NavigateWorx

NR500 Series
Industrial Cellular VPN Router

Application Note 008

OpenVPN Client with Username&Password

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 username and password.

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

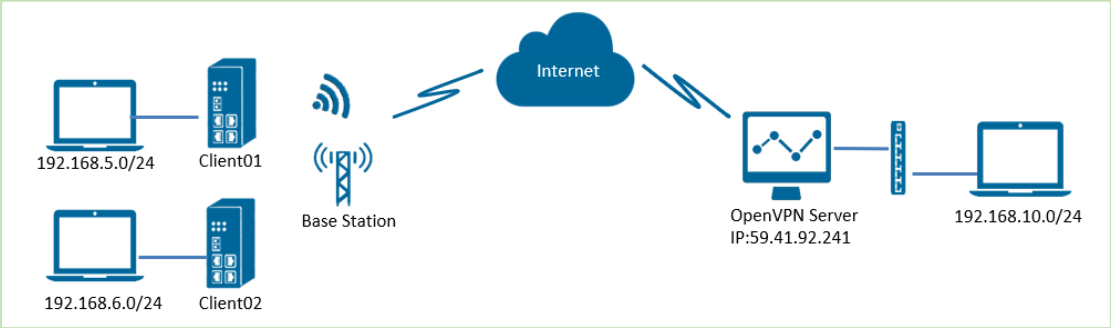
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

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

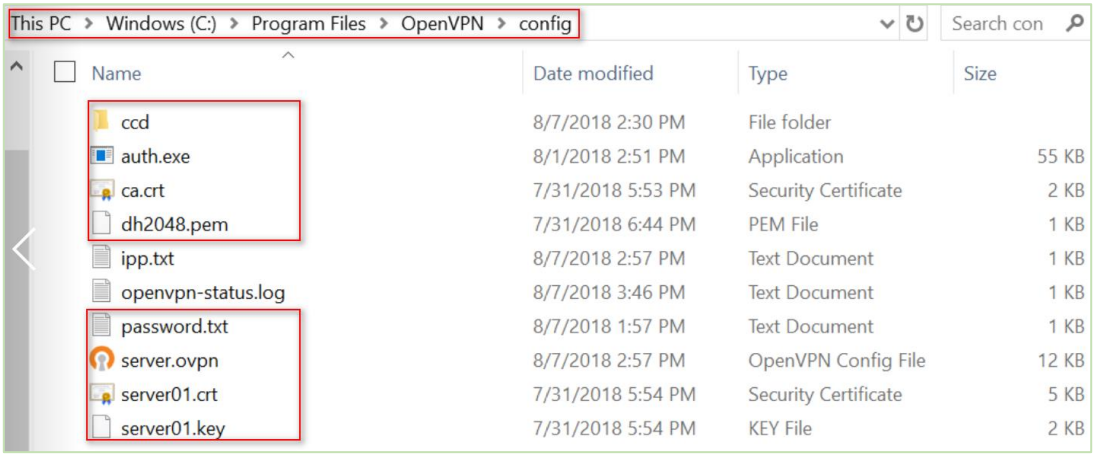


1. Two NR500 Pro run as OpenVPN Client01 and Client02 with any kind of IP, which can ping OpenVPN server IP successfully.
2. A PC runs as OpenVPN Server with a static public IP and open a specified a listening port for OpenVPN.
3. OpenVPN tunnel is established between Server and Client. Client01 can ping Client02 successfully and vice versa.

3. Configuration

3.1 Server Configuration

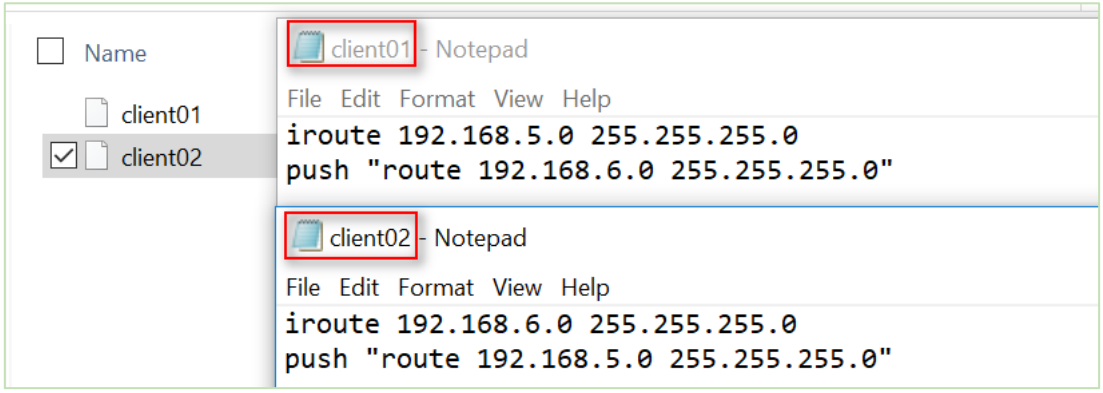
1. Install OpenVPN software on PC and copy the related certifications and configuration to the PC like below:



Note**: a) Kindly download OpenVPN software with: **https://openvpn.net/

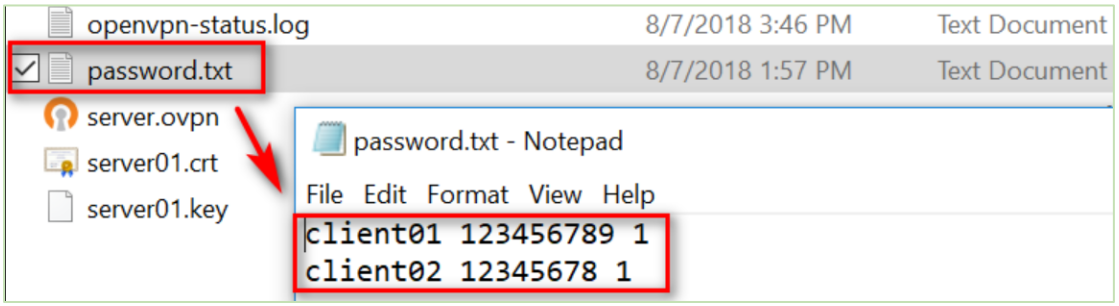
*b) Kindly install and run OpenVPN software with **administrator authority**.*

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



***Note**: client01 and client02 are the common name.*

3.Create a "password.txt" file, which including below content:



The format would be: ***common name password 1or 0(1=enable,0=disable)***

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

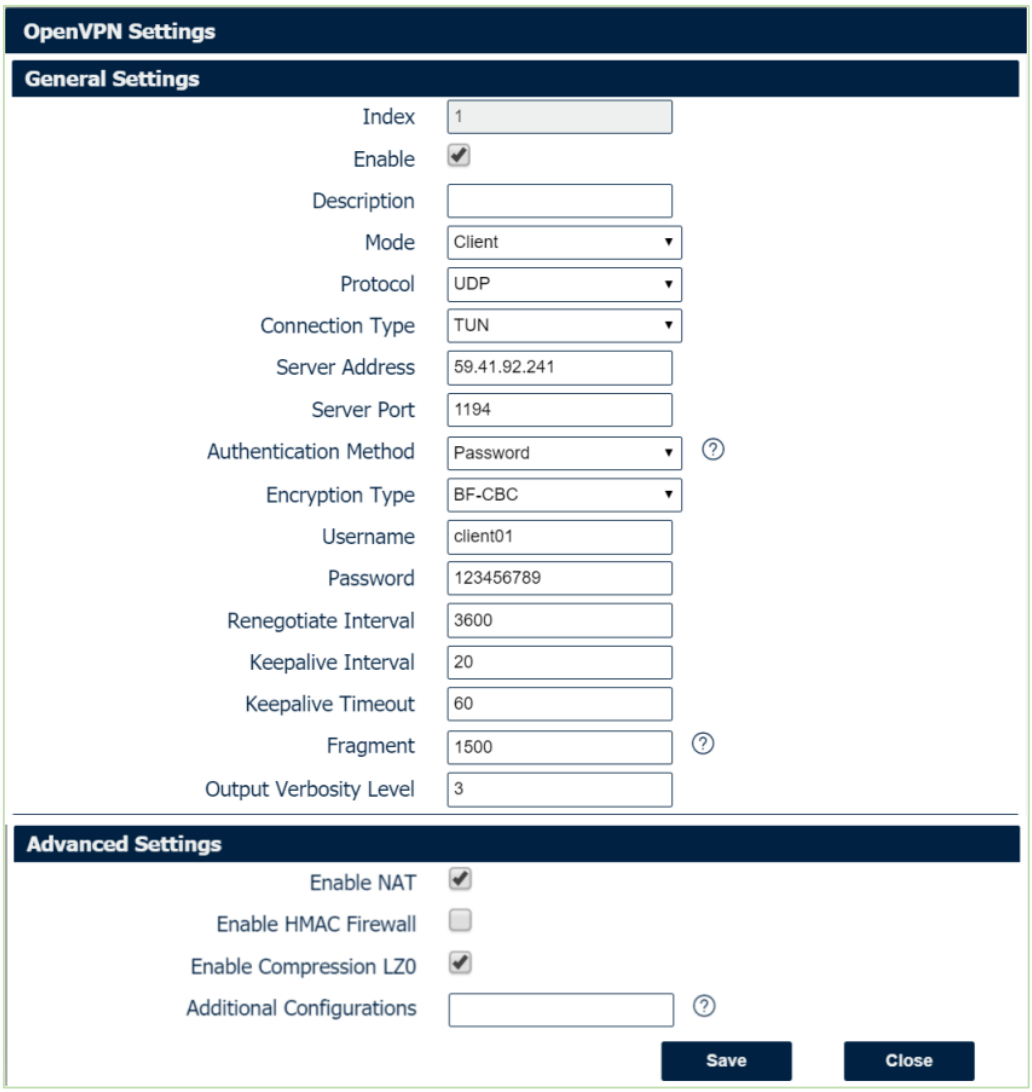
==========

```
local 59.41.92.241
mode server
port 1194
proto udp
client-cert-not-required
username-as-common-name
auth-user-pass-verify auth.exe via-env
script-security 3 system
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
route 192.168.6.0 255.255.255.0
client-to-client
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

==========

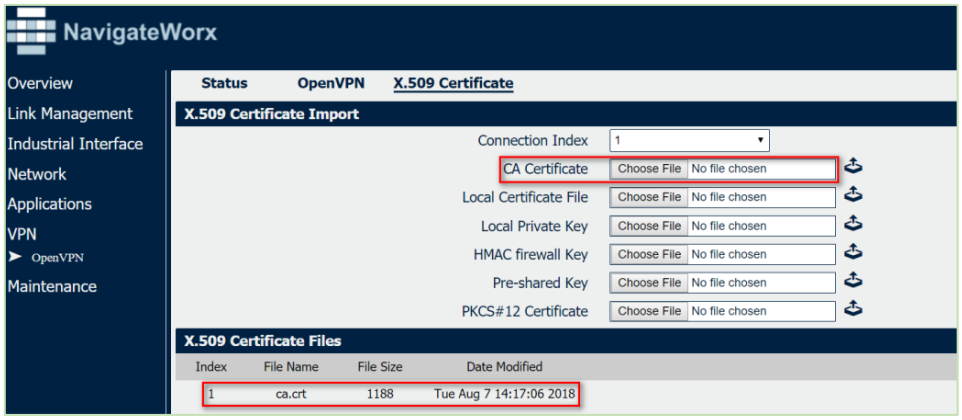
3.2 Client01 Configuration

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

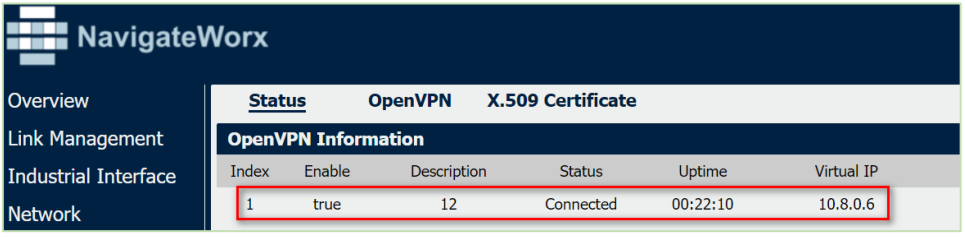


2. Click Save>Apply.

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

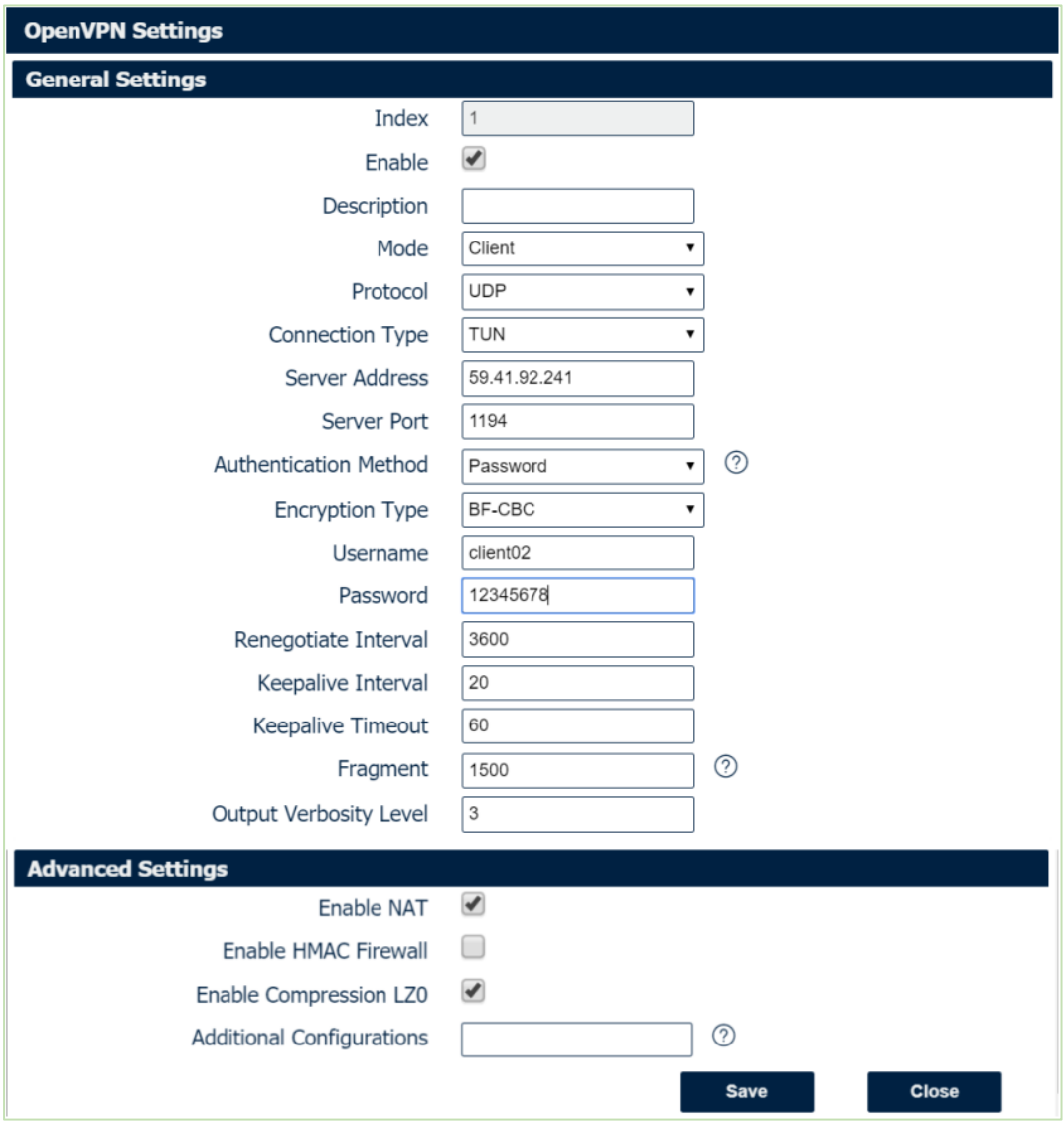


4.Route had connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.



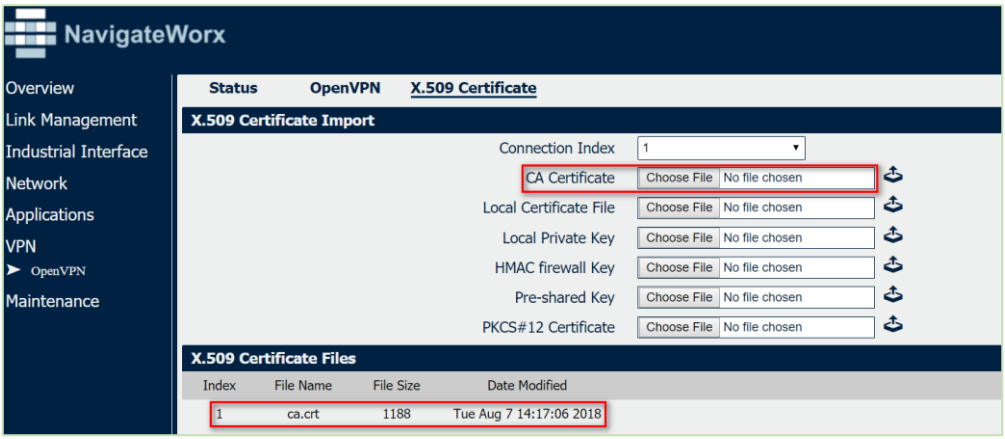
3.3 Client02 Configuration

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

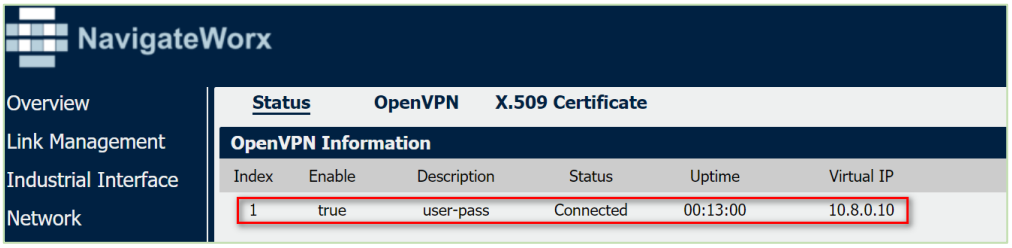


2. Click Save>Apply.

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

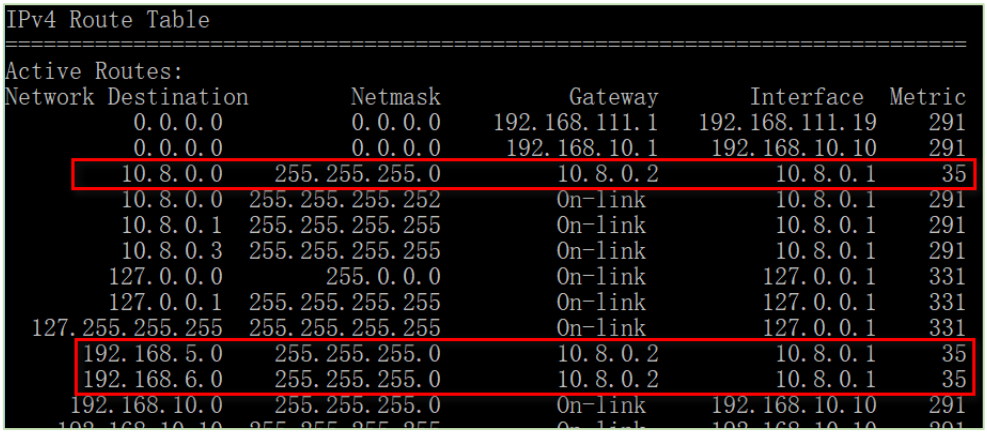


4.Route had connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.

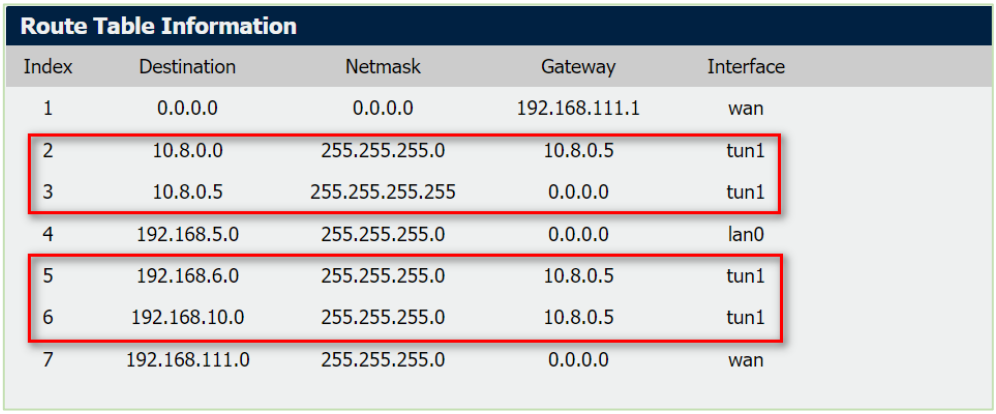


4. Route Table

1. Route Table on OpenVPN Server for reference.



2. Route Table on Client01 for reference.



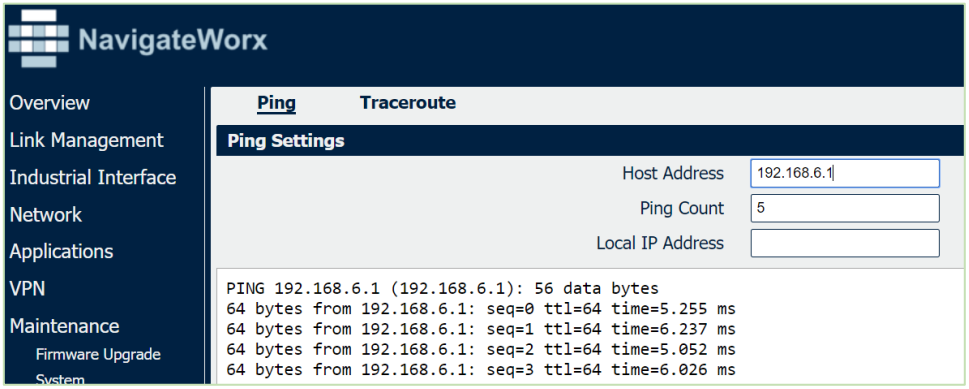
3. Route Table on Client02 for reference.

Route Table Information

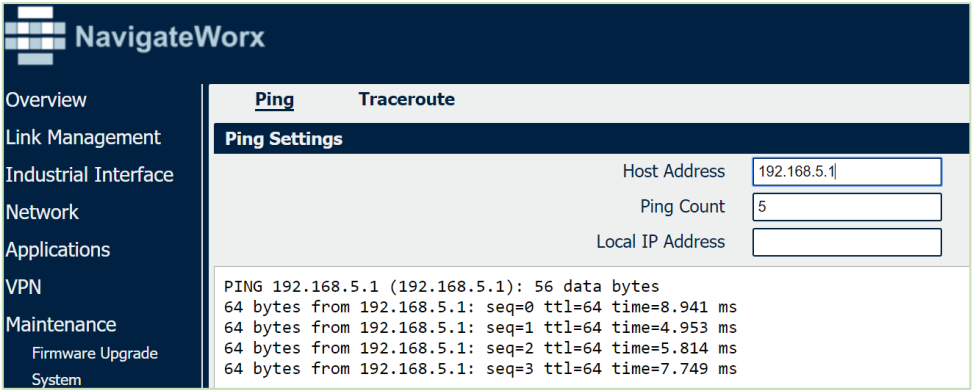
Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.0	255.255.255.0	10.8.0.9	tun1
3	10.8.0.9	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	10.8.0.9	tun1
5	192.168.6.0	255.255.255.0	0.0.0.0	lan0
6	192.168.10.0	255.255.255.0	10.8.0.9	tun1
7	192.168.111.0	255.255.255.0	0.0.0.0	wan

4. Testing

1. Ping from Client01 to Client02 as below:



2. Ping from Client02 to Client01 as below:



3. Test successfully