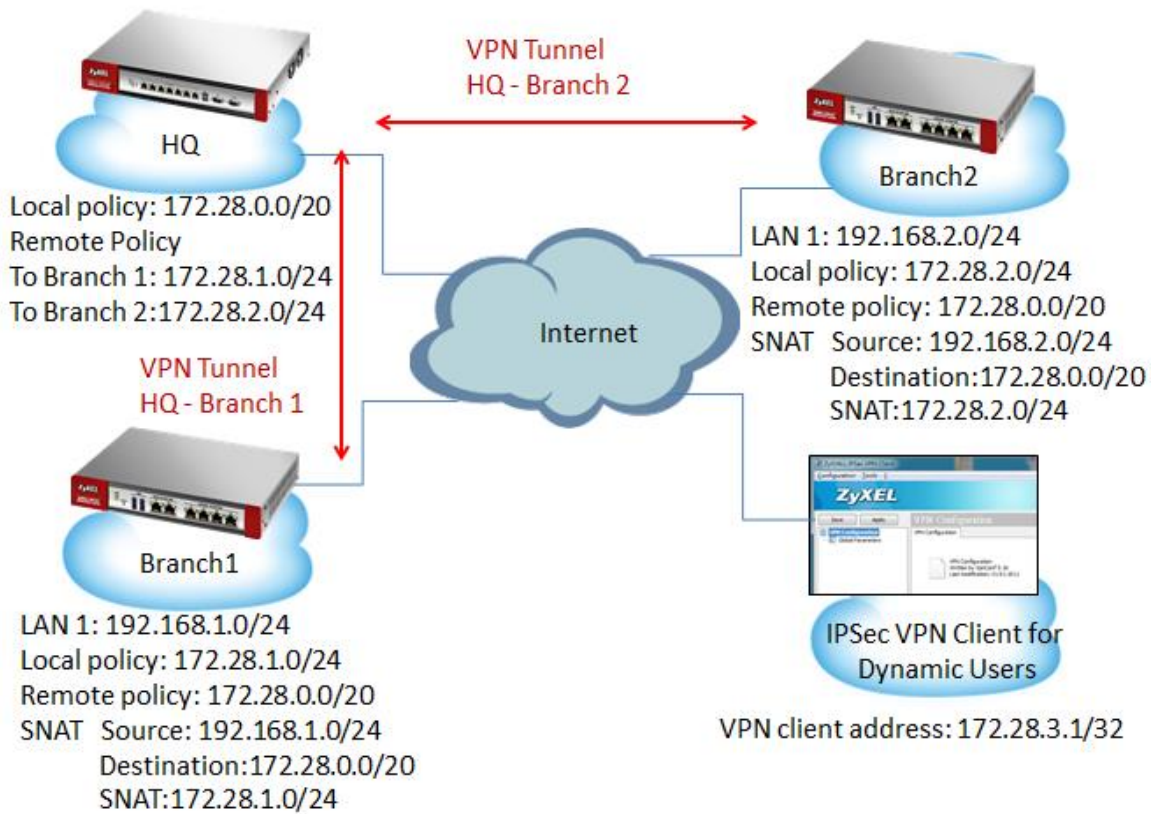


Dynamic users communicate with HQ and all branch offices by using auto created VPN routes

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.



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 divided 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
 - 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)

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

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 '(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' and 'Domain Name / IP', and a 'Peer Gateway Address' section containing radio buttons for 'Static Address' and 'Dynamic Address', with sub-fields for 'Primary' and 'Secondary' addresses; and 'Authentication' with radio buttons for 'Pre-Shared Key' and 'Certificate', and a text field for the key and a dropdown for the certificate. 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)

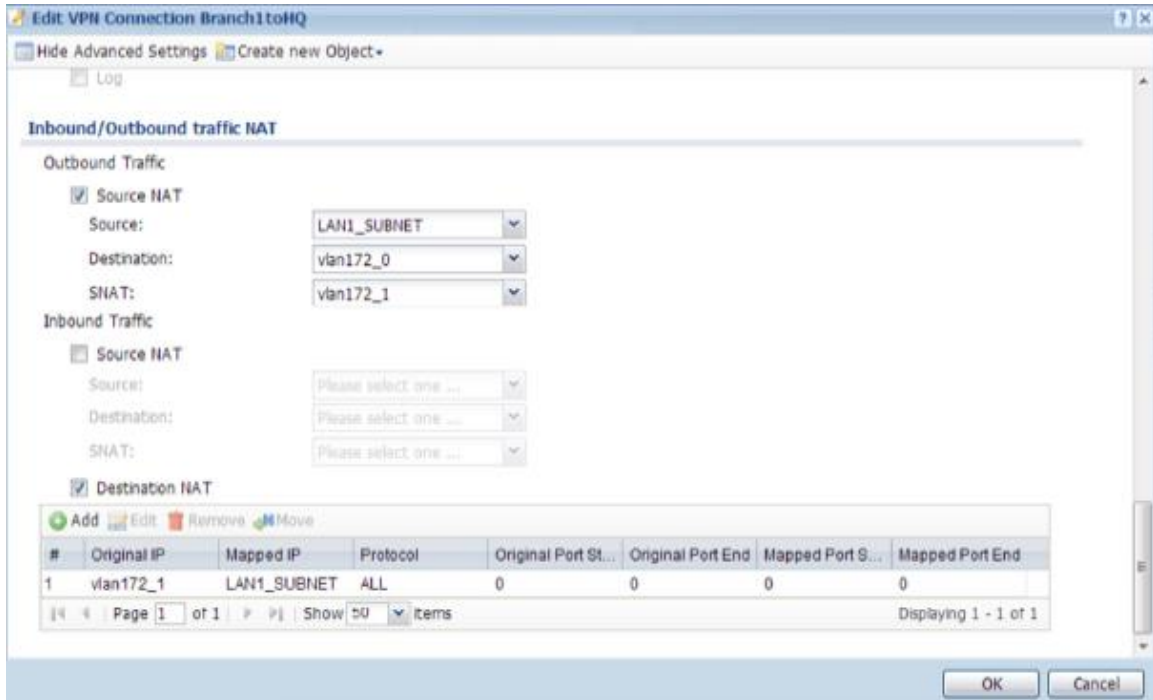
OK Cancel

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



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 checked, with a 'Fall Back Check Interval' of '300' seconds.
 - 'Dynamic Address' is not selected.
- Authentication:** 'Pre-Shared Key' is selected with the value '12345678'. 'Certificate' is not selected, with 'usg300_cert.cer' shown in the dropdown.

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 (180 - 3000000 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 'Branch2toHQ'.
- Gateway Settings:**
 - My Address:** 'Interface' is selected with 'wan1' chosen from the dropdown. The address is 'DHCP client -- 10.59.3.37/255.255.255.0'. 'Domain Name / IP' is empty.
 - Peer Gateway Address:** 'Static Address' is selected. 'Primary' is '10.59.3.201' and 'Secondary' is '0.0.0.0'. The 'Fall back to Primary Peer Gateway when possible' checkbox is checked, and the 'Fall Back Check Interval' is '300' seconds.
 - 'Dynamic Address' is not selected.
- Authentication:** 'Pre-Shared Key' is selected with the value '12345678'. 'Certificate' is set to 'default'.

Buttons for 'OK' and 'Cancel' are 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 'Branch2toHQ'.
- VPN Gateway:**
 - Application Scenario:** 'Site-to-site' is selected. Other options are 'Site-to-site with Dynamic Peer', 'Remote Access (Server Role)', and 'Remote Access (Client Role)'.
 - 'VPN Gateway' is 'Branch2toHQ' and the associated address is 'wan1 10.59.3.201 0.0.0.0'.
- Policy:** 'Local policy' is 'vlan172_2' (SUBNET, 172.28.2.0/24) and 'Remote policy' is 'vlan172_0' (SUBNET, 172.28.0.0/20).
- Phase 2 Setting:** 'SA Life Time' is '86400' seconds (range 180 - 3000000).

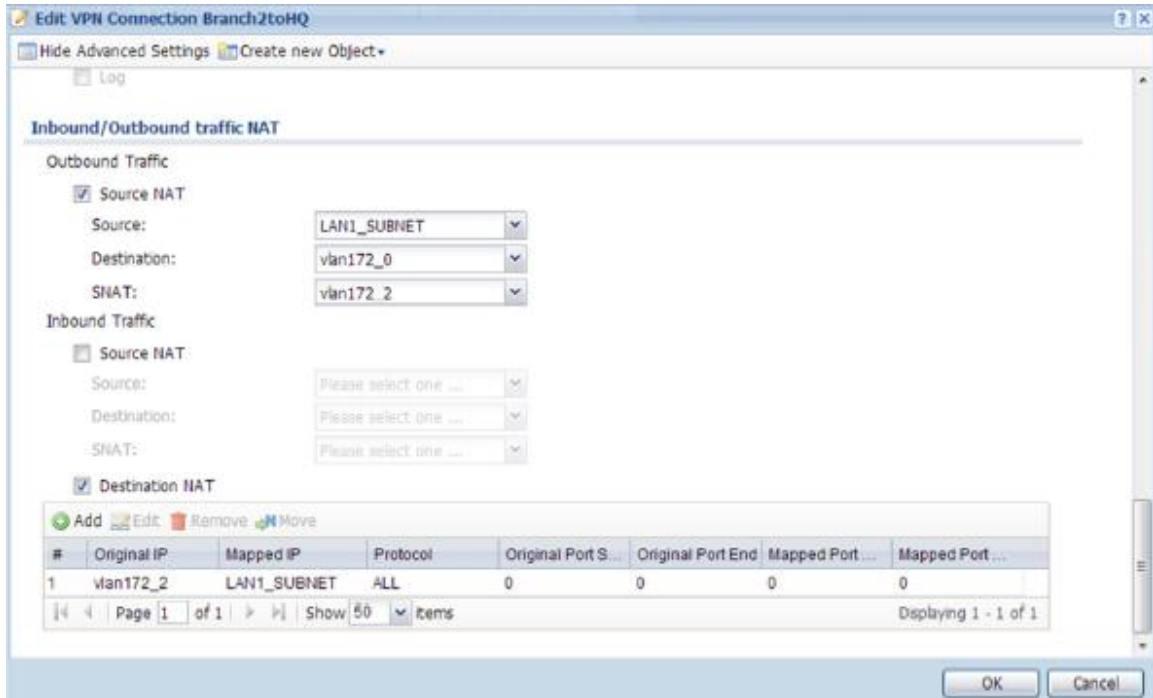
Buttons for 'OK' and 'Cancel' are at the bottom right.

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 set to 'HQtoMobileUser'.
- Gateway Settings:**
 - My Address:** The 'Interface' is set to 'ge2' and the address type is 'DHCP client -- 10.59.3.201/255.255.255.0'. The 'Domain Name / IP' field is empty.
 - Peer Gateway Address:** The 'Static Address' option is selected. The 'Primary' address is '0.0.0.0' and the 'Secondary' address is '0.0.0.0'. The 'Fall back to Primary Peer Gateway when possible' checkbox is checked, and the 'Fall Back Check Interval' is set to '300' seconds (range 60-86400).
 - The 'Dynamic Address' option is also selected.
- Authentication:** The 'Pre-Shared Key' is set to '123456789'. The 'Certificate' option is selected, with 'usg300_cert.cer' chosen from the dropdown menu.

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

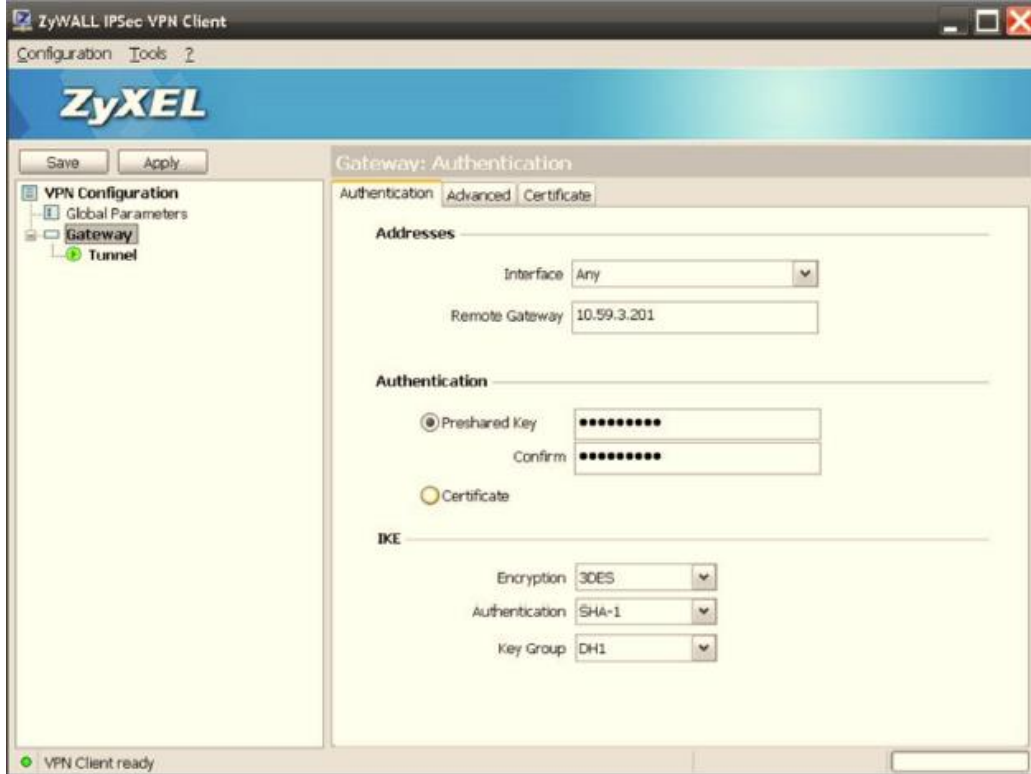
Step 2. Configuration > VPN > IPsec VPN > VPN Connection > Edit

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

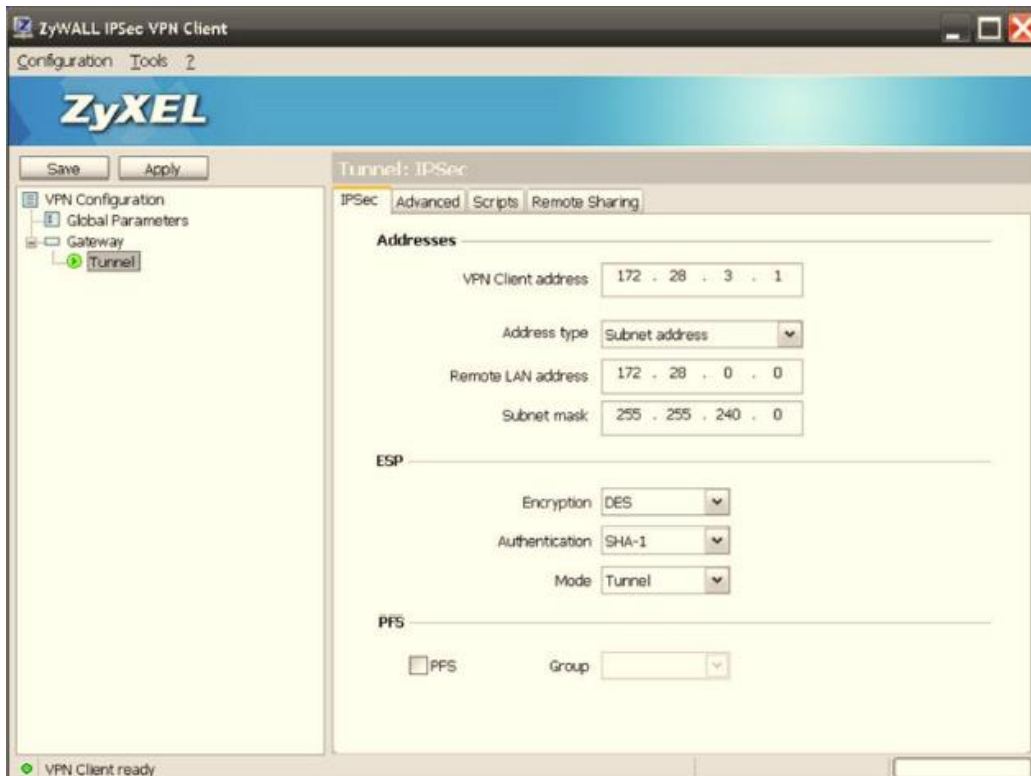
- General Settings:** The 'Enable' checkbox is checked. The 'Connection Name' is set to 'HQtoMobileUser'.
- VPN Gateway:** The 'Application Scenario' is set to 'Remote Access (Server Role)'. The 'VPN Gateway' is set to 'HQtoMobileUser' and the address is 'ge2 0.0.0.0 0.0.0.0'.
- Policy:** The 'Local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

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

Step 3. IPSec VPN client setting

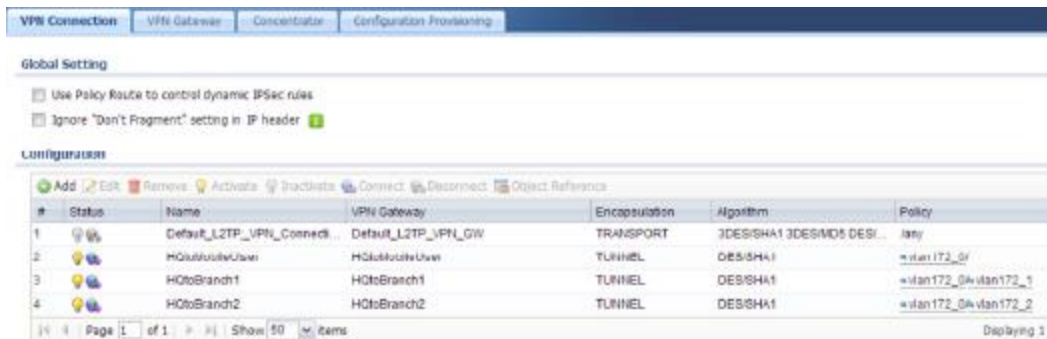


Step 4. In Phase 2, assign one IP for IPSec VPN Client manually.



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
```