NR500 Series
Industrial Cellular VPN Router

Application Note 050

OpenVPN Server with x.509 certificate

Version: V1.0.0
Date: Mar 2020
Status: Confidential

Directory

1. Introduction

1.1 Overview

This document contains information regarding the configuration and use of OpenVPN Server with x.509 certification.

This guide has been written for use by technically competent personnel with a good understanding of the communications technologies used in the product, and of the requirements for their specific application.

1.2 Compatibility

This application note applies to:
Models Shown: NR500 series.
Firmware Version: V1.2.0(68c082c) or newer
Other Compatible Models: None

1.3 Version

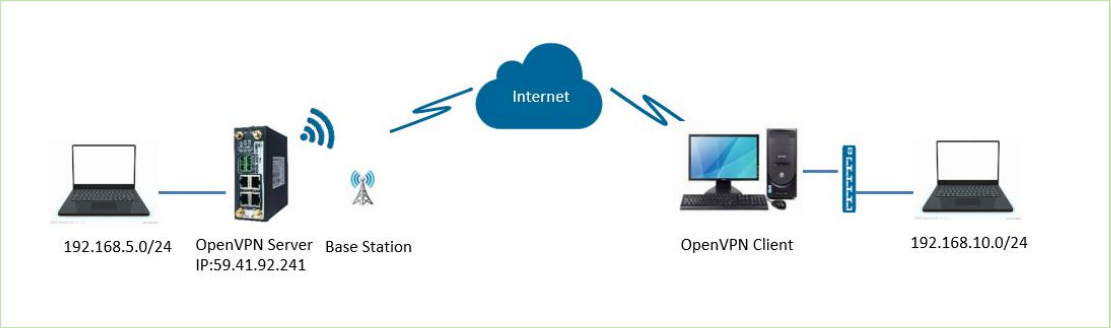
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2020/03/05	V1.0.0	V1.2.0(68c082c)	First released

1.4 Corrections

Appreciate for corrections or rectifications to this application note, and if any request for new application notes please email to: **support@navigateworx.com**

2. Topology

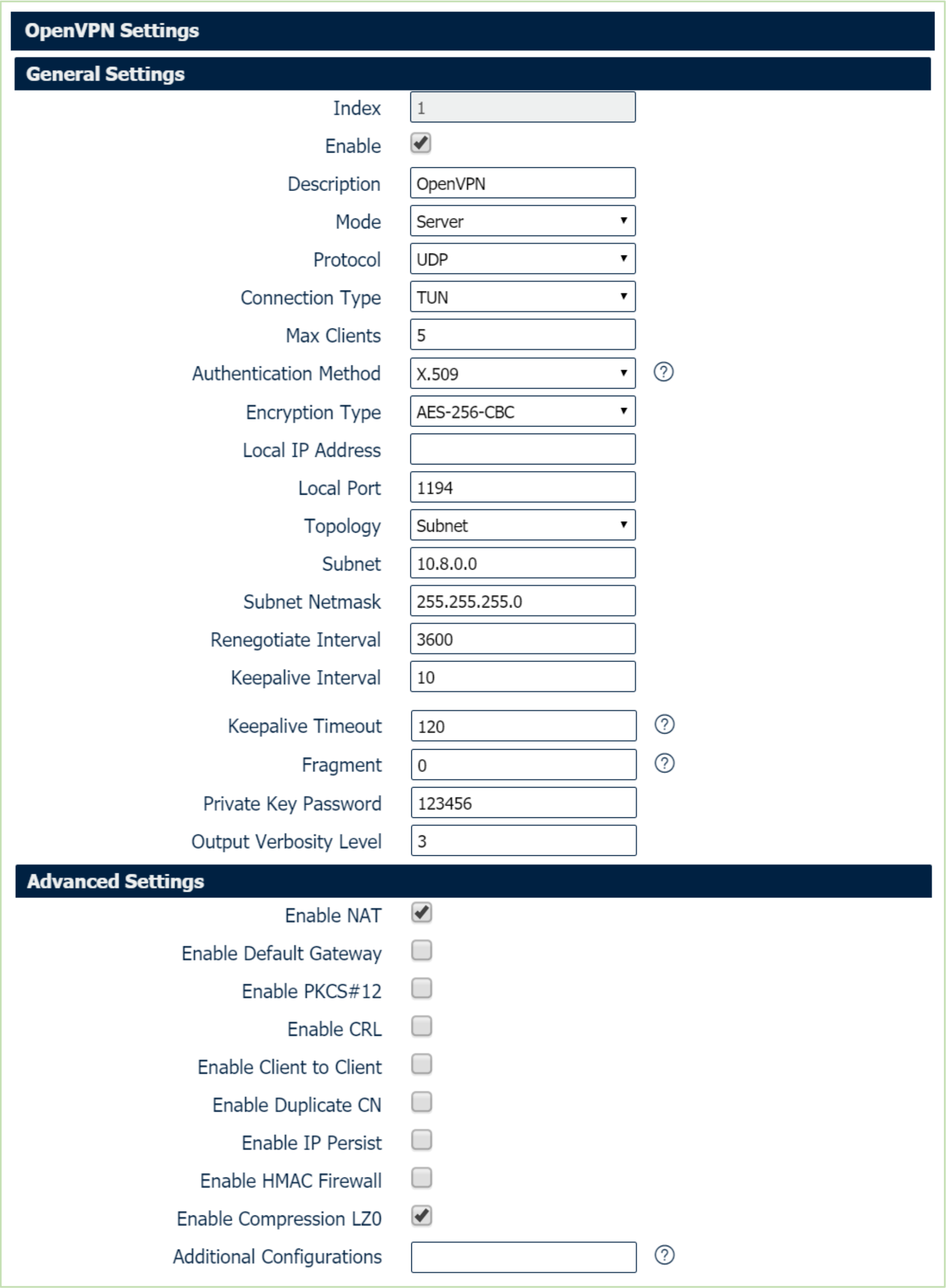


1. NR500 Router runs as OpenVPN Server with Public IP address or Domain Name, which can be ping by OpenVPN Client successfully.
2. A PC runs as OpenVPN Client with any kinds of the IP, just able to connect to internet.
3. OpenVPN tunnel is established between Server and Client, the subnet can PING each other successfully

3. Configuration

3.1 Server Configuration

1. Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as below picture. Click Save.



OpenVPN Settings

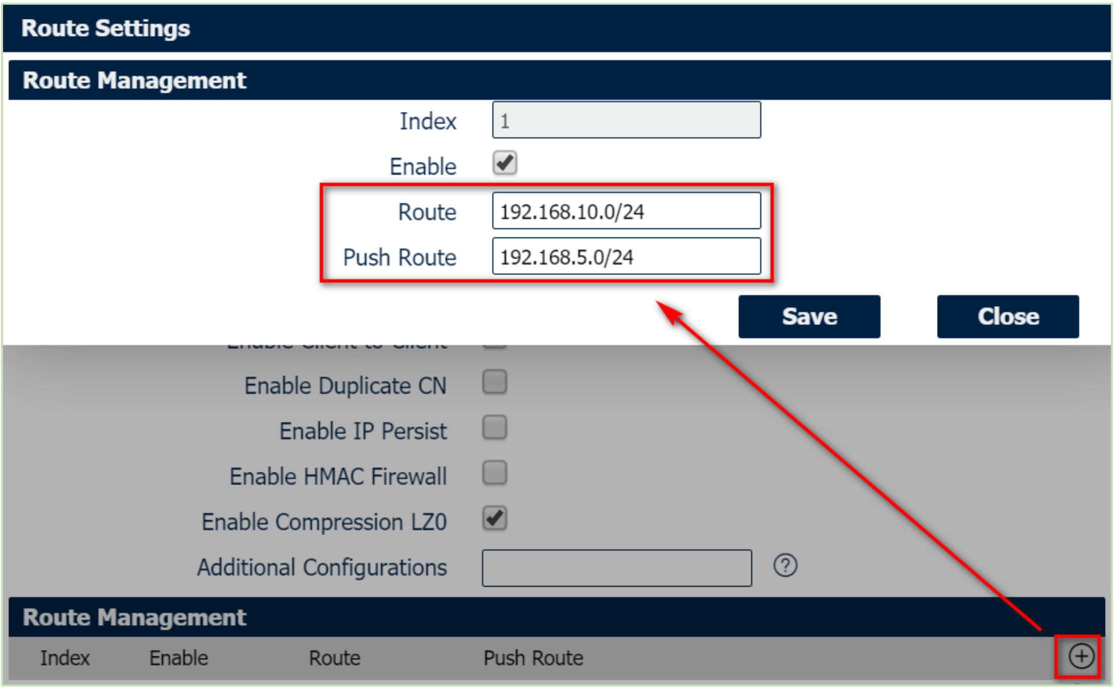
General Settings

Index	1
Enable	☑
Description	OpenVPN
Mode	Server
Protocol	UDP
Connection Type	TUN
Max Clients	5
Authentication Method	X.509
Encryption Type	AES-256-CBC
Local IP Address	
Local Port	1194
Topology	Subnet
Subnet	10.8.0.0
Subnet Netmask	255.255.255.0
Renegotiate Interval	3600
Keepalive Interval	10
Keepalive Timeout	120
Fragment	0
Private Key Password	123456
Output Verbosity Level	3

Advanced Settings

Enable NAT	☑
Enable Default Gateway	□
Enable PKCS#12	□
Enable CRL	□
Enable Client to Client	□
Enable Duplicate CN	□
Enable IP Persist	□
Enable HMAC Firewall	□
Enable Compression LZ0	☑
Additional Configurations	

2. Setting on Router Management like below, click “Save”.



Route Settings

Route Management

Index: 1

Enable: ☑

Route: 192.168.10.0/24

Push Route: 192.168.5.0/24

Enable Duplicate CN: □

Enable IP Persist: □

Enable HMAC Firewall: □

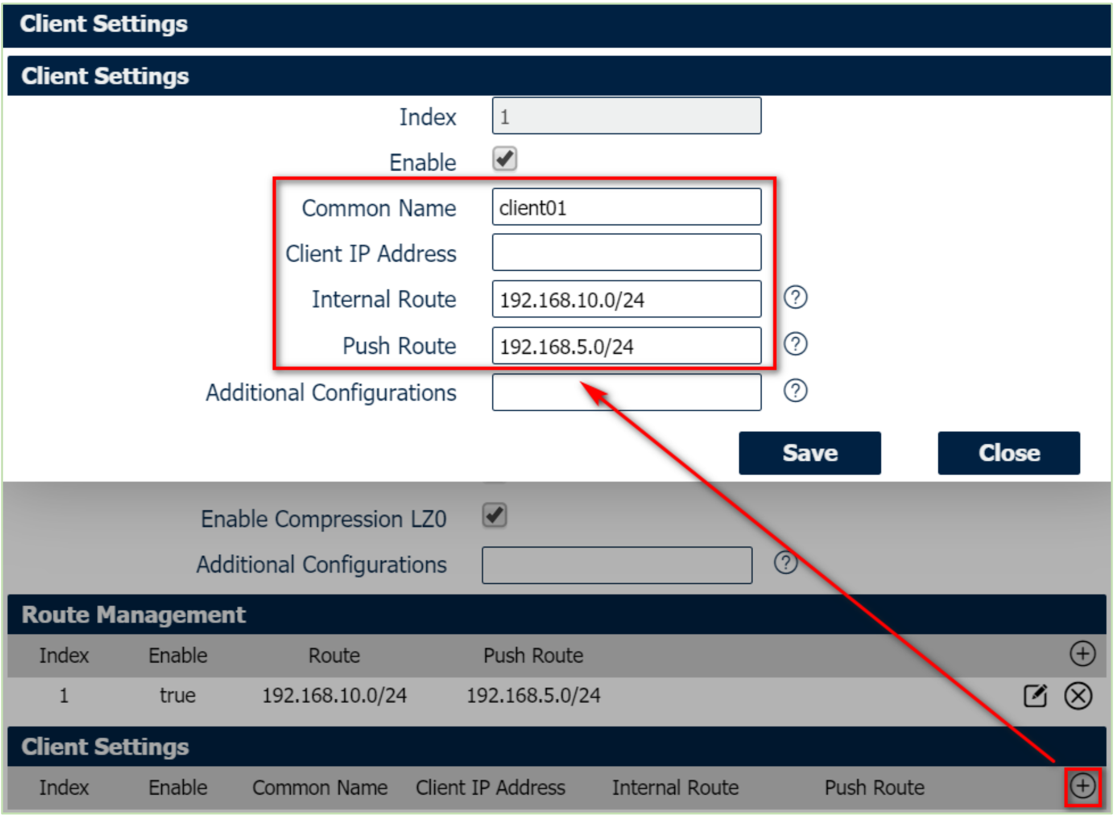
Enable Compression LZ0: ☑

Additional Configurations:

Route Management

Index	Enable	Route	Push Route

3. Setting on Client Settings like below, click “Save”:



Client Settings

Client Settings

Index: 1

Enable: ☑

Common Name: client01

Client IP Address:

Internal Route: 192.168.10.0/24

Push Route: 192.168.5.0/24

Additional Configurations:

Enable Compression LZ0: ☑

Additional Configurations:

Route Management

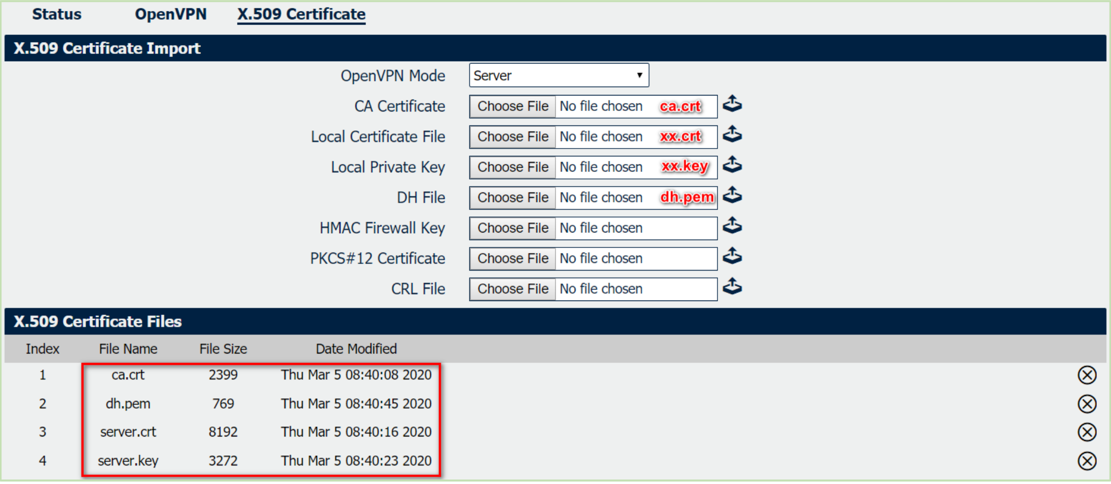
Index	Enable	Route	Push Route
1	true	192.168.10.0/24	192.168.5.0/24

Client Settings

Index	Enable	Common Name	Client IP Address	Internal Route	Push Route

4. After that, click Save>Apply.

5. Go to VPN>OpenVPN>X.509 Certificate, import the related certificates:



X.509 Certificate Import

OpenVPN Mode	Server
CA Certificate	Choose File No file chosen ca.crt
Local Certificate File	Choose File No file chosen xx.crt
Local Private Key	Choose File No file chosen xx.key
DH File	Choose File No file chosen dh.pem
HMAC Firewall Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen
CRL File	Choose File No file chosen

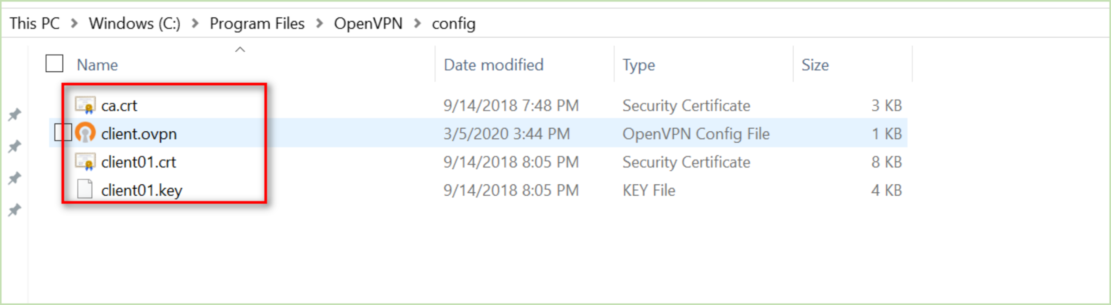
X.509 Certificate Files

Index	File Name	File Size	Date Modified	
1	ca.crt	2399	Thu Mar 5 08:40:08 2020	⊗
2	dh.pem	769	Thu Mar 5 08:40:45 2020	⊗
3	server.crt	8192	Thu Mar 5 08:40:16 2020	⊗
4	server.key	3272	Thu Mar 5 08:40:23 2020	⊗

6. Click Apply.

3.2 Client Configuration

1. Install OpenVPN software on PC and copy the related certifications and configuration to the PC like below:



This PC > Windows (C:) > Program Files > OpenVPN > config

Name	Date modified	Type	Size
ca.crt	9/14/2018 7:48 PM	Security Certificate	3 KB
client.ovpn	3/5/2020 3:44 PM	OpenVPN Config File	1 KB
client01.crt	9/14/2018 8:05 PM	Security Certificate	8 KB
client01.key	9/14/2018 8:05 PM	KEY File	4 KB

***Note**: a) Kindly download OpenVPN software with: https://openvpn.net/*
*b) Kindly install and run OpenVPN software with **administrator authority**.*

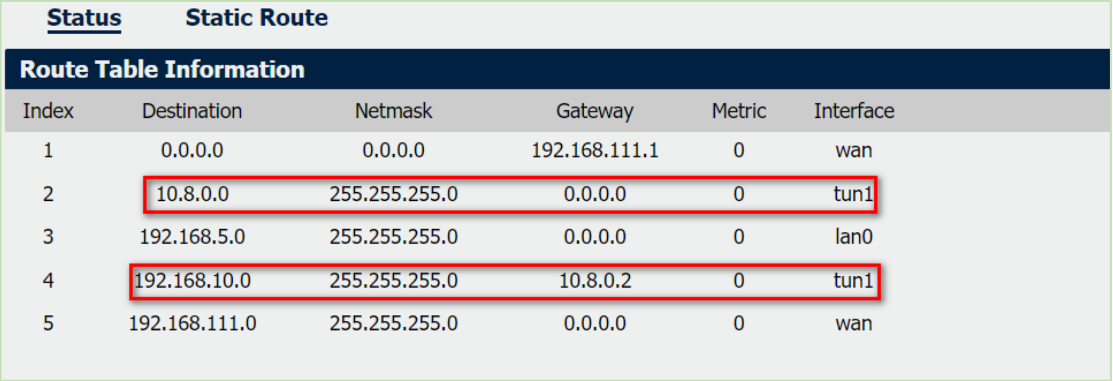
2. The configuration of **client.ovpn** like below:

```
=================================================================
client
remote 59.41.92.241 1194
dev tun
proto udp
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client01.crt
key client01.key
remote-cert-tls server
```

cipher AES-256-CBC
keepalive 10 120
comp-lzo
verb 3
===

6. Route Table

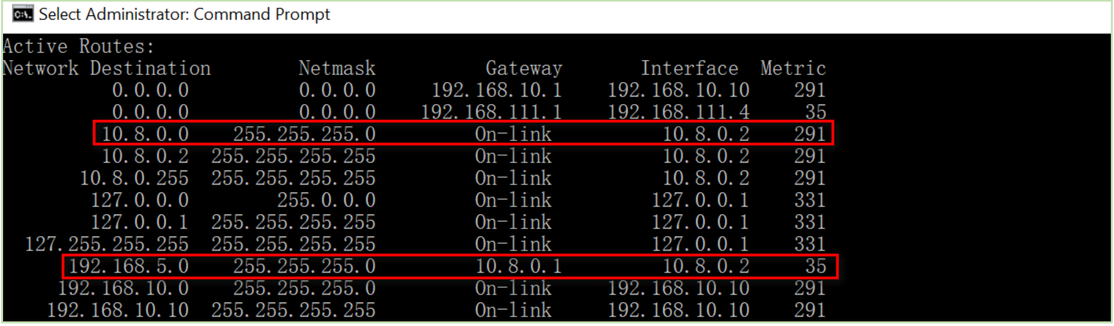
1. Route Table on OpenVPN Server for reference.



Route Table Information

Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	0	wan
2	10.8.0.0	255.255.255.0	0.0.0.0	0	tun1
3	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
4	192.168.10.0	255.255.255.0	10.8.0.2	0	tun1
5	192.168.111.0	255.255.255.0	0.0.0.0	0	wan

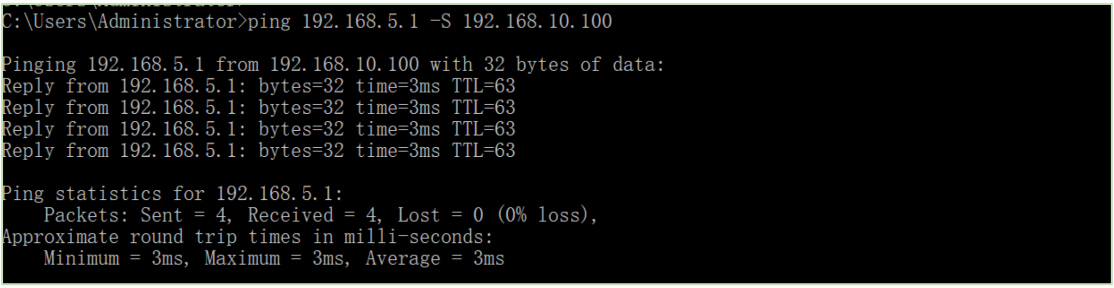
2. Route Table on OpenVPN Client for reference.



```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0     192.168.10.1   192.168.10.10    291
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.4     35
         10.8.0.0    255.255.255.0         On-link         10.8.0.2    291
         10.8.0.2  255.255.255.255         On-link         10.8.0.2    291
       10.8.0.255  255.255.255.255         On-link         10.8.0.2    291
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
        127.0.0.1  255.255.255.255         On-link        127.0.0.1    331
  127.255.255.255  255.255.255.255         On-link        127.0.0.1    331
      192.168.5.0    255.255.255.0         10.8.0.1        10.8.0.2     35
     192.168.10.0    255.255.255.0         On-link    192.168.10.10    291
    192.168.10.10  255.255.255.255         On-link    192.168.10.10    291
```

7. Testing

1. Enable CMD and Ping from OpenVPN Client to LAN of OpenVPN Server.

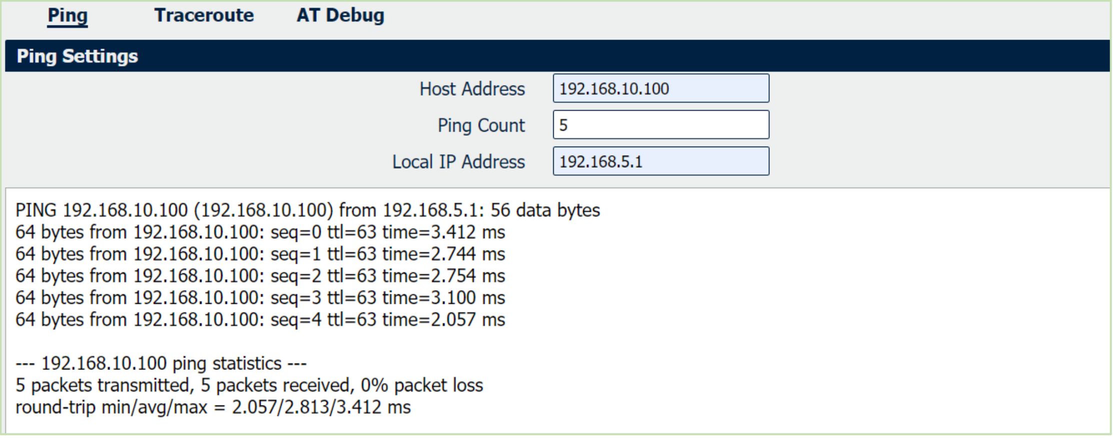


```
C:\Users\Administrator>ping 192.168.5.1 -S 192.168.10.100

Pinging 192.168.5.1 from 192.168.10.100 with 32 bytes of data:
Reply from 192.168.5.1: bytes=32 time=3ms TTL=63
Reply from 192.168.5.1: bytes=32 time=3ms TTL=63
Reply from 192.168.5.1: bytes=32 time=3ms TTL=63
Reply from 192.168.5.1: bytes=32 time=3ms TTL=63

Ping statistics for 192.168.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 3ms, Average = 3ms
```

2. Go to **Maintenance>Debug Tool>Ping** and Ping from OpenVPN Server to OpenVPN Client LAN Device.



Host Address	192.168.10.100
Ping Count	5
Local IP Address	192.168.5.1

```
PING 192.168.10.100 (192.168.10.100) from 192.168.5.1: 56 data bytes
64 bytes from 192.168.10.100: seq=0 ttl=63 time=3.412 ms
64 bytes from 192.168.10.100: seq=1 ttl=63 time=2.744 ms
64 bytes from 192.168.10.100: seq=2 ttl=63 time=2.754 ms
64 bytes from 192.168.10.100: seq=3 ttl=63 time=3.100 ms
64 bytes from 192.168.10.100: seq=4 ttl=63 time=2.057 ms

--- 192.168.10.100 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.057/2.813/3.412 ms
```

3. Test successfully.