NR500 Series
Industrial Cellular VPN Router

Application Note 007

OpenVPN Client with Pre-shared Key

Version:	V1.0.0
Date:	Aug 2018
Status:	Confidential

Directory

1. Introduction

1.1 Overview

This document contains information regarding the configuration and use of OpenVPN client with Pre-shared key.

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: V1.0.0(903.0) or newer
Other Compatible Models: None

1.3 Version

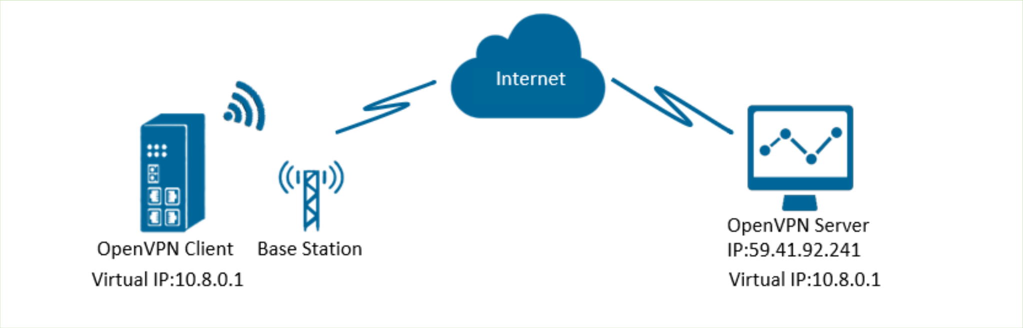
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2018/08/03	V1.0.0	V1.0.0(903.0)	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

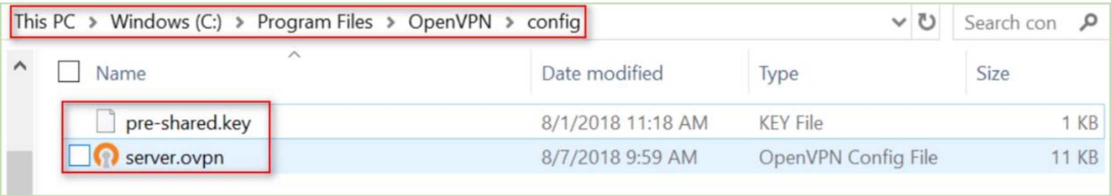


1. NR500 Pro runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the virtual IP can PING each other successfully. This is a point to point application.

3. Configuration

3.1 Server 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
pre-shared.key	8/1/2018 11:18 AM	KEY File	1 KB
server.ovpn	8/7/2018 9:59 AM	OpenVPN Config File	11 KB

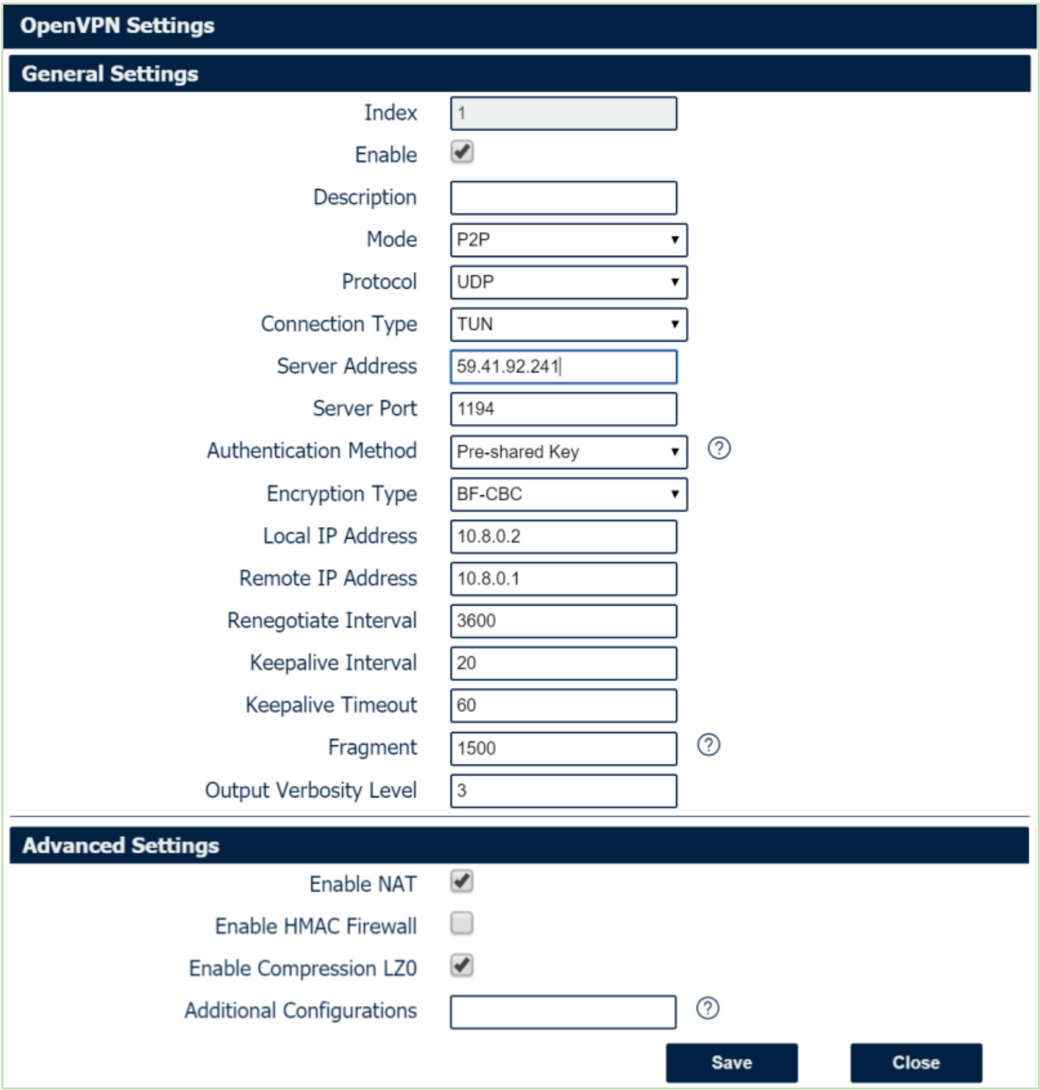
Note: Kindly install and run OpenVPN software with ***administrator authority****.*

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

```
======================================================================
local 59.41.92.241
proto udp
dev tun
tun-mtu 1500
fragment 1500
ifconfig 10.8.0.1 10.8.0.2
keepalive 10 120
secret pre-shared.key
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
======================================================================
```

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

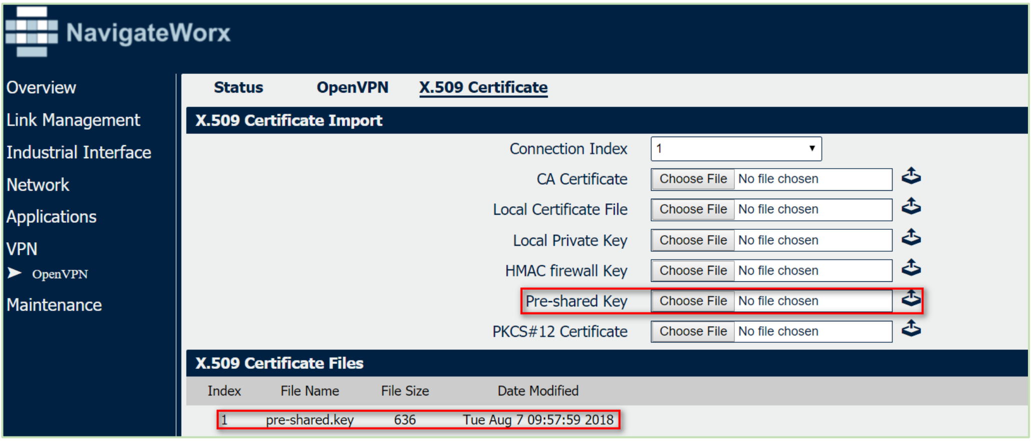
Index	1
Enable	☑
Description	
Mode	P2P
Protocol	UDP
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Pre-shared Key
Encryption Type	BF-CBC
Local IP Address	10.8.0.2
Remote IP Address	10.8.0.1
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Output Verbosity Level	3

Advanced Settings

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

2. Click Save>Apply.

3. Go to **VPN>OpenVPN>X.509 Certificate**, to import the related certification, Click Apply.



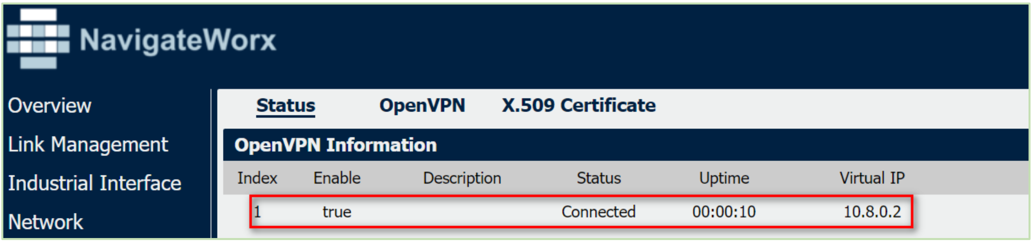
X.509 Certificate Import

Connection Index	1
CA Certificate	Choose File No file chosen
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

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	pre-shared.key	636	Tue Aug 7 09:57:59 2018

4.Route had connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.

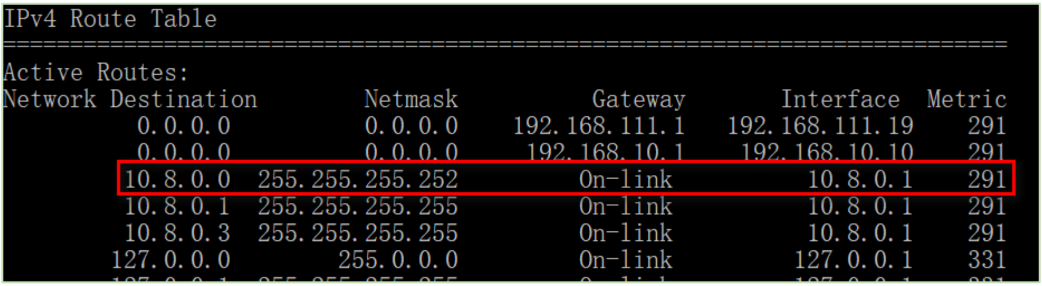


OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true		Connected	00:00:10	10.8.0.2

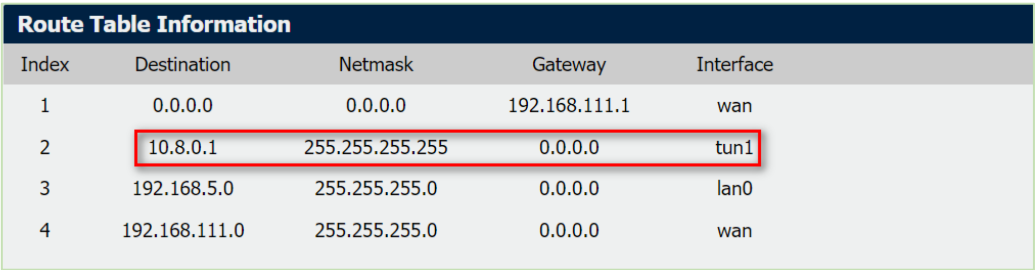
4. Route Table

1. Route Table on PC for reference.



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.111.1  192.168.111.19    291
          0.0.0.0          0.0.0.0     192.168.10.1   192.168.10.10    291
         10.8.0.0  255.255.255.252         On-link         10.8.0.1    291
         10.8.0.1  255.255.255.255         On-link         10.8.0.1    291
         10.8.0.3  255.255.255.255         On-link         10.8.0.1    291
        127.0.0.0        255.0.0.0         On-link        127.0.0.1    331
```

2. Route Table on Router for reference.

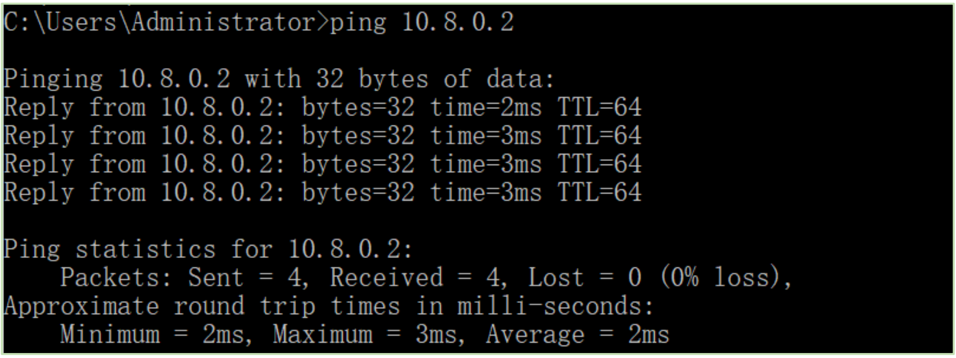


Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.1	255.255.255.255	0.0.0.0	tun1
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

5. Testing

1. Enable CMD and Ping the virtual ip from PC to router.

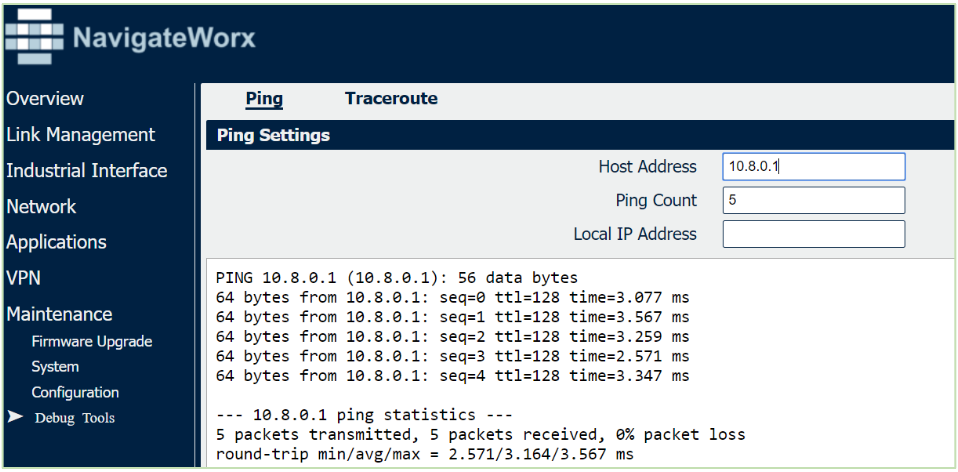


```
C:\Users\Administrator>ping 10.8.0.2

Pinging 10.8.0.2 with 32 bytes of data:
Reply from 10.8.0.2: bytes=32 time=2ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64

Ping statistics for 10.8.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

2. Go to **Maintenance>Debug Tool>Ping** and Ping the virtual ip from router to PC.



Host Address 10.8.0.1

Ping Count 5

Local IP Address

```
PING 10.8.0.1 (10.8.0.1): 56 data bytes
64 bytes from 10.8.0.1: seq=0 ttl=128 time=3.077 ms
64 bytes from 10.8.0.1: seq=1 ttl=128 time=3.567 ms
64 bytes from 10.8.0.1: seq=2 ttl=128 time=3.259 ms
64 bytes from 10.8.0.1: seq=3 ttl=128 time=2.571 ms
64 bytes from 10.8.0.1: seq=4 ttl=128 time=3.347 ms

--- 10.8.0.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 2.571/3.164/3.567 ms
```

3. Test successfully