Grandstream Networks, Inc.

GWN70xx Series

GWN70xx – User Manual

WELCOME

Grandstream GWN70xx offer secure routers ideal for small offices, home offices and remote workers, the GWN7052/GWN7052F are a dual-band Wi-Fi 5 (802.11ac) routers providing Wi-Fi speeds of up to 1.266 Gbps to a 100 wireless devices, while the GWN7062 is a dual-band Wi-Fi 6 (802.11ax) router with DL/UL OFDMA technology. It features a powerful 64-bit 1.2GHz quad-core processor to provide blazing fast Wi-Fi speeds up to 1.77 Gbps with 4 times increased data capacity to 256 wireless devices. The GWN70xx routers can power smart offices, and allow smooth 4K Ultra HD streaming, web meetings, video conferences, and more. They support enterprise-grade security features to ensure secure Wi-Fi and VPN access, they also include a built-in controller embedded within the product's web user interface. By combining accelerated Wi-Fi speeds, mesh networking and wired AP connections with advanced features including VPN and advanced QoS, Grandstream GWN70xx are the ideal routers for a growing home and business network.

> Changes or modifications to these products not expressly approved by Grandstream, or operation of these products in any way other than as detailed by this User Manual, could void your manufacturer warranty.

> Please do not use a different power adaptor with the GWN70xx routers as it may cause damage to the products and void the manufacturer warranty.

PRODUCT OVERVIEW

Technical Specifications

○ **GWN7052/GWN7052F**

	GWN7052	GWN7052F
Memory and NAT Sessions	● 128MB RAM ● 30K NAT sessions	● 256MB RAM ● 60K NAT sessions
NAT Routing & IPSec VPN Performance	● 1Gbps NAT routing ● 300Mbps IPSec VPN performance	
Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac	
Antennas	4 individual external antennas, 2 per band ● 2.4GHz, gain 5.0dBi ● 5 GHz, gain 5.0dBi	
Wi-Fi Data Rates	**5G:** IEEE 802.11ac: 6.5 Mbps to 867 Mbps IEEE 802.11n: 6.5 Mbps to 300 Mbps IEEE 802.11a: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **2.4G:** IEEE 802.11n: 6.5 Mbps to 300 Mbps IEEE 802.11b: 1, 2, 5.5, 11 Mbps IEEE 802.11g: 6, 9, 12, 18, 24, 36, 48, 54 Mbps **Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network*	
Frequency Bands	● **2.4GHz radio:** 2400 – 2483.5MHz ● **5GHz radio:** 5150 - 5850MHz	

	**Not all frequency bands can be used in all regions*	
Channel Bandwidth	● **2.4G:** 20 and 40 MHz ● **5G:** 20, 40 and 80 MHz	
Wi-Fi and System Security	WPA/WPA2-PSK, WPA/WPA2 Enterprise (TKIP/AES); WPA3, anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device	
MIMO	● 2×2:2 **2.4GHz** ● 2×2:2 **5GHz**	
Maximum TX Power	● **2.4G**: 23dBm ● **5G**: 24dBm **Maximum power varies by country, frequency band and MCS rate*	
Receiver Sensitivity	**2.4G** ● **802.11b:** -96dBm@1Mbps, -88dBm@11Mbps; ● **802.11g:** -93dBm @6Mbps, -75dBm@54Mbps; ● **802.11n 20MHz:** -73dBm @MCS7; **802.11n 40MHz:** -70dBm @MCS7; **5G** ● **802.11a:** -92dBm @6Mbps, -74dBm @54Mbps; ● **802.11n 20MHz**: -73dBm @MCS7; **802.11n 40MHz:** -70dBm @MCS7 ● **802.11ac 20MHz:** -67dBm@MCS8; **802.11ac HT40**: -63dBm @MCS9; **802.11ac 80MHz:** -59dBm @MCS9;	
SSIDs	16 SSIDs total **8 per radio (**2.4ghz** and **5ghz**)*	
Concurrent Clients	Up to 100 concurrent clients	
Network Interfaces	● 1x Gigabit Ethernet WAN port ● 4x Gigabit Ethernet LAN ports	● 1x Gigabit SFP WAN port ● 1x Gigabit Ethernet port (WAN/LAN configurable) ● 3x Gigabit Ethernet LAN ports
Auxiliary Ports	● 1x USB 2.0 port ● 1x Reset Pinhole	
Mounting	● Desktop ● Wall mounting	
LEDs	● 1 tri-color LED ● 7x single-color LEDs for device tracking and status indication	
Network Protocols	IPv4, IPv6, 802.1Q, 802.1p, 802.1x, 802.11e/WMM	
QoS	802.11e/WMM, VLAN, TOS	
Firewall	DDNS, Port Forwarding, DMZ, UPnP, Anti-DoS, traffic rules, NAT, ALG	
VPN	● **Client:** L2TP, PPTP, IPSec, ● **OpenVPN Server:** IPSec, OpenVPN	
Network Management	GWN7052 embedded controller can manage itself and **up to 30 GWN APs**; GWN.Cloud offers a free cloud management platform for unlimited GWN7052 routers and GWN APs	GWN7052F embedded controller can manage itself and **up to 50 GWN APs**; GWN.Cloud offers a free cloud management platform for unlimited GWN7052F routers and GWN APs

Power & Green Energy Efficiency	Universal power adaptor included: Input 100-240VAC 50-60Hz Output: 12VDC 1A (12W);
Environmental	Operation: 0°Cto 50°C Storage: -10°C to 60°C Humidity: 10% to 90% Non-condensing
Physical	● **Unit Dimension without antennas:** 205mm(L)x130mm(W)x35.5mm(H) ● **Unit Dimension with antennas of 90°:** 235.5mm(L)x145mm(W)x192mm(H); Unit Weight: 375g ● **Entire Package Dimension:** 250mm(L)x251.5mm(W)x56mm(H); Entire Package Weight: 740g
Package Content	● GWN7052/GWN7052F Router ● Universal Power Supply ● Network Cable ● Quick Installation Guide

Table 1: GWN7052/GWN7052F Technical Specifications

○ **GWN7062**

Wi-Fi Standards	IEEE 802.11 a/b/g/n/ac/ax
Antennas	4 individual internal antennas, 2 per band ● **2.4GHz:** maximum gain 4.5dBi ● **5 GHz:** maximum gain 5dBi
Wi-Fi Data Rates	**5G:** ● **IEEE 802.11ax:** 7.3 Mbps to 1201 Mbps ● **IEEE 802.11ac:** 6.5 Mbps to 867 Mbps ● **IEEE 802.11n:** 6.5 Mbps to 300 Mbps ● **IEEE 802.11a:** 6, 9, 12, 18, 24, 36, 48, 54 Mbps **2.4G:** ● **IEEE 802.11ax:** 7.3 Mbps to 573.5 Mbps ● **IEEE 802.11n**: 6.5 Mbps to 300 Mbps ● **IEEE 802.11b:** 1, 2, 5.5, 11 Mbps ● **IEEE 802.11g:** 6, 9, 12, 18, 24, 36, 48, 54 Mbps **Actual throughput may vary depending on many factors including environmental conditions, distance between devices, radio interference in the operating environment and mix of devices in the network*
Frequency Bands	● **2.4GHz radio:** 2400 – 2483.5 MHz *(2412-2472MHz are channel central frequency range; 2400-2483.5MHz is Frequency band)* ● **5GHz radio:** 5150 - 5850 MHz **Not all frequency bands can be used in all regions*
Channel Bandwidth	● **2.4G:** 20 and 40 MHz ● **5G:** 20, 40 and 80 MHz
Wi-Fi and System Security	WPA/WPA2-PSK, WPA/WPA2 Enterprise (TKIP/AES); WPA3, anti-hacking secure boot and critical data/control lockdown via digital signatures, unique security certificate and random default password per device
MIMO	● 2×2:2 **2.4GHz** ● 2×2:2 **5GHz**

Coverage Range	Up to 175 meters **coverage range can vary based on environment*
Maximum TX Power	● **5G:** 26dBm ● **2.4G:** 27dBm **Maximum power varies by country, frequency band and MCS rate*
Receiver Sensitivity	**2.4G** ● **802.11b:** -96dBm@1Mbps, -88dBm@11Mbps; ● **802.11g:** -93dBm @6Mbps, -75dBm@54Mbps; ● **802.11n 20MHz:** -73dBm @MCS7; **802.11n 40MHz:** -70dBm @MCS7; ● **802.11ax 20MHz:** -64dBm @ MCS11; **802.11ax 40MHz:** -63dBm @MCS11 **5G** ● **802.11a:** -93dBm @6Mbps, -75dBm @54Mbps; ● **802.11n 20MHz:** -73dBm @MCS7; **802.11n 40MHz:** -70dBm @MCS7 ● **802.11ac 20MHz:** -70dBm @MCS8; **802.11ac HT40:**- 66dBm @MCS9; **802.11ac 80MHz:** -62dBm @MCS9; ● **802.11ax 20MHz:** -64dBm @ MCS11; **802.11ax 40MHz**: -61dBm @MCS11; **802.11ax 80MHz:** -58dBm @MCS11
SSIDs	32 SSIDs total **16 per radio (**2.4GHz** & **5GHz**)*
Concurrent Wireless Clients	Up to 256 wireless clients
Network Interfaces	● 1x Gigabit Ethernet WAN port ● 1x Gigabit Ethernet port (WAN/LAN configurable) ● 3x Gigabit Ethernet LAN ports
Auxiliary Ports	● 1x USB 3.0 port ● 1x Reset button ● 1x SYNC button
Mounting	Desktop
LEDs	● 1 tri-color LED ● 7 single-color LEDs for device tracking and status indication
Network Protocols	IPv4, IPv6, 802.1Q, 802.1p, 802.1x, 802.11e/WMM
QoS	802.11e/WMM, VLAN, TOS
Firewall	DDNS, Port Forwarding, DMZ, UPnP, Anti-DoS, traffic rules, NAT, ALG
VPN	● **Client:** L2TP, PPTP, IPSec, OpenVPN ● **Server:** IPSec, OpenVPN
Network Management	GWN7062 embedded controller can manage it self and up to 50 GWN Aps GWN.Cloud offers a free cloud management platform for unlimited GWN7062 routers and GWN APs
Power and Green	Universal power adaptor included:

Energy Efficiency	Input 100-240VAC 50-60Hz Output: 12VDC 1.5A (18W);
Environmental	Operation: 0°Cto 50°C Storage: -30°C to 60°C Humidity: 10% to 90% Non-condensing
Physical	● **Unit Dimension:** 95mm(L)x95mm(W)x193mm(H) ● **Unit Weight:** 690g ● **Entire Package Dimension:** 286mm(L)x126.5mm(W)x105mm(H) ● **Entire Package Weight:** 960g
Package Content	● GWN7062 Router ● Universal Power Supply ● Network Cable ● Quick Installation Guide
Compliance	FCC, CE, RCM, IC, UKCA

Table 2: GWN7062 Technical Specifications

INSTALLATION

Before deploying and configuring the GWN70xx router, the device needs to be properly powered up and connected to the network. This section describes detailed information on the installation, connection, and warranty policy of the GWN70xx router.

Package Contents

○ **GWN7052/GWN7052F**

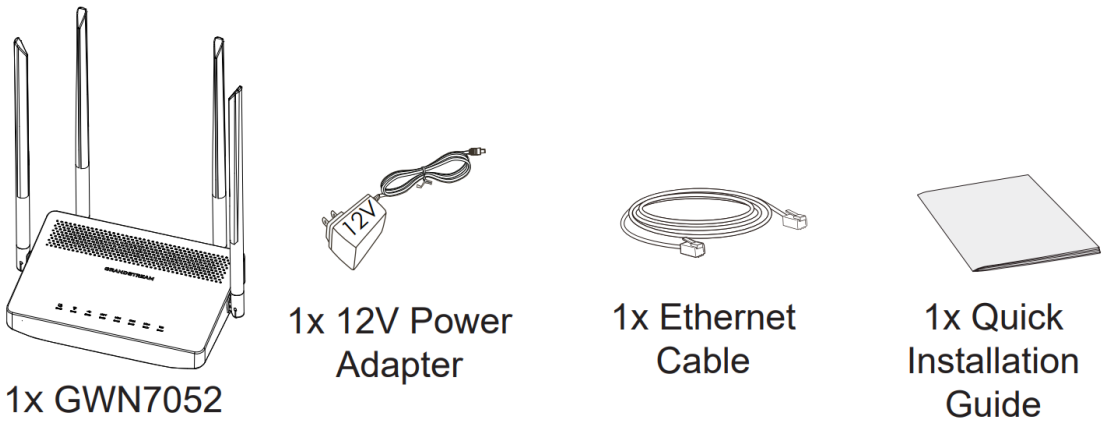

Figure 1: GWN7052/GWN7052F Package Contents

○ **GWN7062**

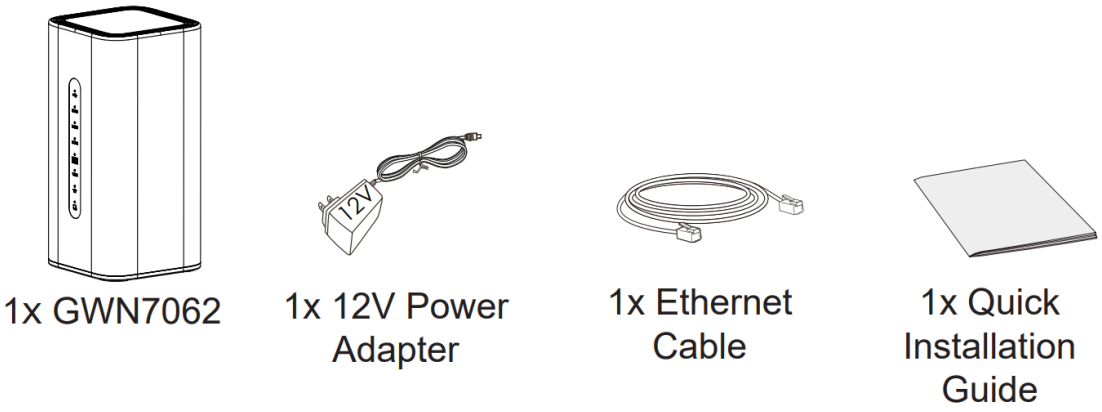

Figure 2: GWN7062 Package Contents

GWN70xx Ports

○ **GWN7052**

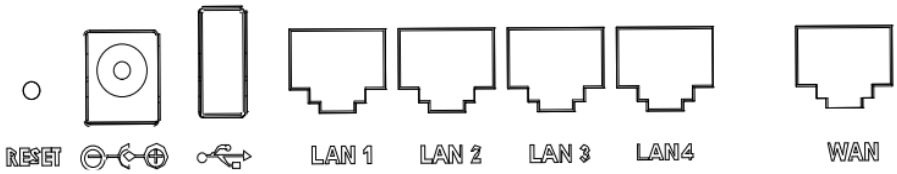

Figure 3: GWN7052 Ports

○ **GWN7052F**

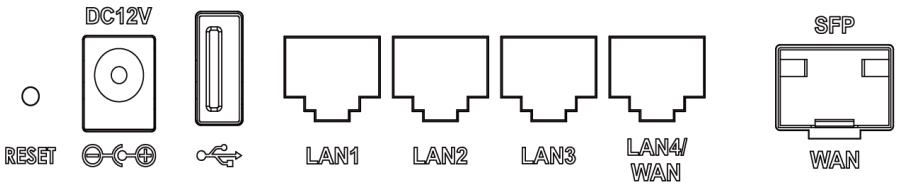

Figure 4: GWN7052F Ports

○ **GWN7062**

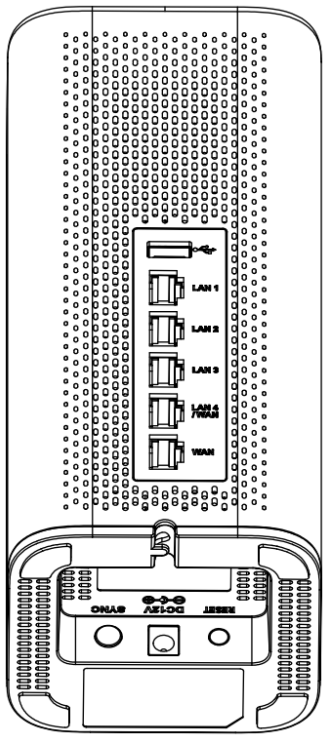

Figure 5: GWN7062 Ports

Powering and Connecting GWN70xx

○ **GWN7052/GWN7052F**

1. Power the GWN7052/GWN7052F

GWN7052/GWN7052F can be powered on using the right PSU (DC 12V, 1A).

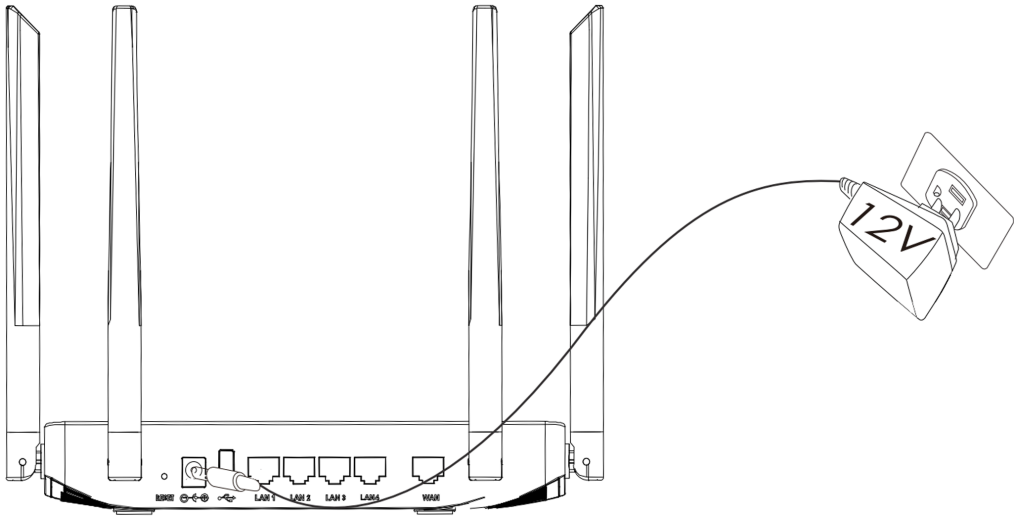

Figure 6: the back of GWN7052

2. Connect to the Internet

Connect the WAN port to an optical fiber broadband modem (through SFP Module), ADSL broadband modem, or community broadband interface.

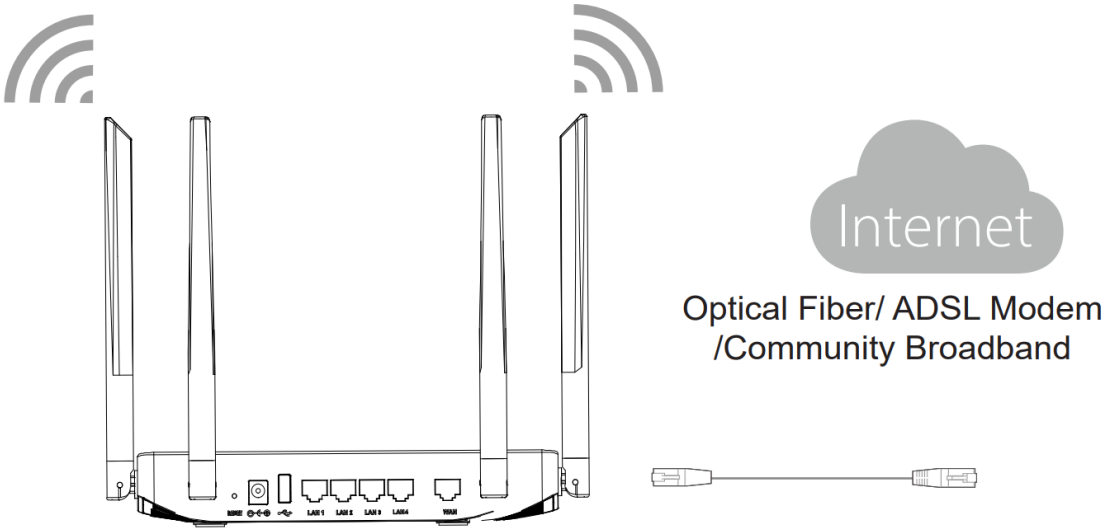

Figure 7: GWN7052 connect

3. Connect to the Default Network

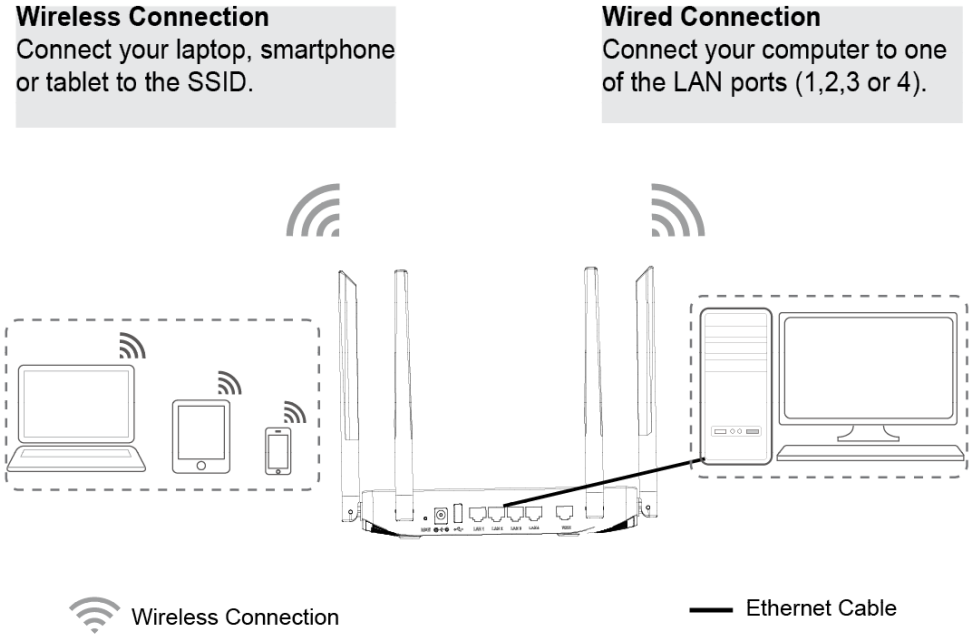

Figure 8: GWN7052 default network

○ **GWN7062**

1. Power the GWN7062

GWN7062 can be powered on using the right PSU (DC 12V, 1.5A).

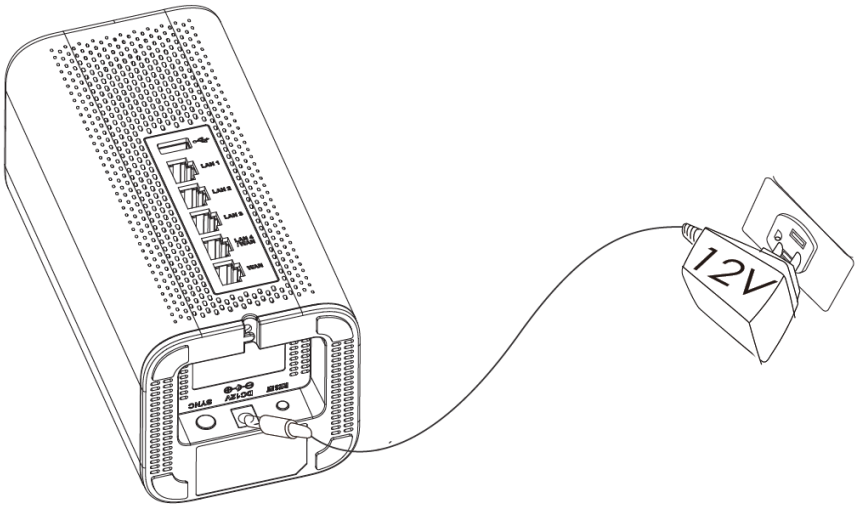

Figure 9: the back of GWN7062

2. Connect to the Internet

Connect the WAN port to an optical fiber broadband modem, ADSL broadband modem, or community broadband interface.

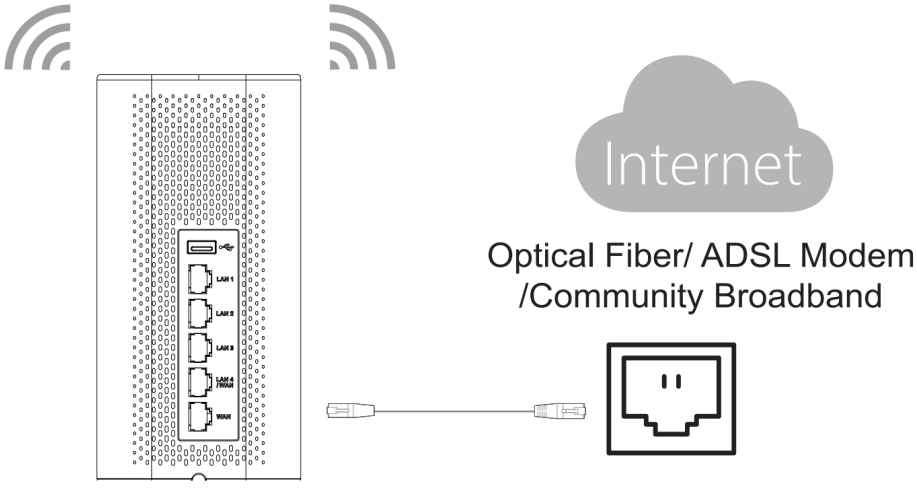

Figure 10: GWN7062 connect

3. Connect to GWN7062 Default Network

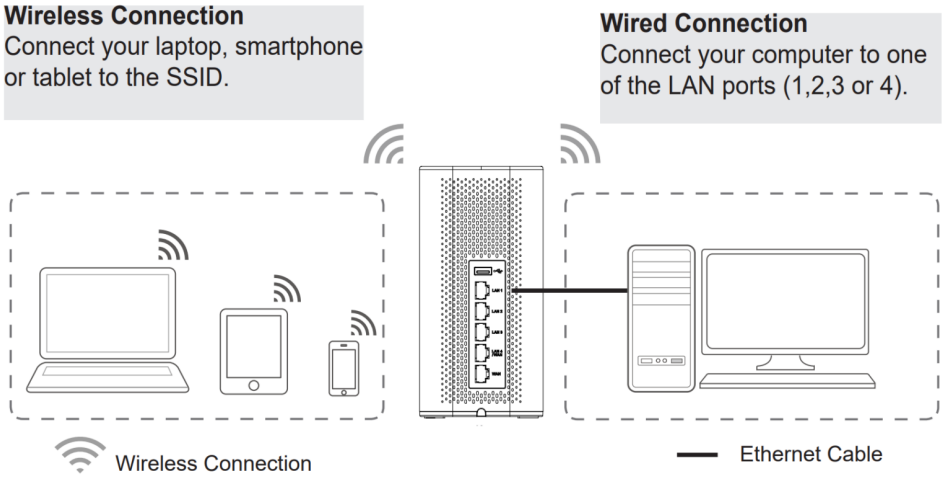

Figure 11: GWN7062 default network

SSID's default password information is printed on the MAC tag at the bottom of the unit.

Safety Compliances

The GWN70xx Dual-Band Wi-Fi Router complies with FCC/CE and various safety standards. The GWN70xx power adapter is compliant with the UL standard. Use the universal power adapter provided with the GWN70xx package only. The manufacturer's warranty does not cover damages to the device caused by unsupported power adapters.

Warranty

If the GWN70xx Dual-Band Wi-Fi Router was purchased from a reseller, please contact the company where the device was purchased for replacement, repair or refund. If the device was purchased directly from Grandstream, contact our Technical Support Team for an RMA (Return Materials Authorization) number before the product is returned. Grandstream reserves the right to remedy the warranty policy without prior notification.

GETTING STARTED

The GWN70xx Dual-Band Wi-Fi Routers provide an intuitive web GUI configuration interface for easy management to give users access to all the configurations and options for the GWN70xx's setup.

This section provides step-by-step instructions on how to read LED indicators and use the Web GUI interface of the GWN70xx.

LED Indicators

The front panel of the GWN70xx has LED indicators for power and interface activities, the table below describes the LED indicators' status.

LED	Status	Indication
Power/Provision	Flashing Red	Resetting
	Solid Red	Upgrade failed
	Pink	No Web login after reset
	Green	Powering

	Blue	Normal use
Wi-Fi	Solid Blue	Wi-Fi enabled
	Off	Wi-Fi disabled
WAN	Flashing Blue	Connected as a client to another network and data is transferring
	Off	No network, cable is disconnected
LAN	Flashing Blue	Connected to the corresponding LAN port and data is transferring
	Off	No network, cable is disconnected
USB	Solid Blue	Connected to USB device
	Off	No USB device is connected

Table 3: LED Indicators

Use the WEB GUI

Access WEB GUI

The GWN70xx embedded Web server responds to HTTPS GET/POST requests. Embedded HTML pages allow users to configure the device through a Web browser such as Microsoft IE, Mozilla Firefox, or Google Chrome.

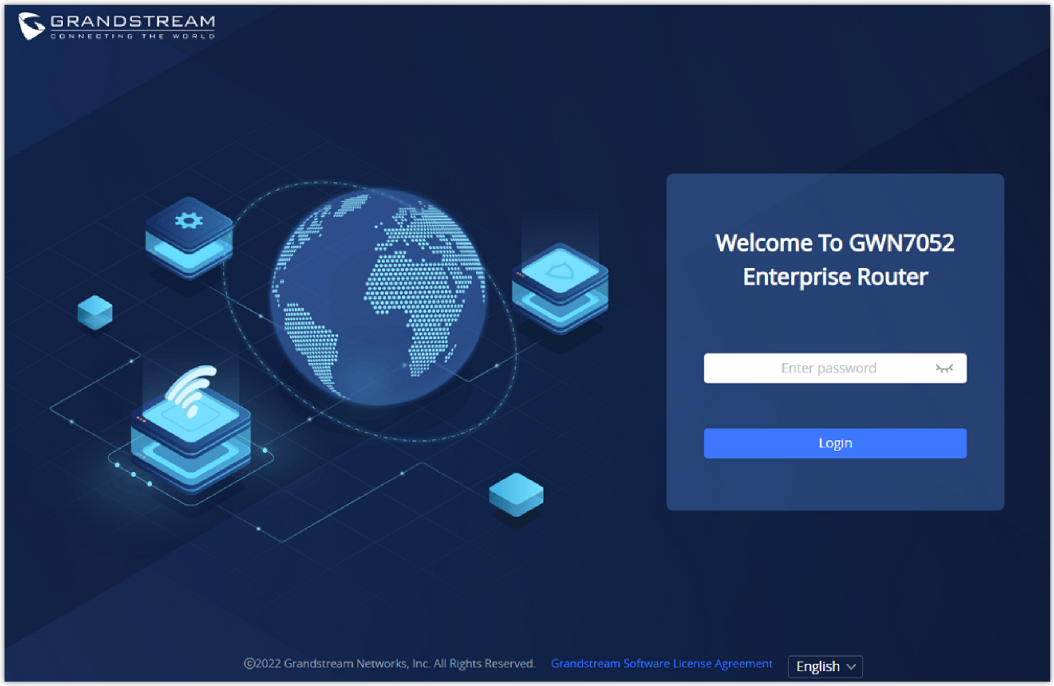

Figure 12: GWN70xx Web GUI Login Page

To access the Web GUI:

1. Connect a computer to a LAN port of the GWN70xx.
2. Ensure the device is properly powered up, and the Power and LAN port LEDs light up in blue.
3. Open a Web browser on the computer and enter the web GUI URL in the following format: https://192.168.80.1 (Default IP address).

4. Enter the administrator's login and password to access the Web Configuration Menu. The default administrator's username is "admin" and the password is the default Wi-Fi SSID Password is printed on the MAC tag at the bottom of the unit.

> At first boot or after factory reset, users will be asked to change the default administrator and user passwords before accessing GWN70xx web interface. The password field is case-sensitive with a maximum length of 32 characters. Using strong passwords including letters, digits, and special characters is recommended for security purposes.

WEB GUI Languages

Currently, the GWN70xx web GUI supports ***English*** and ***Simplified Chinese.***

To change the default language, select the displayed language at the bottom of the web GUI either before or after logging in.

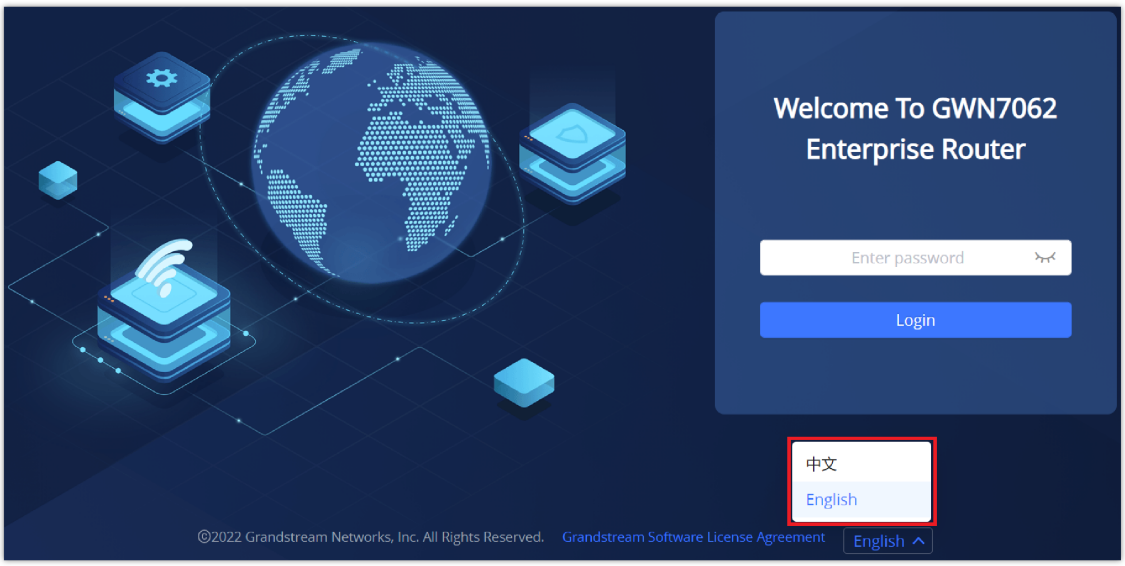

Figure 13: Web GUI Languages – Login Page

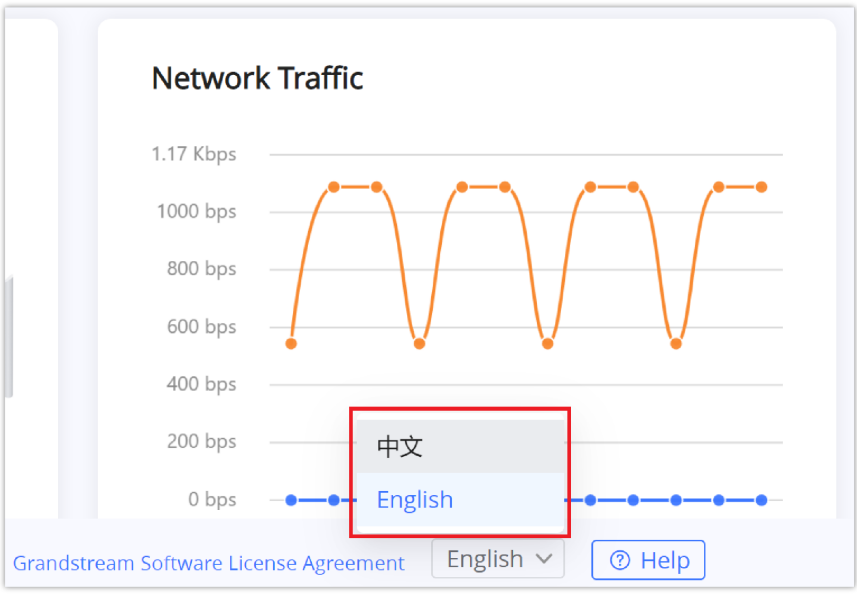

Figure 14: WEB GUI – Start page

WEB GUI Configuration

GWN70xx web GUI includes 13 main sections to configure and manage the router and check the connection status.

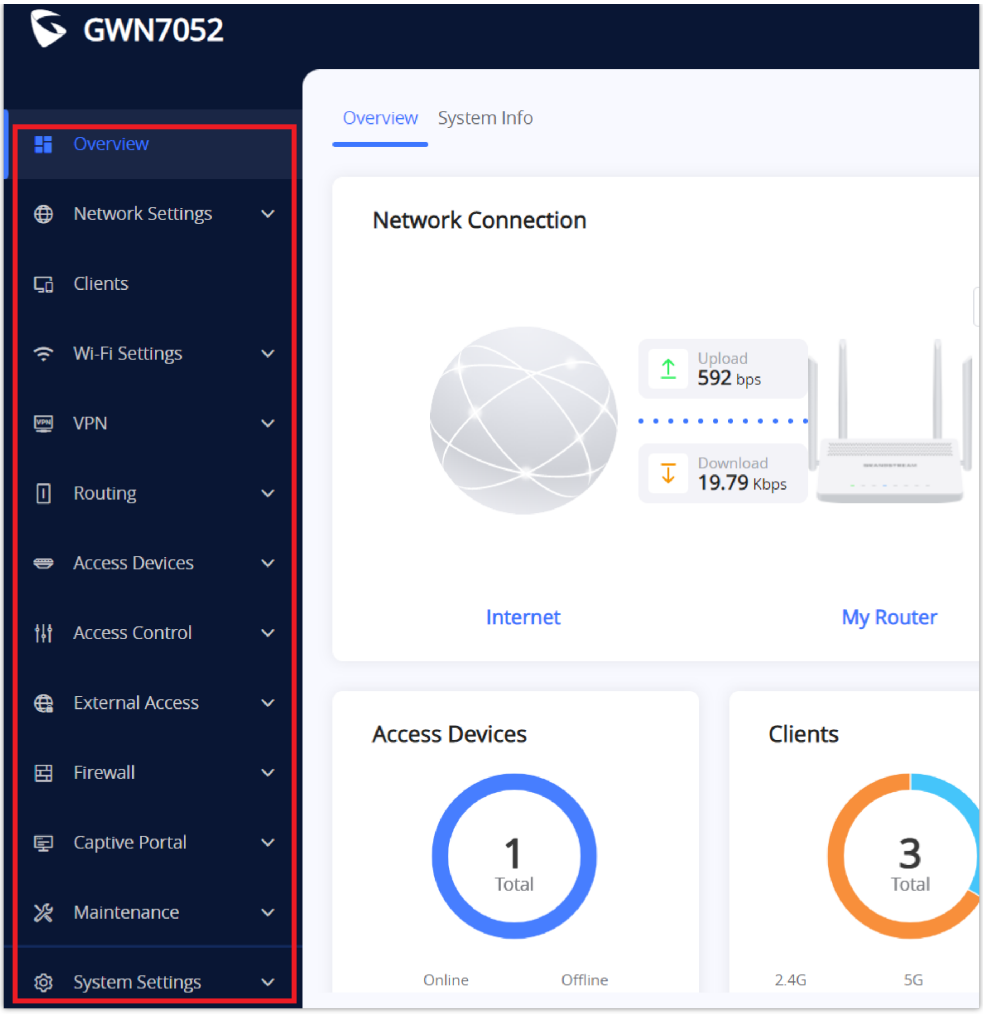

Figure 15: WEB GUI Configuration

Search

In case it's hard to go through every single section, GWN70xx routers have search functionality to help the user find the right configuration, settings or parameters, etc…

On the top of the page, there is a search icon, the user can click on it and then enter the keyword relevant to his search, then he will get all the possible locations of that keyword.

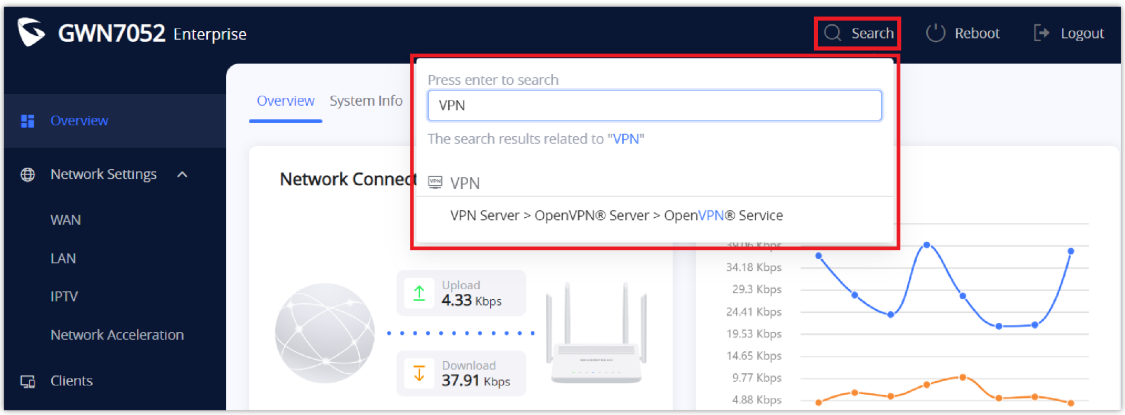

Figure 16: Search

Setup Wizard and Feedback

In case the user confronted an issue with GWN70xx or has feedback. At the bottom of the page, there is a help icon Help to set up the router or to send feedback.

Figure 17: Help

Setup Wizard

If the user missed the Setup Wizard at the first boot of GWN70xx. It's accessible all the time at the bottom of the page and it contains the necessary settings that the user must configure in 3 steps, first country and time zone, Internet Settings, and finally SSID settings.

Click on  button to go through the setup wizard.

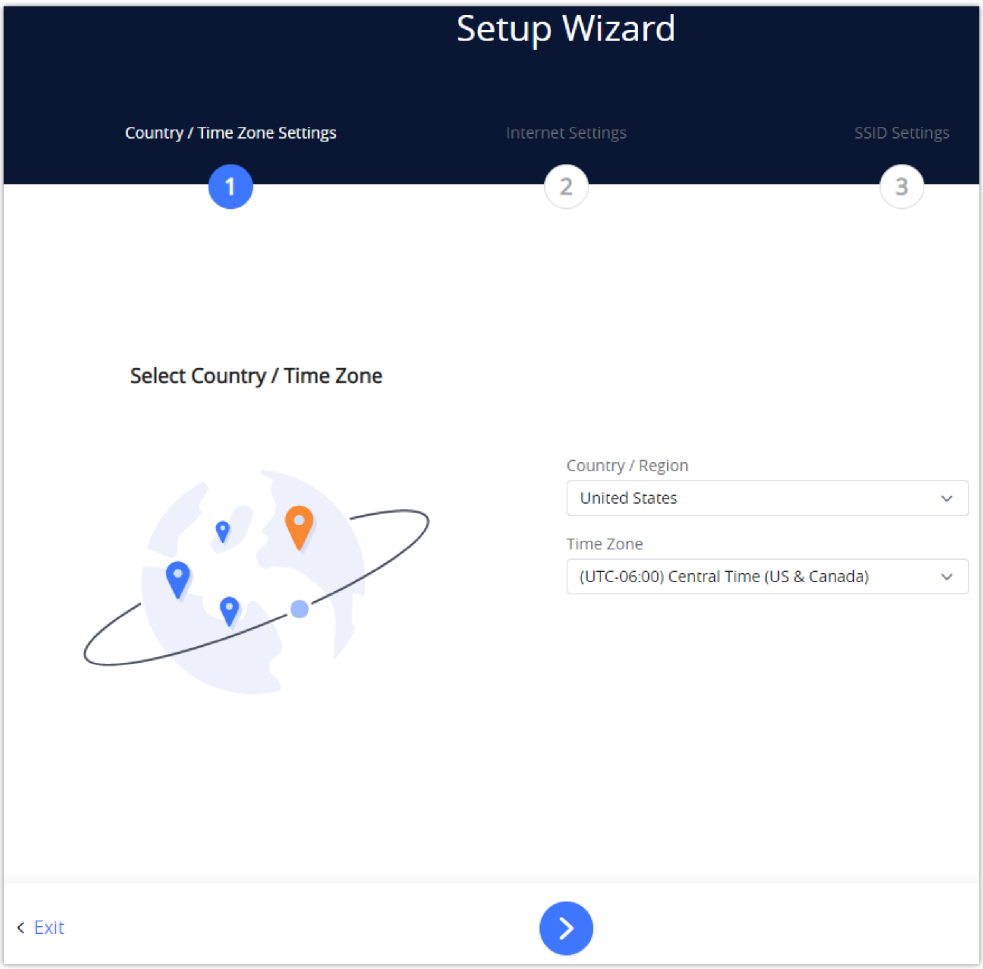

Figure 18: Setup Wizard

Feedback

If the user has a question or a suggestion to make the GWN70xx product even better or has an issue, he can always send feedback, in case of a problem it's better as well to include Syslog as it may help solve the problem faster.

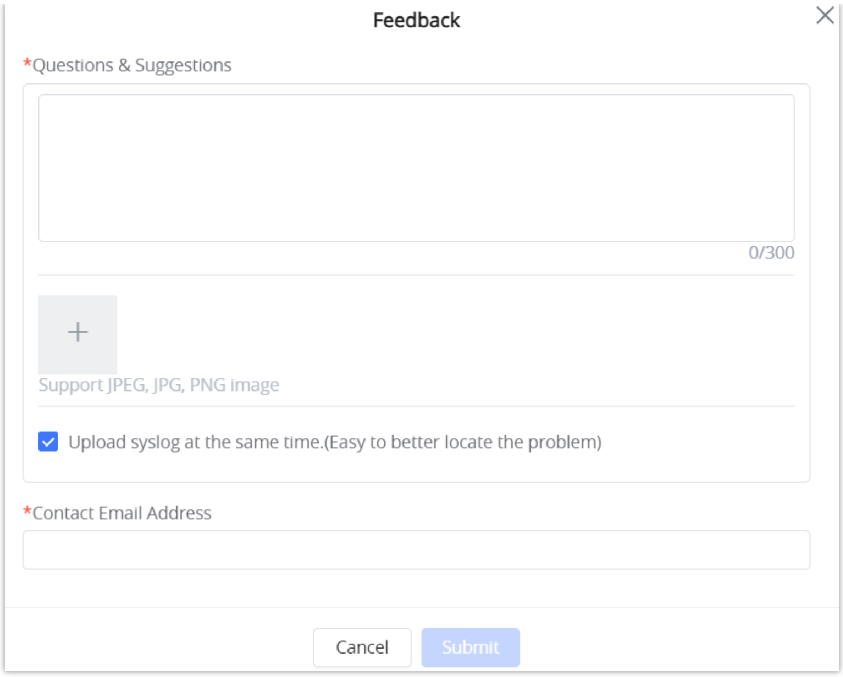

Figure 19: Feedback

Overview Page

Overview is the first page shown after successful login to the GWN70xx's Web Interface. It provides an overall view of the GWN70xx's information presented in a Dashboard style for easy monitoring as well as the System Info (Product Name, System Version, MAC Address ...). It is used to show the status of the GWN70xx for different items like (upload and download speed, number of clients connected, bands used, access devices, network traffic, alerts, top access devices, top SSIDS, and top clients).

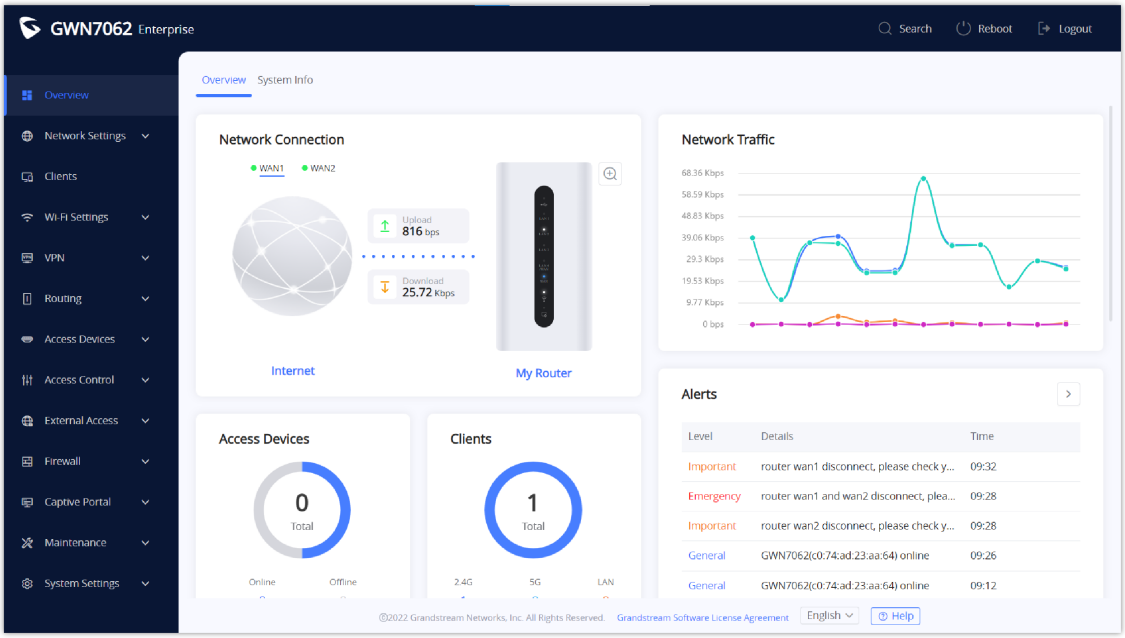

Figure 20: Overview Page

Network Connection	Display the current status of the router, is it connected or not, as well as showing the current upload and downlaod speed.
Network Traffic	Shows network traffic in real time.
Access Devices	shows the total number of Access Devices online and offline.
Clients	Shows the total number of clients connected to 2.4G and 5G as well as the ones connected to the LAN.

Alerts	Shows Alerts General, Important or Emergency with details and time.
Top Access Devices	Shows the Top Access Devices list, assort the list by number of clients connected to each access device including the GWN7052 or data usage combining upload and download. Click on the arrow to go to access Devices page for basic and advanced configuration options.
Top SSIDs	Shows the Top SSIDs list, users may assort the list by number of clients connected to each SSID or data usage combining upload and download. Users may click on to go to SSID page for more options.
Top Clients	Shows the Top Clients list, users may assort the list of clients by their upload or download. Users may click on to go to Clients page for more options.

Table 4: Overview

In addition the user can click on the magnifier icon to check the LED status of the router.

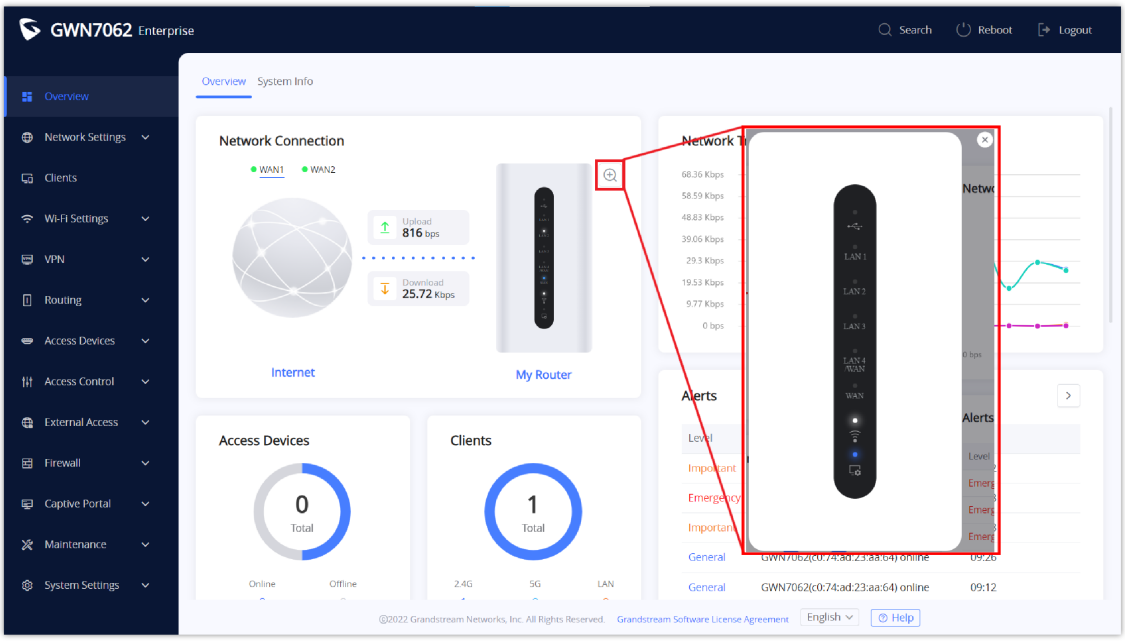

Figure 21: LED status

ROUTER CONFIGURATION

This section includes configuration pages for network WAN ports, LAN ports and shows also the router status.

System Info

System Info displays **Device Status** to check MAC address, Part Number, Firmware related information, and Uptime for the GWN70xx and **WAN Status** showing general information about WAN Port such as IP address and Connection Type.

The router's System Info can be accessed from the **Web GUI → Overview → System Info Tab.**

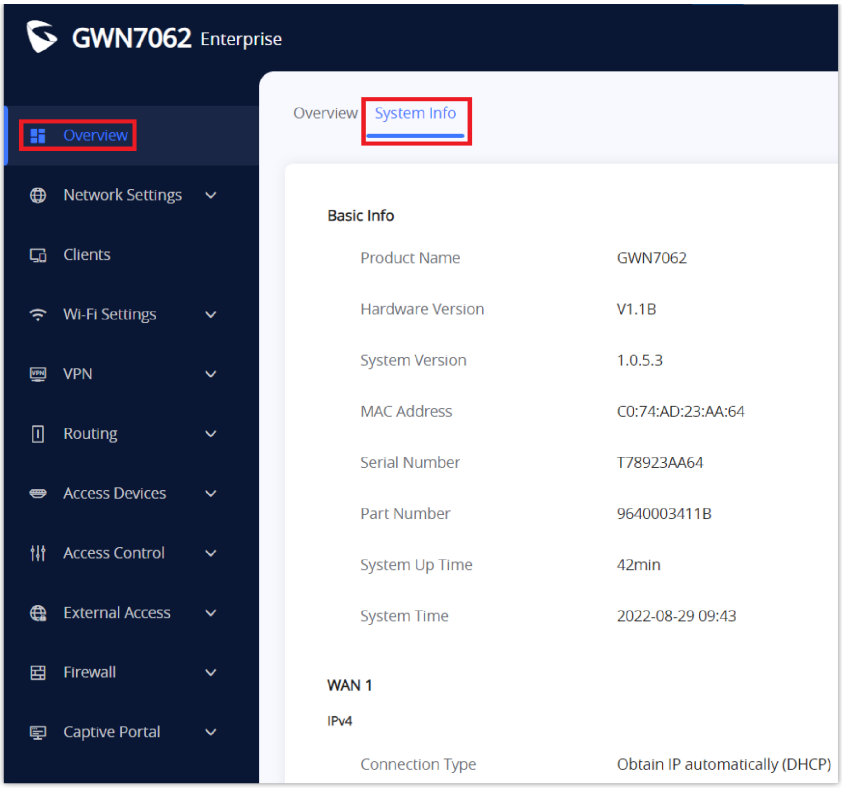

Figure 22: System Info

Router Configuration

Connect to GWN70xx's Web GUI from a computer connected to a LAN port or GWN70xx's Wi-Fi SSID and go to the **Web GUI** → **Network Settings** → **WAN** page for WAN configuration.

WAN Settings

The WAN port can be connected to a DSL modem or a router. WAN port support also setting up static IPv4/IPv6 addresses and configure PPPoE.

> GWN7062 has a port (LAN 4/WAN), by default it's configured as a LAN port. The user can configure this port as a WAN port (WAN 2) and it can be used in a load balancing between WAN 1 and WAN 2.

- **IPv4 Settings**

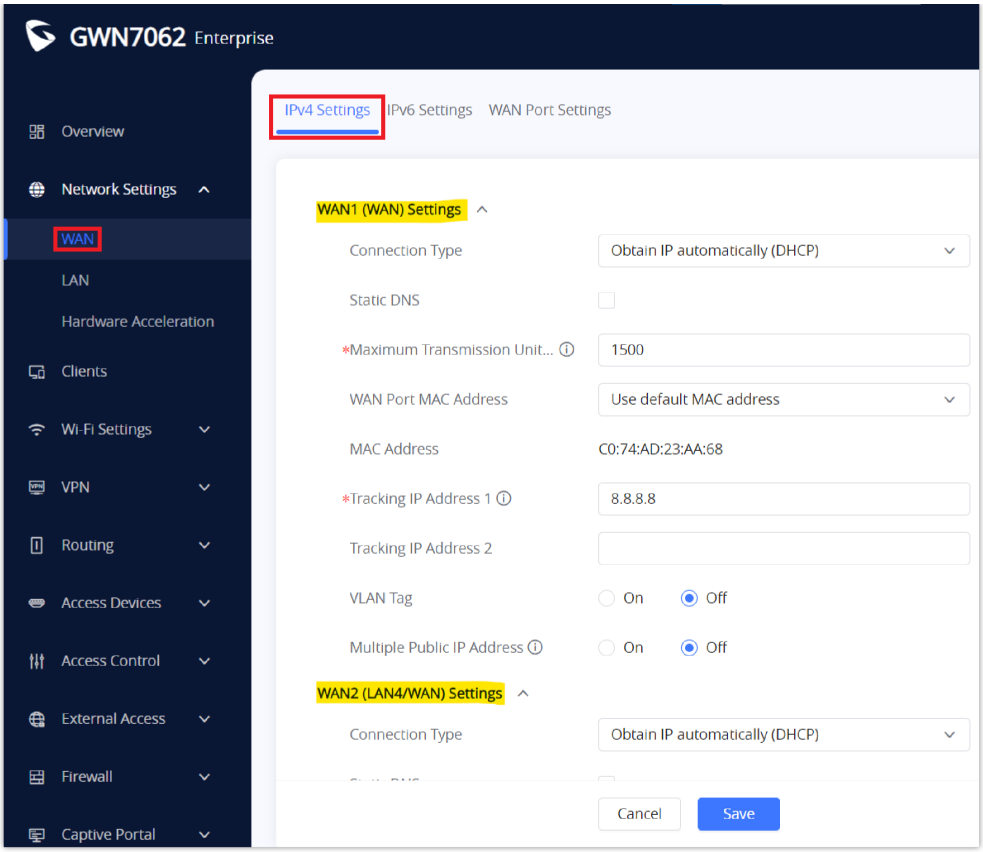

Figure 23: WAN Configuration

Please refer to the following table for basic network configuration parameters on the WAN port with IPv4 for GWN70xx.

Connection Type	• **Obtain IP automatically (DHCP):** When selected, it will act as a DHCP client and acquire an IPv4 address automatically from the DHCP server. • **Enter IP Manually (Static IP):** When selected, the user should set a static IPv4 address, IPv4 Subnet Mask, IPv4 Gateway and adding Additional IPv4 Addresses as well to communicate with the web interface, SSH, or other services running on the device. • **Internet Access with PPPoE account (PPPoE):** When selected, the user should set the PPPoE account and password, PPPoE Keep alive interval and Inter-Key Timeout (in seconds). • **L2TP** Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by internet service providers (ISPs) to enable virtual private networks (VPNs). • **PPTP:** Point-to-Point Tunneling Protocol (PPTP) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a virtual private network (VPN) across TCP/IP-based data networks. *The default setting is "**Obtain IP automatically (DHCP)**".*
Static DNS	Check Static DNS then enter the Preferred DNS Server and the Alternative DNS Server.
Maximum Transmission Unit (MTU)	Configures the maximum transmission unit allowed on the wan port. The valid range is 576-1450 Bytes, and the default value is 1450.
WAN Port MAC Address	Select either to use the default MAC address or use the MAC address of current management PC or use custom MAC address.
MAC Address	the MAC address used for the WAN.
Tracking IP Address 1	Configures tracking IP address of WAN port to determine whether the WAN port network is normal.
Tracking IP Address 2	Add another alternative address for Tracking IP Address
VLAN Tag	Select if either to enable or disable VLAN Tag.

Multiple Public IP Address	Please use with Port Forward function, so that you can access to router via public IP address.

Table 5: WAN Settings

○ IPv6 Settings

GWN70xx routers also support IPv6 configuration.

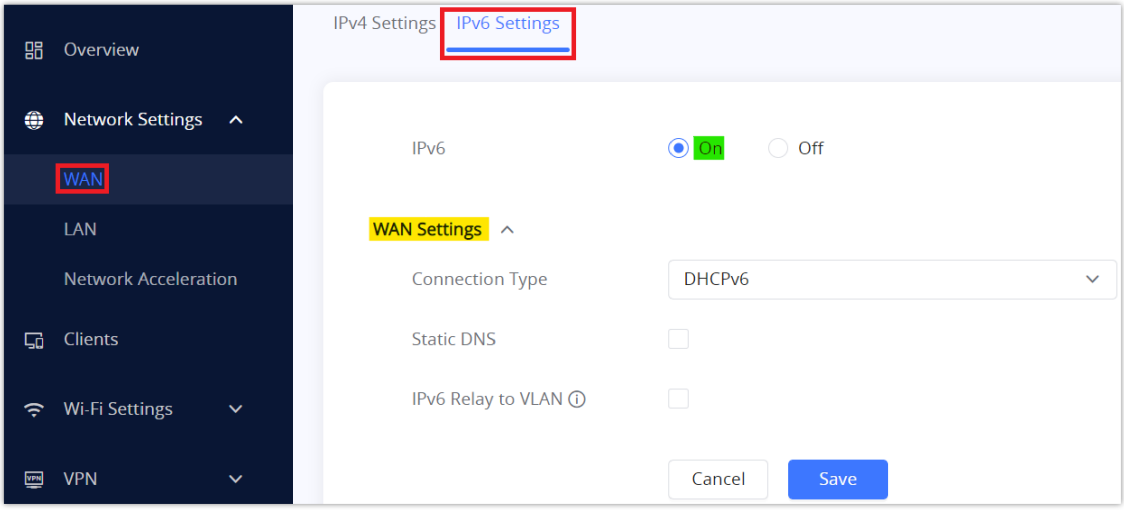

Figure 24: WAN – IPv6 Settings

Please refer to the following table for IPv6 settings:

IPv6	Check "**ON**" to activate IPv6
WAN Settings	
Connection Type	• **DHCPv6 :** When selected, it will act as a DHCP client and acquire an IPv4 address automatically from the DHCP server. • **Static IPv6 :** When selected, the user should set a **static IPv6 address**, **Prefix Length**, **default Gateway** and **Preferred DNS Server**. • **PPPoE (only when IPv4 PPPoE is enabled) :** can be only used if PPPoE IPv4 is already enabled. *The default setting is "**DHCPv6**".*
Static DNS	Check Static DNS then enter the Preferred DNS Server and the Alternative DNS Server.
IPv6 Relay to VLAN	Once enabled, relay IPv6 addresses to clients on the LAN side. ***Note:** This function will take effect only "**IPv6 Relay from WAN**" is enabled on VLAN.*

Table 6: IPv6 Settings

○ WAN Port Settings

The GWN7062 supports dual WAN port setup, by default the fourth LAN port is configured as LAN but the user can enable Dual WAN Port to make it as a secondary WAN port.

To access this page, please navigate to **Network Settings → WAN → WAN Port Settings**.

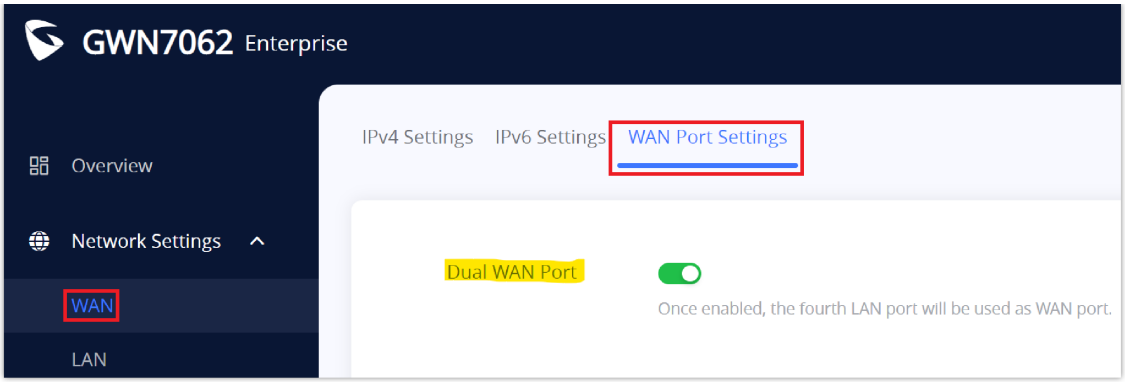

Figure 25: WAN port Settings

LAN

To access the LAN configuration page, log in to the GWN70xx WebGUI and go to **Network Settings** → **LAN**. VLAN configuration such as adding VLANs or setting up a VLAN port can be found here on this page, as well as the ability to add Static IP Bindings.

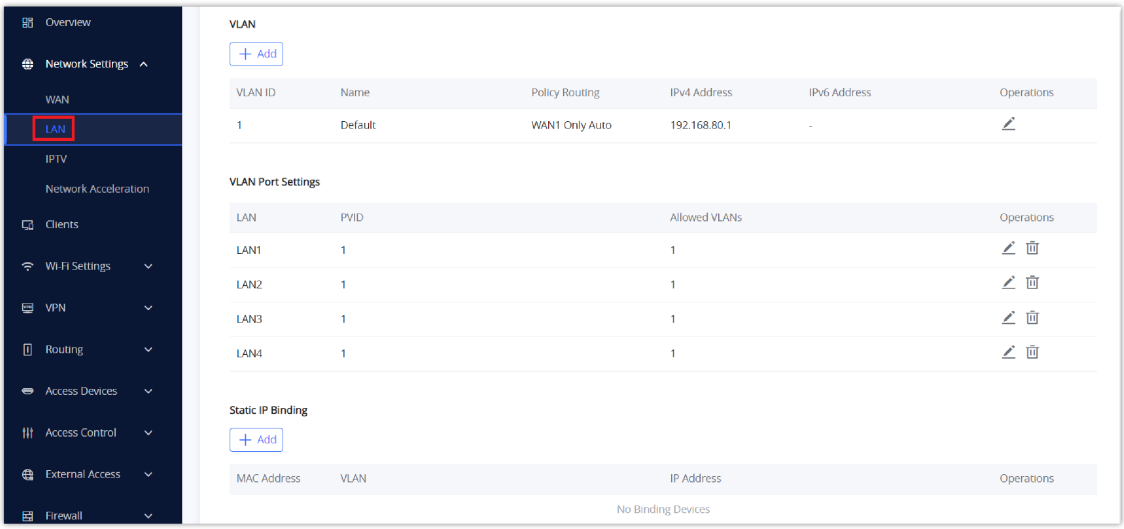

Figure 26: LAN configuration

VLAN

GWN70xx router integrates VLAN to enhance security and add more functionalities and features. VLAN tags can be used with SSIDs to separate them from the rest, also the user can allow these VLANs only on specific LANs for more control and isolation and they can be used as well with policy routing.

○ Add or Edit VLAN

To Add or Edit a VLAN, Navigate to **Router Interface** → **Network Settings** → **LAN**. Click on + Add button or click on Edit button.

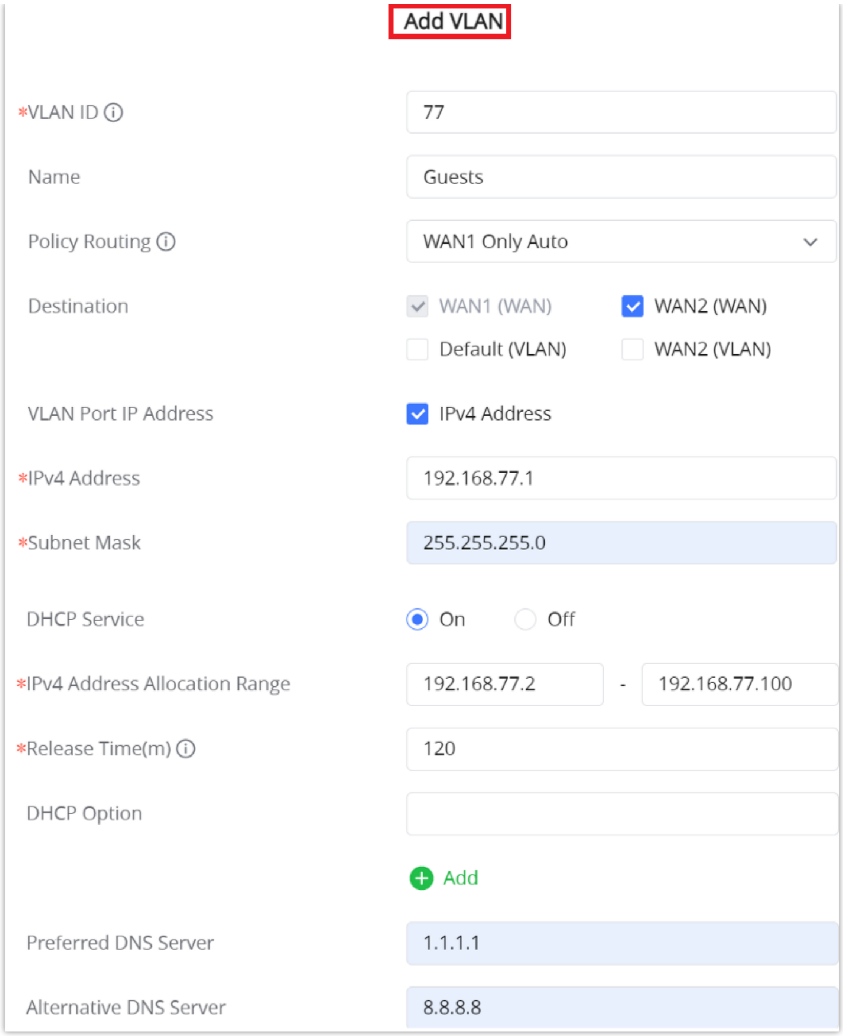

Figure 27: Add or Edit VLAN

VLAN ID	Enter a VLAN ID ***Note**: VLAN ID range is from 3 to 4094.*
Name	Enter the VLAN name
Policy Routing	Select a Policy Routing from the list or Add one.
Destination	To fast configure the VLAN's single-way data communication with WANs, other VLANs and VPNs. The option selected by default will be based on "Policy Routing" option to keep the default route accessible.
VLAN Port IPv4 Address	Check IPv4 Address to specify the Address.
IPv4 address	Enter IPv4 Address
Subnet Mask	Enter Subnet Mask
DHCP Server	By default it's "**Off**", choose "**On**" to specifiy the IPv4 address Allocation Range
IPv4 Address Allocation Range	Enter the start and the end of the IPv4 address Allocation Range.
Release Time(m)	The default value is 120, and the valid range is 60~2880.
DHCP Option	Enter or Add DHCP Options

Preferred DNS Server	Enter the Preferred DNS Server
Alternative DNS Server	Enter the Alternative DNS Server

Table 7: Add or Edit VLAN

○ **VLAN Port Settings**

The user can use LAN ports to allow only specific VLANs on each LAN port and in case there are more than one VLAN then there is an option to choose one VLAN as the default VLAN ID (PVID or Port VLAN Identifier). Click on to edit the VLAN Port Settings or click on to delete that configuration and bring back the default settings which is by default VLAN 1.

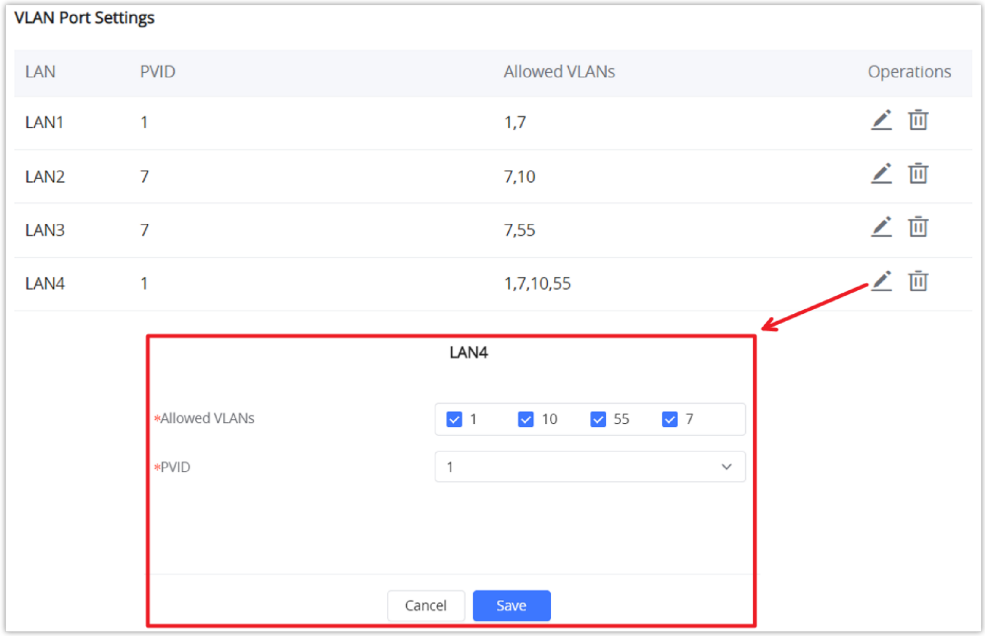

Figure 28: VLAN Ports

Allowed VLANs	Choose the VLANS to be allowed on this port.
PVID	Select the Port VLAN Identifier or the default VLAN ID

Table 8: VLAN Port Settings

Static IP Binding

Users can use the feature to set **Static IP Binding** to certain clients, to whom they do not want the IP address to change.

To configure Static IP Binding, please follow the below steps:
1- Go under the menu **Network Settings → LAN → Static IP Binding**.
2- Click button + Add to create a new entry.
3- Enter the device's MAC address and IP address.

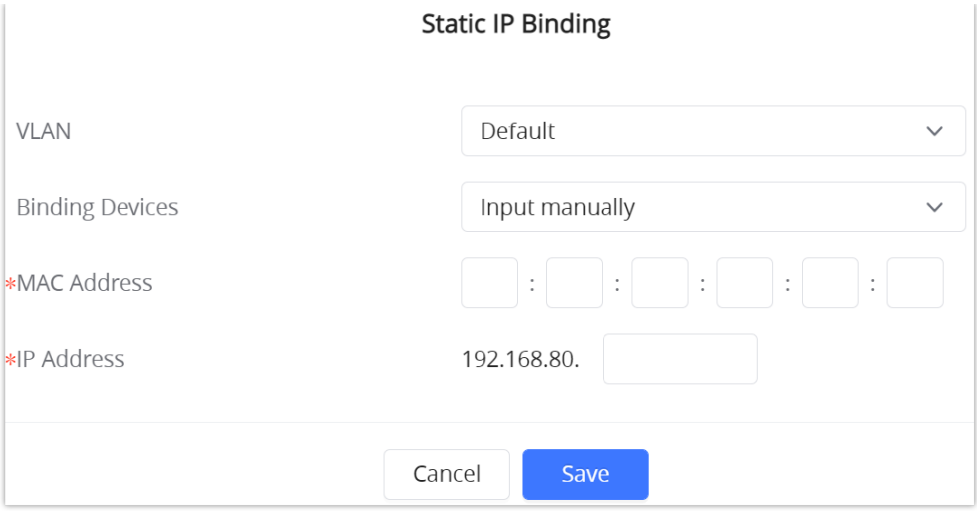

Figure 29: Static IP Binding

VLAN	Select the VLAN or Default VLAN
Binding Devices	Select to input manually by entering the MAC Address and IP Address or select from the clients list.
MAC Address	Enter the MAC Address
IP Address	Enter the IP Address

Table 9: Static IP Binding

Network Acceleration

Acceleration Mode when it's enabled helps to achieve higher speeds and reduce latency.

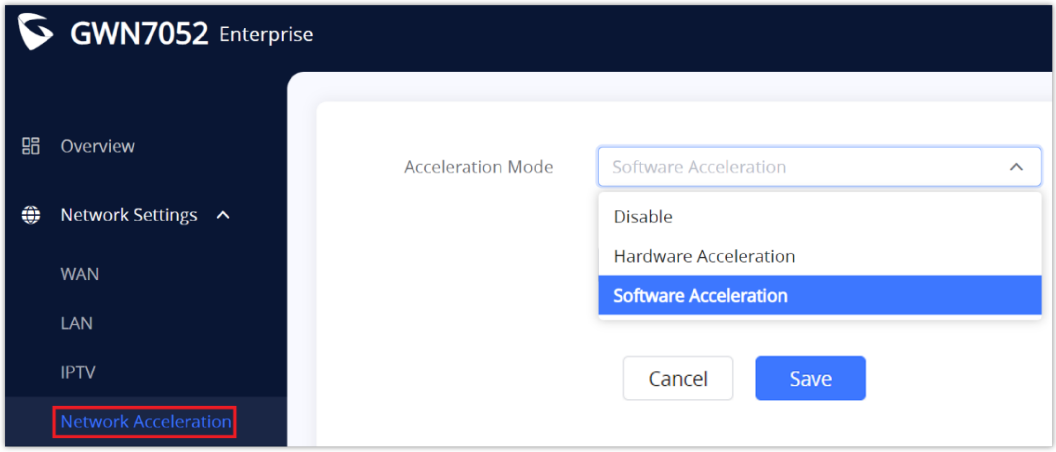

Figure 30: Hardware Acceleration

Once enabled, some features may not work properly or get disabled. Refer to the list below.

1. **Software Acceleration**: disables QoS and rate limit (such as wireless client rate limit).
2. **Hardware Acceleration**: disables QoS, NetFlow, Bonding, Suspend, and Wireless Acceleration.

ROUTING

This section is about adding routes either Static Routing or Policy Routing that can be applied on an Interface WAN or LAN/VLAN where the user can specify the next Hop and Metric for the static routing or priority and weight for the policy routing.

Policy Routing

Feature Overview

The policy-based Routing feature allows a network administrator to make advanced routing decisions for traffic passing through the router. This feature allows for high granularity control over policies that dictate what WAN port and even VLAN, traffic should use. Traffic controlled this way can be balanced across multiple VLANs.

Creating/Configuring Routing Policies

To configure a new routing policy, first users need to create members under the menu **Routing → Policy Routing**.

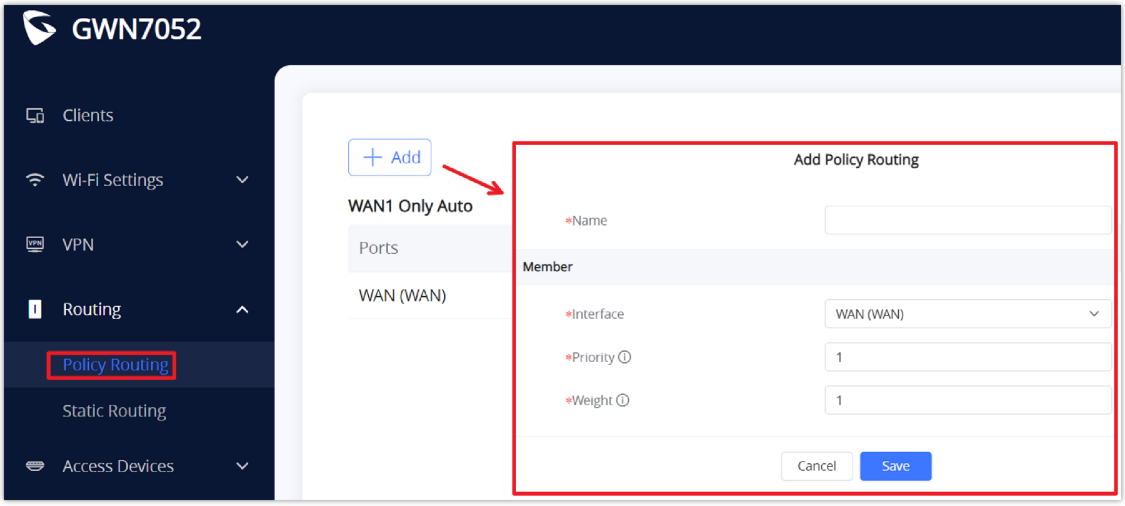

Figure 31: Policy Routing page

Name	Specify a name for the routing Policy
Interface	Select the Interface for example it could be a WAN
Priority	The default value is 1, and the valid range is 1~128. ***Note:** The smaller the priority value, the higher the priority.*
Weight	The default value is 1, and the valid range is 1~10.

Table 10: Policy Routing

Using Routing Policies

○ **Add VLAN**

To use the routing policies created navigate to **"Network Settings → LAN"**, then add a new VLAN or edit previously created ones.

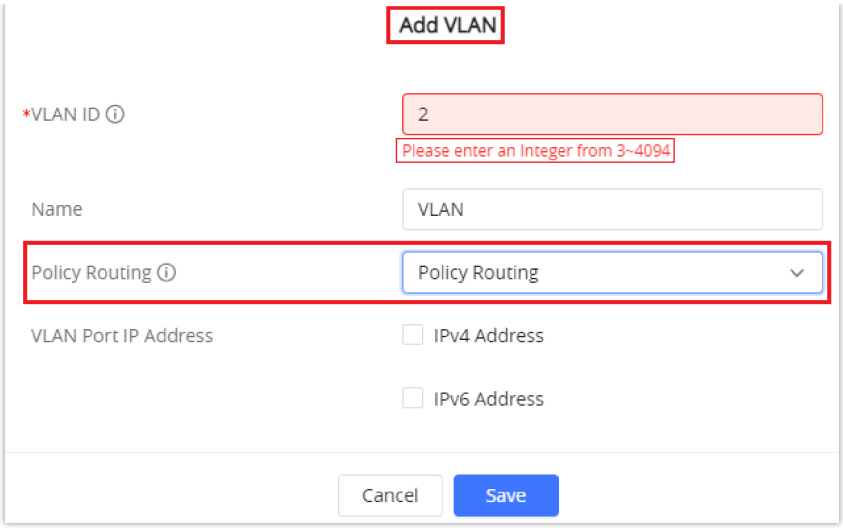

Figure 32: Add VLAN

VLAN ID	Enter a VLAN ID ***Note**: VLAN ID range is from 3 to 4094.*
Name	Enter the VLAN name
Policy Routing	Select a Policy Routing from the list or Add one.
VLAN Port IP Address	Check IPv4 Address or IPv6 Address to specify the Address.

Table 11: Add VLAN

Static Routes

GWN70xx supports setting manually **IPv4 Static Routes** which can be accessed from GWN70xx WebGUI **Network Settings → Routing → Static Routing**.

To add a new Static Route, the user needs to click on + Add

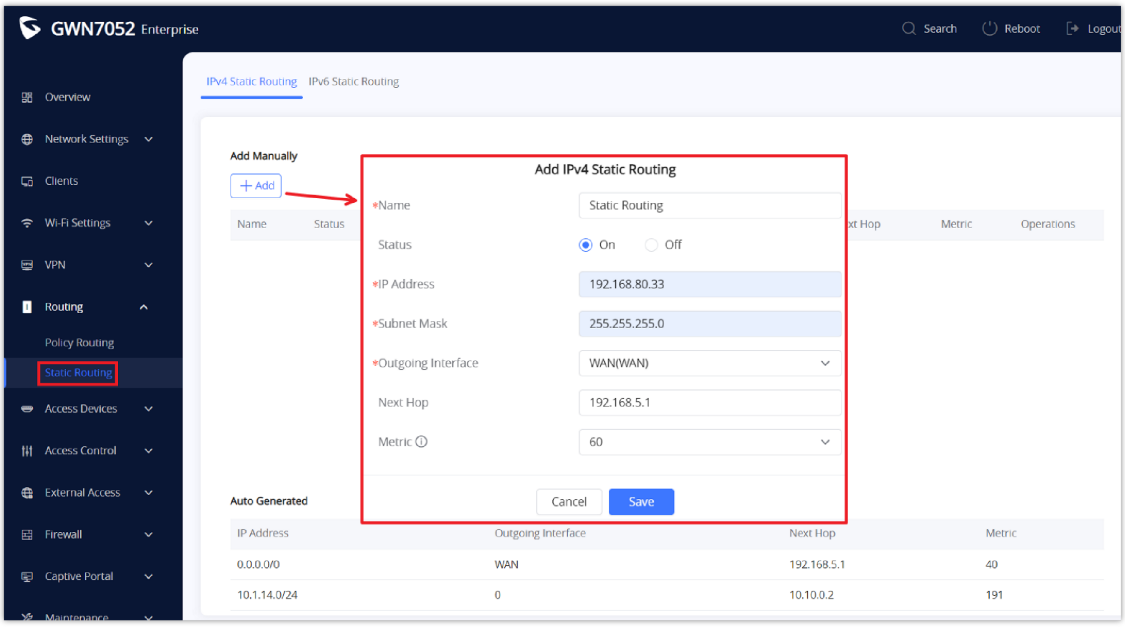

Figure 33: Static Routing Page

Name	Specify a name for the Static Routing

Status	enable or disable the Static Routing
IP Address	Specify the IP address
Subnet Mask	Enter the Subnet Mask
Outgoing Interface	Select the interface
Next Hop	Specify the next Hop
Metric	When there are multiple routings in the network that can reach the same destination, the priority of routing rules can be adjusted by setting metric, and the packets will be forwarded according to the path with the smallest metric.

Table 12: Static Routing

WAN Load-Balancing

Multi-WAN port routers like Grandstream GWN7062 with dual WAN ports can load balance between the WAN ports for networks with redundant internet connections. It reduces network downtime and makes the most out of each link.

To load balance between multiple WAN ports please follow the steps below:

1. **Enable Dual WAN Port**

The first thing to do is to make sure that Dual WAN Port is Enabled under **Network Settings → WAN → WAN Port Settings.**

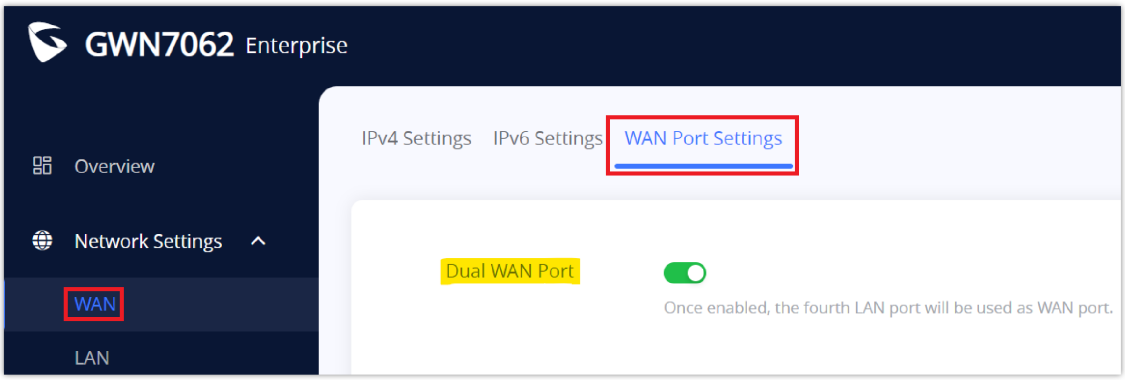

Figure 34: Enable Dual WAN Port

2. Add Policy Routing

Navigate to **Routing → Policy Routing** and click on + Add to add a Policy Routing, then add members where each member refers to an interface either WAN1 or WAN2, each interface will have a Priority from 1 up to 128, and the WAN with the highest priority will be used the most, and also weight from 1 up to 10 which indicates the percentage of traffic that should be sent to this WAN.

> Priorities need to be the same value to make a load balancing upon weight.

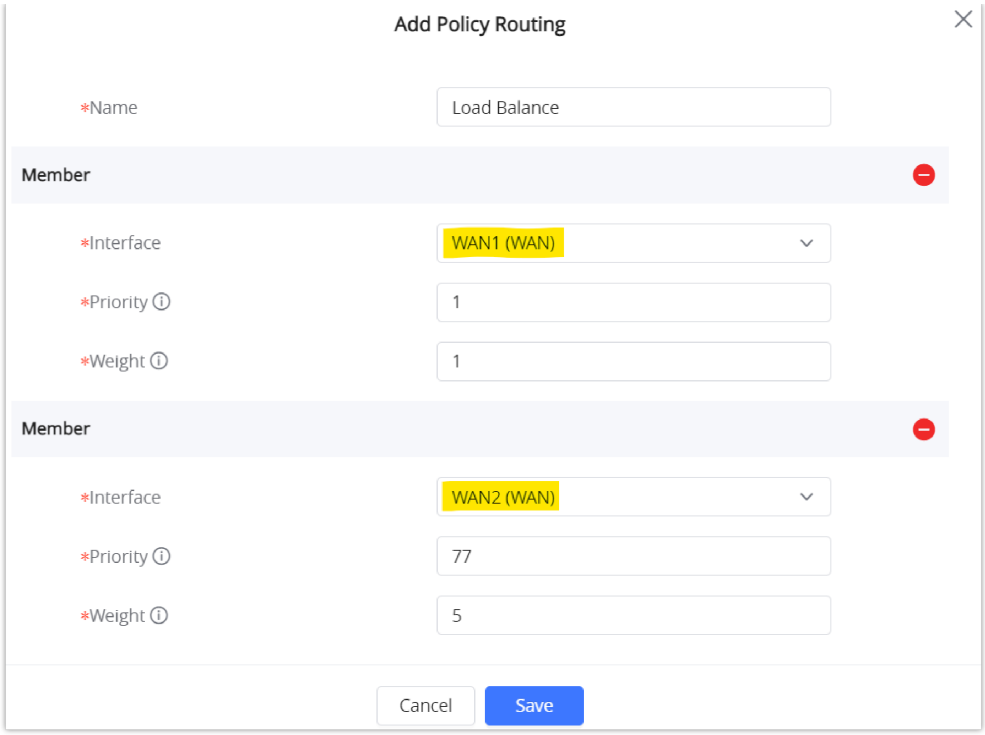

Figure 35: Add Policy Routing

3. Add a VLAN with Policy Routing

To use the Routing Policy, add a VLAN and choose the Routing Policy previously created.

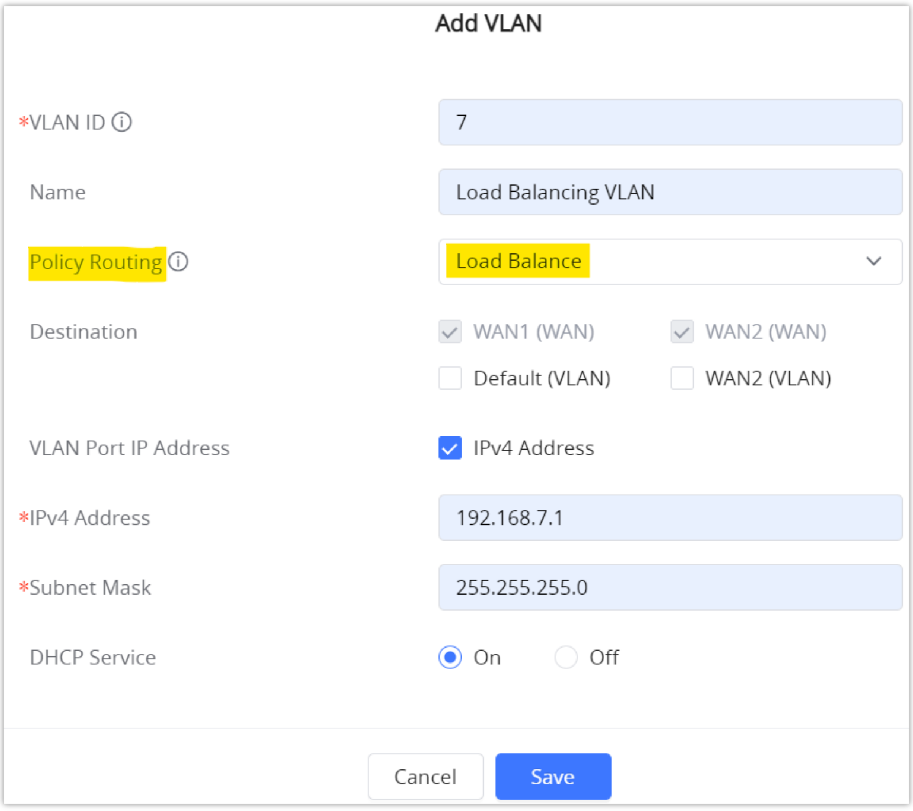

Figure 36: VLAN with a Routing Policy

4. Apply VLAN to an SSID or LAN port

Finally, apply the previously created VLAN to an SSID or a LAN port.

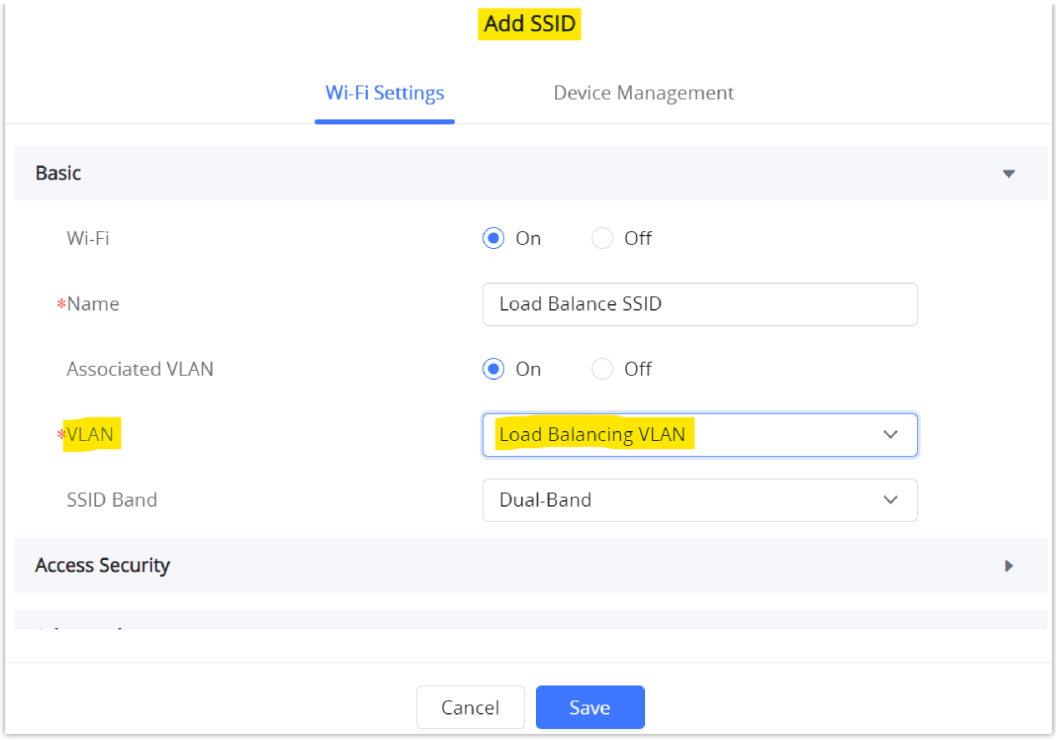

Figure 37: Add SSID

Similarly, the user can apply the VLAN to a LAN port to make the Routing Policy active on that LAN.

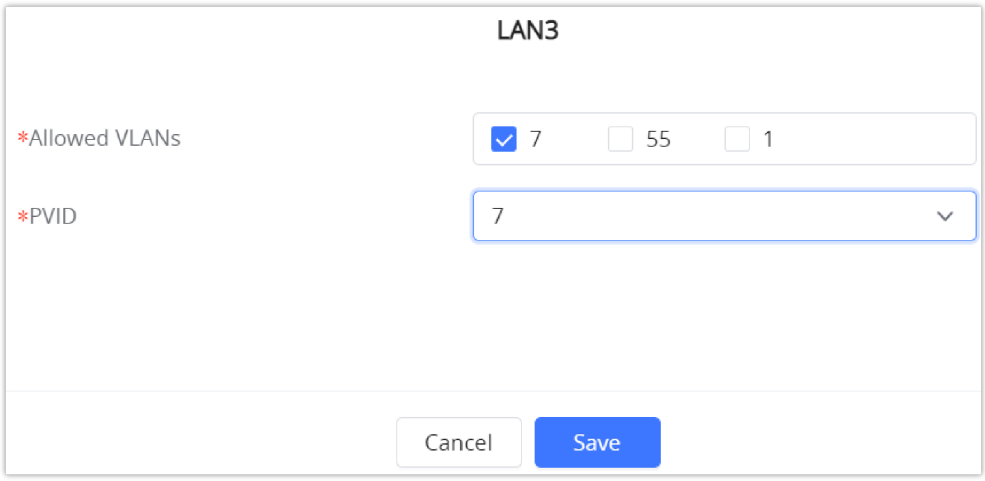

Figure 38: VLAN applied to a LAN

SETTING UP A WIRELESS NETWORK

The GWN70xx Router provides the user with the capability to create a wireless network either directly from the GWN70xx or by adding multiple GWN76xx series access points, with connectivity over the most common wireless standards (802.11a/b/g/n/ac/ax) operating in both 2.4GHz and 5GHz range.

The GWN70xx integrates multiple layers of security including the IEEE 802.1x port-based authentication protocol, Wi-Fi Protected Access (WPA/WPA2, WPA2, WPA2/WPA3, WPA3, and WPA3-192), and firewall and VPN tunnels.

Discover and Pair GWN76xx Access Points

1. Connect to the GWN70xx Web GUI and go to **Access Devices → Configuration**.

2. Click on (Pair AP) Pair AP to Discover access points within GWN70xx's LAN Network, or click on Takeover AP to pair with slaves access points whose master has gone offline.

3. Check the Access points available and then click OK.

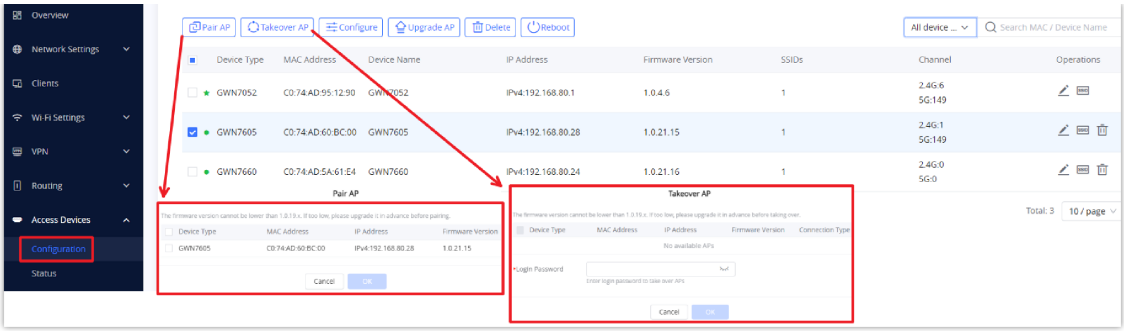

Figure 39: Access Devices – Configuration page

Access Point Location

GWN70xx router has an interesting feature to help users to locate different access points using blinking LED, to do so go under the Access **Devices** → **Status** page then click on and the corresponding LED will start blinking its LEDs. This can help ease locating the Access points on a multi-deployment site.

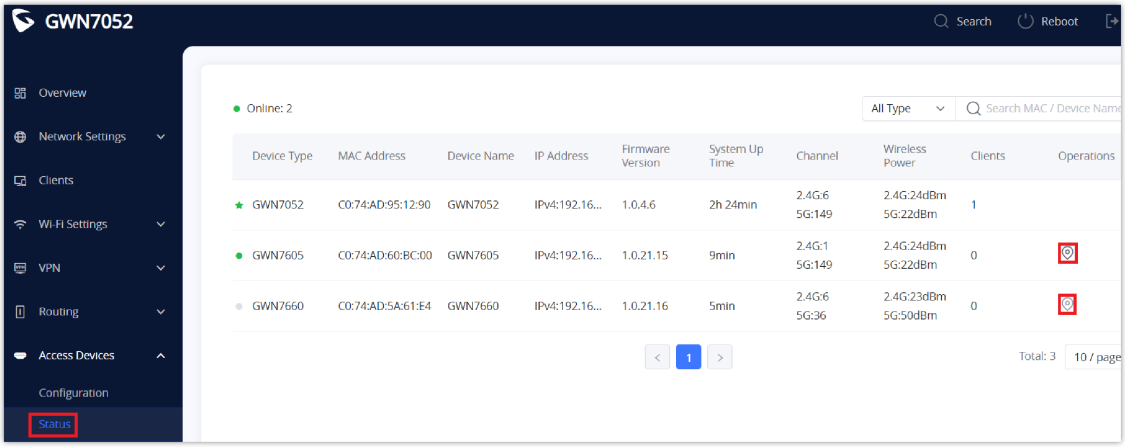

Figure 40: Access Devices – Status page

SSIDs

When using GWN70xx as Master, users can create different SSIDs and add GWN76xx Slave Access Points to each SSID depending on the needs of the customer.

Log in as Master to the GWN70xx Web GUI and go to **Wi-Fi Settings** → **SSIDs.**

Click on + Add to Add new SSID or click on Operations to edit the current SSID.

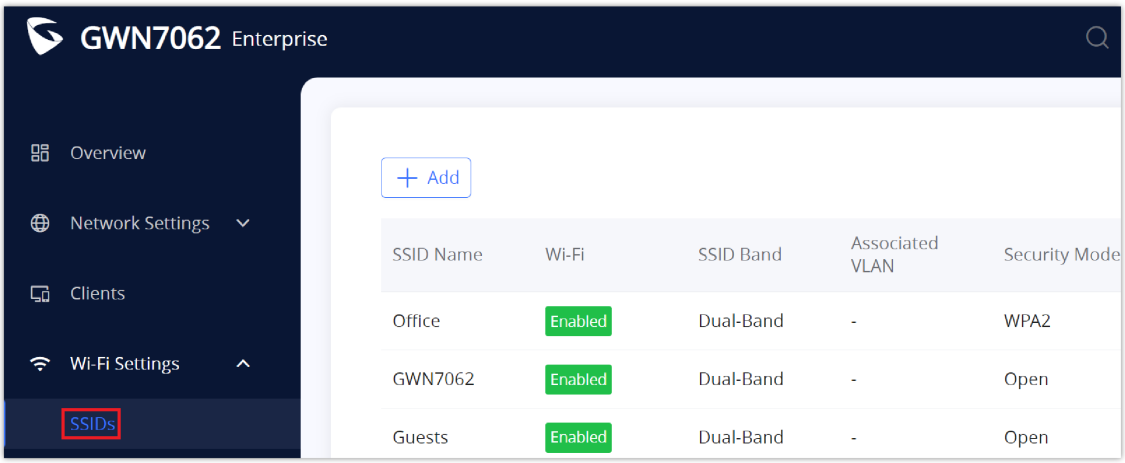

Figure 41: SSIDs Page

When editing or adding a new SSID, users will have two tabs to configure:

In the Wi-Fi Settings Tab, the user can enter all the configurations related to this SSID by specifying the name and the VLAN and the option for dual-band as well as other security options including the password, etc.

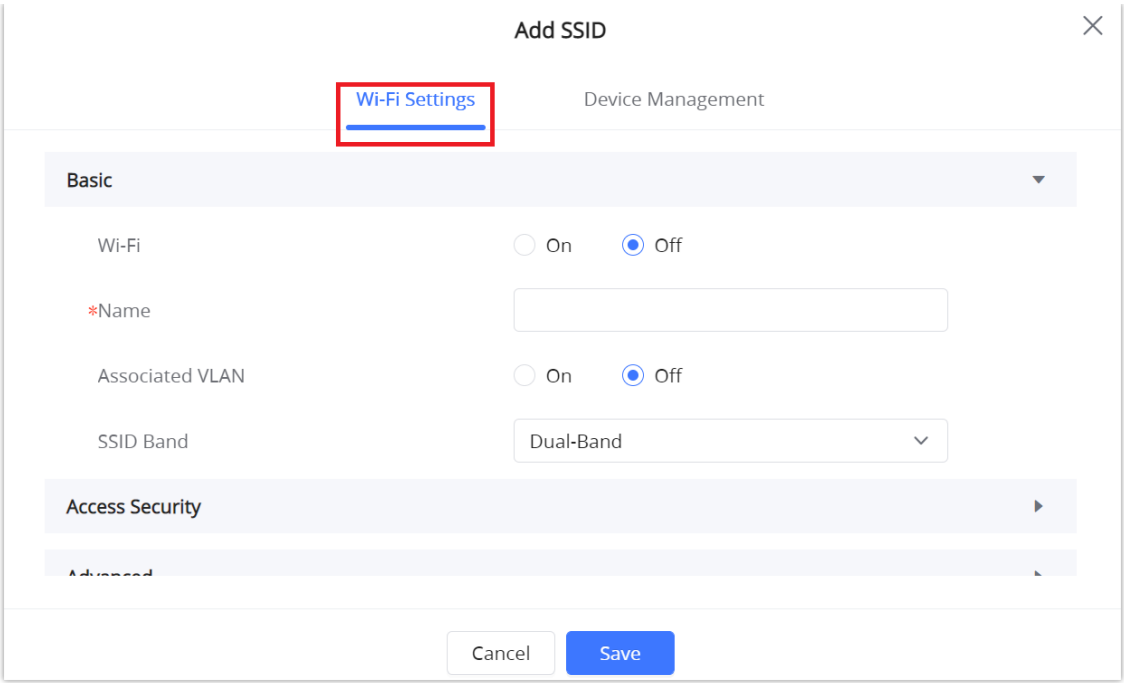

Figure 42: Add SSID Tab

Please refer to the below table for Wi-Fi Settings tab options.

Field	Description
Wi-Fi	Click on **"ON"** to enable the SSID
Name	Set or modify the SSID name.
Associated VLAN	Click on "**ON**" to enable **VLAN,** then specify the **VLAN** from the list or Create **VLAN**.
SSID Band	Select the Wi-Fi band the GWN will use, three options are available: ● **Dual-Band** ● **2.4GHz** ● **5GHz**
Security Mode	Set the security mode for encryption, 6 options are available: ● **WPA/WPA2:** Using “PSK” or “802.1x” as WPA Key Mode, with “AES” or “AES/TKIP” Encryption Type. ● **WPA2:** Using “PSK” or “802.1x” as WPA Key Mode, with “AES” or “AES/TKIP” Encryption Type. Recommended configuration for authentication. ● **Open:** No password is required. Users will be connected without authentication. Not recommended for security reasons. ● **WPA2/WPA3:** WPA2: Using “SAE-PSK” or “802.1x” as WPA Key Mode, with “AES” or “GCMP-128” Encryption Type. Recommended configuration for authentication. ● **WPA3:** Using “SAE” or.“802.1x” as WPA Key Mode, with “AES” or “GCMP-128” Encryption Type. Recommended configuration for authentication. ● **WPA3-192:** Using “802.1x” as WPA Key Mode, with “GCMP-256” or “CCMP-256” Encryption Type. Recommended configuration for authentication.
WPA Key Mode	Two modes are available: ● **PSK:** Use a pre-shared key to authenticate to the Wi-Fi. ● **802.1X:** Use a RADIUS server to authenticate to the Wi-Fi.
WPA Encryption Type	Two modes are available: ● **AES:** This method changes dynamically the encryption keys making them nearly impossible to circumvent.

	• **AES/TKIP:** use both Temporal Key Integrity Protocol and Advanced Encryption Standard for encryption, this provides the most reliable security.
WPA Shared Key	Set the access key for the clients, and the input range should be: 8-63 ASCII characters or 8-64 hex characters.
RADIUS Server Address	Configures RADIUS authentication server address. ***Note:*** *This field is available only when "WPA Key Mode" is set to "802.1x".*
RADIUS Server Port	Configures RADIUS Server Listening port. Default is: 1812. ***Note:*** *This field is available only when "WPA Key Mode" is set to "802.1x".*
RADIUS Server Secret	Enter the secret password for client authentication with RADIUS server. ***Note:*** *This field is available only when "WPA Key Mode" is set to "802.1x".*
Secondary RADIUS Server	Check the box to enable settings a secondary RADIUS server. Then you need to specify below three fields: • **RADIUS Server Address:** Enter the secondary RADIUS server address. • **RADIUS Server Port:** Enter the secondary RADIUS server port. The default port is 1812 and the range is 1-65535. • **RADIUS Server Secret:** Enter the secret password for client authentication with the secondary RADIUS server.
RADIUS Accounting Server Address	Configures the address for the RADIUS accounting server. ***Note:*** *This field is available only when "WPA Key Mode" is set to "802.1x".*
RADIUS Accounting Server Port	Configures RADIUS accounting server listening port. Default is 1813. ***Note:*** *This field is available only when "WPA Key Mode" is set to "802.1x".*
RADIUS Accounting Server Secret	Enter the secret password for client authentication with RADIUS accounting server. ***Note:*** *This field is available only when "WPA Key Mode" is set to "802.1x".*
Secondary RADIUS Accounting Server	Check the box to enable settings a secondary RADIUS accounting server. Then you need to specify below three fields: • **RADIUS Accounting Server Address:** Enter the secondary Accounting RADIUS server address. • **RADIUS Accounting Server Port:** Configures the secondary RADIUS accounting server listening port. Default is 1813. • **RADIUS Accounting Server Secret:** Enter the secret password for client authentication with the secondary RADIUS accounting server.
RADIUS NAS ID	Enter the RADIUS NAS ID. ***Note:*** *This field is available only when "WPA Key Mode" is set to "802.1x".*
Enable Captive Portal	Click on the checkbox to enable the captive portal feature.
Blocklist Filtering	Click Add Blocklist and select from the available devices or add manually the device or selected from previously created blocklist.
Client Isolation	Client isolation feature blocks any TCP/IP connection between connected clients to GWN76XX's Wi-Fi access point. Client isolation can be helpful to increase security for Guest networks/Public Wi-Fi. Three modes are available: • **Internet Mode:** Wireless clients will be allowed to access only the internet services and they cannot access any of the management services, either on the router nor the access points GWN76XX. • **Gateway MAC Mode:** Wireless clients can only communicate with the gateway, the communication between clients is blocked and they cannot access any of the management services on the GWN76XX access points.

	● **Radio Mode:** Wireless clients can access to the internet services, GWN7xxx router and the access points GWN76XX but they cannot communicate with each other.
802.11w	The 802.11w standard is used to prevent certain types of WLAN DoS attacks. 802.11w extends strong cryptographic protection and provides data integrity and replay protection for broadcast/multicast Robust management frames. Set this option to either to ● **Disabled**： disable 802.11w; ● **Optional:** both of the client supported and unsupported 802.11w may have the network access authority; ● **Required:** only the client supported 802.11w have the network access authority.
SSID Hidden	Select to hide SSID. SSID will not be visible when scanning for Wi-Fi, to connect a device to hidden SSID, users need to specify SSID name and authentication password manually.
DTIM Period	Configures the frequency of DTIM (Delivery Traffic Indication Message) transmission per each beacon broadcast. Clients will check the AP for buffered data at every configured DTIM Period. You may set a high value for power saving consideration. ● Default value is 1, meaning that AP will have DTIM broadcast every beacon. ● If set to 10, AP will have DTIM broadcast every 10 beacons. Valid range: 1 – 10.
Wireless Client Limit	Configure the limit for wireless client. If there's an SSID per-radio on a SSID, each SSID will have the same limit. Setting a limit of 50 will limit each SSID to 50 users independently. If set to 0 the limit is disabled.
Client Inactivity Timeout	Router/AP will remove the client's entry if the client generates no traffic at all for the specified time period. The client inactivity timeout is set to 300 seconds by default.
Multicast/Broadcast Suppression	● **Disabled:** all of the broadcast and multicast packages will be forwarded to the wireless interface. ● **Enabled:** all of the broadcast and multicast packages will be discarded except DHCP/ARP/IGMP/ND; ● **Enabled with ARP Proxy enabled:** enable the optimization with ARP Proxy enabled in the meantime.
Convert IP Multicast to Unicast	● **Disabled:** No IP multicast packets will be converted to unicast packets. ● **Passive:** The device will not actively send IGMP queries, and the IGMP snooping entries may be aged after 300s and cannot be forwarded as multicast data. ● **Active:** The device will actively send IGMP queries and keep IGMP snooping entries updated.
Enable Schedule	Schedule is used to make SSID take effect in the specified period.
Enable Voice Entreprise	Check to enable/disable Voice Enterprise. The roaming time will be reduced once enable voice enterprise. The 802.11k standard helps clients to speed up the search for nearby APs that are available as roaming targets by creating an optimized list of channels. When the signal strength of the current AP weakens, your device will scan for target APs from this list. When your client device roams from one AP to another on the same network, 802.11r uses a feature called Fast Basic Service Set Transition (FT) to authenticate more quickly. FT works with both pre-shared key (PSK) and 802.1X authentication methods. 802.11v allows client devices to exchange information about the network topology, including information about the RF environment, making each client network aware, facilitating overall improvement of the wireless network. **Note:** 11R is required for enterprise audio feature, 11V and 11K are optional. This field is available only when "Security Mode" is set to "WPA/WPA2, WPA2 and WPA3"
Enable 802.11r	Check to enable 802.11r
Enable 802.11k	Check to enable 802.11k

Enable 802.11v	Check to enable 802.11v
ARP Proxy	This option will enable the router to answer the ARP requests from its LAN for its connected WiFi clients. This is mainly to reduce the airtime consumed by ARP Packets
Enable U-APSD	Configures whether to enable U-APSD (Unscheduled Automatic Power Save Delivery).
Maximum Upload Rate (Mbps)	Support integer from 1-1000. No limit if empty.
Maximum Download Rate (Mbps)	Support integer from 1-1000. No limit if empty.

Table 13: Wi-Fi Settings

In this tab, you can specify what devices (access points) will be part of this SSID.

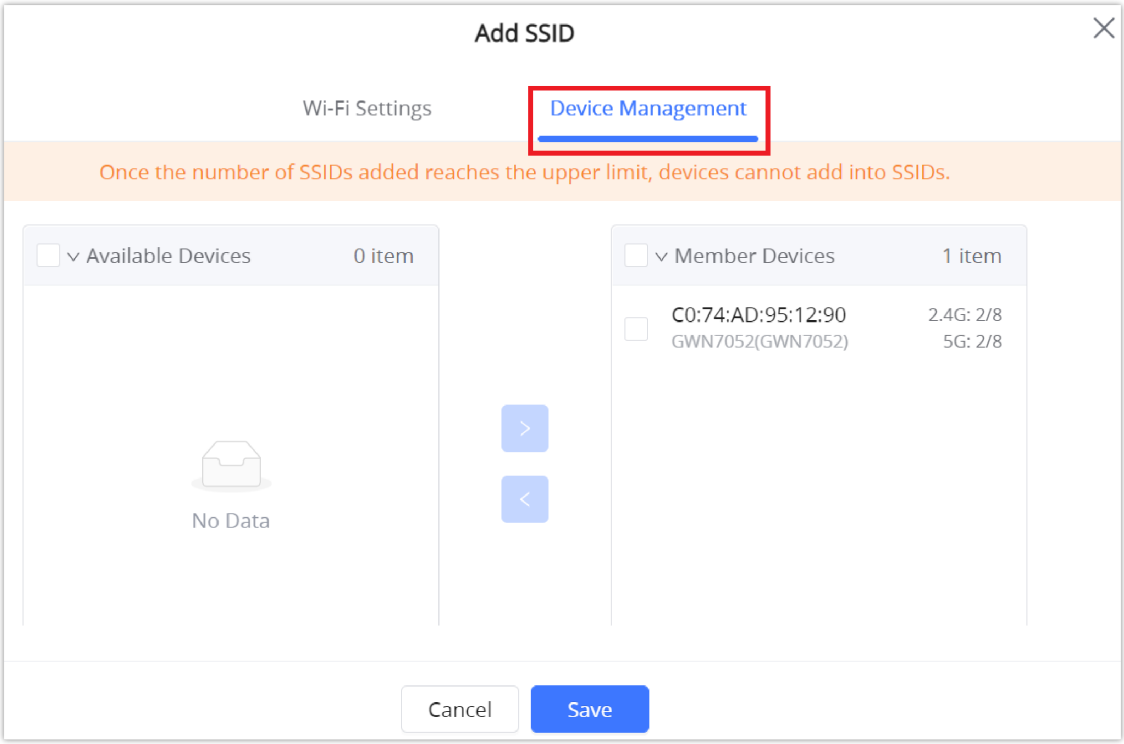

Figure 43: Device Management

Mesh Network

In Mesh Network, the wireless connection is established between multiple APs, which is used to pass through data traffic rather than client association. Each AP will evaluate the performance of wireless channels based on several factors and choose one or multiple appropriate APs to set up the connection.

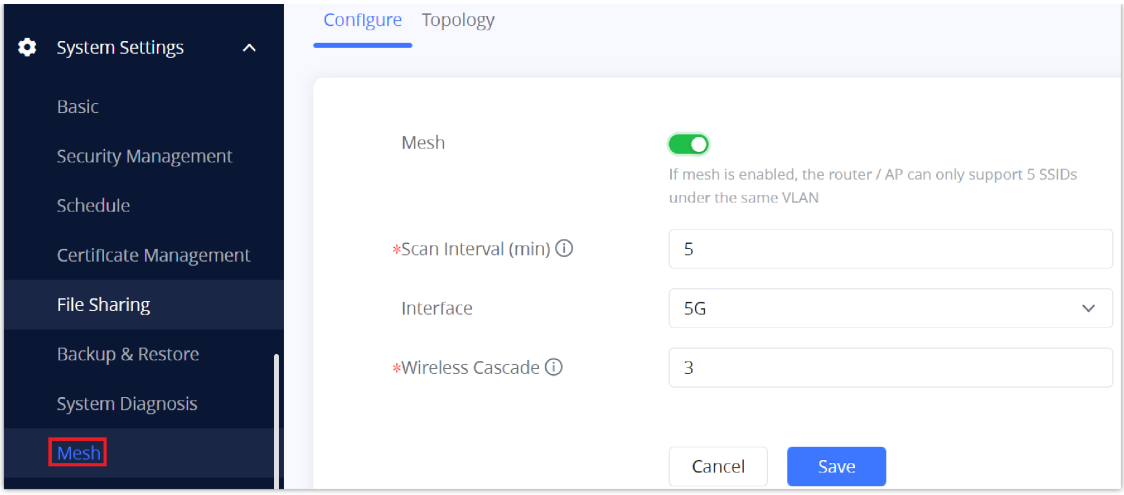

Figure 44: Mesh

In a mesh network, access points are categorized into two types:

○ **CAP (Central Access Point):** this is an access point that has an uplink connection to the wired network.

○ **RE (Range Extender):** This is an access point that participates in the mesh network topology and has a wireless uplink connection to the central network.

To deploy mesh access points (RE), users/installers can follow the below steps:

1. Make sure to have the master and CAP access points already deployed (sometimes the CAP access points can be the master controller of the network).

2. Next, we need to pair the RE access points to the master. This can be done in two ways:

3. Connect all REs to the same wired LAN as the master then perform the normal process of discovery/pairing process, and after successfully pairing the APs they can be deployed on the field.

4. REs can also be discovered wirelessly when powered via PSU or PoE Injector, and the admin can configure them after discovery. This requires that the REs must be within the range of the Master or CAP Slave's signals coverage.

The following table describes the Mesh configuration settings.

Mesh	When checked the Mesh feature will be activated.
Scan Interval (Min)	The valid range is 1~5. *The default value is 5*
Interface	Only 5GHz can be selected.
Wireless cascades	The valid range is 1~3. *The default value is 3*

Table 14: Mesh

Upgrading Access Points

Single Access Point Upgrade

If you want to upgrade a single access point or multiple Access points, users need to select the APs and then simply click on the button Upgrade AP to launch the upgrade process, the AP will use the same parameters configured for the router under the menu **System Settings → Upgrade.**

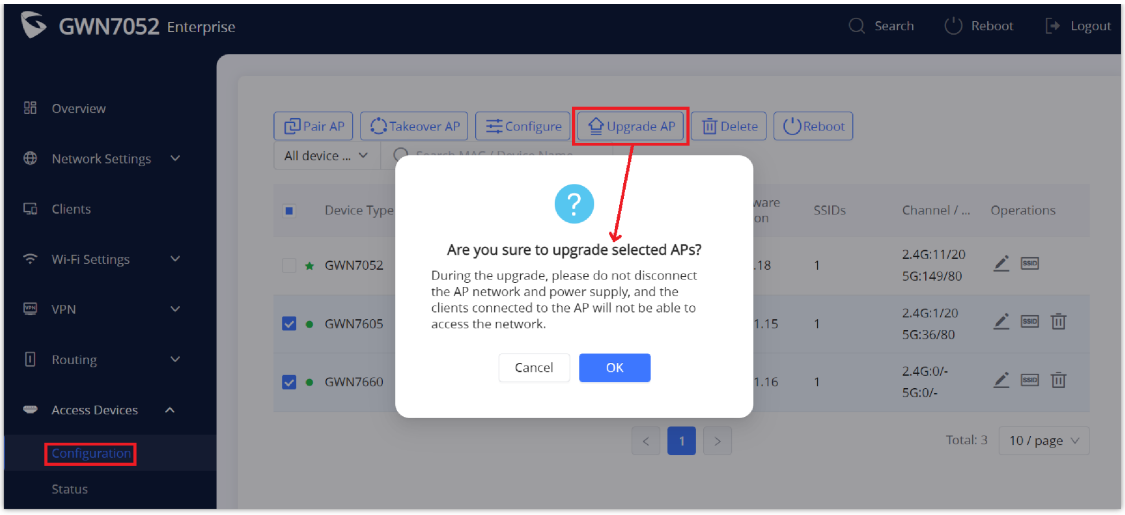

Figure 45: Upgrading APs

CLIENTS CONFIGURATION

Clients

Clients page keeps a list of all the devices and users connected currently or previously to different LAN subnets with details such as the MAC Address, the IP Address, the duration time, and the upload and download information. It's helpful to know about the clients' stats and also who is consuming more bandwidth. Click on Operations to edit the device name or limit its maximum upload or download rate.

The clients' list can be accessed from GWN70xx's Web GUI → Clients to perform different actions for wired and wireless clients.

GWN70xx Enterprise Routers with its DHCP server enabled on the LAN ports level, will assign automatically an IP address to the devices connected to its LAN ports like a computer or GWN76xx access points and wireless clients connected to paired GWN76xx access points.

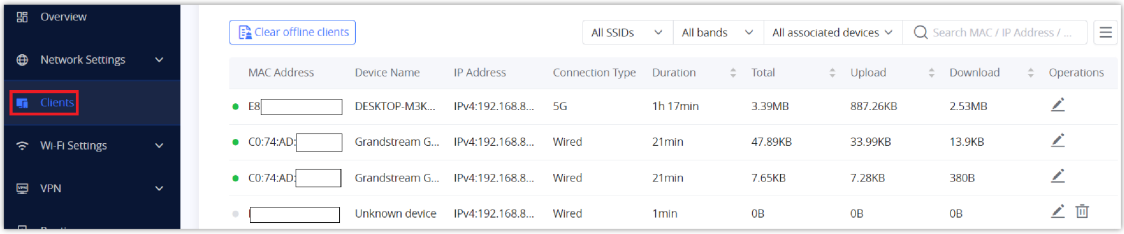

Figure 46: Clients Page

Edit Name and Set Bandwidth Rules

In the operations column click on Edit icon then set the name and the Maximum Upload Rate and Maximum Download Rate (if empty no limit). It's only applicable to wireless clients.

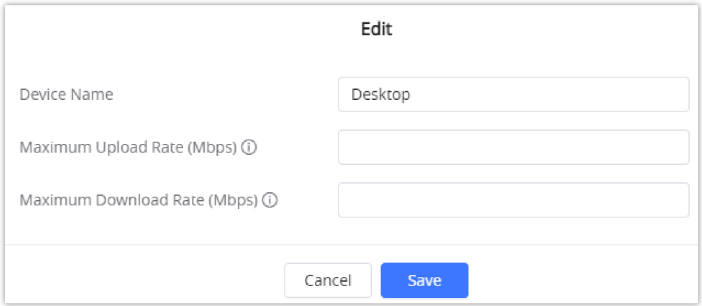

Figure 47: Upload and Download Rate

VPN (VIRTUAL PRIVATE NETWORK)

Overview

VPN allows the GWN70xx routers to be connected to a remote VPN server using PPTP, IPSec, L2TP, and OpenVPN® protocols, or configure an OpenVPN® server and generate certificates and keys for clients, VPN page can be accessed from the GWN70xx **Web GUI → VPN**.

OpenVPN® Server Configuration

To use the GWN70xx as an OpenVPN® server, you will need to start creating a user account, OpenVPN® server certificates, and client certificates. Before generating server/client certificates, it is requested to generate first the Certificate Authority (CA), which will help to issue server/client certificates.

GWN70xx certificates can be managed from **Web GUI → System Settings → Certificate Management.**

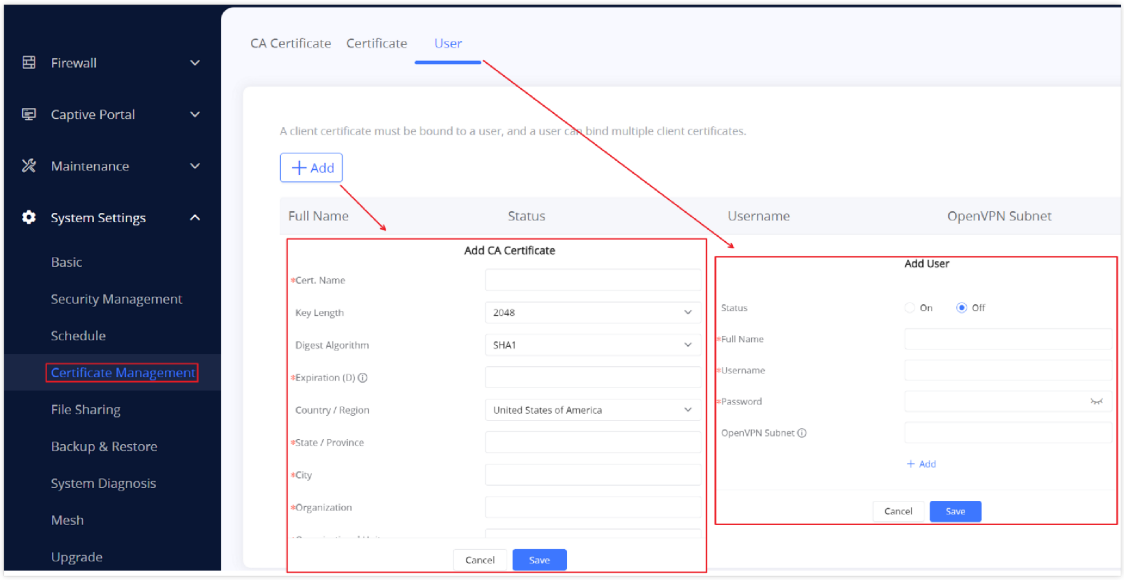

Figure 48: Certificate Management

Generate Self-Issued Certificate Authority (CA)

A certificate authority (CA) is a trusted entity that issues electronic documents that verify a digital entity's identity on the Internet. Electronic documents (a.k.a . digital certificates) are an essential part of secure communication and play an important part in the public key infrastructure (PKI).

To create a Certification Authority (CA), follow the below steps:

1. Navigate to "**Web GUI → System Settings → Certificate Management → CA Certificate**"
2. Click on + Add button. A popup window will appear.
3. Enter the CA values including CN, Key Length, and Digest Algorithm … depending on your needs.

Refer to the below figure showing an example of configuration and the table showing all available options with their respective descriptions.

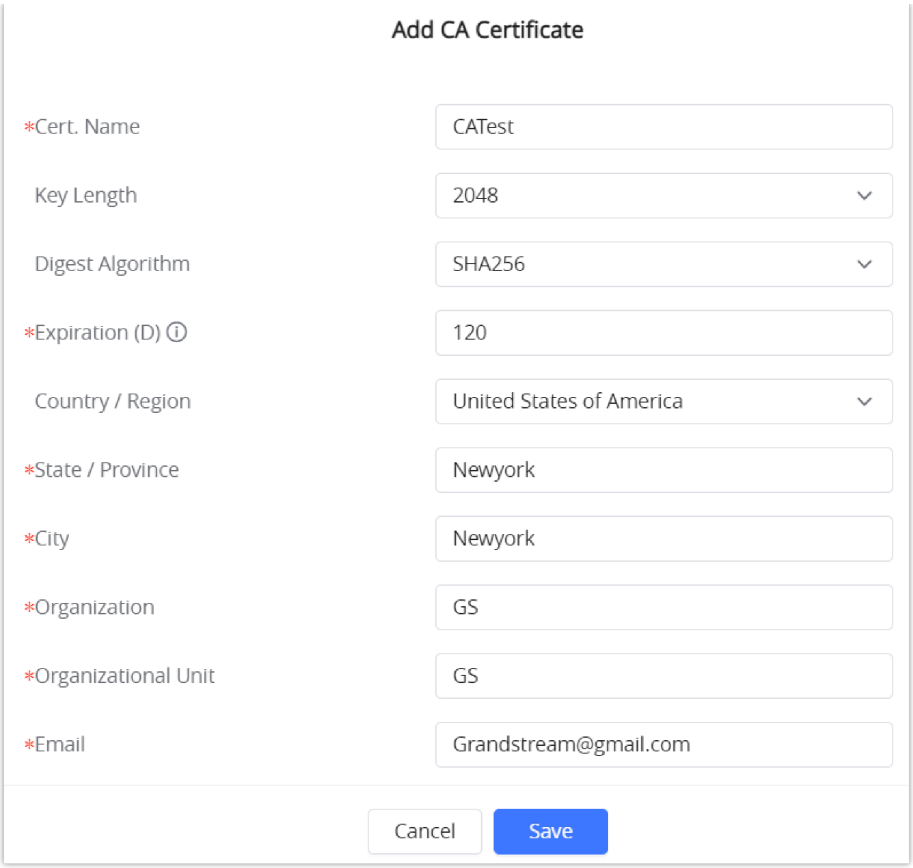

Figure 49: Add CA Certificate

Cert. Name	Enter the Certificate name for the CA. ***Note:*** *It could be any name to identify this certificate. Example: "CATest".*
Key Length	Choose the key length for generating the CA certificate. The following values are available: ● **512:** 512-bit keys are not secure and it's better to avoid this option. ● **1024**: 1024-bit keys are no longer sufficient to protect against attacks. ● **2048:** 2048-bit keys are a good minimum. (Recommended). ● **4096:** 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.
Digest Algorithm	Choose the digest algorithm: ● **SHA1:** This digest algorithm provides a 160-bit fingerprint output based on arbitrary-length input. ● **SHA256:** This digest algorithm generates an almost unique, fixed-size 256 bit hash. ***Note:*** *Hash is a one-way function, it cannot be decrypted back.*
Expiration (D)	Enter the validity date for the CA certificate in days. *In our example, set to "120".*
Country / Region	Select a country code from the dropdown list. *Example: "MA".*
State / Province	Enter a state name or province. *Example: "Casablanca".*
City	Enter a city name. *Example: "Casablanca".*
Organization	Enter the organization's name. *Example: "GS".*

Organizational Unit	This field is the name of the department or organization unit making the request. *Example: "GS Sales".*
Email	Enter an email address. *Example: "grandstream@gmail.com"*

Table 15: CA Certificate

Click on Save button after completing all the fields for the CA certificate.

Click on button to export the CA to the local computer. The CA file has the extension ".crt".

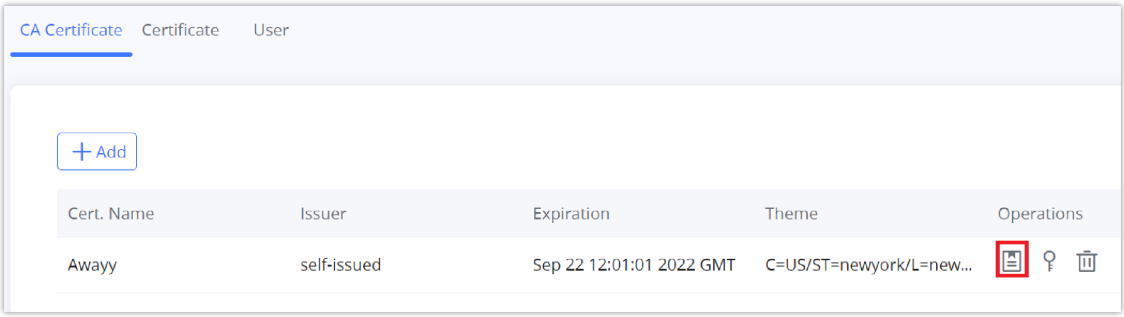

Figure 50: CA Certificate

Generate Server/Client Certificates

Create both server and client certificates for encrypted communication between clients and GWN70xx acting as an OpenVPN® server.

Creating Server Certificate

To create a server certificate, follow the below steps:

1. Navigate to "**Web UI → System Settings → Certificate Management → Certificate**".

2. Click on Add button. A popup window will appear.

Refer to the below figure showing an example of configuration and the table showing all available options with their respective descriptions.

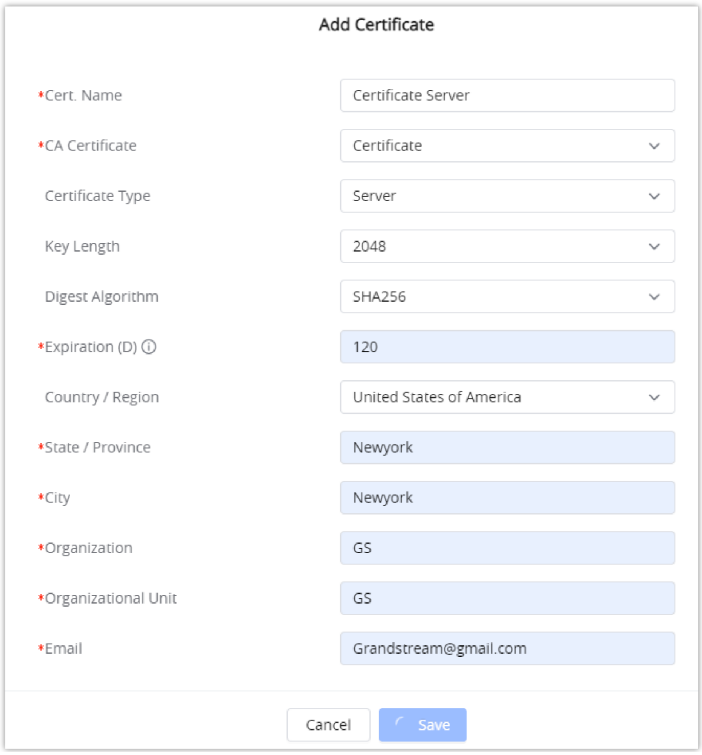

Figure 51: Certificate Server

Cert. Name	Enter the common name for the server certificate. ***Note:*** *It could be any name to identify this certificate.* *Example: "ServerCertificate".*
CA Certificate	Select the CA certificate previously generated from the drop-down list. *Example: "CATest".*
Certificate Type	Choose the certificate type from the drop-down list. It can be either a client or a server certificate. *Choose "Server" to generate a server certificate.*
Key Length	Choose the key length for generating the CA certificate. The following values are available: ● **512:** 512-bit keys are not secure and it's better to avoid this option. ● **1024**: 1024-bit keys are no longer sufficient to protect against attacks. ● **2048:** 2048-bit keys are a good minimum. (Recommended). ● **4096:** 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.
Digest Algorithm	Choose the digest algorithm: ● **SHA1:** This digest algorithm provides a 160-bit fingerprint output based on arbitrary-length input. ● **SHA256:** This digest algorithm generates an almost unique, fixed-size 256 bit hash. ***Note:*** *Hash is a one-way function, it cannot be decrypted back.*
Expiration (D)	Enter the validity date for the CA certificate in days. *In our example, set to "120".*
Country / Region	Select a country code from the dropdown list. *Example: "MA".*
State / Province	Enter a state name or province. *Example: "Casablanca".*
City	Enter a city name. *Example: "Casablanca".*
Organization	Enter the organization's name. *Example: "GS".*
Organizational Unit	This field is the name of the department or organization unit making the request. *Example: "GS Sales".*
Email	Enter an email address. *Example: "grandstream@gmail.com"*

Table 16: Server Certificate

○ Click on Save button after completing all the fields for the server certificate.

○ Click on to export the server certificate file in ".crt" format.

○ Click on to export the server key file in ".key" format.

○ Click on to delete the server certificate if no longer needed.

- The server certificates (.crt and .key) will be used by the GWN70xx router when acting as a server.
- The server certificates (.crt and .key) can be exported and used on another OpenVPN® server

Creating Client Certificate

To create a client certificate, follow the below steps:

1. Create Users

○ Navigate to "**Web UI → System Settings → Certificate Management → User**".

○ Click on + Add button. The following window will pop up.

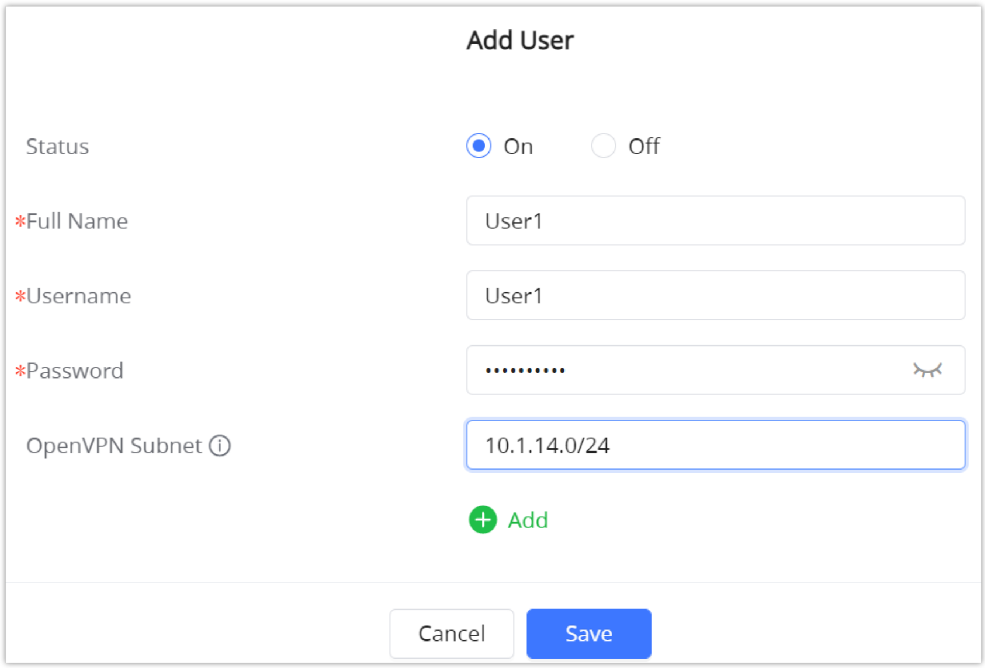

Figure 52: User Certificate

Enter User information based on the below descriptions.

Status	Click on "**ON**" to enable the user.
Full Name	Choose full name to identify the users.
User Name	Choose username to distinguish user's certificate.
Password	Enter user password for each username.
OpenVPN Subnet	Used to indicate which networks are located behind the remote device when the user account is used by an OpenVPN client router to establish a site-to-site VPN.

Table 17: Client Certificate

2. Create Client Certificate

○ Navigate to "**Web UI → System Settings → Certificate Management → Certificate**".

○ Click on + Add button. The following window will pop up.

Enter client certificate information based on the below descriptions.

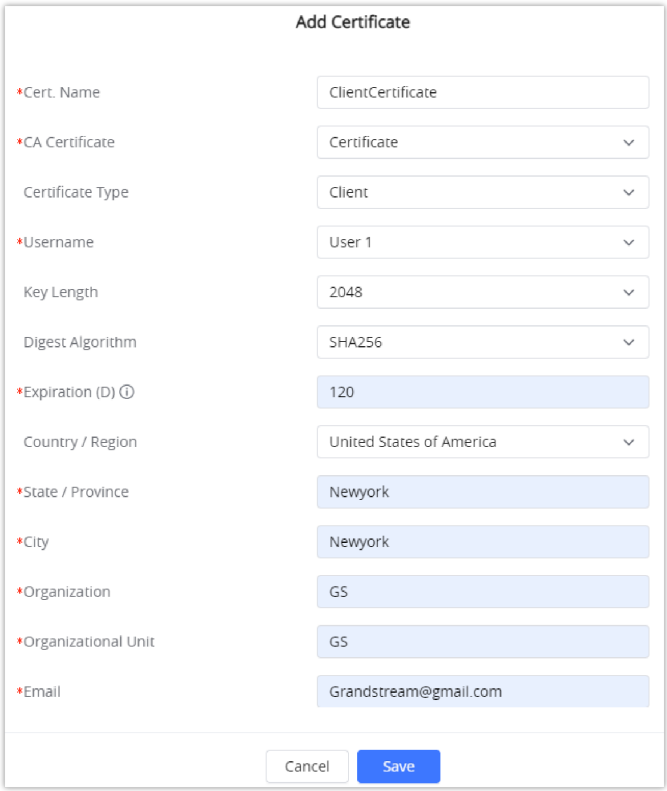

Figure 53: Client Certificate

Cert. Name	Enter the common name for the server certificate. ***Note:*** *It could be any name to identify this certificate.* *Example: "ClientCertificate".*
CA Certificate	Select the CA certificate previously generated from the drop-down list. *Example: "CATest".*
Certificate Type	Choose the certificate type from the drop-down list. It can be either a client or a server certificate. *Choose "Server" to generate a server certificate.*
Username	Select created user to generate his certificate.
Key Length	Choose the key length for generating the CA certificate. The following values are available: ● **512:** 512-bit keys are not secure and it's better to avoid this option. ● **1024**: 1024-bit keys are no longer sufficient to protect against attacks. ● **2048:** 2048-bit keys are a good minimum. (Recommended). ● **4096:** 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.
Digest Algorithm	Choose the digest algorithm: ● **SHA1:** This digest algorithm provides a 160-bit fingerprint output based on arbitrary-length input. ● **SHA256:** This digest algorithm generates an almost unique, fixed-size 256 bit hash. ***Note:*** *Hash is a one-way function, it cannot be decrypted back.*
Expiration (D)	Enter the validity date for the CA certificate in days. *In our example, set to "120".*
Country / Region	Select a country code from the dropdown list. *Example: "MA".*

State / Province	Enter a state name or province. *Example: "Casablanca".*
City	Enter a city name. *Example: "Casablanca".*
Organization	Enter the organization's name. *Example: "GS".*
Organizational Unit	This field is the name of the department or organization unit making the request. *Example: "GS Sales".*
Email	Enter an email address. *Example: "user@grandstream.com"*

Table 18: Client Certificate

○ Click on to export the server certificate file in ".crt" format.

○ Click on to export the server key file in ".key" format.

○ Click on to delete the server certificate if no long

- Client certificates generated from the GWN70xx need to be uploaded to the clients.
- For security improvement, each client needs to have his username and certificate, this way even if a user is compromised, other users will not be affected.

Create OpenVPN® Server

Once client and server certificates are successfully created, you can create a new server, so that clients can be connected to it, by navigating under "**Web UI → VPN → VPN Server → OpenVPN® Server**".

To create a new VPN server, follow the below steps:

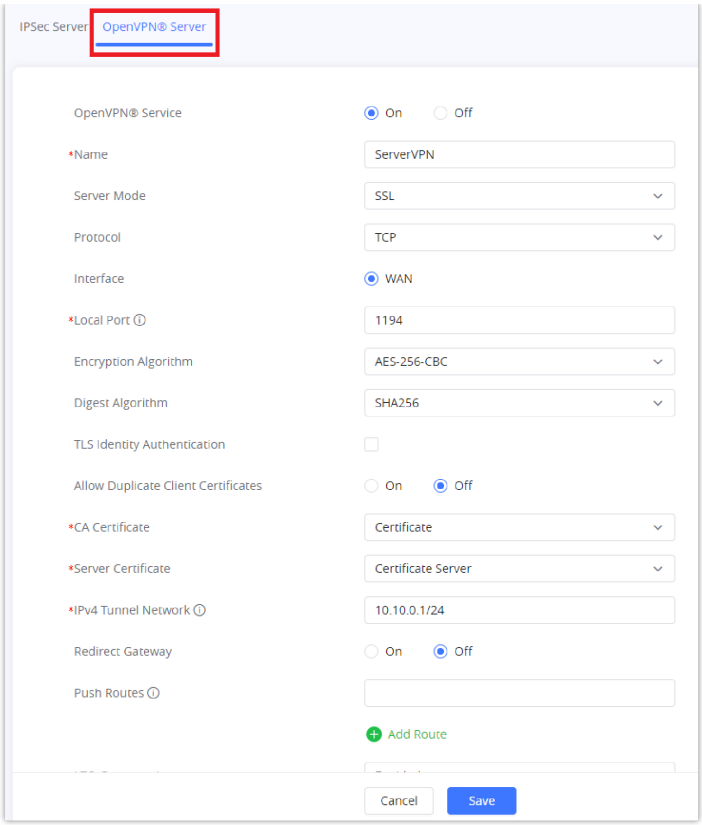

Figure 54: Create OpenVPN® Server

Click Save after completing all the fields.

Refer to the table below:

OpenVPN® Service	Click on "**ON**" to enable the OpenVPN Server
Name	Enter a name for the OpenVPN® server.
Server Mode	Choose the server mode the OpenVPN® server will operate with. 4 modes are available: ● **SSL:** Authentication is made using certificates only (no user/pass authentication). Each user has a unique client configuration that includes their personal certificate and key. This is useful if clients should not be prompted to enter a username and password, but it is less secure as it relies only on something the user has (TLS key and certificate). ● **User Authentication:** Authentication is made using only CA, user and password, no certificates. Useful if the clients should not have individual certificates. Less secure as it relies on a shared TLS key plus only something the user knows (Username/password). ● **SSL + User Authentication:** Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key. ● **PSK:** Used to establish a point-to-point OpenVPN® configuration. A VPN tunnel will be created with a server endpoint of a specified IP and a client endpoint of specified IP. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN® port. Most secure as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know).
Protocol	Choose the Transport protocol from the dropdown list, either TCP or UDP. The default protocol is UDP.
Interface	Select the interface used to connect the GWN70xx to the uplink.
Local Port	Configure the listening port for OpenVPN® server. *The default value is 1194.*
Encryption Algorithm	Choose the encryption algorithm from the dropdown list to encrypt data so that the receiver can decrypt it

	using same algorithm.
Digest Algorithm	Choose digest algorithm from the dropdown list, which will uniquely identify the data to provide data integrity and ensure that the receiver has an unmodified data from the one sent by the original host.
TLS Identicy Authentication	This option uses a static Pre-Shared Key (PSK) that must be generated in advance and shared among all peers. This feature adds extra protection to the TLS channel by requiring that incoming packets have a valid signature generated using the PSK key.
Allow Duplicate Client Certificates	Click on "**ON**" to allow duplicate Client Certificates
CA Certificate	Select a generated CA from the dropdown list or add one.
Server Certificate	Select a generated Server Certificate from the dropdown list or add one.
IPv4 Tunnel Network	Enter the network range that the GWN70xx will be serving from to the OpenVPN® client. ***Note:*** *The network format should be the following 10.0.10.0/16.* *The mask should be at least 16 bits.*
Redirect Gateway	When redirect-gateway is used, OpenVPN® clients will route DNS queries through the VPN, and the VPN server will need to handle them.
Push Routes	Specify route(s) to be pushed to all clients. *Example: 10.0.0.1/8*
LZO Compression	Select whether to activate LZO compression or no, if set to “Adaptive”, the server will make the decision whether this option will be enabled or no.
Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.

Table 19: OpenVPN Server

OpenVPN® Client Configuration

There are two ways to use the GWN70xx as an OpenVPN® client:

1. Upload client certificate created from an OpenVPN® server to GWN70xx.

2. Create client/server certificates on GWN70xx and upload the server certificate to the OpenVPN® server.

Go to Go to “**VPN → VPN Clien**t” and follow the steps below:

Click on + Add button. The following window will pop up.

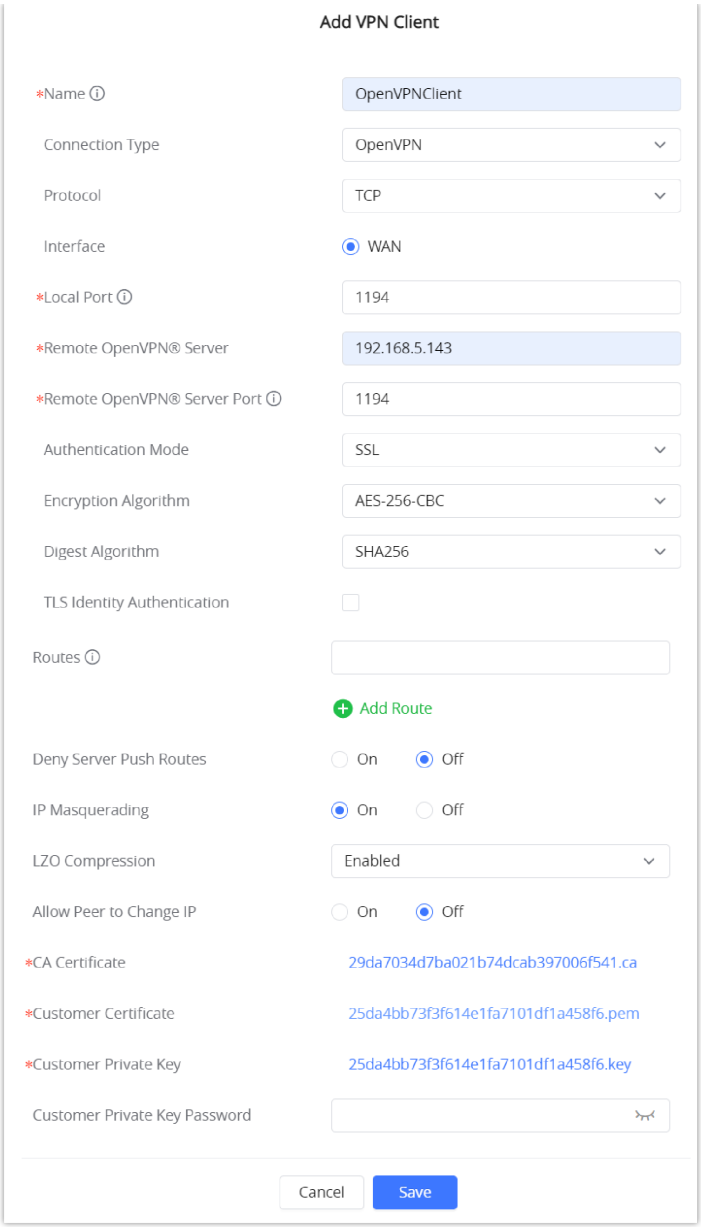

Figure 55: OpenVPN® Client

Click Save after completing all the fields.

L2TP Configuration

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

L2TP Client Configuration

To configure the L2TP client on the GWN70xx router, navigate under **"VPN → VPN Clients"** and set the followings:

1. Click on + Add button and the following window will pop up.

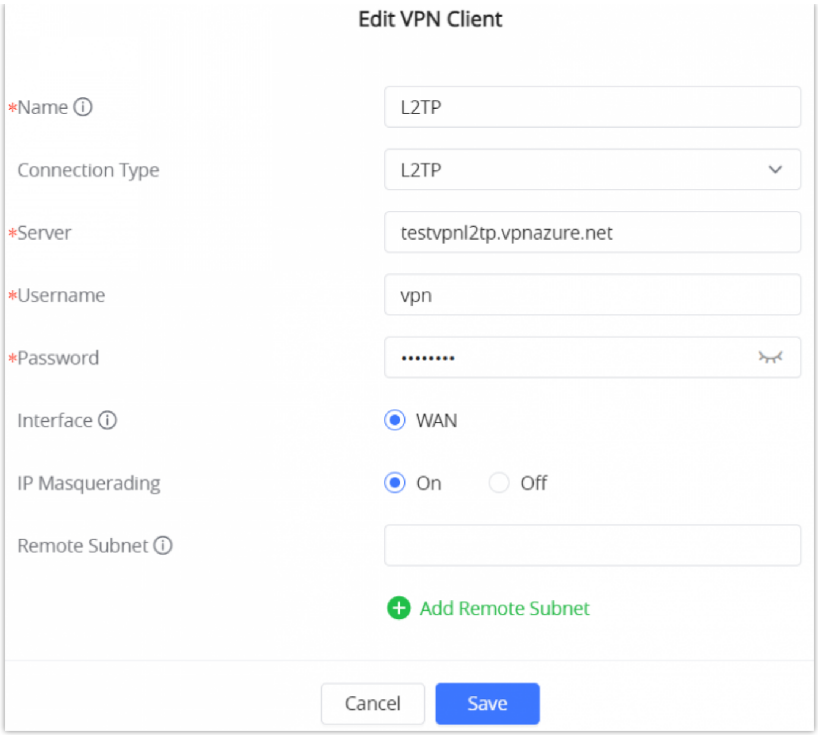

Figure 56: L2TP Client Configuration

Click Save after completing all the fields.

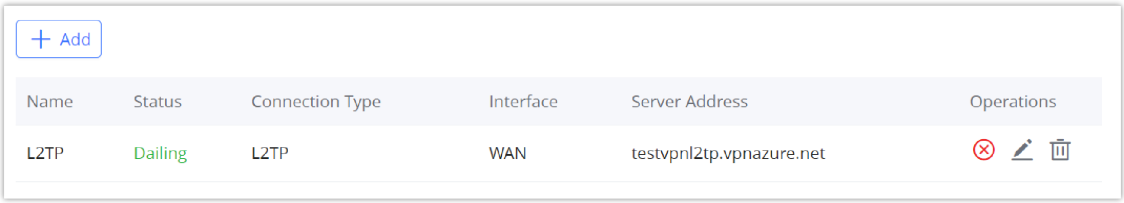

Figure 57: L2TP Client

PPTP Configuration

A data-link layer protocol for wide area networks (WANs) based on the Point-to-Point Protocol (PPP) and developed by Microsoft enables network traffic to be encapsulated and routed over an unsecured public network such as the Internet. Point-to-Point Tunneling Protocol (PPTP) allows the creation of virtual private networks (VPNs), which tunnel TCP/IP traffic through the Internet.

Client Configuration

To configure the PPTP client on the GWN70xx, navigate under "

"VPN → VPN Clients" and set the followings:

1. Click on + Add button and the following window will pop up.

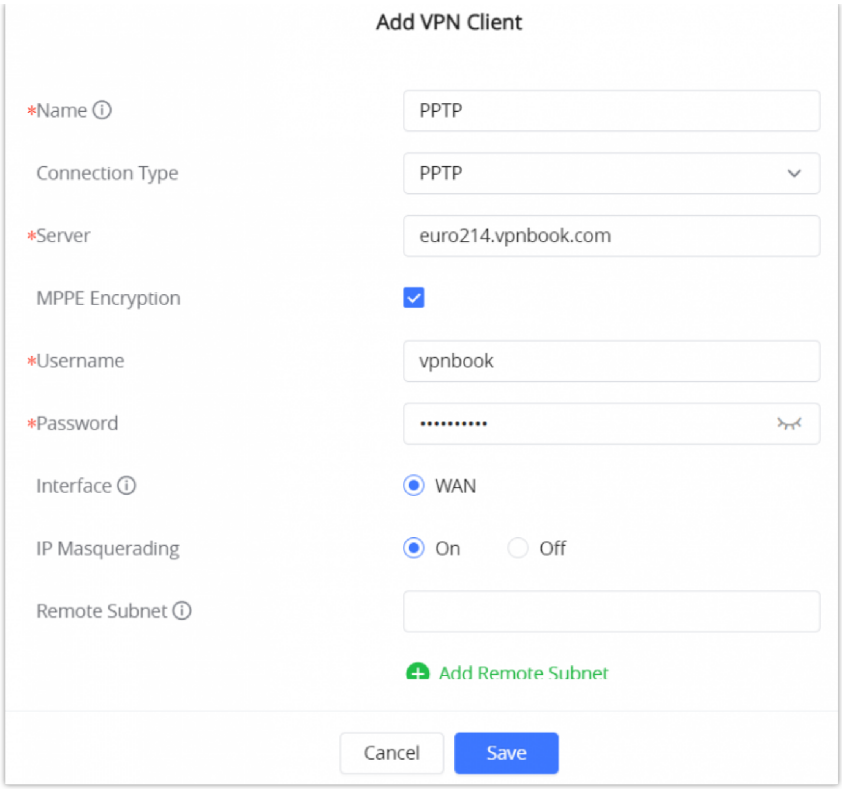

Figure 58: PPTP Client Configuration

Click Save after completing all the fields.

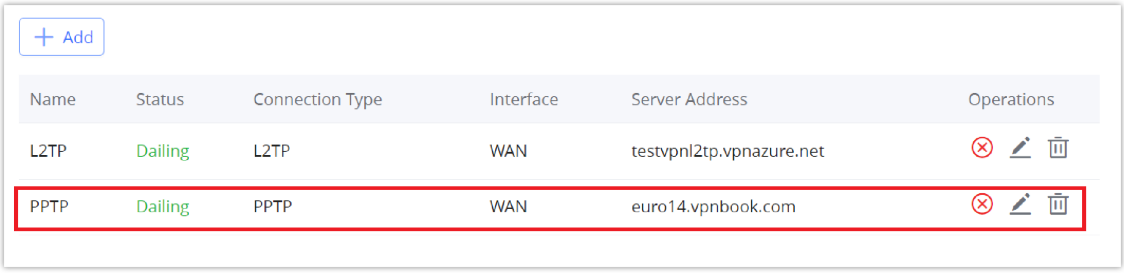

Figure 59: PPTP Client

IPSec VPN Tunnel

Overview

Internet Security protocol- IPsec is mainly used to authenticate and encrypt packets of data sent over the network layer. To accomplish this, they use two security protocols – ESP (Encapsulation Security Payload) and AH (Authentication Header), the former provides both authentications as well as encryption whereas the latter provides only authentication for the data packets. Since both authentication and encryption are equally desirable, most of the implementations use ESP.

IPsec supports two different encryption modes, they are Tunnel (default) and Transport mode. Tunnel mode is used to encrypt both payloads as well as the header of an IP packet, which is considered to be more secure. Transport mode is used to encrypt only the payload of an IP packet, which is generally used in gateway or host implementations.

IPsec also involves IKE (Internet Key Exchange) protocol which is used to set up the Security Associations (SA). A Security Association establishes a set of shared security parameters between two network entities to provide secure network layer communication. These security parameters may include the cryptographic algorithm and mode, traffic encryption key, and parameters for the network data to be sent over the connection. Currently, there are two IKE versions available – IKEv1 and IKEv2. IKE works in two phases:

○ **Phase 1:** ISAKMP operations will be performed after a secure channel is established between two network entities.

○ **Phase 2:** Security Associations will be negotiated between two network entities.

IKE operates in three modes for exchanging keying information and establishing security associations – Main, Aggressive and Quick mode.

• **Main mode:** is used to establish phase 1 during the key exchange. It uses three two-way exchanges between the initiator and the receiver. In the first exchange, algorithms and hashes are exchanged. In the second exchange, shared keys are generated using the Diffie-Hellman exchange. In the last exchange, verification of each other's identities takes place.

• **Aggressive mode**: provides the same service as the main mode, but it uses two exchanges instead of three. It does not provide identity protection, which makes it vulnerable to hackers. The main mode is more secure than this.

• **Quick mode**: After establishing a secure channel using either the main mode or aggressive mode, the quick mode can be used to negotiate general IPsec security services and generate newly keyed material. They are always encrypted under the secure channel and use the hash payload that is used to authenticate the rest of the packet.

Configuring IPSec Tunnel

To build an IPSec secure tunnel between two devices located in different places on the Internet, we can use the sample scenario below:

The branch office router needs to connect to the Headquarters office via an IPSec tunnel, on each side we have a GWN70xx router. Users can configure the two devices as follows:

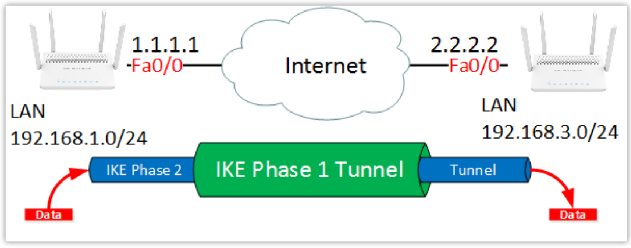

Figure 60: IPSec Tunnel

The branch office router runs a LAN subnet 192.168.1.0/24 and the HQ router runs a LAN subnet 192.168.3.0, the public IP of the branch office router is 1.1.1.1 and the IP of the HQ router is 2.2.2.2.

○ **Configuration of the Branch office router:**

Go under **VPN** → **VPN Clients** then click on + Add to add a VPN Client.

○ **IPSec VPN**

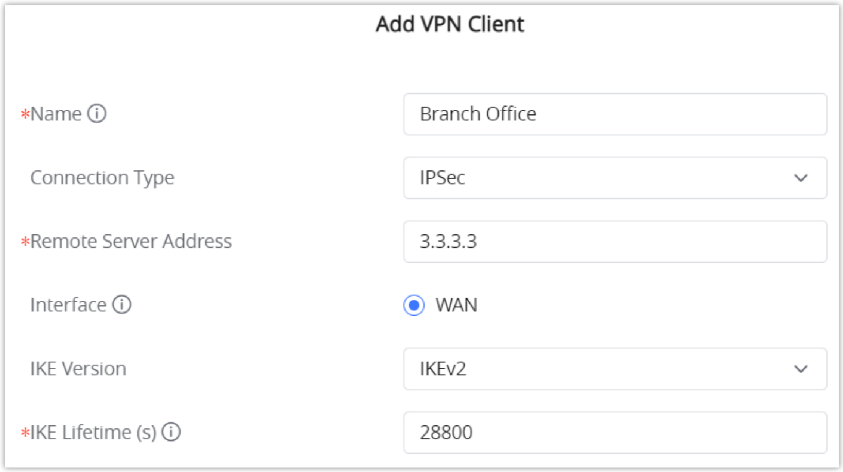

Figure 61: Add VPN Client – IPSec

○ **Phase 1**

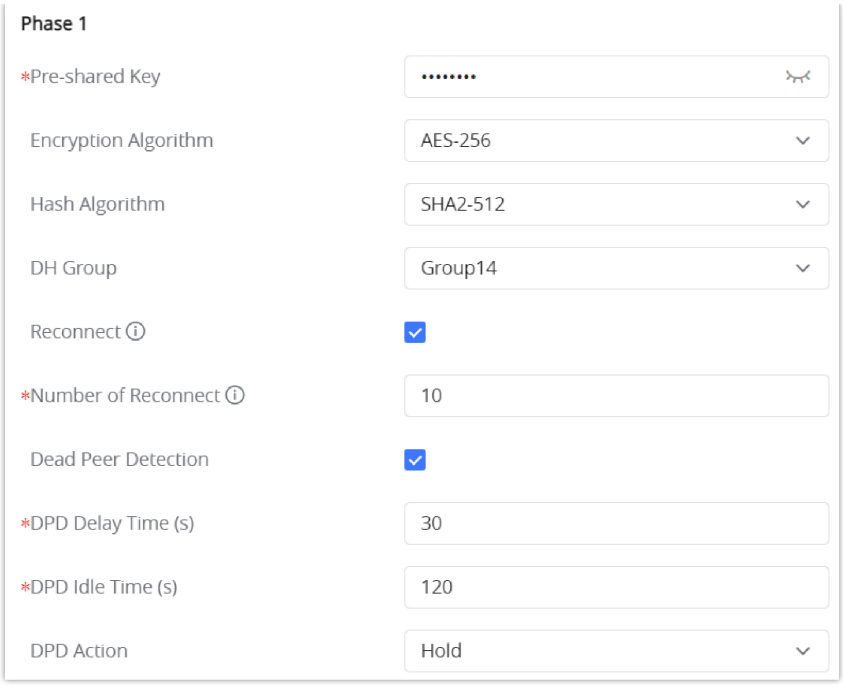

Figure 62: Add VPN Client – Phase 1

○ **Phase 2**

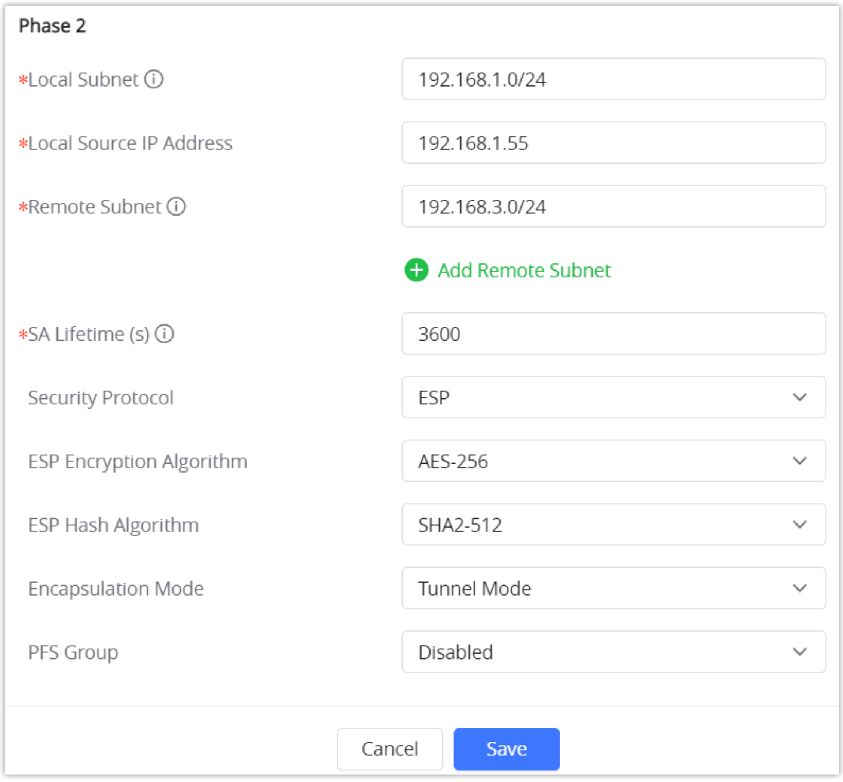

Figure 63: Add VPN Client – Phase 2

After this is done, press “save” and do the same for the HQ Router. The two routers will build the tunnel and the necessary routing information to route traffic through the tunnel back and from the branch office to the HQ network.

○ **Configuration of IPSec Server**

Go under **VPN → VPN Server → IPSec Server Tab** then fill in the following information:

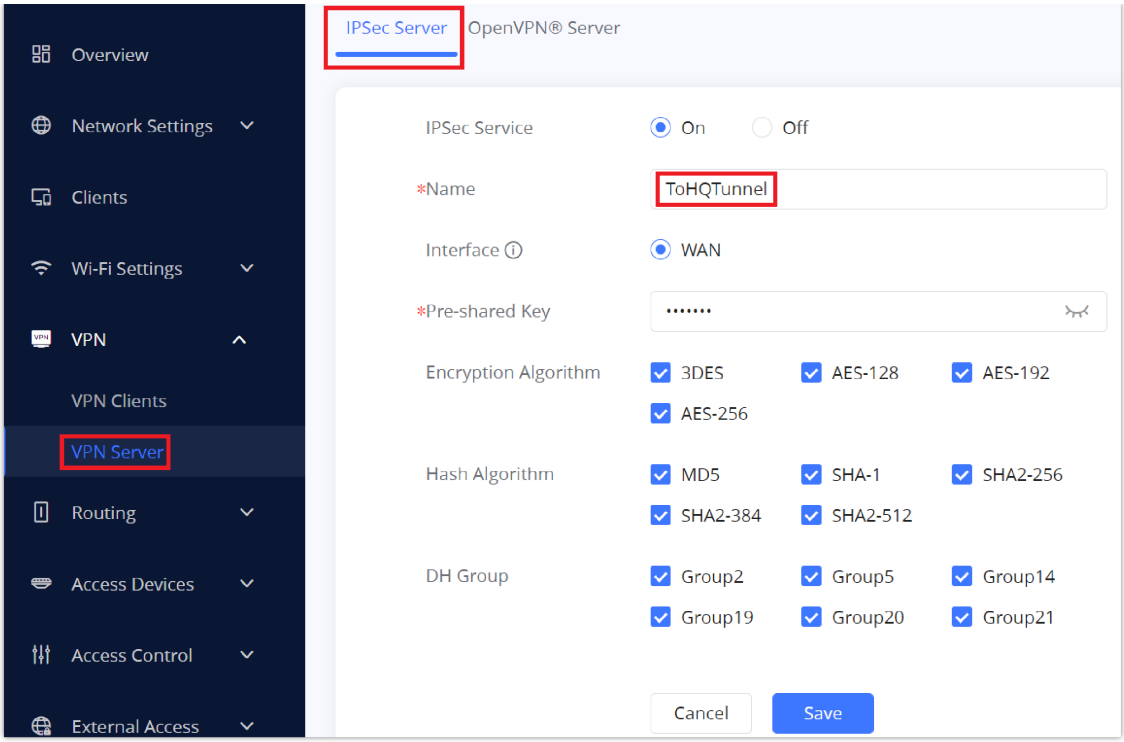

Figure 64: Branch Office IPSec Configuration

Press Save, then click + Add in order to configure **Remote Dial-in User**:

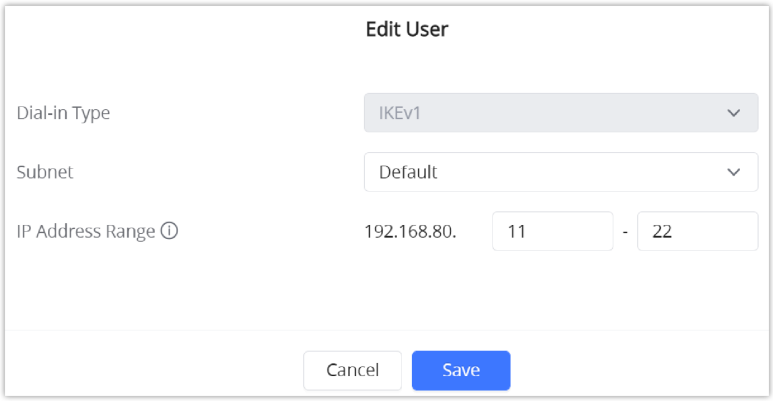

Figure 65: Remote Dial-in User

FIREWALL AND EXTERNAL ACCESS

GWN70xx router supports firewall features to control incoming and outgoing traffic by restricting or rejecting specific traffic, as well as preventing attacks on the GWN70xx networks for enhanced security. And features like DMZ allows a computer to be fully exposed to the internet.

External Access

GWN70xx can enable features like Port Forwarding to access it from outside the network as well as DMZ to expose physical or logical sub-network and also Universal Plug and Play (UPnP).

DDNS

1. Access to GWN70xx web GUI, navigate to **External Access** → **DDNS**, and click + Add to Add Service.

2. Fill in the domain name created with the DDNS provider under the Service Provider field.

3. Enter your account username and password under the User Name and Password fields.

4. Specify the Domain to which DDNS Account is applied under Domain.

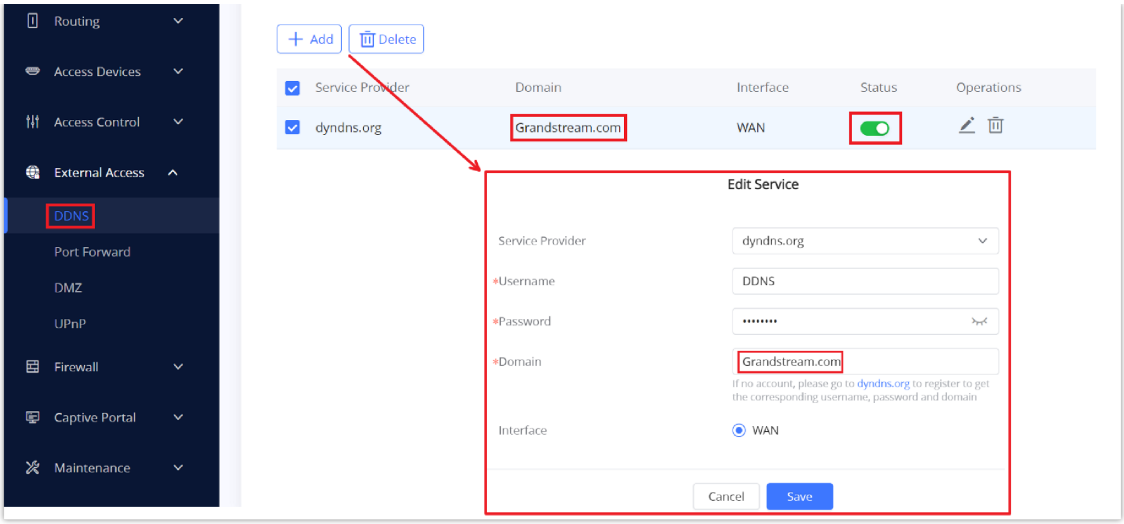

Figure 66: DDNS Page

Service Provider	Select the DDNS provider from the list
Username	Enter the Username
Password	Enter the Password
Domain	Enter the Domain
Interface	Select the Interface

Table 20: DDNS

Port Forward

Port forwarding allows redirecting a communication request from one address and port number combination to another.

Navigate to **GWN70xx WEB UI → External Access → Port Forward**:
Below are different possible actions

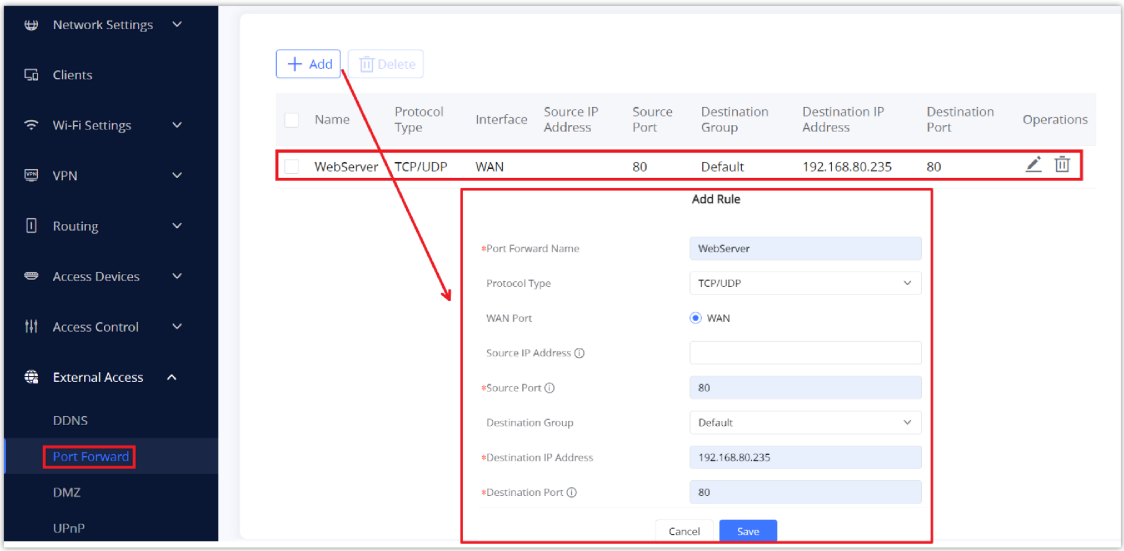

Figure 67: Port Forwarding page

Refer to the following table for the Port Forwarding option when editing or creating a port-forwarding rule:

Port Forward Name	Specify a name for the port forward rule.

Protocol Type	Select a protocol, users can select TCP, UDP or TCP/UDP.
WAN port	Select the WAN port
Source IP Address	Sets the IP address that external users access to this device. If not set, any IP address on the corresponding WAN port can be used
Source Port	Set a single or a range of Ports.
Destination Group	Select VLAN group.
Destination IP Address	Set the destination IP address.
Destination Port	Set a single or a range of Ports.

Table 21: Port Forward

DMZ

This section can be accessed from **GWN70xx Web GUI → External Access → DMZ**.
GWN70xx supports **DMZ**, where it is possible to specify a Hostname IP Address to be put on the **DMZ**.

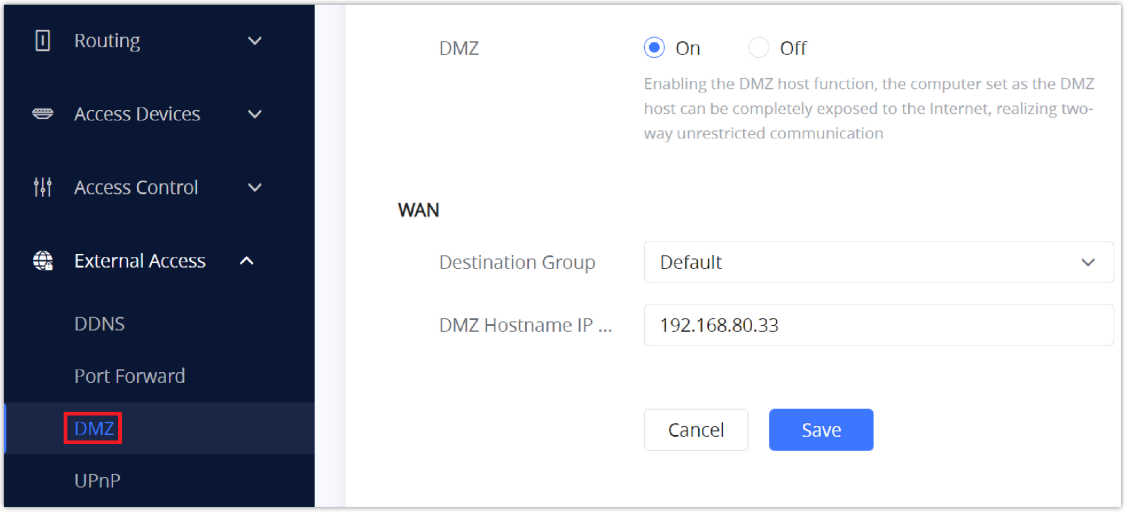

Figure 68: DMZ Page

Enabling the DMZ host function, the computer set as the DMZ host can be completely exposed to the Internet, realizing two-way unrestricted communication.

Refer to the below table for DMZ fields:

DMZ	Click on "**ON**" to enable DMZ
Destination Group	Select the LAN group.
DMZ Hostname IP Address	Set the destination IP address.

Table 22: DMZ

UPnP

GWN70xx supports UPnP that enables programs running on a host to configure automatically port forwarding.

UPnP allows a program to make the GWN70xx open necessary ports, without any intervention from the user, without making any check.

UPnP settings can be accessed from GWN70xx **Web GUI → External Access → UPnP.**

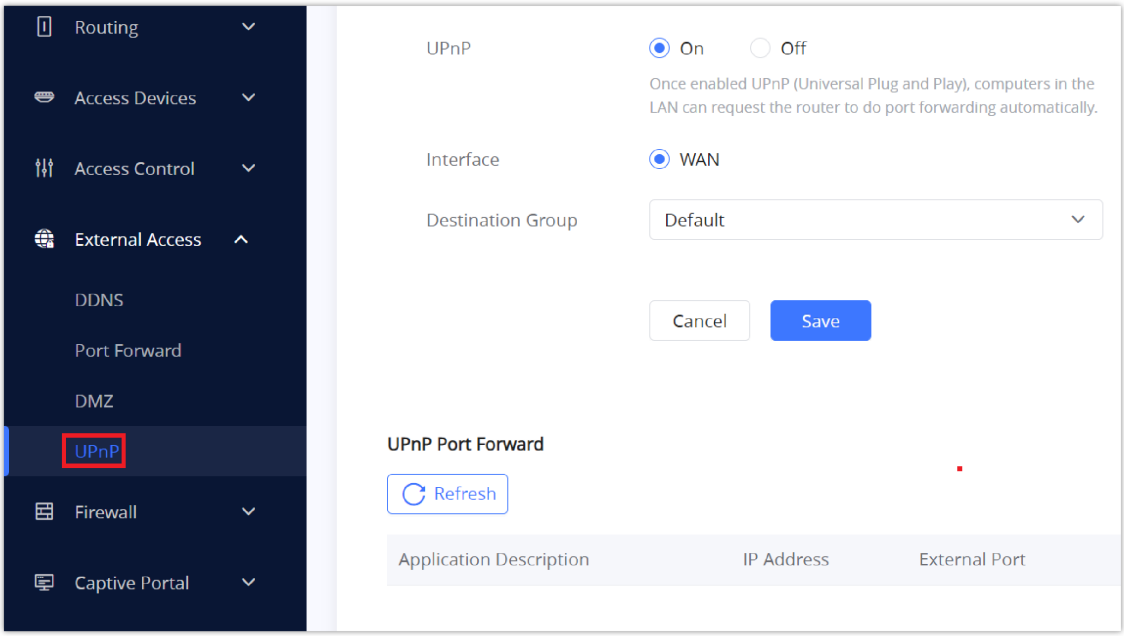

Figure 69: UPnP Settings

UPnP	Click on "**ON**" to enable UPnP. **Note**: Once enabled UPnP (Universal Plug and Play), computers in the LAN can request the router to do port forwarding automatically
Interface	Select the interface (WAN)
Destination Group	Select the LAN Group

Table 23: UPnP

Firewall

The firewall section provides the ability to set up input/output policies for each WAN interface and LAN group as well as setting configuration for Static and Dynamic NAT and ALG.

Attack Defense

DoS, TCP SYN Flood, UDP Flood, and ICMP Flood Attack Defense are all enabled by default as well as the Ping of Death.

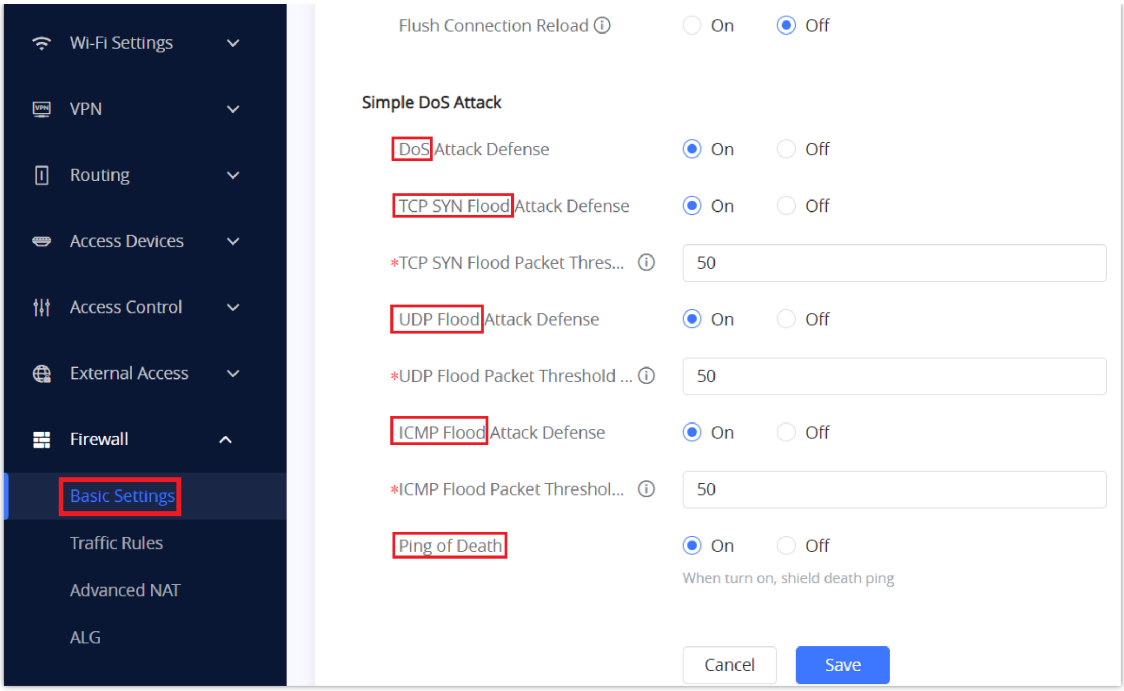

Figure 70: Firewall Basic Settings

Flush Connection Reload: When this option is enabled, and a firewall configuration change is made, existing connections that had been permitted by the previous firewall rules will be terminated. That way if the new firewall rules can't permit a connection that had been previously established, it will be terminated and won't be able to reconnect. When this option is disabled, existing connections are allowed to continue until they do timeout, even if the new rules wouldn't allow these connections to be established.

Traffic Rules

GWN70xx offers the possibility to fully control incoming/outgoing traffic for different protocols in customized scheduled times and take actions for specified rules such as Accept, Reject and Drop.

Traffic Rules settings can be accessed from **GWN70xx Web GUI → Firewall → Traffic Rules.**

Following actions are available to configure Input, output, and forward rules for configured protocols

○ To add new rule, Click on + Add .

○ To edit a rule, click on .

○ To delete a rule, click on .

Inbound Rules

The GWN70xx allows to filter incoming traffic to networks group or port WAN and apply rules such as:

• **Accept:** To allow the traffic to go through.

• **Deny:** A reply will be sent to the remote side stating that the packet is rejected.

• **Drop:** The packet will be dropped without any notice to the remote side.

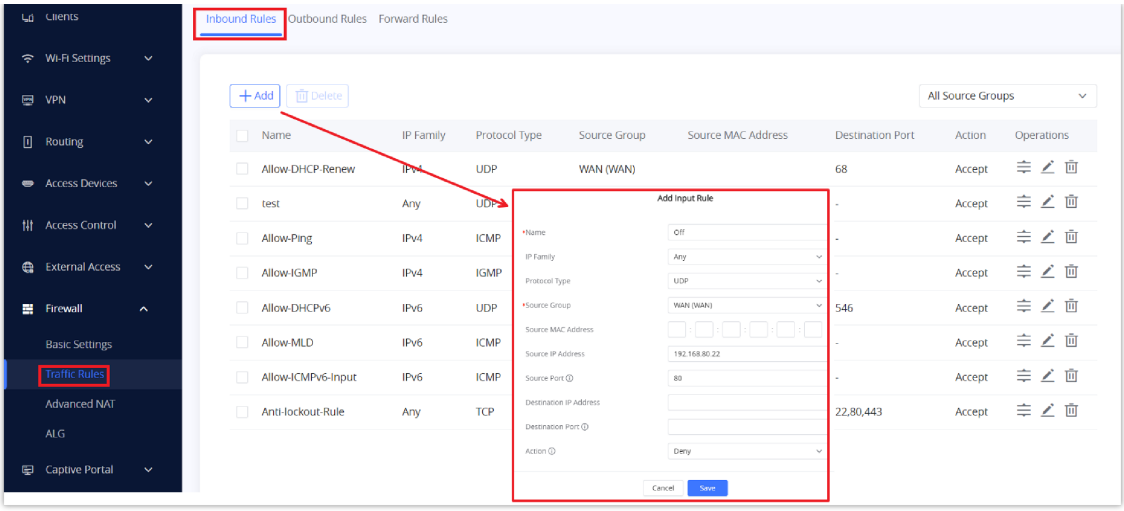

Figure 71: Traffic Rules – Inbound Rules

The following example rejects incoming ICMP requests to the WAN port, this means that whenever the GWN70xx receives an incoming ICMP request on the WAN port the destination IP address will receive a message stating that the destination IP address is unreachable.

Below screenshot shows a configuration example:

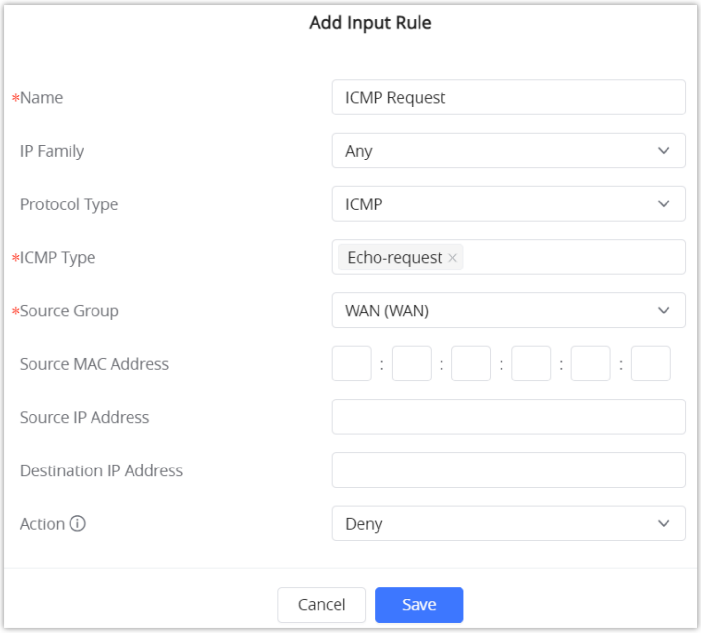

Figure 72: Example of Inbound Rule

Outbound Rules

The GWN70xx allows to filter outgoing traffic from the local LAN networks to outside networks and apply rules such as:

• **Accept:** To allow the traffic to go through.

• **Deny:** A reply will be sent to the remote side stating that the packet is rejected.

• **Drop:** The packet will be dropped without any notice to the remote side.

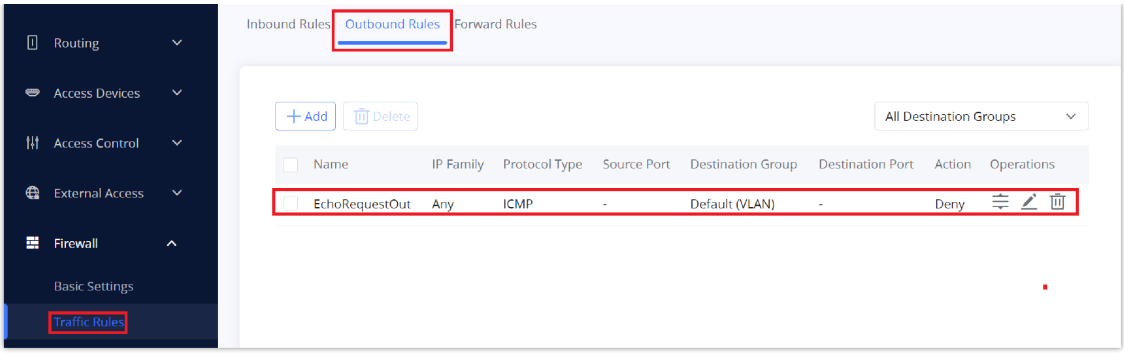

Figure 72: Traffic Rules – Outbound Rules

The following example will deny every outgoing ICMP request from GWN70xx to the default (VLAN), this means that whenever the GWN70xx receives an ICMP "echo-request" from another network group or from a WAN port sent to LAN1 will be rejected.

Below screenshot shows a configuration example:

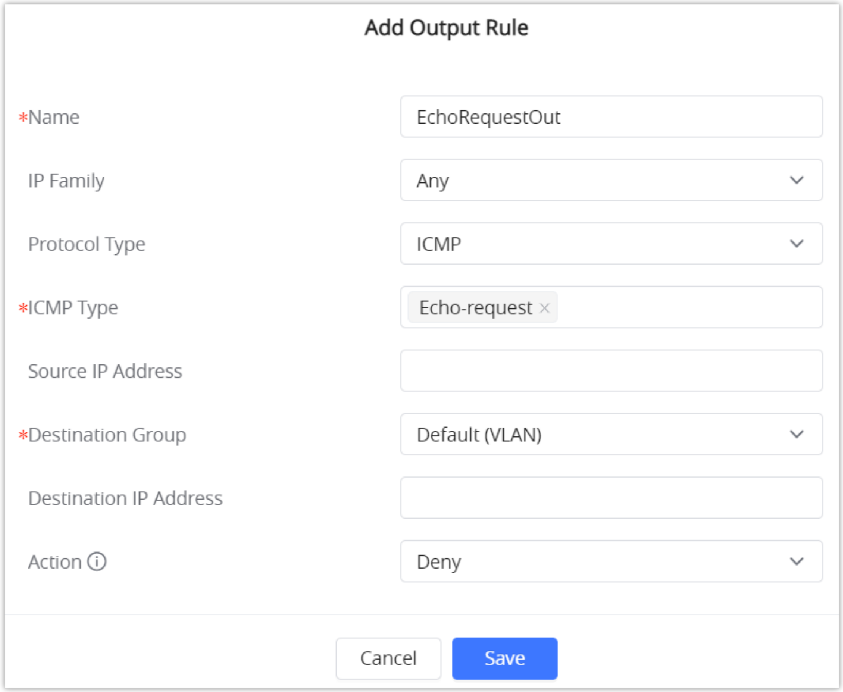

Figure 74: Output Rules Sample

Forward Rules

GWN70xx offers the possibility to allow traffic between different groups and interfaces.

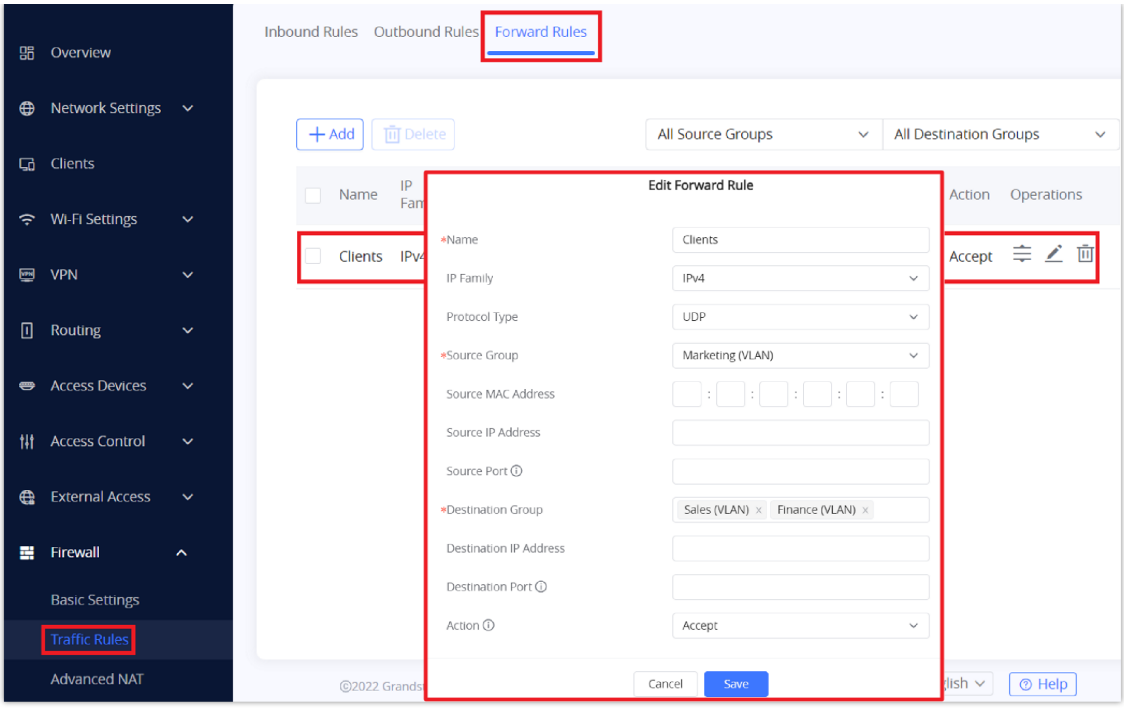

Figure 75: Traffic Rules – Forward Rules

Advanced NAT

The Firewall Advanced NAT page provides the ability to set up the configuration for Static and Dynamic NAT.

SNAT

Following actions are available for SNAT.

Click on + Add to add the Port Forward rule.

Click on to edit a Port Forward rule.

Click on to delete a Port Forward rule.

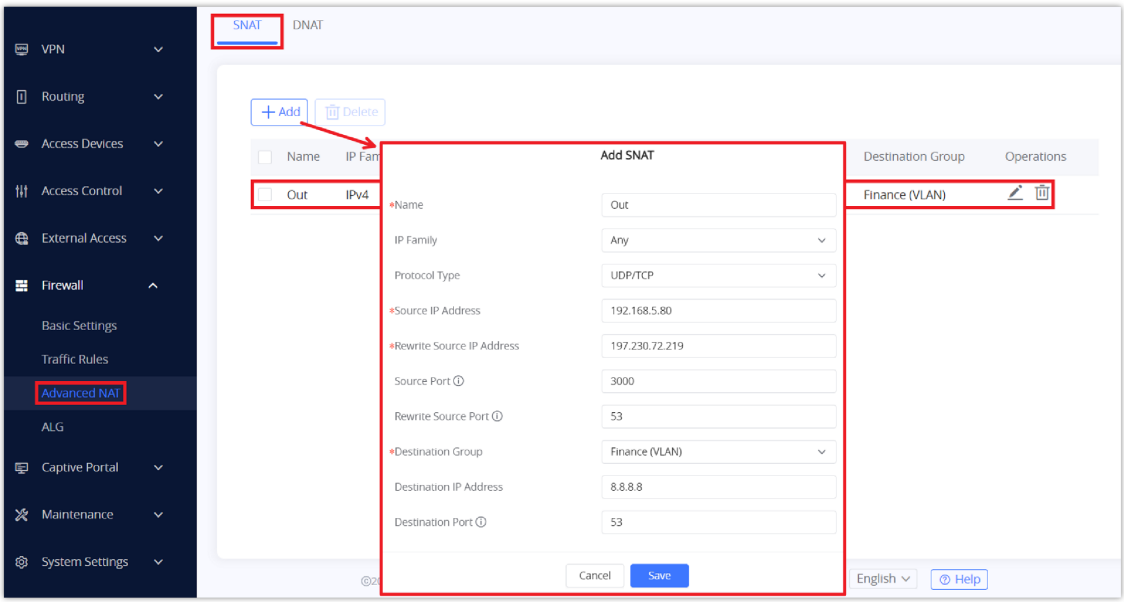

Figure 76: SNAT page

Refer to the below table when creating or editing a SNAT entry:

Name	Specify a name for the SNAT entry

IP Family	Select the IP version, two options are available: IPv4 or Any.
Protocol Type	Select one of the protocols from dropdown list or All, available options are: UDP/TCP, UDP, TCP and All.
Source IP Address	Set the Source IP address.
Rewrite Source IP Address	Set the Rewrite IP. The source IP address of the data package from the source group will be updated to this configured IP.
Source Port	Set the Source Port
Rewrite Source Port	Set the Rewrite source port.
Destination Group	Select a WAN interface or a VLAN for Destination Group.
Destination IP Address	Set the Destination IP address.
Destination Port	Set the Destination Port

Table 24: SNAT

DNAT

The following actions are available for DNAT:

Click on + Add to add the Port Forward rule.

Click on to edit a Port Forward rule.

Click on to delete a Port Forward rule.

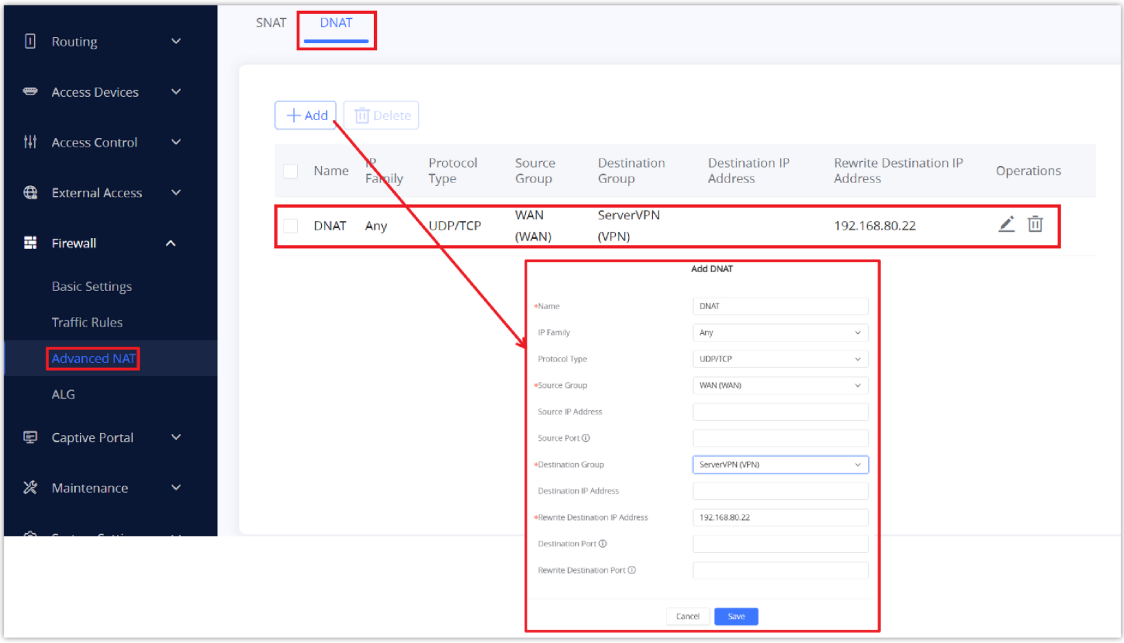

Figure 77: Advanced NAT – DNAT

Refer to the below table when creating or editing a DNAT entry:

Name	Specify a name for the DNAT entry
IP Family	Select the IP version, three options are available: IPv4, IPv6 or Any.

Protocol Type	Select one of the protocols from dropdown list or All, available options are: UDP, TCP, TCP/UCP and All.
Source Group	Select a WAN interface or a LAN group for Source Group, or select All.
Source IP Address	Set the Source IP address.
Source Port	Set the Source Port.
Destination Group	Select a WAN interface or a LAN group for Destination Group, or select All. Make sure that destination and source groups are different to avoid conflict.
Destination IP Address	Set the Destination IP address.
Rewrite Destination IP Address	Set the Rewrite Destination IP Address.
Destination Port	Set the Destination Port.
Rewrite Destination Port	Set the Rewrite Destination Port
NAT Reflection	Click on "**ON**" to enable NAT Reflection
NAT Reflection Source	Select NAT Reflection either Internal or External.

Table 25: DNAT

ALG

ALG stands for **Application Layer Gateway**. Its purpose is to prevent some of the problems caused by router firewalls by inspecting VoIP traffic (packets) and if necessary modifying it. Navigate to **Web GUI → Firewall → ALG** to activate ALG.

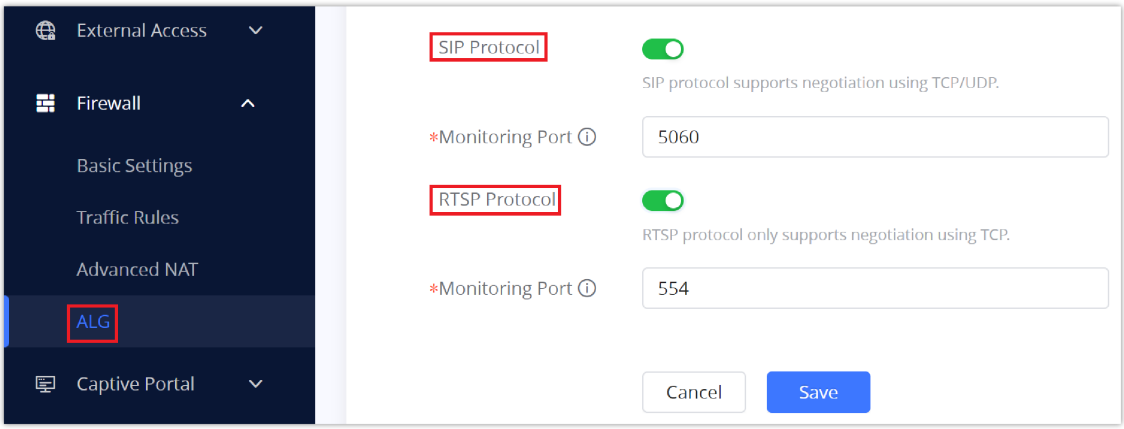

Figure 78: ALG

CAPTIVE PORTAL

Captive Portal feature on GWN70xx helps to define a Landing Page (Web page) that will be displayed on Wi-Fi clients' browsers when attempting to access the Internet. Once connected Wi-Fi clients will be forced to view and interact with that landing page before Internet access is granted.

The Captive Portal feature can be configured from the GWN70xx Web page under "**Captive Portal**".

Policy List

Users can customize a portal policy on this page.

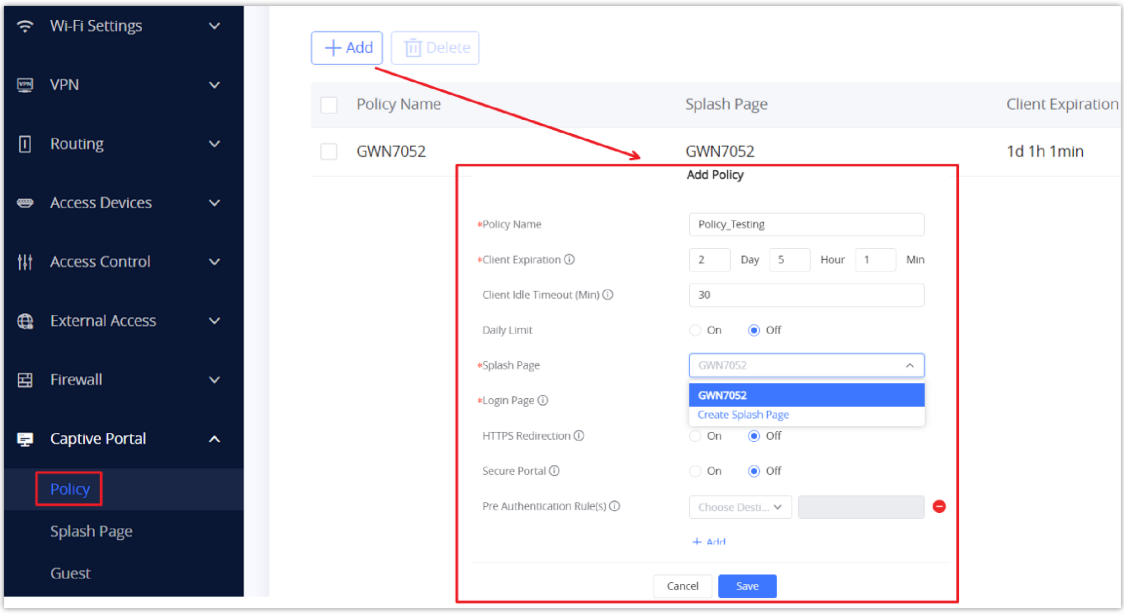

Figure 79: Policy page

Click on + Add to add Port Forward rule.

Click on to edit a Port Forward rule.

Click on to delete a Port Forward rule.

The policy configuration page allows for adding multiple captive portal policies which will be applied to SSIDs and contain options for different authentication types.

Splash Page

The splash page allows users with an easy-to-configure menu to generate a customized splash page that will be displayed to the users when trying to connect to the Wi-Fi.

On this menu, users can create multiple splash pages and assign each one of them to a separate captive portal policy to enforce the select authentication type.

The generation tool provides an intuitive "WYSIWYG" method to customize a captive portal with a very rich manipulation tool.

Users can set the following:

○ **Authentication type**: Add one or more ways from the supported authentication methods (Simple Password, Radius Server, For Free).

○ **Set up a picture (company logo**) to be displayed on the splash page.

○ **Customize** the layout of the page and background colors.

○ **Customize the Terms of use text.**

○ **Visualize a preview** for both mobile devices and laptops.

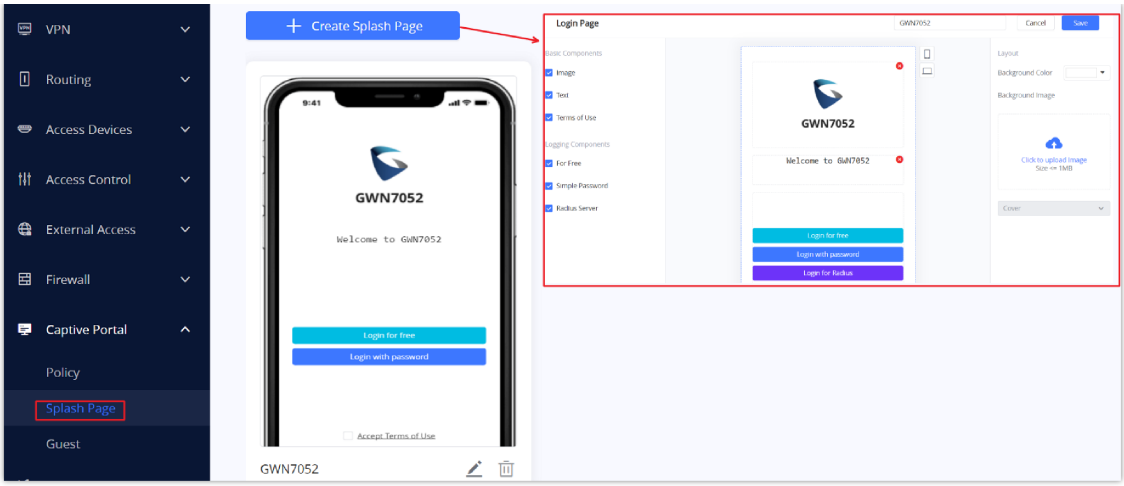

Figure 80: Splash Page

Guest

This section lists the clients connected or trying to connect to Wi-Fi via the Captive Portal.

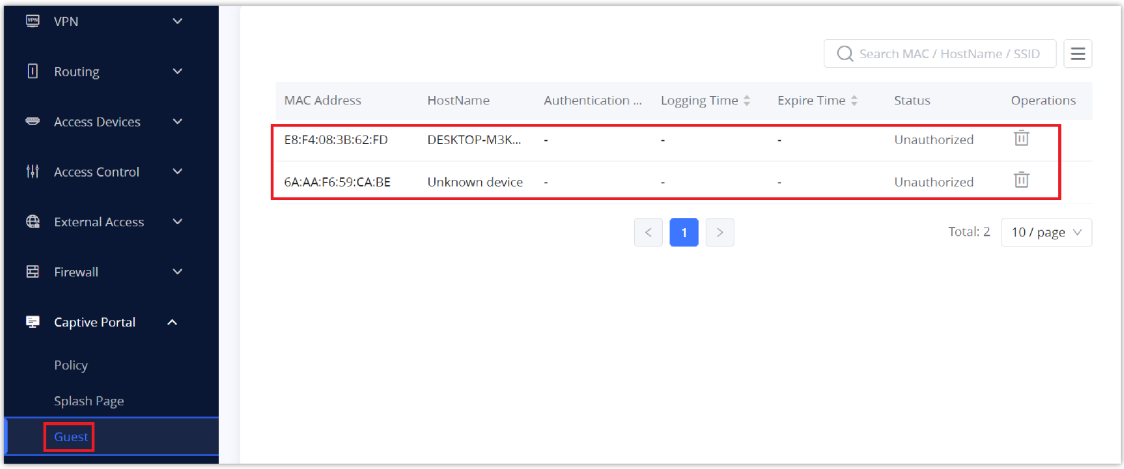

Figure 81: Captive Portal – Guest Page

○ Click on delete button to cancel the authentication, the client must re-authenticate to use the network again.

○ Users can press button to customize items to display on the page. The following items are supported:

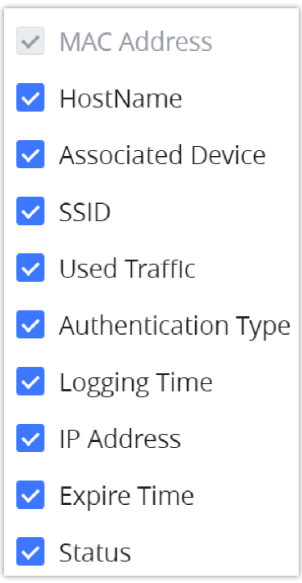

Figure 82: Captive Portal – Guest Page – Select Items

Access Control

GWN70xx has features that can enable the user to block clients and sites as well and also limit the bandwidth per client or SSID.

Blocklist

The Blocklist is a feature in GWN70xx that enables the user to block wireless clients from the available ones or manually add the MAC Address.

To create a new Blocklist, Navigate under: "**Web UI → Access Control → Blocklist**".

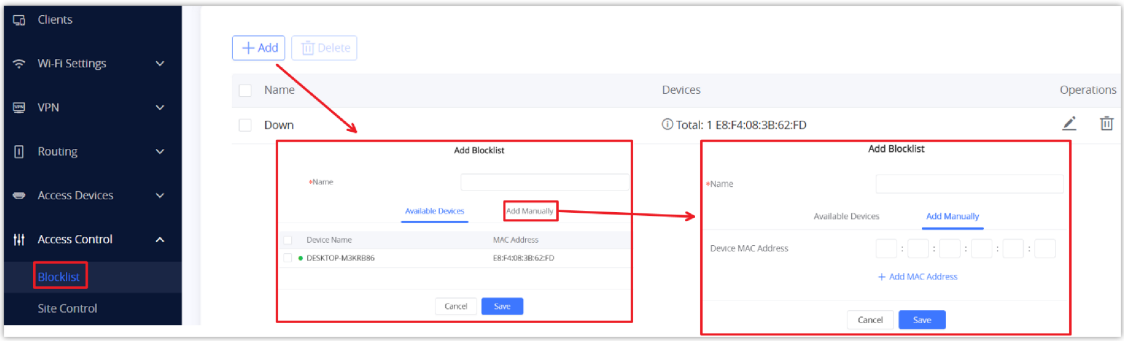

Figure 83: Blocklist Page

Site Control

Site Control is a feature that allows the system administrator to block DNS queries to some domains. This feature can be used to block adware sites, and malware sites, and can be used to block popular social media websites (Facebook, YouTube...etc).

To configure the website blocking policy:

Navigate under: "**Web UI → Access Control → Site Control**".

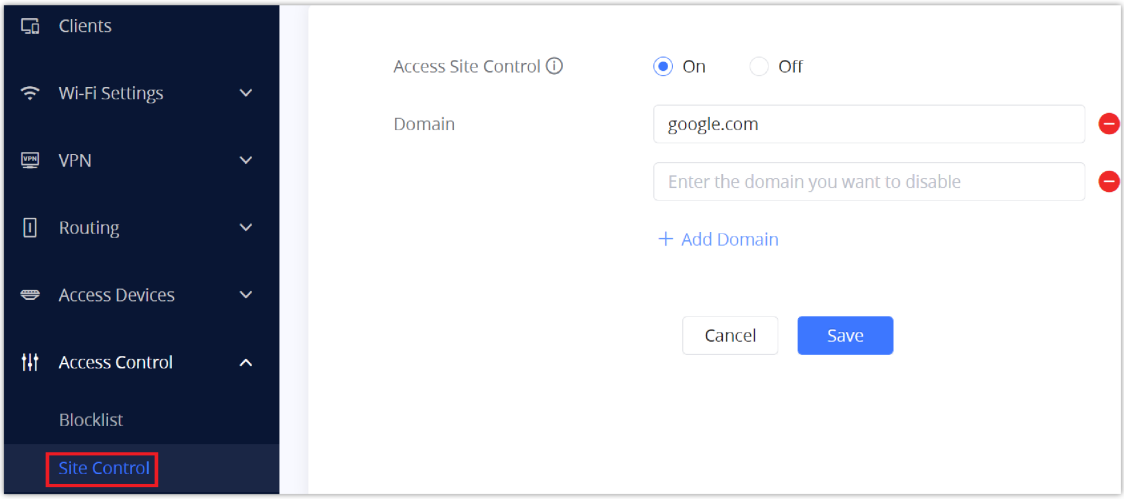

Figure 84: Site Control page

Bandwidth Limit

With GWN70xx the administrator can limit the bandwidth based on the SSID or connected clients or even specify the MAC Address.

Per Client

Under "**Web UI → Clients**". Click on to edit the client then specify a name and maximum upload and download rate for the wireless client.

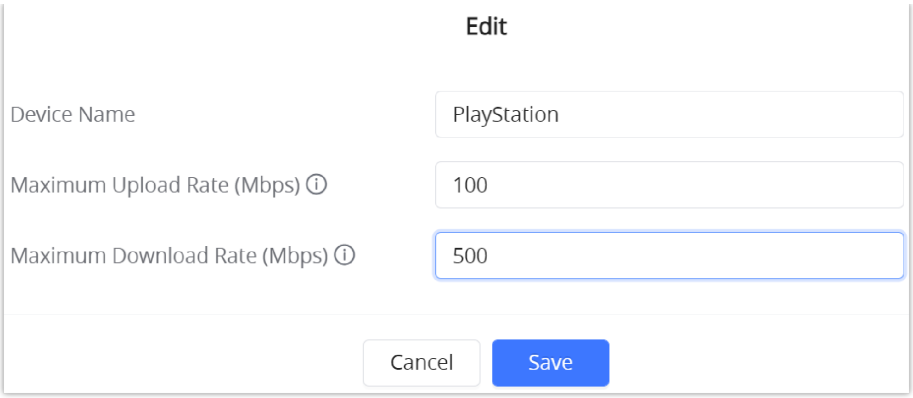

Figure 85: Client bandwidth limit

Per SSID

Under "**Web UI** → **Wi-Fi Settings** → **SSIDs**". Click on edit button, in the "Wi-Fi Settings Tab" and scroll down to "**Advanced**". Then enter the maximum upload and download rate for this SSID.

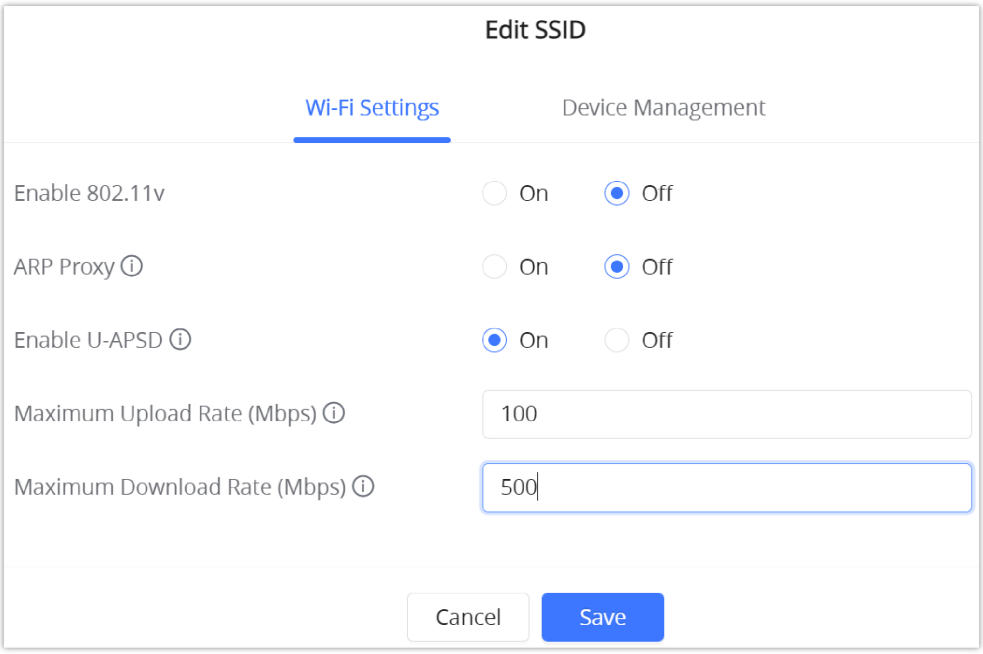

Figure 86: SSID bandwidth limit

MAINTENANCE AND TROUBLESHOOTING

GWN70xx offers multiple tools and options for maintenance and debugging to help further troubleshooting and monitoring the GWN70xx resources.

Maintenance

GWN70xx has many tools to help with maintenance.

Basic Settings

To change the country or region or even schedule a plan for reboot the user can Navigate to "**Web UI** → **System Settings** → **Basic Settings**"

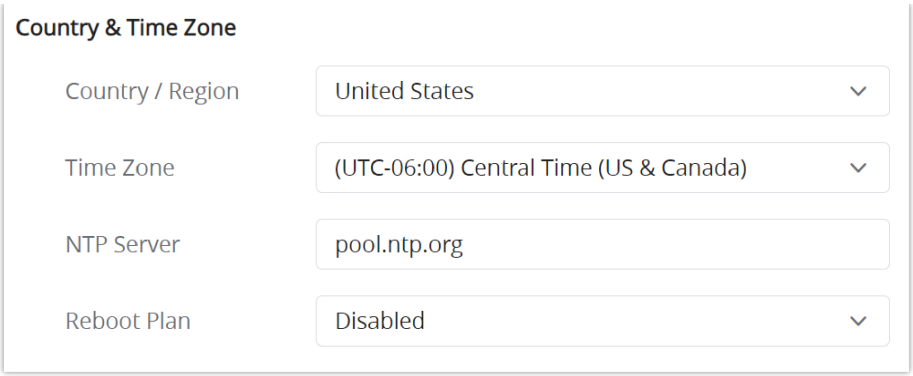

Figure 87: Basic Settings

TR-069

Important Note:

If enabled, GWN70xx router cannot be managed by GWN.Cloud, and cannot continue to manage GWN76xx access points.

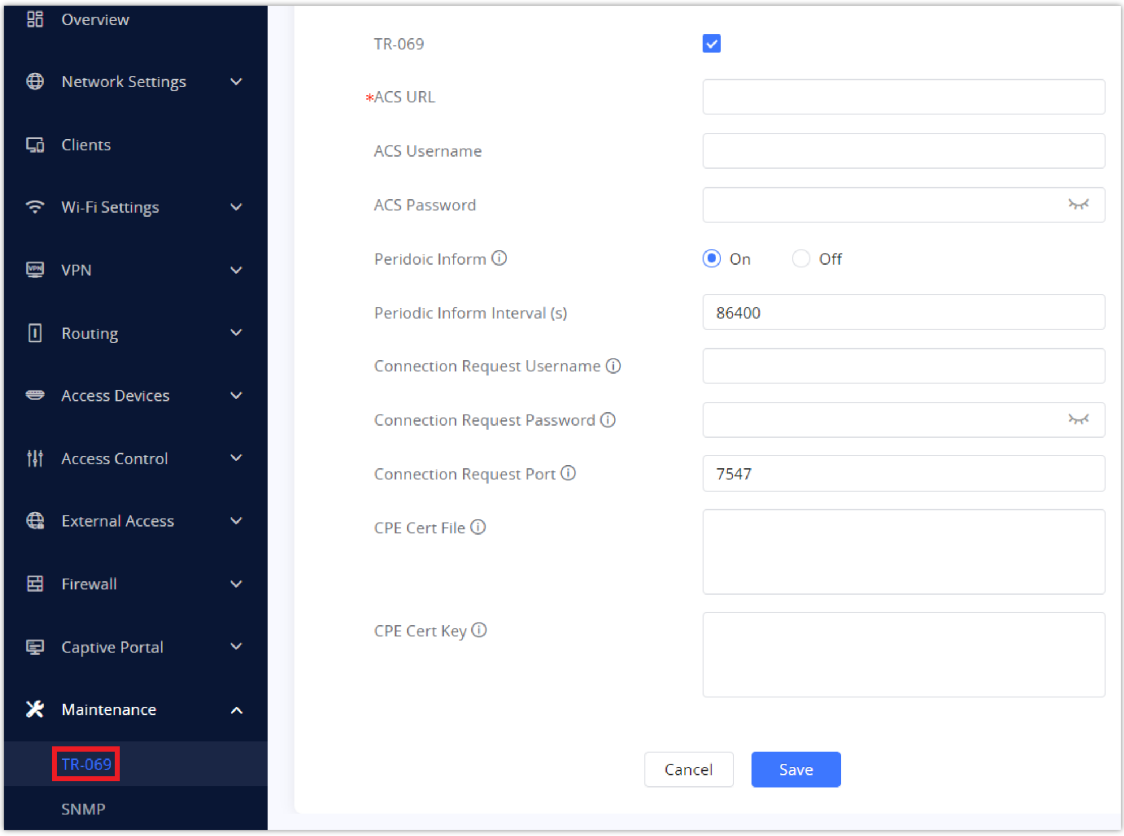

Figure 88: TR-069 page

SNMP

GWN70xx supports SNMP (Simple Network Management Protocol) which is widely used in network management for network monitoring for collecting information about monitored devices.

To configure SNMP settings, go to **GWN70xx Web GUI → Maintenance → SNMP**, in this page the user can either enable SNMPv1, SNMPv2c, or enable SNMPv3, and enter all the necessary parameters.

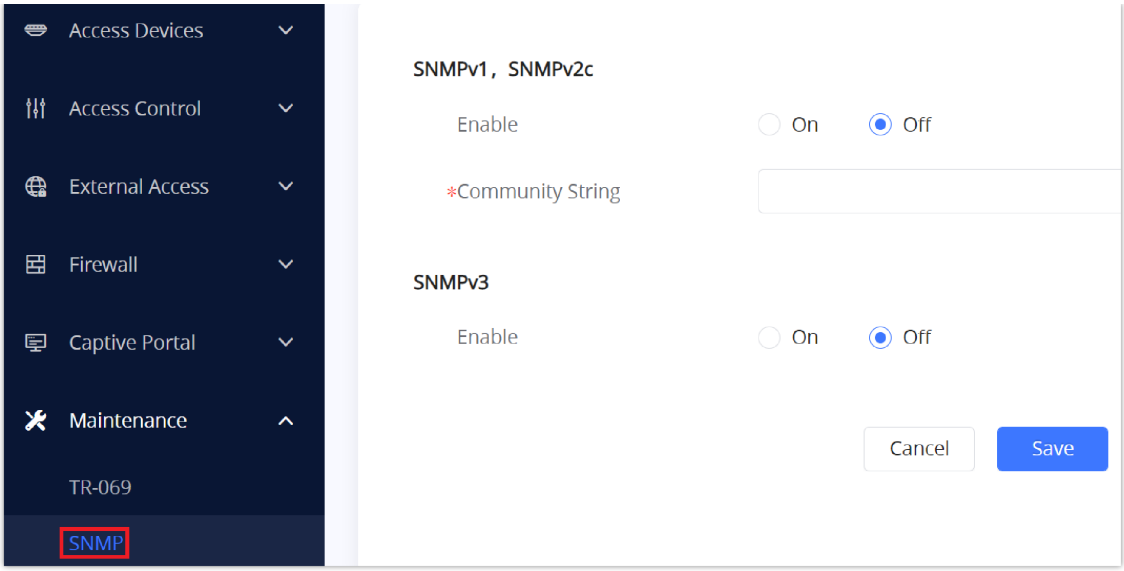

Figure 89: SNMP configuration page

Security Management

Under **"Web UI → System Settings → Security Management"** the user can change the login password and activate the web service for example web WAN port access for HTTPS port 443 as well as enabling SSH remote access.

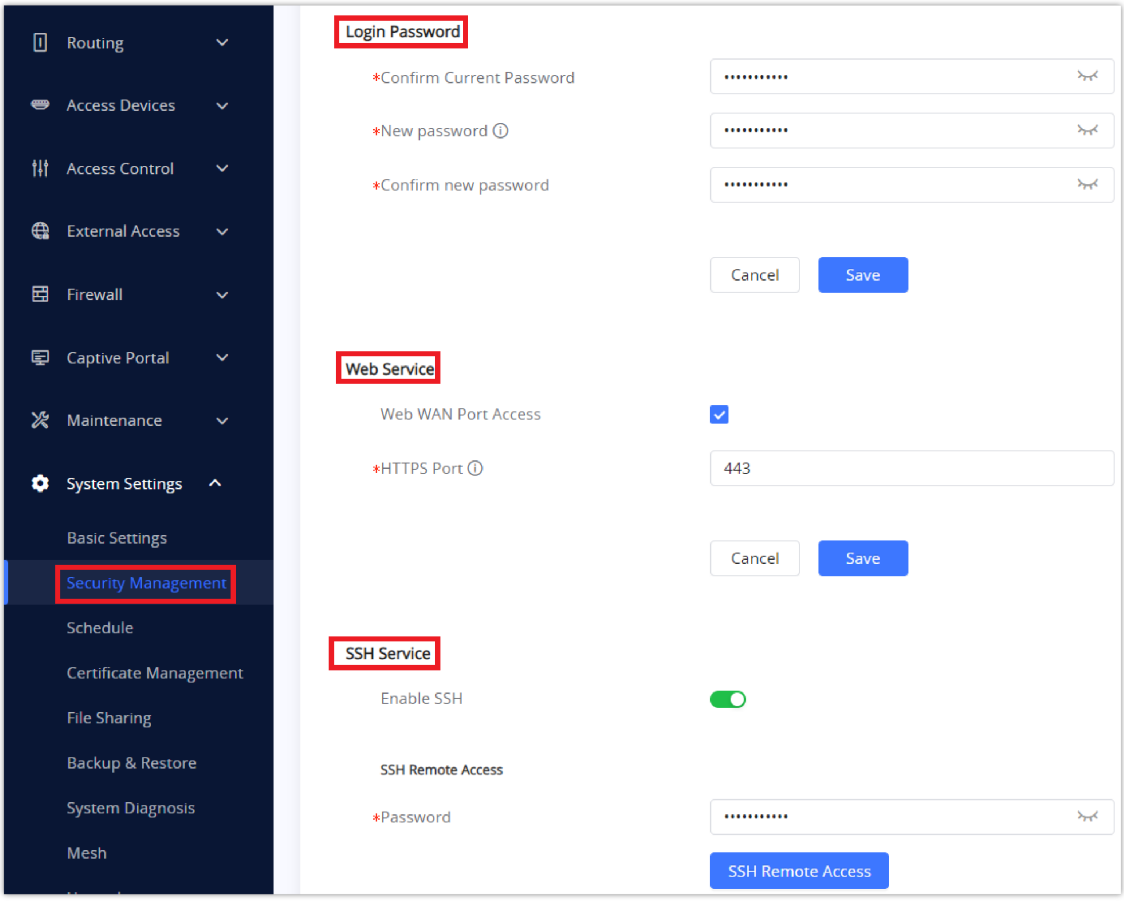

Figure 90: Security Management

Debug

Many debugging tools are available on GWN70xx's Web GUI to check the status and troubleshoot GWN70xx's services and networks.

To access these tools navigate to **"Web UI → System Settings → System Diagnosis"**

Ping/Traceroute

Ping and Traceroute are useful debugging tools to verify reachability with other clients across the network (WAN or LAN). The GWN70xx offers both Ping and Traceroute tools for IPv4 and IPv6 protocols.

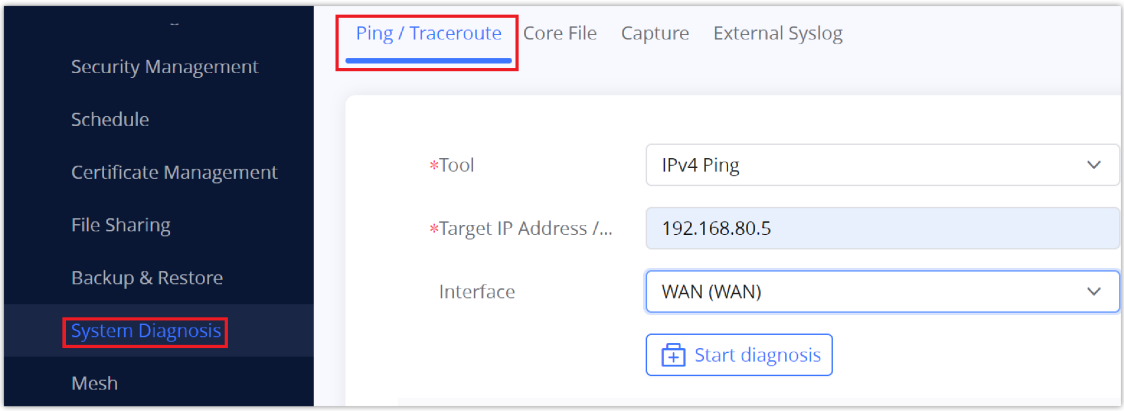

Figure 91: Ping/Traceroute

Core File

when a crash event happens on the unit, it will automatically generate a core dump file that can be used by the engineering team for debugging purposes.

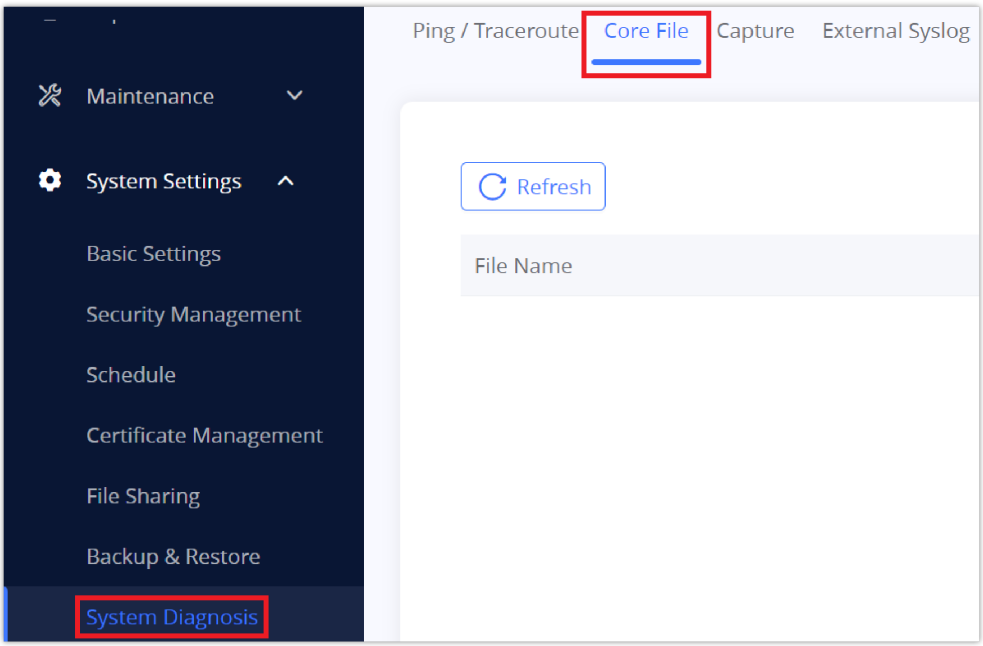

Figure 92: Core File

Capture

This section is used to capture packet traces from the GWN70xx interfaces (WAN ports and network groups) for troubleshooting purposes or monitoring. It's even possible to capture based on MAC address or IP Address, once done the user can click on Start Capturing and the file (CAP) will start downloading right away.

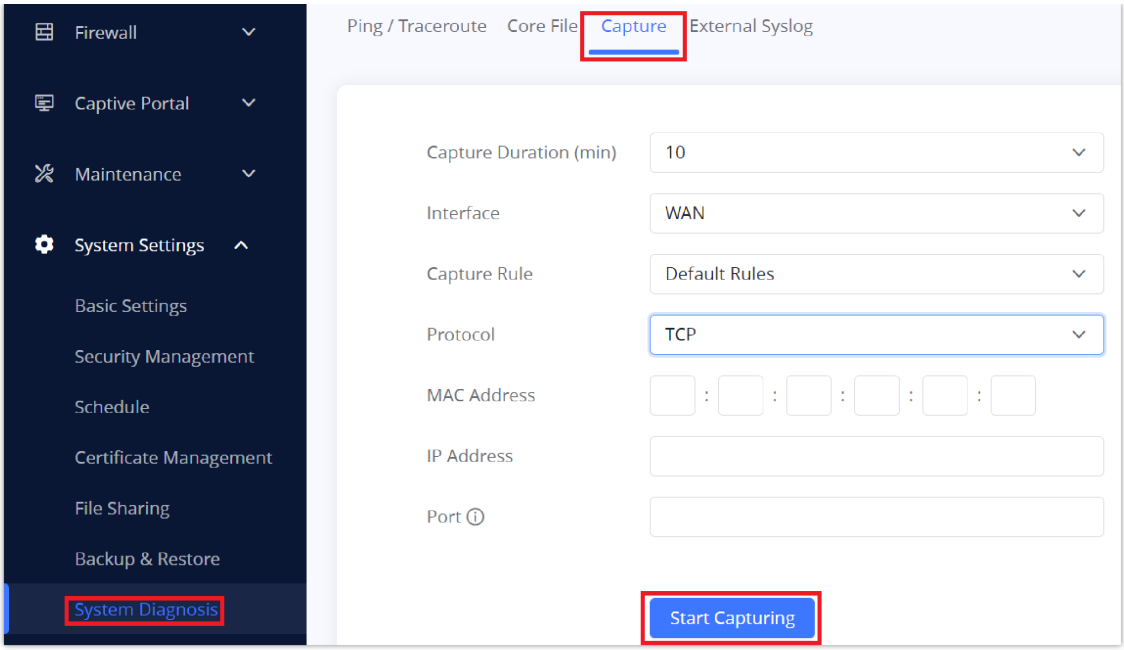

Figure 93: Capture

External Syslog

GWN70xx routers support dumping the Syslog information to a remote server under **Web GUI → System Settings → System Diagnosis → External Syslog Tab**

Enter the Syslog server hostname or IP address and select the level for the Syslog information. Nine levels of Syslog are available: None, Emergency, Alert, Critical, Error, Warning, Notice, Information and Debug.

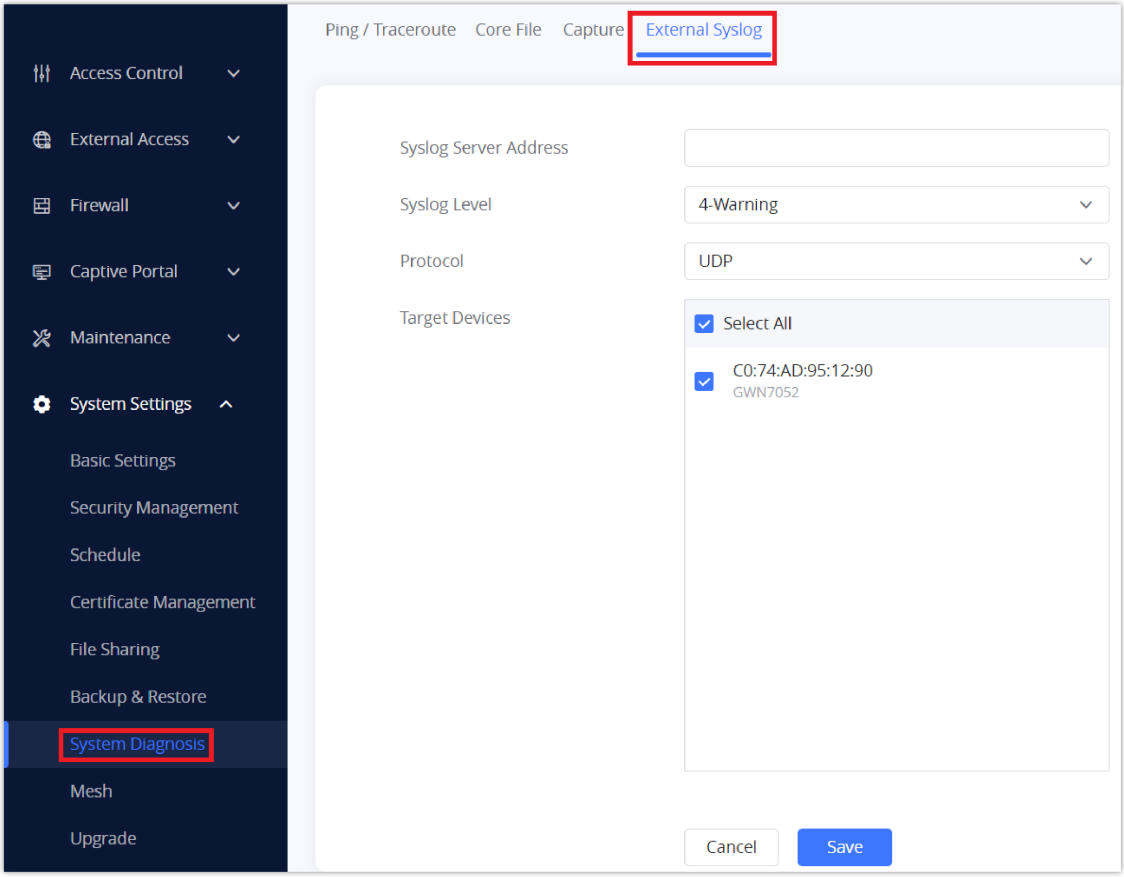

Figure 94: External Syslog

Email/Notification

The E-mail Notification page allows the administrator to select a predefined set of system events and to send notifications upon the change of the set events,

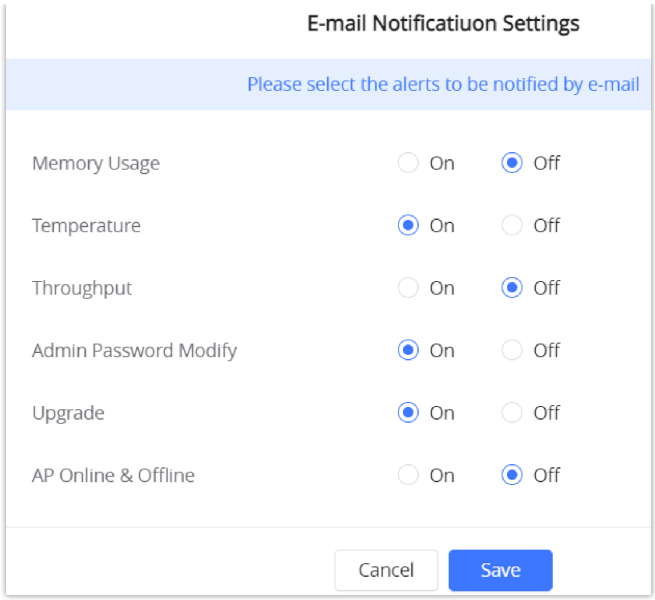

Figure 95: E-mail Notification Events

Schedule

Users can use the schedule configuration menu to set specific schedules for GWN features while giving the flexibility to specify the date and time to turn ON/OFF the selected feature.

The Schedule can be used for settings up a specific time for Wi-Fi where the service will be active or for LED schedule...etc.

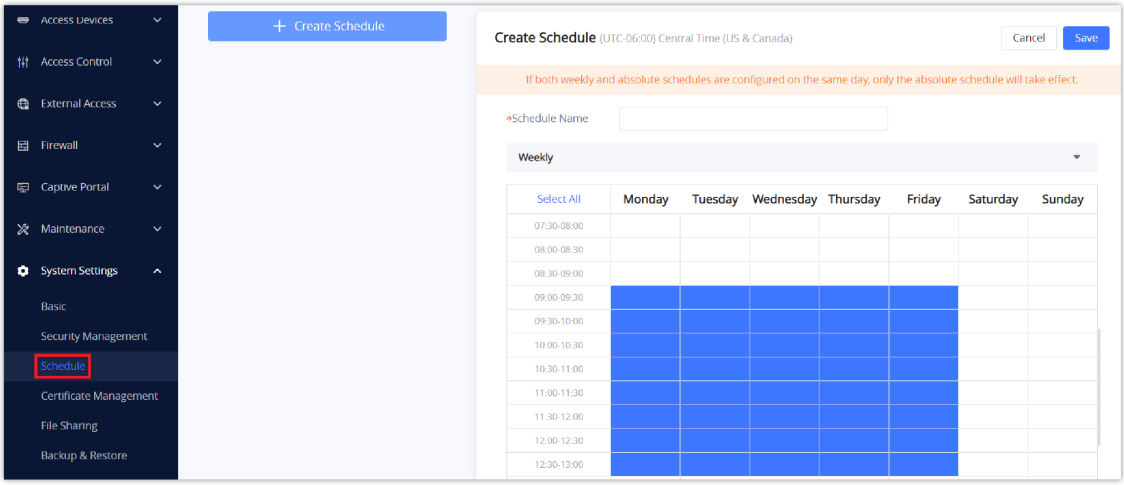

Figure 96: Schedule

To configure a new schedule, follow the below steps:

1. Go under "**Schedule**" and click on **Create New Schedule**

2. Select the periods on each day that will be included on the schedule and enter a name for the schedule (ex: office hours).

3. Users can choose to set a weekly schedule or absolute schedule (for specific days for example), and if both weekly schedule and absolute schedules are configured on the same day then the absolute schedule will take effect and the weekly program will be canceled for that specific date.

4. Once the schedule periods are selected, click on Save to save the schedule.

5. The list of created schedules will be displayed as shown in the figure below. With the possibility to edit or delete each schedule:

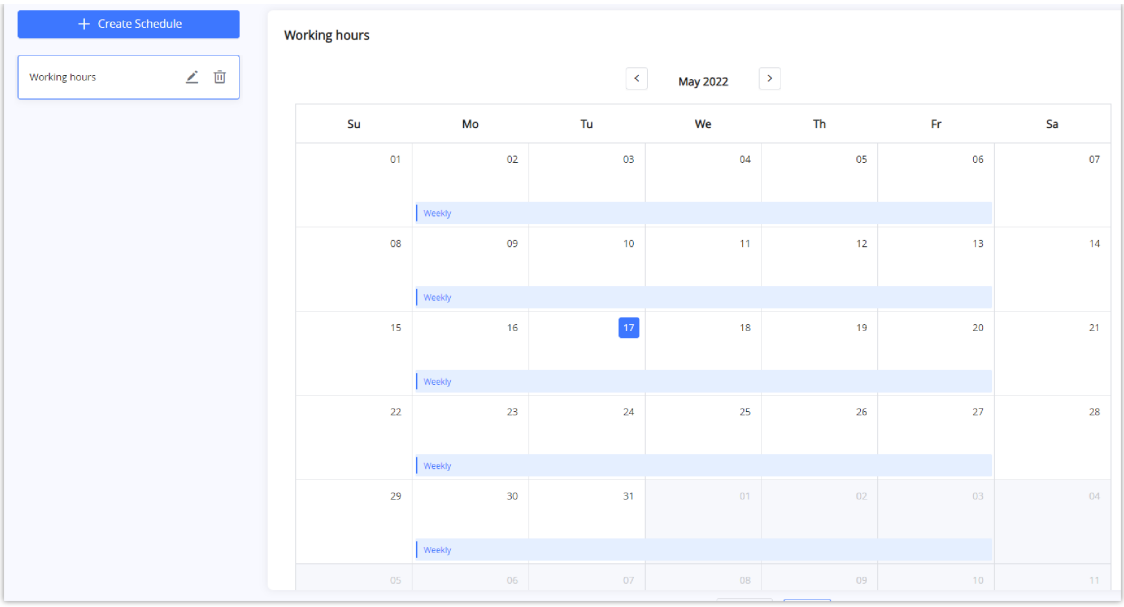

Figure 97: Created Schedule

LED

GWN70xx routers support also the LED schedule feature. This feature is used to set the timing when the LEDs are ON and when they will go OFF at the customer's convenience.

This can be useful for example when the LEDs become disturbing during some periods of the day, this way with the LED scheduler, you can set the timing so that the LEDs are off at night after specific hours and maintain the Wi-Fi service for other clients without shutting down the AP.

To configure the LED schedule, on the GWN70xx Web GUI navigate to "**System Settings → Basic Settings".**

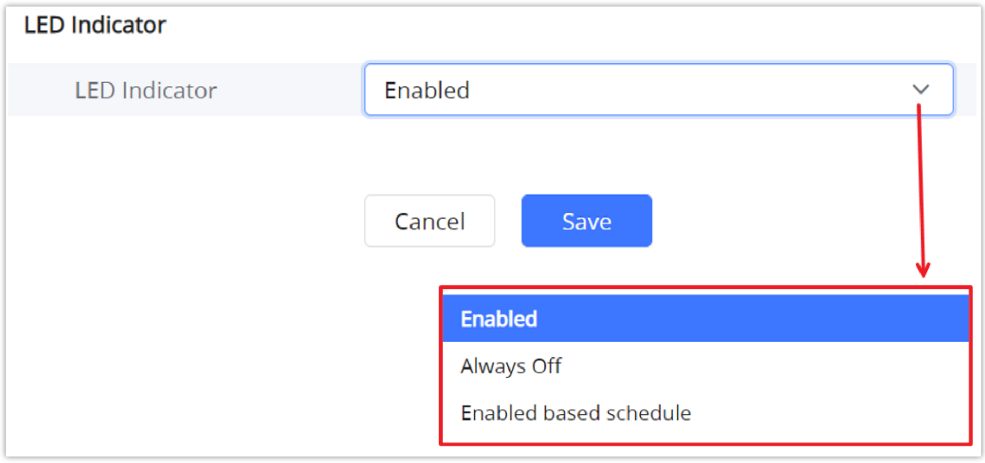

Figure 98: LED Indicator

File Sharing

The GWN70xx has a USB port that can be also used for file sharing, to enable file sharing on devices plugged into the USB port, go to **System Settings → File Sharing.**

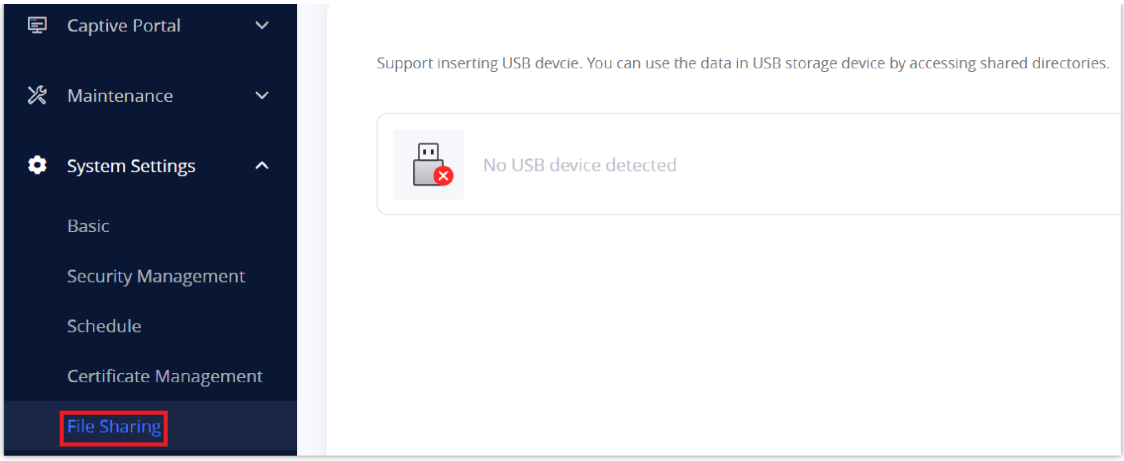

Figure 99: File Sharing

UPGRADING AND PROVISIONING

Upgrading Firmware

Under **System Settings** → **Upgrade.** The administrator has the option to upgrade the GWN70xx via manual upload (a bin file) or via network either HTTP/HTTPS or TFTP or even schedule to upgrade in a specific time.

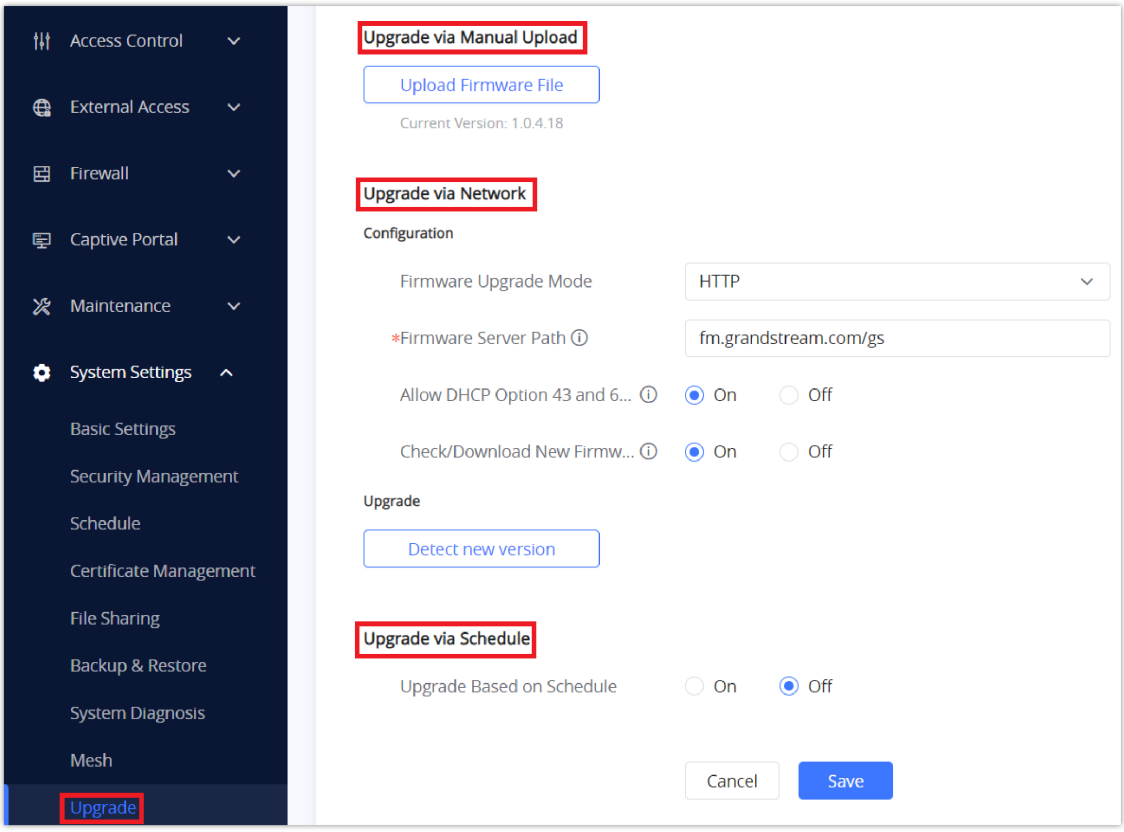

Figure 100: Upgrade page

Backup and Restore

The GWN70xx configuration can be backed up to use later or restore the GWN70xx configuration from a previous backup.

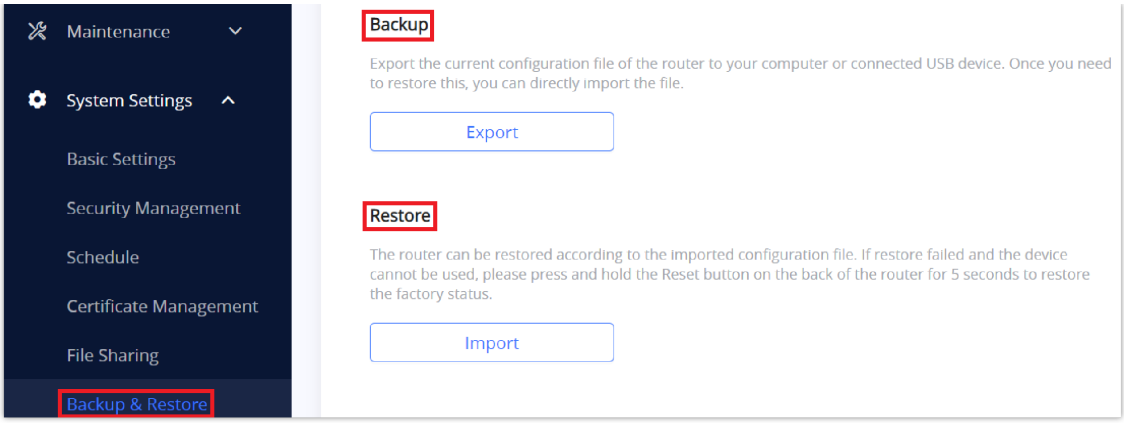

Figure 101: Backup and Restore

Reset and Reboot

Reboot

Users could perform a reboot by clicking on Reboot at the top of the Web UI, and a confirmation message will pop up.

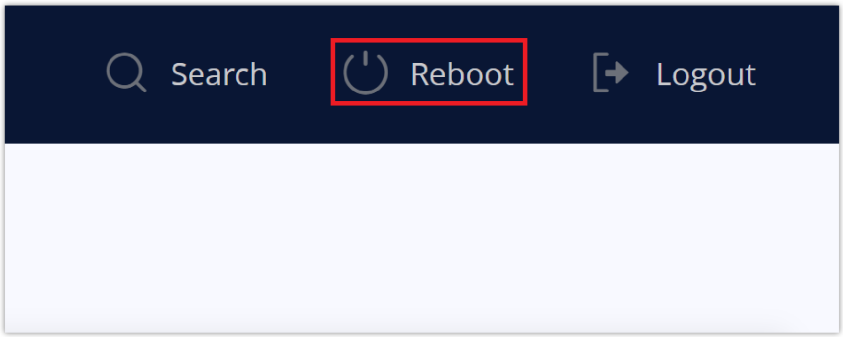

Figure 102: Reboot

Reset

To reset the GWN70xx router to default settings, navigate to **"System Settings → Backup & Restore"** and click on Factory Reset . Another way, press the reset pinhole for 5 seconds on the back of the device.

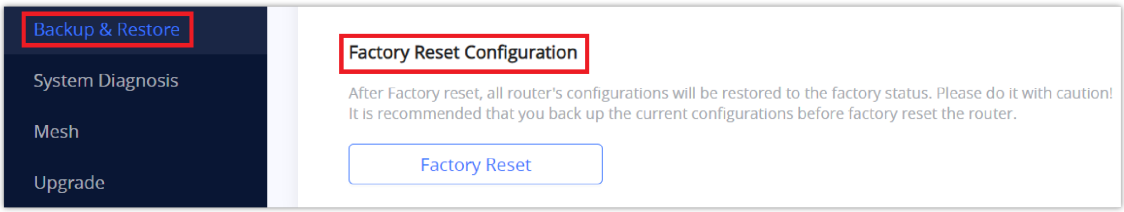

Figure 103: Factory Reset

CHANGELOG

This section documents significant changes from previous versions of the GWN70xx routers user manuals. Only major new features or major document updates are listed here. Minor updates for corrections or editing are not documented here.

Firmware Version 1.0.5.3

Product Name: GWN7052 / GWN7052F / GWN7062

○ This is the initial version.