



Grandstream Networks, Inc.

GWN7000

OpenVPN® Site-to-Site VPN Guide



Table of Contents

| | |
|--|-----------|
| INTRODUCTION | 4 |
| SCENARIO OVERVIEW | 5 |
| CONFIGURATION STEPS | 6 |
| Core Site Configuration | 6 |
| <i>Generate Self-Issued Certificate Authority (CA)</i> | 6 |
| <i>Generate Server/Client Certificates</i> | 7 |
| <i>Create OpenVPN® Server</i> | 11 |
| Branch Site Configuration | 13 |
| VERIFICATION | 16 |



Table of Figures

| | |
|---|----|
| Figure 1: VPN Architecture Overview | 4 |
| Figure 2: Network Diagram | 5 |
| Figure 3: Create CA Certificate | 7 |
| Figure 4: Generate Server Certificates | 8 |
| Figure 5: Create Users | 9 |
| Figure 6: Client Certificate..... | 10 |
| Figure 7: Create OpenVPN® Server | 11 |
| Figure 8: OpenVPN® Server | 13 |
| Figure 9: OpenVPN® Client..... | 14 |
| Figure 10: OpenVPN® Client - Routes | 14 |
| Figure 11: OpenVPN® Client – Upload Certificate and Key | 15 |
| Figure 12: OpenVPN® Client Status from Client Side..... | 15 |
| Figure 13: OpenVPN® Client Status from Server Side | 15 |
| Figure 14: Verification – OpenVPN® Tunnel | 16 |
| Figure 15: Verification – Ping Test..... | 17 |
| Figure 16: Verification – SIP Registration | 17 |

Table of Tables

| | |
|---|----|
| Table 1: OpenVPN® Server Parameters | 12 |
|---|----|



INTRODUCTION

A Virtual Private Network (VPN) is used to create an encrypted connection tunnel, enabling users to exchange data across shared or public networks while 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.

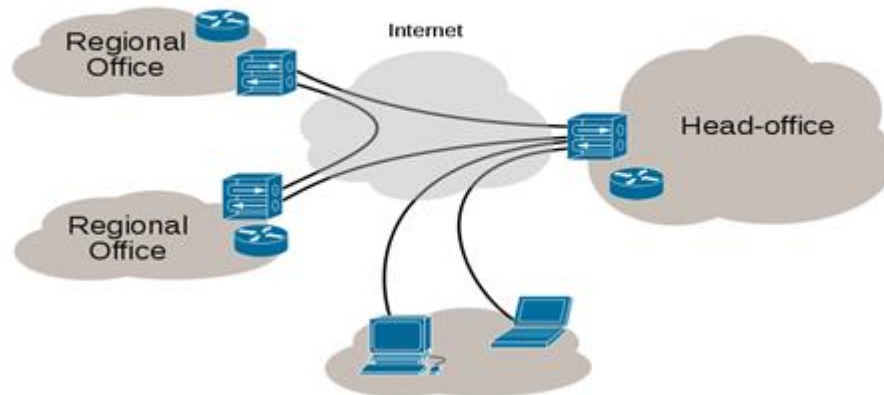


Figure 1: VPN Architecture Overview

The VPN security model provides:

- ✓ Client authentication to forbid any unauthorized user from accessing the VPN network.
- ✓ Encryption, 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.

The purpose of this guide is to underline VPN client/server feature on Grandstream GWN7000 Router and use this feature to implement Site-to-Site VPN using OpenVPN® to connect multiple locations.

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



SCENARIO OVERVIEW

Company ABC has several locations offices connected to the Internet using Grandstream GWN7000 routers and for security reasons the traffic between the main office in LA and one of the branch offices in NY, the admin has decided to establish a VPN Site-to-Site between the two sites to ensure that sensitive data between the two networks is forwarded securely into the encrypted tunnel. This will allow also phone calls to go encrypted and protected against possible rogue eavesdropping of phone calls between the two offices.

- ✓ The main office has a LAN subnet with range of: **192.168.1.0/24**
- ✓ The branch office has a LAN Subnet with range of: **192.168.3.0/24**
- ✓ The VPN tunnel will have the following IP range: **10.1.1.0/24**

The figure below shows the actual diagram of the network:

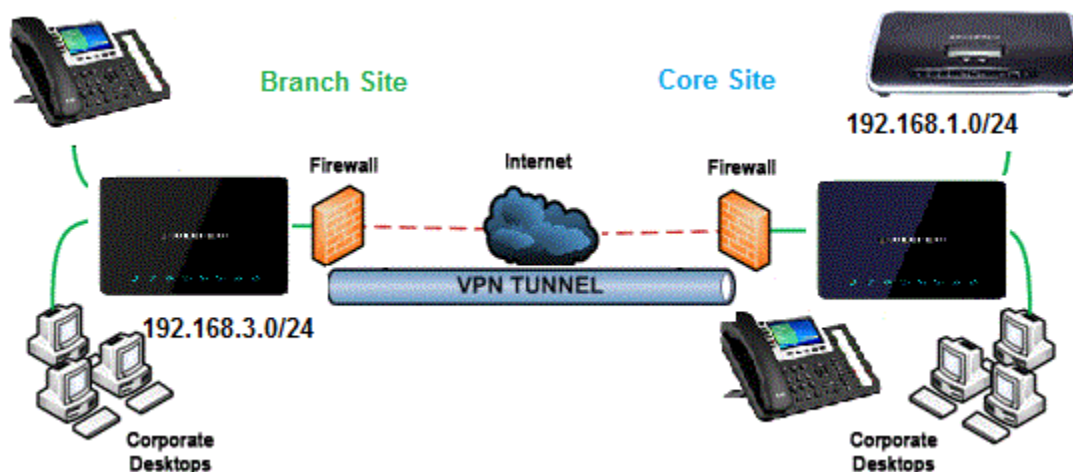


Figure 2: Network Diagram

The main design is to set the client/server architecture to implement the VPN Tunnel, currently GWN supports client/server for both OpenVPN® and PPTP technologies, we will cover through this guide the necessary configurations that are needed to establish the connection and provide at the end some verification procedures.



CONFIGURATION STEPS

In this guide, we are providing necessary steps configuration needed to achieve the described scenario on the first section. For more detailed descriptions for each configuration field/parameter, please refer to [GWN7000 User Manual](#) or [GWN7000 VPN Guide](#).


Core Site Configuration

First, we start by setting up the core site side, we will need to implement an OpenVPN® Server which will be accepting connection from OpenVPN® clients enabled on remote branch offices/sites.

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.



| Add | |
|-------------------|--|
| Common Name | <input type="text" value="CoreSite"/> |
| Key Length | <input type="text" value="512"/> ▼ |
| Digest Algorithm | <input type="text" value="SHA1"/> ▼ |
| Lifetime (days) | <input type="text" value="90"/> |
| Country Code | <input type="text" value="US"/> ▼ |
| State or Province | <input type="text" value="CA"/> |
| City | <input type="text" value="LA"/> |
| Organization | <input type="text" value="GS"/> |
| Organization Unit | <input type="text" value="Main"/> |
| Email Address | <input type="text" value="direction@grandstream.com"/> |

Figure 3: Create CA Certificate


4. Click on  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”.

Generate Server/Client Certificates

Administrator needs to create both server and client certificates for encrypted communication between clients and GWN7000 acting as an OpenVPN® server at the core site.

✓ Creating Server Certificate

To create server certificate, follow below steps:

1. Go to **“System Settings→Cert. Manager→Certificates”**.
2. Click on  button. A popup window will appear.

Refer to below figure showing an example of configuration.



| Add | |
|-------------------|--|
| Common Name | <input type="text" value="CoreOffice"/> |
| CA Certificate | <input type="text" value="CoreSite"/> ▼ |
| Certificate Type | <input type="text" value="Server"/> ▼ |
| Key Length | <input type="text" value="512"/> ▼ |
| Digest Algorithm | <input type="text" value="SHA1"/> ▼ |
| Lifetime (days) | <input type="text" value="90"/> |
| Country Code | <input type="text" value="US"/> ▼ |
| State or Province | <input type="text" value="CA"/> |
| City | <input type="text" value="LA"/> |
| Organization | <input type="text" value="GS"/> |
| Email Address | <input type="text" value="direction@grandstream.com"/> |


Figure 4: Generate Server Certificates

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

✓ **Creating Client Certificate**

To create client certificate, follow below steps:

1- Create Users

- a. Go to **“System Settings→User Manager”**.
- b. Click on  button. The following window will pop up.



Edit

Enabled

PPTP Server

Full Name ?

Username

Password 👁

IPSec Pre-Shared Key 👁

Enable PPTP Client Subnet

OpenVPN Subnet -

Add new item +

Figure 5: Create Users

- c. Make sure to enter the branch site LAN IP range in the field “**OpenVPN Subnet**”. This will allow the GWN7000 acting as OpenVPN® server to build a route pointing to that network and send all traffic destined to that IP range to the GWN7000 located on the branch site.
- d. Repeat above steps for each Site.

2- Generate 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.



Add

| | |
|-------------------|--|
| Common Name | <input type="text" value="BranchSite"/> |
| CA Certificate | <input type="text" value="CoreSite"/> ▼ |
| Certificate Type | <input type="text" value="Client"/> ▼ |
| Username | <input type="text" value="BranchSite"/> ▼ |
| Key Length | <input type="text" value="512"/> ▼ |
| Digest Algorithm | <input type="text" value="SHA1"/> ▼ |
| Lifetime (days) | <input type="text" value="90"/> |
| Country Code | <input type="text" value="US"/> ▼ |
| State or Province | <input type="text" value="NY"/> |
| City | <input type="text" value="NY"/> |
| Organization | <input type="text" value="GS"/> |
| Email Address | <input type="text" value="support@grandstream.com"/> |

Figure 6: Client Certificate

- d. Click on  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.

Notes:


- Client certificates generated from the GWN7000 server need to be uploaded to the GWN client.
- 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.

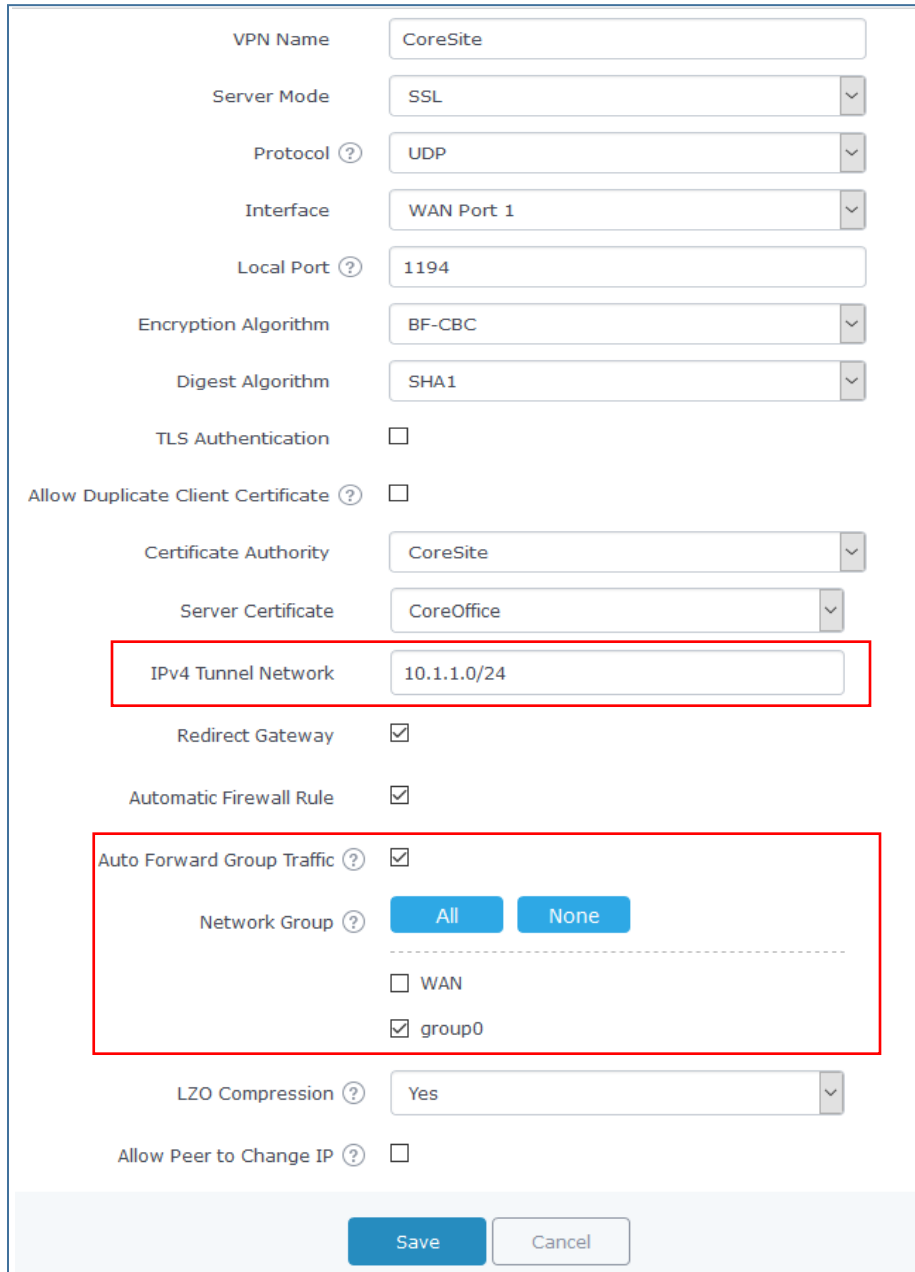


Create OpenVPN® Server

Once client and server certificates are successfully created, administrator can create the OpenVPN® server at the core site router, so that remote branch sites can be connected to it via OpenVPN® client instances.

To create a new VPN server, follow below steps:

1. Go under “**VPN→OpenVPN®→Server**”.
2. Click on  and fill in the required information as shown on the figure below.



VPN Name: CoreSite

Server Mode: SSL

Protocol: UDP

Interface: WAN Port 1

Local Port: 1194

Encryption Algorithm: BF-CBC

Digest Algorithm: SHA1

TLS Authentication:

Allow Duplicate Client Certificate:

Certificate Authority: CoreSite

Server Certificate: CoreOffice

IPv4 Tunnel Network: 10.1.1.0/24

Redirect Gateway:

Automatic Firewall Rule:

Auto Forward Group Traffic:

Network Group: All

WAN:

group0:

LZO Compression: Yes

Allow Peer to Change IP:

Save Cancel

Figure 7: Create OpenVPN® Server




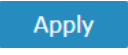
The table below gives the description for each option.

Table 1: OpenVPN® Server Parameters

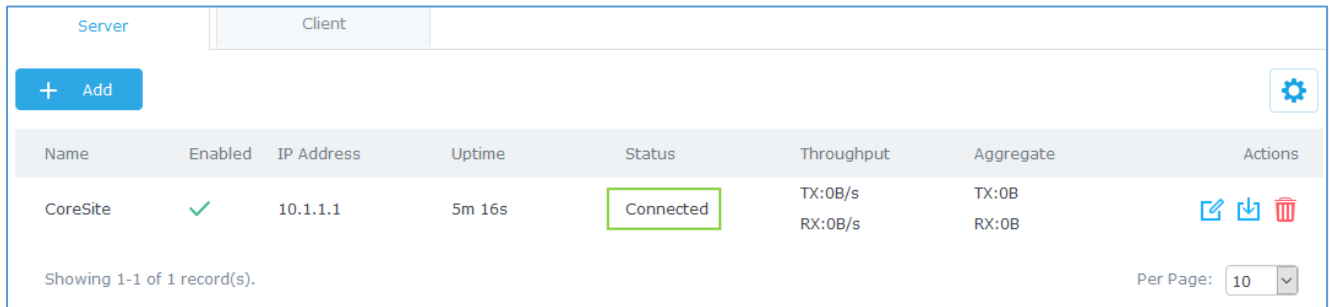
| Field | Description |
|------------------------------|---|
| Enable | Click on the checkbox to enable the OpenVPN® server. |
| VPN Name | Enter a name for the OpenVPN® server. |
| Server Mode | <p>Choose the server mode the OpenVPN® server will operate with. 4 modes are available:</p> <ul style="list-style-type: none"> • PSK: used to establish a point-to-point OpenVPN® configuration. • SSL: Authentication is made using certificates only (no user/pass authentication). • User Auth: Authentication is made using only CA, user and password, no certificates. Useful if the clients should not have individual certificates. • SSL + User Auth: Requires both certificate and username / password. Each user has a unique client configuration that includes their personal certificate and key. |
| 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 | <p>This option uses a static Pre-Shared Key (PSK) that must be generated in advance and shared among all peers.</p> <p>This feature adds extra protection to the TLS channel by requiring that incoming packets have a valid signature generated using the PSK key.</p> |
| 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 on which the GWN7000 OpenVPN® instance will be running and serving IPs to connected clients. Note: In our example, we are using 10.1.1.0/24 |
| 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 and allow access from the VPN tunnel, 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. |

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

Server status can be checked after this under “VPN→OpenVPN®→Server”.







| Name | Enabled | IP Address | Uptime | Status | Throughput | Aggregate | Actions |
|----------|---------|------------|--------|-----------|--------------------|----------------|---|
| CoreSite | ✓ | 10.1.1.1 | 5m 16s | Connected | TX:0B/s RX:0B/s | TX:0B RX:0B |    |

Figure 8: OpenVPN® Server

Branch Site Configuration

Now that the GWN7000 router at the core site is up and running, we move on to configure an OpenVPN® client instance under the GWN7000 router on the branch site. Please follow below steps to set it up.

1. Go to “VPN→OpenVPN®→Client” and follow steps below.
2. Click on  and the following window will pop up.



Edit

Enabled

VPN Name

Protocol

Interface

Local Port

Remote OpenVPN® Server

Remote OpenVPN® Server Port

Auth Mode

Encryption Algorithm

Digest Algorithm

TLS Authentication

Figure 9: OpenVPN® Client

3. Under **Remote OpenVPN® Server** field, put the public IP of the core site router to where the client will initiate tunnel connection.

Auto Forward Group Traffic

Network Group

WAN Port 1

WAN Port 2

group0

Routes

Don't Pull Routes

Force Default Route through Server

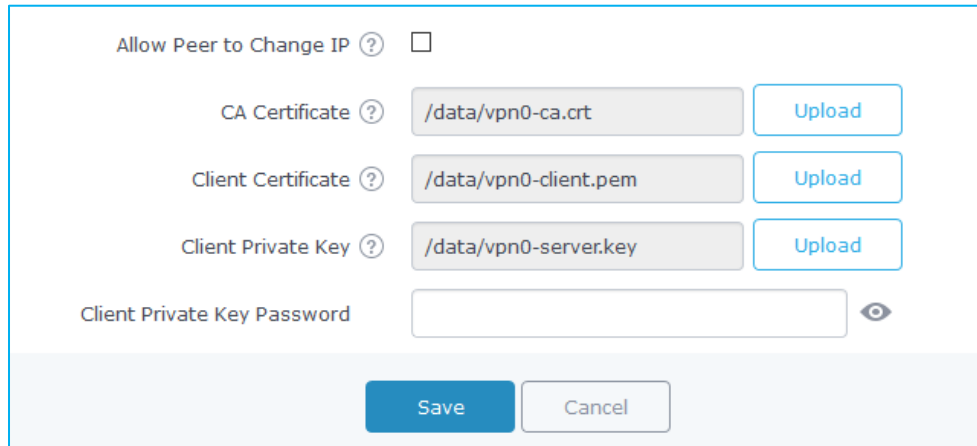
IP Masquerading

LZO Compression

Figure 10: OpenVPN® Client - Routes



- In **Routes** field, add the list of networks that are reachable through the GWN7000 running OpenVPN® server. Here we set the IP range for the core site LAN (i.e. **192.168.1.0/24**).
- The final step would be to upload the client certificate and key, along with CA file which was used to sign the certificates.



Allow Peer to Change IP

CA Certificate

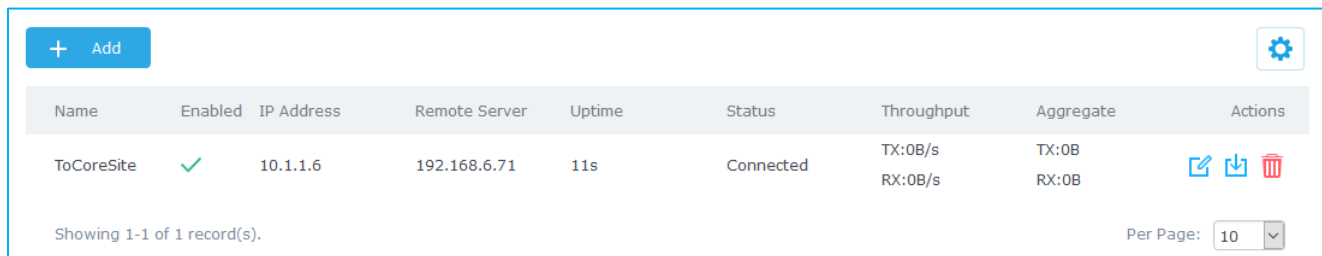
Client Certificate

Client Private Key

Client Private Key Password

Figure 11: OpenVPN® Client – Upload Certificate and Key

- Once this done, press save and apply then check the OpenVPN® client status.

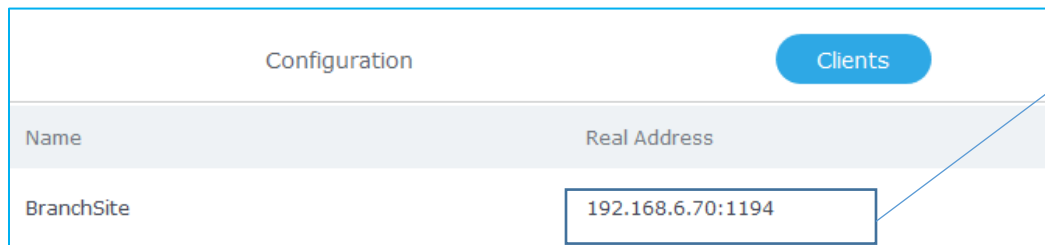


| Name | Enabled | IP Address | Remote Server | Uptime | Status | Throughput | Aggregate | Actions |
|------------|---------|------------|---------------|--------|-----------|--------------------|----------------|---------|
| ToCoreSite | ✓ | 10.1.1.6 | 192.168.6.71 | 11s | Connected | TX:0B/s RX:0B/s | TX:0B RX:0B | |

Showing 1-1 of 1 record(s). Per Page: 10

Figure 12: OpenVPN® Client Status from Client Side

Administrator could check the connected client(s) under the OpenVPN® server under **VPN→OpenVPN®→Server**. hit edit and check the connected clients as shown below:



| Name | Real Address |
|------------|-------------------|
| BranchSite | 192.168.6.70:1194 |

Public IP of branch site should be displayed here.

Figure 13: OpenVPN® Client Status from Server Side



VERIFICATION

For verification purpose, we can do the following:

1. On branch office site, log onto the router and check the routing table to verify that core office LAN is listed as reachable through OpenVPN® tunnel.

| Static Routes | | | | |
|--------------------|-------------|--------|-----------|--|
| IPv4 | IPv6 | Routes | | |
| IPv4 Routes | | | | |
| Target | NextHop | Metric | Interface | |
| 0.0.0.0/0 | 192.168.6.1 | 40 | eth1.1 | |
| 10.1.1.1/32 | 10.1.1.5 | 0 | tun0 | |
| 10.1.1.5/32 | 0.0.0.0 | 0 | tun0 | |
| 192.168.1.0/24 | 10.1.1.5 | 0 | tun0 | |

Figure 14: Verification – OpenVPN® Tunnel

2. Ping from branch site to core site using connected devices to each LAN. Below is a screenshot showing a UCM6102 (IP= 192.168.1.115) on core site initiating successful ping requests to a GXP2140 phone (IP=192.168.3.61) on branch site.



Network Troubleshooting

Ethernet Capture **IP Ping** Traceroute

* Target Host:

Output Result

```

Diagnostic run
PING 192.168.3.61 (192.168.3.61): 56 data bytes
64 bytes from 192.168.3.61: seq=0 ttl=62 time=6.150 ms
64 bytes from 192.168.3.61: seq=1 ttl=62 time=4.800 ms
64 bytes from 192.168.3.61: seq=2 ttl=62 time=5.125 ms
64 bytes from 192.168.3.61: seq=3 ttl=62 time=5.500 ms

--- 192.168.3.61 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 4.800/5.393/6.150 ms
Done
  
```

Figure 15: Verification – Ping Test

3. Finally, users could successfully register phones on branch office to the UCM located on the core site and make phones calls with phones located on core site as well.

| Manage Extensions | | | | | | | |
|--|--------|-----------------|-----------|---------------|-----------------|--------------------------|--------------------|
| <input type="button" value="+ Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/> <input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="E-mail Notification"/> <input type="button" value="Follow Me Options"/> | | | | | | | |
| <input type="checkbox"/> | Status | Presence Status | Extension | CallerID Name | Message | Terminal Type | IP and Port |
| <input type="checkbox"/> | ● Idle | Available | 1000 | | Messages: 0/0/0 | SIP Phone in Branch Site | 192.168.3.225:5060 |
| <input type="checkbox"/> | ● Idle | Available | 1001 | | Messages: 0/0/0 | SIP Phone in Core Site | 192.168.1.61:5060 |

Figure 16: Verification – SIP Registration

