

2013

ZyWALL Series Support Note V1



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:

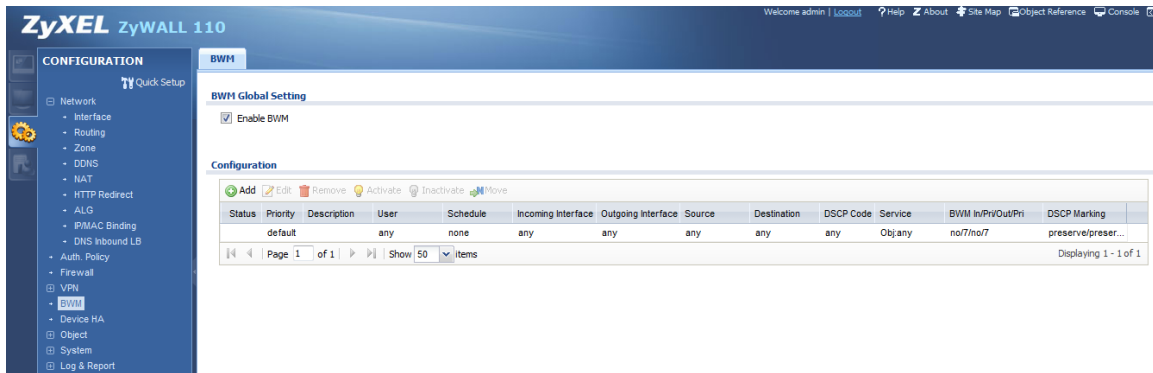
- WAN download bandwidth: 2M
- WAN upload bandwidth: 1M

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**.

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

Global

Enable BWM

Configuration

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 Objects: 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

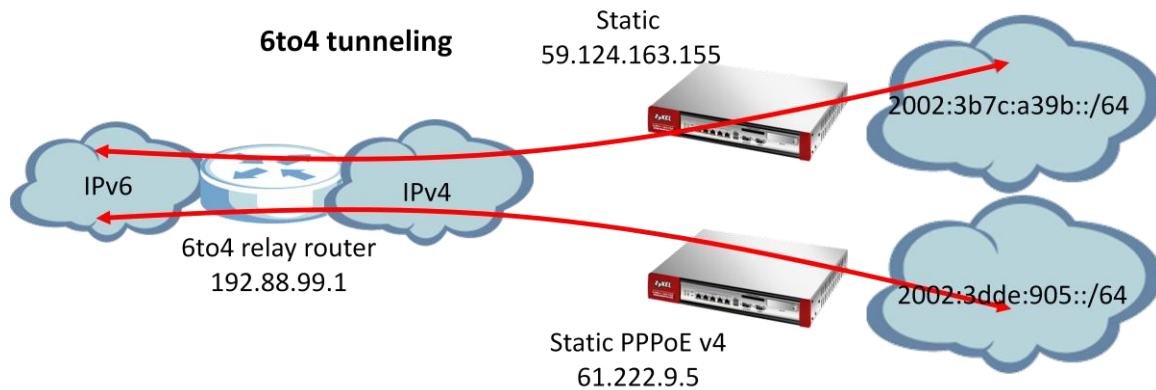
Maximize Bandwidth Usage Maximum: 0 kbps

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:

ZyWALL:

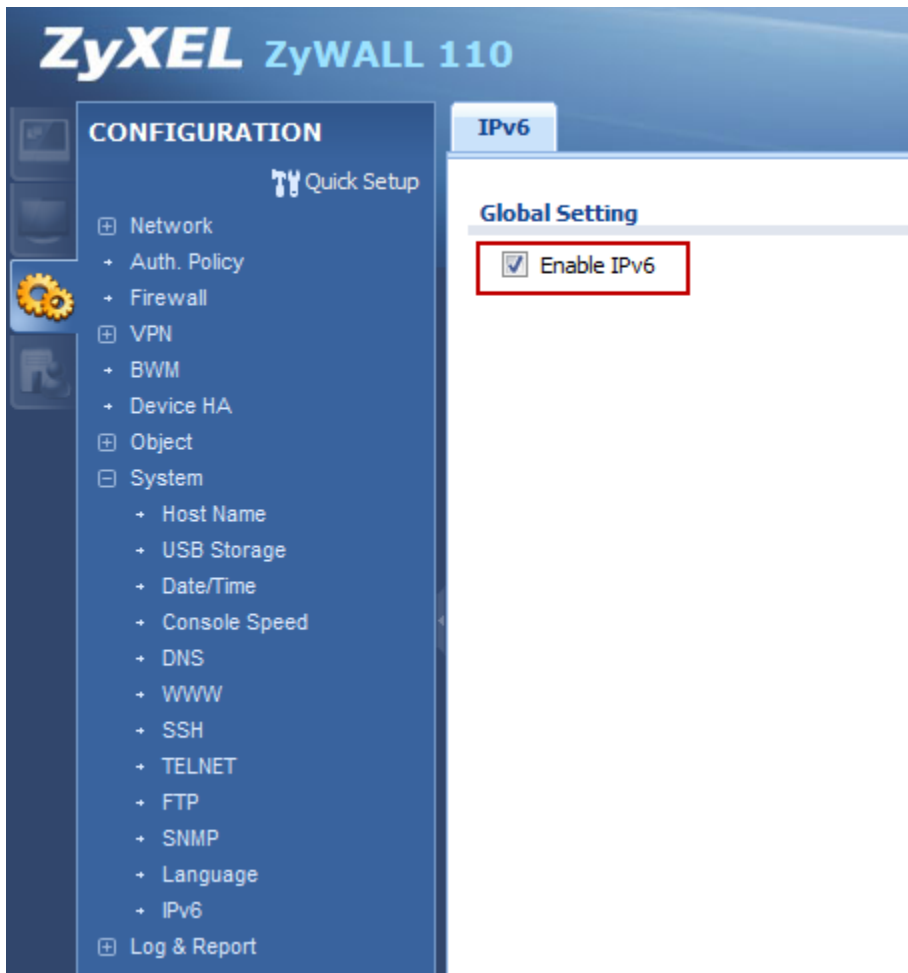
WAN1: 59.124.163.155(Static)

Goal to achieve:

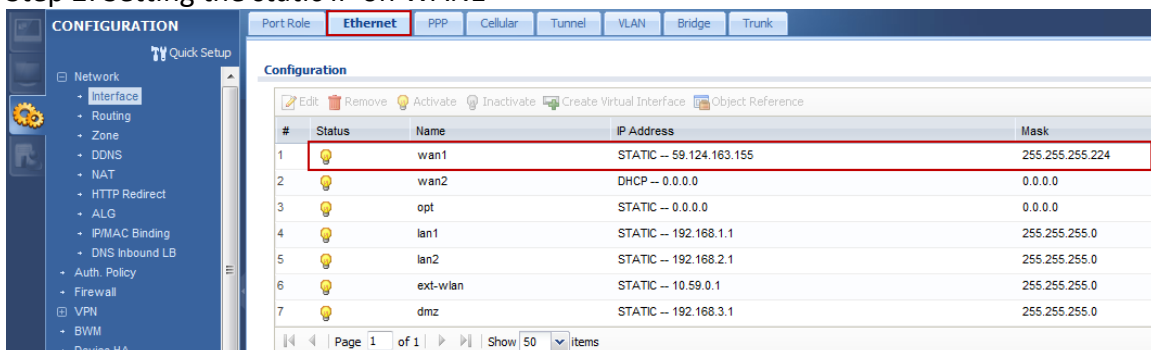
A ZyWALL will assign IPv6 IP address to the clients behind it, and the clients can access remote IPv6 network by using the ZyWALL 6to4 tunnel.

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.

Edit Ethernet

IPv6 View Hide Advanced Settings Create new Object

General Settings

Enable Interface

General IPv6 Setting

Enable IPv6

Interface Properties

Interface Type: internal

Interface Name: lan1

Port: P4

Zone: LAN1

MAC Address: 00:13:49:00:00:04

Description: (Optional)

- (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**.

IPv6 Address Assignment

Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: fe80::213:49ff:fe00:4/64

IPv6 Address/Prefix Length: 2002:3b7c:a39b::/64 (Optional)

DHCPv6 Setting

DHCPv6: N/A

IPv6 Router Advertisement Setting

Enable Router Advertisement

Router Preference: Medium

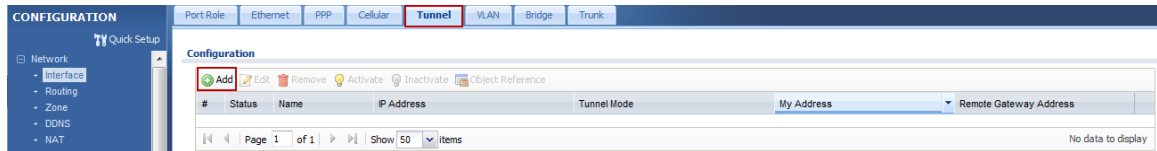
Advertised Prefix Table

#	IPv6 Address/Prefix Length
1	2002:3b7c:a39b::/64

Page 1 of 1 Show 50 items No data to display

Step 4: Enable 6 to 4 tunnel.

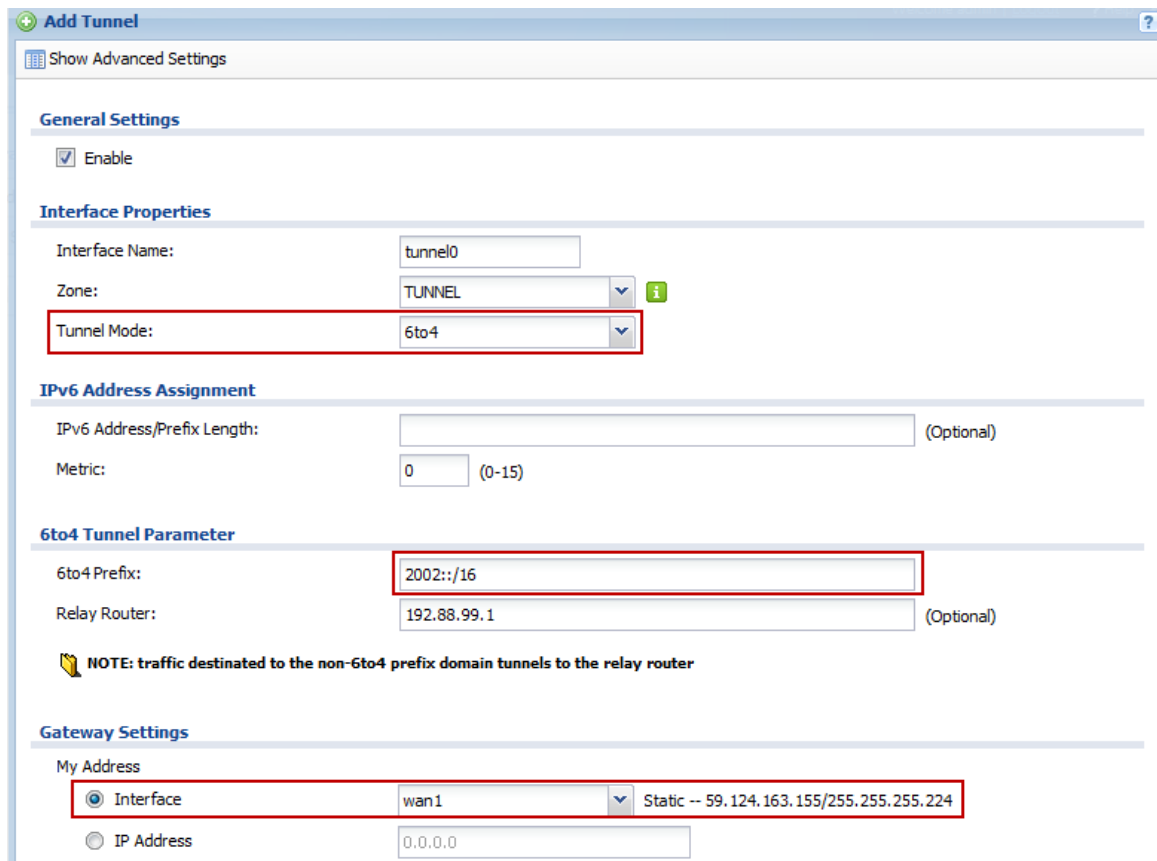
(1) Go to Configuration > Interface > Tunnel > Click Add button



(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

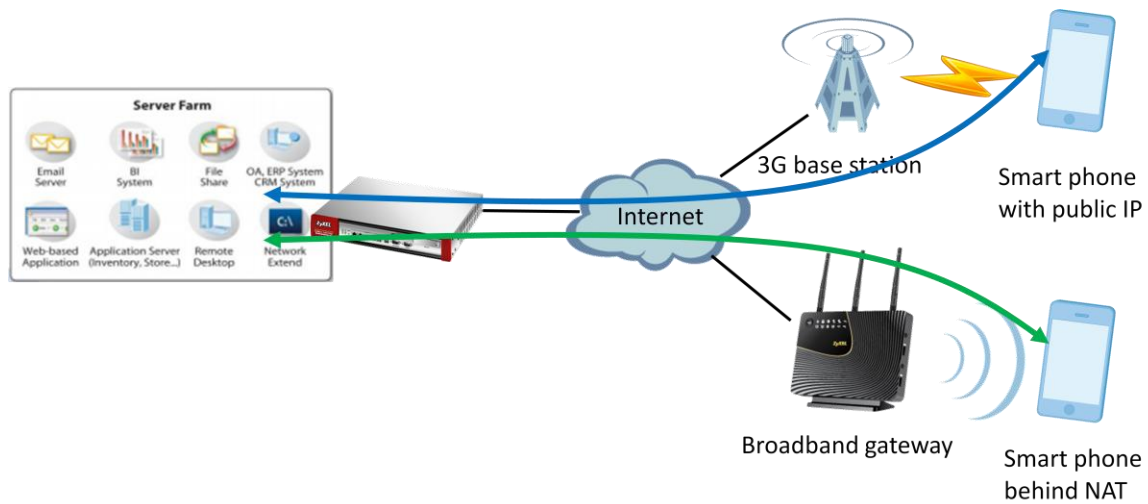
A screenshot of the 'Add Tunnel' configuration page. The page has a 'Show Advanced Settings' button. Under 'General Settings', the 'Enable' checkbox is checked. Under 'Interface Properties', the 'Interface Name' is 'tunnel0', the 'Zone' is 'TUNNEL', and the 'Tunnel Mode' is '6to4'. Under 'IPv6 Address Assignment', the 'IPv6 Address/Prefix Length' field is empty and marked as optional, and the 'Metric' is '0'. Under '6to4 Tunnel Parameter', the '6to4 Prefix' is '2002::/16' and the 'Relay Router' is '192.88.99.1'. A note states: 'NOTE: traffic destined to the non-6to4 prefix domain tunnels to the relay router'. Under 'Gateway Settings', the 'My Address' is set to 'Interface wan1' with a static IP of '59.124.163.155/255.255.255.224'. The 'IP Address' option is also visible with '0.0.0.0' as a placeholder.

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:

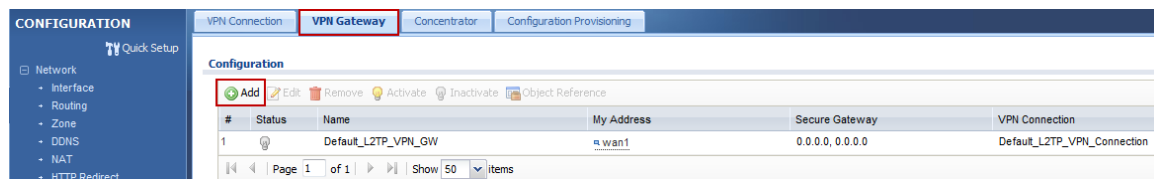
- Encapsulation Mode: Transport mode
- Active protocol: ESP
- Encryption algorithm: 3DES/3DES/DES
- Authentication algorithm:
SHA1/MD5/SHA1
- Perfect Forward Secrecy: none

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:

Gateway Settings

My Address

Interface Static -- 59.124.163.150/255.255.255.224

Domain Name / IP

Peer Gateway Address

Static Address

Primary
Secondary

Fall back to Primary Peer Gateway when possible
Fall Back Check Interval: (60-86400 seconds)

Dynamic Address

Authentication

Pre-Shared Key

Certificate

Local ID Type:

Content:

Peer ID Type:

Content:

Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)

Negotiation Mode:

Proposal

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

Key Group:

NAT Traversal

Dead Peer Detection (DPD)

Extended Authentication

Enable Extended Authentication

Server Mode

Client Mode

User Name :

Password:

Retype to Confirm:

CONFIGURATION

VPN Connection **VPN Gateway** Concentrator Configuration Provisioning

Quick Setup

Network

- Interface
- Routing
- Zone
- DDNS
- NAT
- HTTP Redirect
- ALG

Configuration

[Add](#)
[Edit](#)
[Remove](#)
[Activate](#)
[Inactivate](#)
[Object Reference](#)

#	Status	Name	My Address	Secure Gateway	VPN Connection
1		Default_L2TP_VPN_GW	wan1	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection
2		l2tp_gateway	wan1	0.0.0.0, 0.0.0.0	

Page 1 of 1 | Show 50 items

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

VPN Connection VPN Gateway Concentrator Configuration Provisioning

Global Setting

- Use Policy Route to control dynamic IPsec rules
- Ignore "Don't Fragment" setting in IP header

Configuration

[Add](#)
[Edit](#)
[Remove](#)
[Activate](#)
[Inactivate](#)
[Connect](#)
[Disconnect](#)
[Object Reference](#)

#	Status	Name	VPN Gateway	Encapsulation	Algorithm	Policy
1		Default_L2TP_VPN_Connection	Default_L2TP_VPN_GW	TRANSPORT	3DES/SHA1 3DES/MD5 DES/SHA1	/any

Page 1 of 1 | Show 50 items

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

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

#	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 ...

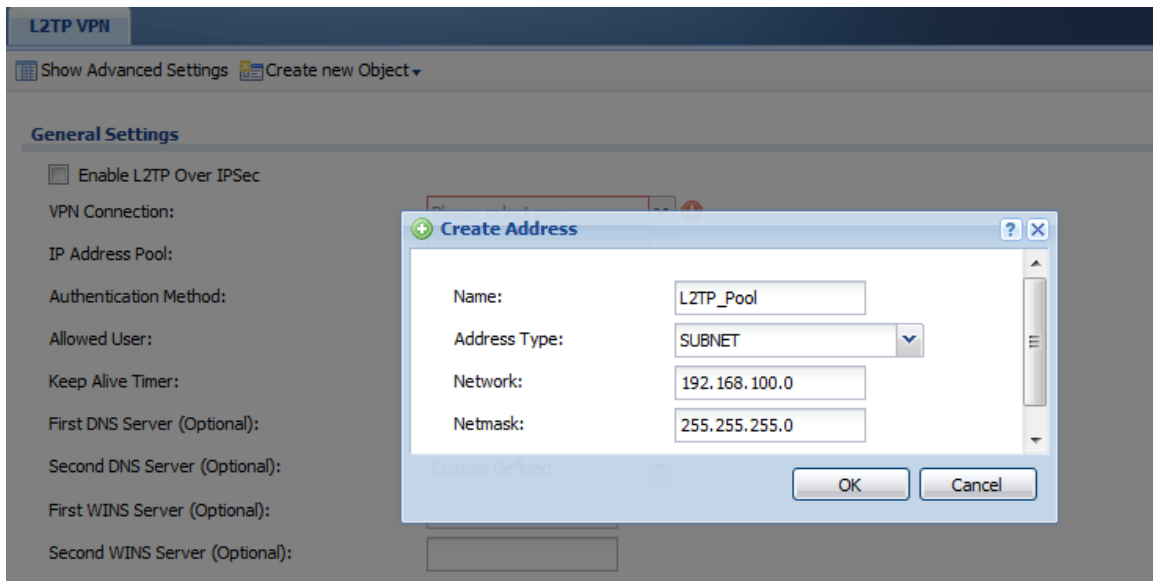
Destination NAT

#	Original IP	Mapped IP	Protocol	Original Port Start	Original Port End	Mapped Port Start	Mapped Port End
No data to display							

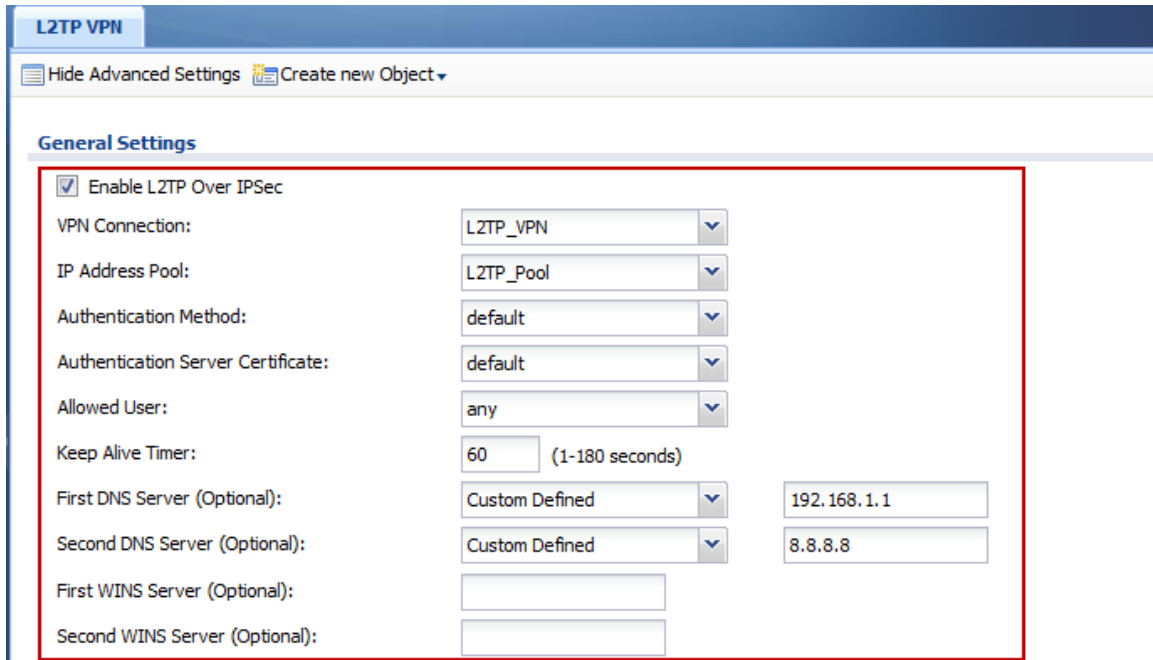
Page 1 of 1 Show 50 items

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.

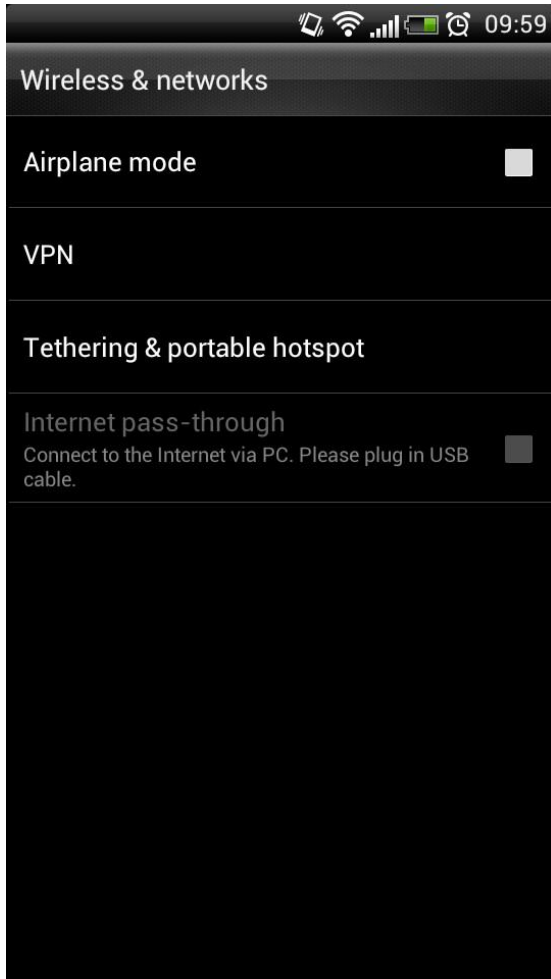
The screenshot shows the 'Session Monitor' interface with a table of 'Current L2TP Session' data. The table has columns for '#', 'User Name', 'Hostname', 'Assigned IP', and 'Public IP'. There is one entry in the table.

#	User Name	Hostname	Assigned IP	Public IP
1	l2tpuser	-iPhone	192.168.100.1	116.59.252.188

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Android mobile client configuration

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



Step 2: Add VPN network



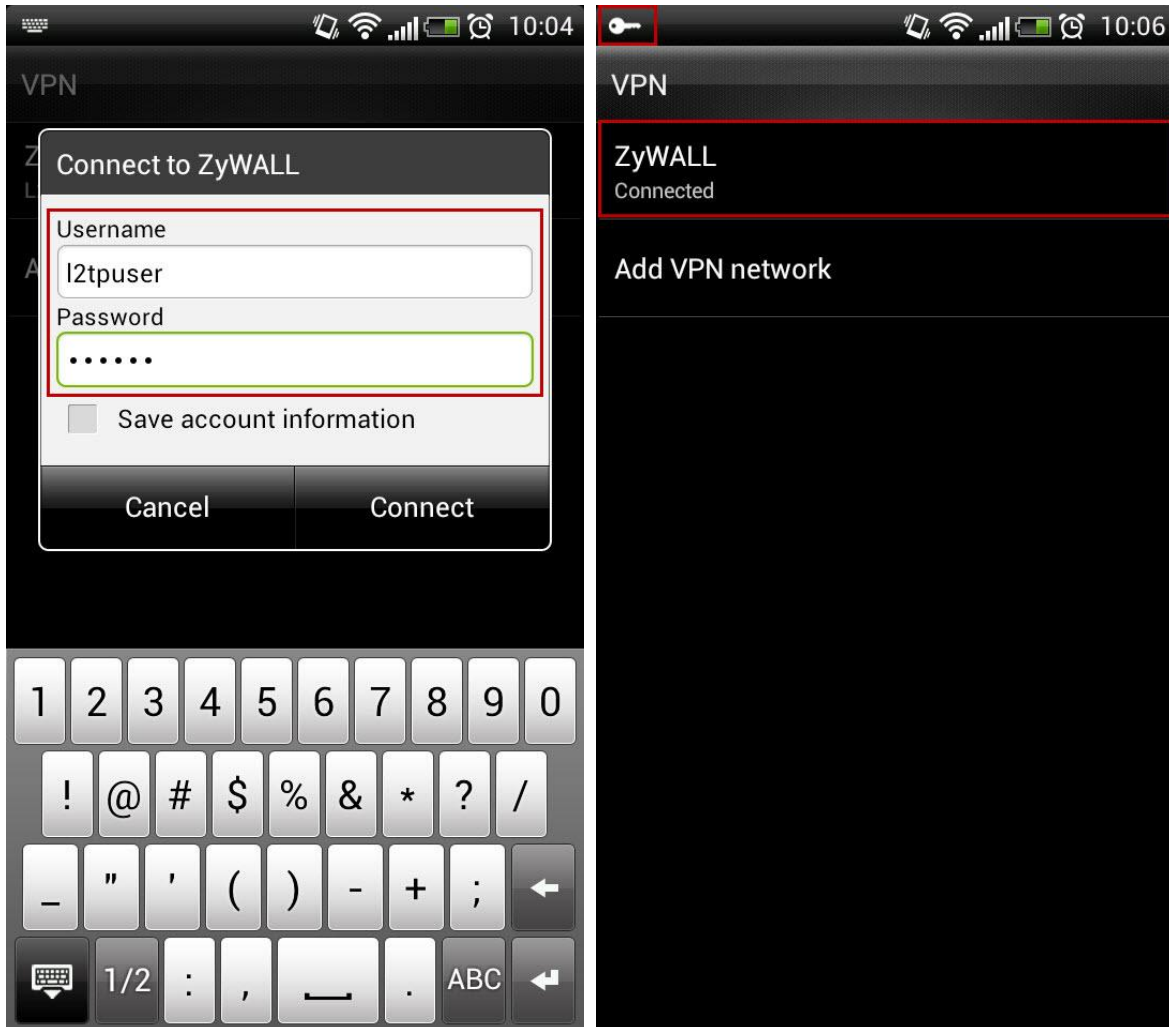
Step 3: Select L2TP/IPSec PSK as the type and fill in the server address.

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.

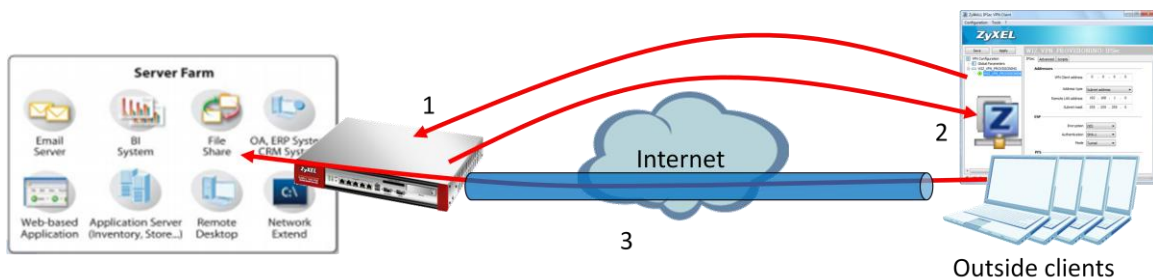
The screenshot shows the 'Session Monitor' interface. At the top, there are 'Disconnect' and 'Refresh' buttons. Below is a table titled 'Current L2TP Session' with the following columns: '#', 'User Name', 'Hostname', 'Assigned IP', and 'Public IP'. There is one entry in the table with the following values: '# 1', 'User Name l2tpuser', 'Hostname anonymous', 'Assigned IP 192.168.100.1', and 'Public IP 59.124.163.130'. At the bottom of the table, there is a pagination control showing 'Page 1 of 1' and 'Show 50 items'. The text 'Displaying 1 - 1 of 1' is also visible at the bottom right.

#	User Name	Hostname	Assigned IP	Public IP
1	l2tpuser	anonymous	192.168.100.1	59.124.163.130

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:

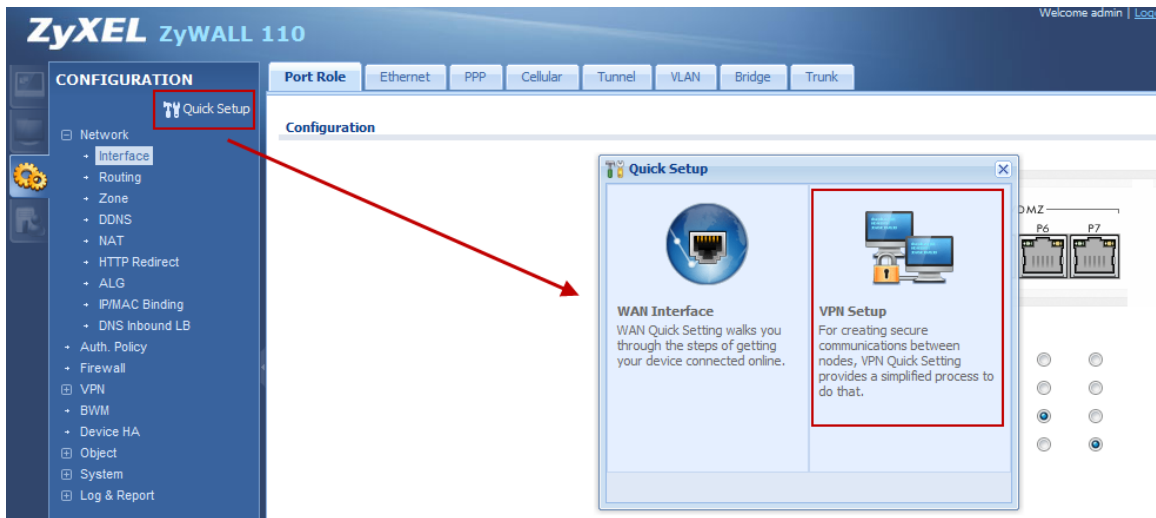
- Encapsulation Mode: Tunnel mode
- Active protocol: ESP
- Encryption algorithm: DES
- Authentication algorithm: SHA1
- Perfect Forward Secrecy: none

Goals to achieve:

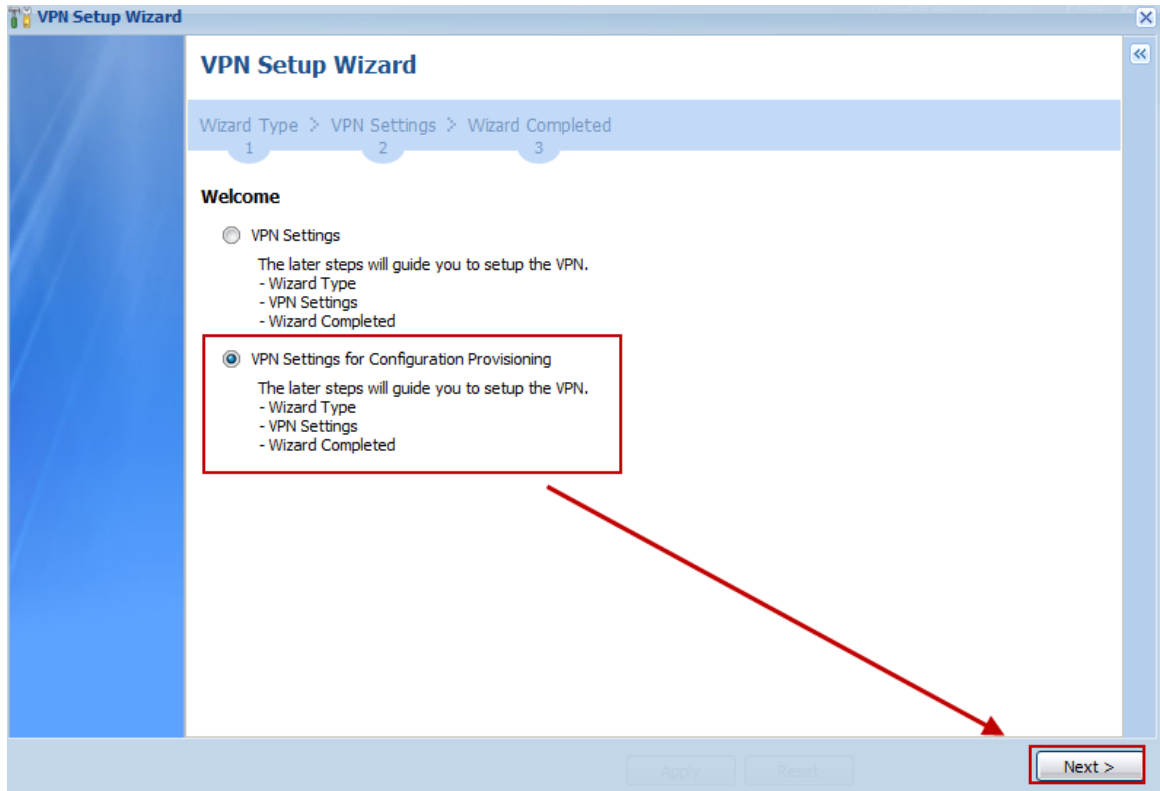
Provide an easy way for outside users to build up IPSec VPN tunnel by using the ZyWALL IPSec VPN Client for accessing internal resource.

ZyWALL configuration

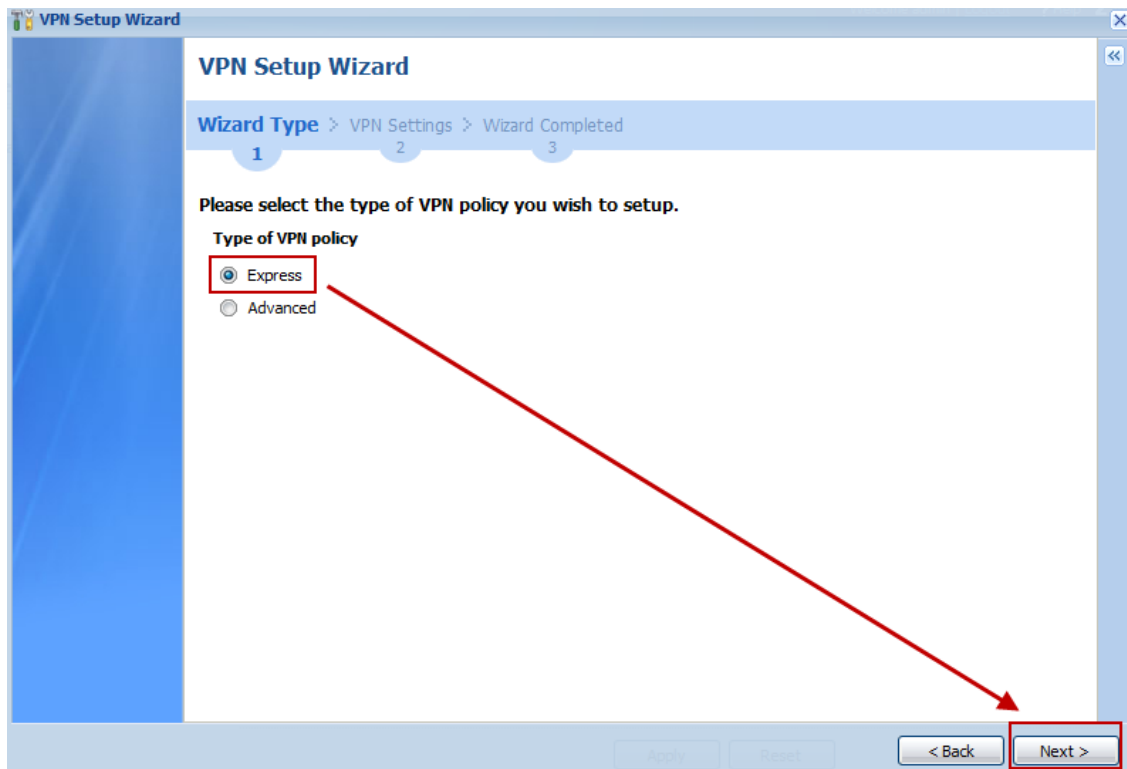
Step 1: Click **Configuration > Quick setup > VPN Setup**



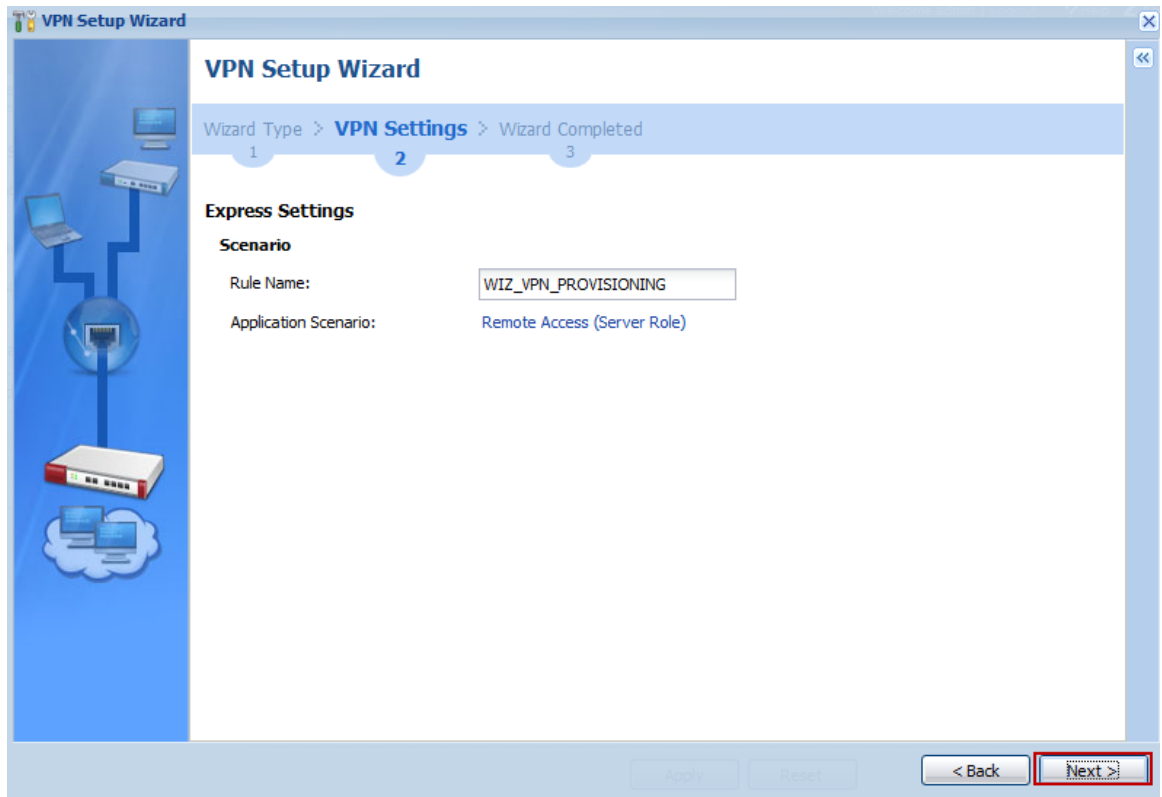
Step 2: Select “VPN settings for Configuration Provisioning”



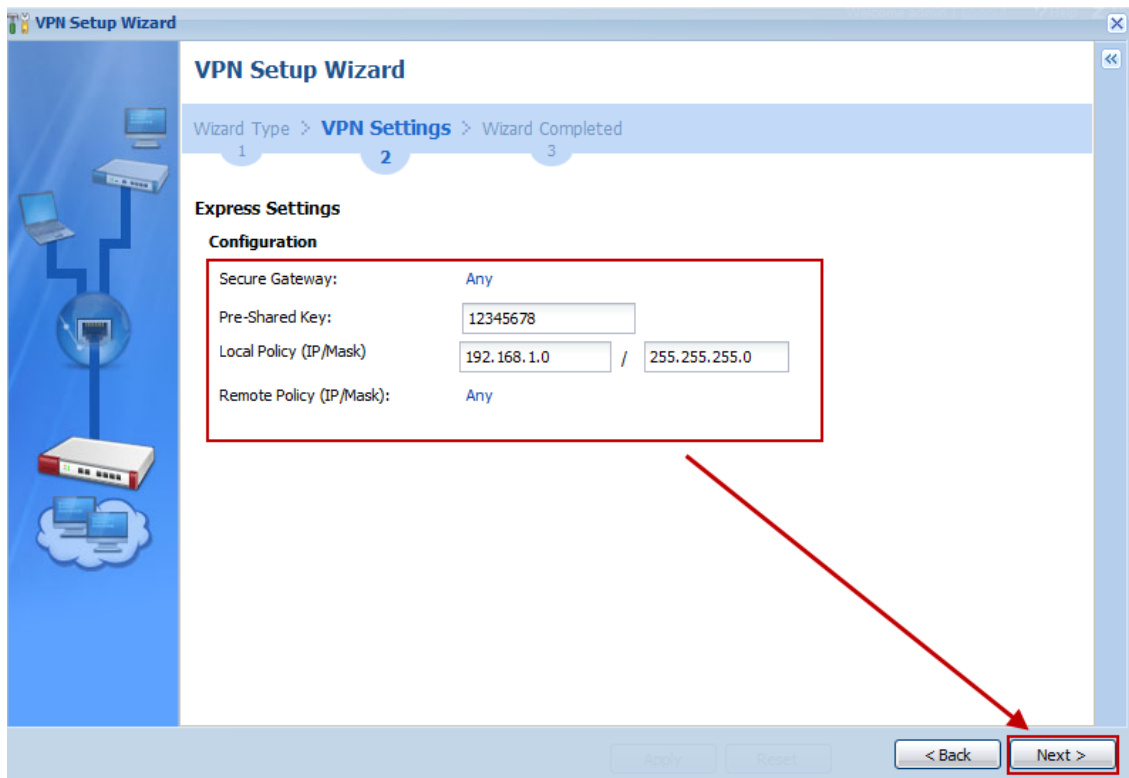
Step 3: Select “Express” (or select “Advance” to define detail settings manually)



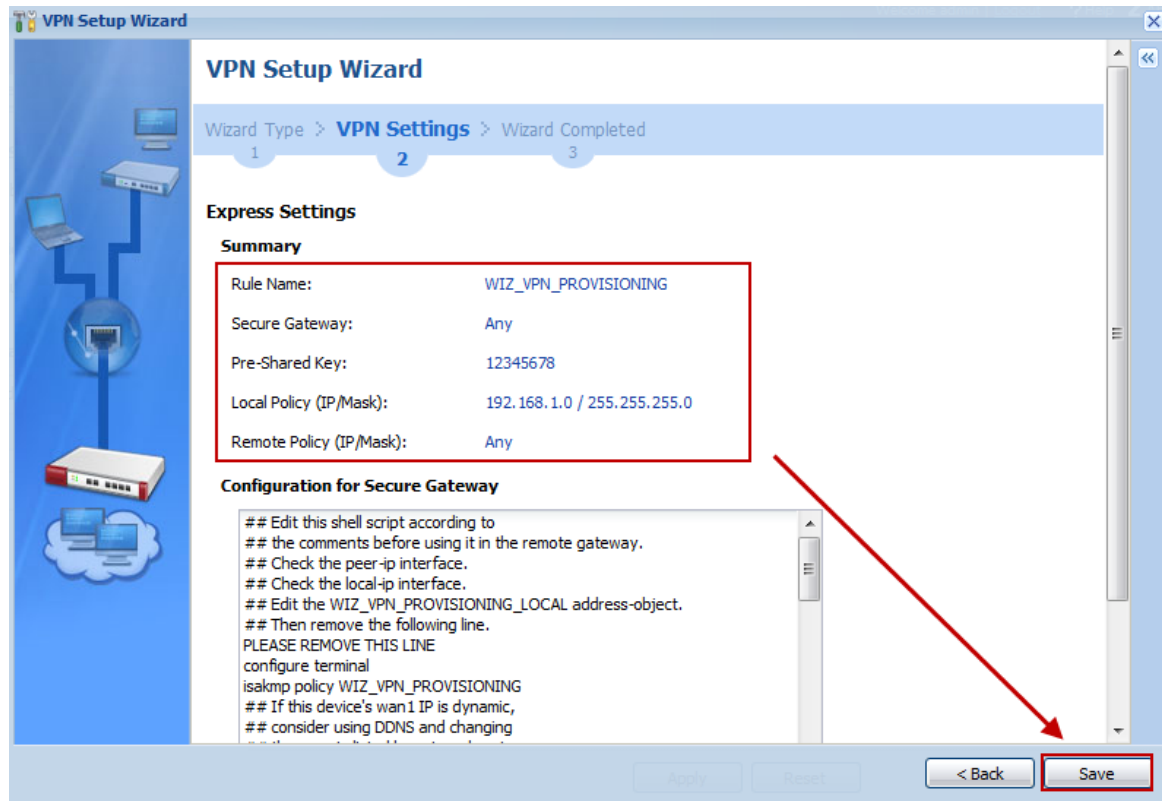
Step 4: Change Rule Name if needed



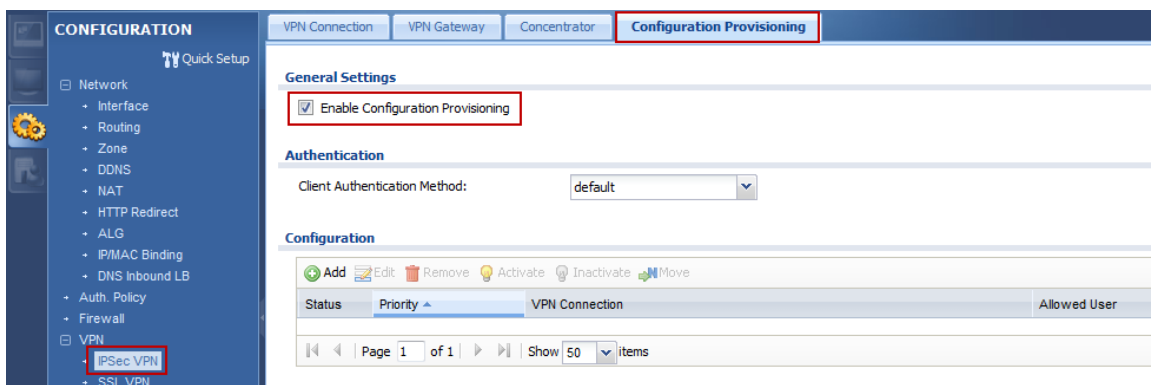
Step 5: Fill in Pre-shared key and Local policy



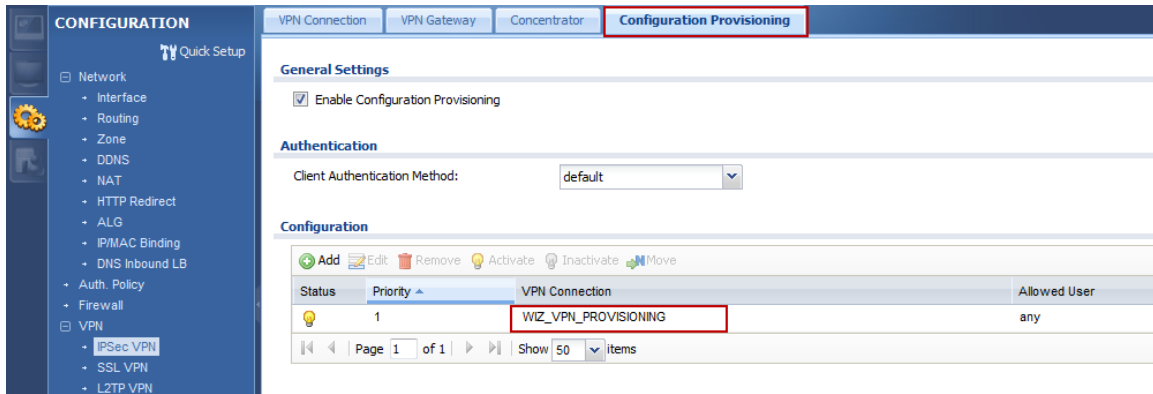
Step 6: Check if IPSec VPN configuration correct and save setting



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

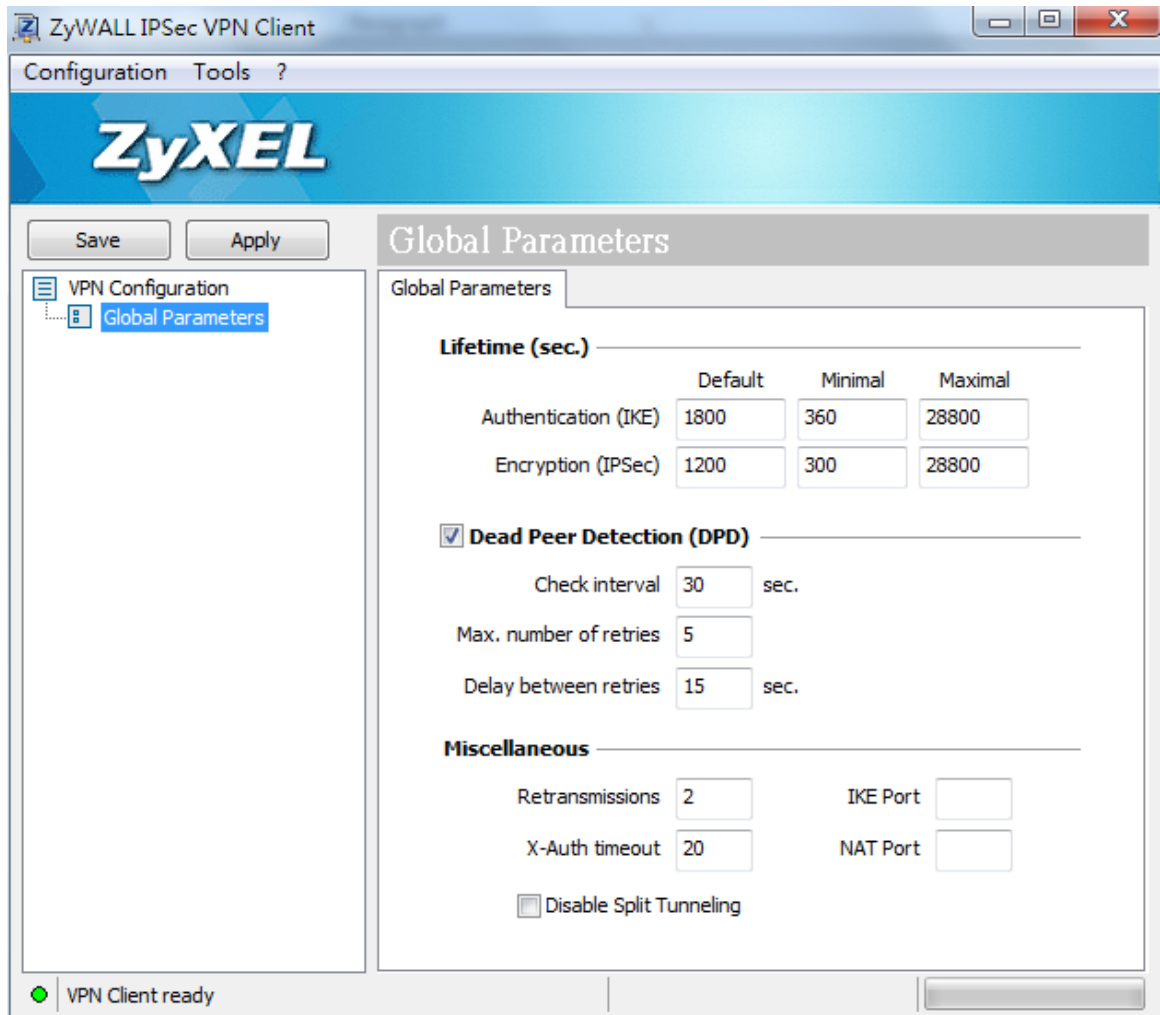


Step 8: Create a provisioning rule for any user

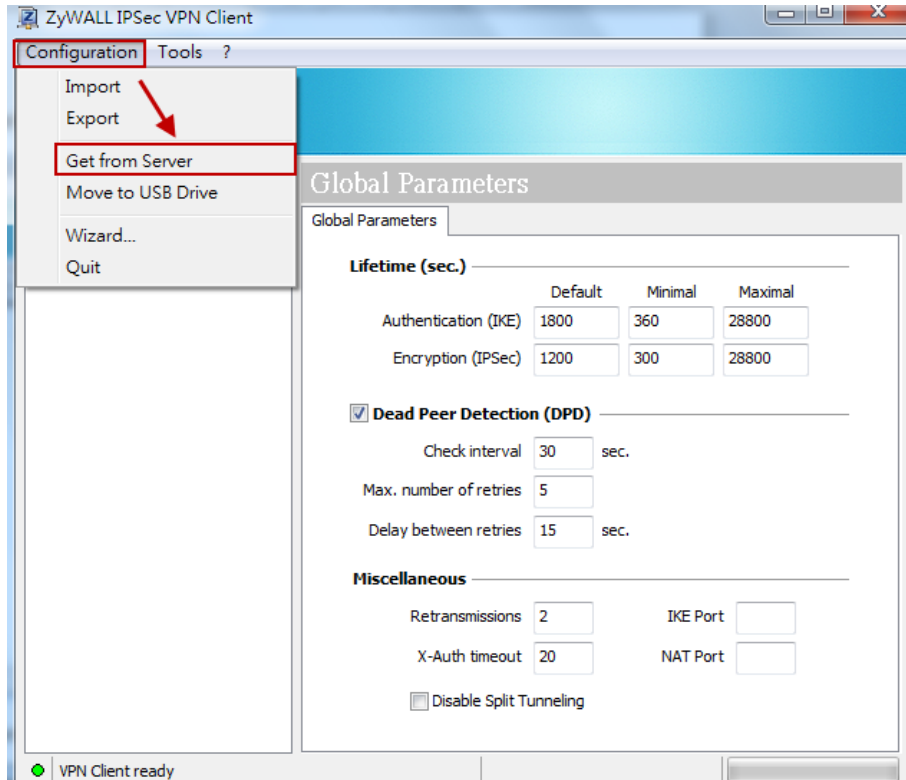


ZyWALL IPsec VPN Client software configuration

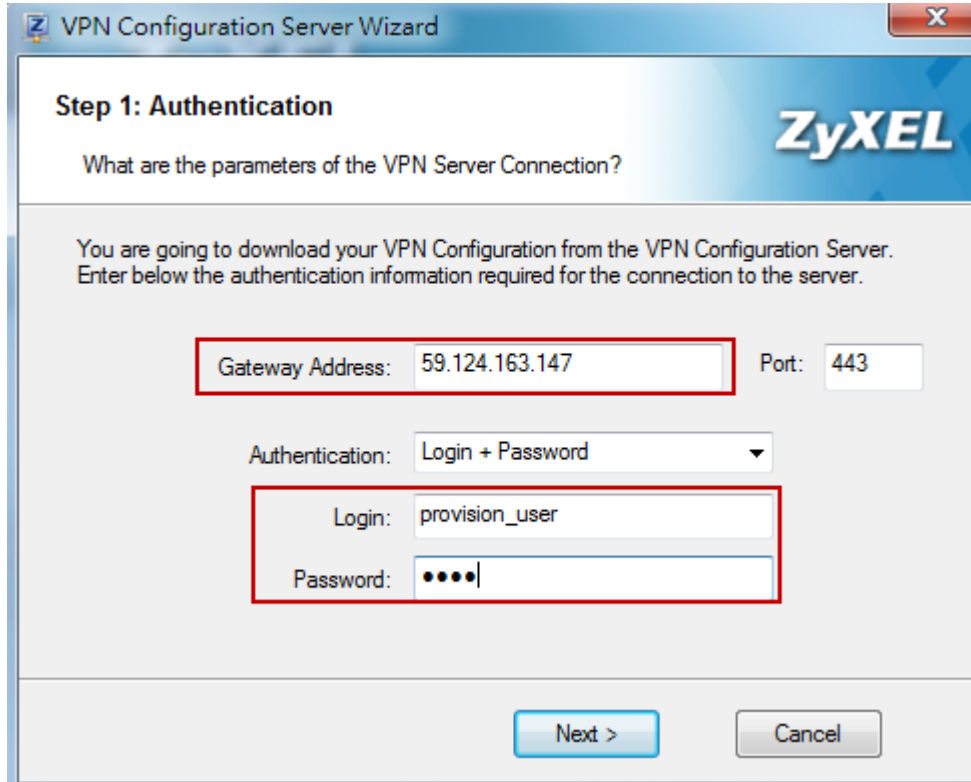
Step 1: Execute ZyWALL IPsec VPN Client



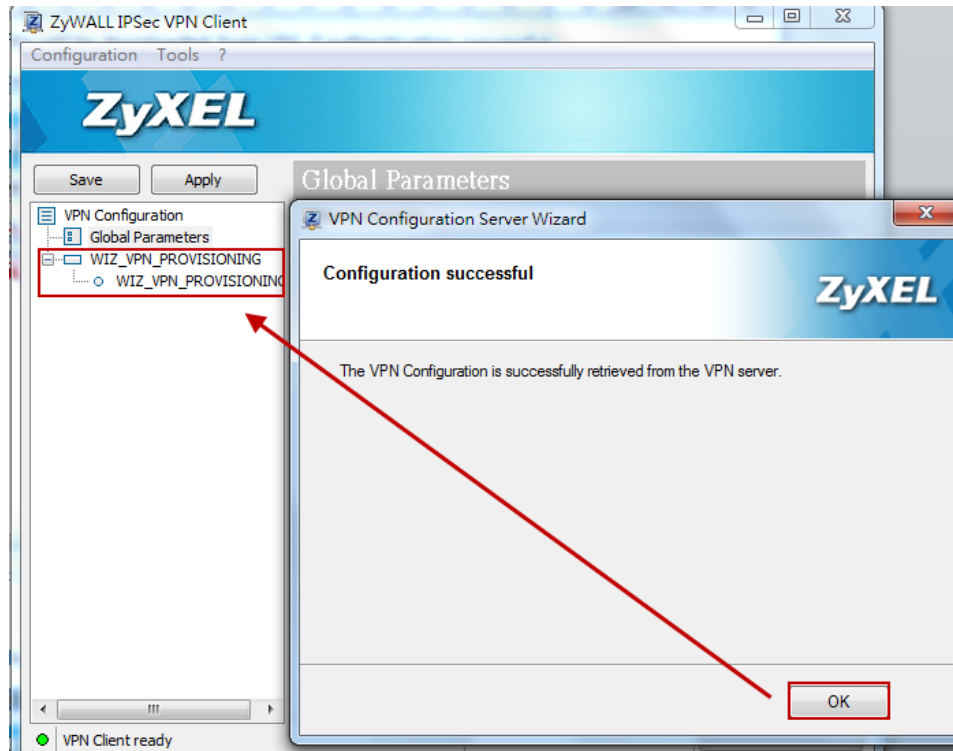
Step 2: Click **Configuration > Get from Server**



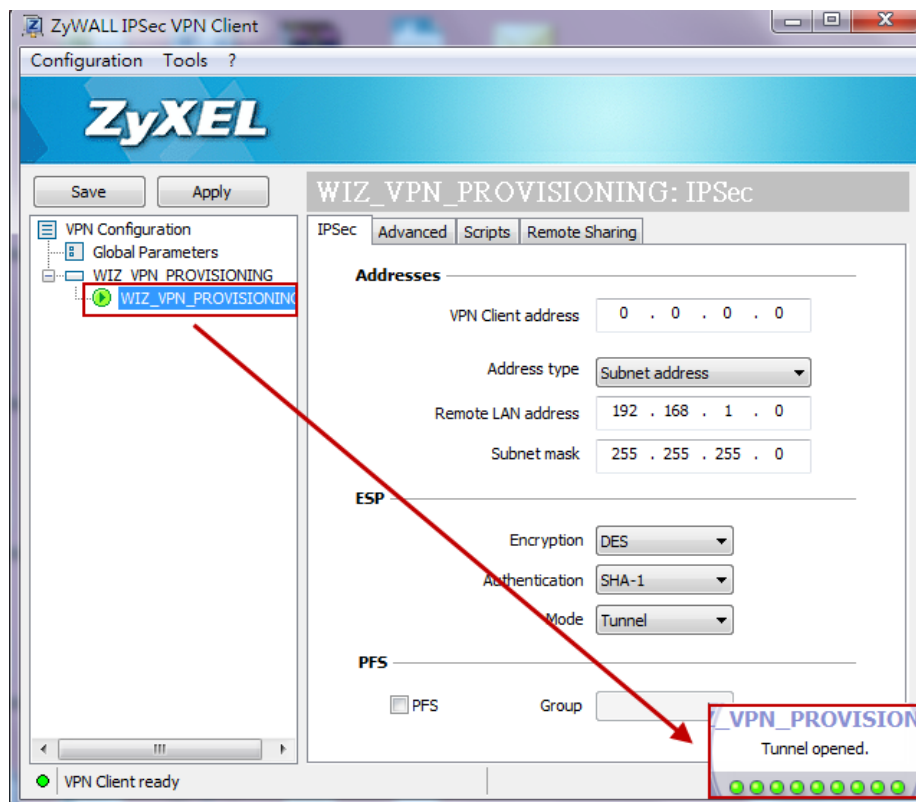
Step 3: Fill in authentication information and click “Next”



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

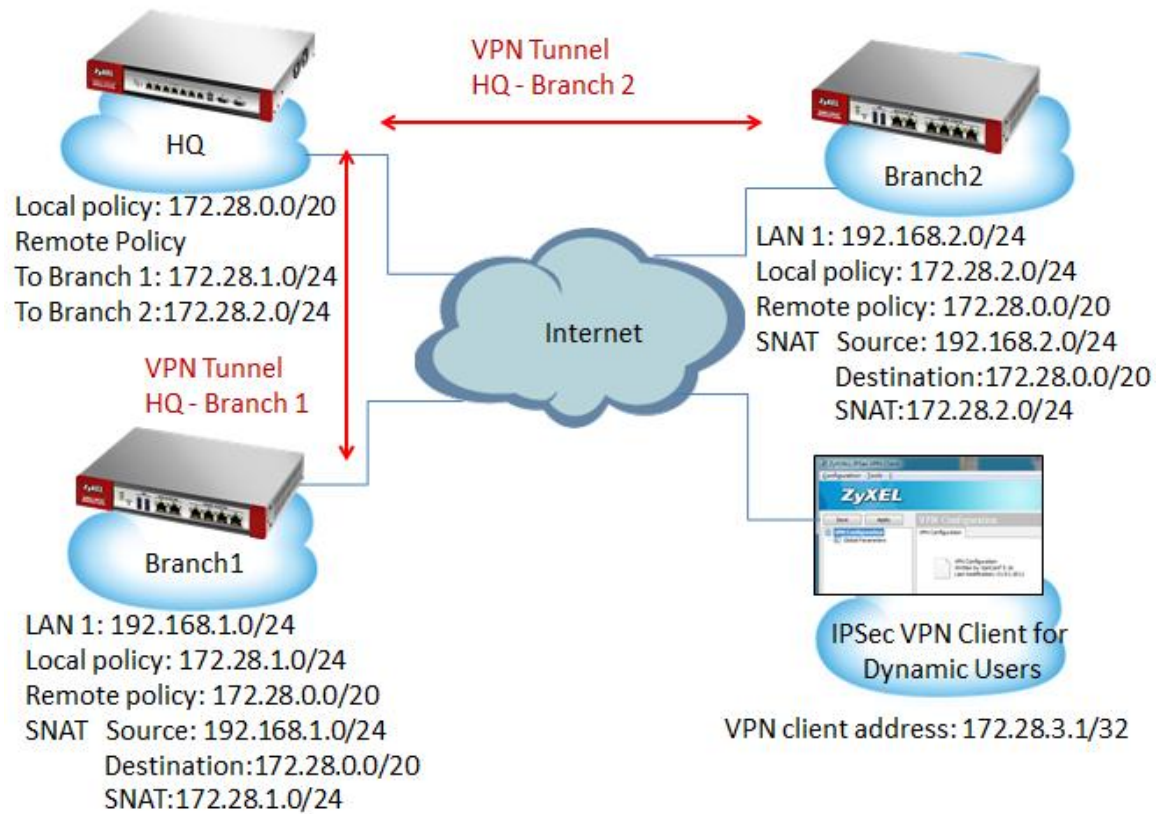
Ping 192.168.1.34 <使用 32 位元組的資料>:
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=2ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=2ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=2ms TTL=126
回覆自 192.168.1.34: 位元組=32 時間=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.



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

The screenshot shows the 'Edit VPN Gateway HQtoBranch1' configuration window. The window is titled 'Edit VPN Gateway HQtoBranch1' and has a 'Show Advanced Settings' button. The configuration is organized into several sections:

- General Settings:**
 - Enable
 - VPN Gateway Name: HQtoBranch1
- Gateway Settings:**
 - My Address:**
 - Interface: ge2 (DHCP client -- 10.59.3.201/255.255.255.0)
 - Domain Name / IP: [Empty]
 - Peer Gateway Address:**
 - Static Address:
 - Primary: 10.59.3.200
 - 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: usq300_cert.cer (See My Certificates)

At the bottom right, there are 'OK' and 'Cancel' buttons.

Step2. Configuration > VPN > IPsec VPN > VPN Connection > Edit

The screenshot shows the 'Edit VPN Connection HQtoBranch1' window. It has a title bar with a question mark and a close button. Below the title bar is a toolbar with 'Show Advanced Settings' and 'Create new Object'. The main area is divided into sections: 'General Settings' with an 'Enable' checkbox and a 'Connection Name' field containing 'HQtoBranch1'; 'VPN Gateway' with an 'Application Scenario' section containing radio buttons for 'Site-to-site', 'Site-to-site with Dynamic Peer', 'Remote Access (Server Role)', and 'Remote Access (Client Role)', and a 'VPN Gateway' field with a dropdown set to 'HQtoBranch1' and a text field containing 'ge2 10.59.3.200 0.0.0.0'; 'Policy' with 'Local policy' and 'Remote policy' fields, each with a dropdown and a text field; and 'Phase 2 Setting' with an 'SA Life Time' field containing '86400' and a note '(180 - 3000000 Seconds)'. At the bottom right are 'OK' and 'Cancel' buttons.

Branch 1 configuration

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

The screenshot shows the 'Edit VPN Gateway Branch1toHQ' window. It has a title bar with a question mark and a close button. Below the title bar is a toolbar with 'Show Advanced Settings'. The main area is divided into sections: 'General Settings' with an 'Enable' checkbox and a 'VPN Gateway Name' field containing 'Branch1toHQ'; 'Gateway Settings' with a 'My Address' section containing radio buttons for 'Interface' (selected) and 'Domain Name / IP', and a 'Peer Gateway Address' section containing radio buttons for 'Static Address' (selected) and 'Dynamic Address', with sub-fields for 'Primary' (10.59.3.201) and 'Secondary' (0.0.0.0) addresses, and a 'Fall back to Primary Peer Gateway when possible' checkbox with a 'Fall Back Check Interval' field containing '300' and a note '(60-86400 seconds)'; and 'Authentication' with radio buttons for 'Pre-Shared Key' (selected) and 'Certificate', with a text field containing '12345678' and a dropdown set to 'default' with a note '(See My Certificates)'. At the bottom right are 'OK' and 'Cancel' buttons.

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

Edit VPN Connection Branch1toHQ

Show Advanced Settings Create new Object

General Settings

Enable

Connection Name: Branch1toHQ

VPN Gateway

Application Scenario

- Site-to-site
- Site-to-site with Dynamic Peer
- Remote Access (Server Role)
- Remote Access (Client Role)

VPN Gateway: Branch1toHQ wan1 10.59.3.201 0.0.0.0

Policy

Local policy: vlan172_1 SUBNET, 172.28.1.0/24

Remote policy: vlan172_0 SUBNET, 172.28.0.0/20

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

OK Cancel

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

Edit VPN Connection Branch1 to HQ

Hide Advanced Settings Create new Object+

Log

Inbound/Outbound traffic NAT

Outbound Traffic

Source NAT

Source: LAN1_SUBNET

Destination: vlan172_0

SNAT: vlan172_1

Inbound Traffic

Source NAT

Source: Please select one ...

Destination: Please select one ...

SNAT: Please select one ...

Destination NAT

#	Original IP	Mapped IP	Protocol	Original Port St...	Original Port End	Mapped Port S...	Mapped Port End
1	vlan172_1	LAN1_SUBNET	ALL	0	0	0	0

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

OK Cancel

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

Add a policy route

Source: any

Destination: 172.28.0.0/20

Next-hop: VPN tunnel

Edit Policy Route

Show Advanced Settings Create new Object

Configuration

Enable
Description: (Optional)

Criteria

User: any
Incoming: any (Excluding ZyWALL)
Source Address: any
Destination Address: vlan172_0
DSCP Code: any
Schedule: none
Service: any

Next-Hop

Type: VPN Tunnel
VPN Tunnel: Branch1toHQ

OK Cancel

Task 2. Establish IPsec VPN between HQ and Branch 2

HQ configuration

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

The screenshot shows the 'Edit VPN Gateway HQtoBranch2' configuration window. It is divided into several sections:

- General Settings:** The 'Enable' checkbox is checked. The 'VPN Gateway Name' is 'HQtoBranch2'.
- Gateway Settings:**
 - My Address:** 'Interface' is selected with 'ge2' chosen from the dropdown. The address is 'DHCP client -- 10.59.3.201/255.255.255.0'. 'Domain Name / IP' is empty.
 - Peer Gateway Address:** 'Static Address' is selected. 'Primary' is '10.59.3.37' and 'Secondary' is '0.0.0.0'. The 'Fall back to Primary Peer Gateway when possible' checkbox is unchecked. 'Fall Back Check Interval' is '300' seconds.
 - 'Dynamic Address' is not selected.
- Authentication:** 'Pre-Shared Key' is selected with the value '12345678'. 'Certificate' is not selected; the dropdown shows 'usg300_cert.cer'.

Buttons for 'OK' and 'Cancel' are at the bottom right.

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

The screenshot shows the 'Edit VPN Connection HQtoBranch2' configuration window. It is divided into several sections:

- General Settings:** The 'Enable' checkbox is checked. The 'Connection Name' is 'HQtoBranch2'.
- VPN Gateway:** 'Application Scenario' is 'Site-to-site'. 'VPN Gateway' is 'HQtoBranch2' with the address 'ge2 10.59.3.37 0.0.0.0'.
- Policy:** 'Local policy' is 'vlan172_0' with 'SUBNET, 172.28.0.0/20'. 'Remote policy' is 'vlan172_2' with 'SUBNET, 172.28.2.0/24'.
- Phase 2 Setting:** 'SA Life Time' is '86400' seconds.

Buttons for 'OK' and 'Cancel' are at the bottom right.

Branch 2 configuration

Step1. Configuration > VPN > IPsec VPN > VPN Gateway > Edit

The screenshot shows the 'Edit VPN Gateway Branch2toHQ' configuration window. It is divided into several sections:

- General Settings:** The 'Enable' checkbox is checked. The 'VPN Gateway Name' is set to 'Branch2toHQ'.
- Gateway Settings:**
 - My Address:** The 'Interface' is set to 'wan1' (DHCP client -- 10.59.3.37/255.255.255.0). The 'Domain Name / IP' field is empty.
 - Peer Gateway Address:** The 'Static Address' radio button is selected. The 'Primary' address is '10.59.3.201' and the 'Secondary' address is '0.0.0.0'. The 'Fall back to Primary Peer Gateway when possible' checkbox is checked, with a 'Fall Back Check Interval' of '300' seconds.
 - The 'Dynamic Address' radio button is unselected.
- Authentication:** The 'Pre-Shared Key' radio button is selected with the value '12345678'. The 'Certificate' radio button is unselected, with a dropdown set to 'default' (See My Certificates).

Buttons for 'OK' and 'Cancel' are located at the bottom right.

Step2. Configuration > VPN > IPsec VPN > VPN Connection > Edit

The screenshot shows the 'Edit VPN Connection Branch2toHQ' configuration window. It is divided into several sections:

- General Settings:** The 'Enable' checkbox is checked. The 'Connection Name' is set to 'Branch2toHQ'.
- VPN Gateway:**
 - Application Scenario:** The 'Site-to-site' radio button is selected. Other options include 'Site-to-site with Dynamic Peer', 'Remote Access (Server Role)', and 'Remote Access (Client Role)'.
 - The 'VPN Gateway' dropdown is set to 'Branch2toHQ' and the 'wan1 10.59.3.201 0.0.0.0' text is visible.
- Policy:**
 - 'Local policy' is set to 'vlan172_2' (SUBNET, 172.28.2.0/24).
 - 'Remote policy' is set to 'vlan172_0' (SUBNET, 172.28.0.0/20).
- Phase 2 Setting:** The 'SA Life Time' is set to '86400' seconds (180 - 3000000 Seconds).

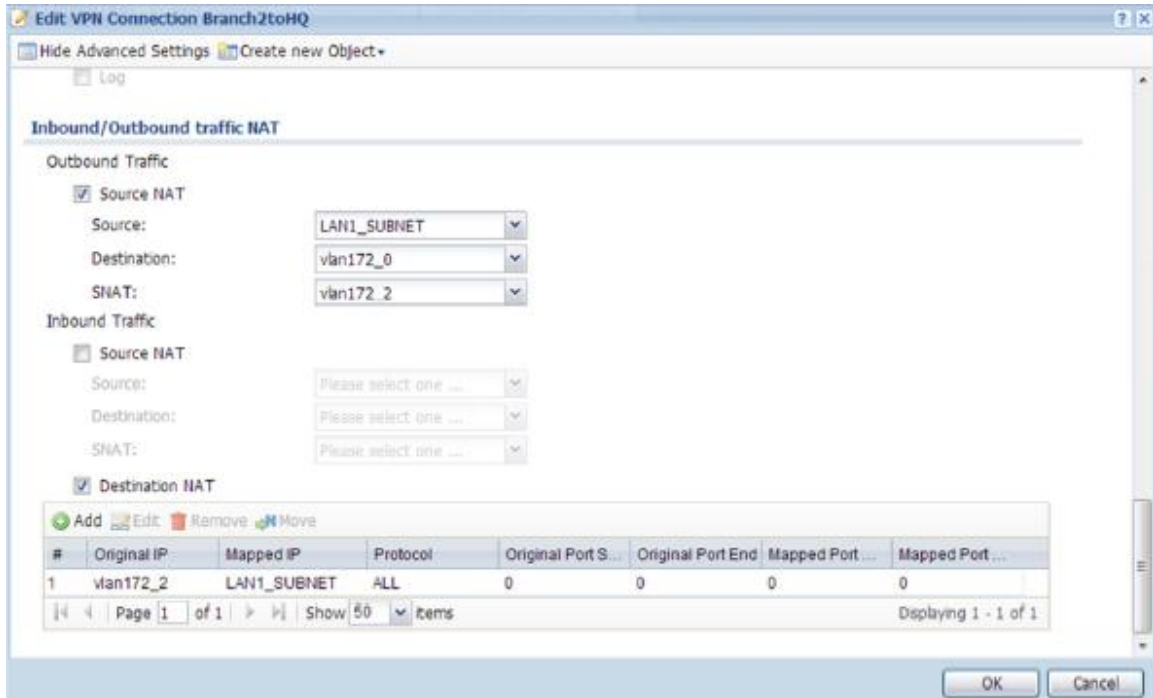
Buttons for 'OK' and 'Cancel' are located at the bottom right.

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

Edit Policy Route

Show Advanced Settings Create new Object

Configuration

Enable
Description: (Optional)

Criteria

User: any
Incoming: any (Excluding ZyWALL)
Source Address: any
Destination Address: vlan172_0
DSCP Code: any
Schedule: none
Service: any

Next-Hop

Type: VPN Tunnel
VPN Tunnel: Branch2toHQ

OK Cancel

Task 3. Establish Dynamic VPN for mobile users

HQ configuration

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

The screenshot shows the 'Edit VPN Gateway HQtoMobileUser' configuration window. It is divided into several sections:

- General Settings:** The 'Enable' checkbox is checked. The 'VPN Gateway Name' is 'HQtoMobileUser'.
- Gateway Settings:**
 - My Address:** 'Interface' is selected, set to 'ge2' with a 'DHCP client -- 10.59.3.201/255.255.255.0'.
 - Peer Gateway Address:** 'Static Address' is selected. Primary and Secondary addresses are both '0.0.0.0'. The 'Fall back to Primary Peer Gateway when possible' checkbox is checked, with a 'Fall Back Check Interval' of '300' seconds.
 - 'Dynamic Address' is also selected.
- Authentication:** 'Pre-Shared Key' is selected with the value '123456789'. 'Certificate' is also selected, pointing to 'usg300_cert.cer'.

Buttons for 'OK' and 'Cancel' are at the bottom right.

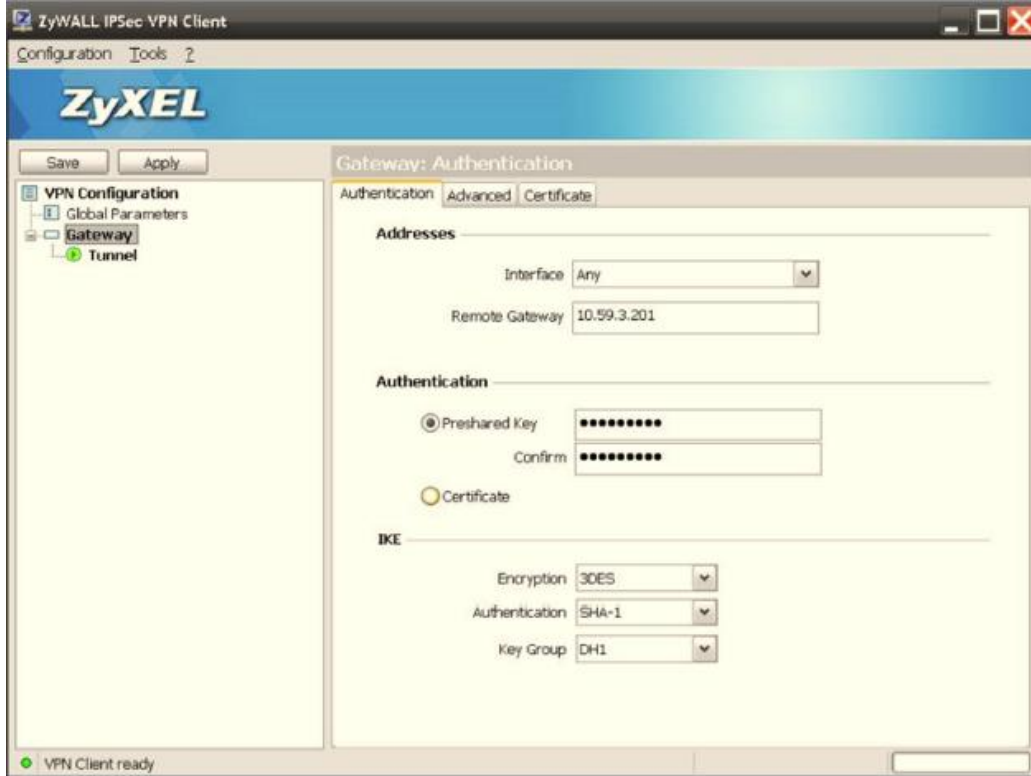
Step 2. Configuration > VPN > IPsec VPN > VPN Connection > Edit

The screenshot shows the 'Edit VPN Connection HQtoMobileUser' configuration window. It is divided into several sections:

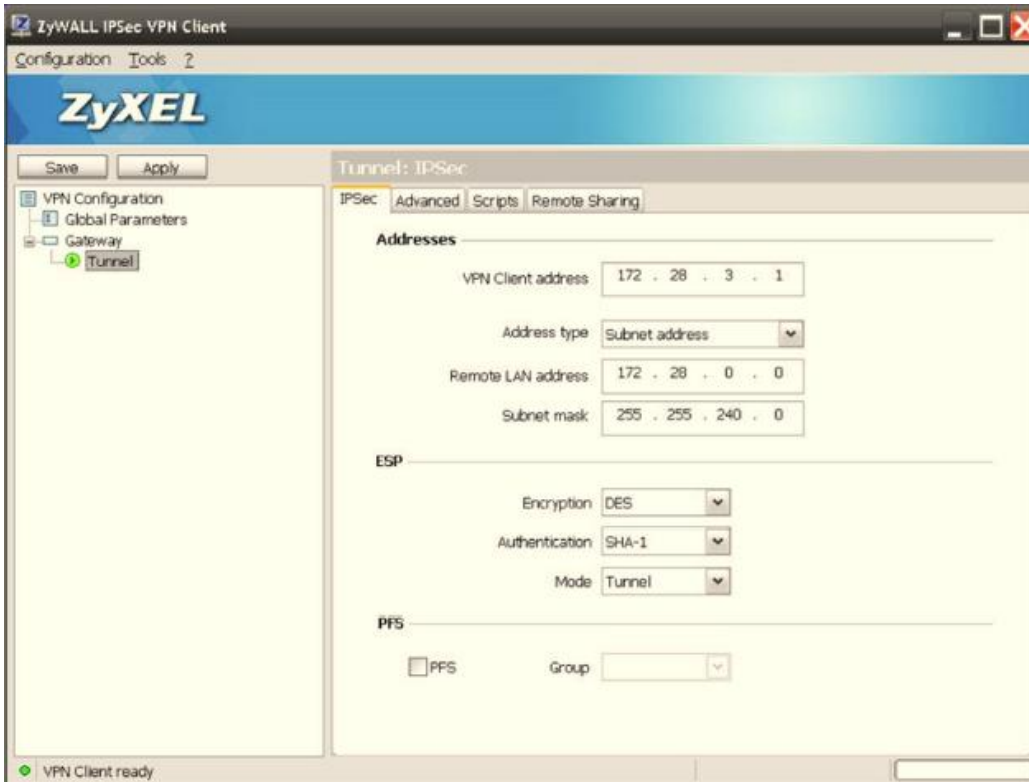
- General Settings:** The 'Enable' checkbox is checked. The 'Connection Name' is 'HQtoMobileUser'.
- VPN Gateway:** 'Application Scenario' is set to 'Remote Access (Server Role)'. The 'VPN Gateway' is 'HQtoMobileUser' with the address 'ge2 0.0.0.0 0.0.0.0'.
- Policy:** 'Local policy' is 'vlan172_0' with the subnet 'SUBNET, 172.28.0.0/20'.
- Phase 2 Setting:** 'SA Life Time' is '86400' seconds (180 - 3000000 Seconds).
- Related Settings:** This section is currently empty.

Buttons for 'OK' and 'Cancel' are at the bottom right.

Step 3. IPSec VPN client setting

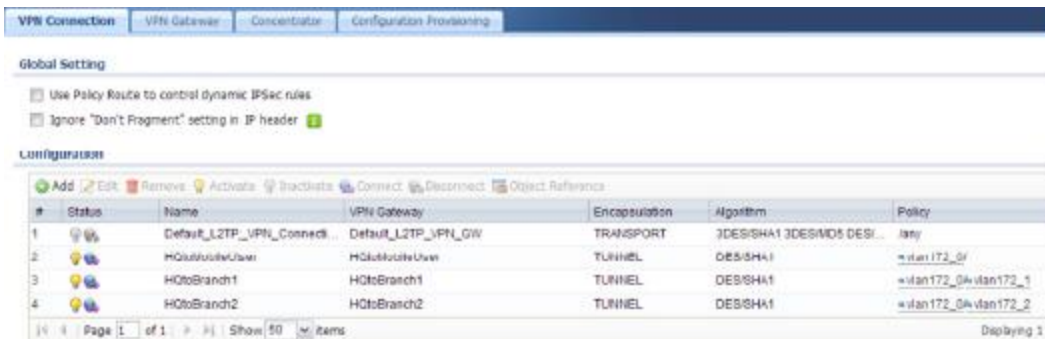


Step 4. In Phase 2, assign one IP for IPSec VPN Client manually.



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
```