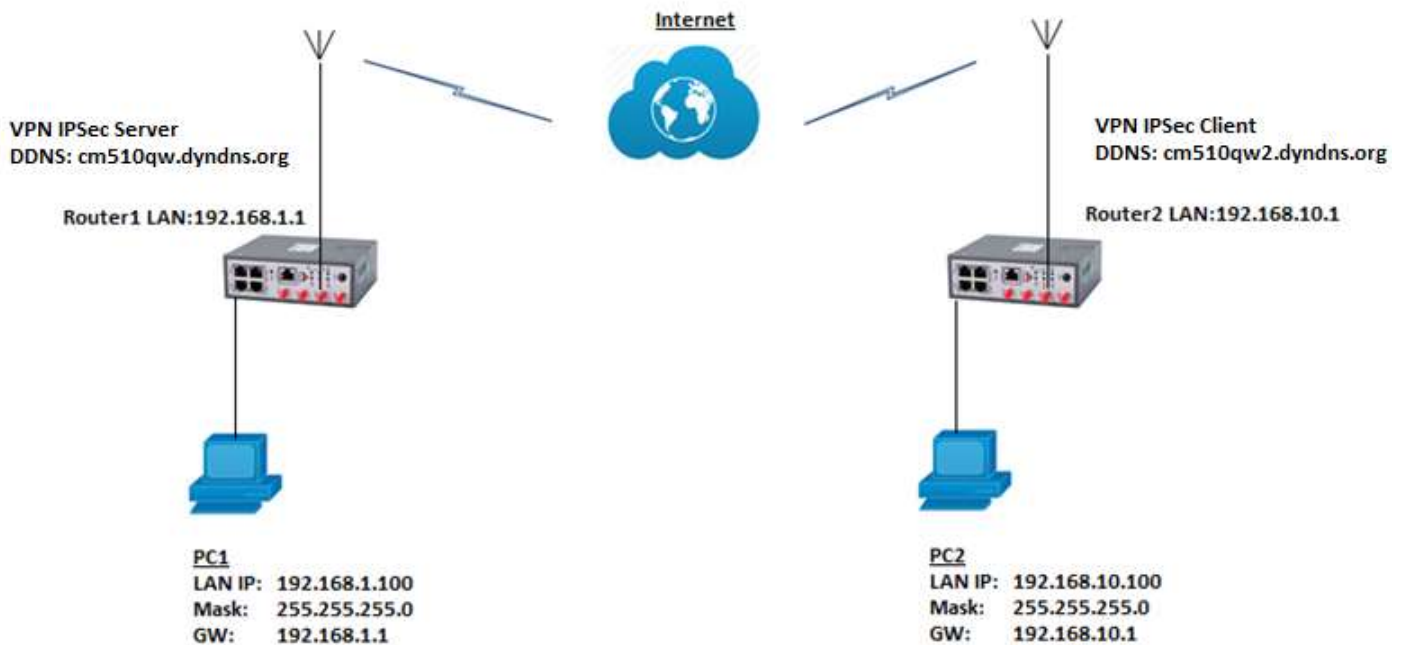


## How to configure VPN IPSec on a Comset CM510Q-W

Network Topology:

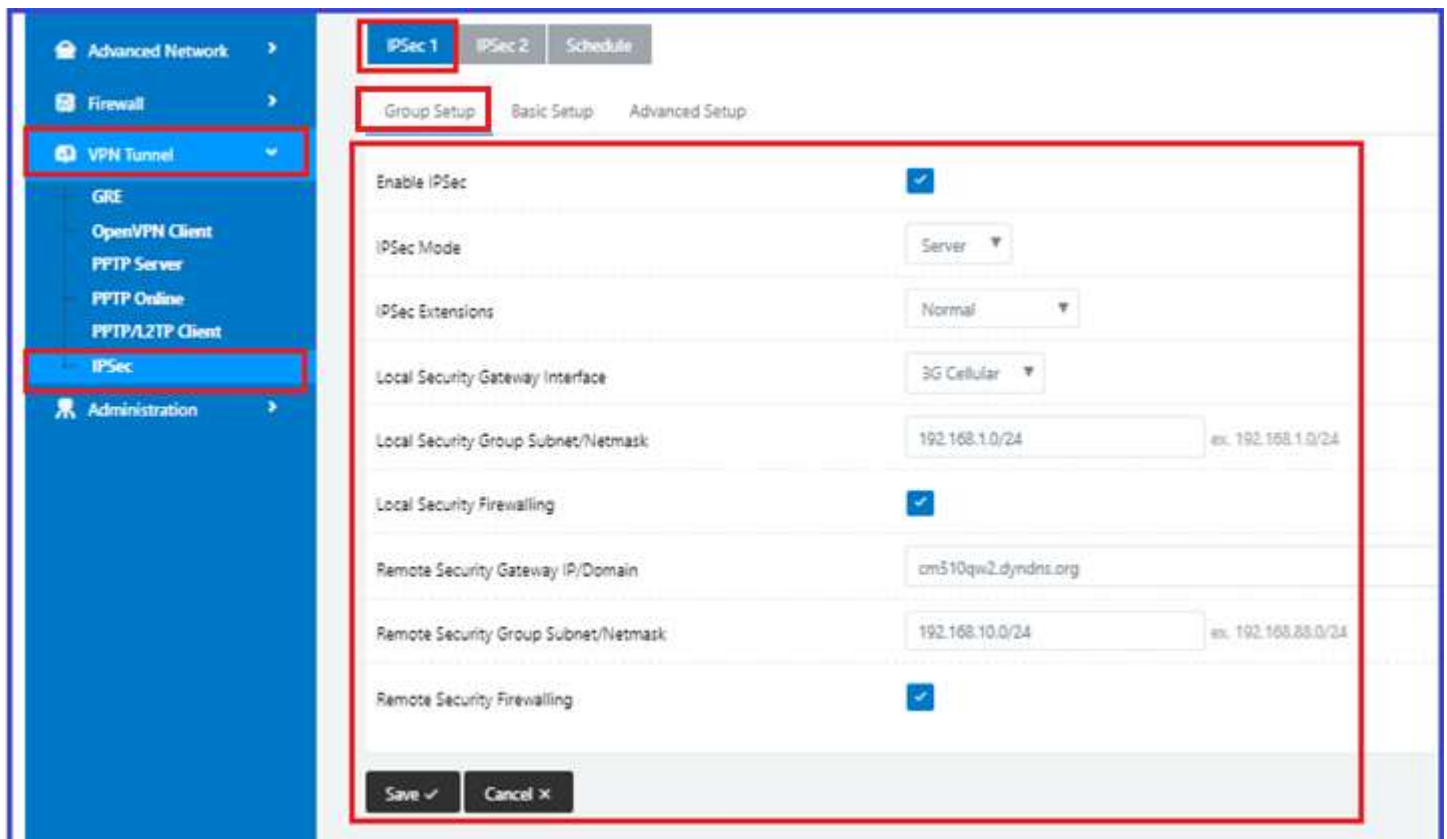


To configure VPN IPSec on the CM510Q-W router, please configure the router with the correct APN that will provide you with a Public WAN IP address, such as **telstra.extranet** for a Telstra Data SIM. You need to ask your carrier to activate your SIM card with a Public WAN IP.

### VPN Server Side

- Go to VPN Tunnel -> IPSec1 -> Group Set-up. Set as below.
 

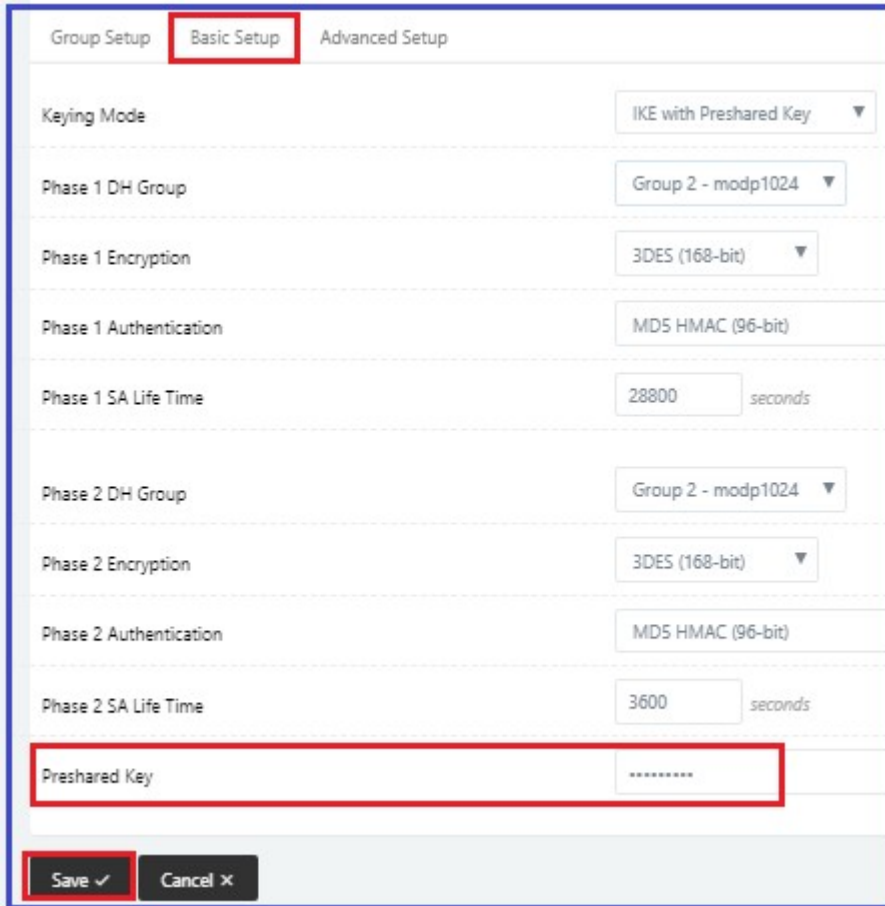
IPsec Mode:	<b>Server</b>
Local Security Group Subnet/Netmask:	<b>192.168.1.0/24</b>
Local Security Firewalling:	<b>Enabled</b>
Remote Security Gateway:	<b>cm510qw2.dyndns.org</b>
Remote Security Firewalling:	<b>192.168.10.0/24</b>
Remote Security Firewalling:	<b>Enabled</b>



2. Click on Basic Set-up.

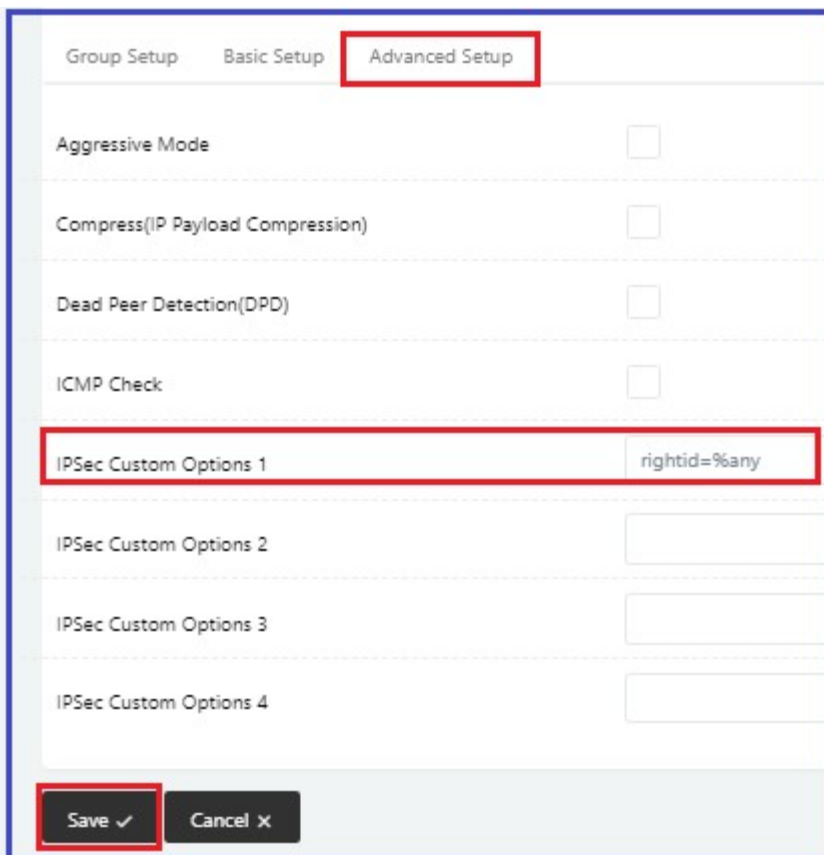
Set default Phase1 and Phase2 Groups such as Encryption, Authentication, Lifetime.  
Set Pre-shared key for VPN IPsec.

**Note:** Pre-shared key should be the same on both routers to establish connection.



3. Click on Advanced Set-up and set IPsec Custom Options 1

IPsec Custom Options 1: **rightid=%any**



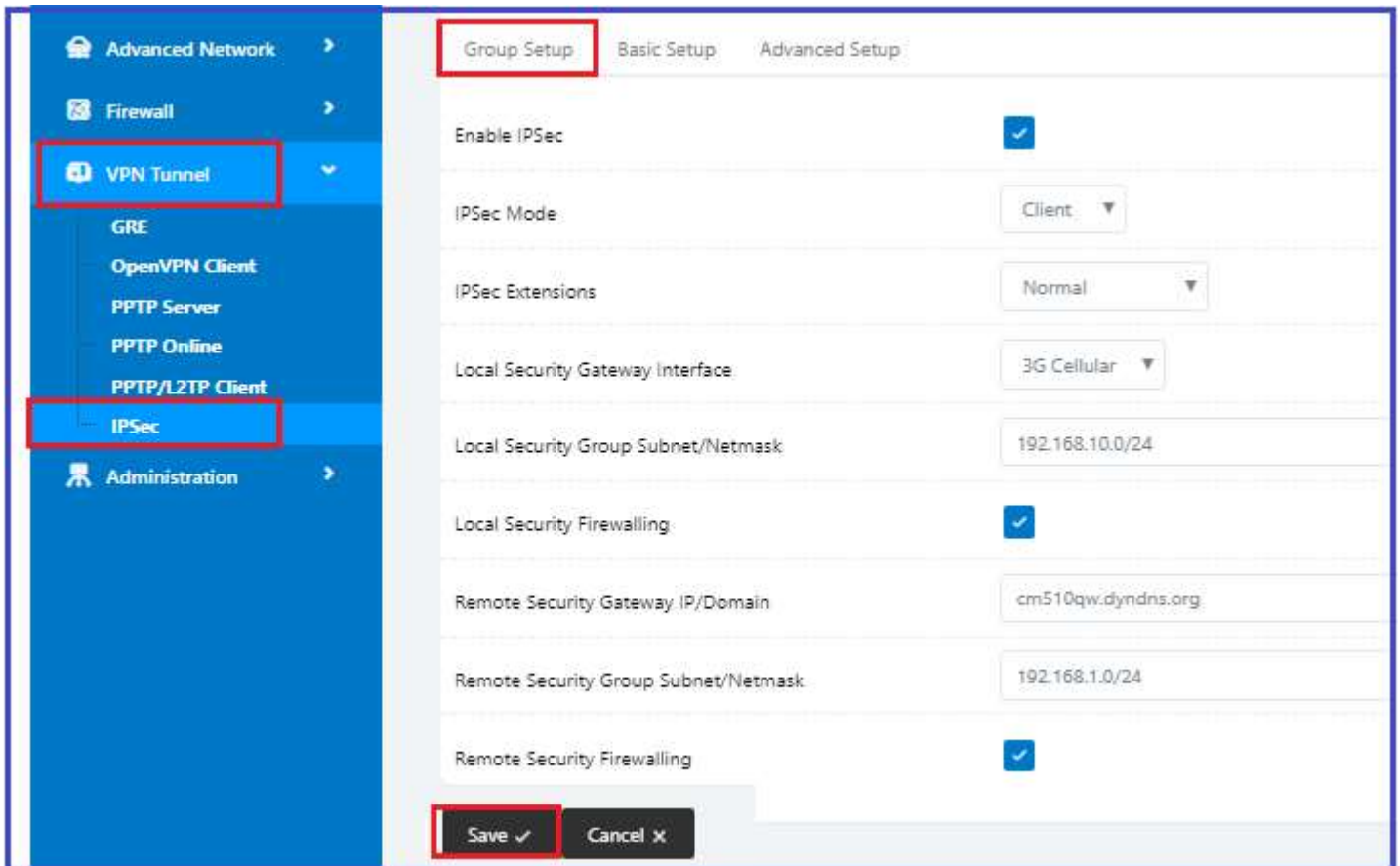
4. Go to Administration -> Admin Access -> **Uncheck** "Block WAN Ping" and Save apply. See below.



## IPSec Client Side

1. Go to VPN Tunnel -> IPSec -> Group Setup

IPsec Mode: **Client**  
Local Security Group Subnet/Netmask: **192.168.10.0/24**  
Local Security Firewalling: **Enabled**  
Remote Security Gateway: **cm510qw.dyndns.org**  
Remote Security Firewalling: **192.168.1.0/24**  
Remote Security Firewalling: **Enabled**



The screenshot shows the 'Group Setup' configuration page for an IPSec client. The left sidebar has 'VPN Tunnel' and 'IPSec' highlighted with red boxes. The main content area has three tabs: 'Group Setup' (selected), 'Basic Setup', and 'Advanced Setup'. The configuration fields are as follows:

Field	Value
Enable IPSec	<input checked="" type="checkbox"/>
IPSec Mode	Client
IPSec Extensions	Normal
Local Security Gateway Interface	3G Cellular
Local Security Group Subnet/Netmask	192.168.10.0/24
Local Security Firewalling	<input checked="" type="checkbox"/>
Remote Security Gateway IP/Domain	cm510qw.dyndns.org
Remote Security Group Subnet/Netmask	192.168.1.0/24
Remote Security Firewalling	<input checked="" type="checkbox"/>

At the bottom, there are 'Save' and 'Cancel' buttons, both highlighted with red boxes.

2. Click on Basic Set-up.  
Set default Phase1 and Phase2 Groups such as Encryption, Authentication, Lifetime.  
Set Pre-shared key for VPN IPSec.  
**Note:** Pre-shared key should be the same on both routers to establish connection.

Group Setup **Basic Setup** Advanced Setup

Keying Mode: IKE with Preshared Key

Phase 1 DH Group: Group 2 - modp1024

Phase 1 Encryption: 3DES (168-bit)

Phase 1 Authentication: MD5 HMAC (96-bit)

Phase 1 SA Life Time: 28800 seconds

Phase 2 DH Group: Group 2 - modp1024

Phase 2 Encryption: 3DES (168-bit)

Phase 2 Authentication: MD5 HMAC (96-bit)

Phase 2 SA Life Time: 3600 seconds

Preshared Key: .....

Save ✓ Cancel ✕

3. Click on Advanced Set-up and set IPSec Custom Options 1  
IPSec Custom Options 1: **rightid=%any**

Group Setup Basic Setup **Advanced Setup**

Aggressive Mode:

Compress(IP Payload Compression):

Dead Peer Detection(DPD):

ICMP Check:

IPSec Custom Options 1: rightid=%any

IPSec Custom Options 2:

IPSec Custom Options 3:

IPSec Custom Options 4:

Save ✓ Cancel ✕

4. Go to Administration -> Admin Access -> **Uncheck** "Block WAN Ping" and Save apply. See below.

**Administration**

Identification

Time

**Admin Access**

Scheduled Robot

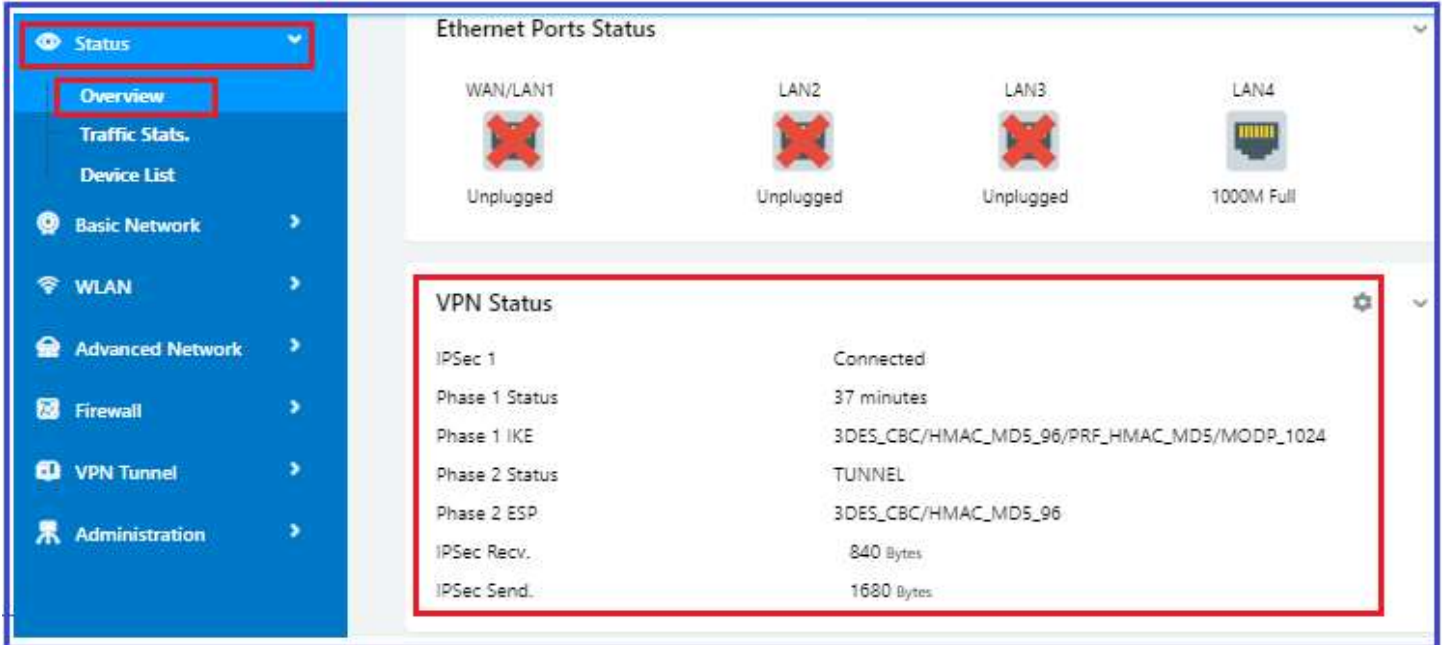
IP Address

Allow Wireless Access:

**Block WAN Ping:**

## Checking VPN IPSec Status and Testing VPN Tunnel.

1. Go to Status -> Overview -> VPN Status



The screenshot shows a network management interface. On the left is a navigation menu with 'Status' selected, and 'Overview' is highlighted. The main area is divided into two sections: 'Ethernet Ports Status' and 'VPN Status'. 'Ethernet Ports Status' shows WAN/LAN1, LAN2, and LAN3 as 'Unplugged' (indicated by red 'X' icons), and LAN4 as '1000M Full'. The 'VPN Status' section is highlighted with a red box and contains the following information:

Item	Status
IPSec 1	Connected
Phase 1 Status	37 minutes
Phase 1 IKE	3DES_CBC/HMAC_MD5_96/PRF_HMAC_MD5/MODP_1024
Phase 2 Status	TUNNEL
Phase 2 ESP	3DES_CBC/HMAC_MD5_96
IPSec Recv.	840 Bytes
IPSec Send.	1680 Bytes

2. Check Ping connection from PC1(192.168.1.100) behind the IPSec\_server to PC2(192.168.10.100) behind the IPSec\_client.

```
C:\Users\Tony>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::9c70:98fe:2b67:b3c8%15
    IPv4 Address. . . . . : 192.168.1.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.1
```

```
C:\Users\Tony>ping 192.168.10.100

Pinging 192.168.10.100 with 32 bytes of data:
Reply from 192.168.10.100: bytes=32 time=70ms TTL=126
Reply from 192.168.10.100: bytes=32 time=63ms TTL=126
Reply from 192.168.10.100: bytes=32 time=73ms TTL=126
Reply from 192.168.10.100: bytes=32 time=92ms TTL=126

Ping statistics for 192.168.10.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 63ms, Maximum = 92ms, Average = 74ms
```

3. Check Ping connection from PC2(192.168.10.100) behind the IPSec\_client to PC1(192.168.1.100) behind the IPSec\_server

```
Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    Link-local IPv6 Address . . . . . : fe80::9571:4168:f214:45c9%15
    IPv4 Address. . . . . : 192.168.10.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.10.1
```

```
C:\Users\A>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time=185ms TTL=126
Reply from 192.168.1.100: bytes=32 time=158ms TTL=126
Reply from 192.168.1.100: bytes=32 time=99ms TTL=126
Reply from 192.168.1.100: bytes=32 time=371ms TTL=126

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 99ms, Maximum = 371ms, Average = 203ms
```