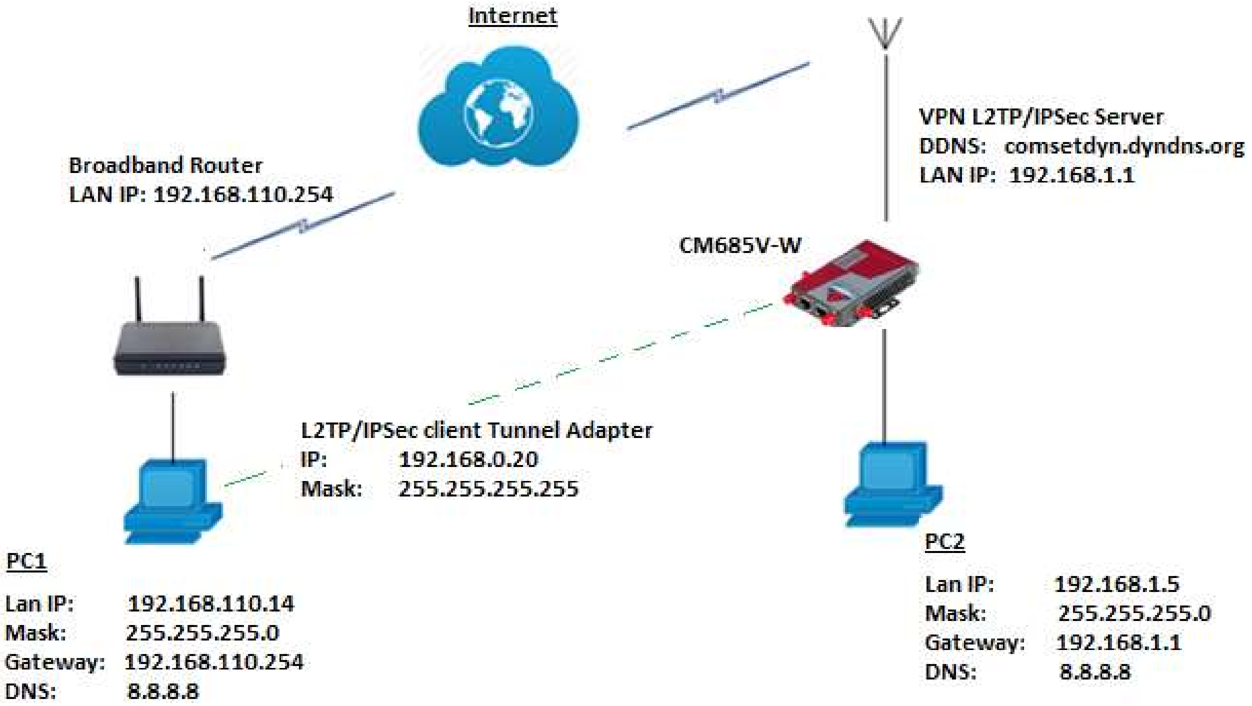
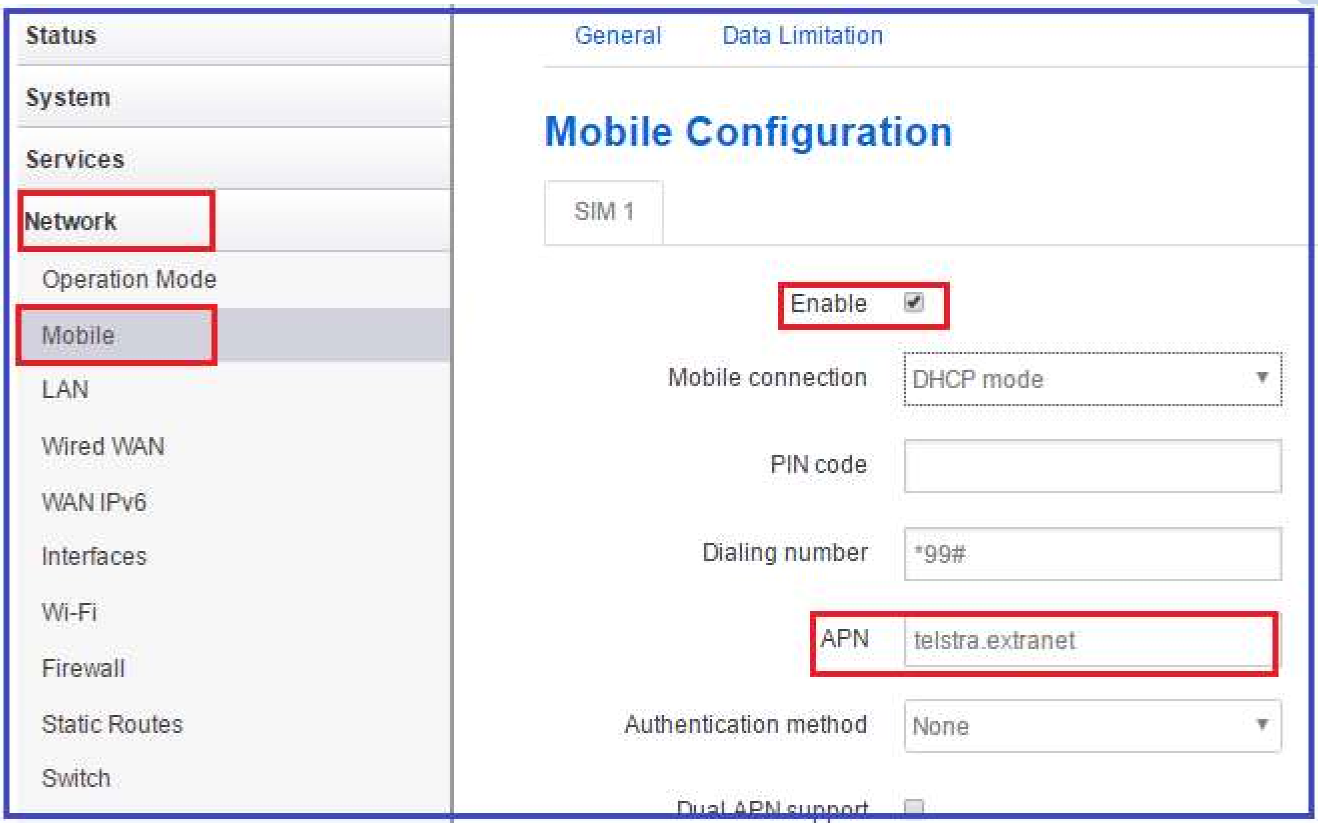
How to configure L2TP over IPSec on the Comset CM685V Router

Network Topology:



To configure VPN L2TP over IPSec on the Comset CM685V 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.

1. Configure APN settings for a Public WAN IP.
   For Telstra Data SIM, go to Network-> Mobile -> APN -> telstra.extranet.



Status

System

Services

Network

Operation Mode

Mobile

LAN

Wired WAN

WAN IPv6

Interfaces

Wi-Fi

Firewall

Static Routes

Switch

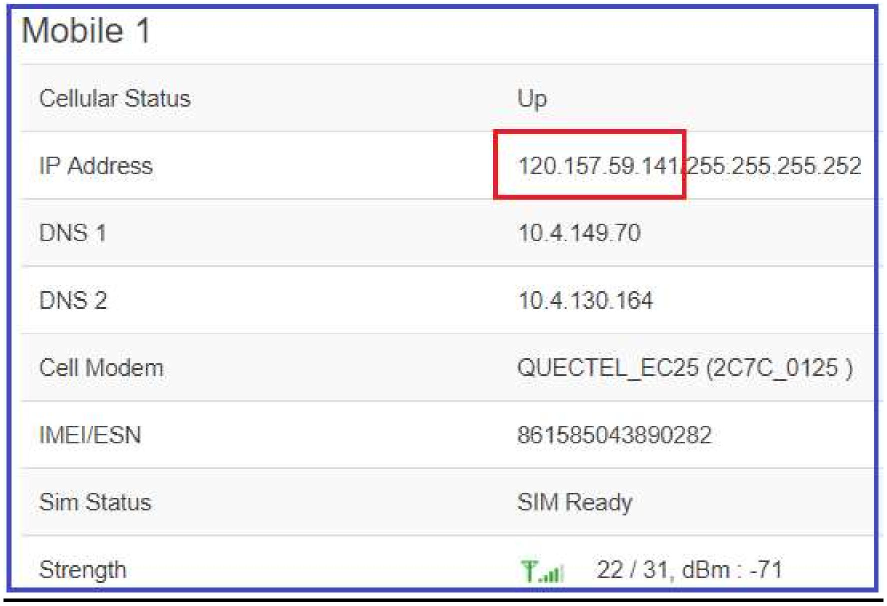
General | Data Limitation

Mobile Configuration

SIM 1

Enable	☑
Mobile connection	DHCP mode
PIN code	
Dialing number	*99#
APN	telstra.extranet
Authentication method	None
Dual APN support	□

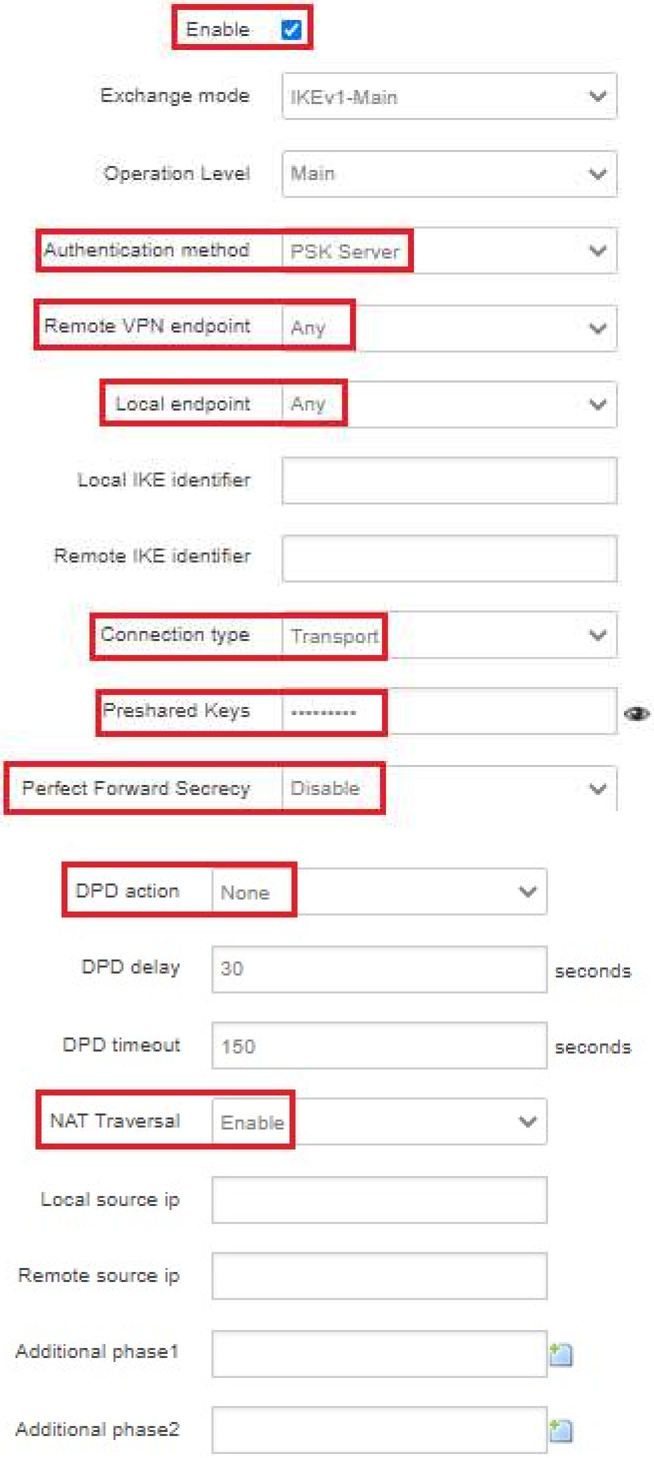
2. Go to the Status Page to check the WAN IP address. The WAN IP address in this example is 120.157.59.141. Use this WAN IP address on the L2TP/IPSec client settings.



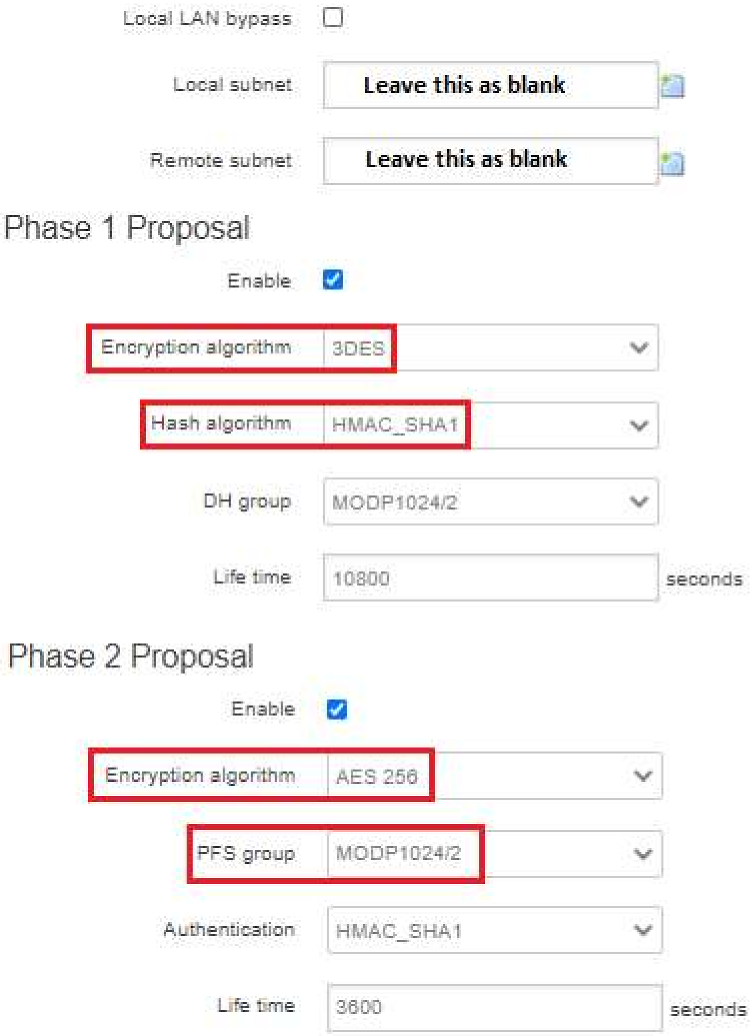
Mobile 1

Cellular Status	Up
IP Address	120.157.59.141/255.255.255.252
DNS 1	10.4.149.70
DNS 2	10.4.130.164
Cell Modem	QUECTEL_EC25 (2C7C_0125)
IMEI/ESN	861585043890282
Sim Status	SIM Ready
Strength	22 / 31, dBm : -71

3. Go to Services -> VPN -> IPSec-> and click on the Edit Button. Configure IPSec settings as shown below.



Enable	☑	
Exchange mode	IKEv1-Main	
Operation Level	Main	
Authentication method	PSK Server	
Remote VPN endpoint	Any	
Local endpoint	Any	
Local IKE identifier		
Remote IKE identifier		
Connection type	Transport	
Preshared Keys	·········	
Perfect Forward Secrecy	Disable	
DPD action	None	
DPD delay	30	seconds
DPD timeout	150	seconds
NAT Traversal	Enable	
Local source ip		
Remote source ip		
Additional phase1		
Additional phase2		



Local LAN bypass ☐

Local subnet: Leave this as blank

Remote subnet: Leave this as blank

Phase 1 Proposal

Enable ☑

Encryption algorithm: 3DES

Hash algorithm: HMAC_SHA1

DH group: MODP1024/2

Life time: 10800 seconds

Phase 2 Proposal

Enable ☑

Encryption algorithm: AES 256

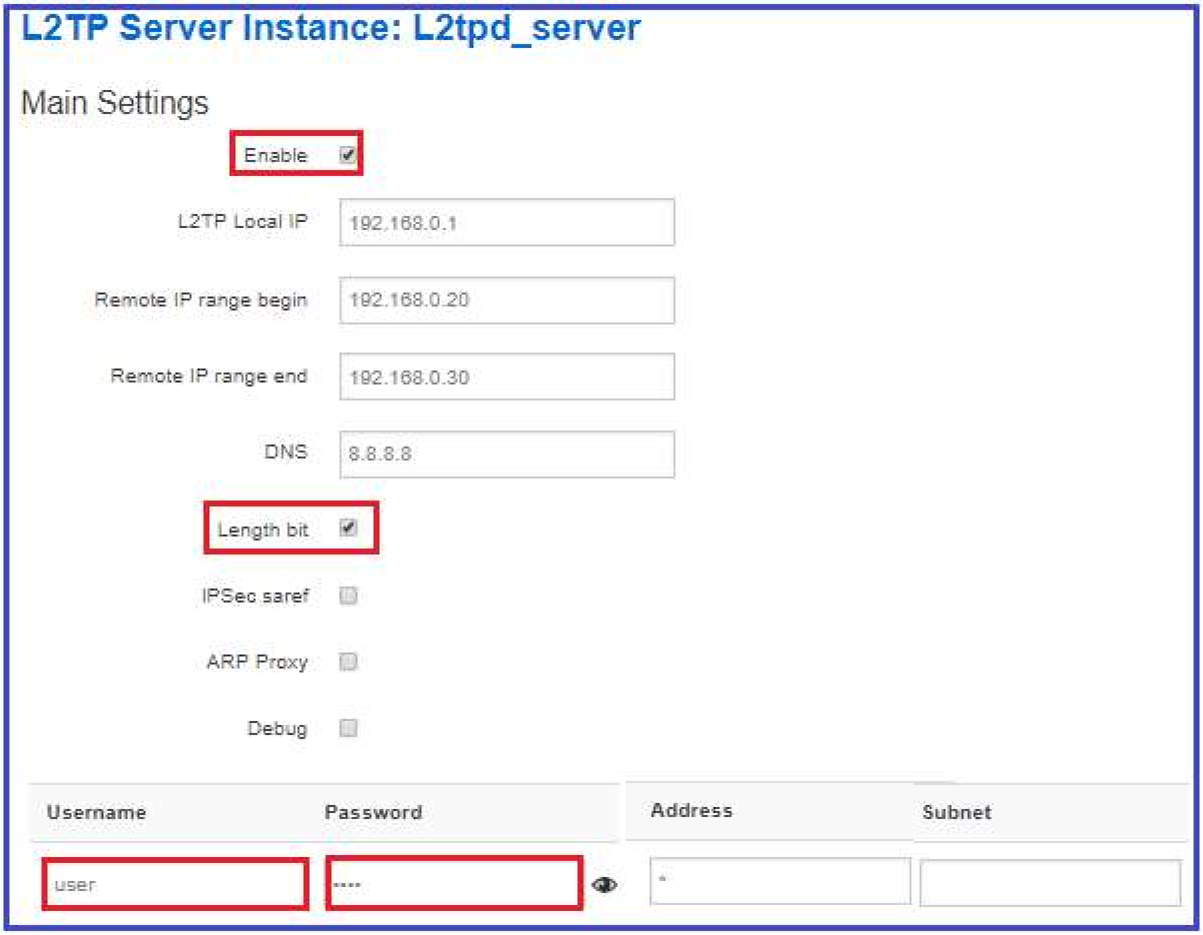
PFS group: MODP1024/2

Authentication: HMAC_SHA1

Life time: 3600 seconds

4. Click on “Save and Apply”.

5. Go to Services -> VPN -> L2TP-> and click on “Edit”. Configure the L2TP server as shown below.



L2TP Server Instance: L2tpd_server

Main Settings

Enable ☑

L2TP Local IP: 192.168.0.1

Remote IP range begin: 192.168.0.20

Remote IP range end: 192.168.0.30

DNS: 8.8.8.8

Length bit ☑

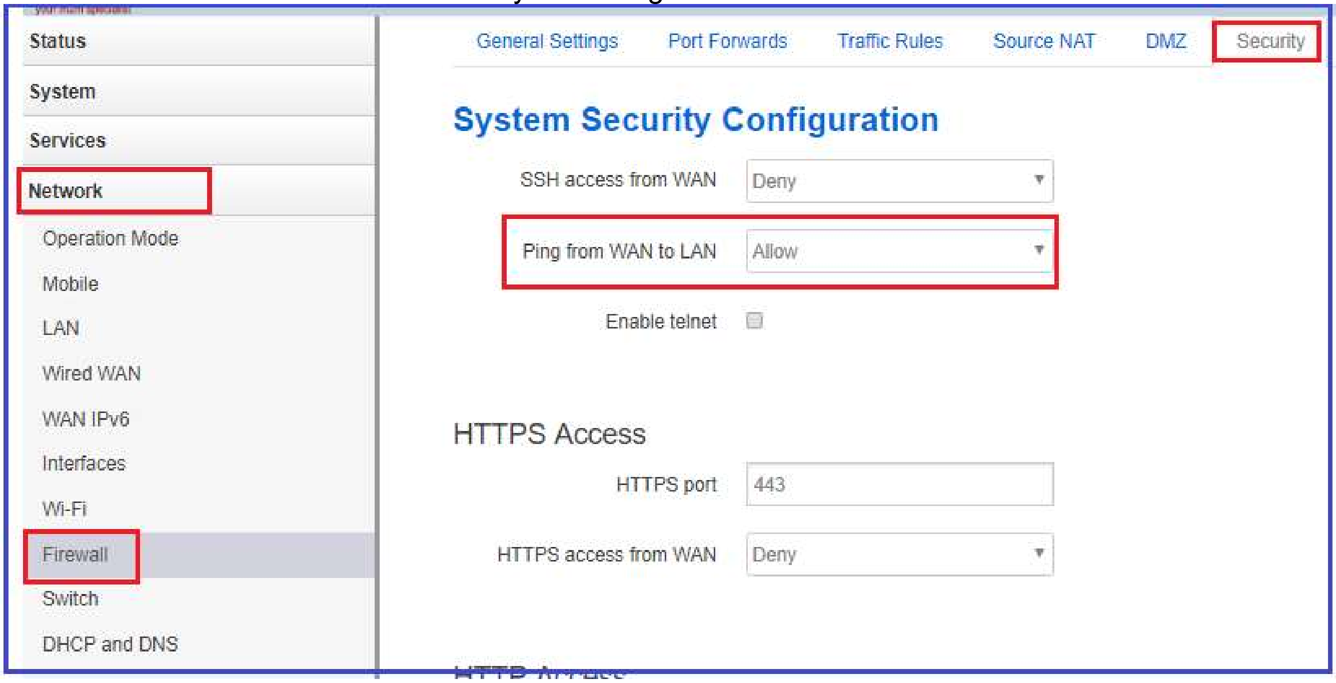
IPSec saref □

ARP Proxy □

Debug □

Username	Password	Address	Subnet
user	••••	*	

6. Allow “Ping from WAN to LAN” on the Firewall security page.
   Go to Network -> Firewall -> Security. Set “Ping from WAN to LAN” to “Allow”.



System Security Configuration

SSH access from WAN: Deny

Ping from WAN to LAN: Allow

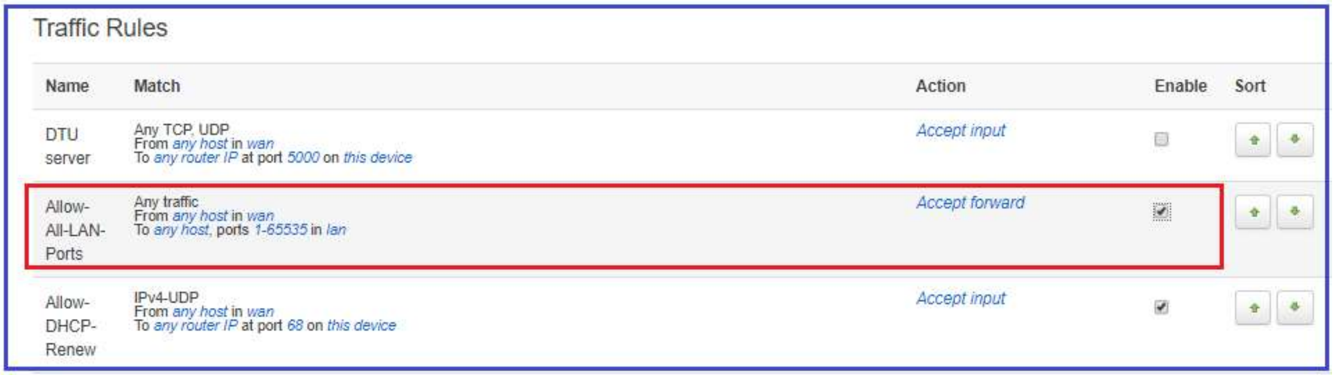
Enable telnet □

HTTPS Access

HTTPS port: 443

HTTPS access from WAN: Deny

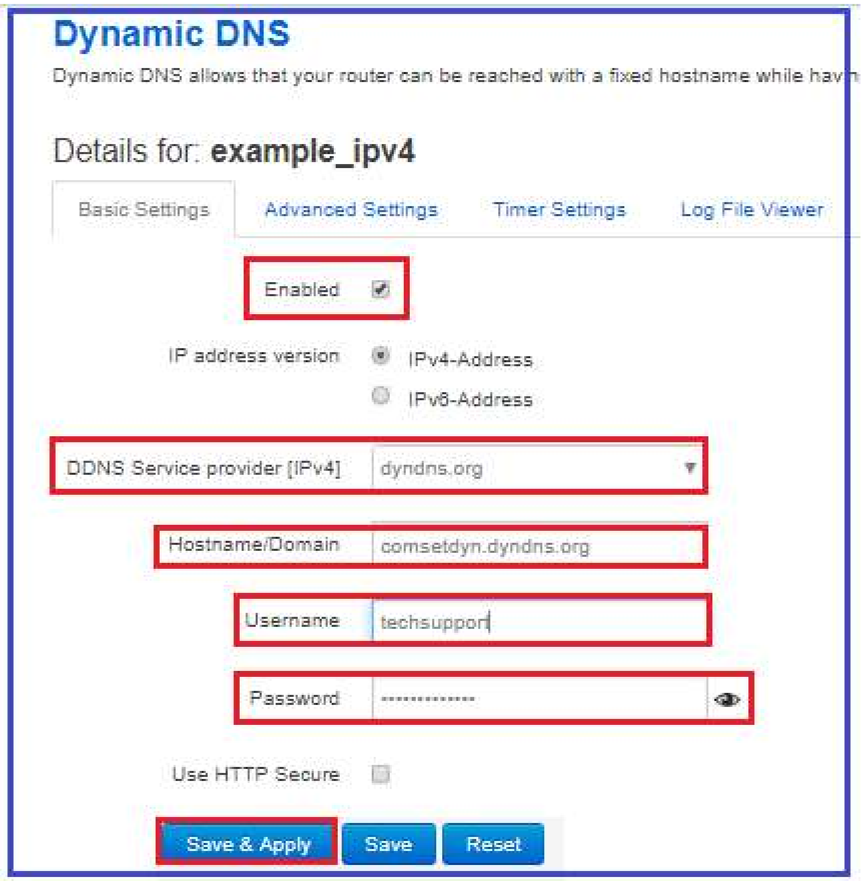
7. Go to Network-> Firewall-> Traffic Rules. Enable “Allow-ALL-LAN-Ports”.



Traffic Rules

Name	Match	Action	Enable	Sort
DTU server	Any TCP, UDP From *any host* in *wan* To *any router IP* at port *5000* on *this device*	*Accept input*	☐	↑ ↓
Allow-All-LAN-Ports	Any traffic From *any host* in *wan* To *any host*, ports *1-65535* in *lan*	*Accept forward*	☑	↑ ↓
Allow-DHCP-Renew	IPv4-UDP From *any host* in *wan* To *any router IP* at port *68* on *this device*	*Accept input*	☑	↑ ↓

8. Configure DDNS settings on the router.
Go to Services -> DDNS -> click Edit on IPv4.



Dynamic DNS

Dynamic DNS allows that your router can be reached with a fixed hostname while hav

Details for: **example_ipv4**

Enabled ☑

IP address version ● IPv4-Address ○ IPv6-Address

DDNS Service provider [IPv4]: dyndns.org

Hostname/Domain: comsetdyn.dyndns.org

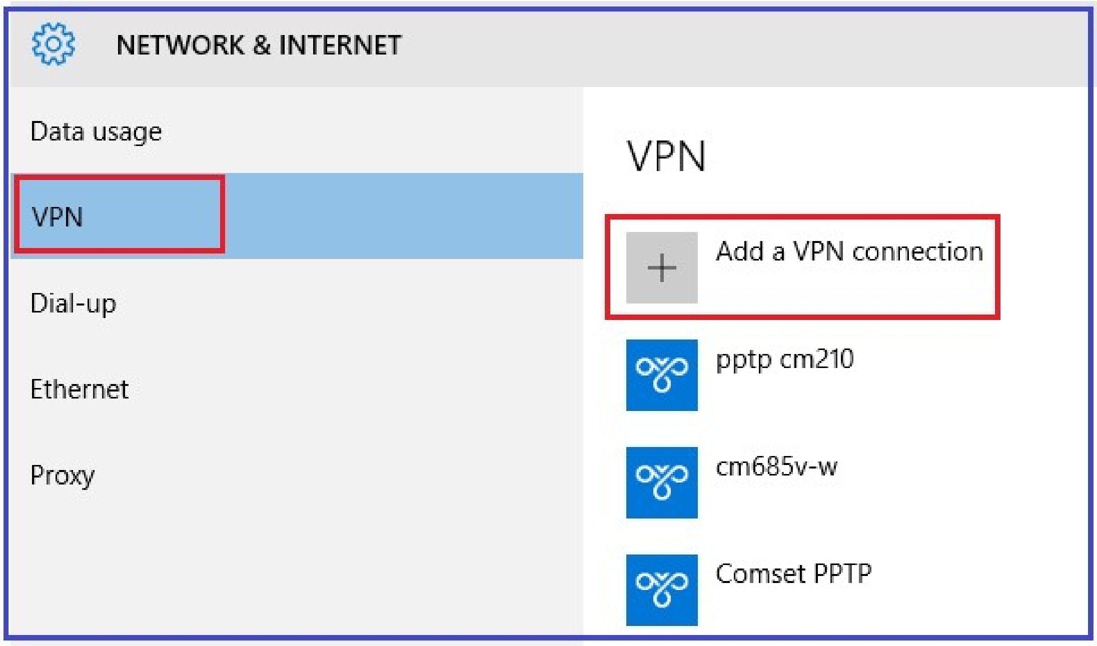
Username: techsuppor

Password: ••••••••••••••

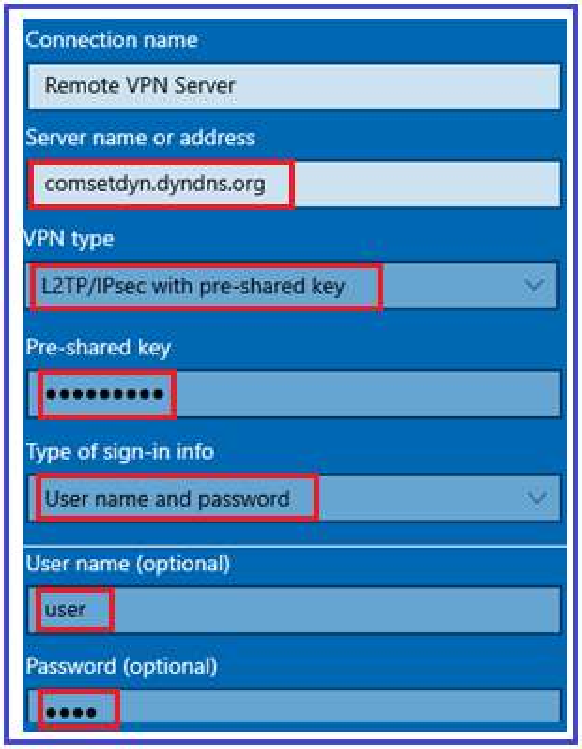
Use HTTP Secure ☐

On your Windows PC

1. Go to Network and Internet Settings -> VPN -> Add a VPN connection.



2. Set VPN Settings as below and click on the **Save** button.



Connection name
Remote VPN Server

Server name or address
comsetdyn.dyndns.org

VPN type
L2TP/IPsec with pre-shared key

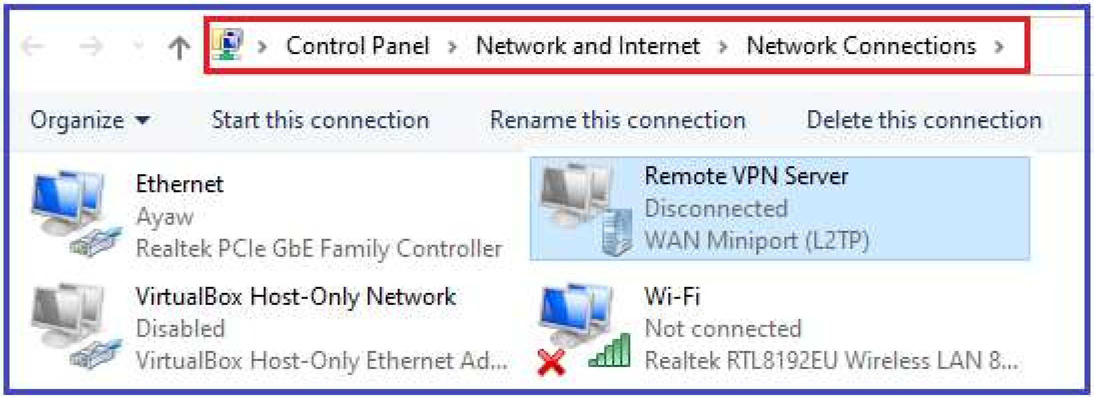
Pre-shared key
••••••••••

Type of sign-in info
User name and password

User name (optional)
user

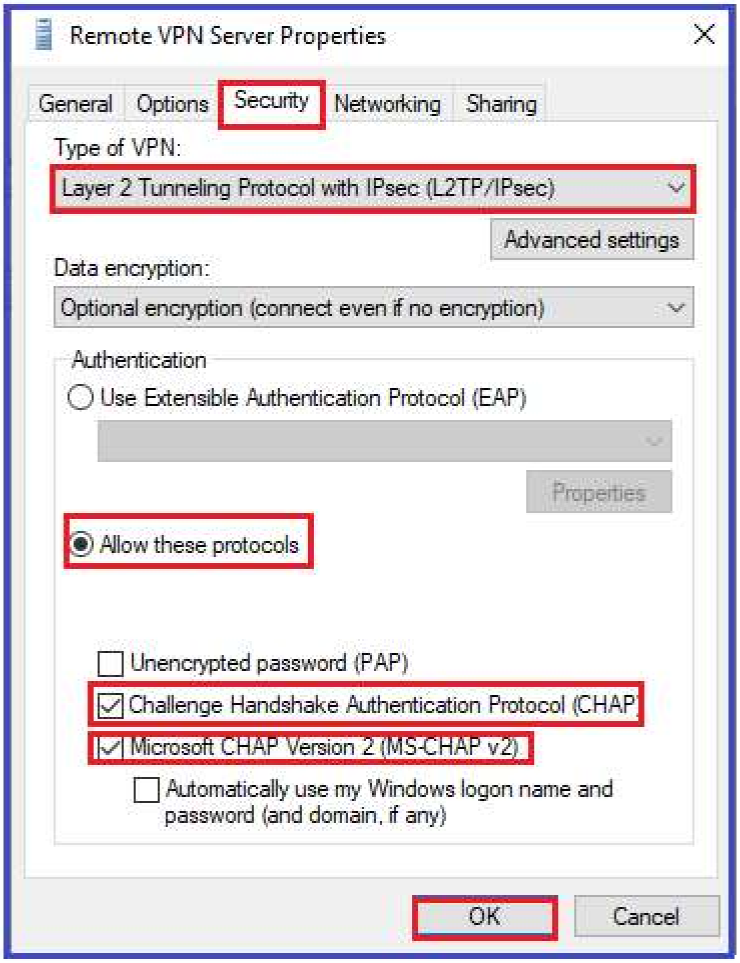
Password (optional)
••••

3. Go to control Panel -> Network and internet -> Network connections -> Right click on “Remote VPN Server” and click on Properties.



Control Panel > Network and Internet > Network Connections >
Organize
Start this connection
Rename this connection
Delete this connection
Ethernet
Ayaw
Realtek PCIe GbE Family Controller
Remote VPN Server
Disconnected
WAN Miniport (L2TP)
VirtualBox Host-Only Network
Disabled
VirtualBox Host-Only Ethernet Ad...
Wi-Fi
Not connected
Realtek RTL8192EU Wireless LAN 8...

4. On the Security tab, select L2TP/IPSec. Enable “Allow these protocols (CHAP and MS-CHAP v2)”.



Remote VPN Server Properties

General | Options | Security | Networking | Sharing

Type of VPN: Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Advanced settings

Data encryption: Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

Properties

● Allow these protocols

□ Unencrypted password (PAP)

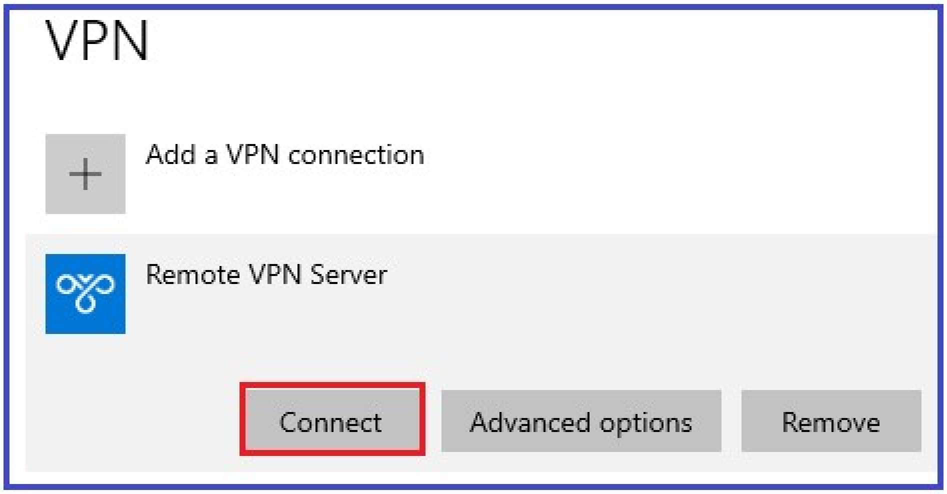
☑ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

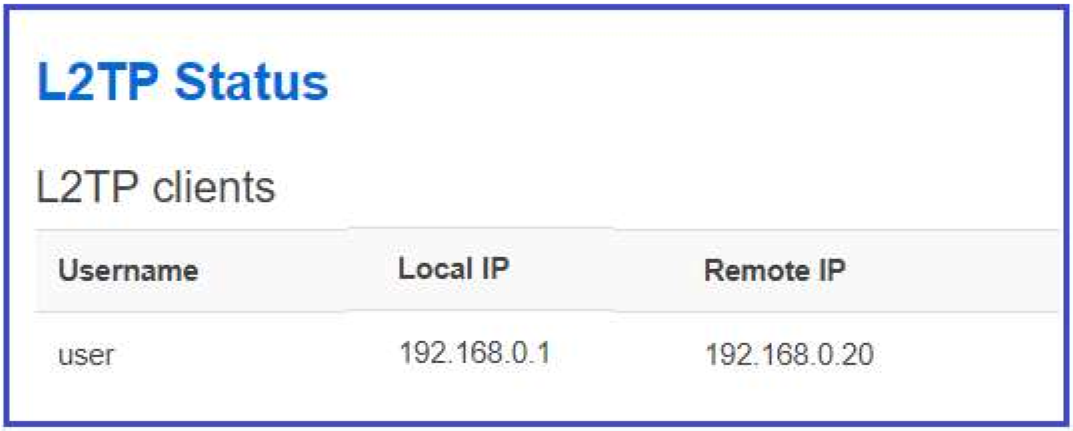
□ Automatically use my Windows logon name and password (and domain, if any)

OK | Cancel

5. On the VPN settings, click Connect on “Remote VPN Server”.



6. On the router GUI, go to Status -> VPN -> L2TP Status to check L2TP client.

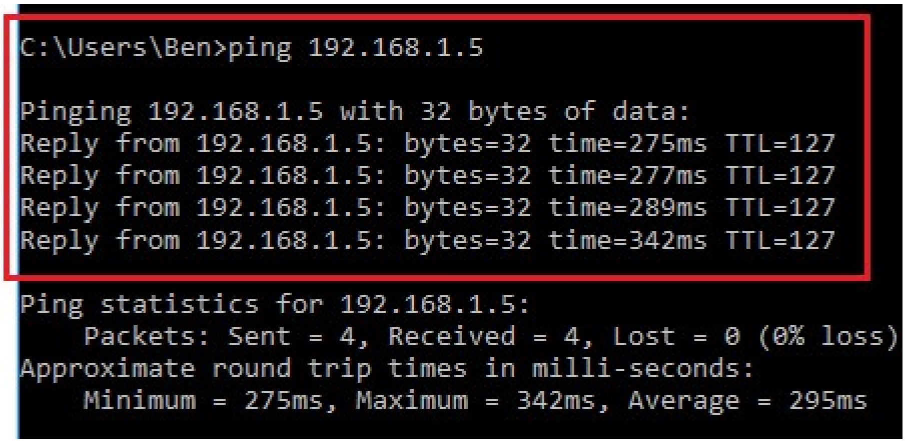


L2TP Status

L2TP clients

Username	Local IP	Remote IP
user	192.168.0.1	192.168.0.20

7. Ping PC2 (192.168.1.5) behind the L2TP/IPSec server from PC1.



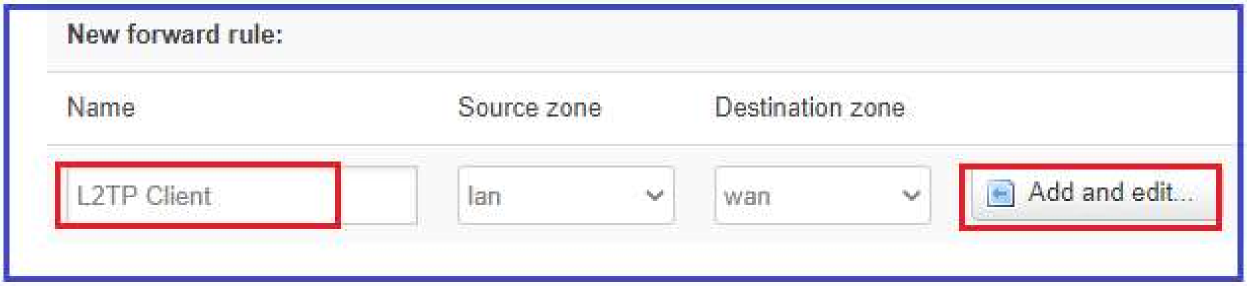
```
C:\Users\Ben>ping 192.168.1.5

Pinging 192.168.1.5 with 32 bytes of data:
Reply from 192.168.1.5: bytes=32 time=275ms TTL=127
Reply from 192.168.1.5: bytes=32 time=277ms TTL=127
Reply from 192.168.1.5: bytes=32 time=289ms TTL=127
Reply from 192.168.1.5: bytes=32 time=342ms TTL=127

Ping statistics for 192.168.1.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss)
Approximate round trip times in milli-seconds:
    Minimum = 275ms, Maximum = 342ms, Average = 295ms
```

8. If L2TP/IPSec client needs to access the internet via L2TP/IPSec server, we need to add a Firewall Rule to allow it.

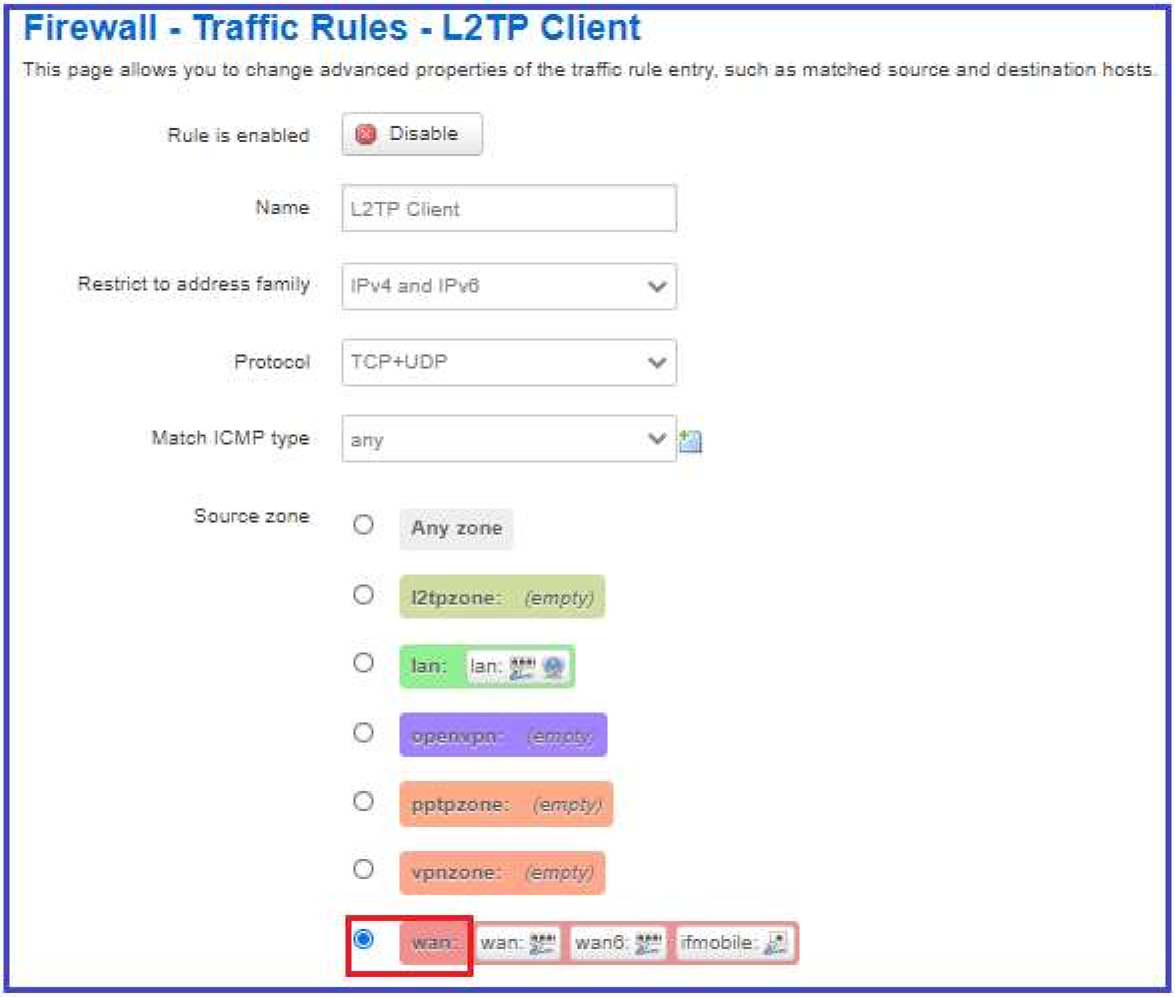
9. Go to Network→Firewall→Traffic Rules , and scroll down. Input rule name and click “Add and edit…”



New forward rule:

Name	Source zone	Destination zone	
L2TP Client	lan	wan	Add and edit...

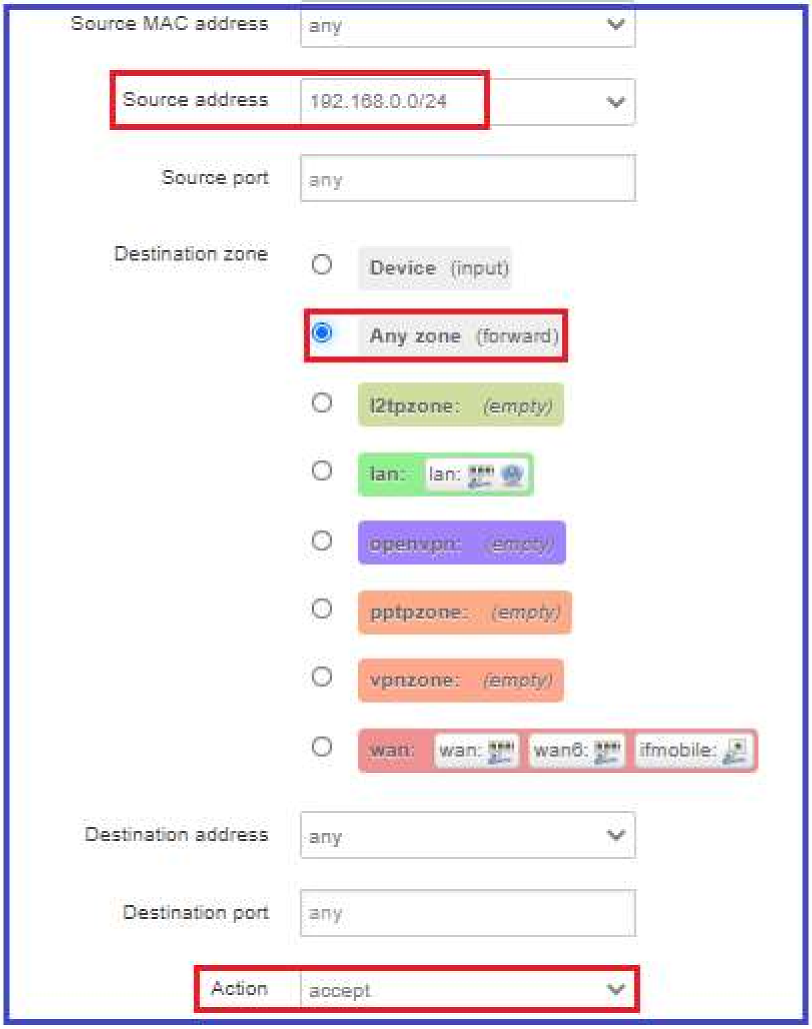
10. Set Protocol to Any, Source zone to **WAN**, source address to the L2TP virtual IP subnet. We use **192.168.0.0/24**. Destination zone set to **Any zone** and action to **ACCEPT**.



Firewall - Traffic Rules - L2TP Client

This page allows you to change advanced properties of the traffic rule entry, such as matched source and destination hosts.

Rule is enabled	Disable
Name	L2TP Client
Restrict to address family	IPv4 and IPv6
Protocol	TCP+UDP
Match ICMP type	any
Source zone	○ Any zone ○ l2tpzone: (empty) ○ lan: lan: ○ openvpn: (empty) ○ pptpzone: (empty) ○ vpnzone: (empty) ● wan: wan: wan6: ifmobile:



Source MAC address: any

Source address: 192.168.0.0/24

Source port: any

Destination zone:
○ Device (input)
● Any zone (forward)
○ l2tpzone: (empty)
○ lan: lan:
○ openvpn: (empty)
○ pptpzone: (empty)
○ vpnzone: (empty)
○ wan: wan: wan6: ifmobile:

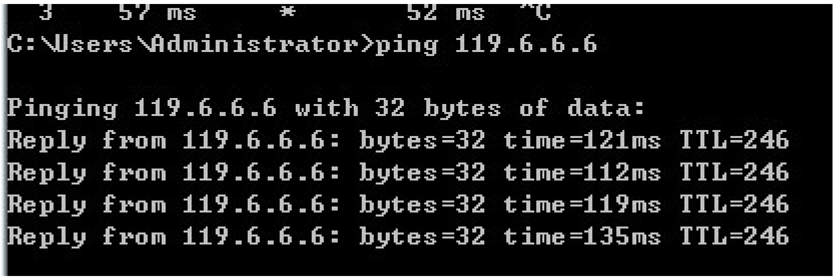
Destination address: any

Destination port: any

Action: accept

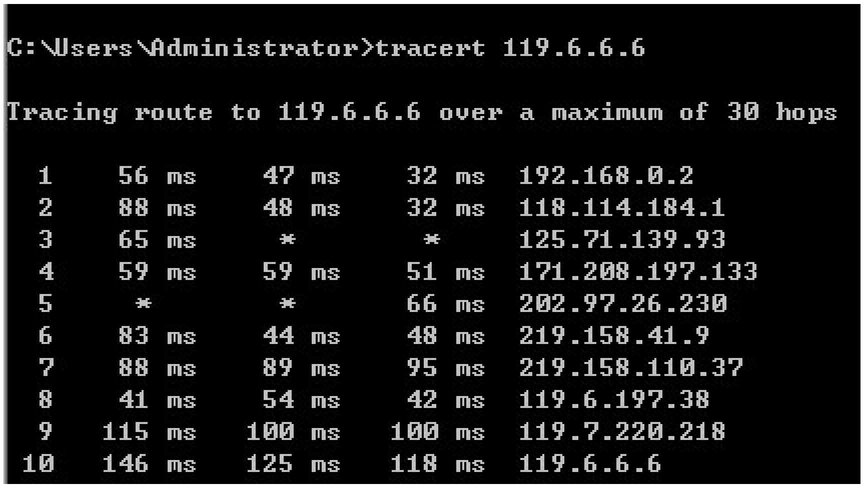
11. Click the “Save & Apply” button.

12. Ping and trace public IP from L2TP client.



```
  3    57 ms     *       52 ms  ^C
C:\Users\Administrator>ping 119.6.6.6

Pinging 119.6.6.6 with 32 bytes of data:
Reply from 119.6.6.6: bytes=32 time=121ms TTL=246
Reply from 119.6.6.6: bytes=32 time=112ms TTL=246
Reply from 119.6.6.6: bytes=32 time=119ms TTL=246
Reply from 119.6.6.6: bytes=32 time=135ms TTL=246
```



```
C:\Users\Administrator>tracert 119.6.6.6

Tracing route to 119.6.6.6 over a maximum of 30 hops

  1    56 ms    47 ms    32 ms  192.168.0.2
  2    88 ms    48 ms    32 ms  118.114.184.1
  3    65 ms     *        *     125.71.139.93
  4    59 ms    59 ms    51 ms  171.208.197.133
  5     *        *       66 ms  202.97.26.230
  6    83 ms    44 ms    48 ms  219.158.41.9
  7    88 ms    89 ms    95 ms  219.158.110.37
  8    41 ms    54 ms    42 ms  119.6.197.38
  9   115 ms   100 ms   100 ms  119.7.220.218
 10   146 ms   125 ms   118 ms  119.6.6.6
```