NR500 Series
Industrial Cellular VPN Router

Application Note 058

OpenVPN with Password Between NR500

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

Directory

1. Introduction

1.1 Overview

This document contains information regarding the configuration and use of OpenVPN with password between NR500s.

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: V1.1.4(0c0c9fa) or newer
Other Compatible Models: None

1.3 Version

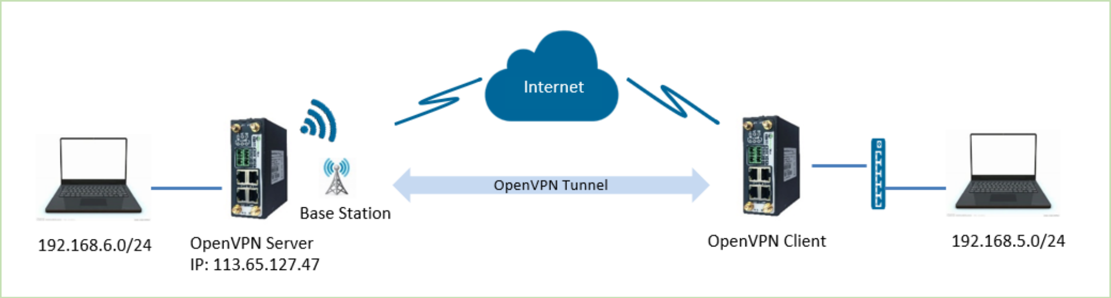
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2020/12/14	V1.0.0	V1.1.4(0c0c9fa)	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

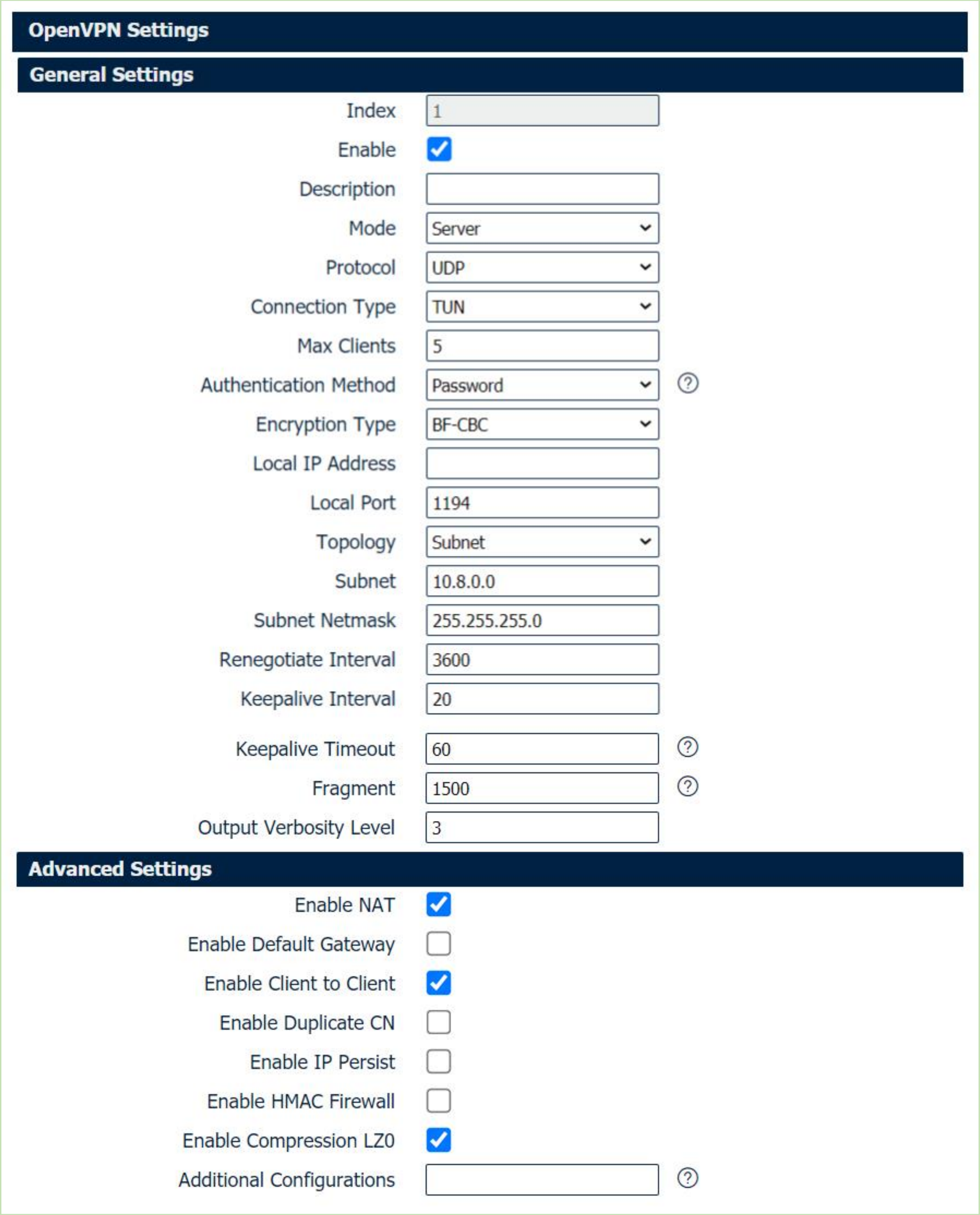


1. NR500 Router runs as OpenVPN Server with Public IP address or Domain Name, which can be accessed by another NR500 as OpenVPN Client successfully.
2. Two PCs connected to the LAN of OpenVPN Server and OpenVPN Client as the subnet.
3. OpenVPN tunnel is established between Server and Client, the subnet 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

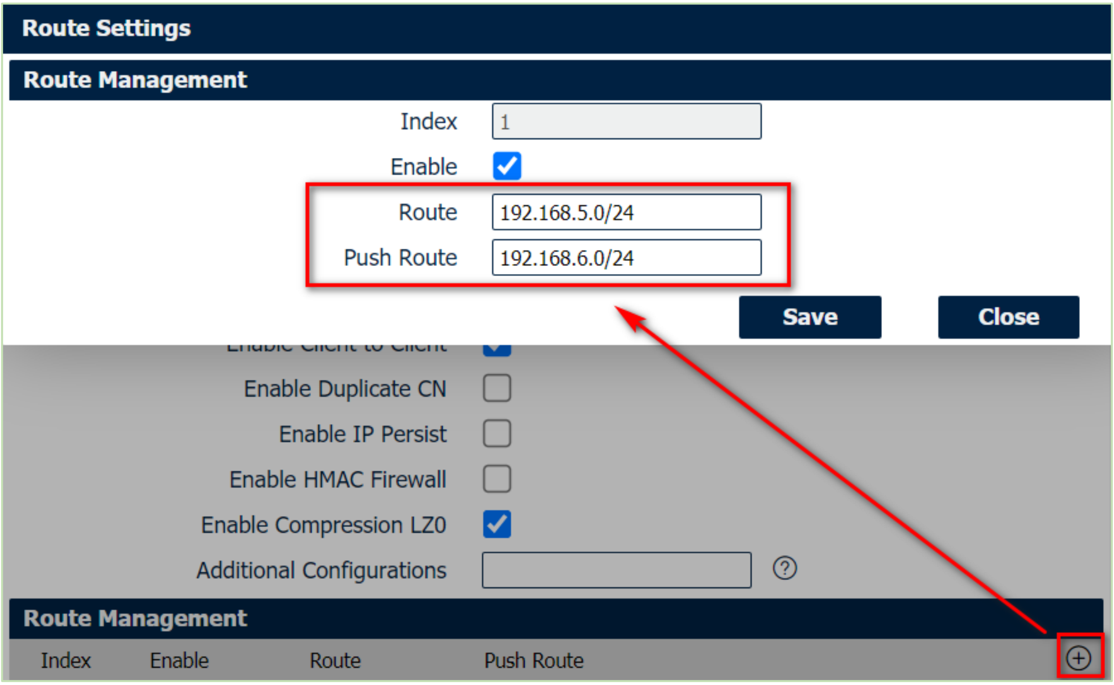
General Settings

Index	1
Enable	☑
Description	
Mode	Server
Protocol	UDP
Connection Type	TUN
Max Clients	5
Authentication Method	Password
Encryption Type	BF-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	20
Keepalive Timeout	60
Fragment	1500
Output Verbosity Level	3

Advanced Settings

Enable NAT	☑
Enable Default Gateway	☐
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: 192.168.5.0/24

Push Route: 192.168.6.0/24

Enable Client to Client: ☑

Enable Duplicate CN: □

Enable IP Persist: □

Enable HMAC Firewall: □

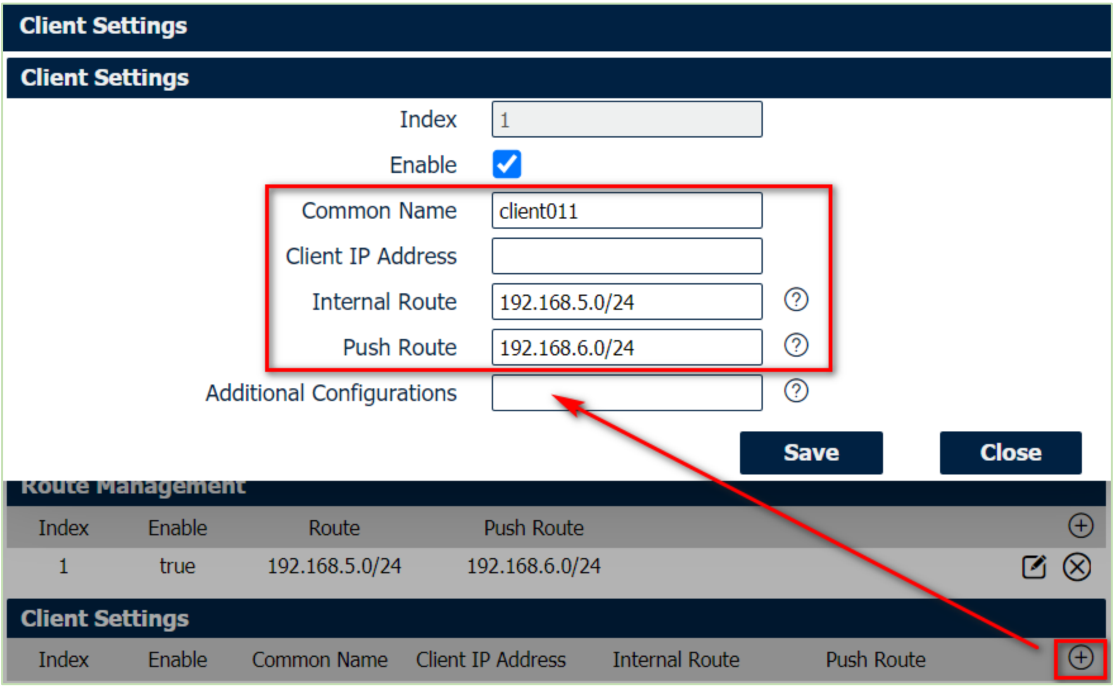
Enable Compression LZ0: ☑

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: client011

Client IP Address:

Internal Route: 192.168.5.0/24

Push Route: 192.168.6.0/24

Additional Configurations:

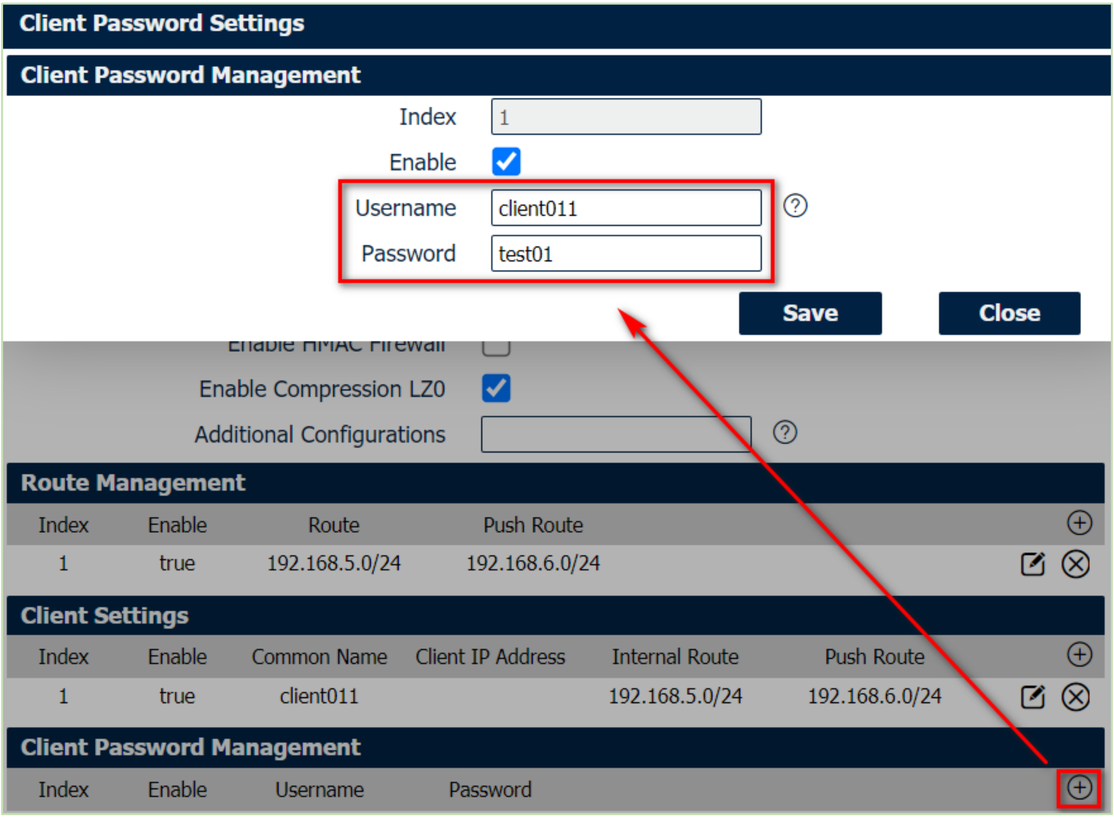
Route Management

Index	Enable	Route	Push Route
1	true	192.168.5.0/24	192.168.6.0/24

Client Settings

Index	Enable	Common Name	Client IP Address	Internal Route	Push Route

4. Setting on Client Password Management like below, click “Save”:



Client Password Settings

Client Password Management

Index	1
Enable	☑
Username	client011
Password	test01

Enable HMAC Firewall	□
Enable Compression LZ0	☑
Additional Configurations	

Route Management

Index	Enable	Route	Push Route
1	true	192.168.5.0/24	192.168.6.0/24

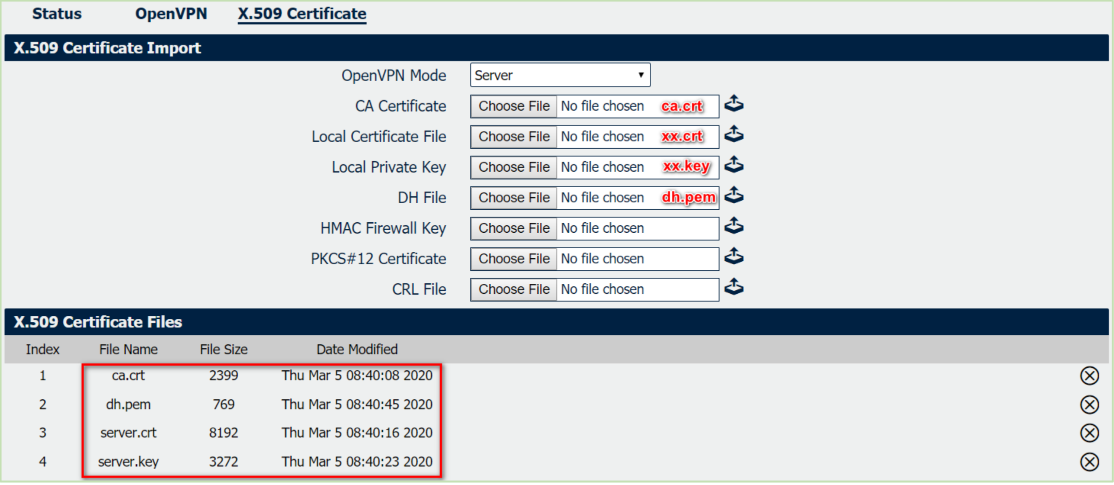
Client Settings

Index	Enable	Common Name	Client IP Address	Internal Route	Push Route
1	true	client011		192.168.5.0/24	192.168.6.0/24

Client Password Management

Index	Enable	Username	Password

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

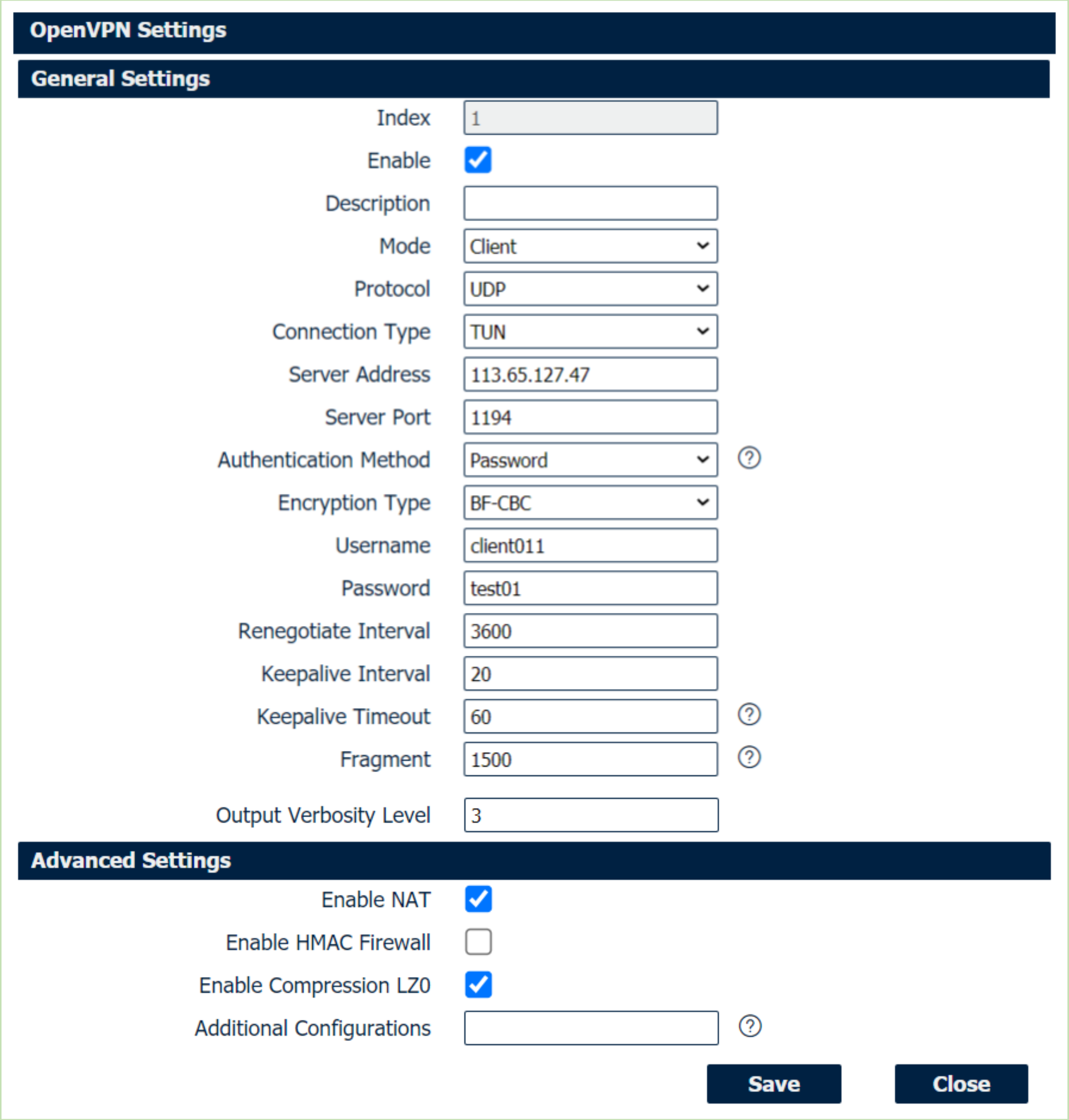
X.509 Certificate Files

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



OpenVPN Settings

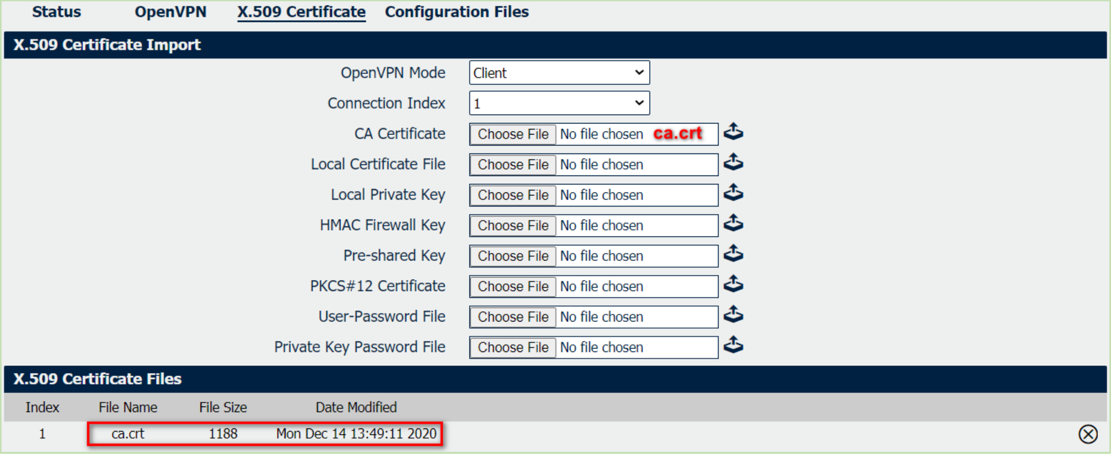
General Settings

Index	1
Enable	☑
Description	
Mode	Client
Protocol	UDP
Connection Type	TUN
Server Address	113.65.127.47
Server Port	1194
Authentication Method	Password
Encryption Type	BF-CBC
Username	client011
Password	test01
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Output Verbosity Level	3

Advanced Settings

Enable NAT	☑
Enable HMAC Firewall	□
Enable Compression LZ0	☑
Additional Configurations	

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



Status OpenVPN X.509 Certificate Configuration Files

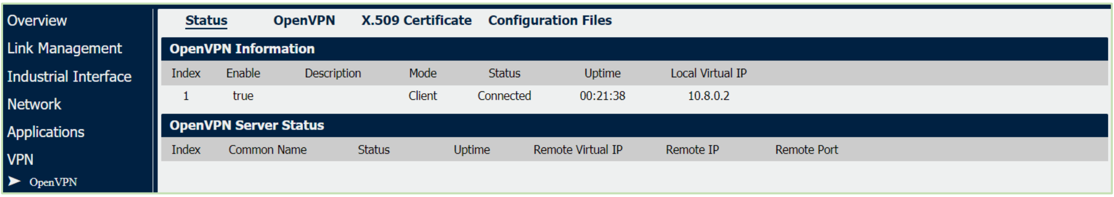
X.509 Certificate Import

OpenVPN Mode	Client
Connection Index	1
CA Certificate	Choose File No file chosen ca.crt
Local Certificate File	Choose File No file chosen
Local Private Key	Choose File No file chosen
HMAC Firewall Key	Choose File No file chosen
Pre-shared Key	Choose File No file chosen
PKCS#12 Certificate	Choose File No file chosen
User-Password File	Choose File No file chosen
Private Key Password File	Choose File No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Mon Dec 14 13:49:11 2020

3. Click Apply. The Client had connected Server successfully:



Overview
Link Management
Industrial Interface
Network
Applications
VPN
➤ OpenVPN

Status OpenVPN X.509 Certificate Configuration Files

OpenVPN Information

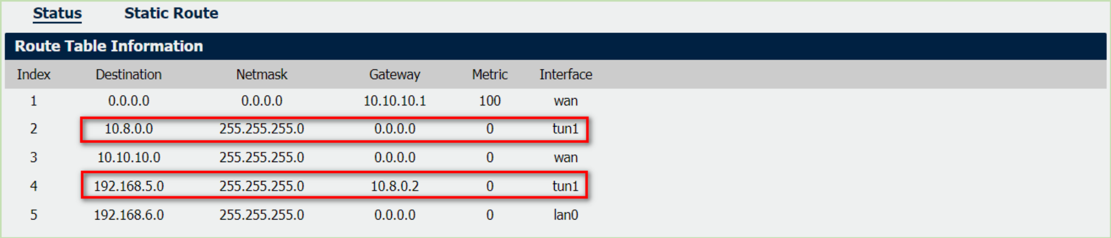
Index	Enable	Description	Mode	Status	Uptime	Local Virtual IP
1	true		Client	Connected	00:21:38	10.8.0.2

OpenVPN Server Status

Index	Common Name	Status	Uptime	Remote Virtual IP	Remote IP	Remote Port

4. Route Table

1. Route Table on OpenVPN Server for reference.

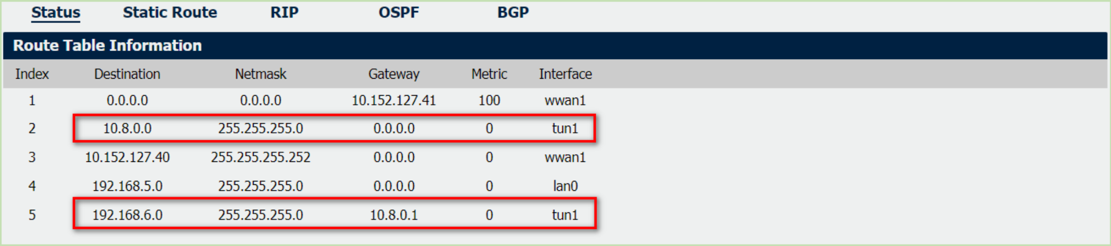


Status Static Route

Route Table Information

Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	10.10.10.1	100	wan
2	10.8.0.0	255.255.255.0	0.0.0.0	0	tun1
3	10.10.10.0	255.255.255.0	0.0.0.0	0	wan
4	192.168.5.0	255.255.255.0	10.8.0.2	0	tun1
5	192.168.6.0	255.255.255.0	0.0.0.0	0	lan0

2. Route Table on OpenVPN Client for reference.



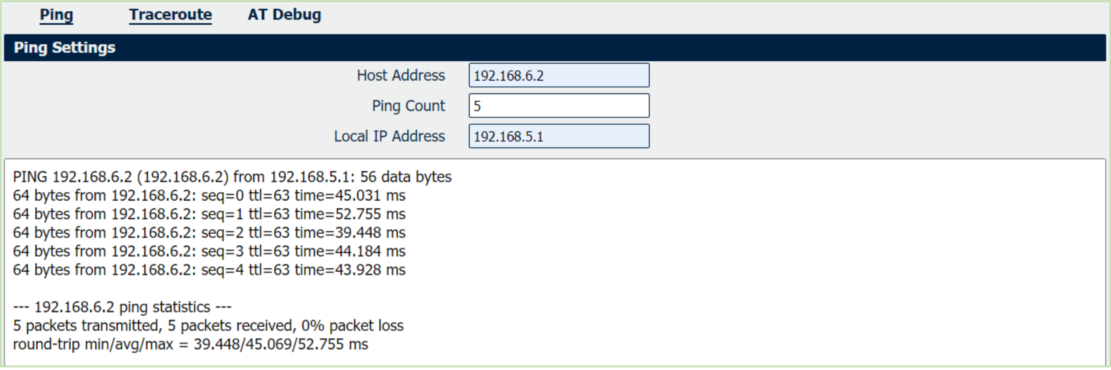
Status Static Route RIP OSPF BGP

Route Table Information

Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	10.152.127.41	100	wwan1
2	10.8.0.0	255.255.255.0	0.0.0.0	0	tun1
3	10.152.127.40	255.255.255.252	0.0.0.0	0	wwan1
4	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
5	192.168.6.0	255.255.255.0	10.8.0.1	0	tun1

5. Testing

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

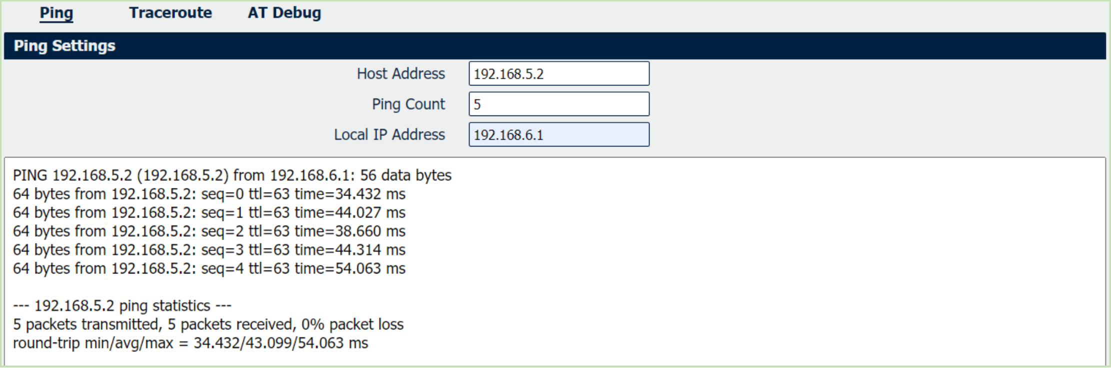


Host Address 192.168.6.2
Ping Count 5
Local IP Address 192.168.5.1

```
PING 192.168.6.2 (192.168.6.2) from 192.168.5.1: 56 data bytes
64 bytes from 192.168.6.2: seq=0 ttl=63 time=45.031 ms
64 bytes from 192.168.6.2: seq=1 ttl=63 time=52.755 ms
64 bytes from 192.168.6.2: seq=2 ttl=63 time=39.448 ms
64 bytes from 192.168.6.2: seq=3 ttl=63 time=44.184 ms
64 bytes from 192.168.6.2: seq=4 ttl=63 time=43.928 ms

--- 192.168.6.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 39.448/45.069/52.755 ms
```

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



Host Address 192.168.5.2
Ping Count 5
Local IP Address 192.168.6.1

```
PING 192.168.5.2 (192.168.5.2) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.5.2: seq=0 ttl=63 time=34.432 ms
64 bytes from 192.168.5.2: seq=1 ttl=63 time=44.027 ms
64 bytes from 192.168.5.2: seq=2 ttl=63 time=38.660 ms
64 bytes from 192.168.5.2: seq=3 ttl=63 time=44.314 ms
64 bytes from 192.168.5.2: seq=4 ttl=63 time=54.063 ms

--- 192.168.5.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 34.432/43.099/54.063 ms
```

3. Test successfully.