NavigateWorx

NR500 Series
Industrial Cellular VPN Router

Application Note 006

OpenVPN Client with x.509 certificate

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

1.3 Version

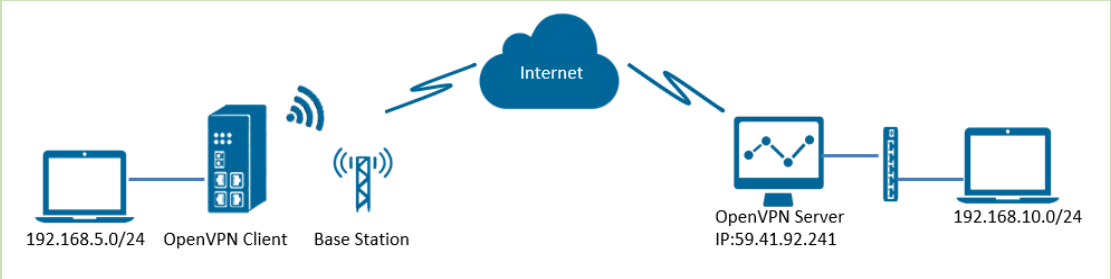
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2018/08/06	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

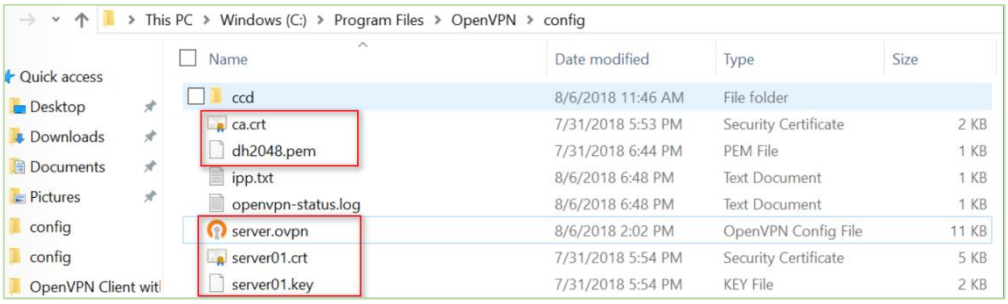


1. NR500 Pro runs as OpenVPN Client with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client, the subnet can PING each other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

3. Configuration

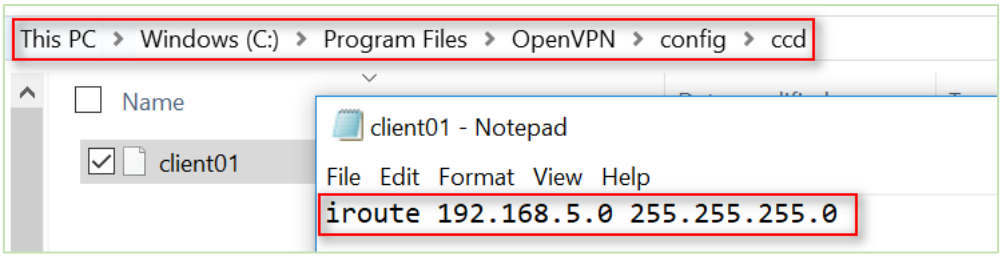
3.1 Server Configuration

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



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

2. Add a "ccd" folder, and create a new notepad, rename it without suffix, configure it like below:



***Note**: client01 is the common name; 192.168.5.0/24 is the subnet behind NR500.*

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

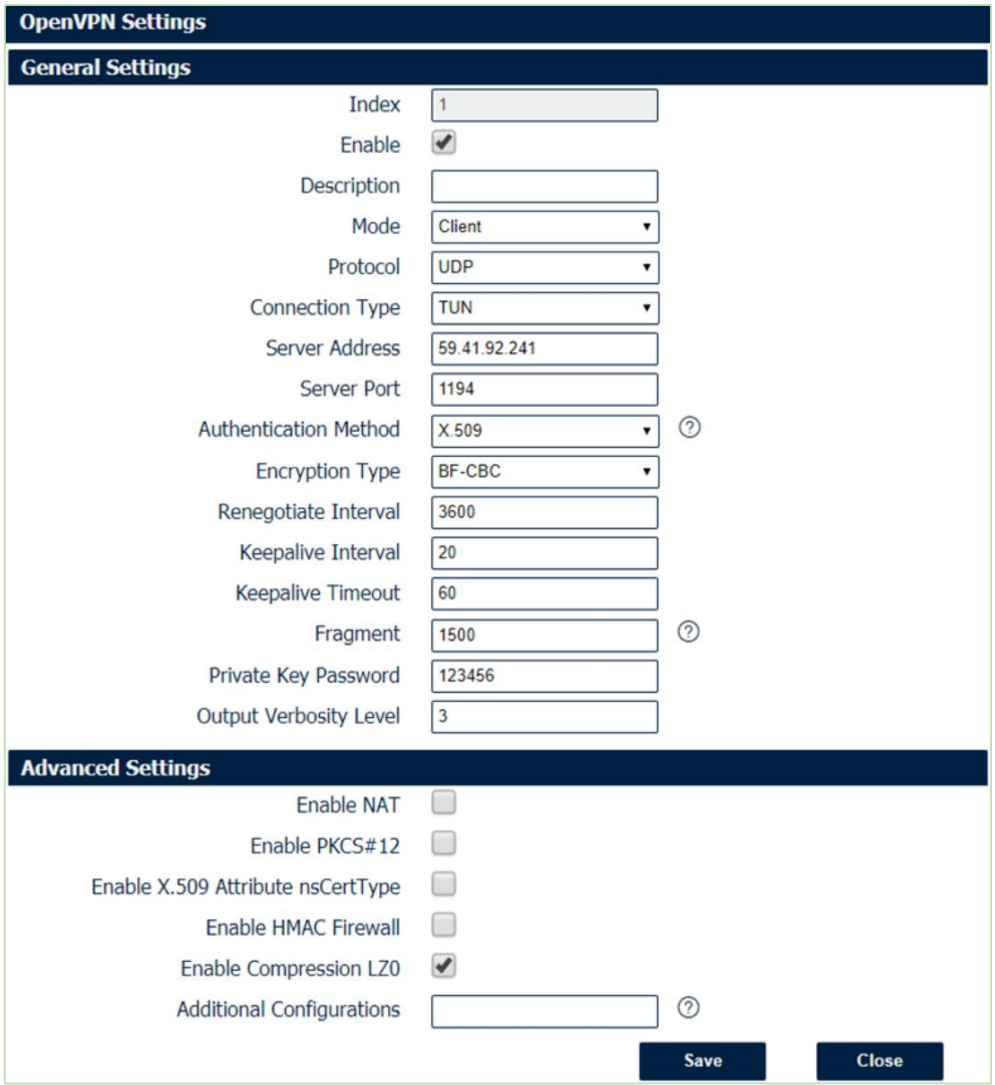
```
================================================================
local 59.41.92.241
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert server01.crt
key server01.key    # This file should be kept secret
dh dh2048.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
```

```
push "route 192.168.10.0 255.255.255.0"
client-config-dir ccd
route 192.168.5.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

==========

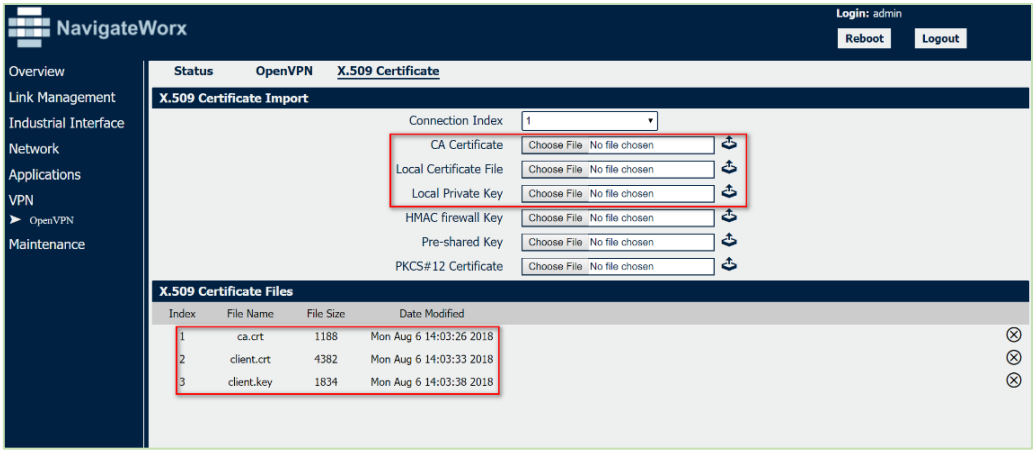
3.2 Client Configuration

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

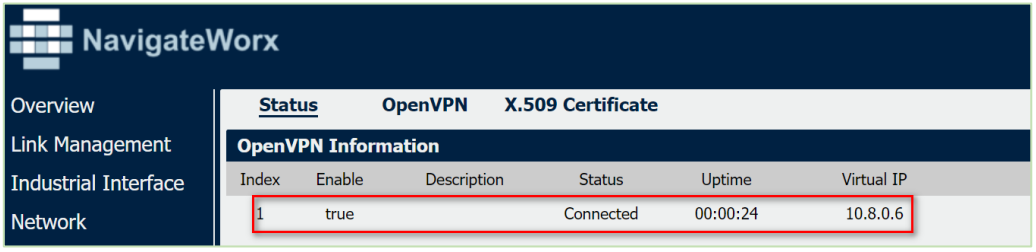


2. Click Save>Apply.

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

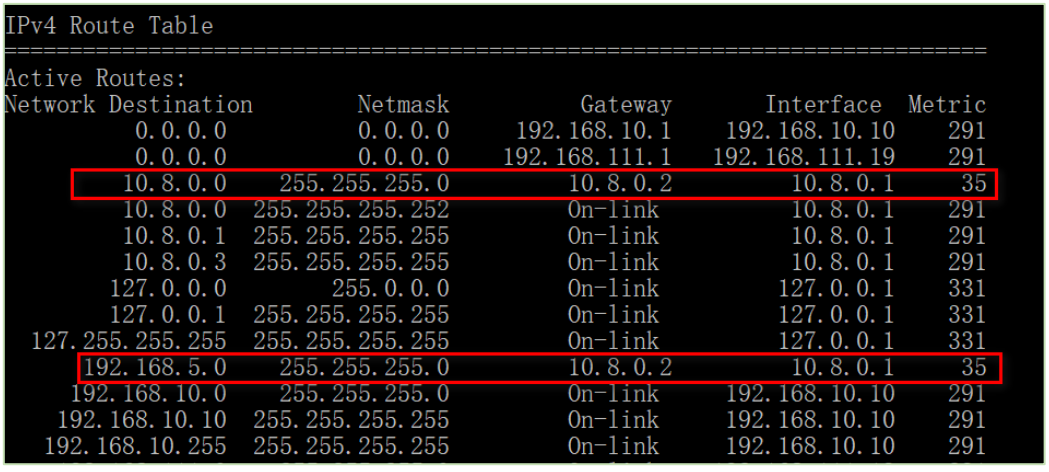


4.Route had connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.



4. Route Table

1. Route Table on OpenVPN Server for reference.



2. Route Table on OpenVPN Client 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	10.8.0.5	tun1
3	10.8.0.5	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	0.0.0.0	lan0
5	192.168.10.0	255.255.255.0	10.8.0.5	tun1
6	192.168.111.0	255.255.255.0	0.0.0.0	wan

5. Testing

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

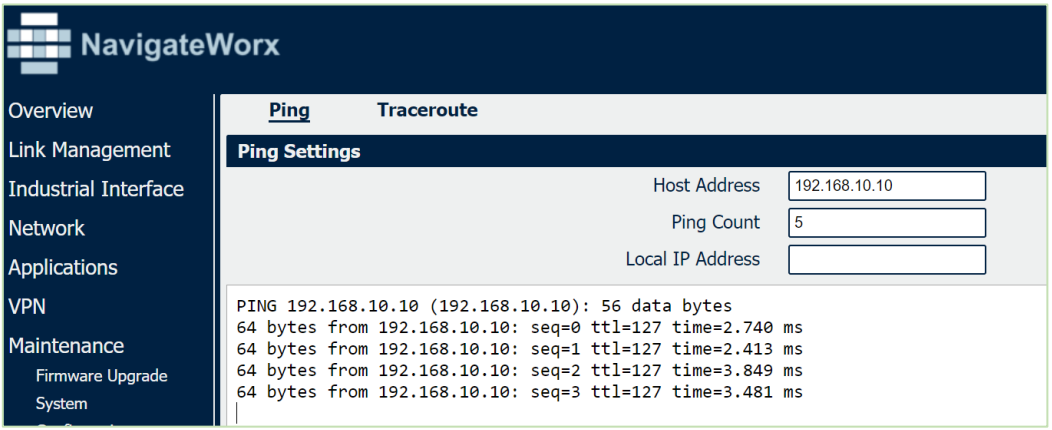
```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.5.1

Pinging 192.168.5.1 with 32 bytes of data:
Reply from 192.168.5.1: bytes=32 time=2ms TTL=64
Reply from 192.168.5.1: bytes=32 time=8ms TTL=64
Reply from 192.168.5.1: bytes=32 time=3ms TTL=64
Reply from 192.168.5.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 8ms, Average = 4ms
```

2. Go to **Maintenance>Debug Tool>Ping** and Ping from OpenVPN client to OpenVPN Server.



3. Test successfully.