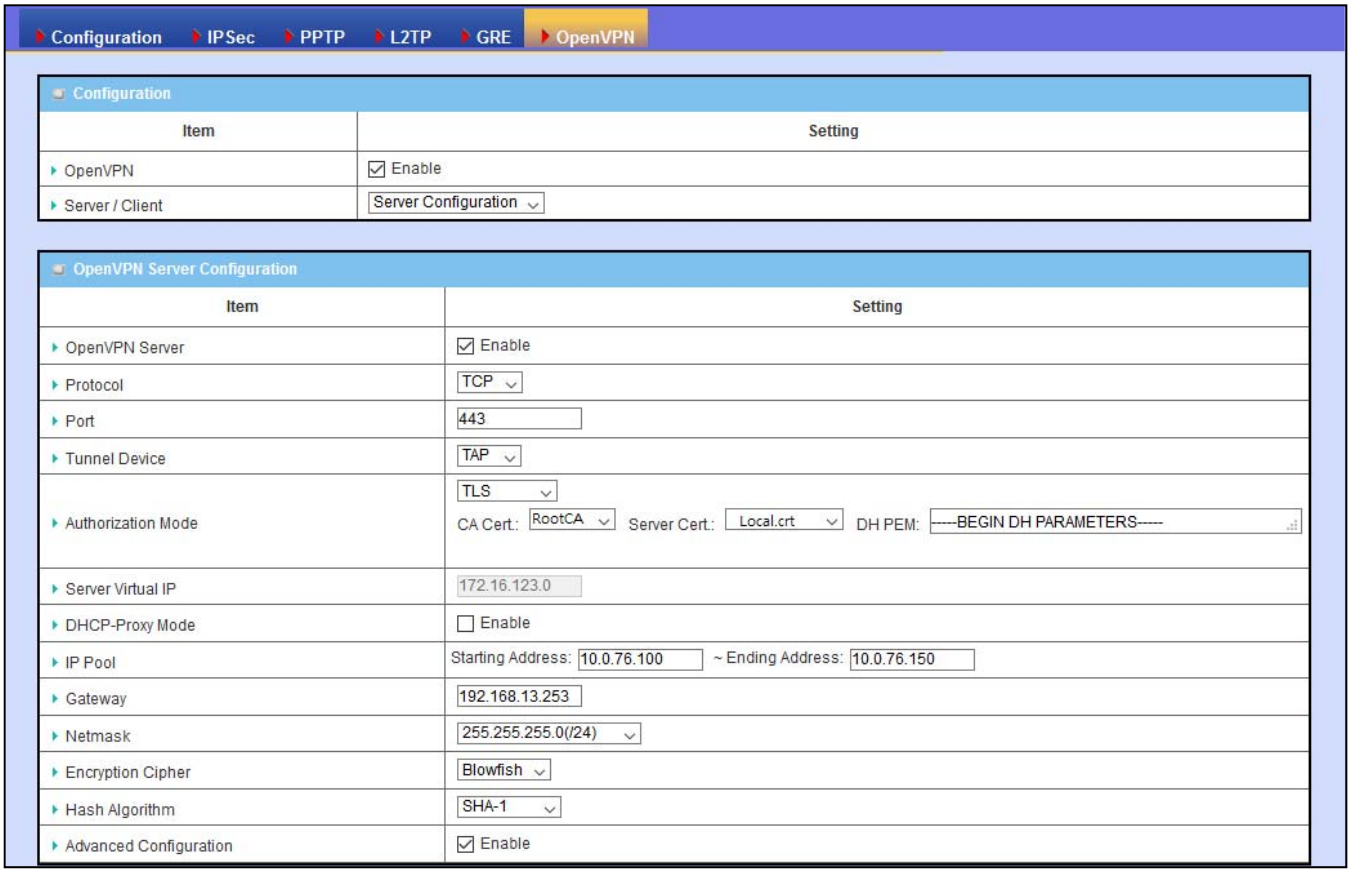
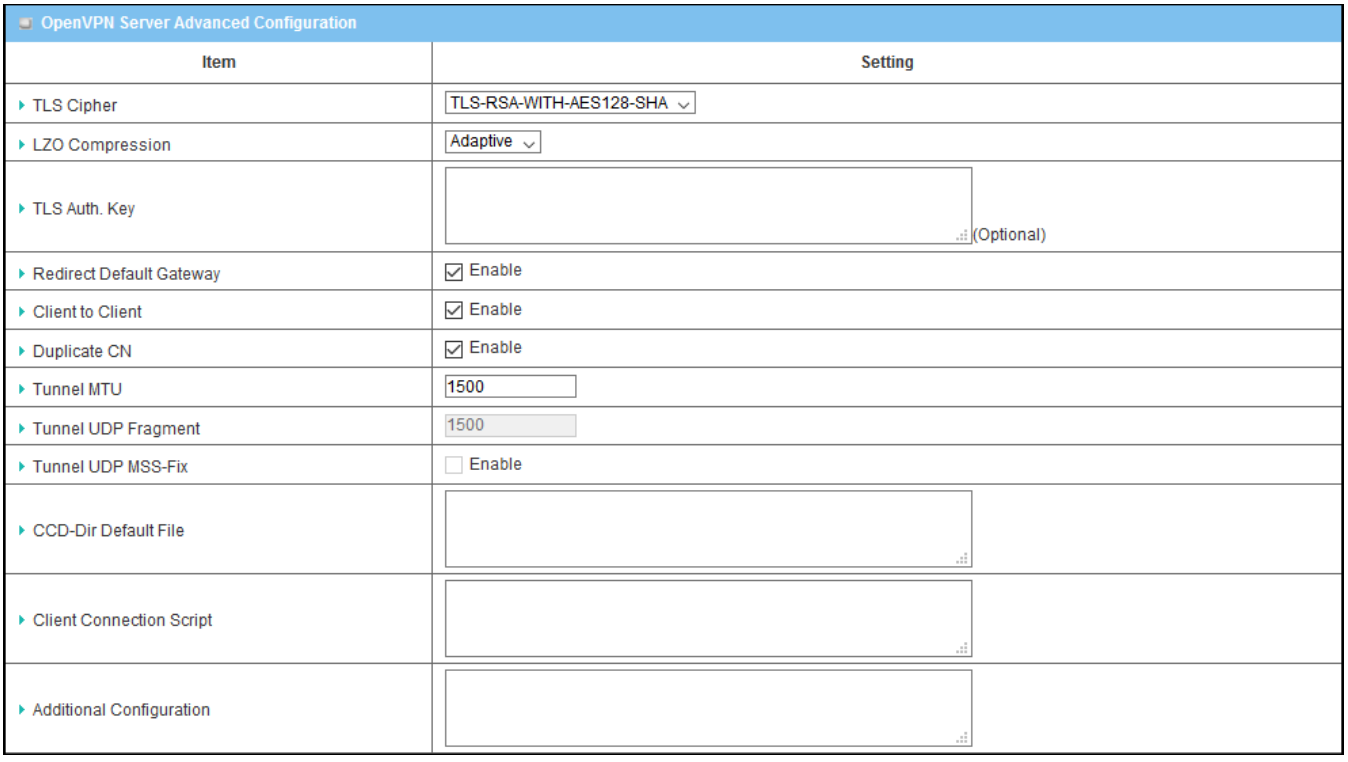
5.5.d OpenVPN

OpenVPN is an 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. It is capable of traversing network address translators (NATs) and firewalls. OpenVPN allows peers to authenticate each other using a Static key or certificates.When used in a multi-client-server configuration, it allows the server to release an authentication certificate for every client, using signature and Certificate authority. It uses the OpenSSL encryption library extensively, as well as the SSLv3/TLSv1 protocol, and contains many security and control features.

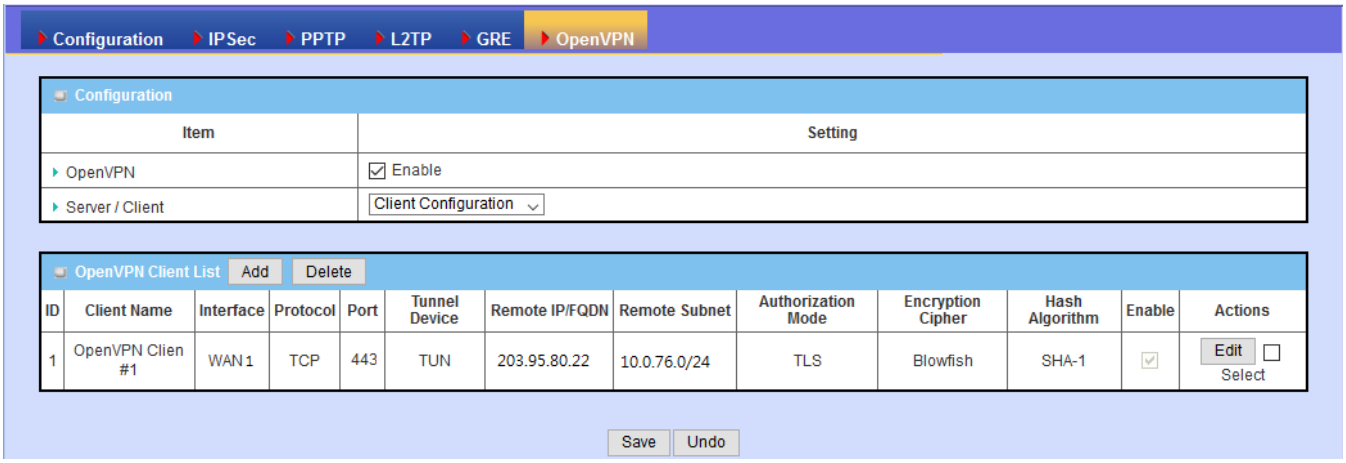
Deploy a security gateway for local office and establish a virtual private network with the remote gateway of another office by using OpenVPN. So, all client hosts behind local security gateway can make data communication with others behind remote gateway.

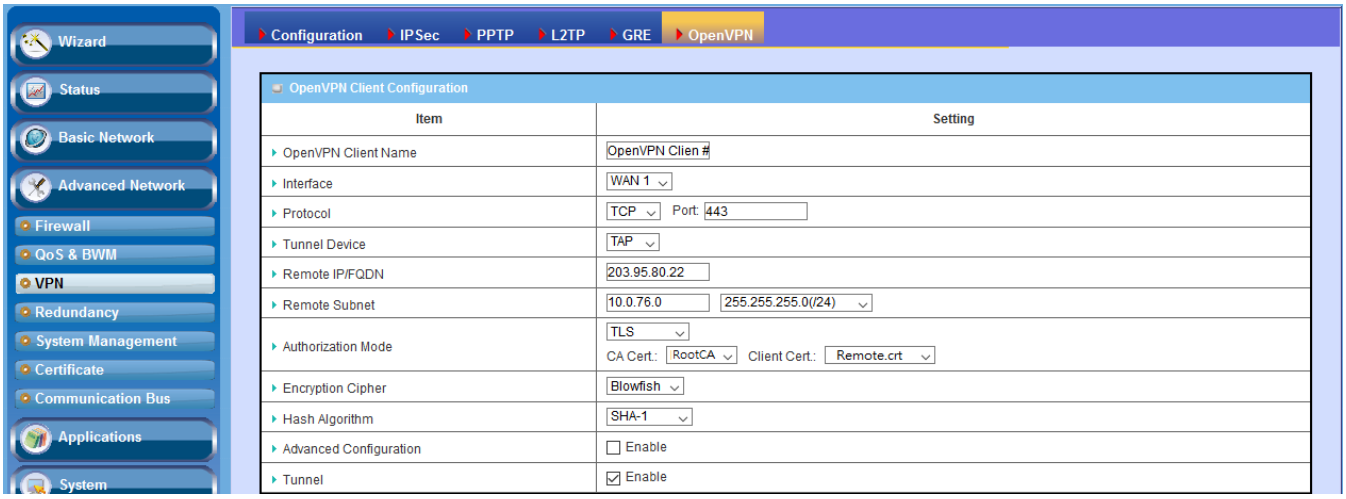
In the case when you are a mobile user with your notebook or carrying along a security gateway to access the servers and database in company headquarters (HQ). And that the security gateway in HQ supports the OpenVPN server function. You can dial in the HQ gateway and access the HQ resources by establishing an OpenVPN tunneling. It is a virtual private network between your device and HQ gateway for your resource accessing.


Configuration
IPSec
PPTP
L2TP
GRE
OpenVPN
Configuration
Item
Setting
OpenVPN
Enable
Server / Client
Server Configuration
OpenVPN Server Configuration
Item
Setting
OpenVPN Server
Enable
Protocol
TCP
Port
443
Tunnel Device
TAP
Authorization Mode
TLS
CA Cert.:
RootCA
Server Cert.:
Local.crt
DH PEM:
-----BEGIN DH PARAMETERS-----
Server Virtual IP
172.16.123.0
DHCP-Proxy Mode
Enable
IP Pool
Starting Address:
10.0.76.100
~ Ending Address:
10.0.76.150
Gateway
192.168.13.253
Netmask
255.255.255.0(/24)
Encryption Cipher
Blowfish
Hash Algorithm
SHA-1
Advanced Configuration
Enable


OpenVPN Server Advanced Configuration
Item
Setting
TLS Cipher
TLS-RSA-WITH-AES128-SHA
LZO Compression
Adaptive
TLS Auth. Key
(Optional)
Redirect Default Gateway
Enable
Client to Client
Enable
Duplicate CN
Enable
Tunnel MTU
1500
Tunnel UDP Fragment
1500
Tunnel UDP MSS-Fix
Enable
CCD-Dir Default File
Client Connection Script
Additional Configuration

In "OpenVPN" page, there is the "Configuration" window to enable the OpenVPN function. The security gateway can either take "OpenVPN Server" role or "OpenVPN Client" role or they both. Define and choose either one role for your router in the "Configuration" window and configure all required parameters beneath the "Configuration" window. Then configure parameters on another gateway to take another role. Above diagram is the server role configuration and following diagram shows the client role configuration.





To configure "OpenVPN Server or Client" role for the security gateway as follows:

Configuration

The "Configuration" window is to enable the OpenVPN by checking the Enable box. In the "Client/Server" field of the "Configuration" window choose either "Server" or "Client". Choose Server to define the gateway as the L2TP VPN server for remote clients to initiate the connection to establish VPN tunnels. Or choose Client to create multiple OpenVPN clients to establish VPN tunnels to remote gateways. Moreover, the security gateway serves as the OpenVPN client and server simultaneously.

OpenVPN VPN Server Scenario

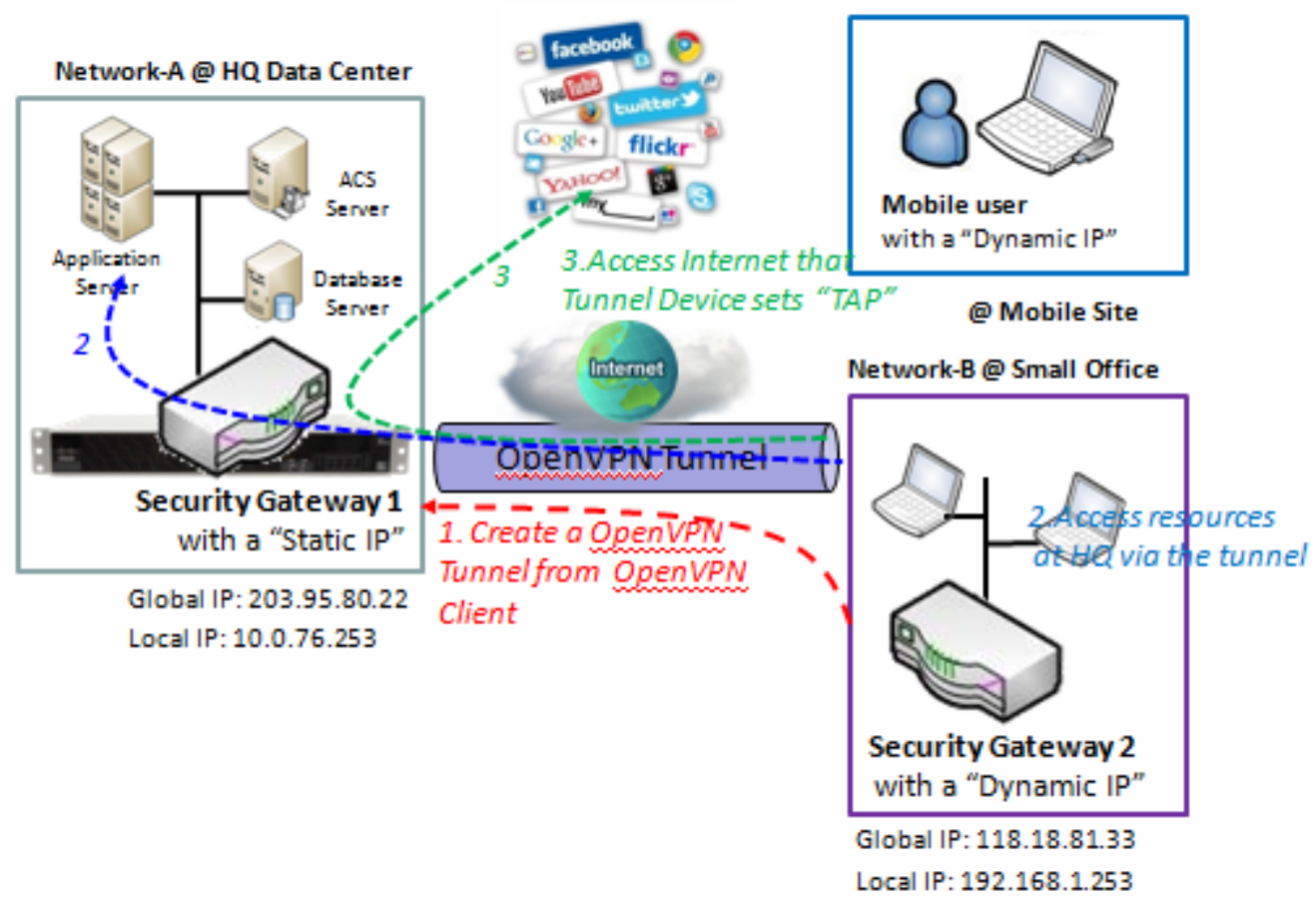
When you want the security gateway to play an OpenVPN server role, check the "Enable" box and choose "Server" option in the "OpenVPN Configuration" window. And make its related configuration in following sections. Also refer to the above server role diagram.

OpenVPN Server Configuration

In the "OpenVPN Server Configuration" window you will enable the OpenVPN server function, specify the virtual IP address of OpenVPN server, define the pool of virtual IP addresses that will assign to remote OpenVPN clients dialing in the security gateway, and the authentication protocol. Once you select "MS-CHAP" or "MS-CHAP v2" for the authentication protocol, you also can specify if the OpenVPN server needs the MPPE encryption and its key length or not for the authentication process.

OpenVPN Server Advanced Configuration

There are advanced settings available. Check the "Enable" box of Advanced Configuration.



Scenario Application Timing

Above diagram illustrates the security gateway at headquarters playing the OpenVPN

server role. The OpenVPN tunnel is established by starting from OpenVPN client, the Security Gateway 2 in Network-B or the mobile device, like notebook. All client hosts behind the Security Gateway 2 or the mobile device can access the resources in the Intranet of Network-A at headquarters via this established OpenVPN tunnel. Usually, these hosts at OpenVPN client peer access the Internet directly via the WAN interface of Security Gateway 2. Only the packets whose destination is in the dedicated subnet to Network-A will be transferred via the OpenVPN tunnel.

Scenario Description

OpenVPN Tunneling is a Client and Server based tunneling technology.

The OpenVPN Server must have a Static IP or a FQDN, and maintain a Client list. The Client may be a mobile user or mobile site, and requesting the OpenVPN tunnel connection.

OpenVPN protocol is used for establishing an OpenVPN VPN tunnel.

Parameter Setup Example

For Network-A at HQ

Following below tables list the parameter configuration for above example diagram of OpenVPN server in Network-A.

Use default value for those parameters that are not mentioned in these tables.

Configuration Path	[OpenVPN]-[Configuration]
OpenVPN	■ ***Enable***
Server/Client	**Server Configuration**

Configuration Path	[OpenVPN]-[OpenVPN Server Configuration]
OpenVPN Server	■ ***Enable***
Protocol	***TCP***
Port	***443***
Tunnel Device	***TAP*** ***PS: TAP also called "Bridging" behaves like a real network adapter and Broadcast traffic can transport.*** ***TUN called "Routing" transports only layer 3 IP packets. The user has to add routing rule according to the environment so that packets transfer smoothly.***
Authorization Mode	***TLS*** ***CA Cert: RootCA, Server Cert: Local.crt*** ***DH PEM : Default*** ***-----BEGIN DH PARAMETERS-----*** ***MIGHAoGBAMq4z88pL8X1dzmDmnr7nyV3w3L1rDU4Q+4SJiGQjR6b2nb4tf9jw/QJ*** ***W/ENgduKKXsltYSAzOZ9gXoNxwFGc9nKd4LfGpjQl9lIoHTp0eTdb9b5EKeR6B7h*** ***QxkfLBwVv1YZh9oUXm6pdewpg2QdZ2KtiOlMpgsJyaqRMQ3MlNB7AgEC*** ***-----END DH PARAMETERS-----*** ***PS: Security Gateway 1 is the role of RootCA and trusted CA.***
IP Pool Starting Address	***10.0.76.100***
IP Pool Ending Address	***10.0.76.150***

Gateway	***10.0.76.253***
Netmask	***255.255.255.0/24***
Encryption Cipher	***Blowfish***
Hash Algorithm	**SHA-1**

Scenario Operation Procedure

In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface. It serves as an OpenVPN server.

Network-B is in the mobile office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 192.168.1.253 for LAN interface and 118.18.81.33 for WAN interface. It serves as an OpenVPN client.

Establish an OpenVPN VPN tunnel by starting from the OpenVPN client site. So hosts in Network-B can access hosts or servers in Network-A. But can't access from Network-A to Network-B.

To communicate each other securely between Intranets of 10.0.75.0/24 and 192.168.1.0/24, please add route policy according to the environment by checking the "Enable" box of Advanced Configuration.

OpenVPN VPN Client Scenario

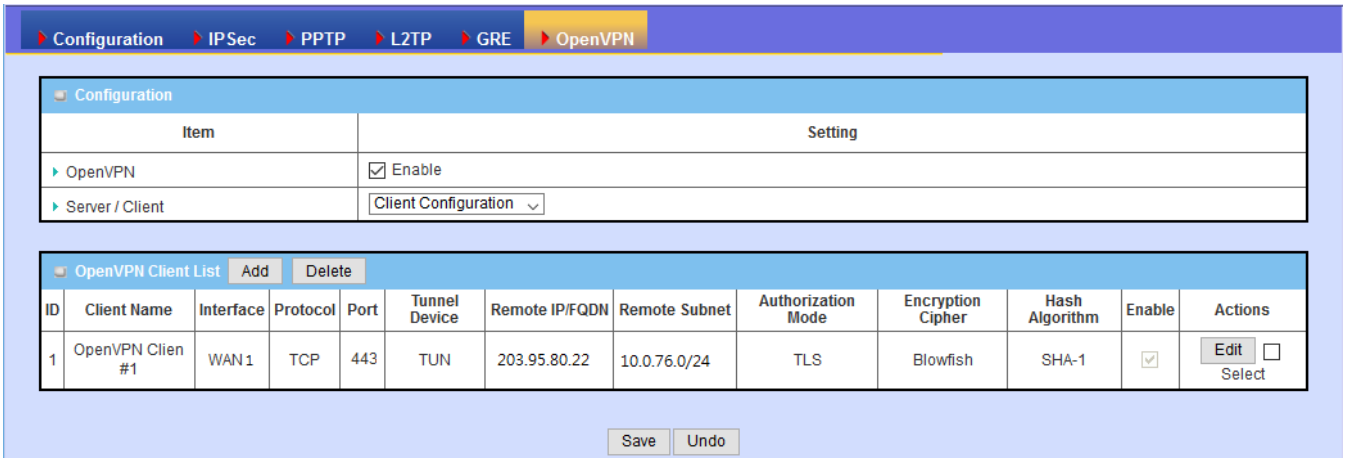
When you want the security gateway to play an OpenVPN client role, check the "Enable" box and choose "Client" option in the "OpenVPN Configuration" window. And make its related configuration in following sections.

OpenVPN Client Configuration

"OpenVPN Client Configuration" window can let you enable the OpenVPN client function by checking the "Enable" box.

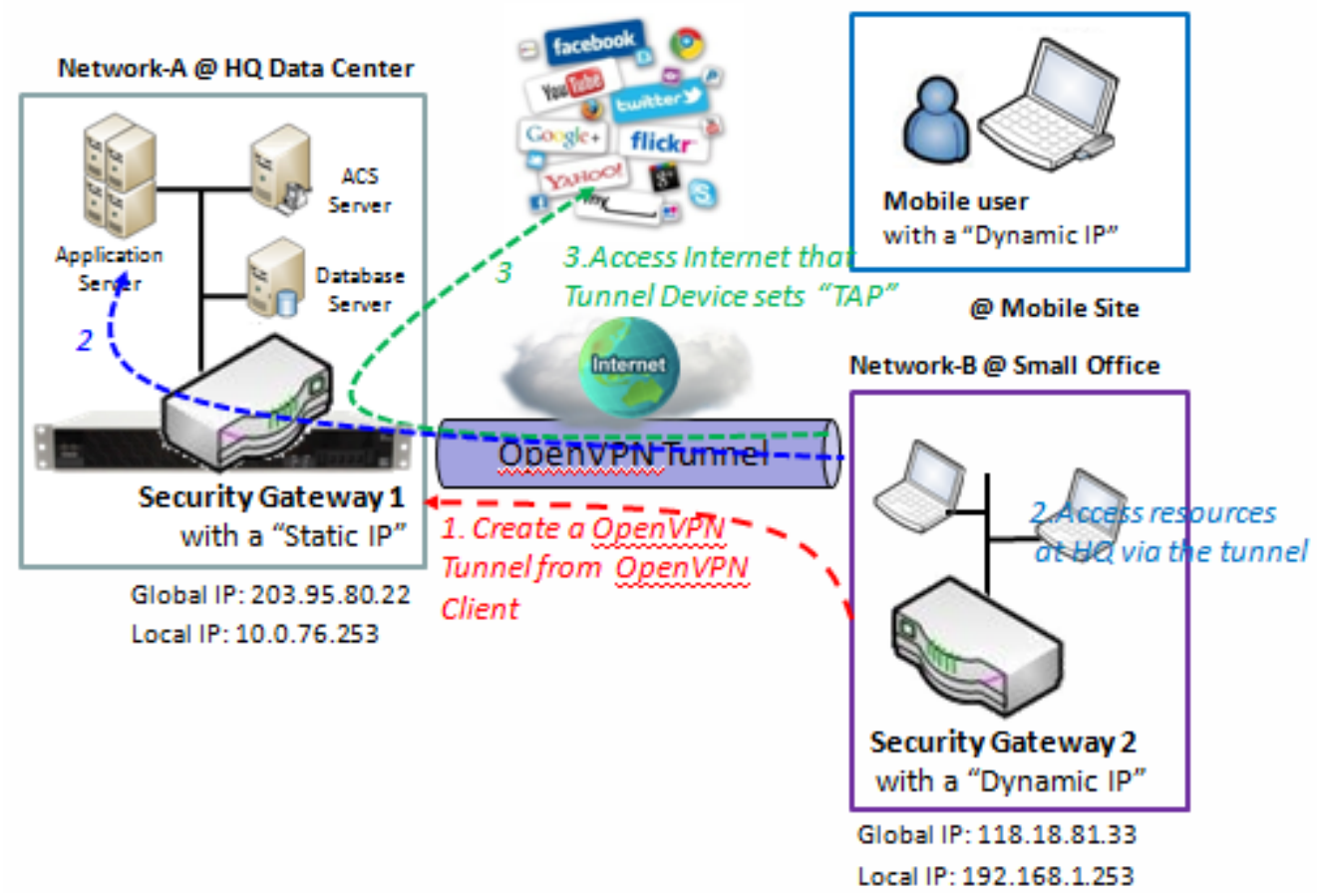
OpenVPN Client List

"OpenVPN Client List" window shows your defined OpenVPN clients and their tunnel status. Only some important information for all tunnels are shown in the list in following diagram.



Configuration for An OpenVPN Client

"Configuration for An OpenVPN Client" window let you specify the required parameters for an OpenVPN VPN client, such as "OpenVPN Client Name", "Interface", "Protocol", "Port", "Remote IP/FQDN", "Remote Subnet", "Authorization Mode", "Encryption Cipher", "Hash Algorithm," and tunnel activation.



Scenario Application Timing

Above diagram illustrates the Security Gateway 2 or the mobile device playing the OpenVPN VPN client role. The OpenVPN tunnel is established by the OpenVPN client making the tunnel connection request initiation and the Security Gateway 1 in Network-A of headquarters serves as the OpenVPN server responding to the request. Once the tunnel has been established, all client hosts behind the Security Gateway 2 or the mobile device can access the resources in the Intranet of Network-A at headquarters via this established OpenVPN tunnel. Moreover, these hosts at OpenVPN client peer access the Internet directly via the WAN interface of Security Gateway 1. As shown in the diagram by configuring the OpenVPN tunnel set "TAP" for OpenVPN client peer, the Internet accessing packets will be also sent to the Security Gateway 1 in Network-A and be re-transferred to the Internet. That means the Internet accessing of OpenVPN Client peer is also controlled by the Security Gateway 1, the OpenVPN VPN server.

Scenario Description

OpenVPN Tunneling is a Client and Server based tunneling technology.

The OpenVPN Server must have a Static IP or a FQDN, and maintain a Client list; The Client may be a mobile user or mobile site, and requesting the OpenVPN tunnel connection.

OpenVPN protocol is used for establishing an OpenVPN tunnel.

Parameter Setup Example

For Network-B at Mobile Office

Following 3 tables list the parameter configuration for above example diagram of OpenVPN VPN client in Network-B.

Use default value for those parameters that are not mentioned in these tables.

Configuration Path	[OpenVPN]-[Configuration]
OpenVPN	■ ***Enable***
Server/Client	**Client Configuration**

Configuration Path	[OpenVPN]-[OpenVPN Client Configuration]
OpenVPN Client Name	**Client1**
Interface	**WAN1**
Protocol	***TCP***
Port	***443***
Tunnel Device	***TAP*** ***PS: TAP also called "Bridging" behaves like a real network adapter and Broadcast traffic can transport.*** ***TUN called "Routing" transports only layer 3 IP packets. The user has to add routing rule according to the environment so that packets transfer smoothly.***
Remote IP/FQDN	***203.95.80.22***
	10.0.76.0/24
Authorization Mode	***TLS*** ***CA Cert: RootCA, Client Cert: Remote.crt***

Encryption Cipher	***Blowfish***
Hash Algorithm	**SHA-1**

Scenario Operation Procedure

In above diagram, Network-A is in the headquarters, and the subnet of its Intranet is 10.0.76.0/24. The security gateway for Network-A has the IP address of 10.0.76.2 for LAN interface and 203.95.80.22 for WAN interface. It serves as an OpenVPN server.

However, Network-B is in the mobile office and the subnet of its Intranet is 10.0.75.0/24. The security gateway for Network-B has the IP address of 192.168.1.253 for LAN interface and 118.18.81.33 for WAN interface. It serves as an OpenVPN client.

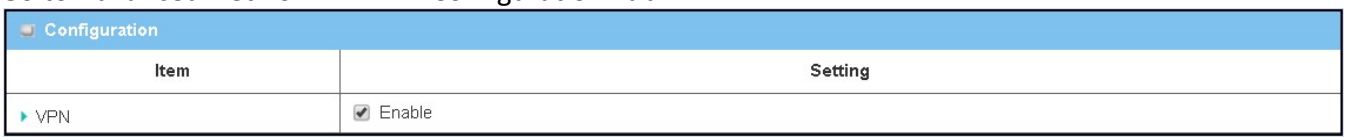
The OpenVPN client dials in the OpenVPN server at HQ for establishing an OpenVPN tunnel. So hosts in Network-B can access hosts or servers in Network-A. But can't access from Network-A to Network-B.

However, if the "Default Gateway/Remote Subnet" parameter in the Security Gateway 2 is configured to "Default Gateway", the Internet accessing of OpenVPN Client peer also go through the established OpenVPN VPN tunnel, and the Security Gateway 1 can control the accessing as same as the HQ resource accessing.

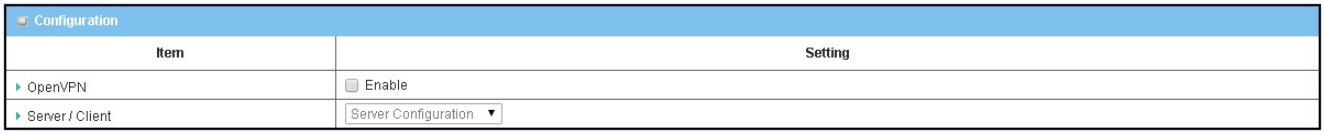
Open VPN Setting

T he configuration setting allows user to use OpenVPN.
Ensure VPN is enabled and saved

Go to Advanced Network > VPN > Configuration Tab

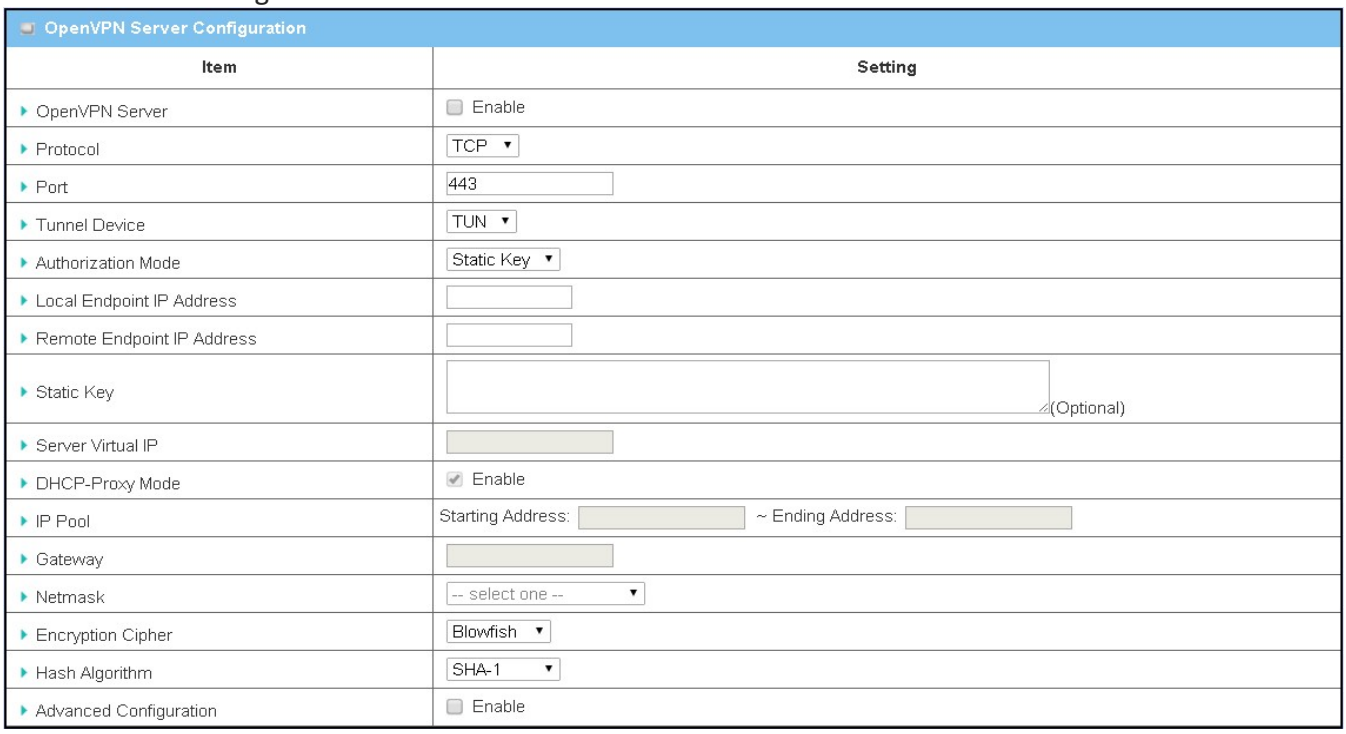


Enable OpenVPN and select which server or client you want



Item	Value setting	Description
OpenVPN	The box is unchecked by default	Check the **Enable** box to activate this OpenVPN function.
Server/ Client	Server Configuration is set by default	When **Server Configuration** is selected, as the name suggest, server configuration will be display below, with **Client Configuration**, you can specifically set client configuration.

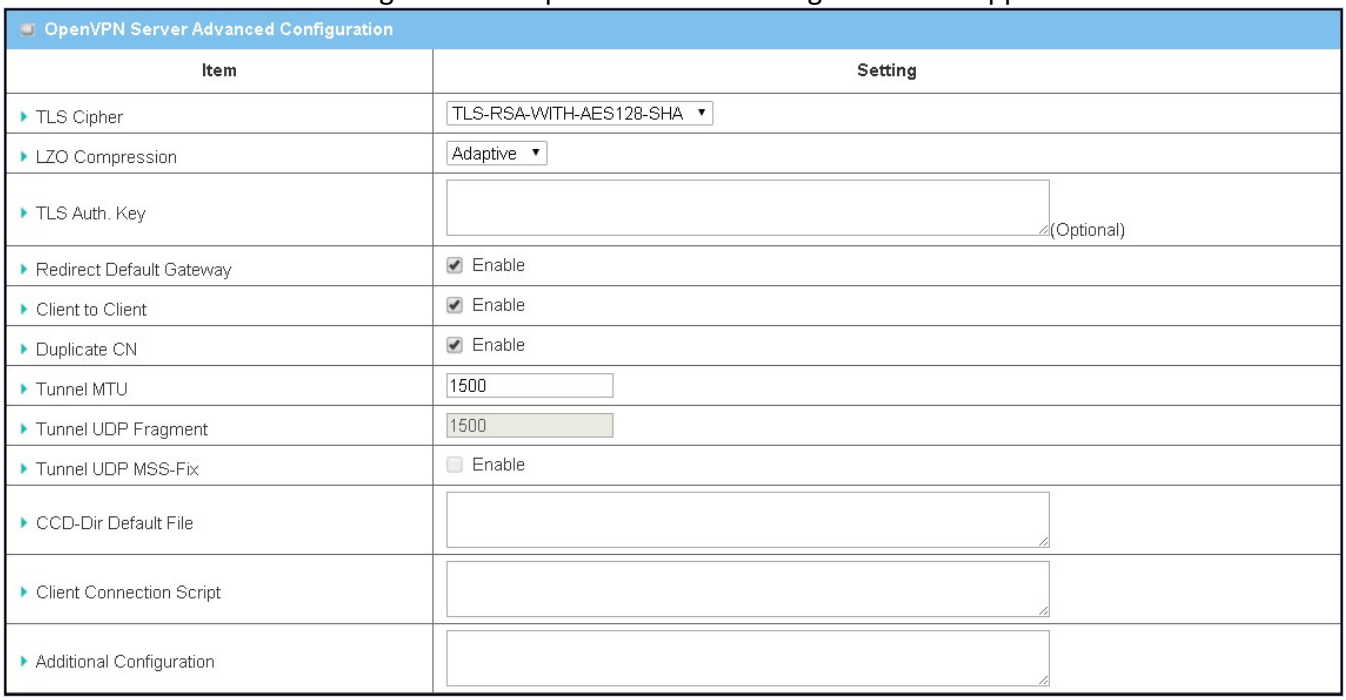
When Server Configuration is selected



Item	Value setting	Description
OpenVPN Server	The box is unchecked by default	Click the **Enable** to activate OpenVPN Server functions.
Protocol	A Must filled setting By default **TCP** is selected.	Define the selected **Protocol** for the OpenVPN Server which to be. Select **TCP /UDP** for OpenVPN Server which to be. Select **TCP** for OpenVPN Server which to be. ->The OpenVPN will use TCP protocol, and **Port** will be set 443 automatically. Select **UDP** for OpenVPN Server which to be. -> The OpenVPN will use UDP protocol, and **Port** will be set 1194 automatically.
Port	A Must filled setting By default **443** is set.	Specify the **Port** for the OpenVPN Server to use.
Tunnel Device	A Must filled setting By default **TUN** is selected.	Specify the **Tunnel Device** for the OpenVPN Server to use. Select **TUN** for OpenVPN Server which to be. ->The OpenVPN will use TUN tunnel device. Select **TAP** for OpenVPN Server which to be. -> The OpenVPN will use TAP tunnel device.
Authorization Mode	A Must filled setting By default **Static Key** is selected.	Specify **Static Key/TLS** for the OpenVPN Server. Select **Static Key** for OpenVPN Server which to be. ->The OpenVPN will use static key authorization mode. The items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be display. Select **TLS** for OpenVPN Server which to be. ->The OpenVPN will use TLS authorization mode. The items **CA Cert.**, **Server Cert.** and **DH PEM** will be display. **CA Cert.** could be generated in Certificate. Refer to

		Advanced Network > **Certificate** > **Trusted Certificates**. **Server Cert.** could be generated in Certificate. Refer to **Advanced Network** > **Certificate** > **My Certificates**. **DH PEM** should let user enter the content.
Local Endpoint IP Address	A Must filled setting	Specify the Local Endpoint IP Address. Note_1: Local Endpoint IP Address will be available only when Static Key is be chose in Authorization Mode.
Remote Endpoint IP Address	A Must filled setting	Specify the Remote Endpoint IP Address. Note_1: Remote Endpoint IP Address will be available only when Static Key is be chose in Authorization Mode.
Static Key	A Must filled setting	Specify the **Static Key**. Note_1: Static Key will be available only when Static Key is be chose in Authorization Mode.
Server Virtual IP	A Must filled setting	Specify the Server Virtual IP. Note_1: Server Virtual IP will be available only when TLS is be chose in Authorization Mode.
DHCP-Proxy Mode	A Must filled setting The box is checked by default.	Specify the DHCP-Proxy Mode. Note_1: DHCP-Proxy Mode will be available only when TAP is be chose in Tunnel Device.
IP Pool	A Must filled setting	Specify the OpenVPN server virtual **IP pool.** **Starting Address:** It will set as the starting IP which assign to OpenVPN client. **Ending Address:** It will set as the ending IP which assign to OpenVPN client. Note_1: IP Pool will be available only when TAP is be chose in Tunnel Device and DHCP-Proxy Mode is unchecked.
Gateway	A Must filled setting	Specify the OpenVPN server **Gateway** Note_1: Gateway will be available only when TAP is be chose in Tunnel Device and DHCP-Proxy Mode is unchecked.
Netmask	By default **- select one -** is selected.	Specify the OpenVPN server **Netmask.** Note_1: Netmask will be available when TAP is be chose in Tunnel Device and DHCP-Proxy Mode is unchecked. Note_2: Netmask will be available when TUN is be chose in Tunnel Device.
Encryption Cipher	By default **Blowfish** is selected.	Specify the Encryption Cipher. Selected the Blowfish/AES-256/AES-192/AES-128/None.
Hash Algorithm	By default **SHA-1** is selected.	Specify the Hash Algorithm Selected the SHA-1/MD5/MD4/SHA2-256/SHA2-512/None.
Advanced Configuration	The box is unchecked by default.	Specify the OpenVPN server **Advanced Configuration** setting. If it is checked, **Advanced Configuration** will be display below.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

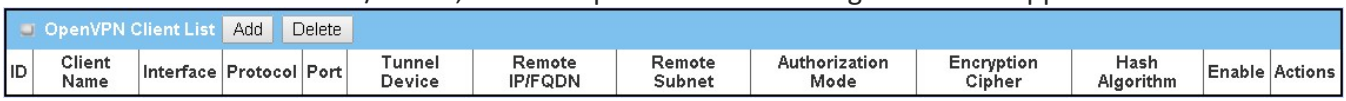
When select Advanced Configuration in OpenVPN Server Configuration will appear.



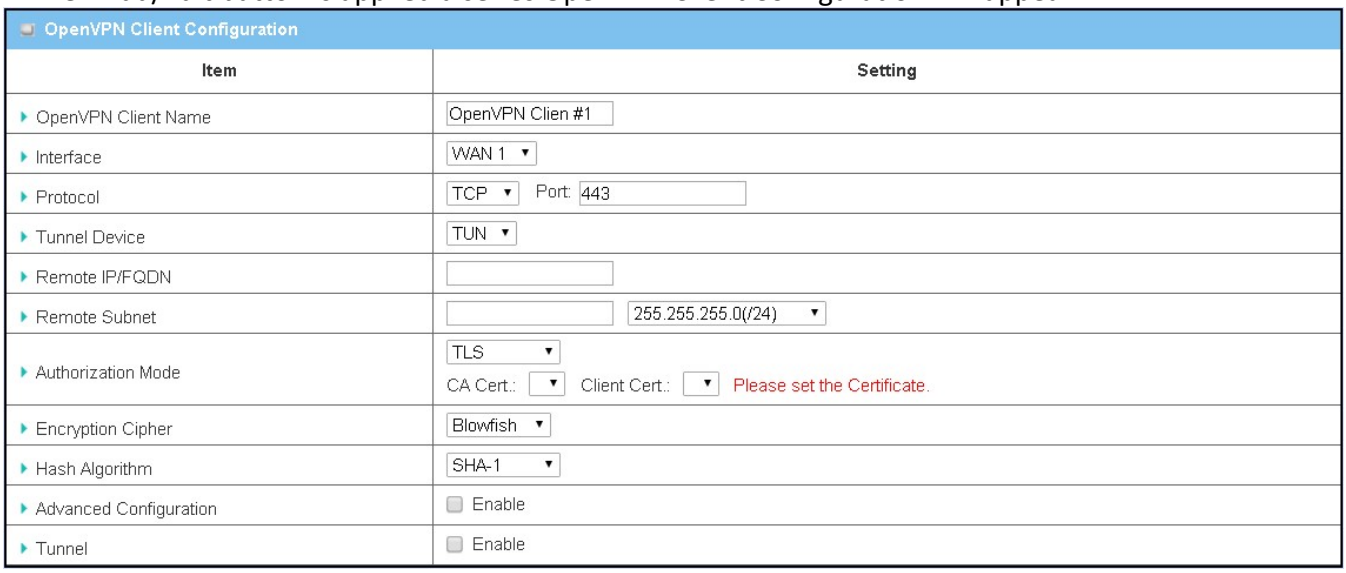
Item	Value setting	Description
TLS Cipher	By default TLS-RSA-WITH-AES128-SHA is selected.	Specify the OpenVPN server **TLS Cipher.** Note_1: TLS Cipher will be available only when TLS is be chose in Authorization Mode.
LZO Compression	By default Adaptive is selected.	Specify the OpenVPN server **LZO Compression.**
TLS Auth. Key	String format: any text	Specify the OpenVPN server **TLS Auth. Key.** Note_1: TLS Auth. Key will be available only when TLS is be chose in Authorization Mode.
Redirect Default Gateway	The box is checked by default	Specify the OpenVPN server **Redirect Default Gateway.**
Client to Client	The box is checked by default	Specify the OpenVPN server **Client to Client.**
Duplicate CN	The box is checked by default	Specify the OpenVPN server **Duplicate CN.**
Tunnel MTU	A Must filled setting The value is 1500 by default	Specify the OpenVPN server **Tunnel MTU.**
Tunnel UDP Fragment	The value is 1500 by default	Specify the OpenVPN server **Tunnel UDP Fragment.** Note_1: Tunnel UDP Fragment will be available only when UDP is be chose in Protocol.
Tunnel UDP MSS-Fix	The box is unchecked by default.	Specify the OpenVPN server **Tunnel UDP MSS-Fix.** Note_1: Tunnel UDP MSS-Fix will be available only when UDP is be chose in Protocol.

CCD-Dir Default File	String format: any text	Specify the OpenVPN server **CCD-Dir Default File.**
Client Connection Script	String format: any text	Specify the OpenVPN server **Client Connection Script.**
Additional Configuration	String format: any text	Specify the OpenVPN server **Additional Configuration.**

When select Client in Client/Server, a series OpenVPN Client Configuration will appear.



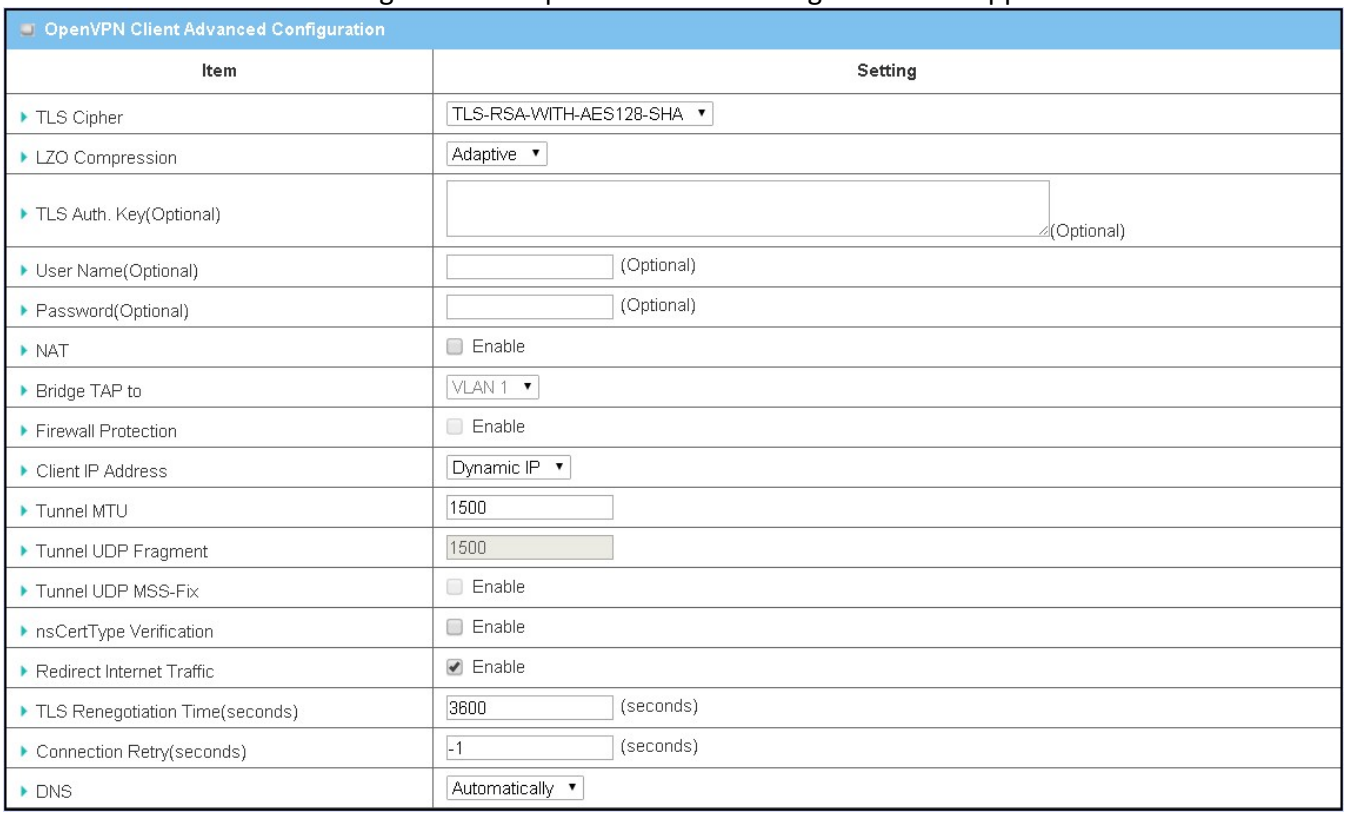
When Add/Edit button is applied a series OpenVPN Client Configuration will appear.



Item	Value setting	Description
OpenVPN Client Name	A Must filled setting	When fill in the name, it will be used to identify it in the tunnel list.
Interface	A Must filled setting	Define the selected interface to be the used for this OpenVPN Client tunnel. Select **WAN-1** for this OpenVPN Client tunnel by default.
Protocol	A Must filled setting By default **TCP** is selected.	Define the selected **Protocol** for the OpenVPN Client which to be. Select **TCP /UDP** for OpenVPN Client which to be. Select **TCP** for OpenVPN Client which to be. ->The OpenVPN will use TCP protocol, and **Port** will be set 443 automatically. Select **UDP** for OpenVPN Client which to be. -> The OpenVPN will use UDP protocol, and **Port** will be set 1194 automatically.
Port	A Must filled setting By default **443** is set.	Specify the **Port** for the OpenVPN Client to use.
Tunnel Device	A Must filled setting By default **TUN** is selected.	Specify the **Tunnel Device** for the OpenVPN Client to use. Select **TUN** for OpenVPN Client which to be. ->The OpenVPN will use TUN tunnel device.

		Select **TAP** for OpenVPN Client which to be. -> The OpenVPN will use TAP tunnel device.
Remote IP/FQDN	A Must filled setting	Specify the **Remote IP/FQDN** for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
Remote Subnet	A Must filled setting	Specify **Remote Subnet** for this OpenVPN Client tunnel. Filled the remote subnet address and selected remote subnet mask.
Authorization Mode	A Must filled setting By default **TLS** is selected.	Specify **Static Key/TLS** for the OpenVPN Server. Select **Static Key** for OpenVPN Server which to be. ->The OpenVPN will use static key authorization mode. The items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be display. Select **TLS** for OpenVPN Server which to be. ->The OpenVPN will use TLS authorization mode. The items **CA Cert.**, and **Client Cert.** will be display. **CA Cert.** could be generated in Certificate. Refer to **Advanced Network** > **Certificate** > **Trusted Certificates**. **Client Cert.** could be generated in Certificate. Refer to **Advanced Network** > **Certificate** > **My Certificates**.
Local Endpoint IP Address	A Must filled setting	Specify the Local Endpoint IP Address. Note_1: Local Endpoint IP Address will be available only when Static Key is be chose in Authorization Mode.
Remote Endpoint IP Address	A Must filled setting	Specify the Remote Endpoint IP Address. Note_1: Remote Endpoint IP Address will be available only when Static Key is be chose in Authorization Mode.
Static Key	A Must filled setting	Specify the **Static Key**. Note_1: Static Key will be available only when Static Key is be chose in Authorization Mode.
Encryption Cipher	By default **Blowfish** is selected.	Specify the Encryption Cipher. Selected the Blowfish/AES-256/AES-192/AES-128/None.
Hash Algorithm	By default **SHA-1** is selected.	Specify the Hash Algorithm. Selected the SHA-1/MD5/MD4/SHA2-256/SHA2-512/None.
Advanced Configuration	The box is unchecked by default.	Specify the OpenVPN client **Advanced Configuration** setting. If it is checked, **Advanced Configuration** will be display below.
Tunnel	The box is unchecked by default	When click Enable, it will enable this OpenVPN tunnel.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	Click the **Back** button to return the last page.

When select Advanced Configuration in OpenVPN Server Configuration will appear.



OpenVPN Client Advanced Configuration		
Item	**Value setting**	**Description**
TLS Cipher	By default TLS-RSA-WITH-AES128-SHA is selected.	Specify the OpenVPN client **TLS Cipher.** Note_1: TLS Cipher will be available only when TLS is be chose in Authorization Mode.
LZO Compression	By default Adaptive is selected.	Specify the OpenVPN client **LZO Compression.**
TLS Auth. Key (Optional)	String format: any text	Specify the OpenVPN client **TLS Auth. Key.** Note_1: TLS Auth. Key will be available only when TLS is be chose in Authorization Mode.
User Name (Optional)	String format: any text	Specify the OpenVPN client **User Name.**
Password (Optional)	String format: any text	Specify the OpenVPN client **Password.**
NAT	The box is unchecked by default.	Specify the OpenVPN client **NAT.**
Bridge TAP to	By default VLAN1 is selected	Specify the OpenVPN client **Bridge TAP to.** Note_1: Bridge TAP to will be available only when TAP is be chose in Tunnel Device and NAT is unchecked.
Firewall Protection	The box is unchecked by default.	Specify the OpenVPN client **Firewall Protection.** Note_1: Firewall Protection will be available only when NAT is checked.

Client IP Address	By default Dynamic IP is selected	Specify the Client IP Address. Selected the Dynamic IP/Static IP Select **Static IP** for OpenVPN client which to be. -> Specify IP Address ->Fill in the IP Address. Specify Subnet Mask ->Fill in the Subnet Mask
Tunnel MTU	A Must filled setting The value is 1500 by default	Specify the OpenVPN client **Tunnel MTU.**
Tunnel UDP Fragment	The value is 1500 by default	Specify the OpenVPN client **Tunnel UDP Fragment.** Note_1: Tunnel UDP Fragment will be available only when UDP is be chose in Protocol.
Tunnel UDP MSS-Fix	The box is unchecked by default.	Specify the OpenVPN client **Tunnel UDP MSS-Fix.** Note_1: Tunnel UDP MSS-Fix will be available only when UDP is be chose in Protocol.
nsCertType Verification	The box is unchecked by default.	Specify the OpenVPN client **nsCertType Verification.**
Redirect Internet Traffic	The box is checked by default.	Specify the OpenVPN client Redirect Internet Traffic.
TLS Renegotiation Time (seconds)	The value is 3600 by default	Specify the OpenVPN client **TLS Renegotiation Time.**
Connection Retry (seconds)	The value is -1 by default	Specify the OpenVPN client **Connection Retry.** The value is -1 which represent infinite.
DNS	By default Automatically is selected	Specify the OpenVPN client **DNS.** Selected the Automatically/Manually Select **Manually** for OpenVPN client which to be. -> Specify Primary DNS ->Fill in the Primary DNS. Specify Secondary DNS ->Fill in the Secondary DNS