

NR500 Series Industrial Cellular VPN Router

Application Note 010

OpenVPN with TAP under P2P mode

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



Directory

1. Introduction.....	3
1.1 Overview.....	3
1.2 Compatibility.....	3
1.3 Version.....	3
1.4 Corrections.....	3
2. Topology.....	4
3. Configuration.....	5
3.1 PC Configuration.....	5
3.2 Router Configuration.....	6
4. Route Table.....	7
5. Testing.....	8

1. Introduction

1.1 Overview

This document contains information regarding the configuration and use of OpenVPN with TAP under P2P mode.

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

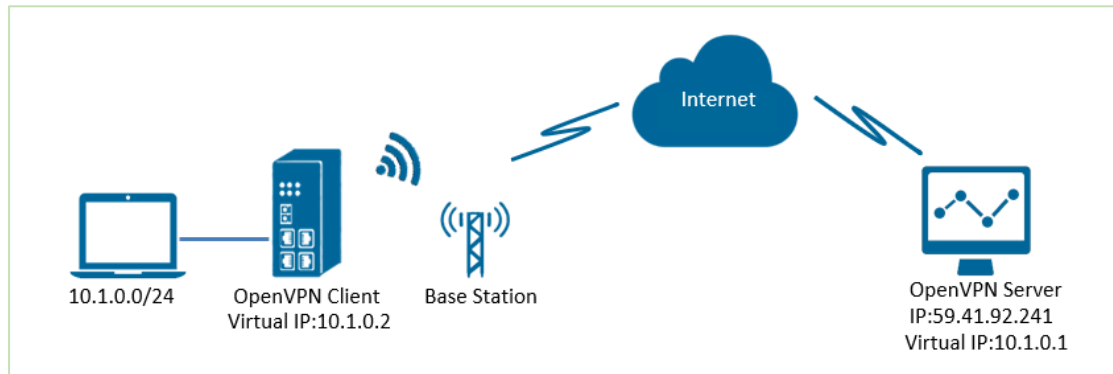
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

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

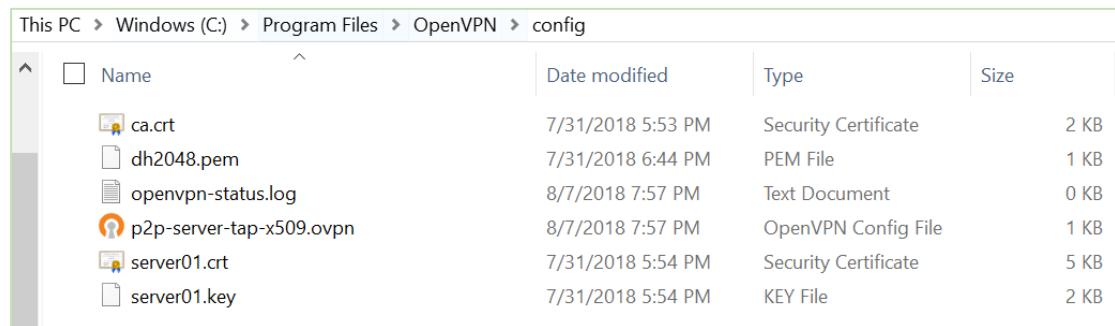


1. NR500 Pro runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the virtual IP can PING each other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

3. Configuration

3.1 PC Configuration

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



Name	Date modified	Type	Size
ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB
dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB
openvpn-status.log	8/7/2018 7:57 PM	Text Document	0 KB
p2p-server-tap-x509.ovpn	8/7/2018 7:57 PM	OpenVPN Config File	1 KB
server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB
server01.key	7/31/2018 5:54 PM	KEY File	2 KB

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

2. The configuration of "p2p-server-tap-x.509.ovpn" like below:

```

=====
mode p2p
port 1194
proto udp
dev tap
# tap
ifconfig 10.1.0.1 255.255.255.0
keepalive 20 120
persist-key
persist-tun
tls-server
ca ca.crt
cert server01.crt
key server01.key
dh dh2048.pem
#tls-auth ta.key 0
cipher BF-CBC
comp-lzo
status openvpn-status.log
verb 3
tun-mtu 1500
fragment 1500
=====

```

3.2 Router 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

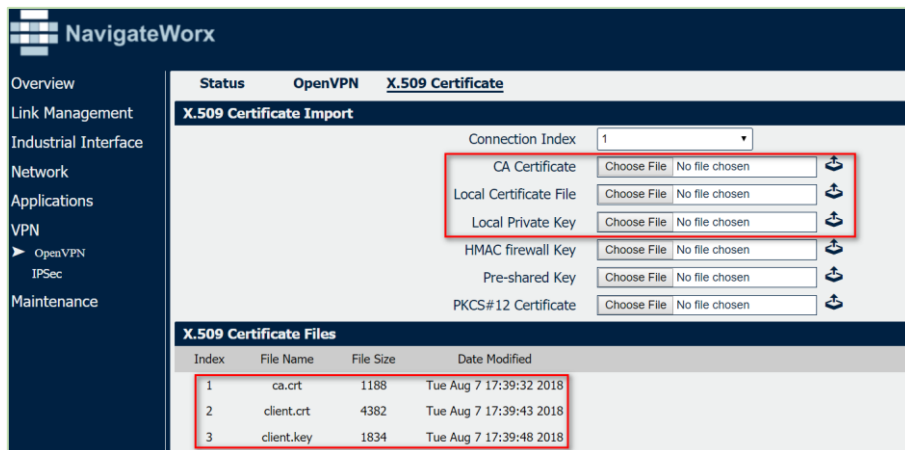
Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>
Description	<input type="text" value="1"/>
Mode	<input type="text" value="P2P"/>
Protocol	<input type="text" value="UDP"/>
Connection Type	<input type="text" value="TAP"/>
Server Address	<input type="text" value="59.41.92.241"/>
Server Port	<input type="text" value="1194"/>
Authentication Method	<input type="text" value="X.509"/> ?
Encryption Type	<input type="text" value="BF-CBC"/>
Local IP Address	<input type="text" value="10.1.0.2"/>
Local Netmask	<input type="text" value="255.255.255.0"/>
TAP Bridge	<input type="text" value="LAN0"/>
Renegotiate Interval	<input type="text" value="3600"/>
Keepalive Interval	<input type="text" value="20"/>
Keepalive Timeout	<input type="text" value="60"/>
Fragment	<input type="text" value="1500"/> ?
Private Key Password	<input type="text" value="123456"/>
Output Verbosity Level	<input type="text" value="3"/>

Advanced Settings

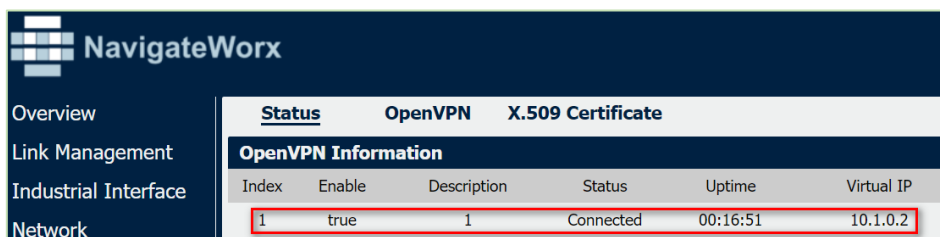
Enable NAT	<input checked="" type="checkbox"/>
Enable PKCS#12	<input type="checkbox"/>
Enable X.509 Attribute nsCertType	<input type="checkbox"/>
Enable HMAC Firewall	<input type="checkbox"/>
Enable Compression LZ0	<input checked="" type="checkbox"/>
Additional Configurations	<input type="text"/> ?

2. Click Save>Apply.

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

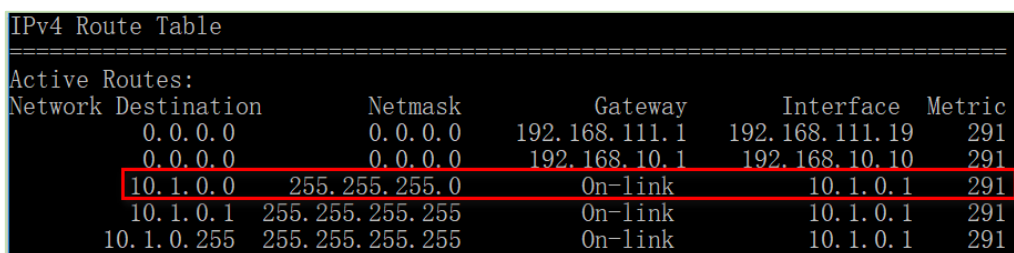


4.Route had connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.



4. Route Table

1. Route Table on PC side for reference.



2. Route Table on router side for reference.

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.1.0.0	255.255.255.0	0.0.0.0	lan0
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 from PC side to LAN device of router.

```
C:\Users\Administrator>ping 10.1.0.20

Pinging 10.1.0.20 with 32 bytes of data:
Reply from 10.1.0.20: bytes=32 time=5ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128

Ping statistics for 10.1.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

2. Ping from LAN device of router to PC side.

```
C:\Users\Administrator>ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data:
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. Test successfully.