Grandstream Networks, Inc.

GWN7000

PPTP Site-to-Site VPN Guide

Table of Contents

Table of Figures

Table of Tables

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.

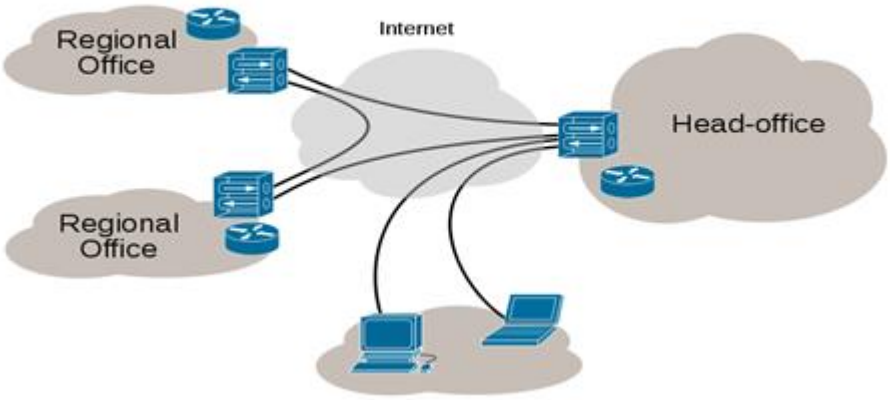

Figure 1: VPN Architecture Overview

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 to connect multiple locations.

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 tunnel between the two sites in order 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 (Start address is 10.1.1.100 and End Address is 10.1.1.200).**

The figure below shows the actual diagram of the network:

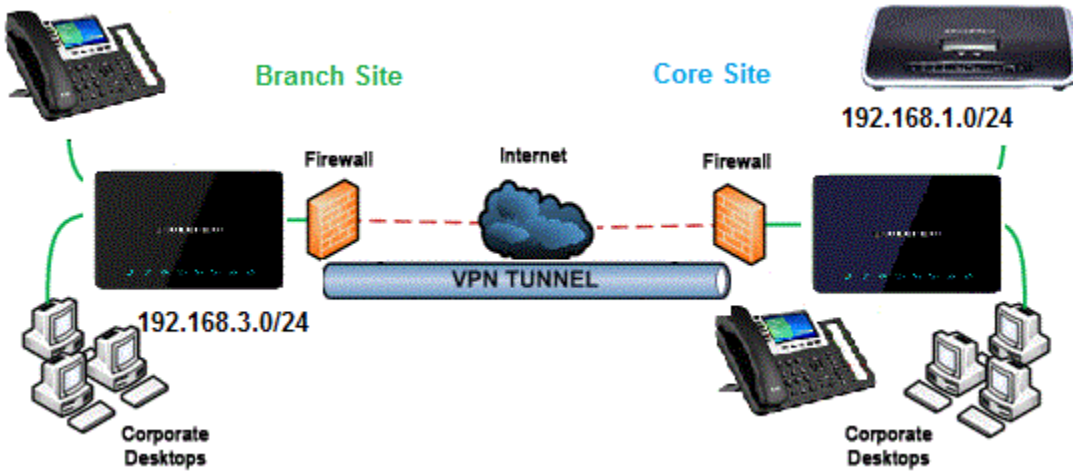

Figure 2: Network Diagram

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 using PPTP protocol 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 where we will need to implement a PPTP server which will be accepting connection from PPTP clients enabled on remote branch offices/sites.

Creating PPTP Users

Administrator needs to create PPTP users under **User Manager** menu to be authenticated by the PPTP server at the core site GWN7000.

To add/create PPTP enabled users, follow below steps:

1. Go to "**System Settings→User Manager**".
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.

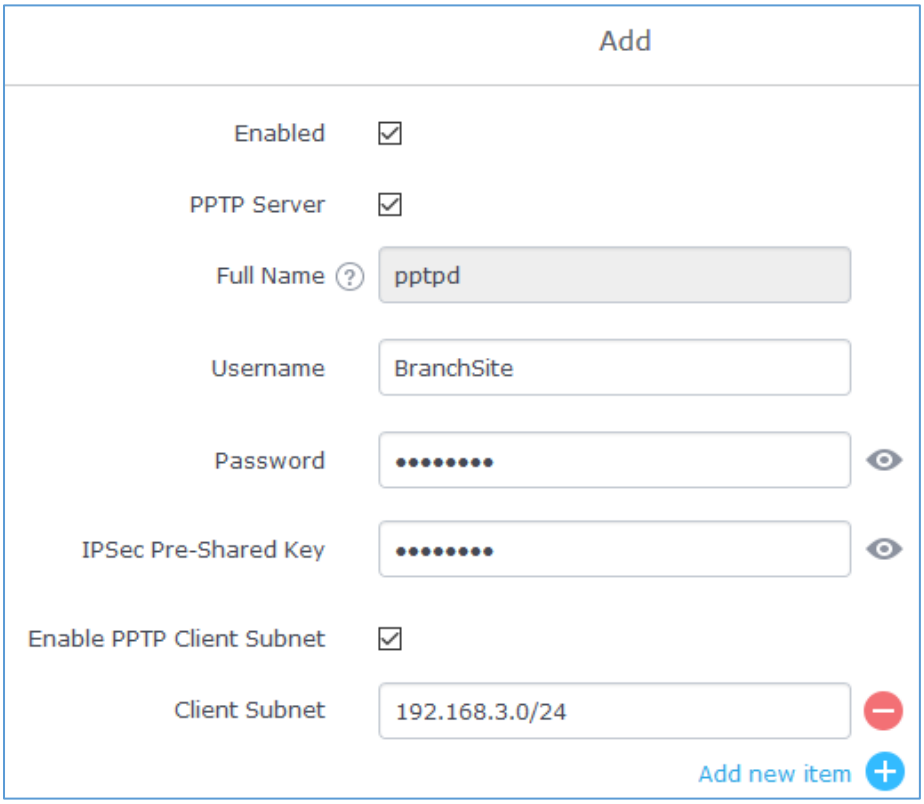

Figure 3: Create PPTP Users

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

Notes:

- Make sure to enable PPTP client Subnet option.
- Under **Client Subnet** field, administrator needs to enter the IP range of branch site LAN, and the GWN7000 server will build a route to that destination, thus allowing site-to-site communication.

Creating PPTP Server

After creating all users for each site that will be connecting to the core site via PPTP tunnel. Administrator needs now to create and enable the PPTP server instance on the GWN7000 located on the core site.

To create a new PPTP server, follow below steps:

1. Go under "**VPN→PPTP→Server**".
2. Click on 

and fill in the required information as shown on the figure below.

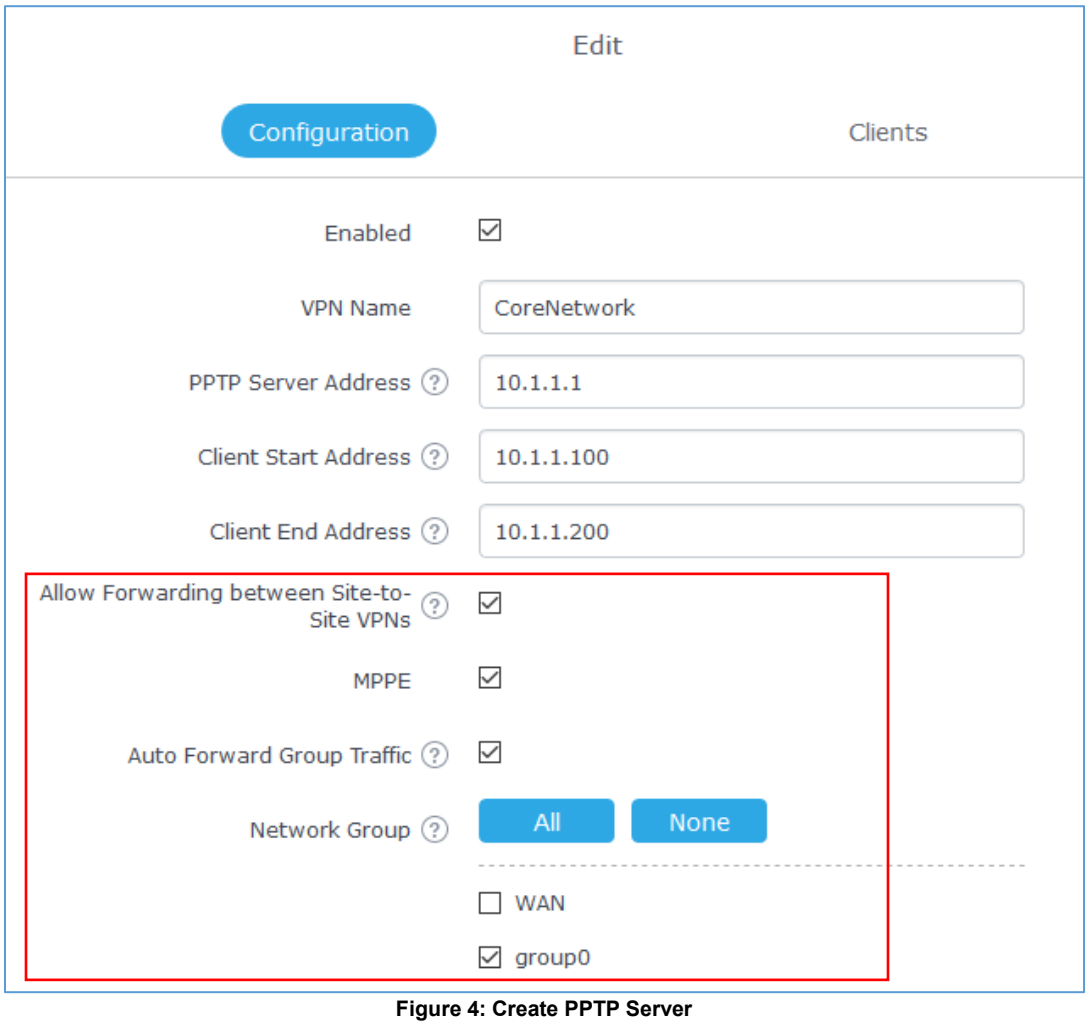

Figure 4: Create PPTP Server

The table below gives the description for each option/parameter.

Table 1: PPTP Server Parameters

Field	Description
Enable	Click on the checkbox to enable the PPTP VPN Server.
VPN Name	Enter a name for the PPTP Server.
PPTP Server Address	Configure the PPTP server local address (ex: 10.1.1.1). **Note:** This is not the public IP of the GWN, this is the IP address of the interface that will be used to build the PPTP tunnel between server and client.
Client Start Address	Configure the remote client IP start address. **Notes:** • This address should be in the same subnet as the end address and PPTP server address. • This is the address that will be used on client side when connecting to the server in order to build the PPTP Tunnel.
Client End Address	Configure the remote client IP end address. **Notes:** • This address should be in the same subnet as the start address and PPTP server address. • This is the address that will be used on client side when connecting to the server in order to build the PPTP Tunnel.
Allow Forwarding between Site-To-Site VPNs	This option allows forwarding between multiple site-to-site VPNs. i.e. if there are multiple PPTP users configured with client subnet enabled, then this option allows one PPTP client subnet to access another PPTP client subnet through the server. **Note:** for this option to work more than one PPTP users with client subnet must be enabled.
MPPE	Enable/disable Microsoft Point-to-Point Encryption.
Auto Forward group traffic	Configures if enable group traffic forwards to be automatic. If enabled, users should choose which groups they want to forward, if not, users can still do it manually via forwarding rules under firewall settings. **Note:** When disabling, the previous group settings will be cleared, administrator needs to re-configure the groups.
Network Group	Configure the network group to access VPN connection. You can choose more than one network group at the same time.

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

Notes:

- Users could enable MPPE encryption for more security under both the PPTP server and the client as we will see later on.
- Make sure to enable the option “Auto Forward Group Traffic” and in order to allow the traffic coming from the PPTP tunnel into the network group(s) at the core site location.

Server status can be checked after this under “**VPN→PPTP→Server**” as shown on the following figure.

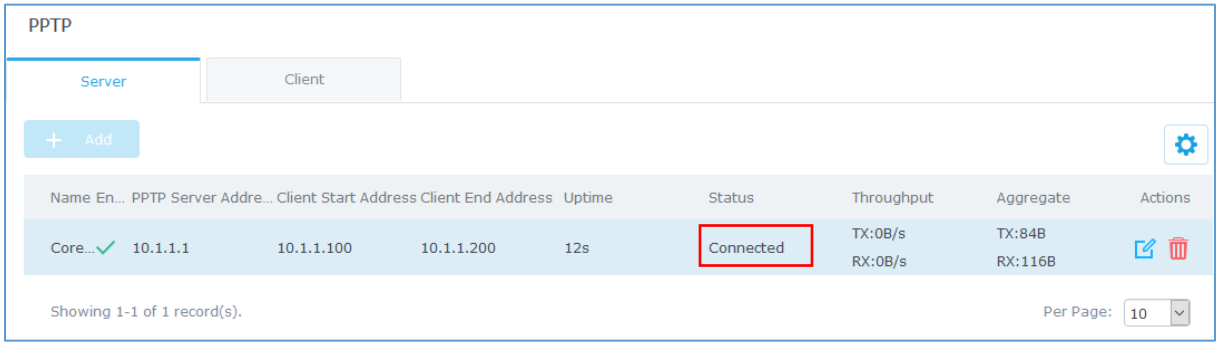

Figure 5: PPTP Server Status

Branch Site Configuration

Now that the GWN7000 router at the core site is UP and running, we move on to configure a PPTP client instance under the GWN7000 router on the branch site. Please follow below steps in order to set it up.

1. Go to “**VPN→PPTP→Client**” and follow steps below:
2. Click on 

and the following window will pop up.
3. Under **Remote PPTP Server** field, put the public IP of the core site router to which the client will initiate tunnel connection (example: 192.168.6.71).
4. Add the list of networks that are reachable through the GWN7000 running PPTP server. Here we set the IP range for the core site LAN **(i.e. 192.168.1.0/24).** This will allow the GWN7000 at the branch site to build a route to the core network to allow full site-to-site communication.

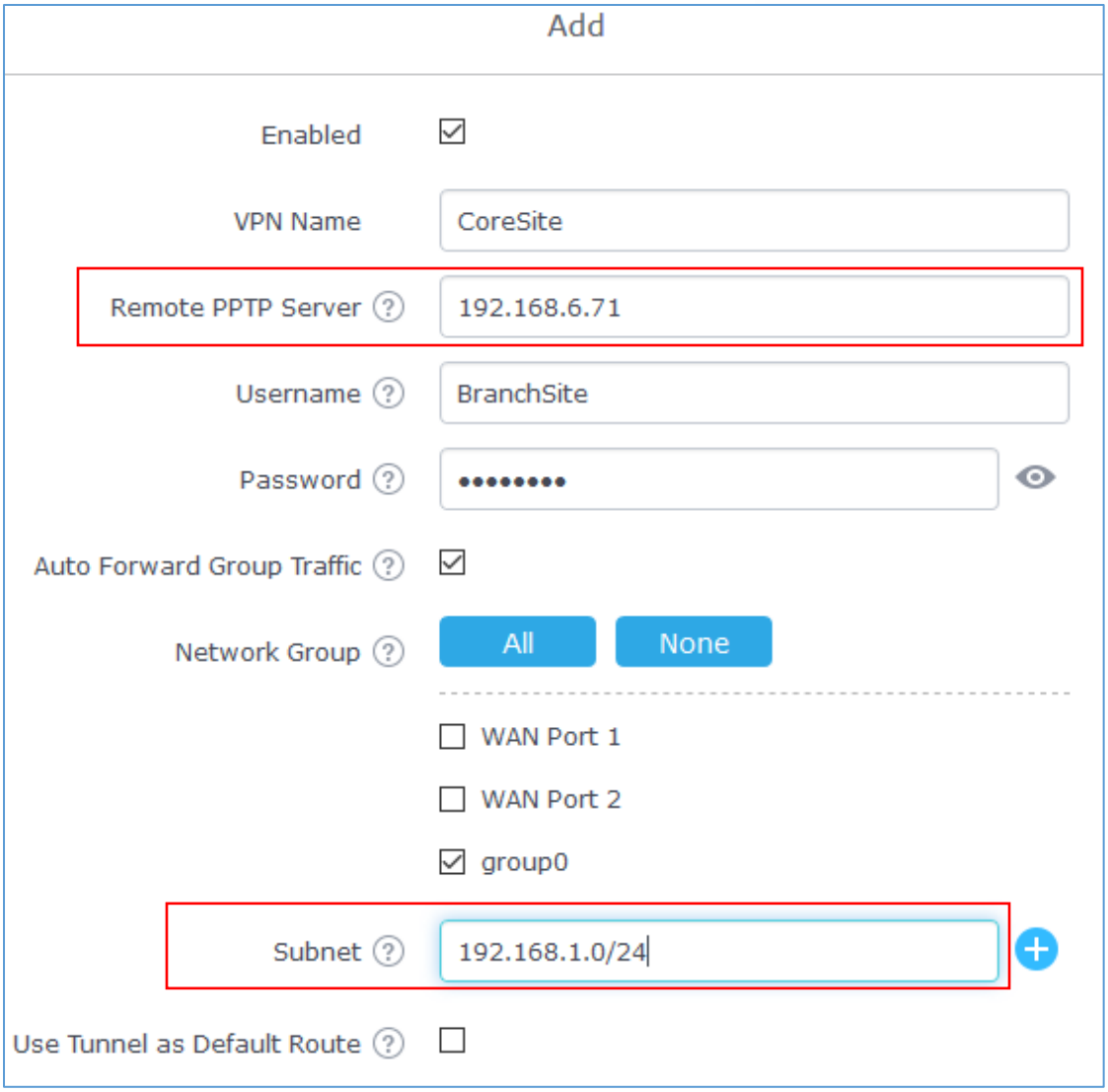

Figure 6: PPTP Client Configuration

5. The final step would be to enable MPPE encryption since it's used for both client and server for more security of the data.

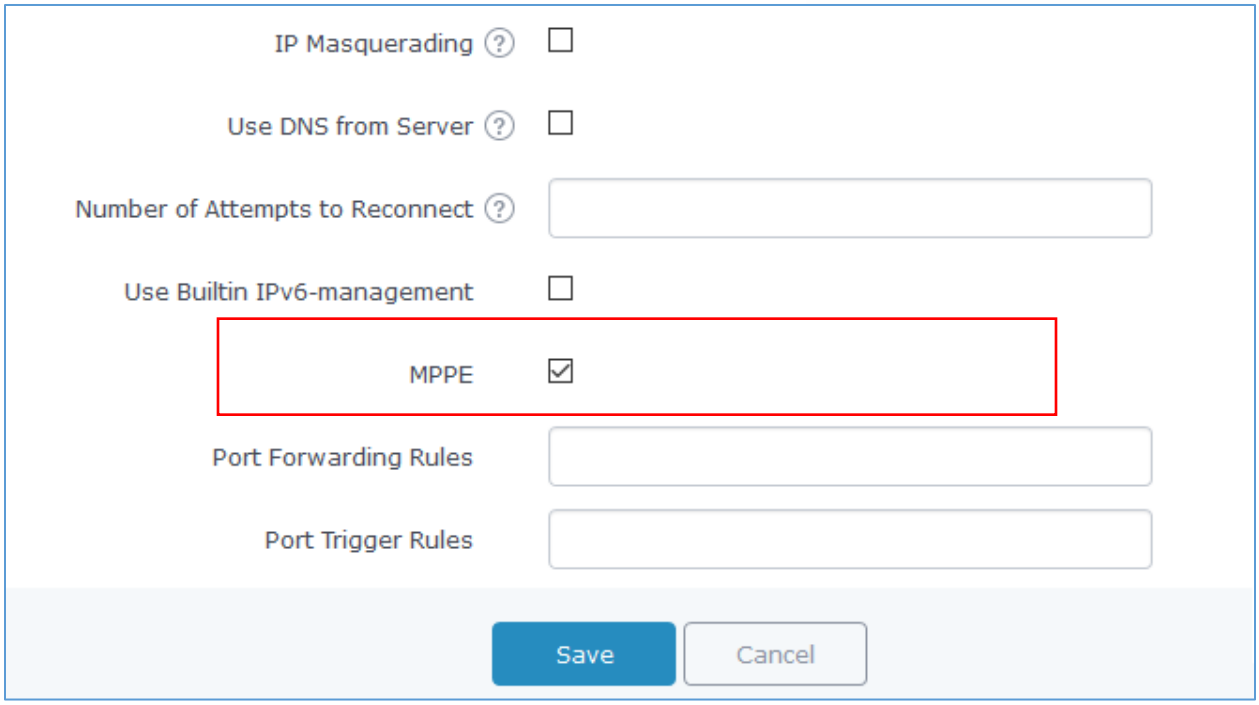

Figure 7: Enable MPPE

Once this done, press save and apply then check the PPTP client status to verify its connection status.

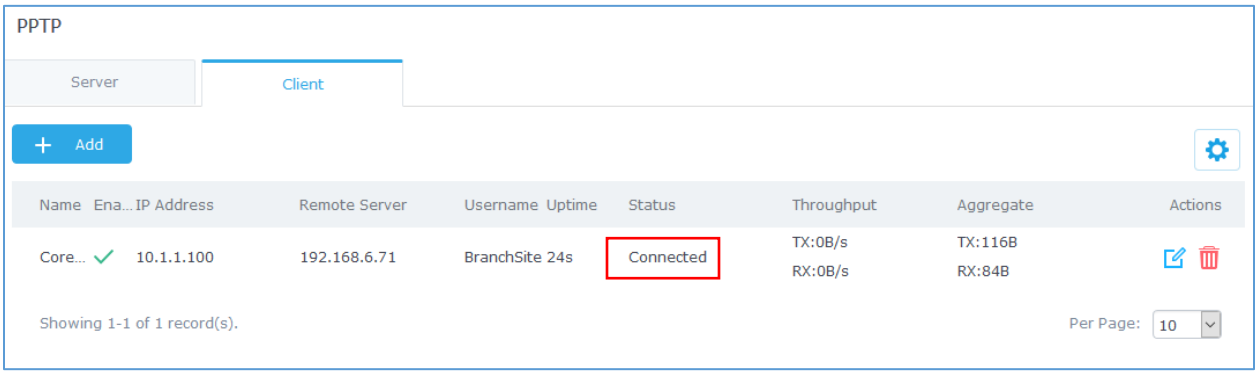

Figure 8: PPTP Client Status

We can see as well that the PPTP client did take the IP 10.1.1.100 from the pool configured under the PPTP server.

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 though PPTP tunnel.

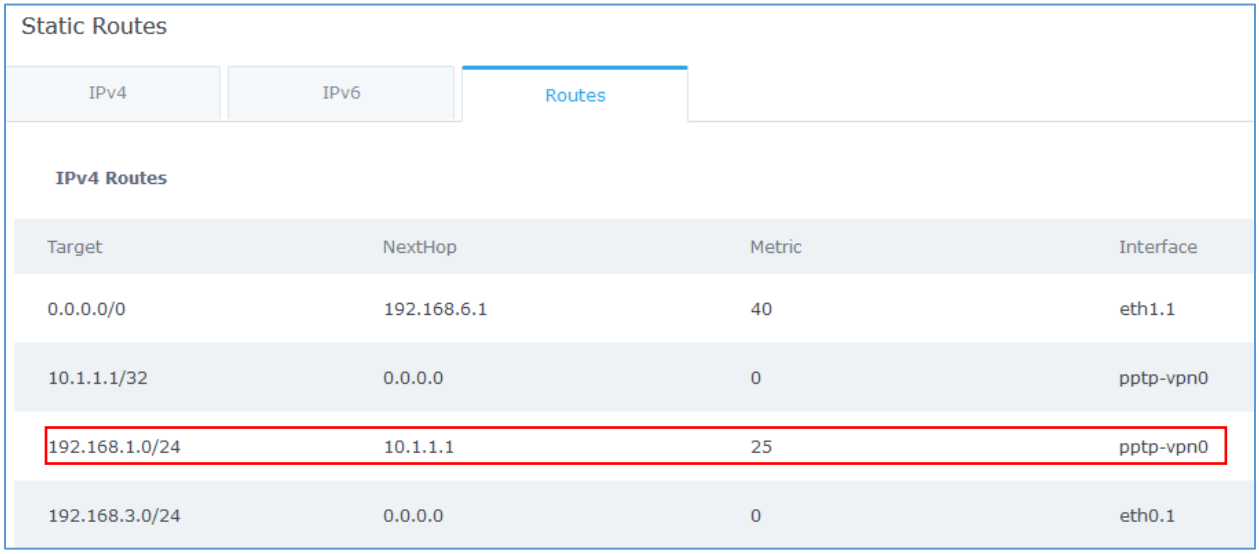

Figure 9: Verification - PPTP Tunnel

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.

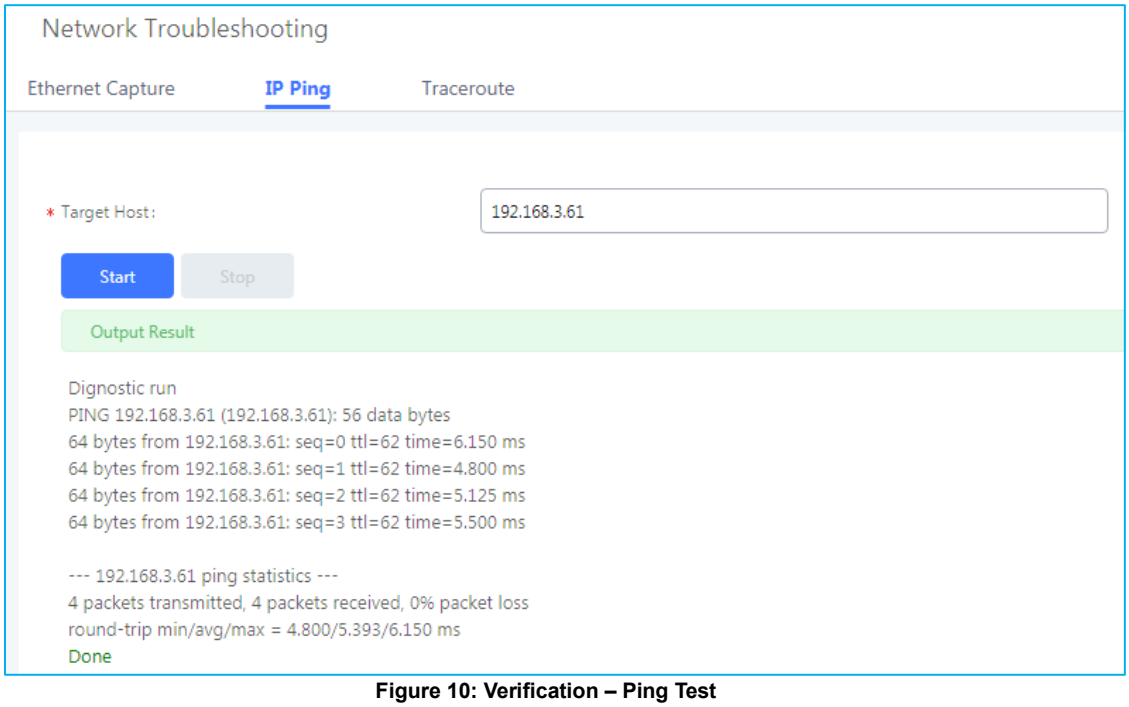

Figure 10: Verification – Ping Test

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.

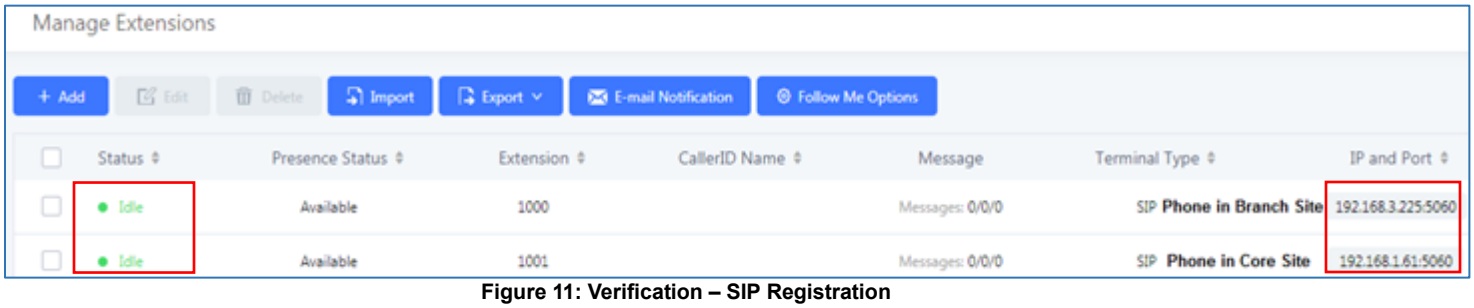

Figure 11: Verification – SIP Registration