NavigateWorx

NR500 Series

Industrial Cellular VPN Router

Application Note 062

GRE over IPsec with RIP

Version: V1.0.0
Date: Feb. 2022
Status: Confidential

Directory

1. Introduction.....3
   1.1 Overview.....3
   1.2 Compatibility.....3
   1.3 Version.....3
   1.4 Corrections.....3
2. Topology.....4
3. GRE over IPsec Server Configuration.....5
4. GRE over IPsec Client Configuration.....8
   4.1 Configuration on IPsec.....8
   4.2 Configuration on GRE VPN.....9
   4.3 Configuration on RIP.....9
5. Testing.....11

1. Introduction

1.1 Overview

This document contains information regarding the configuration and use of GRE over IPsec with rip.

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: V1.1.7(3b5122d) or newer
Other Compatible Models: None

1.3 Version

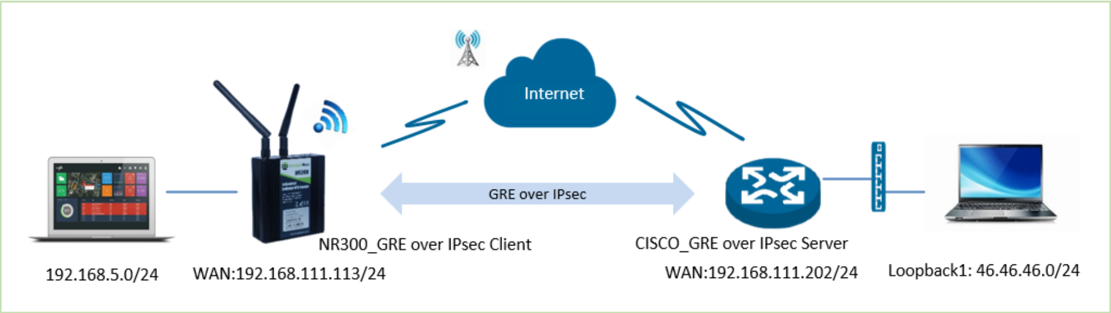
Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2022/02/17	V1.0.0	V1.1.7(3b5122d)	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/NR300 Router connect to the PC via LAN port and run the GRE over IPsec Client.
2. Cisco router run as GRE over IPsec server and enable the loopback1 interface for the testing.
3. GRE over IPsec VPN was established between NR500/NR300 successfully and finally the subnet is able to communicate with each other.

3. GRE over IPsec Server Configuration

1. Login to the cisco router and the configuration of GRE over IPsec and rip as below:

```
=================================================================
R1#show running-config
Building configuration...

Current configuration : 1704 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
aaa new-model
!
aaa authentication ppp default local
!
aaa session-id common
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ip address-pool local
!
multilink bundle-name authenticated
!
username test password 0 test123456
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 2
crypto isakmp key test123456 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set myset esp-aes esp-sha-hmac
 mode transport
!
crypto dynamic-map mydynamic 10
 set transform-set myset
!
crypto map mymap 10 ipsec-isakmp dynamic mydynamic
!
ip tcp synwait-time 5
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.0
!
interface Tunnel0
 ip address 46.46.46.1 255.255.255.0
 no ip split-horizon
 tunnel source FastEthernet0/0
 tunnel destination 192.168.111.113
 tunnel key 123456
!
interface FastEthernet0/0
 ip address 192.168.111.202 255.255.255.0
 duplex full
 crypto map mymap
!
router rip
 version 2
 network 10.0.0.0
 network 46.0.0.0
 no auto-summary
!
ip default-gateway 192.168.111.1
ip forward-protocol nd
no ip http server
no ip http secure-server
!
logging alarm informational
!
control-plane
!
```

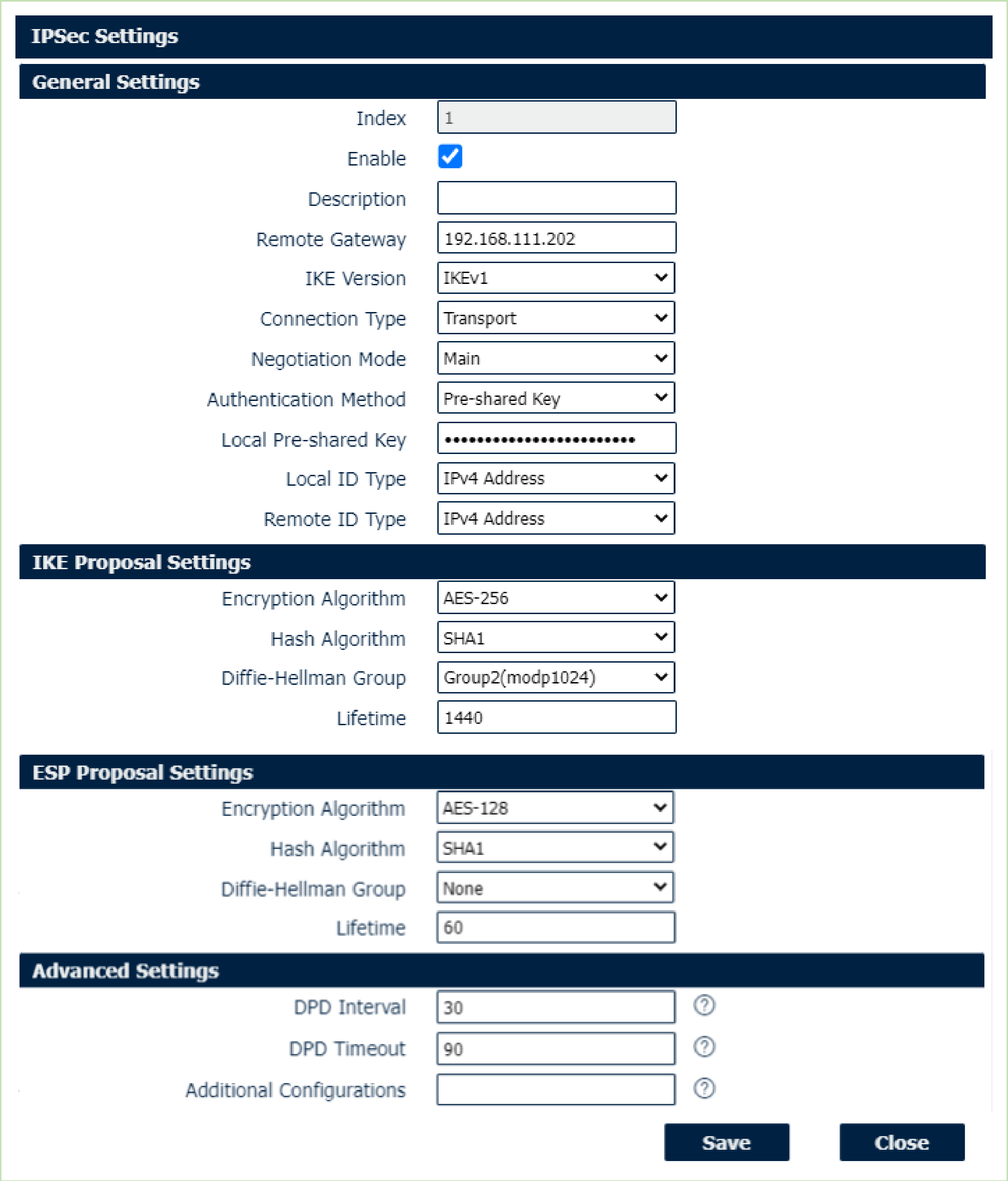
```
gatekeeper
 shutdown
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
!
end

R1#
===========================================================
```

4. GRE over IPsec Client Configuration

4.1 Configuration on IPsec

1. Go to **VPN>IPsec**, specify the IPsec settings as below:



IPSec Settings

General Settings

Index	1
Enable	☑
Description	
Remote Gateway	192.168.111.202
IKE Version	IKEv1
Connection Type	Transport
Negotiation Mode	Main
Authentication Method	Pre-shared Key
Local Pre-shared Key	••••••••••••••••••••••••
Local ID Type	IPv4 Address
Remote ID Type	IPv4 Address

IKE Proposal Settings

Encryption Algorithm	AES-256
Hash Algorithm	SHA1
Diffie-Hellman Group	Group2(modp1024)
Lifetime	1440

ESP Proposal Settings

Encryption Algorithm	AES-128
Hash Algorithm	SHA1
Diffie-Hellman Group	None
Lifetime	60

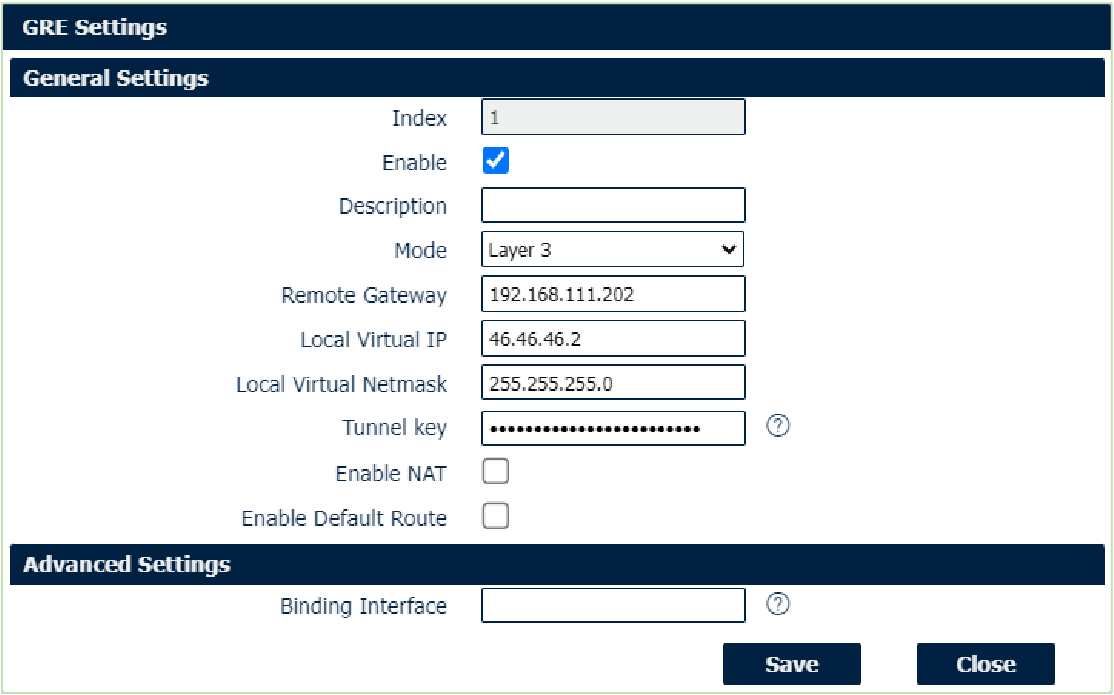
Advanced Settings

DPD Interval	30
DPD Timeout	90
Additional Configurations	

Note: Pre-shared Key is: test123456. It should be the same as the cisco side.

4.2 Configuration on GRE VPN

1. Go to **VPN>GRE**, specify the GRE VPN settings as below:



GRE Settings

General Settings

Index	1
Enable	☑
Description	
Mode	Layer 3
Remote Gateway	192.168.111.202
Local Virtual IP	46.46.46.2
Local Virtual Netmask	255.255.255.0
Tunnel key	••••••••••••••••••••••••
Enable NAT	□
Enable Default Route	□

Advanced Settings

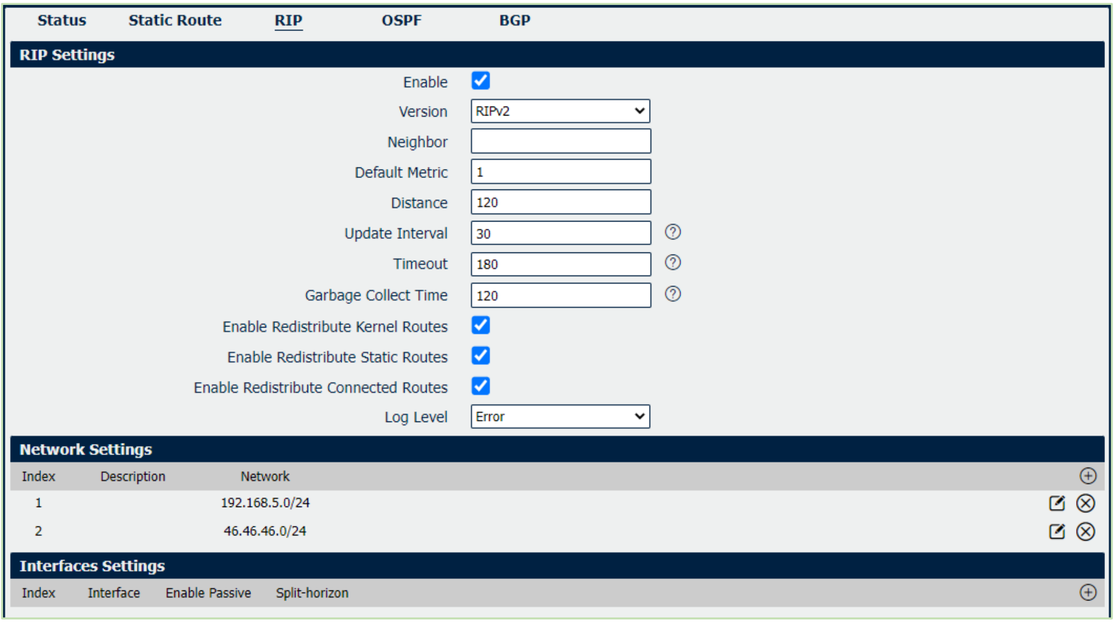
Binding Interface	

Note: The tunnel key is: 123456. It should be the same as cisco side.

2. Click Save>Apply.

4.3 Configuration on RIP

1. Go to Network>Route>RIP, specify the rip settings as below:



RIP Settings

Enable	☑
Version	RIPv2
Neighbor	
Default Metric	1
Distance	120
Update Interval	30
Timeout	180
Garbage Collect Time	120
Enable Redistribute Kernel Routes	☑
Enable Redistribute Static Routes	☑
Enable Redistribute Connected Routes	☑
Log Level	Error

Network Settings

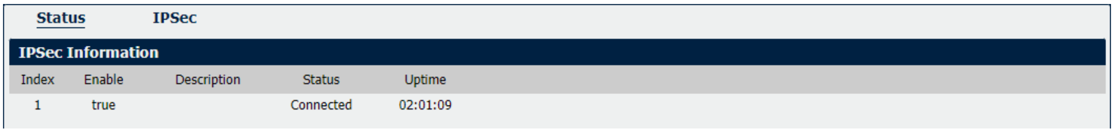
Index	Description	Network
1		192.168.5.0/24
2		46.46.46.0/24

Interfaces Settings

Index	Interface	Enable Passive	Split-horizon

Finally, the NR300/NR500 router is able to connect the CISCO router via GRE over IPsec and the subnet was declared successfully via RIP protocol.

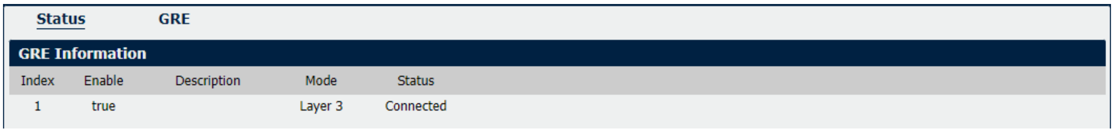
IPsec had been connected to cisco successfully, as below:



IPSec Information

Index	Enable	Description	Status	Uptime
1	true		Connected	02:01:09

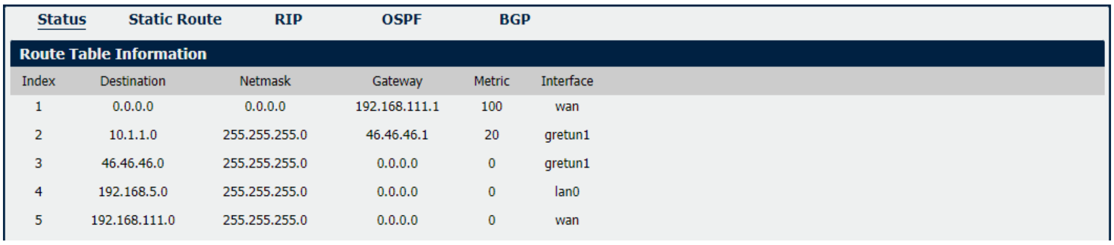
GRE had been connected to cisco successfully, as below:



GRE Information

Index	Enable	Description	Mode	Status
1	true		Layer 3	Connected

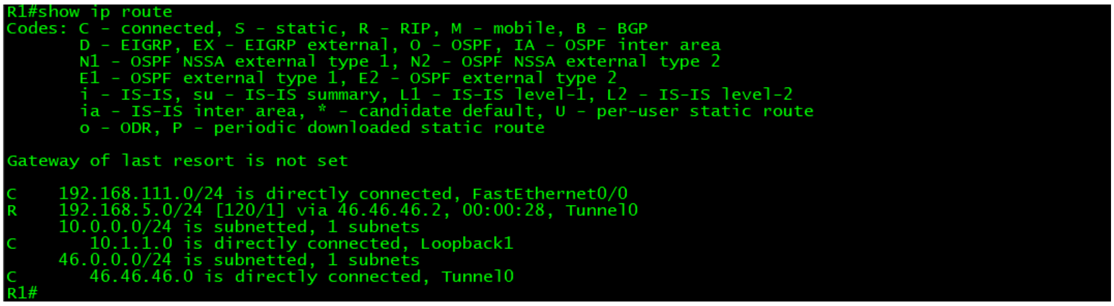
The route table on NR300/NR500, it had been learned the subnet from cisco via rip, as below:



Route Table Information

Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	100	wan
2	10.1.1.0	255.255.255.0	46.46.46.1	20	gretun1
3	46.46.46.0	255.255.255.0	0.0.0.0	0	gretun1
4	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
5	192.168.111.0	255.255.255.0	0.0.0.0	0	wan

The route table on cisco, it had been learned the subnet from NR300/NR500 via rip, as below:



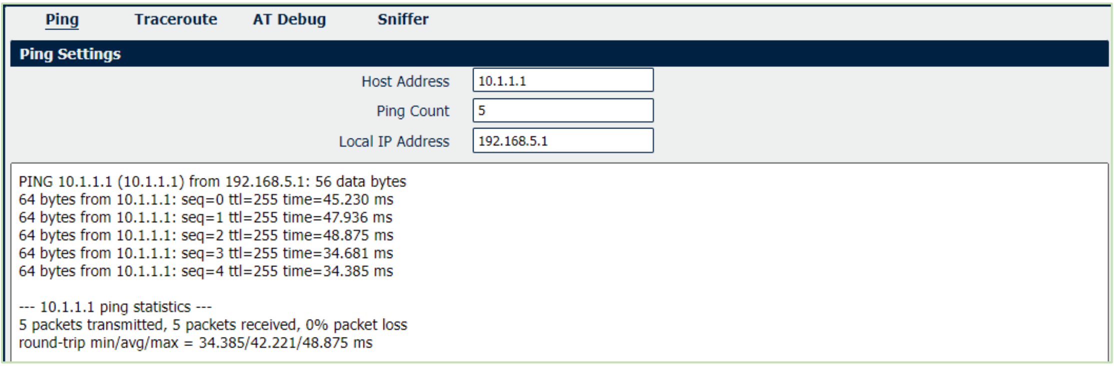
```
R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.111.0/24 is directly connected, FastEthernet0/0
R    192.168.5.0/24 [120/1] via 46.46.46.2, 00:00:28, Tunnel0
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback1
     46.0.0.0/24 is subnetted, 1 subnets
C       46.46.46.0 is directly connected, Tunnel0
R1#
```

5. Testing

NR500/NR300 is able to ping the subnet of cisco successfully, as below:



Host Address: 10.1.1.1

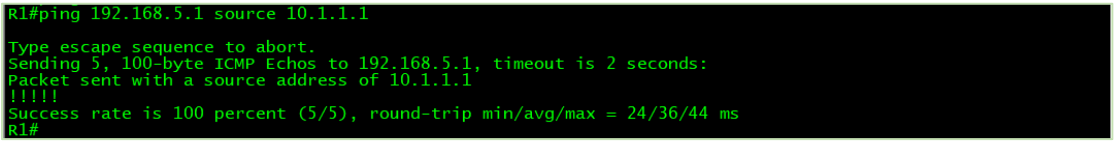
Ping Count: 5

Local IP Address: 192.168.5.1

```
PING 10.1.1.1 (10.1.1.1) from 192.168.5.1: 56 data bytes
64 bytes from 10.1.1.1: seq=0 ttl=255 time=45.230 ms
64 bytes from 10.1.1.1: seq=1 ttl=255 time=47.936 ms
64 bytes from 10.1.1.1: seq=2 ttl=255 time=48.875 ms
64 bytes from 10.1.1.1: seq=3 ttl=255 time=34.681 ms
64 bytes from 10.1.1.1: seq=4 ttl=255 time=34.385 ms

--- 10.1.1.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 34.385/42.221/48.875 ms
```

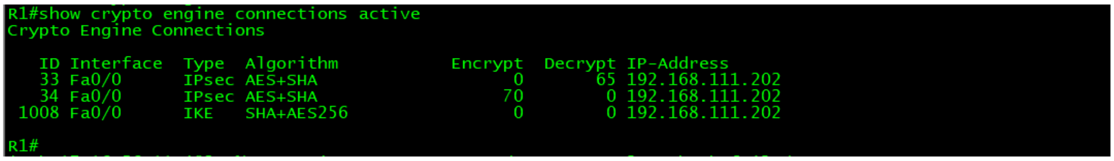
Cisco is able to ping the subnet of NR500/NR300 successfully, as below:



```
R1#ping 192.168.5.1 source 10.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
Packet sent with a source address of 10.1.1.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/36/44 ms
R1#
```

The data go through the VPN tunnel had been encrypted, as below:



```
R1#show crypto engine connections active
Crypto Engine Connections

   ID Interface  Type  Algorithm           Encrypt  Decrypt IP-Address
   33 Fa0/0      IPsec AES+SHA                   0       65 192.168.111.202
   34 Fa0/0      IPsec AES+SHA                  70        0 192.168.111.202
 1008 Fa0/0      IKE   SHA+AES256                0        0 192.168.111.202

R1#
```

Test successfully.