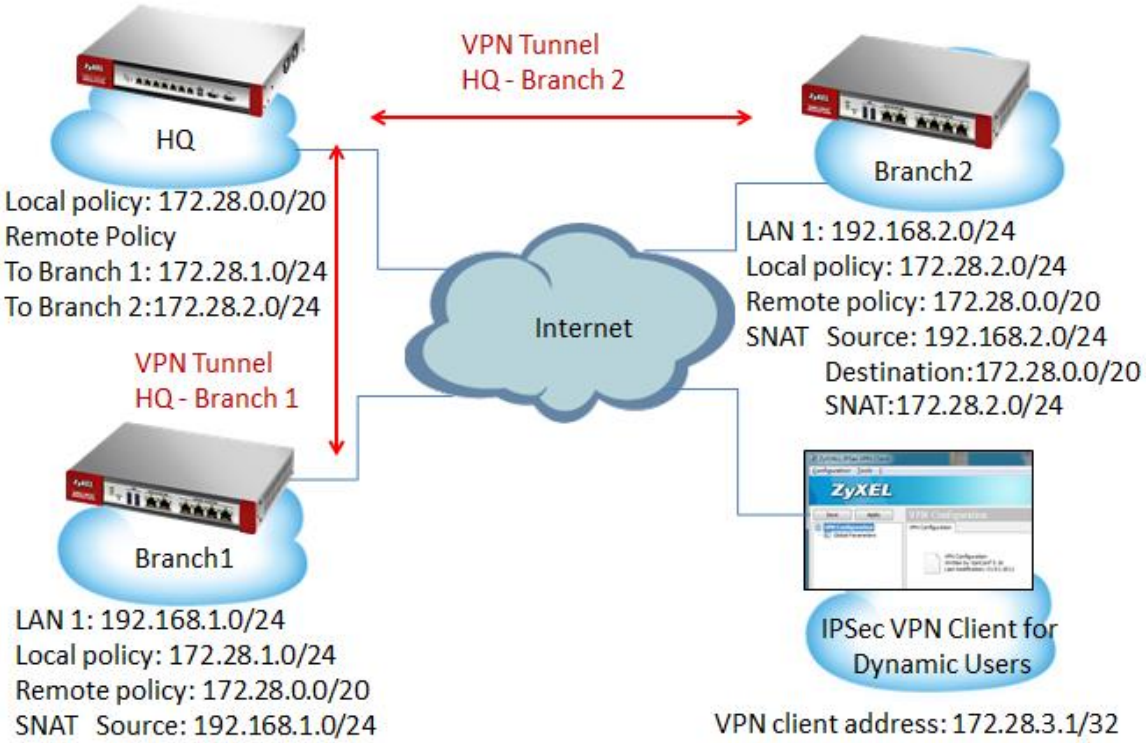
Dynamic users communicate with HQ and all branch offices by using auto created VPN routes

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.


VPN Tunnel
HQ - Branch 2
HQ
Branch2
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
Internet
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
VPN Tunnel
HQ - Branch 1
Branch1
ZyXEL
IPSec VPN Client for
Dynamic Users
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
VPN client address: 172.28.3.1/32

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:

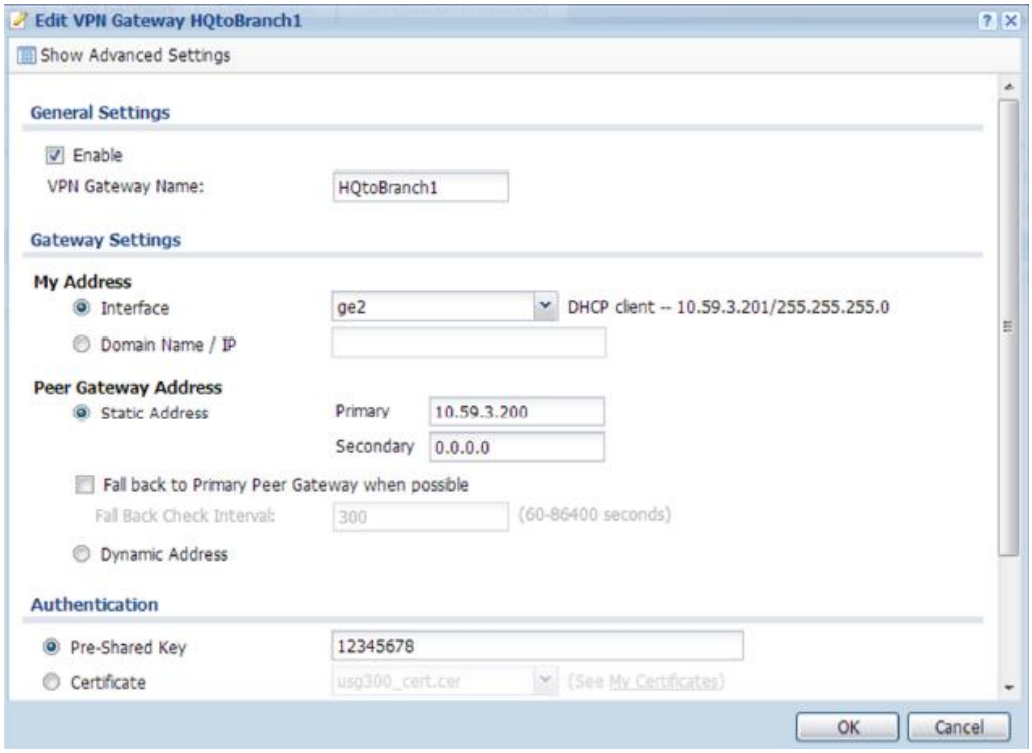
Mobile users can communicate with headquarters and all branch offices with only one VPN tunnel.

ZyWALL configuration:

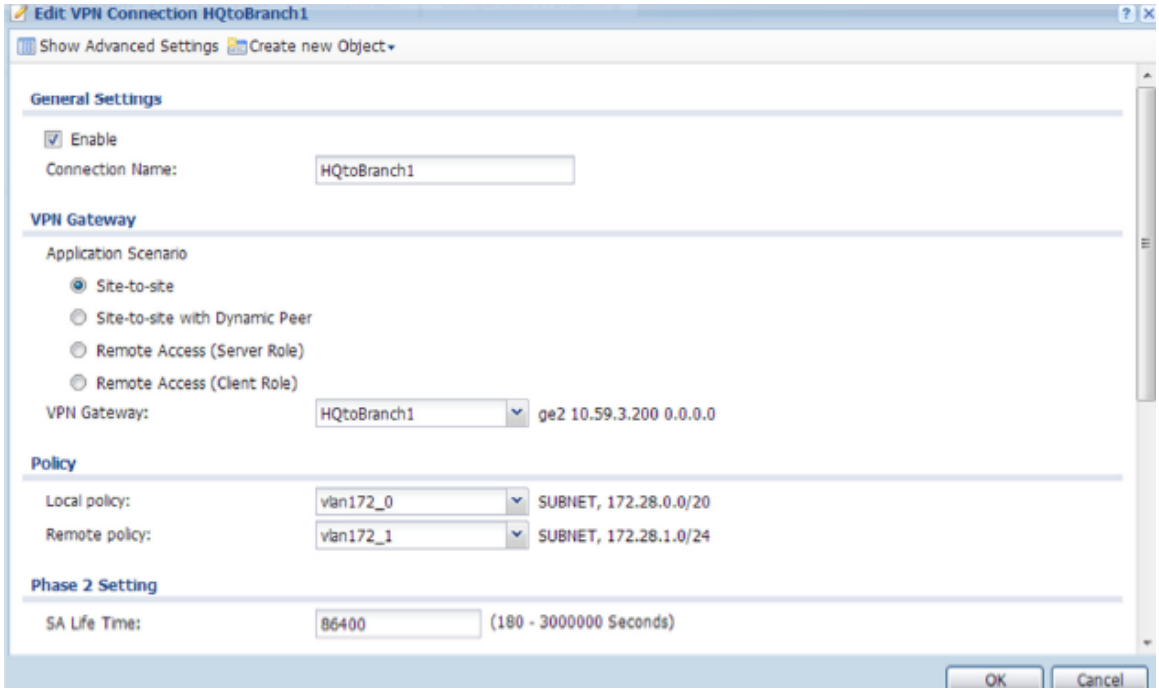
Task 1. Establish IPSec VPN between HQ and Branch 1.

HQ configuration

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

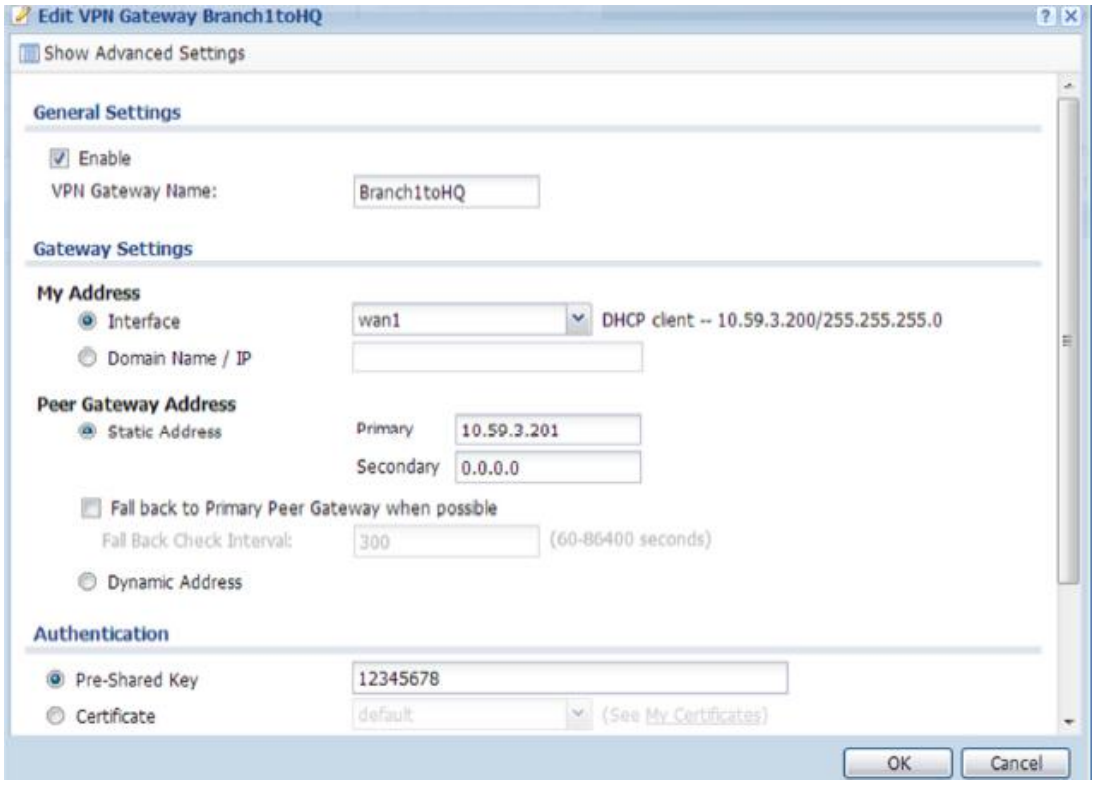


Step2. Configuration > VPN > IPSec VPN > VPN Connection > Edit

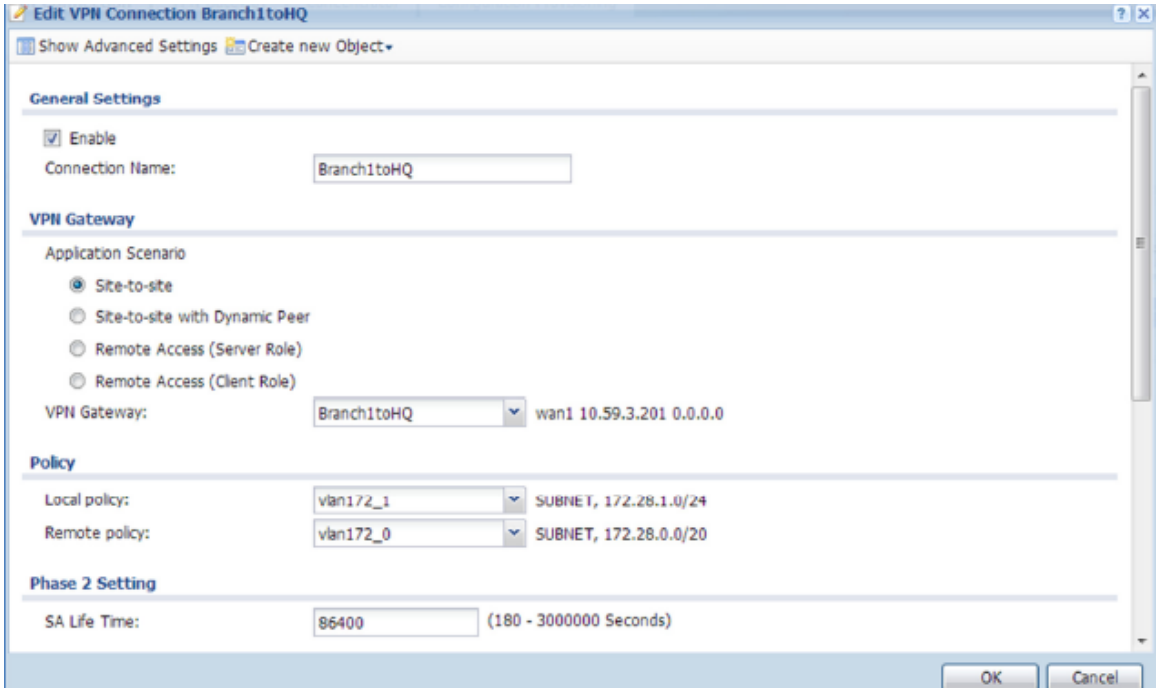


Branch 1 configuration

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



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

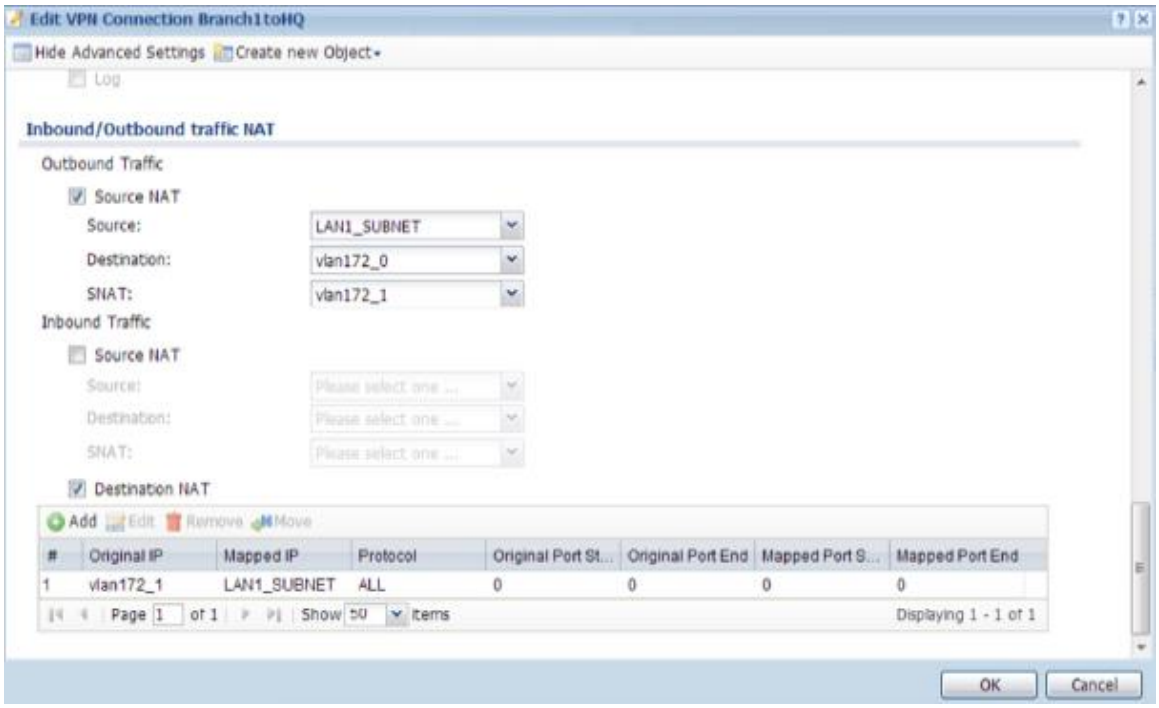


Step 3. Do an SNAT rule in VPN tunnel.

Source: 192.168.1.0/24

Destination:172.28.0.0/20

SNAT:172.28.1.0/24



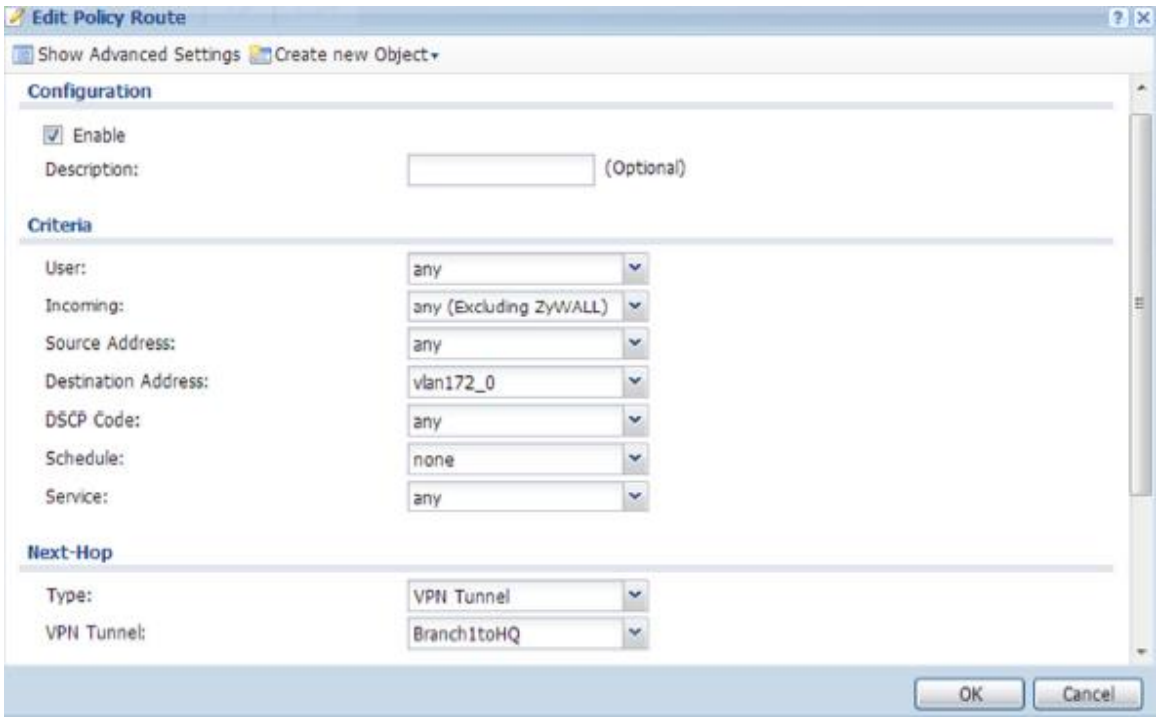
Step 4. Configuration > Network > Routing > Policy Route,

Add a policy route

Source: any

Destination: 172.28.0.0/20

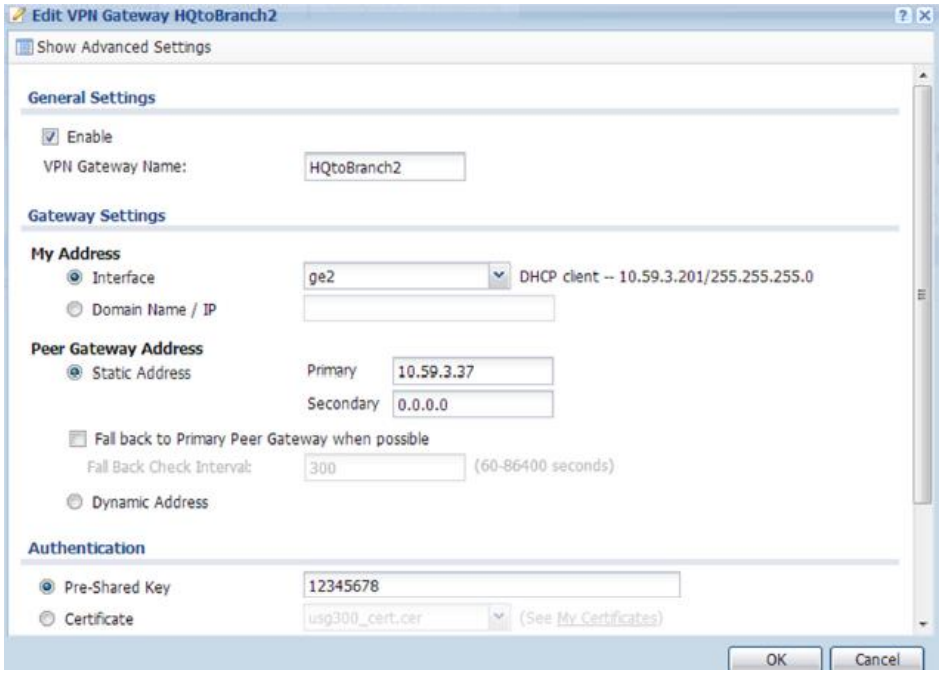
Next-hop: VPN tunnel



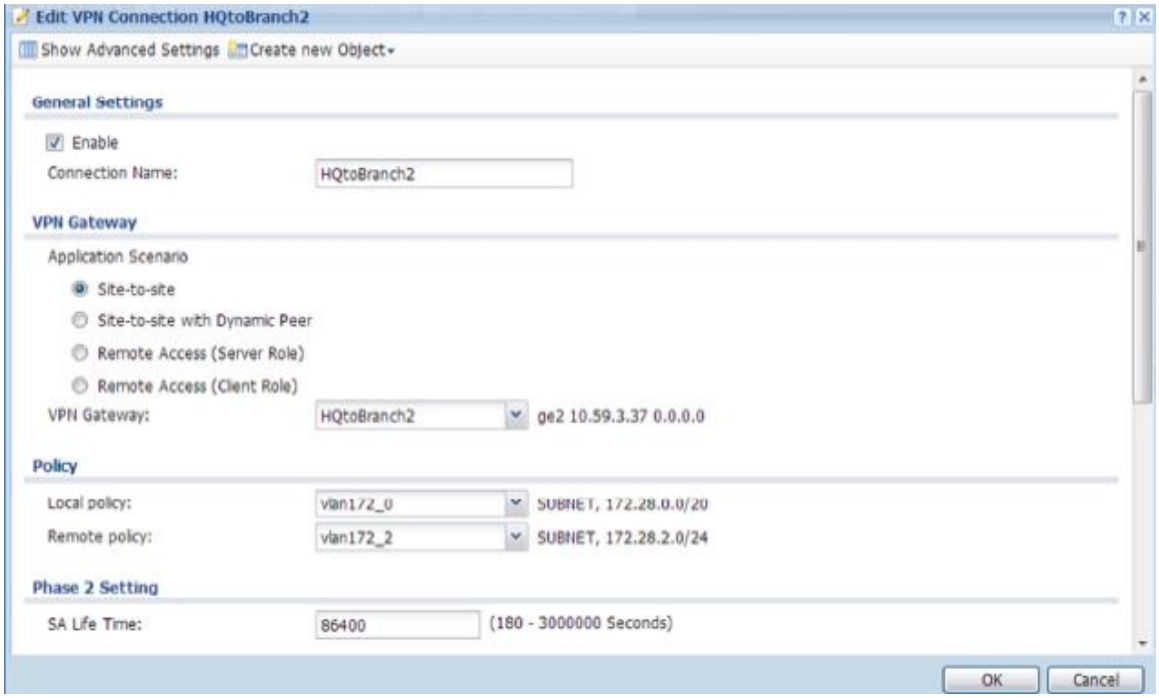
Task 2. Establish IPSec VPN between HQ and Branch 2

HQ configuration

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

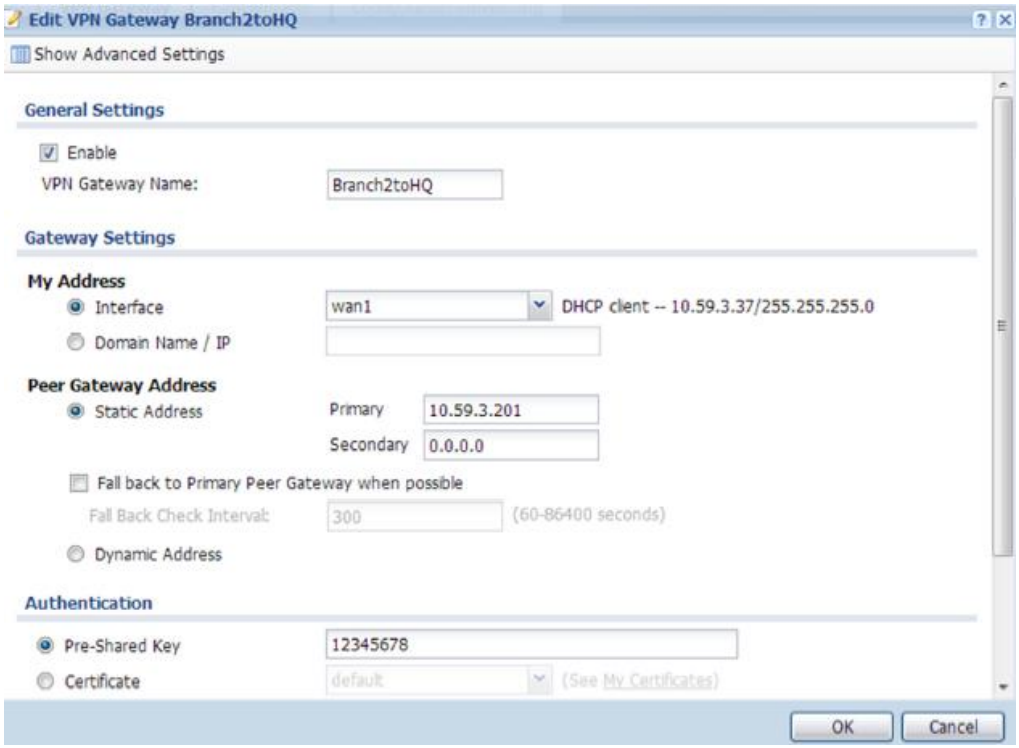


Step 2. Configuration > VPN > IPSec VPN > VPN Connection > Edit

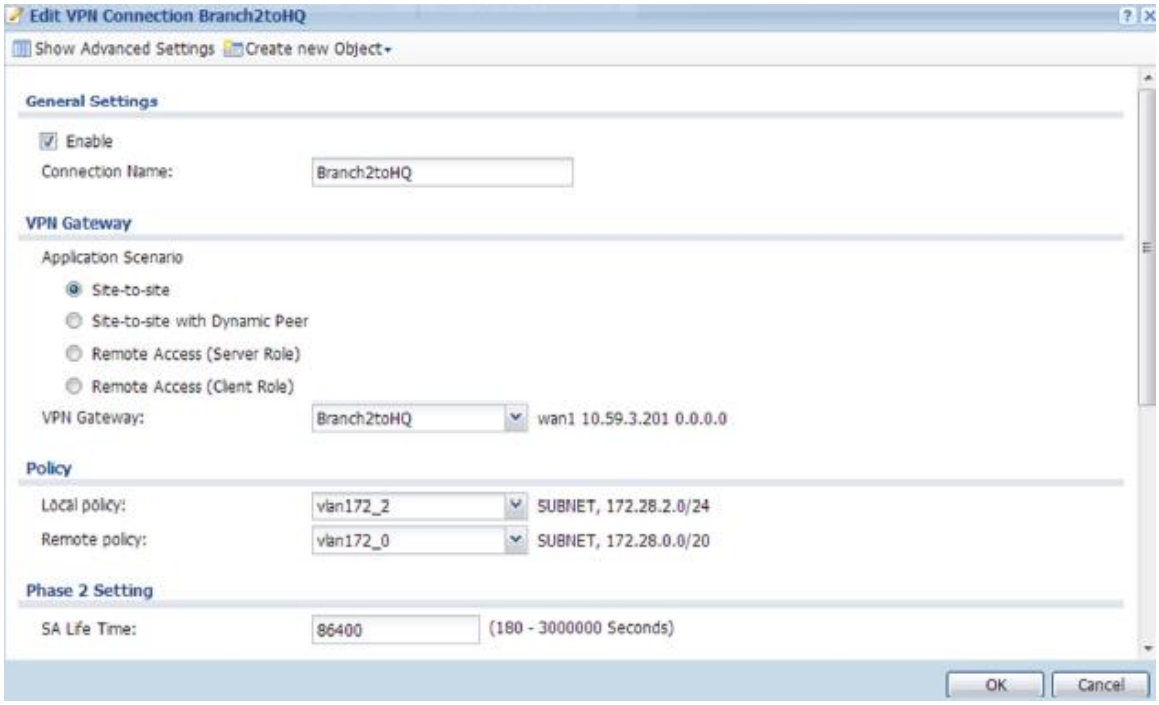


Branch 2 configuration

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



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

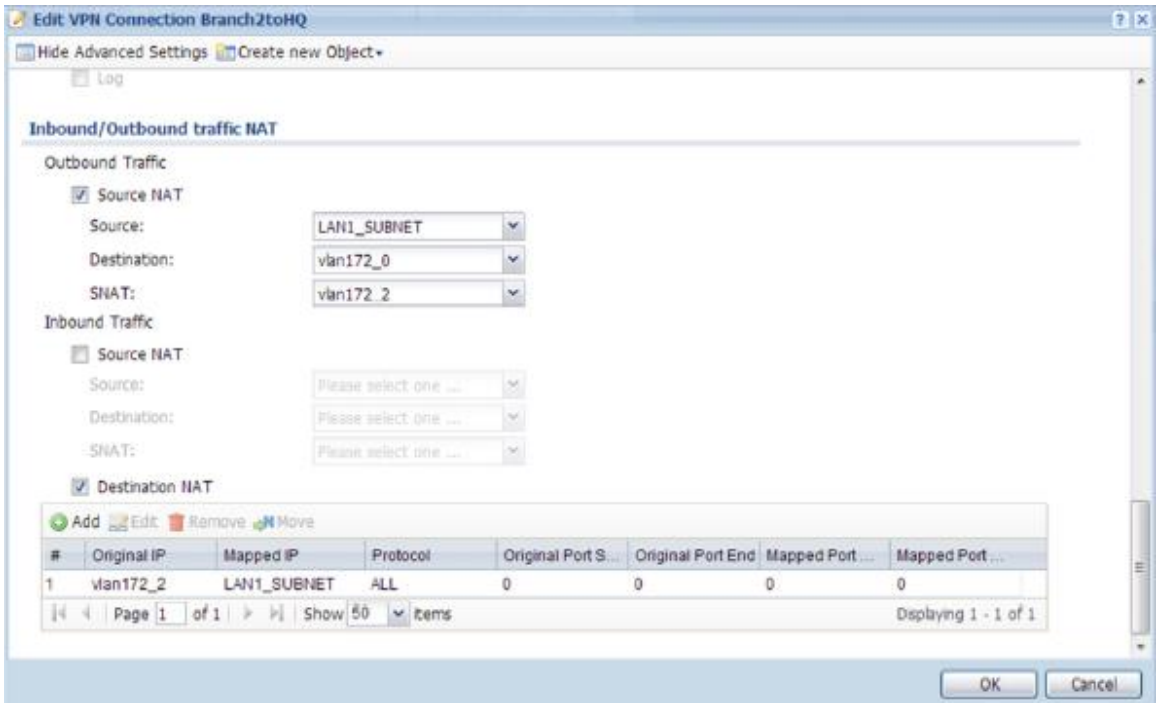


Step 3. Do an SNAT rule in VPN tunnel.

Source: 192.168.2.0/24

Destination:172.28.0.0/20

SNAT:172.28.2.0/24



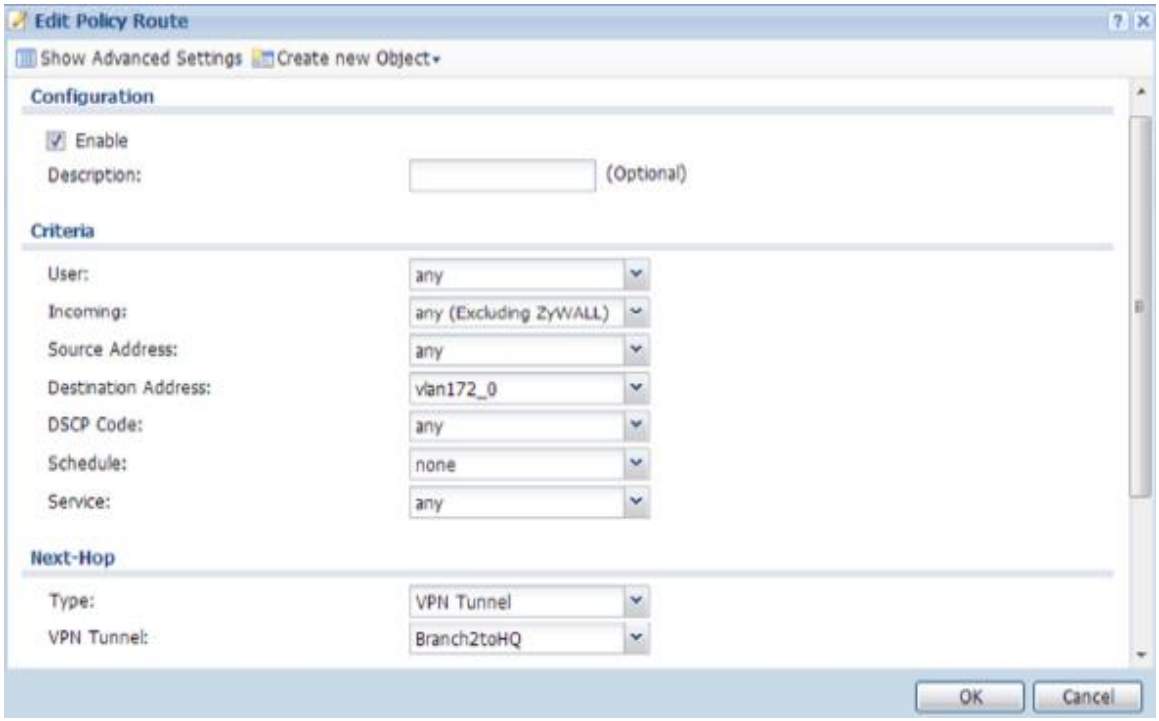
Step 4. Configuration > Network > Routing > Policy Route,

Add a policy route

Source: any

Destination: 172.28.0.0/20

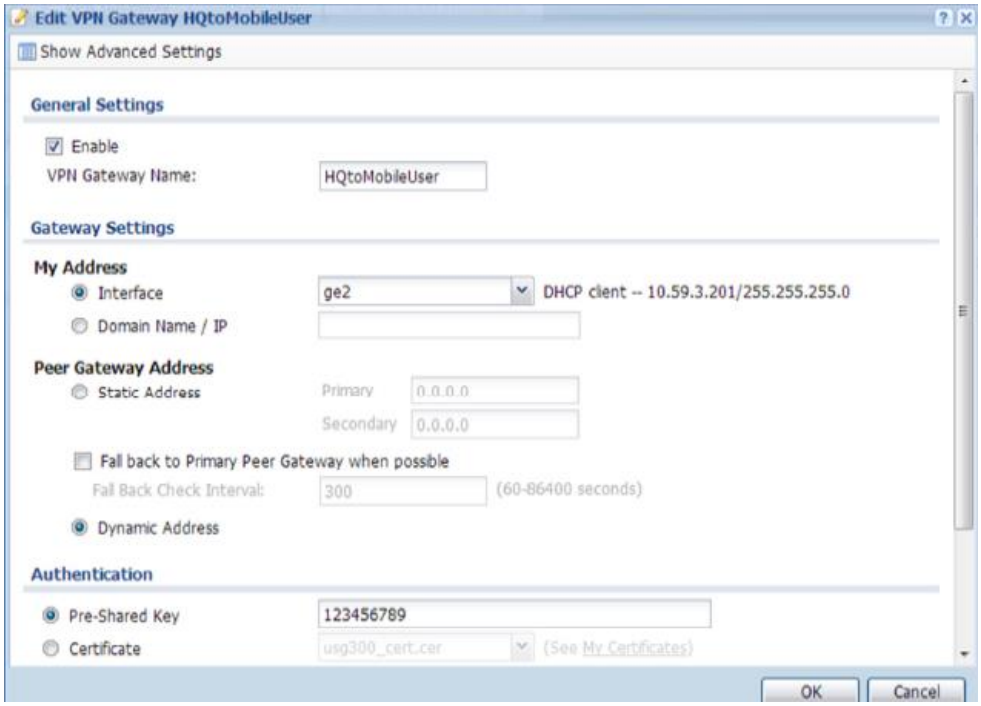
Next-hop: VPN tunnel



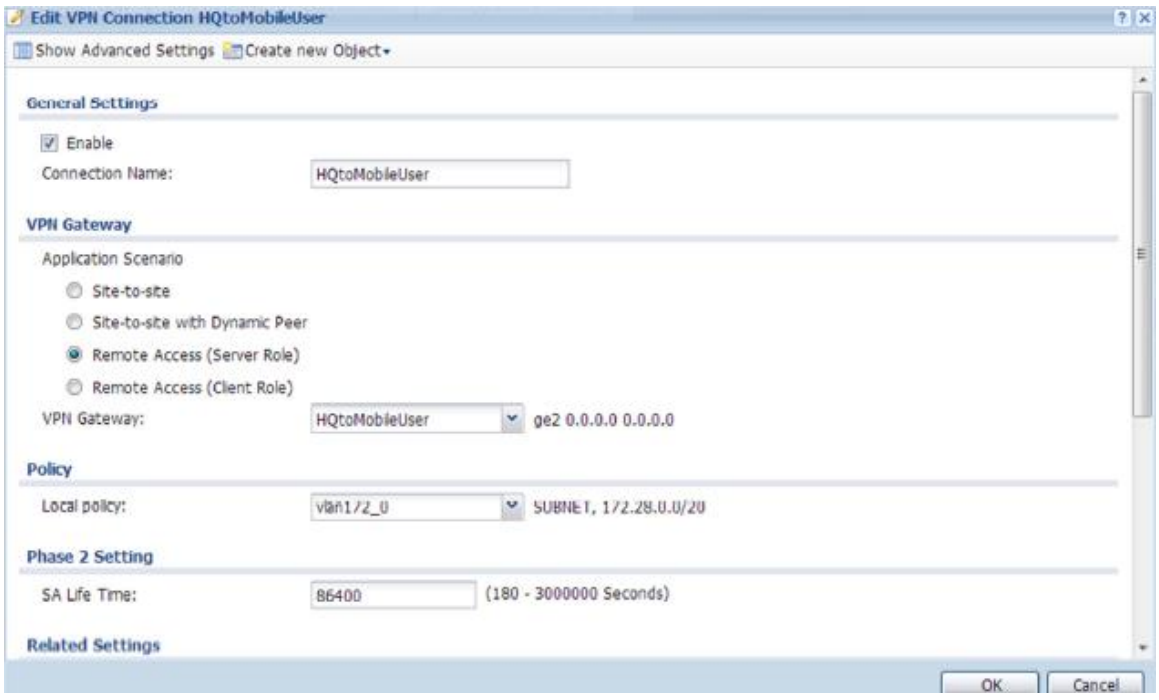
Task 3. Establish Dynamic VPN for mobile users

HQ configuration

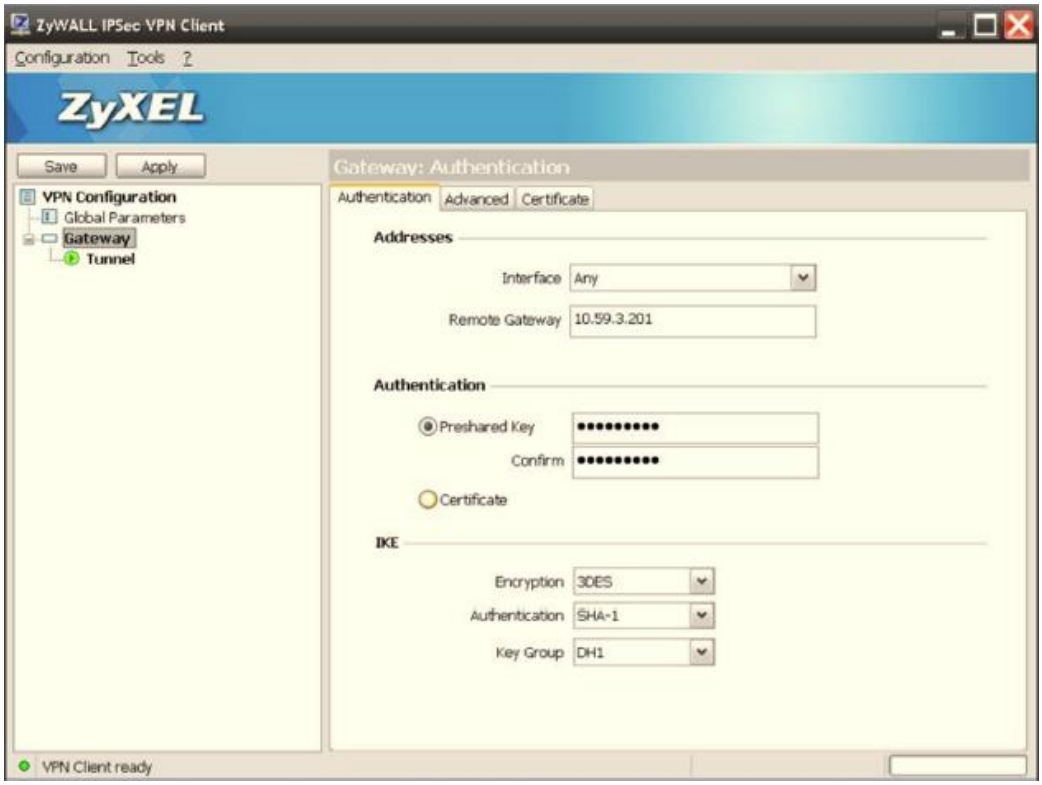
Step 1. Configuration > VPN > IPSec VPN > VPN Gateway > Edit



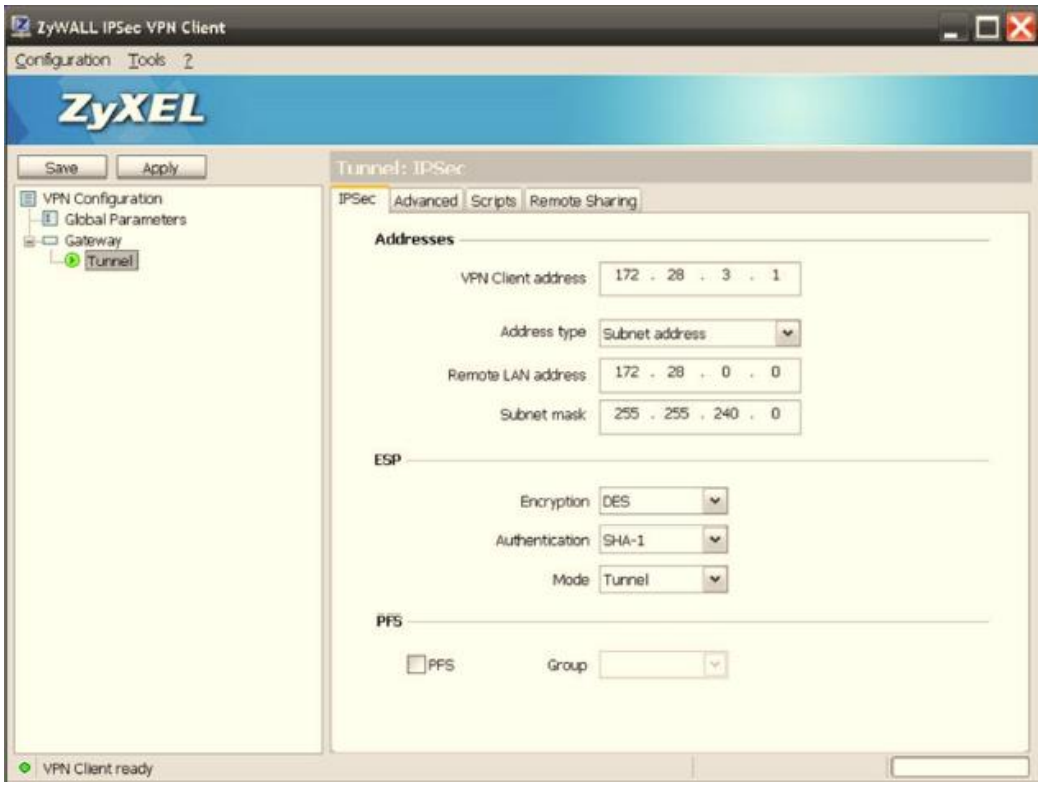
Step 2. Configuration > VPN > IPSec VPN > VPN Connection > Edit



Step 3. IPSec VPN client setting

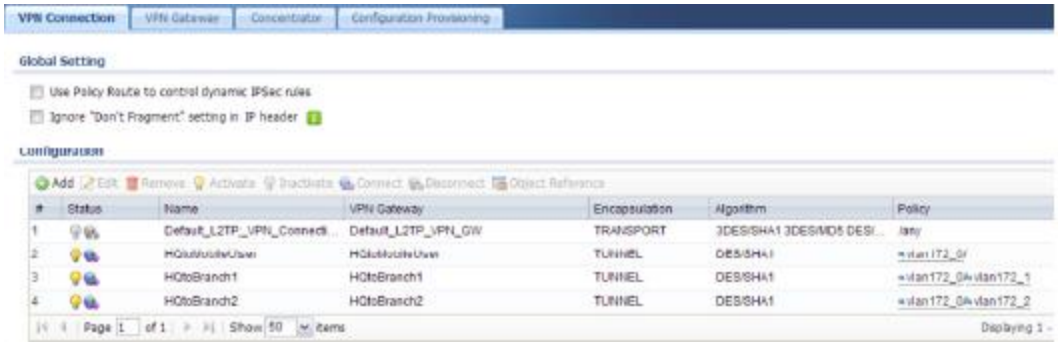


Step 4. In Phase 2, assign one IP for IPSec VPN Client manually.



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

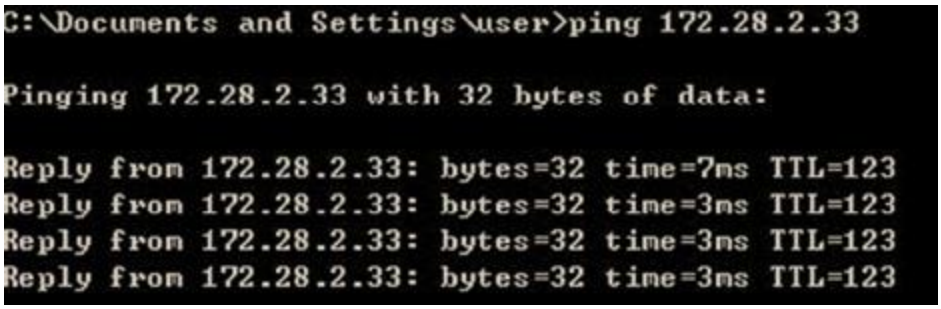
Maintenance > Packet Flow Explore > Routing Status

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