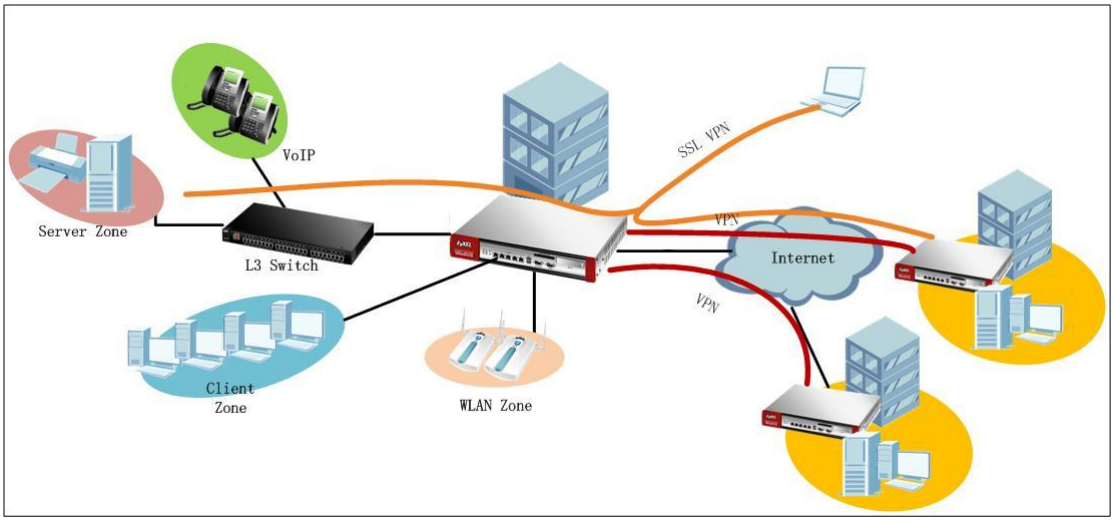
1. Routing and NAT

USG ZyWALL is usually placed at the company network boarder, acting as company network gateway. Routing and NAT are the indispensable functions of USG ZyWALL, responsible for the routing among intranet networks, as well as comprehensive routing between intranet and internet traffic. Thus, correctly set up routing and NAT are very important for the USG ZyWALL to work properly as your requirements.



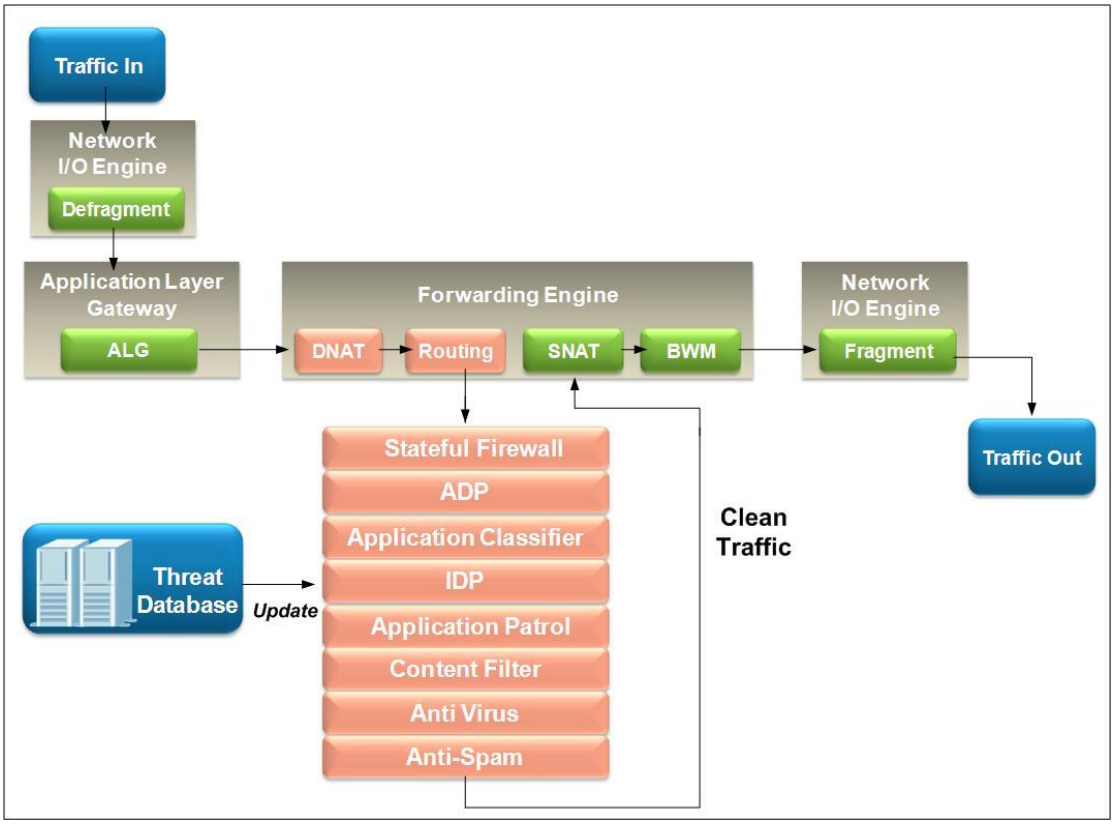
In the scenario above, there're various intranet subnets interconnected. The client zone and WLAN zone are connected directly to the USG ZyWALL, server zone and VoIP client subnets are connected to a switch, and the switch is connected to the USG. All the intranet clients and servers need to be able to access internet, with proper settings of routing and SNAT. The intranet servers should be able to be accessed by internet clients, and also should be able to be accessed by the intranet clients. To enable the branch office intranet clients communicate safely with the HQ internet resources and clients, IPSec VPN are built between the HQ USG and branch office security gateway, so correct VPN routing is also necessary. Telecommunicates not only wants to access the HQ resources via SSL VPN, but also wants to access branch office resources via SSL VPN first to the HQ, then is directed to the branch office via IPSec VPN. To achieve this goal, we also need correct routings set on the USG ZyWALL.

1.1. Understand Packet Flow

Before start setting up Routing and NAT on your USG ZyWALL, understanding its packet flow, Routing and NAT priority may help a lot for your correct setting up.

1.1.1. General Packet Flow

Below is the general packet flow in USG ZyWALL. It reflects how the USG ZyWALL processes traffic from the time it enters ZyWALL from one interface, till it leaves ZyWALL from another interface.



For example, USG ZyWALL receives VoIP packet from LAN interface.

1. The frames sent through network may be fragmented to meet the MTU settings on each router through the path the traffic goes on network. When the USG receives traffic, it will first defragment the frames.
2. The ALG (Application Layer Gateway) will check and alter the application layer information, e.g. Contact information in the SIP message header and SDP information in message body.

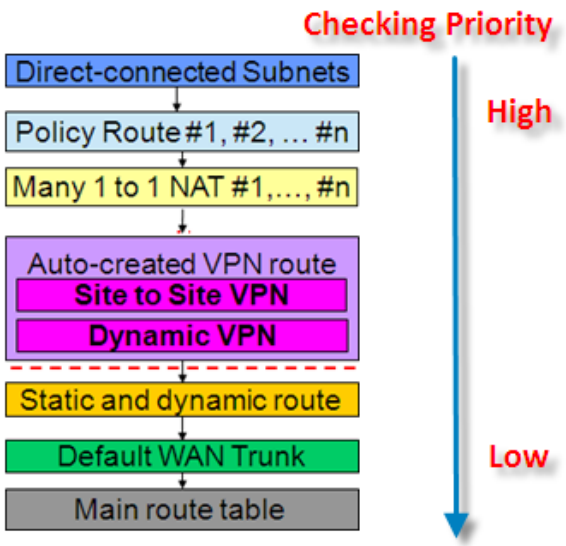
3. Then USG will check whether there's DNAT (Destination NAT) rule set, if there is, it will translate the destination address according to the DNAT rule. If there's not, USG will remain the original destination address. Usually from traffic sent from intranet to outside, there's no DNAT rule set.
4. The traffic is sent to the routing procedure. USG decide where it should send the traffic to, and via which interface.
5. The traffic is sent to the firewall processing stage. If according the firewall rule, the traffic is allowed, USG will allow the traffic to pass, if it's set to Block, the USG will drop the traffic, and generates a log if the firewall rule is set to log.
6. The traffic is sent to the ADP processing stage. USG will perform ADP checking according to ADP rules, and ADP signatures. If the traffic is detected as anomaly attack, the USG will block/log the traffic according to the ADP signatures.
7. The traffic is sent to the IDP processing stage. USG will perform IDP checking according to IDP rules, and IDP signatures. If the traffic is detected as intrusion attack, the USG will block/log the traffic according to the IDP signatures.
8. The traffic is sent to Application Patrol processing stage. USG will check the traffic application layer to determine its class according to relative IDP signatures. If traffic matches some application class, USG will decide how to handle the traffic according to the App Patrol rules.
9. Traffic is sent to Content Filtering processing stage if the traffic is web traffic. USG check what action it should take according to Content Filtering rules.
10. The traffic is sent to Anti-Virus processing stage. USG will examine the traffic with AV signatures. If virus is detected, it will give corresponding action according to AV setting.
11. The traffic is sent to Anti-Spam processing stage if it is mail traffic (SMTP, POP3), then gives corresponding action according to AS settings.
12. The traffic is sent to SNAT procedure. USG will map the traffic's source address according to SNAT rules (outgoing interface, customized address, NAT 1:1 address, etc, which is to be discussed later).
13. The traffic is sent to Bandwidth Management procedure. USG will allocate bandwidth to the traffic if corresponding BWM rule is set.
14. The traffic will be fragmented if the frame is larger than the interface's MTU setting.
15. The traffic is finally sent out.

1.1.2.Routing priority

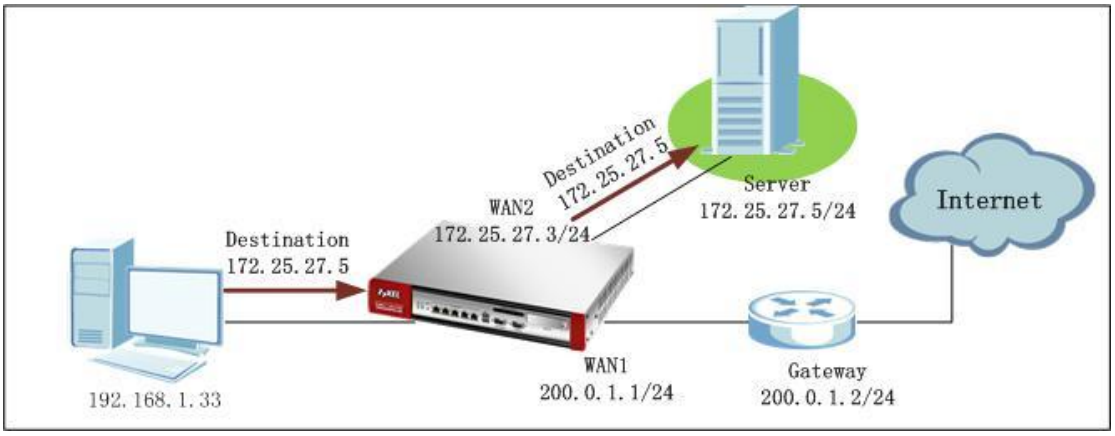
Understanding Routing Priority in USG ZyWALL helps a lot for you to correctly set

up routing rules to fulfill your network scenario requirements.

The picture below shows the routing priority in USG ZyWALL. The priorities determine which routing the USG will take according to the traffic's source, destination, and service type.



1. USG directly connected routing takes first priority over all other routings. Take the following scenario as an example.



On the USG ZyWALL, a policy route is set:

Incoming interface: LAN1

Source Address: LAN subnet 192.168.1.0/24

Destination Address: Any

Service: Any

Next Hop: WAN1 (200.0.1.1)

SNAT: Outgoing Interface

USG receives traffic from LAN1, destination is 172.25.27.5, which is in the direct connected subnet of WAN2 172.25.27.3. Direct route takes first priority. So the traffic will be sent out from WAN2, although in the policy route the next hop is WAN1.

2. Policy Route takes the second routing priority.

There's an advanced setting in Policy Route, which is "Use Policy Route to Override Direct Route". This function will enable Policy Route to take priority over Direct Route. For detail, please go to **1.8 Policy Route vs. Direct Route**

3. One to One NAT routing takes third priority.

Different from ZLD v2.1x, One to One NAT routing is generated automatically by system after One to One NAT rule is set in Configuration>Network>NAT. For detailed explanation, please go to section **1.4 Setting up One to One NAT**

4. IPSec VPN routing takes fourth priority.

Different from ZLD v2.1x, routing for IPSec VPN traffic is generated automatically by system. There's no need to add policy routes for IPSec VPN one by one. For detailed explanation, please go to section **1.9 Routing for IPSec VPN**

5. Static Routes and dynamic routes take fifth priority.

Static routes are manually added by administrator, specifying the next hop for certain destination. Dynamic routes are system dynamically learned routes through routing protocols, such as RIP and OSPF.

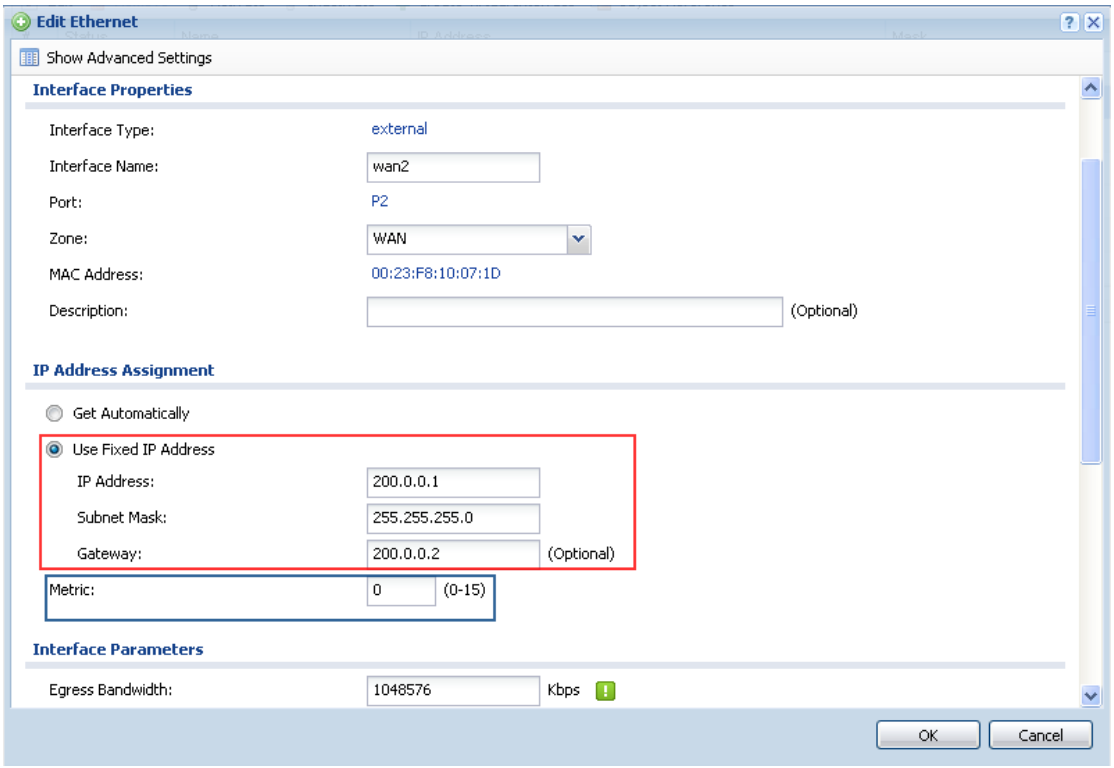
6. Default WAN Trunk takes the sixth priority.

From ZLD v2.20, there's a default WAN Trunk for system routing. If no routings in the higher priorities are present in the device, USG can use the Default WAN Trunk to route traffic. Usually the Default WAN Trunk includes all the systems WAN interfaces and ppp interfaces. For detailed explanation, please go to section **1.2 Default WAN Trunk and Default SNAT.**

7. Routings in system Main route table take last priority in routing.

Main route table generally contains default route learnt from interface default gateway.

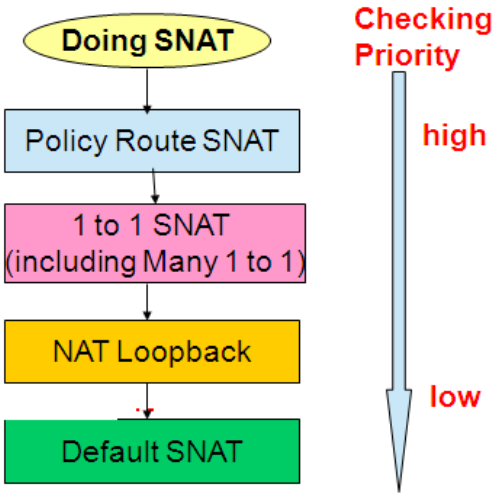
For example, in WAN2 interface, the default gateway is 200.0.0.2. If there's not any routings with higher priorities, the USG will use this route: Sending traffic to gateway 200.0.0.2.



NOTE: Default gateways in different interfaces also have priorities. They're decided by the interface Metric. The smaller the metric value, the higher the priority is. Thus, metric 0 has the highest priority among all the interface default gateways.
If two or more interfaces are using the same metric value, e.g. 0, the first configured interface gateway will have priority over all other later configured interface gateways with the same metric value.

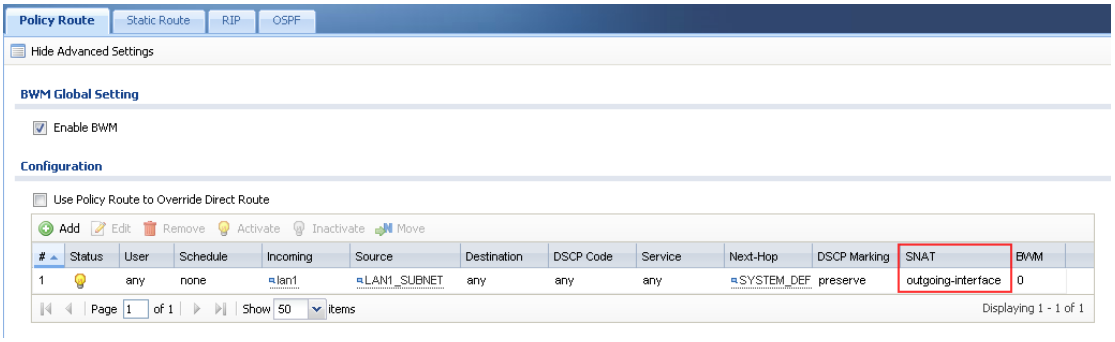
1.1.3.SNAT Priority

The picture below shows the SNAT priorities in USG ZyWALL. The priorities will determine which SNAT rule the USG ZyWALL will use to map the traffic's original source address.



1. Policy Route SNAT takes the first priority.

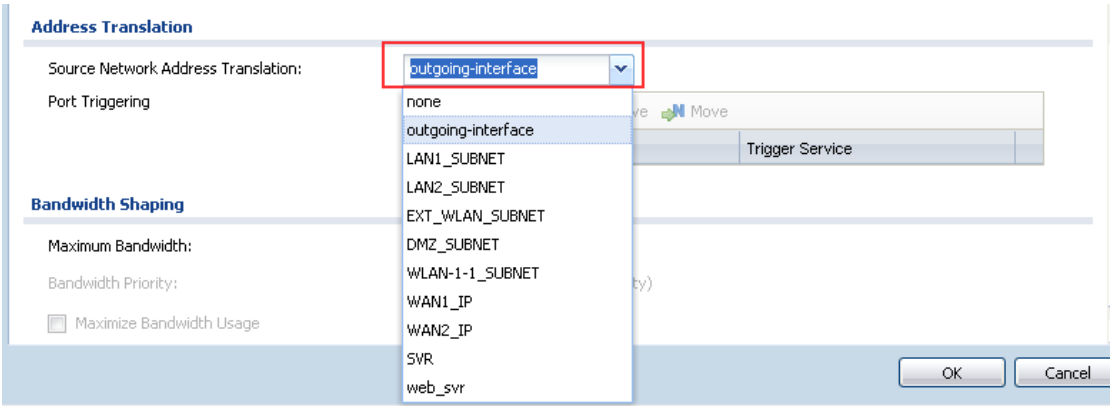
Usually we will set SNAT for traffic in Polity Route.



You can set SNAT to map the original source address to:

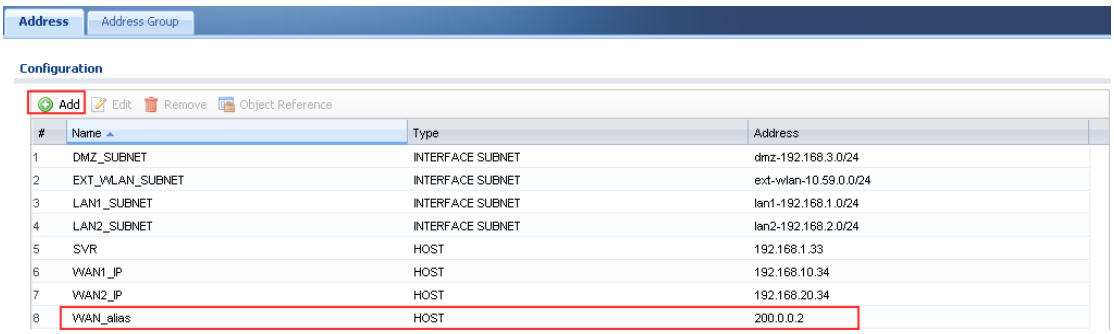
- Outgoing interface
- Customized single address
- Customized group address

Outgoing interface:

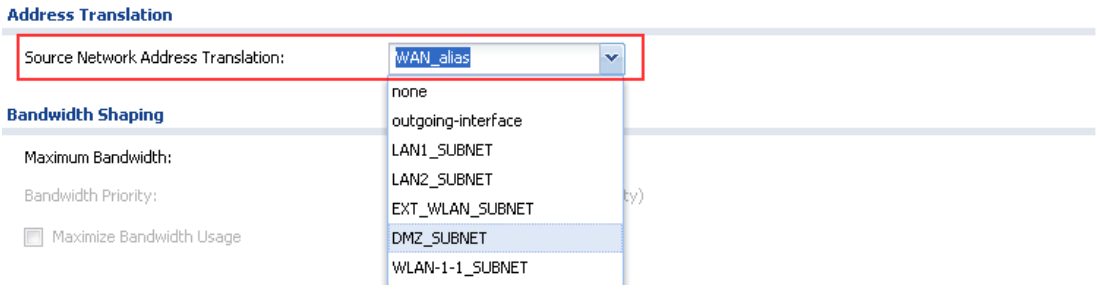


Customized single address:

a. Go to Configuration > Object > Address, add one address object with Type as Host.

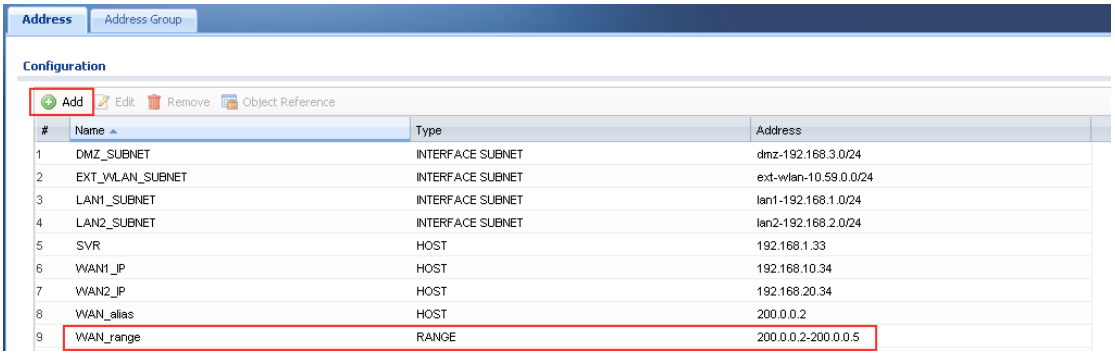


b. Go to Configuration > Network > Routing, add one policy route, and choose the SNAT as the added address object. The source address will be translated to this address 200.0.0.2.

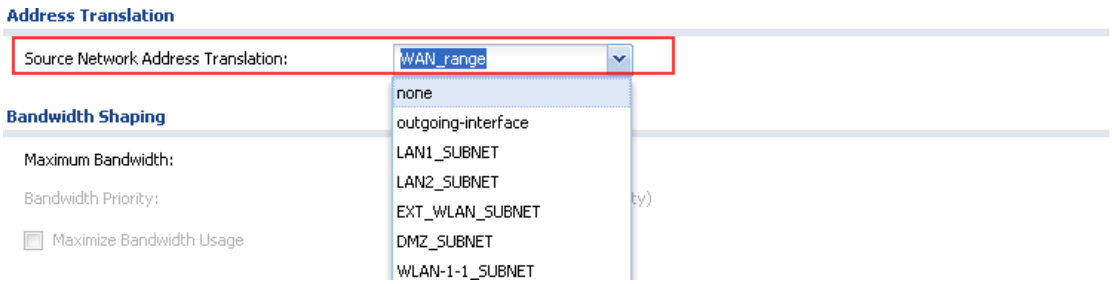


Customized group address:

a. Go to Configuration > Object > Address, add one address object, with Type as Range.

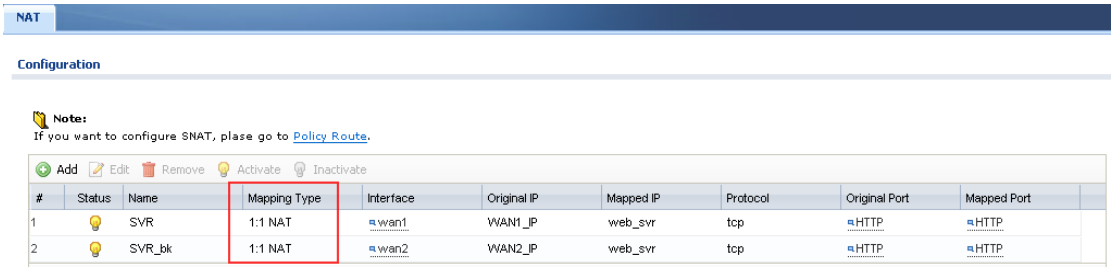


c. Go to Configuration > Network > Routing, add one policy route, and choose the SNAT as the added address object. The source address will be translated to addresses in this range randomly.

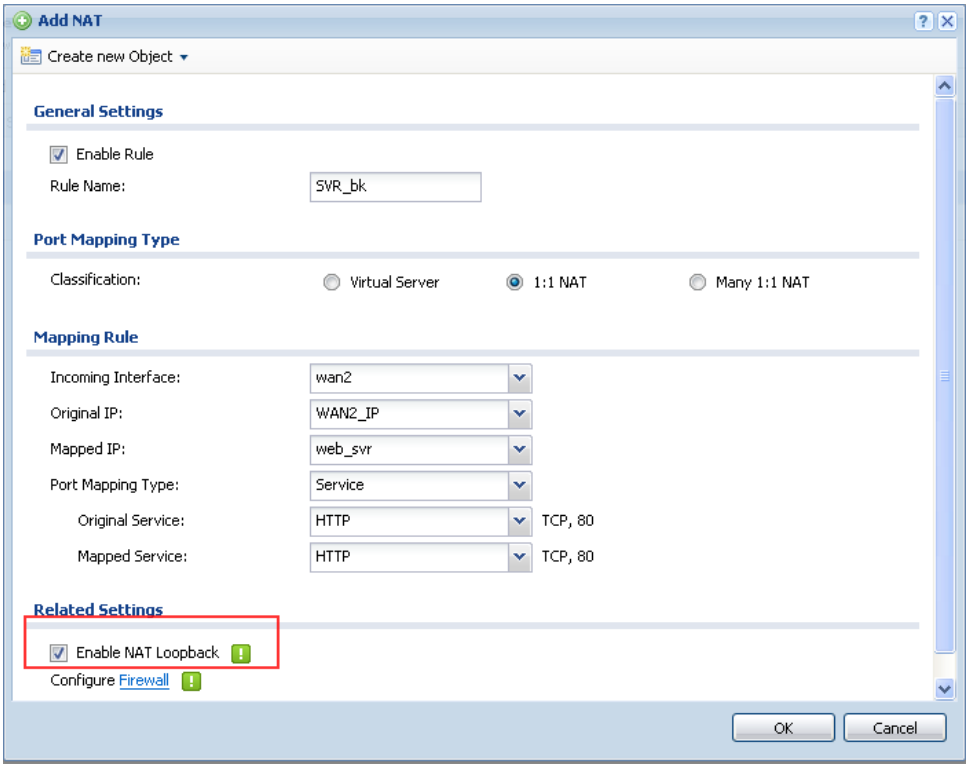


NOTE: If you want to set SNAT as customized single/group address, you cannot set the next hop as Trunk.

2. One to One SNAT takes the second priority. If traffic doesn't match any policy route SNAT, the USG will goes to check whether there's One to One SNAT set. One to One SNAT is set in Configuration > Network > NAT.
   For detailed explanation, please go to section **1.4 Setting up One to One NAT**.

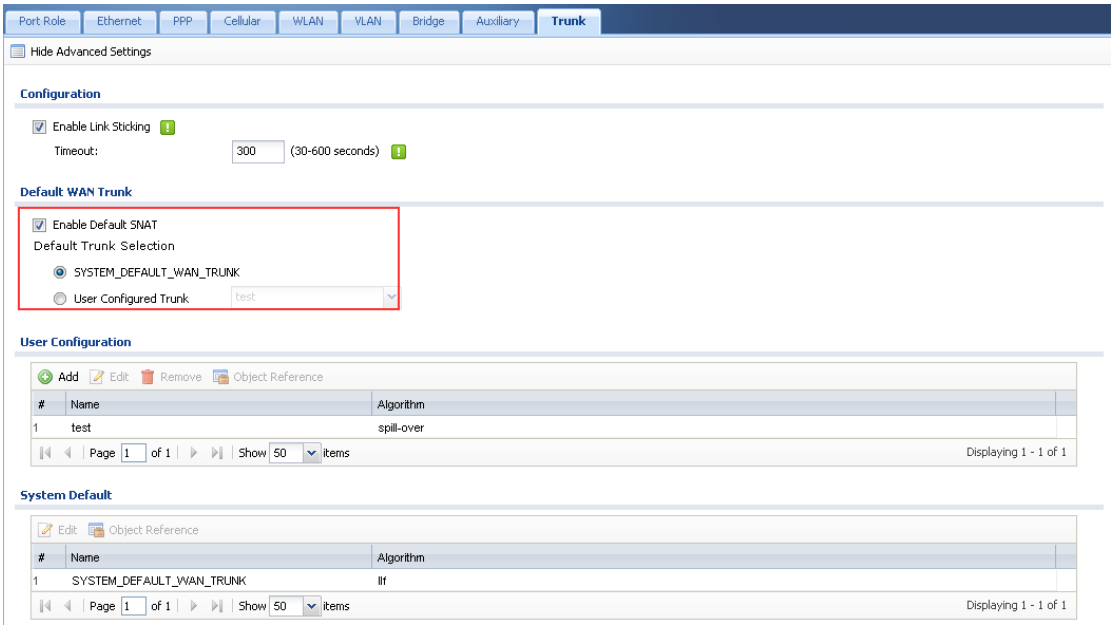


3. NAT Loopback SNAT takes the third priority. NAT Loopback SNAT is generated automatically when you enable NAT Loopback in Configuration > Network > NAT.



For detailed explanation, please go to section **1.6 NAT Loopback**.

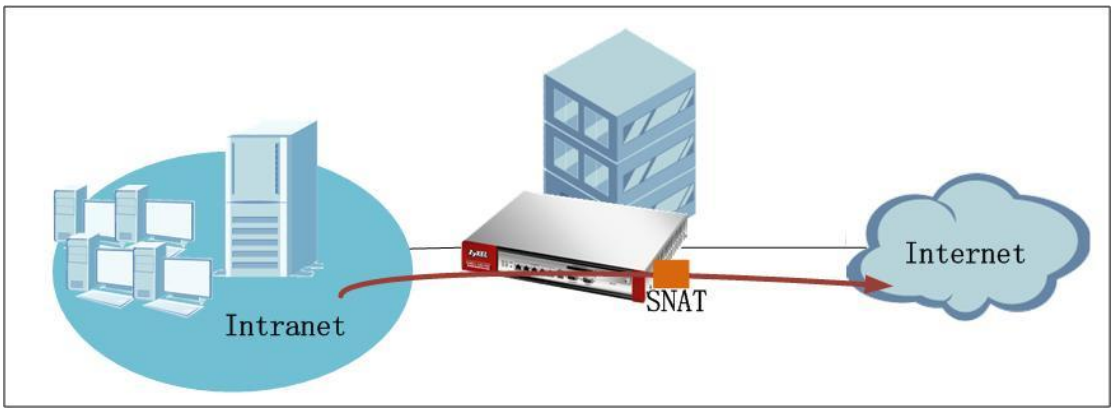
4. Default SNAT takes the last priority. USG ZyWALL uses the Default WAN Trunk to route traffic from intranet to internet, and maps the traffic's original address to the outgoing interface in the Default WAN Trunk.
   Go to Configuration > Network > Interface > Trunk.



For detailed explanation, please go to section **1.2 Default WAN Trunk and Default SNAT.**

1.2. Default WAN Trunk and Default SNAT

Default WAN Trunk and Default SNAT are the newly added features in ZLD v2.20. They're designed for user convenience. With Default WAN Trunk and Default SNAT, user doesn't need to configure policy routes to route intranet traffic to internet. This new routing feature will apply to the traffic from intranet to internet.
USG ZyWALL determines whether the traffic is intranet or internet according to the interface type, which is also a newly added feature in ZLD v2.20.

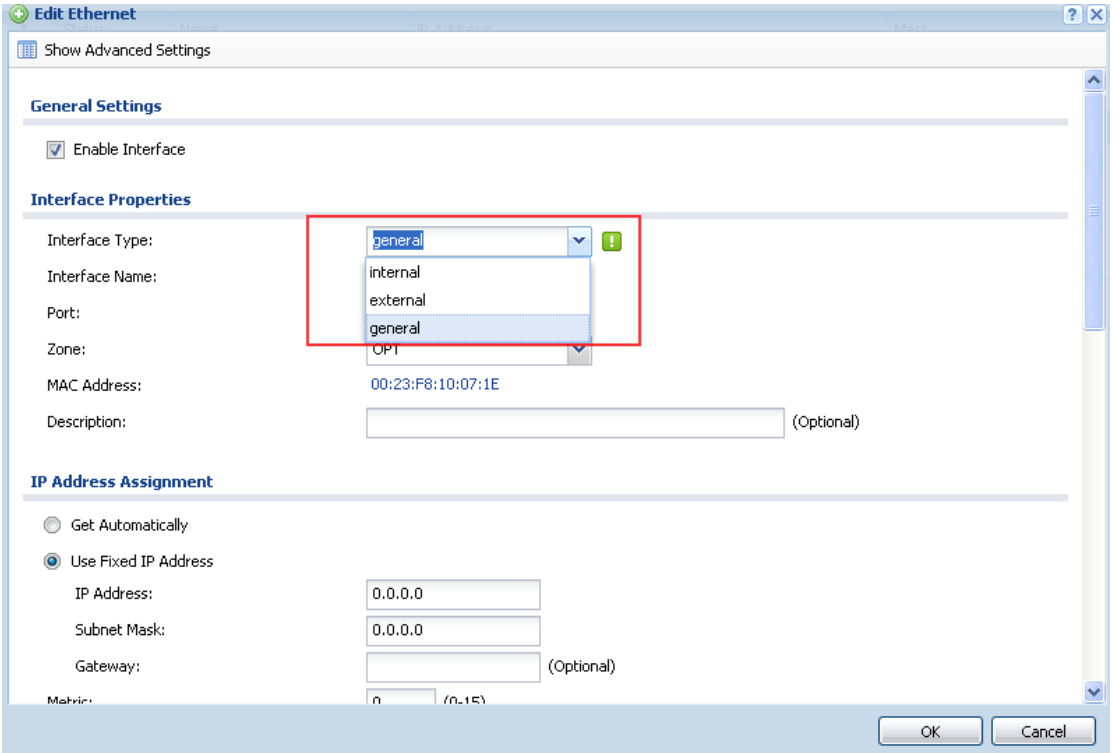


1.2.1. Interface Type

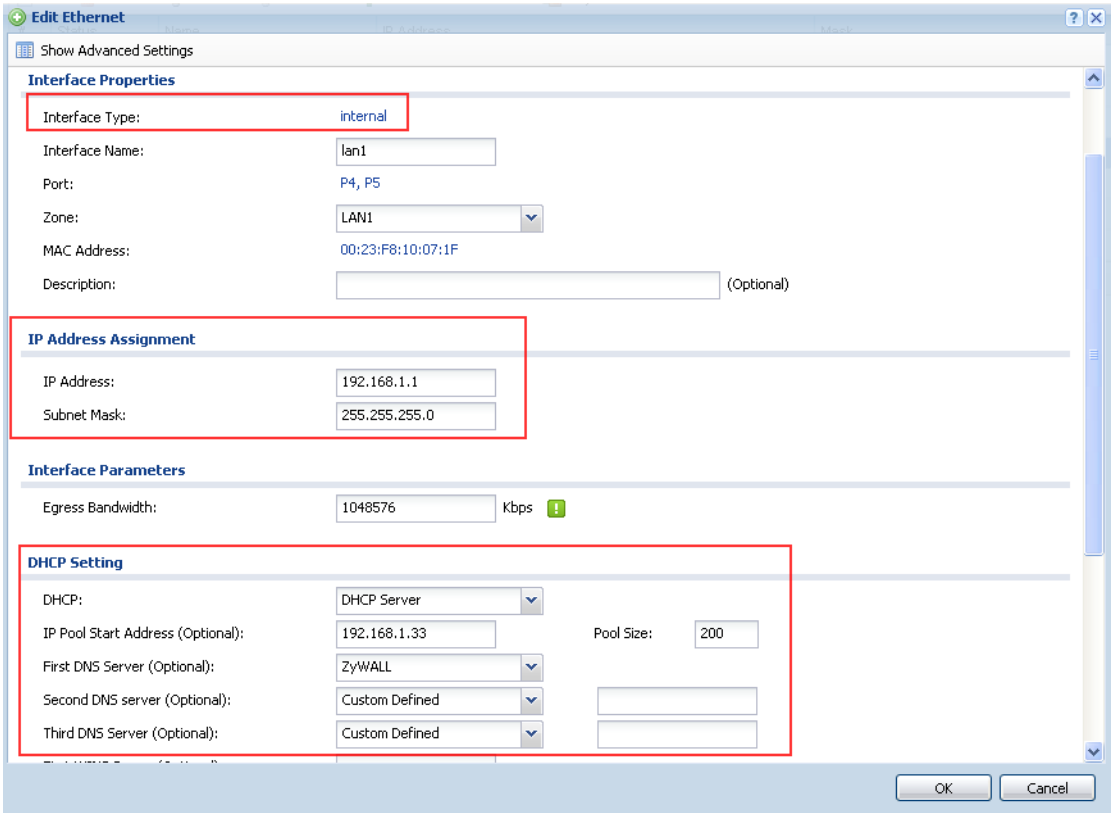
In ZLD v2.2, user can define interface type as the following three types:

- Internal
- External
- General

You can flexibly define each interface's type according to your network scenario.
Go to Configuration > Network > Interface > Ethernet.

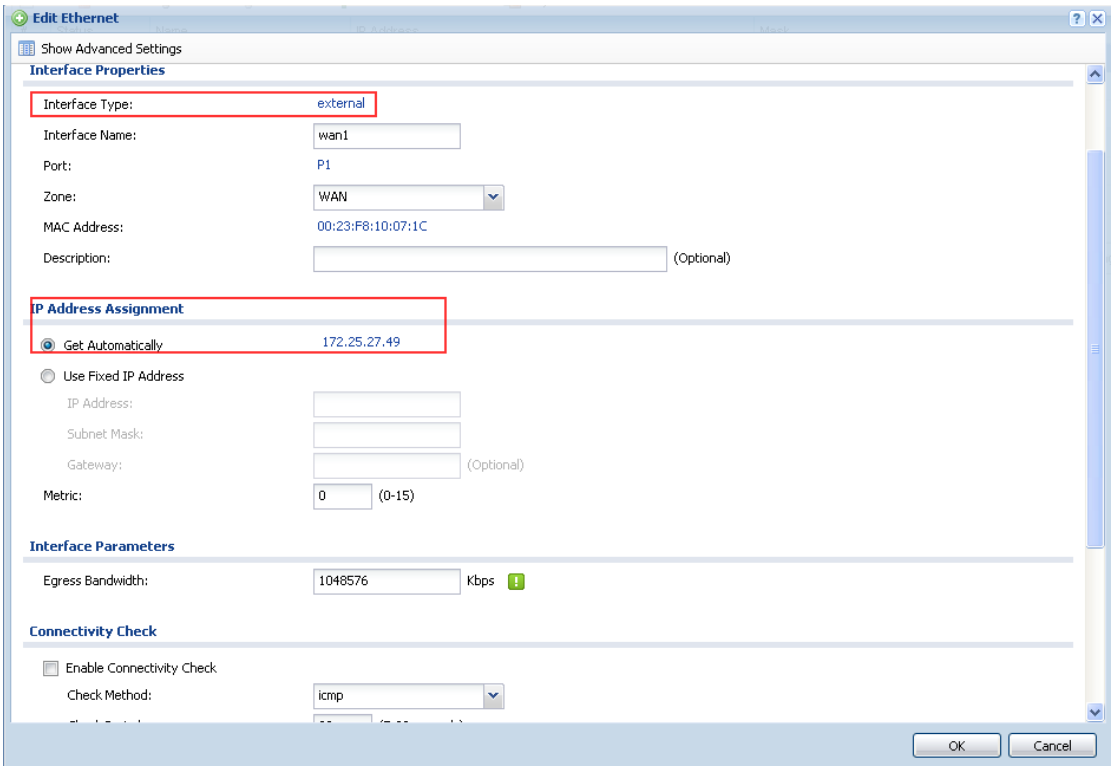


Internal interface is generally connected to the intranet which is behind the USG ZyWALL. An internal interface can act as DHCP server or DHCP Relay. However, it can't act as DHCP client.

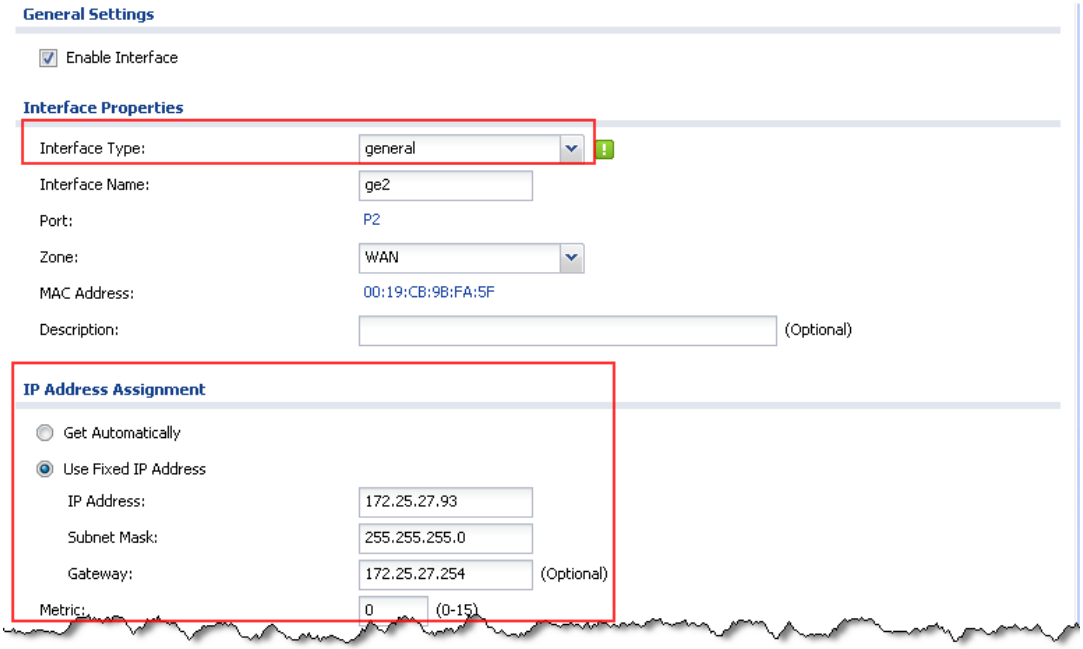


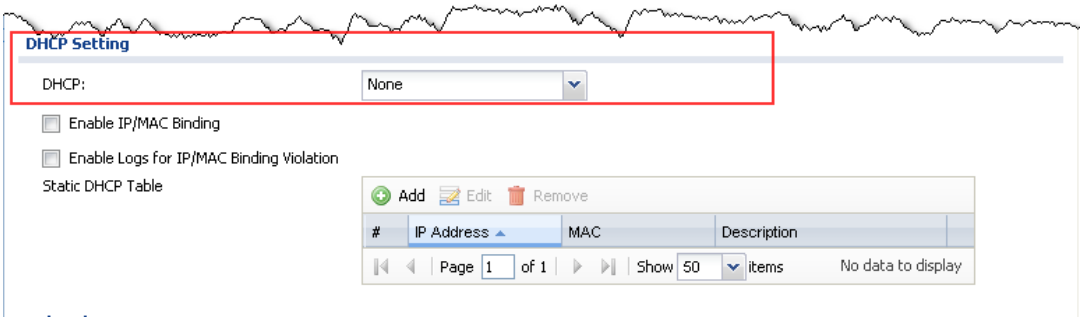
External interface is connected to the WAN side of the USG ZyWALL. An external interface can act as DHCP client. However, it can't act as DHCP server or DHCP relay.

NOTE: All ppp interfaces and aux interface are set as External by system.



General interface can act both as DHCP client or DHCP server and DHCP relay. It's forward compatible with older ZLD versions. Also, if user wants to flexibly configure the interface, he also can set the type as General.





Below is interface type comparison table of different USG models.

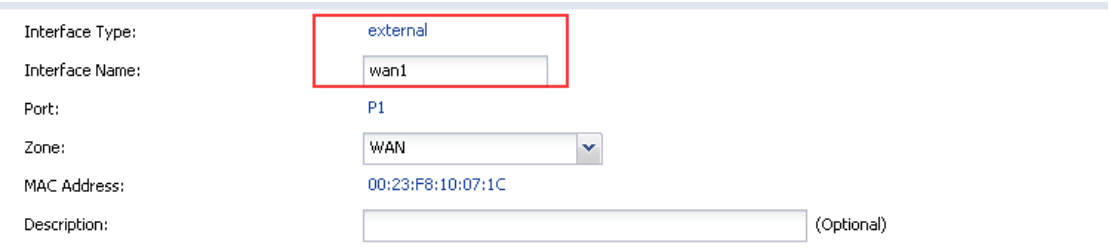
Type	Internal	External	General
Device Model	USG 100/200: LAN1, LAN2, DMZ	USG 100/200: WAN1, WAN2	USG300/1000/2000: ge1, ge2, ge3, ge4. ge5 ...
Set DHCP Client	Not Support	Support	Support
Set DHCP Server	Support	Not Support	Support
Set DHCP Relay	Support	Not Support	Support
Set Default Gateway	Not Support	Support	Support
Set Metric	Not Support	Support	Support
Set Ping Check	Not Support	Support	Support
MAC Address Setting	Not Support	Support	Support

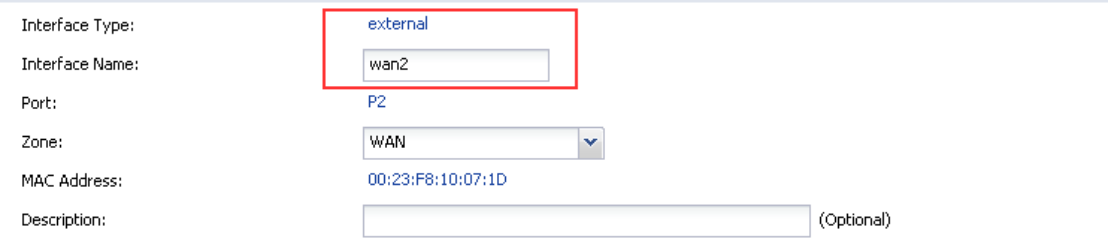
1.2.2.Default WAN Trunk and default SNAT

1.2.2.1. Default WAN Trunk

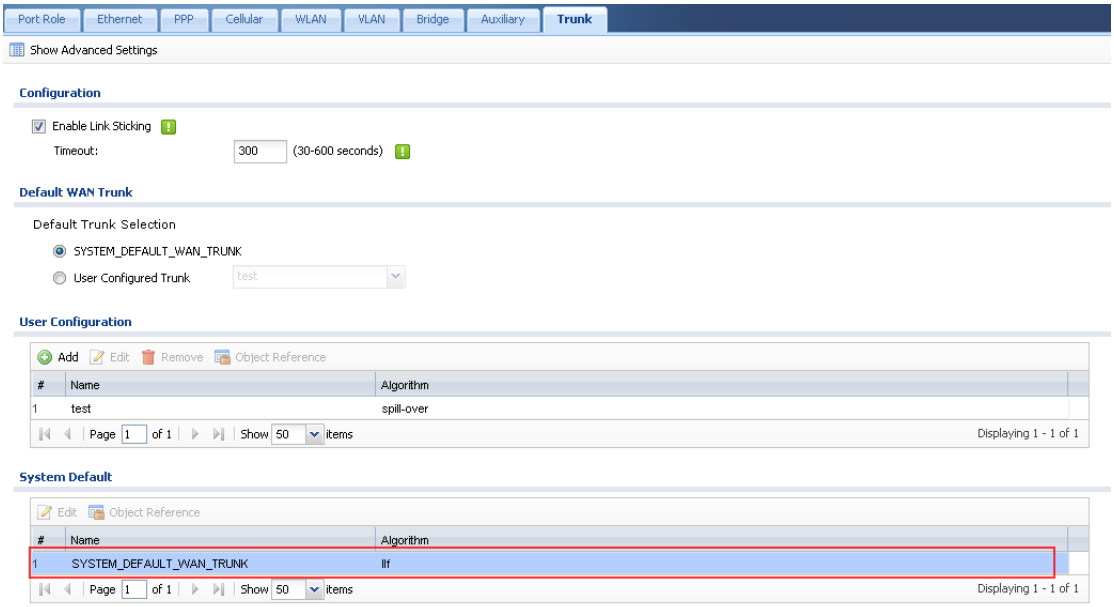
When an interface type is set as External, this interface will be added automatically to the Default WAN Trunk. In other words, the Default WAN Trunk consists of all the USG ZyWALL's external interfaces.

For example, in USG200, interface wan1 and wan2 type are both external.



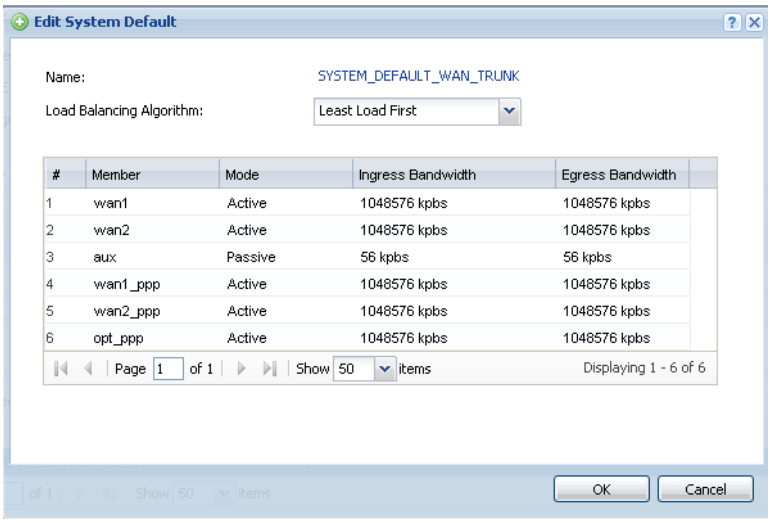


Go to Configuration > Network > Interface > Trunk, check the SYSTEM_DEFAULT_WAN_TRUNK.

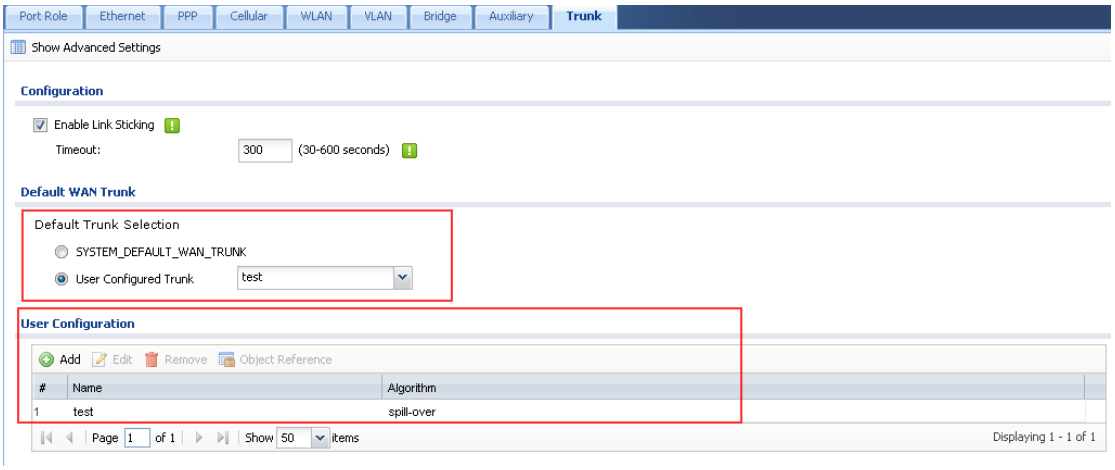


Double click this default WAN trunk, you will find it consists of all the external interfaces.

Please be noted that all ppp interfaces and aux interface are external type by default.

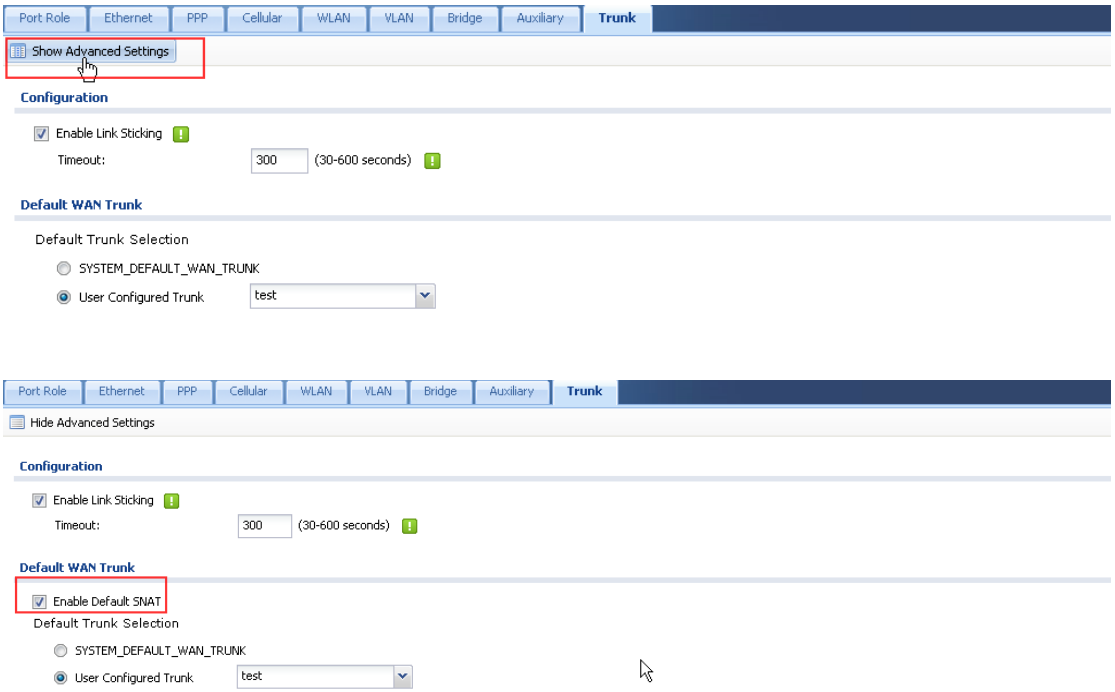


User can also add customized default WAN trunk. Go to Configuration > Network > Interface > Trunk. Add customized WAN trunk in User Configuration, then choose User Configuration Trunk, and select the customized WAN trunk.



1.2.2.2. Default SNAT

Default SNAT is enabled by default. Click Show Advanced Settings, the Default SNAT setting will show. Default SNAT will map traffic's source address to the outgoing interface address in the default WAN Trunk.

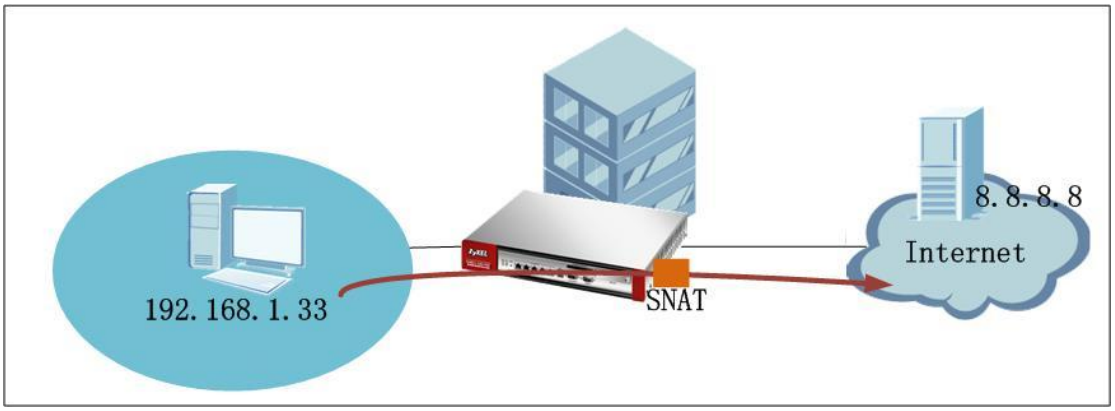


1.2.2.3. Using Default WAN Trunk and Default SNAT

When USG receives traffic from an internal interface, and there's no direct route, policy route, one to one NAT route, static route or dynamic route applicable to this traffic, USG will send it out from the Default WAN Trunk.

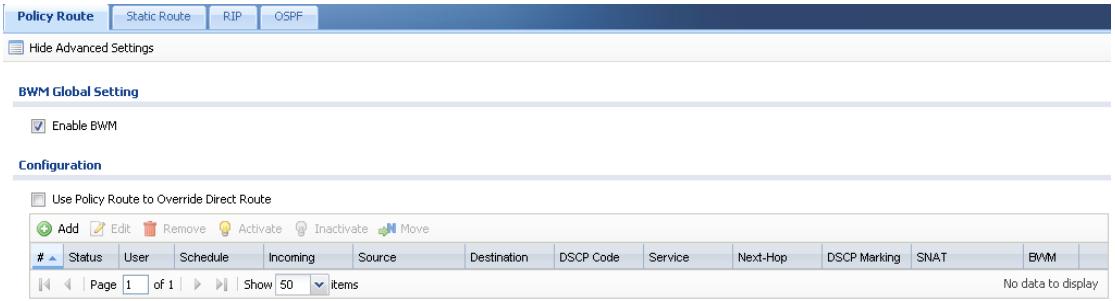
Network scenario:

In the example below, client 192.168.1.33 from intranet wants to ping an internet server 8.8.8.8.

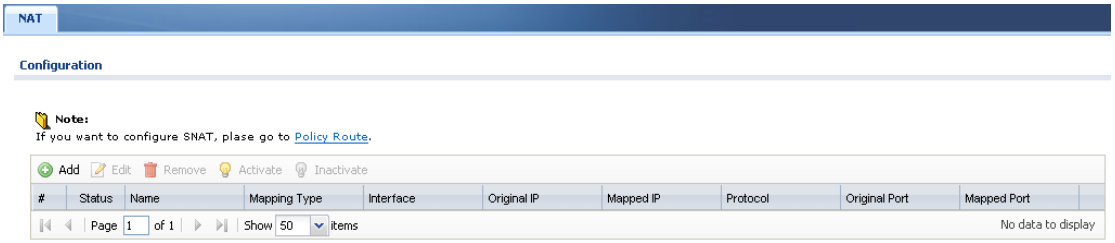


There's no policy route, or NAT 1:1 route set for the traffic.

Policy route setting:



NAT setting:



Clint 192.168.1.33 tries to ping an internet server e.g. 8.8.8.8, the ping is successful. The traffic is in fact sent out from the Default WAN Trunk.

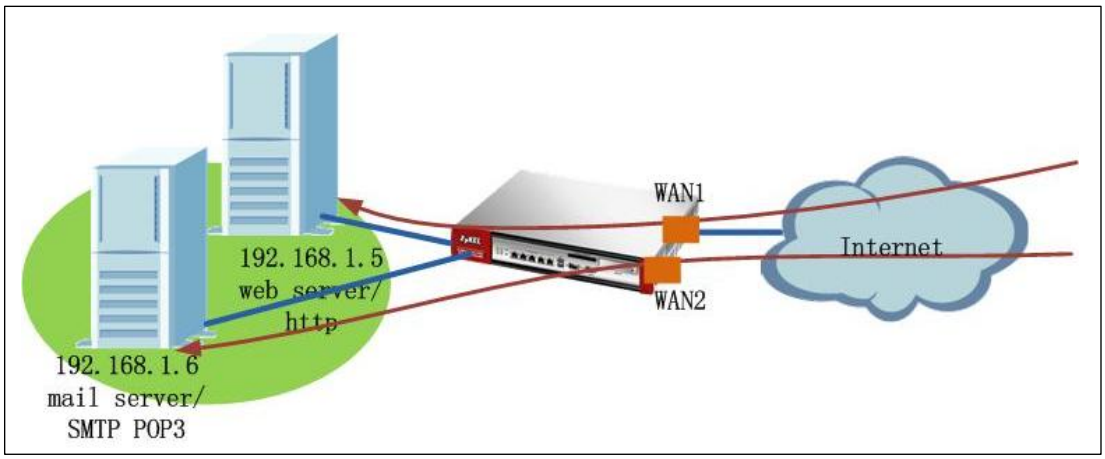
```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.33
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter 本地连接:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time=122ms TTL=236
Reply from 8.8.8.8: bytes=32 time=116ms TTL=236
Reply from 8.8.8.8: bytes=32 time=84ms TTL=236
Reply from 8.8.8.8: bytes=32 time=82ms TTL=236

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 82ms, Maximum = 122ms, Average = 101ms
```

1.3. Setting up Virtual Server

It's a common practice to place company servers behind the USG ZyWALL's protection, and at the mean time, letting WAN side clients/servers accessing the intranet servers. For example, the company may have mail server, which needs to be able to be connect by internet mail servers and clients; the company may also have web server, ftp server, etc, which all need to be accessed from internet. We should configure Virtual Server rules to achieve these applications.

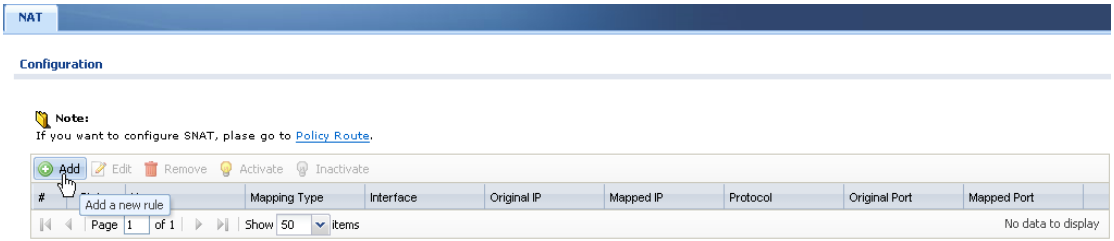
1.3.1. Network Scenario

In the scenario below, network administrator wants the web server (192.168.1.5) to be accessed from WAN1, and the web server (192.168.1.6) to be accessed from WAN2.



1.3.2.Configuration steps

Step1. Go to Configuration > Network > NAT, click Add button to add one NAT rule.



Step2. In the rule editing window, fill in all the necessary fields.

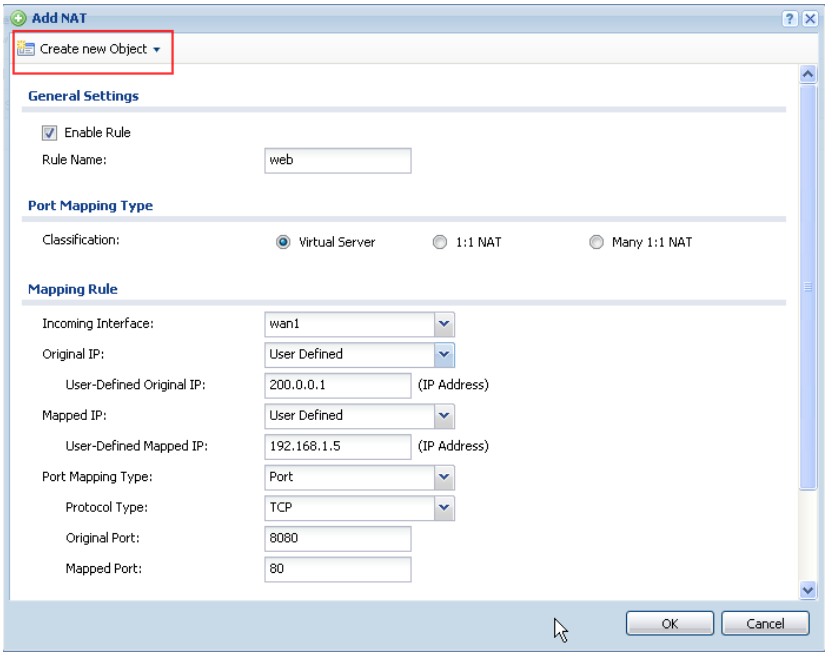
Port Mapping Type: Select Virtual Server

Incoming Interface: For the web server, since you want it to be accessed from WAN1, select wan1.

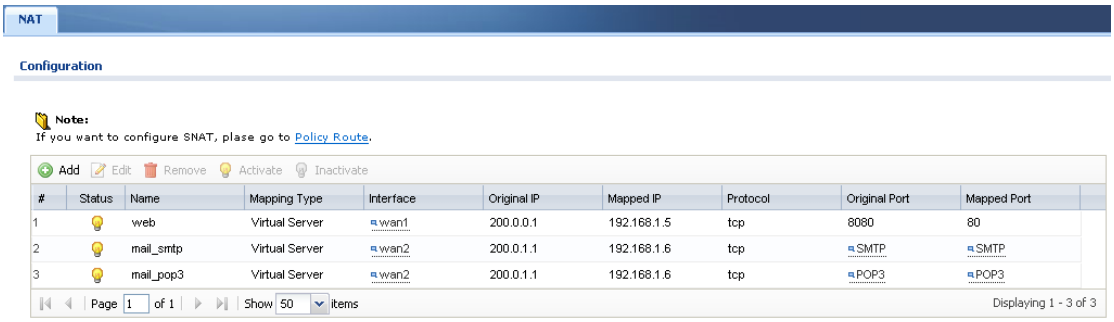
Original IP: You can choose User Defined, and manually enter the WAN1 IP. Or you can first create one address object from the Create new Object field, and then choose this object from the Original IP dropdown list.

Mapped IP: Specify the server IP address. In this case, it's 192.168.1.5. You may also first create one object then select from the dropdown list.

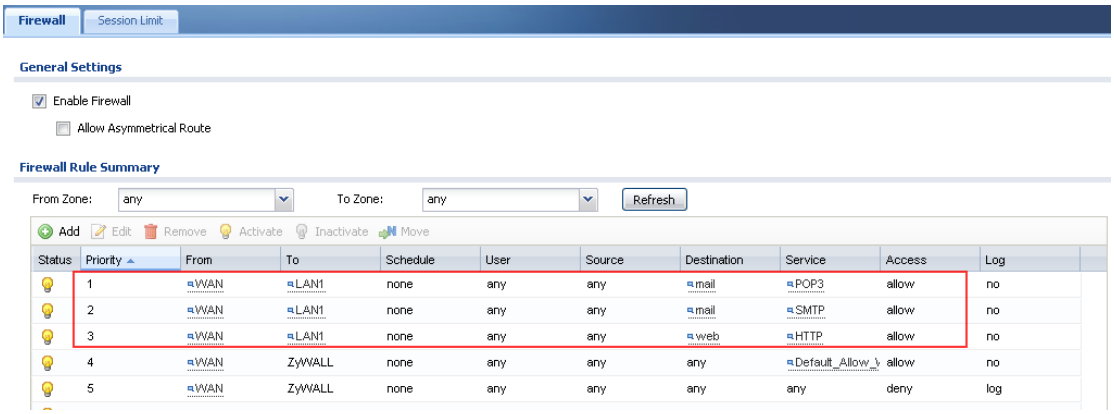
Port Mapping: In this case, to avoid conflicting with the http port of USG itself, we set the original port as TCP 8080, and mapped port as TCP 80.



Following the steps above, add the virtual server rules for the mail server to forward SMTP and POP3 from WAN2 to the server 192.168.1.6.



Don't forget to configure corresponding firewall rule to allow the http, smtp and pop3 traffic from WAN to the LAN servers.

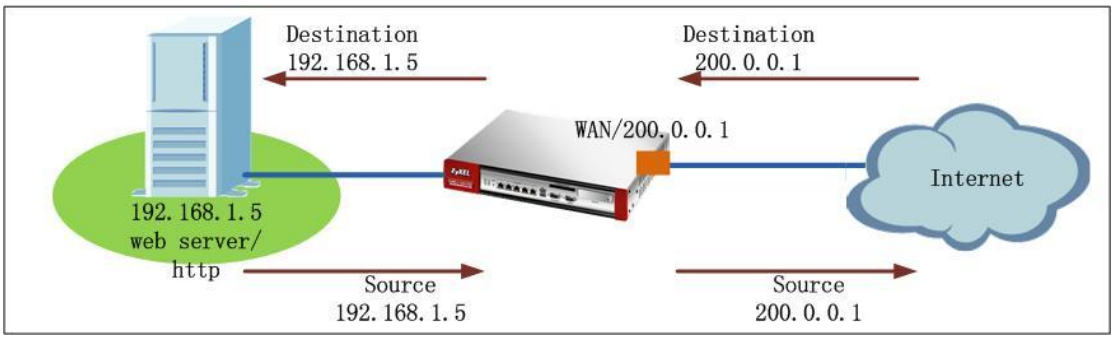


Please not that for the web server forwarding firewall rule, the service is http TCP port 80 instead of TCP 8080. Because in general packet flow, DNAT process precedes firewall checking.

1.4. Setting up One to One NAT

1.4.1. Network Scenario

One to One NAT makes sure one local IP maps to one unique global IP, no matter the traffic is outgoing from local to internet, or incoming from internet to local.

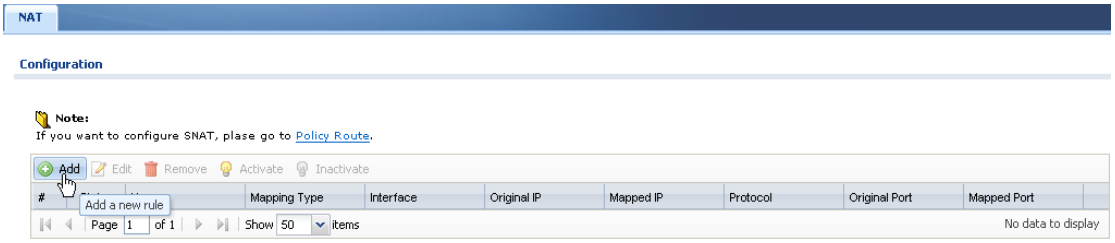


In the scenario above, we map the WAN global IP 200.0.0.1 to the intranet web server 192.168. 1.5. So, when an http client on the internet wants to access the server, its original IP is 200.0.0.1. After the USG receives the traffic, it maps the destination address to 192.168.1.5. When the server replies, its original source IP is 192.168.1.5, when USG receives it, it will translate the source to 200.0.0.1 and send out to the internet client.

After the One to One NAT rule is set, the USG will automatically generate a One to One routing rule in the system, as discussed in section **1.1.2 Routing priority**. So when the server 192.168.1.5 initiates traffic to access internet, if there's no applicable policy route, the USG will use this One to One routing, send out the traffic through the WAN interface 200.0.0.1, and maps the source address to 200.0.0.1.

1.4.2. Configuration Steps

Step1. Go to Configuration > Network > NAT, click Add button to add one NAT rule.



Step2. In the rule editing window, fill in all the necessary fields.

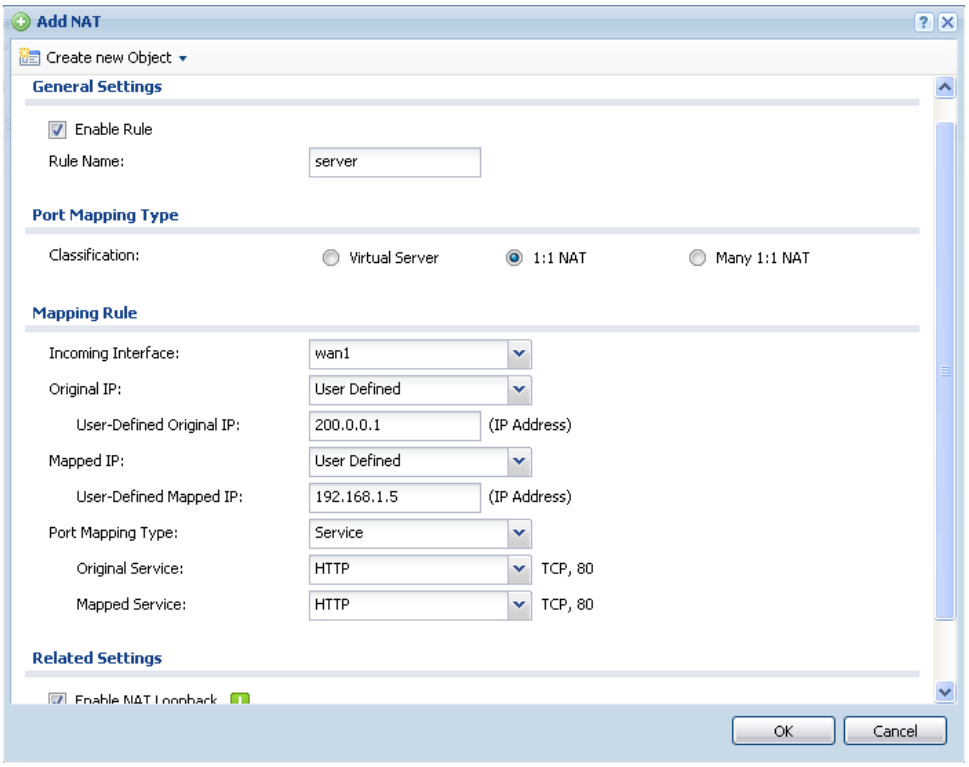
Port Mapping Type: 1:1 NAT.

Incoming Interface: Select the WAN interface you want the USG to receive the incoming traffic to the server.

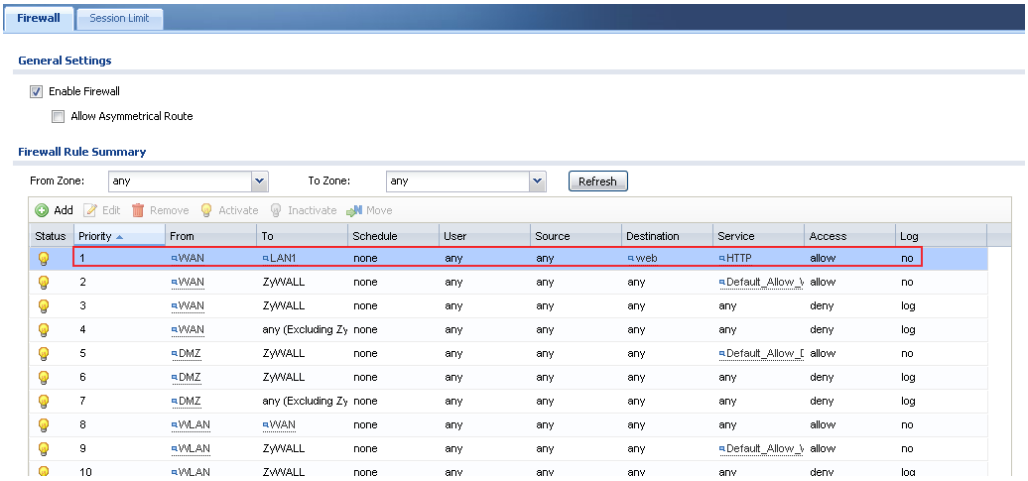
Original IP: You can choose User Defined, and manually enter the WAN1 IP. Or you can first create one address object from the Create new Object field, and then choose this object from the Original IP dropdown list.

Mapped IP: Specify the server IP address. In this case, it's 192.168.1.5. You may also first create one object then select from the dropdown list.

Port Mapping: In this case, we choose mapping type as "Service", and service HTTP.



Don't forget to configure corresponding firewall rule to allow the http traffic from WAN to the LAN server 192.168.1.5.

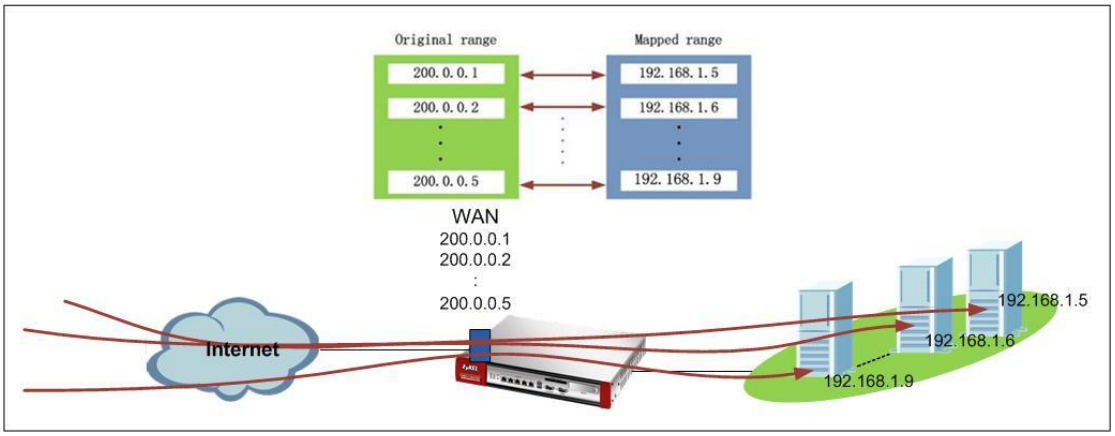


1.5. Setting up Many One to One NAT

Many One to One NAT rule equals setting up the corresponding number of One to One NAT rules.

The number of IP addresses in the original IP Subnet/Range should equal number of IP addresses in the Mapped Subnet/Range. The first IP in the original range will be mapped to the first IP in the mapped range, the second IP in the original range will be mapped to the second IP in the mapped rang… and so on.

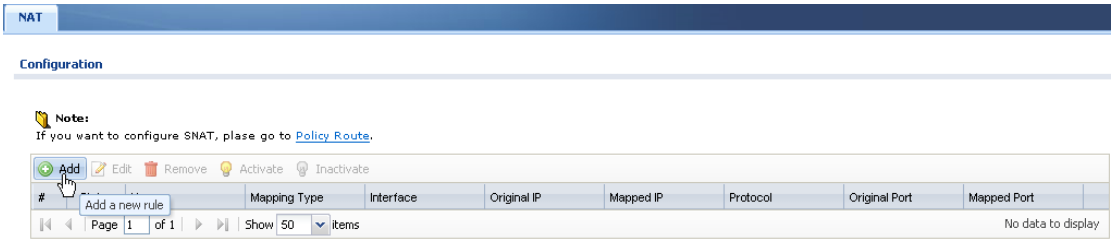
1.5.1. Application Scenario



The scenario above requires that a range of global addresses are mapped to a range of local addresses with the same number of addresses.

1.5.2.Configuration Steps

Step1. Go to Configuration > Network> NAT, click Add button to add one NAT rule.



Step2. In the rule editing window, fill in all the necessary fields.

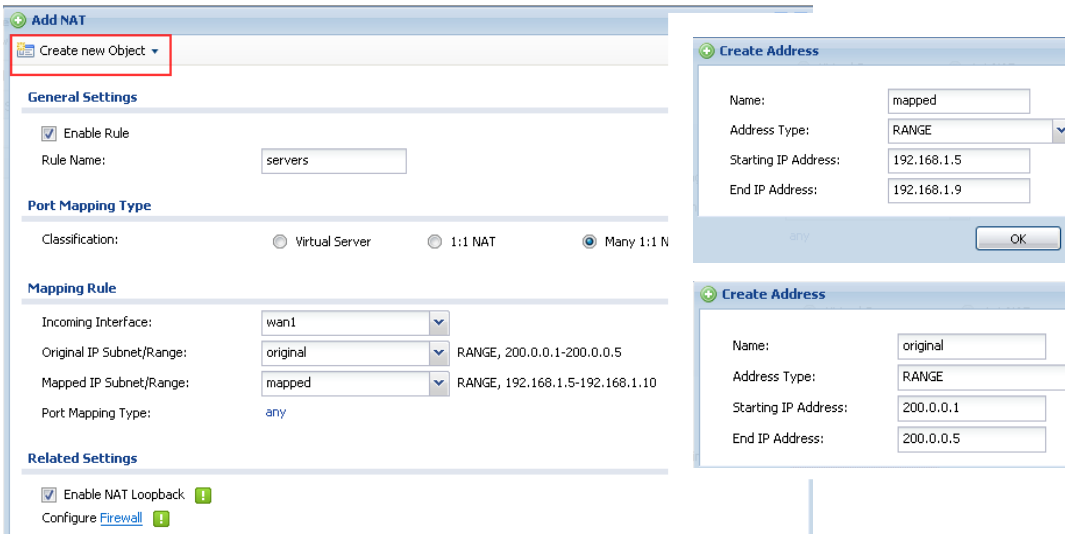
Port Mapping Type: Many 1:1 NAT.

Incoming Interface: Select the WAN interface you want the USG to receive the incoming traffic to the servers.

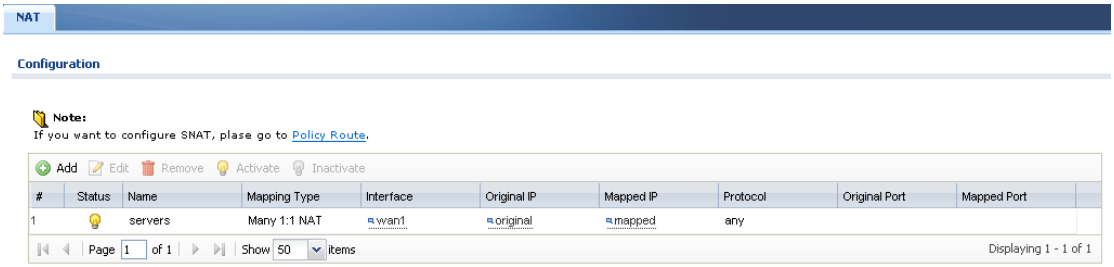
Original IP: First create address objects for the original IP range and mapped IP range from the Create new Object field, and then choose this object from the Original IP dropdown list.

Mapped IP: Choose the address object from the dropdown list.

Port Mapping: It can only set as any.

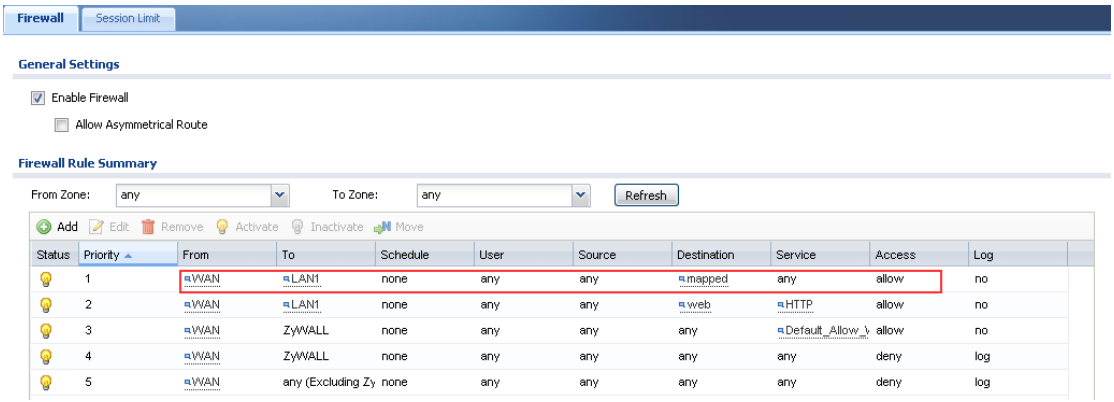


Below is the NAT rule overview after configuration is done.



After the Many 1:1 NAT rule is set up, a set of one to one routing rules will be automatically generated in the USG ZyWALL.

Don't forget to configure corresponding firewall rule to allow traffic from WAN to the LAN server range.



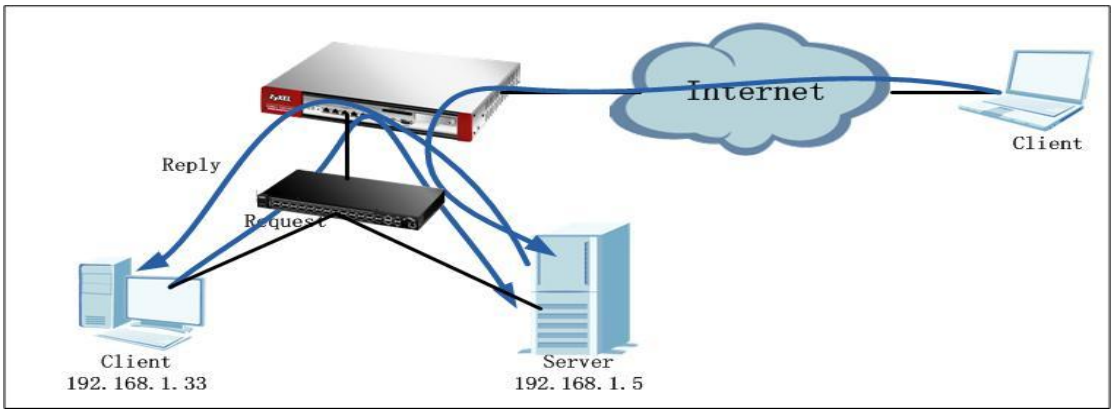
1.6. NAT Loopback

Company server is located in the local network of the USG ZyWALL. You can create Virtual server rule or 1:1 NAT rule to allow WAN side clients to connect to the server. You may also needs the server to be accessed by the local clients via the server's global IP address. For example, local clients try to access the company server by its domain name. The domain name will be resolved to the global IP by DNS. Under this circumstance, you can enable NAT Loopback.

1.6.1. Network Scenario

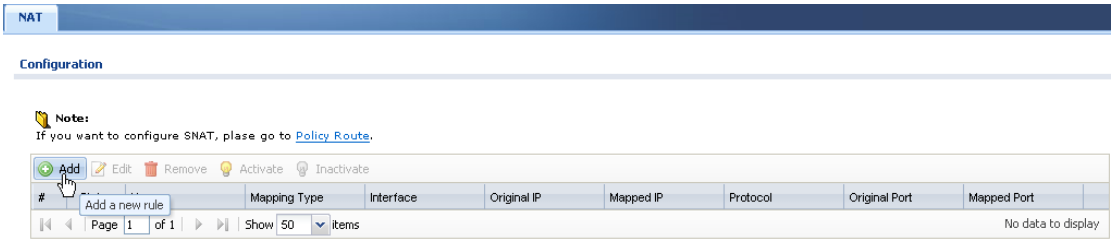
Company server (192.168.1.33) is placed in the local subnet, the local client (192.168.1.33) which is in the same subnet with the server wants to access the server

via the USG's global IP address. Enable NAT Loopback can fulfill this application.

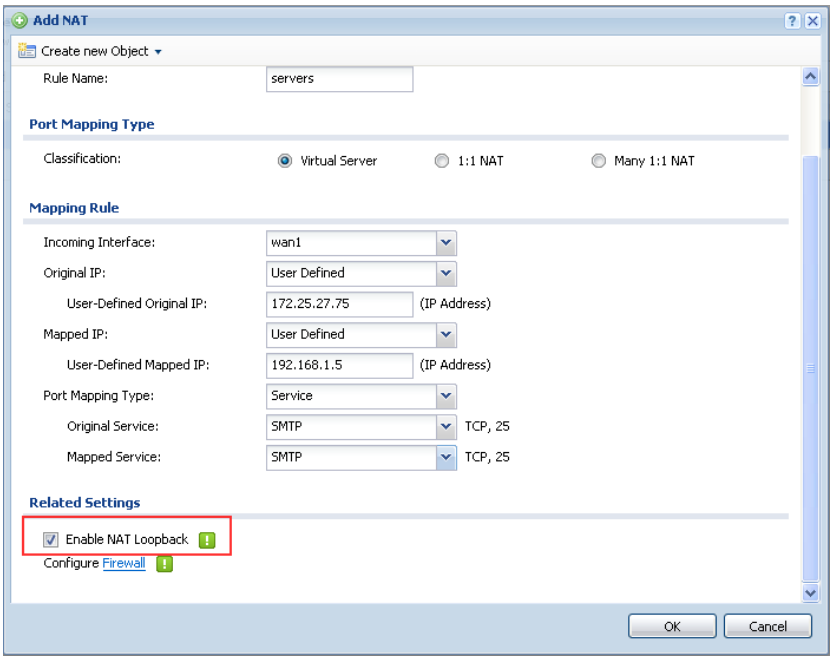


1.6.2.Configuration Steps

Step1. Go to Configuration > Network > NAT, click Add button to add one NAT rule.



Step2. In the rule editing window, fill in all the necessary fields. And enable NAT Loopback.



After NAT Loopback is enabled, no policy route is needed, USG will automatically checking routing table. And it will only do SNAT for the local clients in the same subnet with the server. The source addresses of clients from WAN side and local clients in the other subnets will remain the original.

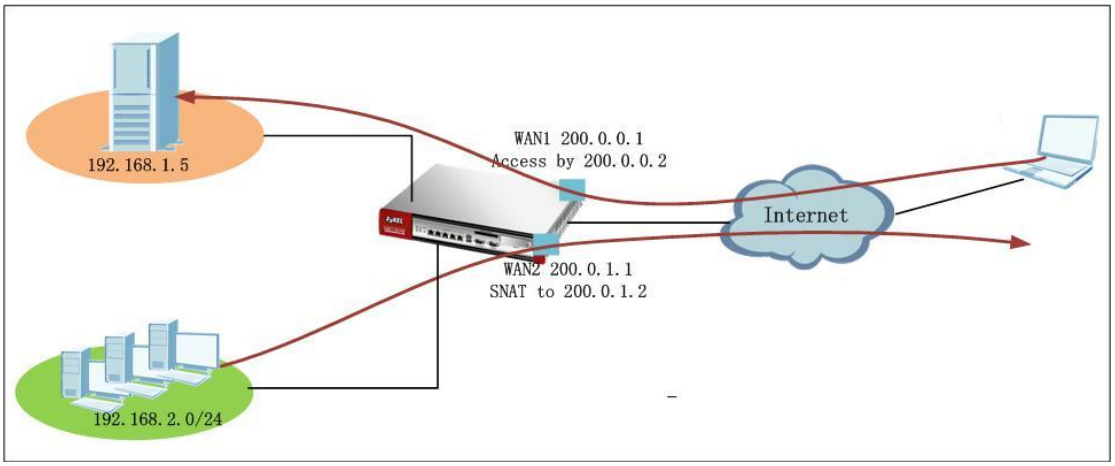
1.7. NAT with Proxy ARP

Sometimes user may want to use some non-interface IP as the global IP for some servers, or want to do SNAT for some local traffic to map the source address to some non-interface IP.
For example, user has 3 public IP from ISP, 200.0.0.1, 200.0.0.2, 200.0.1.1. User set 200.0.0.1 as WAN 1 IP, 200.0.1.1 as WAN2 IP. But he/she wants users to use 200.0.0.2 to access the intranet server, e.g. 192.168.1.5, by adding one NAT rule as below:
Incoming interface: WAN1
Original IP: 200.0.0.2
Mapped IP: 192.168.1.5

In ZLD v2.1x, after user added the NAT rule as above, it will automatically created one Virtual Interface on the Incoming interface with the non-interface IP. In this example, it will add one Virtual interface on WAN1, with IP address 200.0.0.2. However, there's a disadvantage in this way: after the NAT rule is created, not only the traffic to access the intranet server will be allowed, but the USG can also be accessed by this non-interface IP, which brings a security concern that some hackers may use this non-interface IP to login USG to malicious actions on the USG. Besides, you cannot map the outgoing traffic's source IP to a non-interface IP. Because the USG has no way to know that the non-interface IP belongs to itself.
In ZLD v2.20, after user added the NAT rule as above, it will automatically create proxy ARP table to make the non-interface IP corresponding the incoming interface's MAC. It will only allow the traffic accessing the intranet server in this NAT rule, other traffic will be dropped by the USG.
Also, in ZLD v2.20, the USG can map outgoing traffic's source IP to a non-interface IP by creating proxy ARP table to map the non-interface IP to the outgoing interface's MAC.

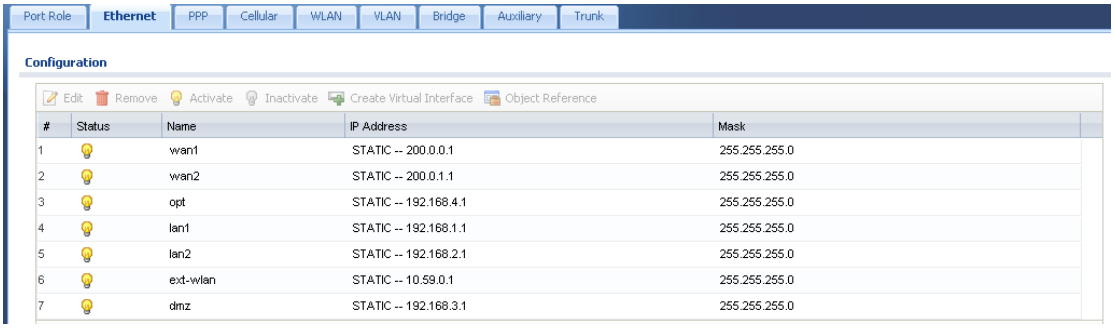
1.7.1.Application Scenario

In the secnario below, the company gets 4 IP addresses: 200.0.0.1, 200.0.0.2, 200.0.1.1, 200.0.1.2. The network administrator set WAN1 200.0.0.1, WAN2 200.0.1.1. And he/she wants the intranet server 192.168.1.5 to be accessed via WAN1 by IP 200.0.0.2. Also, he/she wants the subnet clients 192.168.2.0/24 to go out via WAN2, and maps the source IP to 200.0.1.2.



1.7.2.Configuration Steps

Step1. Go to Configuration > Network > Interface, set up WAN1 and WAN2 address.



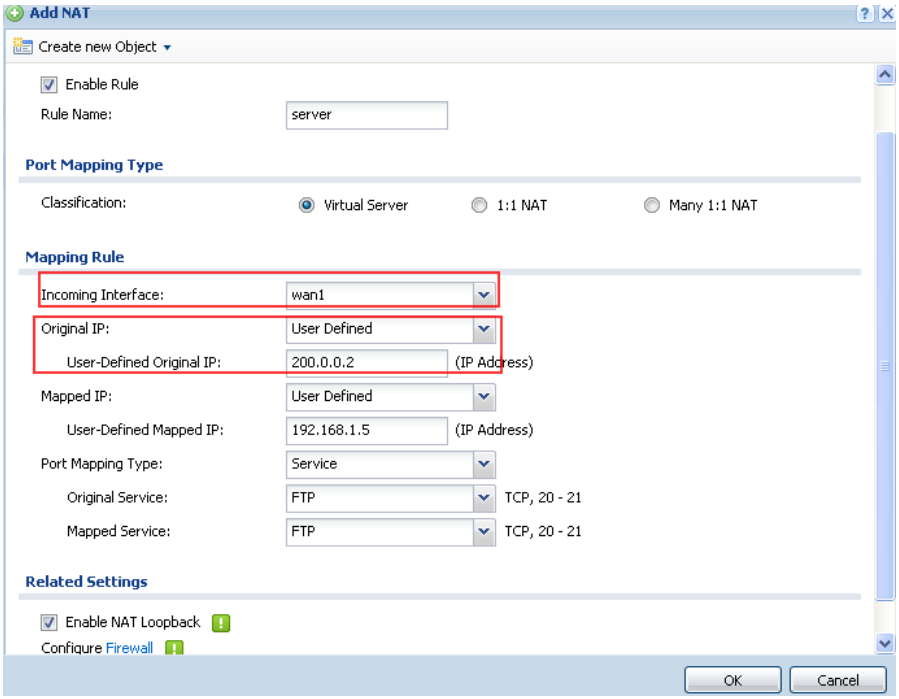
#	Status	Name	IP Address	Mask
1		wan1	STATIC -- 200.0.0.1	255.255.255.0
2		wan2	STATIC -- 200.0.1.1	255.255.255.0
3		opt	STATIC -- 192.168.4.1	255.255.255.0
4		lan1	STATIC -- 192.168.1.1	255.255.255.0
5		lan2	STATIC -- 192.168.2.1	255.255.255.0
6		ext-wlan	STATIC -- 10.59.0.1	255.255.255.0
7		dmz	STATIC -- 192.168.3.1	255.255.255.0

Step2. To fulfill the requirement that the intranet server could be accessed via WAN1 by the non-interface IP 200.0.0.2, go to Configuration > Network > NAT, add one rule as below.

Incoming interface: WAN1

Original IP: 200.0.0.2

Mapped IP: 192.168.1.5



Check the ARP table. You will see the record for 200.0.0.2.

```
Router> show arp-table
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.1.33             ether   00:1B:78:86:86:89   C                     lan1
200.0.0.254                      (incomplete)                              wan1
200.0.0.2                *       <from_interface>    MP                    wan1
```

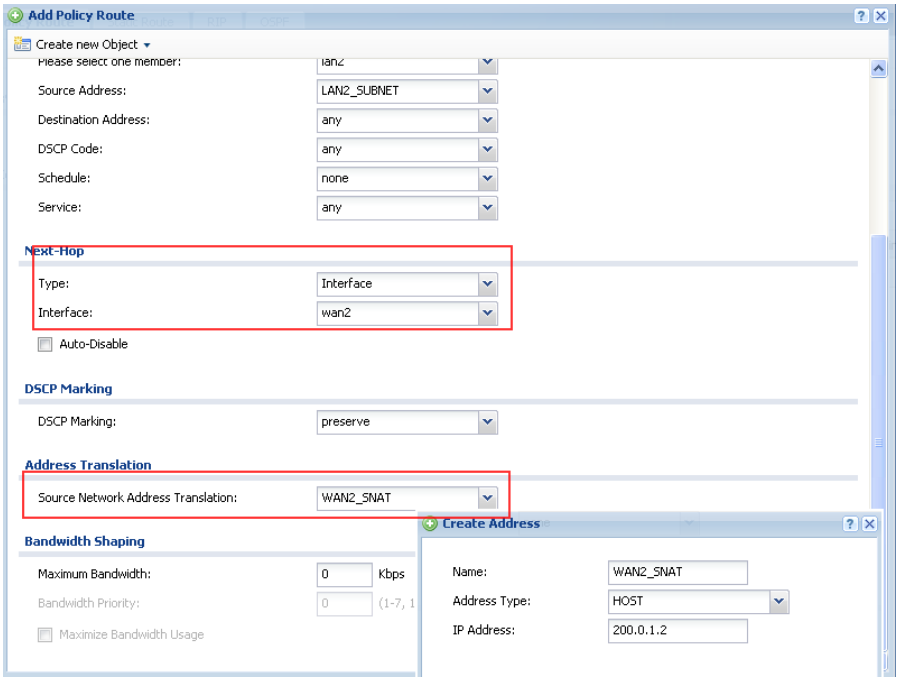
Step3. To fulfill the requirement that the local subnet 192.168.2.0/24 goes out from WAN2, and source addresses mapped to the non-interface IP 200.0.1.2, go to Configuration > Network > Routing > Policy Route, add one rule as below.

Source Address: 192.168.2.0/24

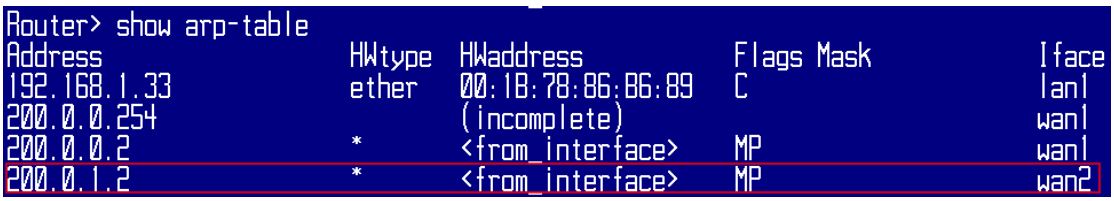
Destination: Any

Next Hop: WAN2

SNAT: Address Object WAN2_SNAT (200.0.1.2)



Check the ARP table. You will see the record for 200.0.1.2.

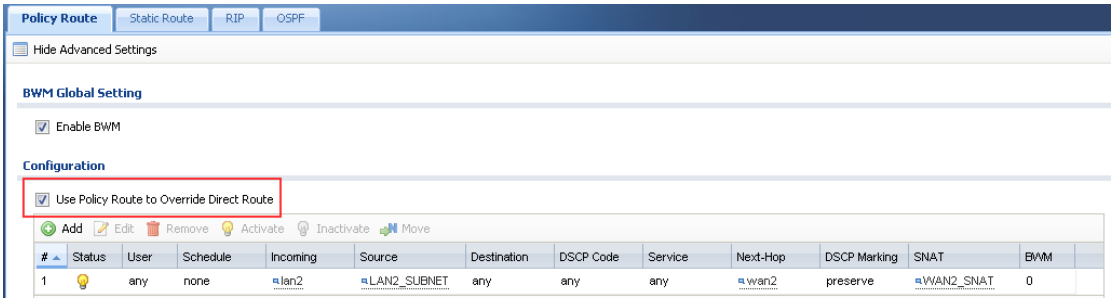


```
Router> show arp-table
Address          HWtype  HWaddress          Flags Mask          Iface
192.168.1.33     ether   00:18:78:86:86:89  C                   lan1
200.0.0.254              (incomplete)                           wan1
200.0.0.2        *       <from_interface>   MP                  wan1
200.0.1.2        *       <from_interface>   MP                  wan2
```

1.8. Policy Route vs. Direct Route

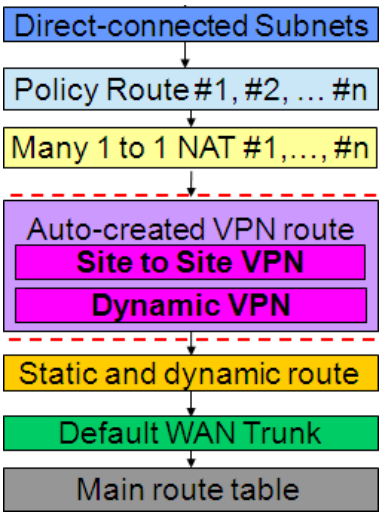
Normally, in USG's routing priority, direct route takes priority over policy routes. Sometimes, you may need the policy route takes priority over direct route, there's an option to allow you to achieve this.

Go to Configuration > Network > Routing > Polity Route, click the icon Show Advanced Settings. Then enable the function Use Polity Route to Override Direct Route.



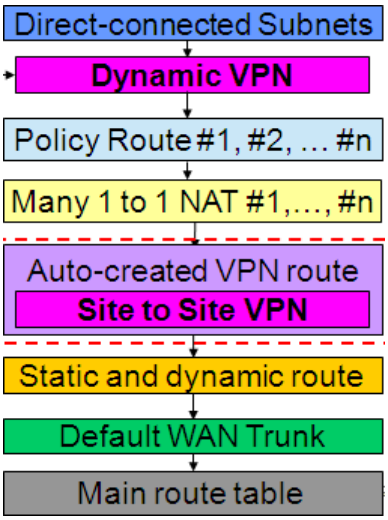
1.9. Routing for IPSec VPN

In ZLD v2.20, after you created IPSec VPN rules, you don't need to add corresponding Policy Route for routing the VPN traffic any more. The USG will automatically add Policy Route according to the phase 2 Local/Remote Policy.

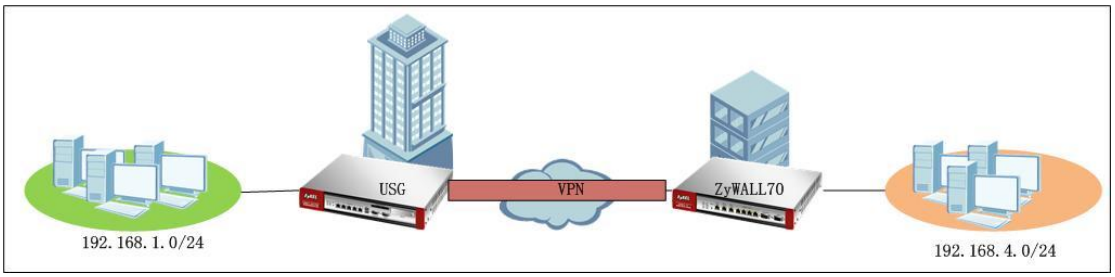


Since Policy Route has higher priority, you can create policy route to override the system auto generated IPSec VPN routes. Or you can also add policy routes to let traffic other than in the VPN Phase 2 Local/Remote policy to use this VPN tunnel.

By default, “Use Policy Route to control dynamic IPSec rules” is enabled, so dynamic VPN routes will be integrated to the Site-to-Site VPN routes.
If you disable this option “Use Policy Route to control dynamic IPSec rules”, dynamic VPN routes will be moved to have higher priority in the routing priority table.



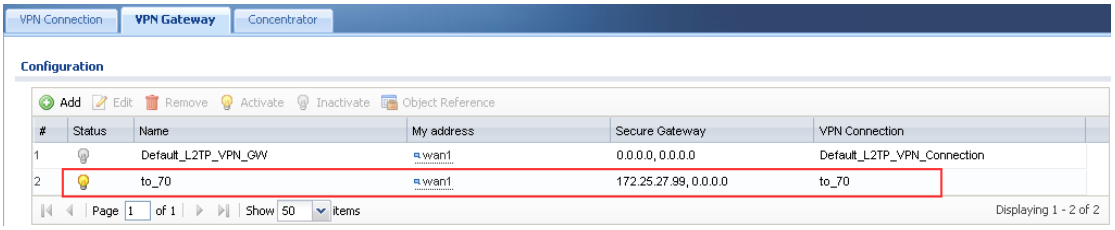
1.9.1.Application Scenario



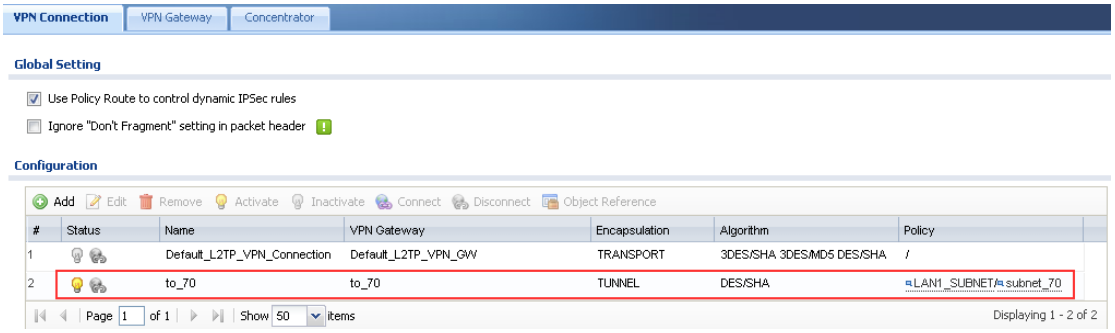
USG is placed at the HQ, local subnet: 192.168.1.0/24.
Remote security gateway ZyWALL 70 local subnet: 192.168.4.0/24.
USG and remote security gateway build IPSec VPN tunnel.

1.9.2.Configuration Steps

On the USG ZyWALL:
Step1. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add VPN gateway (Phase 1) rule.

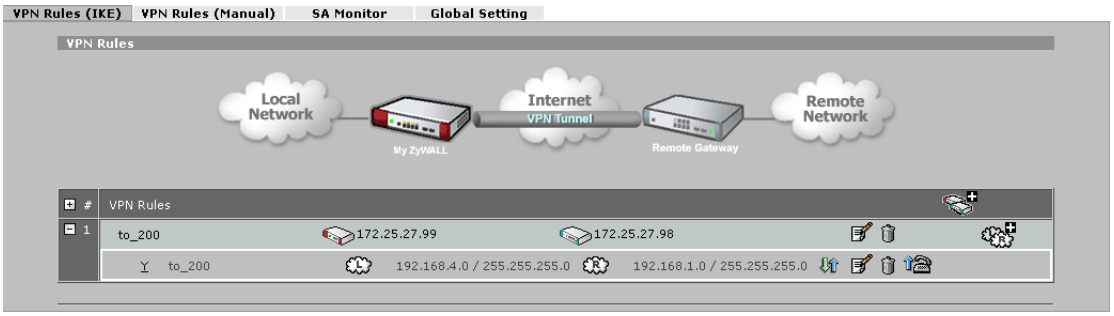


Step2. Go to Configuration > VPN > IPSec VPN > VPN Connection, add VPN Connection (Phase 2) rule.

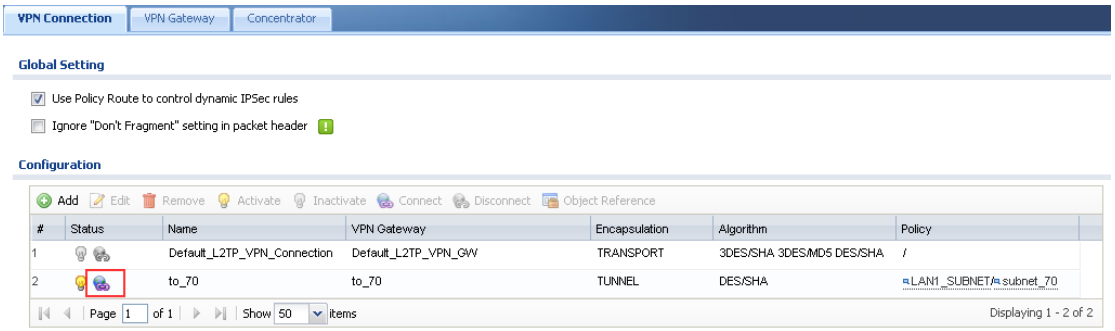


On the ZyWALL 70:

Go to Security > VPN, add VPN phase1 and phse2 rules.



Establish the tunnel.



Traffic can go through this tunnel.

```
C:\Documents and Settings\Administrator>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.1.33
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1

Ethernet adapter 本地连接:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Administrator>ping 192.168.4.33

Pinging 192.168.4.33 with 32 bytes of data:

Reply from 192.168.4.33: bytes=32 time=3ms TTL=126
Reply from 192.168.4.33: bytes=32 time=2ms TTL=126
Reply from 192.168.4.33: bytes=32 time=2ms TTL=126
Reply from 192.168.4.33: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.4.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

1.10. One to One NAT Link Fail Over

1.10.1. Network Scenario

In some cases, network administrator may want to make sure his/her intranet server always available from outside.

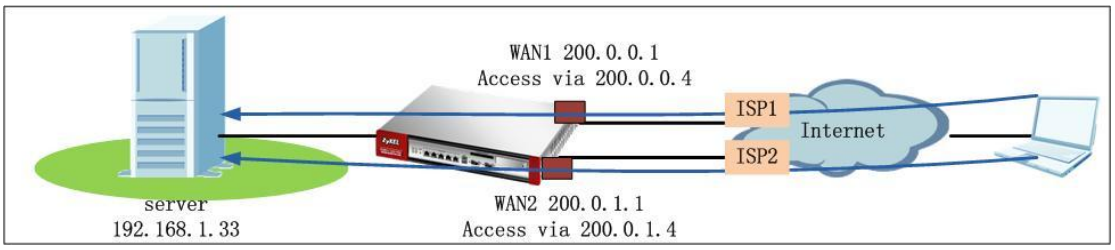
In the scenario below, WAN1 is connected to ISP1, and WAN2 is connected to ISP2.

WAN1: 200.0.0.1. Non-interface IP: 200.0.0.4

WAN2: 200.0.1.1. Non-interface IP: 200.0.1.4

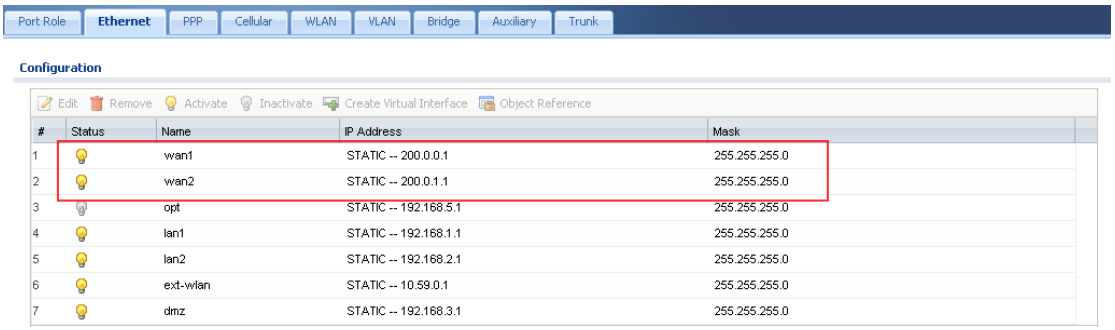
Requirements:

- Outside clients can access the intranet server 192.168.1.33 via both WAN1 and WAN2 from the non-interface IP, performing load balance for the server access traffic between WAN1 and WAN2.
- In case WAN1 fails, the intranet server still can be accessed via WAN2.
- The source address of the outgoing traffic initiated from the server will be mapped to the non-interface IP.

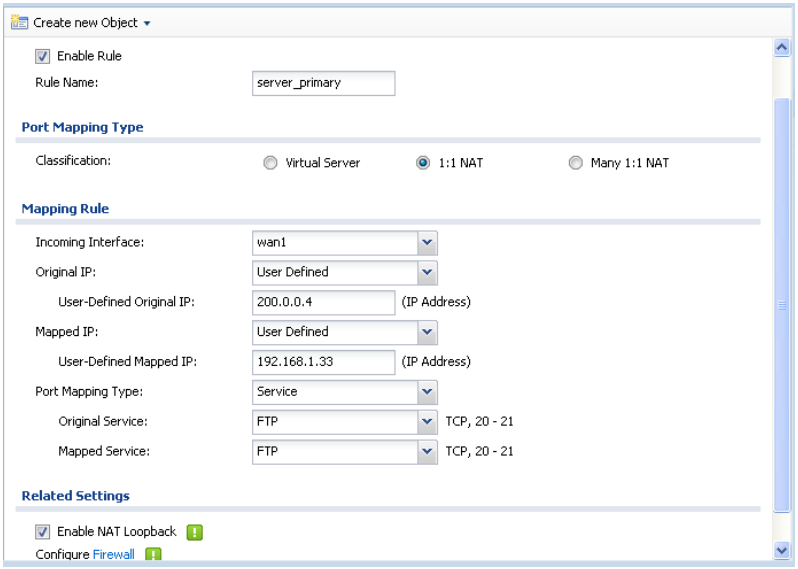


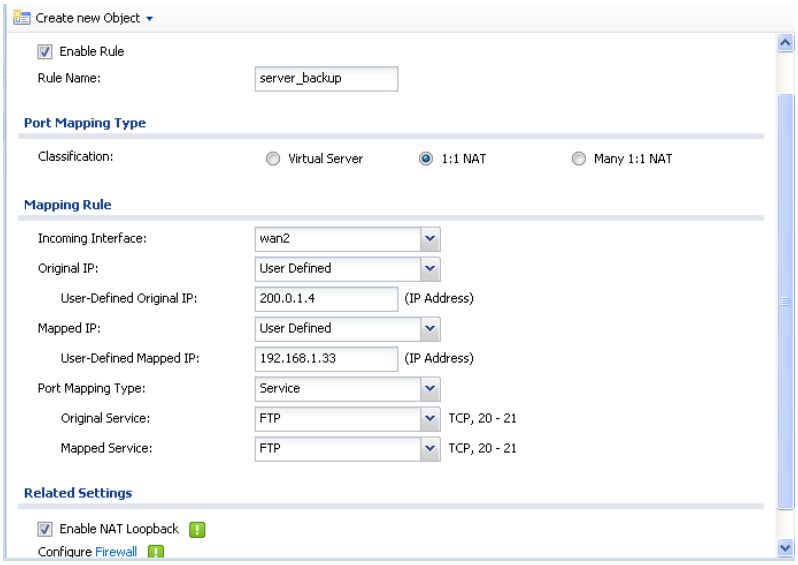
1.10.2. Configuration Steps

Step1. Configure WAN1 and WAN2 IP addresses from Configuration > Network > Interface > Ethernet.

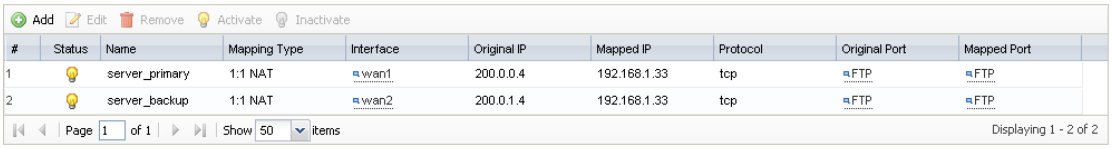


Step2. Go to Configuration > Network > NAT. Add two NAT 1:1 rules.





Below is the NAT rule summary:



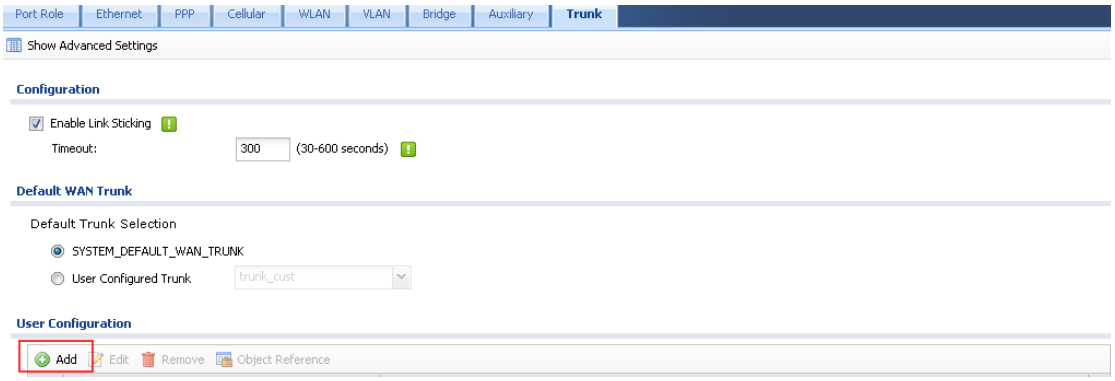
Please note that after the two NAT 1:1 rules are added, system will automatically generate two 1:1 routing rules as below:

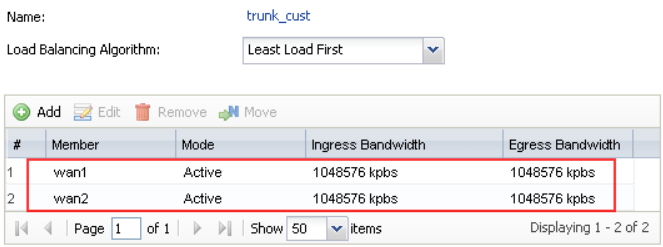
Source: 192.168.1.33 (server IP)| Destination: any| Next hop: wan1

Source: 192.168.1.33 (server IP)| Destination: any| Next hop: wan2

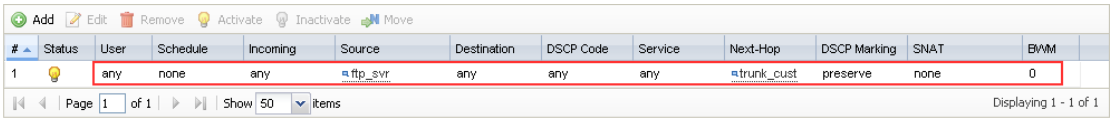
To prevent the traffic from the server to any always match the first 1:1 routing rule, we need to add one policy route to over write these two 1:1 routings.

Step3. Go to Configuration > Network > Interface > Trunk, add one customized WAN trunk.





Step4. Go to Configuration > Network > Routing, add one policy route as below: Source: 192.168.1.33(server)| Destination: any| Next hop: <the newly added WAN trunk>| SNAT: None.



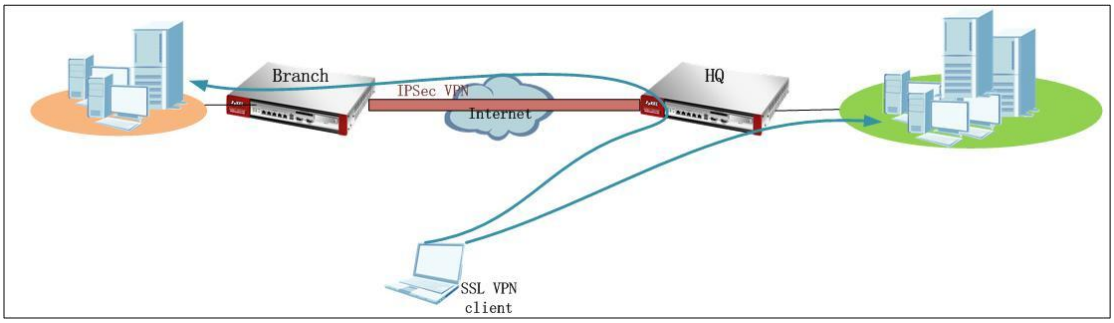
Please not that we set the SNAT to be None, because we still need the 1:1 NAT mapping to translate the server's outgoing traffic source address.

1.11. Accessing IPSec VPN Peer Subnet From SSL VPN Clients

1.11.1. Application Scenario

USG ZyWALL is placed as the HQ gateway. Branch office builds IPSec VPN tunnel to HQ office. Local subnets of branch office and HQ office can communicate via the IPSec VPN tunnel.

SSL VPN client builds SSL VPN full tunnel to HQ to access HQ local subnet resources. Besides, the SSL VPN client also wants to access Brach office local resources first via SSL VPN full tunnel to HQ, then via the IPSec VPN tunnel to branch office.



Let's assume the IP information is as below:
HQ office:
WAN: 172.25.27.126
LAN: 192.168.1.0/24
SSL VPN range: 10.0.0.1~10.0.0.10
Branch office:
WAN: 172.25.27.99
LAN: 192.168.10.0/24

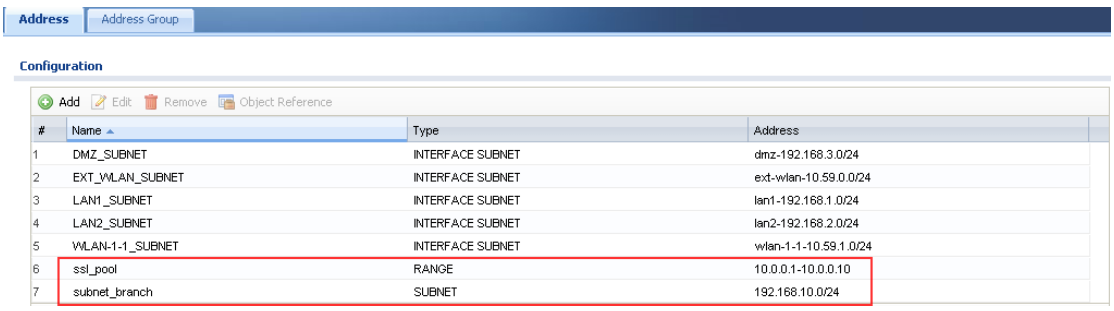
1.11.2. Configuration Steps

Configuration varies when the branch security gateway is a USG ZyWALL and when it's a ZyNOS ZyWALL (policy based). We will discuss the two situations below:

1.11.2.1. When Branch is a USG ZyWALL

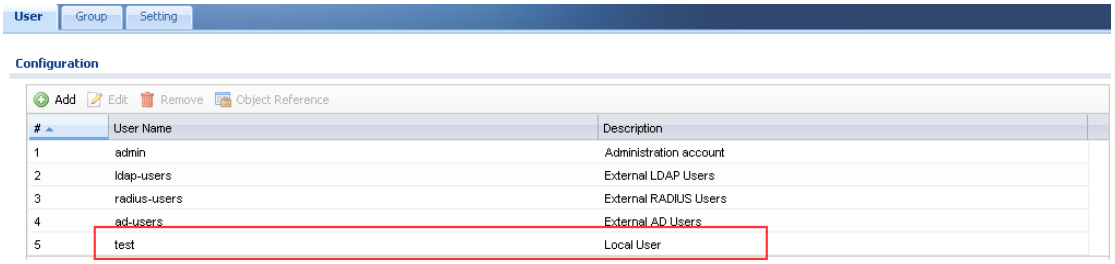
On HQ USG:

Step1. Go to Configuration > Object > Address, add two address objects. One is ssl_pool (range 10.0.0.1~10.0.0.10), the other is branch office subnet subnet_branch(192.168.10.0/24)



#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	EXT_WLAN_SUBNET	INTERFACE SUBNET	ext-wlan-10.59.0.0/24
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
5	WLAN-1-1_SUBNET	INTERFACE SUBNET	wlan-1-1-10.59.1.0/24
6	ssl_pool	RANGE	10.0.0.1-10.0.0.10
7	subnet_branch	SUBNET	192.168.10.0/24

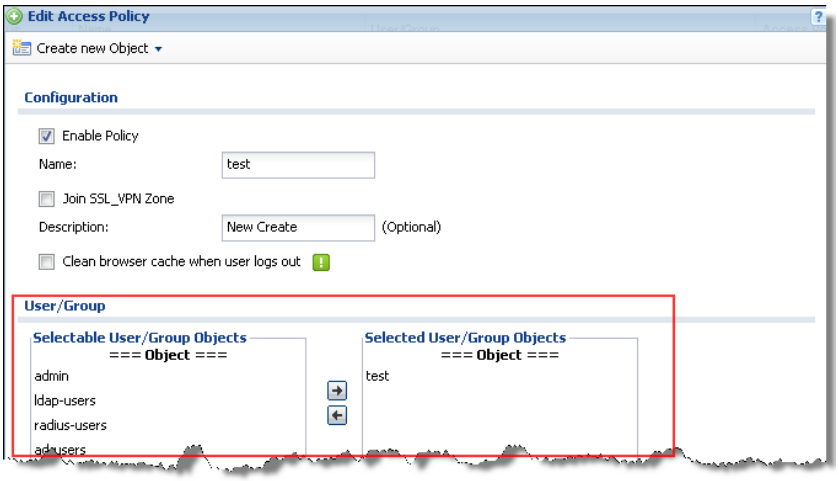
Step2. Go to Configuration > Object > User/Group, add SSL VPN user account, e.g. “test”.

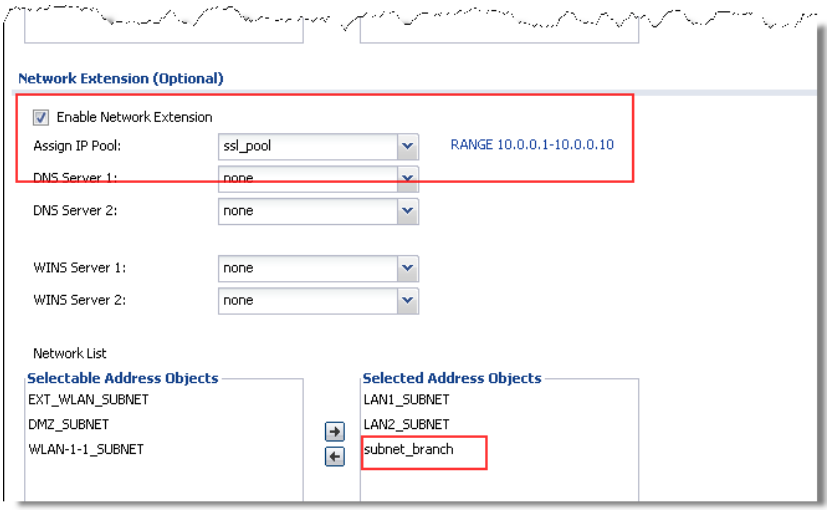


Step3. Go to Configuration > VPN > SSL VPN > Access Privilege, add one SSL VPN rule.

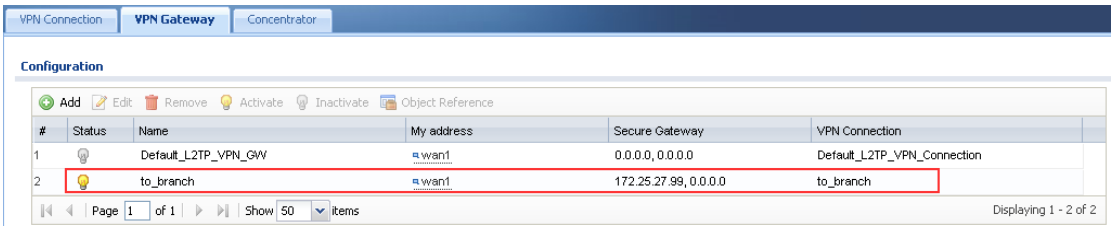
Enable Network Extension (full tunnel).

In the Network List, make sure the subnet_branch object (192.168.10.0) is selected.

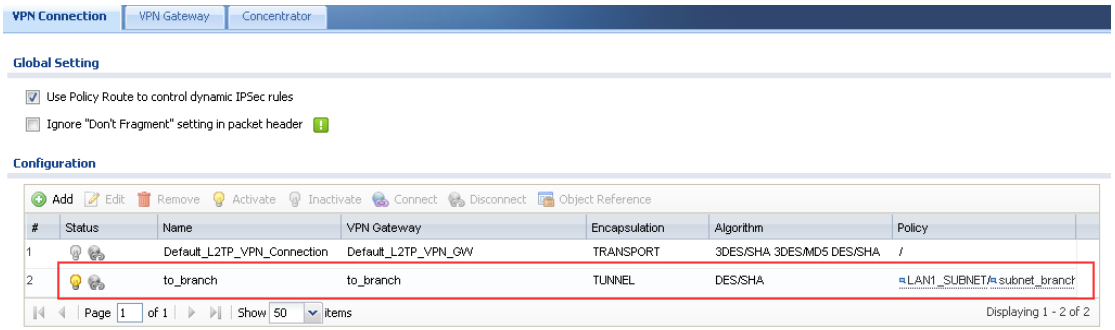




Step4. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add phase1 rule to branch office.



Go to Configuration > VPN > IPSec VPN > VPN Connection, add corresponding phase2 rule to branch office. Local/Remote policy: 192.168.1.0/192.168.10.0



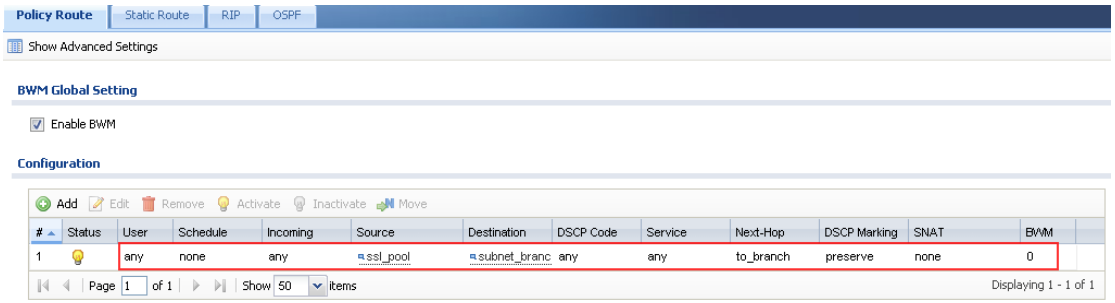
Step5. Go to Configuration > Network > Routing > Policy Route, add one policy route to route the SSL VPN traffic (sent from SSL VPN client to the branch office local subnet) to the IPSec VPN tunnel to_branch.

Source: ssl_pool (10.0.0.1~10.0.0.10)

Destination: subnet_branch (192.168.10.0/24)

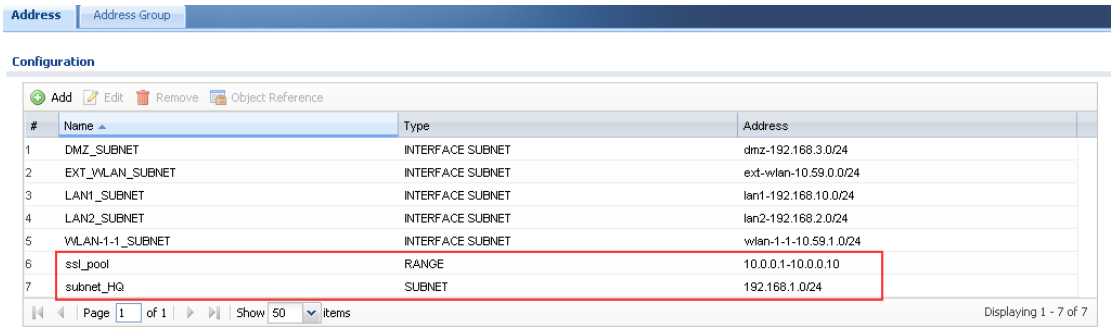
Next Hop: IPSec VPN tunnel to_branch

SNAT: none

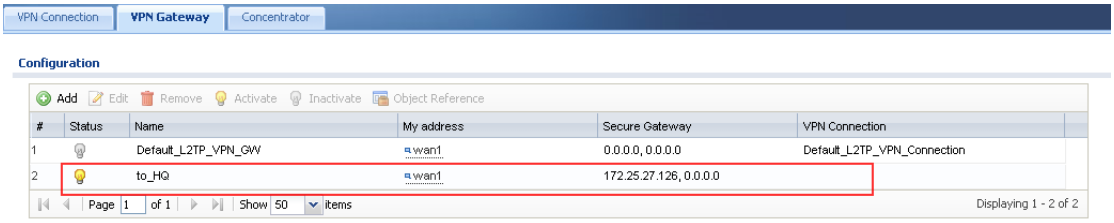


On branch office USG:

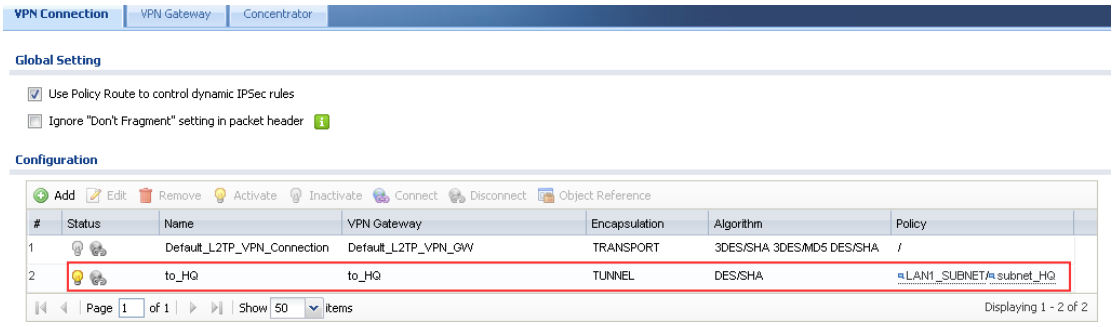
Step1. Go to Configuration > Object > Address, add two address objects. One is subnet_HQ (192.168.1.0/24), the other is ssl_pool (10.0.0.1~10.0.0.10).



Step2. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add one phase1 rule to HQ.



Go to Configuration > VPN > IPSec VPN > VPN Connection, add corresponding phase2 rule to HQ. Local/Remote policy: 192.168.10.0/192.168.1.0.



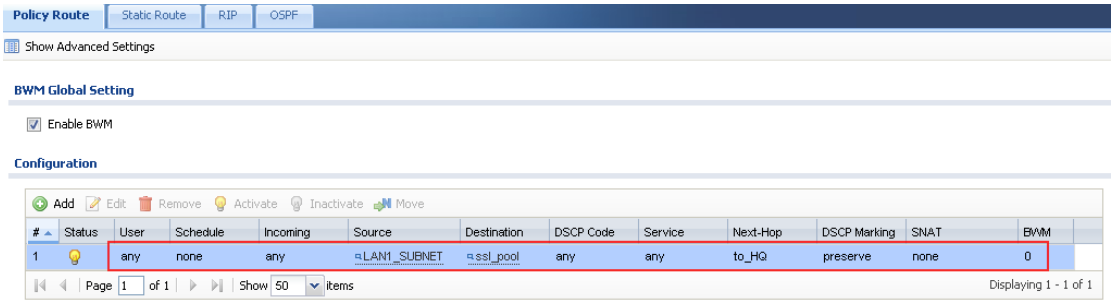
Step3. Go to Configuration > Network > Routing > Policy Route, add one policy route to route the SSL VPN traffic (from local subnet to the SSL VPN client) back to the IPSec VPN tunnel.

Source: LAN1_Subnet (192.168.10.0/24)

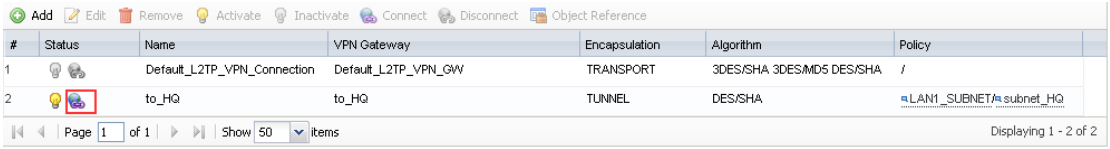
Destination: ssl_pool (10.0.0.1~10.0.0.10)

Next Hop: IPSec VPN tunnel to_HQ

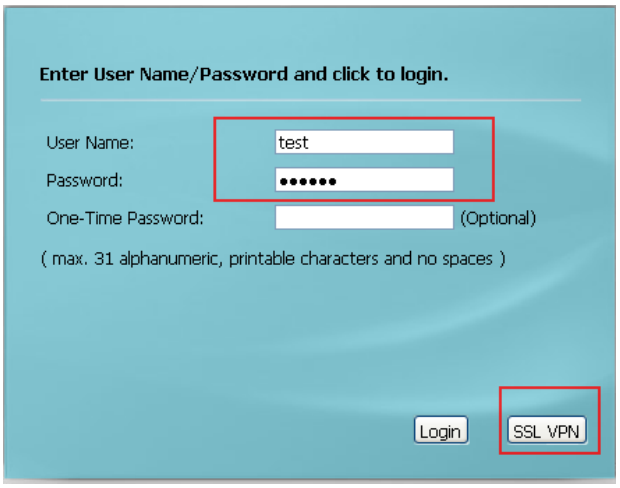
SNAT: none

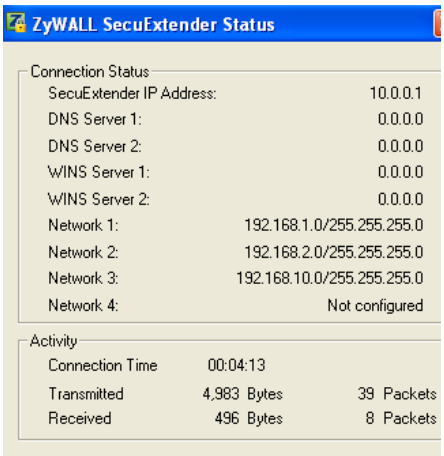


After all the settings on HQ and branch USG, user can verify the result.
Dial up the IPSec VPN tunnel.



SSL client builds a full tunnel to the HQ USG.





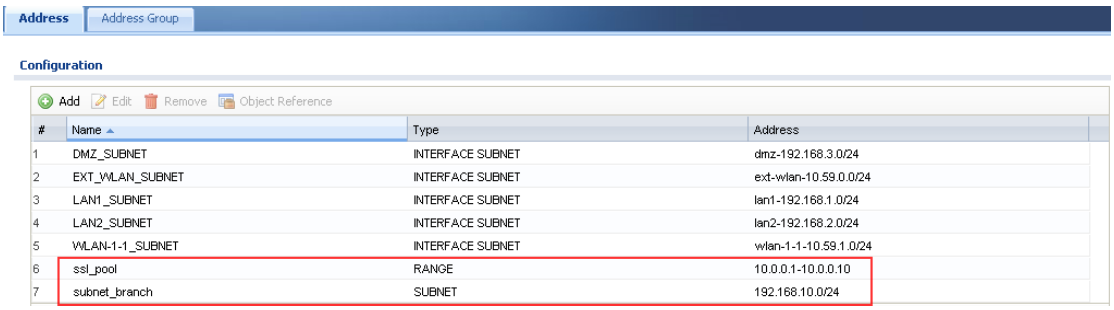
The SSL VPN client can access both the HQ USG local resources 192.168.1.0/24, 192.168.2.0/24, and the branch office USG local resources 192.168.10.0/24.

```
PPP adapter {567A1C90-B4A8-4FE0-B369-1B773853884A}:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.0.0.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms
Control-C
^C
C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms
Control-C
^C
C:\Documents and Settings\Administrator>ping 192.168.10.33

Pinging 192.168.10.33 with 32 bytes of data:

Reply from 192.168.10.33: bytes=32 time=14ms TTL=125
Reply from 192.168.10.33: bytes=32 time=10ms TTL=125

Ping statistics for 192.168.10.33:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 14ms, Average = 12ms
Control-C
^C
C:\Documents and Settings\Administrator>_
```

1.11.2.2. When Branch is a ZyNOS ZyWALL

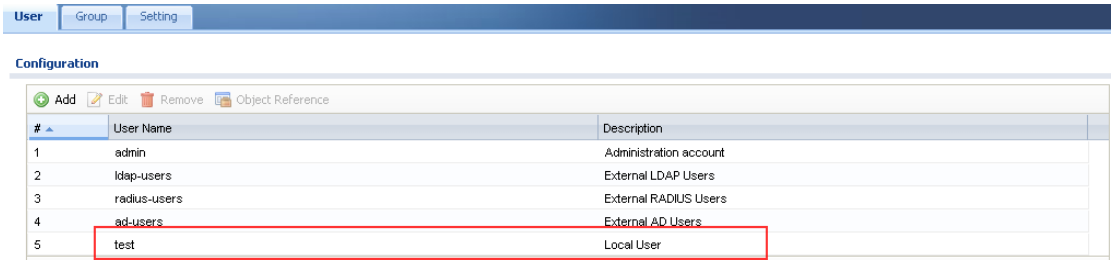
On the HQ USG:

Step1. Go to Configuration > Object > Address, add two address objects. One is ssl_pool (range 10.0.0.1~10.0.0.10), the other is branch office subnet subnet_branch(192.168.10.0/24)



#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	EXT_WLAN_SUBNET	INTERFACE SUBNET	ext-wlan-10.59.0.0/24
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
5	WLAN-1-1_SUBNET	INTERFACE SUBNET	wlan-1-1-10.59.1.0/24
6	ssl_pool	RANGE	10.0.0.1-10.0.0.10
7	subnet_branch	SUBNET	192.168.10.0/24

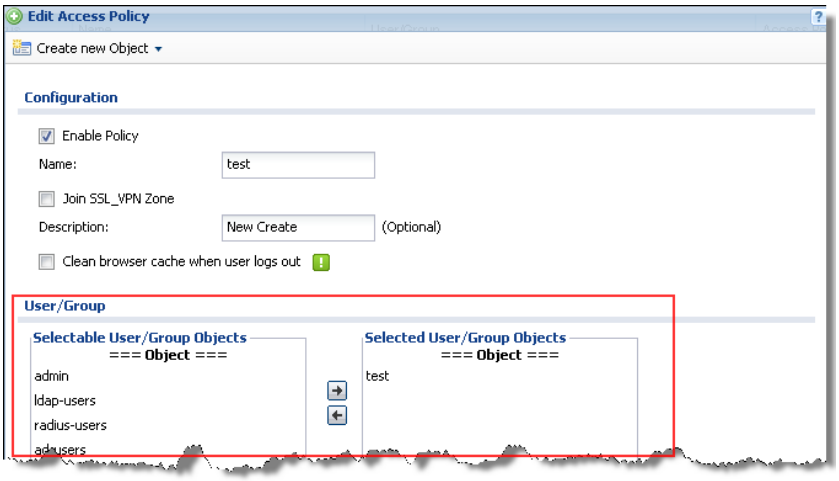
Step2. Go to Configuration > Object > User/Group, add SSL VPN user account, e.g. “test”.

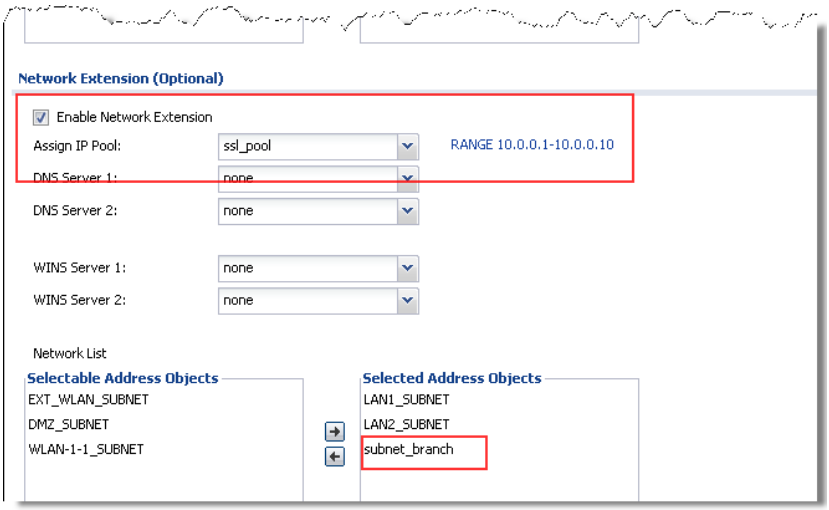


Step3. Go to Configuration > VPN > SSL VPN > Access Privilege, add one SSL VPN rule.

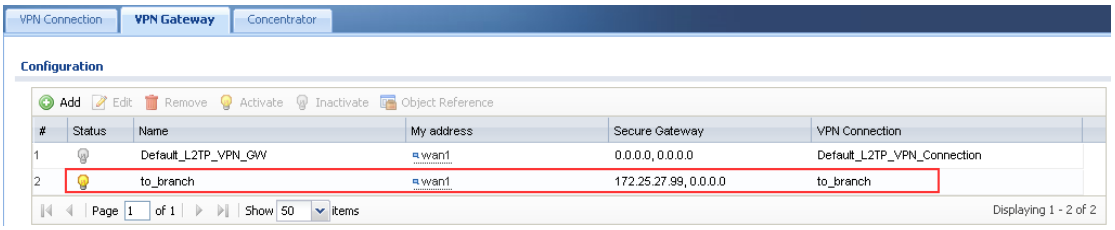
Enable Network Extension (full tunnel).

In the Network List, make sure the subnet_branch object (192.168.10.0) is selected.





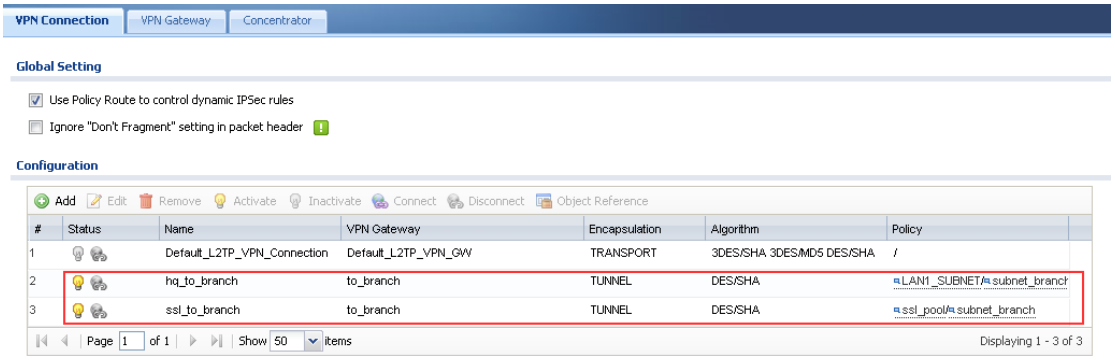
Step4. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add phase1 rule to branch office.



Go to Configuration > VPN > IPSec VPN > VPN Connection, add two phase2 rules to branch office.

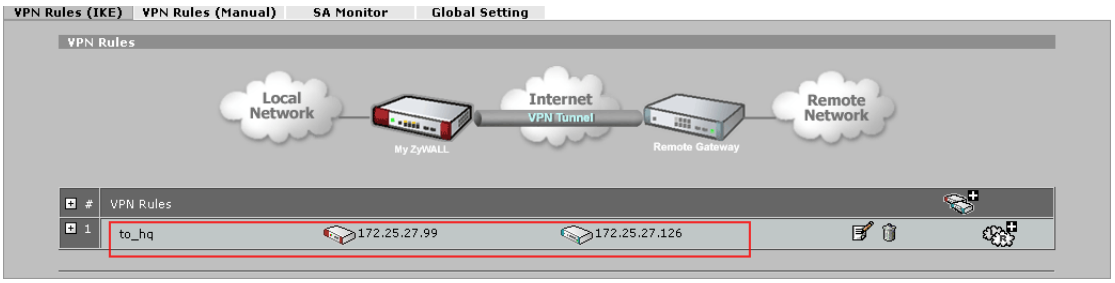
First rule for HQ to branch, Local/Remote policy: 192.168.1.0/192.168.10.0

Second rule for ssl vpn client to branch, Local/Remote policy: 10.0.0.1~10.0.0.10/192.168.10.0



On branch office ZyNOS ZyWALL:

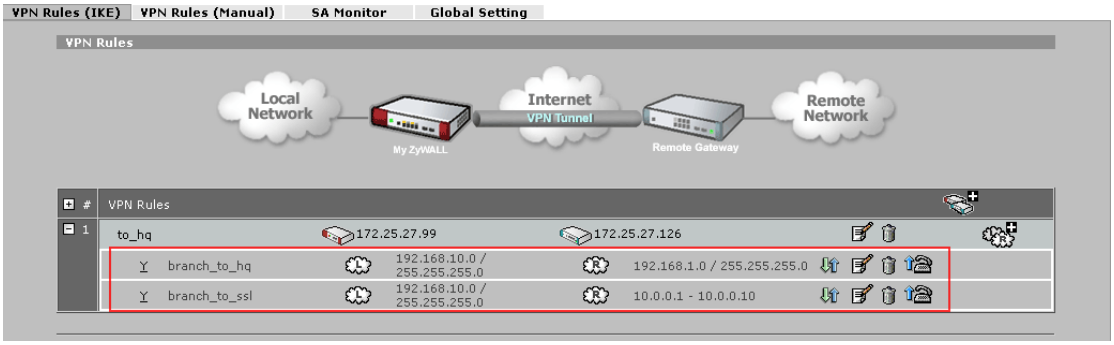
Go to Security > VPN > VPN rules(IKE), add phase 1 rule to HQ.



Add two phase2 rules.

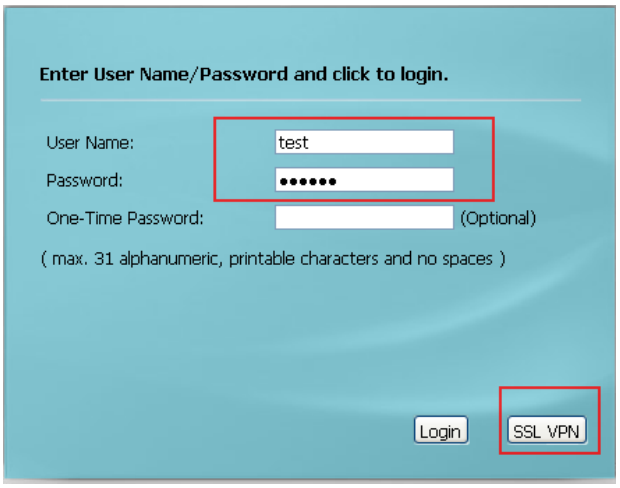
One is for traffic from branch to HQ. Local/Remote policy: 192.168.10.0/192.168.1.0

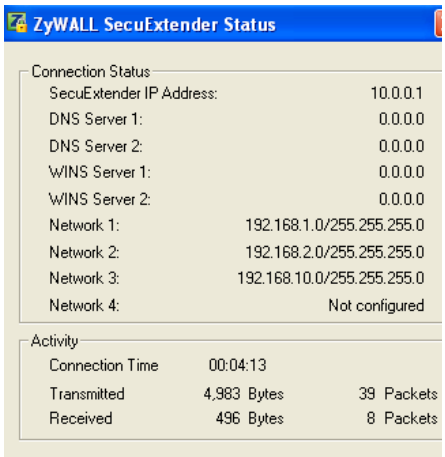
The other is for traffic from branch to ssl vpn client. Local/Remote policy: 192.168.10.0/10.0.0.1~10.0.0.10.



After the settings above are done on both HQ USG and branch ZyNOS ZyWALL, we can verify whether the SSL VPN client can access the remote local resources.

SSL client builds a full tunnel to the HQ USG.





The SSL VPN client can access both the HQ USG local resources 192.168.1.0/24, 192.168.2.0/24, and the branch office USG local resources 192.168.10.0/24.

```
PPP adapter {567A1C90-B4A8-4FE0-B369-1B773853884A}:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.0.0.1
        Subnet Mask . . . . . . . . . . . : 255.255.255.255
        Default Gateway . . . . . . . . . :

C:\Documents and Settings\Administrator>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:

Reply from 192.168.1.1: bytes=32 time=5ms TTL=64
Reply from 192.168.1.1: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.1.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms
Control-C
^C
C:\Documents and Settings\Administrator>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=5ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms
Control-C
^C
C:\Documents and Settings\Administrator>ping 192.168.10.33

Pinging 192.168.10.33 with 32 bytes of data:

Reply from 192.168.10.33: bytes=32 time=14ms TTL=125
Reply from 192.168.10.33: bytes=32 time=10ms TTL=125

Ping statistics for 192.168.10.33:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 10ms, Maximum = 14ms, Average = 12ms
Control-C
^C
C:\Documents and Settings\Administrator>_
```

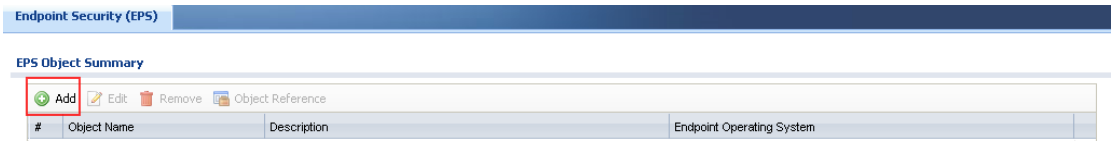
2. Deploying EPS

2.1. EPS Introduction

EPS is short for Endpoint Security.
Endpoint refers to PCs, laptops, handhelds, etc. Endpoint Security is a security concept that assumes each endpoint is responsible for its own security. Network administrator can set restrict policies to allow only the endpoints that comply with its defined security requirements to access network resources. The endpoint security requirement items may contain current anti-virus state, personal firewall, and operating system patch level, etc.
For example, a local endpoint doesn't have any anti-virus software installed. If it surfs internet, there's a high risk that it may be infected with viruses. Then the viruses may be propagated among the entire local network.
Another example is in SSL VPN case. If the SSL VPN client doesn't have anti-virus software installed, when it accesses the HQ local resources through SSL VPN tunnel, it may propagate the virus to HQ local subnet.
To prevent such undesired situation, the network administrator can use EPS checking to restrict endpoints' network access privileges. Only the compliant endpoint can get authority to access certain network resources.

2.1.1. EPS --- WebGUI

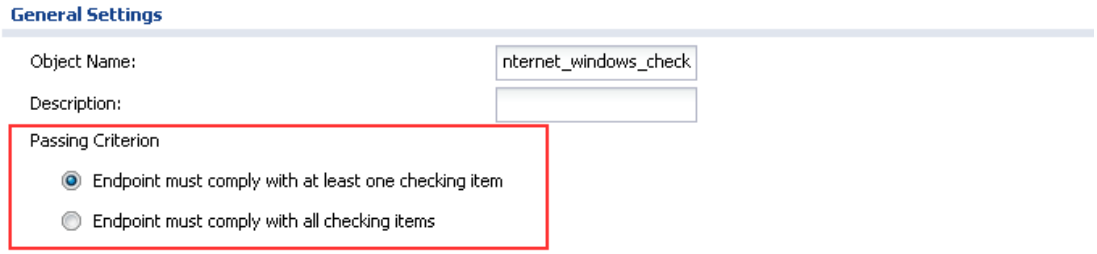
Go to Configuration > Object > Endpoint Security to create EPS objects, which can later be used in User Aware and SSL VPN applications.



Below is the EPS editing page.
For the Passing Criterion, you can choose "Endpoint must comply with at least one checking item", or "Endpoint must comply with all checking items".
If you choose "Endpoint must comply with at least one checking item", then the client can pass the EPS checking as long as it matches at least one checking items that listed

below the Passing Criterion.

If you choose “Endpoint must comply with all checking items”, then the client must comply with all the checking items listed below to pass the EPS checking.

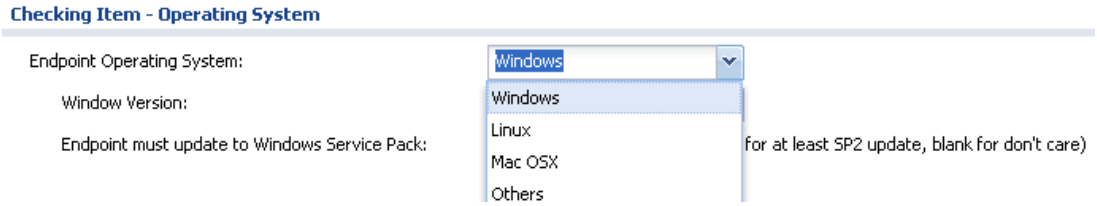


The first checking item is Operating System. You can select Windows, Linux, Mac OSX, and other OS.

If you choose OS as Windows, you can define the OS checking item in detail for its version and service pack.

Windows Version includes Windows 2000, Server 2003, XP, Vista, Windows 7, Server 2008 and Server 2008 R2.

Endpoint must update to Windows Service Pack- We can enter the minimum Windows service pack number the user's computer must have installed. The user's computer must have this service pack or higher.



The other checking items vary according to the OS you selected.

If OS checking item is selected as Windows, there’re additional checking items as the following:

- Windows Update and Security Patch
- Personal Firewall

  Personal firewall support list

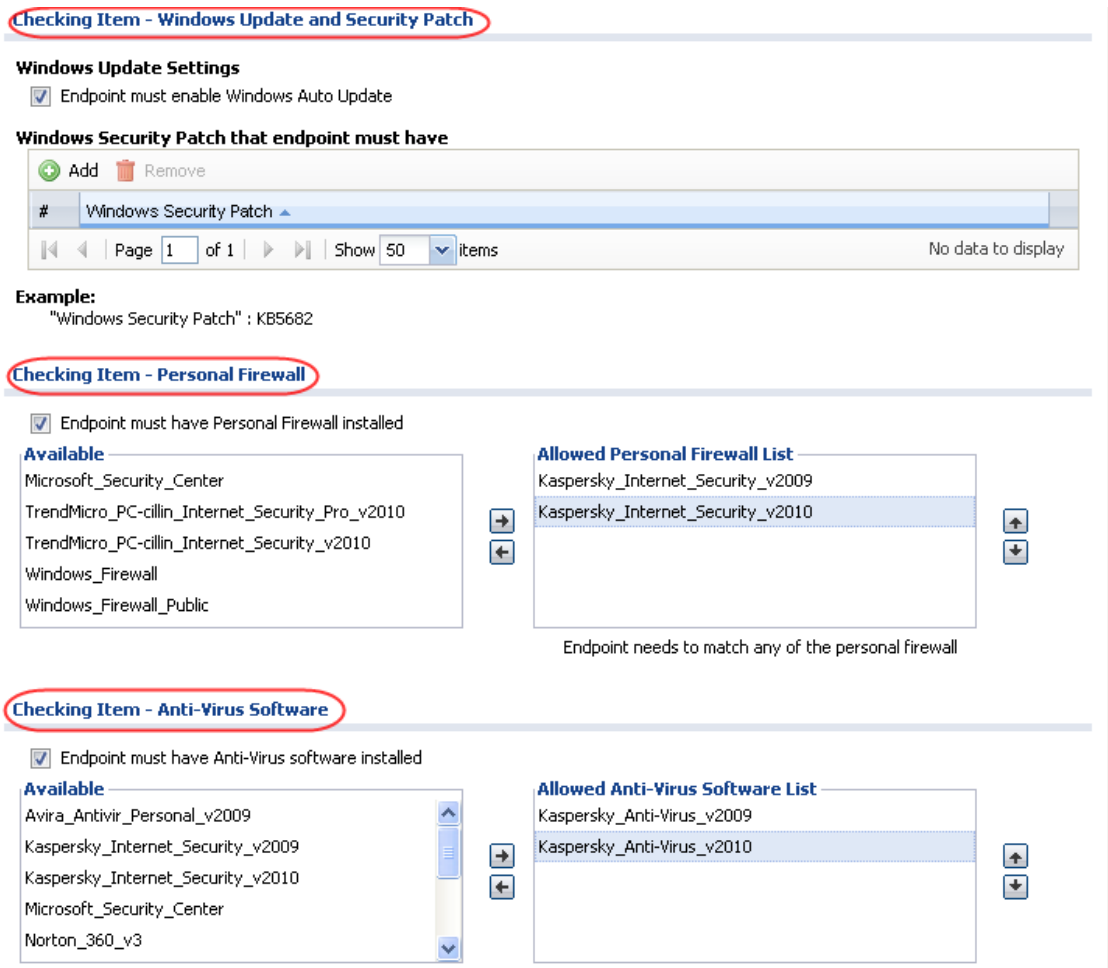
  - Kaspersky_Internet_Security_v2009
  - Kaspersky_Internet_Security_v2010
  - Microsoft_Security_Center
  - Windows_Firewall
  - Windows_Firewall_Public

- TrendMicro_PC-Cillin_Internet_Security_v2010
- TrendMicro_PC-Cillin_Internet_Security_Pro_v2010

▪ Anti-Virus Software

Anti-Virus Software support list

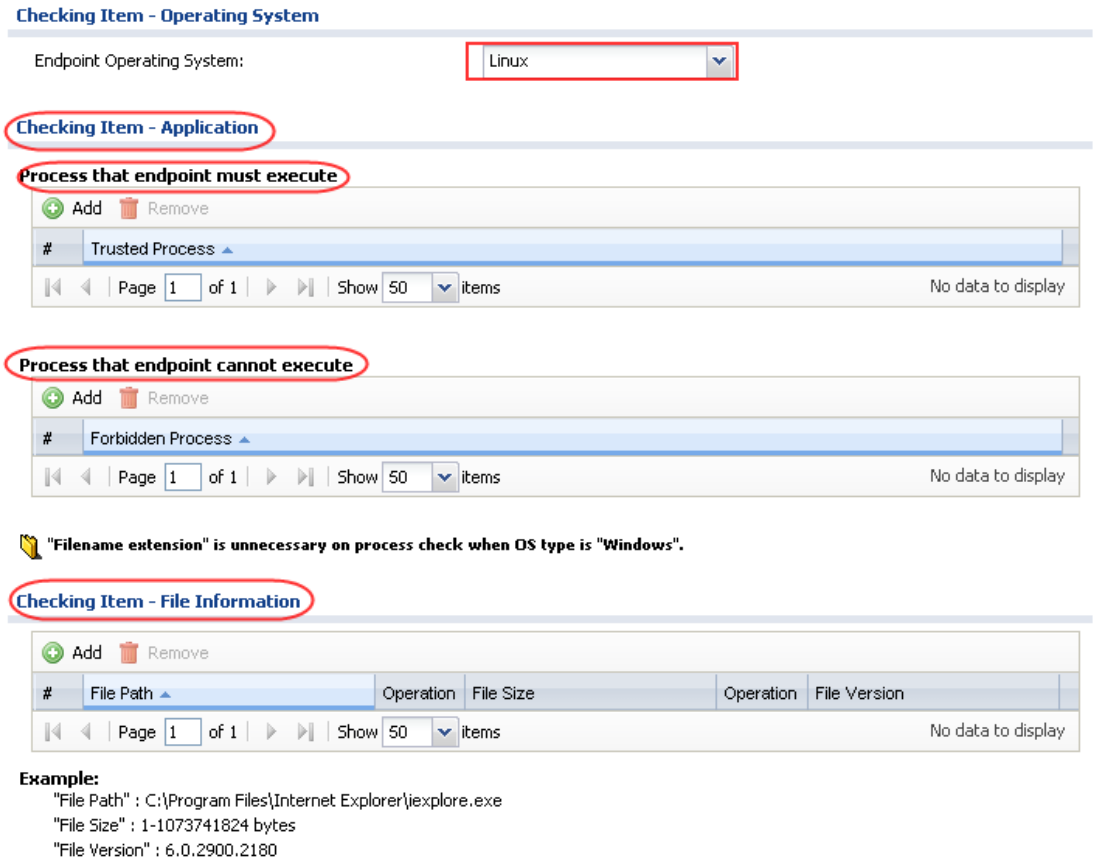
- Kaspersky_Anti-Virus_v2009
- Kaspersky_Anti-Virus_v2010
- Kaspersky_Internet_Security_v2009
- Kaspersky_Internet_Security_v2010
- TrendMicro_PC-Cillin_AntiVirus_v2010
- TrendMicro_PC-Cillin_Internet_Security_v2010
- TrendMicro_PC-Cillin_Internet_Security_Pro2010
- Norton_AntiVirus, 2010
- Norton_Internet_Security, 2010
- Norton_360 Version, version 3
- Avria AntiVir Personal_v2009



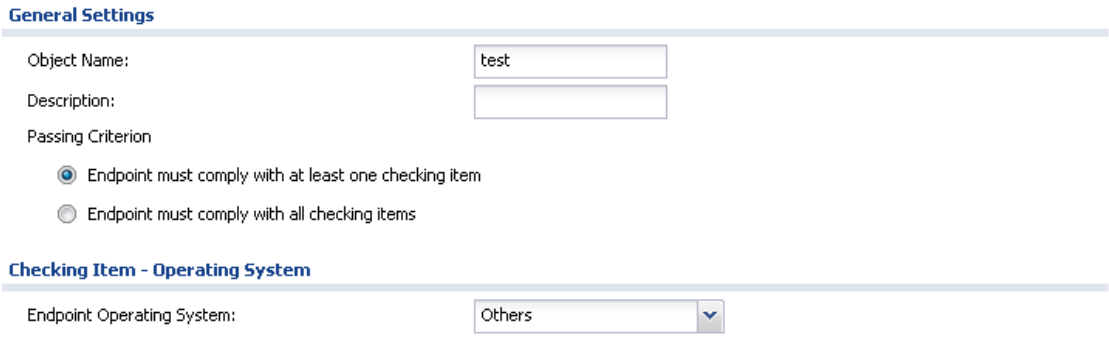
If OS checking item is selected as Linux, there’re additional checking items as the

following:

- Application
  - Process that endpoint must execute
  - Process that endpoint cannot execute
- File Information



If the OS checking item is selected as Mac OSX or Others, there's no additional checking item.



2.1.2.EPS --- CLI

You can use the CLI below to check your USG EPS information.

Router> show eps signature status

This command shows the current EPS signature status, including version, release date and signature numbers on your USG.

```
Router> show eps signature status
EPS signature information:
Current version   : 1.0.0.2
Release date      : 2009-1-21
Signature numbers : 19
Router> show eps signature personal-firewall
```

Router> show eps signature personal-firewall

This command shows current EPS signatures for personal firewall checking.

```
Router> show eps signature personal-firewall
No.  Name                                                          Detection
==============================================================================
1    Kaspersky_Internet_Security_v2009                              yes
2    Kaspersky_Internet_Security_v2010                              yes
3    Microsoft_Security_Center                                      yes
4    Windows_Firewall                                               yes
5    TrendMicro_PC-cillin_Internet_Security_v2010                   yes
6    TrendMicro_PC-cillin_Internet_Security_Pro_v2010               yes
7    Windows_Firewall_Public                                        yes
```

Router> show eps signature anti-virus

This command shows the current EPS signatures for anti-virus program checking.

```
Router> show eps signature anti-virus
No.  Name                                                          Detection
==============================================================================
1    Norton_Anti-Virus_v2010                                        no
2    Norton_Internet_Security_v2010                                 no
3    Norton_360_v3                                                  no
4    Microsoft_Security_Center                                      yes
5    TrendMicro_PC-cillin_AntiVirus_v2010                           yes
6    TrendMicro_PC-cillin_Internet_Security_v2010                   yes
7    TrendMicro_PC-cillin_Internet_Security_Pro_v2010               yes
8    Avira_Antivir_Personal_v2009                                   no
9    Kaspersky_Anti-Virus_v2010                                     yes
10   Kaspersky_Internet_Security_v2010                              yes
11   Kaspersky_Anti-Virus_v2009                                     yes
12   Kaspersky_Internet_Security_v2009                              yes
```

NOTE: If the Detection status is “no”, it means this EPS signature can only detect whether the software is installed, but it cannot detect whether it’s active or not. If the Detection status is “yes”, it means this EPS signature can detect whether the software is installed, as well as detect whether it’s active or not.

2.1.3. EPS Application Note

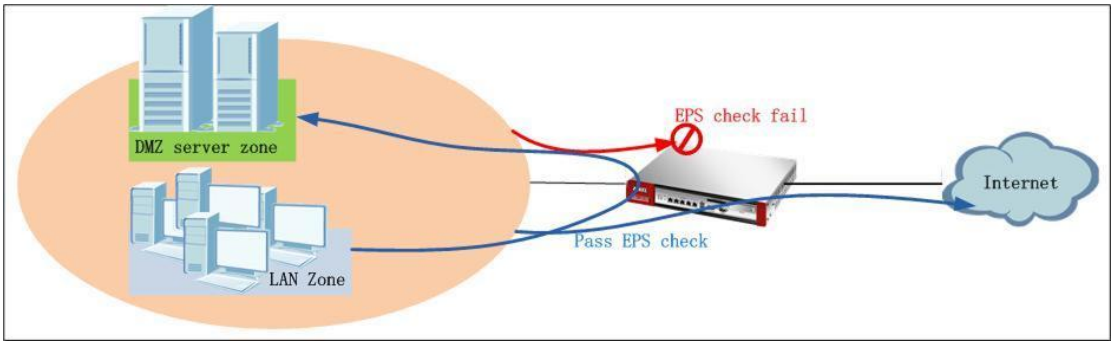
1. If you want to use EPS feature, no matter in User Aware application or in SSL VPN application, you should install Java, and make sure Java is enabled in your browser.
2. Although EPS checking is achieved by EPS signatures, it doesn't need license. The signature is updated with firmware upgrade.

2.2. Deploy EPS in User Aware

To protect company network, the administrator can set Authentication Policies to restrict clients that not only pass user aware authentication, but also pass EPS checking, can reach certain network resources, such internet, or DMZ serves.

2.2.1. Application Scenario

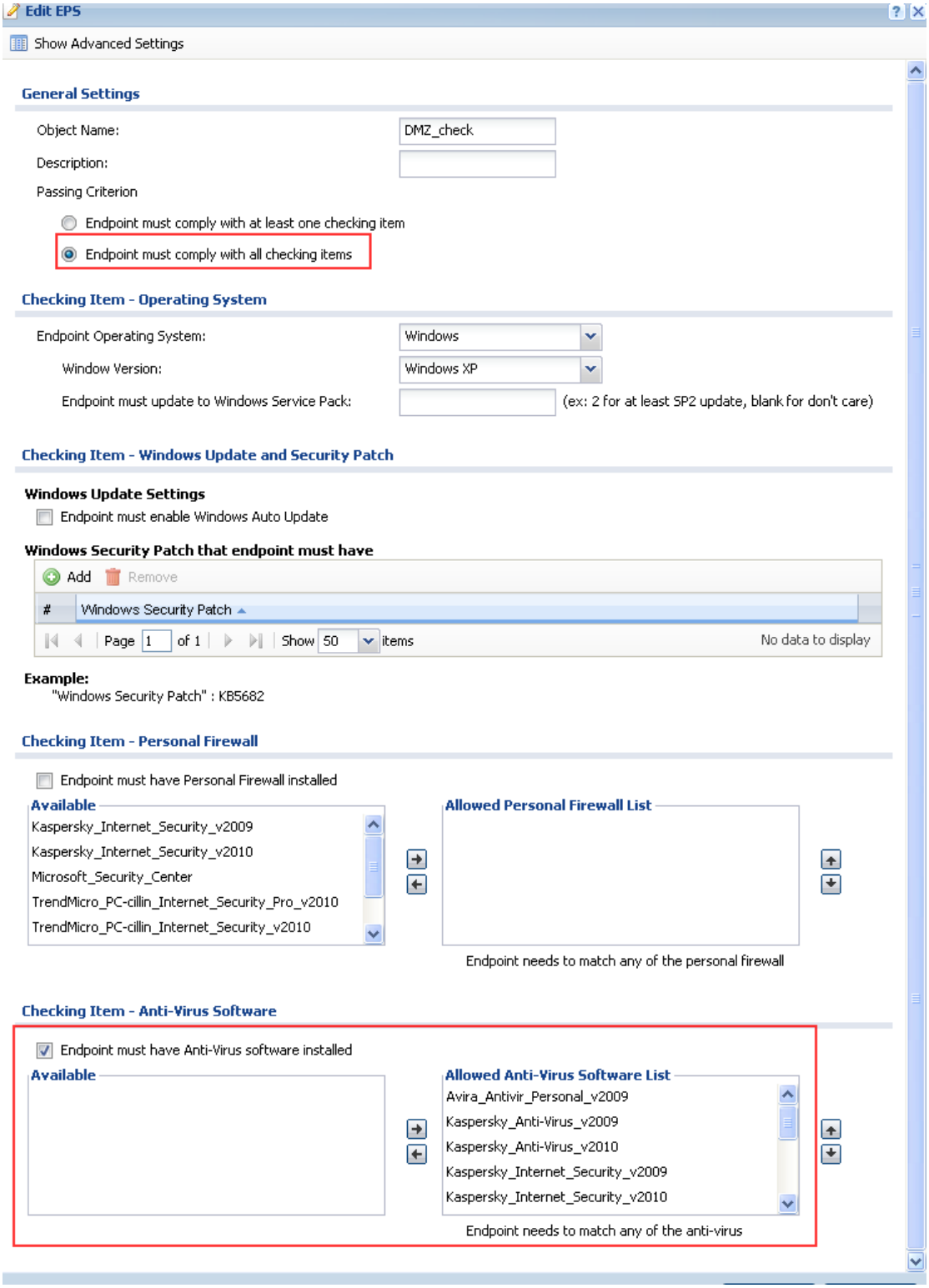
The company has LAN zone and DMZ server zone. The network administrator makes restrictions as following:
Only clients that have anti-virus software installed can access the servers in DMZ zone.
Only clients that have both anti-virus software and personal firewall installed can access internet.



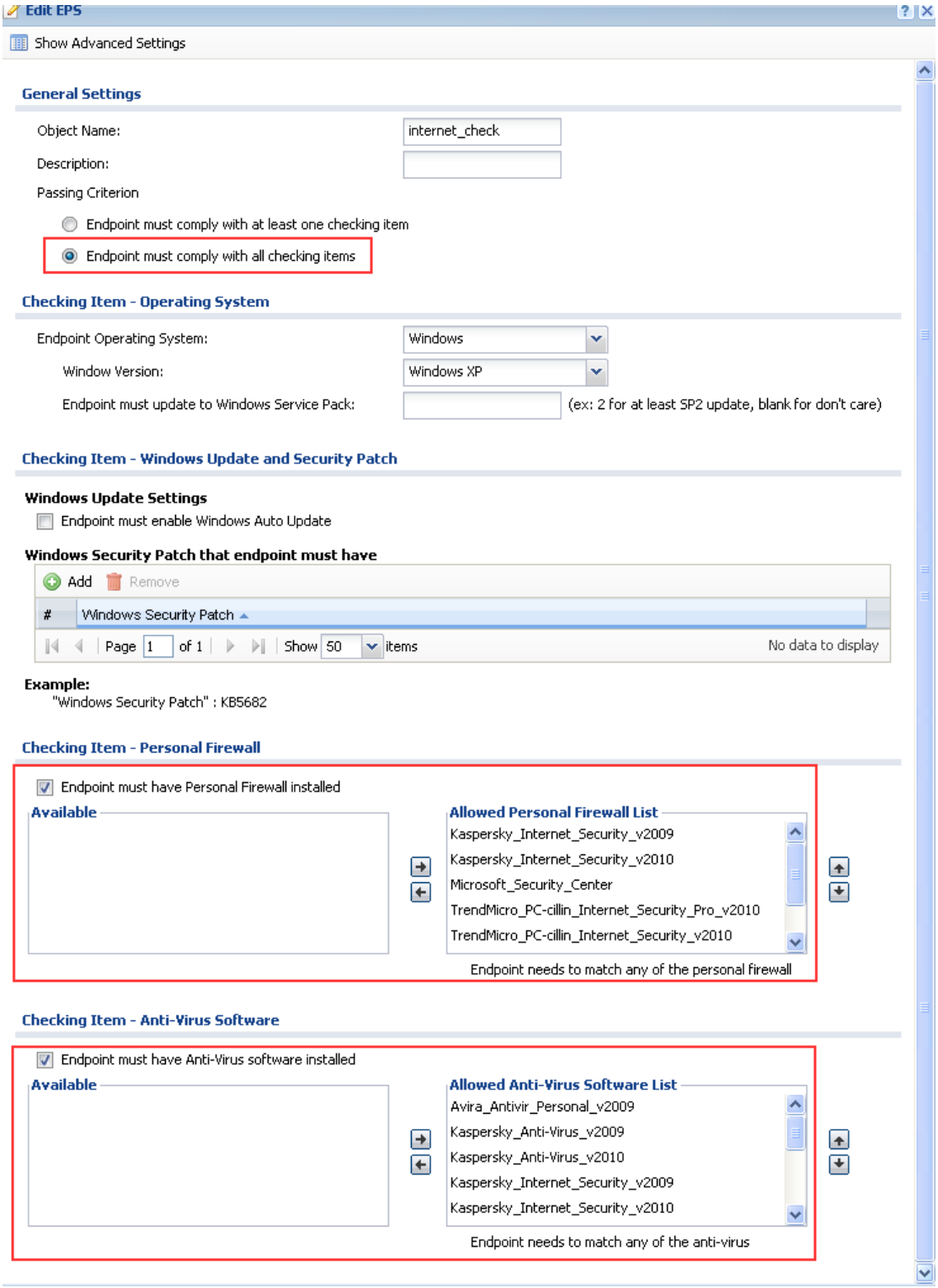
2.2.2. Configuration Steps

Step1. Go to Configuration > Object > Endpoint Security, add EPS objects.

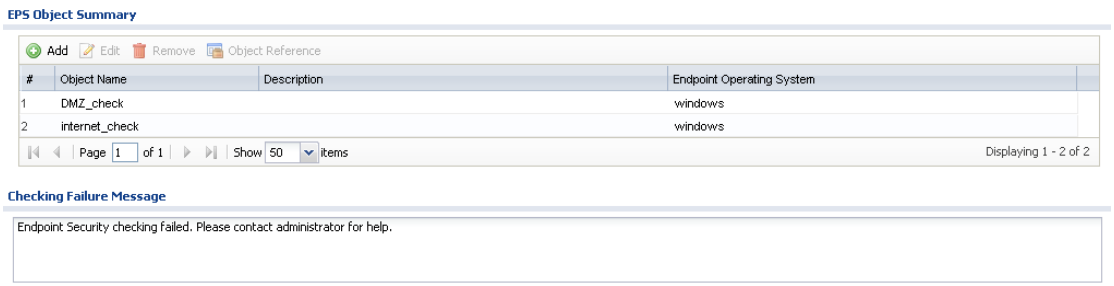
Add EPS object that complies with DMZ checking requirements.



Add EPS object that complies with internet checking requirements.

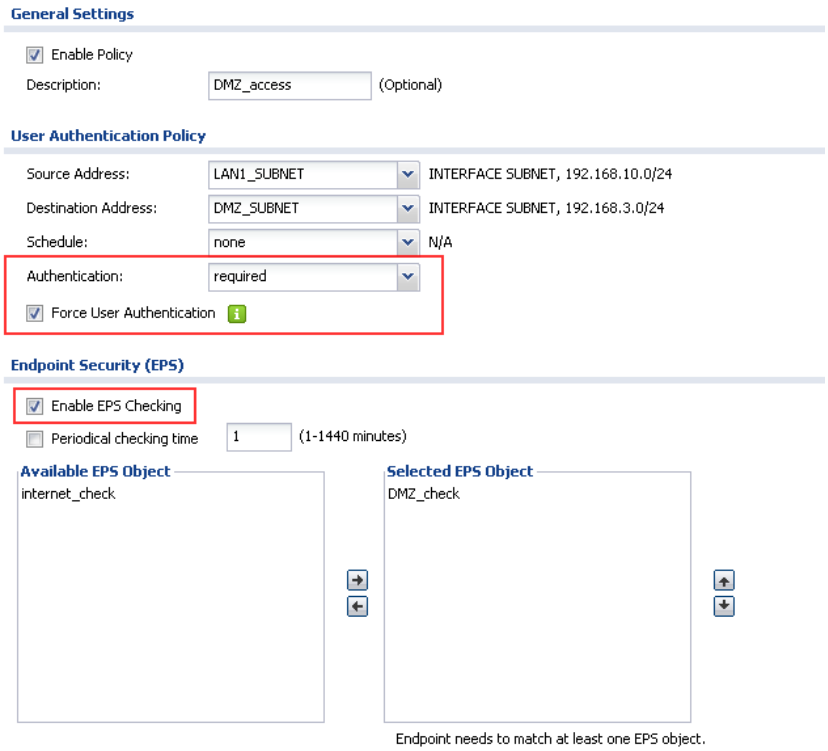


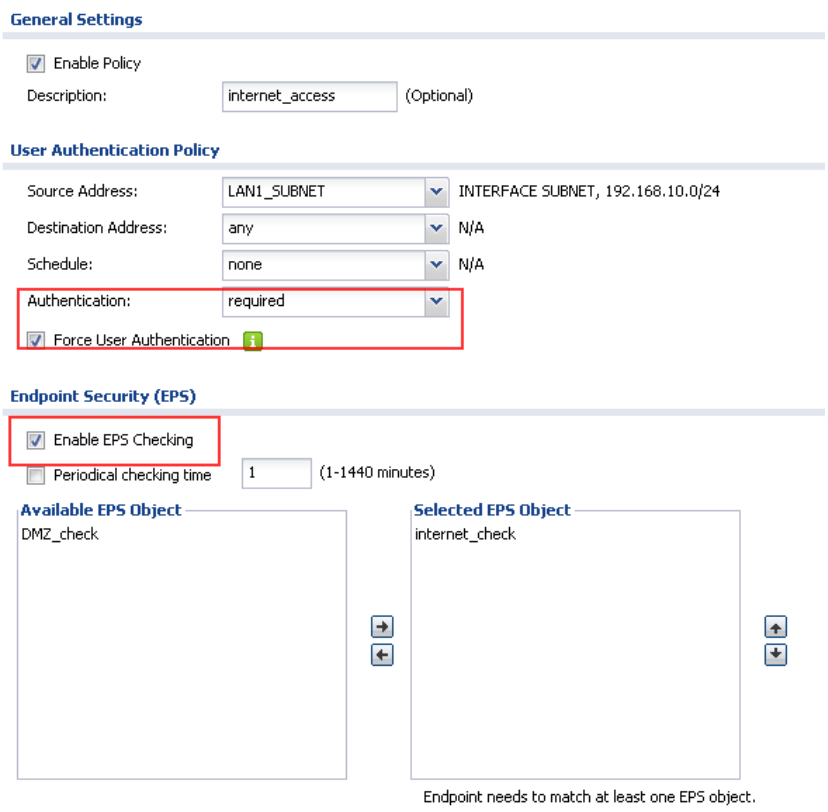
EPS object summary.



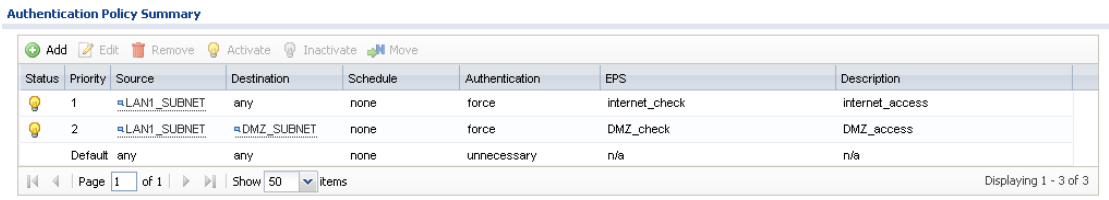
Step2. Go to Configuration > Authentication Policy, enable Authentication Policy.

Add authentication policies for DMZ access and internet access checking.





Below is the Authentication Policy summary.

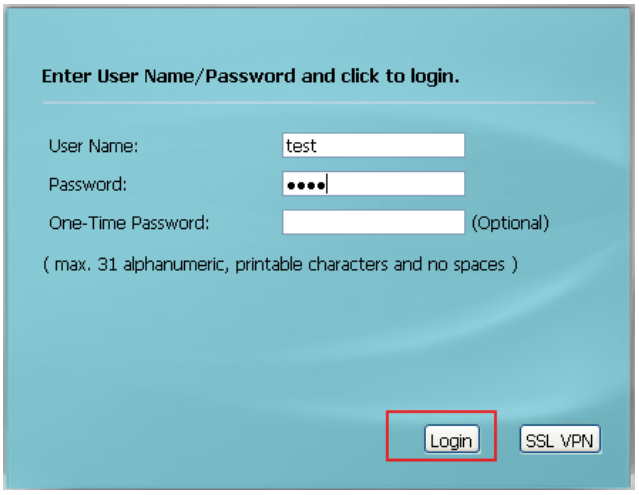


2.2.3.Scenario Verification

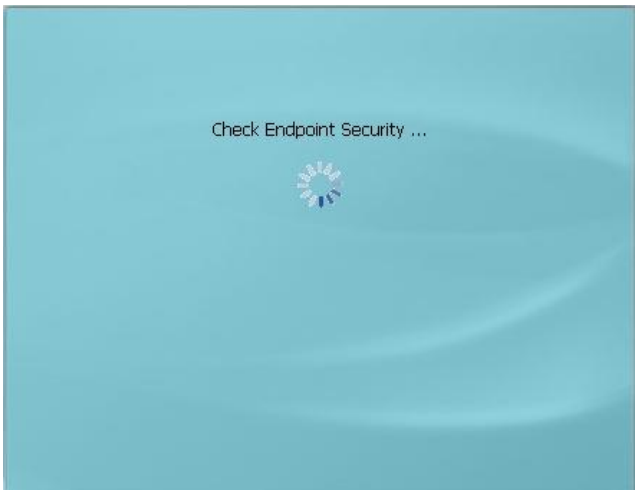
Before LAN clients pass authentication, they cannot access internet.

```
C:\Documents and Settings\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
```

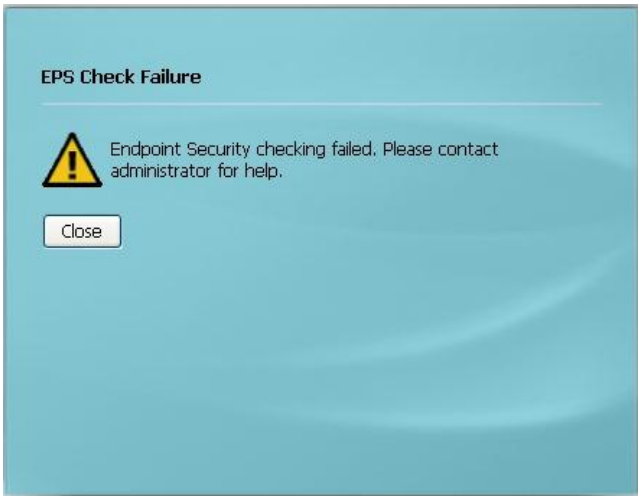
Access the USG login page, and enter username and password to go through the USG checking.



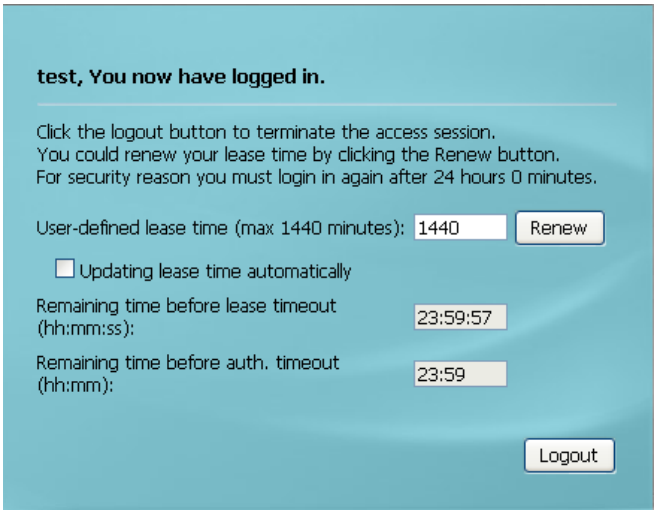
USG will perform the EPS checking action.



If the client's environment doesn't comply with the EPS checking criterion, the USG will give out the message as below.



After the client pass the USG authentication and EPS checking, the USG will grant the client access to the internet.

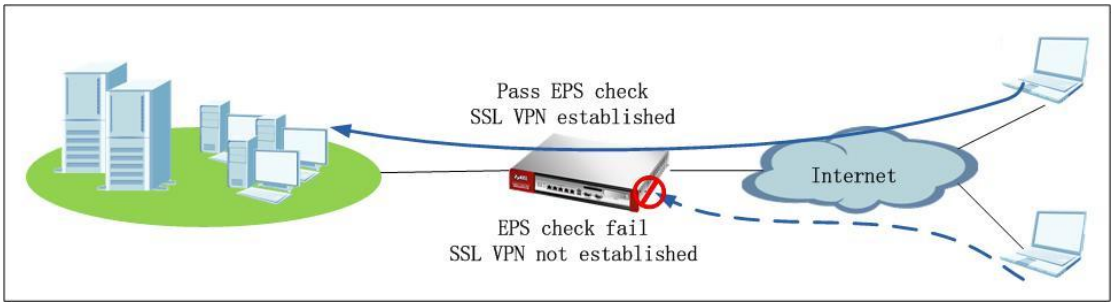


2.3. Deploy EPS in SSL VPN

In SSL VPN application, some SSL VPN clients may not have anti-virus software installed. They may have some virus. If they access HQ network resources through SSL VPN, they may propagate virus to the HQ network. HQ network administrator can utilize EPS to restrict SSL VPN clients that only comply with certain security criterion can build SSL VPN with the HQ USG.

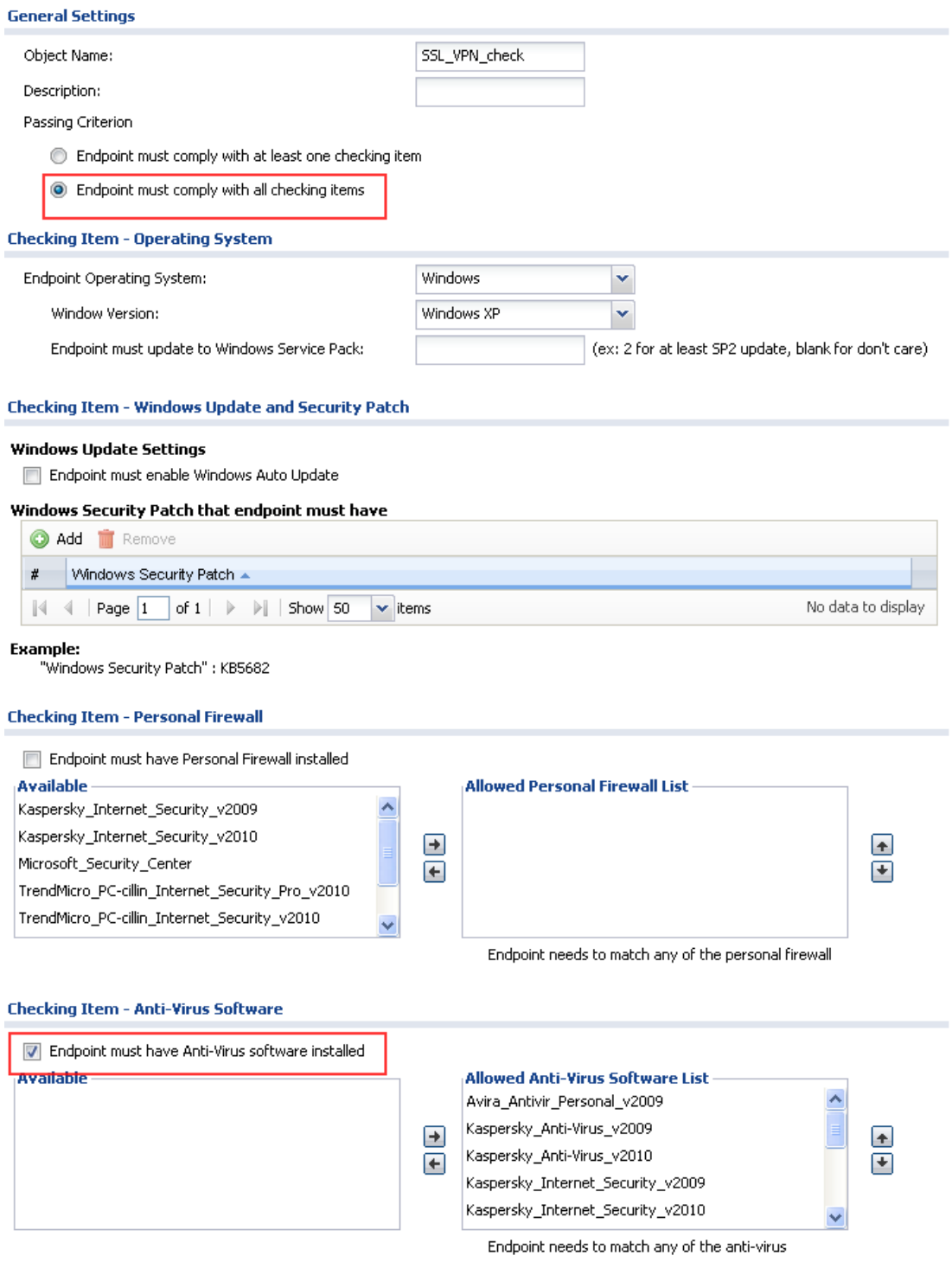
2.3.1. Application Scenario

Internet clients can access HQ resources by building SSL VPN to HQ USG. To prevent any SSL VPN client from bringing virus to HQ network, administrator can enable EPS check in SSL VPN policy, to allow only clients that have anti-virus software installed to build SSL VPN tunnel to USG.



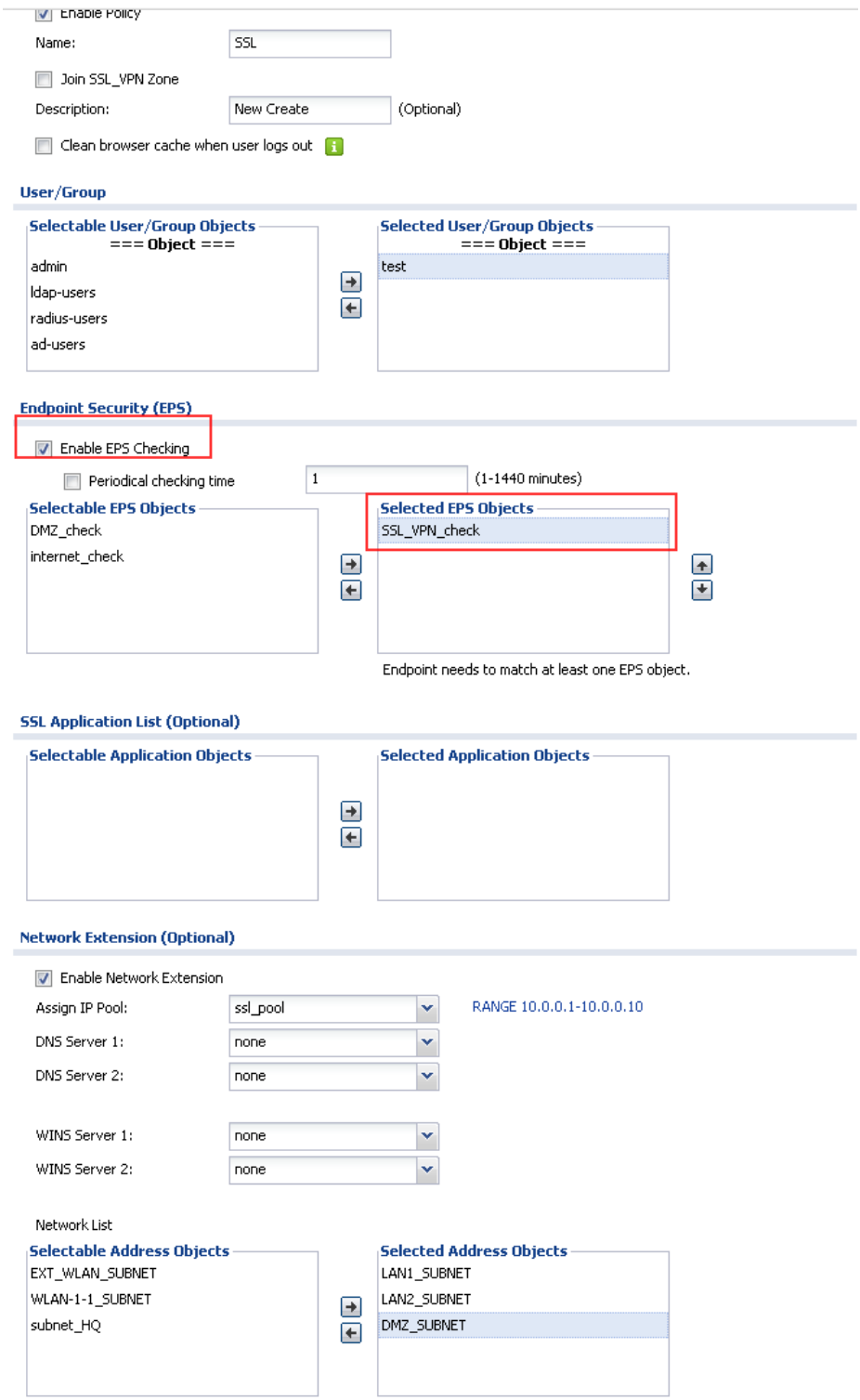
2.3.2.Configuration Steps

Step1. Go to Configuration>Object>Endpoint Security, add EPS object for SSL VPN check.



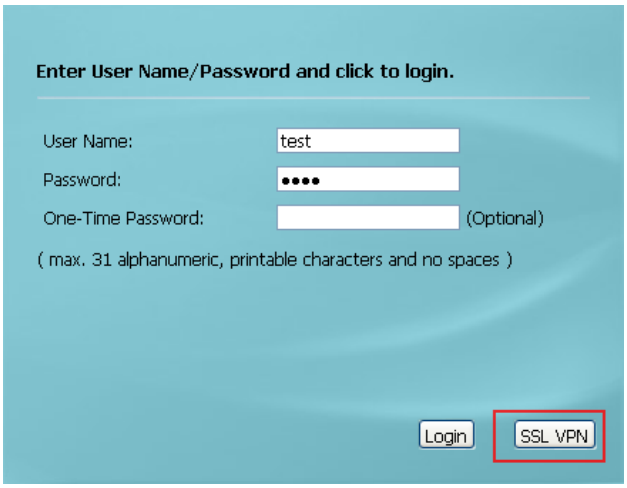
Step2. Go to Configuration > VPN > SSL VPN > Access Privilege, add SSL VPN policy.

Enable EPS checking, and select the EPS object for SSL VPN checking.

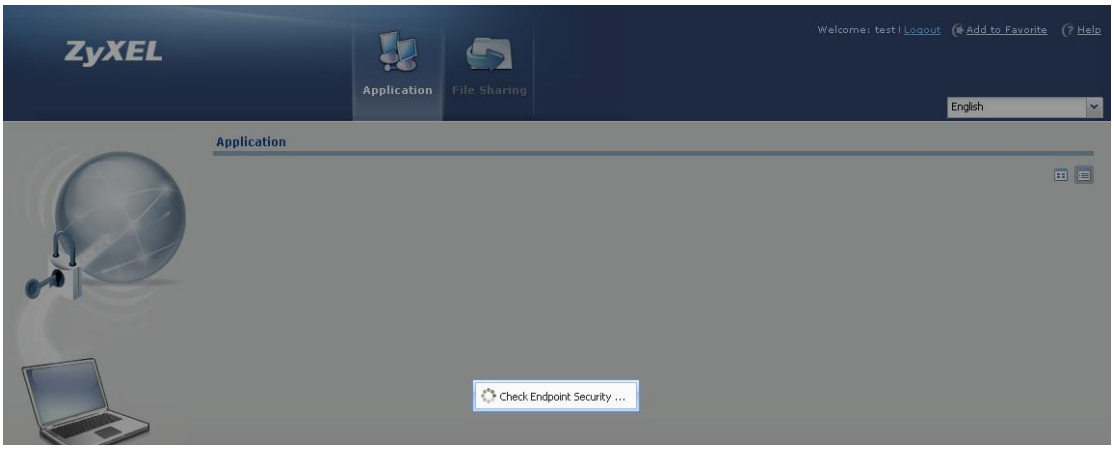


2.3.3.Scenario Verification

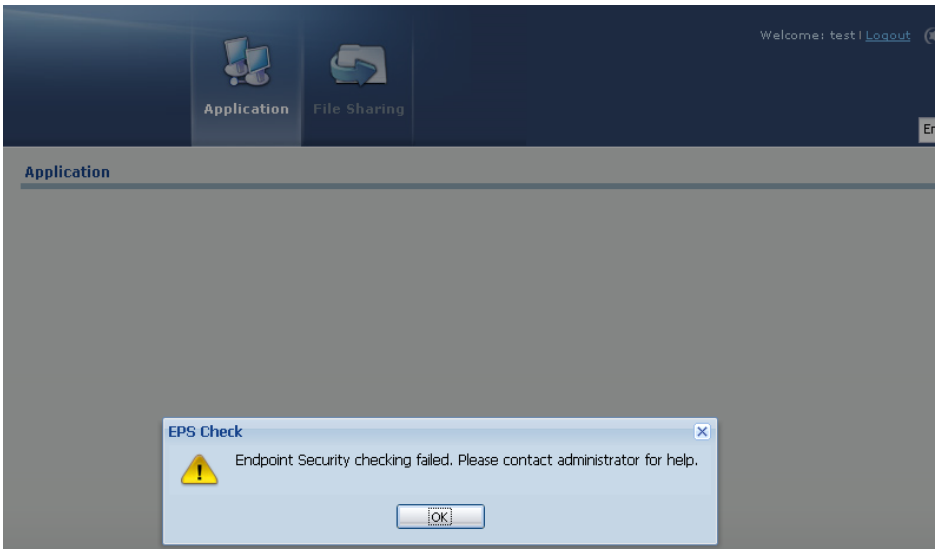
SSL VPN client tries to login to build SSL VPN tunnel to USG.



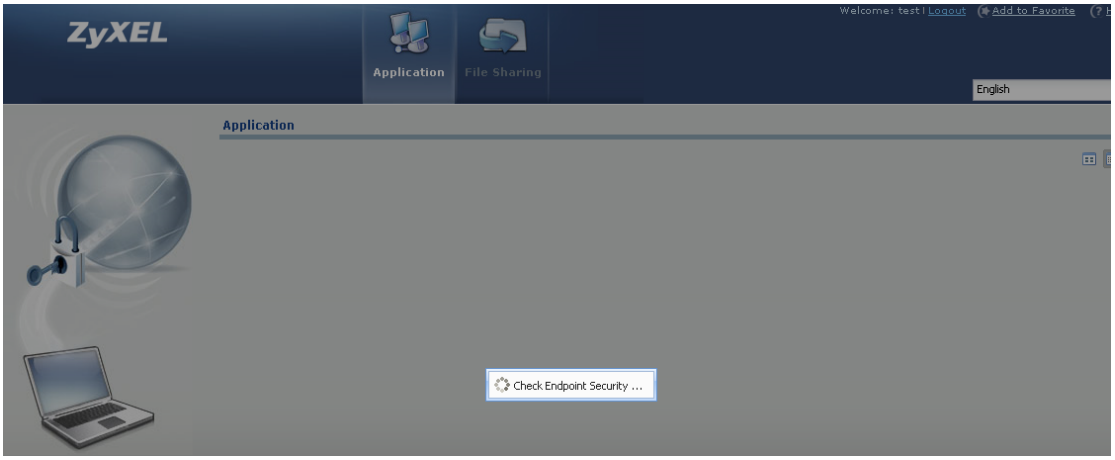
USG starts to perform EPS checking according to the EPS object selected in the SSL VPN policy.

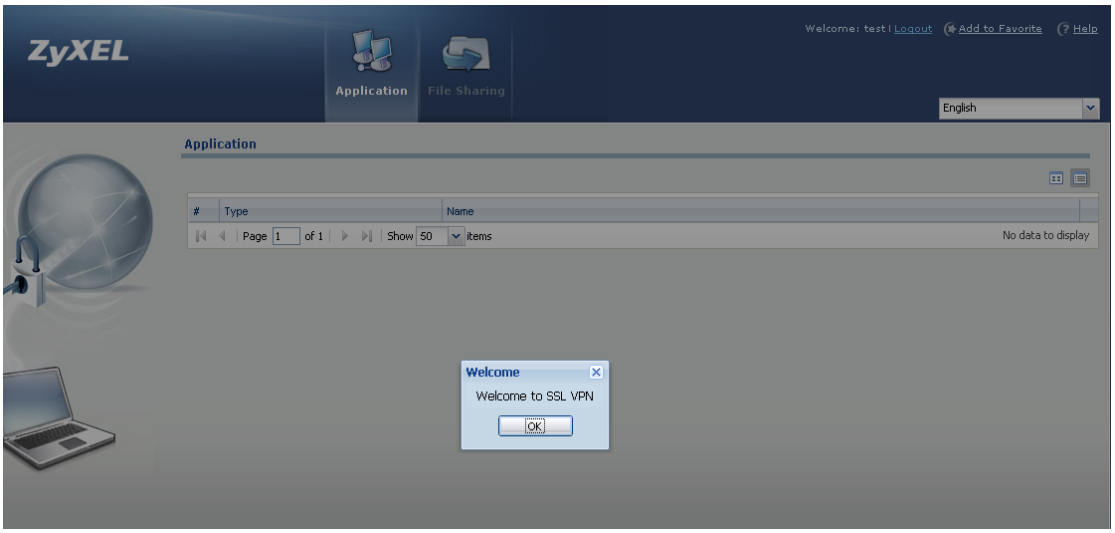


If the SSL VPN client doesn’t comply with the EPS criterion, the EPS check will fail, and SSL VPN tunnel will fail to establish.



If the SSL VPN client complies with the EPS criterion, it will pass the EPS check and SSL VPN tunnel will be established.

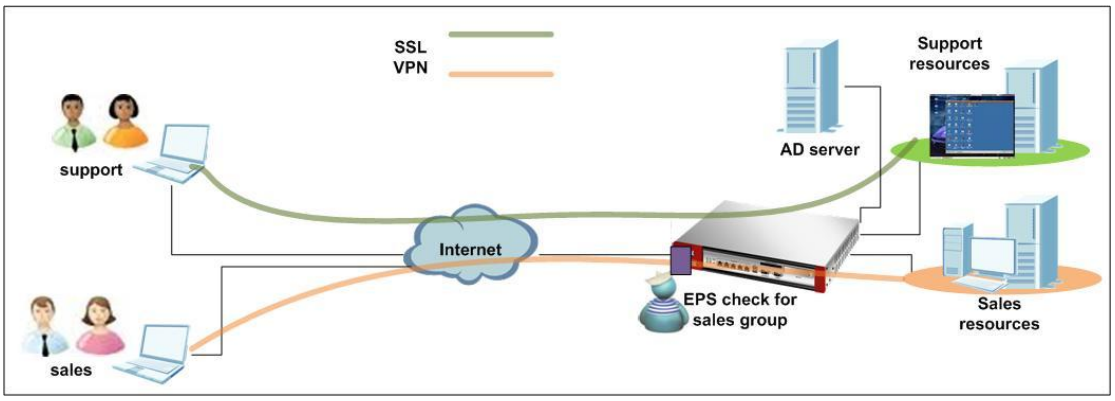




2.4. Deploy AAA and EPS in SSL VPN

2.4.1. Application Scenario

In the scenario below, there're sales group users and CSO support group users in the AD server. Support users and sales users can access company resources by building SSL VPN to the company gateway USG.
The company requires that support users and sales users access different network resources. For example, the support can only access company support fileshares, and sales can only access company sales fileshares. So network administrator can configure different SSL VPN rules for different group users. Also network administrator can deploy different EPS checking policies for different SSL VPN rules. For example, he/she can deploy EPS check for sales, while not deploying EPS check for support.



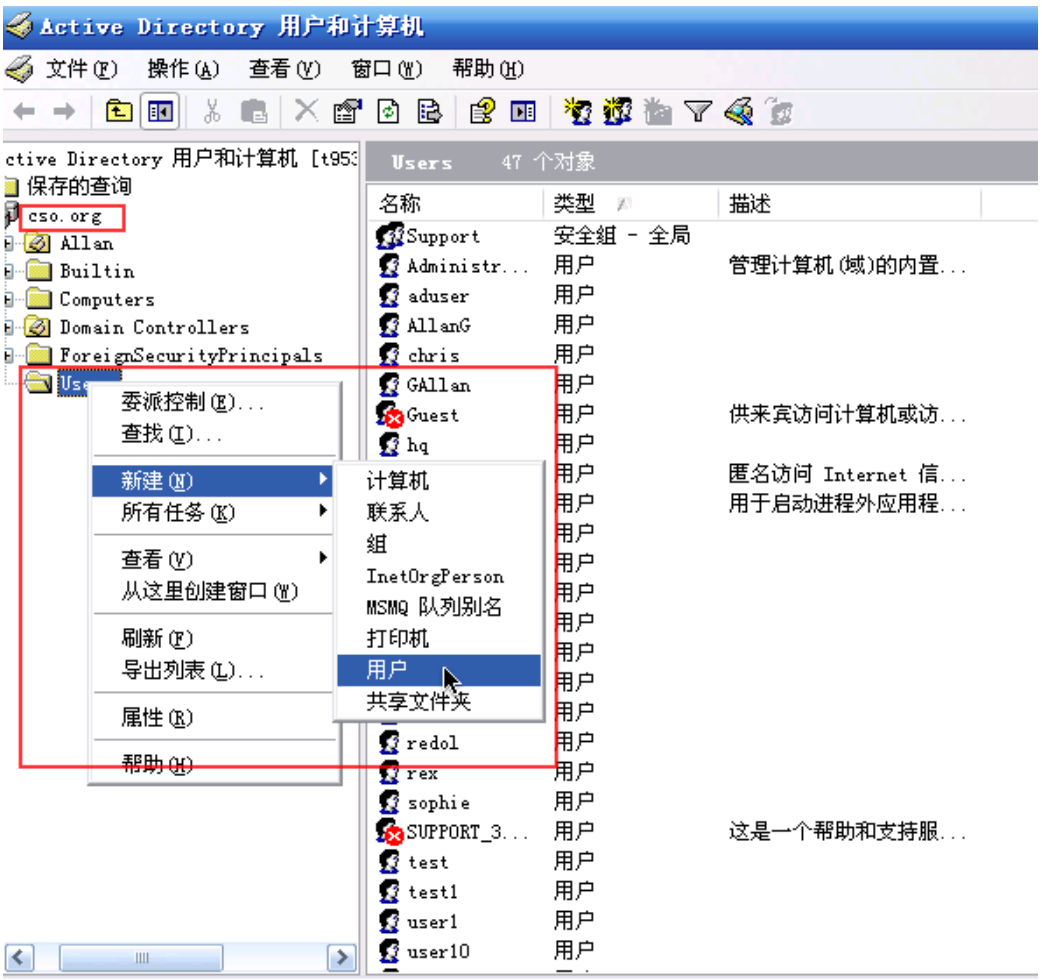
2.4.2. Configuration Steps

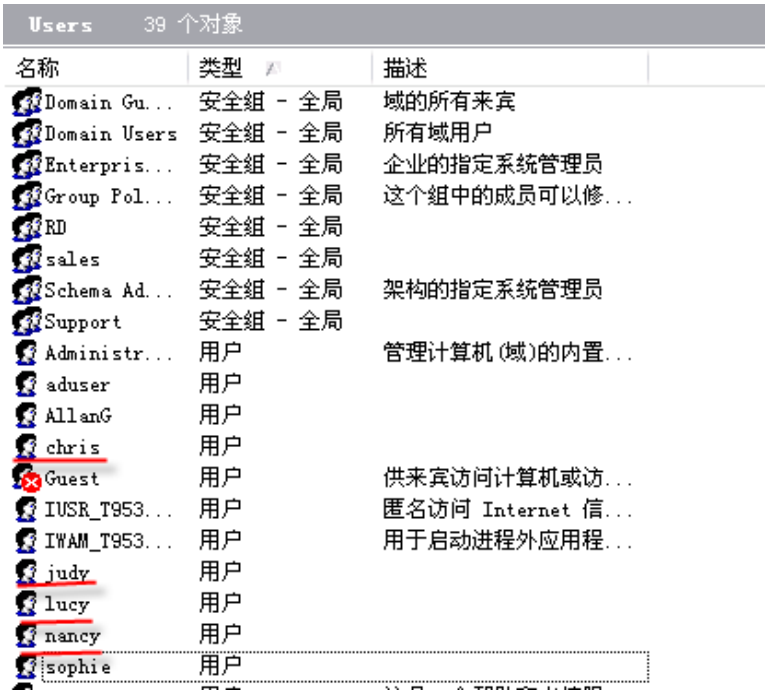
Step1. On AD server, add users/groups in AD server.
Go to Start > Administrative Tools >Active Directory user and computer.

Go to Users > New > Users. Add user accounts.

In this example, we add new users “judy”, “nancy”, “chris” and “lucy”.

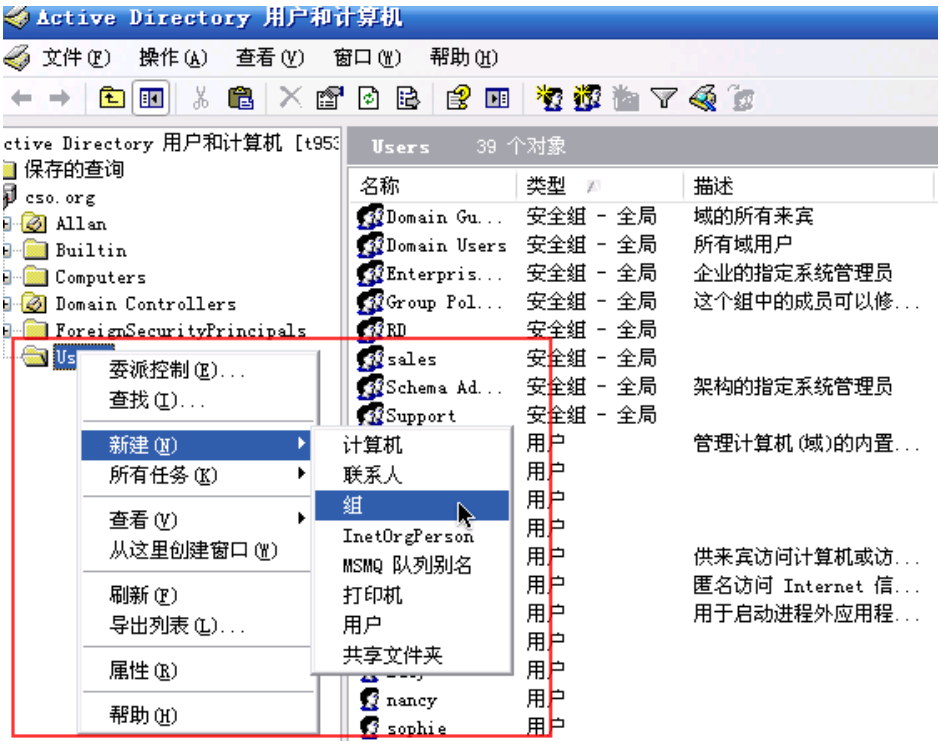
Please note your AD server’s domain name. In this example the AD domain is cso.org.



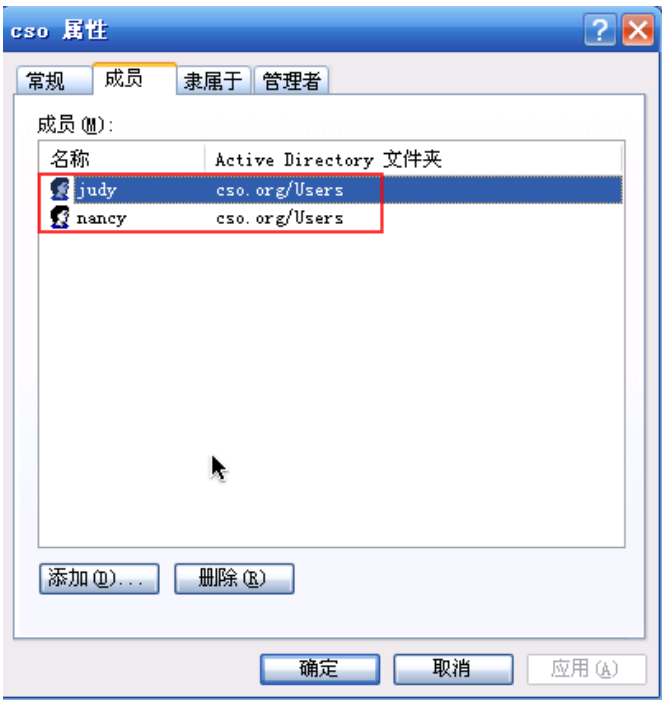


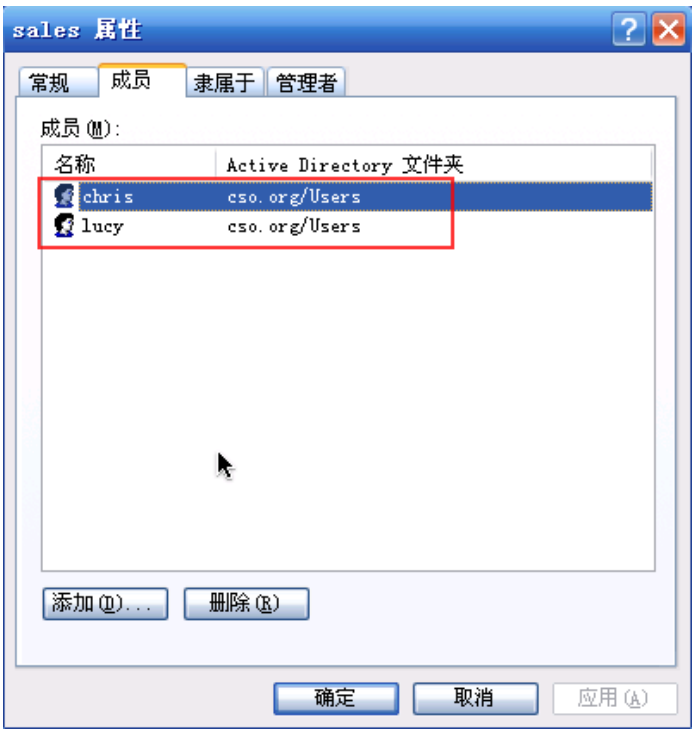
Switch to menu Users > New > Group. Add groups. In this example, we add two “cso”

and “sales”.



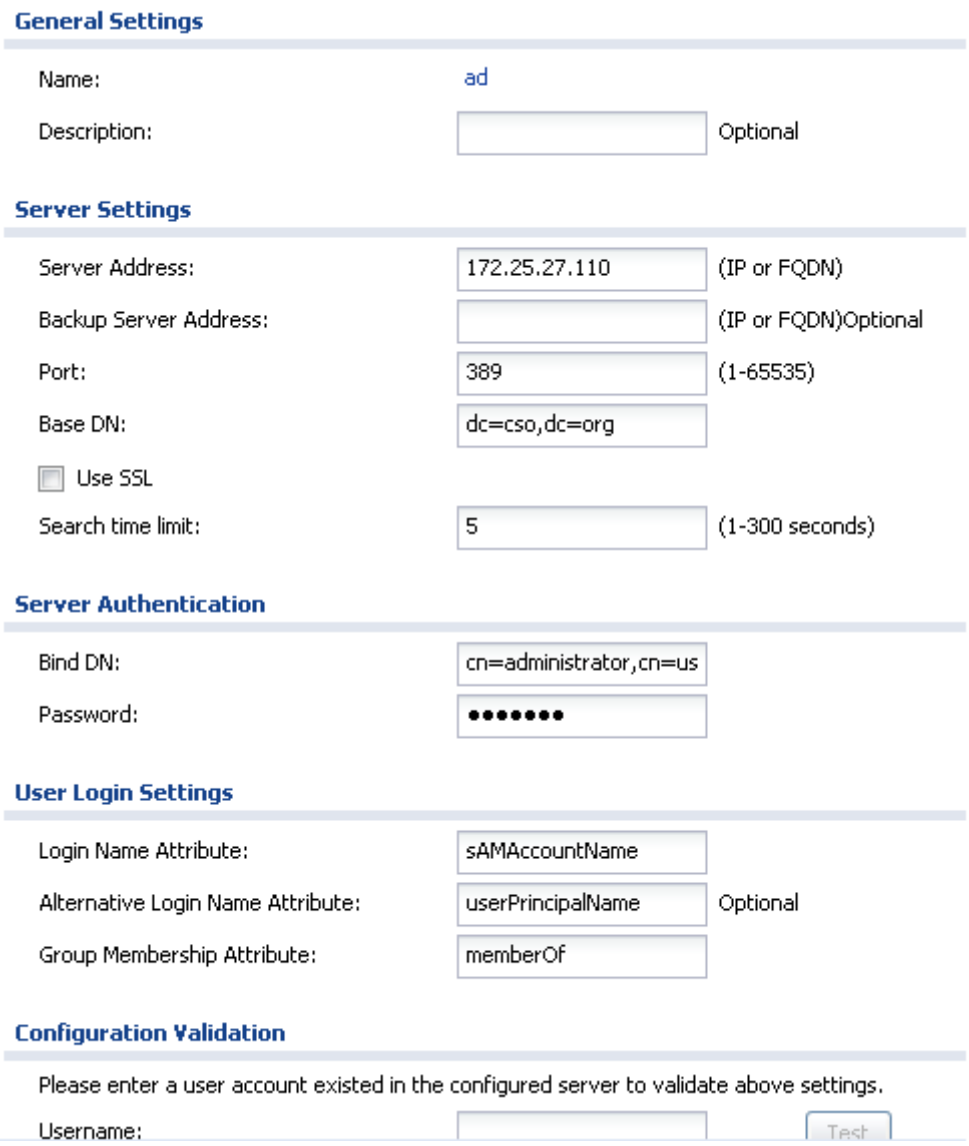
Assign “judy” and “nancy” to the group “cso”. And assign “chris” and “lucy” to the group “sales”.





Step2. On USG, configure AAA Server.

Go to Configuration > Object > AAA Server > Active Directory. Edit the profile “ad”.



Put in the company AD server's address in Server Address field.

The default port of AD server is UDP 389. If your AD server is configured as a different port, please input the corresponding port number here.

For the Base DN field, if your AD server's domain is cso.org, please input like below: dc=cso, dc=org

The Server Authentication part is for the USG get authenticated by the AD server before it can use AD server's active directory database.

Bind DN: Please fill in the field like: cn=<administrator>,cn=users,dc=cso,dc=org

You can replay <administrator> with any user configured in the AD.

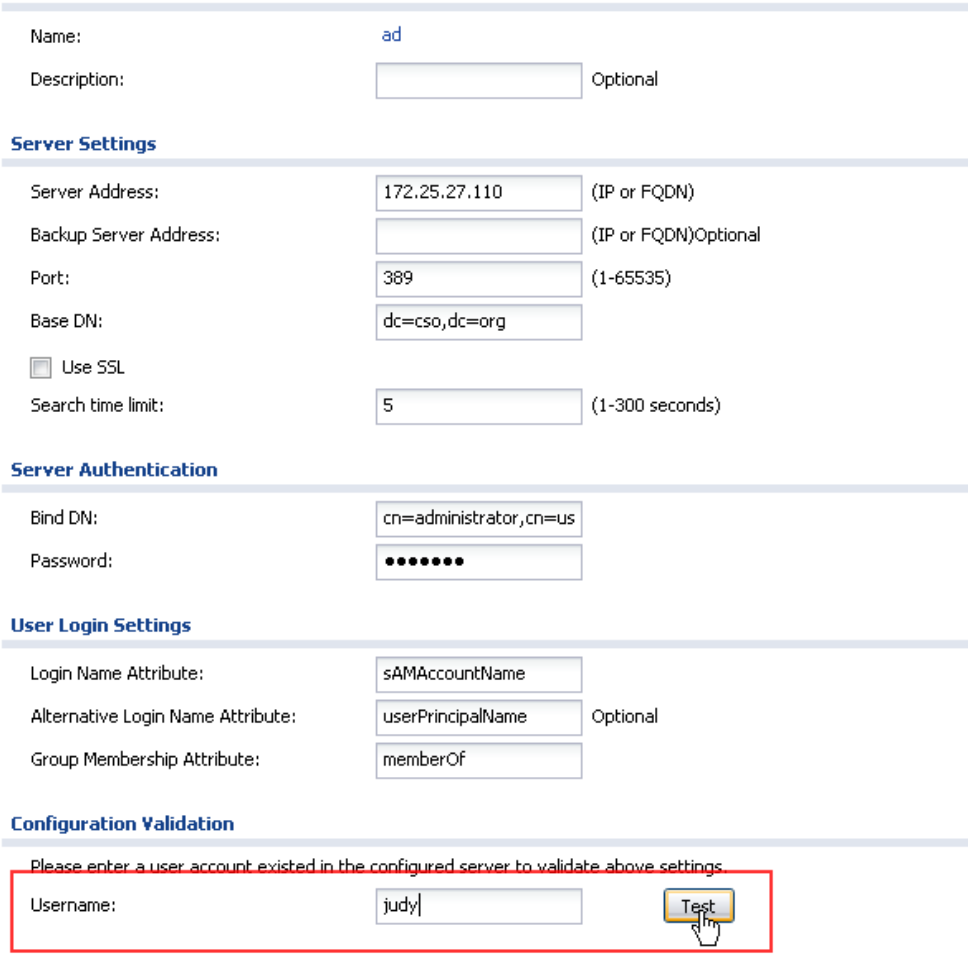
"dc=cso,dc=org" is the AD server's domain. In this example is cso.org.

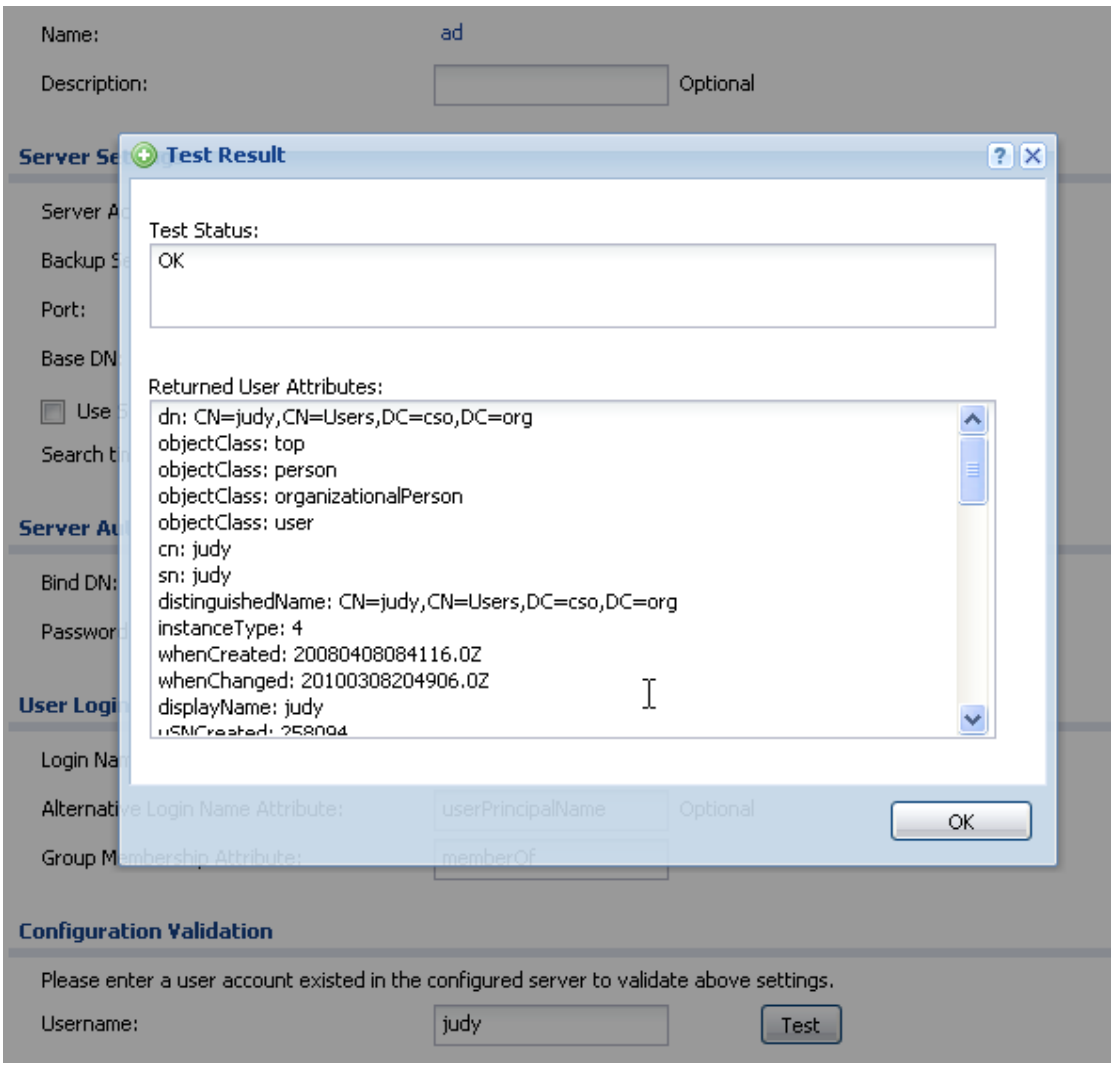
Password is the corresponding password of <administrator>.

When a Bind DN is not specified, the ZyWALL will try to log in as an anonymous user.

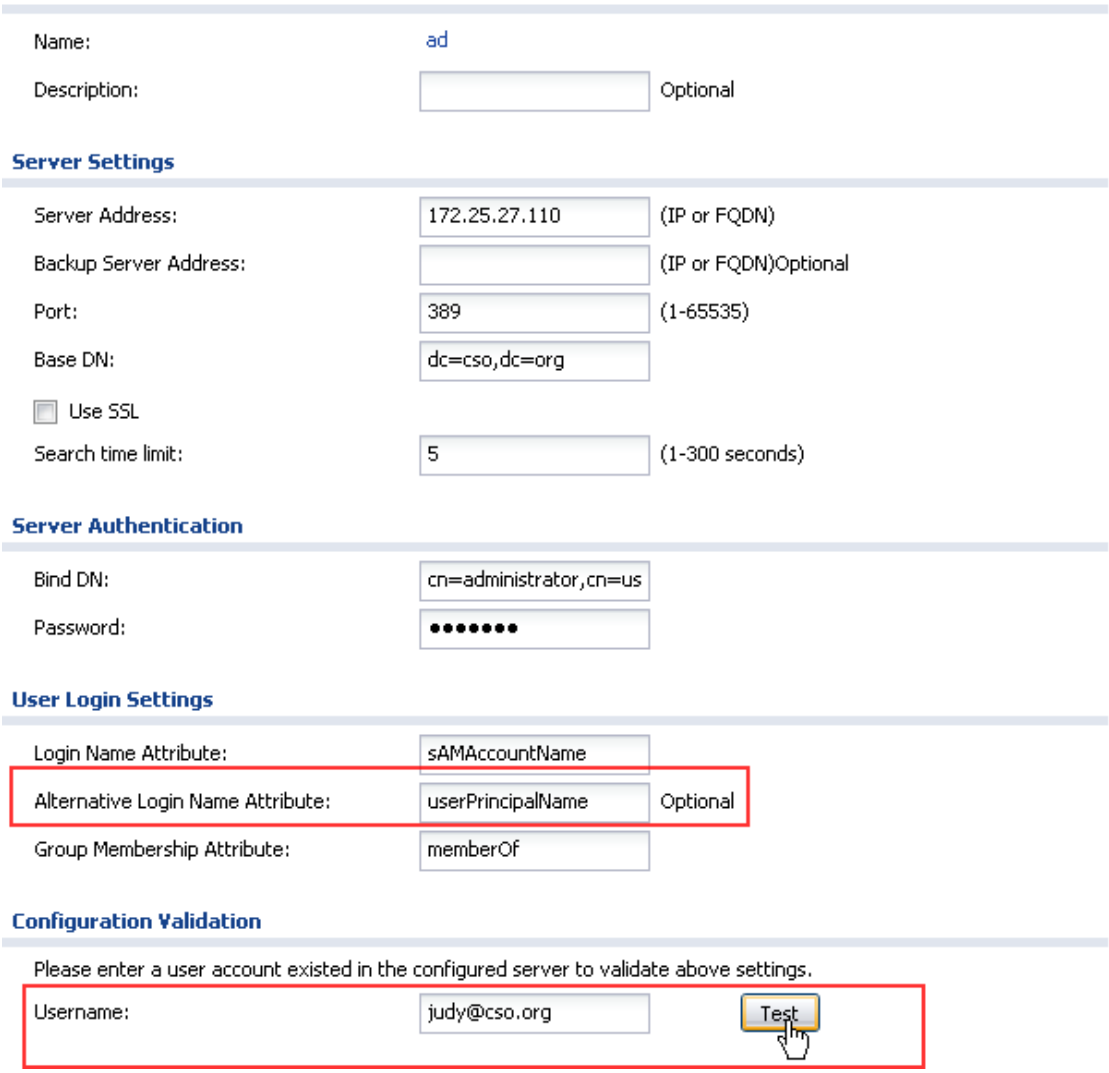
Please leave the “Login Name Attribute” and “Group Membership Attribute” as system default.
Alternative Login Name Attribute is optional. You can fill in “userPrincipalName” here. Then users can login the USG by email address as well as by user name.

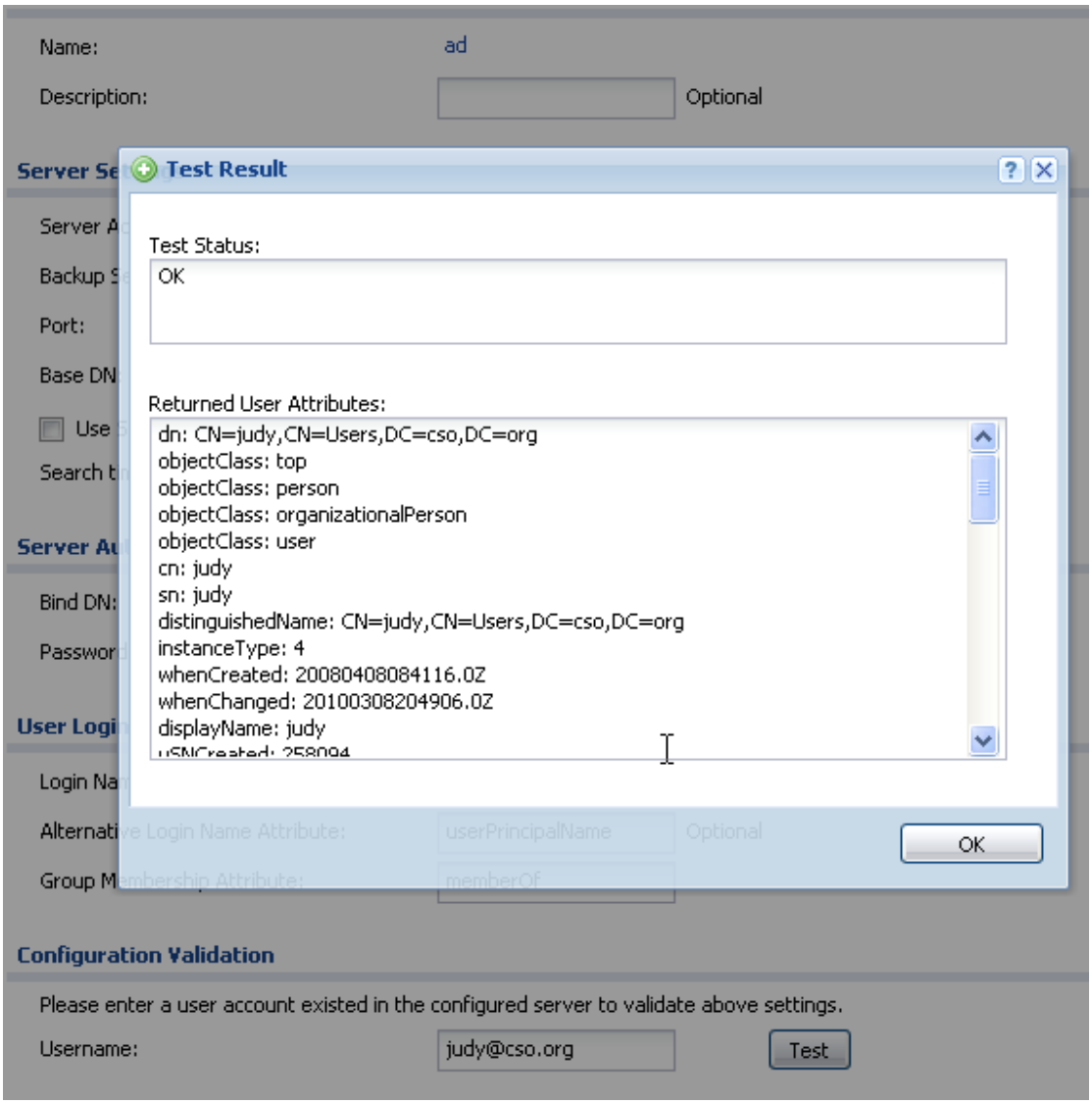
After the configuration of AD is done, you can verify whether the configuration is ok, and the communication between AD and USG is ok.





If you have entered the attribute “Alternative Login Name Attribute” as shown in the picture below, you can also verify by user mail address.





Step3. Go to Configuration > Object > User/Group > User, add user groups corresponding to the groups in the AD server.

In this example, we add two groups that correspond to the ones on the AD server: “cso” and “sales”.

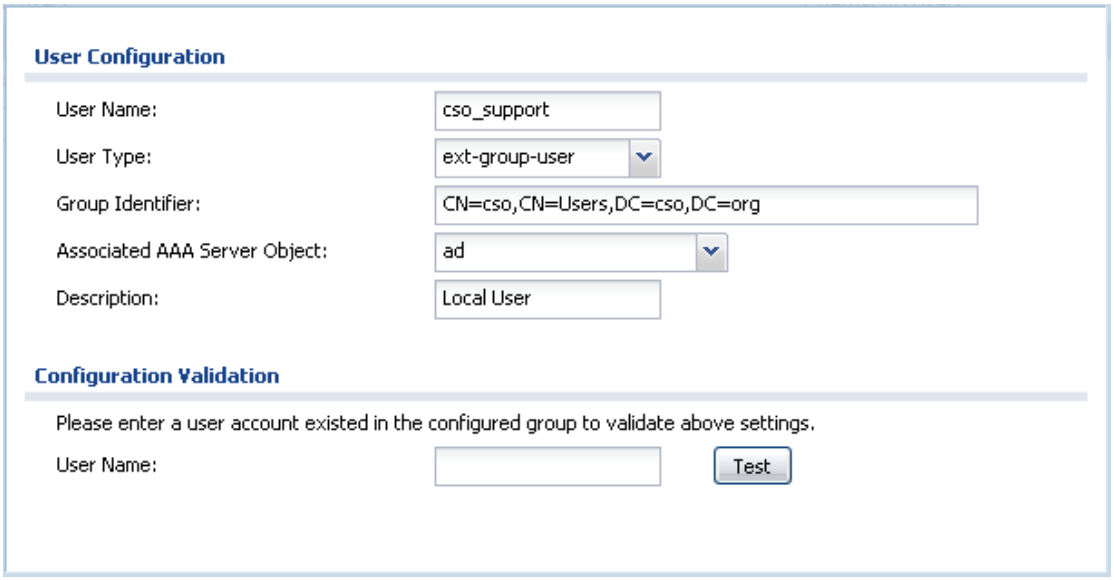
The User Name can be different from the group identifier. E.g. the group identifier of “cso” group is “cso”, but we can specify a different name such as “cso_support”.

The Group Identifier must follow the format as below:

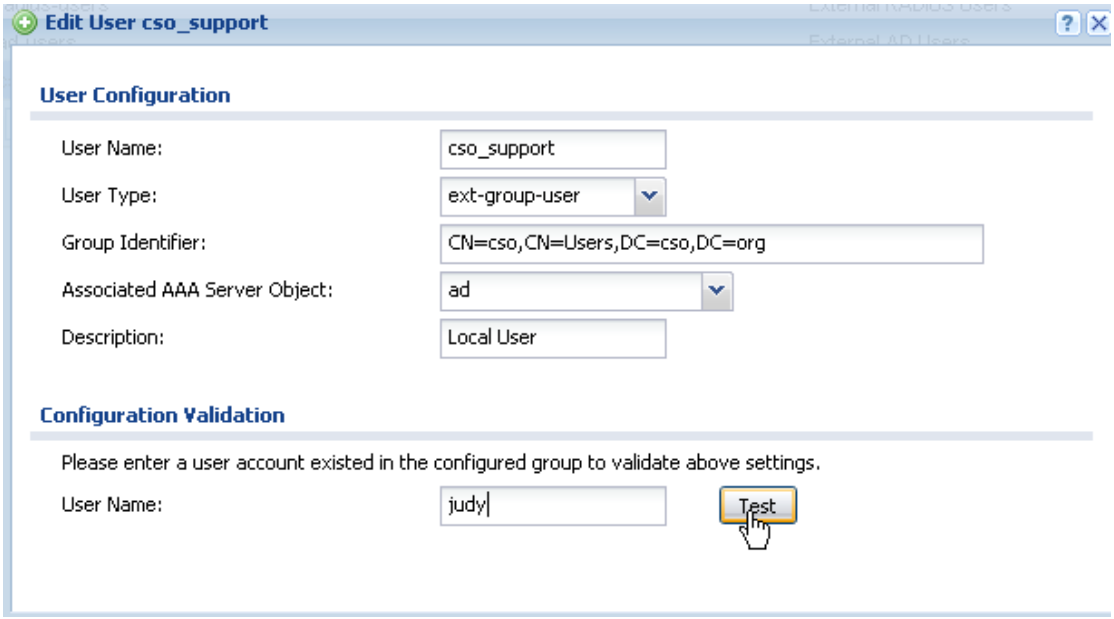
CN=<cso>,CN=Users,DC=<cso>,DC=<org>

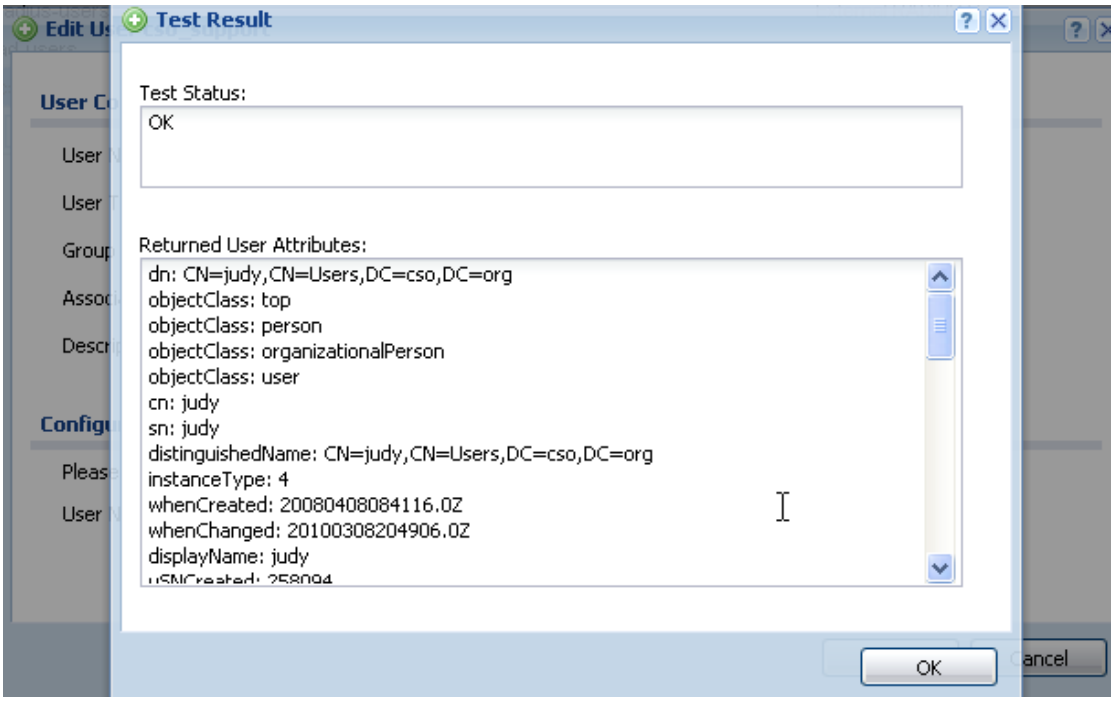
<cso> is the group name on the AD server.

Add group “cso”:

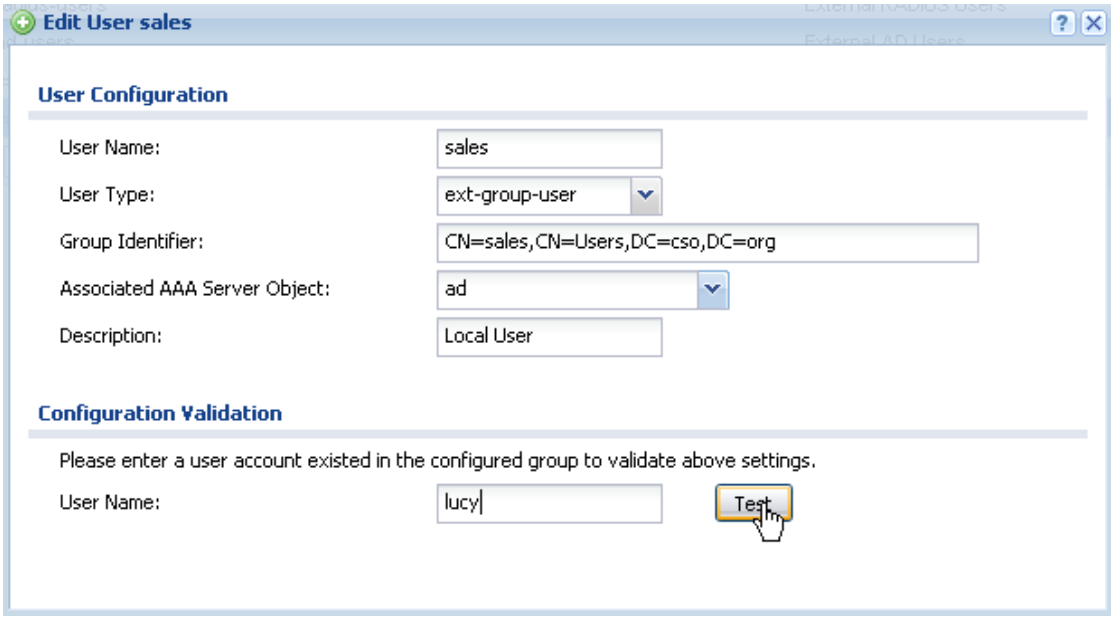


You can verify whether a user is in this group.

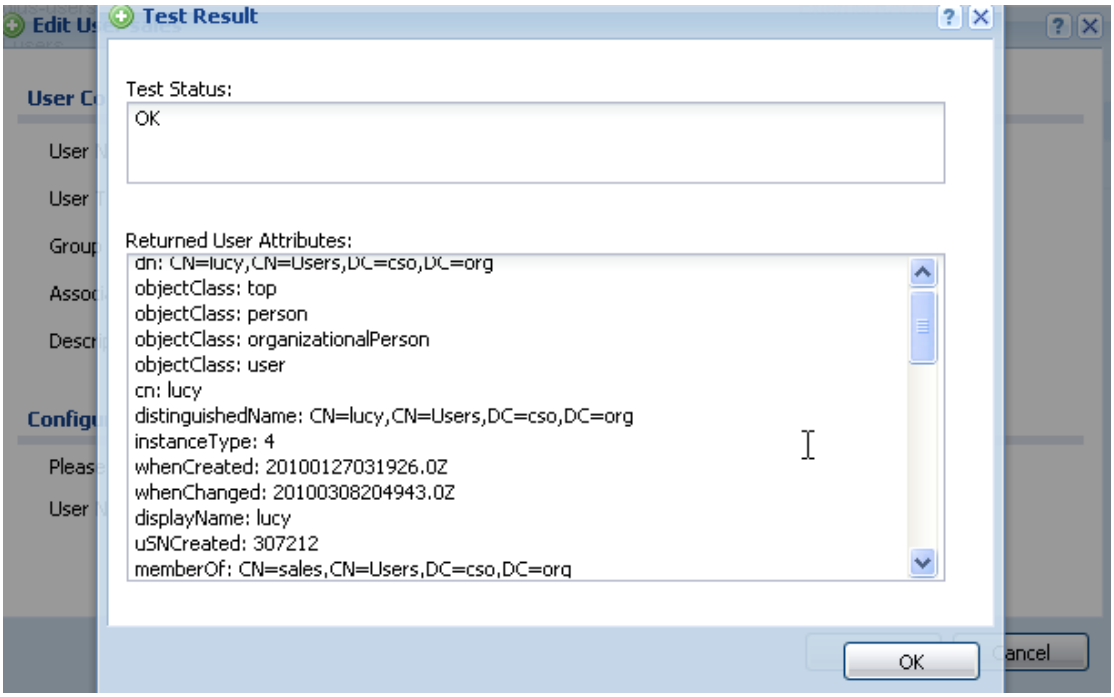




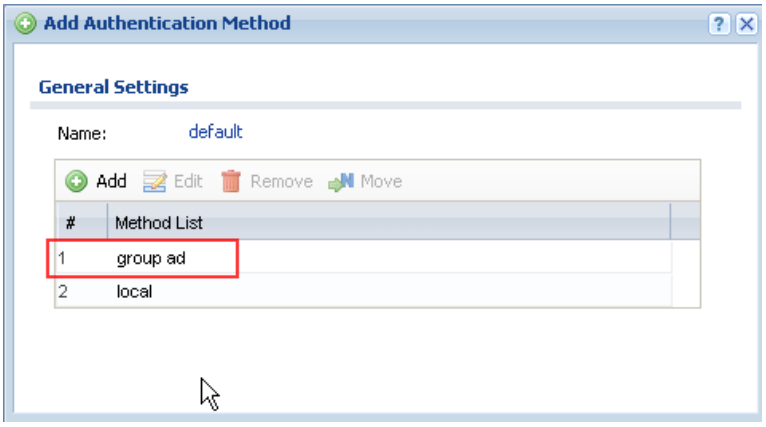
Add group “sales”:



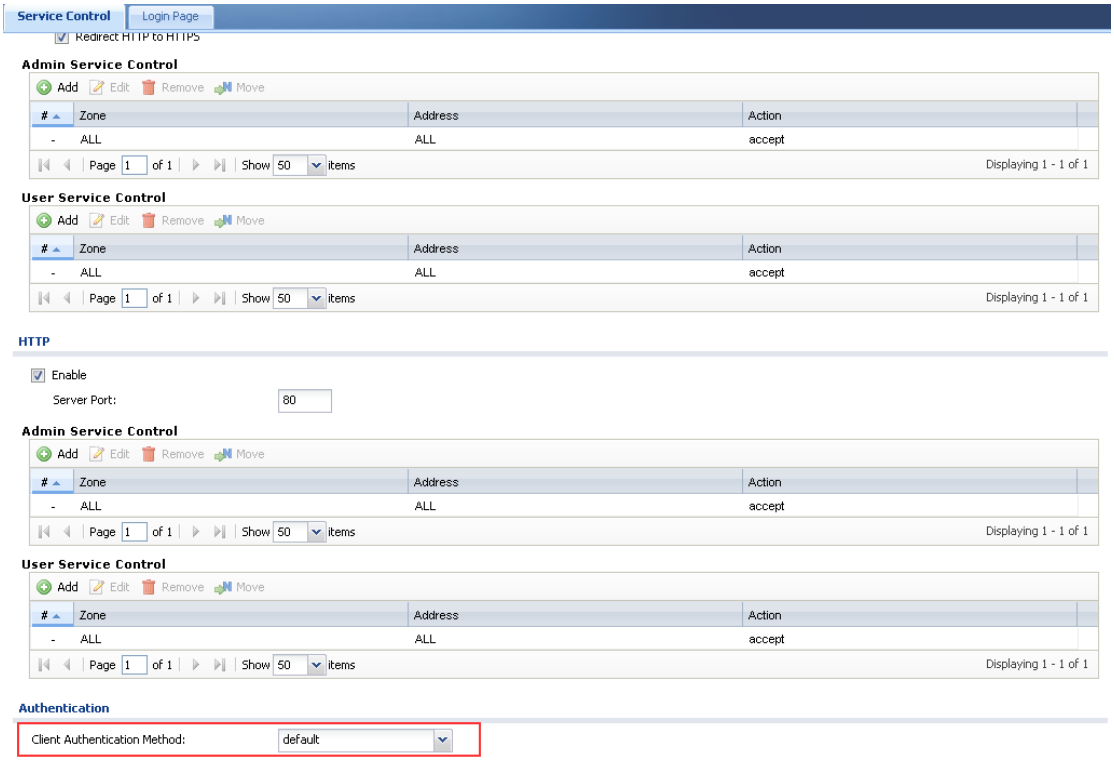
You can verify whether a user is in the group “sales”.



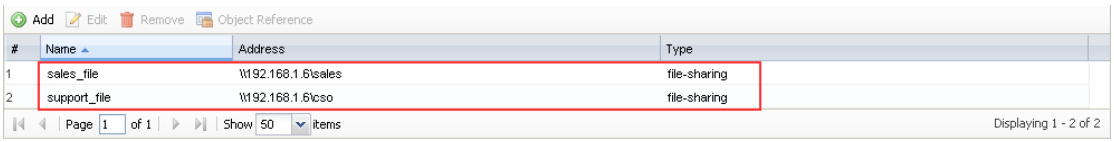
Step4. Go to Configuration > Object >Auth. Method, modify the authentication method of “default”. Add “group ad”.



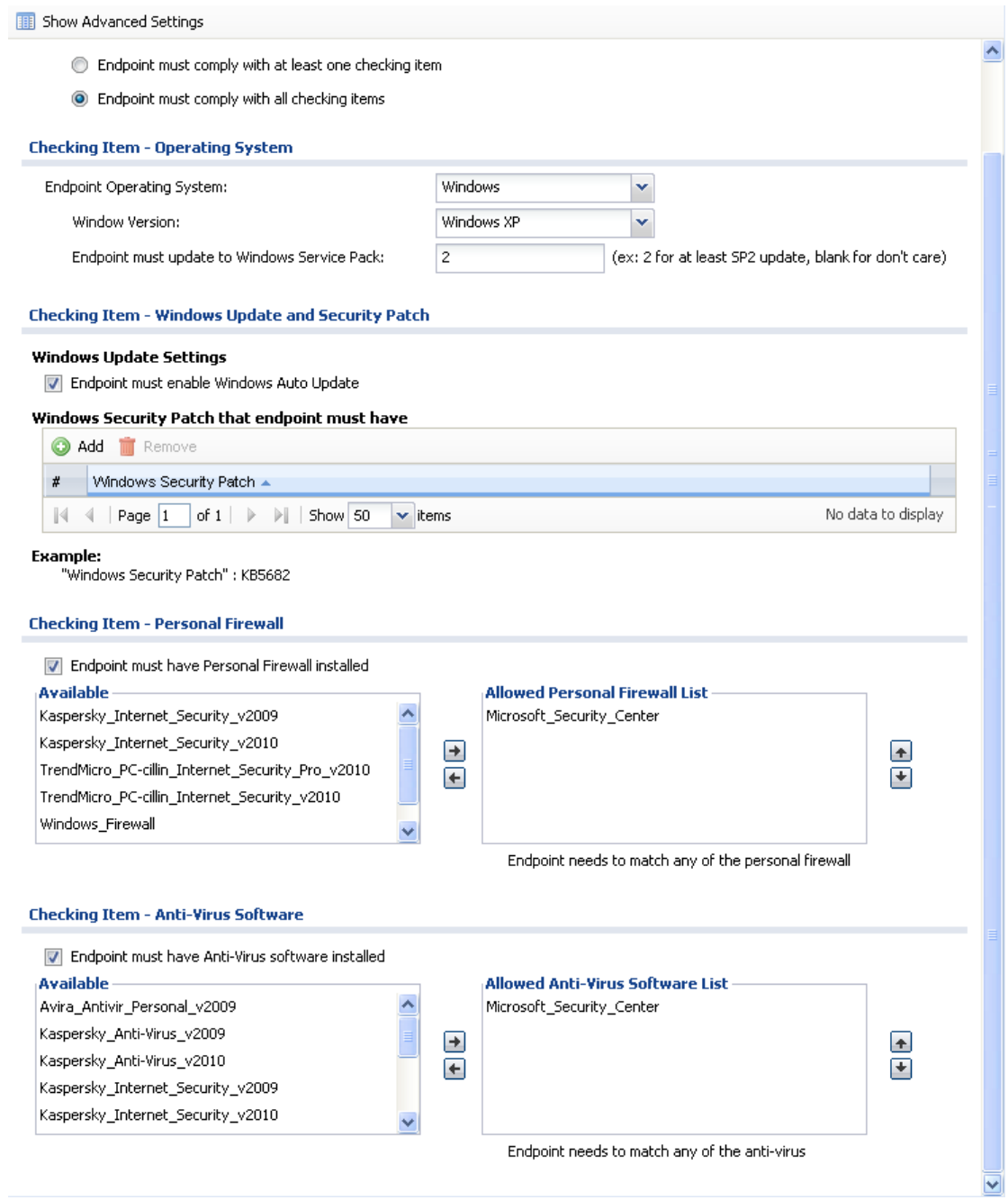
Step5. Go to Configuration > System > WWW > Service Control. In the “Authentication” part, make sure the “Client Authentication Method” is chosen as “default”.



Step6. Go to Configuration > Object > SSL Application, add applications for the support and sales group.



Step7. Go to Configuration > Object > Endpoint Security, add EPS policy for checking the sales group.



Step8. Go to Configuration > VPN >SSL VPN > Access Privilege, add two SSL VPN rules for cso_support and sales.

Create new Object

Enable Policy

Name: for_cso

Join SSL_VPN Zone

Description: New Create (Optional)

Clean browser cache when user logs out

User/Group

Selectable User/Group Objects
=== Object ===
admin
ldap-users
radius-users
ad-users

Selected User/Group Objects
=== Object ===
cso_support

Endpoint Security (EPS)

Enable EPS Checking

Periodical checking time 1 (1-1440 minutes)

Selectable EPS Objects
ssl_check

Selected EPS Objects

Endpoint needs to match at least one EPS object.

SSL Application List (Optional)

Selectable Application Objects
sales_file

Selected Application Objects
support_file

Network Extension (Optional)

Enable Network Extension

Assign IP Pool: Please select one ...

DNS Server 1: none

DNS Server 2: none

WINS Server 1: none

WINS Server 2: none

Network List

Selectable Address Objects
LAN1_SUBNET
LAN2_SUBNET
EXT_WLAN_SUBNET
DMZ_SUBNET
WLAN-1-1_SUBNET

Selected Address Objects

Create new Object

Configuration

Enable Policy

Name: for_sales

Join SSL_VPN Zone

Description: New Create (Optional)

Clean browser cache when user logs out

User/Group

Selectable User/Group Objects
=== Object ===
admin
ldap-users
radius-users
ad-users

Selected User/Group Objects
=== Object ===
sales

Endpoint Security (EPS)

Enable EPS Checking

Periodical checking time 1 (1-1440 minutes)

Selectable EPS Objects

Selected EPS Objects
ssl_check

Endpoint needs to match at least one EPS object.

SSL Application List (Optional)

Selectable Application Objects
support_file

Selected Application Objects
sales_file

Network Extension (Optional)

Enable Network Extension

Assign IP Pool: Please select one ...

DNS Server 1: none

DNS Server 2: none

WINS Server 1: none

WINS Server 2: none

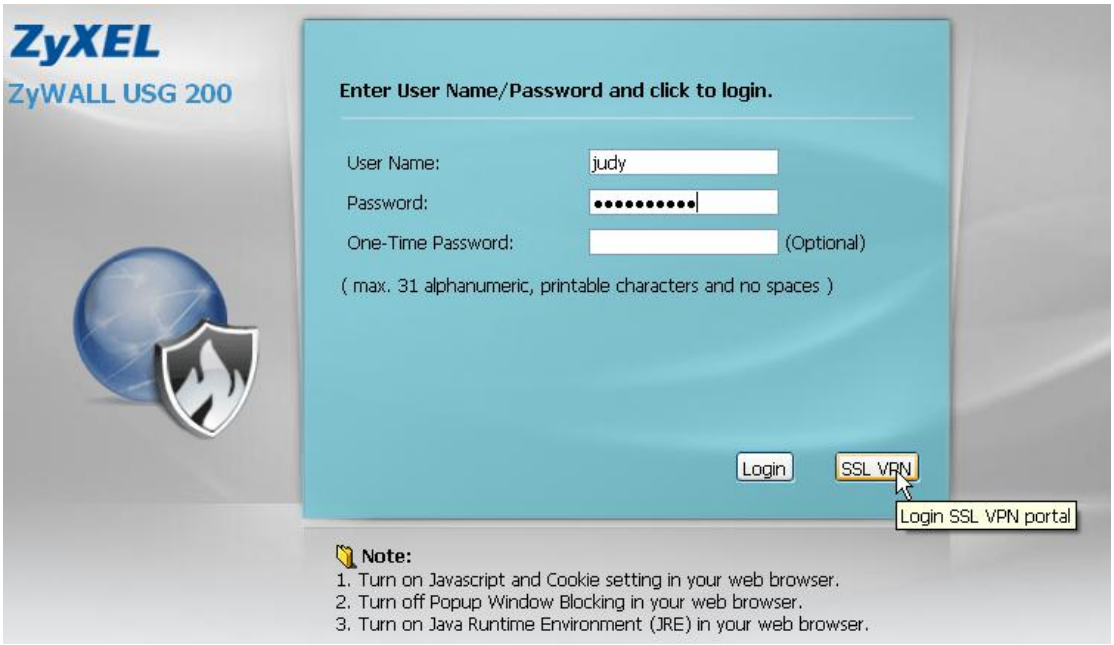
Network List

Selectable Address Objects
LAN1_SUBNET
LAN2_SUBNET
EXT_WLAN_SUBNET
DMZ_SUBNET
WLAN-1-1_SUBNET

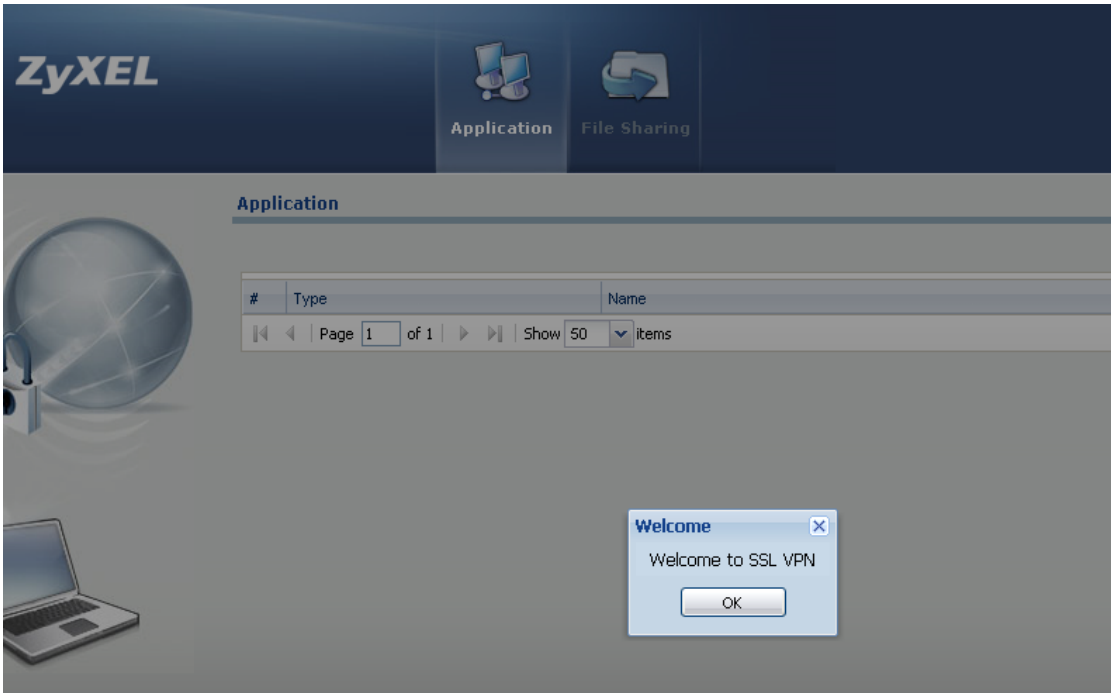
Selected Address Objects

2.4.3.Scenario Verification

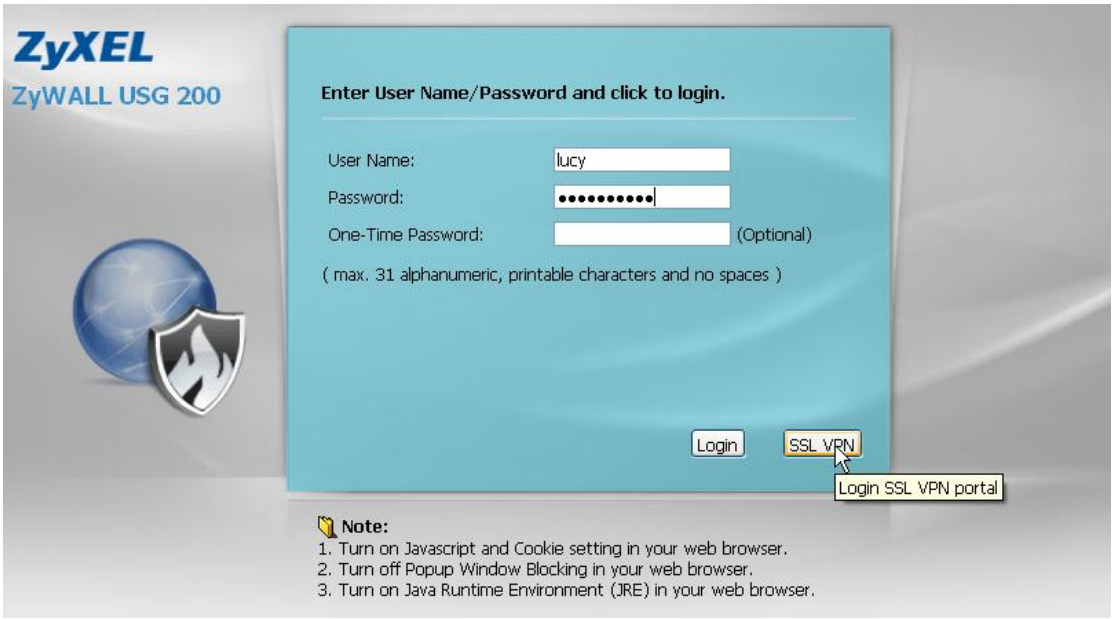
Open the USG login page. Make sure Java is installed and enabled on your browser. Use a user “judy” in the group “cso” to login SSL VPN.

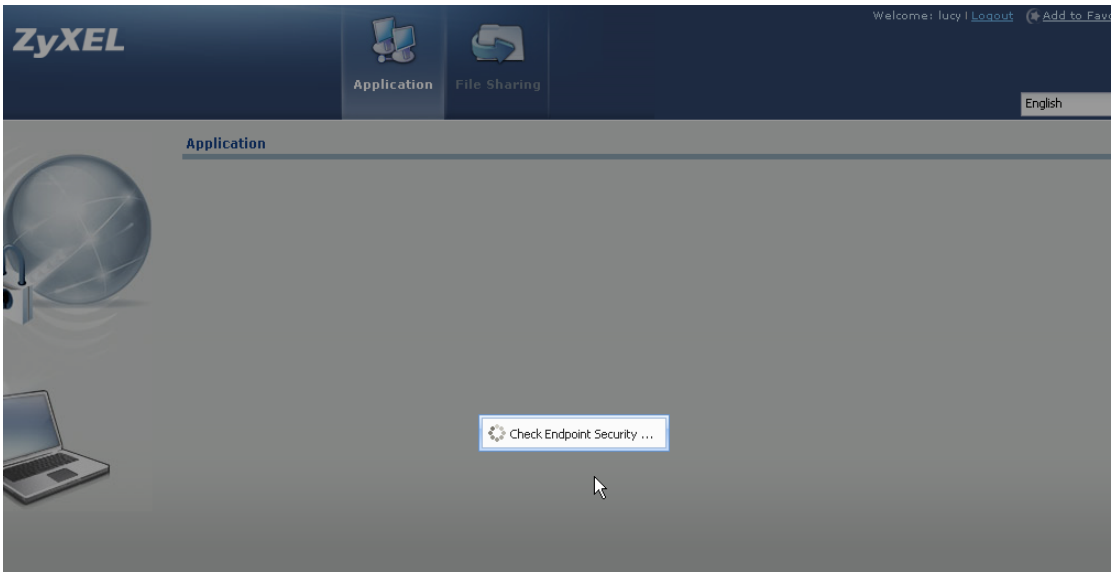


SSL VPN is established, and you can see the fileshare on the portal is for the group AD user “cso”.

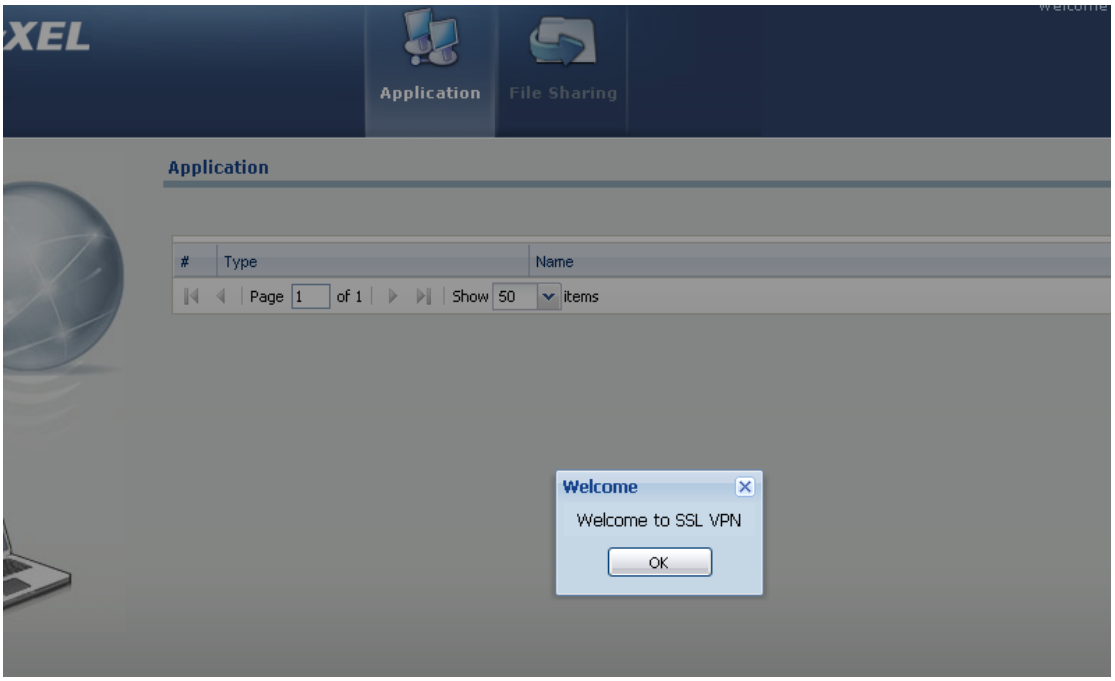


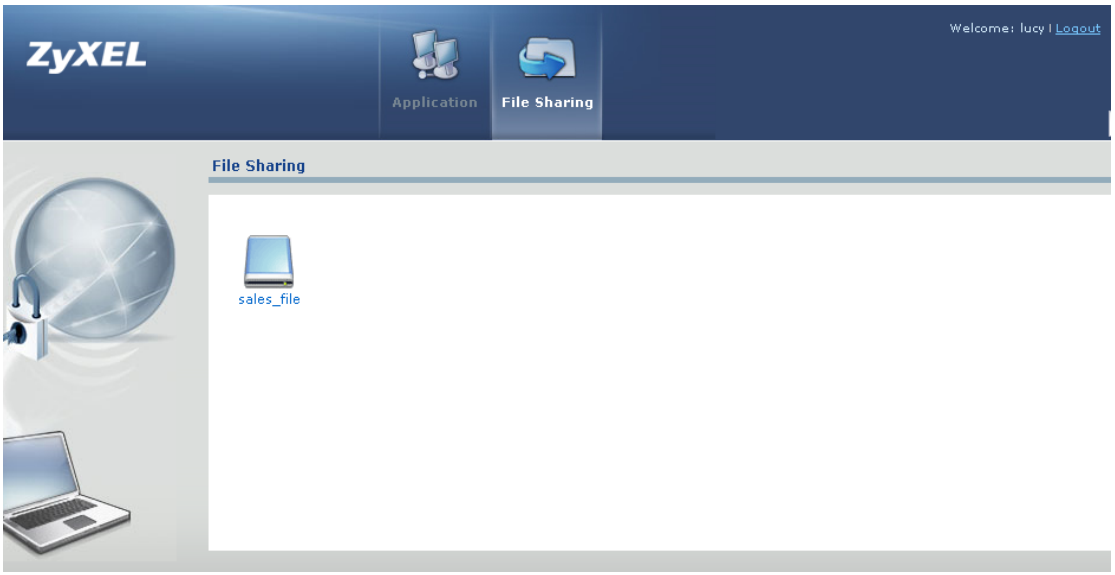
Use a user “lucy” in the group “sales” to login SSL VPN.





SSL VPN is established, and you can see the fileshare on the portal is for the group AD user “sales”.





3. VoIP Application with USG

VoIP (Voice over Internet Protocol) is transportation of voice traffic using the Internet Protocol (IP). It's a cost-effective substitute of PSTN, and nowadays is more and more popular used in Enterprises. However, SIP VoIP is an NAT unfriendly application. USG with its ALG function is compatible with most popular VoIP devices in varies scenarios.

3.1. VoIP Support Device List

The table below lists the USG supported VoIP devices. The devices in the list are compatible with USG SIP ALG when used in NAT scenario, and they are also compatible with USG SIP when they are use in Bandwidth Management applications.

SIP Phone	Version	SIP ALG(PASS/FAIL)	AppPatrol SIP BWM(PASS/FAIL)
Windows Messenger	5.1(5.1.0715)	Pass	Pass
Softphone V100	1.1.89.69.01	Pass	Pass
Softphone V120	1.1.96.69.00	Pass	Pass
V300-T1	1.10(AOW.0)	Pass	Pass
V500-T1	1.10(AOX.0)	Pass	Pass
Click-To-Talk	v1.0.101.69.01	Pass	Pass
Snom820-SIP		Pass	Pass
Linksys SPA-3000		Pass	Pass
Cisco IP Phone 7940	POS3-04-4-00	Pass	Pass
GogoTalk	1.54	Pass	Pass
3CXPhone	1.17	Pass	Pass
X-Lite	3.0 build 29712	Pass	Pass
SJphone	1.65	Pass	Pass
Aastra 6731i	2.5.1.2000	Pass	Pass
Aastra 57i	2.1.0.2145	Pass	Pass
ZyXEL X2002 / X6004	1.11(AVA.0)b2	Pass	Pass

3.2. VoIP in NAT Scenario

SIP VoIP in nature is an NAT unfriendly application, since it uses a different port for the RTP traffic (voice stream) other than the session initiation port which is by default uses UDP 5060.

There're currently the following solutions to solve the SIP and NAT incompatibility issue.

- SIP ALG on the NAT gateway
- STUN
- Outbound Proxy
- Solutions in SIP client devices (such as Use NAT in ZyXEL VoIP clients)

USG ZyWALL supports SIP ALG. Network administrator just needs to enable SIP ALG on the ZyWALL. Then he can deploy VoIP solutions in various NAT scenarios, no matter the SIP server is in the internet, or in the local network.

3.2.1. SIP Server on the Internet

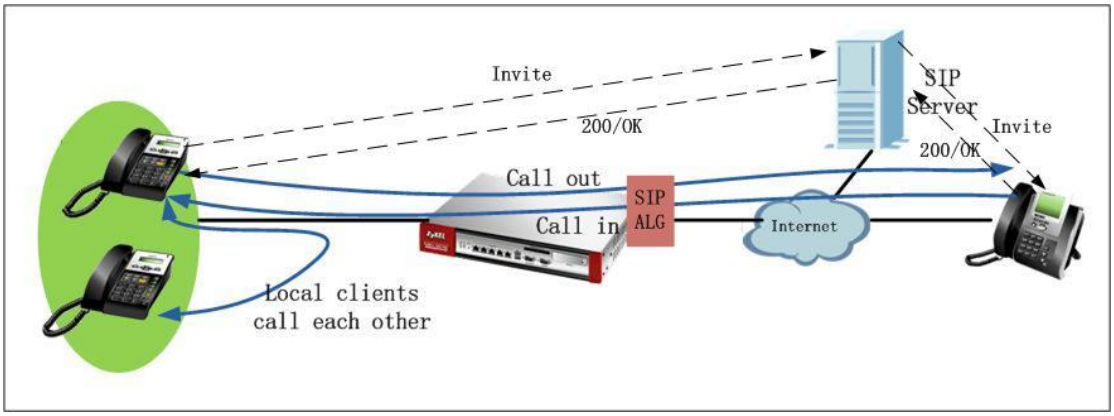
3.2.1.1. Application Scenario

In the scenario below, the SIP server is on the Internet. There're SIP clients both in the USG local network, and on the internet side. All the clients are registered to the SIP server. We want all the clients can call each other:

The local clients can call out to the clients on the Internet.

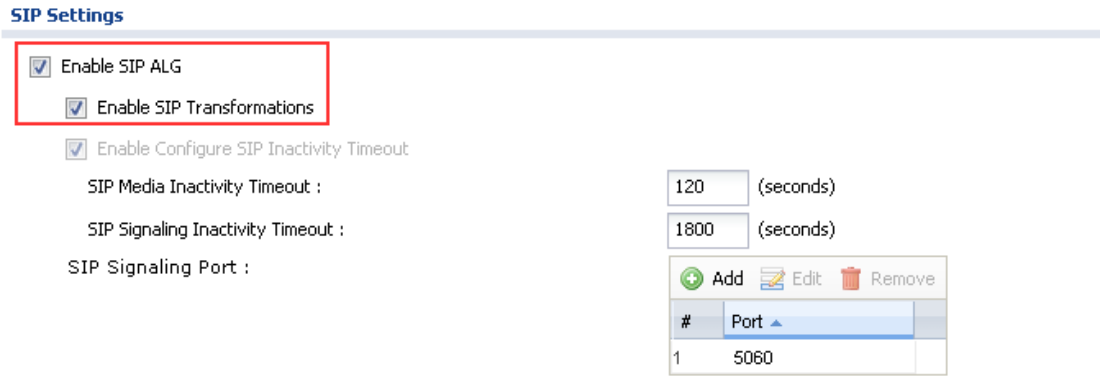
The Internet clients can call in the local clients.

The local clients also can call each other.



3.2.1.2. Configuration Steps

You just need to enable SIP ALG on the USG ZyWALL to make this scenario work. Go to Configuration > Network > ALG, enable SIP ALG, and also please make sure to enable SIP Transformations.

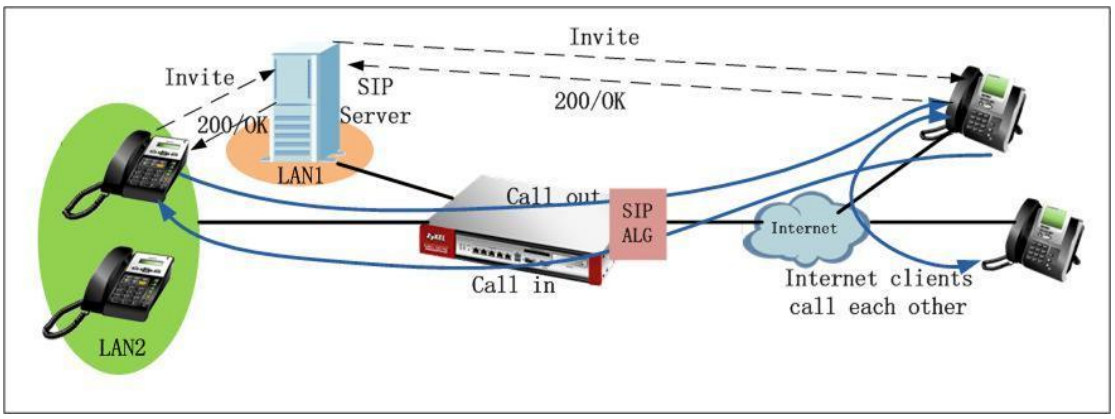


After this setting is done, register all the clients to the Internet SIP server, then all the clients can call each other, no matter they're in the local network, or in the Internet.

3.2.2.SIP Server on the Local Network

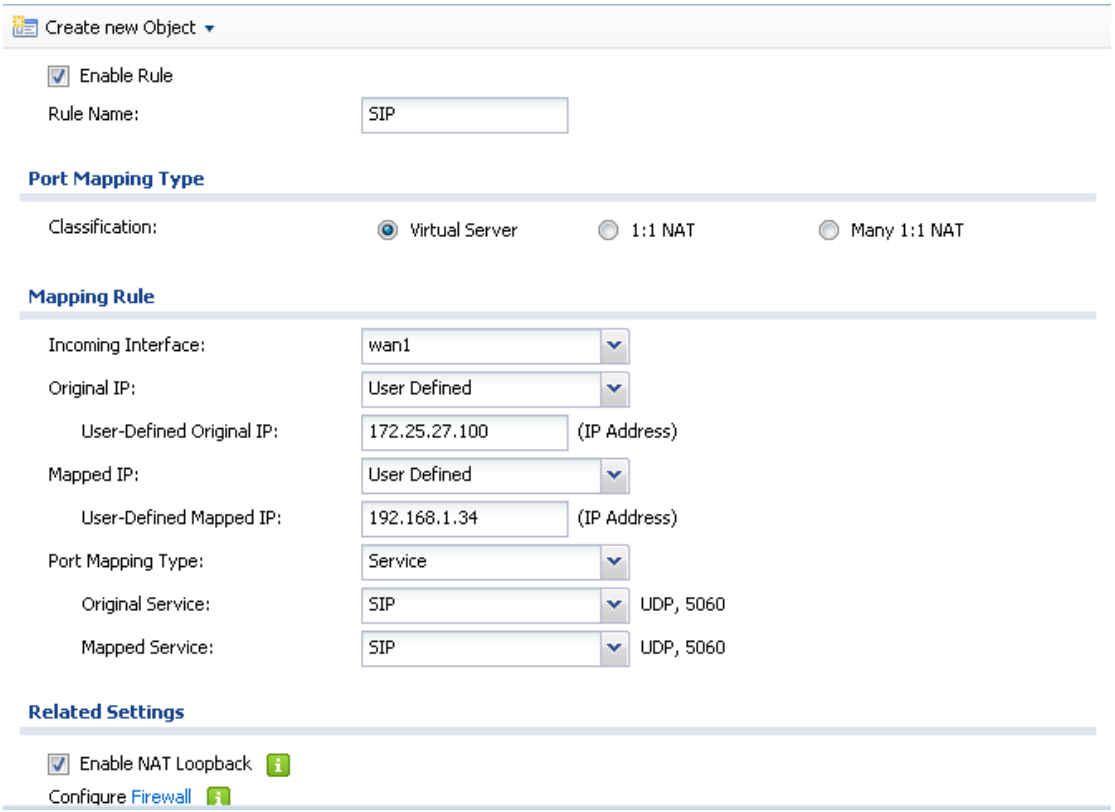
3.2.2.1. Application Scenario

In the scenario below, the SIP server is on the local network. There're SIP clients both in the USG local network, and on the internet side. All the clients are registered to the SIP server. We want all the clients can call each other:
The local clients can call out to the clients on the Internet.
The Internet clients can call in the local clients.
The Internet clients can call each other.
The local clients can call each other.

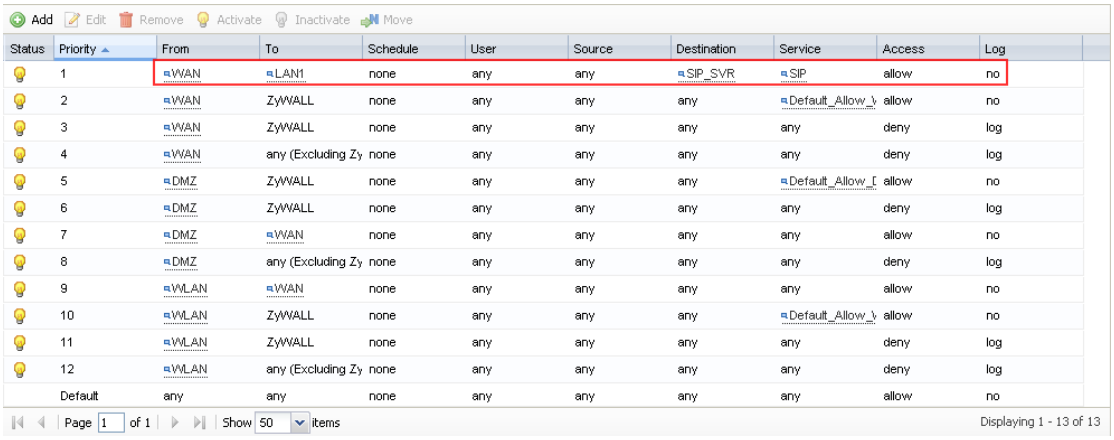


3.2.2.2. Configuration Steps

Step1. Go to Configuration > Network > NAT, add one NAT rule to map the SIP traffic to the local SIP server.

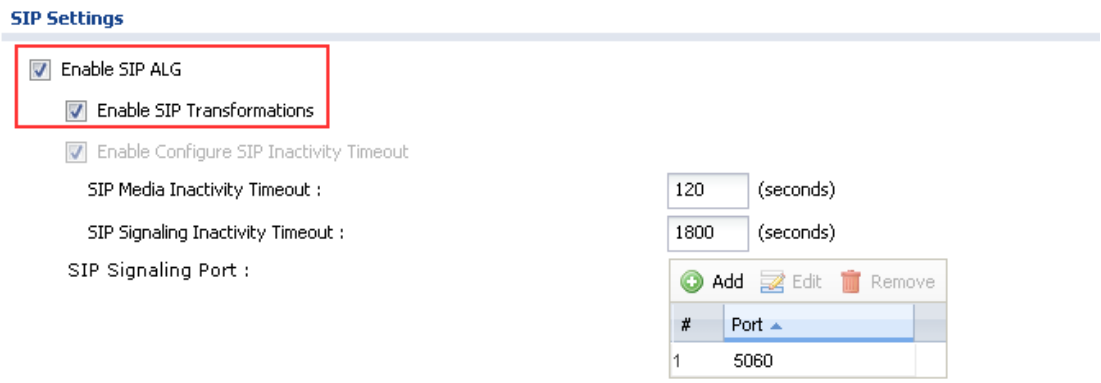


Step2. Go to Configuration>Firewall, add one firewall rule to allow the SIP traffic from WAN to the local SIP server.



Status	Priority	From	To	Schedule	User	Source	Destination	Service	Access	Log
	1	WAN	LAN1	none	any	any	SIP_SVR	SIP	allow	no
	2	WAN	ZyWALL	none	any	any	any	Default_Allow_V	allow	no
	3	WAN	ZyWALL	none	any	any	any	any	deny	log
	4	WAN	any (Excluding Zy	none	any	any	any	any	deny	log
	5	DMZ	ZyWALL	none	any	any	any	Default_Allow_D	allow	no
	6	DMZ	ZyWALL	none	any	any	any	any	deny	log
	7	DMZ	WAN	none	any	any	any	any	allow	no
	8	DMZ	any (Excluding Zy	none	any	any	any	any	deny	log
	9	WLAN	WAN	none	any	any	any	any	allow	no
	10	WLAN	ZyWALL	none	any	any	any	Default_Allow_V	allow	no
	11	WLAN	ZyWALL	none	any	any	any	any	deny	log
	12	WLAN	any (Excluding Zy	none	any	any	any	any	deny	log
	Default	any	any	none	any	any	any	any	allow	no

Step3. Go to Configuration > Network > ALG, enable SIP ALG, and also please make sure to enable SIP Transformations.



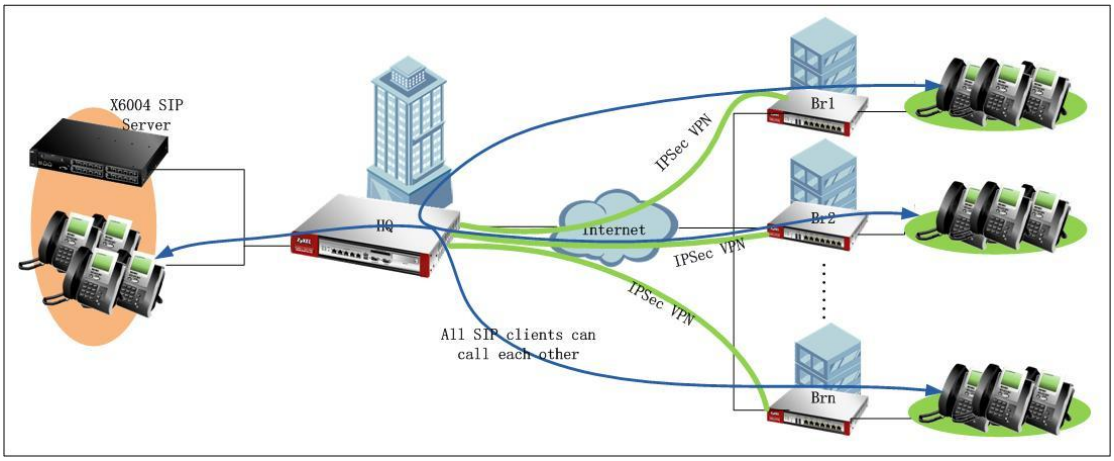
After all these settings are done, all the clients can register to the local SIP server, and all the clients can call each other, no matter they're in the local network, or in the Internet.

3.3. VoIP in VPN Scenario

3.3.1. Application Scenario

In the scenario below, X6004 is placed in the local network of HQ. There're SIP clients in HQ local network, as well as in the branch offices' local networks. SIP clients want to register to the SIP server (X6004) securely through IPSec VPN tunnels. They also want to make calls to each other securely through VPN tunnels. No matter

they're in the HQ local network, or in the branch office networks. To meet the requirements, all the branch offices should build IPSec VPN tunnels to the HQ USG. Also to enable branch offices' SIP clients can call each other via VPN tunnels, the network administrator should also create IPSec VPN concentrator to include all the VPN tunnels built with branch offices.



3.3.2.Configuration Steps

IP address information on the HQ USG and branch USG:

HQ USG:
WAN IP: 172.25.27.140
LAN1 subnet: 192.168.1.0/24
X6004 IP: 192.168.1.33

Branch office 1(Br1) USG:
WAN IP: 172.25.27.90
LAN1 subnet: 192.168.4.0/24

Branch office 2 (Br2) USG:
WAN IP: 172.25.27.39
LAN1 subnet: 192.168.5.0/24

On HQ USG:

Step1. Go to Monitor > System Status > Interface Status, check interface IP information.

Name	Port	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Action
wan1	P1	100M/Full	n/a	WAN	172.25.27.140 / 255.255.255.0	DHCP client	n/a	Renew
wan1_ppp	P1	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wan2	P2	Down	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew
wan2_ppp	P2	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
opt	P3	Down	n/a	OPT	0.0.0.0 / 0.0.0.0	Static	n/a	n/a
opt_ppp	P3	Inactive	n/a	OPT	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
lan1	P4, P5, P6	Up	n/a	LAN1	192.168.1.1 / 255.255.255.0	Static	DHCP server	n/a
lan2	n/a	Down	n/a	LAN2	192.168.2.1 / 255.255.255.0	Static	DHCP server	n/a
ext-wlan	n/a	Down	n/a	WLAN	10.59.0.1 / 255.255.255.0	Static	DHCP server	n/a
dmz	P7	Down	n/a	DMZ	192.168.3.1 / 255.255.255.0	Static	DHCP server	n/a
aux	aux	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wlan-1	n/a	n/a	n/a	n/a	n/a / n/a	n/a	n/a	n/a
wlan-1-1	n/a	Down	n/a	WLAN	10.59.1.1 / 255.255.255.0	static	n/a	n/a

Step2. Go to Configuration > Object > Address, add address objects for Br1 local subnet and Br2 local subnet for later use in IPSec VPN configuration.

Add Edit Remove Object Reference

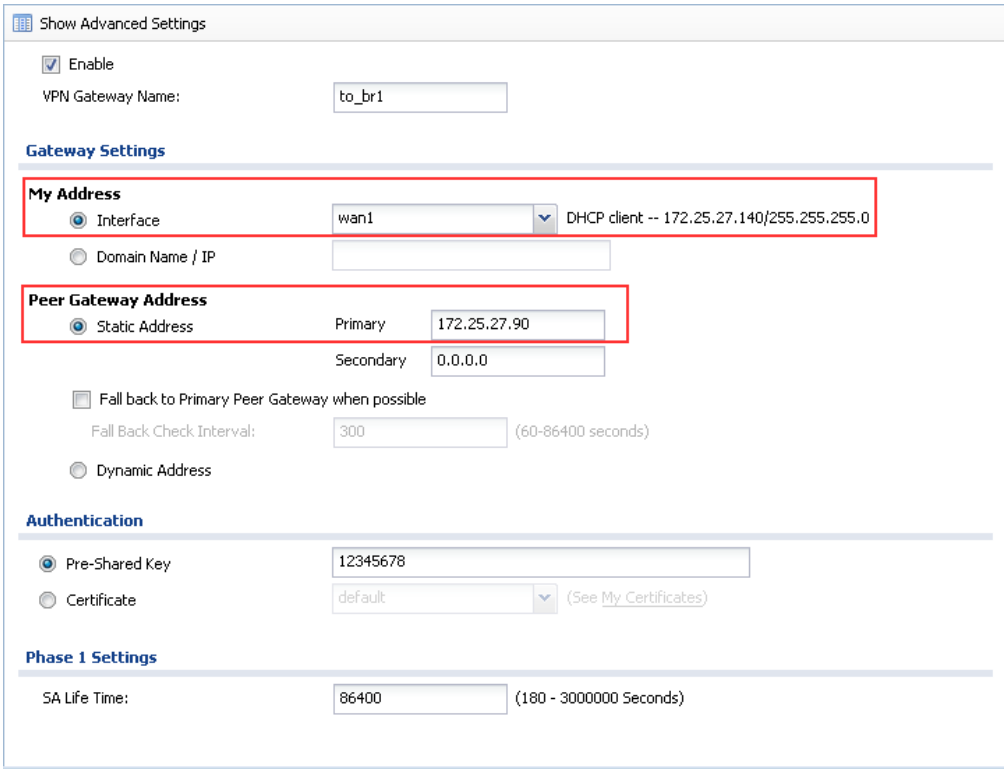
#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	EXT_WLAN_SUBNET	INTERFACE SUBNET	ext-wlan-10.59.0.0/24
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
5	WLAN-1-1_SUBNET	INTERFACE SUBNET	wlan-1-1-10.59.1.0/24
6	subnet_br1	SUBNET	192.168.4.0/24
7	subnet_br2	SUBNET	192.168.5.0/24

Page 1 of 1 Show 50 items Displaying 1 - 7 of 7

Step3. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add VPN phase1 rules for tunnels to Br1 and Br2.

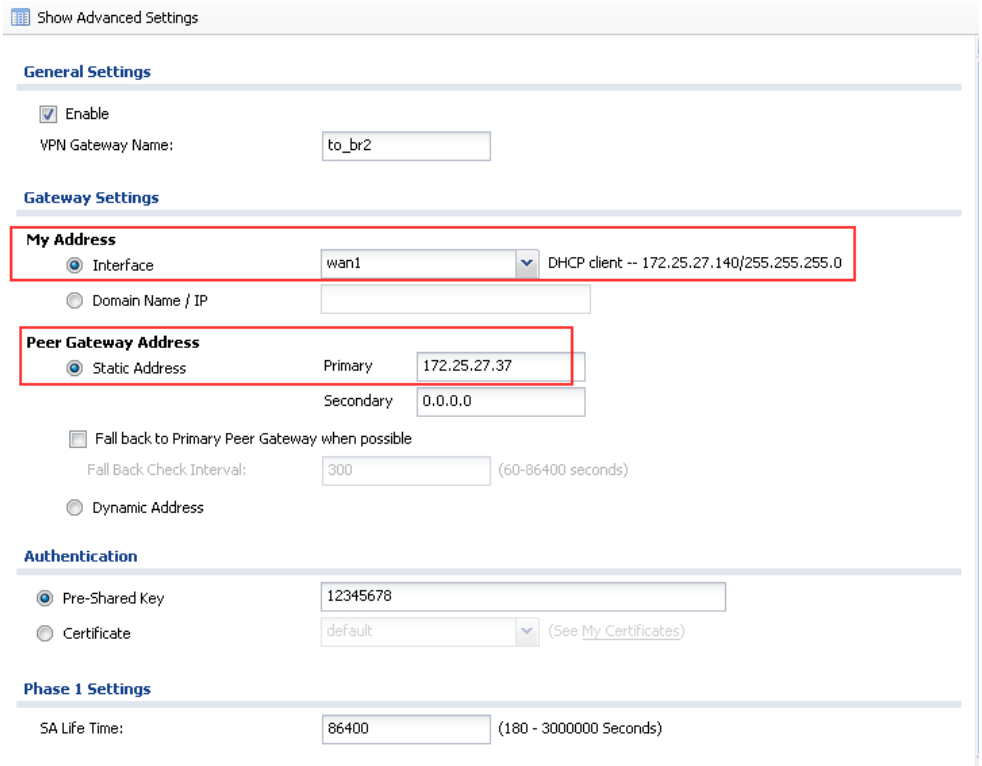
To Br1:

My Address: WAN1 IP (172.25.27.140)
Peer Gateway Address: Br1 WAN IP (172.25.27.90)



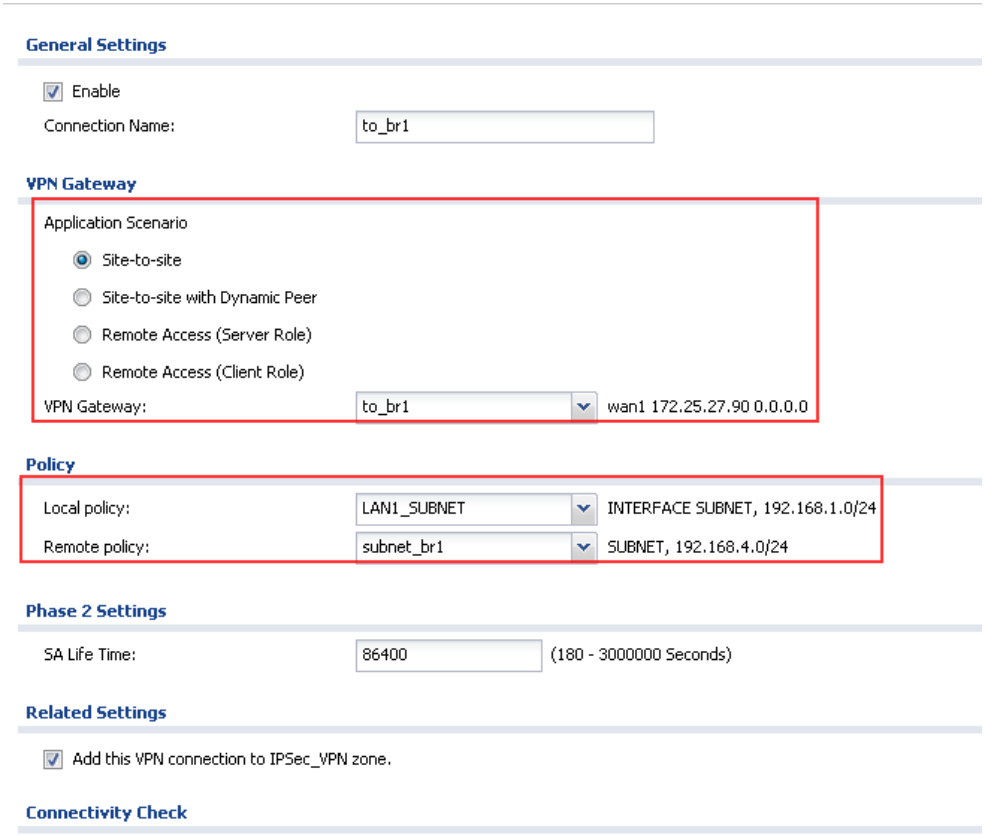
To Br2:

My Address: WAN1 IP (172.25.27.140)
Peer Gateway Address: Br2 WAN IP (172.25.27.37)



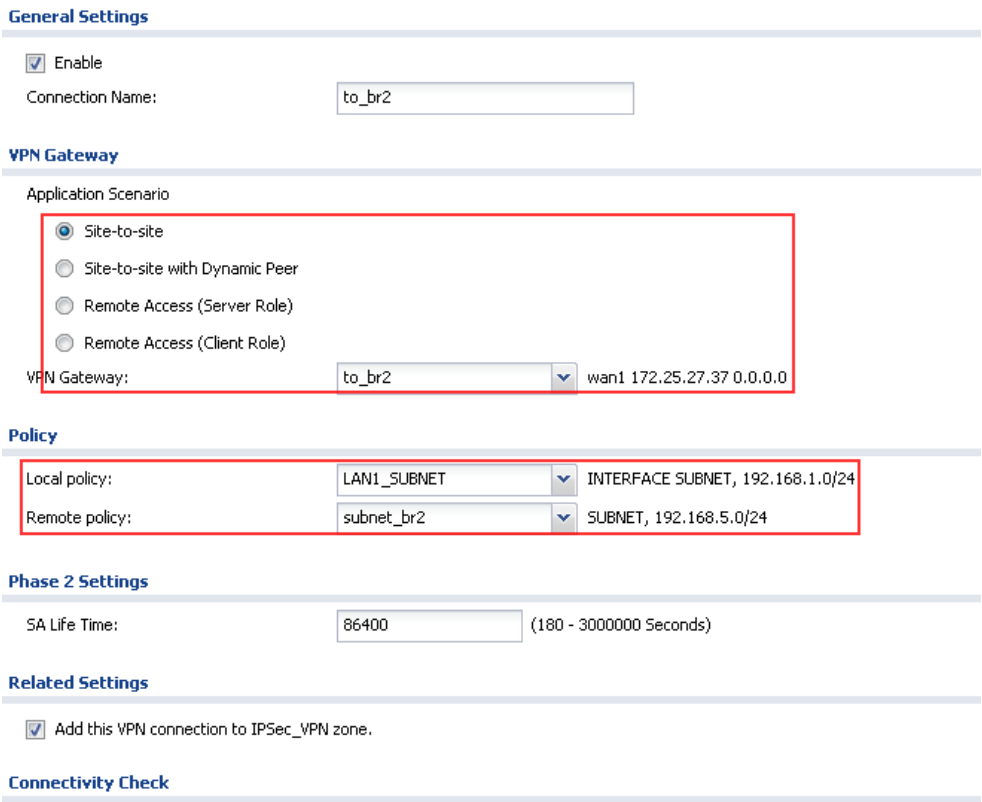
Step4. Go to Configuration > VPN > IPSec VPN > VPN Connection, add VPN phase2 rules to Br1 and Br2.

To Br1:
Local policy: local LAN1 subnet (192.168.1.0/24)
Remote policy: Br1 local subnet (192.168.4.0/24)



To Br2:

Local policy: local LAN1 subnet (192.168.1.0/24)
Remote policy: Br2 local subnet (192.168.5.0/24)



Step5. Go to Configuration > VPN > IPSec VPN > Concentrator, create on VPN concentrator. This concentrator should include all the IPSec VPN tunnels to branch offices.

Step6. Go to Configuration > Network > Zone. By default, Block Intra-zone is enabled for IPSec VPN zone. We should disable it.

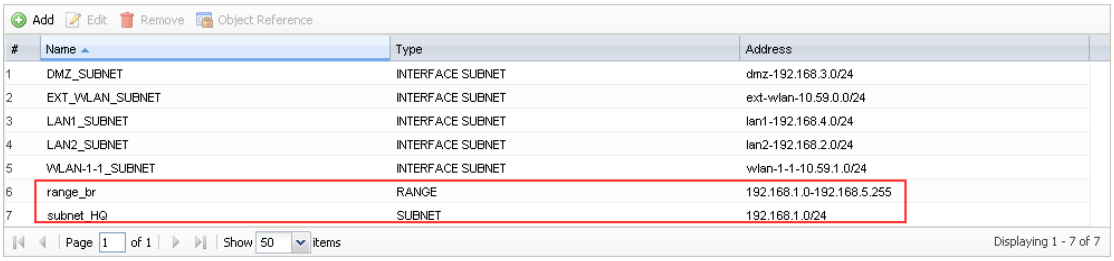
In ZLD v2.20, routing for VPN traffic is automatically created according the VPN phase2 local and remote policy. So we don't need to add any policy routes for the traffic from HQ local subnet to the branch office subnets.

On Br1

Step1. Go to Monitor > System Status > Interface Status, check the interface IP information for later use in IPSec VPN configuration.

Name	Port	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Action
wan1	P1	100M/Full	n/a	WAN	172.25.27.90 / 255.255.255.0	DHCP client	n/a	Renew
wan1_ppp	P1	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wan2	P2	Down	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew
wan2_ppp	P2	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
lan1	P3, P4	Down	n/a	LAN1	192.168.4.1 / 255.255.255.0	Static	DHCP server	n/a
lan2	P5	Down	n/a	LAN2	192.168.2.1 / 255.255.255.0	Static	DHCP server	n/a
ext-wlan	P6	Down	n/a	WLAN	10.59.0.1 / 255.255.255.0	Static	DHCP server	n/a
dmz	P7	Down	n/a	DMZ	192.168.3.1 / 255.255.255.0	Static	DHCP server	n/a
aux	aux	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wlan-1	n/a	n/a	n/a	n/a	n/a / n/a	n/a	n/a	n/a
wlan-1-1	n/a	Down	n/a	WLAN	10.59.1.1 / 255.255.255.0	static	n/a	n/a

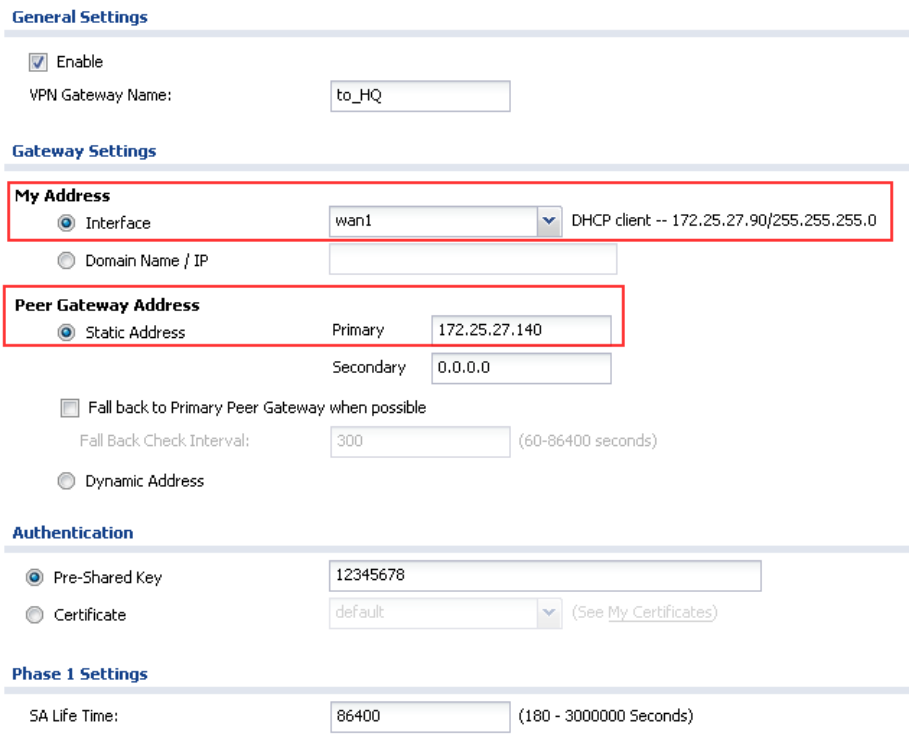
Step2. Go to Configuration > Object > Address, add HQ local subnet address object for later IPSec VPN configuration use. And a range address object for later use in Policy Route configuration to route traffic to all other branch offices' local networks to VPN tunnels. This range object should cover all the branch offices' local subnets. In this case we create it as 192.168.1.0~192.168.5.255.



Step3. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add VPN phase1 rule to build tunnel to HQ.

My Address: WAN1 IP (172.25.27.90)

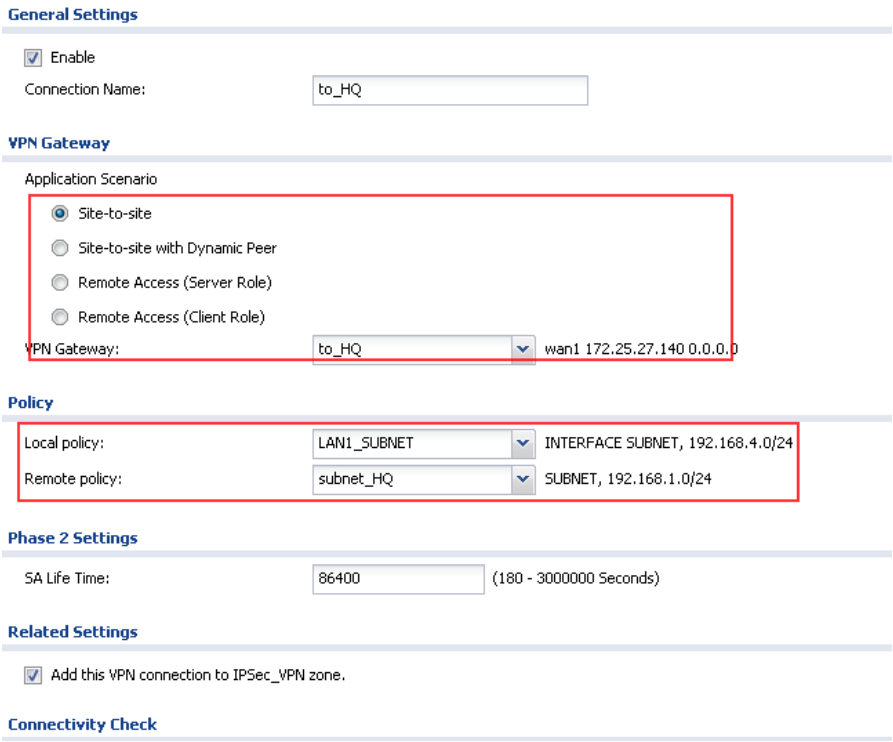
Peer Gateway Address: HQ WAN IP (172.25.27.140)



Step4. Go to Configuration > VPN > IPSec VPN > VPN Connection, add VPN phase2 rule to build tunnel to HQ.

Local policy: local LAN1 subnet (192.168.4.0/24)

Remote policy: HQ local subnet (192.168.1.0/24)



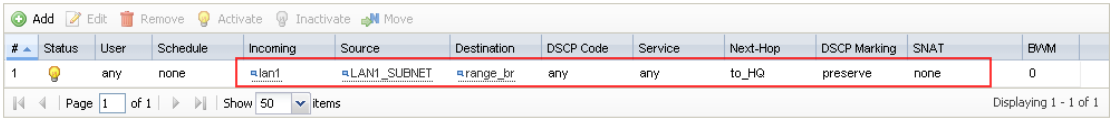
Step5. Go to Configuration > Network > Routing>Policy Route, add a policy route rule to route traffic from local subnets to all branch offices to IPSec VPN tunnel to_HQ.

Incoming interface: LAN1

Source: LAN1_Subnet (192.168.4.0/24)

Destination: range_br(192.168.1.0~192.168.5.255)

Next Hop: VPN tunnel to_HQ



On Br2

Step1. Go to Monitor > System Status > Interface Status, check the interface IP information for later use in IPSec VPN configuration.

Name	Port	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Action
wan1	P1	100M/Full	n/a	WAN	172.25.27.37 / 255.255.255.0	DHCP client	n/a	Renew
wan1_ppp	P1	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wan2	P2	Down	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew
wan2_ppp	P2	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
opt	P3	Down	n/a	OPT	0.0.0.0 / 0.0.0.0	Static	n/a	n/a
opt_ppp	P3	Inactive	n/a	OPT	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
lan1	P4, P5	Up	n/a	LAN1	192.168.5.1 / 255.255.255.0	Static	DHCP server	n/a
lan2	n/a	Down	n/a	LAN2	192.168.2.1 / 255.255.255.0	Static	DHCP server	n/a
ext-wlan	P6	Down	n/a	WLAN	10.59.0.1 / 255.255.255.0	Static	DHCP server	n/a
dmz	P7	Down	n/a	DMZ	192.168.3.1 / 255.255.255.0	Static	DHCP server	n/a
aux	aux	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wlan-1	n/a	n/a	n/a	n/a	n/a / n/a	n/a	n/a	n/a
wlan-1-1	n/a	Down	n/a	WLAN	10.59.1.1 / 255.255.255.0	static	n/a	n/a

Step2. Go to Configuration > Object > Address, add HQ local subnet address object for later IPSec VPN configuration use. And a range address object for later use in Policy Route configuration to route traffic to all other branch offices' local networks to VPN tunnels. This range object should cover all the branch offices' local subnets. In this case we create it as 192.168.1.0~192.168.5.255.

Add Edit Remove Object Reference

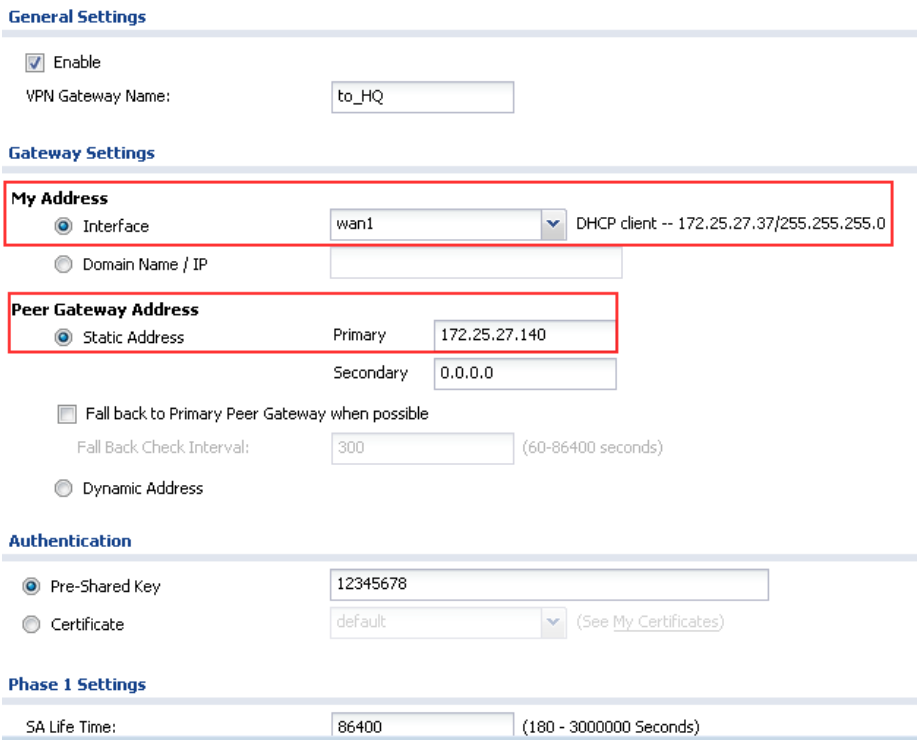
#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	EXT_WLAN_SUBNET	INTERFACE SUBNET	ext-wlan-10.59.0.0/24
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.5.0/24
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
5	WLAN-1-1_SUBNET	INTERFACE SUBNET	wlan-1-1-10.59.1.0/24
6	range_br	RANGE	192.168.1.0-192.168.5.255
7	subnet_HQ	SUBNET	192.168.1.0/24

Page 1 of 1 Show 50 items Displaying 1 - 7 of 7

Step3. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add VPN phase1 rule to build tunnel to HQ.

My Address: WAN1 IP (172.25.27.37)

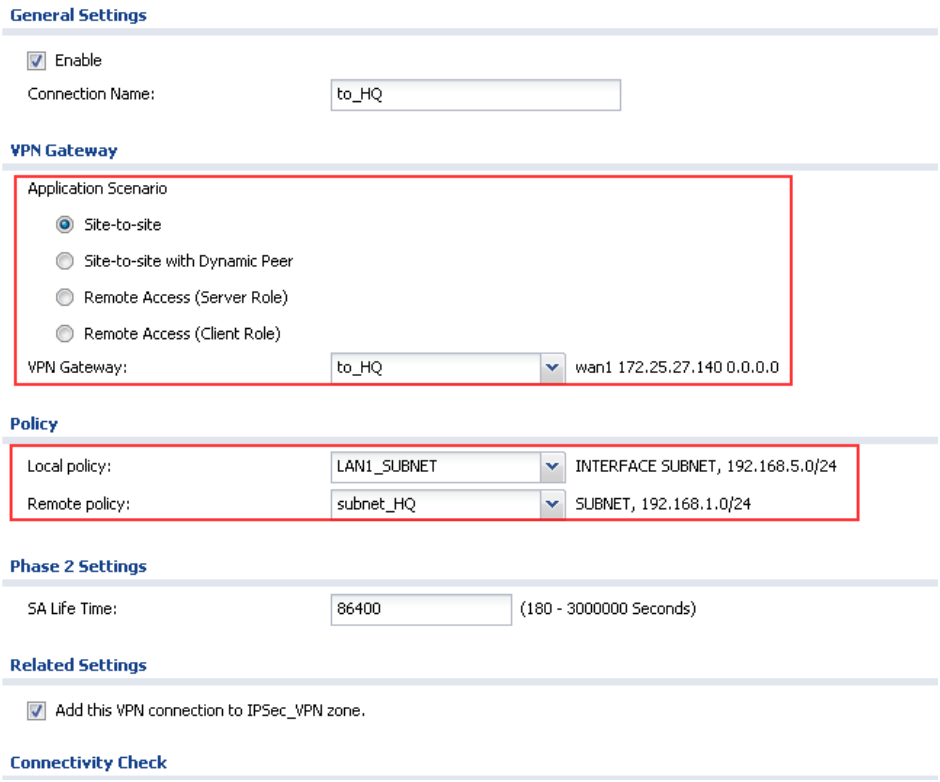
Peer Gateway Address: HQ WAN IP (172.25.27.140)



Step4. Go to Configuration > VPN > IPSec VPN > VPN Connection, add VPN phase2 rule to build tunnel to HQ.

Local policy: local LAN1 subnet (192.168.5.0/24)

Remote policy: HQ local subnet (192.168.1.0/24)



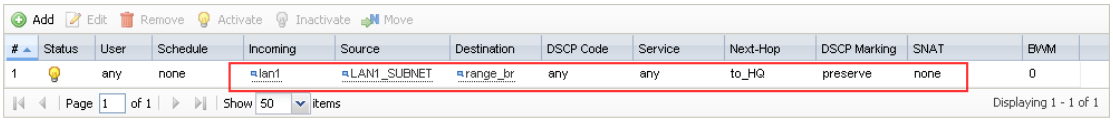
Step5. Go to Configuration > Network > Routing > Policy Route, add a policy route rule to route traffic from local subnets to all branch offices to IPSec VPN tunnel to_HQ.

Incoming interface: LAN1

Source: LAN1_Subnet (192.168.5.0/24)

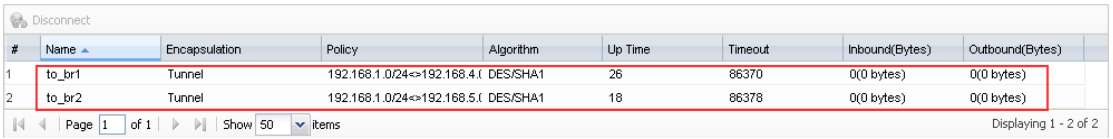
Destination: range_br(192.168.1.0~192.168.5.255)

Next Hop: VPN tunnel to_HQ



Since the SIP clients in branch offices register to the SIP server through IPSec VPN tunnels, the VoIP traffic doesn't go over NAT, we can leave SIP ALG disabled on all the USG ZyWALL.

After all the settings on both the HQ and branch offices are done, dial up the tunnels.



All the VoIP clients can register to the SIP server through the VPN tunnels, and they call make VoIP calls to each other through VPN tunnels.

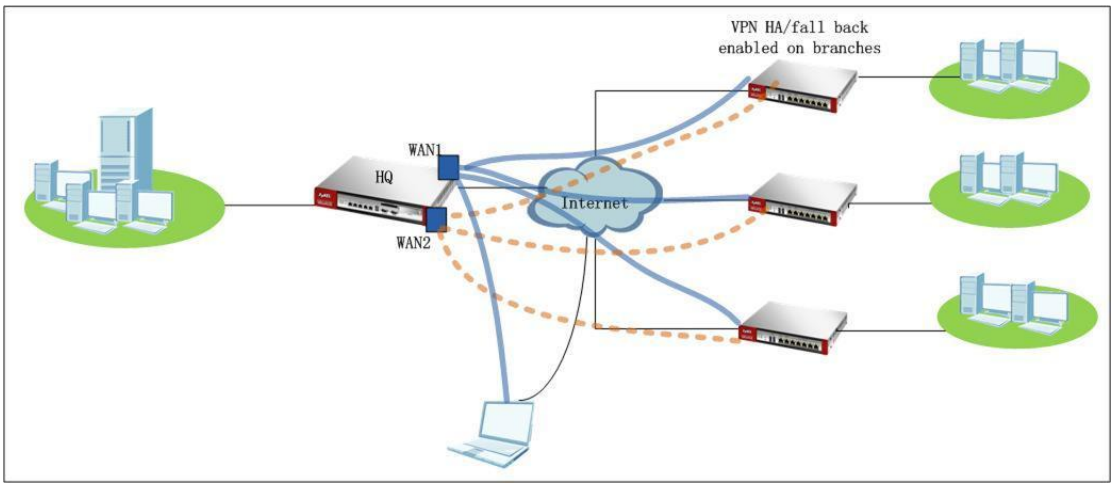
4. IPSec VPN High Availability

For nationwide or worldwide enterprise, it is always important to deploy a secure and flexible enterprise network. For example, network administrator can apply IPSec VPN for their branch offices and mobile employees to provide secured connections to headquarter.

From the secure connections, each branch office has virtual leased line through internet cloud. Hence, the enterprise has no need to pay extra expense for buying leased line(s) and can save their money on long distance call once mobile employees need to remote dial back to company.

Additionally, 7-24 operation with minimum failure time for branch offices to reach HQ through VPN is another issue to deploy enterprise networks. Network administrator can implement IPSec VPN High Availability feature to provide reliable VPN tunnels to branch offices.

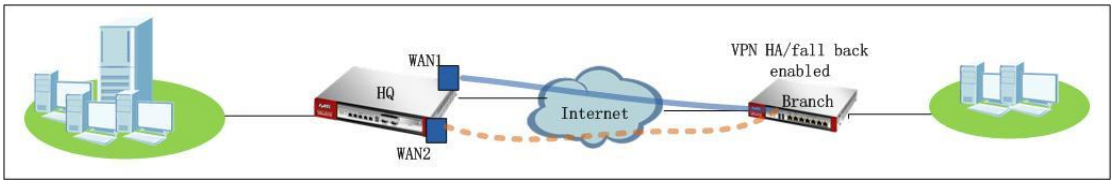
To use IPSec VPN HA feature, the HQ USG should have more than one public IP. Once primary WAN IP is down, it can use secondary WAN IP to build VPN tunnels. As soon as the primary WAN IP is up again, the VPN tunnel can fall back to use the primary WAN IP.



4.1. Site-to-Site IPSec VPN HA/Fall Back

4.1.1. Application Scenario

In the scenario below, HQ USG has two WAN IP, WAN1 and WAN2. Branch office builds IPSec VPN tunnel to HQ. IPSec VPN HA is enabled on branch USG. Primarily branch builds IPSec VPN tunnel to HQ WAN1. In case WAN1 is down, since VPN HA is enabled on branch, branch will build tunnel to HQ WAN2. Thus the branch office can enjoy a secured and reliable tunnel to HQ.
Since WAN1 has higher speed, it's HQ's primary WAN connection. We can enable VPN Fall Back on the branch. Once WAN1 is up again, branch will switch the VPN tunnel to WAN1 again.



4.1.2.Configuration Steps

IP address information on HQ and branch office USG:

HQ USG:
WAN1 IP: 200.0.0.1
WAN2 IP: 201.0.0.1
Local subnet: 192.168.1.0/24

Branch USG:
WAN IP: 202.0.0.1
Local subnet: 192.168.4.0/24

On HQ USG:

Step1. Go to Monitor > System Status > Interface Status, check the interface IP information, which will be used later in IPSec VPN configuration.

Name	Port	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Action
wan1	P1	100M/Full	n/a	WAN	200.0.0.1 / 255.255.255.0	Static	n/a	n/a
wan1_ppp	P1	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wan2	P2	100M/Full	n/a	WAN	201.0.0.1 / 255.255.255.0	Static	n/a	n/a
wan2_ppp	P2	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
opt	P3	Down	n/a	OPT	0.0.0.0 / 0.0.0.0	Static	n/a	n/a
opt_ppp	P3	Inactive	n/a	OPT	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
lan1	P4	100M/Full	n/a	LAN1	192.168.1.1 / 255.255.255.0	Static	DHCP server	n/a
lan2	P5	Down	n/a	LAN2	192.168.2.1 / 255.255.255.0	Static	DHCP server	n/a
ext-wlan	P6	Down	n/a	WLAN	10.59.0.1 / 255.255.255.0	Static	DHCP server	n/a
dmz	P7	Down	n/a	DMZ	192.168.3.1 / 255.255.255.0	Static	DHCP server	n/a
aux	aux	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wlan-1	n/a	n/a	n/a	n/a	n/a / n/a	n/a	n/a	n/a
wlan-1-1	n/a	Down	n/a	WLAN	10.59.1.1 / 255.255.255.0	static	n/a	n/a

Step2. Go to Configuration > Object > Address, add address object for branch office local subnet subnet_br (192.168.4.0/24).

Add Edit Remove Object Reference

#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	EXT_WLAN_SUBNET	INTERFACE SUBNET	ext-wlan-10.59.0.0/24
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
5	WLAN-1-1_SUBNET	INTERFACE SUBNET	wlan-1-1-10.59.1.0/24
6	subnet_br	SUBNET	192.168.4.0/24

Step3. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add VPN phase1 rule for tunnel to branch office.

My Address: Domain Name/IP 0.0.0.0

Peer Gateway Address: Branch WAN IP (202.0.0.2)

General Settings

Enable

VPN Gateway Name: to_br

Gateway Settings

My Address

Interface wan1 Static -- 200.0.0.1/255.255.255.0

Domain Name / IP 0.0.0.0

Peer Gateway Address

Static Address Primary 202.0.0.1

Secondary 0.0.0.0

Fall back to Primary Peer Gateway when possible

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

Dynamic Address

Authentication

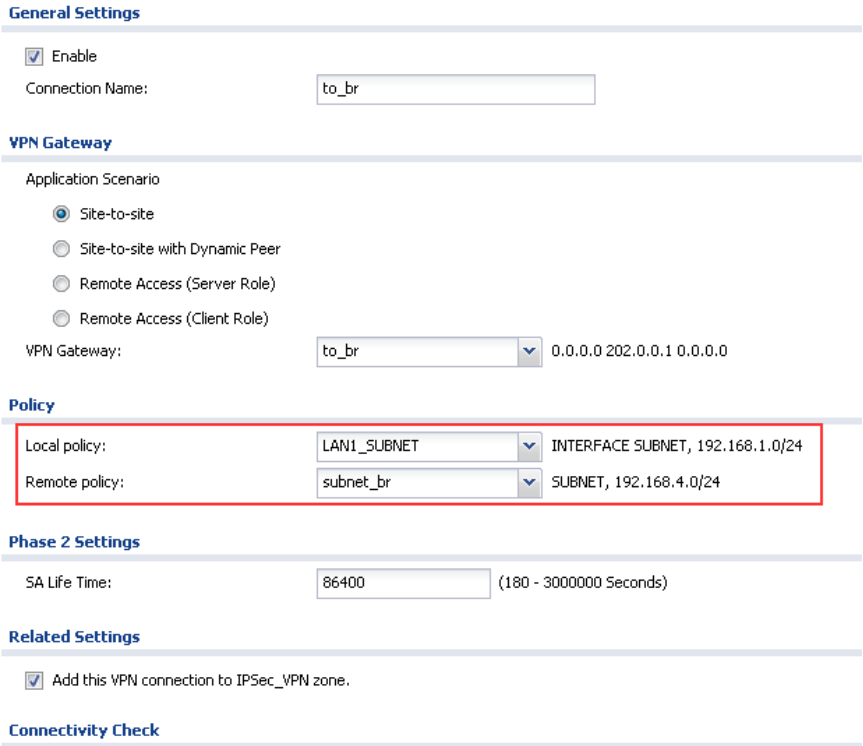
Pre-Shared Key 12345678

Certificate default (See My Certificates)

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Step4. Go to Configuration > VPN > IPSec VPN > VPN Connection, add VPN phase2 rule for tunnel to branch USG.
Local policy: local LAN1 subnet (192.168.1.0/24)
Remote policy: Branch local subnet (192.168.4.0/24)



In ZLD v2.20, system will automatically create routes for VPN traffic according to VPN phase2 (VPN Connection) local/remote policy. Traffic whose source is in the local policy and destination is in the remote policy will be sent to the corresponding VPN tunnel. Thus there's no need to add policy route.

On branch USG:

Step1. Go to Monitor > System Status > Interface Status, check the interface IP information, which will be used later in IPSec VPN configuration.

Name	Port	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Action
wan1	P1	100M/Full	n/a	WAN	202.0.0.1 / 255.255.255.0	Static	n/a	n/a
wan1_ppp	P1	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wan2	P2	Down	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew
wan2_ppp	P2	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
lan1	P3, P4	Up	n/a	LAN1	192.168.4.1 / 255.255.255.0	Static	DHCP server	n/a
lan2	P5	Down	n/a	LAN2	192.168.2.1 / 255.255.255.0	Static	DHCP server	n/a
ext-wlan	P6	Down	n/a	WLAN	10.59.0.1 / 255.255.255.0	Static	DHCP server	n/a
dmz	P7	Down	n/a	DMZ	192.168.3.1 / 255.255.255.0	Static	DHCP server	n/a
aux	aux	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wlan-1	n/a	n/a	n/a	n/a	n/a / n/a	n/a	n/a	n/a
wlan-1-1	n/a	Down	n/a	WLAN	10.59.1.1 / 255.255.255.0	static	n/a	n/a

Step2. Go to Configuration > Object > Address, add address object for HQ office local subnet subnet_HQ (192.168.1.0/24).

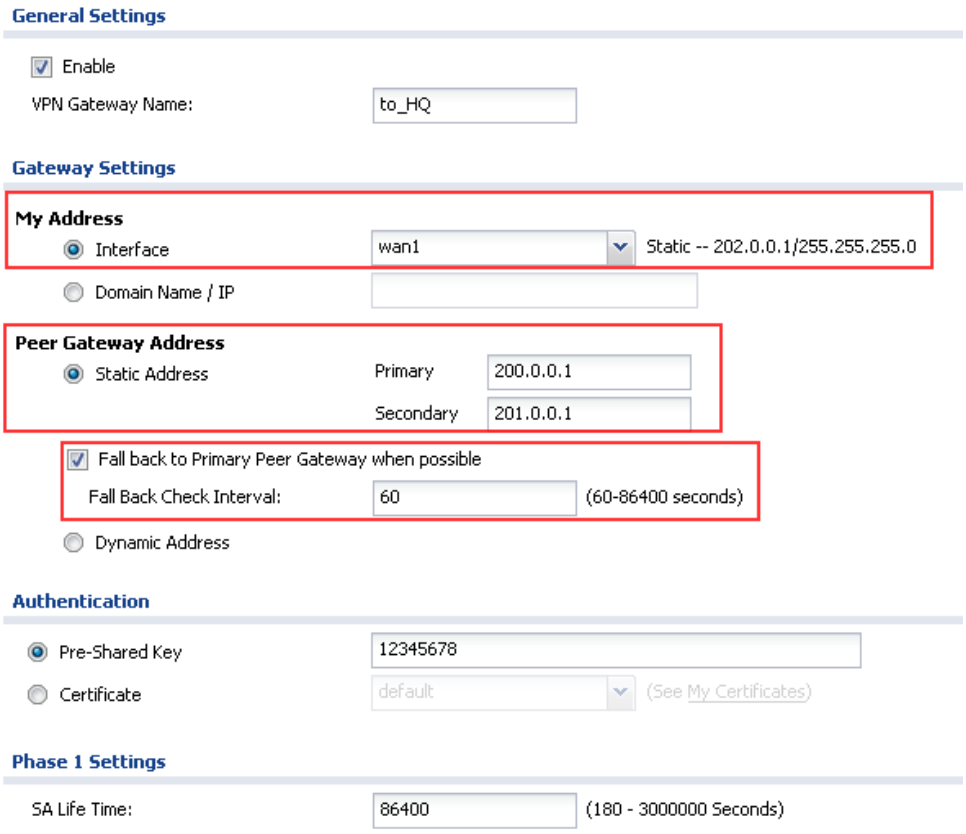
Add Edit Remove Object Reference

#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	EXT_WLAN_SUBNET	INTERFACE SUBNET	ext-wlan-10.59.0.0/24
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.4.0/24
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
5	WLAN-1-1_SUBNET	INTERFACE SUBNET	wlan-1-1-10.59.1.0/24
6	subnet_HQ	SUBNET	192.168.1.0/24

Page 1 of 1 Show 50 items Displaying 1 - 6 of 6

Step3. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add VPN phase1 rule for tunnel to HQ office.
My Address: WAN IP (202.0.0.1)
Peer Gateway Address:
Please choose Static Address.
Primary: HQ WAN1 IP (200.0.0.1)
Secondary: HQ WAN2 IP (201.0.0.1)

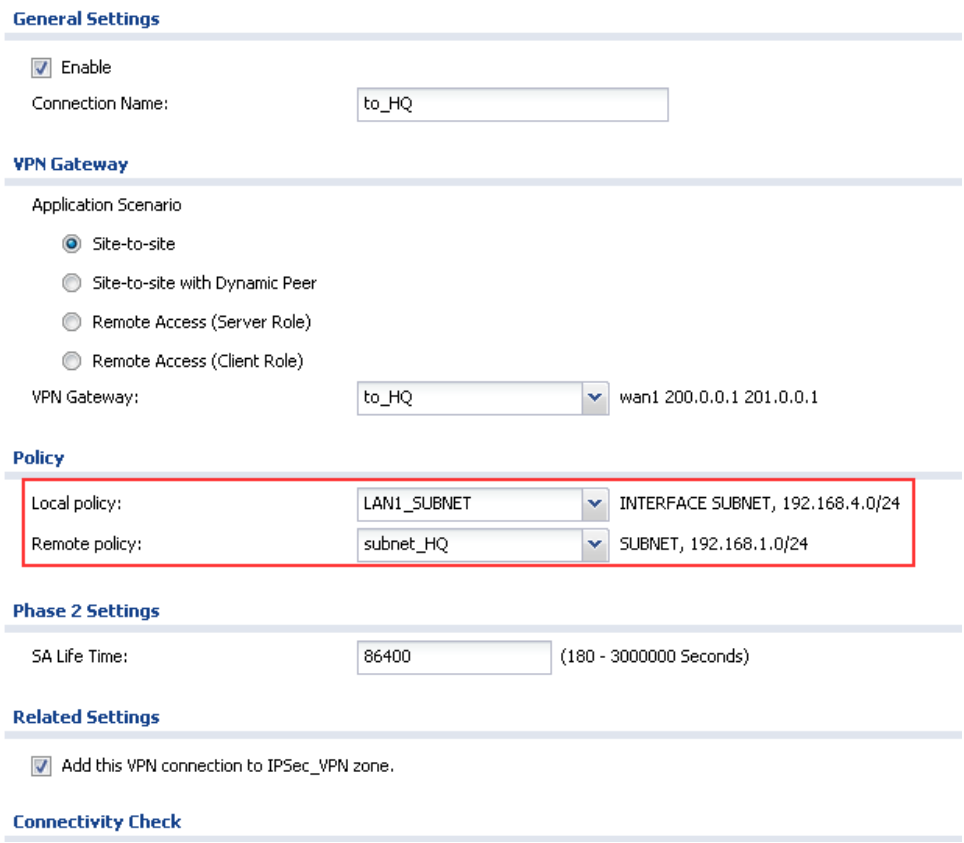
Enable “Fall back to Primary Peer Gateway when possible”.
Set “Fall Back Check Interval” a period in the range of 60s~86400s.



Step4. Go to Configuration > VPN > IPSec VPN > VPN Connection, add VPN phase2 rule for tunnel to HQ USG.

Local policy: local LAN1 subnet (192.168.4.0/24)

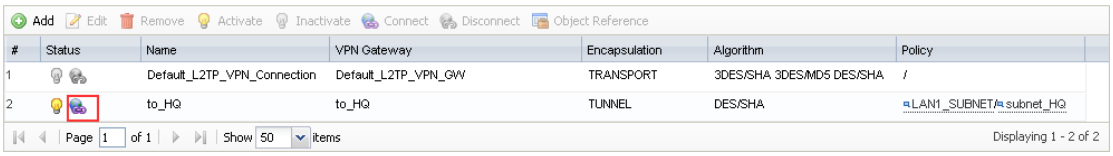
Remote policy: HQ local subnet (192.168.1.0/24)



In ZLD v2.20, system will automatically create routes for VPN traffic according to VPN phase2 (VPN Connection) local/remote policy. Traffic whose source is in the local policy and destination is in the remote policy will be sent to the corresponding VPN tunnel. Thus there's no need to add policy route.

4.1.3.Scenario Verification

On the branch USG, dial up the tunnel to HQ.



Go to Monitor > Log, check the IKE logs, the tunnel is built up to HQ WAN1.

info	IKE	Tunnel [to_HQ:to_HQ:0xb01a8ea0] built successfully	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Send:[HASH]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	[SA]: [Initiator:202.0.0.1][Responder:200.0.0.1][Policy:192.168.4.0/24-192.168.1.0/24][ESP des-cbc	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	Send:[HASH][SA][NONCE][ID][ID]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Start Phase 2: Quick Mode	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Phase 1 IKE SA process done	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Recv:[ID][HASH]	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	Send:[ID][HASH][NOTFY:INITIAL_CONTACT]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Recv:[KE][NONCE]	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	Send:[KE][NONCE]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	The cookie pair is : 0xa321a4c78ef0779b / 0xb5de9e949fdc2b91 [count=8]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Recv:[SA][VID][VID]	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	The cookie pair is : 0xa321a4c78ef0779b / 0xb5de9e949fdc2b91 [count=4]	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	Send:[SA][VID][VID]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Send Main Mode request to [200.0.0.1]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Tunnel [to_HQ] Sending IKE request	202.0.0.1:500	200.0.0.1:500	IKE_LOG

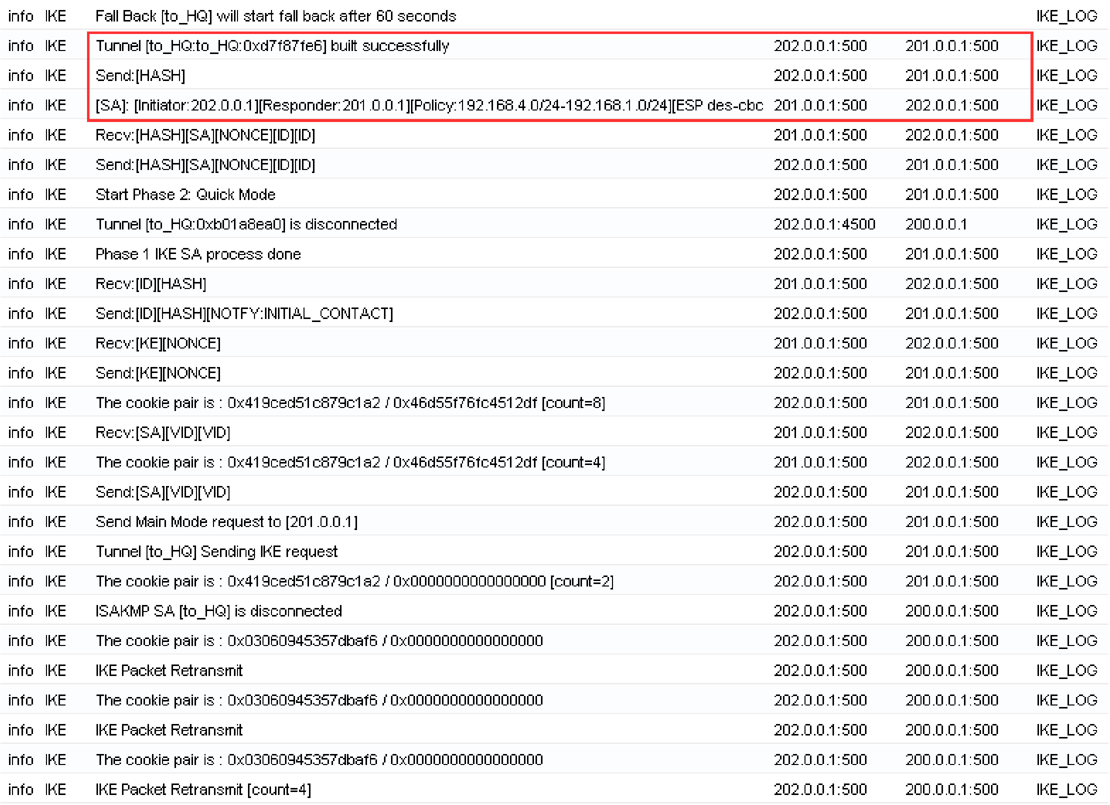
On the PC behind branch office, initiate nonstop ping to a PC behind HQ.

```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.4.33
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.4.1

Ethernet adapter 本地连接:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Administrator>ping 192.168.1.34 -t

Pinging 192.168.1.34 with 32 bytes of data:

Reply from 192.168.1.34: bytes=32 time=4ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
```

Unplug WAN1 of HQ, the ping times out (tunnel disconnected). After several timeouts, the ping resumes. The VPN tunnel is built up again.

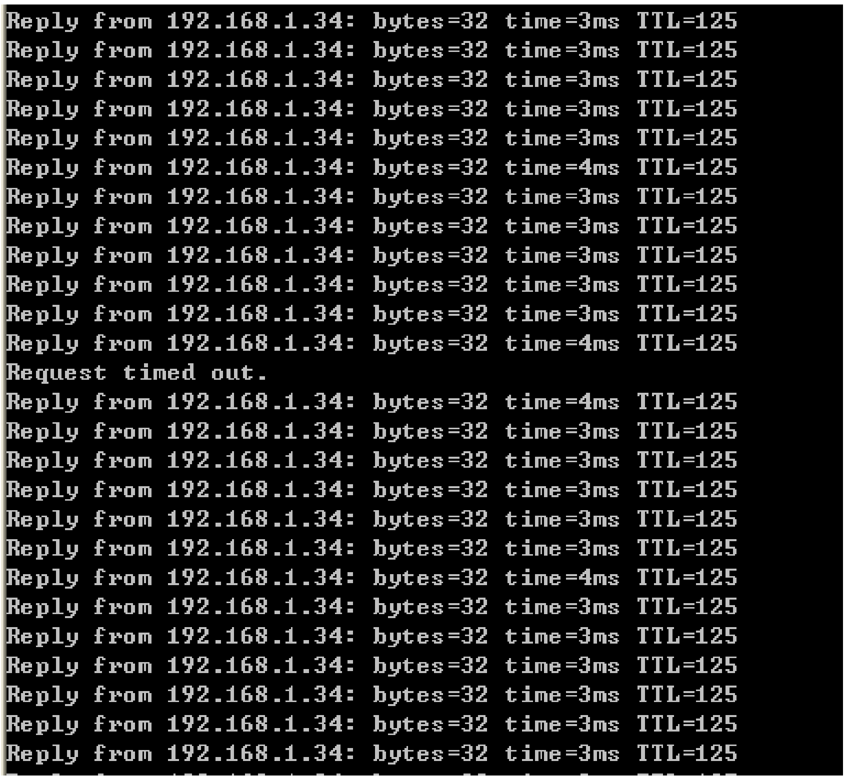
```
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=4ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.34: bytes=32 time=4ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
```

On the branch USG, go to Monitor>Log, check the IKE logs. You will find the tunnel is built up with USG WAN2.



```
info  IKE  Fall Back [to_HQ] will start fall back after 60 seconds                                                                         IKE_LOG
info  IKE  Tunnel [to_HQ:to_HQ:0xd7f87fe6] built successfully                                               202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  Send:[HASH]                                                                                      202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  [SA]: [Initiator:202.0.0.1][Responder:201.0.0.1][Policy:192.168.4.0/24-192.168.1.0/24][ESP des-cbc 201.0.0.1:500   202.0.0.1:500  IKE_LOG
info  IKE  Recv:[HASH][SA][NONCE][ID][ID]                                                                   201.0.0.1:500   202.0.0.1:500  IKE_LOG
info  IKE  Send:[HASH][SA][NONCE][ID][ID]                                                                   202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  Start Phase 2: Quick Mode                                                                        202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  Tunnel [to_HQ:0xb01a8ea0] is disconnected                                                        202.0.0.1:4500  200.0.0.1      IKE_LOG
info  IKE  Phase 1 IKE SA process done                                                                      202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  Recv:[ID][HASH]                                                                                  201.0.0.1:500   202.0.0.1:500  IKE_LOG
info  IKE  Send:[ID][HASH][NOTFY:INITIAL_CONTACT]                                                           202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  Recv:[KE][NONCE]                                                                                 201.0.0.1:500   202.0.0.1:500  IKE_LOG
info  IKE  Send:[KE][NONCE]                                                                                 202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  The cookie pair is : 0x419ced51c879c1a2 / 0x46d55f76fc4512df [count=8]                           202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  Recv:[SA][VID][VID]                                                                              201.0.0.1:500   202.0.0.1:500  IKE_LOG
info  IKE  The cookie pair is : 0x419ced51c879c1a2 / 0x46d55f76fc4512df [count=4]                           201.0.0.1:500   202.0.0.1:500  IKE_LOG
info  IKE  Send:[SA][VID][VID]                                                                              202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  Send Main Mode request to [201.0.0.1]                                                            202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  Tunnel [to_HQ] Sending IKE request                                                               202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  The cookie pair is : 0x419ced51c879c1a2 / 0x0000000000000000 [count=2]                           202.0.0.1:500   201.0.0.1:500  IKE_LOG
info  IKE  ISAKMP SA [to_HQ] is disconnected                                                                202.0.0.1:500   200.0.0.1:500  IKE_LOG
info  IKE  The cookie pair is : 0x03060945357dbaf6 / 0x0000000000000000                                     202.0.0.1:500   200.0.0.1:500  IKE_LOG
info  IKE  IKE Packet Retransmit                                                                            202.0.0.1:500   200.0.0.1:500  IKE_LOG
info  IKE  The cookie pair is : 0x03060945357dbaf6 / 0x0000000000000000                                     202.0.0.1:500   200.0.0.1:500  IKE_LOG
info  IKE  IKE Packet Retransmit                                                                            202.0.0.1:500   200.0.0.1:500  IKE_LOG
info  IKE  The cookie pair is : 0x03060945357dbaf6 / 0x0000000000000000                                     202.0.0.1:500   200.0.0.1:500  IKE_LOG
info  IKE  IKE Packet Retransmit [count=4]                                                                  202.0.0.1:500   200.0.0.1:500  IKE_LOG
```

Plug back HQ USG WAN1, the tunnel will fall back to the HQ USG WAN1.



```
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=4ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=4ms TTL=125
Request timed out.
Reply from 192.168.1.34: bytes=32 time=4ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=4ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
Reply from 192.168.1.34: bytes=32 time=3ms TTL=125
```

On Branch USG, go to Monitor > Log, check the IKE logs, you will find the tunnel

fall back (built to) the HQ USG WAN1 again.

info	IKE	ISAKMP SA [to_HQ] is disconnected	202.0.0.1:500	201.0.0.1:500	IKE_LOG
info	IKE	Fall Back [to_HQ] to primary peer gateway successfully at the 1th time			IKE_LOG
info	IKE	Tunnel [to_HQ:to_HQ:0xd7f87fe6:0x6c3a3dc] rekeyed successfully	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Fall Back [to_HQ] is continue install SA.			IKE_LOG
info	IKE	Fall Back [to_HQ] send delete SA packet successfully			IKE_LOG
info	IKE	Send:[HASH][DEL]	202.0.0.1:500	201.0.0.1:500	IKE_LOG
info	IKE	The cookie pair is : 0x419ced51c879c1a2 / 0x46d55f76fc4512df [count=2]	202.0.0.1:500	201.0.0.1:500	IKE_LOG
info	IKE	Fall Back [to_HQ] is suspended to send delete sa packet to secondary peer gateway			IKE_LOG
info	IKE	Send:[HASH]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	[SA]: [Initiator:202.0.0.1][Responder:200.0.0.1][Policy:192.168.4.0/24-192.168.1.0/24][ESP des-cbc	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	Send:[HASH][SA][NONCE][ID][ID]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Start Phase 2: Quick Mode	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Phase 1 IKE SA process done	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Recv:[ID][HASH]	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	Send:[ID][HASH][NOTFY:INITIAL_CONTACT]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Recv:[KE][NONCE]	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	Send:[KE][NONCE]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	The cookie pair is : 0x32487b5d8b0404e8 / 0x1b4d12360b06766f [count=8]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Recv:[SA][VID][VID]	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	The cookie pair is : 0x32487b5d8b0404e8 / 0x1b4d12360b06766f [count=4]	200.0.0.1:500	202.0.0.1:500	IKE_LOG
info	IKE	IKE Packet Retransmit [count=2]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Send:[SA][VID][VID]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Send Main Mode request to [200.0.0.1]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Tunnel [to_HQ] Sending IKE request	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	The cookie pair is : 0x32487b5d8b0404e8 / 0x0000000000000000 [count=4]	202.0.0.1:500	200.0.0.1:500	IKE_LOG
info	IKE	Fall Back [to_HQ] will start fall back after 60 seconds			IKE_LOG
info	IKE	Tunnel [to_HQ:to_HQ:0xd7f87fe6] built successfully	202.0.0.1:500	201.0.0.1:500	IKE_LOG

4.2. IPSec VPN Fail Over and Fall Back

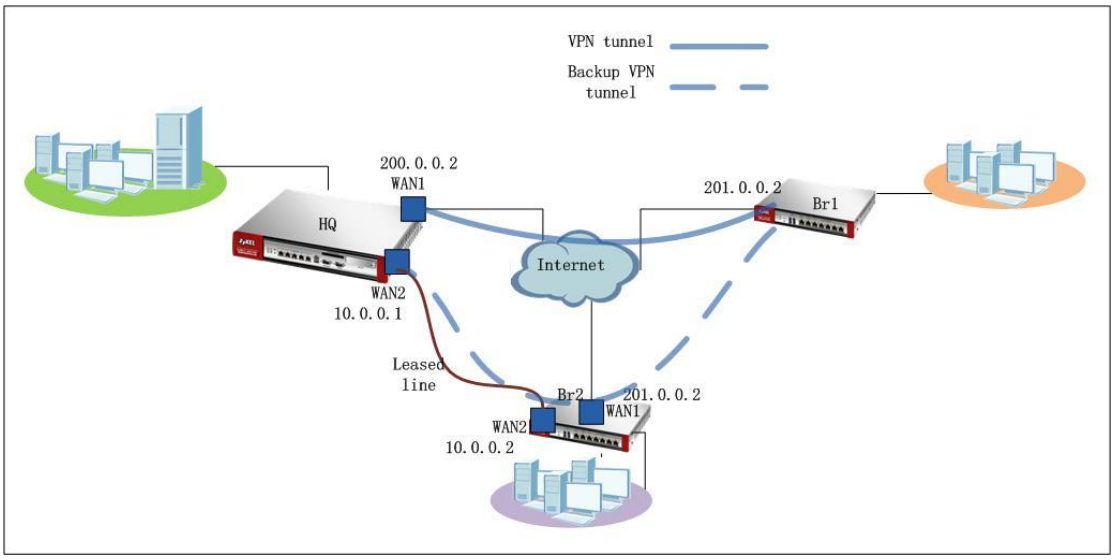
4.2.1. Application Scenario

In the below enterprise network, HQ has two WAN connections. WAN1 is connected to internet while WAN2 is connected to a leased line. Branch office 1 requires a secured connection to HQ with minimum failure time. We can deploy IPSec VPN HA to meet Branch office 1's requirement.

However, since HQ WAN2 is connected to a leased line, it cannot be reached from internet, making building VPN tunnel from Br1 to HQ's WAN2 not possible. Branch office 2's WAN2 is also connected to the leased line. Br2 can reach HQ WAN2. We can use Br2 USG to route VPN traffic from Br1 to HQ. Once HQ WAN1 is done, Br1 can first build a tunnel to Br2 WAN1. Then Br2 WAN2 builds a tunnel to HQ WAN2. Traffic from Br1 to HQ can first go to Br2 through VPN tunnel, then go to HQ through the other VPN tunnel from Br2 to HQ.

We can enable HA Fall Back. Once HQ USG WAN1 is up again, Br1 can build tunnel

directly to HQ again.



4.2.2.Configuration Steps

IP information of HQ and branch offices:

HQ USG:
WAN1 IP: 200.0.0.2
WAN2 IP: 10.0.0.1
Local subnet: 192.168.1.0/24

Br1 USG:
WAN IP: 201.0.0.2
Local subnet: 192.168.4.0/24

Br2 USG:
WAN1 IP: 201.0.0.2
WAN2 IP: 10.0.0.2
Local subnet: 192.168.5.0/24

On HQ USG:

Step1. Go to Monitor > System Status > Interface Status, check the IP address information for later use in IPSec configuration.

Name	Port	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Action
wan1	P1	100M/Full	n/a	WAN	200.0.0.2 / 255.255.255.0	Static	n/a	n/a
wan1_ppp	P1	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wan2	P2	100M/Full	n/a	WAN	10.0.0.1 / 255.255.255.0	Static	n/a	n/a
wan2_ppp	P2	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
opt	P3	Down	n/a	OPT	0.0.0.0 / 0.0.0.0	Static	n/a	n/a
opt_ppp	P3	Inactive	n/a	OPT	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
lan1	P4, P5, P6	Down	n/a	LAN1	192.168.1.1 / 255.255.255.0	Static	DHCP server	n/a
lan2	n/a	Down	n/a	LAN2	192.168.2.1 / 255.255.255.0	Static	DHCP server	n/a
ext-wlan	n/a	Down	n/a	WLAN	10.59.0.1 / 255.255.255.0	Static	DHCP server	n/a
dmz	P7	Down	n/a	DMZ	192.168.3.1 / 255.255.255.0	Static	DHCP server	n/a
aux	aux	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wlan-1	n/a	n/a	n/a	n/a	n/a / n/a	n/a	n/a	n/a
wlan-1-1	n/a	Down	n/a	WLAN	10.59.1.1 / 255.255.255.0	static	n/a	n/a

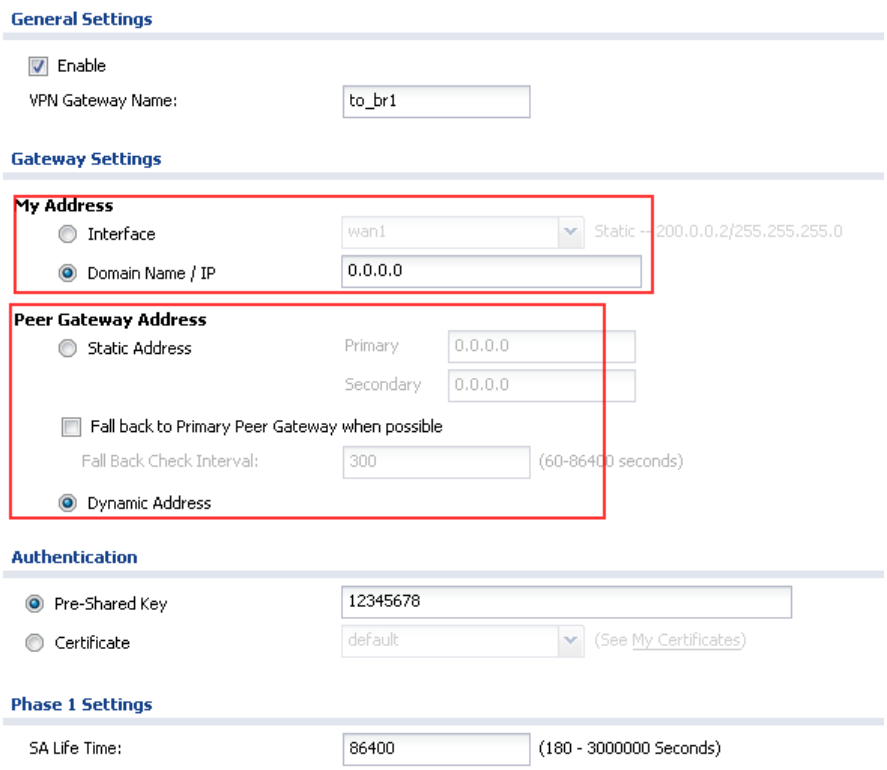
Step2. Go to Configuration > Object > Address, add address object for Br1 subnet. Subnet_br1 (192.168.4.0/24)

Add Edit Remove Object Reference

#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	EXT_WLAN_SUBNET	INTERFACE SUBNET	ext-wlan-10.59.0.0/24
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
5	WLAN-1-1_SUBNET	INTERFACE SUBNET	wlan-1-1-10.59.1.0/24
6	subnet_br1	SUBNET	192.168.4.0/24

Page 1 of 1 Show 50 items Displaying 1 - 6 of 6

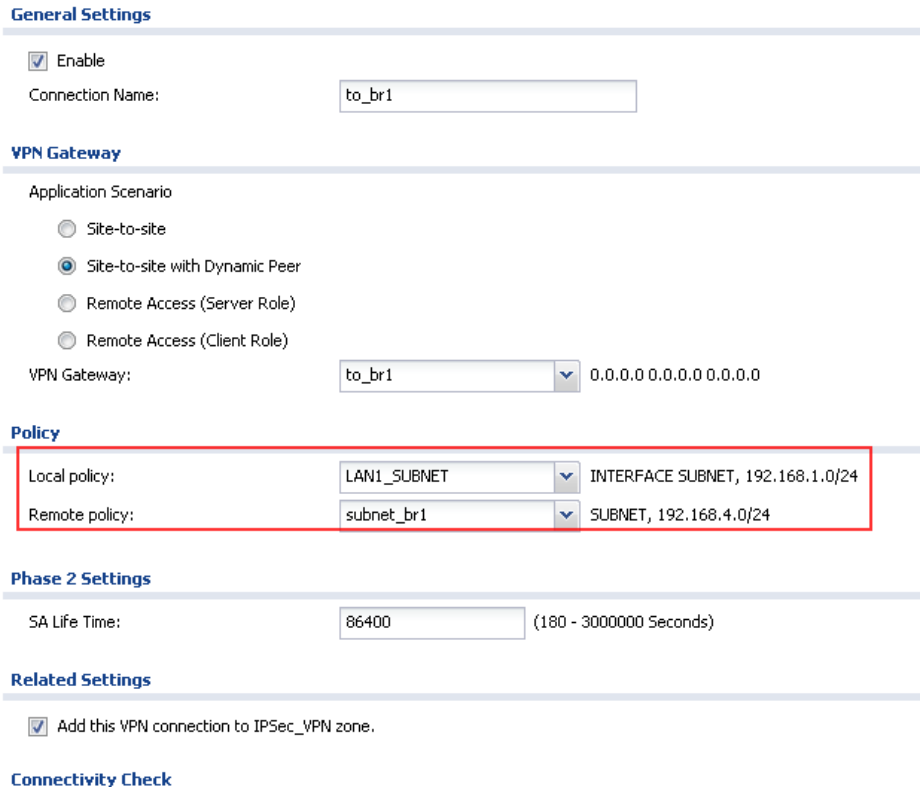
Step3. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add phase 1 rule. Since when WAN1 is up, it uses WAN1 to build VPN tunnel, when WAN1 is down, it uses WAN2 to build VPN tunnel, My Address should be set as 0.0.0.0.
When WAN1 is up, peer IP is Br1 WAN IP. When WAN1 is down, it uses WAN2 to build VPN tunnel, peer IP is Br2 WAN2 IP. So Peer Gateway Address should be set as Dynamic Address.



Step4. Go to Configuraiton > VPN > IPSec VPN > VPN Connnection, add phase2 rule.

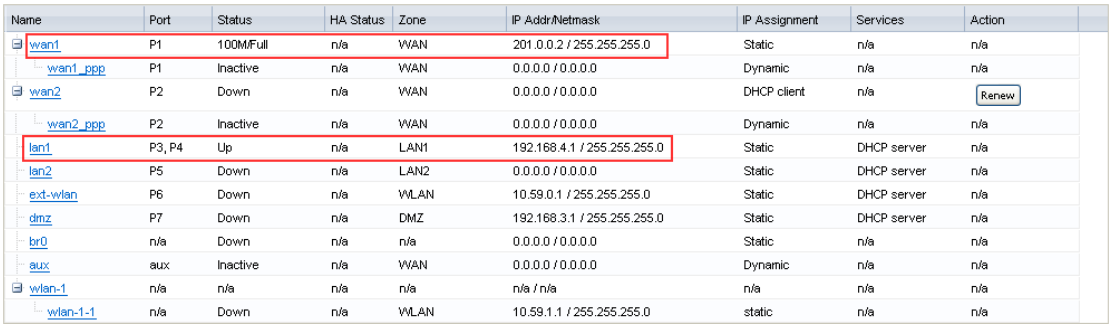
Local policy: Local LAN1 subnet (192.168.1.0/24)

Remote policy: Br1 local subnet (192.168.4.0/24)



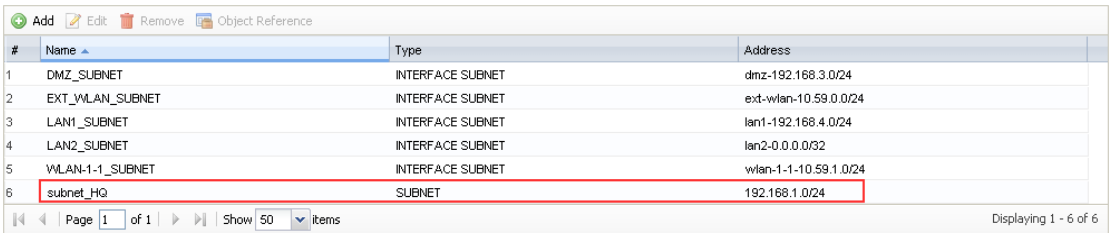
On Br1 USG:

Step1. Go to Monitor > System Status > Interface Status, check the IP address information for later use in IPSec configuration.



Name	Port	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Action
wan1	P1	100M/Full	n/a	WAN	201.0.0.2 / 255.255.255.0	Static	n/a	n/a
wan1_ppp	P1	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wan2	P2	Down	n/a	WAN	0.0.0.0 / 0.0.0.0	DHCP client	n/a	Renew
wan2_ppp	P2	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
lan1	P3, P4	Up	n/a	LAN1	192.168.4.1 / 255.255.255.0	Static	DHCP server	n/a
lan2	P5	Down	n/a	LAN2	0.0.0.0 / 0.0.0.0	Static	DHCP server	n/a
ext-wlan	P6	Down	n/a	WLAN	10.59.0.1 / 255.255.255.0	Static	DHCP server	n/a
dmz	P7	Down	n/a	DMZ	192.168.3.1 / 255.255.255.0	Static	DHCP server	n/a
br0	n/a	Down	n/a	n/a	0.0.0.0 / 0.0.0.0	Static	n/a	n/a
aux	aux	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wlan-1	n/a	n/a	n/a	n/a	n/a / n/a	n/a	n/a	n/a
wlan-1-1	n/a	Down	n/a	WLAN	10.59.1.1 / 255.255.255.0	static	n/a	n/a

Step2. Go to Configuration > Object > Address, add address object for HQ local subnet, subnet_HQ (192.168.1.0/24).

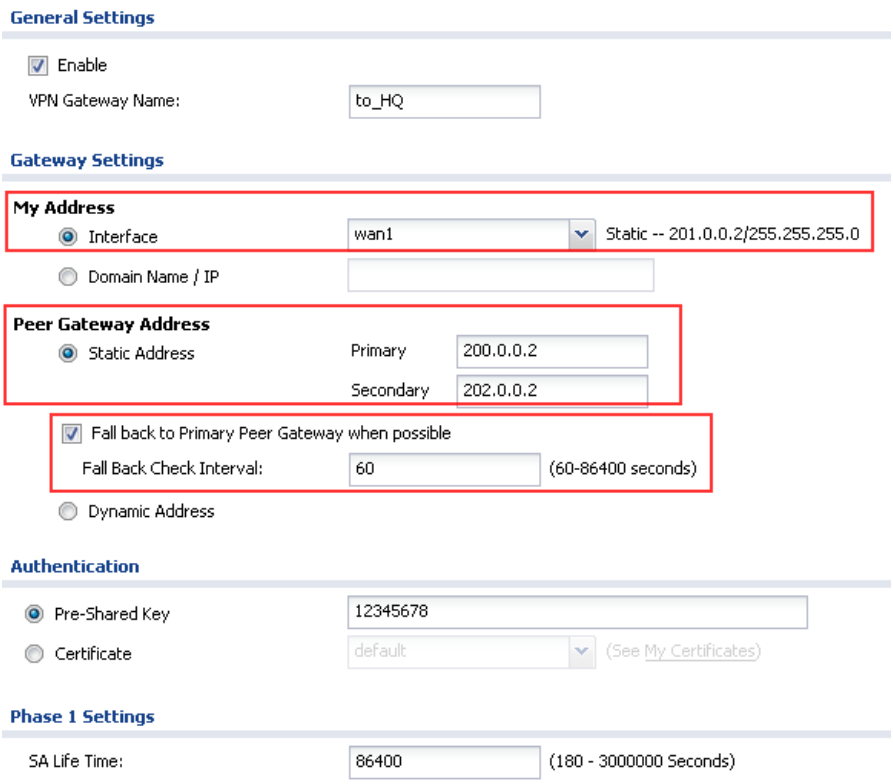


Add Edit Remove Object Reference

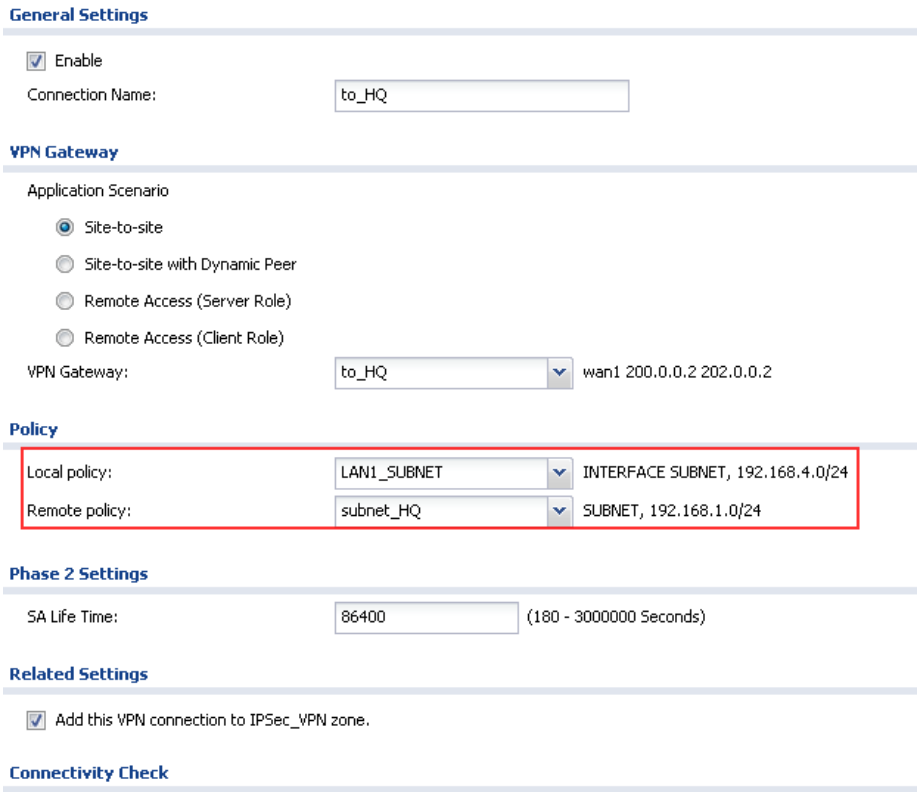
#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	EXT_WLAN_SUBNET	INTERFACE SUBNET	ext-wlan-10.59.0.0/24
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.4.0/24
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-0.0.0.0/32
5	WLAN-1-1_SUBNET	INTERFACE SUBNET	wlan-1-1-10.59.1.0/24
6	subnet_HQ	SUBNET	192.168.1.0/24

Page 1 of 1 Show 50 items Displaying 1 - 6 of 6

Step3. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add phase 1 rule.
My Address: WAN IP (201.0.0.2)
Peer Gateway Address:
To deploy VPN HA, please choose Static Address.
Primary peer gateway: HQ WAN1 IP (200.0.0.2)
Secondary peer gateway: Br1 WAN1 IP (202.0.0.2)
Enable Fall Back to Primary Gateway when possible, and set a Fall Back check interval in the range of 60s~86400s.

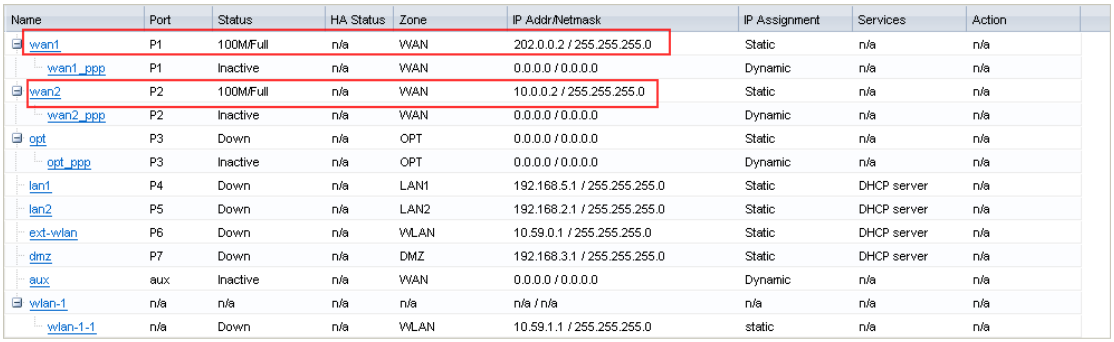


Step4. Go to Configuration > VPN >IPSec VPN > VPN Connection, add phase 2 VPN rule.
Local policy: Local LAN1 subnet (192.168.4.0/24)
Remote policy: HQ local subnet (192.168.1.0/24)



On Br2 USG:

Step1. Go to Monitor > System Status > Interface Status, check the IP address information for later use in IPSec configuration.

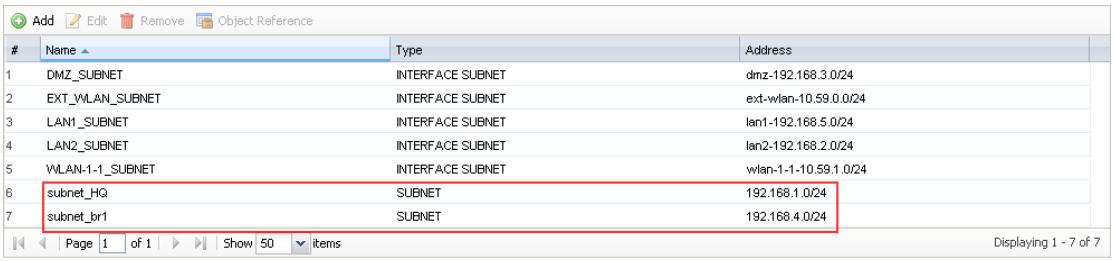


Name	Port	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Action
wan1	P1	100M/Full	n/a	WAN	202.0.0.2 / 255.255.255.0	Static	n/a	n/a
wan1_ppp	P1	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wan2	P2	100M/Full	n/a	WAN	10.0.0.2 / 255.255.255.0	Static	n/a	n/a
wan2_ppp	P2	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
opt	P3	Down	n/a	OPT	0.0.0.0 / 0.0.0.0	Static	n/a	n/a
opt_ppp	P3	Inactive	n/a	OPT	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
lan1	P4	Down	n/a	LAN1	192.168.5.1 / 255.255.255.0	Static	DHCP server	n/a
lan2	P5	Down	n/a	LAN2	192.168.2.1 / 255.255.255.0	Static	DHCP server	n/a
ext-wlan	P6	Down	n/a	WLAN	10.59.0.1 / 255.255.255.0	Static	DHCP server	n/a
dmz	P7	Down	n/a	DMZ	192.168.3.1 / 255.255.255.0	Static	DHCP server	n/a
aux	aux	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a
wlan-1	n/a	n/a	n/a	n/a	n/a / n/a	n/a	n/a	n/a
wlan-1-1	n/a	Down	n/a	WLAN	10.59.1.1 / 255.255.255.0	static	n/a	n/a

Step2. Go to Configuration > Object > Address, add address objects for HQ local subnet and Br1 local subnet.

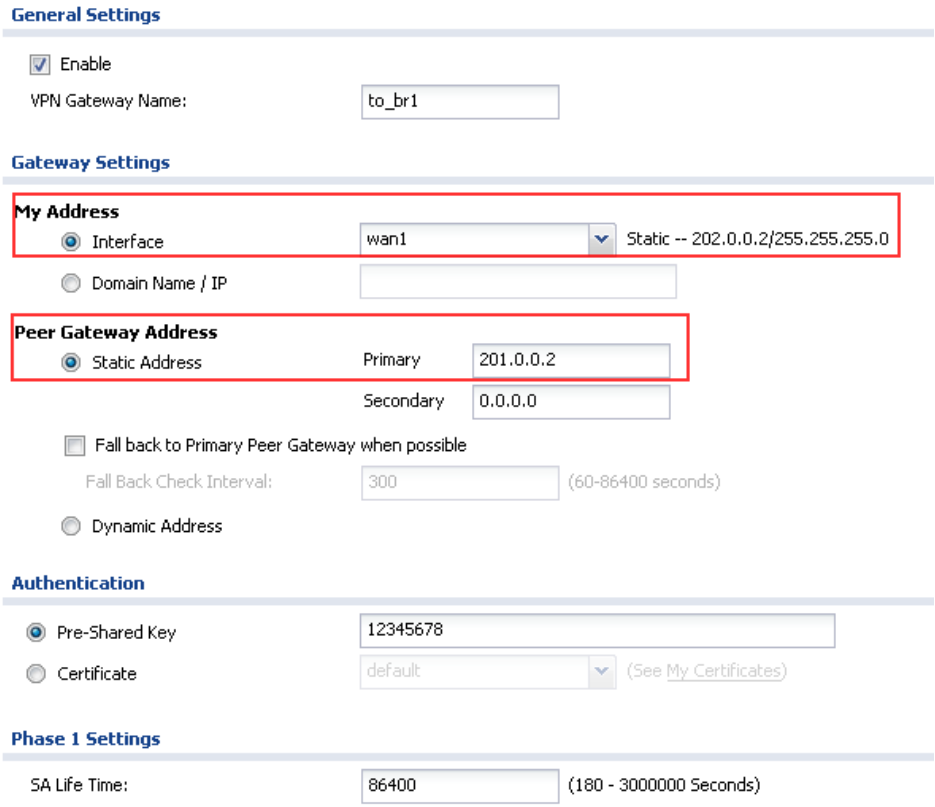
HQ local subnet: subnet_HQ (192.168.1.0/24).

Br1 local subnet: subnet_br1 (192.168.4.0/24)

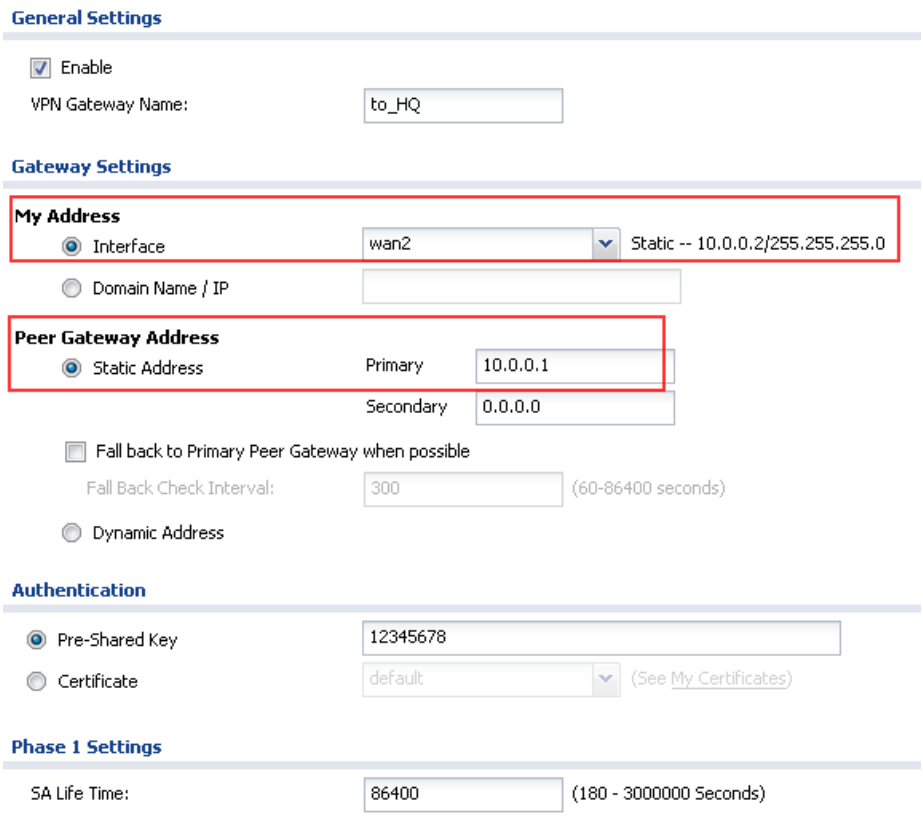


Step3. Go to Configuration > VPN > IPSec VPN > VPN Gateway, add phase 1 VPN rules.

Tunnel to Br1 phase1 rule:
My Address: WAN1 IP (202.0.0.2)
Peer Gateway Address: Br1 WAN IP (201.0.0.2)

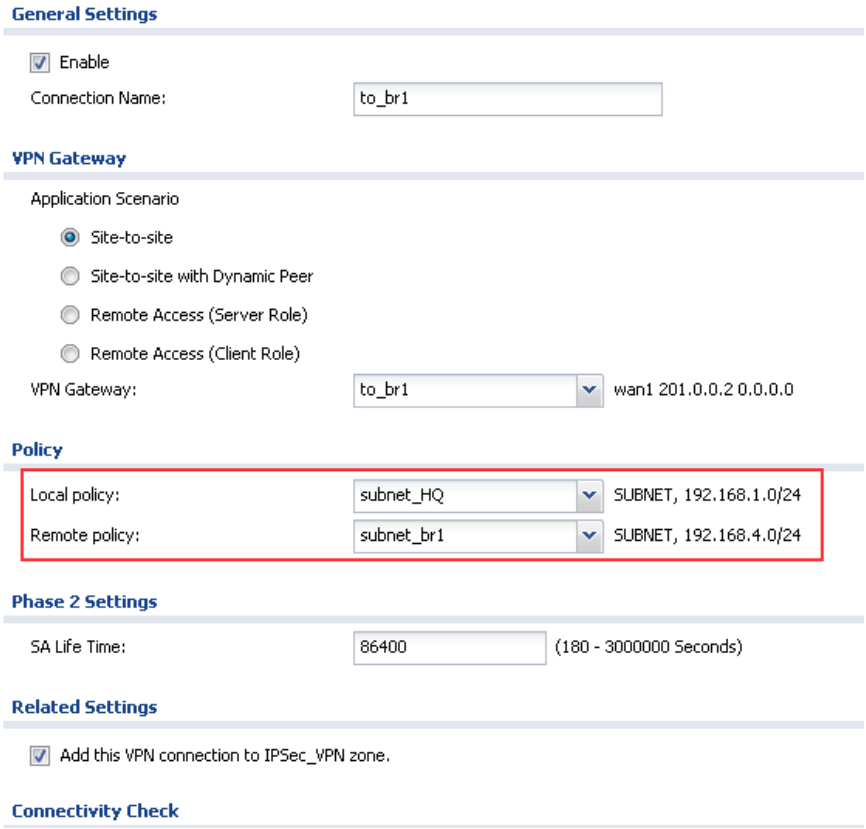


Tunnel to HQ phase1 rule:
My Address: WAN2 IP (10.0.0.2)
Peer Gateway Address: HQ WAN2 IP (10.0.0.1)



Step4. Go to Configuration > VPN > IPSec VPN > VPN Connection, add phase 2 VPN rules.

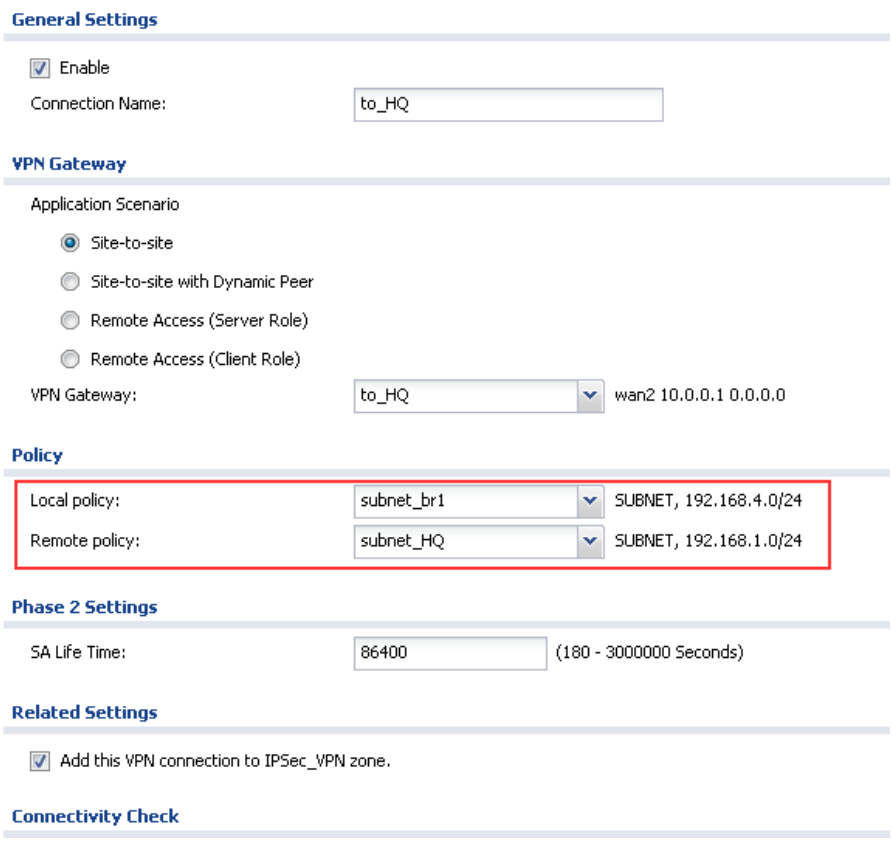
Tunnel to Br1 phase2 rule:
Local policy: HQ local subnet (192.168.1.0/24)
Remote policy: Br1 local subnet (192.168.4.0/24)



Tunnel to HQ phase2 rule:

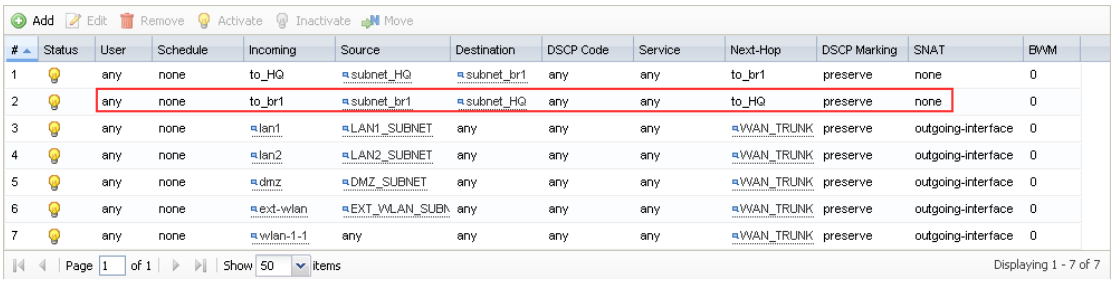
Local policy: Br1 local subnet (192.168.4.0/24)

Remote policy: HQ local subnet (192.168.1.0/24)



Step5. Go to Configuration > Network > Routing > Policy Route, add policy routes to route traffic from Br1 to HQ through VPN tunnels, as well as traffic from HQ to Br1 through VPN tunnels.

For traffic from Br1 local subnet to HQ local subnet:
Incoming interface: VPN tunnel to_br1
Source: Br1 local subnet subnet_br1 (192.168.4.0/24)
Destination: HQ local subnet subnet_HQ (192.168.1.0/24)
Next-Hop: VPN tunnel to_HQ



#	Status	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Next-Hop	DSCP Marking	SNAT	BWM
1		any	none	to_HQ	subnet_HQ	subnet_br1	any	any	to_br1	preserve	none	0
2		any	none	to_br1	subnet_br1	subnet_HQ	any	any	to_HQ	preserve	none	0
3		any	none	lan1	LAN1_SUBNET	any	any	any	WAN_TRUNK	preserve	outgoing-interface	0
4		any	none	lan2	LAN2_SUBNET	any	any	any	WAN_TRUNK	preserve	outgoing-interface	0
5		any	none	dmz	DMZ_SUBNET	any	any	any	WAN_TRUNK	preserve	outgoing-interface	0
6		any	none	ext-wlan	EXT_WLAN_SUBN	any	any	any	WAN_TRUNK	preserve	outgoing-interface	0
7		any	none	wlan-1-1	any	any	any	any	WAN_TRUNK	preserve	outgoing-interface	0

For traffic from HQ local subnet to Br1 local subnet:
Incoming interface: VPN tunnel to_HQ

Source: HQ local subnet subnet_HQ

Destination: Br1 local subnet subnet_Br1

Next-Hop: VPN tunnel to_Br1.

Add Edit Remove Activate Inactivate Move

#	Status	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Next-Hop	DSCP Marking	SNAT	BWM
1		any	none	to_HQ	subnet_HQ	subnet_br1	any	any	to_br1	preserve	none	0
2		any	none	to_br1	subnet_br1	subnet_HQ	any	any	to_HQ	preserve	none	0
3		any	none	lan1	LAN1_SUBNET	any	any	any	WAN_TRUNK	preserve	outgoing-interface	0
4		any	none	lan2	LAN2_SUBNET	any	any	any	WAN_TRUNK	preserve	outgoing-interface	0
5		any	none	dmz	DMZ_SUBNET	any	any	any	WAN_TRUNK	preserve	outgoing-interface	0
6		any	none	ext-wlan	EXT_WLAN_SUBN	any	any	any	WAN_TRUNK	preserve	outgoing-interface	0
7		any	none	wlan-1-1	any	any	any	any	WAN_TRUNK	preserve	outgoing-interface	0

Page 1 of 1 Show 50 items Displaying 1 - 7 of 7

After all the steps above, the configuration for this application scenario is done.

4.2.3.Scenario Verification

On Br1, dial up the tunnel to HQ.

Add Edit Remove Activate Inactivate Connect Disconnect Object Reference

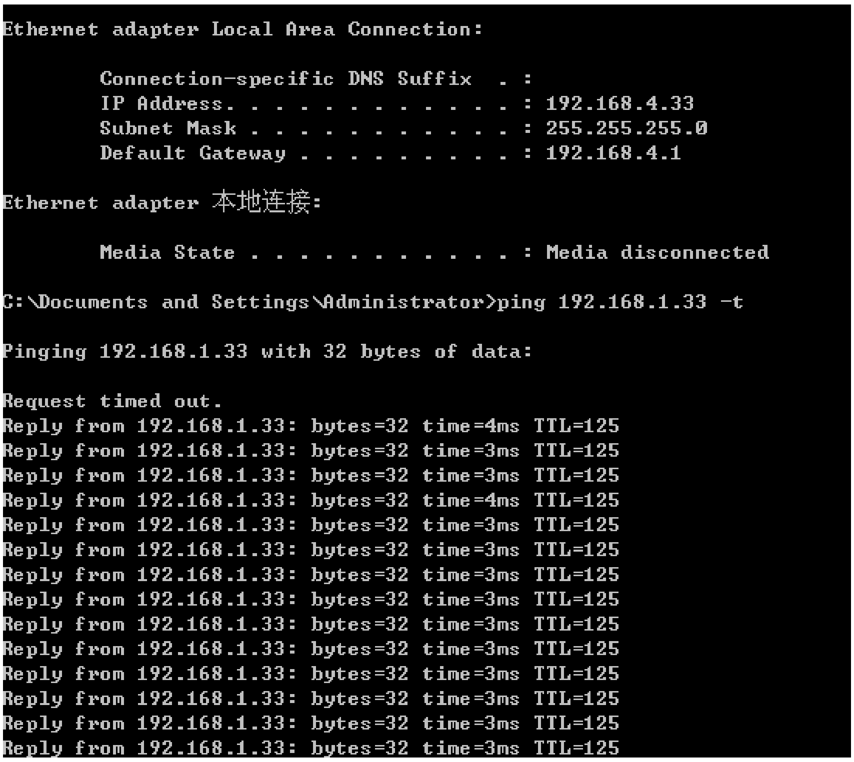
#	Status	Name	VPN Gateway	Encapsulation	Algorithm	Policy
1		Default_L2TP_VPN_Connection	Default_L2TP_VPN_GW	TRANSPORT	3DES/SHA 3DES/MD5 DES/SHA	/
2		to_HQ	to_HQ	TUNNEL	DES/SHA	LAN1_SUBNET/subnet_HQ

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

Go to Monitor > Log, check the IKE logs, the tunnel is built up to HQ WAN1.

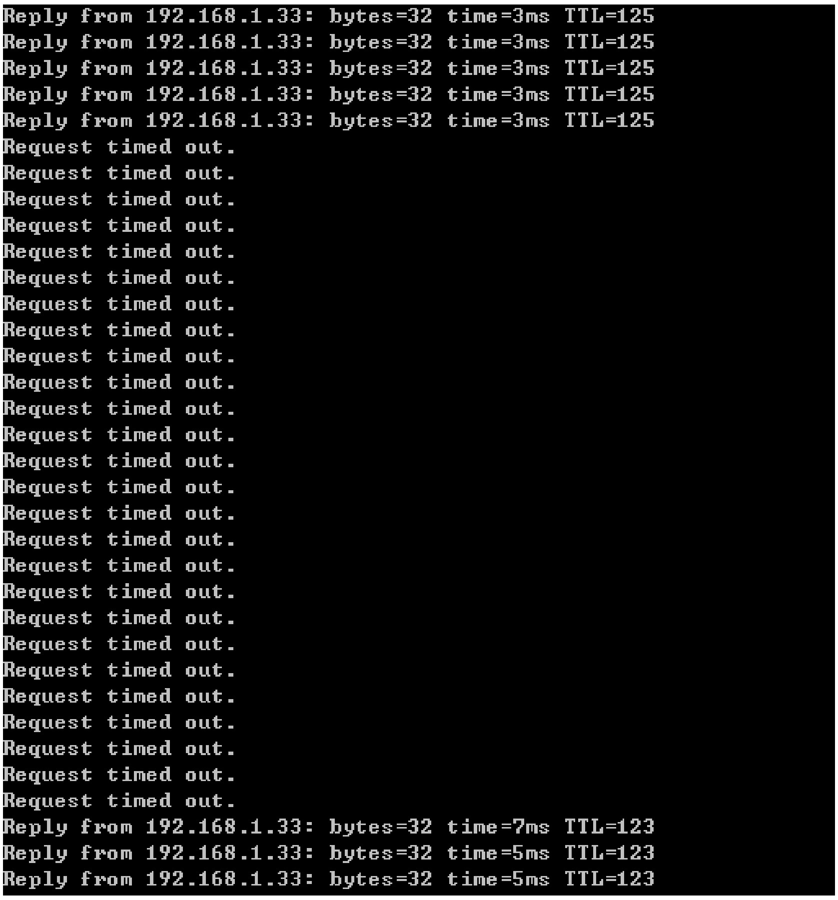
info	IKE	The cookie pair is : 0x07e7bbdd669e8334 / 0xac9bb1d6f47f2839 [count=4]	201.0.0.2:500	200.0.0.2:500	IKE_LOG
info	IKE	Tunnel [to_HQ:to_HQ:0xdd670c2e] built successfully	201.0.0.2:500	200.0.0.2:500	IKE_LOG
info	IKE	Send:[HASH]	201.0.0.2:500	200.0.0.2:500	IKE_LOG
info	IKE	[SA]: [Initiator:201.0.0.2][Responder:200.0.0.2][Policy:192.168.4.0/24-192.168.1.0/24][ESP des-cl	200.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	200.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	The cookie pair is : 0x07e7bbdd669e8334 / 0xac9bb1d6f47f2839	200.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Send:[HASH][SA][NONCE][ID][ID]	201.0.0.2:500	200.0.0.2:500	IKE_LOG
info	IKE	Start Phase 2: Quick Mode	201.0.0.2:500	200.0.0.2:500	IKE_LOG
info	IKE	The cookie pair is : 0x07e7bbdd669e8334 / 0xac9bb1d6f47f2839 [count=5]	201.0.0.2:500	200.0.0.2:500	IKE_LOG

On a PC behind branch office, initiate nonstop ping to a PC behind HQ.



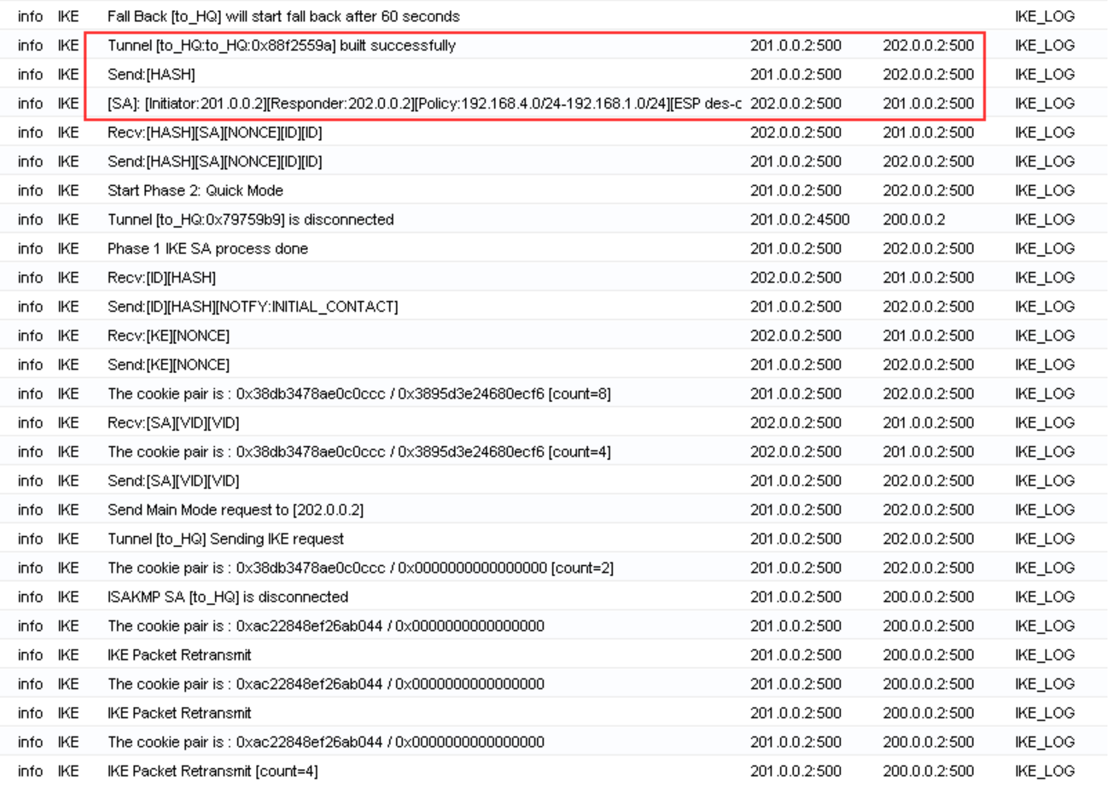
```
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.4.33
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.4.1

Ethernet adapter 本地连接:

        Media State . . . . . . . . . . . : Media disconnected

C:\Documents and Settings\Administrator>ping 192.168.1.33 -t

Pinging 192.168.1.33 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.33: bytes=32 time=4ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=4ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
```

Unplug HQ USG WAN1, the ping times out (tunnel disconnected). After a while, the ping resumes. The VPN tunnel is built up again.



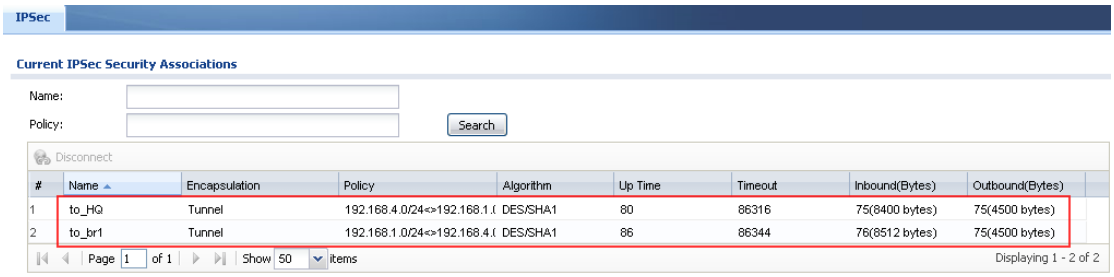
```
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Reply from 192.168.1.33: bytes=32 time=7ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
```

On Br1, go to Monitor > Log, check the IKE logs. You will find the tunnel is built successfully to Br2 WAN1 (202.0.0.2).



info	IKE	Fall Back [to_HQ] will start fall back after 60 seconds			IKE_LOG
info	IKE	Tunnel [to_HQ:to_HQ:0x88f2559a] built successfully	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	Send:[HASH]	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	[SA]: [Initiator:201.0.0.2][Responder:202.0.0.2][Policy:192.168.4.0/24-192.168.1.0/24][ESP des-c	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Send:[HASH][SA][NONCE][ID][ID]	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	Start Phase 2: Quick Mode	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	Tunnel [to_HQ:0x79759b9] is disconnected	201.0.0.2:4500	200.0.0.2	IKE_LOG
info	IKE	Phase 1 IKE SA process done	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	Recv:[ID][HASH]	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Send:[ID][HASH][NOTFY:INITIAL_CONTACT]	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	Recv:[KE][NONCE]	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Send:[KE][NONCE]	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	The cookie pair is : 0x38db3478ae0c0ccc / 0x3895d3e24680ecf6 [count=8]	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	Recv:[SA][VID][VID]	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	The cookie pair is : 0x38db3478ae0c0ccc / 0x3895d3e24680ecf6 [count=4]	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Send:[SA][VID][VID]	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	Send Main Mode request to [202.0.0.2]	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	Tunnel [to_HQ] Sending IKE request	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	The cookie pair is : 0x38db3478ae0c0ccc / 0x0000000000000000 [count=2]	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	ISAKMP SA [to_HQ] is disconnected	201.0.0.2:500	200.0.0.2:500	IKE_LOG
info	IKE	The cookie pair is : 0xac22848ef26ab044 / 0x0000000000000000	201.0.0.2:500	200.0.0.2:500	IKE_LOG
info	IKE	IKE Packet Retransmit	201.0.0.2:500	200.0.0.2:500	IKE_LOG
info	IKE	The cookie pair is : 0xac22848ef26ab044 / 0x0000000000000000	201.0.0.2:500	200.0.0.2:500	IKE_LOG
info	IKE	IKE Packet Retransmit	201.0.0.2:500	200.0.0.2:500	IKE_LOG
info	IKE	The cookie pair is : 0xac22848ef26ab044 / 0x0000000000000000	201.0.0.2:500	200.0.0.2:500	IKE_LOG
info	IKE	IKE Packet Retransmit [count=4]	201.0.0.2:500	200.0.0.2:500	IKE_LOG

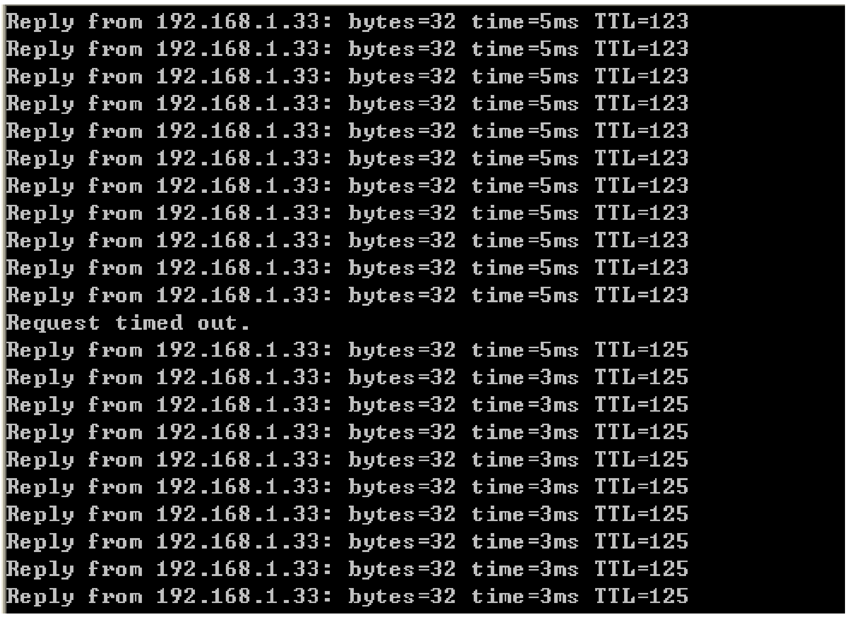
On Br2, go to Monitor > VPN Monitor > IPSec VPN, you will find the two VPN tunnels are up. One is to Br1 (Policy 192.168.1.0 /24<->192.168.4.0/24). The other is to HQ (Policy 192.168.4.0/24<->192.168.1.0/24).



Check the IKE logs on Br2 in Monitor > Log, you can find the tunnel to Br1 and to HQ are both built up successfully.

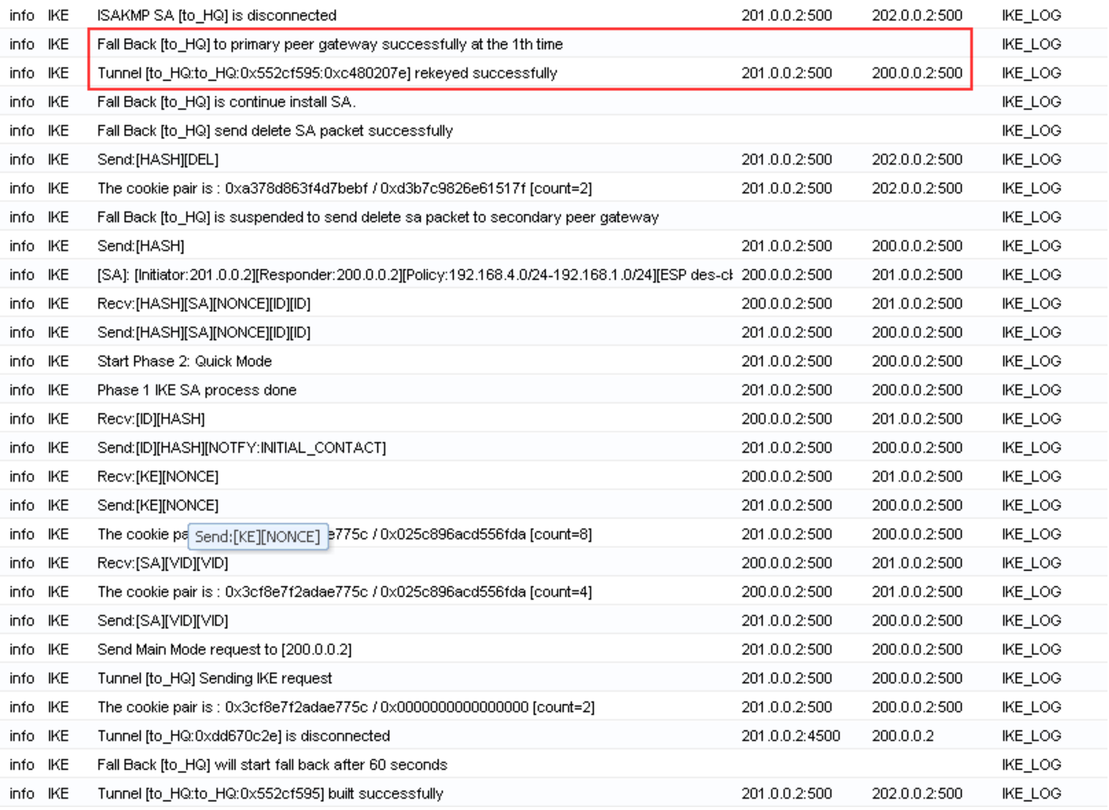
info	IKE	Tunnel [to_HQ:to_HQ:0x717d1c0a] built successfully	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	Send:[HASH]	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	[SA]: [Initiator:10.0.0.2][Responder:10.0.0.1][Policy:192.168.4.0/24-192.168.1.(	10.0.0.1:500	10.0.0.2:500	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	10.0.0.1:500	10.0.0.2:500	IKE_LOG
info	IKE	Send:[HASH][SA][NONCE][ID][ID]	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	Start Phase 2: Quick Mode	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	Phase 1 IKE SA process done	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	Recv:[ID][HASH]	10.0.0.1:500	10.0.0.2:500	IKE_LOG
info	IKE	Send:[ID][HASH][NOTFY:INITIAL_CONTACT]	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	Recv:[KE][NONCE]	10.0.0.1:500	10.0.0.2:500	IKE_LOG
info	IKE	Send:[KE][NONCE]	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	The cookie pair is : 0xf7833c21a0028dbd / 0xa390a70332adf13b [count=8]	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	Recv:[SA][VID][VID]	10.0.0.1:500	10.0.0.2:500	IKE_LOG
info	IKE	The cookie pair is : 0xf7833c21a0028dbd / 0xa390a70332adf13b [count=4]	10.0.0.1:500	10.0.0.2:500	IKE_LOG
info	IKE	Send:[SA][VID][VID]	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	Send Main Mode request to [10.0.0.1]	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	Tunnel [to_HQ] Sending IKE request	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	The cookie pair is : 0xf7833c21a0028dbd / 0x0000000000000000 [count=2]	10.0.0.2:500	10.0.0.1:500	IKE_LOG
info	IKE	Tunnel [to_br1:0x51acfdd7] is disconnected	202.0.0.2:4500	201.0.0.2	IKE_LOG
info	IKE	Tunnel [to_br1:to_br1:0x6c13f55c] built successfully	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	[SA]: [Responder:202.0.0.2][Initiator:201.0.0.2][Policy:192.168.1.0/24-192.168.·	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	Recv:[HASH]	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	Send:[HASH][SA][NONCE][ID][ID]	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	ISAKMP SA [to_br1] is disconnected	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Send:[HASH][DEL] [count=2]	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Tunnel [to_br1:0x51acfdd7] is disconnected	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	The cookie pair is : 0xa378d863f4d7bebf / 0xd3b7c9826e61517f [count=4]	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Send:[ID][HASH]	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Phase 1 IKE SA process done	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Recv:[ID][HASH][NOTFY:INITIAL_CONTACT]	201.0.0.2:500	202.0.0.2:500	IKE_LOG
info	IKE	Send:[KE][NONCE]	202.0.0.2:500	201.0.0.2:500	IKE_LOG
info	IKE	Recv:[KE][NONCE]	201.0.0.2:500	202.0.0.2:500	IKE_LOG

Plug back HQ USG WAN1, the tunnel from Br1 to HQ will fall back to the HQ WAN1.



```
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Reply from 192.168.1.33: bytes=32 time=5ms TTL=123
Request timed out.
Reply from 192.168.1.33: bytes=32 time=5ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
Reply from 192.168.1.33: bytes=32 time=3ms TTL=125
```

On Br1, go to Monitor > Log, you will find the tunnel fall back to HQ WAN1 (200.0.0.2) successfully.



```
info  IKE  ISAKMP SA [to_HQ] is disconnected                                                      201.0.0.2:500   202.0.0.2:500  IKE_LOG
info  IKE  Fall Back [to_HQ] to primary peer gateway successfully at the 1th time                                                IKE_LOG
info  IKE  Tunnel [to_HQ:to_HQ:0x552cf595:0xc480207e] rekeyed successfully                        201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  Fall Back [to_HQ] is continue install SA.                                                                             IKE_LOG
info  IKE  Fall Back [to_HQ] send delete SA packet successfully                                                                  IKE_LOG
info  IKE  Send:[HASH][DEL]                                                                       201.0.0.2:500   202.0.0.2:500  IKE_LOG
info  IKE  The cookie pair is : 0xa378d863f4d7bebf / 0xd3b7c9826e61517f [count=2]                 201.0.0.2:500   202.0.0.2:500  IKE_LOG
info  IKE  Fall Back [to_HQ] is suspended to send delete sa packet to secondary peer gateway                                      IKE_LOG
info  IKE  Send:[HASH]                                                                            201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  [SA]: [Initiator:201.0.0.2][Responder:200.0.0.2][Policy:192.168.4.0/24-192.168.1.0/24][ESP des-ct 200.0.0.2:500   201.0.0.2:500  IKE_LOG
info  IKE  Recv:[HASH][SA][NONCE][ID][ID]                                                         200.0.0.2:500   201.0.0.2:500  IKE_LOG
info  IKE  Send:[HASH][SA][NONCE][ID][ID]                                                         201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  Start Phase 2: Quick Mode                                                              201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  Phase 1 IKE SA process done                                                            201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  Recv:[ID][HASH]                                                                        200.0.0.2:500   201.0.0.2:500  IKE_LOG
info  IKE  Send:[ID][HASH][NOTFY:INITIAL_CONTACT]                                                 201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  Recv:[KE][NONCE]                                                                       200.0.0.2:500   201.0.0.2:500  IKE_LOG
info  IKE  Send:[KE][NONCE]                                                                       201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  The cookie pa Send:[KE][NONCE] e775c / 0x025c896acd556fda [count=8]                    201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  Recv:[SA][VID][VID]                                                                    200.0.0.2:500   201.0.0.2:500  IKE_LOG
info  IKE  The cookie pair is : 0x3cf8e7f2adae775c / 0x025c896acd556fda [count=4]                 200.0.0.2:500   201.0.0.2:500  IKE_LOG
info  IKE  Send:[SA][VID][VID]                                                                    201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  Send Main Mode request to [200.0.0.2]                                                  201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  Tunnel [to_HQ] Sending IKE request                                                     201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  The cookie pair is : 0x3cf8e7f2adae775c / 0x0000000000000000 [count=2]                 201.0.0.2:500   200.0.0.2:500  IKE_LOG
info  IKE  Tunnel [to_HQ:0xdd670c2e] is disconnected                                              201.0.0.2:4500  200.0.0.2      IKE_LOG
info  IKE  Fall Back [to_HQ] will start fall back after 60 seconds                                                               IKE_LOG
info  IKE  Tunnel [to_HQ:to_HQ:0x552cf595] built successfully                                     201.0.0.2:500   202.0.0.2:500  IKE_LOG
```

FAQ

The FAQ from A to P are ZLD v2.12 related. But you can also refer to them for ZLD v2.20 corresponding questions.

A. Device Management FAQ

A01. How can I connect to ZyWALL USG to perform administrator's tasks?

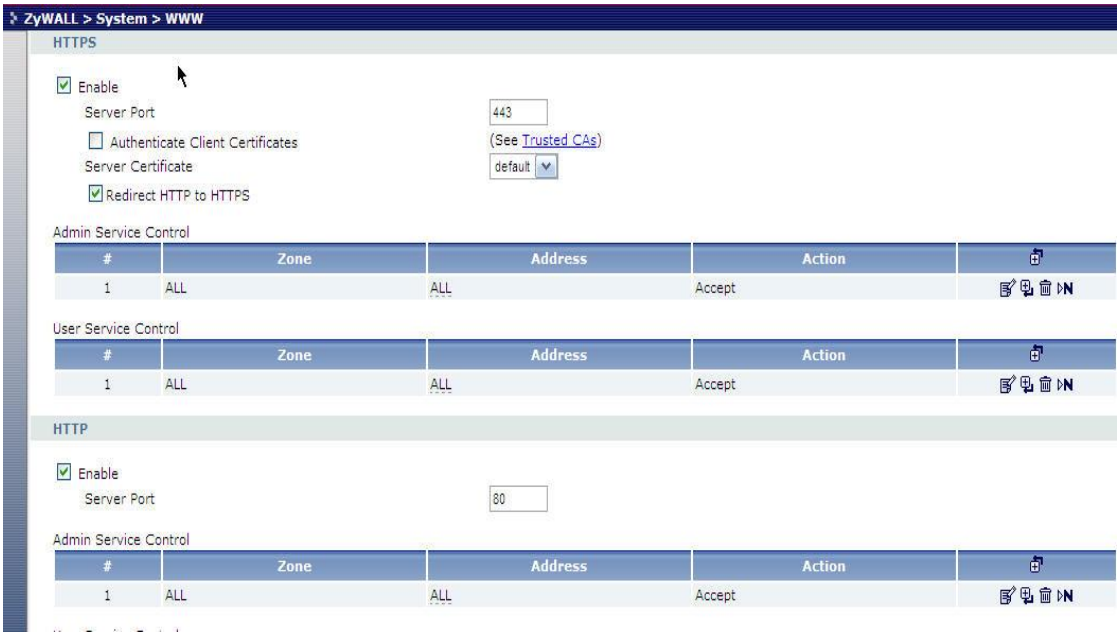
You can connect your PC to ZyWALL USG port 1 interface with Ethernet cable, which is most left Ethernet port. You will get the IP address automatically from DHCP by default. Connect to http://192.168.1.1 using web browser to login ZyWALL USG for management. The default administration username is "**admin**", and password is "**1234**".

A02. Why can't I login into ZyWALL USG?

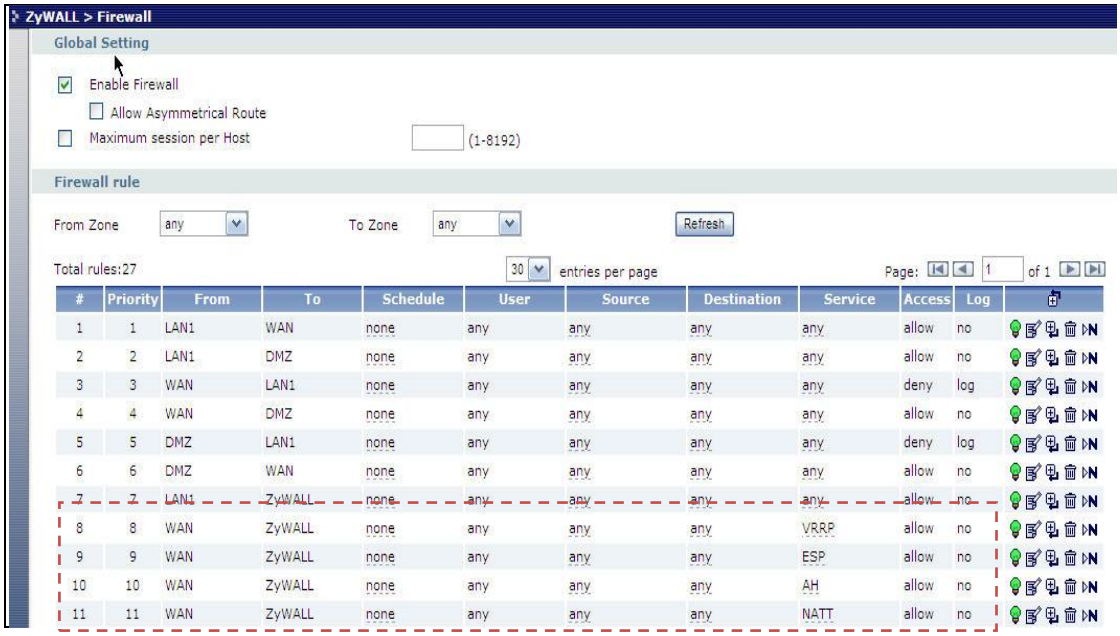
There may have several reasons why you can't login to ZyWALL USG:

1. The ZyWALL USG supports the following types of browsers. Check if you are not using other type of browser.
   - IE 6.0 or above
   - Firefox 1.5.0 or above
   - Netscape 7.2 or above
2. To login ZyWALL USG's GUI, it's mandatory to enable JavaScript and accept cookies in your web browser. Check if you don't have them disabled in the web browser. If you do, enable them.
3. To login ZyWALL USG's GUI, a popup window function in web browser is used. Check if you have the popup windows block enabled in the web browser. If so, please disable the block in the web browser.
4. You may be entering wrong username or password.
5. You might have typed a wrong password for over 5 times. ZyWALL USG blocks login from such an IP address for 30 minutes by default.
6. You can be connecting to ZyWALL USG from a WAN interface which is blocked by default. If you don't want this block rule, go to GUI menu **System** > **WWW** to set to **accep**t the access **from 'WAN' or from 'All'.**

   Then switch to menu Firewall > **To-ZyWALL rules** to add the HTTP access from WAN side.



Note: By default, Firewall blocks all the access except the traffic like VRRP, IPSec ESP, IPSec AH, IPSec NATT, IPSec IKE.



A03. What's difference between "Admin Service Control" and "User Service Control" configuration in GUI menu System > WWW?

The "Admin Service Control" configuration is for controlling user login with admin user-type to perform management task including **Admin** and **Limited-Admin**. And "User Service Control" configuration table is for controlling user login with access user-type to perform user access task including **User** and **Guest**.

A04. Why ZyWALL USG redirects me to the login page when I am performing the management tasks in GUI?

There may be several reasons for ZyWALL USG to redirect you to login page when you are doing configuration.

1. Admin user's re-auth time (force re-login time) has reached. The default time value is 24hours.
2. Admin user's lease time has been reached. The default time value is 24hours.
3. You are trying to login ZyWALL USG using other remote management client (telnet or ssh…etc) after you logged in ZyWALL USG using a web browser.
4. PC's IP address has changed after your previous login. The re-login is required then.

A05. Why do I lose my configuration setting after ZyWALL USG restarts?

There may have two reasons:

1. If you configure ZyWALL USG from CLI. You must type CLI "**write**" to save the configuration before rebooting. If you configure ZyWALL USG from GUI, any configuration will be automatically saved.
2. ZyWALL USG might fail to apply the configuration using the startup-config.conf when booting up. It might because the startup-config.conf is corrupted. If so, ZyWALL USG will try to use the last boot up configuration file (lastgood.conf), which can boot up successfully. Your settings will revert to the last boot up configuration.

A06. How can I do if the system is keeping at booting up stage for a long time?

There are two reasons if your ZyWALL USG boots up for a long time as below.

1. It might because you have many configurations on ZyWALL USG. For example,

you configured over 500 VPN settings. Please connect to console and you can see which process the system is processing at.
Note: If the system is processing ok, admin can connect to ZyWALL USG's lan1 port which is with IP address 192.168.1.1 by default.

2. The ZyWALL USG may get firmware crashed. Generally, it may happen if power off ZyWALL USG when it's during firmware upgrading. For this case, admin could connect to console and see the message as shown below (ensure your terminal baud rate is configured correctly).

If you do see the message, please start the firmware recovery procedure as following steps.
1. Connect a PC with ZyWALL USG's lan1 port via an Ethernet cable.
2. ftp 192.168.1.1 from your FTP client or MS-DOS mode
3. Set the transfer mode to binary (use "bin" in the Windows command prompt).
4. Reload the firmware. (ex. use command "put 1.00(XL.1)C0.bin" to upload firmware file)
5. Wait the FTP uploading completed and it will restart the ZyWALL USG automatically.

B. Registration FAQ

B01. Why do I need to do the Device Registration?

You must first register ZyWALL USG device with myZyXEL.com server, before you activate and use IDP and Content filter external rating service.

B02. Why do I need to activate services?

It's mandatory to activate these security services before you enable and use these services. For IDP and the content filter, you need to activate services first before you can update the latest signatures from myZyXEL.com update server.

B03. Why can't I active trial service?

You must make sure that your device can connect to internet first. Then register ZyWALL USG device with myZyXEL.com server through GUI menu Registration page.

B04. Will the UTM service registration information be reset once restore configuration in ZyWALL USG back to manufactory default?

Yes. Both the device configuration and UTM service registration, e.g. AV/IDP/CF, will be erased once the user reset the device configuration back to manufactory default. However, the service subscription information can be recovered by following the procedures as:

1. Next time device synchronization with myZyXEL.com.
2. User click "Service License Refresh" button from ZyWALL > Licensing > Registration > Service page.

C. File Manager FAQ

C01. How can ZyWALL USG manage multiple configuration files?

From ZyWALL USG GUI menu File Manager > Configuration File, it allows admin to save multiple configuration files. Besides, Admin could “manipulate” files, such as to upload, delete, copy, rename, download the files, and apply a certain file to hot-switching the configuration without hardware reboot.

C02. What are the configuration files like startup-config.conf, system-default.conf and lastgood.conf?

1. **startup-config.conf**: The startup-config.conf is ZyWALL USG system configuration file. When ZyWALL USG is booting, it will use this configuration file for ZyWALL USG as system configuration.
2. **system-default.conf**: The system-default.conf is ZyWALL USG system default configuration file. When you press the reset button, ZyWALL USG will copy system-default.conf over startup-conf.conf.
3. **lastgood.conf**: The lastgood.conf is created after ZyWALL USG successfully applies startup-config.conf. And ZyWALL USG will try to apply lastconfig.conf, if ZyWALL USG fail to apply startup-config.conf. You can check the GUI menu **Maintenance** > **Log** to check the configuration applied status after booting.

Please note the configuration file downloaded through web GUI is text-based which is readable and is very useful for administrator to have a quick overview for the detailed configuration.

C03. Why can’t I update firmware?

It’s mandatory to have at least 70MB free memory before upgrade firmware. If you still can’t get enough memory to upgrade firmware, you can perform upgrade after system reboot which frees up the memory.

C04. What is the Shell Scripts for in GUI menu File manager > Shell Scripts?

Shell scripts are files of commands that you can store on the ZyWALL and run when you need them. When you run a shell script, the ZyWALL only applies the commands that it contains. Other settings do not change.

C05. How to write a shell script?

You can edit shell scripts in a text editor and upload them to the ZyWALL USG through GUI menu **File manager** > **Shell Script** tab. Some notes as followings.

- Must follow ZyWALL USG CLI syntax
- Must add "**configure terminal**" at the beginning of the script file.
- Must save as a ".zysh " file extension.

An example is shown below.

```
# enter configuration mode
configure terminal
# change administrator password
username admin password 4321 user-type admin
# add a user 'anne' and set both the lease and re-auth time to 1440 sec.
username anne user-type ext-user
username anne description External User
username anne logon-lease-time 1440
username anne logon-re-auth-time 1440
exit
write
```

C06. Why can't I run shell script successfully?

Please ensure that you follow the correct CLI command syntax to write this script. And make sure that you add the "**configure terminal**" in the top line of this script file.

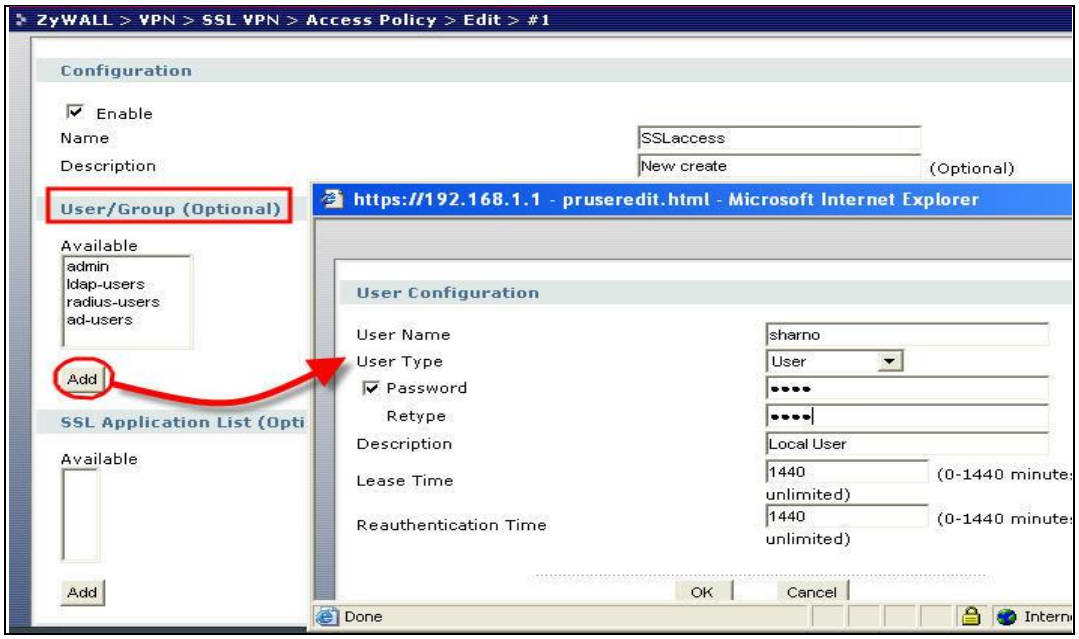
D. Object FAQ

D01. Why does ZyWALL USG use object?

ZyWALL USG object include address, service, schedule, authentication method, certificate, zone, interface group and ISP account object. The ZyWALL USG uses object as a basic configuration block. It can simplify the configuration change once your have some change in the network topology.

For example, User can first create a zone object WAN_ZONE with the WAN1 interface and later add the wan2 interface into WAN_ZONE. All security features that use the WAN_ZONE will change their configuration immediately according to zone object WAN_ZONE change.

We also provide a feature call “in-line object create”, this feature can let you create an object without leaving the original page, for example, during the time creating an Access Policy for SSL VPN, you can simply click the “Add” button, it will pop-up a new windows and link to “User Configuration” page, therefore you don’t have to leave the page you are configuring access policy.



D02. What's the difference between Trunk and the Zone Object?

The trunk concept is used as an interface group for a policy routing. You can add interfaces and define load balance mechanisms in one trunk.

The zone concept is used to group multiple of interfaces, which have the same security policy. For example, you can define two zones, LAN and WAN, and add a firewall rule to control the traffic between LAN and WAN.

D03. What is the difference between the default LDAP and the group LDAP? What is the difference between the default RADIUS and the group RADIUS?

Default LDAP/RADIUS server is a built-in AAA object. If you only have one LDAP/RADIUS server installed, all you need to do is to setup the default LDAP/RADIUS and then select group ldap/radius into authentication method. If you have several redundant LDAP/RADIUS servers, you may need to create your own LDAP/RADIUS server groups. But don't forget selecting the LDAP/RADIUS server groups in the authentication method chosen for authenticating.

E. Interface FAQ

E01. How to setup the WAN interface with PPPoE or PPTP?

First, you need to create an ISP account, which has protocol type of PPPoE or PPTP. Then you need to create PPP interface on GUI menu **Interface** > **PPPOE/PPTP**. You can name this PPP interface, for example 'ppp0' (you can have ppp0~ppp11 ppp interface, ppp12 is reserved to modem dialup interface). After that, you need to create a policy route, which has next-hop interface set to ppp0.

E02. How to add a virtual interface (IP alias)?

To add a virtual interface, go to GUI menu **Interface** > **Ethernet**, click the "+" icon on each interface row. For example, I want to add a virtual interface of lan1. click the "+" icon from the interface lan1 row, and fill out the necessary fields. It will create the virtual interface, lan1:1.

E03. Why can't I get IP address via DHCP relay?

It requires special support from a DHCP server. Some DHCP servers would check special fields in a DHCP discover/request and it is possible for the servers to not to respond them. So make sure your DHCP server supports DHCP relay.

E04. Why can't I get DNS options from ZyWALL's DHCP server?

There could be several reasons. If you configure a static IP on a WAN interface, you should have custom defined DNS servers in the LAN interface or there would be no way to get DNS servers from ISP. If the interface that provides the DNS server goes down, the DNS server would be regarded as dead one and won't pass it to the LAN PCs. So make sure all the interfaces that provide DNS server don't go down because of link down, ping-check or becoming disabled.

E05. Why does the PPP interface dials successfully even its base interface goes down?

The base interface is just a reference which ZyWALL uses to connect to PPP server. If you have another active interface/routes, ZyWALL will try to maintain connectivity.

Routing and NAT FAQ

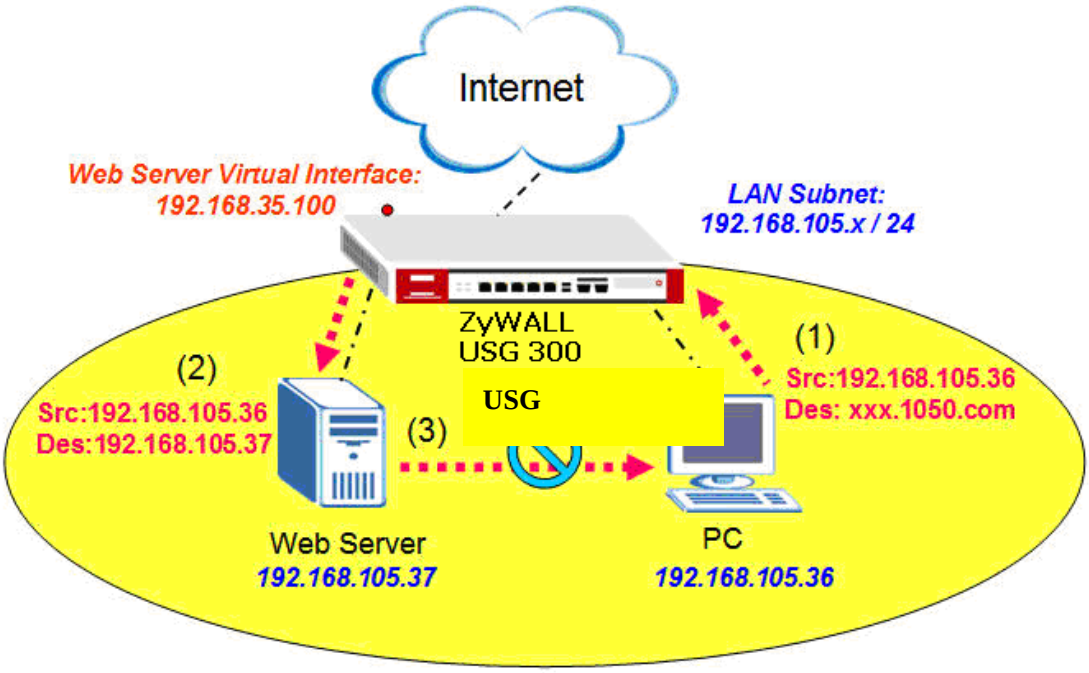
F01. How to add a policy route?

From the GUI menu **Policy** >**Route**, click the "+" icon in the table and define matching Criteria for this route. Then select a next-hop type. If you want to use Link HA and Load Balance, "Trunk" should be selected as a next-hop type. If you want to route traffic into an IPsec tunnel, you need to select "VPN tunnel". Please note that the policy routes will be matched in order. If the first route matches the criteria, ZyWALL USG will use the route setting to direct the traffic to the next hop.

F02. How to configure local loopback in ZyWALL USG?

Local loopback is a feature used in the following scenario.

For a general application the users access to the web service by entering the FQDN (Full Qualify Domain Name, e.g. http://www.zyxel.com) other than an IP address. This is because the domain name is easier to remember. However, when both the Server and Client are located behind the same NAT, a triangle route problem will encounter. See the example as illustrated below to understand the network topology: (Here a Web server is used as an example.)



1. The internal user enter the URL and the DNS client in the computer queries the domain name "xxx.USG2000.com" from the public DNS server and retrieves the Web

server's 1-1 NAT mapping public IP address- 192.168.35.100.

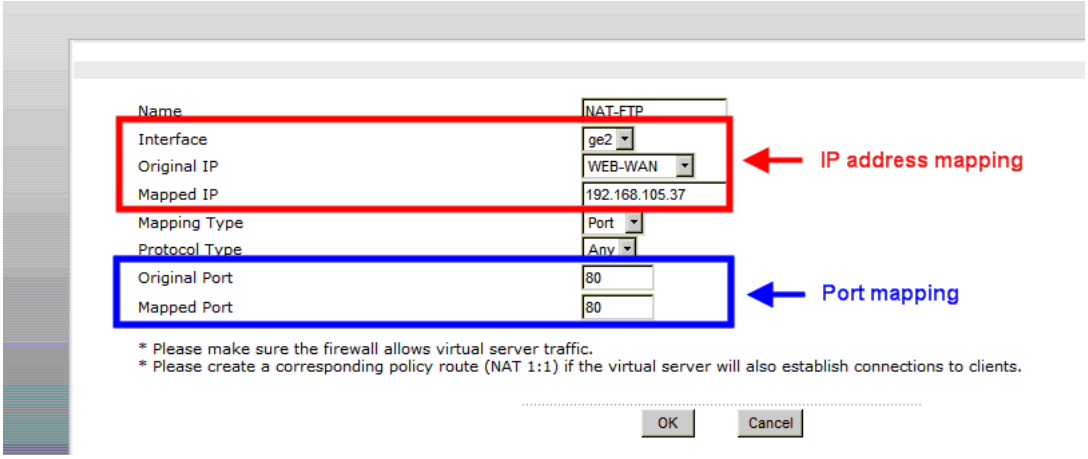
2. From the Virtual Server setting, ZyWALL USG forwards it to the internal IP 192.168.105.37.

3. The Web server receives a request from the same subnet and replies it directly to PC through L2 switch dispatching. This is known as "triangle route".

Please follow these steps to configure the ZyWALL USG in order to solve the triangle route problem:

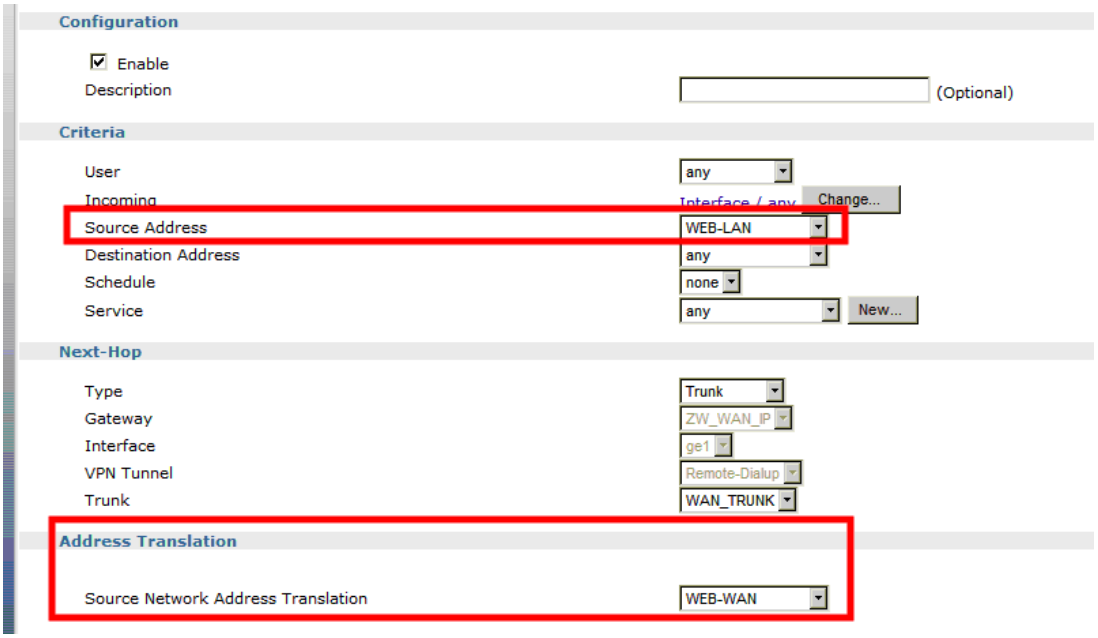
1-1 NAT mapping Configuration:

Firstly create two address object: WEB_WAN as 192.168.35.100 and WEB_LAN as 192.168.105.37. After that, create the Virtual Server rule of incoming DNAT translation to allow the server connect to outside network.



Create one Policy Route rule for outgoing SNAT to translate the private IP to public one.

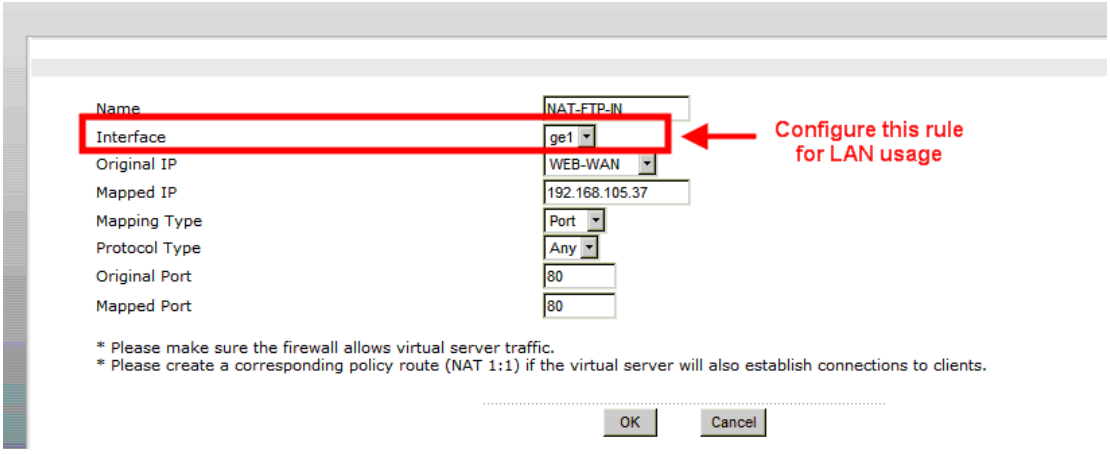
After these two steps, the 1-1 NAT mapping on ZyWALL USG is complete.



NAT loopback Configuration

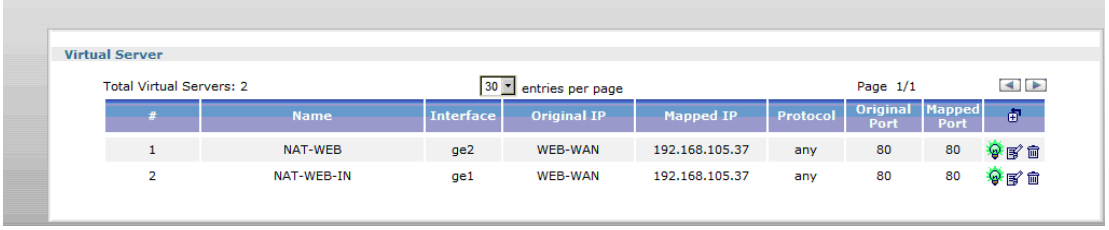
In order to run the NAT loopback on ZyWALL USG, please add these rules after you finish the 1-1 NAT mapping.

Firstly, add one Virtual Server rule for LAN usage. All the parameters are the same as those set on 1-1 NAT mapping, except the Interface item.

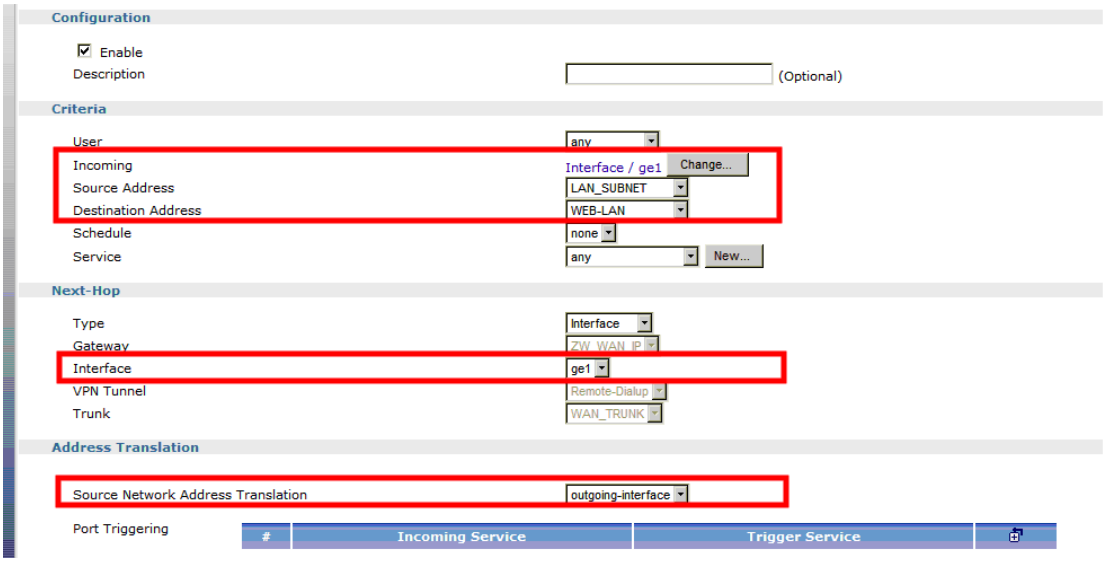


In total there are two Virtual Server rules in this case.

If you put the Web Server on DMZ and access from the LAN, this configuration will do as you requested. However, if you put the Web Server on LAN and access from the LAN, you need another Policy Route rule to realize it.



This Policy Route rule makes all the internal access must do the SNAT translation. This will force all the traffic to go back to the ZyWALL USG and avoid the triangle route problem.



Certainly, the related configuration like the Firewall ACL check must be set.
After the configuration is done, the LAN users are able to access the LAN server by typing FQDN.

F03. How to configure a NAT?

Unlike ZyNOS ZyWALL, the NAT setting in ZyWALL USG is in Policy Route and port forwarding setting is Virtual Server as the configuration page is shown below.

- Configure NAT setting in **Configuration** > **Policy** > **Route**
- Configure port forwarding setting in **Configuration** > **Virtual Server**

In the policy route setting, there is the source network address translation (SNAT) setting is at Address Translation area. Choose 'none' means to turn off the NAT feature for the policy route rule accordingly. To choose "outgoing-interface" or other

address object you defined, it means turn on the NAT feature and it will refer to the next-hop setting to execute routing.

For the specific traffic needs to be re-directed to a certain internal server, the virtual server needs to be configured. This feature allows ports/host mapping from a WAN interface IP to an internal DMZ/LAN IP. For example, if you want to forward HTTP traffic with 8080 port to the ZyWALL5 in ZyWALL USG's DMZ zone, you need to configure virtual server to forward <Original IP(ex. WAN1's IP):8080> to <Internal server IP:8080>.

F04. After I installed a HTTP proxy server and set a http redirect rule, I still can't access web. Why?

Your proxy server must support a transparent proxy. If your proxy does have this feature, turn it on. For example, for Squid, you have to have the option httpd_accel_uses_host_header enabled.

F05. How to limit some application (for example, FTP) bandwidth usage?

In order to restrict the bandwidth usage for a specific application, you need to employ AppPatrol feature.
The following steps allow the user to limit the bandwidth usage from of FTP application:
1. Pick up the FTP application that you want to restrict bandwidth usage and click "Edit" in AppPatrol > Common page.
2. Click the "Edit" button for default policy, and the "Configuration" page appears.
3. On the "Configuration" page, enter the bandwidth amount you want to limit bandwidth usage in direction "Inbound" or "Outbound".
4. Back to "General" page under AppPatrol and check the "Enable BWM" checkbox then click the "Apply" button to complete the entire configuration.

Note. On the ZLD 1.0 the default setting of bandwidth management is ON and you cannot change the setting, but on the ZLD 2.0 the default setting of bandwidth management is off, therefore if you are upgraded from 1.0 to 2.0, the "Enable BWM" checkbox will be checked.

F06. What's the routing order of policy route, dynamic route, and static route and direct connect subnet table?

All these routing information create the ZyWALL USG routing database. When routing, ZyWALL USG will search with the following order:

1. Local and direct connect subnet table.
2. Policy route rule.
3. Main table, which includes routes learned from RIP/OSPF, static routes and default routes.

F07. Why ZyWALL USG cannot ping the Internet host, but PC from LAN side can browse internet WWW?

This is mainly caused by your interface configuration. If you setup two WAN interfaces, which have gateway IP address configured, the default route will have two entries added in ZyWALL USG. If one of the WAN interfaces can't connect to the internet (for example, ppp interface don't dialup successfully), and this interface has smaller metric than the other WAN interface, ZyWALL USG will select this as default route and traffic can't go out from the ZyWALL USG.

F08. Why can't I ping to the, Internet, after I shutdown the primary WAN interface?

ZyWALL USG routes packets by checking session information first. Once packet matched a session that is already created, it would not lookup the routing table. So the interface status change doesn't affect the routing result until a new session is created. If you continually ping internet host and shutdown the ZyWALL USG primary WAN interface, the ping packet still matches the original session, which is bound to primary WAN interface already. The session timeout for ICMP is 15 second.

F09. Why the virtual server or port trigger does not work?

If virtual server or port trigger (or any traffic from WAN zone to LAN zone) doesn't

work, check whether the firewall rule from WAN to LAN is disabled.

F10. Why port trigger does not work?

The port trigger will work only when there is a connection matching that policy route rule. Please note that firewall may block those triggered services. So, if you have problems with triggering the service, check firewall settings and its logs too.

F11. How do I use the traffic redirect feature in ZyWALL USG?

If you have a router located in LAN, you could regard the router as a gateway and fill its address in a gateway field of the LAN interface which connects to the LAN router. Then, configure the interface as a passive member of the trunk which you use in the policy routing. In case all main links in the trunk go down, passive link (i.e. the LAN router) would be activated to maintain the connectivity.

Note: While you configure the gateway address in the interface, please also choose a suitable metric for the gateway or it would interfere with main links.

F12. Why can’t ZyWALL learn the route from RIP and/or OSPF?

ZyWALL blocks RIP/OSPF routing advertisement from WAN/DMZ by default. If you find that it fails to learn the routes, check your firewall to-ZyWALL rules.

G. VPN and Certificate

G01. Why can't the VPN connections dial to a remote gateway?

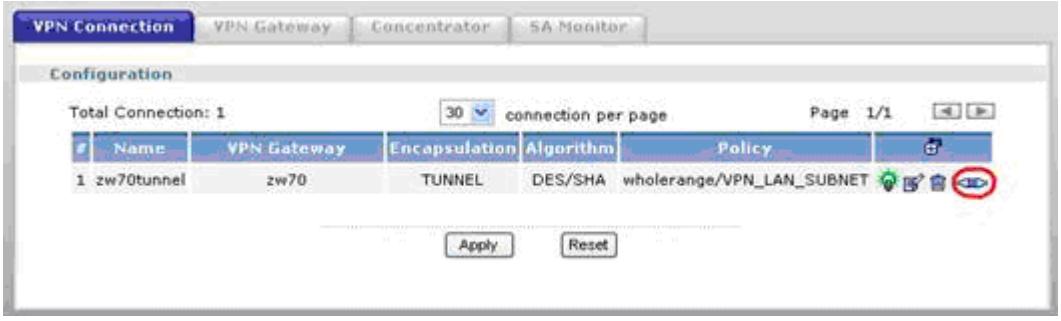
Please check the responder's logs whether the fail occurs in phase 1 or phase 2. If the phase 1 has failed, try to check the VPN gateway configuration, such as proposals or Local/Remote ID. If the phase 2 has failed, try to check the VPN connection configuration, such as whether the policy matches the one of the remote gateway.

G02. VPN connections are dialed successfully, but the traffic still cannot go through the IPsec tunnel.

Check if there is a policy route that directs the traffic into the VPN connection. After the policy route is set, if the traffic still goes through another route path, check the order of policy routes.

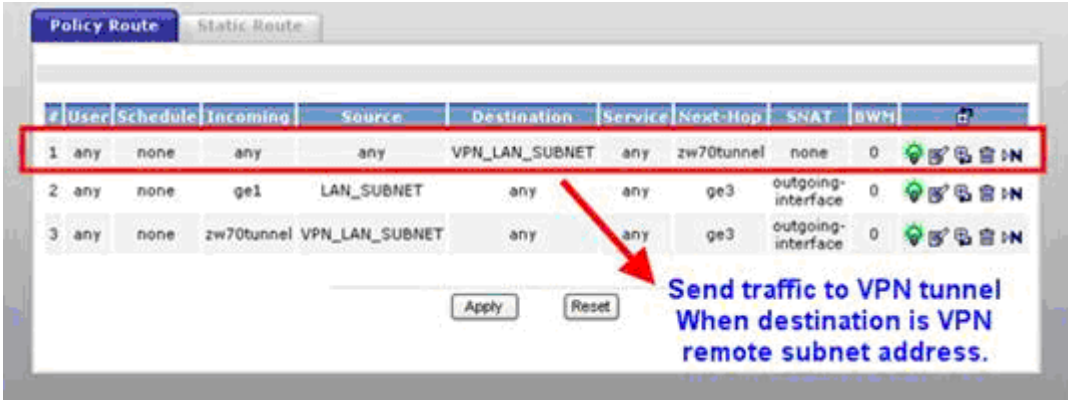
G03. Why ZyWALL USG VPN tunnel had been configured correctly and the VPN connection status is connected but the traffic still can not reach the remote VPN subnet?

ZyWALL USG VPN traffic is the route base VPN, this means we need to configure a policy route rule to guide the ZyWALL USG how to route the VPN traffic to the VPN remote subnet. We can check if our VPN parameter setting is working by clicking connect icon after VPN tunnel has configured in both gateway. The VPN connection status showed below is connected.



We need a policy route to notify the ZyWALL USG send the packet to VPN tunnel when the packet's destination address is VPN remote subnet. Please switch to

ZyWALL USG GUI > Configuration > Policy > Route > Policy Route and check if there is a rule that direct the traffic to VPN tunnel. The VPN tunnel candidates must be preconfigured in VPN connection menu.



The traffic from local subnet can send to VPN remote subnet and get reply successfully after configured VPN tunnel and policy route.

G04. VPN connections are dialed successfully, and the policy route is set. But the traffic is lost or there is no response from remote site.

There are two possibilities. One is that the traffic is blocked by firewall, Anti-Virus, Anti-Spam, IDP…etc. Please check the configuration of these services or search the related dropped logs. Another option is that the remote gateway doesn't know how to route the replied traffic. Please check the route rules of the remote gateway.

G05. Why don’t the Inbound/Outbound traffic NAT in VPN work?

Check the modified traffic for whether the outbound traffic SNAT still matches the VPN connection policy. If the traffic doesn't match the policy and the policy enforcement is active, it will be dropped by the VPN. For Inbound traffic SNAT/DNAT, check if there is a directly connected subnet or a route rule to the destination.

H. Firewall FAQ

H01. Why doesn't my LAN to WAN or WAN to LAN rule work?

There may be some reasons why firewall doesn't correctly constrain the access.

1. The WAN zone doesn't include all WAN interfaces. For example, if you create a PPPoE interface, you need to add this ppp interface into the WAN zone.
2. The firewall rules order is not correct. Since firewall search firewall rules in order, it will apply the first firewall rule that matches criteria.

H02. Why does the intra-zone blocking malfunction after I disable the firewall?

Intra-zone blocking is also a firewall feature. If you want to have intra-zone blocking working, please keep the firewall enabled.

H03. Can I have access control rules to the device in firewall?

If your ZYWALL USG image is older than b6, the answer is No. Firewall only affects the forwarded traffic. You need to set the access control rules in system for each service such as DNS, ICMP, WWW, SSH, TELNET, FTP and SNMP. After b6 image, user can configure to-ZyWALL rules to manage traffic that is destined to ZyWALL.

I. Application Patrol FAQ

I01. What is Application Patrol?

Application Patrol is to inspect and determine the application type accurately by looking at the application payload, OSI layer 7, regardless of the port numbers.

.

I02. What applications can the Application Patrol function inspect?

AppPatrol on ZyWALL USG supports four categories of application protocols at the time of writing.

1. General protocols -- HTTP, FTP, SMTP, POP3 and IRC.
2. IM category -- MSN, Yahoo Messenger, AOL-ICQ, QQ
3. P2P category -- BT, eDonkey, Fasttrack, Gnutella, Napster, H.323, SIP, Soulseek
4. Streaming Protocols -- RTSP (Real Time Streaming Protocol)

Note: The applications support is not configurable (add or remove).

Protocol Type	Protocol	Application Type/Version	Action Block	Block of Access	BWM over the Application
Common	FTP	Filezilla 2.2.18, 2.2.19 (Active)	Protocol detect	Yes	Yes
Common	FTP	Filezilla 2.2.18, 2.2.19 (Passive)	Protocol detect	Yes	Yes
Common	HTTP	IE 6	Protocol detect	Yes	Yes
Common	HTTP	Firefox 2.0, 1.5	Protocol detect	Yes	Yes
Common	IRC		Protocol detect	Yes	Yes
Common	POP3	Outlook Express 6	Protocol detect	Yes	Yes
Common	SMTP	Outlook Express 6	Protocol detect	Yes	Yes
IM	aol-icq	ICQ 5.1	audio	Yes	No
IM	aol-icq	ICQ 5.1	video	Yes	No
IM	aol-icq	ICQ 5.1	file transfer	Yes	No
IM	aol-icq	ICQ 5.1	Login	Yes	No
IM	aol-icq	ICQ 5.1	Message	Yes	No
IM	jabber	Google Talk 1.0	Login	Yes	No
IM	msn	7.5, 8.0	audio	Yes	Yes
IM	msn	7.5, 8.0	file transfer	Yes	Yes
IM	msn	7.5, 8.0	Login	Yes	No
IM	msn	7.5, 8.0	Message	Yes	No
IM	msn	7.5, 8.0	video	Yes	Yes

IM	qq	QQ2006, QQ2007Beta	Login	Yes	No
IM	Web-MSN	NA (Web Application)	Login	Yes	No
IM	Yahoo	8.1.0.195	audio	Yes	Yes
IM	Yahoo	8.1.0.195	file transfer	Yes	Yes
IM	Yahoo	8.1.0.195	Login	Yes	No
IM	Yahoo	8.1.0.195	Message	Yes	No
IM	Yahoo	8.1.0.195	video	Yes	Yes
P2P	bittorrent	Bitcommet 0.79	Protocol detect	Yes	Yes
P2P	eDonkey	emule 0.47c; Vagaa	Protocol detect	Yes	No
P2P	ezpeer	EzPeer Plus 1.0	Login	Yes	No
P2P	fasttrack	Kazaa 3.2	Login	Yes	No
P2P	Gnutella	LimeWire 4.12, Foxy 1.9	Protocol detect	Yes	Yes
P2P	kad	emule 0.47c; Vagaa	Protocol detect	**Yes***	No
P2P	kuro	KuroBang	Login	Yes	No
P2P	poco	Poco 2006	Protocol detect	Yes	No
P2P	pplive	PPLive 1.7.26	Protocol detect	Yes	Yes
P2P	qqlive	QQLive 3.5	Protocol detect	Yes	Yes
IM	rediff	Rediff 8.0	Login	Yes	No
IM	rediff	Rediff 8.0	Message	Yes	No
IM	rediff	Rediff 8.0	audio	Yes	No
IM	rediff	Rediff 8.0	video	Yes	No
IM	rediff	Rediff 8.0	file transfer	Yes	No
P2P	soulseek	Soulseek 156/157test8	Protocol detect	Yes	No
P2P	thunder	Thunder 5.5	Protocol detect	Yes	Yes
Streaming	Rtsp	RealMedia Player v6.0	Protocol detect	Yes	No
VoIP	H323	Netmeeting 3.01	Protocol detect	Yes	Yes
VoIP	SIP	Windows Messenger 5.1	Protocol detect	Yes	Yes
VoIP	SIP	Gizmo 3.0	Protocol detect	Yes	Yes

I03. Why does the application patrol fail to drop/reject invalid access for some applications?

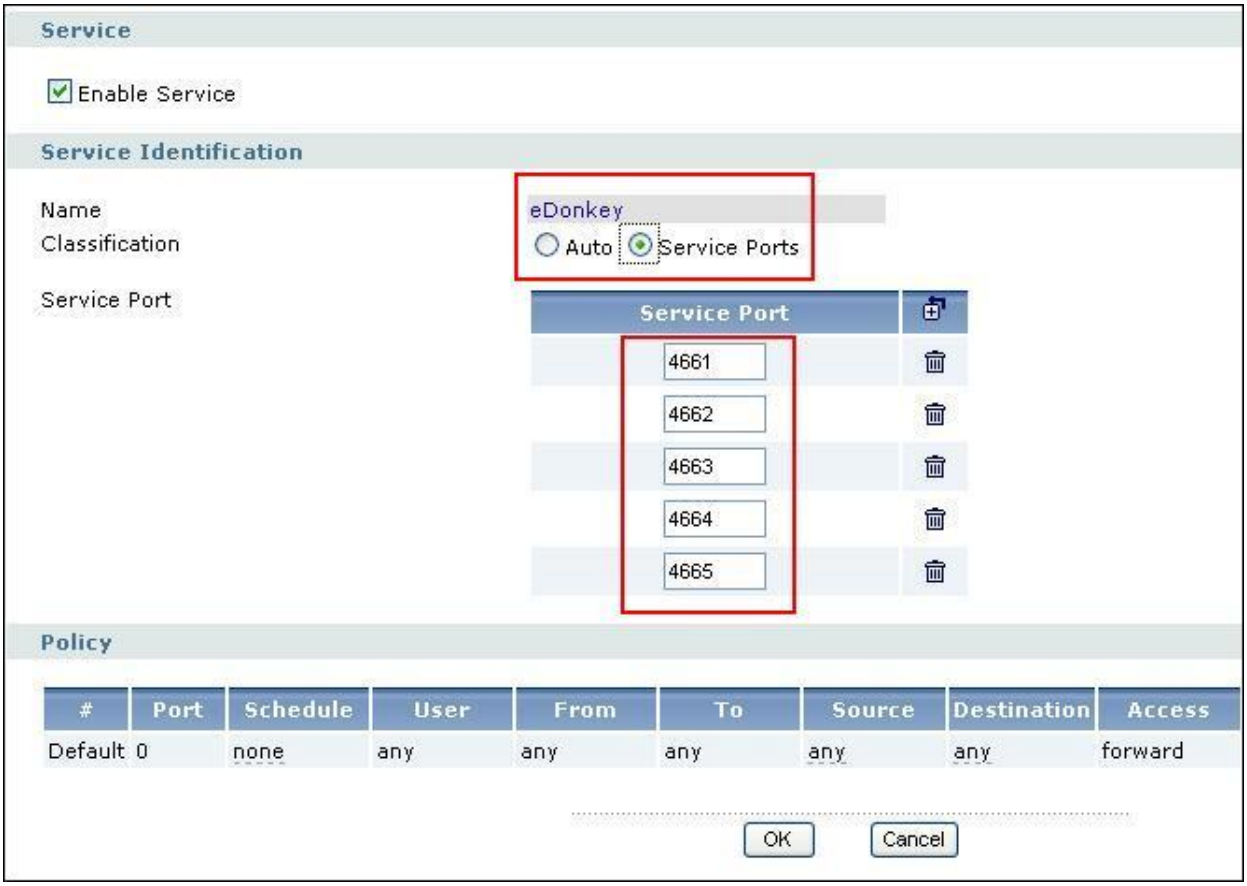
There are two possible reasons for this problem. One is that this application version is not supported by the Application Patrol (please refer to Application Patrol Support List). The other is that the Application Patrol needs several session packets for the application identification. After the session is identified successfully (or it can't be identified), specified action is taken. If the session is terminated before being identified, application patrol won't take any action. But it seldom happens.

I04. What is the difference between "Auto" and "Service Ports"

settings in the Application Patrol configuration page?

If the user selects “Auto”, the ZyWALL inspects packet by OSL layer 7(signature pattern). By selecting “Service Ports”, the ZyWALL inspects the incoming packet based on layer 4. By default, “Auto” will be selected once an AppPatrol rule is enabled. Please refer to the following information in advance to use “Service Ports” option:

(1) Defines the port used in ZyWALL USG. For easy configuration purpose, the ZyWLL has been pre-configured for the frequent use service port. For example: eDonkey service is pre-defined to take action on port 4661 ~ 4665 as shown below.



(2) It could be used when user want to apply bandwidth control for certain allowed or rejected application (which is in Application Patrol support list).

(3) Since the “Service Port” performs up to OSI layer 4 inspections, so the system performance would be better than the “Auto” inspection (layer 7). Therefore, if the user concerns about system performance or user’s network environment is simple, the

"Service Ports" setting could be the choice.

I05. What is the difference between BWM (bandwidth management) in Policy Route and App. Patrol ?

There are two places to set BWM policies:
1. Policy Route – The rule of Policy Route supports Outbound BWM only.
2. App. Patrol – App. Patrol supports both Outbound BWM and Inbound BWM.
If a traffic matches the BWM rules of both Policy Route and App. Patrol, Policy route will be applied on the traffic.

I06. Do I have to purchase iCards specifically for using AppPatrol feature?

AppPatrol can be free for usage.
Pre-Condition & Usage:
AppPatrol packet inspection mechanism relays on signature pattern if you select "auto" mode, which is also employed by IDP feature. You can have the signature download from subscribing IDP/AppPatrol trial service. During the trial period, you can download the signature. After trial program expired, you will no longer able to update the signature unless you subscribe the IDP UTM service (Note: Purchase of IDP iCard is required). However, you still can use AppPatrol feature without signature update. (Remark: New application may not be detected if signature is not updated.)

I07. Can I configure different access level based on application for different users?

Yes, you can configure different access level for different users, for example, you can configure the RD team have the rights to using MSN but only have rights to chat, they cannot transfer files. The managers will have full access rights, but the Guests have no rights to using MSN even login.

I08. Can I migrate AppPatrol policy and bandwidth management control from ZLD1.0x to ZLD2.0x?

No, as the new ZLD platform 2.0x enhances zone-to-zone mechanism which is not capable to migrate into new AppPatrol. Therefore, the user will be required to reconfigure the related setting after complete firmware upgrade.

J. IDP FAQ

J01. Why doesn't the IDP work? Why has the signature updating failed?

Please check if your IDP services are activated and are not expired.

J02. When I use a web browser to configure the IDP, sometimes it will popup "wait data timeout".

For current release, when you configure IDP and enable all the IDP rules at the same time, you may see the GUI showing "wait data timeout". This is because GUI can't get the IDP module setting result for a period of time, even if the configuration of ZyWALL USG is correct.

J03. When I want to configure the packet inspection (signatures), the GUI becomes very slow.

We suggest you had better use "Base Profile" to turn on/off signatures.

J04. After I select "Auto Update" for IDP, when will it update the signatures?

After applying "Auto Update", ZyWALL USG will update signatures Hourly, Daily, or Weekly. But updating will occur at random minute within the hour specified by user.

J05. If I want to use IDP service, will it is enough if I just complete the registration and turn on IDP?

Please ensure to activate the "protected zone" you would like to protect and configure the action for attack of the "protected zone" in the related IDP profile is others than

"none".

J06. What are the major design differences in IDP in ZLD1.0x and latest IDP/ADP in ZLD2.0x?

The following are 3 major differences made from ZLD2.0x 2000:

IDP-Inspects via. Signature

An IDP system can detect malicious or suspicious packets and respond instantaneously. It is designed to detect pattern-based attacks.

The signature is designed for IDP in the purpose of detecting pattern-based attacks.
If a packet matches a signature, the action specified by the signature is taken. You can change the default signature actions in the profile screens.

You can create custom signatures for new attacks or attacks peculiar to your network. Custom signatures can also be saved to/from your computer so as to share with others.

ADP-Anomaly

An ADP (Anomaly, Detection and Prevention) system can detect malicious or suspicious packets and respond instantaneously. It can detect:

- Anomalies based on violations of protocol standards.
- Abnormal flows such as port scans.

ADP on the ZyWALL protects against network-based intrusions. You can also create your own custom ADP rules.

System Protection

System Protection System offers the ZyWALL ability to protect itself against host-based intrusions. ZyXEL can prevent not only network intrusions but also host-based instructions.

Zone to Zone Protection

A zone is a combination of ZyWALL interfaces for security. Traffic direction is defined by the zone the traffic is coming from and the zone the traffic is going to.
The ZyWALL can inspect the traffic from different sources. Therefore, the malicious/suspicious packets from WAN to LAN and the traffic coming from DMZ to

LAN will be treated differently.

J07. Does IDP subscription have anything to do with AppPatrol?

AppPatrol can be free for usage if the user registers the IDP trial license firstly. Due to AppPatrol requires the IDP signatures to identify the application type, by registration to the trial program, the user can use AppPatrol as well to update signatures during the trial period. Once the trial license expires the user can still use the AppPatrol feature but is no longer able to update signatures. AppPatrol is independent from IDP, both features can be turned on or off independently.

IDP/ADP Comparison	IDP	ADP	System Protection
L7 Inspection to Stop Threats & Attacks	Yes	No	Yes
Signature Update	Yes	No	Yes
TA/PA	No	Yes	No
Protecting ZyWALL Itself	No	Yes	Yes
Requiring iCard Subscription	Yes	No	No
	TA: Traffic Anomaly *PA: Protocol Anomaly*		

J08. How to get a detailed description of an IDP signature?

The detailed IDP signature description can be retrieved either by visiting MySecurityZone or by clicking the hyper link in the log.

J09. After an IDP signature updated, does it require ZyWALL to reboot to make new signatures take effect?

No, it is not necessary to reboot the device to make new signatures take effect.

Content Filter FAQ

K01. Why can't I enable external web filtering service? Why does the external web filtering service seem not to be working?

Enabling this feature requires the registration with myZyXEL.com and service license. If your service is expired, the feature would be disabled automatically.

K02. Why can't I use MSN after I enabled content filter and allowed trusted websites only?

MSN messenger tends to access various websites for internal use and if it can't access these websites, the login fails. If allowing trusted websites only is enabled and the websites that MSN messenger wants to access are not in the trusted website, access would be blocked. If you really want this option enabled, you have to add these websites in the trusted websites list.

L. Device HA FAQ

L01. What does the “Preempt” mean?

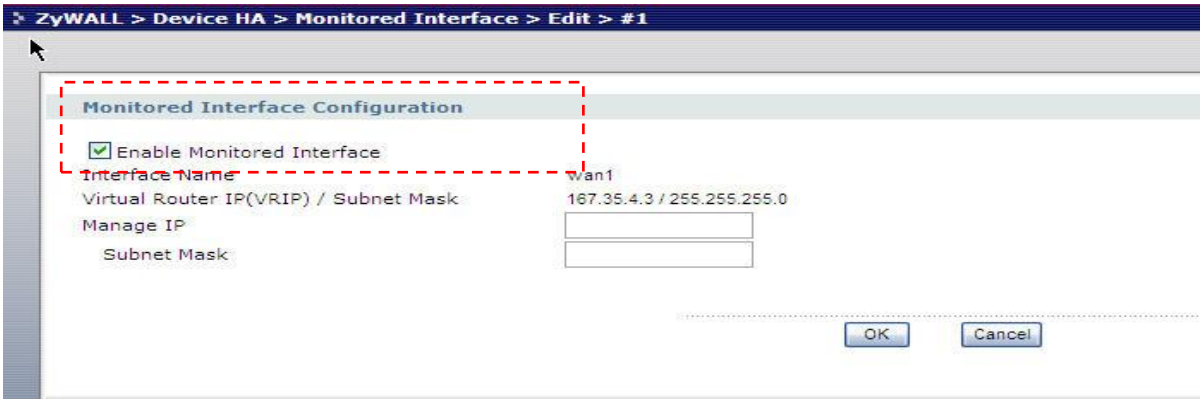
The “Preempt” means that the Backup with high priority can preempt the Backup with low priority when the Backup device is online. And Master can always preempt any Backup.

L02. What is the password in Synchronization?

If the Backup wants to synchronize the configuration from Master, both Master and Backup device must be set the same password.

L03. What is “Link Monitor” and how to enable it?

There is a new feature enhancement “Link Monitor” in ZLD 2.10 of USG. By enabling “Link Monitor” option, the ZyWALL monitors link status of direct-connected cables constantly. If a master ZyWALL device HA interface's link is down, the faulty device HA interface on master's router remains in status active and the rest of HA interface(s) on the master router will turn into fault. The purpose of this design is to prevent the backup router interface in the same HA group cannot detect the faulty event encountered on the master router.
You can click on Device HA from the left panel and check the “Enable” checkbox to enable “Monitored Interface.”



L04. Can Link Monitor of Device HA be used in backup VRRP interfaces?

No, the Link monitor is designed only for master device, if the master VRRP

interface's link is down, "Link Monitor" shuts down all of the master's VRRP interfaces except the failure interface so the backup ZyWALL takes over completely.

L05. Why do both the VRRP interfaces of master ZW USG and backup ZW USG are activated at the same time?

Since the ZWUSG master sends multicast VRRP announcement to backup ZWUSG periodically, if the backup ZWUSG doesn't receive the VRRP announcement, it will activate its VRRP interfaces.

For the application scenario if the VRRP interface of master and backup ZWUSG connect to a switch, the switch MUST forward the VRRP multicast to the backup ZWUSG. Otherwise the backup ZyWALL will never receive VRPT announcement. Please ensure the switch forwards the multicast VRRP announcement (224.0.0.18) by enabling the "Unkown multicast flodding" option in the switch setting.

M. User Management FAQ

M01. What is the difference between user and guest account?

Both “user” and “guest” are accounts for network access. But the difference is that “user” account can login ZyWALL USG via telnet/SSH to view limited personal information.

M02. What is the “re-authentication time” and “lease time”?

For security reasons, administrators and accessing users are required to authenticate themselves after a period of time. The maximum session time is called re-authentication time. Lease time is another timeout mechanism to force access users to renew it manually (or automatically, it is configurable). For administrators, lease time is much like an idle time when configuring GUI.

M03. Why can’t I sign in to the device?

There are several reasons that the device can deny the login for

1. Password is wrong
2. Service access policy violation
3. Too many simultaneous login session for an account
4. The IP address is locked out
5. System capacity reached

M04. Why is the TELNET/SSH/FTP session to the device disconnected? Why is the GUI redirected to login page after I click a button/link?

There are several reasons that device could log you out.

1. Re-authentication, lease or idle timeout
2. IP address is changed after authentication
3. Another account was used to login from the same computer

M05. What is AAA?

AAA stands for Authentication/Authorization/Accounting. AAA is a model for access

control and also a basis for user-aware device. A user-aware device like ZyWALL USG could use authentication method to authenticate a user (to prove who the user is) and give the user proper authority (defining what the user is allowed and not allowed to do) by authorization method. Accounting measures the resources a user consume during access which is used for authorization control, resources utilization and capacity planning activities.

AAA services are often provided by a dedicated AAA server or a local database in a user-aware device. The most common server interfaces are LDAP and RADIUS.

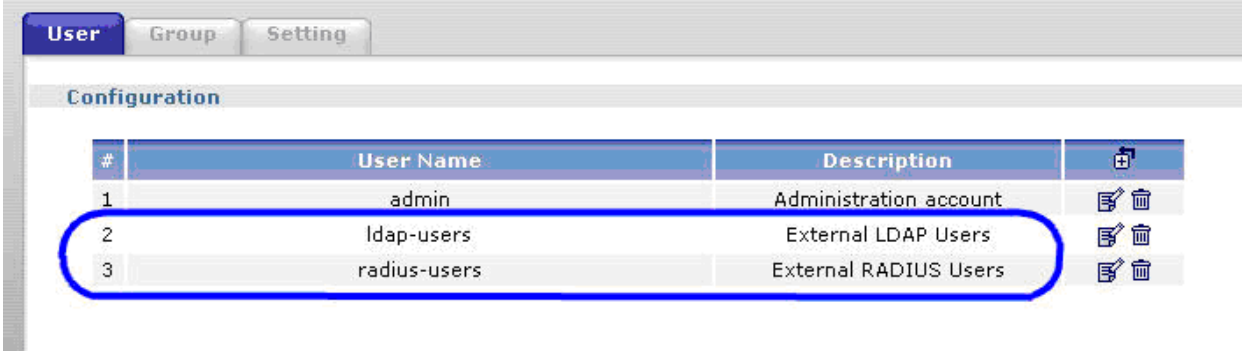
In ZyWALL USG, AAA object allows administrators to define the local database, AAA server(including LDAP server and RADIUS server) and related parameters. AAA groups are ones that could group several AAA servers for those enterprises that have more than one AAA server. Furthermore, if the three kinds of services, LDAP, RADIUS and Local exist at the same time, administrators could decide the order of different AAA services by AAA method.

M06. What are ldap-users and radius-users used for?

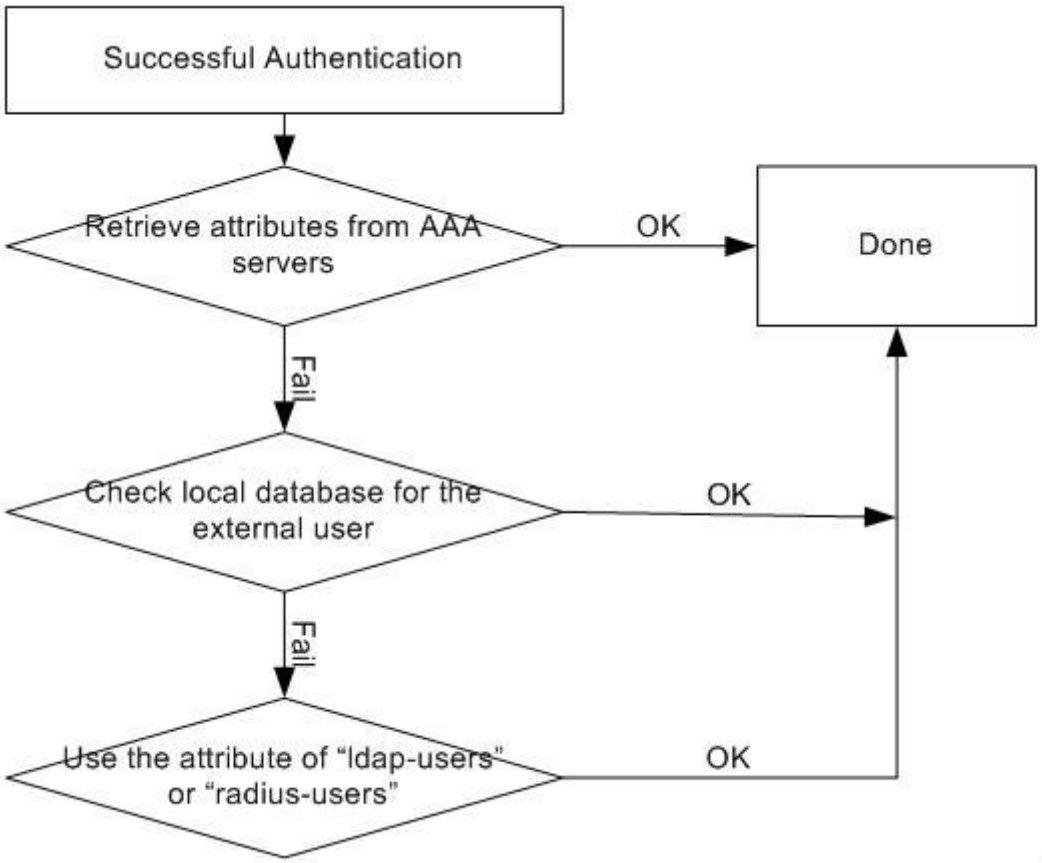
ldap-users/radius-users refer to the users that are authenticated successfully via LDAP/RADIUS server. If you want to perform access control rules or build access policies for the users authenticated via external servers such as LDAP or RADIUS, you can use the ldap-users and radius-users in your access control rules or policies.

M07. What privileges will be given for ldap-users and radius-users?

When a user has been authenticated by external database (ladp or radius server), it will retrieve the user's attributes (like lease timeout and re-auth timeout value) from the external server. If the external server doesn't define the user's attributes, it will try to check local database on ZyWALL USG (at GUI menu **Configuration** > **User/Group** > **User** tab or **Group** tab) instead. If it still cannot find, it will use the attribute of "ldap-users" and "radius-users" at GUI menu **Configuration** > **User/Group** > **User** tab as below. The default lease time and re-authentication time of ldap-users and radius-users are 1440 minutes.



See the flow as shown below.



N. Centralized Log FAQ

N01. Why can't I enable e-mail server in system log settings?

Enabling e-mail server requires necessary fields filled properly. You have to set the mail server, the sender address, event recipient and alert recipient.

N02. After I have the entire required field filled, why can't I receive the log mail?

E-mail server may reject the event/alert mail delivering due to many reasons. Please enable system debug log and find out why the e-mail server refused to receive the mail.

O. Traffic Statistics FAQ

O01. When I use "Flush Data" in Report, not all the statistic data are cleared.

"Flush Data" means that it clears the statistic data for the specified interface, not all interfaces. If users want to clear all data, stop collection and start it again.

O02. Why isn't the statistic data of "Report" exact?

Report module utilizes limited memory to collect data. It means that the longer is the collecting duration or the more connections, the less exact the result the Report module has. This Report function is mainly used for troubleshooting, when a network problem happens.

O03. Does Report collect the traffic from/to ZyWALL itself?

In Report module, only the forwarding traffic will be recorded. The forwarding traffic means the traffic going through ZyWALL. Therefore, only the broadcast traffic in the bridge interface will be recorded.

O04. Why cannot I see the connections from/to ZyWALL itself?

In Session module, only the forwarding traffic will be listed The forwarding traffic means the traffic going through ZyWALL. Therefore, the broadcast traffic in the bridge interface will be listed.

P. Anti-Virus FAQ

P01. Is there any file size or amount of concurrent files

limitation with ZyWALL USG Anti-Virus engine?

Due to ZyWALL USG Anti-Virus engine is a stream-based AV system, there is no strict limitations in file size or amount of concurrent files can be scanned.

P02. Does ZyWALL USG Anti-Virus support compressed file scanning?

Yes, the ZyWALL USG Anti-Virus engine supports virus scanning with compression format ZIP, PKZIP, GZIP and RAR.

P03. What is the maximum concurrent session of ZyWALL USG Anti-Virus engine?

Due to ZyWALL USG Anti-Virus engine is in stream-based; therefore, there is no limitations in concurrent session.

P04. How many type of viruses can be recognized by the ZyWALL USG?

Anti-Virus engine can detect over 20000 common viruses, including worms and Trojans. The amount of virus can be detected is depend on amount of virus signature stored in the ZyWALL. In general, it covers the top 20000 active viruses in the wild list and the number of signatures on device is always at 3200.

P05. How frequent the AV signature will be updated?

The signature is powered by Kaspersky Labs. The signatures are updated 3 times a week. The emergency case will be responded within 48 hours.

P06. How to retrieve the virus information in detail?

Simply you can navigate to the web site with URL http://mysecurity.zyxel.com, and

search any virus relate detail as you required.

P07. I cannot download a file from Internet through ZyWALL USG because the Anti-Virus engine considers this file has been infected by the virus; however, I am very sure this file is not infected because the file is nothing but a plain text file. How do I resolve this problem?

You can add this file to the White List on ZyWALL USG to avoid this situation.

P08. Does ZyWALL USG Anti-Virus engine support Passive FTP?

Yes, ZyWALL USG supports both Active FTP and Passive FTP.

P09. What kinds of protocol are currently supported on ZyWALL USG Anti-Virus engine?

HTTP, FTP, SMTP, POP3 and IMAP4.

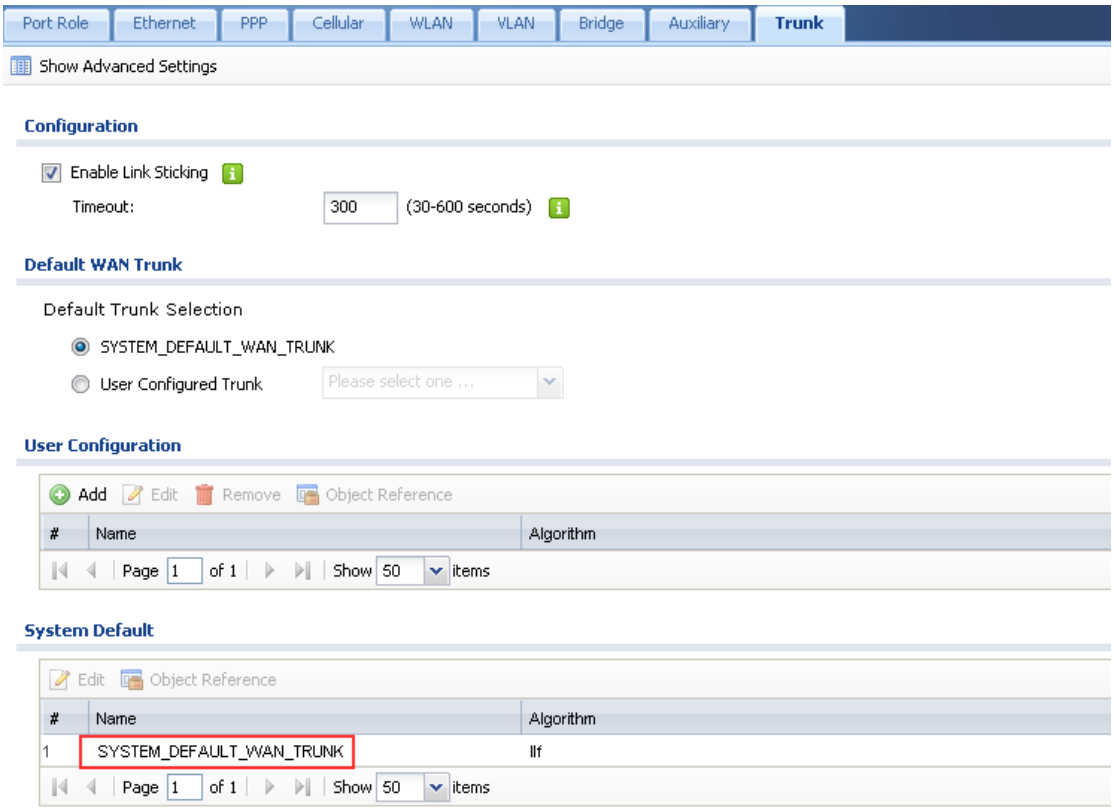
P10. If the Anti-Virus engine detects a virus, what action it may take? Can it cure the file?

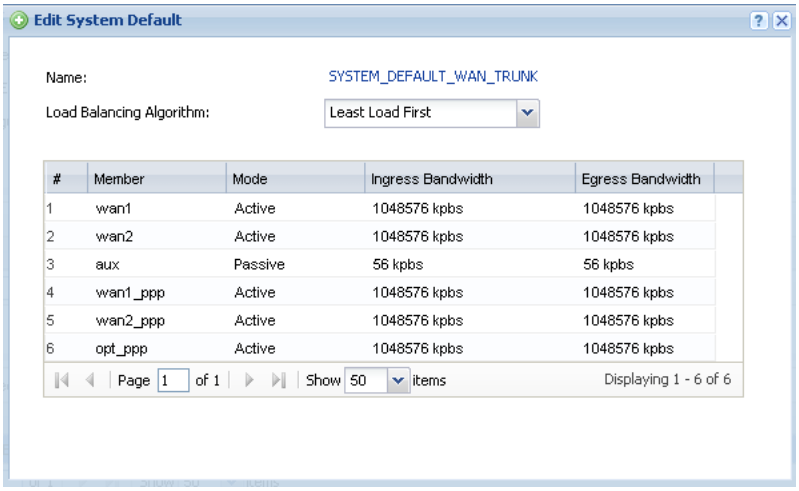
The ZyWALL USG will destroy the infected file, log this event and send alert to system administrator. Anti-Virus

Q. ZLD v2.20 New Feature Related FAQ

Q01. In ZLD v2.20, by default, I don't need to create any policy route to make traffic from intranet to go out to internet. How does USG do this?

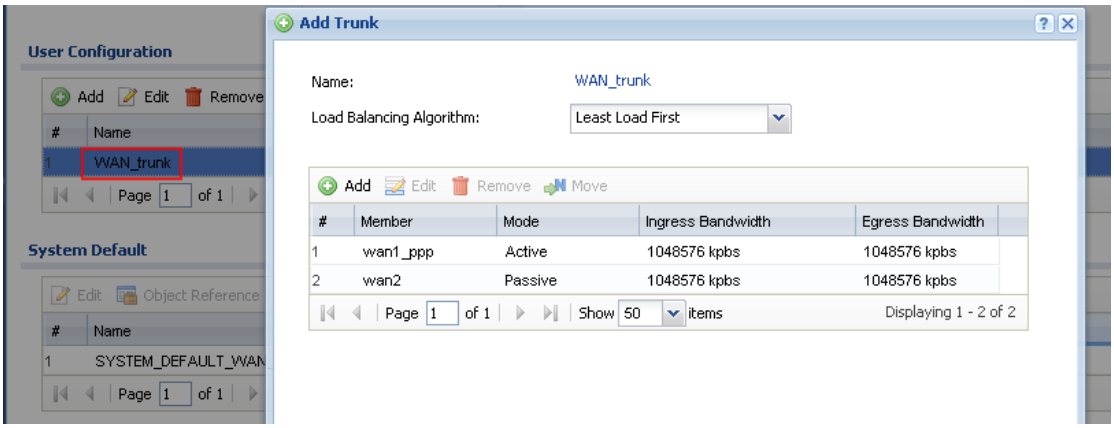
By default, there's a SYSTEM_DEFAULT_WAN_TRUNK. It includes all the interfaces whose type is External. You can find this default WAN Trunk in Network > Interface > Trunk.

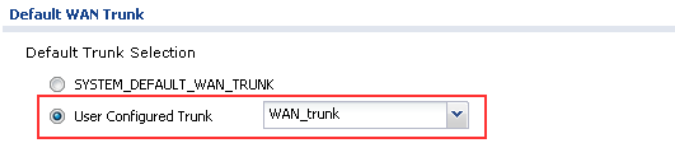




All the traffic received from Internal interfaces and destination to internet, will be sent out from the system default WAN Trunk.

User can also define customized WAN Trunk, and set the customized WAN Trunk as the system default WAN Trunk.





Q02. In ZLD v2.20, when I configure a NAT 1:1 mapping rule, there's not the option of "add corresponding policy route for NAT 1:1 mapping". Then how does the USG achieve the NAT 1:1 mapping?

In ZLD v2.20, after you configure an NAT 1:1 mapping rule, the system will automatically create a routing and NAT rule for the NAT 1:1 mapping of outgoing traffic. The system automatically created 1:1 routing and NAT rule for outgoing traffic has a lower priority than policy routes. So be careful when you create policy routes not to override the 1:1 rules.

Q03. In ZLD v2.20, do I still need to create policy routes for IPSec VPN traffic?

No. In ZLD v2.20, after you set the IPSec VPN rule, system will automatically create corresponding routes for the IPSec VPN traffic according to their phase2 local/remote policy.

Q04. What is EPS?

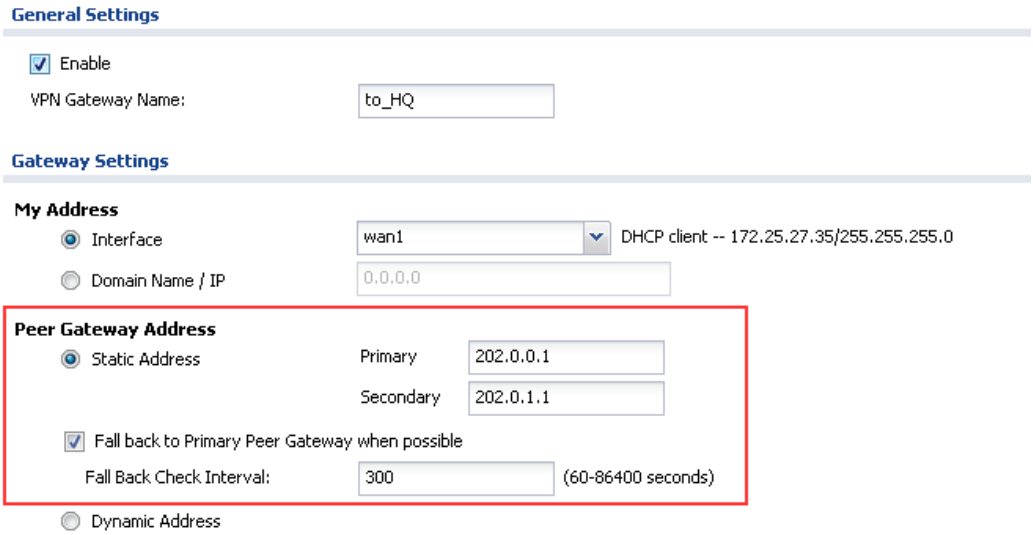
EPS is short for Endpoint Security.
Endpoint refers to PCs, laptops, handhelds, etc. Endpoint Security is a security concept that assumes each endpoint is responsible for its own security. Network administrator can set restrict policies to allow only the endpoints that comply with its defined security requirements to access network resources. The endpoint security requirement items may contain current anti-virus state, personal firewall, and operating system patch level, etc.
For example, a local endpoint doesn't have any anti-virus software installed. If it surfs internet, there's a high risk that it may be infected with viruses. Then the viruses may be propagated among the entire local network.
Another example is in SSL VPN case. If the SSL VPN client doesn't have anti-virus software installed, when it accesses the HQ local resources through SSL VPN tunnel, it may propagate the virus to HQ local subnet.
To prevent such undesired situation, the network administrator can use EPS checking to restrict endpoints' network access privileges. Only the compliant endpoint can get authority to access certain network resources.

Q05. Where can I deploy the EPS function?

We can deploy EPS in User Aware and SSL VPN applications.

Q06. Is IPSec VPN HA fall back function in ZLD v2.20?

Yes, IPSec VPN HA Fall Back is a newly added function in ZLD v2.20. In IPSec VPN HA scenario, you can enable "Fall back to Primary Peer Gateway when possible", and set a fallback check interval in the range of 60s~86400s.



When IPSec VPN fails over to the secondary gateway address, the Fallback checking mechanism is triggered. It will check whether the primary gateway is available once every check interval. If the USG detects that the primary gateway is available again, it will fall back to the primary gateway.

Q07. I want to add a bridge interface to Device HA. What are the correct setup steps to prevent broadcast storm?

You can choose either of the following two suggested setup steps:

Setup strategy 1:

1. Make sure the bridge interfaces of the master USG and the backup USG are not connected.
2. Configure the bridge interface on the master USG, set the bridge interface as a monitored interface, and activate device HA.
3. Configure the bridge interface on the backup USG, set the bridge interface as a monitored interface, and activate device HA.
4. Connect the USG's.

Setup strategy 2:

1. Disable bridge interfaces on the two USG.
2. Connect the USG's according to topology.
3. Configure Device HA and add bridge interfaces into Device HA.
4. Activate Device HA.
5. Reactivate bridge interfaces.

Q08. I upgraded my USG firmware from v2.12 to v2.20. There seem to be some routing issues after the upgrade. I know there're some changes in routing design in v2.20. How can I solve the routing issues related with firmware upgrade?

In previous firmware version, outing going traffic from local to internet, NAT 1:1 mapping, NAT Loopback and VPN site-to-site routings all need policy route to achieve. Please see the screenshot below as an example.

#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM
1	any	none	any	any	VS_ADDR_192_168_2_6	any	auto	outgoing-interface	0
2	any	none	any	LAN_SUBNET	subnet_branch	any	to_br	none	0
3	any	none	any	VS_ADDR_192_168_2_6	any	any	ge2	VS_ADDR_172_25_27_241	0
4	any	none	ge5	DMZ2_SUBNET	any	any	WAN_Trunk	outgoing-interface	0
5	any	none	ge4	DMZ1_SUBNET	any	any	WAN_Trunk	outgoing-interface	0
6	any	none	ge1	LAN_SUBNET	any	any	WAN_Trunk	outgoing-interface	0

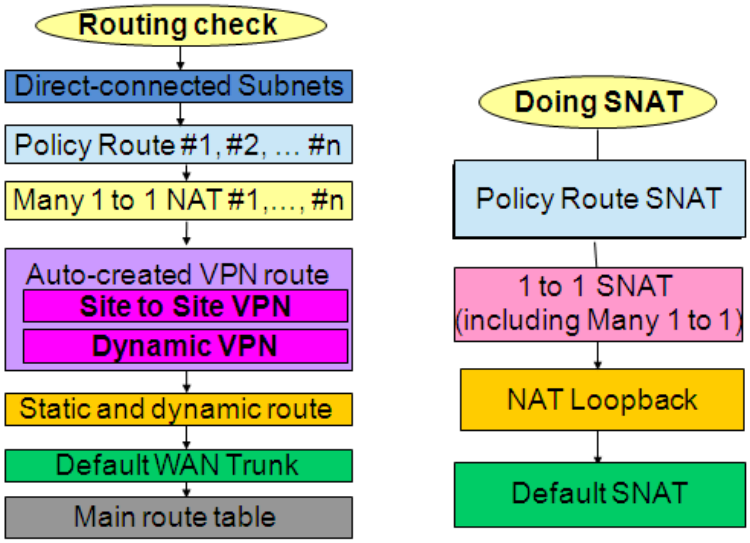
After upgrading firmware version to v2.20, the policy routes configured in old firmware will be kept.

Add Edit Remove Activate Inactivate Move

#	Status	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Next-Hop	DSCP Marking	SNAT	BWM
1		any	none	any	any	VS_ADDR_19	any	any	auto	preserve	outgoing-interface	0
2		any	none	any	LAN_SUBNET	subnet_branc	any	any	to_br	preserve	none	0
3		any	none	any	VS_ADDR_192_16	any	any	any	ge2	preserve	VS_ADDR_172_2	0
4		any	none	ge5	DMZ2_SUBNET	any	any	any	WAN_Trunk	preserve	outgoing-interface	0
5		any	none	ge4	DMZ1_SUBNET	any	any	any	WAN_Trunk	preserve	outgoing-interface	0
6		any	none	ge1	LAN_SUBNET	any	any	any	WAN_Trunk	preserve	outgoing-interface	0

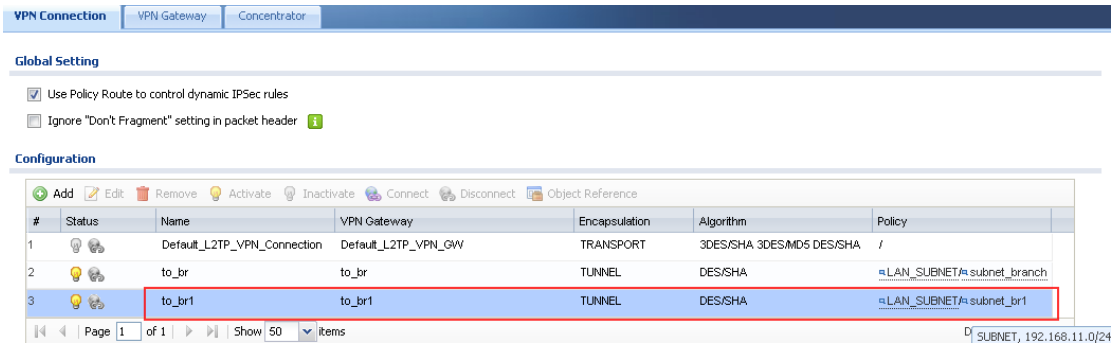
Page 1 of 1 Show 50 items Displaying 1 - 6 of 6

In v2.20, the routings of outgoing traffic from local to internet, NAT 1:1 mapping, NAT Loopback, and VPN site-to-site routing can all be done by system automatically created routes. And different routings and SNAT have the priority shown below:

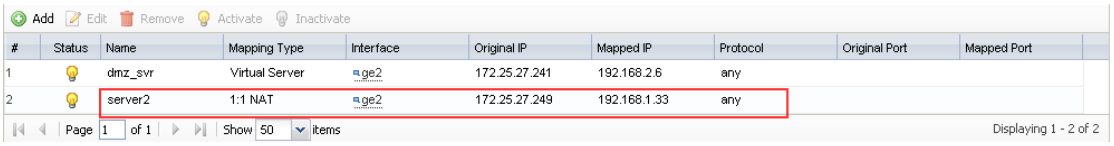


If you want to add new IPSec VPN rules or new 1:1 NAT rules based on original configuration files, the system auto created routing rules for VPN traffic or 1:1 mapping rules will be overridden by the original policy routes according to the routing priority table.

IPsec VPN phase2 rule:



1:1 NAT rule:



Policy routes:

Add Edit Remove Activate Inactivate Move

#	Status	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Next-Hop	DSCP Marking	SNAT	BWM
1		any	none	any	any	VS_ADDR_19	any	any	auto	preserve	outgoing-interface	0
2		any	none	any	LAN_SUBNET	subnet_branc	any	any	to_br	preserve	none	0
3		any	none	any	VS_ADDR_192_16	any	any	any	ge2	preserve	VS_ADDR_172_2	0
4		any	none	ge5	DMZ2_SUBNET	any	any	any	WAN_Trunk	preserve	outgoing-interface	0
5		any	none	ge4	DMZ1_SUBNET	any	any	any	WAN_Trunk	preserve	outgoing-interface	0
6		any	none	ge1	LAN_SUBNET	any	any	any	WAN_Trunk	preserve	outgoing-interface	0

Page 1 of 1 Show 50 items Displaying 1 - 6 of 6

To solve the routing issues, there're two ways:

Way 1 --- Keep the original policy routes, and add new policy routes for the newly added IPSec VPN rules.

Add Edit Remove Activate Inactivate Move

#	Status	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Next-Hop	DSCP Marking	SNAT	BWM
1		any	none	any	LAN_SUBNET	subnet_br1	any	any	to_br1	preserve	none	0
2		any	none	any	any	VS_ADDR_19	any	any	auto	preserve	outgoing-interface	0
3		any	none	any	LAN_SUBNET	subnet_branc	any	any	to_br	preserve	none	0
4		any	none	any	VS_ADDR_192_16	any	any	any	ge2	preserve	VS_ADDR_172_2	0
5		any	none	ge5	DMZ2_SUBNET	any	any	any	WAN_Trunk	preserve	outgoing-interface	0
6		any	none	ge4	DMZ1_SUBNET	any	any	any	WAN_Trunk	preserve	outgoing-interface	0
7		any	none	ge1	LAN_SUBNET	any	any	any	WAN_Trunk	preserve	outgoing-interface	0

Page 1 of 1 Show 50 items Displaying 1 - 7 of 7

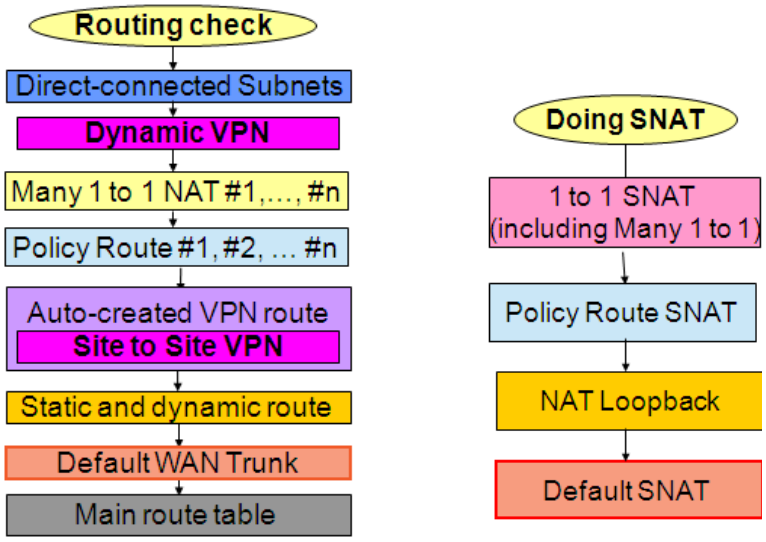
For 1:1 NAT mapping rules, there's a CLI can change the priority of policy route and 1:1 NAT rule.

[no] policy controll-virtual-server-rules activate

This function will be disabled automatically when the system detects the firmware is upgraded from v2.1x to v2.20.

```
Router> show policy-route controll-virtual-server-rules
policy route control virtual server status: off
Router>
```

So after firmware upgrade from v2.1x to v2.20, the routing priority table becomes below:



The newly added NAT 1:1 routing rules will always have higher priority than the policy routes. So it will not be overridden by any policy route.

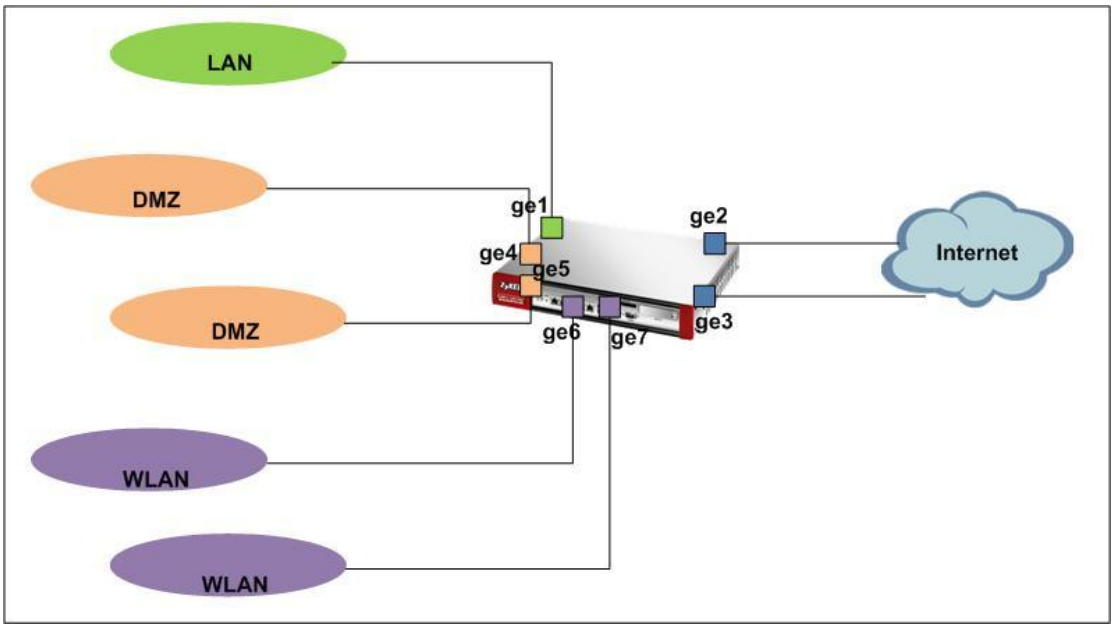
Way2 --- Delete the policy routes for outgoing traffic from local to internet. Use default WAN Trunk and default SNAT for the outgoing traffic, and use the 2.20 default routing priority table.

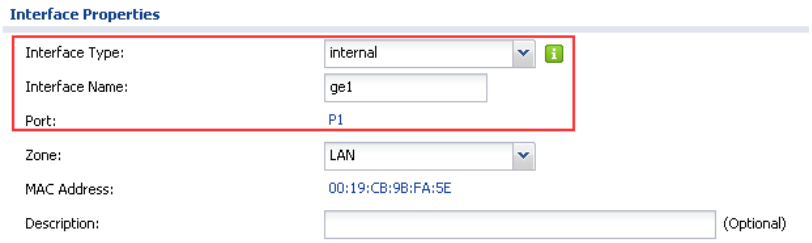
Usually the policy routes that may override IPSec VPN routes and 1:1 NAT routes are the ones for outgoing traffic, since their source is local subnets/range, and destination is “Any”.

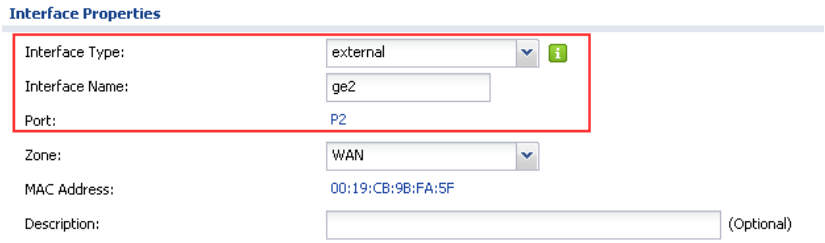
Step1. After firmware upgrade from v2.1x to v2.20, the interfaces’ types are all “general”. They system default WAN Trunk includes all interfaces whose type is External. So after firmware upgrade, there’s no interface in the system default WAN Trunk. We need to change the WAN interfaces’ type to External, and change interfaces connected local subnet to Internal.

See the picture below as an example.

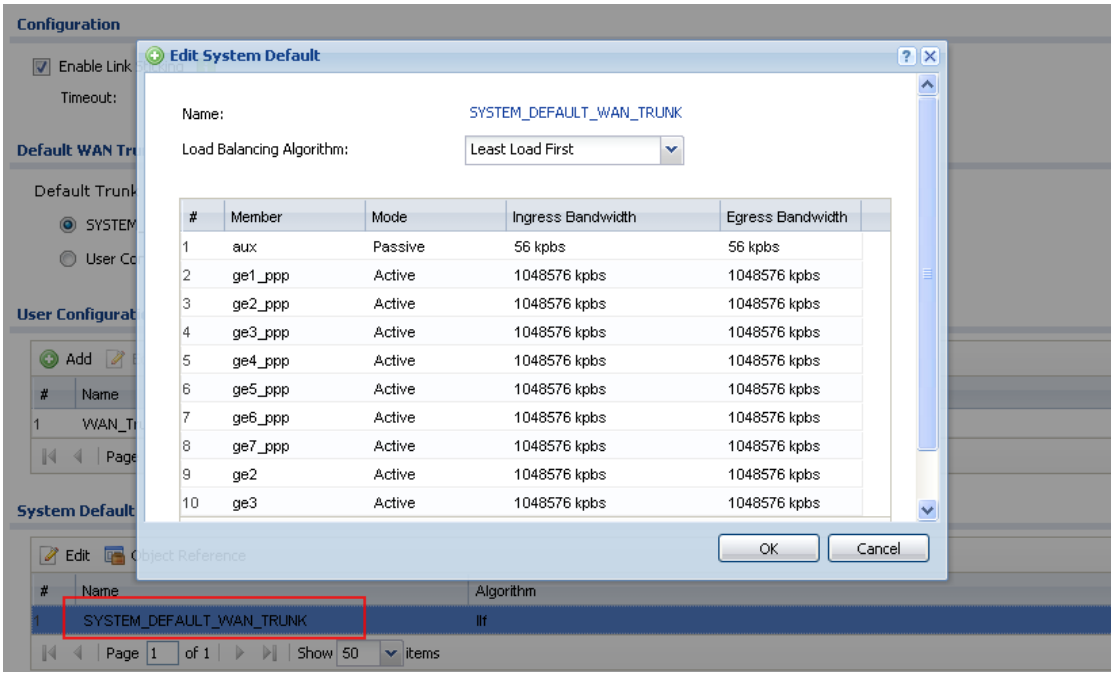
So we need to change ge1, ge4, ge5, ge6, ge7 Interface Type to Internal, and change ge2 and ge3 Interface Type to External.



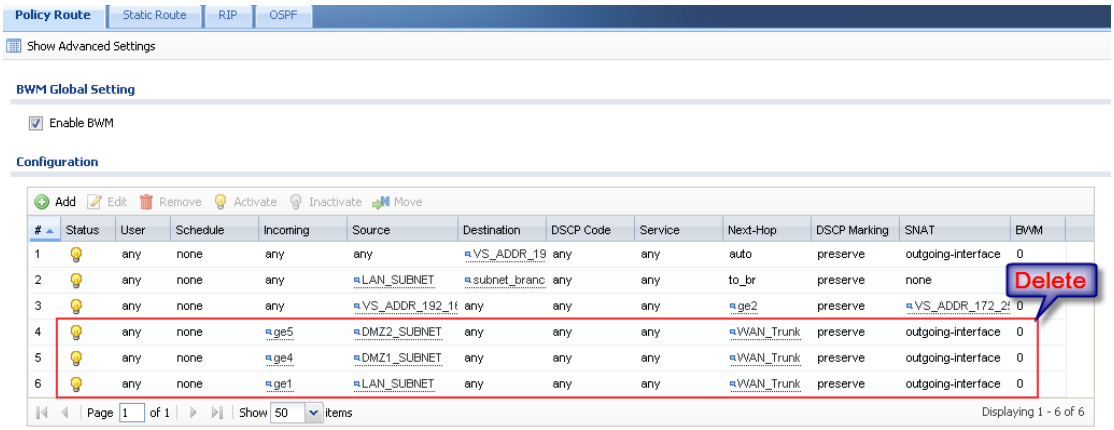




Step2. Go to Configuration > Network > Interface > Trunk, check the SYSTEM_DEFAULT_WAN_TRUNK. All the external interfaces are included in it now.



Step3. Go to Configuration > Network > Routing > Policy Route, delete the original policy routes that were used to route outgoing traffic.



Step4. Use the CLI below to change routing priority of NAT 1:1 rule and policy route, making policy route have higher priority than NAT 1:1 route.

```
Router(config)# policy controll-virtual-server-rules activate
Router(config)#
```

Check the policy route over NAT 1:1 routing status:

```
Router# show policy-route controll-virtual-server-rules
policy route control virtual server status: on
Router#
```

After all these configuration changes, your USG now totally follow the v2.20 new routing and SNAT priority design. You can leave all the routing tasks of outgoing traffic from local to internet, NAT 1:1 mapping, NAT Loopback, and VPN site-to-site to the system automatically generated routes.