NavigateWorx

NR500 Series
Industrial Cellular VPN Router

Application Note 015

IPSec_FQDN_Pre shared key and Xauth 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_Pre shared key and Xauth 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

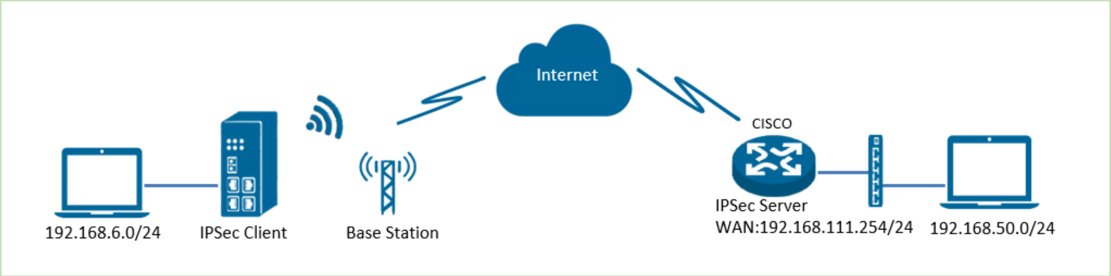
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

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:

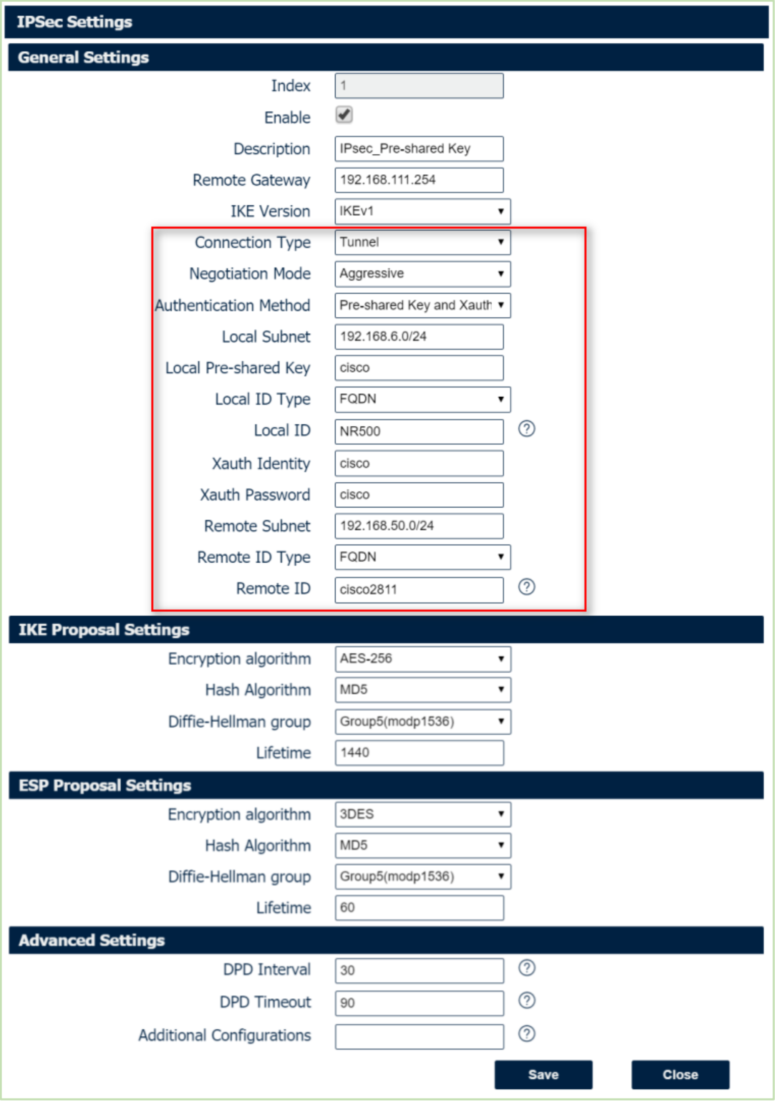
```
============================================================
cisco2811#show running-config
version 12.4
hostname cisco2811
!
logging message-counter syslog
enable secret 5 $1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.!
aaa new-model
!
aaa authentication login LOGIN local
!
aaa session-id common
!
ip name-server 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 cisco hostname NR500
crypto isakmp identity hostname
!
crypto isakmp peer address 0.0.0.0
 set aggressive-mode password ken
 set aggressive-mode client-endpoint fqdn cisco2811
!
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 MAP client authentication list LOGIN
crypto map MAP 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
no mop enabled
 crypto map MAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex 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
line con 0
line vty 5 15
end
=============================================================
```

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.



IPSec Settings

General Settings

Index	1
Enable	☑
Description	IPsec_Pre-shared Key
Remote Gateway	192.168.111.254
IKE Version	IKEv1
Connection Type	Tunnel
Negotiation Mode	Aggressive
Authentication Method	Pre-shared Key and Xauth
Local Subnet	192.168.6.0/24
Local Pre-shared Key	cisco
Local ID Type	FQDN
Local ID	NR500
Xauth Identity	cisco
Xauth Password	cisco
Remote Subnet	192.168.50.0/24
Remote ID Type	FQDN
Remote ID	cisco2811

IKE Proposal Settings

Encryption algorithm	AES-256
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	1440

ESP Proposal Settings

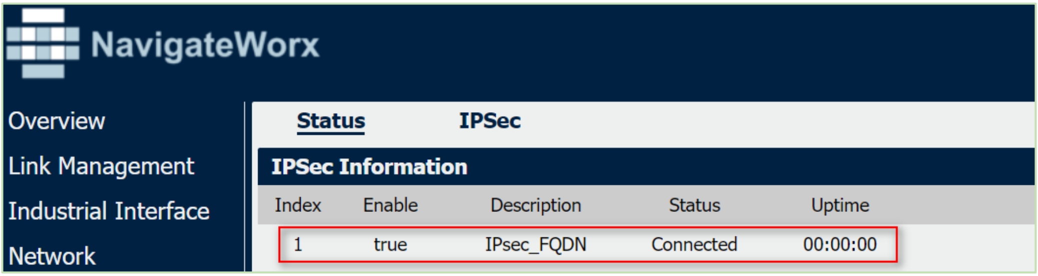
Encryption algorithm	3DES
Hash Algorithm	MD5
Diffie-Hellman group	Group5(modp1536)
Lifetime	60

Advanced Settings

DPD Interval	30
DPD Timeout	90
Additional Configurations	

2. Click Save>Apply.

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

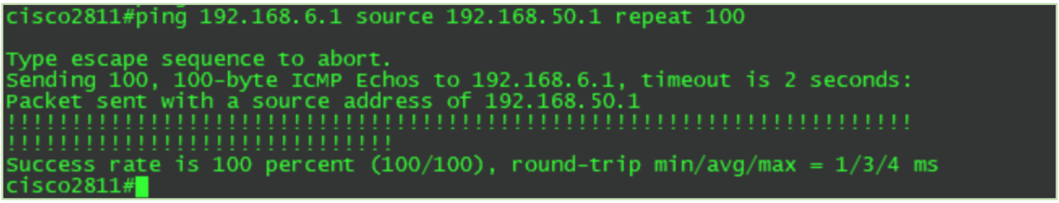


IPSec Information

Index	Enable	Description	Status	Uptime
1	true	IPsec_FQDN	Connected	00:00:00

4. Testing

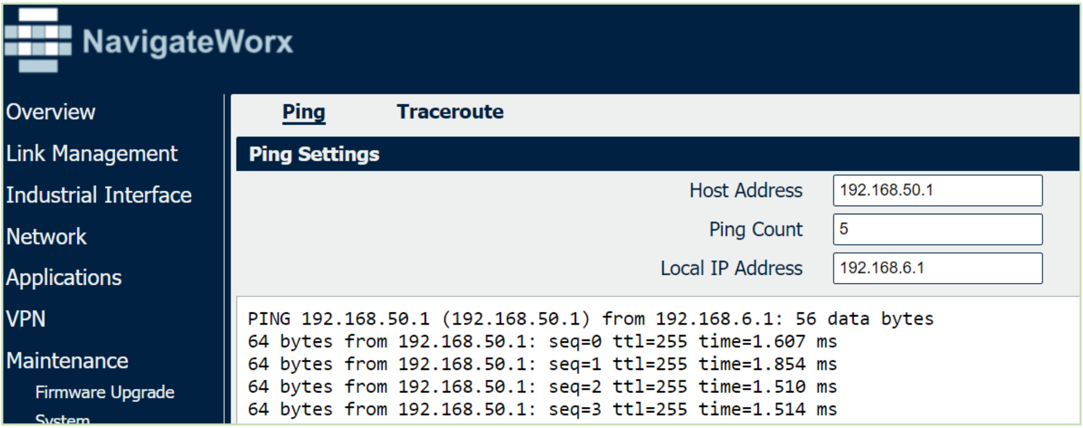
1. Ping from CISCO router to NR500, LAN to LAN communication is working correctly.



```
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.



Ping Settings

Host Address: 192.168.50.1

Ping Count: 5

Local IP Address: 192.168.6.1

```
PING 192.168.50.1 (192.168.50.1) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=255 time=1.607 ms
64 bytes from 192.168.50.1: seq=1 ttl=255 time=1.854 ms
64 bytes from 192.168.50.1: seq=2 ttl=255 time=1.510 ms
64 bytes from 192.168.50.1: seq=3 ttl=255 time=1.514 ms
```

3. Test successfully.