2012

ZyWALL USG ZLD 3.0 Support Notes

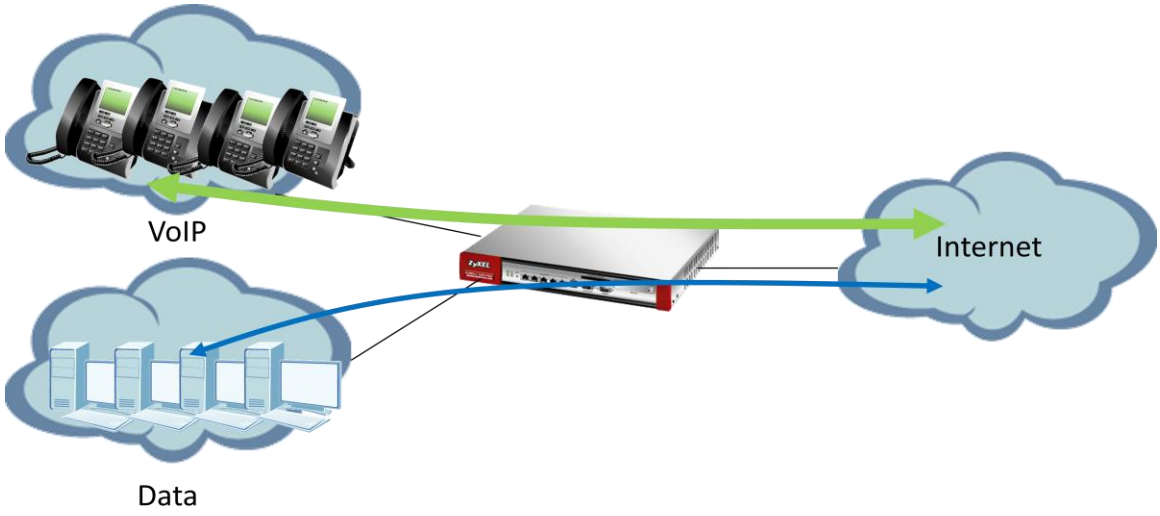
[Type the document subtitle]

CSO
ZyXEL
2/1/2012

Scenario 1 - Reserving Highest Bandwidth Management Priority for VoIP Traffic

1.1 Application scenario

In an enterprise network, there are various types of traffic. But most of the company's Internet bandwidth is limited. All traffic will contend for it and may result in some important traffic, for example, VoIP traffic getting slow or even starved. Therefore, intelligent bandwidth management for improved productivity becomes a matter of high concern for network administrators. A ZyWALL USG provides Bandwidth Management (BWM) function to effectively manage bandwidth according to different flexible criteria. VoIP traffic is quite sensitive to delay and jitter. Therefore, in an enterprise environment, VoIP traffic should usually be awarded the highest priority over all other types of traffic.



Network conditions:

USG:

Data LAN: 192.168.1.0/24

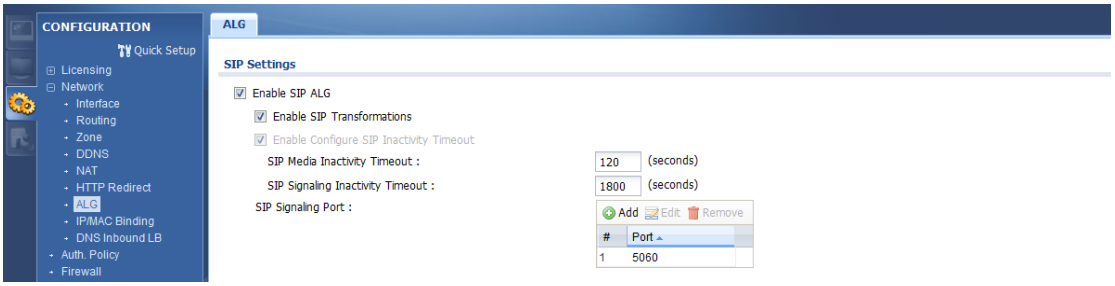
VoIP LAN: 192.168.2.0/24

Goals to achieve:

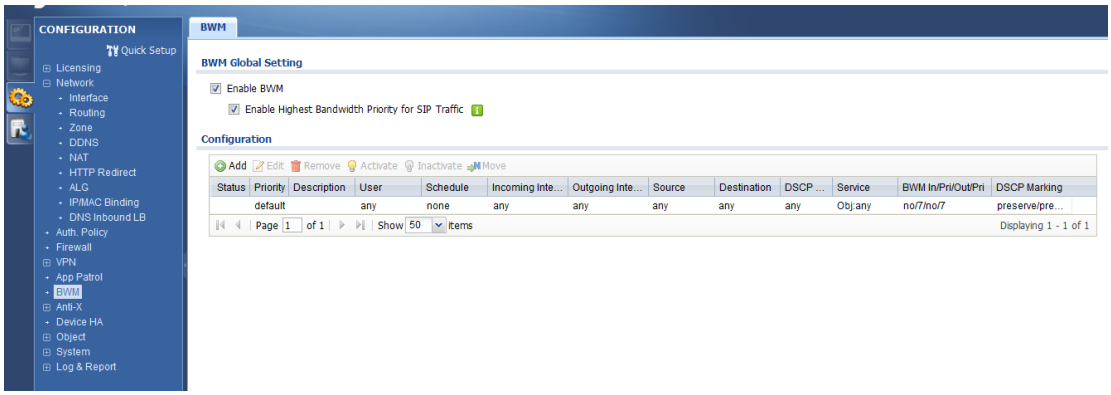
1) The priority of VoIP traffic is the highest and without any bandwidth restriction.
2) Restrict FTP download/upload bandwidth to 1000/500 kbps and set priority of FTP traffic to 4 for all users.

USG configuration:

Step 1: **Configuration** > **ALG** > check "**Enable SIP ALG**" function and "**Enable SIP transformations**".



Step 2: **Configuration** > **BWM** > check "Enable BWM" and "**Enable Highest Bandwidth priority for SIP Traffic**".

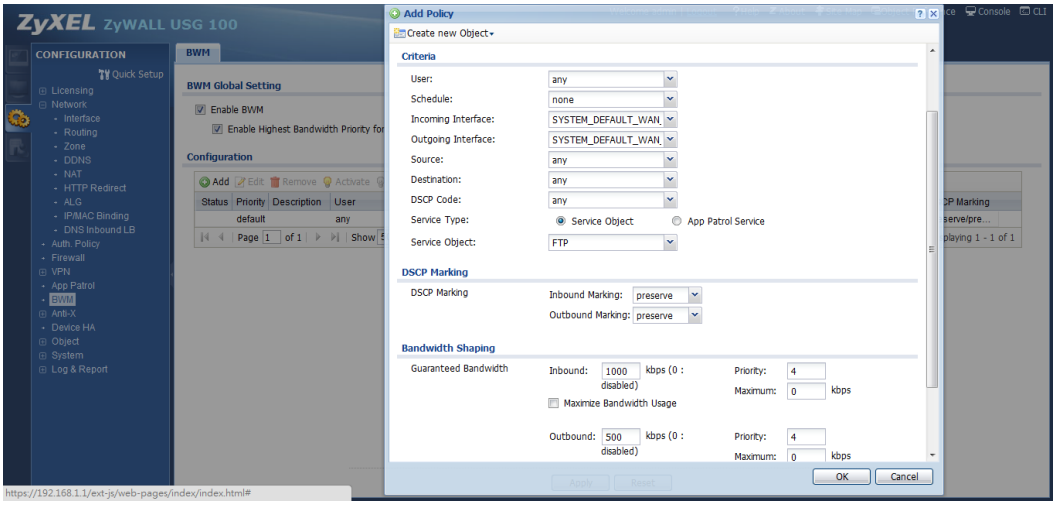


Step 3: **Configuration** > **BWM** > Select the "**Add**"

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

(2) And service object select the "**FTP**".

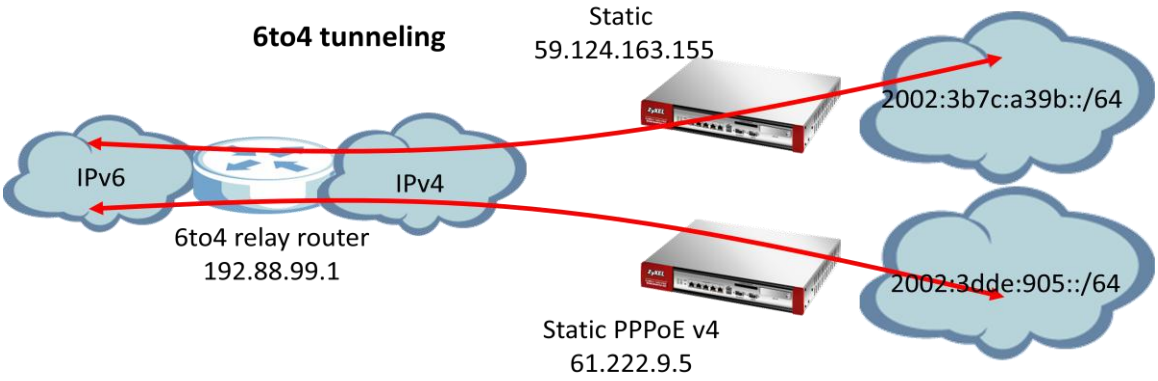
(3) Limit the **inbound** traffic to 1000Kbps and **Outbound** to 500Kbps and set all of the - priority levels to **4**.



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

2.1 Application scenario

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



2.2 6to4 IP translation introduction

Network conditions:

USG:

WAN1: 61.222.9.5(Static PPPoE v4)

Or

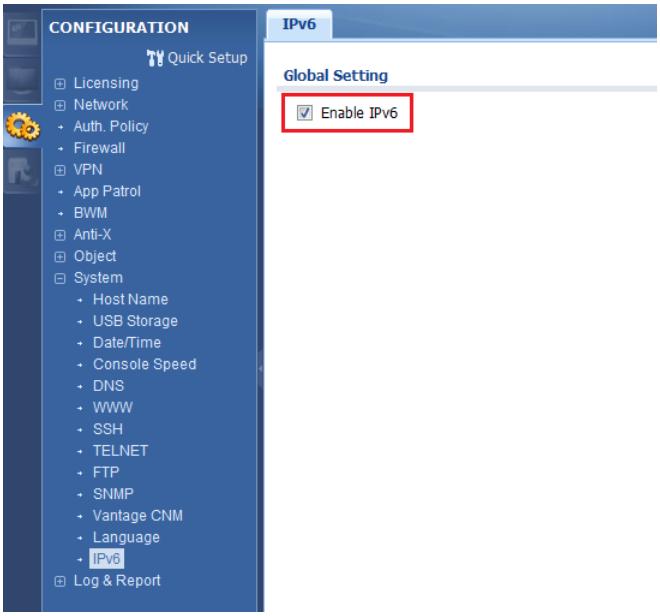
WAN1:59.124.163.155(Static)

Goal to achieve:

A ZyWALL USG will assign IPv6 IP addresses to the clients which are behind it, and the clients can access a remote IPv6 network by using the ZyWALL USG 6to4 tunnel.

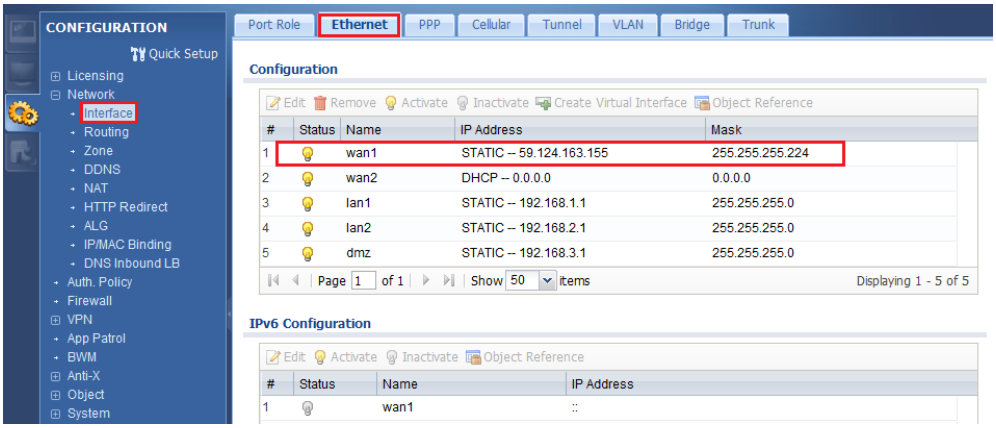
USG configuration

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



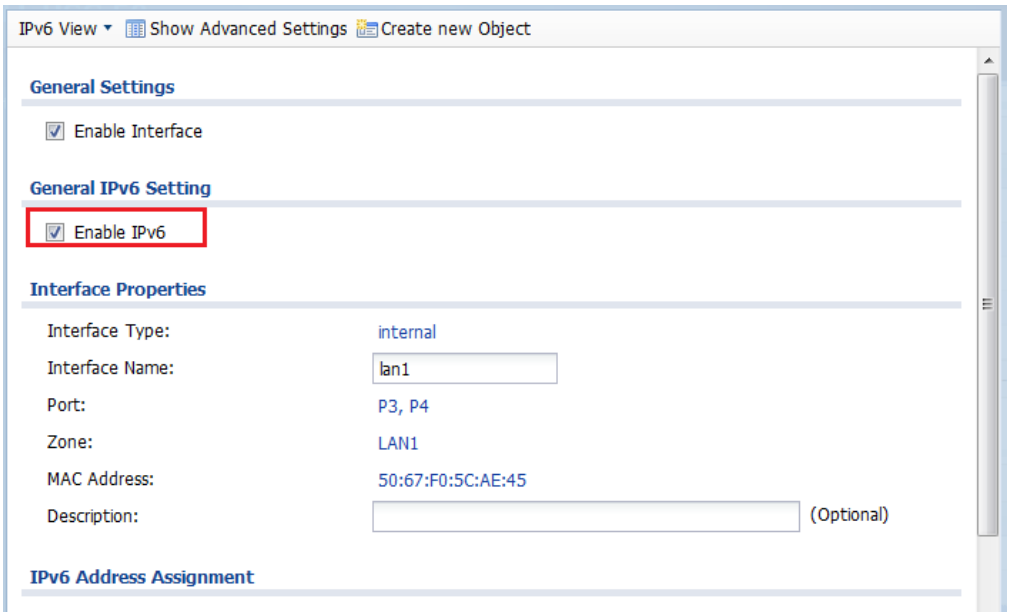
Step 2: Setting the static IP on WAN1

(1) **Configuration** > **Interface > Ethernet** > Double Click **WAN1** interface and configure with static IP address 59.124.163.155.



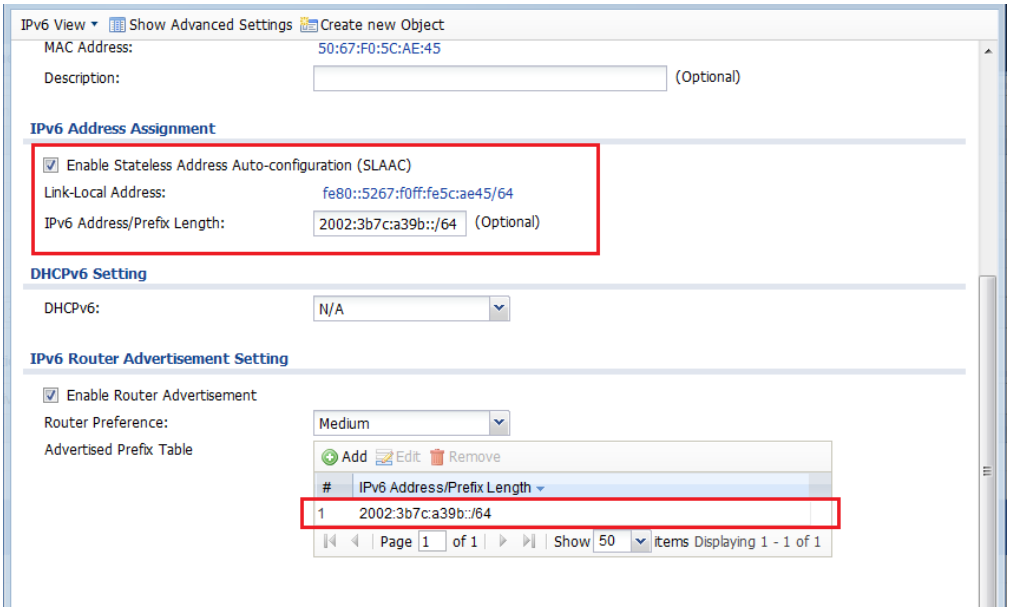
Step 3: Setting IPv6 IP address on LAN1

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



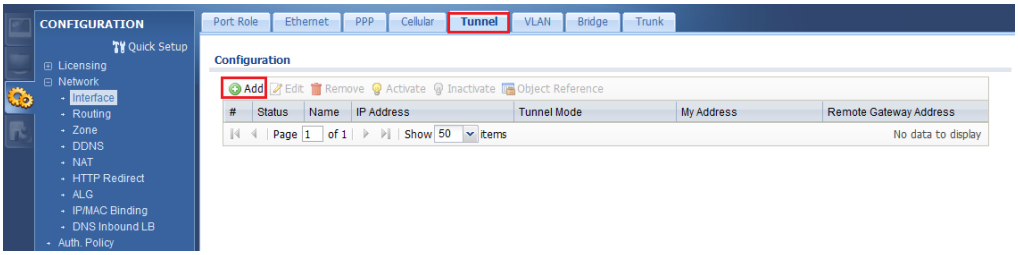
(2) Convert WAN1 IP address to hexadecimal
Check **Enable Stateless Address Auto-configuration(SLAAC)** box and enter **2002:3b7c:a39b::/64** in the prefix table.

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



Step 4: Enable 6 to 4 tunnel.

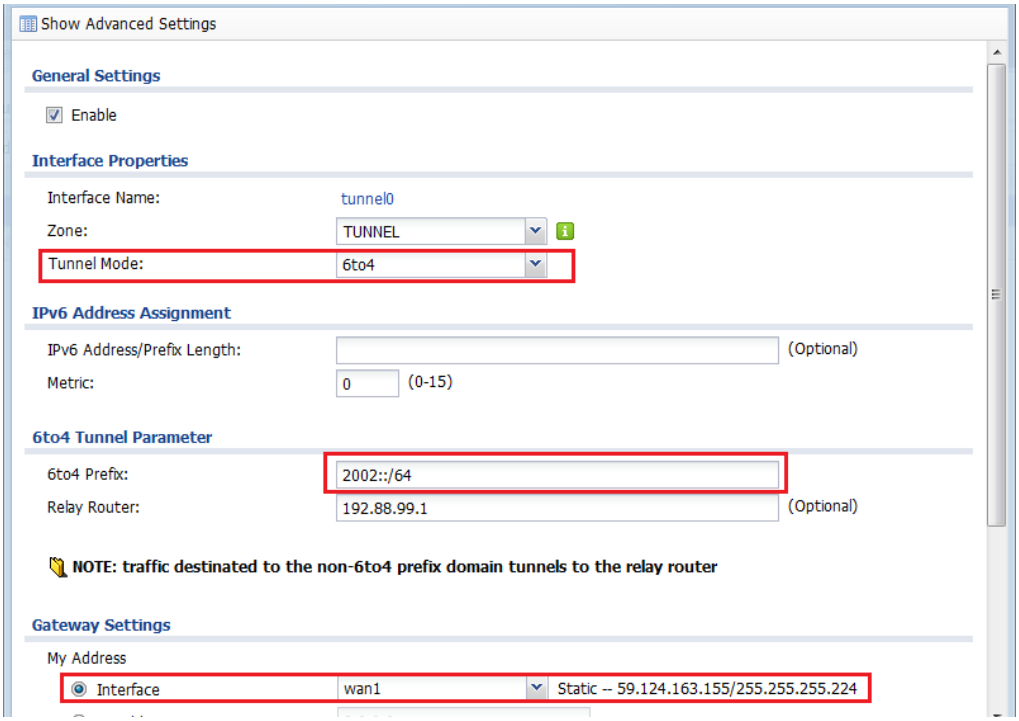
(1) **Configuration** > **Interface** > **Tunnel** > Click **Add** button



(2) Select the **6to4** in that **Tunnel Mode**

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

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

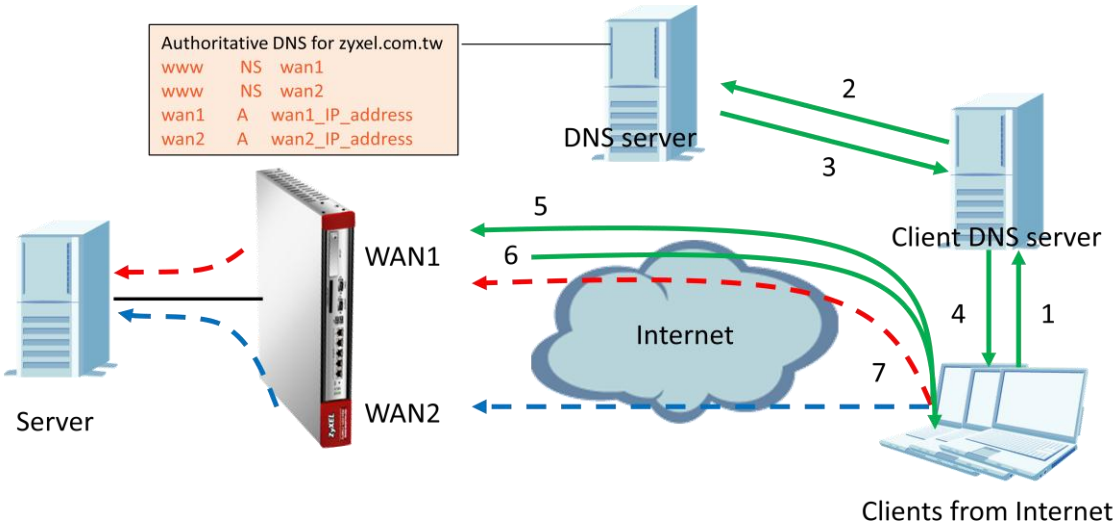


After these configuration steps, connect your computer to the device and check that your computer received an IPv6 IP address from tunnel.

Scenario 3 – DNS Inbound Load Balance

3.1 Application scenario

As an enterprise network gateway, the ZyWALL USG often has more than one WAN connection to share the network traffic. With DNS inbound load balance feature, the ZyWALL USG can reply with its other WAN IP to client according to network administrator's demand. Therefore, clients can visit the server behind ZyWALL USG smoothly via different connections.



1. Clients send DNS query for www.zyxel.com.tw to the client DNS server.
2. The client DNS server asks the query to DNS server.
3. DNS server reply to client DNS server to ask WAN1 IP for www.zyxel.com
4. Client DNS server reply to clients to ask WAN1 IP for www.zyel.com
5. Clients ask www.zyxel.com.tw to WAN1 IP of USG.
6. USG replies with WAN1 or WAN2 IP based on different balancing algorithm.
7. Clients access web page to WAN1 or WAN2.

Network condition:

USG:

- WAN1 IP: 59.124.163.150
- WAN2 IP: 59.124.163.135
- WAN1 downstream bandwidth: 50M
- WAN2 downstream bandwidth: 10M

Global DNS server:

- Leave DNS forward record for zyxel.com.tw to WAN1

Web Server behind USG:

- IP: 192.168.1.33

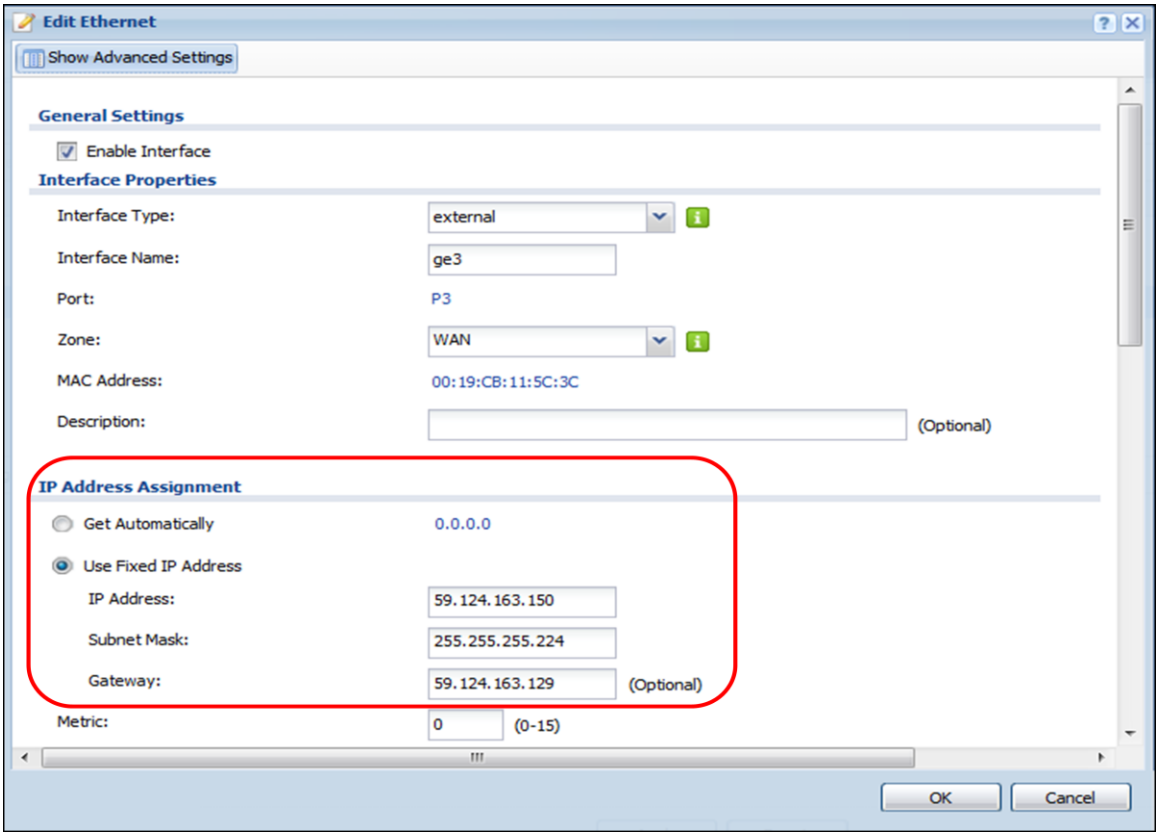
Goals to achieve:

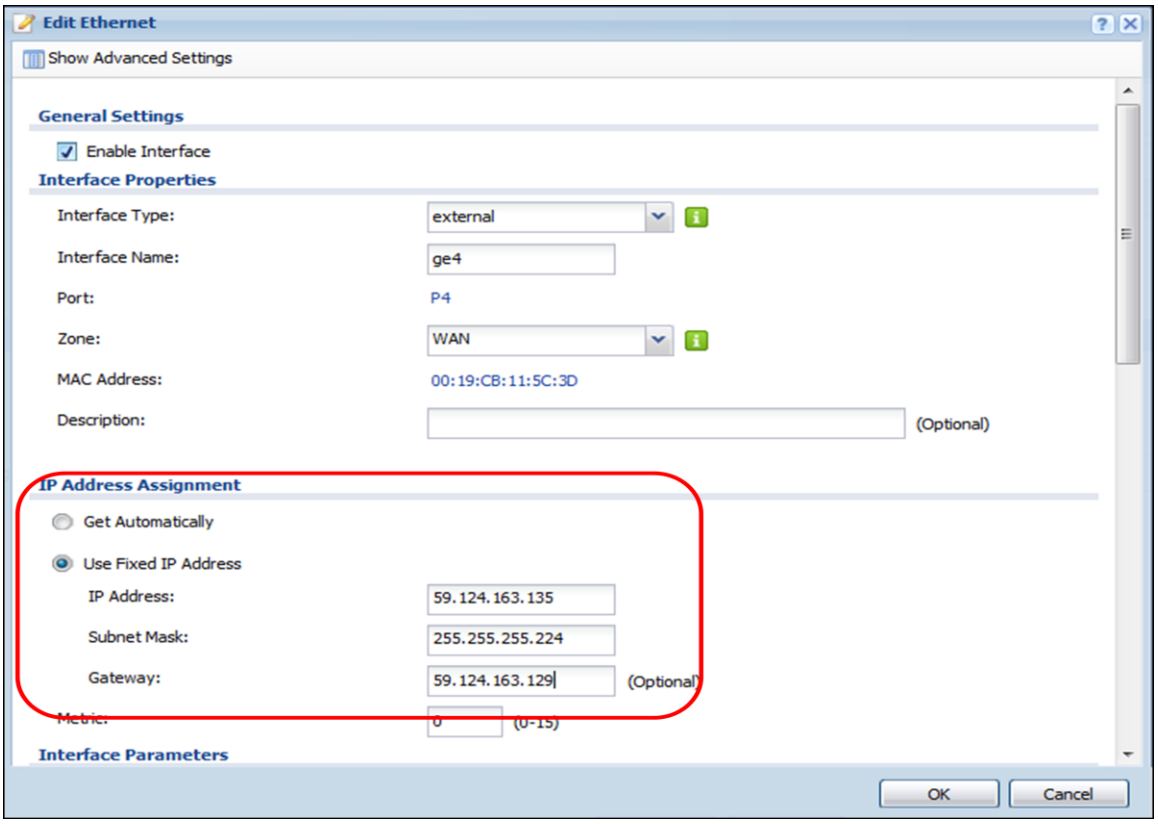
To balance traffic loading from Internet to WAN interfaces by using DNS inbound load balancing feature based on WRR algorithm.

Step 1: Set up the Authoritative DNS for zyxel.com.tw on DNS Global Server.

a. Set up the zone file for entry
   (a) www.zyxel.com.tw NS WAN1
   (b) www.zyxel.com.tw NS WAN2
b. Set up the IP address for wan1 and wan2
   (a) WAN1 A 59.124.163.150
   (b) WAN2 A 59.124.163.135

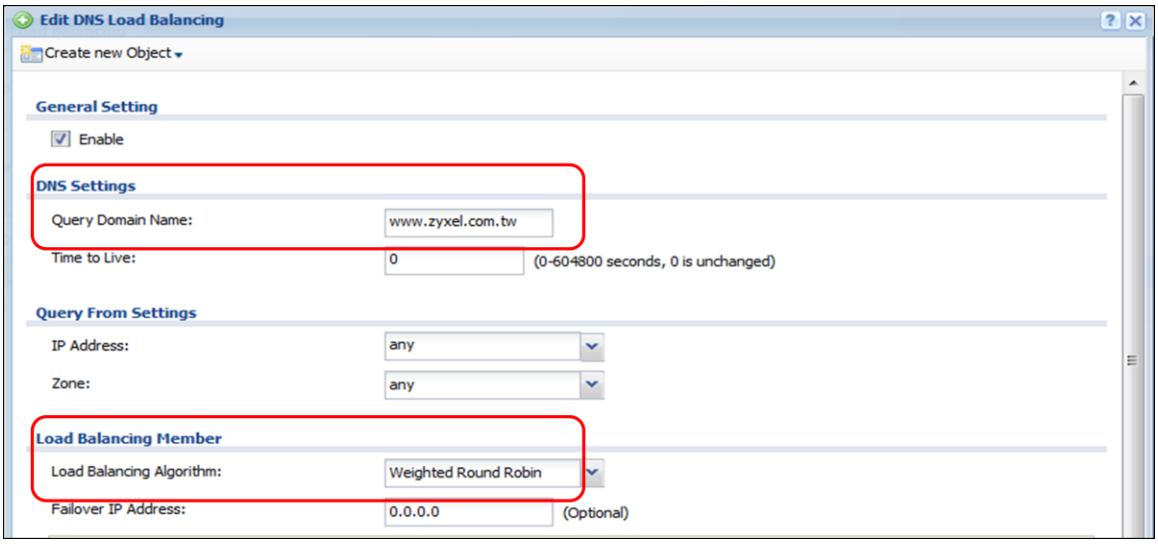
Step 2: Go to **Configuration -> Network -> Interface -> Ethernet**. Configure WAN IP address.



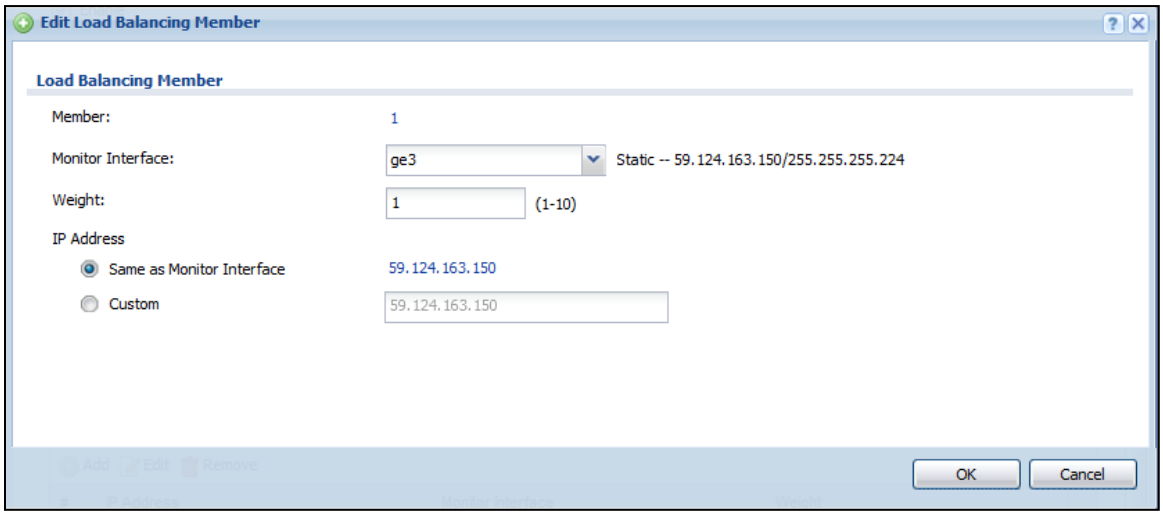


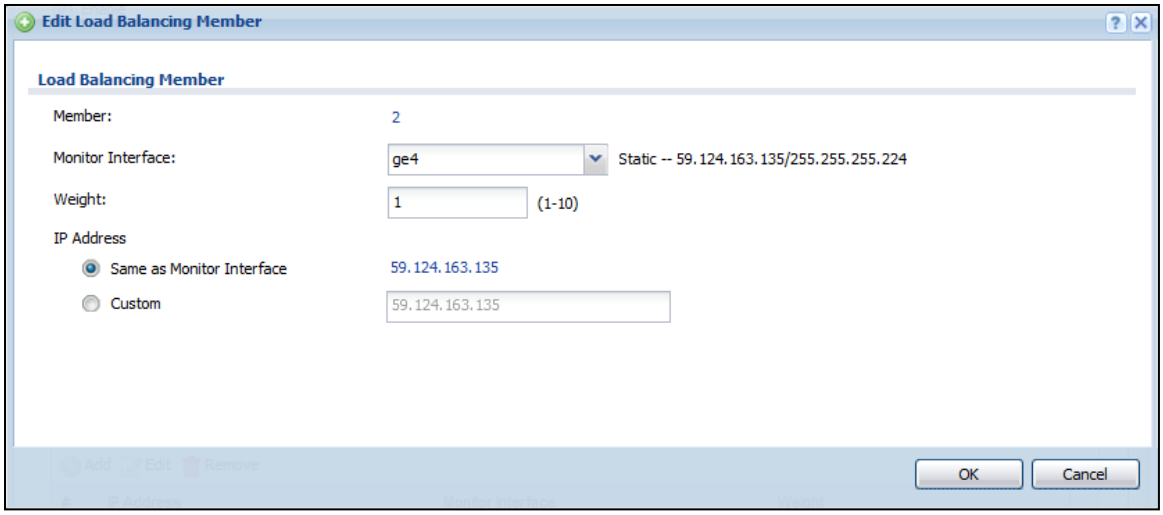
Step 3. Go to Configuration -> Network -> DNS Inbound LB, and add DNS Load Balancing

a. Edit the Query Domain Name that is needed, and choose the Load Balancing Algorithm “Weighted Round Robin”.

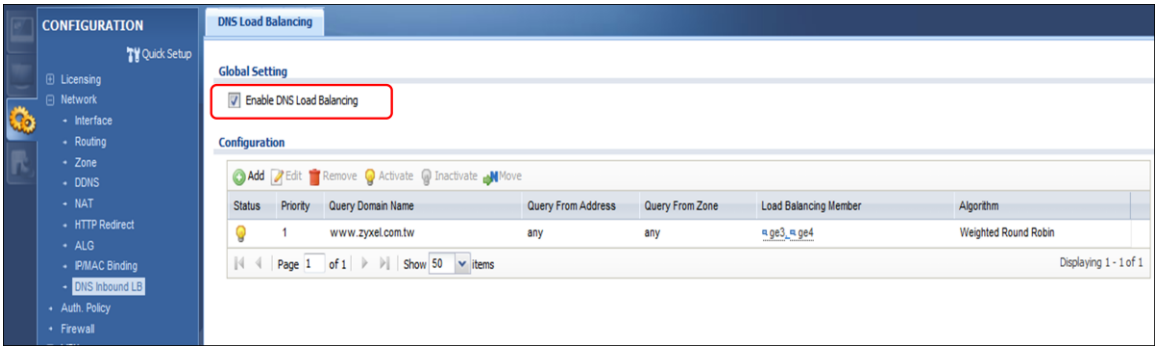


b. Add load DNS Load Balancing member



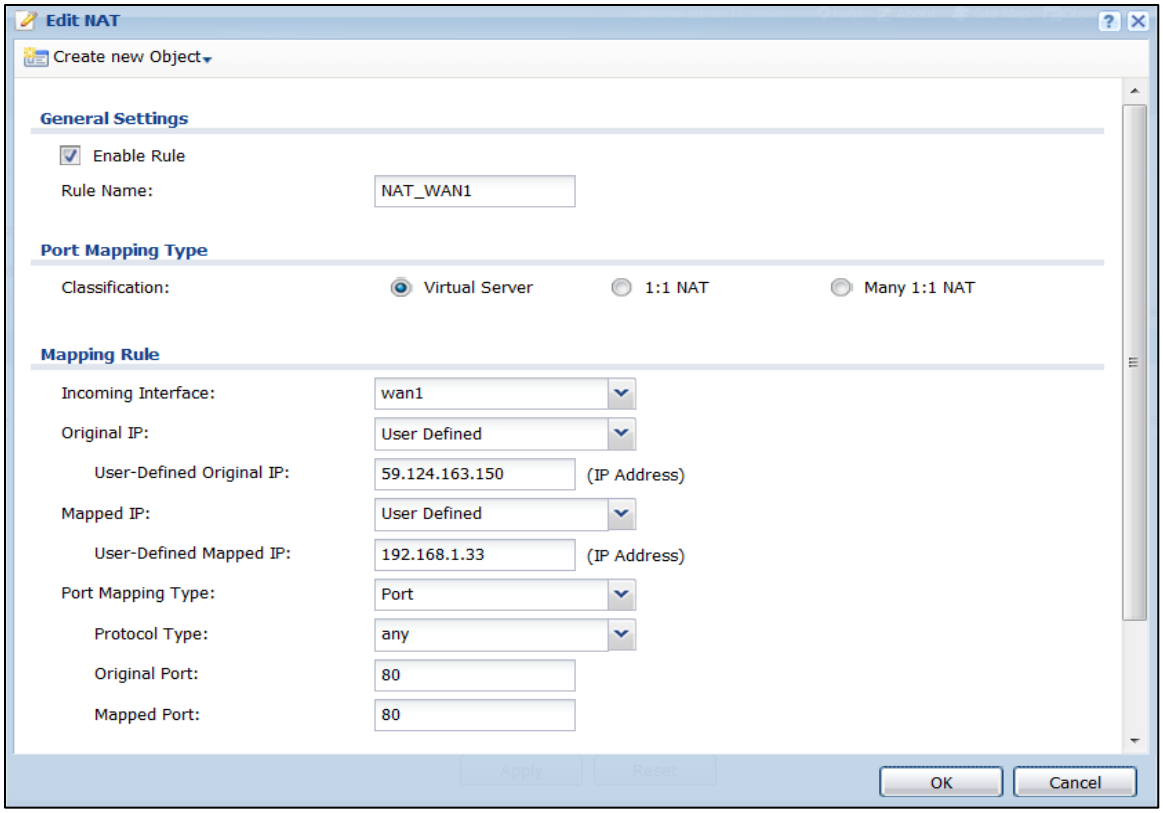


c. Enable DNS Load Balancing.

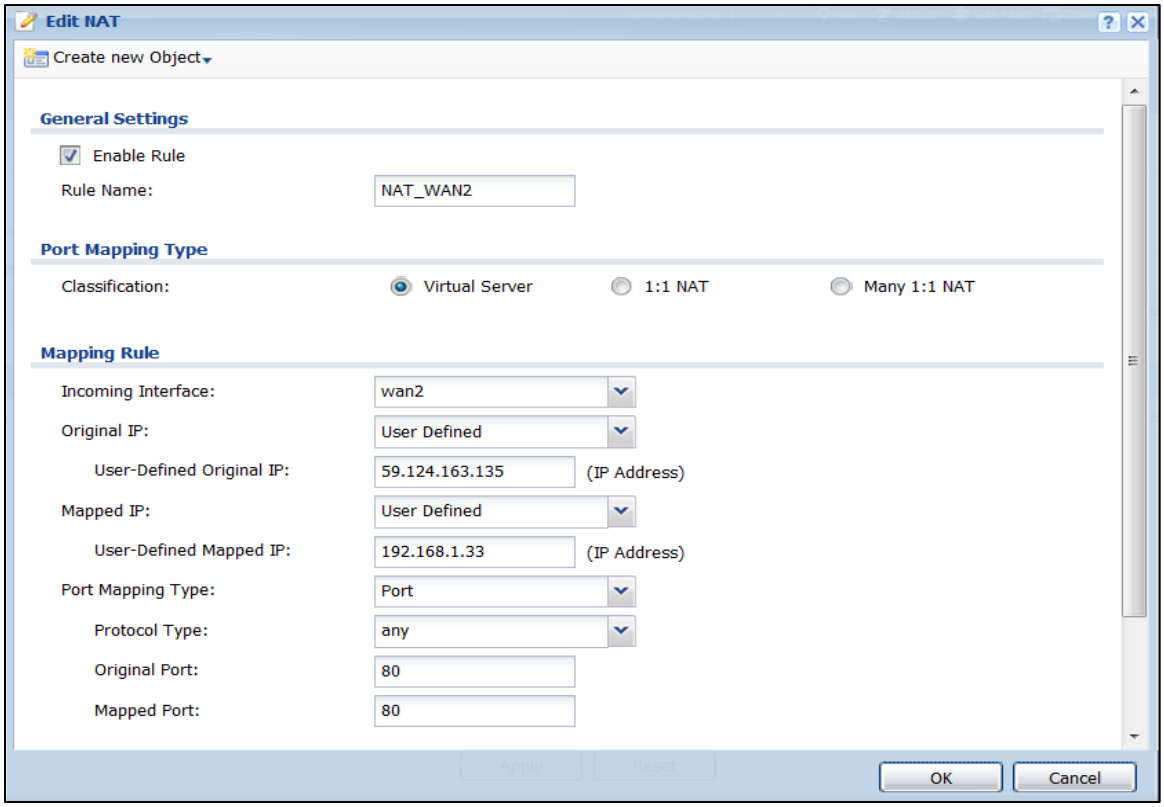


Step 4. Go to Configuration -> Network -> NAT. Configure the Virtual Server to forward the traffic from WAN to DNS Server.

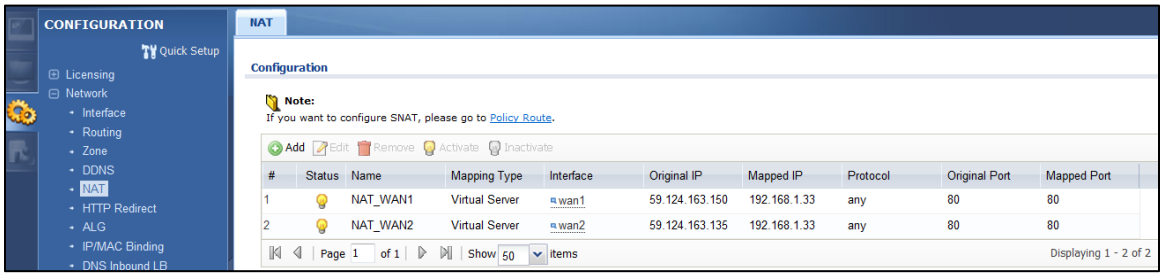
a. Add a NAT rule for WAN1.



b. Add a NAT rule for WAN2.



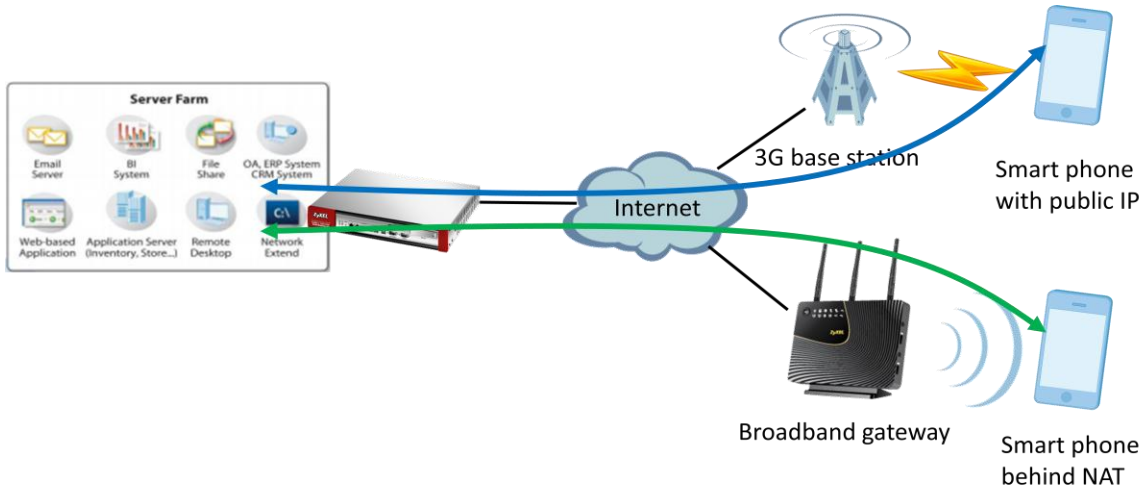
c. Make sure all NAT rules have been added.



Scenario 4 – Dialing up L2TP VPN connection to USG by using iOS/Android mobile device

4.1 Application scenario

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



4.2 Configuration Guide

Network conditions:

USG:

- WAN1 IP: 59.124.163.155
- Local subnet: 192.168.1.0/24
- L2TP pool:192.168.100.0/24
- Intranet website: http://info.zyxel.com

iOS/Android mobile device:

- IP: 118.169.105.67(3G mobile network)
- IP: 192.168.1.33(Behind NAT device)

IPSec VPN conditions:

Phase 1:

- Authentication: 12345678
- Local/Peer IP: WAN1/0.0.0.0
- Negotiation: Main mode
- Encryption algorithm: 3DES/3DES/DES
- Authentication algorithm: SHA1/MD5/SHA1
- Key group: DH2

Phase 2:

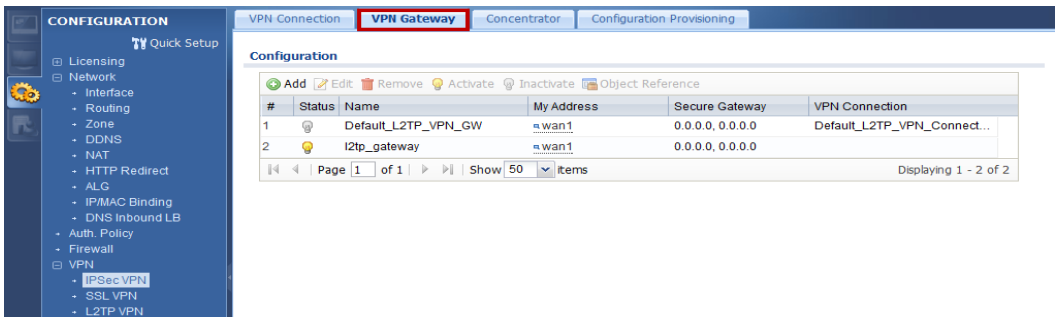
- Encapsulation Mode: Transport mode
- Active protocol: ESP
- Encryption algorithm: 3DES/3DES/DES
- Authentication algorithm: SHA1/MD5/SHA1
- Perfect Forward Secrecy: none

Goals to achieve:

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

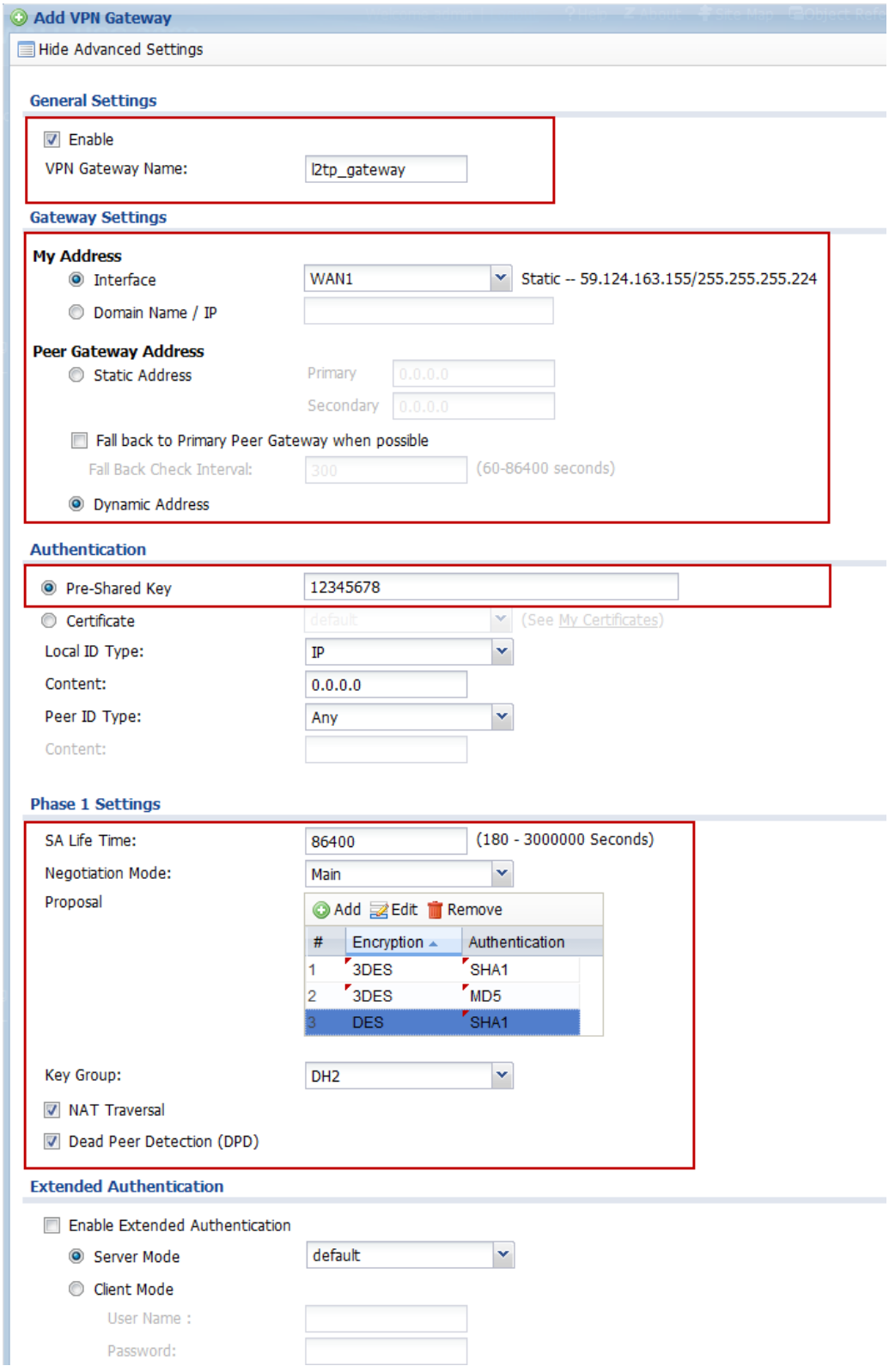
USG configuration

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

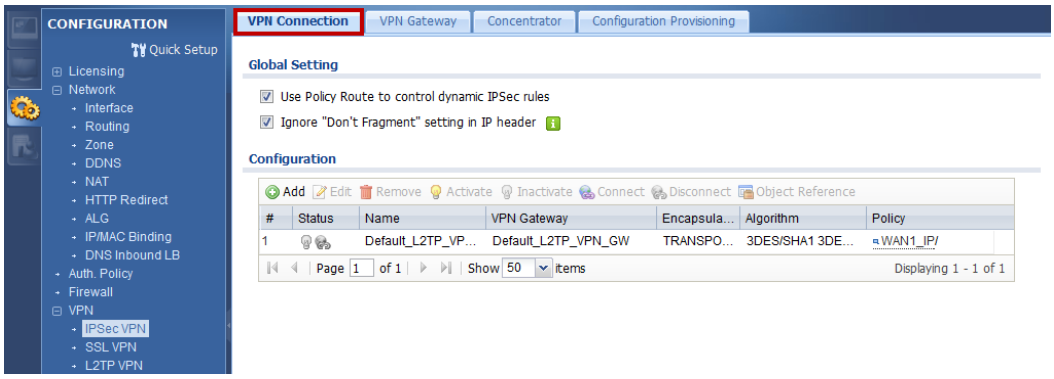


Step 2: Click the “Add” button to add a VPN gateway rule.

Step 3: Fill in the needed VPN gateway configuration.

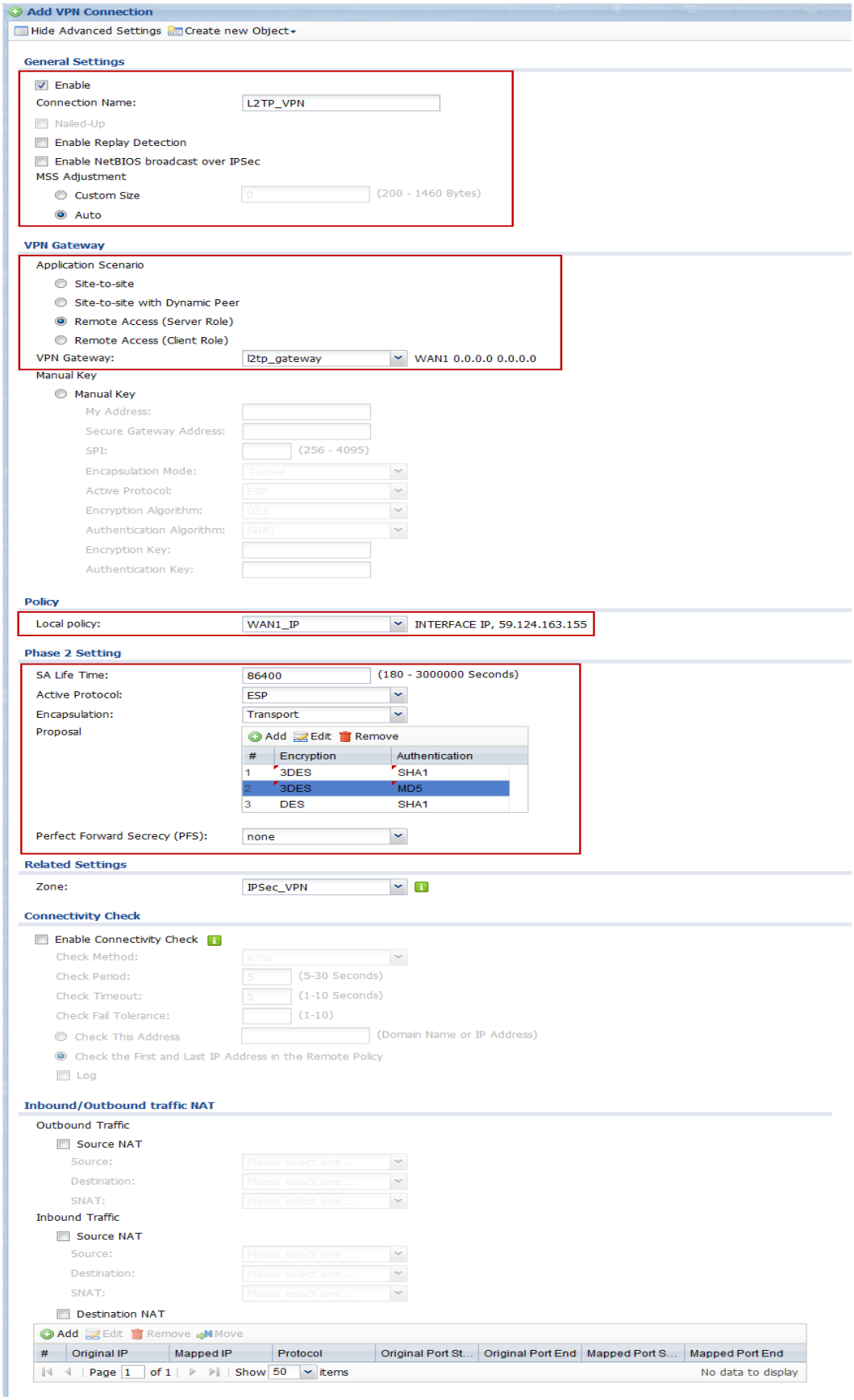


Step 4: Click **Configuration > VPN > IPSec VPN > VPN Connection** to visit the configuration screen to set phase 2 rule



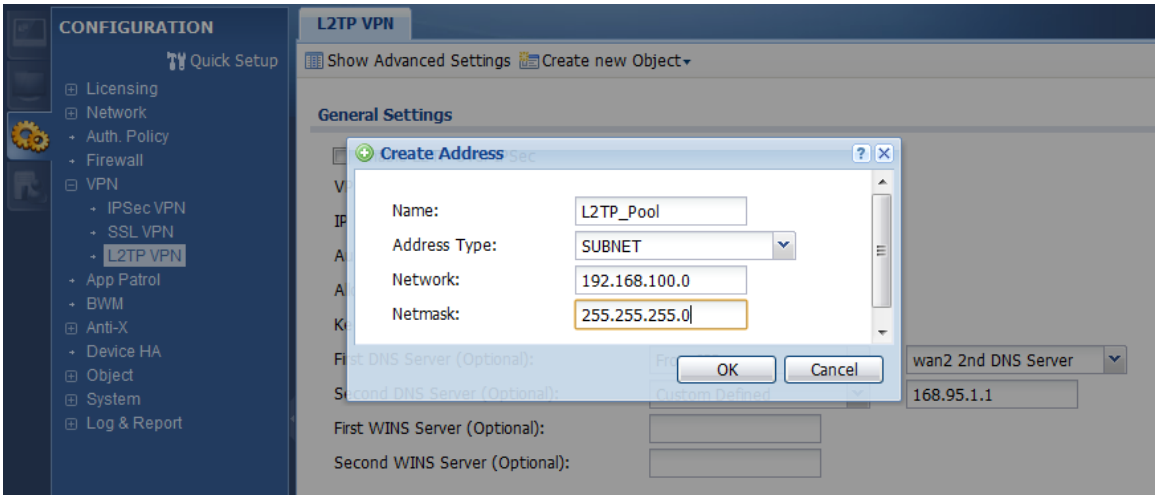
Step 5: Click the “Add” button to add a VPN connection rule.

Step 6: Fill in the needed VPN connection configuration.

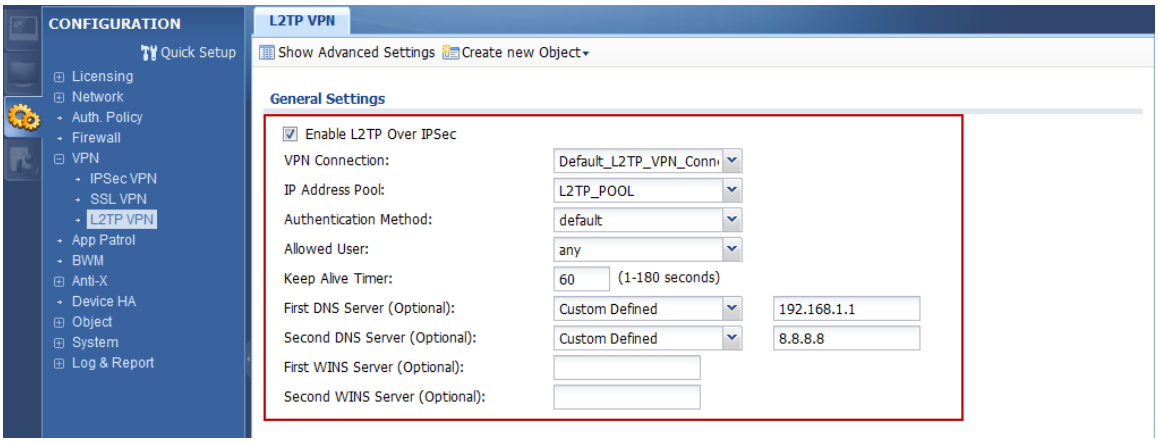


Step 7: Click **Configuration > VPN > L2TP VPN** to visit L2TP VPN configuration screen

Step 8: Create a address object for L2TP users

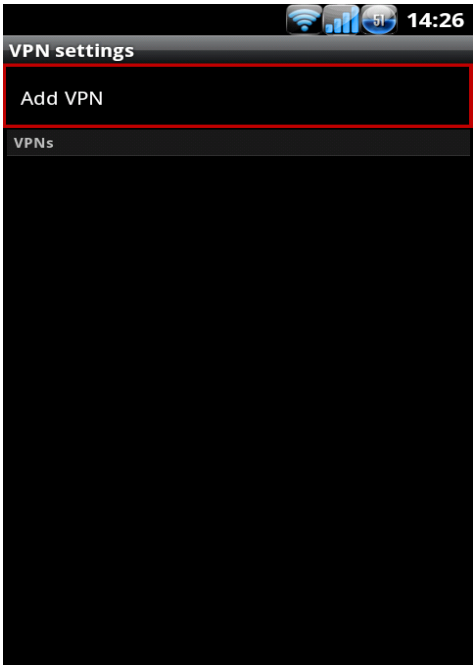


Step 9: Fill in the needed L2TP VPN connection configuration.

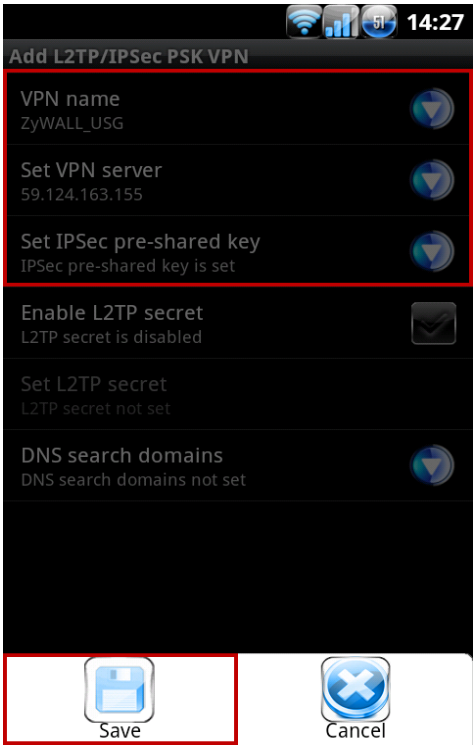


Android mobile client configuration

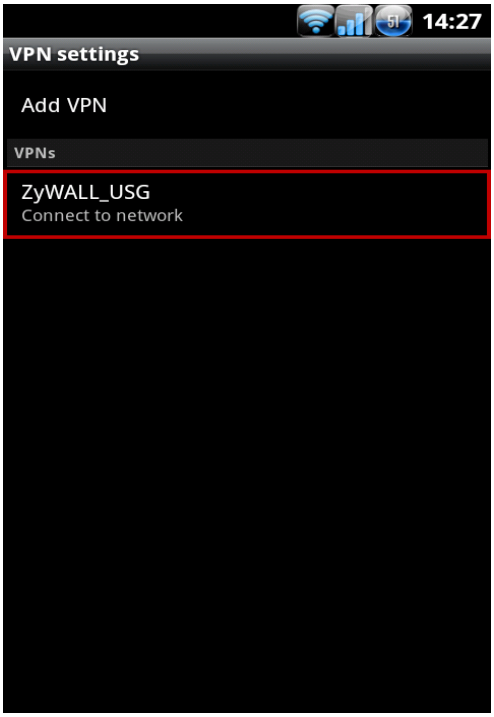
Step 1: **Settings > Wireless & networks > VPN settings > Add VPN**



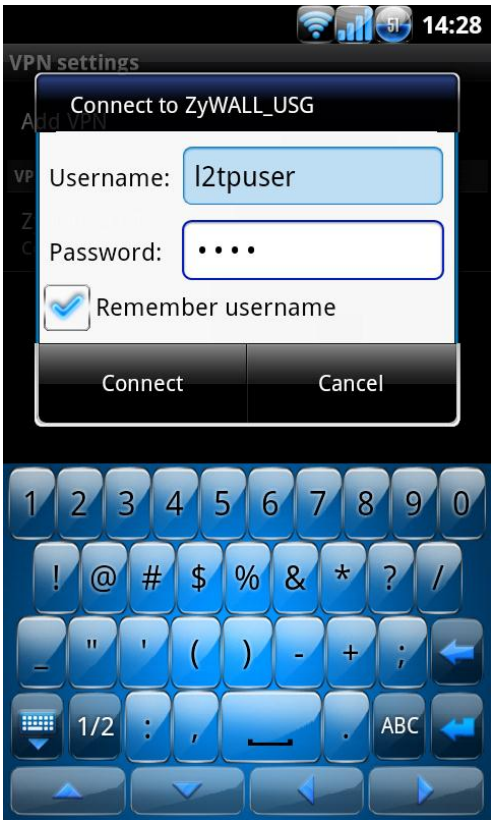
Step 2: Click **Add L2TP/IPSec VPN**, insert needed L2TP VPN settings and save



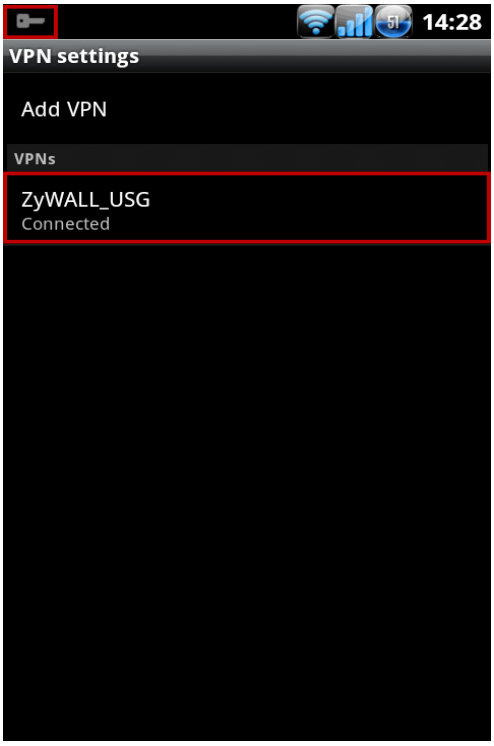
Step 3: Connect to the L2TP VPN



Step 4: Insert L2TP password



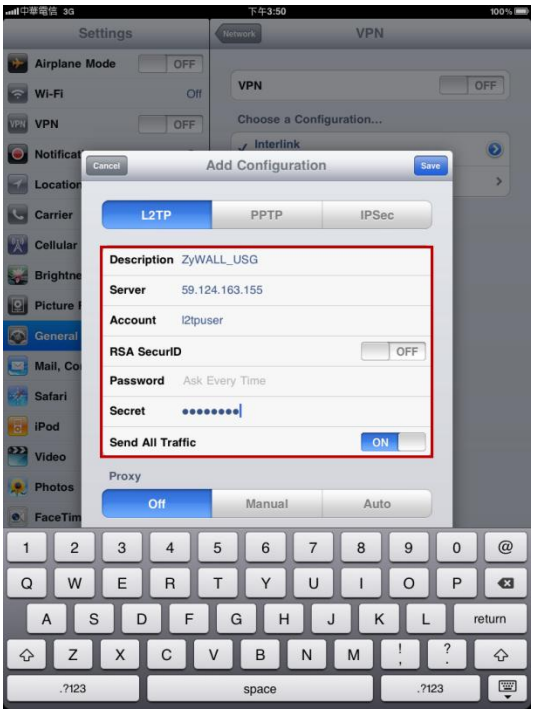
Step 5: Device will show connected when dial up is successful.



Step 6: Visit Intranet web page

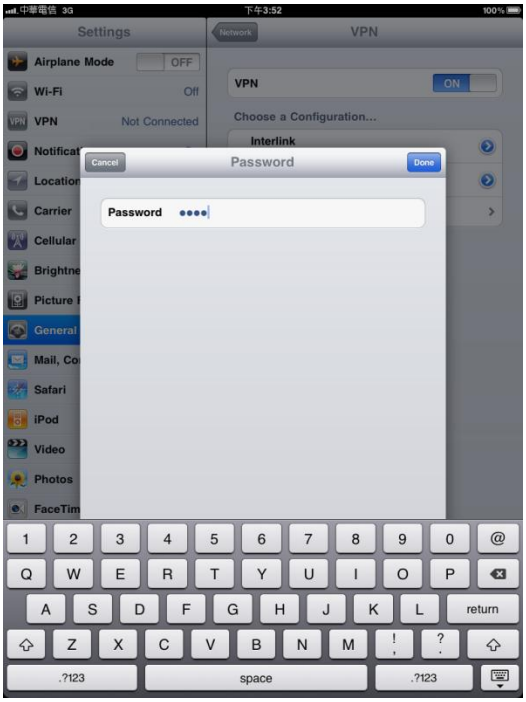
iOS mobile client configuration

Step 1: **Settings > General > Network > VPN > Add configuration** and insert needed L2TP VPN settings



Step 2: Choose the VPN and turn on

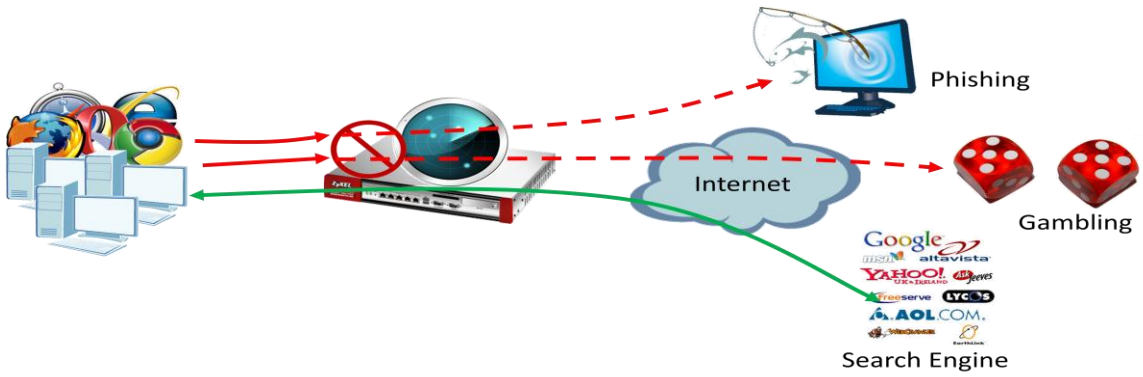
Step 3: Insert L2TP password.



Step 4: Visit an Intranet web page.

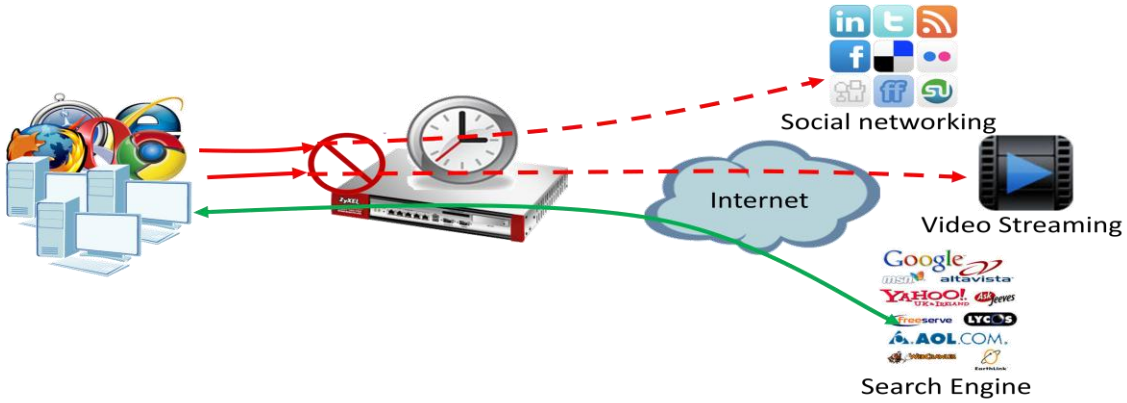
Scenario 5 - Deploying Content Filtering to Manage Employee Browsing Behavior

During their daily productive work for the company, working crew needs to surf the Internet to search for information to conduct their jobs. Browsing websites that are irrelevant to work is a waste of human resources as well as a waste of company network resources. There're also some unsafe websites which may contain phishing or malicious programs. These unsafe websites should also be avoided. So the network administrator needs to make policies to prevent these undesirable types of browsing.



5.1 Application scenario

During office hours, the employees should dedicate their time to their jobs and be restricted from browsing websites irrelevant to their work. But the manager should be able to access all websites without restriction at all times with the exception of unsafe websites. At other times outside of office hours, the restrictions for employees can be removed. The employees may access all websites except ones that pose a security threat (unsafe).



5.2 Configuration guide

Network conditions:

USG:

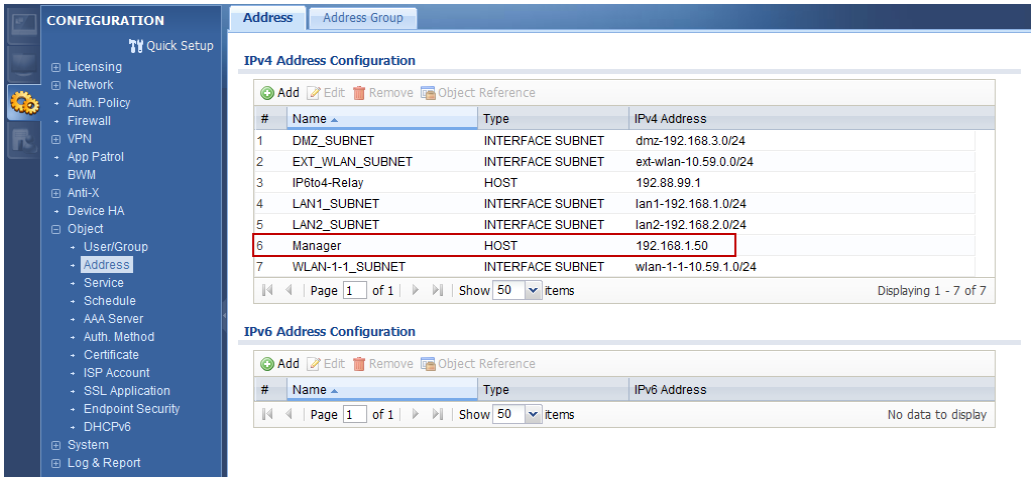
- LAN1 subnet: 192.168.1.0/24
- Manager's IP: 192.168.1.33

Goals to achieve:

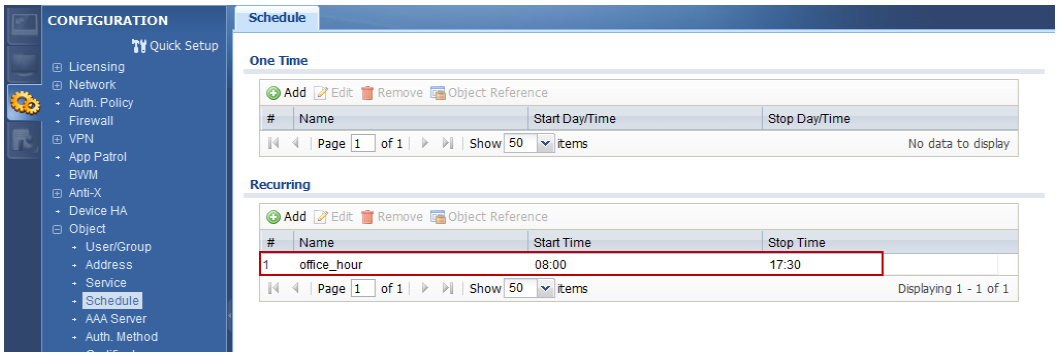
1) The manager can access all websites at any time except security threats (unsafe).
2) During office hours, other employees should be restricted from accessing websites that are irrelevant to their work.
3) All employees may access any websites outside of office hours except sites that pose a security threat (unsafe).

USG configuration

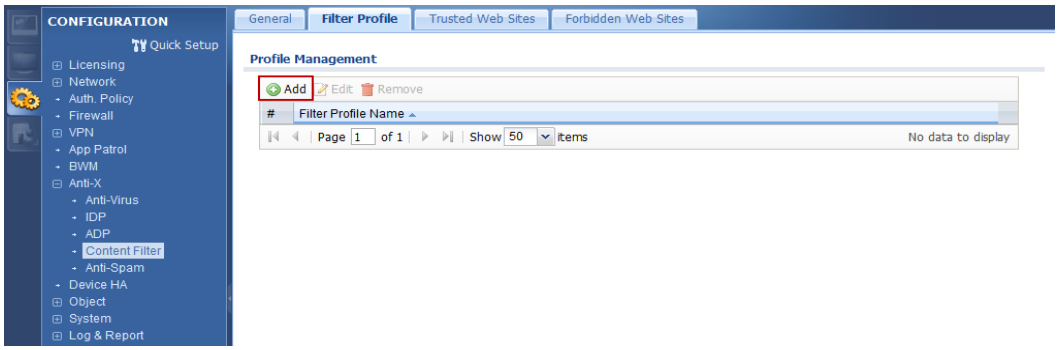
Step 1: Click **Configuration > Object > Address** to add an address object for the manager's IP.



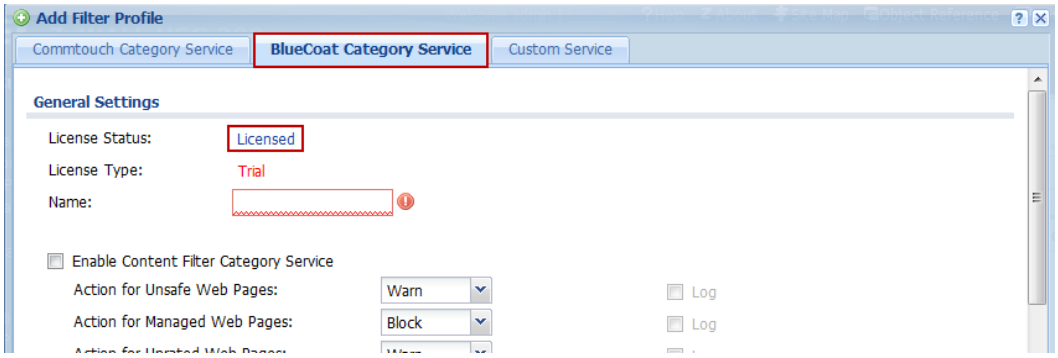
Step 2: Click **Configuration > Object > Schedule** to add a Recurring schedule for office hours.



Step 3: Click **Configuration > Anti-X > Content filter > Filter Profile** to add a filtering profile.



Step 4: Choose your licensed content filtering service and start its setup.



Step 5: Add a profile which allows users to visit all websites.

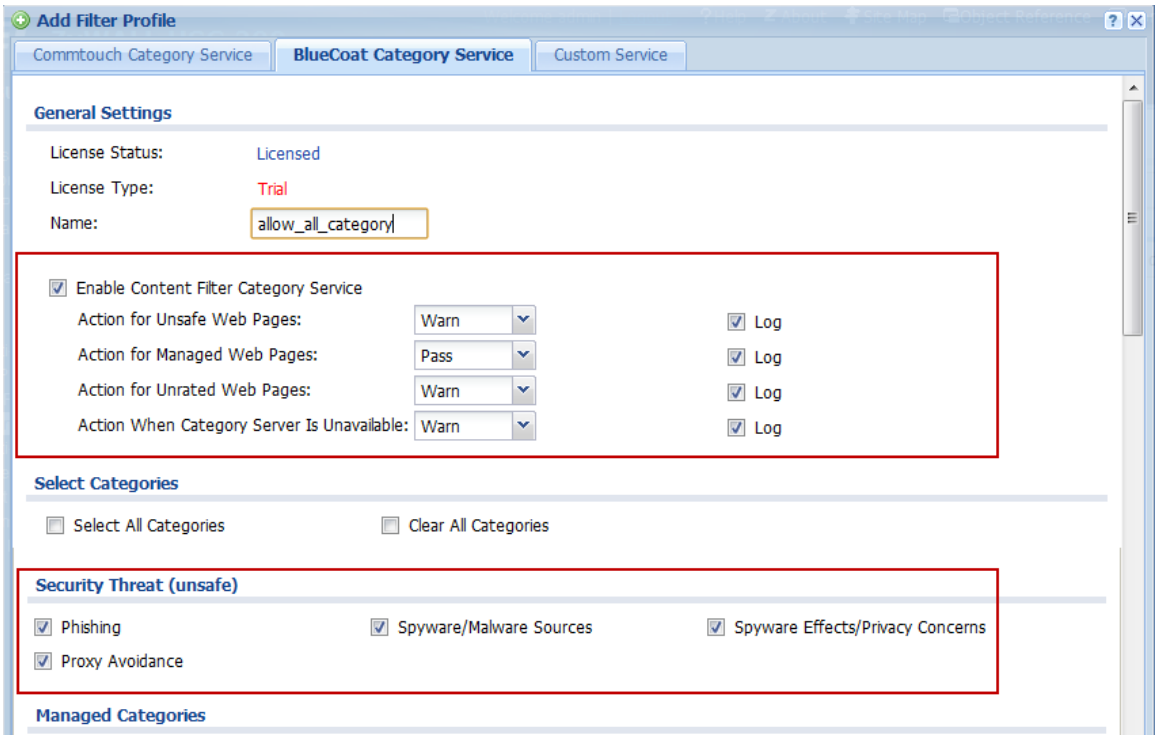
Enable Content Filter Category Service.

Set action for Security threat (Unsafe) to “Warn” and check “Log”.

Set action for Managed Web Pages to “Pass” and check “Log”.

Set action for Unrated Web Pages to “Warn” and check “Log”.

Set action When Category Server is Unavailable to “Warn” and check “Log”.



Step 6: Add a profile for employees to surf only allowed websites.

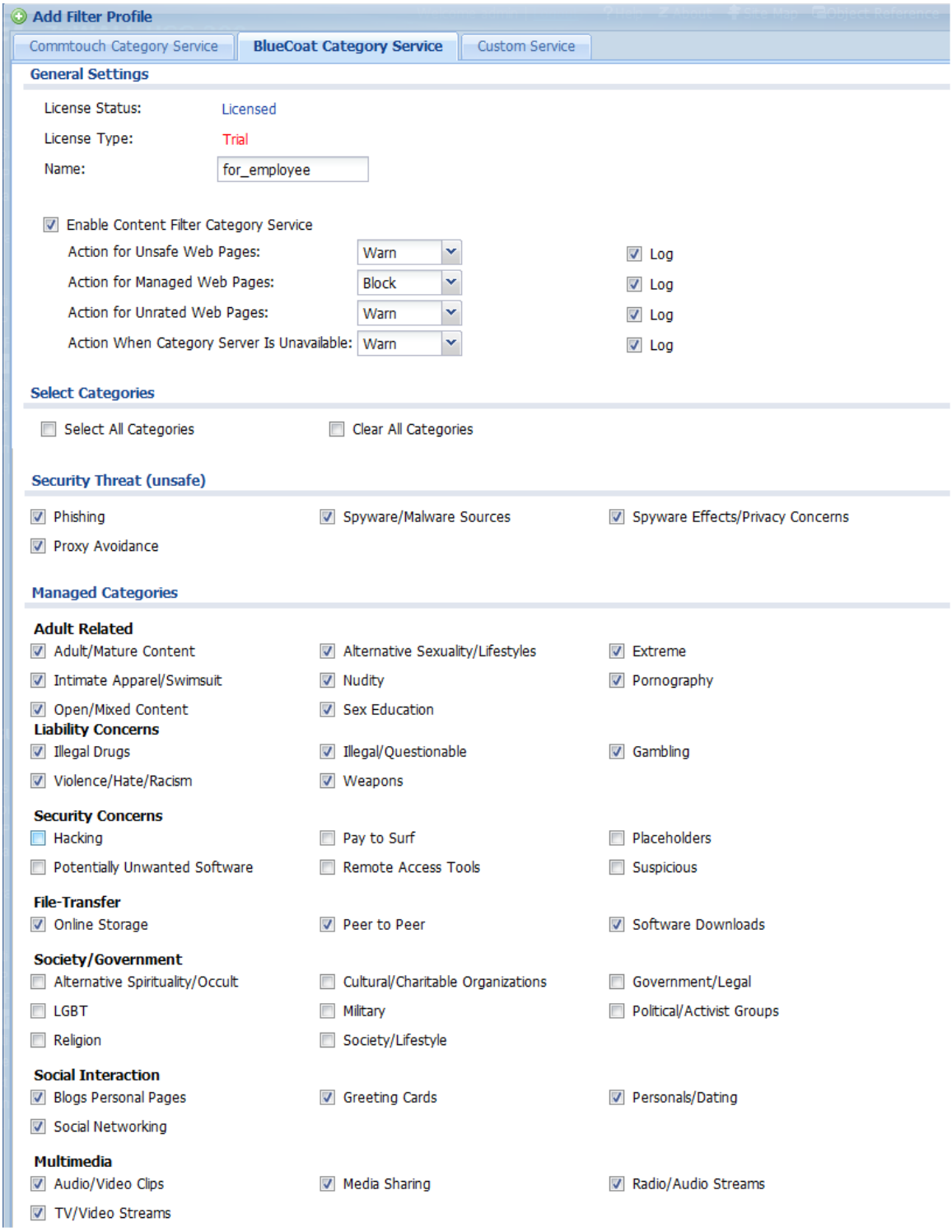
Enable Content Filter Category Service

Set action for Security threat (Unsafe) to “Warn” and check “Log”.

Set action for Managed Web Pages to “Block” and check “Log”.

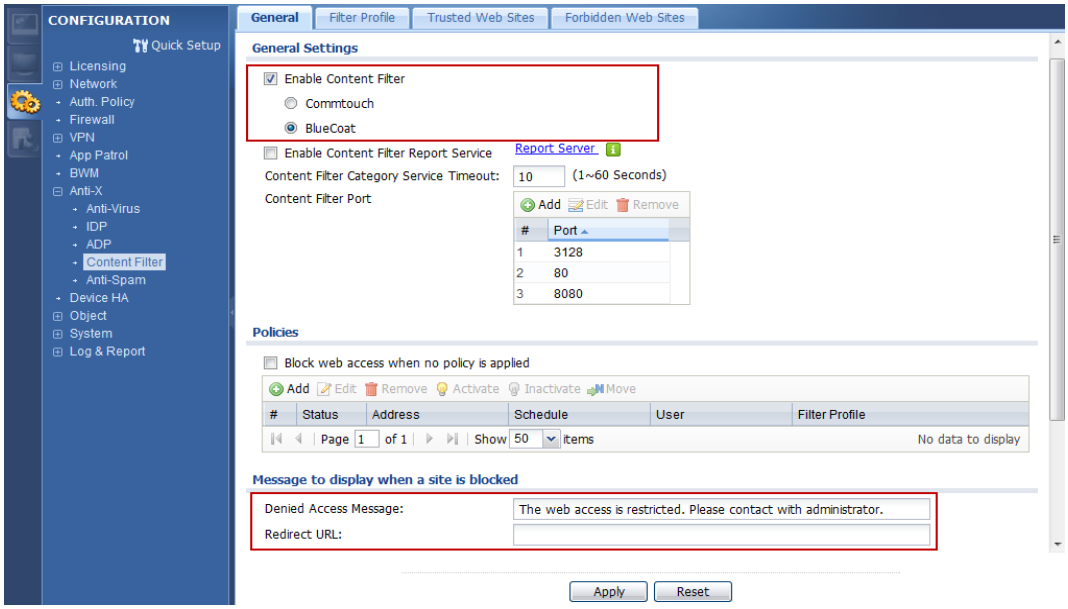
Set action for Unrated Web Pages to “Warn” and check “Log”.

Set action When Category Server is Unavailable to “Warn” and check “Log”.



Step 7: Switch to **Configuration > Anti-X > Content filter > General** to Enable Content Filter.

You can edit the Denied Access Message and Redirect URL if access blocked.

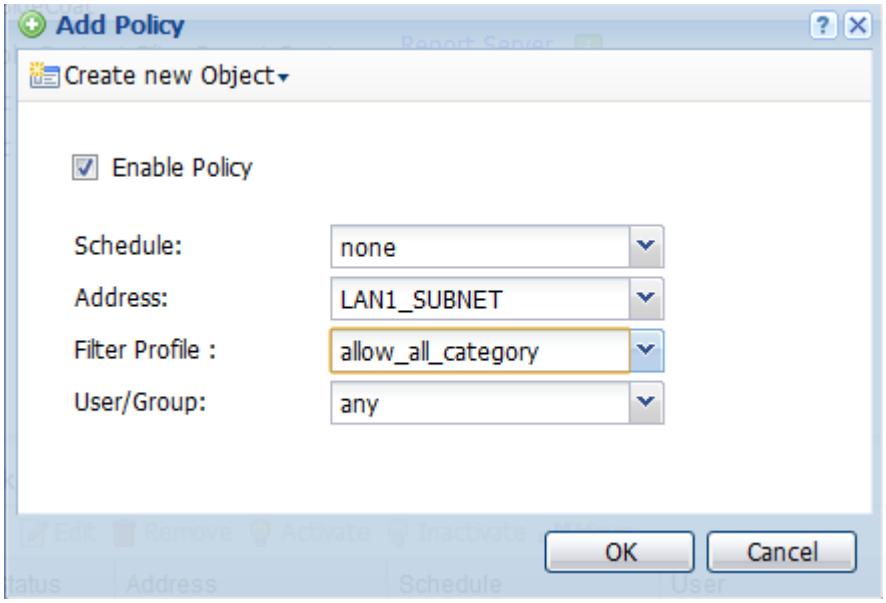


Step 8: Add an access policy for all the staff outside of office hours.

Schedule: none.

Address: LAN1 subnet.

Filter Profile: allow_all_category

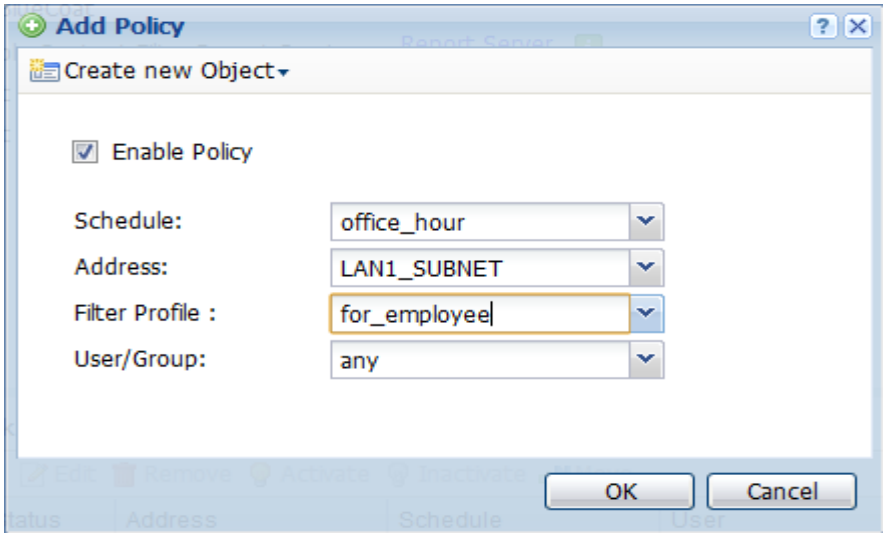


Step 9: Add an access policy for all the employees during office hours.

Schedule: office_hour

Address: select the address object LAN subnet.

Filter Profile: for_employee

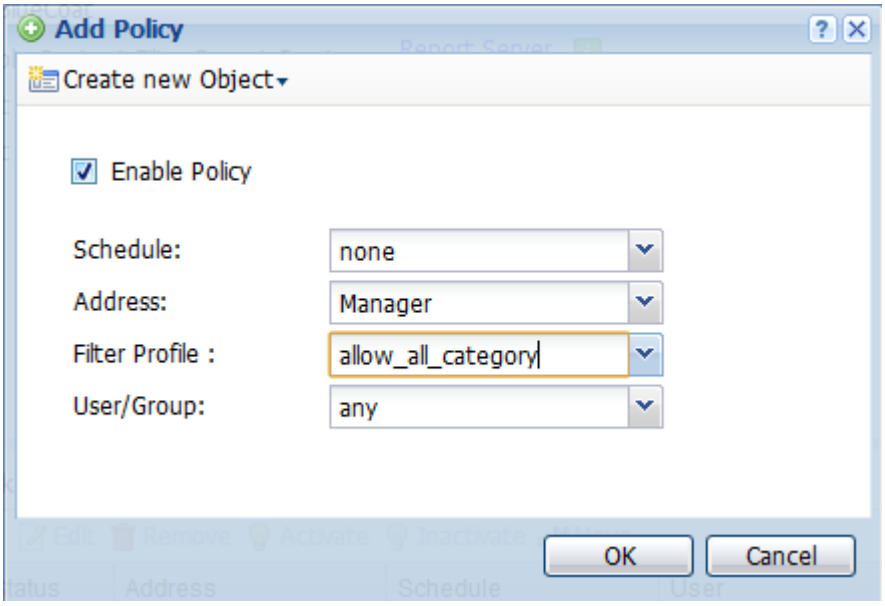


Step 10: Add an access policy for the manager during office hours.

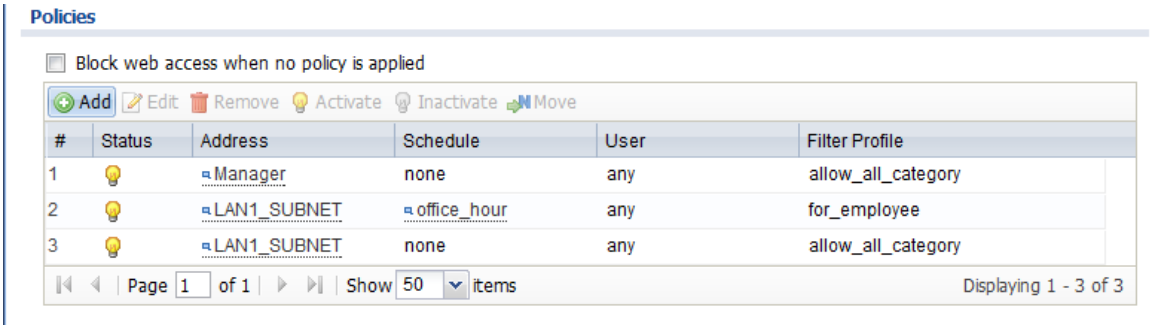
Schedule: none

Address: Manager

Filter Profile: allow_all_category

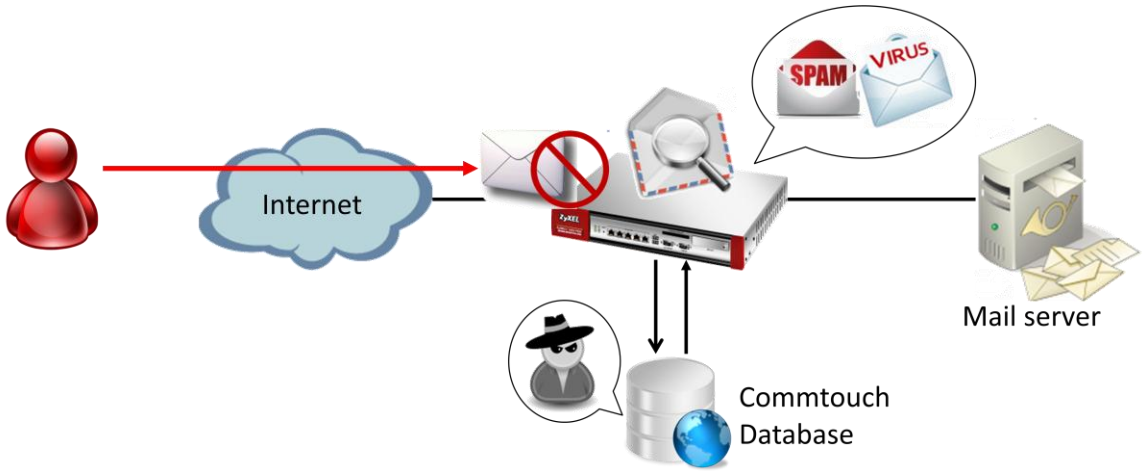


Check the created policies. The USG will check them one by one, and when the manager tries to access a website, he will trigger the first policy.



Scenario 6 - Deploying anti-spam to keep spam off your network

With fraudulent, inappropriate and offensive emails being delivered in vast quantities to adults, children and businesses every day, spam protection is an essential component of your network's security strategy. Spam wastes network users' time and network resources, and can be dangerous too. A ZyWALL USG includes an anti-spam feature to keep spam off your network.



6.1 Anti-Spam Check flow introduction

The ZyWALL USG Anti-Spam checks if sender/mail relay IP is in White/Black list when SMTP/POP3 session is established. If it cannot find it in White/Black list, it will ask to Commtouch IP Reputatation server. If the IP Reputation server reports no risk, the USG will start to scan mail's header and content, if the header/content satisfies the conditions defined by the user, Anti-Spam will act according to the user configuration.

Check flow contains the following steps:

1. Check if sender or mail relay IP address is in White List.
2. Check if sender or mail relay IP address is in Black List.
3. Check mail relay IP address on Commtouch IP Reputation server (SMTP only).
4. Check if mail's header satisfies other conditions in White list.
5. Check if mail's header satisfies other conditions in black list.
6. Scan mail content, check Virus Outbreak and check DNSBL

6.2 Configuration guide

Network conditions:

Trusted email address: admin@zyxel.com

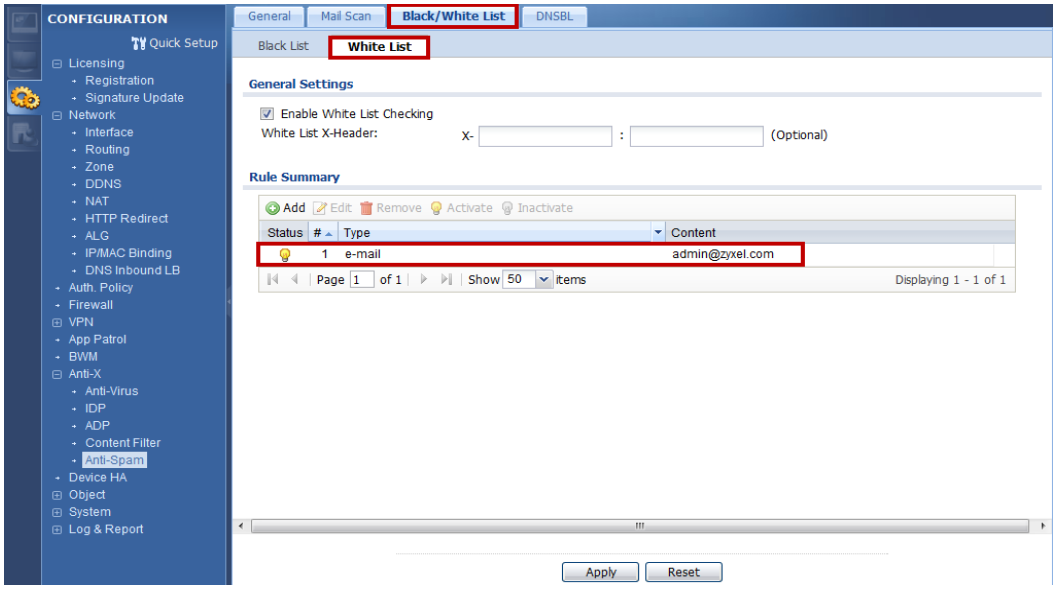
Goals to achieve:

Add [Spam] tag on all suspected spam mail except coming from a trusted email address.

USG configuration

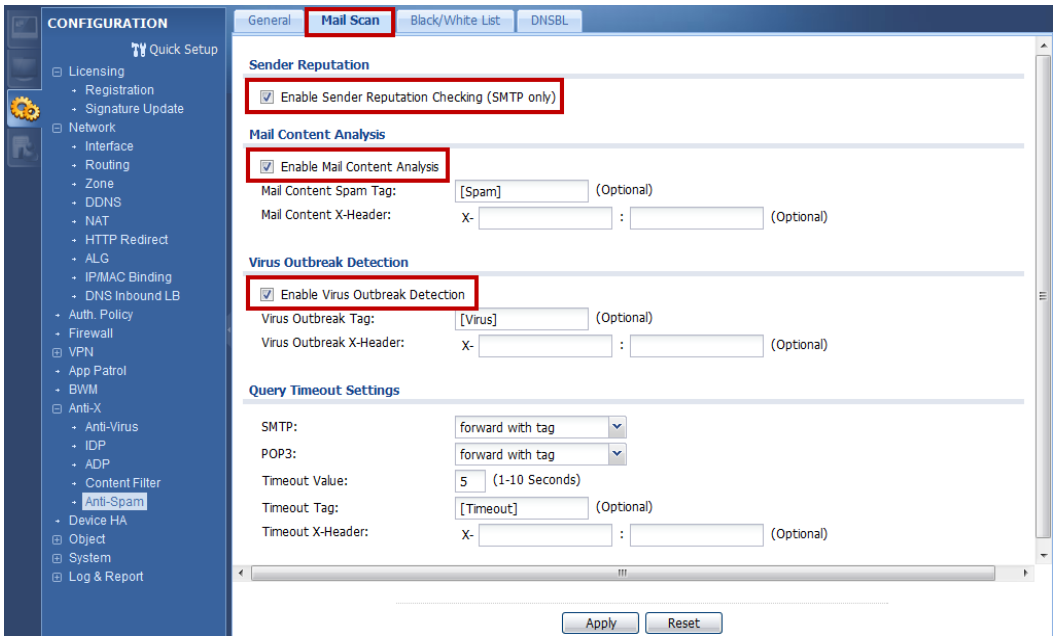
Step 1: Click Configuration > Anti-X > Anti Spam > Black/White List

Step 2: Enable White List Checking and add a rule for admin@zyxel.com



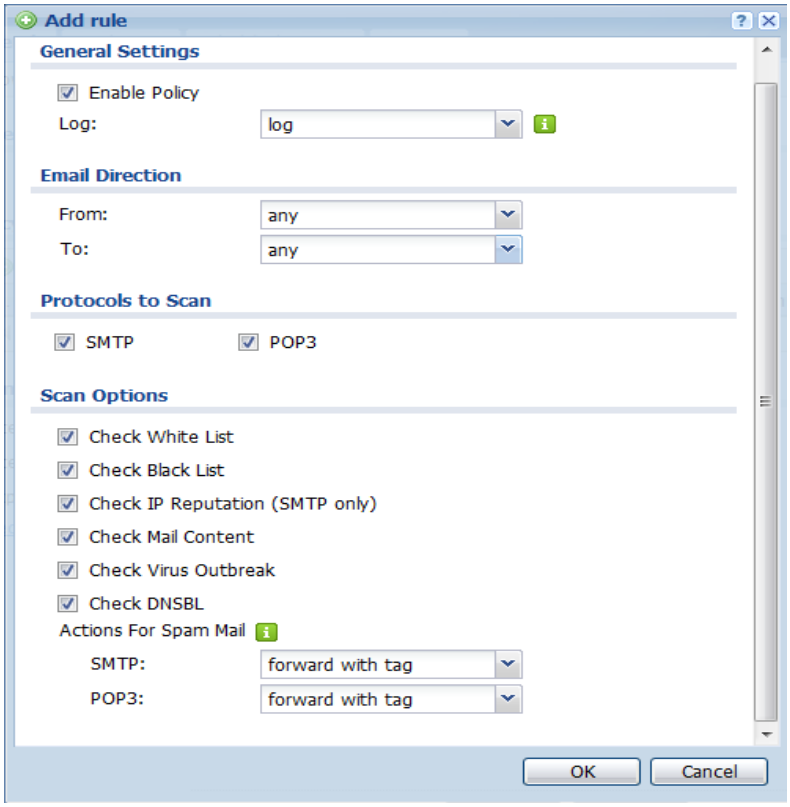
Step 3: Switch **to Configuration > Anti-X > Anti Spam > Mail Scan.**

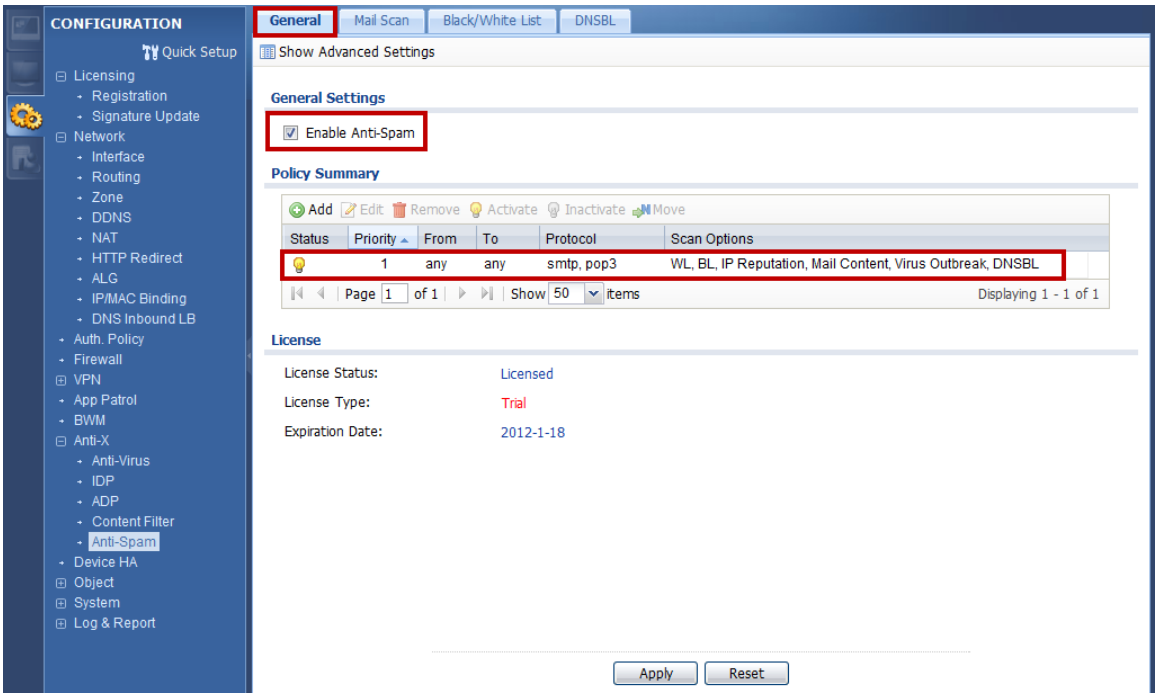
Step 4: Enable Sender Reputation Checking, Mail Content Analysis and Virus Outbreak Detection



Step 5: Switch **to Configuration > Anti-X > Anti Spam > General.**

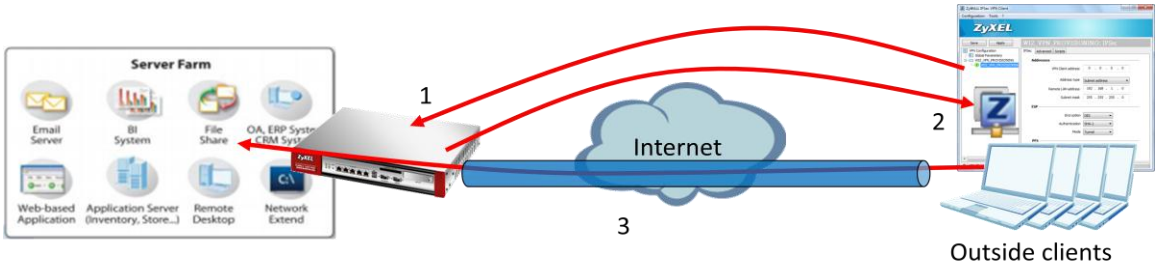
Step 6: Add a rule for Anti-Spam and enable it.





Scenario 7 – One click Setup VPN connection to headquarters

In an enterprise, employees often go on business trips around the world. They might need to access resources inside headquarters during these trips, however, this brings security concerns. One of the solutions is to build an IPsec VPN tunnel to achieve the purpose, but it presents a difficulty for non-technical employees and will increase work load for network administrators who need to assist users with setup. A ZyWALL USG provides an EASY VPN solution with a downloadable VPN configuration file for simple import of configuration and building of the VPN connection.



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

7.2 Configuration guide

Network conditions:

USG:

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

Outside user:

- IP: 114.16.87.56

IPSec VPN conditions:

Phase 1:

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

Phase 2:

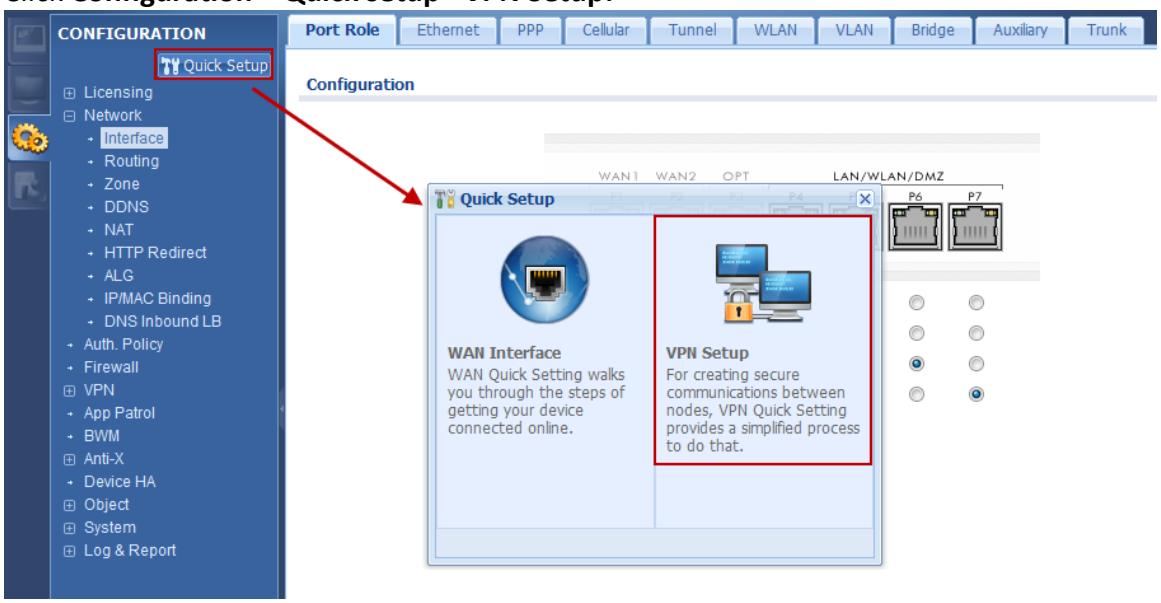
- Encapsulation Mode: Tunnel mode
- Active protocol: ESP
- Encryption algorithm: DES
- Authentication algorithm: SHA1
- Perfect Forward Secrecy: none

Goals to achieve:

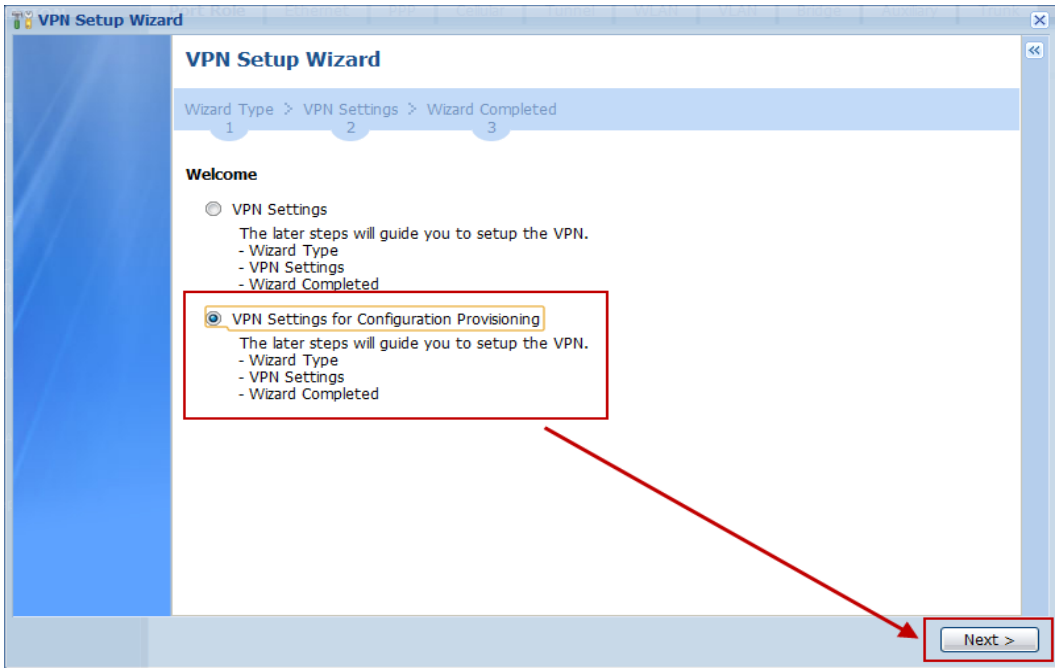
Provide an easy way for outside users to build up an IPSec VPN tunnel by using the ZyWALL IPSec VPN Client software for accessing internal resources.

USG configuration

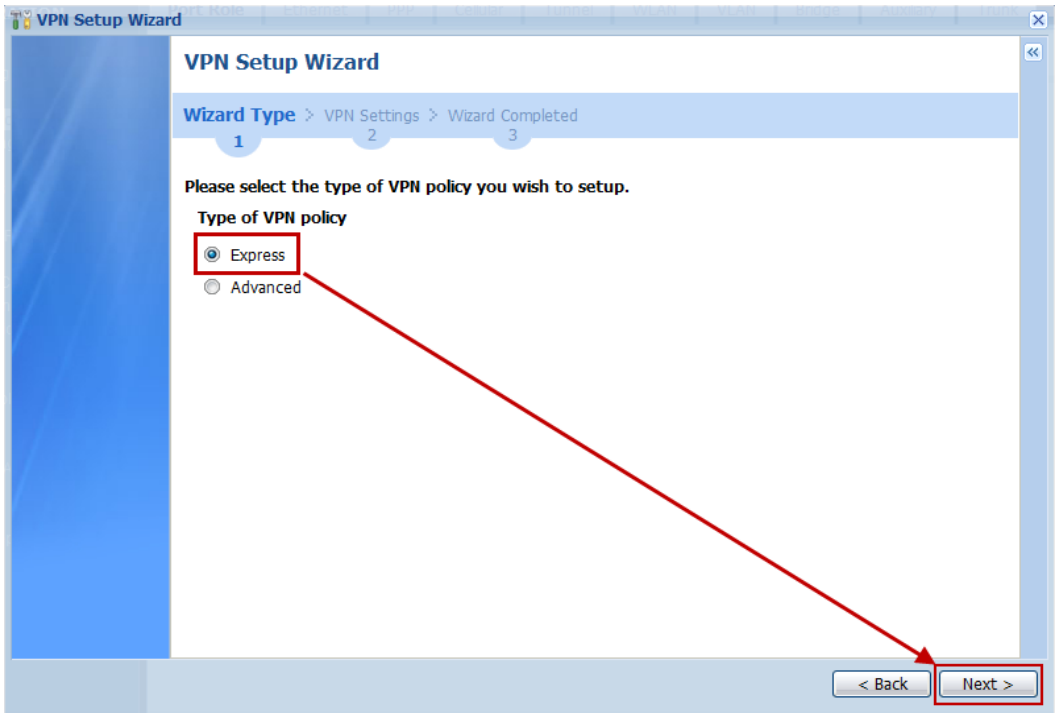
Step 1: Click **Configuration > Quick setup >VPN Setup.**



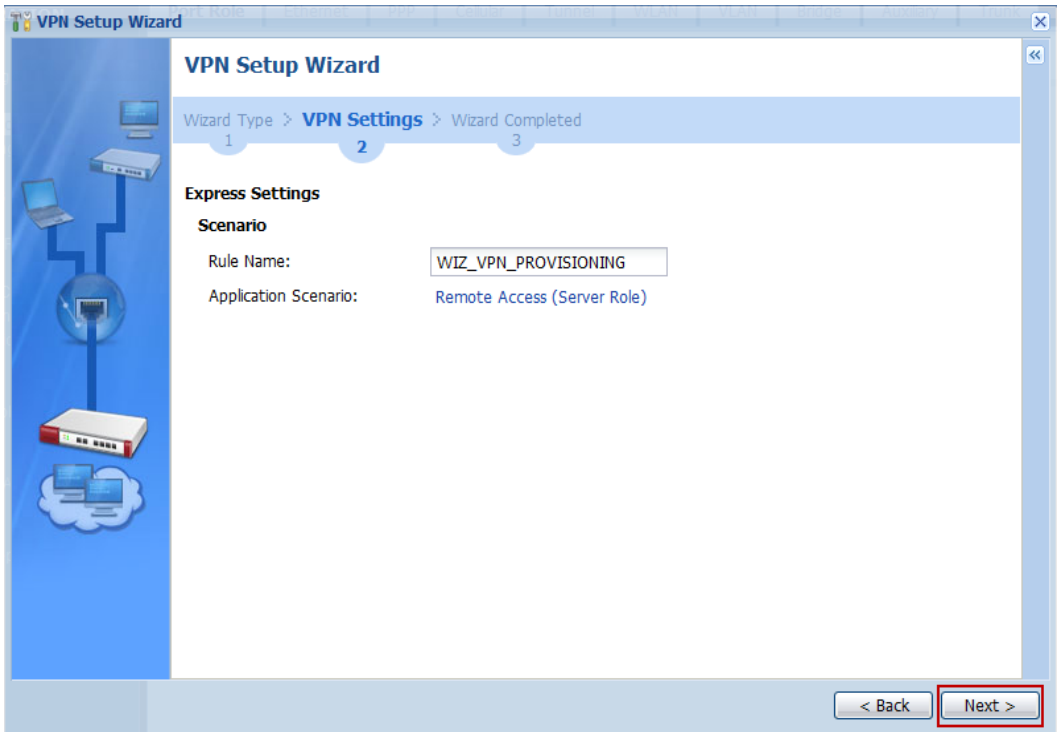
Step 2: Select “VPN settings for Configuration Provisioning”.



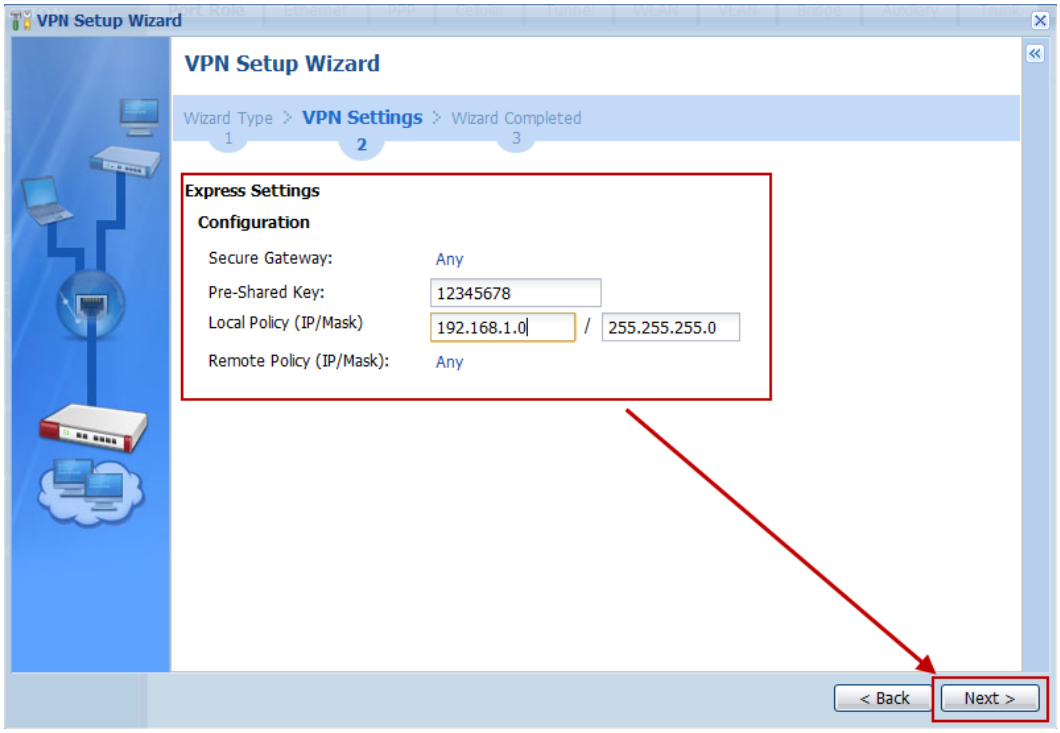
Step 3: Select “Express” (or select “Advanced” to define detailed settings manually).



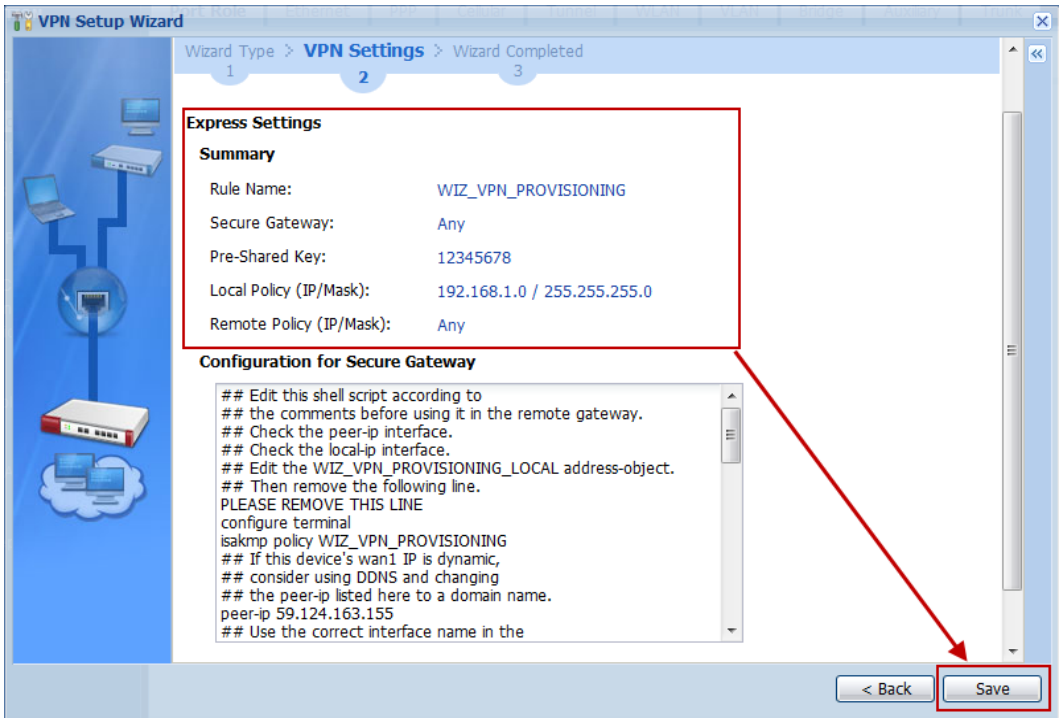
Step 4: Change Rule Name if needed.



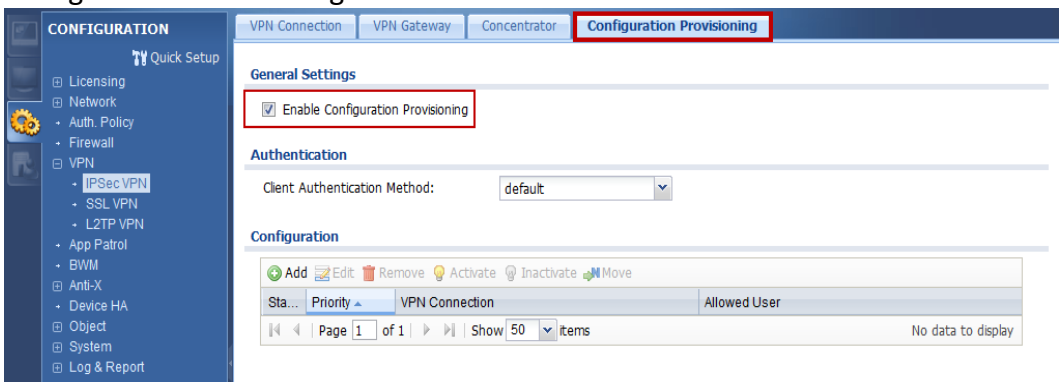
Step 5: Fill in Pre-shared key and local policy.



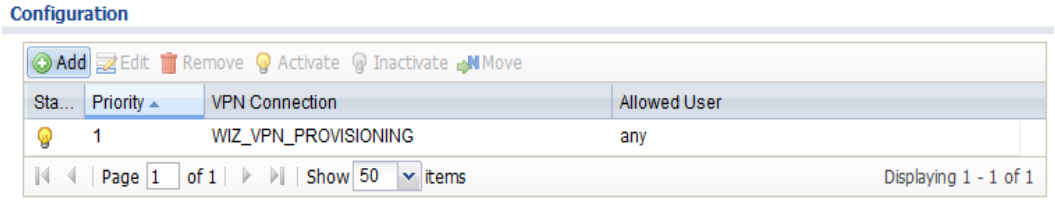
Step 6: Check if IPSec VPN configuration is correct and save the settings.



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

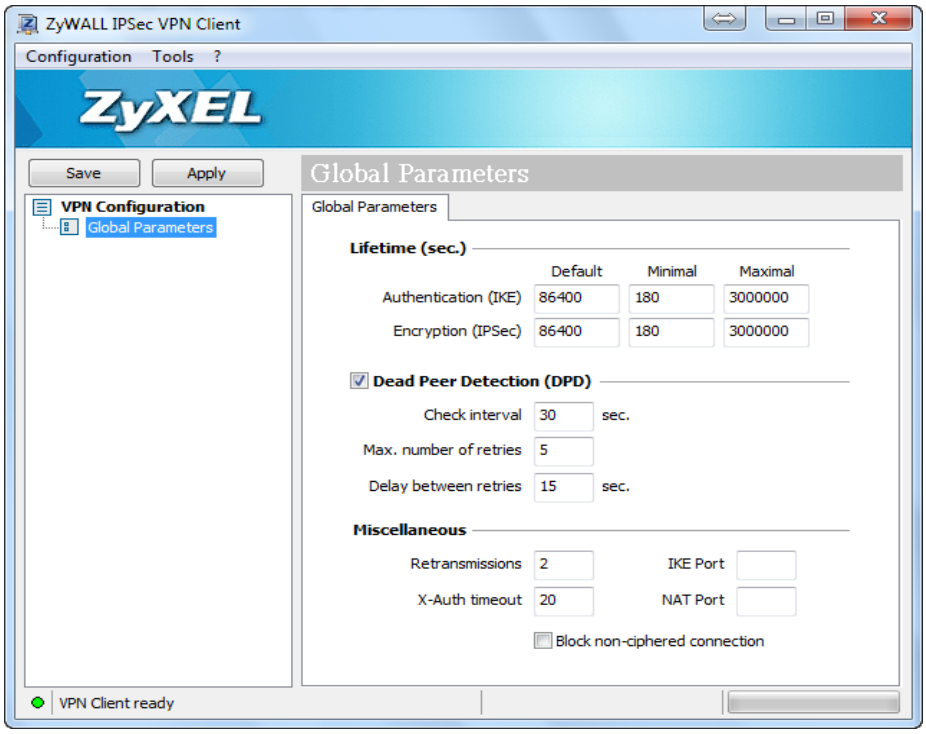


Step 8: Create a provisioning rule for any user

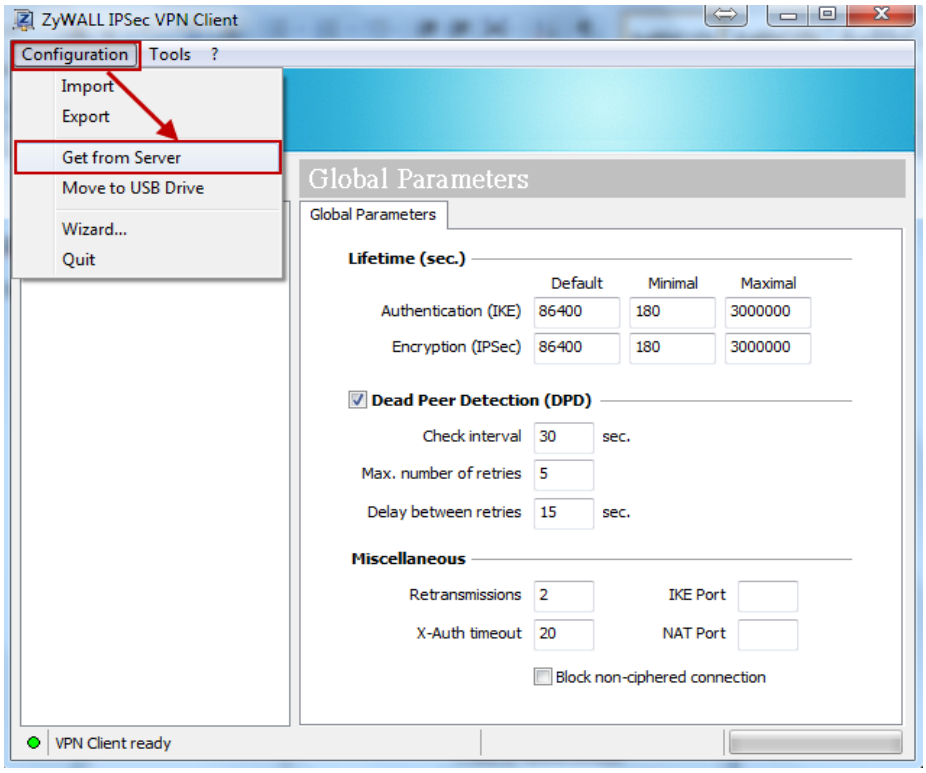


ZyWALL IPSec VPN Client software configuration

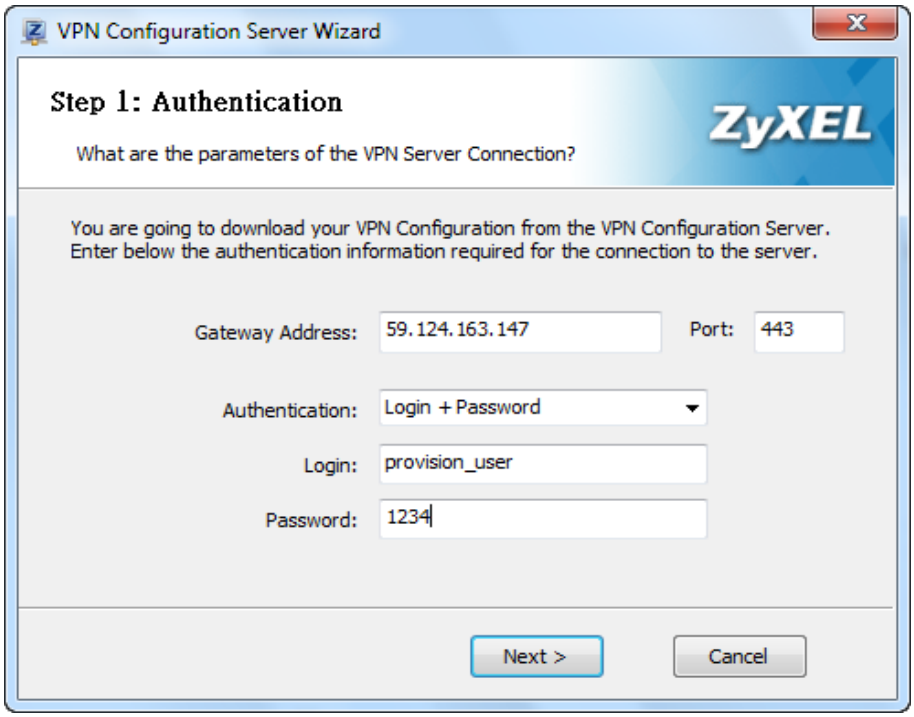
Step 1: Execute ZyWALL IPSec VPN Client



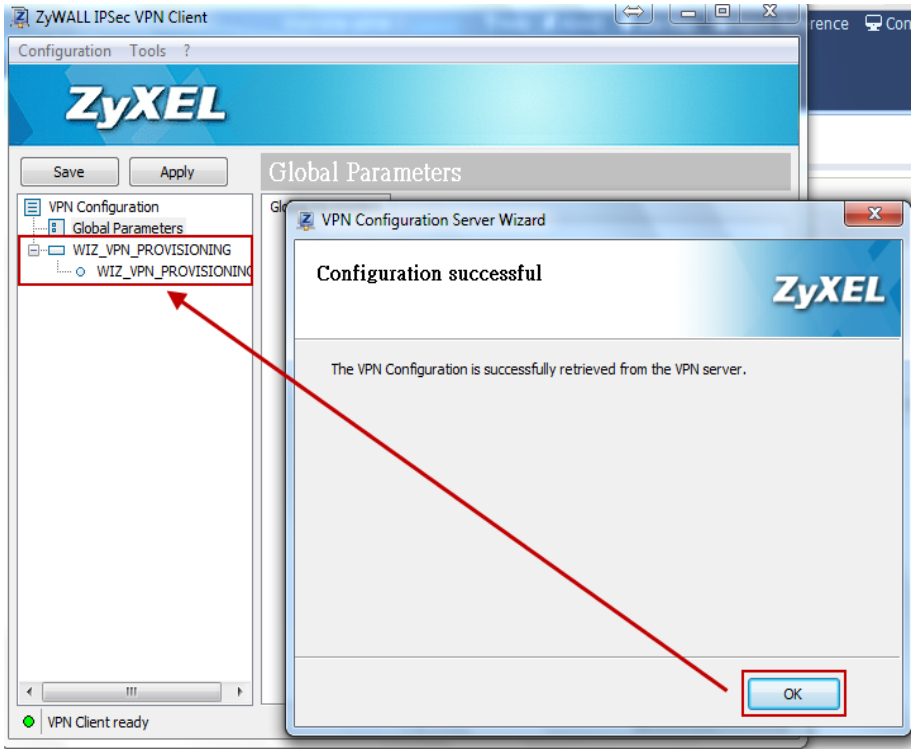
Step 2: Click **Configuration > Get from Server**



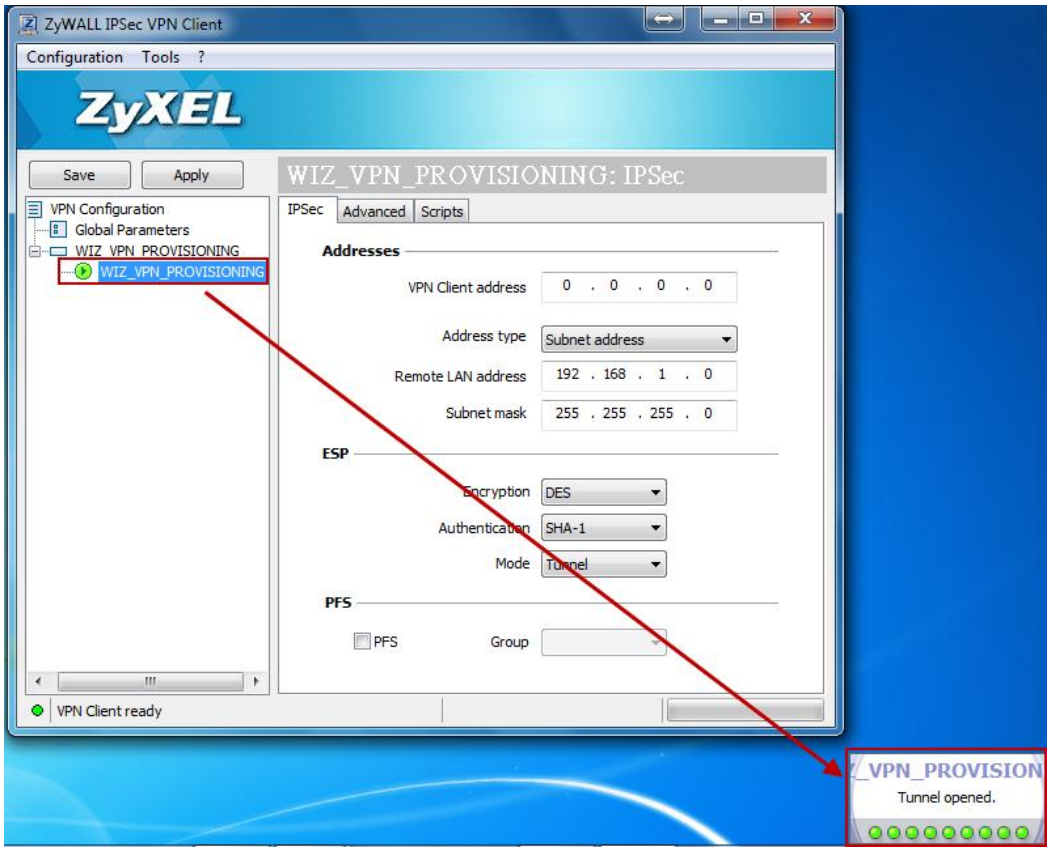
Step 3: Fill in authentication information and click “Next”



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



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



Step 6: Access internal resources.