○ Remote

System: root-vsys

Name: super-admin

Password: •••••••••••• * 10-127 characters, Letters, Numbers, Special Symbols must be contained

Confirm Password: •••••••••••• *

Login Type: ☑ CONSOLE ☑ SSH

Add Administrator

It is recommended to configure a separate management account for each administrator, so that the operations of each administrator can be tracked through logs.

Step 1. Select "System > Device Management > Administration User".

Step 2. Click “Add”.

Step 3. Configure administrator parameters.

Parameter	Description
Name	Configure the login user name corresponding to the administrator account. This account cannot be the same as the existing administrator account on the device. The administrator name must start with a letter, number or Chinese, and may contain special characters such as underscore " ", hyphen "-", dot ".", or @.
Description	Optional. Add necessary description information for administrators.
Authentication type	• Authentication type is local. Indicates that the administrator is a local user. Perform local authentication via password. The password must meet the password complexity required by the system to configure successfully. • Authentication type is remote. Remote means that the administrator is authenticated by the server. Local indicates the local authentication server of the firewall. If authentication is performed through a third-party authentication server (RADIUS server, TACACS+ server, LDAP server, or certificate server, etc.), you need to configure the authentication server first, and then select the authentication server from the drop-down menu.
System	Select the system to which the user belongs. default user belongs to the root system (root-vsys). If you want to create a virtual system administrator, you must create a virtual system first, and only created virtual systems can be selected in the drop-down menu.
Role	The user can select the role to which the administrator belongs in the drop-down list, and authorize the corresponding rights for the administrator account.
Password and Confirm Password	It needs to be configured only when Local is selected as the authentication type. Password complexity can be set on the "Login Settings " page. By default, it must contain letters, numbers and special symbols. The administrator password does not support special characters such as spaces, question marks, single quotes, double quotes, \\, &, <, >, etc. The password corresponding to the administrator account.
Authentication server	It needs to be configured only when Remote is selected as the authentication type. Specifies the server that authenticates the administrator account. The authentication server type can be Local, Radius, LDAP, AD, TACACS+ and POP3.

Parameter	Description
Login type	Specifies the login types that this administrator account can use. The login type supports HTTP, HTTPS, CONSOLE, TELNET, SSH. Only after the corresponding method is selected, it is allowed to use this method to manage the firewall. Multiple login methods can be enabled.

Step 4. Click “OK” after the configuration is complete.

The configured administrators are displayed in the administrator list. Custom administrators can be modified, deleted, and queried.

1.1.4 Administration Role

Custom Admin Role

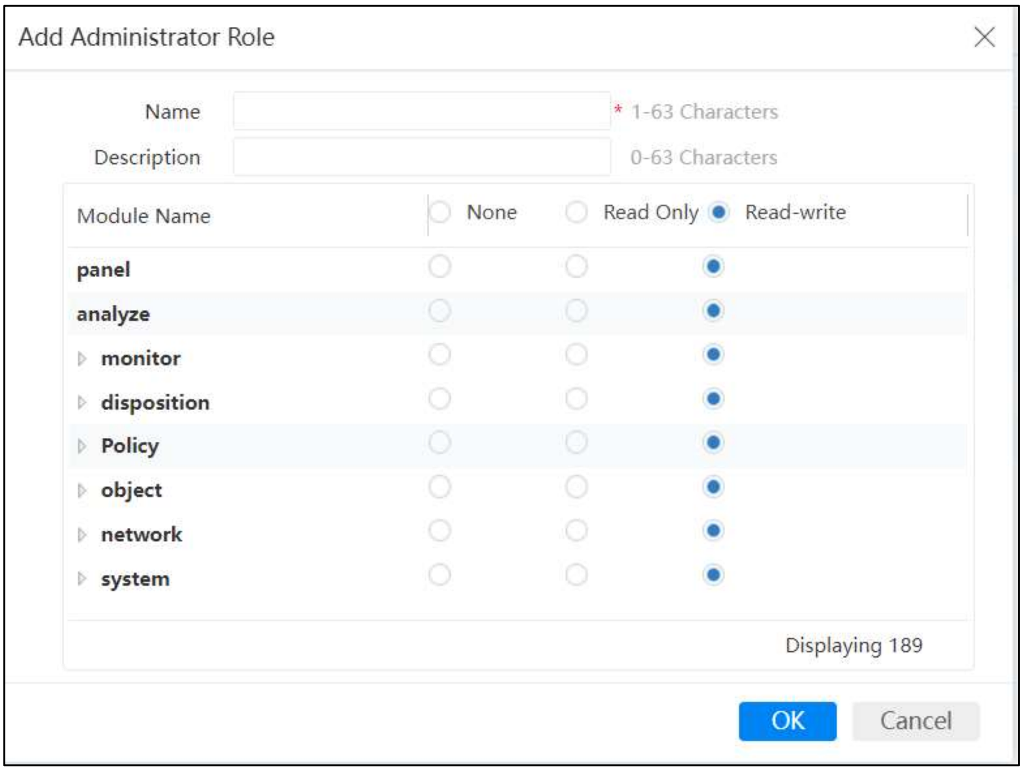
You can add custom roles when the default roles do not meet your needs. In consideration of security, it is recommended to configure the minimum authority within the corresponding scope of authority for the corresponding administrator role.

Step 1. Select "System > Device Management > Administration Role".

Step 2. Click “Add”.

Step 3. Configure the name and authorities of the administrator role.

Configure the role's authorities for each module as required. The roles can be assigned with read-only, read-write, or no-operation authorities on functional modules.



Add Administrator Role

Name * 1-63 Characters

Description 0-63 Characters

Module Name	○ None	○ Read Only	● Read-write
panel	○	○	●
analyze	○	○	●
▷ monitor	○	○	●
▷ disposition	○	○	●
▷ Policy	○	○	●
▷ object	○	○	●
▷ network	○	○	●
▷ system	○	○	●

Displaying 189

Step 4. After the configuration is complete, click “OK”.

The configured administrator roles are displayed in the administrator role list. The custom administrator roles can be modified, deleted and other operations.

1.1.5 Manage Certificate

The native certificate is the certificate of the firewall as the server side. The local certificate uses the default certificate by default. The default local certificate, CA certificate, and administrator certificate are automatically generated by the CA center integrated with the firewall by default.

When a user logs in to the management firewall through HTTPS, the user's browser will authenticate the certificate.

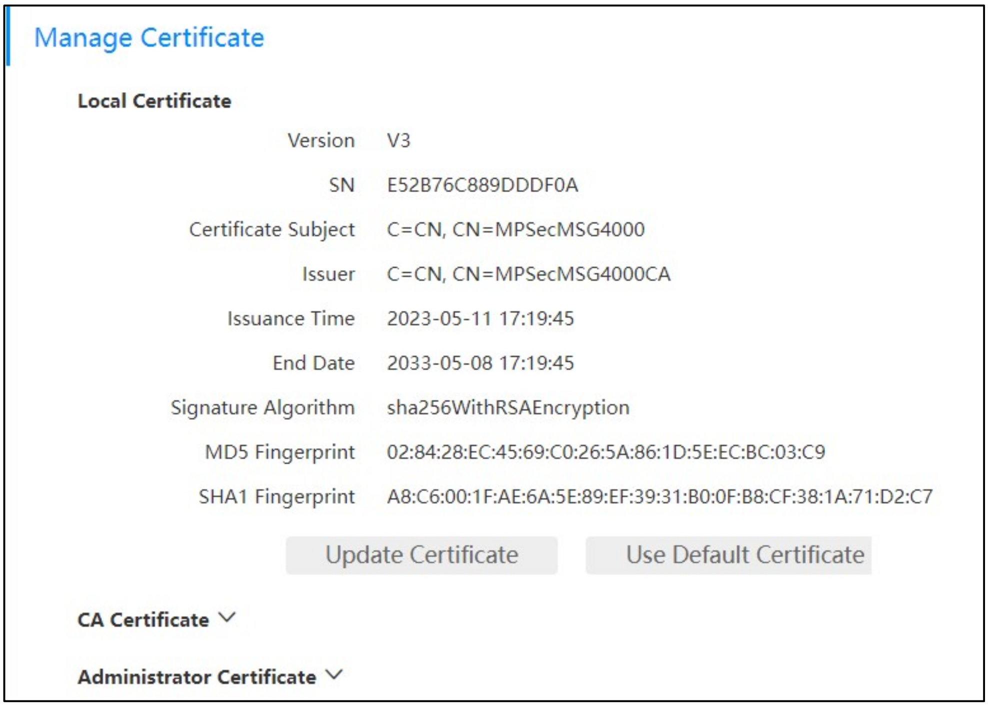
When the firewall is powered on for the first time after leaving the factory, the default integrated CA center in the firewall will automatically generate "Local certificate" and "Administrator certificate", and the default validity period is ten years.

Update Local Certificate and CA Certificate

The administrator can apply for a certificate for this machine from the local CA center or other CA centers. When the local certificate is updated, the CA certificate will also be updated.

Step 1. Select "System > Device Management > Manage Certificate".

Step 2. Click “Update Certificate”.

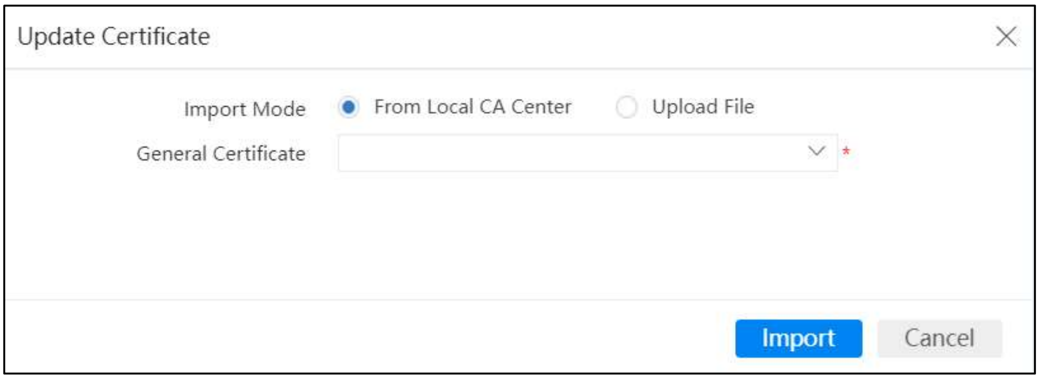


Manage Certificate

Local Certificate

Version	V3
SN	E52B76C889DDDF0A
Certificate Subject	C=CN, CN=MPSecMSG4000
Issuer	C=CN, CN=MPSecMSG4000CA
Issuance Time	2023-05-11 17:19:45
End Date	2033-05-08 17:19:45
Signature Algorithm	sha256WithRSAEncryption
MD5 Fingerprint	02:84:28:EC:45:69:C0:26:5A:86:1D:5E:EC:BC:03:C9
SHA1 Fingerprint	A8:C6:00:1F:AE:6A:5E:89:EF:39:31:B0:0F:B8:CF:38:1A:71:D2:C7

Step 3. Select the certificate import method.



Update Certificate

Import Mode ● From Local CA Center ○ Upload File

General Certificate *

Step 4. Select the certificate, and click “Import”.

After the certificate is imported, both the local certificate and the CA certificate will be replaced with the certificate adopted by the user. The administrator certificate automatically generated by the local CA center is no longer displayed.

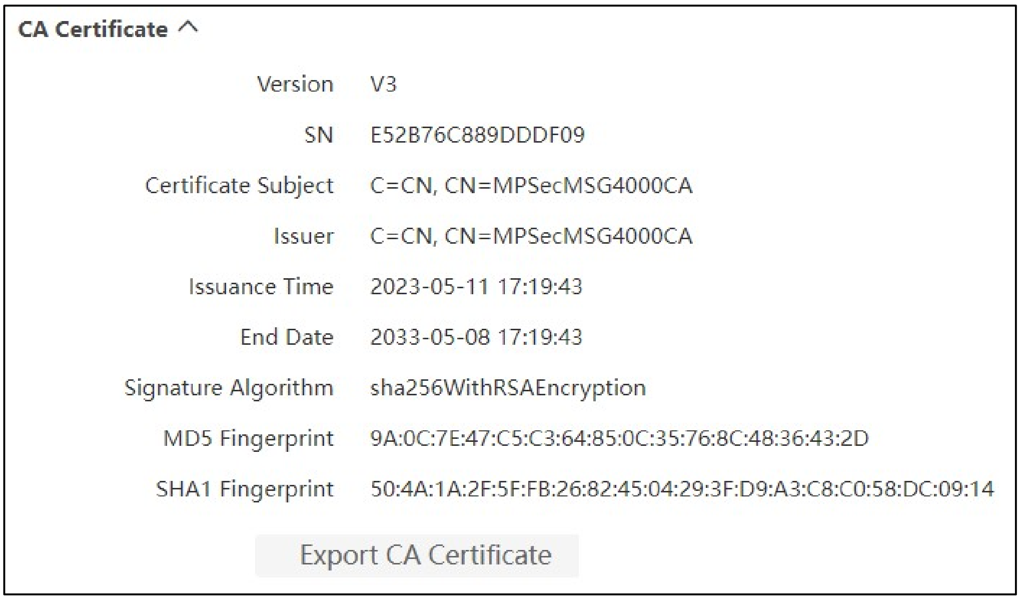
When the user does not need to continue to use the certificate of the third-party CA center and wants to restore the default local certificate, CA certificate, and administrator certificate of the firewall, he only needs to click "Use Default Certificate".

Export CA Certificate

The local CA is the top priority in the PKI system and is the source of all certificates. Local CA supports exporting CA certificates.

Step 5. Select "System > Device Management > Manage Certificate".

Step 6. Click “Export CA Certificate”.



CA Certificate ^

Version V3

SN E52B76C889DDDF09

Certificate Subject C=CN, CN=MPSecMSG4000CA

Issuer C=CN, CN=MPSecMSG4000CA

Issuance Time 2023-05-11 17:19:43

End Date 2033-05-08 17:19:43

Signature Algorithm sha256WithRSAEncryption

MD5 Fingerprint 9A:0C:7E:47:C5:C3:64:85:0C:35:76:8C:48:36:43:2D

SHA1 Fingerprint 50:4A:1A:2F:5F:FB:26:82:45:04:29:3F:D9:A3:C8:C0:58:DC:09:14

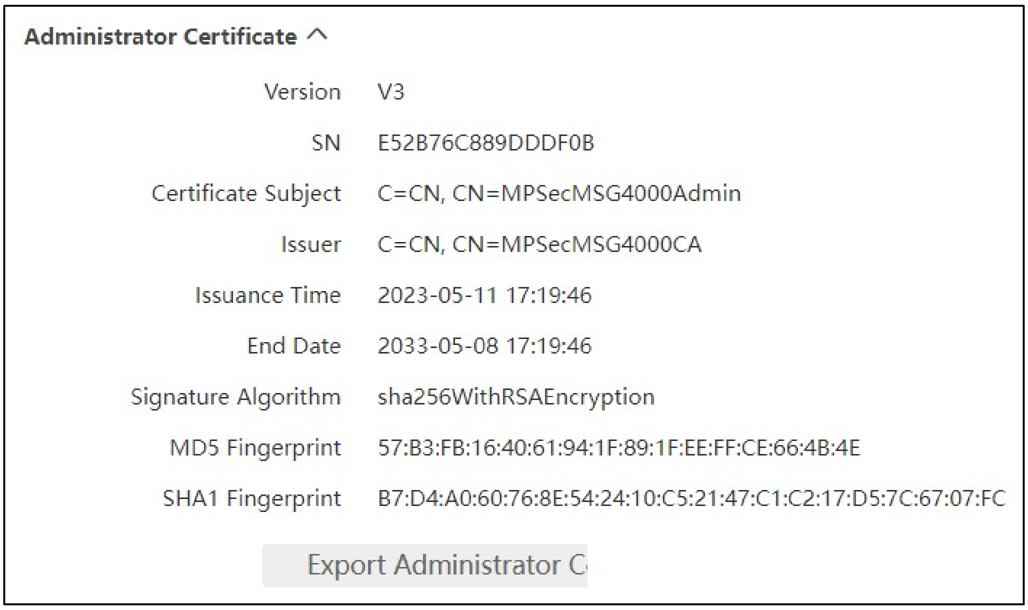
Step 7. Select the path to save the certificate.

Step 8. Click “Download” to save the CA certificate.

Export Admin Certificate

When the user is in "System> Device Management > Login Settings”, after enabling "Authenticate Administrator Certificate", when users manage the firewall through HTTPS, they need to perform certificate authentication on the administration host as the client.

When a user uses the administrator certificate generated by the firewall's default CA center for authentication, the administrator certificate needs to be exported and installed on the host that manages the firewall. After the certificate is updated, the original administrator certificate becomes invalid. You need to use the CA that issues certificates for the firewall to generate a new administrator certificate.



Administrator Certificate ^

Version	V3
SN	E52B76C889DDDF0B
Certificate Subject	C=CN, CN=MPSecMSG4000Admin
Issuer	C=CN, CN=MPSecMSG4000CA
Issuance Time	2023-05-11 17:19:46
End Date	2033-05-08 17:19:46
Signature Algorithm	sha256WithRSAEncryption
MD5 Fingerprint	57:B3:FB:16:40:61:94:1F:89:1F:EE:FF:CE:66:4B:4E
SHA1 Fingerprint	B7:D4:A0:60:76:8E:54:24:10:C5:21:47:C1:C2:17:D5:7C:67:07:FC

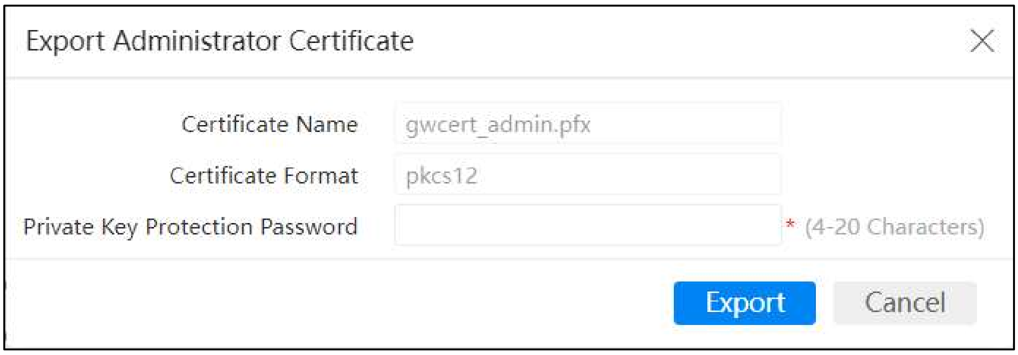
Step 1. Select "System > Device Management > Manage Certificate".

Step 2. Expand “Administrator Certificate”.

Step 3. Click “Export Administrator Certificate”.

Step 4. Set the private key protection password.

The certificate format is pkcs12. The value of the private key protection password is 4 to 20 characters. To ensure the security of the certificate, please keep the password safe.



Export Administrator Certificate

Certificate Name	gwcert_admin.pfx
Certificate Format	pkcs12
Private Key Protection Password	* (4-20 Characters)

Step 5. Click “Export”.

Install Administrator Certificate on Administration Host

Install the exported administrator certificate or the certificate generated by a third-party CA center on the host that manages the firewall.

1.1.6 Lock Administration

After the user enables "Configure Login Security Policy" in the "System > Device Management > Login Settings", when the number of wrong passwords entered for the management account reaches the allowed number of failures, the corresponding management account will be locked. The user cannot log in to the firewall again during the lockout period.

A locked user can use another IP (IP lock) or other management account (username lock) to unlock the locked account. The unlocked administrator must have read and write authority for lock management.

Step 1. Select "System > Device Management > Lock Management".

Step 2. Select the corresponding IP or account in the locked list.

When locking by IP address, the locked object displays the locked IP address; when locking by user name, the locked object displays the locked administrator account name.

Notes

The method of locking based on user name requires users to combine their actual needs. When an untrusted attacker tries to guess the administrator password, if you choose to lock the user name, the real administrator will not be able to log in to the firewall for management during the lock period.

The Lock Time column shows the remaining lock time.

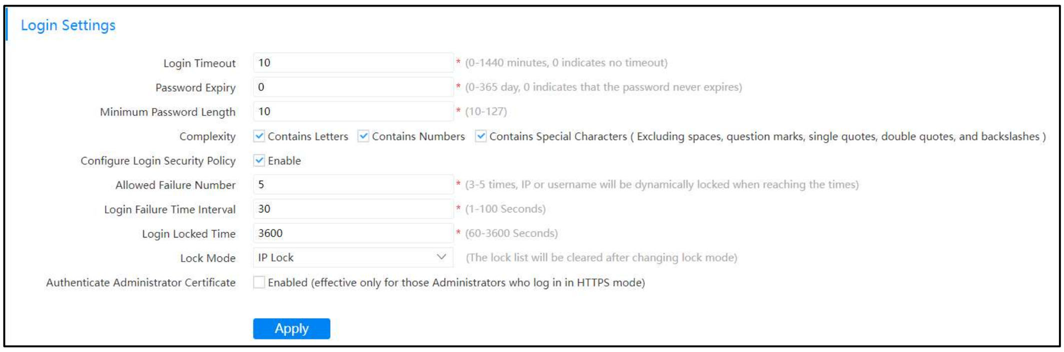
Step 3. Click “Unlock”.

1.1.7 Login Settings

Login settings are used to improve the security of the management account and system.

Step 1. Select "System > Device Management > Login Settings".

Step 2. Set timeout parameters and security parameters.



Login Settings

Login Timeout: 10 * (0-1440 minutes, 0 indicates no timeout)

Password Expiry: 0 * (0-365 day, 0 indicates that the password never expires)

Minimum Password Length: 10 * (10-127)

Complexity: ☑ Contains Letters ☑ Contains Numbers ☑ Contains Special Characters (Excluding spaces, question marks, single quotes, double quotes, and backslashes)

Configure Login Security Policy: ☑ Enable

Allowed Failure Number: 5 * (3-5 times, IP or username will be dynamically locked when reaching the times)

Login Failure Time Interval: 30 * (1-100 Seconds)

Login Locked Time: 3600 * (60-3600 Seconds)

Lock Mode: IP Lock (The lock list will be cleared after changing lock mode)

Authenticate Administrator Certificate: □ Enabled (effective only for those Administrators who log in in HTTPS mode)

Parameter	Description
Login timeout	Set the timeout period for administrators to log in to the firewall, including the web page and cli interface. When it is filled with 0, it means that there is no timeout limit. When an administrator logs in to the firewall web management page and does not perform any operations, and reaches the upper limit set by the timeout period, the firewall will disconnect the session with the administrator, and the user needs to refresh the web management page and log in to the firewall again to continue management.
Password Expiry	The user can specify how many days the administrator password is valid for. Filling in 0 means that there is no restriction on the password valid period. The system defaults to filling in 0. After the password validity period expires, the user needs to change the password again.
Minimum password length	Users can customize the minimum length of the password.
Complexity	Set the complexity requirement for passwords. Checking all checkboxes requires that all conditions be met at the same time.
Configure login security policy	By default, it is enabled. The setting of the login security policy is mainly to prevent untrusted attackers from attempting to brute force crack the password of the administrator account. After enabling it, you can set the login security policy. If it is not enabled, the login security policy function will not be enabled.
Allowed failure number	Users can customize the allowed number of failures. The default is 5 times, and the range is 3-5 times. When the number of wrong passwords entered by the user reaches the allowed number of failures, and the interval between two consecutive logins is less than the interval between two failed logins, the user or IP will be dynamically locked.

Parameter	Description
Login failure time interval	Users can customize the interval between two login failures, and the default is 30 seconds. • When the interval between this login failure and the last login failure is less than this time, it will be continuously counted until the number of failures reaches the allowed number, and the user or IP will be locked. • When the interval between this login failure and the last login failure is greater than this time, it will not be continuously counted.
Login locked time	Dynamic login lock time, the default is 3600 seconds, the range is 60-3600 seconds.
Lock mode	Divided into IP lock and username lock. • When the lock mode is "IP lock ", the IP address will be locked. During the lock period, the IP address will not be able to log in to the firewall through the username. The default locking method is IP lock. • When the lock method is "Username Lock", the username will be locked. This user name cannot log in to the firewall during the lock period.
Authenticate Administrator Certificate	By default, the firewall conducts password authentication for administrators, and after enabling administrator certificate authentication, certificate authentication will be performed for the administration hosts used by administrators. In this way, password and certificate double authentication can be realized. After “Enable” is selected, when a user logs in to the management firewall through HTTPS, the firewall will authenticate the administrator with a certificate. Before enabling this function, users need to confirm that the administrator certificate has been imported on the management host.

Step 3. After the settings are complete, click “Apply”.

1.1.8 View Online Administrator

You can view the number of online administrators in the "System Information" area box of the "Home". Click “View” corresponding to "Online Administrator ", and you can view the details of the online administrator, including the administrator name, role, address, login method, and online duration and other parameters.

The administrator can also check the various operations of the administrator through "Operation Log".

1.2 Configuration File

1.2.1 Restrictions and Precautions

Exporting the configuration does not support exporting the management certificate. After importing the configuration file again, the administrator certificate will automatically become the default certificate. Therefore, if the original certificate used by the user is not the default certificate, after importing the configuration, please export the administrator certificate through "System > Device Management > Manage Certificate ", and update the certificate on the administration host client; or enable http or command line management mode. Otherwise, it may not be possible to manage the firewall.

1.2.2 Export Configuration

The export configuration type supports last saved configuration, current configuration, historical configuration, and supports encrypted configuration files.

Users can choose to export the configuration file to the local, FTP server, or TFTP server.

Export Configuration to Local

Step 1. Choose “System > Configuration File Management> Export Configuration”.

Step 2. Select a configuration type.

- Last saved configuration

Indicates the user's last saved configuration file.

When the configuration type is "Last Saved Configuration", specify the system to which the configuration file belongs.

The virtual system administrator can choose to export the last saved configuration of the current system, and the root system administrator can choose to export the last saved configuration of the root system or all virtual systems.

- Current configuration

Export the configuration file currently viewed by the user.

- History configuration

The configuration files saved by the user for the last three times will be recorded in the historical configuration based on the saved time point.

When selecting "History Configuration", select which time saved configuration file to export.

Exporting historical configurations allows users to select one of the last three recorded historical configurations for export.

Step 3. Select “Export” to “Local”.

Step 4. Choose whether to enable ciphertext.

After selecting "Ciphertext", the configuration file exported by the user will be saved in an encrypted manner. Open the viewed configuration file with text editing software as cipher text.

Step 5. Configure encryption password.

The encryption function requires the user to specify an encryption password and confirm the password again. Please remember the encryption password so that it can be used to decrypt the configuration file when importing the encrypted configuration file again.

Step 6. Click “Export”.

Export to local: The configuration file selected by the user will be exported to the administration host currently managing the firewall.

Export Configuration to FTP Server

Step 1. Choose “System > Configuration File Management > Export Configuration”.

Step 2. Select a configuration type.

- Last saved configuration

Indicates the user's last saved configuration file.

When the configuration type is "Last saved configuration ", specify the system to which the configuration file belongs.

The virtual system administrator can choose to export the last saved configuration of the current system, and the root system administrator can choose to export the last saved configuration of the root system or all virtual systems.

- Current configuration

Export the configuration file currently viewed by the user.

- History configuration

The configuration files saved by the user for the last three times will be recorded in the history configuration based on the saved time point.

Step 3. Select Export to "FTP Server".

Step 4. Configure the parameters related to the FTP server, and click “Apply”. After clicking “Apply”, the relevant FTP parameters will be saved.

Parameter	**Description**
Auto update	Auto upload is supported only when the configuration type is "Last Saved Configuration". After selecting the "Auto Update" check box, the firewall will automatically upload the configuration file of the selected type to the FTP server.
Auto update time	Set an auto update time.

Parameter	Description
Save time	The save time needs to be selected only when Configuration Type is History Configuration. When selecting "History Configuration", select which time saved configuration file to export. Exporting history configurations allows users to select one of the last three recorded history configurations for export.
Server address	Specify the FTP server address. The user needs to ensure that the firewall is reachable to the FTP server.
File name	Specify a filename for the exported configuration file. If the FTP is a Windows server, the file name when exporting the configuration cannot contain: / \ * " ? < > | several special symbols.
Username	Specifies the user name for logging in to the FTP server.
Password	Specifies the password for logging in to the FTP server.

Step 5. Choose whether to enable cipher text.

After selecting "Cipher Text", the configuration file exported by the user will be saved in an encrypted manner. Open the viewed configuration file with text editing software as cipher text.

Step 6. Configure encryption password.

The encryption function requires the user to specify an encryption password and confirm the password again. Please remember the encryption password so that the configuration file can be decrypted when the encrypted configuration file is imported again.

Step 7. Click “Export”.

Export Configuration to TFTP Server

Step 1. Choose “System > Configuration File Management > Export Configuration”.

Step 2. Select a configuration type.

- Last saved configuration

Indicates the user's last saved configuration file.

When the configuration type is "Save configuration last", specify the system to which the configuration file belongs.

The virtual system administrator can choose to export the last saved configuration of the current system, and the root system administrator can choose to export the last saved configuration of the root system or all virtual systems.

- Current configuration

Export the configuration file currently viewed by the user.

- History configuration

The configuration files saved by the user for the last three times will be recorded in the historical configuration based on the saved time point.

Step 3. Select Export to “TFTP Server”.

Step 4. Configure related parameters of the TFTP server and click “Apply”. After clicking “Apply”, the T FTP related parameters will be saved.

Parameter	Description
Automatic update	Automatic upload is supported only when Configuration Type is "Last Saved Configuration". After selecting the "Auto upload" check box, the firewall will automatically upload the configuration file of the selected type to the TFTP server.
Automatic update time	Set an automatic update time.
Save time	The save time needs to be selected only when Configuration Type is History Configuration. When selecting "History Configuration", select which time saved configuration file to export. Exporting historical configurations allows users to select one of the last three recorded historical configurations for export.
Server address	Specify the TFTP server address. The user needs to ensure that the firewall is reachable to the TFTP server.
File name	Specify a filename for the exported configuration file. If TFTP is a Windows server, the file name when exporting the configuration cannot contain: / \ * " ? < > | several special symbols.

Step 5. Choose whether to enable ciphertext.

After selecting "Cipher Text", the configuration file exported by the user will be saved in an encrypted manner. Open the viewed configuration file with text editing software as cipher text.

Step 6. Configure encryption password.

The encryption function requires the user to specify an encryption password and confirm the password again. Please remember the encryption password so that it can be used to decrypt the configuration file when importing the encrypted configuration file again.

Step 7. Click “Export”.

1.2.3 Import Configuration

Users can choose to import firewall configuration from local, FTP server or TFTP server. Before importing the firewall configuration, the user needs to confirm whether the configuration file of the firewall is ciphertext or plaintext. If it is ciphertext, you need to enter the encryption password configured when exporting the ciphertext configuration file.

Local Import

Step 1. Choose “System > Configuration File Management > Import Configuration”.

Step 2. Select "Local" as the configuration type.

Step 3. Select the configuration file to import.

Parameter	**Description**
Name	Select the configuration file to import.
Ciphertext	Select "Ciphertext", indicating that the imported configuration file is a ciphertext configuration file.
Password	Enter the password corresponding to the encrypted configuration file.
History configuration list	Users can view the configuration files recorded by clicking the Save button for the last three times in the history configuration list. Select the imported historical configuration by selecting the corresponding radio button in the Operation column. The system will load the selected history configuration when the device is restarted next time. By default, the last saved configuration file is selected.

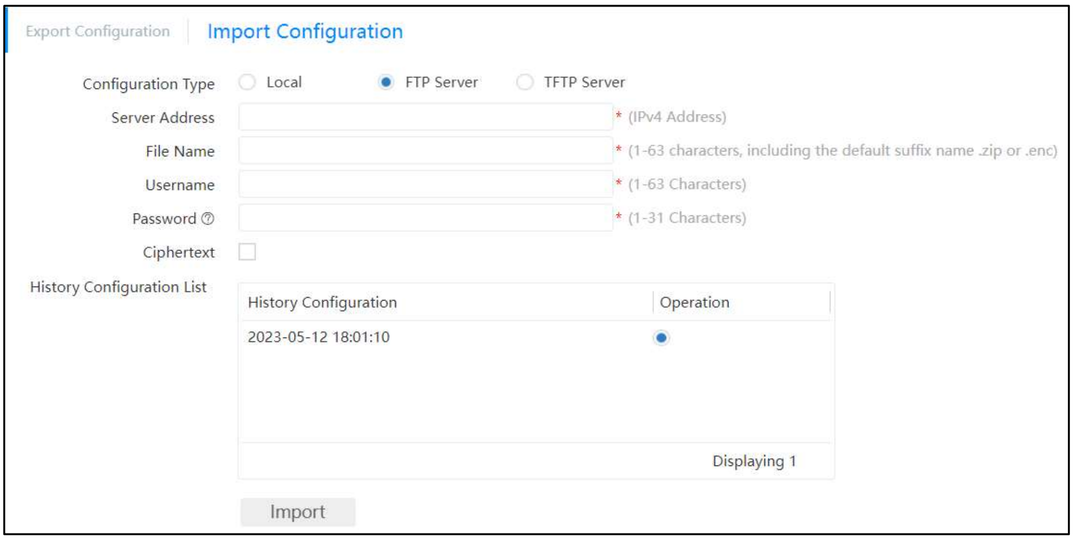
Step 4. Click “Import”.

FTP Server Import

Step 1. Choose “System > Configuration File Management > Import Configuration”.

Step 2. Select "FTP Server" as the configuration type.

Step 3. Set FTP server parameters.



Configuration Type ○ Local ● FTP Server ○ TFTP Server

Server Address * (IPv4 Address)

File Name * (1-63 characters, including the default suffix name .zip or .enc)

Username * (1-63 Characters)

Password * (1-31 Characters)

Ciphertext □

History Configuration List

History Configuration	Operation
2023-05-12 18:01:10	●

Displaying 1

Parameter	Description
Server address	IP address of the FTP server. The user needs to ensure that the firewall is reachable to the FTP server.
File name	Specifies the file name of the configuration file to import into the firewall.
Username	Enter the user name required to log in to the FTP server.
Password	Enter the password required to log in to the FTP server.
Ciphertext	Select "Ciphertext", indicating that the imported configuration file is a ciphertext configuration file.
Password	Enter the password corresponding to the encrypted configuration file.
History configuration list	Users can view the configuration files recorded by clicking the save button for the last three times in the historical configuration list. Select the imported historical configuration by selecting the corresponding radio button in the Action column. The system will load the selected historical configuration when the device is restarted next time. By default, the last saved configuration file is selected.

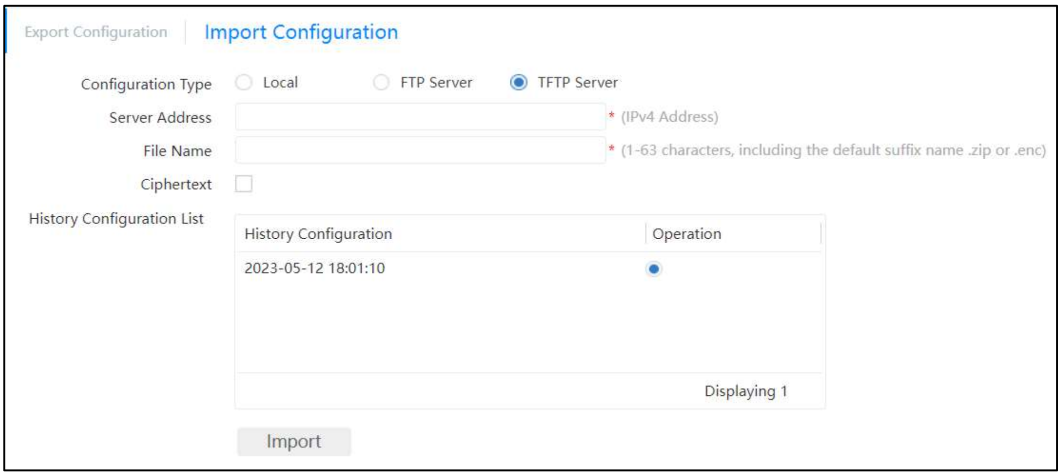
Step 4. Click “Import”.

TFTP Server Import

Step 1. Choose “System > Configuration File Management > Import Configuration”.

Step 2. Select TFTP Server as the configuration type.

Step 3. Set TFTP server parameters.



Configuration Type ○ Local ○ FTP Server ● TFTP Server

Server Address * (IPv4 Address)

File Name * (1-63 characters, including the default suffix name .zip or .enc)

Ciphertext □

History Configuration List

History Configuration	Operation
2023-05-12 18:01:10	●

Displaying 1

Parameter	Description
Server address	The IP address of the FTP server. The user needs to ensure that the firewall is reachable to the TFTP server.
File name	Specifies the file name of the configuration file to import into the firewall.
Ciphertext	Select "Ciphertext", indicating that the imported configuration file is a ciphertext configuration file, and you need to enter the password corresponding to the ciphertext configuration file in the password column.
Password	Enter the password corresponding to the encrypted configuration file.
History configuration list	Users can view the configuration files recorded by clicking the save button for the last three times in the history configuration list. Select the imported history configuration by selecting the corresponding radio button in the Operation column. The system will load the selected history configuration when the device is restarted next time. By default, the last saved configuration file is selected.

Step 4. Click “Import”.

1.3 SNMP

The SNMP function of the firewall is to facilitate the administrator to use the centralized management device to monitor and manage the system information, resources and status of the firewall in a unified manner. Currently supported protocols include SNMP v1, SNMP v2c, and SNMP v3. It can be used in conjunction with centralized management software or equipment using the standard SNMP protocol.

1.3.1 Configure SNMP

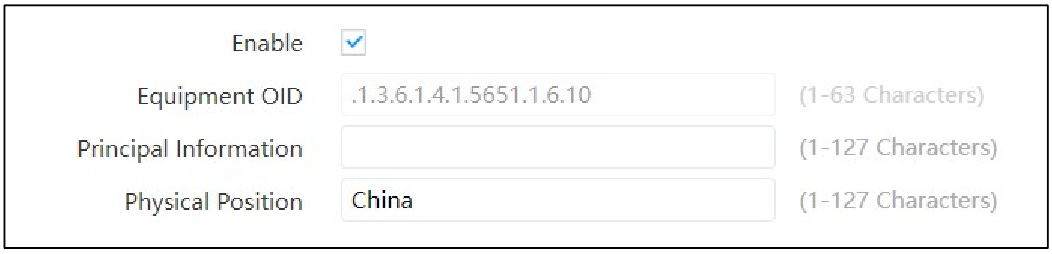
When configuring the SNMP function, the user needs to determine which version of the SNMP protocol to use so that the firewall and the SNMP server use the same SNMP version.

Step 1.   Choose “System > SNMP > SNMP Settings”.

Step 2.   Enable SNMP.

The SNMP configuration takes effect only after "Enable" is selected.

Step 3.   Set common SNMP parameters.



Enable ☑

Equipment OID: .1.3.6.1.4.1.5651.1.6.10 (1-63 Characters)

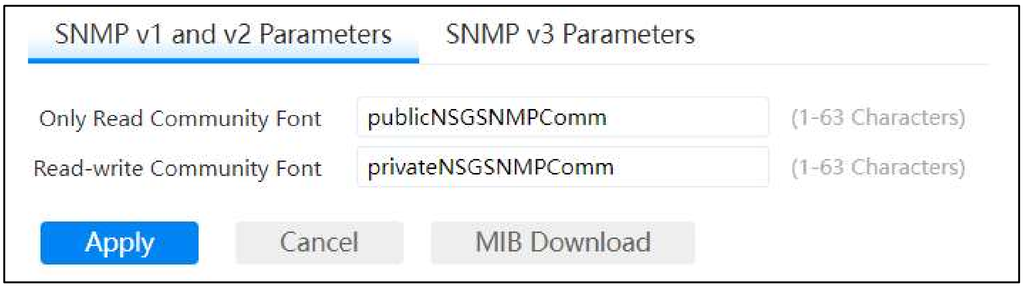
Principal Information: (1-127 Characters)

Physical Position: China (1-127 Characters)

Parameter	Description
Equipment OID	The object identifier of the firewall, which cannot be modified by the user. When using the network management software to collect information such as the memory and CPU utilization of the firewall, the network management software needs to obtain the device OID.
Principle information	To help users maintain devices, the firewall supports recording the person in charge of the device.
Physical position	Record the information such as the computer room and rack where the managed device is located, so that users can quickly find the physical location of the device when maintaining the device.

Step 4.   Select and configure corresponding parameters according to the SNMP version of the SNMP server.

- Configure SNMPv1 or SNMPv2 parameters.

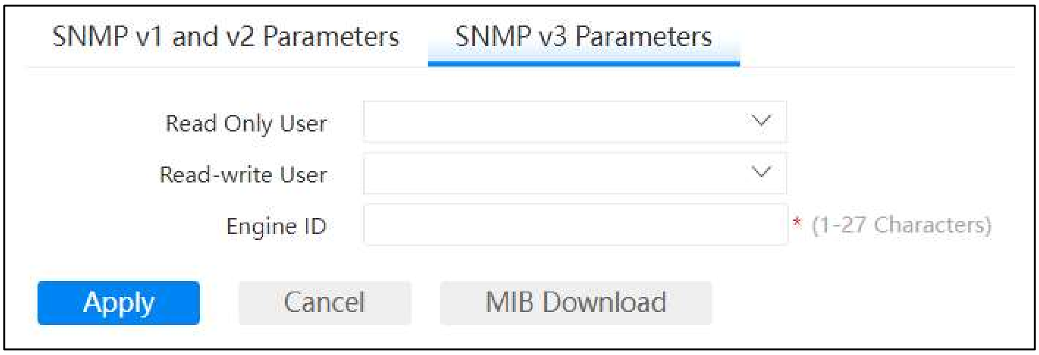

SNMP v1 and v2 Parameters | SNMP v3 Parameters

Only Read Community Font: publicNSGSNMPComm (1-63 Characters)

Read-write Community Font: privateNSGSNMPComm (1-63 Characters)

Parameter	Description
Only ready community font	Adopt the community word for authentication between the firewall and the managed device. If the read-only community font is configured, the administration device (firewall) has read-only authority. The read-only community fonts on the firewall and the managed device must be consistent; otherwise, the firewall will fail to access the managed device through SNMP.
Read-write community font	Adopt the community word for authentication between the firewall and the managed device. If the read-write community font is configured, the administration device (firewall) has read-write authority. The read-write community fonts on the firewall and the managed device must be consistent; otherwise, the firewall will fail to access the managed device through SNMP.

- Configure SNMPv3 parameters.


SNMP v1 and v2 Parameters | SNMP v3 Parameters

Read Only User:

Read-write User:

Engine ID: * (1-27 Characters)

Parameter	Description
Read-only user	Select SNMP v3 user, the selected user will have read-only authority. If you need to add a new user, select "Add Read-Only User". The user used on the firewall must be consistent with the user name configured on the managed device.

Parameter	Description
Read-write user	Select an SNMP v3 user, and the selected user will have read and write authority. If you need to add a new user, select "Add Read-Write User ". The user used on the firewall must be consistent with the user name configured on the managed device.
Engine ID	The engine ID is the unique identifier for identifying the SNMPv3 engine on the device. The user and engine ID used by the SNMP server must be consistent with the configuration on the firewall.

Step 5. After the configuration is complete, click “Apply”.

1.3.2 Add SNMPv3 User

When using SNMPv3 for communication, an SNMPv3 user must be specified. It can be added while selecting, or can be added according to the following steps.

Step 1. Choose “System > SNMP > SNMPv3 User”.

Step 2. Click “Add”.

Step 3. Configure SNMPv3 user parameters.

Parameter	Description
Name	Configure the name of the SNMPv3 user. The name length ranges from 1 to 31 characters.
Security Level	Configure the security level. • Authentication and encryption: The security level is the highest, and authentication and encryption parameters need to be configured at the same time. • Authentication without encryption: The security level is medium, and only authentication parameters need to be configured. • No authentication and no encryption: The security level is lowest, not recommended.
Authentication	Select an authentication algorithm. The authentication algorithm supports MD5 and SHA1. For security reasons, SHA1 is recommended.
Authentication password and confirm authentication password	Set the authentication key corresponding to the authentication algorithm.

Parameter	Description
Encryption	Select an encryption algorithm. The encryption algorithm supports DES and AES-128. For security reasons, AES-128 is recommended.
Encryption Password and Confirm Encryption Password	Set the encryption key corresponding to the encryption algorithm.

Step 4. After the configuration is complete, click "OK".

1.4 Upgrade Management

The upgrade is divided into system upgrade and feature database upgrade. Wherein, the system upgrade includes upgrading the system and patching through the upgrade package. The feature databases that can be upgraded under upgrade management include the intrusion prevention feature database, application identification database, virus database, URL resource database, ISP information database, and region database. Library upgrade settings provide feature library automatic upgrade server settings.

1.4.1 Upgrade via System Package or Upgrade Package

Upgrade Instructions

Select "Upgrade system" or "Upgrade package" according to the upgrade scenario, and the user needs to import the system version or patch upgrade package file in the configuration information.

- Upgrade the system

The firewall system supports dual systems, and two system versions can be imported at most. In the upgrade system list, users can view the historical versions imported on the device. The system in the "selected" state is the currently used system version. To use an alternative system version, simply select its corresponding radio button and the device will start the system the next time it boots. Dual-system backup can help users switch to the standby system when the current system fails, realizing redundant backup of the firewall system.

- Upgrade package

To select an upgrade package, the user is required to import the patch upgrade package in the configuration information. The firewall supports two patch upgrade packages, hotfix (hot patch) and patch (cold patch). The system needs to be restarted after the upgrade package is upgraded through the cold patch type. In the upgrade package list, the user can view the record and status of the upgrade package import.

Upgrade Operation

Notes

Two versions already exist in the system, one needs to be deleted before the new version can be uploaded. Otherwise, after selecting the version to upload or completing the FTP/TFTP settings, a prompt to delete a version will also pop up. A system package can be deleted through this prompt box.

Step 1. Choose “System > Upgrade Management > System Upgrade”.

Step 2. Select the upgrade type as "Upgrade System" or "Upgrade Package ".

Step 3. Select the configuration type for uploading system files.

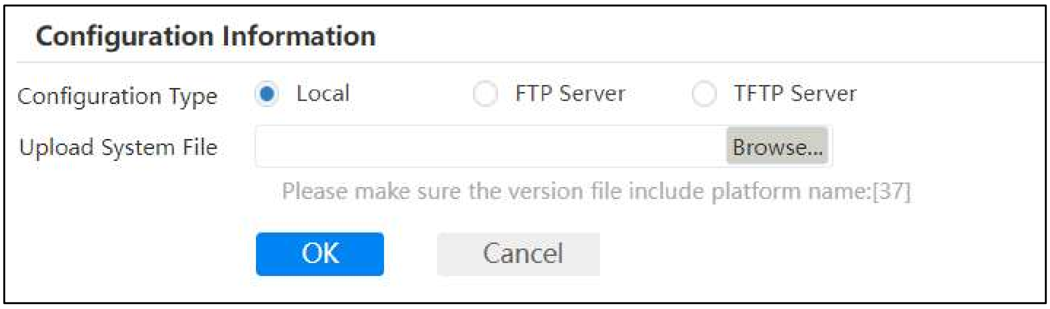
The configuration type can be selected from "Local", "FTP Server" and "TFTP Server". Local mode requires system files to be kept on the management host that manages the firewall.

The FTP server or TFTP server mode requires a client to enable the FTP server or TFTP server, and save system files on the FTP server or TFTP server.

Step 4. Set parameters for uploading system files.

- Local

Click “Browse” and select the system file to upload.



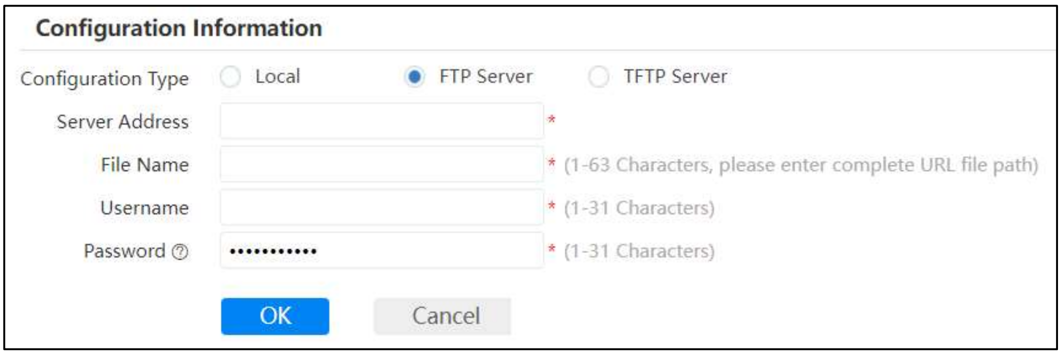
Configuration Information

Configuration Type ● Local ○ FTP Server ○ TFTP Server

Upload System File Browse...

Please make sure the version file include platform name:[37]

- FTP server



Configuration Information

Configuration Type ○ Local ● FTP Server ○ TFTP Server

Server Address *

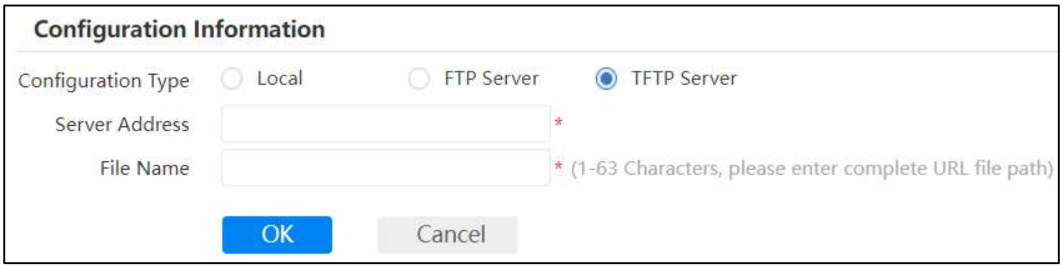
File Name * (1-63 Characters, please enter complete URL file path)

Username * (1-31 Characters)

Password ⓘ ••••••••••• * (1-31 Characters)

Parameter	Description
Server address	Specifies the FTP server address.
File name	Specifies the URL file path of the system file.
Username	Specifies the user name for logging in to the FTP server.
Password	Specifies the password for logging in to the FTP server.

- TFTP method



Configuration Information

Configuration Type ○ Local ○ FTP Server ● TFTP Server

Server Address *

File Name * (1-63 Characters, please enter complete URL file path)

Parameter	Description
Server address	Specify the TFTP server address.
File name	Specify the URL file path of the system file.

Step 5. After the configuration is complete, click “OK”.

Step 6. (Optional) When two versions already exist in the system, a prompt will pop up. Select the file to delete and click “OK”.

Please wait patiently for the upgrade process.

Step 7. After the upgrade is complete, whether to save the configuration and restart the device. Click “OK” to restart the device. Click "Cancel" to upgrade to the new version after the next restart.

Notes

After upgrading through the upgrade package of the "upgrade system" or "hotfix" type, it will take effect without restarting. After upgrading through the "patch" type upgrade package, the system must be restarted to take effect.

1.4.2 Feature Library Upgrade

Only feature libraries within the validity period of the upgrade service can be upgraded. Check the time in the "Valid Time of Upgrade Service" column in the feature library upgrade list to confirm whether the upgrade service is valid. Otherwise, please purchase a new license and update the validity period of the feature library upgrade service.

The feature library upgrade supports automatic upgrade, manual upgrade and immediate upgrade. Automatic upgrade and immediate upgrade require the use of an upgrade server, please perform library upgrade settings first. The library upgrade setting supports users to customize an intranet server as a private upgrade server.

Library Upgrade Settings

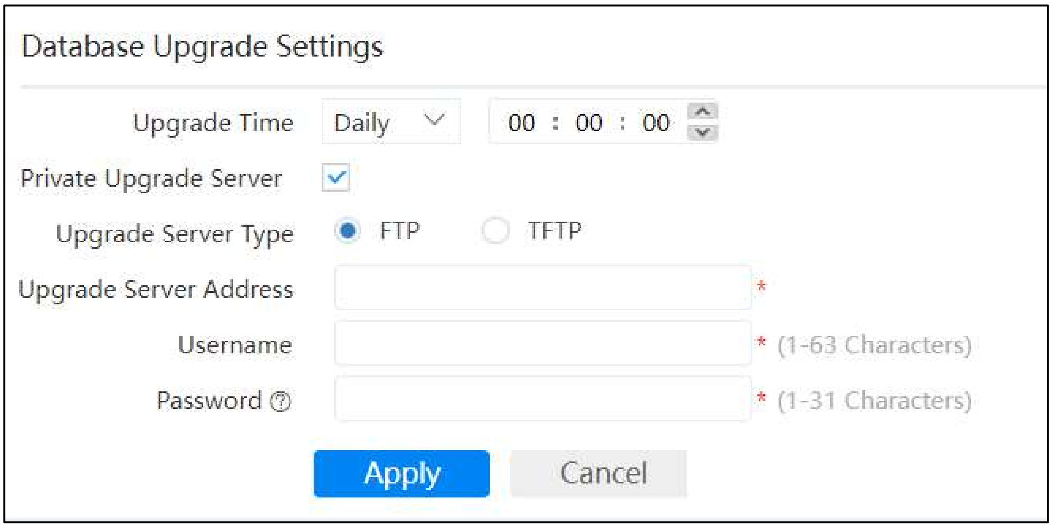
Users can customize a server as the upgrade server of the firewall. You can choose FTP or TFTP to log in to the server to obtain the feature database upgrade package.

Step 1. Choose “System > Upgrade Management > Feature Library Upgrade”.

Step 2. In the “Database Upgrade Settings” area box, set the upgrade time.

Step 3. Enable " Private Upgrade Server".

Step 4. Set private upgrade server parameters.



Database Upgrade Settings

Upgrade Time: Daily; 00 : 00 : 00

Private Upgrade Server: ☑

Upgrade Server Type: ● FTP ○ TFTP

Upgrade Server Address: *

Username: * (1-63 Characters)

Password: * (1-31 Characters)

Parameter	Description
Upgrade time	Set the auto update time. The default update time is 0:00 every day. Within half an hour after the automatic upgrade time is triggered, the firewall will confirm with the upgrade server whether the current feature database version is the latest version. If not, the firewall will automatically upgrade to the latest version. If so, the firewall maintains the current version. For upgrade time, users are advised to fill in the time point with the least traffic, such as 3:00 in the morning.
Private upgrade server	Select the private upgrade server and configure the corresponding parameters.
Upgrade server address	• FTP Select FTP and enter the FTP server address. • TFTP Select TFTP and enter the TFTP server address.
Username	Enter the username for logging in to the FTP server. It needs to be configured only when FTP is selected.
Password	Enter the password for logging in to the FTP server. It needs to be configured only when FTP is selected.

Step 5. After the configuration is complete, click “OK”.

Auto Update

Automatic upgrade needs to configure the upgrade server address in the "Library Upgrade" settings. Upgrade by the update server.

Step 1. Choose “System > Upgrade Management > Feature Library Upgrade”.

Step 2. Select the feature library that needs to be automatically upgraded.

- Select one or more feature databases, and click “Enable Automatic Update”.
- Select the automatic upgrade corresponding to a feature database.

Step 3. In the “Are you sure to enable automatic upgrade" or "Are you sure to enable automatic upgrade in batches" prompt box that pops up, click “OK”.

After confirming to enable, the system will automatically upgrade after detecting a new version of the feature database.

Step 4. To cancel the automatic update function of a feature database, you can uncheck the "Automatic update" check box.

Upgrade Immediately

Immediate upgrade needs to configure the upgrade server address in the "Library Upgrade" settings. Upgrade by the upgrade server.

Step 1. Choose “System > Upgrade Management > Feature Library Upgrade”.

Step 2. Click the “Upgrade Now" button corresponding to a feature database operation.

Step 3. In the displayed confirmation dialog box, click “OK”.

Step 4. The firewall will immediately compare the version of the corresponding feature database with the upgrade server. If the current version is not the latest version, it will immediately upgrade to the latest version.

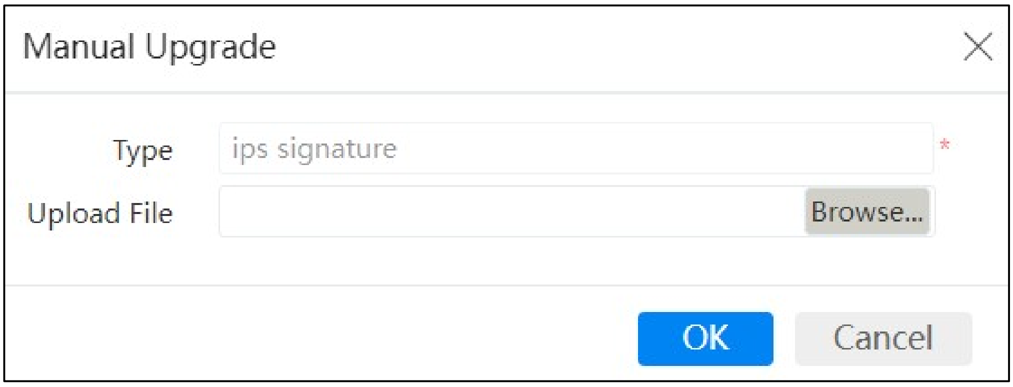
Manual Upgrade

Step 1. Choose “System > Upgrade Management > Feature Library Upgrade”.

Step 2. Click the corresponding "Manual Upgrade" button under a feature database operation.

Step 3. On the displayed manual upgrade page, click “Browse” to select the feature database file saved locally.

Please ensure that the selected feature database upgrade package is consistent with the upgraded feature database type.



Manual Upgrade

Type: ips signature *

Upload File:

Step 4. Click “OK” to import the upgrade package.

Check whether the current version after upgrading is correct. If the current version is the upgraded feature database version, the manual upgrade succeeds.

1.5 Alarm Management

The firewall supports Trap alarms, email alarms, sound alarms and SMS alarms (SMS Modem needs to be installed). Users can specify alarm methods for configuration changes, virus events, attack events, abnormal events, startup events, CPU temperature alarms, CPU fan speed alarms, and chassis fan speed alarms, and can also configure alarm thresholds for NAT port pool utilization, CPU usage, and memory usage, hard disk usage ratio, and interface bandwidth ratio. If the threshold is exceeded, one or more of the alarm methods can be used to alarm.

1.5.1 Configure Alarm Settings

Step 1. Choose “System > Alarm Management > Alarm Settings”.

Step 2. Select the alarm item and alarm method to be enabled.

Alarm settings supports trap alarm, email alarm, sound alarm, and SMS alarm. One or more alarm methods can be selected.

Select the "Select All" check box to enable all alarm methods of all alarm items.

Alarm Item	Description
Configuration changes	When the configuration changes, including adding, deleting, and modifying, an alarm will be triggered.
Virus incident	The virus detection module will trigger an alarm.
Attack event	Attack prevention and intrusion prevention modules generate logs, which will trigger alerts.
Abnormal event	Administrator login lock, HA status changes, IPSec VPN tunnel disconnection log generation, and received emergency response messages will trigger alarms.
Start event	The firewall software restart and hardware restart will trigger an alarm.
CPU temperature alarm	If the CPU temperature of the device is too low or too high, an alarm will be triggered. Different models of devices have different alarm thresholds, and the thresholds cannot be modified.
CPU fan speed alarm	If the CPU fan speed is too low, an alarm will be triggered. Different models of devices have different alarm thresholds, and the thresholds cannot be modified.
Chassis fan speed alarm	If the fan speed of the chassis is too low, an alarm will be triggered. Different models of devices have different alarm thresholds, and the thresholds cannot be modified.
NAT port pool utilization	When the utilization of the NAT port pool reaches the set threshold, an alarm is issued. The default threshold of NAT port pool utilization is 80%, which can be modified by the user according to the actual situation.
CPU usage	When the CPU usage reaches the set threshold, an alarm is issued. The default threshold of CPU usage is 80%, which can be modified by the user according to the actual situation.
Memory usage	When the memory usage reaches the set threshold, an alarm will be issued. The default threshold of memory usage is 80%, which can be modified by the user according to the actual situation.

Alarm Item	Description
HDD usage	When the hard disk usage reaches the set threshold, an alarm will be issued. The default threshold of hard disk usage is 80%, which can be modified by the user according to the actual situation.
Interface Bandwidth Ratio	When the interface bandwidth ratio reaches the set threshold, an alarm is issued. The default threshold of the interface bandwidth ratio is 80%, which can be modified by the user according to the actual situation. Click “Advanced” to set the bandwidth ratio and alarm mode of each interface. When the interface alarm advanced configuration is not configured, the interface alarm global configuration takes effect. When interface alarms and global alarm configurations exist at the same time, the advanced configuration of interface alarms takes effect.

Step 3. After the configuration is complete, click “Apply”.

1.5.2 Configure Trap Alarms

The firewall supports sending SNMP trap alarm to the management device. The user needs to add a host IP address or domain name that receives trap packets. At the same time, you need to specify the SNMP version and community string used to send trap packets. When using SNMPv3, users need to specify SNMPv3 users. By default, the port used to send trap packets is 162.

Step 1. Choose “System > Alarm Management > Trap Alarm”.

Step 2. Click “Add”.

Step 3. Add trap hosts.

Parameter	Description
Trap host	Specifies the IP address or domain name of a host receiving Trap packets.
Port	Specifies the port number used to send Trap packets. By default, the port used to send Trap packets is 162. Modify this item when the user needs to use a port number other than the default port, such as when port 162 is occupied.
SNMP version	Select the SNMP version.
group word	When v1 or v2 is selected for the SNMP version, the community must be specified.

Parameter	Description
SNMPv3 user	When v3 is selected as the SNMP version, SNMPv3 members must be selected. To create a new member, select “Add SNMPv3 User”.

Step 4. After the configuration is complete, click “OK”.

1.5.3 Configure Email Alarm

When email alarm is selected, the firewall, as the sender, will send email alarm information to the email address specified by the user.

SMTP Server Settings

Configure the SMTP server address and email address used by the firewall to send email alarms. If the SMTP server side needs to verify the sender, you also need to fill in the sender's user name and password.

Step 1. Choose “System > Alarm Management > Email Alarm”.

Step 2. Set SMTP server parameters.

Parameter	Description
SMTP name	Indicates the name of the SMTP server.
SMTP server	Specify the IP address or domain name of the SMTP server.
Email sending address	Specify the email address of the sender.
SMTP authentication	Check "SMTP Authentication" to enable this feature. You need to fill in the sender's username and password.
Username	
Password	
Email sending interval	Configure the email sending interval.

Step 3. After the configuration is complete, click “OK”.

Add Recipient Email Address

Configure the recipient's address information, and the user can specify up to 3 recipients.

Step 1. Choose “System > Alarm Management > Email Alarm”.

Step 2. Click “Add” in the “Email Address List” area box.

Step 3. Add an email address.

Parameter	Description
Email address	Fill in the recipient's email address.
SMTP server	Select an SMTP server.

Step 4. After the configuration is complete, click “OK”.

After adding successfully, the recipient's email address is displayed in the email address list.

1.5.4 Interrupt Sound Alarm

If the firewall has enabled the sound alarm in the alarm settings, after the alarm is triggered, the firewall will continue to alarm. To interrupt the audible alarm, proceed as follows.

Step 1. Select "System > Alarm Configuration > Sound Alarm".

Step 2. Click “Interrupt Sound Alarm”.

Step 3. After clicking, it will return the execution success, and the alarm music will be disabled.

1.6 License

The license is used to control certain modules of the firewall.

1.6.1 Import License

The functions that require license authorization can be used normally only after the firewall imports a valid license.

Step 1. Choose “System > License”.

Step 2. Click “Import”.

Step 3. Click “Browse” to select a license file.

Step 4. Before importing a license, you can click the drop-down arrow of “License Details” to query the license content.

Check whether the maximum number of functions supported in the license, validity period, and license type are correct.

Step 5. Click “OK”.

After importing successfully, it prompts whether to restart the device.

Step 6. Click “OK”, restart the device, and the license content takes effect.

If you click “Cancel”, the license content will take effect after the device is restarted next time.

Please save the configuration before restarting the device.

1.6.2 View License

The modules and features that can be controlled by a formal license are shown in the table below.

Function	Description
IPSec Tunnal Number	The maximum number of IPSec tunnels that can be created by the IPSec function of the firewall. The official license has no expiration date or validity period.
Concurrent connection Number	The maximum number of concurrent connections that the firewall can support, and the official license has no expiration time and validity period.
Intrusion prevention system	Firewall exploit protection and anti-spyware feature license. A formal license has no expiration date or validity period. The current status is displayed as 🏅, indicating that the license status of the intrusion prevention function is normal. The current status is displayed as 🏅, indicating that the Intrusion Prevention feature license has expired or the license for this module has not been imported.
IPS Library Upgrade	Firewall vulnerability protection and anti-spyware feature database upgrade license, after the license expires, the IPS feature database cannot be upgraded offline or online. The expiration time is calculated from the time when the license is imported, and is based on the number of years of the upgrade service purchased by the user. If a user purchases a one-year intrusion prevention feature database upgrade service, and the time to import the license is 2017-07-20 18:00:00, the expiration time is 2018-07-20 18:00:00. The validity period displays the remaining days of the license. When the remaining days are less than 30 days (inclusive), the firewall will send an alarm in the log. The current status is displayed as 🏅, indicating that the status of the intrusion prevention feature database upgrade license is normal. The current status is displayed as 🏅, indicating that the license for upgrading the intrusion prevention feature database has expired or the license for this module has not been imported.
Cloud sandbox	Firewall cloud sandbox function license. The function is unavailable after the license expires. The current status is displayed as 🏅, indicating that the license status of the cloud sandbox function is normal. The current status is displayed as 🏅, indicating that the cloud sandbox feature license has expired or the license for the module has not been imported.

Function	Description
Anti-virus	Firewall Anti-Virus feature license. A formal license has no expiration date or validity period. The current status is displayed as 🏵, indicating that the license status of the anti-virus function is normal. The current status is displayed as ⚪, indicating that the license for the anti-virus function has expired or the license for this module has not been imported.
Anti-virus database upgrade	Firewall anti-virus feature database upgrade license; after the license expires, the AV feature database cannot be upgraded offline or online. The expiration time is calculated from the time when the license is imported, and is based on the number of years of the upgrade service purchased by the user. If a user purchases a one-year antivirus feature database upgrade service, and the time to import the license is 2019 - 07 - 20 18:00:00, the expiration time is 20 20 - 07 - 20 18:00:00. The validity period displays the remaining days of the license. When the remaining days are less than 30 days (inclusive), the firewall will send an alarm in the log. The current status is displayed as 🏵, indicating that the status of the antivirus feature database upgrade license is normal. The current status is displayed as ⚪, indicating that the antivirus feature database upgrade license has expired or the license for this module has not been imported.
Threat intelligence	Firewall threat intelligence detection license. The function is unavailable after the license expires. The current status is displayed as 🏵, indicating that the threat intelligence function license status is normal. The current status is displayed as ⚪, indicating that the license for the Threat Intelligence feature has expired or the license for the module has not been imported.
Threat Intelligence Library Upgrade	Firewall threat intelligence library upgrade license; after the license expires, the threat intelligence library cannot be upgraded offline or online. The expiration time is calculated from the time when the license is imported, and is based on the number of years of the upgrade service purchased by the user. If a user purchases a one-year threat intelligence database upgrade service, and the time to import the license is 2019-07-20 18:00:00, the expiration time will be 2020-07-20 18:00:00. The validity period displays the remaining days of the license. When the remaining days are less than 30 days (inclusive), the firewall will send an alarm in the log. The current status is displayed as 🏵, indicating that the threat intelligence database upgrade license status is normal. The current status is displayed as ⚪, indicating that the Threat Intelligence Library upgrade license has expired or the license for this module has not been imported.

Function	Description
App Identification library upgrade	Firewall application identification feature database upgrade license; after the license expires, the application identification feature database cannot be upgraded offline or online. The expiration time is calculated from the time when the license is imported, and is based on the number of years of the upgrade service purchased by the user. If the user purchases a one-year application identification library upgrade service, and the time to import the license is 2019-07-20 18:00:00, the expiration time is 2020-07-20 18:00:00. The validity period displays the remaining days of the license. When the remaining days are less than 30 days (inclusive), the firewall will send an alarm in the log. The current status is displayed as 🏅, indicating that the application recognition library upgrade license status is normal. The current status is displayed as ⚪, indicating that the application recognition library upgrade license has expired or the license for this module has not been imported.
URL library upgrade	Firewall URL feature database upgrade license; after the license expires, the URL feature database cannot be upgraded offline or online. The expiration time is calculated from the time when the license is imported, and is based on the number of years of the upgrade service purchased by the user. If a user purchases a one-year URL feature database upgrade service, and the time to import the license is 2019-07-20 18:00:00, the expiration time is 2020-07-20 18:00:00. The validity period displays the remaining days of the license. When the remaining days are less than 30 days (inclusive), the firewall will send an alarm in the log. The current status is displayed as 🏅, indicating that the URL feature database upgrade license status is normal. The current status is displayed as ⚪, indicating that the URL feature database upgrade license has expired or the license of this module has not been imported.
System function	The basic function license of the firewall; after the license expires, do not affect the policy delivery of the basic functions of the firewall. The current status is displayed as 🏅, indicating that the system function license status is normal. The current status is displayed as ⚪, indicating that the system feature license has either expired or the license for this module has not been imported.
Virtual system function	The basic function license of the firewall virtual system; after the license expires, do not affect the policy delivery of the basic function of the firewall. The current status is displayed as 🏅, indicating that the system function license status is normal. The current status is displayed as ⚪, indicating that the system feature license has either expired or the license for this module has not been

Function	Description
	imported.

1.7 High Availability

1.7.1 Overview

High availability is a very important function for users who require high service continuity.

The firewall supports HA in routing mode and HA in bridge mode.

- Routing mode: Realize two dual-machine hot standby modes: dual-master routing load balancing and master-standby routing redundancy backup. When a firewall fails, the other firewall can take over the routing and forwarding work in time, providing users with transparent switching and improving network reliability.
- Transparent mode: It supports HA redundancy backup and fast switching in bridge mode.

1.7.2 Configure HA

When configuring HA, users need to confirm whether the current requirement is routing mode networking or bridge mode networking, and whether the dual-machine is redundant backup or load balancing.

Step 1. Choose “System > High Availability”.

Step 2. Check “Enable HA” on the “HA Settings” page.

HA must be enabled for the HA function to take effect. It is recommended to connect the heartbeat cable first, and then enable the HA function.

Step 3. Set whether to enable " Configuration Synchronization".

After the configuration synchronization function is enabled, the firewall will automatically synchronize the configuration from the primary wall of HA group 0 to the backup wall of HA group 0.

It should be noted that addresses whose interface address type is float will be synchronized to the standby wall; addresses whose interface address type is static will not be synchronized to the standby wall.

Step 4. Set whether to enable "Dynamic information synchronization ".

After it is enabled, the firewall will automatically synchronize dynamic information such as sessions from the primary wall of HA group 0 to the standby wall of HA group 0.

Step 5. Set whether to enable "Asymmetric mode".

This function is mainly aimed at the inconsistency of the incoming and outgoing paths of the network environment of the users in the dual-active environment in the transparent mode, that is, the data is forwarded from firewall A in the dual-active environment, but the response is received from firewall B. For the rest HA environments, it is recommended to check this function.

If "Asymmetric Mode" is selected, both the primary wall and the standby wall in HA group 0 will forward data and synchronize the session table, and HA group 1 does not need to be configured.

After enabling this function, users can view the management status (Manage_State) of the firewall through the command **show ha group 0**. The firewall displayed as MASTER is the primary firewall of group 0, and the firewall displayed as BACKUP is the backup firewall of group 0. Both firewalls forward data, but the configuration information and dynamic information of the firewalls are synchronized from the primary firewall in group 0 to the standby firewall in group 0.

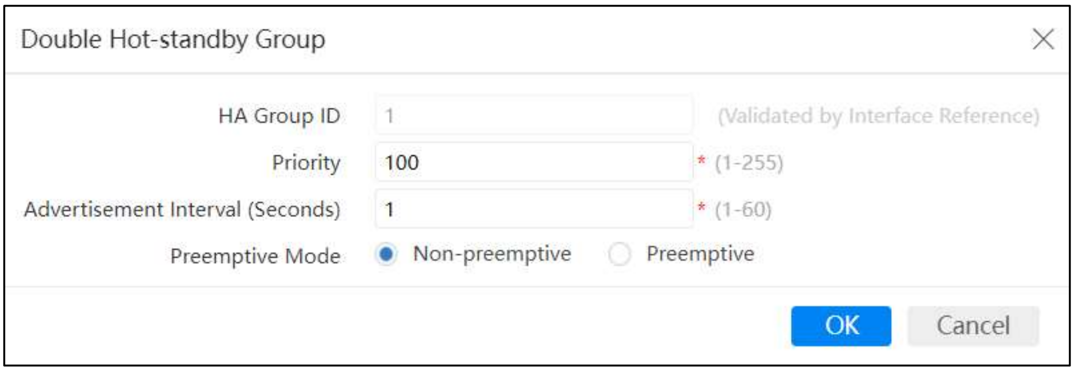
Step 6. Set the parameters of the high availability heartbeat port.

Parameter	Description
HA communication interface (heartbeat interface)	Select one of the physical interfaces that is not referenced by other modules as the HA heartbeat interface, and the two high-availability firewalls are connected through the heartbeat interface. The heartbeat interface can only work in routing mode. If the selected interface works in switching mode, after HA is applied, the interface will automatically change to routing mode, and the local interface IP will be automatically configured as the IP of the interface.
HA communication interface	The default port number is UDP 6260, users are advised not to modify this configuration. The two connected firewalls communicate with the HA module through this port.
Local interface ip	The interface IP of the local heartbeat port must be in the same network segment as the peer interface IP.
Opposite interface IP	The peer interface IP that is connected to the local heartbeat must be on the same network segment as the local interface IP.

Step 7. Add an HA group.

The configuration of the HA group determines whether the currently configured firewall works in the MASTER (main) state or in the BACKUP (standby) state. Therefore, when configuring the HA group, the user needs to understand the network topology and the functions that the firewall needs to implement.

1. Click “Add”.
2. Configure a double hot standby group.



Double Hot-standby Group

HA Group ID: 1 (Validated by Interface Reference)

Priority: 100 * (1-255)

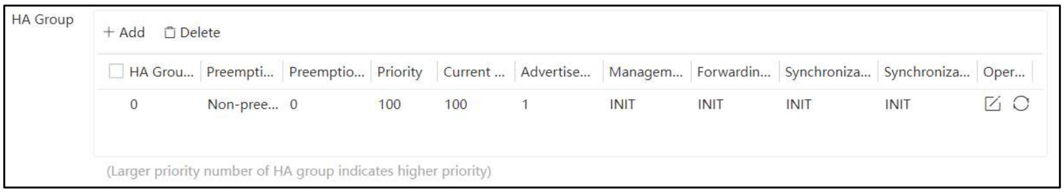
Advertisement Interval (Seconds): 1 * (1-60)

Preemptive Mode: ● Non-preemptive ○ Preemptive

Parameter	Description
HA group ID	The ID policy of the group to which the interface belongs. You can configure two groups, group 0 and group 1, respectively. Which group the interface belongs to needs to be added in the interface configuration. When it is necessary to work in dual-machine hot standby mode, each device only needs to configure group 0. When it is required to work in load balancing mode, if the asymmetric mode is not checked, each device needs to be configured with group 0 and group 1. Each group will elect a corresponding MASTER (primary) and BACKUP (standby). Therefore, the load balancing mode (dual-primary mode) requires the user to add group 1.
Priority	The firewall with high priority is re-elected as the new master wall. When the priorities are the same, the IP addresses of the heartbeat ports will be compared, and the firewall with the higher IP address value of the host on the same network segment is the master wall. At the same time, the priority is associated with the weight value of interface monitoring and link detection. When an interface or link fails, the corresponding weight value will be deducted from the priority for re-election.
Advertisement interval	The interval for sending the detection information between heartbeat ports. The default is 1 second.
Preemptive mode	In non-preemptive mode, after the initial configuration of HA is completed, the device that starts first will change to the MASTER state (master state). In the preemption mode, MASTER fails, and the backup wall is elected as the new master wall. If the original MASTER returns to normal, it will regain its status as the master wall.
Preemption delay	The delay time before preemption starts after all HA states are normal. For example, if it is set to 30 seconds, after all HA states are normal, wait for 30 seconds and start preemption.

3. Click “OK”.

The configured HA group is displayed in the HA group list.



HA Group

+ Add   Delete

□ HA Grou...	Preempti...	Preemptio...	Priority	Current ...	Advertise...	Managem...	Forwardin...	Synchroniza...	Synchroniza...	Oper...
0	Non-pree...	0	100	100	1	INIT	INIT	INIT	INIT	

(Larger priority number of HA group indicates higher priority)

The description of the parameters that need to be explained is shown in the table below.

Parameter	Description
Management state	• INIT: HA not enabled • MASTER: The device is currently the master wall • BACKUP: The device is currently the backup wall • FAULT: HA is working abnormally
Forwarding state	• INIT: HA not enabled • MASTER: The device is currently forwarding data • BACKUP: The device is not currently forwarding data
Synchronization configuration	Master wall: • INIT: HA not enabled • SYNC_CFG: Synchronize initial configuration • COMPLETE: Synchronization configuration is complete Standby wall: • INIT: HA not enabled • COMPLETE: Synchronization configuration is complete • SYNCING: Synchronizing configuration
Synchronization dynamic information	Master wall: • INIT: HA not enabled • SYNC_module_name: Synchronization module configuration • COMPLETE: Synchronization configuration is complete Standby wall: • INIT: HA not enabled • COMPLETE: Synchronization configuration is complete • SYNCING: Synchronizing configuration

Step 8. After the configuration is complete, click “Apply”.

After starting HA, the heartbeat interface will monitor whether there are other devices that are also working in HA mode at the specified interval period. When the non-preemptive mode is configured, if it does not receive any HA heartbeat information from other devices, the device will actively become MASTER state (master state). If the HA heartbeat information from other devices can be received after startup, the device first requests configuration synchronization, and then requests dynamic information synchronization after the synchronization is successful. After the dynamic information synchronization is successful, it will detect its own monitoring information. If the monitoring information is normal, it will set the state to BACKUP state.

If there is no abnormality in the monitoring information, if the preemption mode is configured, HA election will be carried out. The election method is priority + IP address, and the higher the priority value, the higher the priority. In the case of the same priority, the heartbeat port IP addresses will be compared, and the higher the host address value of the IP address value, the higher the priority. The winning party sets the state to MASTER state, and then sends an advertisement packet. After receiving the advertisement packet, the original master wall will switch from the MASTER state to the BACKUP state.

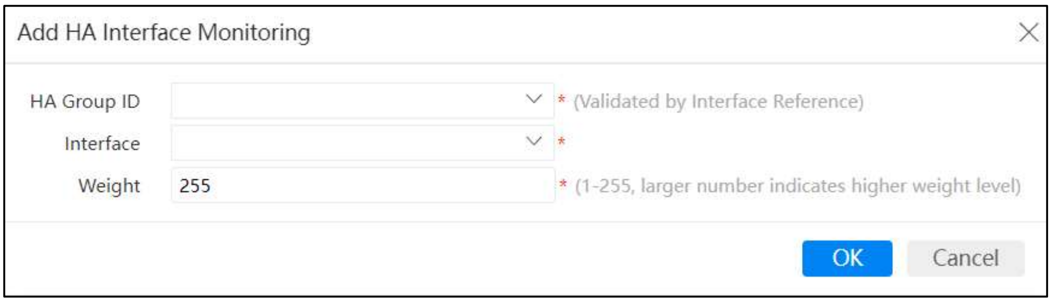
1.7.3 (Optional) Configure HA Interface Monitoring

HA interface monitoring is used to monitor the status of the upstream and downstream service interfaces of the heartbeat interface. When the monitored interface fails, the weight value is deducted according to the priority configured by the user to determine whether the firewall performs active/standby switchover.

Step 1. Choose “System > High Availability”.

Step 2. Click “Interface Monitoring”.

Step 3. Configure monitoring parameters for the HA interface.



Add HA Interface Monitoring

HA Group ID: * (Validated by Interface Reference)

Interface: *

Weight: 255 * (1-255, larger number indicates higher weight level)

Parameter	Description
HA group ID	HA group to which the monitored interface belongs.
Interface	The name of the interface to be monitored.

Weight	After the monitored interface fails, the priority in the HA global configuration will be deducted from the corresponding weight value. The election is carried out again, and the one with higher priority is elected as the master wall, and the higher the priority value, the higher the priority.

Step 4. Click “OK”.

1.7.4 Configure link detection

Link detection mainly detects whether the IP address configured by the user is currently connected, and if the IP address fails, deducts the weight value from the priority configured by the user to determine whether the firewall performs active/standby switchover.

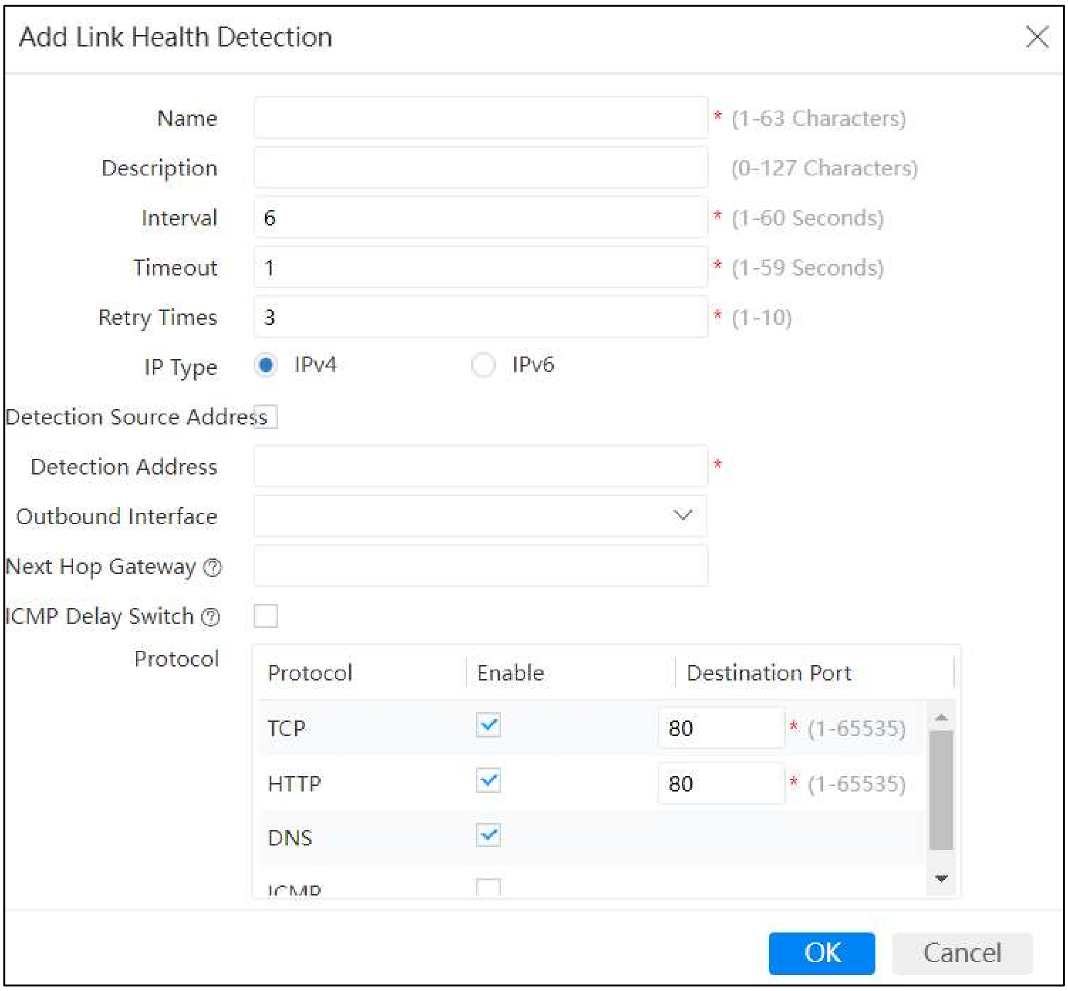
Step 1. Choose “System > High Availability”.

Step 2. Click “Link Detection”.

Step 3. Click “Add”.

Step 4. Select the HA group ID.

Step 5. Select a detection object. If there is no detection object yet, please add a detection object first.



Name * (1-63 Characters)

Description (0-127 Characters)

Interval 6 * (1-60 Seconds)

Timeout 1 * (1-59 Seconds)

Retry Times 3 * (1-10)

IP Type ● IPv4 ○ IPv6

Detection Source Address □

Detection Address *

Outbound Interface

Next Hop Gateway

ICMP Delay Switch □

Protocol

Protocol	Enable	Destination Port
TCP	☑	80 * (1-65535)
HTTP	☑	80 * (1-65535)
DNS	☑	
ICMP	□	

Parameter	Description
Name	Set the name of the link detection object.
Description	Describe the link detection object
Interval	The interval at which ping packets are sent to detect IP addresses.
Timeout	The number of seconds within which a response packet is not received from the probe IP is considered a timeout. The timeout setting must be less than the interval time.
Retry times	The number of retries after a timeout. If the upper limit of the number of attempts is reached and there is still no response packet, it is judged that the detection IP address is invalid.
IP type	Select an IP type. The IP type supports both IPv4 and IPv6 types.

Parameter	Description
Detection address	The detected IP address is the destination IP address of the detection. It is recommended that users choose a stable working IP address in the network as the detection IP.
Outbound interface	The detection interface, on which an IP address with the address type static needs to be configured as the source address for sending detection packets.
Next hop gateway	Configure the IP address of the next gateway to the destination network.
ICMP delay switch	This function is used when configuring the ICMP switch.
Protocol	• TCP • HTTP • DNS • ICMP The corresponding function takes effect after it is enabled.

Step 6. Configure weights for detection objects.

After the detected IP fails, the priority in the HA global configuration will be deducted by the corresponding weight value. The election is carried out again, and the one with higher priority is elected as the main wall, and the higher the priority value, the higher the priority.

Step 7. After the configuration is complete, click “OK”.

1.8 Centralized Management

Centralized management refers to the centralized management of the firewall through the intelligent management and analysis system. The smart management analysis system delivers configurations to the firewall through the HTTPS protocol. The firewall uses random ports to actively connect to the ports provided by the management analysis system. The smart management analysis system obtains resource monitoring data such as the CPU usage rate of the firewall through SNMP.

1.8.1 Restrictions and Precautions

- To use centralized management, the communication interface must enable the SNMP service.
- To use centralized management, the smart management analysis system must be set as a

trusted host and the SNMP service must be enabled.

- To use centralized management, the smart management analysis system must be set as a trap host.
- If the centralized management server wants to obtain the firewall logs, the firewall must be configured to send the logs to the centralized management server.
- After the firewall device is centrally managed through the smart management and analysis system, the default update server address and threat intelligence update address of the device are changed to the addresses of the smart management and analysis system. The equipment is configured and upgraded through the intelligent management analysis system. After the centralized management is cancelled, the device's update server address and threat intelligence update address return to the default addresses.

1.8.2 Enable Centralized Management

Step 1. Select "System > SMAC".

Step 2. Specify the centralized management server address and communication port.

Parameter	Description
Centralized management server address	Enter the IP address of the management analysis system. Both IPv4 and IPv6 addresses are supported.
Port	Enter the port used by the management analysis system, and the port number must be 3601. The management analysis system uses HTTPS protocol port 3601 to communicate with the firewall.

Step 3. Configure advanced parameters.

Parameter	Description
Local interface	Select the interface through which the firewall communicates with the management analytics platform.
Local address	Select the IP address for communication between the firewall and the management analysis platform.

Step 4. Select " Enable " to enable the centralized management function.

Step 5. After the configuration is complete, click “Apply”.

- If the connection status is "Online", it means that the connection between the firewall and the management and analysis system is normal.

- If the connection status is "offline", it means that the connection between the firewall and the management and analysis system is not normal.

1.8.3 Disable Centralized Management

If a certain firewall needs to cancel the centralized management due to its own problems. You can uncheck the “Enabled” checkbox and click “Apply”. At this time, "The firewall is actively detached from the centralized management system (SMAC)" will pop up. Please read the instructions in the dialog box carefully according to the actual situation, select an appropriate policy mode, and click “OK”.

After canceling the centralized management, the device restores the default upgrade server address.

1.8.4 Configure Functions Required for Centralized Management

Configuration Function Description

In addition to configuring centralized management, the functions in the table below must also be configured for better centralized management.

Function	Description	Configuration
SNMP service	The intelligent management analysis system obtains the status information of the firewall through the SNMP protocol, such as CPU usage, memory usage, CPU temperature, etc. The SNMP service of the interface needs to be enabled on the firewall device, the smart management analysis system needs to be set as a trusted host, and the service of the trusted host is set to SNMP.	To enable the SNMP service, you can manually configure it on the firewall device, or you can configure the template through the smart management and analysis system and then deliver the configuration uniformly. Configure through the device side: • Manually enable the SNMP management mode of the interface. • Manually add a trusted host, the address is the address of the smart management analysis system, and the service is set to SNMP. • Configure SNMP manually. Configure through the intelligent management analysis system: Choose “Device Management > Template Configuration > SNMP Settings”. After configuring the SNMP template and delivering the template to the firewall, the SNMP management mode of the corresponding interface of the firewall will be automatically enabled, and the smart management analysis system will be automatically added as a trusted host, and the service will be set to SNMP. After the configuration is complete, the template must be delivered to the firewall via ⇅.

Function	Description	Configuration
Alarm settings	The smart management analysis system receives trap alarm information sent by managed devices through port 162, such as attack event alarms, abnormal event alarms, CPU temperature alarms, and the like.	Trap alarms can be configured on the device side, or can be delivered uniformly after the smart management analysis system configures templates. Configure through the device side: • Select the alarm setting, and enable the trap alarm of the alarm item. • Add a trap host. The IP address of the Trap host is set to the IP address of the intelligent management analysis system. Configure through the intelligent management analysis system: Choose “Device Management > Template Configuration > Alarm Management”. Default alarm settings and default Trap alarms take effect on all managed devices. If you need to configure alarms and trap hosts for a managed device separately, you can set them through " Add ". After the configuration is complete, the template must be delivered to the managed device via ⇅.

Function	Description	Configuration
Log settings	Managed devices upload logs to the smart management analysis system through the log sending function.	Adding a log server and setting log output can be configured on the managed device, or can be distributed uniformly after the smart management analysis system configures the template. Configure through the device side: Add the smart management analysis system as a log server on the device, and set the log to be sent to the smart management analysis system. Configure through the intelligent management analysis system: Choose “Device Management > Template Configuration > Log Configuration”. By default, the smart management analysis system has been added as a log server, and the log server can be edited. The default log outgoing setting is valid for all managed devices. If you need to separately configure log output for a managed device, you can set it through " Add ". After the configuration is complete, the template must be delivered to the managed device via ⇅.

(Optional) Enable the SNMP Service on the Communication Interface

Enable the SNMP service on the interface on the firewall side.

Step 1. Select "Network > Interface" to find the interface through which the firewall communicates with the smart management analysis system.

Step 2. Click the interface name or the corresponding Edit button.

Step 3. Configure the interface mode, IP address, and management mode.

Note that the management method must enable SNMP. The firewall uploads resource monitoring data such as CPU usage and memory usage to the smart management analysis system through SNMP.

Step 4. After the configuration is complete, click “OK”.

(Optional) Set the Smart Management Analysis System as a Trusted Host

The configuration on the firewall side sets the smart management analysis system as a trusted host.

Step 1. Select "System > Device Management > Administration Host".

Step 2. On the “Trusted Host” page, click “Add”.

Step 3. Set the smart management analysis system as a trusted host.

The IP address is set as the IP address of the intelligent management analysis system.

Select SNMP for the service. The firewall uploads resource monitoring data such as CPU usage and memory usage to the smart management analysis system through SNMP.

Step 4. After the configuration is complete, click “OK”.

(Optional) Configure Logs to Be Sent to the Smart Management Analysis System

Add the smart management analysis system as a log server on the firewall side, and set the log to be sent to the smart management analysis system.

Step 1. Choose “Data Center > Log > Log Configuration”.

Step 2. Click “Log Server”.

Step 3. Click “Add”.

Set server parameters. The server address must be the address of the smart management analysis system.

Types can be either text or binary.

Step 4. After the configuration is complete, click “OK”.

Step 5. Click “Log Outgoing" tab and set all the log servers as the log servers corresponding to the added smart management analysis system.

Step 6. After the configuration is complete, click “Apply”.

1.9 Cloud Link Protection

1.9.1 Cloud Protection

Cloud protection refers to the services provided by cloud protection of Tianyu Cloud. After opening the corresponding service, the firewall will upload the IP, URL and other information to Tianyu Cloud, and Tianyu Cloud will return the detection result to the firewall after detection.

The cloud protection of Tianyu Cloud can •provide firewalls with cloud services such as virus cloud detection and killing, URL cloud identification, application cloud identification, cloud sandbox, and emergency response.

Step 1. Select "System > Collaboration > Cloud Link Protection".

Step 2. Please enable or disable cloud services as needed.

Parameter	Description
Virus cloud checking and killing	It is enabled by default. Virus cloud checking and killing is an enhanced function of the anti-virus function of the firewall, and the anti-virus function of the firewall must be enabled at the same time for the virus cloud checking and killing function to take effect. The firewall sends the MD5 code of the files passing through the local to Tianyu Cloud for virus cloud checking and killing. The cloud virus database has a larger scale and is updated more timely, which can improve the virus detection rate of the firewall.
URL cloud recognition	It is enabled by default. URL cloud identification is an enhanced function of the URL filtering function of the firewall. The URL filtering function of the firewall must be enabled at the same time for the URL cloud identification to take effect. The URL cloud recognition function is an effective supplement to the predefined URL filtering class in the firewall URL filtering function. When a certain URL cannot be queried for its corresponding category in the predefined URL filtering class, if the user has enabled the URL cloud recognition function, the URL will be sent to the URL cloud for further query analysis.
Cloud sandbox	It is enabled by default. The cloud sandbox is used with the virus detection function and is mainly used to detect unknown viruses. After the cloud sandbox is enabled, the firewall sends suspicious files detected by the antivirus as black files and gray files to the cloud sandbox. Trigger suspicious files to run through the cloud sandbox to determine whether the files are malicious.
App Cloud Recognition	It is enabled by default and the default action is auto. The cloud identification library can greatly increase the order of magnitude of the identification library, supplement the local application identification library, and speed up the firewall's identification of threats.
Emergency Response	It is enabled by default, and the default action is automatic. The emergency response is issued by Tianyu Cloud, which is used to urgently notify users of the vulnerabilities in the system or the latest threat information. The emergency response checks the user's vulnerability protection or anti-spyware configuration, and prompts the user to upgrade the IPS library or threat intelligence library. In the case of " automatic response", the system will automatically update the intrusion prevention feature database and threat intelligence database. In the case of " manual response", only an alarm is given, and the user needs to manually upgrade.

Step 3. After the configuration is complete, click “Apply”.

1.9.2 Cloud Intelligence Platform

After purchasing a threat intelligence license on the firewall, the firewall supports both threat intelligence cloud detection and local detection. In order to ensure the local detection results of threat intelligence, users need to update the threat intelligence library on the device in time.

Enable Threat Intelligence Cloud Detection

The threat intelligence cloud detection function refers to uploading firewall logs to Tianyu Cloud, and performing threat intelligence collisions in the cloud. Threat intelligence cloud detection is enabled by default.

Enable Local Threat Intelligence Detection

After selecting the "Local intelligence detection" check box, enable the local threat intelligence detection function. This feature is disabled by default. After enabling or disabling the local threat intelligence detection function, click “Apply”.

When the threat intelligence library upgrade function expires, it is recommended to disable the local threat intelligence detection function to avoid false reporting.

Upgrade Local Threat Intelligence Database

The firewall can perform threat intelligence detection on the real-time traffic of the firewall through the local threat intelligence library. In order to ensure the local detection results of threat intelligence, users need to update the threat intelligence library on the device in time.

The threat landscape library supports automatic upgrades, manual imports, and immediate upgrades. By default, "Auto Update" is selected.

- Automatic upgrade

The firewall is upgraded through the default cloud server.

Automatic upgrade periodically checks whether the version number of the current intelligence database is consistent with the latest intelligence database version number according to the configured upgrade period. When the latest intelligence database version number is greater than the current intelligence database version number, it will automatically upgrade. The intelligence library is automatically updated every 6 hours by default, and users can modify it to other time periods.

- Upgrade immediately

The firewall is upgraded through the default upgrade server. Users do not need to upgrade according to the upgrade cycle, just click "Upgrade immediately". After confirming that you want to upgrade immediately, the threat intelligence library is upgraded to the latest version.

- Import manually

Click “Manual Import”, select the desired threat intelligence database file, and click “OK”.

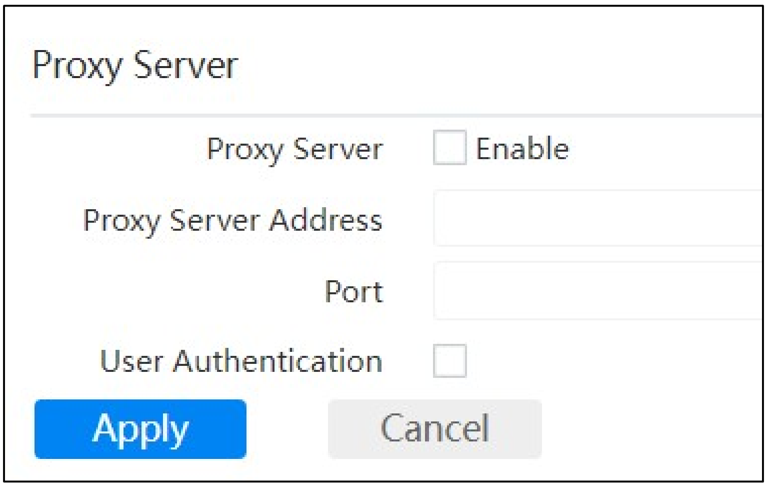
After the configuration is complete, click “Apply”.

Configure Proxy Server

When the firewall in the user environment cannot communicate directly with the cloud protection and cloud intelligence platform, a proxy server can be set. The proxy server works on the cloud protection and cloud intelligence platforms at the same time.

Step 1. Select the "Enable" checkbox to enable the proxy server configuration.

Step 2. Configure proxy server parameters.



Proxy Server

Proxy Server □ Enable

Proxy Server Address

Port

User Authentication □

Parameter	Description
Proxy server address	Enter the address of the proxy server.
Port	Enter the port number of the access proxy server.
User authentication	After selecting "User Authentication", enable user authentication, and user name and password need to be configured.
Username	Enter a username for the proxy server. The user name does not not include special characters such as " ! # ￥ %... * ( ) +{}|"":. Otherwise, the connection may fail.
Password	Enter the corresponding password.

Step 3. After the configuration is complete, click “Apply”.

1.10 Certificate Management

Certificate management is a function of PKI. It is mainly used to manage trusted CAs, perform trusted CA authentication, import and export certificates, and generate request files.

1.10.1 Apply for a Certificate

The firewall supports applying for the certificate offline. Generate a certificate request file on the device and import the certificate request file to the CA center to apply for a certificate. After the certificate is approved, import the approved certificate file.

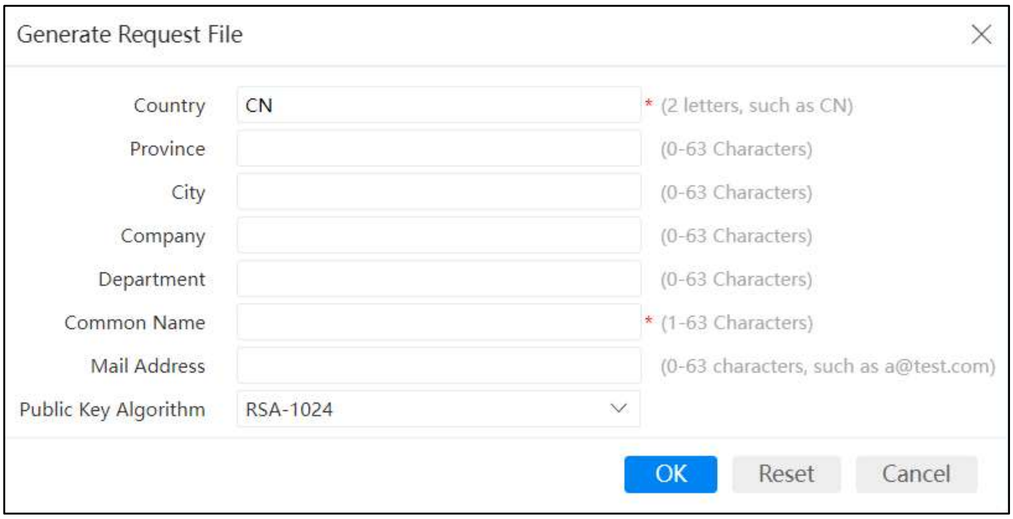
Generate Request File

The request file includes user information, public key, etc., and is signed with its own private key. The request file is used to apply for a certificate offline from the CA center. The CA center can be a local CA center or a trusted third-party CA center.

Step 1. Choose “System > Certificate Management > Request File”.

Step 2. Click “Generate Request File”.

Step 3. Configure the parameters of the request file.



Generate Request File

Country	CN	* (2 letters, such as CN)
Province		(0-63 Characters)
City		(0-63 Characters)
Company		(0-63 Characters)
Department		(0-63 Characters)
Common Name		* (1-63 Characters)
Mail Address		(0-63 characters, such as a@test.com)
Public Key Algorithm	RSA-1024	

The country and common name must be configured, and the other parameters can be selected and configured as required.

Public key algorithms support RSA-1024, RSA-2048 and SM2-256.

Notes

The characters supported by provinces, cities, companies, and departments in the request file include letters, numbers, Chinese characters, single quotes "'", dots ".", hyphens "-", plus signs "+", equal signs "= ', Open brackets "(", right brackets ")", colons ":", "@" symbols or spaces. Spaces cannot appear at the beginning and end. Entering other unsupported characters may cause VPN negotiation failure and other problems when citing certificates.

Step 4. Click “OK”.

The generated request file is displayed in the request file list.

Export Request File

After generating the request file, you must export the request file to the management host, and import the request file to the CA center for certificate application.

Step 1. Select the request file to export and click ⇱ under Operation.

Step 2. Select the certificate format supported by the device.

The certificate format supports PEM and DER formats. The certificate format approved by the CA center must be consistent with the certificate format selected here.

Step 3. Click “Export”.

Step 4. Save the request file to the local path of the management host.

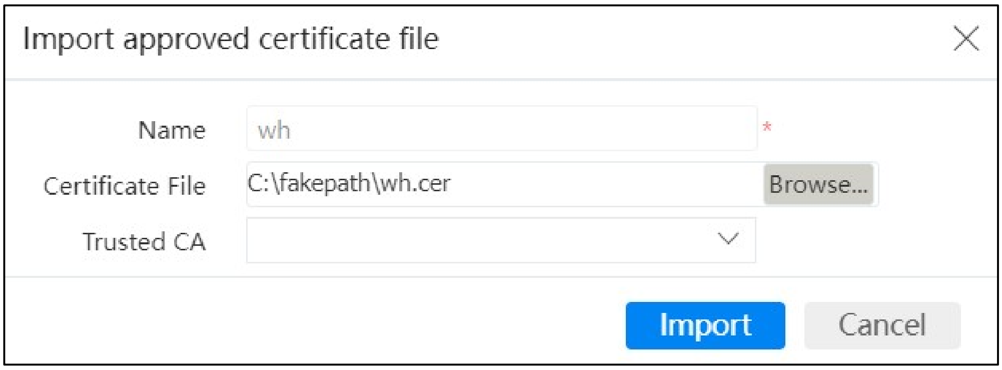
The request file format is req.

Import Approved Certificate Files

After the CA center issues the general certificate according to the request file, import the generated general certificate and trusted CA into the corresponding request file.

Step 1. Choose “System > Certificate Management > Request File”.

Step 2. Find the request file to import the approval certificate in the request file list, and click ⇲.



Import approved certificate file

Name: wh *

Certificate File: C:\fakepath\wh.cer

Trusted CA:

Step 3. Click “Browse” corresponding to "Certificate File ", find the certificate file saved locally, and add the path of the certificate file to the "Certificate File " text box.

Step 4. (Optional) Issue the CA certificate corresponding to the CA of the certificate file in the Trusted CA drop-down menu.

The corresponding CA will be displayed in the trusted CA drop-down menu only after the user has imported in the "Trusted CA" page.

Step 5. Click “Import”.

The certificate file can be imported correctly only if the format and content of the certificate file are correct. The imported certificate is displayed in the certificate list.

1.10.2 Trusted CA Certificate

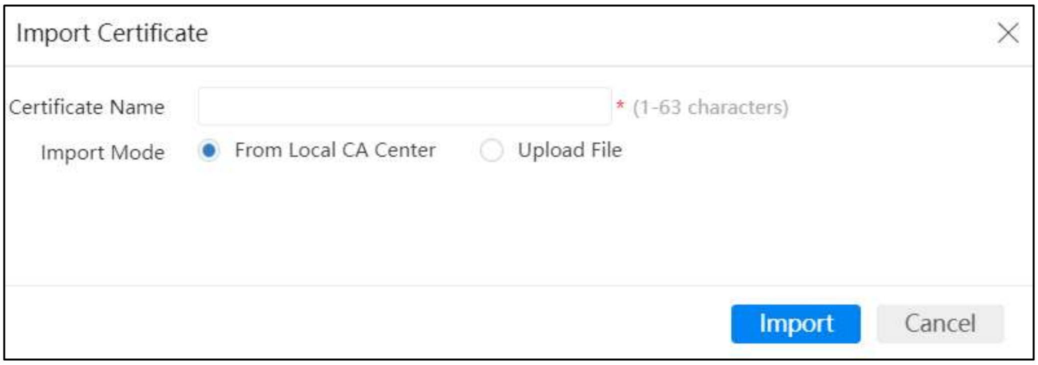
CA is a third-party organization responsible for managing and issuing certificates. Devices using certificates for communication must trust the CA, so that the certificates issued by the CA can be trusted.

Import Trusted CA

Step 1. Choose "System > Certificate Management > Trusted CA".

Step 2. Click “Import”.

Step 3. Fill in the certificate name and select the CA certificate import mode.



Import Certificate

Certificate Name * (1-63 characters)

Import Mode ● From Local CA Center ○ Upload File

Customize the name of the certificate and choose the import mode.

- If you select “From local CA center”, the CA center issued by the firewall will be directly used as the local CA center.
- If you select “Upload File”, select the trusted CA certificate and (optional) the superior CA certificate.

Step 4. Click “Import”.

The imported CA certificate is displayed in the list of trusted CA certificates. You can delete, view information, download and other operations on the imported certificate.

The information such as the certificate name, expiration time, upper-level CA, and reference times of each trusted CA can be queried in the trusted CA certificate list.

Authenticate Trusted CA

Confirm whether the certificate is valid by verifying whether the certificate is expired and whether it is in the CRL list.

Step 1. In the list of trusted CAs, find the trusted CA whose authentication mode needs to be configured.

Step 2. Click the ☑ (Edit) button under the corresponding action.

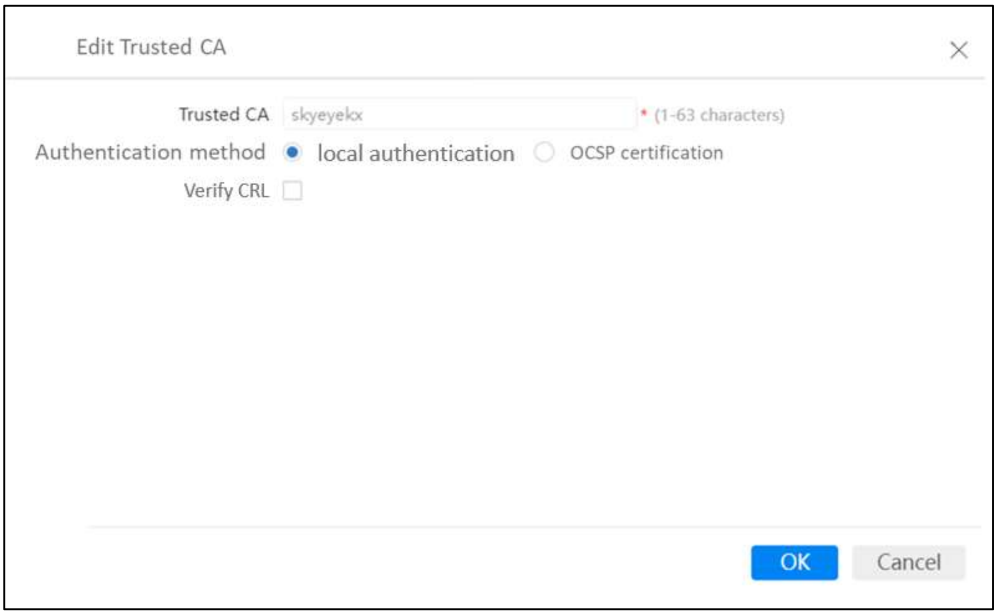
Step 3. Configure the authentication mode and whether the authentication certificate is valid.

The authentication mode supports local authentication and OCSP authentication.

Local authentication verifies the validity period of the certificate to confirm whether the certificate has expired.

When using OCSP authentication, enter the server URL, verification certificate, and timeout period.

The verification certificate needs to be imported into the certificate list before it can be selected from the drop-down menu.



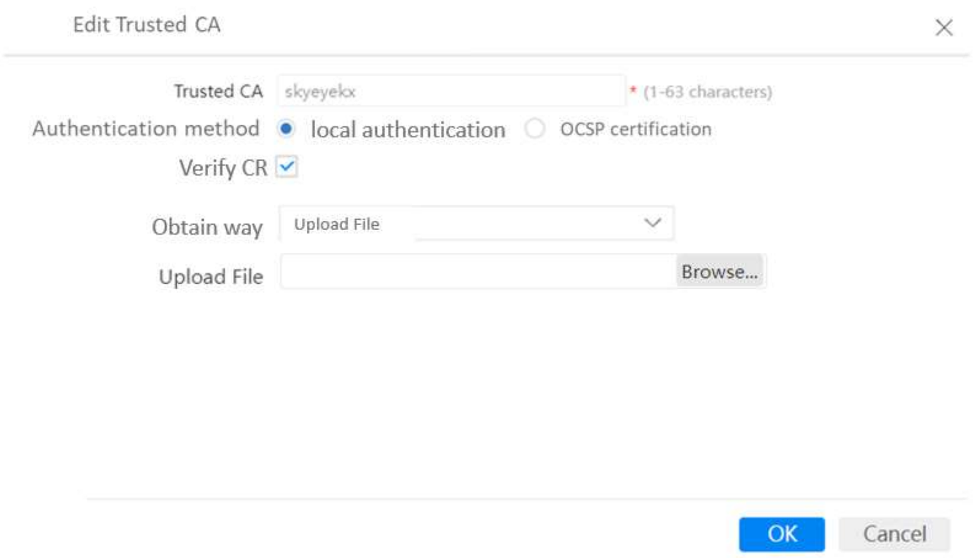
Edit Trusted CA

Trusted CA: skyeyekx * (1-63 characters)

Authentication method: ● local authentication ○ OCSP certification

Verify CRL □

Step 4. When selecting local authentication, support verifying CRL. Select “Verify CRL” to enable the CRL verification function.


Edit Trusted CA

Trusted CA: skyeyekx * (1-63 characters)

Authentication method: ● local authentication ○ OCSP certification

Verify CR ☑

Obtain way: Upload File

Upload File: Browse...

Obtaining CRL supports uploading files and HTTP(S), FTP, and LDAP online acquisition.

- To upload a file, you need to fill in the path of the exported CRL file in the "Upload File" text box. The corresponding file can be found by "Browse".
- For HTTP(S) online acquisition, the following parameters need to be set.

Parameter	Description
URI	Enter the URI that can get the CRL list, which needs to include the file and extension. Such as: http://10.1.2.1:80/root.crl.
Automatic update period	Enter the time interval for automatic updates. The default automatic update period is 24 hours.
Start time	Set the start time to start obtaining CRL files.

- FTP online acquisition, the following parameters need to be set.

Parameter	Description
URI	Enter the URI that can get the CRL list, which needs to include the file and extension. For example: ftp://10.1.2.1:80/root.crl.
Username	Enter the user name for logging in to ftp.
Password	Enter the password used by the user who logs in to ftp.
Automatic update period	Enter the time interval for automatic updates. The default automatic update period is 24 hours.
Start time	Set the start time to start obtaining CRL files.

- LDAP online acquisition, the following parameters need to be set.

Parameter	Description
Server address	Specify the IP v4 address of the LDAP server. Dotted decimal.
Server port	Specify the port of the LDAP server. The default is 389.
Login DN	Specify the directory tree of the authenticated user in the LDAP server.
Login password	Set the password for logging in to the LDAP server.
Base DN	Specify the topmost directory tree of LDAP.
Automatic update period	Enter the time interval for automatic updates. The default automatic update cycle is 24 hours.
Start time	Set the start time to start obtaining CRL files.

Step 5. After the configuration is complete, click “OK”.

1.10.3 Certificate List

In the certificate list, you can import, delete, and view certificate information, and you can view the number of times the certificate is referenced and the name of the referenced module. Support importing the general certificate file in commonly used formats, such as PEM, DER, P12. There are two import methods: local import and external import.

Import General Certificate

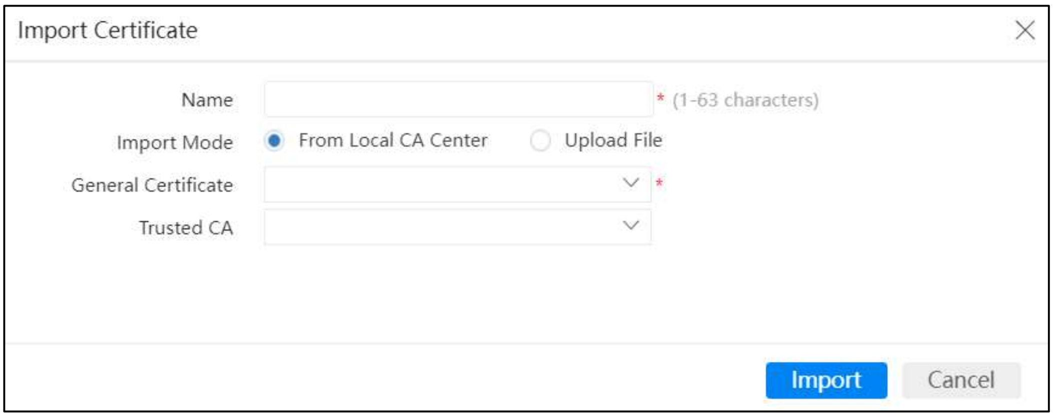
Step 1. Choose “System > Certificate Management > Certificate List”.

Step 2. Click “Import”.

Step 3. Set the parameters for importing the certificate.

Support two import modes:

- From local CA center: select general certificates and trusted CAs.
- Upload the certificate issued by the third-party CA center



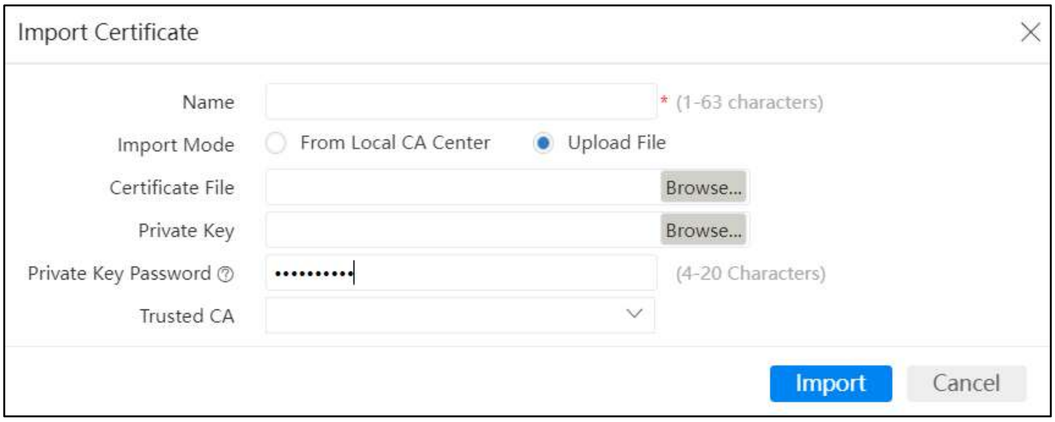
Import Certificate

Name * (1-63 characters)

Import Mode ● From Local CA Center ○ Upload File

General Certificate *

Trusted CA



Import Certificate

Name * (1-63 characters)

Import Mode ○ From Local CA Center ● Upload File

Certificate File

Private Key

Private Key Password •••••••••• (4-20 Characters)

Trusted CA

To upload a file, the user needs to specify the certificate file, private key file, private key password, and trusted CA.

Support importing the general certificate file in commonly used formats, such as PEM, DER, P12.

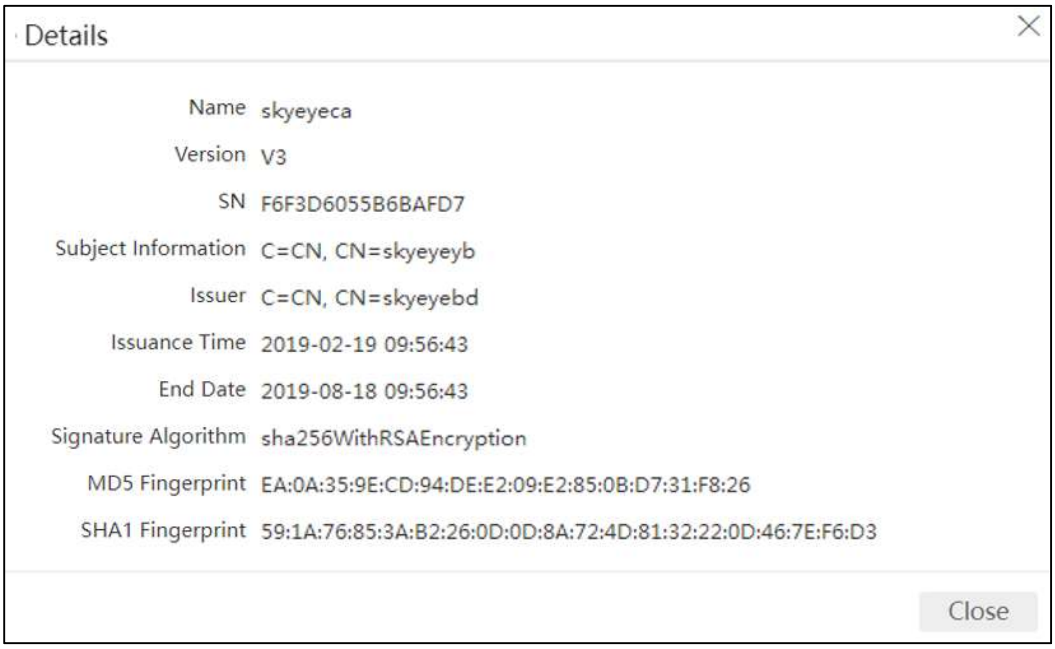
Step 4. Click “Import”.

The imported certificate is displayed in the certificate list. You can delete, view information, download and other operations on the imported certificate.

In the certificate list, you can view information such as the certificate name, expiration time, trusted CA, number of references, and type of each certificate.

View Certificate Details

In the certificate list, find the corresponding certificate and click the "View" button to view the details of the certificate.



Details

Name skyeyeca

Version V3

SN F6F3D6055B6BAFD7

Subject Information C=CN, CN=skyeyeyb

Issuer C=CN, CN=skyeyebd

Issuance Time 2019-02-19 09:56:43

End Date 2019-08-18 09:56:43

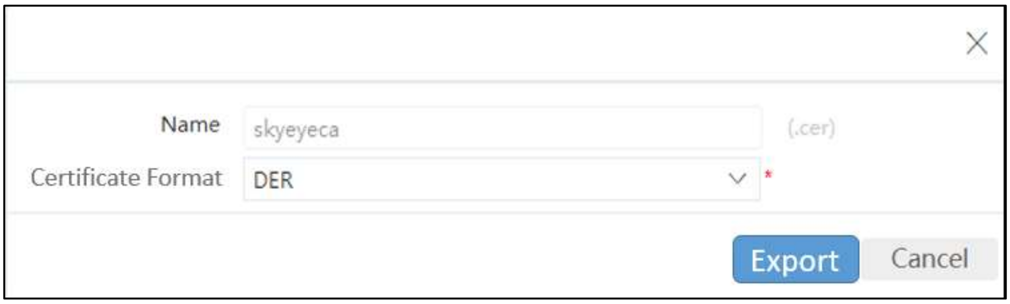
Signature Algorithm sha256WithRSAEncryption

MD5 Fingerprint EA:0A:35:9E:CD:94:DE:E2:09:E2:85:0B:D7:31:F8:26

SHA1 Fingerprint 59:1A:76:85:3A:B2:26:0D:0D:8A:72:4D:81:32:22:0D:46:7E:F6:D3

Export Certificate

In the certificate list, find the corresponding certificate, and click the "Export" button under Operation to export the certificate.



Name skyeyeca (.cer)

Certificate Format DER *

The certificate format supports DER or PEM. Click “Export”, set the save path in the pop -up dialog box, and click “Download” to save the certificate locally.

1.11 CA Center

The firewall supports acting as a CA center to generate digital certificates for this device and other terminal devices, and maintain certificate revocation lists (CRLs). The firewall not only supports generating a self-signed CA certificate as the root CA, but also supports importing a certificate issued by a third-party CA for the device as a lower-level CA center.

1.11.1 Create a Local CA

Overview

The local CA supports two creation methods:

- Generate self-Issued CA

At this time, a "self-issued certificate" is generated for the device. The self-issued certificate is also called the root certificate. It is a certificate issued by the device itself, that is, the issuer and the subject name in the certificate are the same.

- Import third-party CA

The device issues a certificate to itself through a third-party CA certificate. The issuer name in the certificate is the name of the CA server.

Only after a local CA is created can a local certificate be generated or a certificate generated through a request file approved.

Generate Self-Issued CA

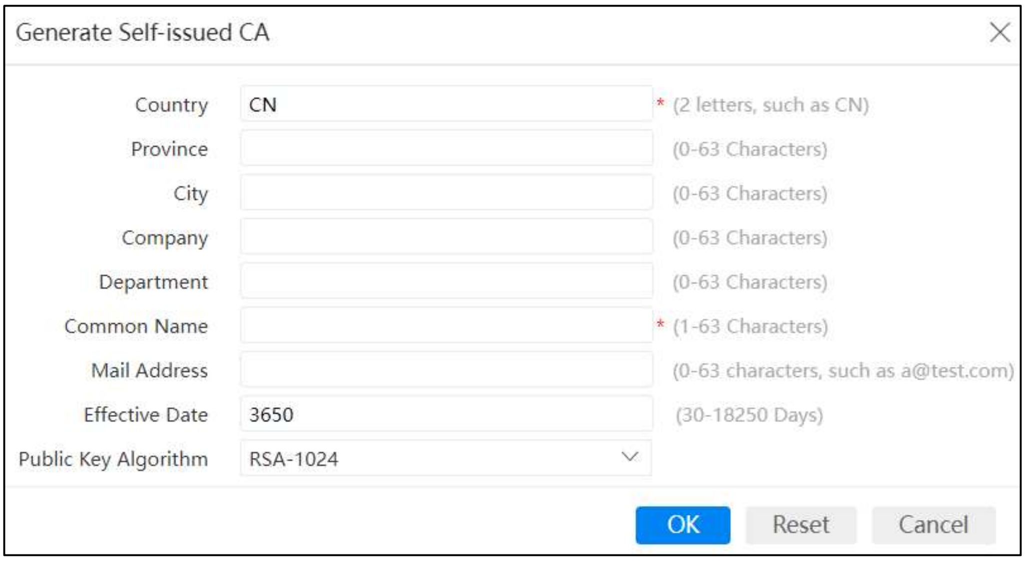
After the self-issued CA is generated, the local CA of the firewall serves as the root CA. Users should keep the private key of the certificate in a safe place, and do not disclose or lose it.

Step 1. Choose “System > CA Center > Local CA”.

Step 2. Click “Generate Self-Issued CA”.

Step 3. Configure CA parameters.

Country and common name are required. The common name is used to uniquely identify a CA. Please configure other options as required. Public key algorithms support RSA-1024 and RSA-2048. RSA2048 is more secure, please choose according to the security requirements.



Generate Self-issued CA

Country	CN	* (2 letters, such as CN)
Province		(0-63 Characters)
City		(0-63 Characters)
Company		(0-63 Characters)
Department		(0-63 Characters)
Common Name		* (1-63 Characters)
Mail Address		(0-63 characters, such as a@test.com)
Effective Date	3650	(30-18250 Days)
Public Key Algorithm	RSA-1024	

Step 4. After the configuration is complete, click “OK”.

Import Third-Party CA

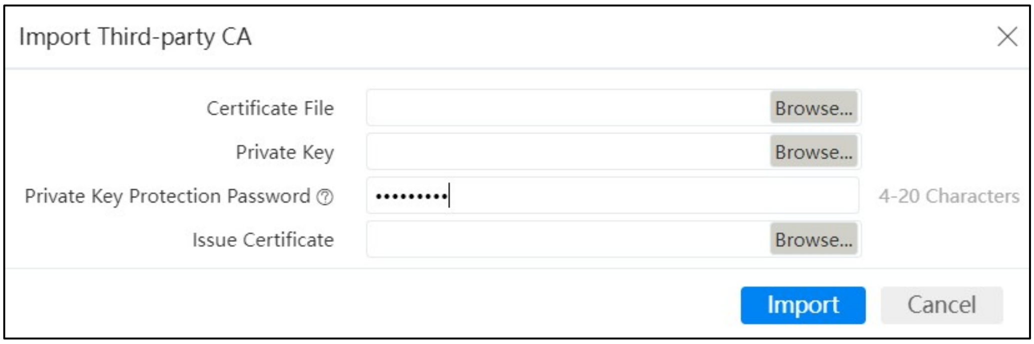
Import a third-party CA, and use the local CA on the firewall as the subordinate CA of the third-party CA. In this case, you need to export the certificate file and issuer certificate from the CA center of other devices.

Step 1. Choose “System > CA Center > Local CA”.

Step 2. Click “Import Third-Party CA”.

Step 3. Select the certificate file, private key file, and issuer certificate of the third-party CA, and set the private key protection password.

When the imported certificate file is a certificate with a private key file (the format is pkcs12, and the file suffix is pfx), the private key file does not need to be imported. However, you need to enter the private key protection password set when exporting the pkcs12 format certificate.



Import Third-party CA

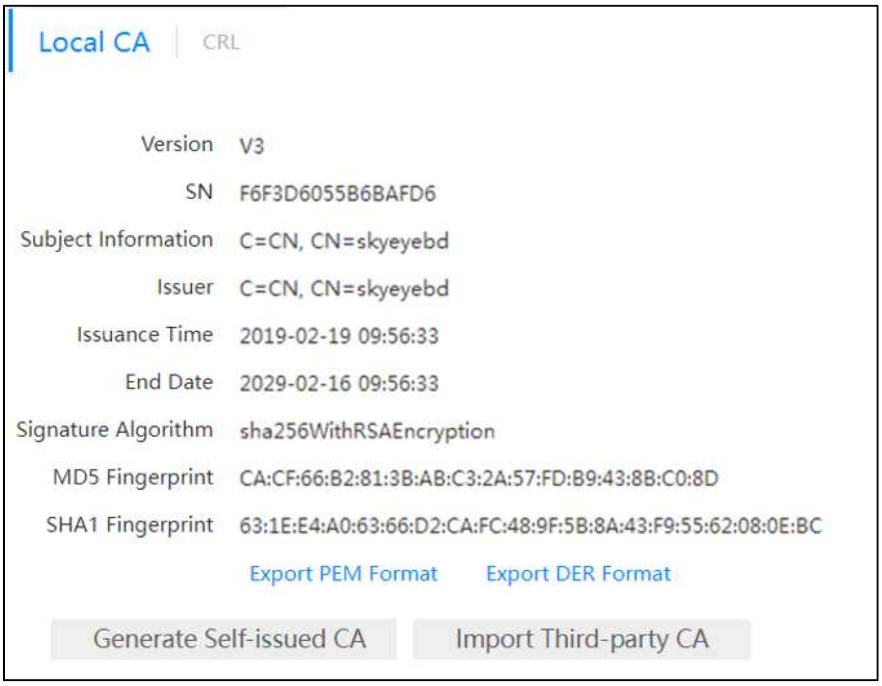
Certificate File	Browse...	
Private Key	Browse...	
Private Key Protection Password	•••••••••	4-20 Characters
Issue Certificate	Browse...	

Step 4. After the configuration is complete, click “Import”.

View Local CA

The displayed parameters of the local CA include version, serial number, certificate subject, issuer, issuance time, expiration time, feature algorithm, MD5 fingerprint value, and SHA1 fingerprint value.

the figure below is "sha256WithRSAEncryption", which means that sha256 authentication is adopted and RSA algorithm is used for encryption.



Version V3

SN F6F3D6055B6BAFD6

Subject Information C=CN, CN=skyeyebd

Issuer C=CN, CN=skyeyebd

Issuance Time 2019-02-19 09:56:33

End Date 2029-02-16 09:56:33

Signature Algorithm sha256WithRSAEncryption

MD5 Fingerprint CA:CF:66:B2:81:3B:AB:C3:2A:57:FD:B9:43:8B:C0:8D

SHA1 Fingerprint 63:1E:E4:A0:63:66:D2:CA:FC:48:9F:5B:8A:43:F9:55:62:08:0E:BC

Export CA Certificate

The firewall local CA can generate generic certificates for other devices. At this point, you need to export the general certificate and its own CA certificate. The CA certificate supports exporting the PEM and DER format certificates, and please select the export format according to your needs.

Step 1. Choose “System > CA Center > Local CA”.

Step 2. Click "Export PEM format " or "Export DER format".

Step 3. In the displayed dialog box, click “Download” to save the CA certificate locally.

1.11.2 General Certificate

A general certificate is a digital certificate generated after the CA center creates or approves a request file. It can be used to prove the identity of the certificate holder.

Generate General Certificate

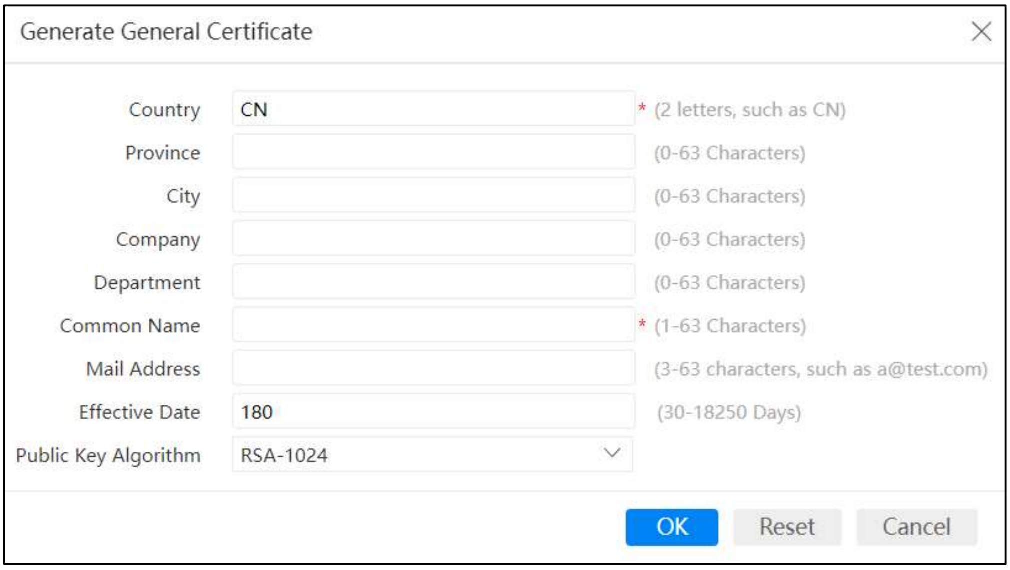
The general certificates generated locally are certificates issued by a local CA. The key length supports 1024 and 2048.

Step 1. Choose “System > CA Center > General Certificate”.

Step 2. Click “Generate Generic Certificate”.

Step 3. Configure parameters for general certificates.

The country and common name are required parameters, and other parameters can be optionally configured by users. The valid date defaults to 180 days, and the public key algorithm defaults to RSA-1024.



Generate General Certificate

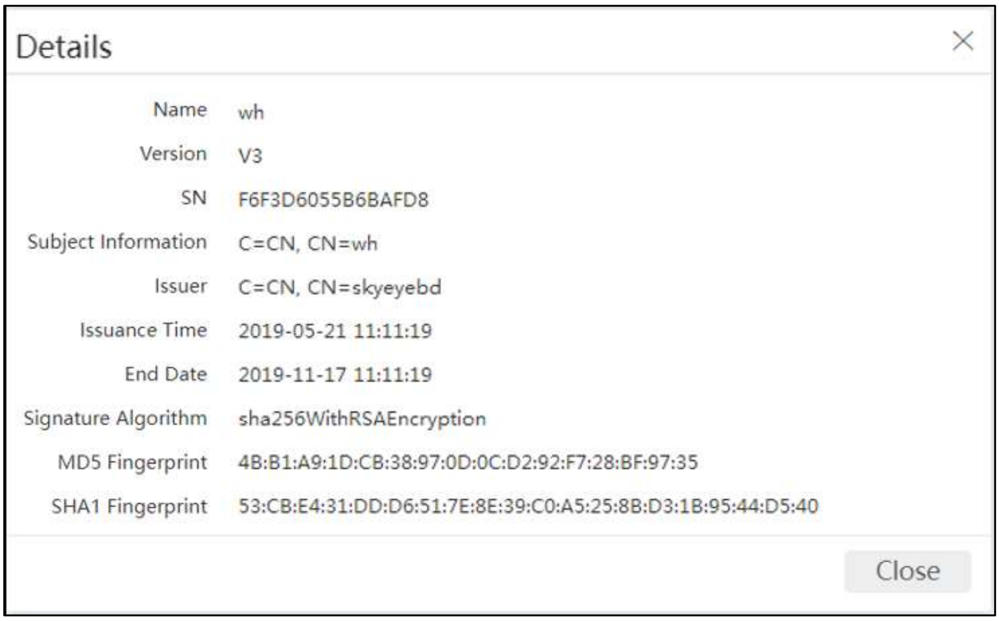
Country	CN	* (2 letters, such as CN)
Province		(0-63 Characters)
City		(0-63 Characters)
Company		(0-63 Characters)
Department		(0-63 Characters)
Common Name		* (1-63 Characters)
Mail Address		(3-63 characters, such as a@test.com)
Effective Date	180	(30-18250 Days)
Public Key Algorithm	RSA-1024	

Step 4. After the configuration is complete, click “OK”.

The configured certificate is displayed in the general certificate list, and the certificate format is 📄(locally generated certificate).

View Certificate Details

Find the desired certificate, click “View” under Operations, and view the details of the certificate.



Details

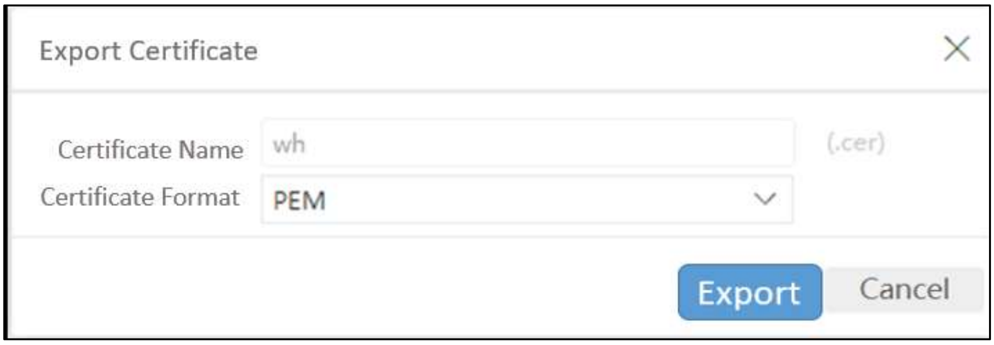
Name	wh
Version	V3
SN	F6F3D6055B6BAFD8
Subject Information	C=CN, CN=wh
Issuer	C=CN, CN=skyeyebd
Issuance Time	2019-05-21 11:11:19
End Date	2019-11-17 11:11:19
Signature Algorithm	sha256WithRSAEncryption
MD5 Fingerprint	4B:B1:A9:1D:CB:38:97:0D:0C:D2:92:F7:28:BF:97:35
SHA1 Fingerprint	53:CB:E4:31:DD:D6:51:7E:8E:39:C0:A5:25:8B:D3:1B:95:44:D5:40

Export General Certificate

Step 1. Find the desired certificate, click "Export" under Operation.

Step 2. In the “Export Certificate” dialog box, select a certificate format.

General certificates support two types: "Locally generated certificate " and "Approved certificate ". "Locally generated certificate" supports exporting to PEM, DER, and P KCS 12 formats, and "Approved certificate " supports exporting to PEM and DER formats.



Export Certificate

Certificate Name: wh (.cer)

Certificate Format: PEM

Step 3. Click “Export”.

Step 4. In the dialog box that pops up, set the save path and click “Download” to save the certificate locally.

Revoke Certificate

After the certificate is revoked, the corresponding certificate becomes invalid. Please confirm that you need to revoke the certificate before doing so.

Step 1. Find the desired certificate, click “Revoke” under Operation.

Step 2. In the displayed Confirm dialog box, click “OK”.

After the certificate is revoked, the corresponding certificate becomes invalid.

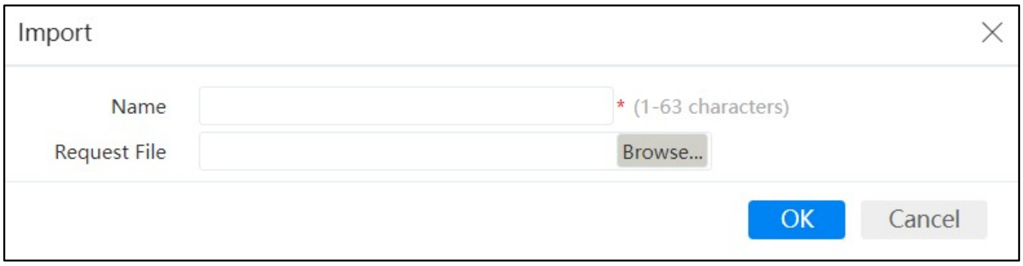
1.11.3 Certificate Approval

Import Certificate Request File

After the terminal device that needs to apply for a certificate generates the request file, save the request file to the management host. Apply for a certificate from the local CA center by importing the request file.

Step 1. Choose “System > CA Center > Certificate Approval”.

Step 2. Import the certificate request file.



Import

Name: * (1-63 characters)

Request File: Browse...

Customize a certificate name, click “Browse” in the “Request File” text box, and select the request file that has been saved locally on the management host.

Step 3. Click “OK”.

Automatically generate a certificate with the corresponding name in the certificate approval list. This certificate requires approval before it can take effect.

Certificate Approval

Step 1. Click ✎ (Approve) under a certificate action.

Step 2. Configure the validity date of the certificate in the "Certificate Request " dialog box.

The default certificate is valid for 180 days. The valid date ranges from 30 to 18250 days.

Step 3. Click “OK”.

The approved certificate is automatically added to the general certificate list of the CA center. The type is Approved Certificate (🗎).

1.11.4 CRLs

Certificates have a specified lifespan, but CAs can shorten this lifespan through a process called certificate revocation. The CA publishes a certificate revocation list, or CRL, listing the serial numbers of certificates that are considered no longer usable.

View CRLs

Step 1. Choose “System > CA Center > Local CA”.

Step 2. Click the CRL tab.

Step 3. View the CRL information.

Including the version, issuer, effective time, next update time, feature algorithm and the number of revoked certificates.

View Revoked Certificate Details

Click the "Revoked Certificate Details" link, and on the "Revoked Certificate Details " page that pops up, you can view the serial number and revocation time of the revoked certificate.

Export CRL

Click “PEM Format” or “Export DER Format” to export the CRL in the corresponding format.

1.12 Diagnostic Tools

1.12.1 Capture Tool

Add Capture Task

The packet capture tool is a useful tool for network troubleshooting. When the administrator suspects that there may be a certain reason for the failure, he can confirm it through packet capture; the administrator can also find the cause of the problem by analyzing the packet capture file. Add a packet capture task and specify the data flow to be captured. Support capturing packets of "TCP", "UDP", "IP", "ARP" and "ICMP" protocols.

Step 1. Choose “System > Diagnostic Tools > Packet Capture Tool”.

Step 2. Click “Add”.

Step 3. Set the capture parameters.

Parameter	Description
Name	Configure the name of the packet capture file.
Capture Count	Set the number of captured packets. After the number of captured packets is completed, the packet capture task ends.
Interface	Select the interface to capture packets. The packet capture interface only supports physical interfaces. Multiple interfaces can be selected.

Parameter	Description
Source address and source port	The device will capture the packets with the specified source IP and source port. Support input IPv4 or IPv6 address. The default source address and source port are any, that is, all packets with source IP and source port are captured.
Destination address and destination port	The device will capture the data packets with the specified destination IP and port number. Support input IPv4 or IPv6 address. The default destination address and destination port are any, that is, all packets with destination IP and destination port are captured.
Expression	The filter expression is used to set the conditions for capturing data packets (the filter expression uses the standard TCPDUMP format under linux). Currently supported protocols include tcp, udp, icmp, icmp 6, arp, ip, ip6, pppoed, pppoes. Parameter format, for example: host 1.1.1.1 and port 80 src host 1.1.1.1 and dst host 2.1.1.1 vlan 100, when configuring vlan, you need to specify the interface. tcp or udp

Step 4. After the configuration is complete, click “OK”.

After the setting is complete, the packet capture rules will be displayed in the list on this page. If multiple interfaces are configured to capture packets, the packet capture files of each interface will be output separately. You can check the capture file name, the number of captured packets (intercepted/target), interface, source address, source port, destination address, destination port and other parameters.

Edit Packet Capture Task

Click the name link of the packet capture file or the Edit button under Operation to edit the packet capture task. Except for the capture file name, the other parameters can be modified.

Start Packet Capture Task

Click ⏵ "Start Capture" under Operation to start capturing packets. By default, the packet capture task ends when the number of captured packets is reached. Users can also click "Stop Packet Capture" under Operation to end the packet capture task.

Only one packet capture task is in executing state in the packet capture task list.

Export Capture File

Click ⇲ "Export" under the operation to export the capture file to the local in the form of a compressed package. Users can analyze the packet through the decompressed packet capture file.

Delete Capture Task

For expired tasks, you can delete them through the "Delete" button.

Select the check box in front of the packet capture task and click “Delete”.

1.12.2 Detection Tool

Ping Detection

Ping detection is used to detect whether the IP address is reachable.

Step 1. Choose “System > Diagnostic Tools”.

Step 2. Click “Detect Tools”.

Step 3. Select Source Address or Source Interface.

Step 4. Enter the ping parameters.

Enter the destination IP or domain name. When selecting "Source Address", you can choose to input the source IP address; when selecting "Source Interface ", you must select an interface in the source interface drop-down menu.

Step 5. Click “Test”.

It prompts that the ping detection is being performed, please wait. After the detection is completed, the ping detection result is displayed. If detecting the interface succeeds, it means that the route is reachable, and the destination address or domain name can be accessed; if the detection fails, it means that the route is unreachable, and the destination address or domain name cannot be accessed.

Port Detection

Port detection is used to detect which TCP or UDP ports are opened on a certain IP or domain name in the network.

Step 1. Choose “System > Diagnostic Tools”.

Step 2. Click “Detect Tools”.

Step 3. Enter the destination IP or domain name for detection.

Both IPv4 and IPv6 are supported.

Step 4. Enter the destination port for detection.

The value range of the port is 1~65535.

Step 5. Choose a protocol. The protocol supports UDP and TCP.

Step 6. Click “Test”.

In the pop-up detection result prompt box, check whether the IP or domain name is reachable and whether the port is enabled.

2 Virtual System

The virtual system function can logically divide a firewall into multiple virtual firewalls. Each virtual system can be regarded as a completely independent firewall with independent system resources, administrators, policies, routes, Data centers, processing centers, analysis centers, etc.

The design of the virtual system is to solve the problem of providing isolated security protection functions for more business servers and business departments without adding additional firewalls. You don't need to make a lot of changes to your existing network environment. Through the virtual system function of the firewall, you can flexibly build a virtual environment to realize the security isolation and access control of various business servers and business departments.

2.1 Composition of Virtual System

2.1.1 Root Virtual System (root-vsys)

The root virtual system is the default virtual system of the system, which cannot be created or deleted, and has all the functions of a firewall. The root system administrator with corresponding permissions can create sub-virtual systems and virtual system administrator accounts, and the corresponding virtual system administrators and root system administrators with virtual system authorities can manage virtual systems.

Notes

The root system super administrator has read and write authority to manage accounts and virtual systems. The root system account administrator has the read and write authority of the management account, but does not have the read and write authority of the virtual system. The root system configuration administrator has the read and write authority of the virtual system, but does not have the read and write authority of the administrative account.

2.1.2 Sub Virtual System (vsys)

The virtual systems created by the root virtual system administrator are all sub-virtual systems. Logically, the sub-virtual system is an independent firewall, which can be independently managed and configured independently.

2.1.3 Virtual System Administrator

The administrator of the root virtual system can manage both the root virtual system and other child virtual systems.

The administrator of the sub-virtual system can only manage this virtual system.

- The root virtual system administrator creates sub-virtual system administrators and assigns them to a sub-virtual system.
- A sub-virtual system administrator can only manage one sub-virtual system to which it belongs.
- A child virtual system can have multiple child virtual system administrators.

For some global configurations (features that exist under the root virtual system but not under the child virtual system, such as high availability), only the root virtual system administrator can configure them. There may be more than one root virtual system administrator. This administrator can manage all virtual systems.

The sub-virtual system administrator can only manage the corresponding sub-virtual system, and has no configuration rights for some global functions (such as high availability).

2.2 Configure Virtual System

2.2.1 Create a Virtual System

Prerequisite

Log in to the firewall (root virtual system) using an administrator with account management and virtual system rights.

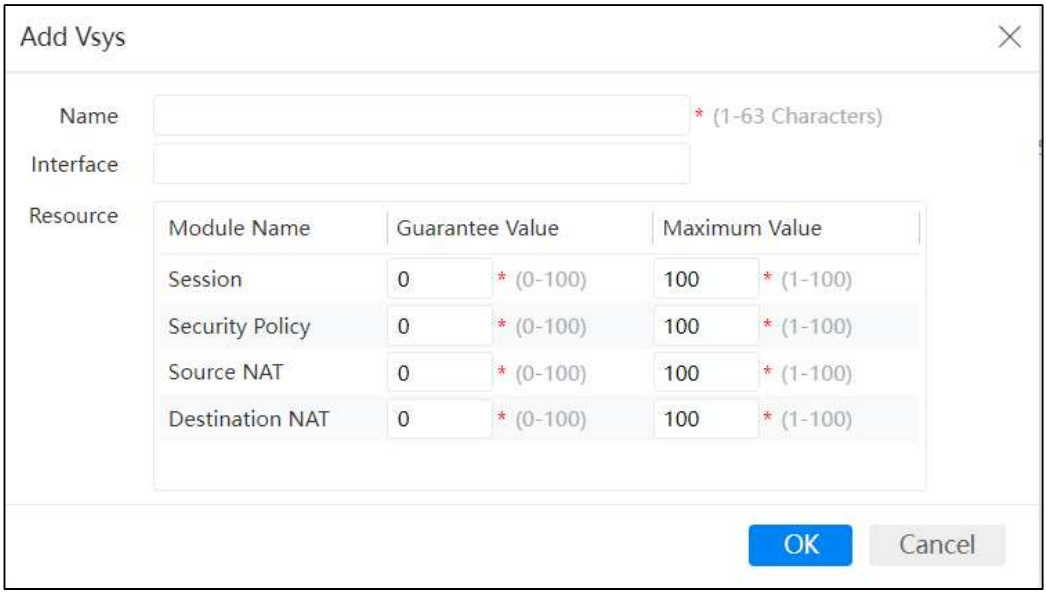
Configuration Steps

Step 1. Choose “System > Vsys”.

Step 2. Click “Add”.

Step 3. Configure virtual system parameters.

Configure the name of the virtual system, and assign interfaces and resources to the virtual system.



Add Vsys

Name: * (1-63 Characters)

Interface:

Resource:

Module Name	Guarantee Value		Maximum Value	
Session	0	* (0-100)	100	* (1-100)
Security Policy	0	* (0-100)	100	* (1-100)
Source NAT	0	* (0-100)	100	* (1-100)
Destination NAT	0	* (0-100)	100	* (1-100)

Parameter	**Description**
Name	Configure the name of the virtual system. The name is used to identify a virtual system, and the names of different virtual systems cannot be the same.
Interface	Assign interfaces to virtual systems. When allocating interfaces, you can only select L2 physical interfaces among idle interfaces (only access and trunk interfaces can be allocated) or L3 physical interfaces, physical subinterfaces, and aggregated subinterfaces without IP addresses.
Advanced Configuration-Resources	
Module name	Resources include sessions, security policies, source NAT, destination NAT, and logs. The log resource can be configured for the virtual system only when the firewall is configured with a hard disk. When allocating resources, you need to specify a guaranteed value and a maximum value, and the measurement method is a percentage. The sum of the minimum values for all virtual systems (including the root system) must not exceed 100%.
Guarantee value	The resources reserved for the virtual system, when the remaining system resources are not enough to allocate to the virtual system, creating the system fails. Resources are allocated by percentage, ranging from 0 to 100. When the assigned resource configuration guarantee value is filled with 0, it means that the minimum resource is not reserved for the virtual system.

Parameter	Description
Maximum value	When not occupied by other virtual systems or reserved by other virtual systems, the virtual system can occupy but will not exceed the maximum resource configuration. Resources are allocated by percentage, ranging from 1 to 100.

Step 4. After the configuration is complete, click “OK”.

2.2.2 Create a Virtual System Administrator

Super administrators, account administrators, or custom administrators with account management read and write rights can create corresponding administrators for virtual systems. After logging in to the administrator of the virtual system on the home page, directly enter the corresponding virtual system. The root system administrator can also manage the virtual system by selecting the corresponding virtual system in the top menu bar at the upper right corner of the Web page.

Step 1. Select "System > Device Management > Administrator User".

Step 2. Click “Add”.

Step 3. Configure virtual system administrator parameters.

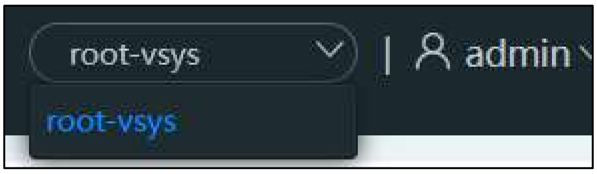
The system selects the virtual system to be managed, and selects the corresponding default role or custom role as required. It is recommended that roles be assigned with the minimum rights.

Step 4. Click “OK”.

2.3 Log in to Virtual System

2.3.1 Switch to Virtual System under Root System

Users use the root virtual system administrator to log in to manage the firewall, click the virtual system drop-down list in the top navigation bar, and select the corresponding virtual system to switch. After the switching is complete, the root system administrator can configure the virtual system.



2.3.2 Virtual System Administrator Logs in directly to Virtual System

After the root system administrator has created the sub-virtual system and the administrator of the sub-virtual system, log out of the firewall system and return to the login page. On the login page, enter the administrator account, password and verification code of the virtual system, and click "Login ".

The interface displayed at this time is the interface corresponding to the virtual system. The name of the corresponding virtual system is displayed in the top navigation bar.

The sub-virtual system administrator can log in through any physical interface (not the interface of the sub-virtual system to which it belongs), and manage the sub-virtual system to which it belongs. For example, there is a sub-virtual system administrator admin_vsys2 under the sub-virtual system vsys2, and physical interfaces ge2 and ge3 belong to the sub-virtual system vsys2. Users can log in to the administrator admin_vsys2 through any physical interface to manage vsys2.

2.4 Virtual System Traffic Forwarding

When no virtual system is configured on the firewall, all traffic is forwarded through the root virtual system. When a virtual system is configured on the firewall, traffic is forwarded according to the system to which the interface or VLAN belongs.

When creating a virtual system, resources need to be allocated for the virtual system. When an interface is assigned to a virtual system, the interface is bound to that virtual system and the interface is automatically removed from the list of root virtual system interfaces.

Configure the interface in the virtual system, specify the interface IP address or the vlan or bridge bound to the interface.

The packets received from interfaces or VLANs of sub-virtual systems enter the virtual system for processing.

2.5 Mutual Access of Virtual System

The firewall supports mutual access between virtual systems through virtual system interfaces, and also supports mutual access between virtual systems through physical connections.

- To achieve mutual access of the virtual systems through the virtual system interface, the user needs to manually create the virtual system, and specify the route to another destination address in the two virtual systems respectively, and specify the next hop of the route as the IP of the virtual system interface of the other virtual system address. Traffic that conforms to the corresponding security policy can be forwarded.

- Realize mutual access of virtual systems through physical connection. The virtual systems that need mutual access each have bound physical interfaces, and connect the two interfaces through physical lines. This scenario requires a physical interface. After specifying the route to the destination address, mutual access is realized. Traffic that conforms to the corresponding security policy can be forwarded.

2.5.1 (Optional) Add a Virtual System Interface

The root virtual system or each sub-virtual system supports one virtual system interface, and the name of the virtual interface is vge1. A virtual system interface is a virtual interface used for communication between various virtual systems. It simulates an internal virtual L3 switch, and the communication between virtual systems does not require an external physical interface connection, but only needs to configure the route to another system.

Virtual system interfaces are created by the respective virtual system administrator or the root virtual system administrator. Only one virtual system interface can be created for each virtual system, and the sub-virtual system administrator can only create virtual system interfaces belonging to its own virtual system.

Add the virtual system interface of the system under the corresponding virtual system.

Step 1. Choose “Network > Interface”.

Step 2. Click "Add" and select " Virtual System Interface" from the drop-down menu.

Step 3. Configure virtual interface parameters.

The name of the virtual system interface is fixed as vge1. For the description of the parameters, see the corresponding parameter descriptions under 4.1.3 Configure Interface.

Step 4. Click “OK”.

2.5.2 Configure Static Routing

For example, configure a route to the root virtual system on the child virtual system vsys1.

Step 1. Log in to the child virtual system vsys1 and select "Network > Routing > Static Route".

Step 2. Add a static route.

Step 3. Configure the route parameters.

Set the destination address/mask to the address and mask of the destination network segment or configure a default route. When accessing each other through the virtual system interface, the gateway address is specified as the IP address of the vge1 interface of the root virtual system. When accessing each other through physical interfaces, the gateway address is specified as the IP address of the interface physically connected to the interface under vsys1 of the root virtual system.

Step 4. After the configuration is complete, click “OK”.

2.5.3 Configure Policy

Traffic entering the sub-virtual system needs to be processed under the sub-virtual system. You need to configure corresponding security policies, NAT policies, and other policies under the sub-virtual system. Entering the root system needs to match the security policy and NAT policy of the root system again.

3 Network Configuration

3.1 Interface

3.1.1 Configure Interface

Select "Network > Interface" to edit the existing physical interface, MGT port or HA port.

Click "Add" to add physical sub-interfaces, aggregated interfaces, aggregated sub-interfaces, VLAN interfaces, bridge interfaces, loopback interfaces, tunnel interfaces, ADSL interfaces, 3G interfaces, 4G interfaces, virtual system interfaces, Overlay NVE interfaces, and Overlay routing interface.

3.1.2 Parameter Description of Interface Page List

Parameter	Description
Name	Display the name of the interface, and the type of the interface can be seen through the interface name. The existing interface names cannot be modified. • In the physical sub-interface or aggregated sub-interface name, the interface before "-" is the physical interface or aggregated interface bound to the sub-interface. The optional physical interface or aggregated interface must work in routing mode. The numbers after "-" represent VLAN IDs, ranging from 1 to 4094. • The name format of the physical interface is slot number + interface number. Among them, s*x* is the slot number, ge stands for Gigabit port, and xg stands for 10G port. The ports without slot numbers are onboard ports of the device. • The name format of the aggregated interface is "ch*x*". • The name of the VLAN interface is VLAN ID and the format is "vlan*x*". • The name of the bridge interface is Bridge ID and the format is "br*x*". • The name format of the tunnel interface is "tun*x* ", and the value range of "*x*" is 1~128. • The format of the loopback interface is "lo*x*", and the value range of "*x*" is 1~4. • The format of the ADSL interface is "adsl*x*". • The name of the 3G interface is 3 g1 and only one 3G interface is supported. • The name of the 4G interface is 4g1, and only one 4G interface is supported. • By default, only 4 virtual system interfaces are supported. You can expand the number of virtual system interfaces by purchasing a license. Each virtual system can only create one virtual system interface, and the virtual system administrator can only create virtual system interfaces belonging to the virtual system to which he belongs. • The name of OverNve interface is nve1, and only one Overlay interface is

Parameter	Description
	supported. • The name format of the overlay routing interface is "vn*x*", and the value range of "*x*" is 1~512.
Alias	The alias can facilitate the administrator to remember and identify the purpose of the interface.
Working Mode	Working modes include routing mode, switching mode and bypass mode.
Access information	The access information displays the IP address of the L3 interface or the vlan ID, bridge ID or aggregation interface bound to the L2 interface.
HA group	Displays the HA group to which the interface belongs. When HA is not enabled, the interface belongs to HA group 0.
Zone	Display the security zone to which the interface belongs.
Speed	Display the speed of the interface.
Status	The status includes the physical interface status, IPv4 status, and IPv6 status of the interface. • The physical interface is 🟩, it means that the physical connection of the interface is normal and the status is UP. • The physical interface is ▨, it indicates that the physical connection of the interface is faulty, and the status is Down. • The IPv4 or IPv6 status is 📄, it means that the interface is normally configured with an IPv4 or IPv6 address and can work normally. • The IPv4 or IPv6 status is 🗋, it means that the interface is not configured with an IPv4 or IPv6 address or the current network failure causes the IP to not work normally.
Quote	Display the number of times the interface is referenced. Click the corresponding number to view the function module and corresponding name of the referenced interface.
Enable	Check or uncheck the " Enable " check box to change the physical status of the interface. If the interface is normal, select the " Enable " check box, and the physical port status of the interface will become UP, and uncheck the "Enable" check box, and the physical port status of the interface will become Down.
Operation	Click Edit to edit interface parameters. ADSL interface supports manual connection operation. Dial-up connection can be made manually.

The following describes the parameters in the interface configuration.

3.1.3 Enable/Disable Interface

Select or uncheck the "Enable" checkbox in the interface list or interface editing page to enable or disable the interface.

You can restart an interface by shutting it down and then enabling it.

3.1.4 Configure Interface MAC and Virtual MAC

The MAC address and virtual MAC address of the interface do not need to be configured by the user. After the interface is added, the firewall automatically assigns the MAC address and virtual MAC address to the interface.

The virtual MAC address is used to be configured to the standby wall synchronously when HA is enabled, and the master wall and the standby wall use the same virtual MAC address for communication. When HA is not enabled, the virtual MAC address does not need to be used.

Users can modify the MAC address and virtual MAC address of an interface.

3.1.5 Configure Security Domain

Select the security zone to which the interface belongs according to the network planning.

3.1.6 Configure the Working Mode of the Interface

The interface supports working in routing mode, switching mode and bypass mode.

- The interface works in the routing mode, that is, the L3 working mode. An IP address must be configured for the interface. L3 interfaces can manage firewalls.
- The interface works in switching mode, that is, L2 working mode.

Notes

- The physical interface switching mode is divided into four modes: Access, Trunk, Bridge, and channel.
- The switching mode of aggregation interface and the switching mode of the virtual system interface are divided into three modes: Access, Trunk, and Bridge.

Parameter	Description
Mode	• An interface whose link type is Access can only belong to a

Parameter	Description
	certain VLAN, and can receive and send packets in this VLAN. Generally, it is used to connect terminal PC. • An interface whose link type is Trunk can receive and send packets of multiple VLANs. Generally, it is connected to the trunk interface of the switching device. • The interface whose link type is Bridge is a bridge interface, and the devices connected to the same bridge belong to a separate LAN. • The interfaces whose link type is Channel are member interfaces of aggregated interfaces.
VLAN in Access mode	In Access mode, you need to select the VLAN to which the interface belongs.
Allowed VLAN IDs in trunk mode	In trunk mode, the user needs to specify the VLAN IDs that the interface is allowed to pass through. **Notes** In Trunk mode, if the user wants Native VLAN to also pass through this interface, in VLAN ID configuration, the ID number of Native VLAN (whether it is the default 1 or a user-defined ID number) must be added to VLAN ID. Otherwise, Native VLAN will not be able to pass through the interface, resulting in network failure.
Native VLAN	The ID of the custom Native VLAN supported by the firewall. Users can change the Native VLAN ID according to actual needs. By default, the Native VLAN ID is 1.
Bridge	In Bridge mode, the user needs to specify the Id of the bridge to which the interface belongs.
Channel	In Channel mode, the user needs to specify the ID of the aggregated interface to which the interface belongs. Firewalls can improve link reliability through aggregated interfaces.

- The bypass mode is mainly used for bypass monitoring data in the user network.

Usually, the peer interface associated with the bypass mode interface is a mirror port, and the user imports the data that needs to be monitored in the network to the firewall interface working in bypass mode through the mirror port, and the firewall will perform a security check on the data. When the firewall detects a threat from an interface in bypass mode, it will send a reset operation to the abnormal session, but this operation requires that other physical interfaces on the firewall that are not working in bypass mode be reachable from the user's network.

3.1.7 Configure Aggregation Parameters of Aggregated Interface

Parameter	Description
Channel mode	Select Channel mode. Channel mode supports: • 802.3ad If the 802.3ad method is selected, the interface aggregation method follows the specified load algorithm. The 802.3ad method adopts the LACP protocol to realize link dynamic aggregation. • Polling mode If the polling mode is selected, the aggregation will be performed in polling mode among the bound interfaces, that is, the packets sent and received will be distributed in order among the available interfaces. • Hot standby mode If the hot standby mode is selected, the interfaces included in the aggregation interface are in a hot standby relationship, one is the master, and the rest are standby. Only one interface is responsible for sending and receiving data packets during normal operation, and switches to a normal interface among the alternative interfaces when a fault is detected. • Manual mode The manual mode is the static LACP mode, which is a link aggregation mode that uses the LACP protocol to negotiate aggregation parameters and determine active interfaces and inactive interfaces.
Load algorithm	Choose a load algorithm. It is set only when the channel mode is set to 802.3 ad and manual mode. Load algorithm support: • Balance based on IP address and TCP/UDP port combination Perform hash algorithm using IP address and TCP/UDP port. • Balance based on combination of source and destination MAC addresses Perform hash algorithm using source and destination MAC. • Balance based on MAC address and IP address combination Perform hash algorithm based on MAC address and IP address.
LACPDU packet transmission rate	Displayed only when Channel Mode is set to 802.3 ad. The 802.3ad method adopts the LACP protocol to realize link dynamic aggregation. You can specify the transmission rate of LACPDU packets. If you specify "slow" (30 seconds per packet), the fault will converge slowly and occupy less resources. Therefore, the effect at this time is high performance and low reliability; otherwise, if you specify "fast" (one packet per 1s), the fault converges quickly and consumes a lot of resources, and the effect is relatively high reliability and low performance.
Monitoring mode	The interface working mode is set to "routing mode " and the default channel is set to "hot standby mode", two monitoring modes of "Link" and "Arp " are supported. In the other cases, only "Link" mode is supported.

Parameter	Description
	• The Link mode is used to periodically detect the link connection status of the network port. The Link mode needs to configure the MII link period, which is the detection period of the network port connection status. • Select the ARP mode and send ARP requests to the destination IP regularly. If the response is received, the network status is normal. If the response packet is not received, the interface will be switched. The ARP mode needs to add the ARP destination IP, that is, the IP of the peer interface to be detected.
MII link period	When the monitoring mode is "Link", you need to configure the MII link period, that is, the detection period of the connection status of the network port. The optional range is 1-5, and the unit is second.
ARP period	When the monitoring mode is "ARP", you need to configure the period for sending ARP requests.
ARP destination IP	When the monitoring mode is "ARP", you need to add the ARP destination IP, that is, the IP of the peer interface to be detected.
Member interface	Select the member to join the aggregated interface from the optional interfaces. The optional interface list only includes physical interfaces in switched mode. Or when editing a physical interface, set the interface to work in switching mode, the submode is channel, and select the channel interface to be added.

3.1.8 Configure PPPoE (ADSL Interface) Related Parameters

Parameter	Description
Name	Required. Select a name for the ADSL interface.
Alias	Set the alias of the interface, which is convenient for the administrator to remember and identify the purpose of the interface.
Security domain	Select the security zone to which the ADSL interface belongs.
Binding interface	ADSL interfaces can be bound to Layer 3 physical interfaces and physical sub-interfaces. There is no need to configure an IP address on the interface. When the ADSL interface is in the connecting or already connected state, the bound interface cannot be modified.
Username	The user name required for ADSL interface dial-up. When the ADSL interface is connecting or already connected, the bound user name cannot be modified.
Password	The password corresponding to the user name when dialing through the ADSL interface. When the ADSL interface is connected, the binding password cannot be

Parameter	Description
	changed.
Auto connect	Select the "Enable" check box, and the dial-up will be performed automatically after the ADSL interface is disconnected.

3.1.9 Configure Interface IP Address

Interfaces support configuring IPv4 addresses and IPv6 addresses. The interface supports configuring IPv4 and IPv6 addresses at the same time. Up to 512 IPv4 addresses and 512 IPv6 addresses can be configured.

Both IPv4 addresses and IPv6 addresses support manual configuration and dynamic acquisition. The IPv4 address can be dynamically allocated through DHCP or obtained through ADSL dial-up. The IPv6 address can be dynamically allocated through DHCP, SLAAC (Stateless Address Autoconfiguration), or obtained through ADSL dial-up.

IP addresses are divided into float and static types. The float type is used by default. The static type needs to be configured only when the standby wall needs to be managed after HA is enabled, and the float type is recommended for other functions. When HA configuration synchronization is enabled, the float type IP will be synchronized to the peer device, but the static type IP will not be synchronized to the peer device.

- When manually configuring an IPv4 address, select “Static Address” and click “Add” to add an IPv4 address. In manual mode, multiple IP addresses can be specified for the interface.
- When manually configuring an IPv6 address, click “Add” to add an IPv6 address. In manual mode, multiple IPv6 addresses can be specified for an interface. You can also select whether to issue an RA. After selecting the “Publish RA” check box, the RA function is enabled. At this point, you can configure the effective life period, preferred life cycle, and whether to enable autonomous marking. Auto making is enabled by default.
- When getting v4 address or IPv6 address through DHCP, select the “DHCP” check box. At this time, the firewall acts as a DHCP client and sends a DHCP request. After receiving the request, the DHCP server assigns an IP address and subnet mask to the firewall interface. Once the IP address is no longer needed, click “Release”. Click “Reacquire” to obtain a new IP address. When the DHCP acquisition fails, the IP address and subnet mask are displayed as empty. When obtaining an IPv4 address through DHCP, it supports automatic configuration of a default route. By default, automatic configuration of the default route is enabled.

- To enable SLAAC to obtain IPv6 addresses, select the "SLAAC" check box. At this time, you can choose whether to enable the default route. The SLAAC method includes generating a unique local address representing the interface and obtaining IPv6 prefixes through RA (routing advertisement). RA adopts the default parameters by default, and the user can modify the parameters after selecting the "Router Advertisement" check box.
- To obtain an IPv4 or IPv6 address through PPPoE, you need to create an ADSL interface and bind it to a physical interface or subinterface in route mode. At this time, the firewall acts as a PPPoE client and sends a PPPoE request. After receiving the request, the PPPoE server assigns an IP address and subnet mask to the ADSL interface. You can check the assigned IPv4 or IPv6 address in the local address list. When PPPoE acquisition fails, the IP address and subnet mask are displayed as empty. Click "Manual Connection" to send PPPoE request immediately. The peer IPv4 address is the address of the PPPoE server.

3.1.10 Specify HA Group of the Interface

When HA is not enabled by default, it only needs to belong to HA group 0; when the HA function is enabled, the user needs to select the HA group according to the actual environment.

3.1.11 Configure Interface Management Mode

The interface supports HTTPS, SSH, Telnet, Ping, HTTP and SNMP management methods.

- HTTPS indicates that the interface is allowed to log in to the web management page through an HTTPS connection.
- SSH indicates that the interface is allowed to log in to the CLI interface through an SSH connection.
- Telnet indicates that it is allowed to log in to the CLI interface through a Telnet connection.
- Ping means that the interface will respond to ping requests.
- SNMP means that the management device is allowed to connect to the management firewall through this interface.

After selecting one or more methods, the user can open the interface IP address to manage the firewall through this method. For security reasons, HTTPS and SSH are recommended.

3.1.12 Configure Operation Mode of a Physical Interface

Parameter	Description
Operating mode	• auto Indicates that the interface is working in auto-negotiation mode. • manual Indicates that the interface works in non-auto-negotiation mode. If you need to configure the rate and duplex mode of the interface, you must first configure the interface to work in manual operation mode.
Rate	In manual operation mode, you need to select the working rate of the Ethernet interface. • Select "10Mb/s", which means that the working rate of the configuration interface is 10Mbit/s. • Selecting "100Mb/s" means that the working rate of the configuration interface is 100Mbit/s. • Selecting "1000Mb/s" means that the working rate of the configuration interface is 1000 Mbit /s. The speed of the Ethernet interface should be the same as that of the connected peer.
Duplex mode	• full duplex When you want the interface to receive packets while sending packets, you can set the interface to full-duplex mode. • half duplex When you want the interface to only send packets or receive packets at the same time, you can set the interface to half-duplex mode.

3.1.13 Configure Interface MTU

A proper MTU can improve the performance of the network. Theoretically, the MTU should be set to the smallest allowable MTU on the link to the destination network to avoid packet fragmentation. When the set MTU is too large and the network performance is degraded, you can try to reduce the size of the MTU several times to find the most suitable MTU size to optimize the network performance.

Different types of interfaces have different default MTU values and ranges. The web interface shall prevail. If there is no special requirement, the default value can be used.

When it is necessary to transmit the frames exceeding the size of 1518 through the firewall interface, jumbo frames need to be enabled. Jumbo frames are disabled by default, and you can execute **jumbo enable** in the configuration view to enable the jumbo frame function. After the jumbo frame function is enabled, the MTU larger than 1518 can be configured on the interface.

3.1.14 Configure Symmetric Routing

The symmetric routing is enabled by default.

The symmetric routing function can be implemented in a multi-exit environment, which interface the user accesses from, and from which interface the data is returned. For example: the user's internal network provides an http service to the outside, and the user has applied for two outlets of China Unicom ge1 and China Telecom ge2. When a Unicom user accesses the http service through the Unicom ge1 port, the symmetric routing function allows the response data returned by the server to the user to also go out through the Unicom ge1 port. When a Telecom user accesses the http service through the Telecom ge2 port, the symmetric routing function allows the response data returned by the server to the user to also go out through the Telecom ge2 port to ensure the consistency of the data return path.

It is recommended that users confirm whether to enable the symmetric routing function according to the actual requirements in a multi-exit environment.

3.1.15 Configure DNS Proxy Server

For traffic that does not match the DNS proxy policy, use the DNS proxy server on the outbound interface for DNS proxy.

Click the "DNS Proxy Server" drop-down box and select an appropriate DNS proxy server from the drop-down menu. If you need to add a new DNS proxy server, please select "Add DNS proxy server".

3.1.16 Configure Interface Mirroring

The interface mirroring function allows users to mirror the sending traffic or receiving traffic of this interface to other designated physical interfaces. The other physical ports designated for sending traffic and receiving traffic can be the same physical interface or different physical interfaces. Users need to configure according to the actual environment.

Interface mirroring configuration needs to specify the interface to send traffic and the interface to receive traffic.

3.1.17 Configure MPLS

By default, "MPLS" is not selected in the firewall. Even if various security protection functions such as security policies are enabled on the firewall, the firewall will still directly transparently transmit MPLS packets.

After selecting "MPLS", the interface receives the packet with MPLS label, and the label will be removed on the inbound interface. According to the configuration of the firewall, the packet will be processed accordingly, and the MPLS label will be re-made when the packet is sent out on the interface.

3.2 Security Domain

3.2.1 Overview

The security zone function of the firewall is to divide the interface into areas, and realize functions such as access control and application security based on the security zone.

The firewall contains five security zones by default:

- Three L3 domains (trust, untrust, dmz)
- Two L2 domains (l2trust, l2untrust)

The five security zone names provided by default are not allowed to be modified, but users can edit the interface members of the security zone.

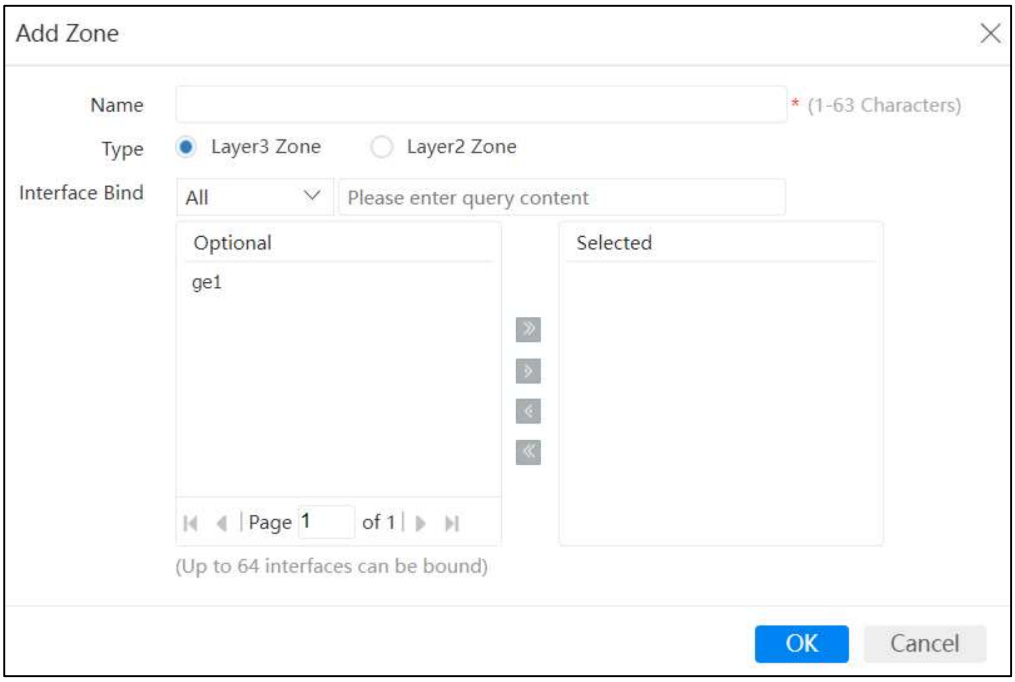
Users can also create new security zones. Different security zones are independent of each other. By directly configuring different security policies in the same security zone or in different security zones, different network access controls are implemented.

3.2.2 Create a Security Domain

Step 1. Choose “Network > Zone”.

Step 2. Click “Add”.

Step 3. Configure security zone parameters.



Add Zone

Name * (1-63 Characters)

Type ● Layer3 Zone ○ Layer2 Zone

Interface Bind All Please enter query content

(Up to 64 interfaces can be bound)

Parameter	Description
Name	Set the name of the security zone.
Type	Set the type of security zone. The type supports L3 and L2 security zones.
Interface bind	Select an interface type or query a specific interface directly, and the interface of the corresponding type will be displayed in the "Optional" area box. Add the interface to be added to the security zone into the "Selected" area box by using the “Add” button. • The interface bound to the L3 security zone must be a L3 interface. • The interface bound to the L2 security zone must be a L2 interface.

Step 4. After the configuration is complete, click “OK”.

The created security zone is displayed in the security zone list. The name, type, interface list, number of references, and operations of the security zone are displayed in the security zone list.

When the number of references is not 0, click the number of references to view all functional modules referenced by this security zone.

3.2.3 Edit Security Domain

Click the "Edit" icon in the operation column to edit and modify the security zone.

3.3 Configure VLANs

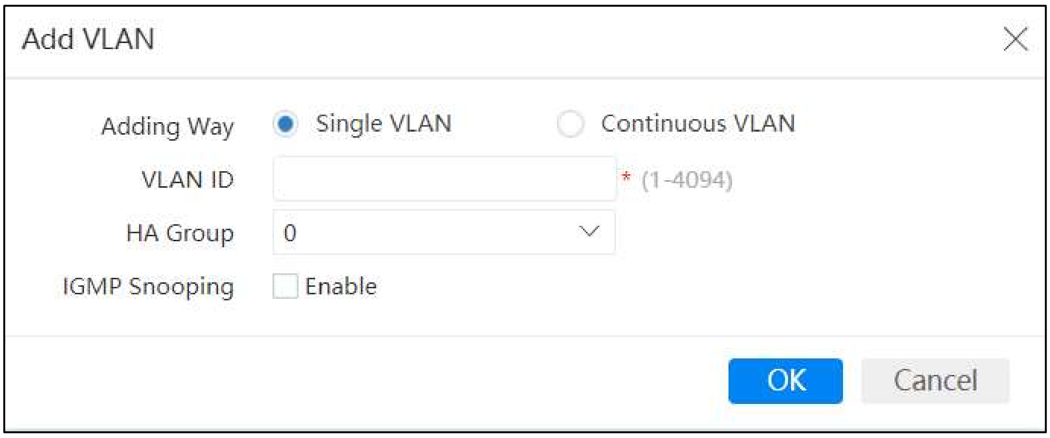
3.3.1 Create VLANs

The firewall supports creating a single VLAN and creating multiple consecutive VLANs in batches. Please select the creation mode according to actual needs.

Step 1. Choose “Network > VLAN”.

Step 2. Click “Add”.

Step 3. Configure VLAN parameters.



Add VLAN

Adding Way ● Single VLAN ○ Continuous VLAN

VLAN ID * (1-4094)

HA Group 0

IGMP Snooping □ Enable

Parameter	Description
Adding way	Adding modes include adding a single VLAN or multiple consecutive VLANs. A single VLAN is added by default. Multiple continuous VLANs can be created after selecting “Continuous VLANs” as the adding way. Support adding a single VLAN or adding multiple consecutive VLANs at a time.
VLAN ID	VLAN ID is used to uniquely identify a VLAN. The VLAN ID ranges from 1 to 4094. When the adding mode is "Single VLAN", specify the corresponding VLAN ID. When the adding method is "Continuous VLAN", specify the range of VLAN IDs, and add up to 64 continuous VLANs.
HA group	When HA is not enabled by default, it only needs to belong to HA group 0; when the HA function is enabled, the user needs to select the HA group according to the actual environment.

Parameter	Description
IGMP Snooping	After the IGMP Snooping function is enabled, the switch between the client and the multicast router will monitor the transmission of IGMP packets, modify the MAC address table to achieve correct and effective forwarding of multicast packets, instead of the default "flooding" processing.

Step 4. After the configuration is complete, click “OK”.

The created VLAN is displayed in the VLAN list. In the VLAN list, you can see the VLAN ID, VLAN name, bound interface, HA group, whether to enable IGMP Snooping, reference times and operations.

3.3.2 Add an Interface to a VLAN

Step 1. Choose “Network > Interface”.

Step 2. Find the L2 interface connected to the VLAN network. Click on the interface name or the “Edit” button.

Step 3. Configure the Access interface.

The working mode of the interface is set to "Switch mode ", and the mode is Access. If the VLAN has been created, select the VLAN connected to the interface in the VLAN drop-down box, if the corresponding VLAN has not been created, select "Add VLAN " in the VLAN drop-down box. After the VLAN is created, click “OK”.

Step 4. After the configuration is complete, click “OK”.

Step 5. Find the L2 interface connected to other switching devices. Click on the interface name or the “Edit” button.

Step 6. Configure the trunk interface.

The working mode of the interface is set to "Switch mode ", and the mode is trunk. Set Allow VLAN ID and Native ID.

Parameter	Description
Allow VLAN IDs	In trunk mode, the user needs to specify the VLAN IDs that the interface is allowed to pass through. Notes In Trunk mode, if the user wants Native VLAN to also pass through this interface, in VLAN ID configuration, the ID number of Native VLAN (whether it is the default 1 or a custom ID number) must be added to VLAN ID. Otherwise Native, VLAN will not be able to pass through the interface, resulting in network failure.

Native VLAN	The firewall supports custom Native VLAN ID. Users can change the Native VLAN ID according to actual needs. By default, the Native VLAN ID is 1.

Step 7. After the configuration is complete, click “OK”.

3.3.3 Configure Realizing Inter-VLAN Communication via VLAN Interfaces

If the hosts in different VLANs want to communicate, forward through a L3 device.

Step 1. Create VLANs.

Step 2. Configure the interface to join the VLAN.

Step 3. Add a VLAN interface and configure an IP address.

Choose “Network > Interface”, click “Add”, and select “VLAN Interface” from the drop-down menu. For detailed description of the parameters, see "4.1.3 Configure Interface".

Each VLAN can be configured with a VLAN interface. Different VLAN interfaces need to be configured as different network segments.

To implement communication between VLANs, the default gateway of hosts in a VLAN must be configured with the IP address of the corresponding VLAN interface.

3.3.4 Configure Realizing Inter-VLAN Communication via L3 Physical Sub-Interfaces

A sub-interface is a virtual sub-interface with a VLAN tag configured on the basis of a L3 physical interface. When users in different VLANs communicate, data forwarding between VLANs can be implemented through sub-interfaces.

Step 1. Create VLANs.

Step 2. Configure the interface to join the VLAN.

Step 3. Create a physical sub- interface corresponding to a VLAN, and configure an IP address.

Choose "Network > Interface", click "Add", and select "Physical Subinterface" from the drop-down menu. For detailed description of the parameters, see "4.1.3 Configure Interface".

A sub-interface is configured for each VLAN, and inter-VLAN communication is implemented through the intercommunication of physical sub-interfaces. Different physical sub-interfaces need to be configured as different network segments.

To implement communication between VLANs, the default gateway of hosts in the VLAN must be configured with the IP address of the corresponding physical sub-interface.

3.4 Configure Bridge

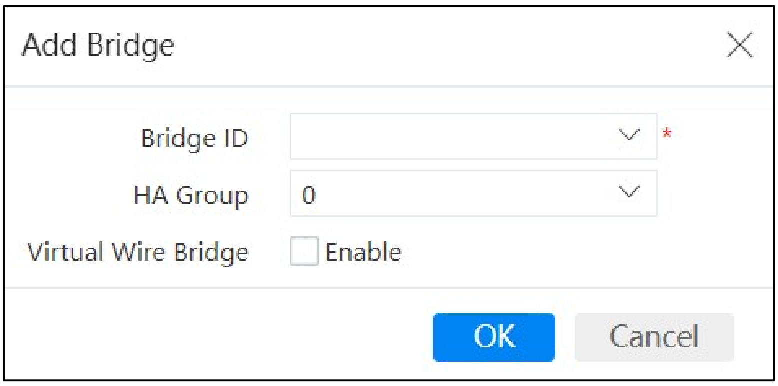
When the firewall acts as a bridge, it works at the data link layer. A bridge is similar to a vlan. The devices connected to the same bridge can only perform L2 forwarding within the bridge. A bridge without a virtual circuit bridge enabled can be bound to a bridge interface as a L3 interface to manage the firewall.

After the virtual wire bridge is enabled, a bridge can only be bound to two physical interfaces. A virtual wire bridge cannot be bound to a bridge interface. Traffic coming in from one physical interface bound to a virtual wire bridge can only be forwarded to the other interface of that virtual wire bridge pair. Other interface traffic cannot be forwarded into the virtual wire bridge.

Step 1. Choose “Network > Bridge”.

Step 2. Click “Add”.

Step 3. Configure bridge parameters.


Add Bridge

Bridge ID *

HA Group 0

Virtual Wire Bridge □ Enable

Parameter	Description
Bridge ID	Used to uniquely identify a bridge.
HA group	When HA is not enabled by default, it only needs to belong to HA group 0; when the HA function is enabled, the user needs to select the HA group according to the actual environment.
Virtual wire bridge	Select the "Enable" checkbox to enable the virtual wire bridge. A virtual wire bridge is an interface pair.

Step 4. After the configuration is complete, click “OK”.

The created bridges are displayed in the bridge list. In the bridge list, you can see the bridge ID, name, bound interface, HA group, whether to enable the virtual circuit bridge, reference times and operations.

Step 5. Bind the physical interface.

After adding the bridge, we need to bind the physical interface to the bridge.

Find the physical interface to be bound, click “Edit”, set the working mode to “Switch Mode”, set the mode to “Bridge”, and select the bridge interface to be bound. After the settings are complete, click “OK”.

3.5 DNS

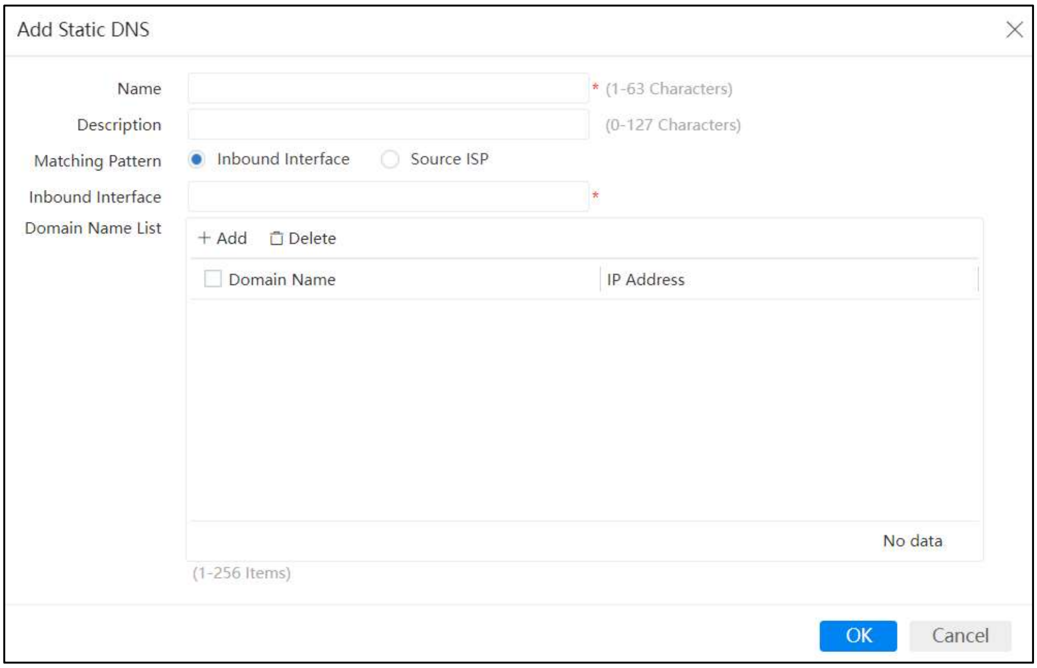
3.5.1 Static DNS

Static DNS is equivalent to a DNS cache list configured on the firewall. Static DNS supports two matching modes: inbound interface and source ISP, which are applied to two scenarios respectively. When the DNS request sent by the user reaches the firewall, it first checks the static DNS. If the incoming interface or the source ISP and the domain name match, the firewall sends the corresponding IP address to the user; if there is a mismatch between the incoming interface or the source ISP and the domain name, then The DNS request is forwarded to the DNS server, and the DNS server sends the IP address to the user after domain name resolution.

Step 1. Select “Network > DNS > Static DNS".

Step 2. Click “Add”.

Step 3. Configure static DNS.



Add Static DNS

Name * (1-63 Characters)

Description (0-127 Characters)

Matching Pattern ● Inbound Interface ○ Source ISP

Inbound Interface *

Domain Name List

□ Domain Name	IP Address

No data

(1-256 Items)

Parameter	Description
Name	Configure the name of the static DNS.
Description	Add the description for DNS rules.
Matching pattern	Select the matching mode according to the scene. The firewall supports two matching modes: • Ingress interface The DNS request received from the incoming interface will judge and reply to the IP address corresponding to the domain name in the static DNS according to the inbound interface. If the domain name is not in the static DNS, the DNS request is forwarded to the domain name server. • Source ISP The DNS request sent from the source ISP will judge and reply to the IP address corresponding to the domain name in the static DNS according to the source ISP. If the domain name is not in the static DNS, the DNS request is forwarded to the domain name server.
Inbound interface	When the configuration mode is inbound interface, specify the corresponding inbound interface. Multiple ingress interfaces can be selected. Only one source ISP can be selected.
Source ISP	When the matching mode is source ISP, select the corresponding source ISP.
Domain name list	Click “Add” to add a domain name and IP address mapping rule. Multiple corresponding rules can be added. The same IP address can be bound to multiple different domain names.

Step 4. After the configuration is complete, click “OK”.

3.5.2 DNS Proxy

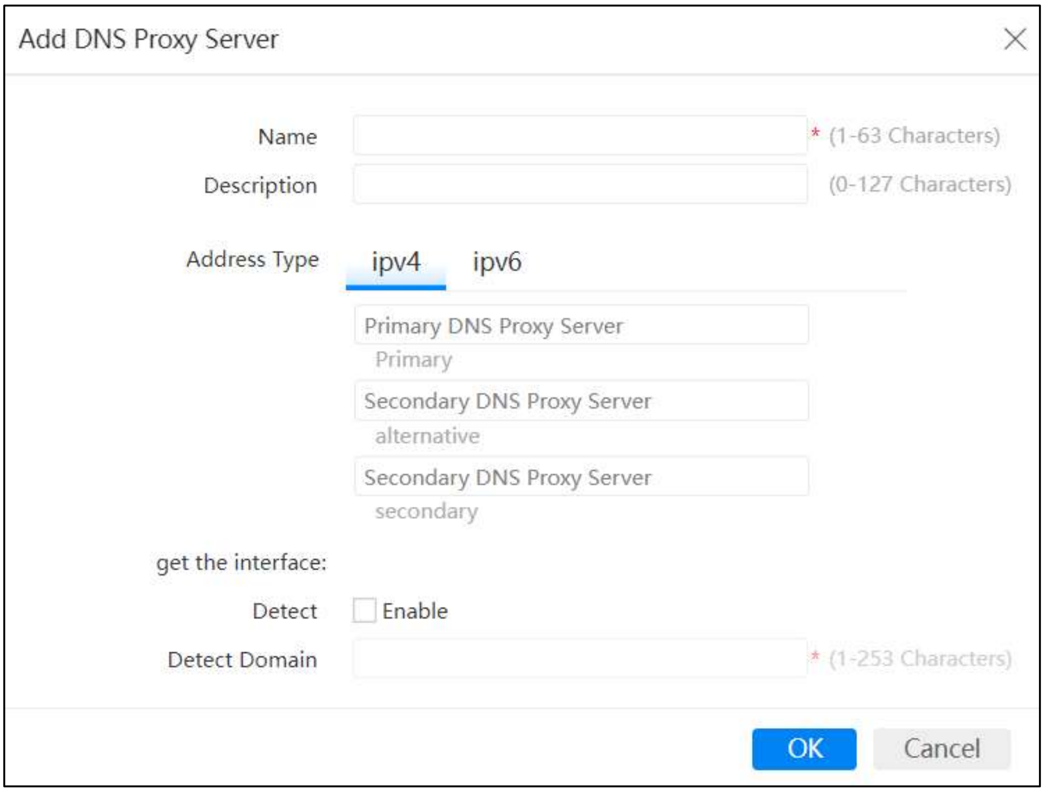
A DNS proxy is used to forward DNS requests and responses between DNS clients and DNS servers. The DNS client sends a DNS request packet to the DNS proxy, and the proxy forwards it to the DNS server, and forwards the response packet from the DNS server to the DNS client, thereby realizing domain name resolution. DNS proxy can conveniently implement local proxy and transparent proxy for clients.

3.5.3 Configure DNS Proxy Server

Step 1. Choose “Network > DNS > DNS Proxy Server”.

Step 2. Click “Add”.

Step 3. Configure DNS proxy server parameters.



Add DNS Proxy Server

Name * (1-63 Characters)

Description (0-127 Characters)

Address Type ipv4 ipv6

Primary DNS Proxy Server
Primary

Secondary DNS Proxy Server
alternative

Secondary DNS Proxy Server
secondary

get the interface:

Detect □ Enable

Detect Domain * (1-253 Characters)

Parameter	Description
Name	The name of the DNS proxy server.
Description	The description information of the DNS proxy server.
Address type	Select ip v4 or ipv6 address type. When the address type is ipv4, configure a DNS proxy server with an IPv4 address type; when the address type is ipv6, configure a DNS proxy server with an IPv6 address type.
Primary DNS proxy server	DNS proxy server preferred by the firewall. When the primary DNS server does not respond, the secondary DNS proxy server is used.
Secondary DNS proxy server	When the preferred DNS server does not respond, the firewall will choose to send a DNS request to the secondary DNS server, and the user can specify two secondary DNS servers.
Detect	Select the "Enable" checkbox to enable the detection function.
Detect domain	Specify the domain name corresponding to the DNS server to be detected.

Step 4. After the configuration is complete, click “OK”.

The configured DNS proxy server can be viewed in the DNS proxy server list.

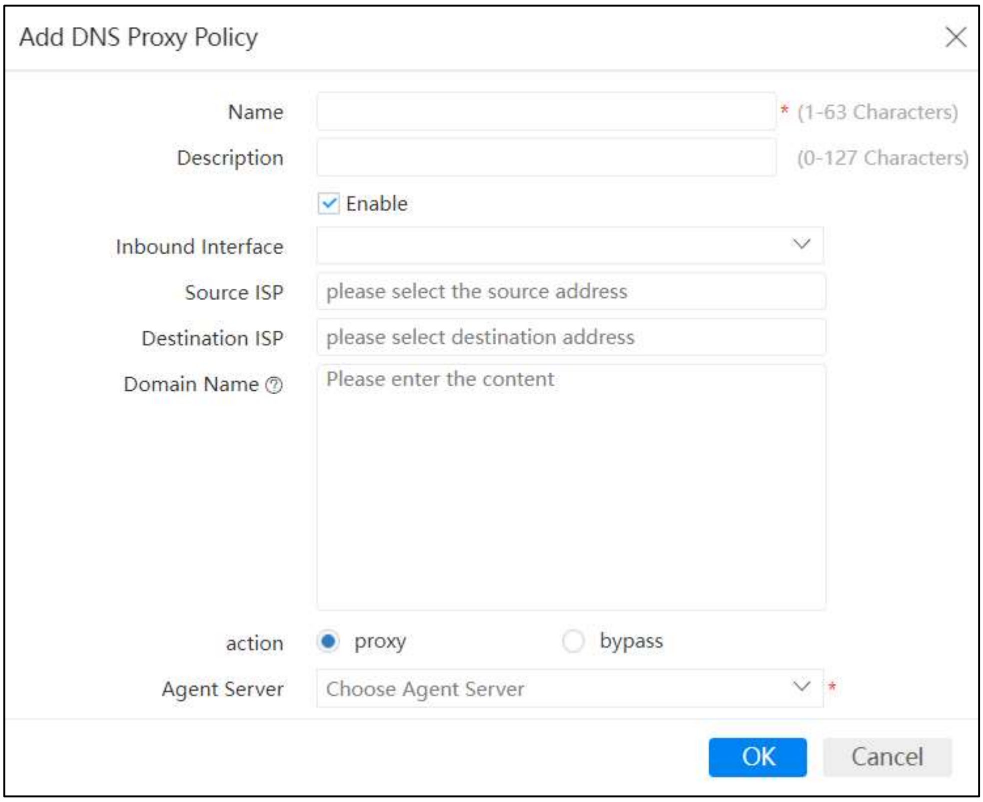
Configure DNS Proxy Policy

After configuring the DNS proxy policy, the DNS request will send the DNS request to the proxy server configured in the policy according to the matched policy. By configuring different proxy policies for different outbound interface traffic, DNS proxy load balancing can be implemented.

Step 1. Choose “Network > DNS > DNS Proxy Policy”.

Step 2. Click “Add”.

Step 3. Configure the parameters of the DNS proxy policy.



Add DNS Proxy Policy

Name * (1-63 Characters)

Description (0-127 Characters)

☑ Enable

Inbound Interface

Source ISP: please select the source address

Destination ISP: please select destination address

Domain Name: Please enter the content

action: ● proxy ○ bypass

Agent Server: Choose Agent Server *

Parameter	Description
Name	Configure the name of the DNS proxy policy.
Description	Configure the description information of the DNS proxy policy.
Enable	You must select the "Enable" check box to enable the DNS proxy policy, and the policy will take effect.
Inbound interface	Select the incoming interface corresponding to the traffic.

Parameter	Description
Source address	Select the source address of the traffic.
Destination address	Select the destination address for the traffic.
Agent server	Select the DNS proxy server to apply to traffic matching the DNS proxy policy.

Step 4. After the configuration is complete, click “OK”.

The configured DNS proxy policy is displayed in the DNS proxy policy list. The higher the position of the DNS proxy policy, the higher the priority.

Adjust the Order of DNS Proxy Policies

The order of DNS proxy policies in the list is related to priority. The higher the order, the higher the priority.

Select the DNS proxy policy to be adjusted in order, and you can put the DNS proxy policy at the top, move it to the end, or change the order.

3.5.4 Configure DDNS

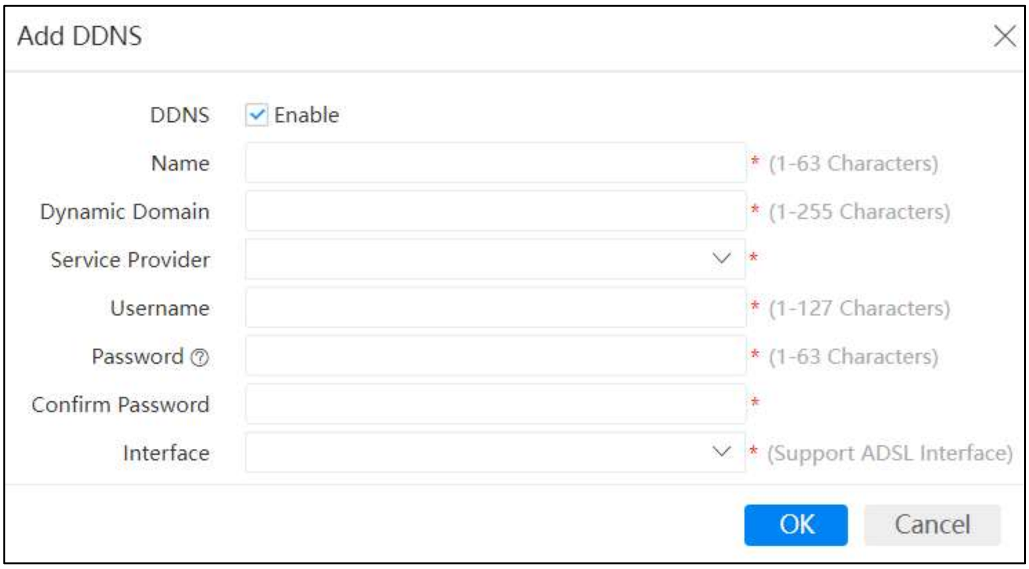
DDNS is the abbreviation of Dynamic Domain Name Service. DDNS is used when the interface IP is not fixed, allowing users to access the services provided by the interface through a fixed domain name. At this time, DDNS rules need to be bound to the interface, and the firewall, as a DDNS client, sends a domain name address change request to the host of the DDNS service provider, and the DDNS service provider notifies the DNS server to modify the corresponding relationship between the domain name and IP on the DNS, so as to achieve correct domain name resolution.

As a client of DDNS service, the firewall can update the IP address of the interface to the host of the service provider, and the service provider will update the corresponding relationship between the domain name and the IP address on the domain name server in real time.

Step 1. Select "Network > DNS > DDNS".

Step 2. Click “Add”.

Step 3. Configure DDNS rules.



Add DDNS

DDNS ☑ Enable

Name * (1-63 Characters)

Dynamic Domain * (1-255 Characters)

Service Provider *

Username * (1-127 Characters)

Password * (1-63 Characters)

Confirm Password *

Interface * (Support ADSL Interface)

Parameter	Description
DDNS	The DDNS function takes effect only after Enable is selected.
Name	Configure the name of the DDNS rule. The name is a unique identifier used to distinguish DDNS policies.
Dynamic domain name	Specify the domain name that the user needs to bind through the DDNS service. The domain name must be a domain name registered with the DDNS service provider.
Service provider	Specify the DDNS service provider. The firewall supports four service providers, namely: • oray • pubyun (3322) • changeip • noip
Username	The username used by the DDNS client (firewall) to access the DDNS service provider. This username needs to be registered with the service provider in advance.
Password, confirm password	Enter the password corresponding to the user name and confirm the password again.
Interface	Specify the interface bound to the DDNS policy, which is the interface where the dynamic IP address bound to the DDNS service. The interface must be an ADSL interface.

Step 4. After the configuration is complete, click “OK”.

3.6 DHCP

The firewall supports comprehensive DHCP functions, including DHCP server, DHCP relay, and DHCP client, and supports both DHCP and DHCPv6.

3.6.1 Configure DHCP Server

The DHCP server can dynamically assign IP addresses to DHCP clients connected to corresponding firewall interfaces, assign fixed IP addresses to DHCP clients with certain MAC addresses, assign domain names, mail servers, etc.

Restrictions and Precautions

- DHCP server is not supported in switch mode.
- It is not necessary to select an interface during DHCP server configuration, but the configured DHCP network address must be on the same network segment as the IP address of the interface. Then the DHCP server is automatically bound to the interface on the same network segment.
- When configuring the DHCP server, the interface must work in routing mode and configure a static IP. L3 physical interfaces, physical sub-interfaces, VLAN interfaces, bridge interfaces, L3 aggregation interfaces, aggregation sub-interfaces, and tunnel interfaces all support the DHCP server.
- DHCP service is disabled by default. The DHCP server will take effect only after the DHCP service is enabled.
- DHCP server, DHCP client, or DHCP relay cannot be configured on an interface at the same time.
- When the firewall acts as a DHCP server and there is a DHCP relay device in the middle, the DHCP request detection cannot be enabled on the firewall at the same time. Otherwise, the client cannot obtain an address.

Configure DHCP server

Step 1. Select “Network > DHCP > DHCP server".

Step 2. Click “Add”.

Step 3. Configure the DHCP network address and network mask.

Parameter	Description
Network address	Specify the network address to which the IP that the DHCP server can assign to the DHCP client belongs. The network address must be in the same network segment as the interface connected to the DHCP client, and the addresses in the DHCP address pool must be addresses or address segments within the network address range.
Network mask	Specify the network mask of the network address.

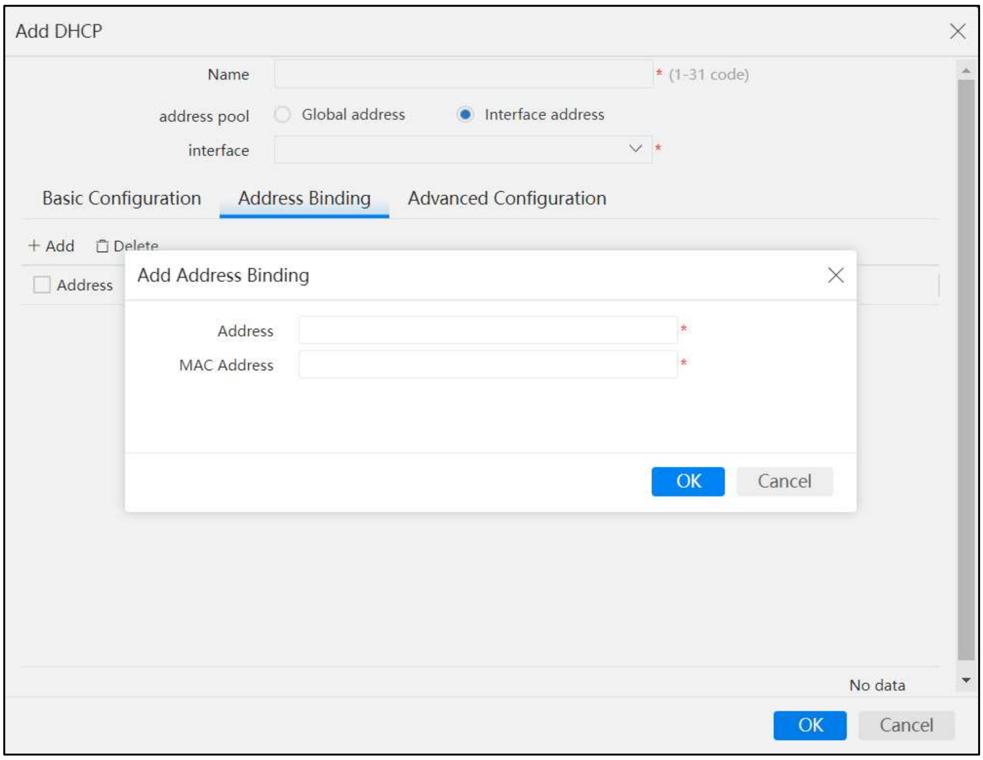
Step 4. Configure basic DHCP configurations.

Parameter	Description
Gateway address	The default gateway assigned by the DHCP server to DHCP clients. That is, the IP address of the interface on which the DHCP service is enabled.
DNS1~3	Domain name server assigned by the DHCP server to DHCP clients. It must be configured when the DHCP client accesses the Internet through the domain name. And it is required that the route between the assigned DNS server and the DHCP server should be reachable. DNS1 is the preferred DNS server, and DNS2 and DNS3 are alternative DNS servers. When the DHCP client fails to resolve the domain name through the preferred DNS server, it requests the secondary DNS server for domain name resolution.
Lease duration	The address assigned by the DHCP server to the DHCP client has a valid time, and the lease needs to be renewed after the expiration. The default renewal time is 43200 seconds (12hours).
Description	The description about the DHCP service is used to distinguish it from other DHCP services.
Address pool list	The IP address range allocated by the DHCP server to DHCP clients. The addresses in the address pool must be IP addresses within the specified network address range. You can add multiple items, but pay attention to exclude the gateway address.

Step 5. (Optional) Configure address binding.

The DHCP address binding function allows the DHCP service to assign a fixed IP address to some fixed MAC addresses when receiving a DHCP request. The address bound to the configured DHCP address is not limited by the lease time.

Click the “Address Binding” tab, click “Add”, and set the local address and MAC address binding. There can be up to 1600 items.



Step 6. Advanced configuration.

Parameter	Description
Domain name	The suffix of the domain name assigned by the DHCP server to DHCP clients. After the DHCP client obtains the domain name suffix assigned by the server, when the DHCP client accesses network resources through the host name, the client system will automatically add the domain name suffix to the incomplete host name to form a complete domain name.
WINS1~2	The WINS server assigned by the DHCP server to the DHCP client. The WINS server user resolves hostnames to IP addresses for hosts communicating through the NetBIOS protocol. WINS1 is the active WINS server, and WINS2 is the standby WINS server. There should be a reachable route between the WINS server and the DHCP server.
SMTP server	The SMTP server assigned by the DHCP server to the DHCP client.
POP3 server	The POP3 server assigned by the DHCP server to the DHCP client.

Step 7. After the configuration is complete, it will be displayed in the DHCP list.

Click the "Edit" button corresponding to the DHCP server to modify the basic configuration, address binding and advanced configuration of DHCP.

Enable DHCP

Select the "Enable" check box, and click "OK" in the displayed prompt box to enable the DHCP service. The DHCP server takes effect only after the DHCP service is enabled.

View DHCP lease information

The lease information is the storage time of the IP address obtained by the DHCP client. After the lease ends, the DHCP client needs to obtain the IP address again.

Step 1. Click the "Edit" button corresponding to the DHCP server.

Step 2. Click the "Lease Information" tab.

Step 3. View the lease information.

The lease information shows the local address, MAC address, DHCP lease start time and end time of the DHCP client. After the lease ends, the IP address is released and can be reassigned to DHCP clients.

3.6.2 Configure DHCP v6 server

DHCPv6 server is used to assign IPv6 addresses to DHCPv6 clients.

Restrictions and Precautions

- In the switch mode, do not support the DHCPv6 server.
- When configuring the DHCPv6 server, the interface must work in routing mode and configure a static IP. L3 physical interfaces, physical subinterfaces, VLAN interfaces, bridge interfaces, L3 aggregation interfaces, aggregation subinterfaces, and tunnel interfaces all support the DHCPv6 server.
- The DHCPv6 service is disabled by default. The DHCPv6 server will take effect only after the DHCPv6 service is enabled.
- DHCPv6 server, DHCPv6 client, or DHCPv6 relay cannot be configured on an interface at the same time.
- When the firewall functions as a DHCP v6 server and there is a DHCP v6 relay device, DHCP v6 request detection cannot be enabled on the firewall at the same time. Otherwise, the client cannot obtain an address.

Configure DHCPv6 Server

Step 1. Select Network > DHCP > DHCP server".

Step 2. Click the “DHCPv6 Server” tab.

Step 3. Click “Add”.

Step 4. Select the interface to enable the DHCPv6 server function.

The interface must be configured with a static IP address.

Step 5. Configure the basic configuration of the DHCPv6 server.

Parameter	Description
DNS1~2	The domain name server assigned by the DHCP v6 server to DHCP v6 clients. It must be configured when the DHCPv6 client accesses the Internet through the domain name. And it is required that the route between the assigned DNS server and the DHCP v6 server should be reachable. DNS 1 is the preferred DNS server, and DNS2 is the alternative DNS server. When the DHCPv6 client fails to resolve the domain name through the preferred DNS server, it requests the secondary DNS server for domain name resolution.
Renewal time	The address assigned by the DHCPv6 server to the DHCPv6 client has a valid period, and the lease needs to be renewed after the expiration. The default lease renewal time ranges from 300 to 4294967295 seconds (representing the permanent lease period). The default is 172800 (two days).
Description	The description about this DHCP v6 service is used to distinguish it from other DHCP v6 services.
Address pool	The IP address range allocated by the DHCPv6 server to DHCPv6 clients. The addresses in the address pool must be IP addresses within the specified network address range.

Step 6. (Optional) Configure reserved addresses.

Click “Add” to configure the start IP and end IP of the reserved address segment. Multiple reserved address segments can be added. Addresses in the reserved address segment will not be assigned to DHCP v6 clients.

Step 7. (Optional) Configure address binding.

The DHCP v6 address binding function allows the DHCP v6 server to assign a fixed IP v6 address to some fixed MAC addresses when receiving a DHCP request.

Click the “Address Binding” tab, click “Add”, and set the local address and DUID (DHCP Unique Identifier) binding. DUID is used to uniquely identify a DHCPv6 client, and the actual length depends on its type. Send the address, lease period, etc. to the client according to the DUID type.

Step 8. Advanced configuration.

Parameter	Description
Domain name	The suffix of the domain name assigned by the DHCPv6 server to DHCPv6 clients. After the DHCP v6 client obtains the domain name suffix assigned by the server, when the DHCP v6 client accesses network resources through the host name, the client system will automatically add the domain name suffix to the incomplete host name to form a complete domain name.
SIP server	The SIP server address assigned by the DHCP v6 server to the DHCP v6 client.
SNTP server	The SNTP server address assigned by the DHCP v6 server to the DHCP v6 client.

Step 9. After the configuration is complete, it will be displayed in the DHCPv6 server list.

Click the "Edit" button corresponding to the DHCPv6 server to modify the DHCPv6 server parameters.

Enable DHCPv6

Select the "Enable" check box, and click "OK" in the displayed prompt box to enable the DHCPv6 service. The DHCPv6 server takes effect only after the DHCPv6 service is enabled.

View DHCPv6 Lease Information

The lease information is the storage time of the IP address obtained by the DHCP client. After the lease ends, the DHCPv6 client needs to obtain the IP address again.

Step 1. Click the "Edit" button corresponding to the DHCPv6 server.

Step 2. Click the "Lease Information" tab.

Step 3. View the lease information.

The lease information shows the DHCP v6 client's local address, client identification (DUID), DHCP lease start time and end time. After the lease ends, the IP address is released and can be reassigned to DHCP v6 clients.

3.6.3 Configure DHCP Relay

When the DHCP server is not on the same network segment as the host, we need a DHCP relay device to send a DHCP request to the DHCP server so that the host can obtain an IP address.

Restrictions and Precautions

- DHCP relay is not supported in switch mode.
- When configuring DHCP relay, the interface must work in routing mode and configure static

IP. L3 physical interfaces, physical sub-interfaces, VLAN interfaces, bridge interfaces, L3 aggregation interfaces, aggregation sub-interfaces, and tunnel interfaces all support DHCP relay.

- DHCP relay is disabled by default. After the DHCP relay is enabled, the DHCP relay will take effect.
- DHCP server and DHCP relay cannot be configured on an interface at the same time.

Configure DHCP Relay

Step 1. Select “Network > DHCP > DHCP Relay".

Step 2. Configure DHCP relay parameters.

Parameter	Description
DHCP relay	Select the "Enable" checkbox to enable the DHCP relay function. This function will take effect only after DHCP relay is enabled.
DHCP server address list	The v4 address of the DHCP server. Up to 32 DHCP server addresses can be filled in. The DHCP relay needs to maintain connectivity with these DHCP servers.
DHCP relay interface	Select the interface connecting the DHCP relay (firewall) to the DHCP server and the interface connecting the DHCP relay to the DHCP client. A maximum of 32 trunk interfaces can be added. The DHCP relay interface connected to the client will monitor the DHCP request packet in the network segment, and after the DHCP relay interface receives the request packet, it will forward it to the DHCP server.

Step 3. After the configuration is complete, click “Apply”.

3.6.4 Configure DHCPv6 Relay

Restrictions and Precautions

- DHCPv6 relay is not supported in switch mode.
- When configuring DHCPv6 relay, the interface must work in routing mode and configure static IP. L3 physical interfaces, physical subinterfaces, VLAN interfaces, bridge interfaces, L3 aggregation interfaces, aggregation subinterfaces, and tunnel interfaces all support DHCPv6 relay.
- DHCPv6 relay is disabled by default. DHCPv6 relay will take effect only after DHCPv6 relay is enabled.

- The DHCPv6 server and a DHCPv6 relay cannot be configured on an interface at the same time.

Configure DHCPv6 Relay

Step 1. Select “Network > DHCP > DHCP Relay".

Step 2. Click the “DHCP Relay” tab.

Step 3. Click “Add”.

Step 4. Configure the relay interface.

The interface must be configured with a static IP address, and the IP address should be on the same network segment as the DHCP client.

Step 5. Add a server.

Add a DHCPv6 server, specify the server address and outbound interface. Up to 8 servers can be added. The DHCPv6 relay needs to maintain connectivity with these DHCPv6 servers.

Step 6. After the configuration is complete, click “OK”.

3.7 ARP

ARP (Address Resolution Protocol) is a TCP/IP protocol for obtaining MAC addresses based on IP addresses. The APR table records the correspondence between the host IP address and MAC address and the firewall interface to which the host is connected.

The firewall supports adding ARP entries manually and generating ARP entries automatically.

3.7.1 Static ARP Entry

Static ARP refers to ARP entries added manually, and there is a fixed binding relationship between IP addresses, MAC addresses, and interfaces.

Background Information

Static ARP entries are manually added and will not be dynamically updated and have no aging time. After being added, they are always valid. Static ARP entries have a higher priority than dynamic ARP entries, and the packets are preferentially matched to static ARP entries.

Configuring a static APR entry can restrict packets using a certain IP address to only use the specified MAC address and enter the firewall only through the specified interface. This prevents other devices from impersonating the IP address.

Configure Static ARP Entries

Step 1. Select "Network > ARP > Static ARP".

Step 2. Click “Add”.

Step 3. Set the ARP parameters.

Parameter	Description
IP address	Set the IP address of the host. Support IPv4 addresses.
MAC address	Fill in the MAC address corresponding to the host IP address.
Interface	Select the interface corresponding to the IP address.

Step 4. After the configuration is complete, click “OK”.

The added ARP entries are displayed in the ARP list. You can view the status information of IP address, MAC address, interface, security domain, and ARP.

3.7.2 Dynamic ARP Entries

Dynamic ARP entries are automatically executed by the firewall and record the correspondence between IP addresses, MAC addresses, and interfaces without manual configuration.

The ARP dynamically learned by the firewall is displayed in the dynamic ARP list. In the list, you can check the dynamic ARP IP address, MAC address, interface, security zone, timeout, status and whether it is bound.

In order to adapt to network changes, the ARP table needs to be updated continuously. The automatically generated entries in the ARP dynamic table are not permanently valid, and each entry has a timeout period. The entries that have not been updated after the timeout expires will be deleted. If the record of the entry is refreshed before the timeout expires, the timeout of the entry will be recalculated.

3.7.3 Dynamic ARP Entry Binding

When dynamically generating ARP entries, legitimate users and hacker users cannot be distinguished, and there are potential security risks. Binding IP addresses, MAC addresses, and interfaces can prevent hacker users from masquerading as legitimate users.

Step 1. Select "Network > ARP > Dynamic ARP".

Step 2. Select one or more ARP entries to be bound.

Step 3. Click “Bind”.

Step 4. Click “OK” in the displayed dialog box.

When the interface of the selected IP-MAC address pair is not bound to a security zone, the IP and MAC addresses cannot be bound.

The bound IP-MAC address pair can be unbound through the IP-MAC binding policy.

3.7.4 Configure ARP Proxy

Only the command-line configuration of proxy ARP is supported.

Command to create an ARP proxy: **arp-proxy** *proxy-name* **interface** *interface-name* **[[vlan** *vlan-id* **target-ip** *ip-object*] **action { proxy | noproxy }]**

3.8 MAC

3.8.1 Add Static MAC

The firewall supports adding MAC entries manually.

Step 1. Select "Network > MAC > Static MAC".

Step 2. Click “Add”.

Step 3. Set the MAC parameters.

Parameter	Description
MAC address	Add the MAC address of the LAN host.
Interface	Select the L2 interface that receives the source MAC data frame.
Mode	Select whether the interface works in VLAN mode or bridge mode. • When the interface mode works in bridge mode, you also need to select the bridge ID to which the interface belongs. • When the interface mode works in VLAN mode, you also need to select the VLAN ID to which the interface belongs.
VLAN	When the interface mode is "VLAN", select the VLAN bound to the interface.
Bridge	When the interface mode is "Bridge", select the bridge bound to the interface.
VLAN ID	After selecting "VLAN ID", you can specify the corresponding VLAN ID of the bridge interface.

Step 4. After the configuration is complete, click “OK”.

3.8.2 View Dynamic MAC Table

The firewall supports dynamic MAC learning, and the firewall automatically adds the MAC address of the device through learning.

The dynamic MAC table is a list automatically learned by the firewall. The dynamic MAC list will display the binding relationship between MAC address, VLAN ID and bridge or interface and the timeout time. Users can manually delete dynamic MAC entries before they expire.

In order to adapt to network changes, the MAC address table needs to be continuously updated. The automatically generated entries in the MAC address table are not permanently valid, and each entry has a timeout period. The entries that have not been updated after the timeout expires will be deleted. If the record of the entry is refreshed before the timeout expires, the timeout of the entry will be recalculated.

You can query, refresh, delete or clear all entries in the dynamic MAC list.

3.9 Long Connection

Long connections are mostly used for frequent operations and point-to-point communication, and there should not be too many connections. Long connections can save more TCP establishment and closing operations, reduce performance waste, and save time. But long connections may also cause too many firewall connections. Long connections can be controlled through security policies.

Step 1. Choose “Network > Long Connection”.

Step 2. Click “Add”.

Custom persistent connections support eight groups of configurations.

Step 3. Configure long connection name and timeout.

Parameter	Description
Name	Specifies the name of the custom long connection object.
Timeout	Uniformly modify the timeout time of the TCP long connection in the default long connection, the unit is second, and the range is 1-4294967 seconds

Step 4. After the configuration is complete, click “OK”.

The configured long connection is displayed in the long connection list, and the custom long connection group can be referenced in the security policy.

3.10 Interface Linkage

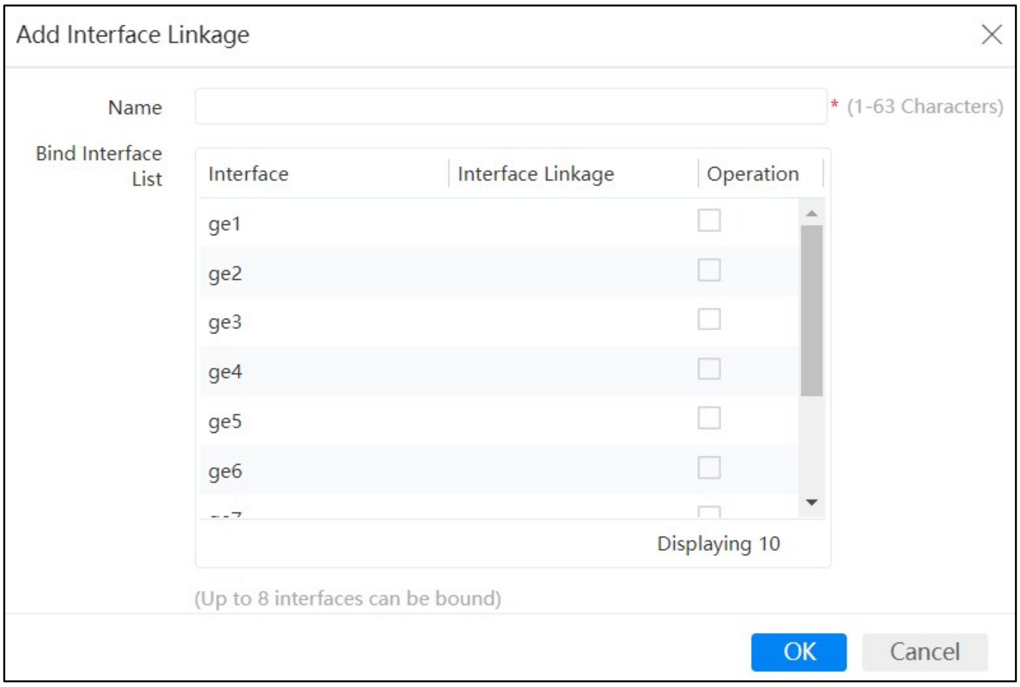
The interface linkage function is mainly used in conjunction with the high availability function.

In the dual-machine serial environment of multiple devices, when the uplink/downlink link of the device fails, in order for the downlink/uplink link to quickly sense the failure and switch over, we need to bind the uplink interface and the downlink interface to a linkage group. When any interface in the group fails, other interfaces will set their status to down, so that the uplink and downlink links can sense that there is a link failure and need to switch.

Step 1. Choose “Network > Interface Linkage”.

Step 2. Click “Add”.

Step 3. Configure the interface linkage parameters.



Add Interface Linkage

Name * (1-63 Characters)

Bind Interface List

Interface	Interface Linkage	Operation
ge1		□
ge2		□
ge3		□
ge4		□
ge5		□
ge6		□
ge7		□

Displaying 10

(Up to 8 interfaces can be bound)

Parameter	Description
Name	Specifies the name of the interface linkage
Binding interface list	Select based on physical interface and channel port. A physical interface or channel port can only belong to one interface linkage group. The assigned interface will display the name of the interface linkage group to which belongs in the interface linkage menu.

Step 4. After the settings are complete, click “OK”.

After the configuration is complete, the interface linkage group is displayed in the interface linkage list. You can view the name, status, faulty interface, and interface list of the interface linkage group. You can edit and delete interface linkage groups.

3.11 Link Health Check

Link health check is a functional module for the firewall to regularly detect adjacent or remote links, from the network layer, transport layer to application layer, and determine the link quality through multi-level detection. The configured link health check policy can be referenced in functions such as HA and link balancing to help dual-device hot backup and link balancing functions select high-quality links to provide services.

Step 1. Choose “Network > Link Health Detection”.

Step 2. Click “Add”.

Step 3. Configure link health check parameters.

Parameter	**Description**
Name	Specifies the name of the link health detection policy.
Description	A brief note on the link health check policy.
Interval	Specify the interval for sending detection packets, the default is 6 seconds, and the range is 1-60 seconds.
Timeout	Specify the timeout period when the detection packet does not receive a response, the default is 1 second, and the range is 1-59 seconds.
Retry times	The times of re-sending the detection packets after the specified detection fails. If there is still no response packet after reaching the upper limit of attempts, it is judged that the detection IP address is invalid. The default is 3 times, and the range is 1-10 times.
IP type	The IP type of the detection address is divided into IPv4 and IPv6. Select the IPv4 address type, and the added detection address must be in IPv4 address format; Select the IPv6 address type, and the added detection address must be in IPv6 address format.
Detection address	The destination IP address to detect
Outbound interface	Select the outbound interface for sending detection packets. When [NONE] is selected, no outgoing interface is specified.
Next hop gateway	The address of the next-hop gateway to the network segment

Parameter	Description
	of the destination address to be detected. After the outgoing interface is selected, the next-hop gateway can be configured. The address of the next-hop gateway is on the same network segment as the address of the outgoing interface of the firewall.
ICMP delay switch	When it is necessary to record ICMP delay and TTL (for example, the policy routing load algorithm selects delay load or hop count load), enable this function. After this function is enabled, the link detection will record the ICMP delay, that is, the response time (Response Time) and TTL of the ICMP detection. After the ICMP delay function is enabled, the detection protocol will automatically select ICMP.
Protocol	Select the protocol used by the detection packets to be sent as required. • TCP detection sends TCP protocol detection packets to confirm whether the TCP service is normal. The default TCP port is port 80. Users can customize the target port, and the range is 1-65535. • HTTP detection sends HTTP protocol detection packets to confirm whether the HTTP service is normal. The default target port is HTTP port 80, users can customize the target port, and the range is 1-65535. • DNS detection sends DNS detection packets to confirm whether the DNS service is normal. • ICMP sends ICMP protocol probe packets. It is mainly used to confirm whether the link is reachable. After the ICMP delay is enabled, the current link quality of the reachable link can be detected.

Step 4. After the configuration is complete, click “OK”.

The configured link health check is displayed in the link health check list. You can view the name, probe address, protocol, port, probe result, and reference count of the link health check policy.

The detection result is "Alive", indicating that the detection object is normal; the detection result is "N/A", indicating that the detection object does not exist, and the detection result is "Dead", indicating that the detection object is faulty.

3.12 802.1x Authentication

3.12.1 Restrictions and Precautions

802.1x selects local authentication, and the user name is not allowed to contain Chinese.

Otherwise, the authentication will fail.

3.12.2 Overview

802.1x is a port-based network access control protocol. Control client access to network resources by authenticating user equipment accessing through ports. The 802.1x authentication system adopts a typical Client/Server(C/S) structure, including three parts: client, device and authentication server.

- Client

The LAN user terminal equipment must be a device (such as a PC) that supports EAPOL (Extensible Authentication Protocol over LAN). The 802.1x authentication can be initiated through the 802.1x client software installed on the client device.

- Device side

A network device (firewall here) that supports the 802.1x protocol authenticates the connected client.

- Authentication server

The firewall supports local authentication and third-party RADIUS server authentication.

Before the authentication is passed, 802.1x only allows EAPoL (Extensible Authentication Protocol for LAN) data to connect to the firewall interface. After the authentication is passed, the client can access network resources.

3.12.3 Configure 802.1x Authentication

Step 1. Choose “Network > 802.1x Authentication”.

Step 2. Click “Add”.

Step 3. Configure 802.1x authentication parameters.

Parameter	Description
Interface name	Select the interface to enable 802.1x authentication.
Description	The remarks of the 802.1x authentication policy are different from other 802.1x authentication policies.
Enable	Check the box to enable this policy.

Parameter	Description
Access control type	• Select "Port-based"; after any client connected to the selected interface passes the authentication, other clients do not need to be authenticated. • If "Based on MAC" is selected, each client connected to the selected interface needs to be authenticated, and no authentication is required when the same MAC passes through the interface again.
Authentication server	Select the authentication server to which 802.1x authentication is bound. You can select a local authentication server or a third-party Radius authentication server. • When using a local authentication server, the internal implementation adopts the EAP termination method, and only supports the MD5-Challenge authentication method. • When the Radius authentication server is used, the internal implementation adopts the EAP relay mode and supports four authentication modes: MD5-Challenge, PEAP, EAP-TLS, and TTLS.
Authentication overtime	The default is 30 seconds. The client sends an authentication request to the authentication server, but the authentication server does not respond for a long time, reaching the time set by the authentication timeout time (such as 30 seconds), and the authentication timeout is judged.
Authentication request retransmission times	The default is 5 times. The times of re-transmitting the request when the authentication server does not receive a reply from the client within the specified time. The retransmission interval is 3 seconds, 6 seconds, 12 seconds, 20 seconds, 20 seconds...20 seconds.
Re-authentication cycle	The default is 300 seconds. The re-authentication cycle is a function enabled by the firewall to detect whether the client is online. When the re-authentication period is set to 300 seconds, the firewall will send a request to the online client every 300 seconds, and the client will reply to the firewall. The client is currently online, and the online time will continue to accumulate. If the client does not answer the firewall, the client is offline. The user is not aware of this process. When it is set to 0, it means that the re-authentication function is not enabled.

Parameter	Description
Silent time	The default is 60 seconds. The silent time of the 802.1x authentication server after the client authentication fails. If it is set to 60 seconds, it means that within 60 seconds after the client authentication fails, even if the client initiates an authentication request again, the authentication server will not respond to the client. When it is set to 0, it means that the silent time function is not enabled.

Step 4. After the configuration is complete, click “OK”.

802.1x authentication monitoring

After the user passes the 802.1X authentication and can access normally, you can view the information of the 802.1x authentication user in "Data Center > Monitoring > User Monitoring > 802.1X Authentication".

Parameter	Description
Username	Username for 802.1x authentication.
Client MAC address	MAC address of the 802.1x authenticated user.
Interface name	The name of the firewall interface through which 802.1x user authentication passes.
Authentication server name	Authentication server name for 802.1x authentication users.
Online time	Accumulated online time of 802.1x authentication users.

4 Object Configuration

Objects are the most basic components of a firewall and can be referenced in various policies of the firewall. Before configuring various policies, you need to configure the referenced objects first.

4.1 Address

4.1.1 Add Address Object

Firewall address objects support adding IPv4 addresses, IPv6 addresses, and domain names. When an address object contains both an IPv4 address and an IPv6 address, the IPv6 address will not take effect. When configuring an IPv6 address object, please do not add an IPv4 address.

Step 1. Choose “Object > Addresses > Addresses”.

Step 2. Click “Add”.

Step 3. Configure address object parameters.

Parameter	Description
Name	Configure the address object name.
Description	Add a description for the address object.
IP address	Add an IPv4 or IPv6 address, and an IPv4 or IPv6 address segment. Each line can be configured with one IP address or IP address segment. Lines are separated by carriage returns. **Notes** A maximum of 512 IPs and domain names can be configured under an address object. For example: 10.10.1.2/255.255.255.0 10.10.1.2/32 10.10.1.2-10.10.1.10 10.10.1.2 8000::1 a234::120/120 a234::a237-b234::b237

Parameter	Description
Domain name	Add one or more host domain names. The length of a single domain name address does not exceed 255 characters.
Exclude address	IP addresses support adding one or more address items that need to be excluded, and the address object will exclude the excluded addresses contained in the IP address. Each line can be configured with one IP address or IP address segment. Lines are separated by carriage returns. For example: 10.10.1.2/255.255.255.0 10.10.1.2/32 10.10.1.2-10.10.1.10 10.10.1.2 8000::1 a234::120/120 a234::a237-b234::b237 **Notes** Up to eight excluded addresses can be configured.

Step 4. After the configuration is complete, click “OK”.

The configured address objects can be viewed in the address object list. You can see the name, address, excluded address, number of references and operations of the address object.

Click the number of references to view which policies the address object is referenced by.

Click the button corresponding to the operation to modify the parameters of the address object.

4.1.2 Add Address Group

The firewall address group object supports adding address objects and address groups.

Step 1. Choose “Object > Address > Address Group”.

Step 2. Click “Add”.

Step 3. Configure address group parameters.

Parameter	Description
Name	Configure the address group name.
Description	Add a description for the address group.

Parameter	Description
Select address object	You can select all address objects or address group objects, or query specific address objects or add address group objects. In the " Optional " area box, add the desired address object or address group to the "Selected" area box. Up to 32 address objects or address groups can be selected.

Step 4. After the configuration is complete, click “OK”.

The configured address group can be viewed in the address group list. You can see the name, content, number of references and operations of the address group.

Click the number of references to view which policies the address group is referenced by.

Click the button corresponding to the operation to modify the parameters of the address group.

4.1.3 Add Server Address

The server address function is used to implement server load balancing and distribute specific services to multiple servers, thereby providing service processing capabilities and ensuring service reliability.

Step 1. Choose “Object > Address > Server Address”.

Step 2. Click “Add”.

Step 3. Configure server address parameters.

Parameter	Description
Name	Configure the name of the server address object.
Description	Add the description for server address object.
Type	The server address type supports IPv4 and IPv6. Please select according to the actual networking.
Load balancing mode	Server load balancing includes three load balancing methods, which are polling, weight polling, and source address HASH. When a service of the user is provided by multiple servers through load balancing, add the IP addresses of multiple servers to the server address object and specify the load balancing mode. When there is only one server, the load balancing mode does not work.

Parameter	Description
Server address	Configure the IPv4 or IPv6 address of the server in the text box, and you can add up to eight server addresses. Please define server address objects that provide different services separately. For example, for the server address objects that provide HTTP services and FTP services, please use two server address objects to define them separately, and do not write them in the same server address object. Otherwise, when being referenced by DNAT, there will be a phenomenon that the service cannot be accessed.

Step 4. After the configuration is complete, click “OK”.

The configured server address can be viewed in the server address list. You can see the name, load balancing method, server address, number of references and operations of the server address object.

Click the number of references to view which policies the server address object is referenced by.

Click the button corresponding to the operation to modify the parameters of the server address object.

4.2 Country/Region

4.2.1 View Predefined Countries/Regions

The firewall supports the region library, and the predefined countries/regions in the region library can be viewed in the country /region.

4.2.2 Add a Custom Country

Step 1. Choose “Object > Region”.

Step 2. Click “Add”.

Step 3. Configure the parameters for the country.

Parameter	Description
Name prefix	Select the country or region to which the region you want to add belongs.
Name	Configure the name of the added region.
Description	Add the necessary description for the region.
Longitude	Add the longitude corresponding to the region, so as to better locate the area.

Parameter	Description
Latitude	Add the latitude corresponding to the region, so as to better locate the area.
IP address	Add the IPv4 addresses that need to be monitored in this region. Each line can be configured with one IP address or IP address segment. Lines are separated by carriage returns. For example: 1 0.10.1.2 / 255.255.255.0 10.10.1.2/32 10.10.1.2-10.10.1.10 10.10.1.2

Step 4. After the configuration is complete, click “OK”.

4.3 Service

The service function module mainly provides basic configuration for security policies, NAT and other rules. Currently supports three types of predefined services, custom services and custom service groups.

4.3.1 View Predefined Services

For the convenience of users, 43 commonly used services have been predefined in the service, which can be directly referenced in security rules, NAT, and other places, and the number of times they are referenced is displayed in the list.

A service named "any" represents any service.

In the predefined service list, you can view the predefined service name, protocol and configured protocol number, source port, destination port and other information, and the number of references.

Predefined services can only be viewed, not modified or deleted.

4.3.2 Add Custom Service

Step 1. Choose “Object > Service > Custom Service”.

Step 2. Click “Add”.

Step 3. Configure the name and description of the custom service.

Step 4. Click “Add” to add a protocol.

Multiple protocols can be added repeatedly, and a maximum of 32 can be added.

Step 5. Configure protocol parameters.

Protocol types include TCP, UDP, ICMP, ICMPv6, and others.

- The protocol is TCP or UDP.

Parameter	Description
Protocol	Select the protocol type for the service.
Source port	Configure the source port of the protocol. The start value of the source port of the TCP or UDP protocol is usually 1, and the end value is usually 65535.
Destination port	Configure the destination port of the protocol, that is, the custom port. When the service is a single port, the start port and end port should be the same.

- The protocol is ICMP.

Configure the type and code range of ICMP.

ICMP types and encoding descriptions are shown in the table below.

ICMP Packet	Name	Type	Code	Description
Query packet	Echo request or reply	0	0	Echo response (Ping response)
		8	0	Echo request (Ping request)
	Router request or Reply	9	0	Router advertisement
		10	0	Router request
	Timestamp request or response	13	0	Timestamp request (obsolete)
		14	0	Timestamp response (obsolete)
	Information request or response	15	0	Request for Information (obsolete)
		16	0	Information response (obsolete)
	Address mask request or reply	17	0	Address mask request
		18	0	Address mask reply
Error report packet	The destination unreachable	3	0	Network unreachable
			1	Host unreachable
			2	Protocol unreachable
			3	Port unreachable

ICMP Packet	Name	Type	Code	Description
			4	Fragmentation is required, but the un-fragmented field of this packet has been set.
			5	Source routing could not be completed
			6	Destination network unknown
			7	Destination host unknown
			8	The source host is isolated (obsolete)
			9	Destination network is forcibly prohibited
			10	The destination host is forcibly prohibited
			11	The network is unreachable for the specified service type
			12	The host is unreachable for the specified service type
			13	Communication is forcibly prohibited due to filtering
			14	host override
			15	Priority suspension in effect
	Source suppression	4	0	source is closed (basic flow control)
	Change route	5	0	Redirect to network
			1	Redirect to host
			2	Redirect to service type and network
			3	Redirect to service type and host
	Timeout	11	0	Time to live is 0 during transfer
			1	A fragmented datagram has a time-to-live of 0 during packet assembly

ICMP Packet	Name	Type	Code	Description
	Parameter problem	12	0	Bad IP header (including various errors)
			1	Missing required option

- The protocol is ICMPv6.

Configure the type and encoding range of ICMPv6.

ICMP v6 types and encoding descriptions are shown in the table below.

ICMPv6 Packet	Name	Type	Code	Description
Error packet	Destination unreachable	1	0	No path to destination
			1	Communication with the destination is administratively prohibited
			2	Exceed the range of the source address
			3	Destination address unreachable
			4	Port unreachable
			5	Source address failed (due to filter policy)
			6	Refuse to forward to destination
	Group too large	2	0	The MTU field in the packet will tell the sender the maximum packet length that the network can accept
	time out	3	0	The packet is discarded by the router because the value of the hop limit field was zero
			1	There are other fragments that have not arrived within the time limit, and the fragments of the packet are discarded
	Parameter problem	4	0	Wrong header field
			1	Unrecognized next header type

ICMPv6 Packet	Name	Type	Code	Description
			2	Unrecognized IPv6 option
Information packet	Echo request or reply	128	0	Echo request (echo-request)
		129	0	Echo reply (echo-reply)
Neighbor discovery packet	Router inquiry message	133	0	The host uses the router inquiry message to discover the router in the network that can forward the IPv6 packet for the host
	Router advertisement packet	134	0	Sent by a router in response to a router query packet
	Neighbor inquiry packet	135	0	Neighbor inquiry packet have the same task as ARP request packet.
	Neighbor Advertisement	136	0	Sent in response to a neighbor query packet, which is equivalent to the ARP reply packet in IPv4
	Change route packet	137	0	In order to update the routing table in the host, the router sends a change route packet to the host
	Reverse neighbor advertisement packet	141	0	When a endpoint knows the link-layer address of a neighbor, but does not know the IP address of the neighbor, the endpoint sends a reverse neighbor query packet
	Reverse Neighbor Advertisement	142	0	Sent in response to a reverse neighbor query packet
Group membership packet	Membership query packet	130	0	Membership query packets are sent by routers to find out active group members in the network
	Membership report packet	143	0	The membership report packet is sent in response to the membership query packet

- Protocol is Other.

Other types require the user to specify the protocol number of the custom service, ranging from 0-255.

Step 6. After the configuration is complete, click “OK”.

4.3.3 Service Group

Step 1. Choose “Object > Service > Service Group”.

Step 2. Click “Add”.

Step 3. Configure service group parameters.

Parameter	Description
Name	Configure the name of the service group.
Description	Add the necessary description for this server.
Select service object	The member of a service group can be predefined services, custom services, or service groups. You can use the query function to find services or service groups that contain the entered characters. Select the desired service or service group in the “Optional” area box and add it to the “Selected” area box. Up to 32 items can be added.

Step 4. After the configuration is complete, click “OK”.

4.4 Application

4.4.1 Overview

The application is a means to identify the corresponding application program by using the unique characteristics of the application program, so as to accurately identify the application program in various scenarios. Different applications with the same protocol and port number can be identified through application characteristics. The firewall supports predefined applications and custom applications.

- Predefined applications: loaded through the application identification library

All applications contained by the application recognition library will be displayed in the application list. The application identification library will be continuously updated to add new applications. Please update the latest application identification library in time to ensure that the policy based on application identification can remain effective.

- Custom application

  Users can customize a new application according to the characteristics of the application, and the system identifies the application according to the application rules configured by the user.

The application includes attributes in five dimensions: classification, sub-category, data transmission method, and risk level and characteristic attributes. Categories and subcategories are described in the table below.

Classification	**Subcategory**
Commercial software	Authentication services Database Enterprise resource planning General business group Management software Office software Software update Storage backup Stock securities
Switching software	Mail Instant messaging Web tool Web conference Social network Video Audio VoIP Page submission
General protocol	File sharing
Multimedia software	Audio stream Game Picture Video stream
Network protocol	Encrypted tunnel Basic agreement IP protocol Proxy protocol Remote access Routing Protocol

The firewall divides the application risk level into five levels. From 1 to 5, the larger the number, the higher the risk level. The system automatically calculates the risk level of the application based on the characteristic attributes of the application.

Characteristic attributes are used to describe the characteristics of the application's security aspects, including:

- Avoid
- Use too much bandwidth
- Used by by malware
- Can transfer files
- With known vulnerabilities
- Other tunneling applications
- Easy to misuse
- commonly used
- Continuously scanned by other applications

4.4.2 View Predefined Applications

Predefined applications cannot be modified or deleted, but can only be viewed and referenced.

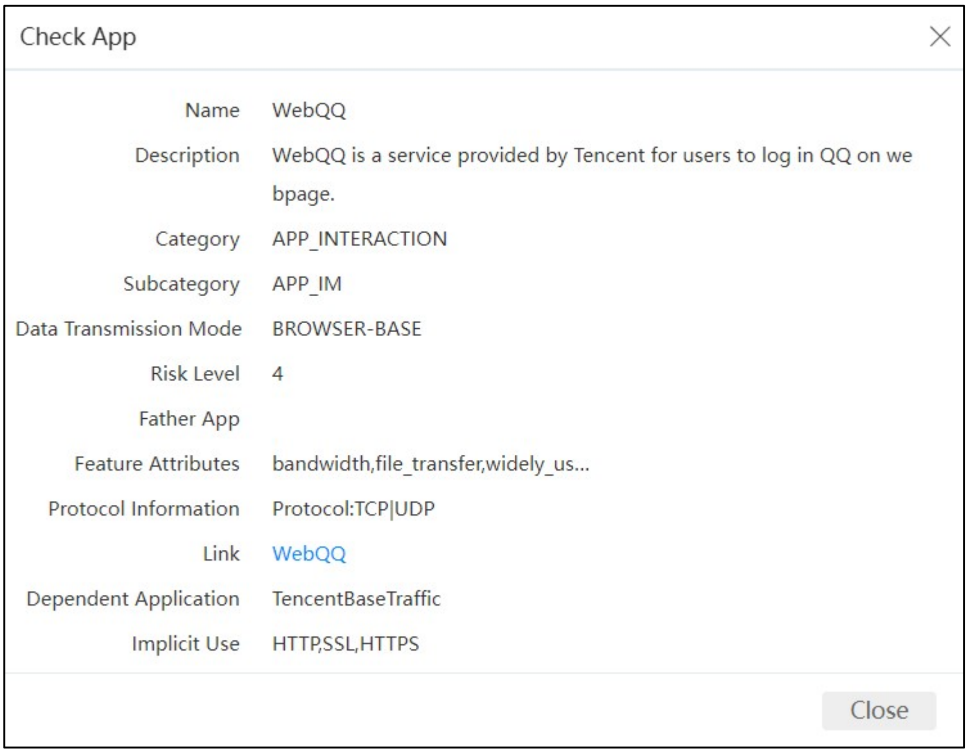
Step 1. Choose “Object > Application > Application”.

Step 2. All predefined apps can be viewed in the app list.

Step 3. (Optional) By selecting a category, subcategory, data transmission method or risk level, you can filter out the application types that meet the selection criteria.

Step 4. (Optional) The filtered application types can also be searched by keywords through the query function in the upper right corner of the page.

Step 5. Click the View button of the application to view the details of the application.



Check App

Name	WebQQ
Description	WebQQ is a service provided by Tencent for users to log in QQ on we bpage.
Category	APP_INTERACTION
Subcategory	APP_IM
Data Transmission Mode	BROWSER-BASE
Risk Level	4
Father App	
Feature Attributes	bandwidth,file_transfer,widely_us...
Protocol Information	Protocol:TCP|UDP
Link	WebQQ
Dependent Application	TencentBaseTraffic
Implicit Use	HTTP,SSL,HTTPS

Click the link to jump to the linked page to view the detailed description of the application.

4.4.3 Add a Custom Application

Step 1. Choose “Object > Application > Application”.

Step 2. Click “Add”.

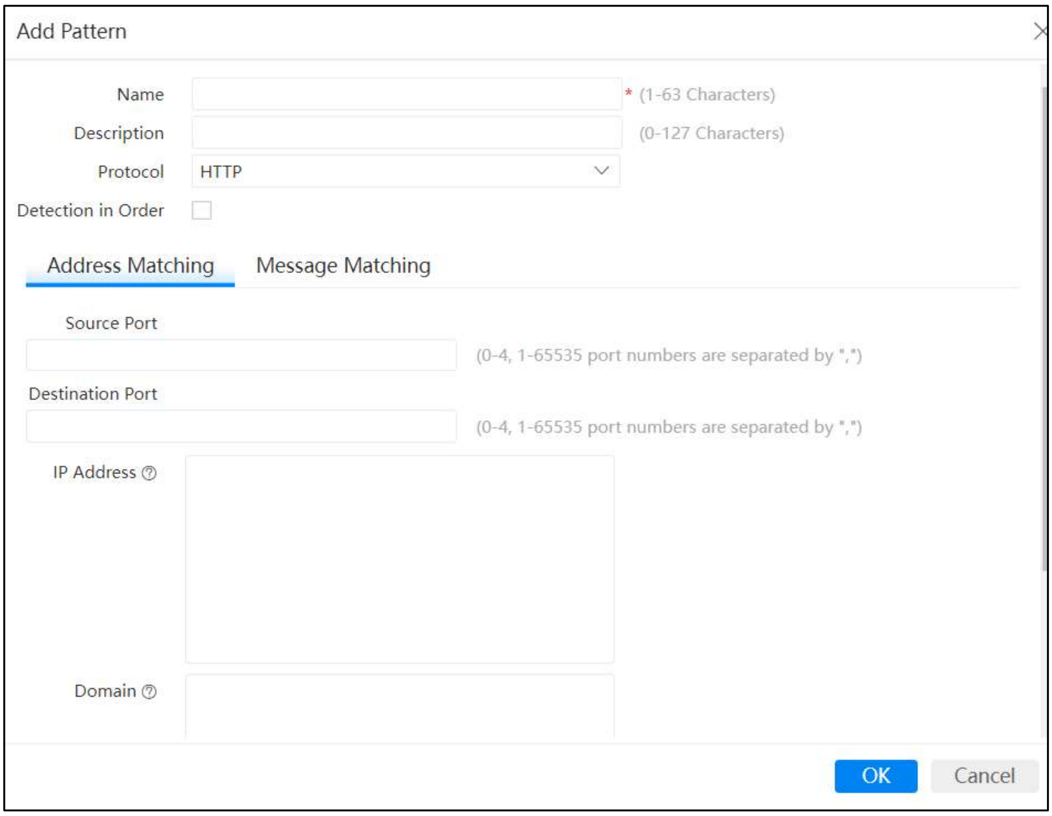
Step 3. Configure the name and description of the application.

Step 4. Configure the basic properties of the application.

Select the category, sub-category, data transmission method, risk level, parent application, feature attributes, etc. to which the application belongs. Multiple feature properties can be selected at the same time.

Step 5. Add the application rules.

Click the “Rules” tab, and click “Add” to add an application rule.



Add Pattern

Name * (1-63 Characters)

Description (0-127 Characters)

Protocol HTTP

Detection in Order □

Source Port (0-4, 1-65535 port numbers are separated by ",")

Destination Port (0-4, 1-65535 port numbers are separated by ",")

IP Address

Domain

1. Configure the name and description of the rule.
2. Choose a protocol. Select the protocol that the rule matches.

   Protocols include: HTTP, TCP, UDP, ICMP, and ICMPv6.

3. Set whether to enable detection in order.
4. Configure address matching rules.

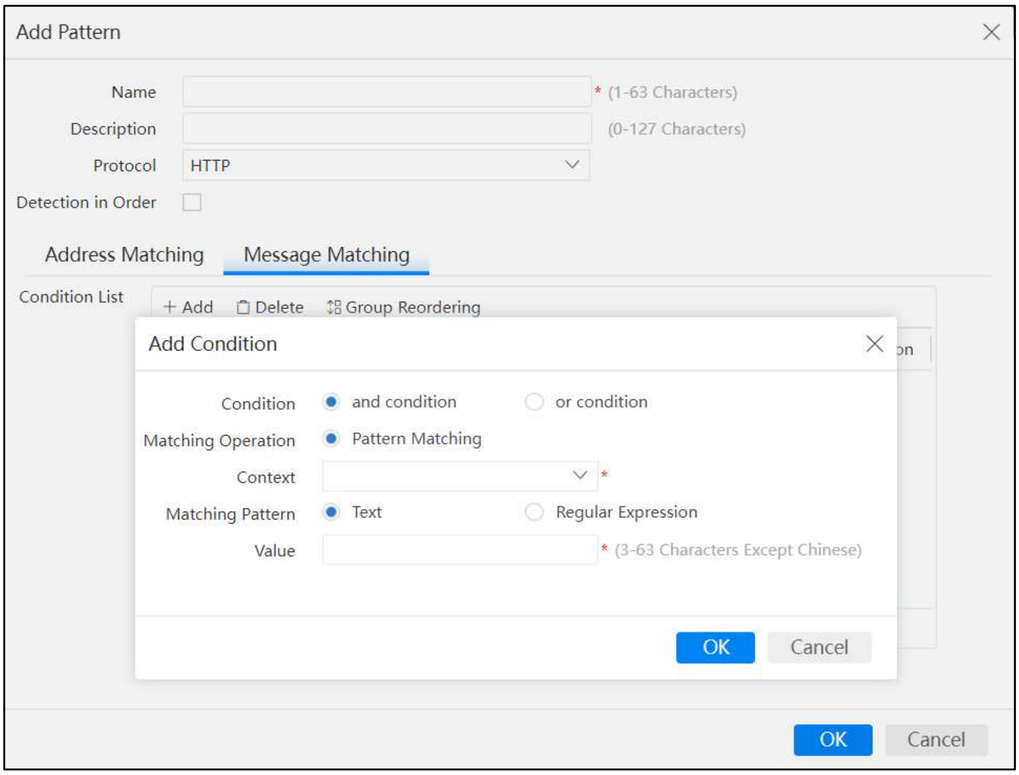
   Choose to configure the source port, destination port, and IP address of the application.

   Configure up to four source port numbers or destination port numbers, and the port numbers are separated by English commas ",".

   Add up to four IP addresses. The IP address can be either an IPv4 address or an IPv6 address.

5. Configure packet matching rules.

   Click “Packet Matching”. Click "Add" to add conditions, and click "OK" after the addition is complete. You can add up to eight AND conditions, 1 to 6 OR conditions.



Add Pattern

Name * (1-63 Characters)

Description (0-127 Characters)

Protocol HTTP

Detection in Order □

Add Condition

Condition ● and condition ○ or condition

Matching Operation ● Pattern Matching

Context *

Matching Pattern ● Text ○ Regular Expression

Value * (3-63 Characters Except Chinese)

Parameter	Description
Condition	Support and condition, or condition.
Matching operation	When the protocol type is "HTTP", "ICMP" or "ICMPv6", the matching operation only supports "pattern matching", and when the protocol type is "TCP" or "UDP", the matching operation supports "Pattern matching " and "Equal to". Among them: • Pattern matching Pattern matching is to match the string specified by the protocol with the value set by the user. • Equal to Equal to is to calculate the position and length filled in first, and matching the calculated value with the value set by the user.

Parameter	Description
Context	Context options are related with protocol. • When the protocol is HTTP, the context options include: HTTP.req_uri_path, HTTP.req_host, HTTP.req_method, HTTP.req_referer, HTTP.req_user_agent, HTTP.req_cookie, HTTP.rsp_body, HTTP.req_body. • When the protocol is TCP, the context options include: TCP.unknown_tcp_req, TCP.unknown_tcp_res. • When the protocol is UDP, the context options include: UDP.unknown_udp_req, UDP.unknown_udp_res. • When the protocol is ICMP, the context options include: ICMP.icmp_req, ICMP.icmp_res. • When the protocol is ICMPv6, the context options include: ICMPv6.icmpv6_req, ICMPv6.icmpv6_res.
Matching pattern	When the operation is "pattern matching ", the matching mode can be set. The matching mode supports "Text matching" and "Regular express". Text matching is to directly match the string of the specified field with the string specified by the value; regular express is to calculate the string and the specified string according to the regular expression before matching.
Location	Enter where the keyword begins.
Length	Enter the length at which the keyword begins. Compare a value calculated by the position and length with the value set by the user.
Value	When the operation is match, the value ranges from 3 to 63 characters except Chinese. Regular expressions need to be written in a professional rule language, such as hexadecimal ascii code or and, or relationship symbols. When the operation is equal to, the value ranges from 0 to 4294967295.

Step 6. After the rule configuration is complete, click “OK”.

Step 7. Click “OK”, and then, customize the app.

Step 8. Click “Submit”.

Only submitted applications will take effect.

4.4.4 Add Application Group

A collection of multiple applications is called an application group. The system supports adding predefined applications and custom applications to the same application group.

Step 1. Choose “Object > Application > Application”.

Step 2. Click “Add”.

Step 3. Configure the name and description of the application group.

Step 4. Click “Add” and select the desired application.

You can find the corresponding application by filtering by classification, transmission method, risk level or keyword query. To add a new application, click “Add”. After the configuration is complete, click “OK”.

Step 5. Click “OK”.

4.5 Time

The time object can be referenced in the policy, so that the policy takes effect within the time range specified by the time object. For users, it is possible to control access to certain services during a certain period of time, and not to control access to certain services during a certain period of time. The time control can be accurate to the second, making the firewall policy more flexible.

4.5.1 Add a Single Time Object

A single time object refers to a time period object that specifies a specific date and time. The time period does not loop.

Step 1. Choose “Object > Schedules”.

Step 2. Click “Add”.

Step 3. Set the parameters of the time object.

Parameter	Description
Name	The name of the time object.
Description	Remarks on the time object, to distinguish it from other time objects.
Period type	Select " Single " for the period type of the time object.
Period	
Start time	Click in the text boxes to select a start date and specific time.
End Time	Click in the text boxes to select an end date and specific time.

Step 4. After the configuration is complete, click “OK”.

4.5.2 Add a Cycle Time Object

Cycle time objects support daily, weekly, and monthly. The daily cycle supports the specified time period; the weekly cycle specifies the weekly execution date and corresponding time period by referring to the daily cycle; the monthly cycle supports the specified execution date, but does not support the specified time period, and the default time period is 24 hours.

Step 1. Choose “Object > Schedules”.

Step 2. Click “Add”.

Step 3. Set the parameters of the time object.

Parameter	Description
Name	The name of the time object.
Description	Remarks on the time object, to distinguish it from other time objects.
Period type	Select "Cycle" for the period type of the time object.
Cycle type	The cycle type supports "Daily", " Weekly ", and "Monthly". • Daily is used to specify the time period of each day. Execute the specified policy only during that time period. Repeat daily. • Weekly forms a weekly time object by referencing a daily time object. Repeat every week, and only execute the specified policy during the specified time on the specified date. • Monthly is used to specify a start date and an end date. Repeats monthly, executing the specified policy from the start date to the end date.
Time period	
Daily	Add a daily plan, select a daily time period, and fill in up to three items for the time period. The time is in 24-hour format and the format is HH:MM:SS-HH:MM:SS. like: 00:00:00-01:00:00 11:00:00-15:00:00.
Weekly	Select daily time objects in the drop-down boxes from Monday to Sunday. At least one day is required to reference the time-of-day object.
Monthly	Specify a start date and an end date. The time period cannot be specified, and the time period defaults to 24 hours a day.

Step 4. After the configuration is complete, click “OK”.

The configured time objects are displayed in the time object list. The type is Daily, Weekly, or Monthly. You can view the name, type, time period, and reference times of the time object in the list.

Time objects can be modified, queried and deleted.

4.6 Assets

Asset management is used to manage all assets in the user network. Before proceeding with asset management, administrators must understand all assets in the network, asset operating systems, and asset levels. By monitoring all assets in the network, attackers can be prevented from using some unsupervised assets as a springboard to attack user networks.

4.6.1 Restrictions and Precautions

- It is recommended not to include Chinese characters in the asset type. Otherwise, the asset type will be displayed as garbled characters when exporting assets.
- Please avoid including special characters such as Chinese and " # ￥ %…@$%^&*()<p>~%[]-/' " in the asset name to avoid failure to import assets.
- The assets that already exist on the device cannot be included in the asset list.
- The asset type in the asset list must be an asset type that has been created on the device.
- If the name of the operating system is in Chinese characters, it cannot exceed 31 characters.

4.6.2 Add Asset Type

Asset types can be added in asset type configuration or when adding assets.

Step 1. Select “Object > Asset".

Step 2. On the “Asset Settings” page, click “Asset Type Configuration”.

Step 3. Click “Add”.

Step 4. Set the name of the asset type.

Step 5. After the configuration is complete, click “OK”.

The configured asset types are displayed in the asset type list. This asset type can be deleted when it is no longer needed.

Configured asset types can be selected when adding assets.

4.6.3 Add Assets

Assets need to be added before asset management. It is recommended to add all assets in the network to asset management for monitoring. By classifying assets, the firewall can focus on monitoring core assets and key assets. Asset classification requires administrators to understand which assets are the most important assets of the organization and the assets most likely to face threats.

Step 1. Select “Object > Asset".

Step 2. Click “Add”.

Step 3. Configure asset parameters.

Parameter	Description
Name	Set the asset name. **Notes** Please avoid special characters such as Chinese and "# ￥%…@$%^&*()<p>~%[]-/'" in the asset name to avoid garbled characters and wrong lines when exporting assets.
Address	Set the IP address of the asset. Only IPv4 addresses are supported.
Asset type	Select the configured asset type from the drop-down list. If you need to add an asset type, select "Add Asset Type " to add an asset type. Select after adding.
Operation	Sets the operation type for the asset.
Asset level	Asset classes include: common, important, and core. • Core assets include servers that provide important services and computers of some important personnel. • Important assets refer to assets that are more important than ordinary assets but not as critical as core assets. • Command assets mainly refer to the computers of ordinary employees. By dividing asset levels, different levels of protection can be provided for different levels of assets, focusing on protecting core assets and important assets.

Step 4. Click “OK”.

The configured assets are displayed in the asset management list.

The invalid assets can be deleted from the asset management list.

4.6.4 Export Assets

Step 1. Select “Object > Asset".

Step 2. Click "Export", set the file name and save path in the pop-up dialog box, and click "Download".

The meaning of the value of the asset level is: 1 (Normal), 2 (Important), 3 (Core).

4.6.5 Import Assets

There are usually dozens or even hundreds or even thousands of devices in the network that need to be protected. If adding assets one by one is too inefficient, users can add multiple assets by importing the asset list.

Prerequisite

Get an asset list template via "Export". Fill in the asset name (Name), asset address (IP), asset type (Type), operating system (OS), and asset level (Asset value) of the asset to be added in the template.

The firewall supports adding 1000 assets by default. The maximum number of assets that can be added varies with the product model.

Steps

Step 1. Select “Object > Asset".

Step 2. Click “Import”, select the asset list file, and click “OK”.

4.6.6 Query Assets

The firewall supports queries and advanced queries on assets.

Query

You can enter the asset name, asset address, asset type, and operating system in the query input box to query the specified asset information.

Advanced Query

Advanced query can display the asset information at this level by specifying the level of the asset, and support users to conduct further queries at this level. When the user needs to display all levels of asset information, he needs to click “Reset” in the advanced query or select NONE and click “Query” to display all levels of asset information again.

4.7 Keyword Group

The keyword group is used as the basic configuration of content filtering keywords. Before configuring content filtering, email filtering, and URL filtering, users need to define the keywords to be filtered and controlled.

4.7.1 Import or Export Predefined Keyword Groups

The firewall pre-defines five types of keyword groups: mailbox, MD5 code, mobile phone number, ID number, and bank card number. These five types of keyword groups include the characteristics of these keywords.

Since the above five types of keywords usually contain user privacy and sensitive information, users can directly filter and control the five predefined types of keywords in the content filtering and mail filtering modules.

It is recommended that users use the predefined keyword group list exported from the firewall as a template when importing the predefined keyword group list. Based on the exported list, modify it according to requirements, and then import it into the firewall to avoid import errors due to format problems. If there is no special requirement, it is not recommended to modify the list of predefined keyword groups.

Step 1. Choose “Object > Keyword Group > Predefined Keyword Group”.

Step 2. Click "Export" to back up the predefined keyword groups.

Step 3. Click "Import", select the backup or edited predefined keyword group, and click “OK” to import.

4.7.2 Add Keyword Group

Step 1. Choose “Object > Keyword Group > Keyword Group”.

Step 2. Click “Add”.

Step 3. Configure keyword group parameters.

1. Configure the name of the keyword group.
2. Configure the number of hits.

One of the conditions for the filter policy to take effect, the number of occurrences of the keyword reaches the number of times specified by the number of hits.

For example: when the number of hits is 1, the keyword appears once, which means the condition is met. When the number of hits is 10, the keyword has accumulatively appeared 10 times, that is, the condition is met.

3. Configure matching conditions.

Two matching conditions are supported:

- As long as there is a keyword hit

There are multiple keywords in the keyword group, and any keyword that satisfies the hit count filtering policy will take effect.

- All keywords hit at least once

There are multiple keywords in a keyword group, and all keywords must satisfy the hit count filtering policy to take effect.

4. Click “Add” to configure the parameters of the custom keyword.

A maximum of 32 custom keywords can be added to a custom keyword group.

Parameter	Description
Name	The name of the custom keyword.
Match pattern	When the keyword belongs to a fixed field, you can choose "Text"; when the keyword is not fixed, please choose "Regular Expression".
Match string	Enter the text or regular expression to match.

Step 4. After the configuration is complete, click “OK”.

Step 5. Click “Submit”.

After configuring keywords or modifying keywords, you must click "Submit" before the configuration or modification takes effect.

4.8 Security Rule Base

The security rule base includes the vulnerability protection rule base and the anti-spyware rule base.

4.8.1 Vulnerability Protection Rule Base

The vulnerability protection rule base displays all the vulnerability protection rules supported by the firewall intrusion prevention feature database, and their corresponding vulnerability protection categories and subcategories.

Vulnerability Protection Classification

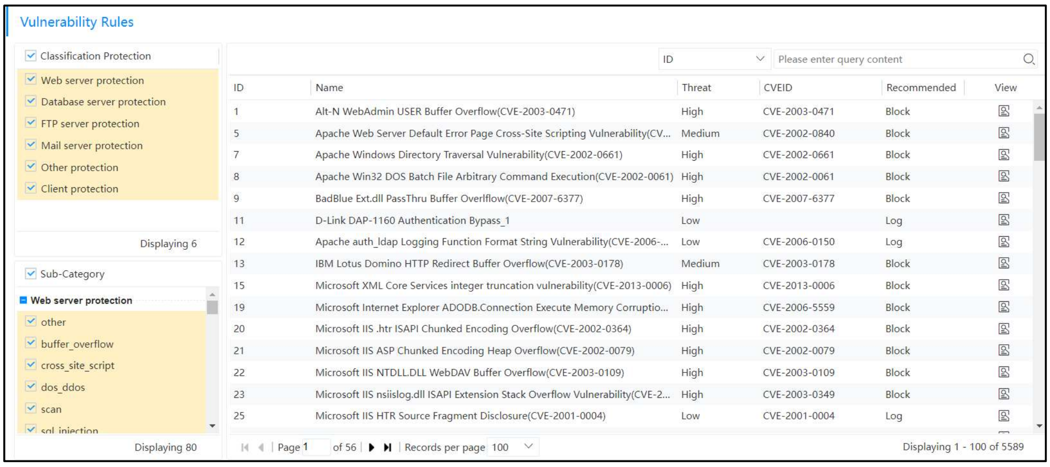
Vulnerability protection is divided into WEB service protection, database service protection, FTP service protection, mail service protection, client protection and other protections. Among them, WEB service protection, database service protection, FTP service protection, and mail service protection respectively implement vulnerability protection for commonly used WEB services, database services, FTP services, and mail services. This protection does not include protection for operating systems and application software; Client protection is to protect the application software installed on the operating system against vulnerabilities; other protection refers to the protection against vulnerabilities of the operating system and services other than WEB services, database services, FTP services, and mail services.

View Vulnerability Protection Rules

Choose “Object > Security Rules> Vulnerability Rules” to view vulnerability protection categories, subcategories, and detailed rules.

By default, the rules under all categories and all subcategories are displayed. You can select the category and subcategory corresponding to the rule to be displayed through the protection category and protection subcategory area boxes on the left.

In the rule list, you can view the rule ID, rule name, severity, CVEID, recommended action and other parameters of each rule.



Vulnerability Rules

☑ Classification Protection
- ☑ Web server protection
- ☑ Database server protection
- ☑ FTP server protection
- ☑ Mail server protection
- ☑ Other protection
- ☑ Client protection

Displaying 6

☑ Sub-Category

Web server protection
- ☑ other
- ☑ buffer_overflow
- ☑ cross_site_script
- ☑ dos_ddos
- ☑ scan
- ☑ sql_injection

Displaying 80

ID | Please enter query content

ID	Name	Threat	CVEID	Recommended	View
1	Alt-N WebAdmin USER Buffer Overflow(CVE-2003-0471)	High	CVE-2003-0471	Block	
5	Apache Web Server Default Error Page Cross-Site Scripting Vulnerability(CV...	Medium	CVE-2002-0840	Block	
7	Apache Windows Directory Traversal Vulnerability(CVE-2002-0661)	High	CVE-2002-0661	Block	
8	Apache Win32 DOS Batch File Arbitrary Command Execution(CVE-2002-0061)	High	CVE-2002-0061	Block	
9	BadBlue Ext.dll PassThru Buffer Overlflow(CVE-2007-6377)	High	CVE-2007-6377	Block	
11	D-Link DAP-1160 Authentication Bypass_1	Low		Log	
12	Apache auth_ldap Logging Function Format String Vulnerability(CVE-2006-...	Low	CVE-2006-0150	Log	
13	IBM Lotus Domino HTTP Redirect Buffer Overflow(CVE-2003-0178)	Medium	CVE-2003-0178	Block	
15	Microsoft XML Core Services integer truncation vulnerability(CVE-2013-0006)	High	CVE-2013-0006	Block	
19	Microsoft Internet Explorer ADODB.Connection Execute Memory Corruptio...	High	CVE-2006-5559	Block	
20	Microsoft IIS .htr ISAPI Chunked Encoding Overflow(CVE-2002-0364)	High	CVE-2002-0364	Block	
21	Microsoft IIS ASP Chunked Encoding Heap Overflow(CVE-2002-0079)	High	CVE-2002-0079	Block	
22	Microsoft IIS NTDLL.DLL WebDAV Buffer Overflow(CVE-2003-0109)	High	CVE-2003-0109	Block	
23	Microsoft IIS nsiislog.dll ISAPI Extension Stack Overflow Vulnerability(CVE-2...	High	CVE-2003-0349	Block	
25	Microsoft IIS HTR Source Fragment Disclosure(CVE-2001-0004)	Low	CVE-2001-0004	Log	

Page 1 of 56 | Records per page 100

Displaying 1 - 100 of 5589

Search for Vulnerability Protection Rules

Support searching for vulnerability protection rules based on rule ID, vulnerability name, CVEID, and CNNVDID.

Enter the rule ID, vulnerability name, CVEID or CNNVDID keyword in the upper right corner of the "Vulnerability Rules" page to perform a fuzzy search. All rules containing this keyword will be searched.

View Rule Details

Click the "View" button under the action to view the detailed information of the rule.

4.8.2 Anti-Spyware Rule Base

The anti-spyware rule library displays all the anti-spyware rules supported by the firewall intrusion prevention feature library.

View Anti-Spyware Rules

Choose “Object > Security Rules > Anti-Spyware Rules” to view the anti-spyware rules.

In the list, you can view the rule ID, name, severity, action and other parameters of the rule.

Search Anti-Spyware Rules

Support searching for the anti-spyware rule based on rule ID and rule name.

Enter the rule ID or rule name in the upper right corner of the “Anti-Spyware Rules” page to perform a fuzzy search. All rules containing this keyword will be searched.

View Rule Details

Click the "View" button under the action to view the detailed information of the rule.

5 Routing

The routing function is a module that must be configured when the device works in routing mode. Without routing, devices cannot forward data.

5.1 Overview

The routing function of the firewall mainly includes static routing, policy routing, ISP routing, dynamic routing, multicast routing and routing monitoring.

5.1.1 Static Route

Static routes are routing entries manually configured by users. If your network environment is not complicated, there are not many routing entries that need to be maintained, and the network environment is fixed and will not change frequently, then adding routing entries through static routing can realize precise manual control of data forwarding. Static routing can sometimes be used as an effective supplement to dynamic routing to create a separate forwarding path for the data you specify.

The traffic flowing out of the firewall can only rely on static routing, not policy routing and ISP routing. For example, when the firewall forwards logs to the log server, the traffic is sent by the firewall itself. Therefore, the user needs to add a static route to the log server to ensure the connectivity between the firewall and the log server.

5.1.2 Dynamic Route

The dynamic routes supported by the firewall include RIP, RIPng, OSPF, OSPFv3, and BGP.

Compared with static routing, dynamic routing is usually used in medium and large network environments. When the network environment is larger and the network segments are more complex, more routing information needs to be maintained. Manual maintenance like static routing adds a lot of work for your administrators. Another obvious problem is that when a link in the network fails, static routing requires your administrator to troubleshoot and adjust the routing. At this time, your network may have been disconnected for a period of time.

The main solution of dynamic routing is to adapt to changes in the network environment and prevent loops. When a link fails, it can be dynamically adjusted. At the same time, by dynamically learning routing information and dynamically maintaining routing tables, the workload of administrators is reduced.

5.2 Static Route

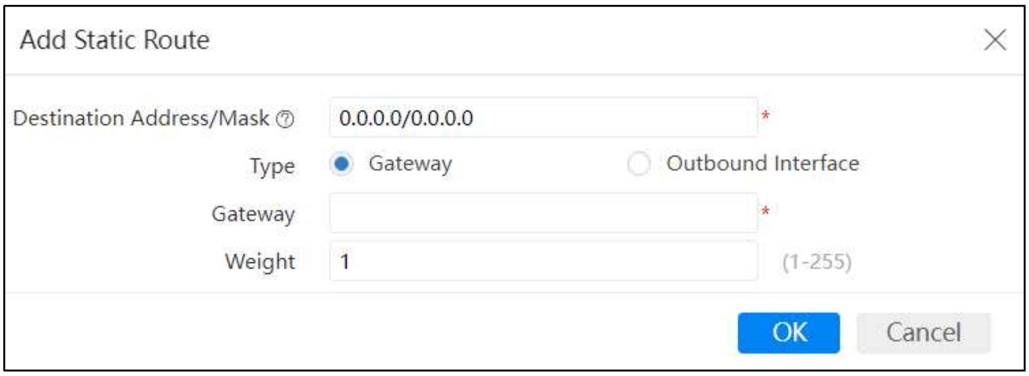
Support adding IPv4 static route and IPv6 static route.

Step 1. Choose "Network > Routing > Static Route".

Step 2. Click “Add”.

Static route is a static routing that specifies the next hop only based on the destination IP address. Among them, up to 32 static routes can be specified to reach the same destination IP address.

Step 3. Configure static routing parameters.



Add Static Route

Destination Address/Mask: 0.0.0.0/0.0.0.0 *

Type: ● Gateway ○ Outbound Interface

Gateway: *

Weight: 1 (1-255)

Parameter	Description
Destination address/mask	Enter the destination network segment, and support the input of IPv4 and IPv6 addresses and masks. • The IPv4 subnet mask supports numbers from 0 to 32 or dotted decimal notation. • The IPv6 subnet mask supports numbers from 0 to 128.
Type	The next hop of a static route can be a gateway or an outgoing interface.
Gateway	"Gateway" is selected as the type. Fill in the next hop IP address. For IPv6, if the user's gateway fills in the Link Local address of the peer device, the user will be required to specify the outgoing interface of the firewall.
Outbound interface	It is configured when the type is selected as “Outbound Interface”. Only the tunnel interface, ADSL interface, and DHCP interface are supported.

Parameter	Description
Weight	Configure the weight of the route. The value range of weight is 1~255. When there are multiple next hops, the data is distributed according to the weight. The greater the weight, the more sessions are allocated and it is the main link.

Step 4. After the configuration is complete, click “OK”.

In the firewall static route list, users can view all static routes on the firewall. You can view the destination address/mask, gateway, outgoing interface, protocol, weight and status of the static route.

The outbound interface is displayed as blackhole, which means that the route is a blackhole route and the egress is unreachable.

Click the “Edit” button to modify the static routing parameters.

5.3 Policy Routing

5.3.1 Add Policy Routing

The firewall provides policy routing function, which supports specifying the next hop address based on the source security domain, source IP address, destination IP address, ISP name, source user, service, application, and other dimensions of the packet. Policy routing supports routing load balancing.

Step 1. Choose “Network > Routing > Policy Route”.

Step 2. Click “Add”, and go to the “Add Policy Route” page.

Step 3. Configure the name and description of the policy route.

The name is the unique identifier of policy route, which is used to distinguish different policy routes.

Step 4. Configure the matching parameters for policy route.

Specify the source security zone, source IP address, destination IP address, ISP name, source user, service, or application that the policy matches. Please configure according to actual needs.

Only when the next hop type is IPv4, you can specify the ISP name referenced by policy routing.

When the user specifies "Destination address" and "ISP name" at the same time, the destination address matched by this policy route is the intersection of the address of the ISP and the address contained in "Destination address".

Step 5. Click “Enable”. Policy route can take effect only after being enabled.

Step 6. (Optional) Configure the load balancing method, next hop type, and next hop gateway.

Load balancing is not performed when there is a single egress, and load balancing does not take effect at this time. When there are multiple egresses, only the best egress interface can be selected through load balancing.

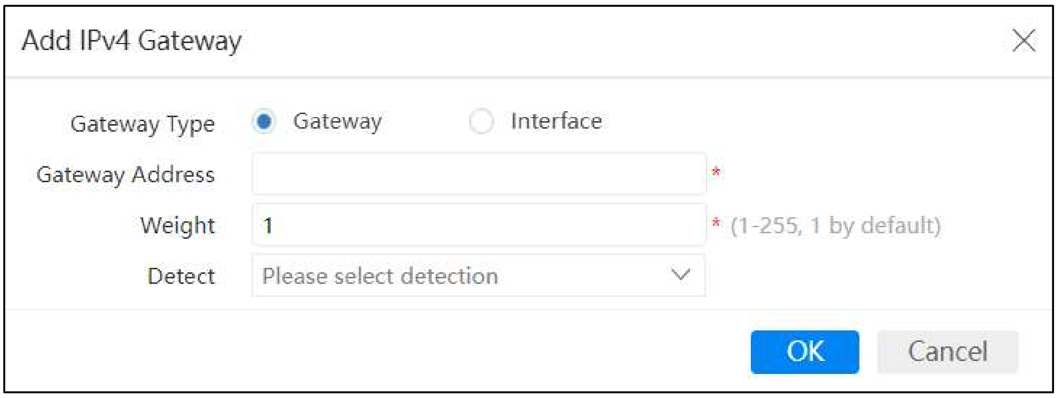
According to the actual situation, configure the load balancing method and the type and parameters of the next gateway.

Parameter	Description
Balance Type	• Source address destination address hash Hash the source address and destination address, and the data packets with the same source address and the same destination address always go out from the same gateway. • Polling The packets that need to be forwarded are allocated to each gateway in turn according to the proportion configured by the weight value. • Source address hash The source address is hashed, and packets with the same source address always go out from the same gateway. Avoid different requests from a client being assigned to different gateways for forwarding. • Destination address hash Check the destination address, and the packets destined for the same destination address always go out from the same gateway. Avoid requests to the same destination address being assigned to different gateways for forwarding. • Source address polling Hash the source address, and the packets with the same source address always go out from the same gateway. At the same time, different source addresses are assigned to each gateway in turn according to the proportion configured by the weight value. • Backup When there are multiple gateways, the gateways are selected according to the priority from high to low. When the link with higher priority fails, the link with lower priority is selected, and so on. When the gateway with a higher priority resumes communication, switch back to the gateway with a higher priority. Under the same priority, when there are multiple gateways, the primary link is composed of multiple outbound interface polling. When all outgoing interfaces on the primary link fail, switch to the standby link. • Optimal Link Bandwidth Load While specifying the gateway address, you also need to specify the corresponding bandwidth of the gateway. The bandwidth of the gateway is mainly based on the size of the egress bandwidth. The egress with the largest bandwidth will be selected by the firewall as the optimal link. • Optimal Link Bandwidth Backup While specifying the gateway address, you also need to specify the

Parameter	Description
	corresponding bandwidth of the gateway. The bandwidth of the gateway is mainly based on the size of the egress bandwidth. When creating a new session and entering the firewall, the link with the largest remaining bandwidth will be selected for forwarding based on the comparison of the remaining bandwidth of each current gateway. • random When there are multiple gateways, one of the gateways is randomly selected for forwarding. Maps to a polling algorithm with equal weight values. • traffic balance If a simple polling or random balancing algorithm is used, the amount of traffic carried by each outgoing interface may be greatly different, and such a result will not achieve true load balancing. The traffic balancing algorithm has a data record for each outgoing interface with load. The content of the record is the load traffic size of the current outgoing interface. When a new packet is forwarded, the packet will be distributed to the node with the least traffic load. Make the balance more in line with the actual situation, and the load is more balanced. • Delay load The delay load will select the egress with the smallest delay among multiple gateways for forwarding according to the delay time fed back by the detection result. • Hop load The hop count load will select multiple gateways with the smallest hop count for forwarding based on the hop count returned by the detection result.
Next hop type	Select the next hop type according to the network type. The next type supports IPv4 and IPv6. When IPv4 is selected, the source address and destination address of the policy routing that references the basic gateway must also be IPv4 addresses. When IPv6 is selected, the source address and destination address of the policy routing that references the basic gateway must also be IPv6 addresses.

Different balancing modes require different gateway parameters to be set, as described below:

- When the balance mode is source address destination address hash, source address hash, polling, source address polling, and destination address hash, add an IPv4 or IPv6 gateway.



Add IPv4 Gateway

Gateway Type ● Gateway ○ Interface

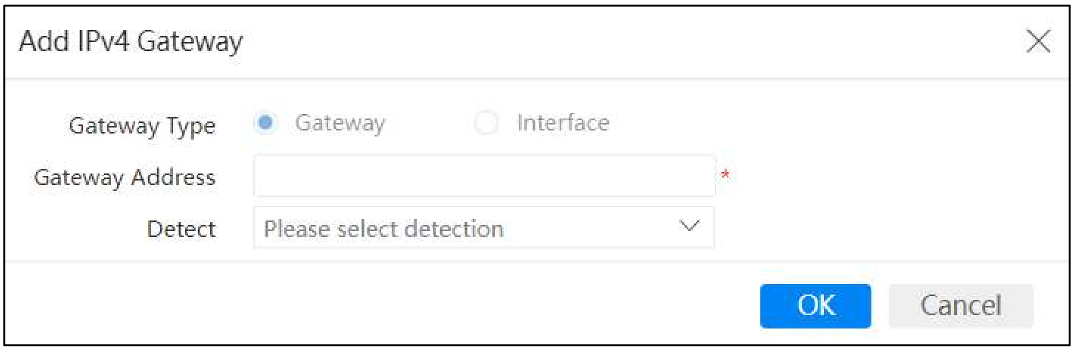
Gateway Address *

Weight 1 * (1-255, 1 by default)

Detect Please select detection

Parameter	Description
Gateway type	The gateway type supports two types: "gateway" and "interface".
Gateway address	When selecting a gateway, you need to fill in the next-hop IP address. When the gateway address is filled with the IPv6 Link Local address, the user needs to specify the outbound interface.
Gateway interface	When selecting an interface, only the tunnel interface and ADSL interface can be selected as the outbound interface.
Weight	The value range of weight is 1~255. When there are multiple next hops, the data is distributed according to the weight. The greater the weight, the more sessions are allocated and it is the primary link.
detection	The detection function needs to select the link health check for detection.

- When the balance mode is delay load or hop load, add an IPv4 or IPv6 gateway.



Add IPv4 Gateway

Gateway Type ● Gateway ○ Interface

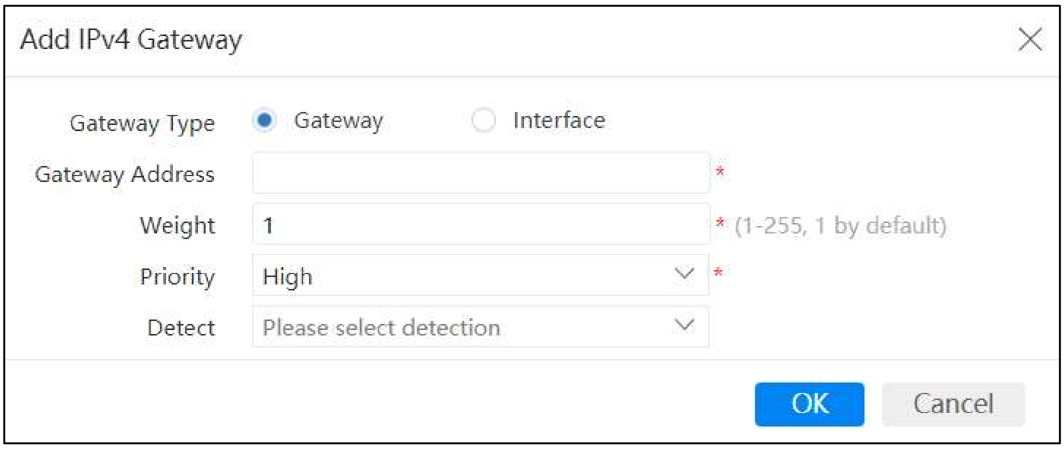
Gateway Address *

Detect Please select detection

Parameter	Description
Gateway type	Gateway type only supports "Gateway".

Parameter	Description
Gateway address	When selecting a gateway, you need to fill in the next-hop IP address. When the gateway address is filled with the IPv6 Link Local address, the user needs to specify the outbound interface.
Detection	The detection function needs to select the link health check for detection.

- When the balancing method is backup, add an IPv4 or IPv6 gateway.



Add IPv4 Gateway

Gateway Type ● Gateway ○ Interface

Gateway Address *

Weight 1 * (1-255, 1 by default)

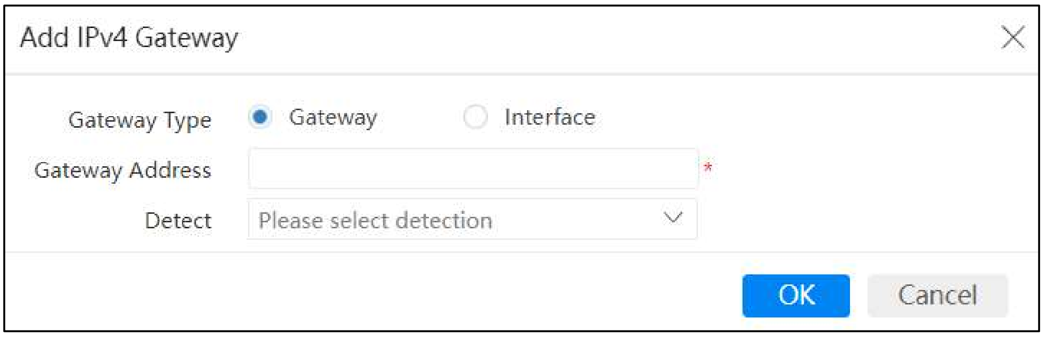
Priority High *

Detect Please select detection

Parameter	Description
Gateway type	The gateway type supports two types: "gateway" and "interface".
Gateway address	When selecting a gateway, you need to fill in the next-hop IP address. When the gateway address is filled with the IPv6 Link Local address, the user needs to specify the outbound interface.
Gateway interface	When selecting an interface, only the tunnel interface and ADSL interface can be selected as the outbound interface.
Weight	The value range of weight is 1~255. When there are multiple next hops, the data is distributed according to the weight. The greater the weight, the more sessions are allocated and it is the primary link.

Parameter	Description
Priority	Priority is divided into "high", "medium", "low" this level. When there are multiple gateways, the gateways are selected according to the priority from high to low. When the link with higher priority fails, the link with lower priority is selected, and so on. Under the same priority, when there are multiple gateways, the primary link is composed of multiple outbound interface polls. When all outgoing interfaces on the primary link fail, switch to the standby link. When there are multiple gateways under the same priority of the back algorithm, the polling algorithm is still used.
Detection	The detection function needs to select the link health check for detection.

- When the balance method is random and traffic balance, add an IPv4 or IPv6 gateway.



Add IPv4 Gateway

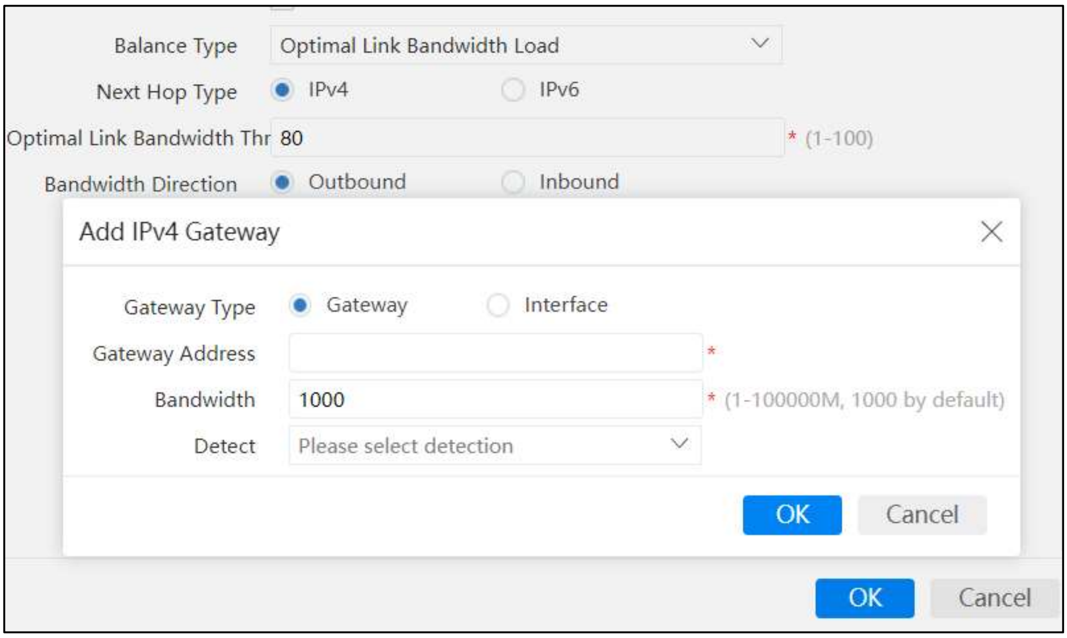
Gateway Type ● Gateway ○ Interface

Gateway Address *

Detect Please select detection

Parameter	Description
Gateway type	The gateway type supports two types: "gateway" and "interface".
Gateway address	When selecting a gateway, you need to fill in the next-hop IP address. When the gateway address is filled with the IPv6 Link Local address, the user needs to specify the outbound interface.
Interface	When selecting an interface, only the tunnel interface and ADSL interface can be selected as the outbound interface.
Detect	The detection function needs to select the link health check for detection.

- When the balancing mode is optimal link bandwidth load and optimal link bandwidth backup, configure the optimal link bandwidth threshold and bandwidth direction, and add a gateway.


Balance Type: Optimal Link Bandwidth Load

Next Hop Type: ● IPv4 ○ IPv6

Optimal Link Bandwidth Thr: 80 * (1-100)

Bandwidth Direction: ● Outbound ○ Inbound

Add IPv4 Gateway

Gateway Type: ● Gateway ○ Interface

Gateway Address: *

Bandwidth: 1000 * (1-100000M, 1000 by default)

Detect: Please select detection

Parameter	Description
Optimal Link Bandwidth Threshold	The optimal link bandwidth utilization rate, in percentage, is the trigger value of the optimal link bandwidth load algorithm. When the bandwidth of the optimal link drops to 80% of the threshold, the newly created session will be forwarded to the optimal link again without load until the bandwidth of the optimal link reaches the specified threshold again. For example, if the optimal link bandwidth is 1000M, and another optimal link bandwidth is 200M, set the optimal link bandwidth threshold to 80%. When the bandwidth used by the optimal link does not reach 800M, that is, before it reaches 80%, all sessions are forwarded through the optimal link. When the bandwidth used by the optimal link reaches or exceeds 80%, the firewall will compare the remaining bandwidth of the optimal link with the remaining bandwidth of the suboptimal link, and use the source-based address hashes are used to load. When the bandwidth of the optimal link drops to 80% of the bandwidth threshold of the optimal link, that is, 80%*80%=64%, the new session will no longer be loaded, and all the sessions will be forwarded by the optimal link until the optimal link bandwidth is again at 80%.
Bandwidth direction	Bandwidth is divided into "uplink" and "downlink" bandwidth.
Gateway type	The gateway type supports two types: "gateway" and "interface".
Gateway address	When selecting a gateway, you need to fill in the next-hop IP address. When the gateway address is filled with the IPv6 Link Local address, the user needs to specify the outbound interface.

Parameter	Description
Interface	When selecting an interface, only the tunnel interface and ADSL interface can be selected as the outbound interface.
Bandwidth	Set the link bandwidth size, the value range is 1~100,000M.
Detect	The detection function needs to select the link health check for detection.

Step 7. After the configuration is complete, click “OK”.

The added policy routes are displayed in the policy route list. You can view the name, source security zone, source address, destination address, service, application, gateway, balancing method, type, number of hits, whether enabled or not, etc. of policy routing.

You can modify, delete, adjust the order, clear the number of hits, query and other operations on the policy route in the list.

Policy route supports advanced query by specifying source IP address, destination IP address, source port, destination port and protocol number.

5.3.2 Adjust Policy Route Order

The policy route in the policy routing list determines the priority of policy routing. The higher the position in the list, the higher the priority. The policy route with higher priority is matched first.

Step 1. Choose “Network > Routing > Policy Route”.

Step 2. In the policy route list, select the policy route whose order needs to be adjusted.

Step 3. Click “Reorder”.

Step 4. Choose a direction and destination.

Parameter	Description
Source location	The name of the policy route to reorder.
Direction	Direction supports "top", "before", "after" and "end". • "Top" puts the policy route to the top, and it is the most preferred matching in the policy route list. • "Before" put this policy route before a certain policy route, and the user needs to specify the specific name of a certain policy route. • "After" put this policy route after a certain policy route, and the user needs to specify the specific name of a certain policy route. • "End" puts this policy route at the end, and it is the last matching in the policy route list.

Parameter	Description
Destination location	The name of the policy route as a "before" or "after" reference.

Step 5. After the configuration is complete, click “OK”.

5.3.3 Set Displayed Policy Route Parameters

By default, the "Description" and "Source zone" parameters are not displayed in the policy routing list. Users can click ⋮ on the left side of the policy route list to select the parameters to be displayed. Select the check box corresponding to the parameter to display the parameter, and uncheck the check box corresponding to the parameter to not display the parameter.

5.3.4 Add ISP Route

The firewall supports the ISP information database, which stores the destination IP addresses of operators such as China Telecom, China Unicom, China Mobile, and Education Network. By directly specifying the operator name in the ISP route, the IP address of the corresponding operator can be accessed through the egress links of different operators.

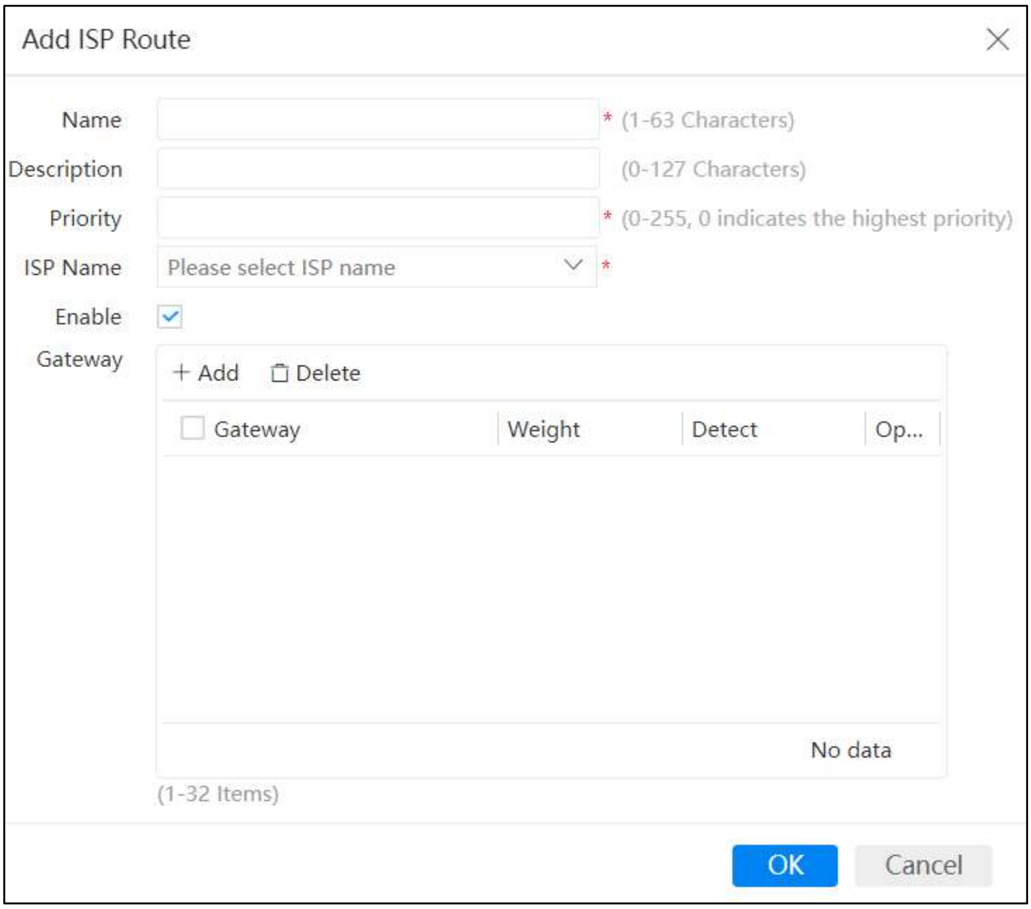
If you need to specify parameters such as source security zone and source address, please select to configure in Policy Route, and you can also specify the ISP name in Policy Route.

Step 1. Choose “Network > Routing > Policy Route”.

Step 2. Click the “ISP Route” tab.

Step 3. Click “Add”.

Step 4. Configure the policy route parameters.



Add ISP Route

Name * (1-63 Characters)

Description (0-127 Characters)

Priority * (0-255, 0 indicates the highest priority)

ISP Name: Please select ISP name *

Enable ☑

Gateway

Parameter	Description
Name	The name of the ISP route.
Description	Add the necessary descriptive information.
Priority	The smaller the value, the higher the priority. 0 means the highest priority.
ISP Name	The resource defined in the ISP information base is the destination address in the ISP route. Displayed as the name of the operator, such as China Mobile, China Unicom, unknown, etc.
Enable	Select " Enable ", and the ISP route will take effect. If " Enable " is not selected, the ISP route will not take effect.
Add gateway	Configure the weight of the route. The next hop is the address of the peer gateway interface connected to the outgoing interface. When there are multiple next hops, the data is distributed according to the weight. The greater the weight, the more sessions are allocated and it is the primary link.

Step 5. After the configuration is complete, click “OK”.

The configured ISP routing information is displayed in the ISP route category. You can view the name of the ISP route, ISP name, gateway, priority, number of hits, whether it is enabled, etc.

You can modify, delete, clear the number of hits, query and other operations on the ISP route.

5.3.5 Set Displayed ISP Route Parameters

Users can click ⋮ on the left side of the ISP list to select the parameters to be displayed. Select the check box corresponding to the parameter to display the parameter, and uncheck the check box corresponding to the parameter to not display the parameter.

5.3.6 Maintain ISP Information

By default, the firewall provides the ISP information of China Telecom, China Unicom, China Mobile, and Education Network. As the operator's address range expands over time, the ISP information provided by default may have incomplete addresses after a period of use, and users can update it regularly by themselves.

Users can maintain the ISP information of the four operators by importing and exporting ISP information.

Users can fill in the ISP information of four operators in one form, and the imported ISP information format only supports the format of IP/mask, such as 103.20.112.0/255.255.252.0. In order to facilitate users to modify and maintain ISP information, it is recommended that users export the template before editing and importing it. The imported ISP information only supports UTF-8 encoding format.

When customizing the ISP information template, the ISP information that does not indicate that it belongs to China Telecom, China Unicom, China Mobile, and Education Network will be classified as "unknown" ISP information.

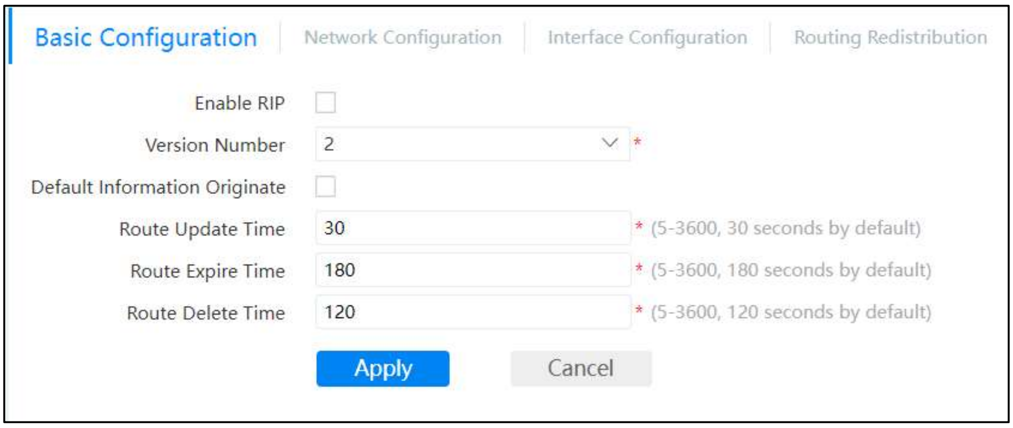
5.4 RIP

RIP (Routing Information Protocol) is an interior gateway routing protocol that exchanges routing information between routers. Routers can dynamically adapt to changes in network connections by constantly exchanging information, including which networks each router can reach, how far these networks are, and so on. RIP belongs to the network layer protocol and uses UDP as the transport protocol.

RIP is mostly used in a network environment with a smaller scale and a simpler structure. RIP uses hop counts to measure the distance to a destination address. Currently, the firewall supports two versions of RIPv1 and RIPv2.

Step 1. Choose "Network > Routing > RIP".

Step 2. Configure basic configuration parameters, and click “Apply” after the configuration is complete.



Enable RIP □

Version Number 2 *

Default Information Originate □

Route Update Time 30 * (5-3600, 30 seconds by default)

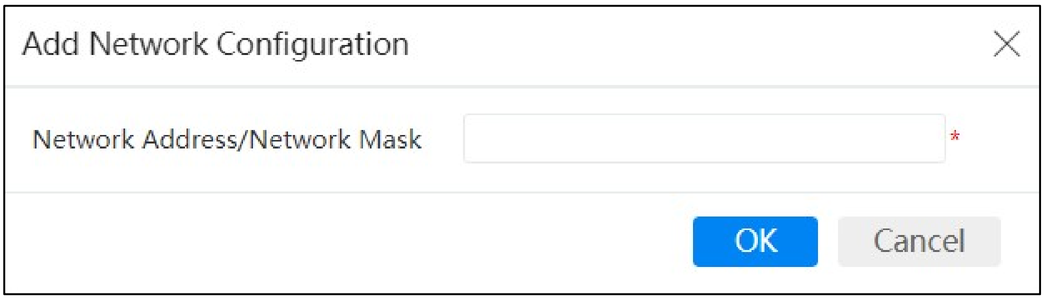
Route Expire Time 180 * (5-3600, 180 seconds by default)

Route Delete Time 120 * (5-3600, 120 seconds by default)

Parameter	Description
Enable RIP	The RIP function can take effect after RIP is enabled.
Version number	The default is RIPv2 version. Both RIPv1 and RIPv2 versions are supported. RIPv1 is a classful routing protocol. RIPv1 protocol packets do not carry mask information, and can only identify routes on natural network segments such as classes A, B, and C. RIPv2 is an optimized version of RIPv1. RIPv2 is a classless routing protocol. RIPv2 packets carry mask information.
Default information originate	Enabled, advertise the default route. If not enabled, the default route will not be advertised.
Route update time	The update time of the RIP route, the default is 30 seconds to update. Support customizing, and the range is 5 ~ 3600 seconds.
Route expire time	The expiration time of the RIP route, the default is 180 seconds. If a RIP route is not updated within 180 seconds, the RIP route will be invalidated. Support customizing, and the range is 5~3600 seconds.

Parameter	Description
Route delete time	The clear time of the RIP route, the default is 120 seconds. If an invalid RIP route is not updated within 120 seconds, the RIP routing table will be cleared. Support customizing, and the range is 5~3600 seconds.

Step 3. Click “Network Configuration”, click “Add”, and add the network to be published.



Add Network Configuration

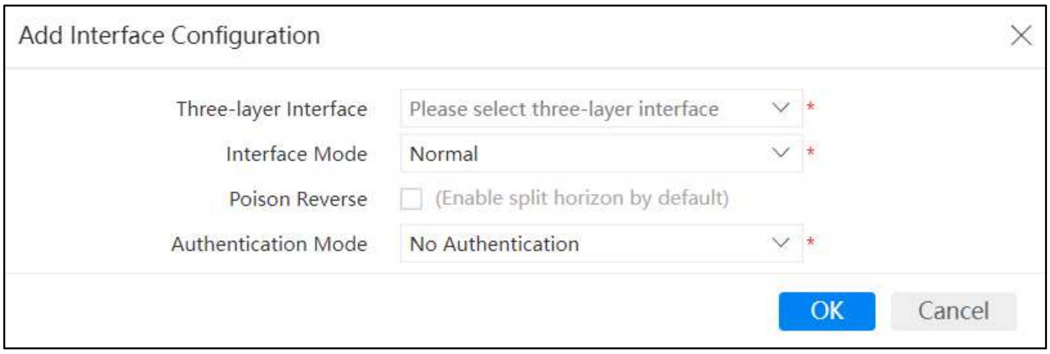
Network Address/Network Mask *

Users can specify multiple networks that need to be published.

Parameter	Description
Network address/Netmask	The IP address that needs to be released through RIP/the mask corresponding to the IP address that needs to be released, *such as:* *10.1.1.0/16* *172.16.1.0/255.255.0.0*

Step 4. Add interfaces.

The interface configuration provides the selection of RIP function interface, interface mode, and authentication mode. At the same time, the user can choose to enable or disable the interface split horizon function. The interface with the split horizon function enabled will not send the routes learned from the interface to avoid loops.



Add Interface Configuration

Three-layer Interface: Please select three-layer interface *

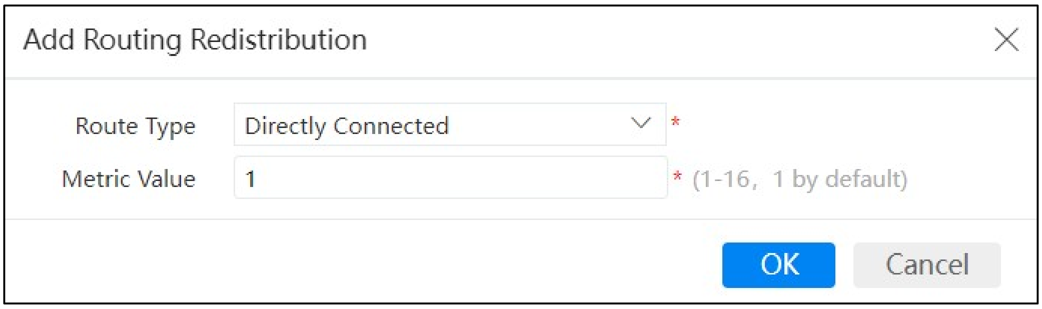
Interface Mode: Normal *

Poison Reverse: □ (Enable split horizon by default)

Authentication Mode: No Authentication *

Parameter	Description
L3 interface	Select the interface to advertise RIP.
Interface mode	Select the working mode of the interface. • Normal: Receive and send RIP updates. • Passive: Receive but do not send RIP updates.
Poison Reverse	Poison reverse means sending out a routing entry with a metric value of 16 hops (infinity), which is used to inform other routers that this route is no longer reachable. If the poison reverse function is enabled, the firewall will send the routing entry received from an interface, and then send it out through this interface, but the metric value is set to 16 hops (infinity). If the poison reverse function is not selected, the firewall enables split horizon by default, and the routing entries received from an interface will not be sent out from this interface.
Authentication mode	• No Authentication: The interface does not enable the authentication function. • Plaintext: Authentication information is transmitted in plaintext. • MD5: The authentication information is transmitted after MD5 verification.
Authentication password and authentication password confirmation	When the authentication mode is "plain text" or "MD 5 ", you need to configure the authentication password and confirm the authentication password again.

Step 5.Add route redistribution.



Add Routing Redistribution

Route Type: Directly Connected *

Metric Value: 1 * (1-16，1 by default)

The RIP protocol allows users to import the routing information of other routing protocols on the device into RIP and publish it to the outside. The route redistribution function is to realize the redistribution of the user-specified type of route to RIP and distribute it to the outside. Users can specify to redistribute direct routes, static routes, OSPF routes, and BGP routes. At the same time, during the process of redistributing routes, users can specify the metric value of redistributed routes. By default, the metric value is 1. A route with a larger metric value has a lower priority, and a RIP route with a metric value of 16 is considered unreachable.

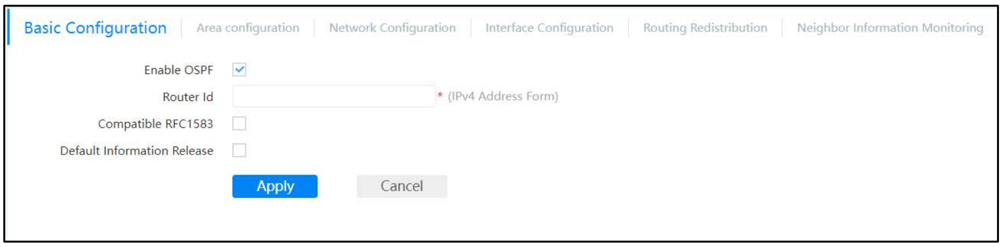
5.5 OSPF

OSPF (Open Shortest Path First) is an interior gateway routing protocol based on link state. OSPF is suitable for networks of various scales. It establishes a link state database by announcing the state of the network interface and generates a shortest path tree. Each device with OSPF enabled uses these shortest paths to construct a routing table. At the same time, convergence can be completed quickly after the network topology changes, reducing route flapping, and the OSPF protocol will not generate routing loops. It is a widely used dynamic routing protocol at present.

The firewall supports OSPFv2, which corresponds to RFC 2328, and uses multicast to transmit routing information.

Step 1. Choose "Network > Routing > OSPF".

Step 2. Configure basic configuration parameters, and click “Apply” after the configuration is complete.



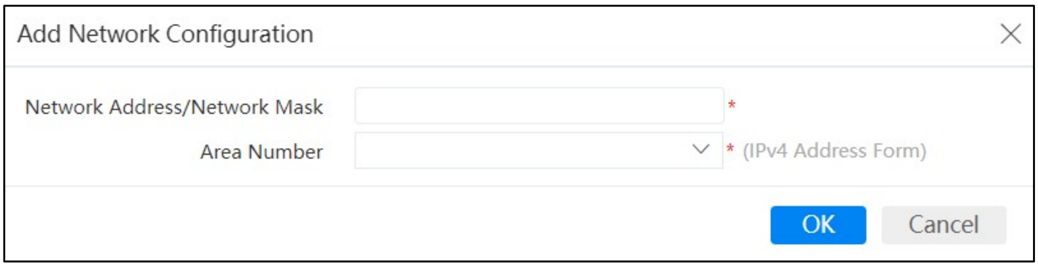
Enable OSPF ☑
Router Id * (IPv4 Address Form)
Compatible RFC1583 □
Default Information Release □

Parameter	Description
Enable OSPF	Select Enable OSPF to make OSPF take effect. Otherwise, the OSPF configuration does not take effect.
Router Id	The user needs to specify the Router Id of the firewall, and the Router ID must be unique within the same autonomous system.
Compatible RFC1583	Check the box to enable RFC1583 compliance.
Default information release	If there are active default routes other than the OSPF process in the routing table, you need to enable the advertisement of default information. After the default information advertisement is enabled, the default route will be advertised to the OSPF domain. If there is no default route, the default information will not be advertised.

Parameter	Description
Always unconditionally generated	After enabling default information releasing, select the "Always unconditionally generated" check box, no matter whether there is a default route in the routing table of the current router, a Type-5 LSA describing the default route can be generated and published.
Metric type	There are currently two types of metrics: ext-1 and ext-2, and ext-2 is selected by default.
Metric value	Customizing is supported, the default is 20, and the range is 1-1800.

Step 3. Click “Network Configuration”, click “Add”, and add the network to be published.

Users can specify multiple networks that need to be published.



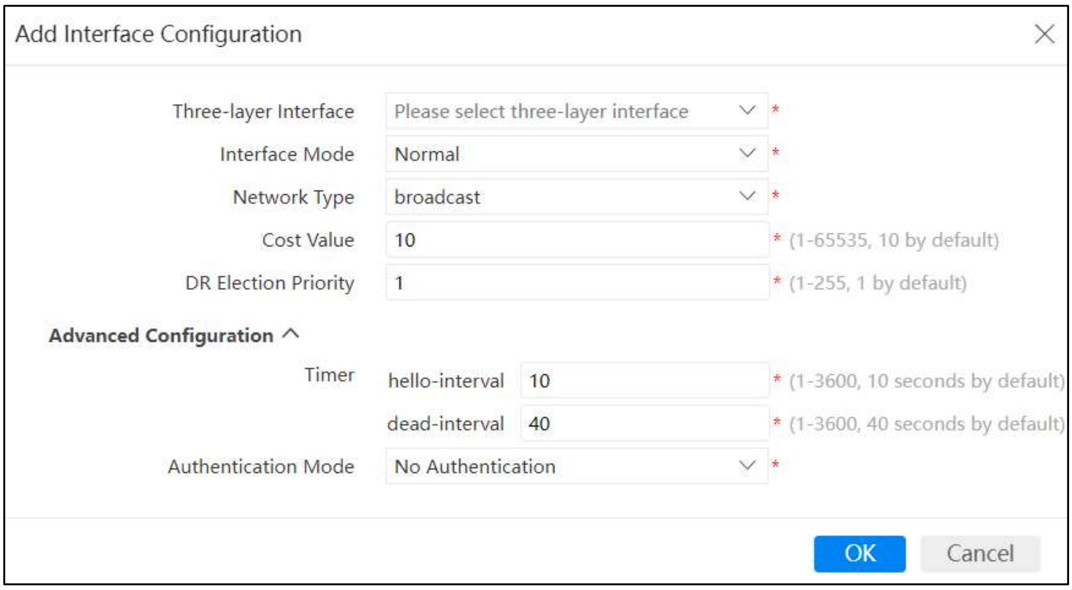
Add Network Configuration

Network Address/Network Mask *

Area Number * (IPv4 Address Form)

Parameter	Description
Network address/Netmask	The IP address to be advertised by OSPF/the mask corresponding to the IP address to be advertised. *like:* *10.1.1.0/16* *172.16.1.0/255.255.0.0*
Area Number	Users can specify the type of the area code as an IPv4 address.

Step 4. Click “Interface Configuration”, click “Add” to add interface configuration.



Add Interface Configuration

Three-layer Interface: Please select three-layer interface *

Interface Mode: Normal *

Network Type: broadcast *

Cost Value: 10 * (1-65535, 10 by default)

DR Election Priority: 1 * (1-255, 1 by default)

Advanced Configuration

Timer: hello-interval 10 * (1-3600, 10 seconds by default)

dead-interval 40 * (1-3600, 40 seconds by default)

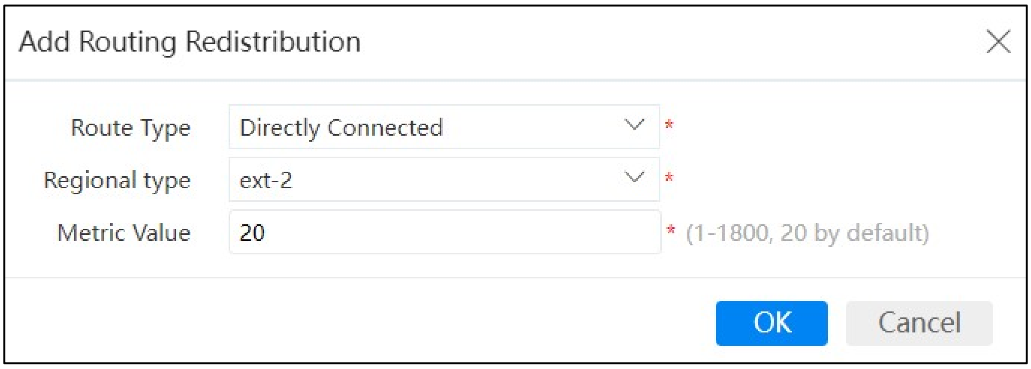
Authentication Mode: No Authentication *

Parameter	Description
L3 interface	Select the interface on which OSPF is enabled. It must work in the L3 mode.
Interface mode	Select the working mode of the interface. ● "Normal" mode can receive and send OSPF packets. ● "Passive" mode prohibits receiving and sending OSPF packets.
Network type	Select a network type. ● " broadcast " broadcast type. ● "point -point " point-to-point type.
Cost value	Cost value of the interface. The default is 10, support customizing, and the range is 1-65535.
DR election priority	This item needs to be configured when "Network Type" is "Broadcast". The priority of the interface when the DR is elected. The default is 1, support customizing, and the range is 0-255. Setting the priority to 0 means that the interface does not participate in DR election. DR election priority can affect the selection of DR/BDR in the network. The larger the value of the DR priority, the higher the priority. Select the priority of the interface. The larger the priority, the higher the priority. It is selected as the DR. The second priority is selected as the BDR. When the DR election priorities of the interfaces are equal, the router ID with a larger router ID takes precedence.

Parameter	Description
Timer	hello-interval: The interval of the neighbor detection hello packet, the default is 10 seconds, support customizing, and the range is 1-3600. dead-interval: neighbor dead timeout, the default is 40 seconds, if no neighbor is detected within 40 seconds, the neighbor will be invalid. Support customizing, and the range is 1-3600.
Authentication mode	• "No authentication", the interface does not enable the authentication function. • "Plain text", the authentication information is transmitted in plain text, requiring the user to specify the authentication password. • "MD5" authentication information is transmitted after MD5 verification, and the user needs to specify the authentication password.

Step 5. Click “Route Redistribution”, and click “Add” to add route redistribution.

OSPF protocol allows users to import the routing information of other routing protocols on the device into OSPF and advertise it to the outside. The route redistribution function is to implement the redistribution of user-specified routes into OSPF and advertise them to the outside world.



Add Routing Redistribution

Route Type: Directly Connected *

Regional type: ext-2 *

Metric Value: 20 * (1-1800, 20 by default)

Parameter	Description
Route type	Users can specify the route type of redistribution, there are four types in total: Direct route, static route, RIP route, BGP route.
Metric type	There are currently two types of metrics: ext-1 and ext-2, and ext-2 is selected by default.
Metric	Support customizing, the default is 20, and the range is 1-1800.

Step 6. Click “Neighbor Information Monitoring”.

Neighbor information monitoring is used to view OSPF neighbor status, neighbor address and other information. Neighbor information is the main source of information for monitoring, debugging OSPF, and troubleshooting OSPF problems.

Table 5-1 Description of neighbor monitoring information interface

Parameter	**Description**
Neighbor ID	The ID of the neighbor.
Priority	The priority of the neighbor.
Status	Neighbor Status/Neighbor Role **Status:** **down,** no hello packets from neighbors are received, but hello packets can be sent. **init,** the hello packet sent by the neighbor has been received. **two-way,** the firewall establishes a bi-directional relationship with the neighbor. **exstart,** when the link type is a broadcast network, before exchanging DBD, elect the master and slave. **exchange,** exchange DBD. **loading,** exchange LSAs. **full,** the adjacency relationship is established.
Failure time	The amount of time after which the current neighbor will expire.
Neighbor address	The neighbor's address, usually an IP address.
Local interface	The format is interface name [interface address], indicating from which interface the firewall establishes a neighbor relationship with the neighbor.

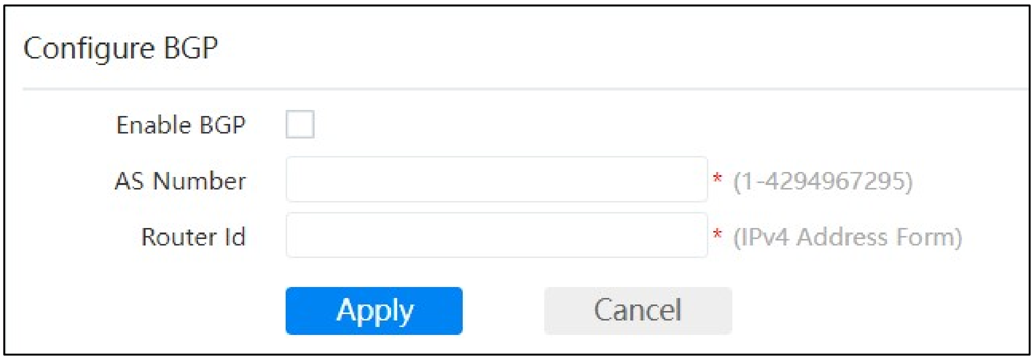
5.6 BGP

BGP (Border Gateway Protocol) is an autonomous system routing protocol running on TCP. BGP is the only protocol used to deal with a network as large as the Internet, and it is also the only protocol that can properly handle multiple connections between unrelated routing domains. The main function of the BGP system is to exchange network reachability information with other BGP systems. The network reachability information includes the listed autonomous systems (AS) information. These information effectively construct the topology of AS interconnection and thus eliminate routing loops, and at the same time, policy decisions can be implemented at the AS level. BGP uses TCP for protocol packet transmission, its port number is 179, and it supports classless inter-domain routing. When BGP runs between autonomous systems, it is EBGP, and when BGP runs within autonomous systems, it is IGBP.

The BGP protocol on the firewall supports routing IPv4 networks and routing IPv6 networks.

Step 1. Choose "Network > Routing > BGP".

Step 2. Configure basic configuration parameters, and click “Apply” after the configuration is complete.


Configure BGP

Enable BGP □

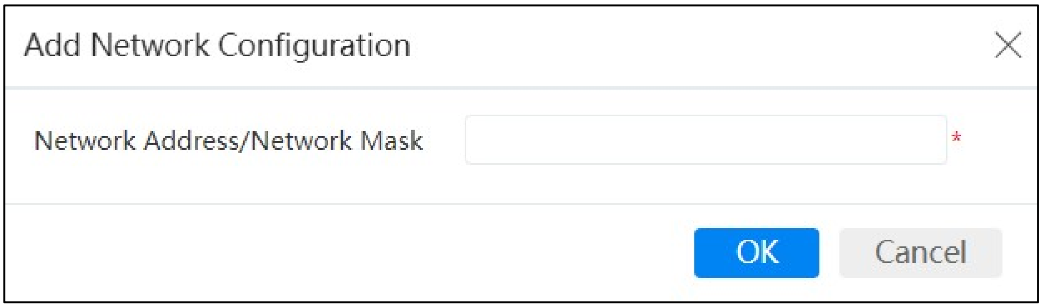
AS Number * (1-4294967295)

Router Id * (IPv4 Address Form)

Parameter	Description
Enable BGP	Check the box to enable the BGP function. Otherwise, the BGP configuration does not take effect.
AS number	The user needs to specify the BGP autonomous system AS number of the firewall, and the AS number in the same autonomous system is the same.
Route ID	In the entire BGP domain, the Route ID must be unique.

Step 3. On the “Network Configuration” page, click “Add” to add the network to be published.

Network configuration is used to specify a certain network to be advertised to BGP. Users can specify multiple networks that need to be published.

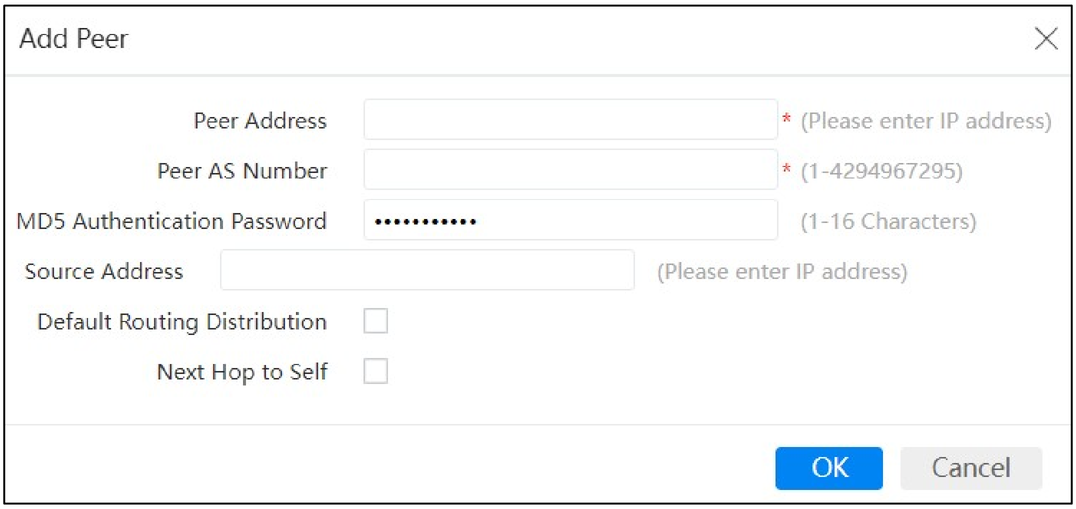

Add Network Configuration

Network Address/Network Mask *

Parameter	Description
Network address/Netmask	The addresses that need to be advertised via BGP. The IPv4 network address and corresponding mask or IPv6 network address and corresponding prefix to be published. *like:* *10.1.1.0/16* *172.16.1.0/255.255.0.0* *2002::1000/128*

Step 4. Click the “Peer” tab, click “Add”, and configure peer parameters.

Peers are BGP neighbors. Once a BGP neighbor is established, the firewall will advertise all optimal routes to its neighbors.



Add Peer

Peer Address: * (Please enter IP address)

Peer AS Number: * (1-4294967295)

MD5 Authentication Password: ••••••••••• (1-16 Characters)

Source Address: (Please enter IP address)

Default Routing Distribution □

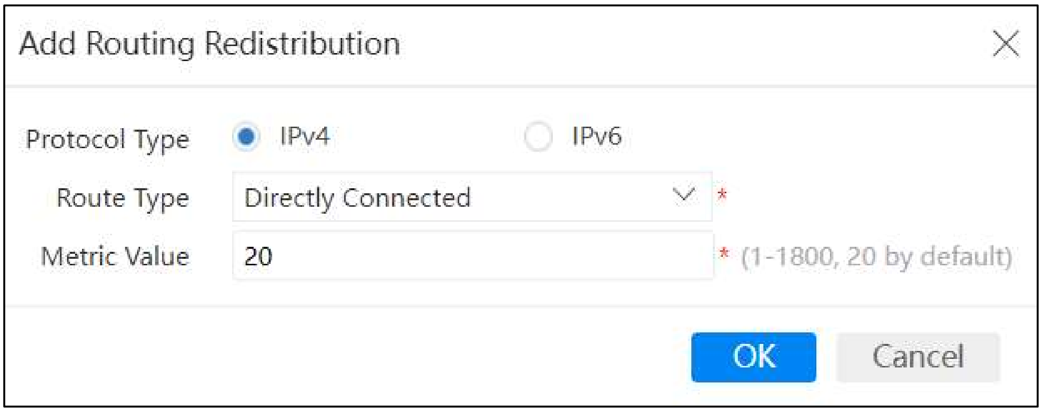
Next Hop to Self □

Parameter	Description
Peer address	Specify the peer address, and support IPv4 and IPv6 peer addresses.
Peer AS number	Specify the AS number of the peer.
MD5 authentication password	If you need to enable BGP neighbor authentication, you need to specify the MD5 authentication password, and the BGP peer must also enable neighbor authentication and specify the same authentication MD5 password. Otherwise, the neighbor relationship will fail to be established; If not enabled, this item is empty.
Source address	Specify the source IP for initiating a BGP connection. When there are multiple IP addresses on the interface, specify the source IP to avoid inconsistency between the source IP that initiates the connection and the peer address configured on the peer end.

Parameter	Description
Default routing distribution	Users can choose whether to enable the sending function of the default route.
Next hop to Self	If the firewall is in the position of EBGP, when advertising the route to its IBGP, you need to check "Next hop to itself". Users need to select based on their own network environment.

Step 5. Click the "Route Redistribution" tab, and click "Add".

The BGP protocol allows users to import the routing information of other routing protocols on the device into BGP and advertise it to the outside. The route redistribution function is to realize the redistribution of the user-specified type of route to BGP and advertise it to the outside.



Add Routing Redistribution

Protocol Type ● IPv4 ○ IPv6

Route Type: Directly Connected *

Metric Value: 20 * (1-1800, 20 by default)

Parameter	Description
Protocol type	Users can specify the protocol type for redistribution: IPv4 or IPv6 type.
Route type	Users can specify the route type of redistribution, there are four types in total: Direct route, static route, RIP route (RIPng route), OSPF route (OSPFv3 route).
Metric value	Users can specify the metric value of the redistribution route, and the default metric value is 20. The range is 1-1800, and the smaller the value, the higher the priority.

5.7 Static Multicast Routing

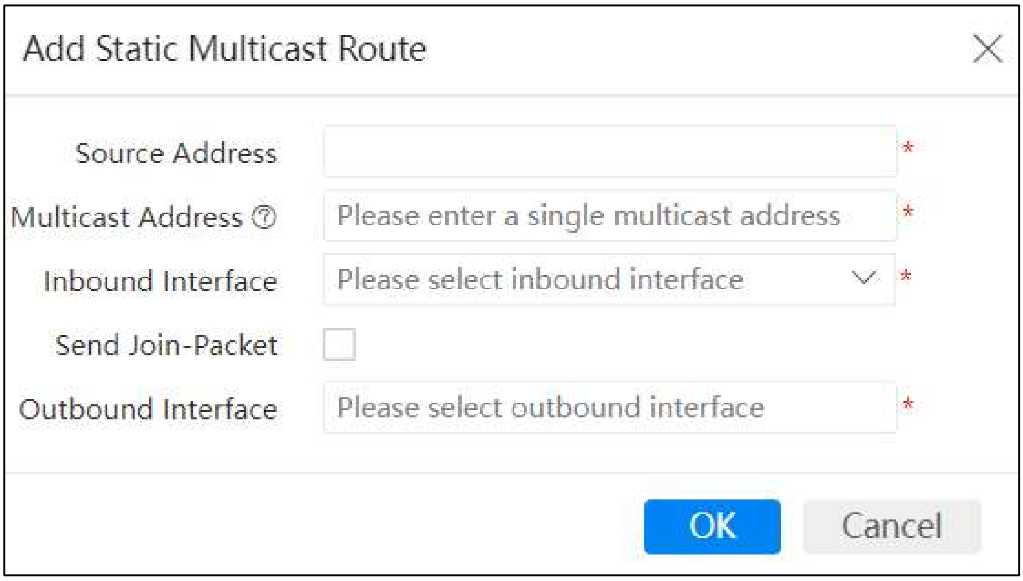
When the same data needs to be sent to multiple hosts, although unicast can be used across routers, it is impractical to send the same data multiple times; while using broadcast only needs to send data once, so that every host in the network must receive data, and the data cannot pass through the router, causing the remote network not to receive the data, so it is not feasible. Considering these factors, a new data transmission method has been developed, which combines the advantages of unicast and broadcast, that is, after a piece of data is sent, such data can be received by multiple hosts at the same time, and the data can pass through routers and be routed to remote networks. Such data is multicast. Therefore, after multicast data is sent out, it can only be received by a specific set of hosts, and the hosts that do not want to receive cannot receive it. The multicast can also be forwarded to the remote network by the router, provided that the router must enable the multicast function. In multicasting, we call the hosts that want to receive the multicast as group members.

Step 1. Choose "Network > Routing > Static Multicast Route".

Step 2. Click “Add”.

Support adding multiple static multicast routes, and the maximum limit is 448.

Step 3. Configure static multicast routing parameters.


Add Static Multicast Route

Source Address *

Multicast Address ⓘ Please enter a single multicast address *

Inbound Interface Please select inbound interface *

Send Join-Packet □

Outbound Interface Please select outbound interface *

Parameter	Description
Source address	The outbound interface address of the sender of the multicast route, which is a unicast address.
Multicast address	The multicast address used by the multicast group. The multicast address range is 224.0.0.0 ~239.255.255.255.

Parameter	Description
Inbound interface	The interface through which the multicast route flows into the firewall.
Send join-packet	If the check box is selected, the firewall will actively send IGMP join messages to the multicast group.
Outbound interface	The interface on which the multicast route exits the firewall. Multiple outbound interfaces can be added, and the maximum limit is 16.

Step 4. After the configuration is complete, click “OK”.

Static multicast routes are shown in the list of multicast routes. You can view the source address, multicast address, ingress interface, egress interface list of the route, and whether to send a join message. The operations such as modifying and deleting multicast routes can be performed.

Step 5. Select the "Enable Multicast Route" checkbox above the multicast routing list to enable the multicast routing function. Otherwise, the multicast routing configuration will not take effect.

5.8 Dynamic Multicast Route

The firewall provides dynamic multicast routing protocols in PIM-SM mode. Before users add dynamic multicast routing protocols, we need to explain the following terms to you to help you better configure dynamic multicast routing.

RP: In PIM-SM mode, due to the method used to record multicast information, it does not care about the multicast source address, so the router does not know what the IP address of the multicast sender is, so it cannot complete the reverse path detection. In this case, PIM-SM selects a multicast convergence point in the network, that is, Rendezvous Point (RP). RP is the core of the multicast network. The sender uniformly sends multicast data to the RP, and then the RP sends the data to the receiver. This means that the data received by the receiver is forwarded by the RP, and the router considers the address of the RP to be the IP address of the multicast source.

DR: In a PIM network, the real source needs to send a registration message to the RP to announce its existence, while sending a registration message is done by the DR in a multi-access network. When the real source sends the first multicast packet to RP, DR encapsulates this packet in unicast and sends it to RP, which is called registration. The sent registration message will establish a source tree from the DR to the RP. In this way, the source tree created from the source to the RP can help avoid RPF detection failure.

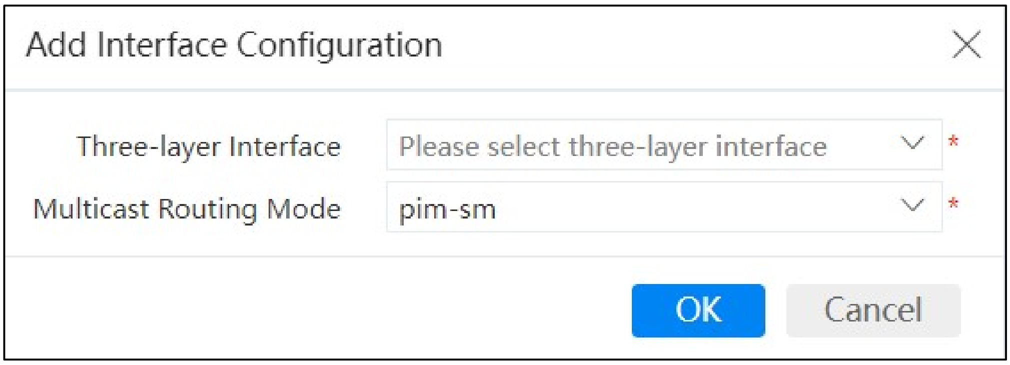
BSR: In the process of automatically generating RP, each IP address participating in the RP election is called a candidate RP (C-RP). In order to avoid the possibility that each PIM router calculates an RP, resulting in inconsistent calculation results, it is necessary to elect an RP referee in the network, called BSR, and all C-RPs send their own campaign RP messages to BSR through unicast. Finally, BSR selects the active RP from the received campaign messages and sends the address of the active RP to each router in the network. This ensures that the messages received by each router are consistent, and the RP address learned by each router is consistent.

5.8.1 Interface Configuration

Step 1. Choose "Network > Routing > Dynamic Multicast Route".

Step 2. On the “Interface Configuration” page, click “Add”.

Step 3. Configure the interface parameters.



Add Interface Configuration

Three-layer Interface: Please select three-layer interface *

Multicast Routing Mode: pim-sm *

Parameter	Description
L3 interface	The interface that needs to join the multicast group must work at L3.
Multicast routing mode	Currently support PIM-SM mode.

Step 4. Click “OK”.

The added interface is displayed in the L3 interface list. You can view the name and multicast routing mode of the L3 interface.

Step 5. Select the “Enable Multicast Route” checkbox.

When it is not selected, the multicast routing function will not take effect.

5.8.2 Candidate RP

Since the static RP does not have the backup function, when the active RP fails, you must manually change the RP, which will interrupt the forwarding of multicast data. Therefore, the firewall provides the function of automatically electing RPs. Each RP that participates in the election is called a candidate RP. There can be multiple candidate RPs in a multicast group, and a unified RP is elected based on BSR calculation. At the same time, one RP can also serve as the RP of multiple multicast groups. If multiple IP addresses are configured on the interface of the firewall, the first configured IP address will be used to participate in the election when RP is elected. When configuring candidate RP addresses, users need to pay attention to selecting the first configured IP address.

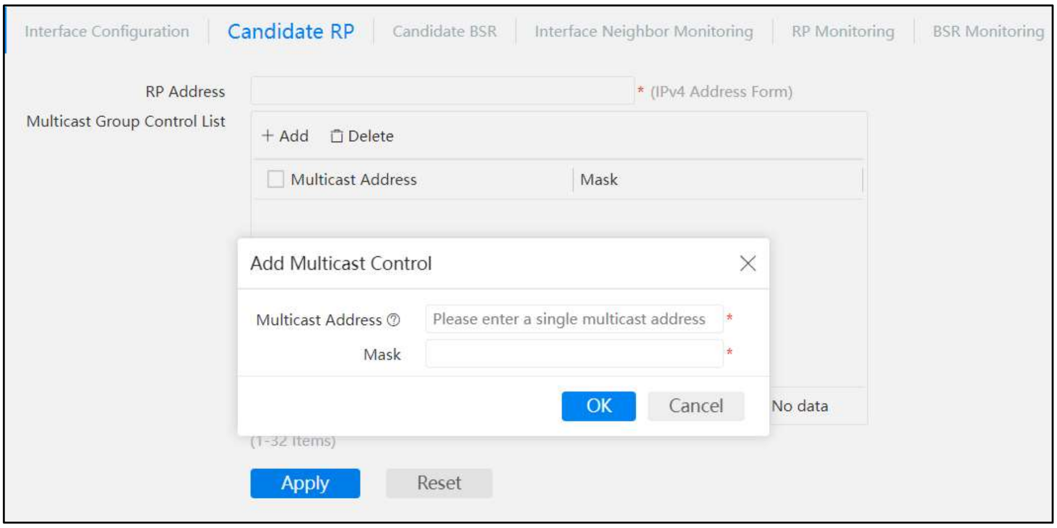
Step 1. Click the "Candidate RP" tab.

Step 2. Configure the RP address.

IPv4 address format, which is the address of the candidate RP participating in the election, usually the IP address of the interface joining the multicast group.

Step 3. Click "Add" to add multicast control.

Multiple multicast addresses can be written, and the maximum limit is 32.



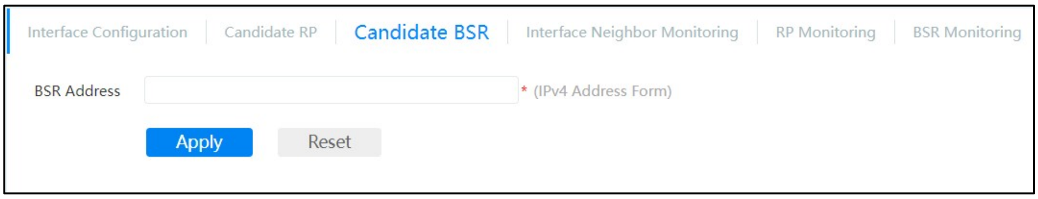
Step 4. Configure the multicast address and mask for multicast control, and click "OK".

Parameter	Description
Multicast address	The multicast address range is 224.0.0.0 ~239.255.255.255.
Mask	The mask format is dotted decimal, such as 255.255.255.0.

Step 5. After the configuration is complete, click "Apply".

5.8.3 Candidate BSR

Specify the candidate BSR address for the firewall to participate in the election, usually the IP address of the interface that joins the multicast group.



5.8.4 Interface Neighbor Monitoring

Interface Neighbor Monitoring provides the monitoring and display of neighbor interfaces that join the multicast group in the surrounding PIM routers. It is convenient for users to know which interfaces in the current network have joined the multicast group. At the same time, it is convenient for the administrator to maintain the multicast route.

Table 5-2 Interface Neighbor Monitoring Parameters

Parameter	Description
Interface name	An interface that is enabled with PIM-SM and has neighbor entries.
Local IP	The local IP address of the interface.
Neighbor IP	The IP address of the multicast neighbor.
Mark	**PIM:** This interface is selected as BDR. **PIM, DR:** This interface is selected as DR.

5.8.5 RP Monitoring

RP monitoring displays the active RP in the current multicast group. Each multicast group has an active RP, and multiple multicast groups can use the same active RP.

RP monitoring can facilitate the administrator to check which address the current active RP is, and facilitate the maintenance of multicast routes. At the same time, you can view the corresponding priority. By default, the larger the RP address, the higher the priority.

5.8.6 BSR Monitoring

BSR monitoring can facilitate the administrator to check which address the current BSR address is, and at the same time facilitate the maintenance of multicast routes. BSR monitoring can check the corresponding priority. By default, the larger the BSR address value is, the higher the priority is.

5.9 Route Monitoring

5.9.1 IPv4 Route Monitoring

IPv4 route monitoring allows users to view the status of all IPv4 direct connections, hosts, static and dynamic routes on the current firewall. It is convenient for administrators to troubleshoot network problems and maintain the routing table of the firewall.

IPv4 route monitoring provides route filtering and route query functions, and users can select route types to view routes of this type. By default, all types of routes are displayed, and you can choose to view routes of "Direct", "Static", "Host", "RIP", "OSPF", and "BGP". The host route refers to the route to a specific host, and the subnet mask is 32. Enter the destination IP address and click “Query” to view the type of route corresponding to the destination IP address.

Parameter	Description
Destination address	The address of the destination network.
Subnet mask	The subnet mask of the destination network.
Gateway	The next hop address of the route.
Egress interface	The egress interface name of the route.
Protocol	The protocol type of the destination route, "Direct", "Static", "Host", "RIP", "OSPF", and "BGP".
Status	Whether the route is currently in effect. ✓: take effect ✗: failed

5.9.2 IPv6 Route Monitoring

IPv6 route monitoring allows users to view the status of all IPv6 direct connections, hosts, static and dynamic routes on the current firewall. It is convenient for administrators to troubleshoot network problems and maintain the routing table of the firewall.

IPv6 route monitoring provides route filtering and route query functions, and users can select route types to view routes of this type. By default, all types of routes are displayed, and you can choose to view routes of "direct connection", "static", "host", "RIP ng ", "OSPF v3 ", and "BGP". A host route is a route to a specific host. Enter the destination IP address and click “Query” to view the type of route corresponding to the destination IP address.

Parameter	Description
Destination address	The destination address of the IPv6 route.
Gateway	The next-hop IPv6 address of the IPv6 route.
Egress interface	The egress interface name of the destination route.
Protocol	The protocol type of IPv6 routing, divided into "direct connection", "static", "host", "RIPng ", "OSPFv3", and "BGP".
Status	Whether IPv6 routing is currently in effect. ✓: take effect ✗: failed

5.9.3 Policy Routing Monitoring

Policy routing monitoring allows users to view the status of all policy routing on the current firewall. It is convenient for administrators to troubleshoot network problems and maintain the routing table of the firewall.

Parameter	Description
Name	The name of the policy route.
Source security zone	The source security zone of policy route.
Source address	The source address of the policy route.
Destination address	The destination address of policy route.
Service	The service referenced by the policy route.
Gateway	The next hop address of the policy route.
Gateway status	Policy routing gateway status.
Status	Whether policy routing is currently in effect. ✓: take effect ✗: failed

5.9.4 ISP Route Monitoring

ISP route monitoring allows users to view the status of all ISP routes on the current firewall. It is convenient for administrators to troubleshoot network problems and maintain the routing table of the firewall

Parameter	Description
name	The name of the ISP route.
ISP	The ISP information referenced by the ISP route
Gateway	The next hop address of the ISP route.
Gateway status	The gateway status of the ISP route.
Priority	The priority of ISP routes.
Status	Whether the ISP route is currently in effect. ✓: take effect ✗: failed

5.9.5 Multicast Routing Monitoring

When the firewall receives the data of the multicast address, it will decide whether to forward the data according to the current multicast routing configuration, and the forwarded data will be checked in the corresponding records in the forwarding table monitoring. It is convenient for users to query which multicast addresses are forwarded by the current firewall, and record the multicast source address and source interface, destination multicast address, and destination interface information at the same time. If the firewall does not receive any multicast data or does not forward the multicast data, it will not view the monitoring information in the forwarding table monitoring.

Parameter	Description
Source address	The source address of the multicast route is a unicast address.
Source interface	The interface for the source address of the multicast route.
Destination multicast address	The destination multicast address of the multicast group.
Destination interface	The egress interface of the destination multicast address.

6 User and Authentication

6.1 Overview

Authentication is used to verify the identity of the administrator and the user or device of the traffic passing through the firewall, so as to ensure the security of the firewall and intranet resources. Authentication scenarios include administrator authentication, web authentication, and VPN user authentication. The user's identity can be identified through user name, password, certificate or two-factor authentication. The firewall supports local server user name and password authentication, authentication server remote user name and password authentication, certificate authentication, two-factor authentication and other authentication methods; supports special IP authentication-free, AD linkage single-point authentication, firewall portal authentication and other authentication methods.

Only when the web authentication policy is enabled can the user be authenticated for accessing the Internet.

VPN users are authenticated during the VPN access process.

The authenticated user IP address is identified as the corresponding user name, and the authenticated user traffic can be further controlled and managed through security policies, QoS, and behavior control.

6.1.1 Authentication Method

- Local user password authentication

The firewall authenticates users through passwords. Users need to be created on the firewall before authentication.

- Authentication server password authentication

The server authentication is applicable to scenarios where multiple firewalls manage the same user or an authentication server has been deployed on the network.

When the authentication server is used for authentication, the firewall sends the user name and password in ciphertext to the authentication server for authentication, and the authentication server sends the authentication result to the firewall.

The firewall supports RADIUS authentication server, TACACS+ authentication server, LDAP authentication server, AD authentication server, and POP3 authentication server.

- Certificate authentication

It is suitable for authenticating terminals or devices in scenarios such as IPSec VPN.

- Two-factor authentication
- ITS linkage certification

The firewall supports the RADIUS PAP and CHAP authentication for administrators, Web authentication users, and VPN users with ITS. Perform two-factor authentication via user/password and OTP.

6.1.2 User Authentication Method

Users can access the network after being authenticated in the following ways:

- Firewall Portal Authentication

The firewall provides HTTP and HTTPS Portal authentication pages to authenticate users.

- Authentication-free

Manually bind the username and IP address. Such users access the firewall without authentication.

- AD single login

Internet users send their user names and passwords to the AD server for authentication. By cooperating with the AD server, the firewall can receive the list of AD-authenticated users. The firewall checks the list of AD-authenticated users, finds the correspondence between IP addresses and user names, and directly allows users to access the Internet without re-authentication.

6.2 User

The firewall supports user authentication based on users, user groups, and user roles.

6.2.1 Restrictions and Precautions

Standard RADIUS server, the user name does not support some special characters (such as: @ \ /: < > | ' %), and the user name using RADIUS authentication should not include these special characters.

6.2.2 Authenticate user

When an internal network user accesses the external network, the authentication user must be added to the firewall for local authentication through the firewall authentication user, and the authentication user group and authentication user role must be properly configured.

Add Authenticated User

Step 1. Select “Object > Users > Users".

Step 2. Choose “Add”.

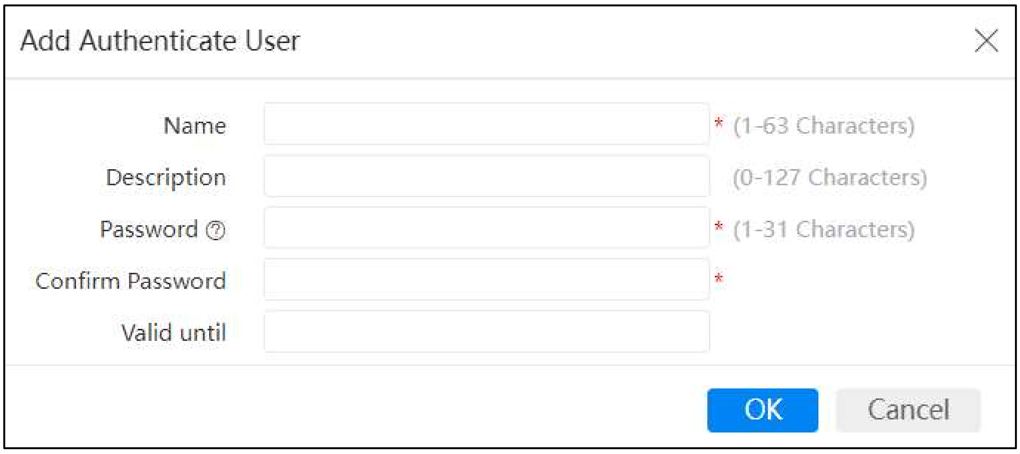
Step 3. Configure authentication user parameters.

The name and password of the authenticated user must be configured. The firewall authenticates users through usernames and passwords.

It is recommended to configure the password to be more than eight characters and meet the complexity requirements of at least three of numbers, uppercase letters, lowercase letters, and special symbols.

If no validity period is selected, the authenticated user account will not become invalid.

If the user is a temporary visitor, an appropriate validity period needs to be configured for the user, and the user will automatically become invalid after the validity period expires.



Add Authenticate User

Name * (1-63 Characters)

Description (0-127 Characters)

Password * (1-31 Characters)

Confirm Password *

Valid until

Step 4. After the configuration is complete, click “OK”.

The configured users are displayed in the authenticated user list, and you can see the validity period, group and role of the user.

Users can be edited and deleted.

⚠注意

When a user is no longer used, please delete the user to avoid security risks.

Authentication User Group

The authentication user group provides the function of managing authentication users in groups. Put users with different rights into different user groups. The same user can be placed under multiple user groups. The firewall supports user group-based authentication.

Step 1. Choose “Object > Users > User Group”.

Step 2. Choose “Add”.

Step 3. Configure the name and description of the authentication user group.

Step 4. Select the desired user from the members list to join the authenticated user group.

Step 5. After the configuration is complete, click “OK”.

The created authentication user group can be viewed in the authentication user group list. Users can view the number of members in the user group.

The user group can be edited and deleted.

Authenticated User Role

Authenticated users can be managed not only based on authenticated user groups, but also based on user roles. Set different user roles for different types of users. The same user can be placed under multiple user roles. The firewall supports user role-based authentication.

Step 1. Choose “Object > Users > User Role”.

Step 2. Choose “Add”.

Step 3. Configure the name and description of the authenticated user role.

Step 4. Select the desired user from the Members list to join the authenticated user role.

Step 5. After the configuration is complete, click “OK”.

The created authenticated user roles can be viewed in the list of authenticated user roles. Users can view the number of members in the user role.

User roles can be edited and deleted.

6.2.3 Authentication Server

The firewall supports user authentication through an authentication server. Before user authentication, the authentication server must be configured. The authentication server type supports local authentication, RADIUS, TACACS+, LDAP, Active Directory, certificate authentication, and POP3.

Add Local Authentication Server

By default, the system creates a local authentication server named local, which can be edited but not deleted by users. When Local is selected for the authentication server in the web authentication policy, it means local authentication on the firewall.

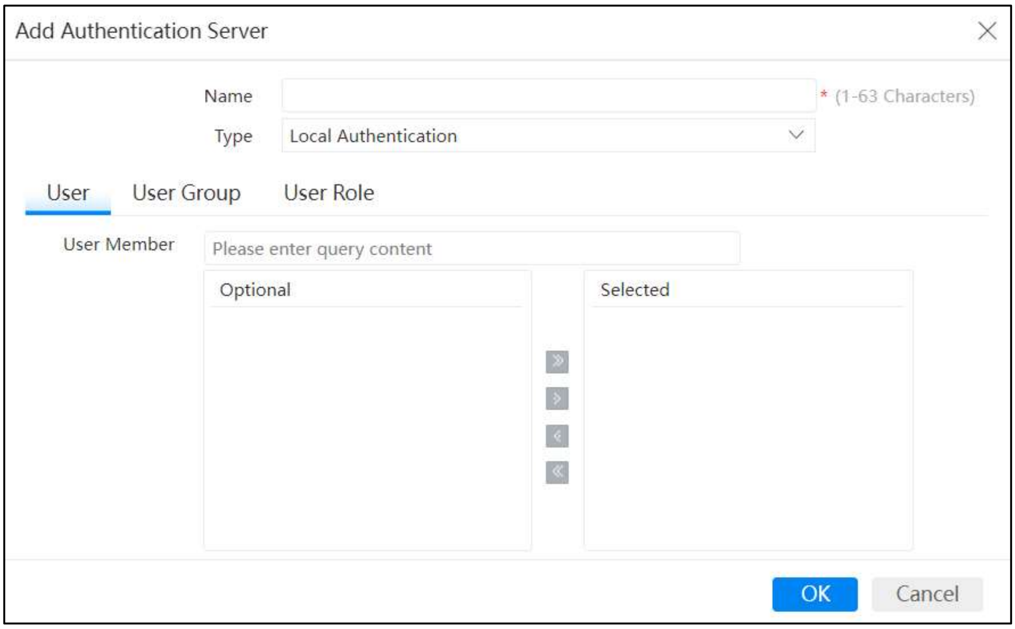
Step 1. Choose “Object > Users > Authentication Server”.

Step 2. Click “Add”.

Step 3. Configure the name and type of the authentication server.

Select "Local Authentication " for the authentication type.

Step 4. Specify the users, user group members and user roles to be authenticated by the authentication server.



Add Authentication Server

Name * (1-63 Characters)

Type Local Authentication

User Member: Please enter query content

Step 5. After the configuration is complete, click “OK”.

The added authentication servers are displayed in the authentication server list. You can view the name, type, detailed information, member information, and reference times of the authentication server. You can perform connection test, modification and deletion operations on the server.

Add RADIUS Authentication Server

RADISU authentication is a widely used authentication method. The RADIUS server authenticates the client through the UDP protocol. As a RADIUS client, the firewall sends the user name and password to the RADIUS server for authentication, and the RADIUS server sends the authentication result to the firewall.

The parameters of the RADIUS authentication server configured on the firewall must be consistent with those of the RADIUS server to communicate normally.

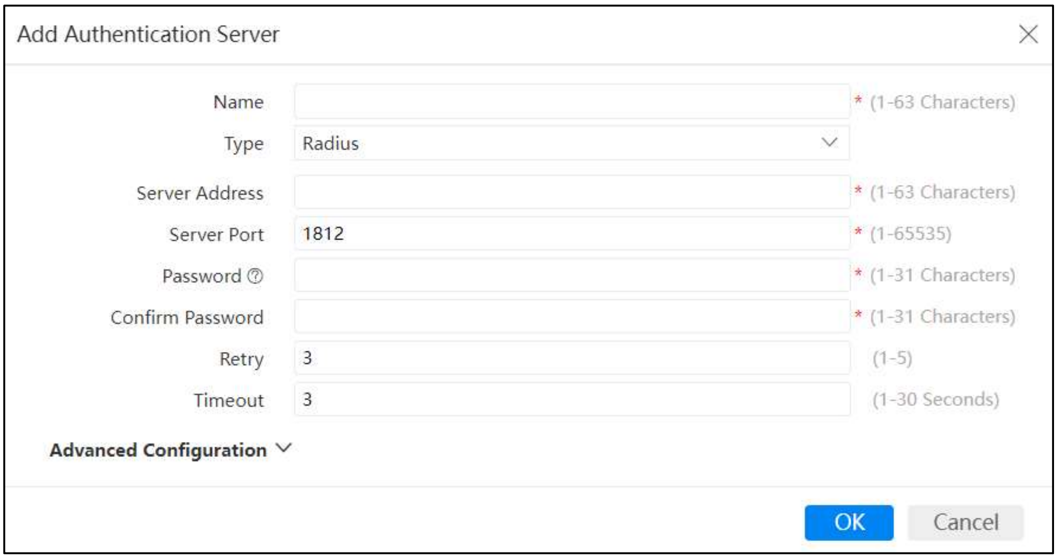
Step 1. Choose “Object > Users > Authentication Server”.

Step 2. Click “Add”.

Step 3. Configure the name and type of the authentication server.

Select "Radius " for the authentication type.

Step 4. Configure other parameters of the RADIUS server.



Add Authentication Server

Name: * (1-63 Characters)

Type: Radius

Server Address: * (1-63 Characters)

Server Port: 1812 * (1-65535)

Password: * (1-31 Characters)

Confirm Password: * (1-31 Characters)

Retry: 3 (1-5)

Timeout: 3 (1-30 Seconds)

Parameter	Description
Server address	Specify the RADIUS server IP v4address, in dotted decimal format
Server port	RADIUS server port, the default is 1812.
Password and Confirm password	Set the RADIUS server key. The key is used to encrypt messages sent between the firewall and the RADIUS server.
Retry	Set the maximum number of retries when connecting to the server fails.
Timeout	The timeout period of the RADIUS server. If there is still no response after the timeout period, the server connection fails.
Advanced configuration	

Parameter	Description
Authentication type	The authentication type supports "CHAP" and "PAP". Select according to the actual authentication type of the server.

Step 5. After the configuration is complete, click “OK”.

The added authentication servers are displayed in the authentication server list. You can view the name, type, detailed information, member information, and reference times of the authentication server. You can perform connection test, modification and deletion operations on the server.

Add TACACS+ Authentication Server

When users use TACACS+ authentication, a TACACS+ authentication server needs to be configured. TACACS+ uses TCP port 49 by default, which is more reliable than RADIUS using UDP.

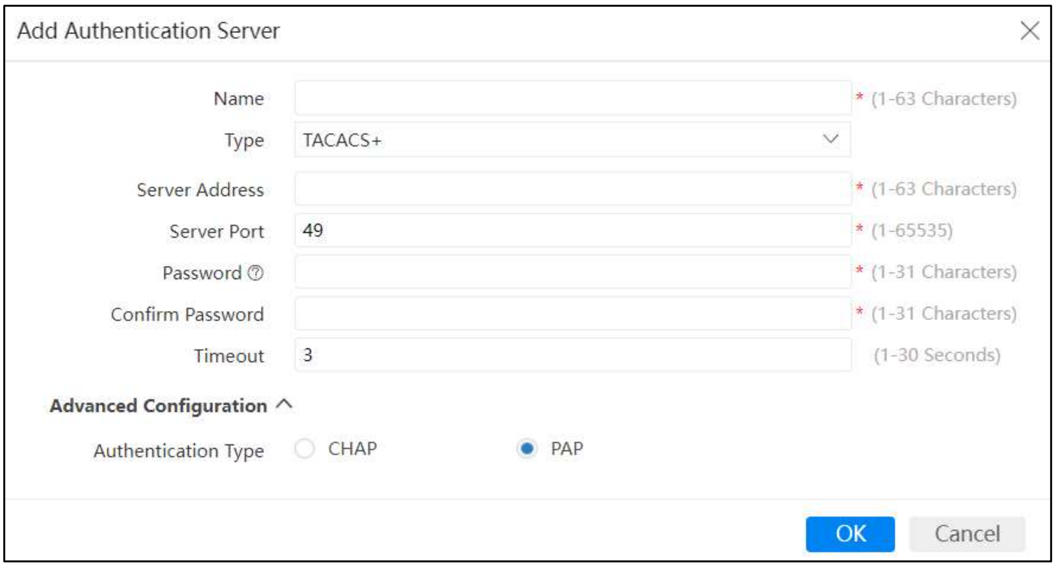
Step 1. Choose “Object > Users > Authentication Server”.

Step 2. Click “Add”.

Step 3. Configure the name and type of the authentication server.

Select " TACACS+ " for the authentication type.

Step 4. Configure other parameters of the TACACS+ server.


Add Authentication Server

Name: * (1-63 Characters)
Type: TACACS+
Server Address: * (1-63 Characters)
Server Port: 49 * (1-65535)
Password: * (1-31 Characters)
Confirm Password: * (1-31 Characters)
Timeout: 3 (1-30 Seconds)

Advanced Configuration

Authentication Type: ○ CHAP ● PAP

Parameter	Description
Server address	Specify the IPv4 address of the TACACS+ server. Dotted decimal.

Parameter	Description
Server port	Specify the port of the TACACS+ server. The default is 49.
Password and Confirm Password	Set the TACACS+ server key.
Timeout	Set the timeout period of the TACACS+ server. If there is still no response after the timeout period, the server connection fails.
Advanced configuration	
Authentication type	Select the authentication type of the TACACS+ server. The authentication type supports CHAP and PAP.

Step 5. After the configuration is complete, click “OK”.

Add LDAP Authentication Server

When LDAP authentication is used for users, an LDAP authentication server needs to be configured.

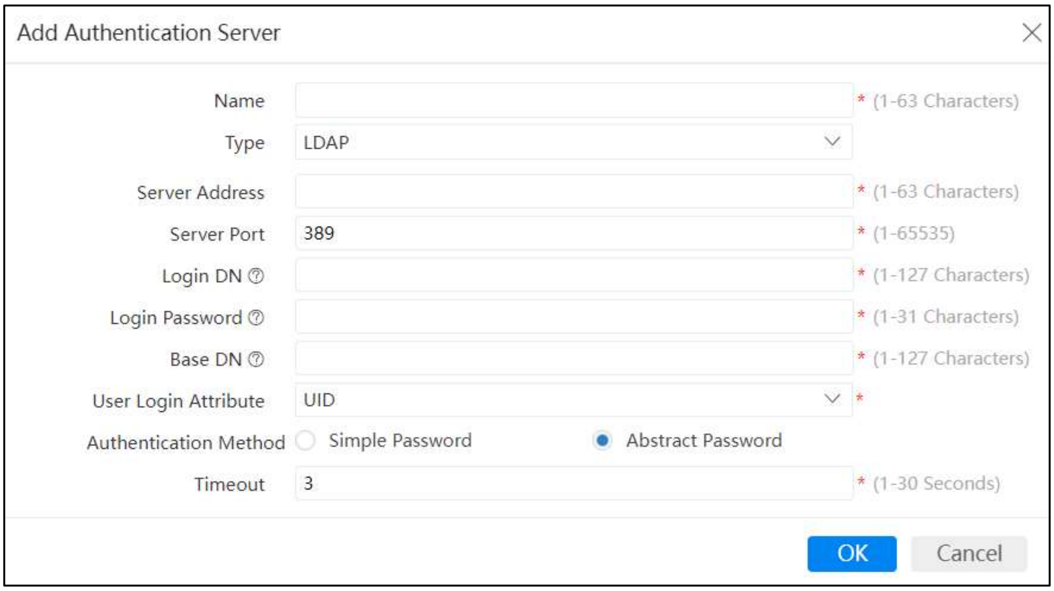
Step 1. Choose “Object > Users > Authentication Server”.

Step 2. Click “Add”.

Step 3. Configure the name and type of the authentication server.

Select " LDAP " for authentication type.

Step 4. Configure other parameters of the LDAP server.



Add Authentication Server

Name		* (1-63 Characters)
Type	LDAP	
Server Address		* (1-63 Characters)
Server Port	389	* (1-65535)
Login DN ⑦		* (1-127 Characters)
Login Password ⑦		* (1-31 Characters)
Base DN ⑦		* (1-127 Characters)
User Login Attribute	UID	*
Authentication Method	○ Simple Password ● Abstract Password	
Timeout	3	* (1-30 Seconds)

Parameter	Description
Server address	Specify the IPv4 address of the LDAP server. Dotted decimal.
Server port	Specify the port of the LDAP server. The default is 389.
Login DN	Specify the directory tree of the authenticated user in the LDAP server.
Login password	Set the password for logging in to the LDAP server.
Base DN	Specify the topmost directory tree of LDAP.
User Login Attribute	Set user login attributes, only "UID" is supported. This configuration must be consistent with the configuration on the LDAP server.
Authentication method	Select simple password authentication or abstract password authentication. This configuration must be consistent with the LDAP server configuration.
Timeout	LDAP server timeout time, if there is still no response after the timeout time, the LDAP server connection fails.

Step 5. After the configuration is complete, click “OK”.

The added authentication servers are displayed in the authentication server list. You can view the name, type, detailed information, member information, and reference times of the authentication server. You can perform connection test, modification and deletion operations on the server.

Add AD Authentication Server

When AD authentication is used for users, an AD authentication server needs to be configured.

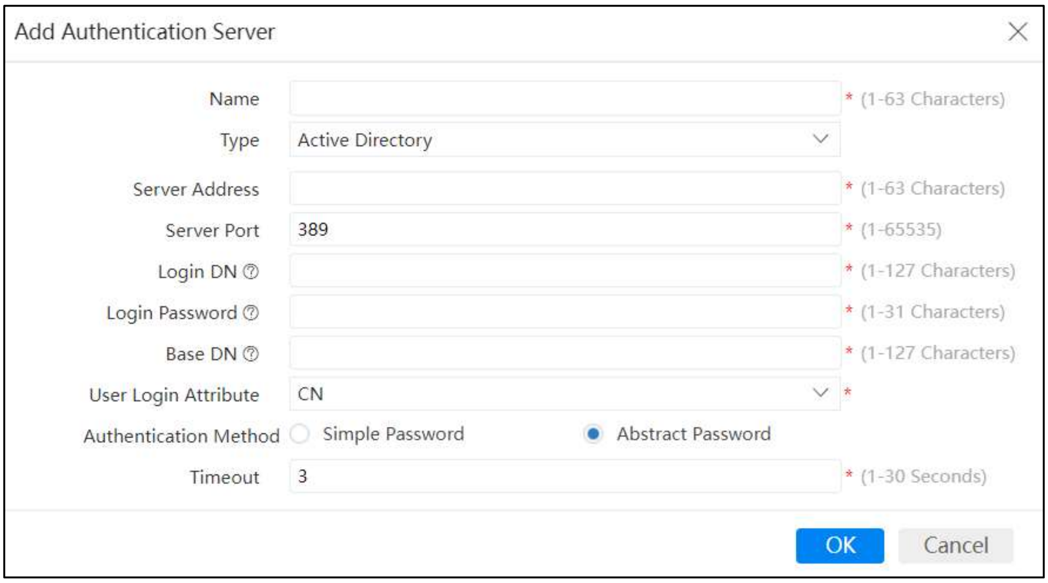
Step 1. Select “Object > Users > Authentication Server".

Step 2. Click “Add”.

Step 3. Configure the name and type of the authentication server.

Select " Active Directory " for the authentication type.

Step 4. Configure other parameters of the AD server.



Add Authentication Server

Name		* (1-63 Characters)
Type	Active Directory	
Server Address		* (1-63 Characters)
Server Port	389	* (1-65535)
Login DN ⓘ		* (1-127 Characters)
Login Password ⓘ		* (1-31 Characters)
Base DN ⓘ		* (1-127 Characters)
User Login Attribute	CN	*
Authentication Method	○ Simple Password ● Abstract Password	
Timeout	3	* (1-30 Seconds)

Parameter	Description
Server address	Specify the AD server IPv4 address, in the dotted decimal format.
Server port	Specify the AD server port, which is 389 by default.
Login DN	The directory tree of the authenticated user on the AD server.
Login password	Password for logging in to the AD server.
Base DN	The top directory tree of AD.
User Login Attribute	Select the user login attribute, which is divided into three types: CN, sAMAccountName, and userPrincipalName. This configuration must be consistent with the configuration on the AD server.
Authentication method	Select simple password authentication or abstract password authentication, which is consistent with the AD server configuration.
Timeout	The AD server timeout period. If there is still no response after the timeout period, the connection to the AD server fails.

Step 5. After the configuration is complete, click “OK”.

The added authentication servers are displayed in the authentication server list. You can view the name, type, detailed information, member information, and reference times of the authentication server. You can perform connection test, modification and deletion operations on the server.

Add Certificate Authentication Server

When certificate authentication is selected for a tunnel, an authentication server of the certificate authentication type needs to be added.

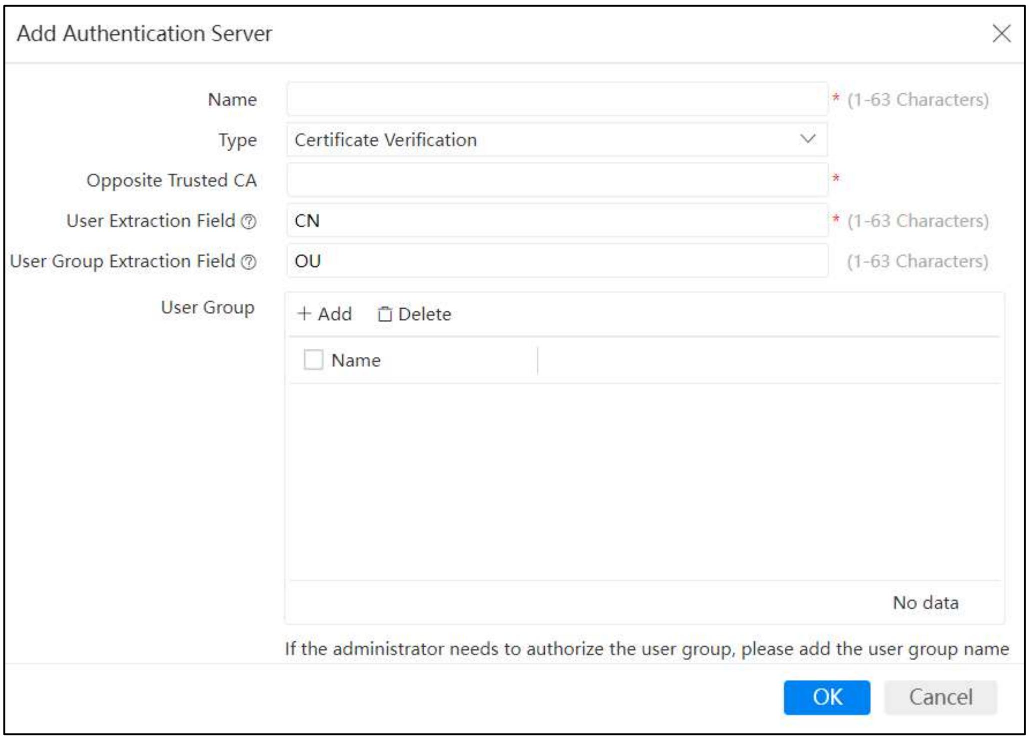
Step 1. Choose “Object > Users > Authentication Server”.

Step 2. Click “Add”.

Step 3. Configure the name and type of the authentication server.

Select "Certificate Verification" for the authentication type.

Step 4. Configure other parameters for certificate authentication.



Add Authentication Server

Name	* (1-63 Characters)
Type	Certificate Verification
Opposite Trusted CA	*
User Extraction Field	CN * (1-63 Characters)
User Group Extraction Field	OU (1-63 Characters)
User Group	

If the administrator needs to authorize the user group, please add the user group name

Parameter	Description
Opposite Trusted CA	Select the CA center that issues the certificate for the client as the trusted CA of the peer end. You can choose but no more than 2.
User extraction field	Extract the field identifier for the username of the certificate, such as CN. It is valid when single-factor authentication is enabled on the tunnel and a certificate authentication server is selected. Please ignore this field for two-factor authentication.

Parameter	Description
User group extraction field	Extract the field ID of the certificate user group name, such as OU. It is valid when single-factor authentication is enabled on the tunnel and a certificate authentication server is selected. Please ignore this field for two-factor authentication.
User group	If the administrator needs to authorize the user group, you need to add the user group name, which is the content of the OU field. Multiple items can be added to the user group name, and the maximum number does not exceed 128 items.

Step 5. After the configuration is complete, click “OK”.

The added authentication servers are displayed in the authentication server list. You can view the name, type, detailed information, member information, and reference times of the authentication server. You can perform connection test, modification and deletion operations on the server.

Add POP3 Authentication Server

If the mail server is used as the authentication server and the authentication account is the same as the mail account, a POP3 server needs to be added.

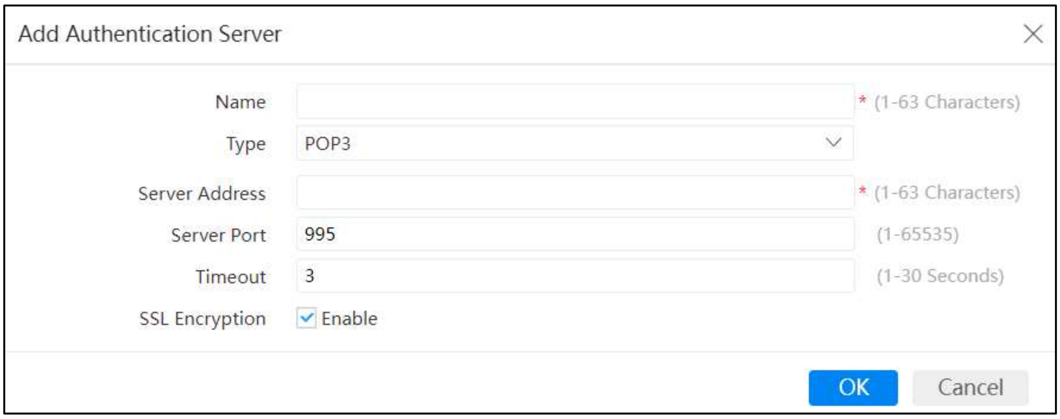
Step 1. Choose “Object > Users > Authentication Server”.

Step 2. Click “Add”.

Step 3. Configure the name and type of the authentication server.

Select "POP3 " for authentication type.

Step 4. Configure authentication server parameters.



Add Authentication Server

Name: * (1-63 Characters)

Type: POP3

Server Address: * (1-63 Characters)

Server Port: 995 (1-65535)

Timeout: 3 (1-30 Seconds)

SSL Encryption: ☑ Enable

Parameter	Description
Server address	POP3 server IPv4 address, in the dotted decimal format

Parameter	Description
Server port	POP3 service port number, the default is 995.
Timeout	POP3 server timeout time, if there is still no response after the timeout time, the POP3 server connection fails.
SSL encryption	Authentication communication data encryption, check to enable SSL encryption, uncheck to disable SSL encryption.

Step 5. After the configuration is complete, click “OK”.

The added authentication servers are displayed in the authentication server list. You can view the name, type, detailed information, member information, and reference times of the authentication server. You can perform connection test, modification and deletion operations on the server.

6.2.4 Manually Bind Users

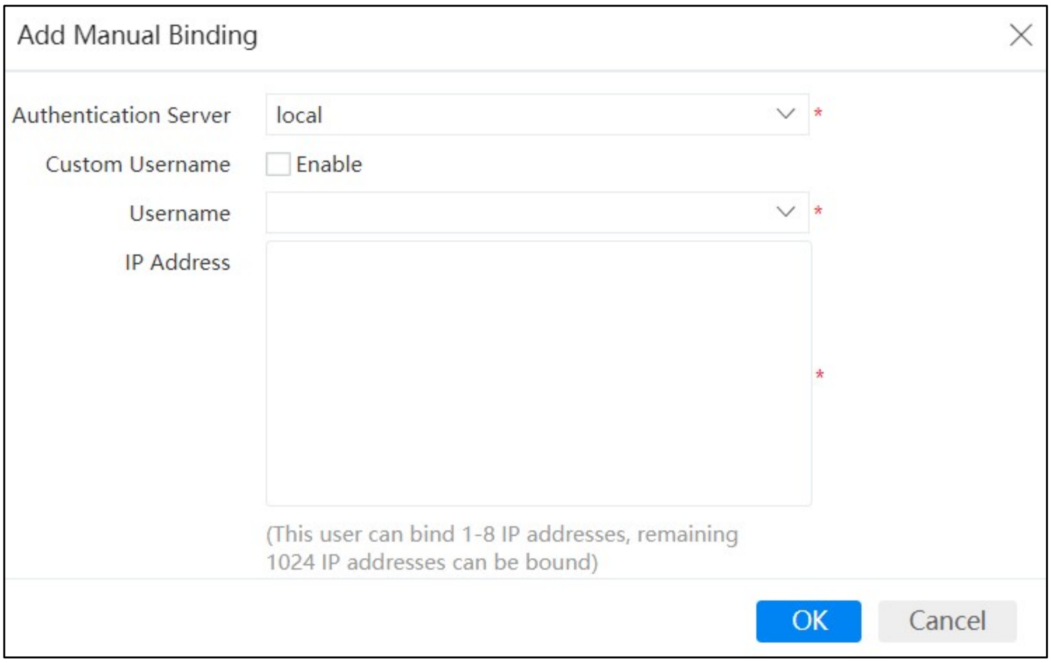
By binding user names with IP addresses, these IP addresses can be identified on the basis of a user without Web authentication. After the user binding takes effect, the logs generated by the IP address in the user binding will be displayed as the corresponding user name in the user binding instead of the IP address in the statistical information of functions such as logs and monitoring.

Add Manual Binding User

Step 1. Choose “Object > Users > Manual Binding”.

Step 2. Click “Add”.

Step 3. Set the manual binding user ID parameter.



Add Manual Binding

Authentication Server: local *

Custom Username: □ Enable

Username: *

IP Address: *

(This user can bind 1-8 IP addresses, remaining 1024 IP addresses can be bound)

Parameter	Description
Authentication server	Select an authentication server. Bind the username and IP address of the user on the authentication server.
Custom username	When enabled, the username can be customized in the username text box.
Username	Choose a username or customize a username. The length of the custom user name ranges from 1 to 63 characters.
IP address	Specify the IP address to which the user is bound.

Step 4. After the configuration is complete, click “OK”.

The configured user name is displayed in the list of manually bound user IDs. You can view the user name and the authentication server and binding IP used by the user. Users can be edited and deleted.

When the relationship between users, groups, roles, and authentication servers changes, click “Synchronize” to update the information about users, authentication servers, and bound IPs.

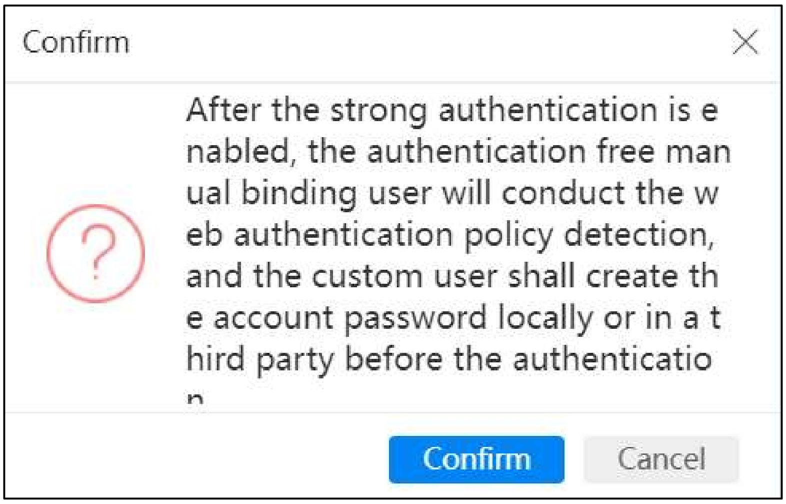
Enable Strong Authentication

Manually bound users are free from authentication by default. After "Strong Authentication" is enabled, authentication is also required for manually bound users. At this time, the user's address and password must match to authenticate successfully.

Step 1. Choose “Object > User > Manual Binding”.

Step 2. Select the "Strong Authentication" checkbox in the menu bar above the list to enable the strong authentication function.

Step 3. In the “Confirm” dialog box, click “OK”.



Confirm

After the strong authentication is enabled, the authentication free manual binding user will conduct the web authentication policy detection, and the custom user shall create the account password locally or in a third party before the authentication

6.2.5 Configure AD Linkage

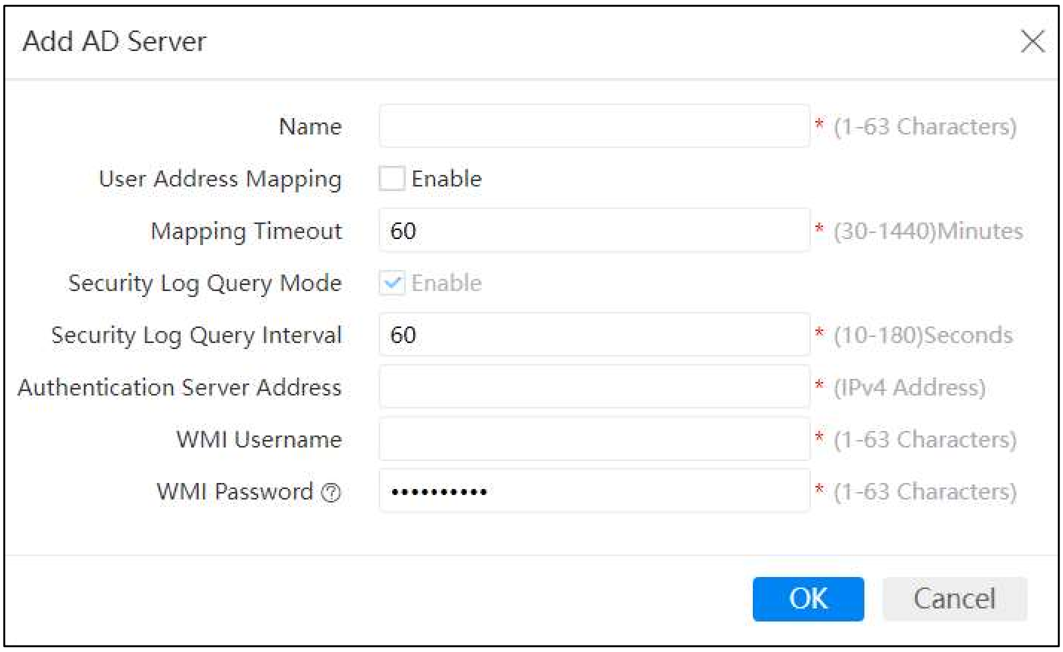
The firewall supports linkage with the AD server, and the user list in the AD server is synchronized to the firewall. For users who have passed the authentication on the AD server, they will not be authenticated after being identified by their usernames.

Step 1. Choose “Object > Users > AD Linkage”.

Step 2. Click “Server Configuration”.

Step 3. Click “Add”.

Step 4. Configure AD server parameters.



Add AD Server

Name		* (1-63 Characters)
User Address Mapping	□ Enable	
Mapping Timeout	60	* (30-1440)Minutes
Security Log Query Mode	☑ Enable	
Security Log Query Interval	60	* (10-180)Seconds
Authentication Server Address		* (IPv4 Address)
WMI Username		* (1-63 Characters)
WMI Password ⓘ	••••••••••	* (1-63 Characters)

Parameter	Description
Name	Specify the name of the AD server.
User address mapping	Select "Enable" to enable the user address mapping function. After the user address mapping function is enabled, the user list can map the relationship between user names and IP addresses.
Mapping timeout	The mapping timeout of the relationship between user name and IP address, the default is 60 minutes, and the range is 30-1440 minutes. After the timeout, the relationship between the user name and the IP address needs to be relearned.
Security log query mode	Select "Enable" to enable the security log query mode.
Security log query time	The interval of the security log query, the default is 60 seconds, and the range is 10-180 seconds.
Authentication server address	The IP address of the AD authentication server.
WMI username	The WMI username name.
WMI password	The password corresponding to the WMI username.

Step 5. After the configuration is complete, click “OK”.

The added server is displayed in the server list.

After the firewall and AD are linked successfully, the obtained user list will be displayed here. Click “Refresh” to update the user list.

6.3 Security Authentication

Security authentication is used to authenticate users, user groups or user roles under the selected authentication server. If there is no authentication policy for a user, the user can directly access the external network without being affected by the web authentication policy and URL redirection authentication policy.

6.3.1 Restrictions and Precautions

- Only TCP data will match the web authentication policy, and other protocols will not. User filtering can be controlled by setting the source user field in the security policy.
- When an IP address configured with user binding triggers http or https access, even if web authentication is enabled, web authentication is not required.
- After the user binding takes effect, the logs generated by the IP address in the user binding will be displayed as the corresponding user name in the user binding instead of the IP address in the statistical information of functions such as system logs and monitoring. The log recorded by web authentication can be viewed under the system log.
- The firewall disables web authentication by default. Only when web authentication is enabled, the web authentication policy will be matched when intranet users access the external network.
- The firewall disables URL redirection by default. Only when URL redirection is enabled, the URL redirection authentication policy will be matched when intranet users access the external network.
- The order of the authentication policy in the authentication list determines the priority of the authentication policy. The earlier the authentication policy is, the higher the priority is. After the data flow matches an authentication policy, it will not match the following authentication policies. That is, if the data flow first matches a URL redirection policy, it will not match the following web authentication policy.
- Users who pass the authentication policy will be recorded as authenticated users. The next time the user accesses the external network, the user's source IP address and user name will be matched. If the user has passed the authentication policy, there is no need to perform web authentication again.

- The destination address of the URL redirection authentication policy cannot be configured as any, because if the destination address contains the address of the redirection URL, a redirection loop will be caused and the redirection page cannot be opened.

6.3.2 Add Authentication Policy

The authentication policy triggers authentication based on HTTP traffic. When the traffic matches the authentication policy, user authentication is performed first. After the authentication is passed, the user's data can be controlled based on IP/application and other attributes according to the configuration in the security policy.

After passing the authentication, the user is not permanently authenticated, and must re-authenticate after the mandatory login interval expires. The re-authentication mechanism can ensure the security of user authentication.

Add Web Authentication Policy

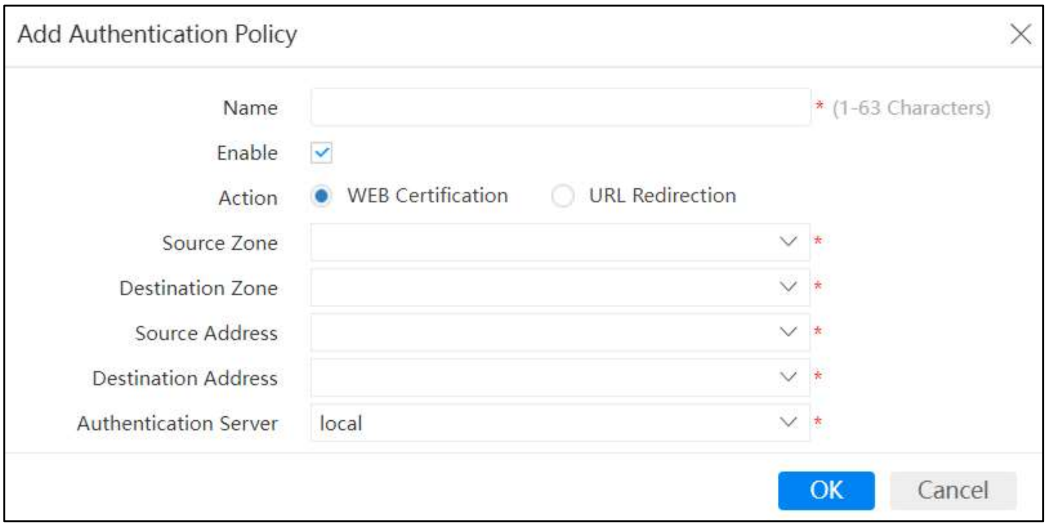
After the web authentication policy is selected, only users who pass the server authentication can access the external network.

Step 1. Choose “Policy > Security Authentication > Authentication Policy”.

Step 2. Click “Add”.

Step 3. Select "WEB Authentication" for “Action.

Step 4. Configure the parameters of the web authentication policy.



Add Authentication Policy

Name * (1-63 Characters)

Enable ☑

Action ● WEB Certification ○ URL Redirection

Source Zone *

Destination Zone *

Source Address *

Destination Address *

Authentication Server: local *

Parameter	Description
Name	Configure the name of the authentication policy.

Parameter	Description
Enable	The authentication policy takes effect only after "Enable" is selected.
Action	The web authentication policy action is " WEB Authentication ".
Source zone	Select the security zone to which the inbound interface of the authentication policy belongs.
Destination zone	Select the security zone to which the outbound interface of the authentication policy belongs.
Source address	Select the source address object of the authentication policy.
Destination address	Select the destination address object of the authentication policy.
Authentication server	Used for web authentication. The authentication server can be a local server or a third-party authentication server.

Step 5. After the configuration is complete, click “OK”.

Add URL Redirection Authentication Policy

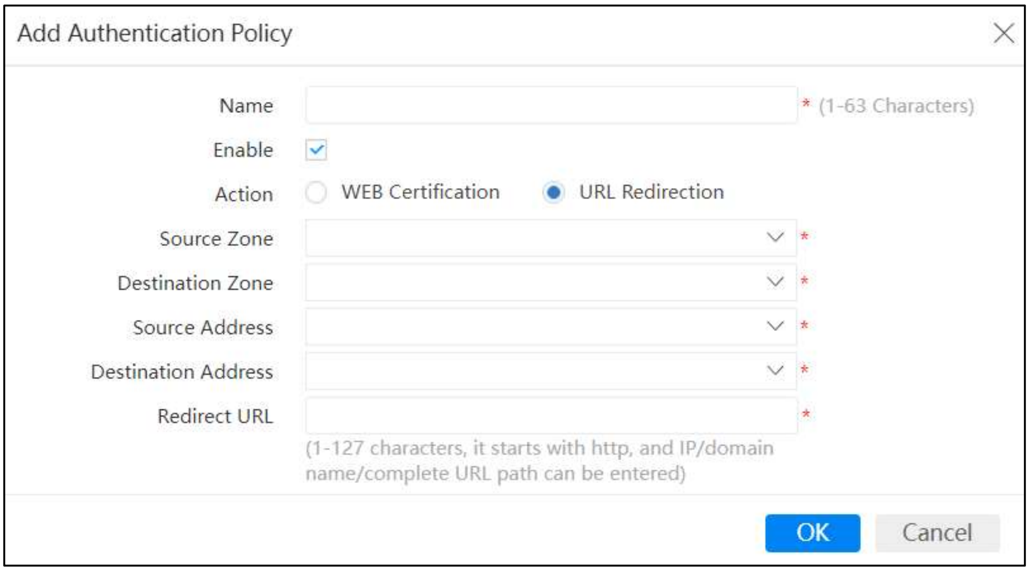
The URL redirection authentication policy is used to configure the redirection URL and redirection matching conditions when users perform HTTP access. The HTTPS redirection URL is set during the HTTPS configuration of WEB authentication.

Step 1. Choose “Policy > Security Authentication > Authentication Policy”.

Step 2. Click “Add”.

Step 3. Select " URL Redirect" for “Action”.

Step 4. Configure URL redirection authentication policy parameters.



Add Authentication Policy

Name * (1-63 Characters)

Enable ☑

Action ○ WEB Certification ● URL Redirection

Source Zone *

Destination Zone *

Source Address *

Destination Address *

Redirect URL *

(1-127 characters, it starts with http, and IP/domain name/complete URL path can be entered)

Parameter	Description
Name	Configure the name of the authentication policy.
Enable	The authentication policy takes effect only after "Enable" is selected.
Action	The URL redirection authentication policy action is "URL redirection".
Source zone	Select the security zone to which the inbound interface of the authentication policy belongs.
Destination zone	Select the security zone to which the outbound interface of the authentication policy belongs.
source address	Select the source address object of the authentication policy.
Destination address	Select the destination address object of the authentication policy.
Redirect URL	URL redirection supports pushing redirection pages to users when they perform HTTP access. The parameters of URL redirection are set on the "URL Redirection " page.

Step 5.After the configuration is complete, click “OK”.

Adjust the Order of Authentication Policies

The order of the authentication policy in the authentication list determines the priority of the authentication policy. The earlier the authentication policy is, the higher the priority is. If the data flow matches a web authentication policy/URL redirection authentication policy, it will not continue to match the following authentication policies. Therefore, the sequence of authentication policies must be properly configured.

Step 1. Choose an authentication policy.

Step 2. Click “Reorder”.

Step 3. Select the keyword to adjust the policy.

The adjustment policy keywords support "top", "before", "after" and "end". These keywords can be used to adjust the authentication policy to the top of the list, before the specified policy, after the specified policy, and at the end.

Step 4. Click “OK”.

6.3.3 Configure web authentication

The WEB authentication of the firewall is used to control the rights of intranet users to access the external network through the Web. The firewall supports user authentication through HTTP and HTTPS.

Step 1. Choose “Policy > Security Authentication > WEB Auth”.

Step 2. Select “Enable” to enable the WEB authentication function.

The WEB authentication function is disabled by default. After the web authentication function is enabled, intranet users must pass web authentication before they can access the extranet. The firewall authenticates users for Web access through Web authentication policies.

Step 3. Configure the WEB authentication mode and port.

The firewall supports user authentication through HTTP and HTTPS.

The HTTP authentication port provided by the firewall is 65080; the HTTPS authentication port is 65443. The value range of the authentication port is 1025 ~65535, and the user can customize it.

Step 4. Users are prohibited from changing passwords.

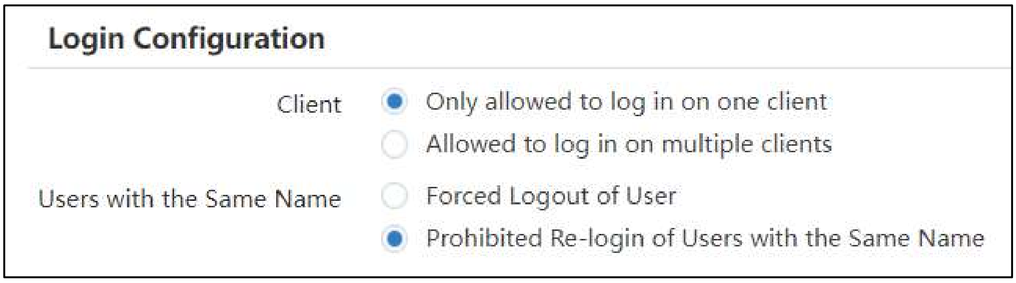
"Web Authentication Login" page pops up by default. After a local authentication user logs in, a "Change Password" button will appear, through which the user can modify the password. Remote server users are not involved in this issue.

If the administrator prohibits users from modifying passwords, please select the "Prevent users from modifying passwords " check box. At this time, the "Change Password" button will no longer be displayed after all users are successfully authenticated.

Step 5. Limit the number of simultaneous logins by the same user.

The same user may log in multiple times on multiple clients. The firewall supports strict or loose settings for users' access to the Internet according to network security requirements.

- Only one user is allowed to log in on one client. When the user logs in again, it is supported to select "Forced logout of user" or "Prohibited Re-login of Users with the Same Name ".

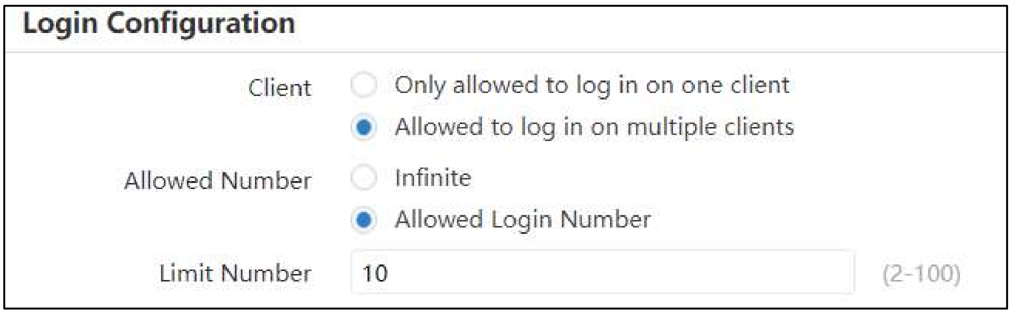


Login Configuration

Client ● Only allowed to log in on one client
○ Allowed to log in on multiple clients

Users with the Same Name ○ Forced Logout of User
● Prohibited Re-login of Users with the Same Name

- Allows the same user to log in on multiple clients at the same time. Limit the number of logins for the same user or allow unlimited logins. The limit number ranges from 2 to 100, and the default is 10. The same user can no longer log in after the number of concurrent online users reaches the limit.



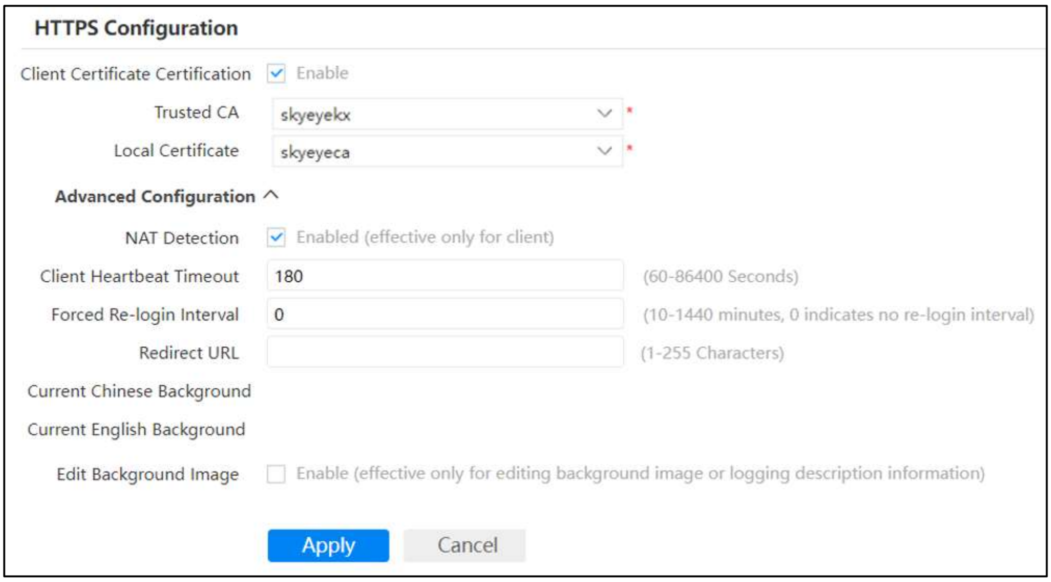
Login Configuration

Client ○ Only allowed to log in on one client
● Allowed to log in on multiple clients

Allowed Number ○ Infinite
● Allowed Login Number

Limit Number 10 (2-100)

Step 6. When using HTTPS authentication, configure HTTPS parameters.



HTTPS Configuration

Client Certificate Certification ☑ Enable

Trusted CA skyeyekx *

Local Certificate skyeyeca *

Advanced Configuration ^

NAT Detection ☑ Enabled (effective only for client)

Client Heartbeat Timeout 180 (60-86400 Seconds)

Forced Re-login Interval 0 (10-1440 minutes, 0 indicates no re-login interval)

Redirect URL (1-255 Characters)

Current Chinese Background

Current English Background

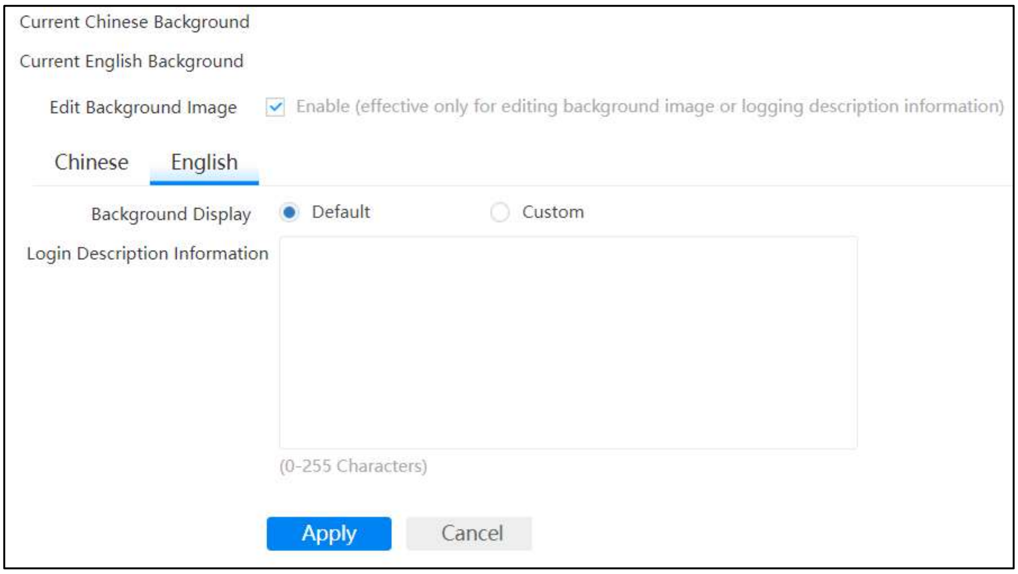
Edit Background Image □ Enable (effective only for editing background image or logging description information)

Parameter	Description
Client certificate authentication	After "Client Certificate Authentication" is enabled, the client's certificate will be verified during the authentication process.
Trusted CA	The certificate of the CA center. The CA centers authenticated by the client and the firewall must be the same.
Local certificate	The certificate of the firewall.
Advanced	
NAT detection	When a user uses the client authentication method, it will detect whether the client has passed through NAT.
Client heartbeat timeout	Client heartbeat timeout time, if the client still does not respond after the set time, the firewall considers the client to be offline.

Parameter	Description
Forced re-login interval	No matter whether the client has traffic or not, the online user will be required to re-authenticate once the mandatory re-login interval expires. 0 means that the forced re-login function is not enabled.
Redirect URL	Optional. the HTTPS authentication is passed, the redirection URL page is automatically pushed to the user.

Step 7. Customize the background in Chinese and English.

Select the "Enable" check box of "Edit Background Image" to set the background in Chinese and English. Users can customize the background image and login description information.



Current Chinese Background

Current English Background

Edit Background Image ☑ Enable (effective only for editing background image or logging description information)

Chinese English

Background Display ● Default ○ Custom

Login Description Information

(0-255 Characters)

Step 8. After the configuration is complete, click “OK”.

6.3.4 Configure URL Redirection

This function is used to redirect the URL of intranet users. Push webpages to users matching the URL redirection policy.

Step 1. Choose “Policy > Security Authentication > URL Redirection”.

Step 2. Select “Enable” to enable the URL redirection authentication function.

URL redirection authentication function is disabled by default. After the URL redirection authentication function is enabled, intranet users will only match the URL redirection authentication policy when surfing the Internet.

Step 3. Configure the HTTP port provided by the firewall to client URL redirection.

The default port number is 65081. The value range of the port is 1025 ~65535. Users can customize the port number.

Step 4. Configure time policy.

Parameter	Description
User timeout redirection	• Select "No data traffic during this period" and set the time period. During the specified time, if the user has no data traffic, a redirection URL will be pushed to the user. The time range ranges from 10 to 1440 minutes. • Select "Beyond this period" and set the time period. If the user surfs the Internet for more than this period of time, a redirection URL will be pushed to the user. The time range ranges from 10 to 1440 minutes.
Redirection page duration	Specify the hold time for redirected pages, and the default is 30 seconds. Users cannot close the redirected page during the hold time. The value range is 0 to 60 seconds.

Step 5. Configure the push method.

Push mode supports manual clicking and auto skipping.

- Push the redirection URL to the user in manual clicking mode, and the user will enter the corresponding page after clicking.
- The auto skipping method pushes the redirection URL to the user and directly jumps to the corresponding page.

Step 6. After the configuration is complete, click “OK”.

6.4 User Monitoring

This section introduces the user lists of authenticated users, VPN users, and 802.1x users and how to delete these users.

6.4.1 Secure Authentication User

Users who have passed security authentication can be viewed on the "Data Center > Monitor > User Monitoring > Security Authentication User" page.

View Security Authentication Users

The security authentication user list displays the user name, user type, peer address, local address, authentication server, number of logins and online time. The peer address is the address of the security authentication user. If the address does not pass through the NAT device, the address may be the user's host IP address. If the address passes through the NAT device, the address may be the converted IP address.

The users in the security authentication user list are valid for a period of time and do not need to be authenticated again. The time is controlled by the "Forced re-login interval " configured in Web authentication. The user must re-authenticate after timeout.

Query Security Authentication Users

By default, all security authentication users are queried, and you can use the first drop-down box to set to query only security authentication users of the "WEB authentication" or "URL redirection" type. Enter the query keyword in the query content text box, and click 🔍 to query the security authentication users matching the keyword.

Security authentication user query supports fuzzy search, and the fields support user name, user type, peer address, local address, and authentication server keywords.

Delete Security Authentication User

After selecting a user, click "Delete" to manually cancel the relationship between the user name and IP. The users deleted from the security authentication user list must be authenticated again.

6.4.2 L2TP VPN

After the remote client dials into the L2TP VPN tunnel, the dialed user information can be viewed in "Data Center>Monitor>User Monitoring>L2TP VPN User", and the dialed user can be deleted.

The L2TP VPN user list displays the username, client IP (the public network address after NAT when passing through the NAT device), tunnel name, received data, sent data, and online duration of the L2TP VPN user.

By selecting a user and clicking “Delete”, the relationship between the username and IP can be manually terminated. The users removed from the L2TP VPN user list must be authenticated again.

6.4.3 PPTP VPN

After the remote client dials into the PPTP VPN tunnel, you can view the dial-in user information in "Data Center > Monitor > User Monitoring > PPTP VPN User", and you can delete the dial-in user.

The PPTP VPN user list displays the PPTP VPN user 's user name, client IP (when passing through a NAT device, it is the public network address after NAT), tunnel name, received data, sent data, and online time.

After selecting a user, click "Delete" to manually cancel the relationship between the user name and IP. The users deleted from the PPTP VPN user list must be authenticated again.

7 Security

Compared with traditional firewalls, smart firewalls provide you with more flexible and adjustable configuration and comprehensive attack protection functions, including network layer attack protection, application layer attack protection, LAN broadcast protection, and DHCP protection. These attack protection functions are used to filter and prevent abnormal packets or attack packets from flowing into your intranet. Once abnormal packets or attack packets flow into the intranet, it will not only exhaust the resources of your server and make the server unable to work normally, but also affect your entire network and cause network congestion. These are the most common and commonly used attack methods in the network.

7.1 Black/White List

7.1.1 Address Blacklist

The address blacklist is an effective means to reject certain illegal IP address or MAC address traffic.

After the firewall interface receives the packet, it first performs blacklist matching. When the IP and MAC addresses in the traffic match the address blacklist policy, the packets will be directly discarded by the firewall.

Step 1. Select “Policy > Black/White List".

Step 2. Click “Add”.

Step 3. Configure the blacklist parameters.

Specify the IP address or MAC address of the address blacklist, and you can specify the effective time.

If "Enable" is selected, the address blacklist will take effect. Otherwise, it will not take effect.

The IP address can be either an IPv4 address or an IPv6 address.

Step 4. After the configuration is complete, click “OK”.

7.1.2 Domain Name Black/White list

The firewall supports black and white lists of domain names. When a user accesses a domain name added to the whitelist, there is no need for content security detection such as AV or IPS, nor is there any need for intelligence detection. When a user accesses a domain name added to the blacklist, the traffic is directly denied. For traffic that does not hit the whitelist or blacklist, it is directly processed according to the normal firewall process.

The domain name whitelist has higher priority than domain name blacklist. If a domain name has been added to the whitelist and then added to the blacklist, the corresponding blacklist will not take effect.

Add Domain Name Blacklist

Step 1. Select “Policy > Black/White List ".

Step 2. Select "Domain Name Blacklist and White List ".

Step 3. Click “Add”.

Step 4. Select "Blacklist" as the type to add a blacklist rule; select "Whitelist" as the type to add a whitelist rule.

Step 5. Enter the domain name to “Add”.

A domain name blacklist and whitelist policy supports only one domain name, and does not support the wildcard character "*".

Step 6. If “Enable” is selected, the black and white list will take effect. Otherwise, it will not take effect.

If “Enable” is not selected, you can also enable the blacklist or whitelist in the domain name blacklist and whitelist.

Step 7. After the configuration is complete, click “OK”.

Enable or Disable a Blacklist or Whitelist

Find a desired whitelist or blacklist, and enable or disable the corresponding whitelist or blacklist by checking or unchecking the "Enable" checkbox.

Batch Enable or Disable Blacklist and Whitelist

Select multiple blacklists and blacklists, and click “Enable” or “Disable”.

Filter or Query Black and White Lists

Through the "Type" drop-down box on the right, you can set to display "all types", "blacklist" or "whitelist", and through the "status" drop-down box, you can set to display "all status", "enable" or "disable" black and white list.

Enter a domain name keyword in the query box to query the black and white lists containing the domain name.

7.2 Attack Protection

The firewall protects servers in the security domain from attacks. After receiving the packet, the firewall first matches the blacklist. The packets that do not hit the blacklist continue to be detected for attack protection. After entering the attack protection module, first check whether the destination address of the packet is added to the attack protection whitelist. If it is added to the whitelist, it is skipped. The attack protection process directly proceeds to the next step of inspection. Otherwise, the attack protection detection is performed. If it hits the attack, it will be dealt with according to the specified action. When the firewall works in interface bypass mode, the firewall will detect attacks and generate logs, but will not block them.

The firewall supports attack protection against SYN Flood, ICMP Flood, UDP Flood, IP Flood, Tracer t, IP scan, port scan, IP spoofing, abnormal packet attack, HTTP Flood, and DNS Flood. By enabling and configuring the attack protection module, users can effectively filter and take corresponding measures to prevent abnormal packets or attack packets from flowing into the user's intranet.

7.2.1 Attack Protection Whitelist

The addresses added to the attack prevention whitelist will not be detected by attack prevention.

Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Configure the attack protection options and specific values to be enabled.

Step 5. Configure a whitelist.

Click the "Address" selection box, and select an address object or an address group object from the drop-down menu. If there is no suitable address object or address group object, click the “Add” button on the right to add it.

Step 6. After the configuration is complete, click “OK”.

7.2.2 SYN Flood Attack Protection

TCP packets establish connections through a three-way handshake. SYN Flood uses this principle to establish a large number of incomplete TCP connections, thereby exhausting the resources of the attacked host.

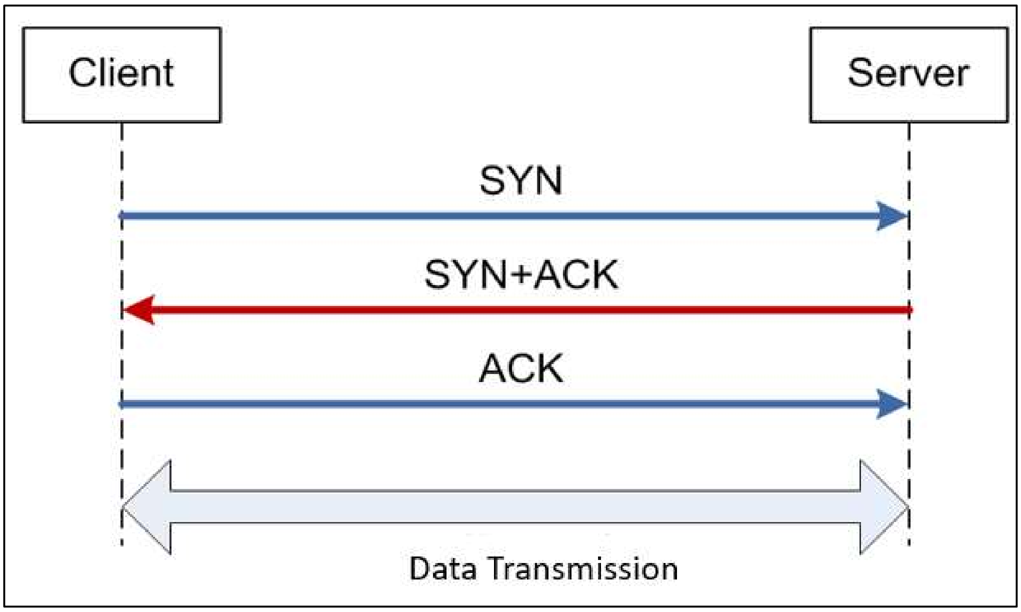
Normal TCP Three-way Handshake Process

The TCP protocol establishes the TCP connection through a three-way handshake. The establishment steps are as follows:

Step 1. The client sends a TCP packet containing the SYN flag, that is, a SYN synchronization message, which indicates the port used by the client and the initial sequence number of the TCP connection.

Step 2. After receiving the SYN packet from the client, the server will return a SYN+ACK packet, indicating that the client's request is accepted, and the TCP sequence number is incremented by 1. At the same time, certain resources are allocated in the server system for subsequent use of this link.

Step 3. The client also returns a confirmation packet ACK to the server, and the TCP sequence number is also increased by 1, and a TCP connection negotiation is completed.



SYN Flood Attack Principle

The attacker sends a large number of TCP packets with the SYN flag to the target host, and the target host replies with a TCP packet with the SYN+ACK flag, and waits for the attacker to reply with the TCP with the ACK flag to establish a three-way handshake. After the attacker sends a large number of TCP packets containing the SYN flag, he will not proceed to the next step. As a result, server resources are heavily occupied and cannot be released, and services can no longer be provided to normal users.

Configure SYN Flood Attack Defense

The firewall supports SYN Flood attack protection through the SYN Flood alarm value flow limit and SYN proxy mode. It is recommended to configure these two methods at the same time to save connection resources and allow normal users to pass through.

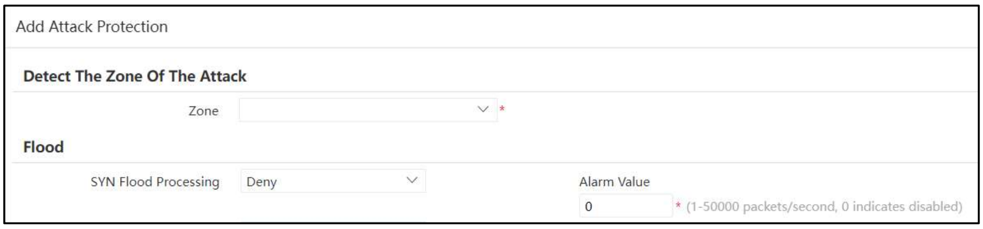
Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Configure the SYN Flood alarm value.


Add Attack Protection

Detect The Zone Of The Attack

Zone *

Flood

SYN Flood Processing: Deny

Alarm Value: 0 * (1-50000 packets/second, 0 indicates disabled)

The threshold value is the number of TCP connections allowed to be created per second. The alarm value is calculated for a single destination IP. When it is detected that the TCP connections to a certain server exceeds the alarm value, the SYN packets requesting to establish a connection with the sending server are discarded or alarmed. Select "Alarm" to process, and record the log and generate alarms only for the attack packets exceeding the alarm value, but do not discard them.

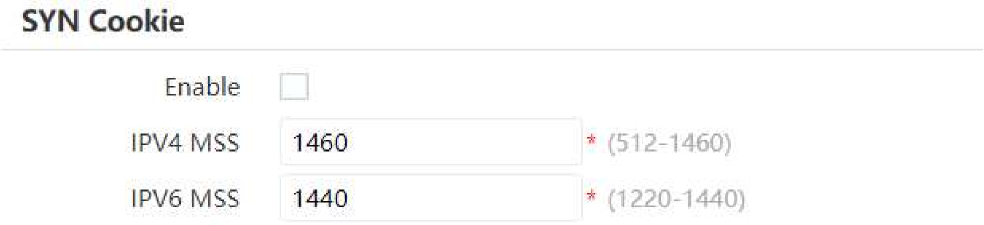
The SYN Flood alarm value defaults to 0, that is, the function is not enabled by default.

The setting of the alarm value is very important, please set an appropriate alarm value according to the actual traffic conditions in the network.

Step 5. Configure the SYN proxy.

The principle of the SYN proxy method is to receive a SYN packet at the firewall, send a SYN+ACK packet instead of the destination host, and calculate a cookie value based on the SYN packet. If the attacker is a forged IP address, the firewall will not respond with an ACK packet. If it is a normal user, it will respond with an ACK packet. The firewall checks the validity of the ACK packet based on the cookie value. After the check is passed, a TCP connection is established.

SYN Cookie method is disabled by default, and this function is enabled after selecting the "Enable" check box. Hit SYN Flood attacks will be discarded and logged.


SYN Cookie

Enable □

IPV4 MSS: 1460 * (512-1460)

IPV6 MSS: 1440 * (1220-1440)

MSS (Maxitum Segment Size) refers to the maximum transmission size in TCP transmission. The IPv4 MSS value is the MTU value minus 20 bytes of the IP header and 20 bytes of the TCP header, so it is usually 1460. The IPv6 MSS value is the MTU value minus 4 0 bytes of the IP header and 20 bytes of the TCP header, so it is usually 1440.

Step 6. After the configuration is complete, click “OK”.

7.2.3 ICMP Flood Attack Protection

ICMP Flood Attack Principle

The attacker sends massive ping request packets to the target server, and the server needs to occupy resources to respond to these massive ping packets, causing the server to be unable to process normal data, or even provide services to normal users.

Configure ICMP Flood Attack Defense

Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

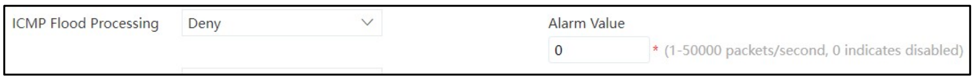
Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Configure the ICMP Flood alarm value.

The threshold value is the number of new ICMP sessions allowed per second. The alert value is calculated for a single destination IP. When it detects that the number of new sessions of ICMP packets to access a certain server exceeds the alarm value, the packets will be discarded or alarmed. Select "Alarm" to process, and record the log and generate alarms only for attack packets exceeding the alarm value, but do not discard them.

The ICMP Flood alarm value defaults to 0, that is, the function is not enabled by default.



ICMP Flood Processing: Deny

Alarm Value: 0 * (1-50000 packets/second, 0 indicates disabled)

Step 5. After the configuration is complete, click “OK”.

7.2.4 UDP Flood Attack Protection

UDP Flood Attack Principle

UDP Flood is a bandwidth attack. Malicious users send a large number of UDP packets to the target server through a botnet. Such UDP packets are usually large packets and the rate is very fast, which usually causes the following hazards:

- Consume network bandwidth resources and cause link congestion in severe cases.
- A large number of UDP Floods that change sources and ports will lead to performance degradation of network devices that rely on session forwarding and even session exhaustion, resulting in network paralysis.

Configure UDP Flood Attack Defense

Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

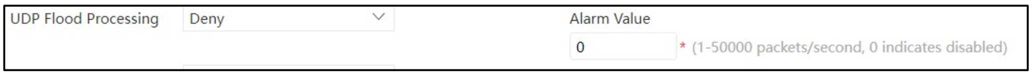
Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Configure the UDP Flood alarm value.

The alarm value is the number of the UDP sessions allowed per second. The alarm value is calculated for a single destination IP. When it detects that the number of new sessions of UDP packets accessing a certain server exceeds the alarm value, the packets are discarded, alarmed, or intelligently defended. Select "Alarm" to process, and record the log and generate alarms only for attack packets exceeding the alarm value, but do not discard them.

The UDP Flood alarm value defaults to 0, that is, this function is not enabled by default.



UDP Flood Processing: Deny

Alarm Value: 0 * (1-50000 packets/second, 0 indicates disabled)

Select "Intelligent Defense" processing, you can count the number of UDP packets based on the characteristics of UDP packets. The intelligent defense process is based on the following rules: when an attacker uses tools to generate UDP floods, a large number of UDP packets have the same characteristics, but UDP packets normally sent by users do not. Through intelligent defense, malicious UDP floods can be distinguished from normal user UDP requests, so that normal user UDP requests can pass through the firewall.

The intelligent defense processing process is that when the UDP packets passing through the firewall within 1 second reach the alarm value, the received UDP packets will trigger the intelligent defense processing and record the characteristics of the newly received UDP packets. When the cumulative number of received UDP packets with the same characteristics reaches the alarm value, it is considered that a UDP flood has occurred. Discard and log UDP packets with corresponding characteristics exceeding the alarm value. When the received UDP packets with the same characteristics do not reach the alarm value, the UDP packets will be released and recorded in the log.

Step 5. After the configuration is complete, click “OK”.

7.2.5 IP Flood Attack Protection

IP Flood Attack Principle

The attacker sends massive IP packets to the target server, and the server needs to occupy resources to respond to these massive IP packets, causing the server to be unable to process normal data, or even provide services to normal users.

Configure IP Flood Attack Defense

Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

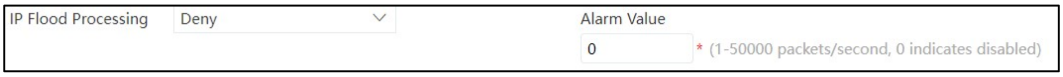
Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Configure the IP Flood alarm value.

The alarm value is the number of IP new sessions allowed per second. The alarm value is calculated for a single destination IP. When it detects that the number of new sessions of IP packets accessing a certain server exceeds the alarm value, the packets are discarded or alarmed. Select "Alarm" to process, and log and generate alarms only for attack packets exceeding the alarm value, but do not discard them.

The IP Flood alarm value defaults to 0, that is, the function is not enabled by default.



IP Flood Processing: Deny

Alarm Value: 0 * (1-50000 packets/second, 0 indicates disabled)

Step 5. After the configuration is complete, click “OK”.

7.2.6 Malicious Scan Protection

Overview

- IP address scanning attack

  Use the scanning software to send a large number of address request broadcast packets to scan the addresses in the network.

- Port scan attack

  Using scanning software to send a large number of port detection packets to scan the opened ports on the host is the most common preparation work for hackers to attack.

Configure Malicious Scan Protection

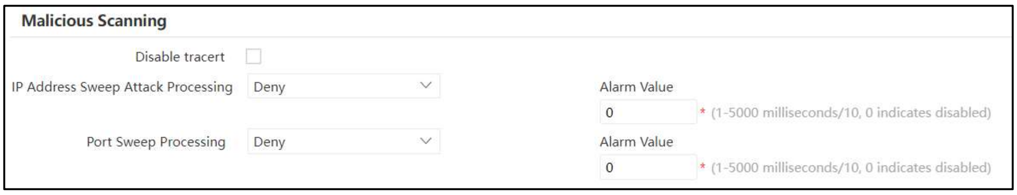
Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Configure the malicious scan protection.



Malicious Scanning

Disable tracert □

IP Address Sweep Attack Processing: Deny

Alarm Value: 0 * (1-5000 milliseconds/10, 0 indicates disabled)

Port Sweep Processing: Deny

Alarm Value: 0 * (1-5000 milliseconds/10, 0 indicates disabled)

Select the “Disable tracert” check box to prohibit tracert packets from passing through the security zone and record logs. Disabling tracert packets can hide network paths and IP addresses, thereby preventing attackers from obtaining IP addresses through tracert.

The firewall supports protection against IP address scanning attacks and port scanning attacks through flow limiting.

When the detected scanning packets exceed the alarm value, corresponding processing is performed on the scanning packets exceeding the alarm value. The alarm value is the time interval for sending every ten packets. 0 means no protection settings for this type of attack.

IP address scanning attack defense and port scanning attack defense support discarding and alarm processing.

- Select "Discard" to process, and the attack packets exceeding the alarm value will be discarded and recorded in the log.
- If "Alarm" is selected, after the alarm value is exceeded, only the log will be recorded and an alarm will be generated, but the packet will not be discarded.

Step 5. After the configuration is complete, click “OK”.

7.2.7 Spoof Protection

Overview

IP spoofing, using the IP address is not fixed with the MAC when it leaves the factory, the attacker uses self-encapsulation and modifying the IP address of the network node to impersonate the IP address of a trusted node to attack. There are three main consequences of IP spoofing:

1. Paralyze the trusted host that really has an IP, and pretend to be a trusted host to attack the server
2. Lead to man-in-the-middle attacks
3. Lead to DNS spoofing and session hijacking

The firewall supports two ways to prevent IP spoofing.

- Determine whether the IP address is fake based on the security zone where the device is located

  Bind IP addresses and security zones by configuring IP security zone associations. The firewall detects the security zone of the passing traffic IP address. When the actual security zone of the IP address is inconsistent with the associated security zone, the user is regarded to have forged the IP address. The firewall will block its access, drop the packet and record the log.

- Use the MAC address of the device to determine whether the IP address is forged

  The firewall performs MAC address detection on the IP addresses of passing traffic. When the MAC address of the IP address is inconsistent with the MAC address in the IP-MAC binding, it is considered that the user forged the IP address. The firewall will block its access, drop the data packet and record the log.

  The static IP-MAC binding added by users have a higher priority than IP-MAC bindings detected by DHCP. If the IP-MAC binding entry is not matched, execute the unbound policy.

Configure Spoof Protection

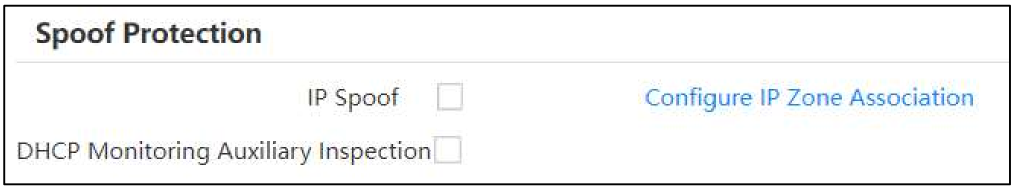
Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Configure spoof protection.



Spoof Protection

IP Spoof □ Configure IP Zone Association

DHCP Monitoring Auxiliary Inspection □

Select the "IP Spoof" check box to enable IP spoofing protection, and support both IP v4 and IPv6 spoofing protection. When the corresponding relationship between the source IP and the source MAC address of the packet received by the firewall is matched in the IP-MAC binding list, the packet is allowed to pass through; Whether the packet is denied or allowed.

Configure IP security zone association. The firewall detects the IP address and security zone of the data flow. If it does not match the settings associated with the IP security zone, it considers the IP spoofing, discards the packet, and records the log.

Select the "DHCP Monitoring Auxiliary Inspection" check box to enable DHCP auxiliary detection. DHCP will automatically detect the IP-MAC correspondence. If the user enables the IP-MAC address binding function, the IP-MAC address binding function takes precedence over the DHCP monitoring auxiliary inspection function. If there is no hit in the binding list and the DHCP monitoring list, it is judged according to the IP-MAC unbound policy whether the packet is denied or allowed to pass. If the user does not configure the IP-MAC unbound policy, when the corresponding relationship between the source IP and the source MAC address of the packet received by the firewall fails to match in the IP-MAC binding list and the DHCP monitoring list, the packet is allowed to pass through the firewall.

Step 5. After the configuration is complete, click “OK”.

Add IP Security Zone Association

The firewall supports preventing IP spoofing by binding the association between IP addresses/IP address segments and security zones. When enabling IP spoofing, users need to configure IP security zone association.

If the IP address in the IP security zone association list is accessed from a non-associated security zone, the firewall will block the data;

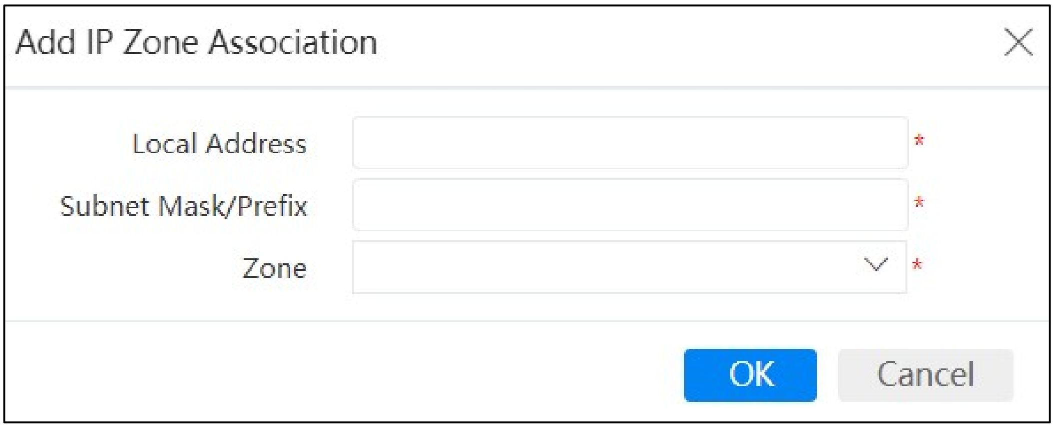
The IP addresses that are not in the IP security zone association list are not in the effective range of this function, and data will be allowed to pass through.

Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click the "IP Spoofing Settings " tab.

Step 3. Click “Add”.

Step 4. Specify an IP address and associated security zone.



Add IP Zone Association

Local Address *

Subnet Mask/Prefix *

Zone *

Parameter	Description
Local Address	Specify the IP address segment included in the security zone. Both IPv4 and IPv6 addresses are supported.
Subnet mask/prefix	Specify the netmask for an IPv4 subnet or the prefix for an IPv6 subnet.
Zone	Specify the security zone to which it belongs.

Step 5. After the configuration is complete, click “OK”.

7.2.8 Abnormal Packet Attack Protection

Overview

- Ping of Death

One of the common means of denial of service attacks. Since the maximum length of an IP packet cannot exceed 65535 bytes, Ping of Death changes the combination of its correct offset and segment length in the last segment so that the system always The length exceeds 65535 bytes, causing memory overflow of the target server and eventually crashing.

- Teardrop

One of the common means of denial of service attacks. Teardrop is a pathological fragmentation packet attack method based on UDP. Its working principle is to send multiple fragmented IP packets to the victim. Some operating systems may experience system crashes, restarts, and other phenomena when they receive forged fragmented packets containing overlapping offsets.

- IP option

There are many options in the IP packet header, and these options are all prepared for a certain function. The attacker has achieved the purpose of attacking the target server by carefully constructing the value of the option in the IP packet header. Different options can implement different attack methods.

- TCP exception

There are many options in the TCP packet header, and these options are all prepared for a certain function. The attacker has achieved the purpose of attacking the target server by carefully constructing the value of the option in the TCP packet header. Different options can implement different attack methods.

- Smurf

The attacker sends a ping echo request packet whose source address is the broadcast address to the target server. When the target server responds to this packet, it will reply to a broadcast address. In this way, all computers on the local network must process these broadcast packets. If the attacker sends enough echo request packets, the generated replay broadcast packets may flood the entire network. In addition to setting the source address of the echo packet as a broadcast address, the attacker may also set the source address as a subnet broadcast address, so that the computer where the subnet is located may be affected.

- Fraggle

Fraggle attack is that the attacker sends a UDP packet to the broadcast address, the destination port number is 7 (ECHO) or 19 (Chargen), and the source IP address of the packet is disguised as the IP address of the target server. In this way, all computers in the broadcast domain with this function enabled will send response packets to the server, thereby generating a large amount of traffic, causing the server's network to be blocked or the victim host to crash.

- Land

The LAND attack packet is that the attacker sends a TCP SYN message whose source IP address and destination IP address are both the IP address of the target server to the target server, so that the target server will send an ACK packet to itself after receiving the SYN packet., and establishes a TCP connection control structure. If the attacker sends enough SYN packets, the resources of the target server may be exhausted, and it may even be unable to provide services to normal users.

- Winnuke

The WinNuke attack uses a vulnerability in the WINDOWS operating system to send some packets carrying TCP out-of-band OOB data to port 139 used by NetBIOS. These attack packets are different from normal packets carrying OOB data, and their pointer fields do not match the actual location of the data. That is, there is overlap, so that the WINDOWS operating system will crash when processing these data.

- DNS exception

Attacks using abnormal DNS packets that do not comply with RFC standards. The firewall will pass through the DNS packets that meet the RFC standard, and discard the non-compliant ones.

- IP Fragmentation

A data fragmentation-based attack method that uses malicious operations to send extremely small fragmentations to bypass packet filtering systems or intrusion detection systems. Attackers can distribute TCP headers (usually 20 bytes) in two fragmentations through malicious operations, so that the destination port number can be included in the second fragmentation.

For a security device with an imperfect detection mechanism, the permission/prohibition measure is firstly adopted by judging the destination port number. However, since the destination port number is located in the second fragment through malicious fragmentation, it is determined whether subsequent fragments are allowed to pass by judging the first fragment. But these fragments will form various attacks after being reorganized on the target host. In this way, some intrusion detection systems and some security filtering systems can be circumvented.

Configure Abnormal Packet Attack Defense

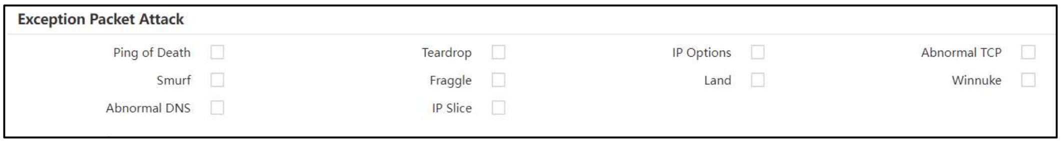
Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Configure exception packet attack defense.



Exception Packet Attack

Ping of Death □ Teardrop □ IP Options □ Abnormal TCP □

Smurf □ Fraggle □ Land □ Winnuke □

Abnormal DNS □ IP Slice □

For abnormal packet attacks, the firewall will identify abnormal packets based on the data packet structure. Abnormal packet attack defense supports both IPv4 and IPv6.

Select the check box corresponding to the abnormal packet type will enable the corresponding abnormal packet identification function, and the hit abnormal packet will be discarded and recorded in the log.

Step 5. After the configuration is complete, click “OK”.

7.2.9 ICMP Control

Overview

- ICMP Fragmentation

The attacks based on ICMP fragmentation, usually, because each device interface limits the size of the MTU, which is generally 1492 or 1500 bytes, and the length of a normal ICMP packet will not exceed 1500 bytes, so it will not be fragmented.

- Route redirection packet

Use ICMP redirection technology to attack and eavesdrop on the network. If host A supports ICMP redirection, then host B sends an ICMP redirection to host A, and then all packets sent by host A to the specified address will be forwarded to host B, so that host B can achieve the purpose of eavesdropping. The windows operating system will check the ICMP packet. If the redirection is not sent by the gateway, it will be discarded directly. But it is easy to forge a gateway packet. If many fake ICMP redirection packets are intentionally forged, the routing table of the host may be changed into a mess.

- ICMP Jumbo Packet

ICMP packet length limit. The ICMP packets exceeding the specified length will be discarded by the firewall.

Configure ICMP Control

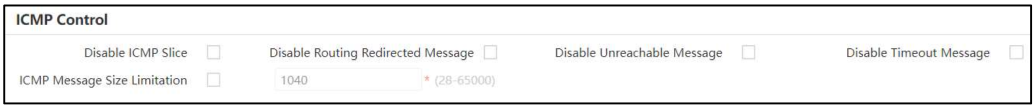
Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Configure ICMP control.



ICMP Control

Disable ICMP Slice □ Disable Routing Redirected Message □ Disable Unreachable Message □ Disable Timeout Message □

ICMP Message Size Limitation □ 1040 * (28-65000)

For ICMP packet attacks, the firewall will prohibit ICMP packet fragmentation, route redirection packets, unreachable packets, timeout packets, and limit the size of ICMP packets according to the ICMP packet structure.

The ICMP packet size includes ICMP packet data + ICMP packet header + IP header. ICMP packets smaller than or equal to the ICMP packet size limit can pass through the firewall, and ICMP packets larger than the ICMP packet size limit are discarded and logged.

Step 5. After the configuration is complete, click “OK”.

7.2.10 ICMPv6 Control

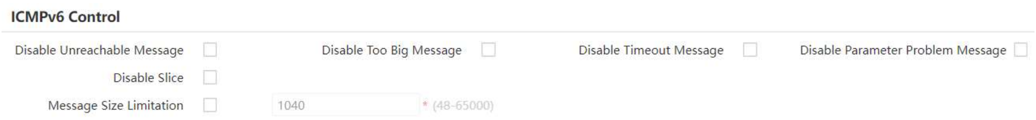
Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Configure ICMPv6 control.



ICMPv6 Control

Disable Unreachable Message □ Disable Too Big Message □ Disable Timeout Message □ Disable Parameter Problem Message □

Disable Slice □

Message Size Limitation □ 1040 * (48-65000)

For ICMPv6 packet attacks, the firewall will prohibit ICMPv6 unreachable packets, packet too large packets, timeout packets, parameter problem packets, packet fragmentation, and limit the size of ICMP packets.

The ICMP v6 packet size includes ICMPv6 packet data + ICMPv6 packet header + IPv6 header. ICMP packets that are smaller than or equal to the ICMPv6 packet size limit can pass through the firewall, but ICMPv6 packets that are larger than the ICMPv6 packet size limit will be discarded and logged.

Step 5. After the configuration is complete, click “OK”.

7.2.11 IPv6 Extension Header Protection

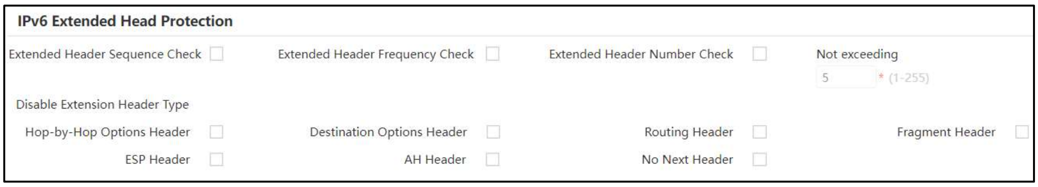
Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Enable IPv6 extension header security detection.



IPv6 Extended Head Protection

Extended Header Sequence Check □ Extended Header Frequency Check □ Extended Header Number Check □ Not exceeding 5 * (1-255)

Disable Extension Header Type

Hop-by-Hop Options Header □ Destination Options Header □ Routing Header □ Fragment Header □

ESP Header □ AH Header □ No Next Header □

IPv6 extension header protection supports extension header sequence detection, extension header frequency detection, extension header number detection (default no more than 5, maximum no more than 255) and prohibition of certain extension header types. The extended header types that can be prohibited include hop-by-hop options, destination address options, routing options, fragmentation options, ESP options, AH options, and None options.

Step 5. After the configuration is complete, click “OK”.

7.2.12 Application Layer Flood Attack Protection

Overview

- DNS Flood

Send a large number of domain name resolution requests to the attacked server. Usually, the domain name requested for resolution is randomly generated or does not exist on the network. When the attacked DNS server receives the domain name resolution request, it will first check whether there is a corresponding cache. If the domain name cannot be found and the domain name cannot be directly resolved by the server, the DNS server will recursively query the domain name information to its upper-level DNS server. The process of domain name resolution brings a lot of load to the server, and if the number of domain name resolution requests per second exceeds a certain number, the DNS server will refuse to serve.

- HTTP Flood

Application-layer attacks specifically targeting HTTP services. By simulating a large number of users, the attacker continuously accesses HTTP pages, even those pages that require a large amount of data operations and consume a large amount of CPU, which eventually leads to overloading of the HTTP server, and denial of service.

Configure Application Layer Flood Attack Defense

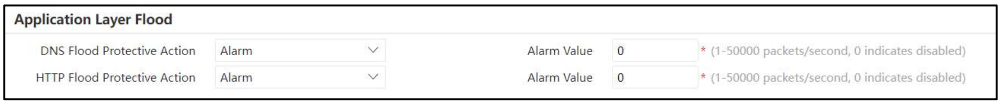
Step 1. Choose “Policy > Dos Protection > Attack Defense”.

Step 2. Click “Add”.

Step 3. Select a security zone.

Attack defense policies are based on security zones. Users can configure attack defense policies for each security zone.

Step 4. Configure application layer Flood attack defense.



Application Layer Flood

DNS Flood Protective Action	Alarm	Alarm Value	0	* (1-50000 packets/second, 0 indicates disabled)
HTTP Flood Protective Action	Alarm	Alarm Value	0	* (1-50000 packets/second, 0 indicates disabled)

- DNS Flood Protection Action

Alarm: After reaching the alarm value, the packets that hit the DNS Flood protection policy will only generate alarm logs.

Deny: After reaching the alarm value, the packets that hit the DNS Flood protection policy will not only generate an alarm log, but will also be discarded by the firewall.

Command defend: After reaching the alarm value, the packets that hit the DNS Flood protection policy will be protected by the technology of discarding the first packet. The applicable scenario is a large number of random DNS requests initiated by a large number of random sources.

Enhanced defend: After reaching the alarm value, the packets that hit the DNS Flood protection policy will be protected by TC rebound technology. Enhanced protection can fine-grained separate attackers and normal users, but may require more DNS server resources.

Authorized server defend: It is specially protected against the authorization server. After reaching the alarm value, the packets that hit the DNS Flood protection policy will be protected by ns redirection technology.

- HTTP Flood Protection Action

Alarm: After reaching the alarm value, the packets that hit the HTTP Flood protection policy will only generate alarm logs.

Discard: After reaching the alarm value, the packets that hit the HTTP Flood protection policy will not only generate an alarm log, but will also be discarded by the firewall.

Common defend: After reaching the alarm value, the packets that hit the HTTP Flood protection policy will be protected by automatic redirection technology. It is suitable for the attacker who has not fully implemented the HTTP protocol stack, but uses attack tools to make a large number of HTTP get requests, and cannot respond to redirection.

Enhanced defend: After reaching the alarm value, the packets that hit the HTTP Flood protection policy will be protected by manual confirmation technology. Fully distinguish between attackers and users, requiring users to manually confirm access.

Step 5. After the configuration is complete, click “OK”.

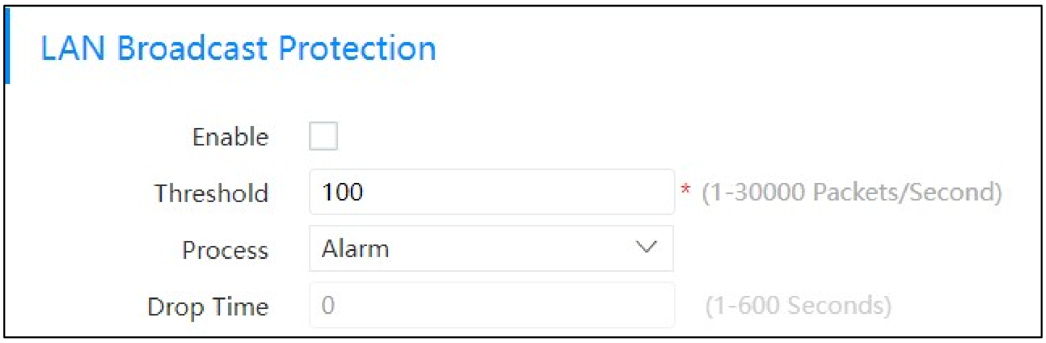
7.3 LAN Broadcast Protection

The firewall supports globally configured LAN broadcast protection and LAN broadcast protection based on L2 interfaces, which can prevent the flooding of broadcast and multicast data packets in the LAN and ensure normal network communication.

Users can limit the threshold of multicast and broadcast packets passing through the firewall per second through global settings or interface settings, and process the part exceeding the threshold.

Step 1. Choose “Policy > Dos Protection > LAN Broadcast Protection”.

Step 2. Configure global LAN broadcast protection.



LAN Broadcast Protection

Enable □

Threshold 100 * (1-30000 Packets/Second)

Process Alarm

Drop Time 0 (1-600 Seconds)

Parameter	Description
Enable	Select the "Enable" check box to enable the global setting function. All multicasts and broadcasts passing through the firewall, no matter which interface receives them, will be accumulated. The global configuration can quickly set the L2 physical interface and aggregated interface, and it will take effect on the current vsys.
Threshold	How many multicast and broadcast packets the firewall allows to forward per second. When configured as 100, it means that the firewall can forward 100 multicast and broadcast packets per second. The parts that exceed the threshold will be processed according to the behavior selected in processing.
Process	• Deny, the part that exceeds the threshold will generate an alarm log and discard it.

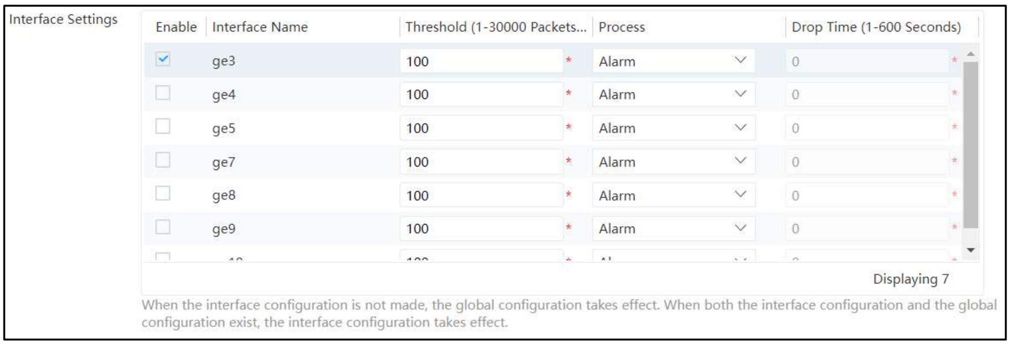
Parameter	Description
	• Alarm, the part that exceeds the threshold will generate an alarm log and release it. • Block, prohibit broadcast and multicast packet forwarding within the blocking time, and output alarm information.
Drop time	When the processing is selected as "Block", the user needs to specify the blocking time. Forwarding will resume after the blocking time has elapsed. The value range is 1-600 seconds.

Step 3. Configure interface-based LAN broadcast protection.

Set a separate LAN broadcast protection for each interface working on the second layer. The parameters of the interface-based LAN broadcast protection configuration are consistent with those of the global configuration. The configuration takes effect only on the corresponding interface.

Notes

When the interface settings are not configured, the global configuration takes effect. The interface settings take effect when the interface configuration and the global configuration exist at the same time.



Interface Settings

Enable	Interface Name	Threshold (1-30000 Packets...	Process	Drop Time (1-600 Seconds)
☑	ge3	100 *	Alarm	0 *
□	ge4	100 *	Alarm	0 *
□	ge5	100 *	Alarm	0 *
□	ge7	100 *	Alarm	0 *
□	ge8	100 *	Alarm	0 *
□	ge9	100 *	Alarm	0 *

Displaying 7

When the interface configuration is not made, the global configuration takes effect. When both the interface configuration and the global configuration exist, the interface configuration takes effect.

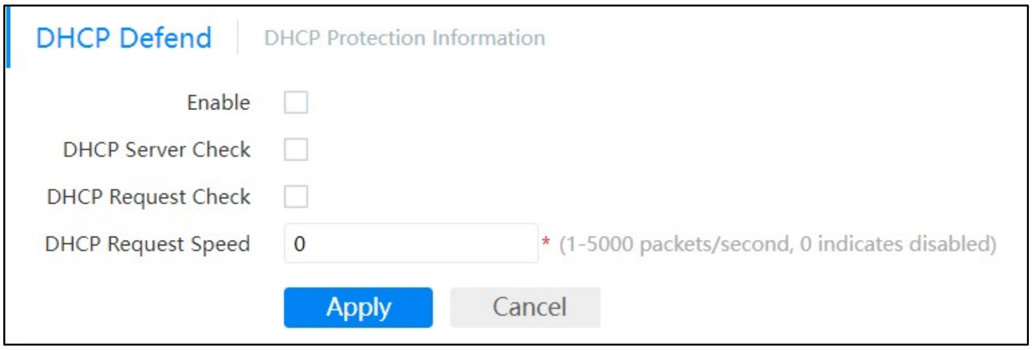
Step 4. After the configuration is complete, click “Apply”.

7.4 DHCP Protection

7.4.1 DHCP Protection

When the firewall works on the second layer and is located between the DHCP server and the DHCP client, the user can enable the DHCP function of the firewall to provide protection for DHCP through the DHCP server check and DHCP request check functions in the DHCP protection. The rate of DHCP request packets on the network is limited.

Step 1. Choose “Policy > Dos Protection > DHCP Defend”.



DHCP Defend | DHCP Protection Information

Enable □

DHCP Server Check □

DHCP Request Check □

DHCP Request Speed 0 * (1-5000 packets/second, 0 indicates disabled)

Step 2. Select the "Enable" checkbox to enable DHCP protection.

Step 3. Configure DHCP server check.

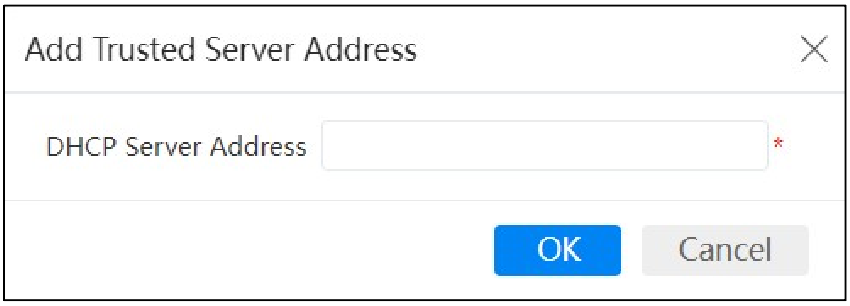
When the firewall monitors the DHCP request, it will check the reply packet of the DHCP server. If the DHCP server address in the DHCP server reply packet is not the address in the trusted DHCP server, it will reset the reply packet of the DHCP server.

1. Select the "DHCP Server Check " check box to enable DHCP server check.
2. Click “Add” to add trusted DHCP servers.

Up to 16 DHCP servers can be added.

3. Configure the trusted server address. After the configuration is complete, click “OK”.

The server address is an IPv4 address in dotted decimal notation.



Add Trusted Server Address

DHCP Server Address *

Step 4. Configure DHCP request checking.

Select the "DHCP request check " check box to enable DHCP request check.

The firewall will check the monitored DHCP request packet, mainly checking whether the MAC address of the client in the DHCP request is consistent with the source MAC address in the DHCP request packet, and if not, reset the DHCP request packet.

Step 5. Configure the DHCP request rate limit.

To limit the sending speed of DHCP requests, the user can specify how many DHCP request packets are allowed to pass per second. The default is 0, which means no rate limit for DHCP request packets, and 50 means that 50 DHCP request packets are allowed to pass per second, and the range is 0-5000 packets/second.

Step 6. After the configuration is complete, click “Apply”.

7.4.2 DHCP Protection Information

When the firewall works at L2 and is located between the DHCP server and the DHCP client, the firewall supports monitoring DHCP address allocation information. Users can view the client IP, client MAC, VLAN to which the client belongs, lease time and DHCP server IP address information assigned by the DHCP address in the DHCP protection information list.

Parameter	Description
Clear	Clicking the “Clear” button will clear all the content currently displayed in the DHCP monitoring information list.
Refresh	Refresh the list of DHCP monitoring information.
Client IP	The IP address assigned to the client by DHCP.
Client MAC	The client MAC address corresponding to the client IP address.
VLAN	The VLAN to which the client belongs.
Lease	The lease time of the IP address obtained by the client.
Server IP	A DHCP server that assigns IP addresses to clients.
Hit number	The number of hits for this piece of DHCP monitoring information.

7.5 IP-MAC Binding

Address binding is an effective means to prevent IP spoofing and IP address theft. Currently, the firewall supports manually adding IP-MAC bindings based on security zones, and supports users to directly bind the IP-MAC correspondence learned in the ARP table and detected in IP-MAC detection. It is also possible to directly bind the learned IPv6 neighbor and MAC address correspondence from the neighbor table.

After the firewall interface receives the packet, it first performs blacklist detection, attack protection detection, and then performs IP -MAC binding inspection.

7.5.1 Restrictions and Precautions

IP supports binding both unicast and multicast MAC addresses.

7.5.2 Manually Bind IP and MAC

Users can manually add IP-MAC address pairs for manual binding. When binding, it should be noted that the same MAC address can correspond to multiple IP addresses at the same time; but the same IP address cannot correspond to multiple MAC addresses at the same time.

Step 1. Select “Policy > IP-MAC Binding > Binding List".

Step 2. Click “Add”.

Step 3. Add a bound list item.

Parameter	Description
IP address	The IP address to be bound in the IP-MAC binding entry.
Description	Add a description of the IP and bound MAC to help users identify it.
MAC address	MAC address corresponding to the bound IP address. IP supports binding both unicast and multicast MAC addresses.
Zone	The security zone to which the IP-MAC binding entry belongs. The security zone can be set to any.

Step 4. After the configuration is complete, click “OK”.

The configured IP-MAC binding entries are displayed in the IP-MAC binding list. The user can view the number of hits for the bound IP-MAC address pair. When the IP-MAC address correspondence of the actual packet is inconsistent with the entry in the IP-MAC binding, the IP-MAC binding policy will be hit. If the number of hits is increased, the packet will be discarded; otherwise, the IP-MAC policy will not be matched, and the packet will be released.

7.5.3 Unbind IP-MAC

Find the desired IP-MAC entry in the IP-MAC list, and click “Delete”. The entry is deleted from the IP-MAC list, and the IP-MAC is also automatically unbound.

7.5.4 Configure an Unbound IP-MAC Policy

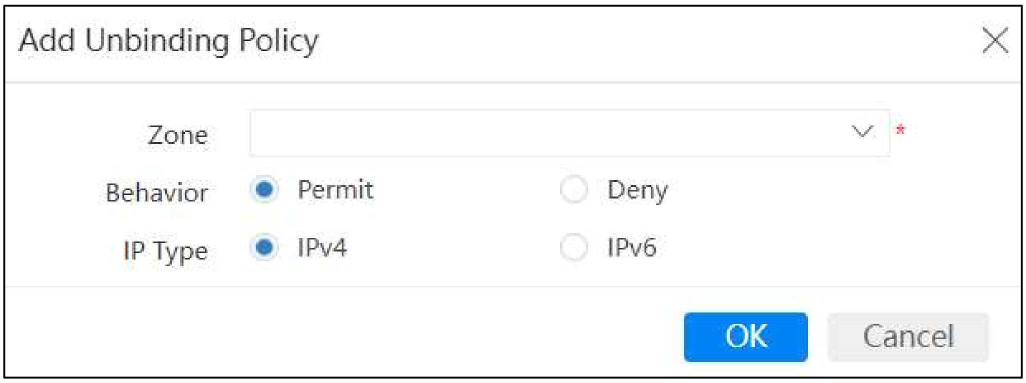
For the IP addresses not bound to the IP-MAC binding list, the user can customize whether the unbound IP addresses are allowed or forbidden to access.

The IP-MAC unbound policy needs to be added based on the security zone.

Step 1. Select “Policy > IP-MAC Binding > Unbinding Policy".

Step 2. Click “Add”.

Step 3. Configure the behavior and IP type of the unbound policy.



Add Unbinding Policy

Zone: *

Behavior: ● Permit ○ Deny

IP Type: ● IPv4 ○ IPv6

Parameter	Description
Zone	Select the security zone where the IP-MAC unbound policy is enabled. It must be a specific security zone, not any.
Behavior	• the action is "Allow", unbound IP-MAC addresses will be allowed to access. • If the action is "Deny", the unbound IP-MAC address will be denied access.
IP type	Select the IP type of the unbound policy, which is divided into IPv4 and IPv6.

Step 4. After the configuration is complete, click “OK”.

The configured IP-MAC unbound policy is displayed in the IP-MAC bound policy list. Users can view the hit count of unbound IP-MAC policies.

Click “Edit” to modify the behavior of the policy.

7.5.5 IP -MAC Detection

The firewall supports the IP-MAC detection function based on the specified range. Through the interface working in the routing mode (layer3), the user can detect the corresponding relationship between the active IP and the MAC address on the same network segment as the interface. At this time, the interface must join a specific security zone. If the security zone is any, it cannot be detected.

The detection range supports both IPv4 address ranges and IPv6 address ranges. Users can directly perform IPv4/IPv6 address binding operations in the detection results.

Step 1. Choose “Policy > IP-MAC Binding > Active Detection”.

Step 2. On the "IP -MAC detection" page, you can see all interfaces whose working mode is routing mode (L3).

You can see the IP address/subnet mask, MAC address, security zone, working mode, detection progress and other parameters of the interface.

Step 3. Click ▶ under the operation corresponding to an interface to set the IP address range for detection.

The user needs to specify an address range in the same network segment as the IP address of the L3 interface for detection. After specifying the detection range, the user can view the detection progress in the progress bar during the operation. After the detection is completed, the user can click 🗎 to view the detection result under the operation.

Click the ⊘ button in the operation to stop IP-MAC address detection.

7.5.6 IP-MAC Batch Binding

After the detection, the user can view the detected IP-MAC entries in the detection results, and can choose to bind the detected IP-MAC address pairs in batches.

At the same time, in the IP-MAC detection result, you can check whether there is an IP-MAC address conflict among the detected active hosts in the network.

Step 1. Choose “Policy > IP-MAC Binding > Active Detection”.

Step 2. Click the “Detection Result” tab.

Step 3. Select the IP-MAC address to be bound.

Step 4. Click “Batch Bind”.

There are three binding states:

- bound

The IP-MAC address pair has been bound in IP-MAC binding.

- unbound

The IP-MAC address pair is not bound in the IP-MAC binding.

- binding conflict

The IP-MAC address pair conflicts with the IP-MAC address pair bound in the IP-MAC binding.

Step 5. To end the binding relationship, delete the corresponding entry from the binding list.

Step 6. To clear the detection results, select the corresponding item and click “Clear”.

7.6 Session Limit

7.6.1 Overview

Session limit is the function of the firewall to limit the number of concurrent and new connections based on the security zone. The firewall supports both IPv4 and IPv6 session restrictions. Session limitation is supported under the virtual system.

Scene Description

The two most common application scenarios at present are:

- Limit the number of concurrent connections for P2P traffic. By limiting the upper limit of the number of connections of a single IP, users who use P2P downloading will not affect other users when reaching the threshold.
- Limit high-creating and high-concurrency attacks from the external network or internal network, and protect the connection table from being filled by DoS attacks.

Glossary

When configuring the connection limit function, you need to understand the following:

- Session table

  Also known as connection table, state table. It is the core entry of detecting the firewall based on the status. Each data flow will have a session table, which records the forwarding state of the packet and some necessary information of the forwarded packet. This entry is used to guide the packet forwarding.
- Maximum number of concurrent connections

  Since the firewall processes packets for connections, the number of concurrent connections refers to the maximum number of connections that the firewall can accommodate at the same time, and one connection is a TCP/UDP access.
- New connections per second

  Refer to the complete TCP/UDP connections that can be established through the firewall per second. This index is mainly used to measure the processing speed of the firewall during the processing of the packet connection. If the index is low, the user will obviously feel that the Internet access speed is slow. As a result, the firewall has poor defense against network attacks.

7.6.2 Add Session Restriction Policy

The session limit rule is based on the security zone, and mainly limits the number of connections for IP addresses in the security zone. There are three types of restricted directions on the security zone, which are bidirectional, outbound, and inbound. The session limit rule supports setting concurrent and new restrictions on a single IP address, and can also set a total concurrent and new restrictions on all IPs in the network segment. When the number of restrictions is set to 0, it means no restrictions.

Step 1. Choose “Policy > Session Limit”.

Step 2. Click “Add”.

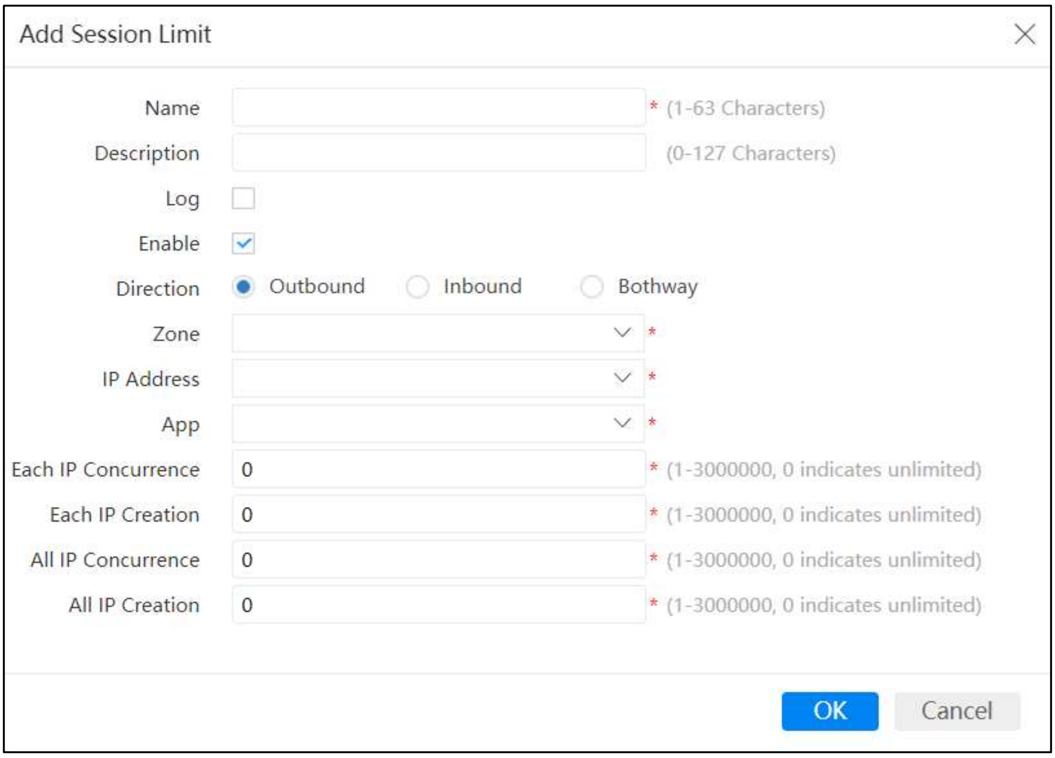
Step 3. Configure the name and description of the session restriction policy.

Step 4. Configure whether to enable the session restriction policy and whether to record logs.

Selecting the "Log" checkbox turns on session limit logging. Logs are generated when reaching the new session limit or concurrency limit.

The session restriction policy takes effect only after the "Enable" check box is selected.

Step 5. Configure the key parameters of the session restriction policy.



Add Session Limit

Name		* (1-63 Characters)
Description		(0-127 Characters)
Log	□	
Enable	☑	
Direction	● Outbound ○ Inbound ○ Bothway	
Zone		*
IP Address		*
App		*
Each IP Concurrence	0	* (1-3000000, 0 indicates unlimited)
Each IP Creation	0	* (1-3000000, 0 indicates unlimited)
All IP Concurrence	0	* (1-3000000, 0 indicates unlimited)
All IP Creation	0	* (1-3000000, 0 indicates unlimited)

Parameter	Description
Direction	Session limit supports three directions: ● Outbound Enable session restriction on outgoing sessions from the specified security zone. ● Inbound Enable session restriction for incoming sessions from the specified domain. ● Bothway Enable session restriction for both incoming and outgoing sessions
Zone	Select the name of the security zone where the session restriction takes effect.
IP address	Select the destination address/address group object that needs to be hit by the session restriction. If you need to add a new address or address group object, select "Add Address " or "Add Address Group " in the drop-down menu. IP address supports IPv4 and IPv6.
App	Click the corresponding text box, and select the application/application group object from the drop-down menu. To add a new application/application group, select "Add App" or "Add App Group" in the drop-down menu.
Each IP Concurrence	The session limit is the threshold set for the number of concurrent connections of each IPv4 address or IPv6 address, and the exceeded part will be discarded. 0 means no limit.
Each IP Creation	Session limit is the threshold set for the number of new connections to each IPv4 address or IPv6 address, and the excess will be discarded. 0 means no limit.
All IP Concurrence	Session limit is the threshold set for the sum of concurrent connections of all IPv4 addresses or IPv6 addresses, and the excess will be discarded. 0 means no limit.
All IP Creation	Session limit is the threshold set for the sum of new connections to all IPv4 addresses or IPv6 addresses, and the excess will be discarded. 0 means no limit.

Step 6. After the configuration is complete, click “OK”.

7.6.3 Adjust the Order of Session Restriction Policies

The order of the session restriction policy in the list determines the priority of the session restriction policy. The higher the policy, the higher the priority.

The session restriction policy delivered by the smart management analysis system has a higher priority than the local session restriction policy of the firewall. Only the order of firewall local session restriction policies can be adjusted.

Step 1. Select a session restriction policy.

Step 2. Click “Reorder”.

Step 3. Select the keywords to adjust your policy.

Adjusting policy keywords supports "top", "before", "after" and "end". These keywords can be used to adjust the session restriction policy to the top of the list, before the specified policy, after the specified policy, and at the end.

Step 4. Click “OK”.

8 NAT Policy

8.1 Traditional NAT

8.1.1 Configure Source NAT

Source NAT is to convert the source address in the IP packet header from a private network address to a public network address, so that intranet users can access the external network. Source NAT supports dynamic port NAT, dynamic address NAT and static address NAT.

Step 1. Select “Policy > NAT > Source NAT”.

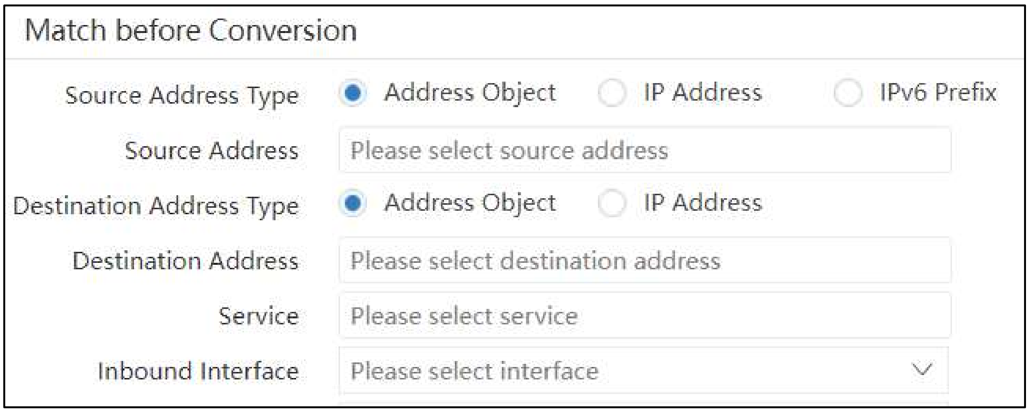
Step 2. Click “Add”.

Step 3. Configure the name and description of source NAT.

Parameter	Description
Name	Configure the name of the source NAT policy.
Description	Add necessary notes for this policy.

Step 4. Set whether to enable NAT policy. The source NAT policy takes effect only after “Enable” is selected.

Step 5. Configure the matching parameters before conversion.



Match before Conversion

Source Address Type ● Address Object ○ IP Address ○ IPv6 Prefix

Source Address: Please select source address

Destination Address Type ● Address Object ○ IP Address

Destination Address: Please select destination address

Service: Please select service

Inbound Interface: Please select interface

Parameter	Description
Source address type	Source address type selects address object or IP address. • When there are multiple source IP addresses that need to be converted, please select "Address Object". • When there is only one source IP address select "IP address".
Source address	• When the type is "Address Object", select the address object or address group object of the source address. If you need to add a new address object or address group object, click + to select "Address" or "Address Group" to set. Select "any" or "IPv4_any" to represent all IPv4 source addresses. • When the type is "IP address", enter the corresponding IPv4 address.
Destination address type	The destination address type supports address objects and IP addresses. • When the destination address to be matched is multiple addresses, please select "Address Object". • When only one destination IP address needs to be matched, select "IP address".
Destination address	• When the type is " Address Object ", select the address object or address group object of the destination address. If you need to add a new address object or address group object, click + to select "Address" or "Address Group" to set. Select "any" or "IPv4_any" to represent all IPv4 destination addresses. • When the type is IP address, enter the corresponding IPv4 address.
Service	Select the service used by this NAT policy. If you need to add a new service, click + to select "Service" or "Service Group" to set. Selecting "any" means no restriction on the service.
Outbound interface	Select the outbound interface of source NAT.

Step 6. When the source address type is "Address Object" or "IP Address", configure the conversion action.

When the source address type is "Address Object " or "IP Address ", dynamic port NAT, dynamic address NAT and static NAT are supported. Please select the conversion mode according to the actual situation:

- Dynamic Port NAT

For address and port translation, select dynamic port NAT. After conversion, the relationship between the public network address and the private network address is "one-to-multiple". A public IP address can be assigned to multiple intranet PCs. Through port conversion, a large number of hosts can share a public network IP to access the Internet, thus saving IP address resources to the greatest extent.

Parameter	Description
Type	When the address mode is "Dynamic Port NAT ", the following types are supported: • Address object Select an address object or an address group object. • IP Set the converted IP address. It is used when there is only one public IP. • BY_ROUTE When the type is BY_ROUTE, the converted address does not need to be configured. At this time, the address after NAT translation is the IP address of the outgoing interface. • do not convert If this type is selected, the source address translation will not be performed on the data matching the rule. It is usually used when IPSec VPN traffic needs to be released, because when IPSec VPN traffic sends user data at the sender, the source address cannot be translated.
Address	• When the type is address object, click ⌄ to select an address or address group. If you need to add a new address object or address group object, please select "Add Address" or "Add Address Group" to make settings. • When the type is IP, enter the converted IPv4 public network address.

- Dynamic address NAT

The address translation of multiple public network IP addresses corresponding to multiple private network IP address selects dynamic address NAT. After conversion, there is a "one-to-one" relationship between the public IP address and the private IP address. A public network IP address can only be allocated to the same intranet PC for the same period of time, and can only be allocated again after the public network IP is released. When the legal IP provided by ISP is slightly less than the number of internal hosts in the network, dynamic address NAT can be used.

Parameter	Description
Type	When the address mode is "dynamic address NAT ", the following types are supported: • Address object Select an address object or an address group object. • IP Set the converted IP address. It is used when there is only one public IP. • do not convert If this type is selected, the source address translation will not be performed on the data matching the rule. It is usually used when IPSec VPN traffic needs to be released, because when IPSec VPN traffic sends user data at the sender, the source address cannot be translated.
Address	• When the type is address object, click ⌄ to select an address or address group. If you need to add a new address object or address group object, please select "Add Address" or "Add Address Group" to make settings. • When the type is IP, enter the converted IPv4 public network address.

- Static NAT

For one-to-one NAT translation, please select Static NAT. There is a one-to-one fixed binding relationship between the public network IP and the private network IP. Static NAT can enable the external network to access some specific devices on the internal network.

Parameter	Description
Type	When the address mode is "Static NAT", the following types are supported: • Address object Select "Address Object" when one-to-one translation is required for multiple source IP addresses. • IP Set the converted IP v4 address. The source address is a single IP, and the destination address is also an IP. • do not convert If this type is selected, the source address translation will not be performed on the data matching the rule. It is usually used when IPSec VPN traffic needs to be released, because when IPSec VPN traffic sends user data at the sender, the source address cannot be translated.

Parameter	Description
Address	• When the type is address object, click the drop-down button to select address or address group. If you need to add a new address object or address group object, please select "Add Address" or "Add Address Group" to make settings. It should be noted that the IP addresses in the address object or address group object of the source address before conversion must correspond to the IP addresses in the converted address object or address group object in sequence. If the source address before translation is any, the source NAT static address translation will not take effect; if the number of source addresses before translation exceeds the number of IP addresses after translation, the part of the source addresses before translation that exceeds the number of static addresses will fail to be translated. • When the type is IP, enter the converted public IPv4 address.

Step 7. After the configuration is complete, click “OK”.

The configured source NAT policy is displayed in the source NAT policy list. You can check the source NAT policy name, source address, destination address, service, outbound interface, converted IP address, number of hits, whether it is enabled, etc.

Users can click ⋮ on the left side of the list to select the parameters to display. Select the check box corresponding to the parameter to display the parameter, and uncheck the check box corresponding to the parameter to not display the parameter.

You can delete, reorder, clear the number of hits, refresh, query, and modify the configured source NAT policy.

8.1.2 Add Destination NAT

Destination NAT is mainly to convert the destination IP of the access to the IP of the internal server. It is generally used for access from the external network to the internal server, and the internal server can use a reserved IP address.

Step 1. Select “Policy > NAT > Destination NAT".

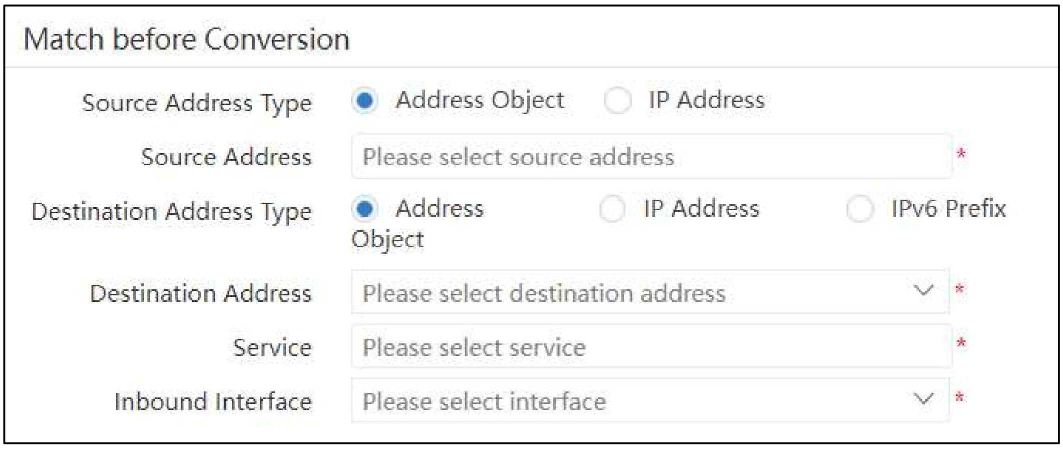
Step 2. Click “Add”.

Step 3. Configure the name and description of the destination NAT.

Parameter	Description
Name	Configure the name of the destination NAT policy.
Description	Add necessary notes for this policy.

Step 4. Select whether to enable the destination NAT policy. The destination NAT policy takes effect only after “Enable” is selected.

Step 5. Configure the matching parameters before conversion.



Match before Conversion

Source Address Type ● Address Object ○ IP Address

Source Address: Please select source address *

Destination Address Type ● Address Object ○ IP Address ○ IPv6 Prefix

Destination Address: Please select destination address *

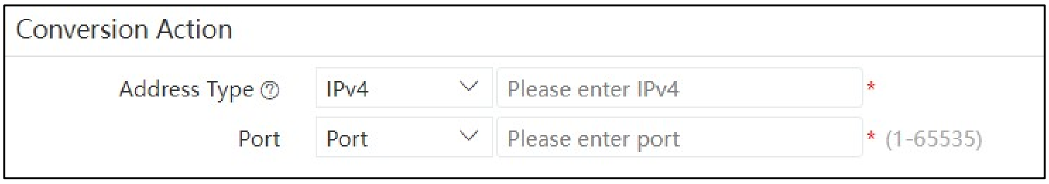
Service: Please select service *

Inbound Interface: Please select interface *

Parameter	Description
Source address type	The source address type supports address objects and IP addresses. • When the source IP address is multiple addresses, please select "Address Object". • Select “IP address” when there is only one source IP address.
Source address	• When the type is “Address Object”, select the address object or address group object of the source address. If you need to add a new address object or address group object, click + to select "Address" or "Address Group" to set. Select "any" or "IPv4_any" to represent all IPv4 source addresses. • When the type is IP address, enter the corresponding IPv4 address.
Destination address type	The destination address type supports address objects and IP addresses. • Select “Address Object” when the destination address to be translated is multiple addresses, address segments, or IPv6 addresses. • Select "IP Address" when only one IPv4 destination IP address needs to be converted.
Destination address	• When the type is " Address Object ", select the address object or address group object of the destination address. If you need to add a new address object or address group object, click + to select "Address" or "Address Group" to set. Select "any" or "IPv4_any" to represent all IPv4 destination addresses. • When the type is IP address, enter the corresponding IPv4 address.

Parameter	Description
Service	Select the service used by this NAT policy. If you need to add a new service, click + to select "Service" or "Service Group" to set. Selecting "any" means no restriction on the service.
Inbound interface	Select the inbound interface to which the destination NAT policy is applied.

Step 6. Configure the translation action of the destination address (that is, the matched address after translation).



Conversion Action

Address Type ⓘ	IPv4	Please enter IPv4	*
Port	Port	Please enter port	* (1-65535)

Parameter	Description
Address type	• IPv4 address Use the IPv4 address after destination NAT translation. Enter the IPv4 address to use after conversion. • Address object Specify address object or address group used after destination NAT translation. When the type is Address Object, click ⌄ to select an address or address group. If you need to add a new address object or address group object, please select "Add Address" or "Add Address Group" to make settings. It should be noted that the IP addresses in the address object or address group object of the destination address before translation must be in one-to-one correspondence with the IP addresses in the address object or address group object of the destination address after translation. If the destination address before translation is any, the destination NAT translation will not take effect; if the number of destination addresses before translation exceeds the number of IP addresses after translation, the part of the destination addresses before translation that exceeds the number of destination addresses after translation will fail to be translated. • Server address Select the corresponding server object in the server load balancing scenario. When the type is "Server Address ", click ⌄ to select the server address. If you need to add a new server address, please select "Add Server Address" to set it. • do not convert The data matching the destination NAT rule does not perform destination address translation, and keeps the original destination address.
Port	• When the type is port, specify the destination port used after destination NAT translation. • When the type is not convert, the data matching the destination NAT rule will not perform the destination port translation, and the original destination port will be kept.
Detection	When the server address is selected as the IP address type, you can check to enable the detection function, and the detection function uses the ICMP method for detection.

Step 7. After the configuration is complete, click “OK”.

The configured destination NAT policy is displayed in the destination NAT policy list. You can view the name, source address, destination address, service, inbound interface, converted IP address, converted port, number of hits, whether to enable or not, etc. of the destination NAT policy. Users can click ⋮ on the left side of the list to select the parameters to display. Select the check box corresponding to the parameter to display the parameter, and uncheck the check box corresponding to the parameter to not display the parameter.

You can delete, reorder, clear the number of hits, refresh, query, and modify the configured destination NAT policy.

8.1.3 Adjust the Order of NAT Policies

The order of the source NAT policy or the destination NAT policy in the NAT policy list is related to the priority of the source NAT policy or the destination NAT policy. The source NAT policy or destination NAT policy at the top has the highest priority and is matched first. You can adjust the execution order of the NAT policies by adjusting the positions of the source NAT policies or destination NAT policies in the list.

Step 1. Select a source NAT policy or destination NAT policy.

Step 2. Click “Reorder”.

Step 3. Select the keywords to adjust your policy.

The keywords for adjusting the policy support "top", "before", "after" and "end". These keywords can be used to adjust the source NAT policy or destination NAT policy to the top of the list, before the specified policy, after the specified policy, and at the end.

Step 4. Click “OK”.

8.2 NAT Transition Technology

8.2.1 NAT64

Overview

NAT64 is used to convert IPv6 addresses into IPv4 addresses, so that IPv6 hosts can access resources on IPv4 networks. NAT64 is usually used in conjunction with DNS 64.

When an IPv6 user needs to access a certain address through a domain name, it needs to send a request to the DNS server. This device is the DNS64 server. If the address type of the target domain name is an IPv6 address, the DNS64 server will return the IPv6 address corresponding to the target domain name to the IPv6 user. If the address type of the target domain name is an IPv4 address, the DNS64 server uses its specified prefix to convert the IPv4 address into an IPv6 address, and then returns it to the IPv6 user. When an IPv6 user accesses, they will go through NAT64 to access the actual IPv4 address of the target domain name.

Restrictions and Precautions

- The priority of the NAT64 policy is lower than that of the SNAT policy. When SNAT is configured, the SNAT policy will be executed instead of the default SNAT dynamic port by-route of NAT64.

- The "dynamic address NAT" mode of SNAT is not supported when the NAT 64 policy cooperates with the SNAT policy.

Configure NAT64

Step 1. Choose “Policy > NAT Policy”.

Step 2. Click the "NAT64" tab.

Step 3. Configure the NAT64 address prefix.

When IPv6 user accesses an IPv4 server, DNAT and SNAT are automatically performed without configuring DNAT and SNAT.

Step 4. Enable DNS 64 after selecting the "DNS64" checkbox.

Step 5. Click “Apply”.

8.2.2 NAT-PT

Overview

NAT-PT (Network Address Translation-Protocol Translation) can realize mutual access between IPv4 network and IPv6 network. NAT-PT combines NAT and PT protocol translation. NAT-PT does not require dual-stack technology support.

NAT-PT will be used for separate IPv6 nodes to communicate with separate IPv4 nodes. NAT-PT is generally not used when IPv6 or other tunneling technologies can be applied.

Use Restrictions and Precautions

- The "Dynamic Address NAT" translation mode of SNAT does not support IPv6.
- SNAT dynamic port NAT full-cone mode (only support being configured in command line) does not support IPv6.

Configure NAT-PT

To implement NAT-PT configuration, you need to configure destination NAT and source NAT. Source NAT can be left un-configured. In this case, by route translation is performed by default.

When IPv6 intranet users access the IPv4 public network, configure destination NAT, and the source and destination addresses before translation are IPv6 addresses. The converted address is an IPv4 address. If source NAT is not configured, the default action is "by route". When configuring source NAT, it should be noted that the source address before translation is an IPv6 address, and the destination address is an IPv4 address (the address after destination

NAT translation). The converted address is an IP v4 address.

When an IPv4 user accesses an IPv6 network, configure destination NAT, and the source address and destination address before translation are both IPv4 addresses. The converted address is an IPv6 address. If source NAT is not configured, the default action is "by route". When configuring source NAT, it should be noted that the source address before translation is an IPv4 address, and the destination address is an IPv6 address (the address after destination NAT translation). The converted address is an IPv6 address.

8.3 NAT66

8.3.1 Configure NAT66 for IP Address Translation

Use Restrictions and Precautions

- When configuring NAT66, the "Dynamic Address NAT" translation mode under SNAT is not supported, and only the "Dynamic Port NAT" and "Static NAT" modes are supported.
- SNAT dynamic port NAT full-cone mode (only supports command-line configuration) does not support IPv6.
- IPv6 address object can only contain IPv6 addresses. If an IPv4 address exists, it is considered an IPv4 address object. At this time, the IPv6 address will not be delivered, resulting in invalid IPv6 addresses.

Configuration Points

The method of implementing NAT66 through address translation is the same as that of traditional NAT, both of which are configured through the "Source NAT" or "Destination NAT" page.

The source address and the destination address before translation and the source address after translation configured by source NAT66 are all IPv6 addresses.

The source address and the destination address before translation and the destination address after translation configured by destination NAT66 are all IPv6 addresses.

8.3.2 Configure NAT66 for Prefix Translation

Source NAT66

Source NAT66 for prefix translation supports static source NAT66 and source NPTv6.

Step 1. Select “Policy > NAT > Source NAT”.

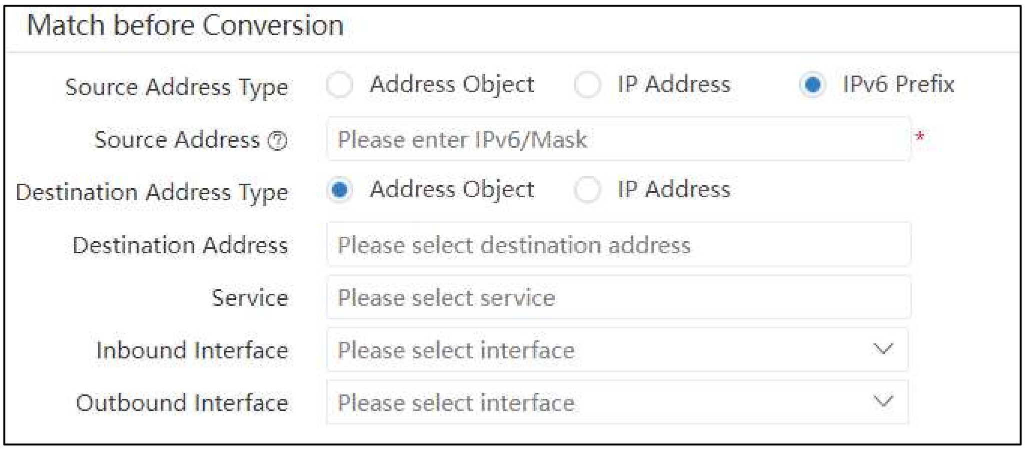
Step 2. Click “Add”.

Step 3. Configure the name and description of source NAT.

Parameter	Description
Name	Configure the name of the source NAT policy.
Description	Add necessary notes for this policy.

Step 4. Set whether to enable NAT policy. The source NAT policy takes effect only after “Enable” is selected.

Step 5. Configure the matching parameters before conversion.



Match before Conversion

Source Address Type ○ Address Object ○ IP Address ● IPv6 Prefix

Source Address ⓘ Please enter IPv6/Mask *

Destination Address Type ● Address Object ○ IP Address

Destination Address Please select destination address

Service Please select service

Inbound Interface Please select interface

Outbound Interface Please select interface

Parameter	Description
Source address type	Select IPv6 prefix for the source address type.
Source address	When the type is "IPv6 Prefix", enter the IPv6 prefix or prefix length. "Static NAT66" supports a prefix length ranging from 4 to 128; "NPTv6" supports a prefix length ranging from 48 to 64. The configured prefix lengths before conversion and after conversion must be the same.
Destination address type	The destination address type supports address objects and IP addresses. • When the destination address to be matched is multiple addresses, please select "Address Object". • Select “IP address” when only one destination IP address needs to be matched.

Parameter	Description
Destination address	• When the type is " Address Object ", select the address object or address group object of the destination address. If you need to add a new address object or address group object, click + to select "Address" or "Address Group" to set. Select "IP v6_any" to represent all IPv6 destination addresses. • When the type is IP address, enter the corresponding IPv6 address.
Service	Select the service used by this NAT policy. If you need to add a new service, click + to select "Service" or "Service Group" to set. Selecting "any" means no restriction on the service.
Outbound interface	Select the outbound interface of source NAT66.

Step 6. When the source address type is "IPv6 prefix", configure the conversion action.

Parameter	Description
Conversion mode	The two translation modes translate addresses differently: • The NPTV6 conversion method is that in addition to replacing the IPv6 network prefix of the source address, the subnet ID part of the IPv6 address will be adjusted according to the algorithm specified in RFC6296. • Static NAT66 translation only replaces the IPv6 network prefix of the source address, and the subnet ID part of the IPv6 address will not change.
Type	Support the IPv6 prefixes.
Address	Enter the converted IPv6 prefix or prefix length. "Static NAT66" supports a prefix length ranging from 4 to 128; "NPTv6" supports a prefix length ranging from 48 to 64. The configured prefix lengths before conversion and after conversion must be the same.

Step 7. After the configuration is complete, click “OK”.

The configured source NAT policy is displayed in the source NAT policy list. You can check the source NAT policy name, source address, destination address, service, outbound interface, converted IP address, number of hits, whether it is enabled, etc.

Users can click ⋮ on the left side of the list to select the parameters to display. Select the check box corresponding to the parameter to display the parameter, and uncheck the check box corresponding to the parameter to not display the parameter.

You can delete, reorder, clear the number of hits, refresh, query, and modify the configured source NAT policy.

Destination NAT66

Destination NAT66 for prefix translation supports static destination NAT66 and destination NPTv6.

Step 1. Select “Policy > NAT > Destination NAT".

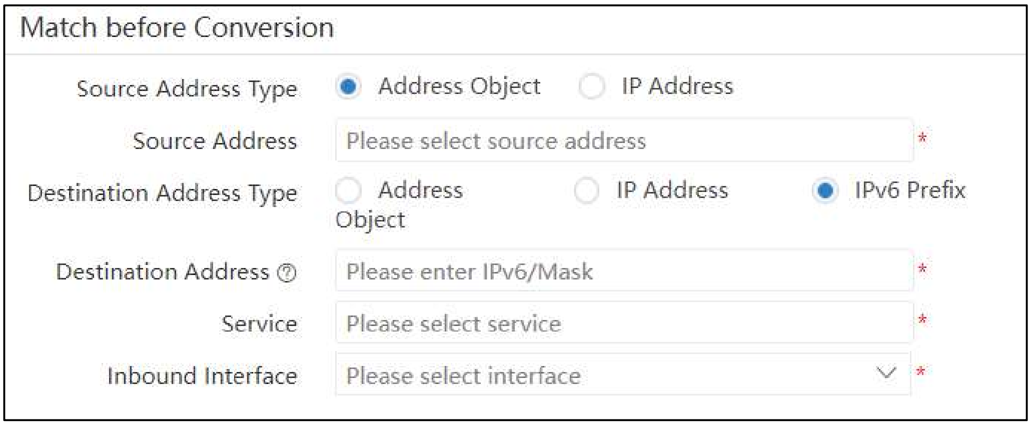
Step 2. Click “Add”.

Step 3. Configure the name and description of the destination NAT.

Parameter	Description
Name	Configure the name of the destination NAT policy.
Description	Add necessary notes for this policy.

Step 4. Select whether to enable the destination NAT policy. The destination NAT policy takes effect only after “Enable” is selected.

Step 5. Configure the matching parameters before conversion.



Match before Conversion

Source Address Type ● Address Object ○ IP Address

Source Address: Please select source address *

Destination Address Type ○ Address Object ○ IP Address ● IPv6 Prefix

Destination Address ⓘ: Please enter IPv6/Mask *

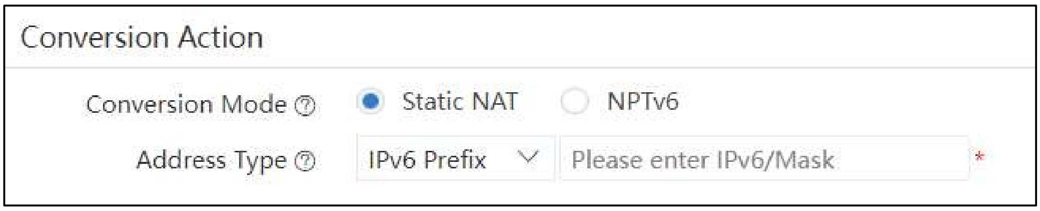
Service: Please select service *

Inbound Interface: Please select interface *

Parameter	Description
Source address type	The source address type supports address objects and IP addresses. • When the source IP address is multiple addresses, please select "Address Object". • Select “IP address” when there is only one source IP address.
Source address	• When the type is “Address Object”, select the address object or address group object of the source address. If you need to add a new address object or address group object, click + to select "Address" or "Address Group" to set. Select "IPv6any" to represent all IPv6 source addresses. • When the type is IP address, enter the corresponding IPv6 address.

Parameter	Description
Destination address type	Select IPv6 prefix for the destination address type.
Destination address	When the type is "IPv6 Prefix", enter the IPv6 prefix or prefix length.
Service	Select the service used by this NAT policy. If you need to add a new service, click + to select "Service" or "Service Group" to set. Selecting "any" means no restriction on the service.
Inbound interface	Select the ingress interface to which the destination NAT66 policy is applied.

Step 6. Configure the translation action of the destination address (that is, the matched address after translation).



Conversion Action

Conversion Mode ⓘ ● Static NAT ○ NPTv6

Address Type ⓘ IPv6 Prefix Please enter IPv6/Mask *

Parameter	Description
Conversion mode	The two conversion modes translate addresses differently: • The NPTV6 conversion method is that in addition to replacing the IPv6 network prefix of the destination address, the subnet ID part of the IPv6 address will be adjusted according to the algorithm specified in RFC6296. • Static NAT66 translation only replaces the IPv6 network prefix of the destination address, and the subnet ID part of the IPv6 address will not change.
Type	Support IPv6 prefixes.
Address	Enter the converted IPv6 prefix or prefix length.

Step 7. After the configuration is complete, click “OK”.

The configured destination NAT policy is displayed in the destination NAT policy list. You can view the name, source address, destination address, service, inbound interface, converted IP address, converted port, number of hits, whether enabled or not, etc. of the destination NAT policy. Users can click ⋮ on the left side of the list to select the parameters to display. Select the check box corresponding to the parameter to display the parameter, and uncheck the check box corresponding to the parameter to not display the parameter.

You can delete, reorder, clear the number of hits, refresh, query, and modify the configured destination NAT policy.

9 VPN

VPN (Virtual Private Network) technology is to establish a virtual secure channel on the Internet through tunneling technology, so as to realize the secure exchange of network access between the headquarters and branches or the secure access of employees from other places to the company network.

Several commonly used VPN technologies are PPTP, L2TP, IPSec, GRE, SSL, and 6to4 and isatap applied in IPv6 environment. Through these technologies, you can build the virtual dedicated tunnels of gateway-to-gateway and client-to-gateway working at different network levels, so as to meet various environmental needs.

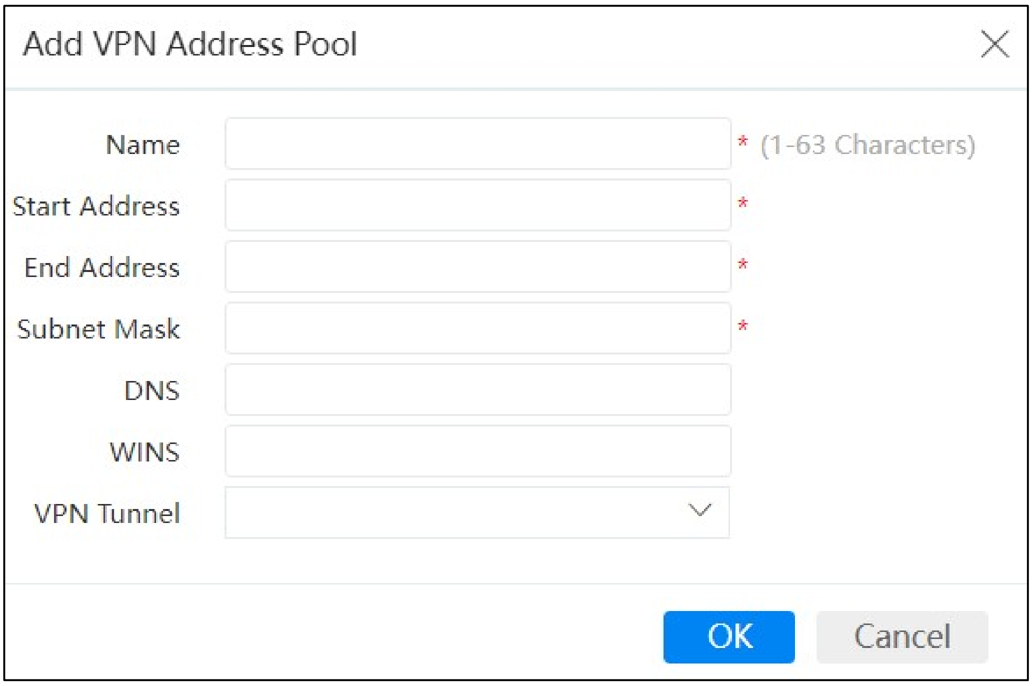
9.1 VPN Address Pool

VPN address pool is used to allocate IP addresses for VPNs.

Step 1. Choose “Network > VPN > VPN Address Pool”.

Step 2. Click “Add”.

Step 3. Configure VPN address pool parameters.



Add VPN Address Pool

Name: * (1-63 Characters)

Start Address: *

End Address: *

Subnet Mask: *

DNS:

WINS:

VPN Tunnel:

Parameter	Description
Name	Configure the name of the VPN address pool.
Start address	Configure the start address of the address pool, in the dotted decimal format.
End address	Configure the end address of the address pool, in the dotted decimal format.
Subnet mask	Configure the subnet mask of the address pool address.
DNS	Specify the DNS address to be delivered together with the IP address when delivering to the client address.
WINS	Specify the WINS address to be delivered together with the IP address when delivering to the client address.
VPN tunnel	Select the name of the VPN tunnel bound to the address pool, and you need to add the tunnel to the VPN tunnel in advance. You can also select a VPN address pool in a VPN tunnel. The operation of these two places has the same effect.

Step 4. After the configuration is complete, click “OK”.

The configured address pool is displayed in the address pool list. You can view the name, start address, end address, subnet mask and VPN tunnel of the address pool.

Click the Edit icon under operation to modify the address pool parameters.

9.2 Configure IPSec Auto-Negotiation

IPSec auto-negotiation uses IKE to negotiate IPSec tunnels, and negotiates key parameters used in IPSec tunnels through IKE. This reduces the work of manually specifying IPSec key parameters and improves security. IPSec VPN configuration generally adopts IPSec auto-negotiation mode, and manual tunnels are only used in very small static networks.

Negotiating IPSec tunnels through IKE supports not only traffic diversion through security policies (that is, IPSec based on security policies), but also traffic diversion through routes (that is, IPSec based on routes).

Support IPv4 IPSec and IPv6 IPSec.

9.2.1 Restrictions and Precautions

- When both ends of the IPSec tunnel are IPSec gateway devices, the tunnel mode is used by default and no configuration is required.
- In client dial-up mode, the IPSec gateway automatically switches to transmission mode without configuration.
- The firewall only supports IKEv1.
- When the asymmetric mode is enabled in a dual-machine environment, the anti-replay must be disabled. Otherwise, the service will be blocked.

9.2.2 (Optional) Add IKE Proposal

The IKE proposal is used to define the parameters used in the first phase of IPSec negotiation SA (usually called "IKE SA" or "ISAKMP SA"), including the authentication type (pre-shared key or certificate), encryption algorithm, authentication algorithm, DH group, lifecycle, etc.

Multiple IKE proposals are preset on the firewall, and users can directly refer to them when configuring the IKE gateway.

When the predefined IKE proposals cannot meet the requirements, you can customize and add IKE proposals.

Step 1. Choose “Network > VPN > IPSec Auto Tunnel”.

Step 2. Click “IKE Proposal”.

Step 3. Click “Add”.

Step 4. Configure IKE proposal parameters.

Parameter	Description
Name	The name of the IKE proposal.
Authentication type	There are two authentication types: pre-shared key and certificate. • When "Pre-Shared Key" is selected, the user needs to specify the pre-shared key. When pre-shared key authentication is used, the IKE gateway of the negotiated tunnel must be configured with the same pre-shared key. • When selecting "Certificate", the user needs to specify a certificate that can prove the identity of the gateway.
Encryption Algorithm	The encryption algorithm supports DES, 3DES, AES - 128, AES-256 and national secret algorithm SM1, SM4. By default, the AES-128 algorithm is used for encryption. For security reasons, the DES algorithm is not recommended. Security AES-256 > AES-128 > 3DES > DES. When multiple encryption algorithms are configured, match them with the peer end according to the order in which the algorithms are configured, and use the algorithm for encryption after matching the same algorithm.
Verification algorithm	The verification algorithm supports MD5, SHA1 and national secret algorithm SM3. By default, the SHA-1 algorithm is used. When multiple authentication algorithms are configured, match with the peer end according to the sequence of algorithm configuration, and use the algorithm for authentication after matching the same algorithm.
DH group	The DH group supports three types: Group1, Group2 and Group5, and Group 2 is used by default. The configuration here at both ends must be consistent. The descending order of security levels of DH key exchange groups is group5 > group2 > group1. When the gateway negotiation mode is aggressive mode, only one DH group algorithm is supported. Multiple DH algorithms are supported in main mode. When configuring multiple DH algorithms, perform DH group matching in the order of configuration, and use the DH group after matching the same DH group. This configuration can be ignored when the national encryption algorithm is used for negotiation.

Parameter	Description
Lifetime (time)	The lifetime after IKE negotiation is successful, 10 seconds before the timeout, the firewall as the initiator will initiate an IKE negotiation request and establish an IKE connection again. The lifetime defaults to 86400 seconds (24 hours), and supports customizing, and the range is 300-86400.

Step 5. After the configuration is complete, click “OK”.

The configured IKE proposals are displayed in the IKE proposal list. You can edit and delete IKE proposals.

9.2.3 (Optional) Add a Dial-up User Group

When the built-in VPN client L2TP over IPSec of Windows or the mobile terminal L2TP over IPSec accesses the VPN gateway, a dial-up user group needs to be added.

Step 1. Choose “Network > VPN > IPSec Auto Tunnel”.

Step 2. Click “Dialup User Group”.

Step 3. Click “Add”.

Step 4. Configure the user group name.

Step 5. Click “Add” to add dial-up user group members.

Step 6. Configure the member parameters.

Parameter	Description
Peer ID	Select the peer ID type. The peer ID type supports "IP address", "U-FQDN (email)", " FQDN (domain name)", " ASN1DN (certificate subject)" and "Accept any peer ID". When the peer ID is "Accept any peer ID", the peer ID is not verified.
Peer ID value	When the peer ID type is "U-FQDN (email)", " FQDN (domain name)" and " ASN1DN (certificate subject)", specify the peer ID value. This value must be consistent with the "Local ID" value configured on the remote end. When the peer ID type is ASN1DN (certificate subject), U-FQDN (email), or FQDN (domain name), configure "*" to match all values.

Parameter	Description
Peer IP address	When the peer ID type is "IP address", specify the peer IP address. The peer IP address is the IP address of the peer IKE gateway interface used to establish the tunnel. Both IPv4 addresses and IPv6 addresses are supported. When the peer ID type is IP, configure "*" to match all values.
Pre-shared configuration	When the peer ID is "IP address", "U-FQDN (email)", " FQDN (domain name)", this parameter is displayed. • When the default configuration of the pre-shared key is selected, the pre-shared key configured in the IKE gateway will be used. At this time, all access users use the same pre-shared key. • When custom configuration is selected, the user can configure the pre-shared key individually for the dial-up user group. The pre-shared key is in the form of a string, and the value ranges from 6 to 31 characters. The pre-shared keys at both ends of the IPSec tunnel must be the same.
Trusted CA configuration	This parameter is displayed when the peer ID is "ASN1DN (certificate subject)". • When the default configuration of trusted CA is selected, the trusted CA configured in the IKE gateway will be used. • When selecting a custom configuration, the user needs to re-designate a new trusted CA. Click the drop-down box and select Trusted CAs from the drop-down menu.

Step 7. After the configuration is complete, click “OK”.

Support adding multiple members. You can repeat the above operations to add new members.

Step 8. After the configuration is complete, click “OK”.

The configured dial-up user groups are displayed in the dial-up user group list. Click the name or edit button to modify the dial-up user group configuration.

9.2.4 Add IPSec IKE Gateway

When configuring an IPSec automatic tunnel, you need to specify an IKE gateway. The IKE gateway defines parameters such as the local interface, IP address, negotiation mode, peer type, peer address, local type, and IKE proposal for IPSec negotiation.

The IP of the headquarters is usually a static IP address, which can establish IPSec tunnels with one or more IPSec gateways or dial-up users. The peer IP address can be a static IP or a dynamic IP.

The IP of the branch is usually a dynamic IP address or an intranet IP address behind NAT.

Step 1. Choose “Network > VPN > IPSec Auto Tunnel”.

Step 2. Click "IKE Gateway".

Step 3. Click “Add”.

Step 4. Configure the name, address type, interface, and local address of the IKE gateway.

The interface supports L3 physical interfaces, physical sub-interfaces, VLAN interfaces, bridge interfaces, aggregation interfaces, aggregation sub-interfaces, loopback interfaces, ADSL interfaces, virtual system interfaces, 3G interfaces, and 4G interfaces.

- For Interface, select the interface used to establish the IPSec VPN tunnel.
- For Local Address, select the IPv4 or IPv6 address of the interface. Select auto when the interface IP address is not fixed. When auto is selected, as the initiator, the first float type IP address on the interface is used by default; as the receiver, any float type IP address on the interface is used by default.

Step 5. Configure the negotiation mode of the IKE gateway.

The first phase of the IKEv1 negotiation supports main mode, aggressive mode, and national secret mode. In the national secret mode, the firewall must be installed with a national secret encryption card, and the encryption algorithm and verification algorithm must use the national secret algorithm.

Step 6. Configure negotiation parameters.

- Configure negotiation parameters in main mode or aggressive mode.

Parameter	**Description**
Address mode	• Static If the peer IKE gateway address is a static fixed IP address, select “Static”. • Dynamic Select " Dynamic " when the peer IKE gateway address is an unfixed dynamic address. • Dial-up user group In the scenario where the Windows built-in VPN client L2TP over IPSec or the mobile terminal L2TP over IPSec accesses the VPN gateway, select “Dialup User Group”.
Peer address	When you select “Static”, you need to specify the IPv4 or IPv6 address of the peer IKE gateway. The peer address supports IP or domain name.

Parameter	Description
Local ID type and peer ID type	The local ID is used to identify the identity of the local device for the peer device to verify its own legitimacy. The "local ID type " on the local device needs to be consistent with the "Peer ID type" parameter set on the peer device or the peer ID type is "Accept any peer ID". When the peer ID type is "Accept any peer ID", the peer ID will not be verified. **Notes** When the address mode is "Dial-up user group ", the peer ID type and peer ID value are configured when creating a dial-up user group. On the IKE gateway, only the local ID type and local ID value need to be configured.
Local ID value and peer ID value	• When the local ID type is "IP type ", you do not need to configure the local ID value. The local ID is the local IP address by default. The peer ID value is the "local IP address" of the peer device. Only when pre-shared key authentication is used, IP type is supported. • When you select U-FQDN or FQDN Type as the local ID type, the local ID is a domain name. "U-FQDN" and "FQDN Type" are supported only when pre-shared key authentication is used. • When "ASN1DN type" is selected as the local ID type, the local ID value uses the value of the " Subject " field in the certificate and does not need to be specified. The peer ID value specifies the value of the " Subject " field in the peer certificate. Only the certificate type supports selecting "ASN1DN Type".
Dial-up user group	When selecting "Dial-up User Group", it needs to be configured. Select "Add dial-up user group" in the drop-down box or select a configured dial-up user group.
IKE proposal (P1 proposal)	Click the drop-down box of IKE Proposal (P1 Proposal) to select an IKE proposal. You can select all IKE proposals predefined by the firewall from the drop-down box. But when you need to add a new IKE proposal, select "Add IKE (p1) proposal" from the drop-down menu.
Pre-shared key	When the selected IKE proposal selects “Pre-shared key”, specify the pre-shared key. The pre-shared key is in the form of a string, and the value ranges from 6 to 31 characters. The pre-shared keys at both ends of the IPSec tunnel must be the same.
Peer Trusted CA	When the authentication type of the selected IKE proposal is "Certificate", specify the trusted CA of the peer end.

Parameter	Description
Local certificate	When the authentication type of the selected IKE proposal is “Certificate”, specify a local certificate.

- Configure negotiation parameters in SM mode.

Parameter	Description
Address mode	• Static If the peer VPN access user address is a static fixed IP address, select “Static”. • Dynamic Select "Dynamic" when the peer VPN access user address is an unfixed dynamic address.
Peer address	When you select “Static”, you need to specify the IP address of the peer IKE gateway. The peer address supports IP or domain name.
Local ID type and peer ID type	The default is ASN 1DN (Certificate Subject), which cannot be modified.
Peer ID value	When "ASN1DN Type" is selected as the local ID type, the local ID value uses the value of the "Subject" field in the certificate. The peer ID value uses the value of the "Subject" field in the peer certificate.
Local encryption certificate	You can select the certificate under "Certificate Management>Certificate List". The certificate can be generated on the firewall, or imported to the firewall after being generated by a third-party device.
Local Signature Certificate	You can select the certificate under "Certificate Management>Certificate List". The certificate can be generated on the firewall, or imported to the firewall after being generated by a third-party device.
IKE proposal (P1 proposal)	Click the drop-down box of IKE Proposal (P1 Proposal) to select an IKE proposal. You can select all IKE proposals predefined by the firewall from the drop-down box. But when you need to add a new IKE proposal, select "Add IKE (p1) proposal" from the drop-down menu.
Opposite Trusted CA	When the authentication type of the selected IKE proposal is "Certificate", specify the trusted CA of the peer end.

Step 7. Advanced configuration.

Parameter	Description
Connection Type	• Bothway The firewall can be the initiator during the negotiation of the IKE phase and actively initiate the negotiation request; it can also be the responder during the negotiation of the IKE phase and receive the negotiation request. As an initiator, the IP address or domain name of the peer interface must be fixed, and as a responder, the IP address or domain name of the local interface must be fixed. • Initiator The firewall is the initiator of the negotiation in the IKE phase and actively initiates the negotiation request. An IPSec gateway with a dynamic IP address or a dial-up user acts as the tunnel initiator. As the initiator, the IP address or domain name of the peer interface must be fixed. • Responder The firewall is the responder during the negotiation of the IKE phase and passively receives the negotiation request. The interface IP address or domain name of the tunnel responder must be fixed.
NAT traversal	When there is a NAT device in front of one of the local IKE gateway or peer IKE gateway or peer client, NAT traversal needs to be enabled.
Dead Peer Detection (DPD)	Detect whether the peer gateway or client is alive. Select the "Dead Peer Detection (DPD)" check box to enable this function. If the local end can receive the IPSec traffic sent by the peer end, it considers the peer end to be in an active state; only when it does not receive IPSec traffic from the peer end within a certain time interval, it will send a DPD packet to detect the status of the peer end. If no response is received from the peer end after sending DPD packets several times, the peer end is considered unreachable, and the security association (IKE SA and IPSec SA) between IKE peers will be deleted at this time.
DPD interval	Specify the interval of sending the DPD detection packets.
DPD retry	Specify the number of DPD probe retransmissions. If the DPD detection does not respond after reaching the number of retransmissions, the peer end is considered to be faulty.

Parameter	Description
Enable extended authentication	It can be configured when the address mode is selected as "Dial-up user group". When the "Enable" check box is selected, Extended Authentication is enabled. After the extended authentication is enabled and the first phase of IKE SA negotiation is completed, the IPSec gateway will initiate extended authentication for the dial-up user of the IPSec client, verify the user name and password of the user, and proceed to the second phase of negotiation after the extended authentication is passed.
Authentication server	Select an authentication server to authenticate dial-up users.

Step 8. After the configuration is complete, click "OK".

9.2.5 (Optional) Add IPSec Proposal

The IPSec proposal is used to configure the negotiation parameters of the second phase. IPSec proposes to support ESP protocol, AH protocol, encryption algorithm DES, 3DES, AES128, AES256 and national secret encryption algorithm SM1, SM4, verification algorithm MD5, SHA1, SHA-256 and national secret verification algorithm SM3, DH group Group1, 2, 5, Perfect Forward Protection (PFS), and 300-86400 seconds time-to-live and traffic-based IPSec tunnel update control.

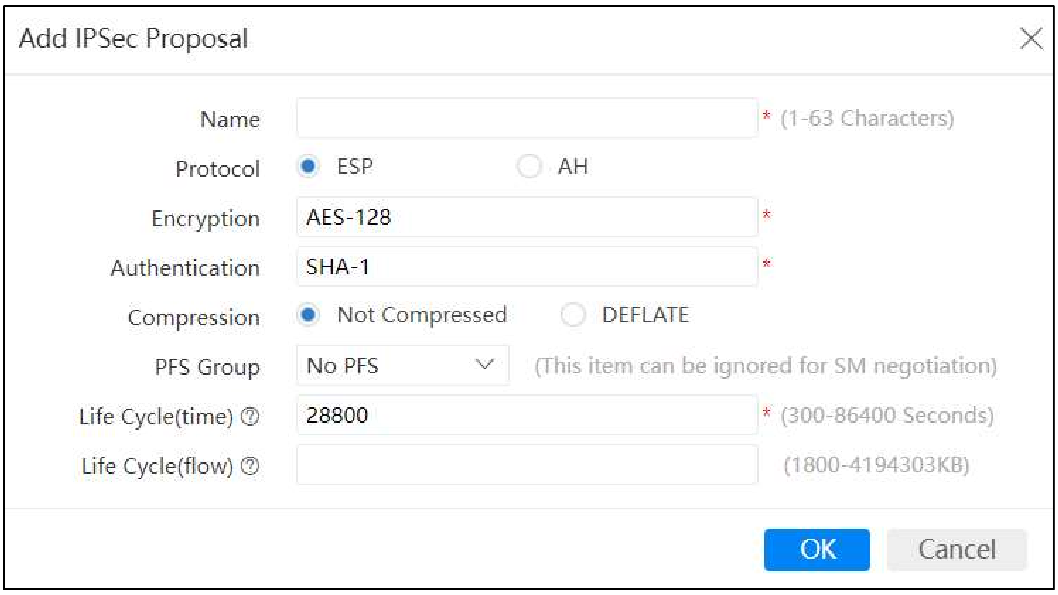
Multiple IPSec proposals are preset on the firewall, and users can directly refer to them when configuring IPSec tunnels. When the predefined IPSec proposals cannot meet the requirements, you can add custom IPSec proposals.

Step 1. Choose "Network > VPN > IPSec Auto Tunnel".

Step 2. Click the "IPSec Proposal" tab.

Step 3. Click "Add".

Step 4. Configure IPSec proposal parameters.



Add IPSec Proposal

Name: * (1-63 Characters)

Protocol: ● ESP ○ AH

Encryption: AES-128 *

Authentication: SHA-1 *

Compression: ● Not Compressed ○ DEFLATE

PFS Group: No PFS (This item can be ignored for SM negotiation)

Life Cycle(time): 28800 * (300-86400 Seconds)

Life Cycle(flow): (1800-4194303KB)

Parameter	Description
Name	Specify the name of the IPSec proposal.
Protocol	The protocol is divided into ESP, AH two kinds. • The ESP protocol can authenticate and encrypt data flow. The user is required to specify the encryption algorithm and authentication algorithm. • The AH protocol only authenticates data flows and does not support encryption. The user is required to specify the authentication algorithm.
Encryption	The encryption algorithm supports DES, 3DES, AES-128, AES-256 and national secret algorithms SM1 and SM4. In consideration of security, it is recommended that users try not to use DES and 3DES algorithms. When multiple encryption algorithms are configured, match them with the peer end according to the order in which the algorithms are configured, and use the algorithm for encryption after matching the same algorithm.
Authentication	The verification algorithm supports MD5, SHA - 1, SHA -256 and national secret algorithm SM3. When multiple authentication algorithms are configured, match with the peer end according to the sequence of algorithm configuration, and use the algorithm for authentication after matching the same algorithm.

Parameter	Description
Compression	When selecting "No Compression", no compression algorithm will be used. When selecting "DEFLATE", use the Deflate data compression algorithm. The configuration of this parameter at both ends must be consistent.
PFS group	PFS, perfect forward protection function, this function is turned off by default. After enabling this function, an additional DH exchange will be performed in phase 2 negotiation to ensure the security of the IPSec SA key and improve communication security. The DH group supports three types: Group1, Group2, and Group5. No PFS means to disable the PFS function. Support selecting multiple DH groups. When configuring the DH algorithm, perform DH group matching in the order of configuration, and use the DH group after matching the same DH group. When using national secret negotiation, this configuration can be ignored.
Life cycle (time)	Control the life time of the IPSec SA based on time. After the timeout, the IPSec SA becomes invalid. If the automatic connection function is enabled on the firewall, 30 seconds before the timeout, the firewall will initiate an IPSec negotiation request again to establish an IPSec connection. The lifetime defaults to 86400 seconds, and supports customizing, ranging from 300 to 86400.
Life cycle (flow)	Control the life cycle of IPSec SA based on data flow. At the same time, the life cycle of IPSec SA is controlled based on traffic and time. As long as one of the values is satisfied, the IPSec SA becomes invalid. Specify the traffic upper limit value of the lifetime. After exceeding the upper limit, IPSec SA is invalid. If the firewall has enabled the automatic connection function, it will initiate an IPSec negotiation request again to establish an IPSec connection. The lifetime (traffic) calculation is the sum of received data and sent data.

Step 5. After the configuration is complete, click “OK”.

The configured IPSec proposals are displayed in the IPSec list. The configured IPSec proposal can be modified by name or edit button.

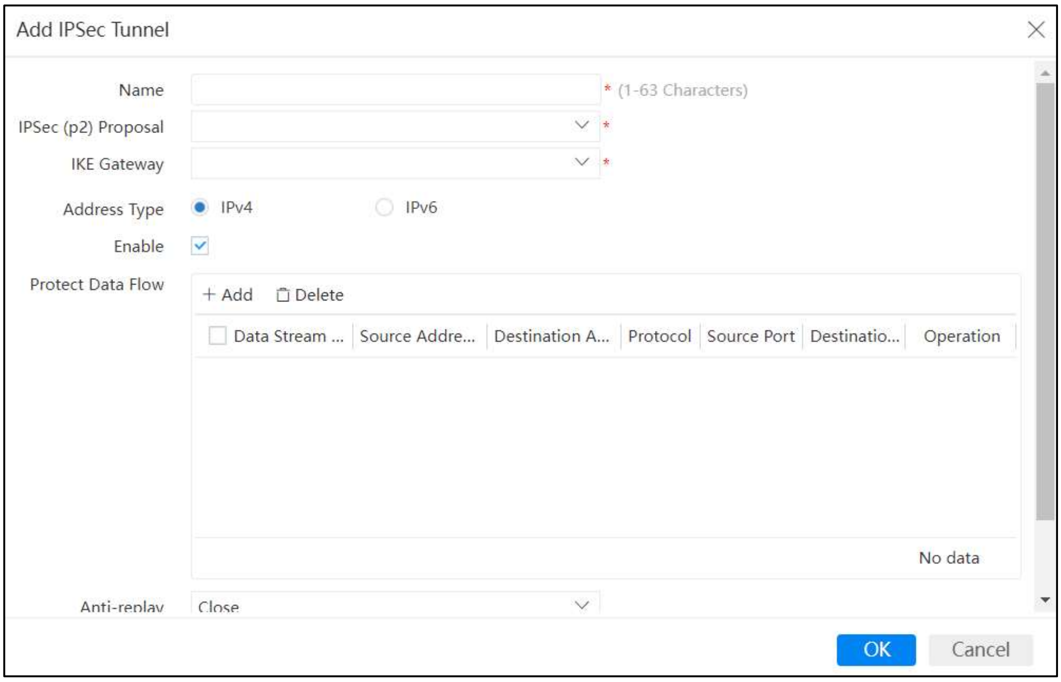
9.2.6 Add IPSec Tunnel

The IPSec tunnel is used for the negotiation parameters of the SA in the second phase of IPSec.

Step 1. Choose “Network > VPN > IPSec Auto Tunnel”.

Step 2. On the “IPSec Tunnel” page, click “Add”.

Step 3. Configure IPSec tunnel parameters.



Add IPSec Tunnel

Name: * (1-63 Characters)

IPSec (p2) Proposal: *

IKE Gateway: *

Address Type: ● IPv4 ○ IPv6

Enable: ☑

Protect Data Flow: + Add 🗑 Delete

□ Data Stream ...	Source Addre...	Destination A...	Protocol	Source Port	Destinatio...	Operation

No data

Anti-replay: Close

Parameter	Description
Name	The name of the IPSec tunnel.
IPSec (P2) Proposal	Click the drop-down box of IPSec Proposal (P2 Proposal) to select an IPSec proposal. All firewall predefined and custom IPSec proposals can be selected from the drop-down box. From the name of the predefined IPSec proposal, you can see the protocol, encryption algorithm, authentication algorithm, and PFS group adopted by the proposal. When you need to add a new IPSec proposal, select "Add IPSec proposal (p2 proposal)" from the drop-down menu.
IKE gateway	Select the IKE gateway name that needs to be used with the IPSec negotiation phase. The key used in the IPSec phase of IKE negotiation.
Address type	Select the address type to protect the traffic. The address type supports IPv4 and IPv6. When IPv4 is selected, the source and destination addresses of the protected data flow are both IPv4 addresses ; when IPv6 is selected, the source and destination addresses of the protected data flow are both IPv6 addresses.

Parameter	Description
Enable	Select the Enable check box to enable the IPSec tunnel negotiation function.
Protect data flow	Specifies the data flow to be protected by the IPSec tunnel. When the address type is IPv4, add IPv4 data flow; when the address type is IPv6, add IPv6 data flow. Click Add to configure the data flow identifier, IPv4 source address/mask, IPv4 destination address/mask or IPv6 source address/prefix length, IPv6 destination address/prefix length, and protocol. The data stream ID is user-defined and used to distinguish different data streams. The value range of the data stream identifier is 1 to 63 characters such as numbers, lowercase letters, uppercase letters, @, etc. Support adding multiple protection data streams, and support adding IPv4 and IPv6 data streams at the same time. The default source address/mask, destination address/mask, and protocol are all any, which means that any traffic can be protected. It is recommended that users configure more fine-grained source and destination addresses. The IPv4 mask supports numeric or dotted decimal notation. For example, you can specify the source address/mask as "10.0.0.1/24" or "10.0.0.1/255.255.255.0 ".
Anti-replay	Anti-replay, that is, to prevent attackers from repeatedly sending packets that have already been sent to deceive the firewall. When a duplicate packet is detected, the packet is discarded. Replay is disabled by default. The replay window can be configured as 32, 64, 128, 256, 512. The larger the window, the larger the scope of anti-replay detection.
Auto connect	After selecting the "Automatic Connection" check box, the IPSec gateway will automatically initiate a connection when the IPSec SA is not established or expires, triggering IPSec negotiation. the automatic connection is not enabled, the negotiation will be triggered to establish an IPSec tunnel when the initiator sends data. The automatic connection method can establish a tunnel when there is no data, thus allowing the responder to actively access the initiator (for example, a gateway- side user accessing a client user), instead of passively waiting for the initiator to initiate a connection and establish a tunnel before accessing.
DHCP over IPSec	Select the "DHCP over IPSec " check box to enable the DHCP over IPSec function. This function needs to be used in conjunction with the client address pool.

Parameter	Description
VPN address pool	This parameter needs to be configured when “DHCP over IPSec ” is selected. Select the configured VPN address pool. Use the addresses in the VPN address pool to assign IP addresses to clients.

Step 4. After the configuration is complete, click “OK”.

9.2.7 IPSec Data Flow Diversion

IPSec not only supports specifying data flows by adding protection subnets, but also supports traffic diversion through security policies and routes. When diverting traffic through routes, the IPSec policy can only be applied to the tunnel interface.

When specifying a protection subnet and diverting traffic through a security policy at the same time, the traffic entering the IPSec tunnel must be the traffic in the protection subnet permitted by the security policy.

When diverting traffic through a tunnel, it is recommended that the protection subnet be configured as a subnet whose default value is any. In this case, implement IPSec protection on the data flow diverted by the tunnel.

IPSec Data Traffic Diversion through Security Policies

Step 1. Choose “Policy > Security Policy”.

Step 2. Click “Add”.

Step 3. Divert traffic through security policies.

Select "Security Connection (Tunnel)" as the action, and specify the tunnel for data encapsulation. When the data is a tunnel packet, it is also necessary to specify which tunnel the data comes from.

The configuration of other parameters is consistent with the common security policy.

Step 4. After the configuration is complete, click “OK”.

Divert IPSec Data Traffic through Routing

Route-based IPSec needs to create a tunnel interface and bind a tunnel through the tunnel interface.

Step 1. Choose “Network > Interface”.

Step 2. Click "Add" and select "Tunnel Interface" from the drop-down menu.

Step 3. Configure the tunnel interface.

Configure the tunnel interface IP address and security zone. Select the tunnel to be bound in Tunnel Binding.

You can the IP addresses freely, but the IP addresses of the tunnel interfaces on both ends of the IPSec tunnel must be configured as IP addresses on the same network segment.

Step 4. After the configuration is complete, click “OK”.

9.2.8 (Optional) Access Extranet Configuration

To enable VPN intranet users to access the external network at the same time, source NAT needs to be configured at the same time to perform NAT translation on the traffic accessing the external network.

You can configure VPN users to access the external network through the local gateway or access the external network through the headquarters network.

- VPN traffic, select "Dynamic Port NAT" for the source NAT translation mode, and set the type to "No translation".
- Internet traffic, perform source NAT translation.

9.2.9 (Optional) Configure IPSec Tunnel Backup

Support IPSec tunnel backup only when diverting traffic via the route. Tunnel backup can be implemented by specifying a policy route to direct data flows to different tunnel ports.

The IPSec gateways at both ends must have at least two interfaces connected to the network to realize link backup.

Bind IPSec tunnels by creating a tunnel interface for each IPSec interface. And through policy routing, the traffic is directed to the tunnel interface corresponding to the active link. When it is detected that the main tunnel is unreachable, the state of the corresponding tunnel interface is changed to down, and the traffic is directed to the IPSec tunnel of another link.

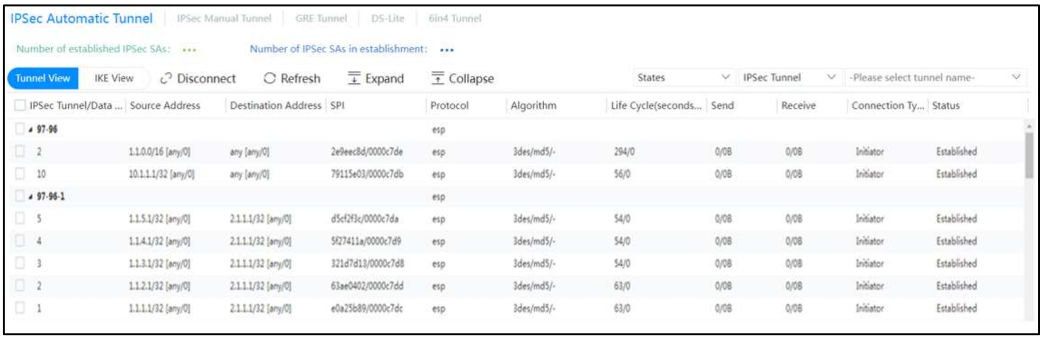
Link detection is enabled in the policy routing. When the primary tunnel fails, the firewall can quickly detect and direct the traffic to another tunnel.

9.2.10 View IPSec Auto Tunnel

Choose “Data Center > Monitor > Tunnel Monitor”, and check the created tunnel information in “IPSec Automatic Tunnel”.

IPSec automatic tunnel provides IPSec tunnel and IKE tunnel status display. By default, the

IPSec automatic tunnel page displays IPSec SA, and the corresponding SAs of data flows belonging to the same IPSec automatic tunnel are displayed under the same tunnel. In the IPSec SA list, you can view the tunnel name, data flow identifier, IPSec SA source address, destination address, SPI, protocol, algorithm, lifetime, sending and receiving data flow, connection type, tunnel status and other information.



Number of established IPSec SAs: ...   Number of IPSec SAs in establishment: ...

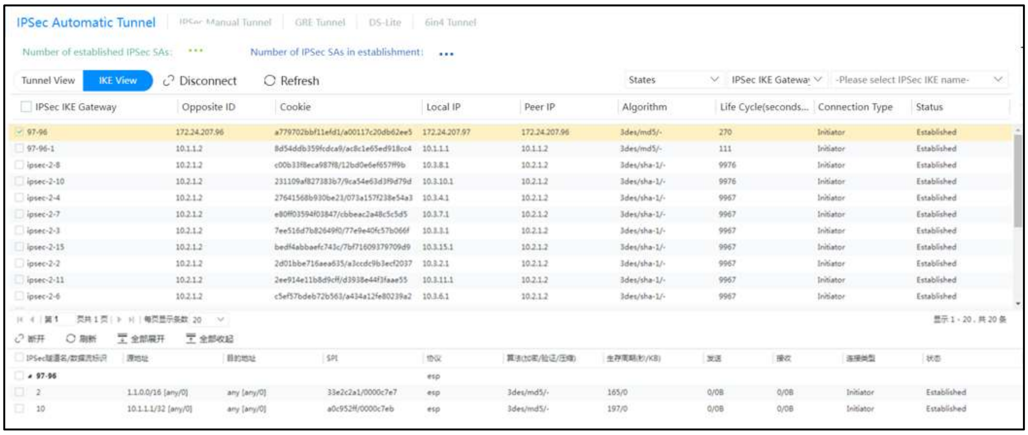
IPSec Tunnel/Data ...	Source Address	Destination Address	SPI	Protocol	Algorithm	Life Cycle(seconds...	Send	Receive	Connection Ty...	Status
97-96				esp						
2	1.1.0.0/16 [any/0]	any [any/0]	2e9eec8d/0000c7de	esp	3des/md5/-	294/0	0/0B	0/0B	Initiator	Established
10	10.1.1.1/32 [any/0]	any [any/0]	79115e03/0000c7db	esp	3des/md5/-	56/0	0/0B	0/0B	Initiator	Established
97-96-1				esp						
5	1.1.5.1/32 [any/0]	2.1.1.1/32 [any/0]	d5cf2f3c/0000c7da	esp	3des/md5/-	54/0	0/0B	0/0B	Initiator	Established
4	1.1.4.1/32 [any/0]	2.1.1.1/32 [any/0]	5f27411a/0000c7d9	esp	3des/md5/-	54/0	0/0B	0/0B	Initiator	Established
3	1.1.3.1/32 [any/0]	2.1.1.1/32 [any/0]	321d7d13/0000c7d8	esp	3des/md5/-	54/0	0/0B	0/0B	Initiator	Established
2	1.1.2.1/32 [any/0]	2.1.1.1/32 [any/0]	63ae0402/0000c7dd	esp	3des/md5/-	63/0	0/0B	0/0B	Initiator	Established
1	1.1.1.1/32 [any/0]	2.1.1.1/32 [any/0]	e0a25b89/0000c7dc	esp	3des/md5/-	63/0	0/0B	0/0B	Initiator	Established

Click "IKE View" to view IKE tunnels.

IKA SA is the SA information consistent with both parties in the first phase of the protocol when establishing an IPSEC VPN tunnel.

In the IKE view tunnel list, the user can view the IPSec IKE gateway name, peer ID, Cookie, local IP, peer IP, algorithm (encryption /authentication/compression), lifetime (seconds/KB), connection type (initiation or response), tunnel status (established or being established) and other information.

IPSEC SA is a secure connection for protecting IPSec data flows negotiated in the second phase of IKE. Select an IKE SA to view all IPSec SAs corresponding to the IKE SA.



Number of established IPSec SAs: ...   Number of IPSec SAs in establishment: ...

IPSec IKE Gateway	Opposite ID	Cookie	Local IP	Peer IP	Algorithm	Life Cycle(seconds...	Connection Type	Status
☑ 97-96	172.24.207.96	a779702bbf11efd1/a00117c20db62ee5	172.24.207.97	172.24.207.96	3des/md5/-	270	Initiator	Established
97-96-1	10.1.1.2	8d54ddb359fcdca9/ac8c1e65ed918cc4	10.1.1.1	10.1.1.2	3des/md5/-	111	Initiator	Established
ipsec-2-8	10.2.1.2	c00b33f8eca987f8/12bd0e6ef657ff9b	10.3.8.1	10.2.1.2	3des/sha-1/-	9976	Initiator	Established
ipsec-2-10	10.2.1.2	231109af827383b7/9ca54e63d3f9d79d	10.3.10.1	10.2.1.2	3des/sha-1/-	9976	Initiator	Established
ipsec-2-4	10.2.1.2	27641568b930be21/073a157f238e54a3	10.3.4.1	10.2.1.2	3des/sha-1/-	9967	Initiator	Established
ipsec-2-7	10.2.1.2	e80ff03594f03847/cbbeac2a48c5c5d5	10.3.7.1	10.2.1.2	3des/sha-1/-	9967	Initiator	Established
ipsec-2-3	10.2.1.2	7ee516d7b82649f0/77e9e40fc57b066f	10.3.3.1	10.2.1.2	3des/sha-1/-	9967	Initiator	Established
ipsec-2-15	10.2.1.2	bedf4abbaefc743c/7bf71609379709d9	10.3.15.1	10.2.1.2	3des/sha-1/-	9967	Initiator	Established
ipsec-2-2	10.2.1.2	2d01bbe716aea635/a3ccdc9b3ecf2037	10.3.2.1	10.2.1.2	3des/sha-1/-	9967	Initiator	Established
ipsec-2-11	10.2.1.2	2ee914e11b8d9cff/d3938e44f3faae55	10.3.11.1	10.2.1.2	3des/sha-1/-	9967	Initiator	Established
ipsec-2-6	10.2.1.2	c5ef57bdeb72b563/a434a12fe80239a2	10.3.6.1	10.2.1.2	3des/sha-1/-	9967	Initiator	Established

IPSec隧道名/数据流标识	源地址	目的地址	SPI	协议	算法(加密/验证/压缩)	生存周期(秒/KB)	发送	接收	连接类型	状态
97-96				esp						
2	1.1.0.0/16 [any/0]	any [any/0]	33e2c2a1/0000c7e7	esp	3des/md5/-	165/0	0/0B	0/0B	Initiator	Established
10	10.1.1.1/32 [any/0]	any [any/0]	a0c952ff/0000c7eb	esp	3des/md5/-	197/0	0/0B	0/0B	Initiator	Established

IPSec Tunnel Filtering

The firewall supports IPSec tunnel filtering based on tunnel status, tunnel name, data flow identifier, source address, and destination address.

IKE Tunnel Filtering

The firewall supports tunnel filtering based on tunnel status, IPSec IKE gateway name, peer ID, local IP, and peer IP.

9.3 Configure an IPSec Manual Tunnel

Manual tunnels are suitable for IPSec configurations in small static networks. Manually specify the SPI and key used at both ends of the IPSec tunnel.

9.3.1 Add IPSec Manual Tunnel

Step 1. Choose “Network > VPN > IPSec Manual Tunnel”.

Step 2. Click “Add”.

Step 3. Configure the name and description of the manual tunnel.

Step 4. Configure basic parameters.

Parameter	**Description**
Local SPI	The value of the local SPI is the same as that of the remote SPI of the peer IPSec VPN gateway.
Remote SPI	The remote SPI is the same as the local SPI value of the peer IPSec VPN gateway.
Address type	Please select IPv4 or IPv6 according to the address type of the network.
Interface	Interface name used to establish IPSec VPN.
Local IP address	IP address of the interface used to establish IPSec VPN.
Peer IP address	The peer IP address of the IPSec VPN needs to be established.

Step 5. Configure the encryption algorithm.

Parameter	Description
Protocol	• ESP, Encapsulating Security Payload Protocol, is used to carry user data that needs to be protected. It not only realizes the authentication function, but also realizes the encryption function. • AH, the authentication header protocol, is used to carry user data that needs to be protected, and only realizes the authentication function.
Authentication Algorithm	When selecting an authentication algorithm for a manual tunnel, the configurations at both ends must be consistent. • MD5: Message Digest Version 5, It is not recommended to configure. • SHA-1: SHA 1 Secure Hash Algorithm. • SHA-256: SHA -256 Secure Hash Algorithm. Recommended configuration. • SM3: National secret algorithm.
Inbound authentication key	Manually configure the authentication key for the incoming firewall. It must be consistent with the manual tunnel authentication key configured on the peer device.
Outbound authentication key	Manually configure the authentication key for the outgoing firewall. It must be consistent with the manual tunnel entry authentication key configured on the peer device.
Encryption	When selecting an encryption algorithm for a manual tunnel, the configurations at both ends must be consistent. Encryption algorithm supports DES, 3DES, AES - 128, AES-256 four kinds, and national secret algorithm SM1, SM4 two kinds. In consideration of security, users are advised not to use the DES algorithm as much as possible. Null means no encryption and configuration is not recommended.
Inbound encryption key	Manually configure the encryption key for the incoming firewall.
Outbound encryption key	Manually configure the encryption key for the outgoing firewall.
Compression algorithm	Select "Not Compressed", no compression algorithm will be used. Select “Deflate” to use the Deflate data compression algorithm. The configuration of this parameter at both ends must be consistent.

Step 6. After the configuration is complete, click “OK”.

9.3.2 Specify Data Flow Entering Tunnel

Step 1. Choose “Policy > Security Policy”.

Step 2. Click “Add”.

Step 3. Divert traffic through security policies.

Select "Security Connection (Tunnel)" as the action, and specify the tunnel for data encapsulation. When the data is a tunnel packet, it is also necessary to specify which tunnel the data comes from.

The configuration of other parameters is consistent with the common security policy.

Step 4. After the configuration is complete, click “OK”.

9.3.3 View IPSec Manual Tunnel

View IPSec manual tunnel

Choose “Data Center > Monitor > Tunnel Monitoring”, and view the created tunnel information on the “IPSec Manual Tunnel” page.

In the manual tunnel list, the user can view the tunnel name, SPI, local address, peer address, algorithm, sent and received packets, tunnel status and other information of the manual tunnel.

IPSec tunnel query

The firewall supports IPSec tunnel query through the tunnel name.

9.4 L2TP VPN

L2TP is a VPN protocol working at the data link layer, using UDP port 1701. The L2TP server function provided by the firewall allocates intranet IPs to L2TP dial-up clients. The client can access the user intranet through the assigned IP.

L2TP itself does not provide the encryption function. By enabling L2TP over IPSec, you can encrypt L2TP packets through IPSec to improve communication security.

9.4.1 Restrictions and Precautions

- To authenticate client users, users must first be created on the firewall or RADIUS server.

  For the configuration of creating users, see 6.2 User.
- It can only be used as an LNS, not a LAC.

9.4.2 Add Authenticated User

Step 1. Choose “Object > Users > Users”, and click “Add”.

Step 2. Configure the parameters such as the name, password, and validity period of the authenticated user.

Step 3. After the configuration is complete, click “OK”.

You can plan the user group and user role to which the user belongs as required.

9.4.3 Add Authentication Server

L2TP users only support local server authentication and RADIUS server authentication.

Step 1. Choose “Object > Users > Authentication Server”, and click “Add”.

Step 2. Configure the authentication server parameters.

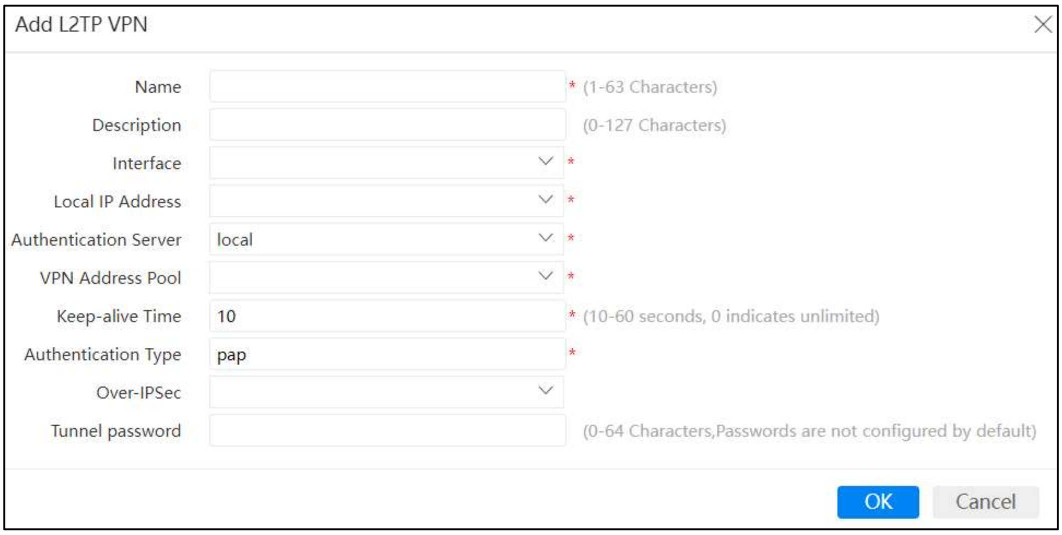
For detailed configuration, see 6.2.3 Authentication Server.

9.4.4 Configure LNS

Step 1. Select "Network > VPN > L2TP VPN".

Step 2. Click “Add”.

Step 3. Configure L2TP VPN parameters.



Add L2TP VPN

Name		* (1-63 Characters)
Description		(0-127 Characters)
Interface		*
Local IP Address		*
Authentication Server	local	*
VPN Address Pool		*
Keep-alive Time	10	* (10-60 seconds, 0 indicates unlimited)
Authentication Type	pap	*
Over-IPSec		
Tunnel password		(0-64 Characters,Passwords are not configured by default)

Parameter	Description
Name	Specify the name of the L2TP VPN.
Description	The remarks of L2TP VPN are to distinguish it from other L2TP VPNs.

Parameter	Description
Interface	Specify the interface to enable the L2TP VPN tunnel.
Local IP address	Select the IP address of the L2TP VPN tunnel interface. When auto is selected, the client can send a request to any float-type IP v4 address on the interface, and the firewall can respond.
Authentication server	The authentication server is used to authenticate dial-up users. Authentication server supports local server and Radius server.
VPN address pool	Specify the name of the address pool that allocates addresses for clients. If you need to add a new address pool, select "Add VPN Address Pool" from the drop-down menu.
Keep alive time	When configured as 0, client keepalive detection is not enabled. The keepalive time can be configured from 10 to 60 seconds. For example, if it is configured as 10 seconds, the firewall will send a keepalive packet to the client every 10 seconds. If the firewall does not receive a response, it will start the keepalive mechanism to continue detection. If there is still no response after 3 detections, then The client is considered offline and disconnected.
Authentication method	One or more of pap, chap, and ms-chap can be selected. The authentication method used by the client must be one of the selected authentication methods.
Over-IPSec	When L2TP VPN is used together with IPSec VPN, the name of the IPSec VPN tunnel needs to be specified. For the L2TP over IPSec of the MAC system, the IKE gateway on the firewall side should be configured as "Dynamic address mode" + "Accept any peer ID"; For the L2TP over IPSec of the Windows system, the IKE gateway on the firewall side should be configured as a "Dial-up user group". The connection type is " responder ". The IPSec tunnel encapsulates the L2TP data. When configuring IPSec, it is recommended to configure the protection data flow as any.
Tunnel password	When a tunnel password is configured on the LAC, a consistent tunnel password must also be specified on the LNS.

Step 4. After the configuration is complete, click “OK”.

In the L2TP VPN list, you can view information such as the interface bound to each L2TP tunnel, authentication server, client address pool, keepalive time, authentication method, and IPSec tunnel name over IPSec.

9.5 PPTP VPN

PPTP is a VPN protocol working at the data link layer, using TCP port 1723. The PPTP client connects to the firewall through PPTP dial-up. After passing the authentication, the firewall assigns the intranet IP to the PPTP client. PPTP clients can use the assigned intranet IP to access the internal network.

9.5.1 Configure PPTP Users

Remote users must pass PPTP authentication before they can access the PPTP VPN network.

To authenticate client users, users must be created on the firewall or RADIUS server.

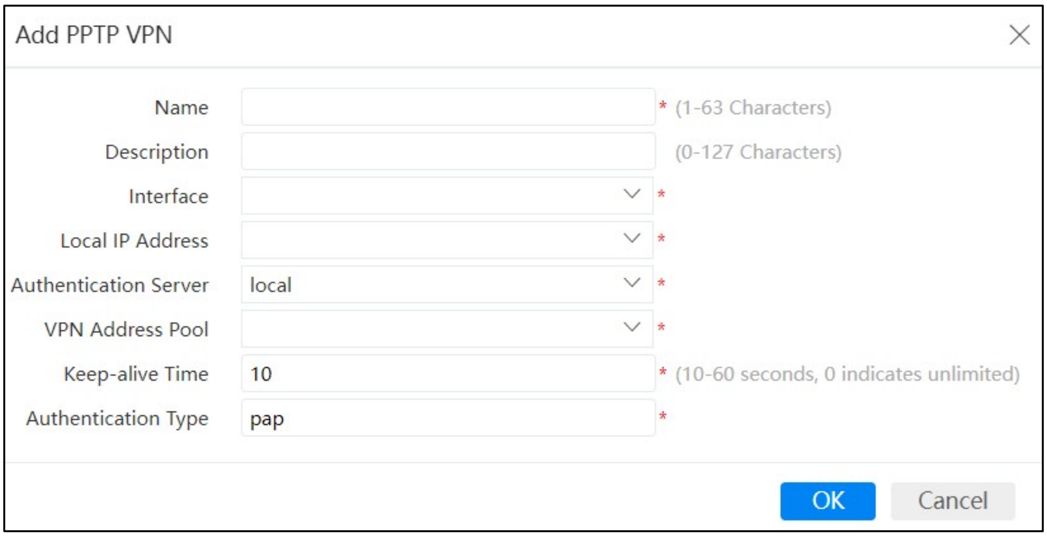
For creating users, see 6.2 User.

9.5.2 Configure PPTP Server

Step 1. Select "Network > VPN > PPTP VPN".

Step 2. Click “Add”.

Step 3. Configure PPTP VPN parameters.



Add PPTP VPN

Name: * (1-63 Characters)

Description: (0-127 Characters)

Interface: *

Local IP Address: *

Authentication Server: local *

VPN Address Pool: *

Keep-alive Time: 10 * (10-60 seconds, 0 indicates unlimited)

Authentication Type: pap *

Parameter	Description
Name	Specify the name of the PPTP VPN.
Description	The remarks of PPTP VPN are to distinguish it from other PPTP VPNs.

Parameter	Description
Interface	Select the interface to enable PPTP VPN.
Local IP address	Select the tunnel interface IP address of the PPTP VPN. When auto is selected, the client can send a request to any float- type IP v4 address on the interface, and the firewall can respond.
Authentication server	Select the PPTP VPN client authentication server name. Authentication server supports local server and Radius server.
VPN address pool	Specify the name of the address pool that allocates addresses for clients. If you need to add a new address pool, select "Add VPN Address Pool " from the drop-down menu.
Keep alive time	The keepalive time can be configured from 10 to 60 seconds. For example, if it is configured as 10 seconds, the firewall will send a keepalive packet to the client every 10 seconds. If the firewall does not receive a response, it will start the keepalive mechanism to continue detection. If there is still no response after 3 detections, then The client is considered offline and disconnected.
Authentication type	One or more of pap, chap, and ms-chap can be selected. The authentication method used by the client must be one of the selected authentication methods.

Step 4. After the configuration is complete, click “OK”.

In the PPTP VPN list, you can view information such as the interface bound to each PPTP tunnel, authentication server, client address pool, keepalive time, and authentication method.

9.6 GRE VPN

GRE (Generic Routing Encapsulation) adopts Tunnel technology, which is a VPN technology working at the network layer.

The firewall supports GRE tunnels, which encapsulate the packets of network layer protocols (such as IP and IPX), so that these encapsulated packets can be transmitted in another network layer protocol (such as IP).

9.6.1 Create a Tunnel Interface

Step 1. Choose “Network > Interface”.

Step 2. Click "Add" and select " Tunnel Interface" from the drop-down menu.

Step 3. Configure the tunnel interface.

Step 4. (Optional) Configure the IP address of the interface.

If no IP address is specified on the tunnel interface, the first float address configured on the source interface will be used when establishing the GRE tunnel.

Step 5. (Optional) Bind the tunnel.

You don't need to configure it here, and you can bind the Tunnel interface when configuring the GRE tunnel.

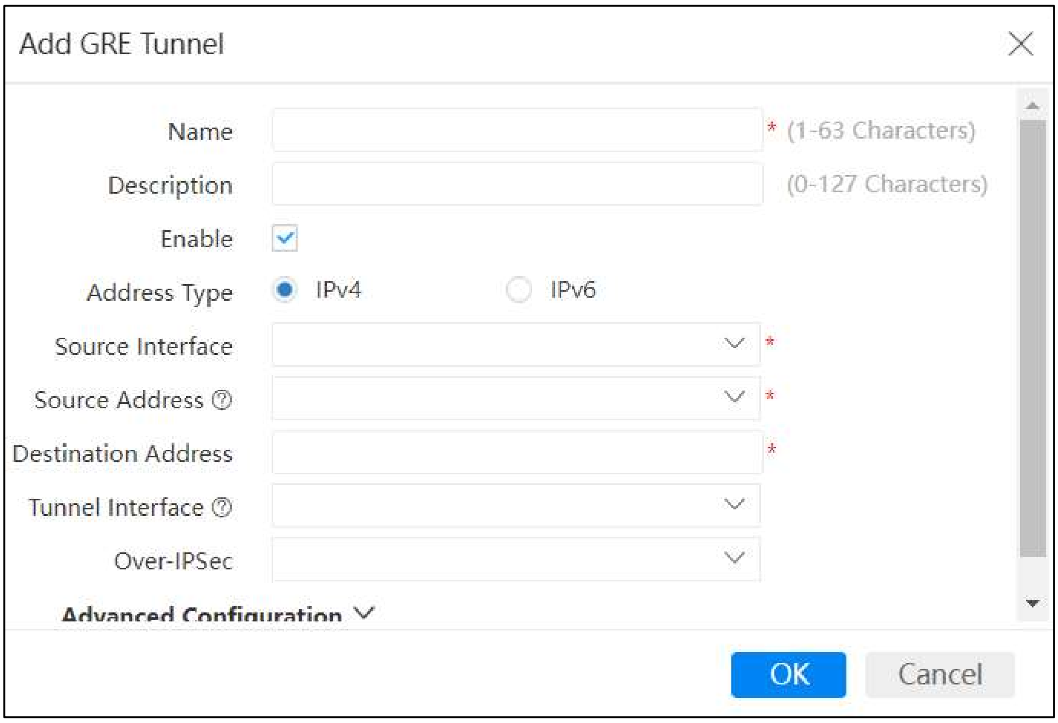
Step 6. Click “OK”.

9.6.2 Configure GRE Tunnel

Step 1. Choose “Network > VPN > GRE Tunnel”.

Step 2. Click “Add”.

Step 3. Configure the GRE tunnel parameters.



Add GRE Tunnel

Name * (1-63 Characters)

Description (0-127 Characters)

Enable ☑

Address Type ● IPv4 ○ IPv6

Source Interface *

Source Address ⓘ *

Destination Address *

Tunnel Interface ⓘ

Over-IPSec

Advanced Configuration

Parameter	Description
Name	Specifies the name of the GRE tunnel.
Description	Add the remarks of the GRE tunnel to distinguish it from other GRE tunnels.
Enable	Check the box to enable GRE tunneling. Otherwise, the GRE tunnel will not take effect.

Parameter	Description
Source interface	Select the name of the source interface used by the GRE tunnel.
Source address	Select the source interface IP address used by the GRE tunnel. When selecting auto, as the initiator, the address of the first float type on the interface is used by default; As the recipient, any float type IP address on the interface is used by default.
Destination address	The destination address of the GRE tunnel, that is, the IP address of the physical interface at the peer end of the GRE tunnel.
Tunnel interface	Select the tunnel interface on the firewall.
Over-IPSec	When used with IPSec, select the IPSec tunnel name.
Advanced configuration	
Key	Used to authenticate the peer tunnel. The key value configuration at both ends should be consistent. Configured as 0 means not enabled.
Set checksum	It is used by the peer end to check whether the GRE packets sent by the firewall are legal. After checking, the firewall will set the checksum when sending the GRE packet. After the peer end receives it, it will calculate a new checksum based on the received packet and compare it with the checksum set in the firewall. If it is inconsistent, the packet will be discarded. If consistent, the packet is legal.
Keep-alive Detection	Check to enable keep-alive detection. Otherwise, it will not be enabled. Detection period: The default is 300 seconds, and a detection is performed every 300 seconds, which can be customized by the user. Number of retries: The default is 10 times, which can be customized by the user. The number of retries after no response to the probe. If the number of retries exceeds the number of retries and there is still no response, the GRE tunnel will fail.

Step 4. After the configuration is complete, click “OK”.

After adding the GRE tunnel, the user also needs to add the corresponding static route to the static route to divert the traffic to be transmitted through the GRE tunnel to the tunnel interface.

In the GRE tunnel list, you can view information such as the tunnel source interface, destination address, tunnel interface, and Over IPSec tunnel name of each tunnel.

9.6.3 View GRE Tunnel

Choose “Data Center > Monitor > Tunnel Monitor”, and select GRE Tunnel from the drop-down list on the right. If you need to query a specific tunnel, you can select the tunnel name in the drop-down box.

In the GRE tunnel monitoring interface, users can view the tunnel name, peer identification, local address, destination address, sent bytes, received bytes, and status after the GRE tunnel is established.

10 VXLAN

10.1 Configure VXLAN

10.1.1 Serve as a L2 VXLAN Gateway

Add Overlay NVE Interface

Step 1. Choose “Network > Interface”.

Step 2. Click “Add”, and select “Overlay Nve Interface” from the drop-down menu.

Step 3. Configure the parameters of the Overlay Nve interface.

The interface name is nve 1 by default, the encapsulation type is vxlan, and the working mode is switching mode Trunk. Select the security domain that the interface belongs to, and configure the VLAN ID and Native VLAN that the interface allows to pass through.

The VLAN IDs allowed to pass through the interface must include the VLAN IDs mapped to the VXLAN network.

If no security domain is selected, the security domain defaults to any, that is, any security domain can be used. The default value of Native VLAN is 1.

Step 4. After the configuration is complete, click “OK”.

Basic Configuration of VXLAN

The VTEP is the endpoint of the VXLAN tunnel. The source IP address in the VXLAN packet is the local VTEP address, and the destination IP address is the VTEP address of the peer node. A pair of VTEP addresses corresponds to a VXLAN tunnel.

Step 1. Choose “Network > VXLAN”.

Step 2. On the " VXLAN Basic Configuration" page, select the " Enable " check box to enable the VXLAN function.

Step 3. Configure the local VTEP address.

The interface is the IP address of the interface communicating with the peer VTEP, and is used for negotiation with the peer VTEP. The interface IP address must be an IPv4 address in dotted decimal format.

Step 4. Configure the local VTEP port.

The value range of the port is 1~ 65535, and the default port is 4789.

Step 5. After the configuration is complete, click “Apply”.

VXLAN Network Management

VXLAN network identifier VNI is similar to the VLAN ID and is used to distinguish VXLAN segments. Virtual machines in different VXLAN segments cannot directly communicate with each other at Layer 2. A VNI represents a tenant.

Step 1. Choose “Network > VXLAN”.

Step 2. Click the “VXLAN Network Management” tab.

Step 3. Click “Add”.

Step 4. Configure VXLAN network parameters.

Parameter	Description
VNI	Specify the VNI of the VXLAN network. VNI consists of 24 bits and uniquely identifies a VXLAN network. Its value range is 1~16777215.
Map VLAN ID	Configure the VLAN ID for VXLAN network mapping. The value range is 0 ~4094. A value of 0 means that the mapping VLAN function is not enabled. Only when the mapping VLAN function is enabled, the overlay nve interface status will be enabled. The VLAN IDs allowed to pass through the interface must include the VLAN IDs mapped by VXLAN.
Peer VTEP	Configure the IP address of the interface through which the peer VTEP communicates with the local VTEP. The IP address of the peer VTEP will be used as the destination address of the VXLAN packet. The value is in dotted decimal format. Multiple items can be configured, separated by a carriage return, and a maximum of 32 items can be configured.

Step 5. After the configuration is complete, click “OK”.

10.1.2 Server as a L3 VXLAN Gateway

Basic Configuration of VXLAN

The VTEP is the endpoint of the VXLAN tunnel. The source IP address in the VXLAN packet is the local VTEP address, and the destination IP address is the VTEP address of the peer node. A pair of VTEP addresses corresponds to a VXLAN tunnel.

Step 1. Choose “Network > VXLAN”.

Step 2. On the "VXLAN Basic Configuration" page, select the "Enable" check box to enable the VXLAN function.

Step 3. Configure the local VTEP address.

The interface is the IP address of the interface communicating with the peer VTEP, and is used for negotiation with the peer VTEP. The interface IP address must be an IPv4 address in dotted decimal format.

Step 4. Configure the local VTEP port. The value range of the port is 1~65535, and the default port is 4789.

Step 5. After the configuration is complete, click “Apply”.

VXLAN Network Management

VNI (VXLAN Network Identifier): The VXLAN network identifier VNI is similar to a VLAN ID and is used to distinguish VXLAN segments. Virtual machines in different VXLAN segments cannot directly communicate with each other at Layer 2. A VNI represents a tenant.

Step 1. Choose “Network > VXLAN”.

Step 2. Click the “VXLAN Network Management” tab.

Step 3. Click “Add”.

Step 4. Configure VXLAN network parameters.

Parameter	Description
VNI	VNI consists of 24 bits, and its value ranges from 1 to 16777215.
Map VLAN IDs	The value range is 0 ~4094. A value of 0 means that the mapping VLAN function is not enabled. Only when the mapping VLAN function is enabled, the overlay nve interface status will be enabled. The VLAN IDs allowed to pass through the interface must include the VLAN IDs mapped by VXLAN.
Peer VTEP	Configure the IP address of the interface through which the peer VTEP communicates with the local VTEP. The IP address of the peer VTEP will be used as the destination address of the VXLAN packet. The value is in dotted decimal format. Multiple items can be configured, separated by a carriage return, and a maximum of 32 items can be configured.

Step 5. After the configuration is complete, click “OK”.

Add Overlay Routing Interface

Step 1. Choose “Network > Interface”.

Step 2. Click “Add” and select “Overlay Routing Interface” from the drop-down menu.

Step 3. Configure the parameters of the overlay routing interface.

The interface name must start with vn, followed by the number 1~512, such as "vn1". The encapsulation type of the interface is vxlan.

Select the VNI and security zone bound to the interface. Configure the IP address of the interface. The IP address of this interface can be specified arbitrarily, but it must be in the same network segment as the IP address of the overlay routing interface on the opposite end.

Add interface address, and the interface address supports IPv4 and IPv6 addresses.

Step 4. After the configuration is complete, click “OK”.

10.1.3 Simultaneously Serve as L2 and L3 VXLAN Gateways

Add Overlay NVE Interface

Step 1. Choose “Network > Interface”.

Step 2. Click “Add”, and select “Overlay Nve Interface” from the drop-down menu.

Step 3. Configure the parameters of the Overlay Nve interface.

The interface name is nve 1 by default, the encapsulation type is vxlan, and the working mode is switching mode Trunk. Select the security zone that the interface belongs to, and configure the VLAN ID and Native VLAN that the interface allows to pass through.

The VLAN IDs allowed to pass through the interface must include the VLAN IDs mapped to the VXLAN network.

If no security zone is selected, the security zone defaults to any, that is, any security zone can be used. The default value of Native VLAN is 1.

Step 4. After the configuration is complete, click “OK”.

Basic Configuration of VXLAN

The VTEP is the endpoint of the VXLAN tunnel. The source IP address in the VXLAN packet is the local VTEP address, and the destination IP address is the VTEP address of the peer node. A pair of VTEP addresses corresponds to a VXLAN tunnel.

Step 1. Choose “Network > VXLAN”.

Step 2. On the "VXLAN Basic Configuration" page, select the "Enable" check box to enable the VXLAN function.

Step 3. Configure the local VTEP address.

The interface is the IP address of the interface communicating with the peer VTEP, and is used for negotiation with the peer VTEP. The interface IP address must be an IPv4 address in dotted decimal format.

Step 4. Configure the local VTEP port. The value range of the port is 1~65535, and the default port is 4789.

Step 5. After the configuration is complete, click “Apply”.

VXLAN Network Management

VNI (VXLAN Network Identifier): The VXLAN network identifier VNI is similar to a VLAN ID and is used to distinguish VXLAN segments. Virtual machines in different VXLAN segments cannot directly communicate with each other at Layer 2. A VNI represents a tenant.

Step 1. Choose “Network > VXLAN”.

Step 2. Click the “VXLAN Network Management” tab.

Step 3. Click “Add”.

Step 4. Configure VXLAN network parameters.

Parameter	Description
VNI	VNI consists of 24 bits, and its value ranges from 1 to 16777215.
Map VLAN IDs	The value range is 0 ~4094. A value of 0 means that the mapping VLAN function is not enabled. Only when the mapping VLAN function is enabled, the overlay nve interface status will be enabled. The VLAN IDs allowed to pass through the interface must include the VLAN IDs mapped by VXLAN.
Peer VTEP	Configure the IP address of the interface through which the peer VTEP communicates with the local VTEP. The IP address of the peer VTEP will be used as the destination address of the VXLAN packet. The value is in dotted decimal format. Multiple items can be configured, separated by a carriage return, and a maximum of 32 items can be configured.

Step 5. After the configuration is complete, click “OK”.

Add Overlay Routing Interface

Step 1. Choose “Network > Interface”.

Step 2. Click “Add” and select “Overlay Routing Interface” from the drop-down menu.

Step 3. Configure the parameters of the overlay routing interface.

The interface name must start with vn, followed by the number 1 ~512, such as "vn1". The encapsulation type of the interface is vxlan.

Select the VNI and security zone bound to the interface. Configure the IP address of the interface. The IP address of this interface can be specified arbitrarily, but it must be in the same network segment as the IP address of the overlay routing interface on the opposite end.

Add interface address, and the interface address supports IPv4 and IPv6 addresses.

Step 4. After the configuration is complete, click “OK”.

10.1.4 VXLAN Dynamic MAC Address

The firewall supports dynamic learning of the VXLAN MAC address table. After the VTEP receives the VXLAN packet sent by the remote VTEP from the tunnel, it records the VNI and decapsulates the packet to restore the original Layer 2 data frame, and adds the source MAC address of the data frame to its VXLAN address table..

On the VXLAN dynamic MAC address page, you can view the VNI and peer VTEP corresponding to the MAC address and the timeout period.

In order to adapt to network changes, the MAC address table needs to be continuously updated. The automatically generated entries in the MAC address table are not permanently valid, and each entry has a timeout period. The entries that have not been updated after the timeout expires will be deleted. If the record of the entry is refreshed before the timeout expires, the timeout of the entry will be recalculated.

10.1.5 VXLAN Static MAC Address

Statically configuring the VXLAN MAC address table refers to manually specifying the VNI and VTEP address to which the MAC address of the remote VM belongs.

Step 1. Choose “Network > VXLAN > VXLAN Static MAC”.

Step 2. Click “Add”.

Step 3. Configure VXLAN static MAC parameters.

Parameter	Description
Encapsulation type	The VXLAN tunnel encapsulation type is " vxlan ".
MAC address	The source MAC address of the VM.
VNI	Identifies the VXLAN segment to which the VM belongs.
Peer VTEP	IP address of the peer VTEP.

Step 4. After the configuration is complete, click “OK”.

After the configuration is complete, the MAC item can be viewed in the VXLAN static MAC list, and the VNI and peer VTEP corresponding to the MAC address can be viewed.

11 Security Policies and Security Configuration Files

The firewall controls traffic through security policies. In the security policy, the content security detection defined by the security configuration file can be performed on the traffic by referring to the security configuration file or the security configuration file group.

Security configuration files include anti-virus, IPS intrusion prevention (including vulnerability protection, anti-spyware), URL filtering, file filtering, content filtering, email filtering, behavior control, and linkage terminal control.

A security configuration file group is the combination of one or more security configuration files including anti-virus, IPS intrusion prevention (including vulnerability protection, anti-spyware), URL filtering, file filtering, content filtering, mail filtering, behavior control, and linkage terminal control.

A security configuration file or security configuration file group can be referenced by multiple security policies.

When the security configuration file is referenced in a security policy, if you need to perform content inspection on SSL-encrypted traffic, you need to configure an SSL decryption policy to decrypt the traffic.

11.1 Security Policy

The firewall controls traffic through security policies. The security policy determines whether the traffic can pass through the firewall and whether it needs to be transmitted through the VPN tunnel. If the traffic matches the security policy and the action is "Allow", the traffic is allowed to pass through the firewall; if the traffic matches the security policy and the action is "Deny" or the traffic cannot match any security policy in the security policy list, the traffic is denied to pass. An action of "Secure Connection" requires the traffic to be encrypted and transmitted through the IPSec tunnel.

11.1.1 Restrictions and Precautions

- The security policies in the security policy list are matched in order from top to bottom, and the higher the security policy, the higher the priority. Therefore, when configuring security policies, you need to follow the order from special to general. In this way, the traffic will preferentially match the finer special policy instead of the general policy.
- The firewall rejects traffic that does not match any security policy by default.
- In consideration of security, it is recommended to specify precise source IP address and destination IP address instead of "any".
- In order to allocate storage and analysis performance more reasonably, enable the logging function only for the traffic that needs to be logged.

11.1.2 Create a New Security Policy

Security policies can restrict traffic based on source security zone, destination security zone, source user, source address/region, destination address /region, service, application, time, parameters, and can implement vulnerability protection, anti- spyware, URL filtering, anti-virus, content filtering, file filtering, mail filtering, behavior control, linkage terminal control and other security detection.

Step 1. Choose “Policy > Security Policy”.

Step 2. Click “Add”.

Step 3. Configure security policy parameters.

Parameter	Description
Name	Configure the name of the security policy.
Description	Add a description to the security policy.
Enable	Security policies must be enabled to take effect.

Parameter	Description
Action	Configure the action to be executed after the traffic matches the security policy. • Permit After the traffic matches the security policy, it is allowed to pass through the firewall. • Deny After the traffic matches the security policy, it is discarded directly, and the traffic is not allowed to pass through the firewall. • Security connection (tunnel) After the traffic matches the security policy, the traffic is encapsulated, and the traffic is transmitted through the tunnel.
Tunnel	When the action selects "Security connection (tunnel)", the tunnel name of this section needs to be specified.
Source zone	Select the security zone to which the inbound interface belongs. Support selecting multiple security zones.
Destination zone	Select the security zone to which the outgoing interface belongs. Support selecting multiple security zones.
Source user	Select the authentication server and user or user group to send traffic. Multiple source users are separated by commas (,). The security policy does not authenticate users, but only controls traffic access based on users.
Source Address/Region	Select the source address/region for the traffic. The source address supports address objects and address groups, and the region supports predefined countries/regions and custom countries/regions. Please configure loose or strict source address /region according to the scenario. Enter the keyword in the text box to search for addresses or regions in the drop-down box. Click the text box of “Source Address/Region” to select the address or region to add. By default, all addresses, address groups, and regions are displayed. You can choose to display only addresses, address groups, predefined areas, or custom areas in the drop-down box. Click the "Add" button to add new address objects, address groups and regions. The selected address or region can be deleted by pressing the "Delete" button.
Destination address/area	Select the destination address /region for the traffic. The selection method is the same as selecting the source address/region.

Parameter	Description
Service	Service is used to set the type of service for traffic that is allowed or denied to pass. All services are displayed by default. Enter keywords in the text box to search. After selecting the check box in front of the service, click anywhere on the security policy page to return to the security policy page, and the service is added to the corresponding text box. The policy restrictions can be applied to traffic by specifying services.
App	Application is used to set the application or group of applications to allow or deny traffic. All apps and app groups are displayed by default. Enter keywords in the text box to search. After selecting the check box in front of the application or application group, click anywhere on the security policy page to return to the security policy page, and the application is added to the corresponding text box. The policy restrictions can be applied to traffic by specifying applications. **Notes** Application parameters are matched only after the traffic application is identified. Only other parameters are matched before the application of traffic is identified.
From tunnel	When the traffic to be hit is sent from the peer end to the firewall through the tunnel, the user needs to specify the name of the tunnel in “From Tunnel”. At the same time, the address range selected in the source address is the peer intranet address, and the address range selected in the destination address is the local intranet address.
Time	Time is used to limit traffic based on time period. For example, configure different security policies for working hours and rest hours.
VLAN	When the firewall works in transparent mode, the traffic of different VLANs can be restricted.
Flow log	Select the "Record Log " checkbox to enable the function of recording traffic logs. Log when session ends. Please enable the logging function as needed. It is recommended to only enable the logging function for important traffic. The domain name log will only be recorded after it hits the security policy and the traffic log switch is enabled.

Parameter	Description
Profile type	You can specify which content inspections are performed on traffic through a security policy file or a security policy file group. When selecting a configuration file, various content filtering profiles can be specified individually. The supported referenced security configuration files include vulnerability protection, anti-spyware, URL filtering, anti-virus, content filtering, file filtering, email filtering, behavior control, and linkage terminal control.
Long connection	After selecting the "Long Connection" check box, enable the long connection function. Select a long connection in the long connection text box, or set the name and time of the long connection by adding. After adding a persistent connection, security policy control can be performed on the persistent connection session.

Step 4. After the configuration is complete, click “OK”.

The configured security policies are displayed in the security policy list. You can see the name of the configured security policy, source security zone, destination security zone, source address/region, destination address /region, service, application, time, security configuration file, action, and number of hits.

You can enable or disable a certain security policy in the list.

The security policies in the security policy list can be edited, copied, deleted, sorted, cleared, searched, and refreshed.

11.1.3 Create Security Policy by Copying

The firewall supports creating a new security policy by copying.

Step 1. Select a created security policy.

Step 2. Click “Copy”.

Step 3. Set the parameters of the security policy.

When a security policy is created through copying, the parameters of the security policy are the same as those of the copied security policy. The settings can be modified on this basis.

Step 4. After the configuration is complete, click “OK”.

11.1.4 Adjust the Order of Security Policies

The order of the security policy in the security policy list is related to the priority of the security policy. The security policy at the top has the highest priority and is matched first. You can adjust the execution order of security policies by adjusting the positions of security policies in the list.

The finer the security policy needs to be, the higher the priority is. Otherwise, if the data flow matches the broader security policy, it will not continue to match the fine security policy.

The security policy delivered by the smart management analysis system has a higher priority than the local security policy of the firewall. Only the order of the local security policy of the firewall can be adjusted.

Step 1. Select a security policy.

Step 2. Click “Reorder”.

Step 3. Select adjusting the policy.

Adjusting the policy relationship supports "top", "before", "after" and "end". These keywords can be used to adjust the security policy to the top of the list, before the specified policy, after the specified policy, and at the end.

Step 4. Click “OK”.

11.1.5 Set Displayed Security Policy Parameters

By default, the "Description" parameter is not displayed in the security policy list. Users can click ⋮ on the left of the security policy list to select the parameters to be displayed. Select the check box corresponding to the parameter to display the parameter, and uncheck the check box corresponding to the parameter to not display the parameter.

11.1.6 Filter and Query Security Policies

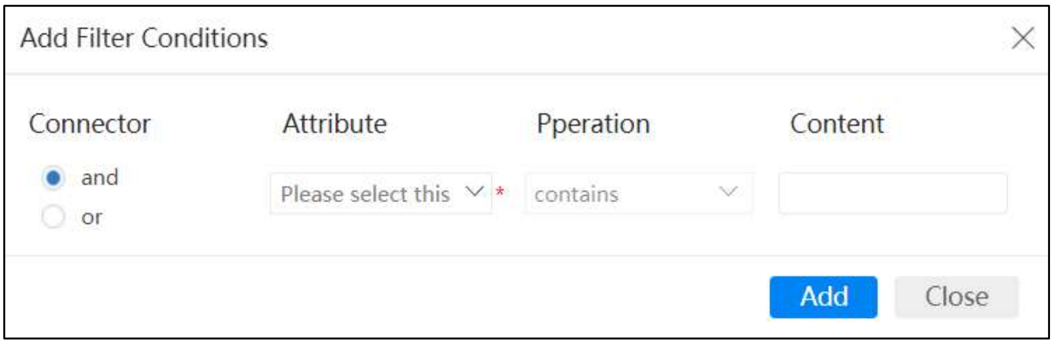
Security policies support multiple query methods such as fuzzy query, advanced query, and conditional query.

Fuzzy Query

Fuzzy query supports query by name, description, source-destination security zone, source-destination address/region, and service keywords. After entering a keyword in the query text box and clicking 🔍, the security policies including the keyword are displayed in the security policy list.

Query by Filtering Conditions

Click + to add filtering conditions. In “Add Filter Condition”, select the connector, attribute name, and operation, enter the query content, and click “Add”.



Add Filter Conditions

Connector	Attribute	Pperation	Content
● and ○ or	Please select this *	contains	

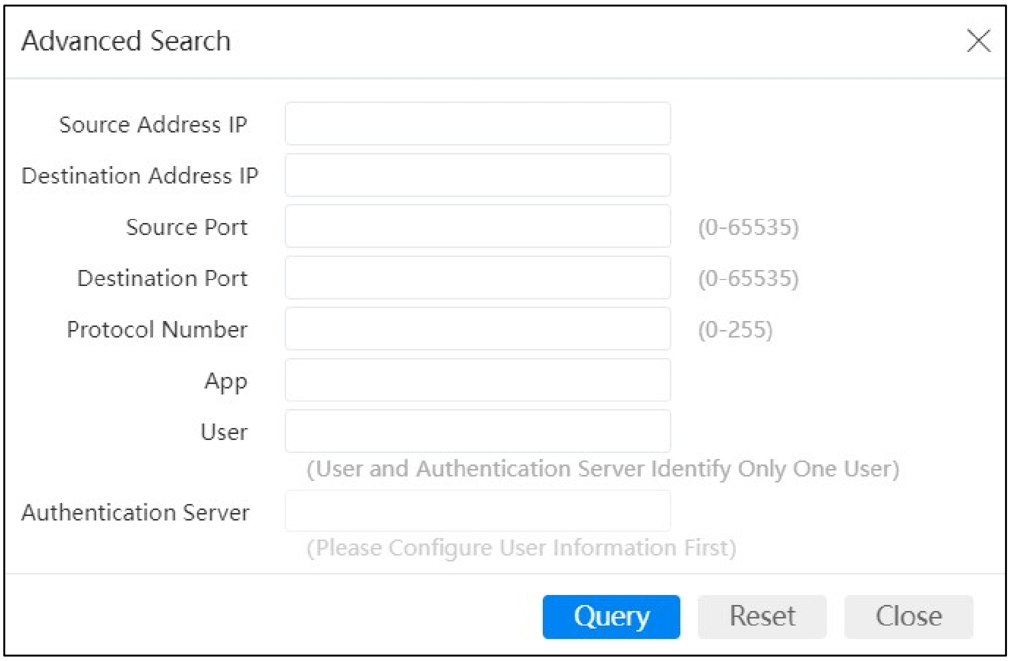
Parameter	Description
Connector	Multiple conditions can be connected by the connector "and (and)" or "or (or)". • and means "and" operation, and the logs that meet all conditions at the same time will be hit. • or means "or" operation, as long as one of the multiple conditions is met, it will be hit. Search in order from left to right. and has higher priority than or. When you want to perform the or operation first, you can add single brackets outside the conditions for performing the or operation.
Attribute	Select the condition to filter from the drop-down box.
Operation	Select the operation to be performed on the attribute value in the drop-down box. The following describes the operations under all attribute names: • =: Only when the information content is completely consistent with the query content can it be hit. • !=: not equal to. Informational content is not equal to a hit to query content. • Contains: As long as the information content contains the query content, it will be hit.
Content	Under a specified attribute, the address, value, or content that the user wants to find needs to be satisfied.

Repeat the process to add another conditional keyword. The default connector is "and", which can be set to "or". After the settings are complete, click “Close”. After closing the add filter page, the search starts automatically.

Click 🧹 to clear existing criteria in the search bar.

Advanced Search

Click the "Advanced Query" button, and in the "Advanced Query" dialog box, set the query conditions for precise query.



Advanced Search

Source Address IP

Destination Address IP

Source Port (0-65535)

Destination Port (0-65535)

Protocol Number (0-255)

App

User

(User and Authentication Server Identify Only One User)

Authentication Server

(Please Configure User Information First)

11.1.7 View Redundancy Policy

The firewall supports redundancy analysis of created security policies. The results of the redundancy analysis are displayed on the "Redundancy Policy" page.

The main function of the policy redundancy analysis function is to help users find whether there are redundant or ineffective rules in the security policy list. If yes, the corresponding security policy will be displayed in the policy redundancy analysis list. Users can check whether redundant security policy rules are caused by repeated configurations, wrong configurations, or wrong order of rules.

Click the button corresponding to each redundant policy to pop up the security policy that has a redundant relationship with this redundant policy and is currently in effect.

Users can compare the effective security policy to determine how to modify the redundancy policy.

Policy redundancy analysis and judgment method:

Assume that there are two security policies a and b, policy a comes first and policy b follows, that is, policy a has a smaller serial number than policy b. The b policy must meet all the following conditions at the same time, and it will be judged as a redundant policy. The conditions are as follows:

1. The source address range of policy a contains the same source address range and type as policy b (both IPv4 or IPv6);
2. The destination address range of policy a includes the destination address range of policy b, and they are of the same type (both IPv4 or IPv6);
3. The application of policy a includes the application of policy b;
4. The service of policy a includes the service of policy b;
5. The source security zone of policy a is the same as the source security zone of policy b;
6. The destination security zone of policy a is the same as that of policy b or the destination security zone of policy a is any
7. The vlan of policy a includes the vlan of policy b (if configured);
8. The time range of the time plan of policy a includes the time range of the time plan of policy b (if configured)

11.2 Anti-Virus

Antivirus describes the antivirus solutions supported by the firewall and how to configure antivirus configuration files. The anti-virus configuration file can configure anti-virus for SMTP, POP3, IMAP, FTP, SMB, and HTTP protocols. By referencing the antivirus configuration file in the security policy, virus detection can be performed on the traffic matching the security policy.

11.2.1 Overview

The next-generation firewall supports local antivirus, cloud antivirus, and cloud sandbox detection. Deploying local anti-virus, cloud anti-virus and cloud sandbox at the same time can improve the anti-virus rate and better ensure the network security of users. Cloud antivirus includes two solutions: private cloud antivirus and public cloud antivirus.

Local Antivirus

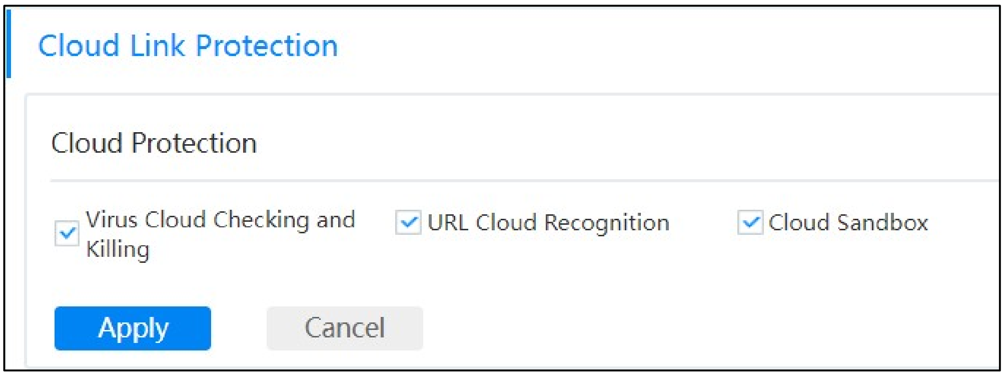
The local anti-virus scans and kills viruses through the anti-virus function built into the firewall. The firewall itself needs to install a virus library. Users can also customize virus features, and support setting virus exceptions. In this mode, the user needs to update the virus database regularly, and the quality of the virus database directly affects the antivirus effect.

After the firewall caches the transmitted files or emails through the anti-virus engine, it performs virus detection on the entire file or email content.

Public Cloud Antivirus Solution

Tianyuyun Yunfang provides cloud scanning and killing functions. It is applicable to scenarios where the firewall can access the public network.

To use public cloud antivirus, the virus cloud antivirus function must be enabled.



Cloud Link Protection

Cloud Protection

☑ Virus Cloud Checking and Killing ☑ URL Cloud Recognition ☑ Cloud Sandbox

Cloud sandbox virus detection

The cloud sandbox is used with the virus detection function and is mainly used to detect unknown viruses. After the cloud sandbox is enabled, the firewall sends suspicious files detected by the antivirus to the cloud sandbox. Trigger suspicious files to run through the cloud sandbox to determine whether the files are malicious.

11.2.2 Restrictions and Precautions

- When using the antivirus function, the antivirus and virus database upgrade functions in the loaded firewall license must be "authorized".
- Cloud anti-virus also needs to use the local anti-virus engine, so when the local anti-virus function cannot be used, the cloud anti-virus function cannot be used either.
- Antivirus profiles must be referenced in security policies and are affected by the application of security policy configurations. For example, HTTP must be specified in the security policy to perform antivirus detection and processing on HTTP.
- The virus database has been upgraded to the latest version.
- In order to ensure processing efficiency, only applications requiring virus detection are enabled in the antivirus configuration file. Applications that are not used on the network do not need to have virus detection enabled.
- The maximum number of decompression layers for virus files is 6 layers, and the maximum number does not exceed 2M. The files that exceed the range will be released directly

without virus detection. The maximum number of decompression layers and the maximum file size can be set under the global configuration of "File Filter".

11.2.3 Add Virus feature

Step 1. Choose “Object > Custom Signatures > Virus”.

Step 2. Click “Add”.

Step 3. Set virus sample parameters.

Parameter	Description
virus name	Set the name of the virus.
MD5	MD5 consists of 32 hexadecimal characters.

Step 4. After the configuration is complete, click “OK”.

The configured virus samples are displayed in the virus list. You can view the virus name, virus ID, MD5 value and the number of references.

11.2.4 Add Antivirus Configuration File

The firewall provides comprehensive and powerful virus detection and protection functions, supporting virus scanning of files uploaded and downloaded through HTTP, SMB, and FTP methods, as well as emails and attachments sent through SMTP, POP3, IMAP protocols, and corresponding processing based on the scanning results.

The antivirus configuration file will only take effect after being referenced in the security policy.

On the virus detection policy list interface, you can view the enabling/disabling status of the virus detection function of each policy for HTTP, SMB, FTP, SMTP, POP3, and IMAP protocols, as well as the reference times and reference modules of this policy.

Configuration Steps

Step 1. Choose “Object > Security Profiles > Antivirus”.

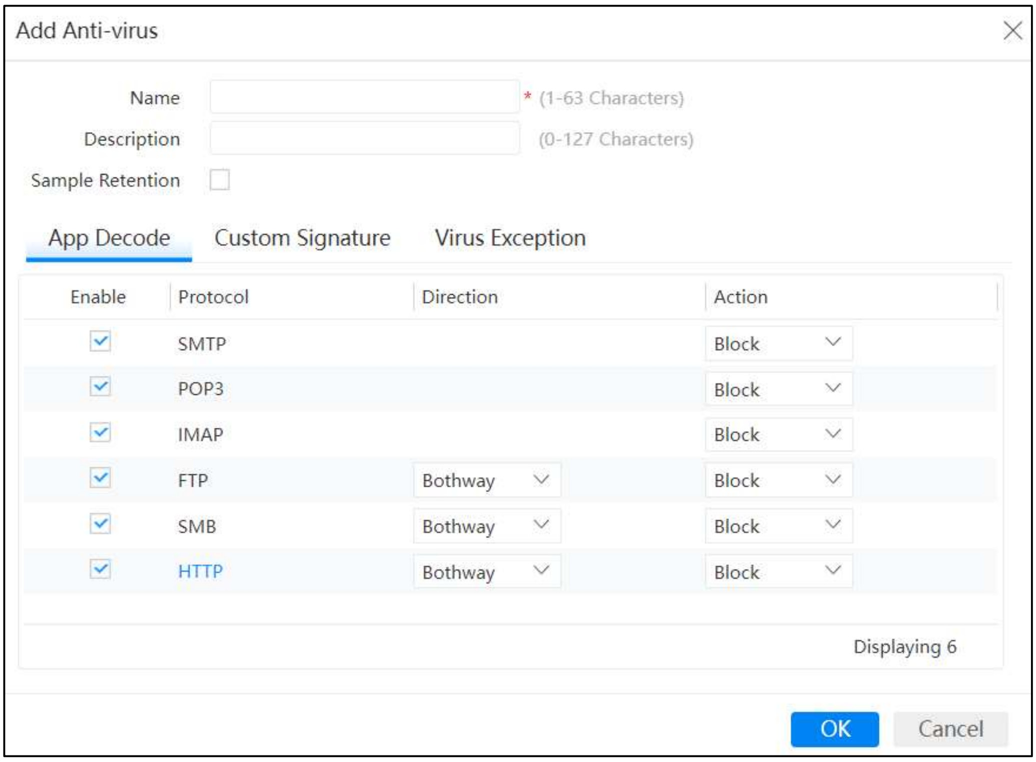
Step 2. Click “Add”.

Step 3. Configure the name and description of the antivirus file.

Step 4. Configure whether to enable sample retention.

After the sample retention is enabled, the sample will be retained when a virus is detected. The virus sample can be downloaded and viewed in the threat log. Only supported by firewall devices with hard drives.

Step 5. Configure the protocol, direction and action for antivirus application decoding.



Add Anti-virus

Name * (1-63 Characters)

Description (0-127 Characters)

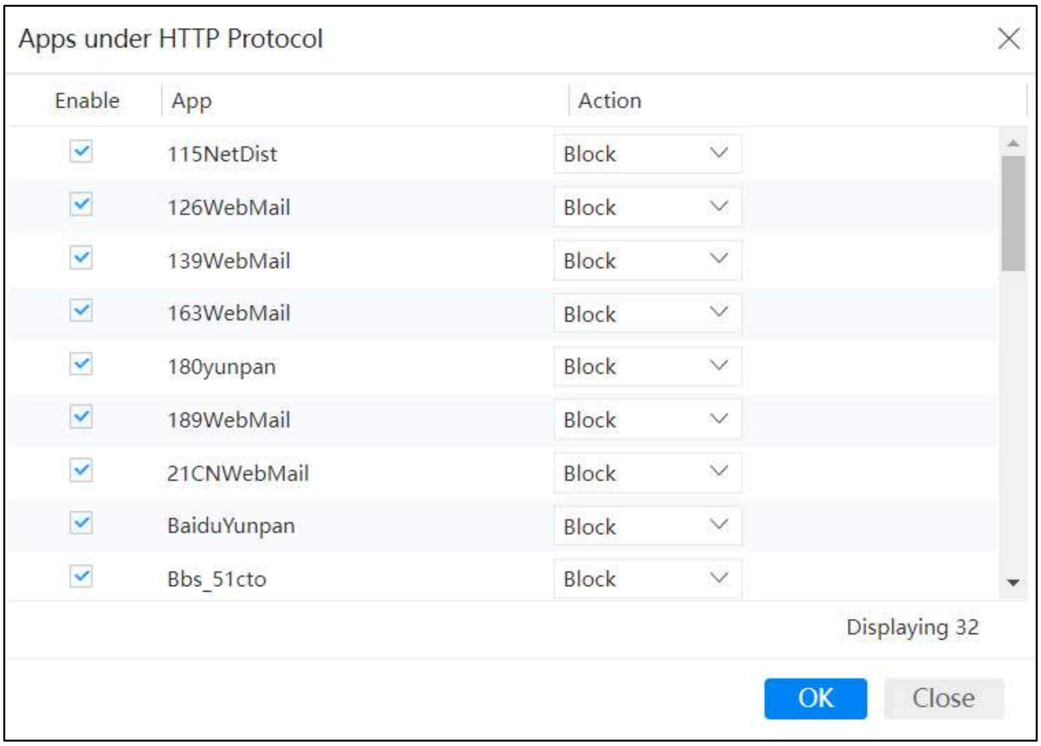
Sample Retention □

Enable	Protocol	Direction	Action
☑	SMTP		Block
☑	POP3		Block
☑	IMAP		Block
☑	FTP	Bothway	Block
☑	SMB	Bothway	Block
☑	HTTP	Bothway	Block

Displaying 6

The protocol types supported by the application decoding are IMAP, SMTP, POP3, FTP, SMB and HTTP. For FTP, SMB, and HTTP protocols, you can choose to enable the virus detection function for the upload direction, download direction, or both directions.

Different actions can be configured for each protocol. The HTTP protocol can also configure different actions for different applications. Click "HTTP" to select the application of the enabled HTTP protocol and the action to be executed on the page.



Apps under HTTP Protocol

Enable	App	Action
☑	115NetDist	Block
☑	126WebMail	Block
☑	139WebMail	Block
☑	163WebMail	Block
☑	180yunpan	Block
☑	189WebMail	Block
☑	21CNWebMail	Block
☑	BaiduYunpan	Block
☑	Bbs_51cto	Block

Displaying 32

Actions include:

- log

Log and release files.

- block

Log and block files.

Step 6.(Optional) Add a custom virus feature. After the configuration is complete, click “OK”.

One antivirus configuration file supports adding multiple custom virus features. Select a custom virus signature from the drop-down list. You can click the drop-down button of the drop-down box, select "Add virus " in the drop-down menu, and set the virus name and virus MD5.

Custom virus signature is a supplement to AV virus database. Custom virus signature takes precedence over those in the virus database. When performing AV detection, it first matches the custom virus feature.

Set actions for custom viruses. Actions include:

- log

  Log and release files.

- block

  Log and block files.

- allow

  Release the file without recording the log.

Step 7. (Optional) Add virus exceptions.

If the user thinks that a certain virus is a false alarm, he can obtain the virus ID from the log, and enter the virus ID in the text box on the "Virus Exceptions" interface. After adding, when a file containing this virus is detected, the system will release the file.

The method to obtain the virus ID is: choose "Data Center > Logs > Threat Log", and the value in the "Threat ID" column in the threat log list is the virus ID.

Step 8. After the configuration is complete, click “OK”.

11.2.5 Push Message Settings

Push message settings include Web browsing virus push message settings, email virus push message settings, and file transfer virus push message settings.

Web Browsing Virus Push Messages

After the Web browsing virus push message is set, when a virus based on the HTTP protocol is detected and the protection action for the virus is blocked, the firewall will push the browsed page to the user and inform the user of the virus ID and other information carried by the page.

Email Virus Push Message

After the email virus push message is set, when the email sent by POP3 or IMAP protocol is detected to be a virus, and the protection action for the virus is blocked, the virus file will be discarded, and the email content will be replaced with the push message defined in the template news.

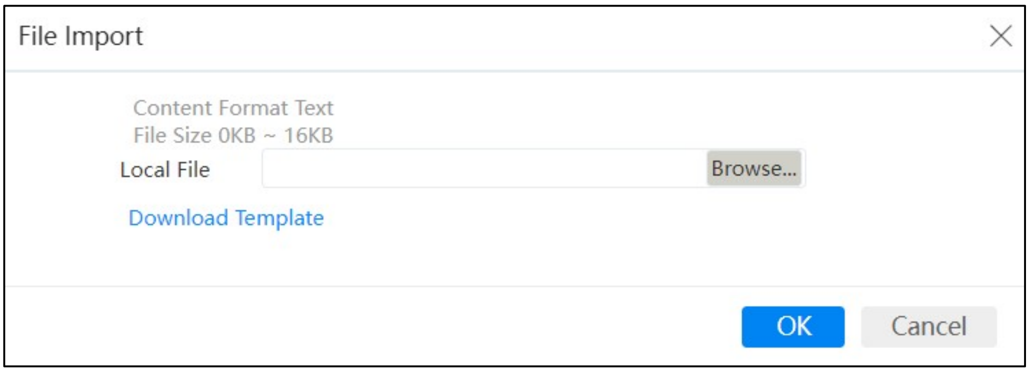
File Transfer Virus Push Notification

After the file transfer virus push message is set, when a file uploaded or downloaded via FTP is detected to be a virus file and the protection action for the virus is block, the virus file will be discarded and a document containing the push message will be sent to the user.

Set Push Message

Step 1. Select the push message to be set, and click ⇲ under the corresponding operation.

Step 2. Click “Download Template”.



File Import

Content Format Text
File Size 0KB ~ 16KB
Local File

Step 3. Edit the template and customize alarm messages.

Step 4. Click ⇲.

Step 5. Click “Browse”, select the configured push message, and click “OK”.

The defined push messages can be saved locally through the export function.

11.3 IPS Intrusion Prevention

11.3.1 Add Vulnerability Protection Signature

Step 1. Choose “Object > Custom Signature > Vulnerabilities”.

Step 2. Click “Add”.

Step 3. Set the name and description of the vulnerability feature.

Step 4. Set the basic parameters of the vulnerability signature.

Parameter	Description
CVEID	Specifies the CVEID of the vulnerability.
CNNVDID	Select CNNVDID of the specified vulnerability.
Severity	Select the severity of the vulnerability.
Protocol	Select the protocol type for the vulnerability. HTTP, TCP, UDP.

Parameter	Description
Action	Select the action to take if the vulnerability is detected. The default is block. Log, block, bypass and reset. • Log: only record the alarm log, do not take any action. • Block: Record alarm logs and discard the packets. • Bypass: Allow the packet to pass without taking any action. • Reset: Log the alarm, drop the packet, and reset the connection.

Step 5. Configure vulnerability rules.

1. Set whether to enable “Detection in Order”.
2. Click "Add" to add a vulnerability rule, and click "OK" after the addition is complete.

Parameter	Description
Operation	Operations support match, more than, less than, and equal to. • The match operation matches the string of the specified field with the value set by the user. • More than, less than, or equal to operations compare the numeric value of the specified field with the value set by the user.
Matching pattern	When the operation is match, the match mode can be set. The matching mode supports "text matching" and "regular matching". Text matching is to directly match the string of the specified field with the string specified by the value ; regular matching is to calculate the string and the specified string according to the regular expression before matching.
Field	Field options are related with the protocol. • When the protocol is HTTP, the field options include: HTTP.req_uri_path, HTTP.rsp_headers, HTTP.req_headers, HTTP.req_host, HTTP.req_method, HTTP.req_referer, HTTP.req_user_agent, HTTP.req_cookie, HTTP.req_content_type, HTTP.rsp_body, HTTP.req_body. • When the protocol is TCP, the field options include: TCP.unknown_tcp_req, TCP.unknown_tcp_res. • When the protocol is UDP, the field options include: UDP.unknown_udp_req, UDP.unknown_udp_res.

Parameter	Description
Value	When the operation is match, the value ranges from 3 to 63 characters except Chinese. Regular expressions need to be written in a professional rule language, such as hexadecimal ascii code or and, or relationship symbols. When the operation is more than, less than or equal to, the value ranges from 0 to 65525.

3. Set source port and destination port.

Step 6. After the rule configuration is complete, click “OK”.

The configured vulnerability features are displayed in the vulnerability list.

Step 7. Click “Submit”.

11.3.2 Add a Spyware Protection Signature

Step 1. Choose “Object > Custom Signature > Spyware”.

Step 2. Click “Add”.

Step 3. Configure the name and description of the spyware protection signature.

Step 4. Set the basic parameters of the spyware protection signature.

Parameter	Description
Severity	Select the severity of the spyware.
Protocol	Select the protocol type for the spyware. The type supports HTTP, TCP, UDP.
Action	Select the action to take if this spyware is detected. The default is block. • Log: only record the alarm log, do not take any action. • Block: Record alarm logs and discard data packets. • Bypass: Allow the packet to pass without taking any action. • Reset: Log the alarm, drop the packet, and reset the connection.

Step 5. Configure spyware rules.

1. Set whether to enable “Detection in Order”.
2. Click "Add" to add a vulnerability rule, and click "OK" after the addition is complete.

Parameter	Description
Operation	Operations support match, more than, less than, and equal to. • The match operation matches the string of the specified field with the value set by the user. • More than, less than, or equal to operations compare the number value of the specified field with the value set by the user.
Matching pattern	When the operation is match, the match mode can be set. The matching mode supports "text matching" and "regular matching". Text matching is to directly match the string of the specified field with the string specified by the value ; regular matching is to calculate the string and the specified string according to the regular expression before matching.
Field	The field options are related with the protocol. • When the protocol is HTTP, the field options include: HTTP.req_uri_path, HTTP.rsp_headers, HTTP.req_headers, HTTP.req_host, HTTP.req_method, HTTP.req_referer, HTTP.req_user_agent, HTTP.req_cookie, HTTP.req_content_type, HTTP.rsp_body, HTTP.req_body. • When the protocol is TCP, the field options include: TCP.unknown_tcp_req, TCP.unknown_tcp_res. • When the protocol is UDP, the field options include: UDP.unknown_udp_req, UDP.unknown_udp_res.
Value	When the operation is match, the value ranges from 3 to 63 characters except Chinese. Regular expressions need to be written in a professional rule language, such as hexadecimal ascii code or and, or relationship symbols. When the operation is more than, less than or equal to, the value ranges from 0 to 65525.

3. Set source port and destination port.

Step 6. After the rule configuration is complete, click “OK”.

The configured vulnerability features are displayed in the vulnerability list.

Step 7. Click “Submit”.

11.3.3 Add a Vulnerability Protection Configuration File

Vulnerability protection configuration files take effect only after being referenced in a security policy.

Prerequisite

The intrusion prevention and intrusion prevention library upgrade functions in the loaded firewall license have been authorized.

Configuration Process

Step 1. Choose “Object > Security Profiles > Vulnerability Protection”.

Step 2. Click “Add”.

Step 3. Configure the name and description of the vulnerability prevention configuration file.

Step 4. Set whether to enable "Sample retention".

After this function is enabled, the original packets that hit the vulnerability protection rules are captured and saved in the threat log. Only supported by devices with hard drives.

Step 5. Configure vulnerability protection.

1. Select a protection category. Select the check box in front of the corresponding category to enable vulnerability protection for the category. Select the check box in front of "Protection Category " in the title row to enable vulnerability protection for all categories.
2. Select the Protection subcategory. All subcategories under the selected protection category are enabled by default. You can disable the vulnerability protection for a subcategory by unchecking the checkbox in front of that subcategory. Action is default. Unified action modification can be performed through the actions in the upper right corner of the area frame. Action types include:

   - Log

   Log and release files.

   - Block

   Log and block files.

   - Bypass

   Release the file without recording the log.

   - Reset

   Log and disconnect from client.

   The actions of individual rules can be edited in the security rule base.
3. Click “Show Rules for Selected Category” to view all enabled rules. You can set exceptions and view rule details on this page.

Step 6. Configure the exception ID.

Click the “Exception Rule” tab, enter the rule name or ID, find the corresponding rule, and add the rule to the exception.

Step 7. Set the application protocol enabled with the vulnerability protection.

Expand “Advanced Configuration”, select the check box in front of the protocol, and enable vulnerability protection for the application protocol.

Step 8. After the configuration is complete, click “OK”.

The configured vulnerability protection files can be viewed in the vulnerability protection list. Click the “Edit” button in the operation to configure different actions for different vulnerabilities or configure the application protocol that enables vulnerability protection.

11.3.4 Add an Anti-Spyware Configuration File

Anti-spyware configuration files will not take effect until being referenced in a security policy.

Prerequisite

The intrusion prevention and intrusion prevention library upgrade functions in the loaded firewall license have been authorized.

Set the Enabled Anti-spyware Type

Step 1. Select “Object > Security Profiles > Anti-Spyware".

Step 2. Click “Add”.

Step 3. Configure the parameters of the anti-spyware profile.

1. Configure the name and description of the anti-spyware profile.
2. Set whether to enable "sample retention". After this function is enabled, the original packets that hit the anti-spyware rules are captured and saved in the threat log. Only supported by devices with hard drives.
3. Select the type of spyware and the action to perform to enable anti- spyware.

The types of vulnerabilities include "Trojan Horse Backdoor", "Virus Worm", "Botnet" and "Custom Feature". Except for "Custom Signature", the spywares of other types are all imported through the IPS feature database. Please make sure to update the latest IPS feature database, upgrade the number of spyware under the spyware category, and better anti-spyware.

- All spyware types perform the default action or perform the same action

  Set by action of header of type list.
- Set different actions for different spyware types

  Set through the actions corresponding to each vulnerability type.

Action types include:

- Log

  Log and release files.
- Block

  Log and block files.
- Bypass

  Release the file without recording the log.
- Reset

  Log and disconnect from client.

4. Open the application protocol configuration under advanced configuration.

   Expand "Advanced Configuration " and check the "Application Protocol" checkbox.

Step 4. After the configuration is complete, click “OK”.

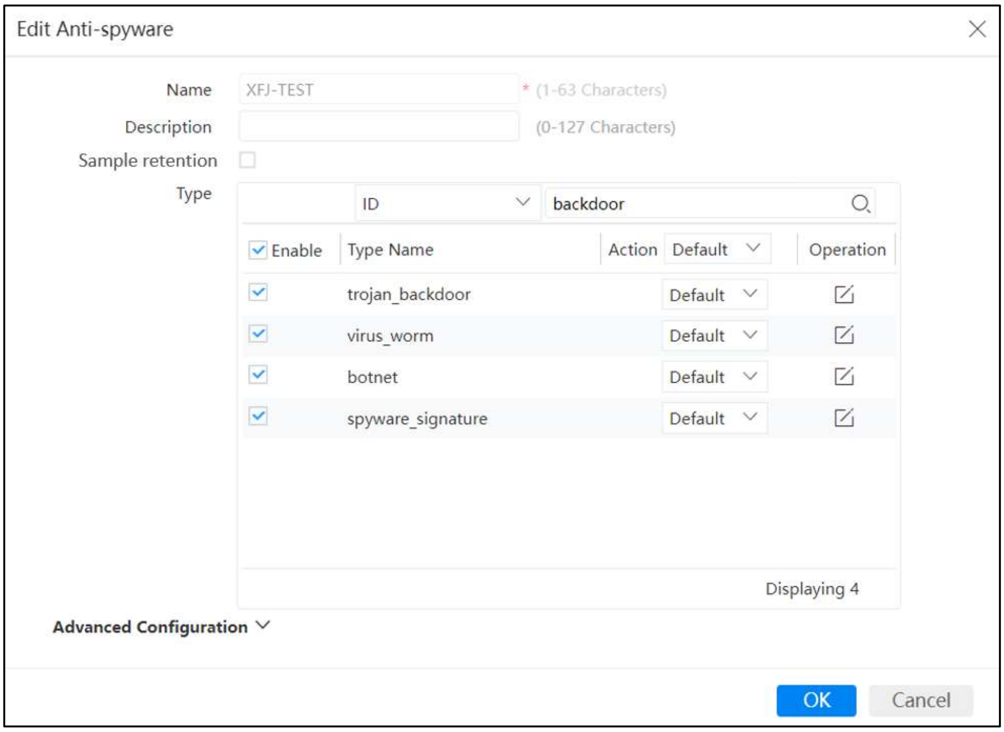
The configured anti-spyware configuration file can be viewed in the list of anti-spyware configuration files. Click the “Edit” button in “Operation” to configure different actions for different spyware or set the application to enable the anti-spyware.

Search for Specific Spyware

Step 1. Locate the desired antispyware file in the antispyware list, click the “Edit” button under the antispyware name link or operations.

Step 2. (Optional) To find a specific spyware, enter a search term in the search box.

Step 3. Click 🔍 or press Enter.



Edit Anti-spyware

Name: XFJ-TEST * (1-63 Characters)

Description: (0-127 Characters)

Sample retention: □

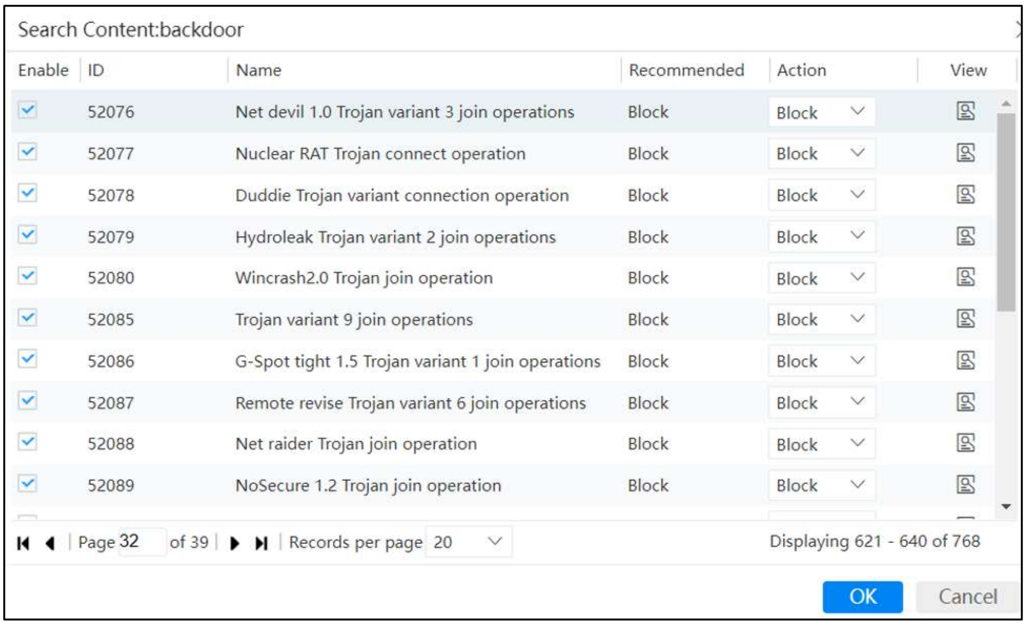
Type: ID, backdoor

☑ Enable	Type Name	Action Default	Operation
☑	trojan_backdoor	Default	✎
☑	virus_worm	Default	✎
☑	botnet	Default	✎
☑	spyware_signature	Default	✎

Displaying 4

Advanced Configuration

Step 4. View the search results, and modify and view the found vulnerabilities.



Search Content:backdoor

Enable	ID	Name	Recommended	Action	View
☑	52076	Net devil 1.0 Trojan variant 3 join operations	Block	Block	
☑	52077	Nuclear RAT Trojan connect operation	Block	Block	
☑	52078	Duddie Trojan variant connection operation	Block	Block	
☑	52079	Hydroleak Trojan variant 2 join operations	Block	Block	
☑	52080	Wincrash2.0 Trojan join operation	Block	Block	
☑	52085	Trojan variant 9 join operations	Block	Block	
☑	52086	G-Spot tight 1.5 Trojan variant 1 join operations	Block	Block	
☑	52087	Remote revise Trojan variant 6 join operations	Block	Block	
☑	52088	Net raider Trojan join operation	Block	Block	
☑	52089	NoSecure 1.2 Trojan join operation	Block	Block	

Page 32 of 39 | Records per page 20 | Displaying 621 - 640 of 768

Step 5. After the settings are complete, click “OK”.

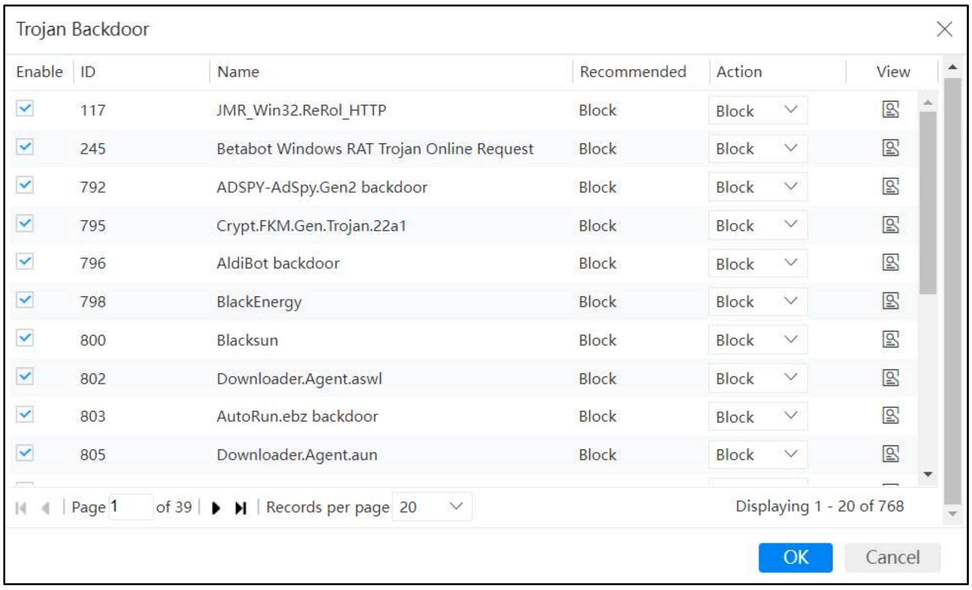
Edit an Anti-Spyware Action

Step 1. Locate the desired antispyware file in the antispyware list, click the “Edit” button under the antispyware name link or operation.

Step 2. Click the “Edit” button for the different log types.

Step 3. Select which spyware to enable under this anti-spyware type and what kind of protection action to take.

When the action for the entire anti-spyware type is Default, the action for each spyware is the default action for that spyware. The default action is the recommended setting in the IPS library based on the severity of the spyware.



Trojan Backdoor

Enable	ID	Name	Recommended	Action	View
☑	117	JMR_Win32.ReRol_HTTP	Block	Block	
☑	245	Betabot Windows RAT Trojan Online Request	Block	Block	
☑	792	ADSPY-AdSpy.Gen2 backdoor	Block	Block	
☑	795	Crypt.FKM.Gen.Trojan.22a1	Block	Block	
☑	796	AldiBot backdoor	Block	Block	
☑	798	BlackEnergy	Block	Block	
☑	800	Blacksun	Block	Block	
☑	802	Downloader.Agent.aswl	Block	Block	
☑	803	AutoRun.ebz backdoor	Block	Block	
☑	805	Downloader.Agent.aun	Block	Block	

Page 1 of 39 | Records per page 20 | Displaying 1 - 20 of 768

Click “View” to view the details for each spyware signature.

Step 4. After the configuration is complete, click “OK”.

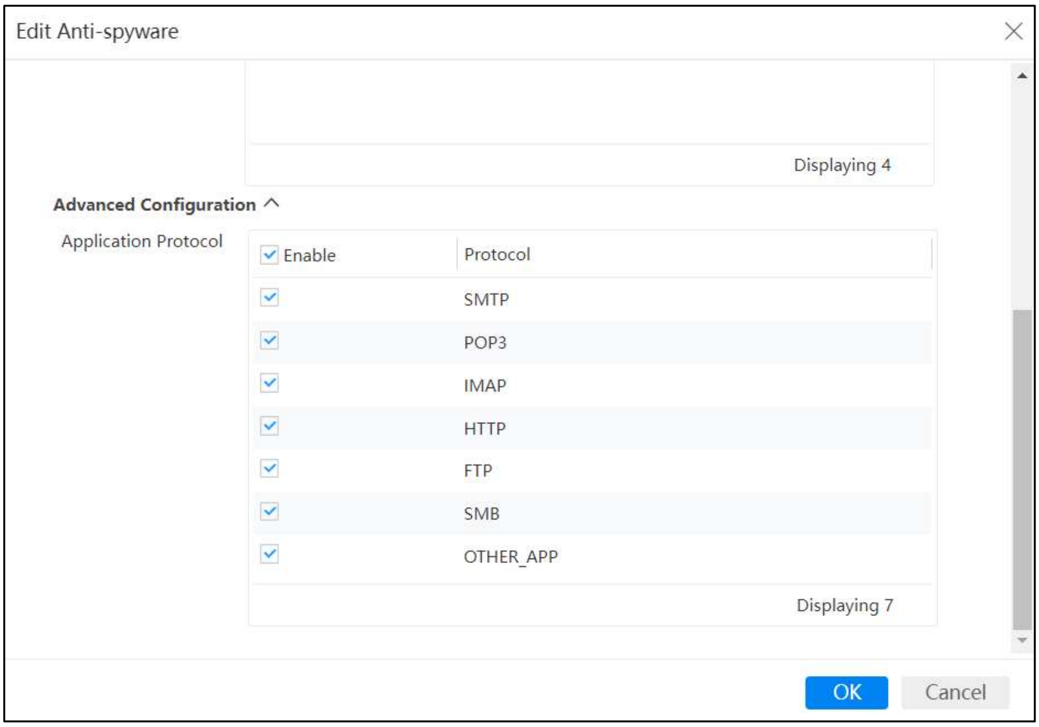
Edit the Enabled Application Protocol

Step 1. Locate the desired antispyware file in the antispyware list, click the “Edit” button under the antispyware name link or operation.

Step 2. Expand “Advanced Configuration”.

Step 3. Select the application protocol to enable anti-spyware protection.

Support FTP, HTTP, IMAP, POP3, SMB, SMTP and other types of application protocols. All are enabled by default.



☑ Enable	Protocol
☑	SMTP
☑	POP3
☑	IMAP
☑	HTTP
☑	FTP
☑	SMB
☑	OTHER_APP

Step 4. After the configuration is complete, click “OK”.

11.4 URL Filtering

11.4.1 URL Categories

View Predefined URL Categories

The URL resource library continuously collects commonly used URLs on the Internet and maintains them by category. It is recommended to update the URL resource library to the latest status through URL resource library upgrade.

Choose “Object > URL Category”. In the URL category list, you can see all predefined categories under “Predefined”.

Add Custom URL Categories

The added custom URL category must select a predefined first-level URL category as the parent category. That is to say, the custom URL category is a subcategory of the predefined URL categories.

Step 1. Choose “Object > URL Category”.

Step 2. Click “Add”.

Step 3. Configure the parameters for URL category.

Parameter	Description
Name	Specify the name of the URL category object.
Description	Simple remarks for URL category objects.
Focus	Select the "Focus " check box, the object will become a focus on the object. Otherwise, it will not enable focus.
Father	Select the parent category to which the URL category object belongs.
URL	Define the URL address, up to 100 URLs can be added. Support the use of "*" characters in wildcards to replace one or more characters in URL addresses, so as to realize fuzzy matching of URL addresses. *For example, when it is necessary to prohibit all QQ web pages, it is impossible to add all QQ web pages to the URL filtering address, but all QQ web pages have qq.com. At this point, we can define a URL "*.qq.com" to represent all the web pages of QQ.*
HOST	Define the HOST address, a maximum of 100 HOSTs can be added. Support using the "*" character in the wildcard to replace one or more characters in the HOST address, so as to realize fuzzy matching of the HOST address. **Note: The HOST address mainly refers to the content of the HOST field in the HTTP header. It can be a domain name or an IP address. In the http1.1 version, it can also be a null value.**

Step 4. After the configuration is complete, click “OK”.

Set Focus URL

Users can set a predefined URL subcategory and custom URL classification as the key focus as needed. When a user visits the URL of focus, a log will be generated to record the users or IP addresses who accessed the URL of focus and the URL visited, and statistics will be made on the situation of focus.

Step 1. In the URL category list, find the desired URL category.

Step 2. Click the button under Focus for that category.

If the state of focus is "Disable", it will be changed to "Enable" after clicking; Otherwise, it will be changed from "Enable" to "Disable".

11.4.2 Add URL Filtering Configuration File

The URL filtering configuration file added must be referenced in the security policy to take effect. Only the traffic matching the security policy will be processed by URL filtering.

Step 1. Choose “Object > Security Profile > URL Filter”.

Step 2. Click “Add”.

Step 3. Configure the parameters of the URL filtering file.

Parameter	Description
Name	Specify the name of the URL policy.
Description	The remarks of the URL policy are different from other URL policies.
Time	Select the time object to be referenced by URL filtering. Within the range defined by the time object, the URL filtering configuration file takes effect.
Action	The URLs that are not explicitly processed in the custom URL filtering class and predefined URL filtering class will match the default actions, which are divided into allow, deny, and log. • Permit, permit to pass and do not log. • Block, not permit to pass and log. • Log, permit to pass and log.

Parameter	Description
URL category	In URL classification, users can select a treatment action for predefined URL classifications and user-defined URL classifications by type. The action selected in the drop-down menu after the “Action” column will take effect on all predefined and custom URL categories. When the user checks “Only showy custom”, only the custom URL classification objects can be viewed. At this time, the processing action selected in the drop-down menu of the “Action” column will only take effect on the custom URL classification objects.

Step 4. Add URL keywords. Up to 16 keyword rules can be added.

The filtering of keyword groups can realize fine-grained control on the access path (subdirectory of website) when users access website resources through URL. For example:

The keyword is "www.a.com/news", and the action is permit, that is, access to the resources under the news subdirectory of the website is allowed;

The keyword is "www.a.com/movie", and the action is block, that is, access to resources under the movie subdirectory of the website is prohibited.

Parameter	Description
Name	Set the name of the keyword filtering policy.
Description	Select the URL filtering keyword group object or click “Add Keyword” to add a new keyword group.
Action	Select the action for this keyword filtering policy. • Permit, permit to pass and do not log. • Block, not permit to pass and log. • Log, permit to pass and log.

Step 5. After the configuration is complete, click “OK”.

11.4.3 Push Message Settings

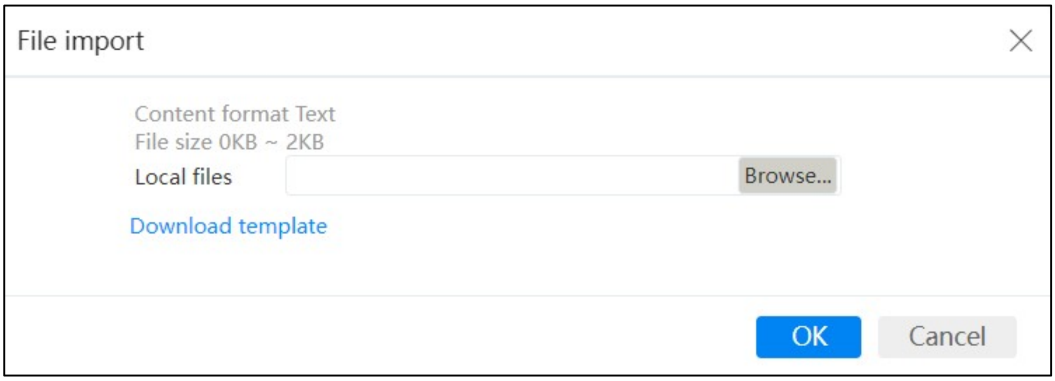
URL Filtering Push Messages

After the URL filtering push message is set, when an illegal URL access is detected, a document containing a push message will be sent to the user.

Set Push Message

Step 1. Select the push message to be set, and click ↘ under the corresponding operation.

Step 2. Click “Download Template”.



Content format Text
File size 0KB ~ 2KB

Step 3. Edit the templates and customize alarm messages.

Step 4. click ⇲.

Step 5. Click “Browse”, select the configured push message, and click “OK”.

The defined push messages can be saved locally through the export function.

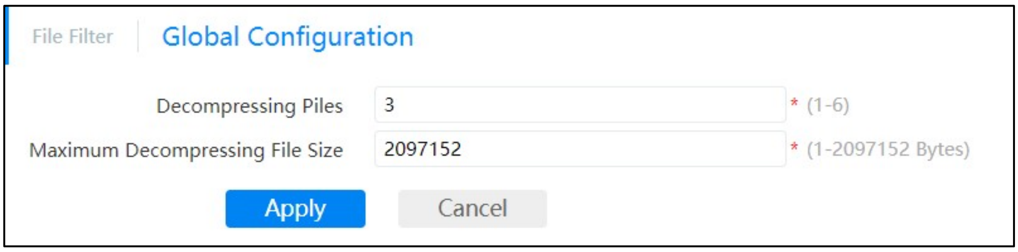
11.5 File Filtering

11.5.1 Overview

File filtering refers to the identification of file types for files transferred by specific applications to control file transfer behavior. The identification of file types by file filtering does not depend on the suffix name, and the file attribute cannot be modified by modifying the suffix name. In this way, important and sensitive internal files can be prevented from being leaked to the outside, and malicious files from the external network can also be prevented from being transmitted to the internal network.

11.5.2 Global Configuration

Global configuration of file filtering policies, users can customize the number of decompression layers of compressed files and the maximum decompression file size. The global configuration here will also limit the anti-virus and content filtering policies. The files that exceed the number of decompression layers and the maximum decompression file size will be released directly without file transfer, virus detection and content filtering.



Decompressing Piles: 3 * (1-6)

Maximum Decompressing File Size: 2097152 * (1-2097152 Bytes)

- Decompression piles

Specify the number of decompression layers of the compressed file, the default is 3 layers of decompression, and the range is 1-6 layers.

- Maximum decompressing file size

Specify the maximum decompression file size, the default is 2M. The range is 1-2097152 bytes, that is, the maximum is 2M.

11.5.3 Add File Filtering Configuration File

The added file filtering configuration file must be referenced in the security policy to take effect. Only the traffic matching the security policy will be filtered.

Step 1. Select “Object > Security Profiles > File filter".

Step 2. Click “Add”.

Step 3. Configure the name and description of the file filter.

Step 4. Click "Add" to configure file filtering rules, and click "OK" after the configuration is complete.

Up to 16 file filtering rules can be added.

parameter	Description
Name	Specify a rule name.
App	Select the scope of application for which file filtering takes effect. The scope supports FTP, HTTP, SMTP, POP3, IMAP, SMB protocols, as well as various forums, blogs, network disks and web mailboxes.
File type	Specify the file types supported by the rule.
Direction	Select the direction of file transfer control, divided into upload, download, and bothway.
Action	Select the processing behavior of file transfer control, divided into block and log. • The block action will block the transmission of specified

parameter	Description
	types of files and record the content log. • The log action will allow the transfer of the specified type of file and record the content log.

Step 5. After the configuration is complete, click “OK”.

11.6 Content Filtering

Content filtering refers to the effective identification and behavior control of data transmitted using specific applications and containing keyword information. Keywords can be customized or use predefined keywords. Content filtering can not only prevent user privacy and sensitive data leakage, but also prohibit intranet users from accessing emails, files, and web pages containing harmful information.

Step 1. Select “Object > Security Profile > Content Filter".

Step 2. Click “Add”.

Step 3. Configure a name and description for content filtering.

Step 4. Configure whether to enable content retention.

After the content retention is enabled, the data matching the content keywords will be captured and saved in the content log.

Step 5. Click “Add” to configure content filtering rules. After the configuration is complete, click “OK”.

Up to 16 content filtering rules can be added.

Parameter	Description
Name	Specify the name of the content filtering rule.
App	Select the application scope for content filtering to take effect. The scope supports FTP, HTTP, SMTP, POP3, IMAP, SMB protocols, as well as various forums, blogs, network disks and web mailboxes. • POP3, SMTP, and IMAP filter email subject, email body and attachments. • FTP filters the file name and file content. • SMB filters the file content. • What HTTP filters is the text content in the WEB page.
Keyword	Click the "Keyword" drop-down box and select a keyword from the drop-down menu. The drop-down menu displays both predefined keywords and custom keywords that have been added. If you need to add a keyword, select "Add

Parameter	Description
	Keyword" in the drop-down menu to add it.
File type	Specify the file types supported by the rule.
Direction	The direction in which the content filtering policy takes effect is divided into upload, download, and bothway.
Action	The actions taken after the content filtering policy takes effect include block and log. • The block action blocks data and records content logs. • The log action forwards data and logs the content.

Step 6. After the configuration is complete, click “OK”.

11.7 Email Filtering

The firewall supports sender-based mail filtering and anti-spam filtering. Receiver and sender support controlling the filtering policy in the direction of receiving and sending emails by specifying the email addresses of recipients and senders. Anti-spam supports RBL-based black and white lists and user-defined local black and white lists to detect and block emails sent by known or suspected malicious servers.

11.7.1 Add Mail Filtering Configuration File

The mail filtering configuration file must be referenced in the security policy to take effect. The traffic conforming to the security policy will be filtered according to the settings of the mail filtering configuration file.

Step 1. Select “Object > Security Profile > Mail Filter".

Step 2. Click “Add”.

Step 3. Configure the name, description and default action of the mail filter.

The default action configured here has a lower priority than the default action in the sender policy. The default action of the sender and sender policy is executed for those matching the sender and sender policy, and the default action configured here is executed for those not matching the sender and sender policy.

The default actions support permit, block and log.

- If the default action is "Permit", the firewall will allow the emails that do not match the sender and sender policies to pass through.
- If the default action is "Block", the firewall will prevent the mail from passing through and record the log if it fails to match the sender or sender policy.

- If the default action is "log", the firewall will allow the emails that do not match the sender and sender policies to pass through and record the logs.

Step 4. Click "Add" to set sender and sender policies, and click "OK" after the configuration is complete.

Parameter	Description
Name	Specify the sender keyword policy name.
Sender keyword	The keywords contained in the sender's email address. Click the “Sender” drop-down box, and select the sender keyword in the drop-down list. To add a new sender keyword, select "Add Sender Keyword" in the drop-down menu to add it.
Receiver keyword	The keywords contained in the receiver's email address. Click the receiver drop-down box, and select receiver keywords in the drop-down list. To add a new receiver keyword, select "Add receiver keyword" in the drop-down menu to add it.
Mode	The operation mode supports "receive", " send " and "two-way". • "Receive", which represents the direction of the sender's mail received by the recipient. • "Send", represents the direction of the mail sent from the sender to the recipient. • "Two-way" refers to the two directions in which the sender sends to the recipient and the recipient receives the sender's mail.
Default action	The processing action performed for the emails that match the keywords and operation methods of the sender and sender. • Permit, directly release the mail. • Block, directly block the mail and record the log. • Log: directly release the mail and record the log.

Step 5. Set RBL detection.

The spam address filtering function based on RBL (Real-time Blacklist List), the firewall will communicate with the RBL server to obtain whether the SMTP server address of the sender of the mail belongs to the server that has sent spam.

Enable check box of “RBL Detection” to enable the RBL detection function.

After RBL detection is enabled, you need to select the action for sending emails that hit the RBL blacklist.

- Block: The sender emails that hit the RBL blacklist will be blocked by the firewall and logged;
- Log: The sender's email that hits the RBL blacklist will be released by the firewall and recorded in the log.

Step 6. Configure IP address blacklist and blacklist detection.

Select the “Enable" check box of " IP Address Black and White List Detection" to enable the IP address black and white list detection function.

The custom spam IP address blacklist and whitelist on the firewall, the firewall will query the local blacklist and whitelist whether the SMTP server address of the sender of the email belongs to the blacklist or whitelist.

The emails from senders that belong to the blacklist of local IP addresses are directly blocked.

Step 7. After the configuration is complete, click “OK”.

⚠Caution

The IP addresses in the RBL and the local blacklist and whitelist usually refer to the sender's SMTP server address. However, in special cases, for example, the location of the user's firewall is between the intranet and the SMTP server, when the intranet user sends mail through the firewall before reaching the SMTP server, the IP addresses that need to be filtered in the local black and white list can be the sender's IP address.

11.7.2 Configure Antispam

The firewall detects and blocks spam through its anti- spam feature. The RBL server and IP address black and white lists configured under anti-spam will take effect only after RBL detection and IP address black and white list detection are enabled in the mail filtering configuration file.

Step 1. Select “Object > Security Profile > Mail filter".

Step 2. Click the “Antispam Panel” tab.

Step 3. Set RBL server address and IP address blacklist and whitelist.

Parameter	Description
RBL server address	Specify the address of the RBL server. The default address of the firewall is cbl.anti-spam.org.cn.
IP address whitelist	Click the drop-down box to select the IP address object or address group added in the whitelist, usually it refers to the sender's SMTP server address. To add a new address object or address group object, select “Add Address” or “Add Address Group” from the drop-down menu. Only IPv4 addresses are supported.

Parameter	Description
IP address blacklist	Click the drop-down box to select the IP address added in the blacklist, which usually refers to the sender's SMTP server address. To add a new address object or address group object, select “Add Address” or “Add Address Group” from the drop-down menu. Only IPv4 addresses are supported.

Notes

In special cases, such as the user's firewall is placed between the intranet and the SMTP server, when the email sent by the intranet user needs to pass through the firewall before reaching the SMTP server, the IP address added in the local black and white list that needs to be filtered can be the sender IP address.

11.8 Behavior Control

11.8.1 HTTP Protocol Behavior Control

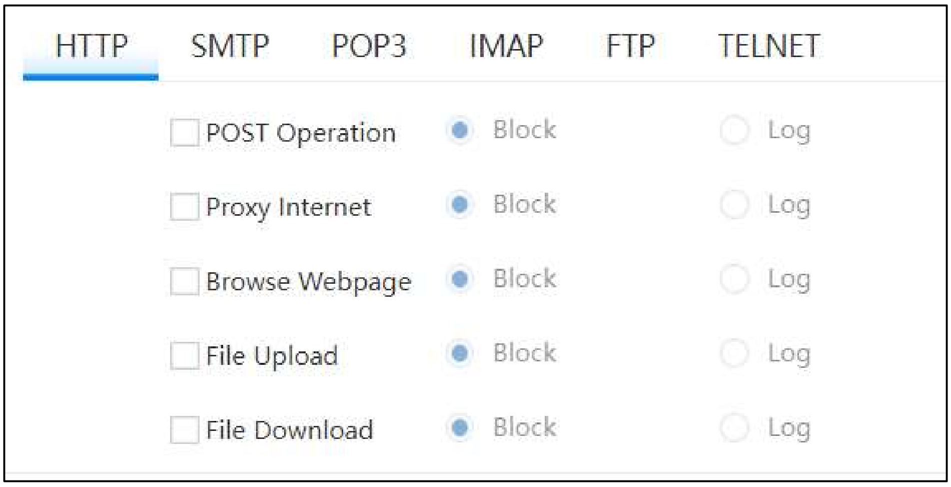
Step 1. Choose “Object > Security Profile > Behavior Control”.

Step 2. Click “Add”.

Step 3. On the “Add Behavior Control” page, set the name and description of the behavior control configuration file.

Step 4. Select the protocol for behavior control as HTTP.

Step 5. Set the corresponding action for each behavior.



HTTP SMTP POP3 IMAP FTP TELNET

□ POST Operation ● Block ○ Log

□ Proxy Internet ● Block ○ Log

□ Browse Webpage ● Block ○ Log

□ File Upload ● Block ○ Log

□ File Download ● Block ○ Log

The firewall supports the management and control of the following HTTP behaviors. If the action is set to "Block", the user cannot perform corresponding operations; if the action is set to " Log ", the user can perform corresponding operations, but corresponding logs will be generated on the firewall.

- POST operation: generally used to send information to the server, such as forum posting, form submission, username /password login.
- Proxy Internet access: Use a proxy server to access a specific website. At this time, it is required that the firewall must be deployed between the proxy server and the Internet users. After blocking, users cannot access the Internet through the proxy server.
- Browsing a web page: A user opens a web page through a browser.
- File upload: Users upload files to the website through the HTTP protocol.
- File download: Users download files from websites through the HTTP protocol.

Step 6. After the configuration is complete, click “OK”.

11.8.2 SMTP Protocol Behavior Control

The firewall supports the control of the following SMTP commands. If the action is set to "Block", the corresponding command is blocked and the operation cannot be successful; if the action is set to "Log", the corresponding command is allowed to be executed, but corresponding logs will be generated on the firewall.

Command	Description
DATA	Start message writing
EHLO	EHLO is extend HELO, which can support user authentication.
EXPN	Validate the existence of the given mailbox list, expand the mailbox list, and it is often disabled.
HELO	Identify the user identity to the server and return the identity of the mail server.
HELP	Return information from the specified command.
MAIL FROM	Initiate a mail session on the host.
NOOP	No operation, the server should respond with “OK”.
QUIT	Terminate the mail session.
RCPT TO	Identify the address of the recipient of the mail.
RSET	Reset the session, canceling the current transfer.
SAML FROM	Send emails to user terminals and mailboxes.
SEND FROM	Send mail to user terminal.
SOML FROM	Send mail to user terminal or mailbox.

Command	Description
TURN	Receiver and sender switch roles.
VRFY	Used to verify that the specified user/mailbox exists; due to security reasons, servers often prohibit this command.

11.8.3 POP3 Protocol Behavior Control

The firewall supports the control of the following POP3 commands. If the action is set to "Block", the corresponding command is blocked and the operation cannot be successful; if the action is set to "Log", the corresponding command is allowed to be executed, but corresponding logs will be generated on the firewall.

Command	Description
APOP	Recognize a method of securely transmitting passwords, where successful execution results in a state transition.
DELE	Handle the server mark deletion, the real deletion is performed when the QUIT command is executed.
LIST	The processing server returns the size of the specified mail, etc.
NOOP	No operation, the server should respond with “OK”.
PASS	Password authentication, if passing the authentication, convert the state.
QUIT	Wish to terminate the session.
RETR	Process the full text of the mail returned by the server.
RSET	Cancel all DELE commands.
STAT	Process the request server to return mailbox statistics material, such as the number of emails and the total number of bytes of emails.
TOP	Process some lines of content returned by the server for an email.
UIDL	The processing server returns a unique ID for the specified message, or all if not specified.
USER	Authentication username.

11.8.4 IMAP Protocol Behavior Control

The firewall supports the control of the following IMAP behaviors. If the action is set to "Block", the corresponding command will be blocked and the operation cannot be successful; if the action is set to " Log ", the corresponding command is allowed to be executed, but the corresponding log will be generated on the firewall.

Command	Description
CREATE	Create a new mailbox with the specified name.
DELETE	Delete the folder with the specified name.
RENAME	Modify the name of the folder.
LIST	List the existing folders in the mailbox, a bit like the list directory command of the operating system.
APPEND	Allow the Client to upload an email to the specified Folder (folder/mailbox).
SELECT	Let the Client select a mailbox (Folder), indicating that the mail in the mailbox (Folder) is about to be operated.
FETCH	Text messages used to read emails and are used for display purposes only.
STORE	It is used to modify the properties of the specified email, including marking the email as read, deleting, etc.
CLOSE	Indicate that the Client ends the access to the current Folder (folder/mailbox), closes the mailbox, and all the mails marked as DELETED in the mailbox are physically deleted.
EXPUNGE	Delete all messages marked DELETED without closing the mailbox. Emails deleted by EXPUNGE cannot be recovered.
EXAMINE	Open the mailbox as read-only.
SUB SCRIBE	Used to add a mailbox to the client's active mailbox list.
UNSUBSCR IBE	Used to remove a mailbox from the active list.
LSUB	Fixed LIST command, LIST returns all files in user's $HOME directory, but LSUB command only shows those files set as active mailbox with SUBSCRIBE command.
STATUS	Query the current status of the mailbox. STATUS can get mailbox information without using SELECT command (open mailbox) or EXAMINE (open mailbox in read-only mode).
CHECK	Used to set a checkpoint on a mailbox.
SEARCH	You can search for messages in active mailboxes based on search criteria and display matching message numbers.

Command	Description
COPY	Copy mail from one mailbox to another.
UID	The UID command is used with the FETCH, COPY, STORE commands, or SEARCH commands, which allows these commands to use the UID number of the message instead of the sequence number in the mailbox. The UID number is a 32-bit certificate that uniquely identifies mail in the mail system. Usually these commands use the sequence number to identify the mail in the mailbox, and the UID can make the IMAP client remember the mail in different IMAP sessions.
CAPABILITY	The request returns the list of functions supported by the IMAP server, and the server will return the functions supported by the server after receiving the CAPABILITY command sent by the client.
NOOP	No operation, the server should respond with “OK”.
LOG OUT	Log out the current login user and close all open mailboxes. Any mail marked \DELETED will be deleted at this time.

11.8.5 FTP Protocol Behavior Control

The firewall supports the management and control of the following FTP behaviors.

- FTP connection control command

If the action is set to "Block", the corresponding command is blocked and the operation cannot be successful; if the action is set to "Log", the corresponding command is allowed to be executed, but corresponding logs will be generated on the firewall.

Command	Description
ABOR	Abandon the transfer.
ACCT	Some systems associate accounts and users with file systems.
allo	Allocate space for files to be transferred.
APPE	Appends a file to an existing file.
CDUP	Change the current directory to the superior parent directory on the remote system.
CWD	Change the working directory of the remote system.
DELE	Delete THE files on the remote system.
LIST	Send a list of filenames in the current working directory on a newly established data connection.

Command	Description
MKD	Create a directory.
MODE	Specify the transfer mode.
NLST	Send a "full" directory listing of the current directory on a newly established data connection.
NOOP	No operation to prevent disconnection.
PASS	Provide a user login password.
PASV	The specified server data transmission process monitors and waits for the client's data connection establishment request.
PORT	Specify the port number on which the client monitors and waits for a connection to be established by the server.
PWD	Display the name of the current working directory on the server side.
REIN	Reinitialize, logging out but not disconnecting.
REST	Restart the transfer from an id of the server.
RETR	Retrieve a file from a remote system.
RMD	Delete a directory.
RNFR	Specify the old pathname of the file to be named, must be followed by an RNTO command.
RNTO	Specify the new pathname of the file to be named.
STAT	Display the current FTP status.
STOR	Upload a file to the server, overwrite if the file already exists.
STOU	Upload a file to the server without overwriting existing files
STRU	Specify the file structure.
SYST	Display the OS type of the remote host.
TYPE	Set or display the file transfer type.
USER	Specify the user to connect to the remote computer.
XCUP	Change to the parent directory.
XCWD	Change to the working directory.
XMKD	Create a directory.
XPWD	Display the current directory.
XRMD	Delete the directory.

- FTP file upload

- FTP file download

If the action is set to "Block", the user cannot perform corresponding operations; if the action is set to "Log", the user can perform corresponding operations, but corresponding logs will be generated on the firewall.

11.8.6 TELNET Protocol Behavior Control

The firewall supports the control of the command line entered after the TELNET connection is established, and the action can be set to "block" or "log".

Input the Telnet command keyword in the command area box, and all commands matching the command keyword will execute the set action.

Each input command line keyword supports 1 to 63 characters, including special symbol characters. Up to 64 items are supported.

11.9 Linkage Terminal Management and Control

Enable the linkage between the firewall and the terminal, and the terminal security management system will evaluate the risk level of the terminals in the intranet protected by the firewall. In the configuration file, perform the block setting for the terminal not installed with the terminal security management system or the terminal on which the terminal security management system detects risks, thereby improving the security of the network.

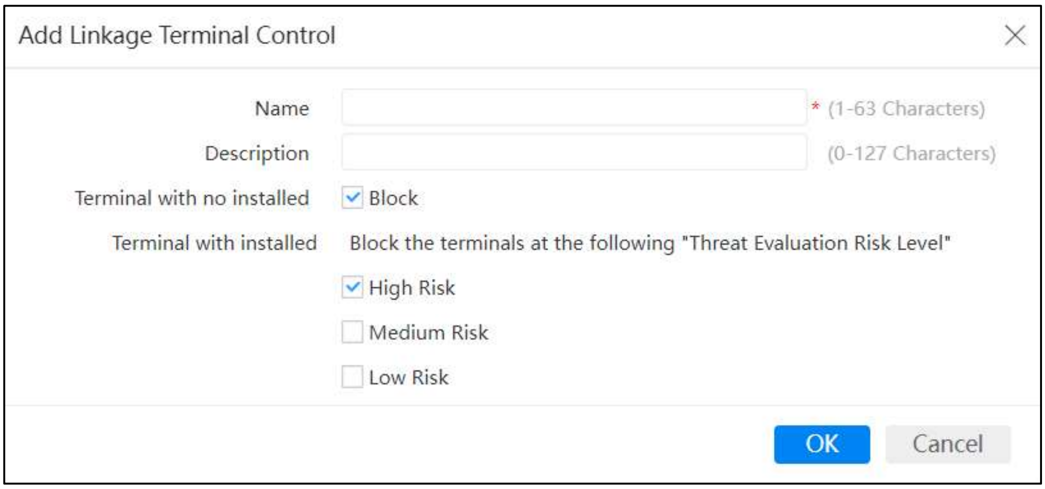
The terminals detected by the terminal security management system can be viewed in the "Linked Terminal List" of "Data Center > Monitor > Asset Monitor".

Step 1. Select “Object > Security Profiles > Linkage Terminal Control".

Step 2. Click “Add”.

Step 3. Configure the name and description of the linkage terminal control policy.

Step 4. Configure the block policy.



Add Linkage Terminal Control

Name * (1-63 Characters)

Description (0-127 Characters)

Terminal with no installed ☑ Block

Terminal with installed Block the terminals at the following "Threat Evaluation Risk Level"

☑ High Risk

□ Medium Risk

□ Low Risk

- Terminals without terminal security management system installed

  It is impossible to determine whether a terminal without a terminal security management system is a risk host. It is recommended to install a terminal security management system or set blocking to reduce the risk of network existence.

- high risk

  High-risk terminal detected by the terminal security management system. Block is enabled by default.

- medium risk

  Medium-risk terminals detected by the terminal security management system.

- low risk

  Low-risk terminals detected by the terminal security management system.

Step 5. After the configuration is complete, click “OK”.

11.10 Configure Security Configuration File Groups

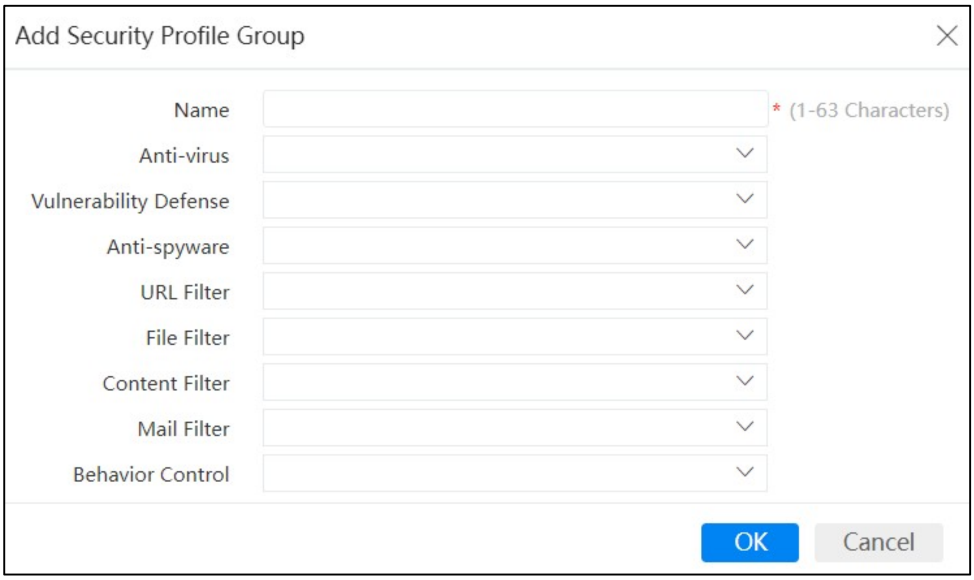
A security configuration file group can form a security configuration file group by referencing multiple security configuration files. Security configuration file groups take effect by being referenced in security policies.

Step 1. Choose “Object > Security Profile Groups”.

Step 2. Click “Add”.

Step 3. Configure the name of the security configuration file group and specify the security configuration file to be referenced.

Users can refer to security configuration files for different functions as needed.



Add Security Profile Group

Name * (1-63 Characters)

Anti-virus

Vulnerability Defense

Anti-spyware

URL Filter

File Filter

Content Filter

Mail Filter

Behavior Control

Step 4. After the configuration is complete, click “OK”.

12 SSL Decryption

12.1 Configure SSL Proxy

12.1.1 Restrictions and Precautions

- The SSL proxy decryption policy is executed after the security policy. Only when the action of the security policy is "Permit" and one or more content security configuration files are referenced in the security policy, the SSL encrypted data will further match the SSL decryption policy, and decrypt or not decrypt according to the matched decryption policy.
- The order of the SSL proxy decryption policy in the authentication list determines the priority of the SSL decryption policy. The earlier the decryption policy is, the higher the priority is. Therefore, the finer rules need to be configured with a higher priority. Otherwise, the data flow will not continue to match more precise rules after matching broader rules.
- SSL proxy decryption is not supported in bypass mode.
- You need to install the SSL decryption certificate on the client. If not installed, you will be prompted whether to continue accessing.

12.1.2 (Optional) Importing Server CA Certificate

When the firewall acts as a proxy to establish an SSL connection with the SSL server, it needs to verify the certificate of the server. When the HTTPS service that the user wants to access is trusted by the firewall, the server-side CA certificate that will issue the certificate to the server can be directly imported into the firewall.

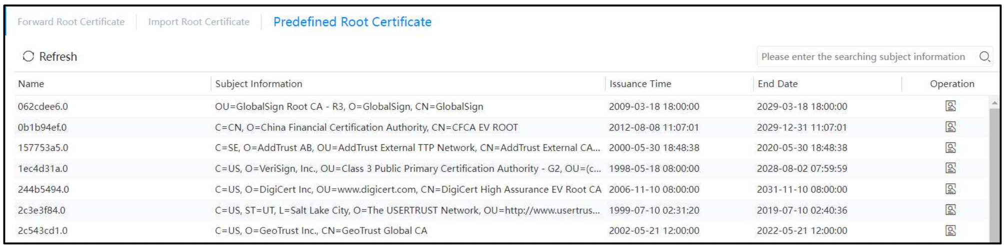
View Preset Root Certificates

The preset root certificate is the server-side CA certificate preset by the firewall, and is used to verify whether the server-side certificate is trustworthy. The preset trusted CA certificate cannot be deleted, and users can view the detailed configuration information of the preset trusted CA certificate.

Step 1. Choose “System > Certificate Management > SSL Decryption Certificate”.

Step 2. Click “Predefined Root Certificate”.

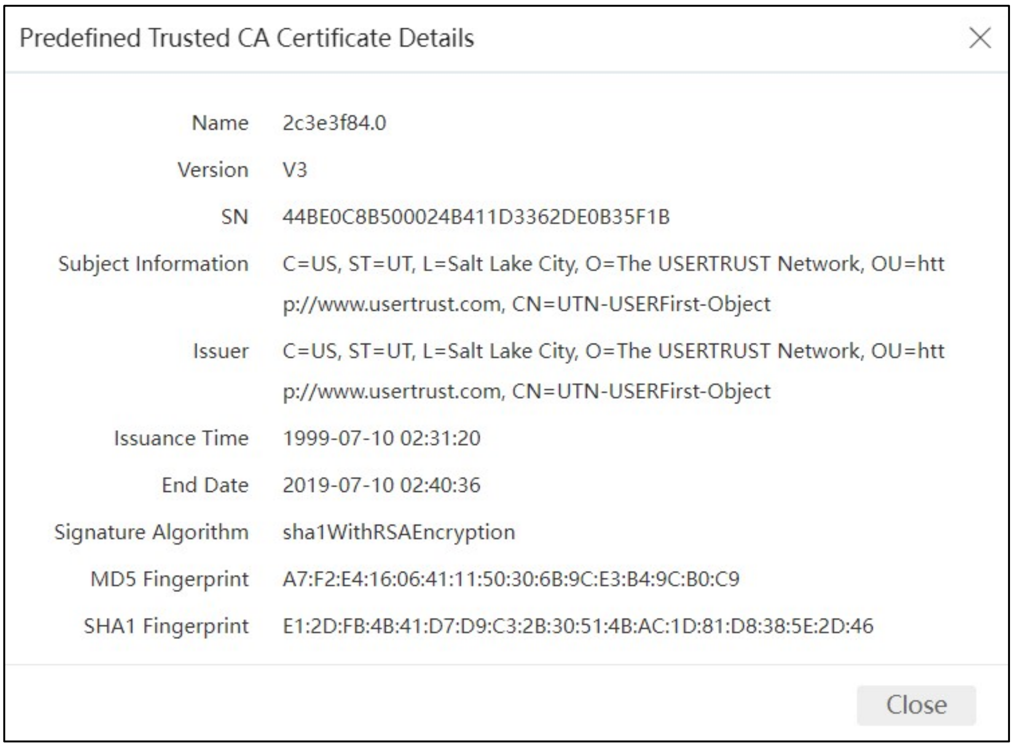
Step 3. View the list of root certificates.


Forward Root Certificate
Import Root Certificate
Predefined Root Certificate
Refresh
Please enter the searching subject information

Name	Subject Information	Issuance Time	End Date	Operation
062cdee6.0	OU=GlobalSign Root CA - R3, O=GlobalSign, CN=GlobalSign	2009-03-18 18:00:00	2029-03-18 18:00:00	🔍
0b1b94ef.0	C=CN, O=China Financial Certification Authority, CN=CFCA EV ROOT	2012-08-08 11:07:01	2029-12-31 11:07:01	🔍
157753a5.0	C=SE, O=AddTrust AB, OU=AddTrust External TTP Network, CN=AddTrust External CA...	2000-05-30 18:48:38	2020-05-30 18:48:38	🔍
1ec4d31a.0	C=US, O=VeriSign, Inc., OU=Class 3 Public Primary Certification Authority - G2, OU=(c...	1998-05-18 08:00:00	2028-08-02 07:59:59	🔍
244b5494.0	C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert High Assurance EV Root CA	2006-11-10 08:00:00	2031-11-10 08:00:00	🔍
2c3e3f84.0	C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrus...	1999-07-10 02:31:20	2019-07-10 02:40:36	🔍
2c543cd1.0	C=US, O=GeoTrust Inc., CN=GeoTrust Global CA	2002-05-21 12:00:00	2022-05-21 12:00:00	🔍

Step 4. (Optional) Query the preset root certificate to be viewed by the keyword.

Step 5. Click the "View" button under the operation corresponding to the certificate to view the details of the certificate.



Predefined Trusted CA Certificate Details

Name	2c3e3f84.0
Version	V3
SN	44BE0C8B500024B411D3362DE0B35F1B
Subject Information	C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Object
Issuer	C=US, ST=UT, L=Salt Lake City, O=The USERTRUST Network, OU=http://www.usertrust.com, CN=UTN-USERFirst-Object
Issuance Time	1999-07-10 02:31:20
End Date	2019-07-10 02:40:36
Signature Algorithm	sha1WithRSAEncryption
MD5 Fingerprint	A7:F2:E4:16:06:41:11:50:30:6B:9C:E3:B4:9C:B0:C9
SHA1 Fingerprint	E1:2D:FB:4B:41:D7:D9:C3:2B:30:51:4B:AC:1D:81:D8:38:5E:2D:46

Import Root Certificate

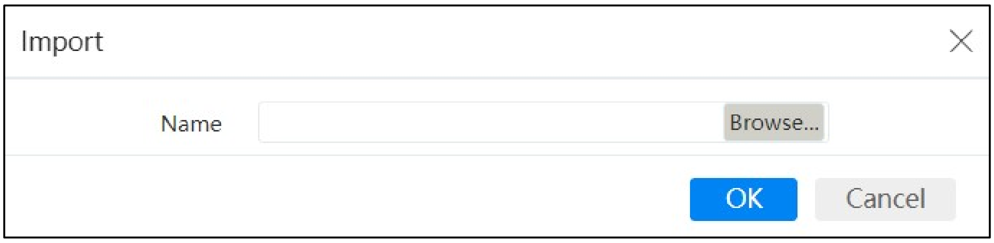
In addition to presetting some commonly used trusted CA certificates, the firewall also supports users to manually import server-side CA certificates. When the HTTPS service that the user wants to access is trusted by the firewall, the server-side CA certificate that will issue the server certificate can be directly imported into the firewall.

Step 1. Choose “System > Certificate Management > SSL Decryption Certificate”.

Step 2. Click “Import Root Certificate”.

Step 3. Click “Import”.

Step 4. Select the trusted CA certificate to import.



Step 5. Click “OK”.

The imported CA certificate can be displayed in the list of trusted CA certificates.

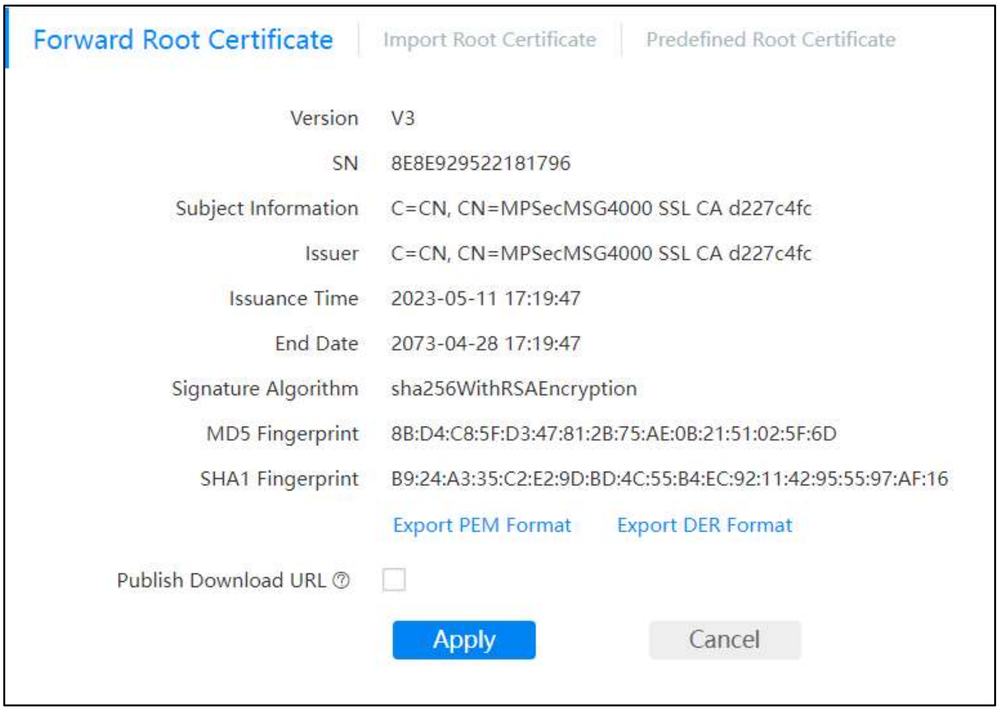
12.1.3 Download SSL Decryption Certificate and Install It on Client

For the SSL connection established between the firewall and the client, the client also needs to verify the certificate on the firewall. Therefore, the client needs to import the certificate issued by the firewall's SSL decryption certificate.

Step 1. Choose “System > Certificate Management > SSL Decryption Certificate”.

Step 2. Click “Forward Root Certificate”.

Step 3. Export a trusted CA forwarding certificate or generate a certificate URL.



Version V3

SN 8E8E929522181796

Subject Information C=CN, CN=MPSecMSG4000 SSL CA d227c4fc

Issuer C=CN, CN=MPSecMSG4000 SSL CA d227c4fc

Issuance Time 2023-05-11 17:19:47

End Date 2073-04-28 17:19:47

Signature Algorithm sha256WithRSAEncryption

MD5 Fingerprint 8B:D4:C8:5F:D3:47:81:2B:75:AE:0B:21:51:02:5F:6D

SHA1 Fingerprint B9:24:A3:35:C2:E2:9D:BD:4C:55:B4:EC:92:11:42:95:55:97:AF:16

Publish Download URL ⓘ □

- The trusted forwarding certificate supports exporting in PEM format and DER format.
- Select "Publish download URL ", the trusted forwarding certificate will publish the certificate URL.

  Specify the interface for issuing certificates, and specify the port number for publishing, ranging from 1025-65535.

Step 4. Click “Apply”.

Step 5. Install the certificate to the client.

The exported certificate needs to be installed on the client (terminals such as PC or mobile phone).

The client (the terminals such as PC or mobile phone) opens “http://*interface IP address: port number /sslca.cer"* through a browser, and then, you can download the trusted forwarding certificate directly and install the certificate.

12.1.4 Configure SSL Proxy Decryption Policy

The firewall acts as an SSL proxy to establish SSL connections with the client and server respectively. After the firewall decrypts the SSL encrypted traffic sent by the client, it performs content security inspection on the traffic. After the inspection is complete, the firewall encrypts the traffic again and sends it to the server.

Step 1. Choose “Policy > SSL Decryption Policy”.

Step 2. Click “Add”.

Up to 16 SSL decryption policies can be added.

Step 3. Configure the parameters of the SSL decryption policy.

Parameter	Description
Name	Configure the name of the SSL decryption policy. In string format, the value ranges from 1 to 63 characters.
Enable	After selecting “Enable”, enable the SSL decryption policy.
Source zone	Specifies the source security zone of the SSL decryption policy.
Destination zone	Specifies the destination security zone of the SSL decryption policy.
Source address	Specifies the source address of the SSL decryption policy.
Destination address	Specifies the destination address of the SSL decryption policy.

Parameter	Description
SSL protocol service	Configure the service of the SSL protocol. HTTPS is supported in the default drop-down list, and other protocols need to be added by the user.
Action	The processing action of the decryption policy is divided into two types: decryption and non- decryption.
Decryption type	Select "SSL Proxy" for the decryption type.

Step 4. After the configuration is complete, click “OK”.

The configured SSL decryption policy is displayed in the SSL decryption policy list. You can view the policy name, source security zone, destination security zone, source address, destination address, service, whether to enable it, actions, etc.

12.2 Configure an SSL Inbound Inspection Policy

SSL inbound inspection supports bypass deployment, and is usually bypassed on the egress switch. The firewall enables SSL inbound inspection, which does not affect the communication between the SSL server and the SSL client, but obtains SSL encrypted traffic through mirroring for SSL decryption.

12.2.1 Restrictions and Precautions

- Decryption of DH encrypted files is not supported.
- The current version supports imported HTTPS website certificate formats as follows:
  - The certificate file contains the private key, and the format supports: *.p12, *.pfx.
  - The certificate file and the private key file are independent of each other and exist in pairs. The format supports: certificate file (*.crt *.cer, *.der *.pem), private key file (*.key).
- For unsupported certificate formats, you can convert them to supported certificate formats through a Linux host with openssl installed.
- Batch import only supports importing compressed packages in zip format, and the compressed package cannot contain directories and duplicate certificates. If there are passwords for the certificate files in the compressed package, the private key passwords of all certificate files must be the same. Otherwise, the import will fail.
- If the certificate file and private key file of the same website are two independent files, the names of the certificate file and the private key file must be consistent. For example, the certificate file is "a.crt", and the private key file is "a.key".

- When using TSL encryption, the extended item "Extended master secret" cannot be enabled. Otherwise, the decryption will fail.
- The SSL inbound inspection decryption policy is executed after the security policy. Only when the SSL encrypted data that hits the security policy, the advanced security policy inspection is enabled or the plaintext traffic mirroring is enabled, the SSL decryption policy will be further matched, and decide whether the SSL encrypted data needs to be decrypted according to the processing action of the decryption policy that is hit.
- The order of the SSL inbound inspection decryption policy in the authentication list determines the priority of the SSL inbound inspection decryption policy. The earlier the decryption policy is, the higher the priority is. Therefore, finer rules need to be configured with a higher priority. Otherwise, the data flow will not continue to match more precise rules after matching broader rules.

12.2.2 Configure SSL Inbound Inspection Configuration File

Before configuring the decryption policy of the SSL inbound inspection method, you must first configure the SSL inbound inspection configuration file. The premise of using the SSL inbound inspection method to decrypt SSL traffic is that the SSL certificate of the website server corresponding to the traffic must be imported on the firewall. Perform the SSL decryption for the encrypted HTTPS traffic through imported certificates.

Add SSL Inbound Inspection Configuration File

Step 1. Choose “Object > Decryption Profile > SSL Inbound Inspection”.

Step 2. Click “Add”.

Step 3. Set the name and description.

Step 4. After the configuration is complete, click “OK”.

Import the Certificate File for SSL Inbound Inspection

After clicking “OK”, the import certificate page will pop up automatically. A configuration check file can import up to 500 certificates.

Step 1. Click “Import”.

Step 2. Configure the import method.

The import mode supports three methods: "Upload file", "Batch " and "Local CA center".

Step 3. Configure the corresponding parameters.

- When the import method is "Upload file", only one certificate file can be uploaded at a time. If the certificate file and private key file are two independent files, you need to specify the file name and upload the certificate file and private key file; if the certificate public and private key files are the same file, you need to specify the file name and upload the certificate file, and then enter the private key password. At this time, there is no need to set the "Private Key File" option. The name is customized by user.

- When the import method is "Batch ", multiple certificate files can be compressed into one compressed package. Only the compressed package in ZIP format is supported, and the compressed package cannot contain directories. If the certificate file and the private key file are two files, the names of the two files need to be the same; if the certificate files in the compressed package have passwords, the private key passwords of all the certificate files must be the same. Otherwise, the import will fail.
- When the import method is "Local CA center", you need to generate a general certificate in the local CA center before importing it on this page. The name is customized by the user.

Step 4. Click “Import”.

The imported certificate is displayed in the certificate list. You can view the certificate name, subject information, issuance time, and expiration time. And you can delete the certificate and other operations.

Step 5. Click “Finish”.

12.2.3 Configure SSL Inbound Inspection Decryption Policy

Step 1. Choose “Policy > SSL Decryption”.

Step 2. Click “Add”.

Up to16 SSL decryption policies can be added.

Step 3. Configure the parameters of the SSL decryption policy.

Parameter	Description
Name	Configure the name of the SSL decryption policy. In string format, the value ranges from 1 to 63 characters.
Enable	After selecting “Enable”, enable the SSL decryption policy.
Source zone	Specify the source security zone of the SSL decryption policy.
Destination zone	Specify the destination security zone of the SSL decryption policy.
Source address	Specify the source address of the SSL decryption policy.
Destination address	Specify the destination address of the SSL decryption policy.
SSL protocol service	Configure the service of the SSL protocol. HTTPS is selected by default, and other protocols need to be added by the user.
Action	The processing action of the decryption policy is divided into two types: Decode and Un-decode.

Parameter	Description
Decryption type	Select “SSL Inbound Inspection" for Decryption Type.
SSL Inspection Profile	Select the SSL inbound inspection configuration file.

Step 4. After the configuration is complete, click “OK”.

The configured SSL decryption policy is displayed in the SSL decryption policy list. You can view the policy name, source security zone, destination security zone, source address, destination address, service, whether to enable it, actions, etc.

12.2.4 (Optional) Specify Mirroring Interface

The firewall supports mirroring the decrypted plaintext traffic to other devices for analysis and statistics. In this case, you need to enable the mirroring function and specify the mirroring interface. Only support configuration under the command line.

Step 1. Execute **config terminal** to enter the configuration view.

Step 2. Run **decrypt pt policy ssl** to enter the SSL decryption policy view.

Step 3. Execute **mirror enable** to enable the mirroring function.

Step 4. Execute **exit** to return to the configuration view.

Step 5. Execute **decrypt mirror interface** *interface -name,* and specify the mirroring interface. *interface-name* indicates the interface name.

12.3 Adjust the Order of SSL Decryption Policy

The order of the SSL decryption policy in the authentication list determines the priority of the SSL decryption policy. The earlier the decryption policy is, the higher the priority is. Therefore, finer rules need to be configured with a higher priority. Otherwise, the data flow will not continue to match more precise rules after matching broader rules.

The SSL decryption policy delivered by the smart management analysis system has a higher priority than the local SSL decryption policy of the firewall. Only the order of the firewall's local SSL decryption policy can be adjusted.

Step 1. Choose a decryption policy.

Step 2. Click “Reorder”.

Step 3. Select the keywords to adjust the policy.

The keywords for adjusting the policy support "top", "before", "after" and "end". These keywords can be used to adjust the decryption policy to the top of the list, before the specified policy, after the specified policy, and at the end.

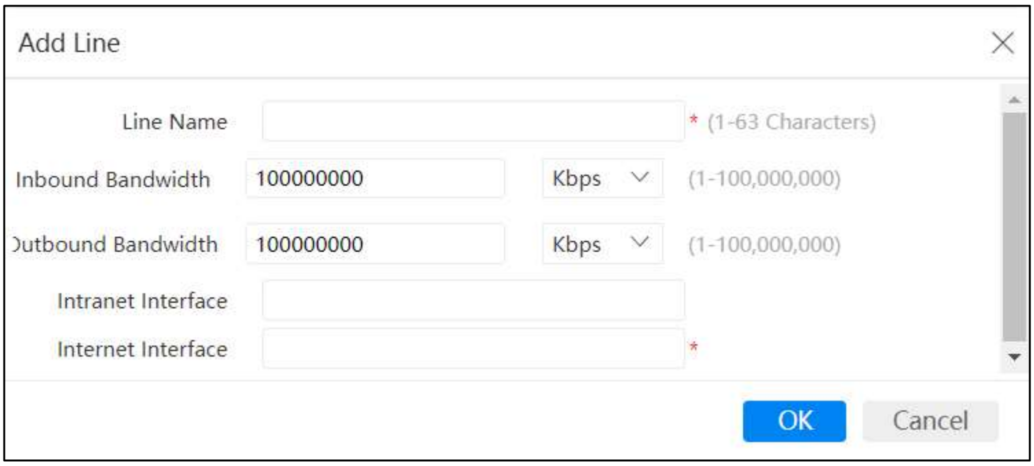
Step 4. Click “OK”.

13 QoS

13.1 Configure QoS

Step 1. Choose “Policy > QoS”.

Step 2. Click “Add”. On the "Add Line" page, specify the line name, uplink and downlink bandwidth, intranet interface (optional), and extranet interface.



Add Line

Line Name		* (1-63 Characters)	
Inbound Bandwidth	100000000	Kbps	(1-100,000,000)
Outbound Bandwidth	100000000	Kbps	(1-100,000,000)
Intranet Interface			
Internet Interface		*	

The uplink and downlink bandwidths are usually determined by the egress bandwidth provided by the operator to the corresponding external network interface.

By specifying the internal network interface, multiple lines can be configured for the same external network interface. Each intranet interface exclusively enjoys the specified bandwidth and does not preempt each other.

The sum of the uplink bandwidth or downlink bandwidth of all lines on the same external network interface is the bandwidth of the external network interface.

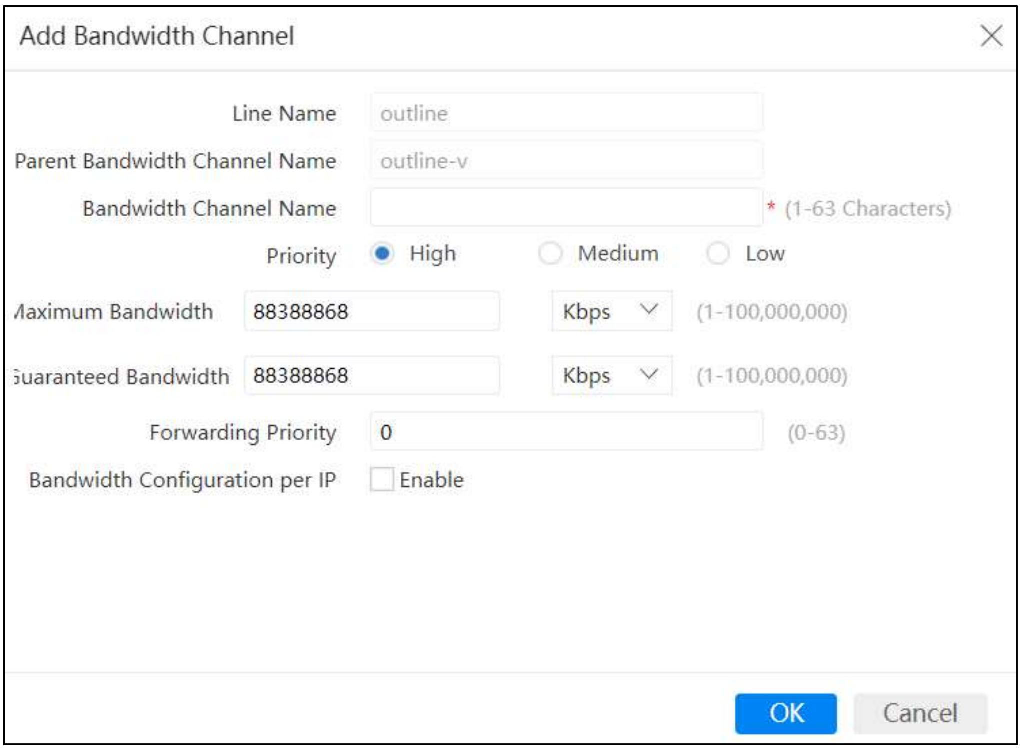
Step 3. Click + corresponding to the line to add virtual QoS.

Configure the virtual QoS name and specify the direction. The name of virtual QoS cannot be repeated.

A QoS line supports a maximum of two uplink and two downlink virtual QoS. When multiple virtual QoSs are configured in the same direction, these virtual QoSs are matched in series, and they are matched in order from top to bottom.

Step 4. Add a level of bandwidth channel.

Select a virtual QoS, in the channel configuration list, click + to add a bandwidth channel, the parent channel of this channel is virtual QoS (virtual QoS can be regarded as the root channel).



Add Bandwidth Channel

Line Name: outline

Parent Bandwidth Channel Name: outline-v

Bandwidth Channel Name: * (1-63 Characters)

Priority: ● High ○ Medium ○ Low

Maximum Bandwidth: 88388868 Kbps (1-100,000,000)

Guaranteed Bandwidth: 88388868 Kbps (1-100,000,000)

Forwarding Priority: 0 (0-63)

Bandwidth Configuration per IP: □ Enable

Parameter	Description
Line name	The name of the line bound to the bandwidth channel cannot be modified.
Parent bandwidth channel name	The name of the upper-level bandwidth channel to which the bandwidth channel is bound.
Bandwidth channel name	Specify the bandwidth channel name. The name of the bandwidth channel cannot be repeated, nor can it be the same as the name of the virtual QoS.
Priority	The priority of the channel is divided into high, medium and low. The channel bandwidth provides bandwidth service guarantee according to the priority, and the channel bandwidth with higher priority is satisfied first.
Maximum bandwidth	The maximum bandwidth that can be achieved by the bandwidth channel cannot exceed the line bandwidth.
Guaranteed bandwidth	The guaranteed bandwidth of the bandwidth channel, the sum of the guaranteed bandwidth of all child bandwidth channels cannot exceed the guaranteed bandwidth of the parent bandwidth channel. The sum of the first-level bandwidth channels cannot exceed the guaranteed

Parameter	Description
	bandwidth of the QoS line.
Forwarding priority	The forwarding priority is used to mark the DSCP priority of the packet, so that the upstream and downstream devices connected to the firewall can distinguish traffic according to the DSCP priority marked by the firewall. When configured as 0, the forwarding priority function is not enabled.
Bandwidth Configuration Per IP	
Bandwidth per IP	After enabling bandwidth configuration per IP, you can limit the maximum bandwidth per IP. It can be configured to 83886080kbps at most.
Quota traffic	Specify the upper limit of cumulative traffic that can be allocated to users. After the upper limit is reached, traffic allocation will no longer be possible. If it is set to 0, it means that there is no limit to the user's accumulated traffic.
Quota type	The configuration types are divided into "Everyday" and "Every week". That is, whether the specified configured traffic is every day or every week.
Shaping bypass	After the shaping bypass is enabled, the bandwidth allocation will not be shaped according to the guaranteed bandwidth and maximum bandwidth settings, but will be restricted according to the traffic allocated by each IP bandwidth, and the forwarding priority is still valid.

Step 5. Add subbandwidth channels.

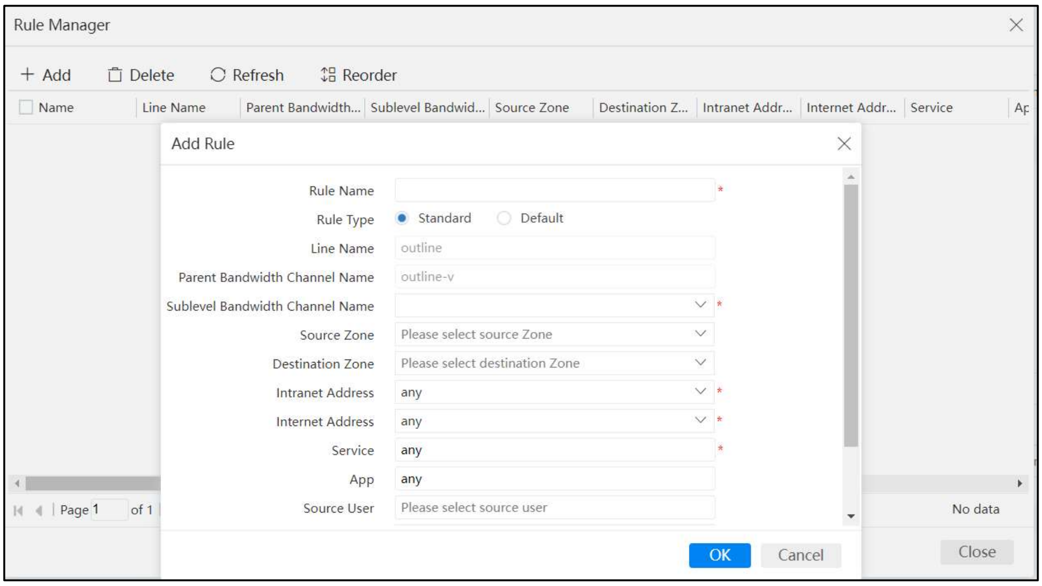
Select a bandwidth channel, and in the channel configuration list, click + in Operation to add a sub-bandwidth channel. A maximum of three bandwidth channels can be added under a virtual QoS.

The configuration method is the same as step 4.

Step 6. Add rules.

Add rules for each parent bandwidth channel starting from the first-level bandwidth channel, and the rules are used to control the traffic entering the sub-channel. In the "Rule Management" column of the bandwidth channel, click the rule number link to add a QoS rule. It is displayed as "0" when there is no rule.

When there are multiple rules, the rule that comes first has a higher priority. If there is duplication between two rules, the stricter rule needs to be placed first. After the traffic hits a rule, it will not continue to match.



Rule Name: *

Rule Type: ● Standard ○ Default

Line Name: outline

Parent Bandwidth Channel Name: outline-v

Sublevel Bandwidth Channel Name: *

Source Zone: Please select source Zone

Destination Zone: Please select destination Zone

Intranet Address: any *

Internet Address: any *

Service: any *

App: any

Source User: Please select source user

Parameter	Description
Rule name	Specify the name of the rule.
Rule type	Specify the type of rule. Common rules allow users to specify the internal network address, external network address, service, application, source user, and time period of the data. The default rule will take effect on all data that hits the line. The hit line is based on the internal network interface and external network interface configuration of the line.
Line name	The name of the line to which the rule is bound, which cannot be modified.
Parent bandwidth channel name	The parent bandwidth channel bound to the rule, which cannot be modified.
Sublevel Bandwidth Channel Name	Select the sub-bandwidth channel. The data that hits the bandwidth channel will be allocated according to the sub-bandwidth channel.
Intranet address	Specify the source address of the data that the user needs to perform flow control on, and it needs to be filled in according to whether the current restriction is uplink or downlink. You can choose IPv4 type address or IPv6 type address.
Extranet address	Specify the destination address of the data that the user needs to perform flow control, and it needs to be filled in according to whether the current restriction is uplink or downlink. You can choose IPv4 type address or IPv6 type address.

Parameter	Description
Service	Select the service object that needs to hit the rule. When it is not necessary to fill in the information accurately to the service, you can leave it blank.
App	Select the application object that needs to hit the rule, and you can leave it blank if it does not need to be accurate to the application.
Source user	Select the source user object that needs to hit the rule. If it does not need to be accurate to the user, you can leave it blank.
Period	Select the time object for the rule to take effect. You can leave it blank if it does not need to accurate to the time.
Enable	Check to enable the rule. If not checked, it will not be enabled.

Step 7. After the configuration is complete, click “OK”.

Step 8. Click “Close”.

14 Asset Management

14.1 Asset Identification

The asset identification function is used to monitor, count and match users for the clients who access and add assets. At the same time, it monitors whether these clients attack the server in real time. When the administrator suspects that the server has received an attack, he can immediately monitor the screening and positioning.

The terminal identification can realize the identification and detection of the corresponding relationship between the user's intranet terminal IP address, name, type and operating system, and can help users understand the online terminal information and the number of online terminals in the network.

Step 1. Choose “Object > Asset > Asset Identification”.

Step 2. Enable the asset monitoring function switch.

Step 3. Set whether to enable VPN monitoring.

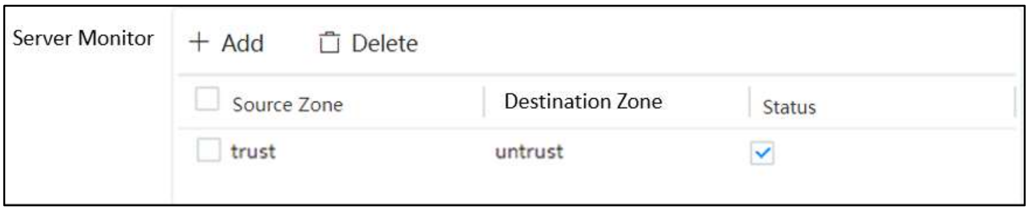
After selecting "VPN", the asset management monitoring will monitor and count the users dialing in through the firewall PPTP and L2TP, which has nothing to do with the configuration of the source security zone and the destination security zone.

If “VPN” is not selected, asset management monitoring will not monitor and count users who dial in through the firewall through PPTP and L2TP.

Step 4. Configure the server cache timeout.

Step 5. Configure the client cache timeout.

Step 6. Add server monitoring.



□ Source Zone	Destination Zone	Status
□ trust	untrust	☑

Click “Add” to add the source security zone and destination security zone to which the data flow monitored by the server belongs.

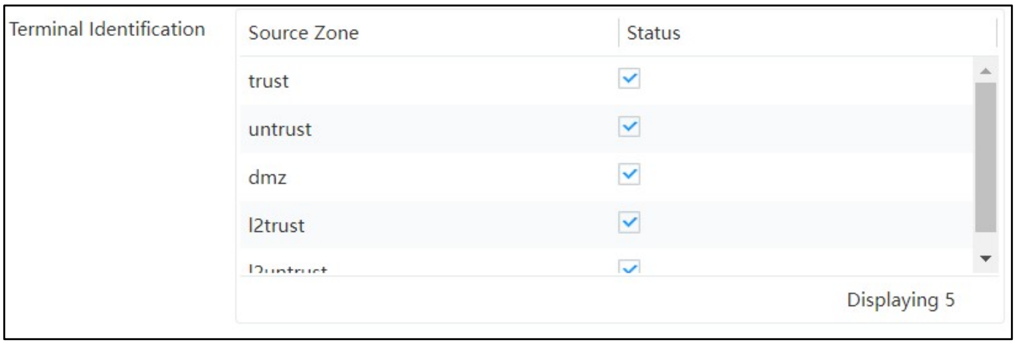
The server monitoring will take effect only after “Enable” is selected. You can also enable server monitoring by checking “Status”.

Since the asset management monitoring function mainly identifies and protects intranet servers, it is recommended that users select the security zone to which the intranet belongs when selecting a security zone.

The identification result of server monitoring is displayed on the “Server Monitoring” page of “Data Center > Monitor > Asset Monitor”. You can choose to display based on IP address, or based on the services provided. Service classification currently supports: IIS, Apache, Lighttp, SMTP, POP3, FTP, SVN, DHCP.

Step 7. Select the security zone that needs to enable the terminal identification function.

Select the “Status” check box to enable terminal identification for the corresponding security zone.



Terminal Identification

Source Zone	Status
trust	☑
untrust	☑
dmz	☑
l2trust	☑
l2untrust	☑

Displaying 5

Step 8. Click “Apply” after the configuration is complete.

14.2 Asset Monitoring

14.2.1 Server Monitoring

After asset monitoring is enabled, the firewall identifies the servers in the user network by identifying the data application layer and monitors and counts the clients accessing these servers. At the same time, real-time monitoring is performed on whether these clients launch attacks on the server. When the administrator suspects that the server is under attack, he can screen and locate it in the asset monitoring at the first time.

In the asset management list on the left, you can set the priority to display based on the IP or service of the asset.

Service classification currently supports: IIS, Apache, Lighttp, SMTP, POP3, FTP, SVN, NGINX, SMB.

When displaying IP first, you can enter the IP address in the input box to query the asset monitoring information of the specified IP address.

Click a server, and you can view the asset address, access times, last activity time, application users, and authenticated users in the asset monitoring list on the right.

Clicking “Clear Cache” will clear identified servers.

14.2.2 Terminal Monitoring

Terminal monitoring can realize the identification and detection of the corresponding relationship between the IP address of the user's intranet terminal and the operating system, and can help users understand the online terminal information and the number of online terminals in the network.

Parameter	Description
Terminal address	The IP address of the terminal. Only IPv4 terminals are supported.
whether to share	Whether the terminal is a shared device. A shared device means that there are multiple devices behind the terminal that use the address of the terminal for business access.
Operating system	The operating system to which the identified terminal belongs.
Security zone	The security zone to which the terminal belongs.
Risk level	After the terminal linkage is configured, the terminal security management system will send the terminal risk level to the firewall.

Clicking "Clear Cache " will clear the identified terminals.

15 IPv6 Features

15.1 Neighbor Table

The firewall supports configuring IPv6 addresses on interfaces. When the interface uses an IPv6 address for interconnection, the interface address of the peer device directly connected to the firewall should also be an IPv6 address. We refer to the IPv6 address of the peer device interface directly connected to the firewall as the IPv6 neighbor of the firewall, and the IPv6 neighbor list is used to view all IPv6 neighbors directly connected to the firewall and their IPv6 addresses.

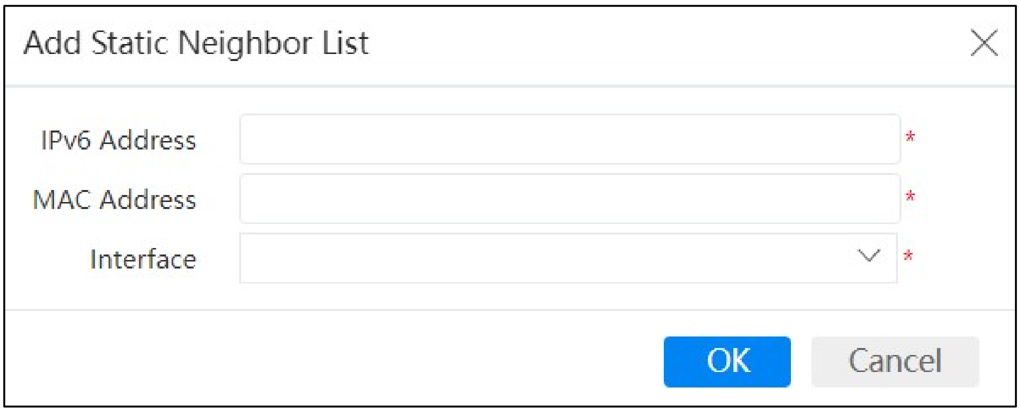
15.1.1 Add a Static Neighbor

Static neighbors are the correspondence between IPv6 addresses and MAC addresses manually added by users. Users can manually add those not learned by the firewall in the static neighborhood.

Step 1. Choose “Network > Neighbor Table > Static Neighbor”.

Step 2. Click “Add”.

Step 3. Configure neighbor parameters.



Add Static Neighbor List

IPv6 Address *

MAC Address *

Interface *

Parameter	Description
IPv6 address	Specify the IPv6 address of the static neighbor.
MAC address	Specify the MAC address corresponding to the IPv6 address.
Interface	Select the L3 interface connected to the IPv6 address in the static neighbor.

Step 4. After the configuration is complete, click “OK”.

The configured static neighbors are displayed in the static neighbor list. You can view the IP address, MAC address, connected interface, security zone, status, etc. of static neighbors. If the status of the static neighbor is STATIC (INCALID), it means that the static neighbor is unreachable.

Support operations such as editing, deleting, and querying static neighbors.

15.1.2 Bind Dynamic Neighbors

The dynamic neighbor table is the IPv6 neighbors actively learned by the firewall. The firewall supports binding the IP and MAC of dynamic neighbors.

Step 1. Choose “Network > Neighbor Table > Dynamic Neighbor List”.

Step 2. Select one or more dynamic neighbors to be bound.

In the dynamic neighbor table, you can view the neighbor's IP address, MAC address, bound interface, security zone, timeout, state, and binding state. The neighbor remaining timeout is 600 seconds by default. After the timeout period is 0, the neighbor will be deleted from the firewall's dynamic neighbor until it is learned again.

If there are too many dynamic neighbors, you can use the query function to find the dynamic neighbors to be bound.

Step 3. Click “Bind”.

After the binding is successful, the binding status of the neighbor changes to "Bound", which can also be checked in "Policy > IP-MAC Binding > Binding List".

Clicking "Clear All" will clear all IPv6-MAC address correspondence entries that the firewall has learned so far, and learn again.

You can release the binding relationship between IPv6 address and MAC address in IP-MAC binding.

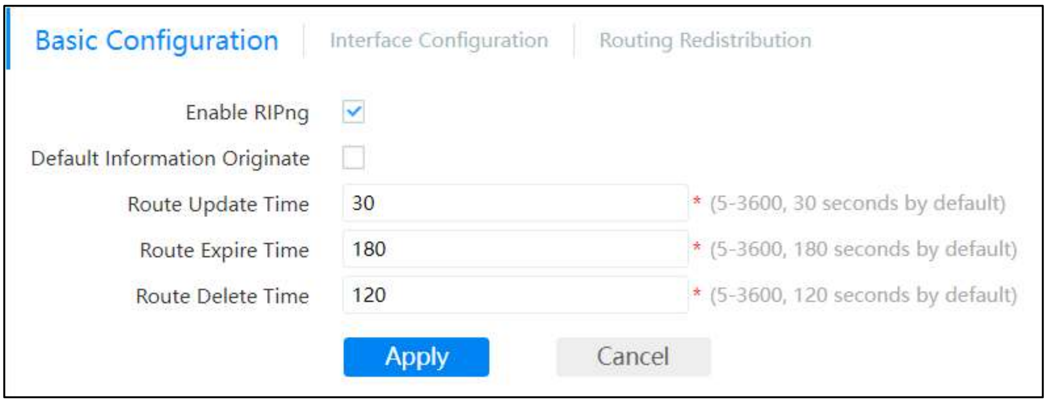
15.2 IPv6 Routing

15.2.1 RIPng

RIPng (RIP next generation) routing protocol. As a supplement to the RIP protocol supporting IPv6, it is not a brand new protocol. Therefore, it is consistent with the RIP protocol in principle.

Step 1. Choose "Network > Routing > RIPng".

Step 2. Configure basic configuration parameters, and click “Apply” after the configuration is complete.



Enable RIPng ☑

Default Information Originate □

Route Update Time 30 * (5-3600, 30 seconds by default)

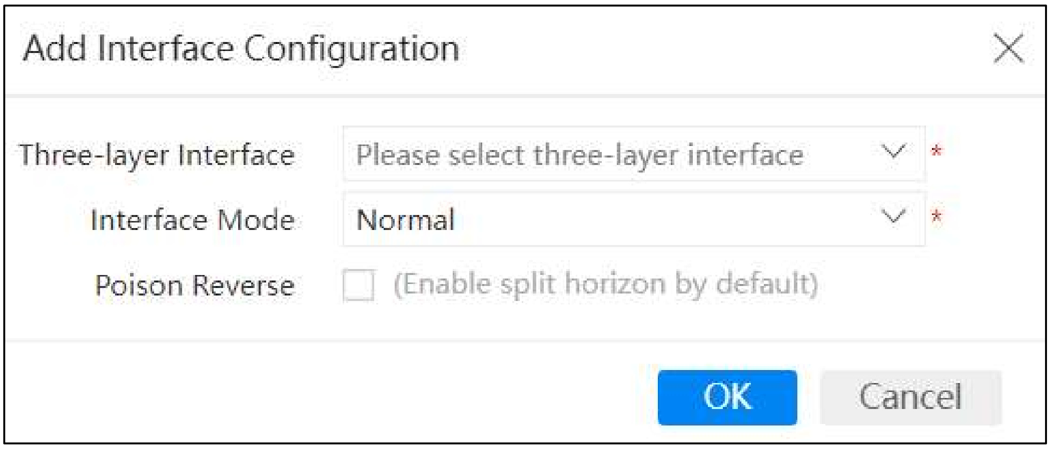
Route Expire Time 180 * (5-3600, 180 seconds by default)

Route Delete Time 120 * (5-3600, 120 seconds by default)

Parameter	Description
Enable RIPng	The RIPng function takes effect only after RIPng is enabled.
Default information originate	Enabled, advertise the default route. If not enabled, the default route will not be advertised.
Route update time	RIP routing update time; by default, it is 30 seconds to update once. Support customizing, and the range is 5-3600 seconds.
Route expire time	The expiration time of the RIP route, the default is 180 seconds. If a RIP route is not updated within 180 seconds, the RIP route will become invalid. Support customizing, and the range is 5-3600 seconds.
Route delete time	The clearing time of the RIP route, the default is 120 seconds. If an invalid RIP route is not updated within 120 seconds, the RIP routing table will be cleared. Support customizing, and the range is 5-3600 seconds.

Step 3. Add interfaces.

Interface configuration provides RIPng function interface selection and interface mode configuration. At the same time, the user can choose to enable or disable the interface split horizon function. The interface with the split horizon function enabled will not send out the routes learned from the interface through the interface, preventing loops.



Add Interface Configuration

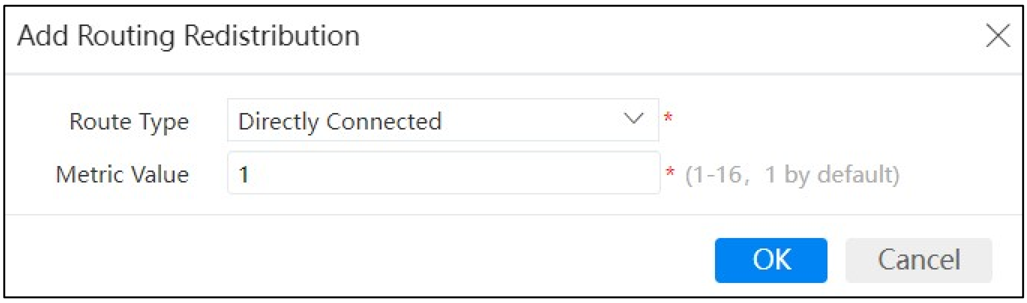
Three-layer Interface: Please select three-layer interface *

Interface Mode: Normal *

Poison Reverse: □ (Enable split horizon by default)

Parameter	Description
Three-layer interface	Select the interface to advertise RIP.
Interface mode	Select the working mode of the interface. Normal: Receive and send RIP updates. Passive: Receive but do not send RIP updates.
Poison reverse	Poison reverse means sending out a routing entry with a metric value of 16 hops (infinity), which is used to inform other routers that this route is no longer reachable. Check to enable the poison reverse function, the firewall will send the routing entry received from an interface, and then send it out through this interface, but the metric value is set to 16 hops (infinity). If the poison reverse function is not checked, the firewall enables split horizon by default, and the routing entries received from an interface will not be sent out from this interface.

Step 4. Add route redistribution.



Add Routing Redistribution

Route Type: Directly Connected *

Metric Value: 1 * (1-16, 1 by default)

The RIPng protocol allows users to import the routing information of other routing protocols on the device into RIPng and publish it to the outside. The route redistribution function is to realize the redistribution of the user-specified type of route to RIP and distribute it to the outside. Users can specify to redistribute direct routes, static routes, OSPF v3 routes, and BGP routes. At the same time, during the process of redistributing routes, users can specify the metric value of redistributed routes. By default, the metric value is 1. A route with a larger metric value has a lower priority, and a RIPng route with a metric value of 16 is considered unreachable.

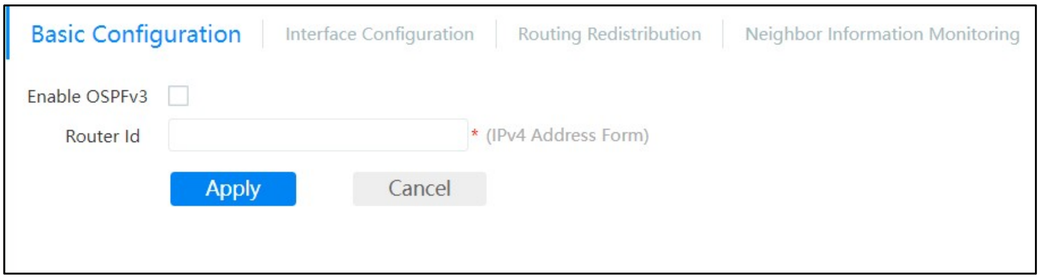
15.2.2 OSPFv3

OSPFv3 uses the same basic mechanism as OSPFv2, such as algorithms, DR election, and metric variables. Mainly used for routing IPv6 addresses.

However, OSPFv3 is not backward compatible with OSPFv2, so if users need to route IPv4 addresses, they need to enable OSPFv2 separately.

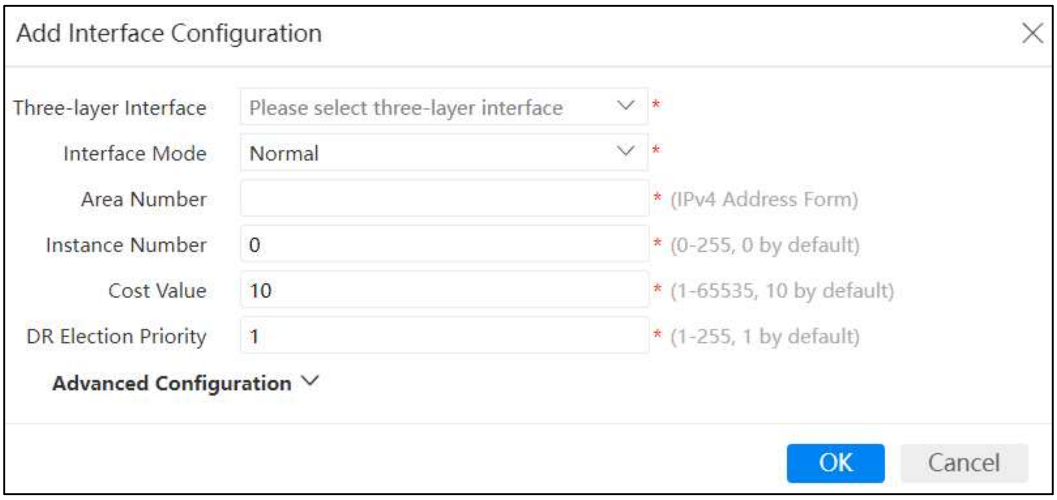
Step 1. Choose "Network > Routing > OSPF".

Step 2. Configure basic configuration parameters, and click “Apply” after the configuration is complete.



Parameter	Description
Enable OSPFv3	Select the check box to enable the OSPFv3 function. Otherwise, the OSPFv3 configuration does not take effect.
Route ID	Specify the Route ID (in the form of an IPv4 address) of the firewall. The Route ID must be unique within the same AS. At the same time, the Router ID is also used to uniquely identify neighbors.

Step 3. Click “Interface Configuration”, click “Add” to add interface configuration.



Add Interface Configuration

Three-layer Interface: Please select three-layer interface *

Interface Mode: Normal *

Area Number: * (IPv4 Address Form)

Instance Number: 0 * (0-255, 0 by default)

Cost Value: 10 * (1-65535, 10 by default)

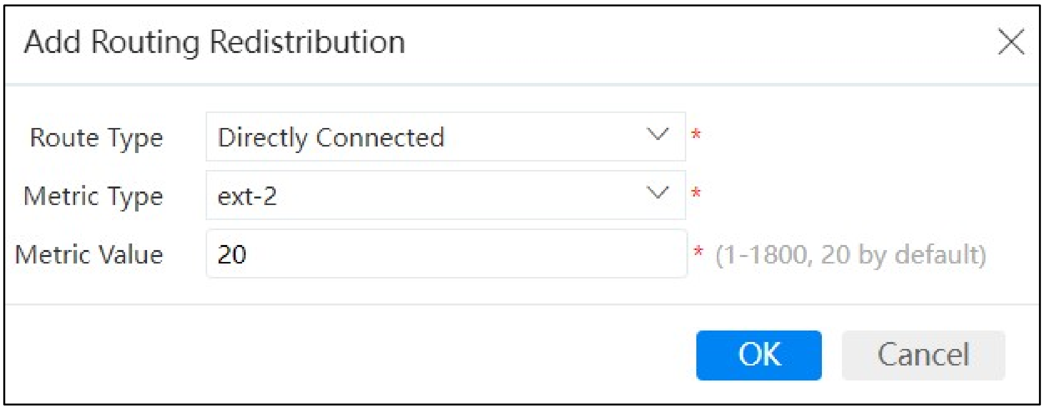
DR Election Priority: 1 * (1-255, 1 by default)

Parameter	Description
Three-layer interface	Select the interface to enable the OSP Fv3 function. It must work in L3 mode.
Interface mode	Select the working mode of the interface. • "Normal" mode allows receiving and sending OSPFv3 packets. • "Passive" mode prohibits receiving and sending OSPF v3 packets.
Area number	Specify the OSPFv3 domain of the interface, whose ID is in the form of an IPv4 address.
Instance number	Specify the instance number of the interface, that is, instance ID. The range is 0-255, and the default is 0. OSPFv3 supports running multiple instances on the same link to implement link multiplexing. Therefore, the firewall can establish neighbor relationships with different routers based on specified instances. This function is realized by instance ID. If the Instance ID configured on the interface does not match the Instance ID of the received OSPF 6 packet, the packet is discarded, and a neighbor relationship cannot be established.
Cost value	The cost value of the interface. The default is 10, support customizing, and the range is 1-65535.
DR election priority	The priority of the interface when the DR is elected. The default is 1, support customizing, and the range is 0-255.

Parameter	Description
Timer	**hello-interval:** The interval of the neighbor detection hello packet, the default is 10 seconds, support customizing, and the range is 1-3600. **dead-interval: The** neighbor dead timeout, the default is 40 seconds, if no neighbor is detected within 40 seconds, the neighbor will be dead. Support customizing, and the range is 1-3600.

Step 4. Click "Route Redistribution", and click "Add" to add route redistribution.

OSPFv3 allows users to import the routing information of other routing protocols on the device into OSPF and advertise it to the outside. The route redistribution function is to implement the redistribution of user-specified routes into OSPF and advertise them to the outside world.


Add Routing Redistribution

Route Type: Directly Connected *

Metric Type: ext-2 *

Metric Value: 20 * (1-1800, 20 by default)

Parameter	Description
Route type	Users can specify the route type of redistribution, there are four types in total: Direct routing, static routing, RIPng routing, BGP routing.
Metric type	There are currently two types of metrics: ext-1 and ext-2, and ext-2 is selected by default.
Metric value	Support customizing, the default is 20, and the range is 1-1800.

Step 5. Click "Neighbor Monitoring Information".

Neighbor information monitoring is used to view OSPFv3 neighbor status, neighbor address and other information. Neighbor information is the main source of information for monitoring, debugging OSPF v3, and troubleshooting OSPF v3 problems.

Table 15-1 Description of neighbor monitoring information interface

Parameter	Description
Neighbor ID	The ID of the neighbor.
Priority	The priority of the neighbor.
Status	Neighbor Status/Neighbor Role **state:** **down,** no hello packets from neighbors are received, but hello packets can be sent. **init,** the hello packet sent by the neighbor has been received. **two-way,** the firewall establishes a bi-directional relationship with the neighbor. **exstart,** when the link type is a broadcast network, before exchanging DBD, elect the master and slave. **exchange,** exchange DBD. **loading,** exchange LSAs. **full,** the adjacency relationship is established.
Failure time	The amount of time after which the current neighbor will expire.
Duration	How long the neighbor was created.
Neighbor address	The address of the neighbor, usually an IP address.
Local interface	The interface through which the firewall establishes a neighbor relationship with the neighbor. The interface name [interface role]

15.3 Dual-Stack

Due to the depletion of IPv4 addresses, the Internet is currently in a period of transition from IPv4 to IPv6. Therefore, not all the resources accessed by IPv6 terminals are IPv6 resources, and a large part of Internet resources actually still use IPv4 addresses. IPv6 transition technology is to realize mutual access between IPv6 network and IPv4 network.

Dual-stack technology enables both IPv4 and IPv6 protocol stacks on the device. The dual-stack protocol system can support IPv4 and IPv6 protocols at the same time, that is, it has an IPv4 address and an IPv6 address, so it can send and receive both IPv4 and IPv6 packets, communicate with IPv4 hosts through IPv4 addresses, and communicate with IPv6 hosts through IPv6. Realize the intercommunication between IPv4 hosts and IPv6 hosts.

Dual-stack protocol technology is the most widely used transition technology among IPv6 transition technologies, and it is also the basis of all other transition technologies.

15.4 DS-Lite

DS -Lite is to solve the problem that the private network IPv4 packets need to pass through the IPv6 network to access the public network IPv4 network.

15.4.1 Restrictions and Precautions

- The firewall only supports B4, that is, it supports the CPE access side function.
- B4 and AFTR must support dual-stack protocol.
- The DS-Lite manual mode is supported in the hot standby mode, but the automatic mode configuration is not supported.
- The DS-Lite source interface can be a physical interface or a logical interface, but must obtain an IP address dynamically through DHCPv6.
- The system must also support the IPv6 DNS server function.
- In the web mode, the default AFTR information acquisition method in the automatic mode is "stateful (DHCPv6)", and the stateless acquisition method must be configured through the command line.
- To use DHCP to obtain an address, you must first set the interface to DHCP mode, that is, it is not allowed to configure ds-lite first, and then configure the interface as dhcp.

15.4.2 Configure DS-Lite

Configure the DS-Lite function on the CPE side, and specify parameters such as source interface, tunnel interface, and mode.

Step 1. Select "Network > VPN > DS-Lite".

Step 2. Click “Add”.

Step 3. In the "Add DS-Lite" dialog box, select the "Enable" check box.

only if the DS-Lite policy is enabled.

Step 4. Configure DS-Lite parameters.

Parameter	Description
Name	Configure the DS-Lite tunnel name.
Description	Configure the corresponding description information for the tunnel, which is easy for the administrator to identify.

Parameter	Description
Source interface	Specify the interface of the DS-Lite tunnel. The IP address of the interface must be obtained through DHCPv6. An interface can be a physical interface or a logical interface.
Tunnel interface	Optional. Specify the tunnel interface used by DS-Lite.
Mode	• automatic mode In the automatic mode, the tunnel address is obtained automatically. The AFTR acquisition mode defaults to stateful, which automatically obtains the stateful IPv6 address, AFTR domain name, and DNS server address of the interface. No user configuration parameters are required. If the AFTR acquisition mode needs to be changed to stateless, it needs to be modified through the command line. • manual mode In manual mode, the user needs to configure the local address and AFTR address.

Step 5. After the configuration is complete, click “OK”.

The configured DS-Lite policy is displayed in the DS -Lite list. You can view the name, description, source interface, tunnel interface, mode, and enablement of the DS-Lite policy.

The configured DS-lite policy cannot be modified.

15.4.3 View DS-Lite Tunnel Information

Step 1. Choose “Data Center > Monitor > Tunnel Monitor”.

Step 2. Click “DS-Lite”.

Step 3. View the DS -Lite tunnel information.

After the DS -Lite tunnel is established, on the DS-Lite tunnel monitoring interface, the user can view the tunnel name, mode, AFTR domain name, local address, AFTR address, sending traffic, and receiving traffic of the DS-Lite tunnel.

The tunnels can be searched by tunnel name.

15.5 6in4 Manual Tunnel

6in4 manual tunnel refers to a 6in4 tunnel configured by manually specifying the destination and source addresses of the tunnel. Manual tunnels are easy to implement, but each tunnel must be manually configured and managed.

15.5.1 (Optional) Create a Tunnel Interface

A tunnel interface can be added under the interface, or it can be added when configuring a 6in4 manual tunnel.

Step 1. Choose “Network > Interface”.

Step 2. Click “Add” and select “Tunnel Interface”.

Step 3. Configure the name and IP address of the tunnel interface.

After the tunnel interface is added, the state is automatically up, and no address configuration is required.

Step 4. Click “OK”.

15.5.2 Configure a 6in4 Manual Tunnel

Step 1. Select " Network > VPN > 6in4 Tunnel".

Step 2. Click “Add”.

Step 3. Configure the parameters of the 6in4 manual tunnel.

Parameter	Description
Name	Specify the name of the 6in4 tunnel.
Description	The remarks of the 6in4 tunnel are to distinguish it from other 6in4 tunnels.
Tunnel type	Select "Manual Tunnel" as the tunnel type.
Destination address	The destination address is the peer gateway IPv4 address for establishing the tunnel.
Source interface	The interface on the firewall used to establish a 6in4 tunnel. The interface is required to be configured with an IPv4 address.
Source address	Select the IPv4 address of the interface used to establish the 6in4 tunnel. When "auto" is selected, as the initiator, the first IPv4 address whose type is float on the interface is used by default; as the receiver, any IPv4 address on the interface is used by default.
Tunnel interface	Select the tunnel interface bound to the source interface to establish a 6in4 tunnel. To create a new tunnel interface, click Add in the drop-down menu.
Enable	Check the "Enable" checkbox for the tunnel to take effect.

Step 4. After the configuration is complete, click “OK”.

After the configuration is complete, the tunnel is displayed in the 6in4 tunnel list. In the 6in4 tunnel list, you can check the name, source interface, destination address, tunnel type, tunnel interface, enabling status and other information of each 6in4 tunnel. You can edit, delete, update, and query the tunnels in the list.

15.5.3 Configure Route Drainage

After 6in4 tunnel is configured, the corresponding route needs to be added to the static route, and the IPv6 data that needs to be transmitted through the 6in4 tunnel is pulled into the tunnel.

Step 1. Choose "Network > Routing > Static Route".

Step 2. Click “Add”.

Step 3. Configure a static route to the destination IPv6 network, and the outbound interface is the corresponding tunnel interface.

Step 4. After the configuration is complete, click “OK”.

15.5.4 View 6in4 Tunnel

Choose “Data Center > Monitor > Tunnel Monitor”, and click the “6in4 Tunnel” tab. If you need to query a specific tunnel, you can select the tunnel name in the drop-down box.

After 6in4 tunnel is established, on the 6in4 tunnel monitoring interface, the user can view the tunnel name, tunnel type, local address, destination address, sent bytes, and received bytes after the 6in4 tunnel is established.

15.6 ISATAP tunnel

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is an IPv6 automatic tunnel technology.

15.6.1 Configure Tunnel Interface as an ISATAP Interface

To configure an ISATAP tunnel, you need to configure the tunnel interface as an ISATAP interface on the command line.

Step 1. Enter configuration view.

Execute **config terminal** in user view.

Step 2. Enter the tunnel interface view.

Execute **interface tunnel** *tunnel -name, where tunnel-name is the name* of the tunnel interface.

Step 3. Enable the IPv6 Router Advertisement sending function.

Execute **ipv6 ra send on.**

Step 4. Configure the link type of an IPv6 interface to support only unicast.

Execute **ipv6 ra unicasonly on** to only send notifications to ISATAP clients.

Step 5. Set the function of IPv6 router advertisement assignment address.

Execute **ipv6 ra prefix** *ipv6-address/prefix max-value best-value,* assign IPv6 prefixes to ISATAP clients. *max-value* indicates the valid time of the allocated address. Integer format, the value range is 0~4294967295, and the unit is second. *best-value* indicates the preferred time of the assigned address. Integer format, the value range is 0~4294967295, and the unit is second.

15.6.2 Configure ISA TAP Tunnel

Step 1. Select " Network > VPN > 6in4 Tunnel".

Step 2. Click “Add”.

Step 3. Configure the parameters of the 6in4 manual tunnel.

Parameter	Description
Name	Specify the name of the ISATAP tunnel.
Description	The remarks of the ISATAP tunnel, used to distinguish it from other 6in4 tunnels.
Tunnel type	Select "ISATAP" for the tunnel type.
Source interface	The interface on the firewall used to establish a 6in4 tunnel. The interface is required to be configured with an IPv4 address.
Source address	Select the IPv4 address of the interface used to establish the 6in4 tunnel. When "auto" is selected, as the initiator, the first IPv4 address whose type is float on the interface is used by default; as the receiver, any IPv4 address on the interface is used by default.
Tunnel interface	Select the tunnel interface bound to the source interface to establish a 6in4 tunnel. To create a new tunnel interface, click “Add” in the drop-down menu.
Enable	Check the "Enable" checkbox for the tunnel to take effect.

Step 4. After the configuration is complete, click “OK”.

15.6.3 View ISATAP Tunnel

Choose “Data Center > Monitor > Tunnel Monitor”, and click the “6in4 Tunnel” tab. If you need to query a specific tunnel, you can select the tunnel name in the drop-down box.

After the ISATAP tunnel is established, on the 6in4 tunnel monitoring interface, the user can view the tunnel name, tunnel type, local address, destination address, sent bytes, and received bytes after the ISATAP tunnel is established.

15.7 6to4 Tunnel

Through 6to4 tunnels, isolated IPv6 networks can be interconnected through IPv4 networks. The 6to4 tunnel is implemented through the Tunnel interface.

15.7.1 Configure 6to4 Address of Intranet Interface

Step 1. Select " Network > Interface" to find the corresponding intranet interface.

Step 2. Click “Edit” or the interface name link.

Step 3. Add the IP v6 address of the interface.

The IPv6 address of the interface is configured to correspond to the address of the 6to4 network subnet mapped from the IPv4 address of the external network interface.

Step 4. After the configuration is complete, click “OK”.

15.7.2 (Optional) Create a Tunnel Interface

The tunnel interface can be added under the interface, or it can be added when configuring the 6to4 tunnel.

Step 1. Choose “Network > Interface”.

Step 2. Click “Add” and select “Tunnel Interface”.

Step 3. Configure the name and IP address of the tunnel interface.

When the network environment does not require a relay, the tunnel interface bound to the 6to4 tunnel does not need to be configured with an address.

When the firewall needs to be relayed in the network environment, specify the IPv6 address of the tunnel interface according to the environment. At the same time, the specified IPv6 address must meet the requirements of 6to4 tunnel relay.

Step 4. Click “OK”.

15.7.3 Configure 6to4 Tunnel

Step 1. Select " Network > VPN > 6in4 Tunnel".

Step 2. Click “Add”.

Step 3. Configure the parameters of the 6to4 tunnel.

Parameter	Description
Name	Specify the name of the 6 to 4 tunnel.
Description	The remarks of the 6to4 tunnel, used to distinguish it from other 6in4 tunnels.
Tunnel type	Select "6to4" for the tunnel type.
Source interface	Select the external network interface connected to the IPv4 network as the source interface.
Source address	Select the IPv4 address of the interface used to establish the 6to4 tunnel. When "auto" is selected, as the initiator, the first IPv4 address whose type is float on the interface is used by default; as the receiver, any IPv4 address on the interface is used by default.
Tunnel interface	Select the tunnel interface bound to the source interface to establish a 6to4 tunnel. To create a new tunnel interface, click “Add” in the drop-down menu.
Enable	Check the "Enable" checkbox for the tunnel to take effect.

Step 4. After the configuration is complete, click “OK”.

15.7.4 View 6to4 Tunnel

Choose “Data Center > Monitor > Tunnel Monitor”, and click the “6in4 Tunnel” tab. If you need to query a specific tunnel, you can select the tunnel name in the drop-down box.

After the 6to4 tunnel is established, on the 6in4 tunnel monitoring interface, the user can view the tunnel name, tunnel type, local address, destination address, sent bytes, and received bytes after the 6 to 4 tunnel is established.

16 Disposal

The disposal center includes manual disposal, compromised hosts, risk hosts, and emergency response. Among them, manual disposal is to manually create a handling policy to deal with anomalies or threats; compromised hosts or risky hosts are the result of threat intelligence detection; emergency response is to use cloud big data to discover the latest IPS vulnerabilities or threat intelligence information and notify the firewall in time to perform configuration checks, repairs, upgrades, and other processing.

The priority of the manual handling policy is higher than that of threat intelligence. To configure a certain action in the threat intelligence library as "block" intelligence action as "permit", you can configure it by adding the handling object of the threat event type in the manual handling., add the ID of this piece of information, and configure the action as permit.

16.1 Threat Intelligence Detection

The firewall supports the threat intelligence detection function. After the user purchases the threat intelligence function, the firewall will install a threat intelligence library locally, and the firewall also supports the threat intelligence cloud detection function. By linking with cloud threat intelligence, compromised hosts and risky hosts can be found faster and more timely, helping users to respond faster.

16.1.1 Threat Intelligence Detection Instructions

Local Detection

As long as the threat intelligence function is purchased, the firewall will be installed with a local threat intelligence library by default, which can detect threats on the traffic passing through the firewall. The local threat intelligence library needs to be upgraded to the latest version in time, so as to better detect threats and reduce false positives.

Select "System > Collaboration > Cloud Link Protection" to set the local intelligence update method and update period.

Cloud Detection

Select "System > Collaboration > Cloud Link Protection", select the "Enable" check box to enable the threat intelligence cloud detection function.

16.1.2 View Threat Detection Results via Host View

The compromised hosts and risky hosts detected by threat intelligence can be viewed on the “Compromised Hosts” and “Risk Hosts” pages of the “Disposal”. The detected at the local are all compromised hosts. If the cloud detection is not enabled, there will be no content on the risk hosts page.

Compromised hosts or risky hosts can be displayed in two perspectives: host view and IOC list view.

The host view shows the detected compromised or risky hosts from the perspective of the host. In the compromised host view or risky host view, you can view the IP address, number of hits, actions, latest discovery time, first discovery time, source, user name, assets, etc. of the compromised host or risky host. Asset is the asset name corresponding to the IP address of the host. Click “Expand” to view IOCs hit by compromised or risky hosts.

The hit IOC may be IP, domain name or URL, etc. The IOC description is the description of the IOC in the IOC library (threat intelligence library). The source of the compromised host is local. The source of the risk host is Tianyuyun.

The upper end of the list of compromised hosts displays the number of compromised hosts to respond, the number of blocked compromised hosts, the number of compromised hosts to be logged only, the number of ignored compromised hosts, and the total number of compromised hosts.

The upper end of the risk host list displays the number of risk hosts to respond, the number of risk hosts to be blocked, the number of risk hosts to be logged only, the number of risk hosts to be ignored, and the total number of risk hosts.

Filter Compromised or Risky Hosts

Select the time and actions of compromised or risky hosts to view.

The firewall supports the filtering of compromised hosts or risky hosts by time and action.

- time

You can select " Last 1 day", "Last 7 days", "Last 30 days" or "Last 90 days".

- action

Actions support "Block", "Wait for response", "Ignore" and "Log Only".

Query Compromised Hosts or Risky Hosts

Type what you want to see in the query box. Support the query of IP and IOC in the lost host information, input the IP address and IOC keywords in the query box to query the lost host.

Dispose Compromised Hosts or Risky Hosts in Batches

Select the check boxes of compromised hosts or risky hosts to be disposed, and click “Response” or “Ignore” above the list to dispose hosts in batches.

- The response action supports "block" and "log only".
- After the compromised host or risky host is blocked, it cannot actively access resources on the intranet or extranet, but it can respond to access requests.
- The disposal time can be set to "Permanent", "90 days", "30 days", "7 days" and "1 day".
- After ignoring this information, the traffic of the compromised or risk host will be released, and the traffic of the host will not be blocked or logged.
- The information that has been ignored and processed can be undone through the undo operation.

Deal with a Single Compromised or Risky Host

Click "Response" or "Ignore" under the corresponding operation of a compromised or risky host to dispose of the host.

- The response action supports "block" and "log only".
- The disposal time can be set to "Permanent", "90 days", "30 days", "7 days" and "1 day".
- After ignoring the lost or risky host information, the host will not be dealt with.
- The information that has been ignored and processed can be undone through the undo operation.

View Disposition Results

Click "View" under the operation of a record to view the disposition result.

Check the IOC Details in the Local Library

Click an IOC name under a compromised host to view IOC details. IOC details include IOC name, ID, alarm name, threat level, malicious type, malicious family name and description, etc.

View Cloud IOC Details

Click an IOC name under a risky host to jump to the threat analysis page to view the details of the IOC.

Delete Compromised or Risky Hosts

When the administrator judges that the handling policy of a compromised or risky host is unreasonable or the IOC has expired, the administrator can click “Delete” to delete the compromised or risky host.

If the IOC corresponding to the compromised or risky host only appears under the host, the IOC entry in the IOC list will be deleted when the host is deleted.

Export Compromised or Risky Hosts

The compromised hosts or risky hosts can be exported in the form of an excel sheet. After filtering by time or action, or by keyword, the corresponding compromised or risky hosts can be exported.

Click 导出 , and click “Download” in the pop-up prompt box to export the lost host file to the local path.

16.1.3 View Threat Detection Results via IOC List View

The IOC list view shows the situation of the compromised host or risk host from the perspective of hitting the IOC. The list shows the IOC, the description of the IOC, the number of IOC hits, actions, and sources. Expand an IOC record, and you can view the host that hits the IOC, the latest hit time, the first hit time, user name, and asset.

The number of blocked IOCs is displayed above the IOC list of the compromised host, and only the number of log IOCs, ignored IOCs, and total IOCs are recorded.

The number of the IOCs to be responded, the number of blocked IOCs, the number of log IOCs, the number of ignored IOCs, and the total number of IOCs are displayed above the risk host IOC list.

Filter Compromised or Risky Hosts

Select the time and action of the IOC hit by the compromised host or risk host to be viewed.

The firewall supports the filtering of compromised hosts or risky hosts based on time and status.

- time

You can choose to view the IOCs of " Last 1 Day", "Last 7 Days", "Last 30 Days" or "Last 90 Days".

- action

  Actions support "Block", "Wait for response", "Ignore" and "Log Only".

Query the Compromised Host

Type what you want to see in the query box. Support querying the IP and IOC in the information of the compromised host or risk host that hits the IOC, and enter the IP address and IOC keyword in the query box to query the compromised host or risk host.

Check IOC Details in the Local Library

On the “IOC List View” page of “Compromised Host”, click an IOC name to view the IOC details. The IOC details include IOC name, ID, alarm name, threat level, malicious type, malicious family name and description, etc.

View Cloud IOC Details

Click an IOC name under a risky host to jump to the threat analysis page to view the details of the IOC.

Export Compromised or Risky Hosts

Compromised hosts or risky hosts can be exported in the form of an excel sheet. After filtering by time or action, or by keyword, the corresponding compromised or risky hosts can be exported.

Click ⇲ 导出 , and click “Download” in the pop-up prompt box to export the file of the compromised host or risky host to the local path.

Batch Process IOCs Detected in the Cloud

After the local IOC library detects a malicious IOC, it will automatically deal with it according to the response actions set in the IOC library, without the need for users to set.

On the “IOC List View” page of “Risk Host”, select the check boxes of the IOCs to be disposed, and click “Response” or “Ignore” at the top of the list to dispose IOCs in batches.

- The response action supports "block" and "log only".

  After an IOC is blocked, users cannot access the IOC.
- The disposal time can be set to "Permanent", "90 days", "30 days", "7 days" and "1 day".
- After the IOC is ignored, the IOC traffic will be allowed, and the IOC will not be blocked or logged.

- The ignored and disposed IOCs can be undone by canceling the previous disposal.

Handle a Single IOC Detected by the Cloud

On the “IOC List View” page of “Risk Host”, click “Response” or “Ignore” under the corresponding operation of an IOC to dispose of the hit IOC.

- The response action supports "block" and "log only".
- The disposal time can be set to "Permanent", "90 days", "30 days", "7 days" and "1 day".
- After the IOC is ignored, the IOC traffic will be allowed, and the IOC will not be blocked or logged.
- The ignored and disposed IOCs can be undone by canceling the previous disposal.

View IOC Response Details

Click “View” under the operation of a record to view the details of the IOC response.

16.2 Manual Disposal

The firewall supports direct handling of the corresponding abnormal behaviors in the logs, and the handling results will be listed in the "Manual Disposal" of the "Disposal". Users can also add disposal objects on the manual disposal page for disposal.

In the centralized management mode, the disposal policies issued by the smart management analysis system are also displayed on the manual disposal page.

For SkyEye linkage or NGSOC linkage configured, you can also issue a disposal policy to the firewall after threat intelligence detection is performed on the SkyEye or NGSOC analysis platform.

16.2.1 Restrictions and Precautions

- The firewall first matches the manual handling policy, and then matches the threat intelligence library.
- The priority of disposal policy issued by the intelligent management analysis system, Tianyan, and NGSOC is higher than manual disposal policy created locally in the firewall.

16.2.2 Add a Disposal Policy Locally

Step 1. Choose “Disposal > Manual Disposal”.

Step 2. Click “Add”.

Step 3. Configure the disposal type and corresponding parameters.

The disposition type supports " Network Connection", " Domain Name ", "URL", "Threat Name", "Application Name" and "Instant Messaging".

Disposal type	Related parameters	Description
Network connection	IP type	Support IPv4 address type and IPv6 address type.
	Source address	Enter the source address of the network connection. Enter an IPv4 address for the IPv4 address type, and enter an IPv6 address for the IPv6 address type.
	Source port	Enter the source port of the network connection. The port range is 1 ~65535.
	Destination address	Enter the source address of the network connection. Enter an IPv4 address for the IPv4 address type, and enter an IPv6 address for the IPv6 address type.
	Destination port	Enter the destination port for the network connection. The port range is 1 ~65535.
	Protocol	Select the protocol type for the network connection. The protocol type defaults to any, and can be set to TCP, UDP, ICMP, ICMPv6.
Domain name	Domain name	Enter the malicious domain name to dispose of. It is allowed to enter 1~128 domain names, and the maximum number of characters for a single domain name is no more than 255. Multiple domain names are separated by a carriage return, one domain name per line.
URL	URL	Enter the malicious URL to dispose of. It is allowed to enter 1~128 URLs, and the maximum length of a single URL cannot exceed 1023 characters. Multiple URLs are separated by carriage returns, one URL per line.
Threat name	Threat type	Click “Add” to add a threat event. Multiple Threat Events can be added. Threat types support "antivirus", "intelligence detection" and "other threats".
	Threat ID	Enter the threat ID or intelligence ID corresponding to the threat type. Threat ID or Intelligence ID can be obtained from threat logs.
Application	Application	Click the “Application Name” drop-down box

Disposal type	**Related parameters**	**Description**
Name	Name	and select an application from the drop-down menu. All predefined and custom apps can be selected from the drop-down menu. If the required application is not in the drop-down menu, please add a custom application first.
Instant messaging	QQ account	Enter the QQ account number to be processed. It is allowed to enter 1~128 QQ account numbers, and the maximum number of characters for a single QQ account number shall not exceed 31. Multiple QQ accounts are separated by carriage return characters, one QQ account per line.

Step 4. Configure the disposal action and disposal time.

Parameter	**Description**
Action	The processing action supports block, log and permit. • Block means discarding packets and recording log alarms. • Log, which means that the packet is allowed to pass, but the log alarm is recorded. • Permit, means to allow the packet to pass. Only the threat name type supports it. When the user judges that the threat event is not a threat, the action can be set to permit.
Disposal time	Indicates the time period during which the action is valid. The disposal time supports "permanent", "90 days", "3 0 days", "7 days" and "1 day".

Step 5. After the configuration is complete, click “OK”.

16.2.3 View Manual Disposal Policy

Step 1. Choose “Disposal > Manual Disposal”.

Step 2. Select the source, time, and action of the manual disposal policy to view.

The firewall supports manual disposal policy filtering by source, time, and status.

- Source

  All sources are supported by default. The source supports "SMAC", "SkyEye", "NGSOC" and "Local".

- Type

Support all types by default. Types include "Network Connection ", "Domain Name", "URL", "Threat Name", "App Name", and "IM".

- Action

  Actions support "Block", "Wait for Response", "Ignore" and "Log".

Step 3. Query manual disposal policies for specific conditions.

Type what you want to see in the query box.

Support the query of IP addresses, domain names, URL addresses, QQ numbers, threat IDs, and application names for processing information in manual disposal.

Step 4. View manual disposition policies.

Parameter	Description
Create time	The time when this manual disposal policy was created.
Disposition type	Types include "Network Connection", "Domain Name", "URL", "Threat ID", "Application Name", and "Instant Messaging".
Disposal information	Source and destination information in manual disposal policies. Click on the destination information to jump to the "Network Activity" of the "Analysis Center" with conditions, and view the network activities related to the disposal information.
Source	The source supports "SMAC", "SkyEye", "NGSOC" and "Local".
Effective time	The time when this manual handling policy takes effect.
Expiry time	If the manual disposal policy has been disposed and the effective time is not permanent, the expiration time will be displayed here. If it is permanent, it will be displayed as "-".
Hit number	The number of times this manual handling policy hits.
Action	Disposal actions support wait for response, block, log only, permit (only supported by threat event types) and ignore.

Step 5. Click “Dispose” or “Ignore” under “Actions” to dispose of the manual disposition policy.

Different types of manual disposal policies are processed separately. The disposal actions are divided into block, log, and bypass (only supported by the threat ID type), and the disposal time is divided into permanent, 90 days, 30 days, 7 days, and 1 day.

Ignore the risky host information, and do not take any action on the risky host and IOC content.

The ignored and processed risk host intelligence can be revoked, and the previous processing can be revoked.

Step 6. View the number of hit details.

Click to view hit count details.

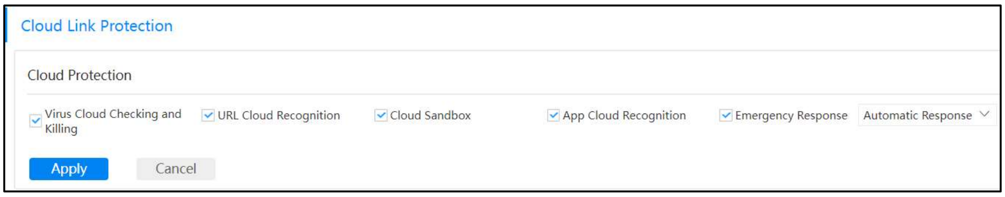
16.3 Emergency Response

The emergency response is issued by Tianyuyun, which is used to urgently notify users of the vulnerabilities in the system or the latest threat information. The emergency response checks the user's vulnerability protection or anti-spyware configuration, and prompts the user to upgrade the IPS library or threat intelligence library.

16.3.1 Enable Emergency Response

The prerequisite for receiving emergency response alerts is to enable the emergency response function and ensure that the routing from the firewall to the cloud is reachable.

Select "System > Collaboration > Cloud Link Protection", select the "Emergency Response" check box in the "Cloud Link Protection" area box, and select the emergency response method.



Cloud Link Protection

Cloud Protection

☑ Virus Cloud Checking and Killing ☑ URL Cloud Recognition ☑ Cloud Sandbox ☑ App Cloud Recognition ☑ Emergency Response Automatic Response

The response mode supports "Manual Response " and "Automatic Response ". The differences between the two methods are as follows:

- manual response

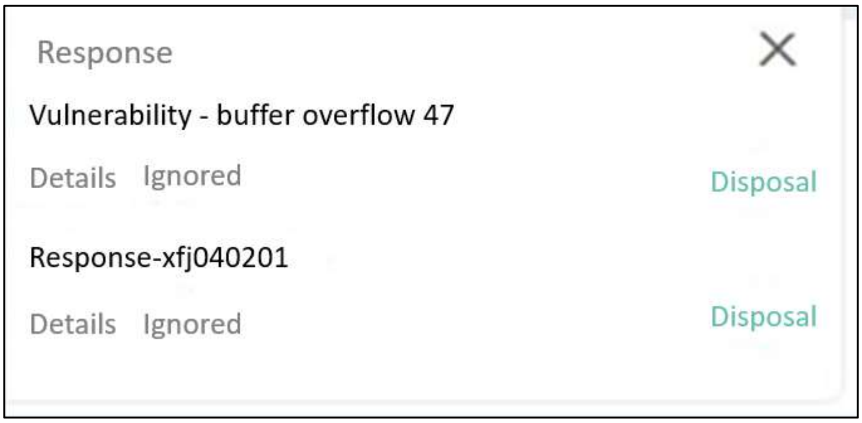
  In the case of manual response, only an alarm is given, and the user needs to manually upgrade the IPS library or threat intelligence library.

- automatic response

  In the case of automatic response, the system will automatically upgrade the IPS library and threat intelligence library.

16.3.2 View Emergency Response Notifications

When the firewall receives emergency response information, the system will pop up an emergency response prompt box below the alarm information button. This prompt page is visible in the upper right corner of all pages. Each page displays up to two emergency response messages.



Response

Vulnerability - buffer overflow 47

Response-xfj040201

In automatic mode, the notification will be automatically closed after 5s. In the manual mode, users can click the "Dispose" or "Ignore" button to dispose of the emergency response information or ignore the emergency response. After disposing successfully, the notification will be automatically closed and the next alarm will be displayed; click "Details", and you can view the emergency response details.

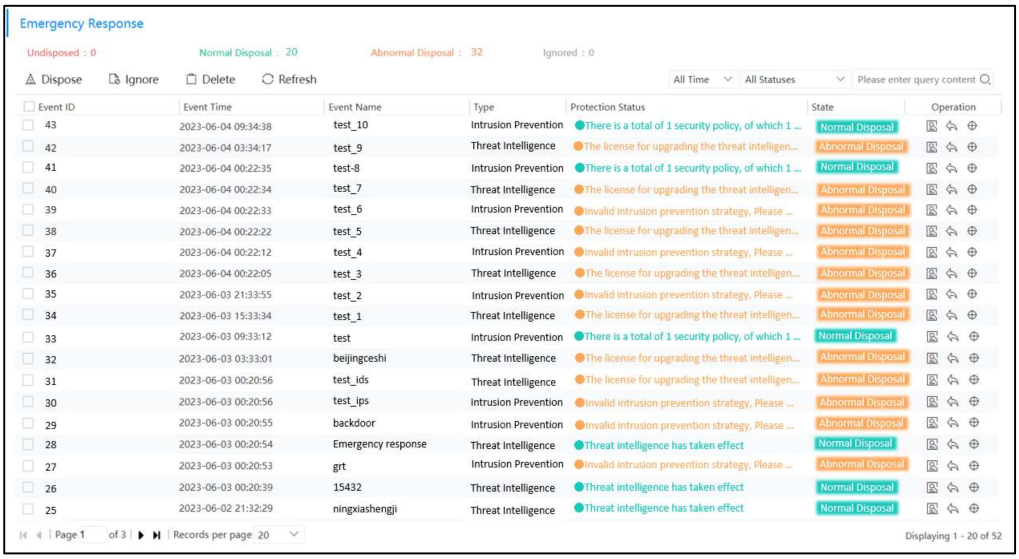
After clicking "Dispose" or "Ignore", a prompt box will prompt whether to confirm the operation. After confirming the execution, jump to the "Emergency Response" page to view the status of the emergency response execution. If the disposition fails, "Disposition exception" is displayed.

Click the "Close" button to close the emergency response prompt box.

16.3.3 Description for Emergency Response Event List

Emergency response events are displayed on the “Emergency Response” page of the “Disposal Center”. The first line of the emergency response shows the number of emergency response announcements of "undisposed", "normal", "abnormal" and "ignored".

The emergency response list displays information such as the event ID, event time, event name, type, protection status, and state of the emergency response event.



Emergency Response

Undisposed : 0 Normal Disposal : 20 Abnormal Disposal : 32 Ignored : 0

□ Event ID	Event Time	Event Name	Type	Protection Status	State	Operation
□ 43	2023-06-04 09:34:38	test_10	Intrusion Prevention	●There is a total of 1 security policy, of which 1 ...	Normal Disposal	
□ 42	2023-06-04 03:34:17	test_9	Threat Intelligence	●The license for upgrading the threat intelligen...	Abnormal Disposal	
□ 41	2023-06-04 00:22:35	test-8	Intrusion Prevention	●There is a total of 1 security policy, of which 1 ...	Normal Disposal	
□ 40	2023-06-04 00:22:34	test_7	Threat Intelligence	●The license for upgrading the threat intelligen...	Abnormal Disposal	
□ 39	2023-06-04 00:22:33	test_6	Intrusion Prevention	●Invalid intrusion prevention strategy, Please ...	Abnormal Disposal	
□ 38	2023-06-04 00:22:22	test_5	Threat Intelligence	●The license for upgrading the threat intelligen...	Abnormal Disposal	
□ 37	2023-06-04 00:22:12	test_4	Intrusion Prevention	●Invalid intrusion prevention strategy, Please ...	Abnormal Disposal	
□ 36	2023-06-04 00:22:05	test_3	Threat Intelligence	●The license for upgrading the threat intelligen...	Abnormal Disposal	
□ 35	2023-06-03 21:33:55	test_2	Intrusion Prevention	●Invalid intrusion prevention strategy, Please ...	Abnormal Disposal	
□ 34	2023-06-03 15:33:34	test_1	Threat Intelligence	●The license for upgrading the threat intelligen...	Abnormal Disposal	
□ 33	2023-06-03 09:33:12	test	Intrusion Prevention	●There is a total of 1 security policy, of which 1 ...	Normal Disposal	
□ 32	2023-06-03 03:33:01	beijingceshi	Threat Intelligence	●The license for upgrading the threat intelligen...	Abnormal Disposal	
□ 31	2023-06-03 00:20:56	test_ids	Threat Intelligence	●The license for upgrading the threat intelligen...	Abnormal Disposal	
□ 30	2023-06-03 00:20:56	test_ips	Intrusion Prevention	●Invalid intrusion prevention strategy, Please ...	Abnormal Disposal	
□ 29	2023-06-03 00:20:55	backdoor	Intrusion Prevention	●Invalid intrusion prevention strategy, Please ...	Abnormal Disposal	
□ 28	2023-06-03 00:20:54	Emergency response	Threat Intelligence	●Threat intelligence has taken effect	Normal Disposal	
□ 27	2023-06-03 00:20:53	grt	Intrusion Prevention	●Invalid intrusion prevention strategy, Please ...	Abnormal Disposal	
□ 26	2023-06-03 00:20:39	15432	Threat Intelligence	●Threat intelligence has taken effect	Normal Disposal	
□ 25	2023-06-02 21:32:29	ningxiashengji	Threat Intelligence	●Threat intelligence has taken effect	Normal Disposal	

Page 1 of 3 | Records per page 20 Displaying 1 - 20 of 52

The emergency response event supports "Intrusion Prevention" and "Threat Intelligence ", and the protection status refers to the emergency protection response status of Intrusion Prevention or Threat Intelligence.

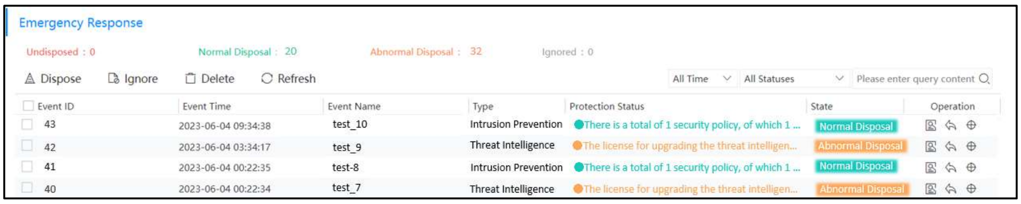
Status refers to the disposition status of the emergency response event. Disposition statuses include normal disposal, abnormal disposal, undisposed, and ignored.

16.3.4 Operation Instructions

In addition to handling emergency events in the emergency response notification prompt box, you can also handle emergency response events on the "Emergency Response" page of the "Disposal". It can also perform operations such as filtering, searching, and viewing details of emergency events.

Click Status Statistics to Filter by Status

The first line of the emergency response shows the number of emergency response announcements of "Undisposed", "Normal disposal" and "Abnormal disposal".



Emergency Response

Undisposed : 0 Normal Disposal : 20 Abnormal Disposal : 32 Ignored : 0

□ Event ID	Event Time	Event Name	Type	Protection Status	State	Operation
□ 43	2023-06-04 09:34:38	test_10	Intrusion Prevention	●There is a total of 1 security policy, of which 1 ...	Normal Disposal	
□ 42	2023-06-04 03:34:17	test_9	Threat Intelligence	●The license for upgrading the threat intelligen...	Abnormal Disposal	
□ 41	2023-06-04 00:22:35	test-8	Intrusion Prevention	●There is a total of 1 security policy, of which 1 ...	Normal Disposal	
□ 40	2023-06-04 00:22:34	test_7	Threat Intelligence	●The license for upgrading the threat intelligen...	Abnormal Disposal	

- Click the “Undisposed” link to display all undisposed alarms.
- Click the “Normal disposal” link to display all normal disposed alarms.

- Click the “Abnormal disposal” link to display all abnormal disposed alarms.
- Click the “Ignore” link to display all ignored alarms.

Select Parameters in the Time or State Drop-down Box to Filter

Emergency response events support filtering by time and status. By default, emergency response events of all time and all states are displayed. Select parameters in the "Time" or "Status" drop-down box on the right to filter.

- time

  Support selecting "Last 1 day", "Last 7 days" and "Last 30 days".
- state

  Status supports "Normal disposal", "Abnormal disposal", "Undisposed" and "Ignored".

Filter by Event Name

Emergency response events support searching by event name. Enter the event name of the emergency response event to be viewed in the query box, and click Enter to display all emergency response events of the protection event name keyword in the search results.

View Details

Click 🔍 under “Operation” to view the details of the corresponding emergency response announcement.

Handle a Single Emergency Response Event

The emergency response events that have been automatically disposed of do not require manual disposal. For emergency response events that are “Undisposed” or “Abnormal disposed”, users need to manually handle them.

Click the "Dispose" button of the operation corresponding to the emergency response event to dispose of it. Carry out corresponding emergency response protection procedures. The protection process is consistent with the protection process of automatic disposal.

Ignore a Single Emergency Response Event

Click the "Ignore" button corresponding to the emergency response event to ignore the emergency response event.

Batch Dispose Emergency Response Events

Select the check boxes of one or more emergency response events, and click ⚠ 处置 on the top of the list to process emergency response events in batches.

Batch Ignore Emergency Response Events

Select the check boxes of one or more emergency response events, and click 忽略 on the top of the list to ignore the selected emergency response events.

View Protection Status

Click the “Protection Status” link for an emergency response event to view the protection status of the emergency response event. The protection status displayed in different stages is different. Please modify and check according to the prompts.

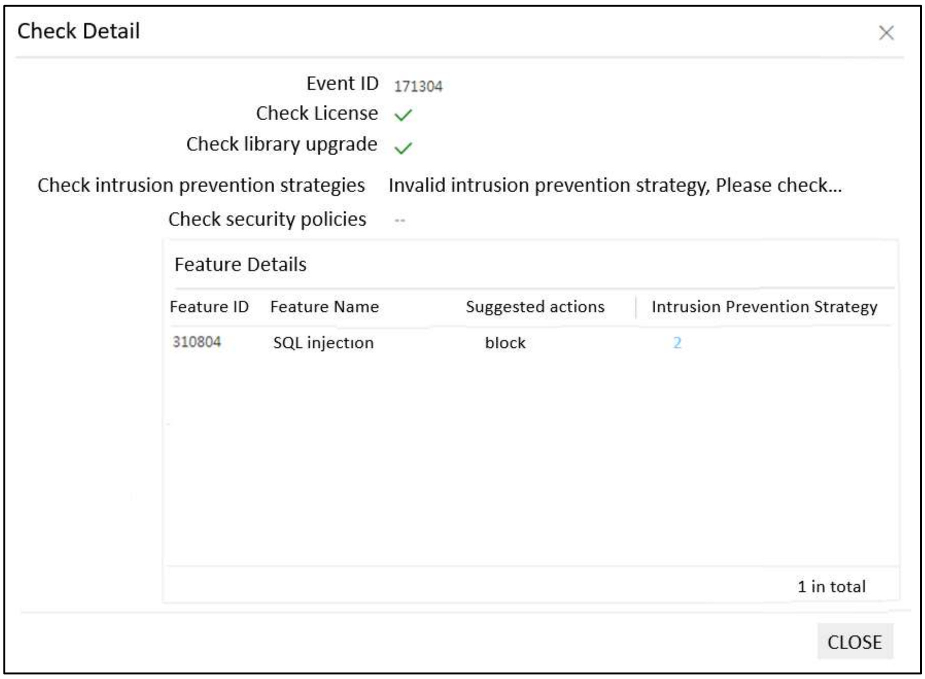
16.3.5 Description of Protection Process

Emergency response event supports “Intrusion Prevention” and “Threat Intelligence”. The following describes the protection process of intrusion prevention emergency response and threat intelligence emergency response respectively.

Intrusion prevention process

IPS emergency response protection is as follows:

1. Check the license. The license allows the IPS upgrade before proceeding to the following steps. If the license expires, please purchase a new license.
2. Check library upgrade. Automatically upgrade the library. If the upgrade encounters a problem, the following steps cannot be performed. Please troubleshoot according to the reason for the upgrade failure. After the library upgrade is successful, proceed to the next steps.
3. Check intrusion prevention policies. Check whether the intrusion prevention configuration file is configured and whether the vulnerability configuration in the intrusion prevention configuration file is valid. Please add an intrusion prevention configuration file or modify the action configured in the intrusion prevention policy according to the vulnerability characteristics details.
4. Check security policy. Check how many security policies exist in total, and how many security policies refer to intrusion prevention policies.



Event ID 171304
Check License ✓
Check library upgrade ✓
Check intrusion prevention strategies Invalid intrusion prevention strategy, Please check...
Check security policies --

Feature Details

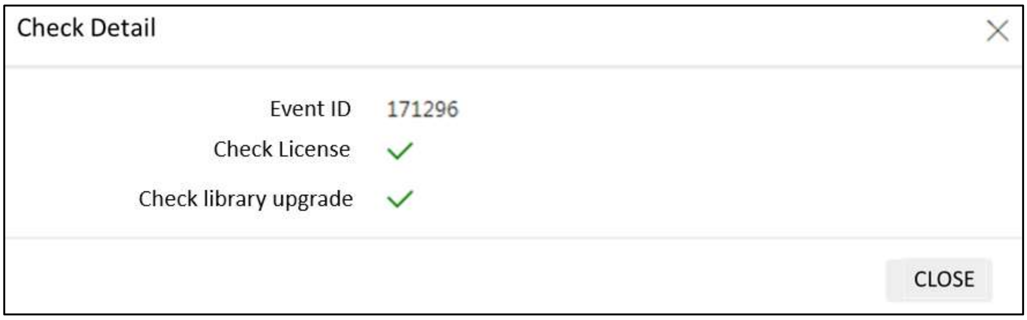
Feature ID	Feature Name	Suggested actions	Intrusion Prevention Strategy
310804	SQL injection	block	2

1 in total

Threat Intelligence Protection Process

The process of threat intelligence emergency response protection is as follows:

1. Check the license. The license allows the threat intelligence library to be upgraded before proceeding with the steps below. If the license expires, please purchase a new license.
2. Check the library upgrade. Automatically upgrade the library. If the upgrade encounters a problem, the following steps cannot be performed. Please troubleshoot according to the reason for the upgrade failure. After the library upgrade is successful, proceed to the next steps.



Event ID 171296
Check License ✓
Check library upgrade ✓

17 Data Center

17.1 Log

17.1.1 Overview

The log module is used to record and display events that are valuable to users, and can be used to discover and trace security issues.

Logs include traffic logs, threat logs, domain name logs, URL filtering logs, mail filtering logs, content logs, behavior logs, instant messaging logs, operation logs, and system logs. Logs are valuable information recorded by the firewall to reflect network conditions, and the network conditions can be displayed by analyzing the logs. The analysis center and statistical data are the results of analysis and statistics based on logs.

Traffic Log

The traffic logs generated when the data flow matches the security policy of the firewall and the traffic logging function is enabled in the security policy. Traffic logs are full storage of traffic. By analyzing traffic logs, you can grasp the situation of network activities.

Sandbox Log

The sandbox log is the log generated when the firewall receives the sandbox detection result when the firewall is linked with the SkyEye sandbox. Through the sandbox log, you can view parameters such as file name, detected threat name, severity, attacker, victim, file MD5, file type, application, source IP, destination IP, protocol, etc.

Threat Log

Threat logs are logs generated when the firewall detects threats. Threat log types include "vulnerability protection", "anti-spyware", "anti-virus", "attack protection", "IPMAC binding protection", "DHCP protection", "threat handling", "threat intelligence", "address blacklist" and "Domain blacklist" generated logs. This type of threat will be detected and a threat log will be generated only if the user has enabled the corresponding function and configured the corresponding policy.

When the threat type in the threat log is "antivirus", the threat name displays the corresponding "threat type (threat subtype)/threat name" in the virus database. Threat types include Worm (worm), Trojan (trojan horse), GrayWare (grayware), RiskWare (riskware), etc.; the severity is the severity level corresponding to the threat defined in the virus database, divided into "high risk" and "medium risk" and "low risk"; the application corresponds to the protocol and application supported by the anti-virus (IMAP, SMTP, POP3, FTP, SMB and the specific HTTP application identified) ; the threat log of the anti-virus type contains the virus samples that can be downloaded, the sample type (black means virus), sample MD5 and detection method (local means local virus detection, cloud means cloud virus detection).

When the threat type of the threat log is " anti-spyware " or " vulnerability protection ", the threat name corresponds to the spyware or vulnerability name defined in the IPS library; the severity is the severity level corresponding to the threat defined in the IPS library, divided into "high risk", “Medium Risk” and “Low Risk”. The Threat subcategory corresponds to the antispyware or vulnerability protection category.

The threat log of the "Threat Intelligence" type is a threat log generated by local IOC intelligence detection. The threat name of this type of threat log is the threat name defined in the IOC intelligence database, and the severity is the severity level corresponding to the threat defined in the IOC intelligence database. The severity level is divided into "high risk", "middle risk" and "low risk". When the threat intelligence preset action is not enabled, the threat log action for all intelligence detection types is "log". After the threat intelligence preset action is enabled, the "high-risk" threats are blocked and recorded in the log. The "middle risk" and "low risk" threats are not blocked and only recorded in the log. Click the link on the left side of the intelligence ID to log in to the "Threat Intelligence Center" and query the details of the threat intelligence.

Threat logs of the "Threat Disposal " type are threat logs generated after the user disposes of a compromised host, a risk host, or a disposition policy manually added by the user. The threat level of this type of threat log is "high risk".

Domain Log

The domain name log records the successfully resolved DNS packet information in the traffic that hits the security policy of the firewall. Only when the traffic log switch is enabled, the domain name log will be recorded.

Users can query domain name logs according to conditions in the domain name log. When a user discovers a DNS-related threat, he can query the domain name log to learn the details of the domain name request, and further determine and deal with the problem.

If a domain name exists in the domain name blacklist, the log that hits the domain name will be recorded in the "Threat Log"; if a certain domain name exists in the domain name white list, the log that hits a domain name outside the white list will be recorded in "Threat logs", no logs will be generated if the whitelist is hit.

URL Filtering Log

The URL log records the logs generated by the URL filtering function. Users can view the URLs allowed and blocked by the firewall and the detailed information on accessing these URLs through the URL filtering logs, and query all generated URL filtering logs according to conditions. If abnormal URL accesses are found, they can be dealt with.

Mail Filtering Log

The mail filtering log records the logs generated by the mail filtering function. Users can check the email filtering allowed and blocked by the firewall and their detailed information through the email filtering log. And perform conditional query on all generated email filtering logs. If abnormal email sending and receiving behaviors are found, it can be dealt with.

Content Log

The content log records the logs generated by the content filtering function and file filtering function. Users can view the content or files that are allowed or blocked by the firewall and the detailed information about accessing the content or files through the content log. And perform conditional query on all generated content logs. If any abnormal behavior is found, it can be dealt with.

Behavior Log

Behavior logs record the logs generated by behavior control and linkage terminal control functions. Users can check the behavior of HTTP, SMTP, POP 3, IMAP, FTP, and Telnet allowed or blocked by the firewall through the behavior log, or the terminals blocked by linkage terminal control. And query all the generated behavior logs according to the conditions. If any abnormal behavior is found, it can be dealt with.

IM Log

IM log records the log generated by QQ online and offline.

Notes

QQ is forced to go offline and instant messaging logs will not be recorded.

Operation Log

The log generated by the firewall configuration change will be recorded in the operation log. From the operation log, the user can view the change time, module, source user, source IP, login method, device, and detailed information of the addition, deletion, and modification of the firewall configuration.

System Log

During the running of the firewall, all events automatically generated by the system will be recorded in the system log, such as administrator login and logout, interface status change, tunnel status change, library upgrade information, optical module incompatibility information, system generated warning information, etc.

17.1.2 Log Operation

Set the Displayed Log Parameters

Some log parameters are displayed by default in the log list, and the user can click ⋮ on the left side of "Operation" to select the parameters to be displayed. Select the check box corresponding to the parameter to display the parameter, and uncheck the check box corresponding to the parameter to not display the parameter.

Search Log Description

Firewall logs support fuzzy search and search by filter criteria. Fuzzy search is only supported on the “Fuzzy Search” page. The “Fuzzy Search” page supports content for all log types. Search by filter criteria supports searching on a single log type page, and also supports multi-log type range log search on the "Fuzzy Search" page.

Both fuzzy search and search by filter criteria are supported on the "Fuzzy Search" page:

- Fuzzy search

On the "Fuzzy Search" page, you can enter character strings or Chinese characters in the search box to perform fuzzy searches. The query content must completely match the value of the corresponding attribute to search for results.

- Search by filter

Check “Criteria” to search by entering grammatically compliant conditions or by adding filter conditions.

- Click the parameter displayed in green in the traffic log list to add search criteria in the search bar. When multiple conditions are clicked, the relationship between parameters is "and" by default. After the settings are complete, click “Search”.
- Manually enter the search criteria in the search box, and click “Search” after the device is completed.
- Click + at the right of the search bar to add search criteria. Multiple searches can be added, and after the addition is complete, click "Close". Search directly.
- Click 🧹 on the right side of the search bar to clear the search criteria.
- Click 💾 on the right side of the search bar to bookmark the search criteria.
- Click ⧉ on the right side of the search bar to display favorite search criteria. And you can select it and add it to the search box to search.
- Click the time drop-down box on the right side of the search bar to select the log time range to be searched.

Fuzzy Search

For fuzzy search, you only need to enter the value of the corresponding parameter or the number containing the number in the search box, and no parameter item is required. Search is more convenient. However, fuzzy search only supports the input of a single parameter value, and does not support multiple parameter values to be searched together.

Step 1. Choose “Log > Fuzzy Search”.

Step 2. Set the desired log time range. For the time range, select a predefined time period, or you can customize the time range. The minimum predefined period is "the last day" and the maximum is "the last month".

Step 3. To perform a fuzzy search, enter a character string or Chinese character in the search box, and click Search.

For fuzzy search, do not check "Condition". When the "Condition" checkbox is selected, enable search by filtering conditions.

Notes

For all parameters of the log, only URL, domain name, sender, recipient, email subject, cc, sample MD5, intelligence ID, and IM account can be searched if they contain search values. Other parameters must fully match the parameter values, so as to be searched.

Threat Log Filtering

Threat logs support filtering by log type. Select the check box in front of "All Threat Types " to display all types of threat logs. You can set the threat log types to be displayed by checking or unchecking a threat type in the drop-down menus of the “Intrusion”, “Malware”, “Attack”, and “Intelligence” drop-down boxes.

Search by Filtering Conditions

Step 1. Choose “Data Center > Log”.

Step 2. Click the desired log type.

The log types that can be searched by filtering conditions include "traffic log", "threat log", "domain name log", " URL filtering log", "mail filtering log", "content log", "behavior log", "instant messaging log", “Operation Log” and “System Log”.

For log content search of multiple log types, please select the " Fuzzy Search" page.

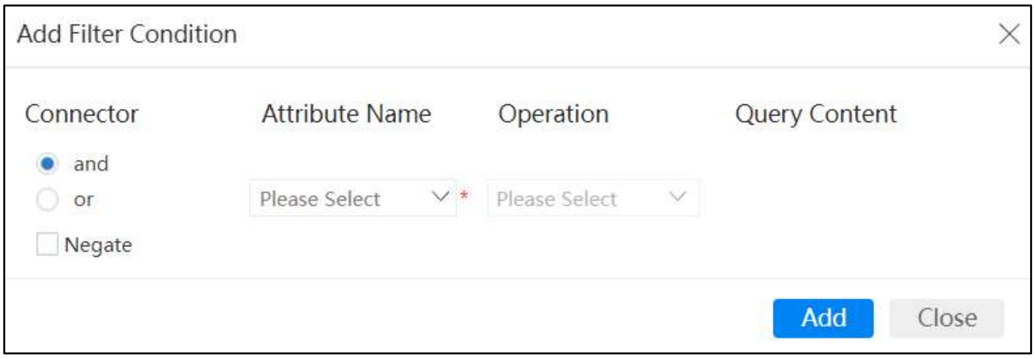
Step 3. Set the desired log time range. For the time range, select a predefined time period, or you can customize the time range. The minimum predefined period is "the last day" and the maximum is "the last month".

Step 4. Add filtering conditions.

On the fuzzy search page, you need to select "Condition" to search by filter conditions. The query content must completely match the value of the corresponding attribute to search for results.

The system supports three methods of specifying keywords:

- Click + to select the connector, attribute name and operation in “Add Filter Condition”, enter the query content, and click “Add”.


Add Filter Condition

Connector
● and
○ or
□ Negate

Attribute Name
Please Select *

Operation
Please Select

Query Content

Parameter	Description
Connector	Multiple conditions can be connected by connectors "and", "or" or "not”. • and means "and" operation, and the logs that meet all conditions at the same time will be hit. • or means "or" operation, as long as one of the multiple conditions is met, it will be hit. • not represents the negation operation. Search in order from left to right. and has higher priority than or. When you want to perform the or operation first, you can add single brackets outside the conditions for performing the or operation.
Attribute name	Select the condition to filter from the drop-down box.

Parameter	Description
Operation	Select the operation to be performed on the attribute value in the drop-down box. The following describes the operations under all attribute names: • =: Only when the information content is completely consistent with the query content can it be hit. • !=: When the informational content is not equal to the query content, it can be hit. • >, <, >=, <=: When the information content is greater than, less than, greater than or equal to, and less than or equal to query content, it can be hit. • In: The query address needs to be filled in the form of "network number/netmask", and the logs generated by the IP addresses included in the network segment all hit. • Contains: As long as the information content contains the query content, it will be hit. • not empty: Hit if the information content of the specified attribute is not empty.
Query content	Under a specified attribute, the address, value, or content that the user wants to find needs to be satisfied.

Repeat the process to add another conditional keyword. The default connector is "and", which can be set to "or", which can invert the condition keyword. After the settings are complete, click “Close”. After closing the “Add filter conditions” page, the search starts automatically.

- Click to select criteria

In the logs that have been generated, click the log content in one or more attributes, and the system will automatically configure it as a retrieval condition. The default operation between multiple attributes is "and". Click " 🔍" to retrieve logs.

- In the search box, enter a condition that meets the syntax of the conditional rule, and click the "Search" button.

The values do not support single quotes, double quotes, $.

Click 🧹 to clear existing criteria in the search bar.

Add a Disposition Policy by Logging

Step 1. Choose “Log”.

Step 2. Click a log type.

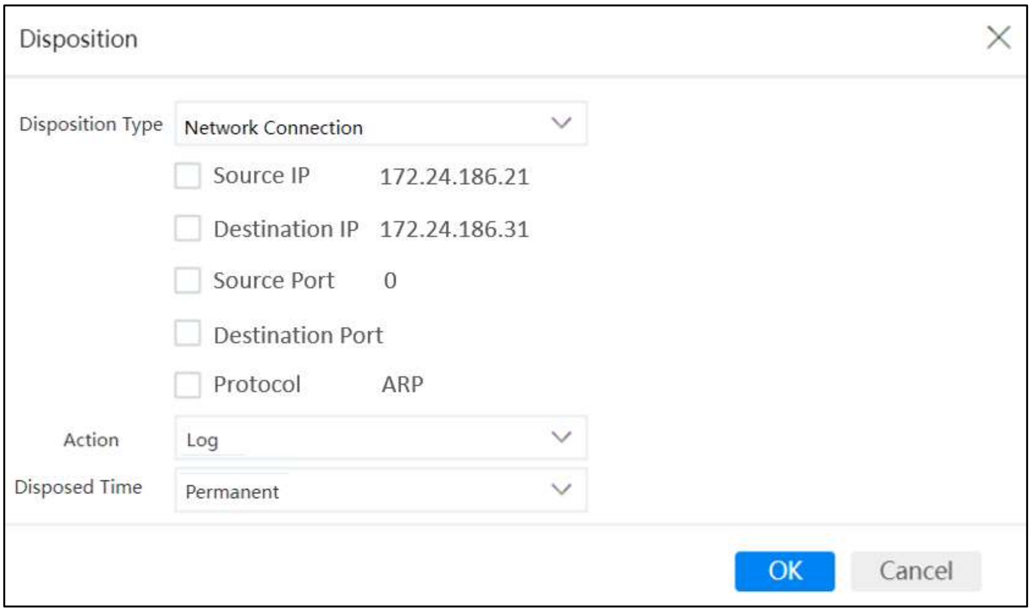
The log types that support log processing include “Traffic Logs”, “Threat Logs”, “Domain Name Logs”, “URL Filtering Logs”, “Email Filtering Logs”, “Content Logs”, “Behavior Logs”, and “Instant Messaging Logs”.

Step 3. Find the desired log, select the” Dispose” button under “Actions”.

Step 4. Configure the disposition type.

Different log types support different disposition types. All disposition types are described below.

- Network connections: check the desired parameters. The parameters include source IP, destination IP, source port, destination port, and protocol, and perform corresponding processing actions on data streams that meet the selected conditions.
- App name: select the application name. Execute the appropriate handling action on the data flow of the application.
- Threat name: check the desired parameters. The parameters include Threat Type and Threat ID. Perform corresponding processing actions on data streams that meet the selected conditions.
- Domain name: select the domain name. Execute the appropriate handling action on the data flow accessing the domain name.
- URL: select URL. Execute the corresponding action on the data flow accessing this URL.
- IM: select the QQ number. Execute the disposal action on the data stream of the QQ.



Disposition

Disposition Type: Network Connection

□ Source IP 172.24.186.21

□ Destination IP 172.24.186.31

□ Source Port 0

□ Destination Port

□ Protocol ARP

Action: Log

Disposed Time: Permanent

Step 5. Configure disposition actions. Disposition actions support "log" and "block".

- "Log", release the packet but record the log.
- "Block", drop packets and record the log.

Step 6. Select the disposal time, that is, the time when the disposal action takes effect.

The disposal time supports "permanent", "90 days", "30 days", "7 days" and "1 day".

Step 7. After the configuration is complete, click “OK”.

After disposal, you can view the corresponding disposal policy under “Disposal > Manual Disposal”. The policy status of "Immediate Disposition " is " Disposed ", and the policy status of "Delay Disposition" is "Undisposed ".

View Log Details

Step 1. Choose “Log”.

Step 2. Click a log type.

The log types that support log processing include Traffic Logs, Threat Logs, Domain Name Logs, URL Filtering Logs, Email Filtering Logs, Content Logs, Behavior Logs, and IM Logs.

Step 3. Find the desired log, and click the "View" button under the operation.

Step 4. View log details.

The log detail parameters are different for each type. Log details include general information, source and destination information, and display related log information.

Step 5. Click “Close”.

Export Log

Step 1. Choose “Log”.

Step 2. Click a log type to enter the corresponding log page.

The supported log types include "traffic log", " threat log", "domain name log", " URL filtering log", " mail filtering log", "content log", "behavior log", "instant messaging log", "Operation Log" and "System Log".

Step 3. (Optional) Log time range and other filter conditions, set the desired logs.

Step 4. Click ⇱ to export the log. Logs are exported to excel format.

If exceeding the maximum export item, it needs to be exported in multiple times.

Download Threat Samples

After the user activates the "Sample Retention" function in the antivirus, vulnerability protection, and anti-spyware configuration files, the threat log will save the threat samples. Users can download samples to view locally. Only firewall devices with hard drives supports the function.

Step 1. Choose “Data Center > Log > Threat Log”.

Step 2. Click ⤓ to download the sample.

Download Content Retention Sample

After the user enables the "Content Retention" function under the content filtering configuration file, the content files that match the keyword filtering rules will be saved in the content log, and can be downloaded to the local for viewing. Only the firewall devices with hard drives supports the function.

Step 1. Choose “Data Center > Log > Content Log”.

Step 2. Click ⤓ to download the content retention sample.

17.2 Log Configuration

Log settings are used to configure functions such as sending logs to the log server and clearing logs.

17.2.1 Log Level Description

The outgoing log level is divided into 8 levels, which are emergency, alarm, serious, error, warning, notification, information, and debugging. The meaning of each level is as follows:

Log Level	Description
Urgent	The system is unavailable
Warning	Events requiring immediate action
Serious	Key event
Error	Error event
Alarm	Alarm event
Notice	Ordinary but important event
Information	Useful information
Debugging	Debug information

17.2.2 Add Log Server

The log server is used to receive firewall logs. Connectivity must be maintained between the firewall and the log server. Users need to specify a static route to the log server on the firewall.

Step 1. Choose “Data Center > Log Configuration > Log Server”.

Step 2. Click “Add”.

Step 3. Configure log server parameters.

Parameter	Description
Server name	Configure the name of the log server.
Server address	Specify the server address for outgoing logs. Both IPv4 and IPv6 addresses are supported.

Parameter	Description
Protocol	Select the protocol for sending logs. The firewall supports using UDP to send logs. The protocol and port must be consistent with the configuration of the log server. Otherwise, the log server will not be able to receive the logs of the firewall.
Type	Select the type of log server. Both "text" and "binary" types are supported.
Port	By default, text type logs use port 514 of the UDP protocol, and binary type logs use port 20000 by default. The protocol and port must be consistent with the configuration of the log server. Otherwise, the log server will not be able to receive the logs of the firewall.

Step 4. After the configuration is complete, click “OK”.

The added server is displayed in the server list. Servers can be edited and deleted.

17.2.3 Add Log Server Group

Multiple log servers in a log server group can implement redundant backup of logs.

Step 1. Choose “Data Center > Log Configuration > Log Server Group”.

Step 2. Click “Add”.

Step 3. Configure log server group parameters.

Parameter	Description
Name	Configure the name of the log server group.
Description	Add description information to help identify and remember this log server group.
Select log server	Select the log server or log server group from the “Optional” box and add it to the “Selected” box as a member of the log server group. You can filter the selectable members by selecting "Log Server" or "Log Server Group", or entering query criteria.

Step 4. After the configuration is complete, click “OK”.

The configured log server group is displayed in the log server group list. You can view the log server's name, members, reference relationship, etc.

Click the “Edit” button under the name link or operation to modify the parameters of the log server group.

17.2.4 Log Outgoing

The log Outgoing function is used for log dumping. Historical logs can be saved by dumping them to the log server. The log outgoing function supports setting log servers for logs of different log types and log levels.

Global Settings

Step 1. Choose “Data Center > Log Configuration > Log Outgoing”.

Step 2. Select “Global Set Conditions”.

- If "All" is selected as the global setting condition, the server or server group used by all log types will be uniformly specified.
- If "Custom" is selected as the global setting condition, click the log text box, select one or more log types to be configured in the optional area box, and specify the server or server group. After specifying completely, the servers in the corresponding list become the specified server or server group.

Step 3. After the configuration is complete, click “Apply”.

Select from List

Step 1. Choose “Data Center > Log Configuration > Log Outgoing”.

Step 2. Set directly in the list of log servers.

Different log servers can be set for different log types and different log levels.

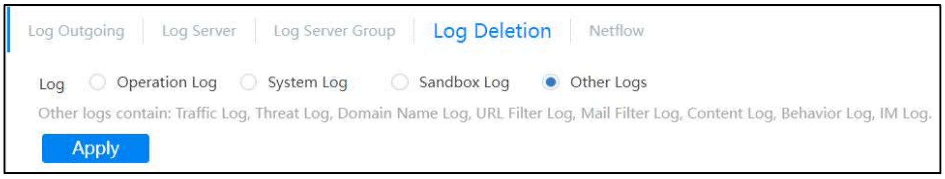
Step 3. After the settings are complete, click “Apply”.

17.2.5 Log Clearing

The historical logs that have been backed up can be cleared through the log clearing function. After the log is cleared, it cannot be recovered. It is recommended that you perform a log backup before clearing the log.

Step 1. Choose “Data Center > Log Configuration > Log Deletion”.

Step 2. Select the desired log type.



Log ○ Operation Log ○ System Log ○ Sandbox Log ● Other Logs

Other logs contain: Traffic Log, Threat Log, Domain Name Log, URL Filter Log, Mail Filter Log, Content Log, Behavior Log, IM Log.

Step 3. Click “Apply”.

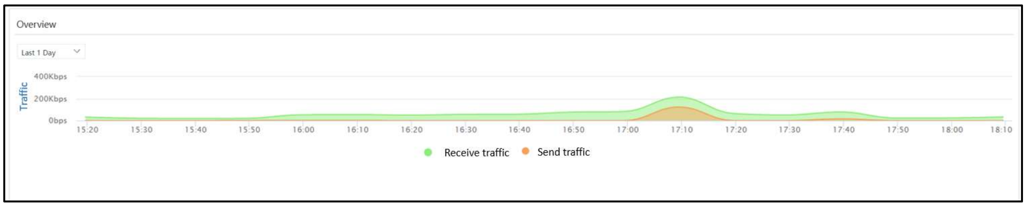
17.3 Statistics

17.3.1 Network Overview

The network overview shows the traffic trend in the network and the source IP, application, and application category that consume the most bandwidth. And perform statistical display on TOP5 threats.

Overview

The overview shows traffic trends for the selected time period. The abscissa is time, and the ordinate is the number of traffic bytes. The overview only shows the trend of total incoming and outgoing traffic.



Overview

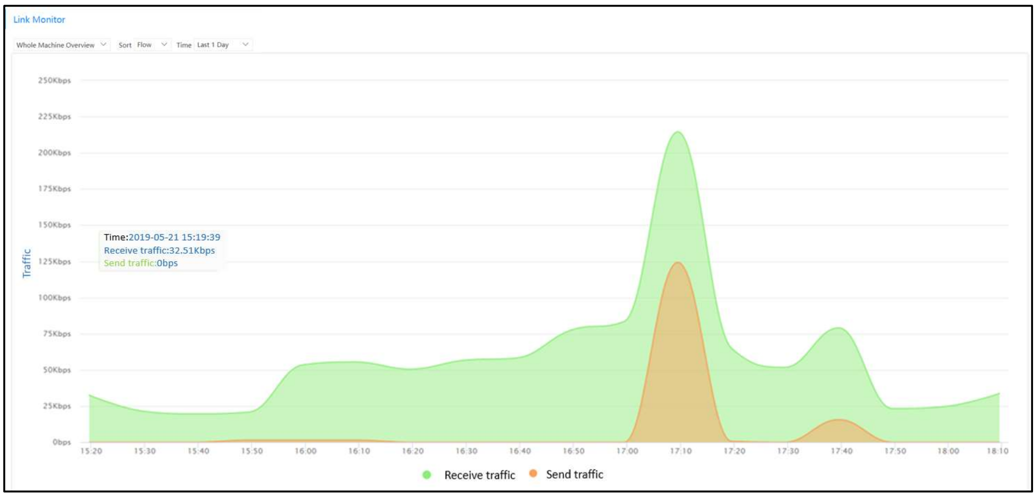
Last 1 Day

Click the time range drop-down box and select a time range from the drop-down list. You can view traffic trends in the last 15 minutes, last 1 hour, last 6 hours, last 12 hours, last 1 day, and last 7 days.

Please pay attention to traffic peaks, traffic troughs and traffic trends. When the traffic has an obviously abnormal peak, you can further check whether there is an attack during this period of time.

Put the mouse on a certain position on the graph, and the time and flow size of the position will be displayed.

To view the trend of receiving traffic, sending traffic, concurrent number, and new creation, you can click "Link Monitor " and choose to view the trends of traffic, concurrent number, and new creation in the overview of the whole machine. You can also view the traffic trend of a single interface under the "Link Monitor" page.



Link Monitor

Whole Machine Overview   Sort Flow   Time Last 1 Day

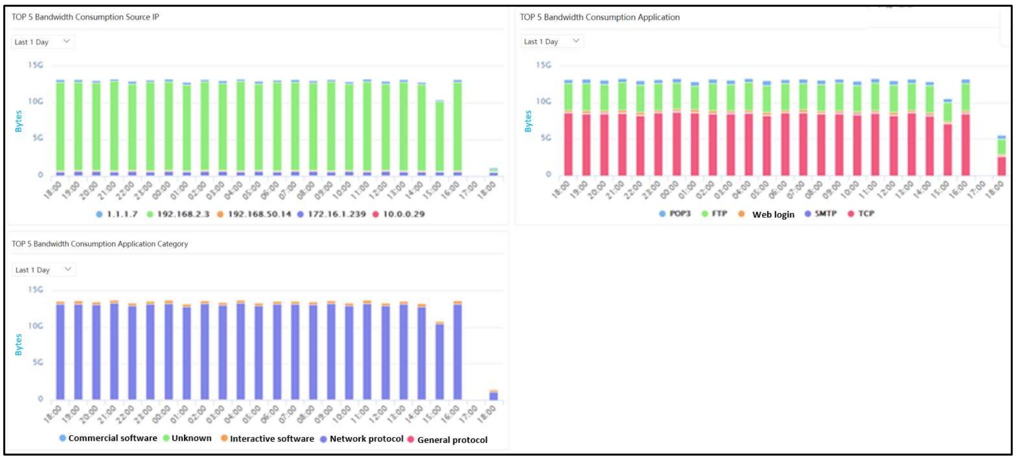
Time:2019-05-21 15:19:39
Receive traffic:32.51Kbps
Send traffic:0bps

TOP5 bandwidth consumption statistics

TOP5 bandwidth consumption statistics include TOP5 bandwidth consumption source IP, TOP5 bandwidth consumption application, TOP bandwidth consumption application classification.

Click the time range drop-down box and select a time range from the drop-down list. The time period supports "last 15 minutes", "last 1 hour", "last 6 hours", "last 12 hours", "last 1 day", and "last 7 days".

Different IPs, applications or application classifications are distinguished by different colors. Click a legend to close or open the area in the graph corresponding to the legend.



TOP 5 Bandwidth Consumption Source IP

Last 1 Day

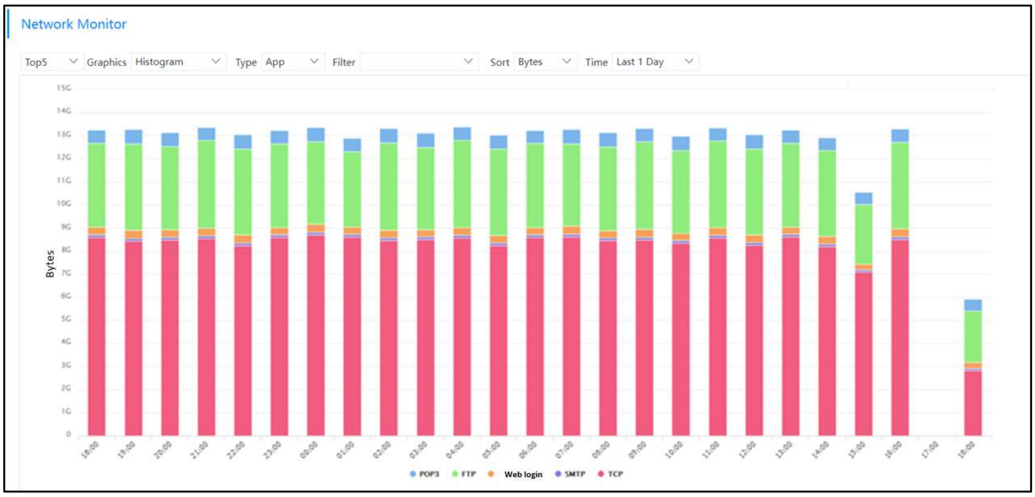
TOP 5 Bandwidth Consumption Application

Last 1 Day

TOP 5 Bandwidth Consumption Application Category

Last 1 Day

Through "Network Monitor", you can view more source IP, application, application classification byte count and session ranking, and you can also view destination IP and user byte count and session ranking. Not only can you view the "TOP5 " objects, but you can also view the statistics or trend graphs of the traffic (bytes) or sessions of the "TOP10 " or "TOP20" objects. You can view the traffic or session status of a single object of a certain type by filtering.

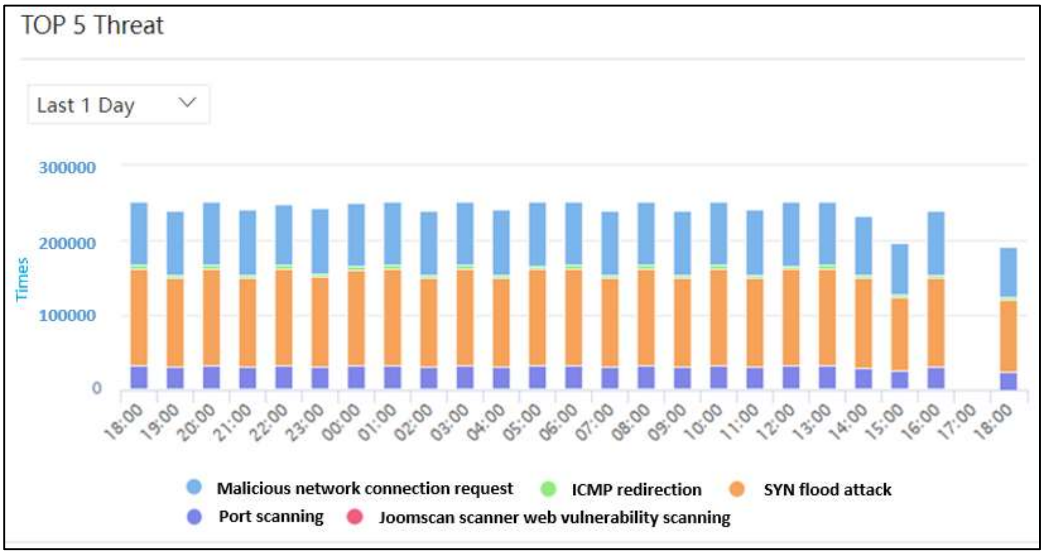


Network Monitor

Top5 Graphics Histogram Type App Filter Sort Bytes Time Last 1 Day

TOP5 Threats

The "Network Overview" shows the statistics of the TOP5 threats for a selected time period.



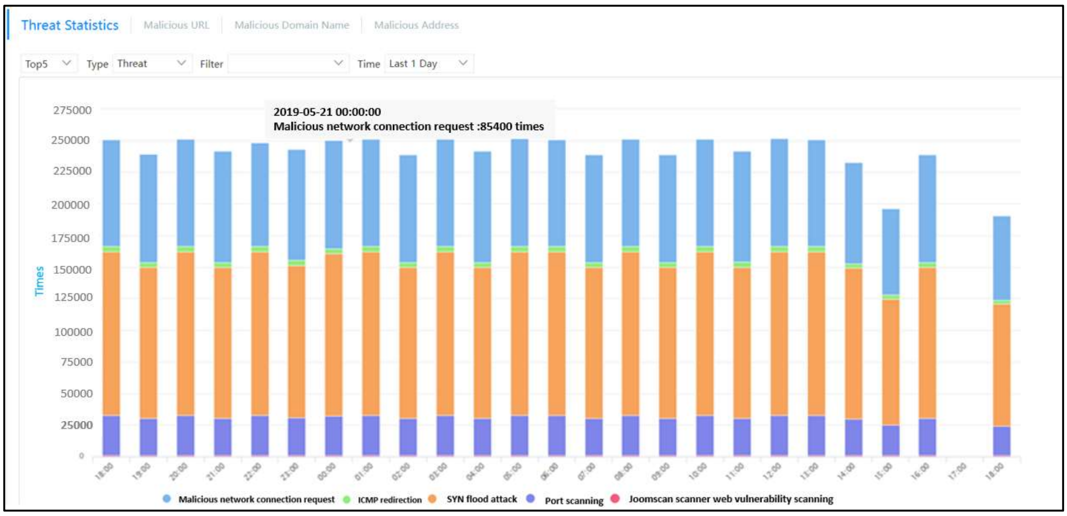
TOP 5 Threat

Last 1 Day

Click the time range drop-down box and select a time range from the drop-down list. You can view the TOP5 threat rankings in the last 15 minutes, last 1 hour, last 6 hours, last 12 hours, last 1 day, and last 7 days. Through the TOP5 threat ranking, users can know the top5 threats currently existing in the network, the names of these threats, and the number of attacks.

Threats are differentiated by colors. Click the legend corresponding to a threat to disable or enable the display of the corresponding application in the graph.

Through the "Threat Statistics" page, you can also view threat statistics graphics based on threat type, threat subcategory, source IP, destination IP and user. For the statistics object, you can also choose "TOP10" or "TOP20".


Top5 Type Threat Filter Time Last 1 Day

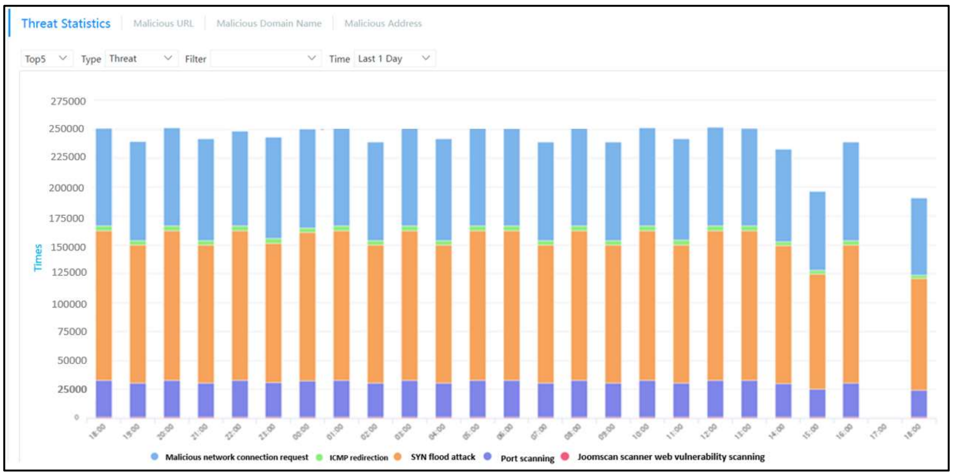
2019-05-21 00:00:00
Malicious network connection request :85400 times

17.3.2 Threat Statistics

Threat Statistics collects statistics on threats in the network. Perform statistics on network traffic based on threat, threat type, threat subcategory, source IP, destination IP, and user, and display TOPN threats, threat type, threat subcategory, source IP, destination IP, and user. Make special statistics on malicious URLs, malicious domain names and malicious addresses.

Threat Statistics Based on Threat Name

Select "Threat" as the type to display the number of occurrences of TOPN threat names within the selected time period.

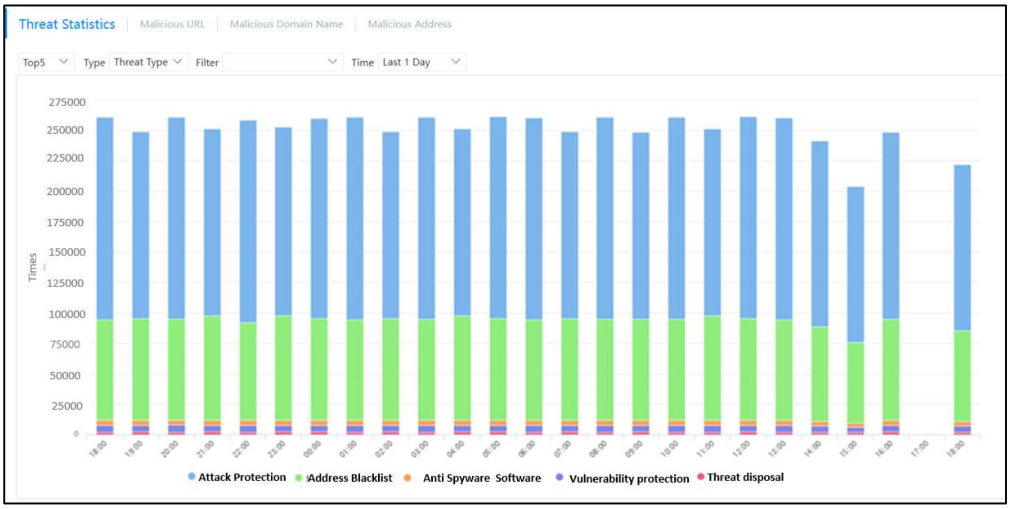

Top5 Type Threat Filter Time Last 1 Day

Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20. The time range for displaying threat statistics can be selected in the last 15 minutes, last 1 hour, last 6 hours, last 12 hours, last 1 day, or last 7 days.

The abscissa of the threat statistics is time, and the ordinate is the number of threats. TOP Threats Displays the top TOPN threats and the number of threats. By setting filter conditions, only the threats and the number of threats of the selected name are displayed.

Threat Statistics Based on Threat Type

Select "Threat Type" as the type to display the number of occurrences of threats under the TOP N threat type within the selected time period.


Top5 Type Threat Type Filter Time Last 1 Day

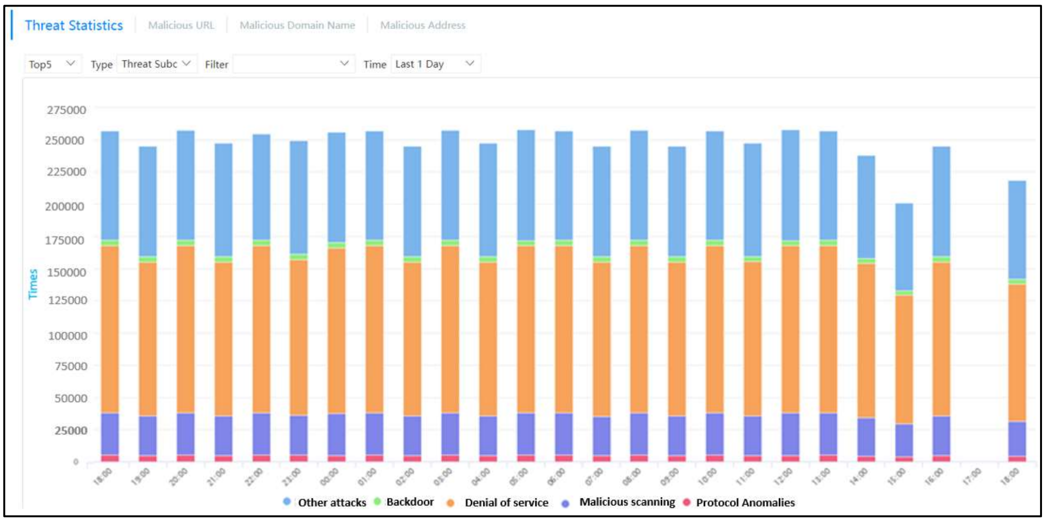
Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

The time range for displaying threat statistics can be selected in the last 15 minutes, last 1 hour, last 6 hours, last 12 hours, last 1 day, or last 7 days.

The abscissa of threat type statistics is time, and the ordinate is the number of threats. TOP Threats displays the top TOPN threat types and the number of threats. You can set filter conditions to display only the threat type and the number of threats of the selected name.

Threat Statistics Based on Threat Subcategories

Select "Threat Subcategory" as the type to display the number of occurrences of threats under the TOPN threat subcategory within the selected time period.



Top5 Type Threat Subc Filter Time Last 1 Day

Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

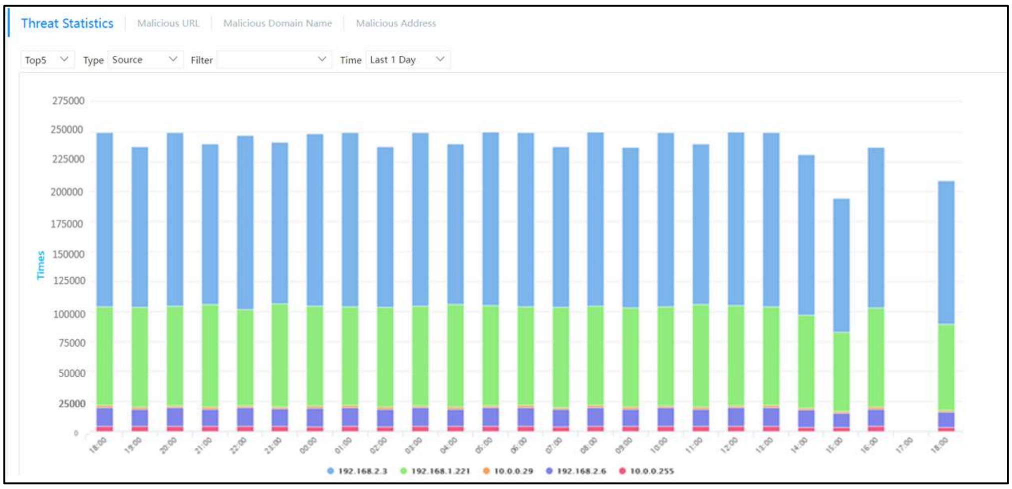
The time range for displaying threat statistics can be selected in the last 15 minutes, last 1 hour, last 6 hours, last 12 hours, last 1 day, or last 7 days.

Threat subcategories include "botnet ", "other attacks", "malicious scanning", "denial of service", "trojan backdoor", "virus worm ", "web attack", "SQL injection", "cross-site scripting", "Malicious Scanning", "Custom Feature", "Protocol Abnormality ", etc.

The abscissa of threat subcategory statistics is time, and the ordinate is the number of threats. TOP threat subcategories displays the top TOPN threat subcategories and the number of threats. You can set filter conditions to display only the threat subcategories and threat times of the selected name.

Threat Statistics Based on Source IP

Select “Source” as the type to display the number of threats in TOPN source IP traffic during the selected time period.



Top5 Type Source Filter Time Last 1 Day

Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

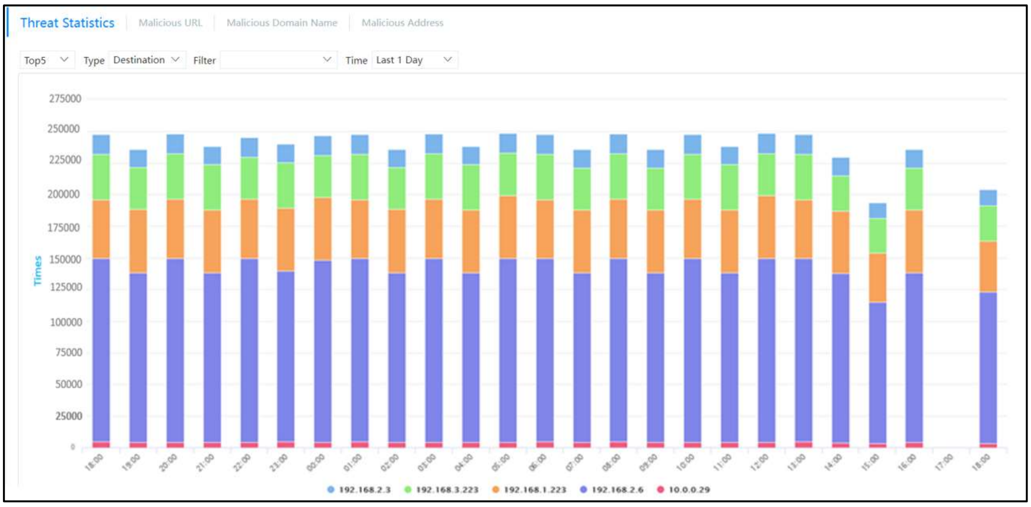
You can set filter conditions to display only the threat statistics of the selected source IP address.

The time range for displaying threat statistics can be selected in the last 15 minutes, last 1 hour, last 6 hours, last 12 hours, last 1 day, or last 7 days.

The abscissa of source IP threat statistics is time, and the ordinate is the number of threats. TOP sources display the top TOPN source IPs and the number of threats.

Threat Statistics Based on Destination IP

Select "Destination" as the type to display the number of threats in TOPN destination IP traffic within the selected time period.



Top5 Type Destination Filter Time Last 1 Day

Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

You can set filter conditions to display only the threat statistics of the selected destination IP address.

The time range for displaying threat statistics can be selected in the last 15 minutes, last 1 hour, last 6 hours, last 12 hours, last 1 day, or last 7 days.

The abscissa of the target IP threat statistics is time, and the ordinate is the number of threats. TOP destinations display the top-ranked TOPN destination IP addresses and the number of threats.

Threat Statistics Based on Users

Select "User" as the type to display the number of threats in the IP traffic of TOPN users within the selected time period.

Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

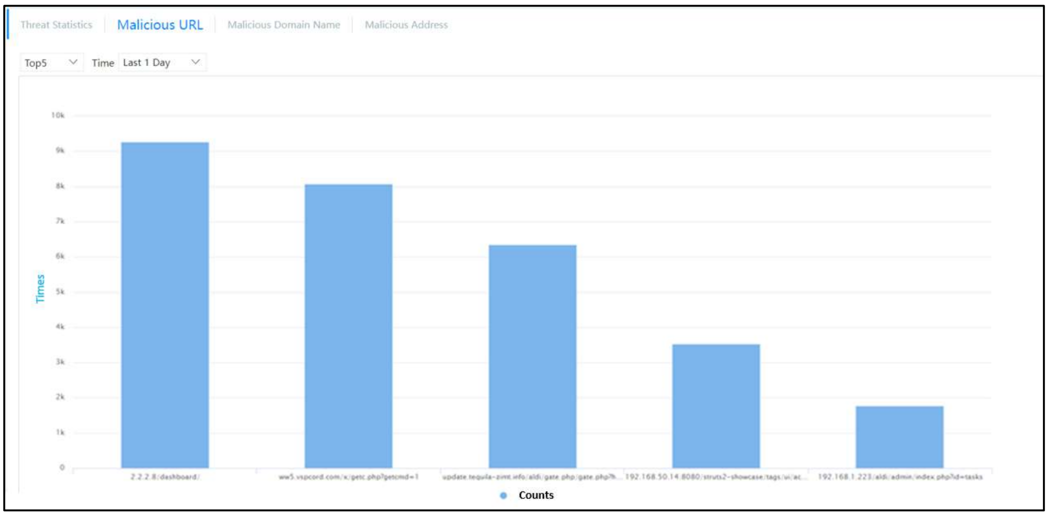
You can set filter conditions to display only the threat statistics of selected users.

The time range for displaying threat statistics can be selected in the last 15 minutes, last 1 hour, last 6 hours, last 12 hours, last 1 day, or last 7 days.

The abscissa of user threat statistics is time, and the ordinate is the number of threats. TOP purpose displays the top TOPN source users and the number of threats.

Malicious URL

Malicious URLs displays the TOP malicious URLs within the selected time period. The statistics of malicious URLs in the network are displayed. The main sources are URLs processed by the processing center, malicious websites, and malicious URLs detected by anti-virus. Users can view malicious URL addresses and access times that are mainly accessed in the network through malicious URL statistics.

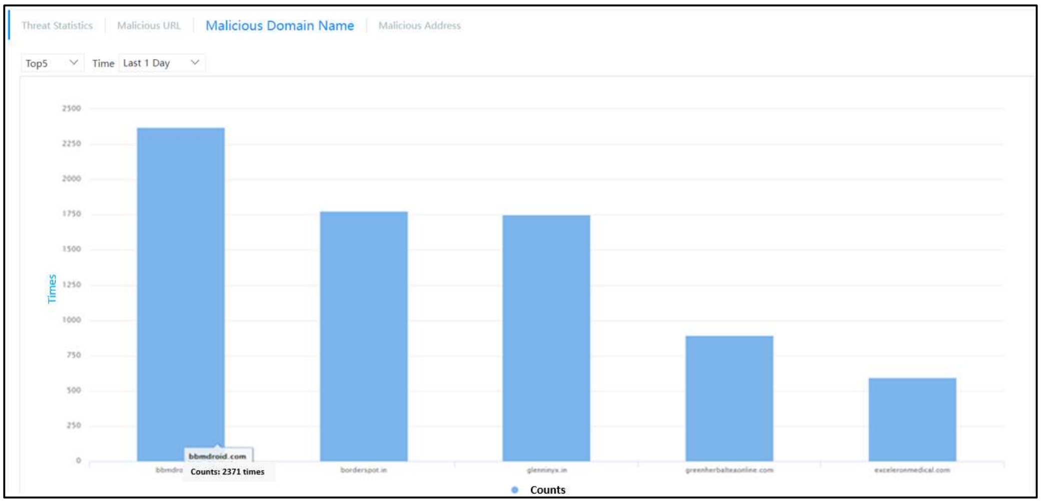

Threat Statistics
Malicious URL
Malicious Domain Name
Malicious Address
Top5
Time
Last 1 Day
Times
10k
9k
8k
7k
6k
5k
4k
3k
2k
1k
0
2.2.2.8/dashboard/
ww5.vspcord.com/x/getc.php?getcmd=1
update.tequila-zimt.info/aldi/gate.php/gate.php?h...
192.168.50.14:8080/struts2-showcase/tags/ui/ac...
192.168.1.223/aldi/admin/index.php?id=tasks
Counts

Through the TOP drop-down box, you can select the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

Through the time drop-down box, you can choose the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

Malicious Domain Name

The statistical display of access to malicious domain names in the network mainly comes from the black domain names recorded in the domain name blacklist and the compromised IOC recorded in the IOC.



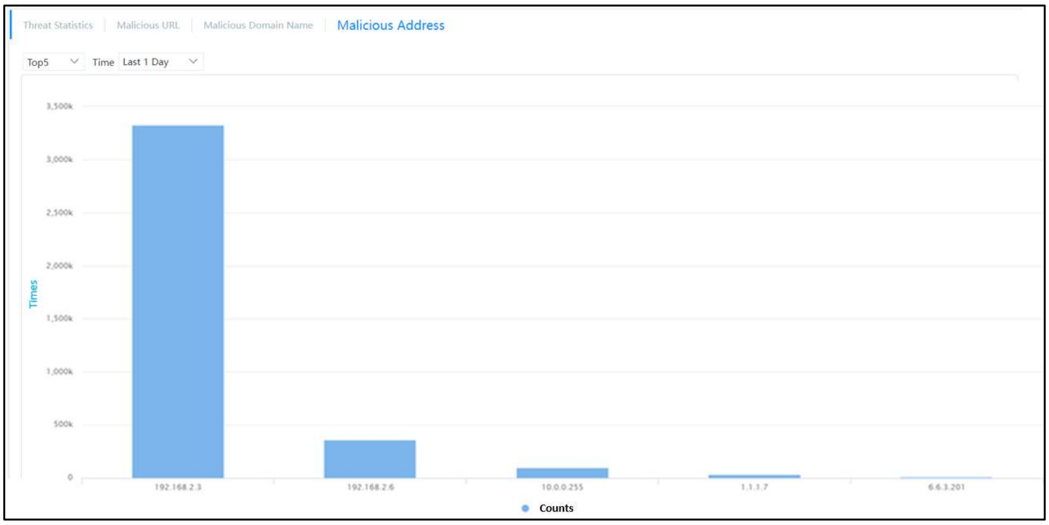
Through the TOP drop-down box, you can select the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

Through the time drop-down box, you can choose the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

Users can view malicious domain names and access times that are mainly accessed in the network through malicious domain name statistics.

Malicious Address

The statistical display of malicious addresses that launched attacks in the network mainly comes from black IPs that have been disposed of by the disposal center, attackers detected by advanced security functions, and so on.



Top5

Time Last 1 Day

Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

Through the time drop-down box, you can choose the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

Users can view the key malicious addresses in the network and the number of attacks launched or the number of accesses to malicious addresses through malicious address statistics.

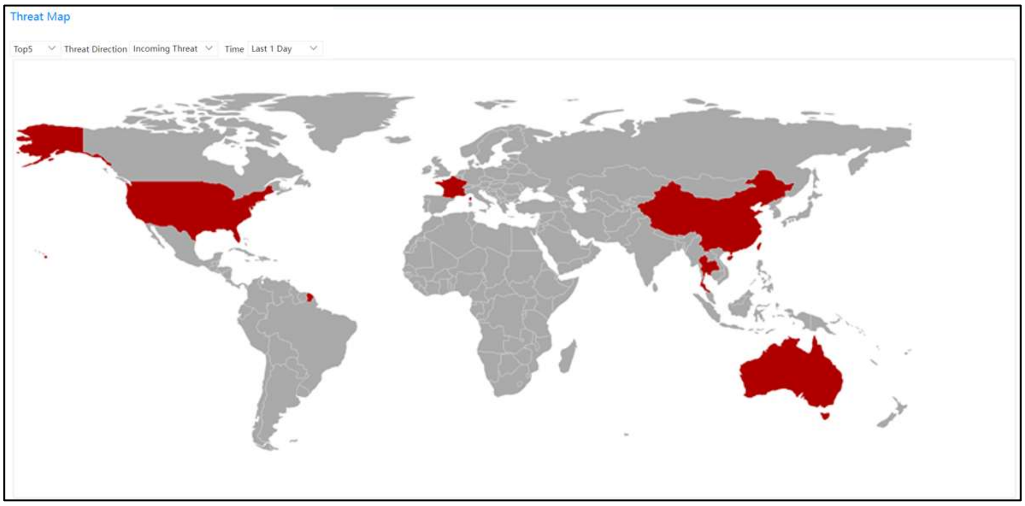
17.3.3 Threat Map

Threat map shows the countries or regions with the most incoming or outgoing threats as a map. Different colors correspond to different risk levels.

Incoming threats refer to attacks on the user's local network from the outside world. Outgoing threats refer to threats initiated by the user 's intranet.

You can choose the number of TOP rankings you want to view, divided into TOP5, TOP10, and TOP20.

The time range for displaying the threat map. You can choose the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.



Threat Map

Top5 Threat Direction Incoming Threat Time Last 1 Day

Place the mouse on a country name in the threat map to display the area.

17.3.4 Network Monitor

Network monitor supports five types of application, application classification, source, destination, and user, and sorts the number of bytes and sessions of the corresponding type within a specified time range, which can be displayed in the form of statistical graphs and trend graphs.

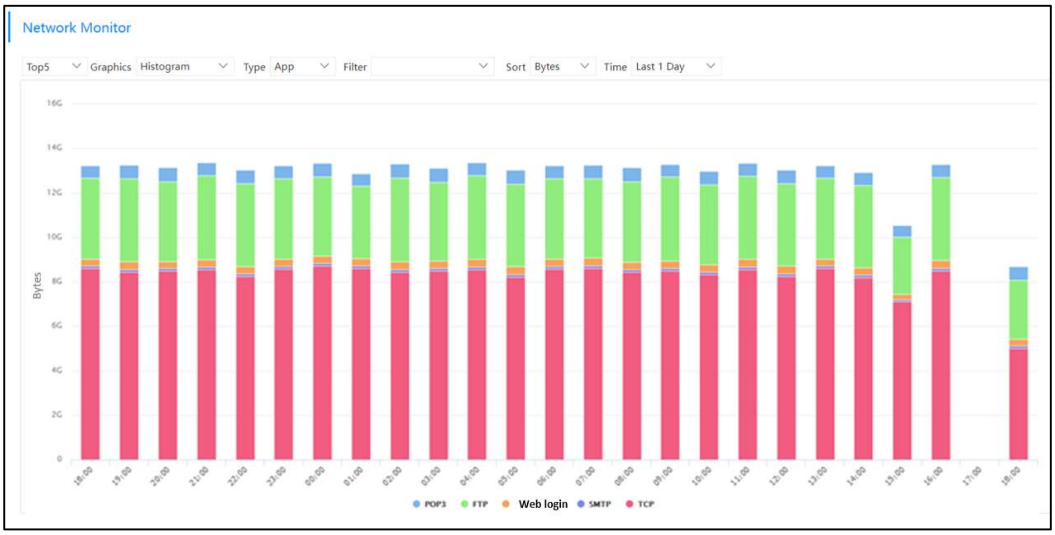
TOP Application Traffic

Select "App" for Type. By setting filter conditions, you can choose to only display the situation of a certain application. Select "Bytes" for sorting.

Through the TOP drop-down box, you can select the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

For graphics, you can choose statistical graphs or trend graphs.

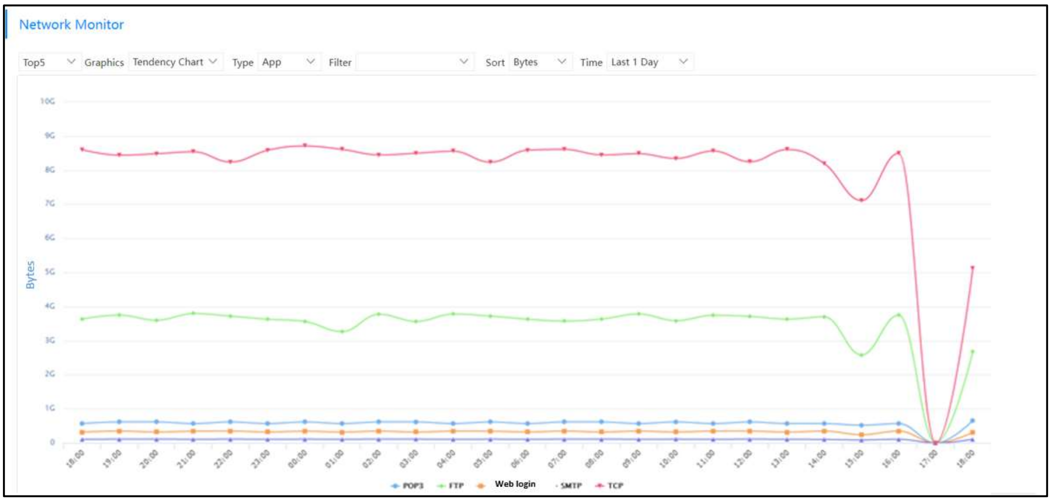
Statistical charts focus on the comparison of the proportion of the target object compared to other objects in the time range.



Network Monitor

Top5 | Graphics Histogram | Type App | Filter | Sort Bytes | Time Last 1 Day

The trend chart focuses on the change trend of the target object within the time range.



Network Monitor

Top5 | Graphics Tendency Chart | Type App | Filter | Sort Bytes | Time Last 1 Day

The time range can be the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

The abscissa of the statistics graph or trend graph is time, and the ordinate is the number of bytes. TOP applications display the top TOPN applications and their byte counts.

TOP Application Classification Traffic

Select "App Classification" for Type. By setting filter conditions, you can choose to only display the situation of a certain application category. Select "Bytes" for sorting.

Application classification includes business software, interactive software, common protocols, multimedia software, network protocols, and unknown types.

Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

For graphics, you can choose statistical graphs or trend graphs. Statistical charts focus on the comparison of the proportion of the target object compared to other objects in the time range. The trend chart focuses on the change trend of the target object within the time range.

The time range can be the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

The abscissa of the statistics graph or trend graph is time, and the ordinate is the number of bytes. TOP App Types displays the TOPN application types and byte counts with the highest byte count.

TOP Source IP Traffic

Select "Source" for Type. By setting filter conditions, you can choose to only display the situation of a certain source IP. Select "Bytes" for sorting.

Through the TOP drop-down box, you can select the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

For graphics, you can choose statistical graphs or trend graphs. Statistical charts focus on the comparison of the proportion of the target object compared to other objects in the time range. The trend chart focuses on the change trend of the target object within the time range.

The time range can be the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

The abscissa of the statistics graph or trend graph is time, and the ordinate is the number of bytes. TOP sources display the top TOPN source IPs and byte counts with the highest byte count.

TOP Destination IP Traffic

Select "Purpose" for Type. By setting filter conditions, you can choose to only display a certain destination IP. Select "Bytes" for sorting.

Through the TOP drop-down box, you can select the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

For graphics, you can choose statistical graphs or trend graphs. Statistical charts focus on the comparison of the proportion of the target object compared to other objects in the time range. The trend chart focuses on the change trend of the target object within the time range.

The time range can be the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

The abscissa of the statistics graph or trend graph is time, and the ordinate is the number of bytes. TOP Destination displays the TOPN destination IPs and byte counts with the highest byte count.

TOP Source User Traffic

Select "User" as the type. By setting filter conditions, you can choose to only display the situation of a certain user. Select "Bytes" for sorting. Select "Bytes" for sorting.

Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

For graphics, you can choose statistical graphs or trend graphs. Statistical charts focus on the comparison of the proportion of the target object compared to other objects in the time range. The trend chart focuses on the change trend of the target object within the time range.

The time range can be the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

The abscissa of the statistics graph or trend graph is time, and the ordinate is the number of bytes. TOP users display the TOPN users and their byte count.

TOP App Sessions

Select "App" for Type. By setting filter conditions, you can choose to only display the situation of a certain application. Sort by selecting "Sessions".

Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

For graphics, you can choose statistical graphs or trend graphs. Statistical charts focus on the comparison of the proportion of the target object compared to other objects in the time range. The trend chart focuses on the change trend of the target object within the time range.

The time range can be the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

The abscissa of the statistics graph or trend graph is time, and the ordinate is the number of sessions. TOP applications display the topN applications and session numbers with the highest number of sessions.

TOP Application Classification Sessions

Select "App Classification" for Type. By setting filter conditions, you can choose to only display the situation of a certain application category. Sort by selecting "Sessions".

When displaying network monitors by application and application type, you can choose to display application categories, including all application categories, business software, interactive software, general protocols, multimedia software, network protocols, and unknown types.

Through the TOP drop-down box, you can select the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

For graphics, you can choose statistical graphs or trend graphs. Statistical charts focus on the comparison of the proportion of the target object compared to other objects in the time range. The trend chart focuses on the change trend of the target object within the time range.

The time range can be the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

The abscissa of the statistics graph or trend graph is time, and the ordinate is the number of bytes. TOP App Types displays the topN application types and session numbers with the highest number of sessions.

TOP source IP sessions

Select "Source" for Type. By setting filter conditions, you can choose to only display the situation of a certain source IP. Sort by selecting "Sessions".

Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

For graphics, you can choose statistical graphs or trend graphs. Statistical charts focus on the comparison of the proportion of the target object compared to other objects in the time range. The trend chart focuses on the change trend of the target object within the time range.

The time range can be the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

The abscissa of the statistics graph or trend graph is time, and the ordinate is the number of bytes. TOP source displays the top N source IPs and session numbers with the highest number of sessions.

TOP Destination IP Sessions

Select "Purpose" for Type. By setting filter conditions, you can choose to only display a certain destination IP. Select "Bytes" for sorting.

Through the TOP drop-down box, you can choose the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

For graphics, you can choose statistical graphs or trend graphs. Statistical charts focus on the comparison of the proportion of the target object compared to other objects in the time range. The trend chart focuses on the change trend of the target object within the time range.

The time range can be the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

The abscissa of the statistics graph or trend graph is time, and the ordinate is the number of bytes. TOP Destination displays the TOPN destination IPs and the number of sessions with the highest number of sessions.

TOP Source User Sessions

Select "User" as the type. By setting filter conditions, you can choose to only display the situation of a certain user. Sort by selecting "Sessions".

Through the TOP drop-down box, you can select the number of TOP rankings to be viewed, which are divided into TOP5, TOP10, and TOP20.

For graphics, you can choose statistical graphs or trend graphs. Statistical charts focus on the comparison of the proportion of the target object compared to other objects in the time range. The trend chart focuses on the change trend of the target object within the time range.

The time range can be the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

The abscissa of the statistics graph or trend graph is time, and the ordinate is the number of bytes. TOP users displays the topN users and the number of sessions with the highest number of sessions.

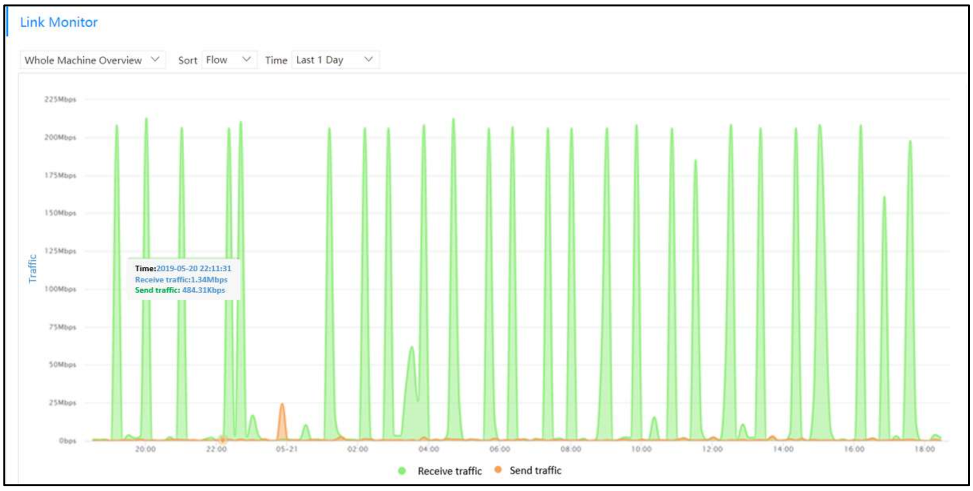
17.3.5 Connection Monitor

The connection monitor displays the traffic of the whole machine or interface, the number of concurrent sessions of the whole machine and the number of new sessions of the whole machine in the network.

Machine Traffic Trend

The abscissa of the machine flow trend graph is time, and the ordinate is flow. The time range displayed by the connection monitor can be real-time, the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

The flow of the whole machine includes two curves, namely the receiving flow and the sending flow. Click the legend below the graph to turn off or turn on the display of the corresponding curve.



Link Monitor

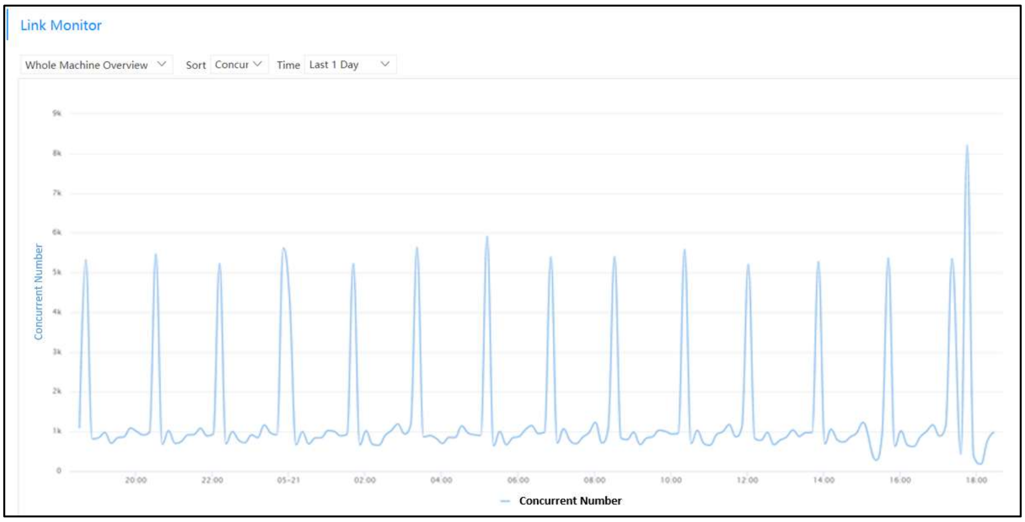
Whole Machine Overview Sort Flow Time Last 1 Day

Time:2019-05-20 22:11:31
Receive traffic:1.34Mbps
Send traffic: 484.31Kbps

Move the mouse to a certain position on the curve to view the corresponding time and flow at that position.

Trend of Concurrent Sessions on the Whole Machine

The abscissa of the concurrent session trend graph of the whole machine is time, and the ordinate is the number of concurrent sessions. The time range displayed by the connection monitor can be real-time, the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.



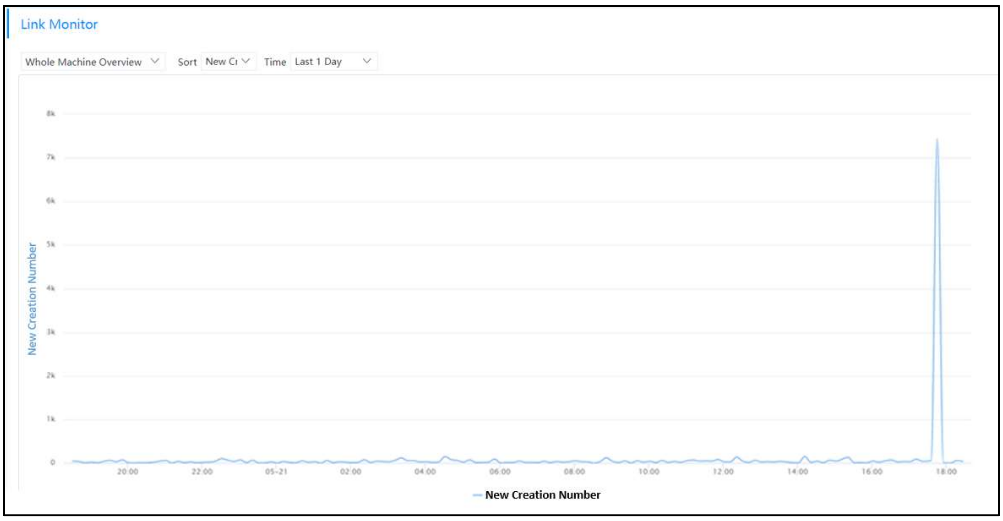
Link Monitor

Whole Machine Overview Sort Concur Time Last 1 Day

Move the mouse to a certain position on the curve to view the corresponding time and number of concurrent sessions at that position.

New Session Trend of the Whole Machine

The abscissa of the new session trend graph of the whole machine is time, and the ordinate is the number of new sessions. The time range displayed by the connection monitor can be real-time, the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.



Link Monitor

Whole Machine Overview Sort New Cr Time Last 1 Day

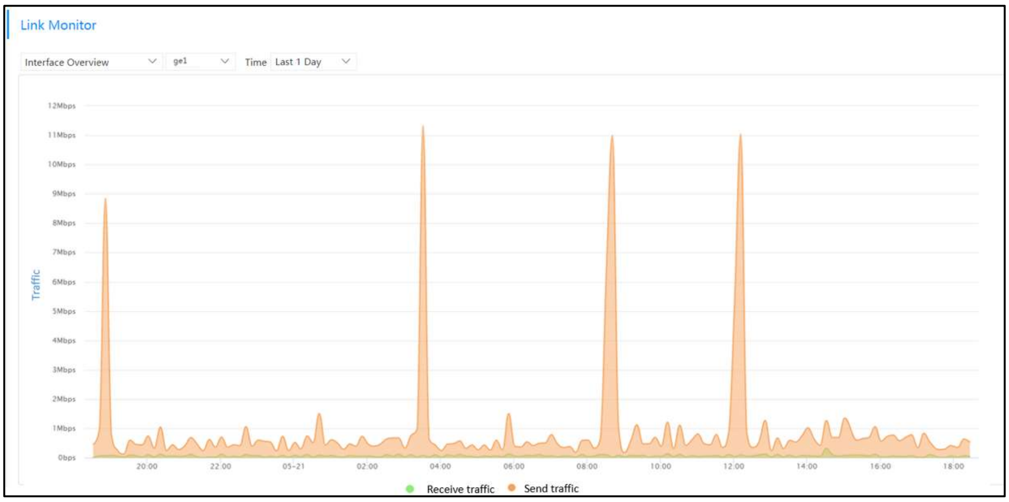
Move the mouse to a certain position on the curve, and you can view the corresponding time and the number of new sessions at that position.

Interface Traffic Trend

The abscissa of the interface traffic trend graph is time, and the ordinate is traffic. The time range displayed by the connection monitor can be real-time, the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, or the last 7 days.

You can choose to view traffic trends for a physical interface. Watch for unusual spikes or lows in traffic trends.

The interface traffic includes two curves, the received traffic and the sent traffic. Click the legend below the graph to turn off or turn on the display of the corresponding curve.



Link Monitor

Interface Overview | ge1 | Time Last 1 Day

Move the mouse to a certain position on the curve to view the corresponding time and flow at that position.

17.3.6 Focus

Key focus is the statistics of key URLs, key applications, and key users. Key users refer to users who access key URLs and key applications.

The key application is set in "Object > Application > App Group", and set the key URL in "Object > URL Category".

Key Users

Key users are automatically generated by the firewall, no need to manually specify.

When there is an address/user accessing the focused URL/focused application in the network, the firewall will record the IP address/user name in the focused user.

When there is a corresponding username for the IP address of the key focused URL/application, it will be recorded in the form of username in the key focused user. If there is no corresponding username for the IP address of the key focused URL/application, it will be recorded in the form of IP address in the key focused user.

Among key users, you can record their internet traffic, internet duration, and number of URL accesses within a specified time range. And it supports sorting by internet traffic, internet duration, and number of URL accesses. You can choose to view the sorting status of TOP5, TOP10, and TOP20.

The displayed time range supports the last 15 minutes, the last 1 hour, the last 6 hours, the last

12 hours, the last 1 day, and the last 7 days.

Key Focused URL Category

Select the desired URL to focus on in "Object > URL Category" in advance. Support focusing on the predefined URL categories and custom URL categories.

The key focused URL classification can record the number of URL accesses within a specified time range, and you can choose to view the ranking of TOP5, TOP10, and TOP20.

The displayed time range supports the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, and the last 7 days.

Key Focused Applications

Users need to select the application they focus on in "Object > Application>App Group" in advance. Predefined applications and custom applications are supported.

Key focused applications can record Internet traffic and Internet time within a specified time range, and you can choose to view the ranking of TOP5, TOP10, and TOP20.

The displayed time range supports the last 15 minutes, the last 1 hour, the last 6 hours, the last 12 hours, the last 1 day, and the last 7 days.

17.3.7 Packet Loss Statistics

The packet loss statistics displays the number of packet loss caused by firewall attack protection. Attack defense is configured under “Policy > Dos Protection > Attack Defense”. Malicious traffic is dropped when the firewall detects a corresponding attack or threat.

17.4 Sessions

The session monitoring list displays the current session information of the firewall. Session monitoring provides a list display based on conditions such as addresses, ports, applications, and bytes, allowing users to monitor the details of the number of sessions on the current firewall and the timeout time in real time. It also provides a filtering function to satisfy the administrator to view the detailed information of the session under certain conditions.

17.4.1 Show Latest Session Information

Click “Refresh” to refresh the current session display.

17.4.2 View Session Monitoring Details

Click “View” under a certain session operation to view the detailed information of the session monitoring.

Detailed information displays the session information from client to server and from server to client. The information includes source IP, destination IP, source port, destination port, source security zone, destination security zone, protocol, application, remaining timeout time, survival time, security Policy, source NAT, destination NAT, traffic, user, authentication server, etc.

Timeout refers to the remaining timeout period of the session. The session is automatically disconnected after it times out.

17.4.3 Disconnect Session

When an abnormality is found in a session, you can click “Disconnect” under the operation of a session to disconnect the session.

Click "Disconnect All" to disconnect all current sessions in the session monitor.

17.4.4 Session Advanced Query

When a user needs to view the current session of a certain user or application, an advanced query can be used to find it.

Advanced query supports specifying session source IP address/range, destination IP address/range, source port number/range, destination port number/range, protocol number/range, source NAT, destination NAT, source security zone, destination security zone, application, security policy, user, and authentication server information to query the specified session.

17.5 Monitor

17.5.1 System Monitoring

CPU usage

Resource monitoring provides a detailed display of CPU usage. Users can view the name and current usage of each CPU core under the multi-core architecture. It is convenient for users to evaluate the performance usage of the firewall.

Fan Status

Resource monitoring provides fan status display. According to the number of fans, the fan speeds are displayed one by one.

17.5.2 Session Limit Monitoring

After the session limit function is configured, the user can view the statistics of hit rules in the session limit statistics menu. According to the three directions of the security zone, it is divided into bi-directional statistics, egress statistics, and ingress statistics.

Parameter	Description
IP address	The IP address for session limit statistics.
Quantity	The number of sessions corresponding to the IP address is displayed.
Rule name	The name of the session restriction rule that is hit.

18 Analysis Center

18.1 Overview

The analysis center visually displays the network situation in the form of graphs through comprehensive analysis of firewall logs. By viewing the charts in the analysis center, it is convenient for users to find abnormalities in the network and make reasonable adjustments to the policy.

Analysis Center supports predefined analysis activities and custom analysis activities. The custom function allows users to customize the dimensions of concern to meet the individual needs of users.

Predefined analysis activities include:

- Network activity

  Network activities are used to display the daily activities of the protected network, including which applications are mainly used in the traffic, which active source users, destination users, source IPs, destination IPs, which countries/regions these users or IPs belong to, and which traffic mainly Which policies are matched.

- Threat activity

  Threat activity analyzes threat logs to display threats that need to be focused on or activities with high threat potential in network activities. The content includes detected threat activities, hosts accessing malicious URLs, hosts requesting malicious domain names, non-standard port applications, and policies allowing non-standard port applications.

- Block activity

  Blocking activities focus on blocked activities in network activities, including blocked applications, blocked user activities, blocked threats, blocked content, blocked domain names, blocked URLs, and policy blocked activities.

18.2 Instructions

By default, the analysis center analyzes all logs within the time range set by the user and displays them in charts.

18.2.1 Set Analysis Time Period

Click the time drop-down box on the left side of the page to select a time period or a custom time period. Custom time requires the user to set the start time and end time of the logs to be viewed.

18.2.2 Set Global Filter Criteria

Global filtering is to filter the entire analysis center.

Step 1. Click the filter condition drop-down box on the left side of the page, and select the filter parameter to be added in the drop-down menu.

Step 2. Click the "Add" button to add a filter item for this filter parameter.

Step 3. Set the value and operator of the filter parameters to be queried.

Select from the drop-down menu or enter the desired value in the drop-down box. Firewall supports adding filter conditions from graph and list. When the area box is set to "Global Query", click the corresponding area in the graph or list, and add a global filter condition in the corresponding global search.

The equal sign on the right side of the item means to filter out the items that match the value. Click the equal sign and set it to an inequality sign, which means to filter out all items that do not meet the value.

Step 4. Repeat the above operations to add new filter conditions.

There is an "and" relationship between multiple filter conditions, and only traffic that meets multiple filter conditions will be filtered out and displayed. Multiple filter parameters under one filter condition are in an "or" relationship, and all traffic that hits one of the filter parameters will be filtered and displayed.

Step 5. Click the " Delete " or "Select All" button to edit the filter conditions.

Step 6. Click “Search” to perform global filtering.

18.2.3 Set Private Filtering Conditions

A private filtering condition is only valid for the area box where the private filtering condition is located.

Firewall supports adding private filter conditions from graph and list. Click "Local Query", the filter conditions added from the chart are added to the private filter conditions, and the number next to "Local Query" shows the number of private filter conditions.

Click ✎ to manually add private filter conditions.

18.2.4 Check Corresponding Log

Click the "Jump" button, select a log, and jump to the corresponding log page. If filter conditions are set, the log page will only display logs that meet the filter conditions.

18.2.5 Minimize Area Box

Click ⊟ to minimize the frame of the area that does not need attention temporarily.

18.3 Network Activity

Network activity counts the vital bytes (traffic) and sessions on the firewall and displays them in visual charts, so that users can grasp which applications, source users, destination users, source IPs, and destination IPs are mainly responsible for the traffic and sessions, Source Country/Region, Destination Country /Region, Policies Occupied. Combined with the actual situation of your own network, you can see whether there is any abnormality in the use of traffic and session numbers.

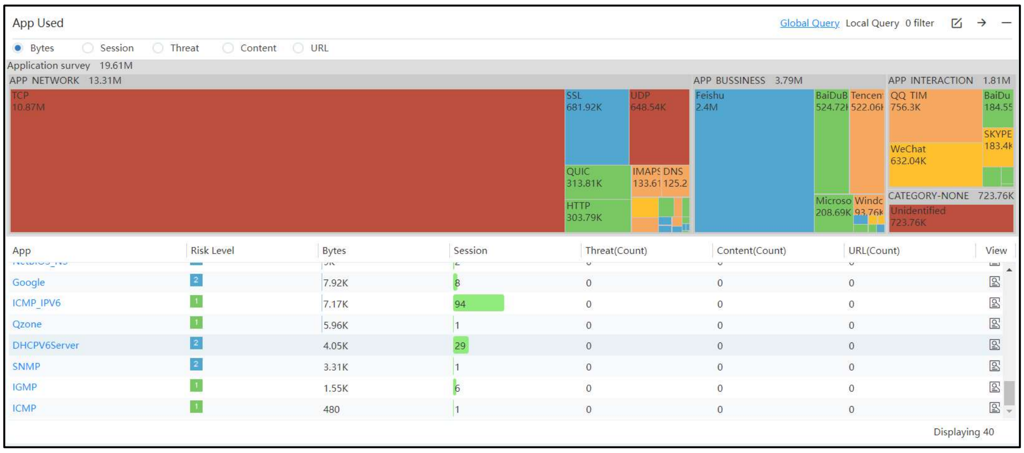
Network activities also collect statistics on threats, content, and URLs to see which applications, source users, destination users, source IPs, destination IPs, source countries /regions, destination countries /regions, number of threats hit by policies, times of malicious content, and malicious URLs most times. Analyze and deal with these abnormal users or IPs.

Application, source user, destination user, source IP, destination IP, source country /region, destination country /region, and policy are interrelated to help discover and locate anomalies. For example, click an application that may be abnormal in the "Application Usage" graph or table, add global filter conditions, and view the source user, destination user, source IP, destination IP, and source country/region corresponding to the abnormal application through global search, destination country, and policy. Similarly, click the source user, destination user, source IP, destination IP, source country/region, destination country/region or policy that may be abnormal to view other corresponding parameters.

18.3.1 Application Use

Bytes

The application bytes use a rectangular tree diagram to display the application type and the number of bytes occupied by the specific application. The larger the area occupied in the rectangular tree diagram, the larger the type of application or the number of bytes occupied by the application. The color of the fields matches the color of the application's risk class. The risk level is divided into 5 levels, from green to red, and the risk is small to large. For applications with a small area, the application name and value cannot be seen clearly. Put the mouse on the corresponding area to view the corresponding parameter name and byte count in this area.



App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
Google	2	7.92K	8	0	0	0	
ICMP_IPV6	1	7.17K	94	0	0	0	
Qzone	1	5.96K	1	0	0	0	
DHCPV6Server	2	4.05K	29	0	0	0	
SNMP	2	3.31K	1	0	0	0	
IGMP	1	1.55K	6	0	0	0	
ICMP	1	480	1	0	0	0	

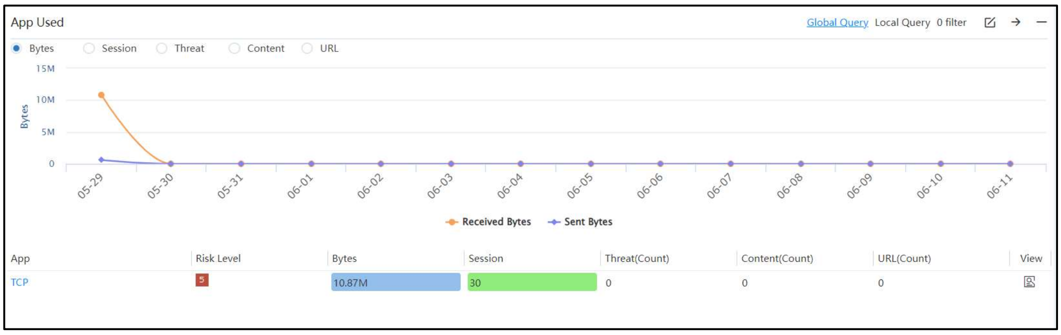
Displaying 40

The application list displays the application name, risk level, byte count, session, threat, content, URL, etc. When displaying the number of bytes, the applications in the list are displayed in descending order of the number of bytes and from top to bottom.

Click “View” to view the rule description of the application in the application identification library. Applications of unknown categories cannot view rule descriptions.

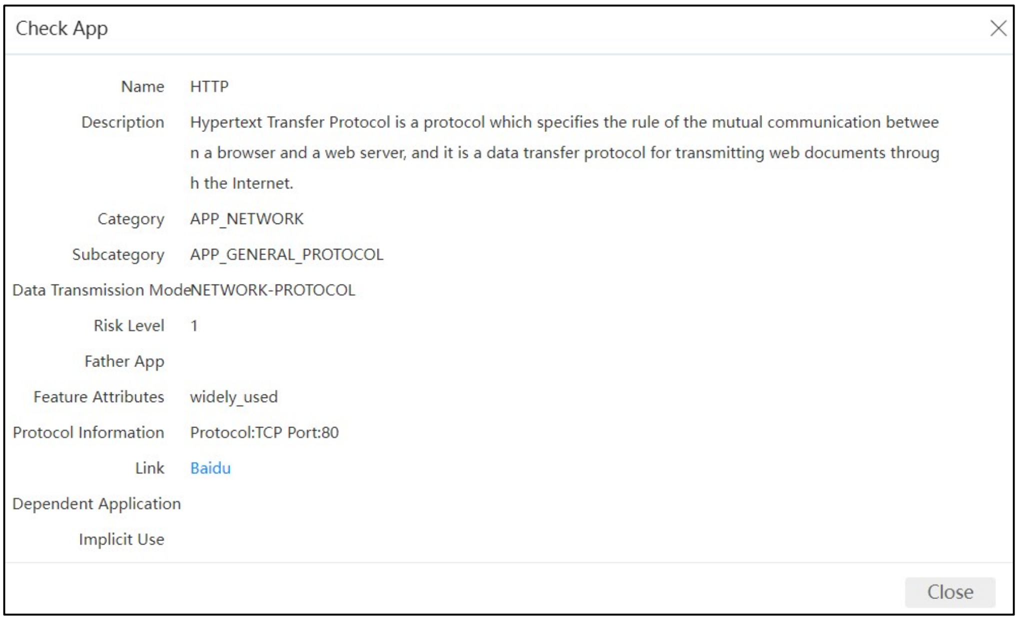
Click an area in the graph or click an application in the table to add that application to the filter criteria.

The abscissa of the searched graph is time, and the ordinate is the number of bytes. Through this graph, you can check whether the traffic distribution in time is normal.



App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
TCP	5	10.87M	30	0	0	0	

After the global search, the corresponding parameters of other area boxes also change. It can be seen that the source user, destination user, source IP, destination IP, source country /region, destination country/region and policy corresponding to the application.

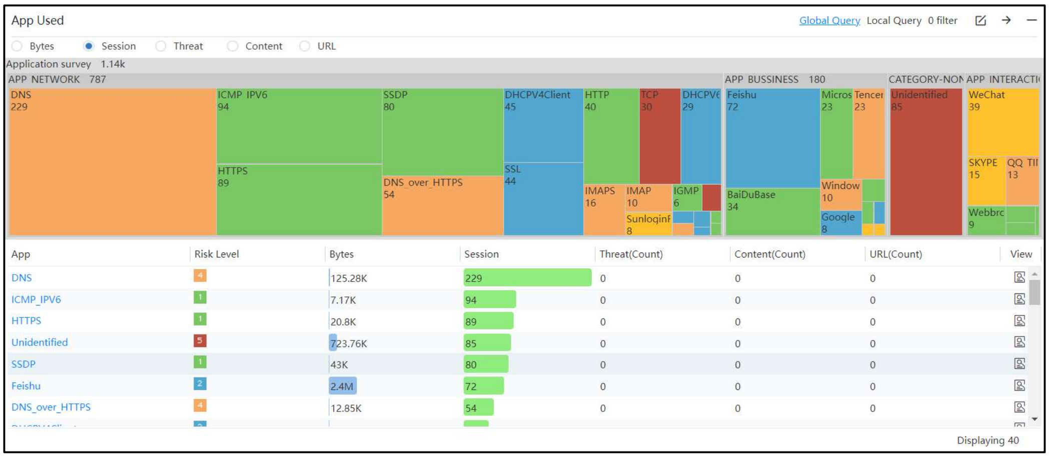


Check App

Name	HTTP
Description	Hypertext Transfer Protocol is a protocol which specifies the rule of the mutual communication between a browser and a web server, and it is a data transfer protocol for transmitting web documents through the Internet.
Category	APP_NETWORK
Subcategory	APP_GENERAL_PROTOCOL
Data Transmission Mode	NETWORK-PROTOCOL
Risk Level	1
Father App	
Feature Attributes	widely_used
Protocol Information	Protocol:TCP Port:80
Link	Baidu
Dependent Application	
Implicit Use	

Sessions

Application sessions shows the application type and the number of sessions occupied by specific applications in a rectangular tree diagram. The larger the occupied area in the rectangular tree diagram, the larger the application type or the number of sessions occupied by the application. The color of the fields matches the color of the application's risk class. The risk level is divided into 5 levels, from green to red, and the risk is small to large. For applications with a small area, the application name and value cannot be seen clearly. Put the mouse on the corresponding area to view the corresponding parameter name and session number in this area.



App Used

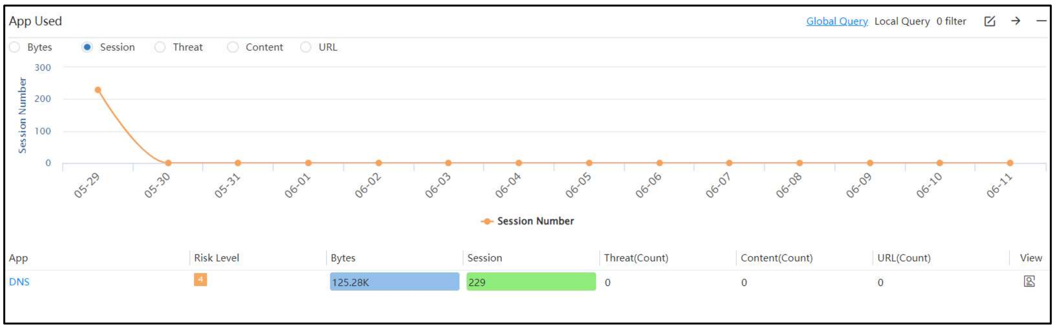
App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
DNS	4	125.28K	229	0	0	0	
ICMP_IPV6	1	7.17K	94	0	0	0	
HTTPS	1	20.8K	89	0	0	0	
Unidentified	5	723.76K	85	0	0	0	
SSDP	1	43K	80	0	0	0	
Feishu	2	2.4M	72	0	0	0	
DNS_over_HTTPS	4	12.85K	54	0	0	0	

Displaying 40

In the application list, the applications are displayed in order of session number from large to small, and from top to bottom.

Click an area in the graph or click an application in the table to add that application to the filter criteria.

The abscissa of the searched graph is time, and the ordinate is the number of sessions. Through this graph, you can see whether the distribution of the number of sessions over time is normal.

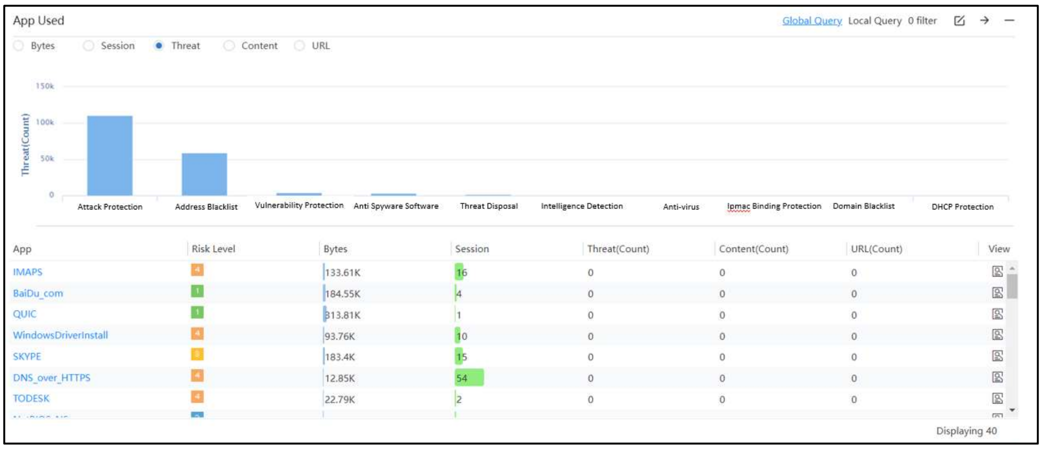


App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
DNS	4	125.28K	229	0	0	0	

After the global search, the corresponding parameters of other area boxes also change. It can be seen that the source user, destination user, source IP, destination IP, source country /region, destination country/region and policy corresponding to the application.

Threats

Application threats displays the number of logs of different threat types in the threat log in a histogram. Threat Type is the threat type of the threat log. Columns are arranged in descending order from largest to smallest, left to right.

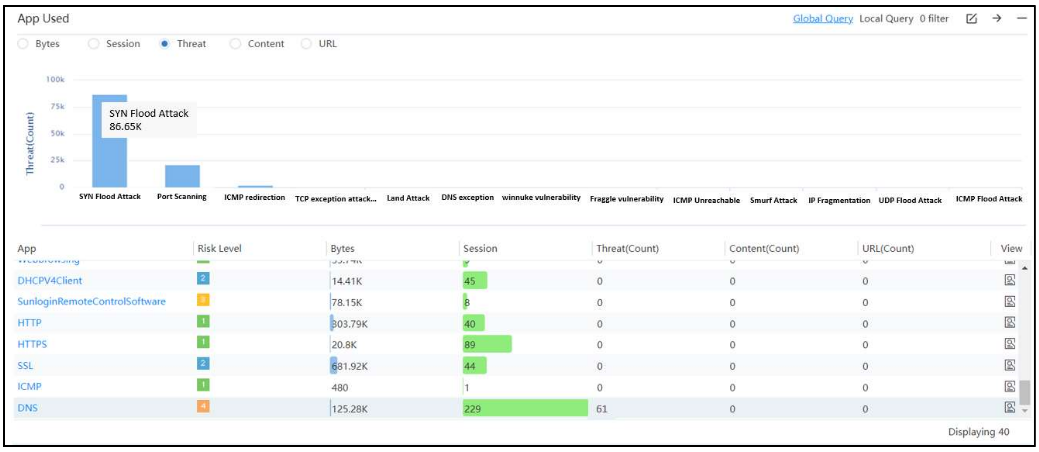


App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
IMAPS	4	133.61K	16	0	0	0	
BaiDu_com	1	184.55K	4	0	0	0	
QUIC	1	313.81K	1	0	0	0	
WindowsDriverInstall	4	93.76K	10	0	0	0	
SKYPE	3	183.4K	15	0	0	0	
DNS_over_HTTPS	4	12.85K	54	0	0	0	
TODESK	4	22.79K	2	0	0	0	

Displaying 40

The applications in the application list are displayed in descending order of the number of threats and from top to bottom.

Click the column corresponding to a threat type in the figure to add the threat type to the filter condition. After searching, the figure shows which threats exist under this threat type and the number of threats, and the content in the table changes accordingly.



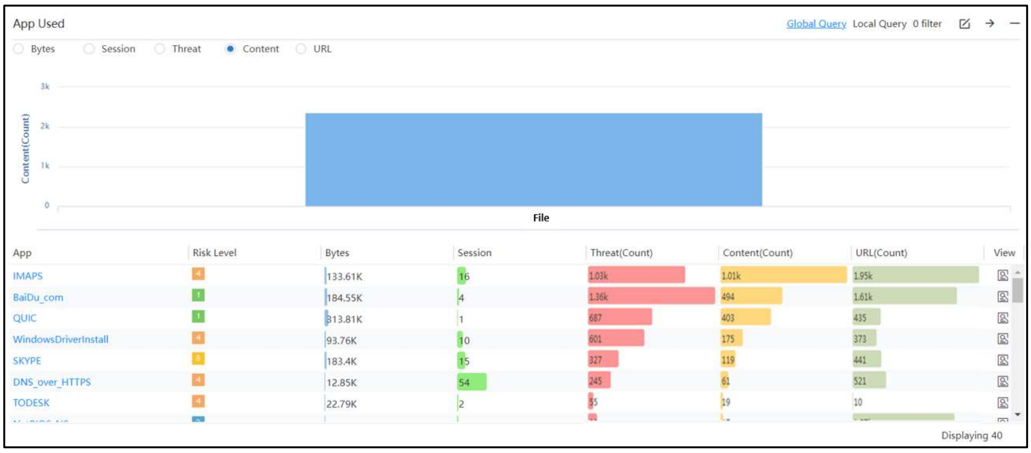
App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
DHCPV4Client	2	14.41K	45	0	0	0	
SunloginRemoteControlSoftware	3	78.15K	8	0	0	0	
HTTP	1	303.79K	40	0	0	0	
HTTPS	1	20.8K	89	0	0	0	
SSL	2	681.92K	44	0	0	0	
ICMP	1	480	1	0	0	0	
DNS	4	125.28K	229	61	0	0	

Displaying 40

After the global search, the corresponding parameters of other area boxes also change. It can be seen that the threat corresponds to the application, source user, destination user, source IP, destination IP, source country/region, destination country /region, and policy.

Content

The application content displays the number of logs for file filtering and content filtering in a histogram. Columns are arranged in descending order from largest to smallest, left to right.

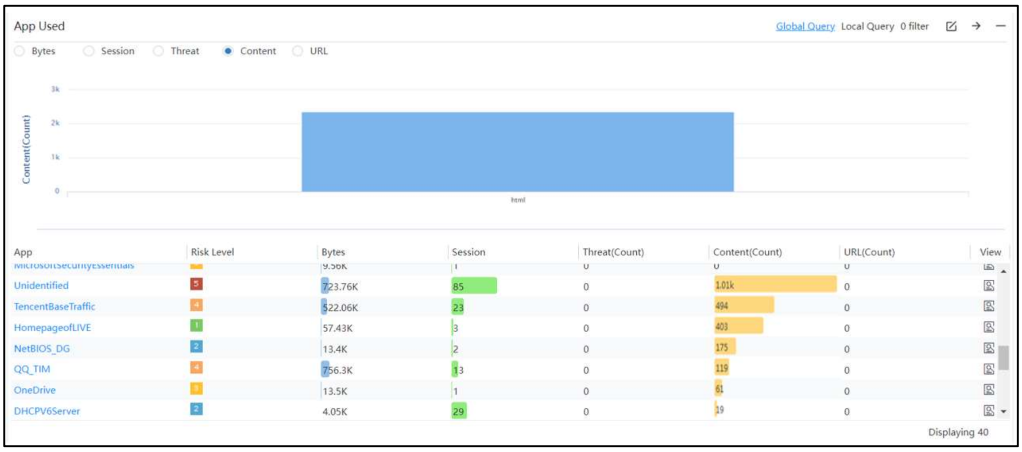


App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
IMAPS	4	133.61K	16	1.03k	1.01k	1.95k	
BaiDu_com	1	184.55K	4	1.36k	494	1.61k	
QUIC	1	313.81K	1	687	403	435	
WindowsDriverInstall	4	93.76K	10	601	175	373	
SKYPE	3	183.4K	15	327	119	441	
DNS_over_HTTPS	4	12.85K	54	245	61	521	
TODESK	4	22.79K	2	55	19	10	

Displaying 40

The applications in the application list are displayed in descending order according to the number of contents, from the largest to the smallest, and from top to bottom.

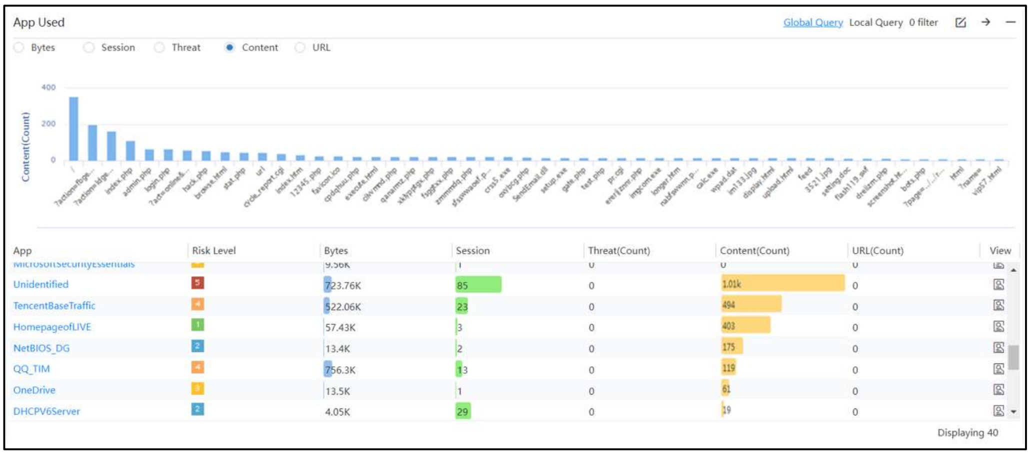
Click the column corresponding to "File" or "Content" to add "File" or "Content" to the filter condition. After searching, the figure shows the number of contents of different file types, and the contents in the table change accordingly.



App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
MicrosoftSecurityEssentials	[illegible]	9.56K	1	0	0	0	
Unidentified	5	723.76K	85	0	1.01k	0	
TencentBaseTraffic	4	522.06K	23	0	494	0	
HomepageofLIVE	1	57.43K	3	0	403	0	
NetBIOS_DG	2	13.4K	2	0	175	0	
QQ_TIM	4	756.3K	13	0	119	0	
OneDrive	3	13.5K	1	0	61	0	
DHCPV6Server	2	4.05K	29	0	19	0	

Displaying 40

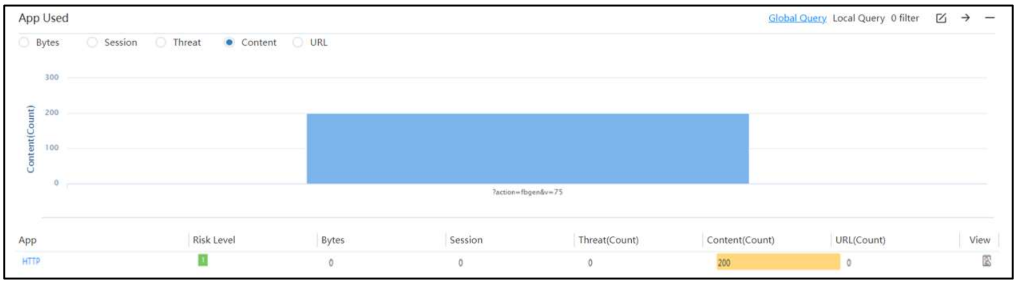
Click the column corresponding to a "file type" to add " file " or "content" to the filter condition. After searching, the number of contents of different file names is displayed in the figure, and the contents in the table also change accordingly.



App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
MicrosoftSecurityEssentials	[illegible]	9.56K	1	0	0	0	
Unidentified	5	723.76K	85	0	1.01k	0	
TencentBaseTraffic	4	522.06K	23	0	494	0	
HomepageofLIVE	1	57.43K	3	0	403	0	
NetBIOS_DG	2	13.4K	2	0	175	0	
QQ_TIM	4	756.3K	13	0	119	0	
OneDrive	3	13.5K	1	0	61	0	
DHCPV6Server	2	4.05K	29	0	19	0	

Displaying 40

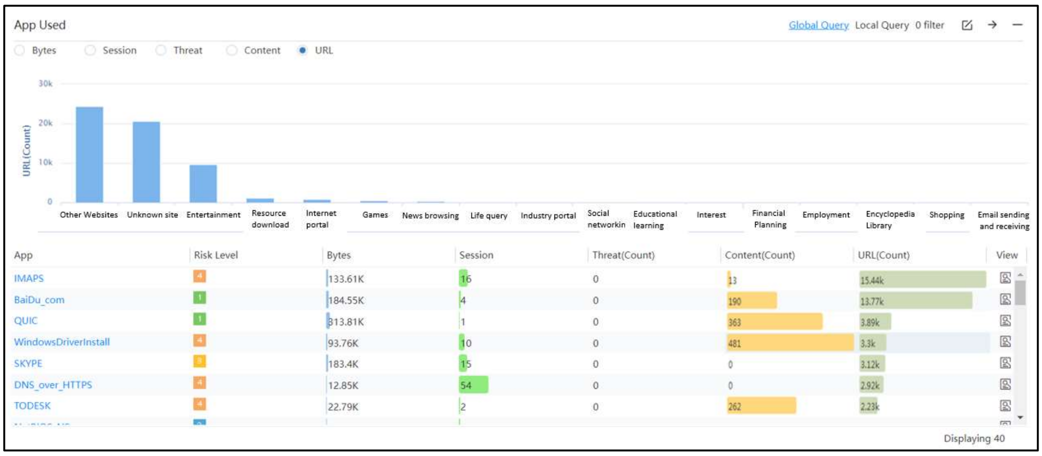
Click the column corresponding to a "file" to add "file name" to the filter condition. After searching, the number of contents of the file is displayed in the figure, and the contents in the table also change accordingly.



App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
HTTP	1	0	0	0	200	0	

URL

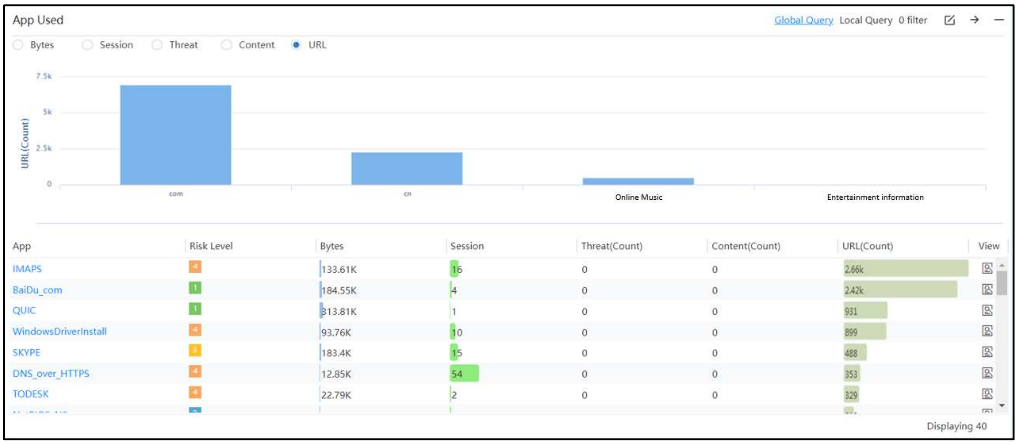
Application URL displays the number of logs classified by URL in a histogram. URL categories are divided into URL libraries and custom URL categories. Columns are arranged in descending order from largest to smallest, left to right.



App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
IMAPS	4	133.61K	16	0	13	15.44k	
BaiDu_com	1	184.55K	4	0	190	13.77k	
QUIC	1	313.81K	1	0	363	3.89k	
WindowsDriverInstall	4	93.76K	10	0	481	3.3k	
SKYPE	3	183.4K	15	0	0	3.12k	
DNS_over_HTTPS	4	12.85K	54	0	0	2.92k	
TODESK	4	22.79K	2	0	262	2.23k	

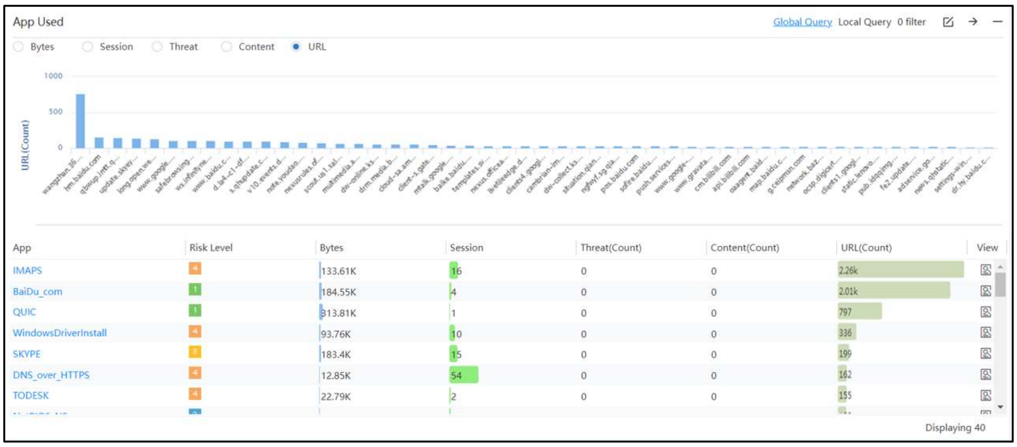
In the application list, the applications are displayed in order of URL number from large to small, and from top to bottom.

Click the bar corresponding to a URL category to add the URL category to the filter condition. After searching, the figure shows the number of URL logs of different URL subcategories, and the content in the table changes accordingly.



App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
IMAPS	4	133.61K	16	0	0	2.66k	
BaiDu_com	1	184.55K	4	0	0	2.42k	
QUIC	1	313.81K	1	0	0	931	
WindowsDriverInstall	4	93.76K	10	0	0	899	
SKYPE	3	183.4K	15	0	0	488	
DNS_over_HTTPS	4	12.85K	54	0	0	353	
TODESK	4	22.79K	2	0	0	329	

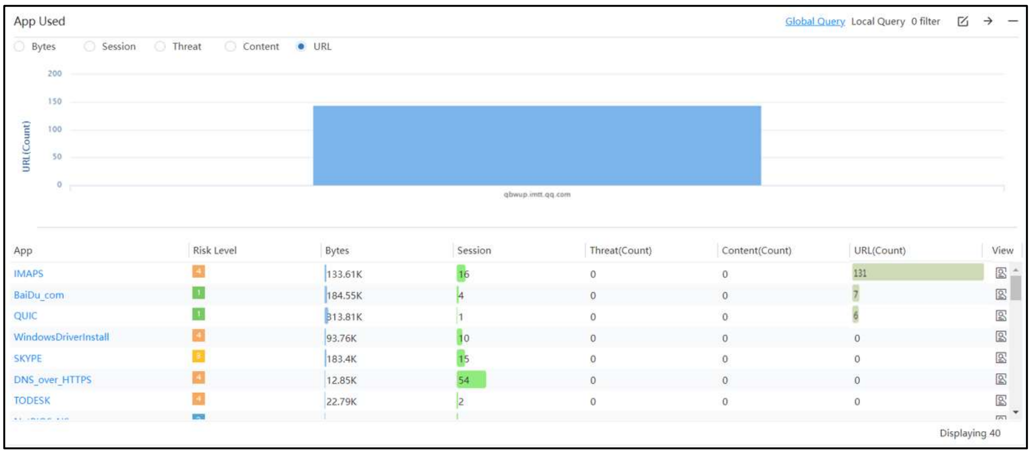
Click the bar corresponding to a URL subcategory to add the URL subcategory to the filter condition. After searching, the figure shows the number of URL logs of different URLs, and the content in the table changes accordingly.



App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
IMAPS	4	133.61K	16	0	0	2.26k	
BaiDu_com	1	184.55K	4	0	0	2.01k	
QUIC	1	313.81K	1	0	0	797	
WindowsDriverInstall	4	93.76K	10	0	0	336	
SKYPE	3	183.4K	15	0	0	199	
DNS_over_HTTPS	4	12.85K	54	0	0	162	
TODESK	4	22.79K	2	0	0	155	

Displaying 40

Click a URL to add the URL to the filter condition. After searching, the figure shows the log number of the URL, and the content in the table changes accordingly.



App	Risk Level	Bytes	Session	Threat(Count)	Content(Count)	URL(Count)	View
IMAPS	4	133.61K	16	0	0	131	
BaiDu_com	1	184.55K	4	0	0	7	
QUIC	1	313.81K	1	0	0	6	
WindowsDriverInstall	4	93.76K	10	0	0	0	
SKYPE	3	183.4K	15	0	0	0	
DNS_over_HTTPS	4	12.85K	54	0	0	0	
TODESK	4	22.79K	2	0	0	0	

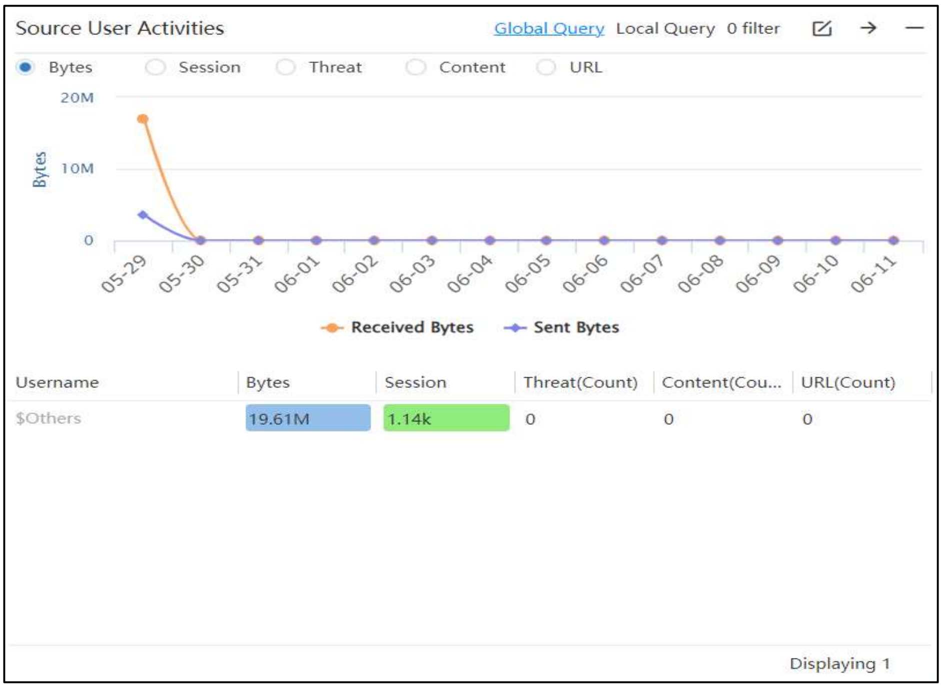
Displaying 40

18.3.2 Source User Activity

Bytes

The abscissa of the number of source user bytes is time, and the ordinate is the number of bytes. Display the traffic change trend of the source user within the selected time period. Through this graph, you can check whether the distribution of the source user traffic in time is normal.

The two traffic curves are the trend graphs of received bytes and sent bytes respectively.



Source User Activities Global Query Local Query 0 filter

● Bytes ○ Session ○ Threat ○ Content ○ URL

Username	Bytes	Session	Threat(Count)	Content(Cou...	URL(Count)
$Others	19.61M	1.14k	0	0	0

Displaying 1

The source user list displays the source user, byte count, session count, threat log count, content (file filtering and content filtering) log count, and URL log count. Source users are sorted by the number of bytes from largest to smallest, and from top to bottom.

Click the source user in the list to add the source user to the filter condition. After the search, the change trend of the user's byte count is displayed.

After the global search, the corresponding parameters of other area boxes also change. You can see the application, destination user, source IP, destination IP, source country /region, destination country/region, and policy corresponding to the source user.

Sessions

The abscissa of the number of source user sessions is time, and the ordinate is the number of sessions. Display the change trend of the number of sessions of the source user within the selected time period. Through this graph, you can check whether the distribution of the number of sessions occupied by the source user over time is normal.

In the source user list, the source users are sorted by the number of sessions from large to small, and from top to bottom.

Click the source user in the list to add the source user to the filter condition. After searching, the changing trend of the user's session number is displayed.

After the global search, the corresponding parameters of other area boxes also change. You can see the application, destination user, source IP, destination IP, source country /region, destination country /region, and policy corresponding to the source user.

Threats

Threats under source user and threats under application usage display the same content, both of which display the number of logs of different threat types in the threat log in a histogram. But the list below shows the source user list.

In the source user list, the source users are sorted by the number of threats from large to small, and from top to bottom.

Click the column corresponding to a threat type in the figure to add the threat type to the filter condition. After searching, the figure shows which threats exist under this threat type and the number of threats, and the content in the table changes accordingly.

Content

The content displayed under the source user is the same as the content displayed under the application usage, both displaying the log numbers of file filtering and content filtering in a histogram. But the list below shows the source user list.

In the source user list, the source users are sorted by the number of content from large to small, and from top to bottom.

Click the column in the figure to add filter conditions to search, and you can perform a more detailed search after the search.

URL

The content under the source user is the same as the content displayed under the URL under the application usage, and the number of logs classified by URL is displayed in a histogram. But the list below shows the source user list.

In the source user list, the source users are sorted according to the number of URLs from large to small, and from top to bottom.

Click the column in the figure to add filter conditions to search, and you can perform a more detailed search after the search.

18.3.3 Destination User Activity

Destination user activity is to analyze the number of bytes, sessions, threats, content and URLs from the perspective of the destination user.

18.3.4 Source IP Activity

Source IP activity is the analysis of bytes, sessions, threats, content, and URLs from a source IP perspective.

18.3.5 Destination IP Activity

Destination IP activity is to analyze the number of bytes, sessions, threats, content and URLs from the perspective of destination IP.

18.3.6 Source Country Activity

Source country activity is to analyze bytes, sessions, threats, content and URLs from a source country perspective.

18.3.7 Destination Country Activities

Destination country activity is to analyze bytes, sessions, threats, content and URLs from a destination country perspective.

18.3.8 Policy Usage

Policy usage is to analyze byte count, session count, threat, content, and URL from the perspective of policy matching.

18.4 Threat Activity

Threat activities analyze threats from hosts accessing malicious URLs, hosts requesting malicious domain names, non-standard port applications, and policies that allow non-standard port applications. Through association, you can discover the host, application, and policy that allows the application corresponding to the threat.

18.4.1 Threat Activity

Threats displays the number of logs of different threat types in the threat log in a bar graph. Threat type is the threat type of the threat log. Columns are arranged in descending order from largest to smallest, left to right.

The threat list displays the 50 most detected threats. You can view the threat name, threat type, severity, and number of threats. Severities include high, medium, and low.

Threat names are sorted by the number of threats from largest to smallest, and from top to bottom.

Click a threat type in the figure or a threat name in the list to add global filter conditions or private filter conditions for filtering, and you can view threats of certain threat types or threat names.

18.4.2 Hosts Accessing Malicious URLs

The abscissa of the host accessing the malicious URL is time, and the ordinate is the number of threats. Use a graph to display the trend of accessing malicious URLs within the time period selected by the user.

The list displays the host IP, username, and times of accessing the malicious URL.

Click the host IP in the list to add filter conditions. After the global search, the corresponding parameters of other area boxes also change. It can be seen the threats involved in the host IP, the non-standard port application used, and the policy that allows the non-standard port application.

18.4.3 Hosts Requesting Malicious Domain Names

The abscissa of the host requesting the malicious domain name is time, and the ordinate is the number of threats. The trend of requesting malicious domain names within the time period selected by the user is displayed through a graph.

The list displays the host IP, username, and times of accessing the malicious URL.

Click the host IP in the list to add filter conditions. After the global search, the corresponding parameters of other area boxes also change. It can be seen the threats involved in the host IP, the non-standard port application used, and the policy that allows the non-standard port application.

18.4.4 Non-Standard Port Application

Non-standard port applications show the applications using non-standard ports, so that it is convenient to find out whether there is any abnormality in the non-standard port applications.

Non-standard applications perform statistics on byte count, session, threat, content, and URL. This section displays similarly to "Network Activity > App Usage".

The application's port is displayed in the list of non-standard port applications.

18.4.5 Policy to Allow Non-Standard Port Applications

The policies that permit non-standard application cooperate with non-standard port applications. When anomalies are found in non-standard port applications, the corresponding policies can be directly located and modified.

18.5 Blocked Activity

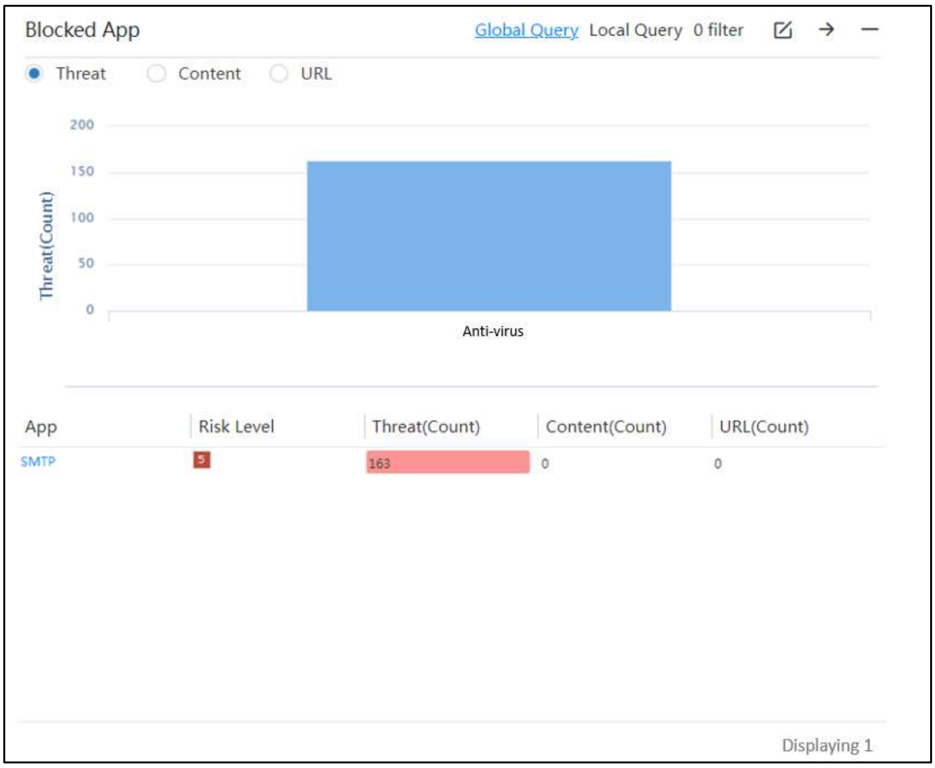
Blocked activities are analyzed in terms of applications, users, threats, content, domains, URLs, and policies.

18.5.1 Blocked Apps

Blocked Apps analyzes blocked threats, content, and URLs from an application perspective.

Threats

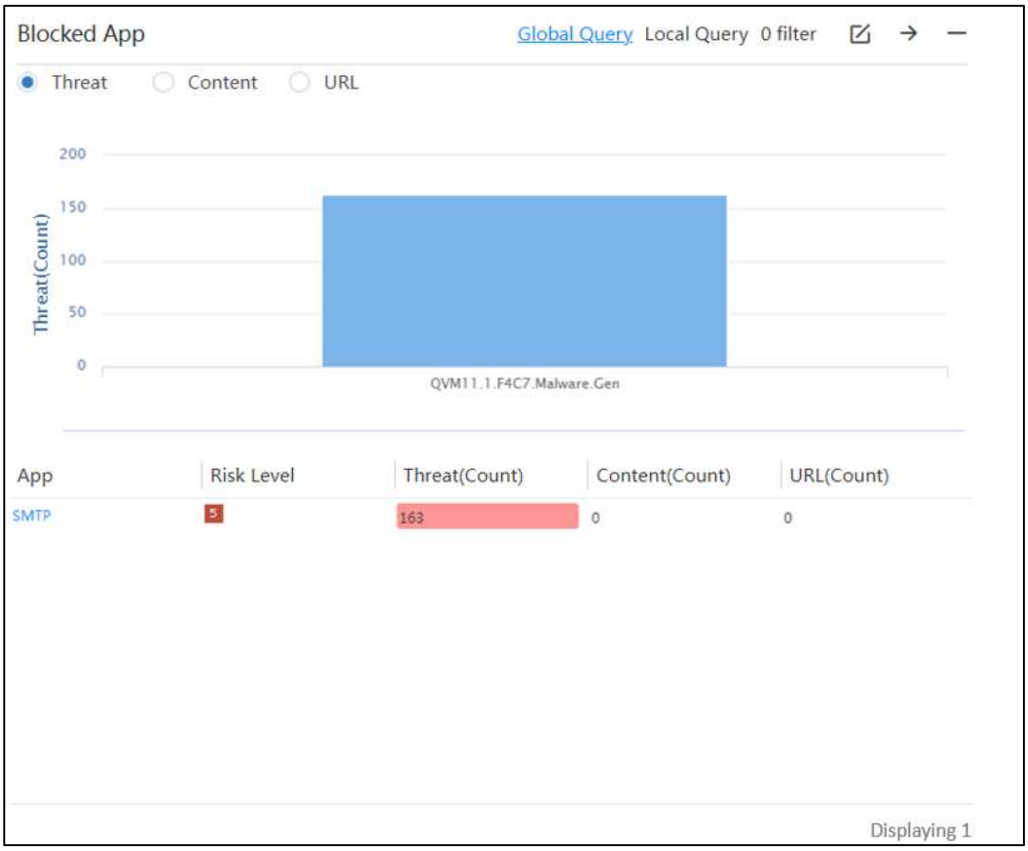
Blocked app threats display the types of threats and the number of threats that exist in the app. The number of threats of each threat type is displayed in columns, arranged in descending order, from left to right.



App	Risk Level	Threat(Count)	Content(Count)	URL(Count)
SMTP	5	163	0	0

The blocked application list displays the application name, risk level, threat count, content count, and URL filtering log count of the blocked apps. The threat list is sorted by the number of threats from large to small and from top to bottom.

Click a threat type in the figure to add filter conditions. After the search, the statistics graph of the number of threats blocked under this threat type is displayed. The application corresponding to the threat type is displayed in the list.



App	Risk Level	Threat(Count)	Content(Count)	URL(Count)
SMTP	5	163	0	0

Click the threat name in the figure to add the threat name to the filter condition. After searching, you can view the number of threats for this threat. The application corresponding to the threat is displayed in the list.

After the global search, the corresponding parameters of other area boxes also change. You can see the application, user, and policy corresponding to the threat.

Content

The content of blocked applications displays the log times of URL keyword filtering and content filtering. The URL or content is displayed in columns, arranged in descending order of the number of logs, and from left to right.

The list of blocked applications is sorted by the number of content logs from the largest to the smallest and from the top to the bottom.

Click “URL” or “Content” to add content filtering conditions. Display the number of logs by URL category or file type after searching. In the figure, continue to click “Add the filter condition”, and you can view the log times of the detailed URL or file. The application corresponding to the content is displayed in the list.

URL

The blocked application URL display shows the logs of the blocked URL categories in a histogram. URL categories are divided into URL libraries and custom URL categories. Columns are arranged in descending order from largest to smallest, left to right.

The blocked application list is sorted by the number of blocked URL logs from large to small and from top to bottom.

Click a URL category to add filter conditions. After the search, the number of logs of the URL subcategory is displayed. In the figure, continue to click to increase the filter condition to view the log times of the detailed URL. The application corresponding to the content is displayed in the list.

18.5.2 Blocked User Activity

Blocked user activity analyzes blocked threats, content, and URLs from the user's perspective.

The blocked users list displays usernames, threats, content, and URLs.

18.5.3 Blocked Threat

The blocked threat list displays the blocked threat name, threat type, severity and times.

It is sorted by the number of threats from largest to smallest, and from top to bottom.

18.5.4 Blocked Content

Blocked content statistics include log statistics for files, content, and URL keywords.

The list shows the blocked file names and times.

18.5.5 Blocked Domains

The abscissa of the blocked domain names is the time, and the ordinate is the number of times. Display the trend of blocked domains for the selected time period.

The list shows the blocked domain names and times.

18.5.6 Blocked URL

The abscissa of the blocked URLs is time, and the ordinate is times. Show the trend of blocked URLs during the selected time period.

The list shows the blocked URLs and the number of times.

18.5.7 Activities Blocked by Policy

The list of the threats blocked by policy displays the policy name, threat, content, and URL.

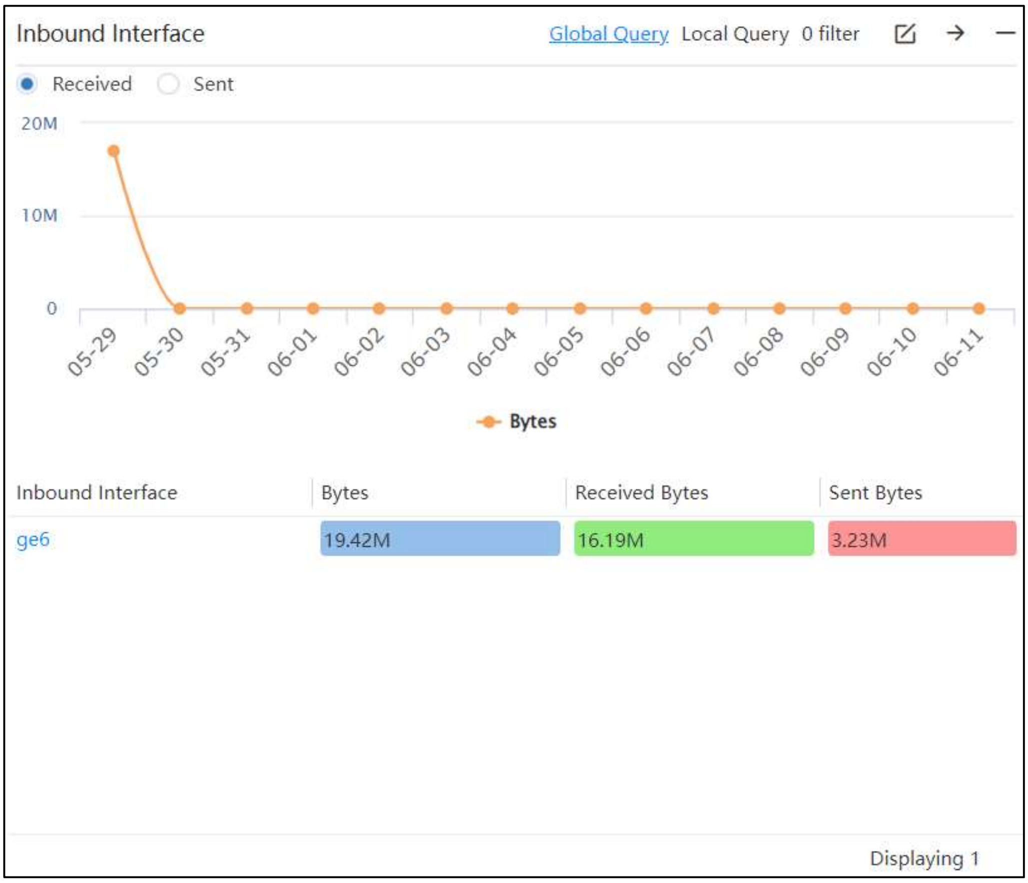
18.6 Custom

By clicking “Custom”, users can customize the analysis page.

In addition to items under network activity, threat activity and blocking activity, optional items also support "Ingress interface", "Egress interface", "Source security zone", "Destination security zone" and "Unidentified application".

18.6.1 Ingress Interface

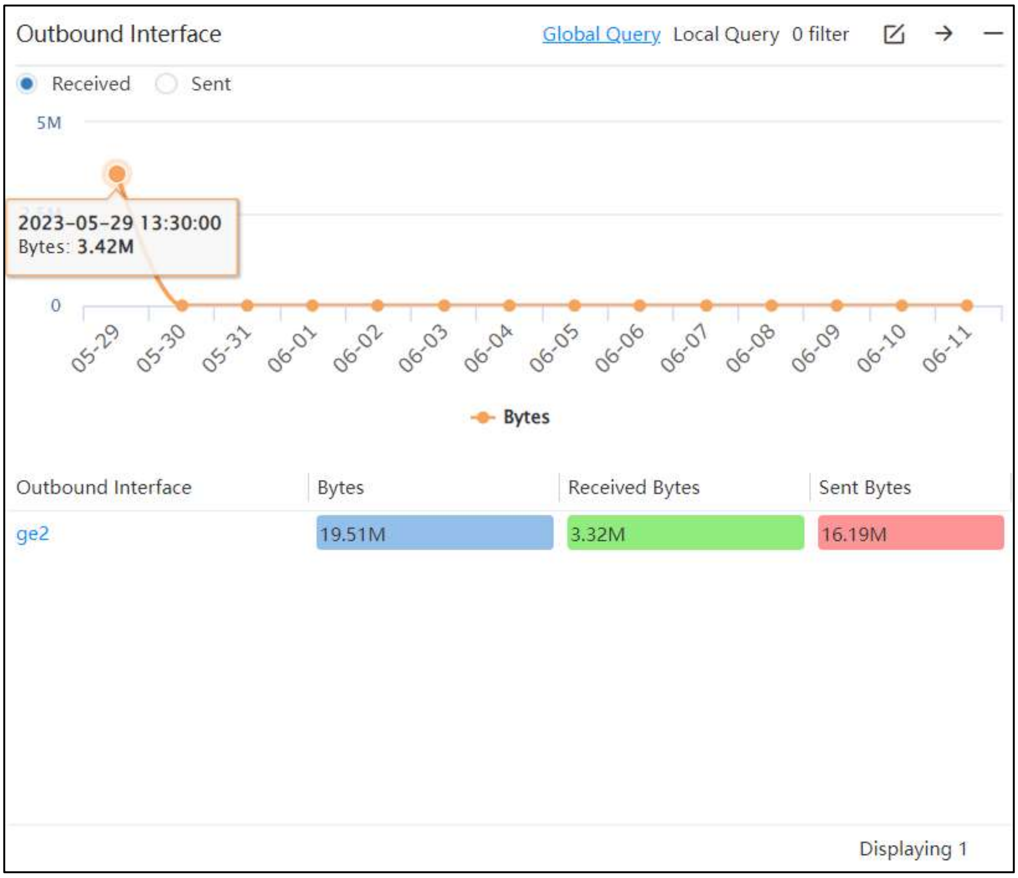
Ingress Interface analyzes the number of bytes received and transmitted by the different physical interfaces during the selected time period. Monitor the traffic on the interface.



Inbound Interface	Bytes	Received Bytes	Sent Bytes
ge6	19.42M	16.19M	3.23M

18.6.2 Egress Interface

The egress interface analyzes the number of bytes received and sent by the different physical interfaces during the selected time period. Monitor the traffic on the interface.



Outbound Interface

Global Query Local Query 0 filter

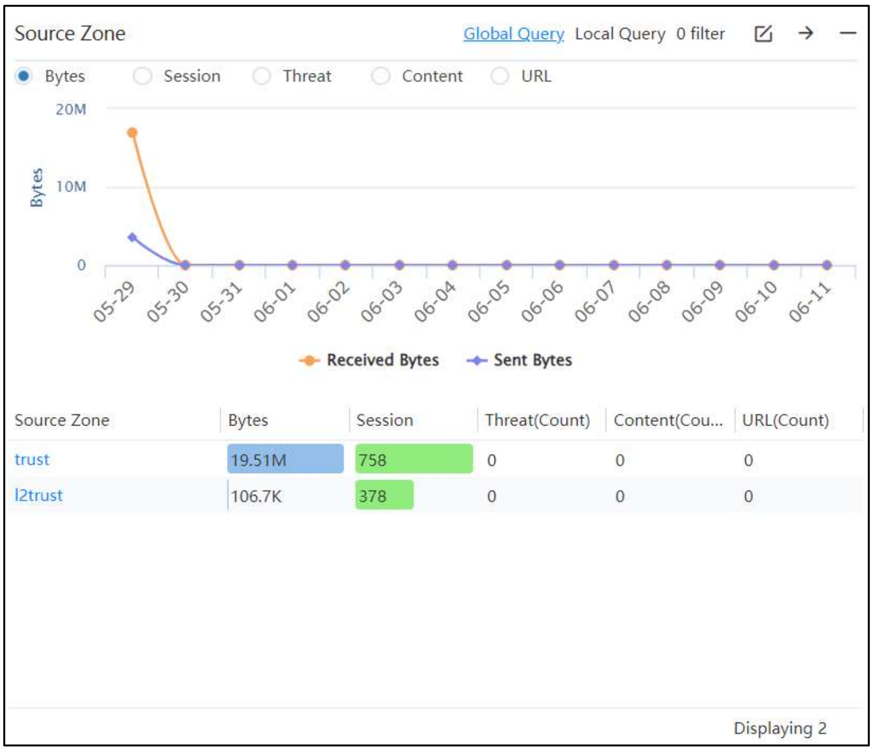
● Received ○ Sent

Outbound Interface	Bytes	Received Bytes	Sent Bytes
ge2	19.51M	3.32M	16.19M

Displaying 1

18.6.3 Source Security Zone

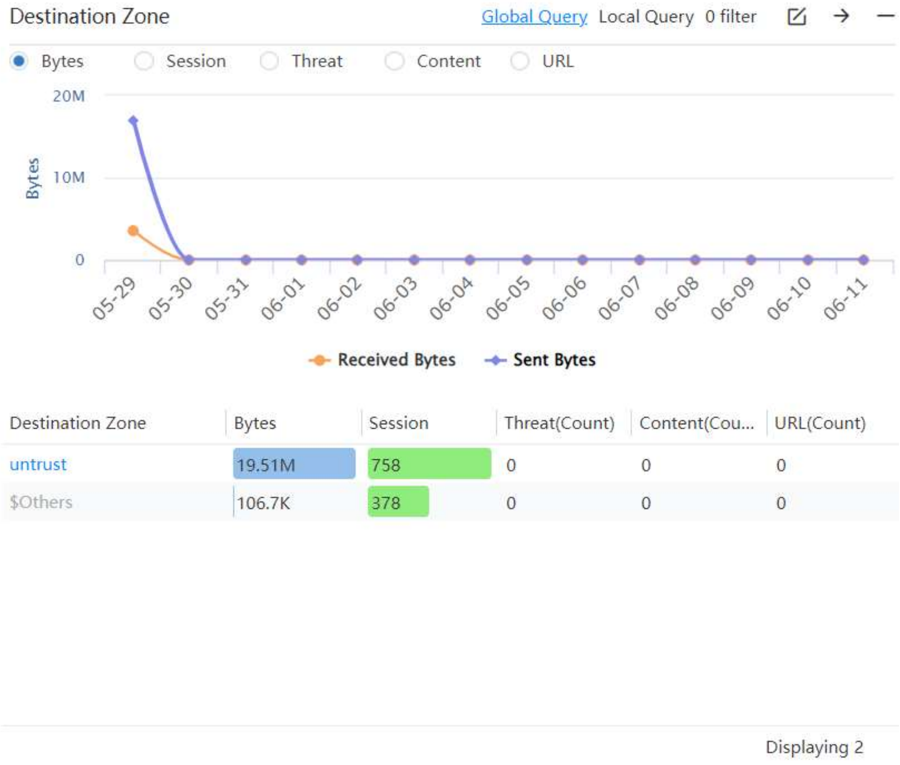
The source security zone analyzes the number of bytes, sessions, threats, content, and URLs in the source security zone.



Source Zone	Bytes	Session	Threat(Count)	Content(Cou...	URL(Count)
trust	19.51M	758	0	0	0
l2trust	106.7K	378	0	0	0

18.6.4 Destination Security Zone

The destination security zone analyzes the number of bytes, sessions, threats, content, and URLs in the destination security zone.

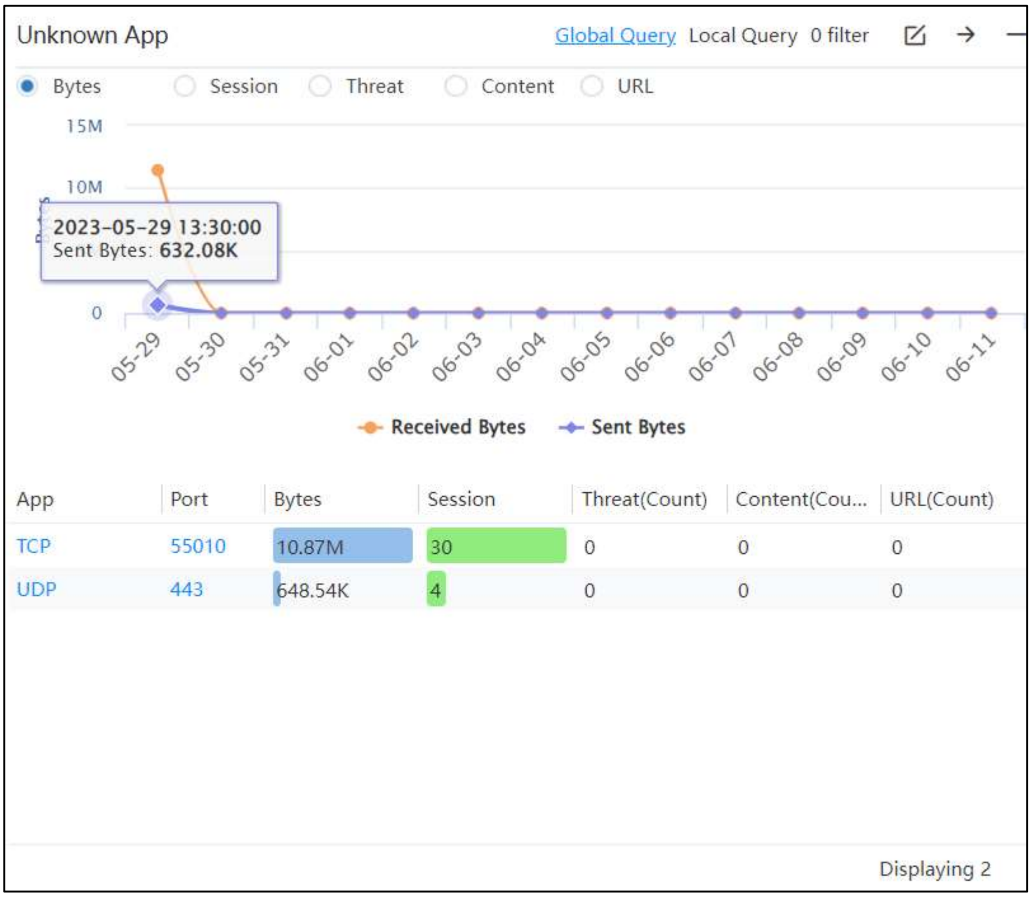


Destination Zone	Bytes	Session	Threat(Count)	Content(Cou...	URL(Count)
untrust	19.51M	758	0	0	0
$Others	106.7K	378	0	0	0

Displaying 2

18.6.5 Unidentified Application

Unidentified applications may be risky. Analyzing the traffic, sessions, threats, content, and URLs of unidentified applications can help users find abnormalities as soon as possible.



App	Port	Bytes	Session	Threat(Count)	Content(Cou...	URL(Count)
TCP	55010	10.87M	30	0	0	0
UDP	443	648.54K	4	0	0	0

Displaying 2