NR500 Series
Industrial Cellular VPN Router

Application Note 013

IPSec_FQDN with CISCO router

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 IPSec_FQDN with CISCO router.

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
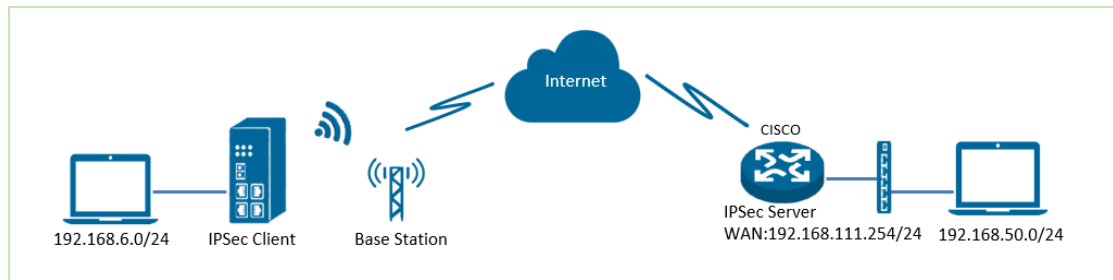**Other Compatible Models:** None

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 IPSec Client with any kind of IP, which can ping IPSec server IP successfully.
2. CISCO router runs as IPSec Server with a static public IP.
3. IPSec tunnel is established between NR500 Pro and cisco router.

3. Configuration

3.1 Server Configuration

1. Login to CISCO router and setting like below:
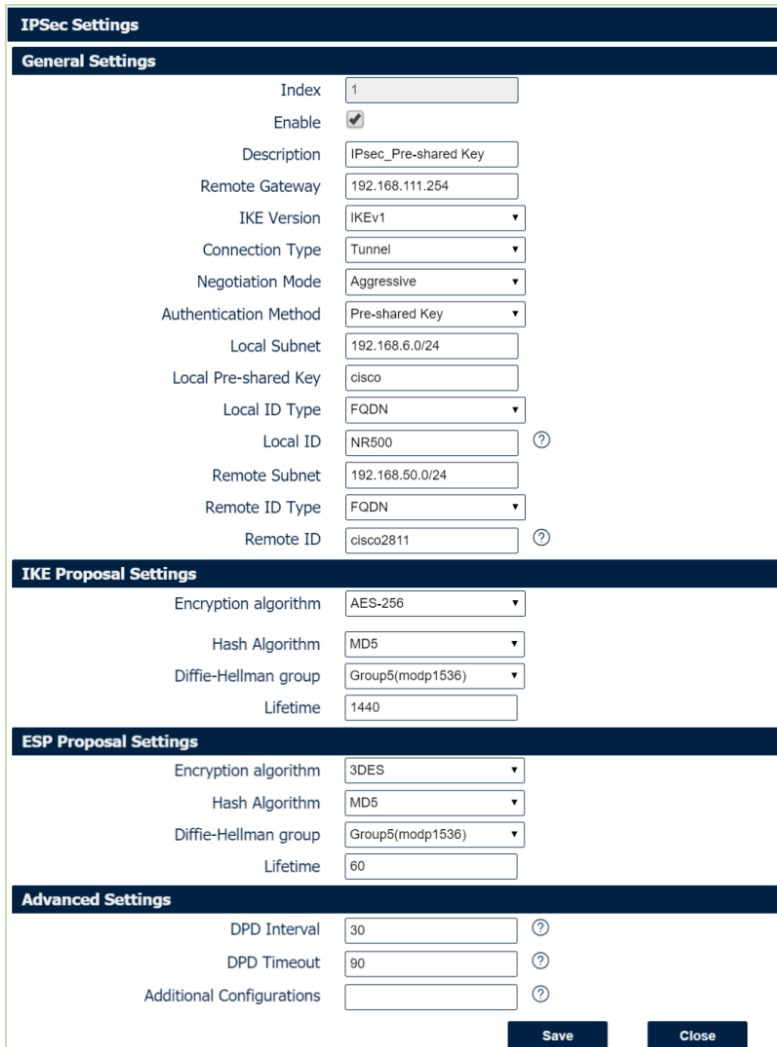==
cisco2811#show running-config
Building configuration...
version 12.4
hostname cisco2811
!
logging message-counter syslog
enable secret 5 1tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
!
no aaa new-model
ip cef
!
ip name-server 192.168.111.1
ip address-pool local
multilink bundle-name authenticated
!
username cisco password 0 cisco
archive
  log config
    hidekeys
!
crypto isakmp policy 10
  encr aes 256
  hash md5
  authentication pre-share
  group 5
crypto isakmp key 6 cisco hostname NR500
crypto isakmp identity hostname
!
crypto isakmp peer address 0.0.0.0
  set aggressive-mode password cisco
  set aggressive-mode client-endpoint fqdn NR500
!
crypto ipsec transform-set NR500 esp-3des esp-md5-hmac
!
crypto dynamic-map DYN 10
  set transform-set NR500

```
 set pfs group5
 match address 101
 reverse-route
!
crypto map SMAP 10 ipsec-isakmp dynamic DYN
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
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 SMAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto

ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface FastEthernet0/0 overload
!
ip access-list extended VPN
  permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0 0.0.0.255 192.168.6.0 0.0.0.255
snmp-server community public RO
!
end
cisco2811#
============================================================
```

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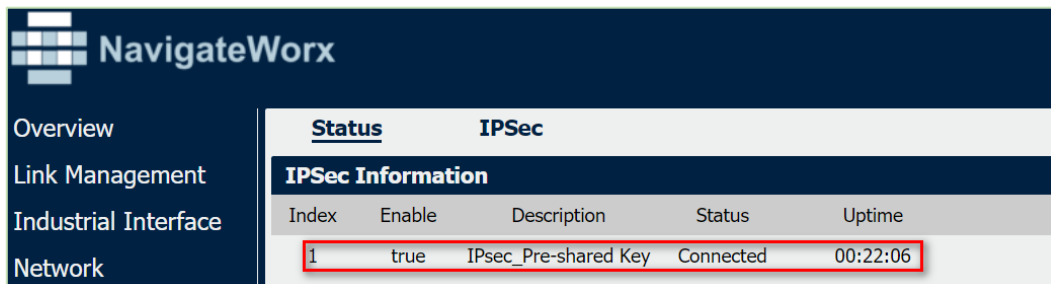
1. Go to **VPN>IPSec>IPSec>General Settings**, click the Edit Button and configure IPSec VPN as below picture. Click Save.

2. Click Save>Apply.

3.IPSec had been connected successfully. Go to **VPN>IPSec>Status** to check the connection status.

4. Testing

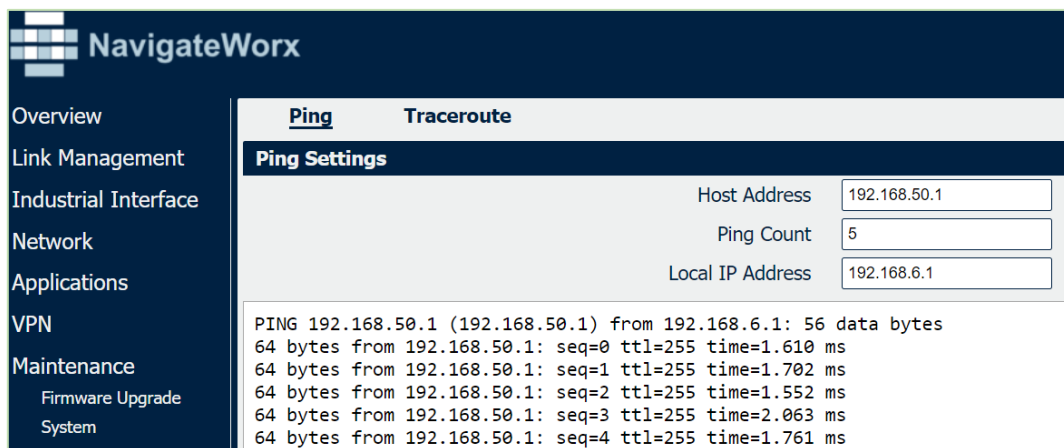1. Ping from CISCO router to NR500, LAN to LAN communication is working correctly.

```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

2. Ping from NR500 to CISCO router, LAN to LAN communication is working correctly.

NavigateWorx	
Overview	**Ping** **Traceroute**
Link Management	**Ping Settings**
Industrial Interface	Host Address 192.168.50.1
Network	Ping Count 5
Applications	Local IP Address 192.168.6.1
VPN	PING 192.168.50.1 (192.168.50.1) from 192.168.6.1: 56 data bytes
Maintenance	64 bytes from 192.168.50.1: seq=0 ttl=255 time=1.610 ms
Firmware Upgrade	64 bytes from 192.168.50.1: seq=1 ttl=255 time=1.702 ms
System	64 bytes from 192.168.50.1: seq=2 ttl=255 time=1.552 ms
	64 bytes from 192.168.50.1: seq=3 ttl=255 time=2.063 ms
	64 bytes from 192.168.50.1: seq=4 ttl=255 time=1.761 ms

3. Test successfully.