2013

ZyWALL Series Support Note

V1

4/1/2013

Scenario 1 - Restricting Bandwidth Management Priority for Traffic

1.1 Application Scenario

In an enterprise network, there are various types of traffic. However, most company's Internet bandwidth is limited. All traffic will contend for it and may result in some important traffic, for example. Therefore, intelligent bandwidth management for improved productivity becomes a matter of high concern for network administrators. A ZyWALL provides Bandwidth Management (BWM) function to effectively manage bandwidth according to different flexible criteria. Here is the example to limit FTP traffic by BWM.

1.2 Configuration Guide

Network conditions:

- WAN download bandwidth: 2M

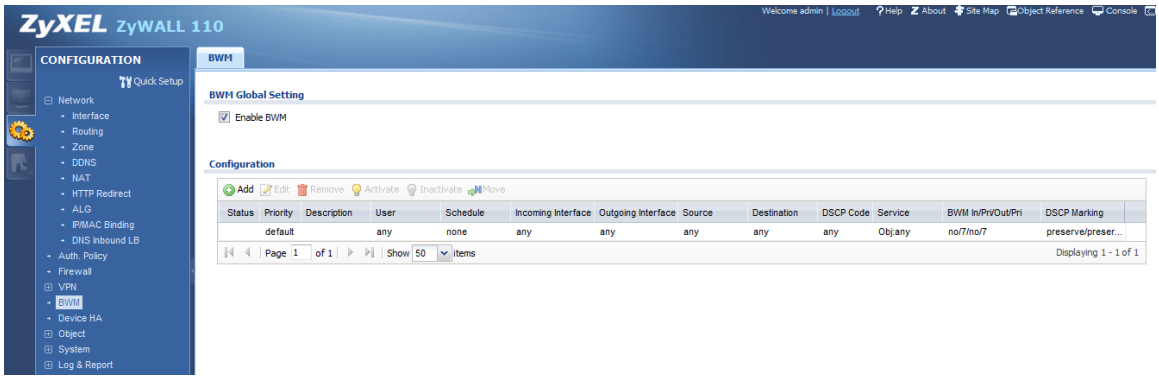
- WAN upload bandwidth: 1M

Goals to achieve:

Restrict FTP download/upload bandwidth to 1000/500 kbps and set priority of FTP traffic to 4 for all users.

ZyWALL configuration:

Step 1: **Configuration** > **BWM** > check “Enable BWM”

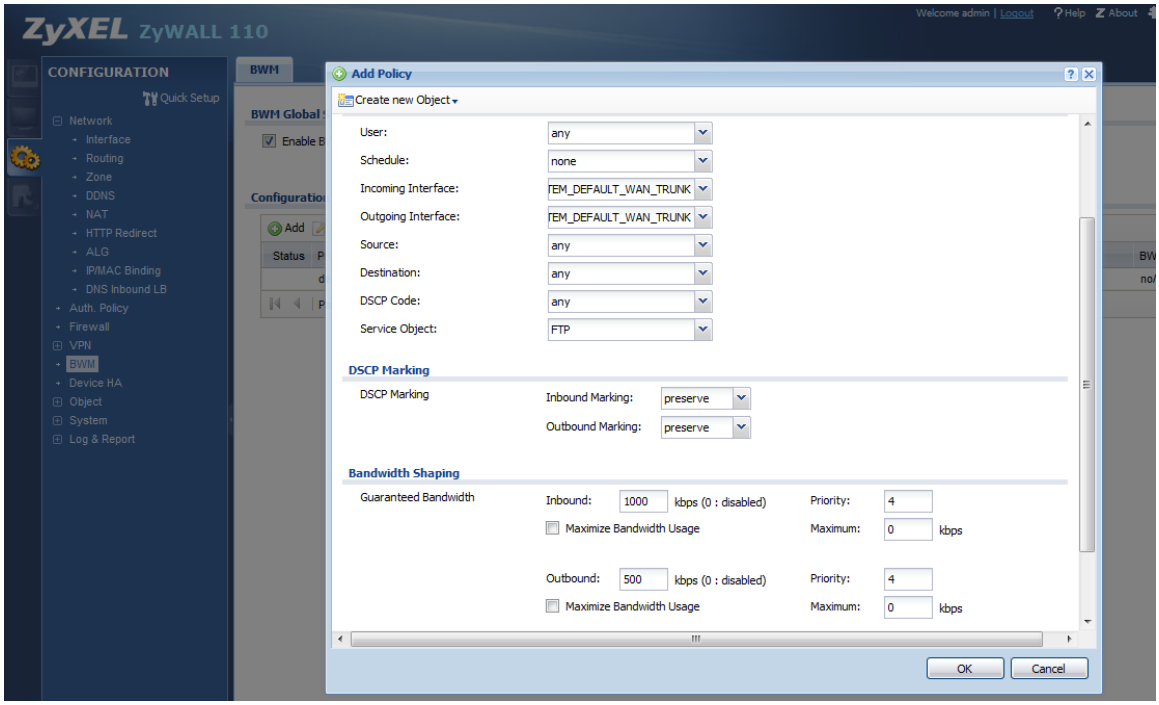


Step 2: **Configuration** > **BWM** > Select the “**Add**”

(1) Select the “WAN trunk interface” in **incoming** and **outgoing** interface

(2) And service object select the “**FTP**”.

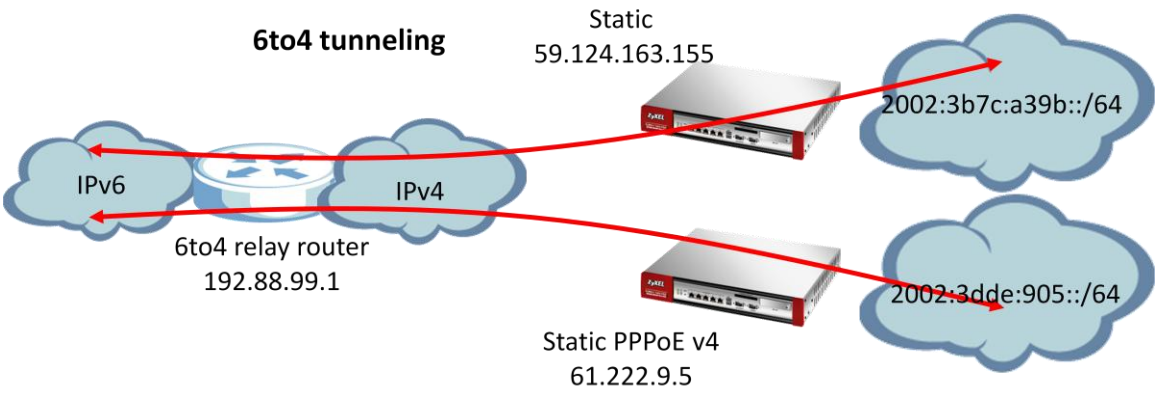
(3) Limit the **inbound** 1000Kbps and **Outbound** 500Kbps and the all of the priority is **4**.


ZyXEL ZyWALL 110
Welcome admin | Logout
Help
About
CONFIGURATION
Quick Setup
Network
Interface
Routing
Zone
DDNS
NAT
HTTP Redirect
ALG
IP/MAC Binding
DNS Inbound LB
Auth. Policy
Firewall
VPN
BWM
Device HA
Object
System
Log & Report
BWM
BWM Global
Enable B
Configuratio
Add
Status
Add Policy
Create new Object
User:
any
Schedule:
none
Incoming Interface:
TEM_DEFAULT_WAN_TRUNK
Outgoing Interface:
TEM_DEFAULT_WAN_TRUNK
Source:
any
Destination:
any
DSCP Code:
any
Service Object:
FTP
DSCP Marking
DSCP Marking
Inbound Marking:
preserve
Outbound Marking:
preserve
Bandwidth Shaping
Guaranteed Bandwidth
Inbound:
1000
kbps (0 : disabled)
Priority:
4
Maximize Bandwidth Usage
Maximum:
0
kbps
Outbound:
500
kbps (0 : disabled)
Priority:
4
Maximize Bandwidth Usage
Maximum:
0
kbps
OK
Cancel

Scenario 2 - Assign IPv6 to your LAN to access remote IPv6 network

2.1 Application Scenario

Nowadays, more and more Internet service providers provide IPv6 environment. With IPv6 feature enabled on ZyWALL, it can assign an IPv6 to clients under it and pass IPv6 traffic through IPv4 environment to access remote IPv6 network.



2.2 6to4 IP Translate Introduction

Network conditions:

<u>ZyWALL:</u>

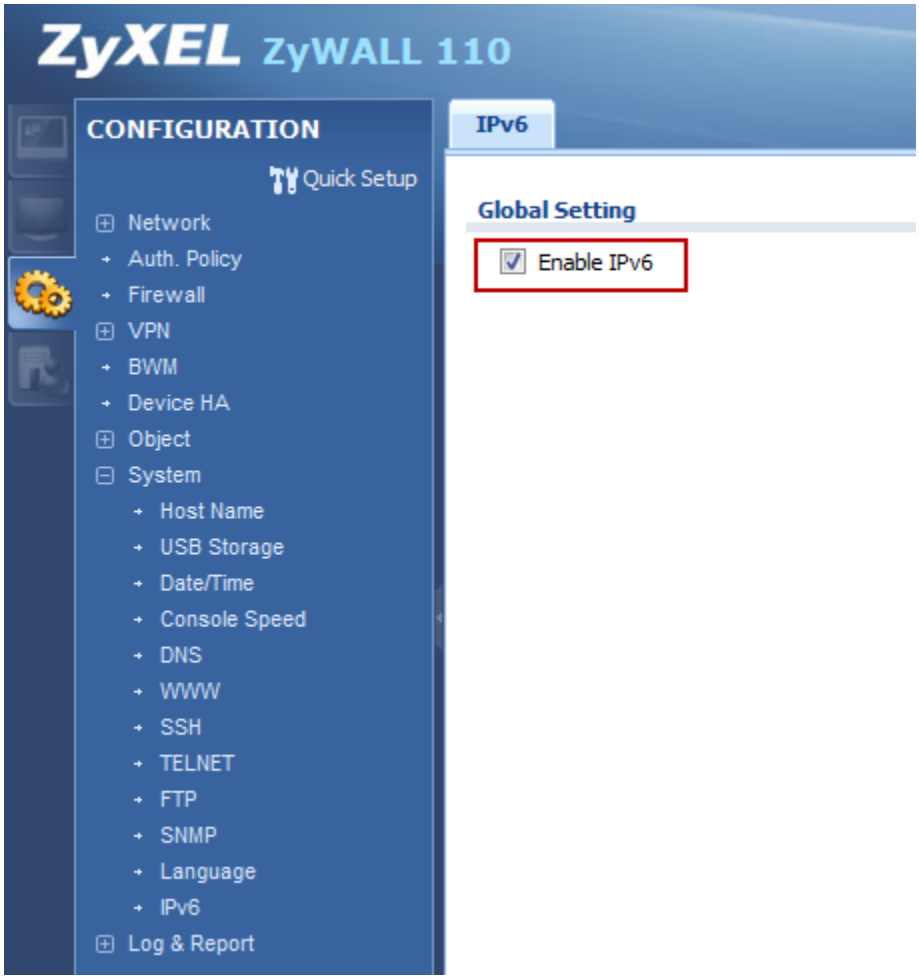
WAN1: 59.124.163.155(Static)

Goal to achieve:

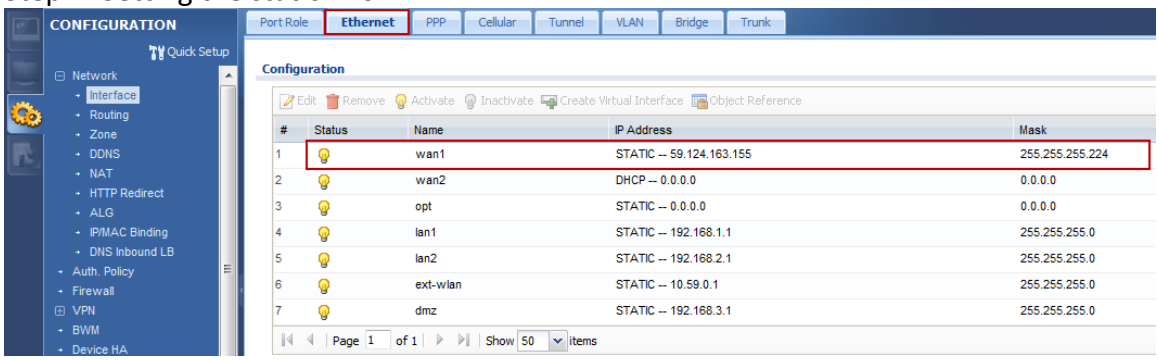
A ZyWALL will assign IPv6 IP address to the clients behind it, and the clients can access remote IPv6 network by using the ZyWALL 6to4 tunnel.

ZyWALL Configuration:

Step 1: **Configuration** > **System** > **IPv6** > Click **Enable IPv6**

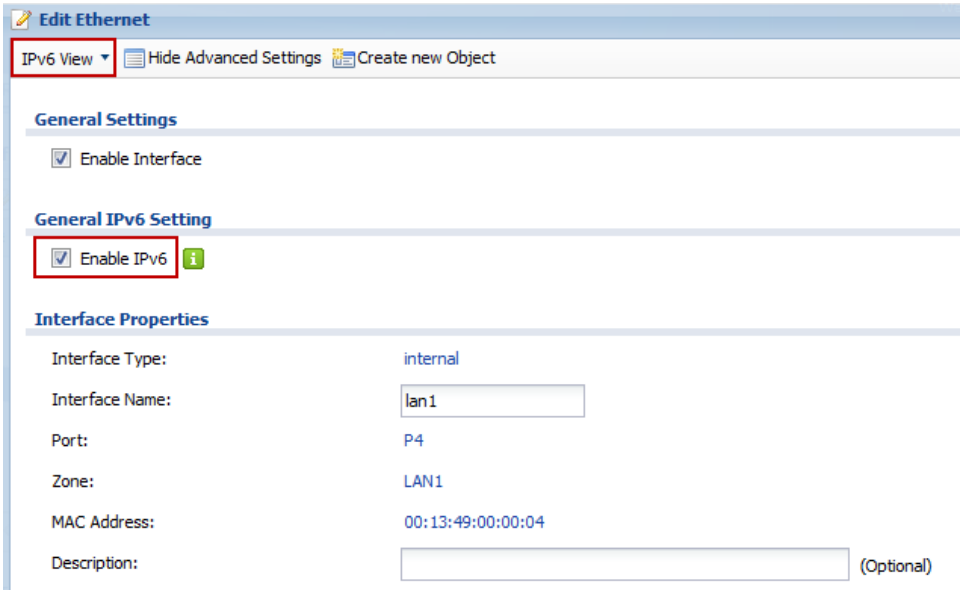


Step 2: Setting the static IP on WAN1



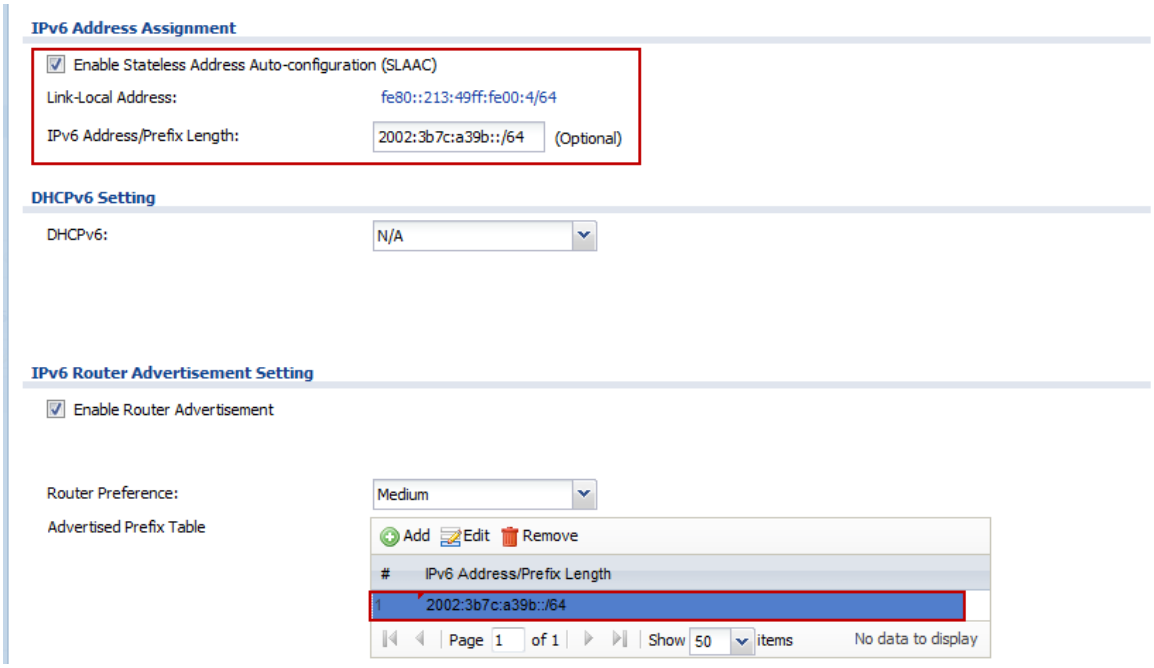
Step 3: Setting IPv6 IP address on LAN1

(1) Go to Configuration > Interface > Ethernet > double click LAN1 interface in IPv6 configuration.



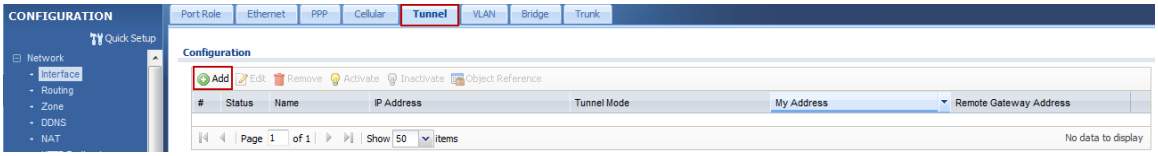
(2) Convert WAN1 IP address to hexadecimal
Check Enable Stateless Address Auto-configuration (SLAAC) box and enter 2002:3b7c:a39b::/64 in the prefix table.

(3) Check **IPv6 Router Advertisement Setting** box and add the prefix in the **Advertised Prefix Table**.



Step 4: Enable 6 to 4 tunnel.

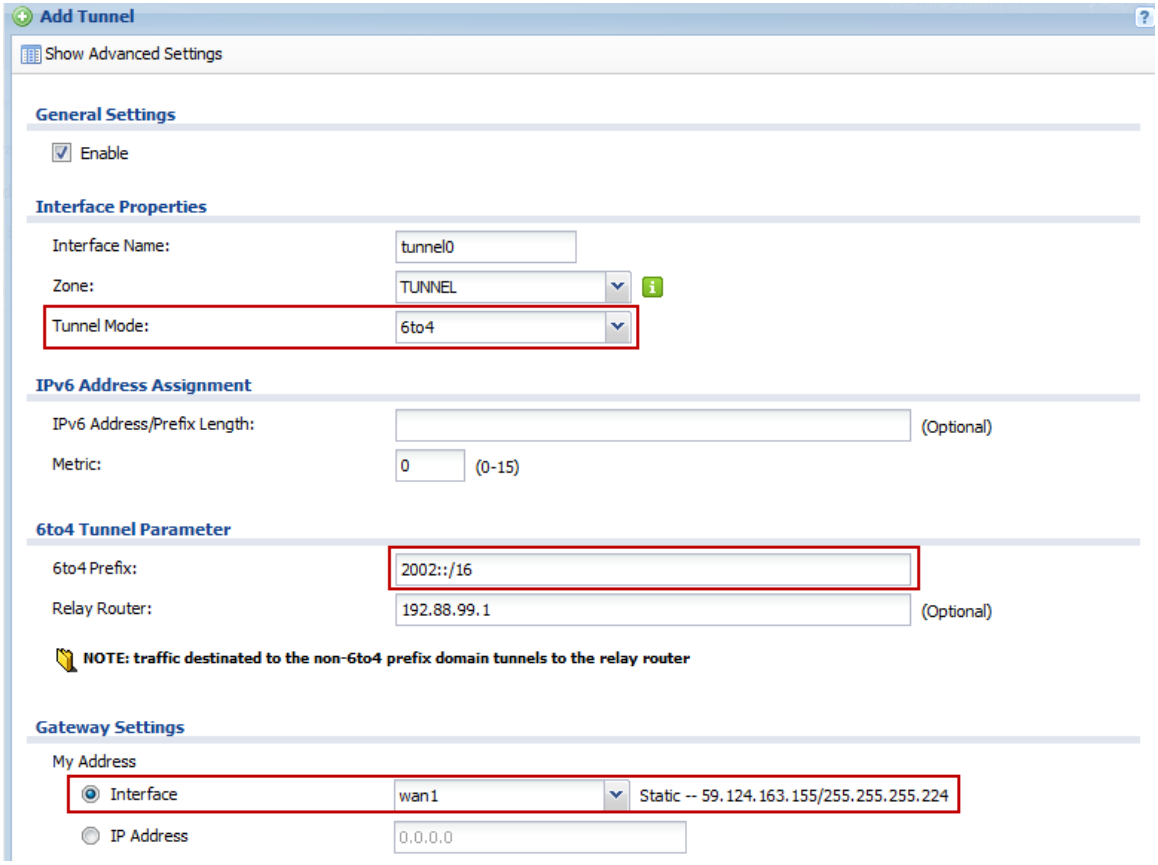
(1) Go to Configuration > Interface > Tunnel > Click Add button



(2) Select the 6to4 in that Tunnel Mode

(3) Check the Prefix in the 6tp4 tunnel Parameter

(4) Select the WAN1 interface as the gateway in the Gateway Setting

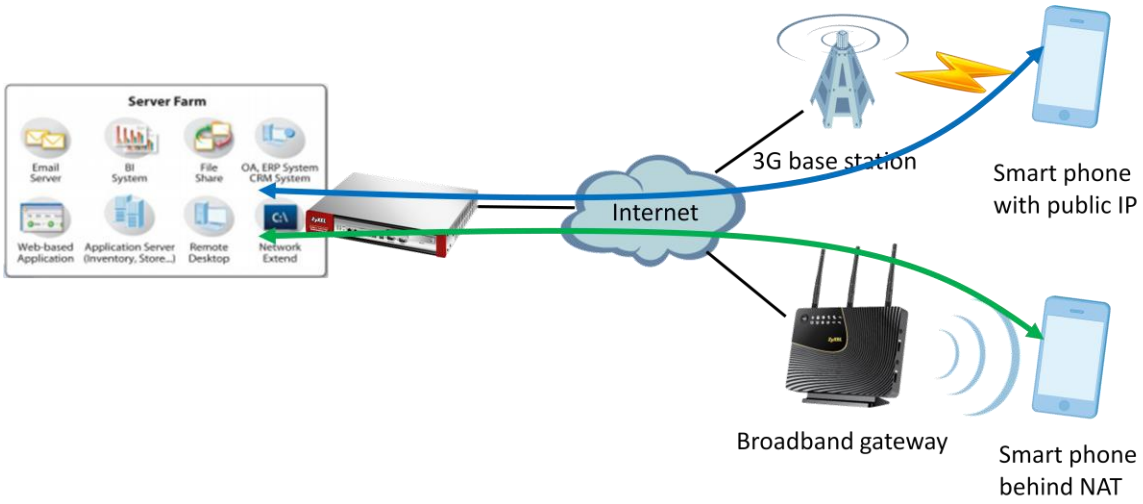


After these configuration steps, connect your computer to the device and check that your computer received an IPv6 IP address from tunnel.

Scenario 3 – Dialing up L2TP VPN connection to ZyWALL by using iOS/Android mobile device

3.1 Application Scenario

Smart phone become increasingly popular with consumers. Though it brings us much more convenience, but also brings security concerns. A ZyWALL is compatible with iOS/Android mobile devices to establish L2TP VPN connection, provide secure and private mobile data transferring no matter if your mobile devices is behind NAT. In the following diagram, outside employees need to visit an internal website in Intranet, they can just dial up L2TP VPN to ZyWALL and access needed internal resource.



3.2 Configuration Guide

Network conditions:

ZyWALL:

- WAN1 IP: 59.124.163.150
- Local subnet: 192.168.1.0/24
- L2TP pool:192.168.100.0/24
- Intranet website: http://info.zyxel.com

iOS/Android mobile device:

- IP: 116.59.252.188 (3G mobile network)
- IP: 10.59.3.103 (Behind NAT device)

IPSec VPN conditions:

Phase 1:

- Authentication: 12345678
- Local/Peer IP: WAN1/0.0.0.0
- Negotiation: Main mode
- Encryption algorithm: 3DES/3DES/DES
- Authentication algorithm: SHA1/MD5/SHA1
- Key group: DH1

Phase 2:

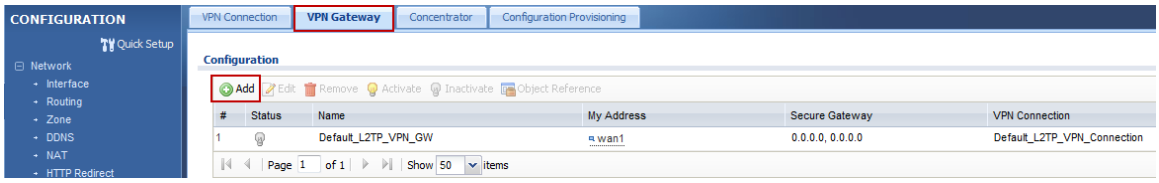
- Encapsulation Mode: Transport mode
- Active protocol: ESP
- Encryption algorithm: 3DES/3DES/DES
- Authentication algorithm: SHA1/MD5/SHA1
- Perfect Forward Secrecy: none

Goals to achieve:

Build up an L2TP over IPSec VPN tunnel for mobile users to access Intranet website.

ZyWALL configuration

Step 1: Click **Configuration > VPN > IPSec VPN > VPN Gateway** to visit VPN gateway configuration screen



Step 2: Click the “Add” button to add a VPN gateway rule.

Step 3: Fill in the needed VPN gateway configuration.

Edit VPN Gateway l2tp_gateway

Hide Advanced Settings

General Settings

Enable

VPN Gateway Name: l2tp_gateway

Gateway Settings

My Address

Interface: wan1 — Static -- 59.124.163.150/255.255.255.224

Domain Name / IP:

Peer Gateway Address

Static Address — Primary: 0.0.0.0 — Secondary: 0.0.0.0

Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

Dynamic Address

Authentication

Pre-Shared Key: 12345678

Certificate: default

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: Any

Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Proposal

Add Edit Remove

#	Encryption	Authentication
1	3DES	SHA1
2	3DES	MD5
3	DES	SHA1

Key Group: DH1

NAT Traversal

Dead Peer Detection (DPD)

Extended Authentication

Enable Extended Authentication

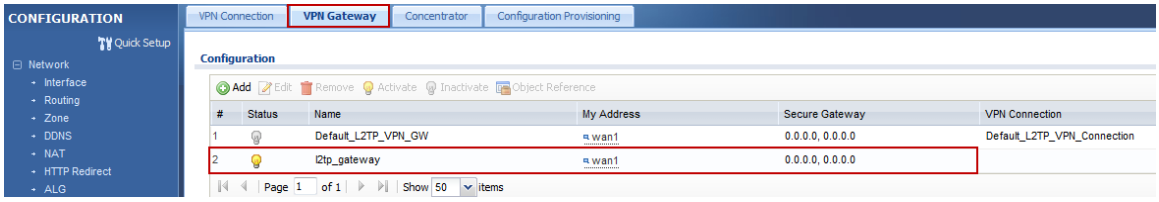
Server Mode: default

Client Mode

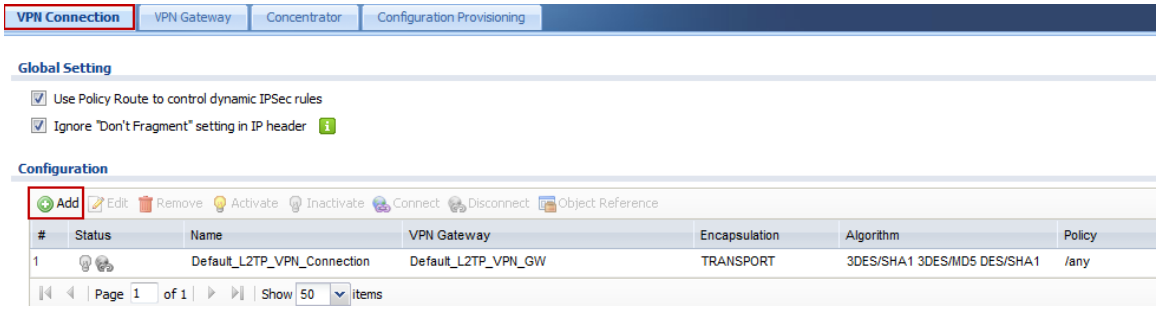
User Name :

Password:

Retype to Confirm:



Step 4: Click **Configuration > VPN > IPSec VPN > VPN Connection** to visit the configuration screen to set phase 2 rule



Step 5: Click the “Add” button to add a VPN connection rule.

Step 6: Fill in the needed VPN connection configuration.

Edit VPN Connection L2TP_VPN

Hide Advanced Settings | Create new Object

General Settings

- [x] Enable
- Connection Name: L2TP_VPN
- [ ] Nailed-Up
- [ ] Enable Replay Detection
- [ ] Enable NetBIOS broadcast over IPSec
- MSS Adjustment
  - ( ) Custom Size: 0 (200 - 1460 Bytes)
  - (•) Auto

VPN Gateway

- Application Scenario
  - ( ) Site-to-site
  - ( ) Site-to-site with Dynamic Peer
  - (•) Remote Access (Server Role)
  - ( ) Remote Access (Client Role)
- VPN Gateway: l2tp_gateway — wan1 0.0.0.0 0.0.0.0
- Manual Key
  - ( ) Manual Key
    - My Address:
    - Secure Gateway Address:
    - SPI: (256 - 4095)
    - Encapsulation Mode: Tunnel
    - Active Protocol: ESP
    - Encryption Algorithm: DES
    - Authentication Algorithm: SHA1
    - Encryption Key:
    - Authentication Key:

Policy

- Local policy: WAN1_IP — HOST, 59.124.163.150

Phase 2 Setting

- SA Life Time: 86400 (180 - 3000000 Seconds)
- Active Protocol: ESP
- Encapsulation: Transport
- Proposal

Add | Edit | Remove

#	Encryption	Authentication
1	3DES	SHA1
2	3DES	MD5
3	DES	SHA1

- Perfect Forward Secrecy (PFS): none

Related Settings

- Zone: IPSec_VPN

Connectivity Check

- [ ] Enable Connectivity Check
  - Check Method: icmp
  - Check Period: (5-30 Seconds)
  - Check Timeout: (1-10 Seconds)
  - Check Fail Tolerance: (1-10)
  - (•) Check This Address (Domain Name or IP Address)
  - ( ) Check the First and Last IP Address in the Remote Policy
  - [ ] Log

Inbound/Outbound traffic NAT

Outbound Traffic

- [ ] Source NAT
  - Source: Please select one ...
  - Destination: Please select one ...
  - SNAT: Please select one ...

Inbound Traffic

- [ ] Source NAT
  - Source: Please select one ...
  - Destination: Please select one ...
  - SNAT: Please select one ...
- [ ] Destination NAT

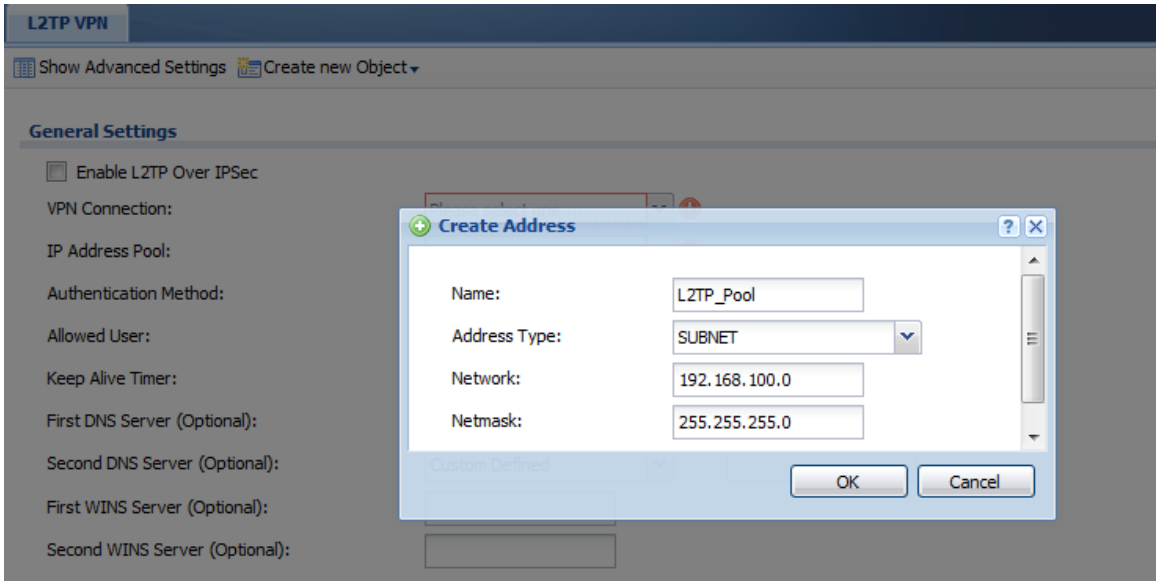
Add | Edit | Remove | Move

#	Original IP	Mapped IP	Protocol	Original Port Start	Original Port End	Mapped Port Start	Mapped Port End

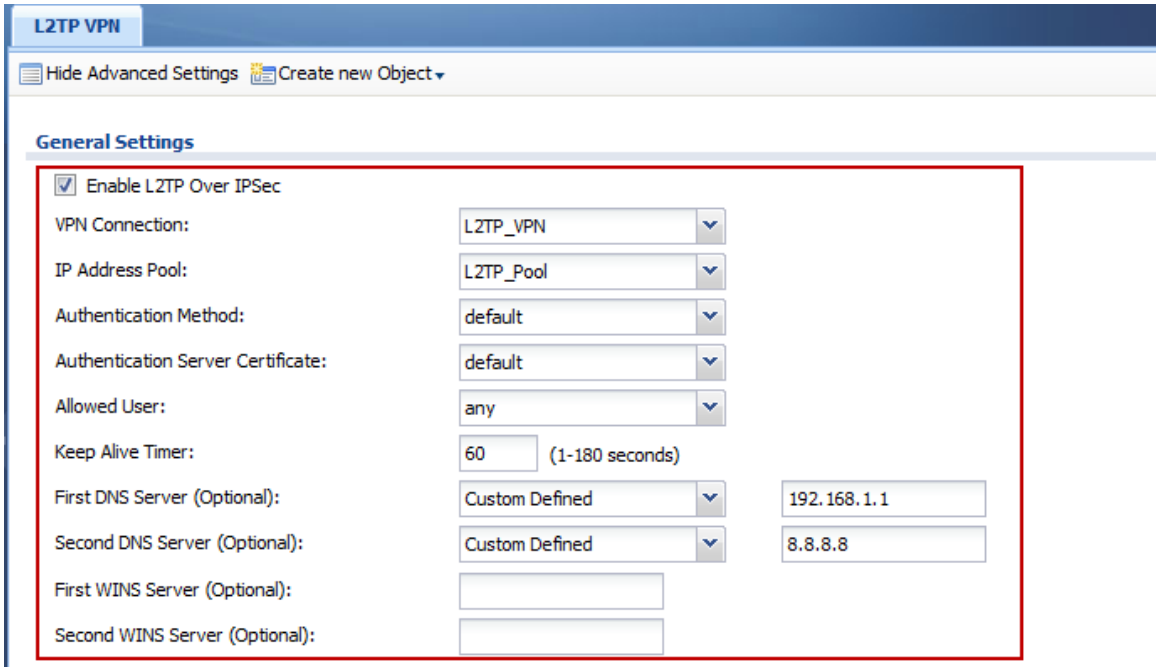
Page 1 of 1 | Show 50 items | No data to display

Step 7: Click **Configuration > VPN > L2TP VPN** to visit L2TP VPN configuration screen

Step 8: Create a address object for L2TP users

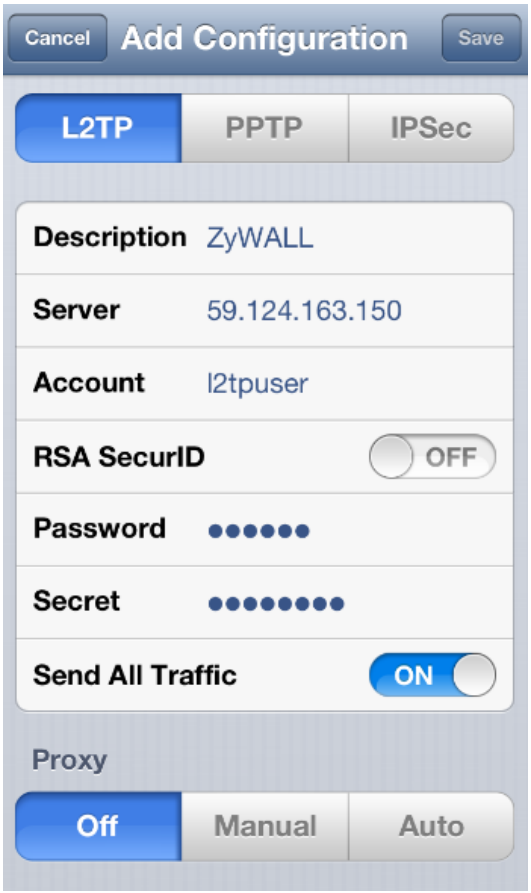


Step 9: Fill in the needed L2TP VPN connection configuration.

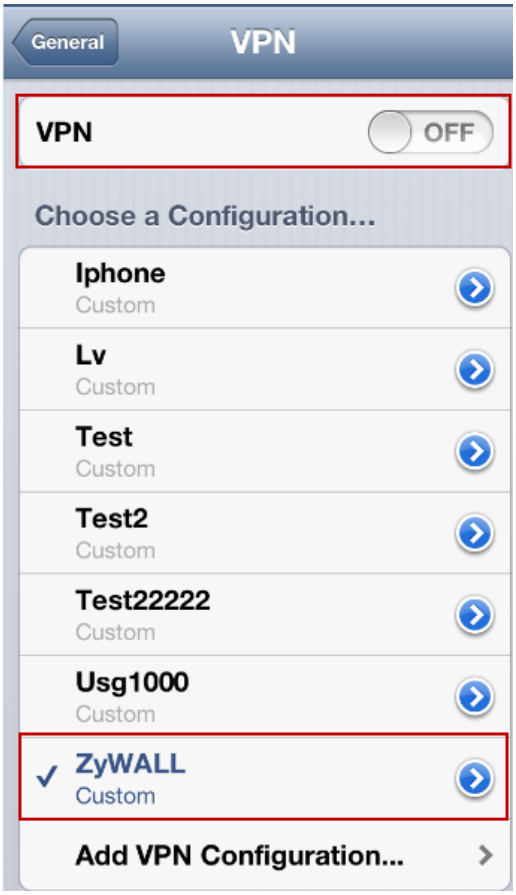


iOS mobile client configuration

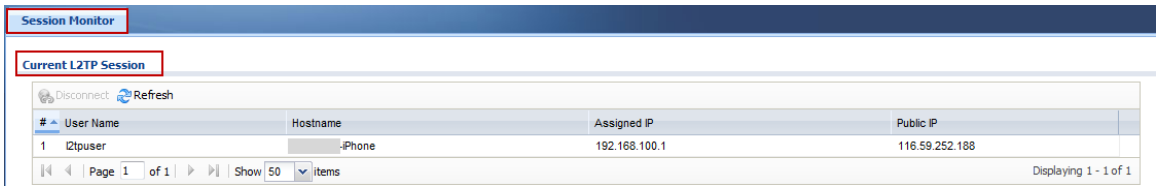
Step 1: **Settings > General > Network > VPN > Add configuration** and insert needed L2TP VPN settings.
Secret is the pre-shared key 12345678.



Step 2: Choose the VPN and turn on

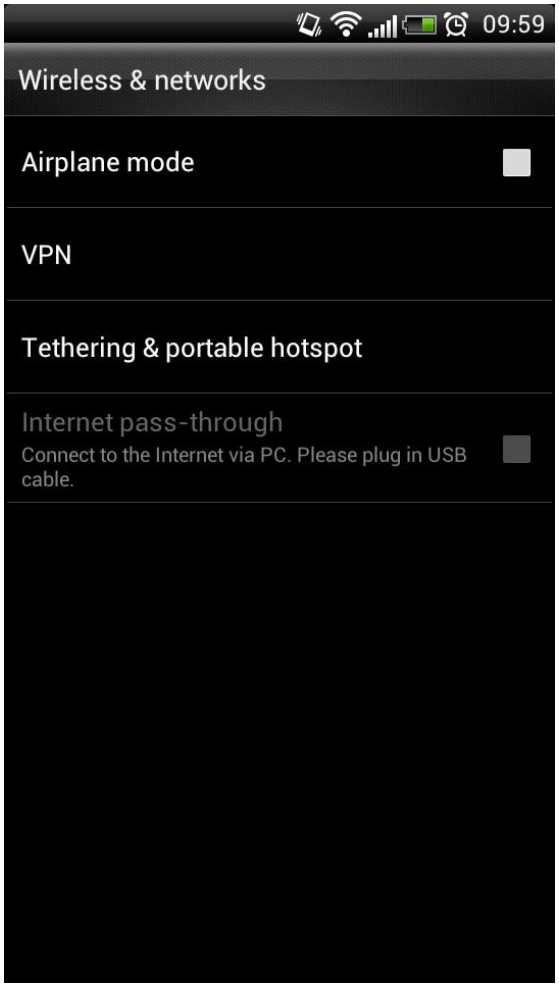


Step 3. Go to **Monitor > VPN Monitor > L2TP over IPSec** to check the L2TP session.

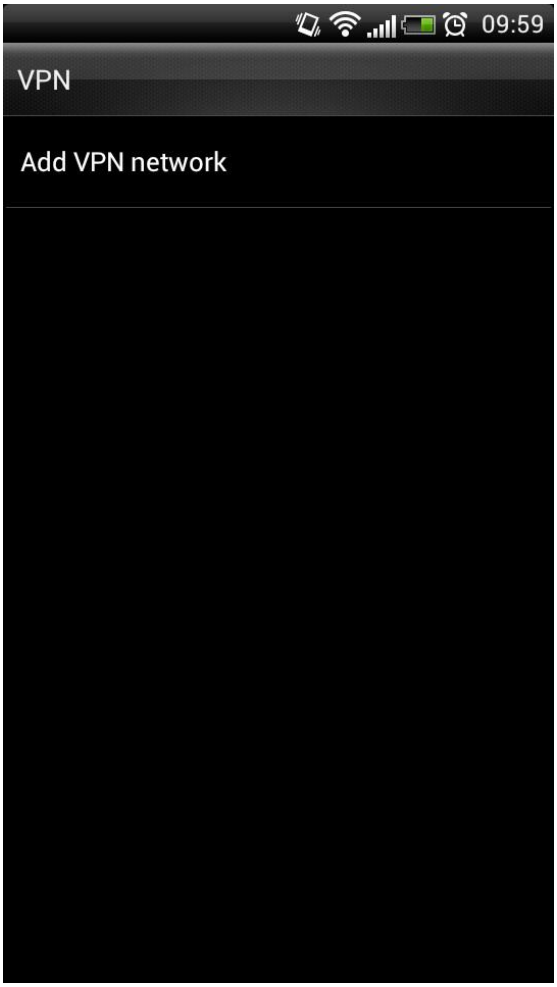


Android mobile client configuration

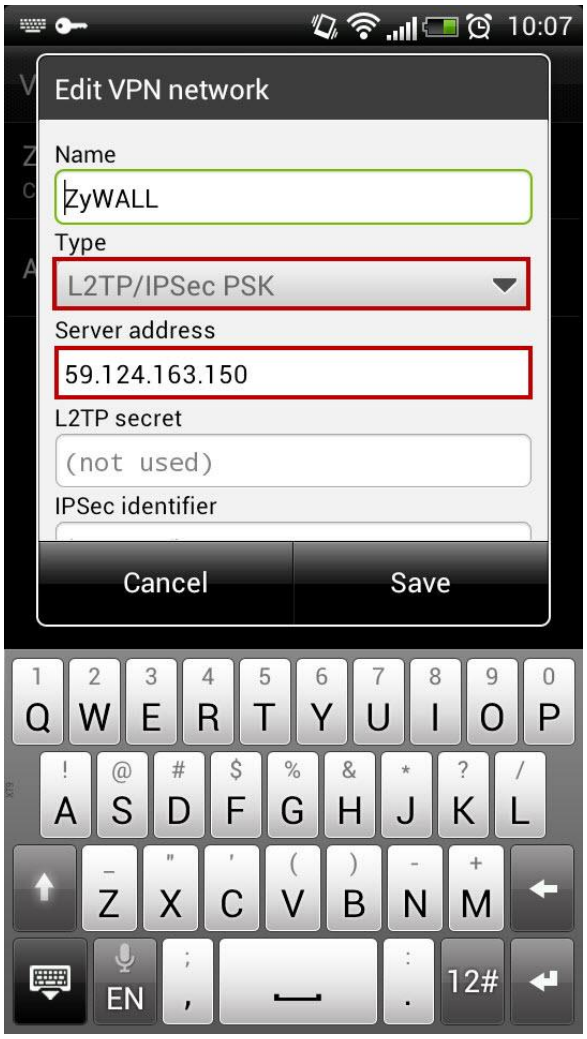
Step 1: **Settings > Wireless & networks > VPN**



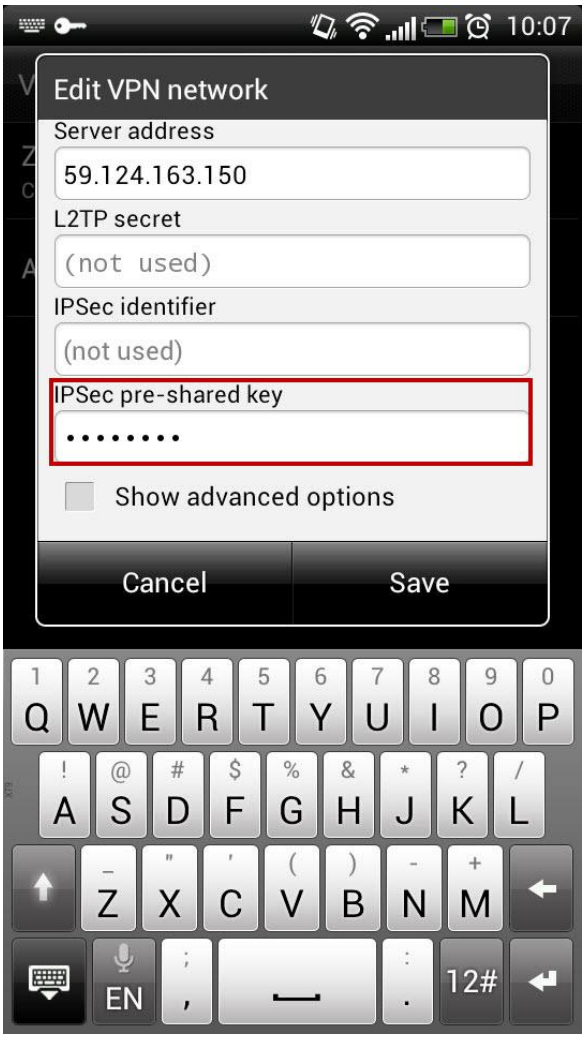
Step 2: Add VPN network



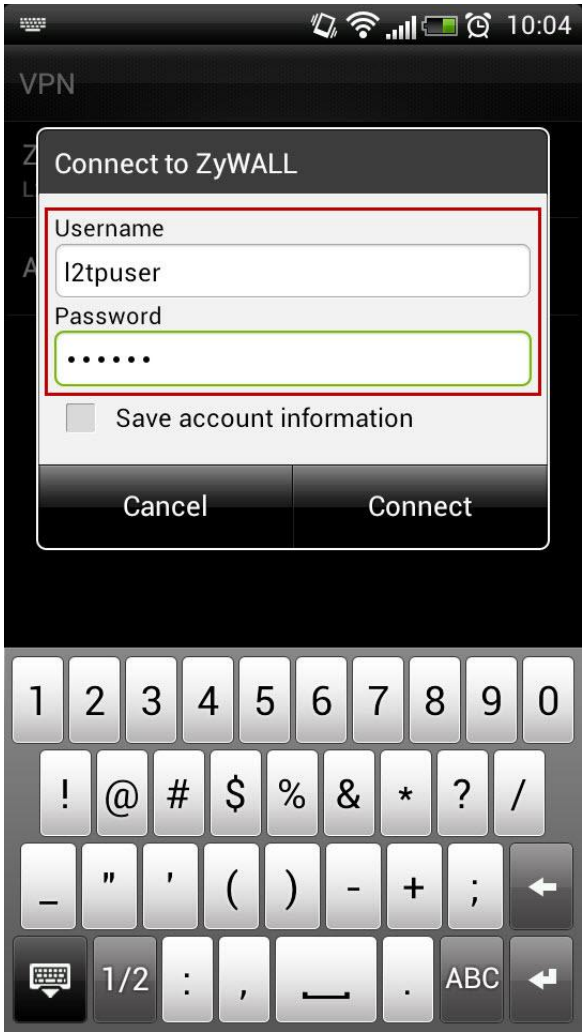
Step 3: Select L2TP/IPSec PSK as the type and fill in the server address.



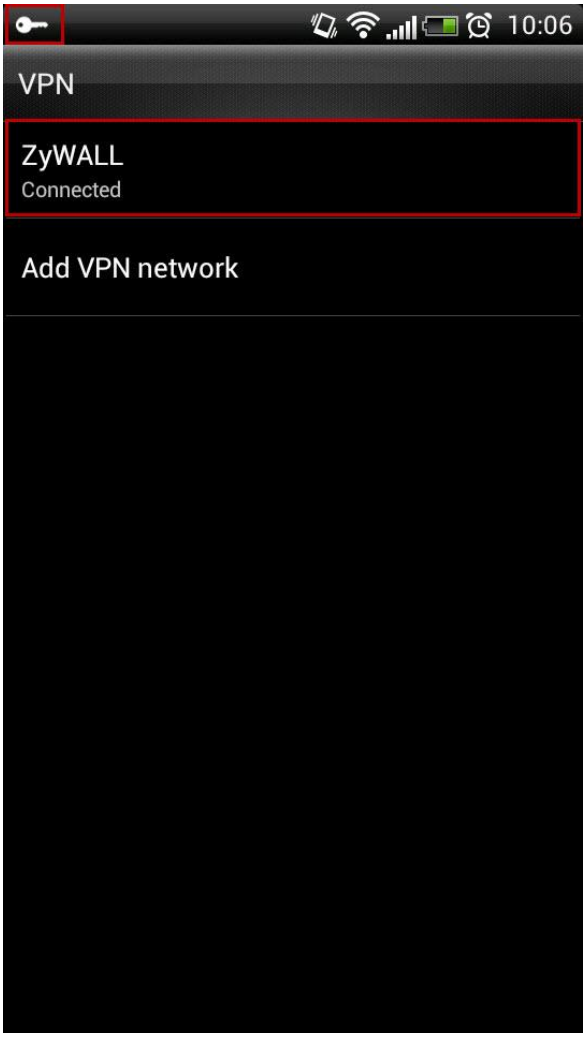
Step 4: Fill in the Pre-shared key 12345678 and click “Save”.



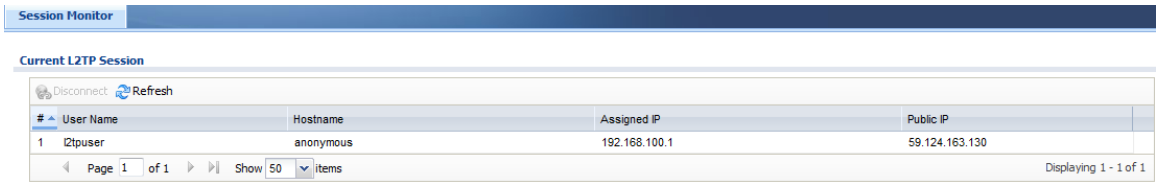
Step 5: Click on “ZyWALL” to connect to the L2TP VPN. Fill in the L2TP password and click “Connect”.



Step 6: Device will show connected when dial up successfully



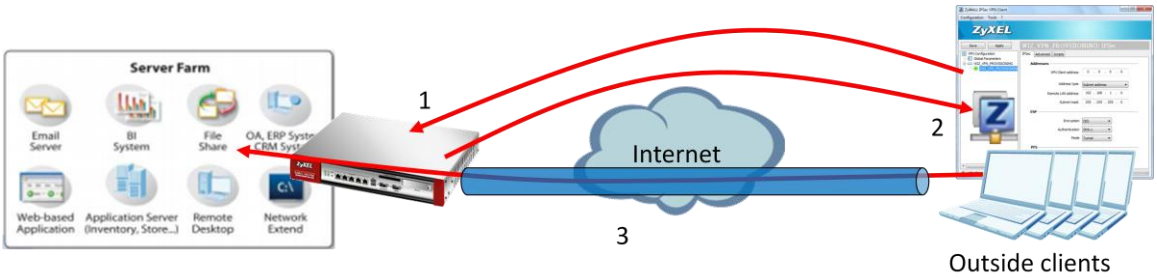
Step 7. Go to **Monitor > VPN Monitor > L2TP over IPSec** to check the L2TP session.



Scenario 4 – One click Setup VPN connection to headquarter

4.1 Application Scenario

As an enterprise, employees often have business trip around the world. They might need to access the resource which inside headquarter during trip and it brings secure concerns. One of the solutions is to build a IPSec VPN tunnel to reach the purpose, but it has difficulty for non-technical employees and will increase work loading on network administrator to help them setup. A ZyWALL provides an EASY VPN solution to download a VPN configuration file from it and import the configuration file to build up the VPN connection.



1. Login ZyWALL via IPSec VPN client software for authentication.
2. Retrieve IPSec VPN configuration profile from ZyWALL.
3. Double click profile to build up IPSec VPN tunnel and access internal resource.

4.2 Configuration Guide

Network conditions:

ZyWALL:

- WAN 1 IP: 59.124.163.147
- Local subnet: 192.168.1.0/24

IPSec VPN conditions:

Phase 1:

- Authentication: 12345678
- Local/Peer IP: WAN1/0.0.0.0
- Negotiation: Main mode
- Encryption algorithm: DES
- Authentication algorithm: MD5
- Key group: DH1

Outside user:

- IP: 114.16.87.56

Phase 2:

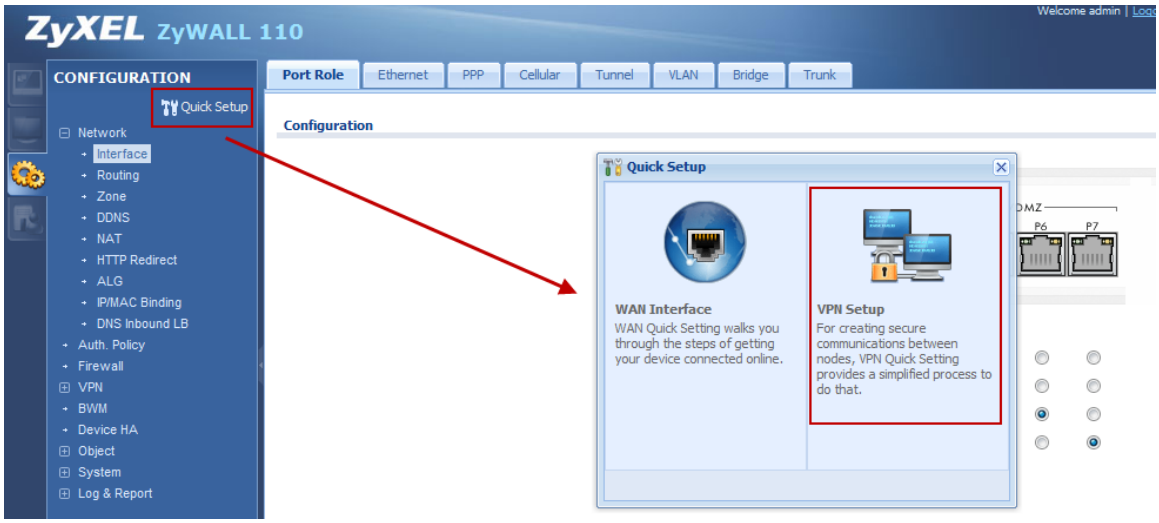
- Encapsulation Mode: Tunnel mode
- Active protocol: ESP
- Encryption algorithm: DES
- Authentication algorithm: SHA1
- Perfect Forward Secrecy: none

Goals to achieve:

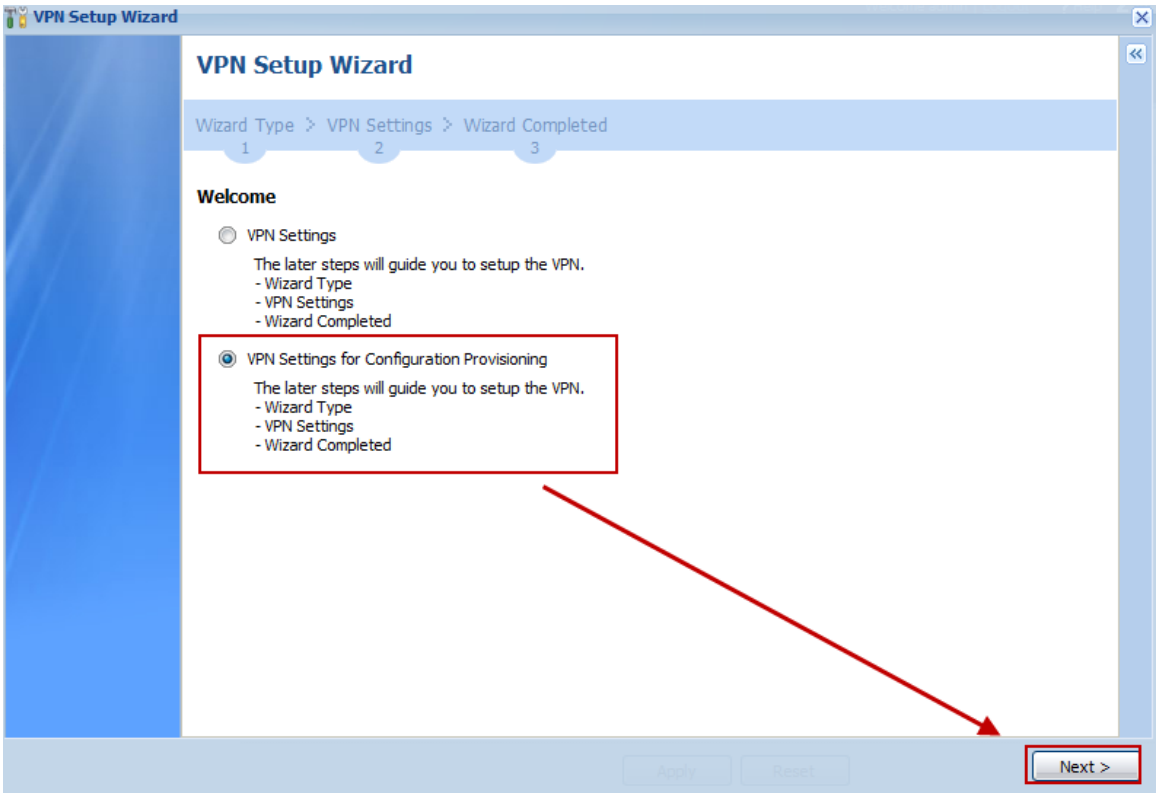
Provide an easy way for outside users to build up IPSec VPN tunnel by using the ZyWALL IPSec VPN Client for accessing internal resource.

ZyWALL configuration

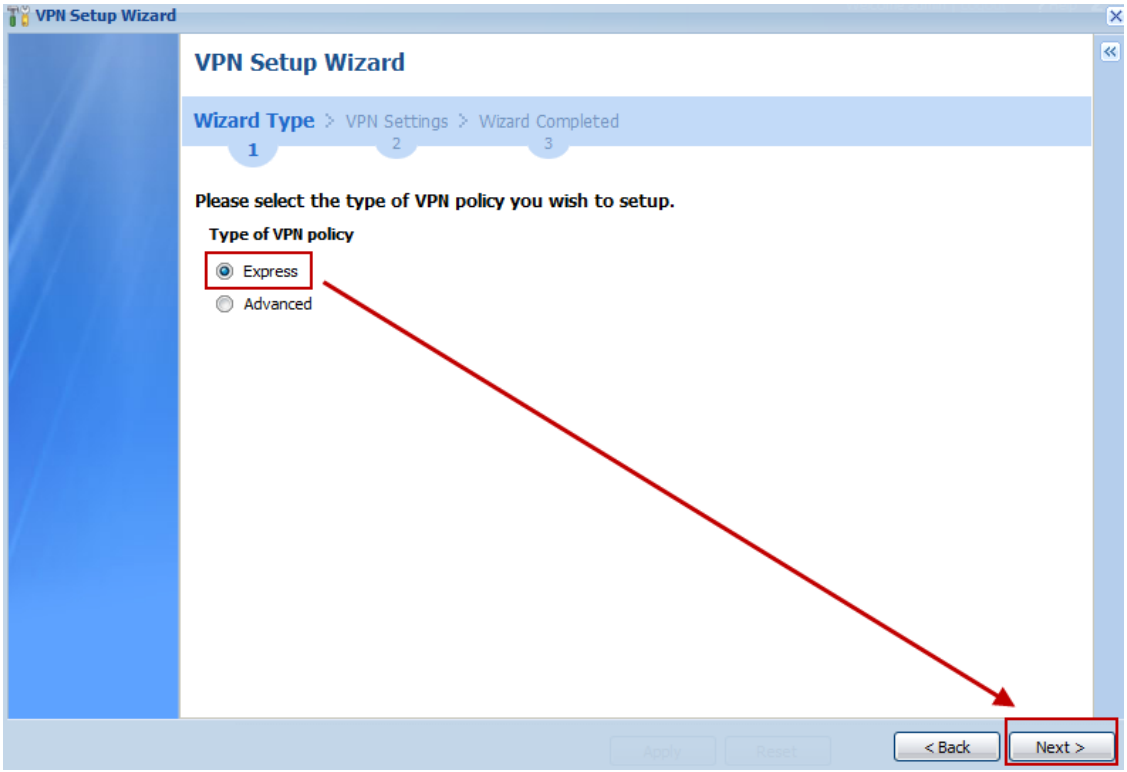
Step 1: Click **Configuration > Quick setup >VPN Setup**



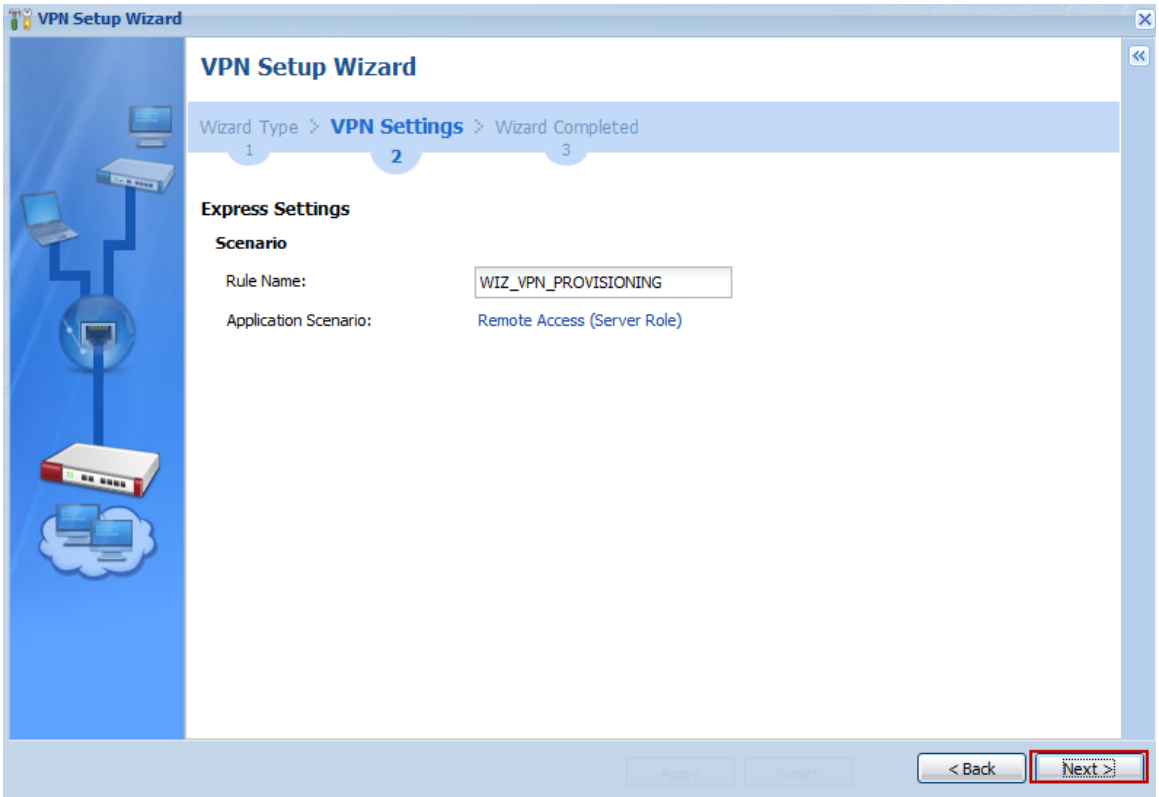
Step 2: Select “VPN settings for Configuration Provisioning”



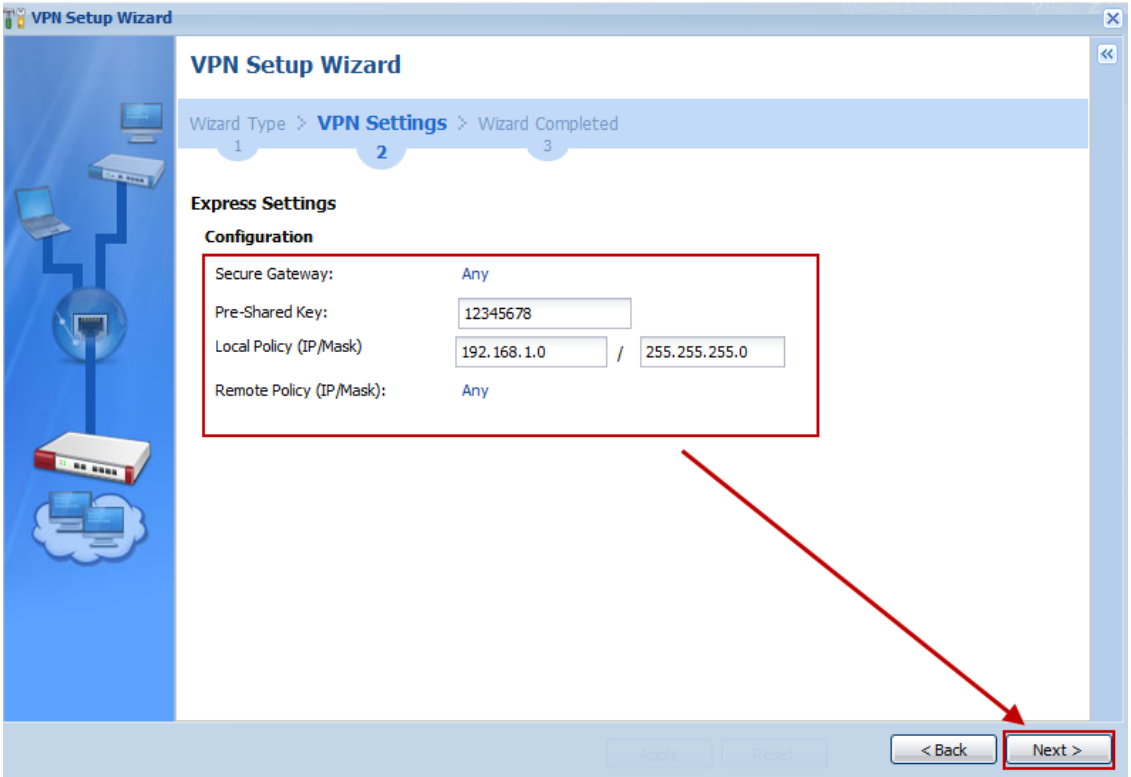
Step 3: Select “Express” (or select “Advance” to define detail settings manually)



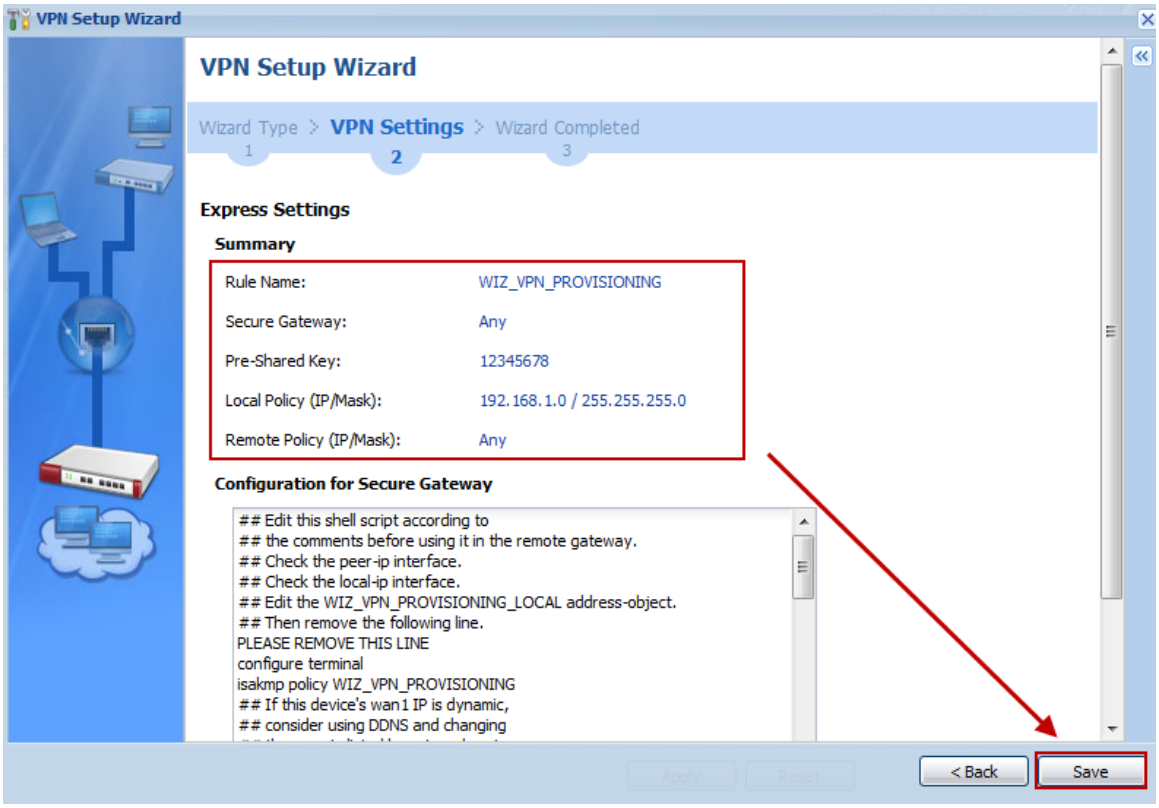
Step 4: Change Rule Name if needed



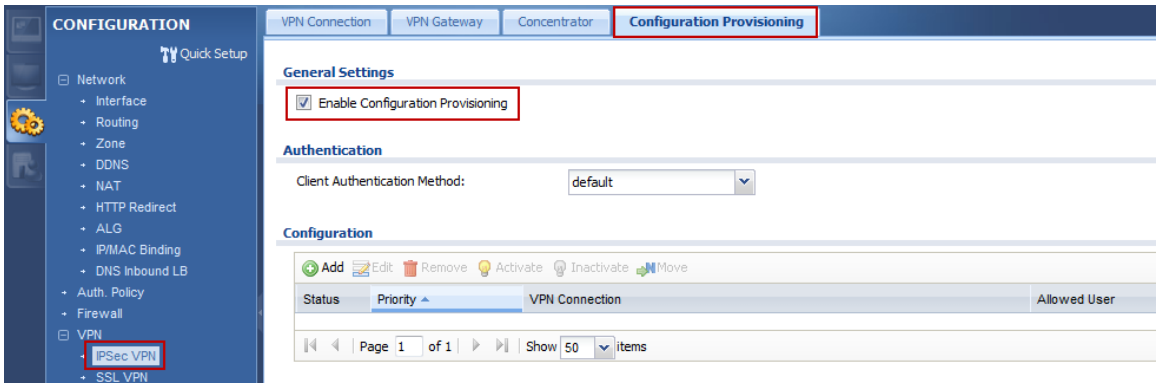
Step 5: Fill in Pre-shared key and Local policy



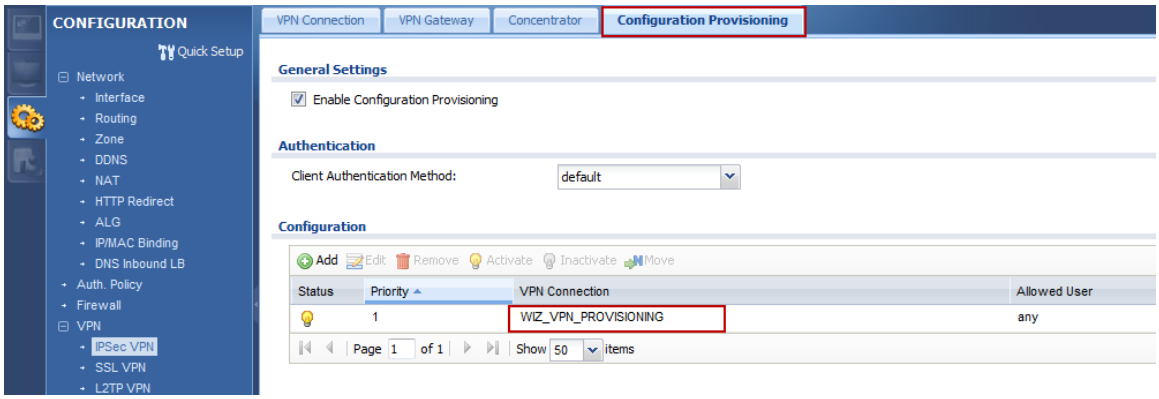
Step 6: Check if IPSec VPN configuration correct and save setting



Step 7: Click **Configuration > VPN > IPSec VPN > Configuration Provisioning** and enable Configuration Provisioning

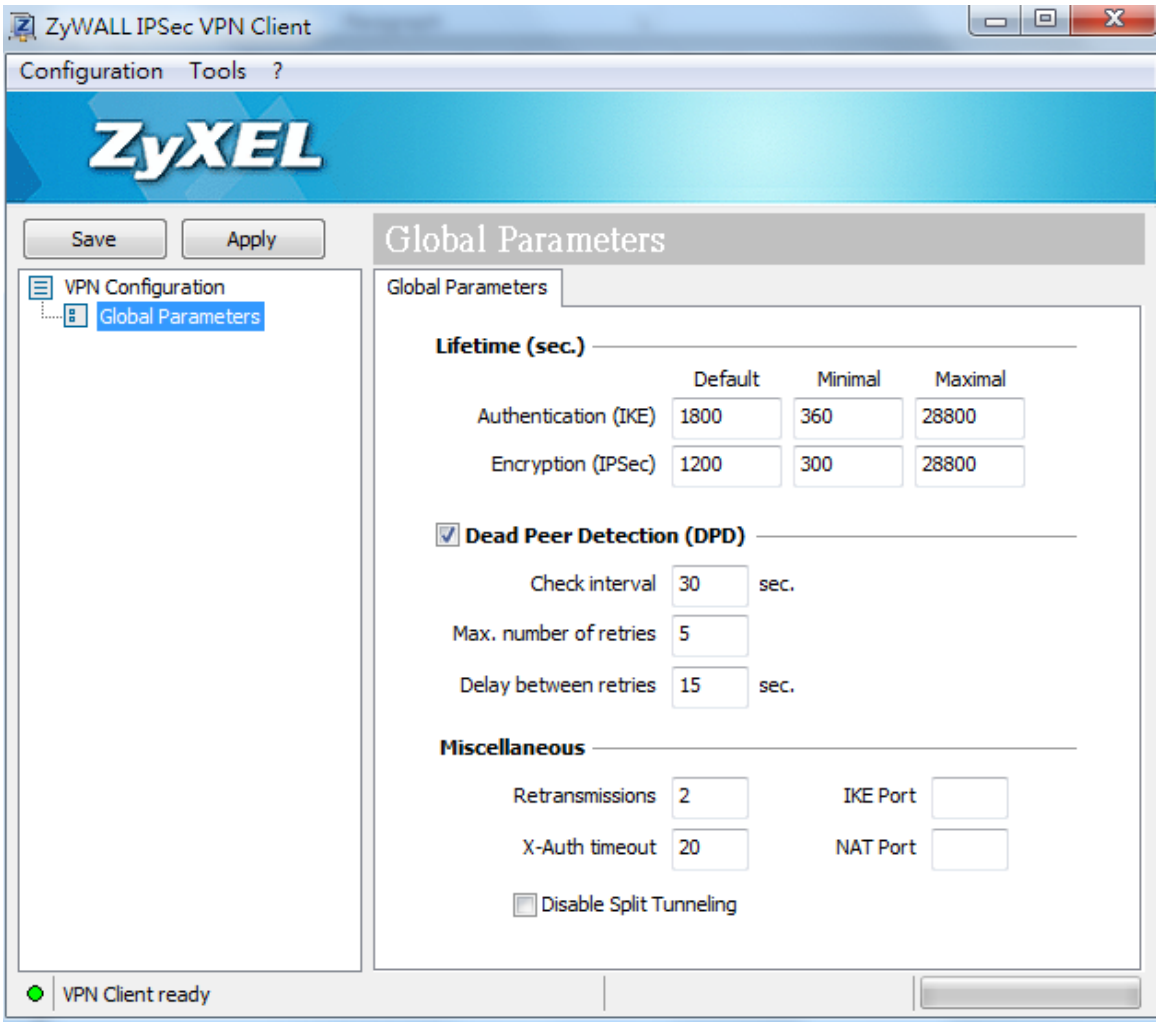


Step 8: Create a provisioning rule for any user

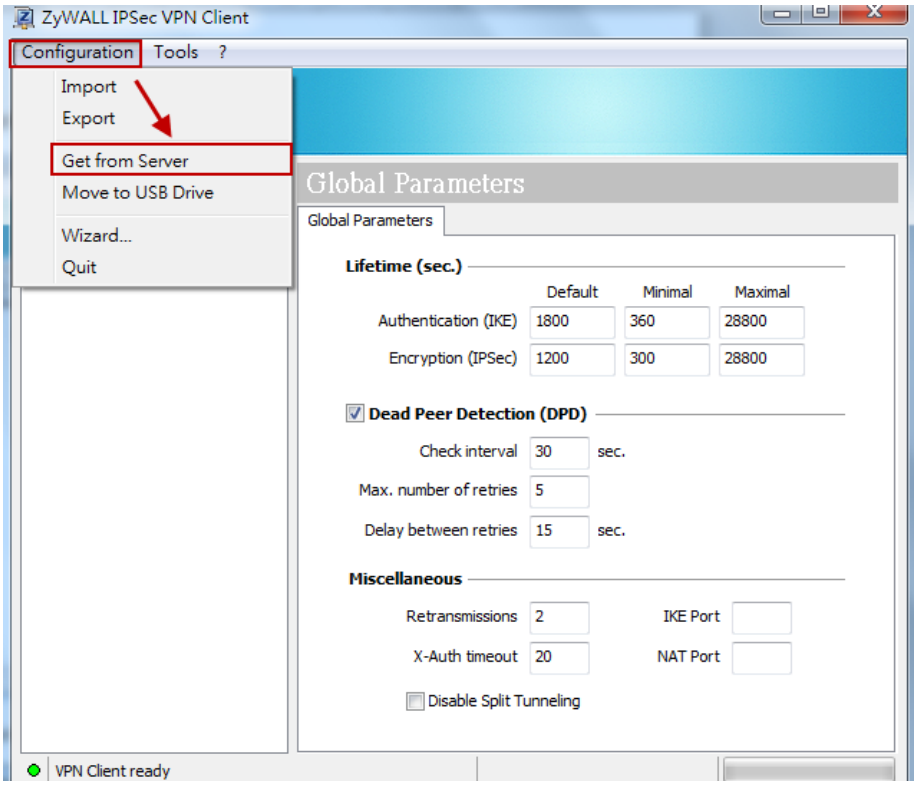


ZyWALL IPSec VPN Client software configuration

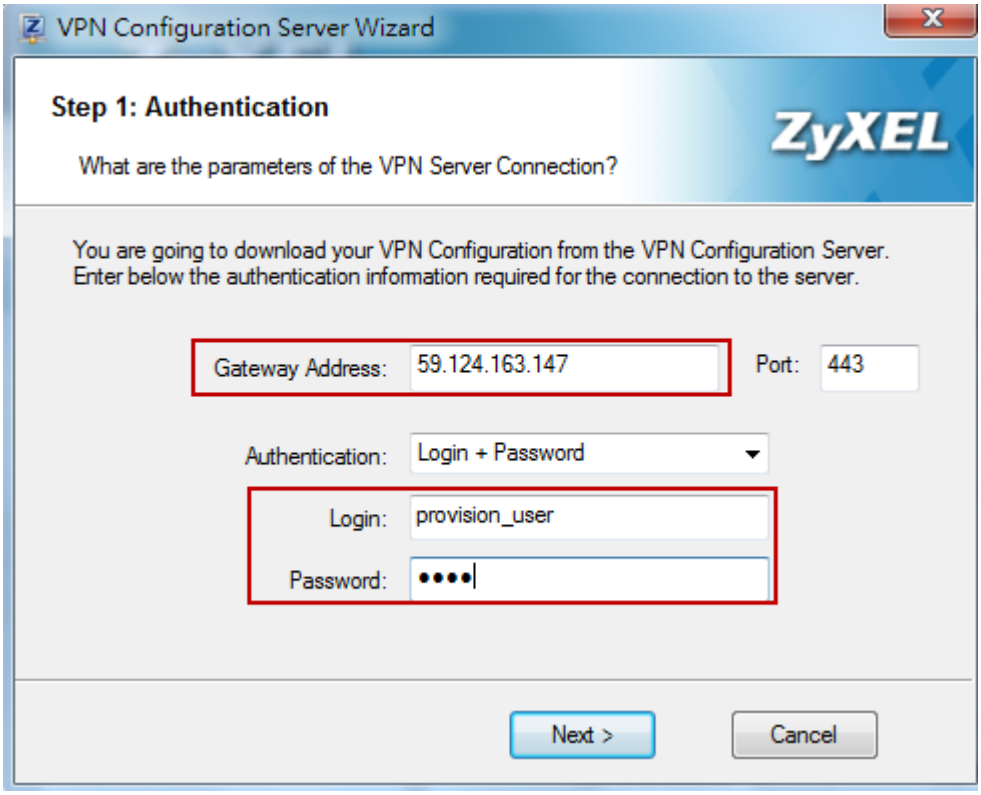
Step 1: Execute ZyWALL IPSec VPN Client



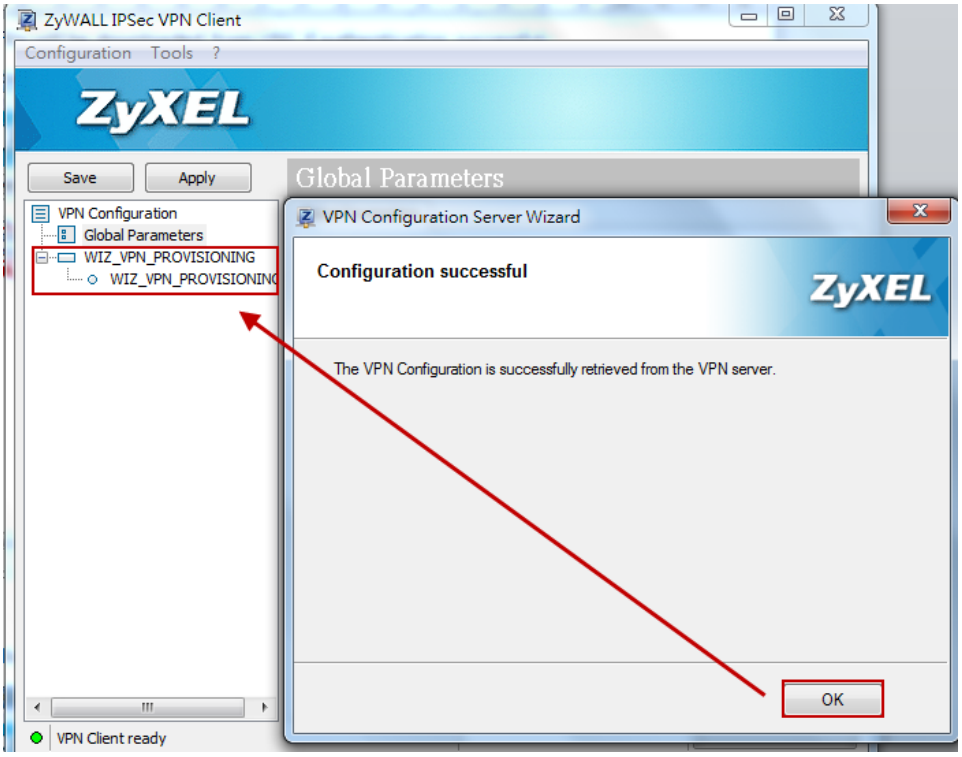
Step 2: Click **Configuration > Get from Server**



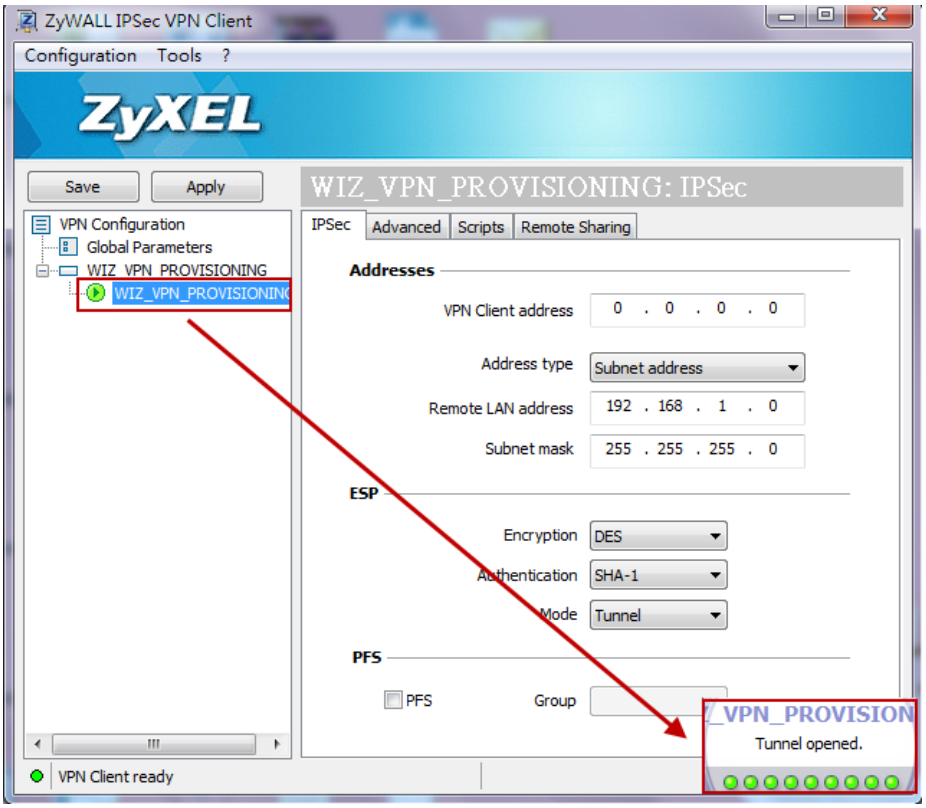
Step 3: Fill in authentication information and click “Next”



Step 4: The VPN profile will be downloaded from USG if authentication successful



Step 5: Double left click on the phase 2 profile to dial up IPSec VPN tunnel



Step 6: You can reach the internal server

系統管理員: C:\Windows\system32\cmd.exe - ping 192.168.1.34 -t

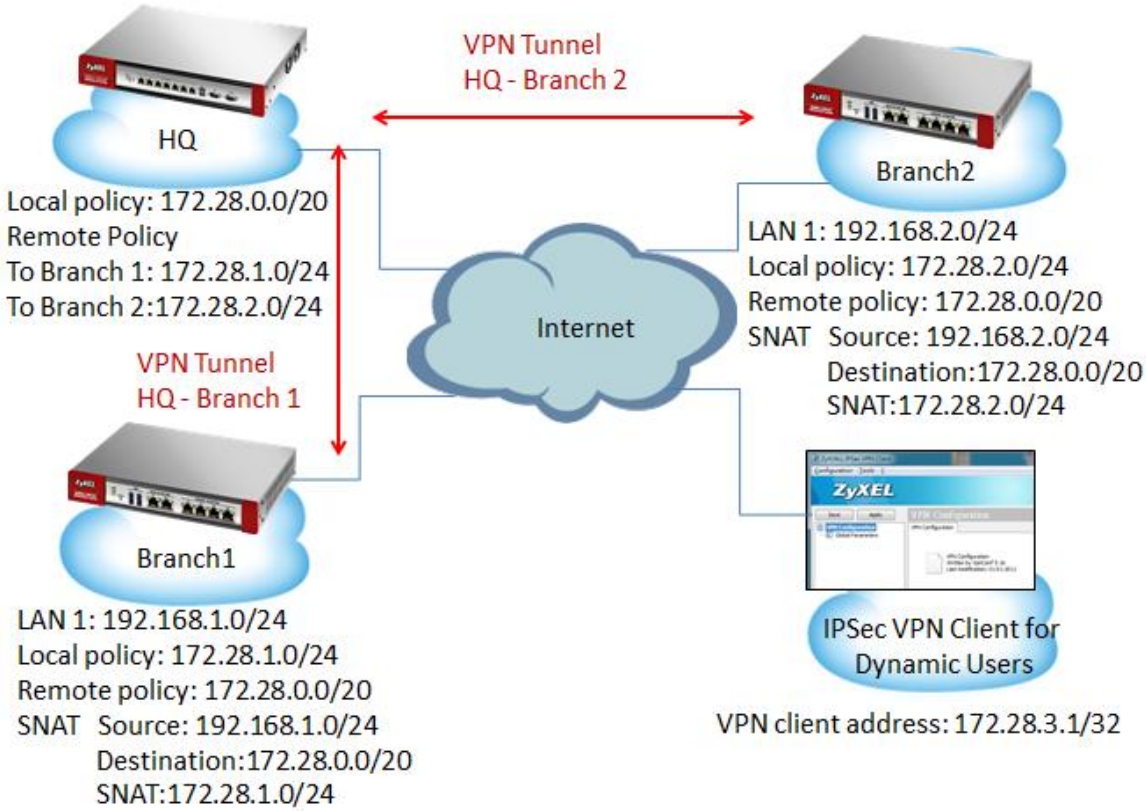
```
Microsoft Windows [版本 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Emily>ping 192.168.1.34 -t

Ping 192.168.1.34 (使用 32 位元組的資料):
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=2ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=2ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=2ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=2ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=126
```

Scenario 5 – Dynamic users communicate with HQ and all branch offices by using auto created VPN routes

5.1 Application Scenario

For world-wide enterprises, network communication between each branch and the headquarter office is very important. A VPN concentrator combines several IPSec VPN connections into one secure network for site-to-site VPN and reduces the number of VPN connections that need to be set up and maintained in the network. However a VPN concentrator is not suitable for every situation, many companies have several mobile users, travelers who are not located in a fixed office. When the network receives traffic from these dynamic users, we cannot know their subnets or IP addresses in advance.

Supposing a company has a headquarter and two branch offices. Two VPN tunnels are built up, each between the HQ and one of the branch offices. Undoubtedly, road warriors and telecommuters can access network of HQ and branch offices respectively by building IPSec VPN tunnel to each office. However, it is inconvenient and inefficient for mobile users to disconnect one VPN tunnel and then connect to another VPN tunnel if they just want to access some resource of branch office 1 while they're accessing resources of the HQ. How to let mobile users access the networks of HQ and branch offices at the same time with just one VPN tunnel? Now, you can achieve this goal via an "Auto-created VPN Route". If the subnets are aggregated, auto created VPN routes can achieve this request without VPN concentrator rules.


VPN Tunnel
HQ - Branch 2
HQ
Local policy: 172.28.0.0/20
Remote Policy
To Branch 1: 172.28.1.0/24
To Branch 2:172.28.2.0/24
Branch2
LAN 1: 192.168.2.0/24
Local policy: 172.28.2.0/24
Remote policy: 172.28.0.0/20
SNAT Source: 192.168.2.0/24
Destination:172.28.0.0/20
SNAT:172.28.2.0/24
Internet
VPN Tunnel
HQ - Branch 1
Branch1
LAN 1: 192.168.1.0/24
Local policy: 172.28.1.0/24
Remote policy: 172.28.0.0/20
SNAT Source: 192.168.1.0/24
Destination:172.28.0.0/20
SNAT:172.28.1.0/24
ZyXEL
IPSec VPN Client for
Dynamic Users
VPN client address: 172.28.3.1/32

5.2 Configuration Guide

Network conditions:

ZyWALL:

Site	WAN IP	VPN Tunnel	VPN Policy(Local-Remote)
HQ	10.59.3.201	HQ-Branch 1 HQ-Branch 2	172.28.0.0/20 - 172.28.1.0/24 172.28.0.0/20 - 172.28.2.0/24
Branch 1	10.59.3.200	Branch 1-HQ	172.28.1.0/24 - 172.28.0.0/20 Outbound Traffic (SNAT) Source: 192.168.1.0/24 Destination:172.28.0.0/20 SNAT:172.28.1.0/24 Inbound Traffic(DNAT) Original IP: 172.28.1.0/24 Mapped IP: 192.168.1.0/24
Branch 2	10.59.3.37	Branch 2-HQ	172.28.2.0/24 - 172.28.0.0/20 Outbound Traffic (SNAT) Source: 192.168.2.0/24 Destination:172.28.0.0/20 SNAT:172.28.2.0/24 Inbound Traffic(DNAT) Original IP: 172.28.2.0/24 Mapped IP: 192.168.2.0/24

Goals to achieve:

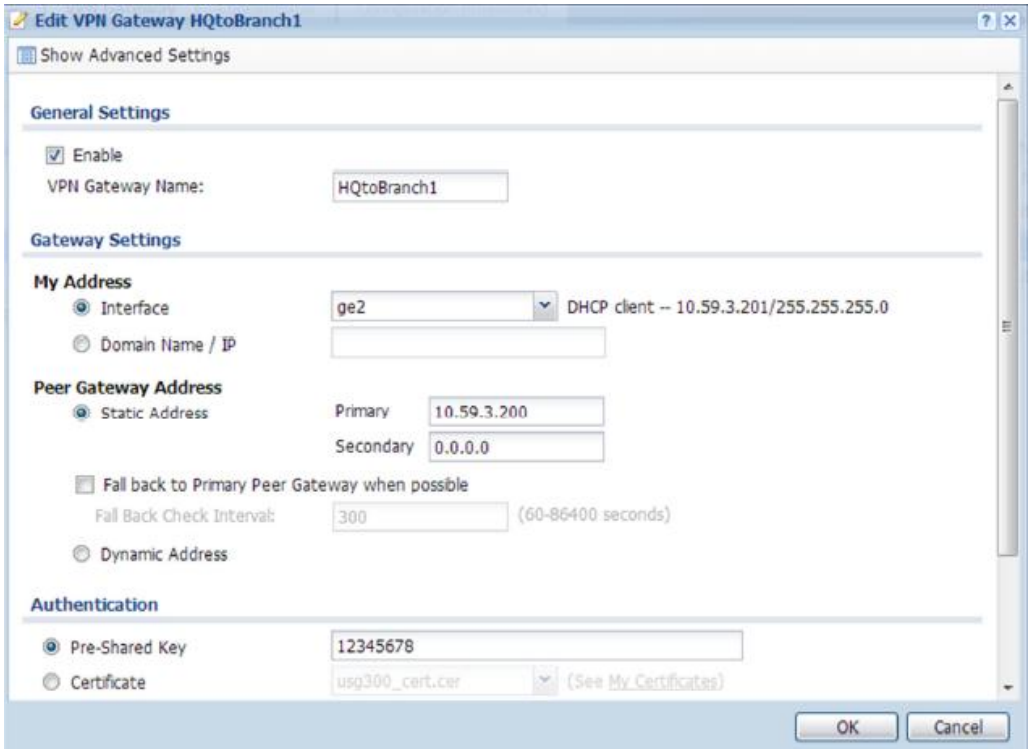
Mobile users can communicate with headquarters and all branch offices with only one VPN tunnel.

ZyWALL configuration:

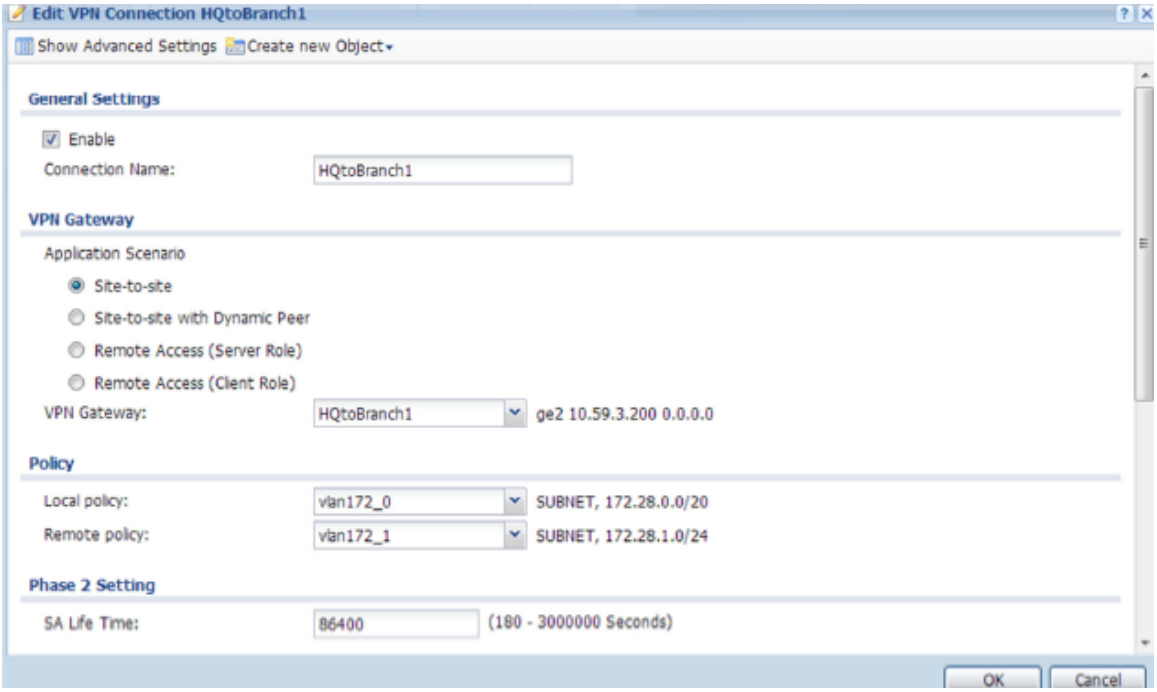
Task 1. Establish IPSec VPN between HQ and Branch 1.

HQ configuration

Step1. Configuration > VPN > IPSec VPN > VPN Gateway > Edit

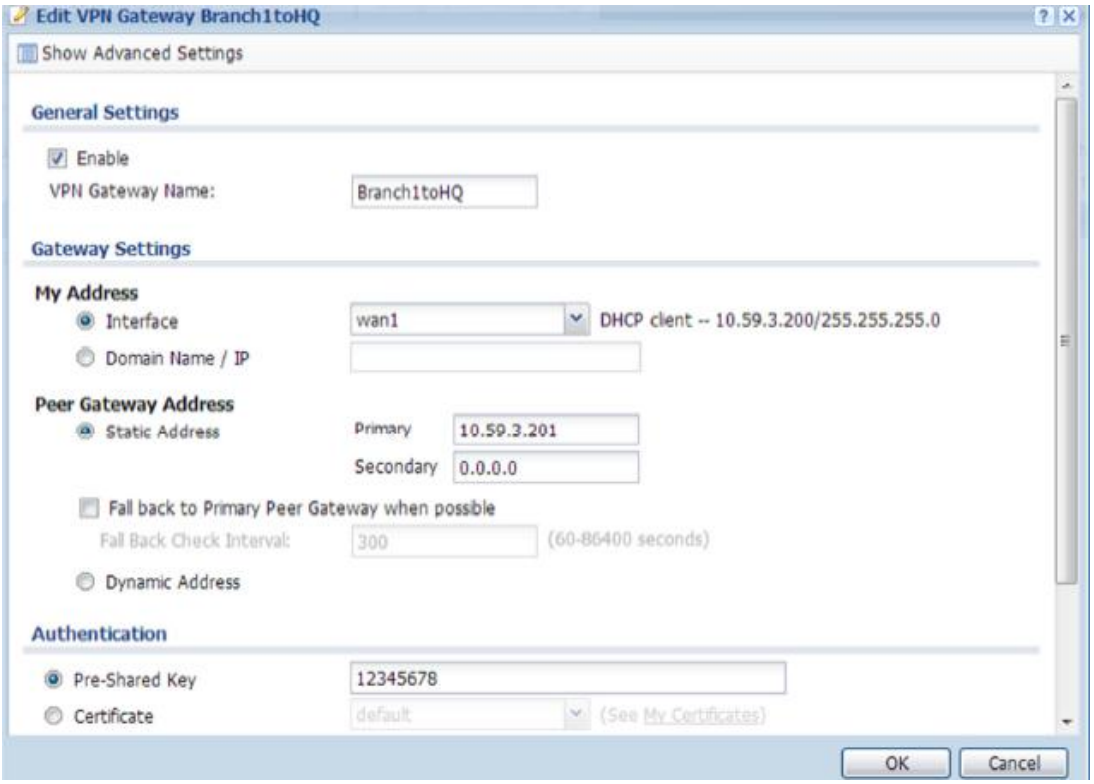


Step2. Configuration > VPN > IPSec VPN > VPN Connection > Edit

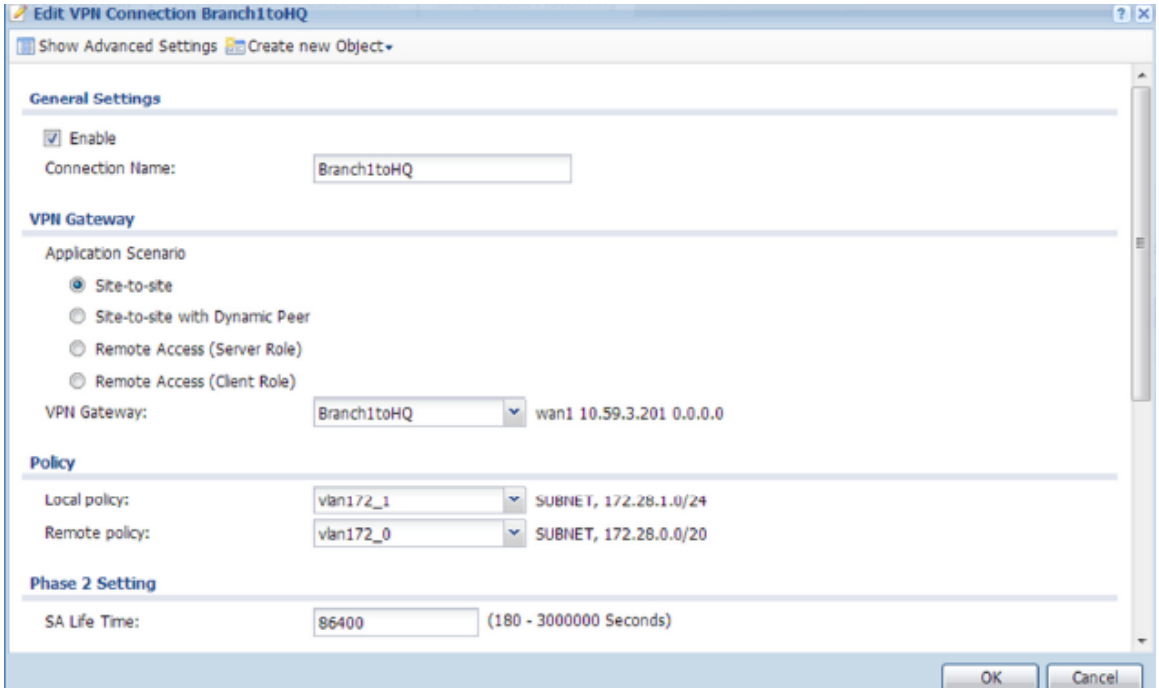


Branch 1 configuration

Step 1. Configuration > VPN > IPSec VPN > VPN Gateway > Edit



Step 2. Configuration > VPN > IPSec VPN > VPN Connection > Edit

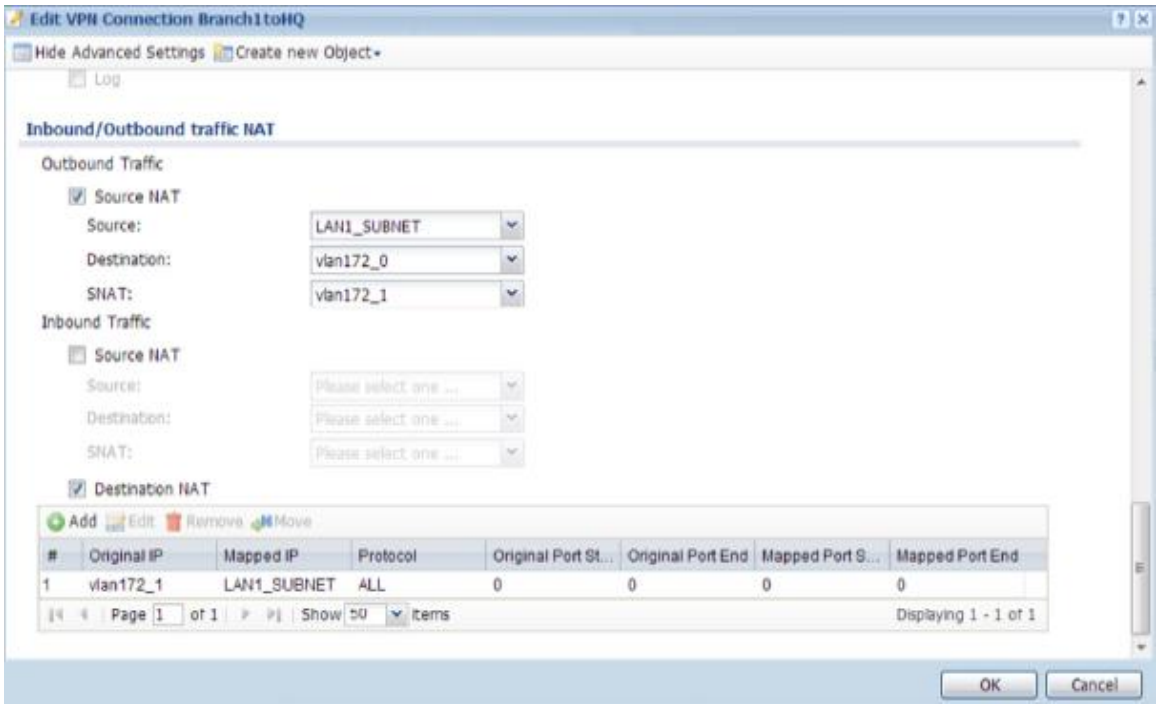


Step 3. Do an SNAT rule in VPN tunnel.

Source: 192.168.1.0/24

Destination:172.28.0.0/20

SNAT:172.28.1.0/24



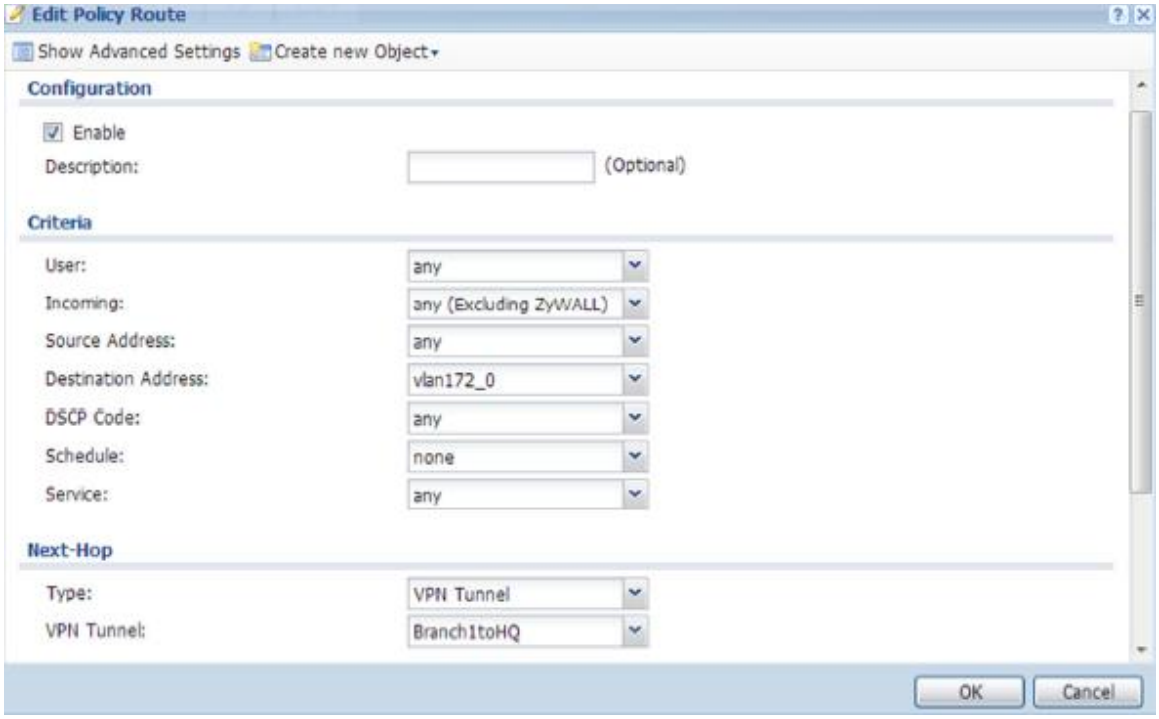
Step 4. Configuration > Network > Routing > Policy Route,

Add a policy route

Source: any

Destination: 172.28.0.0/20

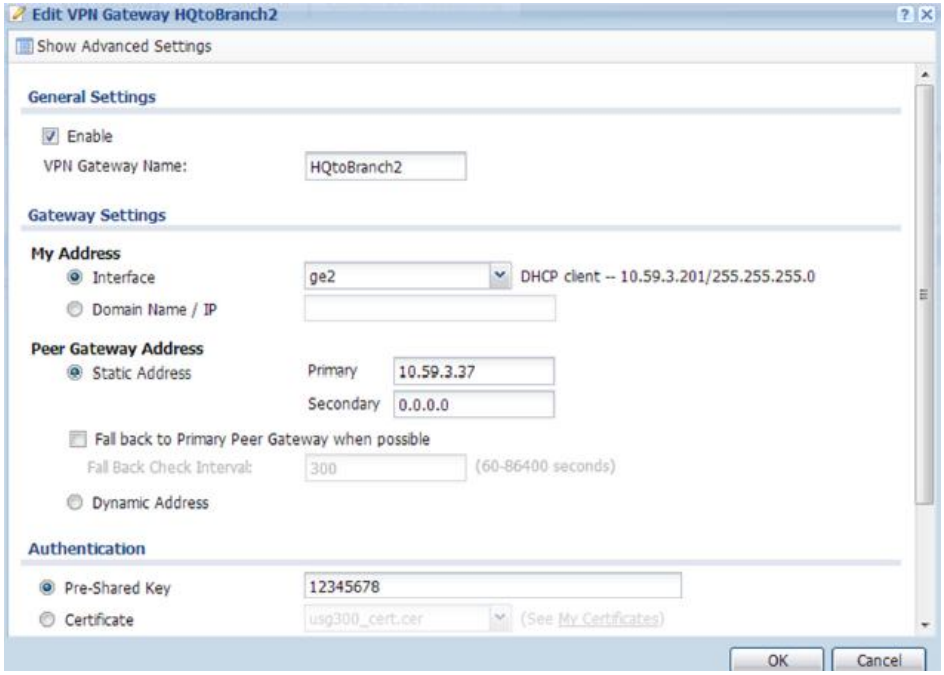
Next-hop: VPN tunnel



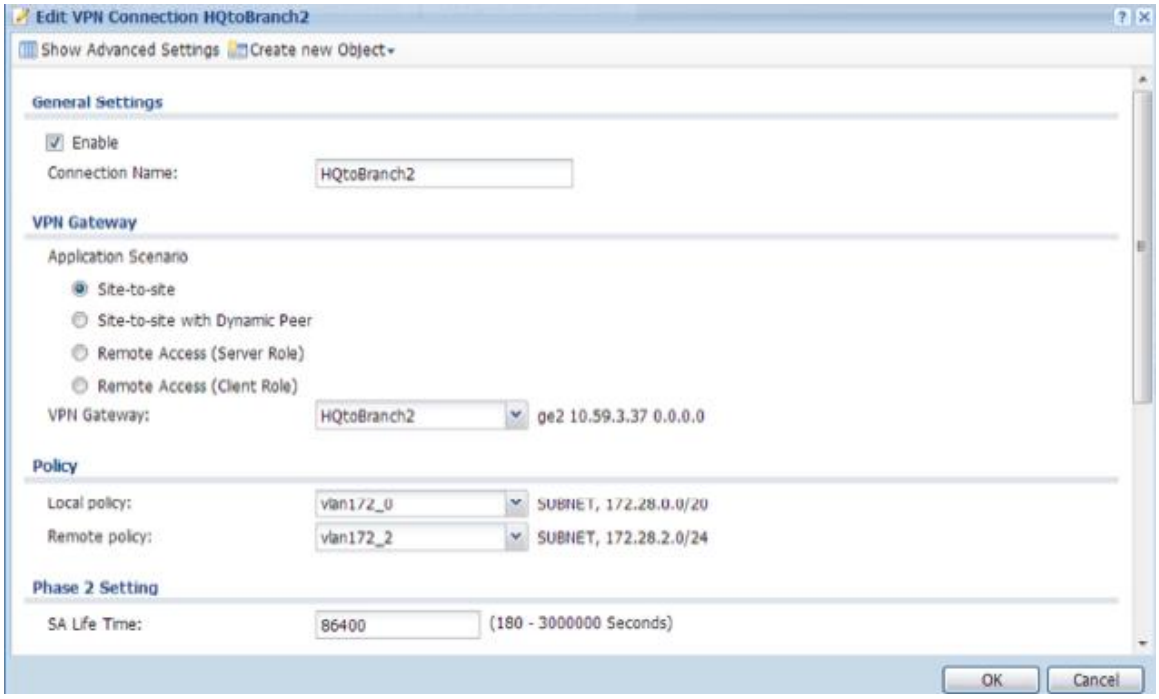
Task 2. Establish IPSec VPN between HQ and Branch 2

HQ configuration

Step 1. Configuration > VPN > IPSec VPN > VPN Gateway > Edit

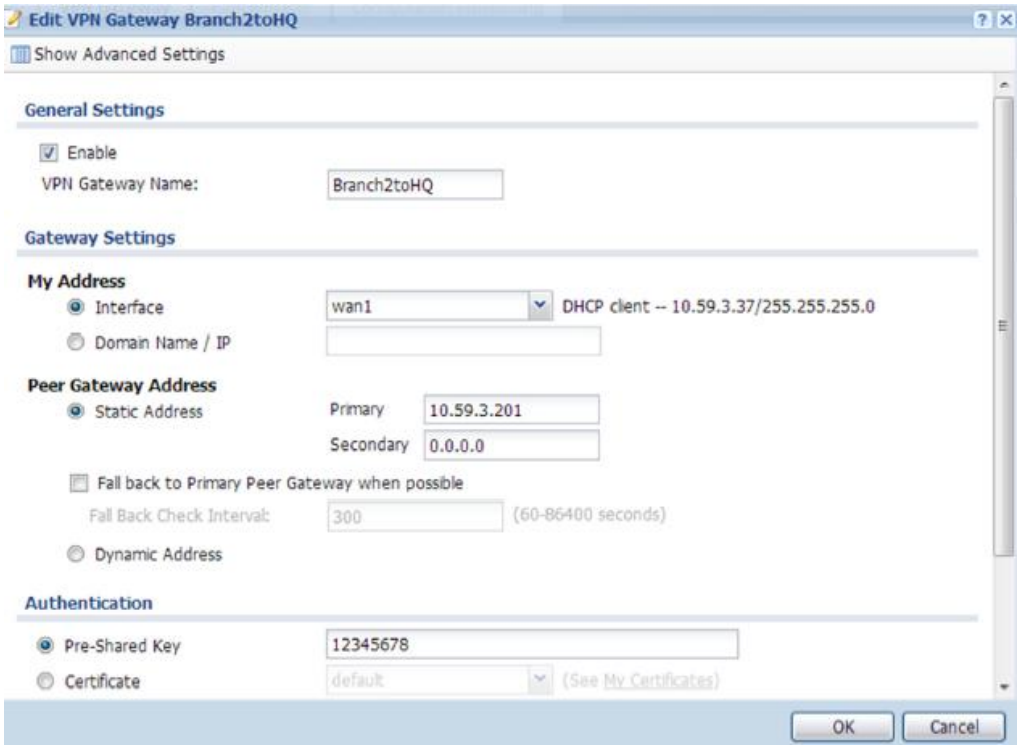


Step 2. Configuration > VPN > IPSec VPN > VPN Connection > Edit

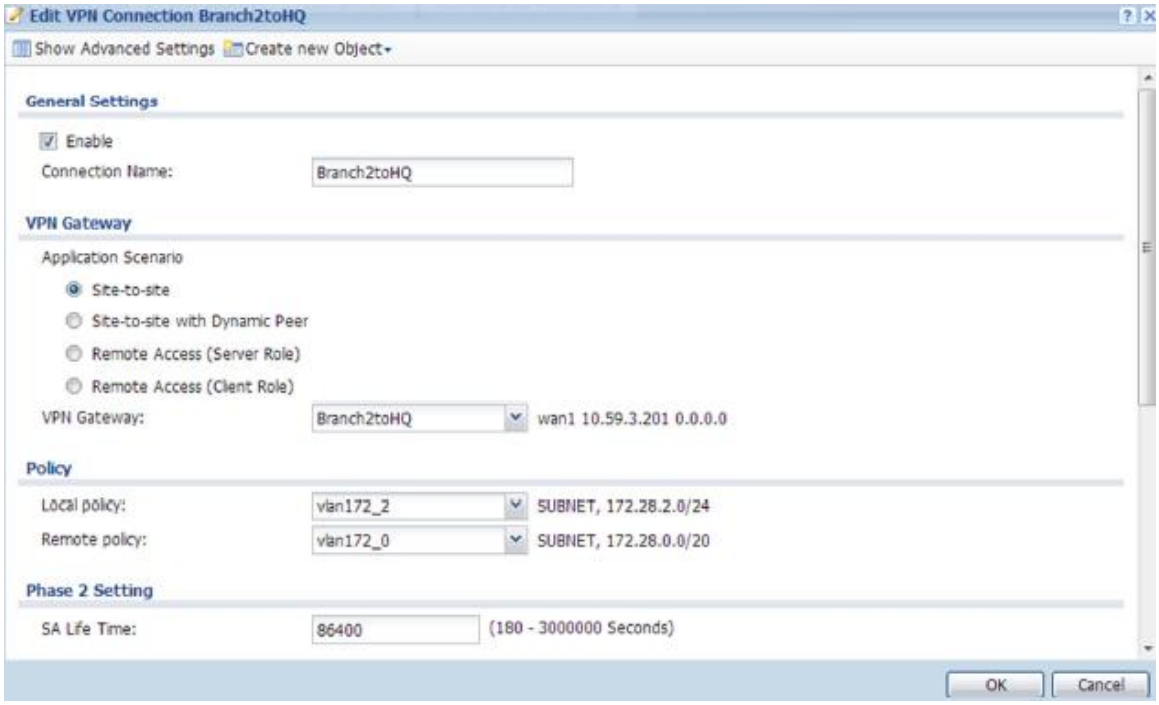


Branch 2 configuration

Step1. Configuration > VPN > IPSec VPN > VPN Gateway > Edit



Step2. Configuration > VPN > IPSec VPN > VPN Connection > Edit

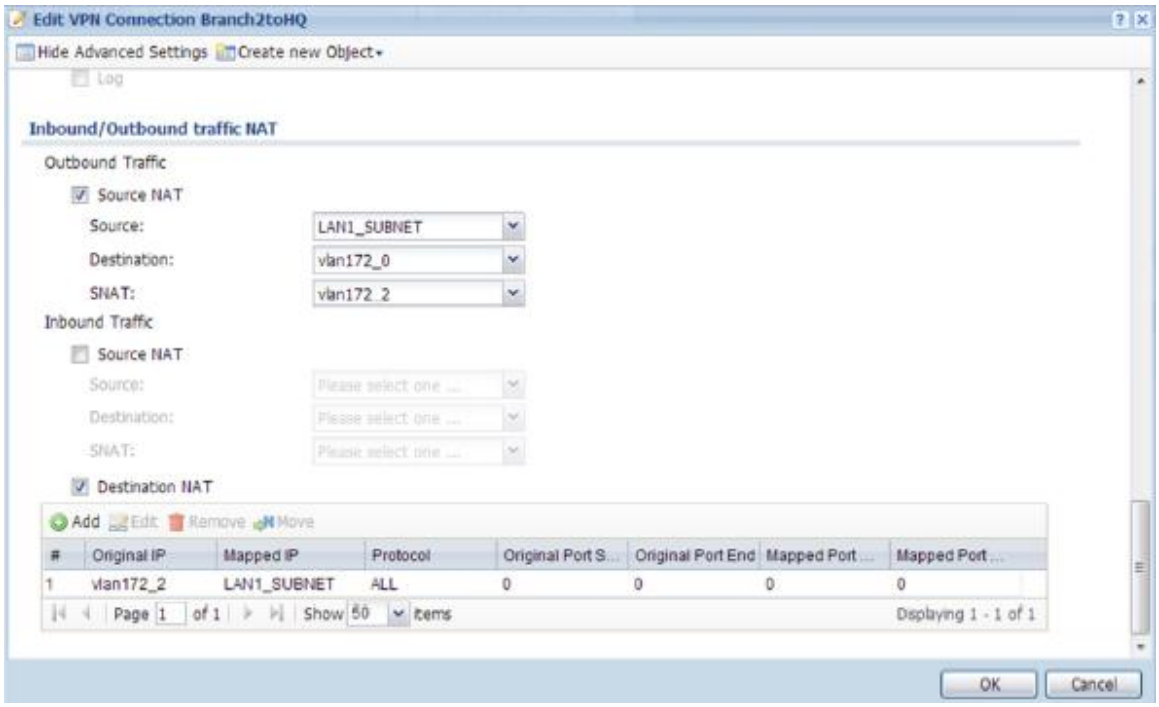


Step 3. Do an SNAT rule in VPN tunnel.

Source: 192.168.2.0/24

Destination:172.28.0.0/20

SNAT:172.28.2.0/24



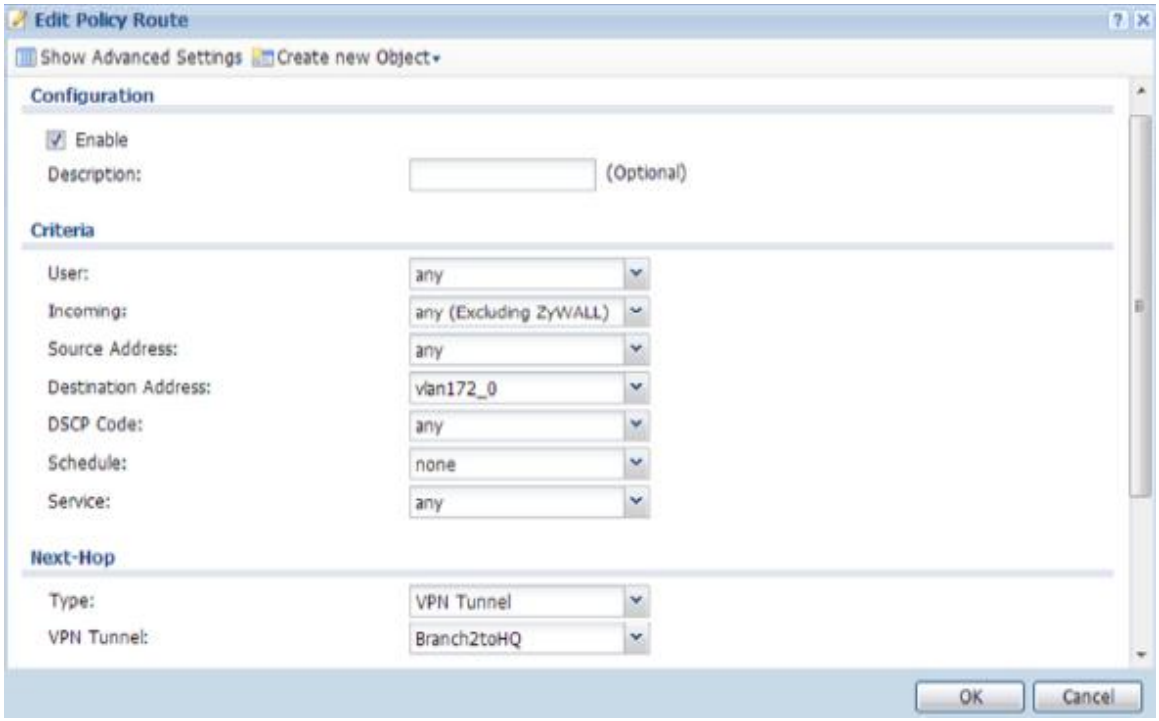
Step 4. Configuration > Network > Routing > Policy Route,

Add a policy route

Source: any

Destination: 172.28.0.0/20

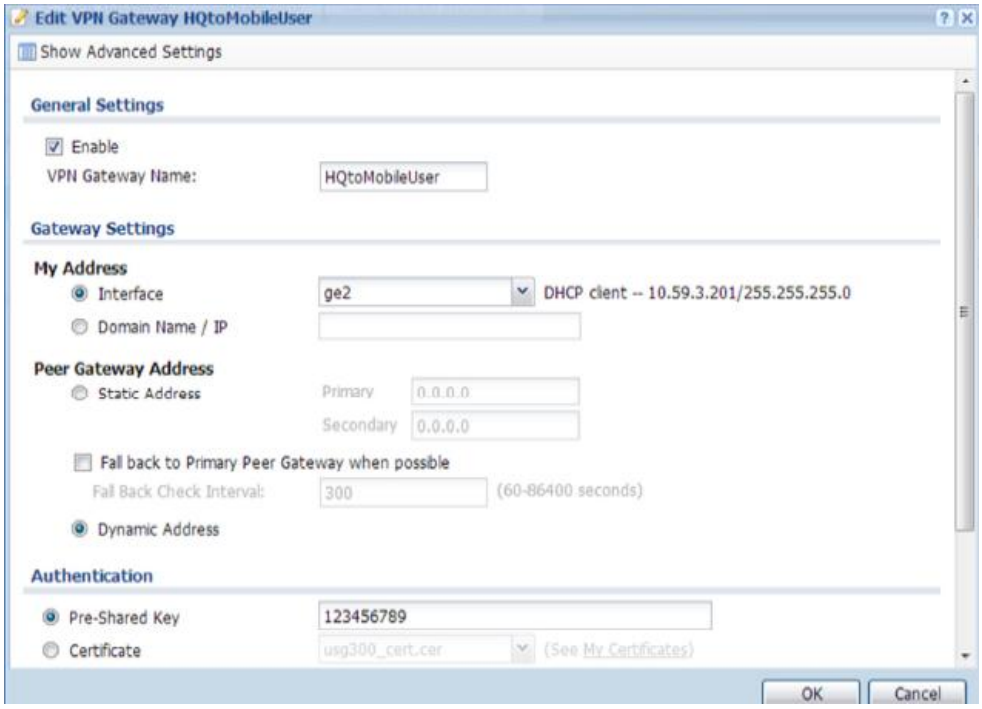
Next-hop: VPN tunnel



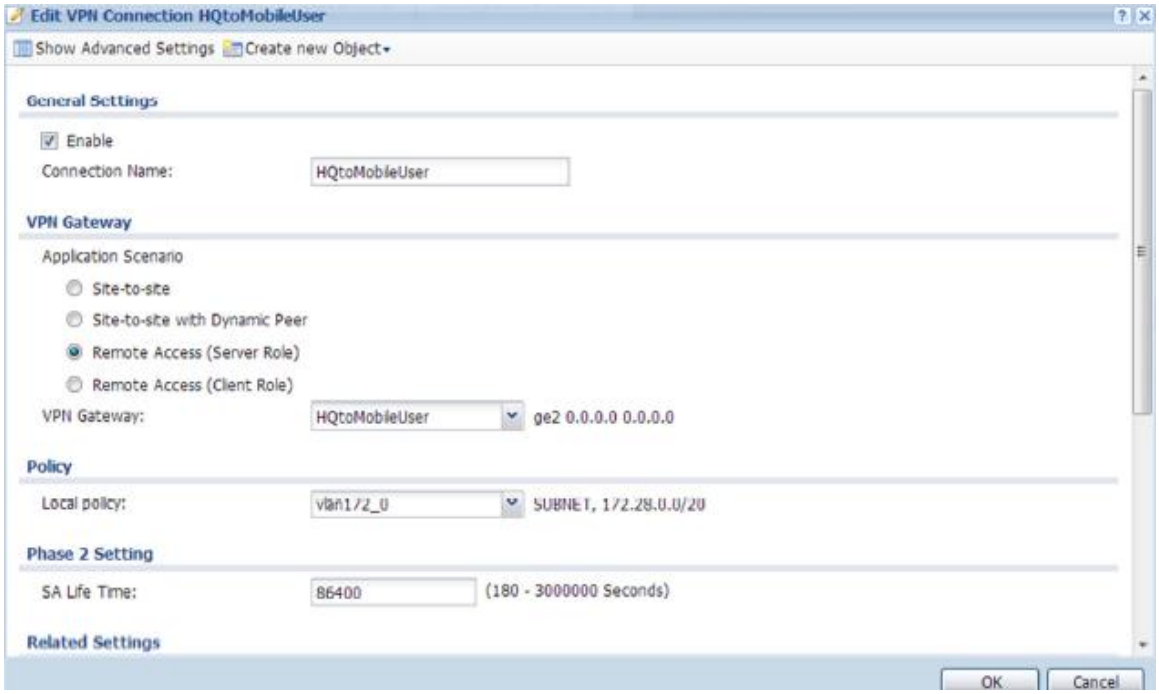
Task 3. Establish Dynamic VPN for mobile users

HQ configuration

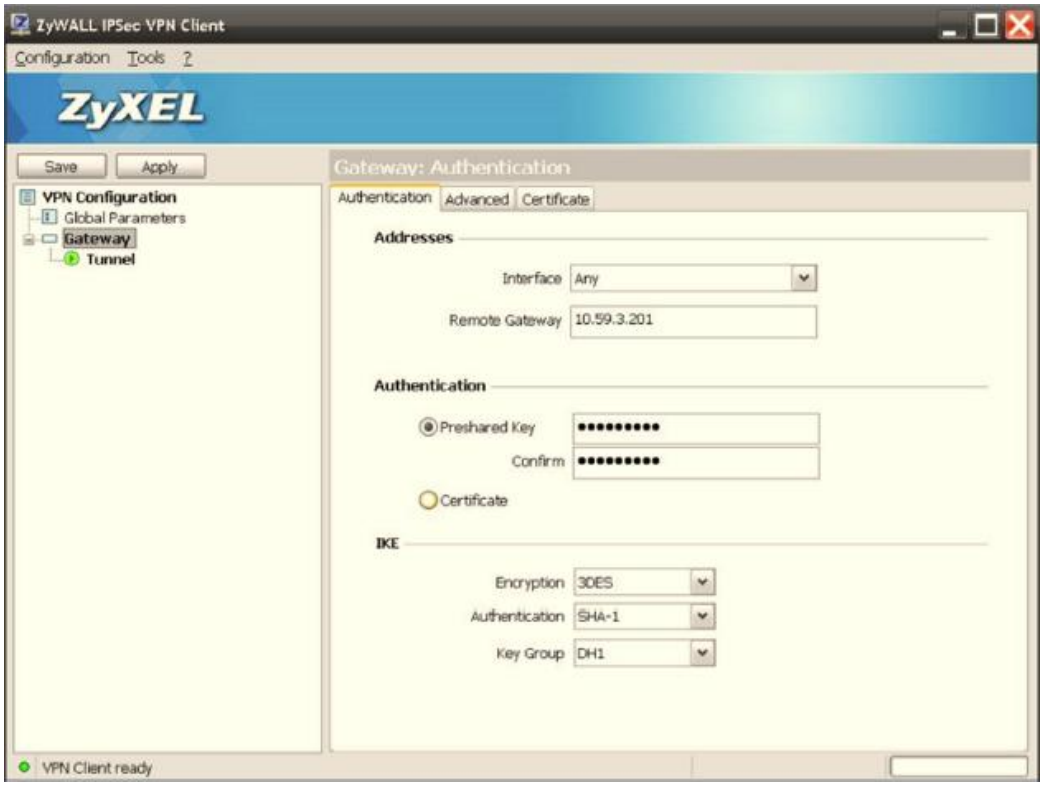
Step 1. Configuration > VPN > IPSec VPN > VPN Gateway > Edit



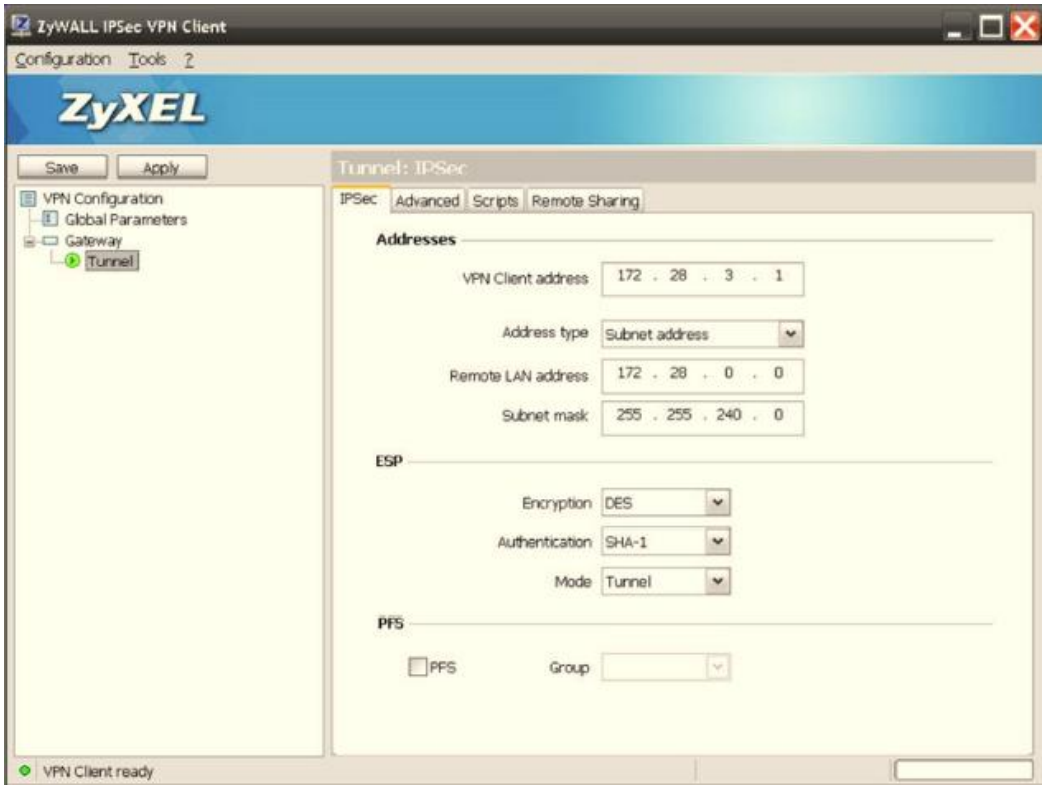
Step 2. Configuration > VPN > IPSec VPN > VPN Connection > Edit



Step 3. IPSec VPN client setting

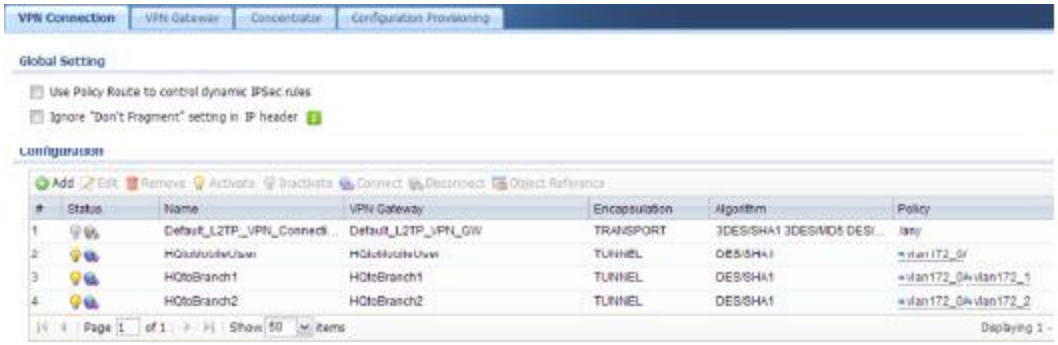


Step 4. In Phase 2, assign one IP for IPSec VPN Client manually.



Step 5. Disable “Use Policy Route to control dynamic IPSec rules” on HQ device.

Configuration > VPN > IPSec VPN > VPN Connection > Global Setting



HQ Routing Packet Flow

Maintenance > Packet Flow Explore > Routing Status

Verification

IPSec VPN client can ping HQ, branch 1 and branch 2 successfully at the same time.

```
C:\Documents and Settings\user>ping 172.28.0.33

Pinging 172.28.0.33 with 32 bytes of data:

Reply from 172.28.0.33: bytes=32 time=1ms TTL=126
Reply from 172.28.0.33: bytes=32 time=2ms TTL=126
Reply from 172.28.0.33: bytes=32 time=3ms TTL=126
Reply from 172.28.0.33: bytes=32 time=1ms TTL=126
```

```
C:\Documents and Settings\user>ping 172.28.1.33

Pinging 172.28.1.33 with 32 bytes of data:

Reply from 172.28.1.33: bytes=32 time=4ms TTL=123
Reply from 172.28.1.33: bytes=32 time=3ms TTL=123
Reply from 172.28.1.33: bytes=32 time=3ms TTL=123
Reply from 172.28.1.33: bytes=32 time=3ms TTL=123
```

```
C:\Documents and Settings\user>ping 172.28.2.33

Pinging 172.28.2.33 with 32 bytes of data:

Reply from 172.28.2.33: bytes=32 time=7ms TTL=123
Reply from 172.28.2.33: bytes=32 time=3ms TTL=123
Reply from 172.28.2.33: bytes=32 time=3ms TTL=123
Reply from 172.28.2.33: bytes=32 time=3ms TTL=123
```