VOLKTEK

User Manual

3100-6GT-I

Managed 6x 10/100/1000 RJ45 with LAN Bypass

Industrial Firewall

Version-1.0 6th Nov 2025

Table of Content

Chapter 1. Installation and Information

1-1. Hardware Information

3100-6GT-I Hardware External Interface (See Figure 1-1):

Figure 1-1

- **[Power Connector]**: 2-Pin Terminal Block +9~36V DC Power Input.
- **[USB Port]**: Using USB to save configuration files, in case of device malfunction, preventing abnormal operation.

- **[LAN1~6]**: LAN1 is the default management interface. Other LANs can be configured as an internal network zone, allowing multiple ports to be grouped into a single zone and function as a bridge or switch.
- **[Console Port]**: Utilizing RS-232 connectivity to access the system, providing basic device management commands such as viewing network interfaces, restoring factory settings, and resetting to default management account and password.
- **[Installation]**: Supports wall-mount or din-rail.

1-2. Initial Installation

When 3100-6GT-I is shipped, it comes with default IP addresses and login credentials. Administrators need to configure their computer's IP address to be in the same network segment as 3100-6GT-I, and then use the default login credentials to access the device. Subsequently, they can configure new IP addresses based on the usage environment.

After accessing the device for the first time, it is recommended for administrators to change the default password of the admin account. Additionally, administrators get to limit the permissions of the default admin account after completing the configuration. The administrator privilege settings can be adjusted from "System Settings > Administrators."

First-time Network Setup

Connect the administrator's computer and the 3100-6GT-I labeled as MGMT to the same hub or switch, then use a browser (IE, Firefox, or Chrome) to access to the 3100-6GT-I management interface.

The default IP address of 3100-6GT-I is https://192.168.1.1, so the IP address of the administrator's computer must be one of 192.168.1.2 to 192.168.1.254, with a subnet mask of 255.255.255.0.

1. **Authentication Prompt in Browser**

   Upon accessing the system, the browser will prompt for a username and password. Enter the administrator's information:

   - **Username**: admin
   - **Password**: admin

   For convenience, users may choose the option to "**Remember Login Credentials**", which allows automatic authentication for subsequent logins using the same device and browser.

   Click "**OK**" to proceed to the management interface.

2. **Automatic Language Detection**

   The 3100-6GT-I device automatically detects the browser's language settings and switches the interface language accordingly. For example, if the browser is set to Traditional Chinese, the management interface will default to Traditional Chinese.

   The interface supports **Traditional Chinese, Simplified Chinese, and English**. If the browser uses a language other than these three, the interface will default to English to ensure usability.

3. **Language and Session Information Management**

   After logging in, administrators can manually switch the interface language from the upper-right corner of the dashboard. In this area, additional session-related information is also displayed, including: (See Figure 1-2)

   - A quick link to the **home page**
   - **Logout** button
   - The **IP address** of the logged-in administrator
   - The **number of active administrator sessions**

Figure 1-2

4. After successfully logging into the administrator interface, an installation wizard will automatically launch to guide the administrator through the initial configuration process. (See Figure 1-3)

   Note: The installation wizard will erase all existing data before saving the new configuration settings. Ensure that any important data has been backed up prior to proceeding.

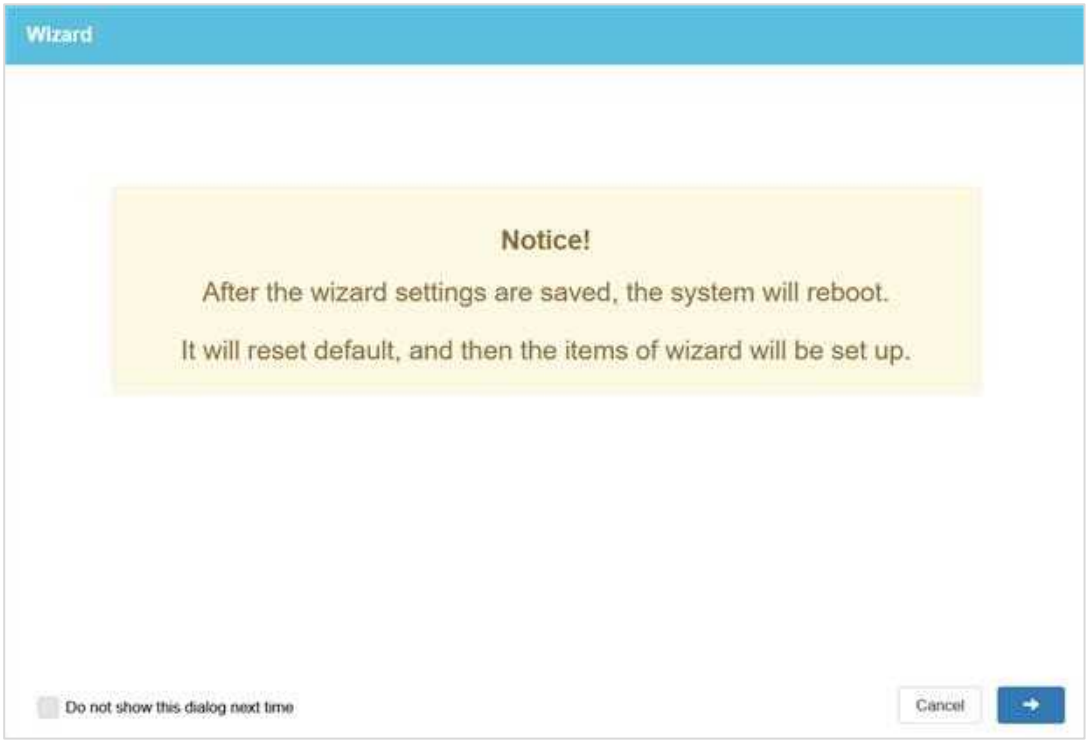


Figure 1-3

5. **Proceeding with Installation Wizard Configuration**

   To continue the setup process within the installation wizard, the administrator should click the Next button located at the bottom right corner of the interface.

   (1) Network Interface LAN

   Enter the appropriate IP address and subnet mask for the device. (See Figure 1-4)

Figure 1-4

(2) Network Interface WAN

Select the desired connection mode. At least one WAN must be configured to proceed with the installation process. (See Figure 1-5)

[STATIC]: Requires manual configuration of the IP address, subnet mask, and gateway. The default subnet mask is 255.255.255.0.

[DHCP]: The IP address, subnet mask, and gateway are automatically assigned by the upstream device. No manual configuration is needed.

[PPPOE]: The IP address, subnet mask, and gateway are dynamically assigned by the Internet Service Provider (ISP). If a static IP address is provided by the ISP, you may choose the STATIC mode instead.

Note: Proper WAN configuration is critical for ensuring secure and stable network communication.

Figure 1-5

(3) Security Settings

Enabled by default. Administrators can configure actions for abnormal IP addresses based on security requirements, such as logging, alerting, or blocking. (See Figure 1-6)

Figure 1-6

(4) OPC

By default, high-risk protection is enabled with the action set to Block and Log. (See Figure 1-7)

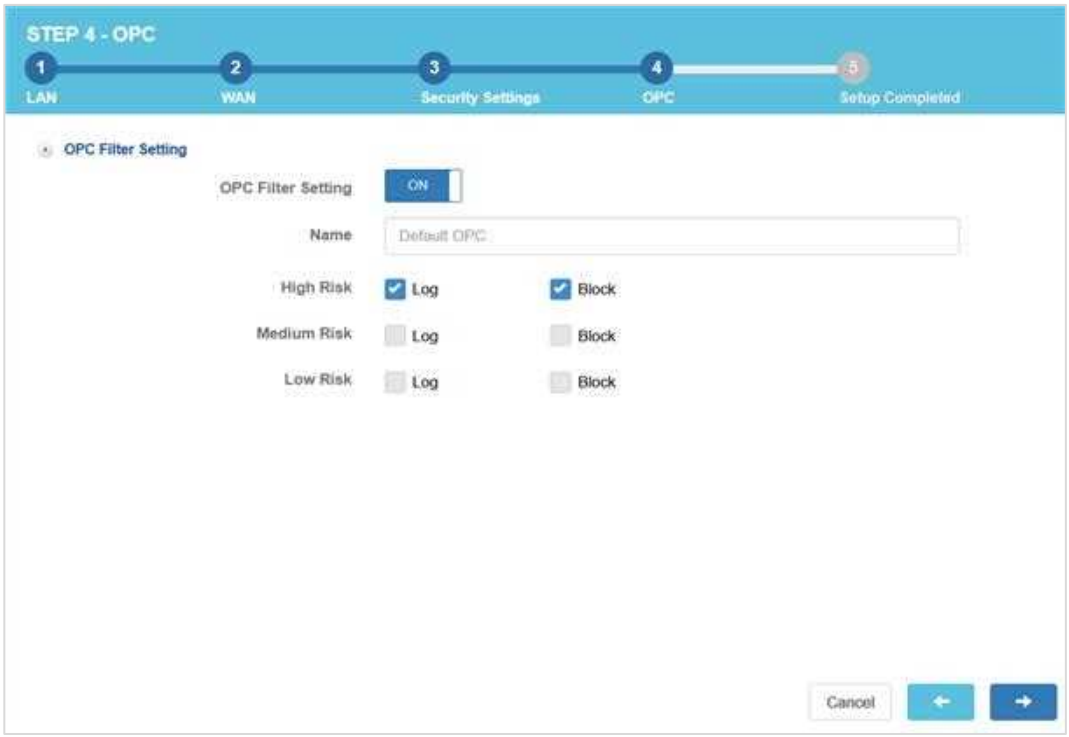


Figure 1-7

(5) Setup Completed

The final configuration summary will be displayed. After verifying the settings, click the Save button and wait for 120 seconds. The installation wizard will then save the configuration. (See Figure 1-8)

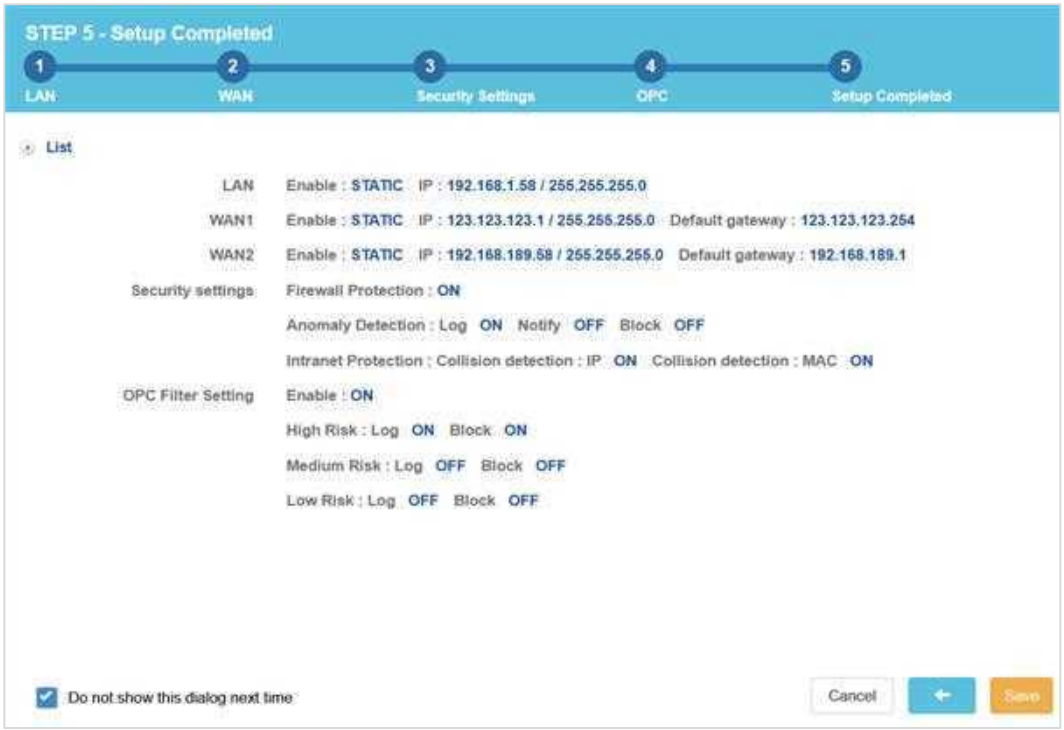


Figure 1-8

1-3. Management and Dashboard Modes

The 3100-6GT-I provides two interface modes: a management interface for administrators and a threat intelligence dashboard for monitoring network activity.

All configuration, management, and logging tasks are handled through the management interface. The threat intelligence dashboard offers real-time monitoring and report generation capabilities.

Under **[Configuration] > [Basic Setting] > [Homepage Setting]**, select the desired mode. The system will launch in that mode upon next login.

1. Management Interface

The management interface is divided into 5 main sections: Logo area, Title area, IP address switch (IPv4/v6), Main Menu area, and Settings area. Except for the Main Menu and Settings areas, which may display different configuration options based on the administrator's privilege, every administrator sees the same content in other sections. (See Figure 1-9)

Figure 1-9

- **[Logo Section]**: By changing the icon here, it not only facilitates device recognition but also highlights the overall image of the enterprise. The image format should be 150*90 pixels.

  You can go to "Configuration > Basic Setting > General Setting > Upload Logo" to upload the image. Supporting formats include gif, png, jpeg.

- **[Title Section]**: There are three blocks in this area: Homepage Title, Port Information, and Administrator Information.

  Homepage Title area: To recognize the device, enter the title text.

  Port Information: Displays the status of all hardware ports.

  Administrator Information: Displays the data of the logged-in administrator.

  The path for setting the homepage title is "Configuration > Basic Settings > General Setting.

- **[IP Address Switching]**: 3100-6GT-I is a multi-functional device that supports both IPV4 and IPV6. IPV4 and IPV6 have some differences in network security and management. For example, rejecting IPV4 web usage does not equal rejecting IPV6 web usage at the same time, so the two IP addressing modes are managed separately. Administrators can switch addresses here, and all management interface addresses will be switched together.
- **[Main Menu]**: The main menu of the management interface is divided into two layers: **main menu** and **sub-menu**. After selecting a sub-menu under the main menu, the setting area will display **tab menus** for detailed function settings. (See Figure 1-10)

Figure 1-10

In general, settings that apply to the entire 3100-6GT-I and belong to the system management level will be found under the main menu of "Configuration." Then, depending on the specific setting requirement, users will choose the corresponding sub-menu and tab menu.

- **[Setting Area]**: All detailed function settings and records for the system can be set up in this area.

2. Dashboard Interface

The Dashboard interface provides various statistical information and consolidates threats, allowing administrators to quickly understand the status of the device or identify abnormal users through graphical interfaces, and generate reports for export. Here are the functions displayed:

(1) Threats Information
(2) Flow Analysis
(3) Connection Status
(4) Firewall Protection
(5) OPC
(6) Web Control
(7) Mail Service

1-4. Homepage Information of Management Interface

After logging into 3100-6GT-I, the system provides information for administrators to understand the current operational status of the device.

1. Server System Resources

It displays the current time, time zone and even boot time of the device. It also shows the current usage of important resources such as CPU, RAM, Flash, HDD, etc. Administrators can use this information to determine if the device is overloaded. (See Figure 1-11)

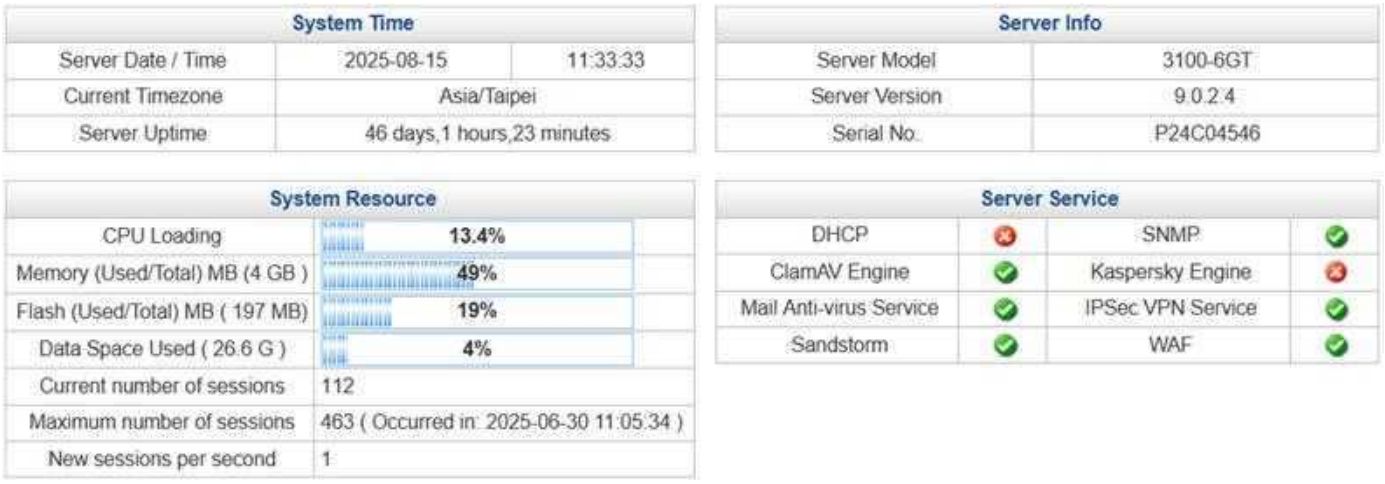


Figure 1-11

- **[Current Number of Sessions]**: The total number of connections (Concurrent Sessions) that 3100-6GT-I is currently handling.
- **[Maximum number of sessions]**: The maximum number of connections (Maximum Sessions) that the device has ever processed. 3100-6GT-I also marks the time when it occurred. Administrators can use this data to infer the peak loading time of the system. The time can also be detected once the system's attacked.

  Note: The information here is real-time data. To look up historical connection information, please go to "Status > System Status > History Status". Check the option for total connections and select the desired time range for inquiry.
- **[New sessions per second]**: The number of new connections created per second.
- **[Server Model/Version]**: The model and firmware version of 3100-6GT-I.
- **[Server Uptime]**: Record the time span since the last reboot. Whether in the situation where the administrator reboots the device or due to a power outage, the time will be recalculated.

2. Port Information

In the title area of the management interface, there is a hidden feature called "Port Information", which instantly displays the connection status of all ports in the current device. By default, it is in a closed state, you can click "Port Information" to expand it. (See Figure 1-12)

Zone List : (Click save after completing setting.)

Interface	Interface Name	Name	Color	Port
LAN	zone0	LAN		Port: 1
WAN1	zone1	WAN1		Port: 2
Bridge1	zone2	Bridge1		Port: 3, 4
LAN2	zone3	LAN2		Port: 5
HA	ha	HA		Port: 6

Figure 1-12

Light green indicates that the port is currently active and successfully connected to another device. The connected speed is also displayed on the device. **Red** indicates that the port is inactive. When any port is selected, the system will automatically navigate to the network configuration page.

The port numbers displayed here correspond to the actual port numbers on the physical device, although their physical locations may vary. Therefore, administrators should use the **port numbers** as the basis when configuring network zones.

In **[System Settings] > [Network]**, network interfaces that belong to the same zone are marked with the same color block. This allows administrators to quickly identify which ports are bonded or operating independently.

3. Port Information

At the right of the management interface header is the Administrator Information Area, which includes language switching, administrator information, and the number of administrators currently logged into the device.

- **[Language Switch]**: The system automatically detects the browser language used by the administrator and operates in the same language. Administrators can manually switch the language.

  The system currently supports Traditional Chinese, Simplified Chinese, and English. If the browser is set to a language other than these three, the system will default to English.

- **[Administrator and Login IP Address]**: Displays the source IP address and account used by the administrator to log in.

  New administrator accounts can be added under [Configuration] > [Administration] > [Account and Privilege].

- **[Current Online Users]**: Shows how many administrators are currently logged into the system. Clicking the number opens a new page displaying each administrator's login time, source IP address, and actions performed. Action details include granted permissions and operations performed.

  This section only displays real-time activities of currently logged-in administrators. For example, if two administrators are logged in, each can see the other's ongoing configurations. Once an administrator logs out, their information will no longer be shown here.

  To view historical administrator activity, go to **[Logs] > [System Operation]**.

- **[Home / Logout]**: Provides quick links to return to the homepage or log out of the system.

4. Network Interfaces

It displays network interface information and real-time traffic for all areas in **[Network] > [Interface]**. Administrators can switch to view all, connected, or customized areas.

Customization requires selecting areas in "[Configuration] > [Basic Setting] > [General Setting] > [Homepage Message]".

Real-time traffic dynamically presents upload and download traffic for the past 60 seconds.

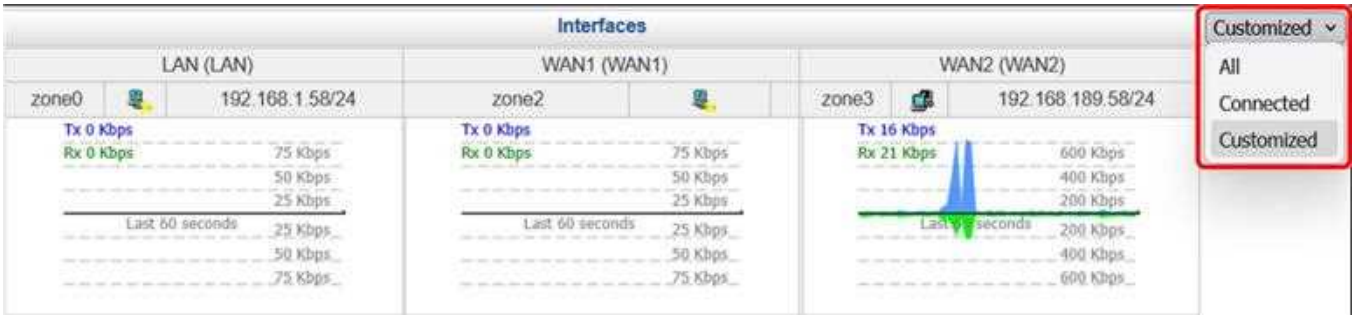


Figure 1-13

Upload/download indicators use blue to denote uploads and green for downloads. The direction is determined from the device's standpoint: upload refers to traffic leaving the device, whereas download refers to traffic entering the device.

For interfaces connecting to the Internet, such as WAN interfaces (e.g., PPPOE), the upload and download traffic direction aligns with the perspective of general users.

However, for interfaces connecting to internal devices, like LAN interfaces, the upload and download traffic direction is opposite from the user's perspective. Upload traffic from LAN interfaces is considered download traffic from the user's perspective.

The traffic information displayed on the homepage is real-time, with a duration of only 60 seconds. If administrators need to access traffic data for a longer period, they can find more options in **[Status]**:

A. **3-minute Traffic Graph**: [Status] > [System Status] > [Timely Flow]

   This provides information about real-time traffic for specific interfaces over a period.

B. **Historical Traffic Graph**: [Status] > [System Status] > [History Status]

   This stores device data, offering longer-term records. Historical traffic graphs can be displayed based on the desired network interface and time range.

Chapter 2. Configuration

Configuration is the basic setting of the entire machine, including the allocation of permissions to subordinate administrators, system upgrades, backup and restoration, and notification of critical events. Not every administrator with access to the device has the same level of privilege. Only the primary administrator has the authority to perform system settings.

3100-6GT-I provides multiple levels of administrative privilege, and administrator privilege settings can be accessed through [Configuration] > [Administration] > [Account and Privilege].

2-1. Basic Setting

2-1-1. General Setting

1. General Setting

The basic operations of the 3100-6GT-I, such as browser message, memory settings, and connection timeout, can be configured by the administrator according to personal preferences. Administrators can set the title and logo displayed in the browser, as well as customize the text that appears on the homepage after logging into the 3100-6GT-I. All these configurations are available under **[General Setting]**. (See Figure 2-1)

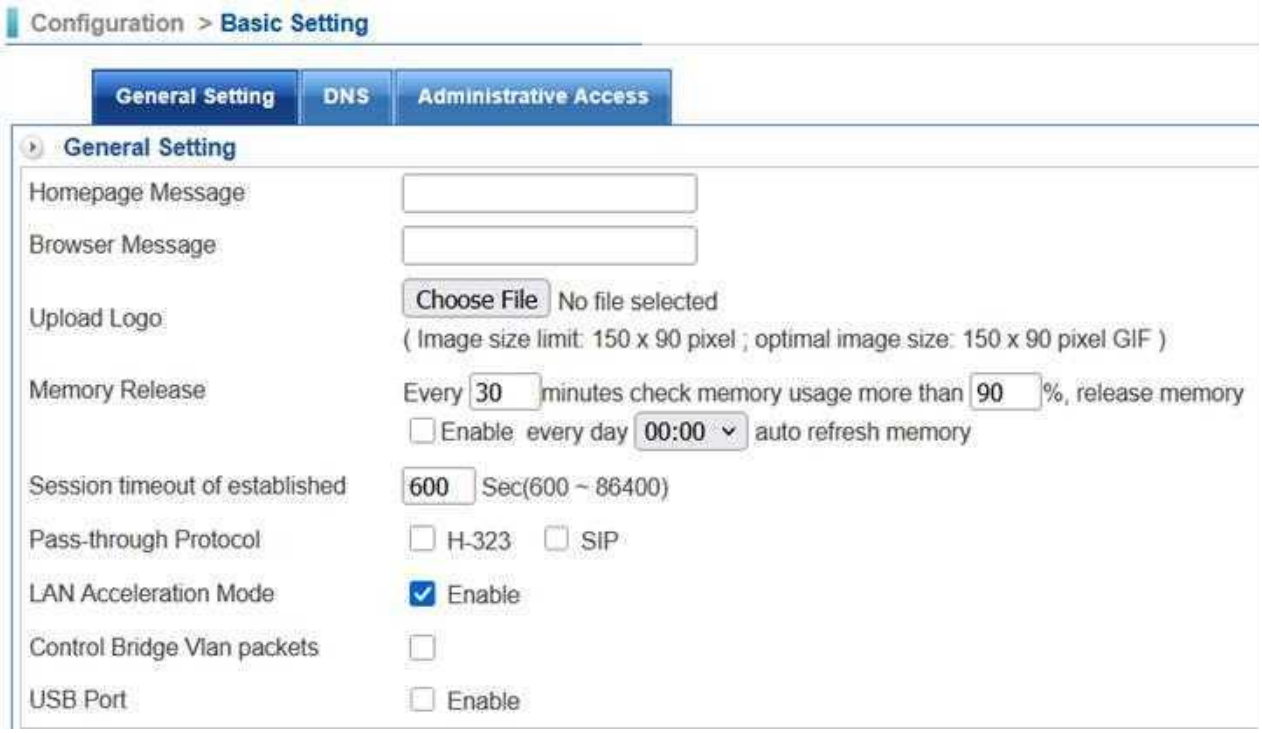


Figure 2-1

- **[Homepage Message]**: The text displayed in the title area of the management interface. When managing multiple devices simultaneously, the homepage title can effectively help administrators identify and correctly configure settings for the devices they intend to operate.
- **[Browser Message]**: The text displays in the browser title when logging into the management interface. Setting an easily recognizable title allows administrators to quickly identify this interface when opening multiple web pages.
- **[Upload Logo]**: Image size is limited to 150 x 90 pixels. PNG, JPEG, GIF formats are supported.

- **[Memory Release]**: To prevent memory from being occupied by unnecessary processes, causing system instability, 3100-6GT-I has a built-in mechanism for automatically clearing memory

  The system checks memory usage every 30 minutes. When memory usage exceeds 90%, a clearing mechanism is triggered to release unused memory. Administrators can adjust the checking interval and the threshold for triggering based on usage status.

  Regular Memory Cleanup: Default is OFF. Administrators can specify a time for the system to perform regular memory checks and cleanup instead of waiting for memory usage to reach the trigger condition before initiating the cleanup process, thus enhancing system stability. Typically, the cleanup schedule is set when the system is less busy, such as midnight at 00:00.

- **[Session time out of established]**: This setting determines the duration within which an established TCP connection, with no data transmission, will be actively terminated by the system. The default value is 600 seconds. If the timeout is set too long, such as 86400 seconds (1 day), the system may be overwhelmed by numerous idle TCP connections, which might consume memory resources.

  In general, a communication session will automatically be terminated after data transmission ends. However, in cases of abnormal termination or malicious attacks, these TCP connections may remain in the system, occupying memory resources.

  When too many connections occupy the memory, it may stop the normal connection requests from being serviced. In such cases, this mechanism is needed to terminate these abnormal connections.

  Note: The setting for “Session timeout of established” only applies to established TCP connections and does not affect incomplete TCP connections or UDP protocol. UDP protocol is unaffected because it lacks a three-way handshake mechanism. Incomplete TCP connections present many possible risks, such as SYN attacks in DDoS attacks, which consume resources.

  3100-6GT-I provides protection against SYN attacks. In [Policy] > [Security Policy] > [SYN Protection], you can specify the hosts that require SYN protection mechanisms.

- **[Pass-through Protocol]**: Once enabled, packets for the SIP protocols are automatically passed through without additional control.

- **[LAN Acceleration Mode]**: Switch the virtual interface bound to multiple physical interfaces from Bridge mode to Switch mode. Different modes have different settings in sections.

- **[Control Bridge VLAN Packets]**: When the firewall is positioned for filtering between two switches, and packets carry VLAN tags, this option must be selected to allow the firewall to control these packets.

- **[USB Port]**: When a device is plugged into the USB port, inspect its functionality to ensure proper operation and mitigate the risk of deliberately connected malicious USB devices.

2. Auto VPN

Auto VPN simplifies the setup of IPSec VPNs, especially when dealing with many dynamically assigned IP addresses. It accelerates VPN establishment and enhances overall operational stability. For detailed information about this feature, please refer to 12-1-2. Auto VPN Server. This setting specifies the communication port used by Auto VPN. The default is 24088. Setting the port to 0 disables this feature.

3. Login Failure Block Settings

The 3100-6GT-I protects itself from brute-force password guessing mechanisms, regardless of whether the password is used by the primary administrator or secondary administrators. The protection method is to limit the number of login attempts from each source IP address. When the number of failed attempts exceeds the set threshold, the 3100-6GT-I will block that source IP address to prevent further password guessing. The blocked IP address will remain locked until the configured blocking period expires or until another user with primary administrator privileges logs in and performs the unblock action.

- **[Temporarily block when login failed more than]**: Defines the maximum number of failed password attempts allowed per account. When an account exceeds the configured number of failed attempts, the source IP address will be blocked.

  The default value is 0, meaning there is no limit to the number of failed attempts.

- **[IP blocking period]**: When the number of failed login attempts from an IP address exceeds the threshold, the 3100-6GT-I will temporarily block that IP address for a certain period. The time is measured in minutes, and after the specified period, the IP address will be allowed to attempt logging in again.

  The default value is 0, meaning no limit is set, effectively blocking the IP address permanently from logging into the management interface unless an administrator with primary management rights goes to **[Unblock IP]** and unblocks the IP address.

- **[Unblocked IP]**: Blocked IP addresses will be listed here. The primary administrator can decide whether to unblock them. If the IP address is not permanently blocked, the system will automatically unblock it once the set time in **[IP blocking period]** has elapsed.

4. Homepage Setting

3100-6GT-I provides two types of user interfaces: the traditional management interface and the Dashboard interface. The former allows for the management of the entire 3100-6GT-I device, enabling various administrative actions. The latter, on the other hand, presents graphical representations of network traffic, intrusion detection records, and other related information, offering a visual overview of 3100-6GT-I's inbound and outbound traffic or hacker attack-defense records.

- **[Homepage Setting]**: There are two options, "Management page" and "Dashboard." It determines which screen is displayed when an administrator logs in. The default is the "Management page."

5. Homepage Interfaces Setting

When the primary administrator logs into the 3100-6GT-I management interface, it displays real-time traffic for each network zone. However, when there are numerous network zones, it can be challenging for the administrator to identify them. In this setting, the administrator can configure which network zone to be displayed.

- **[Homepage Interfaces Setting]**: There are 3 modes to choose from: All, Connected Interfaces, and Customized.

  All: All ZONE interfaces are listed.

  Connected Interfaces: Only connected interfaces are shown. Other interfaces that are not enabled or connected are hidden.

  Customized: The administrator selects the ZONE to be displayed. (See Figure 2-2)

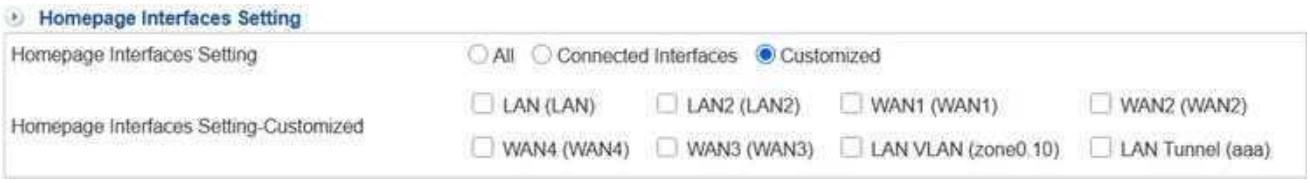


Figure 2-2

By default, traffic across all zones is displayed. After configuration, only the specified interfaces will be shown on the home page.

Real-time zone selection remains available, including All, Connected, and Customized. However, upon the next login, the default display will correspond to the interfaces selected in this configuration.

6. Drop Session Log

The feature in the policy displays **packet communication records**. By default, only established connections are displayed. Typically, established connections indicate compliance with the policy. For packets that violate it, the system discards them without any record. When this feature is enabled, the system retains records of discarded packets.

2-1-2. DNS

DNS servers are configured for 3100-6GT-I's own queries. Since 3100-6GT-I may not necessarily be placed on the external gateway, it needs to set up DNS servers for domain name resolution. The DNS servers can be either IPv4 or IPv6. (See Figure 2-3)

- **[DNS Server 1]**: The first DNS server used by NG-UTM, such as 168.95.192.1
- **[DNS Server 2]**: The second DNS server used by NG-UTM, such as 8.8.8.8
- **[DNS Server 3]**: The third DNS server used by NG-UTM, such as 2001:b000::1

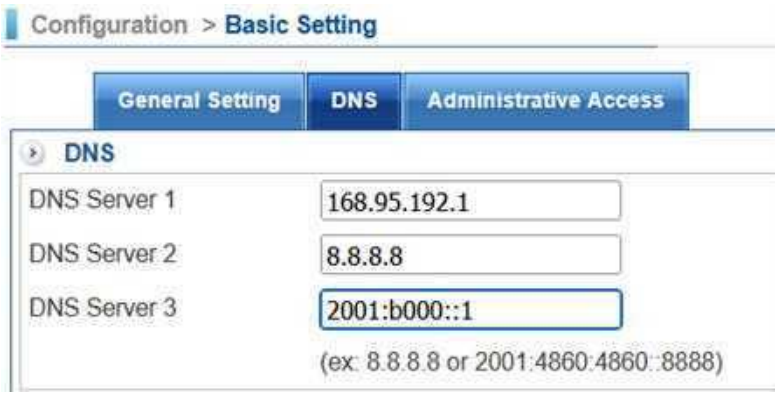


Figure 2-3

When 3100-6GT-I needs to query DNS records, it will first query DNS Server 1. If the configured DNS server does not respond, it will then proceed to query the other DNS servers in sequence.

2-1-3. Administrative Access

1. Administrative Access

3100-6GT-I is configured to use HTTPS protocol for accessing the management interface via a web browser. HTTPS typically uses port 443 by default. However, administrators can customize this port to any number from 1 to 65535 according to their requirements. Once the port is changed, users will need to use the new port to access the management interface next time they log in. (See Figure 2-4)

- **[HTTPS Port]**: This setting determines the port number used to access the 3100-6GT-I management interface. The default number is 443.

  If the default IP address of 3100-6GT-I is 192.168.1.1 and its management port is changed to 10443, after saving this configuration, users will need to use the new port for subsequent logins (e.g., https://192.168.1.1:10443).

- **[Idle Timeout]**: This setting determines how long the management interface will remain active when it's idle. If the idle time exceeds the configured duration, 3100-6GT-I will automatically terminate the administrator's connection. To re-enter the management interface, the administrator needs to log in again.

  The idle time range is from 5 to 60 minutes, with a default of 60 minutes.

- **[Security]**: The administrator can adjust the connection encryption to use TLSv1.1, TLSv1.2, or TLSv1.3

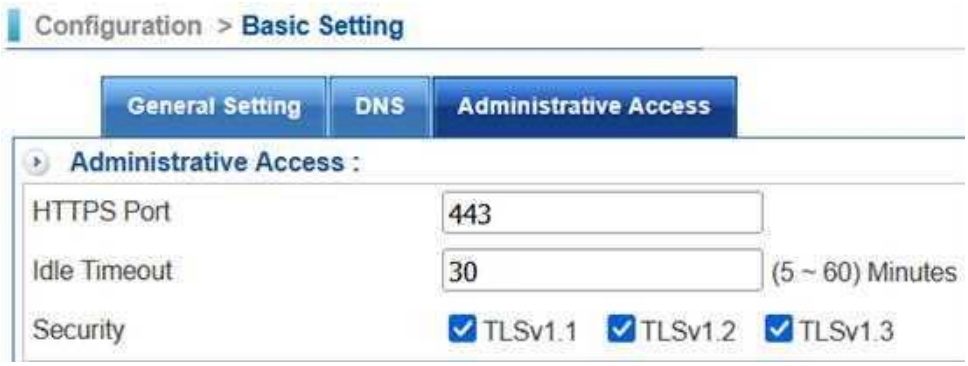


Figure 2-4

3100-6GT-I can configure multiple ZONES, and each ZONE can have its own IP address. These IP addresses can then be provided to primary administrators or subordinate administrators to access the management interface.

2. Administrator Custom the rule of Password

To prevent administrator passwords from being guessed—especially common weak passwords such as 123456 or qazwsx—and to stop malicious actors from taking control of the 3100-6GT-I, the system provides two measures: password complexity configuration and periodic reminders for administrators to change their passwords. (See Figure 2-5)

When setting password complexity, the system also prompts whether to require certain special characters, such as uppercase letters, to strengthen the password.

- **[Enable]**: Enables the feature of customizing administrator password rules. This is disabled by default.
- **[The Shortest Length (3-64 characters)]**: Sets the minimum length for passwords. Generally, longer passwords provide higher security.

- **[Must Contain]**: Specifies the characters that must be included in the password to increase the strength.

  Typically, a combination of uppercase letters, lowercase letters, and numbers in an 8-character password provides sufficient security, significantly reducing the probability of being guessed compared to passwords composed solely of numbers or lowercase letters.

- **[The Password Cannot Contain the Previous Password]**: When enabled, each time a password is changed, the new password set by the administrator cannot be the same as the old password. This feature is disabled by default.

- **[PSWD cannot be the same as old one(s)]**: The new password cannot be the same as the previous (1-5 times) password.

- **[Need to update password]**: Set the frequency when the system reminds administrators to change their passwords. The default is 90 days; setting it to 0 can disable this feature.

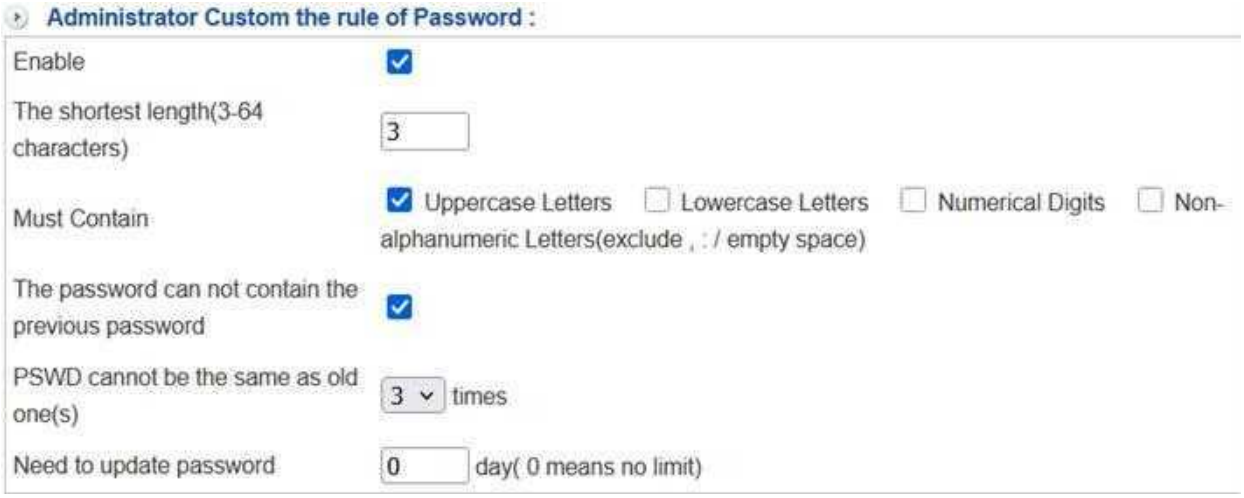


Figure 2-5

3. 2-Step Verification Rule for Administrator

A 2-Step Verification Rule is available, requiring administrators to complete two separate authentication procedures during login. The process begins with entering the correct password, followed by secondary identity verification—such as a time-based one-time password generated via a TOTP Authenticator. This approach greatly improves account security and mitigates the risk of unauthorized access or information leakage. (See Figure 2-6)

- **[Verify every time you login]**: Two-step verification is required each time you log in.

- **[After the account verification is successful, how long does it take for the 2-step verification to be unnecessary]**: Defines how long two-step verification can be skipped after a successful login. However, the administrator account must log in from the same source IP; otherwise, two-step verification will be required again.

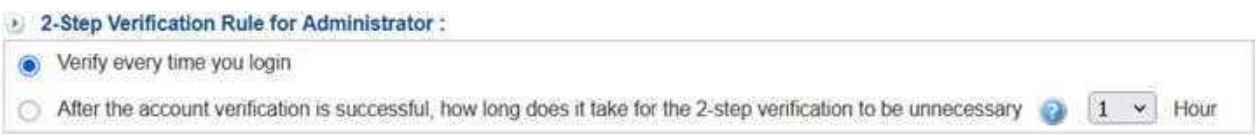


Figure 2-6

2-2. Date and Time

The 3100-6GT-I records are timestamped, so the accuracy of time is crucial. The system has an automatic time correction feature, which synchronizes with the configured time zone and time server for network adjustment. (See Figure 2-7)

1. Time Zone and Time

- **[Time Zone]**: Set the time zone for 3100-6GT-I by selecting one from the list of time zones where 3100-6GT-I is located.
- **[Time]**: Set the time for 3100-6GT-I.
- **[Date]**: Set the date for 3100-6GT-I.

After configuring the time zone and time, press save to complete the time setting action.

Figure 2-7

2. Sync with NTP Server

Enable the option for **[Sync with NTP Server]** and choose either a publicly available time server from the internet or manually input a specific time server. 3100-6GT-I will synchronize with the time server every 30 minutes.

The corrected data display will be available in the “Time Zone and Time” section. All synchronization processes with the time server will be recorded in the [Time Log].

- **[Sync with NTP Server]**: Choose whether to enable this feature. Default is disabled.
- **[Time Server]**: The time server currently in use.
- **[Time Log]**: Record the synchronization data between 3100-6GT-I and the time server. All data will be retained for 3 days.
- **[Refresh]**: If immediate correction is needed, press [Refresh] button, and the system will promptly synchronize with the configured time server.
- **[Select Time Server]**: Choose a suitable time server based on the time zone.
- **[Define Time Server]**: Enter the time server to be used.

2-3. Administration

According to the administrative privilege, there are two levels: **primary administrators** and **sub-administrators.** The default admin account serves as the default primary administrator, and there can be multiple primary administrators.

For example, the default primary administrator “admin” can add another primary administrator named “Joy” to assist in managing the entire device. Joy can also change admin’s permissions to that of a sub-administrator. To avoid situations where there is no primary administrator due to permission settings errors, the system automatically retains the last account with primary administrator privileges.

3100-6GT-I allows several sub-administrators with varying levels of privilege, along with customized administrator item selection, enabling sub-administrators to carry the workload of primary administrators. Sub-administrators can also be allocated via the web interface (ZONE) for greater flexibility in device management.

Considering scenarios for the application of sub-administrators, several operational situations can be envisioned, which can be easily achieved by customizing administrator item selection based on the situation:

A. An administrator can only handle VPN operations such as establishing VPN channels, controlling them, etc., without knowing too much about other detailed functions.

B. Auditors can access 3100-6GT-I to review recorded information.

C. Network administrators can manage the device but cannot view recorded data.

Explanation of account and privilege are as follows:

1. Account

The “admin” account is the default primary administrator for 3100-6GT-I, and its default password is “admin”. This default account cannot be deleted. During the initial setup, it is necessary to log in using the default admin account. At this point, admin can create other primary or sub-administrator accounts.

Due to its frequent use in similar network management interfaces and for security reasons, the admin’s privilege can be restricted to “Read”.

2. Privilege

Privileges are divided into three categories: **Read**, **Write**, and **All Privileges**. When combined with customized menu functionality, certain item management permissions can be assigned to different sub-administrators.

3100-6GT-I’s permission configuration is highly flexible. Administrators with **All Privileges** are referred to as primary administrators, while those with **Read** or **Write** privileges are referred to as sub-administrators.

Only primary administrators have the permission to add, modify, or delete other sub-administrators. Detailed explanations are as follows:

- **[Read]**: Enables browsing functionality without write (configuration) permissions.

  When paired with a customized menu, sub-administrators can only view the items assigned to them. In the absence of a customized menu, this privilege grants viewing rights across the entire device.

- **[Write]**: Enables both browsing and configuration capabilities.

  When used with a customized menu, sub-administrators may configure only the items explicitly granted to them. For example, if Sub-Administrator A is granted authority over VPN tunnels, the menu upon login will display only the VPN section, with all others hidden. Without a customized menu, this privilege provides configuration rights across the entire device.

- **[All Privileges]**: Provides comprehensive browsing and configuration rights to primary administrators. No customized menu settings are required.

2-3-1. Administrator

Account management will list all administrator accounts with access to the 3100-6GT-I management interface, along with their respective privileges. This includes functionalities for browsing or configuration, as well as estimated password change time.

Add New Administrator

Click on the Add button to access the settings for adding a new administrator. The instructions are as follows:

- **[Account]**: The username used for the new administrator. Any combination of English letters and numbers is acceptable.
- **[Password]**: Passwords are case-sensitive and must be between 3 and 64 characters long. The password cannot be the same as the username.

  Typically, a combination of 8 characters consisting of letters and numbers provides a certain level of strength.
- **[Password Strength]**: 3100-6GT-I automatically evaluate the password strength. To enhance password security, consider the following:

  A. Use a combination of letters and numbers.

  B. Incorporate special characters such as “@”, but avoid using colon “:” and comma “,”.

  C. Use a mixture of upper and lower case letters. For example, “Joy123” has higher complexity than “joy123”.
- **[Confirm Password]**: Re-enter the password to ensure consistency.
- **[Next time need to alter the password]**: After the new administrator successfully logs in for the first time, this option determines whether they are forced to change their password. By default, this option is disabled.
- **[Need to update password]**: Specify how often the system needs to remind the administrator to change their password. The default frequency is 90 days. Setting it to 0 disables this feature.
- **[PSWD cannot be the same as old one(s)]**: The new password cannot be the same as the previous (1-5 times) password.
- **[Account Expiration Date]**: Cannot log in with this account after the account expiration date.
- **[Notes]**: A recognizable description for the new administrator.
- **[2-step Verification]**: When enabled, logging in requires entering not only the original password but also a verification code generated by TOTP Authenticator.
- **[Privilege]**: Set the privilege for the administrator, with 3 options: **Read**, **Write**, and **All Privileges**.

  Choosing Read or Write permissions without selecting **[User Defined Menu]** means the administrator can access all function options. Since **All Privileges** corresponds to the primary administrator role, the **[User Defined Menu]** option will be automatically hidden when **All Privileges** is chosen.
- **[User Defined Menu]**: Specify which items the primary administrator grants the sub-administrator access to browse or configure. If not enabled, sub-administrators are granted access to the entire system.

  3100-6GT-I’s configuration structure consists of **a main item, a sub-menu, and a tab menu(s)**, with actual settings in the **tab menu**.

Permission control for sub-administrators is achieved by regulating visibility of the main item and sub-menu. As both elements reside in the left-hand main navigation panel, the **[User Defined Menu]** corresponds to the left-side main menu.

Examples: create a **[User Defined Menu]** and see the differences between Read and Write privilege.

A. Setting up a **[User Defined Menu]** includes items such as “Basic Setting,” “Notifications,” “Zone Settings,” “IP Tunnel” and more. (See Figure 2-8)

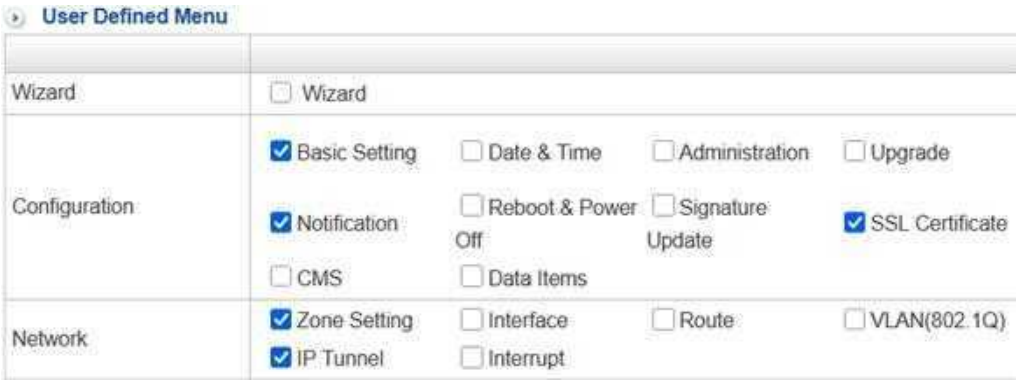


Figure 2-8

B. When an account with **Read** privileges logs into the management interface, the menu items are visible, but the **Confirm** and **Save** buttons are not available. (See Figure 2-9)

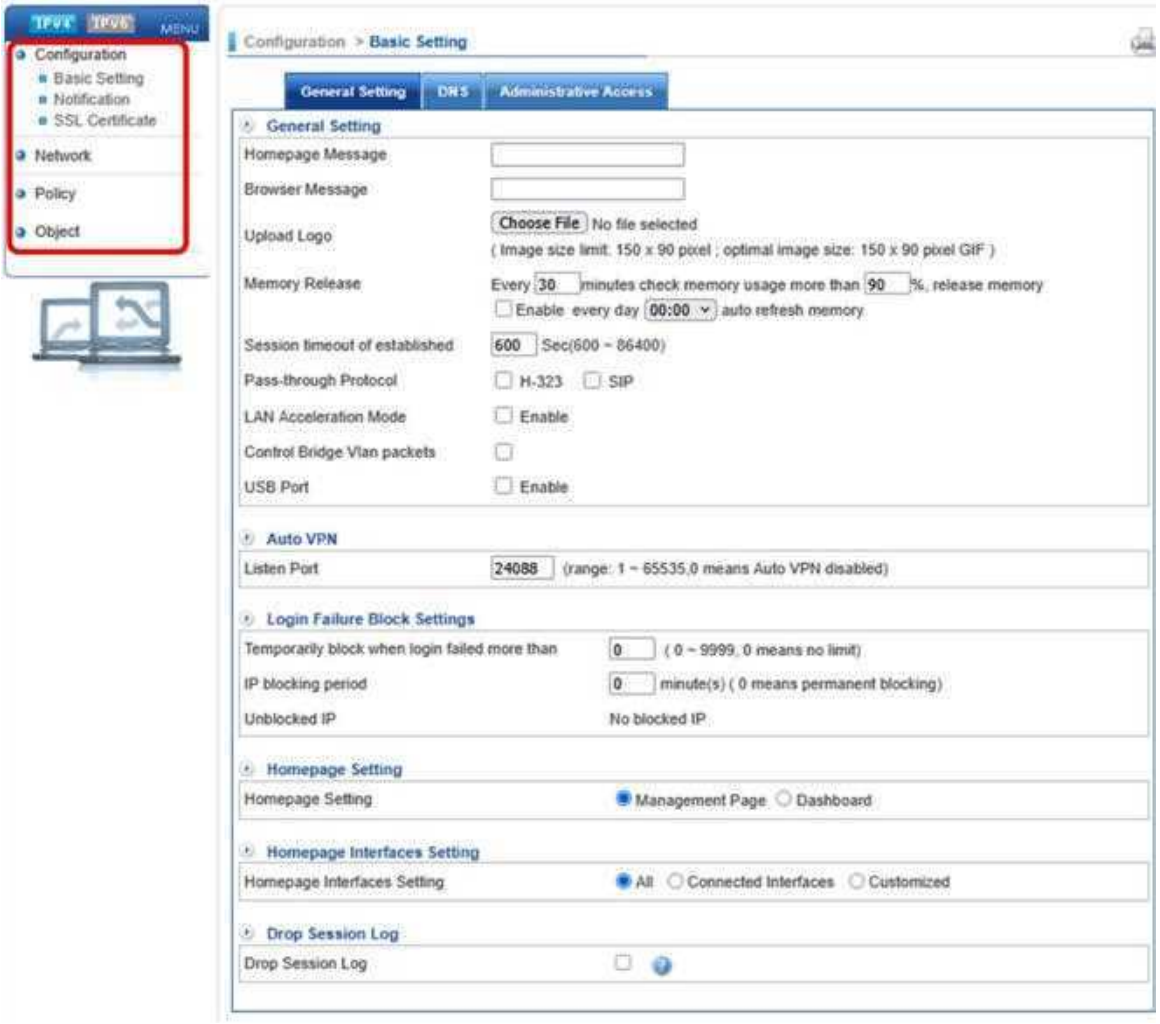


Figure 2-9

C. When an account with **Write** privileges logs into the management interface, the menu items are visible, and the **Confirm** and **Save** buttons are available. (See Figure 2-10)

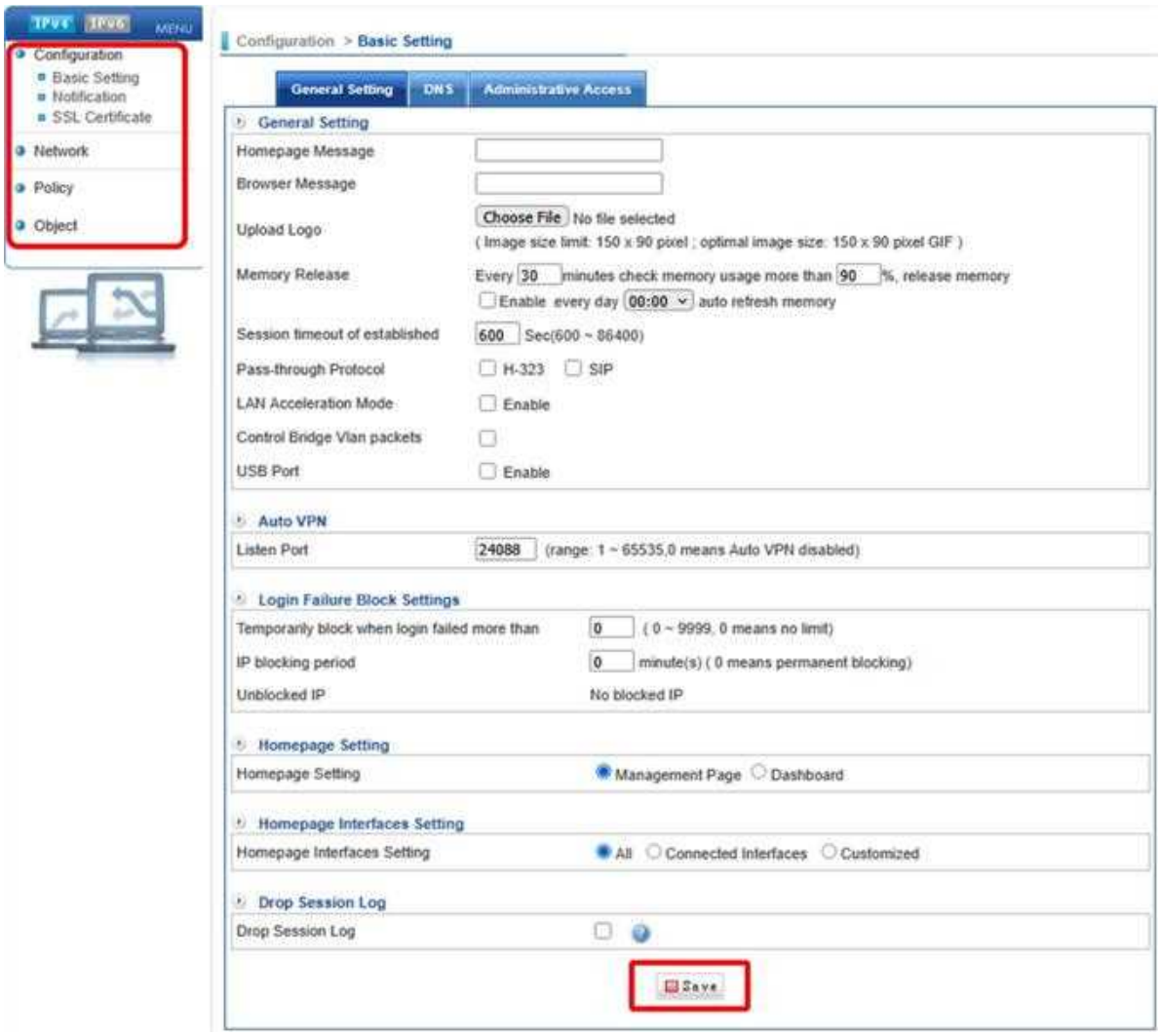


Figure 2-10

2-3-2. IP Address

The 3100-6GT-I enables the restriction of specific source IP address from accessing the management interface, thereby decreasing the risk of unauthorized individuals attempting to guess account credentials. The default setting is blank, which means there's no limitation on source IP addresses. Thus, any internal or external network source IP address can access the management interface.

The 3100-6GT-I may be configured to function in **Bridge** or **NAT** mode based on environmental requirements. Therefore, when specifying source IP addresses, careful consideration must be given to the network architecture in which the device resides. For instance, if internal IP address is configured to access the management interface but no source IP address for external networks, connections from external networks will be denied.

Once an IP address is configured, it activates this filtering mechanism, allowing only matching source IP addresses to access the interface. Therefore, **administrators must ensure their own IP addresses are included in the configuration** to prevent being locked out of the management interface.

When adding the first source IP address, it typically includes the IP address of the current administrator. Failing to do so will result in being unable to access the management interface after saving (as the source IP address is not permitted).

Add Manager IP Address and Netmask

Click the "Add" button to access the page for adding new source IP address. The process is as follows: (See Figure 2-11)

- **[Notes]**: Set up recognizable name for source IP address.
- **[IP Address and Netmask]**: Both legal and private IP addresses in a certain section can access the management interface. When setting up, it's important to notice the netmask. **Legal IP addresses** typically utilize 255.255.255.255, denoting a fixed IP address. **Private IP addresses** commonly employ 255.255.255.0, representing the source IP address of a specific internal zone.

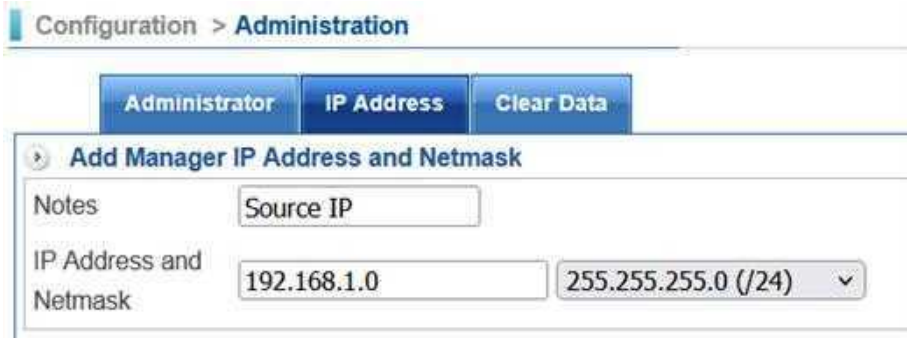


Figure 2-11

Administrators generally begin by registering their internal network IP address to ensure uninterrupted access to the management interface, followed by the addition of other IP addresses.

Should the administrator's own subnet be omitted, access to the management interface via the network will be denied. In such cases, entry through the **console** interface is required to disable the restriction before network-based access can be reestablished.

2-3-3. Clear Data

The 3100-6GT-I stores enormous data, including records of administrator logins, logouts, and actions on the device, as well as user activity passing through the device, such as email, WEB/HTTPS, system operations, and protection logs including firewall attack/defense records, OPC, and virus incidents. When the data reaches a certain threshold, either based on capacity or time, the system must clear them.

1. Smart Clear Settings

When the data storage usage meets the following conditions, the system will automatically adjust the record retention settings and clear the records:

(1) Data storage usage rate reaches certain value (80~99%)

(2) Database usage exceeds 40% of the data storage.

- **[Enable]**: When enabled, the system will automatically adjust the content retention time below when the system capacity usage rate reaches the set value.
- **[Record Retention Period Log]**: After enabling the Smart Clear Settings, each automatic adjustment of record retention time will be recorded here.
- **[Automatically Clear Data]**: When the record retention time reaches the minimum value and the capacity is still insufficient, records will be cleared starting from the database with the highest usage until the capacity is sufficient.
- **[Clear Data Log]**: A log will be kept here for each automatic content clearing event.

2. Clear Data

This menu refers to **[Manual Record Clearing]**, which administrators may use when they deem it necessary to purge certain system records. The number of log categories varies by model, with up to 11 categories supported.

Administrators can clear specific logs as required or select **[Select All]** to remove all entries. Upon pressing the “Clear” button, all chosen data stored in the 3100-6GT-I will be deleted, and the system will resume logging from a clean state.

3. Data Retention Period

The 3100-6GT-I utilizes built-in storage to maintain system records. An automatic threshold is applied, with the clearing mechanism activated once storage usage exceeds approximately 90%.

By default, the system retains records for 15 days, though administrators may configure the retention period within a range of 1 to 31 days to suit operational requirements.

Certain high-volume logs that are not critical to system operation, such as mail filtering, traffic statistics, and DNS query logs are stored for shorter durations.

2-4. Upgrade

As the 3100-6GT-I does not include an internal hard drive, firmware updates require downloading the firmware to a PC and subsequently uploading it to the 3100-6GT-I for installation.

2-4-1. Firmware Message

1. Firmware Message

This function automatically checks for new firmware. Once a new version is detected, the administrator should log into the management interface, download the firmware to a local PC, and manually upload it to the 3100-6GT-I to complete the upgrade process. (See Figure 2-12)

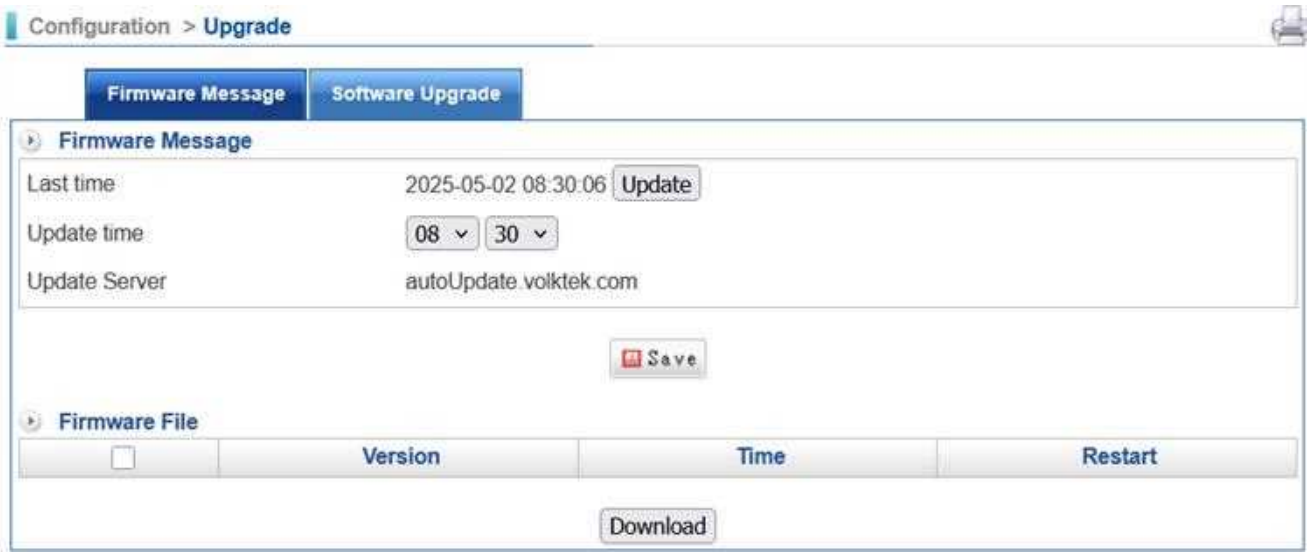


Figure 2-12

- **[Last time]**: The timestamp of the most recent firmware check. If the administrator wants to verify whether new firmware is currently available, clicking the **Update** button will prompt the 3100-6GT-I to immediately contact the update server.
- **[Update Time]**: Sets the time for the device to perform daily firmware checks. This setting only defines the check time—it does not trigger a firmware upgrade.
- **[Update Server]**: It is the server that the 3100-6GT-I uses to check for the latest firmware. This is system-defined and cannot be modified by the administrator. The default server address is: autoUpdate.volktek.com.

2. Firmware File

After the 3100-6GT-I checks with the update server, the latest available firmware version will be displayed if an update is found. Since the 3100-6GT-I does not have a built-in hard disk, the administrator must manually download the firmware to a local computer. (If multiple versions are available, each version must be updated sequentially.)

Firmware updates typically take about three minutes. The system will automatically reboot after the update is complete. Do not power off the device, disconnect the network, or leave the webpage during the update process, as this may result in unexpected update failures.

2-4-2. Software Upgrade

Software Upgrade

The firmware must first be obtained and then manually uploaded to the 3100-6GT-I.

- **[Server Model]**: The model name of the device, 3100-6GT-I.
- **[Software Version]**: The current software version running on the 3100-6GT-I. Version 9.0.2.4 is the initial release, and newer versions have higher version numbers. The current version is 9.0.2.4.
- **[Software Upgrade]**: Select the firmware file to upload to the 3100-6GT-I.

Once the upload button is clicked, the system will begin the upgrade process.

Upgrade Log

All firmware upgrade actions are recorded in the **Upgrade Log**, including the date, time, and the user who performed the upgrade. For example:

- 2025-04-27 12:37:24 → 9.0.2.2 to 9.0.2.3

  Indicates a version upgrade performed on April 27, 2025.

- 2025-05-12 11:09:08 → 9.0.2.3 fix language files

  Indicates that the update on May 12, 2025 was a patch to fix language files.

2-5. Backup & Restore

Once the 3100-6GT-I has been properly configured and is operating normally, the administrator should back up all configuration data and store the backup file separately for future use. If the hardware specifications are the same, the backup file can be imported to another 3100-6GT-I to restore the configuration.

There are two options for saving the backup file:

1. Save to a USB drive
2. Download to the computer's local storage

2-5-1. Backup & Recovery

All backup and restore operations are performed manually. The system only backs up the current configuration at the time of execution. The 3100-6GT-I supports two backup modes: USB drive and Backup File.

1. **USB drive**: The configuration file is directly saved to a connected USB drive.
2. **System Backup**: The configuration file is saved to the administrator’s computer as a local file.

These two backup methods serve different purposes and have slightly different procedures when restoring. Administrators can use both methods as needed.

System Backup to USB

Insert a USB drive into the device and click the backup button. The system will automatically detect the USB drive and, if present, copy all configuration files to it. Once the backup is complete, the USB drive can be safely removed.

When the device restarts, it will check for the presence of a USB drive. If a valid USB backup is detected, the system will automatically restore the configuration files. This USB backup function is designed to quickly restore the device to its original configured state.

Each time the 3100-6GT-I reboots, it will automatically detect whether a backup USB drive is connected. If found, the system will load the backup file from the USB drive and perform a configuration restore.

This feature is especially useful when replacing faulty hardware: inserting the original backup USB into a new device will restore it to the same configuration as the original unit.

System Backup

By clicking the backup button, the administrator can export the current system configuration. The 3100-6GT-I will compress the entire configuration data into a **.tgz** format compressed file. To restore the system, simply import this file—once uploaded, the system will revert to the exact state at the time the backup was created. (See Figure 2-13)

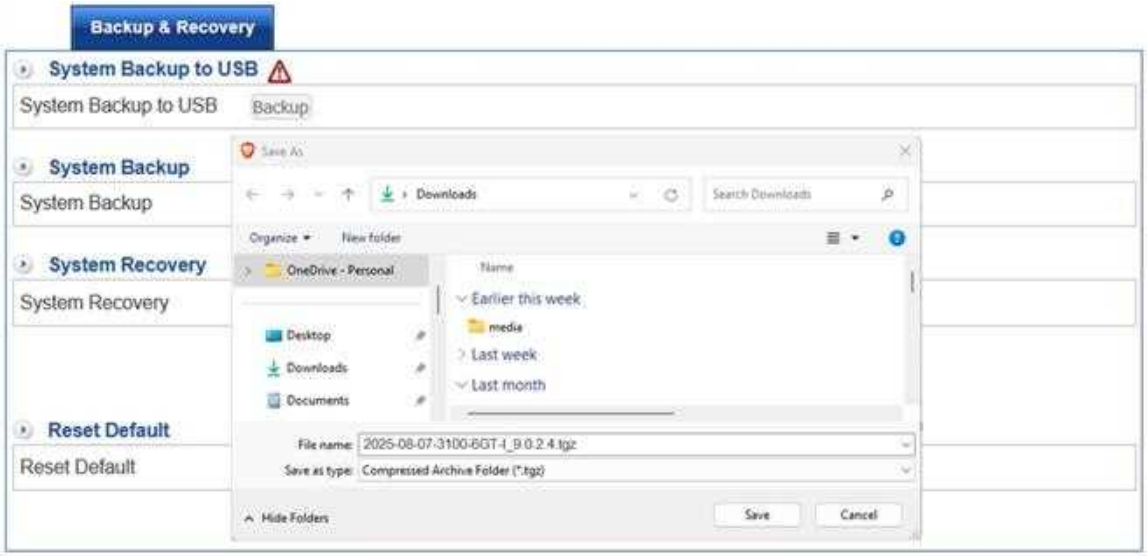


Figure 2-13

System Recovery

The administrator selects the configuration file to be restored. The file must be in **.tgz** compressed format. After selecting the file, click the confirm button to begin the upload. During the upload process, the 3100-6GT-I will automatically verify the integrity of the configuration file. If the file is found to be corrupted, the restore process will be aborted.

Only when the file passes validation will the system extract and restore the configuration. After rebooting, the 3100-6GT-I will return to the exact state captured at the time of the backup.

Reset Default

The administrator can restore the device to its factory default settings. After clicking the “OK” button, the 3100-6GT-I will erase all configuration data and reset the IP address of LAN Port 1 to 192.168.1.1.

- **[Reset Default] > [Keep Interface Setting]**: This option determines whether to retain the existing IP configurations of network interfaces when performing a factory reset. If enabled, the system will revert to factory defaults but preserve all IP address settings.

  This feature is useful when the network topology remains functional, but policy settings or internal configurations have become too complex. In such cases, administrators can reset all non-network settings while keeping the original network configuration intact.

2-6. Notification

The 3100-6GT-I can notify administrators via email about all system events—ranging from critical issues such as security attacks to routine operations like backup success or failure—allowing administrators to monitor the device and network status in real time.

The notification mechanism is email-based, so administrators must first configure the SMTP server settings and recipient email addresses. Only after these settings are completed will the 3100-6GT-I be able to send notifications immediately when events occur.

2-6-1. Notification

When an event occurs, the 3100-6GT-I sends an email notification to the administrator. Different events can be configured to use different sender accounts, and each notification can be sent to multiple recipients.

Notification

The 3100-6GT-I supports a total of 20 event types for email notifications. Each event can be configured for either **periodic** or **scheduled** checks. If an issue is detected during a check, the system will send a notification email to the recipients specified by the administrator. (See Figure 2-14)

Figure 2-14

- **[Sender Account]**: Choose the sender account to use when sending notification emails. Sender accounts are configured on the “SMTP Server” tab. There are two available modes: Automatic and Customed SMTP Account

  Automatic:

  When selected, the system will prioritize using a sender account from “SMTP Server” tab that matches the recipient's domain name.

  For example, if there are two sender accounts configured—a@abcd.com and b@ghij.com—and the recipient is kkk@ghij.com, the 3100-6GT-I will automatically select b@ghij.com as the sender.

  If no matching domain is found, the system will use the first available sender account to send the notification email.

  Customed SMTP Account:

  The system uses sender accounts configured under “SMTP Server” tab to send notification emails. If no sender account is configured, no notification emails will be sent.

- **[Recipient]**: Enter the recipient email address for the notification. Each event can have multiple recipients, with one email address per line.
- **[Try to send times]**: Specifies how many times the system will retry sending a notification email if the initial attempt fails.

  The valid range is 1 to 5 attempts. If all attempts fail, the notification email will not be sent.
- **[Notification Language]**: Select the language used in the notification email. Available options are English, Traditional Chinese, and Simplified Chinese. If the language setting is incorrect, the recipient may receive garbled or unreadable content.

Message Notification Items

The 3100-6GT-I currently supports 21 types of event notification emails. Each event check is based on its specific nature, and therefore follows different checking intervals and mechanisms.

For example, “Zone Disconnection” detection is not based on scheduled checks—it relies on periodic real-time monitoring. Another example is the frequency of checks: “Firewall Protection” is checked more frequently than “System Log”, to ensure timely alerts in case of security threats.

Regardless of the event type, the email subject line for each notification can be customized. Administrators can modify the default subject to make it more easily understood by recipients.

For instance, the default subject for a link disconnection event is “Zone Disconnection”, but it can be renamed to something more descriptive like "Taipei 3100-6GT-I Disconnected" so recipients can quickly understand the context of the email.

If a specific notification type is not enabled, the system will not send emails for that event. Note that depending on the device model, the total number of notification items may vary—up to 21 types in some models. A detailed description of each notification type is provided below:

1. **Zone Disconnection**: Check if the Wide Area Network (WAN) connection to the outside is working.
2. **Master-Slave Abnormal Synchronization**: Indicate when there’s a switch between Master and Slave in HA mode or abnormalities during data synchronization between two devices.
3. **Firewall Protection (SYN, ICMP, UDP, PortScan)**: Notify when the 3100-6GT-I faces attack.
4. **Anomaly IP**: Alert when internal computers exceed the set traffic limit.
5. **Virus Blocking (Web, mail, etc.)**: Detect virus in emails or files accessed during web browsing.
6. **System Log**: Indicate changes in system operation logs.
7. **Administrator Login Failure**: Notify when there’s an error during administrator login.
8. **SSL-VPN and Web Authentication Login Failure**: Alert when there’s an authentication failure during SSL VPN user login.
9. **Software Upgrade**: Inform the release of new firmware.
10. **Low Data Space, Usage over 90%**: Alert when available data space is low or there are bad tracks.

11. **Co-Defense (Switch)**: Send notifications about collaborative defense actions with switches and wireless APs.
12. **Database Anomaly**: Alert about abnormalities in the local database.
13. **IPSec Disconnection**: Alert when IPSec VPN disconnect.
14. **IPSec Switchover**: Notifies when any IPSec channel disconnects in an SD-WAN environment.
15. **Authentication Expiration**: Notifies when user accounts for web authentication are about to expire.
16. **Remove Expired Authentication**: Alert before deleting expired web authentication accounts.
17. **Traffic Quota Ran Out**: Alert when configured traffic quotas are about to be exhausted.
18. **UPS Log**: Record communications with UPS.
19. **CMS (client's mgmt. requests, abnormal connection status, backup failed, recovery failed)**: Send notifications related to CMS operations.
20. **Abnormal System Space Usage**: Alert when system storage space is too low or quickly fills up.
21. **Abnormal System Shutdown**: Alert when system encountered abnormal shutdown.

2-6-2. Notification Log

The 3100-6GT-I records every message notification, regardless of its success or failure, for future reference by administrators. (See Figure 2-15)

Search Notification Log

1. **[Date]**: Search for notification records within a specified time frame.
2. **[Event]**: Select specific event items or view all events.
3. **[Recipient]**: The recipient of the message notification. "*" can be used as a wildcard search keyword, for example: *@abcd.com.

Figure 2-15

2-6-3. SMTP Server

To send notification emails, the 3100-6GT-I requires at least one valid sender account configured in the "SMTP Server" settings. If no valid sender account is set, all notification emails will fail to be sent. Administrators can configure multiple sender accounts.

When the **[Sender Account]** in the "Notification" tab is set to **Automatic**, and more than one sender account is available, the system will automatically match the domain of the recipient's email address with the domains of the configured sender accounts.

If a match is found, the system will select the sender account with the same domain. If no matching domain is found, the system will use the first valid sender account. If the first attempt fails, the system will try the next available sender account, continuing until it either successfully sends the email or reaches the maximum retry attempts.

Add SMTP Server

1. **[Sender Alias]**: The default name is "Admin". Check "Customize" to change it to a name that recipients can easily recognize, such as "Notifications from the 3100-6GT-I".
2. **[Sender Name]**: The sender's name displayed in the notification email to the recipient.

   This is the display name, not the sender account. Most email clients will display the sender's name. If the sender's name is not set, the email account will be displayed as the sender's name.
3. **[Mail Server IP Address]**: The SMTP mail server hostname. For example, abcd.com or 211.22.22.22.
4. **[Port]**: SMTP is TCP 25, SMTPS is 465 or 587, depending on the SMTP server.
5. **[Account]**: The account used to log in to the SMTP mail server. Enter the account or full email address, for example, jean or jean@abcd.com.
6. **[Password]**: The password for the sender account on the SMTP mail server.
7. **[Authentication]**: Check if the SMTP mail server requires account authentication.
8. **[TLS]**: Select whether to enable TLS based on the requirements of the SMTP mail server. (TLS provides authenticity, integrity, and confidentiality over the Internet.)
9. **[Delivery Domain Name]**: The sender's domain used for sending emails. It typically needs to match the recipient's domain to avoid issues with filtering.

   For example, if the sender's account is a@ghij.com and only sends emails to ppp@ghij.com, enter ghij.com here to indicate that the sender's account will not send notification emails to domains other than ghij.com.
10. **[Bind specific Source IP]**: Some mail servers only serve specific sender IP addresses. Enter the specified IP address of the mail server here.

Sender Account Verification and Email Sending

After configuring the SMTP sender account, administrators can verify the correctness of the settings using the SMTP Test Mail function, to ensure that recipients will be able to receive notification emails without issues.

Under “SMTP Server” tab, the 3100-6GT-I displays detailed information for each configured sender account. In the “SMTP Test Mail” section, click the “Test” button to open a dialog box. Enter the recipient’s email address in the dialog box. (See Figure 2-16)

For example, enter jordan@abcd.com. After clicking “Confirm”, if the sender account settings are correct, the recipient (jordan@abcd.com) will receive a test email with the subject line: “This is an SMTP Test Mail”. This confirms that the SMTP server configuration is valid and that notification emails will be sent successfully.

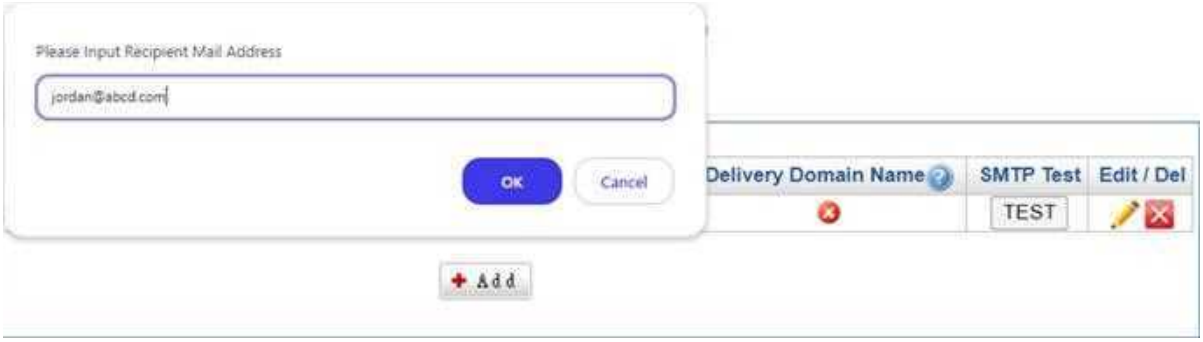


Figure 2-16

2-7. Reboot and Power Off

The 3100-6GT-I provides two buttons for performing normal power on/off operations. In addition, to enhance operational stability, the system supports scheduled reboots at regular intervals.

2-7-1. Reboot & Power Off

This is the normal startup and shutdown procedure for the 3100-6GT-I. The system provides two buttons: **“Reboot”** and **“Power Off”**.

1. **Reboot**: When the Reboot button is clicked, the system will terminate all running services, restart the device, and reload the information stored in the configuration file.
2. **Power Off**: When the Shutdown button is clicked, the 3100-6GT-I will power off following the normal shutdown process.

2-7-2. Auto Reboot

The system supports automatic periodic reboots. Rebooting helps clear unnecessary or corrupted temporary files occupying memory, thereby improving system stability. The reboot interval can be set to daily, weekly, or monthly. In most cases, rebooting once per month is sufficient.

- **[Enable]**: Enables the automatic reboot function. The default setting is **Disabled**. A “Log” button is provided on the right side to record reboot time and status (success or failure).
- **[Recurrence]**: Defines the reboot cycle. Options are **Every Day**, **Every Week**, or **Every Month**. Under normal operation, a monthly reboot is recommended.
- **[Reboot Time]**: Specifies the exact time for executing the reboot, typically scheduled during off-peak hours when the system is not providing services.

2-8. Signature Update

The 3100-6GT-I relies on packet signature matching to determine whether network traffic is normal or potentially harmful. Volktek periodically distributes updated signatures to each device, ensuring that all data remains up to date.

Currently, the system includes one automatically updated database: **OPC**. (See Figure 2-17)

Figure 2-17

The administrator can also click the **"Update"** button or manually upload the signature file.

2-9. SSL Certificate

During network data transmission, SSL encryption is used to ensure security. The 3100-6GT-I also makes extensive use of the SSL protocol. In the SSL encryption process, certificates are required to verify authenticity.

In general, SSL certificates include Server Certificates, Root Certificates, and Intermediate Certificates. Whether obtained from a trusted Certificate Authority (CA) or self-signed, once the certificate is imported into the client computer, the operator's computer will no longer display certificate error warnings.

SSL Certificate Message

SSL certificates can be obtained from three different sources. One option is to apply for a trusted certificate from a Certificate Authority (CA) and manually import it using the **"SSL Certificate Import"** function. Another option is to manually create a private SSL certificate through the **[SSL Certificate Set]** menu. Finally, administrators may choose to use a certificate issued by Let's Encrypt, which provides free and trusted certificates; however, the limitation of this method is that the certificate must be renewed every 90 days.

SSL Certificate Set

1. Manual Input

Choose "Manual Input" in **[SSL Certificate Set]** to create a self-signed private certificate. Once the certificate has been created, it can be downloaded and imported into the operator's computer, preventing certificate error warnings from appearing. The following is a configuration example:

Two-letter Country Codes: TW

State/Province: TAIWAN

City: TC

Organization Name: L7FW

Unit Name: L7FW

Domain Name: www.example.com

Application Personnel Email: help@example.com

After the input, download the **server.csr** files and import it into the browser. In the browser's certificate viewer, the following information will be displayed. (See Figure 2-18)

Figure 2-18

2. Importing SSL Certificates

In addition to self-signed server certificates, it is also possible to import certificates obtained from an external Certificate Authority (CA). Only Server Certificates and Intermediate Certificates are supported in this section.

3. Let's Encrypt Certificates

Let's Encrypt is a trusted Certificate Authority (CA). The 3100-6GT-I simplifies the application process—administrators only need to submit a request and configure the corresponding DNS settings to complete the setup.

Each certificate issued by Let's Encrypt is valid for 90 days, and the system will automatically renew the certificate before it expires. (See Figure 2-19)

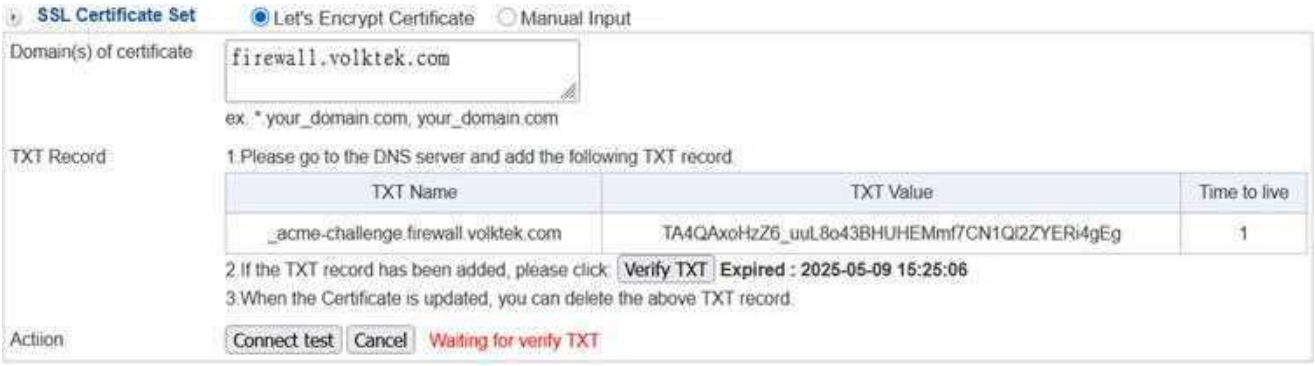


Figure 2-19

- **[Domain(s) of certificate]**: Enter the domain name for which the certificate will be requested. After clicking "Apply Certificate", the system will automatically send a request to Let's Encrypt.
- **[TXT Record]**: Once the request is successful, Let's Encrypt will issue a TXT value. The administrator must add a TXT record to the DNS server. For example, the TXT name could be _acme-challenge.m2chat.com.tw, and the corresponding TXT value should be entered under this name.

After Let's Encrypt validates the TXT record, the trusted certificate will become available for use.

2-10. Uninterruptible Power System

To prevent hardware damage caused by sudden power outages—such as motherboard failure—the 3100-6GT-I supports integration with an Uninterruptible Power Supply (UPS).

In the event of a power failure, if the UPS power level drops below the configured threshold, the system will automatically initiate a shutdown procedure to protect the valuable data stored within the device.

2-10-1. Uninterruptible Power System

The 3100-6GT-I supports three connection methods with an UPS devices: SNMP, USB, and network-enabled UPS devices.

When using USB or a network-enabled UPS connection, the system will display a list of Volktek-verified brands and models. When SNMP is selected, the system communicates with the UPS via the SNMP protocol. Currently, SNMP v1/v2c/v3 are supported.

Administrators must first select the desired operating mode under **[Connection Mode]**, as each mode requires different configuration settings.

Setup

1. **USB Connection Mode**

   In USB connection mode, the 3100-6GT-I can also serve as a communication bridge between the UPS and other devices. UPS status information can be transmitted over the network, allowing other devices on the network to access and utilize the data. (See Figure 2-20)

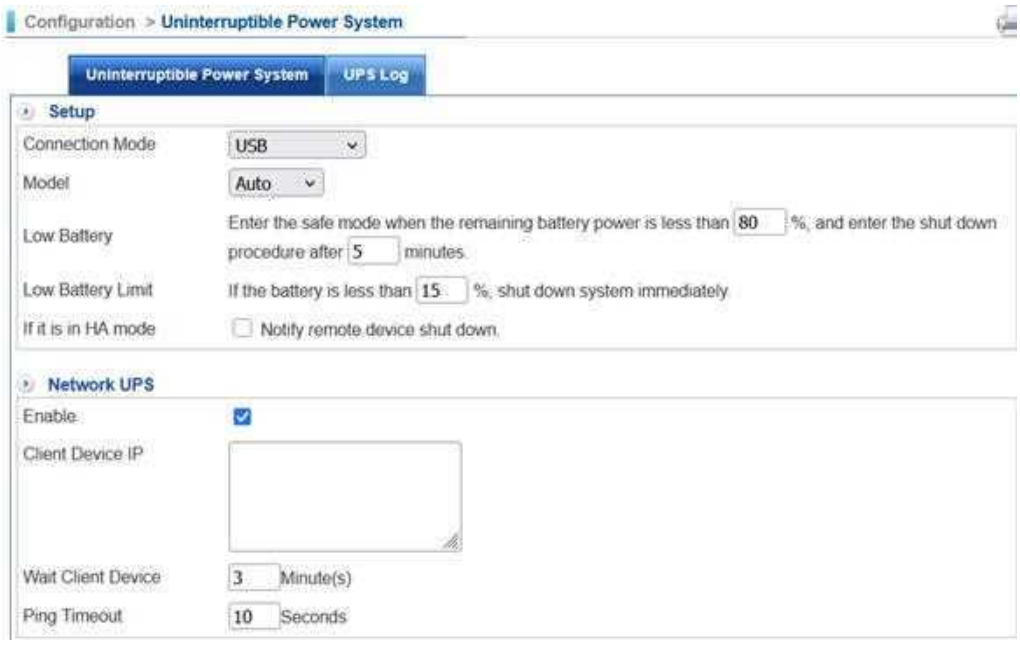


Figure 2-20

- **[Model]**: Select the UPS model. Two options are available: Automatic and Custom.

  Automatic: The system automatically communicates with the configured IP address, and the detected model will be displayed under **[UPS Information]**.

  Custom: Select a model from the list of Volktek-verified UPS models. Currently, five UPS models have been verified.

- **[Low Battery]**: When the UPS battery level falls below the configured threshold (default: 80%), the system enters safe mode. At this point, external backup mechanisms are disabled, and after the configured delay (in minutes), the system will proceed with a shutdown sequence.
- **[Low Battery Limit]**: If the UPS battery level drops below this setting, the system will immediately initiate a shutdown.
- **[If it is in HA mode]**: In HA mode, the system will notify the paired device to perform a synchronized shutdown.

2. **Network UPS Connection Mode**

- **[Model]**: Select the UPS model. Two options are available: Automatic and Custom.

  Automatic: The system automatically communicates with the configured IP address, and the detected model will be displayed under **[UPS Information]**.

  Custom: Select a model from the list of Volktek-verified UPS models. Currently, five UPS models have been verified.

- **[Network UPS IP/port]**: Enter the IP address and port number of the UPS. The system will then automatically communicate with the UPS.
- **[Low Battery]**: When the UPS battery level falls below the configured threshold (default: 80%), the system enters safe mode. At this point, external backup mechanisms are disabled, and after the configured delay (in minutes), the system will proceed with a shutdown sequence.
- **[Low Battery Limit]**: If the UPS battery level drops below this setting, the system will immediately initiate a shutdown.
- **[If it is in HA mode]**: In HA mode, the system will notify the paired device to perform a synchronized shutdown.

3. **SNMPv1 Connection Mode**

- **[UPS Device IP]**: Enter the IP address and port number of the UPS. The system communicates with the UPS automatically using the SNMPv1 protocol, and the retrieved status information will be displayed under **[UPS Information]**.
- **[Low Battery]**: When the UPS battery level falls below the configured threshold (default: 80%), the system enters safe mode. At this point, external backup mechanisms are disabled, and after the configured delay (in minutes), the system will proceed with a shutdown sequence.
- **[Low Battery Limit]**: If the UPS battery level drops below this setting, the system will immediately initiate a shutdown.
- **[If it is in HA mode]**: In HA mode, the system will notify the paired device to perform a synchronized shutdown.

4. **SNMPv2c Connection Mode**

- **[UPS Device IP]**: Enter the IP address and port number of the UPS.
- **[User name]**: Enter the SNMPv2c account configured on the UPS. The system will communicate with the UPS automatically using the SNMPv2c protocol, and the retrieved status information will be displayed under **[UPS Information]**.
- **[Low Battery]**: When the UPS battery level falls below the configured threshold (default: 80%), the system enters safe mode. At this point, external backup mechanisms are disabled, and after the configured delay (in minutes), the system will proceed with a shutdown sequence.

- **[Low Battery Limit]**: If the UPS battery level drops below this setting, the system will immediately initiate a shutdown.
- **[If it is in HA mode]**: In HA mode, the system will notify the paired device to perform a synchronized shutdown.

5. **SNMPv3 Connection Mode**
   - **[UPS Device IP]**: Enter the IP address and port number of the UPS.
   - **[User name]**: Enter the SNMPv3 account configured on the UPS. The system will communicate with the UPS automatically using the SNMPv2c protocol, and the retrieved status information will be displayed under **[UPS Information]**.
   - **[Authentication Passphrase]**: The password used for SNMPv3 account authentication. Supported authentication methods are **SHA** and **MD5**. These settings must match the configuration on the UPS host.
   - **[Privacy Passphrase]**: The encryption key used for SNMPv3 data transmission. Supported encryption modes are **DES** and **AES**. These settings must also match the configuration on the UPS host.
   - **[Low Battery]**: When the UPS battery level falls below the configured threshold (default: 80%), the system enters safe mode. At this point, external backup mechanisms are disabled, and after the configured delay (in minutes), the system will proceed with a shutdown sequence.
   - **[Low Battery Limit]**: If the UPS battery level drops below this setting, the system will immediately initiate a shutdown.
   - **[If it is in HA mode]**: In HA mode, the system will notify the paired device to perform a synchronized shutdown.

Network UPS Server

In USB and SNMP modes, the 3100-6GT-I can also serve as a communication bridge between the UPS and other devices. UPS status information can be transmitted over the network, allowing other devices to utilize it.

- **[Enable]**: By default, this function is disabled. When disabled, the UPS is accessible only to the local device.
- **[Client Device IP]**: The IP address of the device that requires UPS information. A notification will be sent to this device when the UPS battery is low.
- **[Wait Client Device]**: The amount of time required for the remote device to shut down. The 3100-6GT-I will wait for this duration before initiating its own shutdown procedure.
- **[Ping Timeout]**: The 3100-6GT-I uses ICMP (PING) to verify whether the remote device is still alive.

2-10-2. UPS Log

All communication logs between the system and the UPS are recorded here.

2-11. CMS (Central Management System)

In simple terms, once a central device is configured as the CMS Server, it can manage all remote 3100-6GT-I units.

Although CMS and cloud management services both provide similar device management functions, their operations differ:

1. CMS requires the central device to have a **fixed IP address** or **DNS hostname** so that remote clients can locate it.
2. The central-end of CMS requires a 3100-6GT-I with a **hard drive**.
3. CMS **cannot manage mail servers**.

The Volktek CMS provides essential functions for remote configuration management, including system backup, data restore, and firmware updates. This allows administrators at headquarters to centrally manage multiple remote devices based on their needs or according to scheduled tasks. In addition, the Log function provides detailed records of events on monitored devices, enabling administrators to track the latest operational status.

As illustrated in the CMS system diagram (See Figure 2-21), each remote 3100-6GT-I reports its current status and configuration to headquarters. Administrators at headquarters can then monitor the real-time status of all remote devices and intervene when necessary.

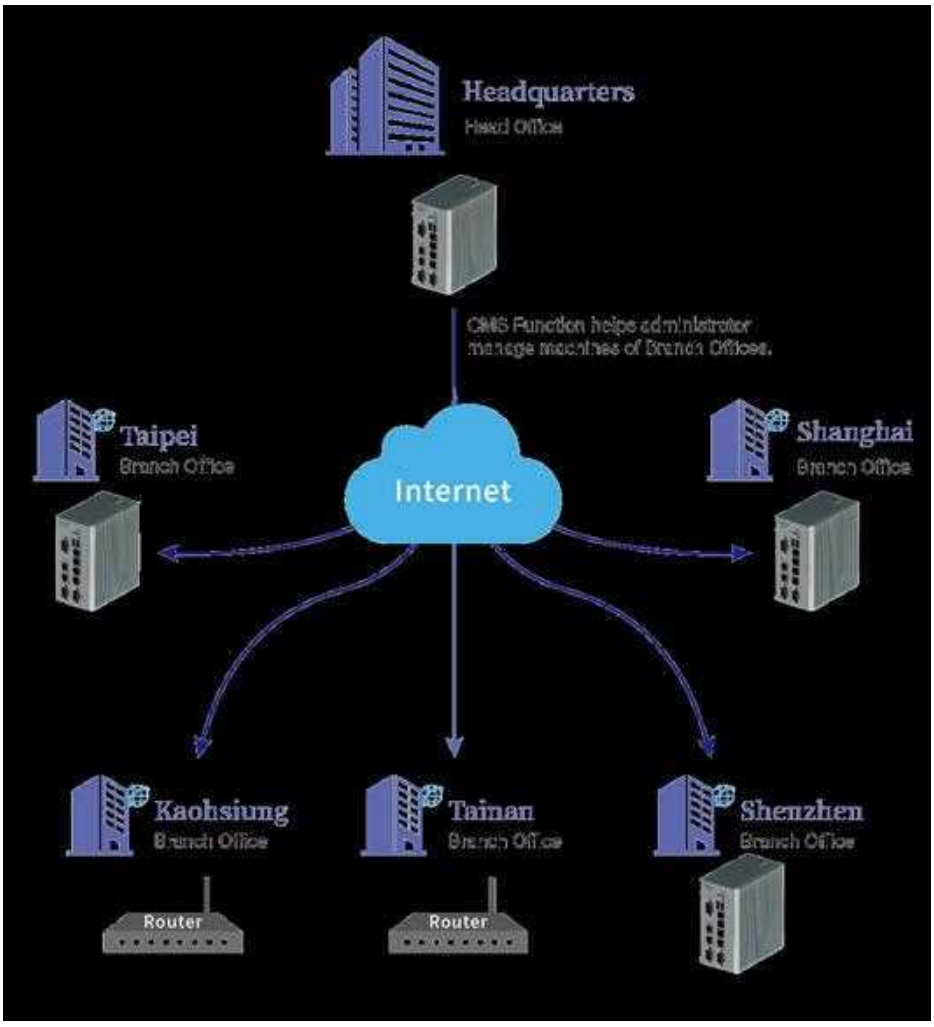


Figure 2-21

2-11-1. CMS Setting

Each 3100-6GT-I in the CMS system can function either as a Client or as a Server. The operating principle of CMS is straightforward: a device configured as a Client will periodically send messages to the Server, granting the Server management authority over the Client.

1. Client Mode

The operating principle of CMS is straightforward in Client mode. Devices set as Clients periodically send messages to the Server and grant management authority to the Server.

- **[Enable]**: Enables the CMS function.
- **[Mode]**: Sets the CMS operating mode to Client.
- **[Server]**: The domain name or IP address of the CMS Server must be accessible on the internet.
- **[Alias]**: The name displayed for the Client on the Server such as 3100-6GT-I-Taipei.
- **[Update Time]**: How often data is updated to the Server, with a setting range of 1 to 30 minutes.
- **[Administrator Account]**: The administrative privileges are granted by the Client to the Server. The administrator on the Server side uses this account to log into the Client device. If no administrator is specified, access to the management interface via CMS is not possible.

  For detailed administrator privileges, please refer to “Configuration > Administration” settings.
- **[Connect Interface]**: Specify which interface is used to report to the Server. The system automatically lists all outbound interfaces for the administrator to choose from.

2. Server Mode

Configuring this device as the Server also records data sent by Client devices. Therefore, administrators only need to manage the Server to oversee all devices.

- **[Enable]**: Enables the CMS function.
- **[Mode]**: Sets the CMS operating mode to Client.

When the CMS is set up as the server, enabling periodic backup of Client configuration files allows for customization of the backup interval. After backup, in case of Client failure or misconfiguration, the previous settings can be restored through the CMS server.

- **[Enable]**: Enable the backup of Client configuration files.
- **[Automatic Backup Time]**: Specify the interval for periodic backups. Shorter intervals increase system load.
- **[The Number of Backup to Keep]**: Determine the number of backup configuration files to retain. Typically, 5 backups are sufficient, but a higher count occupies more storage space.

2-11-2. CMS Monitor

1. Accepting a Client

After each Client is successfully configured, it sends a **takeover request** to the CMS Server. The administrator on the Server side must approve the request before the CMS Server begins processing the Client's data. (See Figure 2-22)

Figure 2-22

2. Managing Clients

Each Client can be organized into different groups, and the Server will display the real-time status of the devices, as shown in the example below. (See Figure 2-23)

Figure 2-23

- **[Activity]**: The status is color-coded:

  Green: The Client reports to the Server on schedule as configured.

  Orange: The device has missed more than three reports.

  Red: The device is currently disconnected.

  Gray: No update data is available.

- **[Alias]**: The Client name. By default, it follows the Client's own setting, but the Server can rename it as needed.
- **[Model]**: The model of the Client device.
- **[IP]**: The current IP address of the Client.
- **[Real-time monitoring]**: Clicking the icon opens the Client's web management interface. If blank, it indicates the Client has not granted management authority to the Server.
- **[Backup]**: The number of configuration backups stored on the Server. The number is shown in parentheses. By clicking, administrators can view changes or perform a restore operation.
- **[Auto Backup]**: Indicates whether the automatic configuration backup function is enabled.
- **[Action]**: Modify or delete the Client's settings.

- **[Log]**: Includes two categories—Connection and Control.
  - **Connection**: Records communication history between the Client and Server (e.g., connection and disconnection times).
  - **Control**: Records control commands issued by the Server to the Client.
- **[Group Collapse]**: Administrators can click the “Group Collapse” button to instantly switch between group displays.
- **[Backup Now]**: After selecting a Client, clicking the “Backup Now” button triggers an instant backup.

[Action] → Modify Client Information

When the “Modify” button is clicked, the Client’s display information can be updated. (See Figure 2-24)

- **[Model / MAC Address]**: Displays the Client’s model and MAC address. These two fields cannot be changed.
- **[Alias]**: The Client’s name. By default, it follows the Client’s own setting, but the Server can rename it as needed.
- **[Group]**: Defines which group the Client belongs to. You may select from existing groups or choose Custom. If Custom is selected, enter the new group name in the provided field.
- **[Auto Backup]**: Specifies whether to enable the automatic configuration backup function.

Figure 2-24

[Backup] → Backup List

One of the major advantages of the CMS system is its ability to automatically and periodically back up Client configuration files. (See Figure 2-25)

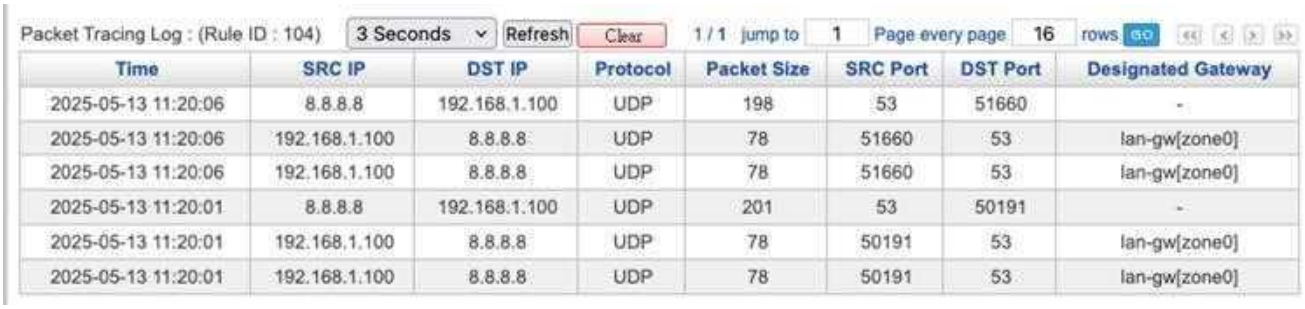
- **[Backup Time]**: The time when the configuration file was backed up.
- **[Version]**: The Client software version at the time of backup.
- **[Download]**: Click the icon to download the configuration file to the local device.
- **[Delete]**: Remove this backup record.
- **[Log]**: Displays which settings were modified in this backup file.

Figure 2-25

[Backup] → [Backup List] → [Restore]

Another advantage of the CMS system is the ability to quickly restore a Client device to a specified state using its backup configuration file. The restore process can also be scheduled to run at a designated time. (See Figure 2-26)

1. From the [Backup List], select the backup configuration file corresponding to the desired restore point.
2. Under [Restore Immediately], click the “Restore” button. The Server will then deliver the selected backup file to the Client device.



Time	SRC IP	DST IP	Protocol	Packet Size	SRC Port	DST Port	Designated Gateway
2025-05-13 11:20:06	8.8.8.8	192.168.1.100	UDP	198	53	51660	-
2025-05-13 11:20:06	192.168.1.100	8.8.8.8	UDP	78	51660	53	lan-gw[zone0]
2025-05-13 11:20:06	192.168.1.100	8.8.8.8	UDP	78	51660	53	lan-gw[zone0]
2025-05-13 11:20:01	8.8.8.8	192.168.1.100	UDP	201	53	50191	-
2025-05-13 11:20:01	192.168.1.100	8.8.8.8	UDP	78	50191	53	lan-gw[zone0]
2025-05-13 11:20:01	192.168.1.100	8.8.8.8	UDP	78	50191	53	lan-gw[zone0]

Figure 2-26

2-12. Data Items

Configure the number of records displayed per page in the UTM. The range is **10 to 50 records**. Each main item may contain multiple sub-items. The sub-item page size setting takes effect only when **[Detailed Settings]** is selected; otherwise, the system follows the main item setting. The default display for policy rules is **16 records per page**. (See Figure 2-27)

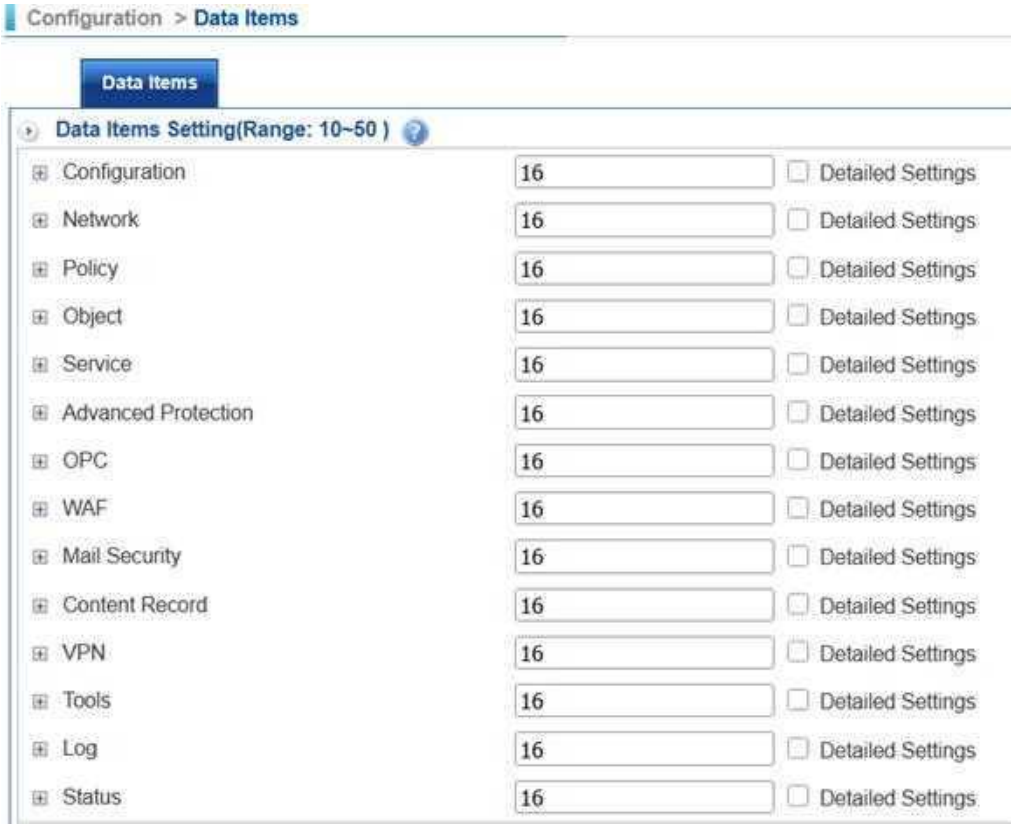


Figure 2-27

Chapter 3. Network

The 3100-6GT-I is not a traditional firewall; it is designed based on the concept of a router. Instead of distinguishing between the typical LAN, DMZ, and WAN, it adopts a **Zone-to-Zone control model**. However, to align with common user conventions, the system still adjusts the naming and related information to resemble the traditional format.

This chapter provides a detailed explanation of how to combine one or more **physical network interfaces**, or even **virtual network interfaces** created via IP Tunnel protocols, into a **Zone**. It also describes how to add **PPPoE** connections as WAN-type interfaces. Additionally, routing management, VLAN configuration, and other router-related features will be covered.

3-1. Zone Setting

By default, the 3100-6GT-I designates **Port 1** as **LAN**. The combination of Port 1 and LAN cannot be deleted by the administrator, but other physical ports may be added to the LAN. The default IPv4 address for the LAN is **192.168.1.1**.

When a Zone consists of more than one physical port, no additional configuration is required for each port within that Zone. All ports inside the same Zone can communicate with each other without restriction.

3-1-1. Zone Setting

The area lists each physical port and its assigned Zone, using colors and numbers to differentiate them. Ports belonging to the same Zone share the same color. If any port is not assigned to a Zone, the administrator can click the **"Add Zone"** button to create a new Zone, or add the unassigned port to an existing Zone.

For example, if **Port-X** needs to be reassigned from **LAN2** to **LAN3**, the administrator must first remove Port-X from LAN2, leaving it unassigned. Then, Port-X can be added to LAN3.

Creating a new zone

If there are empty physical ports not yet assigned to a zone, administrators can add a new zone by pressing **"Add Zone"** button to begin adding a new zone.

- **[Interface]**: Set the interface name, such as LAN, WAN, Bridge, or HA, and a numeric code selected.
- **[Interface Name]**: Select the numeric code for the new ZONE. The system prefixes the ZONE with the code, followed by a number.

  For example: ZONE 0, ZONE 1, etc. Since each physical port can be a separate ZONE, the maximum number represents the number of physical ports on the device. When choosing a number, it can be selected arbitrarily without following any specific order.
- **[Name]**: Add a memorable name for the ZONE, such as Accounting, Engineering, etc.
- **[Color]**: Select the color for the ZONE.
- **[Port]**: Select the physical port(s) for the ZONE. Any port not marked with a number can be selected, and multiple ports can be combined to form a ZONE.

After completing the selection, the system returns to the Zone List. The 3100-6GT-I displays each Zone along with its name, color, and assigned physical ports. To modify a Zone, click the “pencil” icon to enter the edit screen. To delete a Zone, click the “X” icon.

Note that in the Zone List, only **ZONE 0 / LAN** does not have a delete option. (See Figure 3-1)

Zone List : (Click save after completing setting.)

Interface	Interface Name	Name	Color	Port	
LAN	zone0	LAN		Port: 1	
LAN2	zone1	LAN2		Port: 2	
WAN1	zone2	WAN1		Port: 3	
WAN2	zone3	WAN2		Port: 4	
WAN4	zone4	WAN4		Port: 5	
WAN3	zone5	WAN3		Port: 6	

Figure 3-1

Each ZONE listed will appear in the menu of [Network] > [Interface], allowing administrators to configure network settings for that specific ZONE.

3-1-2. Speed and Duplex Mode

Each ZONE in 3100-6GT-I can specify the network speed, and there are two methods for setting the network speed:

1. From [Network] > [Zone Setting] > [Speed and Duplex Mode], administrators can set the network speed from the menu.
2. From the [Port Information] section accessible from the homepage: by clicking on the desired physical port, administrators can adjust the network speed.

- **[Interface]**: Indicate which ZONE this port belongs to.
- **[Port]**: Specify the physical port’s position.
- **[Zone Status]**: Indicate the current connection status of this port. It will display “Disconnected” if no device is connected and “Connected” for a normal connection.
- **[MAC Address]**: Display the MAC address of the physical port.
- **[Speed and Duplex Mode]**: Show the current speed of the network card and record past connection statuses.

  Administrators can manually adjust the network card speed, choosing from options such as 10Mbps, 100Mbps, 1000Mbps, and full or half duplex modes.

3-2. Interface

After completing [Network] > [Zone Settings], all created interfaces will appear in the [Interface] page. Administrators can then proceed to configure network IP addresses, connection speeds, and other network information for each interface. (See Figure 3-2)

Figure 3-2

3-2-1. Network Interface Settings

Except for LAN, the network interface settings for each Zone are the same, as described below (See Figure 3-3):

- **[Interface Name]**: A combination of ZONE + number, where the number is assigned under [Zone Setting].
- **[MAC Address]**: The unique MAC address of the Zone. Within the same 3100-6GT-I, MAC addresses must not be duplicated.
- **[Enable]**: LAN is enabled by default and cannot be disabled. Newly created Zones have three options: Disabled, STATIC, or DHCP.
    1. **STATIC**: The interface IP address must be added under Interface Addresses / PPPoE. Each interface requires at least one IP address.
    2. **DHCP**: The interface IP address is assigned by a DHCP server. Once selected, the Interface Addresses / PPPoE option is automatically hidden.
- **[MTU]**: Defines the maximum packet size in bytes. The default is 1500, with a configurable range of 1400~1500.

Figure 3-3

3-2-2. Control packet in the region between the port

Appears when multi-port mode is set to Bridge:

- **[Network Address Translation]**: Whether to access the internet through other network interfaces.
- **[Source Interface]**: Configuring which physical interfaces within the Bridge need to access the internet through other interfaces.
- **[Source]**: Configuring the network segments included in packets from the source interface.
- **[ARP Reply]**: Conducting ARP Reply when the outbound line detects disconnection.
- **[Designated Gateway]**: After configuring in 3-3-2. Designated Gateway, selectable lines will appear.

3-2-3. Visit Control

- **[Enable Visit]**: Specify whether the interface accepts queries from or allows access to management interfaces from other IP addresses.
  - ✓ **SNMP**: Specify whether the interface accepts SNMP queries. When it's enabled, this interface will send certain information via SNMP protocol to remote SNMP servers.
  - ✓ **Ping**: Specify whether the IP address assigned to this interface that responds to ICMP protocol. When it's enabled, the IP address configured on the interface will respond to ICMP packets.
  - ✓ **HTTPS**: Specify whether the interface accepts access to the management interface via the HTTPS protocol. When it's enabled, all IP addresses configured on the interface can receive HTTPS services.

3-2-4. Firewall Protection

- **[Firewall Protection Items]**: Specify whether this interface should be protected by the firewall. When enabled, the interface IP addresses assigned to this Zone are safeguarded against five types of attacks: **SYN flood, ICMP flood, UDP flood, Port Scan, and Sandstorm**.

  Protections against **SYN flood, ICMP flood, and UDP flood** can be configured under [Object] > [Firewall Protection].

3-2-5. Interface Address / PPPoE

Define the IP address for each physical interface. If **PPPoE** is selected, the system will automatically redirect to the PPPoE configuration page. (See Figure 3-4)

- **[Type]**: Choose between **STATIC** or **PPPoE**. STATIC settings can be configured in this page, while PPPoE settings will redirect to the PPPoE setup screen. For more details, please refer to [Network] > [PPPoE].
- **[Name]**: Assign a recognizable name to this interface such as Wan1:2.
- **[IP Address]**: Add an IP address to the interface.
- **[Subnet Mask]**: Specify the range of the IP address. For example, for a Class C subnet, enter 255.255.255.0.

- **[Default Gateway]**: Specifies the planned IP address and subnet for the interface. Only WAN-type interfaces require a default gateway. For other types, the default gateway field can remain blank, since the configured IP address itself acts as the gateway for Zone users.
- **[Auto set designated gateway]**: When checked, the system will automatically create a default outbound route. Any packets without defined routes will use this default path.
- **[Management IP]**: Specifies whether the IP address on the interface allows administrators to log in for management.

Figure 3-4

3-3. Route

After the administrator configures the IP address and subnet mask under **[Network]** > **[Interface]**, the information is automatically added to the system's default route. The 3100-6GT-I then lists all static routes in the table. The figure below shows an example of the IPv4 static routing table. (See Figure 3-5)

Figure 3-5

"IPv4" indicates that the system is currently displaying/configuring in IPv4 mode. "IPv6" indicates that the system is currently displaying/configuring in IPv6 mode.

These two buttons apply to the entire system. Wherever IP addresses need to be configured, clicking the gray icon will switch the configuration screen between IPv4 and IPv6 modes.

The system's default routing table cannot be modified. To make changes, the administrator must reconfigure the IP address and subnet mask under [Network] > [Interface]. Only manually created routing tables can be exported and imported; system default routes cannot.

3-3-1. Static Routing

In addition to the default routing table generated by network interfaces, the 3100-6GT-I allows the addition of static routing tables. Static routes can be specified to be effective on specific interfaces.

Add a static routing

Press the "Add" button will take you to add a new static route. (See Figure 3-6)

- **[Name]**: A descriptive name for easy identification, for example: "10 Network" or "Default Gateway".
- **[Destination IP]**: Any IP address within the destination network such as 10.10.10.1.
- **[Mask]**: Specify the range covered by the destination network's IP addresses. For example, for a Class C subnet, enter 255.255.255.0.
- **[Gateway]**: Enter the gateway address for the destination network.
- **[Interface]**: Specify which interface the added route belongs to. Upon selecting from the dropdown menu, the system will display all established interfaces for the administrator to choose from.

  The options are color-coded to distinguish between different network interfaces, including **Interfaces (Zone), IP Tunnel, PPPoE dial-up interfaces, VLANs, PPTP, and SSL VPN**.

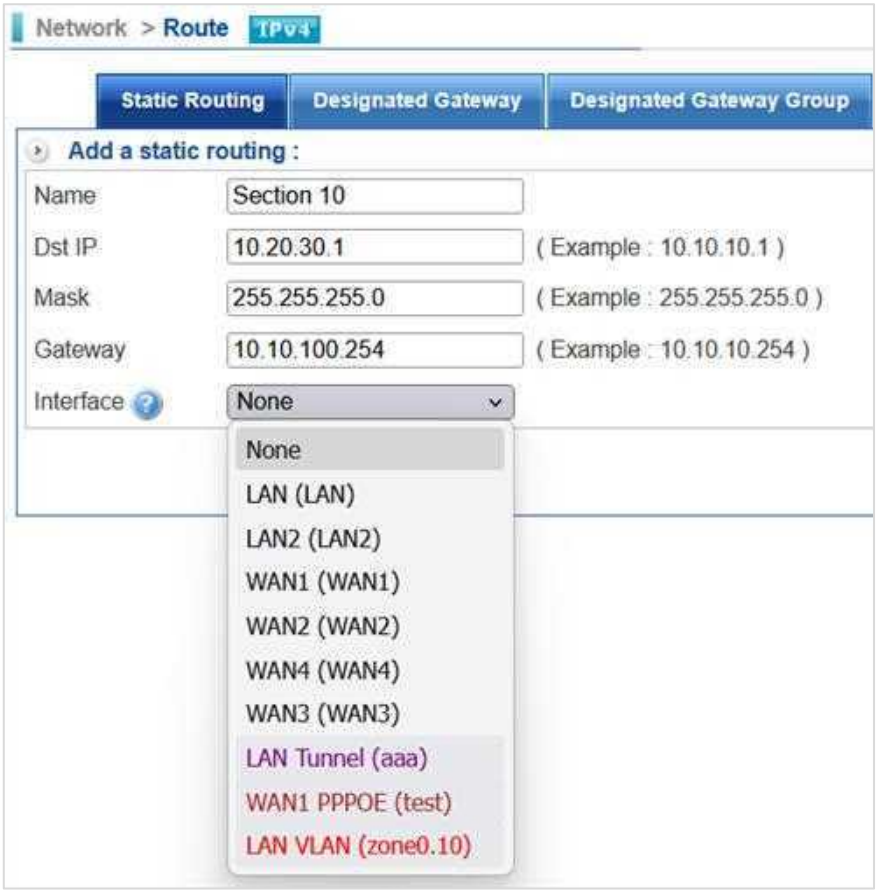


Figure 3-6

If a specific interface is assigned, the static route will only have effect on that interface. If the interface is set to **NONE**, the route will apply to all interfaces on the device. All administrator-defined static routes can be exported or imported.

3-3-2. Designated Gateway

The 3100-6GT-I can connect one or multiple interfaces to WAN lines. To add WAN-type connections, dedicated lines, or MPLS internal VPN connections to the 3100-6GT-I, they must be configured here. This ensures that when packets are transmitted externally, the 3100-6GT-I knows how to forward them to the next gateway.

After administrators create several **Designated Gateway**, they can bind **Designated Gateway** of the same type into a **Designated Gateway Group**. For WAN **Designated Gateway**, each **Designated Gateway** represents a WAN line. Binding several **Designated Gateway** into a **Designated Gateway Group** accomplishes load balancing across the lines.

Each line providing internet connection is an exit route, and there are two methods for configuration:

1. Assigning each external line to a zone.
2. Connecting all external lines to a switch via an external zone. In this case, all external lines are connected to the switch, and you need to configure all IP addresses provided by the external lines in [Network] > [Interface] > [3-2-5. Interface Addresses / PPPoE].

Each method has its advantages. The former one is convenient for management, line recognition, and problem finding. The latter one allows for connection to many external lines, exceeding the port limit of the 3100-6GT-I itself. Pressing the “Add” button will take you to configure exit routes. (See Figure 3-7)

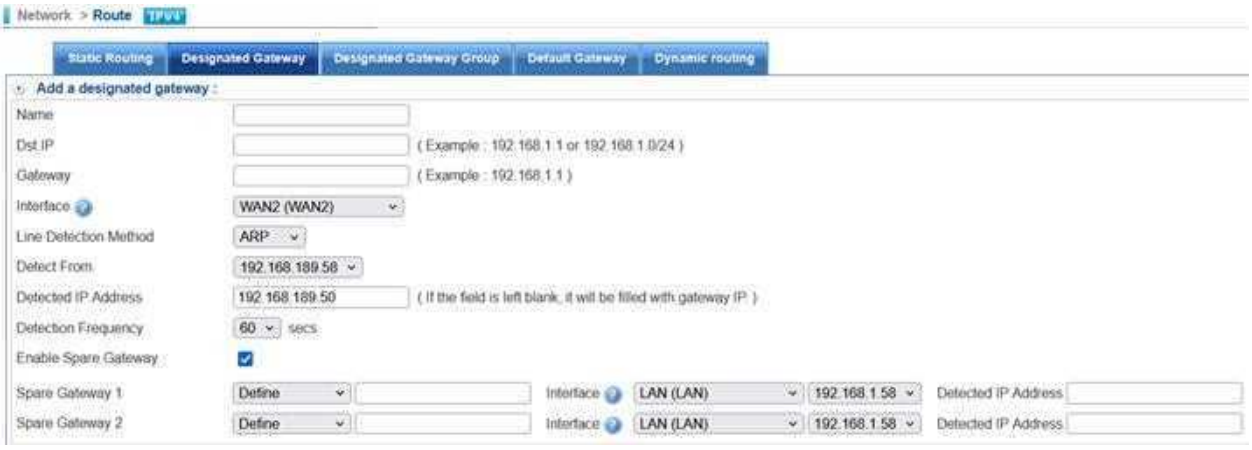


Figure 3-7

- **[Name]**: A descriptive name for the designated gateway, e.g., WAN-1 or PPPoE-1.
- **[Destination Address]**: Optional. Any IP address within the target network. If left blank, it defaults to 0.0.0.0/0. For WAN-type lines, this field is usually left empty.
- **[Gateway]**: Required. The gateway address of the outbound line.
- **[Interface]**: Specifies which interface the outbound line belongs to. Different types of interfaces are color-coded, including Physical Interfaces (Zone), IP Tunnel, PPPoE Dial-up Interface, VLAN, PPTP, and SSL VPN. The drop-down menu lists all available interfaces for selection.
- **[Line Detection Method]**: When the Zone is WAN-type, the system checks whether the line is disconnected. Three methods are available: ARP, ICMP, and DNS. At defined intervals, the 3100-6GT-I sends ARP/ICMP packets or DNS queries to the gateway IP address and determines the line status based on the server's response. The default method is **ICMP**. Selecting NONE disables disconnection checks, and the line is always treated as active.

  For WAN lines using PPPoE, an additional PPPoE detection mode is available, which automatically uses DNS to perform connectivity tests with the PPPoE server.
- **[Detect From]**: Specifies which IP address to use as the source IP for line detection. Typically, this is the IP address assigned to the outbound line.
- **[Detected IP Address]**: Optional. Defines the destination IP address for line detection. If not specified, the system uses the gateway address assigned to the outbound line by default.
- **[Detection Frequency]**: How often to send detection packets. The default is 60 seconds, with a configurable range of 1~999 seconds.
- **[Enable Spare Gateway]**: When the outbound line goes down, traffic is redirected to the redundant **Designated Gateway**, ensuring uninterrupted packet transmission. Up to two redundant gateways can be configured.

  The redundant gateway function differs from the **Designated Gateway Group** load balancing feature. Redundant gateway has no weighting mechanism—when the original line fails, all traffic is redirected to the redundant line.

  In contrast, **Designated Gateway Group** can distribute traffic (e.g., a 100 Mbps connection) across multiple active outbound lines based on configured weights or load balancing policies. With three or more WAN lines, administrators are encouraged to use **Designated Gateway Group**.
- In the **Designated Gateway** list, each WAN-type line or any line with Line Detection enabled maintains connection and disconnection logs. By clicking **"Log"**, administrators can review the line's historical connection status, including disconnection and reconnection times.

3-3-3. Designated Gateway Group

The 3100-6GT-I provides a line load balancer function, treating each outbound line as a WAN-type connection. Based on the selected load balancing mode and assigned weights, network traffic is distributed across the lines accordingly.

By clicking the “Add” button, a new outbound gateway group can be created. Administrators may configure multiple groups as needed, making them available for selection in **[Policy]**.

- **[Group Name]**: A descriptive name for the outbound line group, e.g., WAN-ALL or All External Networks.
- **[Load Balance Mode]**: Defines how network traffic is distributed. Four modes are available:
  1. **Session**: Distributes traffic based on session weighting. For example, if Line A has weight 1 and Line B has weight 2, then one-third of the sessions go to Line A and two-thirds go to Line B.
  2. **Source IP**: Distributes traffic based on the source IP address. Sessions from the same source IP always follow the same path.
  3. **Destination IP**: Distributes traffic based on the destination IP address. Sessions to the same destination IP always follow the same path.
  4. **MINFIRST**: Distributes traffic according to the actual load of each line, assigning more traffic to less-loaded interfaces.
- **[Line break check]**: Specifies the interval (in seconds) to check line availability, used as the basis for line switching.
- **[Designated Gateway]**: Lists the outbound lines and their assigned weights included in this group. All gateways configured under [Designated Gateway] appear here for selection.
- **[Weight]**: Defines the load capacity assigned to each outbound line. For example, if Outbound Line A is assigned weight 1 and Outbound Line B weight 10, the 3100-6GT-I will allocate 1/11 of the traffic to Line A and 10/11 to Line B.

3-3-4. Default Gateway

When no outbound line is configured and no destination IP address is defined in the static routes, packets to those destinations cannot be delivered and will be discarded. To avoid this, a default gateway should be configured on the 3100-6GT-I. All traffic destined for undefined routes will be forwarded to this default gateway.

In addition to the default gateway, in a multi-WAN environment, a backup gateway can be configured. If the default gateway goes down, traffic will automatically switch to the backup gateway.

- **[Detection Frequency]**: Defines how often (in seconds) the system checks the availability of the default gateway. The default value is 10 seconds.
- **[Default Gateway]**: The IP address of the default gateway. All traffic to destinations not defined in the routing table will be forwarded to this gateway.
- **[Interface]**: Specifies which interface the default gateway belongs to. The system lists all available interfaces for selection.
- **[Assign Internet IP]**: When an interface has multiple IP addresses, specify which one will be used as the NAT translation address. Either an existing interface IP or a custom-defined IP may be selected. (See Figure 3-8)

Figure 3-8

[Line Detection Setting] are used to verify whether the device can access the Internet through the specified gateway. Three detection modes are available: **ICMP, ARP, and DNS**. The system periodically sends packets of the selected type to the designated detection IP address and checks for a response.

If no response is received, the device determines that the gateway is down and automatically switches to the next backup gateway. For example, if **ICMP** is selected and the detection IP address is **8.8.8.8**, the system will periodically send ICMP (PING) packets to 8.8.8.8 to verify connectivity. (See Figure 3-9)

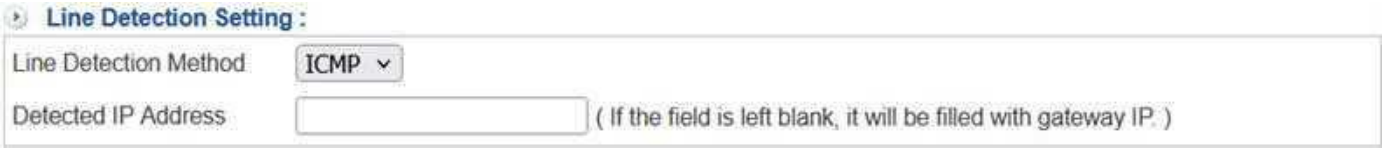


Figure 3-9

3-3-5. Dynamic Routing

The 3100-6GT-I supports the **RIP dynamic routing protocol**. By specifying the interface and route update interval, the device can learn all routing information and make it available to the system.

- **[Interface]**: Select which physical interfaces should enable RIP routing protocol. Multiple interfaces can be selected.
- **[Update Period]**: The interval at which the routing table is updated. Default is 30 seconds, configurable from 30~3600 seconds.
- **[Timeout]**: Defines how long a route remains valid before being considered expired. Default is 180 seconds, configurable from 30~3600 seconds.

All learned routes are displayed in the **[Dynamic Routing List]**.

3-4. VLAN (802.1Q)

VLAN 802.1Q is a fundamental feature in switches, allowing the segmentation of internal networks into several independent subnetworks. Each segment operates independently without interfering with each other.

For example (see Figure 3-10), Switch-A connects to three different subnets: **192.168.1.0/24**, **192.168.2.0/24**, and **192.168.3.0/24**. Three VLAN IDs are configured on Switch-A: **10**, **20**, and **30**. Computers within the same VLAN ID can communicate with each other. However, devices in different VLAN IDs cannot communicate until routing is configured on Switch-A or an upstream network device.

When network packets are sent from Switch-A to the **3100-6GT-I**, the device needs to disassemble and assemble these VLAN-tagged network packets to determine their next destination. This chapter explains how to disassemble VLAN ID settings. The 3100-6GT-I supports up to **4064 VLAN IDs**.

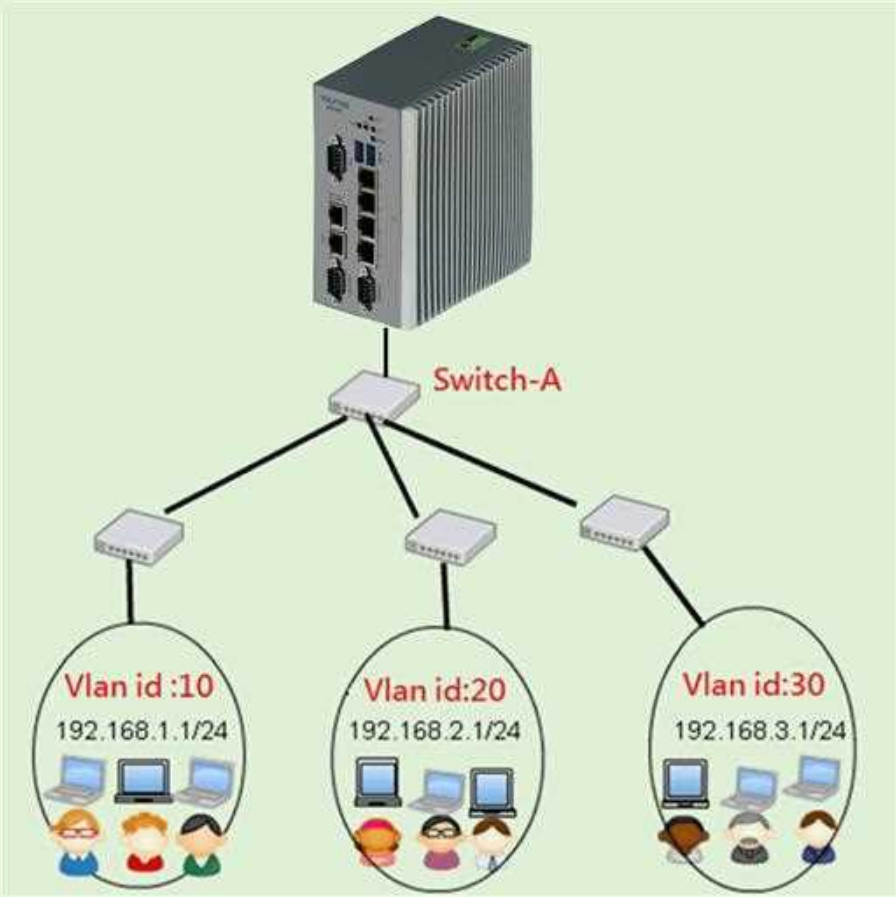


Figure 3-10

Click the “Add” button to create a new VLAN. Before adding, ensure that the connected switch has been configured with the **same VLAN ID** and **network segment**. The network segment may include either IPv4 or IPv6 addresses. If the VLAN ID and network segment do not match the settings on the peer switch, packets cannot be properly encapsulated/decapsulated, resulting in loss of connectivity. (See Figure 3-11)

- **[Name]**: The default VLAN name is “VLAN” and cannot be modified. Different VLANs are distinguished by their IDs.
- **[Enable]**: Determines whether this VLAN ID is active. Administrators can pre-configure VLAN IDs and selectively enable them when needed.
- **[Interface]**: Specifies which Zone the new VLAN belongs to. The 3100-6GT-I lists all available Zones for selection.

- **[MTU]**: Defines the maximum packet size in bytes. Default is **1500**, configurable from **1400~1500**.
- **[VLAN ID]**: Assigns a unique numeric identifier to the VLAN. VLAN IDs must not be duplicated on the same 3100-6GT-I. The valid range is **1~4064**.
- **[IPv4]**: Defines the IPv4 addresses and subnets assigned to this VLAN ID. Enter one subnet per line. Example: 192.168.1.0/24.
- **[IPv6]**: Defines the IPv6 addresses and subnets assigned to this VLAN ID. Enter one subnet per line. Example: 2001:b030:9999:abcd::1111/64.
- **[Visit Control]**: Specifies whether the interface for this VLAN ID accepts SNMP queries and **ICMP replies**.

Figure 3-11

After configuring the VLAN ID and network segment, the 3100-6GT-I lists all VLAN IDs along with their assigned IP addresses and current status. A green “enabled” icon indicates that the VLAN ID is active, while a pause icon indicates that the VLAN ID is currently disabled. To change the status, select the VLAN ID to be modified and check **“Enable”**.

Once configuration is complete, the 3100-6GT-I can receive VLAN IDs from downstream switches. The device decapsulates these VLAN-tagged packets and forwards them to the destination network based on the routing configuration. Similarly, packets received from the destination network are encapsulated with the appropriate VLAN ID and sent to the corresponding VLAN.

3-5. PPPoE

In WAN connections, PPPoE is a common dial-up method, and the 3100-6GT-I supports standard PPPoE functionality. Regardless of whether they are in the same or different zones, multiple PPPoE accounts can be configured for each zone.

Clicking “Add” button and begin adding a PPPoE account. Before adding, ensure that the **PPPoE account** and **password** are ready, and confirm which **Zone** and **Port** the PPPoE connection is connected to. The 3100-6GT-I currently supports up to **nine PPPoE accounts**. (See Figure 3-12)

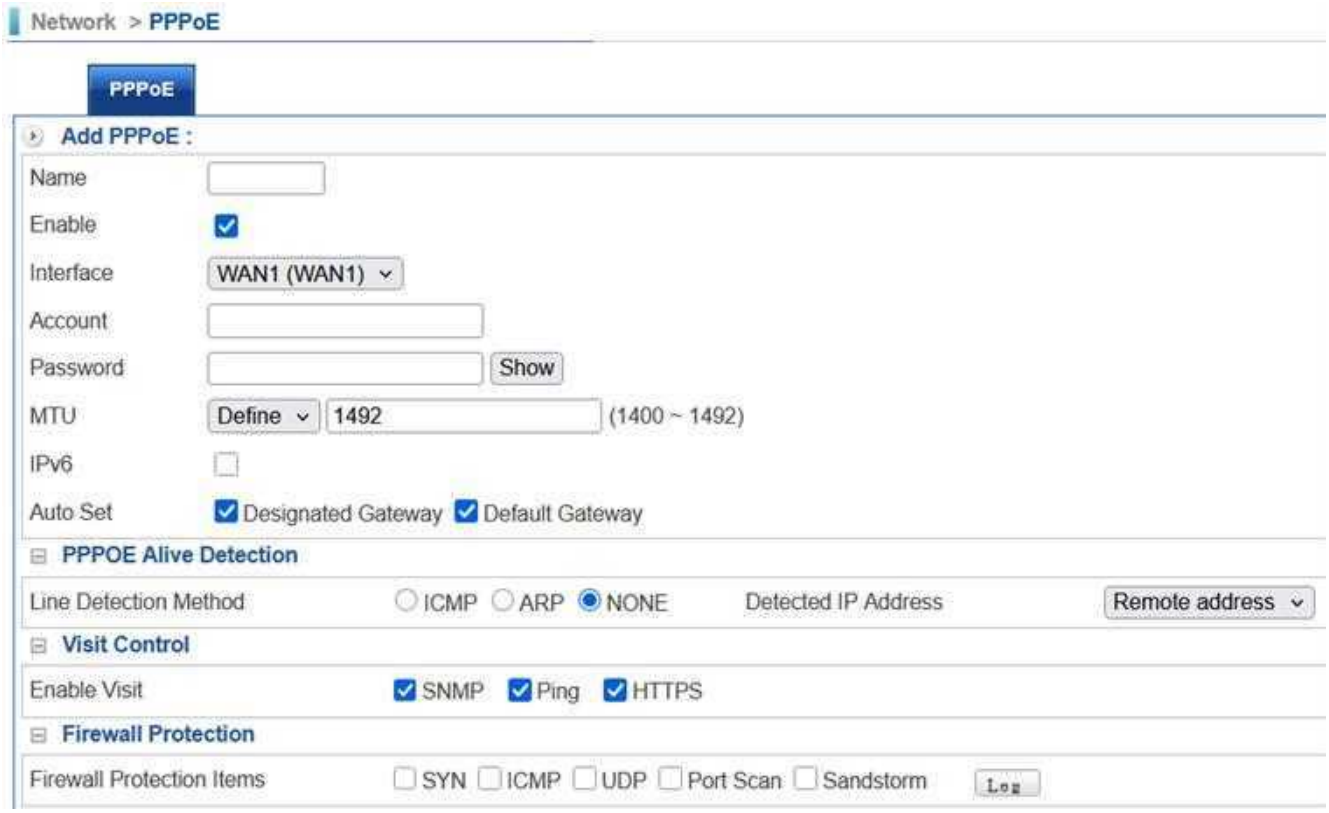


Figure 3-12

- **[Name]**: The system default name for a PPPoE connection is “PPPoE”. Administrators can assign any number between **4001 and 4009**, forming names like ppp4001 through ppp4009. If the naming convention is not followed, the PPPoE account will not function properly.
- **[Enable]**: Determines whether the PPPoE account is active. Administrators can pre-configure PPPoE accounts and selectively enable them when needed.
- **[Interface]:** Specifies which Zone the new PPPoE account belongs to. The 3100-6GT-I lists all predefined Zones for selection.
- **[Account]**: The PPPoE account name. Example: 75139012@hinet.net.
- **[Password]**: The PPPoE account password (case-sensitive).
- **[MTU]**: Specify the maximum packet size that can pass through the data link layer, typically **1492**.
- **[IPv6]**: Specifies whether the PPPoE account supports IPv6 address allocation. By default, this option is unchecked, and the PPPoE connection will only obtain an IPv4 address.
- **[Auto Set]**: In PPPoE mode, to simplify configuration, selecting **“Designated Gateway”** and **“Default Gateway”** automatically adds the settings, eliminating the need to configure them separately.

- **[Line Detection Method]**: When the Zone is WAN-type, the system must check whether the line is disconnected. Two methods are available: **ARP** and **ICMP**. At defined intervals, the 3100-6GT-I sends ARP or ICMP packets to the configured Detection Server IP Address and determines the line status based on the server's response.

  The default value is **NONE**. All detection results are logged, and by clicking the "Log" button in the PPPoE List, administrators can view the historical status of the PPPoE connection.

- **[Visit Control]**: Determines whether this interface accepts **SNMP queries**, **ICMP responses**, and **management interface login**.

- **[Firewall Protection]**: Specifies whether to enable firewall protection on this interface to prevent attacks.


between enabling and disabling.


failed connection. (See Figure 3-13)

Clicking on "Log" button in the "Detection" and "Log" sections respectively provides access to different record information.

"Detection" shows whether the PPPoE connection to the Internet is functioning properly after successful dial-up, while "Log" indicates whether the PPPoE account has passed authentication from the remote PPPoE server.

Figure 3-13

3-6. IP Tunnel

IP Tunnel is a unique feature of the 3100-6GT-I. In addition to establishing VPN connections between two 3100-6GT-I devices, it can also build IP Tunnels with other gateways that support the IP Tunnel protocol.

Unlike typical gateways, once an IP Tunnel is established, the 3100-6GT-I can apply traffic control policies to the packets within the tunnel. For example, only **Web**, **SMTP**, and **POP3** traffic may be allowed through the tunnel, while all other packets are denied.

The scenario for IP Tunnel operation

As shown in the network architecture diagram, the 3100-6GT-I is deployed at the central site, managing all external network connections. Gateways or firewalls with IP Tunnel functionality are deployed at branch sites. The basic requirement is that branch devices, such as POS systems or computers, can securely access server resources at the central site—for example, accounting systems or ERP platforms. (See Figure 3-14)

Using IP Tunnels, such a network architecture can be quickly established and deployed. Furthermore, the 3100-6GT-I allows administrators to control which applications from each branch are permitted to connect to the Internet or the internal network, while denying all other application services.

The advantage of centralized management is that administrators only need to manage a single 3100-6GT-I to oversee the entire network, since all traffic—including that from the central site and all branch sites—passes through it.

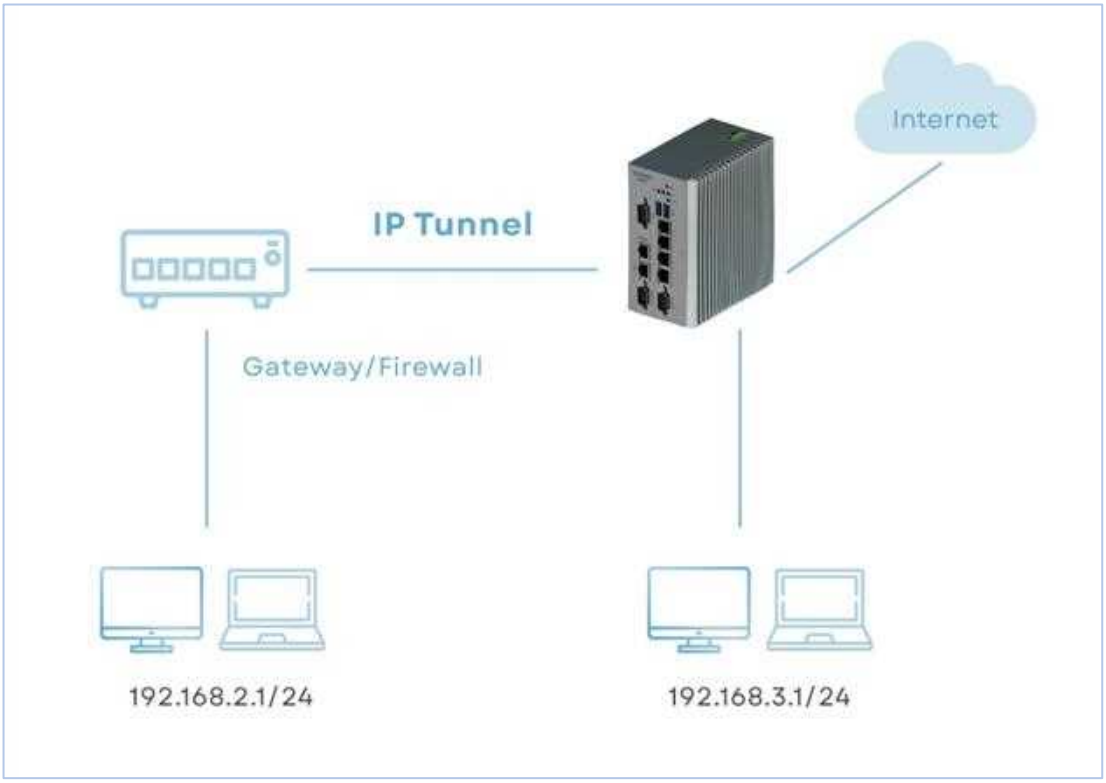


Figure 3-14

To establish a new IP Tunnel

For each IP Tunnel created, the system automatically adds a **virtual network interface**. The default naming convention for virtual interfaces is **tunl + number** (e.g., tunl1, tunl2). The numbering starts at 1, so the first IP Tunnel interface created will be *tunl1*, the second will be *tunl2*, and so on.

Once the tunnel is created, a corresponding static route is also automatically generated. This new static route appears under **[Network] > [Route] > [Static Routing]**, with the interface name labeled as tunl + number.

Administrators can also specify a gateway under **[Network] > [Route] > [Designated Gateway]**. If the 3100-6GT-I is to function as the IP Tunnel Client (i.e., accessing the Internet through a remote IP Tunnel), a **Designated Gateway** must be created, and administrators must define in **Policy** which services should access the Internet through this tunnel.

Click the "Add" button to create a new IP Tunnel. Before adding, ensure that the remote peer's WAN IP address and the Tunnel subnet are prepared. (See Figure 3-15)

- **[Name]**: Any descriptive name that makes the IP Tunnel easy to identify.
- **[Enable]**: Determines whether the IP Tunnel is active. Administrators can pre-configure IP Tunnels and selectively enable them when needed.
- **[Encryption Mode]**: Specifies whether encryption should be enabled within the IP Tunnel. If enabled, every packet passing through the tunnel is encrypted again. Three options are available:
  - **NONE**: No encryption is applied.
  - **GRE**: Packets are encrypted and decrypted using a GRE encryption key.
  - **IPSec**: Packets are encrypted and decrypted using an IPSec encryption key. Administrators can choose between 256-bit or 128-bit encryption strength.
- **[Remote IP Address]**: The remote IP address with which the 3100-6GT-I establishes the IP Tunnel. Example: 5.5.5.5.
- **[Local IP Address]**: The IP address used by the 3100-6GT-I to establish the IP Tunnel. This must be an address managed locally, typically a physical port IP bound under **[Network] > [Interfaces]**. Example: 192.168.189.169.
- **[Tunnel Interface Address]**: The gateway address of the IP Tunnel for internal traffic. Packets sent to this address are automatically forwarded through the tunnel to the remote side.
- **[Detection IP Address]**: An IP address used to verify tunnel connectivity. The system periodically checks this IP to detect disconnections, typically the remote gateway address of the tunnel.
- **[Detection Rate]**: The time interval (in seconds) for performing line detection. Configurable from 1–999 seconds.
- **[Encryption Scheme]**: Appears only when **IPSec** is selected as the encryption protocol. Two modes are available:
  - **High Security**: Uses AES 256-bit encryption.
  - **Low Security**: Uses AES 128-bit encryption.
- **[Key]:** The pre-shared encryption password used for both GRE and IPSec tunnels. It can be any combination of letters and numbers.
- **[MTU]**: The maximum packet size in bytes. Default is 1480, configurable from 1400~1500. This default value is smaller than the standard 1500 because IP Tunnels require an additional packet header. If set to 1500, the extra tunnel header would exceed the standard MTU, causing packets to fail during transmission.

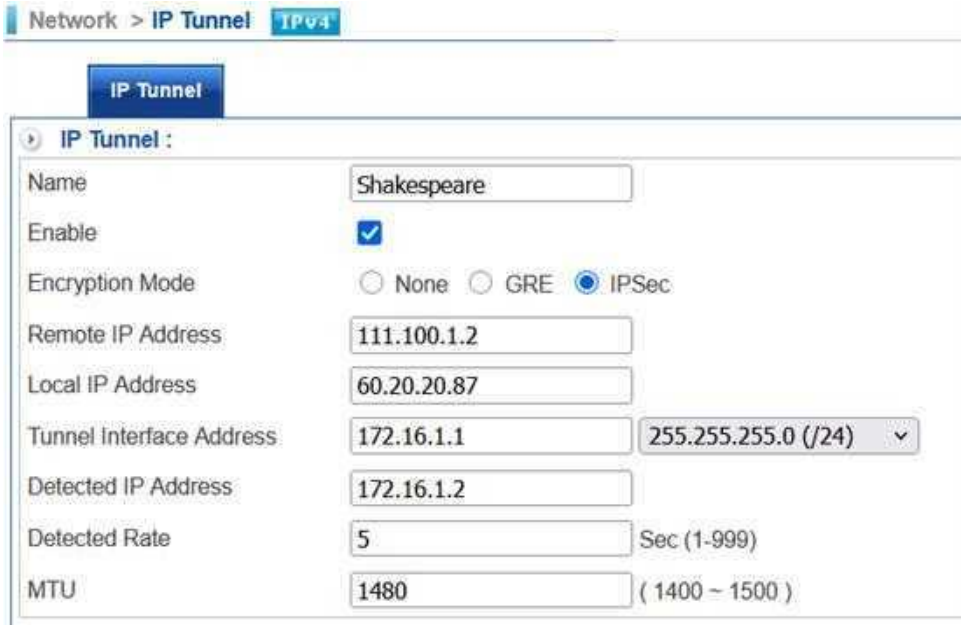

Network > IP Tunnel
IPv4
IP Tunnel
IP Tunnel :
Name
Shakespeare
Enable
Encryption Mode
None
GRE
IPSec
Remote IP Address
111.100.1.2
Local IP Address
60.20.20.87
Tunnel Interface Address
172.16.1.1
255.255.255.0 (/24)
Detected IP Address
172.16.1.2
Detected Rate
5
Sec (1-999)
MTU
1480
(1400 ~ 1500)

Figure 3-15

3-7. Interrupt

The 3100-6GT-I uses **multi-core CPU architecture** to support its wide range of services. Since each service and network interface generates different traffic loads, the system automatically allocates CPU resources to each service by default.

However, in cases where certain network interfaces experience particularly heavy traffic, automatic CPU allocation may result in imbalanced workloads—some CPUs becoming overloaded while others remain underutilized. To address this, the 3100-6GT-I provides **CPU Interrupt Service** management, allowing administrators to manually adjust system resource allocation.

After configuration, administrators can monitor each CPU's real-time usage under **[Status] > [System Status] > [CPU Usage]**.

3-7-1. Hardware Interrupt

Based on the interrupt requests from physical interfaces, CPU resources are allocated accordingly. For instance, when each network interface's TX/RX issues an interrupt request, specific CPU services are assigned. (See Figure 3-16)

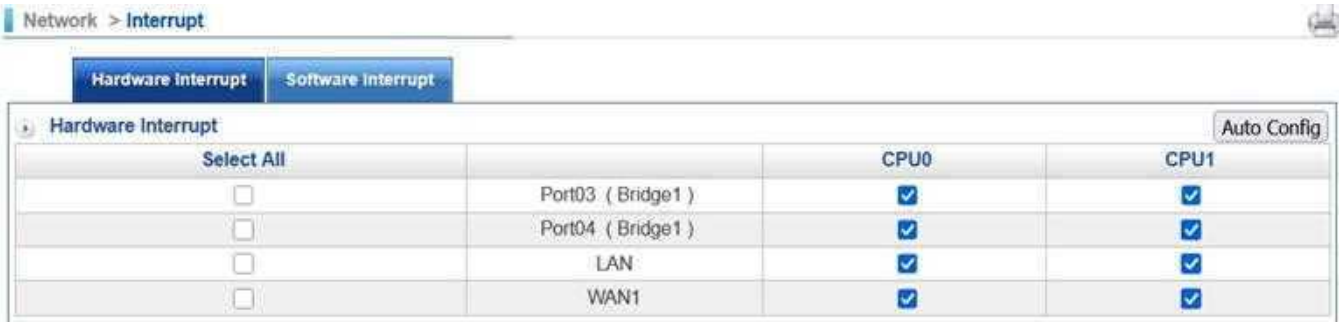


Figure 3-16

3-7-2. Software Interrupt

CPU resources are allocated based on interfaces already defined as Zones. When the load becomes concentrated on a single CPU, the system uses software interrupts to allow other CPU cores to share the workload. (See Figure 3-17)

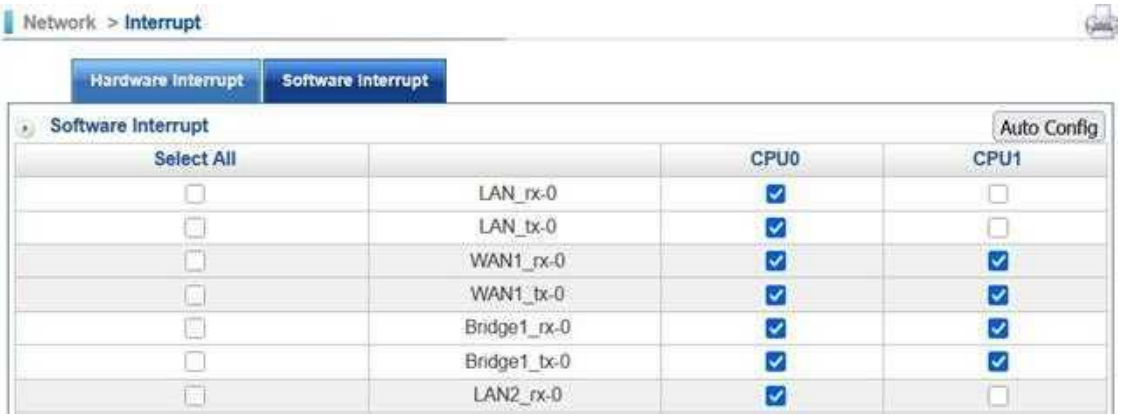


Figure 3-17

Chapter 4. Policy

Policy is the core of the 3100-6GT-I. Every packet entering or leaving the device is controlled here, including encrypted channels such as IPSec VPN tunnels, IP Tunnels, PPTP, and SSL VPN.

When a packet enters or exits an interface, it is evaluated sequentially against the policy rules from the top down. Once the packet matches a rule, the defined action—**allow** or **drop—**is applied, and the packet will not be checked against subsequent rules. If a packet reaches the last policy rule without matching any, it will be **denied**.

Because rules are processed in order, their sequence directly affects how traffic is handled. Administrators must carefully ensure that intended traffic matches the corresponding rule. To assist with verification, the 3100-6GT-I provides **packet tracing logs** and **statistics mechanisms**. Packet tracing logs allow administrators to check whether a packet matched and passed through a rule. By clicking the statistics link on a specific rule, the system opens a new window showing all inbound and outbound packets for that rule.

Each policy rule consists of three sections: **Basic Setting**, **Policy** (Extra Setting), and **Firewall Protection**. In simple terms:

1. **Basic Setting**: Who is coming from where, through which path, and going to where.
2. **Policy** (Extra Setting): Inspection of carried content.
3. **Firewall Protection**: Whether it needs protection.

For **IPSec VPN tunnels**, since they are typically used in site-to-site VPN scenarios, the rules are comparatively simpler and consist only of **Basic Setting** and **Policy** (Extra Setting).

4-1. Security Policy

When entering the Policy menu, the 3100-6GT-I lists all rules that have been created. By default, it displays all rules for every interface, with 16 rules shown per page. Administrators may specify to view the policies for a particular interface.

The policy rules are organized into four tabs—**Outgoing**, **Incoming**, **Advanced**, and **SYN Protection**. The four tabs are explained as follows:

- **Outgoing**: Defines rules governing traffic from internal to external networks. For IP address translation, only **Routing** and **NAT** are available. Routing is applied in Zone-to-Zone communication, while general Internet access typically uses NAT.
- **Incoming**: Defines rules governing traffic from external to internal networks. For IP address translation, the available options are **IP Mapping**, **Port Mapping**, and **Server Load**. These mechanisms are used when directing external traffic into the internal network.
- **Advanced**: Provides a more flexible rule set without distinguishing between inbound and outbound directions. Administrators can freely define traffic rules. All translation options are available—**Routing**, **NAT**, **IP Mapping**, **Port Mapping**, and **Server Load**. While this tab is the most powerful, it is also the most complex.
- **SYN Protection**: Provides defense against SYN-based connection attacks. Instead of simply blocking by connection count, it evaluates SYN connection behavior, making it more effective for protecting internal resources from external threats.

In cases of conflicting rules within tabs, the priority is as follows:

- **Outgoing**: Advanced > Outgoing
- **Incoming**: SYN Protection > Advanced > Incoming

Icon Explanation

In the policy rules, icons are used to represent the action performed by each rule, allowing administrators to quickly identify their functions. The icon descriptions are as follows:

Image	Name	Description
	Bandwidth Management	Bandwidth management functionality is enabled.
	Time Schedule	Activate a schedule to automatically execute rules within a set time range.
	URL Control	URL control functionality is enabled.
	Application Control	Manage which applications, such as web, FTP, Skype, etc., are allowed.
	Virus Scan Control	Web and FTP virus scanning.

Image	Name	Description
	Authentication	Requires login credentials to connect to the internet.
	OPC	OLE for Process Control
	Logging Control	Logging for HTTP and email.
	Bulletin Board	Users must view the content of the bulletin board.
	Gateway	Specification Select which gateway to use.
	Protection	Enable firewall protection.
	Any Protocol	Any protocol including TCP/UDP/ICMP, etc.
	TCP	TCP communication protocol.
	UDP	UDP communication protocol.
	ICMP	ICMP communication protocol.
	Permit	NAT operating mode, allowing packets that match the policies to pass through.
	Deny	Deny packets that match the policies from passing through.
	Pause	Pause the operation of the policies.
	Activate	Activate the operation of the policies.
	Modify	Modify the content of the policies.
	Delete	Delete the policies.

Instructions for The Policy Page

Regardless of whether IPv4 or IPv6 is selected, the following items can be configured on this page: (See Figure 4-1)

Figure 4-1

- **[No.]**: The 3100-6GT-I executes policies starting from the first IPSec policy. The order of evaluation is critical in determining whether packets are allowed or denied. A smaller number indicates higher priority.

  To adjust priority, select the policy and assign a number. For example, if a rule with priority 5 needs to be changed to priority 2, selecting 2 moves that rule to the second position, shifting the original second rule to third, and so on.

- **[On/Off]**: Toggles a policy rule between active and inactive. Clicking this icon suspends an active rule or reactivates a suspended rule.

- **[NAT]**: Defines the IP address translation mode. A blank field represents **Routing mode**, **DST** represents **Port Mapping**, and **SRC** represents **IP Mapping**.

- **[Policy]**: Specifies the advanced control items applied to the policy rule.

- **[Edit/Del]**: Modifies or removes the selected policy rule.

- **[Statistics]**: Number of packets and traffic volume entering and exiting each policy. Pausing and re-enabling will reset the values to zero. Clicking the number will display detailed records of all network packets that match this rule.

- **[Refresh]**: Immediately refreshes the policy rule list.

- **[Delete All Rules]**: Removes all policy rules, restoring the 3100-6GT-I to its initial state.

- **[Zero Counter]**: Resets all numbers in the **[Statistics]** column for every rule, starting a fresh count.

- **[Interface]**: Filters the interface policies by the selected network interface. Interfaces include physical interfaces (ZONE0, 1…), PPPoE, IP Tunnel, PPTP, and SSL VPN. By default, rules from all interfaces are displayed.

When troubleshooting network issues, administrators may need to verify whether specific traffic has entered the policies. The 3100-6GT-I provides a real-time packet session monitoring feature for this purpose. By clicking the number in the **[Statistics]** column of a policy, the 3100-6GT-I captures inbound and outbound packets and opens a new window for administrators to observe. (See Figure 4-2)

- [**Refresh**]: The 3100-6GT-I automatically refreshes the packet session records every 3~30 seconds for easier monitoring.

- **[Clear]**: Deletes all session records and restarts logging and display.
- **[Time]**: The timestamp when the packet passed through.
- **[SRC IP/Port]**: The source IP address and port of the packet that matched the policy.
- **[DST IP/Port]**: The destination IP address and port of the packet that matched the policy.
- **[Protocol]**: The communication protocol of the packet (TCP, UDP, or ICMP).
- **[Packet Size]**: Size of the packet for this connection, measured in Bytes.
- **[Designated Gateway]**: The outbound line used when traffic flows from inside to outside. If shown as "-", it indicates a TCP response packet from the remote side.

Packet Tracing Log : (Rule ID : 104) 30 Seconds Refresh Clear 1 / 2 jump to 1 Page every page 16 rows go

Time	SRC IP	DST IP	Protocol	Packet Size	SRC Port	DST Port	Designated Gateway
2025-05-09 11:46:10	8.8.8.8	192.168.1.100	ICMP	60	TYPE=0	CODE=0	-
2025-05-09 11:46:10	192.168.1.100	8.8.8.8	ICMP	60	TYPE=8	CODE=0	lan-gw[zone0]
2025-05-09 11:46:10	203.10.98.202	192.168.1.100	TCP	52	443	63548	-
2025-05-09 11:46:10	192.168.1.100	203.10.98.202	TCP	41	63548	443	lan-gw[zone0]
2025-05-09 11:46:09	8.8.8.8	192.168.1.100	ICMP	60	TYPE=0	CODE=0	-

Figure 4-2

Combination of Policies

Each policy consists of three parts: **Basic Setting**, **Policy** (Extra Setting), and **Firewall Protection**. Except for the required data in the basic setting section, the configurations in the other two areas are determined by the administrator.

4-1-1. Outgoing

All internal-to-external network traffic is controlled here, while control of internal Zone-to-Zone traffic is set in the Advanced section.

Clicking on the edit icon of a policy will take the administrator to the configuration screen to modify Basic Setting, Policy (Extra Setting), and Firewall Protection setting.

A) Outgoing > Basic Setting

The source and destination for each policy are defined in the basic settings. To enhance management convenience and readability, administrators can pre-define address tables, service tables, and applications in **"Object"** for selection.

Apart from network interfaces, which need to be planned beforehand, other parts provide customizable options for administrators to directly input information, such as IP addresses, network Ports, etc. (See Figure 4-3)

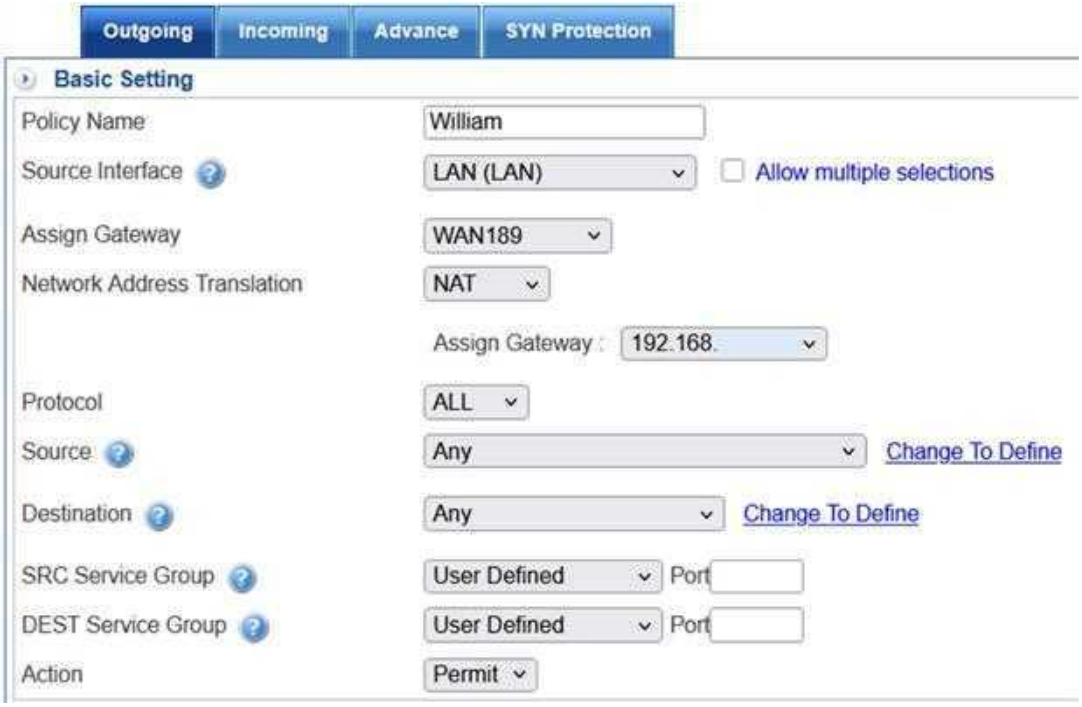


Figure 4-3

- **[Policy Name]**: The name of the policy rule. Administrators may enter any text in Chinese or English for easy identification, e.g., Block Internet Access.
- **[Source Interface]**: The 3100-6GT-I manages traffic based on interfaces/Zones, and all packets entering or leaving a Zone can be monitored and controlled. Since this is an Outgoing policy, the selectable Zones should be those from which internal traffic exits, including internal Zones as well as client interfaces for PPTP, L2TP, and SSL VPN.

  Network interfaces are divided into two types: **physical interfaces** and **virtual interfaces**. Any physical interface or VPN interface (PPTP, L2TP, SSL VPN) added under [Network] > [Interface] will automatically appear in the source interface options.

- **[Assign Gateway / Network Address Translation]**: Refer to the following section Outgoing > Basic Setting > Assign Gateway and Network Address Translation for details.
- **[Protocol]**: Four options are available—All, TCP, UDP, and ICMP. This specifies which type of protocol the rule applies to. The default is All.
- **[Source]**: Defines the source IP address that matches the policy. For interfaces (Zones), this refers to IP addresses exiting from within the 3100-6GT-I. Two modes are available for configuration: **Option Mode** and **Define Mode**. The default is Option Mode.
  - **Option Mode**: The system automatically adds the following source IP addresses for selection:

    A. Internal Zone defined in [Network] > [Interface].

    B. Address tables or groups created in [Object] > [IP Address].

    C. IP addresses assigned in various VPNs, including PPTP servers, SSL VPN, and L2TP assigned to remote users.
  - **Define Mode**: Administrators directly input source IP addresses or MAC addresses.
- **[Destination]**: Destination IP address to reach. For Outgoing policies, this is the IP address of external networks. There are two modes for administrators to choose from: **Option mode** and **Define Mode**. Default is Option mode.
  - **Option Mode**: The system automatically adds address tables or groups already created in [Object] > [IP Address] for selection.
  - **Define Mode**: Administrators directly input destination IP addresses or MAC addresses.

  Note: The 3100-6GT-I does not control different source and destination IP addresses within the same interface (Zone). Its behavior is like that of a switch's bridging function, where only network packets entering and exiting interfaces (Zone) will apply policies.
- **[SRC Service Group]**: Defines the restricted source ports. Three options are available: Default Service Table, User Defined, or directly input port numbers. The 3100-6GT-I provides a default list of common services (e.g., HTTP, FTP).

  To simplify the number of policies, multiple services can be combined into a service group. All such groups must first be defined in **[Object] > [Service]**, after which they will appear as selectable options. If **User Defined** is selected, the administrator must manually enter the port number in the field provided.

  Note: In an IPv4 environment, due to extensive use of PAT, the source port is often dynamic and may be any value from **1~65535**. Therefore, administrators should carefully consider whether to specify a source port. If no group is defined, the default is **All Ports**.
- **[DEST Service Group]**: Defines the restricted destination ports. Three options are available: Default Service Table, User Defined, or directly input port numbers. The 3100-6GT-I provides a default list of common services (e.g., HTTP, FTP).

  To simplify the number of policies, multiple services can be combined into a service group. All such groups must first be defined in **[Object] > [Service]**, after which they will appear as selectable options. If **User Defined** is selected, the administrator must manually enter the port number in the field provided.

  Note: In both IPv4 and IPv6 environments, the destination port corresponds to the network service being controlled. For example, if **only** HTTP traffic is allowed, HTTP **must be entered** here. If no group is defined, the default is **All Ports**.

- **[Action]**: Defines how packets that match the above conditions are handled. Two options are available: Permit (allow the traffic) or Drop (drop the traffic).

  Note: To use advanced features such as OPC or URL Filtering, the action must be set to "Permit"; otherwise, the packet will be dropped and will not enter advanced processing.

B) Outgoing > Basic Settings > Assign Gateway and Network Address Translation

For packets that match the policy, specify which Designated Gateway they should be sent to. Designated Gateway can be configured under [Network] > [Route] > [Designated Gateway] or [Designated Gateway Groups].

- **[Assign Gateway]**: Defines which gateway the matched packets should be sent to.

  Administrators must first configure [Designated Gateway] or [Designated Gateway Groups] under [Network] > [Route]. All routes defined in Designated Gateway or Designated Gateway Groups are listed for administrators to select.

  By default, the 3100-6GT-I uses "Default", meaning that all network packets are forwarded to the Default Gateway.

- **[Network Address Translation]**: Specifies whether packets passing through the interfaces perform NAT/PAT or simple Routing. The available modes are described below:

  (1) Routing:

  When "Routing" is selected, the source IP address of packets passing through the interfaces remains unchanged. In this case, the device operates as a pure Layer 3 router. Combined with source and destination IP-based policies, this mode provides the functionality of a standard Layer 3 core switch.

  (2) NAT:

  When packets are sent through an interface, they are translated into a specific IP address using PAT (Port Address Translation) by default. If the "Assign Gateway" selection is "Default", the system automatically chooses the translation IP during PAT and lists all available translated IP addresses. However, if administrators wish to specify the translation IP, they cannot use "Default".

  When a specific gateway (rather than the default gateway) is selected as the outbound line, NAT is performed, and administrators can choose which IP address will serve as the PAT/NAT source address.

  For example, if the IP address range 192.168.100.0/24 is configured under **[Network] > [Route] > [Designated Gateway] > [Interface]**, any IP address within 192.168.100.0–192.168.100.254 can be selected here.

  If the outbound line selection is an [Designated Gateway Group], administrators can specify which IP address each outbound line will use as the PAT/NAT source address. (See Figure 4-4)

Figure 4-4

C) Outgoing > Common Industrial Protocol

In addition to controlling traffic by IP and service port numbers, the 3100-6GT-I also provides critical control over industrial control protocols within OT environments. Specifically, it supports management of Modbus/TCP traffic, such as device IDs and function codes. (See Figure 4-5)

- **[Comment]**: Add a description for this setting to make future reference easier.
- **[Slave ID]**: Enter the ID of the device to be inspected and filtered.
- **[Function Code]**: Select the function codes to be allowed. For example, selecting *Read* function codes will permit only Read-related operations to pass.
- **[Address]**: Enter the address number of the device to be inspected.

  Only the fields with values entered will be evaluated. For example, if only ID and Address are specified while others are left blank, packets that match these two values will be permitted, regardless of function code.

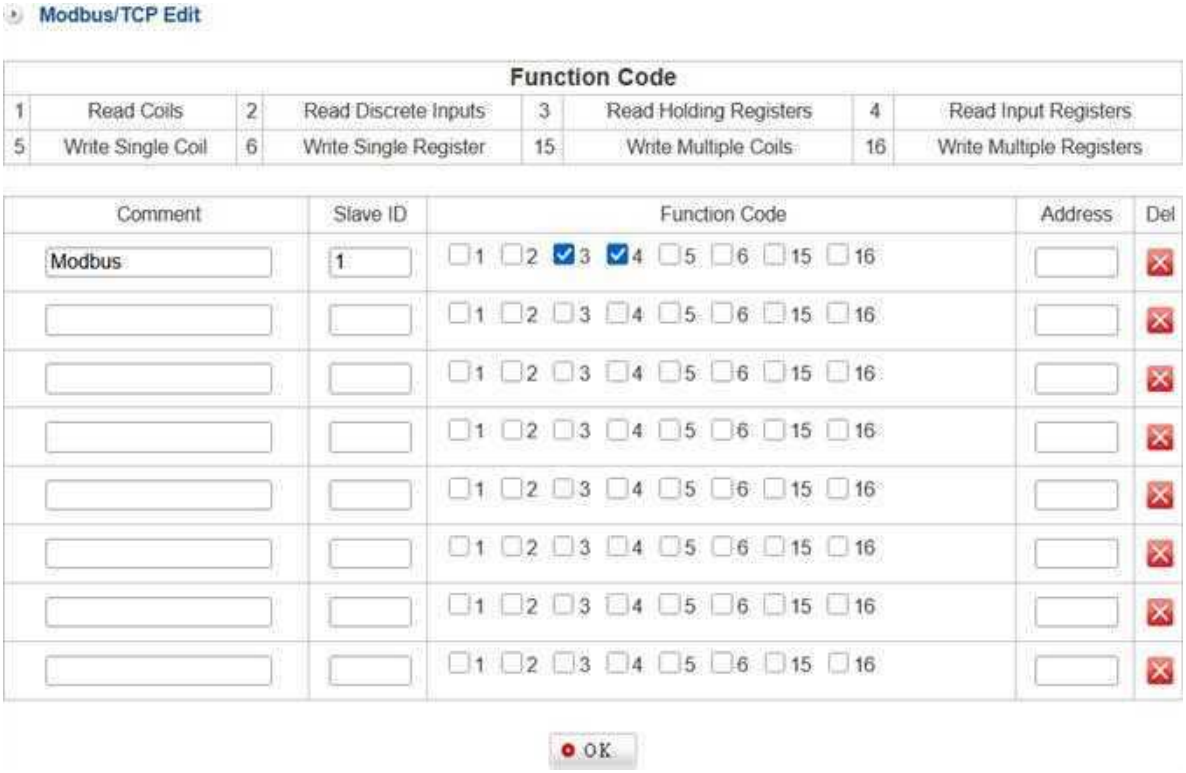


Figure 4-5

D) Outgoing > Policy (Extra Setting)

For network packets that match the rules of the **Basic Settings** and have the **Action** set to allow, the 3100-6GT-I can perform more advanced actions, including scheduling, OPC, and virus scanning, etc. Each item needs to be set in the corresponding **Object** in advance for the entire policy to take effect. (See Figure 4-6)

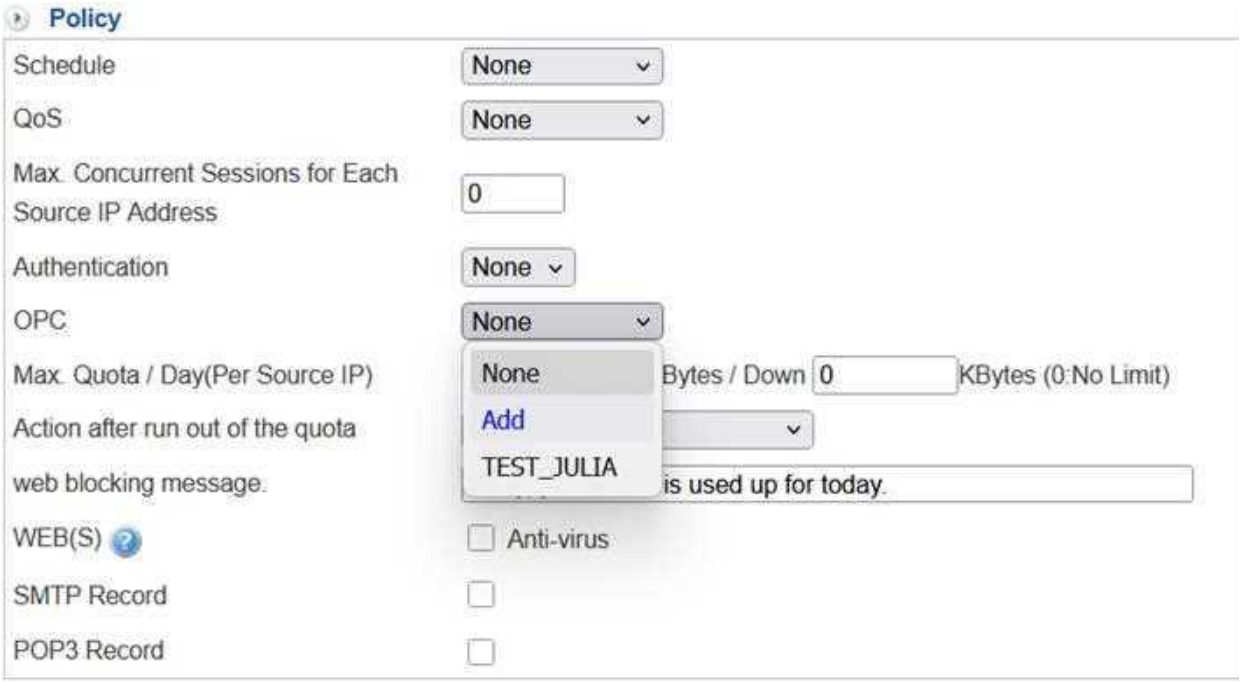


Figure 4-6

Each option includes an **"Add"** function. If the required item is not listed, selecting **"Add"** automatically opens a new window for administrators to quickly create the item. For example, if a new address object needs to be added but is not available in the selection list, clicking **"Add"** opens a window to create the address object directly—without switching to **[Object] > [IP Address]**.

- **[Schedule]**: Create a schedule under **[Object] > [Schedule]**. The policy is only effective within the defined schedule period. Outside of the schedule, the rule becomes invalid.
- **[QoS]**: Create bandwidth limits under **[Object] > [QoS].** The policy restricts traffic usage according to the configured bandwidth.
- **[Max. Concurrent Sessions for Each Source IP Address]**: Default is 0 (no restriction). When set to a non-zero value, each source IP that matches the policy is limited to the specified maximum number of concurrent connections.
- **[Authentication]**: Create authentication groups under **[Object] > [Authentication]**. When applied, traffic from the source IP to the destination IP triggers a login prompt, requiring user authentication.
- **[OPC]**: Create a group under **[OPC] > [OPC Setting]**. When applied, packets under this policy are compared against OPC signatures, and the action (log or block) is determined by the OPC configuration.
- **[Max. Quota / Day (per Source IP)]**: Defines the daily upload/download quota for each source IP under this rule. Default is 0 (unlimited). When the quota is exceeded, the action specified in **[Action after run out of the quota]** is applied.
- **[Action after run out of the quota]**: Defines how to handle packets once the quota is exceeded. Two options are available:

- **Drop**: Drops all packets beyond the quota. The user's browser displays the message defined in [Web Blocking Message].
- **Continue to Run Next Policy**: Forwards packets to the next policy rule for further evaluation.

- **[Web Blocking Message]**: Defines the message displayed in the user's browser when access is blocked due to exceeding the quota.
- **[WEB(S)]**: This function provides only the **Antivirus** option, which scans all HTTP/HTTPS packets passing through the device to ensure secure web browsing.
- **[SMTP Record]**: Configure items under [Mail Security] > [Filter and Log]. Currently, it supports antivirus scanning for email. For detailed adjustments, use [Mail Security] > [Antivirus].
- **[POP3 Record]**: When enabled, scans and logs email traffic on port 110 (POP3). Detailed settings can be adjusted under [Mail Security] > [Filter and Log] > [Retrieve Mail Anti-Virus].

Note: The functions **[WEB(S)]**, **[SMTP Record]**, and **[POP3 Record]** apply globally across the entire 3100-6GT-I. Policies cannot be customized per interface. Administrators can only enable or disable these features. Once enabled, the same mechanism is applied system-wide.

E) Outgoing > Firewall Protection

For incoming packets, administrators can configure whether firewall protection is applied. Each policy rule allows enabling or disabling firewall protection, as defined in the Protection Settings section. (See Figure 4-7)

Figure 4-7

4-1-2. Incoming

All rules governing traffic from external sources into internal Zones can be configured here. For example, if there is an ERP server inside the network that must be accessible from the outside, it can be defined in this section.

There are three IP address translation modes: **IP Mapping**, **Port Mapping**, and **Server Load**. Each serves a different purpose. In simple terms:

1. **IP Mapping**: A one-to-one mapping between IP addresses.
2. **Port Mapping** and **Server Load**: One-to-many mappings between IP addresses.

A) Incoming > Basic Setting

- **[Policy Name]**: The name of the policy rule. Administrators may enter any text in Chinese or English for easy identification, e.g., ERP Server.
- **[Source Interface]**: The 3100-6GT-I manages traffic based on Zones, and all packets entering or leaving a Zone can be monitored and controlled. Since this is an **Incoming** policy, the selectable Zones should be the external interfaces through which traffic enters. The system lists all external network interfaces for administrators to choose from.
- **[Network Address Translation]**: Refer to the following section Incoming > Basic Setting > Network Address Translation for details.
- **[Protocol]**: Four options are available—All, TCP, UDP, and ICMP. This specifies which type of protocol the rule applies to. The default is All.
- **[Source]**: The source IP address that matches the policy. For interfaces (Zones), this represents the IP address from which traffic is entering the 3100-6GT-I. Two configuration modes are available: **Option Mode** and **Define Mode**. The default is Option Mode.
  - **Option Mode**: The system automatically includes the address objects or groups created under [Object] > [IP Address], allowing administrators to select from them.
  - **Define Mode**: Administrators directly input source IP addresses or MAC addresses.
- **[Destination]**: Destination IP address to reach. For **Incoming** policy rules, this refers to the internal network IP addresses. Two configuration modes are available: **Option mode** and **Define Mode**. Default is Option mode.
  - **Option Mode**: The system automatically provides the following source IP addresses for selection:

    A. Internal Zones defined under [Network] > [Interface].

    B. Address objects or groups created under [Object] > [IP Address].
  - **Define Mode**: Administrators directly input destination IP addresses or MAC addresses.
- **[SRC Service Group]**: Defines the restricted source ports. Three options are available: Default Service Table, User Defined, or directly input port numbers. The 3100-6GT-I provides a default list of common services (e.g., HTTP, FTP).

  To simplify the number of policies, multiple services can be combined into a service group. All such groups must first be defined in **[Object] > [Service]**, after which they will appear as selectable options. If **User Defined** is selected, the administrator must manually enter the port number in the field provided.

Note: In an IPv4 environment, due to extensive use of PAT, the source port is often dynamic and may be any value from **1~65535**. Therefore, administrators should carefully consider whether to specify a source port. If no group is defined, the default is **All Ports**.

- **[DEST Service Group]**: Defines the restricted destination ports. Three options are available: Default Service Table, User Defined, or directly input port numbers. The 3100-6GT-I provides a default list of common services (e.g., HTTP, FTP).

  To simplify the number of policies, multiple services can be combined into a service group. All such groups must first be defined in **[Object] > [Service]**, after which they will appear as selectable options. If **User Defined** is selected, the administrator must manually enter the port number in the field provided.

  Note: In both IPv4 and IPv6 environments, the destination port corresponds to the network service being controlled. For example, if **only** HTTP traffic is allowed, HTTP **must be entered** here. If no group is defined, the default is **All Ports**.

- **[NAT]**: When enabled, the source IP address in the rule is translated into an internal IP address, typically the IP bound to the internal interface. This option is useful when internal servers restrict access based on source IP addresses (allowing only internal users). To enable external access without modifying server policies, administrators can enable **NAT** in the policy.

- **[Action]**: Defines how packets that match the above conditions are handled. Two options are available: Permit (allow the traffic) or Drop (drop the traffic).

  Note: To use advanced features such as OPC or URL Filtering, the action must be set to “Permit”; otherwise, the packet will be dropped and will not enter advanced processing.

B) Incoming > Basic Setting > Network Address Translation

1. Mapped IP

In [Network] > [Interface] > [WAN] > [IP Address / PPPoE], an external IP address can be mapped to the actual internal service IP address. This is a one-to-one NAT address mapping mechanism.

For example, if 192.168.1.200 is configured under [WAN] > [IP Address / PPPoE], and it maps to the internal IP 10.10.1.200. When an external user accesses 192.168.1.200, all packets are automatically translated to 10.10.1.200.

To illustrate the setup of IP Mapping based on the example above:

(1) In the policy’s [Basic Setting] > [Network Address Translation], select “**Mapped IP**”, then enter the internal IP address 10.10.1.200 in the field.

(2) Choose **ANY** for [Source]. If restricting the source network segment, select the IP set already configured in the address table or click the “Change To Define” button to input the restricted source IP.

(3) Choose the IP address 192.168.1.200 already set in [Network] > [Interface] > [WAN] > [IP Address / PPPoE] for [Destination] or click “Change To Define” to input the external IP address directly.

(4) Also, make sure to check [Source] and select the correct source interface to allow external connections.

2. Mapped Port

Port Mapping is a one-to-many NAT technology that redirects an external IP address to different internal service hosts based on different service ports.

Similar to IP Mapping, Port Mapping also requires the selection of the source interface. If the source interface is not set, access is denied. In theory, a legitimate IP address can be assigned to a maximum of 65,535 internal IP addresses.

After selecting "**Mapped Port**" and clicking the "Edit" button, a new window will appear, where the IP address set in this setting is the internal IP address and port number. (See Figure 4-8)

Figure 4-8

For example, in [WAN] > [IP Address / PPPoE], an external IP address is defined as 192.168.1.200. The server 192.168.1.200 provides three services externally: **WEB**, **FTP**, and **DNS**. These three services correspond to different internal hosts: 10.10.1.200, 10.10.1.100, and 10.10.1.50, respectively.

In the Port Mapping modification table, enter the following in the "DNAT IP Address" field:

A. 10.10.1.200 / Destination Port: 80

B. 10.10.1.100 / Destination Port: 21

C. 10.10.1.50 / Destination Port: 53

The "DNAT DEST Port" generally matches the "Original DEST Port," but it can be set differently. If set differently, the internal and external port numbers will not be the same.

Additionally, in the basic setting:

(1) Check **[Source Interface]** and select the correct source interface to allow external connections.

(2) Choose **ANY** for [Source]. If restricting the source network segment, select the IP set already configured in the address table or click the "Change To Define" button to input the restricted source IP.

(3) Choose the IP address for [Destination]. Based on the example above, select 192.168.1.200.

3. Server Load Balance

The 3100-6GT-I can perform **server load balancing**, which distributes a service across two or more internal servers. Based on the configured weight or service mode, traffic is distributed to different servers accordingly. Similar to IP Mapping, load balancing also requires selecting the **Source Interface**; traffic cannot enter if the source interface is not defined.

When **Server Load Balancing** is selected and the "**Edit**" button is clicked, the 3100-6GT-I opens a new window where administrators can define which IP addresses and services are included in the load balancing task.

For example, the picture below shows how the **Web service on 192.168.1.200** is distributed across two internal servers, 10.10.1.100 and 10.10.1.200, according to the configured weight. (See Figure 4-9)

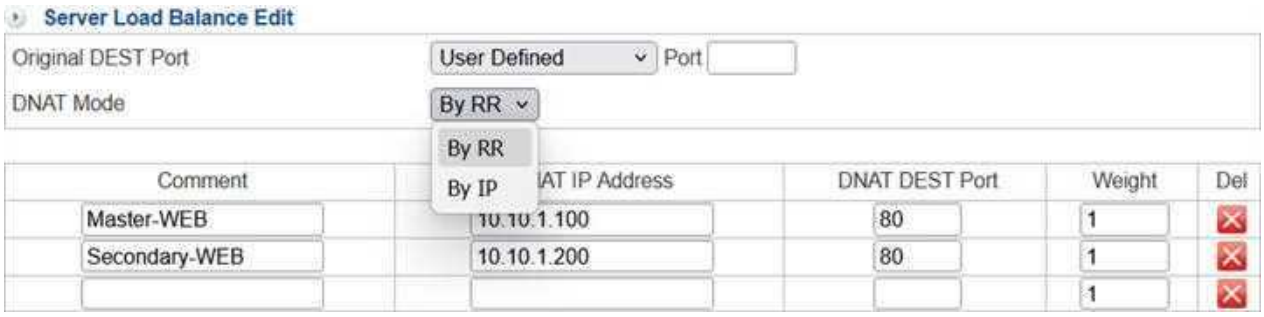


Figure 4-9

First, confirm the **original destination port**. Administrators may either select an item from the **Service Table** or manually enter a TCP port. Since the server load balancing mechanism distributes traffic based on each service, a separate mapping entry is required for each port.

Two distribution modes are available: **Sequential Round Robin** and **By Source IP**. Both modes incorporate the concept of **weight** to allocate traffic across translated IP addresses:

(1) **Sequential Round Robin**: Connections are assigned sequentially to backend IP addresses based on weight. For example, if 10.10.1.200 has weight 1 and 10.10.1.201 has weight 2, the first connection goes to 10.10.1.200, the second and third to 10.10.1.201, the fourth to 10.10.1.200, the fifth and sixth to 10.10.1.201, and so forth.

(2) **By Source IP**: Connections are distributed according to the source IP address. For example, the first source IP is assigned to 10.10.1.200, the second and third source IPs are assigned to 10.10.1.201, and so on.

Additionally, administrators must select the [Source]. By enabling all listed source interfaces, traffic from all external users can be allowed. In this case, set the [Source] to **ANY**. If restrictions are required, a specific source IP address can be entered.

For the [Destination], select the corresponding IP address. In the above example, this would be 192.168.1.200. The system automatically lists the IP addresses configured under the [Address Table] for selection, or administrators may click [Change To Define] to manually enter the external IP address.

C) Incoming > Common Industrial Protocol

Similar to the **Outgoing** policies for industrial protocols, the 3100-6GT-I not only controls traffic based on IP addresses and service ports, but also supports management of industrial control protocols within OT environments. Through this feature, the 3100-6GT-I can restrict Modbus/TCP packets, allowing only those that match the defined settings to pass, while all others are blocked. (See Figure 4-10)

- **[Comment]**: Add a description for this setting to make future reference easier.
- **[Slave ID]**: Enter the ID of the device to be inspected and filtered.
- **[Function Code]**: Select the function codes to be allowed. For example, selecting *Read* function codes will permit only Read-related operations to pass.
- **[Address]**: Enter the address number of the device to be inspected.

Only the fields with values entered will be evaluated. For example, if only ID and Address are specified while others are left blank, packets that match these two values will be permitted, regardless of function code.

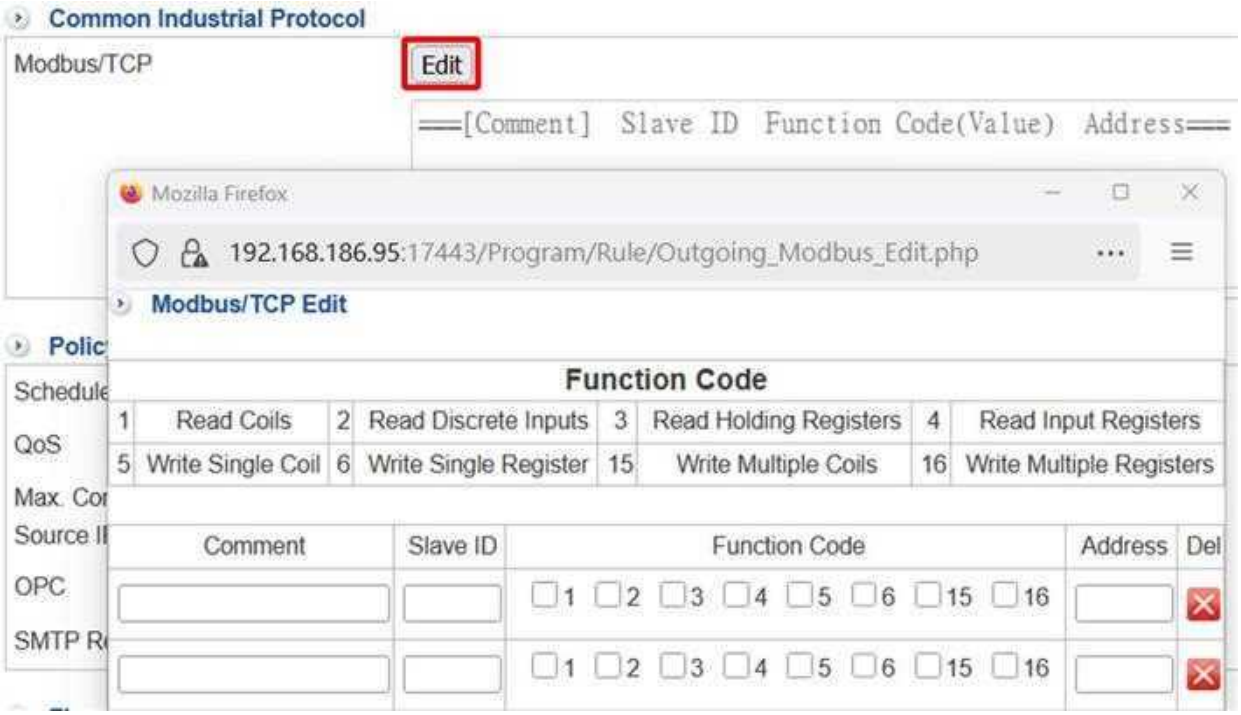


Figure 4-10

D) Incoming > Policy (Extra Setting)

For network packets that match the rules of the **Basic Settings** and have the **Action** set to allow, the 3100-6GT-I can perform more advanced actions, including scheduling, OPC, and virus scanning, etc. Each item needs to be set in the corresponding **Object** in advance for the entire policy to take effect.

Each option includes an **"Add"** function. If the required item is not listed, selecting **"Add"** automatically opens a new window for administrators to quickly create the item. For example, if a new address object needs to be added but is not available in the selection list, clicking **"Add"** opens a window to create the address object directly—without switching to **[Object] > [IP Address]**.

- **[Schedule]**: Create a schedule under **[Object] > [Schedule]**. The policy is only effective within the defined schedule period. Outside of the schedule, the rule becomes invalid.
- **[QoS]**: Create bandwidth limits under **[Object] > [QoS].** The policy restricts traffic usage according to the configured bandwidth.
- **[Max. Concurrent Sessions for Each Source IP Address]**: Default is 0 (no restriction). When set to a non-zero value, each source IP that matches the policy is limited to the specified maximum number of concurrent connections.
- **[OPC]**: Create a group under **[OPC] > [OPC Setting]**. When applied, packets under this policy are compared against OPC signatures, and the action (log or block) is determined by the OPC configuration.
- **[SMTP Record]**: Configure items under [Mail Security] > [Filter and Log]. Currently, it supports antivirus scanning for email. For detailed adjustments, use [Mail Security] > [Antivirus].

  For the features **[SMTP Record]** and **[OPC]**, the same rule set applies across the entire 3100-6GT-I. It is not possible to customize rules per interface. Administrators can only enable or disable these functions, and once enabled, the same mechanism is applied system-wide.

- **[WAF]**: Under [WAF] > [WAF Setting], administrators can select the items to be scanned and then configure monitoring on web ports 80 or 443. For more details, refer to Chapter 9: WAF.

F) Incoming > Firewall Protection

For incoming packets, administrators can configure whether firewall protection is applied. Each policy rule allows enabling or disabling firewall protection, as defined in the Protection Settings section.

4-1-3. Advance

Advanced policies are essentially a combination of **Outgoing** and **Incoming** policies. The main configuration difference compared to **4-1-1. Outgoing** and **4-1-2. Incoming** lies in the settings for **Assign Gateway** and **Network Address Translation**. Please refer to B) Advance > Basic Setting > Assign Gateway / Network Address Translation. (See Figure 4-11)

A) Advance > Basic Setting

- **[Policy Name]**: The name of the policy rule. Administrators may enter any text in Chinese or English for easy identification, e.g., ERP Server.
- **[Source Interface]**: The 3100-6GT-I manages and controls traffic based on interfaces (Zones). Since Advanced policies cover both **Outgoing** and **Incoming** traffic, the selectable Zones include both internal (for outgoing) and external (for incoming) interfaces. The system lists all internal interfaces, PPTP, L2TP, and SSL VPN clients, as well as external network interfaces, for administrators to choose from.
- **[Assign Gateway / Network Address Translation]**: Refer to the following section Advanced > Basic Setting > Assign Gateway and Network Address Translation for details.
- **[Protocol]**: Four options are available—All, TCP, UDP, and ICMP. This specifies which type of protocol the rule applies to. The default is All.
- **[Source]**: Defines the source IP address that matches the policy. For interfaces (Zones), this refers to IP addresses going **outbound from inside** the 3100-6GT-I or **inbound from external networks**. Two modes are available for configuration: **Option Mode** and **Define Mode**. The default is Option Mode.
  - **Option Mode**: The system automatically adds the following source IP addresses for selection:

    A. Internal Zone defined in [Network] > [Interface].

    B. IP addresses assigned in various VPNs, including PPTP servers, SSL VPN, and L2TP assigned to remote users.
  - **Define Mode**: Administrators directly input source IP addresses or MAC addresses.
- **[Destination]**: The destination IP address. For **Outgoing** policies, this refers to the external network IP address; for **Incoming** policies, it refers to the internal network IP address. There are two modes for administrators to choose from: **Option mode** and **Define Mode**. Default is Option mode.
  - **Option Mode**: The system automatically provides the following source IP addresses for selection:

    A. Internal Zones defined under [Network] > [Interface].

B. Address objects or groups created under [Object] > [IP Address].

- **Define Mode**: Administrators directly input destination IP addresses or MAC addresses.

- **[SRC Service Group]**: Defines the restricted source ports. Three options are available: Default Service Table, User Defined, or directly input port numbers. The 3100-6GT-I provides a default list of common services (e.g., HTTP, FTP).

  To simplify the number of policies, multiple services can be combined into a service group. All such groups must first be defined in **[Object] > [Service]**, after which they will appear as selectable options. If **User Defined** is selected, the administrator must manually enter the port number in the field provided.

  Note: In an IPv4 environment, due to extensive use of PAT, the source port is often dynamic and may be any value from **1~65535**. Therefore, administrators should carefully consider whether to specify a source port. If no group is defined, the default is **All Ports**.

- **[DEST Service Group]**: Defines the restricted destination ports. Three options are available: Default Service Table, User Defined, or directly input port numbers. The 3100-6GT-I provides a default list of common services (e.g., HTTP, FTP).

  To simplify the number of policies, multiple services can be combined into a service group. All such groups must first be defined in **[Object] > [Service]**, after which they will appear as selectable options. If **User Defined** is selected, the administrator must manually enter the port number in the field provided.

  Note: In both IPv4 and IPv6 environments, the destination port corresponds to the network service being controlled. For example, if **only** HTTP traffic is allowed, HTTP **must be entered** here. If no group is defined, the default is **All Ports**.

- **[Action]**: Defines how packets that match the above conditions are handled. Two options are available: Permit (allow the traffic) or Drop (drop the traffic).

  Note: To use advanced features such as OPC or URL Filtering, the action must be set to “Permit”; otherwise, the packet will be dropped and will not enter advanced processing.

Figure 4-11

B) Advance > Basic Setting > Assign Gateway and Network Address Translation

Designated Gateway can be configured under [Network] > [Route] > [Designated Gateway] or [Designated Gateway Groups].

- **[Assign Gateway]**: Defines which gateway the matched packets should be sent to.

  Administrators must first configure [Designated Gateway] or [Designated Gateway Groups] under [Network] > [Route]. All routes defined in Designated Gateway or Designated Gateway Groups are listed for administrators to select.

- **[Network Address Translation]**: Selecting **[Network Address Translation]** displays the available configuration items. Typically, the first consideration for creating a new policy is IP address translation. In **Advance**, there are five applicable types: (See Figure 4-12)

  (1) **Routing**: Commonly used for traffic control between internal Zones.

  (2) **NAT**: Typically applied when internal Zones access external networks.

  (3) **IP Mapping**: Maps an external IP address to a specific internal IP address, with all ports translated together.

  (4) **Port Mapping**: Maps a specific port of an external IP address to a specific port of an internal IP address.

  (5) **Server Load Balance**: Maps a specific port of an external IP address to two or more internal IP addresses running the same service, such as web servers.

  The five types in Advance settings have already been described in earlier sections. Please refer to:

  4-1-1 Outgoing: Routing (1) and NAT (2).

  4-1-2 Incoming: IP Mapping (3), Port Mapping (4), and Server Load Balancing (5).

  Note: Advance policies take precedence over both Outgoing and Incoming policies. If identical rules are configured in both Outgoing/Incoming and Advance, only the Advance rule will take effect.

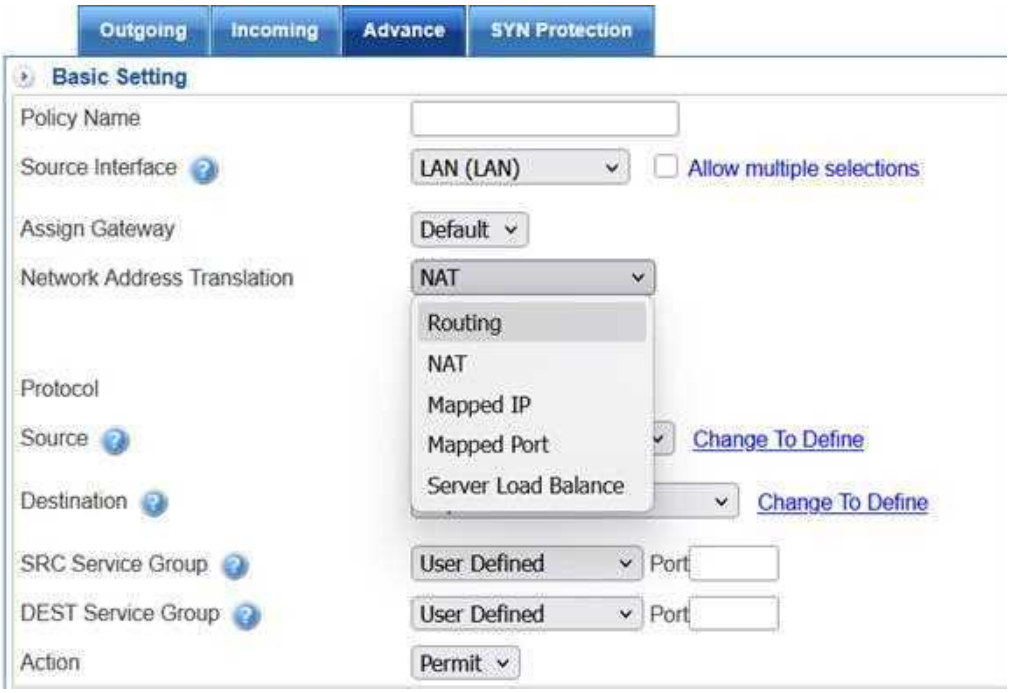


Figure 4-12

C) Advance > Common Industrial Protocol

Refer to 4-1-1. Outgoing or 4-1-2. Incoming, section C) Common Industrial Protocol.

D) Advance > Policy (Extra Setting)

Refer to 4-1-1 Outgoing, section D) Outgoing > Policy (Extra Setting).

E) Advance > Firewall Protection

Refer to 4-1-1. Outgoing or 4-1-2. Incoming, section E) Firewall Protection.

4-1-4. SYN Protection

Hackers often launch **SYN Flood Attacks** to overwhelm and disable servers. The 3100-6GT-I provides a **SYN Protection** mechanism that shields backend servers from abnormal and excessive SYN requests, ensuring that services remain operational. Since this mechanism protects backend servers, its configuration is similar to **Incoming** policies, supporting three types of IP address translation: **IP Mapping**, **Port Mapping**, and **Server Load Balance**.

How SYN Protection Works

The three-way handshake of TCP occurs when a client wants to establish a TCP connection with a server. In sequential order, the client and server exchange information as follows:

1. The client sends a **SYN packet** to request a connection.
2. The server responds with **SYN-ACK** to acknowledge the request.
3. The client replies with **ACK**, completing the TCP connection. During an SYN attack, the client does not respond with an ACK.

Hackers send a large number of SYN requests, consuming server resources and preventing legitimate TCP connection attempts, ultimately causing a denial of service.

The 3100-6GT-I mitigates this attack by handling steps 1~3 itself. Only when the connection is verified as legitimate will it be passed to the backend server. This ensures that the attack traffic is absorbed by the 3100-6GT-I, not by the protected servers.

Rule Application Modes for SYN Protection

The configuration is performed under **[Network Address Translation]**. Once selected, the interface switches to SYN Protection settings. When creating a new policy, administrators typically begin with IP address translation. The available modes include:

- **Mapped IP**: Maps an external IP address to a specific internal IP address, with all ports translated.
- **Mapped Port**: Maps a specific port of an external IP address to a specific port of an internal IP address.
- **Server Load Balance**: Maps a specific port of an external IP address to two or more internal IP addresses running the same service (e.g., web servers).

For explanations of these three options, please refer to Incoming > Basic Setting > Network Address Translation.

The Policy (Extra settings) for SYN protection only includes [Schedule], [QoS], and [Max. Concurrent Sessions for Each Source IP Address]. (See Figure 4-13)

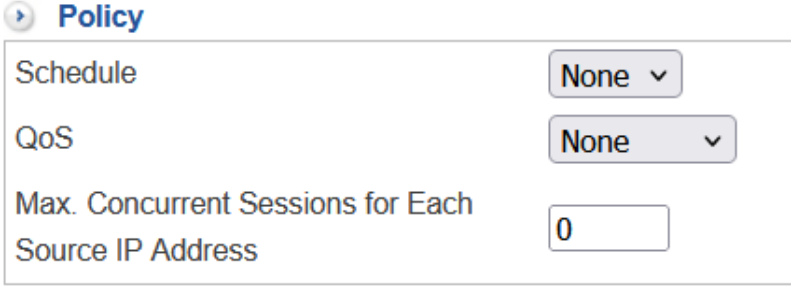


Figure 4-13

4-2. IPSec Policy

The configuration of IPSec policies is the same as other policy settings, except with fewer options and without the need to select a source interface.

Explanation of IPSec Policy Display Page

When accessing the IPSec policy section, the 3100-6GT-I lists all configured policies sequentially. Policies for IPv4 and IPv6 are displayed separately. By default, the system displays IPv4 policies. To switch to IPv6, click the IPv6 button at the top of the main menu, and the policy view will change accordingly.

Regardless of IPv4 or IPv6 mode, administrators can adjust the following items on this page: (See Figure 4-14)

- **[No.]**: The 3100-6GT-I executes IPSec policies starting from the first policy. The order of evaluation directly affects whether a packet is allowed or denied. To change a policy's priority, select the policy and assign a new number. For example, if the policy currently at priority 5 is changed to 2, it will be moved to the second position, and the policy originally at priority 2 will shift to priority 3, and so forth.
- **[On/Off]**: The toggle button for enabling or disabling an IPSec policy. Clicking the icon will disable a currently active policy, or enable one that is paused.
- **[Edit/Del]**: Allows modification or removal of the selected IPSec policy.
- **[Statistics]**: Displays the number of packets and total traffic matching each policy. Resetting or re-enabling a policy clears the counters. Clicking the numbers opens a detailed log of all packets that matched the policy.

  After configuring IPSec policies, this feature helps administrators verify whether packets are being matched by the intended rule.

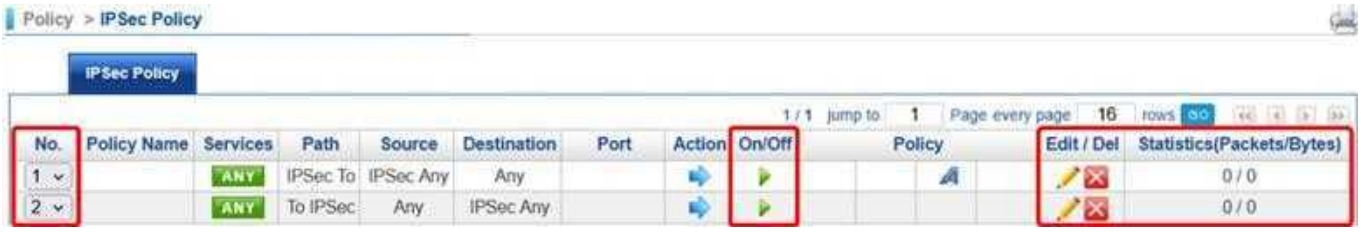
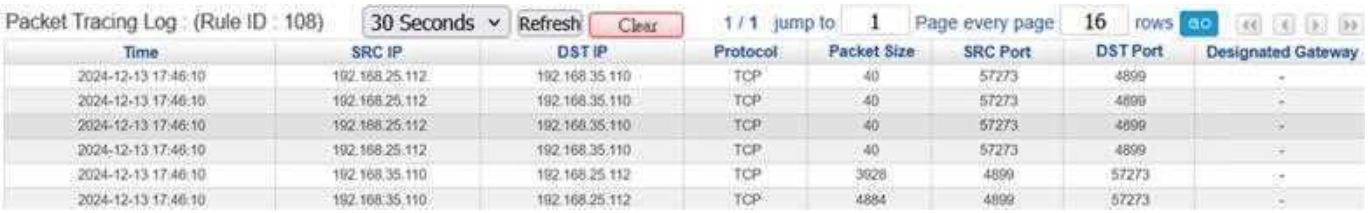


Figure 4-14

When troubleshooting IPSec network issues, administrators may need to verify whether traffic is being matched by a specific policy. The 3100-6GT-I provides a **real-time packet tracing log** feature for this purpose. By clicking the number shown under the **[Statistics]** column of an IPSec policy, the feature is activated, and the 3100-6GT-I captures the incoming and outgoing packets. A new window will then open to display the details for observation. (See Figure 4-15)

- **[Refresh]**: Updates the packet session records automatically every 3~30 seconds for easier monitoring.
- **[Clear]**: Deletes all current session records and restarts packet capture and display.
- **[Time]**: The timestamp when the IPSec packet passed through.
- **[SRC IP/Port]**: The source IP address and port that matched this IPSec policy.
- **[DST IP/Port]**: The destination IP address and port that matched this IPSec policy.
- **[Protocol]**: The protocol used by the IPSec policy, such as TCP, UDP, or ICMP.

- **[Packet Size]**: The size of the packet in bytes.
- **[Designated Gateway]**: The outbound line used by the packet when going from inside to outside. If "-" is displayed, it indicates that the packet is a TCP return packet from the remote side.



Time	SRC IP	DST IP	Protocol	Packet Size	SRC Port	DST Port	Designated Gateway
2024-12-13 17:46:10	192.168.25.112	192.168.35.110	TCP	40	57273	4899	-
2024-12-13 17:46:10	192.168.25.112	192.168.35.110	TCP	40	57273	4899	-
2024-12-13 17:46:10	192.168.25.112	192.168.35.110	TCP	40	57273	4899	-
2024-12-13 17:46:10	192.168.25.112	192.168.35.110	TCP	40	57273	4899	-
2024-12-13 17:46:10	192.168.35.110	192.168.25.112	TCP	3928	4899	57273	-
2024-12-13 17:46:10	192.168.35.110	192.168.25.112	TCP	4884	4899	57273	-

Figure 4-15

Basic Settings

Each IPSec policy defines its source and destination in the Basic Settings. Since this mechanism applies exclusively to IPSec VPN tunnels, one side of the source or destination will always be the IPSec tunnel. (See Figure 4-16)

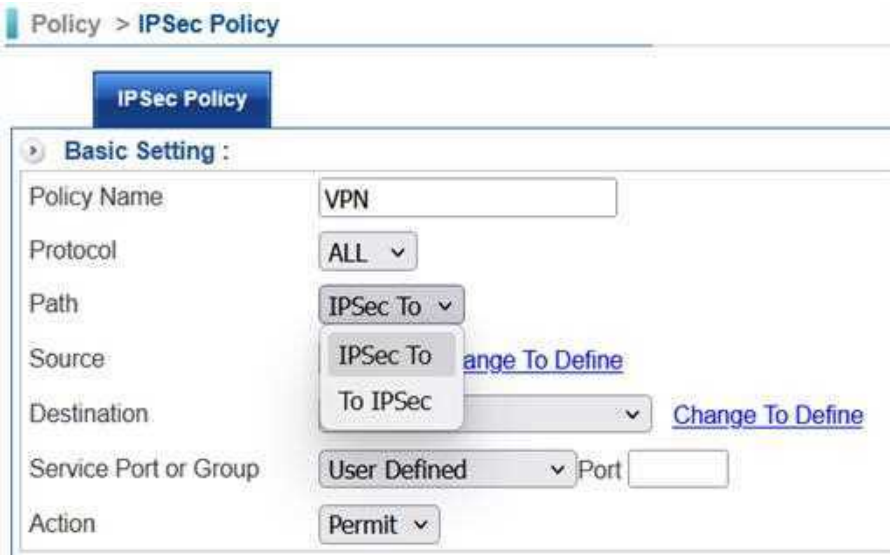


Figure 4-16

- **[Policy Name]**: The name of the IPSec policy. Any combination of Chinese or English characters can be used to make it easier to identify, for example, *Block Internet Access*.
- **[Protocol]**: Three protocol options are available: All, TCP, and UDP. The default is All.
- **[Path]**: Specifies the traffic direction, with two options: **To IPSec** and **IPSec To**.

  To IPSec: From the internal network through the IPSec VPN tunnel to the remote site.

  IPSec To: From the IPSec VPN tunnel into the internal network.
- **[Source]**: Determined by the previously defined **[Path]**. For example:

  If **Path = To IPSec**, the source network is the internal Zone IP address, and the destination network is the IP address on the remote side of the IPSec tunnel.

  If **Path = IPSec To**, the source network is the IP address on the remote side of the IPSec VPN tunnel, and the destination network is the internal Zone IP address.

- **Option Mode**: The system lists the address objects or groups that have been created under **[Object] > [IP Address]**, allowing administrators to select from predefined entries.
- **Define Mode**: Manually enter the source IP address or MAC address.

- **[Destination]**: Determined by the previously defined **[Path]**. For example:

  If **Path = To IPSec**, the destination network is the IP address on the remote side of the IPSec VPN tunnel.

  If **Path = IPSec To**, the destination network is the internal Zone IP address.

  - **Option Mode**: The system lists the address objects or groups that have been created under **[Object] > [IP Address]**, allowing administrators to select from predefined entries.
  - **Define Mode**: Manually enter the destination IP address.

- **[Service Port or Group]**: Defines which service ports are allowed through the IPSec VPN tunnel. There are three categories: **Default Service Table**, **Custom Service Group**, and **User-Defined**. The 3100-6GT-I provides a list of common services (e.g., HTTP, FTP).

  To simplify policy management, multiple services can be grouped into one service group, which must be defined under **[Object] > [Services]**. Defined objects will appear in the selection list, but administrators may also manually specify port numbers.

  Note: In both IPv4 and IPv6 environments, if no group is specified, all service ports are included by default.

- **[Action]**: Defines how packets matching the above criteria should be handled. Two modes are available: **Permit** (allow the traffic) or **Drop** (drop the traffic)

Policy (Extra Settings)

For network packets that match the **[Basic Settings]** rules and whose action is set to **Permit**, the 3100-6GT-I can apply the following three additional actions: **Schedule**, **QoS**, and **NAT** (only applicable when the path is **IPSec To**) (See Figure 4-17).

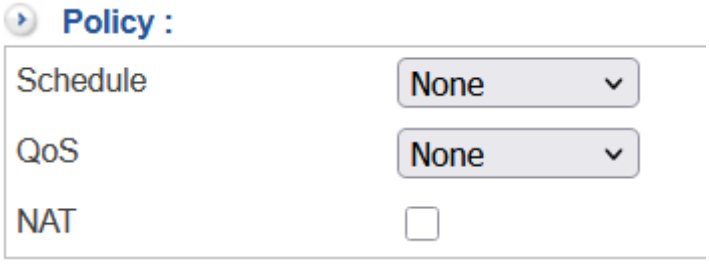


Figure 4-17

- **[Schedule]**: Define a schedule under **[Object]** > **[Schedule]**. The IPSec policy will only be effective during the defined schedule; outside the schedule, the policy becomes inactive.
- **[QoS]**: Define bandwidth limits under **[Object] > [QoS]**. The entire policy will be subject to the configured bandwidth limitation. If no bandwidth is defined, the policy uses the maximum available bandwidth of the line.
- **[NAT]**: For packets entering the network interface through the IPSec VPN tunnel, NAT can be applied. Once enabled, the source IP address of the packet is replaced with the internal IP address, typically the one bound to the internal interface. This is useful when internal servers restrict access to

specific source IP addresses (e.g., only allowing internal addresses). In such cases, instead of modifying the server's access rules, administrators can simply enable "**NAT**" in the policy.

4-3. Example of Policy Application

Using a practical example and configuration steps, we will demonstrate how to apply the 3100-6GT-I's policies to monitor all network traffic.

In this case, a factory deploys the 3100-6GT-I to control traffic between different network segments. Based on the environment, the network security architecture is divided into three major zones: **Internal Office**, **Remote Monitoring (Server Zone)**, and **Factory Zone (including production and manufacturing)**.

The overall network architecture is shown below (See Figure 4-18).

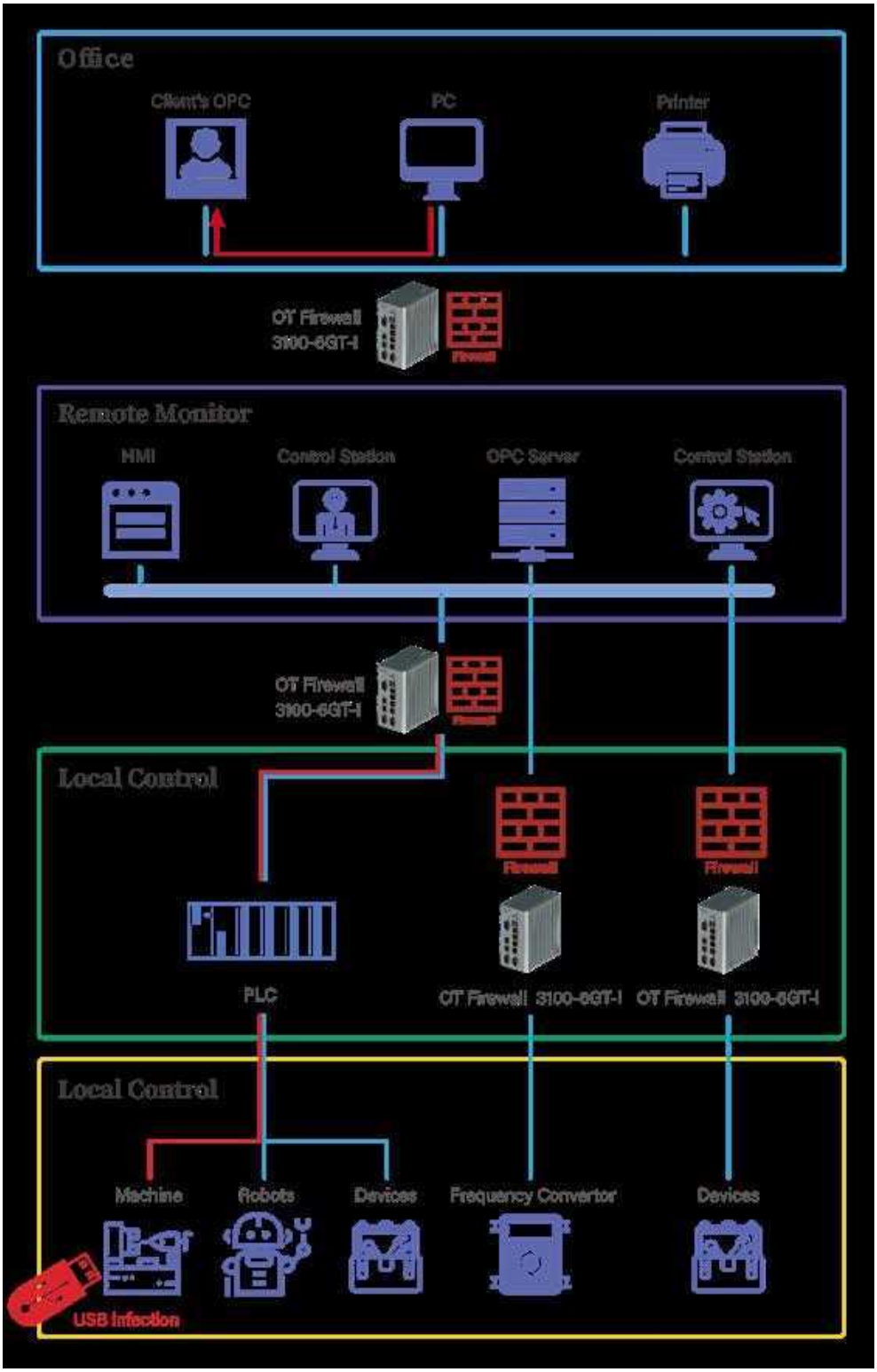


Figure 4-18

Example of Network Zones and Management Requirements

No.	Network Connection	Management Requirement
1	Internal Office ←→ Remote Monitoring	Since the Office Area can connect to the external network, access to the Remote Monitoring Area must be restricted. Only **WEB (Port 80)** connections are allowed, and OPC service must be enabled for the connection.
2	Remote Monitoring ←→ Factory Area	Connections between the Factory Area and Remote Monitoring Area must be restricted by **source**. The system should validate whether the connection behavior allows **read/write operations** and enable the **Modbus** service.

Common Configuration

In this example, a 3100-6GT-I model with six Gigabit ports is used to demonstrate the requirements of Example 1 and Example 2. All configurations are implemented in **Bridge mode** for traffic control and filtering.

Interface	Ports	IPv4 Address	Description
LAN	1 port (Port1)	192.168.1.0/24	Used as the management interface
Bridge	2 ports (Port2~Port3)	192.168.5.0/24	Bridges the two zones and applies filtering policies

Alternatively, the **Bridge** can be configured on **Port3~Port4**. For the 3100-6GT-I, these ports also support the **Bypass function**. When the system encounters a failure, network traffic will still pass through without interruption. (Ports that support the Bypass function are displayed in **[Network]** > **[Zone Setting]**.)

Step 1. Assign Physical Ports

In **[Network] > [Zone Setting]**, assign physical ports and zones according to the requirements described earlier. (See Figure 4-19)

Figure 4-19

Step 2. Configure IP Addresses for Each Interface (See Figure 4-20)

1. In **[Network] > [Interface]**, configure the IP address and subnet for each interface.
2. Newly created zones will automatically appear in the tabs at the top.
3. By default, new zones are set to **OFF**. They must be switched to **STATIC**, with the source interface checked and the source network entered before saving. (When enabling Bridge mode, the **LAN Acceleration Mode** must be disabled under [Configuration] > [Basic Setting] > [General Setting].)
4. If you wish to log in to the management interface through the **Bridge** interface, add the planned IP address and subnet under [Interface]. Except for WAN-type interfaces, which require a default gateway, other newly added zones can leave the default gateway field blank, as the configured IP address itself serves as the gateway for that Zone.
5. Whether to enable [Visit Control] and [Firewall Protection] is determined by the administrator.

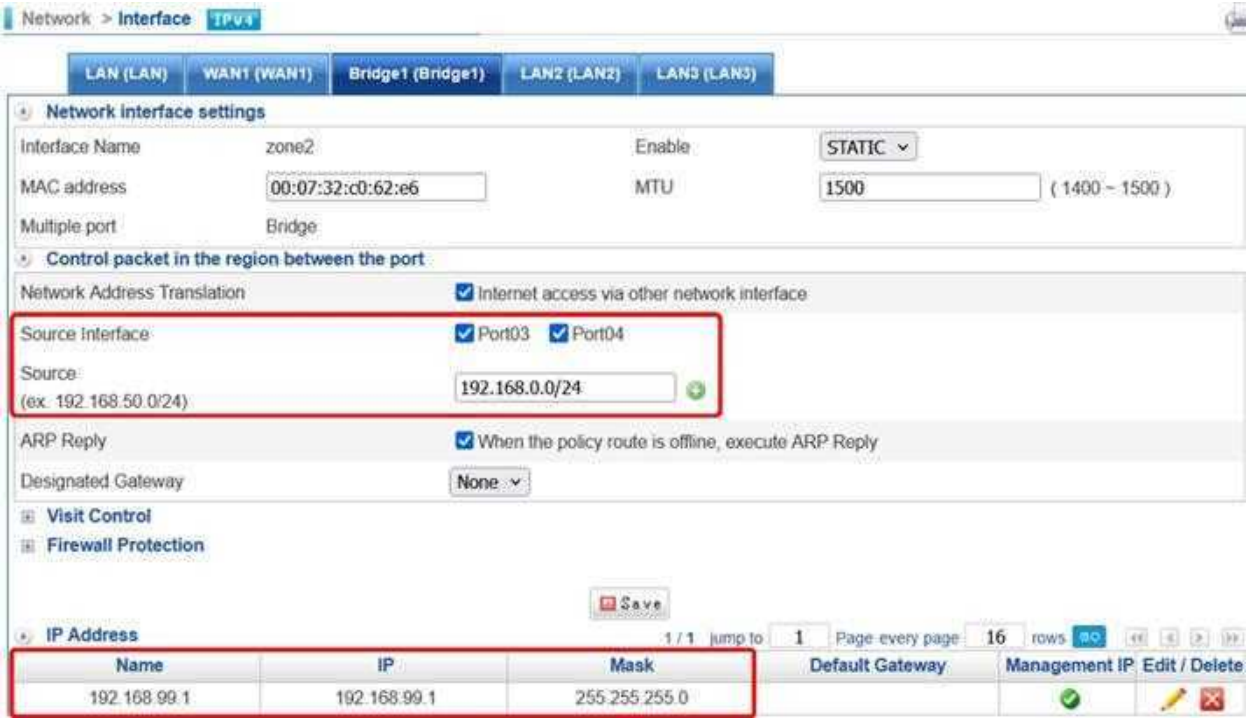


Figure 4-20

Step 3. Configure the Gateway (See Figure 4-21)

The 3100-6GT-I comes with a built-in database that is updated regularly, with online automatic updates enabled by default.

1. Go to **[Network] > [Route] > [Designated Gateway]** to configure the outbound connection.
2. If there are more than two connections, you can create a **[Designated Gateway Group]** to enable load balancing.

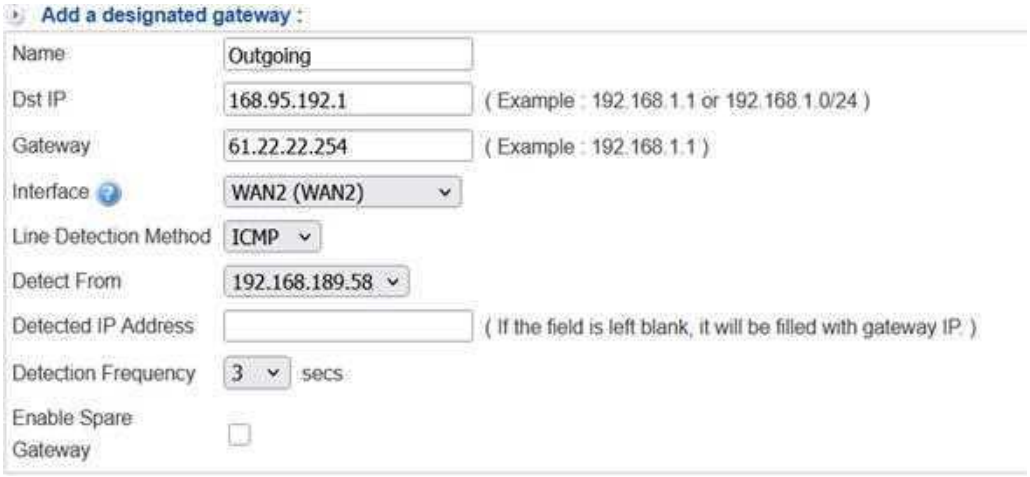


Figure 4-21

At this point, the entire network configuration of the 3100-6GT-I has been completed. The next step is to configure each requirement accordingly.

4-3-1. Example 1: Restrict Connections and Enable OPC Service

Example 1: Restrict office network connections and enable OPC

Step 1. Configure OPC Risk Level Filtering (See Figure 4-22)

Go to **[OPC] > [OPC Setting]** and add an "OPC Filter Setting".

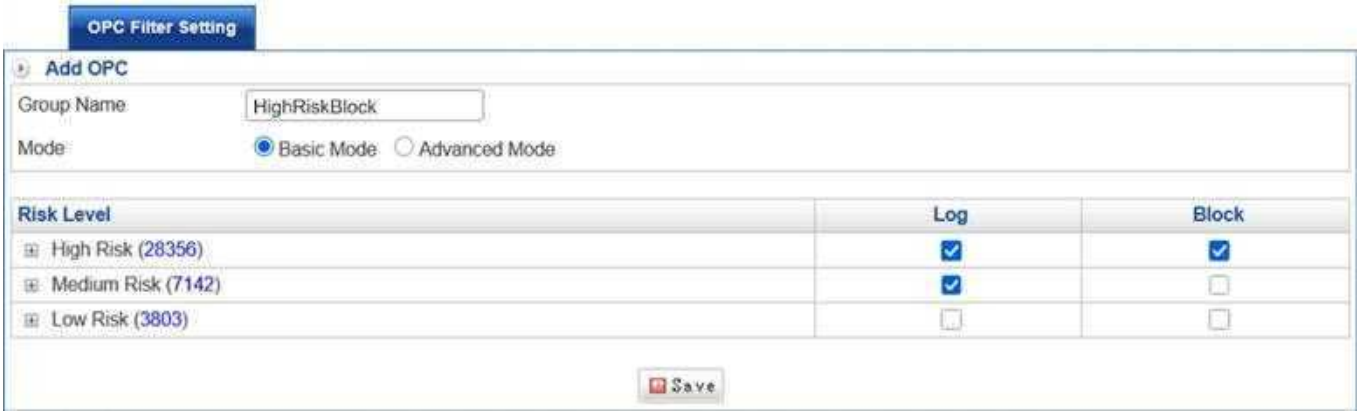


Figure 4-22

Step 2. Configure Policy

Create a new policy and configure it under the **Advanced** tab. Since earlier we set Port2~Port3 as a Bridge interface (with Port2 connected to the office network and Port3 connected to the remote monitoring network), the remote monitoring network will not actively connect to the outside.

Therefore, only one policy needs to be configured for the office network connecting to the monitoring network (default behavior is to block all traffic) (See Figure 4-23).

Figure 4-23

In the Policy (Extra settings), expand and select the previously created OPC "**HighRiskBlock**" (See Figure 4-24).

Figure 4-24

This completes the policy configuration (See Figure 4-25).

Figure 4-25

4-3-2. Example 2: Enable Modbus Monitoring and Restrict Connections

Example 2: Restrict connections between the remote monitoring network and the factory network, while enabling Modbus to control permitted read/write actions. (This example demonstrates the monitoring network retrieving data from the production network.)

Step 1. Configure Modbus Parameters

For demonstration purposes, Modbus is simulated using software tools. First, configure the related parameters (ID: 1, Function Code: 03, Address: 0).

Since the monitoring area continuously pulls data from the production network, only one policy needs to be set for this traffic direction, with the **Read** command enabled. (If write access is required, then enable the related Write function codes.)

Modbus Slave/Modbus Poll simulator configuration (See Figures 4-26 and 4-27).

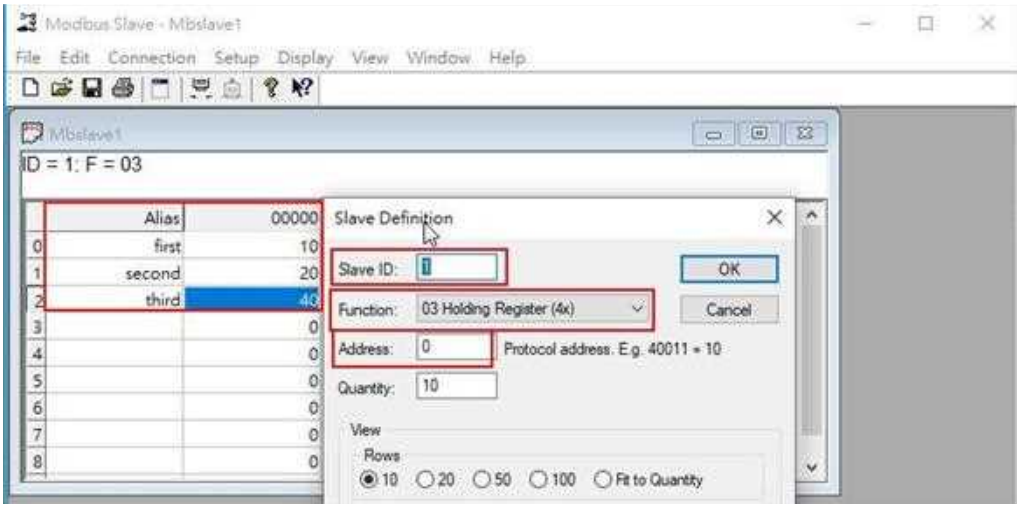


Figure 4-26

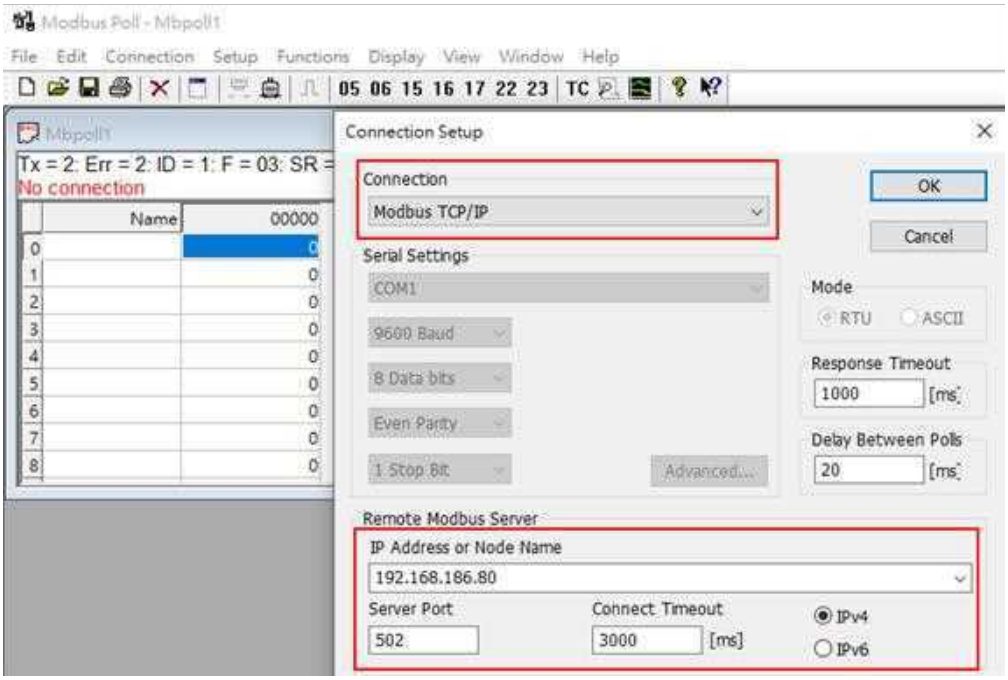


Figure 4-27

Step 2. Configure Policy

Create a policy, specifying the connection direction and service port, then configure Modbus/TCP parameters (See Figure 4-28).

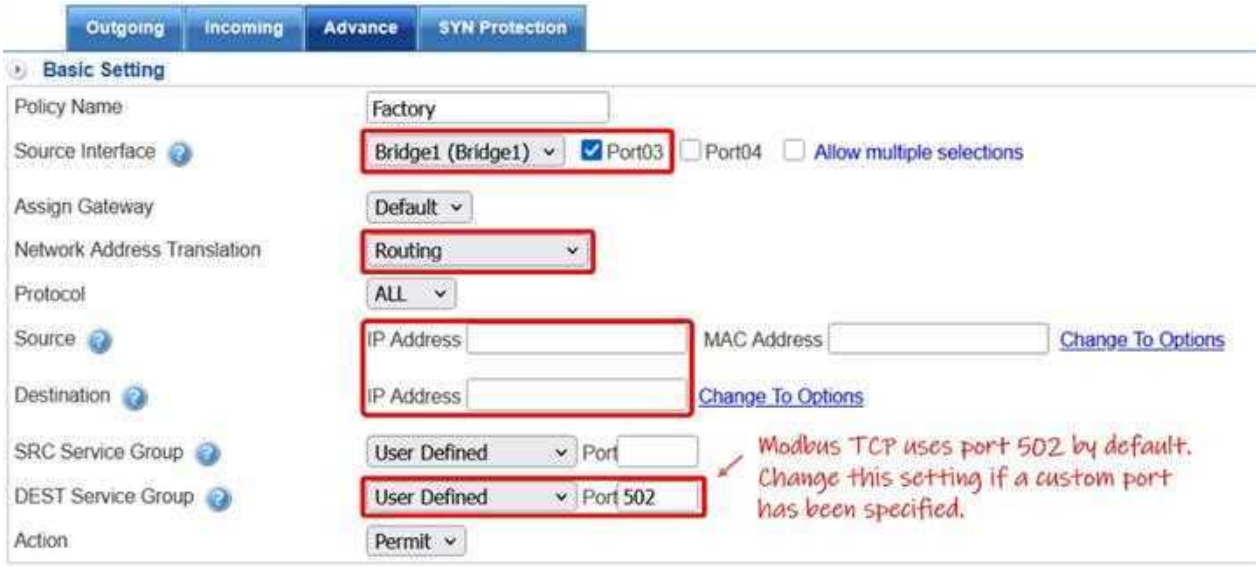


Figure 4-28

Industrial Protocol – Configure Modbus/TCP parameters (example allows only Function Code 3 - Read) (See Figure 4-29).

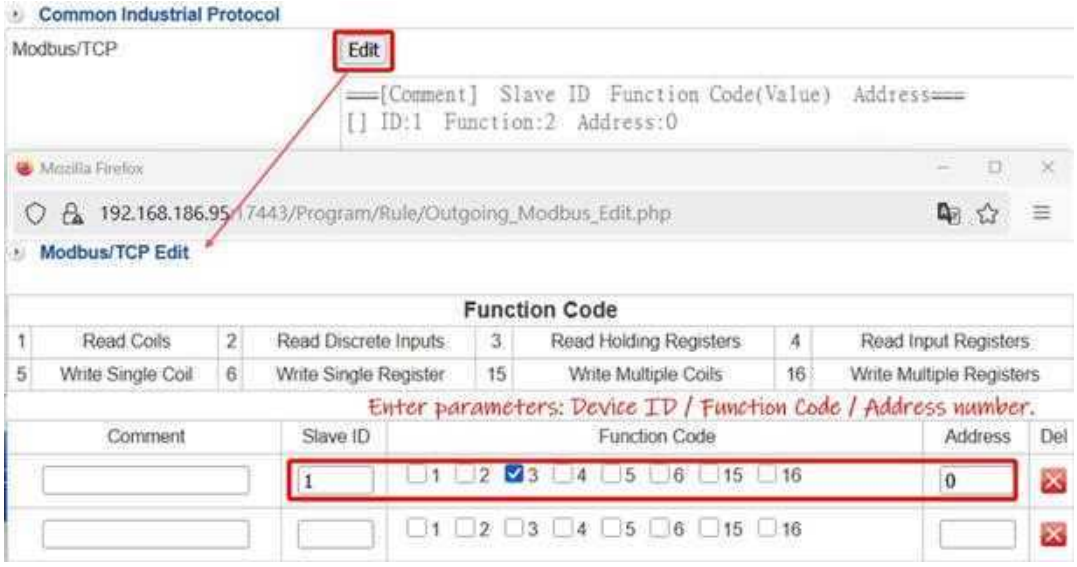


Figure 4-29

The policy is now complete (See Figure 4-30).

Figure 4-30

After completing the setup, test with the Modbus simulation software. The client values can be retrieved. The slave is configured with three values on the left. The Poll tool reads and displays the three values. It has polled 6 times with Function Code 3 on the right (See Figure 4-31).

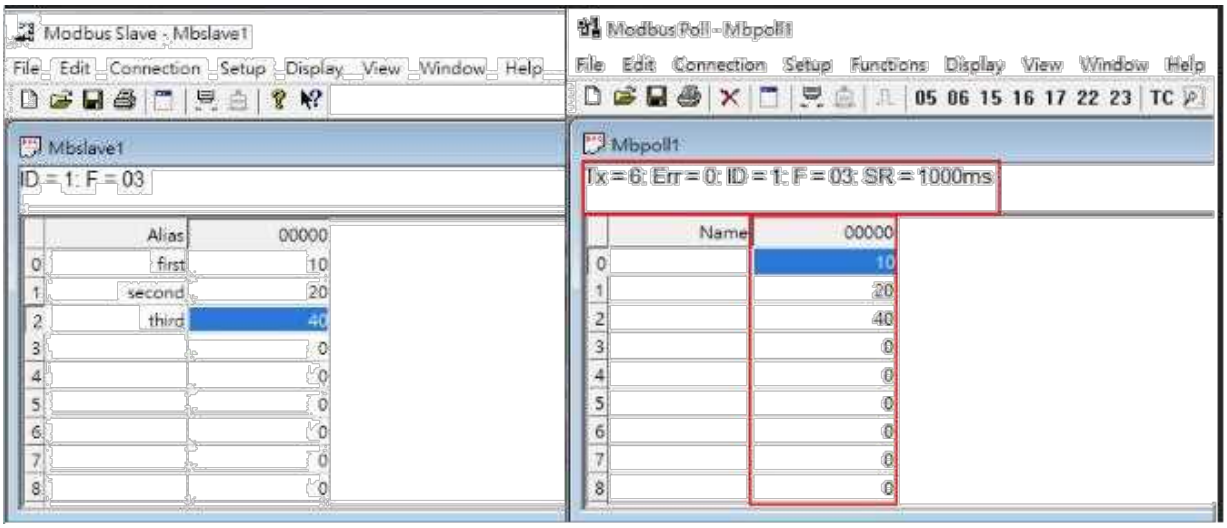


Figure 4-31

If Function Code 3 is removed from the policy and replaced with Function Code 2, the values will no longer be retrievable (See Figure 4-32).

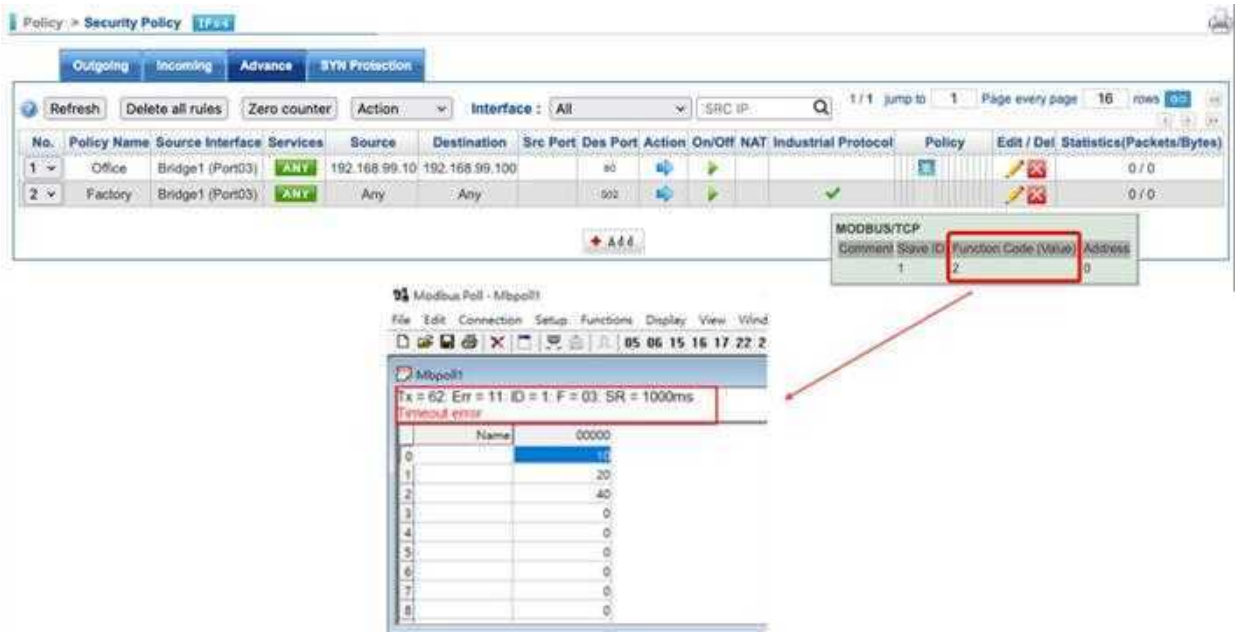


Figure 4-32

Chapter 5. Object

The 3100-6GT-I adopts an object-oriented approach to manage the entire device. All objects or targets must be predefined before being applied in policy rules to allow or deny traffic. In addition to the traditional **IP Address** as a management object, elements such as Zones, interface addresses, routing tables, and even designated gateways can also serve as objects.

The purpose of defining management objects is to make it easier for administrators to identify the intent and usage of each policy when creating them. However, administrators may also choose not to define any management objects in advance, and instead directly enter IP addresses and ports within the policies to enforce control.

5-1. IP Address

The 3100-6GT-I supports both IPv4 and IPv6 address modes. The blue buttons displayed above the menu indicate the current mode. IPv4 represents the IPv4 address mode being displayed/set, while IPv6 represents the IPv6 address mode being displayed/set. Clicking on the gray button (such as IPv6) directly switches the display and settings to the other mode.

These two buttons apply to the entire system, allowing for switching at any time. The settings interface will switch to the selected IPv4 or IPv6 mode accordingly.

5-1-1. IP Address

Predefined **IP Address Object** make the creation of policies clearer and more straightforward. Each address object can represent a single IP address, an IP subnet, or an IP range.

Assist

This feature only supports **IPv4**. Any device that has network packets passing through the 3100-6GT-I, whether from the external or internal network, will be recorded by the system to help administrators build address objects more easily.

By clicking the "**Assist**" icon, the system will display all detected computer names, IP addresses, and MAC addresses, including fixed IP addresses obtained from the DHCP server. The administrator can simply select the desired IP or MAC address and click the "**Add**" button, and the system will automatically add the information to the address object. (See Figure 5-1)

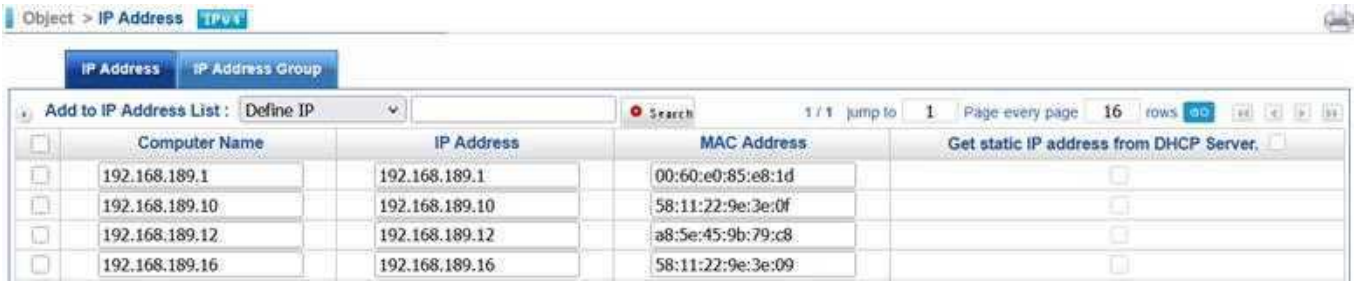


Figure 5-1

Add Address Object

Click the "Add" button to create a new address object. There are six available creation modes, each serving a specific purpose.

1. **IP Address**

   This method supports both IPv4 and IPv6. It identifies users based on their IP addresses and is suitable for network environments where each device uses a fixed IP.

   - **[Computer Name]**: A descriptive name for the IP address, e.g., “John’s PC.”
   - **[IP Address]**: Enter the IP address, e.g., 192.168.1.1.

2. **IP and MAC Address**

   This mode is applicable to IPv4 only. It binds a user to both an IPv4 address and a MAC address. Suitable for environments where each device either uses a fixed IP or receives a static IP via DHCP.
   Note: There must be no Layer 3 router between the device and the 3100-6GT-I.

   - **[Computer Name]**: A descriptive name for the IP address, e.g., “John’s PC.”
   - **[IP Address]**: Enter the IPv4 address, e.g., 192.168.1.1.
   - **[MAC Address]**: The physical MAC address of the device, e.g., 00:01:02:03:04:05.
   - **[DHCP]**: In DHCP environments, the DHCP server can assign a fixed IPv4 address to the same MAC address. Select this option if the device is assigned a static IPv4 address via DHCP.

3. **MAC Address**

   Applicable to IPv4 only. Identifies users based solely on their MAC address, regardless of IP address.

   - **[Computer Name]**: A descriptive name for the MAC address, e.g., “John’s PC.”
   - **[MAC Address]**: The physical MAC address of the device, e.g., 00:01:02:03:04:05.

4. **IP/Mask**

   Supports both IPv4 and IPv6. Identifies a group of users within a subnet using an IP address and subnet mask.

   - **[Computer Name]**: A descriptive name for the subnet, e.g., “Engineering Department PCs.”
   - **[IP Address]**: Enter the IP address, e.g., 192.168.1.1.
   - **[Netmask Mask]**: Select the appropriate subnet mask, e.g., 255.255.255.0/24.

5. **IP Range**

   Supports both IPv4 and IPv6. Identifies a group of users based on a range of IP addresses.

   - **[Computer Name]**: A descriptive name for the range, e.g., “Engineering Department PCs.”
   - **[Start IP]**: Enter the starting IP address of the range, e.g., 192.168.1.1.
   - **[End IP]**: Enter the ending IP address of the range, e.g., 192.168.1.100. This defines a pool of 100 IPv4 addresses for the engineering department.

6. **User-defined Domain**

   Supports both IPv4 and IPv6. Identifies a group of users by domain name. Suitable for external servers or environments with valid domain name resolution.

   - **[Computer Name]**: A representative name for the domain, e.g., “John’s Home.”
   - **[Domain]**: Enter the domain information. Multiple entries can be specified, one per line. Wildcards (*) are supported, e.g., *.example.com or example.com.*.

5-1-2. IP Address Group

Each address object can represent a single IP address or an IP subnet. Multiple address objects can be grouped into an **address group**. An address group may include both individual address objects and other address groups. Click the “Add” button to begin creating an address group. (See Figure 5-2)

- **[Group Name]**: A descriptive name for the address group, e.g., “2F Computers.”
- **[All Members]**: Displays all address objects that have been created. Administrators can select from this list.

  >>>

- **[All Other Groups]**: Displays all previously created address groups. Administrators can select from this list.

  >>>

- **[All Locations]**: Provides a list of selectable address objects organized by location.

  >>>

- **[User-defined]**: Manually enter entries that are not pre-defined.

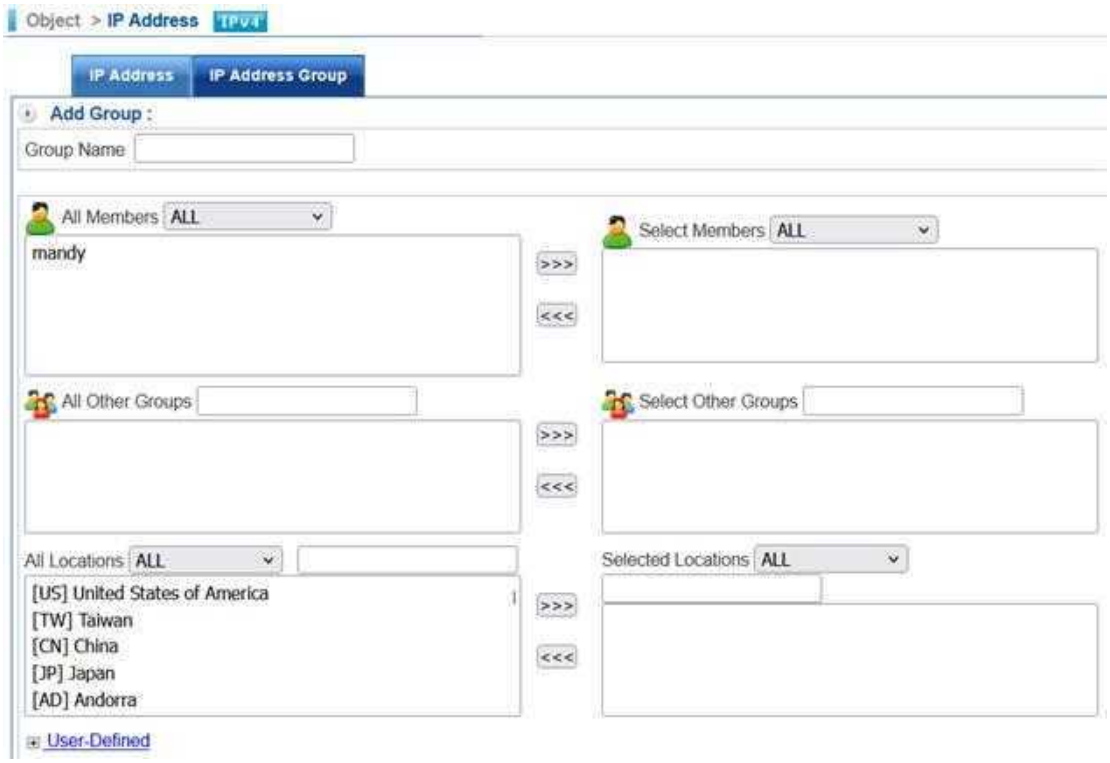


Figure 5-2

5-2. Services

TCP and UDP protocols provide various services, each identified by a specific TCP port or UDP port number—for example, TELNET (23), FTP (21), SMTP (25), and POP3 (110), among others.

The “Assist” section lists commonly used TCP/UDP services for quick selection. These built-in services are predefined and cannot be modified or deleted.

Additionally, users can create custom services by specifying appropriate TCP and UDP port numbers in the user-defined service list. When defining custom services, the client port range is typically set from **1024 to 65535**, while the server port range can be **0 to 65535**.

Note that services defined in the service list differ slightly from those defined at the application level. For example, HTTP is defined in the service list as TCP port 80. However, not all traffic on TCP port 80 is guaranteed to be HTTP, and HTTP traffic does not always use TCP port 80.

At the application level, HTTP is identified based on protocol behavior, regardless of source or destination port. As a result, application-based service recognition provides more accurate protocol detection.

System administrators can create service groups under the **[Services] > [Service Group]**. A service group consists of multiple services grouped under a single name.

Using service groups significantly simplifies policy configuration. For example, suppose there are 10 different IP addresses that need access to 5 different services—HTTP, FTP, SMTP, POP3, and TELNET. Without service groups, administrators would need to define **10 × 5 = 50 separate policies**.

However, by grouping the services and referencing the group in the policy, only **one policy** is needed to achieve the same effect.

5-2-1. Basic Service

The 3100-6GT-I provides a basic service list that includes commonly used services and protocols. (See Figure 5-3)

Figure 5-3

Service List Icons

The following icons are used in the service list. These icons are standardized and apply throughout the 3100-6GT-I interface.

Icon	Introduction
ANY	Any service.
TCP	TCP-based services include: Gopher, ICQ, Ident, LDAP, NNTPoverSSL, PPTP, SFTP, SSH, Terminal, WINFRAME, AFPoverTCP, FTP, H.323, L2TP, MSN Messenger, POP2, SMTPoverSSL, Yahoo, AOL, Finger, HTTP, IMAPoverSSL, LDAP Admin, NNTP, POP3overSSL, RLOGIN, SMTP, VNC, BGP, Gnutella, HTTPS, IMAP, LDAPoverSSL, POP3, RealAudio, Telnet, WAIS.
UDP	UDP-based services include: DNS, TFTP, NTP, SNMP, IKE, SYSLOG, RIP, UUCP, and others.

5-2-2. Service Group

By default, when creating a new service group, 8 blank entries are provided. Administrators can begin adding services sequentially starting from entry No. 1.

If more than 8 services are required, click **"More"** to add 4 additional blank entries. (See Figure 5-4)

- **[Group Name]**: Identifies the name of this service group, e.g., "Mail Server."
- **[Assist]**: Select from the predefined service list.
- **[Protocol]**: Specify whether the service uses TCP, UDP, or a custom protocol.
- **[Port (Start:End)]**: Define the start and end port numbers used by the service.
  1. Example: SMTP uses only TCP port 25 → enter 25:25.
  2. Example: POP3 uses only TCP port 110 → enter 110:110.

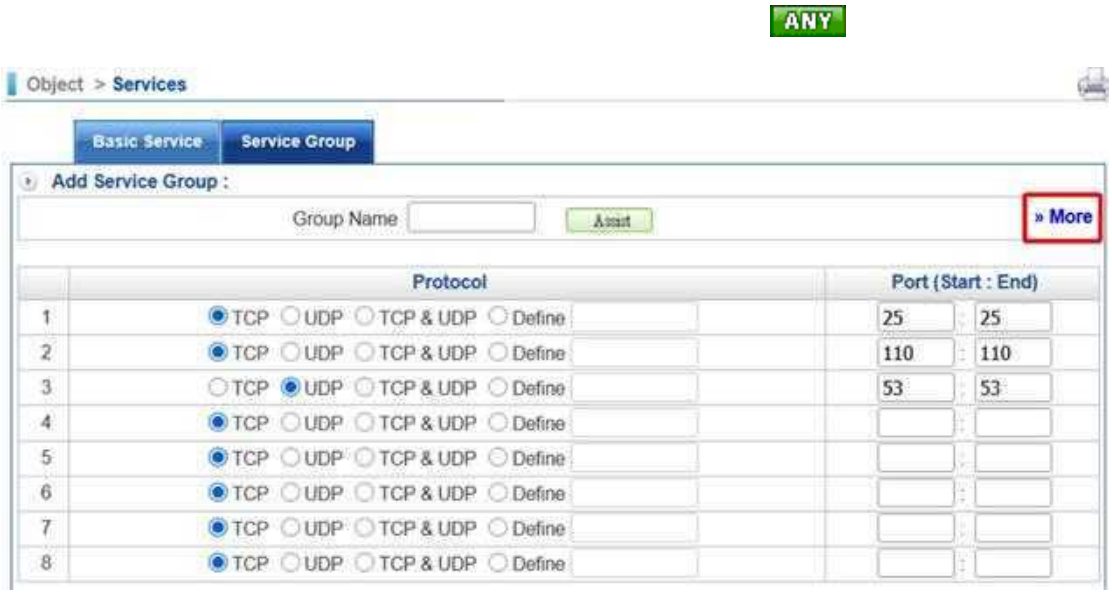


Figure 5-4

Assist

When creating a new service group, click the **"Assist"** icon to display the service list built into the 3100-6GT-I. Administrators can simply select the required services. Switching between Industrial Protocols, TCP, UDP, or Other Protocols will list the corresponding available communication protocols. (See Figure 5-5)

- **[Industrial Protocol]**: Includes commonly used industrial control protocols, e.g., EtherCAT, Citrix.
- **[TCP]**: Includes commonly used TCP-based services, e.g., SSL, HTTP.
- **[UDP]**: Includes commonly used UDP-based services, e.g., DNS, SNMP.
- **[Other Protocol]**: Includes less frequently used services, e.g., EGP, RDP.

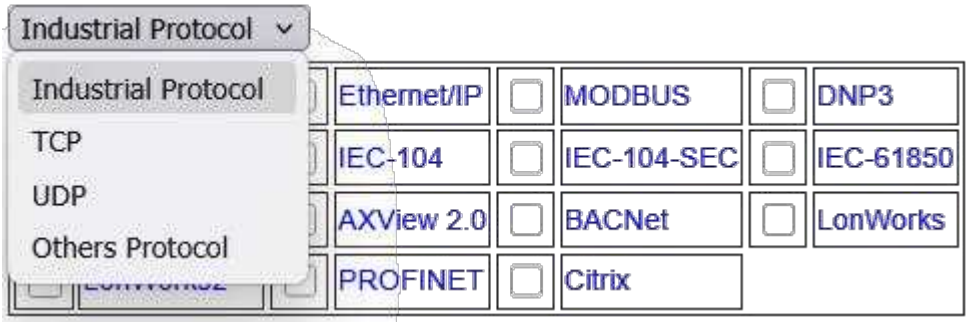


Figure 5-5

After the creation, the 3100-6GT-I displays a list of all defined service groups, along with their associated port numbers. (See Figure 5-6)

Figure 5-6

5-3. Schedule

The 3100-6GT-I provides a scheduling function that allows system administrators to define time periods in advance based on operational requirements. These schedules can then be applied to policies, enabling a policy to take effect only during specified time periods.

The same policy can also be applied with different schedules, effectively creating two distinct policies to meet different time-based control requirements.

Schedule List

The schedule configuration provides three modes:

1. **Mode 1**: Weekly cycle — define the active time range for each day.
2. **Mode 2**: Custom — specify custom start and end dates and times.
3. **Mode 3**: Graphical — configure the schedule by selecting time blocks from a chart.

- **[Schedule Name]**: Identifies the name of this schedule, e.g., “Daytime Policy,” “Nighttime Policy.”
- **[Setting Mode]**: Three modes are available.
  - **Mode 1**: Weekly cycle — define daily active time periods. Three options are available: *Disable*, *All Day*, or *Start to End Time*. For example, if the start time is set to 00:00 and the end time is set to 00:00, the schedule represents **All Day**. (See Figure 5-7)

Figure 5-7

  - **Mode 2**: Custom — Administrators can configure a schedule to be effective during specific dates. For example, a schedule can be set to start on September 8, 2025 and end on September 16, 2025. (See Figure 5-8)

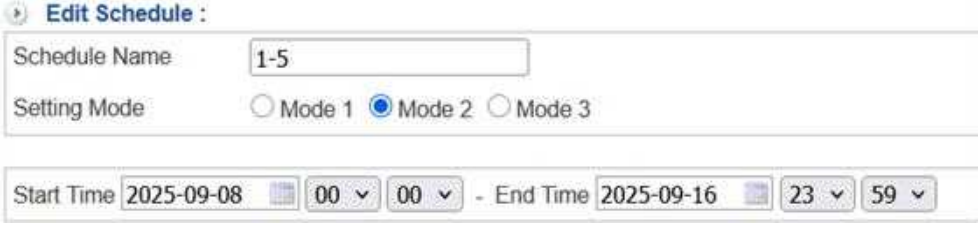


Figure 5-8

- **Mode 3**: Graphical — Administrators can define the active schedule by selecting time blocks from a chart. Unlike **Mode 1**, multiple active periods can be set within the same day.

  For example, Monday through Friday may be configured as 06:00–11:59 and 13:00–20:59, while Saturday and Sunday are configured as All Day. (See Figure 5-9)

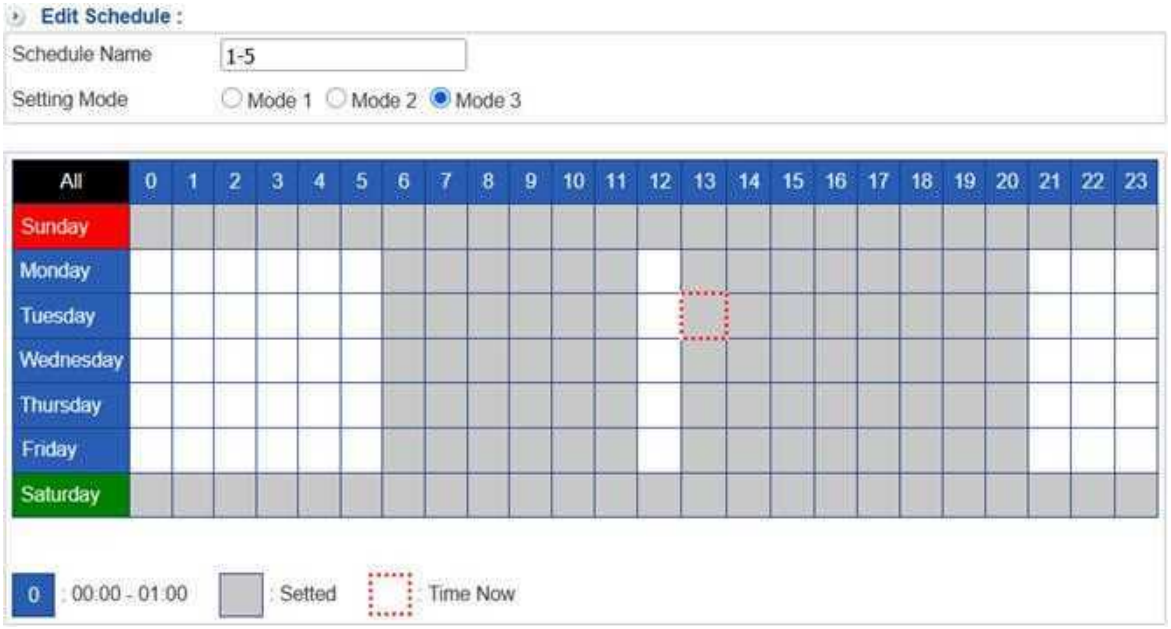


Figure 5-9

5-4. QoS (Bandwidth Management)

The 3100-6GT-I can manage the transmission speed of network service packets passing through interfaces. By using pre-defined **bandwidth tables**, administrators can precisely control the upload and download bandwidth for each policy across a Zone. With the concept of **bandwidth priority**, higher-priority packets can be forwarded more quickly.

Two configuration modes are available:

1. Bandwidth management per policy.
2. Bandwidth management per source IP address within a policy.

Since bandwidth management is based on Zone interfaces that connect the entire network, it is necessary to define the upload and download speeds for each Zone in advance.

For example, assume **Zone1** contains two physical ports—**Port A** and **Port B**—each with a link speed of 1 Gbps. If the bandwidth table assigns **10 Mbps for Internet access** and this is applied per source IP address, then regardless of whether traffic comes from Port A or Port B, any IP address within this Zone will be limited to **10 Mbps upload and 10 Mbps download**.

5-4-1. QoS Setting

Interface Speed Configuration

The maximum network speed for each interface is set here, including **Zone Out (TX)** and **Zone In (RX)** traffic. Incoming network packets to physical ports are considered Zone In (RX) traffic, while outgoing network packets from physical ports to downstream devices are considered Zone Out (TX) traffic.

This configuration works seamlessly in symmetric networks—such as internal LANs or switches—where upload and download speeds are equal. However, in asymmetric WAN environments, the directions differ.

For WAN connections (e.g., ADSL), the bandwidth provided by the ISP for upload and download is reversed relative to how the 3100-6GT-I perceives traffic. Therefore, when configuring Zone speeds in such environments, administrators must carefully account for this directionality. (See Figure 5-10)

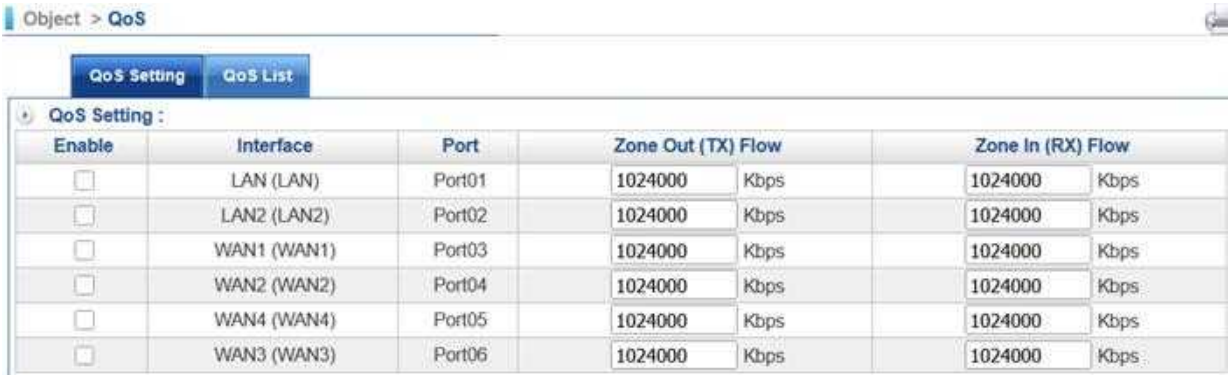


Figure 5-10

By default, the 3100-6GT-I sets the upload and download speed of all Zones to 1 Gbps (1024 Mbps = 1,024,000 Kbps) and lists the physical ports included in each Zone.

Administrators can modify these speeds to match actual line conditions. Once saved, the configured speed becomes the **maximum bandwidth limit** that can be applied when creating bandwidth tables.

5-4-2. QoS List

Each configured QoS will be listed here for easy reference and management. Modifications and deletions can also be made here.

Add QoS Rule

- **[QoS Name]**: Identifies the name of the bandwidth table, e.g., “Daytime Internet” or “Evening Access.”
- **[Priority]**: When interface bandwidth is still available, the 3100-6GT-I allocates the remaining bandwidth according to priority, allowing users to potentially reach their configured maximum bandwidth.
- **[Setting Mode]**: Two options are available: **Basic Mode** and **Advanced Mode**.

  ■ **Basic Mode**

  Bandwidth management is applied per Zone, regardless of how many physical interfaces the Zone contains. For example, if each WAN line is configured as an independent WAN ZONE, this mode is suitable. (See Figure 5-11)

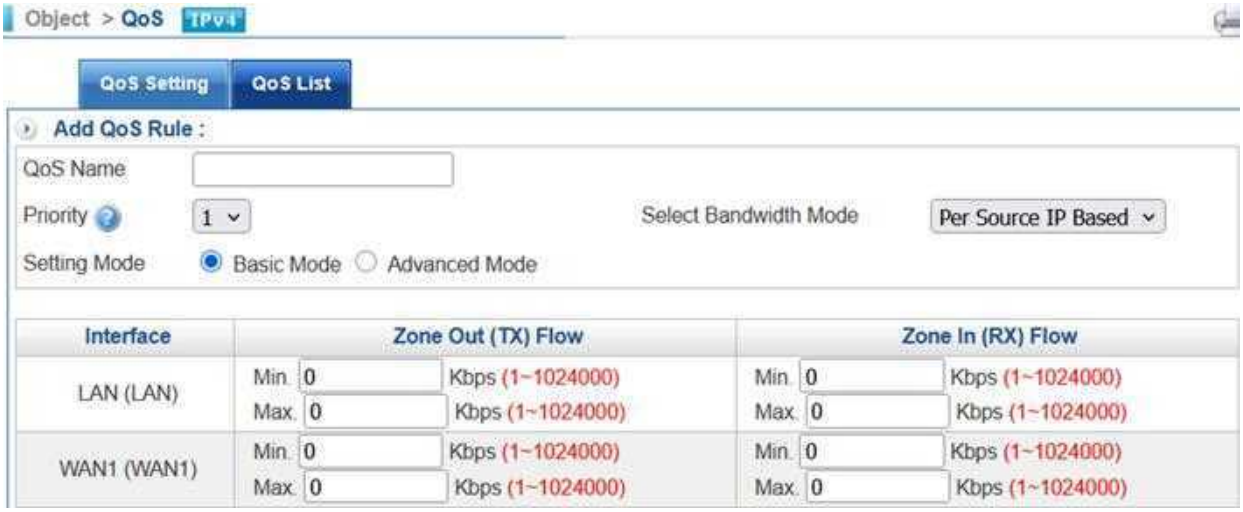


Figure 5-11

  ■ **Advanced Mode**

  Bandwidth management is applied per physical interface. For example, if three lines are grouped into a single WAN Zone, selecting this mode allows each line to be managed individually. (See Figure 5-12)

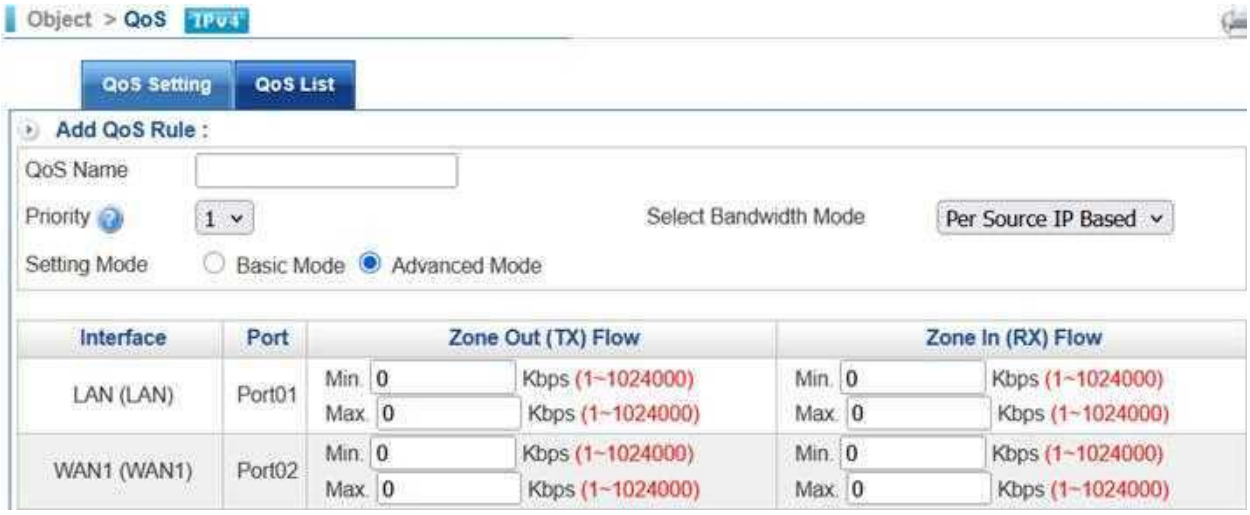


Figure 5-12

- **[Select Bandwidth Mode]**: Two options are available: **Per Policy Based** and **Per Source IP Based**.

  - **Per Policy Based**

    When a bandwidth table is applied to a policy, all source IP addresses (IPv4 or IPv6) that match the policy share the same bandwidth limit defined in the table. This means the total bandwidth available is divided among all matching users.

    Example: If the bandwidth table is set to **10 Mbps upload / 10 Mbps download**, and both 192.168.1.2 and 192.168.1.3 match the policy, then:

    - If 192.168.1.2 consumes **9.9 Mbps / 9.9 Mbps**,
    - 192.168.1.3 will only have **0.1 Mbps / 0.1 Mbps** available.

  - **Per Source IP Based**

    When a bandwidth table is applied to a policy, each source IP address (IPv4 or IPv6) that matches the policy is allowed to use the full bandwidth defined in the table. This means every IP address has its own allocation, independent of other users.

    Example: If the bandwidth table is set to **10 Mbps upload / 10 Mbps download**, and both 192.168.1.2 and 192.168.1.3 match the policy, then:

    - 192.168.1.2 can use up to **10 Mbps / 10 Mbps**,
    - 192.168.1.3 can also use up to **10 Mbps / 10 Mbps**.

  Note: Administrators must carefully consider the number of IP addresses and the total allocated bandwidth to avoid exceeding the maximum interface speed.

  For example, if the policy covers **100 IP addresses** and each is allocated **20 Mbps**, the total possible bandwidth is: 100 × 20 Mbps = 2000 Mbps = 2 Gbps

  Since this exceeds an interface limit of **1 Gbps**, the system may not be able to enforce bandwidth distribution accurately.

- **[Interface – Minimum]**: Select the interface where the QoS table will be applied. The system displays the maximum available network speed. This setting defines the guaranteed bandwidth for users under this policy when the 3100-6GT-I experiences network congestion.

- **[Interface – Maximum]**: The system displays the maximum available network speed. This setting defines the maximum bandwidth a user under this policy can receive when the 3100-6GT-I is not congested. Bandwidth is allocated based on priority.

5-5. Firewall Protection

This feature proactively detects and blocks attacker traffic—mitigating threats such as DoS, DDoS, UDP flood, and similar attacks—to protect internal users.

Attacks do not always originate from outside; lateral/internal attacks also occur in real-world environments. Volktek applies a “reasonable traffic and connection count” principle: a single host should not generate an excessive number of simultaneous connections. If a host exceeds those reasonable thresholds, the firewall—combined with applicable policies—will block the excess connections.

Common Attacker Techniques (Denial-of-Service Attacks)

- **SYN Attack (SYN Flood)**

  A SYN Flood is a form of DDoS that exploits a weakness in the TCP handshake. The attacker sends a large volume of spoofed TCP SYN requests, causing the target to exhaust resources (CPU or memory) while waiting for handshake completion.

- **ICMP Attack (ICMP Flood)**

  ICMP (Internet Control Message Protocol) is used within the TCP/IP suite for control and diagnostic messages. ICMP-based attacks send a large volume of ICMP traffic (for example, echo requests) to overwhelm the target and disrupt service.

- **UDP Attack (UDP Flood)**

  Attackers send a large volume of spoofed UDP packets or UDP requests to consume the target’s resources (CPU, bandwidth, or memory), resulting in service disruption.

- **Land Attack**

  Using IP spoofing, the attacker sends a stream of SYN packets to the target with identical source and destination addresses/ports. The victim attempts to reply to itself (SYN-ACK to itself), which can cause the system to malfunction or crash.

- **Smurf Attack**

  Named after the original exploit tool “Smurf,” this attack combines IP spoofing with ICMP echo requests sent to broadcast addresses. Many hosts reply to the spoofed victim IP, amplifying traffic and overwhelming the victim (an amplification/reflection effect).

- **Teardrop Attack (Teardown / Teardrop)**

  Exploits flaws in IP fragment reassembly. The attacker crafts overlapping IP fragments with conflicting fragment offsets; when the target attempts to reassemble them, the overlap can trigger kernel/stack errors and cause system crashes.

- **Ping of Death**

  Sends oversized or specially malformed ICMP Echo Request (ping) packets that cause buffer overflows on the target, potentially leading to crashes or instability.

5-5-1. Firewall Protection

To protect against DoS and DDoS attacks, the 3100-6GT-I allows administrators to configure threshold values for SYN, ICMP, and UDP protocols. (See Figure 5-13)

Generic Settings

- **[Permanently Block]**: If the same source IP triggers one of the detections below more than a set number of times, it will be permanently blocked. The threshold count can be viewed under section 5-5-2. Attack Log.
- **[Unblock IP]**: Blocked IPs will appear here.

Sandstorm

- **[Sandstorm]**: Displays the operating status of Sandstorm.

SYN Attack Detection Setting

- **[Maximum Allowed Flow]**: The maximum number of packets per second that each external IP address protected by the firewall can handle. The default is 10,000 packets/second. If exceeded, the firewall considers it an attack.
- **[Maximum Flow per Source IP]**: The maximum number of packets per second allowed from a single source IP. The default is 100 packets/second. If exceeded, the firewall considers it an attack.
- **[Block Duration]**: The amount of time the firewall will drop packets from an attacker’s IP once an attack is detected. The default is 60 seconds.

ICMP Attack Threshold Settings

- **[Maximum Allowed Flow]**: Default is 10,000 packets per second. If this value is exceeded, the firewall considers the protected IP to be under attack.
- **[Maximum Flow per Source IP]**: Default is 100 packets per second. If this value is exceeded, the firewall considers the protected IP to be under attack.
- **[Block Duration]**: The time the firewall will automatically drop packets from the attacker's IP once an attack is detected. Default is 60 seconds.

UDP Attack Threshold Settings

- **[Maximum Allowed Flow]**: Default is 10,000 packets per second. If this value is exceeded, the firewall considers the protected IP to be under attack.
- **[Maximum Flow per Source IP]**: Default is 100 packets per second. If this value is exceeded, the firewall considers the protected IP to be under attack.
- **[Block Duration]**: The time the firewall will automatically drop packets from the attacker's IP once an attack is detected. Default is 60 seconds.

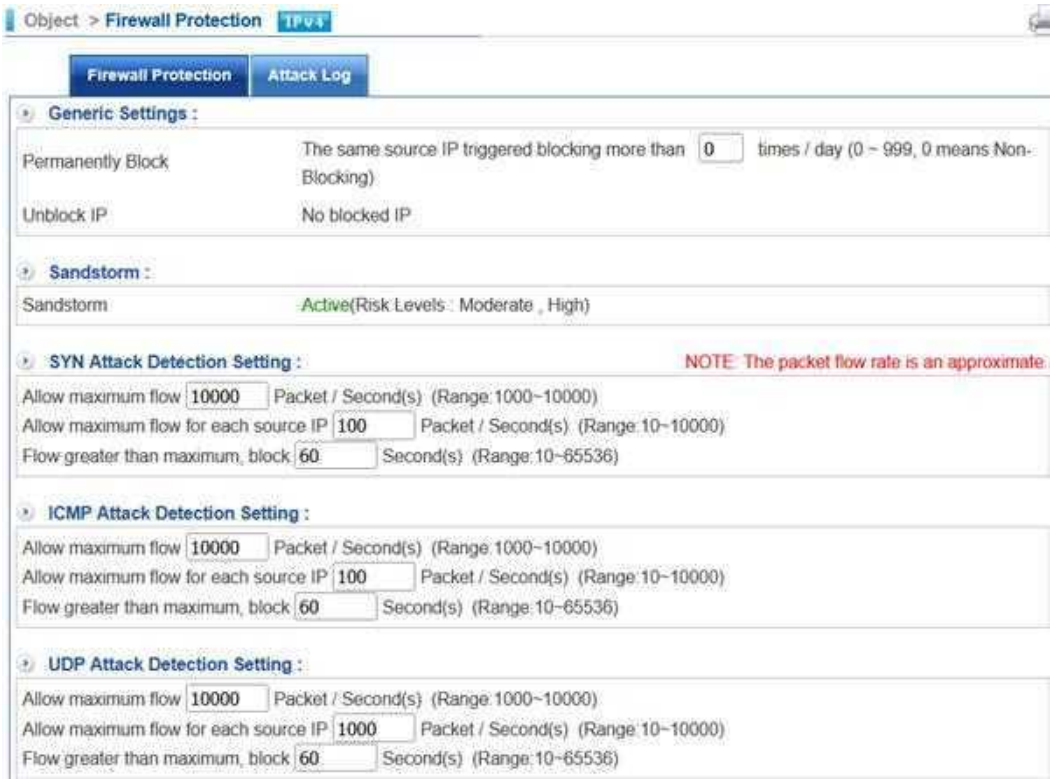


Figure 5-13

IP Address Block

- **[Source/Destination IP address]**: Enter the source or destination IP addresses to be blocked. Traffic from these addresses cannot pass through the firewall's protection mechanism, and all connection requests from these networks will be **rejected**. For example, set 192.168.1.1 or 192.168.1.1/24.

IP Address Exception

- **[Source/Destination IP address]**: Enter the source or destination IP addresses to be exempted from the firewall's protection mechanism. All connection requests from these networks will be **accepted**, even if their network packet quantity may be significantly higher than the set value.

Other Items

In addition to detecting SYN, ICMP, and UDP attacks, the 3100-6GT-I provides administrators with the ability to block common network attack methods. (See Figure 5-14)

Figure 5-14

These protection rules can be applied to the interface addresses of the 3100-6GT-I or to individual firewall policies. When incoming traffic from the Internet exceeds the defined thresholds, the 3100-6GT-I will automatically block packets from the attacker's IP address, ensuring the network security of connected devices.

5-5-2. Attack Log

The 3100-6GT-I logs all attack activities. Administrators can search by criteria such as attack type, source IP address, and target IP address. The system provides detailed information including the time of attack, attack type, protocol, port, interface, source IP address, and target IP address (See Figure 5-15).

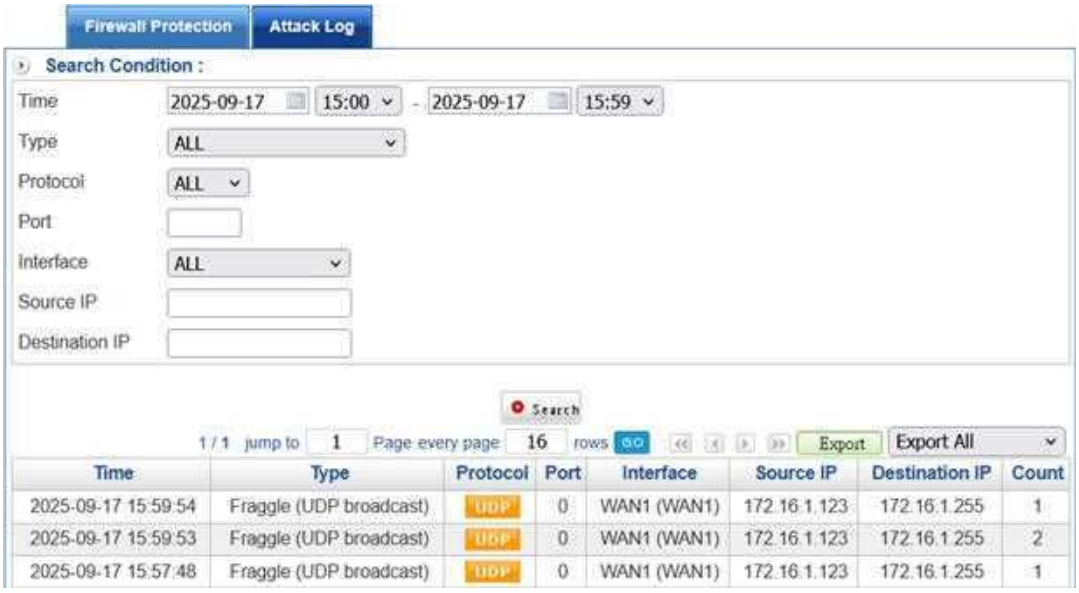


Figure 5-15

5-6. Authentication

The 3100-6GT-I offers web authentication that require users to enter a username and password to access the internet. The authentication can be done via HTTP or HTTPS.

Administrators can pre-define the web page users see before and after authentication. Additionally, administrators can redirect users to a predefined URL while browsing.

There are four sources available for authentication accounts. The default priority order is **L, A, P, R**, described as follows:

1. **L**: Built-in local users
2. **A**: External Active Directory (AD) server
3. **P**: External POP3 server
4. **R**: External RADIUS server

Administrators can use any combination of these four sources to build the authentication mechanism and customize the priority order. For example, if both local and AD user accounts are configured and the priority is set to A, L, P, R, then when a username (e.g., Peter) exists in both sources, the system will authenticate against the AD server, and the password must match the AD credentials.

To enforce authentication before granting Internet access, the web authentication feature must be enabled. When a firewall policy requires user authentication, users will be prompted to enter their credentials upon opening a web browser. Once the correct credentials are provided, the system will automatically redirect them to the default homepage or a custom URL set by the administrator.

After creating a user group, administrators can apply specific user groups in control policies. When specific source IP addresses need internet access, the 3100-6GT-I requests users to enter their username and password before granting access.

> To ensure web authentication functions properly, follow these steps in order:
>
> ➤ [Auth Setting] > [Page Settings] > [Define Account Source (POP3, IMAP, or Radius] > [Create User Group] > [Apply to Policy]

5-6-1. Authentication Setting

The 3100-6GT-I provides shared authentication settings that can be applied to each user group. Administrators may also configure different values for specific accounts as needed. Details are as follows (See Figure 5-16):

- **[Authentication Port]**: The port number used by the web authentication mechanism. Default is TCP 82.
- **[Authentication Page]**: The IP address used for the authentication page. This can be the default gateway of each user or a custom interface IP.
- **[Allow Connection]**: When enabled, IP addresses that are not subject to web authentication control can still connect to the authentication port.
- **[Authentication Connection Protocol]**: The protocol used to deliver the authentication page. Options are HTTP and HTTPS, with HTTPS as the default.
- **[Max. Concurrent Connections]**: The maximum number of IP addresses that can simultaneously request authentication from the server. Default is 256, with a configurable range of 10–256.
- **[Idle Timeout]**: After successful authentication, users can access the Internet. If no network activity occurs within the specified idle time, the 3100-6GT-I requires re-authentication. Default is 60 minutes, with a configurable range of 1–1000 minutes.
- **[Re-login after user has logged in for]**: The maximum duration a user can stay connected after successful authentication. Once exceeded, the 3100-6GT-I requires re-authentication. Default is 24 hours, with a configurable range of 0–24 hours. A value of 0 disables this feature, meaning the session remains valid unless the **[Idle Timeout]** is triggered.
- **[Allow Change Password]**: Determines whether users can change their authentication password after successful login. Default is disabled. When enabled, users can update their password, and the new password takes effect at the next login.
- **[Deny Multi-login]**: When enabled, each account can only be used by one IP address at a time. If another IP attempts to log in with the same account, the 3100-6GT-I authentication mechanism denies access. Default is disabled, allowing multiple logins from different IP addresses.
- **[Temporary Block When Login Failed More Than]**: To prevent brute-force attacks, administrators can specify a maximum number of failed login attempts for the same account. If exceeded, the account is temporarily blocked from authentication. Default is 0, meaning the feature is disabled and users can attempt unlimited logins.
- **[IP Blocking Period]**: This setting applies only when the **[Temporary Block When Login Failed More Than]** feature is enabled. It specifies how long a blocked IP address must wait before it can attempt authentication again. Default is 0, meaning the feature is disabled and the IP address is permanently blocked.
- **[Permanently Block When Login Failed More Than]**: Administrators can permanently block an account if incorrect login attempts exceed the configured value. Default is 0, meaning the feature is disabled and no accounts will be permanently blocked.
- **[Not Show Block Page]**: When enabled, users who are blocked due to excessive failed login attempts will not see a block message in their browser. This option enhances the ability of web authentication to prevent malicious programs.
- **[Unblocked IP]**: All IP addresses blocked by the system are listed here. Administrators can manually unblock any of them.

- **[Account Expiration Notification]**: Applicable only to built-in local accounts. When an account has an expiration date, the system will notify the administrator before it expires. Default is 0, meaning the feature is disabled. For example, if set to 3, the administrator will receive an email notification three days before the account expires.
- **[Delete Expired Account]**: Applicable only to built-in local accounts. When an account reaches its expiration date, the system automatically deletes it. Default is 0, meaning the feature is disabled and no local accounts will be deleted. For example, if set to 3, the account will be deleted three days after expiration.
- **[Select Authentication Mode]**: Defines the authentication priority among the four account sources. The default order is **L, A, P, R**, which corresponds to Local users, Active Directory (AD) server, POP3 server, and RADIUS server. Administrators can adjust the sequence of letters to change the authentication priority.

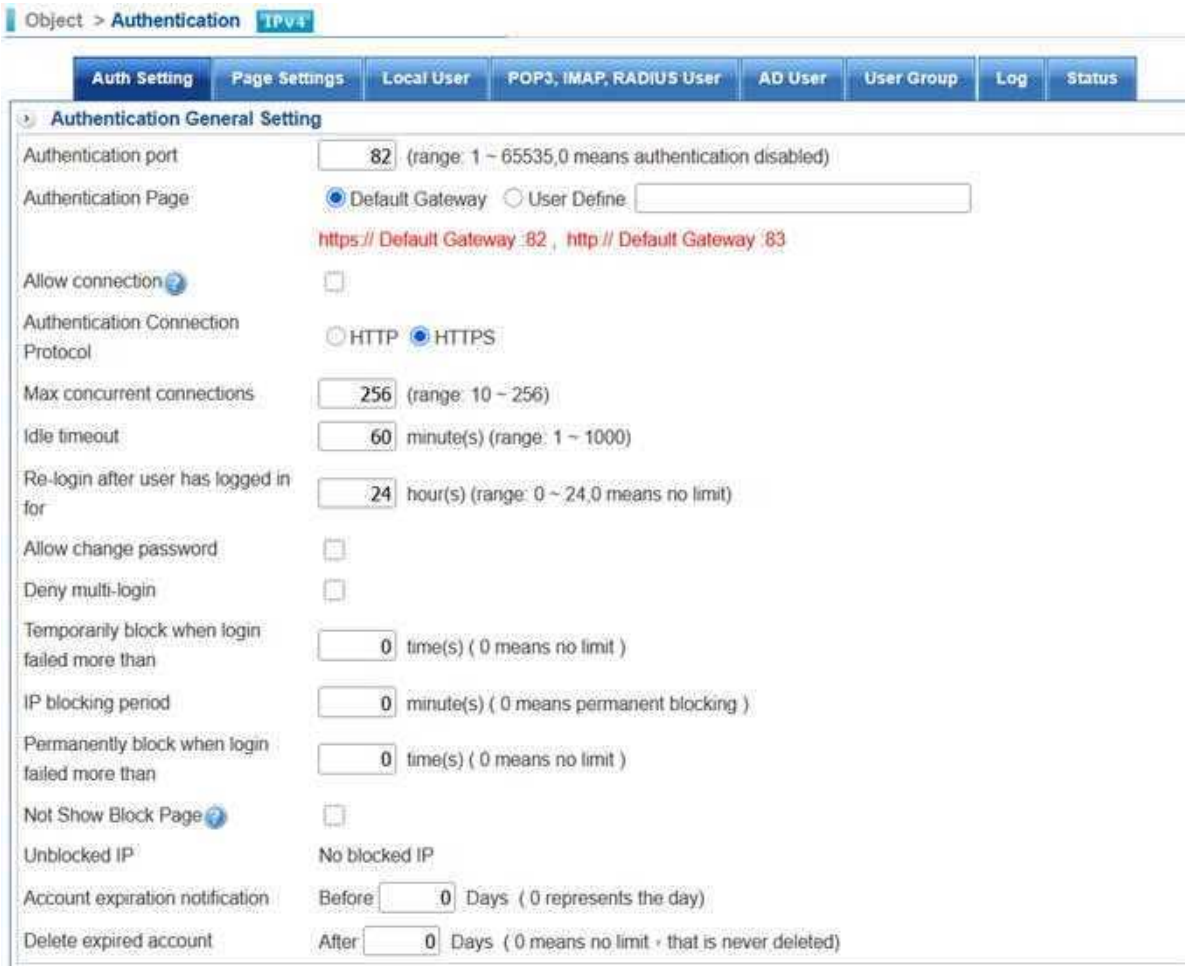


Figure 5-16

5-6-2. Page Settings

Administrators can configure the information displayed in users' browsers during web authentication to ensure that the required messages are properly presented.

Default Page Setup

These settings are applied across the entire page configuration (See Figure 5-17).

- **[Redirect Successfully Authenticated Users to]**: Administrators can redirect authenticated users to a specified webpage, such as the company website, a news page, or an announcement page. Default is blank. When left blank, users are redirected to the homepage configured in their browser after successful authentication.
- **[Display A Read Page]**: Administrators can require authenticated users to view a specified webpage where users must confirm they have read the page. Default is disabled.
- **[Display A Pop-up Logout Page After Successful Login]**: After successful authentication, a logout window will be displayed.
- **[Delay Redirecting the Page When Login Successful]**: Administrators can configure a waiting period before redirecting users to the specified URL after successful authentication.
- **[Redirect Page Waiting Time]**: The waiting time before redirecting to the specified page. The configurable range is 3–10 seconds.
- **[Default Language]**: Options include English, Traditional Chinese, and Simplified Chinese.
- **[Page Color Settings]**: Administrators can select colors for five different sections of the page.

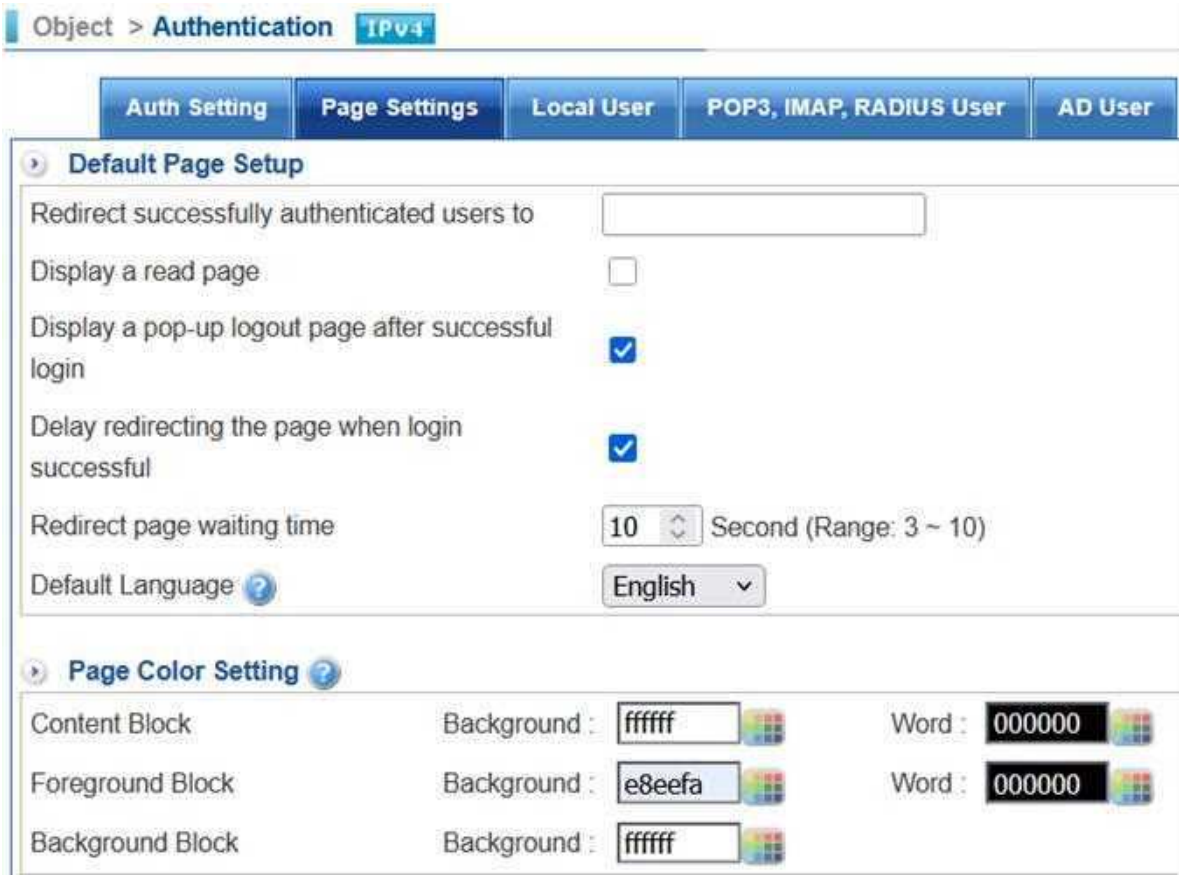


Figure 5-17

Login Message

Each user will see two pages during the login process: the **Login Page**, where the username and password are entered, and the **Post-Login Page**, which appears after successful authentication. The 3100-6GT-I allows administrators to customize both pages.

- Client Login Message

- **[Subject]**: The text displayed in the subject area. For example: *Please enter your username and password.*
- **[Content]**: The text displayed in the content area. For example: *This is the authentication system of ABC Company.*
- **[Upload Logo]**: Replaces the default logo with a custom image. By default, the logo is set to the logo of Volktek Security.
- **[Login Preview]**: Allows administrators to preview the login page after entering custom text. The configuration must be saved before previewing. If the preview is satisfactory, clicking the Accept button will set the customized login page as the system default. (See Figure 5-18)

Figure 5-18

- Client Logged-in Message

- **[Logged-in Message]**: The message displayed to users after successful login. For example: *Please do not misuse network resources.*
- **[Logged-in Preview]**: Allows administrators to preview the customized message. The configuration must be saved before previewing. The preview page will also display additional information, including the user's current IP address, **Log out**, and **Change Password** options.
- **[Change Password]**: When the account source is a built-in local user, this option allows users to change their authentication password directly from the post-login page. (See Figure 5-19)

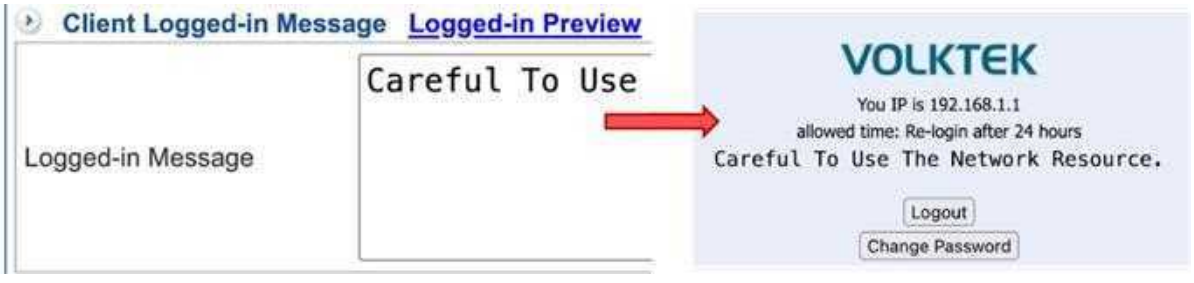


Figure 5-19

5-6-3. Local User

The 3100-6GT-I supports four sources for authentication accounts. The default priority order is **L, A, P, R**, described as follows:

1. **L**: Built-in local users
2. **P**: External POP3 server
3. **R**: External RADIUS server
4. **A**: External Active Directory (AD) server

When creating a local user account, one advantage is that users can change their own passwords and set expiration dates (see Figure 5-20).

- **[Name]**: The display name of the account. This can be any descriptive text, such as *John Smith* or *Jane Doe*, up to 16 characters.
- **[Account]**: The username used for authentication. Must consist of letters and numbers only, up to 16 characters. Example: *jean*.
- **[Password]**: The password used for authentication. To enhance security, use the following practices:
  - Combine letters and numbers
  - Include special characters (e.g., @#$)
  - Mix uppercase and lowercase letters

  Passwords are case-sensitive, must be 3–16 characters long, and must not be identical to the username. Example: *@jean39*.
- **[Password Strength]**: The system automatically evaluates the complexity of the entered password for administrator reference.
- **[Confirm Password]**: Re-enter the password to confirm and prevent login issues caused by typos.
- **[Require Password Change at Next Login]**: Determines whether the user must change their password upon the next login. Default is disabled.
- **[Account Expiration Date]**: Sets an expiration date for the account. The system provides a calendar for selection. Leaving this field blank means the account never expires. Default is blank.
- **[2-step Verification]**: When enabled, in addition to the regular password, the user must also enter a verification code generated by a TOTP authenticator to log in.

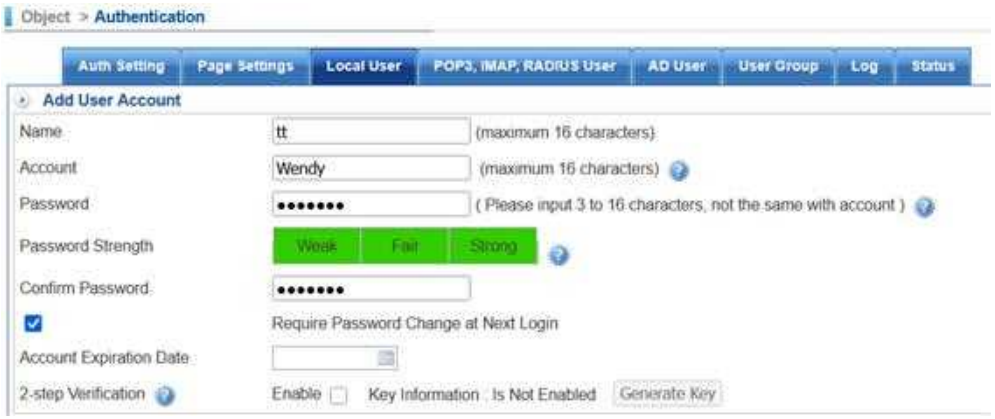


Figure 5-20

- **[Expired Log]**: All expired accounts are listed in the expiration log.
- **[Account/Name Search]**: When the number of local accounts grows large (e.g., more than 50 entries), it may be difficult for administrators to identify users. The 3100-6GT-I provides a search function that allows searching by either account name or display name.
- **[Import/Export]**: Local user accounts can be imported or exported for backup and management purposes.

5-6-4. POP3, IMAP, RADIUS User

POP3, IMAP Server List

The 3100-6GT-I can integrate authentication accounts with email server accounts (POP3/IMAP), allowing users to log in without managing multiple usernames and passwords (see Figure 5-21).

- **[POP3/IMAP Domain Name]**: The domain name of the POP3/IMAP server. For example, for the account *Jean@abc.com*, the domain name is *abc.com.*
- **[POP3/IMAP Server]**: The IP address or A record of the POP3/IMAP server, e.g., *9.9.9.9* or *pop.abc.com*.
- **[Login with Domain]**: Determines whether the authentication account must include the POP3/IMAP domain name. Default is disabled (domain not included). For example, for the account *jean@abc.com*, if the domain is not included, the login name is jean. If enabled, the login name becomes *jean@abc.com*.
- **[Protocol]**: Two authentication protocols are available: POP3 and IMAP. When selecting IMAP, ensure that the server IP address or domain points to the correct IMAP server.
- **[Security]**: Specifies whether to use an encryption protocol for authentication communication. Default is *None* (no encryption). Administrators may select TLS or SSL depending on the server's supported connection method.
- **[Port]**: The port number used for authentication. Default is 110 for POP3 and 143 for IMAP.
- **[Certification]**: When an encrypted port is selected, it determines whether to ignore certificate warnings. Default is to not ignore warnings.
- **[Connection Test]**: After completing the configuration, administrators can test the connection to verify that the settings work correctly. Clicking the **Connection Test** button prompts for a POP3/IMAP account. Once submitted, the system returns the test result.

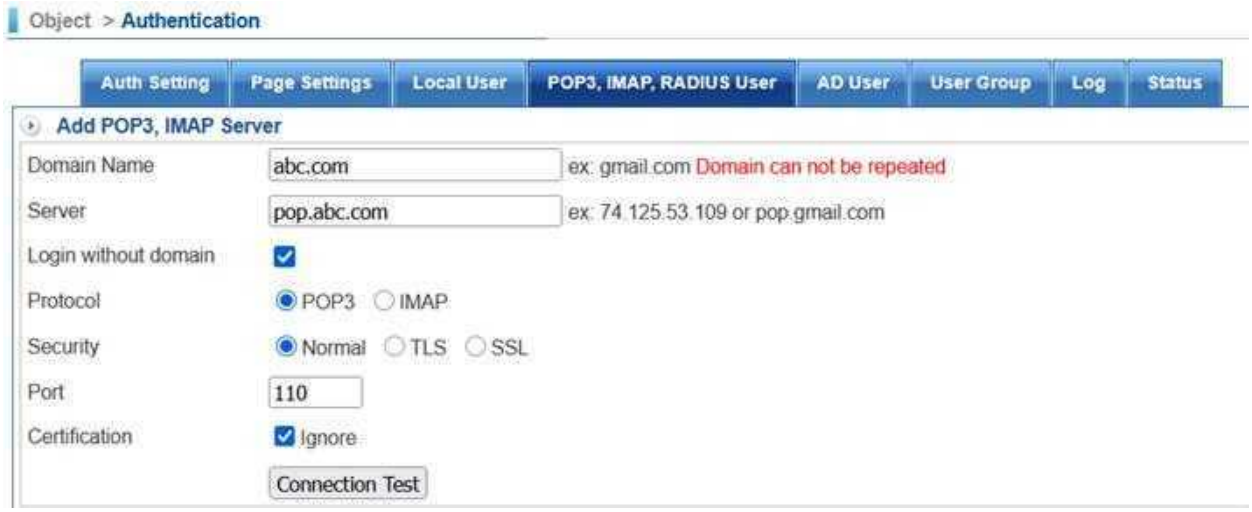


Figure 5-21

RADIUS Server List

The 3100-6GT-I can integrate authentication accounts with external RADIUS servers, allowing users to log in without managing multiple usernames and passwords (see Figure 5-22).

- **[RADIUS Name]**: The name of the RADIUS server, e.g., *my_radius*.
- **[Server]**: The IP address or domain name of the RADIUS server, e.g., *192.168.1.100* or *radius.abc.com*.
- **[Port]**: The communication port used between the 3100-6GT-I and the RADIUS server. Default is 1812.
- **[Shared Secret]**: The shared key used between the 3100-6GT-I and the RADIUS server. If the key does not match, authentication will fail.
- **[Interface]**: The 3100-6GT-I uses **Zone** as the interface. Not all interfaces may communicate with the RADIUS server, so the administrator must select one that can. If *No Assign* is selected, the 3100-6GT-I will communicate with the server based on the default routing table.
- **[Connection Test]**: After configuration is complete, administrators can test whether the settings are functioning properly. Clicking the **Connection Test** button prompts for a RADIUS server account. Once submitted, the system returns the test result.

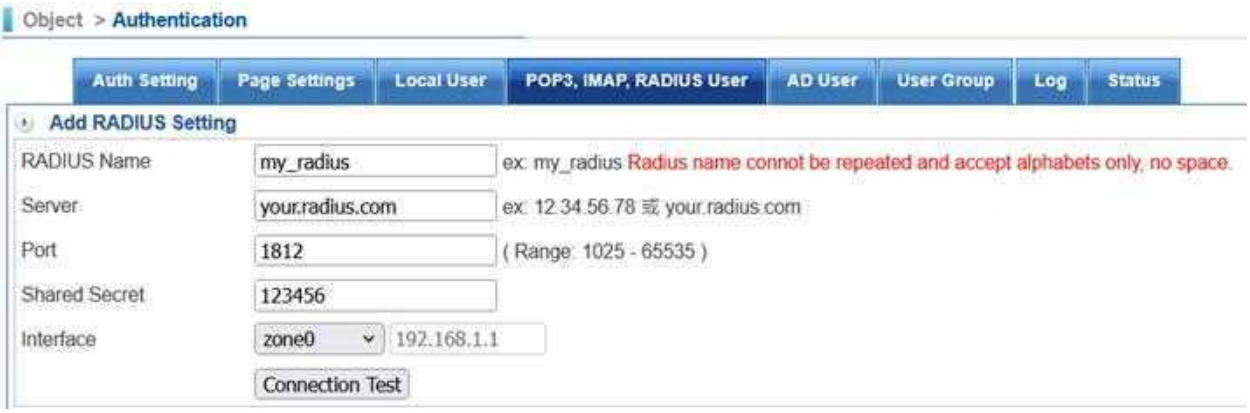


Figure 5-22

5-6-5. AD User

The 3100-6GT-I can integrate authentication accounts with external Active Directory (AD) servers, allowing users to log in without managing multiple usernames and passwords (see Figure 5-23).

- **[AD Address]**: The IP address of the AD server, e.g., *192.168.1.5*.
- **[Domain Name]**: The domain name of the AD server, e.g., *ad.abc.com*. Maximum length is 16 characters.
- **[Account]**: The AD administrator account with account management privileges, e.g., *administrator*. Maximum length is 16 characters.
- **[Password]**: The password for the AD administrator account with account management privileges.
- **[Connection Test]**: After entering the above information, administrators can click the **Connection Test** button to verify that the configuration works properly.
- **[Ignore the AD Group]**: Specifies AD groups whose users will not be granted authentication access.
- **[Ignore the AD User]**: Specifies AD users who cannot log in through the authentication mechanism.
- ★ **[2-Step Verification Setting]**: When enabled, in addition to the account password, users must also enter a verification code generated by a TOTP authenticator to log in.

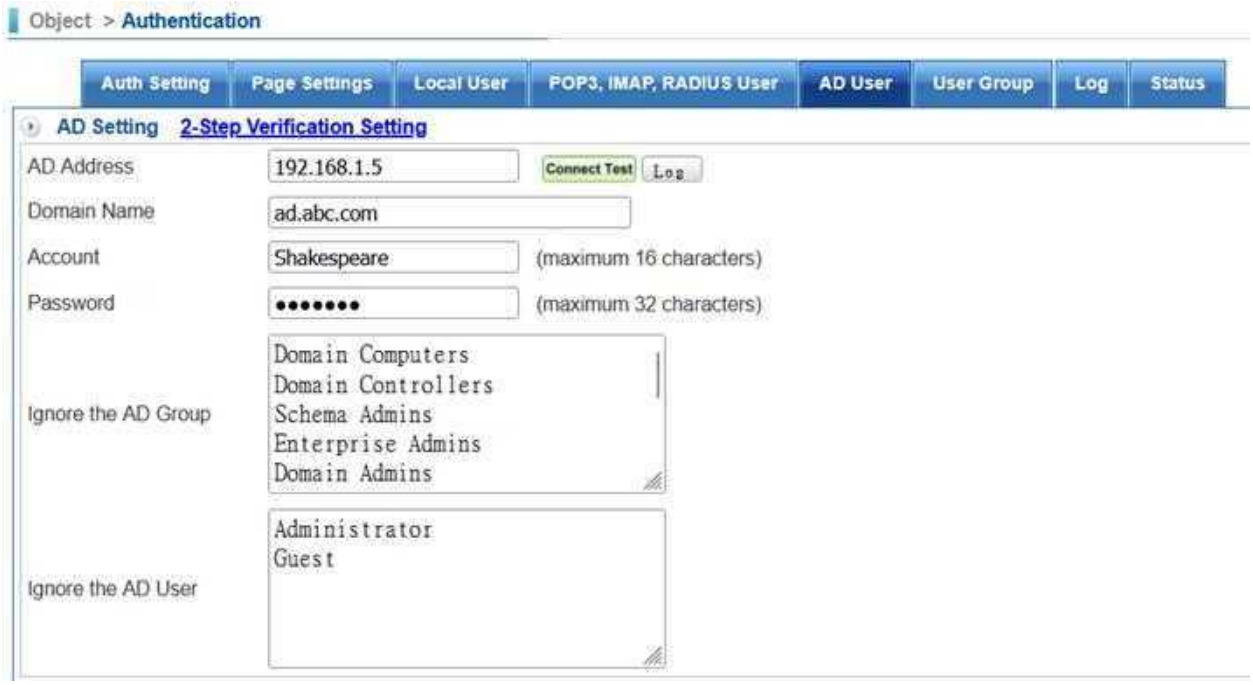


Figure 5-23

5-6-6. User Group

Administrators can define multiple user groups. These groups can either apply preconfigured authentication settings and account sources or be assigned new custom settings and account sources (see Figure 5-24).

- **[Group Name]**: The name of the user group. This can be any text, for example, *Engineering Department Group*.
- **[Auth Setting]**: Two modes are available. One is to apply predefined **General Settings**; the other is the **User Defined Settings**. In User Defined Settings mode, administrators can redefine attributes based on user requirements. For detailed descriptions of these options, refer to section 5-6-1, Authentication Setting.
- **[Select User Type]**: Three options are available, and they can be mixed:

  1. **Local** – Select users from local accounts. For example, if there are 200 local accounts and the group should include 50 of them, select those 50 accounts and add them to the group.
  2. **POP3/IMAP** – Select a predefined POP3/IMAP server, then add the corresponding users to the group.
  3. **RADIUS** – Select a predefined RADIUS server, then add the corresponding users to the group.

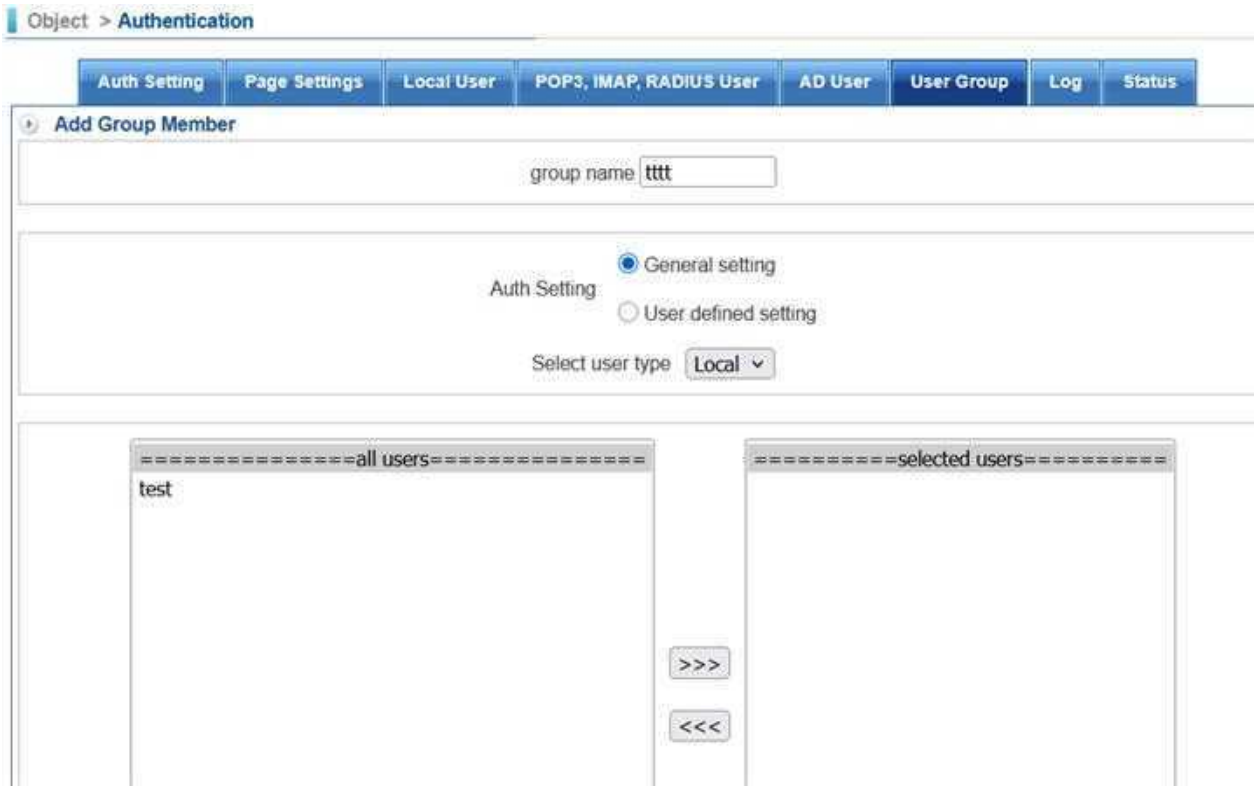


Figure 5-24

5-6-7. Log

The authentication records of each user group, whether successful or failed, are logged by the system. Administrators can search for records based on IP address, account, connection status, or the authentication source. There are six possible authentication results: **Login Success**, **Login Fail**, **Logout Success**, **Idle Logout**, **Login Timeout**, and **Admin Kick-out** (see Figure 5-25).

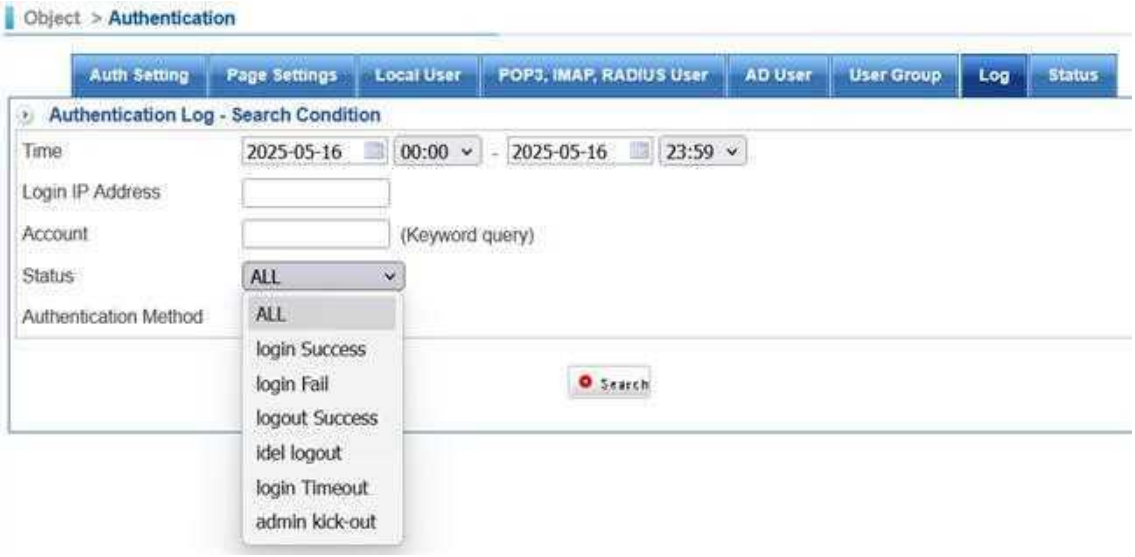


Figure 5-25

5-6-8. Status

This page lists the users currently connected through web authentication and the total number of active sessions. The information includes group name, user account, user IP address, use MAC address, as well as individual kick-out and group kick-out records.

Chapter 6. Service

The 3100-6GT-I provides the following network service functionalities:

1. **DHCP**

   When the DHCP function is enabled, internal PCs can obtain IP addresses, DNS servers, and other information through the interface of the 3100-6GT-I.

2. **SNMP**

   SNMP is a protocol specifically used for managing network nodes (servers, workstations, routers, switches, etc.).

   Network administrators can use SNMP to receive messages, promptly identify and resolve network issues, or assist in planning the utilization of network resources.

3. **DNS**

   DNS, Domain Name Service, is a system software that allows computers in the network system to perform domain name-to-IP address conversions.

4. **Anti-Virus Engine**

   Provide ClamAV and Kaspersky anti-virus engine settings.

5. **Sandstorm**

   Sandstorm effectively detects unknown, advanced malware and malicious file attachments, unmasking hidden threats.

6. **WEB Service**

   The 3100-6GT-I provides WEB virus scanning, including scanning graphic files, virus connection numbers, scanning file sizes, and can also specify certificate information for HTTPS.

7. **High Availability**

   The 3100-6GT-I's hardware redundancy mechanism adopts a Master/Backup mode. When the system operates normally, network access is through the specified MASTER host.

   At the same time, there is a BACKUP host that instantly backs up all data from the MASTER host. When the currently operating MASTER host encounters a fault, the BACKUP host immediately takes over as the MASTER host to maintain uninterrupted internal/external network connections.

8. **Remote Syslog**

   Remote Syslog allows remote backup of related log records, including firewall policy, application logs, IPS logs, and email logs.

6-1. DHCP

Connecting a computer requires settings like IP, subnet mask, gateway, and DNS. Since manual configuration is complex—especially in large networks—DHCP automates the process by assigning these settings to clients at startup.

When configuring a DHCP server, administrators define the IP range, gateway, and DNS settings. Once activated, the server stores this information and assigns it to clients upon request. DHCP clients broadcast a request, the server replies with the configuration, and the client applies the assigned IP and DNS settings.

In DHCP, assigning an IP to a client is called **leasing**. Leases expire and must be renewed, and administrators can set a maximum duration to prevent indefinite reuse of the same IP.

Besides dynamic assignment, DHCP can assign fixed IP addresses to devices using their unique MAC addresses, which can be viewed with commands like ifconfig (FreeBSD) or ipconfig /all (Windows).

Example:

#**ifconfig**

fxp0:flags=88c3<UP,BROADCAST,RUNNING,NOARP,SIMPLEX,MULTICAST>mtu1500

options=b<RXCSUM,TXCSUM,VLAN_MTU>

inet6fe80::202:b3ff:fe48:7c74%fxp0prefixlen64scopeid0x1

inet10.0.0.1netmask0xff000000broadcast10.255.255.255

ether**00:08:c3:96:8c:22**

media:Ethernetautoselect（100baseTX<full-duplex>）

status:active

In the example above, the value **00:08:c3:96:8c:22** represents the MAC address of a network card. A specific MAC address can be assigned a fixed IP address. This ensures that whenever the device requests an IP address through DHCP, the DHCP server will always assign it to the same fixed address.

The 3100-6GT-I is a ZONE-based device, meaning that each interface includes 802.1Q VLAN support. Independent DHCP servers can be configured for each interface. In general, DHCP server settings for physical ports are identical, while VLAN settings differ slightly.

6-1-1. DHCP User List

6-1-2. DHCP Server

- **[Interface]**: First, select the interface to configure. Both physical Zone interfaces and virtual VLAN (802.1Q) interfaces are listed for administrators to choose from.

  If a virtual VLAN interface (802.1Q) is selected, an additional field will appear listing the available virtual port interfaces for selection.

  - **IP Address of Physical Zone**

    Select the interface address already set in [Network] > [Interface] > [IP Address].

  - **IP Address of Virtual VLAN**

    Select the IP address already set in [Network] > [VLAN (802.1Q)].

DHCP Server Settings

Each DHCP server can be configured with two address ranges (see Figure 6-1).

- **[IP Range 1 – Start and End Address]**: Enter the starting and ending IP addresses of the DHCP range. For example, *192.168.1.20* to *192.168.1.30* provides 11 IP addresses.
- **[IP Range 2 – Start and End Address]**: Enter the starting and ending IP addresses of the second DHCP range. For example, *192.168.1.200* to *192.168.1.230* provides 31 IP addresses.
- **[Primary/Secondary DNS]**: The DNS servers assigned to DHCP clients, e.g., *8.8.8.8* and *168.95.1.1*.
- **[Primary/Secondary WINS]**: (Optional) The WINS servers assigned to DHCP clients, mainly used for name resolution in Windows networks, e.g., *192.168.1.100* and *192.168.1.200*.
- **[Default Lease Time]**: The default lease duration for each DHCP-assigned IP address. Default is 720 minutes (12 hours).
- **[Maximum Lease Time]**: The maximum lease duration for each DHCP-assigned IP address. Default is 720 minutes (12 hours).
- **[Default Gateway]**: The gateway IP address for DHCP clients, e.g., *192.168.100.254*.
- **[Domain Name]**: (Optional) The domain name assigned to DHCP clients.
- **[Enable]**: Enables or disables this DHCP server.

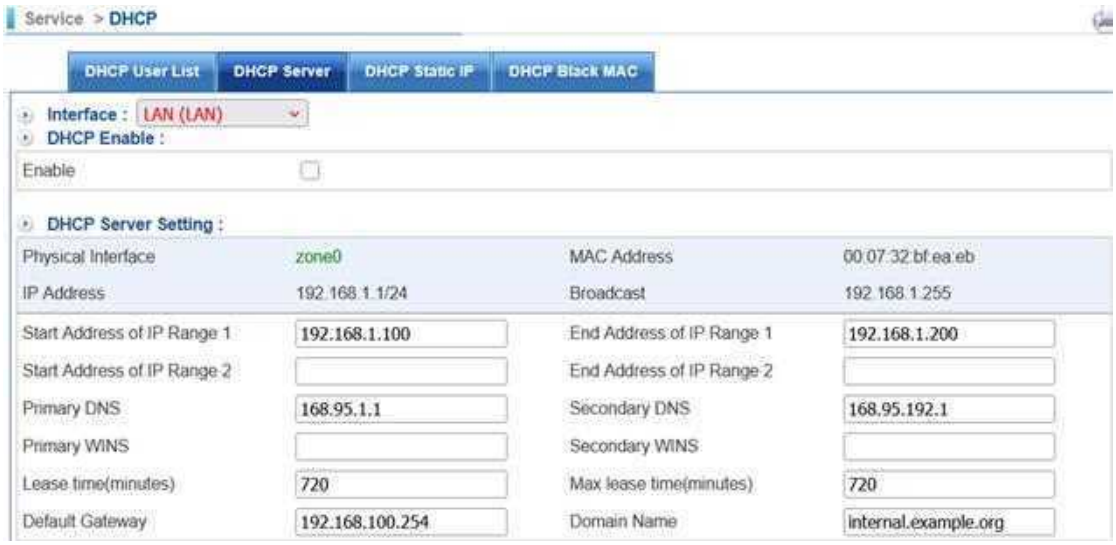


Figure 6-1

6-1-3. DHCP Static IP

In 5-1-1 IP Address under **Objects**, if **[Mode]** is set to **"IP and MAC Address"** and the option **"Get static IP address from DHCP Server"** is selected, the computer with this MAC address will always receive the same fixed IP address from the DHCP server (see Figure 6-2).

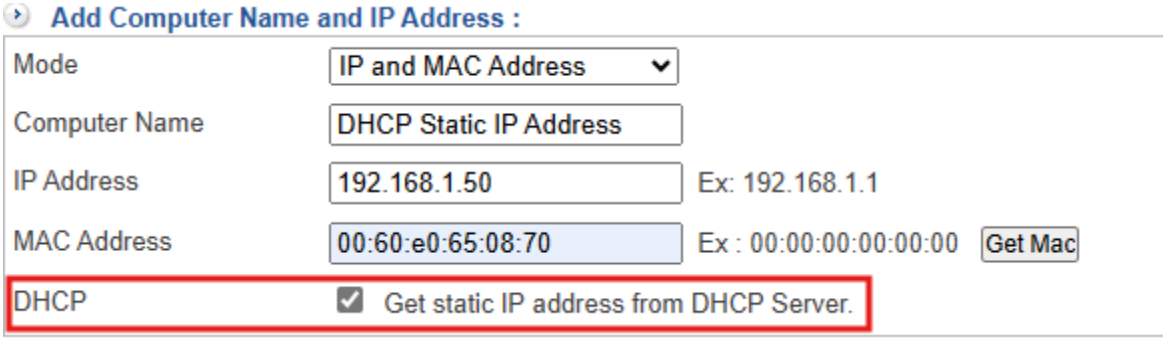


Figure 6-2

The following table shows the DHCP Static IP Address (see Figure 6-3).

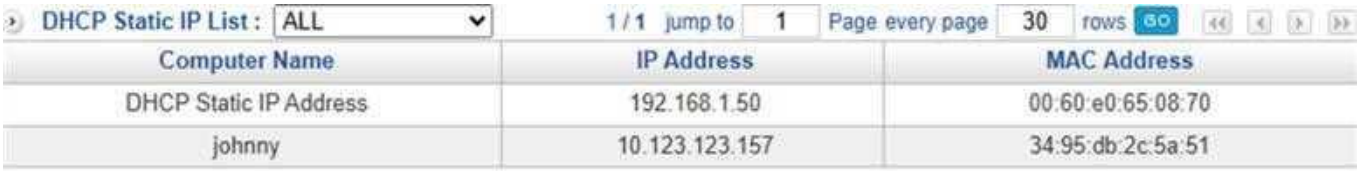


Figure 6-3

6-1-4. DHCP Black MAC

MAC addresses listed in the blacklist cannot use DHCP services.

6-2. SNMP

Simple Network Management Protocol (SNMP) is used to manage network nodes such as servers, workstations, routers, and switches. It allows administrators to monitor devices, detect issues in real time, and optimize resource usage.

An SNMP-managed network has three components: Managed devices, Agents, and Network Management Systems (NMSs).

Currently, there are three versions of SNMP:

1. **SNMPv1**: Basic implementation; no encryption or authentication. Data, including passwords, is transmitted in plaintext, creating major security risks.
2. **SNMPv2**: Improves security over v1 but is slower and incompatible with it. Adoption is limited.
3. **SNMPv3**: Encrypts all transmissions, supports mutual authentication between agents and NMSs, ensures message integrity with digital signatures, and enforces access control for each request.

Enabling SNMP Service

- **[Service State]**: Displays whether the service is inactive or active. (See Figure 6-4)
- **[SNMP Agent]**: Enable this option to activate SNMP. If unchecked, the service is disabled.
- **[Device Name]**: The SNMP display name, e.g., *Office-3100-6GT-I*.
- **[Device Location]**: Can be set to any text in English.
- **[Contact Person]**: The contact's email address.

- **[SNMPv1/v2]**: Enables or disables SNMPv1/v2.
- **[Community]**: The community string (username) for SNMPv1/v2.

- **[SNMPv3]**: Secure version of SNMP. When enabled, the following security settings apply:
- **[Security Level]**:
  - *AuthPriv*: Authentication and encryption
  - *AuthNoPriv*: Authentication without encryption
  - *NoAuthNoPriv*: No authentication and no encryption
- **[User Name]**: Username for SNMPv3.
- **[Auth Protocol]**: Authentication method: *MD5* or *SHA* (SHA is more secure).
- **[Auth Password]**: Password for authentication.
- **[Privacy Protocol]**: Encryption method: *DES* or *AES* (AES is more secure).
- **[Privacy Password]**: Password for encryption.

- **[Visit Control]**: Allows SNMP access through specified interfaces.
- **[Restrict Source IP Access]**: Restricts SNMP access to specified IP addresses or leaves it unrestricted.

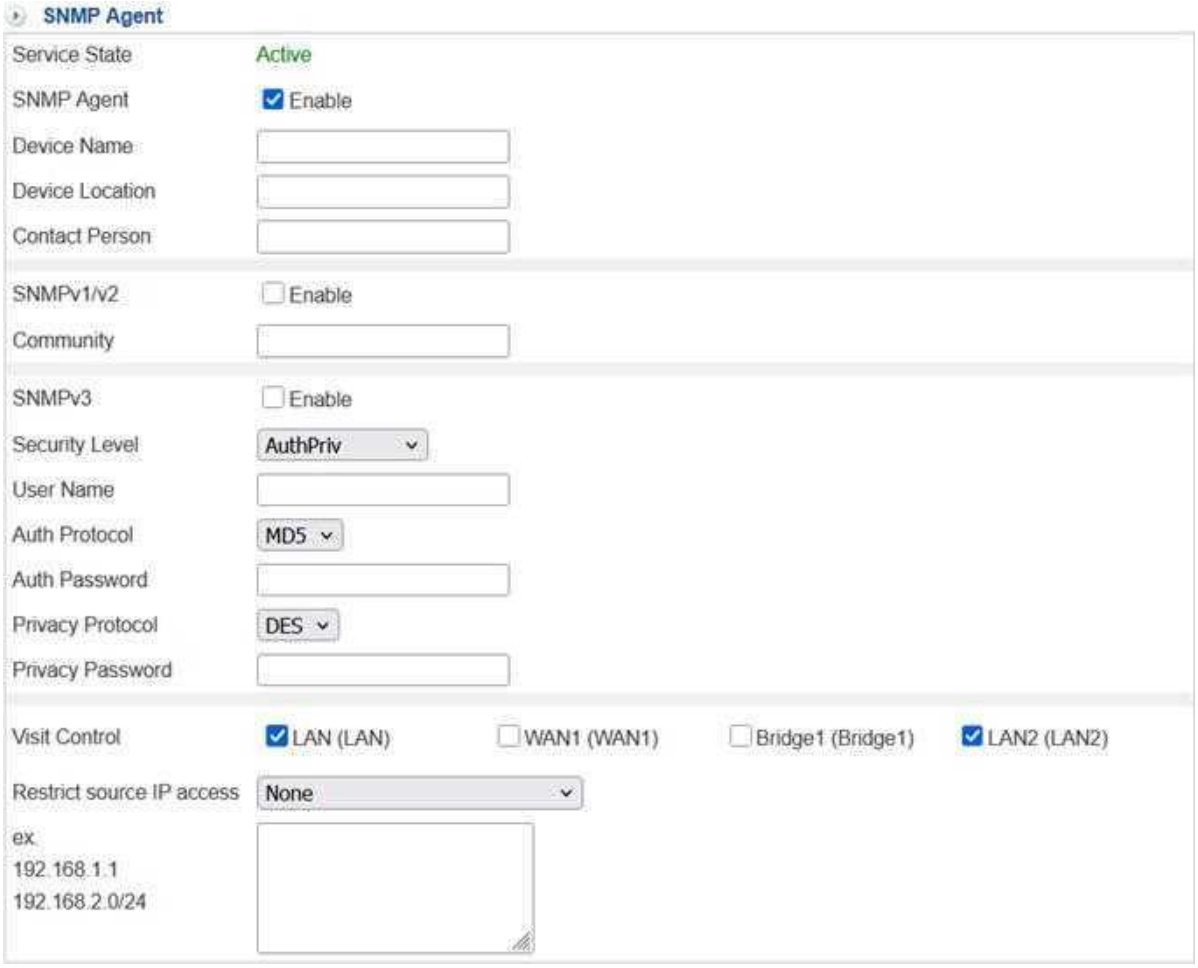

SNMP Agent
Service State
Active
SNMP Agent
Enable
Device Name
Device Location
Contact Person
SNMPv1/v2
Enable
Community
SNMPv3
Enable
Security Level
AuthPriv
User Name
Auth Protocol
MD5
Auth Password
Privacy Protocol
DES
Privacy Password
Visit Control
LAN (LAN)
WAN1 (WAN1)
Bridge1 (Bridge1)
LAN2 (LAN2)
Restrict source IP access
None
ex
192.168.1.1
192.168.2.0/24

Figure 6-4

6-3. DNS Proxy

The Internet is composed of countless interconnected computers. To ensure accurate data transmission, each computer is assigned a unique fixed address, known as an IP address, consisting of numbers from 0 to 255.

As the number of connected hosts grows, IP addresses become difficult for users to remember and manage, which led to the introduction of **domain names**. Similar to how every person has an ID number that is hard to memorize, domain names serve as an easier-to-remember alias.

A website address consists of a hostname and a domain name. For example, the domain name www.net-chinese.com.tw is resolved by DNS into the IP address *202.153.205.77*. This allows users to access the website without memorizing the numeric IP address. The correspondence between *www.net-chinese.com.tw* and *202.153.205.77* is handled by a **DNS server**.

Since the Internet is fundamentally addressed by IP, domain names must be recorded on a DNS server along with their corresponding IP addresses to provide resolution services.

The 3100-6GT-I DNS server provides **proxy query functionality**, allowing devices behind the firewall to resolve DNS requests through external DNS servers.

A proxy query occurs when a user queries a domain name that is not stored locally, the DNS server automatically forwards the request to an external DNS server and returns the result to the user.

General Settings

The built-in DNS server can accept proxy queries from users. For example, internal users can configure their DNS server to point to the 3100-6GT-I. When a user queries www.abc.com, the 3100-6GT-I will proxy the DNS request and return the result to the internal user (see Figure 6-5).

- **[Allow Query from]**: Defines which interfaces are allowed to send DNS queries. Queries from unchecked interfaces will be rejected.
- **[Allow Recursive Queries from]**: Defines the IP addresses allowed to use the proxy query service. Both IPv4 and IPv6 addresses are supported, and multiple entries can be added.

Figure 6-5

6-4. Anti-Virus Engine

The 3100-6GT-I provides two antivirus engines: the free ClamAV and the licensed Kaspersky. By default, ClamAV is enabled and serves as the active antivirus engine. Once a Kaspersky license is uploaded, Kaspersky becomes the primary antivirus engine.

- **[Virus Engine]**: Select the antivirus engine to use (ClamAV or Kaspersky), or disable the feature.

6-4-1. ClamAV Engine

ClamAV, short for *Clam Antivirus*, is an open-source, free-licensed antivirus solution, similar in philosophy to Linux. ClamAV updates and maintains its virus database 24/7. Anyone who discovers a suspicious virus can report it, and ClamAV will immediately update the virus signatures (see Figure 6-6).

- **[ClamAV Status]**: Enabled by default, with no option to disable.
- **[Version]**: The current antivirus engine version, e.g., *ClamAV 1.0.8*.
- **[Update Log]**: Lists the update history of the antivirus engine.
- **[Clear Log]**: Deletes the update log.
- **[Update Period]**: The update interval for the virus database. Default is every 6 hours, configurable from 1 to 24 hours.
- **[ClamAV Database Mirrors]**: Select the server to update the virus database from.
- **[Update Now]**: Immediately updates the virus database.

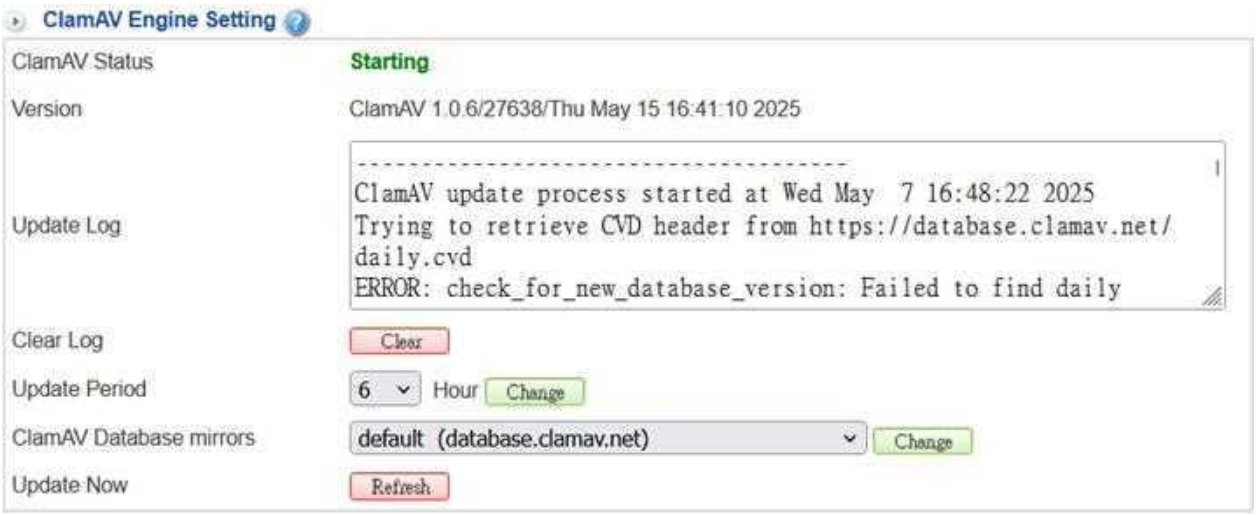


Figure 6-6

6-4-2. Kaspersky Engine

The Kaspersky engine requires a valid license key to function. Until uploaded, only ClamAV is active. After importing the Kaspersky license key and saving settings the system updates from the remote database, and within about two minutes Kaspersky becomes active (see Figure 6-7).

Figure 6-7

- **[Kaspersky Status]**: Disabled by default. Requires uploading a license file to enable.
- **[Version]**: The current antivirus engine version.
- **[Pattern Number]**: Displays the number of the latest virus signatures.
- **[Update Log]**: Lists the update history of the antivirus engine.
- **[Update Period]**: The update interval for the virus database. Default is every 6 hours, configurable from 1 to 24 hours.
- **[Clear Log]**: Deletes all update history.
- **[Update Now]**: Immediately updates the virus database.
- **[Licenses Info]**: Uploads the license file for the antivirus engine (see Figure 6-8).

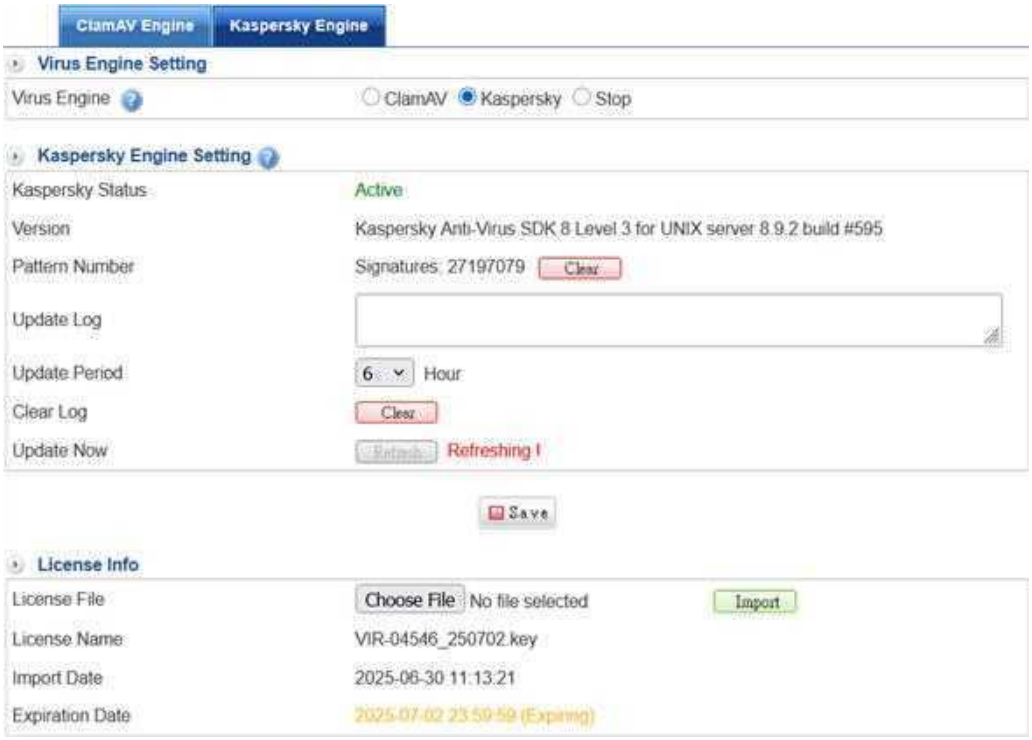


Figure 6-8

6-5. Sandstorm

With the rise of phishing emails and malicious URLs, users may unknowingly click harmful links. Such threats, including trojans and malicious sites, cannot be fully addressed by traditional antivirus software. As the firewall is both the first line of defense (external to internal) and the last line of defense (internal to external), the 3100-6GT-I integrates advanced protection mechanisms at this critical point.

6-5-1. Sandstorm

Sandstorm automatically scans and matches unknown malicious files. When such files are detected, the 3100-6GT-I proactively blocks them. Sandstorm's threat database is regularly updated to maintain high detection and blocking capabilities.

Sandstorm

Sandstorm allows administrators to enable a file hash-based inspection to detect suspicious files (see Figure 6-9).

Figure 6-9

- **[Cloud Test]**: Administrators can upload files to the Sandstorm cloud engine to check if they exist in the blacklist database. By clicking **"Cloud Test"**, a new window opens where administrators can upload files or input URLs to perform the blacklist check. The database then responds with whether the item is blacklisted (see Figure 6-10).

Figure 6-10

- **[Enable Function]**: Sandstorm scans two types of threats: file-based malware and URL-based threats, which may be delivered via web browsing or email. Administrators should determine whether both or only one type of threat detection is needed.

  Since file-based threats can appear in both web and email services, additional configurations must be performed in their respective management interfaces. Hyperlinks are provided for quick access to these settings.

- **[Last Update Time]**: Sandstorm regularly updates its threat database. Clicking **"Refresh"** allows administrators to manually update the blacklist information.

File Hash

- **[Version]**: Displays the current Sandstorm version and the number of malware samples (in parentheses).
- **[Risk Levels]**: Each sample is categorized into **High**, **Medium**, or **Low** risk levels. Administrators can adjust detection behavior accordingly. For example, to reduce the risk of false positives, blocking of **Low**-risk items may be disabled.
- **[WEB/Mail]**: After enabling this function, administrators must further configure settings in the respective **Web service** or **Mail Security** management interfaces. Convenient links to these interfaces are provided (see Figure 6-11).

Figure 6-11

IP

- **[IP Test]**: Administrators can test whether a specific IP address exists in the blacklist database. By clicking **[IP Test]**, a new window will open where the IP address can be entered for verification. The system will then respond with whether it is blacklisted (see Figure 6-12).

Figure 6-12

- **[Version]**: Displays the current version and the number of blocked IPs (shown in parentheses).
- **[Risk Levels]**: Each IP entry is categorized into **High**, **Medium**, or **Low** risk levels. Administrators can customize actions accordingly. If concerned about over-blocking, **Low**-risk IPs can be excluded from blocking.
- **[Interface/Policy]**: After enabling this function, additional configuration is required in the **Network Interface** or **Policy Rules** management sections. Links are provided for quick access (see Figure 6-13).

Figure 6-13

6-5-2. Sandstorm Record

Search results can be filtered by date, function type, service type, risk level, or IP address. The system will display and count the number of occurrences for each attack signature (see Figure 6-14).

Date	Function	Malware Type	Destination Info	Risk Levels	Times	Detail	Enable
2024-05-10 10:34:05	File Hash	CVE-2017-0199	ef04a12bc8c36b451d4b9da3cd9d36d6	High	1		

Figure 6-14

- **[Function]**: Sandstorm includes two detection categories: **File Hash** and **IP**. This field shows the corresponding category of each log entry.
- **[Malware Type]**: Indicates whether the detected threat was a **trojan**, **phishing attempt**, or another malware type.
- **[Times]**: Displays how many times a specific threat has been triggered during the logging period.

If administrators believe that Sandstorm has mistakenly blocked legitimate user activities, the specific entry can be disabled in the log interface to avoid future false positives. All disabled items can be reviewed in the **Sandstorm Disable List**.

By clicking the **Details** icon, information such as the internal IP address that triggered the action is displayed (see Figure 6-15).

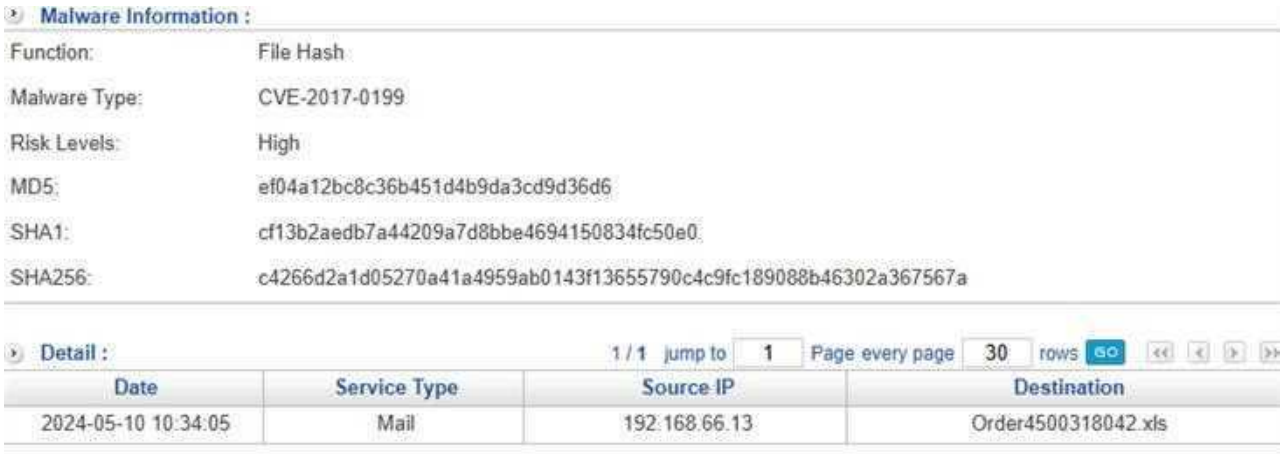


Figure 6-15

6-5-3. Sandstorm Disable List

Files that have been blocked by Sandstorm and later excluded by the administrator will be listed here.

6-6. WEB Service

The 3100-6GT-I can scan both HTTP and HTTPS protocols to check whether the transmitted content contains any viruses. In addition to inspecting packets for these two protocols, it also records the URLs visited by users, allowing administrators to easily query and manage access logs later. It operates in **Transparent Proxy** mode, requiring no browser configuration.

For HTTPS, administrators must generate an **SSL root certificate** on the 3100-6GT-I and install it on user devices.

Apple devices reject untrusted root certificates, so web service features won't function on macOS or iOS. **Windows** and **Firefox** store trusted root certificates in different locations—administrators must ensure the browser trusts the correct root certificate.

6-6-1. WEB

WEB Anti-Virus Setting

Set the antivirus engine for HTTP scanning. Administrators can adjust settings based on network conditions to ensure stable web service operation (see Figure 6-16).

- **[Sandstorm]**: In addition to the antivirus engine, the system also references the Sandstorm database for threat detection.
- **[Max. Scan File Size (KB)]**: Files exceeding this size will not be scanned. Default is 1024 KB.
- **[Listen Port]**: Specifies which ports will be processed by the HTTP proxy. The default is port 80. Multiple ports can be entered (e.g., 80,81,88) to apply scanning to each.
- **[Virus Engine]**: Uses the built-in ClamAV engine.
- **[Warning Setting]**: Message shown to users when a virus is detected.
- **[Warning Subject]**: Custom text for the warning subject line.
- **[Warning Message]**: Custom content for the warning page.
- **[Preview]**: Allows administrators to preview and verify the warning message content.

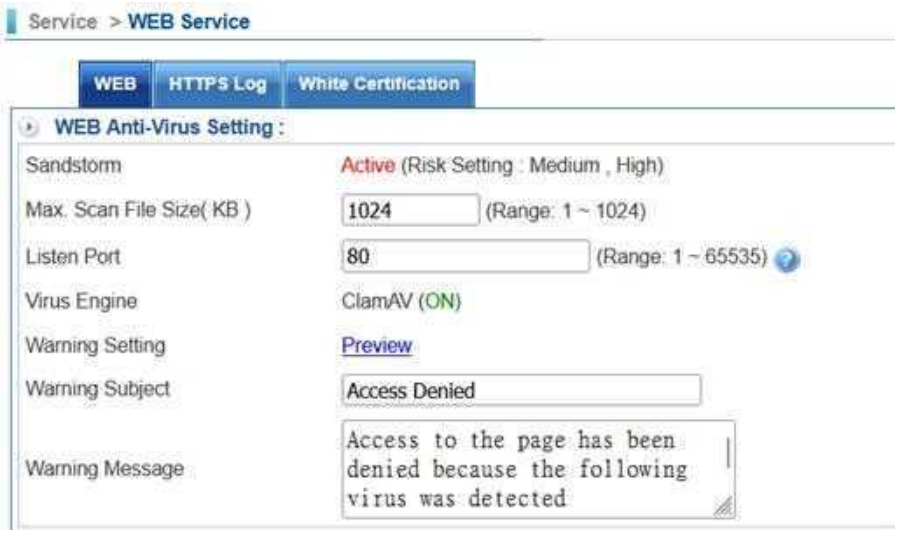


Figure 6-16

Encryption Connect Setting

In addition to managing HTTP traffic, the 3100-6GT-I also supports HTTPS scanning and website control. To enable HTTPS management, an **SSL root certificate** must be generated and imported to each user's device.

Since HTTPS also uses **Transparent Proxy** technology, no browser configuration is required—only certificate installation is needed.

- **[SSL Listen Port]**: Specifies which ports to inspect via HTTPS proxy. The default is 443. Multiple ports can be entered (e.g., 443,8443,888) to enable scanning on each.
- **[Certificate Time]**: Displays the timestamp of the current locally generated root certificate.
- **[Download SSL Certificate]**: Click to download the root certificate from the 3100-6GT-I to the administrator's computer, then distribute it to users.

  If any changes are made to the certificate, it must be regenerated and downloaded again. Click **"Re-generate Certificate"** to open the prompt (see Figure 6-17).

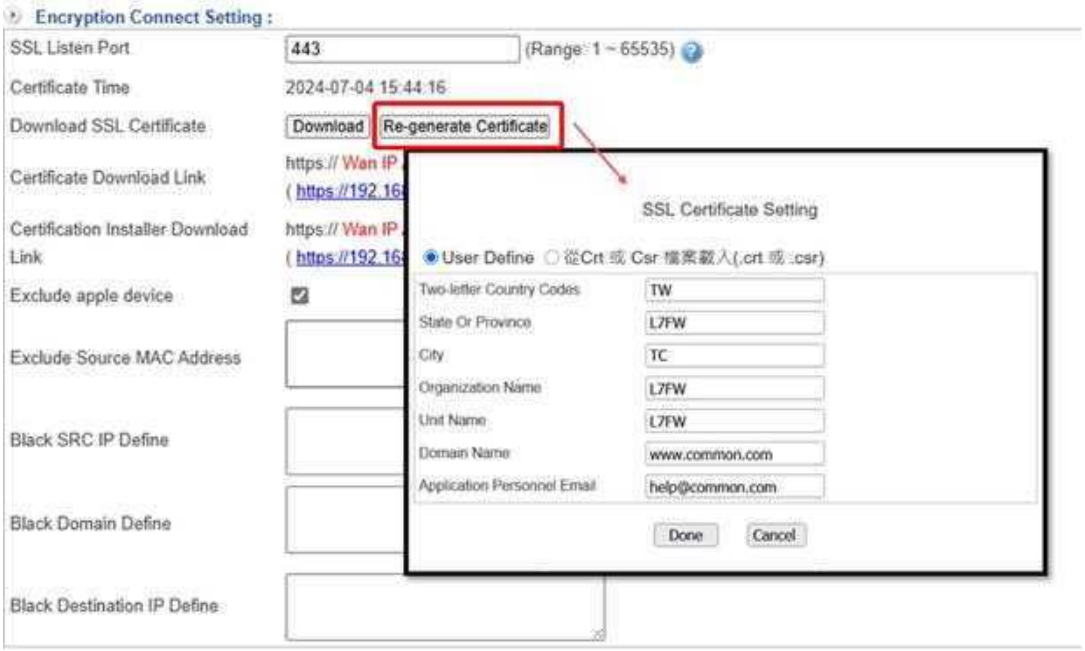


Figure 6-17

- **[Certificate Download Link]**: Administrators can provide users with a URL to download and install the root certificate manually. The link consists of three parts:

  1. The IP address or domain name of the network interface (e.g., the IP of ZONE1 is 192.168.1.254).
  2. The port set under **[Network] > [Interface] & [Route] > [HTTPS Port]**, default is 443.
  3. The file name of the root certificate (e.g., myca.crt).

  In this example, the download URL is: https://192.168.1.254:443/myca.crt. Users can click the link to install the certificate directly.

- **[Certification Installer Download Link]**: When users switch between browsers, each browser may require separate certificate trust settings. To simplify this process, Volktek provides a **Windows-based installer** that automatically installs the root certificate for **Microsoft Edge, Chrome, and Firefox**.

Administrators can provide users with a URL to download the installer. The link consists of three parts:

1. The IP address or domain name of the network interface (e.g., ZONE1 = 192.168.1.254).
2. The port set under **[Network] > [Interface] & [Route] > [HTTPS Port]**, default is 443.
3. The installer file: download_certinstaller.php

In this example, the download URL is: https://192.168.1.254:443/download_certinstaller.php. Users can click the link to download the installer. Once executed, the required root certificate is installed automatically (see Figure 6-18).

Figure 6-18

- **[Exclude Apple Device]**: Apple's trusted certificate list cannot be modified. Enabling HTTPS proxy on Apple devices may cause connection failures. When this option is selected, all Apple devices are excluded from HTTPS proxy.
- **[Exclude Source MAC Address]**: Exclude connections from specified MAC addresses from HTTP/HTTPS filtering.
- **[Black SRC IP Define]**: Exclude connections from specified source IP addresses from HTTP/HTTPS filtering.
- **[Black Domain Define]**: Excludes connections to specified domains from HTTP/HTTPS filtering.
- **[Black Destination IP Define]**: Exclude connections to specified destination IP addresses from HTTP/HTTPS filtering.

Certification Installer Setting

To simplify SSL certificate installation, when a user tries to access a website, the 3100-6GT-I checks if the source IP has installed the SSL certificate. If not, the system automatically redirects the user to the certificate download page for easy access (see Figure 6-19).

Figure 6-19

- **[Redirect Port]**: Port number used for redirection; must not be in use.
- **[Connection Protocol]**: Protocol used for redirection, either HTTP or HTTPS.
- **[Source IP address]**: Specifies which source IP addresses the redirection applies to; other IPs are unaffected.
- **[The IP has been redirected]**: Lists IPs that have already been redirected.

  If a source IP is not yet trusted, the user's web request will be redirected to a page containing the certificate installer and installation instructions (see Figure 6-20).

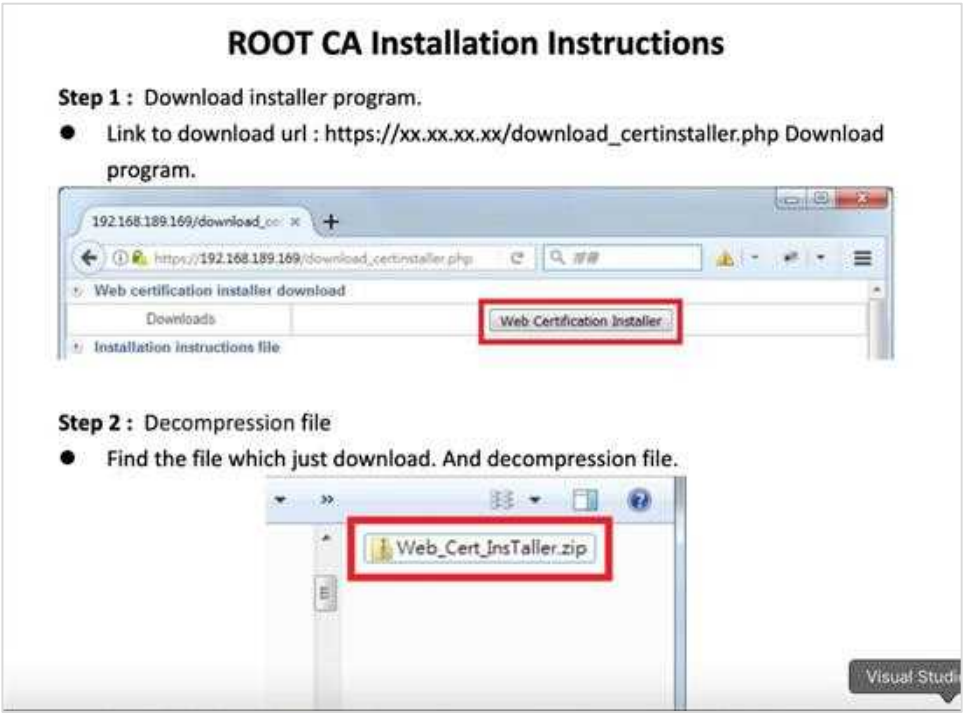


Figure 6-20

SSL Certificate Message

Displays the current SSL certificate in use. Configure settings under [Configuration] > [SSL Certificate] > [SSL Certificate Set]. If modified, users must reinstall and trust the updated root certificate.

SSL Certification Import

Imports SSL certificates, including manually entered or officially issued certificates.

6-6-2. HTTPS Log

All HTTPS proxy connection logs are recorded here. Disabled by default (see Figure 6-21).

Date	HTTPS Name	Interface	Source IP Address	Destination IP Address
2024-08-16 14:58:13	play.google.com	LAN2	192.168.66.66	142.251.42.238
2024-08-16 14:58:13	waa-pa.clients6.google.com	LAN2	192.168.66.66	172.217.163.42
2024-08-16 14:58:12	www.googleapis.com	LAN2	192.168.66.66	172.217.163.42
2024-08-16 14:58:11	powerpoint-telemetry.officeapps.live.com	LAN2	192.168.66.66	52.108.78.27
2024-08-16 14:58:07	scan.sharetech.com.tw	LAN2	192.168.66.66	125.227.221.218
2024-08-16 14:58:05	browser.pipe.aria.microsoft.com	LAN2	192.168.66.23	20.189.173.27

Figure 6-21

6-6-3. White Certification

Some websites or applications may trigger certificate failures when passing through the 3100-6GT-I, causing service disruptions. In such cases, administrators can whitelist the failed certificates here. Once whitelisted, the 3100-6GT-I will no longer replace them, ensuring uninterrupted user access.

Certifications Failed Log

Clicking the **"Search"** button lists all certificate failures within the selected period. Select the certificates to whitelist, then click **"Add Whitelist Certification"** to complete the process (see Figure 6-22).

Certifications Failed Log — 1 / 104 jump to 1 Page every page 30 rows GO Export Export All

Date	Source IP Address	Destination IP Address	Domain	Count
2024-08-08 10:27:51	192.168.66.23	20.118.138.130	www.telecommandsvc.microsoft.com	14
2024-08-08 10:27:50	192.168.66.23	20.3.187.198	fe3cr.delivery.mp.microsoft.com	52
2024-08-08 10:27:42	192.168.66.23	20.189.173.12	mobile.events.data.microsoft.com	1
2024-08-08 10:27:40	192.168.66.23	40.119.249.228	settings-win.data.microsoft.com	299
2024-08-08 10:27:28	192.168.66.23	20.44.248.159	wdcpalt.microsoft.com	34
2024-08-08 10:27:27	192.168.66.23	20.44.248.159	wdcp.microsoft.com	15
2024-08-08 10:27:25	192.168.66.23	118.214.246.236	storecatalogrevocation.storequality.microsoft.com	8
2024-08-08 10:27:24	192.168.66.23	20.44.220.42	displaycatalog.mp.microsoft.com	30
2024-08-08 10:27:21	192.168.66.23	20.247.184.142	licensing.mp.microsoft.com	16

Figure 6-22

White Certification List

Whitelisted certificates are listed below (see Figure 6-23).

White Certification List — 1 / 1 jump to 1 Page every page 30 rows GO Export Export All

Destination IP Address	Domain
52.179.209.218	options.skype.com
13.94.112.175	api.mcr.skype.com
13.93.149.41	api.mcr.skype.com

Figure 6-23

6-7. High Availability

The 3100-6GT-I supports High Availability (HA) by pairing two identical units—one as **Master**, the other as **Backup**. If the Master fails, the Backup immediately takes over, ensuring continuous network traffic and uninterrupted business operations.

Administrators are promptly notified of any HA failover events, allowing them to repair the failed unit and restore redundancy as quickly as possible.

The 3100-6GT-I uses an **Active-Backup** HA model, where only one unit is active at a time. The Backup remains in standby mode and takes over traffic only if the active unit fails.

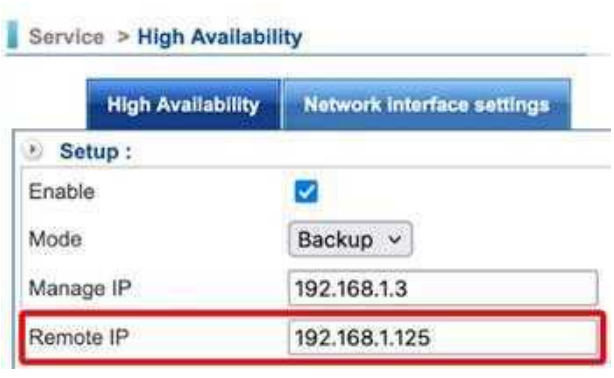
Before enabling HA, go to **[Network] > [Zone Settings]** to assign the HA port.

High Availability – Master

- **[Enable]**: Enable or disable the HA function.
- **[Mode]**: Sets this device as the Master.
- **[Manage IP]**: When HA is enabled, both devices share a virtual IP address. Regardless of which device is active, the system can be accessed via its physical IP or this shared virtual IP, which serves as the management IP.
- **[Remote IP]**: The physical IP address of the Backup device when this device is operating as the Master.

High Availability – Backup

- **[Enable]**: Enable or disable the HA function.
- **[Mode]**: Sets this device as the Backup.
- **[Manage IP]**: When HA is enabled, both devices share a virtual IP address. Regardless of which device is active, the system can be accessed via its physical IP or this shared virtual IP, which serves as the management IP.
- **[Remote IP]**: The physical IP address of the Master device when this device is operating as the Backup.

Master	Backup
	

After HA is enabled on both units, the interface IP addresses must be within the same subnet but use different IPs. Otherwise, IP conflicts may occur.

For example, if this unit is set as the Master and the remote IP is set to *192.168.1.126*, then *192.168.1.126* is the Backup unit. The 3100-6GT-I will verify that the remote unit has the same model group and firmware version before synchronization is allowed.

The Backup unit displays the latest synchronization time. By default, the Backup requests data sync from the Master every five minutes. Administrators can also manually trigger synchronization.

Note 1: When HA switches to the Backup unit, any configuration changes made on the Backup will **not** be synced back to the Master once it recovers. To retain the changes made on the Backup, you can swap the roles—set the current Master as Backup and the Backup as Master. This ensures the system uses the data from the previously active Backup.

Note 2: The following data will **not** be synchronized:

1. Content log data
2. System operation logs
3. System/network status diagrams
4. Computer member list
5. Traffic analysis data

6-8. Remote Syslog

Remote Connect Setup

The 3100-6GT-I can send connection logs to an external Syslog server for storage or analysis.

- **[Enable]**: Enable or disable the Syslog function.
- **[Server IP]**: IP address of the remote Syslog server (e.g., 192.168.1.100).
- **[Server Port]**: Port used by the remote Syslog server. Default is UDP 514.
- **[Device Hostname]**: The name used when sending logs. This name will appear on the Syslog server, helping identify which device the logs came from.

Log Setting

The 3100-6GT-I supports two Syslog formats: **standard Syslog** and **CEF**. The format used is determined by the Syslog server.

Log Item

The 3100-6GT-I can send seven types of logs to the Syslog server. Each category contains sub-items that can be selected by the administrator.

1. Object
2. Advanced Protection
3. Mail Security
4. Content Log
5. VPN
6. Log
7. Status

Chapter 7. Advanced Protection

The 3100-6GT-I employs **collaborative protection between abnormal IP analysis and switches** to monitor the status of internal machines in real-time. When abnormal traffic occurs, it blocks the packets and identifies which device is on which switch port—helping prevent network disruptions.

Cooperative protection works by allowing the 3100-6GT-I to communicate with switches. When threats are detected, it can send **SNMP** or **TELNET/SSH** commands to the switch to block the affected port.

This isolates the problematic device immediately without disrupting normal user activity (see Figure 7-1).

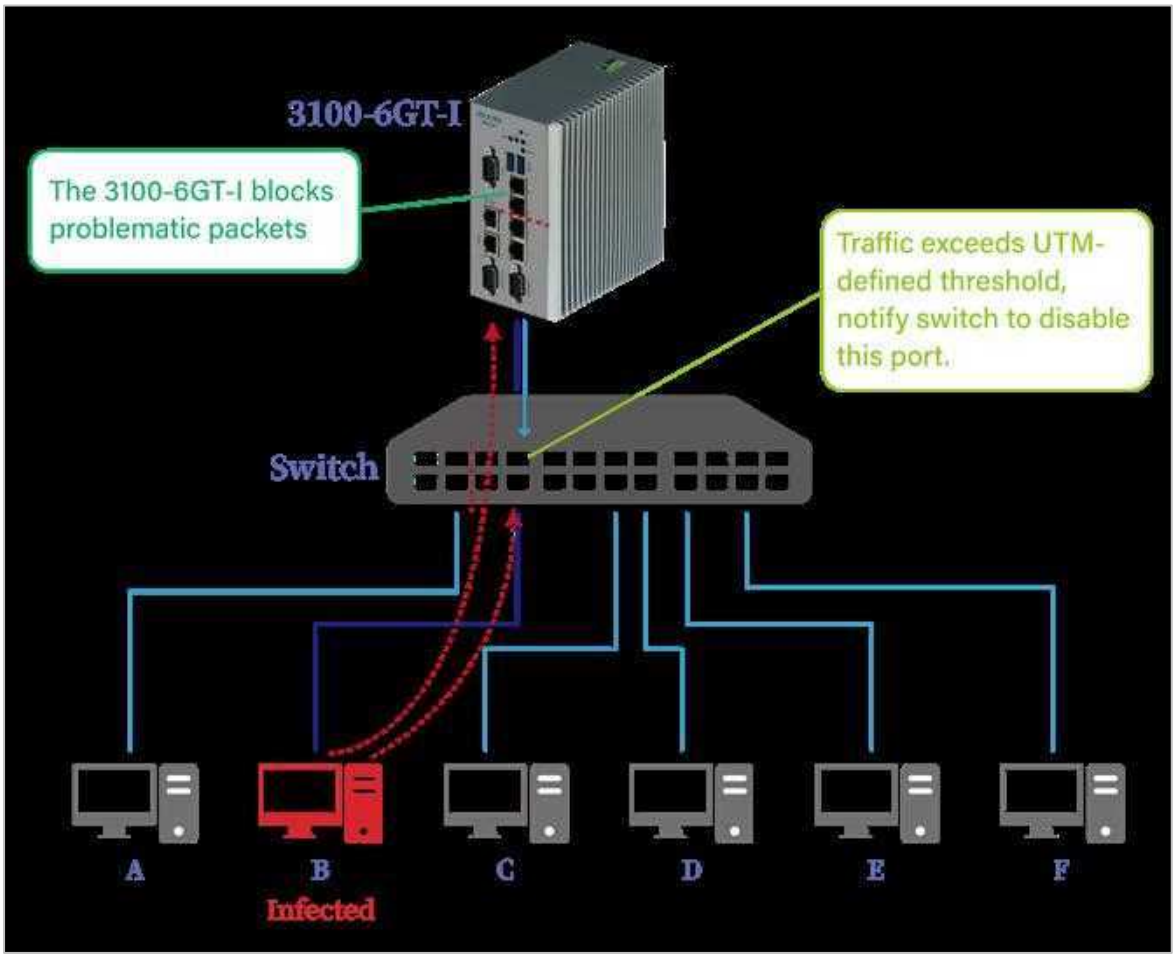


Figure 7-1

In general, **Layer 2 switches with SNMP support** are affordable in the market. This makes the cooperative protection solution both practical and cost-effective—avoiding the common issue where a good idea becomes difficult to implement due to high costs or deployment complexity.

Even if full replacement is not feasible, deploying these switches in key segments can help contain internal network issues within a limited area.

Switches that support cooperative protection also enable **IP–PORT–MAC binding**, enhancing control and visibility.

7-1. Anomaly IP Analysis

When the 3100-6GT-I detects abnormal connection counts or traffic volume between internal interfaces, it can take one or more of the following actions: **Log**, **Notify**, and **Block**. Administrators may enable all or select any combination to maintain normal network operation.

1. **Log**

   If the number of connections or traffic volume entering or leaving an interface exceeds the threshold, the 3100-6GT-I logs the event and source IP for later review.

2. **Notify**

   In addition to logging, the system notifies the administrator based on the configured alert method.

3. **Block**

   Along with logging, the system blocks the offending traffic according to the defined rules.

Regardless of the application in use, user behavior can be analyzed through network packet patterns such as **connection count (sessions)**, **traffic volume (flow)**, and **duration (time)**. By monitoring these metrics, the 3100-6GT-I can determine whether the behavior is normal or abnormal.

When abnormal activity is detected, administrators can apply various policies—such as blocking internet access, limiting bandwidth, triggering cooperative protection to block the port via switch, or simply sending a notification.

For example, streaming a video typically uses around 5 Mbps of download bandwidth over time, but does not generate high upload usage or excessive connections. Administrators can define thresholds that are safe under normal usage, allowing the 3100-6GT-I to serve as the first layer of defense.

If a user exceeds the defined limits, the system can apply one of three actions: **bandwidth limiting**, **blocking**, or **switch-level port shutdown**. Administrators can choose actions based on their needs. For instance, in managed dormitory networks, strict enforcement is common—violators may have their bandwidth throttled, allowing only limited access.

In terms of configuration sensitivity: **Log < Notify < Block**.

7-1-1. Common Setup

Select the interfaces for anomaly detection. The 3100-6GT-I lists all configured interfaces, and only enabled interfaces will perform detection.

7-1-2. Log Anomaly

When traffic exceeds the threshold, the 3100-6GT-I logs the source IP, trigger count, and duration. Settings apply globally across all interfaces (Zones) on the device.

Anomaly detection thresholds for outbound traffic from internal hosts to external interfaces (Zones).

- **[Connection Session exceeds]**: Logs the source IP and exceeded value when **the number of outbound connections** from a single IP exceeds the set threshold for a specified duration.
- **[Zone Out (TX) Flow exceeds]**: Logs the source IP and exceeded value when **outbound traffic (TX)** from a single IP exceeds the threshold for a specified duration.
- **[Zone In (RX) Flow exceeds]**: Logs the source IP and exceeded value when **inbound traffic (RX)** from a single IP exceeds the threshold for a specified duration (see Figure 7-2).

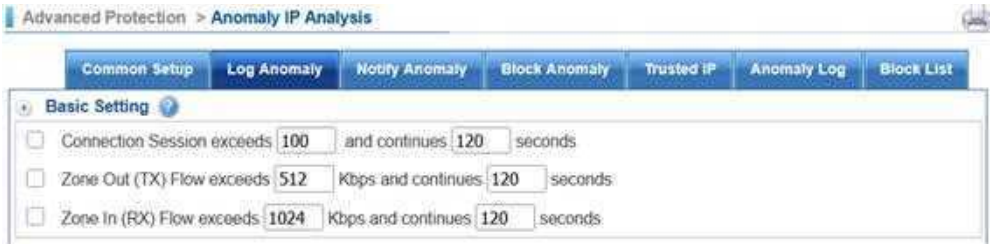


Figure 7-2

7-1-3. Notify Anomaly

When traffic exceeds the threshold, the 3100-6GT-I logs the source IP, trigger count, and duration, and immediately notifies the administrator. Settings apply to all interfaces (Zones).

Anomaly detection thresholds for outbound traffic from internal hosts to external interfaces (Zones).

- **[Session exceeds]**: Logs the source IP and exceeded session count when **the number of outbound connections** from a single IP exceeds the set value for a defined duration.
- **[Zone Out (TX) Flow exceeds]**: Logs the source IP and exceeded value when **outbound traffic (TX)** from a single IP exceeds the threshold for a defined duration.
- **[Zone In (RX) Flow exceeds]**: Logs the source IP and exceeded value when **inbound traffic (RX)** from a single IP exceeds the threshold for a defined duration. (See Figure 7-3)

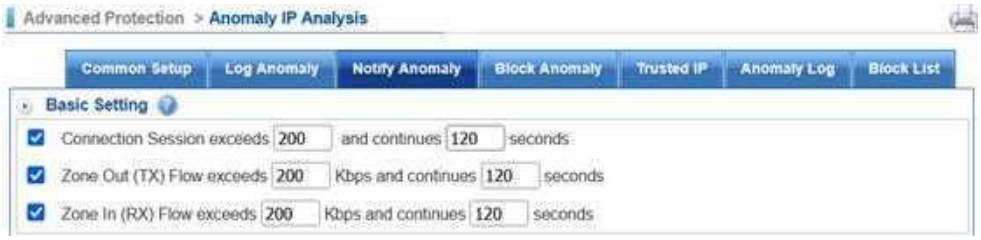


Figure 7-3

7-1-4. Block Anomaly

When traffic exceeds the defined threshold, the 3100-6GT-I logs the source IP, trigger count, and duration, and triggers the default blocking action to stop further abnormal activity. These settings apply across all interfaces (Zones) on the device.

Basic Setting

Anomaly detection thresholds for outbound traffic from internal hosts to external interfaces (Zones).

- **[Session exceeds]**: Logs the source IP and exceeded session count when **the number of outbound connections** from a single IP exceeds the set value for a defined duration.
- **[Zone Out (TX) Flow exceeds]**: Logs the source IP and exceeded value when **outbound traffic (TX)** from a single IP exceeds the threshold for a defined duration.
- **[Zone In (RX) Flow exceeds]**: Logs the source IP and exceeded value when **inbound traffic (RX)** from a single IP exceeds the threshold for a defined duration. (See Figure 7-4)

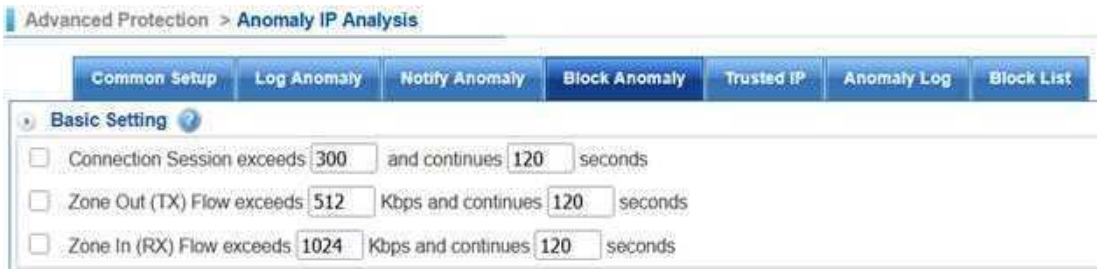


Figure 7-4

Action

When thresholds are triggered, administrators can choose from six predefined actions for handling abnormal behavior:

1. **Temporary Block (few minutes)**

   The source IP is blocked from accessing external Zones for a few minutes. Internal traffic within the Zone remains unaffected. This is suitable for temporary or accidental spikes.

2. **Block All Day**

   The source IP is blocked from external Zones for the rest of the day (until 24:00), as a penalty for severe violations. Internal Zone traffic is not affected.

3. **Block until administrator to unlock**

   The source IP remains blocked from external Zones until manually unblocked by an administrator. Internal Zone traffic is not affected.

4. **Bandwidth Limit (few minutes)**

   The source IP is throttled for a few minutes to address unfair bandwidth usage. Limit values are set under **[Other Settings]**.

5. **Bandwidth Limit for All Day**

The source IP is bandwidth-limited for the entire day (until 24:00). Limit values are set under **[Other Settings]**.

6. **Bandwidth Limit Until Released by Admin**

   The source IP is bandwidth-limited until the administrator manually lifts the restriction. Limit values are set under **[Advanced Setup]**. (See Figure 7-5)

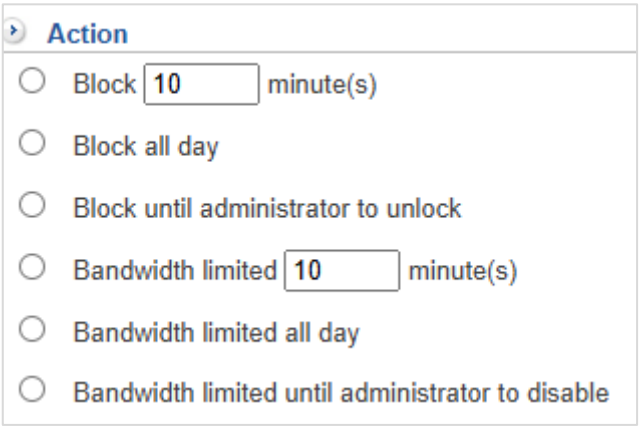


Figure 7-5

Advanced Setup

When a threshold is triggered and bandwidth limiting is selected as the action, the defined limit will automatically apply to the offending device.

- **[Bandwidth Limited]**: Once triggered—whether by session count or traffic volume—the 3100-6GT-I reduces the source IP's bandwidth to the specified value (e.g., 200 Kbps), slowing down its network usage.
- **[Block Message]**: When bandwidth limiting is active, a custom message will appear on the user's web browser, indicating that speed restrictions are in effect. (See Figure 7-6)

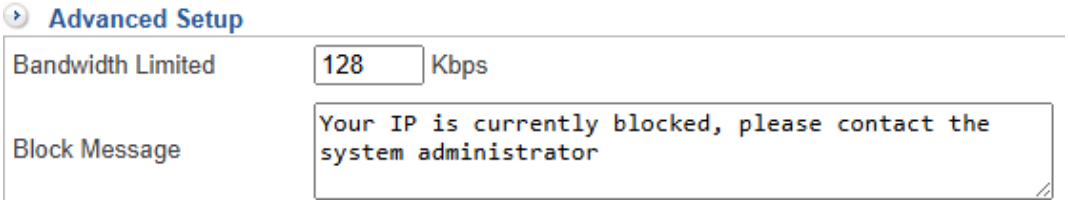


Figure 7-6

7-1-5. Trusted IP

The 3100-6GT-I can log, notify, and block abnormal sessions, upload, and download traffic. However, in some cases, you may want to exclude specific users from anomaly detection. This can be done using the **Trusted IP** setting.

- **[IP/Netmask]**: Specifies IP addresses or subnets to be excluded from anomaly analysis. For example, *192.168.1.5/32* is a single IP, while *192.168.1.1/24* represents a Class C subnet.
- **[Type]**: Select one or more actions to exclude—Log, Notify, or Block.
- **[Comment]**: Optional description for the source IP. (See Figure 7-7)

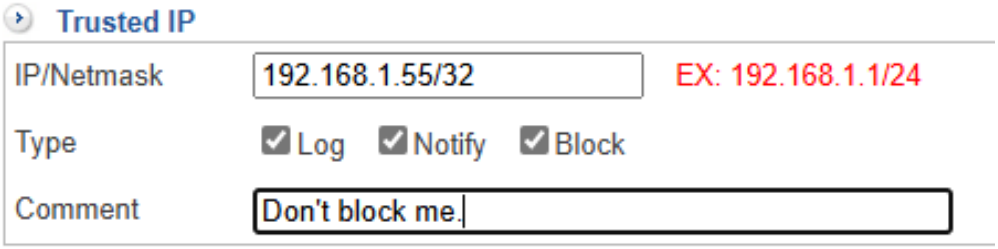


Figure 7-7

7-1-6. Anomaly List

For all abnormal activities, the system logs detailed information including Date, IP, Authentication, Action, Event, Actual Value, Period, and Limited Time. (See Figure 7-8)

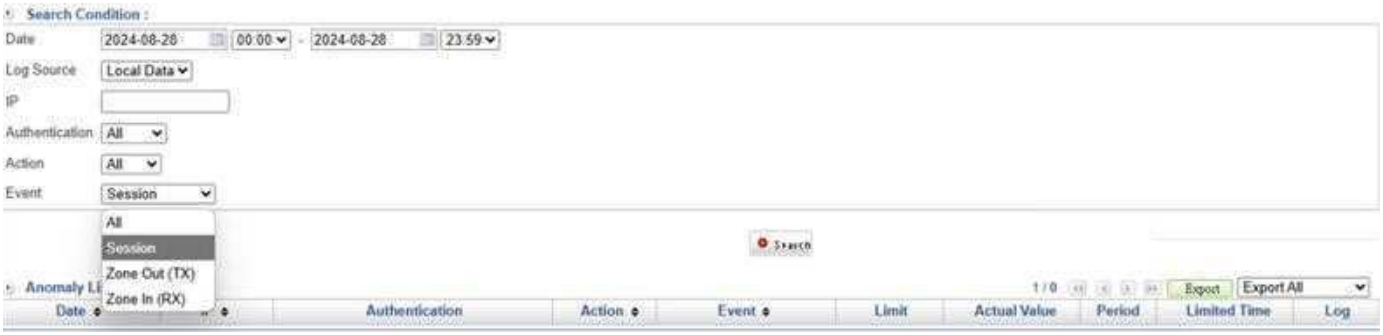


Figure 7-8

7-1-7. Block List

Displays the list of source IP addresses currently blocked by the 3100-6GT-I. Administrators have the authority to manually release these IPs.

7-2. Switch

The 3100-6GT-I works with switches to monitor internal device distribution in real time. When abnormal traffic occurs, it blocks the packets and helps prevent network outages.

Administrators may focus on different needs—traffic per IP or physical device location. Internal cabling can make this difficult.

Volktek simplifies this with a hierarchical view showing uplink/downlink connections from the 3100-6GT-I's LAN or DMZ. As shown in Figure 7-9, administrators can easily trace and locate problematic devices.

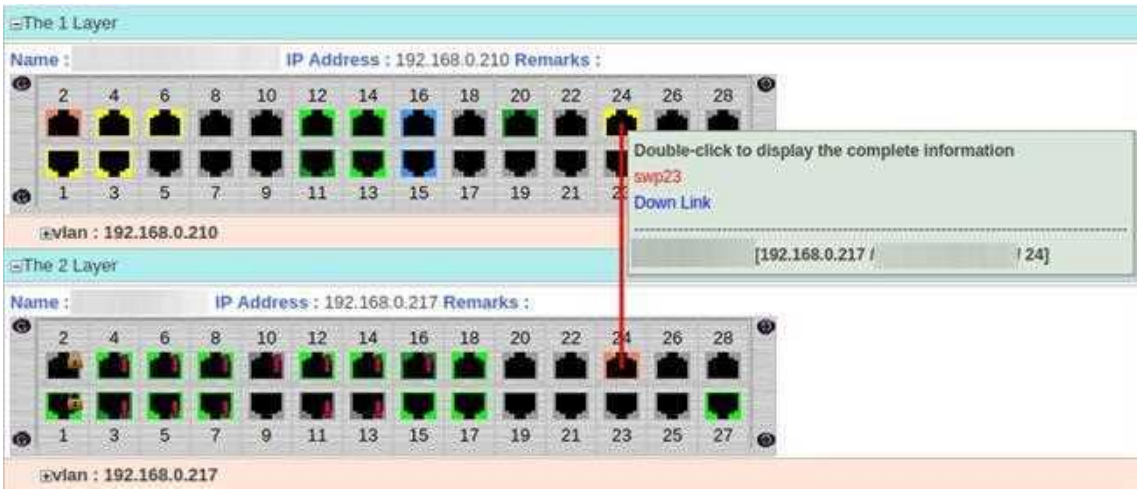


Figure 7-9

The graphical interface shows which switch port each IP is connected to, making the network structure easy to understand—including switch interconnections.

Paired with the 3100-6GT-I's address table view, network management becomes visual and precise. Every IP is tied to a switch port, making user behavior and admin actions traceable.

3100-6GT-I Supported Switch Types

The 3100-6GT-I supports cooperative defense with core switches. In addition to displaying the network topology, it can automatically block problematic devices on the switch based on administrator settings.

For example, if ZONE1 is a high-traffic internal network, a core switch with cooperative defense capability can be deployed for enhanced control.

7-2-1. Switch Setup

When switch management is enabled, switch details must be added via **[Advanced Protection] > [Switch] > [Switch Setup]**.

- **[Interface]**: Select the interface (Zone) where the switch is connected, e.g., ZONE1.
- **[Switch Type]**: Select a core switch that supports cooperative defense.
- **[Switch Model]**: Lists verified and supported cooperative defense switches. Currently supports only Volktek Managed Switches.
- **[Name]**: Custom name for the switch, e.g., “1F,” for easy identification.
- **[Remarks]**: Optional notes, e.g., “Core Switch.”
- **[IP Address]**: IP address of the switch, e.g., 192.168.2.55.
- **[Port]**: Number of ports on the switch.
- **[SNMP Read Community]**: Community name with read access for SNMP communication. Default is “public.” Use **[Connection Test]** to verify access.
- **[SNMP Write Community]**: Community name with write access for SNMP communication. Default is “private.” Use **[Connection Test]** to verify access.
- **[Web Management]**: Port used to access the switch’s web interface, typically 80.
- **[Advanced Command]**: Protocol used for command communication—**Telnet** or **SSH**. Choose based on the switch's supported mode.
- **[Command Port]**: Communication port—**23** for Telnet, **22** for SSH (fixed, cannot be changed).
- **[Login Account]**: Username for command-based login, e.g., “admin” or “root.”
- **[Login Password]**: Password for the login account.
- **[Enable Password]**: Optional secondary password required to apply configuration changes on the switch.
- **[Bind Mode]**: Uses **MAC + PORT** binding. Each MAC address is tied to a specific switch port. For example, a device with MAC *00:01:02:03:04:05* can only access the network via port 21. If plugged into another port, access is denied. (See Figure 7-10)

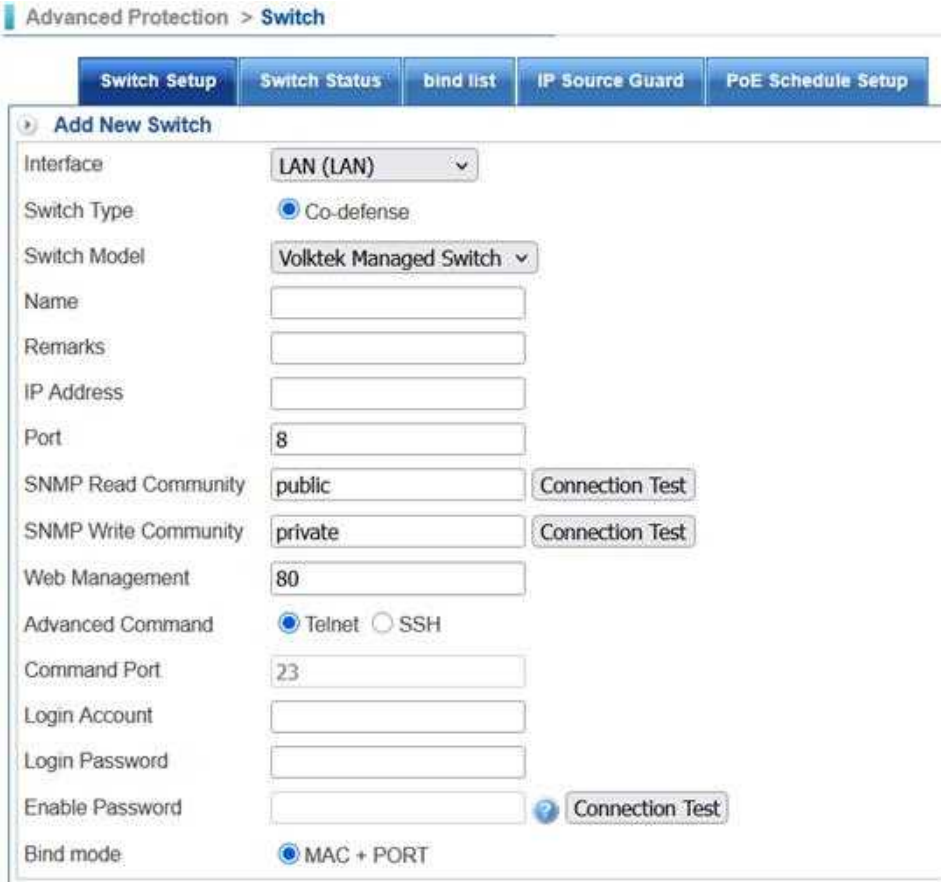


Figure 7-10

Search Switch

In the switch list, click the **"Search Switch"** button to let the 3100-6GT-I automatically locate all SNMP switches under each interface. The search results will open in a separate window.

To manage a switch, click the "plus" button under the Action column to enter switch configuration mode. Set the account credentials, port number, and designate the operating interface to complete the switch addition process. (See Figure 7-11)

Figure 7-11

After the switch configuration, the 3100-6GT-I will display a list of all switches. Administrators can verify settings or click the **"gear"** icon to open the switch management interface in a new window, based on the selected mode. (See Figure 7-12) This feature allows administrators to manage all internal switches through a unified interface.

Figure 7-12

7-2-2. Switch Status

Cable tracing is a major challenge for enterprises, especially in cluttered environments where identifying which PC connects to which switch is difficult.

The 3100-6GT-I, combined with collaborative defense and SNMP-managed switches, provides real-time visibility into the network—including switch stacking relationships and the ports used.

Administrators can clearly see each user's connection status, which switch they're connected to, whether the device is on, and even trace connections through secondary switches. (See Figure 7-13)

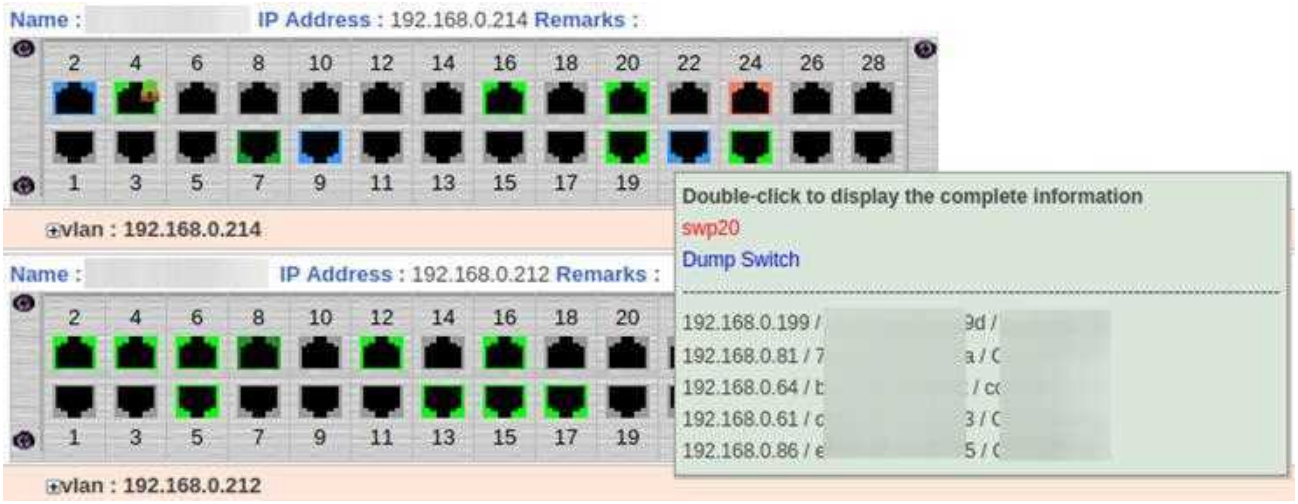
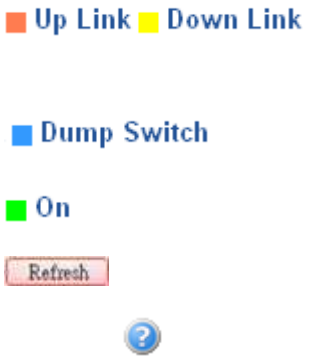


Figure 7-13

Diagram Explanation:



To view the connection between switches and computers, the 3100-6GT-I offers three display modes: **graphic**, **list view**, and **IP-based view**. Administrators can also filter by interface (ZONE).

You can schedule automatic updates to keep network status current. A search function is also available—enter an IP address, and the 3100-6GT-I will identify which switch and port the device is connected to. (See Figure 7-14)

Figure 7-14

Clicking either icon will display detailed information for the selected switch port in the 3100-6GT-I interface. (See Figure 7-15)

- **[Up Link Port]**: Designates this port as the uplink port.
- **[Enable/Disable]**: Enables or disables the port.
- **[In/Out]**: Displays inbound and outbound traffic for the port.
- **[Zone Out (TX)/Zone In (RX) (bps)]**: Shows traffic between this IP address and the Internet.
- **[Binding]**: In collaborative defense mode, binds a specific IP/MAC to this port.

Figure 7-15

7-2-3. Bind List

For security or internal management, administrators can restrict switch ports to specific devices. Unauthorized computers will be blocked. The 3100-6GT-I's collaborative defense supports this feature.

There are two binding modes: **[IP+MAC+Port]** and **[MAC+Port]**. The former requires entering an IP address; the latter does not. All other settings are the same. The following instructions use the **[MAC+Port]** mode as an example. Select the collaborative switch IP address from the binding list.

Add Bind List

- **[MAC Address]**: The MAC address to be bound, e.g., *02:03:04:05:06:07*. Devices with a different MAC address will be denied network access.
- **[Co-defense]**: Indicates which collaborative defense switch this device is bound to.
- **[Port]**: The specific port on the switch where the device is bound, e.g., Port 24.
- **[VLAN]**: Specify the VLAN to which the binding IP belongs.
- **[Bind mode]**: The current binding mode in use is [MAC+Port]. (See Figure 7-16)

Figure 7-16

7-2-4. IP Source Guard

The 3100-6GT-I also supports another IP+MAC+Port binding mode—**IP Source Guard**. In addition to enforcing IP+MAC+Port bindings, it includes a DHCP snooping mechanism to block unauthorized internal DHCP servers.

IP Source Guard requires VLAN configuration, so related VLAN settings must be completed on the switch first.

Add IP Source Guard Binding List

Click the "Add" button under IP Source Guard to create a new IP+MAC+Port binding.

- **[Co-defense]**: Select the IP address of the collaborative defense switch for the IP+MAC+Port binding, e.g., *192.168.14.2*.
- **[VLAN]**: Select the VLAN where the binding will be applied. The system will list all active VLANs for selection, e.g., VLAN1.
- **[Trusted Ports]**: Specify which ports in the VLAN are exempt from IP+MAC+Port binding. These are called **Trusted Ports**, where any IP and MAC address can access the network. Click **[Assist]** to display a visual diagram of the switch. Administrators can select ports belonging to the VLAN—clicking an **"X"** will toggle the port to a Trusted Port with a **"V"** status.
- **[Assist in Adding]**: The 3100-6GT-I can auto-fill binding entries using previously recorded IP+MAC+Port data for devices that have connected to the switch VLAN, reducing manual input. (See Figure 7-17)

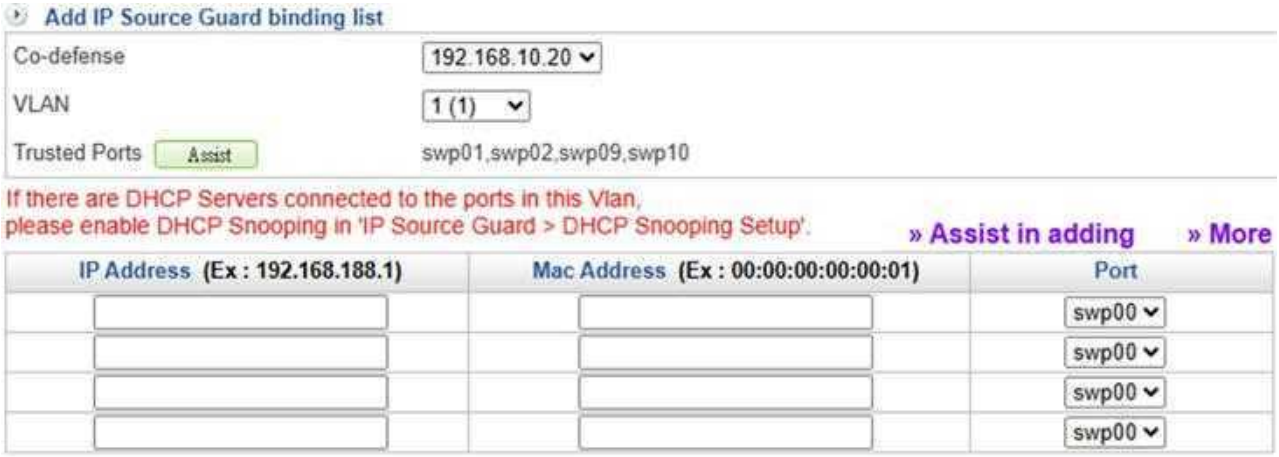


Figure 7-17

Adding DHCP Snooping Configuration

IP Source Guard blocks unauthorized DHCP servers within each VLAN, allowing only approved ones to assign IP addresses. Administrators must know which switch port the DHCP server is connected to for each VLAN.

When configuring IP Source Guard, the 3100-6GT-I opens a new window. (See Figure 7-18) Selecting a VLAN displays its ports—**red** for untagged, **green** for tagged.

Trusted Ports are exempt from IP+MAC+Port binding and allow any IP/MAC to connect. At least one Trusted Port is required when DHCP Snooping is enabled. Click the **"X"** to toggle a port to **"V"** (Trusted).

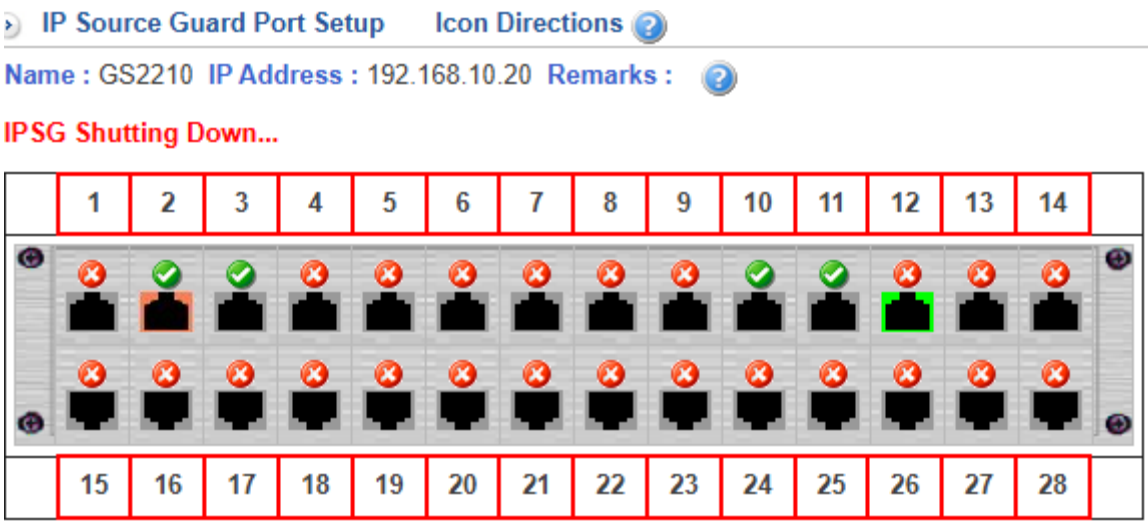

IP Source Guard Port Setup
Icon Directions
Name : GS2210 IP Address : 192.168.10.20 Remarks :
IPSG Shutting Down...
1 2 3 4 5 6 7 8 9 10 11 12 13 14
15 16 17 18 19 20 21 22 23 24 25 26 27 28

Figure 7-18

7-3. Intranet Protection

Broadcast-based attacks—such as ARP spoofing and rogue DHCP servers—are among the hardest to detect due to protocol-level limitations. Even if an attacker is identified, traditional systems can't communicate directly with first-line devices like the 3100-6GT-I or switches to block threats in real time. In most cases, physical cable tracing at each switch is the only option.

The 3100-6GT-I addresses this by offering built-in tools to block such attacks.

When collaborative defense is enabled, the 3100-6GT-I activates advanced protection features for the internal network, including **ARP Protection**, **IP Collision**, **MAC Collision**, and **Abnormal IP Blocking**.

These features can be applied by selecting the desired detection mechanisms per interface (Zone).

7-3-1. Spoofing Setup

Detection Interface

Select the network interface (ZONE) where internal protection will be applied. Multiple interfaces can be selected, and this feature is typically used on internal networks.

detection rule will be directly blocked.

advanced blocking may result in all devices under that port being mistakenly blocked.

ARP Spoofing Alert Value

ARP-based attacks are harder for the 3100-6GT-I to handle because ARP uses broadcast packets and operates before any TCP/UDP connection is established.

Volktek's ARP detection mechanism identifies devices that are aggressively sending ARP requests—often a sign of pre-attack behavior. At this stage, the activity may appear borderline between normal and malicious.

When used with a collaborative defense switch, the system can pinpoint the physical location of the suspicious IP, leaving the attacker nowhere to hide. (See Figure 7-19)

Figure 7-19

If a victim is detected on the network, administrators can suspect IPs previously flagged for excessive ARP traffic as potential attackers. Using collaborative defense, the switch port of the attacker can be blocked to isolate the device and prevent further impact.

- **[Each Source IP Address Exceeds]**: Number of ARP requests per second from a single IP that triggers detection. Default is 100. Higher values reduce sensitivity; lower values may cause false positives.
- **[Automatically Blocked by Switch]**: Automatically blocks devices showing abnormal ARP behavior.
- **[True Address]**: IP addresses excluded from ARP detection, e.g., 192.168.1.100. (See Figure 7-20)

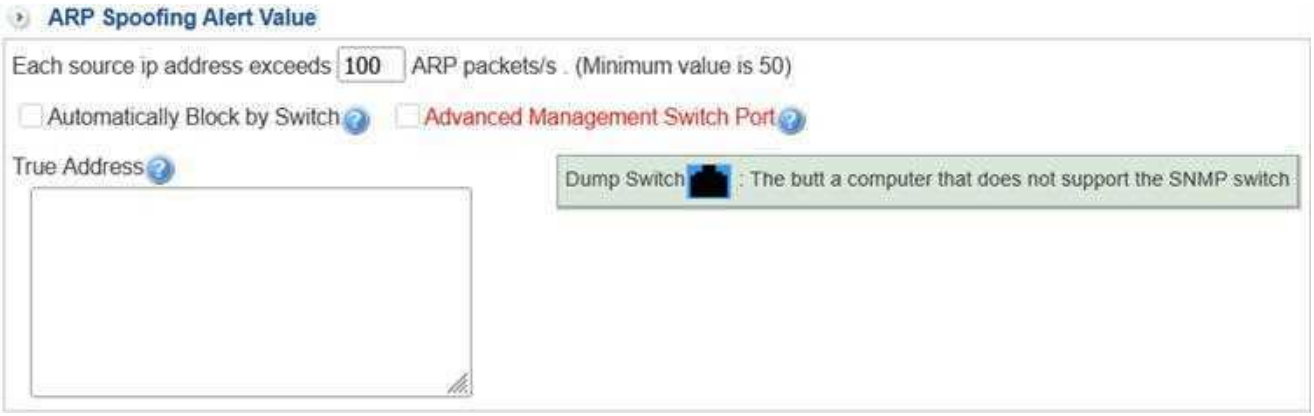


Figure 7-20

IP/MAC Collision Detection

Internal IP or MAC conflicts can disrupt network operations. The 3100-6GT-I includes built-in detection mechanisms to help administrators manage these issues.

- **[IP Address Collision Detection]**: Enables detection of IP conflicts. Disabled by default.
- **[Automatically Blocked by Switch]**: Automatically blocks devices with forged IP addresses upon detection.
- **[True Address]**: IP addresses excluded from conflict detection, e.g., 192.168.1.100.
- **[MAC Address Collision Detection]**: Frequency of MAC conflict checks; default is every 3 hours.
- **[Automatically Blocked by Switch]**: Blocks devices with duplicated or forged MAC addresses.
- **[True Address]**: MAC addresses excluded from detection, e.g., 00:01:02:03:04:05. (See Figure 7-21)

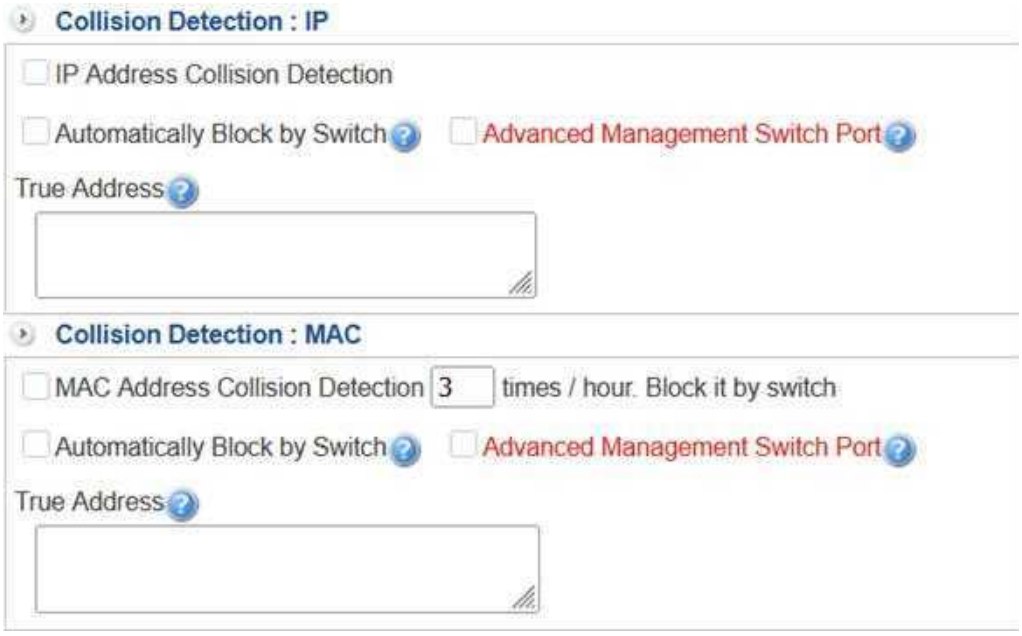


Figure 7-21

Co-defense

In **[Advanced Protection]** > **[Anomaly IP Analysis]**, the **[Block Anomaly]** function works with collaborative defense switches to enforce automatic response.

When a user exceeds connection limits or upload/download bandwidth, the 3100-6GT-I notifies the switch to block the device, preventing further access. (See Figure 7-22)

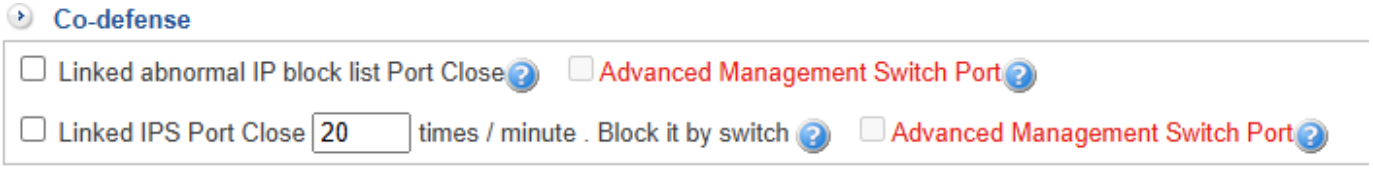


Figure 7-22

Notify Item

When the above events occur, the 3100-6GT-I can immediately notify administrators for action.

Select the types of events to be notified. Available options include: **[Linked abnormal IP block]**, **[OPC Port blocking linked]**, **[ARP Protection]**, **[IP collision]**, and **[MAC collision]**.

7-3-2. ARP Spoofing Log

The ARP spoofing log records details such as time, interface, IP address, MAC address, event type, status, and action taken. It also identifies attackers and victims to help administrators investigate incidents.

- **[IP Address]**: Indicates the IP sending large volumes of ARP packets (attacker) or receiving them (victim).
- **[Interface]**: Select the internal network interface (ZONE) to filter results.
- **[Event]**: Identifies whether the device is a suspected attacker or victim. Attackers are flagged for exceeding threshold values.
- **[Status]**: Indicates whether the ARP attack is ongoing or has stopped. (See Figure 7-23)

Figure 7-23

7-3-3. MAC Collision Log

All MAC spoofing activities are logged. When used with a collaborative defense switch, the connection point is also recorded to assist in investigation.

- **[MAC Address]**: The forged MAC address involved in the conflict.
- **[IP Address]**: IP address of the device using the forged MAC.
- **[Interface]**: The physical port on the collaborative defense switch where the attacker or victim is connected.
- **[Status]**: Description of the MAC spoofing activity.
- **[Re-record Address]**: Clears all learned MAC data and restarts spoofing detection. (See Figure 7-24)

Figure 7-24

7-3-4. IP Collision Log

All IP spoofing incidents are logged. With a collaborative defense switch, the physical connection point is also shown to help administrators investigate.

- **[IP Address]**: The conflicting IP address involved in the spoofing.
- **[Forged IP Address]**: The IP address used by the spoofing device.
- **[Interface]**: The physical port on the collaborative defense switch where the suspected attacker or victim is connected.
- **[Status]**: Description of the IP spoofing event. (See Figure 7-25)


IP address Collision List | Clear | Log Source: Local Data | 1 / 1 jump to 1 Page every page 50 rows GO | Export | Export All

Time	Mac Address	IP Address	Interface	Co-Defense Switch	Event	Status	Action
2024-08-27 10:35:32		192.168.1.24 >> 192.168.1.20	LAN (LAN)	GS1900-48.15	Arp Request	Detected the same ip	
2024-08-27 10:35:03		192.168.1.20	LAN (LAN)	GS1900-48.15	Arp Request	Detected the same ip	
2024-08-27 10:32:32		192.168.1.20	LAN (LAN)	GS1900-48.15	Arp Request	Detected the same ip	
2024-08-27 10:31:03		192.168.1.20	LAN (LAN)		Arp Reply	Detected the same ip	
2024-08-27 10:31:03		192.168.1.20	LAN (LAN)		Arp Request	Detected the same ip	
2024-08-15 14:09:54		192.168.1.168 >> 192.168.1.99	LAN (LAN)		Arp Reply	Detected the same ip	
2024-08-15 14:09:49		192.168.1.168 >> 192.168.1.99	LAN (LAN)		Arp Request	Detected the same ip	
2024-08-15 11:11:54		192.168.1.168 >> 192.168.1.99	LAN (LAN)	GS1900-48.15	Arp Request	Detected the same ip	
2024-08-15 11:09:01		192.168.1.168 >> 192.168.1.99	LAN (LAN)	GS1900-48.15	Arp Request	Detected the same ip	
2024-08-15 11:07:43		192.168.1.168 >> 192.168.1.99	LAN (LAN)		Arp Request	Detected the same ip	
2024-08-15 10:55:22		192.168.1.99	LAN (LAN)	GS1900-48.15	Arp Request	Detected the same ip	

Figure 7-25

7-3-5. Lock Status

The 3100-6GT-I provides advanced internal network protection, including **ARP protection**, **IP spoofing detection**, **MAC spoofing detection**, and **abnormal IP blocking**.

If any IP or MAC address violates access rules and is blocked, all related information will be displayed here. Administrators can also manually unblock devices from this interface.

Chapter 8. OPC

The 3100-6GT-I OT Firewall is equipped with OPC (OT Packet Content) protection, which functions as an Intrusion Prevention System (IPS). It inspects network traffic in real time to detect known attack signatures and immediately blocks malicious packets to prevent external intrusions or internal threats from propagating to the outside

Why OPC Protection?

While traditional firewalls using Stateful Inspection can monitor traffic at OSI Layers 2 to 4—commonly controlling parameters such as:

- Source IP Address
- Destination IP Address
- Source Port
- Destination Port
- TCP Flag Fields

—this is insufficient against Layer 7 application-layer attacks.

For example, SQL Slammer uses a "buffer overflow" attack technique. Since the firewall had the SQL communication port open, external actors were able to access the internal SQL Server. The attacker then used buffer overflow exploit code to attack the internal SQL server and steal the desired data.

How OPC Protection Works

The OPC (Operational Packet Content inspection) function analyzes Layers 4 through 7 of the OSI model to detect malicious code or viruses hidden within TCP/IP communication protocols. Through deep packet inspection, any matching threat signatures are identified and flagged. Once detected, OPC can immediately block these packets, preventing malicious traffic from bypassing the firewall undetected.

Unlike traditional firewalls—which primarily inspect headers and enforce access control—OPC performs content- and behavior-based inspection. The effectiveness of OPC depends heavily on the size and update frequency of its signature database. A more comprehensive database allows the system to identify a wider range of abnormal content and network behaviors. However, this comes at a cost: more extensive inspection requires greater processing power. Without adequate performance, the benefits of detection may be offset by reduced network throughput.

Typically, the OPC signature database is categorized by threat severity into **high**, **medium**, and **low** levels. Network administrators can configure the system to allow or block traffic based on these classifications. In small to mid-sized networks, it is generally sufficient for OPC systems to include complete high- and medium-risk signatures—such as those for viruses and trojans. Lower-risk signatures intended for warnings or notifications are often unnecessary and may be excluded to preserve performance.

To activate OPC protection, follow these configuration steps:

1. **Create an OPC Group:**

   Within the OPC Settings menu, add an OPC group, and specify which signatures to block or log.

2. **Apply the Group via Policy:**

   In the Policy menu, go to “Policy” to apply the pre-configured OPC group.

Given the vast number of OPC signatures, there is a potential risk that legitimate network traffic may be incorrectly identified and blocked, resulting in false positives and network performance issues—counteracting the intended security benefits of OPC inspection.

To address this, the 3100-6GT-I classifies all OPC events into three predefined risk levels: High, Medium, and Low. Correspondingly, two action modes are provided: Block and Log. To minimize the likelihood of unintentional packet blocking, it is recommended that administrators initially enable the Log mode. This allows for monitoring and analysis of OPC-triggered events without impacting network traffic. Once a clear understanding of the traffic patterns is established, appropriate Block actions can be configured based on actual security requirements

8-1. OPC Settings

Each OPC group can operate in one of two modes: **Basic Mode** or **Advanced Mode**. Both modes utilize the same set of signatures; however, the grouping and selection criteria differ. In **Basic Mode**, the 3100-6GT-I pre-classifies signatures into three risk levels—High, Medium, and Low—for easier selection by administrators. In **Advanced Mode**, signatures are categorized by type, such as **Virus** or **Trojan**, allowing administrators to select specific categories or individual signatures for blocking or logging.

- **[Group Name]**: The name of the OPC group, which can be any text combination (e.g., “High-Risk Blocking”).
- **[Mode]**: Two modes are available—**Basic**, which organizes signatures by risk level, and **Advanced**, which organizes signatures by type.

Basic Mode

Signatures are grouped by **severity**: High, Medium, Low risk levels.

Administrators can choose to **Block** or **Log** each severity group. The number of available signatures in each group is shown for reference. (See Figure 8-1)

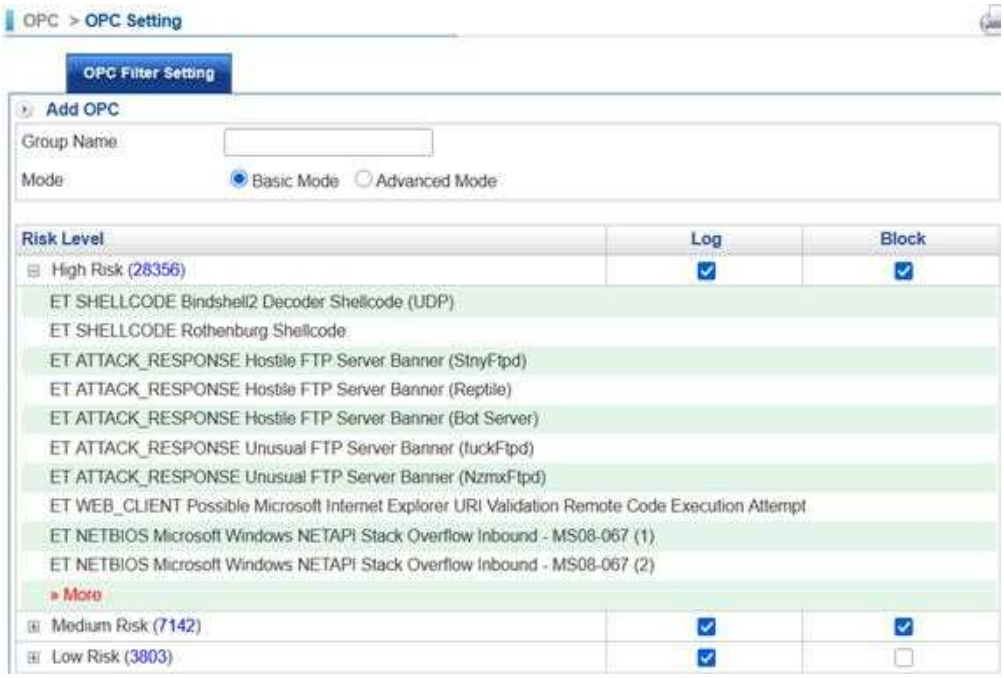


Figure 8-1

Advanced Mode

Signatures are grouped by **attack type**: Virus, Trojan, Exploit, etc. (See Figure 8-2)

Each category and individual signature can be independently configured for Block or Log actions.

- **[Group Name]**: Custom name for the OPC policy (e.g., “High-Risk Block Policy”)
- **[Mode]**: Choose between Basic (risk-based) or Advanced (type-based) modes

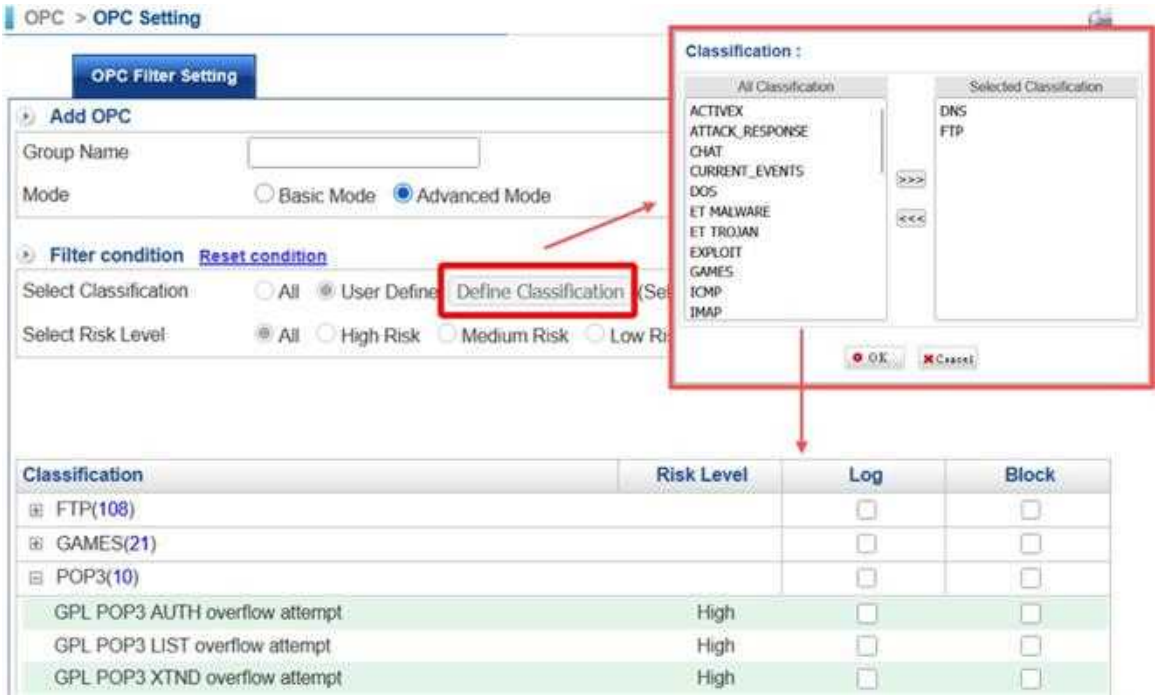

OPC > OPC Setting
OPC Filter Setting
Add OPC
Group Name
Mode
Basic Mode
Advanced Mode
Filter condition
Reset condition
Select Classification
All
User Define
Define Classification
Select Risk Level
All
High Risk
Medium Risk
Low Ri
Classification :
All Classification
ACTIVEX
ATTACK_RESPONSE
CHAT
CURRENT_EVENTS
DOS
ET MALWARE
ET TROJAN
EXPLOIT
GAMES
ICMP
IMAP
Selected Classification
DNS
FTP
>>>
<<<
OK
Cancel
Classification
Risk Level
Log
Block
FTP(108)
GAMES(21)
POP3(10)
GPL POP3 AUTH overflow attempt
High
GPL POP3 LIST overflow attempt
High
GPL POP3 XTND overflow attempt
High

Figure 8-2

8-2. OPC Logs and Event Tracking

Each OPC blocking event is logged for administrator review. By default, the interface displays today's OPC protection records, showing events from 00:00 (midnight) up to the current time. Administrators can also use the OPC Log Search function to view protection records from previous days. (See Figure 8-3)

Each log entry includes the following details: the time of the event, the OPC category, the signature name, source/destination IP address, protocol, source/destination port, the action taken by the 3100-6GT-I, and the associated risk level.

Date	Classification	Event	Source IP Address	Destination IP Address	Protocol	Source Port	Destination Port	Action	Risk Level	Count
2025-07-31 17:18:22	SNMP	GPL SNMP public access udp	192.168.190.15	192.168.43.231	UDP	53741	161	Log	Medium	1
2025-07-31 17:18:21	SNMP	GPL SNMP public access udp	192.168.190.15	192.168.43.231	UDP	53741	161	Log	Medium	1
2025-07-31 17:18:20	SNMP	GPL SNMP public access udp	192.168.190.15	192.168.43.231	UDP	53741	161	Log	Medium	1
2025-07-31 17:18:19	SNMP	GPL SNMP public access udp	192.168.190.15	192.168.43.231	UDP	53741	161	Log	Medium	1
2025-07-31 17:18:18	SNMP	GPL SNMP public access udp	192.168.190.15	192.168.43.230	UDP	47925	161	Log	Medium	1
2025-07-31 17:18:17	SNMP	GPL SNMP public access udp	192.168.190.15	192.168.43.230	UDP	47925	161	Log	Medium	1

Figure 8-3

Chapter 9. WAF

The 3100-6GT-I includes a Web Application Firewall (WAF) that provides advanced protection for public-facing web servers. It blocks common attack methods such as **SQL Injection** and **Cross-site Scripting (XSS)**, preventing attackers from disrupting services or stealing database information.

Web servers use two protocols: **HTTP** and **HTTPS**. WAF functions as a proxy. If the backend web server uses HTTPS, its certificate must be imported into the WAF. Otherwise, users will encounter certificate errors when accessing the site. No additional setup is needed for HTTP.

3 Steps to Enable WAF

WAF setup involves three main steps: configuring policies to forward HTTP/HTTPS traffic and enable WAF, importing certificates (for HTTPS), and enabling WAF settings.

1. **Configure Security Policy**

   In **[Security Policy]** under **[Incoming]** or **[Advance]**, forward HTTP or HTTPS traffic to the internal web server and enable the WAF function. For example, the internal server might be https://192.168.90.90 (HTTPS). (See Figure 9-1)

2. **Website Management**

   Go to **[WAF]** > **[Website Management]**. The 3100-6GT-I will list all servers with WAF enabled. If using HTTPS, import the server's certificate. No configuration is needed for HTTP.

3. **WAF Setting**

   Go to **[WAF]** > **[WAF Setting]** to enable WAF and select the desired **objects** and **policies**.

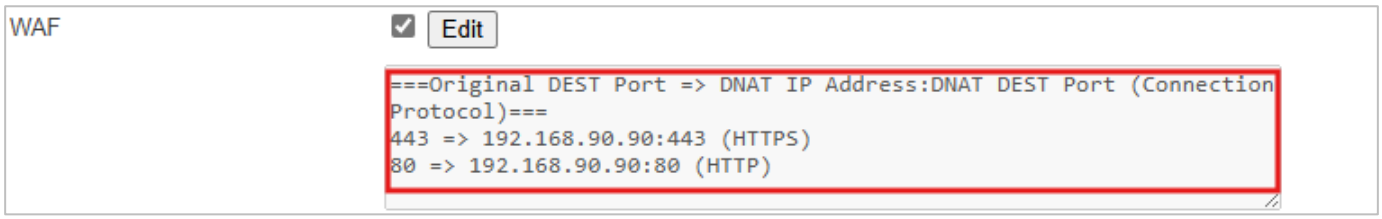


Figure 9-1

9-1. WAF Settings

9-1-1. WAF Setting

The 3100-6GT-I's WAF includes 19 main categories, each with multiple sub-rules. Administrators can configure each rule based on specific needs.

Each rule supports two actions: **[Log]** and **[Block]**.

- **Log**: Records the matching behavior but allows the request through. Useful for auditing and tuning.
- **Block**: Immediately blocks the request, preventing it from reaching the backend web server. (See Figure 9-2)

For initial deployment, it is recommended to enable only **[Log]** to avoid unintended blocks. You can then review the WAF logs to identify which rules were triggered.

Since WAF rules are strict, web applications that don't follow secure coding standards may be blocked. These detections help prevent vulnerabilities that attackers often exploit—WAF serves as a layer of protection for such flaws.

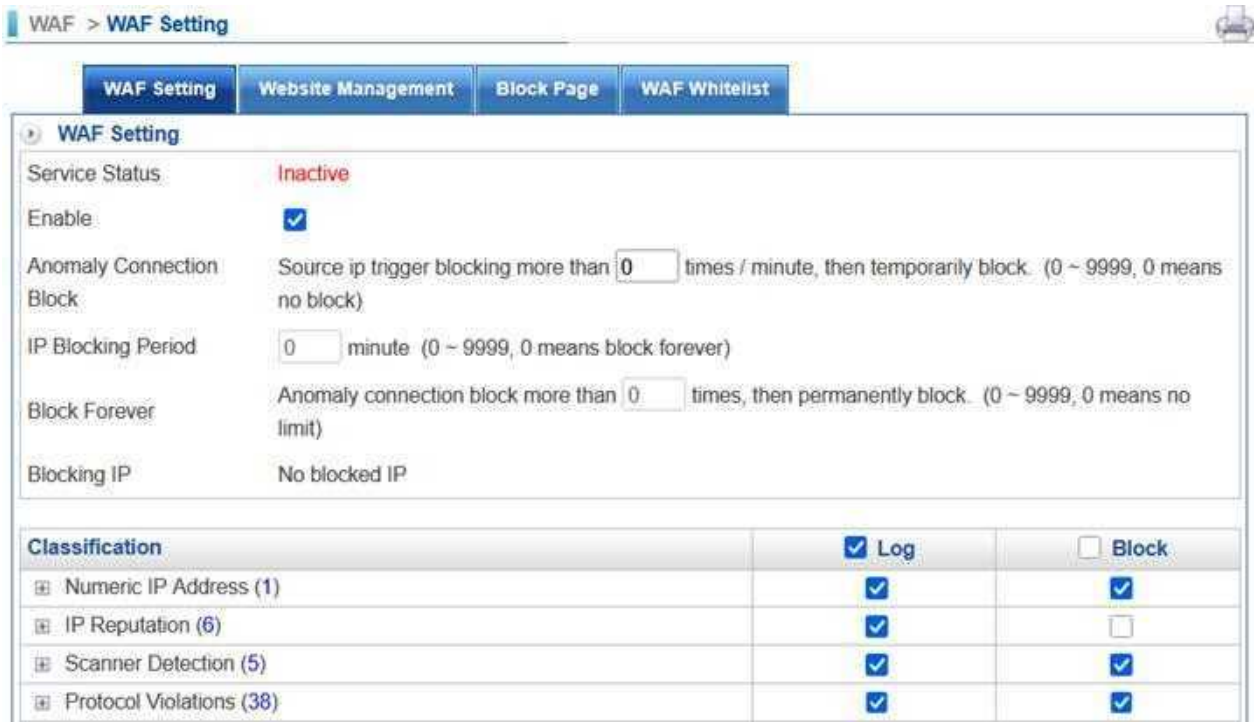


Figure 9-2

- **[Enable]**: Enables the WAF function.
- **[Anomaly Connection Block]**: Temporarily blocks a source IP if it triggers WAF rules more than the defined number of times per minute. Range: 0–9999 (0 = no blocking).
- **[IP Blocking Period]**: Duration (in minutes) before the system unblocks an IP after triggering an anomaly. Range: 0–9999 (0 = never unblock).
- **[Block Forever]**: Permanently blocks a source IP after exceeding the defined number of anomaly blocks. Range: 0–9999 (0 = no permanent block).
- **[Blocking IP]**: Displays currently blocked source IPs. Administrators can unblock individual IPs or clear all.

Classification

There are 19 main categories, each containing several sub-rules. For example, as shown in Figure 9-3, the category **Numeric IP Address (1)** contains a single rule: **"Host header is a numeric IP address"**, which means the incoming request uses an IP address instead of a domain name.

- **[Log/Block]**: Defines how matching traffic is handled—either logged only or actively blocked.

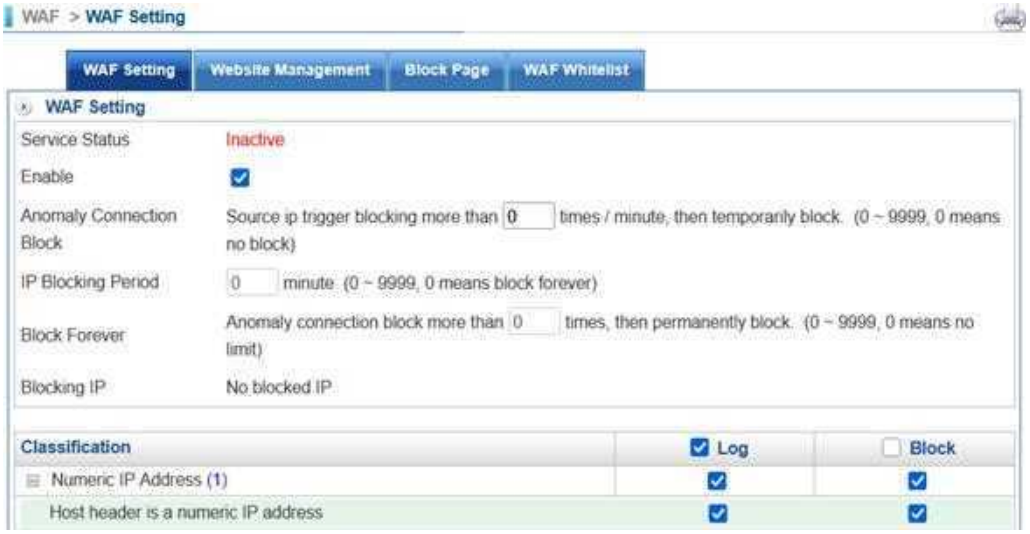


Figure 9-3

9-1-2. Website Management

All web servers with WAF enabled via security policies are listed here. The list is based on the **internal server IPs**, not the external IPs.

For example, two WAF-enabled rules may point to the same backend server:

1. www.def.com (Public IP: 1.1.1.1) → Internal server: 192.168.1.1
2. www.def.com (Public IP: 2.2.2.2) → Internal server: 192.168.1.1

Although two public IPs are used for load balancing, only **192.168.1.1** appears in the website list. (See Figure 9-4)

Figure 9-4

- **[Server IP]**: The actual IP address of the internal web server.
- **[Server Port]**: The server's communication port. Common ports are 80 (HTTP) and 443 (HTTPS), but custom ports like 8080, 8000, or 8443 can also be used.
- **[Protocol]**: The protocol used (HTTP or HTTPS). For HTTPS, you must import the original server certificate into the WAF; otherwise, users will receive browser certificate warnings.
- **[Security]**: Supported TLS versions for WAF protection. Options include TLS 1.0, 1.1, 1.2, and 1.3.
- **[Server Name]**: The name of the web server. If left blank, external requests are forwarded directly. If the backend server supports multiple virtual hosts, enter the actual Virtual Host name to enable SNI identification. This setting can be modified as needed. (See Figure 9-5)

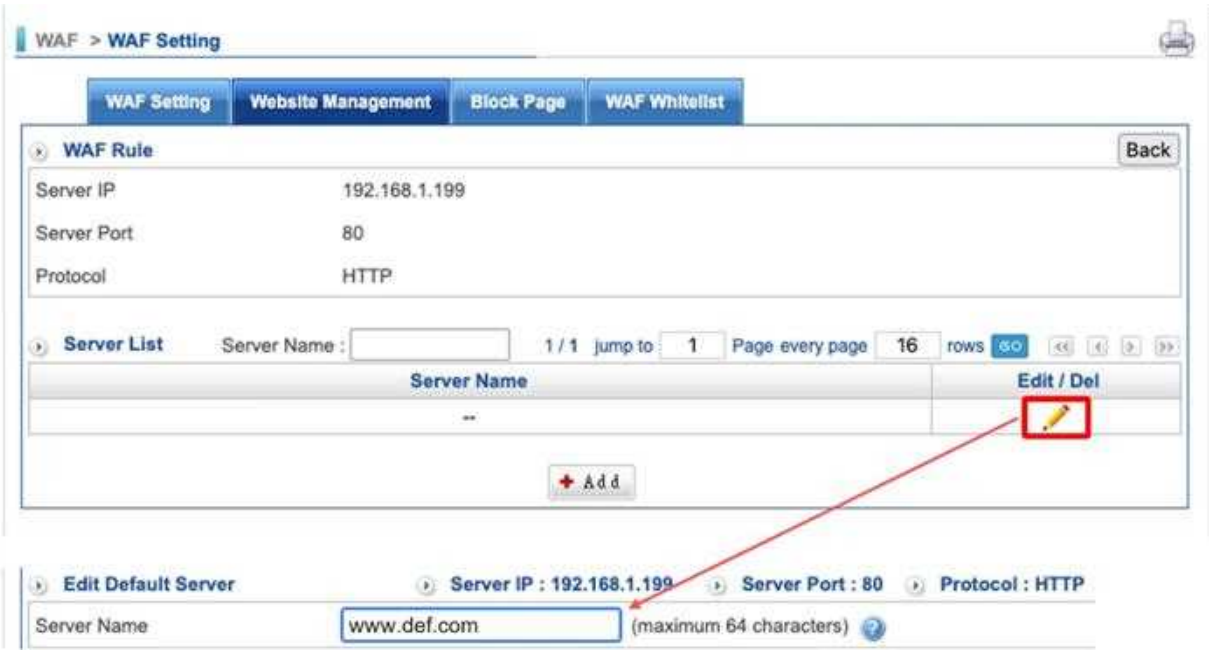


Figure 9-5

- **[Certificate Message]**: For HTTPS, each virtual host must have its certificate imported. Modify settings via the server certificate list. (See Figure 9-6)

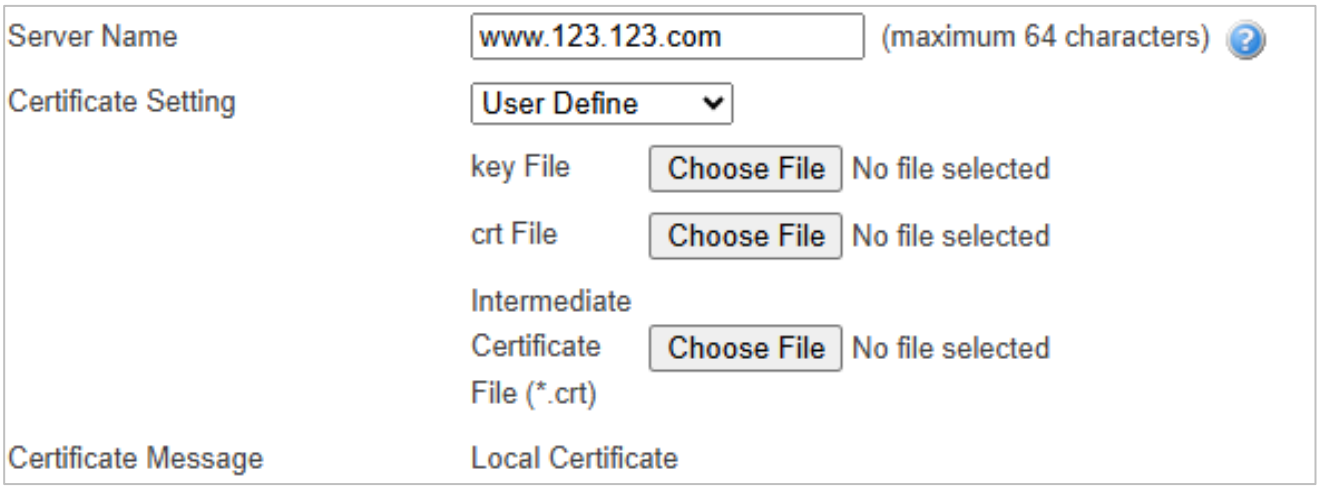


Figure 9-6

- **[Certificate Configuration]**: Certificate sources include **Local Certificate** and **User Define**. **User Define** allows you to import the server's existing certificate by uploading the original **.key** and **.crt** files. **Local Certificate** uses a certificate file generated by the 3100-6GT-I.

9-1-3. Block Page

When WAF is active, multiple backend servers may be involved, each with different content. The block messages shown to users can be customized here.

Default Block Page Setting

The system uses a default block page. Administrators can view it by clicking **[Block Page Setting]** > **[View]**.

For servers requiring custom block pages, go to **[Define Block Page List]**. First, select the server from the list provided. Then, enter a name and the desired block message. Once saved, the custom block page is applied. (See Figure 9-7)

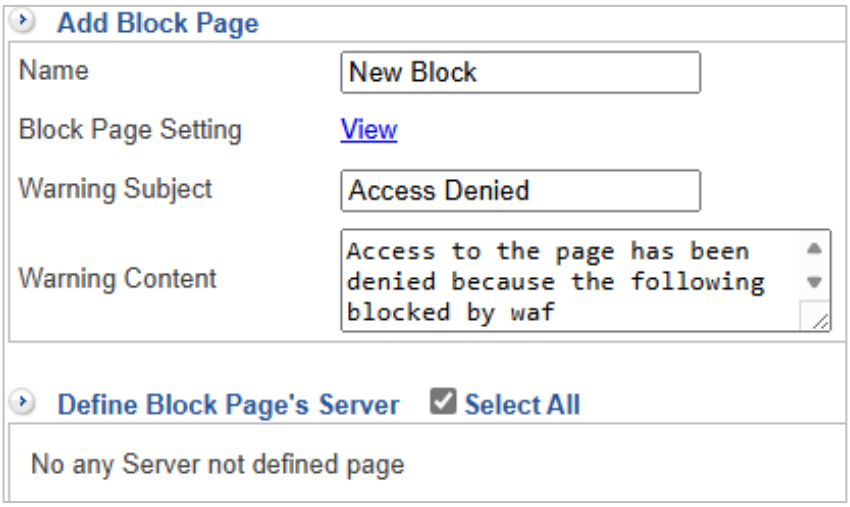


Figure 9-7

9-1-4. WAF Whitelist

Some websites may trigger WAF rules due to the way their code is written. Since modifying the code can be complex, administrators can whitelist specific cases if the triggered rule is low-risk. Whitelisted items will be excluded from WAF inspection. (See Figure 9-8)

- **[Name]**: The name of the whitelist entry.
- **[URL]**: The specific URL that triggered the WAF rule and should be excluded.
- **[Whitelist Item]**: The rule item that was triggered. Once selected, WAF will no longer inspect that rule for the given URL. Administrators can identify false positives in the WAF block log and add them to the whitelist directly from the log.

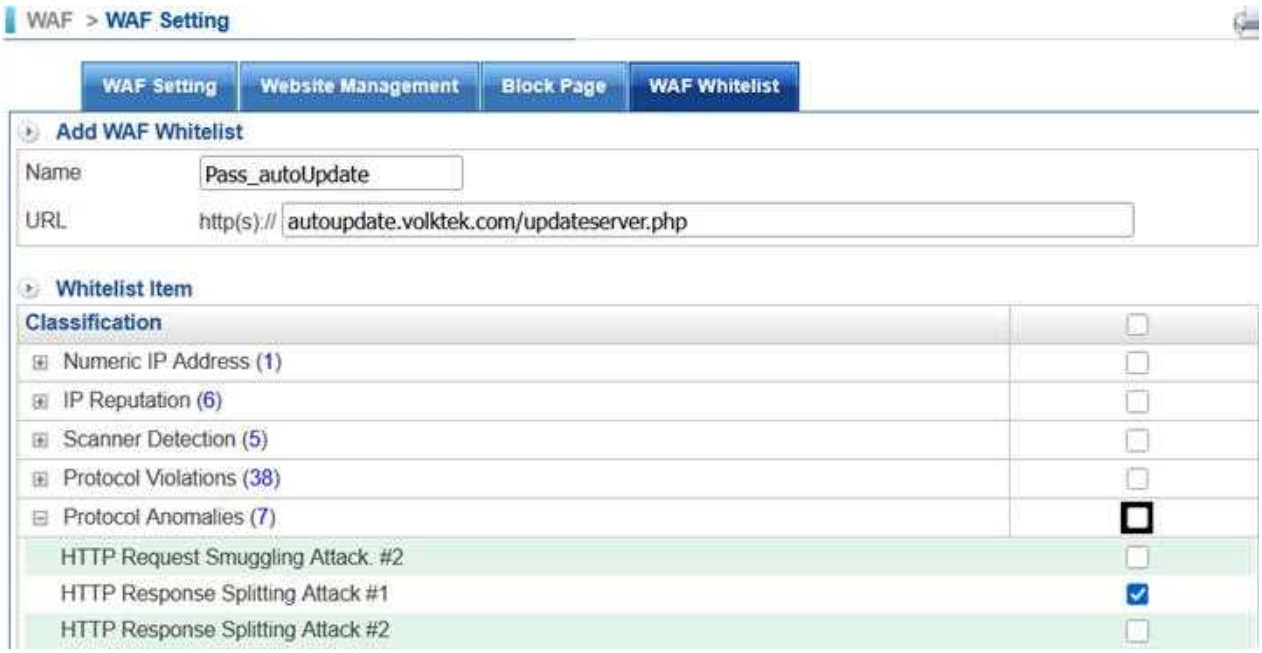
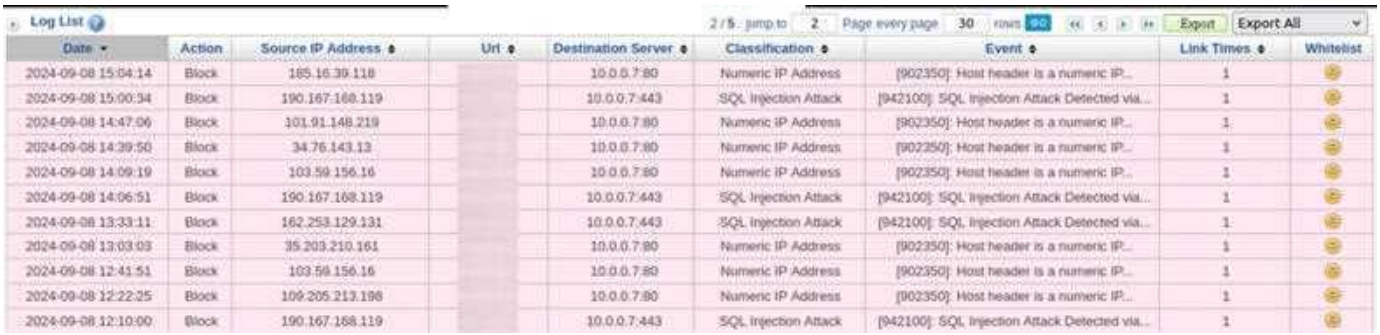


Figure 9-8

9-2. WAF Log

9-2-1. WAF Log

All events triggered by the 3100-6GT-I WAF are listed here. Administrators can use this log to identify the types of attacks being attempted. (See Figure 9-9)


Log List

2 / 5 jump to 2 Page every page 30 rows 90 Export Export All

Date	Action	Source IP Address	Url	Destination Server	Classification	Event	Link Times	Whitelist
2024-09-08 15:04:14	Block	185.16.39.118		10.0.0.7:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1	
2024-09-08 15:00:34	Block	190.167.168.119		10.0.0.7:443	SQL Injection Attack	[942100]: SQL Injection Attack Detected via...	1	
2024-09-08 14:47:06	Block	101.91.148.219		10.0.0.7:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1	
2024-09-08 14:39:50	Block	34.76.143.13		10.0.0.7:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1	
2024-09-08 14:09:19	Block	103.59.156.16		10.0.0.7:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1	
2024-09-08 14:06:51	Block	190.167.168.119		10.0.0.7:443	SQL Injection Attack	[942100]: SQL Injection Attack Detected via...	1	
2024-09-08 13:33:11	Block	162.253.129.131		10.0.0.7:443	SQL Injection Attack	[942100]: SQL Injection Attack Detected via...	1	
2024-09-08 13:03:03	Block	35.203.210.161		10.0.0.7:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1	
2024-09-08 12:41:51	Block	103.59.156.16		10.0.0.7:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1	
2024-09-08 12:22:25	Block	109.205.213.198		10.0.0.7:80	Numeric IP Address	[902350]: Host header is a numeric IP...	1	
2024-09-08 12:10:00	Block	190.167.168.119		10.0.0.7:443	SQL Injection Attack	[942100]: SQL Injection Attack Detected via...	1	

Figure 9-9

- **[Action]**: Two types—**Log** and **Block**. Color-coded: pink for blocked items, white for logged entries.
- **[Source IP Address]**: IP address of the attacker.
- **[URL]**: The targeted URL. This helps identify which web page was attacked. If triggered by non-standard coding, adjustments can be made.
- **[Destination Server]**: The internal server IP where WAF is enabled.
- **[Classification]**: The WAF rule category triggered.
- **[Event]**: The specific sub-rule within the classification that was triggered.
- **[Link Times]**: Number of times the same source IP triggered the rule.
- **[Whitelist]**: If confirmed as a false positive, clicking this will automatically add the rule to the whitelist.

9-2-2. WAF Reject Log

This section lists all source IP addresses that have been blocked by the 3100-6GT-I WAF.

Chapter 10. Mail Security

The 3100-6GT-I can manage all email traffic passing through its interfaces, regardless of whether the mail server is hosted internally or externally.

In this chapter:

- **[Local]** refers to mail servers hosted inside the 3100-6GT-I network. External senders deliver emails via the WAN interface to internal servers.
- **[Remote]** refers to mail servers on the internet. When internal users send emails or receive messages via POP3 over a WAN connection, the 3100-6GT-I can intercept and manage these communications.

The 3100-6GT-I functions as a **mail gateway**, providing the following capabilities for both inbound and outbound mail:

1. **Email Antivirus**: Scans incoming and outgoing emails for viruses.
2. **SMTP Log Search**: Records detailed SMTP communication logs between mail servers to help administrators identify issues with email delivery or reception.

A typical application scenario is shown in Figure 10-1.

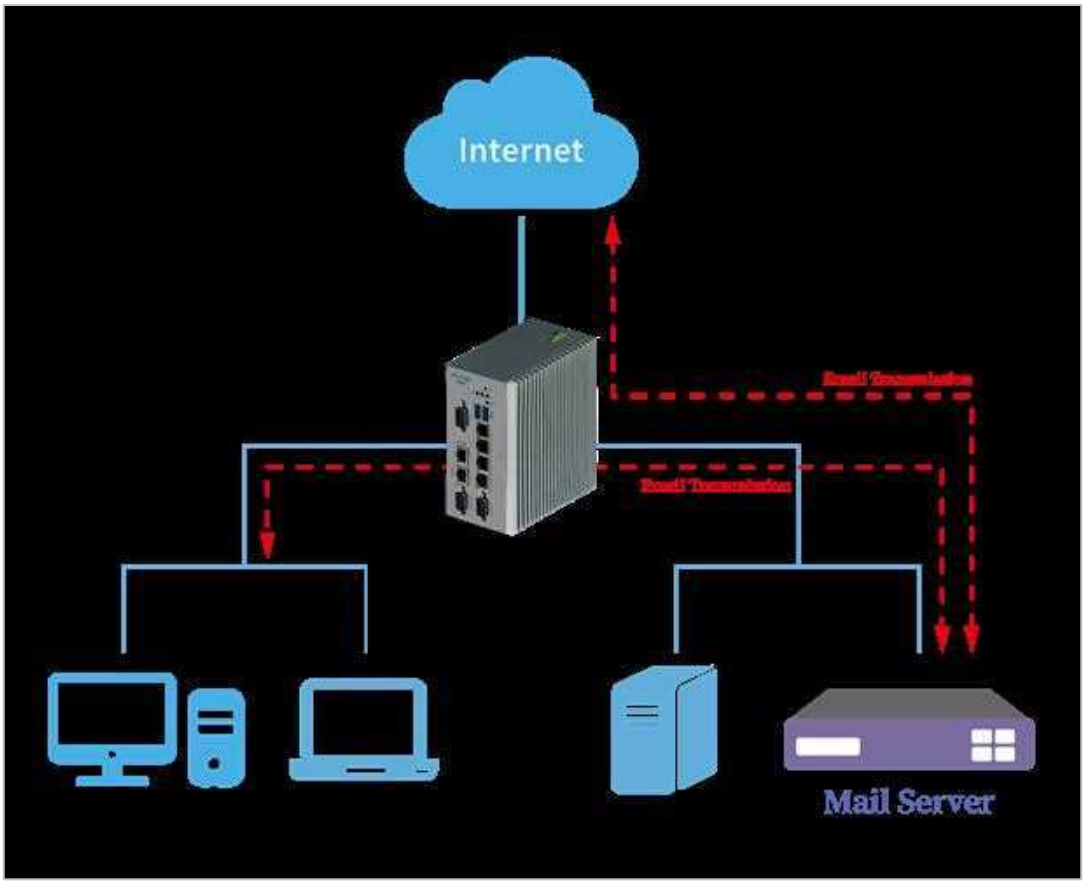


Figure 10-1

10-1. Filter & Log

The 3100-6GT-I allows administrators to enable **SMTP inbound scanning**, **SMTP outbound scanning**, and **inbound mail scanning**. As a mail gateway, it does not have its own mail user accounts and must verify them with the backend mail server.

Acting as a proxy, the 3100-6GT-I intercepts all mail, applies antivirus and logging, then forwards it to the original mail server, filling gaps in its native functions.

It handles three main flows:

1. External → internal mail server (inbound sending)
2. Internal → external mail server (outbound sending)
3. Internal → external mail server (retrieving mail)

Each flow can be configured independently. (Figure 10-2)

Incoming Mail Anti-Virus

- **[Function]**: Enables anti-virus scanning for emails sent from external sources to the local mail server.

Outgoing Mail Anti-Virus

- **[Function]**: Enables anti-virus scanning for emails sent from the local mail server to external servers.

Retrieve Mail Anti-Virus

- **[Function]**: Enables anti-virus scanning for retrieving emails from external servers to the local server.
  [Enable POP3s]: When enabled, anti-virus scanning applies when users connect via POP3 (Port 110) or POP3s (Port 995).

SMTP Log Setting

The 3100-6GT-I can record detailed SMTP session logs for each email, including server-to-server communication. When troubleshooting delivery failures, SMTP logs provide detailed records. Administrators can choose to enable, partially enable, or disable this function.

- **[Incoming]**: Three options — *Disable*, *Accept*, *All*. Default is *Disable*. With *Accept*, only SMTP sessions permitted for communication are logged, while blocked sessions are not, reducing unnecessary logs.
- **[Outgoing]**: Three options — *Disable*, *Fail*, *All*. Default is *Disable*. With *Fail*, only failed SMTP session attempts are logged; successful deliveries are not, minimizing unnecessary records.
- **[Log Type]**: Can be set to *Simple* or *Detailed*. Use *Detailed* when troubleshooting mail delivery issues.

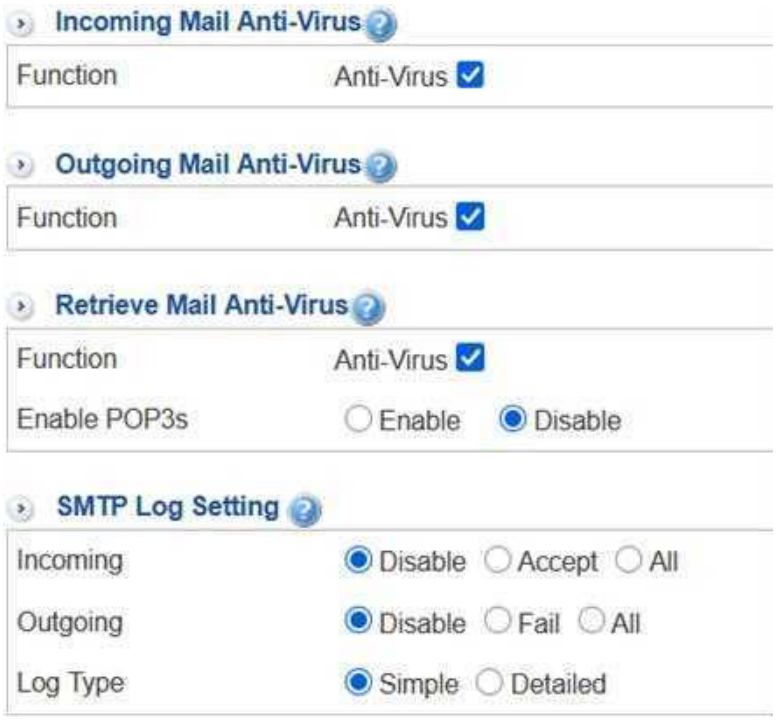


Figure 10-2

Mail Record Setting

When the 3100-6GT-I performs mail logging, emails exceeding the configured file size limit will bypass antivirus scanning. (See Figure 10-3)

- **[Retrieve Mail]**: If an email exceeds the set size, attachments will not be backed up in the log. The default threshold is **640 KB**, meaning files larger than 640 KB will not undergo virus scanning.

Source IP Replaced by Firewall IP

This function applies only when external mail servers send emails to internal (local) mail servers. Acting as a mail gateway, the 3100-6GT-I proxies emails for virus scanning and spam filtering before forwarding them to the original mail server. At this point, the source IP address used can be either **the 3100-6GT-I interface IP** or the **original sending server's IP**.

- **[Incoming Mail (Send)]**: *Enable* uses the 3100-6GT-I interface IP as the source IP when forwarding mail. *Disable* uses the original sending mail server's IP as the source IP.

Release to Carry the Subject

This function applies to the mail backup feature. When a quarantined email is released by an administrator, the system can optionally insert text into the subject line to differentiate it from the original email, so both administrators and users know it was released.

- **[Join Subject]**: *Enable*: Adds a predefined string to the released email subject. Default is *Disable*.
- **[Subject]**: Allows custom text or a timestamp. For example, entering "$Y-$m-$d $H:$i:$s" inserts the release timestamp (e.g., 2025-06-30 12:12:30) at the beginning of the subject line.


Mail Record Setting
Mail File Backup Type
Processed Mail
Original Mail
Mail File Backup
Mail file larger than
0
MB does not backup file attachment (0 means no limit)
Retrieve Mail
Mail file larger than
640
KB do not scan Anti-Virus and Anti-Spam , only check black and whitelist
Source IP replaced by FireWall IP
Incoming Mail(Send)
Enable
Disable
Release to carry the subject
Join Subject
Enable
Disable
Subject
$Y-$m-$d $H:$i:$s
ex: $Y-$m-$d $H:$i:$s
Connection Setting of Spam List and Audit Mail
IP or Domain
192.168.186.172
(Ex : FireWall IP Address or Domain)
Port
3444
Change
(Note : To specify connecting protocol, Can not be the same as HTTPS PORT)

Figure 10-3

10-2. Anti-Virus

Email viruses are a persistent threat. While IT staff can often recognize suspicious content—like strange images, hyperlinks, or .exe files—most users cannot, and only realize the danger after clicking. If endpoint antivirus fails, the issue escalates to IT.

The 3100-6GT-I reduces this risk by scanning incoming emails using its built-in ClamAV engine. Infected messages are quarantined or deleted before reaching users.

This feature consumes additional system resources (CPU, RAM). If a separate mail gateway with antivirus is already in place, this function can be disabled.

Quarantined emails appear in the **[Quarantined Mail]** list, showing sender, recipient, time, subject, infected file, and virus type. Admins can search for specific emails using filters.

10-2-1. Anti-Virus Settings

The 3100-6GT-I uses its built-in virus engine to scan incoming emails. If a virus is detected, the system can rename the attached file and modify the email subject to warn the recipient.

Basic Setting

- **[Sandstorm]**: Depends on whether Sandstorm is enabled in section 6-5. Sandstorm.
- **[Anti-Virus]**: Enables email antivirus scanning.
- **[Virus Engine]**: Select whether to enable the ClamAV virus scanning engine. If the Kaspersky engine is not enabled in section 6-4. Virus Engine, only ClamAV will be available here.
- **[Exclude files ending in]**: Lists file types (e.g., jpg, gif) to skip during scanning, improving performance. One file extension per line.
- **[Max. Scan Size (KB)]**: Files exceeding this size will not be scanned. (See Figure 10-4)

Actions Taken on Infected Mail

- **[Move to the quarantine]**: Quarantines infected emails. If disabled, the user receives a virus notification instead.
- **[Rename file extensions]**: Renames infected attachments (e.g., to “virus”) to prevent accidental opening.
- **[Insert an email subject]**: Changes the subject line (e.g., “Infected Mail”) to alert the recipient.

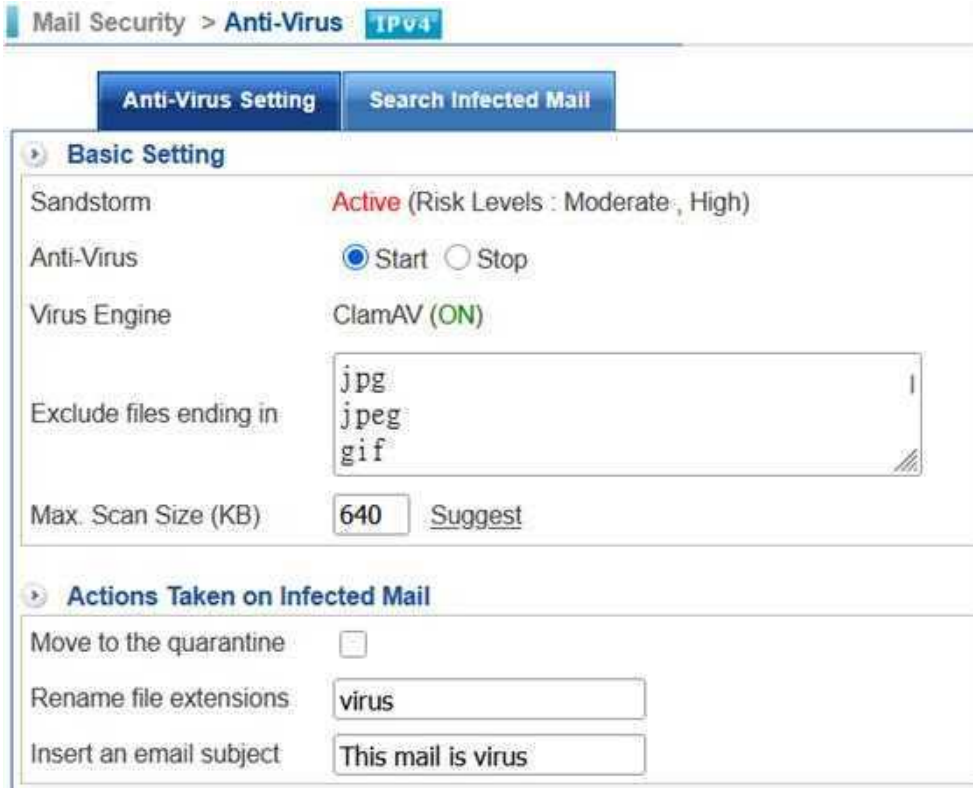


Figure 10-4

10-2-2. Quarantined Mail

Quarantined virus emails can be searched using the following criteria:

- **[Date]**: The date the infected email was quarantined. A specific date range can be set.
- **[Sender Account]**: The account that sent the virus email.
- **[Sender IP Address]**: The IP address of the sender.
- **[Recipient Account]**: The recipient of the virus email.
- **[Subject]**: The subject line of the infected email.
- **[Size Range (KB)]**: The file size of the infected email.

10-3. Mail Log

The 3100-6GT-I logs all emails sent or received through the device. Only the subject headers are recorded, allowing administrators to quickly search historical records. All logged emails are listed here for easy tracking of email activity.

10-3-1. Today Mail

The 3100-6GT-I displays a list of all emails sent or received today, sorted by time, for administrator review. (See Figure 10-5)

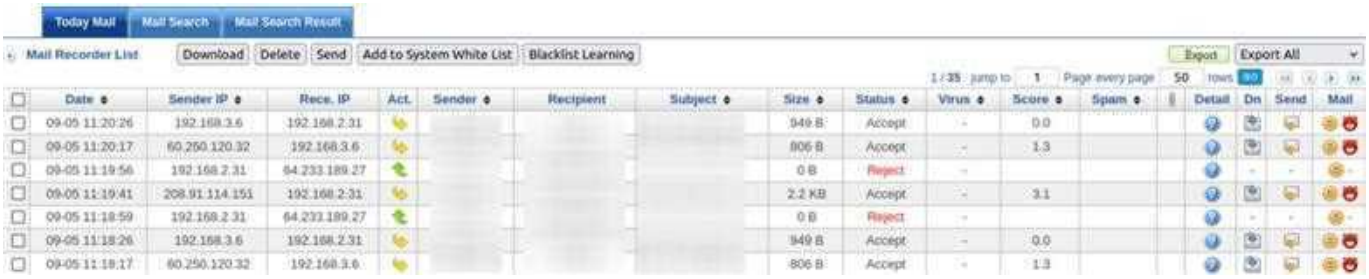


Figure 10-5

- **[Date]**: The date and time the email passed through the 3100-6GT-I.
- **[Sender IP]**: IP address of the sender.
- **[Recipient IP]**: IP address of the recipient.
- **[Act.]**: Direction of email flow, with three types:
  - ■ : External to internal mail server (**Local**)
- **[Sender]**: Sender’s email account.
- **[Recipient]**: Recipient’s email account.
- **[Subject]**: Subject of the email.
- **[Size]**: Email size.
- **[Status]**: Indicates whether the email was delivered successfully or rejected by the recipient mail server. Possible statuses include **Sent (Outgoing Mail)**, **Reject**, **Accept (Incoming Mail)**, **Fail**, and **TLS**.
- **[Virus]**: Shows whether the email contained a virus.
- **[Detail]**: Displays detailed information on how the 3100-6GT-I processed the email, including spam filtering, virus scanning, and audit filtering. (See Figure 10-6)

Mail

Date	2024-05-10 10:34:05
Sender	allen3@
Subject	This is virus test
Size (bytes)	322917
Virus	
SPAM	-
Mail Backup	✔
Delivery status	Reject
Response to the message	550 Content Rejected

Attachment file

Filename	File size(byte)	Virus
Order4500318042.xls	235008	[Sandstorm] CVE-2017-0199

Quaratine zone

Separated mail type	Separate zone of virus letters
Reserve quaratined file	✔
Notified the administrator	-

Receiver

Filter(Cc copy)	Receiver	Status	The user notification list	Action	Actors	Date of dealing
	allen5@	Separate by virus				

Figure 10-6

10-3-2. Mail Search

The [Mail Search] feature allows administrators to search all emails processed by the 3100-6GT-I, including both outbound and inbound traffic. (See Figure 10-7)

- **[Date]**: Specify the date range to search.
- **[Source]**: Select whether to search local records or data backed up to external storage.
- **[Sender IP Address]**: IP address of the sender.
- **[Recipient IP Address]**: IP address of the recipient.
- **[Action]**: Choose the direction—internal to external (send), internal to external (receive), or external to internal.
- **[Sender Account]**: Email address of the sender.
- **[Mail size (KB)]**: Define a file size range for the email.
- **[Recipient Account]**: Email address of the recipient.
- **[Virus Mail]**: Indicates whether the email was identified as containing a virus.
- **[Status]**: Delivery result—options include **Sent (Outgoing Mail)**, **Reject**, **Accept (Incoming Mail)**, **Fail**, and **TLS**.
- **[Subject]**: Keywords in the email subject line.

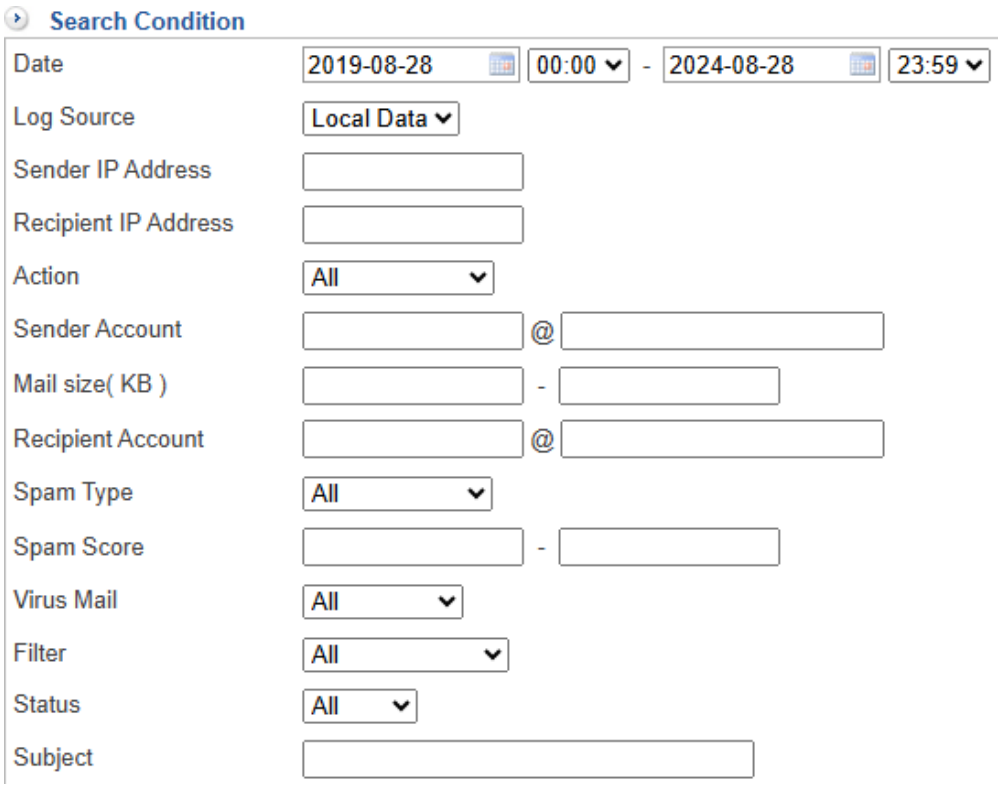


Figure 10-7

10-4. SMTP Log

The [SMTP Log] function allows administrators to review detailed SMTP communication records for each email. This helps diagnose delivery failures. (See Figure 10-8)

- **[Date]**: Specify the date range for the query.
- **[Sender Account]**: Email address of the sender.
- **[Mail Size (KB)]**: Define a file size range for the email.
- **[Recipient Account]**: Email address of the recipient.
- **[Status]**: Delivery result—options include **Sent (Outgoing Mail)**, **Reject**, **Accept (Incoming Mail)**, **Fail**, and **TLS**.

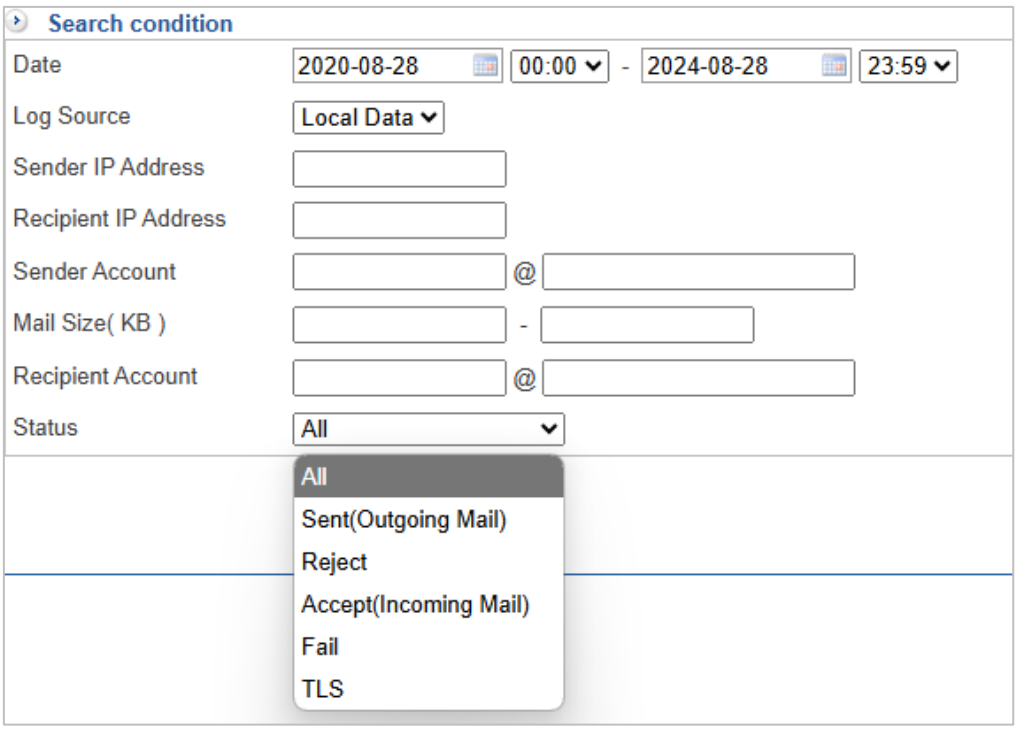


Figure 10-8

Simple SMTP Log

By default, the 3100-6GT-I uses the **simple SMTP log** format. After a search, the system displays a list showing the reason for any failed email delivery. This log type only shows the final cause of failure. (See Figure 10-9)

- **[Message]**: Displays the reason why the email failed to send.

Detailed SMTP Log

To enable full logging, go to **[Mail Security]** > **[Filter & Log]** > **[SMTP Log Setting]** > **[Log Type]**, and select **"Detailed"**.

When enabled, the **[Detail]** column provides clickable access to complete SMTP communication logs for each email. (See Figure 10-10)


Smtp connection detailed records
Date
2024-09-05 11:24:18
Sender
Recipient
Size (bytes)
806
Delivery status
Accept
Response to the message
250 OK
Communication process
(24:18) > 220 (SMTP PROXY)
(24:18) < EHLO apcEFAA87
(24:18) > 250
(24:18) > 250-SIZE 699050666
(24:18) > 250-AUTH LOGIN CRAM-MD5
(24:18) > 250-8BITMIME
(24:18) > 250-DSN
(24:18) > 250 OK
(24:18) < AUTH LOGIN

Figure 10-10

Chapter 11. Content Record

The 3100-6GT-I logs all web access records, including both HTTP and HTTPS traffic. Even virus scan activities are recorded.

11-1. WEB Virus Record

11-1-1. Today WEB Virus

The 3100-6GT-I automatically records web access data, including timestamps and URLs. (See Figure 11-1)

Figure 11-1

- **[No.]**: Listed by total traffic, combining both HTTP and HTTPS.
- **[Computer Name]**: The name of the device accessing the web.
- **[IP Address]**: IP address of the device.
- **[MAC Address]**: MAC address of the device.
- **[Authentication Users]**: If both web logging and web authentication are enabled in the policy, the authenticated username is shown here.
- **[Flow]**: Data volume of HTTP traffic.
- **[Export]**: Export HTTP traffic records.

  ➤ Clicking the **[IP Address]** displays detailed web access logs for that IP, sorted by number of records. It shows the start and end time of visits to each website.

- **[Website]**: Name of the accessed website. Clicking the **[Website]** link opens a list of all recorded valid URLs for that site. (See Figure 11-2)


Computer Name 192.168.2.28 IP Address 192.168.2.28 MAC Address 34:95:db:2c:5a:51 Export Export All
Auth Users ALL 1 / 1 jump to 1 Page every page 30 rows GO

Time	Auth Users	Website
2024-08-29 09:51:30	johnny	[SSL] azwcus1-client-s.gateway.messenger.live.com
2024-08-29 09:51:05	johnny	[SSL] azwcus1-client-s.gateway.messenger.live.com
2024-08-29 09:50:14	johnny	[SSL] outlook.live.com
2024-08-29 09:49:25	johnny	[SSL] azwcus1-client-s.gateway.messenger.live.com
2024-08-29 09:47:48	johnny	[SSL] login.live.com
2024-08-29 09:47:47	johnny	[SSL] login.live.com
2024-08-29 09:47:26	johnny	[SSL] azwcus1-client-s.gateway.messenger.live.com
2024-08-29 09:47:25	johnny	[SSL] azwcus1-client-s.gateway.messenger.live.com
2024-08-29 09:46:35	johnny	EyeCloud
2024-08-29 09:46:25	johnny	International Business, World News & Global Stock Market Analysis
2024-08-29 09:46:10	johnny	MantisBT

Figure 11-2

- **[Time]**: The timestamp when the website was accessed.
- **[Authentication Users]**: The authenticated account used by the IP during web access.
- **[Website]**: The actual URL visited. Clicking the link opens a new window showing the webpage viewed at that time.

- **[Count]**: Total number of valid URLs recorded for the website.
- **[Start Time]**: The time the website visit started.
- **[End Time]**: The time the website visit ended.

11-1-2. WEB Virus Search

Web virus records stored in the 3100-6GT-I can be searched based on criteria such as date, IP address etc. (See Figure 11-3)

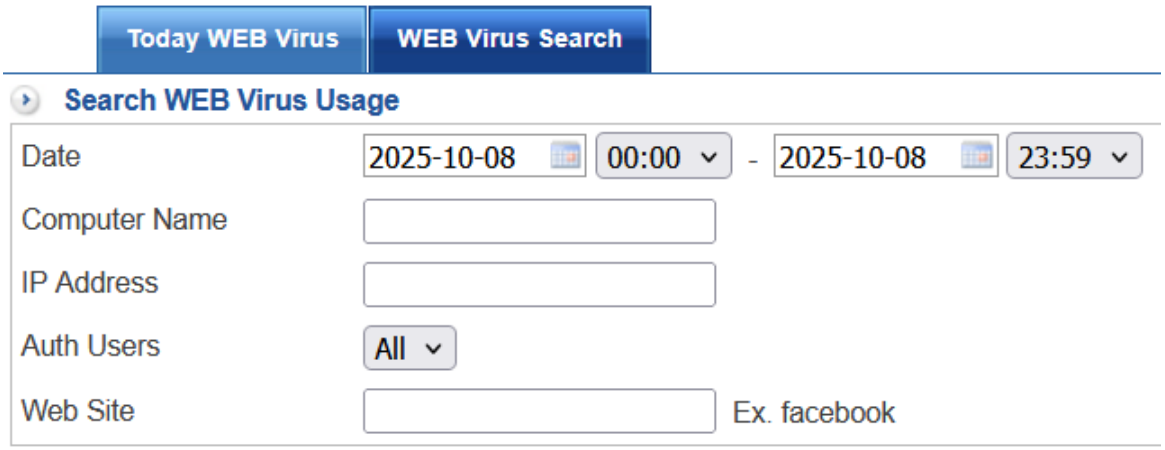


Figure 11-3

The 3100-6GT-I can scan for HTTP/HTTPS-based web viruses using the built-in **ClamAV** engine or the optional **Kaspersky** engine. Any web pages found to be infected or suspicious are filtered out, and a list of detected threats is displayed here. (See Figure 11-4)

Time	Computer Name	IP Address	Auth Users	Website	Anti-virus
2024-12-23 14:53:07	Olivia	192.168.190.116		http://kali.cs.nycu.edu.tw/kali/pool/main/c/crackmapexec/crac	stream: HackTool.Win64.HandleKatz.c FOUND
2024-12-23 14:52:43	Olivia	192.168.190.116		http://mirror.twds.com.tw/kali/pool/main/e/ettercap/ettercap-c	stream:DoS.Linux.Agent.c FOUND
2024-12-23 14:51:30	Olivia	192.168.190.116		http://mirror.twds.com.tw/kali/pool/main/a/aircrack-ng/aircrack	stream:HackTool.Linux.Aircrak.a FOUND

Figure 11-4

Chapter 12. VPN

The 3100-6GT-I supports secure Virtual Private Network (VPN) connections for enterprise sites and remote users, enabling encrypted data transfers over the Internet with high confidentiality and performance.

It supports four VPN types: **IPSec**, **PPTP**, **L2TP**, and **SSL VPN**, each designed for different use cases. IPSec focuses on tunnel-based connections (e.g., Site-to-Site), while PPTP, L2TP, and SSL VPNs allow external users to securely access internal resources via the Internet.

IP Tunnel is also a form of VPN and is treated as a virtual interface based on tunnel configurations.

VPN Types Overview:

1. **IPSec VPN Tunnel**: System administrators can utilize the IPSec protocol to establish a Site-to-Site VPN tunnel, and the communication data on both sides of the channel will be encrypted with DES, 3DES, AES, so that even if others intercept the packets of the channel, they will not be able to decrypt the transmission.

2. **PPTP** & **L2TP**: The administrator can make PPTP or L2TP dial-in accounts here, so that external users can use the resources within 3100-6GT-I.

3. **SSL VPN**: Administrators can set up SSL VPN dial-in accounts here so that the external users can use 3100-6GT-I internal resources.

> To establish a VPN, it is necessary to establish a Tunnel in the IPSec VPN or an account in the PPTP/L2TP/SSL VPN server.
>
> Otherwise, to manage these outlets, the rules of IPSec VPN are referred to 4-2. IPSec Policy to build management regulation. PPTP, L2TP and SSL VPN are referred to 4-1. Security Policy.

12-1. IPSec Tunnel

12-1-1. IPSec Tunnel

To establish an IPSec VPN tunnel, the same settings are required on both ends for a successful connection. The information required for each connection is described below. Under the IPSec VPN tunnel list, click the “Add” button: (See Figure 12-1)

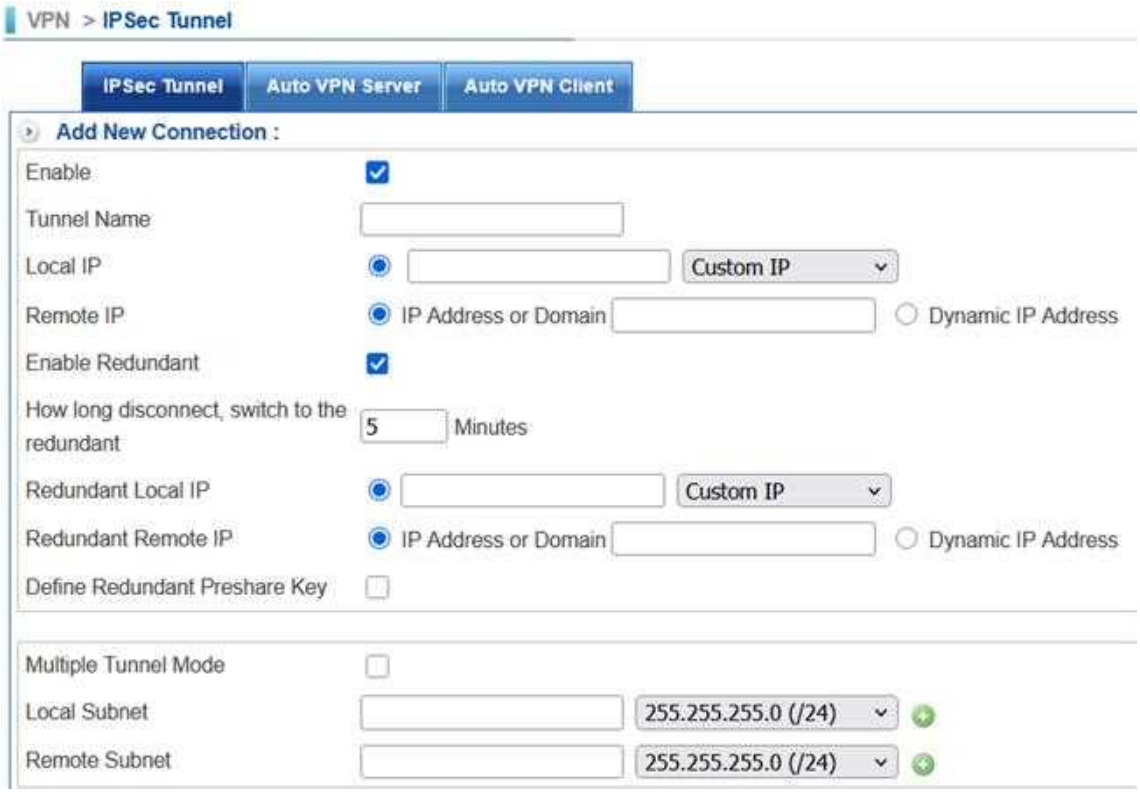


Figure 12-1

- **[Enable]**: Shall we proceed with the activation of this IPSec VPN tunnel.
- **[Tunnel Name]**: It could be any Chinese or English word, easily to be recognized by administrator.
- **[Local IP]**: Which IP Address or domain would accept the packet of IPSec VPN Tunnel, usually referring to the IP Address from extranet.
- **[Remote IP]**: The IP Address or domain name of remote IPSec VPN Tunnel.

  If the remote endpoints’ information is unknown, use dynamic IP addresses. Additionally, when multiple IPSec VPN tunnels have dynamic external IP addresses, ensure that their Preshare keys are the same.
- **[Enable Redundant]**: Shall it enable the service of back-up, when this IPSec VPN Tunnel disconnected, the system will automatically enable the back-up one.
- **[How long disconnect, switch to the redundant]**: After how long the primary IPSec VPN Tunnel should be disconnected before switching to the backup route. The default value is 5 minutes.
- **[Redundant Local IP]**: Which WAN IP Address or domain would be the back-up route, accepting the packet of IPSec VPN Tunnel.
- **[Redundant Remote IP]**: The IP address or domain name of the remote IPSec VPN Tunnel for the backup route. If this information is not known, use a dynamic IP address.
- **[Define Redundant Preshare Key]**: The encryption of Preshare Key for the backup route.

Since the backup route establishes a new IPSec tunnel to replace the original one, this key must match the setting on the remote device as well.

- **[Multiple Tunnel Mode]**: Diverting data among 2 or more IPSec VPN channels to achieve a mechanism similar to load balancing. Below are the settings for both enabling and disabling this feature.

IPSec VPN Connected Subnets

IPSec VPN tunnels typically connect two different internal subnets, often in continuous ranges—for example, **192.168.1.0/24** to **192.168.2.0/24**. If either side includes **non-contiguous subnets**, click the "+" icon to add additional subnets for the connection.

For instance, if Site A includes **192.168.1.0/24** and **172.16.1.0/24**, and Site B includes **192.168.2.0/24** and **172.16.2.0/24**, all subnets can be connected through the same IPSec VPN tunnel. (See Figure 12-2)

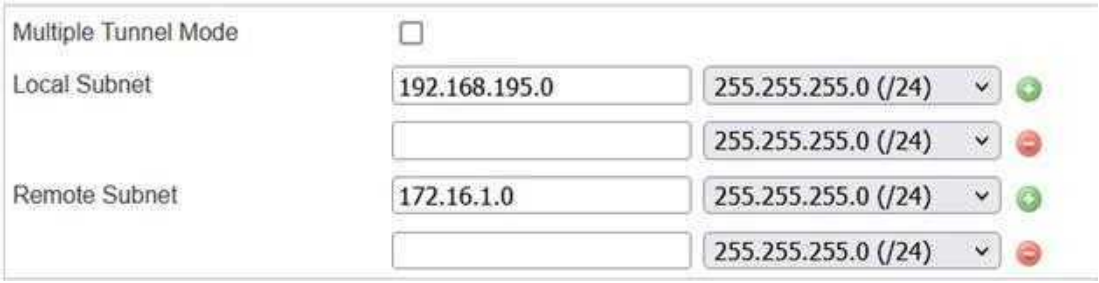


Figure 12-2

- **[Multiple Tunnel Mode]**: Enables multi-tunnel mode.
- **[Local Subnet]**: Specifies the local subnet to be connected via the IPSec VPN tunnel (e.g., 192.168.1.0/24). Click the "+" icon to add more subnets.
- **[Remote Subnet]**: Specifies the remote subnet at the other end of the IPSec VPN tunnel (e.g., 192.168.61.0/24). Click the "+" icon to add additional subnets.

IPSec VPN Multiple Tunnels

Entering the tunnel ID of both sides to enable Multiple Tunnel Mode, the general tunnel ID format involves prefixing the external network IP address with "@", for instance: "@1.1.1.1" or "@vpn.dyndns.org".

Therefore, its operational scenario mostly involves both ends having fixed IPv4 addresses or utilizing dynamic domain names. This setup enables the identification of the remote IP address or domain name.

In multi-channel mode, adding two non-adjacent IP segments is available. Click the "+" icon to add another segment. (See Figure 12-3)

Figure 12-3

- **[Local IP]**: The external network IP address of the local end utilizing the IPSec VPN tunnel, prefixed with "@" symbol, for instance: "@1.1.1.1".
- **[Remote IP]**: The external network IP address of the remote end utilizing the IPSec VPN tunnel, prefixed with "@" symbol, for instance: "@1.1.1.1".

IPSec Tunnel Encryption Settings

There are two configuration sections: IKE (Phase 1) and IPSec Settings (Phase 2). (See Figure 12-4)

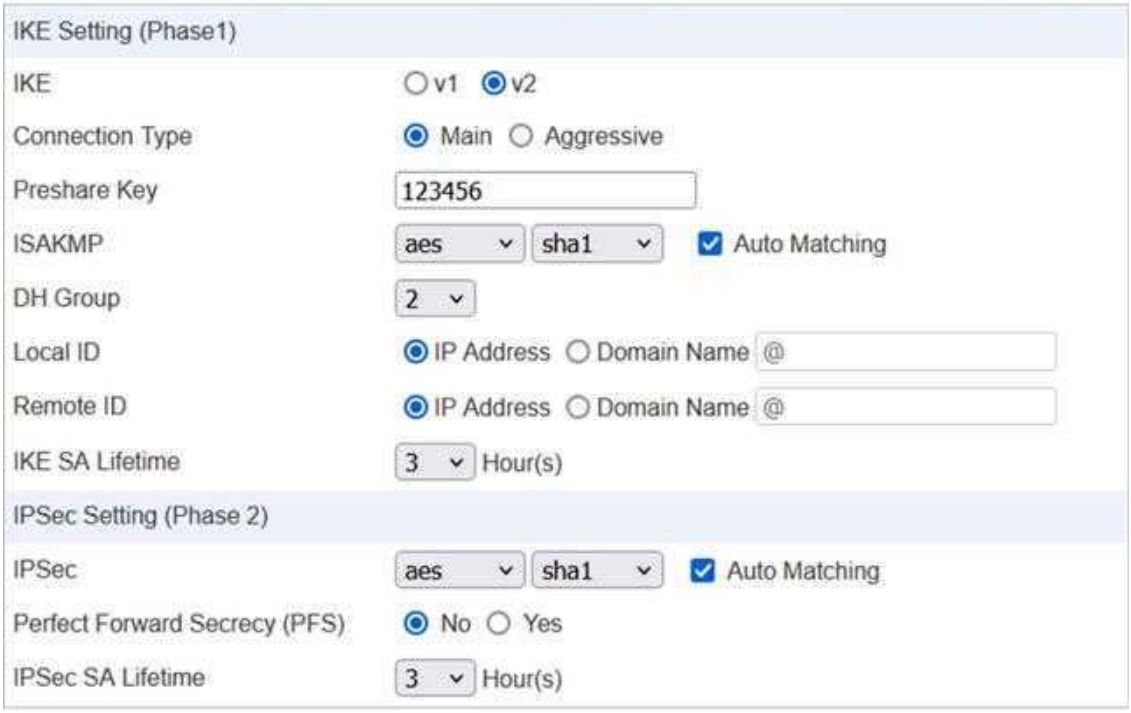


Figure 12-4

1. IKE Setting (Phase 1)

- **[IKE]**: Choosing V1 or V2, IKE V2 is the new protocol. It's necessary to pay attention before setting that both sides of IKE should be the same.
- **[Connection Type]**: Choosing main mode or aggressive mode, usually choosing main mode. In the aggressive mode, all the VPN Tunnel use one Preshare Key commonly.
- **[Preshare Key]**: The key used for IPSec encryption while establishing connections between both sides of the IPSec VPN tunnel.
- **[ISAKMP]**: "IP Security Association Key Management Protocol (ISAKMP)" provides an encryption logically for two equipments to establish SA.

Description of SA

Security Association (SA) is used to encrypt connections between two computers, specifying which algorithms and key lengths or actual encryption keys to use.

There is not just one SA connection way: starting from the ISAKMP SA for two computers, it is essential to specify which encryption algorithm to use (DES, triple DES, AES), and which packet authentication method (MD5 or SHA1)

DES/3DES:

3DES (Triple Data Encryption Standard) offers stronger encryption than DES, using a 168-bit key instead of DES's 56-bit key.

AES:

Advanced Encryption Standard (AES) is a more rigorous encryption standard compared to DES. DES encryption key length is 56 bits, while AES encryption key lengths range from 128 bits, 192 bits, to 256 bits.

Most current INTEL CPUs support AES hardware encryption and decryption, so under equivalent CPU conditions, AES is faster than 3DES.

MD5:

One-way string hashing algorithm, which takes any length string and computes a 128-bit hash using the MD5 hashing algorithm.

SHA:

It's an algorithm used for generating message digests or hashes. The original SHA algorithm has been replaced by the improved SHA1 algorithm, which can compute a 160-bit hash.

- **[DH Group]**: Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process.
- **[Local ID]**: The input field for this ID won't be displayed, if enabling the "multiple tunnels mode". By default, the local IP address will be automatically used as the ID, but administrators can also input a domain name as the local ID.

  The system will automatically prepend "@" to the front before sending it to the remote end, for example: "@1.1.1.1" or "@ghi.com".

  When configuring, it's essential to ensure that the data on both sides are symmetrically matched.
- **[Remote ID]**: The input field for this ID won't be displayed, if enabling the "multiple tunnels mode". By default, the remote IP address will be automatically used as the ID, but admin can also input a domain name as the remote ID. The system will automatically remove "@" to the front before sending it to the remote end, considering as the IP from remote to local, for example: @2.2.2.2 or @def.com

  When configuring, it's essential to ensure that the data on both sides are symmetrically matched.
- **[IKE SA Lifetime]**: According to ISAKMP to calculate the expiration date of SA, the system will automatically produce another SA to replace the previous one while proceeding with the setting timing. The default time is 3 hours, with the setting range between 1 to 24 hours.

2. IPSec Setting (Phase 2)

- **[IPSec Algorithm]**: Specify which encryption algorithm to use (DES, Triple DES, AES) and which packet authentication method (MD5 or SHA1).
- **[Perfect Forward Secrecy (PFS)]**: Ensuring that even if the private key is compromised, historical communications remain secure. This feature provides forward secrecy, guaranteeing security even in the event of a proactive attack on the system.
- **[Lifetime of IPSec SA]**: According to IPSec Algorithm to calculate the expiration date of SA, the system will automatically produce another SA to replace the previous one while proceeding the setting timing. The default time is 3 hours, with the setting range between 1 to 24 hours.

IPSec Other Settings (See Figure 12-5)

Figure 12-5

- **[Dead Peer Detection]**: DPD is a standard protocol of automatically detecting VPN disconnecting system, it could automatically determine whether the IPSec tunnel on the other tunnel of the VPN is operating normally.

  When an issue is detected with the IPSec tunnel, actions such as Hold/Clear/Restart can be executed for that VPN tunnel.

  - **Hold**: Wait for the tunnel to recover.
  - **Clear**: Remove related data and wait for reconnection.
  - **Restart**: Reconnect the VPN tunnel immediately.

- **[Closing the Network Neighborhood]**: Establishing IPSec VPN tunnel leads both sides to use network neighborhood protocol to research computer's name. The default is enabled, referring permitting the packet of network neighborhood pass from the VPN tunnel to another one.

  For example: two 3100-6GT-I establish IPSec VPN connection to access specific internet resources.

  Company A: WAN IP is 61.11.11.11, LAN IP is 192.168.188.0/24

  Company B: WAN IP is 211.22.22.22, LAN IP is 192.168.200.0/24

  Under this situation, the connection environment structure of IPSec VPN Tunnel shows below: (See Figure 12-6)

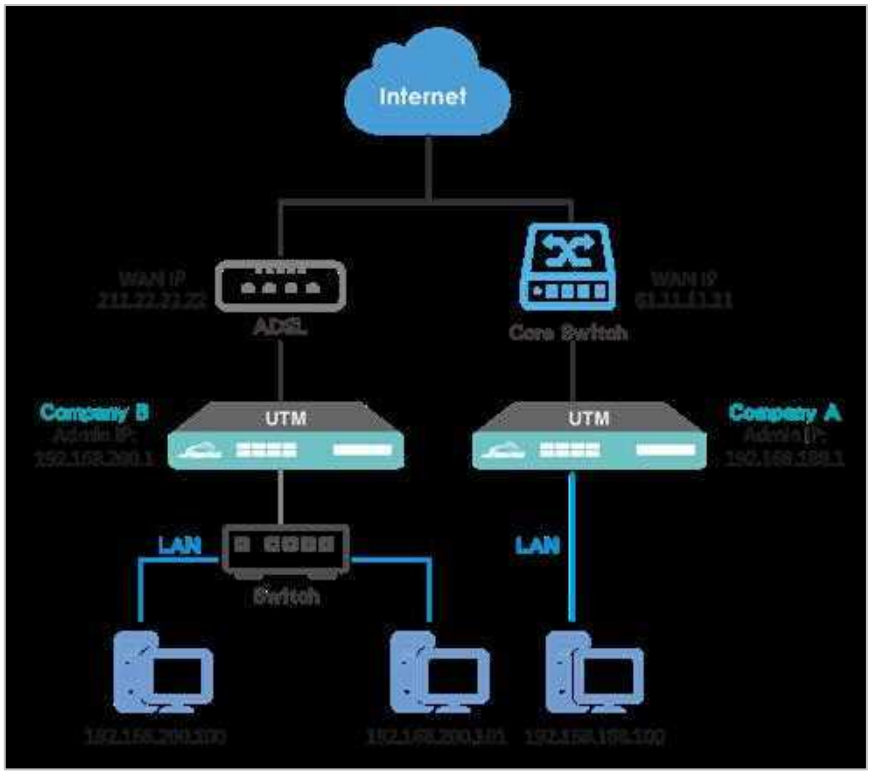


Figure 12-6

1. Settings of Company A

Default settings are not listed in the 3100-6GT-I IPSec VPN configuration for Company A.

- **[Enabled]**: Choosing to enable
- **[Name of VPN Tunnel]**: connecting to Company B
- **[Local IP Address]**: 61.11.11.11
- **[Remote IP Address]**: 211.22.22.22
- **[Local Internet]**: 192.168.188.0/24
- **[Remote Internet]**: 192.168.200.0/24
- **[Enabling back-up]**: Do not enable back-up service

IPSec Phase 1 Setting

- **[Connection Mode]**: Main mode
- **[Preshare Key]**: 123456789
- **[ISAKMP Algorithm]**: AES / SHA-1, DH Group2

IPSec Phase 2 Setting

- **[IPSec Algorithm]**: AES / SHA-1, DH Group2

IPSec Other Setting

- **[Dead Peer Detection]**: Restart

2. Settings of Company B

Default settings are not listed in the 3100-6GT-I IPSec VPN configuration for Company B.

- **[Enabled]**: Choosing to enable
- **[Name of VPN Tunnel]**: connecting to Company A
- **[Local IP Address]**: 211.22.22.22
- **[Remote IP Address]**: 61.11.11.11
- **[Local Internet]:** 192.168.2000/24
- **[Remote Internet]**: 192.168.188.0/24
- **[Enabling back-up]**: Do not enable back-up service

IPSec Phase 1 Setting

- **[Connection Mode]**: Main mode
- **[Preshare Key]**: 123456789
- **[ISAKMP Algorithm]**: AES / SHA-1, DH Group2

IPSec Phase 2 Setting

- **[IPSec Algorithm]**: AES / SHA-1, DH Group2

IPSec Other Setting

- **[Dead Peer Detection]**: Restart

Differences between both sides of the network are highlighted in red and must be entered accurately—any mistake in subnet or external IP will cause the VPN to fail.

Setting up a new IPSec VPN tunnel involves careful configuration of IDs, subnets, and other parameters. As the number of tunnels grows, identification becomes harder, increasing the risk of misconfiguration—especially since many remote sites use dynamic IPs, making IPSec VPN stability a challenge.

Volktek's **Auto VPN** is based on IPSec VPN but simplifies setup using two core components for faster deployment:

1. **Auto VPN Server**: Configures IPSec VPN and generates an ID for client use.
2. **Auto VPN Client**: Inputs the server-generated ID and Auto VPN IP to complete setup.

For details, see 12-1-2 Auto VPN Server and 12-1-3 Auto VPN Client.

IPSec Tunnel List

All configured IPSec VPN tunnels are displayed in the interface. (See Figure 12-7)

Figure 12-7

- **[Local Interface]**: The physical interface used by the IPSec VPN.

- **[Enable]**: Toggle to start or pause the tunnel. **Enable icon** = active; **Pause icon** = paused.
- **[Switch]**: Indicates whether the tunnel is primary or backup.
- **[Edit icon]**: Modify this tunnel's settings.
- **[Log]**: Click the "Log" button to view communication records. If traffic exists, a new window opens with logs sorted by time (newest last). (See Figure 12-8)

Figure 12-8

12-1-2. Auto VPN Server

When creating a new Auto VPN tunnel, the process is the same as a standard IPSec VPN—except for the **[Identifier]**. (See Figure 12-9)

- **[Identifier]**: A unique code automatically generated for each VPN tunnel. Copy and send this to the Auto VPN Client.

Figure 12-9

12-1-3. Auto VPN Client

Once the **[Identifier]** is received from the Auto VPN Server, configuration on the client side is simplified, with no need for detailed IPSec settings. (See Figure 12-10)

- **[Enable]**: Activates the VPN tunnel.
- **[Tunnel Name]**: A user-defined name for easy identification.
- **[Server IP]**: The external IP of the Auto VPN Server.
- **[Identifier]**: Enter the unique code provided by the Auto VPN Server.
- **[Local IP]**: The IP address used to establish the VPN tunnel.

Figure 12-10

A list of established VPN tunnels is shown below. (See Figure 12-11)

- **[AutoVPN Status]**: **Green icon** shows that the client is connected. **Gray icon** shows that Client is not connected.

- **[Enable]**: Toggle to start or pause the tunnel. **Enable icon** = active; **Pause icon** = paused.

Figure 12-11

12-2. PPTP Server

PPTP is supported across most operating systems like Windows and Linux with built-in dial-in clients. By entering a pre-assigned username and password, users can connect to the 3100-6GT-I via PPTP VPN over the Internet.

To use PPTP on the 3100-6GT-I, follow these steps:

1. Enable the PPTP server.
2. Create user accounts.
3. Define access rules in the policy section for PPTP users in **[Policy] > [Security Policy]**.

12-2-1. PPTP Account List

To establish an IPSec VPN tunnel, the same settings are required on both ends for a successful

All created PPTP accounts are displayed in the **[PPTP Account List]**, where administrators can manage each account's connection status and activation. (See Figure 12-13)

- **[Account]**: Username used by the PPTP client.

- **[Enable]**: Controls whether the PPTP VPN account is active. **Enable icon** = active; **Pause icon** = paused. Paused accounts cannot connect via PPTP.

Figure 12-13

12-2-2. Add Account

In **[Add Account]**, new PPTP dial-in user accounts can be configured. (See Figure 12-14)

- **[Enable]**: Activate or disable the account.
- **[Account]**: The username used for PPTP dial-in (e.g., jordan).
- **[Password]**: The associated password.
- **[Client IP Address]**: The IP address (or range) assigned to the client. The server can automatically allocate addresses based on the defined range, or a specific address can be manually configured for each account.
- **[User Define IP Address]**: If **[Client IP Address]** is selected, enter the specific IP (e.g. 192.168.1.5).

Figure 12-14

12-2-3. PPTP Server

Enable PPTP Server so that remote users can connect via PPTP: (See Figure 12-15)

- **[Enable]**: Activate the PPTP server.
- **[Compression & Encryption]**: Optionally enable compression in the PPTP tunnel.
- **[Client IP Address (Start-End)]**: Range of IPs assigned to dial-in users, e.g., 10.1.1.1–10.1.1.10.
- **[DNS1/2]**: DNS server addresses given to remote clients.
- **[WINS1/2]**: WINS server addresses given to remote clients.

Figure 12-15

12-2-4. PPTP Server Log

- **[Time]**: Time when PPTP dial-in begins.
- **[Account]**: Username used for dial-in.
- **[Source IP]**: Original client IP before VPN.
- **[Assigned IP]**: IP allocated to client for this session. If using [**User Define IP Address]**, it's fixed.
- **[Event]**: Dial-in start or end. The system calculates usage duration in "hours:minutes". Durations under 1 minute appear as **00:00**. (See Figure 12-16)

Figure 12-16

12-3. SSL VPN Server

SSL VPN is a secure virtual private network technology that allows remote users to access internal network resources (such as ERP, inventory systems, or IP-restricted library systems) as if they were locally connected. Because data is encrypted, transmitted traffic cannot be deciphered over the Internet, preserving confidentiality.

SSL VPN supports two control modes for remote users:

1. Access to internal network resources.
2. Internet access via the VPN server (this mode can be enabled or disabled).

Both directions can be regulated—bandwidth, services, and access schedule can all be restricted.

SSL VPN requires downloading client software and certificates from the server. The client software is portable and doesn't require installation—just run it. Thus, users can store it and the certificate on USB drives or any portable storage and execute it on any computer.

Client Software and Certificate Access

Clients may log in to the SSL VPN server to download the client software and certificate. Since the 3100-6GT-I client software and certificate are bundled, the package can be executed directly after downloading and extracting it.

The default download URL format is: https://<interface IP or domain>:<HTTPS port>/sslvpn.php

(The HTTPS port is defined under **[Configuration] > [Basic Settings] > [Administrative Access] > [HTTPS Port]**)

Example: If the management interface IP and port are https://211.2.2.2:8443, the download URL will be https://211.2.2.2:8443/sslvpn.php.

12-3-1. SSL VPN Setup

SSL VPN is disabled by default. Click **[Modify the Server Setting]** to enable and open its configuration interface.

Server Setting

- **[Service Status]**: Toggle to enable or disable SSL VPN service.
- **[Local Interface]**: Select the interface(s) and IP address(es) that will host the SSL VPN service. Multiple can be selected (e.g. LAN: 192.168.1.1 and WAN1: 172.16.1.11). Click **[Modify the Server Setting]** to apply changes.
- **[Client Linking Setting]**: Defines the connection address or hostname users download for client configuration. Clicking **"Change"** opens a new window. Normally, select WAN interface IP(s). In multi-WAN setups, multiple IPs may be chosen. Or use a custom DNS hostname, so future IP changes need only DNS updates. (See Figures 12-17, 12-18)

Figure 12-17

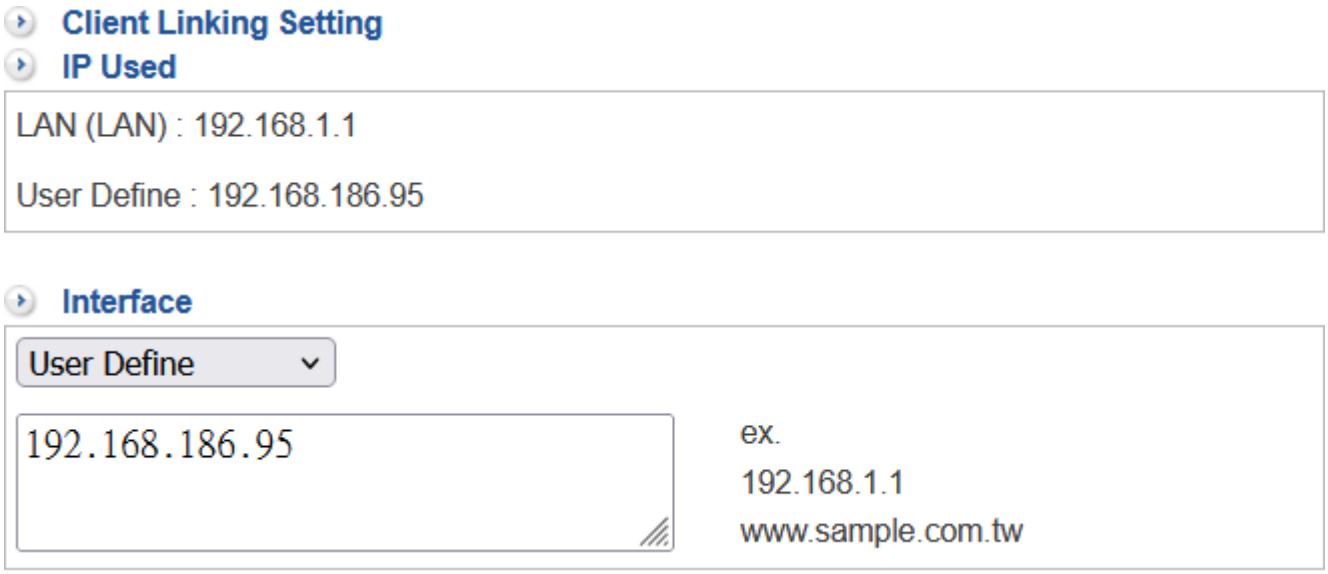


Figure 12-18

- **[Local Port]**: Specifies which ports accept SSL VPN connections. Administrators can define a single port or a range (e.g. 387 or 387–400). This port must not conflict with the WAN management interface port.
- **[Max Concurrent Connections]**: Maximum number of simultaneous SSL VPN users (default is 20).
- **[Client IP Range]**: The IP pool assigned to VPN clients (e.g. 10.8.0.0/24). This must not overlap with internal subnets.
- **[DNS Server]**: DNS IP address assigned to clients upon successful SSL VPN connection.
- **[WINS Server]**: WINS IP address assigned to clients. (See Figure 12-19)

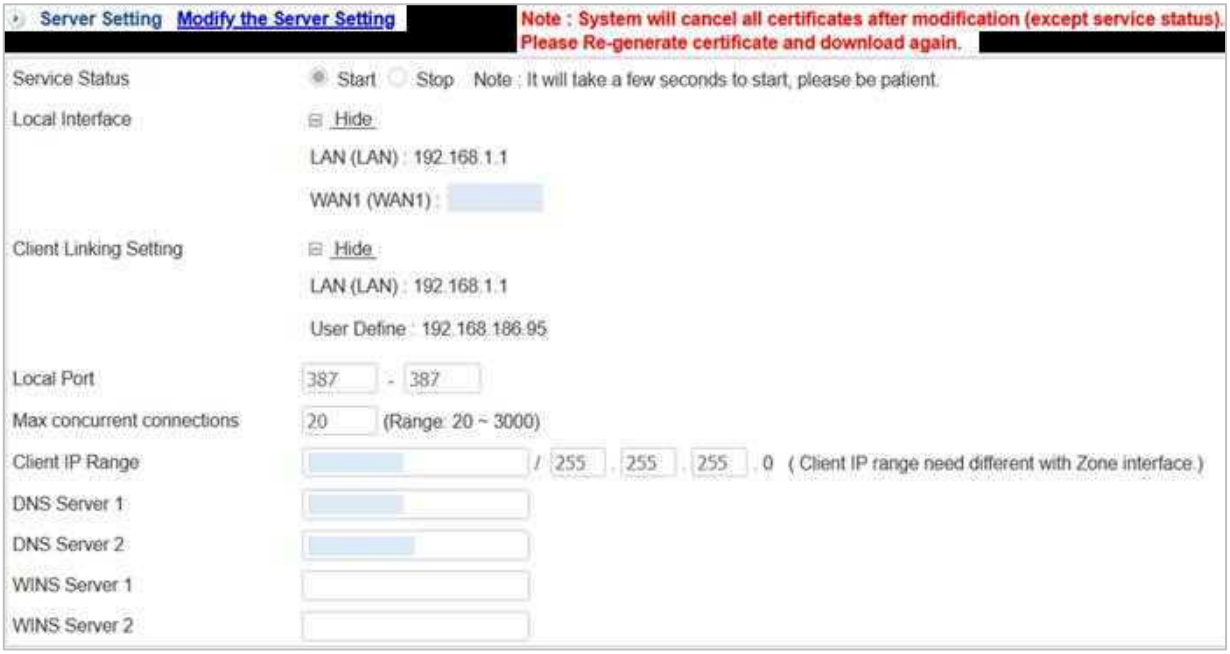


Figure 12-19

Client Route Setup

- **[Push Route]**: Defines which subnets should be routed through SSL VPN when the client does not have local routes. (See Figure 12-20)

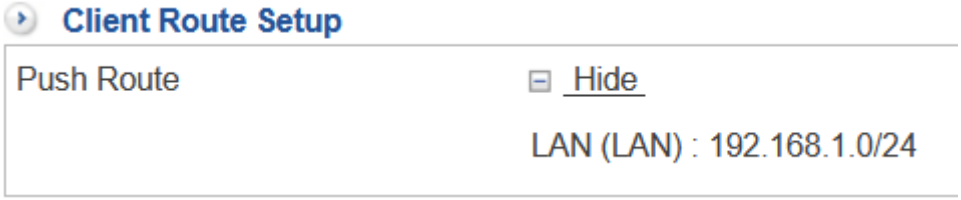


Figure 12-20

Certificate Message

- **[Issuer]**: The entity that issued the certificate.
- **[Subject]**: The user or server to whom the certificate belongs, including identifying info such as name, domain, email, etc.
- **[Term]**: The certificate's validity period. (See Figure 12-21)

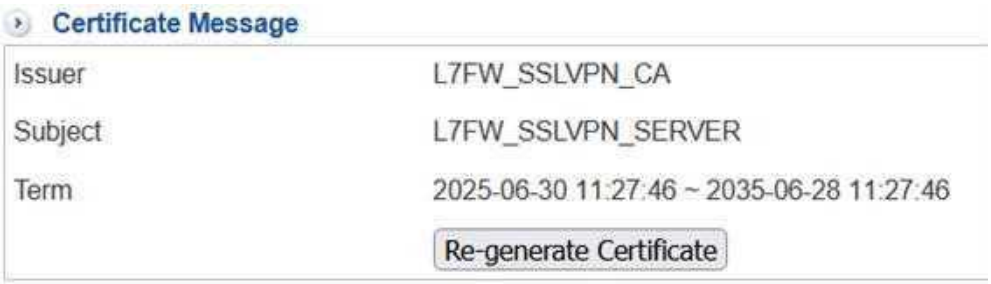


Figure 12-21

Certificate Settings

SSL VPN client certificates are signed by the **SSL Server**. When issuing a certificate, certain fields must be filled in (none may be left blank). If any character in these fields is changed, all client certificates must be re-downloaded. (See Figure 12-22)

Figure 12-22

12-3-2. SSL Client List

Before adding an SSL VPN client, an authentication group must first be created under the internet authentication settings, with members assigned accordingly. For details on creating group members, refer to 5-6-6. User Group.

Once the user group has been created, it can be added to the SSL Client List. The newly configured user group will then appear under the selected authentication group. (See Figure 12-23)

- **[Comment]**: A label used to describe the SSL VPN client, such as “SSLVPN-TEST”.
- **[Authentication Group]**: Displays user groups created under 5-6. Authentication that have not yet been applied.
- **[Address of information message]**: Specifies the destination webpage to redirect to after a successful SSLVPN connection. If not configured, the browser’s default homepage will be used.

Figure 12-23

After an authentication group is added, the Client SSLVPN list will display all SSL clients. (See Figure 12-24)

Figure 12-24

Re-generate All Certificate

Whenever any text is modified in the certificate server settings, all certificates for existing SSL VPN users must be regenerated. By clicking the **“Re-generate All Certificate”** button, the 3100-6GT-I will update all certificates. After re-downloading, users can resume use. (See Figure 12-25)

Clicking the “folder” icon opens the current certificate details.

- **[User Account]**: Users added during the group creation process.
- **[Cancel]**: Revokes the user's certificate, preventing connection. To restore access, a new certificate must be obtained.
- **[Re-generate]**: Cancels the user's certificate or reconfigures its contents. The user will be unable to connect and must re-generate a new certificate.
- **[Download]**: Downloads the client software and certificate.
- **[User Static IP Address]**: Assigns a fixed IP address to this SSL VPN client after each successful connection. Click the “pencil” icon to access the IP selection page and assign an unallocated IP address to the user.

- **[Enable/Disable]**: Temporarily disables the certificate. The certificate remains valid but connection is denied. Re-enabling access does not require a new certificate.
- **[User Static MAC Address]**: Allows the administrator to specify the MAC address of the SSL VPN client to prevent credential or certificate misuse. This ensures only approved devices can connect. If left blank, MAC address verification will not be performed.

  Click the “pencil” icon to enter the MAC address. If the client has multiple network interfaces, the SSL VPN client will automatically use the MAC address of the first interface for verification.

Figure 12-25

12-3-3. Client Download Page Setting

Users can log in to the 3100-6GT-I SSLVPN client download page to obtain the SSLVPN software. The download URL is: https://<interface IP address>:<port>/sslvpn.php

- **Step 1**: Download the file from https://SSLSERVER/sslvpn.php. (See Figure 12-26)

Figure 12-26

- **Step 2**: Run the SSL VPN client, **openvpn-gui-1.0.3-en.exe**, from the extracted folder.

right-click the icon .

- **Step 4**: Select **"EDIT Config"**. Language settings, SSLVPN server address, and port number can be modified. It is also possible to choose whether to access the internet via remote connection.

  If remote internet access is not enabled, only traffic to the remote LAN and DMZ segments will be routed through the SSLVPN tunnel; all other traffic will use the local network. (See Figure 12-27)

Figure 12-27

- **Step 5**: To establish an SSLVPN connection, enter the account and password provided by the administrator. This account and password are the same as those used to download the software and certificate. (See Figure 12-28)

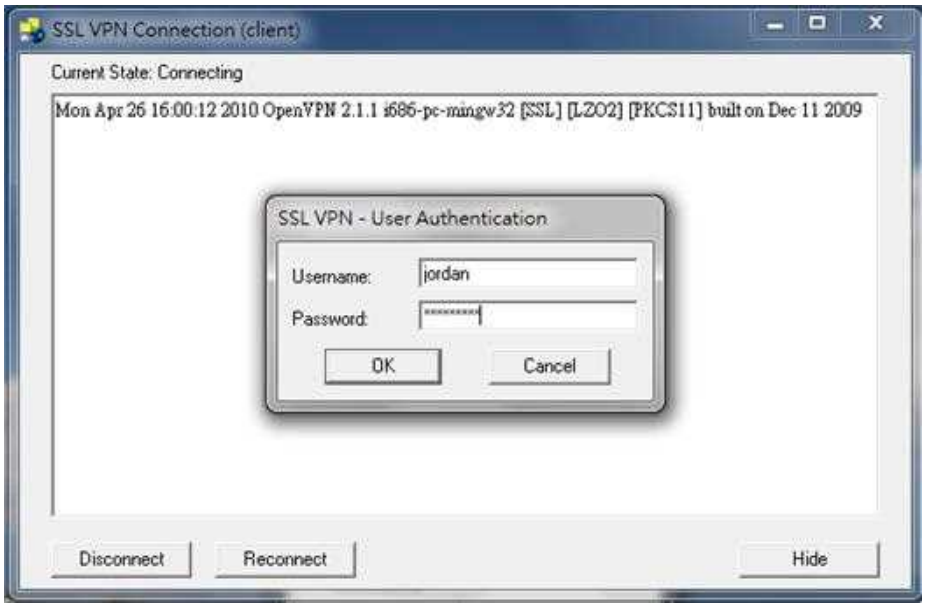


Figure 12-28

- **Step 6**: Once connected, the icon in the system tray will change from red to green, indicating a successful SSLVPN connection. (See Figure 12-29)

Figure 12-29

12-3-4. SSL VPN Status

Each SSL VPN connection is recorded in detail on the 3100-6GT-I. (See Figure 12-30)

- **[Refuse Connection Log]**: Enables or disables logging of rejected SSL VPN connection attempts. When enabled, all failed connection attempts will be logged. The administrator can click the log button to view related information.
- **[Online]**: Displays the total number of active SSL VPN connections.
- **[Kick]**: Allows the administrator to forcibly disconnect a user who is currently connected via SSL VPN. Clicking **Kick + Username** will terminate that user's session.

  All accounts permitted to connect via SSL VPN are listed in the user list. For each user, login and logout times can be tracked.

Figure 12-30

12-3-5. SSL VPN Log

The system records all SSL VPN connections in detail. Administrators can filter and search for abnormal logs based on specific criteria. (See Figure 12-31)

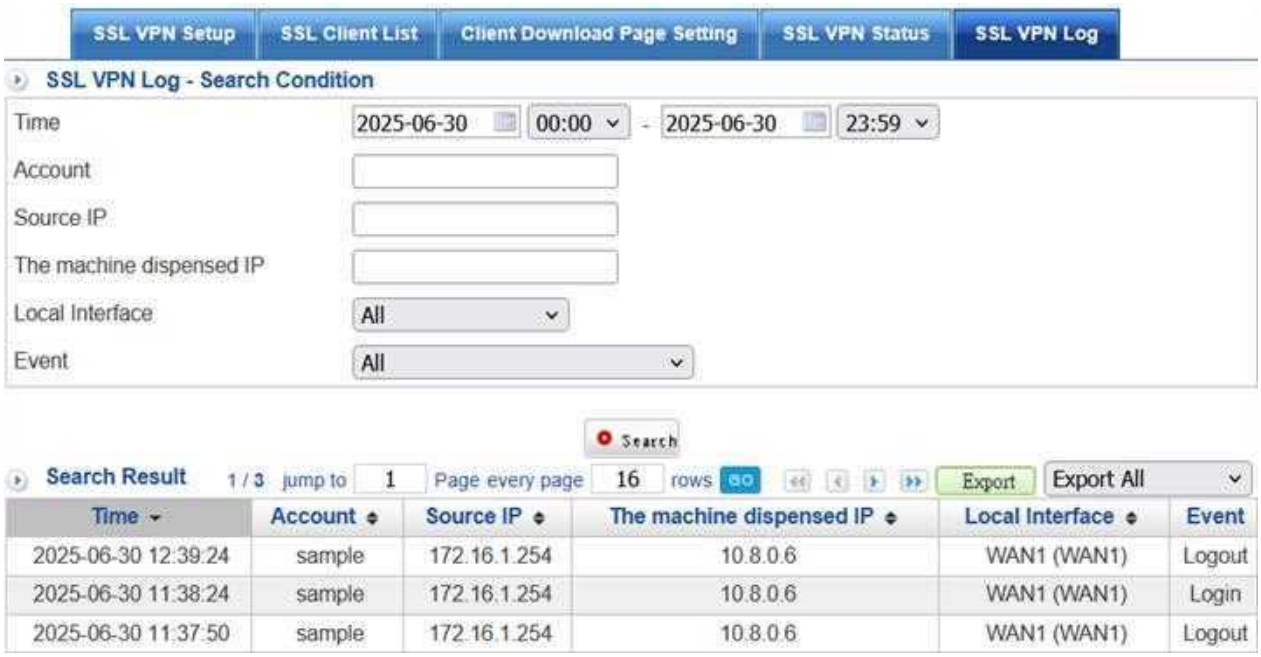


Figure 12-31

12-4. L2TP

The 3100-6GT-I supports L2TP VPN. L2TP provides a pre-shared key encryption mechanism via IPSec, offering stronger encryption protection than PPTP.

12-4-1. Account List

Created L2TP accounts will appear in the **[Account List]**, where administrators can enable or disable each account as needed.

Add Account

Account credentials required for L2TP dial-in. (See Figure 12-32)

- **[Enable]**: Enables or disables the account.
- **[Account]**: The account name assigned to the L2TP user, e.g., l2tptest.
- **[Password]**: The password for the account.
- **[Client IP Address]**: Two options are available — **Assigned by L2TP Server** or **User-defined IP address**.

Figure 12-32

Account List

After account creation, the status of each account can be viewed under **[Status]**. (See Figure 12-33)

See Figure 12-33

12-4-2. Basic Settings

L2TP is built on IPSec encryption technology; therefore, the pre-shared key and IP address range must be configured in advance. (See Figure 12-34)

- **[Enable]**: Enables or disables the L2TP server.
- **[Client IP Address (Start-End)]**: The IP address range assigned to L2TP clients, e.g., 10.1.1.1~10.1.1.10.
- **[The First DNS Server]**: The DNS server address assigned to remote clients.
- **[The Second DNS Server]**: The secondary DNS server address assigned to remote clients.
- **[Interface IP]**: Specifies which external interface IP will be used for L2TP dial-in. Clicking **"Assist"** will display all available external interfaces. Multiple interfaces can be selected for L2TP VPN access.
- **[PreshareKey]**: The encryption key used for L2TP.

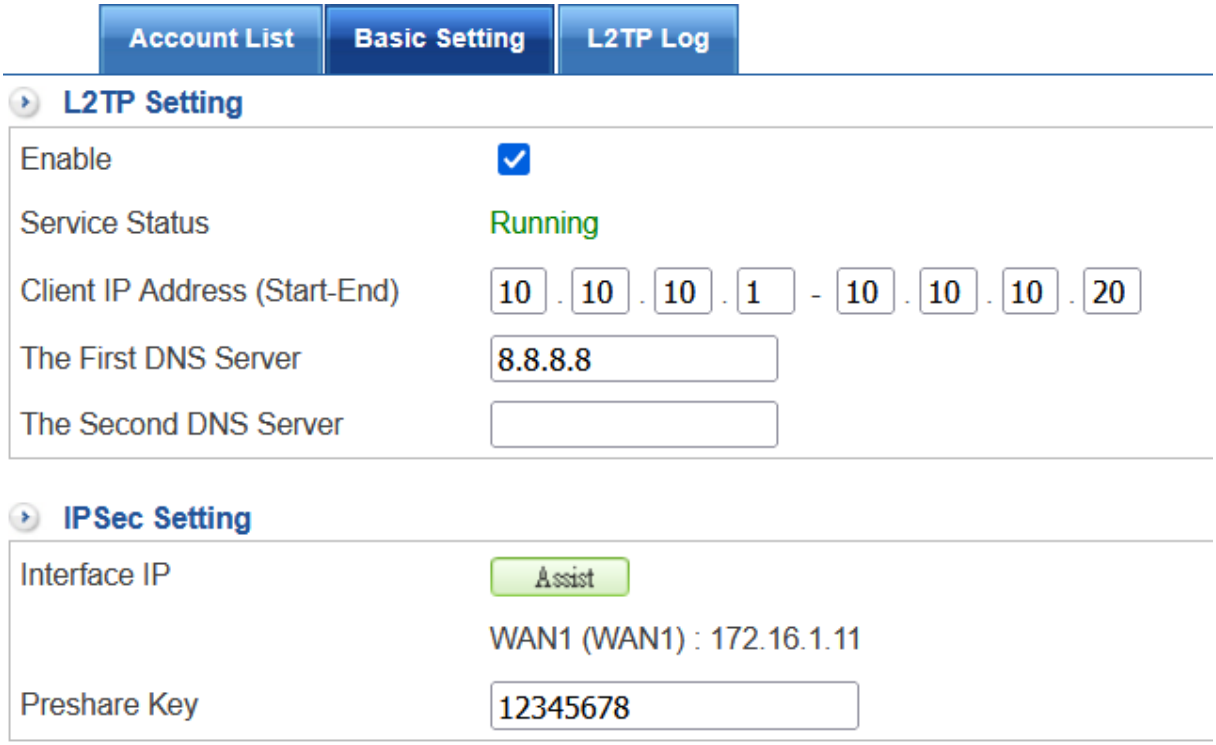


Figure 12-34

12-4-3. L2TP Log

- **[Time]**: The timestamp when the L2TP client connection started.
- **[Account]**: The account name used for the connection.
- **[Source IP]**: The original IP address of the L2TP client.
- **[The machine dispensed IP]**: The IP address assigned to the client by the L2TP server for the current session. If **"User-defined IP address"** is used, a fixed IP will be assigned.
- **[Event]**: Indicates whether the L2TP client has started or ended a session. For disconnection events, the system automatically calculates the total session time in the format **hours:minutes**. Durations shorter than one minute are recorded as **00:00**. (See Figure 12-35)

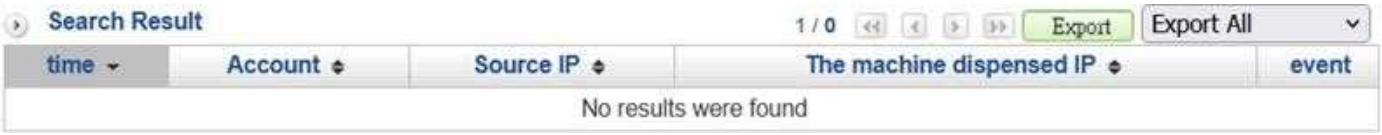


Figure 12-35

Chapter 13. Tools

The system provides a set of network tools that allow administrators to actively send diagnostic packets to verify the external connection quality and DNS resolution status of the 3100-6GT-I. Available tools include **PING**, **Traceroute**, **DNS Query**, **Port Scan**, **Wake up**, and **SNMP**. The **PING** function supports both IPv4 and IPv6 address modes.

13-1. Connection Test

13-1-1. Ping

When encountering network issues, it is common to use the PING command (available in both Windows and Linux) to check the connectivity between the local and remote networks. The **PING** command uses the ICMP protocol to send packets of a specified size at fixed intervals and measures the response time from the destination, helping determine the status of the network connection. (See Figure 13-1)

- **[Target IP or Domain]**: The IPv4/IPv6 toggle in the menu allows switching between address modes. For IPv4, both IP addresses and domain names can be entered, e.g., 168.95.1.1 or www.hinet.net.
- **[Package Size]**: The size of each ICMP packet sent. Default is **32 bytes**. Configurable range: 1–9999 bytes.
- **[Count]**: Number of ICMP packets to send. Default is **4**. Configurable range: 1–9999.
- **[Timeout]**: Maximum wait time for ICMP response. If exceeded, the connection is considered lost. Default is **1 second**. Configurable range: 1–9999 seconds.
- **[Using Interface & IP]**: Specifies the interface and corresponding IP address from which the test packet is sent.
- **[Assign Gateway]**: Specifies the gateway used to send the test packet from the selected interface.

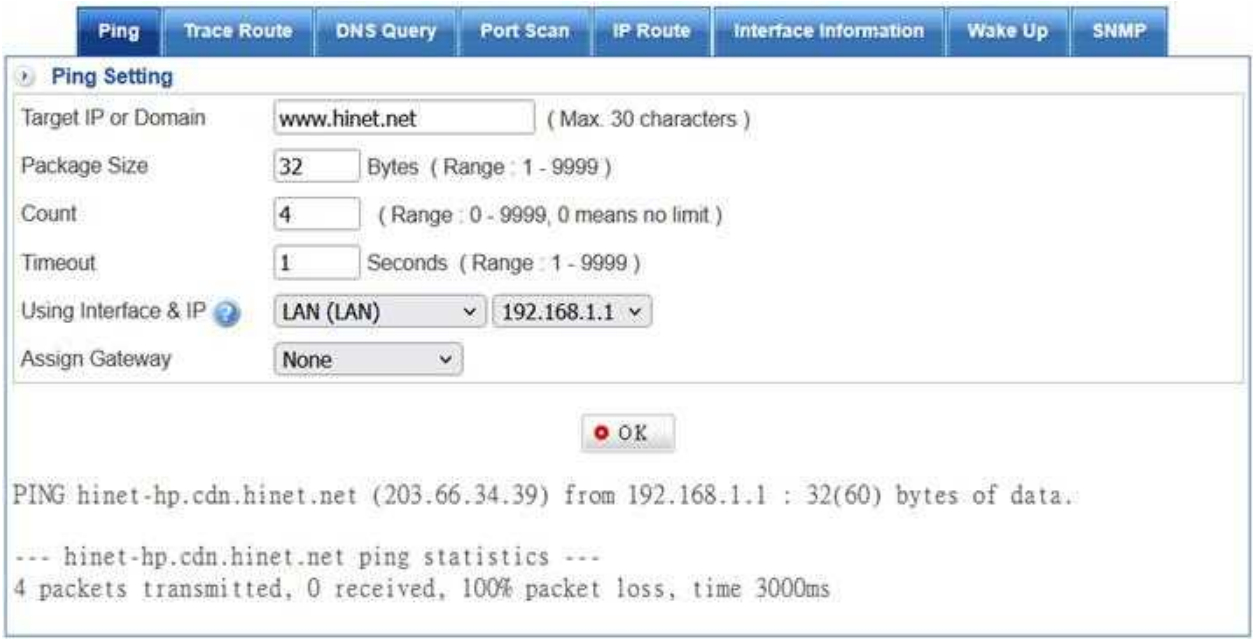


Figure 13-1

13-1-2. Trace Route

This tool displays the IP addresses of routers that packets traverse from the source to the destination. When facing network connectivity issues, besides using **PING** to verify the connection, **Trace Route** helps identify the intermediate routers or where the disconnection occurs. Currently, only IPv4 addresses are supported. (See Figure 13-2)

- **[Target IP or Domain]**: Enter the IP address or domain name to be tested, e.g., 168.95.1.1 or www.hinet.net.
- **[Package Size]**: The size of each ICMP/UDP/TCP packet sent. Default is **40 bytes**. Configurable range: 40–9999 bytes.
- **[Max. Next Hop]**: Maximum number of routers to trace through. Default is **30**. Configurable range: 1–255.
- **[Wait Time]**: Maximum wait time for ICMP response. If exceeded, the connection is considered dropped. Default is **2 seconds**. Configurable range: 2–9999 seconds.
- **[Tracing Methods]**: Protocol used to send the trace packets. Options include ICMP, UDP, or TCP. Default is **ICMP**.
- **[Source Interface]**: Specifies the interface and its corresponding IP address to send the test packet.

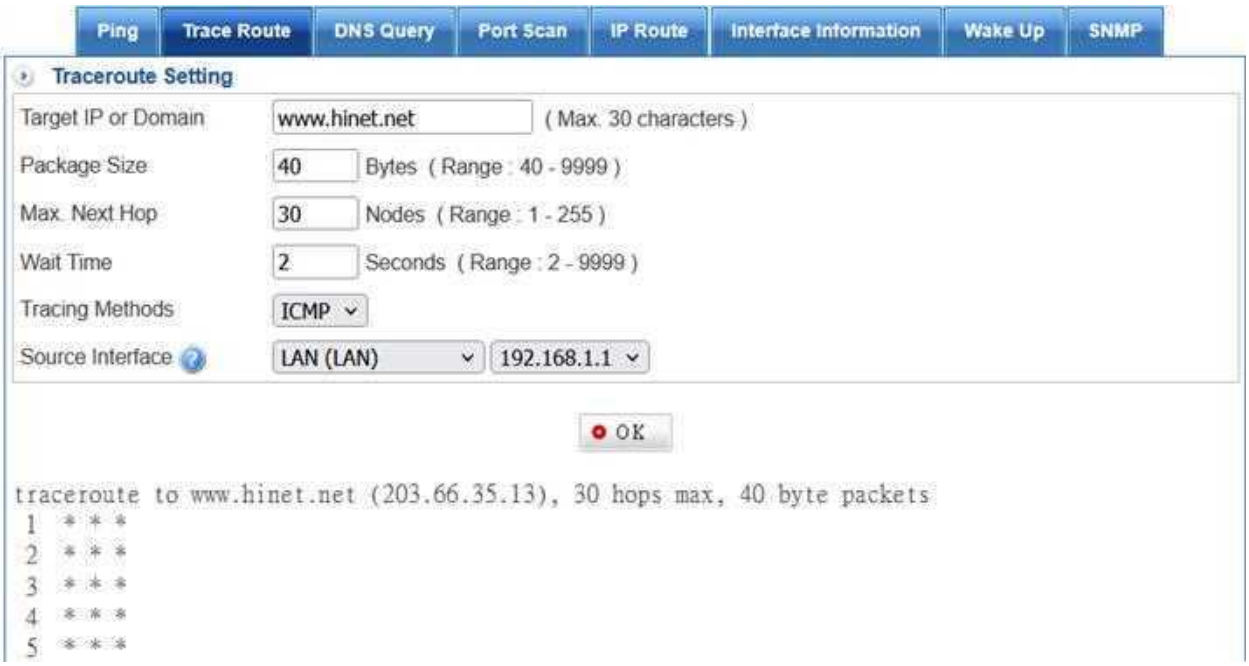


Figure 13-2

13-1-3. DNS Query

This tool allows detailed DNS record lookups, supporting query types such as **ANY**, **SOA**, **NS**, **A**, **MX**, **CNAME**, and **PTR**. Administrators can perform queries using the local DNS server or specify an external DNS server. (See Figure 13-3)

- **[Using DNS Server]**: Allows selection of the DNS server used by the 3100-6GT-I or manual input of a different DNS server, e.g., 8.8.8.8.
- **[Domain or IP to Query]**: Enter the domain name or IP address to query. Domain names perform forward lookups, while IP addresses perform reverse lookups. For example, 168.95.1.1 or www.hinet.net.
- **[Query Type]**: Specifies the type of DNS record to query, including ANY, SOA, NS, A, MX, CNAME, and PTR.

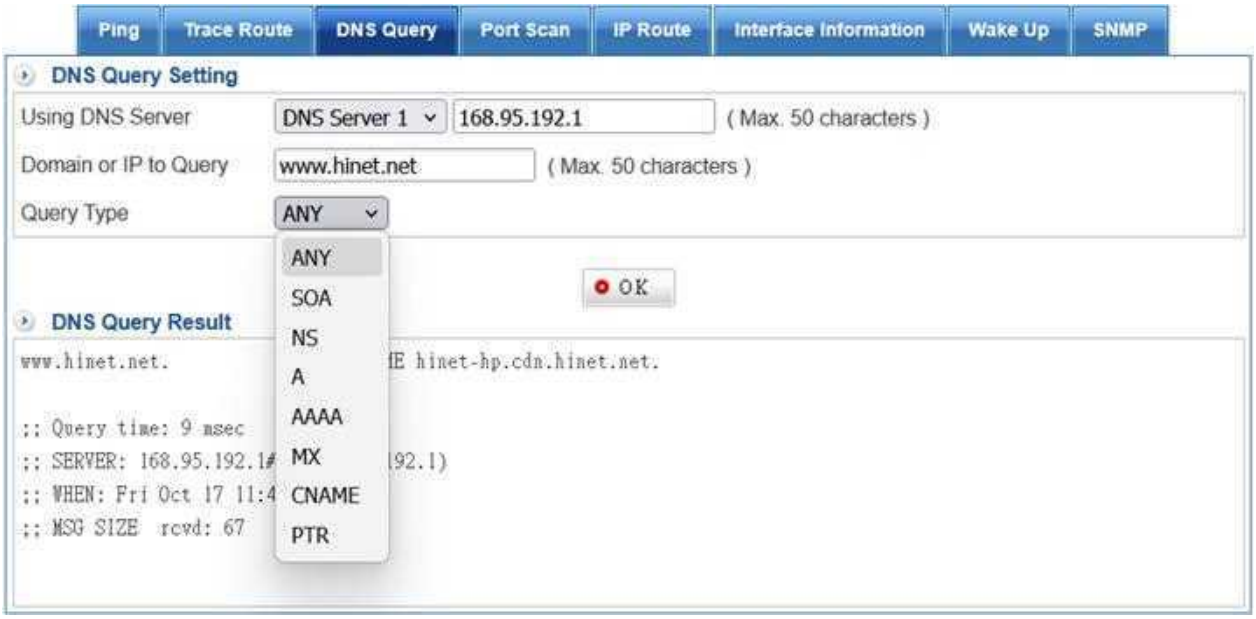


Figure 13-3

13-1-4. Port Scan

This tool uses the 3100-6GT-I to scan a remote host for commonly used open ports. (See Figure 13-4)

- **[Domain or IP to Scan]**: Enter the IP address or domain name of the target host, e.g., 8.8.8.8.
- **[Scan Serve]**: Select whether to scan default or custom ports.
- **[Source IP]**: Specifies the zone and IP address used during the scan.
- **[Port Scan Result]**: If a port is open, **OK** will be displayed. If it is closed, **FAIL** will be shown.

Figure 13-4

13-1-5. IP Route

Displays the complete routing table of the 3100-6GT-I for administrator reference. (See Figure 13-5)

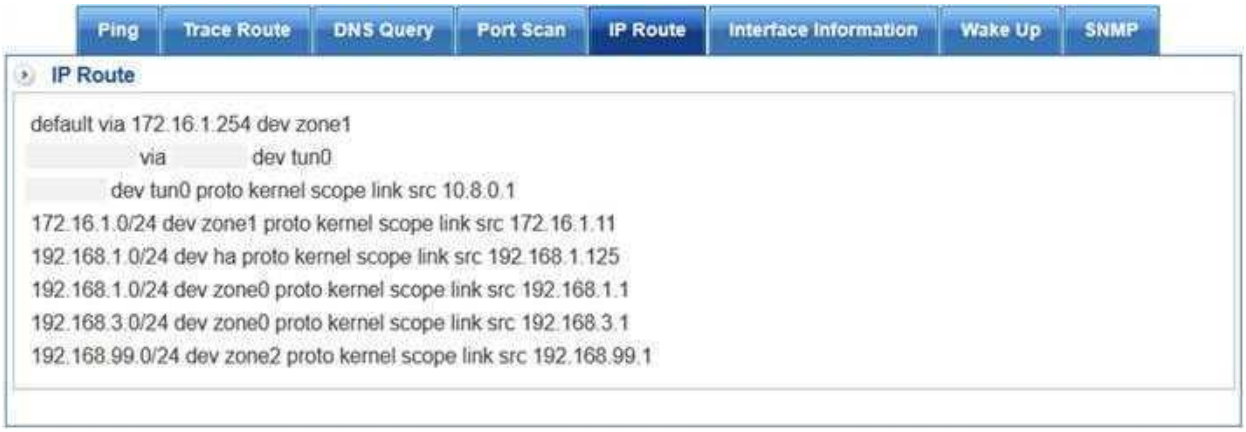


Figure 13-5

13-1-6. Interface Information

The 3100-6GT-I displays the bound address segments, user IPs, and MAC addresses within each zone. (See Figure 13-6)

Figure 13-6

13-1-7. Wake Up

The 3100-6GT-I can send Wake Up packets to remote computers. By entering the target computer's MAC address and clicking "**OK**", the system will automatically send a Wake Up packet. Administrators can also click **"Assist"** to select the device to be woken up. (See Figure 13-7)

- **[Using Interface & IP]**: Specifies which interface the target device belongs to.
- **[MAC Address]**: The MAC address of the computer to be woken up. If unknown, use the **"Assist"** button to select it.

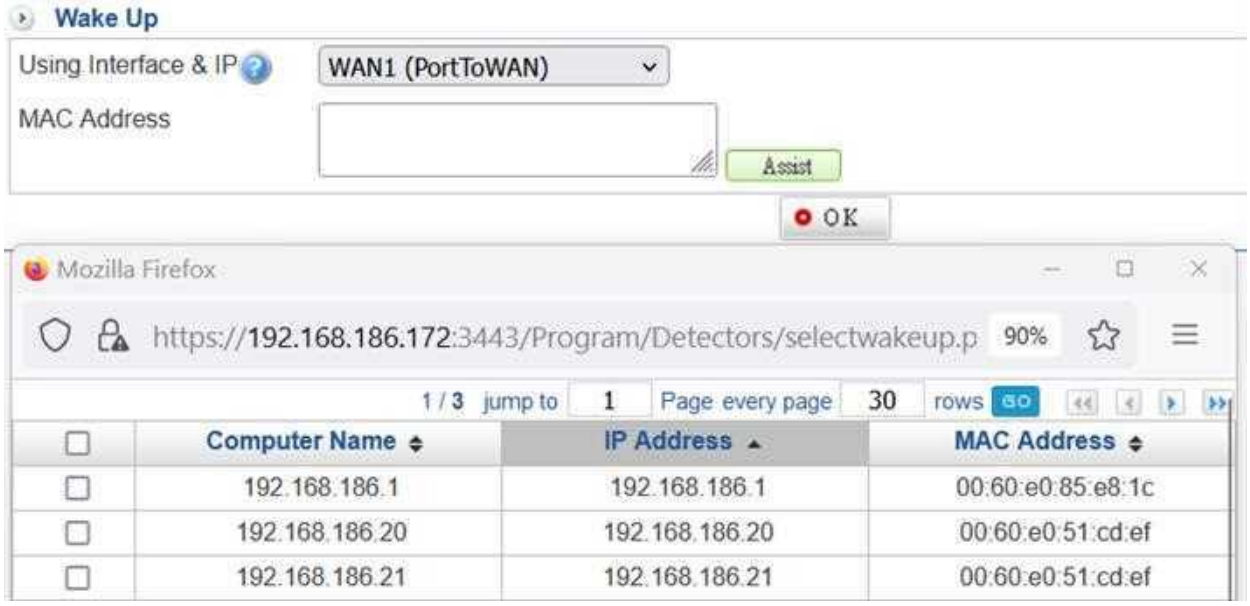


Figure 13-7

13-1-8. SNMP

The 3100-6GT-I uses the SNMP protocol to query switch information, including real-time traffic on each port, VLAN ID, and more.

- **[Switch IP]**: The IP address of the switch to be queried.
- **[Read permissions]**: Since only query operations are performed, only the read permission password is required.
- **[OID]**: The data to be queried. SNMP queries are based on Object Identifiers (OID). (See Figure 13-8)
- **[VlanID]**: Indicates which VLAN the switch belongs to.

Explan

oid	Explan	Example
Necessary		
iso.3.6.1.2.1.2.2.1.10	search port in flow	iso.3.6.1.2.1.2.2.1.10.515 = Counter32: 3692512
iso.3.6.1.2.1.2.2.1.16	search port out flow	iso.3.6.1.2.1.2.2.1.16.515 = Counter32: 11238968
iso.3.6.1.2.1.17.1.4.1.2	search port Corresponding Ifindex	iso.3.6.1.2.1.17.1.4.1.2.515 = INTEGER: 509
iso.3.6.1.2.1.31.1.1.1.1	search port interface	iso.3.6.1.2.1.31.1.1.1.1.515 = STRING: "ge-0/0/6"
iso.3.6.1.2.1.2.2.1.2	search port interface	iso.3.6.1.2.1.2.2.1.2.515 = STRING: "ge-0/0/6"
iso.3.6.1.2.1.17.4.3.1.2	search mac port Corresponding	iso.3.6.1.2.1.17.4.3.1.2.0.13.72.50.168.248 = INTEGER: 522
iso.3.6.1.2.1.17.7.1.2.2.1.2	search mac port Corresponding	iso.3.6.1.2.1.17.7.1.2.2.1.2.2.0.28.240.40.57.191 = INTEGER: 21
iso.3.6.1.2.1.2.2.1.7	search port disable	iso.3.6.1.2.1.2.2.1.7.515 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.8	search port Plug	iso.3.6.1.2.1.2.2.1.8.515 = INTEGER: 2
Vlan Necessary		
iso.3.6.1.4.1.9.9.46.1.3.1.1.2.1	search Vlan ID	iso.3.6.1.4.1.9.9.46.1.3.1.1.2.1.10 = INTEGER: 1
iso.3.6.1.2.1.4.20.1.2	search Vlan id	iso.3.6.1.2.1.4.20.1.2.128.0.0.1 = INTEGER: 38
iso.3.6.1.2.1.17.1.4.1.1	search vlan port	iso.3.6.1.2.1.17.1.4.1.1.515 = INTEGER: 515
Append		
iso.3.6.1.2.1.17.1.2	search switch total port counts	iso.3.6.1.2.1.17.1.2.0 = INTEGER: 24
iso.3.6.1.2.1.4.22.1.2	search ip mac Corresponding	iso.3.6.1.2.1.4.22.1.2.38.128.0.0.1 = Hex-STRING: 00 0B CA FE 00 00
iso.3.6.1.2.1.1.1	search switch name	iso.3.6.1.2.1.1.1.0 = STRING: "24G + 4 SFP Web Smart Switch - 2.03"
iso.3.6.1.4.1.9.2.2.1.1.1	search port interface	iso.3.6.1.4.1.9.2.2.1.1.1.10101 = STRING: "Gigabit Ethernet"

Figure 13-8

13-2. Capture Packet

When troubleshooting network issues, it is sometimes necessary to capture packets for analysis. The 3100-6GT-I provides a scheduled packet capture tool, allowing administrators to record traffic and later download the captured files from the **[Completed List]**.

13-2-1. Schedule List

- **[Enable]**: Enables the packet capture function.
- **[Time Range]**: Specifies the time range for packet capture.
- **[Interface]**: Selects the interface from which to capture packets, including its associated zone.
- **[Protocol]**: Options include capturing all packets or filtering by **TCP** or **UDP** only.
- **[Filter Condition]**: Two modes are available:
  - Simple: Enter an IP address or IP range.
  - Advanced: Enter a full **tcpdump** command.
- **[pcap File Size (MB)]**: Size of each captured file. Configurable range: 1–10 MB.
- **[pcap File Num]**: Total number of capture files to create. Configurable range: 1–100.

  Note: Storage requirements should be calculated based on the maximum file size. For example, 10 MB × 100 files = 1000 MB = 1 GB. Ensure that enough disk space is available, especially if multiple capture schedules are running simultaneously.
- **[pcap Length]**: Maximum length per packet capture. The typical MTU for networks is 1500 bytes. (See Figure 13-9)

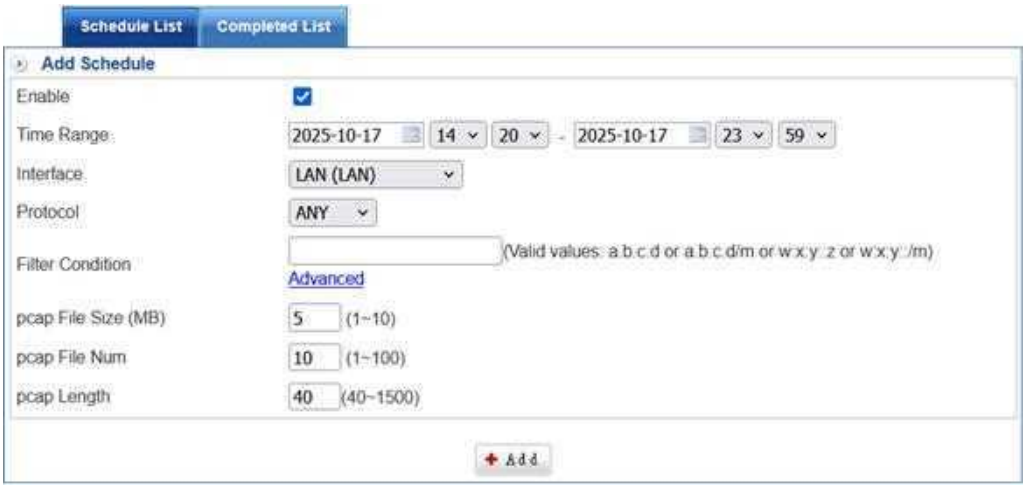


Figure 13-9

13-2-2. Completed List

Successfully captured packets will be listed here. Click the **"Log"** button to download the file to the local machine. (See Figure 13-10)

Figure 13-10

Chapter 14. Log

The 3100-6GT-I precisely records all actions performed by administrators within the system, including failed login attempts. This logging provides a reliable audit trail for administrators to review their own actions or those of other administrators and serves as an accurate historical record for retrospective analysis.

14-1. System Operation

14-1-1. Logs

All events are recorded with their timestamp, login account, source IP address, function path, action, and content. Logs can be retained for up to 12 months.

Detailed records are available for all login events. Every action performed on the 3100-6GT-I—whether by **View**, **Read**, **Write**, or **View-Read-Write** permission levels—such as add, modify, delete, search, or download, will be fully logged. Entries can be sorted alphabetically or numerically. (See Figure 14-1)

- **[Time]**: The time the event occurred.
- **[Account]**: The administrator account that triggered the event.
- **[IP Address]**: The IP address used by the administrator account.
- **[Management IP]**: The firewall IP address used to access the management interface.
- **[Menu Path]**: The navigation path of the management interface accessed.
- **[Action]**: The type of action performed, such as login, add, modify, delete, search, or download.
- **[Events Content]**: Detailed information about the action before and after execution. The 3100-6GT-I highlights differences between the original and modified settings for administrator review.


Logs List

1 / 277 jump to 1 Page every page 30 rows GO Export Export All

Time	Account	IP Address	Management IP	Menu Path	Action	Events Content
2024-08-28 10:36:28	oli	192.168.190.116	192.168.186.172	System Login	Login	Login False
2024-08-28 10:36:23	oli	192.168.190.116	192.168.186.172	System Login	Login	Login False
2024-08-28 10:22:32	admin	192.168.190.124	192.168.186.172	System Login	Login	Login Successful
2024-08-28 09:03:15	admin	192.168.190.124	192.168.186.172	System Login	Login	Login Successful
2024-08-28 08:48:43	admin	192.168.190.116	192.168.186.172	Service > Sandstorm > Sandstorm Record	Search	Date
2024-08-28 08:46:52	admin	192.168.190.116	192.168.186.172	System Login	Login	Login Successful
2024-08-27 18:07:58	admin	192.168.66.66	192.168.186.172	Configuration > Reboot & Power Off > Reboot & Power Off	Power Off	-

Figure 14-1

14-1-2. Logs Search

Allows searching through all stored records in the 3100-6GT-I based on specific IP addresses or event characteristics. (See Figure 14-2)

- **[Account]**: Displays all administrator accounts. Select **"All"** or a specific account.
- **[IP Address]**: The IP address used to log into the system.
- **[Management IP]**: The firewall's IP address.
- **[Time]**: The time range for the log search.
- **[Event]**: The event type to search for. **Select All** is also available.

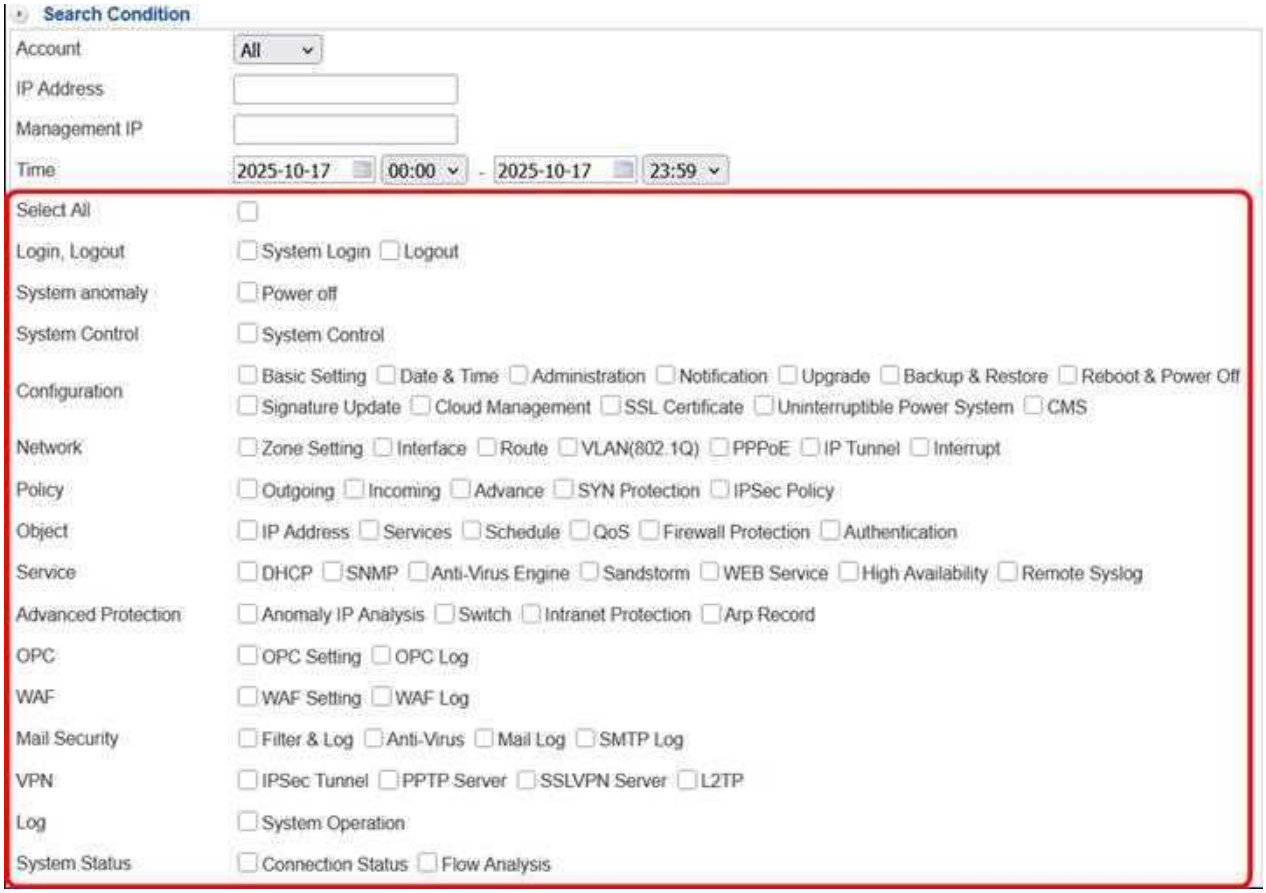


Figure 14-2

Chapter 15. Status

Users can monitor system resource usage of the 3100-6GT-I at any time, including statistics for CPU, RAM, and storage. Real-time connection information and traffic statistics are also available. In addition to real-time data, historical data is provided for administrator reference.

The system status is divided into four main sections:

1. **[System Status]**: Displays current CPU usage, load, memory usage, and system load of the 3100-6GT-I. Upload and download traffic for each interface is also shown. Historical statistics for these metrics are available.
2. **[Connection Status]**: Records connection usage details on the 3100-6GT-I, including the number of active connections and packet logs.
3. **[Flow Analysis]**: Provides usage statistics categorized by **port**, **application**, or **location**.
4. **[Dashboard]**: Presents various statistics in graphical format.

15-1. System Status

15-1-1. System Status

The **[System Status] > [System Status]** section displays statistical data from the current time up to the past 24 hours. It includes the following three categories:

- **[CPU Usage]**: Shows the 3100-6GT-I's CPU usage over the past 24 hours. (See Figure 15-1)

  Clicking **"More"** will display usage graphs for each individual CPU.

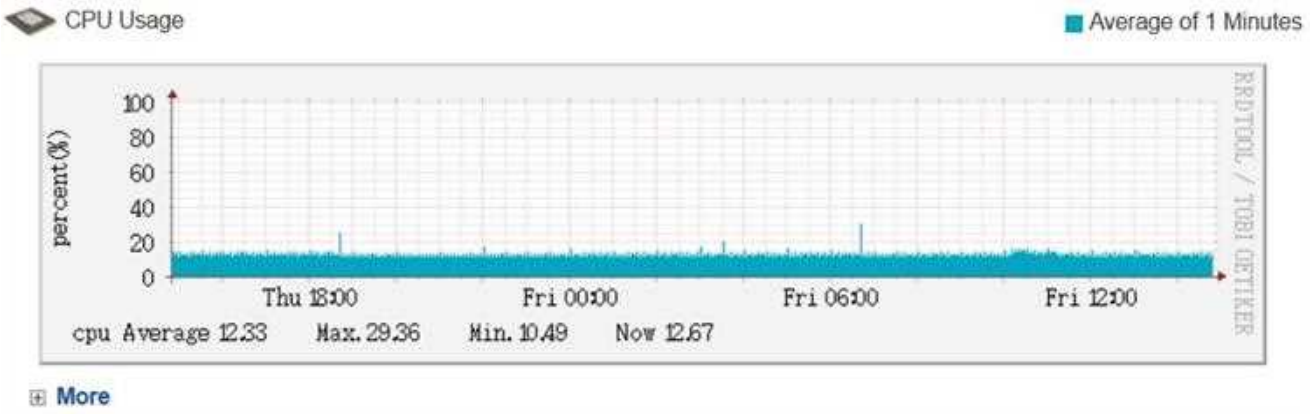


Figure 15-1

- **[Memory Usage]**: Displays memory usage of the 3100-6GT-I over the past 24 hours. (See Figure 15-2)

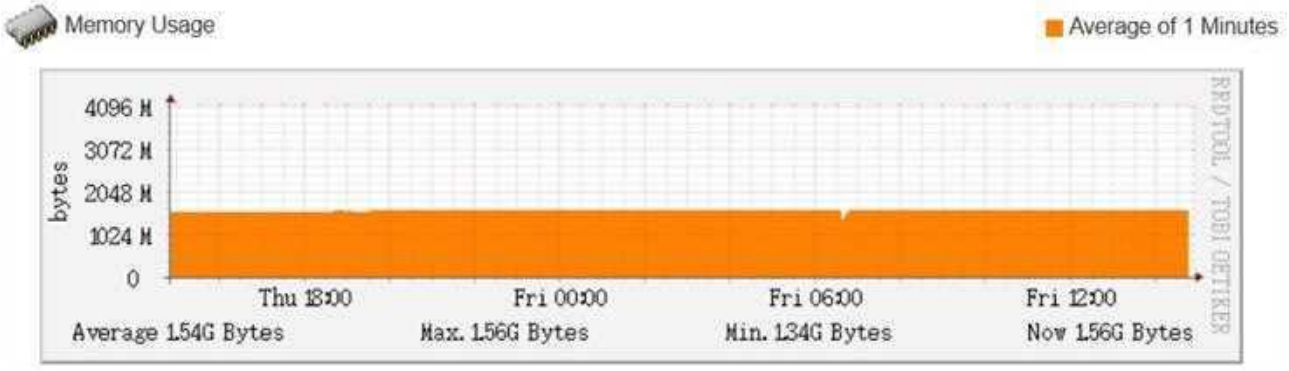


Figure 15-2

- **[System Usage]**: Displays system load over the past 24 hours on the 3100-6GT-I. (See Figure 15-3)

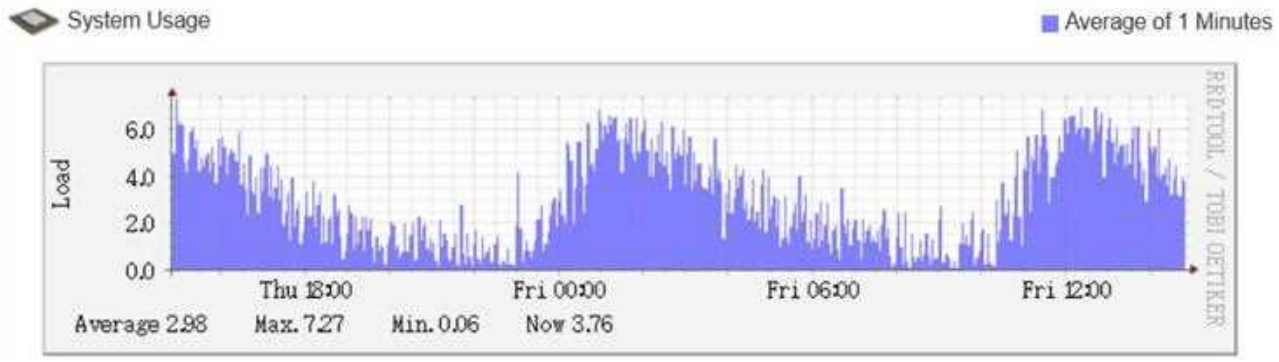


Figure 15-3

15-1-2. Interface Flow

In the **[System Status] > [Interface Flow]** section, the network traffic of all interfaces on the 3100-6GT-I over the past 24 hours is displayed. Traffic statistics are based on the interface level.

For example, if an interface has two physical 1G links, the maximum displayed traffic can reach 2G when fully utilized.

In the chart:

- **Blue** (upper area) represents **upload traffic** — traffic entering the interface.
- **Green** (lower area) represents **download traffic** — traffic exiting the interface.

For **WAN-type interfaces**, note that the upload/download directions shown in the graph may differ from the upstream/downstream directions defined by the service provider. (See Figure 15-4)

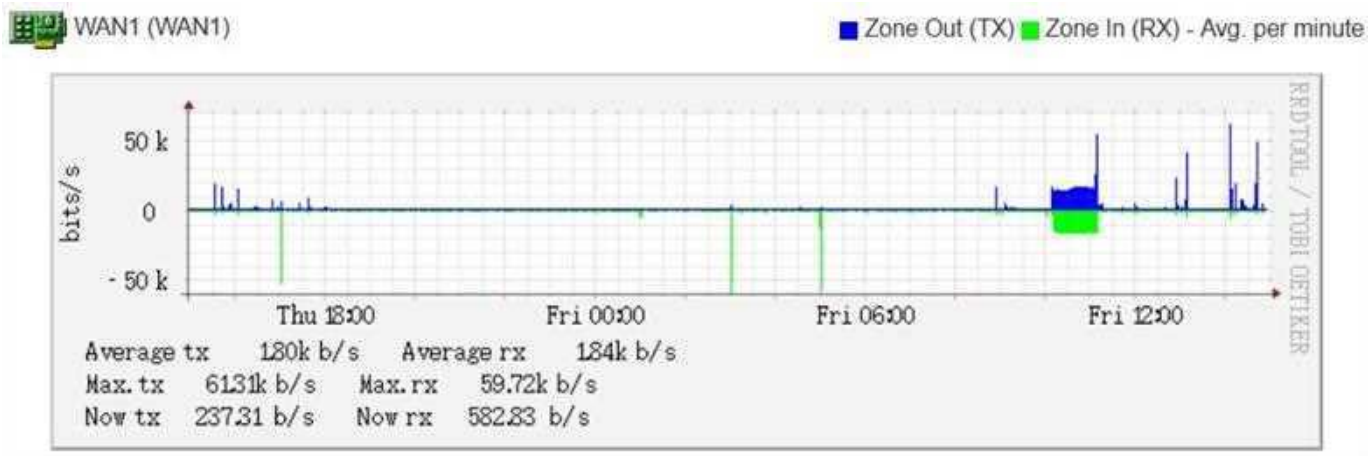


Figure 15-4

15-1-3. Connection Status

The 3100-6GT-I provides charts showing the number of online users and active connections over the past 48 hours. This allows administrators to quickly observe usage trends within a given time frame. For longer timeframes, refer to 15-1-4. History Status. (See Figure 15-5)

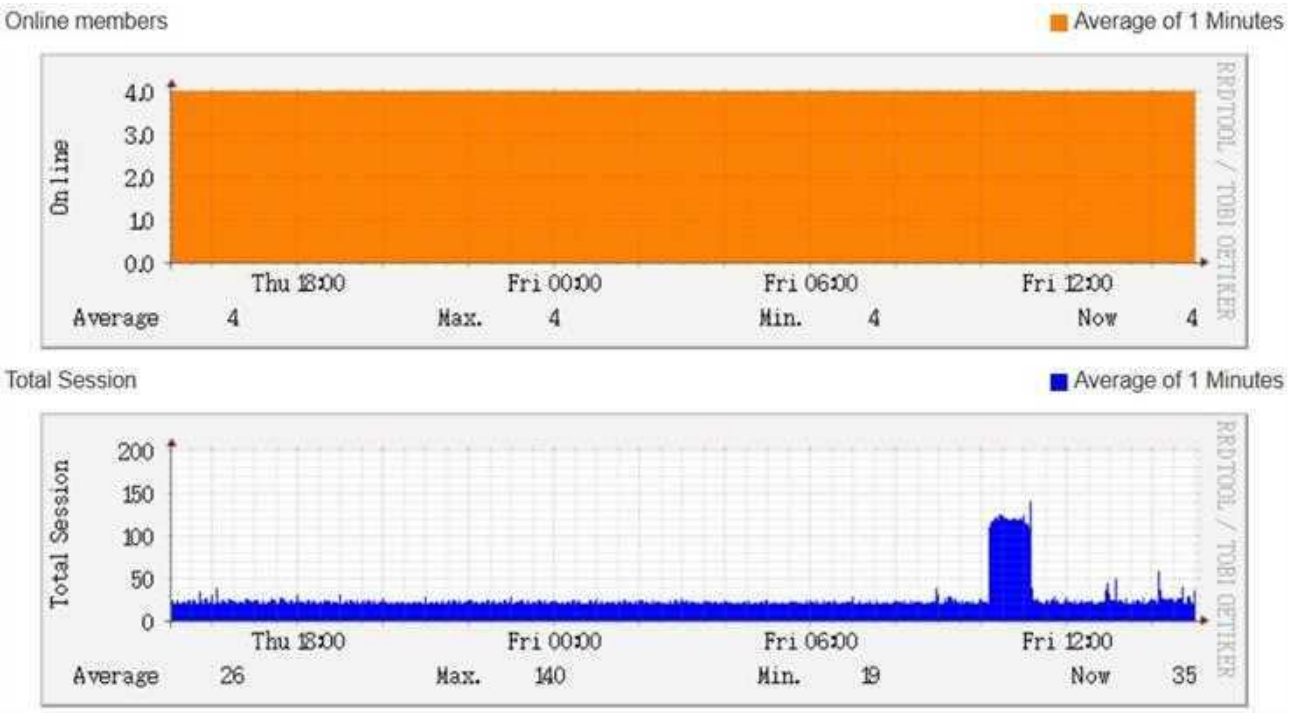


Figure 15-5

15-1-4. History Status

Displays historical statistics for CPU, RAM, system load, and traffic for each interface. After selecting a time range, the 3100-6GT-I automatically generates graphs for that period.

This feature helps administrators identify problematic time intervals and analyze potential causes and solutions. (See Figure 15-6)

- **[Search Object(s)]**: Select the metrics to query. Available options include CPU, RAM, system load, interface traffic, online members, and total connection count. For interface traffic, the system lists all available network interfaces for selection.
- **[Date]**: Select the date range to search.

Figure 15-6

15-1-5. Timely Flow

Unlike the **[Interface Flow]** section, which shows traffic statistics over the past 24 hours, this section displays **real-time traffic over the past 3 minutes** for each interface.

Both physical interfaces and virtual interfaces—such as **IP Tunnel** and **PPPoE**—are supported. A maximum of two interfaces can be displayed simultaneously. (See Figure 15-7)

Traffic is calculated per interface. For example, if an interface has two physical 1G links, its maximum displayed throughput can reach 2G under full load.

In the graph:

- **Blue** represents **upload traffic** (incoming to the interface)
- **Green** represents **download traffic** (outgoing from the interface)

For **WAN-type interfaces**, the traffic direction in the graph may differ from the upstream/downstream direction defined by the ISP.

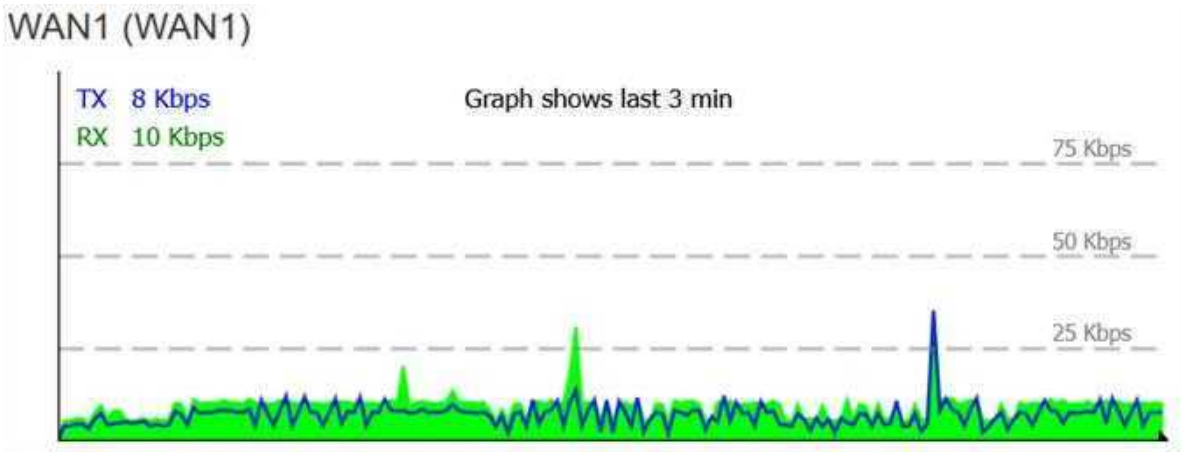


Figure 15-7

15-1-6. CPU Info

In the **[System Status] > [CPU Info]** section, the real-time load of each CPU core is displayed. This helps administrators determine whether a single CPU core is being overutilized.

If such a condition is detected, administrators can redistribute the network traffic to other CPU cores via **[Network] > [Interrupt]**. (See Figure 15-8)

Name	Idle	User	System	Nice	I/O	irq	Softirq	CPU Use
Average	95.00%	1.00%	1.50%	1.00%	1.50%	0.00%	0.00%	5.00%
cpu0	97.00%	1.00%	1.00%	0.00%	0.00%	0.00%	1.00%	3.00%
cpu1	94.95%	0.00%	2.02%	1.01%	2.02%	0.00%	0.00%	5.05%

Figure 15-8

15-2. Connection Status

Displaying all IP information that passes through the 3100-6GT-I interface. For intranet, it is possible to determine whether the device is powered on and from which network interface it connected to.

15-2-1. System Status

In the **[Connection Status] > [Computer List]** section, all IP information passing through the 3100-6GT-I interfaces is displayed.

For devices within the internal network, the system can also determine whether a device is online or offline, and from which interface it connected. The list can be sorted by various criteria. (See Figure 15-9)

- **[Computer List Preserve]**: Defines how many days to retain IP address records passing through the 3100-6GT-I. Default is **7 days**. Configurable range: 0–365. A value of **0** means the records will not be cleared.
- **[Online]**: Displays statistics by subnet. For example, All (141/220) indicates that 220 IP addresses have passed through the configured interfaces within the past 7 days, and 141 are currently online.
- **[Interface Display]**: Select the interfaces to be shown, including physical interfaces and 802.1Q VLANs.
- **[Alias]**: The NETBIOS name of the computer. Custom names can be defined in the address object table.
- **[IP Address]**: The IP address of the device.
- **[MAC Address]**: The MAC address of the device.
- **[Interface]**: The source interface of the device, including both physical and 802.1Q VLAN interfaces.
- **[Status]**:
  - **Power-on icon**: Indicates the device is online.
  - **Power-off icon**: Indicates the device is offline.
- **[Last Update Time]**: Displays the timestamp of the most recent update.

Figure 15-9

15-2-2. Connection Track

Through packet analysis and session tracking, this function monitors and analyzes each user's network activity from system startup to shutdown.

It records when and how long a user accessed the network, as well as what actions were performed.

The data is categorized by source device name, and includes information such as IP address, number of connections, upload/download traffic, and detailed logs (including protocol used, source IP, destination IP, ports, number of packets, and data volume for both upload and download).

In the **[Connection Status] > [Connection Track]** section, current upload and download traffic statistics for all internal users on the 3100-6GT-I are displayed. (See Figure 15-10)

- **[Total Session]**: Displays the number of active sessions currently passing through the 3100-6GT-I. The format is **This Page / Total Session**.

  For example, **1245 / 1976** means there are 1,976 total sessions, with 1,245 displayed on the current page, and the rest shown on other pages.
- **[SRC IP]**: Enter the source IP address to filter. Leave blank to view all.
- **[DST IP]**: Enter the destination IP address to filter. Leave blank to view all.
- **[Computer Name]**: Shows the computer's NetBIOS name or the name defined in the address table. If unavailable, the IP address is displayed instead.
- **[IP Address]**: The device's IP address.
- **[Session]**: The number of active connections established by the device.
- **[Zone Out (TX)/ Zone In (RX) flow bits]**: The number of bits transmitted / received by the firewall for this IP.

Figure 15-10

After selecting a target device, clicking the **"Log"** button displays detailed session and packet information for the past 3 minutes. In the **Application** section, the 3100-6GT-I categorizes each connection based on application type. (See Figure 15-11)

- **[Clear]**: Clears all data and refreshes the packet session display.
- **[Refresh]**: Instantly updates the session and traffic information.
- **[Export]**: Exports the data table for further analysis using external tools.
- **[Protocol]**: Which protocol this connection use, which usually are TCP or UDP.
- **[Source IP]**: The IP address of the selected device.
- **[Destination IP]**: The destination IP address of the connection.

- **[Port]**: Displays both source and destination ports, e.g., 62506 > 53 indicates that the source port is 62506 and the destination port is 53. Based on the protocol (e.g., UDP), this can be identified as DNS traffic.
- **[Zone Out (TX) / Zone In (RX) Packets]**: The number of packets sent/received by the firewall for this connection.
- **[Zone Out (TX) / Zone In (RX) Bytes]**: The number of bytes sent/received by the firewall for this connection.
- **[Application]**: Identifies the application used in this session. The 3100-6GT-I classifies applications using its built-in DPI engine, which recognizes over 900 application types.
- **[Designated Gateway]**: Indicates which outbound interface was used for internet access.
- **[Policy]**: The policy applied to this connection.

Refresh | Clear | 1 / 7 jump to 1 | Page every page 30 rows | Export | Export All

Protocol	Source IP	Destination IP	Port	Zone Out (TX) Packets	Zone In (RX) Packets	Zone Out (TX) Bytes	Zone In (RX) Bytes	Application	Designated Gateway	Policy
tcp	192.168.66.66	35.71.178.8	50510 -> 443	80	78	56.3K	104.6K	HTTPS	toInternet_ (WAN1: PortToWAN)	Outgoing [19]
tcp	192.168.66.66	172.67.26.105	34130 -> 443	101	64	62.34K	255.36K	HTTPS	toInternet_ (WAN1: PortToWAN)	Outgoing [19]
udp	192.168.66.66	172.217.163.46	52510 -> 443	13	15	61.5K	48.54K		toInternet_ (WAN1: PortToWAN)	Outgoing [19]
tcp	192.168.66.66	142.251.43.3	47710 -> 443	16	12	20.55K	12.88K	Google.com	toInternet_ (WAN1: PortToWAN)	Outgoing [19]

Figure 15-11

15-3. Flow Analysis

The 3100-6GT-I provides traffic analysis tools that allow administrators to review each IP's usage based on overall traffic volume, application type, or TCP port.

15-3-1. Flow Rank

The Flow Rank feature allows administrators to view each user's network usage, sorted by traffic volume. By selecting a user, additional details such as application usage can be viewed.

- **[Time range for preset loading]**: When the **Flow Rank** tab is selected, the system loads data based on the predefined time range.
  - The default option is **Today** (starting from 00:00).
  - Another option is to load only the **last 1 hour** of data.
  - If the dataset is large and causes page loading delays, the third option — **Do Not Show** — can be selected. In this case, no data is shown until the **"Change"** button is clicked to manually load it.
- **[Flow Direction]**: Specifies whether traffic is ranked by **source IP** or **destination IP**. Click **"Search"** after switching to apply the selected mode.
- **[Statistics By]**: Determines the grouping criteria for statistics. Options include **IP Address** or **User Account** (from authentication records). The default is IP Address.
- **[Time Range]**: Sets the time window for the analysis. Only **Today** and **1 Hour** are available. (See Figure 15-12)

Figure 15-12

After selecting the search criteria, all traffic statistics passing through the 3100-6GT-I are listed. In the **[Flow Direction]** section, traffic can be aggregated by **source IP** or **destination IP**, with **source IP** as the default. If web authentication is enabled, traffic can also be analyzed by **user account**. (See Figure 15-13)

- **[Computer Name]**: The computer's NETBIOS name.
- **[IP Address]**: The IP address of the computer.
- **[MAC Address]**: The MAC address of the computer.
- **[Authentication]**: If the IP address is associated with a web authentication account, the account name will be shown. Otherwise, this field remains blank.
- **[Up Flow]**: The total upload traffic, measured in K/M/GBytes.
- **[Down Flow]**: The total download traffic, measured in K/M/GBytes.

Computer Name	IP Address	MAC Address	Authentication	Up Flow	Down Flow
192.168.66.13	192.168.66.13	6c:02:e0:b8:f1:fc		41.76 MB	2.53 GB
LAPTOP-HN66PKPA	192.168.66.66	6c:02:e0:b8:f1:fc		155.88 MB	711.20 MB
laptop	192.168.66.23	00:13:74:00:00:00		19.04 MB	281.32 MB
192.168.189.17	192.168.189.17			1.03 MB	5.17 MB
192.168.1.99	192.168.1.99			347.05 KB	0.00 KB

Figure 15-13

By clicking on any computer or IP address in the list, more detailed information can be viewed, including the proportion of upload and download traffic consumed by specific applications or protocols. (See Figure 15-14)

- **[Time Range]**: The time range for traffic statistics.
- **[IP Address]**: The IP address used for statistics, based on either source or destination.
- **[Data Type]**: Two options are available — **Basic Service** and **Application Category**.

  The toggle button on the right allows switching between them. If **Basic Service** is currently selected, the toggle will show **Application**, and vice versa.
- **[IP Location (Destination)]**: Displays the geographic region of the destination host accessed by the source IP. Clicking this will switch the lower section of the list to show destination IP locations.
- **[Basic Service / Application]**: Indicates the type of service.
  - **Basic Service**: Categorized by protocol (e.g., HTTP, HTTPS).
  - **Application**: Categorized by app name (e.g., WhatsApp, Teams).

Time_Range : 2024-08-28 08:04:57 ~ 2024-08-28 09:04:57

Src IP : 192.168.66.66 Data Type : Basic Service IP Location(Destination) Application

Basic Service	Up Flow		Down Flow		Packet Record
HTTPS	6.18 MB	70%	38.53 MB	87%	Log
HTTP	132.47 KB	1%	2.70 MB	6%	Log
999	741.43 KB	8%	1.83 MB	4%	Log

Figure 15-14

By clicking the **"Log"** button for any item in the list, the 3100-6GT-I displays more detailed information for that specific statistic, including upload/download traffic by time interval, the gateway used, and the applied policy rule. (See Figure 15-15)

- **[Duration]**: Duration of the specific connection.
- **[Up/Down Flow]**: Accumulated upload and download traffic for the connection.
- **[Gateway]**: Indicates which outbound interface (gateway) was used.
- **[Policy]**: The policy rule applied to the traffic.

Time_Range : 2024-08-28 09:23:11 ~ 2024-08-28 10:23:11

Src IP : 192.168.66.66

Basic Service : HTTPS

Back

1 / 94 jump to 1 Page every page 30 rows GO Export Export All

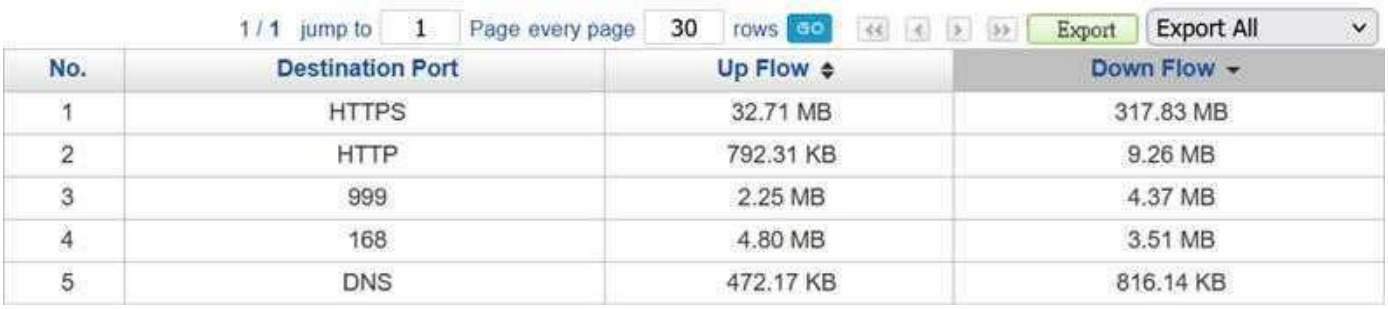
Date	Duration (S)	Protocol	Src IP	Dst IP	Port	Up Flow	Down Flow	Gateway	Policy
2024-08-28 10:23:03	50	tcp	192.168.66.66	142.251.43.10	45912->443	2.14 KB	6.92 KB	toInternet_ (WAN1: PortToWAN)	Outgoing [19]
2024-08-28 10:23:01	95	tcp	192.168.66.66	18.214.38.91	50484->443	5.86 KB	7.08 KB	toInternet_ (WAN1: PortToWAN)	Outgoing [19]

Figure 15-15

15-3-2. Flow Rank By Port

The 3100-6GT-I displays a ranked list of total traffic by communication protocol within the selected time range.

Protocols such as HTTP (TCP 80), HTTPS (TCP 443), etc., are included in the ranking. Traffic is sorted by **upload** and **download** volumes separately, allowing administrators to clearly understand traffic distribution by protocol. (See Figure 15-16)


1 / 1 jump to 1 Page every page 30 rows GO Export Export All

No.	Destination Port	Up Flow	Down Flow
1	HTTPS	32.71 MB	317.83 MB
2	HTTP	792.31 KB	9.26 MB
3	999	2.25 MB	4.37 MB
4	168	4.80 MB	3.51 MB
5	DNS	472.17 KB	816.14 KB

Figure 15-16

15-3-3. Flow Rank By App

The 3100-6GT-I displays a ranked list of total traffic by application within the selected time range. Applications such as WhatsApp, HTTPS, Teams, etc., are included in the ranking, with separate statistics for upload and download traffic.

By default, the 3100-6GT-I does **not** display unidentified applications. If desired, administrators can enable the **[Display Unknown]** option to include unidentified applications in the results. (See Figure 15-17)


1 / 1 jump to 1 Page every page 30 rows GO Export Export All

No.	Application	Up Flow	Down Flow
1	HTTPS	18.83 MB	275.35 MB
2	Google.com	6.24 MB	25.12 MB
3	SSL/TLS	6.79 MB	7.69 MB
4	HTTP	528.21 KB	5.41 MB
5	Yahoo Mail	178.69 KB	4.58 MB

Figure 15-17

15-3-4. Flow Rank By Location

The 3100-6GT-I displays the geographic locations of destination IP addresses within the selected time range. It also provides total traffic statistics grouped by region, helping administrators understand traffic distribution by location. (See Figure 15-18)

1 / 1 jump to 1 Page every page 30 rows GO Export Export All

No.	IP Location	Up Flow	Down Flow
1	United States of America	28.52 MB	275.93 MB
2	Taiwan	8.92 MB	25.93 MB
3	Singapore	2.35 MB	21.47 MB
4	other	808.60 KB	6.01 MB
5	United Kingdom	109.46 KB	3.64 MB
6	Japan	831.89 KB	2.75 MB

Figure 15-18

15-3-5. Flow Rank Search

This feature allows querying the **top 10 to 500 users** based on specified conditions. The available search criteria are as follows:

- **[Date]**: The time range for the query.
- **[Flow Direction]**: Two types of connection directions are available — Source and Destination.
- **[Search Condition]**: Filter options include **Source IP**, **Destination IP**, **Destination Port**, **Authentication**, **Application**, **IP Location**, and **Gateway**.
- **[Search Rank]**: Allows selection of the top 10 to 500 users. The system defaults to showing the top 10.
- **[Search Type]**: Choose to rank by Flow or Session.

After clicking **"Search"**, the results will be displayed in the list below. (See Figure 15-19)

Search Result :

Search Rank	Top 10
Date	2024-08-28 00:00 ~ 2024-08-28 23:00

Export

Computer Name	IP Address	MAC Address	Authentication	Up Flow	Down Flow
ALLEN583	192.168.66.66	6c:02:e0:b8:f1:fc		42.07 MB	336.62 MB

Figure 15-19

15-3-6. Flow Rank Search Quota

If a total traffic quota is configured for each IP address in the **Policy** settings, this section allows administrators to query users who have exceeded their assigned quota.

Chapter 16. Dashboard

The 3100-6GT-I **Threat Intelligence Dashboard** provides a different style of data visualization compared to traditional firewalls. It presents information graphically, including **network traffic**, **content**, and **hacker attack and defense records**. Using drill-down techniques, the dashboard enables administrators to trace and identify the root causes of issues.

Currently, the Threat Intelligence Dashboard includes the following modules: **Flow Analysis**, **Session**, **Defense**, **OPC**, **Web Control**, and **Mail**. At the top of the dashboard homepage, tabs allow switching between these modules. The **Management** tab returns to the traditional management interface.

By default, the dynamic charts calculate percentage ratios based on the total volume of data. If an administrator wishes to **exclude certain data types from the overall statistics**, simply click on the specific item. The 3100-6GT-I will automatically exclude that data and recalculate the distribution accordingly.

16-1. Threat Intelligence

The Threat Intelligence section presents the 3100-6GT-I's attack and defense records in a clear and straightforward manner, helping administrators quickly understand the overall security status. It is divided into two main areas: **Instant Information** and **Historical Information**.

- **Instant Information** displays the most recent attack events.
- **Historical Information** organizes records by month, including statistics on **anti-virus**, **anti-spam**, **OPC**, **firewall protection**, and various policies, along with a basic comparison to the previous month.

The default Threat Intelligence overview on the homepage is a summarized view. To access more detailed information, click the **Threat Intelligence icon** at the top of the page. If administrators wish to export the statistics, clicking the **PDF** or **PNG** icon in the upper right corner will generate the data in the selected format. (See Figure 16-1)

Figure 16-1

16-2. Flow Analysis

The 3100-6GT-I is built on a DPI (Deep Packet Inspection) core. Every network connection passing through the device is identified by its associated application, and its usage is recorded.

The traffic analysis (Application) on the Dashboard presents this statistical data through a graphical interface. (See Figure 16-2)

Figure 16-2

- **[Area Chart]**: Summarize the total upload/download traffic passing through the 3100-6GT-I in the past 24 hours, with each hour as the basic unit. After clicking on the statistical number for each hour, the Dashboard will list the usage distribution of all applications during that hour. (See Figure 16-3)

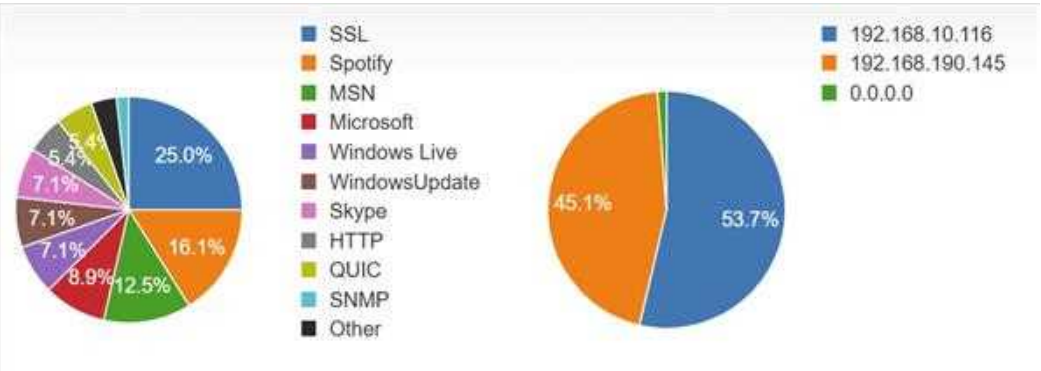


Figure 16-3

- **[Pie Chart]**: Show the distribution ratio of each application.
- **[Top 10 of Application Flow]**: List the top 10 applications with the most usage in the past 24 hours. Clicking on any application type prompts the system to analyze and display its traffic distribution within the 24-hour period. (See Figure 16-4)

  By clicking the **Detail** icon for any application, more in-depth statistics are shown.

For example, selecting SSH will prompt the 3100-6GT-I to display a breakdown of source or destination IP addresses that used SSH during the past 24 hours, along with the port usage distribution. (See Figure 16-4)

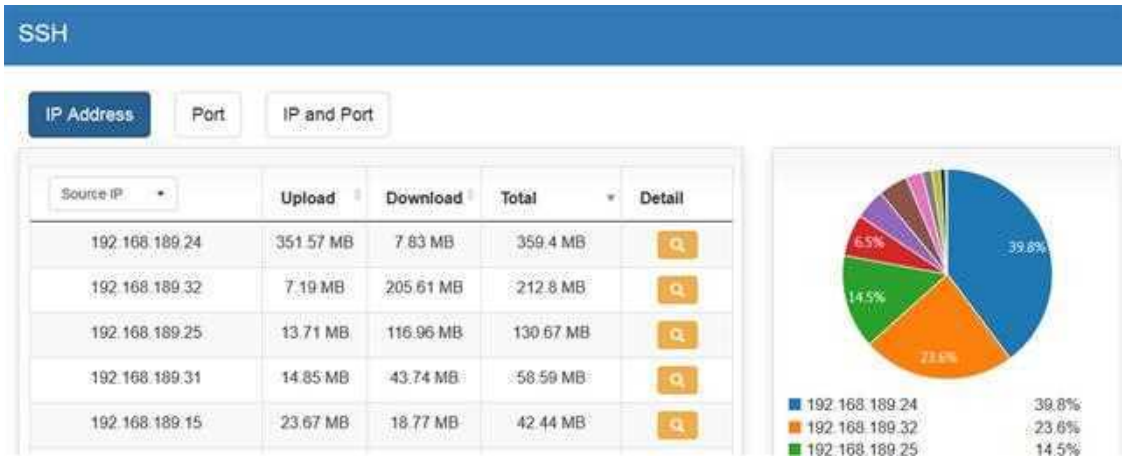


Figure 16-4

Clicking the **Detail** icon next to any IP address further displays the destination addresses that the selected source IP accessed using SSH, along with the corresponding traffic volume for each connection. (See Figure 16-5)

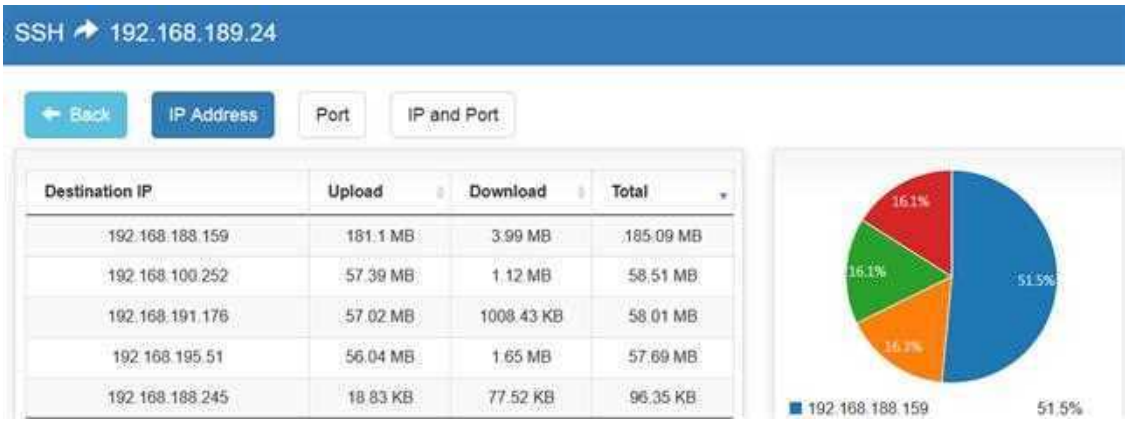


Figure 16-5

- **[Top 10 of IP Address Flow]**: List the top 10 source or destination IP addresses with the largest usage over the past 24 hours. Clicking on any IP address prompts the system to analyze that IP's traffic distribution during the selected period.

  This feature functions similarly to the application-based query, but the analysis is based on **source or destination IP addresses** instead. For example, for source IP address 192.168.188.126, the system will display which applications were used in the past 24 hours and how much traffic each application generated.

16-3. Sessions

The 3100-6GT-I displays all real-time sessions currently passing through the device. Sessions are categorized by **application type**, and the system provides real-time statistics for the number of connections per **source IP address**.

This feature is particularly useful for identifying users with abnormal connection behavior in real time. (See Figure 16-6)

- **[Pie Chart]**: Displays the distribution ratio of real-time sessions, categorized by **application** and **number of connections**.

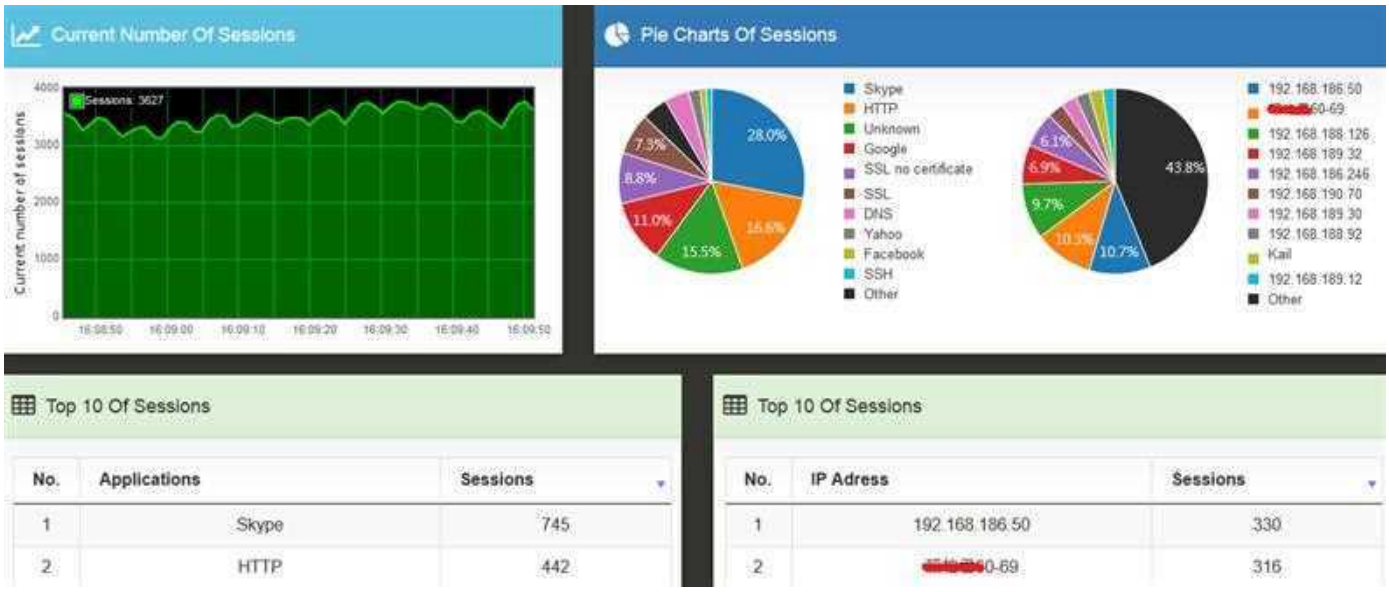


Figure 16-6

16-4. Defense

To view the statistics of **Defense**, the following actions need to be confirmed in advance:

1. **[Other items]** in **[Object] > [Firewall Protection]** must be checked.
2. By default, the system logs and analyzes attacks targeting the local device. When administrators use the **[Policy]** interface for user access to the network, and one of the regulations applies firewall protection settings, the Dashboard will also count these records.

After meeting above two conditions, the 3100-6GT-I will automatically perform statistical analysis. (See Figure 16-7)

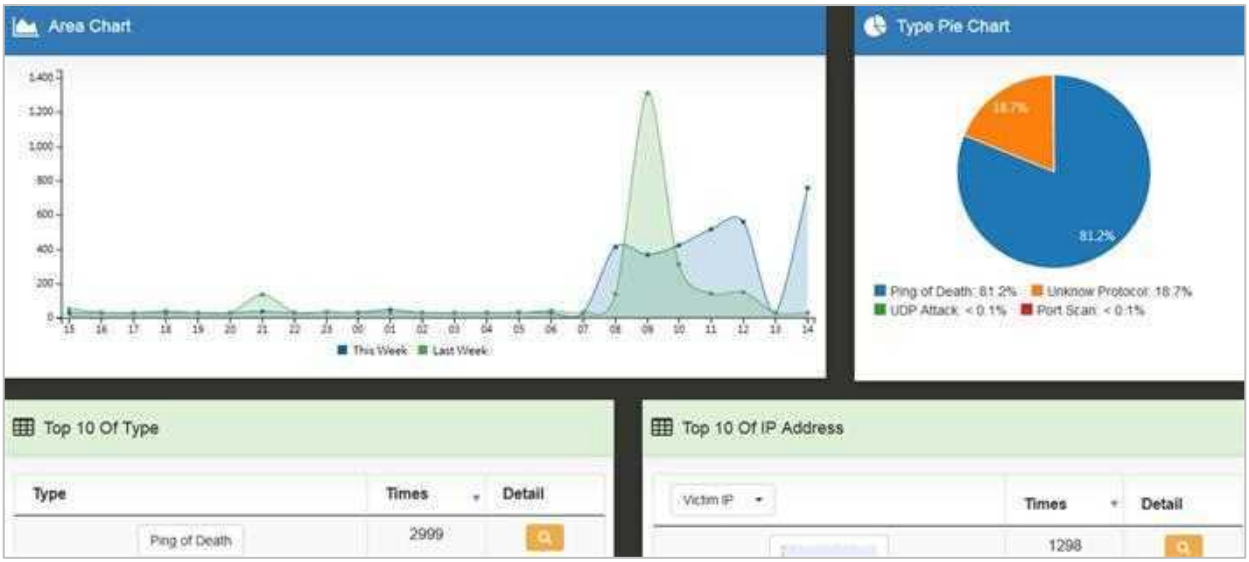


Figure 16-7

- **[Pie Chart]**: Displays the distribution ratio of attack types, categorized by the nature of the attack.
- **[Top 10]**: Includes two ranking categories — **Source IP** and **Destination IP**. Clicking the **Detail** icon allows further drill-down into more specific information. (See Figure 16-8)

Figure 16-8

16-5. OPC

To view OPC statistics, the following actions need to be confirmed in advance:

1. The **"Log"** function in **[OPC] > [OPC Settings]** must be enabled.
2. In the **[Policy]** interface for user access to the network, there must be one policy applied to OPC settings.

After meeting the above two conditions, the 3100-6GT-I will automatically perform statistical analysis. (See Figure 16-9)

Figure 16-9

- **[Pie Chart]**: Displays the distribution of OPC threat signatures categorized by **risk level** — **High**, **Medium**, and **Low**.
- **[Top 10]**: Includes two categories — **Source IP** and **Destination IP**. Clicking the **Detail** icon allows further drill-down into more specific information. (See Figure 16-10)

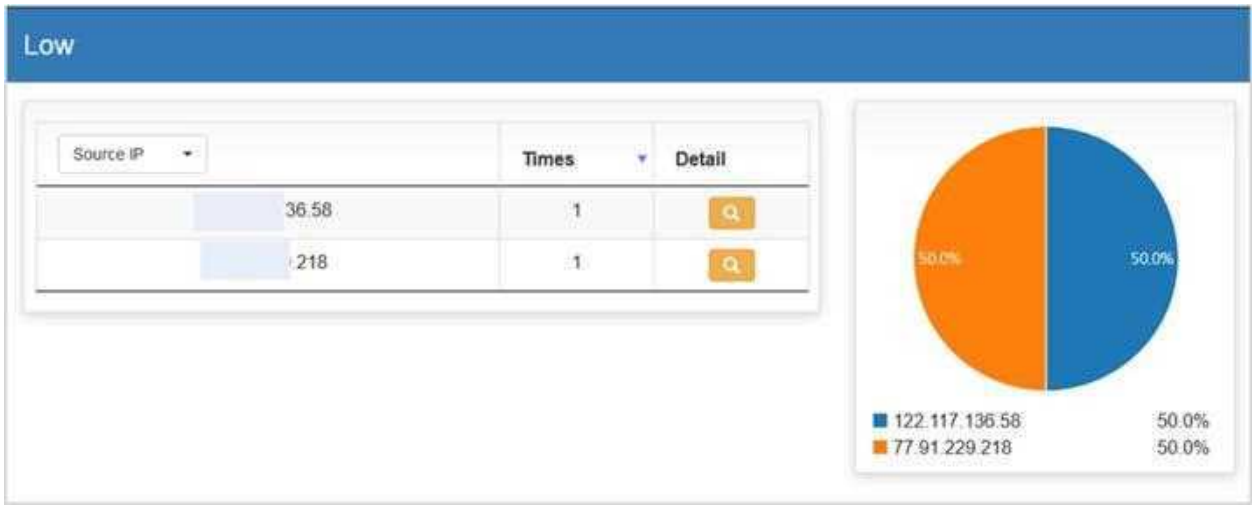


Figure 16-10

16-6. Web Control

To view Web Control statistics, the following needs to be confirmed:

1. The **[Policy]** interface for user access to the network must have one policy with the **WEB(S)** option checked.

After meeting this condition, the 3100-6GT-I will automatically perform statistical analysis. (See Figure 16-11)

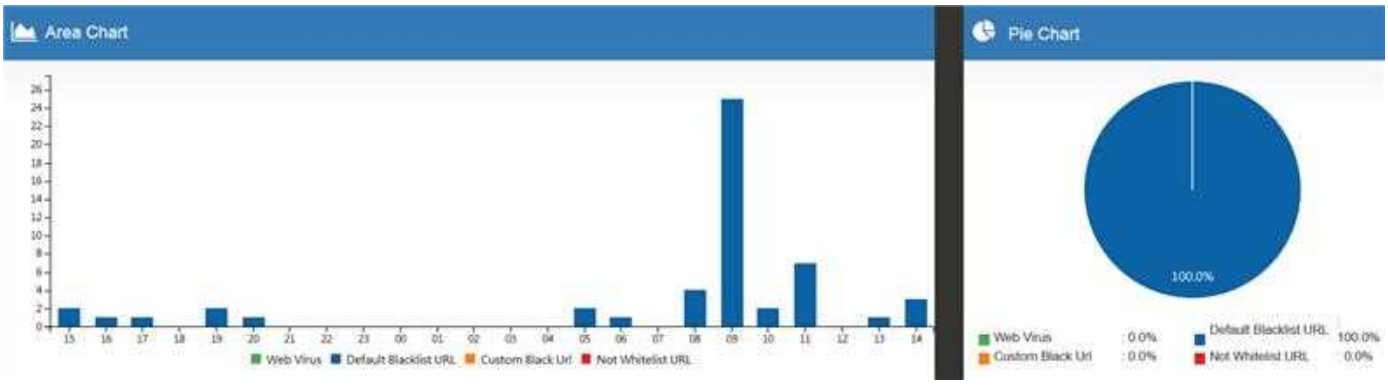


Figure 16-11

- **[Pie Chart]**: Displays statistics based on Web (including both HTTP and HTTPS) URLs triggering the blacklist database or malicious programs.

16-7. Mail

To view Mail statistics, the following needs to be confirmed:

1. [Mail Security] > [Filter & Log] > [SMTP Log Settings] > [Action for Spam Mail] must have one option enabled. If administrators prefer not to change the existing mechanism but only want to analyze it, they can select “Data analysis only.”
2. In the **[Policy]** interface for user access to the network, there must be one policy with SMTP logging enabled.

After meeting the above 2 conditions, the 3100-6GT-I will automatically perform statistical analysis. (See Figure 16-12)

Figure 16-12

- **[Area Chart]**: Summarize all mail traffic entering and leaving the 3100-6GT-I over the past 24 hours, displaying statistics for normal mail, spam, virus-infected mail, failed connections, and rejected connections. Clicking on each hourly statistic will display the distribution of mail usage for that hour. Further clicking on each mail item allows for detailed usage tracking. (See Figure 16-13)

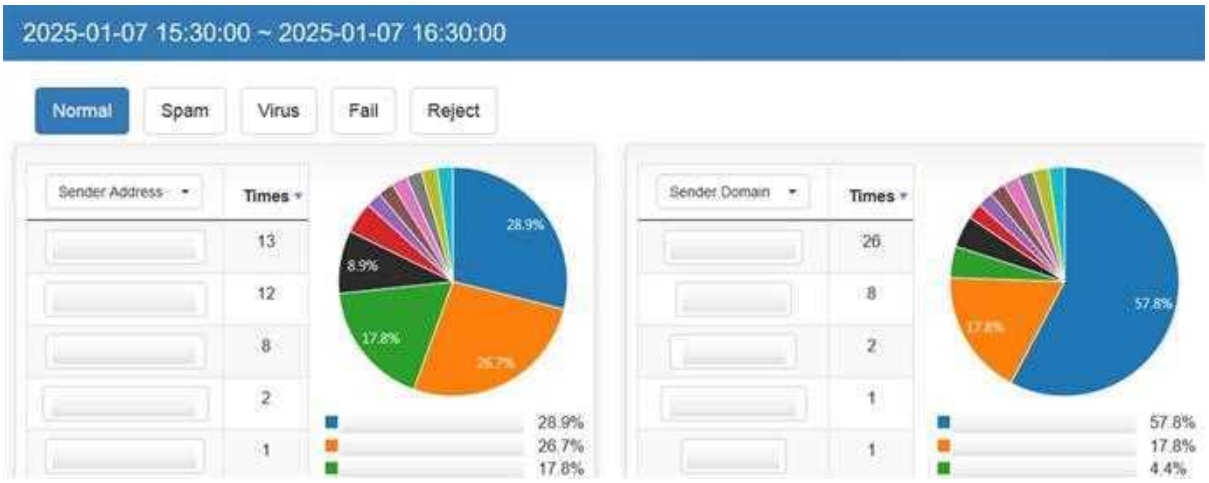


Figure 16-13

- **[Pie Chart]**: Statistical analysis of five types of mail: normal, spam, virus-infected, failed connections, and rejected connections.

- **[Top 10]**: There are 7 types of Top 10 statistical analyses. Clicking on **Detail** icon allows for further drill-down into more detailed information. The example below presents the sending time, subject, size, and other details of emails exchanged between internal and external accounts. (See Figure 16-14)

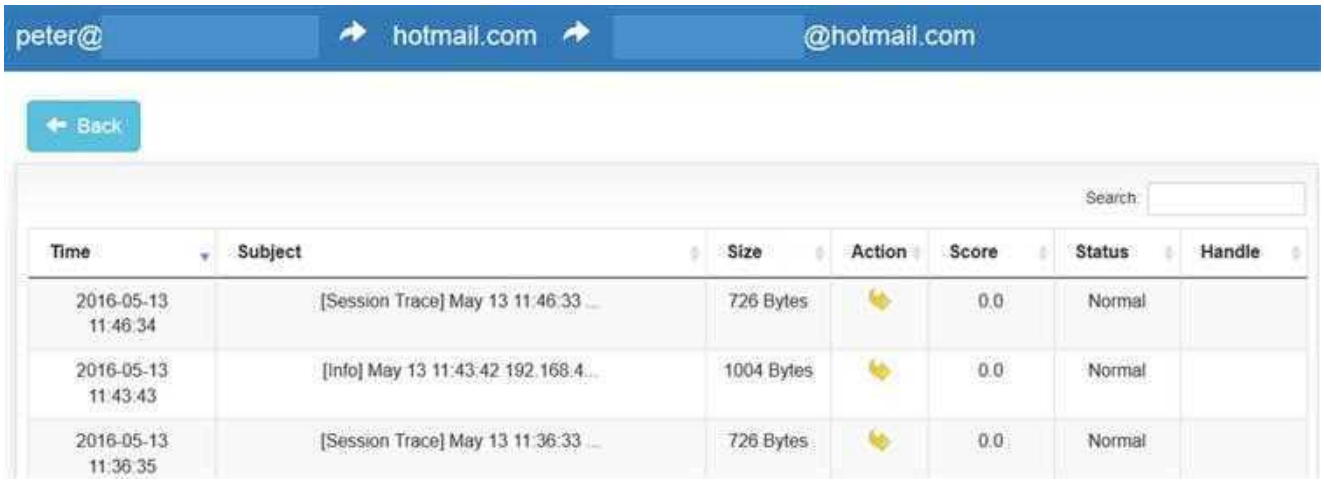


Figure 16-14

16-8. Statistics

Allows administrators to manually set query conditions. After clicking **Search**, the system will generate graphical reports based on the specified criteria. (See Figure 16-15)

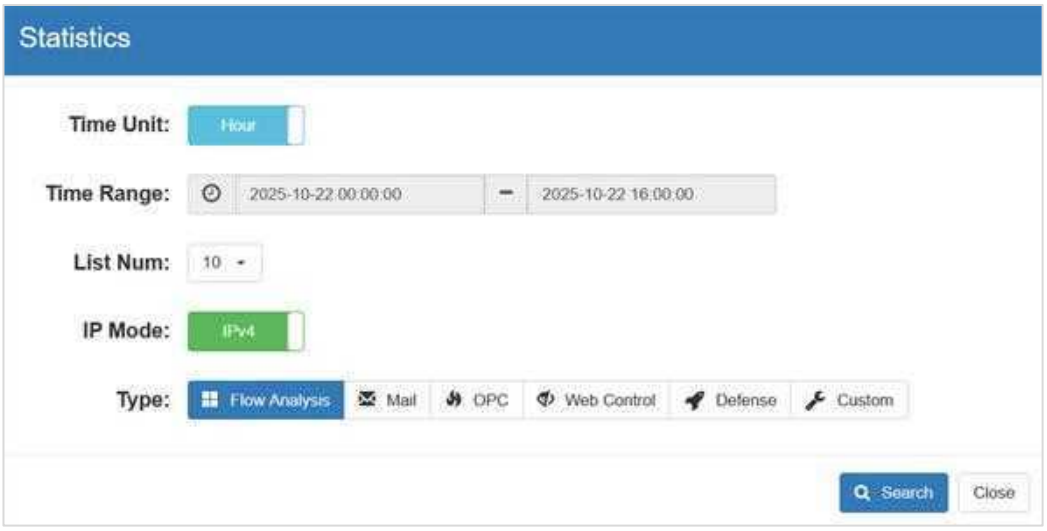


Figure 16-15

16-9. Report

Generates reports based on the collected statistics and allows them to be sent to designated administrators. Configure the **[SMTP Server]** under **[2-6. Notification]**, and then select the account(s) to receive the reports in this section. (See Figure 16-16)

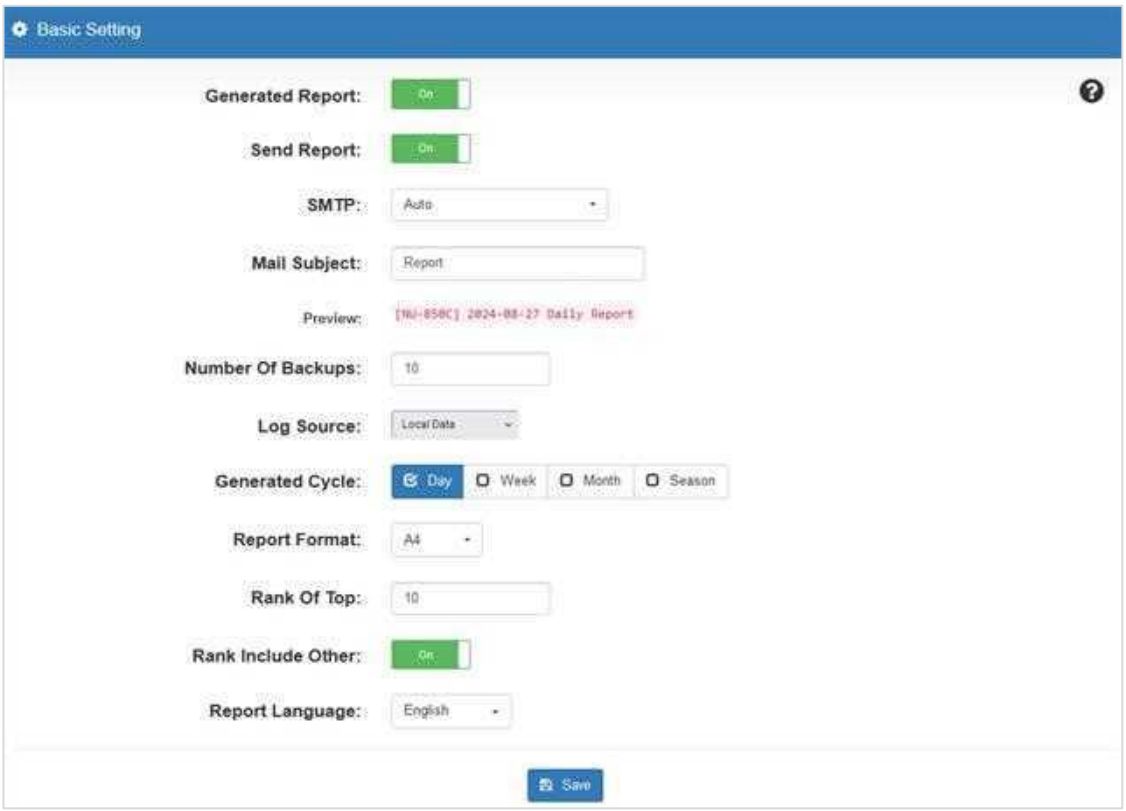


Figure 16-16