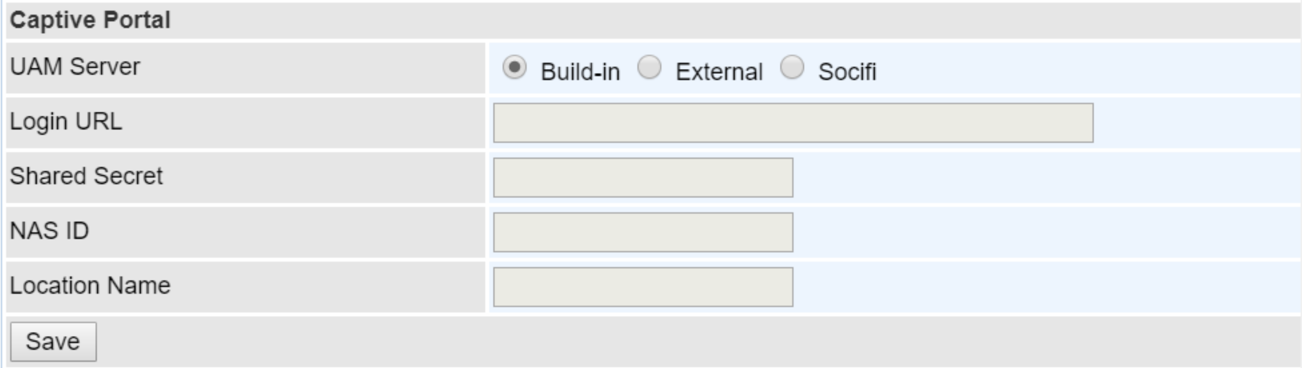
Maximum Total Data Usage (in MBytes): Pre-configure total data usage allowed for each session. value range from 0 ~ 5120MB; **0** means no speed limitation.

Captive Portal



Captive Portal	
UAM Server	● Build-in ○ External ○ Socifi
Login URL	
Shared Secret	
NAS ID	
Location Name	
Save	

UAM Server: Select a server you wish to use, **Build-in**, **External** or **Socifi**. Fill in the blanks to use External UAM server.

UAM Server: Built-in & External

Login URL: Enter the login URL offered by the UAM server.

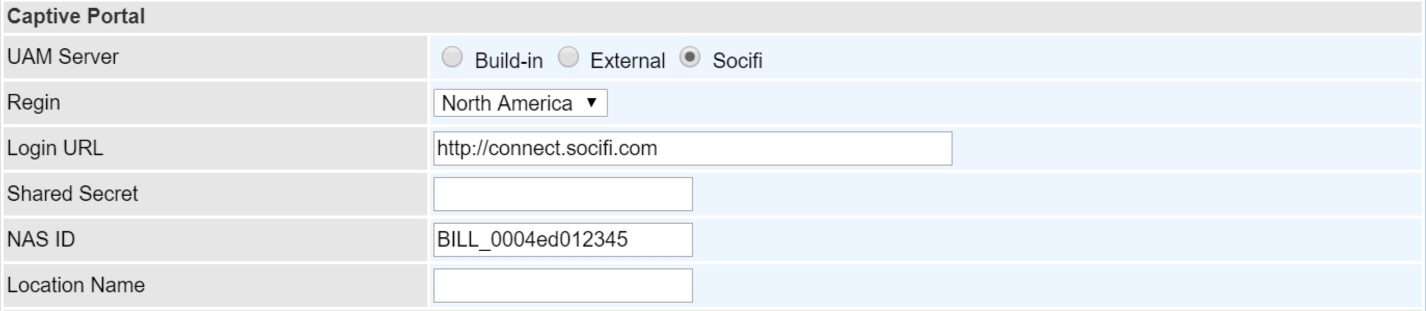
Shared Secret: Set the shared secret password offered.

NAS ID: An assigned string for identification.

Location Name: An assigned string for identification.

UAM Server: Socifi

SOCIFI is a cloud-based technology platform that enables the monetization of 4G/WiFi networks.



Captive Portal	
UAM Server	○ Build-in ○ External ● Socifi
Regin	North America ▼
Login URL	http://connect.socifi.com
Shared Secret	
NAS ID	BILL_0004ed012345
Location Name	

Regin: Select your location.

Login URL: Enter the new login page of Socifi if different.

Shared Secret: Enter the shared secret given from Socifi.

NAS ID: It is the device MAC address. Use this MAC address to create or add a new hotspot in your Socifi dashboard.

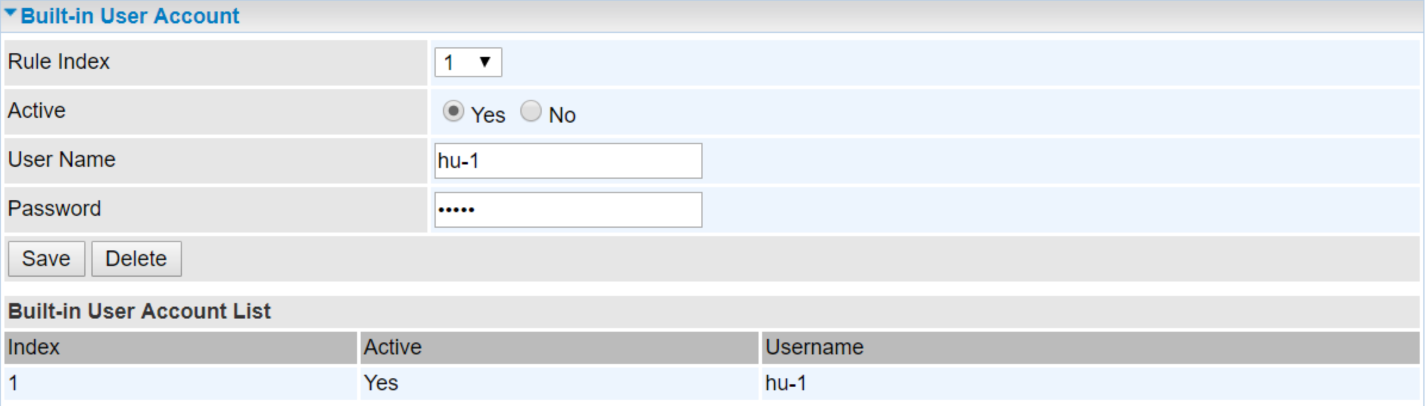
Location Name: It is not used by Socifi. Use it if needed.

Click Save to apply settings.

Built-in User Account

It is a local database on the router with pre-defined user accounts authorized by the BEC 4700A/AZ to grant and provide Wi-Fi hotspot access for Wi-Fi capable devices/users.

16, maximum, accounts are allowed.



▾Built-in User Account

Rule Index	1 ▼
Active	● Yes ○ No
User Name	hu-1
Password	•••••

Built-in User Account List

Index	Active	Username
1	Yes	hu-1

Rule Index: The indication of the rule number. The maximum entry is up to 16.

Active: Select **Yes** to enable the rule of the account.

Username / Password: Create a username and password for this user account.

Save: Click the **Save** button to apply the settings

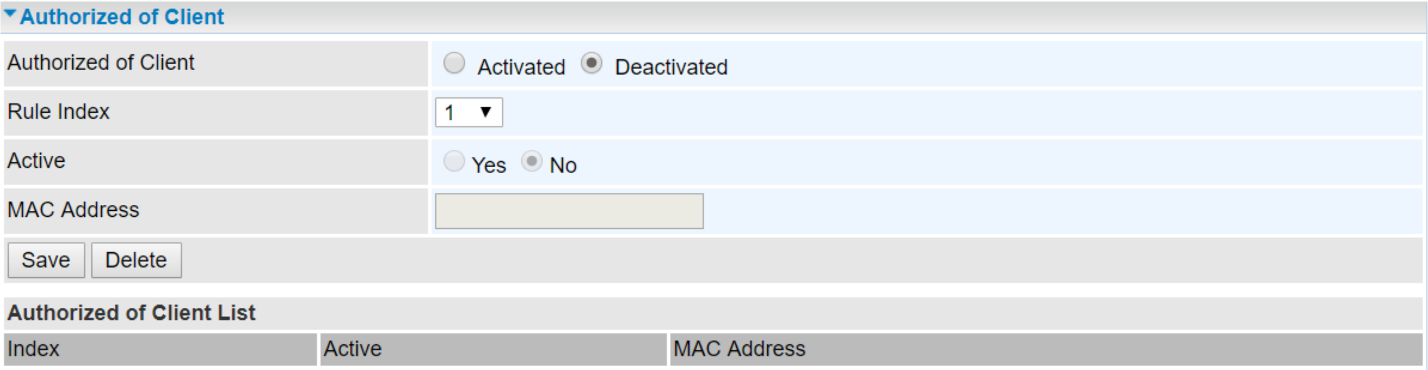
Delete: Use the **Rule Index** to select an unwanted rule then click **Delete** button to remove it from the Account list.

Click Save to apply the settings

Authorized of Client

Add and predefine a trusted wireless MAC address of a Wi-Fi capable device for an immediate hotspot/Internet access. Hotspot/Internet access requires no authentication.

16, maximum, accounts are allowed.



▾Authorized of Client

Authorized of Client	○ Activated ● Deactivated
Rule Index	1 ▼
Active	○ Yes ● No
MAC Address	

Save Delete

Authorized of Client List

Index	Active	MAC Address

Authorized of Client: Select **Activated** to enable this feature.

Rule Index: The indication of the rule number. The maximum entry is up to 16.

Active: Select **Yes** to enable the rule of the client.

MAC Address: Enter the wireless MAC address of the Wi-Fi device.

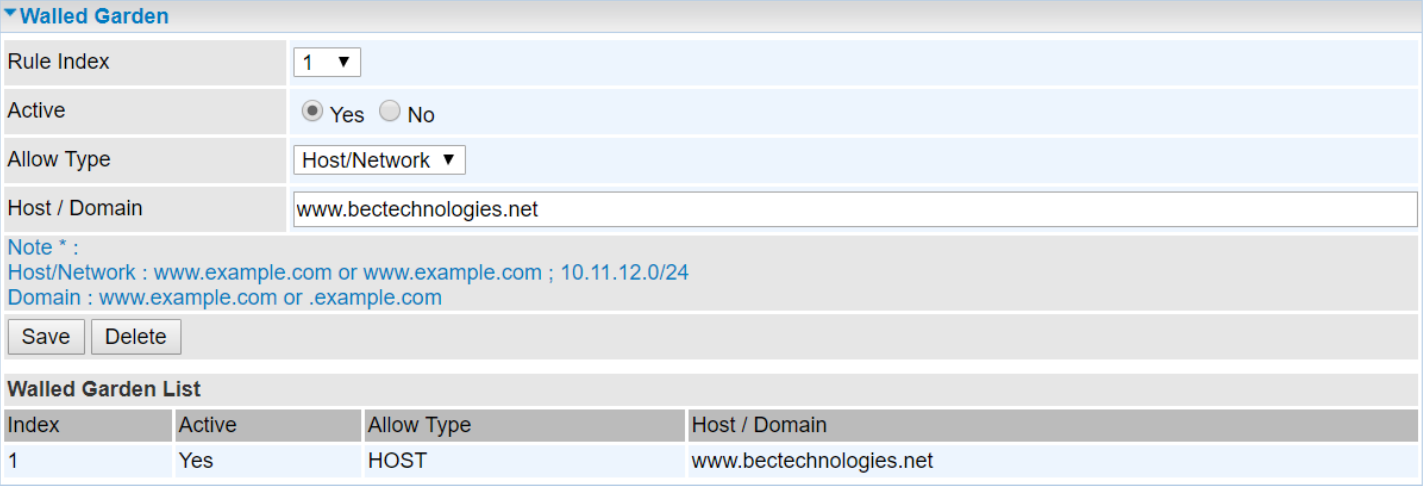
Save: Click the **Save** button to apply settings

Delete: Use the **Rule Index** to select an unwanted rule then click **Delete** button to remove it from the Client list.

Walled Garden

Add and predefine websites (domain names) or web IP address to allow Wi-Fi devices / clients to access to. Web site access requires no authentication.

16, maximum, websites / domains are allowed.



Rule Index	1 ▼
Active	● Yes ○ No
Allow Type	Host/Network ▼
Host / Domain	www.bectechnologies.net

Note * :
Host/Network : www.example.com or www.example.com ; 10.11.12.0/24
Domain : www.example.com or .example.com

Walled Garden List

Index	Active	Allow Type	Host / Domain
1	Yes	HOST	www.bectechnologies.net

Rule Index: The indication of the rule number. The maximum entry is up to 16.

Active: Select **Yes** to enable the rule of the walled garden.

Allow Type: Either a **Host/Network** or **Domain**.

Host / Domain Name: Enter a valid domain, network, or website for unauthorized clients to access to.

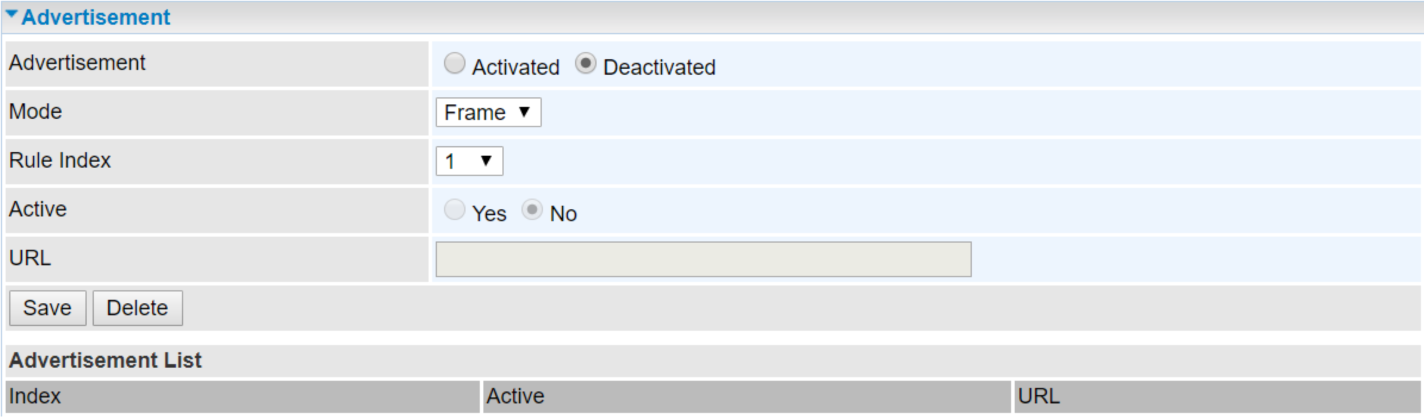
Save: Click the **Save** button to apply the settings

Delete: Use the **Rule Index** to select an unwanted rule then click **Delete** button to remove it from the Walled Garden list.

Advertisement

Add pop-ups ads and redirects to BEC 4700A/AZ Wi-Fi Hotspot, and only a random ad will be displayed per a login.

16, maximum, ads are allowed.



▾Advertisement

Advertisement	○ Activated ● Deactivated
Mode	Frame ▼
Rule Index	1 ▼
Active	○ Yes ● No
URL	

Advertisement List

Index	Active	URL

Advertisement: Select **Activated** to enable this feature.

Mode: Two (2) web advertising methods are available.

- **Frame:** Redirect to a random ad site, a full-page ad, before reaching to the login page. This full-page ad will get redirect to the login page after 5-10 seconds.
- **Popups:** A random pop-up ad display in a separate window after the login page.

Rule Index: The indication of the rule number. The maximum entry is up to 16.

Active: Select **Yes** to enable the rule.

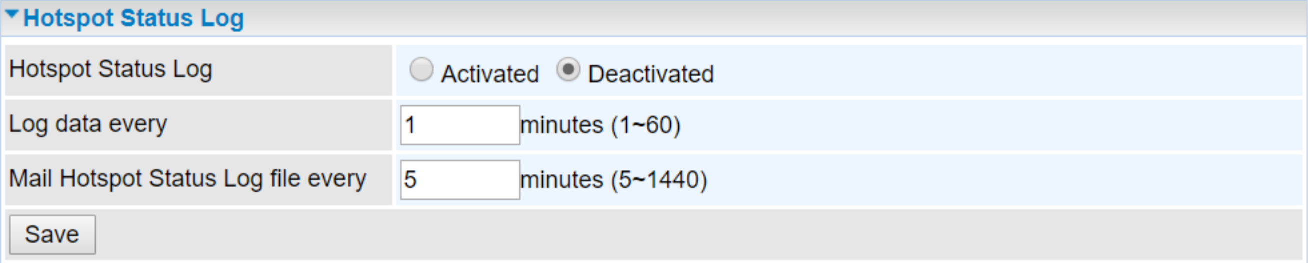
URL: Enter a valid

Save: Click the **Save** button to apply settings

Delete: Use the **Rule Index** to select an unwanted rule then click **Delete** button to remove it from the Walled Garden list.

Hotspot Status Log

Record all hotspot access information and e-mail the statistics report of the hotspot clients in a specific duration.



Hotspot Status Log

Hotspot Status Log	○ Activated ● Deactivated
Log data every	1 minutes (1~60)
Mail Hotspot Status Log file every	5 minutes (5~1440)

Session Log: Select **Activated** to enable this feature.

Log Session Data in every (minute): Input session log time duration, (min)1 to (max) 60 minutes.

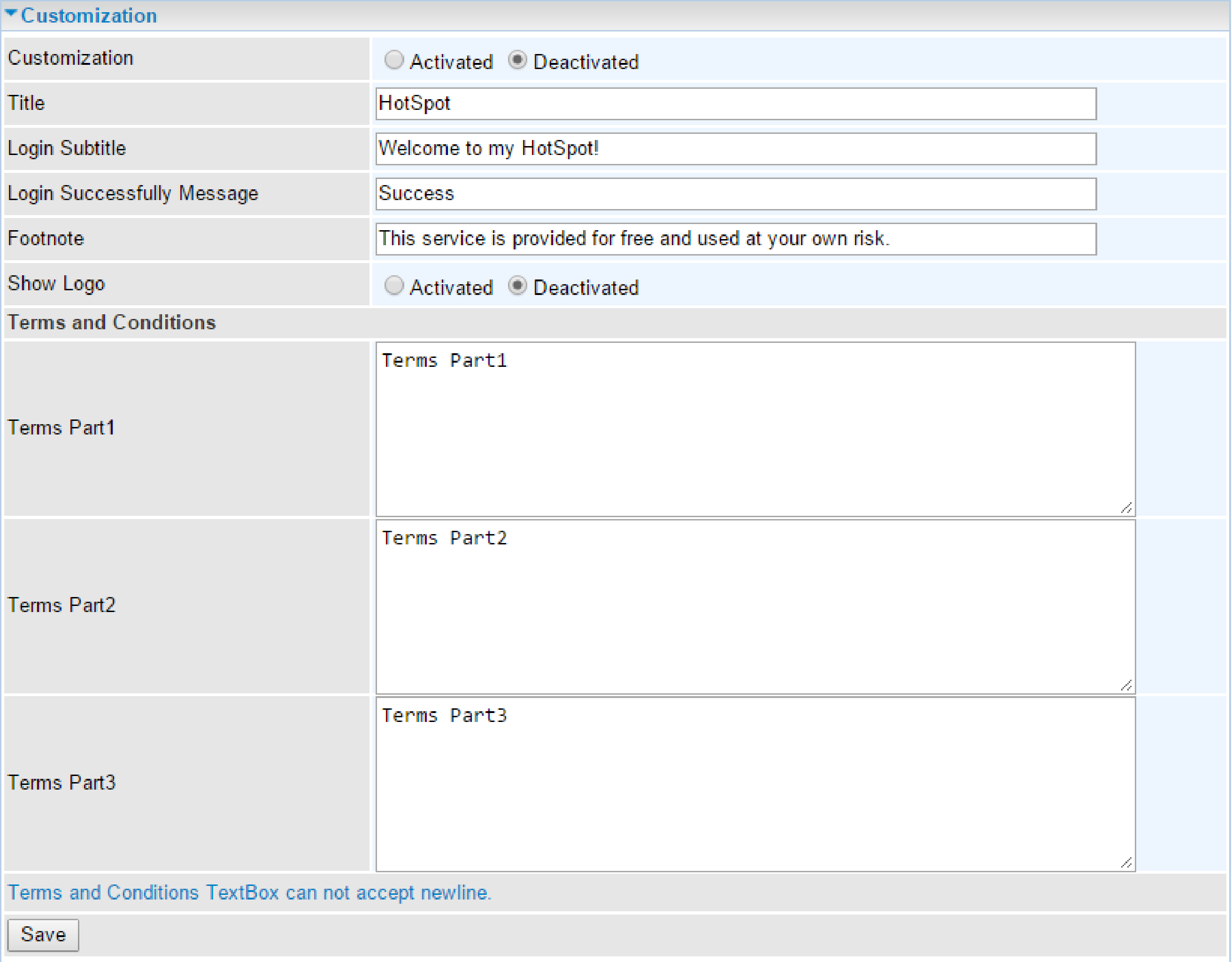
Mail Session Log File in every (minute): BEC 4700A/AZ will send all access information, such as access IP addresses, NAT tables, etc., to the administrator's mailbox in the specific time/minute.

NOTE: Please set up a dedicated or administrator e-mail account to receive Hotspot access information in the **Mail Alert.**

Click **Save** to apply settings.

Customization

Allow modification to some of the captive portal settings.



▾Customization

Customization	○ Activated ● Deactivated
Title	HotSpot
Login Subtitle	Welcome to my HotSpot!
Login Successfully Message	Success
Footnote	This service is provided for free and used at your own risk.
Show Logo	○ Activated ● Deactivated
Terms and Conditions	
Terms Part1	Terms Part1
Terms Part2	Terms Part2
Terms Part3	Terms Part3

Terms and Conditions TextBox can not accept newline.

Save

Customization: Select **Activated** to enable this feature.

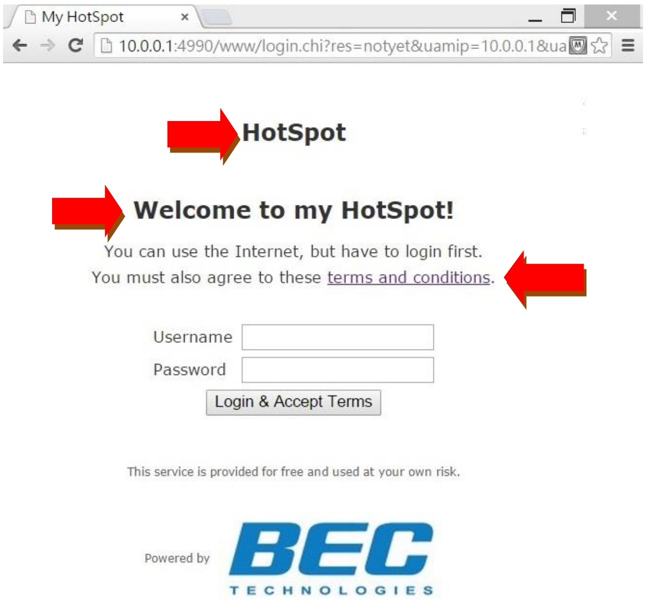
Title: The Banner message. Default is “Hotspot”

Login Subtitle: Default is “Welcome to my Hotspot”

Term Part 1 / 2 / 3: Create your own Terms and Conditions. To use default, same terms, please skip this part.

NOTE: No newline is accepted in each text box.

Login Successfully Message: BEC 4700A/AZ will send all access information, such as access IP addresses, NAT tables, etc., to the administrator’s mailbox in the specific time/minute.



My HotSpot

10.0.0.1:4990/www/login.chi?res=notyet&uamip=10.0.0.1&ua

HotSpot

Welcome to my HotSpot!

You can use the Internet, but have to login first.
You must also agree to these terms and conditions.

Username
Password

Login & Accept Terms

This service is provided for free and used at your own risk.

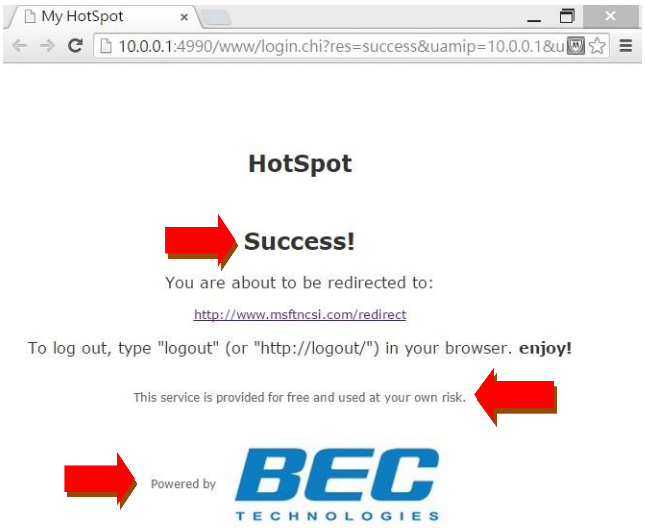
Powered by BEC TECHNOLOGIES

Login Successfully Message: A greeting message after successful login to the Wi-Fi hotspot. Default is “Success!”

Footnote: Additional information, if needed.

Default is “This service is provided for free and used at your own risk.”

Show Logo: Select **Activated** to display company Logo on the portal. (To change logo, please contact with BEC technical support for more information).



HotSpot

Success!

You are about to be redirected to:

http://www.msftncsi.com/redirect

To log out, type "logout" (or "http://logout/") in your browser. **enjoy!**

This service is provided for free and used at your own risk.

Powered by BEC TECHNOLOGIES

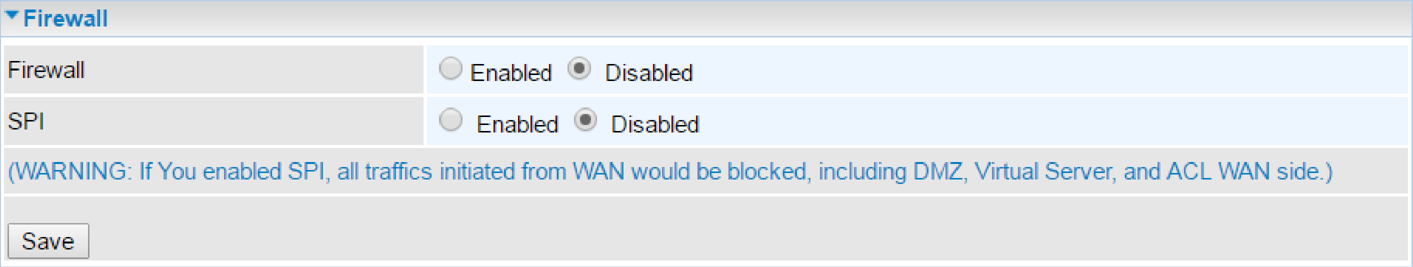
Click **Save** to apply settings.

Advanced Setup

Advanced Setup provides advanced features including Firewall, Routing, Dynamic Routing, NAT, VRRP, Static DNS, QoS, Interface Grouping, Port Isolation, Time Schedule, and Mail Alert for advanced users.

Firewall

Your router includes a firewall for helping to prevent attacks from hackers. In addition to this, when using NAT (Network Address Translation) the router acts as a "natural" Internet firewall, since all PCs on your LAN use private IP addresses that cannot be directly accessed from the Internet.



▾Firewall

Firewall	○ Enabled ● Disabled
SPI	○ Enabled ● Disabled

(WARNING: If You enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.)

Firewall: To automatically detect and block Denial of Service (DoS) attacks, such as Ping of Death, SYN Flood, Port Scan and Land Attack.

- **Enabled:** Activate your firewall function.
- **Disabled:** Deactivate the firewall function.

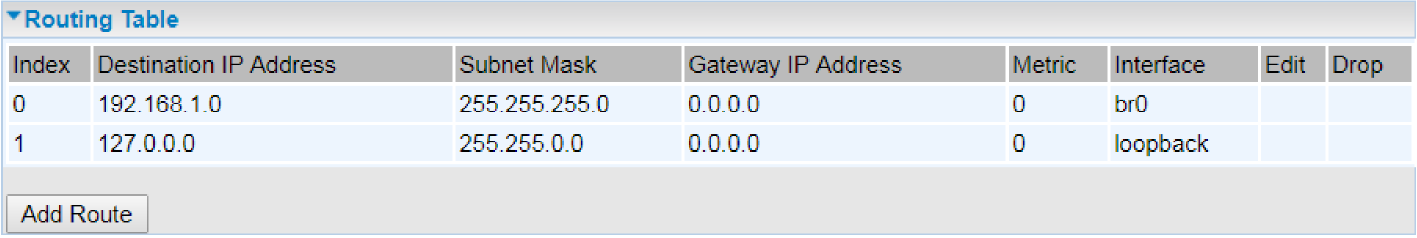
SPI: If you enabled SPI, all traffics initiated from WAN would be blocked, including DMZ, Virtual Server, and ACL WAN side.

- **Enabled:** Activate your SPI function.
- **Disabled:** Deactivate the SPI function.

Click **Save** to apply settings.

Static Routing

This is static route feature. You are equipped with the capability to control the routing of all the traffic across your network. With each routing rule created, user can specifically assign the destination where the traffic will be routed to.



▾Routing Table

Index	Destination IP Address	Subnet Mask	Gateway IP Address	Metric	Interface	Edit	Drop
0	192.168.1.0	255.255.255.0	0.0.0.0	0	br0		
1	127.0.0.0	255.255.0.0	0.0.0.0	0	loopback		

Index #: The indication of the routing table number.

Destination IP Address: IP address of the destination network

Subnet Mask: The subnet mask of destination network.

Gateway IP Address: IP address of the gateway or existing interface that this route uses.

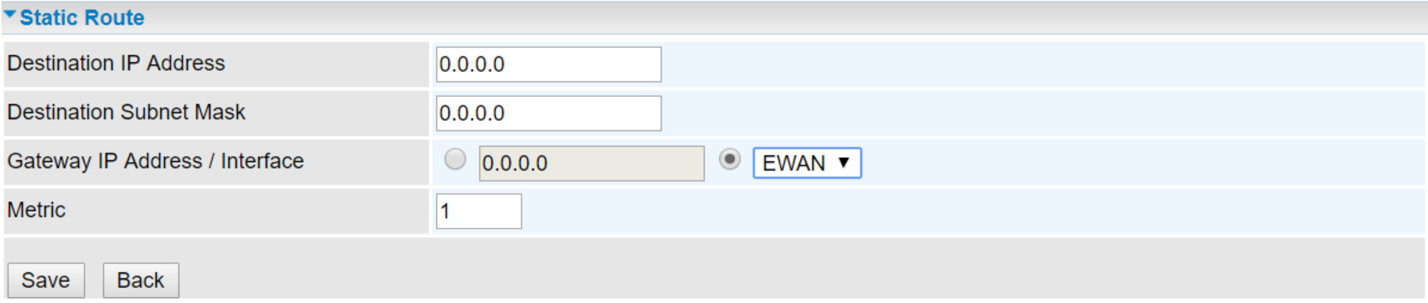
Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Interface: Media/channel selected to append the route.

Edit: Edit the route; this icon is not shown for system default route.

Drop: Drop the route; this icon is not shown for system default route.

Add Route



▾Static Route

Destination IP Address	0.0.0.0
Destination Subnet Mask	0.0.0.0
Gateway IP Address / Interface	○ 0.0.0.0 ● EWAN ▾
Metric	1

Destination IP Address: This is the destination subnet IP address.

Destination Subnet Mask: The subnet mask of destination network.

Gateway IP Address or Interface: This is the gateway IP address or existing interface to which packets are to be forwarded.

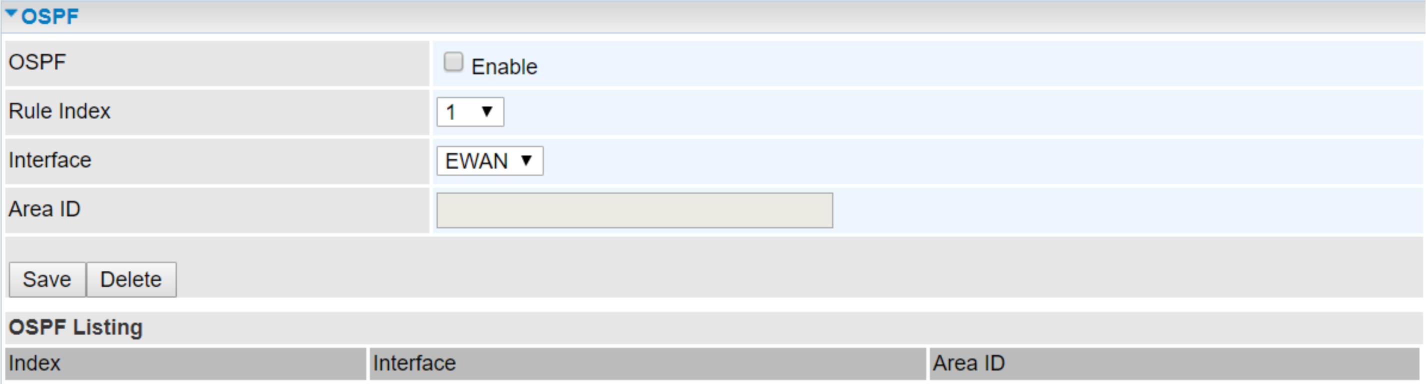
Metric: It represents the cost of transmission for routing purposes. The number need not be precise, but it must be between 1 and 15.

Click **Save** to add this route.

Dynamic Routing

The NAT (Network Address Translation) feature transforms a private IP into a public IP, allowing multiple users to access the internet through a single IP account, sharing the single IP address. NAT break the originally envisioned model of IP end-to-end connectivity across the internet so NAT can cause problems where IPSec/ PPTP encryption is applied or some application layer protocols such as SIP phones are located behind a NAT. And NAT makes it difficult for systems behind a NAT to accept incoming communications.

❖ Open Shortest Path First (OSPF)



▾OSPF

OSPF	□ Enable
Rule Index	1 ▼
Interface	EWAN ▼
Area ID	

OSPF Listing

Index	Interface	Area ID

OSPF: Enable to activate OSPF routing.

Rule Index: The indication of the rule number. The maximum entry is up to 10, ranging from 0 to 9.

Interface: Set the interface which runs the OSPF process (involved in OSPF routing). It can be WAN interfaces or established GRE tunnels.

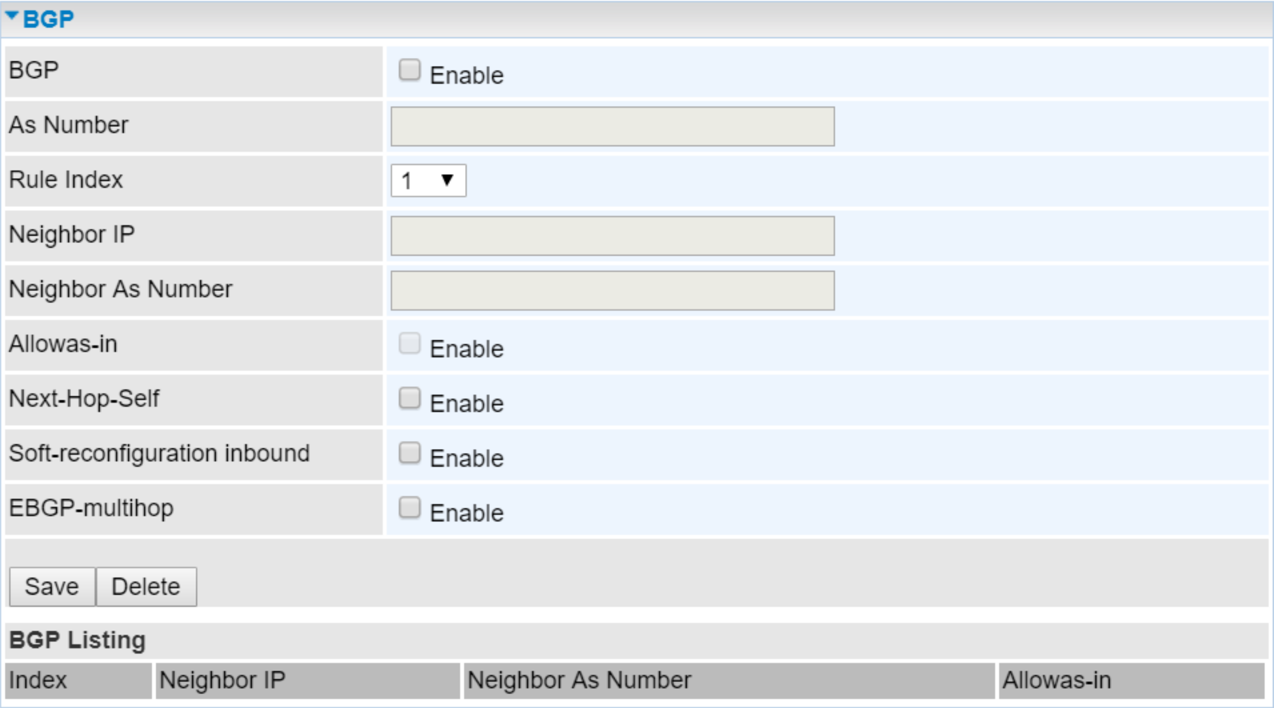
Area ID: The OSPF area identifier. It is a decimal number in the range of 0-4294967295. Enter the area ID in which the interface belongs to. The area with area-id=”0” is the backbone area.

If the router has networks in more than one area, then an area with area-id=”0” (the backbone) must always be present. All other areas are connected to it. The backbone is responsible for distributing routing information between non-backbone areas. The backbone must be contiguous, i.e. there must be no disconnected segments. However, area border routers do not need to be physically connected to the backbone - connection to it may be simulated using a virtual link.

Click **Save** to apply settings.

❖ Border Gateway Protocol (BGP)

A standardized exterior gateway protocol (an uniquely TCP based inter-Autonomous System routing protocol) designed to allow setting up an inter-domain dynamic routing system that automatically updates routing tables of devices running BGP in case of network topology changes.



▾BGP

BGP	□ Enable
As Number	
Rule Index	1 ▼
Neighbor IP	
Neighbor As Number	
Allowas-in	□ Enable
Next-Hop-Self	□ Enable
Soft-reconfiguration inbound	□ Enable
EBGP-multihop	□ Enable

Save Delete

BGP Listing

Index	Neighbor IP	Neighbor As Number	Allowas-in

BGP: Enable to activate BGP routing.

AS Number: Designate the AS number of the local router. The AS number is used to identify the IBGP or EBGP your neighbor is running. The same AS number means the IBGP, and the different means EBGP.

Rule Index: The indication of the rule number. The maximum entry is up to 10, ranging from 0 to 9.

Neighbor IP: Enter the neighbor IP address.

Neighbor AS Number: Enter the neighbor AS number.

Allowas-in: Enable to allow inter-communication between devices in the same AS. If the local and neighbor AS number are the same, thus, an inter-AS communication, please enable the allowas-in. Otherwise, the router only support EBGP routing between different domains.

Next-Hop-Self: Enable to use the router's own loopback address as the next-hop address.

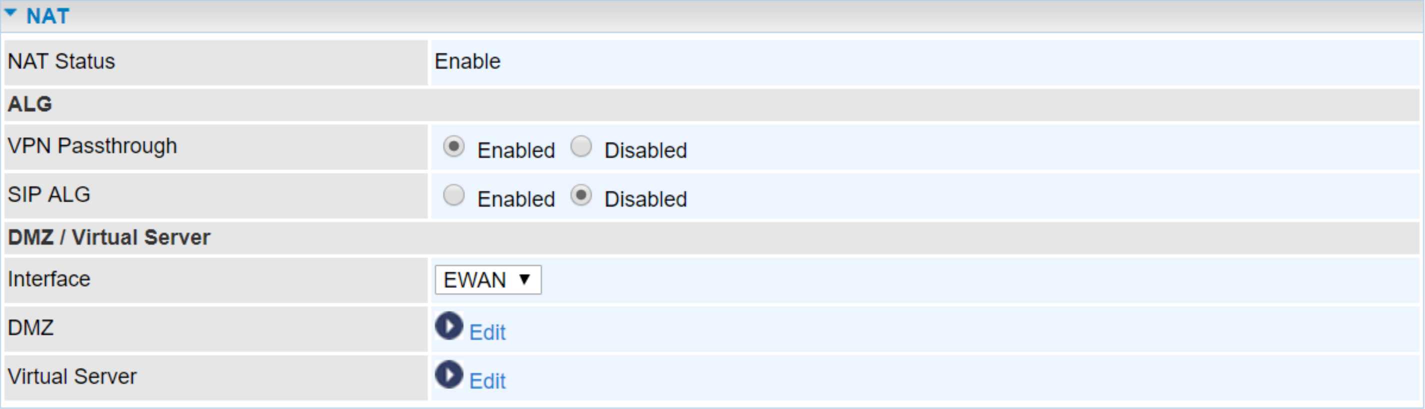
Soft-reconfiguration inbound: Enable to save, pre-stored, a new inbound policy to the BGP table without interrupting the network when applying this new policy.

EBGP (External BGP)-multihop: Enable to build up peer connection/information with external neighbors.

Click **Save** to apply settings.

NAT

The NAT (Network Address Translation) feature transforms a private IP into a public IP, allowing multiple users to access the internet through a single IP account, sharing the single IP address. NAT break the originally envisioned model of IP end-to-end connectivity across the internet so NAT can cause problems where IPSec/ PPTP encryption is applied or some application layer protocols such as SIP phones are located behind a NAT. And NAT makes it difficult for systems behind a NAT to accept incoming communications.



▾ NAT

NAT Status	Enable
ALG	
VPN Passthrough	● Enabled ○ Disabled
SIP ALG	○ Enabled ● Disabled
DMZ / Virtual Server	
Interface	EWAN ▾
DMZ	▶ Edit
Virtual Server	▶ Edit

NAT Status: Enabled. (Disabled if WAN connection is in **BRIDGE** mode)

VPN Passthrough: VPN pass-through is a feature of routers which allows VPN client on a private network to establish outbound VPNs unhindered.

SIP ALG: Enable the SIP ALG when SIP phone needs ALG to pass through the NAT. Disable the SIP ALG when SIP phone includes NAT-Traversal algorithm.

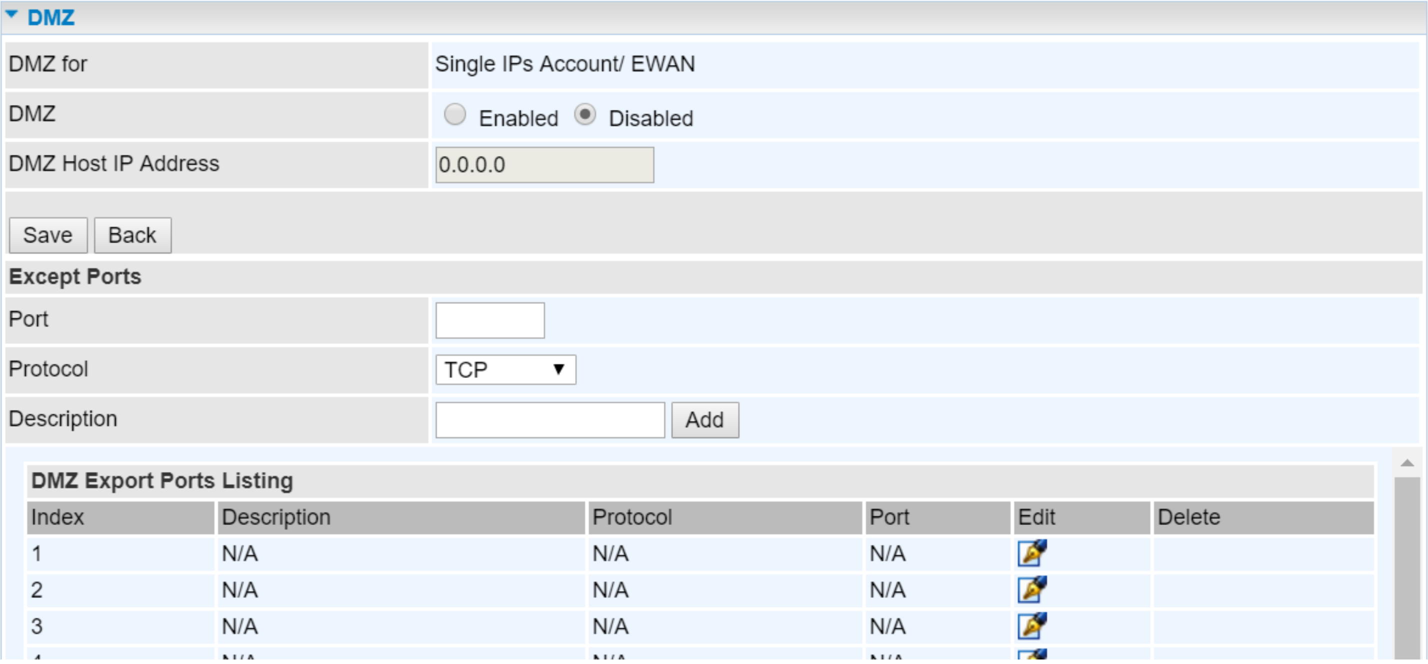
Interface: Select a WAN interface connection to allow external access to your internal network.

Click **DMZ** ▶ Edit or **Virtual Server** ▶ Edit to move on to set the DMZ or Virtual Server parameters, which are represented in the following scenario.

DMZ

NOTE: This feature disables automatically if WAN connection is in BRIDGE mode or NAT is being turned OFF.

The DMZ Host is a local computer which has all UDP and TCP ports exposed to the Internet. When setting an internal IP address as the DMZ Host, all incoming packets will be forwarded to this local host device. Packet filter or virtual server entries will take priority over forwarding internet packets to the DMZ host.



DMZ for	Single IPs Account/ EWAN
DMZ	○ Enabled ● Disabled
DMZ Host IP Address	0.0.0.0

Except Ports

Port	
Protocol	TCP ▼
Description	

DMZ Export Ports Listing

Index	Description	Protocol	Port	Edit	Delete
1	N/A	N/A	N/A	✎	
2	N/A	N/A	N/A	✎	
3	N/A	N/A	N/A	✎	

DMZ for (via a WAN Interface): Allows outside network to connect in and communicate with internal LAN devices via a specific WAN interface.

DMZ:

- **Enabled:** Activate the DMZ function.
- **Disabled:** Deactivate the DMZ function.

DMZ Host IP Address: Give a static IP address to the DMZ Host when **Enabled** radio button is checked. Be aware that this IP will be exposed to the WAN/Internet.

Click **Save** to apply settings.

Except Ports

Except Ports: Bypass UDP or/and TCP ports, in the list, being forwarded to the DMZ host.

Port: Enter port to be monitored.

Protocol: Enter the protocol to be monitored.

Description: Enter a description to this rule.

Example: Skip port 80 (UDP/TCP) in the list. All Incoming request to access to port 80 (Web GUI) will be forwarded to the embedded HTTP server of BEC 4700A/AZ instead of the DMZ host.

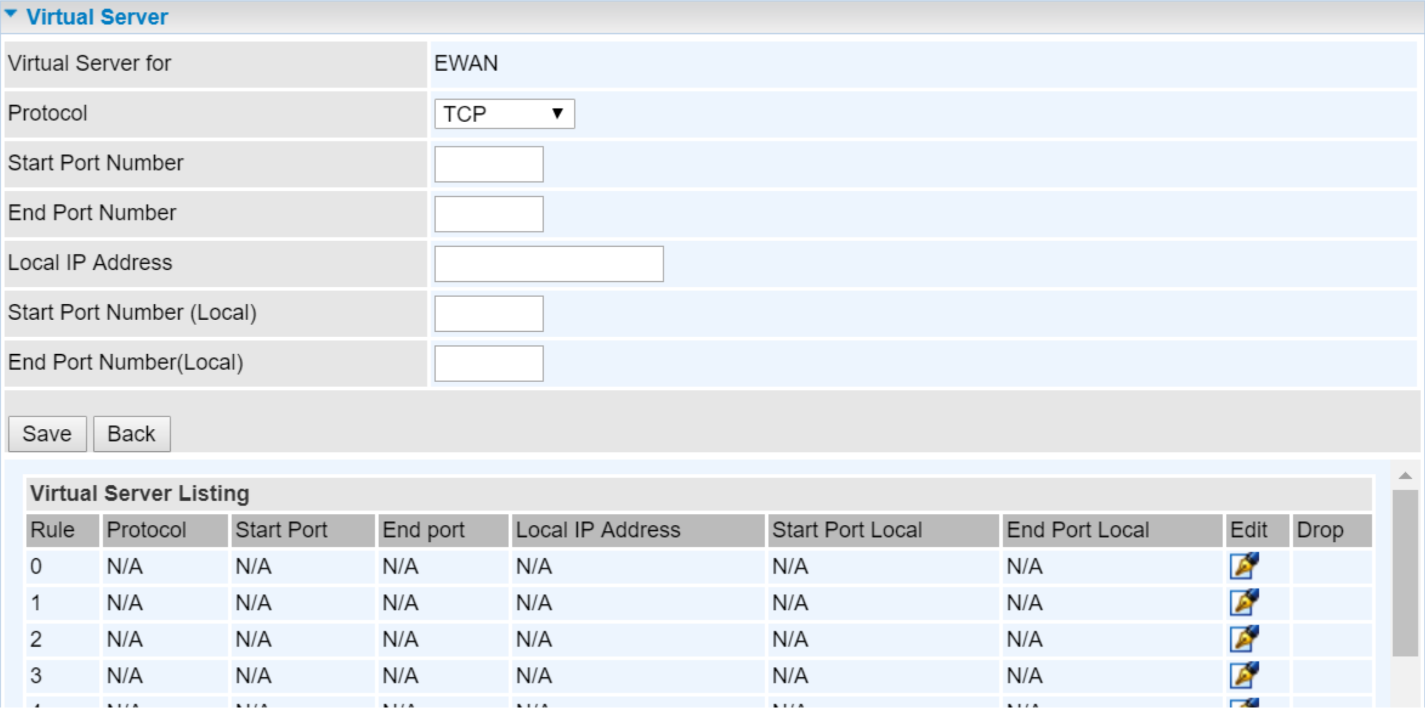
Click **Add** to add an entry to the Except Listing.

Virtual Server

NOTE: This feature disables automatically if WAN connection is in BRIDGE mode or NAT is being turned OFF.

Virtual Server is also known as Port Forwarding that allows BEC 4700A/AZ to direct all incoming traffic to the servers on the LAN.

Configure a virtual rule in BEC 4700A/AZ for remote users accessing services such as Web or FTP services via the public (WAN) IP address that can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.



▼ Virtual Server

Virtual Server for	EWAN
Protocol	TCP ▼
Start Port Number	
End Port Number	
Local IP Address	
Start Port Number (Local)	
End Port Number(Local)	

Virtual Server Listing

Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	N/A	N/A	N/A	N/A	N/A	N/A	✎	
1	N/A	N/A	N/A	N/A	N/A	N/A	✎	
2	N/A	N/A	N/A	N/A	N/A	N/A	✎	
3	N/A	N/A	N/A	N/A	N/A	N/A	✎	

Virtual Server for: Indicate the related WAN interface to allow outside network to communicate with the internal LAN device.

Protocol: Choose the application protocol.

Start / End Port Number: Enter a port or port range you want to forward.

(Example: Start / End: 1000 or Start: 1000 & End: 2000).

The starting port must be greater than zero (0). The end port must be greater than or equal to the start port.

Local IP Address: Enter the server IP address in the network to receive the traffic/packets.

Start / End Port Number (Local): Enter the start / end port number of the local application (service).

Click **Save** to apply settings.

Examples of well-known and registered port numbers are shown below. For further information, please see IANA’s website at http://www.iana.org/assignments/port-numbers

Well-known and Registered Ports

Port Number	Protocol	Description
21	TCP	FTP Control
22	TCP & UDP	SSH Remote Login Protocol
23	TCP	Telnet
25	TCP	SMTP (Simple Mail Transfer Protocol)
53	TCP & UDP	DNS (Domain Name Server)
69	UDP	TFTP (Trivial File Transfer Protocol)
80	TCP	World Wide Web HTTP
110	TCP	POP3 (Post Office Protocol Version 3)
443	TCP & UDP	HTTPS
1503	TCP	T.120
1720	TCP	H.323
7070	UDP	RealAudio

Attention

Using port forwarding does have security implications, as outside users will be able to connect to PCs on your network. For this reason you are advised to use specific Virtual Server entries just for the ports your application requires, instead of using DMZ. As doing so will result in all connections from the WAN attempt to access to your public IP of the DMZ PC specified.

If you have disabled the NAT option in the WAN-ISP section, the Virtual Server function will hence be invalid.

If the DHCP server option is enabled, you have to be very careful in assigning the IP addresses of the virtual servers in order to avoid conflicts. The easiest way of configuring Virtual Servers is to manually assign static IP address to each virtual server PC, with an address that does not fall into the range of IP addresses that are to be issued by the DHCP server. You can configure the virtual server IP address manually, but it must still be in the same subnet as the router.

Example: How to setup Port Forwarding for port 21 (FTP server)

If you have FTP server in your LAN network and want others to access it through WAN.

Step 1: Assign a static IP to your local computer that is hosting the FTP server.

Step 2: Login to the Gateway and go to **Configuration / Advanced Setup / NAT / Virtual Server.**

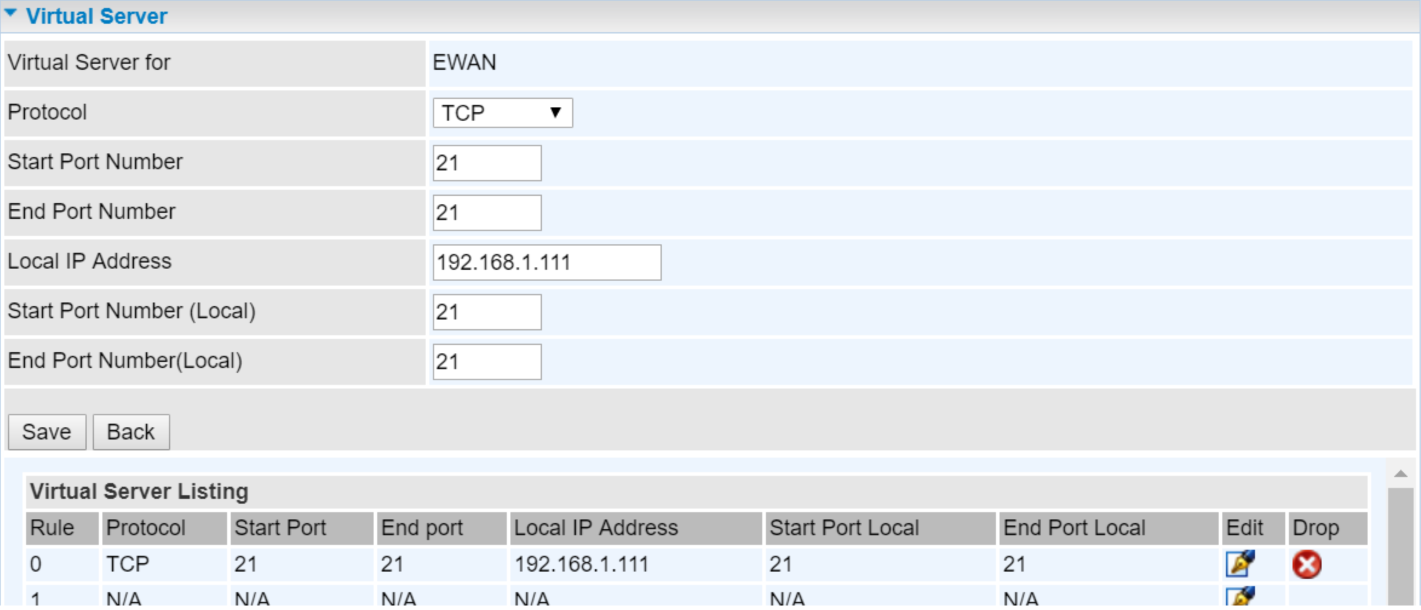
FTP server uses TCP protocol with port 21.

Enter ”21” to Start and End Port Number. The BEC 4700A/AZ will accept port 21 requests from WAN side.

Enter the static IP assigned to the local PC that is hosting the FTP server. Ex: 192.168.1.111

Enter ”21” to Local Start and End Port number. The BEC 4700A/AZ will forward port 21 request from WAN to the specific LAN PC (Example: 192.168.1.111) in the network.

Step 3: Click **Save** to save settings.



Virtual Server

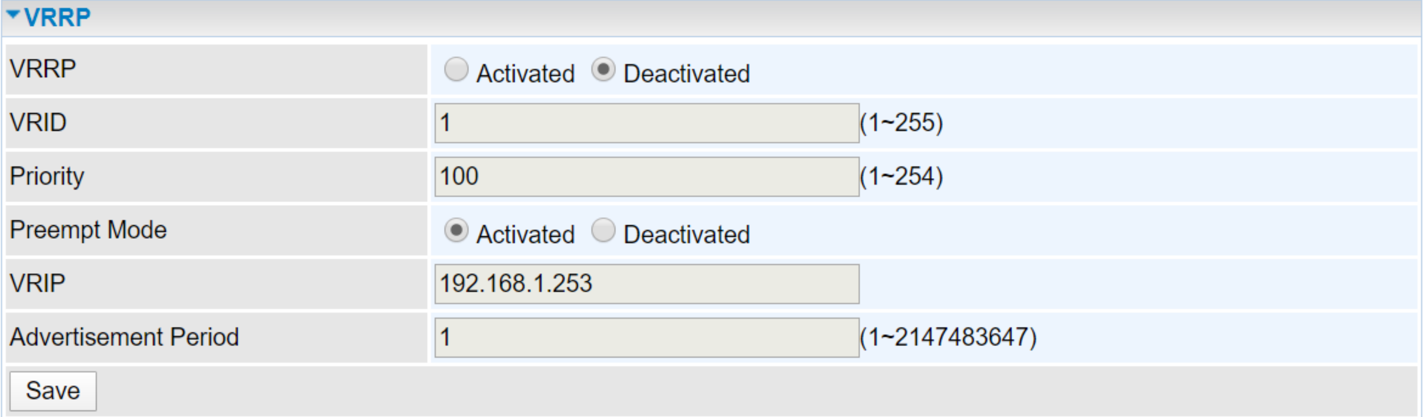
Virtual Server for	EWAN
Protocol	TCP ▼
Start Port Number	21
End Port Number	21
Local IP Address	192.168.1.111
Start Port Number (Local)	21
End Port Number(Local)	21

Virtual Server Listing

Rule	Protocol	Start Port	End port	Local IP Address	Start Port Local	End Port Local	Edit	Drop
0	TCP	21	21	192.168.1.111	21	21	✎	✖
1	N/A	N/A	N/A	N/A	N/A	N/A	✎	

VRRP

VRRP is designed to eliminate the single point of failure inherent in the static default routed environment. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers in a LAN. The VRRP router controlling the IP address associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the Master become unavailable. Any of the virtual router's IP addresses in a LAN can then be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.



▾VRRP

VRRP	○ Activated ● Deactivated
VRID	1 (1~255)
Priority	100 (1~254)
Preempt Mode	● Activated ○ Deactivated
VRIP	192.168.1.253
Advertisement Period	1 (1~2147483647)

VRRP: Click to activate the feature.

VRID: Virtual Router Identifier, range from 1-255 (decimal). A master or backup router running the VRRP protocol may participate in one VRID instance.

Priority: Specifies the sending VRRP router's priority for the virtual router. Higher values equal higher priority. The priority value for the VRRP router that owns the IP address associated with the virtual router MUST be 255. VRRP routers backing up a virtual router MUST use priority values between 1 and 254. The default priority value for VRRP routers backing up a virtual router is 100. The priority value zero (0) has special meaning indicating that the current Master has stopped participating in VRRP. This is used to trigger Backup routers to quickly transition to Master without having to wait for the current Master to timeout.

Preempt Mode: When preempt mode is activated, a backup router always takes over the responsibility of the master router. When deactivated, the lower priority backup is left in the master state.

VRIP: An IP address which is associated with the virtual router.

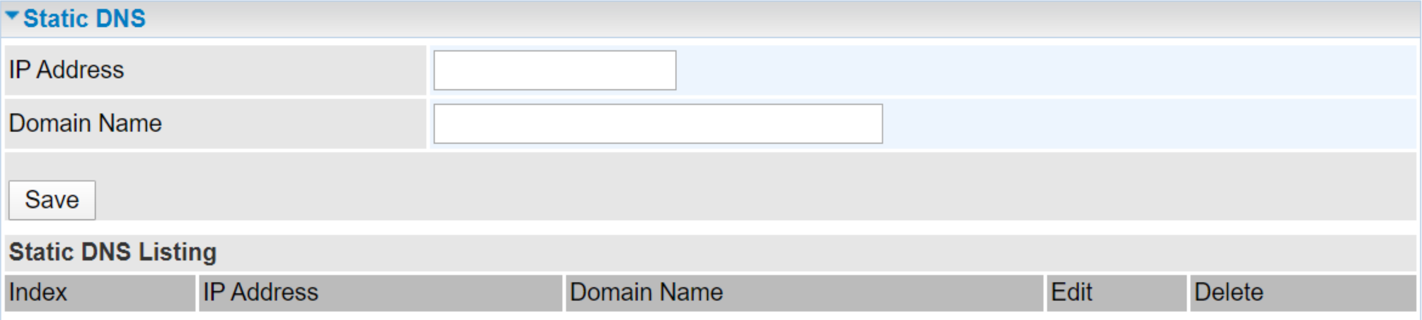
Advertisement period: Indicates the time interval in seconds between advertisements. Default in 1 second.

Click **Save** to apply settings.

Static DNS

The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network associated with various information with domain names assigned to each of the participating entities. Most importantly, it translates domain names meaningful to humans into the numerical identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

An often-used analogy to explain the Domain Name System is that it serves as the phone book for the Internet by translating human-friendly computer hostnames into IP addresses. For example, the domain name www.example.com can be translated into the addresses 192.0.32.10 (IPv4).



▾Static DNS

IP Address	
Domain Name	

Static DNS Listing

Index	IP Address	Domain Name	Edit	Delete

IP Address: Enter a static DNS IP address.

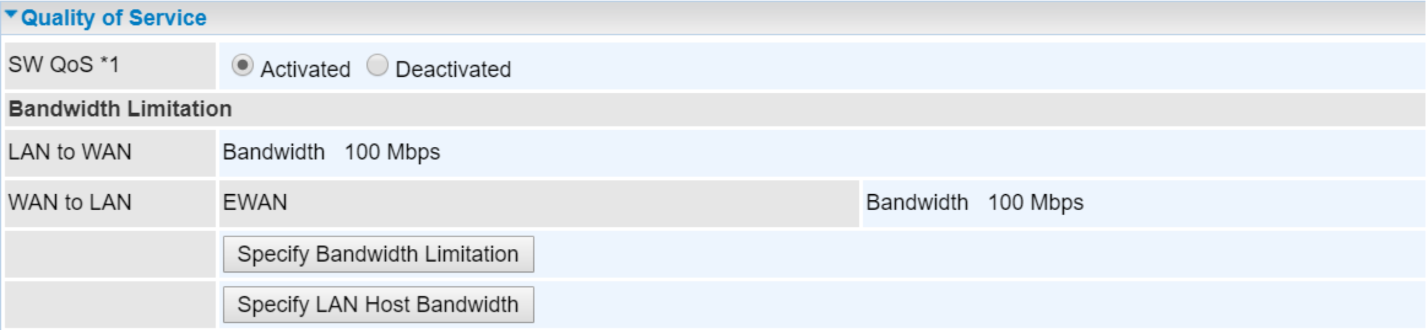
Domain Name: Enter a domain name which can be converted to the IP address from above.

Click **Save** to apply settings.

QoS

QoS helps you control the upload traffic of each application from LAN (Ethernet and/or Wireless) to WAN (Internet).

It facilitates you the features to control the quality of throughput for each application. This is useful when there on certain types of data you want giver higher priority to, such as voice data packets given higher priority than web data packets.



Quality of Service

SW QoS *1	● Activated ○ Deactivated	
Bandwidth Limitation		
LAN to WAN	Bandwidth 100 Mbps	
WAN to LAN	EWAN	Bandwidth 100 Mbps
	Specify Bandwidth Limitation	
	Specify LAN Host Bandwidth	

SW QoS: Select **Activate** to enable the feature.

Bandwidth Limitation

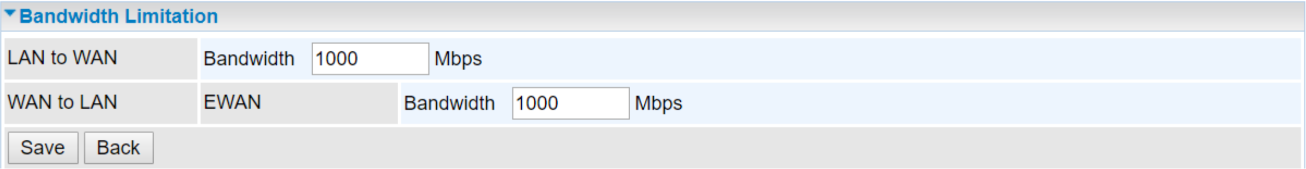
LAN to WAN (Bandwidth): Display maximum upstream bandwidth.

WAN to LAN (Bandwidth): Display maximum downstream bandwidth.

Specify Bandwidth Limitation: Click to update/change the allowed bandwidth.

- **LAN to WAN (Upstream):** Enter the maximum upstream bandwidth.
- **WAN to LAN (Downstream):** Enter the maximum downstream bandwidth.

Click **Bandwidth Save** to save settings.



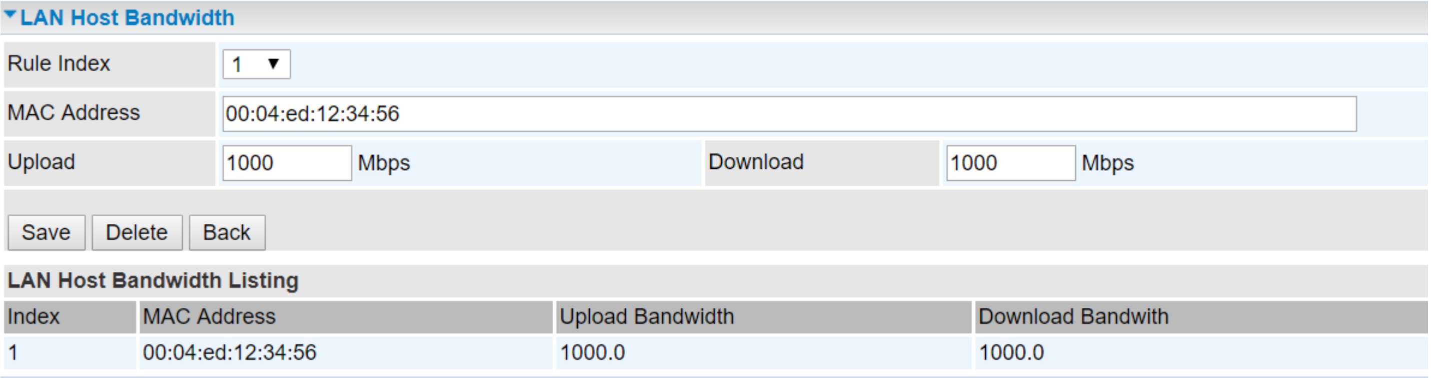
Bandwidth Limitation

LAN to WAN	Bandwidth 1000 Mbps	
WAN to LAN	EWAN	Bandwidth 1000 Mbps
Save Back		

Specify LAN Host Bandwidth: Allow specific LAN device(s) to skip the bandwidth control.

- **Index:** The rule indicator (1-32) for identifying each host device.
- **MAC Address:** Enter the host's MAC address. For example: 00:04:ed:12:34:56
- **Upload / Download (Bandwidth):** Enter maximum available upload and download bandwidth for the specific device.

Click **Save** to apply settings.



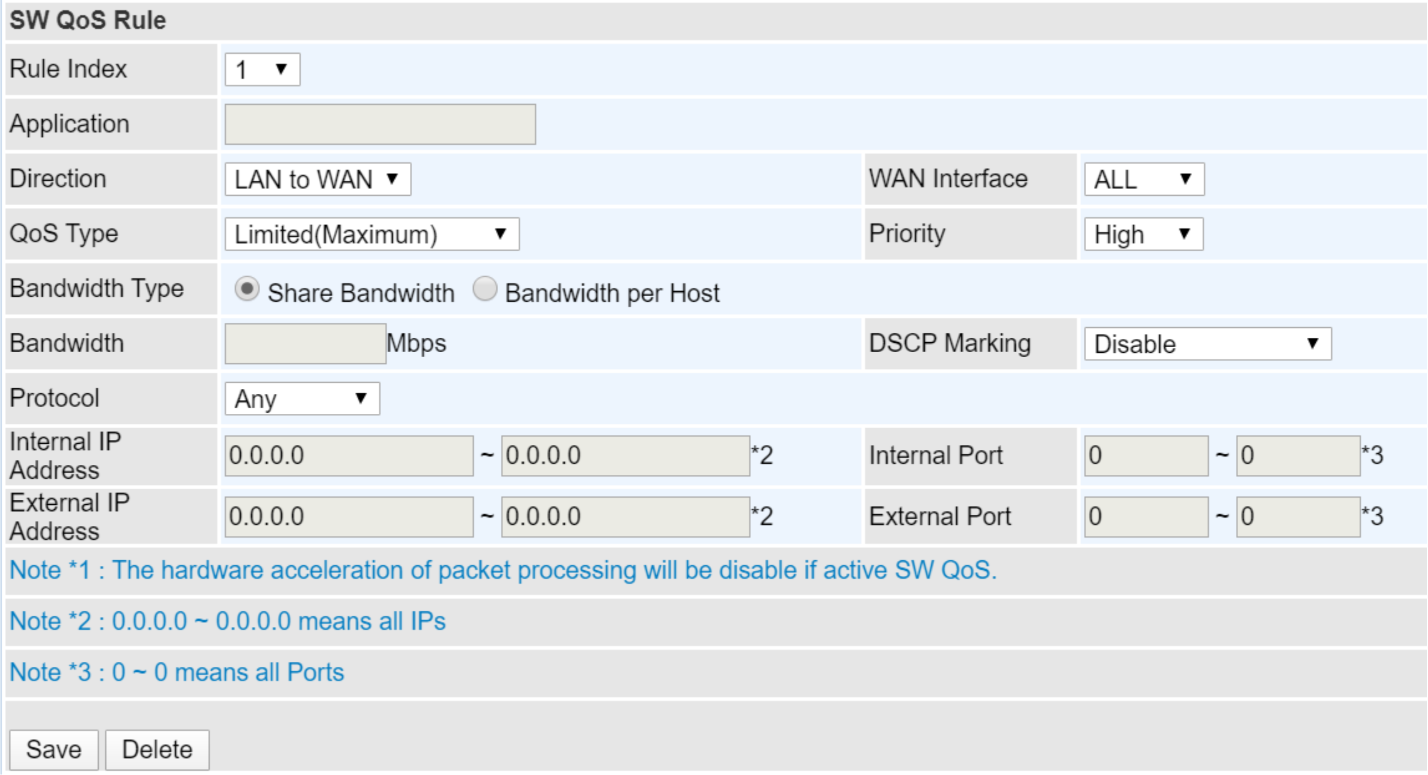
▾LAN Host Bandwidth

Rule Index	1 ▼		
MAC Address	00:04:ed:12:34:56		
Upload	1000 Mbps	Download	1000 Mbps

LAN Host Bandwidth Listing

Index	MAC Address	Upload Bandwidth	Download Bandwith
1	00:04:ed:12:34:56	1000.0	1000.0

SW QoS Rule



SW QoS Rule

Rule Index	1 ▼		
Application			
Direction	LAN to WAN ▼	WAN Interface	ALL ▼
QoS Type	Limited(Maximum) ▼	Priority	High ▼
Bandwidth Type	● Share Bandwidth ○ Bandwidth per Host		
Bandwidth	Mbps	DSCP Marking	Disable ▼
Protocol	Any ▼		
Internal IP Address	0.0.0.0 ~ 0.0.0.0 *2	Internal Port	0 ~ 0 *3
External IP Address	0.0.0.0 ~ 0.0.0.0 *2	External Port	0 ~ 0 *3

Note *1 : The hardware acceleration of packet processing will be disable if active SW QoS.

Note *2 : 0.0.0.0 ~ 0.0.0.0 means all IPs

Note *3 : 0 ~ 0 means all Ports

Rule Index: Index marking for each rule up to maximum of 16.

Application: Assign a name that identifies the new QoS application rule, e.g. FTP, HTTP, etc.

Direction: Shows the direction mode of the QoS application

- **WAN Interface:** Select a WAN interface connection to allow external access to your internal network.

QoS Type: Choose ***Limited*** (Maximum) or ***Guaranteed*** (Minimum) to specify the date rate is allowed for this policy.

- **Priority:** Set the priority given to each policy/application. Specify the priority for the use of bandwidth. You can specify which application can have higher priority to acquire the bandwidth. Its default setting is set to High. You may adjust this setting to fit your policy / application.

Bandwidth Type: It is available when select **Limited (Maximum)** of QoS Type.

- **Share Bandwidth –** The specific bandwidth, can be configured below, is shared by all devices within the internal IP address/range.

  - **Example:** Share Bandwidth**,** Bandwidth set to 100Mbps, Internal IP Address: 192.168.1.100-104 (total of 5).

    Result: IP 192.168.100-104, those 5 devices will share bandwidth of 100Mbps.

- **Bandwidth per Host –** Each of the LAN devices within the internal IP address/range obtain the specific bandwidth configured below.
  - **Example:** Bandwidth per Host**,** Bandwidth set to 50Mbps, Internal IP Address: 192.168.1.100-104 (total of 5).

    Result: The IP address/device, 192.168.100-104, each will obtain up to 50Mbps bandwidth/data to access to the Internet.

Bandwidth (Mbps): Specify the bandwidth for this application.

DSCP Marking: Differentiated Services Code Point (DSCP), it is the first 6 bits in the ToS byte. DSCP Marking allows users to classify the traffic of the application to be executed according to the DSCP value.

Protocol: Select a protocol from the drop-down list

Internal IP Address: The IP address values for Local LAN devices you want to give control.

- **Internal Port:** The Port number on the LAN side, it is used to identify an application.

External IP Address: The IP address on remote / WAN side.

- **External Port:** The Port number on the remote / WAN side.

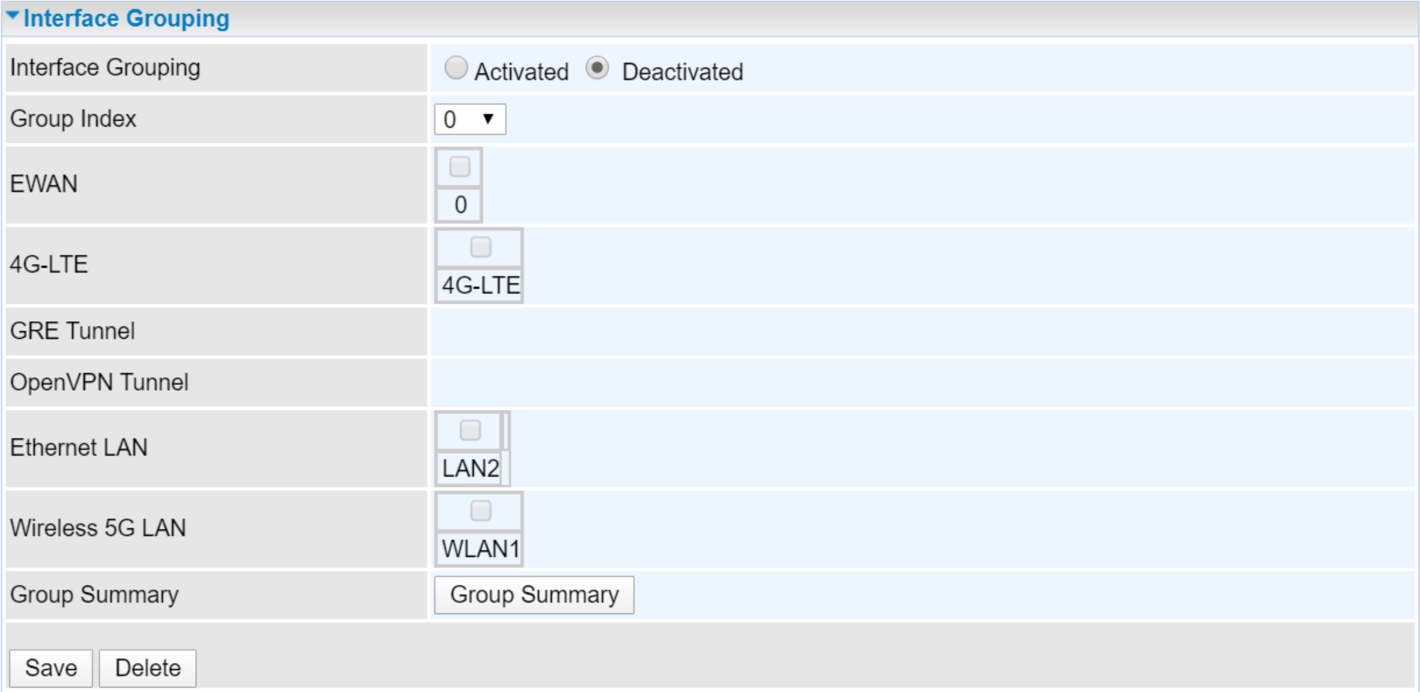
Click **Save** to apply settings.

To Remove a Policy: Simply select the Index then hit the **Delete** button to remove from the list.

Interface Grouping

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, commonly known as a VLAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Similarly, they may also have been split into two different groups, even if they are on the same switch.

Each group will perform as an independent network. To support this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Save** button.



▾Interface Grouping

Interface Grouping	○ Activated ● Deactivated
Group Index	0 ▾
EWAN	□ 0
4G-LTE	□ 4G-LTE
GRE Tunnel	
OpenVPN Tunnel	
Ethernet LAN	□ LAN2
Wireless 5G LAN	□ WLAN1
Group Summary	Group Summary

Interface Grouping: Select **Yes** to enable Interface Grouping feature.

Group Index: The index number indicating the current group ranging from 0 to 15.

EWAN Service: The available EWAN interface. Move to Interface Setup to add another EWAN interface.

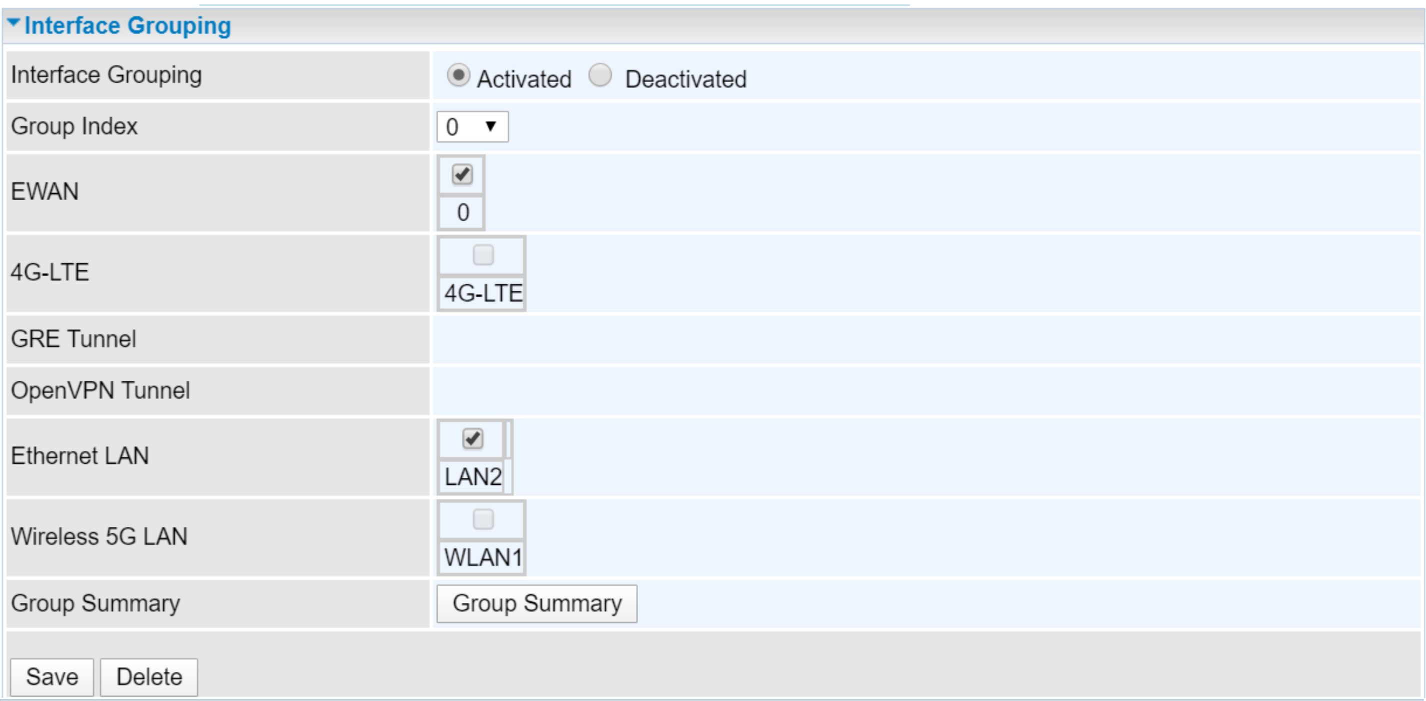
4G-LTE / GRE Tunnel / OpenVPN Tunnel / Ethernet LAN / Wireless LAN: If the interface is ready/available, the click box will be shown.

Group Summary: Click to review all configured grouping information.

Example: Create two WAN services, 4G/LTE and EWAN

You are going to group the ports and services into two working group, as shown below.

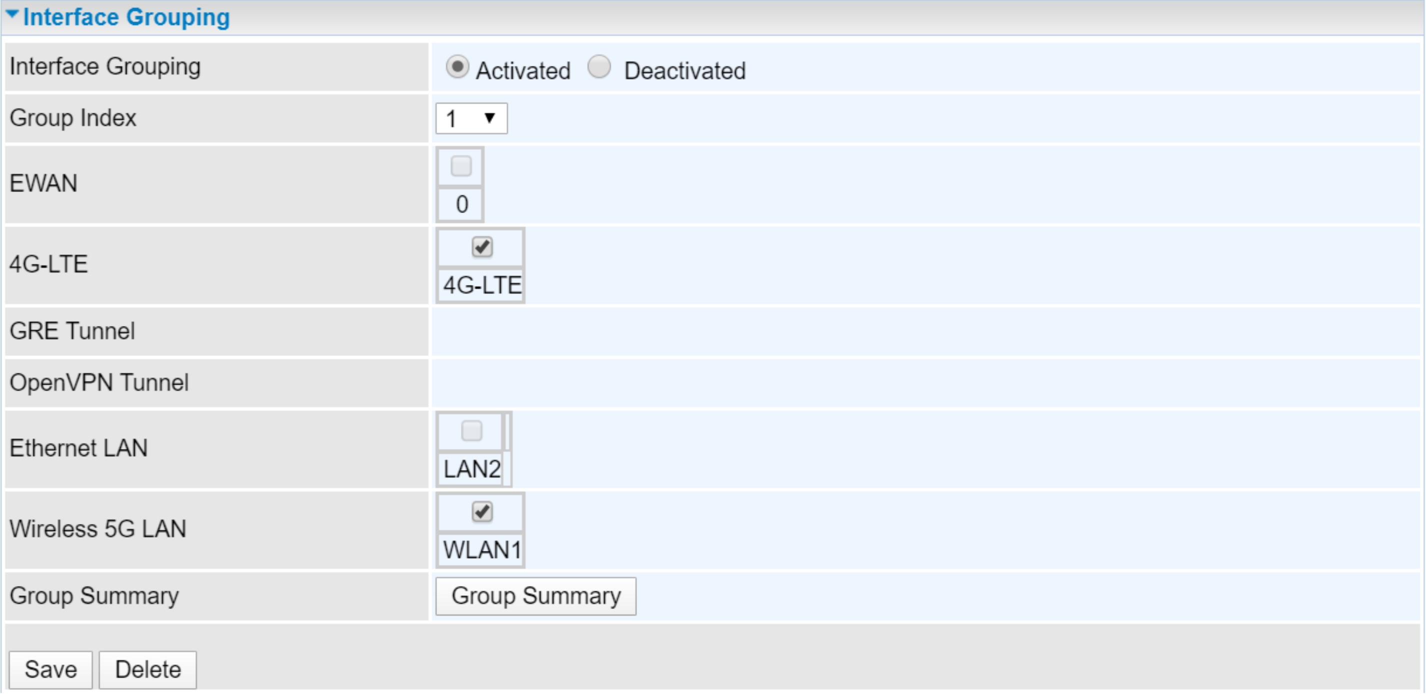
Group Index	Group Port
0	4G-LTE, LAN2
1	EWAN, Wi-Fi



Interface Grouping

Interface Grouping	● Activated ○ Deactivated
Group Index	0 ▼
EWAN	☑ 0
4G-LTE	□ 4G-LTE
GRE Tunnel	
OpenVPN Tunnel	
Ethernet LAN	☑ LAN2
Wireless 5G LAN	□ WLAN1
Group Summary	Group Summary

Save Delete

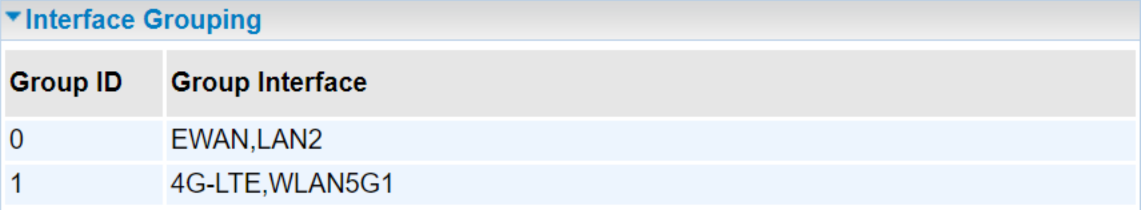


Interface Grouping

Interface Grouping	● Activated ○ Deactivated
Group Index	1 ▼
EWAN	□ 0
4G-LTE	☑ 4G-LTE
GRE Tunnel	
OpenVPN Tunnel	
Ethernet LAN	□ LAN2
Wireless 5G LAN	☑ WLAN1
Group Summary	Group Summary

Save Delete

Click **Group Summary** to show the configuration results.



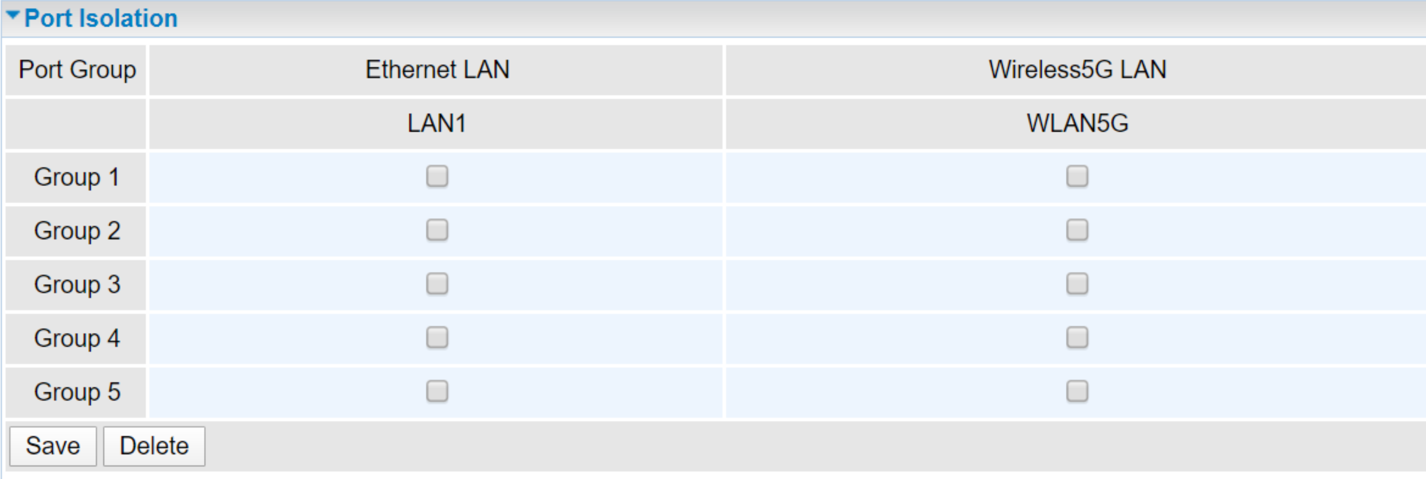
▾Interface Grouping

Group ID	Group Interface
0	EWAN,LAN2
1	4G-LTE,WLAN5G1

Port Isolation

Port isolation is to prevent LAN (Wired or Wireless) devices, e.g. PC, Notebook, to associate or communicate with each other devices. By default, all ports (LAN port and WLAN port) are sharing one group, and devices in all these ports can have access to each other.

Available LAN interfaces of the BEC 4700A/AZ are LAN, Wireless 2.4G, and Wireless 5G.



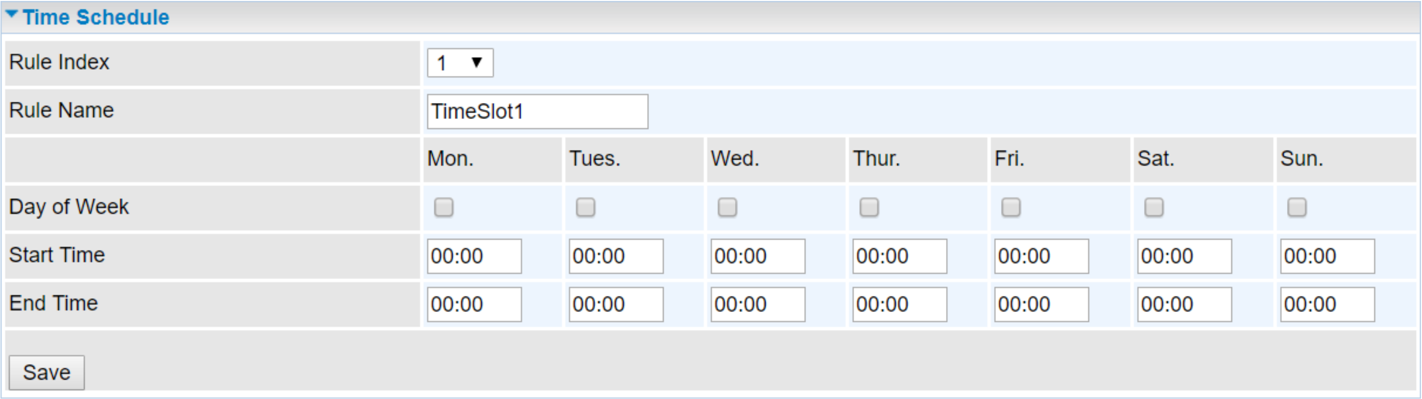
▼Port Isolation

Port Group	Ethernet LAN	Wireless5G LAN
	LAN1	WLAN5G
Group 1	□	□
Group 2	□	□
Group 3	□	□
Group 4	□	□
Group 5	□	□

Time Schedule

The Time Schedule supports up to **16** timeslots which helps you to manage your Internet connection. In each time profile, you may schedule specific day(s) i.e. Monday through Sunday to restrict or allowing the usage of the Internet by users or applications.

This Time Schedule correlates closely with router's time, since router does not have a real time clock on board; it uses the Simple Network Time Protocol (SNTP) to get the current time from an SNTP server from the Internet.



▾ Time Schedule

Rule Index	1 ▼						
Rule Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	□	□	□	□	□	□	□
Start Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time	00:00	00:00	00:00	00:00	00:00	00:00	00:00

Save

Time Index: The rule indicator (1-16) for identifying each timeslot.

Name: User-defined identification for each time period.

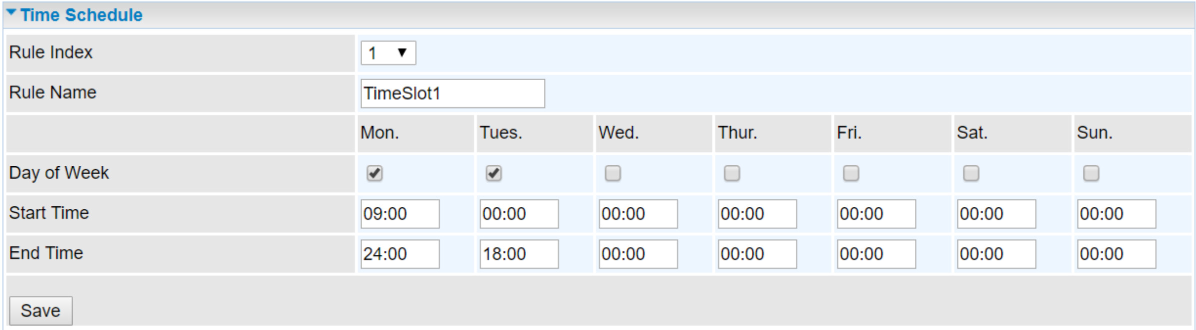
Day of Week: Mon. to Sun. Specify the time interval for each timeslot from "Day of Week".

Start Time: The starting point of the interval for the timeslot, anytime in 00:00 – 24:00.

End Time: The ending point of the interval for the timeslot, anytime in 00:00 – 24:00.

Click **Save** to apply your settings.

Example, you can add a timeslot named "TimeSlot1" which features a period from 9:00 of Monday to 18:00 of Tuesday.

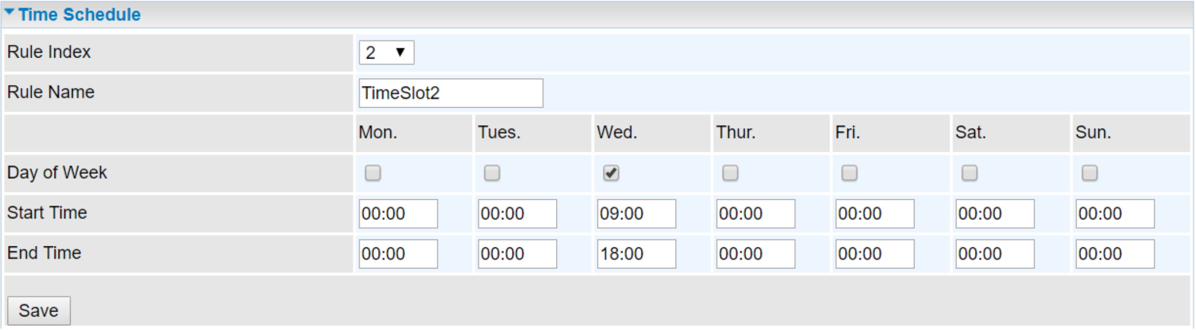


▾ Time Schedule

Rule Index	1 ▼						
Rule Name	TimeSlot1						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	☑	☑	□	□	□	□	□
Start Time	09:00	00:00	00:00	00:00	00:00	00:00	00:00
End Time	24:00	18:00	00:00	00:00	00:00	00:00	00:00

Save

"TimeSlot2" from 09:00 to 18:00 of Wednesday



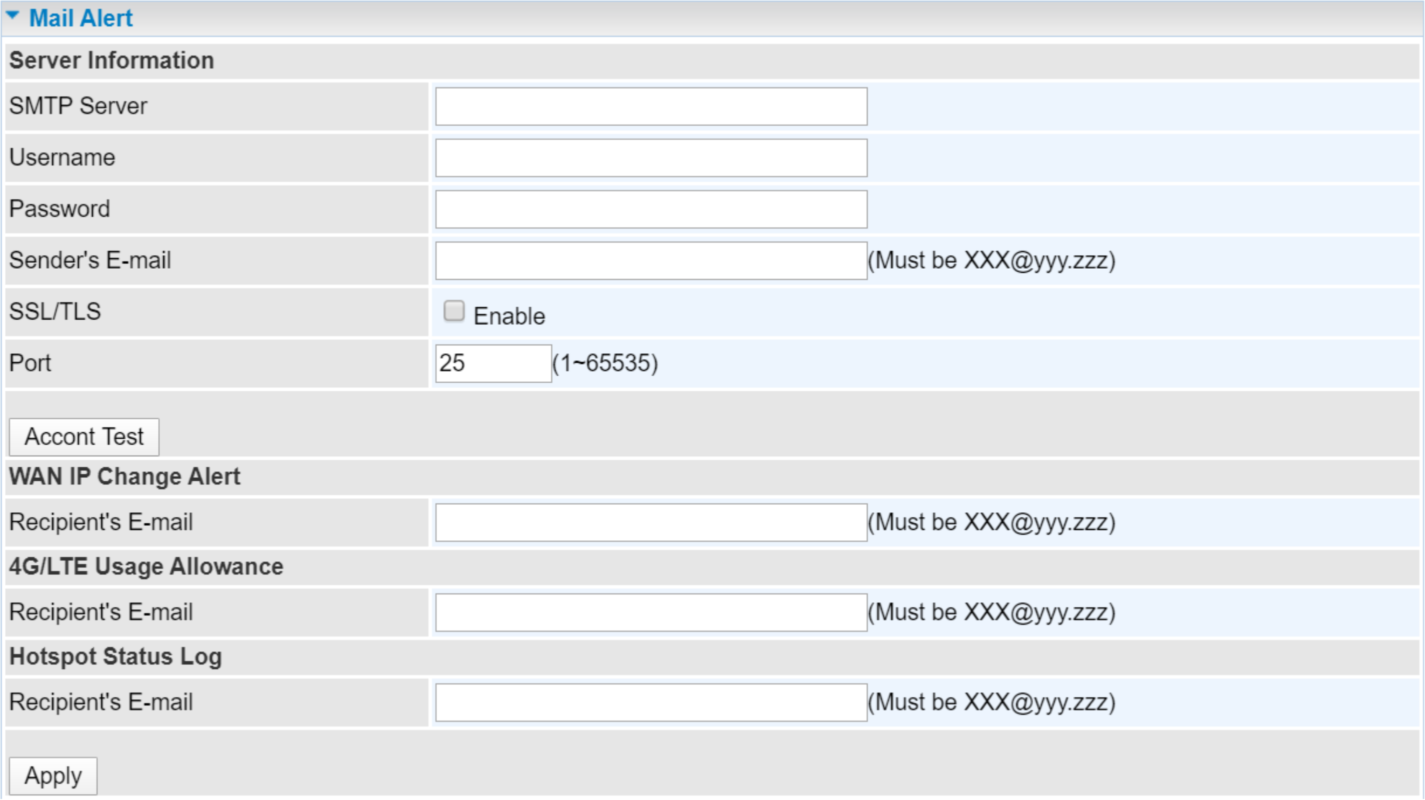
▾ Time Schedule

Rule Index	2 ▼						
Rule Name	TimeSlot2						
	Mon.	Tues.	Wed.	Thur.	Fri.	Sat.	Sun.
Day of Week	□	□	☑	□	□	□	□
Start Time	00:00	00:00	09:00	00:00	00:00	00:00	00:00
End Time	00:00	00:00	18:00	00:00	00:00	00:00	00:00

Save

Mail Alert

Mail alert is designed to keep system administrator or other relevant personnel alerted of any unexpected events that might have occurred to the network computers or server for monitoring efficiency. With this alert system, appropriate solutions may be tackled to fix problems that may have arisen so that the server can be properly maintained.



Server Information	
SMTP Server	
Username	
Password	
Sender's E-mail	(Must be XXX@yyy.zzz)
SSL/TLS	□ Enable
Port	25 (1~65535)
Accont Test	
WAN IP Change Alert	
Recipient's E-mail	(Must be XXX@yyy.zzz)
4G/LTE Usage Allowance	
Recipient's E-mail	(Must be XXX@yyy.zzz)
Hotspot Status Log	
Recipient's E-mail	(Must be XXX@yyy.zzz)
Apply	

SMTP Server: Enter the SMTP server that you would like to use for sending emails.

Username: Enter the username of your email account to be used by the SMTP server.

Password: Enter the password of your email account.

Sender's Email: Enter your email address.

SSL/TLS: Check to whether to enable SSL encryption feature.

Port: the port, default is 25.

Account Test: Click the button to test the connectivity and feasibility to your sender's e-mail.

WAN IP Change Alert

WAN IP Change Alert (Recipient's Email): Enter a valid e-mail address to receive an alert message when WAN IP change has been detected.

4G/LTE Usage Allowance (Recipient's Email): Enter a valid e-mail address to receive an alert message when the 4G/LTE data usage is over the maximum (See **Interface Setup > Internet (4G/LTE) > Usage Allowance**)**Hotspot Status Log (Recipient's Email):** Enter a valid e-mail address to receive hotspot status log.

Click **Apply** button to save settings.

VPN

A **Virtual Private Network** (**VPN**) is a private network that interconnects remote (and often geographically separate) networks through primarily public communication infrastructures such as the Internet. VPNs provide security through tunneling protocols and security procedures such as encryption. For example, a VPN could be used to securely connect the branch offices of an organization to a Headquarter office network through the public Internet.

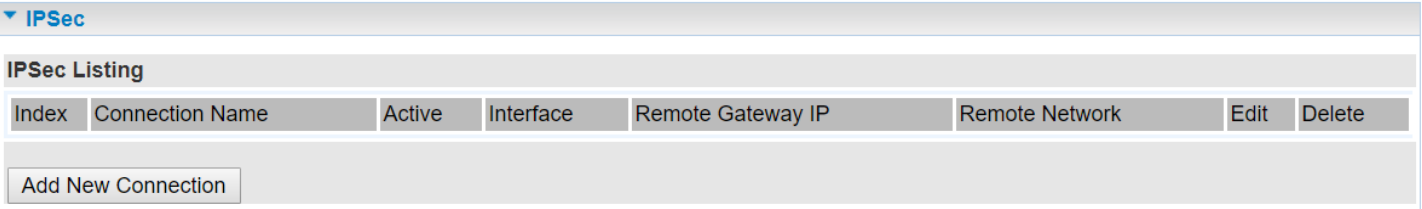
BEC 4700A/AZ supports IPSec, PPTP, L2TP, GRE, and OpenVPN Server / Client VPN features.

IPSec

Internet Protocol Security (**IPSec**) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (*network-to-network*), or between a security gateway and a host (*network-to-host*).

A total of 8 IPSec tunnels can be added.



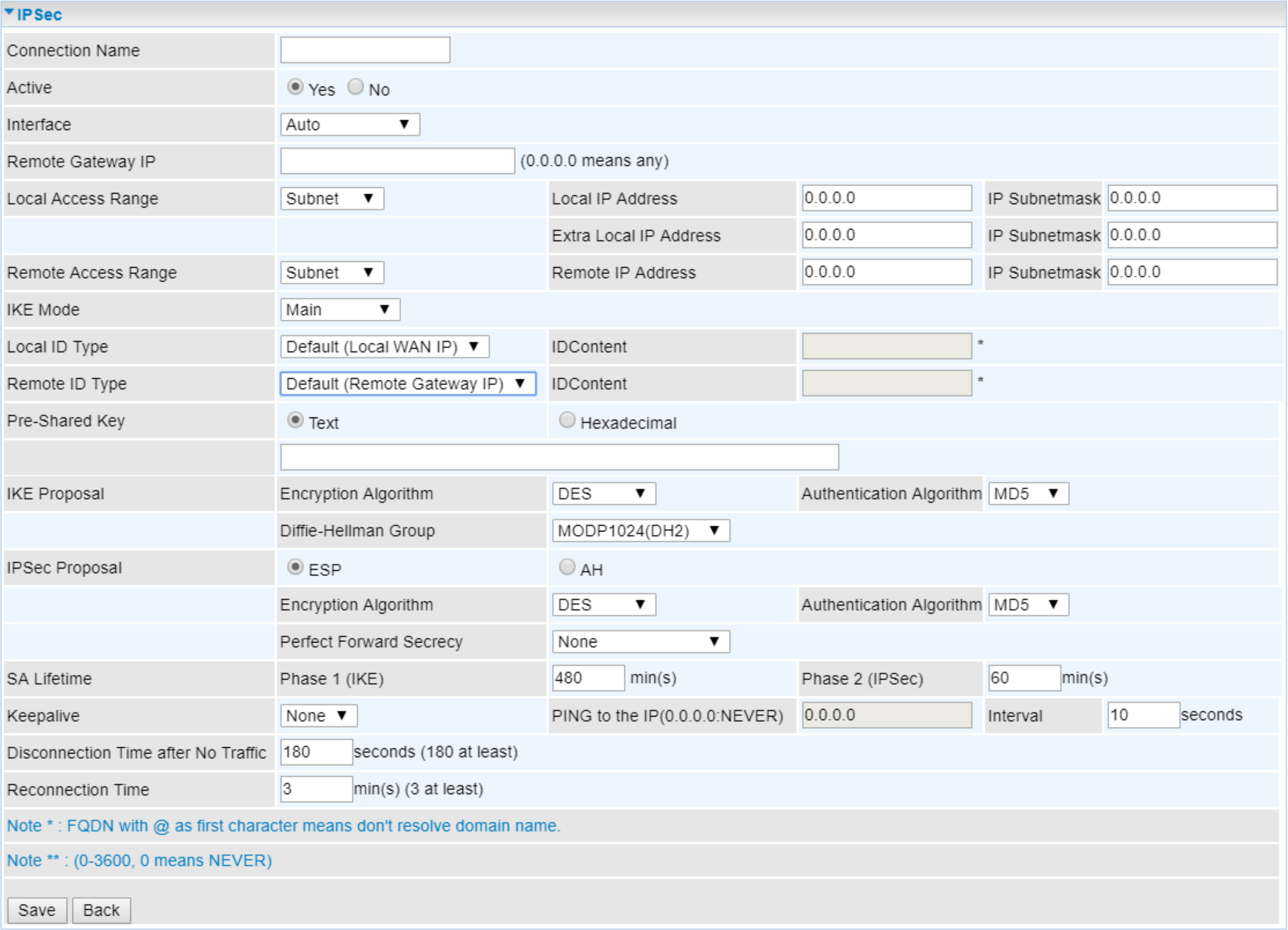
IPSec

IPSec Listing

Index	Connection Name	Active	Interface	Remote Gateway IP	Remote Network	Edit	Delete

Click **Add New Connection** to create a new IPSec profile.

IPSec Connection Setting



Connection Name					
Active	● Yes ○ No				
Interface	Auto ▼				
Remote Gateway IP	(0.0.0.0 means any)				
Local Access Range	Subnet ▼	Local IP Address	0.0.0.0	IP Subnetmask	0.0.0.0
		Extra Local IP Address	0.0.0.0	IP Subnetmask	0.0.0.0
Remote Access Range	Subnet ▼	Remote IP Address	0.0.0.0	IP Subnetmask	0.0.0.0
IKE Mode	Main ▼				
Local ID Type	Default (Local WAN IP) ▼	IDContent	*		
Remote ID Type	Default (Remote Gateway IP) ▼	IDContent	*		
Pre-Shared Key	● Text	○ Hexadecimal			
IKE Proposal	Encryption Algorithm	DES ▼	Authentication Algorithm	MD5 ▼	
	Diffie-Hellman Group	MODP1024(DH2) ▼			
IPSec Proposal	● ESP	○ AH			
	Encryption Algorithm	DES ▼	Authentication Algorithm	MD5 ▼	
	Perfect Forward Secrecy	None ▼			
SA Lifetime	Phase 1 (IKE)	480 min(s)	Phase 2 (IPSec)	60 min(s)	
Keepalive	None ▼	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds
Disconnection Time after No Traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

Note * : FQDN with @ as first character means don't resolve domain name.

Note ** : (0-3600, 0 means NEVER)

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate the connection.

Interface: Select a WAN interface to establish a tunnel with the remote VPN device. **Auto** allows system to automatically initiate a connection via current connected WAN interface.

Remote Gateway IP: The WAN IP address of the remote VPN device. Enter **0.0.0.0** for unknown remote WAN IP address – only the peer can initiate the tunnel connection.

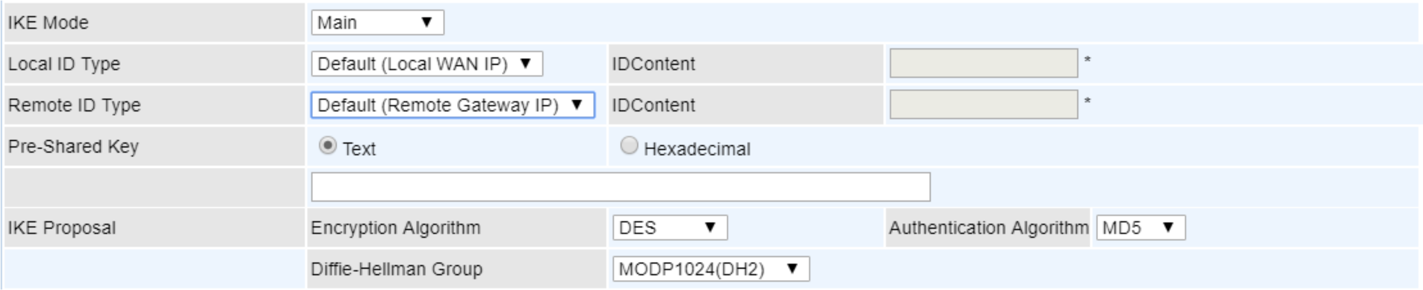
Local Access Range: Set the IP address or subnet of the local network.

- **Single IP:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (*network-to-host*).
- **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (*network-to-network*)

Remote Access Range: Set the IP address or subnet of the remote network.

- **Single IP:** The IP address of the local host, for establishing an IPSec connection between a security gateway and a host (network-to-host). If the remote peer is a host, select Single Address.
- **Subnet:** The subnet of the local network, for establishing an IPSec tunnel between a pair of security gateways (network-to-network), if the remote peer is a network, select Subnet.

IPSec Phase 1(IKE)



IKE Mode	Main ▼				
Local ID Type	Default (Local WAN IP) ▼	IDContent	*		
Remote ID Type	Default (Remote Gateway IP) ▼	IDContent	*		
Pre-Shared Key	● Text	○ Hexadecimal			
IKE Proposal	Encryption Algorithm	DES ▼	Authentication Algorithm	MD5 ▼	
	Diffie-Hellman Group	MODP1024(DH2) ▼			

IKE Mode: IKE, Internet Key Exchange, is the mechanism to negotiate and exchange parameters and keys between IPSec peers to establish security associations (SA). Select Main or Aggressive mode.

Local ID Type / **Remote ID Type:** When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs.

IDContent: Enter IDContent the name you want to identify when the Local and Remote Type are Domain Name; Enter IDContent IP address you want to identify when the Local and Remote Type are IP addresses (IPv4 and IPv6 supported).

Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

IKE Proposal & Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

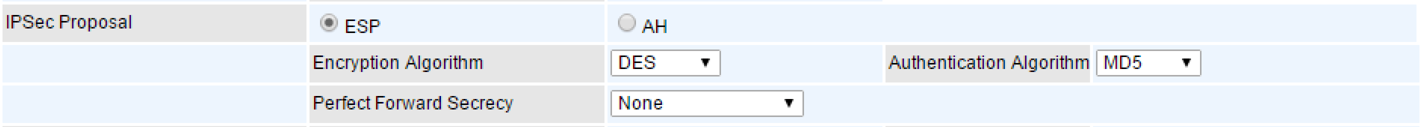
- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

Diffie-Hellman Group: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponential Groups.

IPSec Phase 2(IPSec)



IPSec Proposal	● ESP	○ AH		
	Encryption Algorithm	DES ▼	Authentication Algorithm	MD5 ▼
	Perfect Forward Secrecy	None ▼		

IPSec Proposal: Select the IPSec security method. There are two methods of verifying the authentication information, AH (Authentication Header) and ESP (Encapsulating Security Payload). Use ESP for greater security so that data will be encrypted, and the data origin be authenticated but using AH data origin will only be authenticated but not encrypted.

Encryption Algorithm: Select the encryption algorithm from the drop-down menu. There are several options: DES and AES (128, 192 and 256). 3DES and AES are more powerful but increase latency.

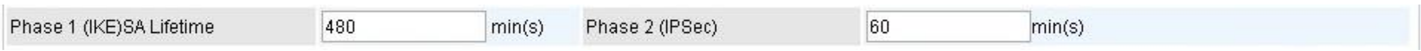
- **DES:** Stands for Data Encryption Standard, it uses 56 bits as an encryption method.
- **3DES:** Stands for Triple Data Encryption Standard, it uses 168 (56*3) bits as an encryption method.
- **AES:** Stands for Advanced Encryption Standards, you can use 128, 192 or 256 bits as encryption method.

Authentication Algorithm: Authentication establishes the integrity of the datagram and ensures it is not tampered with in transmission. There are 3 options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

- **MD5:** A one-way hashing algorithm that produces a 128−bit hash.
- **SHA1:** A one-way hashing algorithm that produces a 160−bit hash.

Perfect Forward Secrecy: It is a public-key cryptography protocol that allows two parties to establish a shared secret over an unsecured communication channel (i.e. over the Internet). MODP stands for Modular Exponentiation Groups.

IPSec SA Lifetime

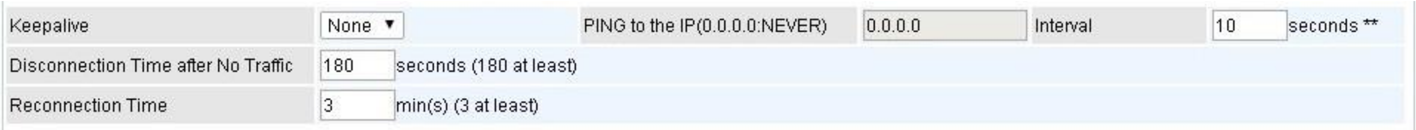


Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)

SA Lifetime: Specify the number of minutes that a Security Association (SA) will stay active before new encryption and authentication key will be exchanged. There are two kinds of SAs, IKE and IPSec. IKE negotiates and establishes SA on behalf of IPSec, and IKE SA is used by IKE.

- **Phase 1 (IKE):** To issue an initial connection request for a new VPN tunnel. The range can be from 5 to 15,000 minutes, and the default is 480 minutes.
- **Phase 2 (IPSec):** To negotiate and establish secure authentication. The range can be from 5 to 15,000 minutes, and the default is 60 minutes. A short SA time increases security by forcing the two parties to update the keys. However, every time the VPN tunnel re-negotiates, access through the tunnel will be temporarily disconnected.

IPSec Connection Keep Alive



Keepalive	None ▼	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds **
Disconnection Time after No Traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

Keep Alive:

- **None:** Disable. The system will not detect remote IPSec peer is still alive or lost. The remote peer will get disconnected after the interval, in seconds, is up.
- **PING:** This mode will detect the remote IPSec peer has lost or not by pinging specify IP address.
- **DPD:** Dead peer detection (DPD) is a keeping alive mechanism that enables the router to be detected lively when the connection between the router and a remote IPSec peer has lost.

Please be noted, it must be enabled on the both sites.

PING to the IP: It is able to IP Ping the remote PC with the specified IP address and alert when the connection fails. Once alter message is received, Router will drop this tunnel connection. Reestablish of this connection is required. Default setting is 0.0.0.0 which disables the function

Interval: This sets the time interval between Pings to the IP function to monitor the connection status. Default interval setting is 10 seconds. Time interval can be set from 0 to 3600 second, 0 second disables the function.

Ping to the IP	**Interval (sec)**	**Ping to the IP Action**
0.0.0.0	0	No
0.0.0.0	2000	No
xxx.xxx.xxx.xxx (A valid IP Address)	0	No
xxx.xxx.xxx.xxx(A valid IP Address)	2000	Yes, activate it in every 2000 second.

Disconnection Time after No Traffic: It is the NO Response time clock. When no traffic stage time is beyond the Disconnection time set, Router will automatically halt the tunnel connection and re-establish it base on the Reconnection Time set. 180 seconds is minimum time interval for this function.

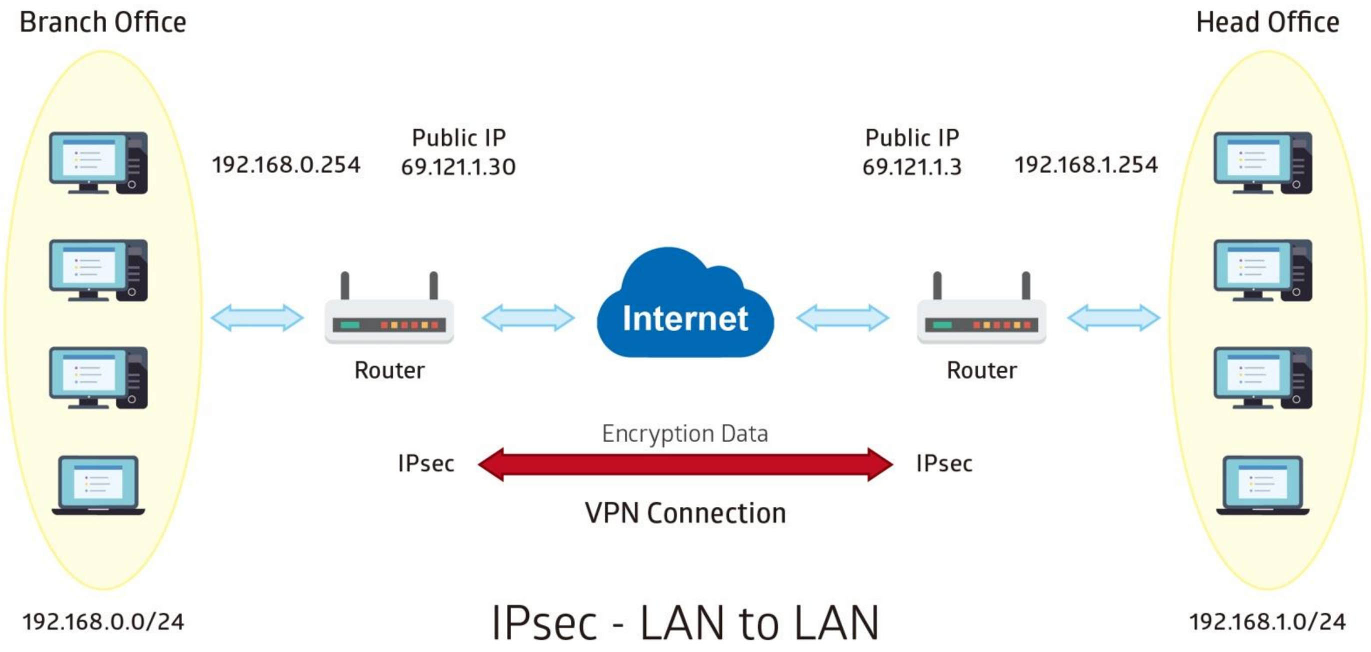
Reconnection Time: It is the reconnecting time interval after NO TRAFFIC is initiated. 3 minutes is minimum time interval for this function.

Click **Save** to apply settings.

Examples: IPSec – Network (LAN) to Network (LAN)

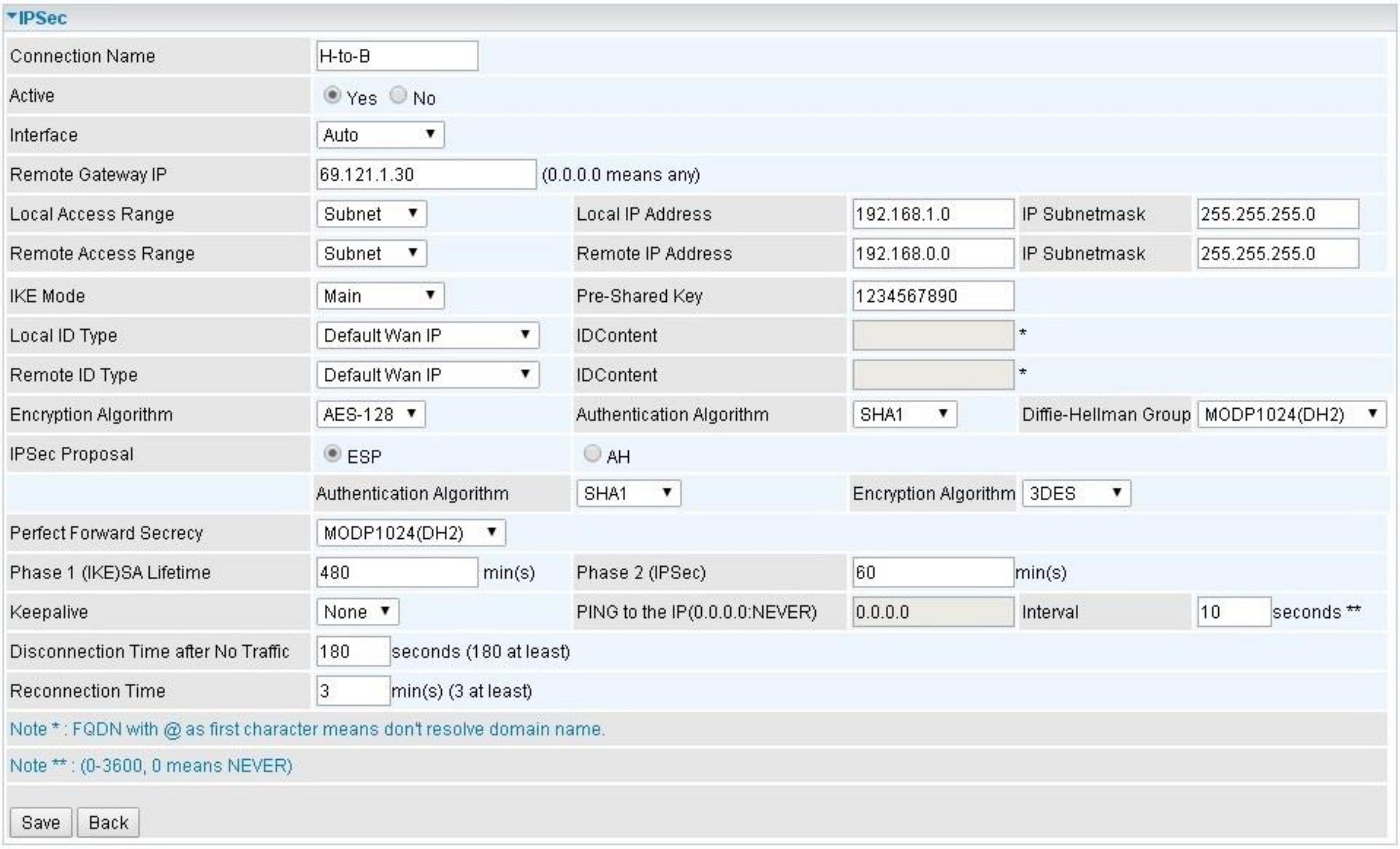
Two of the BEC 4700A/AZ devices want to setup a secure IPSec VPN tunnel

NOTE: The IPSec Settings shall be consistent between the two routers.



Headquarter office Side:

Configuration Settings		Description
Connection Name	H-to-B	Assigned name to this tunnel/profile
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Network		
Local Access Range	Subnet	Headquarter office network
Local Network IP Address	192.168.1.0	
Local Network Netmask	255.255.255.0	
Remote Access Range	Subnet	Branch office network
Remote Network IP Address	192.168.0.0	
Remote Network Netmask	255.255.255.0	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	AES-128	
Phase 1 Authentication	SHA1	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	SHA1	
Phase 2 Encryption	3DES	
Prefer Forward Security	MODP 1024(group2)	



▾IPSec

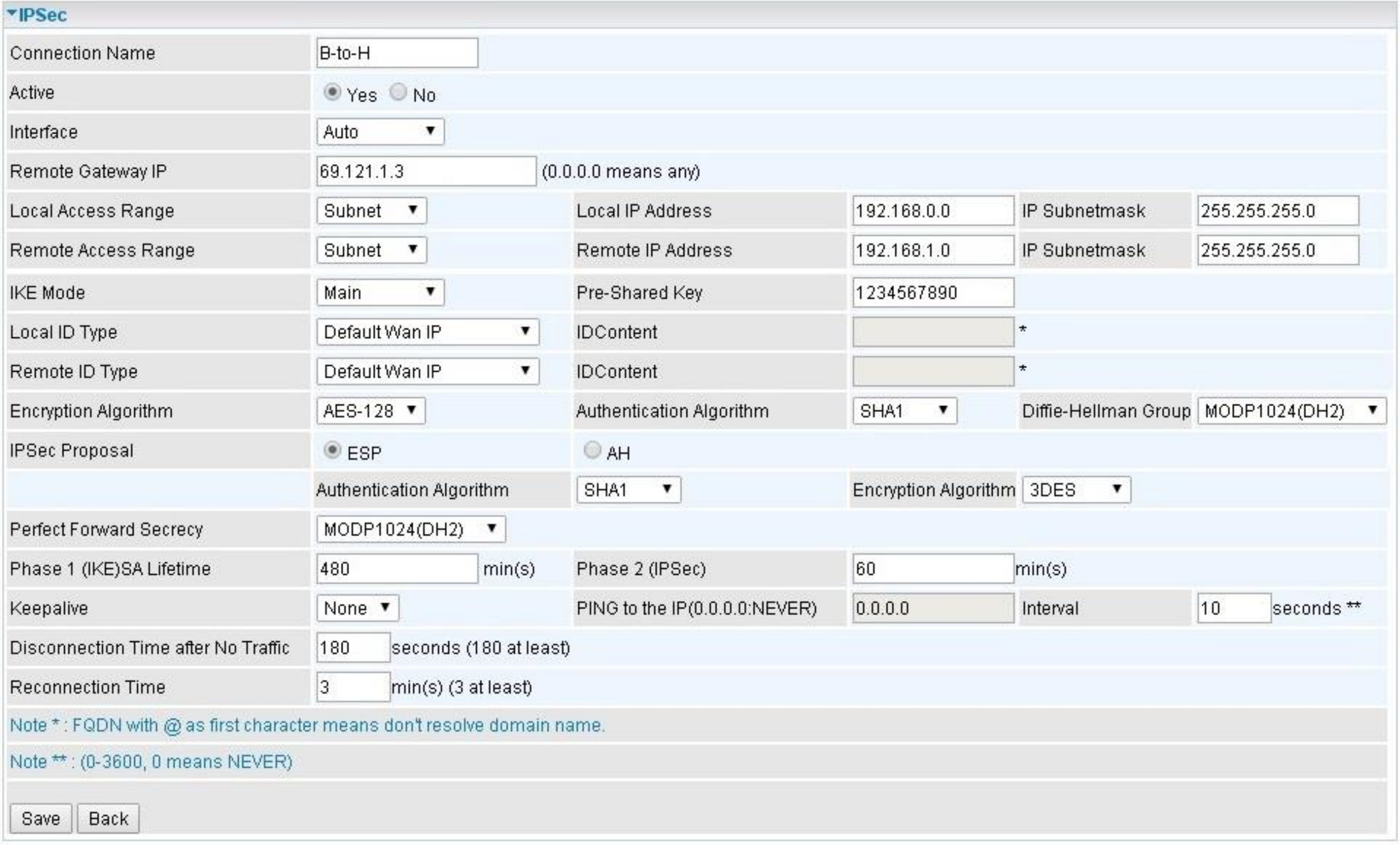
Connection Name	H-to-B				
Active	● Yes ○ No				
Interface	Auto				
Remote Gateway IP	69.121.1.30 (0.0.0.0 means any)				
Local Access Range	Subnet	Local IP Address	192.168.1.0	IP Subnetmask	255.255.255.0
Remote Access Range	Subnet	Remote IP Address	192.168.0.0	IP Subnetmask	255.255.255.0
IKE Mode	Main	Pre-Shared Key	1234567890		
Local ID Type	Default Wan IP	IDContent	*		
Remote ID Type	Default Wan IP	IDContent	*		
Encryption Algorithm	AES-128	Authentication Algorithm	SHA1	Diffie-Hellman Group	MODP1024(DH2)
IPSec Proposal	● ESP	○ AH			
	Authentication Algorithm	SHA1	Encryption Algorithm	3DES	
Perfect Forward Secrecy	MODP1024(DH2)				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
Keepalive	None	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds **
Disconnection Time after No Traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

Note * : FQDN with @ as first character means don't resolve domain name.

Note ** : (0-3600, 0 means NEVER)

Branch Office Side:

Configuration Settings		Description
Connection Name	B-to-H	Assigned name to this tunnel/profile
Remote Secure Gateway	69.121.1.3	IP address of the Branch office gateway
Access Network		
Local Access Range	Subnet	Headquarter office network
Local Network IP Address	192.168.0.0	
Local Network Netmask	255.255.255.0	
Remote Access Range	Subnet	Branch office network
Remote Network IP Address	192.168.1.0	
Remote Network Netmask	255.255.255.0	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	AES-128	
Phase 1 Authentication	SHA1	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	SHA1	
Phase 2 Encryption	3DES	
Prefer Forward Security	MODP 1024(group2)	



IPSec

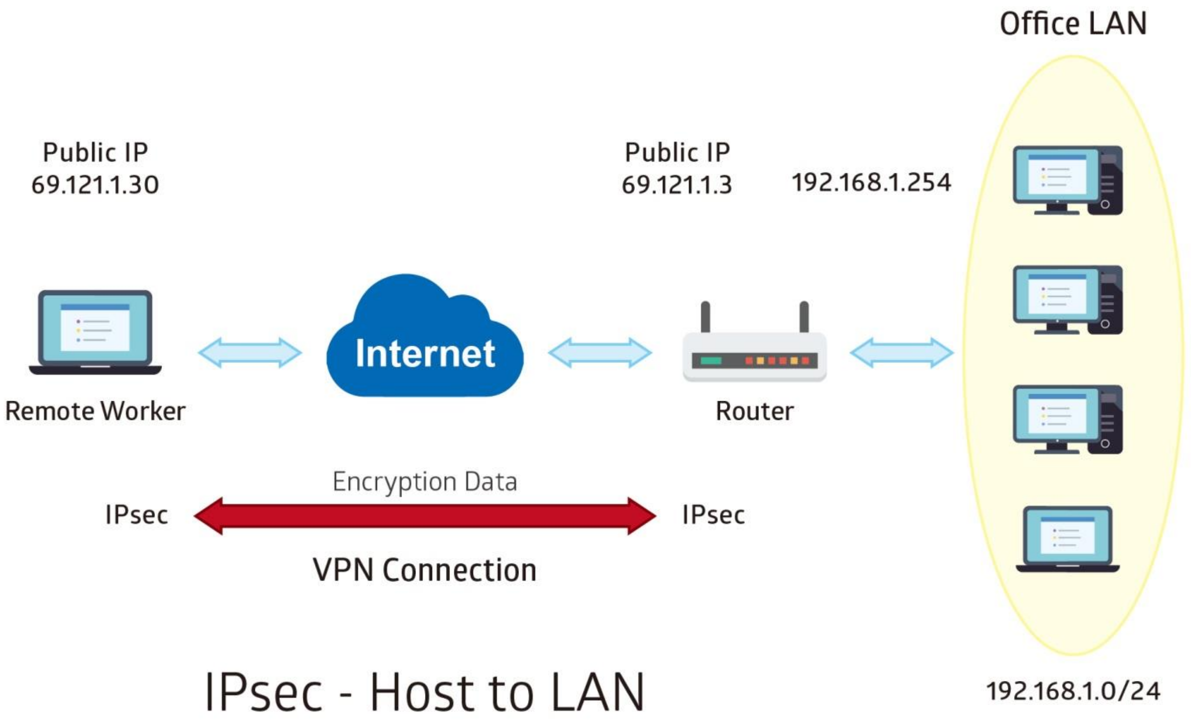
Connection Name	B-to-H				
Active	● Yes ○ No				
Interface	Auto				
Remote Gateway IP	69.121.1.3 (0.0.0.0 means any)				
Local Access Range	Subnet	Local IP Address	192.168.0.0	IP Subnetmask	255.255.255.0
Remote Access Range	Subnet	Remote IP Address	192.168.1.0	IP Subnetmask	255.255.255.0
IKE Mode	Main	Pre-Shared Key	1234567890		
Local ID Type	Default Wan IP	IDContent	*		
Remote ID Type	Default Wan IP	IDContent	*		
Encryption Algorithm	AES-128	Authentication Algorithm	SHA1	Diffie-Hellman Group	MODP1024(DH2)
IPSec Proposal	● ESP	○ AH			
	Authentication Algorithm	SHA1	Encryption Algorithm	3DES	
Perfect Forward Secrecy	MODP1024(DH2)				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
Keepalive	None	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds **
Disconnection Time after No Traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

Note * : FQDN with @ as first character means don't resolve domain name.

Note ** : (0-3600, 0 means NEVER)

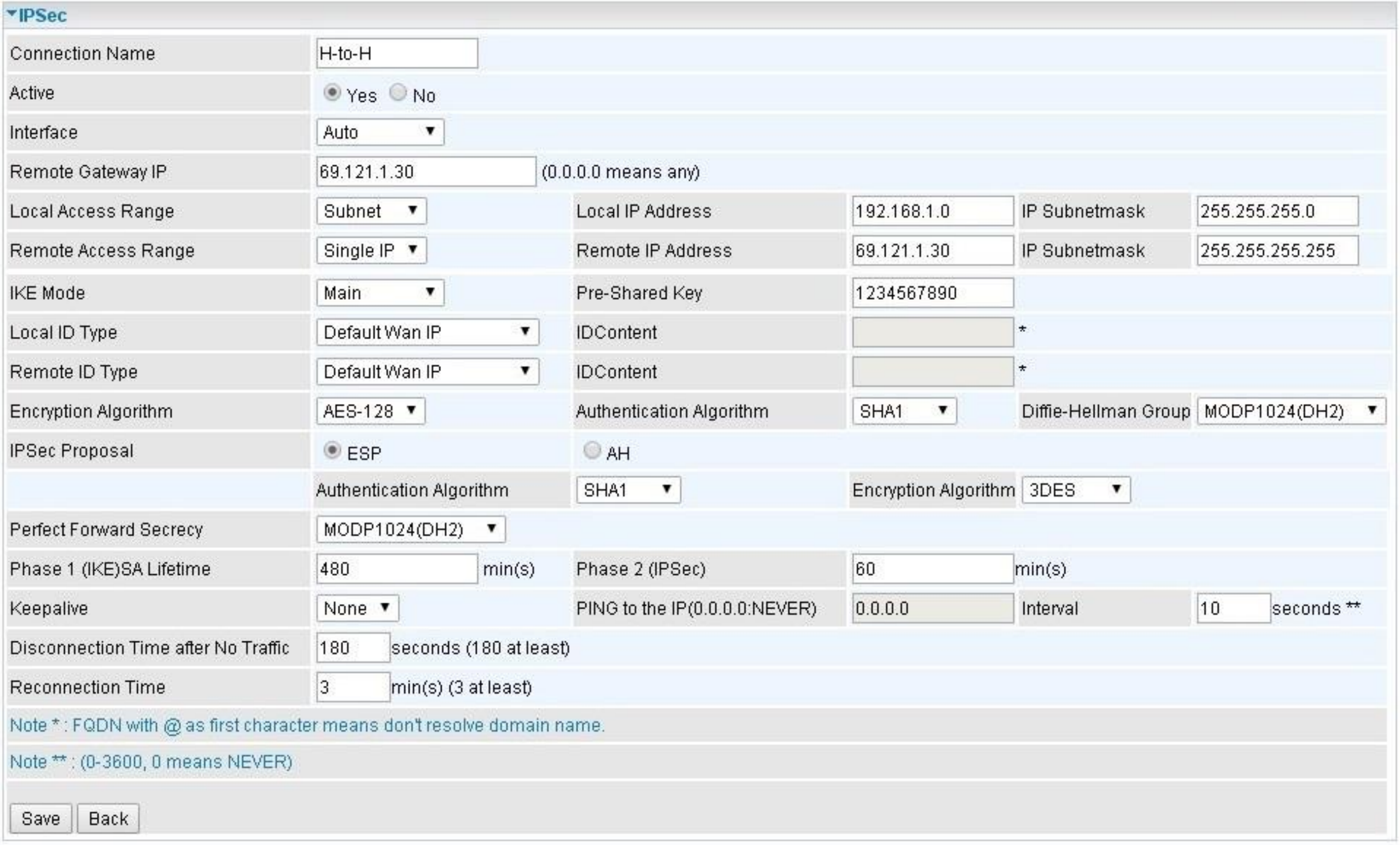
Examples: IPSec – Remote Employee to BEC 4700A/AZ Connection

Router servers as VPN server, and host should install the IPSec client to connect to Headquarter office through IPSec VPN.



Headquarter office Side:

Configuration Settings		Description
Connection Name	H-to-H	Assigned name to this tunnel/profile
Remote Secure Gateway	69.121.1.30	IP address of the Branch office gateway
Access Network		
Local Access Range	Subnet	Headquarter office LAN network information
Local Network IP Address	192.168.1.0	
Local Network Netmask	255.255.255.0	
Remote Access Range	Signal IP	Remote worker IP address
Remote Network IP Address	69.121.1.30	
Remote Network Netmask	255.255.255.255	
IPSec Proposal		
IKE Mode	Main	Security Plan
Pre-Shared Key	1234567890	
Phase 1 Encryption	AES-128	
Phase 1 Authentication	SHA1	
Phase 1 Diffie-Hellman Group	MODP 1024(group2)	
Phase 2 Proposal	ESP	
Phase 2 Authentication	SHA1	
Phase 2 Encryption	3DES	
Prefer Forward Security	MODP 1024(group2)	



IPSec

Connection Name	H-to-H				
Active	● Yes ○ No				
Interface	Auto ▼				
Remote Gateway IP	69.121.1.30 (0.0.0.0 means any)				
Local Access Range	Subnet ▼	Local IP Address	192.168.1.0	IP Subnetmask	255.255.255.0
Remote Access Range	Single IP ▼	Remote IP Address	69.121.1.30	IP Subnetmask	255.255.255.255
IKE Mode	Main ▼	Pre-Shared Key	1234567890		
Local ID Type	Default Wan IP ▼	IDContent	*		
Remote ID Type	Default Wan IP ▼	IDContent	*		
Encryption Algorithm	AES-128 ▼	Authentication Algorithm	SHA1 ▼	Diffie-Hellman Group	MODP1024(DH2) ▼
IPSec Proposal	● ESP	○ AH			
	Authentication Algorithm	SHA1 ▼	Encryption Algorithm	3DES ▼	
Perfect Forward Secrecy	MODP1024(DH2) ▼				
Phase 1 (IKE)SA Lifetime	480 min(s)	Phase 2 (IPSec)	60 min(s)		
Keepalive	None ▼	PING to the IP(0.0.0.0:NEVER)	0.0.0.0	Interval	10 seconds **
Disconnection Time after No Traffic	180 seconds (180 at least)				
Reconnection Time	3 min(s) (3 at least)				

Note * : FQDN with @ as first character means don't resolve domain name.

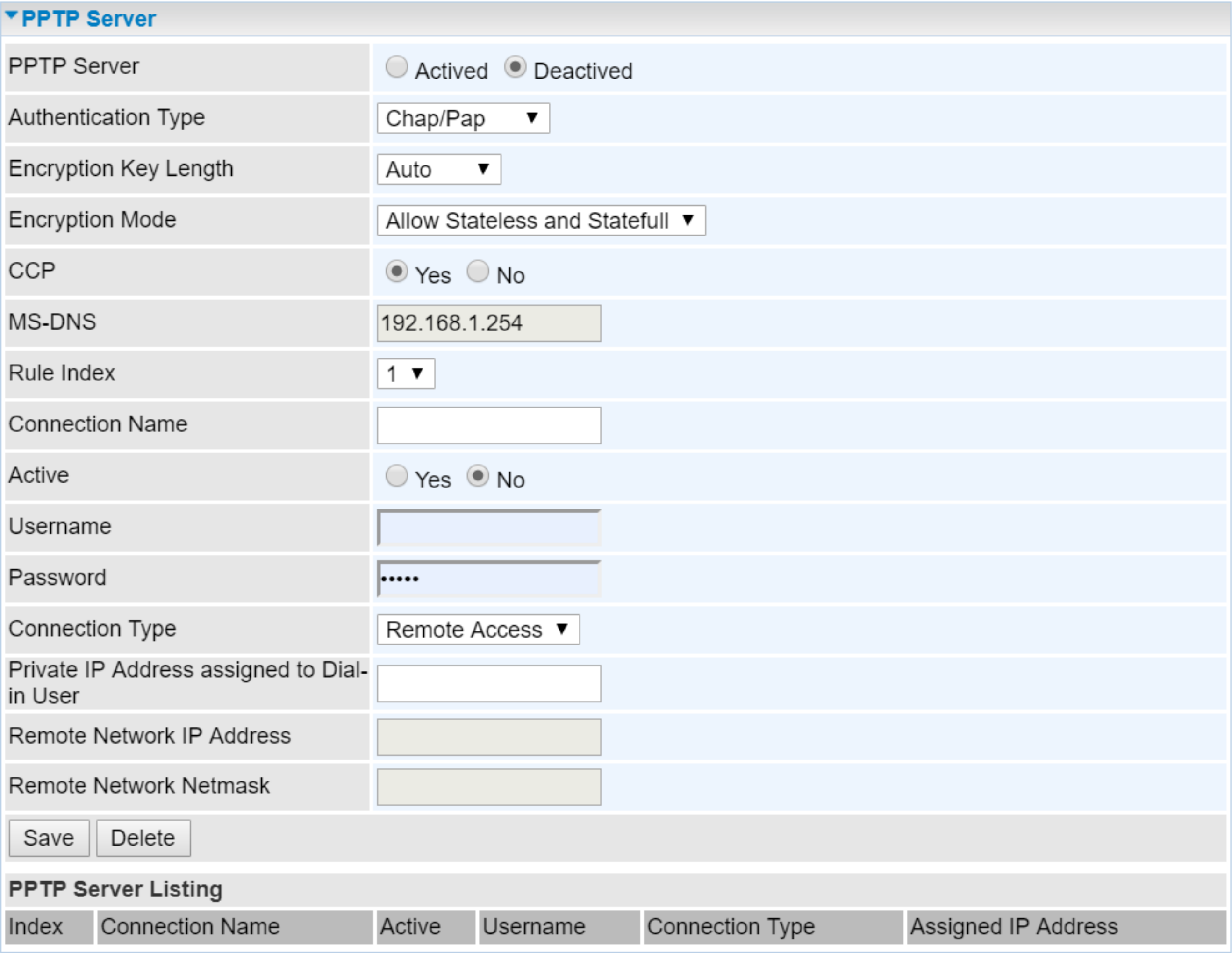
Note ** : (0-3600, 0 means NEVER)

PPTP Server

The **Point-to-Point Tunneling Protocol** (PPTP) is a Layer2 tunneling protocol for implementing virtual private networks through IP network.

In the Microsoft implementation, the tunneled PPP traffic can be authenticated with PAP, CHAP, and Microsoft CHAP V1/V2 . The PPP payload is encrypted using Microsoft Point-to-Point Encryption (MPPE) when using MSCHAPv1/v2.

NOTE: 4 sessions for Client and 4 sessions for Server respectively.



▾PPTP Server

PPTP Server	○ Actived ● Deactived
Authentication Type	Chap/Pap ▼
Encryption Key Length	Auto ▼
Encryption Mode	Allow Stateless and Statefull ▼
CCP	● Yes ○ No
MS-DNS	192.168.1.254
Rule Index	1 ▼
Connection Name	
Active	○ Yes ● No
Username	
Password	•••••
Connection Type	Remote Access ▼
Private IP Address assigned to Dial-in User	
Remote Network IP Address	
Remote Network Netmask	

PPTP Server Listing

Index	Connection Name	Active	Username	Connection Type	Assigned IP Address

PPTP Server: Select **Activate / Deactivate** to enable or disable the PPTP Server.

Authentication Type: Pick an authentication type from the drop-down list. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

Encryption Key Length: Auto, data encryption and key length, with 40-bit or 128-bit, is automatically negotiated when establish a connection. 128-bit keys provide strong stronger encryption than 40-bit keys.

Encryption Mode: The encryption key will be changed every 256 packets with Stateful mode. With Stateless mode, the key will be changed in each packet.

CCP (Compression Control Protocol): Enable to compress data to save bandwidth and increase data transfer speed.

MS-DNS: Assign a DNS server or use router default IP address to be the MS-DNS server IP address.

Rule Index: The indication of the rule number. The maximum entry is up to 4.

Connection Name: Enter a description for this connection/profile.

Active: **Yes** to activate the account. PPTP server is waiting for the client to connect to this account.

Username / Password: Enter the username / password for this profile.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Private IP Address Assigned to Dial-in User: Specify the private IP address to be assigned to dial-in clients, and the IP should be in the same subnet as local LAN, but not occupied.

Remote Network IP Address: Enter the subnet IP of the remote LAN network.

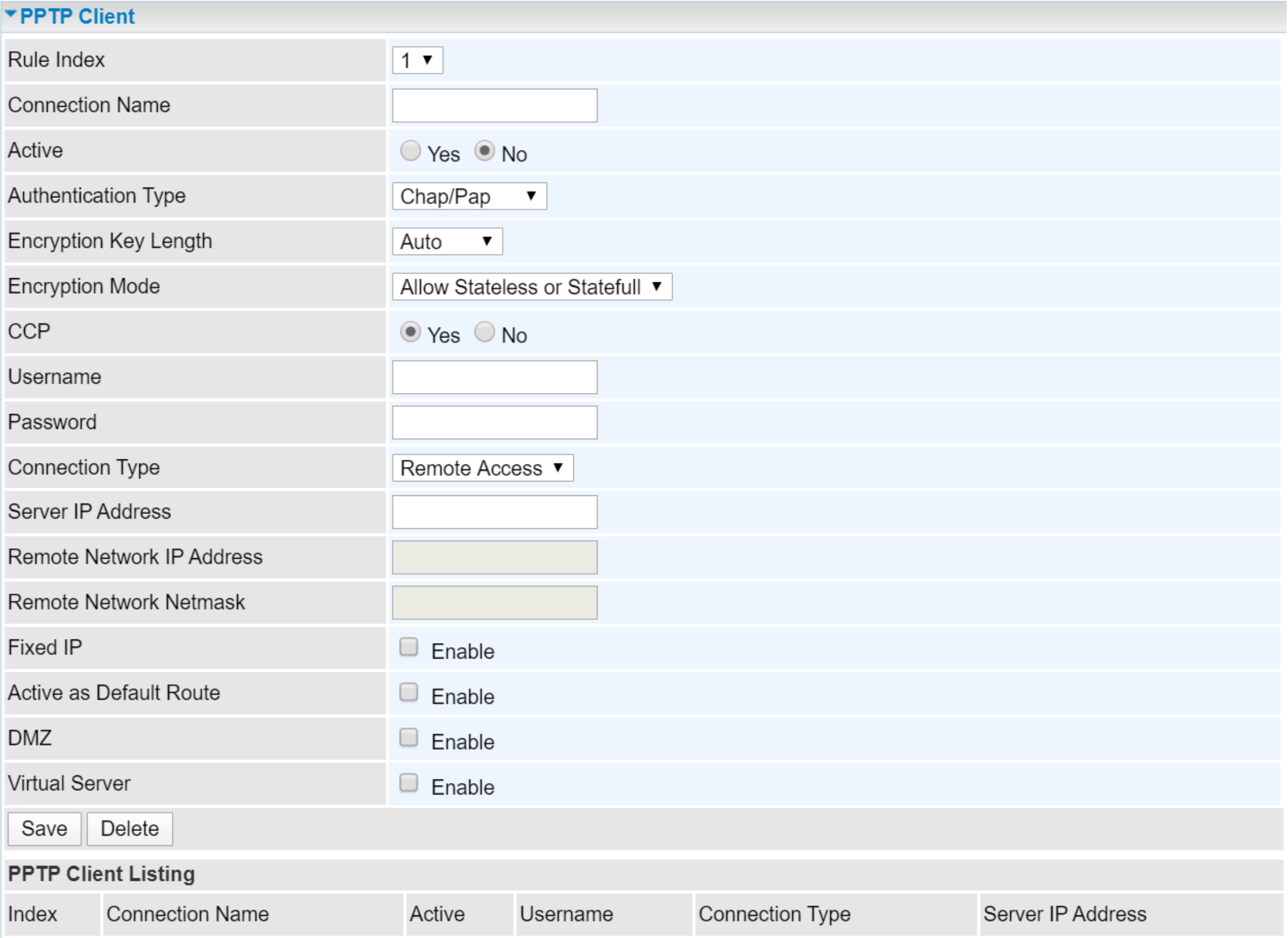
Remote Network Netmask: Enter the Netmask of the remote LAN network.

Click **Save** to apply settings.

PPTP Client

Establish a PPTP tunnel over Internet to connect with a PPTP server.

A total of 4 PPTP Client sessions can be created.



▾PPTP Client

Rule Index	1 ▾
Connection Name	
Active	○ Yes ● No
Authentication Type	Chap/Pap ▾
Encryption Key Length	Auto ▾
Encryption Mode	Allow Stateless or Statefull ▾
CCP	● Yes ○ No
Username	
Password	
Connection Type	Remote Access ▾
Server IP Address	
Remote Network IP Address	
Remote Network Netmask	
Fixed IP	□ Enable
Active as Default Route	□ Enable
DMZ	□ Enable
Virtual Server	□ Enable

PPTP Client Listing

Index	Connection Name	Active	Username	Connection Type	Server IP Address

Rule Index: The indication of the rule number. The maximum entry is up to 4.

Connection Name: Enter a description for this connection/profile.

Active: **Yes** to activate the account. PPTP server is waiting for the client to connect to this account.

Authentication Type: Pick an authentication type from the drop-down list. When using PAP, the password is sent unencrypted, whilst CHAP encrypts the password before sending, and also allows for challenges at different periods to ensure that an intruder has not replaced the client. When passed the authentication with MS-CHAPv2, the MPPE encryption is supported.

Encryption Key Length: Auto, data encryption and key length, with 40-bit or 128-bit, is automatically negotiated when establish a connection. 128-bit keys provide strong stronger encryption than 40-bit keys.

Encryption Mode: The encryption key will be changed every 256 packets with Stateful mode. With Stateless mode, the key will be changed in each packet.

CCP (Compression Control Protocol): Enable to compress data to save bandwidth and increase data transfer speed.

Username / Password: Enter the username / password provided by the PPTP server/host.

Connection Type: Select Remote Access for single user, Select LAN to LAN for remote gateway.

Server IP Address: Enter the WAN IP address of the PPTP server.

Remote Network IP Address: Enter the subnet IP of the server/host LAN network.

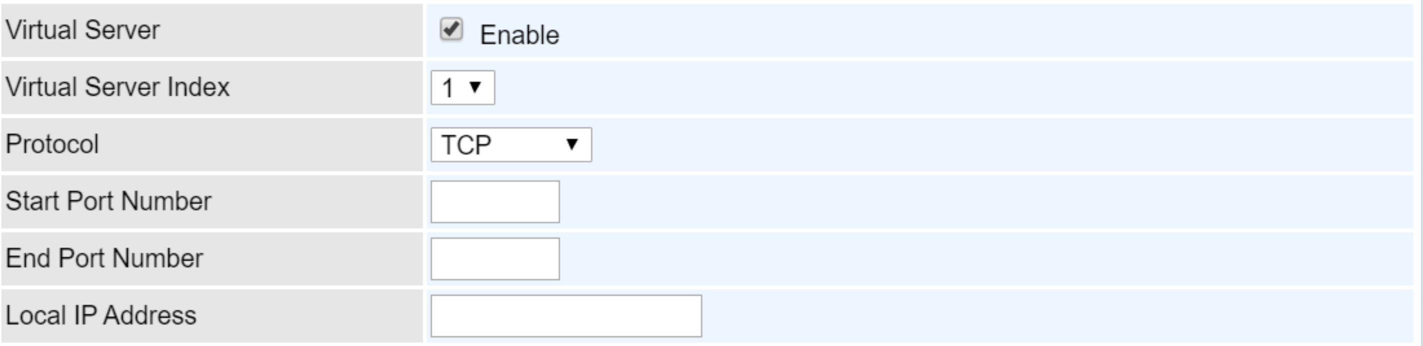
Remote Network Netmask: Enter the Netmask of the server/host LAN network.

Fixed IP: Specific and reserve a LAN IP address from the remote PPTP server. Click **Enable** then enter the request IP address.

Active as Default Route: Enabled to let the tunnel to be the default route for traffic, under this circumstance, all packets will be forwarded to this tunnel and routed to the next hop.

DMZ: Specific an internal DMZ host to add an additional layer of protection to the network. All received incoming packets will first go through the Virtual Server list, if no service redirection required, then packets can get forwarded to the DMZ host. Click **Enable** then enter the DMZ IP address.

Virtual Server: Click **Enable** to enable redirection of Internet packets.



Virtual Server	☑ Enable
Virtual Server Index	1 ▼
Protocol	TCP ▼
Start Port Number	
End Port Number	
Local IP Address	

Virtual Server Index: Index marking for each rule up to maximum of 4.

Protocol: Choose the application protocol.

Start / End Port Number: Enter the start / end port number of the local application (service).

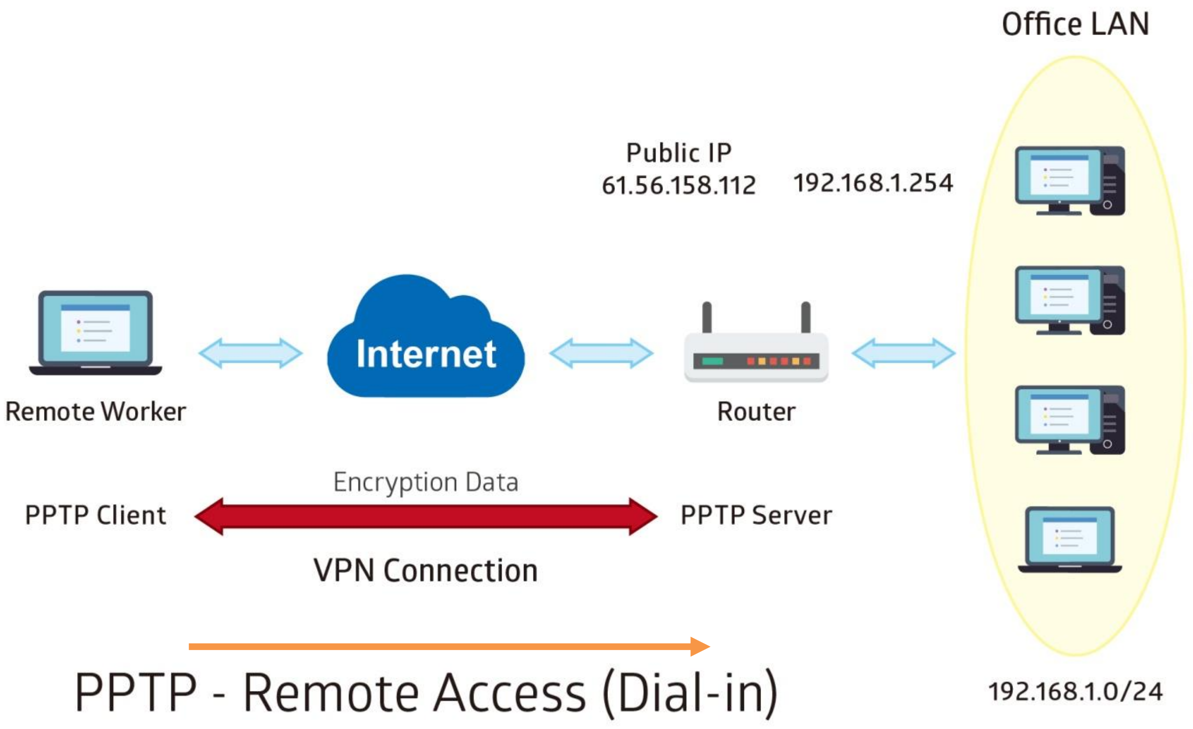
(Example: Start / End: 1000 or Start: 1000, End: 2000).

The starting greater than zero (0) and the ending port must be the same or larger than the starting port.

Local IP Address: Enter the local IP address of the default start/end port of the application / service.

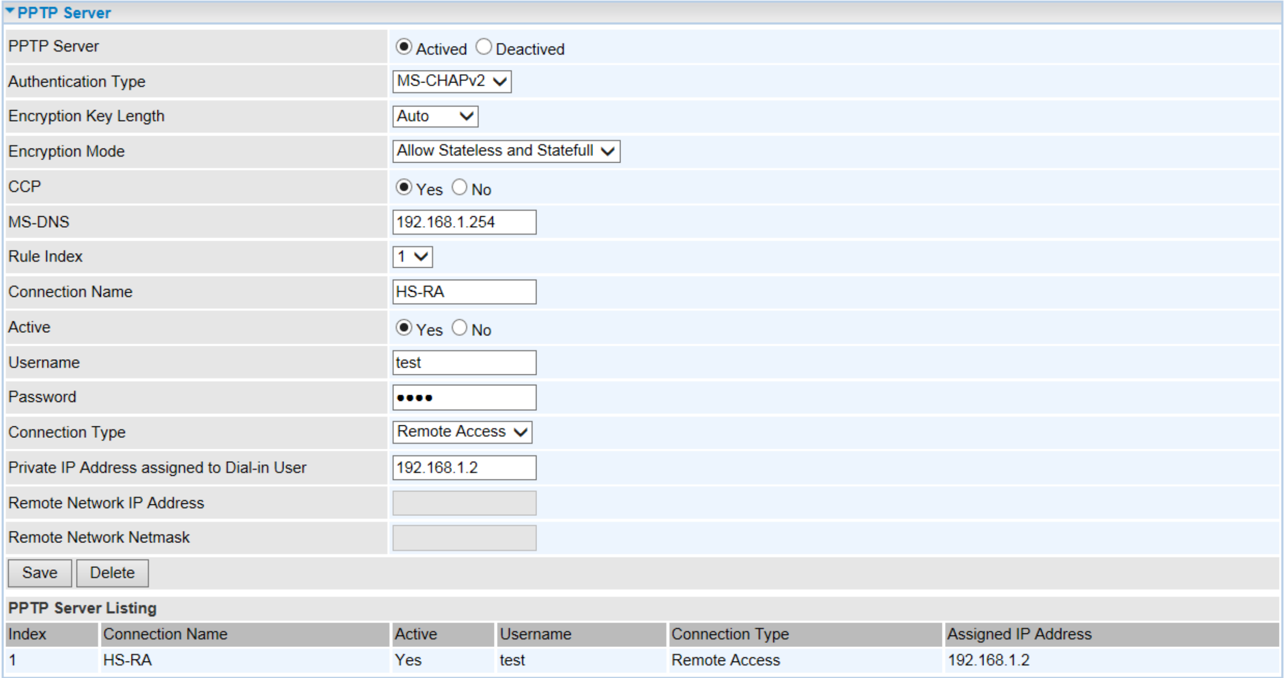
Click **Save** to apply settings.

Example: PPTP – Remote Employee Dial-in to BEC 4700A/AZ



The input IP address 192.168.1.2 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.

Configuration Settings		Description
Connection Name	HS-RA	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential created from the device to a PPTP client to dial-in to the network.
Password	test	
Connection Type	Remote Access	Remote access for a dial-in
Assigned IP	192.168.1.2	Local IP assigned to the dial-in client



▾PPTP Server

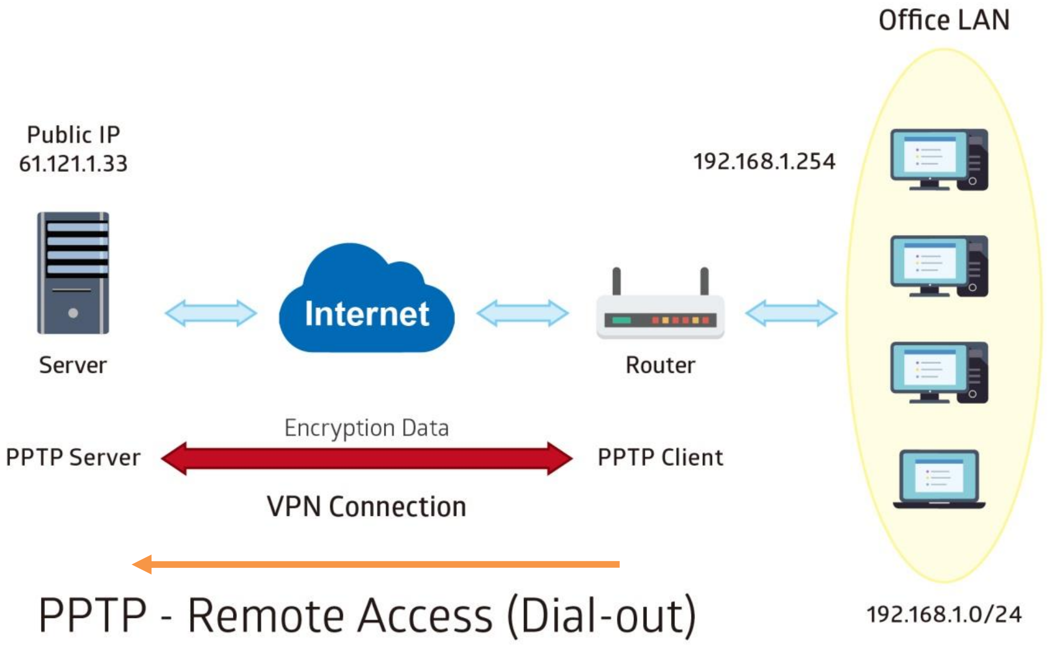
PPTP Server	● Actived ○ Deactived
Authentication Type	MS-CHAPv2
Encryption Key Length	Auto
Encryption Mode	Allow Stateless and Statefull
CCP	● Yes ○ No
MS-DNS	192.168.1.254
Rule Index	1
Connection Name	HS-RA
Active	● Yes ○ No
Username	test
Password	••••
Connection Type	Remote Access
Private IP Address assigned to Dial-in User	192.168.1.2
Remote Network IP Address	
Remote Network Netmask	

PPTP Server Listing

Index	Connection Name	Active	Username	Connection Type	Assigned IP Address
1	HS-RA	Yes	test	Remote Access	192.168.1.2

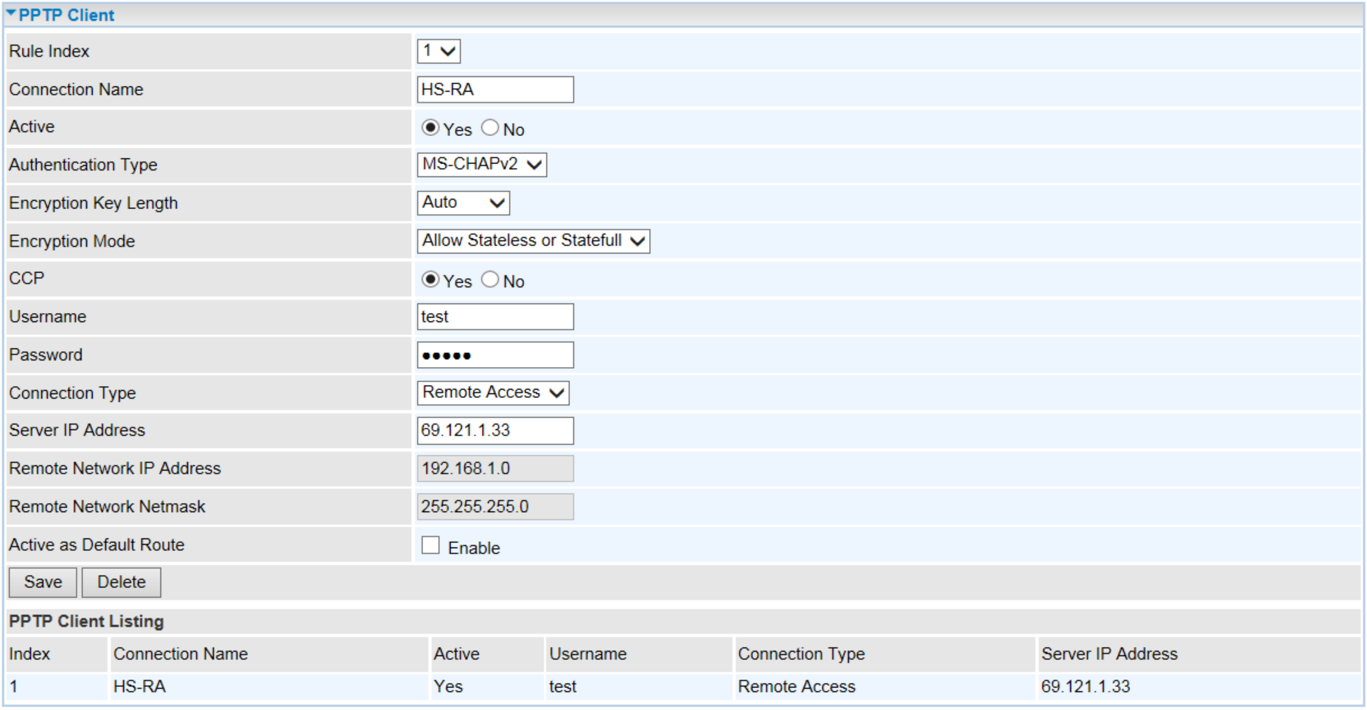
Example: PPTP – Remote Employee Dial-out to BEC 4700A/AZ

A company's office establishes a PPTP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.



PPTP Server WAN IP address is 61.121.1.33 of the Headquarter office.

Configuration Settings		Description
Connection Name	HS-RA	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential assigned from the PPTP server for PPP client to dial-in to its network.
Password	test	
Connection Type	Remote Access	Remote access for a dial-in
Server IP	61.121.1.33	VPN server WAN IP address



PPTP Client

Rule Index	1
Connection Name	HS-RA
Active	● Yes ○ No
Authentication Type	MS-CHAPv2
Encryption Key Length	Auto
Encryption Mode	Allow Stateless or Statefull
CCP	● Yes ○ No
Username	test
Password	●●●●●
Connection Type	Remote Access
Server IP Address	69.121.1.33
Remote Network IP Address	192.168.1.0
Remote Network Netmask	255.255.255.0
Active as Default Route	□ Enable

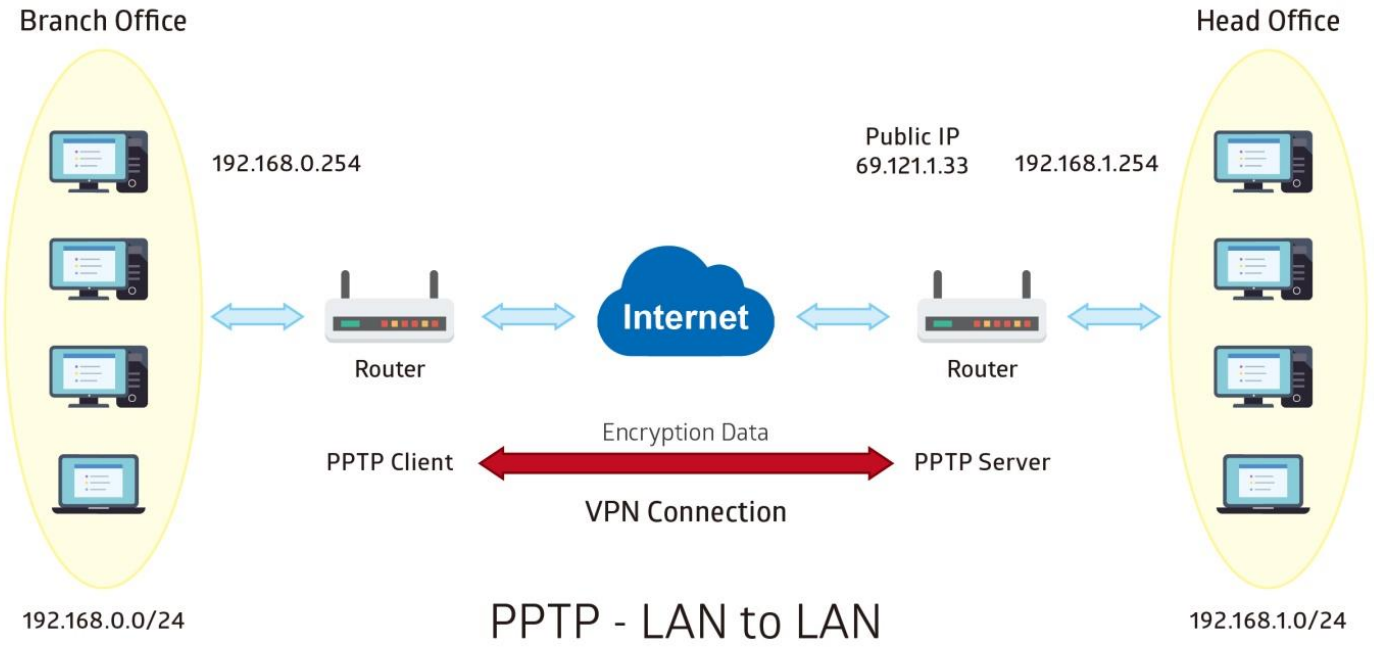
PPTP Client Listing

Index	Connection Name	Active	Username	Connection Type	Server IP Address
1	HS-RA	Yes	test	Remote Access	69.121.1.33

Example: PPTP – Network (LAN) to Network (LAN) Connection

The branch office establishes a PPTP VPN tunnel with Headquarter office to connect two private networks over the Internet. The routers are installed in the Headquarter office and branch offices accordingly.

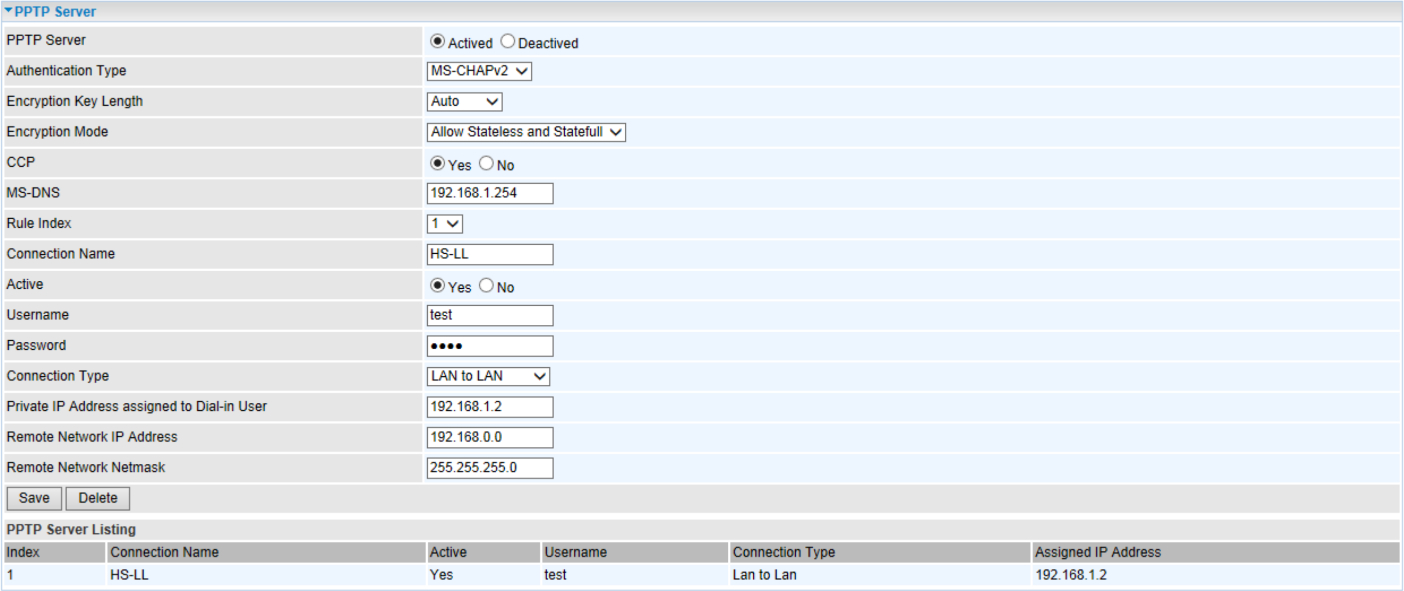
NOTE: Both office LAN networks must be in **different subnets** with the LAN-LAN application.



Configuring PPTP Server in the Headquarter office

The IP address 192.168.1.2 will be assigned to the router located in the branch office. Please make sure this IP is not used in the Headquarter office LAN.

Configuration Settings		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential created for a PPTP client to dial-in to its local network.
Password	test	
Connection Type	LAN to LAN	LAN to LAN connection
Assigned IP	192.168.1.2	Local IP assigned to the dial-in client
Remote Network IP	129.168.0.0	Remote, Branch office, LAN network IP address and Netmask
Remote Network Netmask	255.255.255.0	



PPTP Server

PPTP Server	● Actived ○ Deactived
Authentication Type	MS-CHAPv2
Encryption Key Length	Auto
Encryption Mode	Allow Stateless and Statefull
CCP	● Yes ○ No
MS-DNS	192.168.1.254
Rule Index	1
Connection Name	HS-LL
Active	● Yes ○ No
Username	test
Password	••••
Connection Type	LAN to LAN
Private IP Address assigned to Dial-in User	192.168.1.2
Remote Network IP Address	192.168.0.0
Remote Network Netmask	255.255.255.0

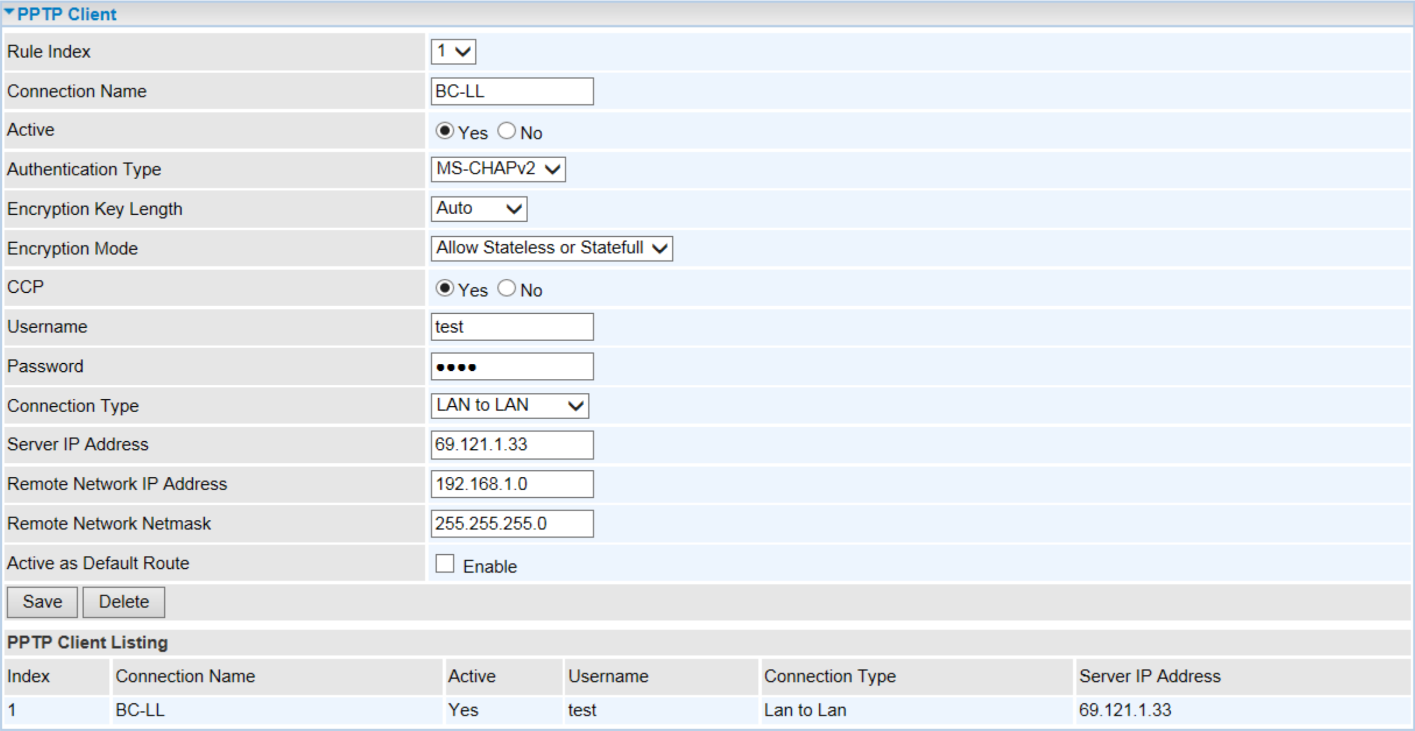
PPTP Server Listing

Index	Connection Name	Active	Username	Connection Type	Assigned IP Address
1	HS-LL	Yes	test	Lan to Lan	192.168.1.2

Configuring PPTP Client in the Branch office

The IP address 69.1.121.33 is the Public IP address of the router located in Headquarter office.

Configuration Settings		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Authentication Type	MS-CHAPv2	Authentication type
Username	test	Credential assigned from the Headquarter Server to dial-in.
Password	test	
Connection Type	LAN to LAN	LAN to LAN connection
Server IP	69.121.1.33	Headquarter Serve WAN IP address
Remote Network IP	129.168.1.0	Remote, Headquarter office, LAN network IP address and Netmask
Remote Network Netmask	255.255.255.0	



PPTP Client

Rule Index	1
Connection Name	BC-LL
Active	● Yes ○ No
Authentication Type	MS-CHAPv2
Encryption Key Length	Auto
Encryption Mode	Allow Stateless or Statefull
CCP	● Yes ○ No
Username	test
Password	●●●●
Connection Type	LAN to LAN
Server IP Address	69.121.1.33
Remote Network IP Address	192.168.1.0
Remote Network Netmask	255.255.255.0
Active as Default Route	□ Enable

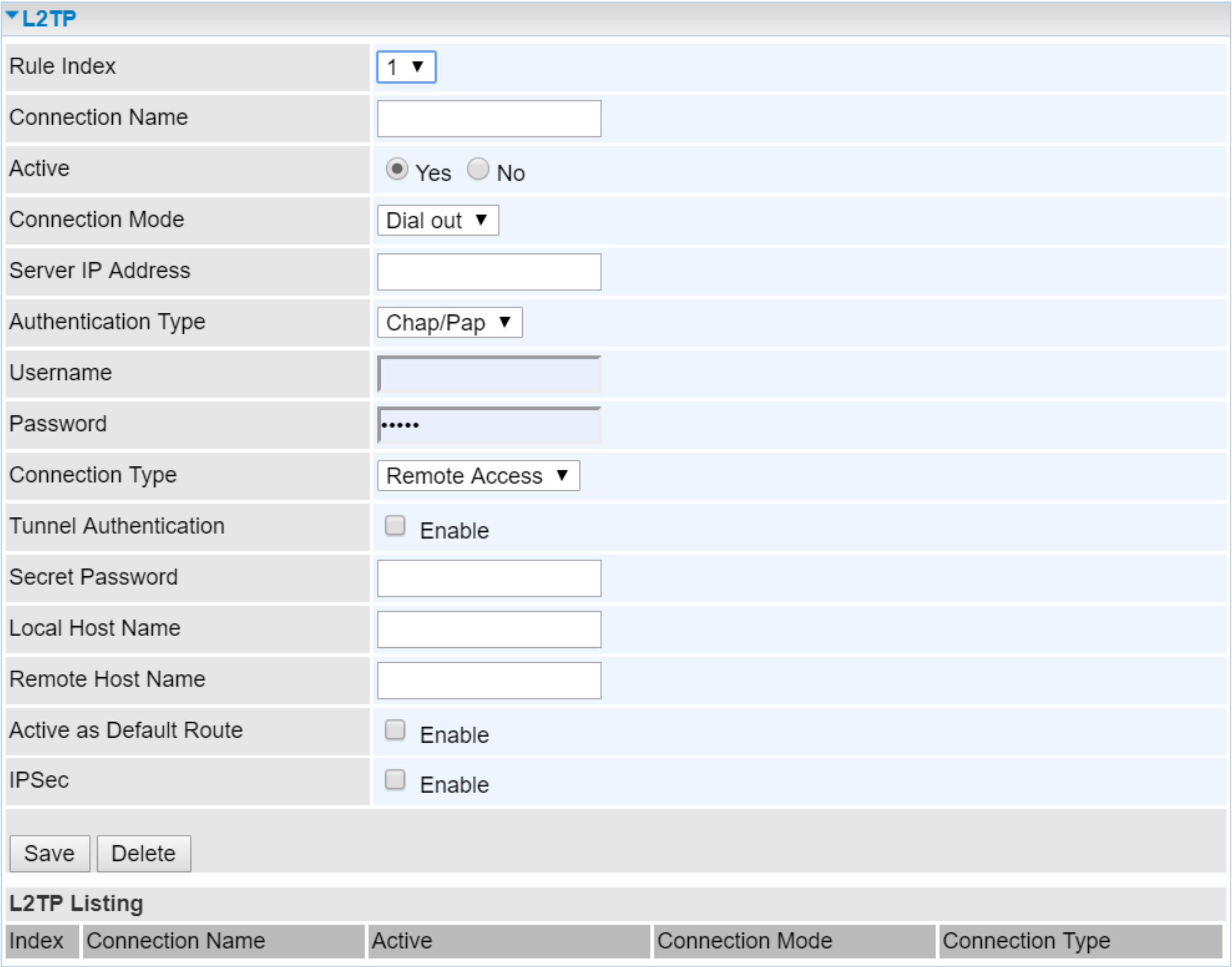
PPTP Client Listing

Index	Connection Name	Active	Username	Connection Type	Server IP Address
1	BC-LL	Yes	test	Lan to Lan	69.121.1.33

L2TP

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

NOTE: 4 sessions for dial-in connections and 4 sessions for dial-out connections



▾L2TP

Rule Index	1 ▼
Connection Name	
Active	● Yes ○ No
Connection Mode	Dial out ▼
Server IP Address	
Authentication Type	Chap/Pap ▼
Username	
Password	•••••
Connection Type	Remote Access ▼
Tunnel Authentication	□ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	□ Enable
IPSec	□ Enable

L2TP Listing

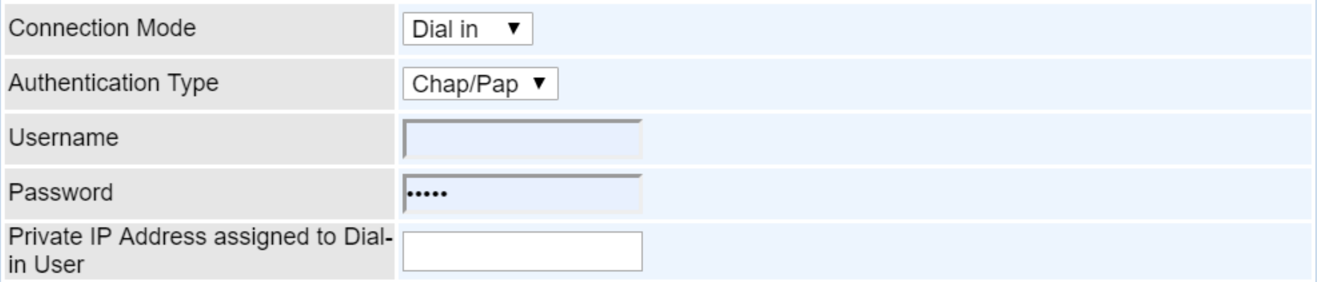
Index	Connection Name	Active	Connection Mode	Connection Type

Rule Index: The indication of the rule number. The maximum entry is up to 8 (4 dial-in and 4 dial-out profiles).

Connection Name: Enter a description for this connection/profile.

Active: To enable or disable this profile.

Connection Mode (Dial in)



Connection Mode	Dial in ▼
Authentication Type	Chap/Pap ▼
Username	
Password	•••••
Private IP Address assigned to Dial-in User	

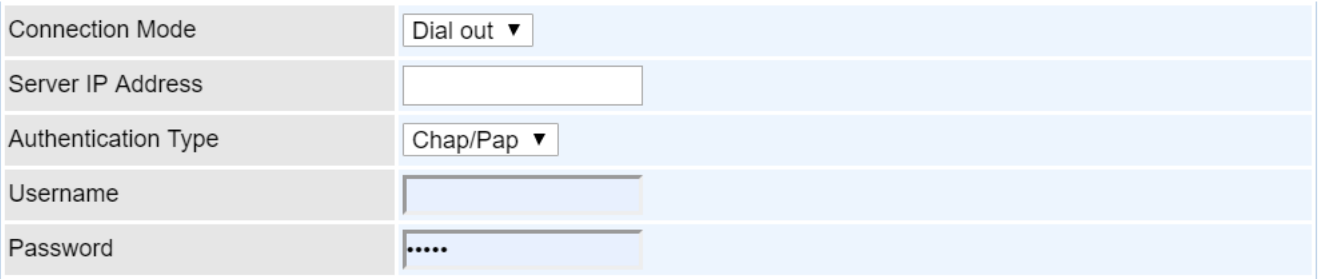
Connection Mode: Select Dial In to operate as a L2TP server.

Authentication Type: Default in Chap/Pap (CHAP, Challenge Handshake Authentication Protocol. PAP, Password Authentication Protocol). If you want the router to determine the authentication type to use, or else manually specify PAP if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server).

Username / Password (Server/Host): Enter the username / password for this profile.

Private IP Address Assigned to Dial-in User: The private IP to be assigned to dial-in user by L2TP server. The IP should be in the same subnet as local LAN and should not be occupied.

Connection Mode (Dial out)



Connection Mode	Dial out ▼
Server IP Address	
Authentication Type	Chap/Pap ▼
Username	
Password	•••••

Connection Mode: Choose Dial Out if you want your router to operate as a client (connecting to a remote L2TP Server, e.g., your office server).

Server IP Address: Enter the IP address of your VPN Server.

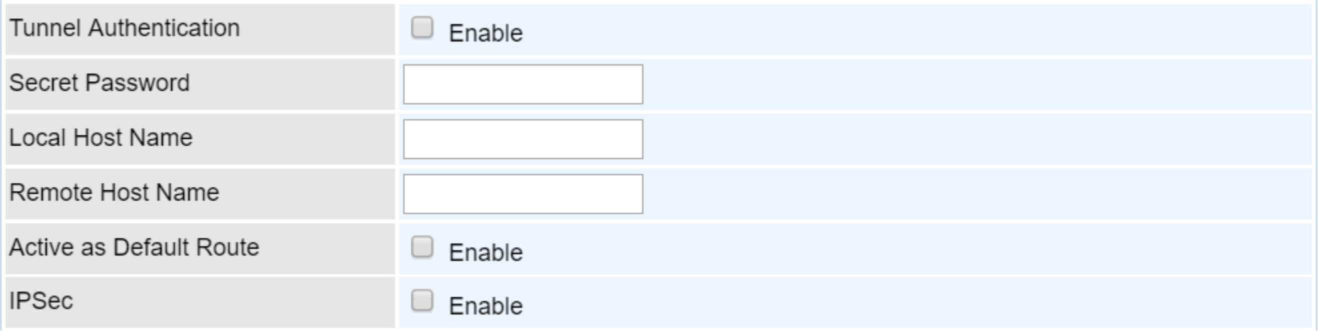
Authentication Type: Default is Chap/Pap (CHAP, Challenge Handshake Authentication Protocol. PAP, Password Authentication Protocol). If you want the router to determine the authentication type to use, or else manually specify PAP if you know which type the server is using (when acting as a client), or else the authentication type you want clients connecting to you to use (when acting as a server).

Username / Password (Client): Enter the username / password provide by the Server/Host.

Connection Type

- **Remote Access:** From a single user.
- **LAN to LAN:** Enter the peer network information, such as network address and Netmask.

Tunnel Authentication and Active



Tunnel Authentication	□ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	□ Enable
IPSec	□ Enable

Tunnel Authentication: This enables router to authenticate both the L2TP remote and L2TP host. This is only valid when L2TP remote supports this feature.

Secret Password: The secure password length should be 16 characters which may include numbers and characters.

Local Host Name: Enter hostname of Local VPN device that is connected / established a VPN tunnel.

Remote Host Name: Enter hostname of remote VPN device. It is a tunnel identifier from the Remote VPN device matches with the Remote hostname provided. If remote hostname matches, tunnel will be connected; otherwise, it will be dropped.

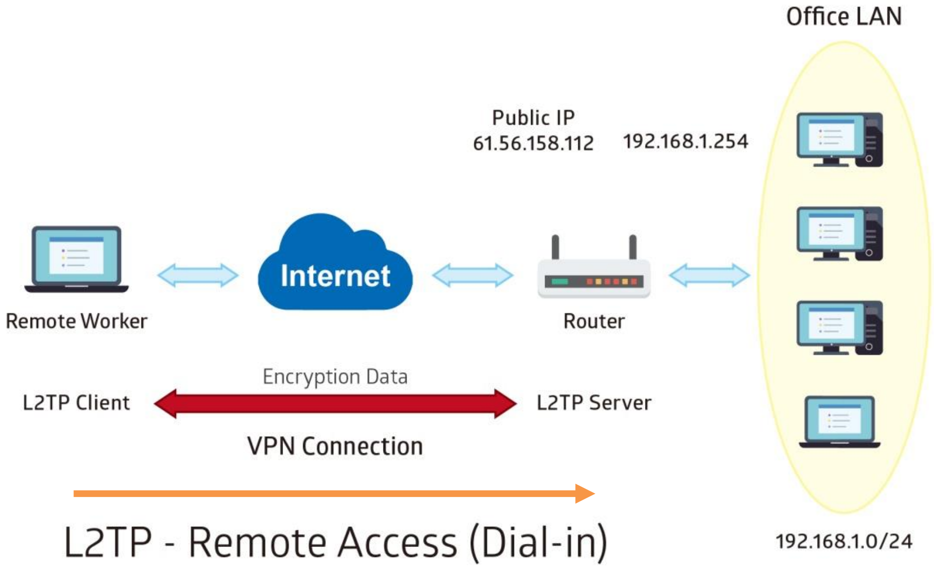
Active as Default Route: Enabled to let the tunnel to be the default route for traffic, under this circumstance, all packets will be forwarded to this tunnel and routed to the next hop.

IPSec: Click the checkbox to establish a L2TP tunnel inside of the IPSec tunnel.

Click **Save** to apply settings.

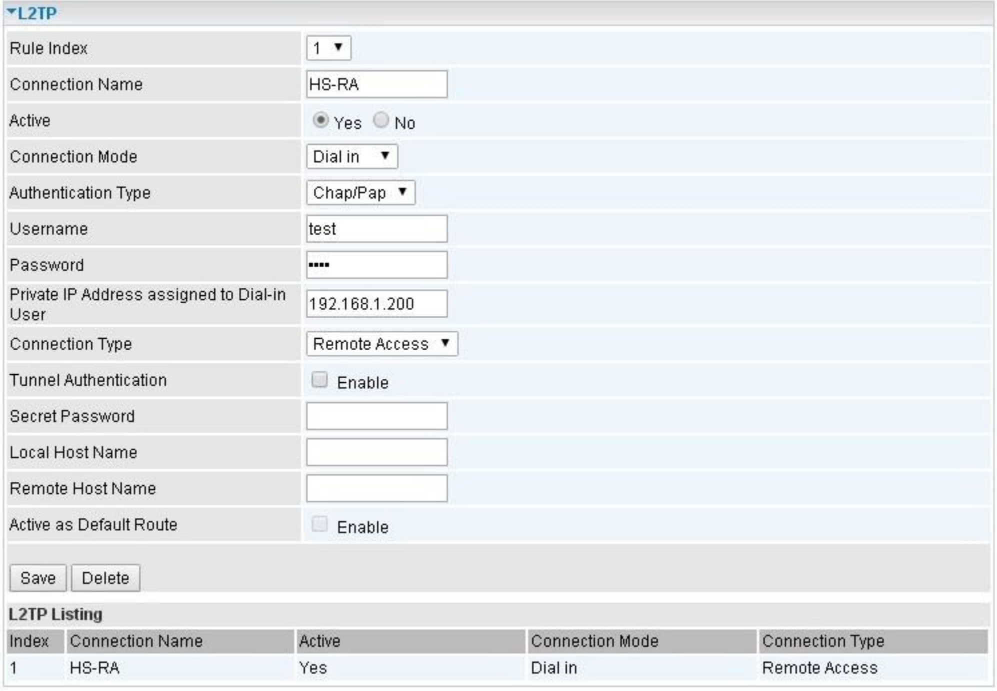
Example: L2TP VPN – Remote Employee Dial-in to BEC 4700A/AZ

A remote worker establishes a L2TP VPN connection with the Headquarter office using Microsoft's VPN Adapter The router is installed in the Headquarter office, connected to a couple of PCs and Servers.



The input IP address 192.168.1.200 will be assigned to the remote worker. Please make sure this IP is not used in the Office LAN.

Configuration Settings		Description
Connection Name	HS-RA	Assigned name to this tunnel/profile
Connection Mode	Dial in	Operate as L2TP server
Authentication Type	Chap/Pap	Authentication type
Username	test	Credential from the device for remote client to dial-in to the network.
Password	test	
Assigned IP	192.168.1.200	An IP assigned to the dial in client
Connection Type	Remote Access	Remote access for dial in


▾L2TP

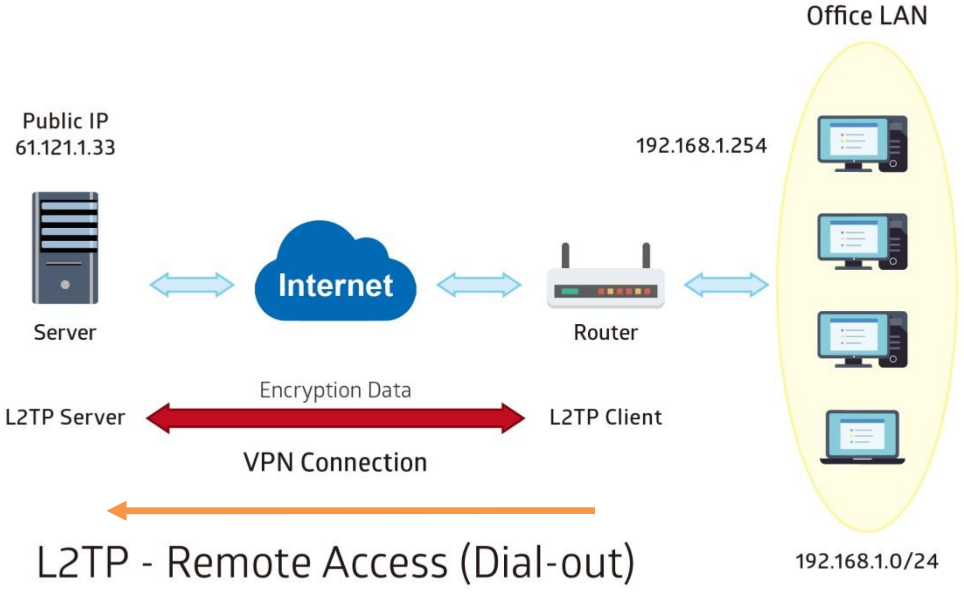
Rule Index	1 ▼
Connection Name	HS-RA
Active	● Yes ○ No
Connection Mode	Dial in ▼
Authentication Type	Chap/Pap ▼
Username	test
Password	••••
Private IP Address assigned to Dial-in User	192.168.1.200
Connection Type	Remote Access ▼
Tunnel Authentication	□ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	□ Enable

L2TP Listing

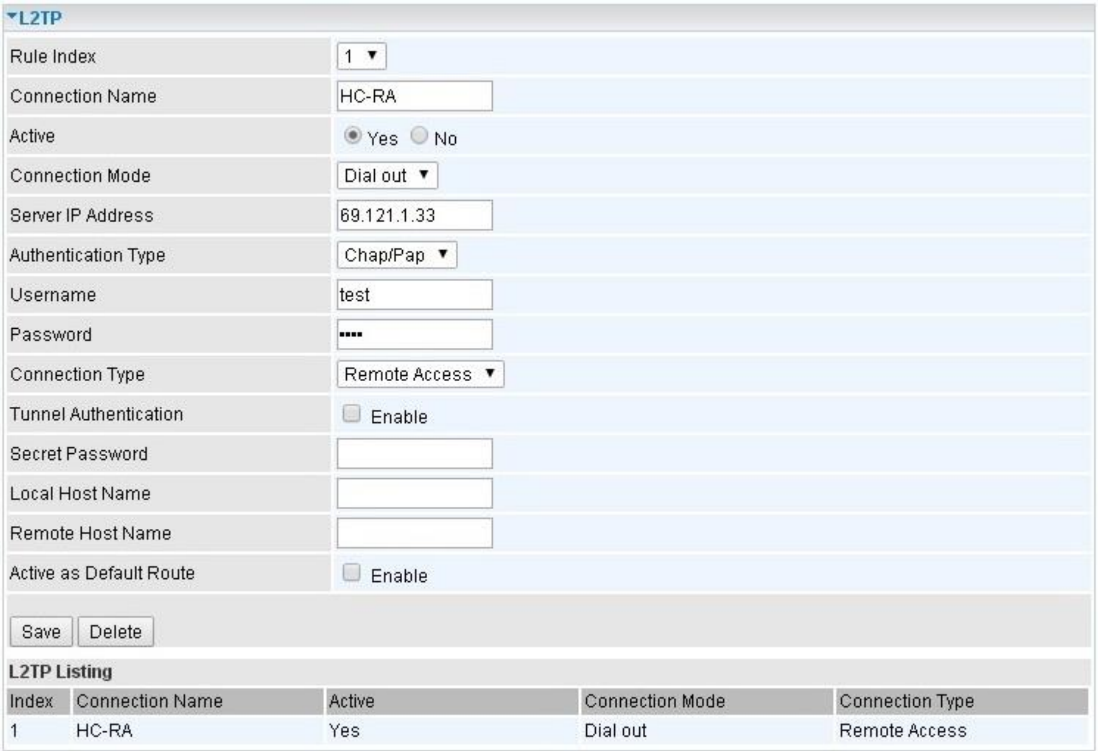
Index	Connection Name	Active	Connection Mode	Connection Type
1	HS-RA	Yes	Dial in	Remote Access

Example: L2TP VPN – BEC 4700A/AZ Dial-out to a Server

A company's office establishes a L2TP VPN connection with a file server located at a separate location. The router is installed in the office, connected to a couple of PCs and Servers.



Item		Description
Connection Name	HC-RA	Assigned name to this tunnel/profile
Connection Mode	Dial out	Operate as L2TP client
Server IP	69.121.1.33	VPN server WAN IP address
Authentication Type	Chap/Pap	Authentication type
Username	test	Credential from the VPN Server for remote clients to dial-in to the network.
Password	test	
Connection Type	Remote Access	Remote access for dial out



▾L2TP

Rule Index	1 ▾
Connection Name	HC-RA
Active	● Yes ○ No
Connection Mode	Dial out ▾
Server IP Address	69.121.1.33
Authentication Type	Chap/Pap ▾
Username	test
Password	••••
Connection Type	Remote Access ▾
Tunnel Authentication	□ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	□ Enable

Save Delete

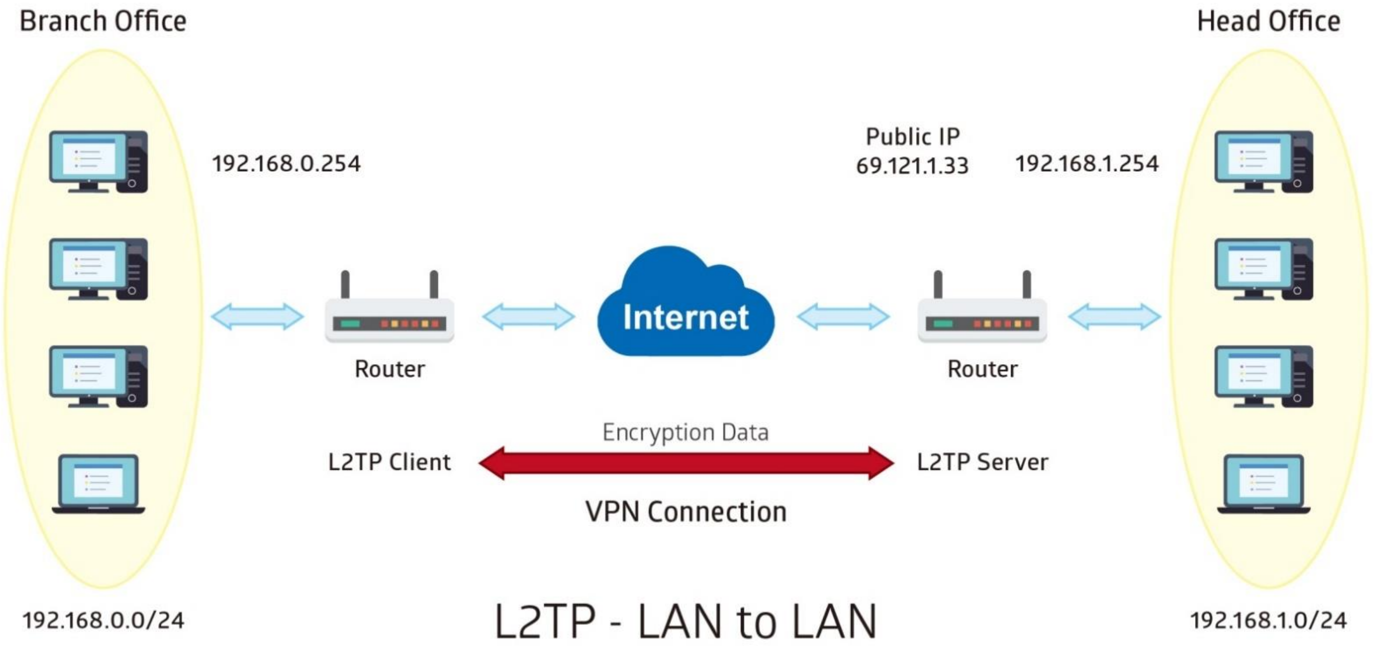
L2TP Listing

Index	Connection Name	Active	Connection Mode	Connection Type
1	HC-RA	Yes	Dial out	Remote Access

Example: L2TP VPN – Network (LAN) to Network (LAN) Connection

The branch office establishes a L2TP VPN tunnel with Headquarter office to connect two private networks over the Internet. The routers are installed in the Headquarter office and branch office accordingly.

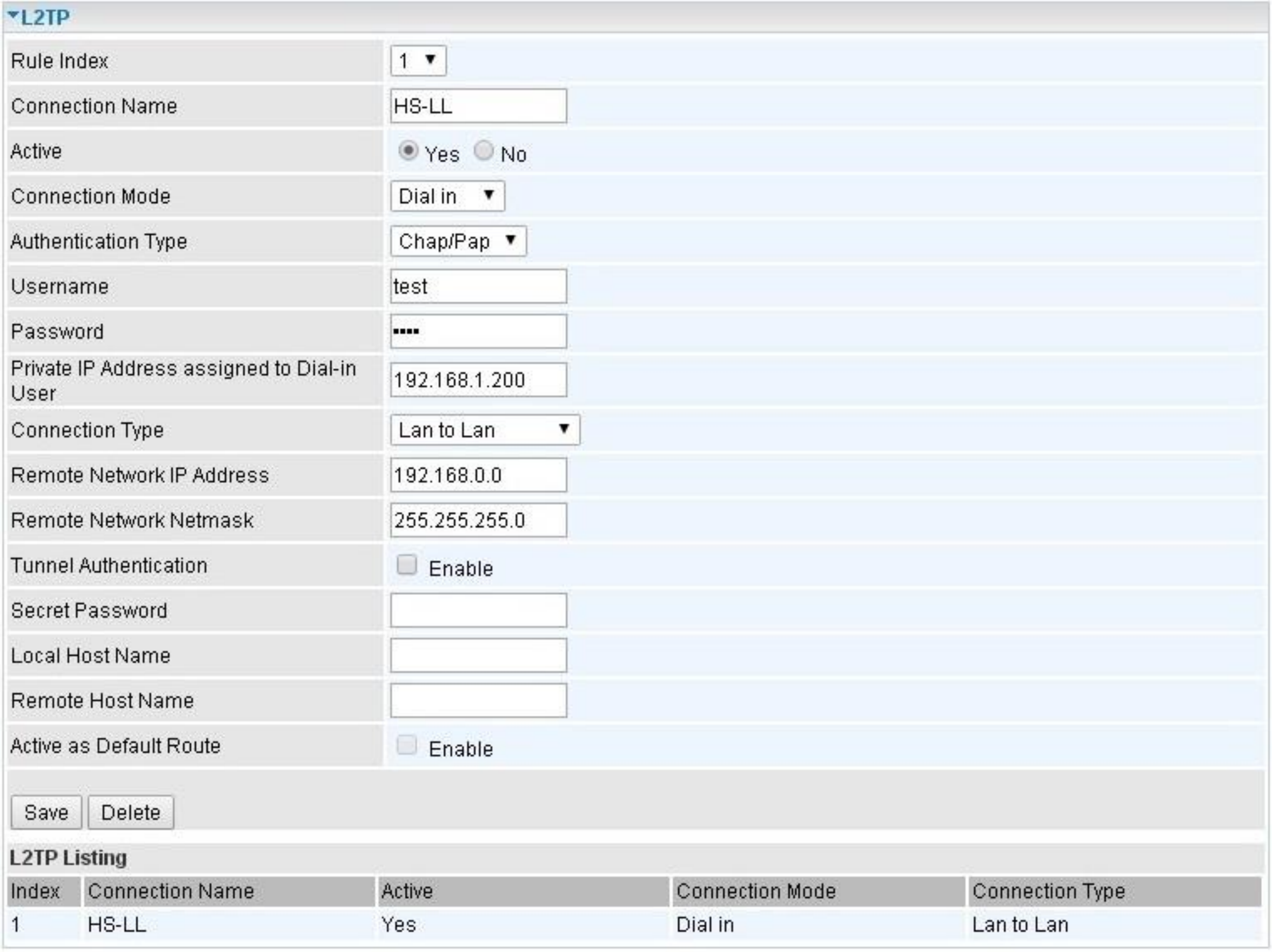
NOTE: Both office LAN networks must be in different subnets with the LAN-LAN application.



Configuring L2TP VPN Dial-in in the Headquarter office

The IP address 192.168.1.200 will be assigned to the router located in the branch office.

Item		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Connection Mode	Dial in	Operate as L2TP server
Authentication Type	Chap/Pap	Authentication type
Username	Test	Credential for a PPTP client to dial-in to the network.
Password	Test	
Assigned IP	192.168.1.200	An IP assigned to the dial in client
Connection Type	LAN to LAN	LAN to LAN for dial in
Remote Network IP	129.168.0.0	Remote, Branch office, LAN network IP address and Netmask
Remote Network Netmask	255.255.255.0	



▾L2TP

Rule Index	1 ▾
Connection Name	HS-LL
Active	● Yes ○ No
Connection Mode	Dial in ▾
Authentication Type	Chap/Pap ▾
Username	test
Password	••••
Private IP Address assigned to Dial-in User	192.168.1.200
Connection Type	Lan to Lan ▾
Remote Network IP Address	192.168.0.0
Remote Network Netmask	255.255.255.0
Tunnel Authentication	□ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	□ Enable

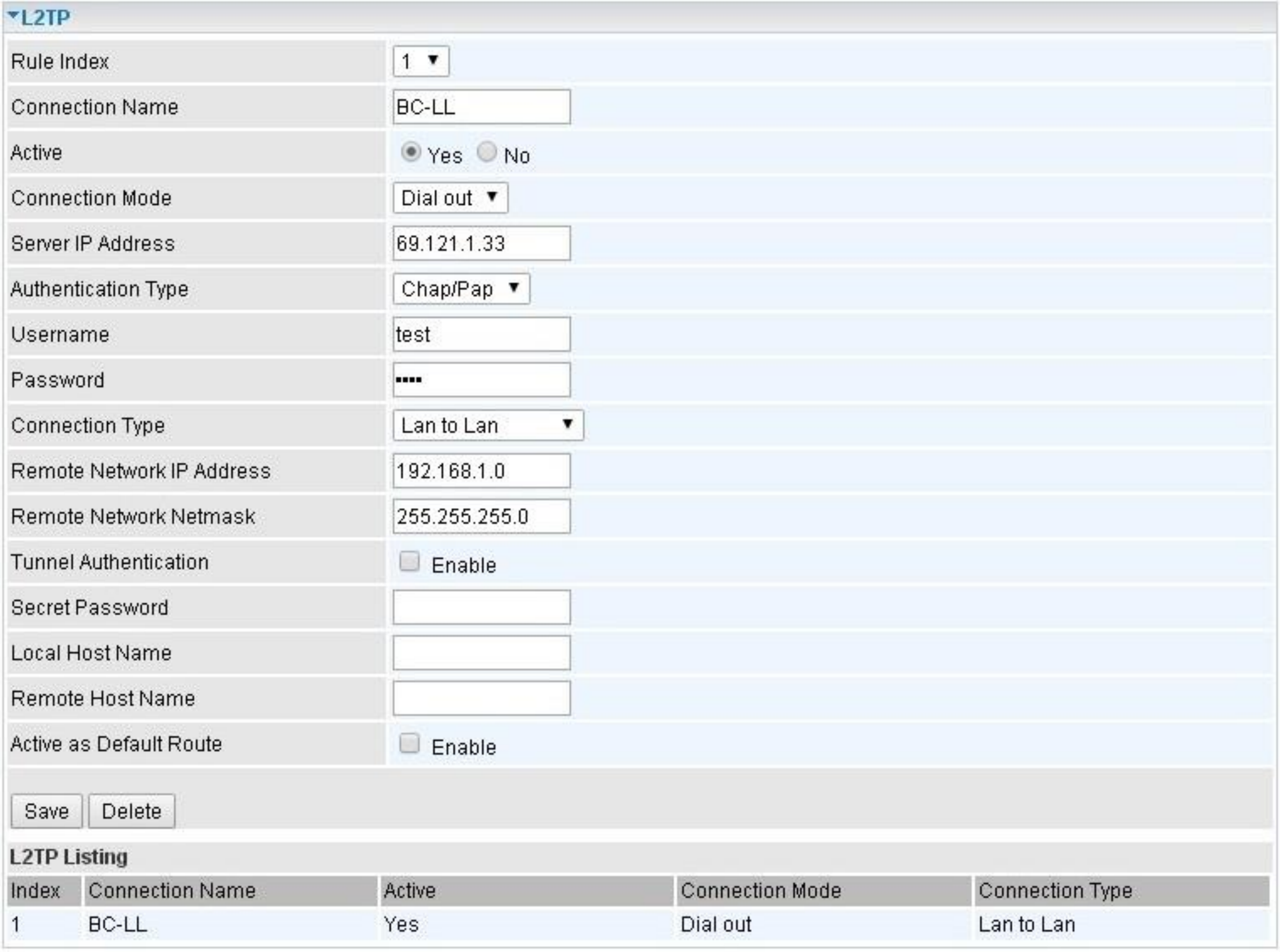
L2TP Listing

Index	Connection Name	Active	Connection Mode	Connection Type
1	HS-LL	Yes	Dial in	Lan to Lan

Configuring L2TP VPN Dial-out in the Branch office

The IP address 69.1.121.33 is the Public IP address of the router located in Headquarter office.

Item		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Connection Mode	Dial out	Operate as L2TP client
Server IP	69.121.1.33	Dialed server IP
Authentication Type	Chap/Pap	Authentication type
Username	test	Credential from the PPTP server to dial-in to the network
Password	test	
Connection Type	LAN to LAN	LAN to LAN for dial out
Remote Network IP	129.168.1.0	Remote, Headquarter office, LAN network IP address and Netmask
Remote Network Netmask	255.255.255.0	



▾L2TP

Rule Index	1 ▾
Connection Name	BC-LL
Active	● Yes ○ No
Connection Mode	Dial out ▾
Server IP Address	69.121.1.33
Authentication Type	Chap/Pap ▾
Username	test
Password	••••
Connection Type	Lan to Lan ▾
Remote Network IP Address	192.168.1.0
Remote Network Netmask	255.255.255.0
Tunnel Authentication	□ Enable
Secret Password	
Local Host Name	
Remote Host Name	
Active as Default Route	□ Enable

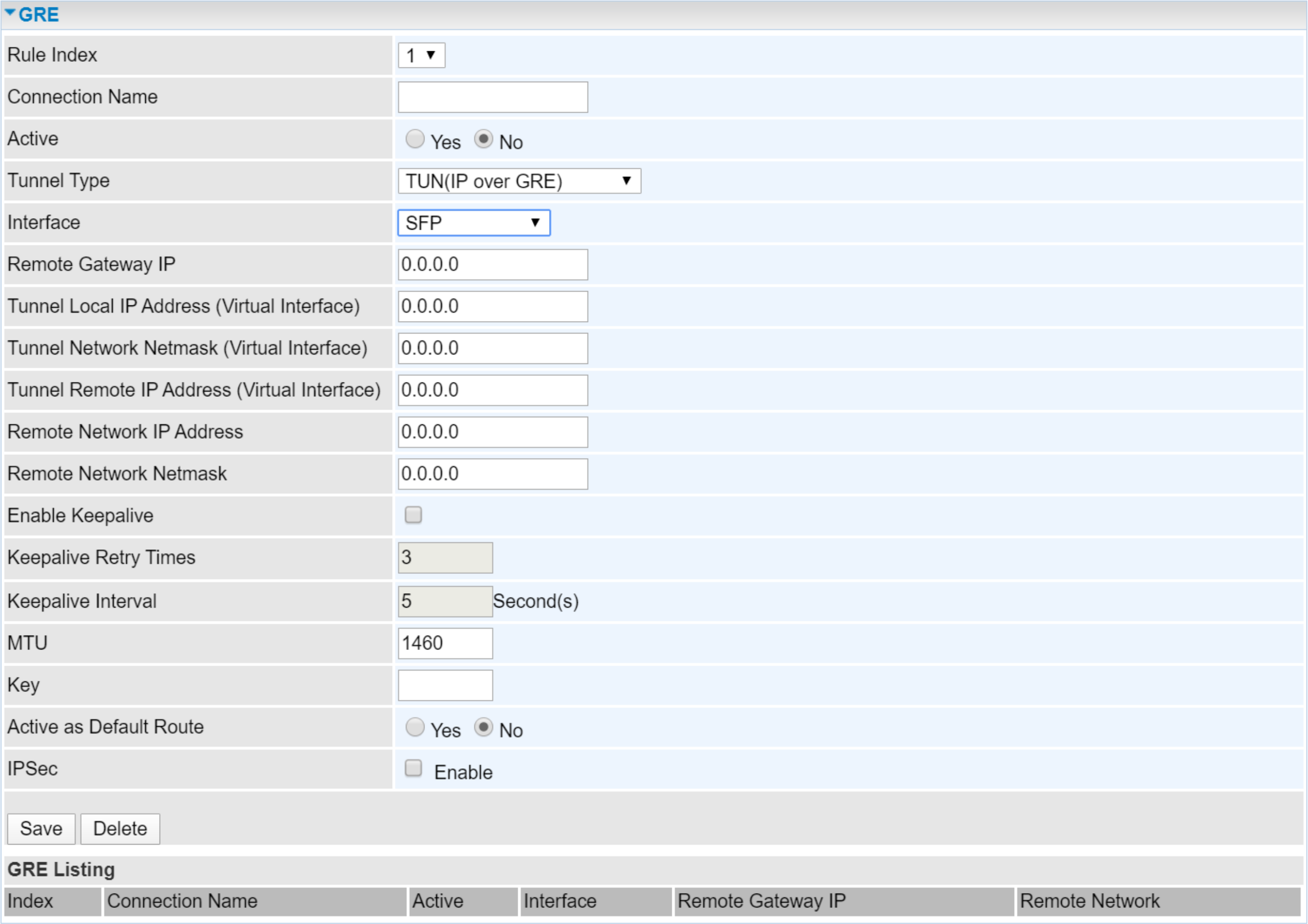
L2TP Listing

Index	Connection Name	Active	Connection Mode	Connection Type
1	BC-LL	Yes	Dial out	Lan to Lan

GRE Tunnel

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocol packets inside virtual point-to-point links over an IP network.

NOTE: Up to 8 GRE tunnels supported.



▾GRE

Rule Index	1 ▾
Connection Name	
Active	○ Yes ● No
Tunnel Type	TUN(IP over GRE) ▾
Interface	SFP ▾
Remote Gateway IP	0.0.0.0
Tunnel Local IP Address (Virtual Interface)	0.0.0.0
Tunnel Network Netmask (Virtual Interface)	0.0.0.0
Tunnel Remote IP Address (Virtual Interface)	0.0.0.0
Remote Network IP Address	0.0.0.0
Remote Network Netmask	0.0.0.0
Enable Keepalive	□
Keepalive Retry Times	3
Keepalive Interval	5 Second(s)
MTU	1460
Key	
Active as Default Route	○ Yes ● No
IPSec	□ Enable

GRE Listing

Index	Connection Name	Active	Interface	Remote Gateway IP	Remote Network

Rule Index: The numeric rule indicator for GRE. The maximum entry is up to 8.

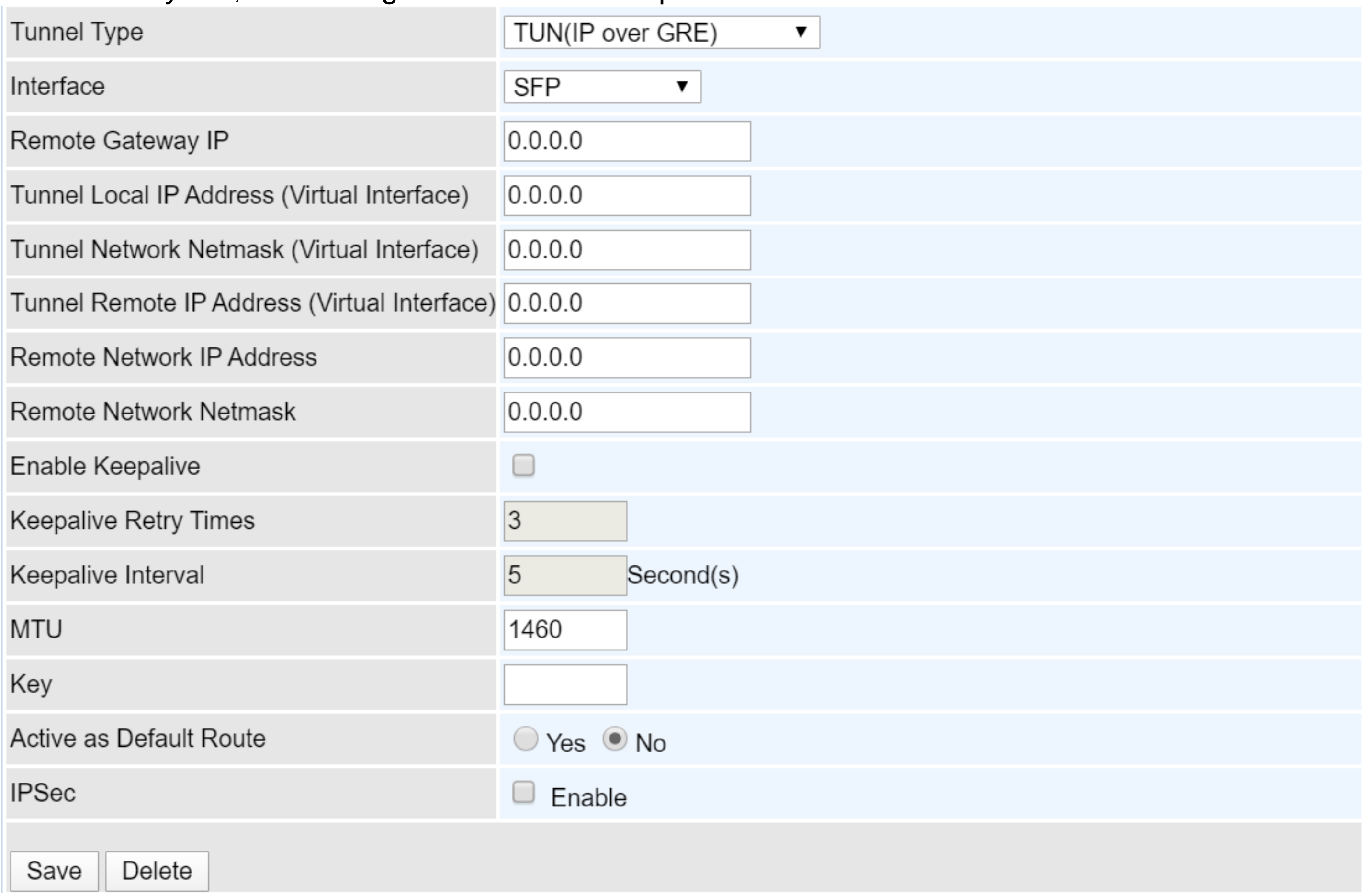
Connection Name: Enter a description for this connection/profile.

Active: Yes to activate this GRE profile.

Tunnel Type: Two types of tunnels, **TUN (IP over GRE)** and **TAP (Ethernet over GRE)**.

TUN (IP over GRE)

TUN is in layer 3, networking level which routes packets via GRE tunnels.



Tunnel Type	TUN(IP over GRE) ▼
Interface	SFP ▼
Remote Gateway IP	0.0.0.0
Tunnel Local IP Address (Virtual Interface)	0.0.0.0
Tunnel Network Netmask (Virtual Interface)	0.0.0.0
Tunnel Remote IP Address (Virtual Interface)	0.0.0.0
Remote Network IP Address	0.0.0.0
Remote Network Netmask	0.0.0.0
Enable Keepalive	☐
Keepalive Retry Times	3
Keepalive Interval	5 Second(s)
MTU	1460
Key	
Active as Default Route	○ Yes ● No
IPSec	☐ Enable

Interface: Select a WAN interface to establish a tunnel with the remote VPN device.

Remote Gateway IP: Enter the remote GRE WAN IP address.

Tunnel Local IP Address & Remote IP Address (Virtual Interface): Enter a virtual IP address for local and peer network of the GRE tunnel.

Tunnel Network Netmask (Virtual Interface): Enter the Netmask for this virtual interface.

NOTE: The virtual Local and Remote IP addresses must in **same subnet** and **cannot be existed or used** in both networks.

Remote Network IP Address: Enter the actual remote LAN network IP address.

Remote Network Netmask: Enter the actual remote LAN network Netmask.

Enable Keepalive: Check the box to enable the keepalive. The system will detect remote peer is still alive or lost. If no responses from the remote peer after certain times, **#-of-retry-time x interval**, the connection will get dropped.

Keep-alive Retry Times: Set the keep-alive retry times, default is 3.

Keep-alive Interval: Set the keep-alive Interval, unit in seconds. Default is 5 seconds.

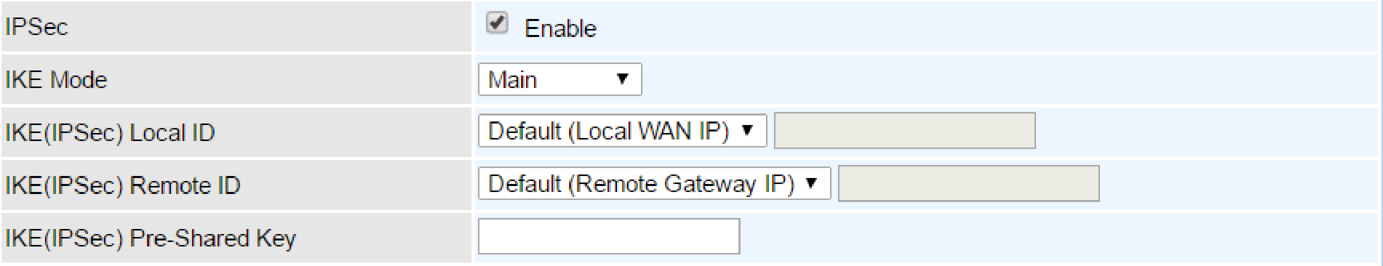
Example: Keepalive retry time (3) x keepalive interval (5) = 15 seconds. If no responses for 15 seconds, GRE connection will get aborted.

MTU: Maximum Transmission Unit in byte. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

Key: This tunnel key has a maximum string of 5 containing alphanumeric characters. Both sides, local and remote, should use the same key.

Active as Default Route: Select if to set the GRE tunnel as the default route.

IPSec: Click the checkbox to establish a GRE tunnel inside of the IPSec tunnel.



IPSec	☑ Enable
IKE Mode	Main ▼
IKE(IPSec) Local ID	Default (Local WAN IP) ▼
IKE(IPSec) Remote ID	Default (Remote Gateway IP) ▼
IKE(IPSec) Pre-Shared Key	

IKE Mode: IKE, Internet Key Exchange, is the mechanism to negotiate and exchange parameters and keys between IPSec peers to establish security associations (SA). Select Main or Aggressive mode.

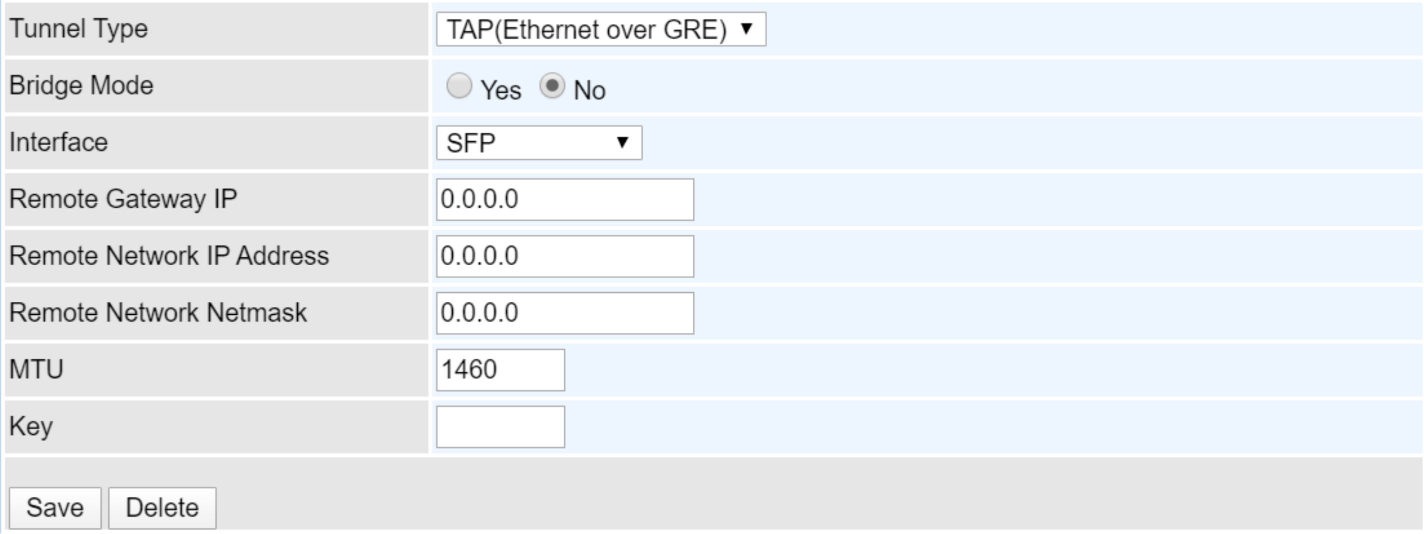
IKE (IPSec) Local ID Type and **Remote ID Type:** When the mode of IKE is aggressive, Local and Remote peers can be identified by other IDs.

IKE (IPSec) Pre-Shared Key: This is for the Internet Key Exchange (IKE) protocol, a string from 4 to 128 characters. Both sides should use the same key. IKE is used to establish a shared security policy and authenticated keys for services (such as IPSec) that require a key. Before any IPSec traffic can be passed, each router must be able to verify the identity of its peer. This can be done by manually entering the pre-shared key into both sides (router or hosts).

Click **Save** to apply settings.

TAN (Ethernet over GRE)

TAN is in layer 2, Ethernet level which acts as a switch adding Ethernet frame passed over the GRE tunnels.



Tunnel Type	TAP(Ethernet over GRE) ▾
Bridge Mode	○ Yes ● No
Interface	SFP ▾
Remote Gateway IP	0.0.0.0
Remote Network IP Address	0.0.0.0
Remote Network Netmask	0.0.0.0
MTU	1460
Key	

Bridge Mode: Select **Yes** to enable TAN bridge mode.

Bridge Mode – No

Interface: Select a WAN interface to establish a tunnel with the remote VPN device.

Remote Gateway IP: Enter the remote GRE WAN IP address.

Remote Network IP Address: Enter the actual remote LAN network IP address.

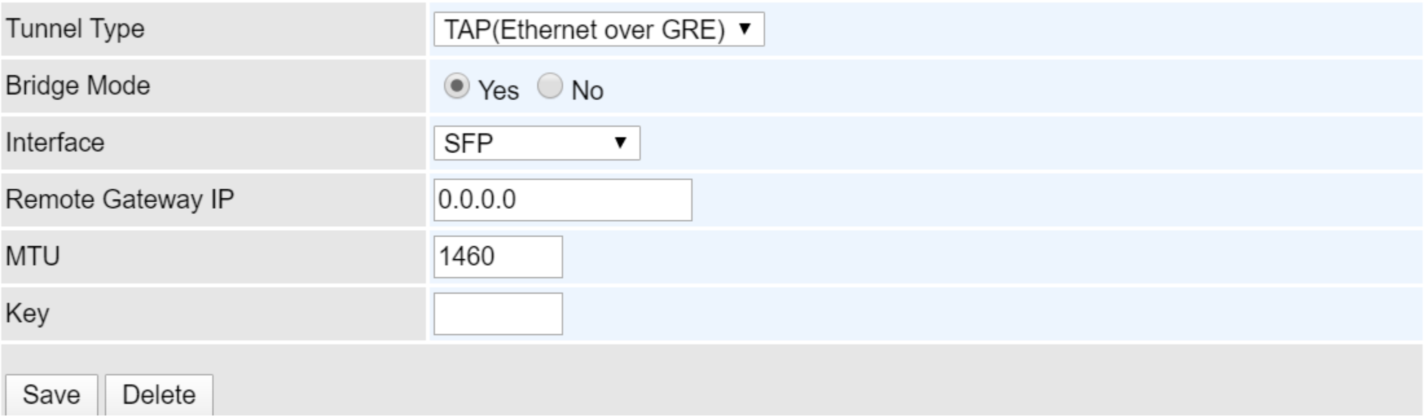
Remote Network Netmask: Enter the actual remote LAN network Netmask.

MTU: Maximum Transmission Unit in byte. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

Key: This tunnel key has a maximum string of 5 containing alphanumeric characters. Both sides, local and remote, should use the same key.

Click **Save** to apply settings.

Bridge Mode – Yes



Tunnel Type	TAP(Ethernet over GRE) ▾
Bridge Mode	● Yes ○ No
Interface	SFP ▾
Remote Gateway IP	0.0.0.0
MTU	1460
Key	

Interface: Select a WAN interface to establish a tunnel with the remote VPN device.

Remote Gateway IP: Enter the remote GRE WAN IP address.

MTU: Maximum Transmission Unit in byte. The size of the largest datagram (excluding media-specific headers) an IP attempts to send through the interface.

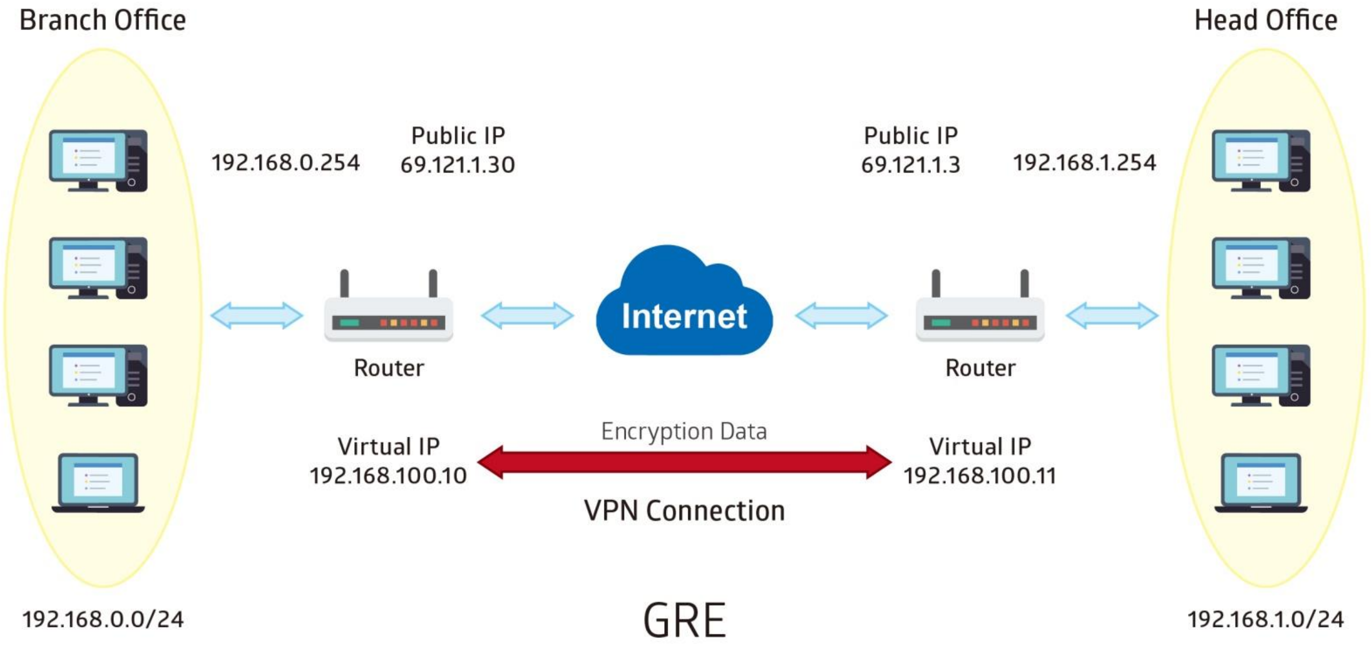
Key: This tunnel key has a maximum string of 5 containing alphanumeric characters. Both sides, local and remote, should use the same key.

Click **Save** to apply settings.

Example: GRE VPN – Network (LAN) to Network (LAN) Connection

The branch office establishes a GRE VPN tunnel with Headquarter office to connect two private networks over the Internet. The routers are installed in the Headquarter office and branch office accordingly.

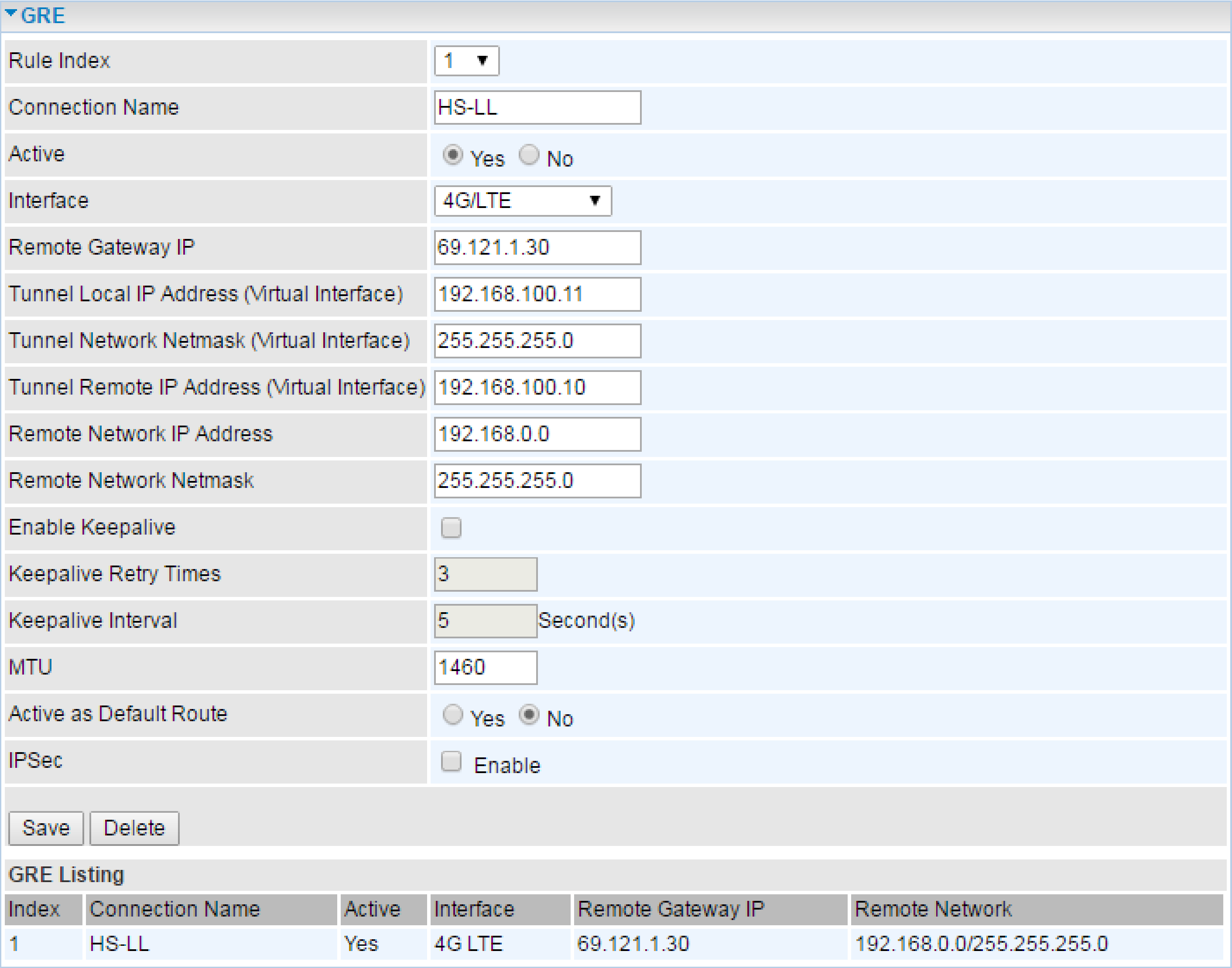
NOTE: Both office LAN networks must be in different subnets with the GRE VPN connection.



Configuring GRE connection in the Headquarter office

The IP address 69.1.121.30 is the Public IP address of the router located in branch office.

Item		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Remote Gateway IP	69.121.1.30	WAN IP address of Branch office
Tunnel Local IP Address (Virtual Interface)	192.168.100.11	Local and remote virtual interface IP address must be in same Netmask.
Tunnel Remote IP Address (Virtual Interface)	192.168.100.10	
Tunnel Network Netmask (Virtual Interface)	255.255.255.0	Network Netmask of this virtual interface.
Remote Network IP/ Netmask	192.168.0.0/ 255.255.255.0	The remote, branch office, LAN network IP and Netmask.



▾GRE

Rule Index	1 ▾
Connection Name	HS-LL
Active	● Yes ○ No
Interface	4G/LTE ▾
Remote Gateway IP	69.121.1.30
Tunnel Local IP Address (Virtual Interface)	192.168.100.11
Tunnel Network Netmask (Virtual Interface)	255.255.255.0
Tunnel Remote IP Address (Virtual Interface)	192.168.100.10
Remote Network IP Address	192.168.0.0
Remote Network Netmask	255.255.255.0
Enable Keepalive	□
Keepalive Retry Times	3
Keepalive Interval	5 Second(s)
MTU	1460
Active as Default Route	○ Yes ● No
IPSec	□ Enable

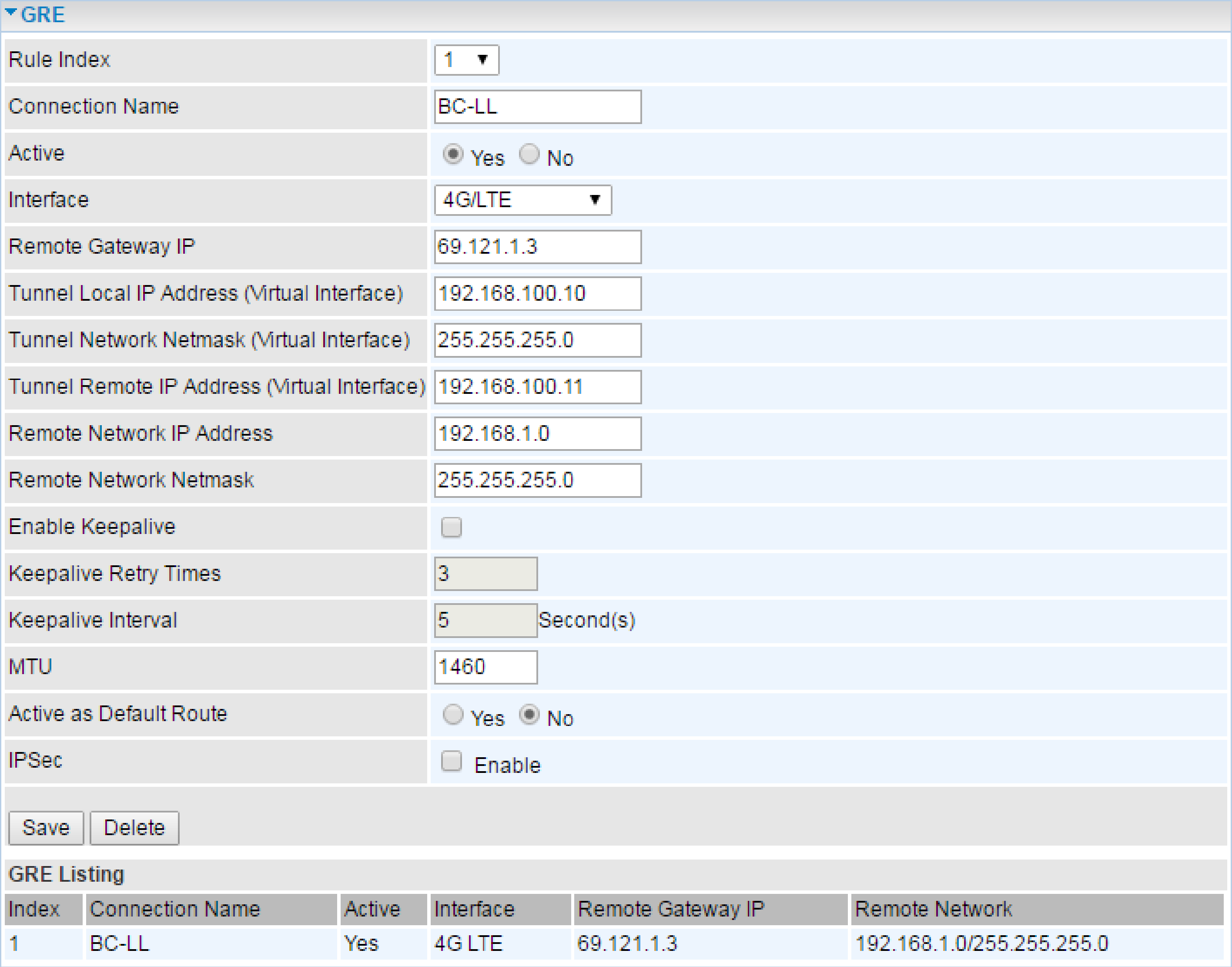
GRE Listing

Index	Connection Name	Active	Interface	Remote Gateway IP	Remote Network
1	HS-LL	Yes	4G LTE	69.121.1.30	192.168.0.0/255.255.255.0

Configuring GRE connection in the Branch office

The IP address 69.1.121.3 is the Public IP address of the router located in Headquarter office.

Item		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Remote Gateway IP	69.121.1.3	WAN IP address of Headquarter office
Tunnel Local IP Address (Virtual Interface)	192.168.100.10	Local and remote virtual interface IP address must be in same Netmask.
Tunnel Remote IP Address (Virtual Interface)	192.168.100.11	
Tunnel Network Netmask (Virtual Interface)	255.255.255.0	Network Netmask of this virtual interface.
Remote Network IP/ Netmask	192.168.1.0/ 255.255.255.0	The remote, Headquarter office, LAN network IP and Netmask.



▾GRE

Rule Index	1 ▾
Connection Name	BC-LL
Active	● Yes ○ No
Interface	4G/LTE ▾
Remote Gateway IP	69.121.1.3
Tunnel Local IP Address (Virtual Interface)	192.168.100.10
Tunnel Network Netmask (Virtual Interface)	255.255.255.0
Tunnel Remote IP Address (Virtual Interface)	192.168.100.11
Remote Network IP Address	192.168.1.0
Remote Network Netmask	255.255.255.0
Enable Keepalive	☐
Keepalive Retry Times	3
Keepalive Interval	5 Second(s)
MTU	1460
Active as Default Route	○ Yes ● No
IPSec	☐ Enable

GRE Listing

Index	Connection Name	Active	Interface	Remote Gateway IP	Remote Network
1	BC-LL	Yes	4G LTE	69.121.1.3	192.168.1.0/255.255.255.0

OpenVPN

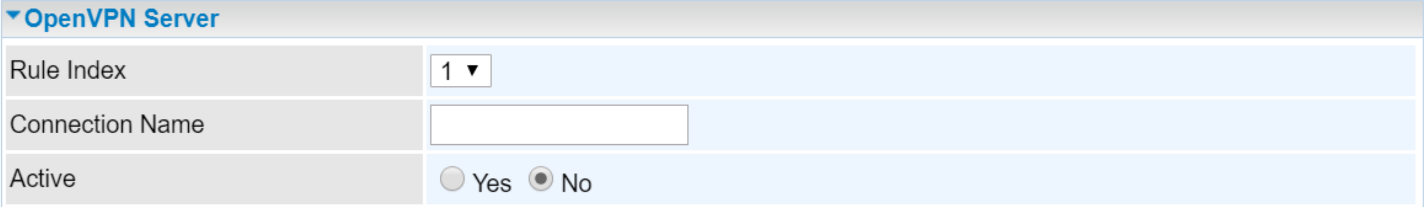
OpenVPN is an open source software application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. It uses a custom security protocol that utilizes SSL/TLS for key exchange. OpenVPN can run over User Datagram Protocol (UDP) or Transmission Control Protocol (TCP) transports, multiplexing created SSL tunnels on a single TCP/UDP port. It is capable of traversing network address translation (NAT) and firewalls.

OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. Preshared secret key is the easiest, with certificate based being the most robust and feature-rich. It uses the OpenSSL encryption library extensively, allowing OpenVPN to use all the ciphers available in the OpenSSL package, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

It has integrated with OpenVPN package, allowing users to run OpenVPN in server or client mode from their network routers.

OpenVPN Server

NOTE: Up to 1 profile.



▾OpenVPN Server

Rule Index	1 ▼
Connection Name	
Active	○ Yes ● No

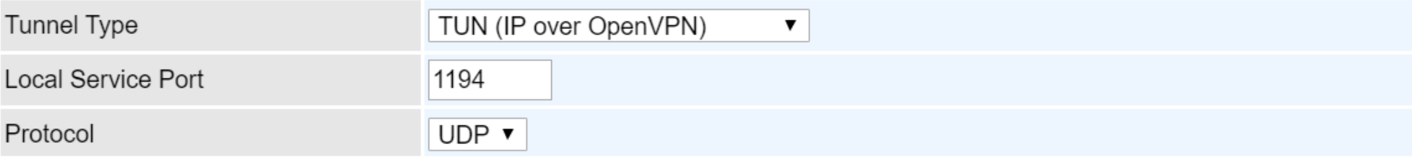
Rule Index: The numeric rule indicator for OpenVPN.

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate this profile.

Device Type: TUN (IP over OpenVPN) and TAN (Ethernet Over OpenVPN) to choose.

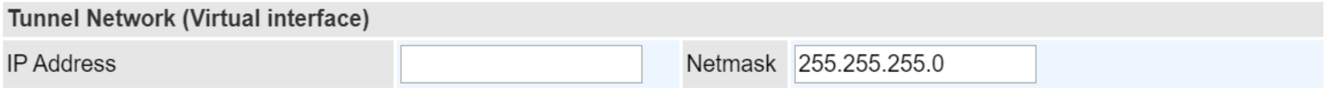
- **TUN (IP Over OpenVPN):** Layer 3 networking level which routes packets on the VPN (Routing).



Tunnel Type	TUN (IP over OpenVPN) ▼
Local Service Port	1194
Protocol	UDP ▼

- **Local Service Port:** Port 1194 is the default assigned port for OpenVPN.
- **Protocol:** OpenVPN can run over either UDP or TCP transports. Select the protocol.

Tunnel Network (Virtual Interface)



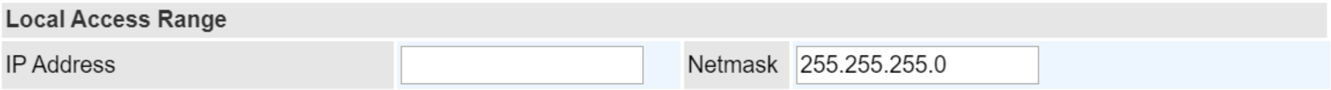
Tunnel Network (Virtual interface)

IP Address		Netmask	255.255.255.0

IP Address / Netmask: Enter a virtual IP address and Netmask for this tunnel.

NOTE: The virtual IP addresses **cannot be existed or used** in both networks.

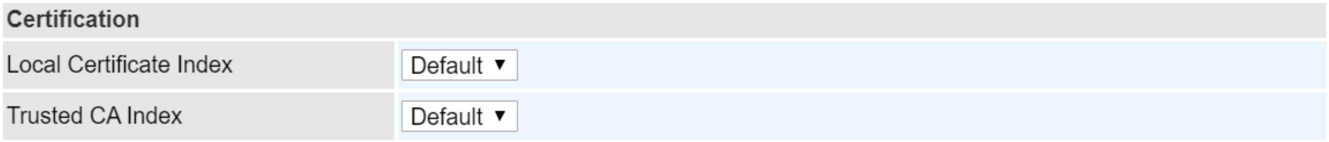
Local Access Range



Local Access Range			
IP Address		Netmask	255.255.255.0

IP Address / Netmask: Enter local OpenVPN Server's LAN network IP address and Netmask.

Certification

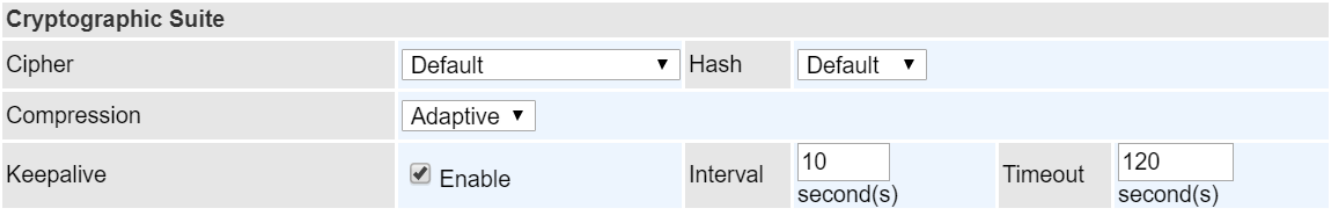


Certification	
Local Certificate Index	Default ▼
Trusted CA Index	Default ▼

Local Certificate / Trusted CA Index: OpenVPN mutually authenticate the server and client based on certificates and CA. Select a certificate and CA.

To import certificates and CAs, go to **Maintenance >> Certificate Management** to upload files. Otherwise, select **Default** certificate and CA.

Cryptographic Suite



Cryptographic Suite					
Cipher	Default ▼	Hash	Default ▼		
Compression	Adaptive ▼				
Keepalive	☑ Enable	Interval	10 second(s)	Timeout	120 second(s)

Cipher: OpenVPN uses all the ciphers available in the OpenSSL package to encrypt both the data and channels. Select an encryption method.

Hash: To establish the integrity of the datagram and ensures it is not tampered with in transmission. There are options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

Compression: Choose **adaptive** to use the LZO compression library to compress the data stream.

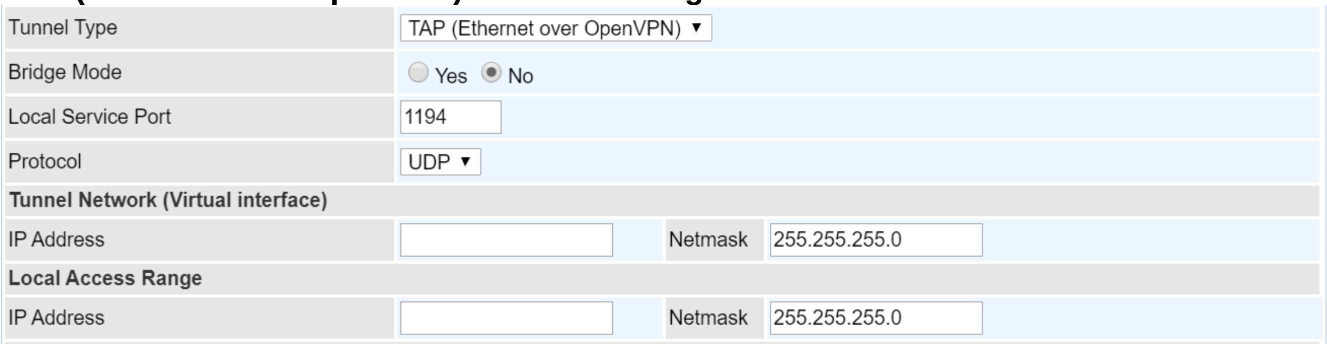
Keepalive: Check the box to enable the keepalive feature. The system will automatically send ping packet to remote peer to keep the tunnel active.

Interval: Set the keep-alive Interval, unit in seconds. Default is **10** seconds. Valid interval range is from **0 to 3600** seconds.

Timeout: Re-establish tunnel if no responses from peer network after timeout period expires. Default is 120 seconds.

Click **Save** to apply settings.

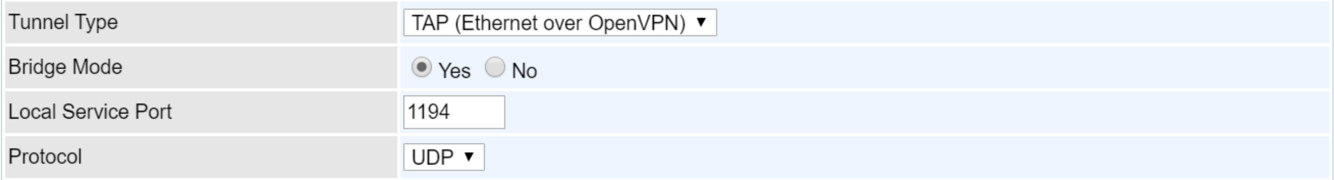
TAP (Ethernet Over OpenVPN) in Server-Bridge Mode



Tunnel Type	TAP (Ethernet over OpenVPN) ▼		
Bridge Mode	○ Yes ● No		
Local Service Port	1194		
Protocol	UDP ▼		
Tunnel Network (Virtual interface)			
IP Address		Netmask	255.255.255.0
Local Access Range			
IP Address		Netmask	255.255.255.0

- **Bridge: No** – Using its own client IP address.
- **Local Service Port:** Port 1194 is the default assigned port for OpenVPN.
- **Protocol:** OpenVPN can run over either UDP or TCP transports. Select the protocol.
- **Tunnel Network IP Address / Netmask:** Enter a virtual IP address and Netmask for this tunnel. **NOTE:** The virtual IP addresses **cannot be existed or used** in both networks.
- **Local IP Address / Netmask:** Enter local LAN network IP address and Netmask.

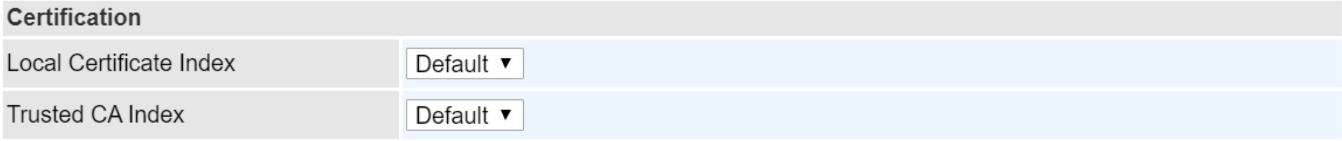
TAP (Ethernet Over OpenVPN) in Bridge mode



Tunnel Type	TAP (Ethernet over OpenVPN) ▼
Bridge Mode	● Yes ○ No
Local Service Port	1194
Protocol	UDP ▼

- **Bridge: Yes** – Can use local DHCP server on LAN to assign IP address to VPN clients.
- **Local Service Port:** Port 1194 is the default assigned port for OpenVPN.
- **Protocol:** OpenVPN can run over either UDP or TCP transports. Select the protocol.

Certification

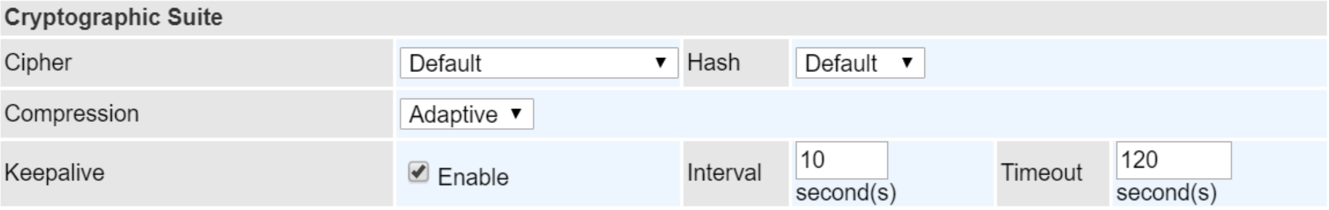


Certification	
Local Certificate Index	Default ▼
Trusted CA Index	Default ▼

Local Certificate / Trusted CA Index: OpenVPN mutually authenticate the server and client based on certificates and CA. Select a certificate and CA.

To import certificates and CAs, go to **Maintenance >> Certificate Management** to upload files. Otherwise, select **Default** certificate and CA.

Cryptographic Suite



Cryptographic Suite					
Cipher	Default ▼	Hash	Default ▼		
Compression	Adaptive ▼				
Keepalive	☑ Enable	Interval	10 second(s)	Timeout	120 second(s)

Cipher: OpenVPN uses all the ciphers available in the OpenSSL package to encrypt both the data and channels. Select an encryption method.

Hash: To establish the integrity of the datagram and ensures it is not tampered with in transmission. There are options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

Compression: Choose **adaptive** to use the LZO compression library to compress the data stream.

Keepalive: Check the box to enable the keepalive feature. The system will automatically send ping packet to remote peer to keep the tunnel active.

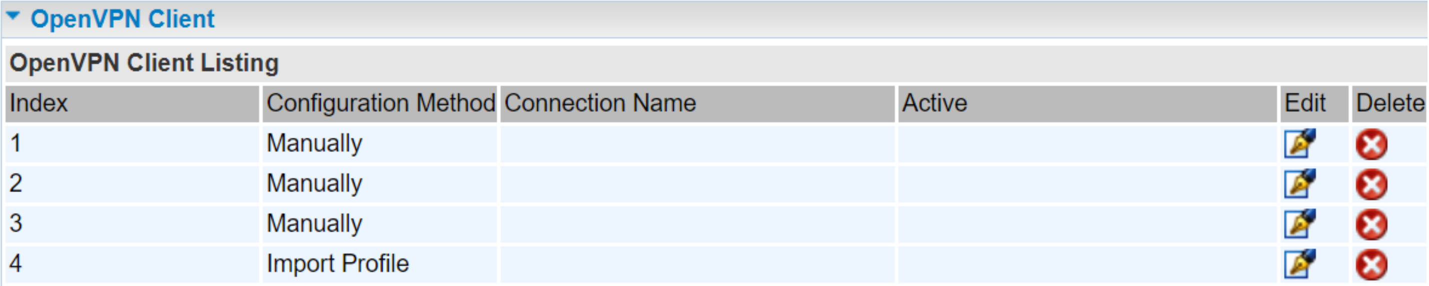
Interval: Set the keep-alive Interval, unit in seconds. Default is **10** seconds. Valid interval range is from **0 to 3600** seconds.

Timeout: Re-establish tunnel if no responses from peer network after timeout period expires. Default is 120 seconds.

Click **Save** to apply settings.

OpenVPN Client

OpenVPN client must match the VPN information / settings with the OpenVPN Server.



▾ OpenVPN Client

OpenVPN Client Listing

Index	Configuration Method	Connection Name	Active	Edit	Delete
1	Manually			✎	✖
2	Manually			✎	✖
3	Manually			✎	✖
4	Import Profile			✎	✖

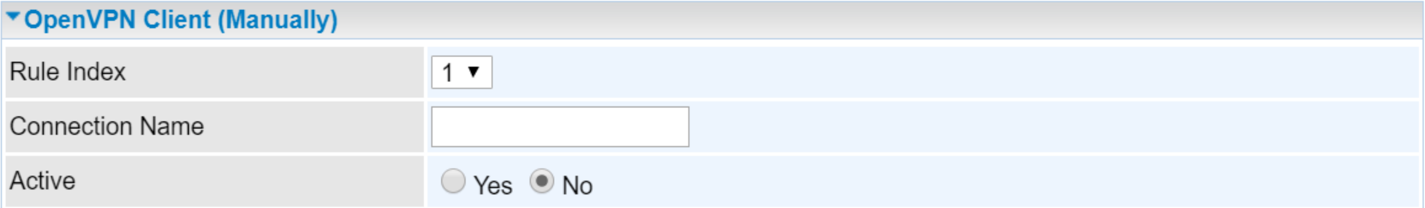
Rule Index: The indication of the rule number. Maximum up to 4 profile/tunnels

Configuration Method: OpenVPN client profiles can be manually entered or imported a pre-configured client profile.

Connection Name: Display the name of the connection or profile.

Active: Display whether the connection or profile is set to active or not.

Manual Input Client Information



▾ OpenVPN Client (Manually)

Rule Index	1 ▾
Connection Name	
Active	○ Yes ● No

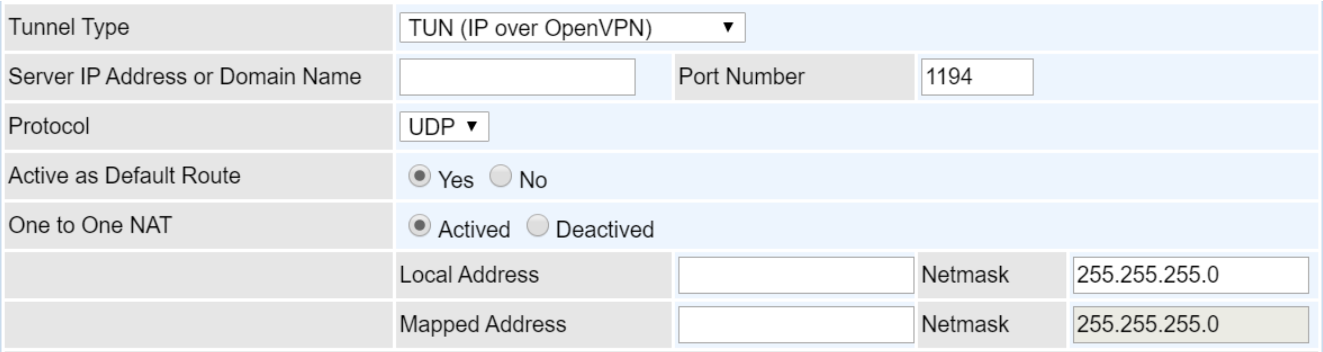
Rule Index: The indication of the rule number. Maximum up to 3 profile/tunnels

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate this profile.

Device Type:

- **TUN (IP Over OpenVPN):** Works only in Layer 3 networking level which routes packets on the VPN.

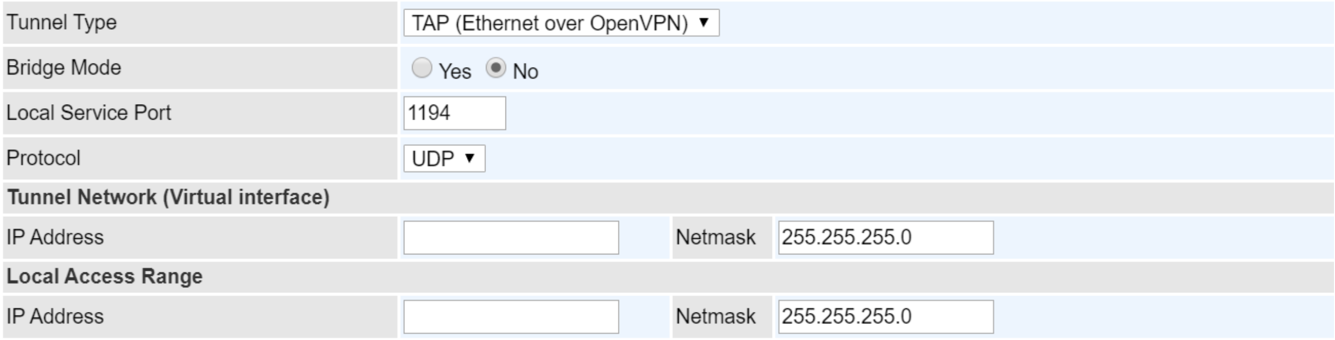


Tunnel Type	TUN (IP over OpenVPN) ▾			
Server IP Address or Domain Name		Port Number	1194	
Protocol	UDP ▾			
Active as Default Route	● Yes ○ No			
One to One NAT	● Actived ○ Deactived			
	Local Address		Netmask	255.255.255.0
	Mapped Address		Netmask	255.255.255.0

- **Server IP Address or Domain Name:** Enter OpenVPN Server's WAN IP address or Domain name.
- **Service Port:** Port 1194 is the official assigned port number for OpenVPN.
- **Protocol:** OpenVPN can run over either UDP or TCP transports. Select the protocol.

- **Active as Default Route:** Choose **Yes** to let the OpenVPN tunnel/connection be the default route for traffic, under this circumstance, all outgoing packets will be forwarded to this tunnel and routed to the next hop.
- **Remote Network IP Address / Netmask:** Enter the LAN network IP address and Netmask of the OpenVPN Server.
- **One-to-One NAT:** Create a one-to-one mapping for a specific or a range of internal LAN IP address of the OpenVPN client to the VPN tunnel.
  - **Local IP Address / Netmask:** This is the internal LAN network IP address & netmask of the OpenVPN client.
  - **Mapped Tunnel IP Address / Netmask:** This is the IP address & netmask of the OpenVPN tunnel.

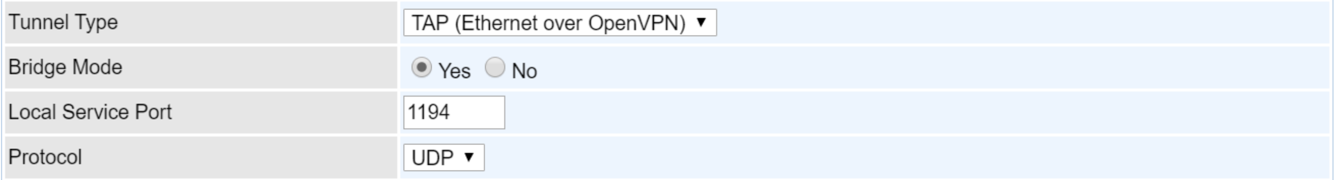
TAP (Ethernet Over OpenVPN) in Server-Bridge Mode



Tunnel Type	TAP (Ethernet over OpenVPN) ▾		
Bridge Mode	○ Yes ● No		
Local Service Port	1194		
Protocol	UDP ▾		
Tunnel Network (Virtual interface)			
IP Address		Netmask	255.255.255.0
Local Access Range			
IP Address		Netmask	255.255.255.0

- **Bridge: No** – Using its own client IP address.
- **Local Service Port:** Port 1194 is the default assigned port for OpenVPN.
- **Protocol:** OpenVPN can run over either UDP or TCP transports. Select the protocol.
- **Tunnel Network IP Address / Netmask:** Enter a virtual IP address and Netmask for this tunnel. **NOTE:** The virtual IP addresses **cannot be existed or used** in both networks.
- **Local IP Address / Netmask:** Enter local LAN network IP address and Netmask.
- **Server IP Address or Domain Name:** Enter OpenVPN Server's WAN IP address or Domain name.
- **Bridge: No** – Using its own client IP address.
- **Local Service Port:** Port 1194 is the default assigned port for OpenVPN.
- **Protocol:** OpenVPN can run over either UDP or TCP transports. Select the protocol.

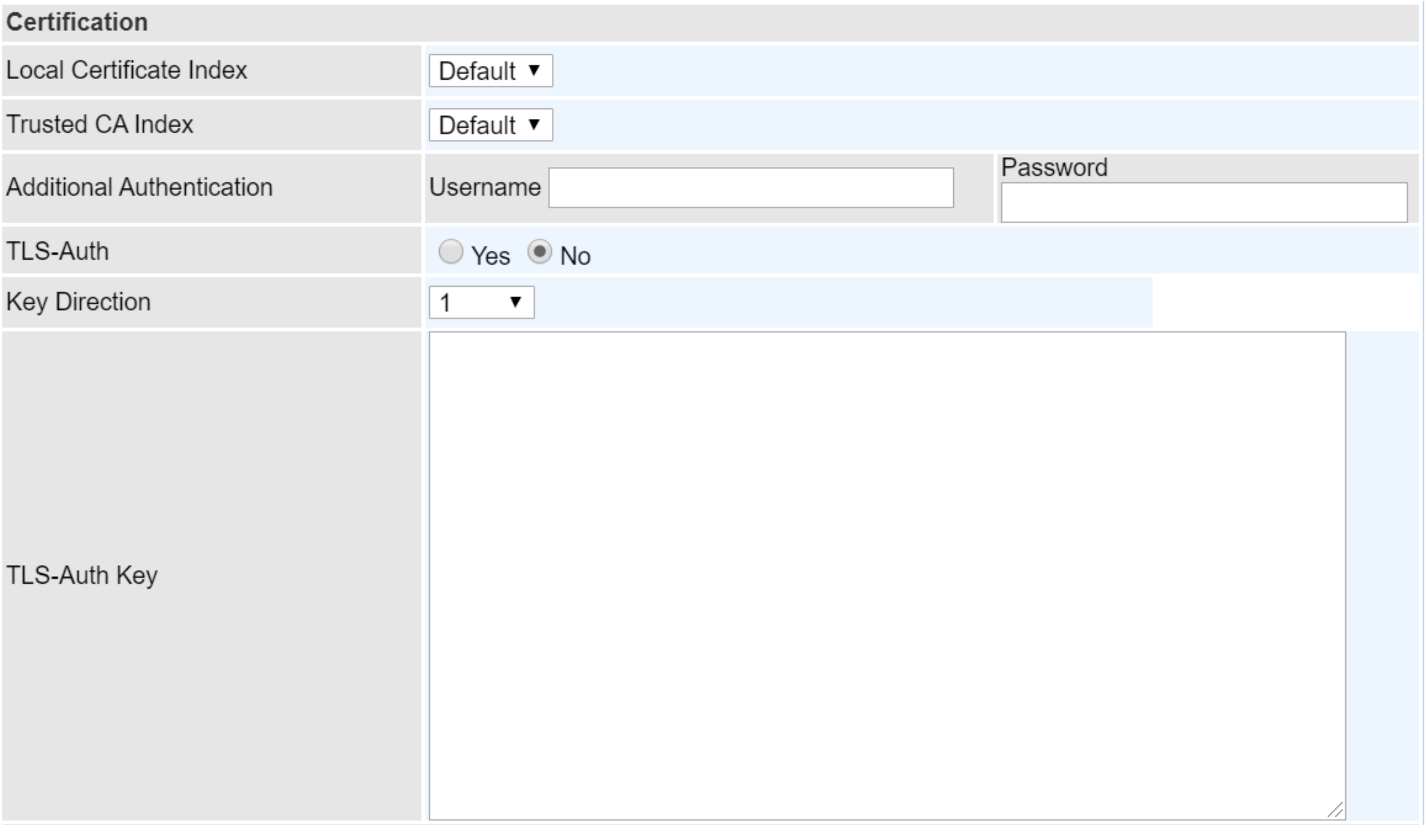
TAP (Ethernet Over OpenVPN) in Bridge Mode



Tunnel Type	TAP (Ethernet over OpenVPN) ▾
Bridge Mode	● Yes ○ No
Local Service Port	1194
Protocol	UDP ▾

- **Bridge: Yes** if used in bridge.
- **Local Service Port:** Port 1194 is the default assigned port for OpenVPN.
- **Protocol:** OpenVPN can run over either UDP or TCP transports. Select the protocol.

Certification



Certification		
Local Certificate Index	Default ▼	
Trusted CA Index	Default ▼	
Additional Authentication	Username	Password
TLS-Auth	○ Yes ● No	
Key Direction	1 ▼	
TLS-Auth Key		

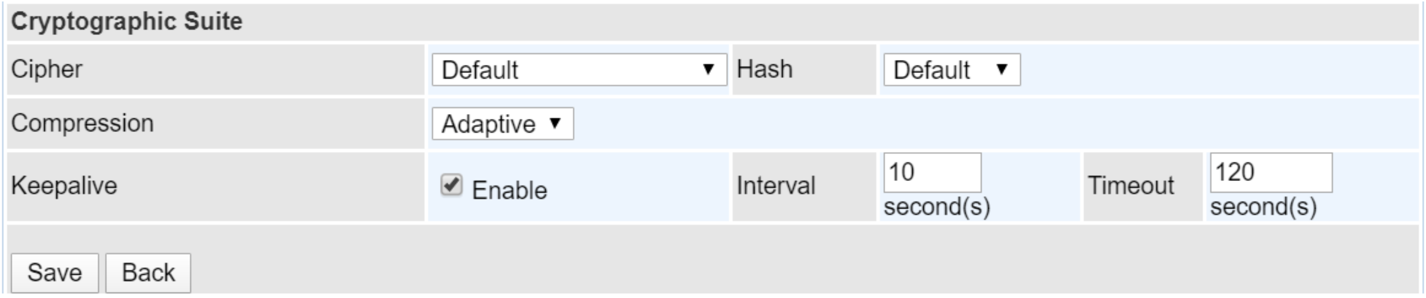
Local Certificate / Trusted CA Index: OpenVPN mutually authenticate the server and client based on certificates and CA. Select a certificate and CA.

To import certificates and CAs, go to **Maintenance >> Certificate Management** to upload files. Otherwise, select **Default** certificate and CA.

Additional Authentication: Enter the extra credential requested by the OpenVPN server.

TLS-Auth / Key Direction / TLS-Auth Key: These are optional functions which must be activated on the server side.

Cryptographic Suite



Cryptographic Suite					
Cipher	Default ▼	Hash	Default ▼		
Compression	Adaptive ▼				
Keepalive	☑ Enable	Interval	10 second(s)	Timeout	120 second(s)

Cipher: OpenVPN uses all the ciphers available in the OpenSSL package to encrypt both the data and channels. Select an encryption method.

Hash: To establish the integrity of the datagram and ensures it is not tampered with in transmission. There are options: Message Digest 5 (MD5) and Secure Hash Algorithm (SHA1, SHA256). SHA1 is more resistant to brute-force attacks than MD5. However, it is slower.

Compression: Choose **adaptive** to use the LZO compression library to compress the data stream.

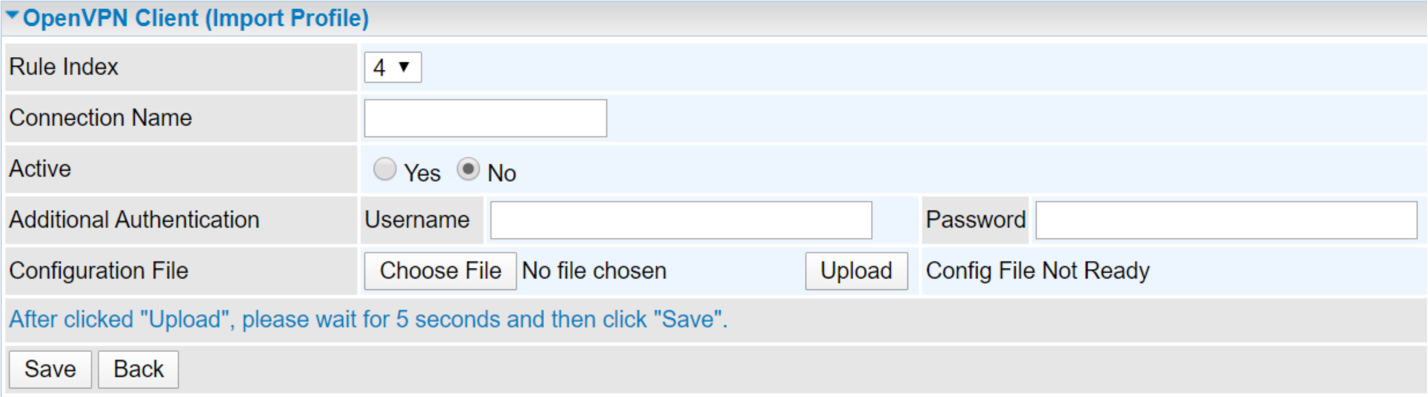
Keepalive: Check the box to enable the keepalive feature. The system will automatically send ping packet to remote peer to keep the tunnel active.

Interval: Set the keep-alive Interval, unit in seconds. Default is **10** seconds. Valid interval range is from **0 to 3600** seconds.

Timeout: Re-establish tunnel if no responses from peer network after timeout period expires. Default is 120 seconds.

Click **Save** to apply settings.

Import an OpenVPN Client Profile



▾OpenVPN Client (Import Profile)

Rule Index	4 ▾			
Connection Name				
Active	○ Yes ● No			
Additional Authentication	Username		Password	
Configuration File	Choose File No file chosen	Upload	Config File Not Ready	

After clicked "Upload", please wait for 5 seconds and then click "Save".

Save Back

Rule Index: The indication of the rule number.

Connection Name: Enter a description for this connection/profile.

Active: Yes to activate this profile.

Additional Authentication: Enter the extra credential requested by the OpenVPN server.

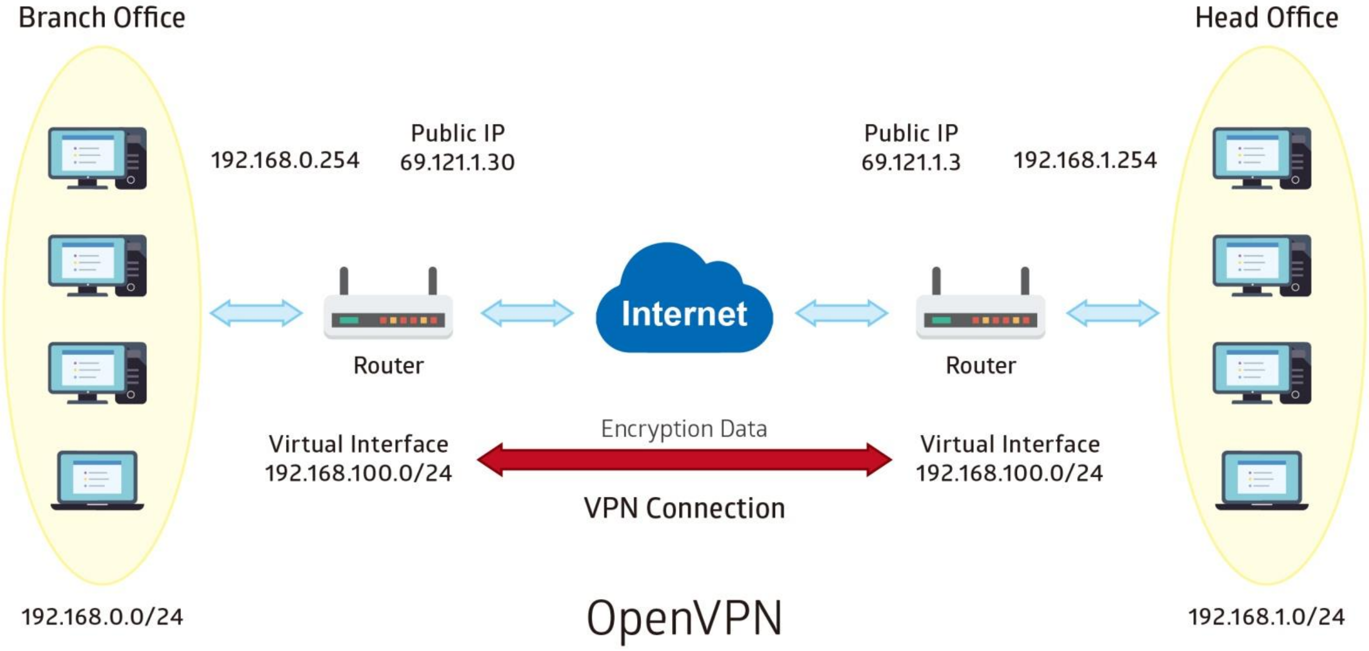
Configuration File: Click **"Choose File"** to find the OpenVPN client profile you want to upload. If the .ovpn file is in zip format, you must extract / decompress / unzip the file prior to the upload.

Upload: Click **Upload** to begin the upload process.

Example: OpenVPN – Network (LAN) to Network (LAN) Connection

The Branch office establishes a tunnel with Headquarter office to connect two private networks over the OpenVPN.

NOTE: Both office LAN networks must be in different subnets.

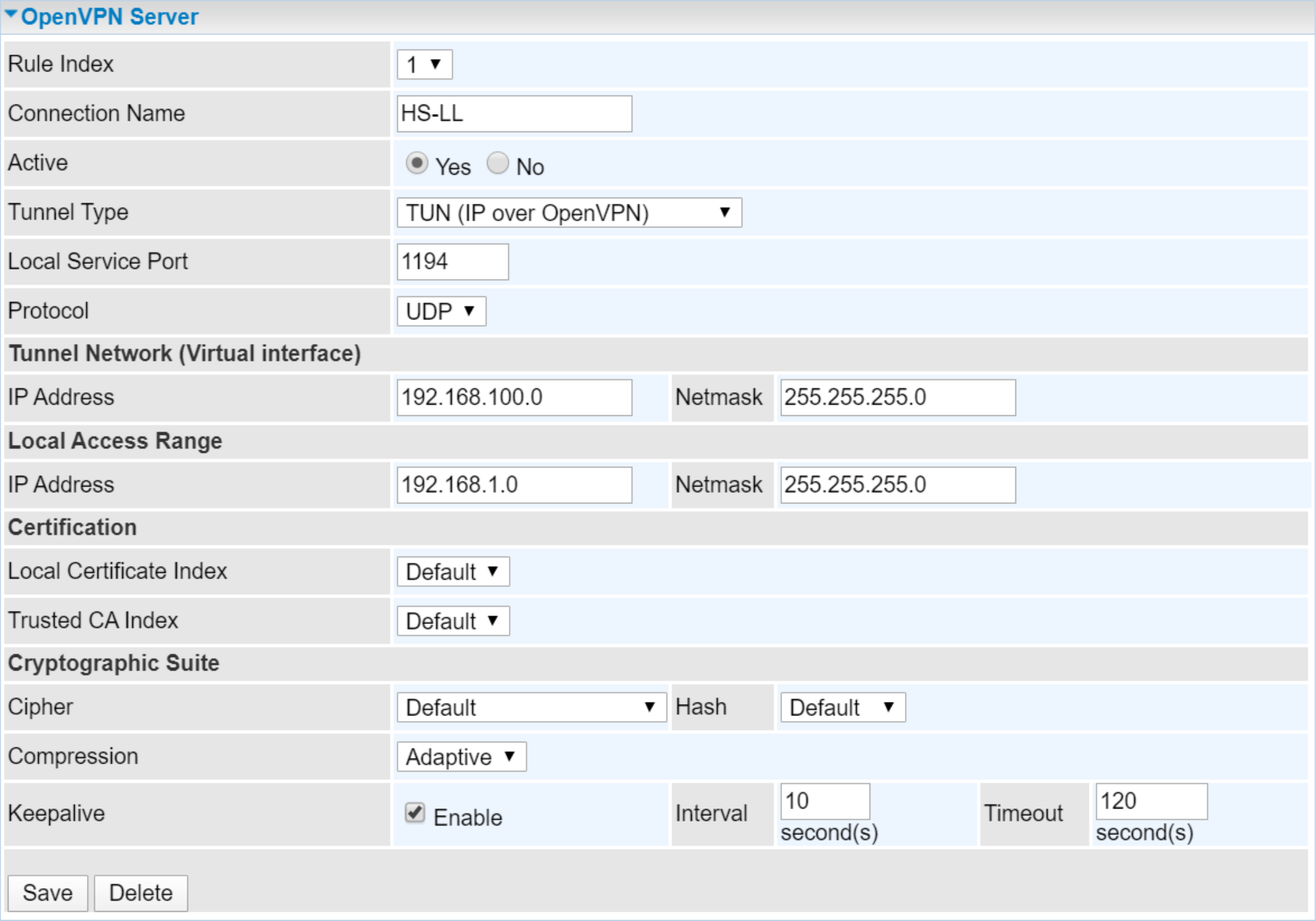


Configuring OpenVPN server in Headquarter office

The IP address 69.1.121.30 is the WAN IP address of the router located in the Branch office.

The OpenVPN tunnel network virtual interface is set to 192.168.100.0/24.

Item		Description
Connection Name	HS-LL	Assigned name to this tunnel/profile
Tunnel Network (Virtual Interface)	192.168.100.0/ 255.255.255.0	IP address & Netmask of the virtual tunnel.
Local Access Range	192.168.1.0/ 255.255.255.0	OpenVPN Server's local LAN network.



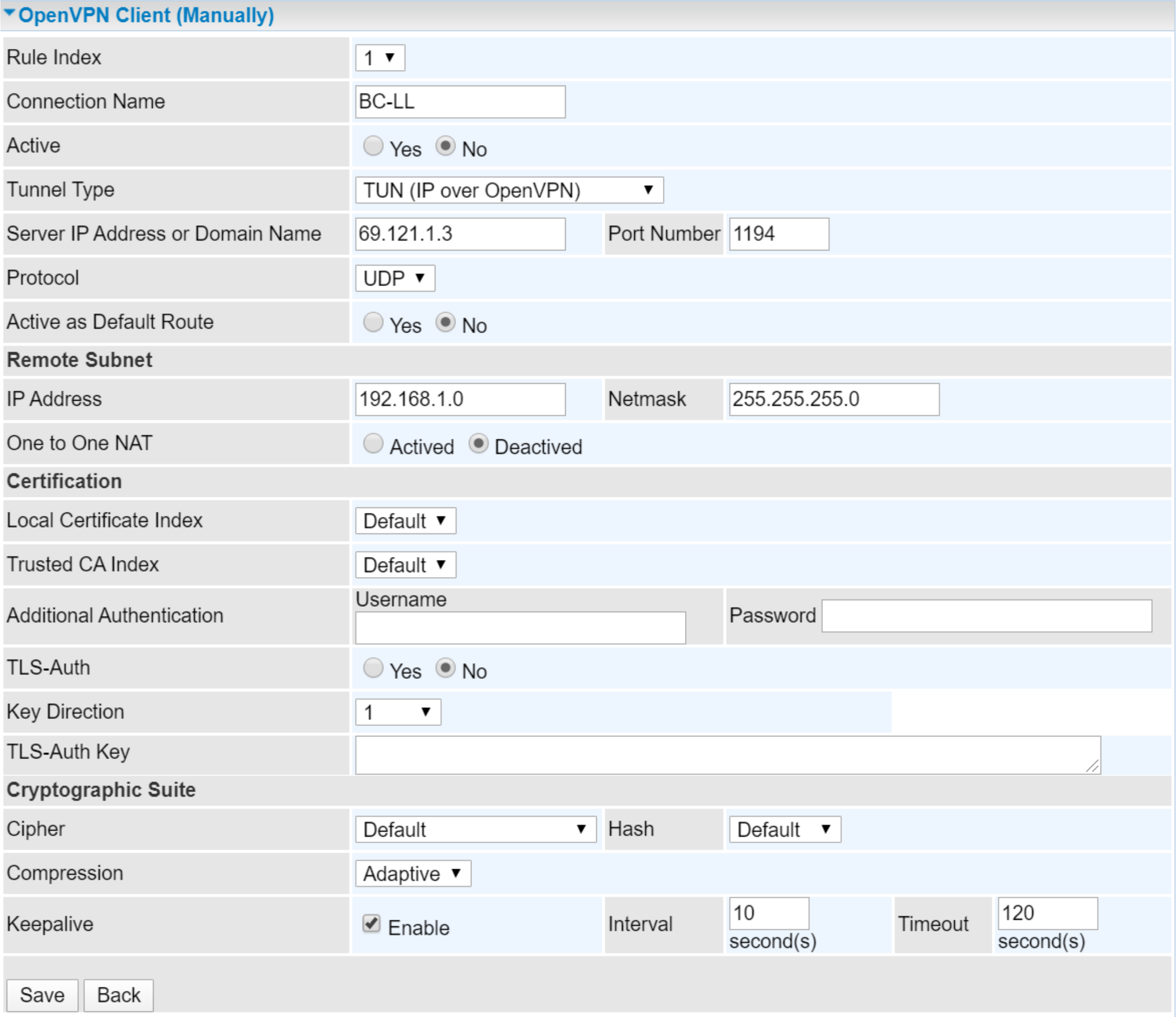
▾OpenVPN Server

Rule Index	1 ▾				
Connection Name	HS-LL				
Active	● Yes ○ No				
Tunnel Type	TUN (IP over OpenVPN) ▾				
Local Service Port	1194				
Protocol	UDP ▾				
Tunnel Network (Virtual interface)					
IP Address	192.168.100.0	Netmask	255.255.255.0		
Local Access Range					
IP Address	192.168.1.0	Netmask	255.255.255.0		
Certification					
Local Certificate Index	Default ▾				
Trusted CA Index	Default ▾				
Cryptographic Suite					
Cipher	Default ▾	Hash	Default ▾		
Compression	Adaptive ▾				
Keepalive	☑ Enable	Interval	10 second(s)	Timeout	120 second(s)

Configuring OpenVPN client in Branch office

The IP address 69.1.121.3 is the WAN IP address of the router located in Headquarter office.

Item		Description
Connection Name	BC-LL	Assigned name to this tunnel/profile
Server IP Address	69.121.1.3	The WAN IP address of OpenVPN server.
Remote Subnet	192.168.1.0/ 255.255.255.0	Local LAN IP & Netmask of the Server office

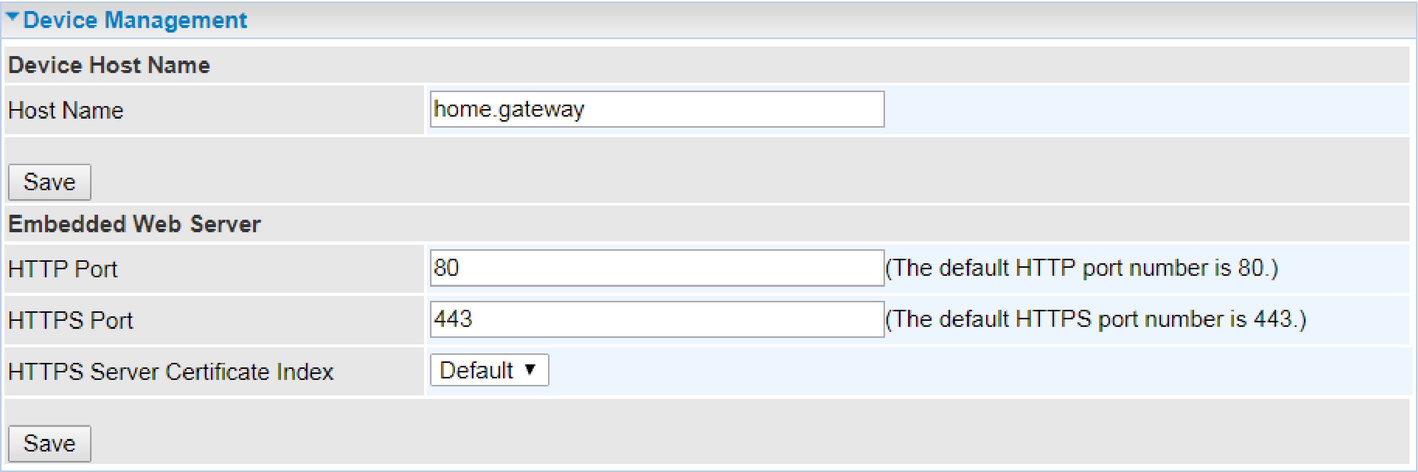


▾OpenVPN Client (Manually)

Rule Index	1 ▾		
Connection Name	BC-LL		
Active	○ Yes ● No		
Tunnel Type	TUN (IP over OpenVPN) ▾		
Server IP Address or Domain Name	69.121.1.3	Port Number	1194
Protocol	UDP ▾		
Active as Default Route	○ Yes ● No		
Remote Subnet			
IP Address	192.168.1.0	Netmask	255.255.255.0
One to One NAT	○ Actived ● Deactived		
Certification			
Local Certificate Index	Default ▾		
Trusted CA Index	Default ▾		
Additional Authentication	Username	Password	
TLS-Auth	○ Yes ● No		
Key Direction	1 ▾		
TLS-Auth Key			
Cryptographic Suite			
Cipher	Default ▾	Hash	Default ▾
Compression	Adaptive ▾		
Keepalive	☑ Enable	Interval	10 second(s)
		Timeout	120 second(s)

Access Management

Device Management



▼Device Management

Device Host Name

Host Name	home.gateway

Embedded Web Server

HTTP Port	80 (The default HTTP port number is 80.)
HTTPS Port	443 (The default HTTPS port number is 443.)
HTTPS Server Certificate Index	Default ▼

Device Host Name

Host Name: Enter the host name of the router. Default is **home.gateway**

Embedded Web Server

HTTP Port: It is the embedded web server (Web GUI) accessing port, default is **80**. It can be changed other port other than port 80, e.g. port 8080.

HTTPS Port: Similar to HTTP which is an unencrypted communication using port 80. HTTPS is encrypted by SSL using port 443 instead.

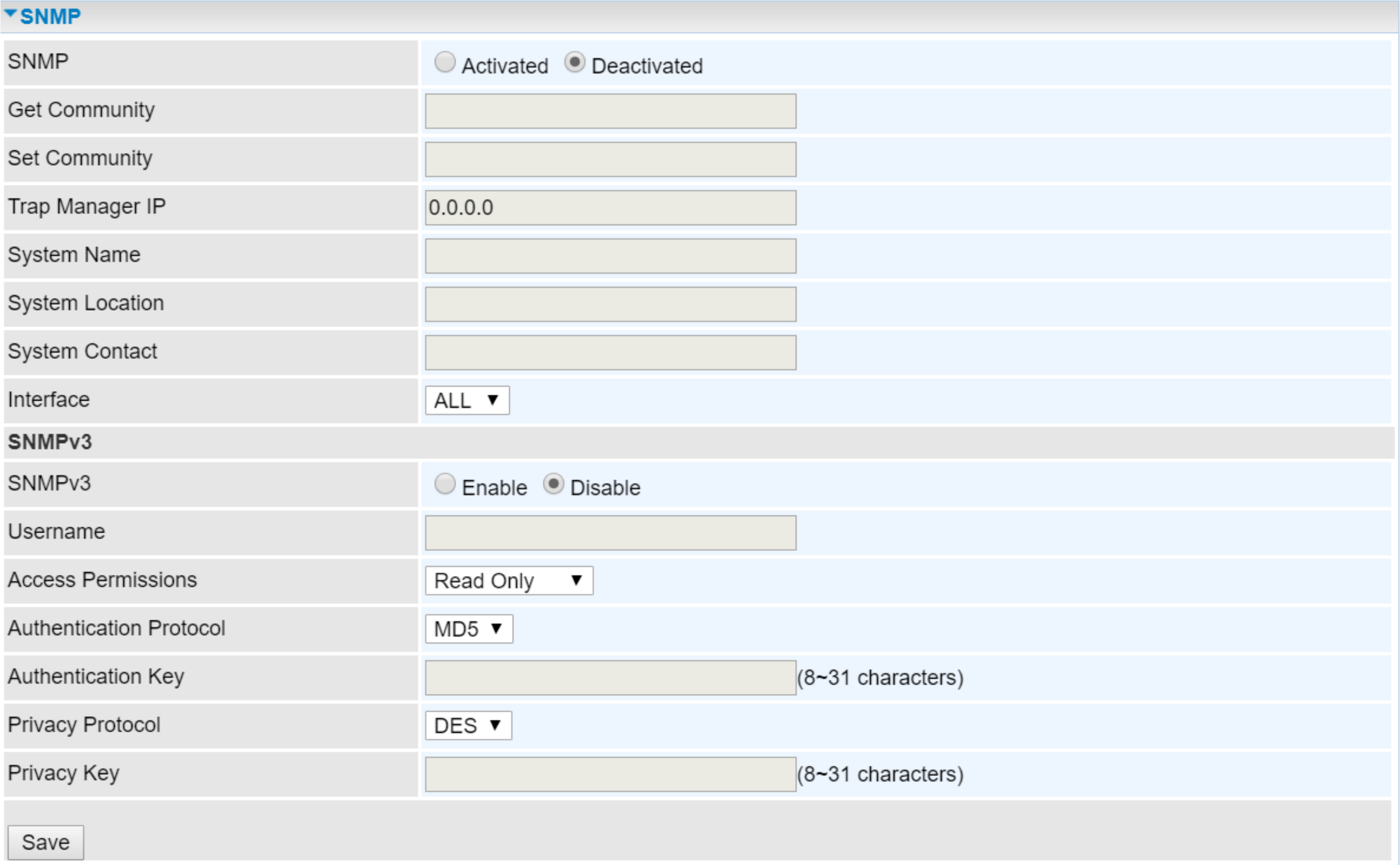
HTTPS Server Certificate Index: *HTTPS* known as HTTP-over-SSL tunnel protocol. Select a certificate to identify the system web server. When accessing to the web server (Web GUI), the browser will issue a warning page.

To import certificates, go to **Maintenance >> Certificate Management** to upload files. Otherwise, select **Default** certificate and CA.

Click **Save** to apply settings.

SNMP

Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. Your BEC 4700A/AZ serves as a SNMP agent that allows a manager station to manage and monitor the router through the network.



▾SNMP

SNMP	○ Activated ● Deactivated
Get Community	
Set Community	
Trap Manager IP	0.0.0.0
System Name	
System Location	
System Contact	
Interface	ALL ▼
SNMPv3	
SNMPv3	○ Enable ● Disable
Username	
Access Permissions	Read Only ▼
Authentication Protocol	MD5 ▼
Authentication Key	(8~31 characters)
Privacy Protocol	DES ▼
Privacy Key	(8~31 characters)

SNMP: Activate to enable SNMP.

Get Community: Type the Get Community, which is the password for the incoming Get-and-GetNext requests from the management station.

Set Community: Type the Set Community, which is the password for incoming Set requests from the management station.

Trap Manager IP: Enter the IP of the server receiving the trap message (when some exception occurs) sent by this SNMP agent.

System Name / Location / Contact: String descriptions of the SNMP agent.

Interface: Select the access interface. Choices are **LAN** or **ALL** (Both LAN and WAN).

SNMPv3

SNMPv3: Enable to activate the SNMPv3.

Username: Enter the name allowed to access the SNMP agent.

Access Permissions: Set the access permissions for the user; RO--read only and RW--read and writer.

Authentication Protocol: Select the authentication protocol, MD5 and SHA. SNMP agent can communicate with the manager station through authentication and encryption to secure the message exchange. Set the authentication and encryption information here and below.

Authentication Key: Set the authentication key, 8-31 characters.

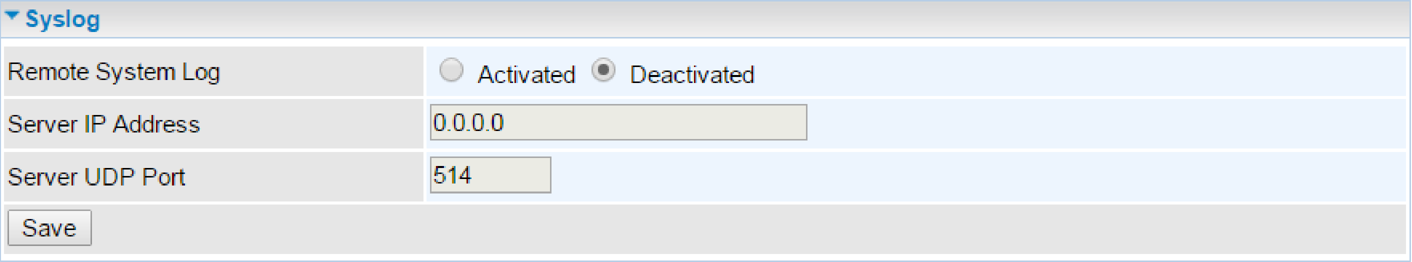
Privacy Protocol: Select the privacy mode, DES and AES.

Privacy Key: Set the privacy key, 8-31 characters.

Click **Save** to apply settings.

Syslog (System Log)

Use the Syslog to collect system event information to a remote log server.



▾ Syslog

Remote System Log	○ Activated ● Deactivated
Server IP Address	0.0.0.0
Server UDP Port	514

Remote System Log: Select **Activated** to enable this feature

Server IP Address: Assign the remote log server IP address.

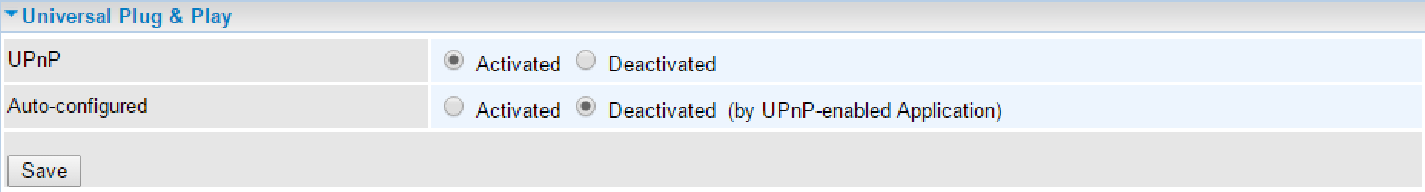
Server UDP Port: Assign the remote log server port, 514 is commonly used.

Click **Save** to apply settings.

Universal Plug & Play

UPnP offers peer-to-peer network connectivity for PCs and other network devices, along with control and data transfer between devices. UPnP offers many advantages for users running NAT routers through UPnP NAT Traversal, and on supported systems makes tasks such as port forwarding much easier by letting the application control the required settings, removing the need for the user to control advanced configuration of their device.

Both the user’s Operating System and the relevant application must support UPnP in addition to the router.



Universal Plug & Play

UPnP	● Activated ○ Deactivated
Auto-configured	○ Activated ● Deactivated (by UPnP-enabled Application)

UPnP: Select this checkbox to activate UPnP. Be aware that anyone could use an UPnP application to open the web configuration’s login screen without entering the BEC 4700A/AZ's IP address

Auto-configured: Select this check box to allow UPnP-enabled applications to automatically configure the BEC 4700A/AZ so that they can communicate through the BEC 4700A/AZ, for example by using NAT traversal, UPnP applications automatically reserve a NAT forwarding port in order to communicate with another UPnP enabled device; this eliminates the need to manually configure port forwarding for the UPnP enabled application.

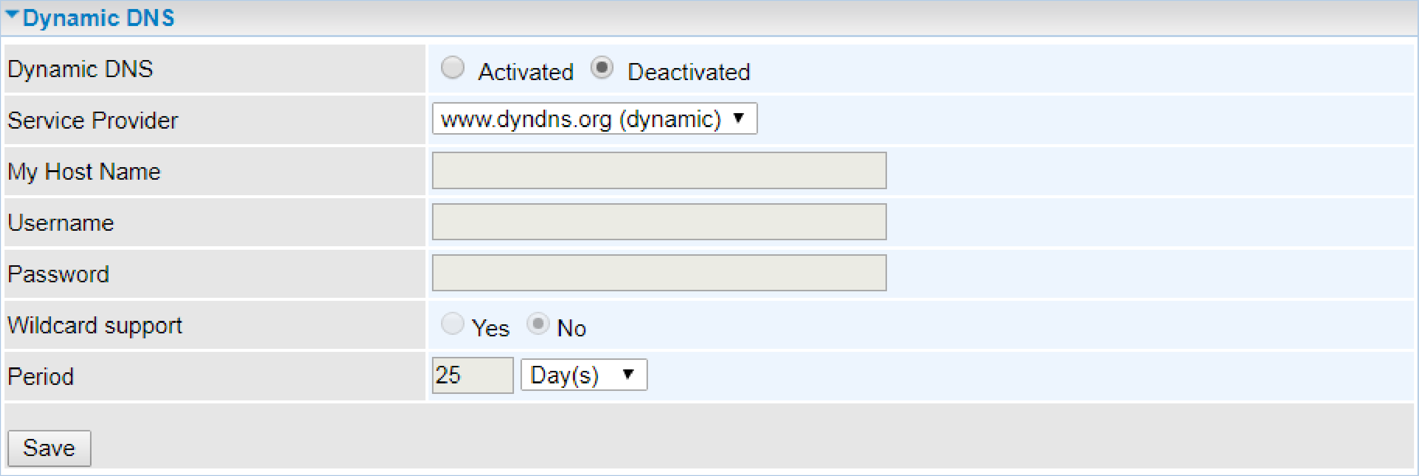
Click **Save** to apply settings.

Dynamic DNS (DDNS)

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your internet connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

Here users can register different WAN interfaces with different DNS Providers.

If you do not have a DDNS account, please choose a DDNS Service Provider from the list then go to their website to create an account first.



▾Dynamic DNS

Dynamic DNS	○ Activated ● Deactivated
Service Provider	www.dyndns.org (dynamic) ▼
My Host Name	
Username	
Password	
Wildcard support	○ Yes ● No
Period	25 Day(s) ▼

Dynamic DNS: Select this check box to activate Dynamic DNS.

Service Provider: Select from drop-down menu for the appropriate service provider, for example: www.dyndns.org.

My Host Name: Type the domain name assigned to your BEC 4700A/AZ by your Dynamic DNS provider.

Username / Password: Enter the username and password of the account you created with this service provider.

Wildcard support: Select this check box to enable DYNDNS Wildcard.

Period: Set the time period on how often the BEC 4700A/AZ will update the DDNS server with your current external IP address.

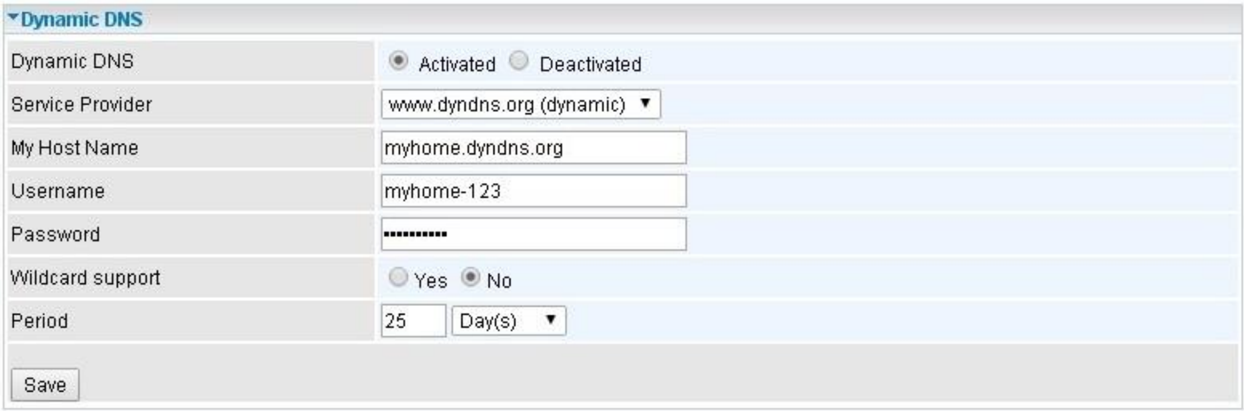
Click **Save** to apply settings.

Example: How to register a DDNS account

If you do not have an account with Dynamic DNS, please go to www.dyndns.org to register an account first.

User ***test1*** register a Dynamic Domain Names in DDNS provider **http://www.dyndns.org/** .

DDNS: www.hometest.com using username/password test/test



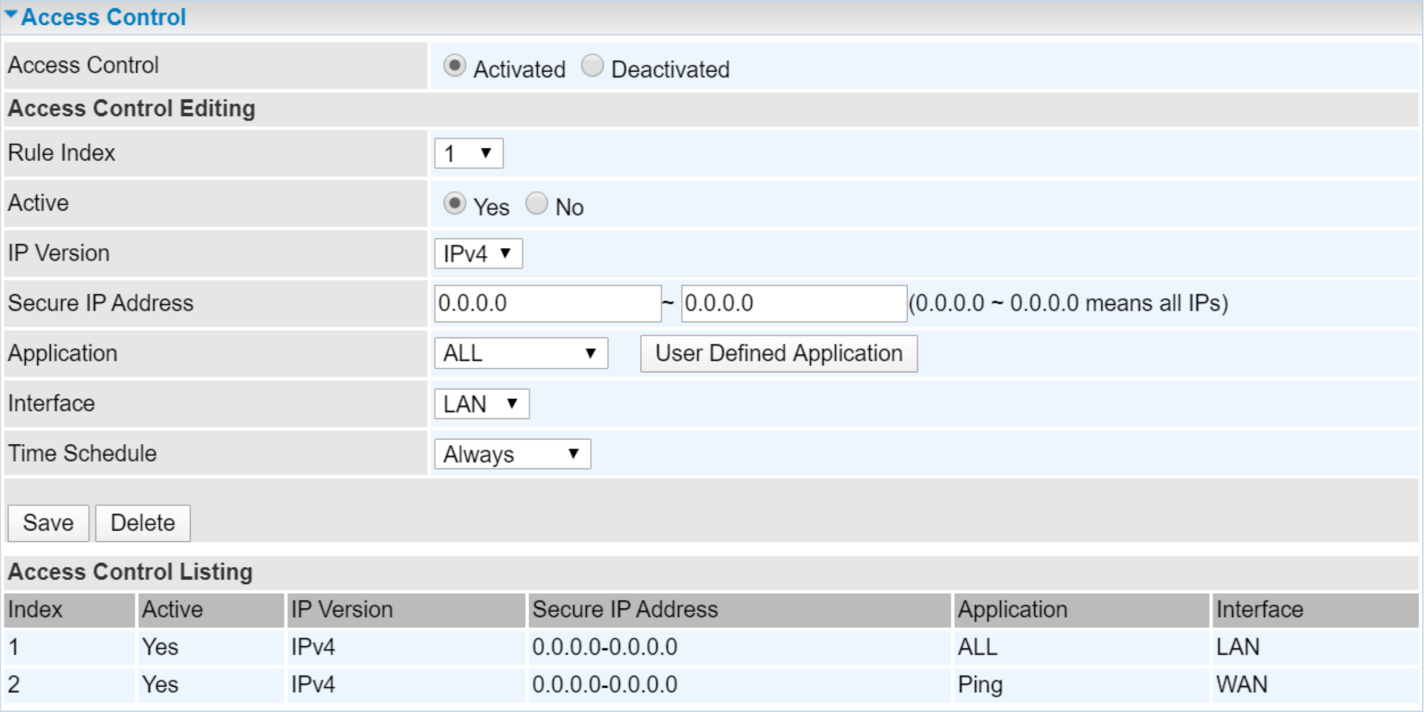
▾Dynamic DNS

Dynamic DNS	● Activated ○ Deactivated
Service Provider	www.dyndns.org (dynamic) ▼
My Host Name	myhome.dyndns.org
Username	myhome-123
Password	••••••••••
Wildcard support	○ Yes ● No
Period	25 Day(s) ▼

Access Control

Access Control Listing allows you to determine which services/protocols can access your BEC 4700A/AZ interface from which computers. It is a management tool aimed to allow IPs (set in secure IP address) to access specified embedded applications (Web, etc., user can set) through some specified interface (LAN, WAN or both). User can have an elaborate understanding in the examples below.

The maximum number of entries is **16**.



▾Access Control

Access Control	● Activated ○ Deactivated
Access Control Editing	
Rule Index	1 ▾
Active	● Yes ○ No
IP Version	IPv4 ▾
Secure IP Address	0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application	ALL ▾ User Defined Application
Interface	LAN ▾
Time Schedule	Always ▾

Access Control Listing

Index	Active	IP Version	Secure IP Address	Application	Interface
1	Yes	IPv4	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	IPv4	0.0.0.0-0.0.0.0	Ping	WAN

Access Control: Click **Activate** to enable the Access Control function.

Rule Index: The numeric rule indicator.

Active: Yes to activate the rule.

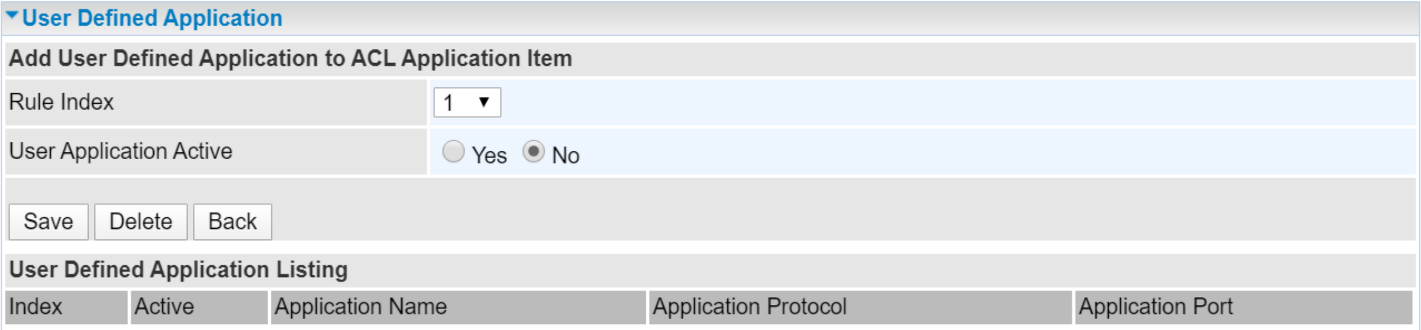
Secure IP Address: The default 0.0.0.0 allows any client to use this service to manage the 4700A/AZ. Type an IP address range to restrict access to the client(s) without a matching IP address.

Application: Choose a service that you want to all access to all the secure IP clients. The drop-down menu lists all the commonly used applications or manually create an application.

Interface: Select the access interface. Choices are **LAN**, **WAN**, **GRE** and **ALL**.

Click **Save** to apply settings.

User Defined Application



▾User Defined Application

Add User Defined Application to ACL Application Item

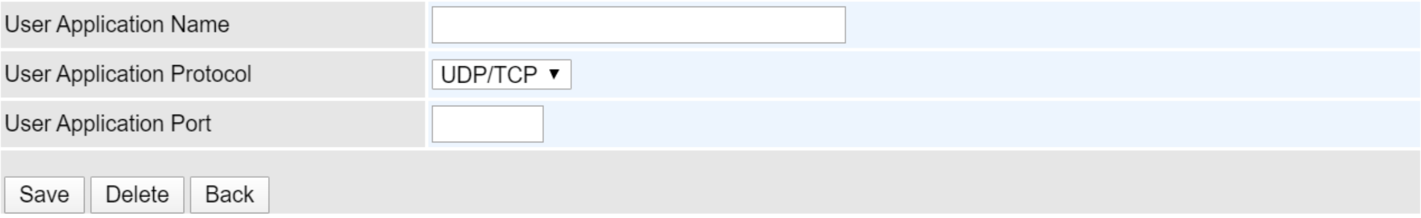
Rule Index	1 ▼
User Application Active	○ Yes ● No

User Defined Application Listing

Index	Active	Application Name	Application Protocol	Application Port

Rule Index: The numeric rule indicator.

User Application Active: Yes to add a new rule.



User Application Name	
User Application Protocol	UDP/TCP ▼
User Application Port	

User Application Name: A self-define name to identify the application.

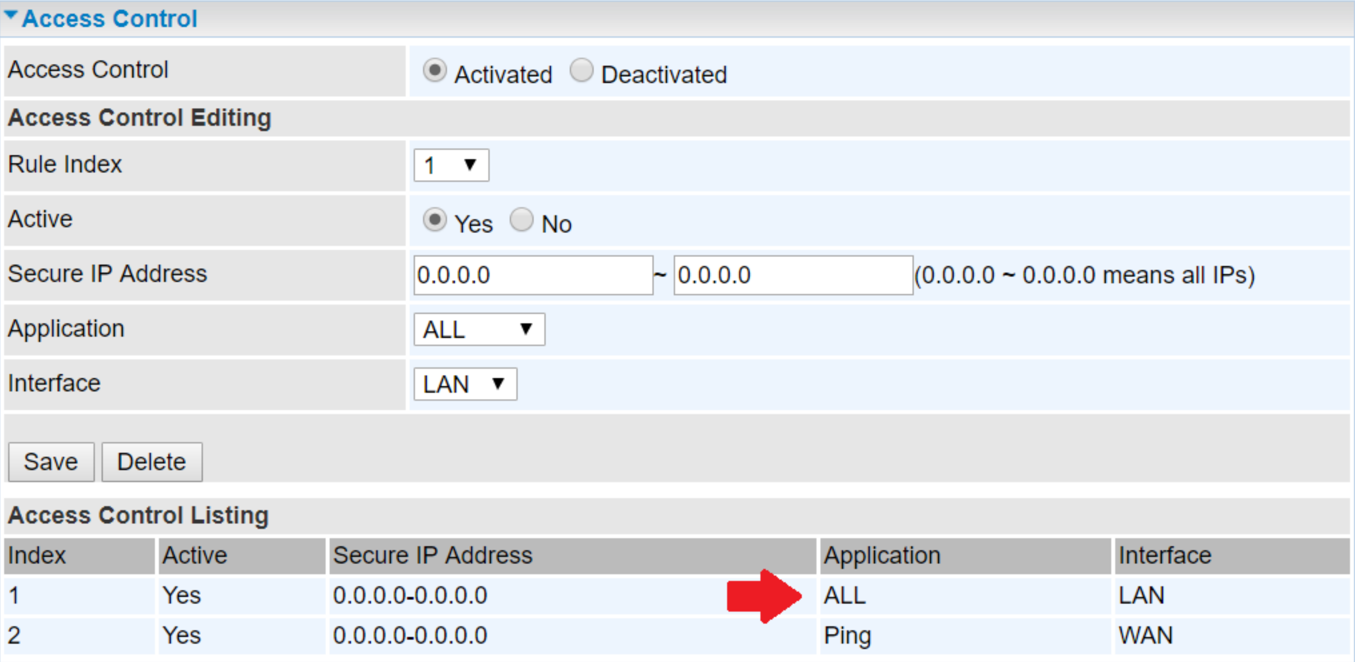
User Application Protocol: Enter a protocol, TCP, UDP, UDP/TCP, to use for this application.

User Application Port: Enter the port number which defines the application.

Click **Save** to save the rule.

By default, the "Access Control" has **two default rules**.

Default Rule 1: (Index 1), a rule to allow only clients from LAN to have access to all embedded applications (Web, FTP, etc.). Under this situation, clients from WAN cannot access the router even from Ping.



▾Access Control

Access Control	● Activated ○ Deactivated

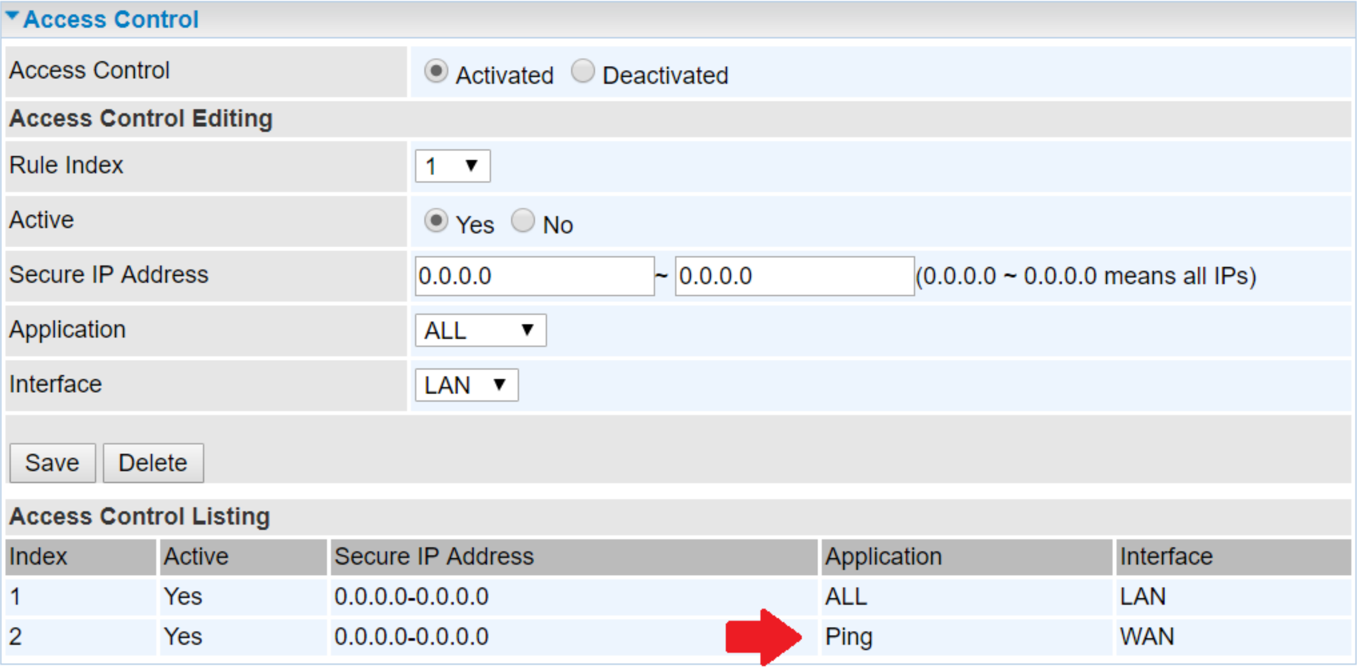
Access Control Editing

Rule Index	1 ▼
Active	● Yes ○ No
Secure IP Address	0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application	ALL ▼
Interface	LAN ▼

Access Control Listing

Index	Active	Secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Default Rule 2: (Index 2), an ACL rule to open Ping to WAN side.



Access Control

Access Control	● Activated ○ Deactivated
Access Control Editing	
Rule Index	1 ▼
Active	● Yes ○ No
Secure IP Address	0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application	ALL ▼
Interface	LAN ▼

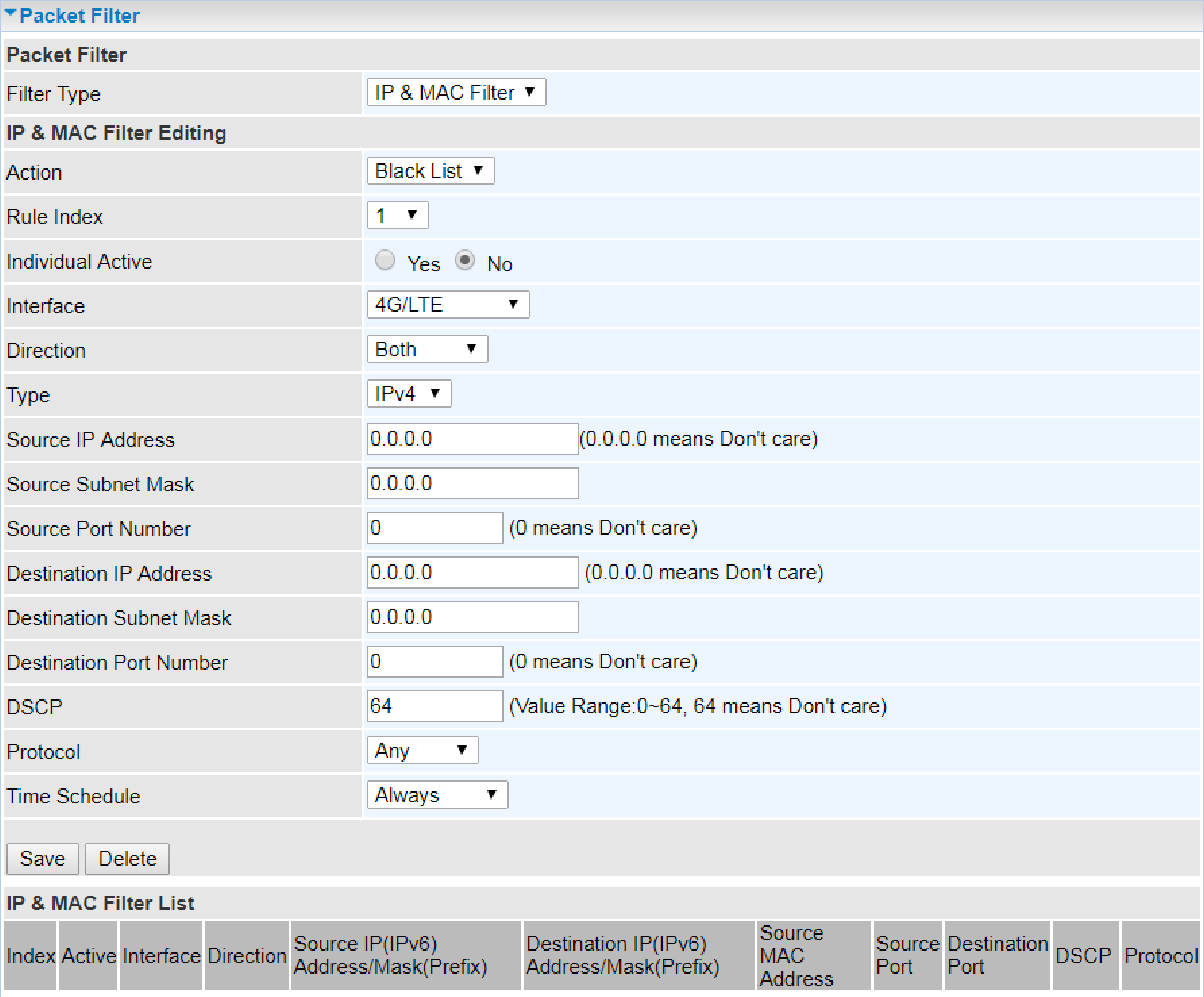
Access Control Listing

Index	Active	Secure IP Address	Application	Interface
1	Yes	0.0.0.0-0.0.0.0	ALL	LAN
2	Yes	0.0.0.0-0.0.0.0	Ping	WAN

Packet Filter

You can filter the packages by MAC address, IP address, Protocol, Port number and Application or URL.

❖ Packet Filter - IP & MAC Filter



▾Packet Filter

Packet Filter

Filter Type	IP & MAC Filter ▾

IP & MAC Filter Editing

Action	Black List ▾
Rule Index	1 ▾
Individual Active	○ Yes ● No
Interface	4G/LTE ▾
Direction	Both ▾
Type	IPv4 ▾
Source IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Source Subnet Mask	0.0.0.0
Source Port Number	0 (0 means Don't care)
Destination IP Address	0.0.0.0 (0.0.0.0 means Don't care)
Destination Subnet Mask	0.0.0.0
Destination Port Number	0 (0 means Don't care)
DSCP	64 (Value Range:0~64, 64 means Don't care)
Protocol	Any ▾
Time Schedule	Always ▾

IP & MAC Filter List

Index	Active	Interface	Direction	Source IP(IPv6) Address/Mask(Prefix)	Destination IP(IPv6) Address/Mask(Prefix)	Source MAC Address	Source Port	Destination Port	DSCP	Protocol

IP & MAC Filter Editing

Rule Index: The indication of the rule number.

Individual Active: Yes to enable the rule.

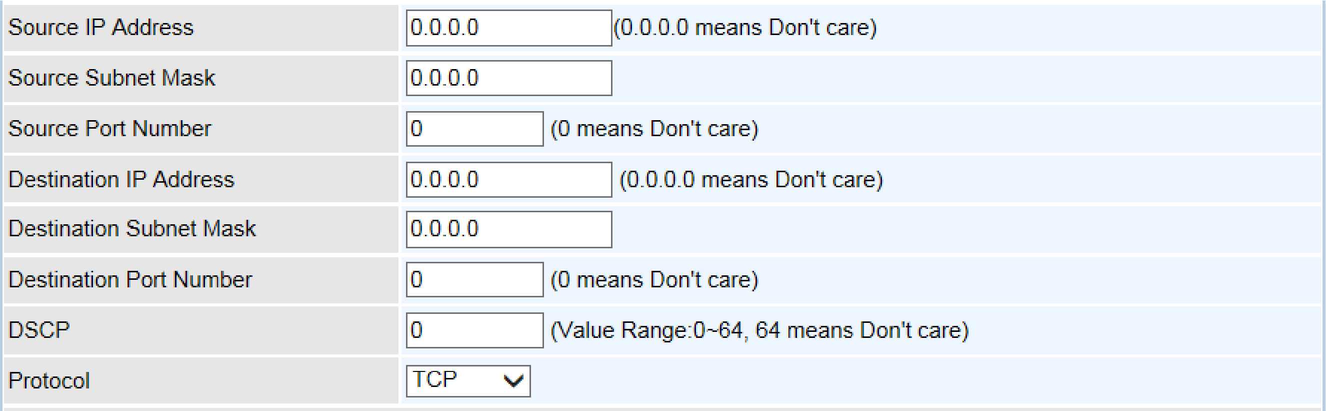
Action: This is how to deal with the packets matching the rule. Allow please select White List or Black selecting Blacklist.

Interface: Select to determine which interface the rule will be applied to.

Direction: Select to determine whether the rule applies to outgoing packets, incoming packets or packets of both directions.

Type: Choose type of field you want to specify to monitor. Select “IPv4” for IPv4 address, port number and protocol. Select “IPv6” for IPv6 address, port number and protocol. Select “MAC” to enter a source MAC address”.

IPv4



Source IP Address	0.0.0.0	(0.0.0.0 means Don't care)
Source Subnet Mask	0.0.0.0	
Source Port Number	0	(0 means Don't care)
Destination IP Address	0.0.0.0	(0.0.0.0 means Don't care)
Destination Subnet Mask	0.0.0.0	
Destination Port Number	0	(0 means Don't care)
DSCP	0	(Value Range:0~64, 64 means Don't care)
Protocol	TCP	

Source IP Address: The source IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.

Source Subnet Mask: Enter the subnet mask of the source network.

Source Port Number: The source port number of packets to be monitored. 0 means “Don’t care”.

Destination IP Address: The destination IP address of packets to be monitored. 0.0.0.0 means “Don’t care”.

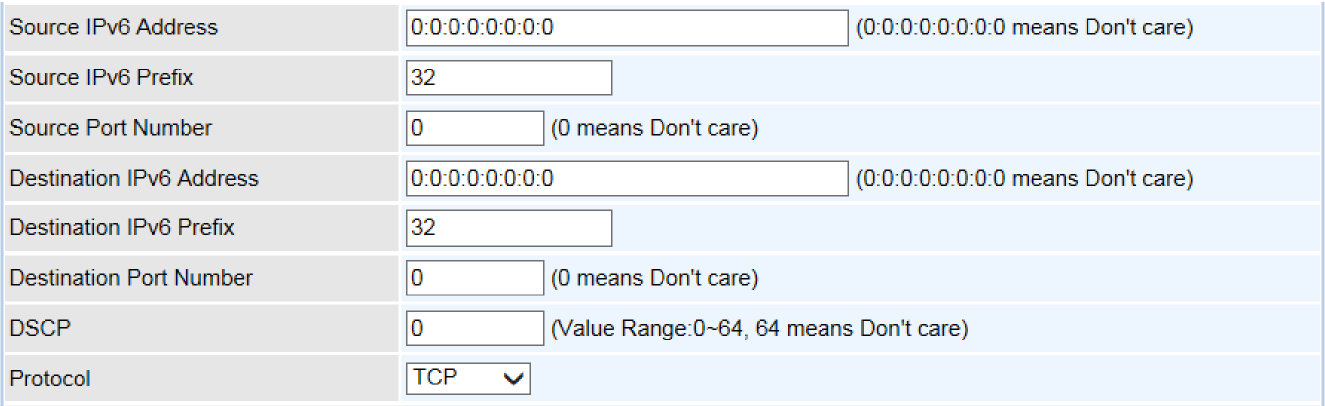
Destination Subnet Mask: Enter the subnet mask of the destination network.

Destination Port Number: This is the Port that defines the application. (E.g. HTTP is port 80.)

DSCP: Differentiated Services Code Point, it is recommended that this option be configured by an advanced user or keep 0. (0 means Don’t care.)

Protocol: Specify the packet type (TCP, UDP, ICMP, and ICMPv6) that the rule applies to.

IPv6



Source IPv6 Address	0:0:0:0:0:0:0:0	(0:0:0:0:0:0:0:0 means Don't care)
Source IPv6 Prefix	32	
Source Port Number	0	(0 means Don't care)
Destination IPv6 Address	0:0:0:0:0:0:0:0	(0:0:0:0:0:0:0:0 means Don't care)
Destination IPv6 Prefix	32	
Destination Port Number	0	(0 means Don't care)
DSCP	0	(Value Range:0~64, 64 means Don't care)
Protocol	TCP	

Source IP (IPv6) Address/ Prefix: The source IP address or range of packets to be monitored.

Source Port Number: The source port number of packets to be monitored.

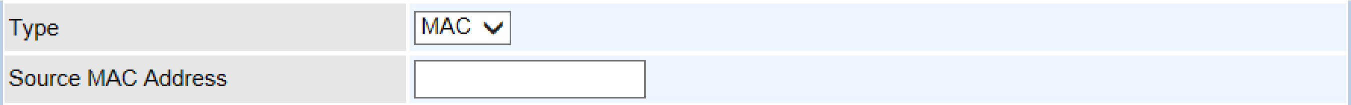
Destination IP (IPv6) Address/ Prefix: The destination subnet IP address.

Destination Port Number: This is the Port or Port Ranges that defines the application.

DSCP: show the set DSCP.

Protocol: It is the packet protocol type used by the application. Select either **TCP** or **UDP** or **ICMP or ICMPv6 .**

MAC



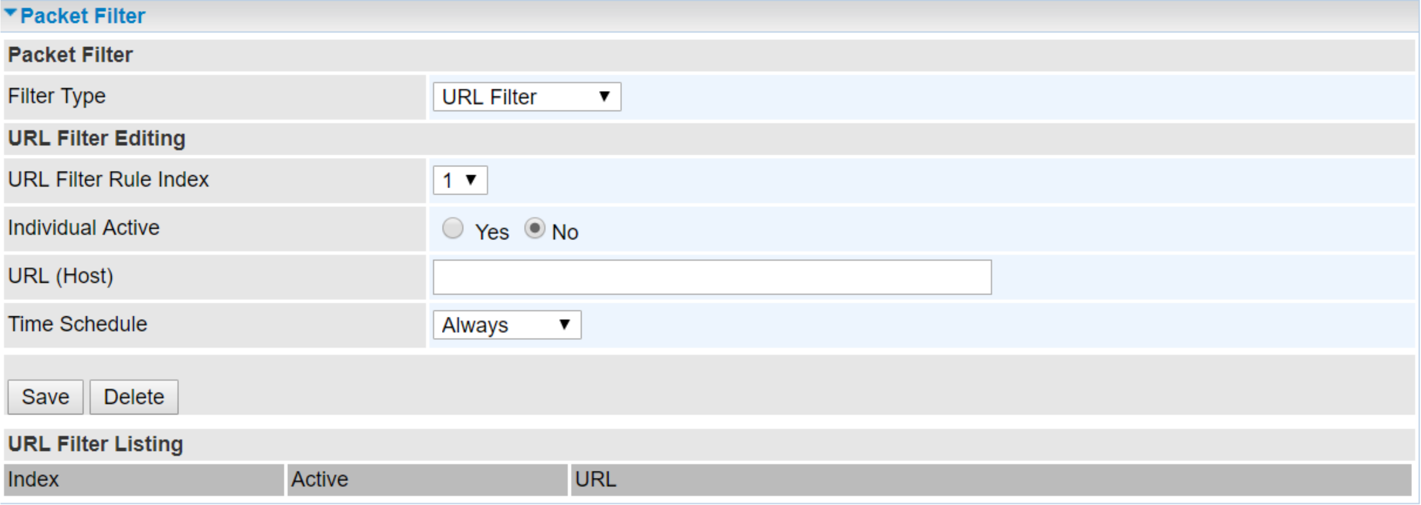
Type	MAC
Source MAC Address	

Source MAC Address: show the MAC address of the rule applied.

Time Schedule: Select a TimeSlot to activate the rule. Go to **Time Schedule** to configure a time control first.

Click **Save** to apply settings.

Filter Type - URL Filter



Packet Filter

Packet Filter	
Filter Type	URL Filter ▼
URL Filter Editing	
URL Filter Rule Index	1 ▼
Individual Active	○ Yes ● No
URL (Host)	
Time Schedule	Always ▼

URL Filter Listing

Index	Active	URL

URL Filter Rule Index: The indication of the rule number.

Individual Active: Click **Yes** to enable this rule/policy.

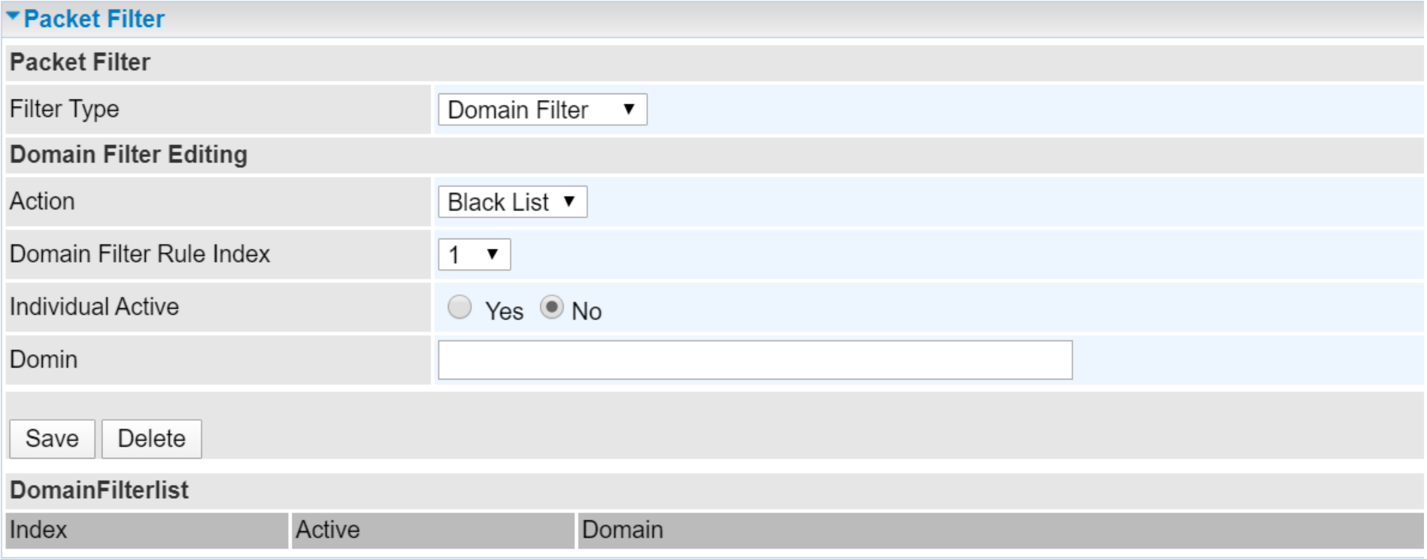
Domain: Enter the domain name in the blank field to be allowed or prohibited.

URL (Host): Enter the specific URL in the blank field to be blocked.

Time Schedule: Select a TimeSlot to activate the rule. Go to **Time Schedule** to configure a time control first.

Click **Save** to apply settings.

❖ Filter Type - Domain Filter



▾Packet Filter

Packet Filter	
Filter Type	Domain Filter ▼
Domain Filter Editing	
Action	Black List ▼
Domain Filter Rule Index	1 ▼
Individual Active	○ Yes ● No
Domin	

DomainFilterlist

Index	Active	Domain

Action: This is how to deal with the packets matching the rule. Allow please select White List or Black selecting Blacklist.

Domain Filter Rule Index: The indication of the rule number.

Individual Active: Click **Yes** to enable this rule/policy.

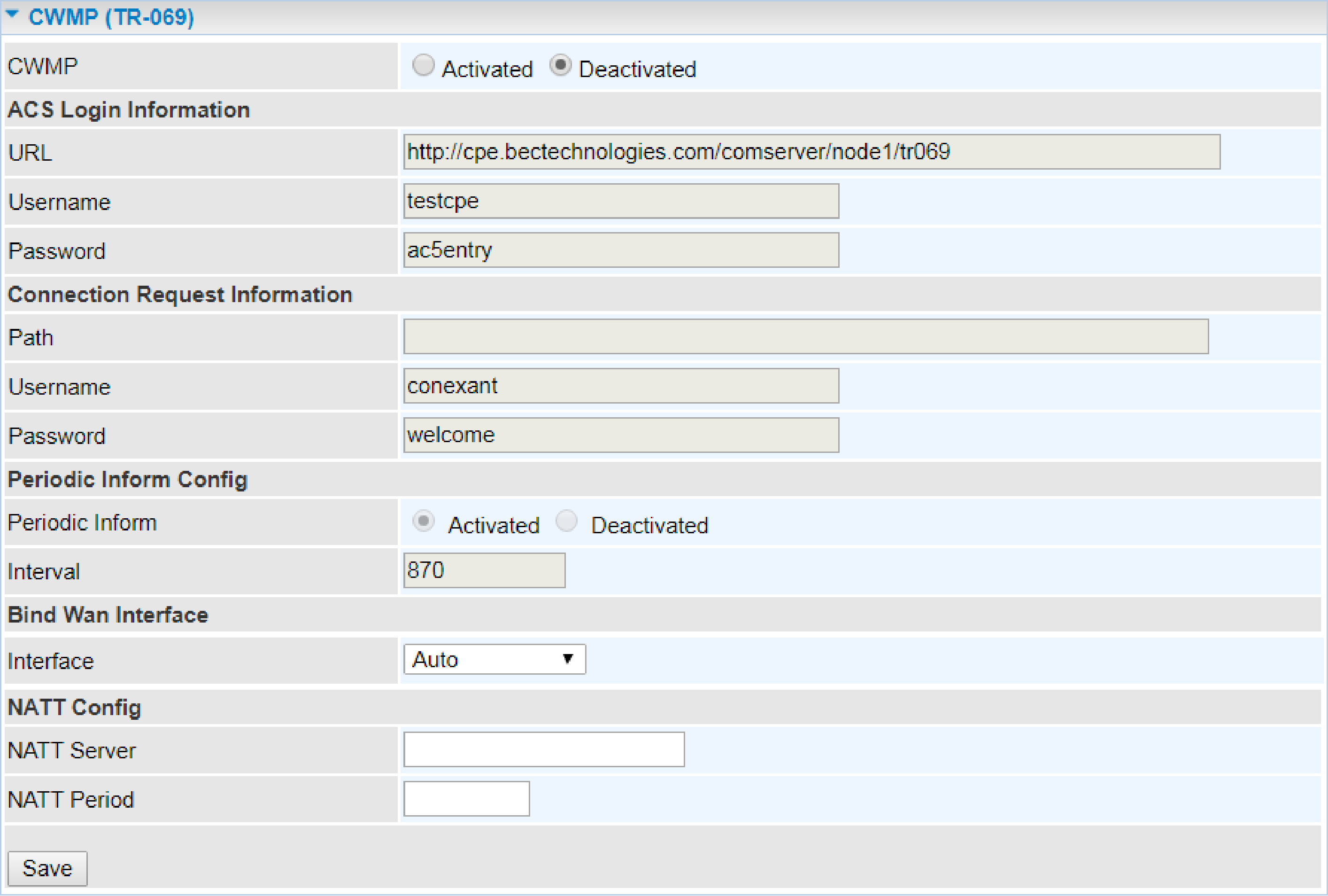
Domain: Enter the domain name in the blank field to be allowed or prohibited.

Click **Save** to apply settings.

CWMP (TR-069)

CWMP, short for CPE WAN Management Protocol, also called TR069 is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. It defines an application layer protocol for remote management of end-user devices.

As a bidirectional SOAP/HTTP based protocol it can provides the communication between customer premises equipment (CPE) and Auto Configuration Server (ACS). It includes both a safe configuration and the control of other CPE management functions within an integrated framework. In the course of the booming broadband market, the number of different internet access possibilities grew as well (e.g. modems, routers, gateways, set-top box, VoIP-phones).At the same time the configuration of this equipment became more complicated –too complicated for end-users. For this reason, TR-069 was developed. It provides the possibility of auto configuration of the access types. Using TR-069 the terminals can get in contact with the Auto Configuration Servers (ACS) and establish the configuration automatically and let ACS configure CPE automatically.



CWMP (TR-069)

CWMP	○ Activated ● Deactivated
ACS Login Information	
URL	http://cpe.bectechnologies.com/comserver/node1/tr069
Username	testcpe
Password	ac5entry
Connection Request Information	
Path	
Username	conexant
Password	welcome
Periodic Inform Config	
Periodic Inform	● Activated ○ Deactivated
Interval	870
Bind Wan Interface	
Interface	Auto ▼
NATT Config	
NATT Server	
NATT Period	

CWMP: Select activated to enable CWMP.

ACS Login Information

URL: Enter the ACS server login URL.

Username: Specify the ACS Username for ACS authentication to the connection from CPE.

Password: Enter the ACS server login password.

Connection Request Information

Path: Local path in HTTP URL for an ACS to make a Connection Request notification to the CPE.

Username: Username used to authenticate an ACS making a Connection Request to the CPE.

Password: Password used to authenticate an ACS making a Connection Request to the CPE.

Periodic Inform Config

Periodic Inform: Select Activated to authorize the router to send an Inform message to the ACS automatically.

Interval(s): Specify the inform interval time (sec) which CPE used to periodically send inform message to automatically connect to ACS. When the inform interval time arrives, the CPE will send inform message to automatically connect to ACS.

Bind WAN Interface

Interface: Specify any available or a single WAN interface to handle TR-069 requests.

NATT Config - This is a proprietary feature provided by BEC. May leave them in blank, no configuration is required.

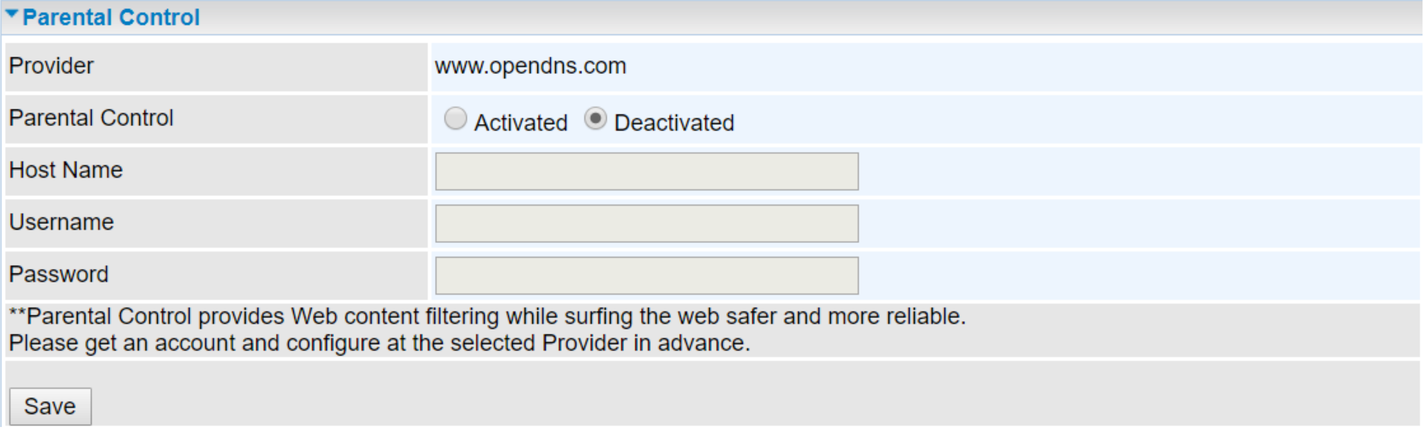
NATT Server: By BEC administrator only.

NATT Period: By BEC administrator only.

Click **Save** to apply settings

Parental Control

This feature provides Web content filtering offering safer and more reliable web surfing for users especially for parents to protect network security and control the contents for children at home.



Provider	www.opendns.com
Parental Control	○ Activated ● Deactivated
Host Name	
Username	
Password	

**Parental Control provides Web content filtering while surfing the web safer and more reliable.
Please get an account and configure at the selected Provider in advance.

To activate this feature, please log on to www.opendns.com to get an OpenDNS account first.

Parent Control Provider: Hosted by www.opendns.com

Parent Control: Enable the feature by clicking the **Activate**d

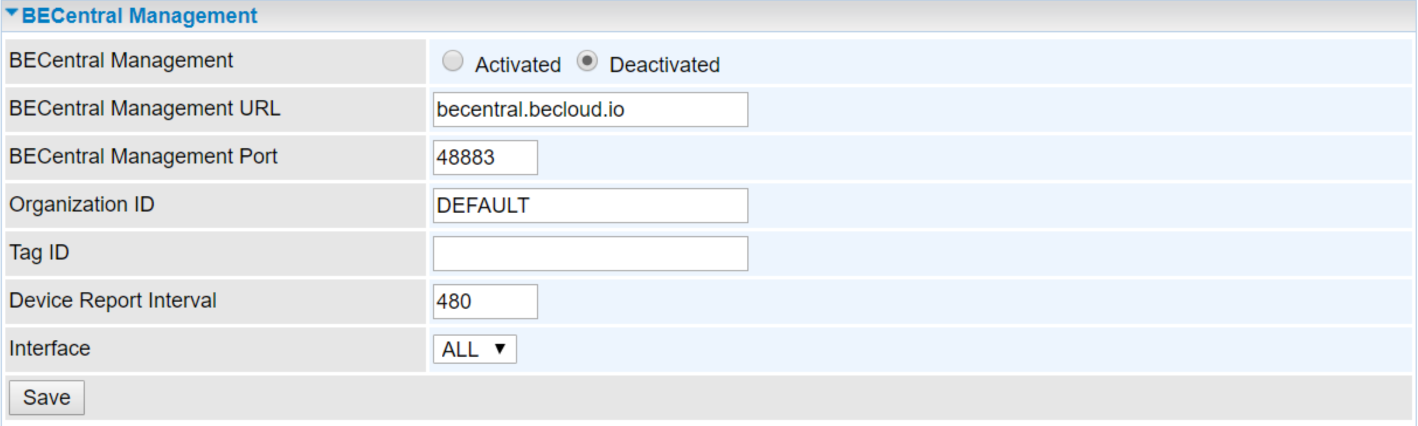
Host Name: It is the domain name of your OpenDNS. If you don’t have one, please leave it blink.

Username / Password: Put down your OpenDNS account username and password

Click **Save** to apply settings.

BECentral Management

BECentral is a cloud-based device management platform that provides operators with a comprehensive suite of services to manage devices in real-time.



BECentral Management	○ Activated ● Deactivated
BECentral Management URL	becentral.becloud.io
BECentral Management Port	48883
Organization ID	DEFAULT
Tag ID	
Device Report Interval	480
Interface	ALL ▼

BECentral Management: Activate to enable the feature.

BECentral Management URL: Access path to the BECentral.

BECentral Management Port: Port listened by the BECentral.

Organization ID: Customer ID (By BE C administrator only)

Tag ID: By BEC administrator only.

Device Report Interval: Enter the interval time in seconds to send inform message periodically to the BECentral.

Interface: Specify any available or a single WAN interface to handle BECentral requests.

Click **Save** to apply settings.

Maintenance

Maintenance equipment the users with the ability of maintaining the device as well as examining the connectivity of the WAN connections, including User Management, Certificate Management, Time Zone, License, Firmware & Configuration, System Restart, Auto Reboot and Diagnostic Tool.

User Management

User Management provides the Administrator with the ability to grant access control and manage GUI login credentials for each user.

There are two access management levels, Administrator and User.

The default root account, Administrator (admin), has full access to all the features listed and ability to create other accounts with features to allow other users to access to. The User account is with limited access (specified by advanced users with admin account) to the GUI.

Total of **8** accounts can be created to grant access to manage the BEC 4700A/AZ via the web page.

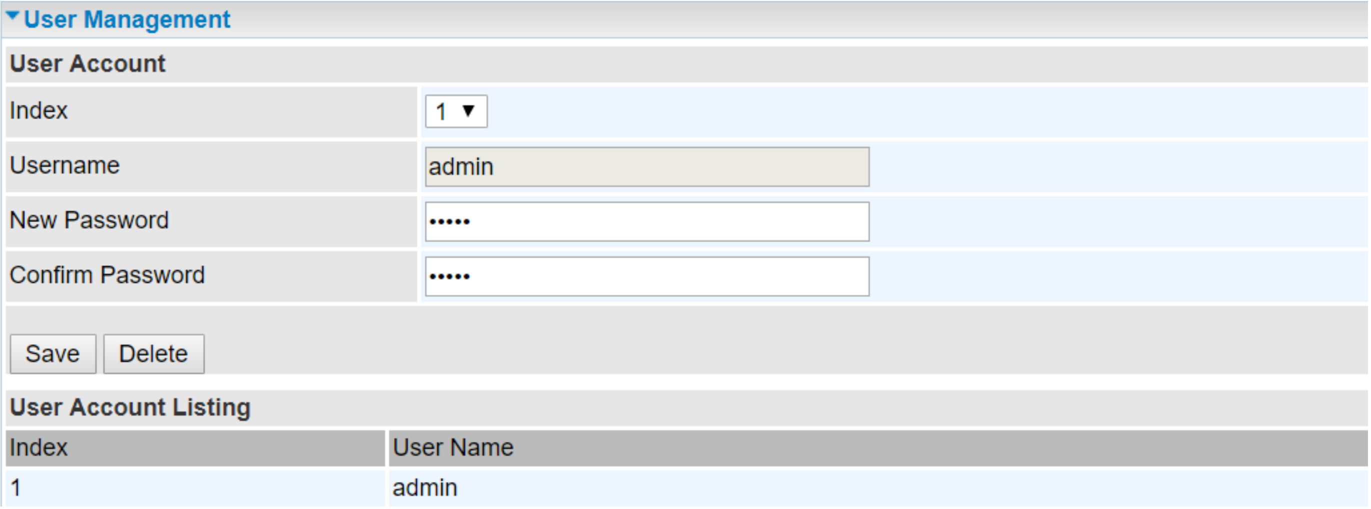
❖ Administrator Account

admin/admin is the root/default account username and password.

NOTE: This username / password may vary by different Internet Service Providers.

Login using the Administrator account, you will have the full accessibility to manage & control your gateway device and can also create user accounts for others to control some of the open configuration settings.

The Administrator account cannot be deleted or removed.



User Management

User Account

Index	1 ▼
Username	admin
New Password	•••••
Confirm Password	•••••

User Account Listing

Index	User Name
1	admin

User Account

Index: The indication of the rule number. The maximum entry is up to 8 accounts.

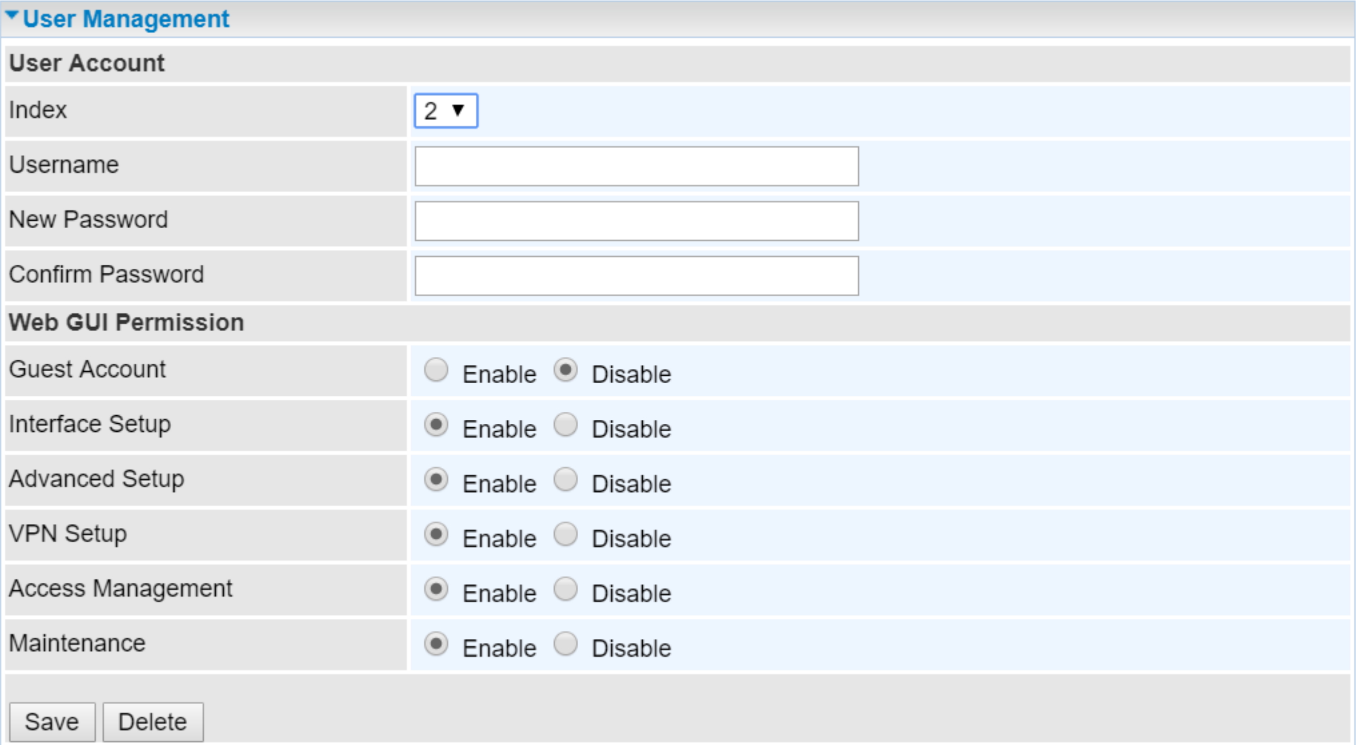
Username: Create account(s) username for GUI management.

New Password: Enter a new password for this user account.

Confirmed Password: Re-enter the new password again; you must enter the password exactly the same as in the previous field.

Click **Save** to apply settings.

❖ Creating Other User Accounts



▾User Management

User Account	
Index	2 ▼
Username	
New Password	
Confirm Password	
Web GUI Permission	
Guest Account	○ Enable ● Disable
Interface Setup	● Enable ○ Disable
Advanced Setup	● Enable ○ Disable
VPN Setup	● Enable ○ Disable
Access Management	● Enable ○ Disable
Maintenance	● Enable ○ Disable

User Account Setup

Index #: The indication of the rule number. The maximum entry is up to 8.

Username: Create account(s) username for GUI management.

New Password: Password for the user account.

Confirm Password: Re-enter the password.

Web GUI Permission

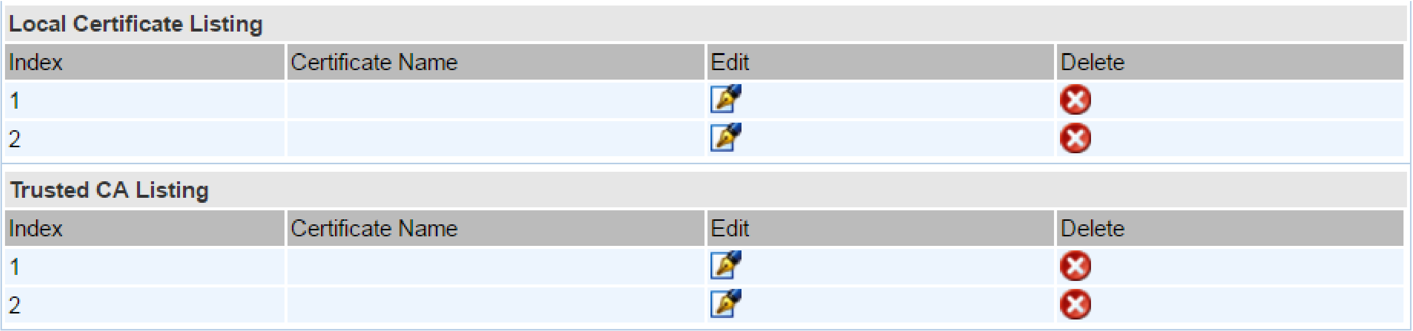
Guest Account: Enable to create this new guest account and select features to allow user account to access to.

When someone accesses to your BEC 4700A/AZ using this "user" account, he/she can only manage and configure the features that is pre-selected in **Web GUI Permission** for this account.

Click **Save** to apply settings.

Certificate Management

This feature is used for OpenVPN and HTTPS Server authentication of the device using certificate. If the imported certificate doesn't match the authorized certificate with the Server, then no access is allowed.



Local Certificate Listing

Index	Certificate Name	Edit	Delete
1		✎	✖
2		✎	✖

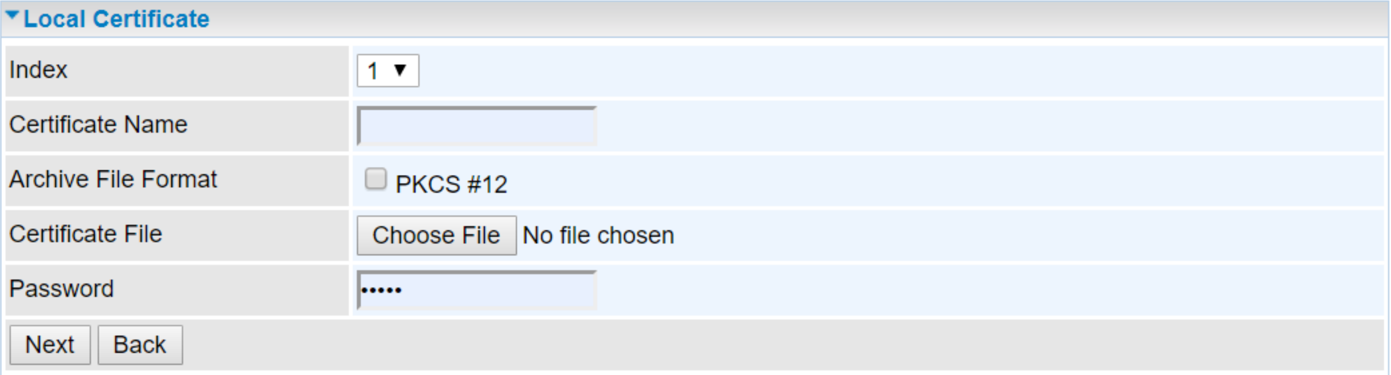
Trusted CA Listing

Index	Certificate Name	Edit	Delete
1		✎	✖
2		✎	✖

Edit: Click ✎ (Edit) to import a certificate.

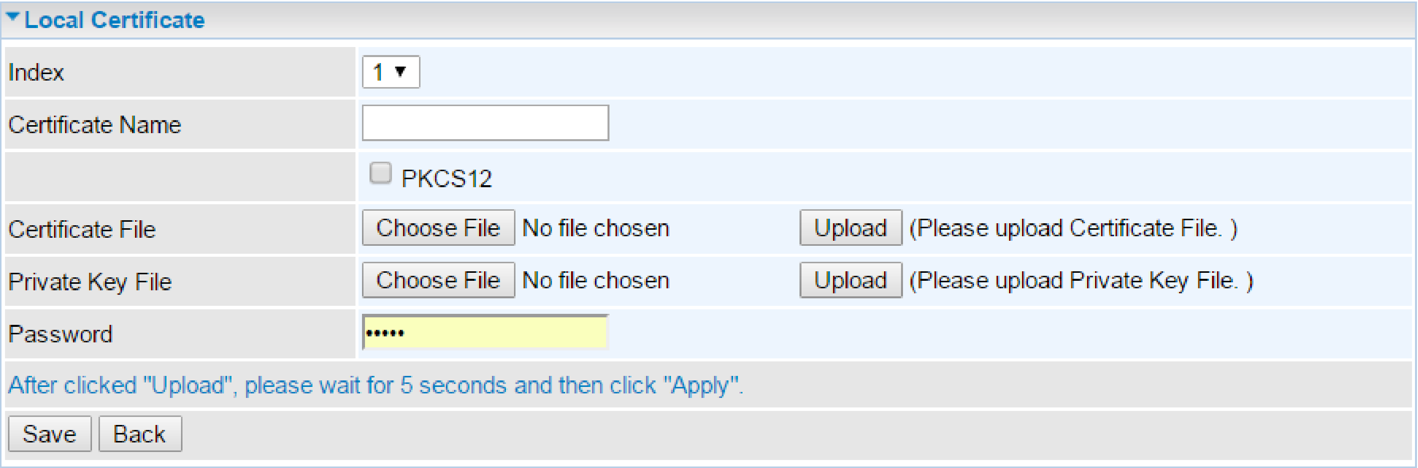
Delete: Click ✖ (Delete) to remove the certificate from the list.

Local Certificate Listing



▼Local Certificate

Index	1 ▼
Certificate Name	
Archive File Format	□ PKCS #12
Certificate File	Choose File No file chosen
Password	•••••



▼Local Certificate

Index	1 ▼	
Certificate Name		
	□ PKCS12	
Certificate File	Choose File No file chosen	Upload (Please upload Certificate File.)
Private Key File	Choose File No file chosen	Upload (Please upload Private Key File.)
Password	•••••	

After clicked "Upload", please wait for 5 seconds and then click "Apply".

Index #: The indication of the rule number. The maximum entry is up to 2.

Certificate Name: Description of the certificate.

Archive File Format (PKCS12): Every certificate is accompanied by a private key. Upload both files if PKCS is disabled. Enable PKCS12 to put Certificate & Private Key in the same file, like *.p12, *.pfx.

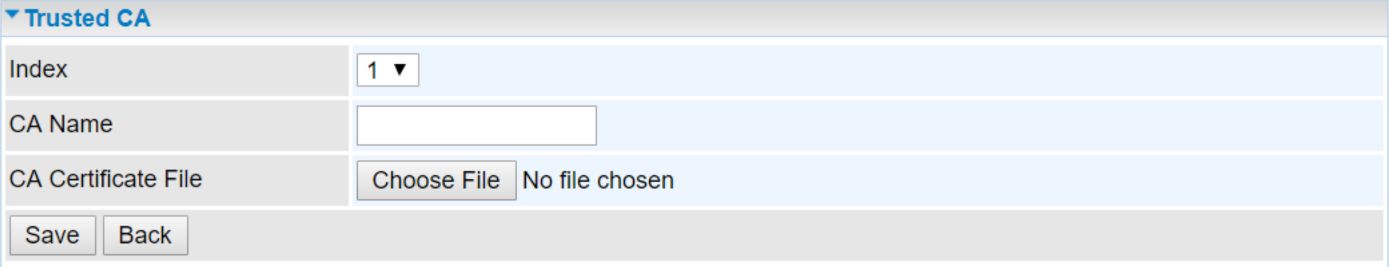
Certificate File: Browse to locate the target certificate file on PC before uploading it.

Private Key File: Browse to locate the target file on PC before uploading it. If PKCS enabled, please ignore this setting.

Password: Enter the password if any, which is used to protect the private key. Otherwise, leave it empty.

Click **Apply** to save settings.

Trusted CA Listing



Trusted CA

Index	1 ▼
CA Name	
CA Certificate File	Choose File No file chosen

Index #: The indication of the rule number. The maximum entry is up to 2.

CA Name: Description of the CA.

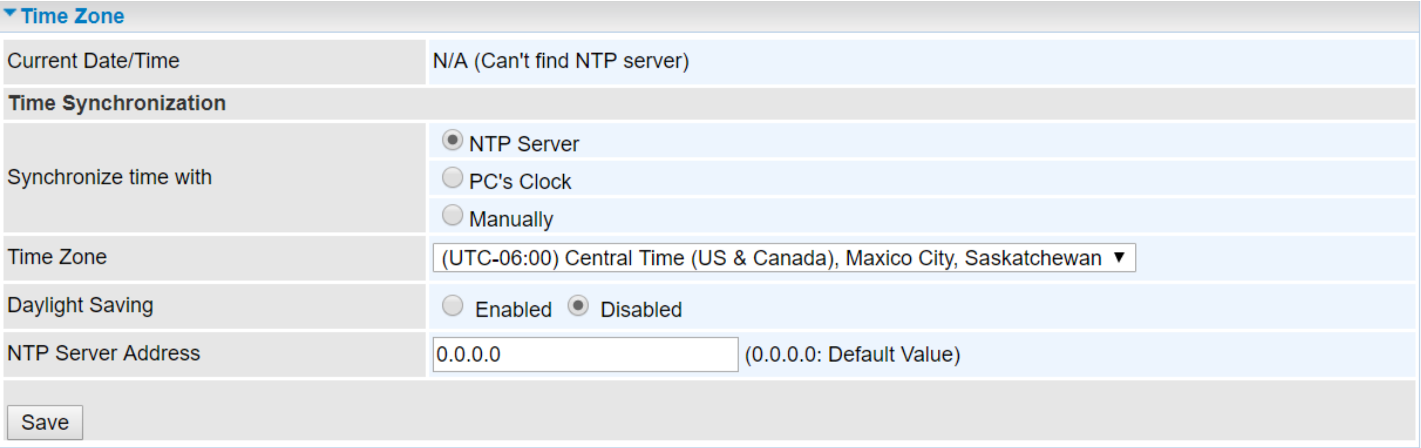
CA Certificate File: Browse to locate the target certificate file on PC before uploading it.

Click **Save** to save settings.

Time Zone

With default, BEC 4700A/AZ does not contain the correct local time and date.

There are several options to setup, maintain, and configure current local time/date on the BEC 4700A/AZ. If you plan to use **Time Schedule** feature, it is extremely important you set up the Time Zone correctly.



Time Zone

Current Date/Time	N/A (Can't find NTP server)
Time Synchronization	
Synchronize time with	● NTP Server ○ PC's Clock ○ Manually
Time Zone	(UTC-06:00) Central Time (US & Canada), Maxico City, Saskatchewan ▼
Daylight Saving	○ Enabled ● Disabled
NTP Server Address	0.0.0.0 (0.0.0.0: Default Value)

Synchronize time with: Select the methods to synchronize the time.

- **NTP Server automatically:** To synchronize time with the NTP servers to get the current time from an NTP server outside your network then choose your local time zone. After a successful connection to the Internet, BEC 4700A/AZ will retrieve the correct local time from the NTP server this is specified.
- **PC's Clock:** To synchronize time with the PC's clock.
- **Manually:** Select this to enter the SNMP server IP address manually.
  - **Date:** Month / Date / Year. Month – 1 ~ 12 (January ~ December).
  - **Time:** Hour: Minute: Second

Time Zone: Choose the time zone of your location. This will set the time difference between your time zone and Greenwich Mean Time (GMT).

Daylight Saving: Select this option if you use daylight savings time.

NTP Server Address: Enter the IP address of your time server. Check with your ISP/network administrator if you are unsure of this information.

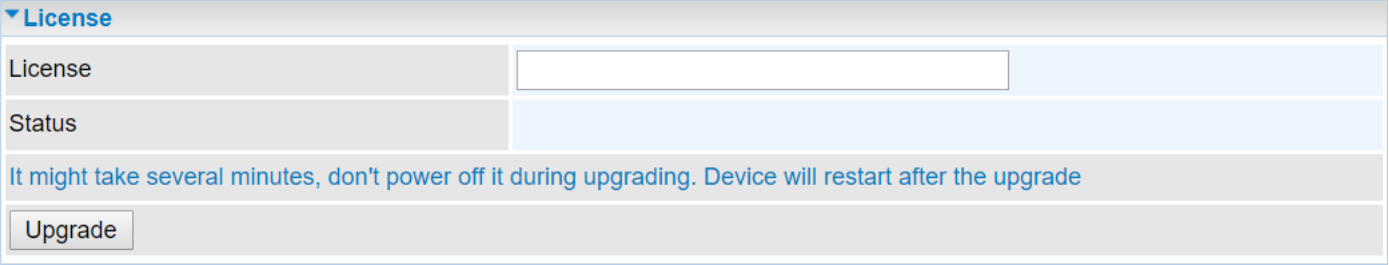
Click **Save** to apply settings

License

Some of the advanced features are required for a license. For more information, please contact with Billion/BEC for more information.

Input your license key here and click “Upgrade” to enable the features.

NOTE: Device will reboot after the upgrade.



▾License

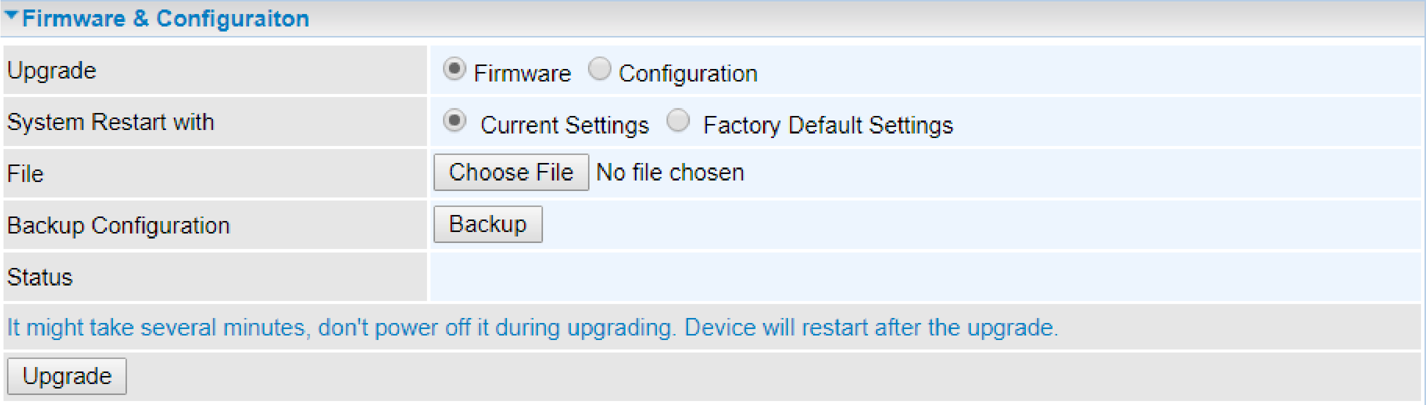
License	
Status	

It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade

Firmware & Configuration

Firmware is the software that controls the hardware and provides all functionalities which are available in the GUI. This software may be improved and/or modified; your BEC 4700A/AZ provides an easy way to update the code to take advantage of the changes. .

To upgrade the firmware of BEC 4700A/AZ, you should download or copy the firmware to your local environment first. Press the **"Browse…"** button to specify the path of the firmware file. Then, click **"Upgrade"** to start upgrading. When the procedure is completed, BEC 4700A/AZ will reset automatically to make the new firmware work.



Firmware & Configuraiton

Upgrade	● Firmware ○ Configuration
System Restart with	● Current Settings ○ Factory Default Settings
File	Choose File No file chosen
Backup Configuration	Backup
Status	

It might take several minutes, don't power off it during upgrading. Device will restart after the upgrade.

Upgrade

Upgrade: Choose Firmware or Configuration you want to update.

System Restart with:

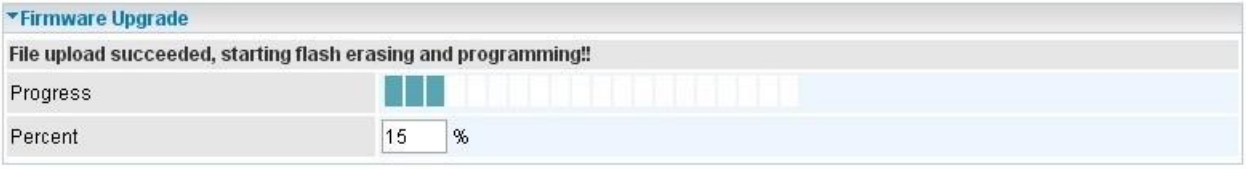
- **Current Settings:** Restart the device with the current settings automatically when finishing upgrading.
- **Factory Default Settings:** Restart the device with factory default settings automatically when finishing upgrading.

File: Type in the location of the file you want to upload in this field or click **Browse** to find it.

Choose File: Click **"Choose File"** to find the configuration file or firmware file you want to upload. Remember that you must extract / decompress / unzip the .zip files before you can upload them.

Backup Configuration: Click **Backup** button to back up the current running configuration file and save it to your computer in the event that you need this configuration file to be restored back to your BEC 4700A/AZ device when making false configurations and want to restore to the original settings.

Upgrade: Click **"Upgrade"** to begin the upload process. This process may take up to two minutes.



Firmware Upgrade

File upload succeeded, starting flash erasing and programming!!

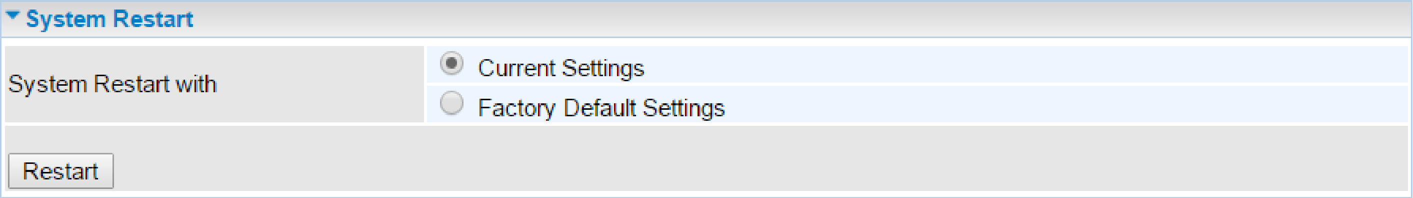
Progress	
Percent	15 %

DO NOT turn off or power cycle the device while firmware upgrading is still in process.

Improper operation could damage your BEC 4700A/AZ.

System Restart

Click **System Restart** with option **Current Settings** to reboot your router.



System Restart

System Restart with
● Current Settings
○ Factory Default Settings

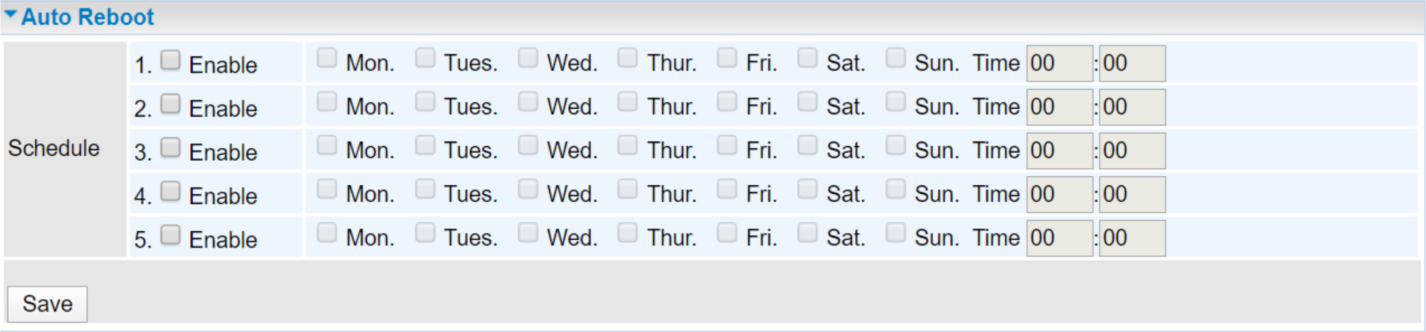
If you wish to restart the router using the factory default settings (for example, after a firmware upgrade or if you have saved an incorrect configuration), select **Factory Default Settings** to restore to factory default settings.

You may also restore your router to factory settings by holding the small Reset pinhole button on the back of your router in about more than 6s seconds whilst the router is turned on.

Auto Reboot

Schedule an automatic reboot for your 4700A/AZ to ensure proper operation and best performance.

This reboot will only reboot with current configuration settings and not overwrite any existing settings.

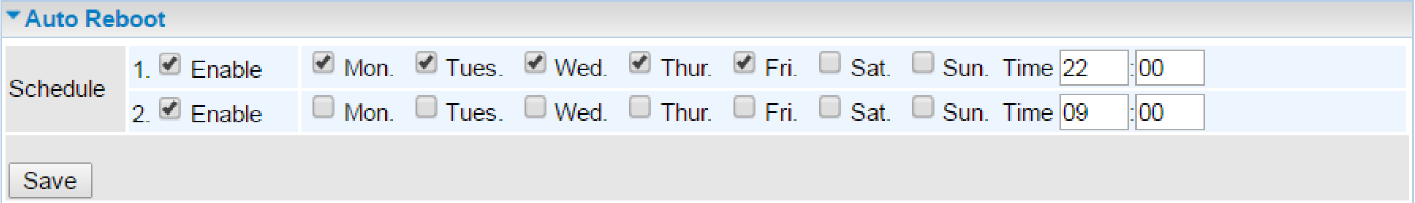


▾ Auto Reboot

Schedule	1. □ Enable	□ Mon.	□ Tues.	□ Wed.	□ Thur.	□ Fri.	□ Sat.	□ Sun.	Time 00 : 00
	2. □ Enable	□ Mon.	□ Tues.	□ Wed.	□ Thur.	□ Fri.	□ Sat.	□ Sun.	Time 00 : 00
	3. □ Enable	□ Mon.	□ Tues.	□ Wed.	□ Thur.	□ Fri.	□ Sat.	□ Sun.	Time 00 : 00
	4. □ Enable	□ Mon.	□ Tues.	□ Wed.	□ Thur.	□ Fri.	□ Sat.	□ Sun.	Time 00 : 00
	5. □ Enable	□ Mon.	□ Tues.	□ Wed.	□ Thur.	□ Fri.	□ Sat.	□ Sun.	Time 00 : 00

Click **Save** to apply settings

Example: Schedule your 4700A/AZ to reboot at 10:00pm (22:00) every weekday (Monday thru Friday) and reboot at 9:00am on Saturday and Sunday.



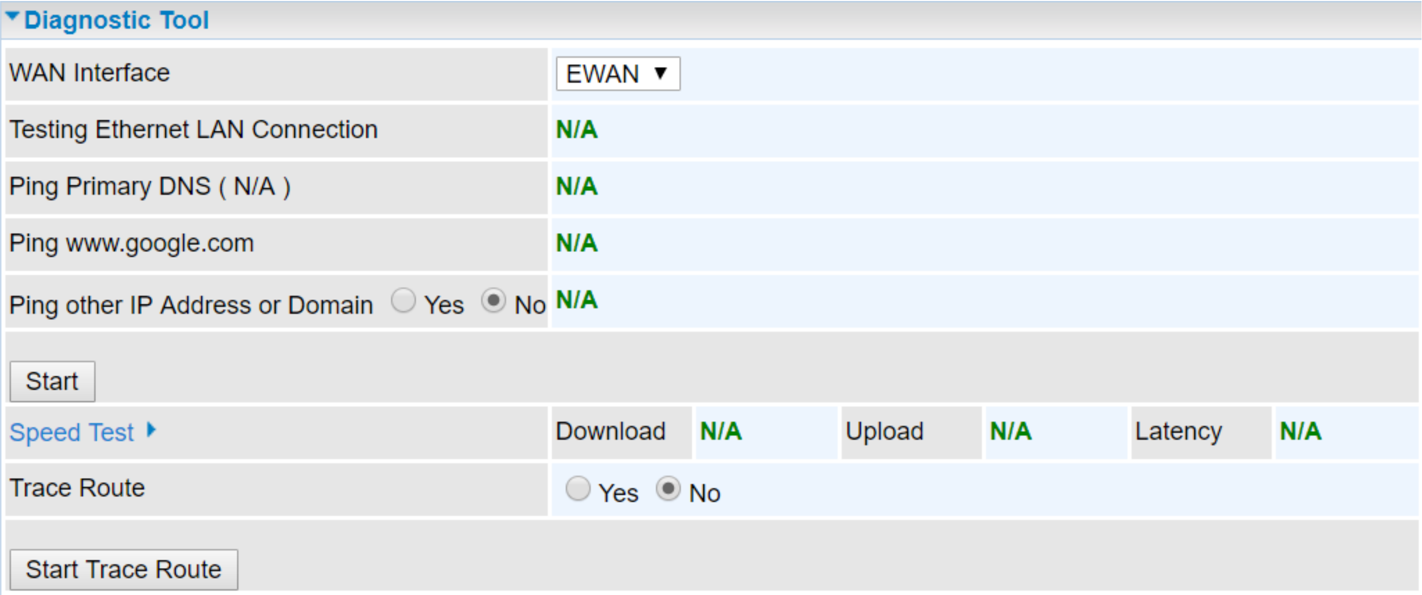
▾ Auto Reboot

Schedule	1. ☑ Enable	☑ Mon.	☑ Tues.	☑ Wed.	☑ Thur.	☑ Fri.	□ Sat.	□ Sun.	Time 22 : 00
	2. ☑ Enable	□ Mon.	□ Tues.	□ Wed.	□ Thur.	□ Fri.	□ Sat.	□ Sun.	Time 09 : 00

Diagnostics Tool

The Diagnostic Test page shows the test results for the connectivity of the physical layer and protocol layer for both LAN and WAN sides.

4G/LTE or EWAN

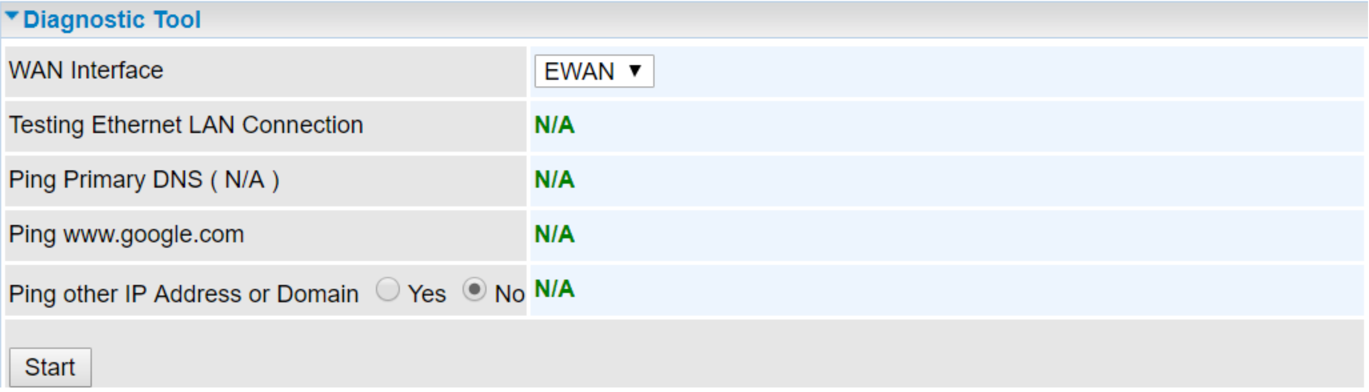


Diagnostic Tool

WAN Interface	EWAN ▼				
Testing Ethernet LAN Connection	N/A				
Ping Primary DNS (N/A)	N/A				
Ping www.google.com	N/A				
Ping other IP Address or Domain ○ Yes ● No	N/A				
Start					
Speed Test ▸	Download	N/A	Upload	N/A	Latency N/A
Trace Route	○ Yes ● No				
Start Trace Route					

Ping other IP Address: Click **Yes** if you wish to ping other IP address rather than google.com

Click **START** to begin to diagnose the connection.

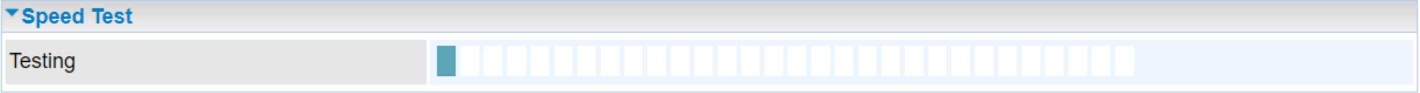


Diagnostic Tool

WAN Interface	EWAN ▼
Testing Ethernet LAN Connection	N/A
Ping Primary DNS (N/A)	N/A
Ping www.google.com	N/A
Ping other IP Address or Domain ○ Yes ● No	N/A
Start	

Speed Time: Measure the current uplink and downlink speed rate.

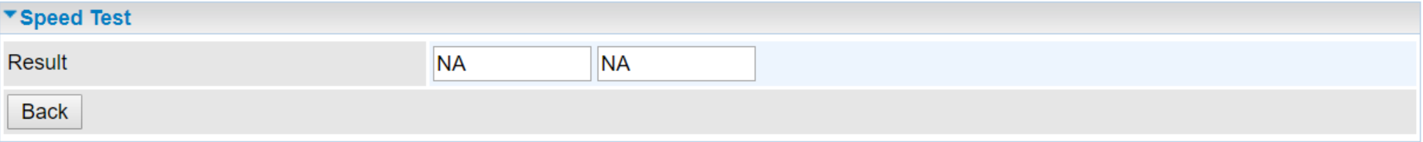
- Take less than a minute to run the test.



Speed Test

Testing

- Result in Uplink / Downlink

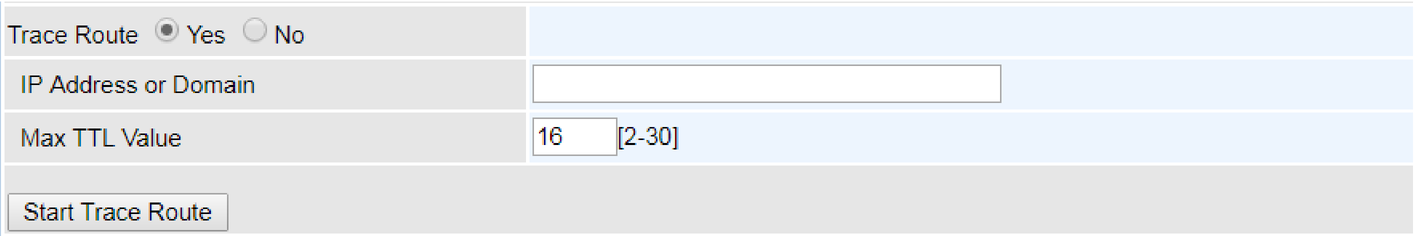


Speed Test

Result	NA	NA
Back		

Click **Back** to go back to the Diagnostic Tool

Trace Route is to display how many hops (also view the exact hops) required to get to the destination. Click **Yes**, enter the IP address or domain then **Start Trace Route**.



Trace Route ● Yes ○ No

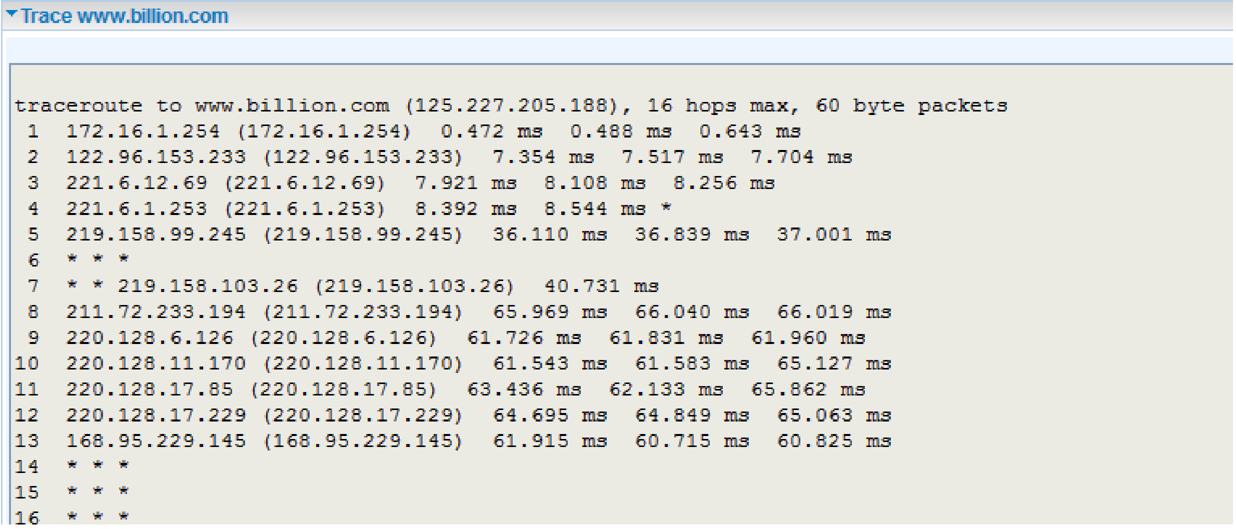
IP Address or Domain

Max TTL Value 16 [2-30]

IP Address or Domain: Set the destination host (IP, domain name) to be traced.

Max TTL value: Set the max Time to live (TTL) value.

Shown as we "trace" www.billion.com below.



```
traceroute to www.billion.com (125.227.205.188), 16 hops max, 60 byte packets
 1  172.16.1.254 (172.16.1.254)  0.472 ms  0.488 ms  0.643 ms
 2  122.96.153.233 (122.96.153.233)  7.354 ms  7.517 ms  7.704 ms
 3  221.6.12.69 (221.6.12.69)  7.921 ms  8.108 ms  8.256 ms
 4  221.6.1.253 (221.6.1.253)  8.392 ms  8.544 ms *
 5  219.158.99.245 (219.158.99.245)  36.110 ms  36.839 ms  37.001 ms
 6  * * *
 7  * * 219.158.103.26 (219.158.103.26)  40.731 ms
 8  211.72.233.194 (211.72.233.194)  65.969 ms  66.040 ms  66.019 ms
 9  220.128.6.126 (220.128.6.126)  61.726 ms  61.831 ms  61.960 ms
10  220.128.11.170 (220.128.11.170)  61.543 ms  61.583 ms  65.127 ms
11  220.128.17.85 (220.128.17.85)  63.436 ms  62.133 ms  65.862 ms
12  220.128.17.229 (220.128.17.229)  64.695 ms  64.849 ms  65.063 ms
13  168.95.229.145 (168.95.229.145)  61.915 ms  60.715 ms  60.825 ms
14  * * *
15  * * *
16  * * *
```

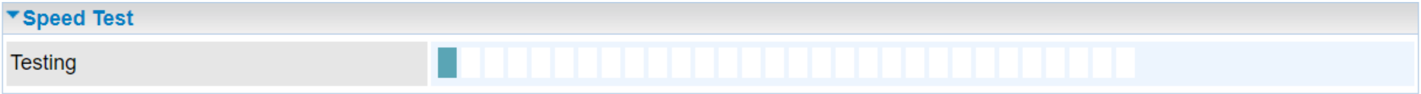
LAN

Ping other IP Address: Click **Yes** to ping any desired IP address or a domain.

Click **START** to begin to diagnose the connection.

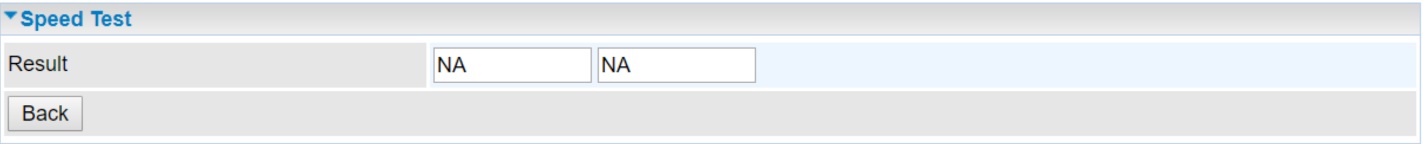
Speed Time: Measure the current uplink and downlink speed rate.

- Take less than a minute to run the test.



Testing

- Result in Uplink / Downlink



Result NA NA

Click **Back** to go back to the Diagnostic Tool.

Chapter 5: Troubleshooting

If your BEC 4700A/AZ is not functioning properly, you can refer to this chapter for simple troubleshooting before contacting your service provider support. This can save you time and effort but if symptoms persist, consult your service provider.

Problems with the Router

Problem	Suggested Action
None of the LEDs is on when you turn on the router	Check the connection between the router and the adapter. If the problem persists, most likely it is due to the malfunction of your hardware. Please contact your service provider or BEC for technical support.
You have forgotten your login username or password	Try the default username "admin" and password "admin". If this fails, you can restore your router to its factory settings by pressing the reset button on the device rear side.

Problem with LAN Interface

Problem	Suggested Action
Cannot PING any PC on LAN	Check the Ethernet LEDs on the front panel. The LED should be on for the port that has a PC connected. If it does not light, check to see if the cable between your router and the PC is properly connected. Make sure you have first uninstalled your firewall program before troubleshooting.
	Verify that the IP address and the subnet mask are consistent for both the router and the workstations.

Recovery Procedures

Problem	Suggested Action
- The front LEDs display incorrectly **- Still cannot access to the router management interface after pressing the RESET button.** **- Software / Firmware upgrade failure**	Before starting recovery process, please configure the IP address of the PC as 192.168.1.100 and proceed with the following step-by-step guide. 1. Power the router off. 2. Press reset button and power on the router, once the Power lights Red, keeping press reset button over 6 seconds. 3. Internet LED flashes Green, router entering recovery procedure and router's IP will reset to Emergency IP address (Say 192.168.1.1). 4. Open browser and access http://192.168.1.1 to upload the firmware. 5. Internet LED lit Red, and router starts to write firmware into flash. Please DO NOT power off the router at this step. 6. Internet LED lit Green when successfully upgrade firmware. 7. Power cycle off/on the BEC 4700A/AZ

APPENDIX: PRODUCT SUPPORT & CONTACT

If you come across any problems, please contact the dealer from where you have purchased the product.

Contact BEC @ http://www.bectechnologies.net

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference

(2) This device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. . This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

Co-location statement

This device and its antenna(s) must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Professional Installation Instruction

1.Installation personnel
This product is designed for specific application and needs to be installed by qualified personnel who has RF and related rule knowledge. The general user shall not attempt to install or change the settings.

2.Installation location
The product shall be installed at a location where the radiating antenna can be kept 20 cm from nearby person in normal operation condition to meet Regulatory RF exposure requirement. The installation applies to both indoor and outdoor location.

3.External antenna(s)
Use only the antenna(s) that have been approved by the manufacturer. The non-approved antenna(s) may produce unwanted spurious or excessive RF transmitting power that may lead to the violation of FCC/ISED limit and is prohibited.

4.Warning
Please carefully select the installation position and ensure that the final output power does not exceed the limit set forth in relevant rules. The violation of the rule could lead to serious federal penalty.