NavigateWorx

NR500 Series
Industrial Cellular VPN Router

Application Note 027

GRE VPN Between NR500 and CISCO

Version: V1.0.0
Date: 2018/09/30
Status: Confidential

Directory

1. Introduction

1.1 Overview

This document contains information regarding the configuration and use of GRE VPN between NR500 router and CISCO.

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 (930.3) or newer
Other Compatible Models: None

1.3 Version

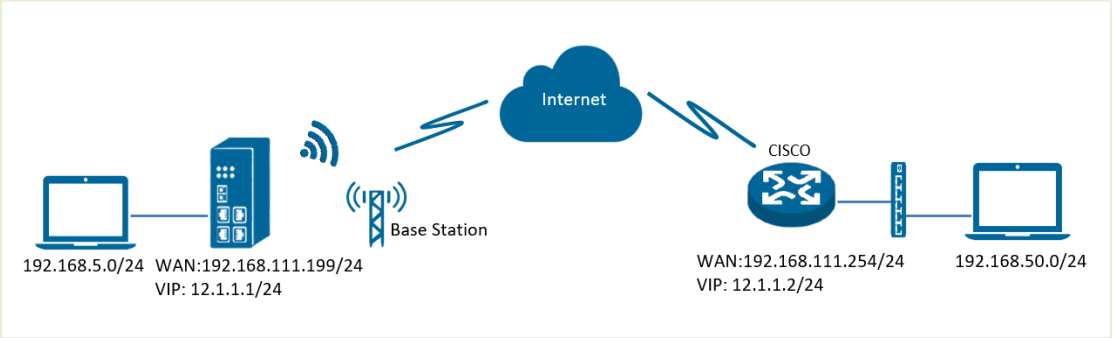
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2018/09/30	V1.0.0	V1.0.0(930.3)	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



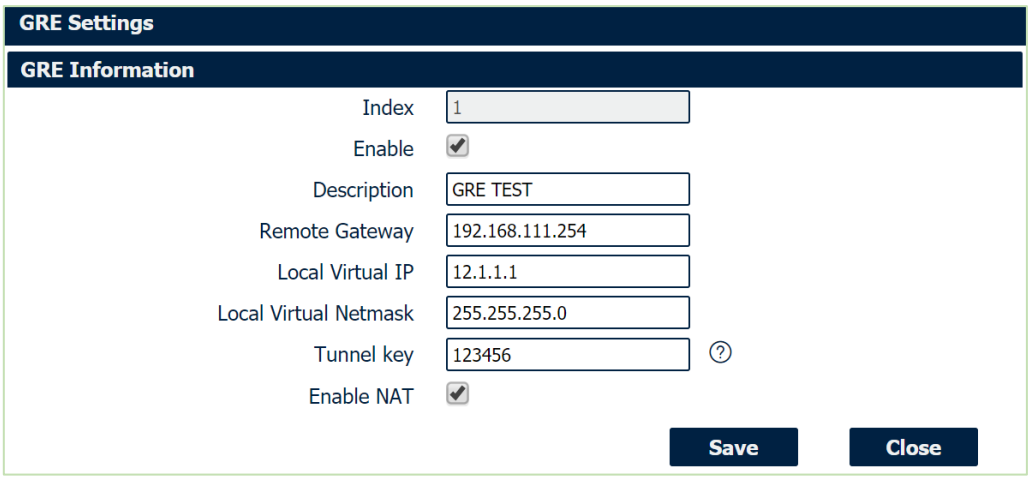
1. NR500 Pro work with static public IP or dynamic public IP with domain name .
2. CISCO router run as central router with static public IP or dynamic public IP with domain name.
3. GRE VPN tunnel establish between NR500 Pro and CISCO router.

3. Configuration

3.1 Router Configuration

1. Go to **VPN>GRE>GRE**, Click the Edit button of GRE, like below:

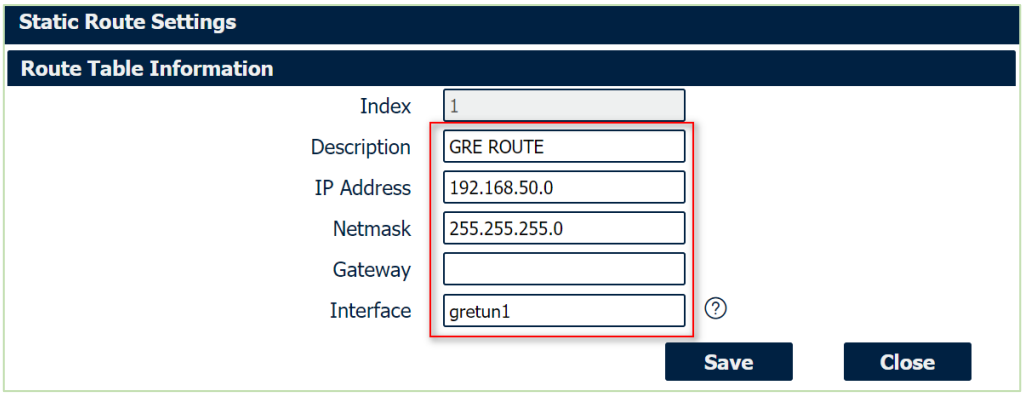
2. Configure GRE VPN like below picture:



3. Click Save>Apply.

4. Go to **Network>Route>Route**, to configure the route to the subnet of cisco, to make sure that the subnet can reach each other.

5. The static route setting like below:



3.2 CISCO Router Configuration

1. Telnet to cisco route and configure cisco route GRE VPN like below:

==========

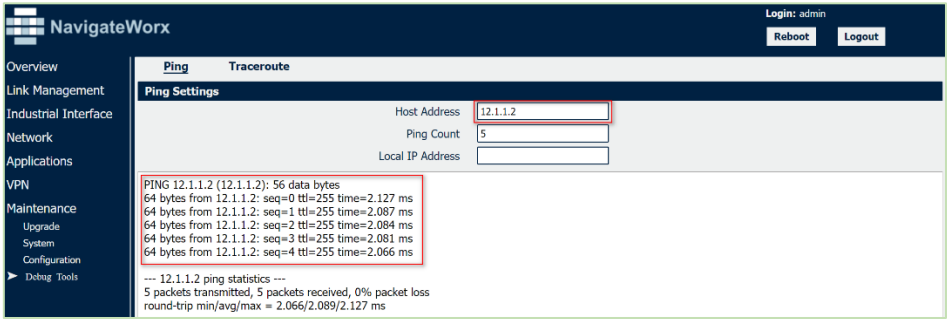
```
cisco2811#
cisco2811#SHOW RUNning-config
Building configuration...
version 12.4
!
hostname cisco2811
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
username admin password 0 admin
archive
 log config
  hidekeys
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface Tunnel1
 ip address 12.1.1.2 255.255.255.0
 tunnel source 192.168.111.254
 tunnel destination 192.168.111.199
 tunnel key 123456
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
```

```
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map MAP
!
interface FastEthernet0/1
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
ip route 192.168.5.0 255.255.255.0 12.1.1.1
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface FastEthernet0/0 overload
!
access-list 10 permit 192.168.5.0 0.0.0.255
!
end
```

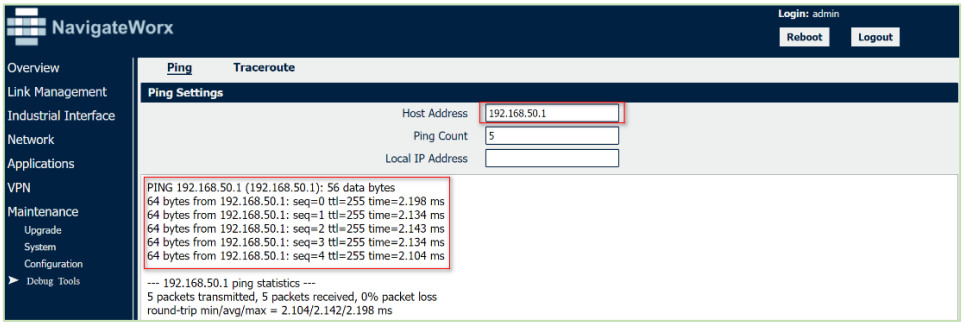
==========

4. Test

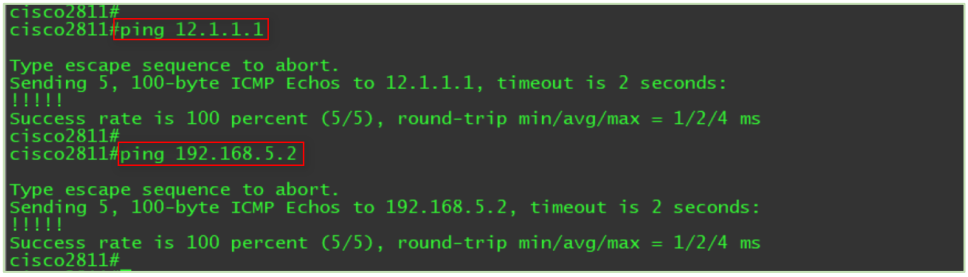
1. Ping the virtual IP from NR500 to cisco route.



2. Ping subnet from NR500 to cisco.



3. Ping virtual IP and subnet from CISCO to NR500.



4. Test successfully.