Grandstream Networks, Inc.

GWN7000 Multi-WAN Gigabit VPN Router

VPN Configuration Guide

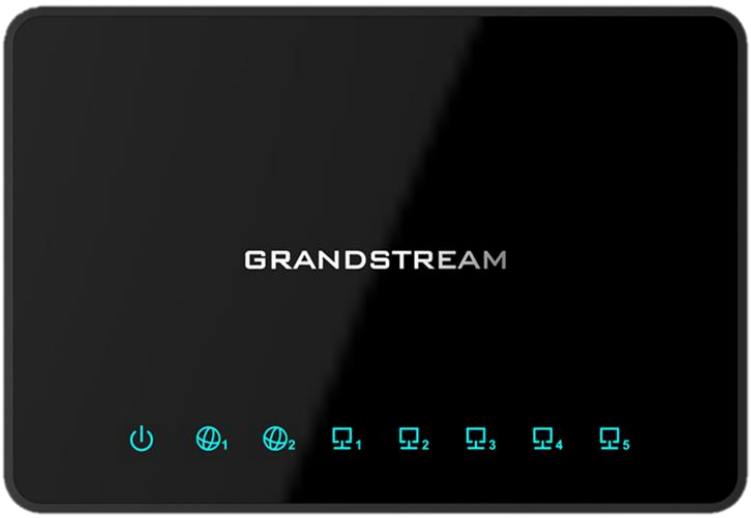

Table of Contents

INTRODUCTION 4

GWN7000 VPN FEATURE 5

OPENVPN® CONFIGURATION 6

OpenVPN® Server Configuration 6

Generate Self-issued Certificate Authority (CA) 6

Generate Server/Client Certificates 8

Create OpenVPN® Server 14

OpenVPN® Client Configuration 16

L2TP/IPSEC CONFIGURATION 20

GWN7000 L2TP/IPSec Client Configuration 20

PPTP CONFIGURATION 22

GWN7000 Client Configuration 22

Table of Figures

Figure 1: VPN Architecture Overview 4
Figure 2: GWN7000 as OpenVPN® Server 5
Figure 3: GWN7000 acting as a VPN Client 5
Figure 4: Create CA Certificate 7
Figure 5: CA Certificate 8
Figure 6: Generate Server Certificates 9
Figure 7: User Management 11
Figure 8: Client Certificat 12
Figure 9: Create OpenVPN® Server 14
Figure 10: OpenVPN® 16
Figure 11: OpenVPN® Client 17
Figure 12: OpenVPN® Client 19
Figure 13: L2TP Client Configuration 20
Figure 14: L2TP Client 21
Figure 15: PPTP Client Configuration 22
Figure 16: PPTP Client 23

Table of Tables

Table 1: CA Certificate 7
Table 2: Server Certificate 9
Table 3: Client Certificat 12
Table 4: OpenVPN® Server 15
Table 5: OpenVPN® Client 18
Table 6: L2TP Configuration 21
Table 7: PPTP Configuration 23

INTRODUCTION

A Virtual Private Network (VPN) is used to create an encrypted connection enabling users to exchange data across shared or public networks acting as clients connected to a private network. The benefit of using a VPN is to ensure the appropriate level of security to connected systems when the underlying network infrastructure alone cannot provide it. The most common types of VPNs are remote-access VPNs and site-to-site VPNs.

VPNs can be defined between specific end points such as IP-Phones and computers, and servers in separate data centers, when security requirements for their exchanges exceed what the enterprise network can deliver. Increasingly, enterprises use VPNs to secure data and voice exchange.

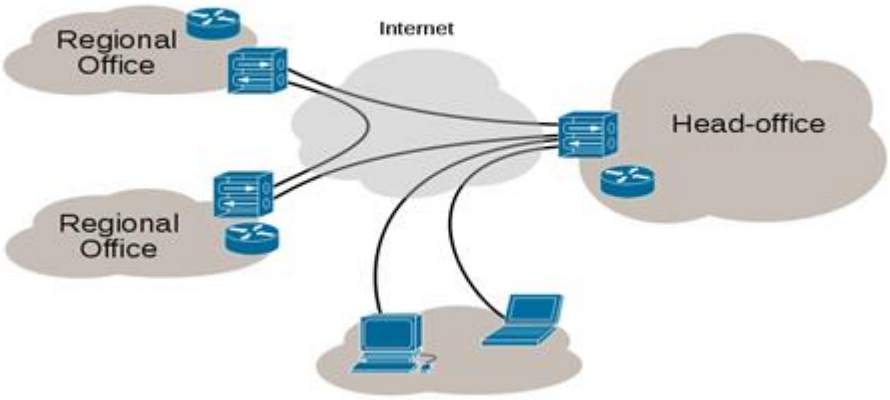

Figure 1: VPN Architecture Overview

The VPN security model provides:

- Client authentication to forbid any unauthorized user from accessing the VPN network.
- Encryption and confidentiality that will prevent man in middle attacks and eavesdropping on the network traffic.
- Data integrity to maintain the consistency, and trustworthiness of the messages exchanged.

Users must be authenticated before establishing secure VPN tunnels. Client/server tunnels use passwords or digital certificates. It is possible to permanently store the key to allow the tunnel to be established automatically.

The purpose of this guide is to underline VPN client/server feature on Grandstream GWN7000 Router. This guide covers OpenVPN® client/server configuration, L2TP client configuration and PPTP client configuration.

© 2002-2014 OpenVPN Technologies, Inc.
OpenVPN is a registered trademark of OpenVPN Technologies, Inc

GWN7000 VPN FEATURE

Grandstream GWN7000 router supports VPN feature giving ability to create an encrypted connection across shared or public networks allowing users to exchange data securely. GWN7000 router supports 3 VPN types:

- **OpenVPN®:** GWN7000 can act as VPN server with remote VPN clients, or it can as VPN client connected to a remote VPN server.
- **L2TP/IPSec:** GWN7000 can act as VPN client only and it can be connected to remote L2TP server.
- **PPTP:** GWN7000 can act as VPN client only and it can be connected to remote PPTP server.

The following figure illustrates GWN7000 acting as an OpenVPN® server with remote clients connected via VPN tunnel.

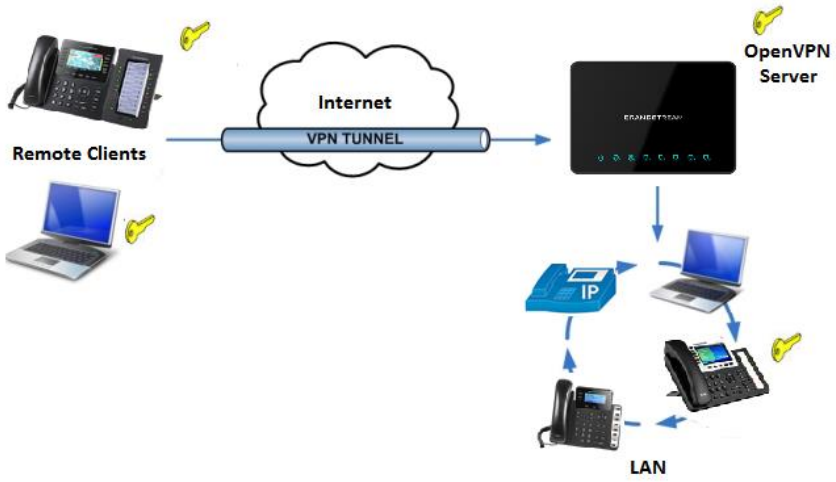

Figure 2: GWN7000 as OpenVPN® Server

The following figure illustrates GWN7000 acting as OpenVPN®, L2TP or PPTP client connected to a remote VPN server.

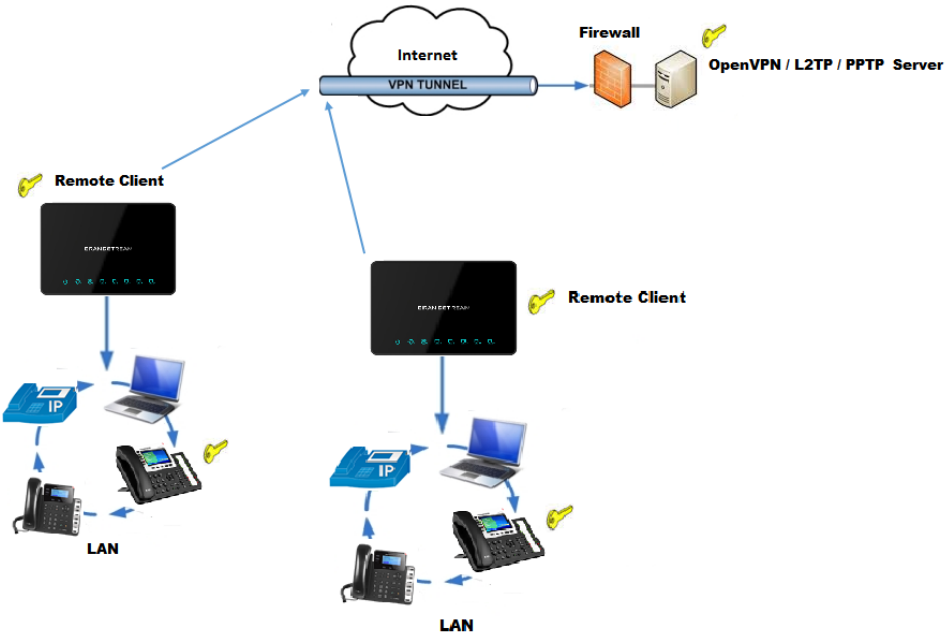

Figure 3: GWN7000 acting as a VPN Client

OPENVPN® CONFIGURATION

VPN configuration is accessible from the GWN7000 web GUI under “VPN”. Three options are available, OpenVPN®, L2TP/IPSec or PPTP.

OpenVPN® Server Configuration

To use the GWN7000 as an OpenVPN® server, users need to start creating OpenVPN® certificates and client certificates. Before generating server/client certificates, users should generate first the Certificate Authority (CA) which will help to issue server/clients certificates.

GWN7000 certificates can be managed from web UI > System Settings > Cert. Manager.

Generate Self-issued Certificate Authority (CA)

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

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

1. Go to “System Settings > Cert. Manager > CAs” on the GWN7000 web GUI.
2. Click on

button. A popup window will appear.
3. Enter the CA values including CN, Key Length, Digest algorithm… depending on your needs.

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

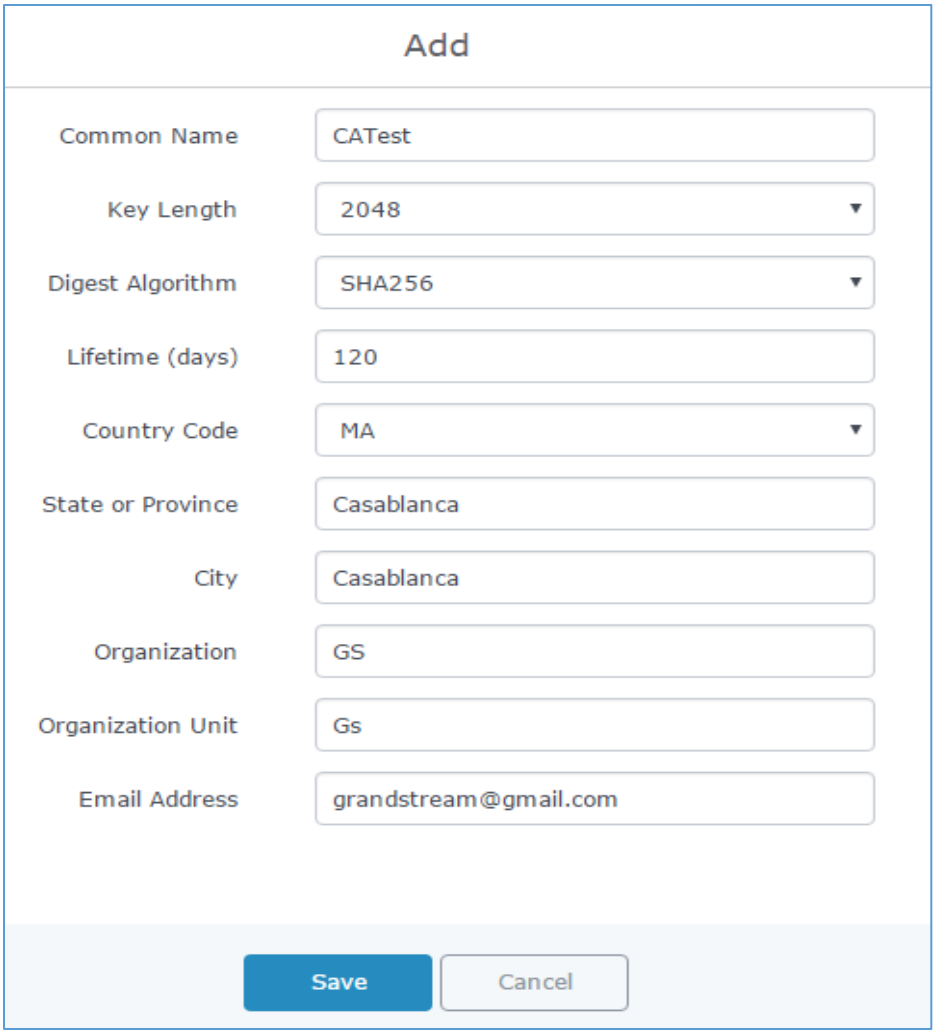

Figure 4: Create CA Certificate

Table 1: CA Certificate

Field	Description
Common Name	Enter the common name for the CA. It could be any name to identify this certificate. In our example, set to “CATest”.
Key Length	Choose the key length for generating the CA certificate. Following values are available: • **1024**: 1024-bit keys are no longer sufficient to protect against attacks. • **2048**: 2048-bit keys are a good minimum. (Recommended). • **4096**: 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.

Digest Algorithm	Choose the digest algorithm: • **SHA1:** This digest algorithm provides a 160-bit fingerprint output based on arbitrary length input. • **SHA-256:** This digest algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one-way function – it cannot be decrypted back.
Lifetime (days)	Enter the validity date for the CA certificate in days. In our example, set to "120".
Country Code	Select a country code from the dropdown list. In our example, set "MA".
State or Province	Enter a state name or province. In our example, set to "Casablanca".
City	Enter a city name. In our example, set to "Casablanca".
Organization	Enter the organization name. In our example, set to "GS".
Organization Unit	Enter the organization unit name. In our example, set to "Gs".
Email Address	Enter an email address. In our example its "grandstream@gmail.com"

4. Click on Save button after completing all the fields for the CA certificate.
5. Click on button to export the CA to local computer. The CA file has extension ".crt".

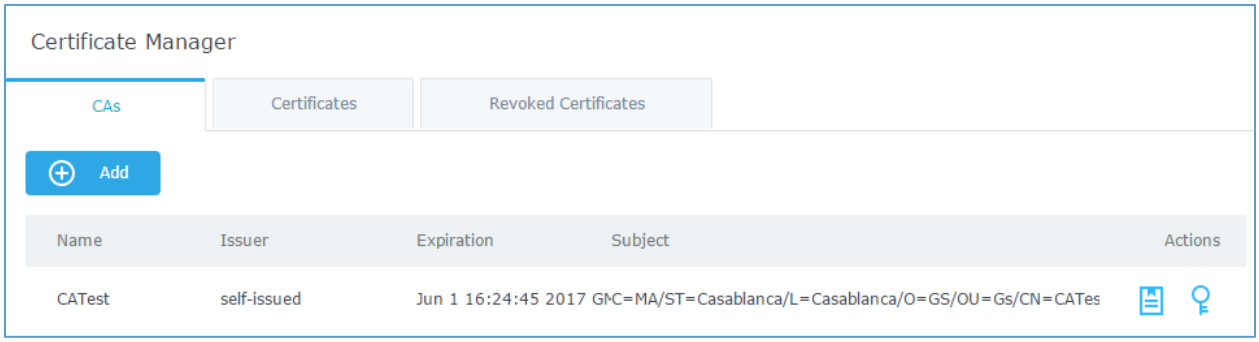

Figure 5: CA Certificate

Generate Server/Client Certificates

Users need to create both server and client certificates for encrypted communication between clients and GWN7000 acting as an OpenVPN® server.

❖ Creating Server Certificate

To create server certificate, follow below steps:

1. Go to "System Settings > Cert. Manager > Certificates".

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

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

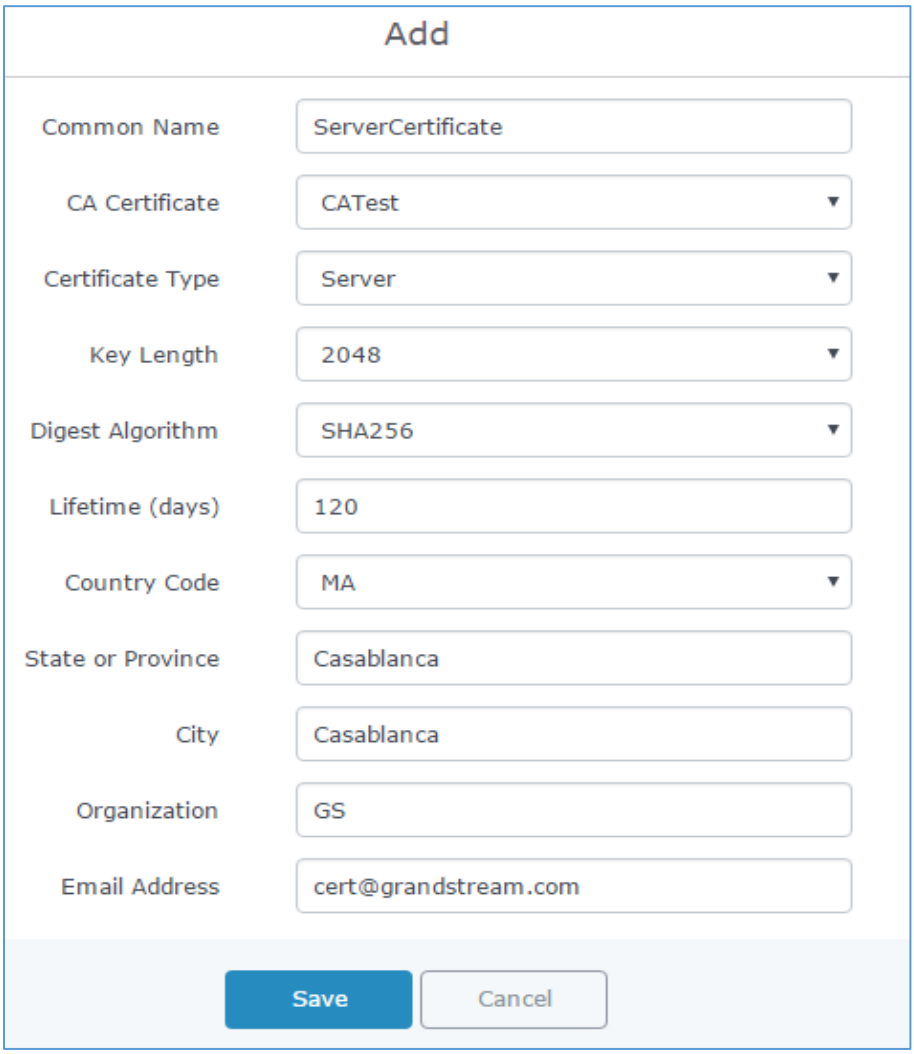

Figure 6: Generate Server Certificates

Table 2: Server Certificate

Field	Description
Common Name	Enter the common name for the server certificate. It could be any name to identify this certificate. In our example, set to “ServerCertificate”.
CA Certificate	Select CA certificate previously generated from the dropdown list. In our example, “CATest”.
Certificate Type	Choose the certificate type from the dropdown list. It can be either a client or a server certificate. Choose “Server” to generate server certificate.

Key Length	Choose the key length for generating the server certificate. Following values are available: • **1024**: 1024-bit keys are no longer sufficient to protect against attacks. Not recommended. • **2048**: 2048-bit keys are a good minimum. Recommended. • **4096**: 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.
Digest Algorithm	Choose the digest algorithm: • **SHA1:** This digest algorithm provides a 160-bit fingerprint output based on arbitrary length input. • **SHA-256:** This digest algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one-way function – it cannot be decrypted back
Lifetime (days)	Enter the validity date for the server certificate in days. In our example, set to "120".
Country Code	Select a country code from the dropdown list. In our example, set to "MA".
State or Province	Enter a state name or province. In our example, set to "Casablanca".
City	Enter a city name. In our example, set to "Casablanca".
Organization	Enter the organization name. In our example, set to "GS".
Email Address	Enter an email address. In our example its "Cert@grandstream.com".

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

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

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

Click on button to revoke the server certificate if no longer needed.

Notes:

- The server certificates (.crt and .key) will be used by the GWN7000 when acting as a server.
- The server certificates (.crt and .key) can be exported and used on another OpenVPN® server.

❖ Creating Client Certificate

To create client certificate, follow below steps:

1- Create Users

a. Go to “System Settings > User Manager”.

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

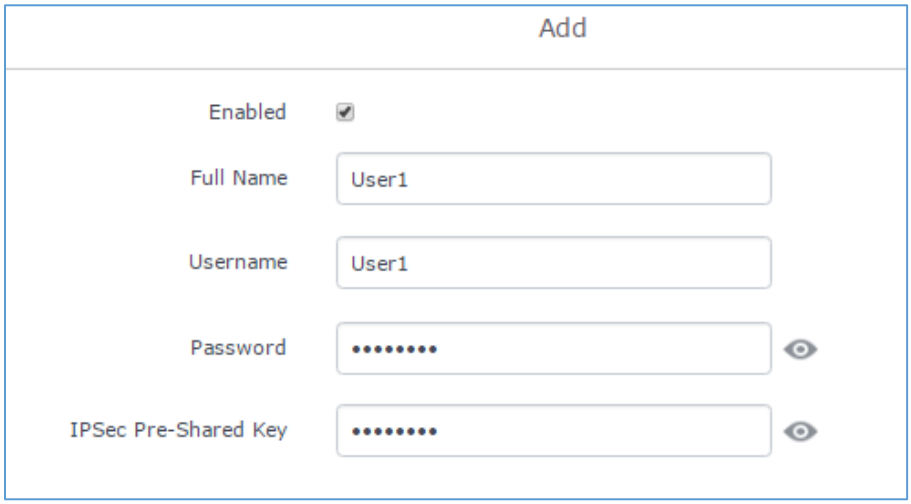

Figure 7: User Management

c. Enter User information based on below descriptions.

Field	Description
Enabled	Check to enable the user.
Full Name	Choose full name to identify the users.
Username	Choose username to distinguish client’s certificate.
Password	Enter user password for each username.
IPSec Pre-Shared Key	Enter the pre-shared key to connect to VPN server. This field is used when clients are using pre-shared key.

d. Repeat above steps for each user.

2- Create Client Certificate

a. Go to “System Settings > Cert. Manager > Certificates”.

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

c. Enter client certificate information based on below descriptions.

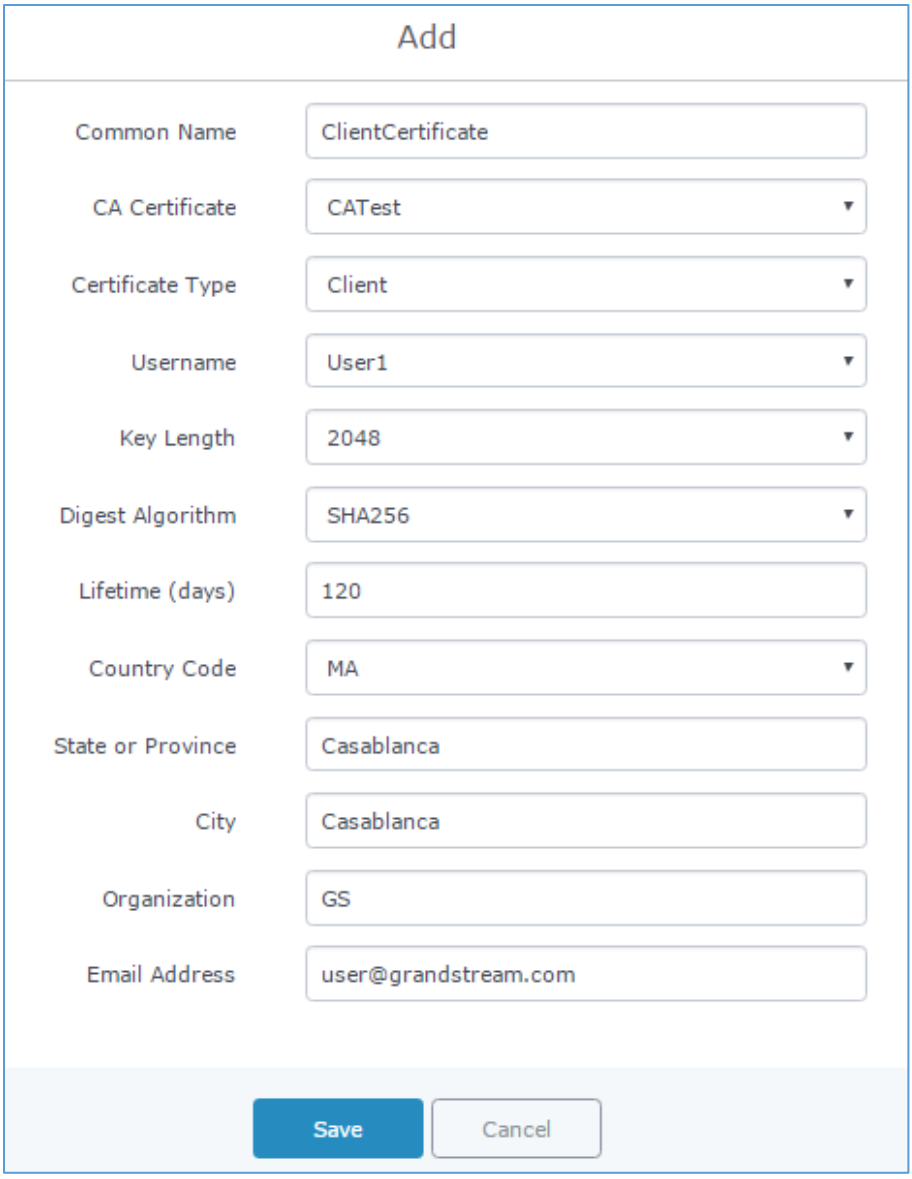

Figure 8: Client Certificat

Table 3: Client Certificat

Field	Description
Common Name	Enter the common name for the client certificate. It could be any name to identify this certificate. In our example, set to “ClientCertificate”.
CA Certificate	Select the generated CA certificate from the dropdown list. In our example, select “CATest”.
Certificate Type	Choose the certificate type from the dropdown list. It can be either a client or server certificate. In our example, select “Client”.
Username	Select created user to generate his certificate. In our example, select “User1”.

Key Length	Choose the key length for generating the client certificate. Following values are available: • **1024**: 1024-bit keys are no longer sufficient to protect against attacks. Not recommended. • **2048**: 2048-bit keys are a good minimum. Recommended. • **4096**: 4096-bit keys are accepted by nearly all RSA systems. Using 4096-bit keys will dramatically increase generation time, TLS handshake delays, and CPU usage for TLS operations.
Digest Algorithm	Choose the digest algorithm: • **SHA1:** This digest algorithm provides a 160-bit fingerprint output based on arbitrary length input. • **SHA-256:** This digest algorithm generates an almost-unique, fixed size 256-bit (32-byte) hash. Hash is a one-way function – it cannot be decrypted back
Lifetime (days)	Enter the validity date for the client certificate in days. In our example, set to "120".
Country Code	Select a country code from the dropdown list. In our example, set to "MA".
State or Province	Enter a state name or province. In our example, set to "Casablanca".
City	Enter a city name. In our example, set to "Casablanca".
Organization	Enter the organization name. In our example, set to "GS".
Email Address	Enter an email address. In our example, set to "user@grandstream.com".

d. Click on Save after completing all the fields for the client certificate.

e. Click on to export the client certificate file in ".crt" format.

f. Click on to export the client key file in ".key" format.

Click on to revoke the client certificate if no longer needed.

The client certificates (".crt" and ".key") will be used by clients connected to the GWN7000 in order to establish TLS handshake.

Notes:

- Client certificates generated from the GWN7000 need to be uploaded to the clients.
- For security improvement, each client needs to have his own username and certificate, this way even if a user is compromised, other users will not be affected.

Create OpenVPN® Server

Once client and server certificates are successfully created, users can create a new server, so that clients can be connected to it, by navigating under “VPN > OpenVPN® > Server”.

To create a new VPN server, follow below steps:

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

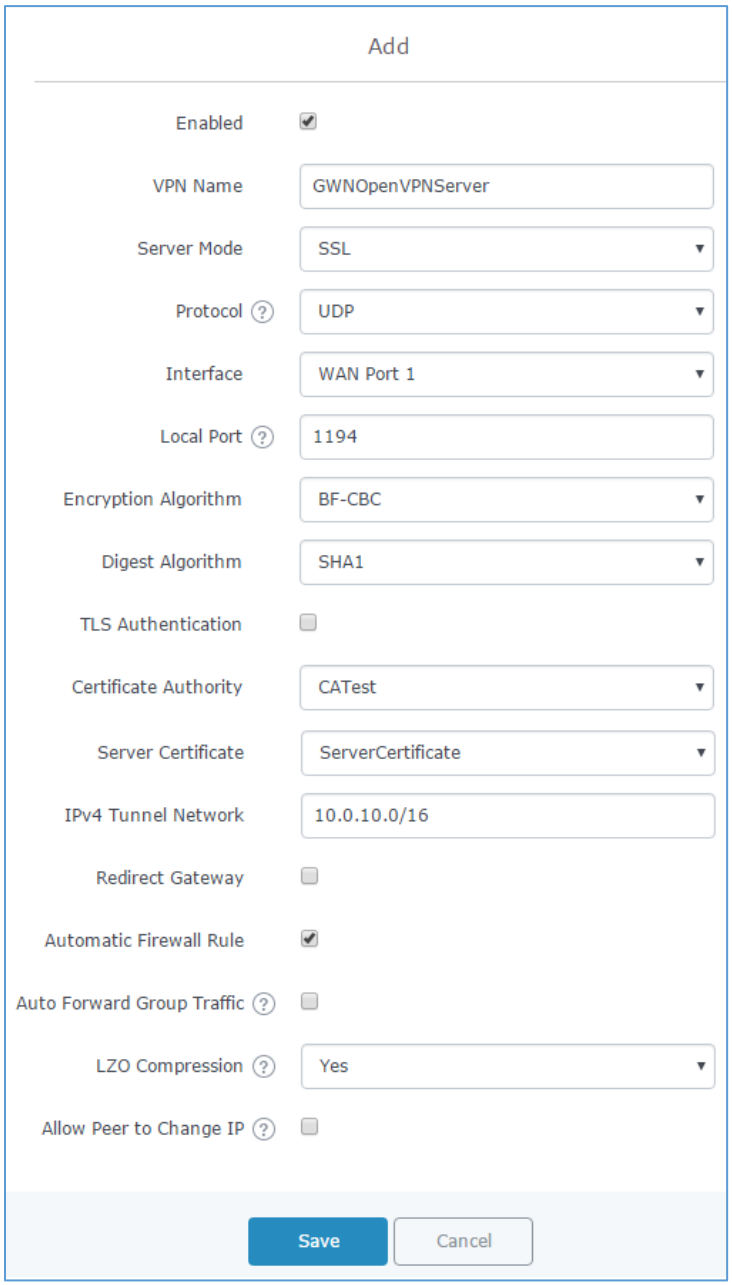

Figure 9: Create OpenVPN® Server

Table 4: OpenVPN® Server

Field	Description
Enable	Click on the checkbox to enable the OpenVPN® server feature.
VPN Name	Enter a name for the OpenVPN® server.
Server Mode	Choose the server mode the OpenVPN® server will operate with. 4 modes are available: • **PSK:** used to establish a point-to-point OpenVPN® configuration. A VPN tunnel will be created with a server endpoint of a specified IP and a client endpoint of specified IP. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN® port. • **SSL:** Authentication is made using certificates only (no user/pass authentication). Each user has a unique client configuration that includes their personal certificate and key. This is useful if clients should not be prompted to enter a username and password, but it is less secure as it relies only on something the user has (TLS key and certificate). • **User Auth:** Authentication is made using only CA, user and password, no certificates. Useful if the clients should not have individual certificates. Less secure as it relies on a shared TLS key plus only something the user knows (Username/password). • **SSL + User Auth:** Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key. Most secure as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know).
Protocol	Choose the Transport protocol from the dropdown list, either TCP or UDP. The default protocol is UDP.
Interface	Select the interface used to connect the GWN7000 to the uplink, either WAN1, WAN2 or All.
Local Port	Configure the listening port for OpenVPN® server. The default value is 1194.
Encryption Algorithm	Choose the encryption algorithm from the dropdown list to encrypt data so that the receiver can decrypt it using same algorithm.
Digest Algorithm	Choose digest algorithm from the dropdown list, which will uniquely identify the data to provide data integrity and ensure that the receiver has an unmodified data from the one sent by the original host.

TLS Authentication	This option uses a static Pre-Shared Key (PSK) that must be generated in advance and shared among all peers. This feature adds extra protection to the TLS channel by requiring that incoming packets have a valid signature generated using the PSK key.
TLS Pre-Shared Key	Enter the generated TLS Pre-Shared Key when using TLS Authentication.
Certificate Authority	Select a generated CA from the dropdown list.
Server Certificate	Select a generated Server Certificate from the dropdown list.
IPv4 Tunnel Network	Enter the network range that the GWN7000 will be serving from to the OpenVPN® client. **Note:** The network format should be the following **10.0.10.0/16**. The mask should be at least 16 bits.
Redirect Gateway	When redirect-gateway is used, OpenVPN® clients will route DNS queries through the VPN, and the VPN server will need to handle them.
Automatic Firewall Rule	Enable automatic firewall rule.
Auto Forward Group Traffic	If enabled, choose which groups you want to forward, if not, you can manually configure the forward rules under firewall settings.
LZO Compression	Select whether to activate LZO compression or no, if set to "Adaptive", the server will make the decision whether this option will be enabled or no.
Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.

2. Click Save after completing all the fields.
3. Click Apply on top of the web GUI to apply changes.

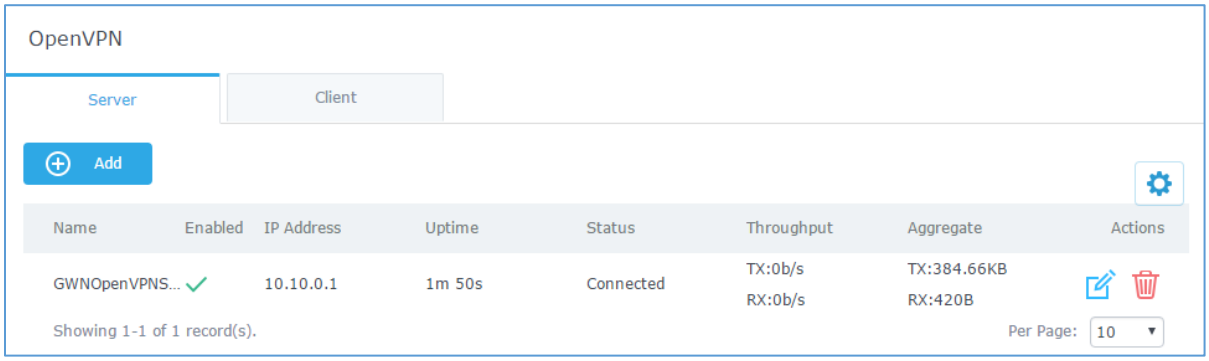

Figure 10: OpenVPN®

OpenVPN® Client Configuration

There are two ways to use the GWN7000 as an OpenVPN® client:

1) Upload client certificate created from an OpenVPN® server to GWN7000.
2) Create client/server certificates on GWN7000 and upload server certificate to the OpenVPN® server.

Go to “VPN > OpenVPN® > Client” and follow steps below:

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

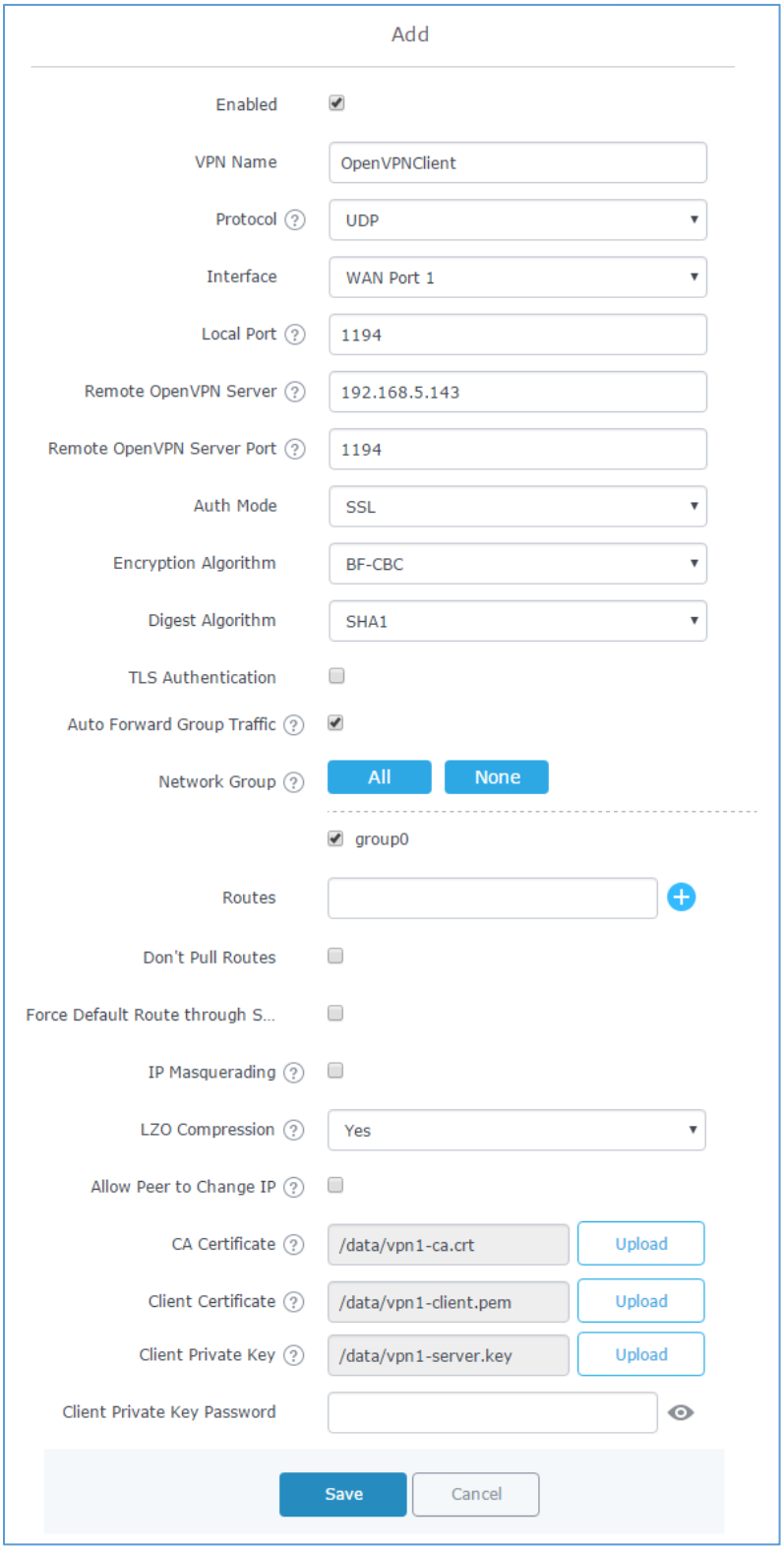

Figure 11: OpenVPN® Client

Table 5: OpenVPN® Client

Field	Description
Enable	Click on the checkbox to enable the OpenVPN® client feature.
VPN Name	Enter a name for the OpenVPN® client.
Protocol	Choose the Transport protocol from the dropdown list, either TCP or UDP. The default protocol is UDP.
Interface	Select the interface used to connect the GWN7000 to the uplink, either WAN1, WAN2 or All.
Local Port	Configure the listening port for OpenVPN® server. The default value is 1194.
Remote OpenVPN® Server	Configure the remote OpenVPN® server IP address.
Remote OpenVPN® Server Port	Configure the remote OpenVPN® server port.
Auth Mode	Choose the server mode the OpenVPN® server will operate with, 4 modes are available: • **PSK:** used to establish a point-to-point OpenVPN® configuration. A VPN tunnel will be created with a server endpoint of a specified IP and a client endpoint of specified IP. Encrypted communication between client and server will occur over UDP port 1194, the default OpenVPN® port. • **SSL:** Authentication is made using certificates only (no user/pass authentication). Each user has a unique client configuration that includes their personal certificate and key. This is useful if clients should not be prompted to enter a username and password, but it is less secure as it relies only on something the user has (TLS key and certificate). • **User Auth:** Authentication is made using only CA, user and password, no certificates. Useful if the clients should not have individual certificates. Less secure as it relies on a shared TLS key plus only something the user knows (Username/password). • **SSL + User Auth:** Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key. Most secure, as there are multiple factors of authentication (TLS Key and Certificate that the user has, and the username/password they know).
Encryption Algorithm	Choose the encryption algorithm from the dropdown list to encrypt data so that the receiver can decrypt it using the same algorithm.
Digest Algorithm	Choose digest algorithm from the dropdown list, which will uniquely identify the data to provide data integrity and ensure that the receiver has an unmodified data from the one sent by the original host.

TLS Authentication	This option uses a static Pre-Shared Key (PSK) that must be generated in advance and shared among all peers. This feature adds extra protection to the TLS channel by requiring that incoming packets have a valid signature generated using the PSK key.
TLS Pre-Shared Key	Enter the generated TLS Pre-Shared Key when using TLS Authentication.
Auto Forward Group Traffic	If enabled, choose which groups you want to forward, if not, you can manually configure the forward rules under firewall settings.
Routes	This feature allows users to add routes.
Don't Pull Routes	If enabled, client will ignore routes pushed by the server.
Force Default Route through Server	Force a default route to the server.
IP Masquerading	This feature is a form of network address translation (NAT) which allows internal computers with no known address outside their network, to communicate to the outside. It allows one machine to act on behalf of other machines.
LZO Compression	LZO encoding provides a very high compression ratio with good performance. LZO encoding works especially well for CHAR and VARCHAR columns that store very long character strings.
Allow Peer to Change IP	Allow remote change the IP and/or Port, often applicable to the situation when the remote IP address changes frequently.
CA Certificate	Click on "Upload" and select the "CA" certificate generated previously on OpenVPN® server.
Client Certificate	Click on "Upload" and select the "Client Certificate" generated previously on OpenVPN® server.
Client Private Key	Click on "Upload" and select the "Client Private Key" generated previously on OpenVPN® server.
Client Private Key Password	Enter the client private key password

2. Click Save after completing all the fields.
3. Click Apply on top of the web GUI to apply changes.

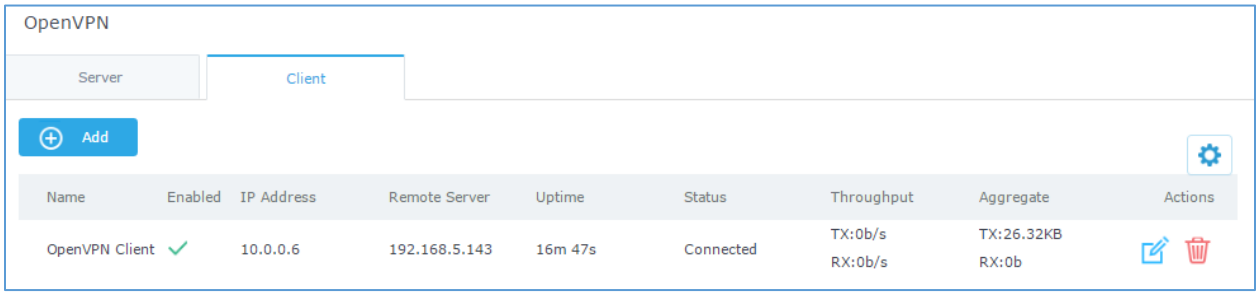

Figure 12: OpenVPN® Client

© 2002-2014 OpenVPN Technologies, Inc.
OpenVPN is a registered trademark of OpenVPN Technologies, Inc

L2TP/IPSEC CONFIGURATION

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

GWN7000 L2TP/IPSec Client Configuration

To configure L2TP client on the GWN7000, go to "VPN > L2TP/IPSec" and set the following:

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

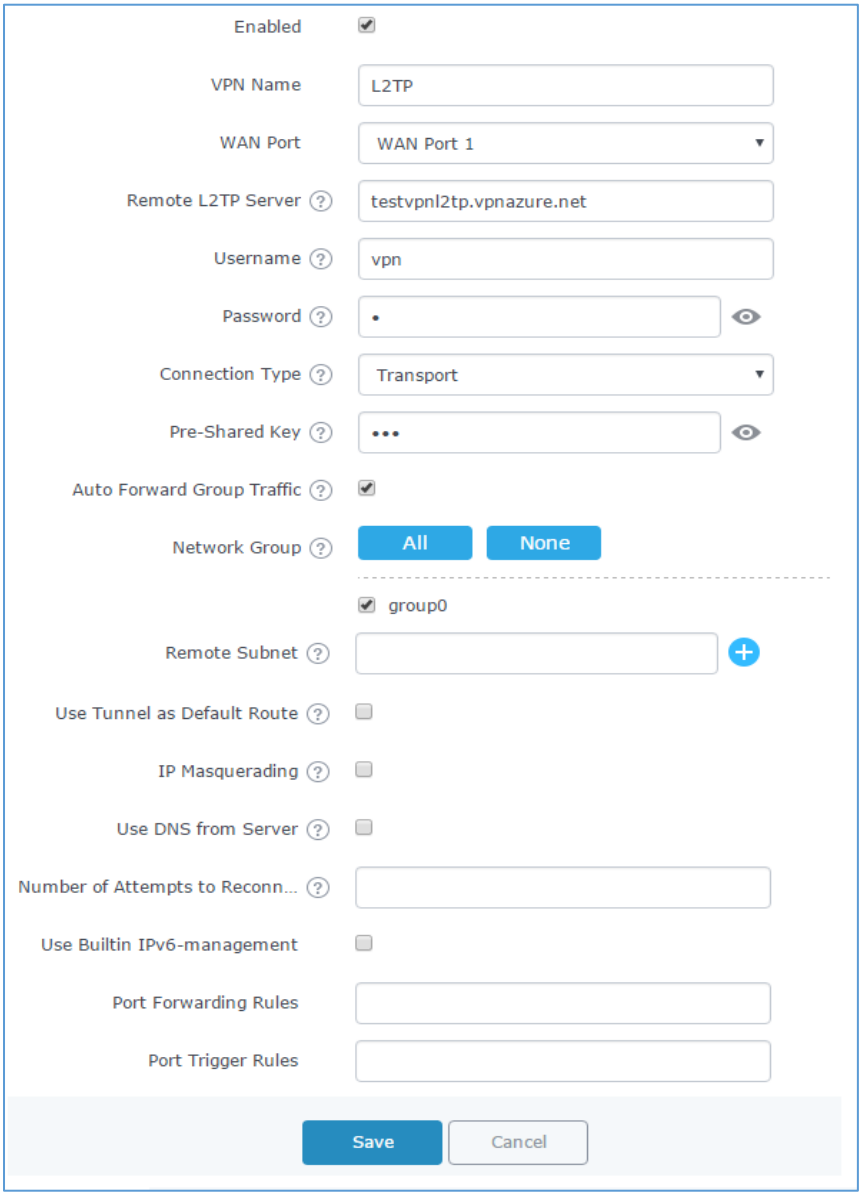

Figure 13: L2TP Client Configuration

Table 6: L2TP Configuration

Field	Description
Enable	Click on the checkbox to enable the L2TP client feature.
VPN Name	Enter a name for the L2TP client.
WAN Port	Select WAN port connected to the uplink, either WAN1 or WAN2.
Remote L2TP Server	Enter the IP/Domain of the remote L2TP Server.
Username	Enter the Username for authentication against the VPN Server.
Password	Enter the Password for authentication against the VPN Server.
Connection Type	Select either Transport mode or Tunnel mode: • **Transport mode** is commonly used between end stations or between an end station and a gateway, if the gateway is being treated as a host. • **Tunnel mode** is used between gateways, or at an end station to a gateway, the gateway acting as a proxy for the hosts behind it.
Pre-Shared Key	Enter the L2TP pre-shared key.
Auto Forward Group Traffic	If enabled, choose which groups you want to forward, if not, you can manually configure the forward rules under firewall settings.
Remote Subnet	Configures the remote subnet for the VPN. The format is "IP/Mask", IP can be either IPv4 or IPv6. For example: 192.168.5.0/24
Use Tunnel as Default Route	If enabled, L2TP/IPSec VPN Tunnel will be used by default.
IP Masquerading	When using L2TP/IPSec client mode, enable this option to allow devices behind GWN7000 to reach L2TP/IPSec server LAN (LAN to LAN scenario). If disabled, only GWN7000 will be able to reach L2TP/IPSec server LAN (client to LAN scenario).
Use DNS from Server	Enable this option to retrieve DNS from the VPN server.
Number of Attempts to Reconnect	Configures the number of attempts to reconnect the L2TP client, if this number is exceeded, the client will be disconnected from the L2TP/IP Server.
Use Built-in IPv6 management	Enable the IPv6 management for the VPN.
Port Forwarding Rules	Enter the port-forwarding rule to be used for the VPN.
Port Trigger Rules	Enter the port trigger rule to be used for the VPN.

2- Click Save after completing all the fields.

3- Click Apply on top of the web GUI to apply changes.

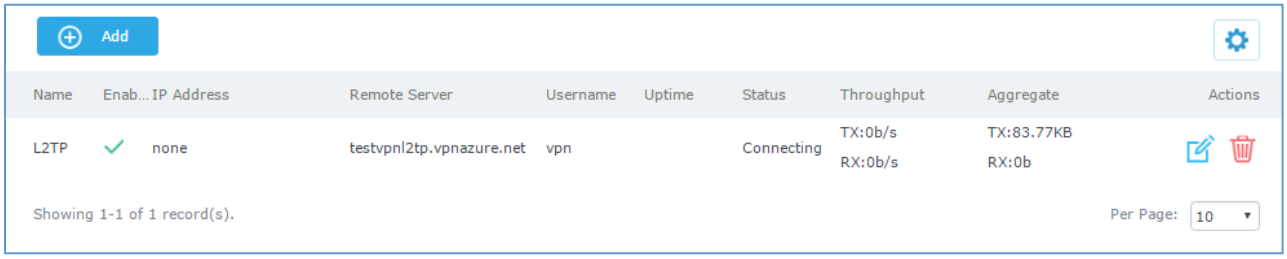

Figure 14: L2TP Client

PPTP CONFIGURATION

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

GWN7000 Client Configuration

To configure PPTP client on the GWN7000, go to "VPN > PPTP" and set the following:

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

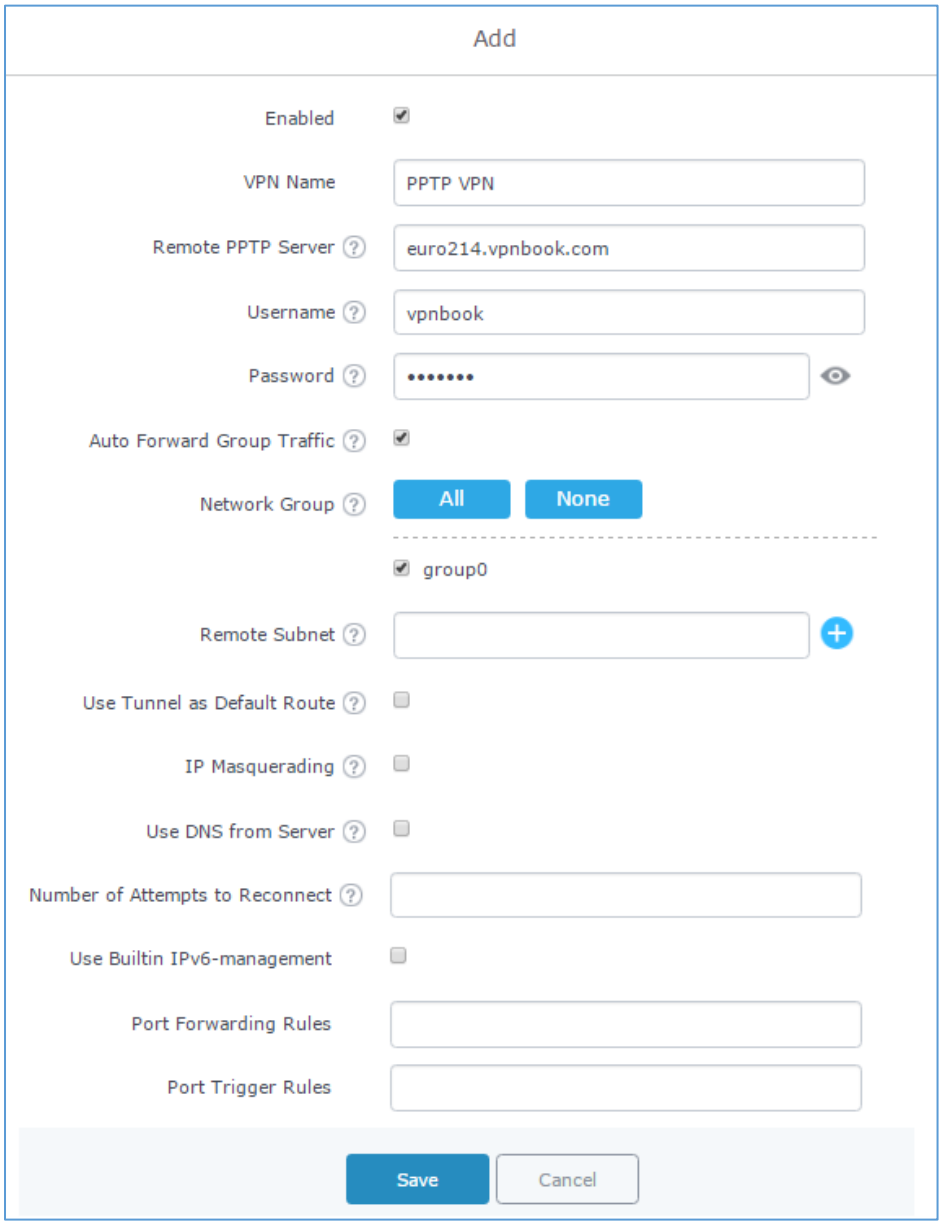

Figure 15: PPTP Client Configuration

Table 7: PPTP Configuration

Field	Description
Enable	Click on the checkbox to enable the PPTP VPN client feature.
VPN Name	Enter a name for the PPTP client.
Remote PPTP Server	Enter the IP/Domain of the remote PPTP Server.
Username	Enter the Username for authentication against the VPN Server.
Password	Enter the Password for authentication against the VPN Server.
Auto Forward Group Traffic	If enabled, choose which groups you want to forward, if not, you can manually configure the forward rules under firewall settings.
Remote Subnet	Configures the remote subnets for the VPN. The format is "IP/Mask", IP can be either IPv4 or IPv6. For example: 192.168.5.0/24
Use Tunnel as Default Route	Enable this option so that PPTP VPN Tunnel will be used by default.
IP Masquerading	When using PPTP client mode, enable this option to allow devices behind GWN7000 to reach PPTP server LAN (LAN to LAN scenario). If disabled, only GWN7000 will be able to reach PPTP server LAN (client to LAN scenario).
Use DNS from Server	Enable this option to retrieve DNS from the VPN server.
Number of Attempts to Reconnect	Configures the number of attempts to reconnect the PPTP client, if this number is exceeded, the client will be disconnected from the PPTP Server.
Use Built-in IPv6 management	Enable the IPv6 management for the VPN.
Port Forwarding Rules	Enter the port-forwarding rule to be used for the VPN.
Port Trigger Rules	Enter the port trigger rule to be used for the VPN.

2- Click Save after completing all the fields.

3- Click Apply on top of the web GUI to apply changes.

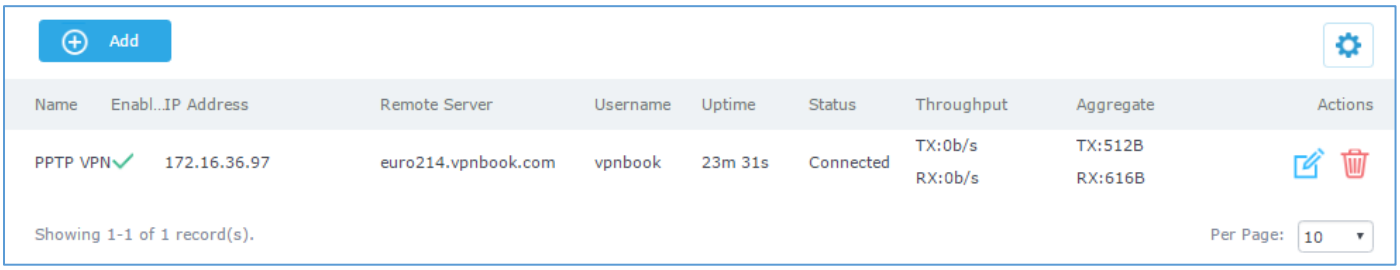

Figure 16: PPTP Client