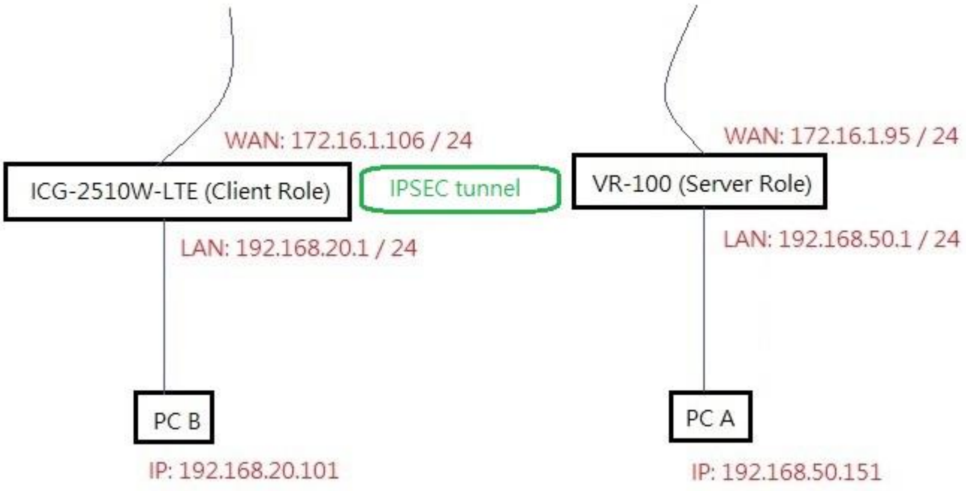
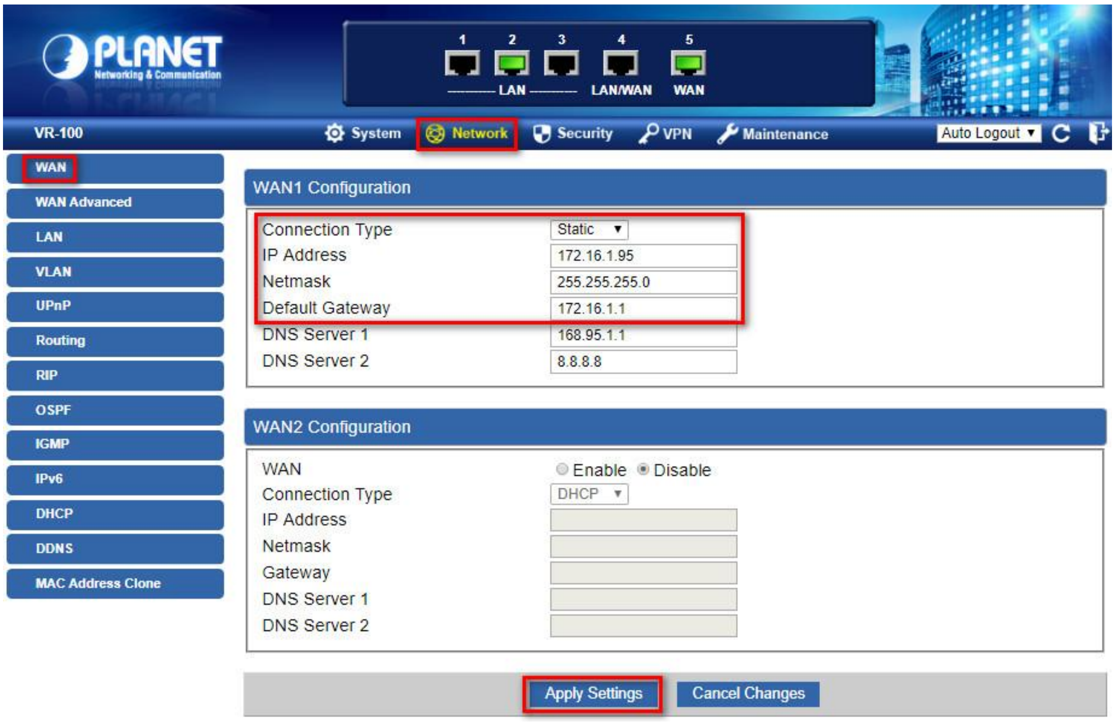
Establish a IPSEC VPN between VR-100 and ICG-2510W-LTE. VR-100 as the VPN Server, ICG-2510W-LTE as the VPN Client.

Topology:



Follow the following steps for setting up VPN server: (VR-100)

1. WAN Configuration
   a. Go to the **Network** -> **WAN** page.
   b. Select **Connection Type** as Static
   c. Input the **IP Address** you use.
   d. Click **Apply Settings** button to save changes.



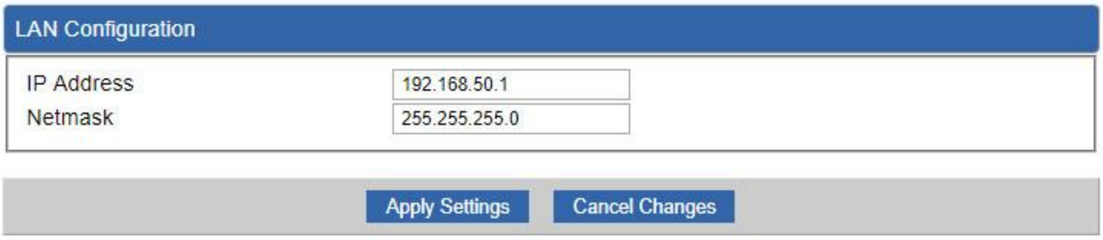
WAN1 Configuration

Connection Type	Static
IP Address	172.16.1.95
Netmask	255.255.255.0
Default Gateway	172.16.1.1
DNS Server 1	168.95.1.1
DNS Server 2	8.8.8.8

WAN2 Configuration

WAN	○ Enable ● Disable
Connection Type	DHCP
IP Address	
Netmask	
Gateway	
DNS Server 1	
DNS Server 2	

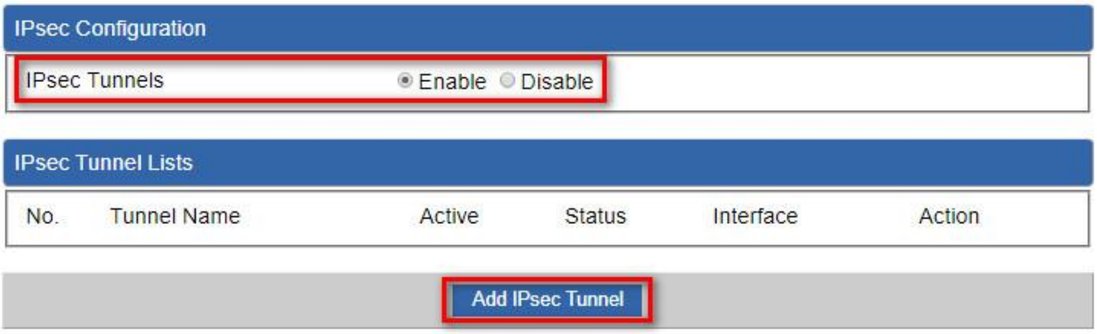
2. LAN Configuration
    a. Go to the **Network** -> **LAN** page.
    b. Input the **IP Address** and **Netmask**.



LAN Configuration

IP Address	192.168.50.1
Netmask	255.255.255.0

3. VPN Configuration
    a. Go to the **VPN** -> **IPsec** page.
    b. Set the **IPsec Tunnels** as enable.
    c. Click **Add IPsec Tunnel** button to add a tunnel



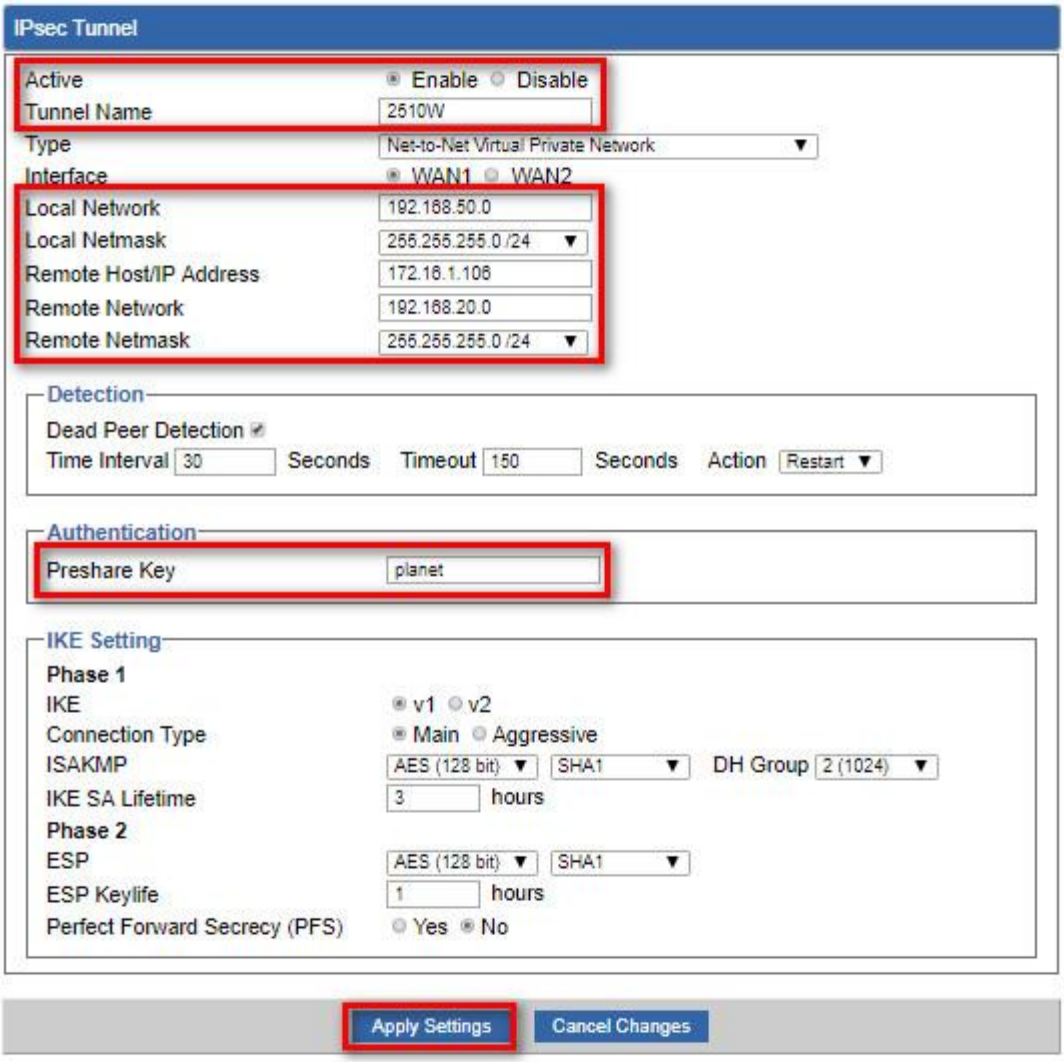
IPsec Configuration

IPsec Tunnels ● Enable ○ Disable

IPsec Tunnel Lists

No.	Tunnel Name	Active	Status	Interface	Action

    d. Set the **Active** as enable, and input the **Tunnel Name**.
    e. Input the **Local Network** and **Netmask** as the router’s LAN IP address.
    f. Input the **Remote Host/IP Address** as client router’s WAN IP address.
    g. Input the **Remote Network and Netmask** as client router’s LAN IP address.
    h. Input the **Preshare Key** as the same as the one set on both router.
    i. Click **Apply Settings** button to save changes.



IPsec Tunnel

Active	● Enable ○ Disable
Tunnel Name	2510W
Type	Net-to-Net Virtual Private Network ▼
Interface	● WAN1 ○ WAN2
Local Network	192.168.50.0
Local Netmask	255.255.255.0 /24 ▼
Remote Host/IP Address	172.16.1.106
Remote Network	192.168.20.0
Remote Netmask	255.255.255.0 /24 ▼

Detection

Dead Peer Detection ☑

Time Interval 30 Seconds Timeout 150 Seconds Action Restart ▼

Authentication

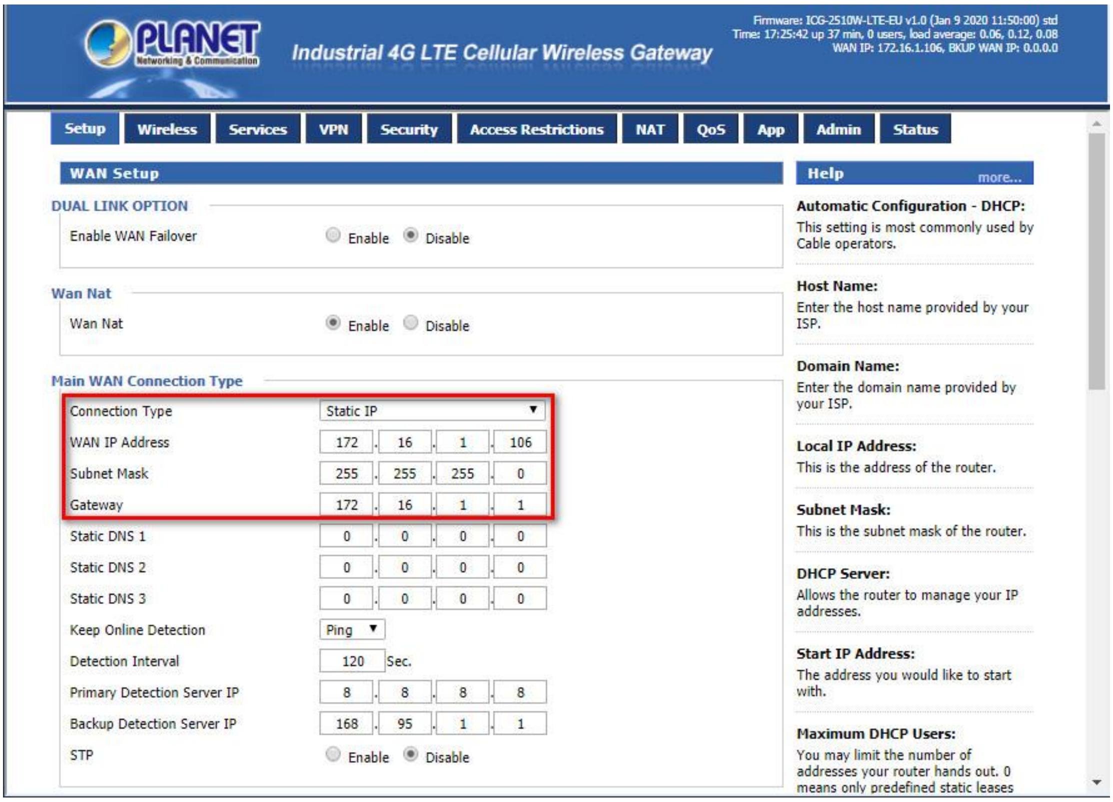
Preshare Key planet

IKE Setting

Phase 1	
IKE	● v1 ○ v2
Connection Type	● Main ○ Aggressive
ISAKMP	AES (128 bit) ▼ SHA1 ▼ DH Group 2 (1024) ▼
IKE SA Lifetime	3 hours
Phase 2	
ESP	AES (128 bit) ▼ SHA1 ▼
ESP Keylife	1 hours
Perfect Forward Secrecy (PFS)	○ Yes ● No

Follow the following steps for setting up VPN Client: (ICG-2510W-LTE)

1. WAN and LAN Configuration
   a. Go to the **Setup** -> **Basic Setup** page -> Main WAN Connection Type.
   b. Select **Connection Type** as Static IP
   c. Input the **WAN IP Address** you use.



Firmware: ICG-2510W-LTE-EU v1.0 (Jan 9 2020 11:50:00) std
Time: 17:25:42 up 37 min, 0 users, load average: 0.06, 0.12, 0.08
WAN IP: 172.16.1.106, BKUP WAN IP: 0.0.0.0

WAN Setup

DUAL LINK OPTION

Enable WAN Failover ○ Enable ● Disable

Wan Nat

Wan Nat ● Enable ○ Disable

Main WAN Connection Type

Connection Type	Static IP
WAN IP Address	172 . 16 . 1 . 106
Subnet Mask	255 . 255 . 255 . 0
Gateway	172 . 16 . 1 . 1
Static DNS 1	0 . 0 . 0 . 0
Static DNS 2	0 . 0 . 0 . 0
Static DNS 3	0 . 0 . 0 . 0
Keep Online Detection	Ping
Detection Interval	120 Sec.
Primary Detection Server IP	8 . 8 . 8 . 8
Backup Detection Server IP	168 . 95 . 1 . 1
STP	○ Enable ● Disable

Help

Automatic Configuration - DHCP:
This setting is most commonly used by Cable operators.

Host Name:
Enter the host name provided by your ISP.

Domain Name:
Enter the domain name provided by your ISP.

Local IP Address:
This is the address of the router.

Subnet Mask:
This is the subnet mask of the router.

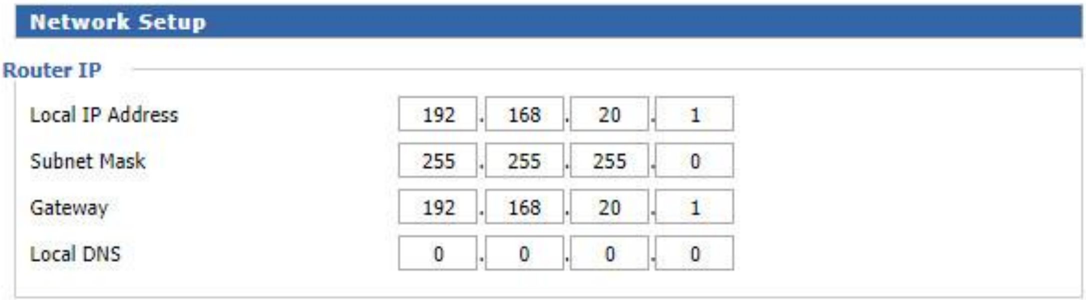
DHCP Server:
Allows the router to manage your IP addresses.

Start IP Address:
The address you would like to start with.

Maximum DHCP Users:
You may limit the number of addresses your router hands out. 0 means only predefined static leases

d. Go to the **Router IP**.

e. Input the **Local IP Address**, **Subnet Mask** and **Gateway**.



Network Setup

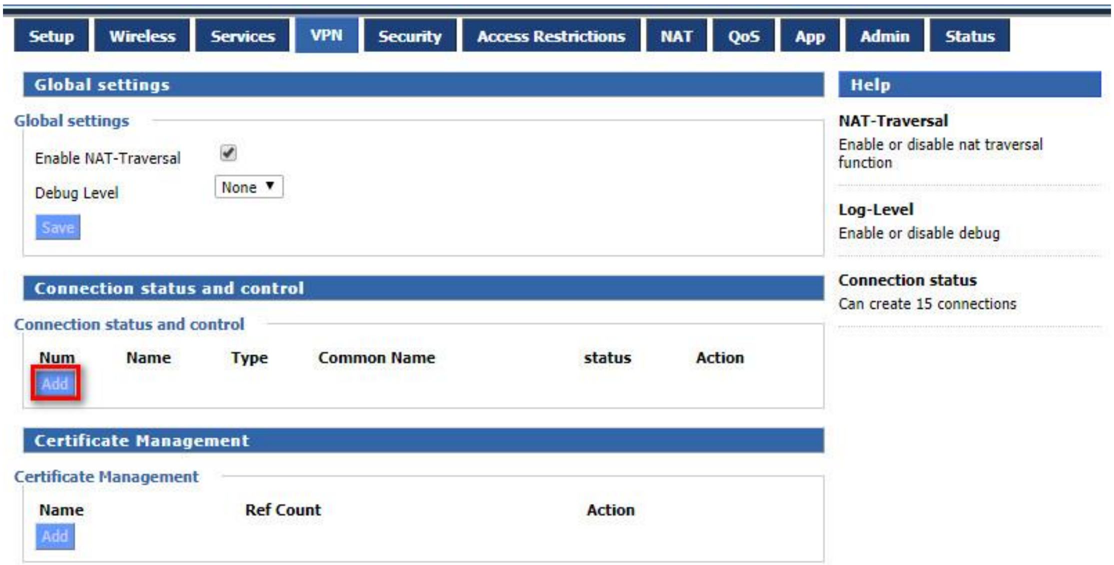
Router IP

Local IP Address	192 . 168 . 20 . 1
Subnet Mask	255 . 255 . 255 . 0
Gateway	192 . 168 . 20 . 1
Local DNS	0 . 0 . 0 . 0

2. VPN Configuration

a. Go to the **VPN** -> **IPSEC** page.

b. Click **Add** button to add a VPN profile.



Global settings

Global settings

Enable NAT-Traversal ☑

Debug Level: None

Connection status and control

Connection status and control

Num	Name	Type	Common Name	status	Action

Certificate Management

Certificate Management

Name	Ref Count	Action

Help

NAT-Traversal
Enable or disable nat traversal function

Log-Level
Enable or disable debug

Connection status
Can create 15 connections

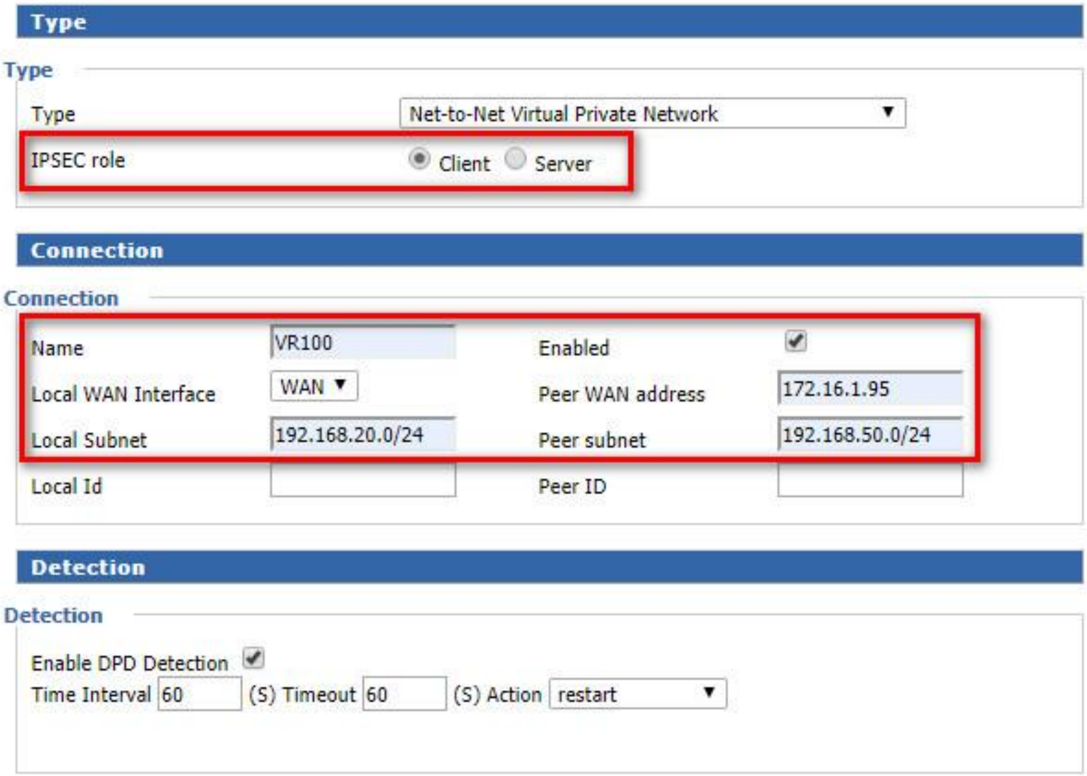
c. Set the **IPSEC role** as Client.

d. Input the **Name**, and check **Enabled**.

e. Input the **Local Subnet** as the router’s LAN IP address.

f. Input the **Peer WAN address** as the VPN Server router’s WAN IP address.

g. Input the **Peer Subnet** as the VPN Server router’s LAN IP address.



Type

Type

Type: Net-to-Net Virtual Private Network

IPSEC role: ● Client ○ Server

Connection

Connection

Name	VR100	Enabled	☑
Local WAN Interface	WAN	Peer WAN address	172.16.1.95
Local Subnet	192.168.20.0/24	Peer subnet	192.168.50.0/24
Local Id		Peer ID	

Detection

Detection

Enable DPD Detection ☑

Time Interval 60 (S) Timeout 60 (S) Action restart

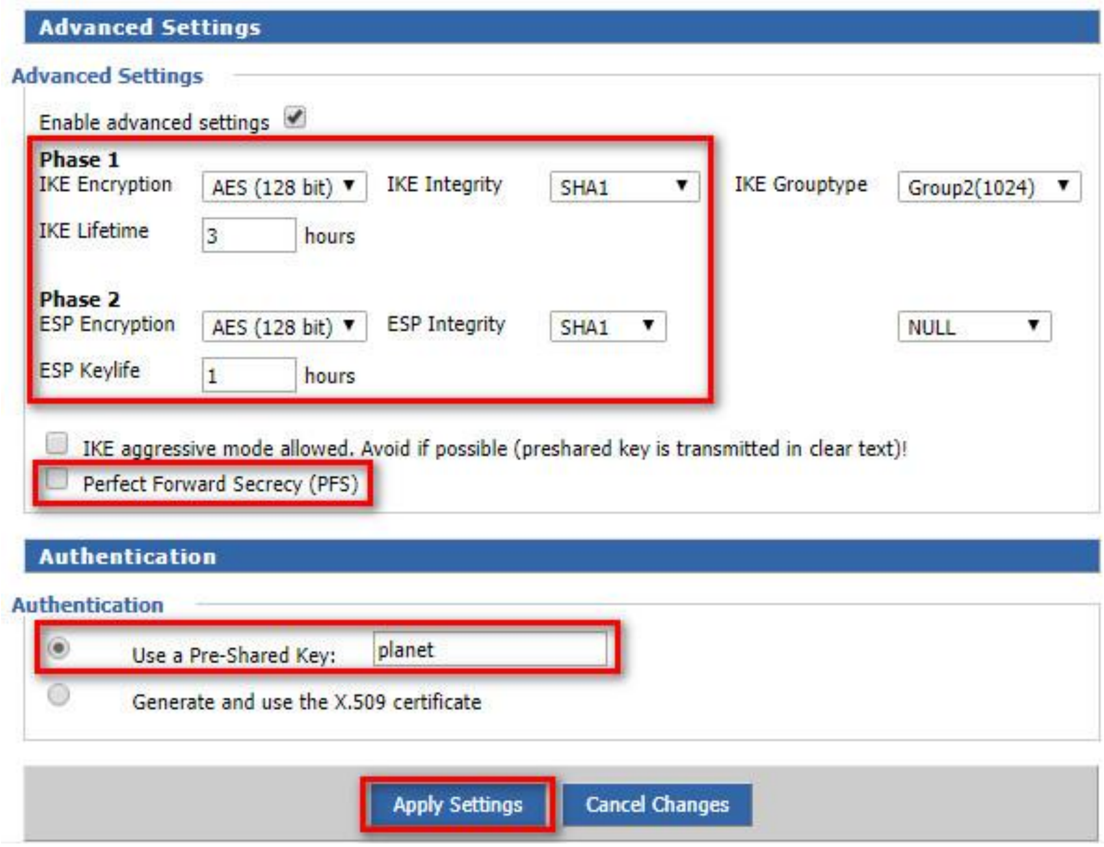
h. Set the Advanced Settings. **It should be** the same as the VPN server router. In this example, IKE Encryption is AES(128 bit), IKE Integrity is SHA1, ESP Encryption is

AES(128 bit), ESP Integrity is SHA1.

i. Disable Perfect Forward Secrecy(PFS)

j. Input **Pre-Shared Key**.

k. Click **Apply Settings** button to save changes.



Advanced Settings

Advanced Settings

Enable advanced settings ☑

Phase 1

IKE Encryption: AES (128 bit) ▼ IKE Integrity: SHA1 ▼ IKE Grouptype: Group2(1024) ▼

IKE Lifetime: 3 hours

Phase 2

ESP Encryption: AES (128 bit) ▼ ESP Integrity: SHA1 ▼ NULL ▼

ESP Keylife: 1 hours

□ IKE aggressive mode allowed. Avoid if possible (preshared key is transmitted in clear text)!

□ Perfect Forward Secrecy (PFS)

Authentication

Authentication

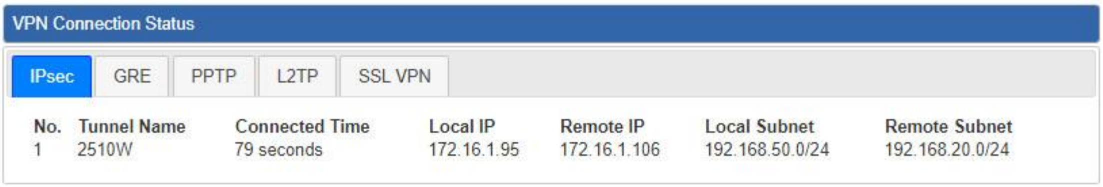
● Use a Pre-Shared Key: planet

○ Generate and use the X.509 certificate

VPN Connection Status

1. VPN Server

Go to the **VPN** -> **VPN Connection** -> **IPsec** page.

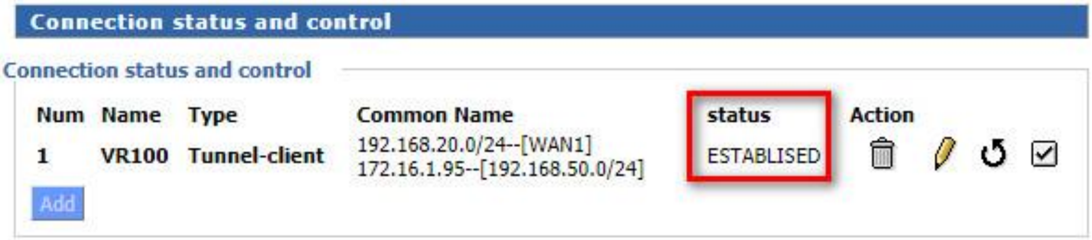


VPN Connection Status

No.	Tunnel Name	Connected Time	Local IP	Remote IP	Local Subnet	Remote Subnet
1	2510W	79 seconds	172.16.1.95	172.16.1.106	192.168.50.0/24	192.168.20.0/24

2. VPN Client

Go to the **VPN** -> **IPSEC** page.

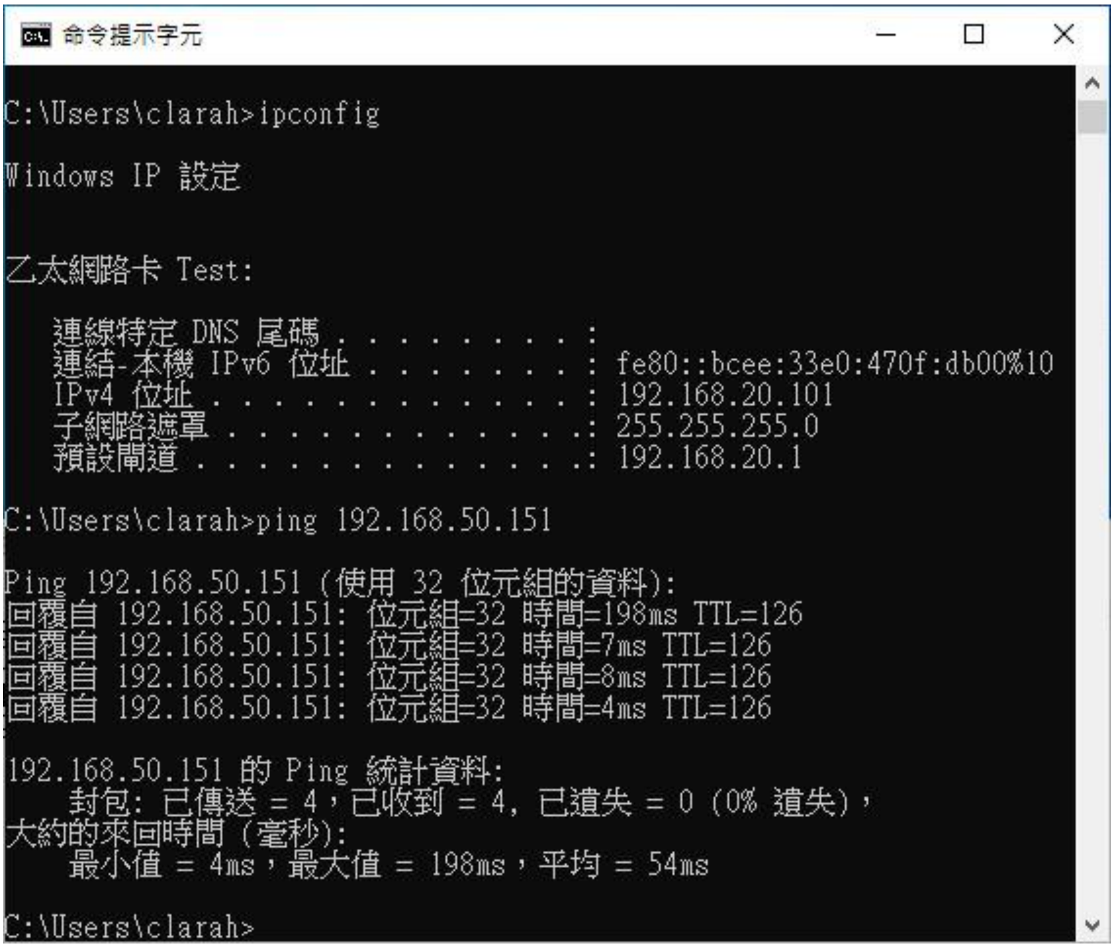


Connection status and control

Connection status and control

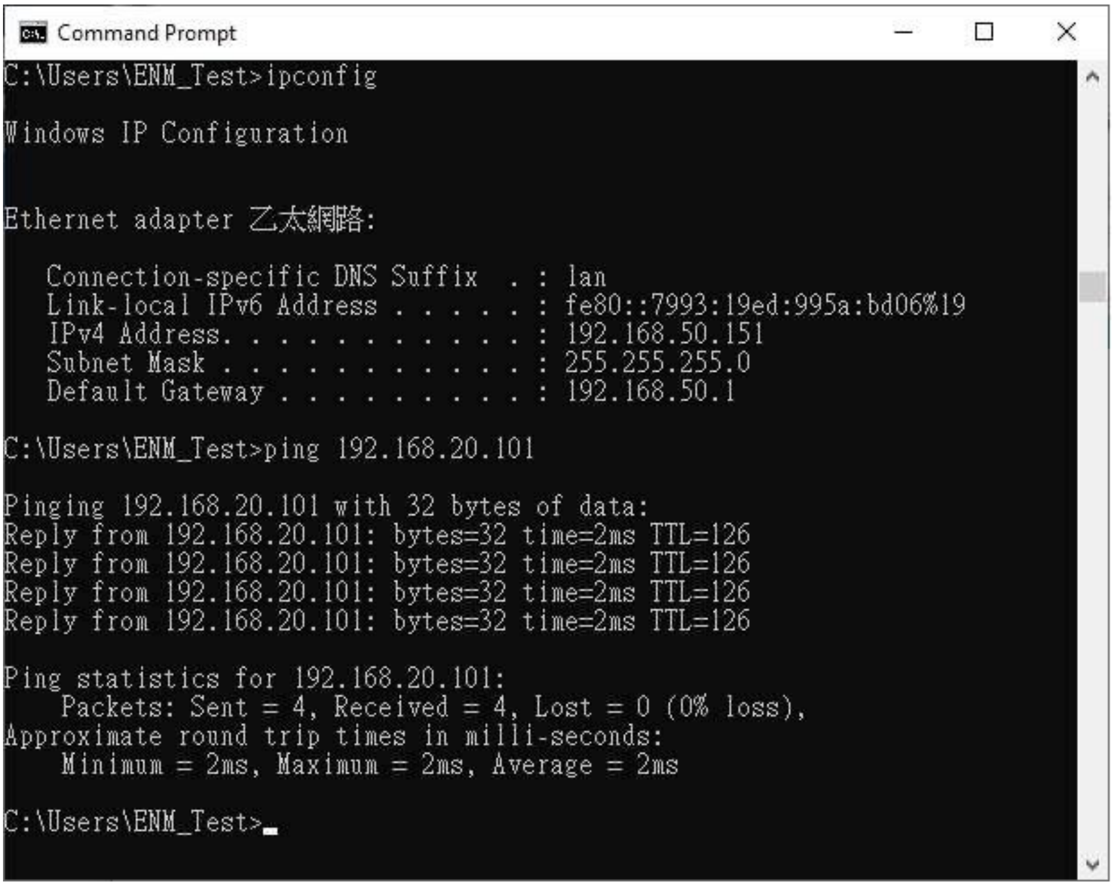
Num	Name	Type	Common Name	status	Action
1	VR100	Tunnel-client	192.168.20.0/24--[WAN1] 172.16.1.95--[192.168.50.0/24]	ESTABLISED	

3. PC B ping the PC A.



```
C:\Users\clarah>ipconfig

Windows IP 設定


乙太網路卡 Test:

   連線特定 DNS 尾碼 . . . . . . . . :
   連結-本機 IPv6 位址 . . . . . . . . : fe80::bcee:33e0:470f:db00%10
   IPv4 位址 . . . . . . . . . . . . : 192.168.20.101
   子網路遮罩 . . . . . . . . . . . .: 255.255.255.0
   預設閘道 . . . . . . . . . . . . .: 192.168.20.1

C:\Users\clarah>ping 192.168.50.151

Ping 192.168.50.151 (使用 32 位元組的資料):
回覆自 192.168.50.151: 位元組=32 時間=198ms TTL=126
回覆自 192.168.50.151: 位元組=32 時間=7ms TTL=126
回覆自 192.168.50.151: 位元組=32 時間=8ms TTL=126
回覆自 192.168.50.151: 位元組=32 時間=4ms TTL=126

192.168.50.151 的 Ping 統計資料:
    封包: 已傳送 = 4，已收到 = 4, 已遺失 = 0 (0% 遺失)，
大約的來回時間 (毫秒):
    最小值 = 4ms，最大值 = 198ms，平均 = 54ms

C:\Users\clarah>
```

4. PC A ping the PC B.



```
C:\Users\ENM_Test>ipconfig

Windows IP Configuration


Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::7993:19ed:995a:bd06%19
   IPv4 Address. . . . . . . . . . . : 192.168.50.151
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.50.1

C:\Users\ENM_Test>ping 192.168.20.101

Pinging 192.168.20.101 with 32 bytes of data:
Reply from 192.168.20.101: bytes=32 time=2ms TTL=126
Reply from 192.168.20.101: bytes=32 time=2ms TTL=126
Reply from 192.168.20.101: bytes=32 time=2ms TTL=126
Reply from 192.168.20.101: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.20.101:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 2ms, Average = 2ms

C:\Users\ENM_Test>
```