

# ZyWALL USG 2000

Unified Security Gateway

## Support Notes

Revision 2.10

Dec, 2008



## INDEX

The comparison of ZyNOS and ZLD.....	8
1. Deploying VPN.....	9
1.1 Extended Intranets.....	11
1.1.2 Site to Site VPN solutions (ZyWALL 1050 ⇔ ZyWALL USG 2000): .....	11
1.2 Extranet Deployment .....	18
1.2.1 Site to site VPN solutions (ZyWALL USG 2000 to ZyWALL70).....	19
1.2.2 Interoperability – VPN with other vendors .....	23
1.2.2.1 ZyWALL with FortiGate VPN Tunneling.....	23
1.2.2.2 ZyWALL with NetScreen VPN Tunneling .....	30
1.2.2.3 ZyWALL with SonicWall VPN Tunneling.....	38
1.3 Remote Access VPN .....	45
1.3.1 IPSec VPN for Remote Access .....	45
1.3.1.1 Steps to configure.....	47
1.3.2 SSL VPN Application - Reverse Proxy.....	52
1.3.2.1 Scenario topology.....	52
1.3.2.2 Configuration flow .....	52
1.3.2.3 Configuration procedure .....	52
1.3.3 SSL VPN Application – Network Extension .....	55
1.3.3.1 Scenario topology.....	55
1.3.3.2 Configuration flow .....	55
1.3.3.3 Configuration procedure .....	56
1.3.4 L2TP over IPSec Application.....	62
1.3.4.1 Scenario topology.....	62
1.3.4.2 Configuration flow .....	62
1.3.4.3 Configuration Procedure .....	62
1.4 Large-scale VPN Deployment .....	73
1.4.1 Fully Meshed Topology .....	73
1.4.2 Star Topology .....	74
1.4.3 Star-Mesh Mixed Topology.....	83
1.5 Device HA.....	99
1.5.1 Device HA.....	101
1.5.1.1 Configuration procedure .....	101
1.5.2 Device High Availability (HA) Active-Passive mode.....	113
1.5.2.1 Scenario Topology .....	113

1.5.2.2 Configuration Flow .....	113
1.5.2.3 Configuration procedure .....	114
1.5.2.4 Steps to configure.....	115
2. Security Policy Enforcement.....	125
2.1 Managing IM/P2P Applications .....	125
2.1.1 Why bother with managing IM/P2P applications?.....	125
2.1.2 What does ZyWALL USG 2000 provide for managing IM/P2P applications? .....	126
2.1.3 Configuration Example .....	126
2.2 Zone-based Anti-Virus Protection.....	134
2.2.1 Applying Zone-Based Anti-Virus to ZyWALL USG 2000 .....	134
2.2.2 Enabling Black and White List .....	141
2.2.3 Enabling Anti-Virus Statistics Report .....	142
2.2.4 Dual AV .....	143
2.3 Configuring ZyWALL USG 2000 as a Wireless Router .....	143
2.3.1 Configuration procedure .....	143
2.3.2 MAC filter in WLAN.....	145
2.4 Mobility Internet Access .....	147
2.4.1 Utilize 3G Wireless for Accessing the Internet .....	148
2.4.1.1 Configuration procedure .....	149
3. Seamless Incorporation .....	156
3.1 Transparent Firewall.....	156
3.1.1 Bridge mode & Router (NAT) mode co-exist .....	156
3.1.2 NAT & Virtual Server.....	159
3.2 Zone-based IDP Protection .....	162
3.2.1 Applying Zone-Based IDP to ZyWALL USG 2000.....	163
3.3 Anti-spam on the ZyWALL USG 2000.....	169
3.3.1 How Anti-Spam works on ZyWALL USG .....	170
3.3.2 Using DNSBL (DNS-based blacklist).....	170
3.3.2.1 Application scenario to apply DNSBL.....	170
3.3.2.1.1 Scenario I: Email server is located in the ISP/ Internet .....	170
3.3.2.1.2 Scenario II: Company's Email server located in the DMZ .....	173
3.3.3 Using Black/White list (B/W list) .....	176
3.3.3.1 Configuration procedure .....	176
3.3.3.2 Scenario topology.....	177
3.3.3.3 Steps to configure B/W list .....	177
3.4 Guaranteed Quality of Service .....	180
3.4.1 Priority & Bandwidth management .....	181

FAQ.....	188
A. Device Management FAQ.....	188
A01. How can I connect to ZyWALL USG 2000 to perform administrator's tasks?	188
A02. Why can't I login into ZyWALL USG 2000? .....	188
A03. What's difference between "Admin Service Control" and "User Service Control" configuration in GUI menu System > WWW? .....	189
A04. Why ZyWALL USG 2000 redirects me to the login page when I am performing the management tasks in GUI? .....	190
A05. Why do I lose my configuration setting after ZyWALL USG 2000 restarts? ...	190
A06. How can I do if the system is keeping at booting up stage for a long time?.....	190
B. Registration FAQ.....	192
B01. Why do I need to do the Device Registration?.....	192
B02. Why do I need to activate services? .....	192
B03. Why can't I active trial service? .....	192
B04. Will the UTM service registration information be reset once restore configuration in ZyWALL USG 2000 back to manufactory default? .....	192
C. File Manager FAQ.....	193
C01. How can ZyWALL USG 2000 manage multiple configuration files? .....	193
C02. What are the configuration files like startup-config.conf, system-default.conf and lastgood.conf?.....	193
C03. Why can't I update firmware? .....	193
C04. What is the Shell Scripts for in GUI menu File manager > Shell Scripts?.....	194
C05. How to write a shell script? .....	194
C06. Why can't I run shell script successfully? .....	194
D. Object FAQ.....	195
D01. Why does ZyWALL USG 2000 use object?.....	195
D02. What's the difference between Trunk and the Zone Object? .....	196
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? .....	196
E. Interface FAQ .....	197
E01. How to setup the WAN interface with PPPoE or PPTP?.....	197
E02. How to add a virtual interface (IP alias)? .....	197
E03. Why can't I get IP address via DHCP relay?.....	197
E04. Why can't I get DNS options from ZyWALL's DHCP server? .....	197
E05. Why does the PPP interface dials successfully even its base interface goes down? .....	198
F. Routing and NAT FAQ.....	199



F01. How to add a policy route? .....	199
F02. How to configure local loopback in ZyWALL USG 2000?.....	199
F03. How to configure a NAT? .....	203
F04. After I installed a HTTP proxy server and set a http redirect rule, I still can't access web. Why? .....	204
F05. How to limit some application (for example, FTP) bandwidth usage? .....	204
F06. What's the routing order of policy route, dynamic route, and static route and direct connect subnet table? .....	204
F07. Why ZyWALL USG 2000 cannot ping the Internet host, but PC from LAN side can browse internet WWW? .....	205
F08. Why can't I ping to the, Internet, after I shutdown the primary WAN interface?205	
F09. Why the virtual server or port trigger does not work?.....	205
F10. Why port trigger does not work? .....	205
F11. How do I use the traffic redirect feature in ZyWALL USG 2000? .....	206
F12. Why can't ZyWALL learn the route from RIP and/or OSPF? .....	206
G. VPN and Certificate .....	207
G01. Why can't the VPN connections dial to a remote gateway?.....	207
G02. VPN connections are dialed successfully, but the traffic still cannot go through the IPsec tunnel. ....	207
G03. Why ZyWALL USG 2000 VPN tunnel had been configured correctly and the VPN connection status is connected but the traffic still can not reach the remote VPN subnet?.....	207
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. ....	208
G05. Why don't the Inbound/Outbound traffic NAT in VPN work? .....	208
H. Firewall FAQ.....	209
H01. Why doesn't my LAN to WAN or WAN to LAN rule work? .....	209
H02. Why does the intra-zone blocking malfunction after I disable the firewall? ....	209
H03. Can I have access control rules to the device in firewall? .....	209
I. Application Patrol FAQ.....	210
I01. What is Application Patrol? .....	210
I02. What applications can the Application Patrol function inspect? .....	210
I03. Why does the application patrol fail to drop/reject invalid access for some applications?.....	211
I04. What is the difference between "Auto" and "Service Ports" settings in the Application Patrol configuration page? .....	212
I05. What is the difference between BWM (bandwidth management) in Policy Route	

and App. Patrol ? .....	213
I06. Do I have to purchase iCards specifically for using AppPatrol feature? .....	214
I07. Can I configure different access level based on application for different users? .....	214
I08. Can I migrate AppPatrol policy and bandwidth management control from ZLD1.0x to ZLD2.0x? .....	214
J. IDP FAQ .....	215
J01. Why doesn't the IDP work? Why has the signature updating failed? .....	215
J02. When I use a web browser to configure the IDP, sometimes it will popup "wait data timeout" .....	215
J03. When I want to configure the packet inspection (signatures), the GUI becomes very slow. ....	215
J04. After I select "Auto Update" for IDP, when will it update the signatures? .....	215
J05. If I want to use IDP service, will it is enough if I just complete the registration and turn on IDP? .....	215
J06. What are the major design differences in IDP in ZLD1.0x and latest IDP/ADP in ZLD2.0x? .....	215
J07. Does IDP subscription have anything to do with AppPatrol? .....	216
J08. How to get a detailed description of an IDP signature? .....	217
J09. After an IDP signature updated, does it require ZyWALL to reboot to make new signatures take effect? .....	217
K. Content Filtering FAQ .....	218
K01. Why can't I enable external web filtering service? Why does the external web filtering service seem not to be working? .....	218
K02. Why can't I use MSN after I enabled content filter and allowed trusted websites only? .....	218
L. Device HA FAQ .....	219
L01. What does the "Preempt" mean? .....	219
L02. What is the password in Synchronization? .....	219
L03. What is "Link Monitor" and how to enable it? .....	219
L04. Can Link Monitor of Device HA be used in backup VRRP interfaces? .....	220
L05. Why do both the VRRP interfaces of master ZW USG 2000 and backup ZW USG 2000 are activated at the same time? .....	220
M. User Management FAQ .....	221
M01. What is the difference between user and guest account? .....	221
M02. What is the "re-authentication time" and "lease time"? .....	221
M03. Why can't I sign in to the device? .....	221
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? .....	221
M05. What is AAA? .....	222
M06. What are ldap-users and radius-users used for? .....	222
M07. What privileges will be given for ldap-users and radius-users? .....	222
N. Centralized Log FAQ .....	224
N01. Why can't I enable e-mail server in system log settings? .....	224
N02. After I have the entire required field filled, why can't I receive the log mail? ..	224
O. Traffic Statistics FAQ .....	225
O01. When I use "Flush Data" in Report, not all the statistic data are cleared.....	225
O02. Why isn't the statistic data of "Report" exact? .....	225
O03. Does Report collect the traffic from/to ZyWALL itself? .....	225
O04. Why cannot I see the connections from/to ZyWALL itself? .....	225
P. Anti-Virus FAQ .....	226
P01. Is there any file size or amount of concurrent files limitation with ZyWALL USG 2000 Anti-Virus engine? .....	226
P02. Does ZyWALL USG 2000 Anti-Virus support compressed file scanning? .....	226
P03. What is the maximum concurrent session of ZyWALL USG 2000 Anti-Virus engine? .....	226
P04. How many type of viruses can be recognized by the ZyWALL USG 2000? ....	226
P05. How frequent the AV signature will be updated? .....	226
P06. How to retrieve the virus information in detail? .....	226
P07. I cannot download a file from Internet through ZyWALL USG 2000 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? .....	226
P08. Does ZyWALL USG 2000 Anti-Virus engine support Passive FTP? .....	227
P09. What kinds of protocol are currently supported on ZyWALL USG 2000 Anti-Virus engine? .....	227
P10. If the Anti-Virus engine detects a virus, what action it may take? Can it cure the file? .....	227

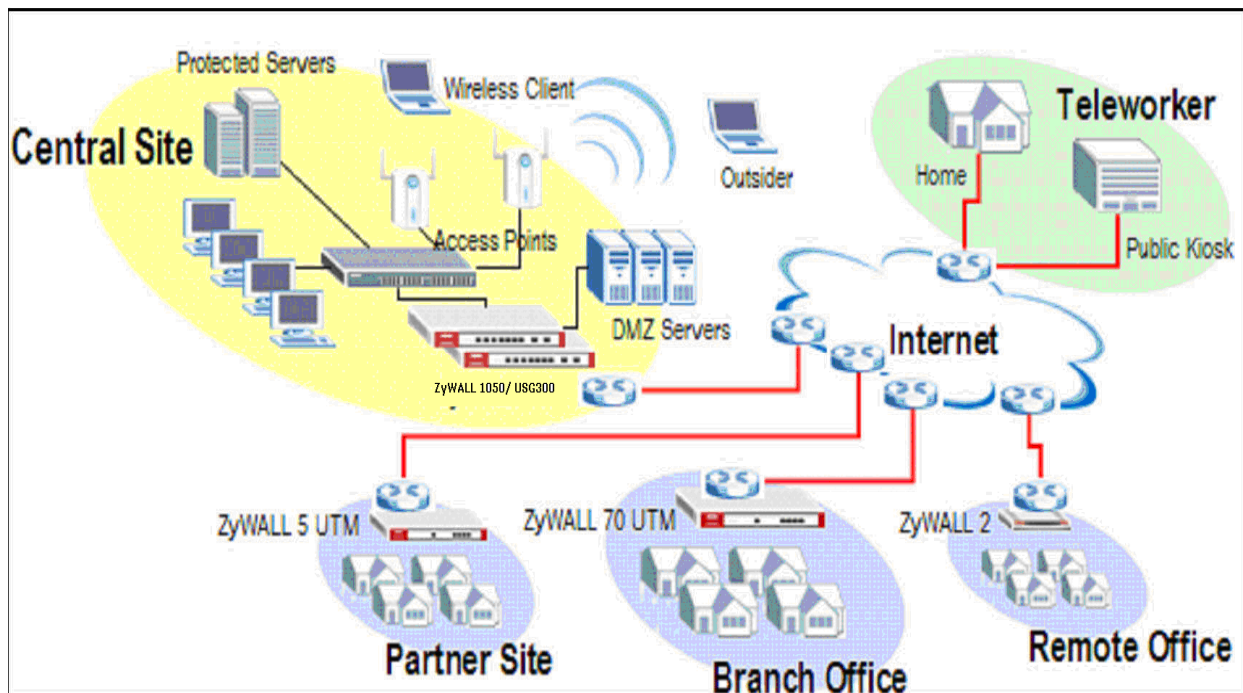
# The comparison of ZyNOS and ZLD

Since ZyXEL USG 2000 adopt ZLD 2.10 as their network operating system. Additionally, ZLD 2.10 provides many new features and new design in GUI. Hence, the layout in ZyNOS might not be the same as the one in ZLD 2.10. Accordingly, we provide a comparison table for your reference.

Platform Feature/Term	ZyNOS	ZLD	Chapter in Support Note
<b>NAT</b>	Advanced > NAT > Address Mapping	Network > Routing > Policy Route SNAT	
	Advanced > NAT Port forwarding	Network > Virtual Server	3.1.2 NAT & Virtual Server
	Advanced > NAT Port Trigger	Network > Routing > Policy Route Port Triggering	
<b>VPN</b>	Security> VPN > Gateway Policy	VPN > IPSec VPN> VPN Gateway	1.1.2 Site to site VPN solutions
	Security> VPN > Network Policy	VPN > IPSec VPN> VPN Connection	1.1.2 Site to site VPN solutions
	Security> VPN > Gateway Policy & Network Policy (Hub & Spoke VPN network)	VPN > IPSec VPN> Concentrator	
<b>Others</b>	Advanced > BW MGMT	AppPatrol & Network > Policy Route	
	Network > LAN/DMZ/WLAN> IP alias	Network > Interface > LAN/DMZ/VLAN/Brid ge> Virtual Interface	
	Wireless > Wi-Fi	Network > Interface > WLAN	
	Wireless > 3G	Network > Interface > Cellular	2.4 Mobility Internet Access
	Security > Auth Server	Object > AAA Server	

# 1. Deploying VPN

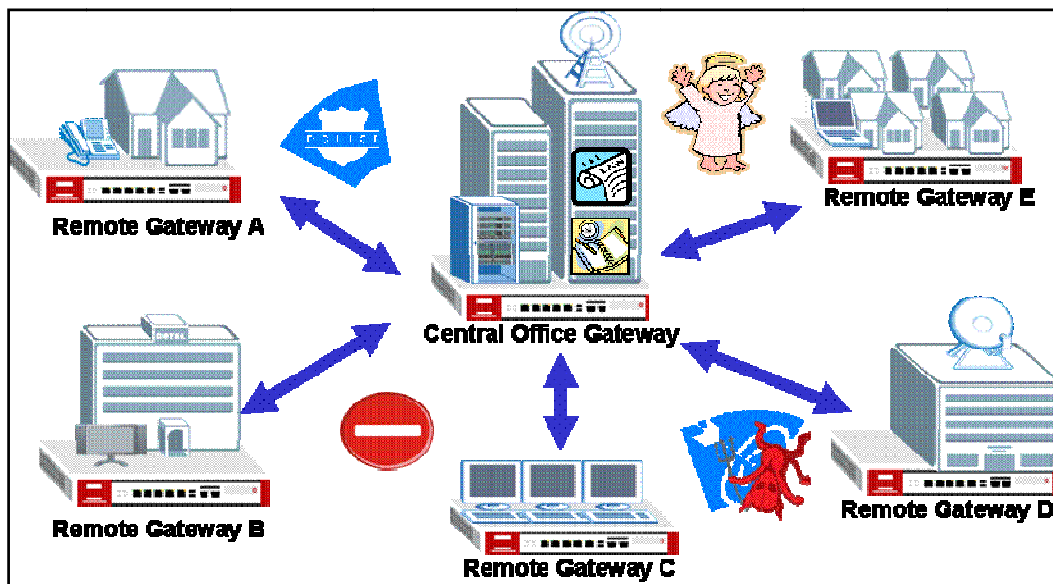
VPN (Virtual Private Network) allows you to establish a virtual direct connection to remote locations or for the telecommuters to access the internal network in the office. VPN is a replacement for the traditional site-to-site lease lines like T1 or ISDN. Through the VPN applications, it reduces setup cost, works for various types of Internet connection devices (ISDN modem, ADSL modem and FTTX...) and is easy to troubleshoot.



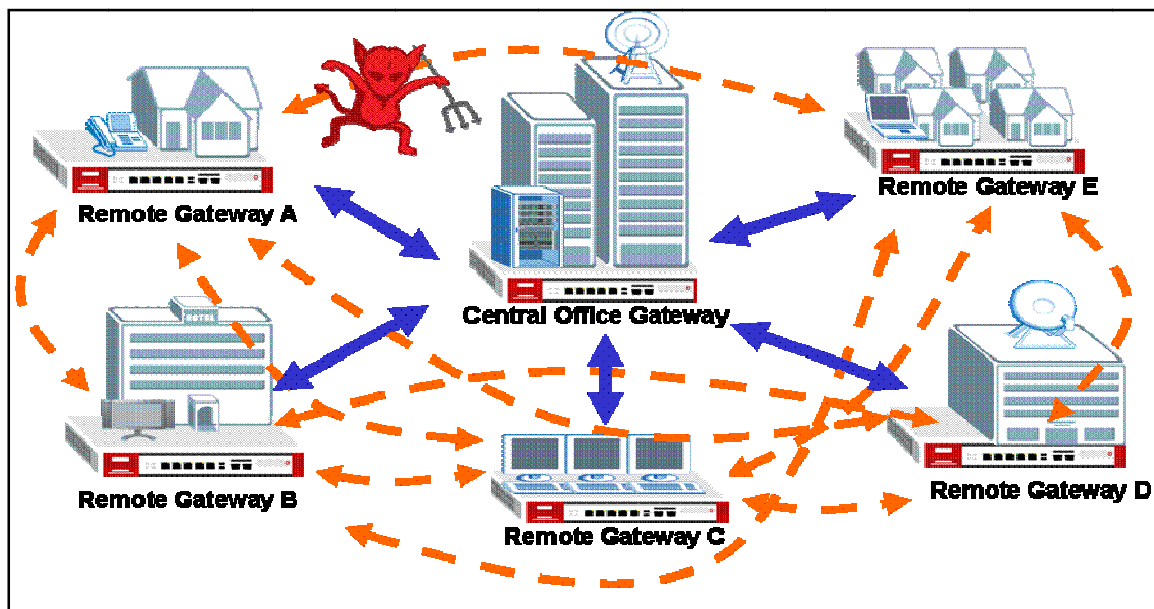
VPN gives you site-to-site connection flexibility. However, with multiple VPN connections between sites, it can become more difficult to maintain. Typically, an administrator has to configure many site-to-site VPN connections to allow a truly global VPN network.

VPN connection management is made easily using the VPN concentrator. The VPN concentrator routes VPN traffic across multiple remote sites without complex setting, thus reduces the configuration overhead and the possibility of improper configuration. The VPN concentrator is also a centralized management tool for administrators because all the traffic sent between remote sites has to go through the central office first and administrators can set up different access control rules. These are based on the source address, remote address, user and schedule to enhance VPN security. To help to reduce network intrusion attacks, administrators can configure the built-in IDP engine to inspect VPN traffic. For easy

troubleshooting and monitoring, the VPN concentrator logs and stores system information and network status for further easy troubleshooting and analysis.



The VPN concentrator enhances the VPN routing ability and helps network administrators in setting up a global VPN network with less effort but stronger security and management possibilities.



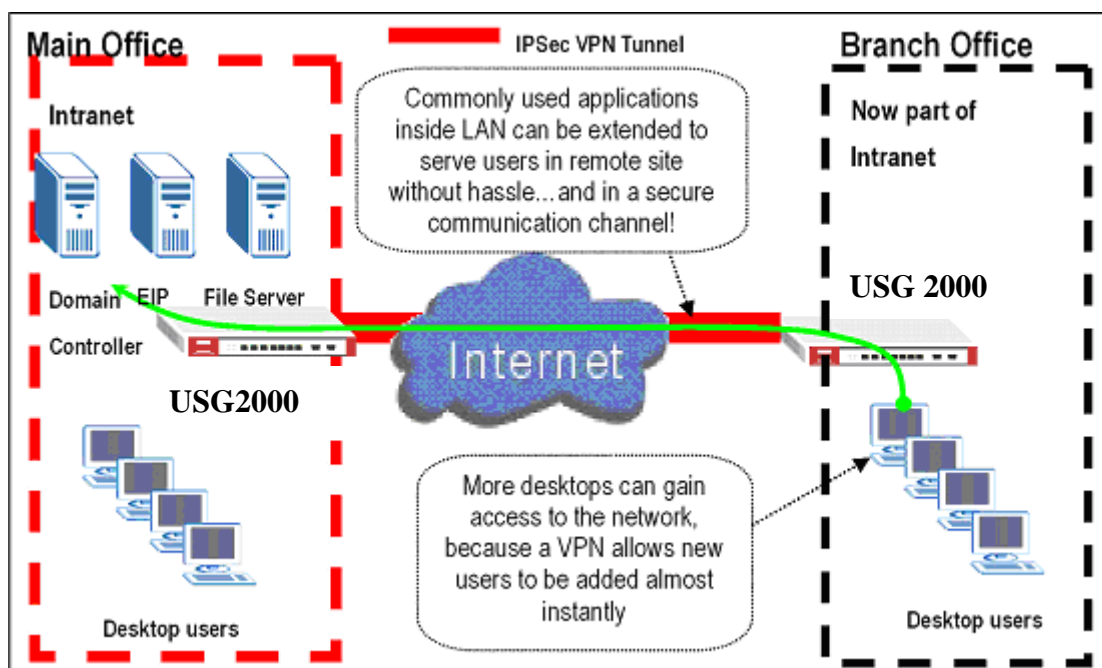
For SMB customer, ZyXEL provides a total VPN solution from a personal client to a 500+ people firewall where all of these devices have the VPN connection ability.

- The benefit from deployment of ZyXEL VPN solutions

- Security and Reliability
- Improved communications
- Increased flexibility
- Lower cost

## 1.1 Extended Intranets

The ZyXEL VPN solutions primarily can be used to extend the intranet and deliver increased connectivity between operation sites. The branch office subnet will be considered a part of main office internet. Therefore, user behind branch office also can use the internal network resources as if he was in the main office. Because of the VPN connection, user will feel like he is using a local LAN even though he is accessing the network resources via Internet. Use of a VPN for smaller branch offices, franchise sites and remote workers provides nearly the same level of connectivity and reliability as a private network. The remote connection cost also can decrease by leveraging the Internet connections to replace expensive leased lines.

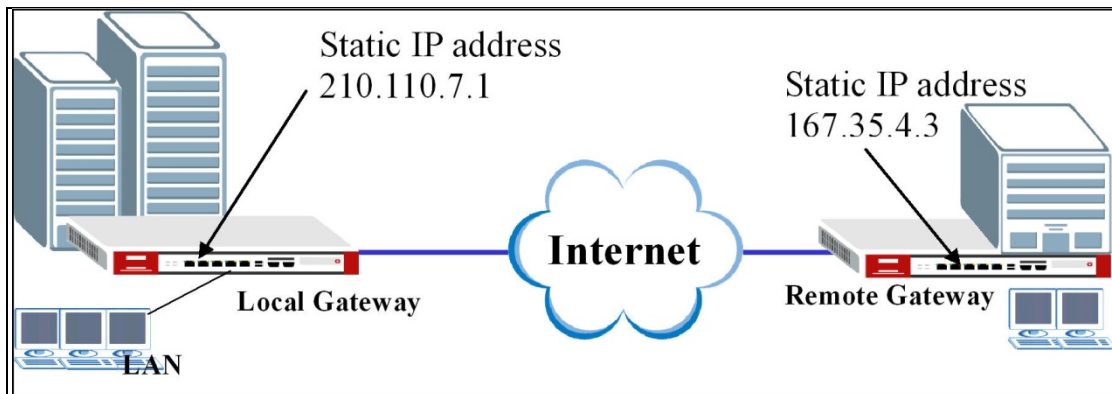


### 1.1.2 Site to Site VPN solutions (ZyWALL 1050 ⇔ ZyWALL USG 2000):

Site to Site VPN is the basic VPN solution between local and remote gateway. This type of VPN connection is used to extend and join local networks of both sites into a single intranet. There are two kinds of connection interface. Static IP and dynamic DNS.

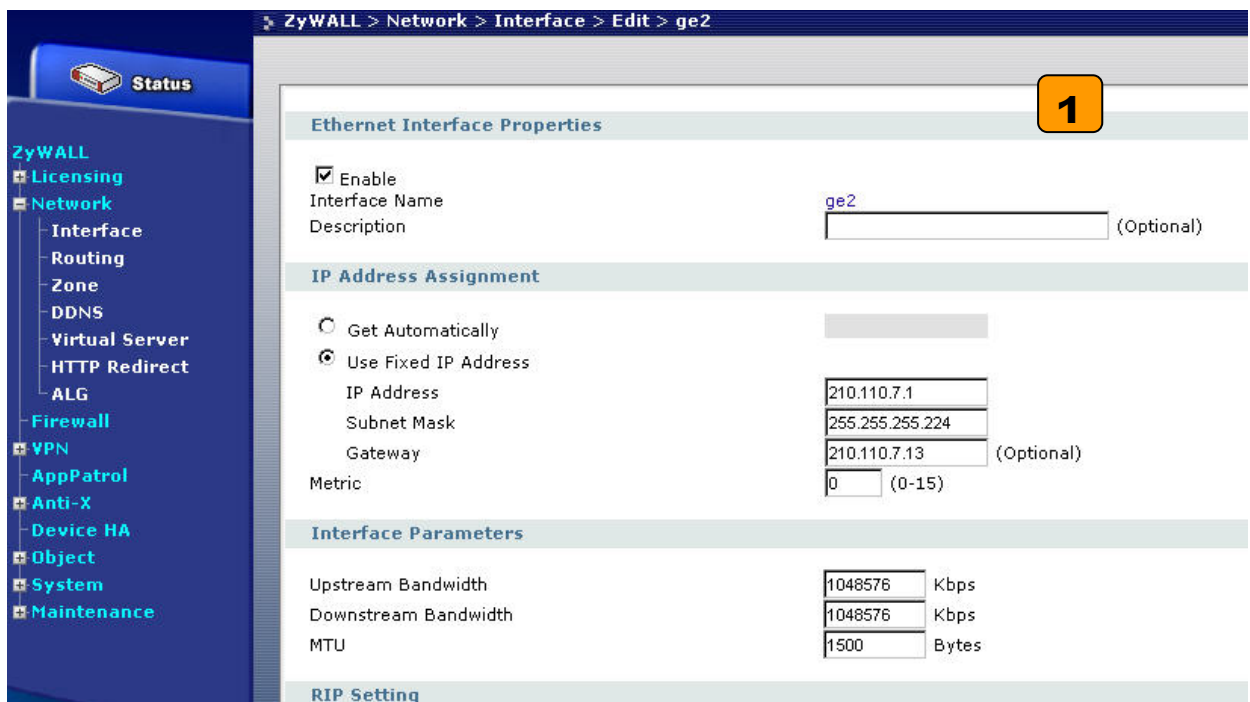
Configure ZyWALL 1050 with Static IP address:

ZyWALL 1050 uses the static IP address for VPN connection. The topology is shown on the following figure.



User needs to configure the static IP address and then apply to the VPN Gateway configuration page. The configuration steps are stated below:

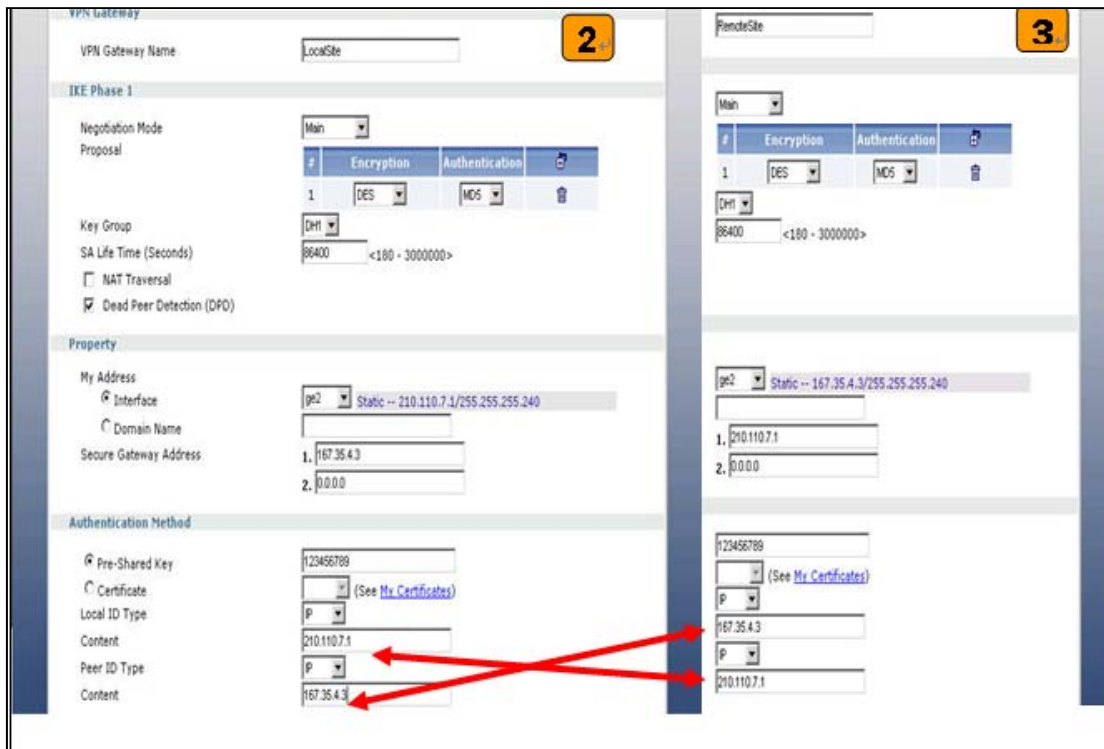
- 1) Login ZyWALL 1050 GUI, setup the ge2 interface for internet connection and manually assign a static IP. The configuration path in ZyWALL 1050 is **Network > Interface > Ethernet > Edit > ge2**



- 2) Switch to **VPN > IPSec VPN > VPN Gateway** select interface ge2 as **My Address** and



then in **Security Gateway Address** field set the remote gateway IP to 167.35.4.3. The **Local ID Type** and content are IP and 210.110.7.1, **Peer ID Type** and content are IP and 167.35.4.3.



- 3) User can refer to the user guide to complete the rest of the settings for VPN tunnel.
- 4) The ZyWALL1050 and ZyWALL USG 2000 VPN are route-based VPN. This means the VPN tunnel can be an interface to route the VPN traffic. Thus, we need to configure a policy route for VPN traffic from the local subnet to the remote subnet after configuring the VPN gateway and connection (phase1 and phase2). The purpose of this policy route is to tell the ZyWALL1050 to send the traffic to VPN tunnel when the traffic flows from the local subnet to a destination that is in the remote subnet. Switch to ZyWALL 1050 > Network > Routing > Policy Route and add a new policy route. The source and the destination addresses are the local and remote subnets. The **Next-Hop** type is VPN tunnel. Then choose the corresponding VPN connection rule from the VPN tunnel drop down menu. Now, the VPN tunnel and routing is configured and user can start to test it.

**ZyWALL > Network > Routing > Policy Route > Edit > #1**

4

---

**Configuration**

☒ Enable

Description:  (Optional)

---

**Criteria**

User:

Incoming:  [Change...](#)

Source Address:

Destination Address:

Schedule:

Service:

---

**Next-Hop**

Type:

VPN Tunnel:

---

**Bandwidth Shaping**

Maximum Bandwidth:  Kbps

Bandwidth Priority:  (1-7, 1 is highest priority)

☐ Maximize Bandwidth Usage

- 5) Login ZyWALL USG 2000 GUI, setup the ge2 interface for internet connection and manually assign a static IP. The configuration path in ZyWALL USG 2000 menu is **ZyWALL > VPN > IPsec VPN > VPN Gateway > Add**. Select Static site to site VPN and then create an object if you have not created any wan interface.

**ZyWALL > VPN > IPsec VPN > VPN Gateway**

VPN Connection | **VPN Gateway** | Concentrator | SA Monitor

---

**Configuration**

Total Connection: undefined  connection per page Page:  of NaN

#	Name	My address	Secure Gateway	VPN Connection	
1					

- 6) Switch to **VPN > IPSec VPN > VPN Gateway > Edit** select interface ge2 as **My Address** and then in **Security Gateway Address** field set the remote gateway IP to 210.110.7.1. The **Local ID Type** and content are IP and 167.35.4.3, **Peer ID Type** and content are IP and 210.110.7.1.

- 7) Create VPN by selecting **ZyWALL > VPN > IPSec VPN > VPN Connection > Edit**. As for more detail, user can refer to the user guide to complete the rest of the settings for VPN tunnel.

The screenshot displays the ZyWALL USG 2000 VPN Configuration interface. The breadcrumb navigation at the top reads: **ZyWALL > VPN > IPSec VPN > VPN Connection > Edit > #1**.

The interface is divided into four main sections:

- General Settings:** Contains a text input field for "Connection Name".
- VPN Gateway:** Contains radio buttons for "Static" (selected) and "Dynamic". Under "Static", there is a dropdown menu showing "IKE\_Gateway" and a text input field below it containing "ge2". Under "Dynamic", there are two radio buttons: "Site-to-site with Dynamic Peer" and "Remote Access", each followed by a dropdown menu.
- Policy:** Contains two dropdown menus for "Local policy" and "Remote policy".
- Phase 2 Settings:** Contains a text input field for "SA Life Time" with the value "86400" and a label "(180 - 3000000 Seconds)".

- 8) The ZyWALL1050 and ZyWALL USG 2000 VPN are route-based VPN. This means the VPN tunnel can be an interface to route the VPN traffic. Thus, we need to configure a policy route for VPN traffic from the local subnet to the remote subnet after configuring the VPN gateway and connection (phase1 and phase2). The purpose of this policy route is to tell the ZyWALL1050 to send the traffic to VPN tunnel when the traffic flows from the local subnet to a destination that is in the remote subnet. Switch to ZyWALL 1050 > Network > Routing > Policy Route and add a new policy route. The source and the destination addresses are the local and remote subnets. The **Next-Hop** type is VPN tunnel. Then choose the corresponding VPN connection rule from the VPN tunnel drop down menu. Now, the VPN tunnel and routing is configured and user can start to test it.

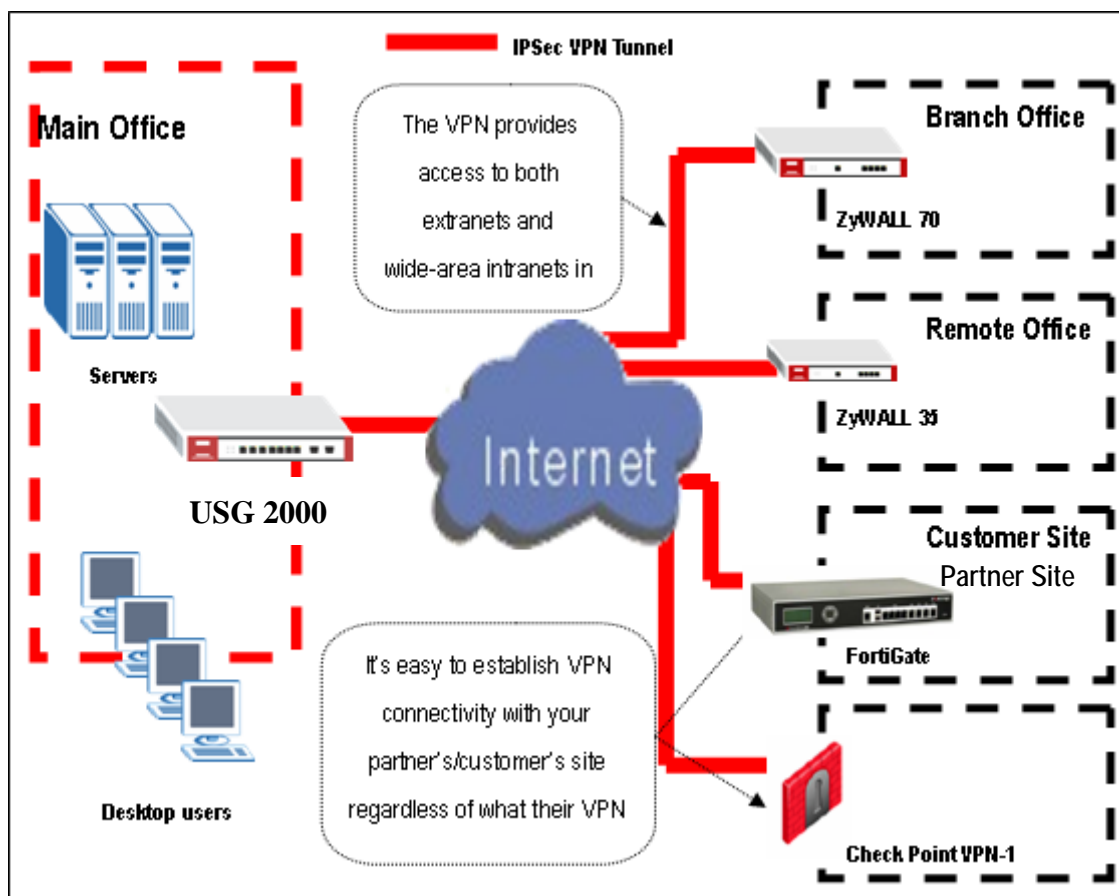
### Tips for application:

1. Make sure the **presharekey** is the same in both local and remote gateways.
2. Make sure the **IKE & IPSec proposal** is the same in both local and remote gateways.

3. Select the correct **interface** for VPN connection.
  4. The **Local** and **Peer** ID type and content must be the opposite and contain the same.
- Make sure the **VPN policy route** has been configured in ZyWALL1050.

## 1.2 Extranet Deployment

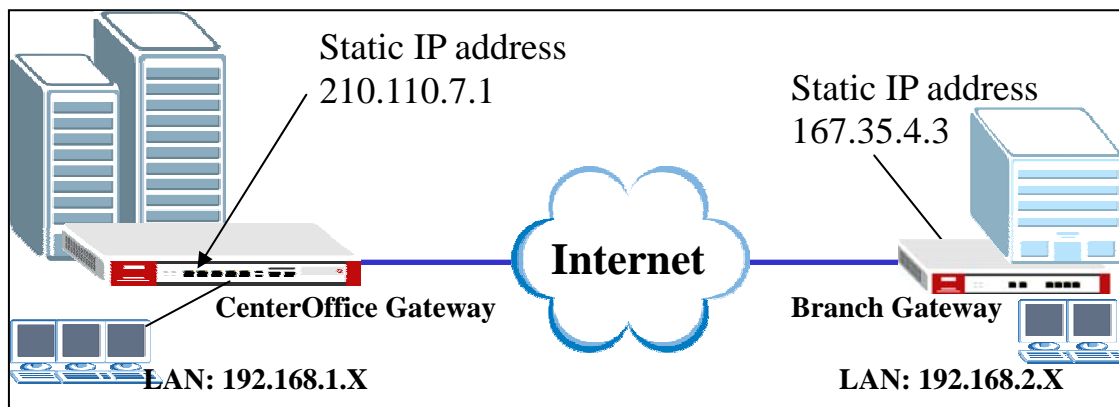
The VPN provides the access to extranets which can provide the security path over internet to improve the client service, vendor support and company communication. Different flexible business models have been developed based on the global VPN extranet architecture. For example, customers can order equipment over the VPN and also suppliers can check the orders electronically. Another result of its application is that the employees across different branches can collaborate on project documents and share the different site's internal resource to complete the project.



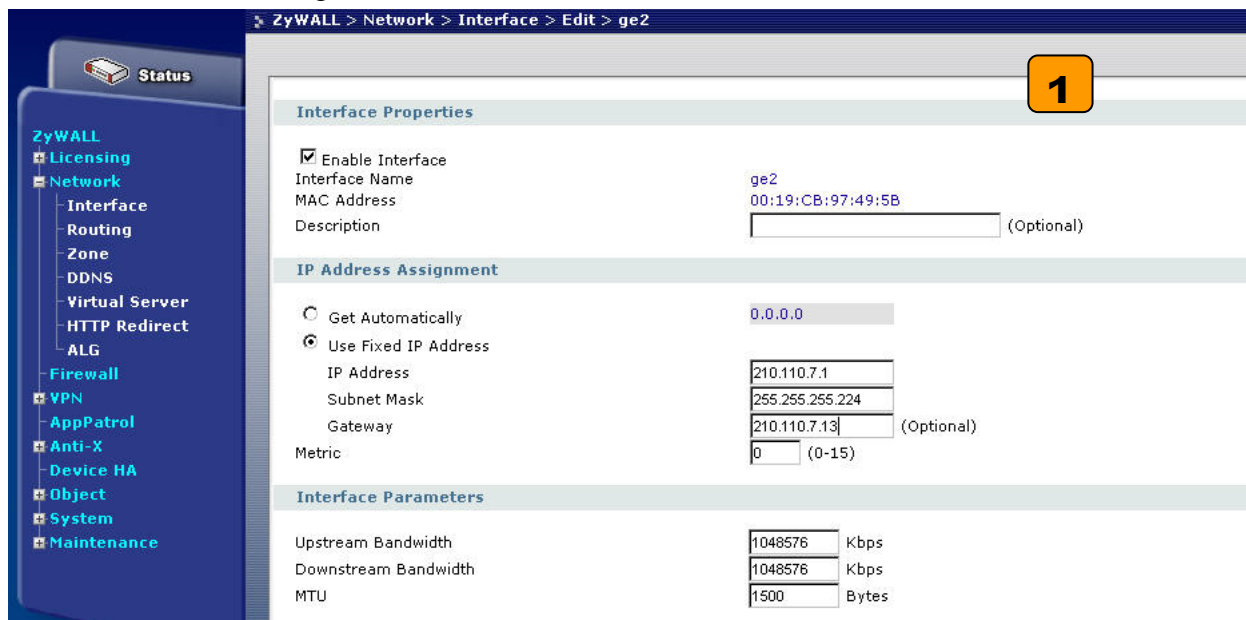
The ZyWALL USG 2000 can be placed as a VPN gateway in the central site. It can communicate with other ZyXEL's VPN-capable products as well as VPN products from other major vendors in the network device industry, e.g. Cisco PIX/IOS VPN products, Check Point VPN Pro, Juniper NetScreen 100/200 and others...

### 1.2.1 Site to site VPN solutions (ZyWALL USG 2000 to ZyWALL70)

The existing ZyWALL35 or 70 in central office gateway can be replaced by ZyWALL USG 2000, and the ZyWALL35 or 70 moved to a remote office. The ZyWALL USG 2000 can provide higher VPN throughput and deal with multiple VPN tunnels at the same time. To show how to build tunnel between ZyWALL5/35/70 and ZyWALL USG 2000 we used ZyWALL 70 as an example.



- 1) Login ZyWALL USG 2000 GUI and setup the ge2 interface for the internet connection and manually assign a static IP. The configuration path is ZyWALL USG 2000 > Network > Interface > Edit > ge2



- 2) Switch to **VPN > IPSec VPN > VPN Gateway**, select **My Address** as interface ge2 and then in **Security Gateway Address** field set the remote gateway IP to 167.35.4.3. The **Local ID Type** and content are IP and 210.110.7.1, **Peer ID Type** and content are IP and

167.35.4.3.

- 3) Login to ZyWALL70 and go to **Security > VPN > Gateway Policy**, add a new gateway policy to connect with central office's ZyWALL USG 2000. **My Address** and **Remote Gateway Address** are ZyWALL70 and ZyWALL USG 2000 WAN IP addresses. The **Pre-Shared Key** configured on both sides must exactly the same **Local ID Type** & content and **Peer ID Type** & content are reverse to the Local ZyWALL USG 2000.
- 4) The **IKE Proposal** is very important setting when configuring the VPN tunnel. The proposal includes Negotiation Mode, Encryption and Authentication Algorithm and.... Make sure the IKE proposal parameters are must the same on both ends.

The screenshot shows the 'VPN - GATEWAY POLICY - EDIT' configuration page. Key sections include:

- IKE Phase I:** Negotiation Mode (Main), Encryption (DES), Authentication (MD5), Key Group (DH1), SA Life Time (96400).
- Property:** My Address (167.35.4.3), My Domain Name (chindirection.selp.net), Remote Gateway Address (210.110.7.1).
- Authentication Key:** Pre-Shared Key (123456789), Local ID Type (P), Content (210.110.7.1), Peer ID Type (P), Content (167.35.4.3).
- Extended Authentication:** Enable Extended Authentication (Client Mode), User Name, Password.

- 5) Switch to **Network > IPSec VPN > VPN Connection**, add a new **VPN connection** (IPSec phase2). Setup the Phase2 proposal and local and remote policies. The chosen phase2 proposal chosen must be the same as on the remote site's ZyWALL70.



- 6) In ZyWALL70, VPN is a rule based VPN. This means that whether the traffic is going to the tunnel or not will depend on the local and remote policies. In this example, ZyWALL70 **local and remote policies** are 192.168.2.0 and 192.168.1.0 and the traffic from 192.168.2.X subnet to 192.168.1.X subnet will go through the VPN tunnel to the remote site as predefined. The ZyWALL USG 2000 local and remote policies must be reverse to the ZyWALL70's settings, otherwise the tunnel will not be built up.
- 7) Check whether the **IPSec proposal** on both sites is the same and the configuration is done on both sites.

The screenshot displays the ZyWALL USG 2000 VPN configuration interface. The main configuration area is divided into several sections:

- VPN Connection:** Shows the Connection Name as 'RemoteTunnel' (labeled 5).
- VPN Gateway:** Shows the Name as 'LocalSite' and the Gateway as 'ge2'.
- Phase 2:** Shows the Active Protocol as 'ESP', Encapsulation as 'Tunnel', and Proposal as '1'. The Encryption is 'DES' and Authentication is 'SHA1'. The SA Life Time (Seconds) is '86400'.
- Policy:** Shows Policy Enforcement checked. Local policy is 'LAN\_SUBNET' and Remote policy is 'Remote\_Subnet'. The Local policy is 'SUBNET, 192.168.1.0/24' and the Remote policy is 'SUBNET, 192.168.2.0/24'.
- Property:** Shows the 'Active' checkbox checked (labeled 6). The Name is 'RemoteTunnel'.
- IPSec Proposal:** A detailed view of the proposal configuration (labeled 7) showing Encapsulation Mode as 'Tunnel', Active Protocol as 'ESP', Encryption Algorithm as 'DES', Authentication Algorithm as 'SHA1', SA Life Time (Seconds) as '28800', and Perfect Forward Secrecy (PFS) as 'NONE'.
- Gateway Policy Information:** Shows the Gateway Policy as 'BranchOffice'.
- Local Network:** Shows the Address Type as 'Subnet Address', Starting IP Address as '192.168.2.0', Ending IP Address / Subnet Mask as '255.255.255.0', and Local Port as '0'.
- Remote Network:** Shows the Address Type as 'Subnet Address', Starting IP Address as '192.168.1.0', Ending IP Address / Subnet Mask as '255.255.255.0', and Remote Port as '0'.

Red arrows indicate the flow of configuration: from the Connection Name (5) to the IPSec Proposal (7), from the Policy tab to the Local and Remote Network settings, and from the Property tab (6) to the IPSec Proposal (7).

- 8) The ZyWALL USG 2000 VPN is a route-based VPN, this means the VPN tunnel can be an interface to route the VPN traffic. Thus, we need to configure a policy route for VPN traffic from the local subnet to the remote subnet after configuring the VPN gateway and

the connection (phase1 and phase2). The purpose for this policy route is to tell the ZyWALL USG 2000 to send the traffic to the VPN tunnel when the traffic goes from the local subnet to the destination that is in a remote subnet. Switch to **Network > Routing > Policy > Policy Route** and add a new policy route, the source and destination address are the local and remote subnet and the **Next-Hop** type is a VPN tunnel. Then choose the corresponding VPN connection rule from the VPN tunnel drop down menu. Now, the VPN tunnel and routing is built and user can start to test it.

**ZyWALL > Network > Routing > Policy Route > Edit > #3**

**8**

**Configuration**

☒ Enable  
 Description: VPN\_route (Optional)

**Criteria**

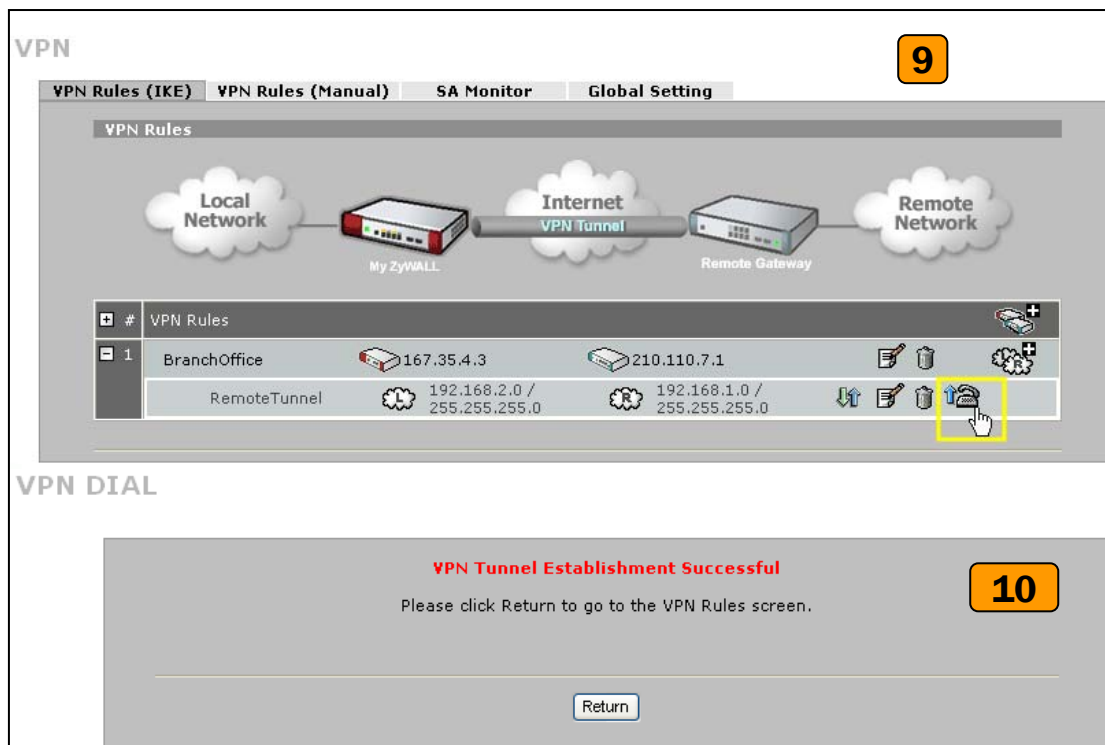
User: any  
 Incoming: Interface / any Change...  
 Source Address: LAN\_SUBNET  
 Destination Address: Remote\_Subne  
 Schedule: none  
 Service: any

**Next-Hop**

Type: VPN Tunnel  
 VPN Tunnel: RemoteTunnel  
☐ Auto Destination Address

9) After configuring both sides of the VPN, click the “Dial up” icon to test the VPN connectivity.

10) “VPN tunnel establishment successful,” message appears.



### Tips for application:

1. Make sure the **presharekey** is the same in both the local and the remote gateways.
2. Make sure the **IKE & IPSec proposal** is the same in both the local and the remote gateways.
3. Select the correct **interface** for the VPN connection.
4. The **Local** and **Peer** ID type and content must be the opposite and not of the same content.
5. Make sure the **VPN policy route** had been setup in ZyWALL USG 2000.

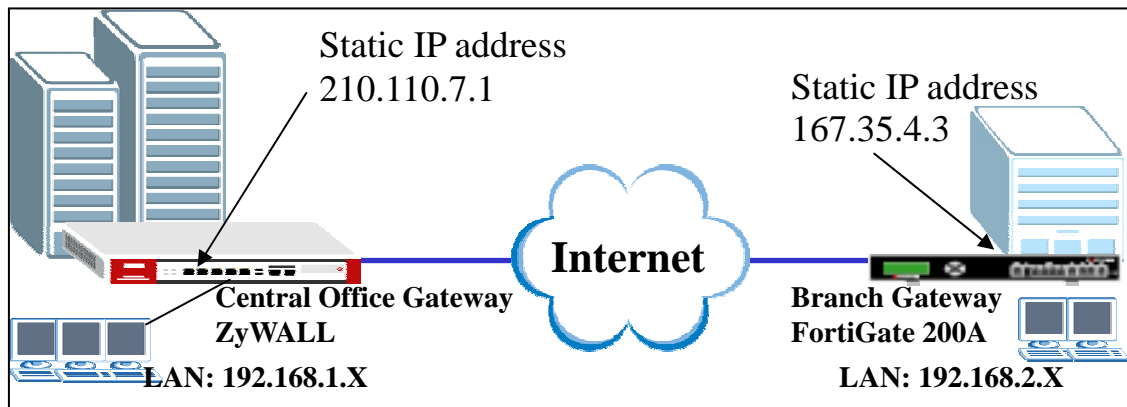
## 1.2.2 Interoperability – VPN with other vendors

### 1.2.2.1 ZyWALL with FortiGate VPN Tunneling

This page guides how to setup a VPN connection between the ZyWALL USG 2000 and FortiGate 200A.

As on the figure shown below, the tunnel between Central and Remote offices ensures the packet flow between them are secure, because the packets go through the IPSec tunnel are

encrypted. To setup this VPN tunnel, the required settings for ZyWALL and FortiGate are explained in the following sections.



The central office gateway ZyWALL USG 2000's interface and VPN setting retain the same setting as in the previous example. If you jumped this section first, please refer to 'ZyWALL USG 2000 to ZYWALL70 VPN tunnel setting' on page 8.

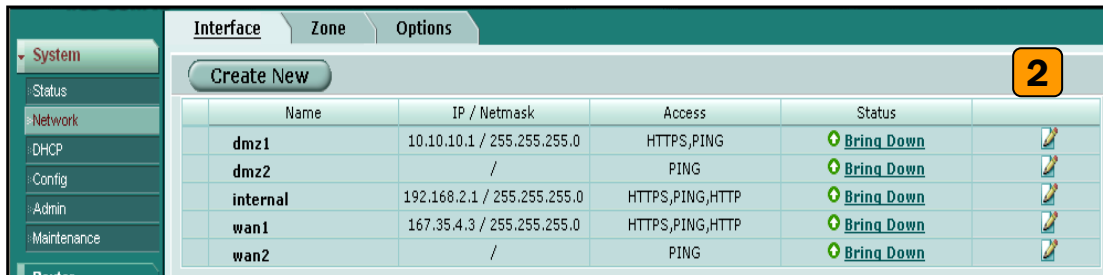
This list below is to briefly show the VPN phase1 and phase2 configuration parameters:

ZyWALL	FortiGate
WAN: 210.110.7.1 LAN: 192.168.1.0/24	WAN: 167.35.4.3 LAN: 192.168.2.0/24
Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1	Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1
Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None	Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None

- 1) Configure the ZyWALL USG 2000 's VPN gateway and VPN connection as on the list. Also, remember to configure the policy route for the VPN traffic routing. Refer to the

previous scenario or user guide to find help on setting the ZyWALL USG 2000 VPN.

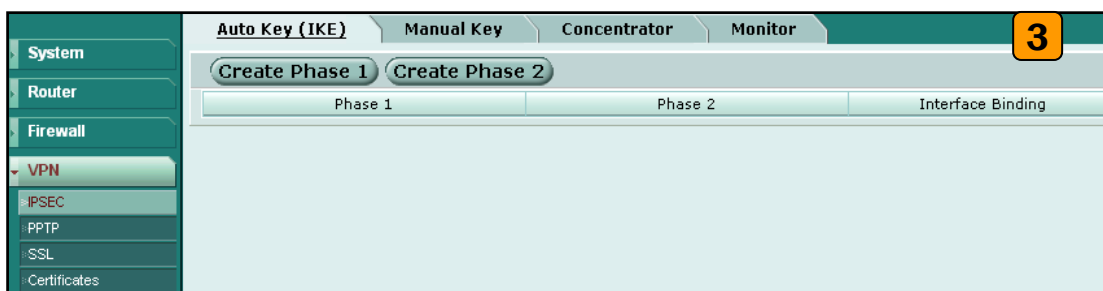
- 2) Login to the FortiGate GUI and switch to System > Network > Interface and set the wan1 interface to 167.35.4.3 and internal interface to 192.168.2.1/255.255.255.0.



Interface				
Name	IP / Netmask	Access	Status	
dmz1	10.10.10.1 / 255.255.255.0	HTTPS,PING	Bring Down	
dmz2	/	PING	Bring Down	
internal	192.168.2.1 / 255.255.255.0	HTTPS,PING,HTTP	Bring Down	
wan1	167.35.4.3 / 255.255.255.0	HTTPS,PING,HTTP	Bring Down	
wan2	/	PING	Bring Down	

Note: About the detail interface settings, refer to FortiGate user guide.

- 3) Switch to System > VPN > IPSEC and select the **Auto Key** (IKE) tab and click the **Create Phase 1** button. This will open a new page for VPN phase1 setup.



Auto Key (IKE)		
Phase 1	Phase 2	Interface Binding
<div> <div>Create Phase 1</div> <div>Create Phase 2</div> </div>		

- 4) Fill-in the VPN phase1 setting according to the table listed. We don't have to setup the ID type and content because the FortiGate accepts any peer ID. Make sure both the pre-shares key and proposal are the same as in the ZyWALL USG 2000.

- 5) Get back to the VPN configuration page again and click the **Create Phase 2** button to add a new Phase2 policy.

- 6) Select the “ZyWALL”(configured in the step 4) policy from the Phase 1 drop down menu and click the **Advanced...** button to edit the phase 2 proposal and source and destination address. Please make sure the phase 2 proposal is the same as in ZyWALL USG 2000 phase 2.

- 7) The VPN tunnel configuration is finished and the VPN IPsec page will show the VPN phase 1 and phase 2 rules in the Auto Key (IKE) tab.

- 8) We need to setup the firewall rules for IPsec VPN traffic transmitting from ZyWALL to FortiGate and from FortiGate to ZyWALL. Switch to Firewall > VPN > Address menu and add two new address object which stand for ZyWALL LAN subnet and FortiGate LAN subnet. Using the “Create New” button to create a new address object.

- 9) Switch to Firewall > Policy and click “Insert Policy Before” icon to add new policy for the VPN traffic from FortiGate to ZyWALL.

- 10) We will setup the FortiGate to ZyWALL policy in the new page. The source interface is **internal** and Address name is Fortinet (192.168.2.0/255.255.255.0 address object). The destination interface is **wan1** and Address name is Zynet (192.168.1.0/255.255.255.0 address object). Schedule and service type are “always” and “ANY” to ensure that all kinds of traffic can pass through the VPN tunnel at any time. There are three kinds of “Action” available for user to configure, because the traffic is send from “internal” to WAN and will be encrypted by IPsec VPN tunnel. Thus, we select “IPSEC” as action and chose allow inbound and outbound traffic in the ZyWALL tunnel.

- 11) Switch to **Firewall > Policy** and click “Create New” button to add new policy for the VPN traffic from ZyWALL to FortiGate.

- 12) We setup the ZyWALL to FortiGate policy in the new page. The source interface is **wan1** and Address name is Zynet (192.168.1.0/255.255.255.0 address object). The destination interface is **internal** and the Address name is Fortinet (192.168.2.0/255.255.255.0 address object). Schedule and service type are always and ANY to ensure that all kinds of traffic



can pass through the VPN tunnel at any time. Select “ACCEPT” as an action this time because the traffic sent from wan to internal must be decrypted first and only then can be transmitted. Don’t select the IPSec as the **Action** in this VPN traffic flow direction.

**Policy**

**New Policy**

Source Interface/Zone: wan1  
Address Name: Zynet

Destination Interface/Zone: internal  
Address Name: Fortinet  
Schedule: always  
Service: ANY  
Action: ACCEPT

☐ NAT ☐ Dynamic IP Pool  
☐ Fixed Port

☐ Protection Profile: unfiltered  
☐ Log Allowed Traffic  
☐ Authentication: Firewall  
☐ Traffic Shaping

Comments (maximum 63 characters)

OK Cancel

13) The overall firewall policy is shown on the following figure. The VPN tunnel between ZyWALL and FortiGate has been successfully setup.

**Policy**

Create New

ID	Source	Dest	Schedule	Service	Action	Enable
▼ internal -> wan1 (2)						
2	Fortinet	Zynet	always	ANY	ENCRYPT	<input checked="" type="checkbox"/>
1	all	all	always	ANY	ACCEPT	<input checked="" type="checkbox"/>
▼ wan1 -> internal (1)						
3	Zynet	Fortinet	always	ANY	ACCEPT	<input checked="" type="checkbox"/>

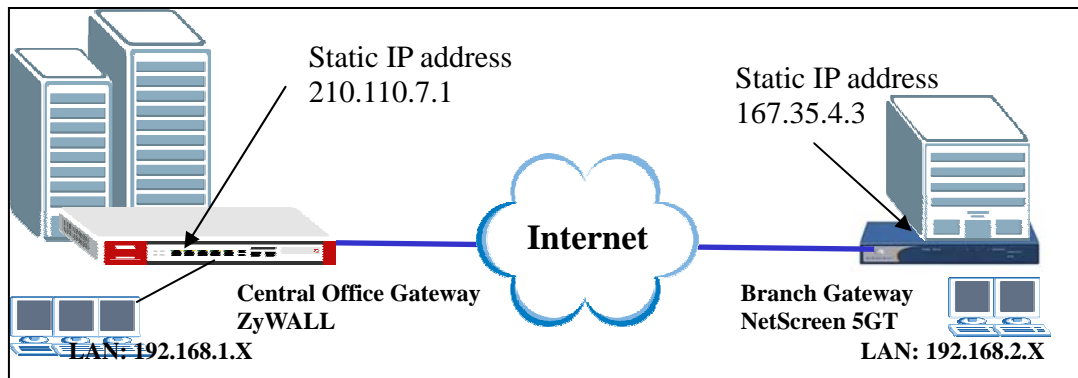
### Tips for application:

1. Make sure the **Pre-Shared Key** is the same in both local and remote gateways.
2. Make sure both **IKE** and **IPSec proposal** are the same in both local and remote gateways.
3. Make sure the **VPN policy route** has been configured in ZyWALL USG 2000.
4. Make sure the **Firewall rule** has been configured in FortiGate.

### 1.2.2.2 ZyWALL with NetScreen VPN Tunneling

This section guides how to setup a VPN connection between the ZyWALL USG 2000 and NetScreen 5GT.

As on the figure below, the tunnel between Central and Remote offices ensures the packet flows between them are secure. This is because the packets flowing through the IPSec tunnel are encrypted. The required settings to setup this VPN tunnel using ZyWALL and NetScreen are stated in the following section.



The central office gateway ZyWALL USG 2000's interface and VPN setting retain the same settings as in the previous example. If you jumped to this section first, please refer to 'ZyWALL USG 2000 to ZYWALL70 VPN tunnel setting' on the page 8.

This list below is to briefly show the VPN phase1 and phase2 configuration parameters:

ZyWALL	NetScreen
WAN: 210.110.7.1 LAN: 192.168.1.0/24	WAN: 167.35.4.3 LAN: 192.168.2.0/24
Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1	Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1

<p>Phase2</p> <p>Encapsulation: Tunnel</p> <p>Active Protocol: ESP</p> <p>Encryption: DES</p> <p>Authentication: SHA1</p> <p>Perfect Forward Secrecy (PFS): None</p>	<p>Phase2</p> <p>Encapsulation: Tunnel</p> <p>Active Protocol: ESP</p> <p>Encryption: DES</p> <p>Authentication: SHA1</p> <p>Perfect Forward Secrecy (PFS): None</p>
--	--

- 1) Configure the ZyWALL USG 2000 's VPN gateway and VPN connection as on the list. Also, remember to configure the policy route for the VPN traffic routing. Refer to the pervious scenario or user guide to find help on setting the ZyWALL USG 2000 VPN.
- 2) Using a web browser, login NetScreen by entering the LAN IP address of the NetScreen in the URL field. The default username and password is netscreen/netscreen.
- 3) Switch to menu **Network > Interfaces** and configure the WAN/LAN IP addresses to WAN: 167.35.4.3 / LAN: 192.168.2.0/24. The **trust interface** is for **LAN**, the **untrust interface** is for **WAN**.

Network > Routing > Routing Entries

List 20 per page

List route entries for All virtual routers

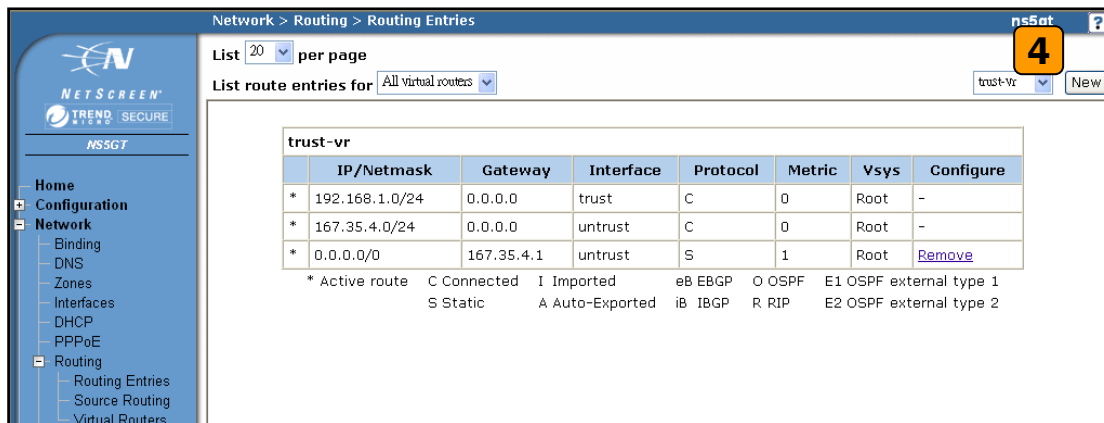
trust-vr

	IP/Netmask	Gateway	Interface	Protocol	Metric	Vsys	Configure
*	0.0.0.0/0	167.35.4.1	untrust	S	1	Root	<a href="#">Remove</a>
*	167.35.4.0/24	0.0.0.0	untrust	C	0	Root	-
*	192.168.2.0/24	0.0.0.0	trust	C	0	Root	-

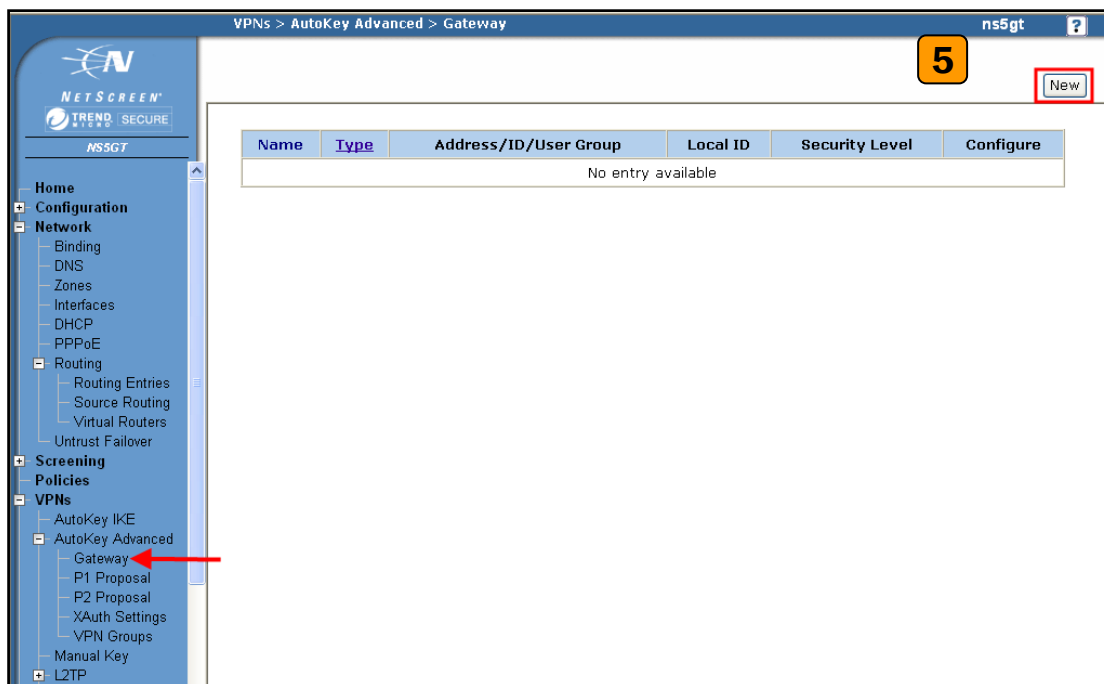
\* Active route C Connected I Imported eB EBGP O OSPF E1 OSPF external type 1  
S Static A Auto-Exported iB IBGP R RIP E2 OSPF external type 2

Note: Regarding the detail interface settings, please refer to NetScreen user guide to get the detail info.

- 4) NetScreen won't setup a route for the traffic to the external network. We have to manually add a route for it. After configuring a static IP address in untrust interface, switch to Network -> Routing -> Routing Entries to edit a default Gateway IP address. In this example, the Gateway IP address is 167.35.4.1.



- 5) To edit the IPSec rule, first set the gateway policy and then edit the IKE policy. Switch to **VPNs > AutoKey Advanced > Gateway**, and then press the **New** button.



- 6) Choose a name for the policy, for example **"ToZyWALL"**. **Remote Gateway IP Addr** is the **ZyWALL's WAN IP address**. In this example, we select **Static IP Address** option and enter IP **210.110.7.1** in the text box. Enter the key string **123456789** in **Preshared Key** text box, and then press **Advanced** button to edit the advanced settings.

6

Gateway Name

Security Level ☐ Standard ☐ Compatible ☐ Basic ☒ Custom

---

**Remote Gateway Type**

☒ Static IP Address IP Address/Hostname

☐ Dynamic IP Address Peer ID

☐ Dialup User User

☐ Dialup User Group Group

---

Preshared Key  Use As Seed ☐

Local ID  (optional)

Outgoing Interface

---

- 7) On Security Level settings, we can set up phase 1 proposal. In this example, we select User Defined, and choose pre-g1-des-md5 rule. The pre-g1-des-md5 means **Pre-Share Key, group1, DES for Encryption Algorithm and MD5 for Authentication Algorithm**. Select Main (ID Protection) option for Mode (Initiator). Then, press Return button, and press OK button on next page to save your settings.

7

**Security Level**

Predefined ☐ Standard ☐ Compatible ☐ Basic

User Defined ☒ Custom

**Phase 1 Proposal**

---

**Mode (Initiator)** ☒ Main (ID Protection) ☐ Aggressive

---

☐ Enable NAT-Traversal

UDP Checksum ☐

Keepalive Frequency  Seconds (0~300 Sec)

---

**Heartbeat**

Hello  Seconds (0~3600 Sec)

Reconnect  Seconds (60~9999 Sec)

Threshold

---

☒ None  
☐ XAuth Server  
☒ Use Default  
☐ Local Authentication

- 8) After applying the previous settings, the new IKE rule is shown on the page.

Name	Type	Address/ID/User Group	Local ID	Security Level	Configure
ToZyWALL	Static	210.110.7.1	-	Custom	<a href="#">Edit</a> <a href="#">Remove</a>

- 9) To edit the IPSec rule, switch to **VPNs > AutoKey IKE**, and then press the **New** button to edit your IPSec rules.

- 10) Give a name for the VPN, for example **“ToZyWALL IPSec”**. In Remote Gateway, choose the Predefined option and select the ToZyWALL rule. Then, press **Advanced** button to edit the advanced settings.

- 11) In **Security Level** settings, choose the option **User Defined** and choose **nopfs-esp-des-sha** rule on **Phase 2 Proposal**. The **nopfs-esp-des-sha** means no PFS, **ESP Protocol, Encryption Algorithm** to **DES** and **Authentication Algorithm** to **SHA1**. Check the **VPN Monitor** check box so that you can monitor your VPN tunnels. Then, press Return button and OK button on next page to save the settings.

**Security Level**

Predefined ☐ Standard ☐ Compatible ☐ Basic

User Defined ☒ Custom

**Phase 2 Proposal**

nopfs-esp-des-sha / None

None / None

**11**

---

Replay Protection ☐

Transport Mode ☐ (For L2TP-over-IPSec only)

---

Bind to ☒ None ☐ Tunnel Interface ☐ Tunnel Zone

none / Untrust-Tun

---

Proxy-ID ☒

Local IP / Netmask 192.168.2.0 / 24

Remote IP / Netmask 192.168.1.0 / 24

Service ANY

---

VPN Group None Weight 0

---

VPN Monitor ☒

Source Interface default

Destination IP 0.0.0.0

Optimized ☐

Rekey ☐

---

Return Cancel

- 12) After applying the settings, the VPN IKE page will show the new IPSec rule.

Name	Gateway	Security	Monitor	Configure	
ToZyWALL IPSec	ToZyWALL	Custom	On	<a href="#">Edit</a>	-

**12**

- 13) Switch to **Policies** to set up policy rules for VPN traffic. In the field **From** choose **Trust** and in the field **To** choose **Untrust** (it means from LAN to WAN). Then press the **New** button to edit the policy rules.

Policies (From Trust To Untrust)

ns5gt 13

List 20 per page

From Trust To Untrust Go

New

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
1	Any	Any	ANY	✓		Edit Clone Remove	✓	↕ ➡

14) Assign a name to this policy, for example “VPN”. In **Source Address**, set the Local LAN IP addresses. In this example, we select **New Address** option. Type **192.168.2.0 / 255.255.255.0** in the text box. Set the remote IP addresses as **Destination Address**. In this example, we select **New Address** option, and type **192.168.1.0 / 255.255.255.0** in the text box. In drop down menu **Action** select the option **Tunnel** and then select the **ToZyWALLIPSec** VPN rule. Check **Modify matching bidirectional VPN policy** check box, so that you can create/modify the VPN policy for the opposite direction. Then, press **OK** button to save your settings.

Name (optional) VPN

Source Address

Destination Address

Service ANY

Application None

Action Tunnel

Antivirus Objects

Tunnel VPN ToZyWALL IPSec

Modify matching bidirectional VPN policy

L2TP None

Logging

OK Cancel Advanced



15) After applying the settings, the new policy rules will be displayed in the **Policies** page.

Policies (From All zones To All zones) ns5gt

List 20 per page

From All zones To All zones Go

15

Search New

From Trust To Untrust, total policy: 2

ID	Source	Destination	Service	Action	Options	Configure	Enable
1	Any	Any	ANY	✓		Edit Clone Remove	✓
3	192.168.2.0/255.255.255.0	192.168.1.0/255.255.255.0	ANY	⬅➡	📋	Edit Clone Remove	✓

From Untrust To Trust, total policy: 2

ID	Source	Destination	Service	Action	Options	Configure	Enable
2	Any	Any	ANY	✓		Edit Clone Remove	✓
4	192.168.1.0/255.255.255.0	192.168.2.0/255.255.255.0	ANY	⬅➡	📋	Edit Clone Remove	✓

16) Move the added policy rules to the top, so that the VPN policies will be checked first.

Policies (From All zones To All zones) ns5gt

List 20 per page

From All zones To All zones Go

16

Search New

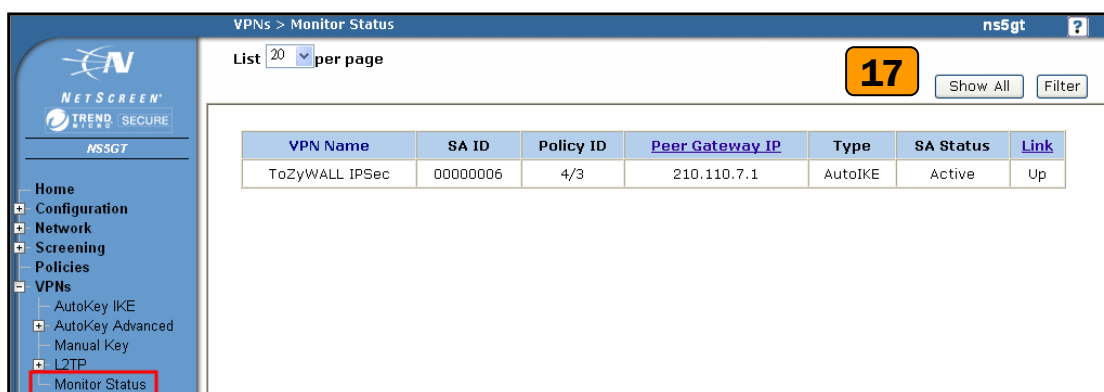
From Trust To Untrust, total policy: 2

ID	Source	Destination	Service	Action	Options	Configure	Enable
3	192.168.2.0/255.255.255.0	192.168.1.0/255.255.255.0	ANY	⬅➡	📋	Edit Clone Remove	✓
1	Any	Any	ANY	✓		Edit Clone Remove	✓

From Untrust To Trust, total policy: 2

ID	Source	Destination	Service	Action	Options	Configure	Enable
4	192.168.1.0/255.255.255.0	192.168.2.0/255.255.255.0	ANY	⬅➡	📋	Edit Clone Remove	✓
2	Any	Any	ANY	✓		Edit Clone Remove	✓

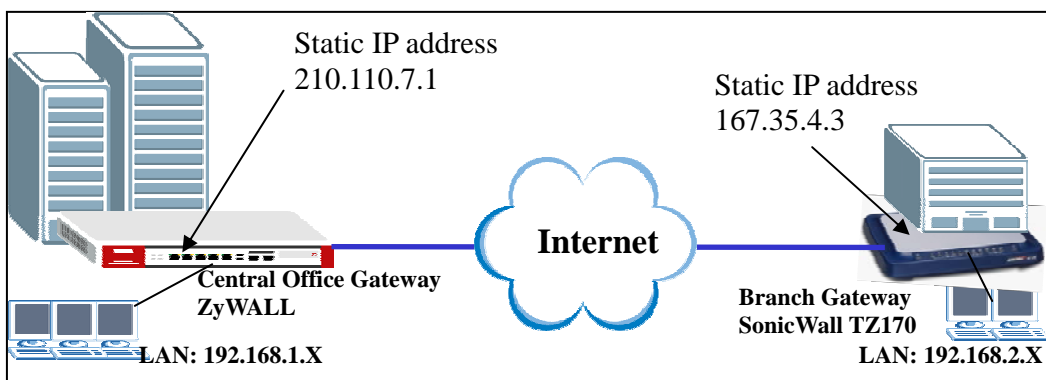
17) Ping the remote host and switch to VPNs > Monitor Status to check the VPN link status. If the **Link** status is Up, it means the VPN tunnel between ZyWALL and NetScreen has been successfully built.



### 1.2.2.3 ZyWALL with SonicWall VPN Tunneling

This section guides how to setup a VPN connection between the ZyWALL USG 2000 and SonicWall TZ170.

As on the figure below, the tunnel between Central and Remote offices ensures the packet flows between them are secure. This is because the packets flowing through the IPSec tunnel are encrypted. The required settings to setup this VPN tunnel using ZyWALL and SonicWall are stated in the following sections.

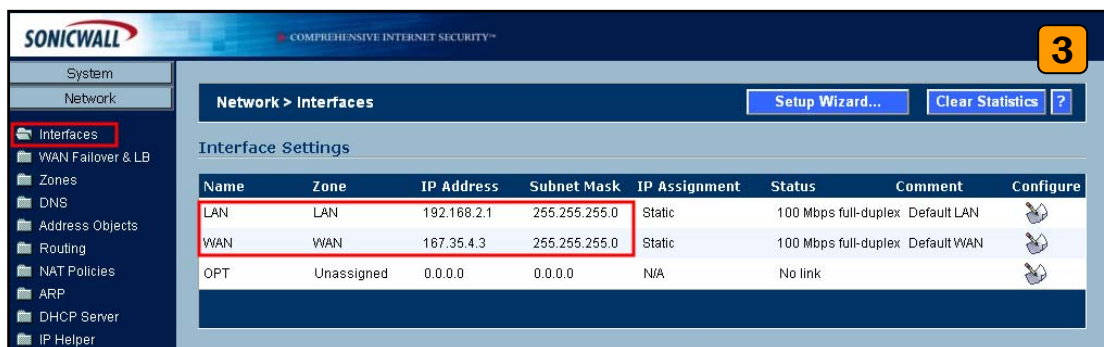


The central office gateway ZyWALL USG 2000's interface and VPN setting retain the same settings as in the previous example. If you jumped to this section first, please refer to 'ZyWALL USG 2000 to ZYWALL70 VPN tunnel setting' on the page 8.

This list below is to briefly show the VPN phase1 and phase2 configuration parameters:

ZyWALL	SonicWall
WAN: 210.110.7.1 LAN: 192.168.1.0/24	WAN: 167.35.4.3 LAN: 192.168.2.0/24
Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1	Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1
Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None	Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None

- 1) Configure the ZyWALL USG 2000 's VPN gateway and VPN connection as on the list. Also, remember to configure the policy route for the VPN traffic routing. Refer to the previous scenario or user guide to find help on setting the ZyWALL USG 2000 VPN.
- 2) Using a web browser, login SonicWall by entering the LAN IP address of SonicWall in the URL field. The default username and password is admin/password.
- 3) Switch to menu **Network > Interfaces** and configure the WAN/LAN IP address to WAN: 167.35.4.3 LAN: 192.168.2.1/24.



- 4) Switch to VPN > Settings, check **Enable VPN** check box and press **Add** button. This will bring the VPN settings.

Note: The **VPN Policy Wizard** is an alternative way to set up the VPN rules.

**VPN > Settings** VPN Policy Wizard... Apply Cancel ?

**VPN Global Settings**

☒ **Enable VPN**

Unique Firewall Identifier: 0006B10418D8

**VPN Policies** Items 1 to 2 (of 2)

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	
2	WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	

Add... Delete Delete All

Site To Site Policies: 0 Policies Defined, 0 Policies Enabled, 2 Maximum Policies Allowed  
GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 6 Maximum Policies Allowed

- 5) Click the tab **General**, to bring the Security Policy settings and assign a name to this policy. In this example, we use **ToZyWALL**. **IPSec Primary Gateway Name or Address** is the **ZyWALL's WAN IP Address** (IP address of the remote gateway). In this example, we use 210.110.7.1 in **IPSec Primary Gateway Name or Address** text box. Then, enter the key string **123456789** in the text box **Shared Secret**.

**General** **Network** **Proposals** **Advanced**

**Security Policy**

IPSec Keying Mode: IKE using Preshared Secret

Name: ToZyWALL

IPSec Primary Gateway Name or Address: 210.110.7.1

IPSec Secondary Gateway Name or Address:

Shared Secret: 123456789

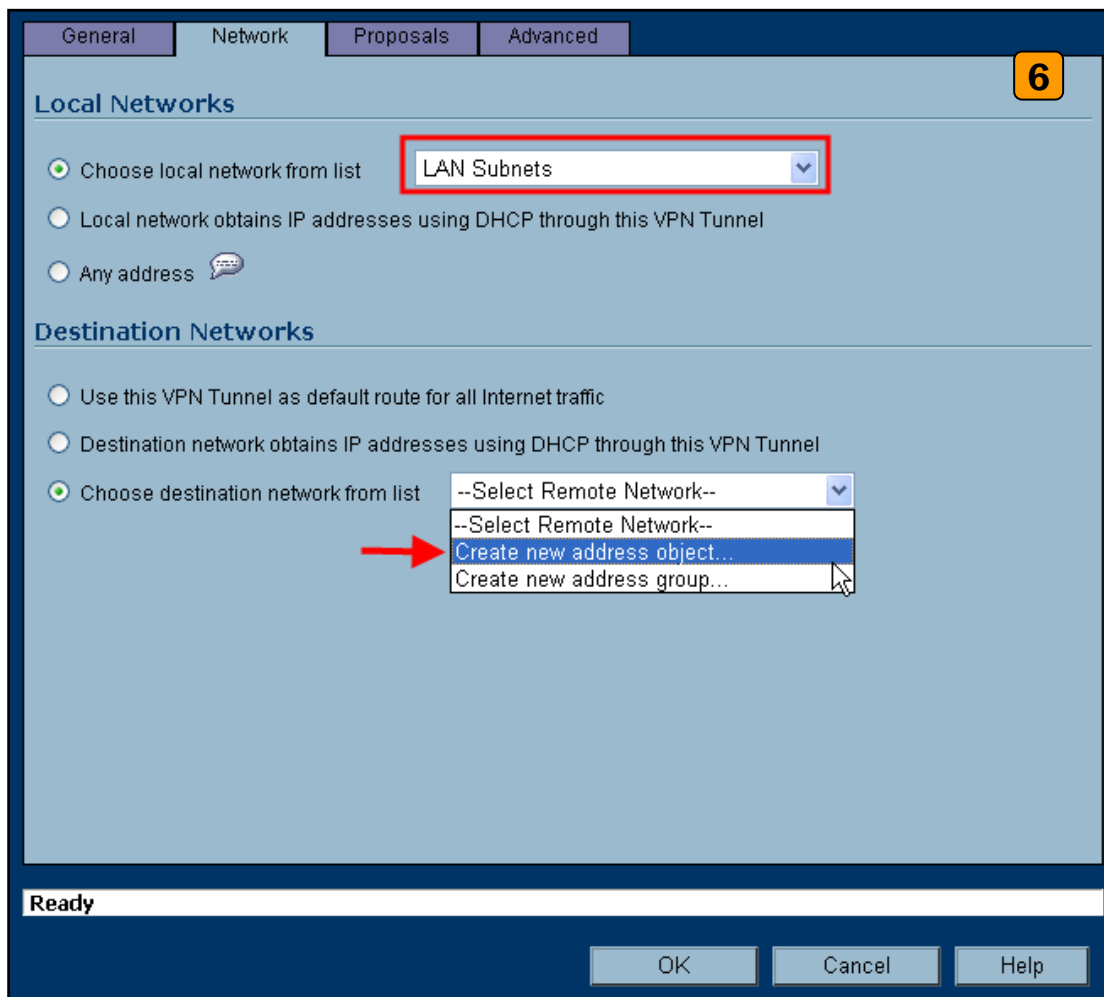
Local IKE ID (optional): IP Address

Peer IKE ID (optional): IP Address

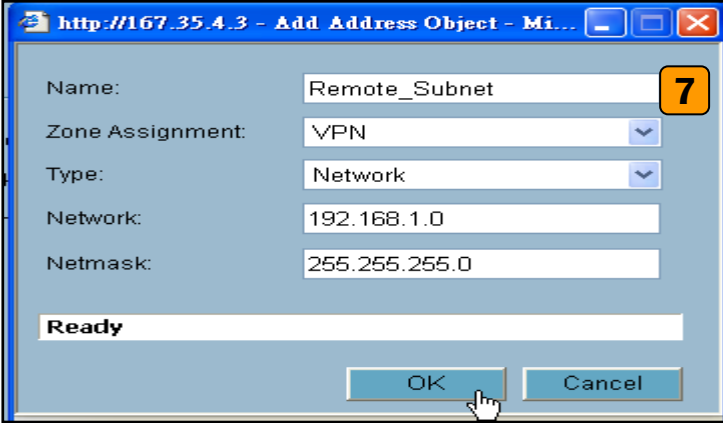
**Ready**

OK Cancel Help

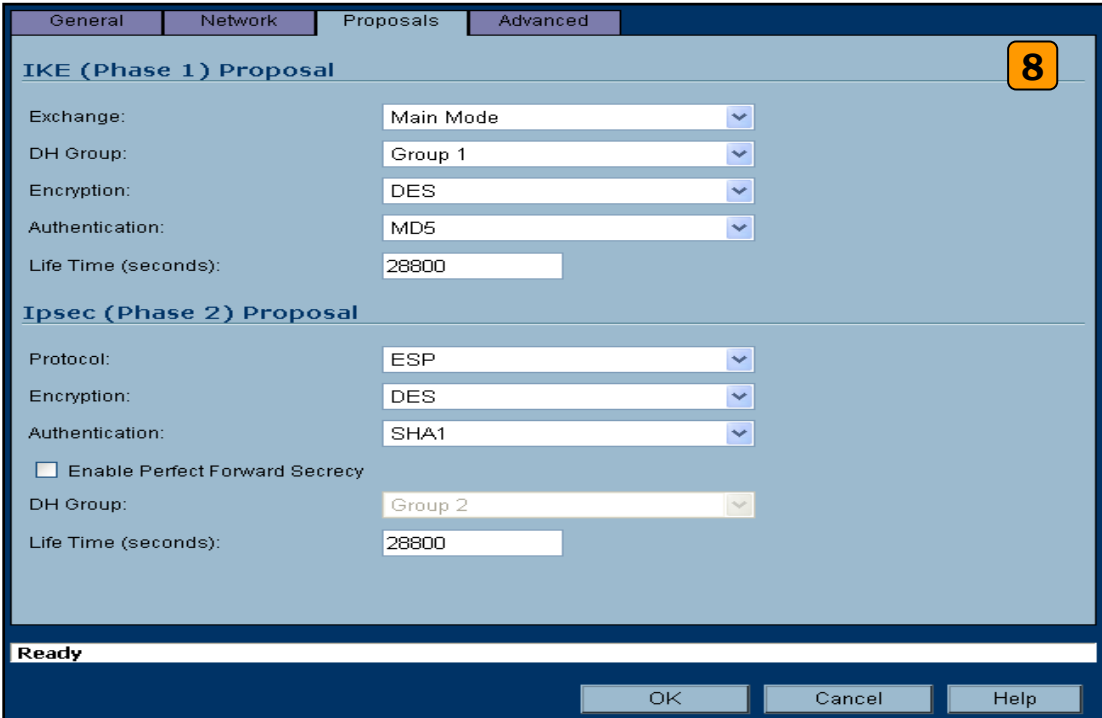
- 6) Switch to **Network** tab to configure the local and remote networks for VPN tunnel. We choose the predefined “LAN Subnets” object from the local network drop down list. There is no predefined address object for remote subnet. Therefore, we have to create a new address object in the remote network drop down list. Then a new address object window will pop-up.



- 7) The name for this object can be for example “Remote\_Subnet”. The **Network IP Address** and the **Subnet Mask** are the remote site LAN subnet. In this example, enter 192.168.1.0 in **Network** text box and then type 255.255.255.0 in **Subnet Mask** text box. Then press **OK**. Now after the address object successfully configured, the new address object “Remote\_Subnet” can be selected from the destination network drop down list.



- 8) Switch to **Proposals** tab. In IKE (Phase1) proposal settings, select **Main mode**, set **DH Group** to **Group1**, **Encryption** to **DES** and **Authentication** to **MD5**. In IPSec (Phase2) proposal settings, select **ESP Protocol**, **Encryption** to **DES** and **Authentication** to **SHA1**. Then press the **OK** button.



- 9) Switch to **Advanced** tab. In the setting **VPN policy bound to** select **Interface WAN**. Then press the **OK** button.

**Advanced Settings**

☐ Enable Keep Alive

☐ Suppress automatic Access Rules creation for VPN Policy

☐ Require authentication of VPN clients by XAUTH

User group for XAUTH users: --Select a user group--

☐ Enable Windows Networking (NetBIOS) Broadcast

☐ Enable Multicast

☐ Apply NAT Policies

Translated Local Network: --Select Translated Local Network--

Translated Remote Network: --Select Translated Remote Network--

Management via this SA: ☐ HTTP ☐ HTTPS

User login via this SA: ☐ HTTP ☐ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Interface WAN

**Ready**

OK Cancel Help

- 10) The VPN status page will show a new VPN rule. Make sure the rule has been enabled.

**VPN Policies**

Items 1 to 3 (of 3)

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1	WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	
2	WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	
3	ToZyWALL	210.110.7.1	192.168.1.1 - 192.168.1.255	ESP DES HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

Add... Delete Delete All

- 11) Ping the remote host to dial up the tunnel. We can check the connected VPN status in the VPN status page. The VPN tunnel should appear in the **Currently Active VPN Tunnels** page. It should show that the tunnel had been successfully built-up.

VPN Policies

Items 1 to 3 (of 3)

11

#	Name	Gateway	Destinations	Crypto Suite	Enable	Configure
<input type="checkbox"/>	1 WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	
<input type="checkbox"/>	2 WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)	<input type="checkbox"/>	
<input type="checkbox"/>	3 ToZyWALL	210.110.7.1	192.168.1.1 - 192.168.1.255	ESP DES HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>	

Add...
Delete
Delete A

Site To Site Policies: 1 Policies Defined, 1 Policies Enabled, 2 Maximum Policies Allowed  
GroupVPN Policies: 2 Policies Defined, 0 Policies Enabled, 6 Maximum Policies Allowed

Currently Active VPN Tunnels

Items 1 to 1 (of 1)

#	Name	Local	Remote	Gateway	
1	ToZyWALL	192.168.2.1 - 192.168.2.255	192.168.1.1 - 192.168.1.255	210.110.7.1	Renegotiate

1 Currently Active VPN Tunnels



## **1.3 Remote Access VPN**

Remote Access VPN provides a cost-effective alternative to standard dial-in remote access to a company network. The users can connect to the network via the Internet, eliminating the expensive long-distance or the toll-free dial-in costs.

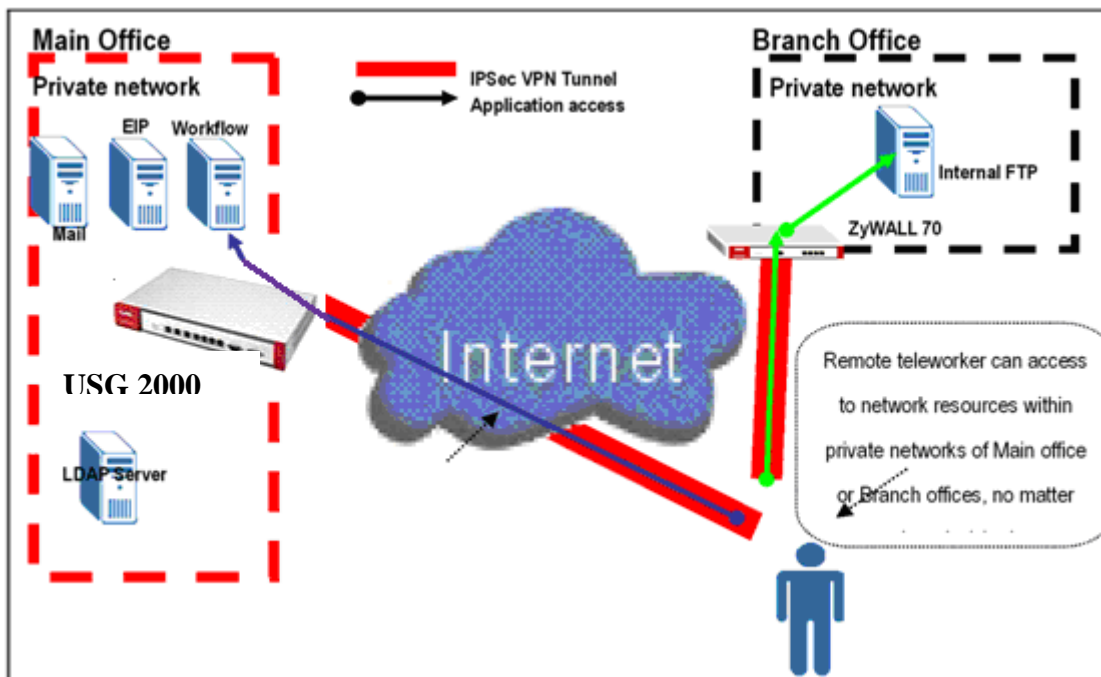
The most common scenario for application might look like this: An employee is on the road (i.e. teleworker). He can gain full network access simply by connecting to the Internet. During the data transmission between remote and host, this connection should also provide confidentiality (Data transferring in VPN tunnel with encryption).

Another genius application is a “Mobile office”: Teleworker or home & SOHO employee can work at airport, cyber café, hot spots, hotel or home. The office building scope can be eliminated and a global office can start to fully utilize the global resources.

ZyWALL USG 2000 incorporates IPSec, SSL VPN and L2TP over IPSec into a single box. The customers can choose the most appropriate application for the remote access application.

### **1.3.1 IPSec VPN for Remote Access**

In this scenario, we assume the ZyWALL USG 2000 admin configured the VPN settings in a way to allow teleworker access internal network resource through remote access VPN. Since it is unknown what IP address will the remote teleworker’s PC/notebook connect from, 0.0.0.0 is used as for ZyWALL USG 2000’s remote gateway setting it represents “any IPs”. On the other end, the teleworker use ZyWALL VPN client on their notebooks to establish IPSec VPN with the main office.



So we are going to complete the following tasks.

- In ZyWALL USG 2000 create object 'address' for both local and remote networks
- In ZyWALL USG 2000 configure a VPN gateway and the VPN connection setting
- In ZyWALL VPN client configure the corresponding VPN setting in ZyWALL VPN client

ZyWALL USG 2000	ZyWALL VPN Client
My address: <b>ge2(10.59.1.45)</b> Secure gateway address: <b>0.0.0.0</b> Local: <b>192.168.2.0/24</b> Remote: <b>0.0.0.0/24</b>	My address: <b>Any</b> Secure gateway address: <b>10.59.1.45</b> Local: <b>Any</b> Remote: <b>192.168.2.0/24</b>
Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1	Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1

Phase2	Phase2
Encapsulation: Tunnel	Encapsulation: Tunnel
Active Protocol: ESP	Active Protocol: ESP
Encryption: DES	Encryption: DES
Authentication: SHA1	Authentication: SHA1
Perfect Forward Secrecy (PFS): None	Perfect Forward Secrecy (PFS): None

### 1.3.1.1 Steps to configure

Below is step by step configuration:

- 1) Login ZyWALL USG 2000 GUI and go to **Object > Address** to create an address object (local subnet) for remote access.

- 2) Create another address object for the remote host. The **IP Address** of the host should be **0.0.0.0**, which means that remote user dials in dynamically.

- 3) Go to **VPN > IPSec VPN > VPN Gateway** to create gateway for remote a VPN client. Because this kind of VPN is initialed from remote user, the Secure Gateway should be set as

dynamic, 0.0.0.0. Also, the VPN peers should keep consistence with each other for other parameters, such as Pre-Shared Key, ID Type, Encryption and Authentication proposal and so on.

**ZyWALL > VPN > IPSec VPN > VPN Gateway > Edit > #1**

VPN Gateway Name: RemoteAccess

---

**Gateway Settings**

My Address

☒ Interface: ge2 Static -- 10.59.1.45/255.255.255.0

☐ Domain Name / IP

Peer Gateway Address

☐ Static Address

1. 0.0.0.0

2. 0.0.0.0

☒ Dynamic Address

---

**Authentication**

☒ Pre-Shared Key

☐ Certificate

Local ID Type: P

Content: 192.168.2.0

Peer ID Type: P

Content: 0.0.0.0

---

**Phase 1 Settings**

SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Proposal

#	Encryption	Authentication	
1	DES	MD5	

Key Group: DH1

☐ NAT Traversal

☒ Dead Peer Detection (DPD)

**Less Settings**

---

**Extended Authentication**

☐ Enable Extended Authentication

☒ Server Mode: default

☐ Client Mode

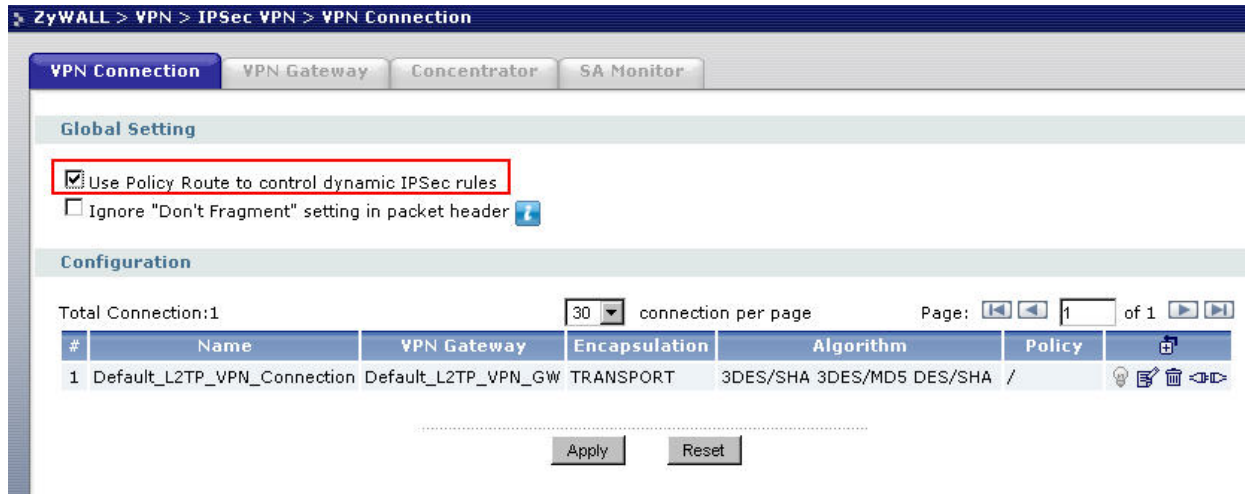
User Name:

Password:

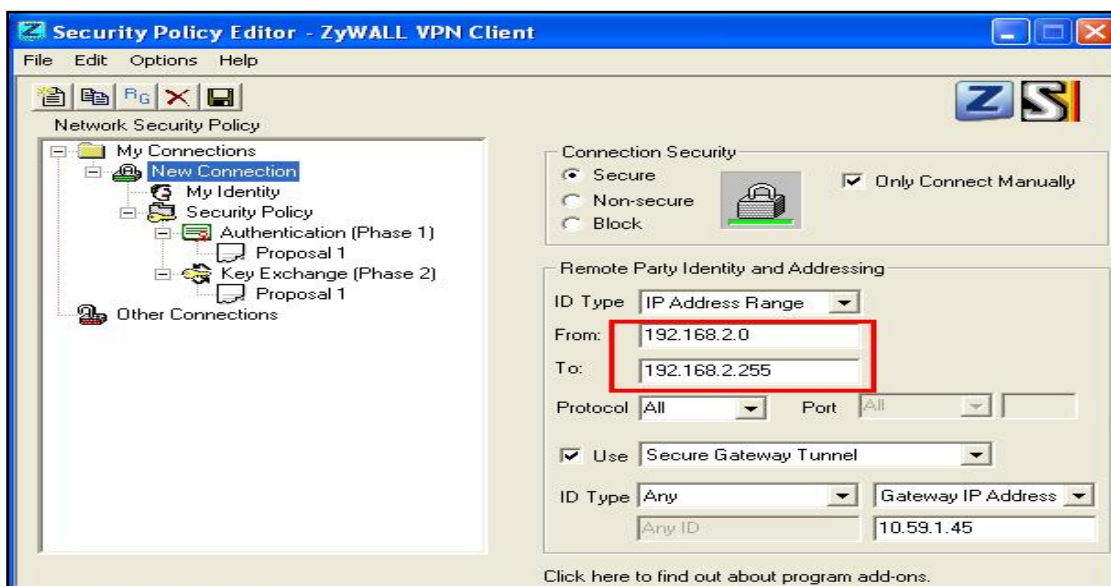
OK Cancel

Message: Ready.

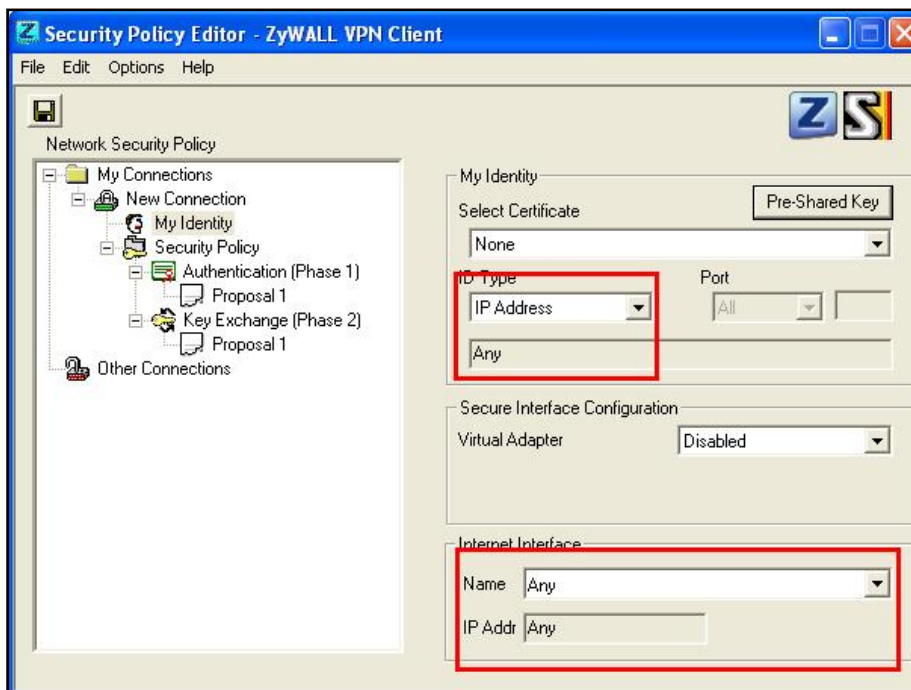
4) To create a VPN rule, go to **VPN > IPSec VPN > VPN Connection**. Check the “**Use Policy Route to control dynamic IPSec rules.**” as defined in step 1 and step 2. Remote policy should be a dynamic host address. We put **VPN Gateway** as dynamic as was defined in step 3.



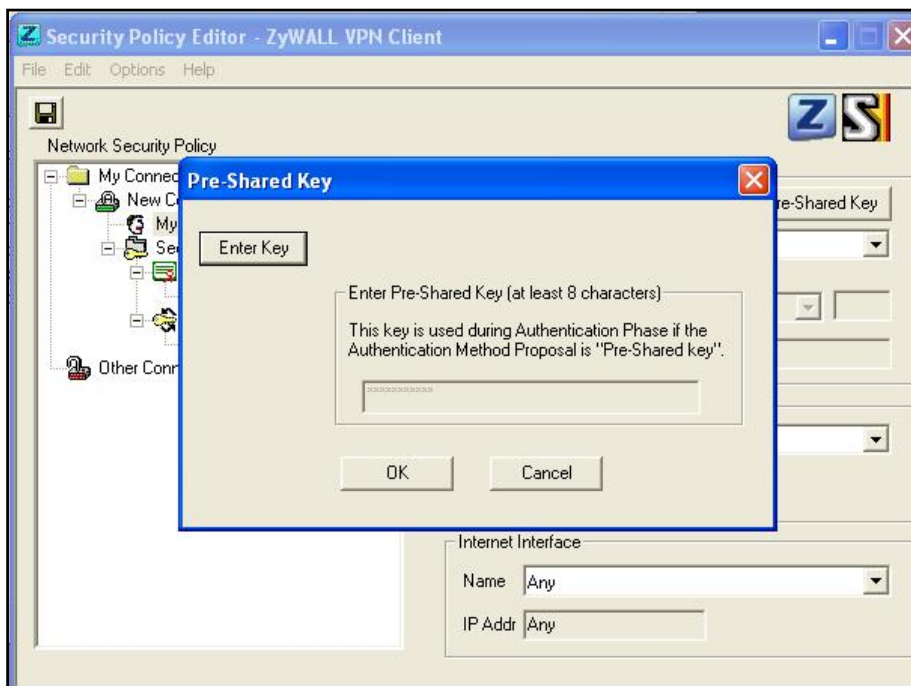
5) Go to remote host to configure ZyXEL VPN Client. We create a **Net Connection** set remote access subnet to 192.168.2.x.



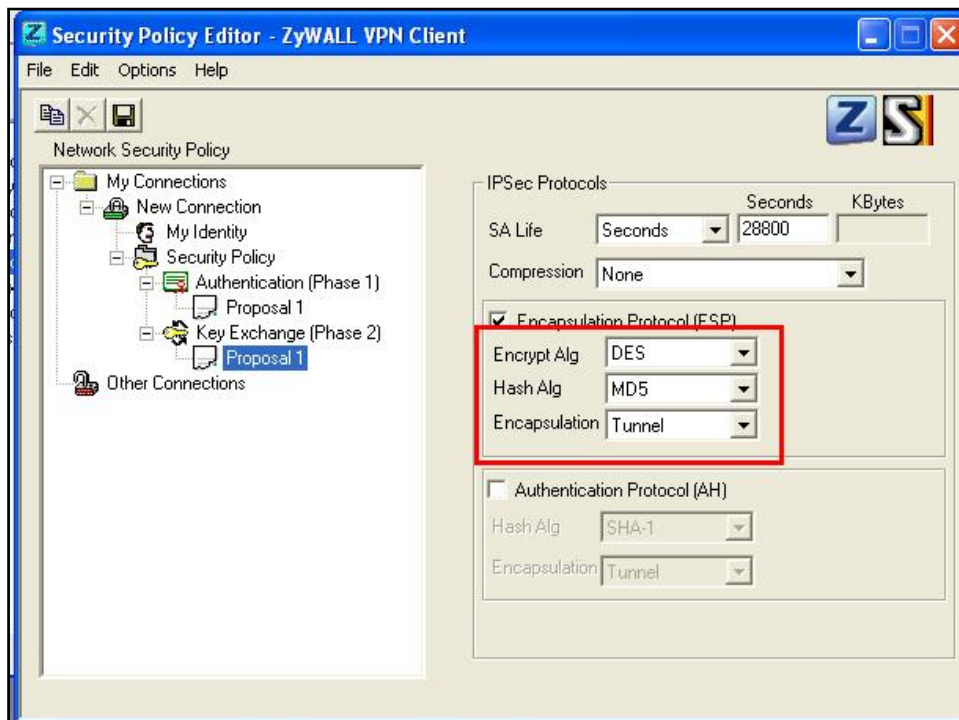
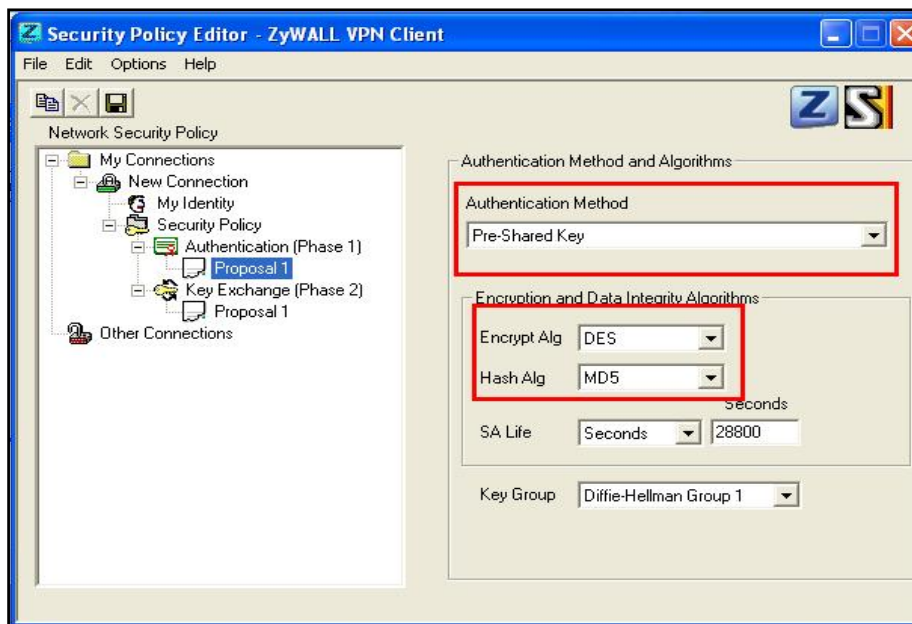
In **My Identity**, select local **ID type** as Any.



Note: Do not forget to enter Pre-Shared Key by clicking the button **Pre-Shared Key**.



The last step is to go to **Security Policy** to configure parameters for Phase1 and Phase 2. After saving the configuration, the VPN connection should be initialed from the host site.



### Tips for application:

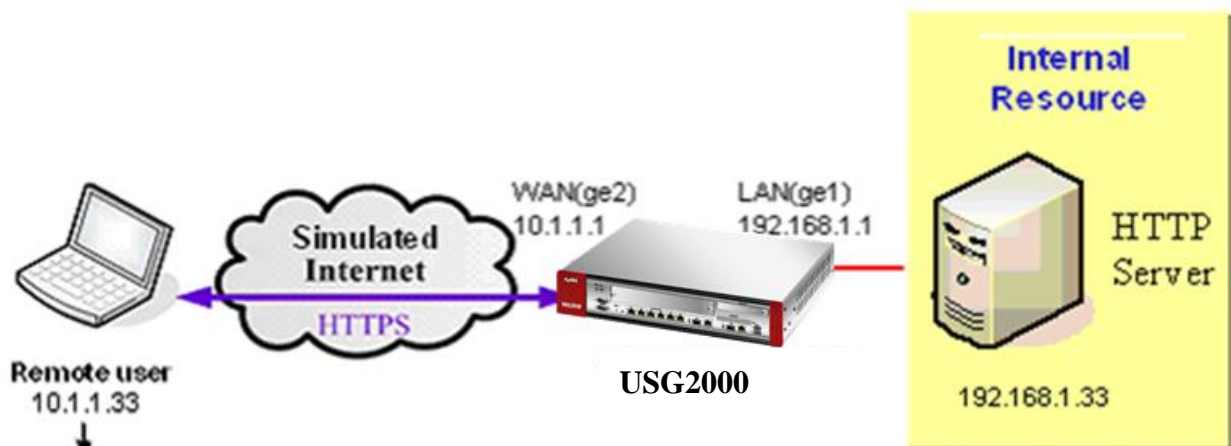
1. Make sure both **pre-shared key** settings are the same in local and remote gateway.
2. Make sure both **IKE proposal** settings are the same in local and remote gateway.
3. Select the correct **interface** for the VPN connection.
4. The **Local** and **Peer ID type** and content must be the opposite and not of the same content.
5. The **Local Policy** of ZyWALL USG 2000 should be 'dynamic single host with the value 0.0.0.0'. The VPN tunnel should be initiated from the remote host site.



### 1.3.2 SSL VPN Application - Reverse Proxy

In order to provide a proper access for remote users, a web server is considered to implement behind ZyWALL USG 2000. So, remote users can access the internal resource anywhere via a secure path.

#### 1.3.2.1 Scenario topology



The default LAN subnet is combined to ge1 and default IP is 192.168.1.1. Please connect to lan1 and ZyWALL USG 2000 will dispatch an IP for your PC then we can start to setup the basic interface and routing setting.

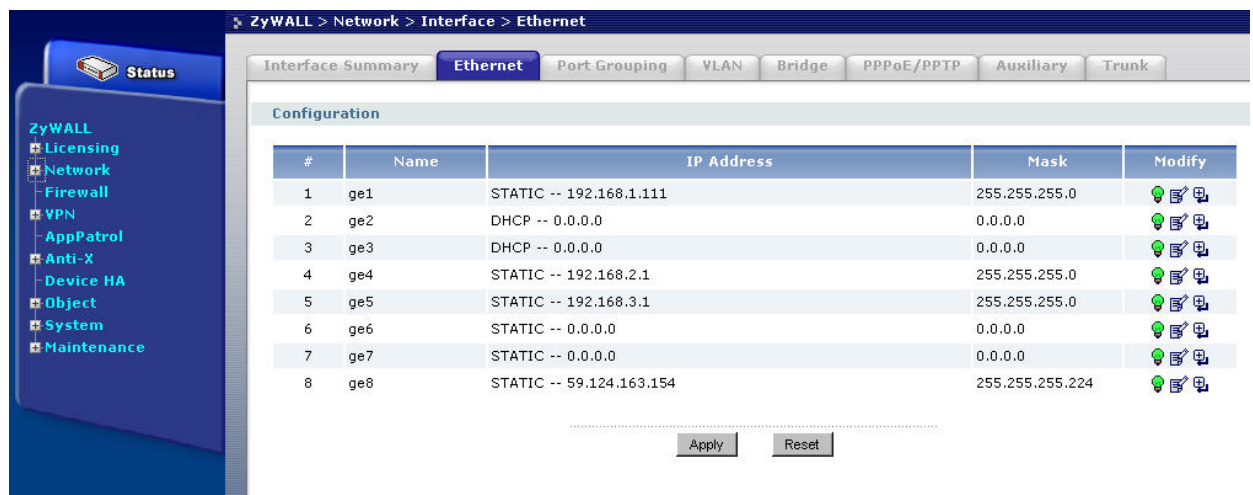
#### 1.3.2.2 Configuration flow

- Network setup
- Test

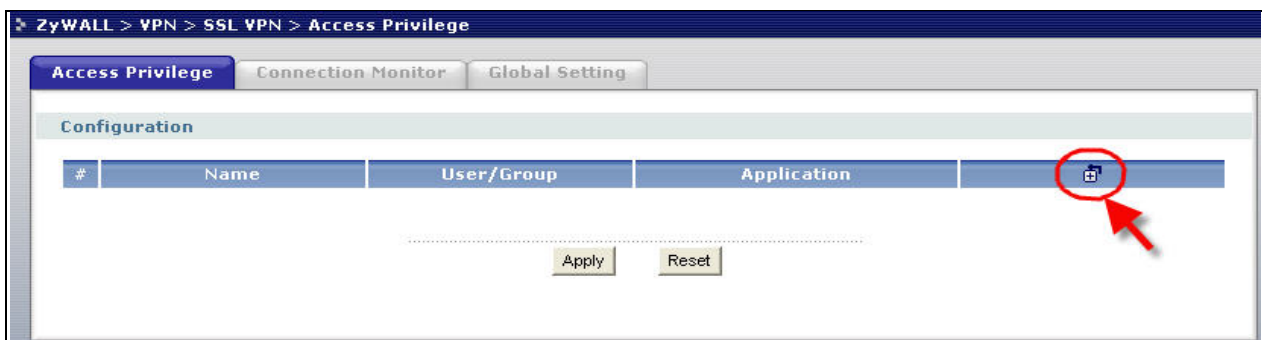
#### 1.3.2.3 Configuration procedure

1) Connect your NB at ZyWALL USG 2000's ge1 port. Get the IP address by DHCP and login to ZyWALL USG 2000 by <http://192.168.1.1>. Configure the ZyWALL USG 2000's ge1 and ge2 interface with proper IP address.

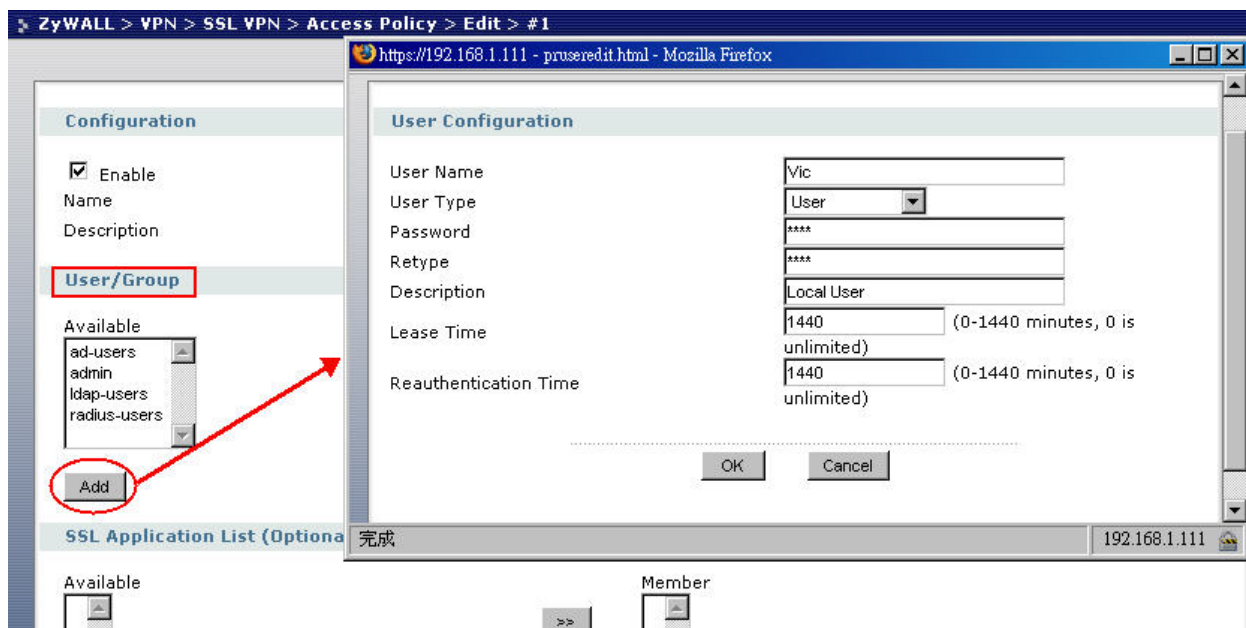




2) Go to menu **ZyWALL> VPN > SSL VPN**, create one access privilege rule by clicking the **Add** icon.



Then continue to create user or group object. Here we create one user by click the “Add” button.



Then, continue to create one application object. Here we create one for reverse proxy rule using web application by click the “Add” button.



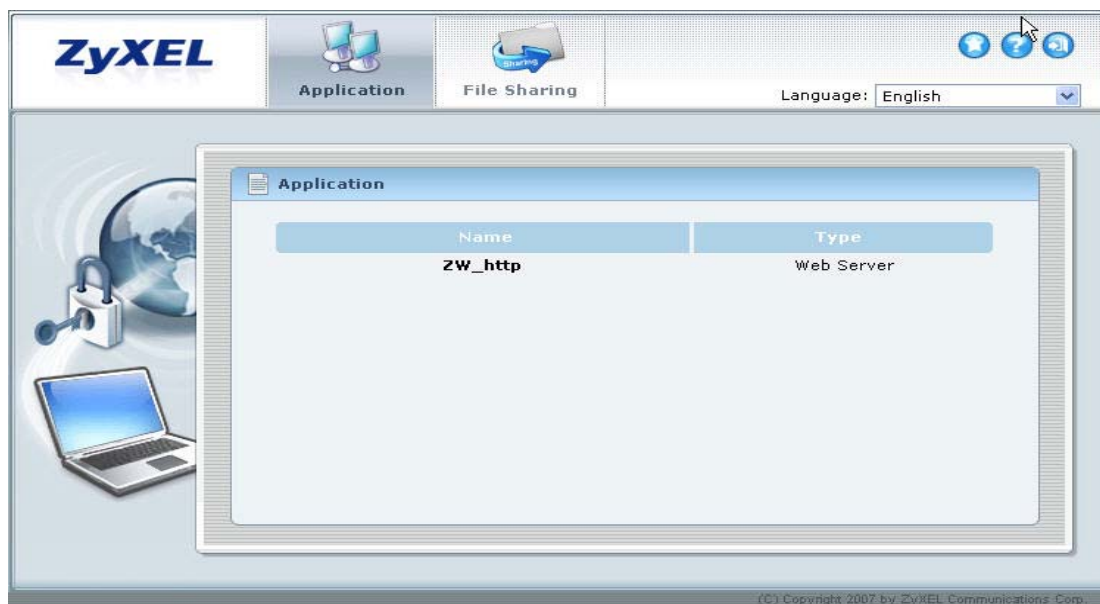
**Login and check if WAN user can access to the ZyWALL GUI by HTTP.**

Step 1. Initial a browser and try to connect to <http://10.1.1.1>

Step 2. Enter the ID/password, check the “log into SSL VPN” and click **Login** button.



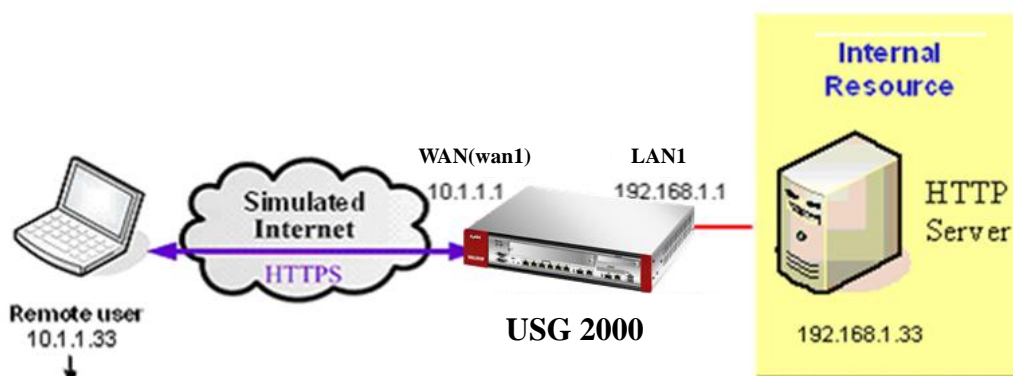
Step 3. Click the **Yes** buttons until you see the following page, which is the ZW\_http link available in the application list.



### 1.3.3 SSL VPN Application – Network Extension

The network extension application enables the user to use specific client tools to access the server. Unlike reverse proxy applications, the user won't be limited to the access to the available application list only. They can access any destination which is allowed and is pre-defined in "SSL VPN network" list.

#### 1.3.3.1 Scenario topology



#### 1.3.3.2 Configuration flow

- Network setup

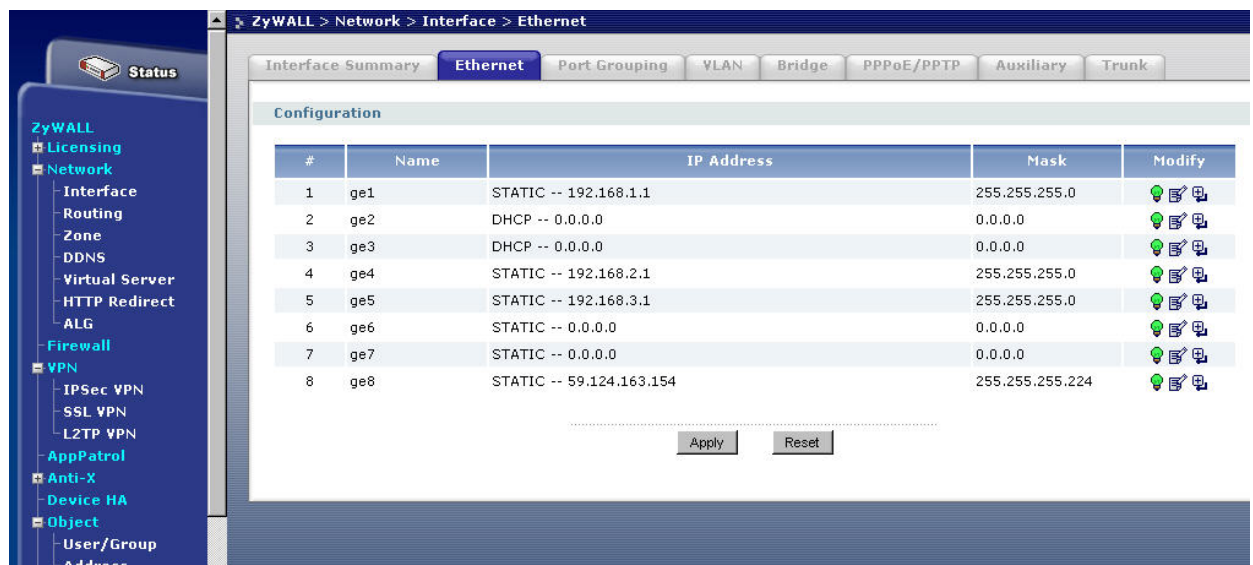
- Test

### 1.3.3.3 Configuration procedure

#### Network setup

The default ge1 subnet is combined to ge1 and default IP address is 192.168.1.1. Please connect your NB to ge1 port and ZyWALL USG 2000 will dispatch an IP address. Then we can start to setup the basic interface setting.

- Step 1. Connect your NB at ZyWALL USG 2000's LAN (lan1). Get the IP address by DHCP and login to ZyWALL USG 2000 by <http://192.168.1.1>. Configure the ZyWALL USG 2000's LAN and WAN interface with proper IP address in **ZyWALL> Network > Interface**.



- Step 2. Create address Object for remote IP assignment. Switch to menu **Object > Address** and click **Add** icon to add new user.



Configure a network range from 8.1.1.33 to 8.1.1.50 for remote IP assignment.

**Configuration**

Name

SSLremoteIP

Address Type

RANGE

Starting IP Address

8.1.1.33

End IP Address

8.1.1.50



OK

Cancel

- Step 3. Create address Object for VPN network which allows remote users to access to. Switch to menu **Object** > **Address** and click **Add** icon to add new address.

**Address**
Address Group

**Configuration**

#	Name	Type	Address	
1	LAN_SUBNET	SUBNET	192.168.1.0/24	
2	SSLremoteIP	RANGE	8.1.1.33-8.1.1.50	

Configure a network subnet 192.168.1.0/24.

**Configuration**

Name

network\_192\_168\_1

Address Type

SUBNET

Network

192.168.1.0

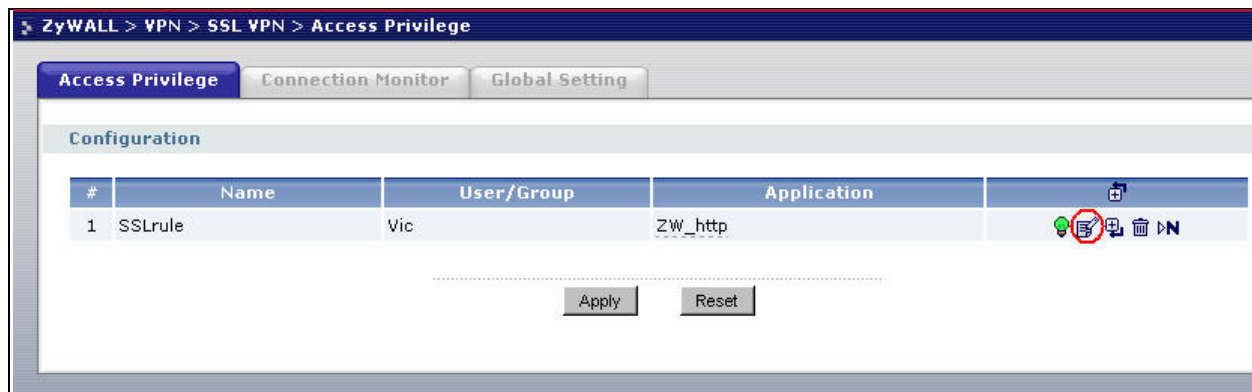
Netmask

255.255.255.0

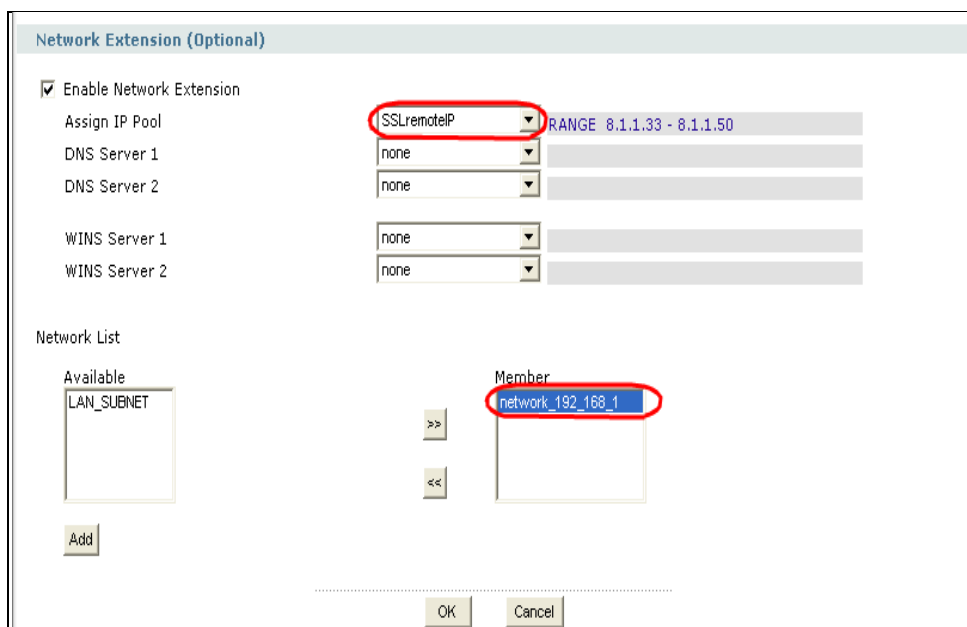
OK

Cancel

- Step 4. Modify the SSL rule we created for LAB1 by clicking the **modify** icon.



Step 5. Keep other settings but choose object we just created for network extension settings as follows. Click **OK** button.



**Test: Login and check if WAN user can access to the ZyNOS ZyWALL GUI by HTTP**

Step 1. Config your NB with IP address 10.1.1.33 and connect it to ZyWALL USG 2000's WAN site (ge2). Initial a browser and try to connect to <https://10.1.1.1>

Step 2. Enter the ID/password, check the **"log into SSL VPN"** and click **Login** button.



The image shows the login interface for a ZyWALL USG 2000. At the top is a blue header with the 'ZyXEL' logo. Below it, the text 'ZyWALL USG 2000' is centered. A prompt 'Enter User Name/Password and click to login.' is displayed. There are three input fields: 'User Name' with 'admin' entered, 'Password' with '\*\*\*\*' entered, and 'One-Time Password' which is empty. A checkbox labeled 'Log into SSL VPN' is checked. Below the fields is a 'Note' section with three instructions. At the bottom are 'Login' and 'Reset' buttons.

**ZyXEL**

ZyWALL USG 2000

Enter User Name/Password and click to login.

😊 **User Name:**

🔒 **Password:**

🔑 **One-Time Password:**  **(Optional)**  
( max. 31 alphanumeric, printable characters and no spaces )

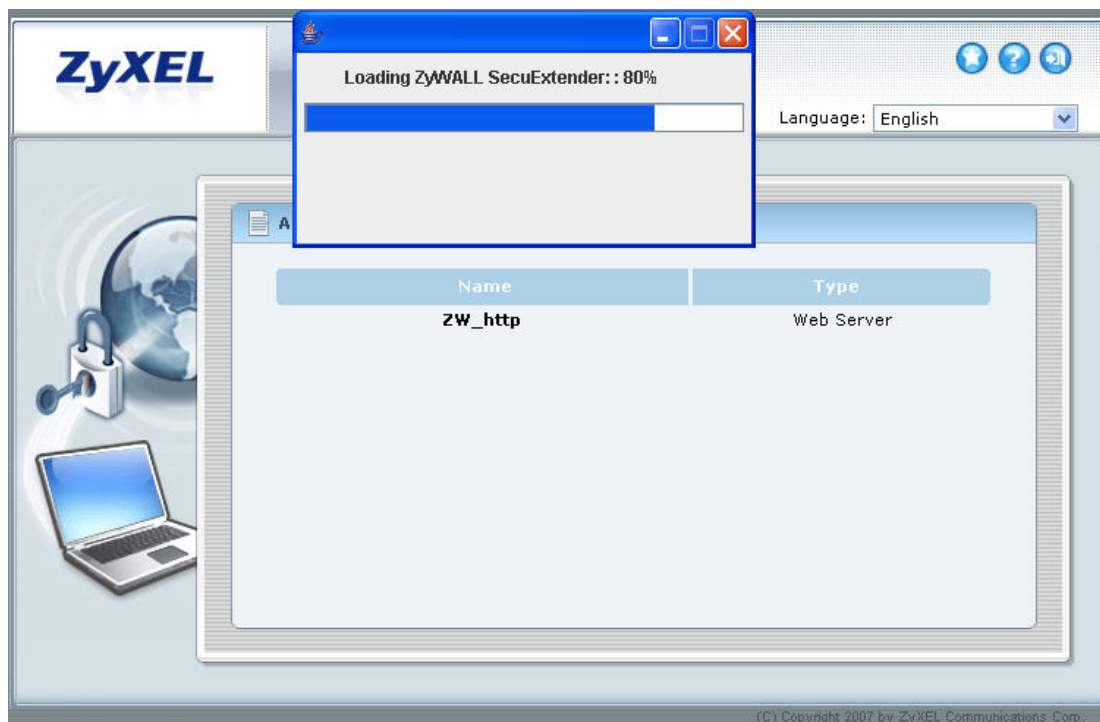
☒ **Log into SSL VPN**

📌 **Note:**

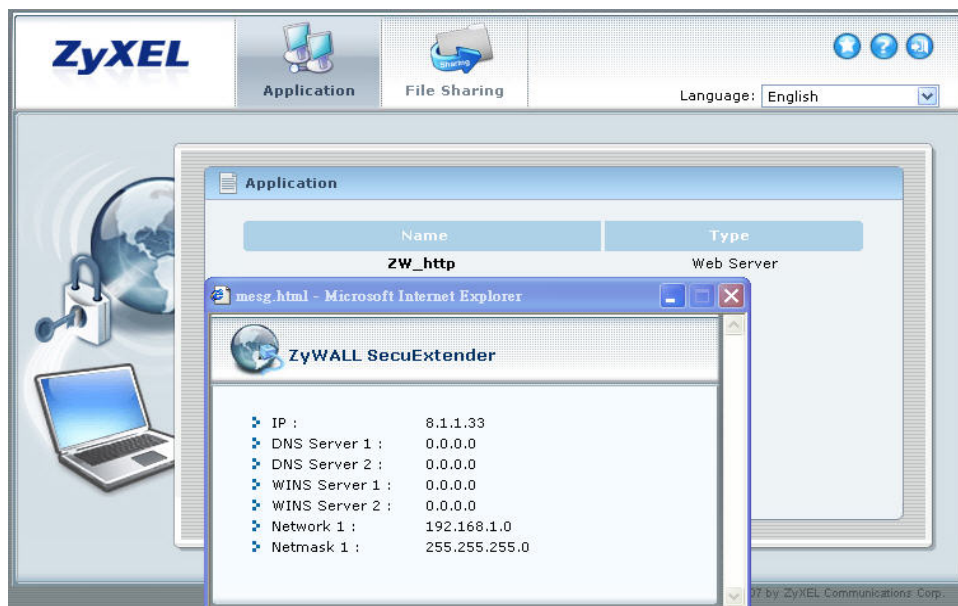
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.

- Step 3. Click **Yes** buttons until you see the following page. You can find a small window is processing about the security extender rule (for network extension).





Step 4. After a while, the window will show you the information about network extension.



Step 5. Please check the IP address assigned and routing info on the remote PC/NB.

You will see one PPP interface as below by typing 'ipconfig' on command prompt.

```
Windows IP Configuration
PPP adapter RAS Server (Dial In) Interface:

Connection-specific DNS Suffix . : 
IP Address. . . . . : 8.1.1.33
Subnet Mask . . . . . : 255.255.255.255
Default Gateway . . . . . :
```

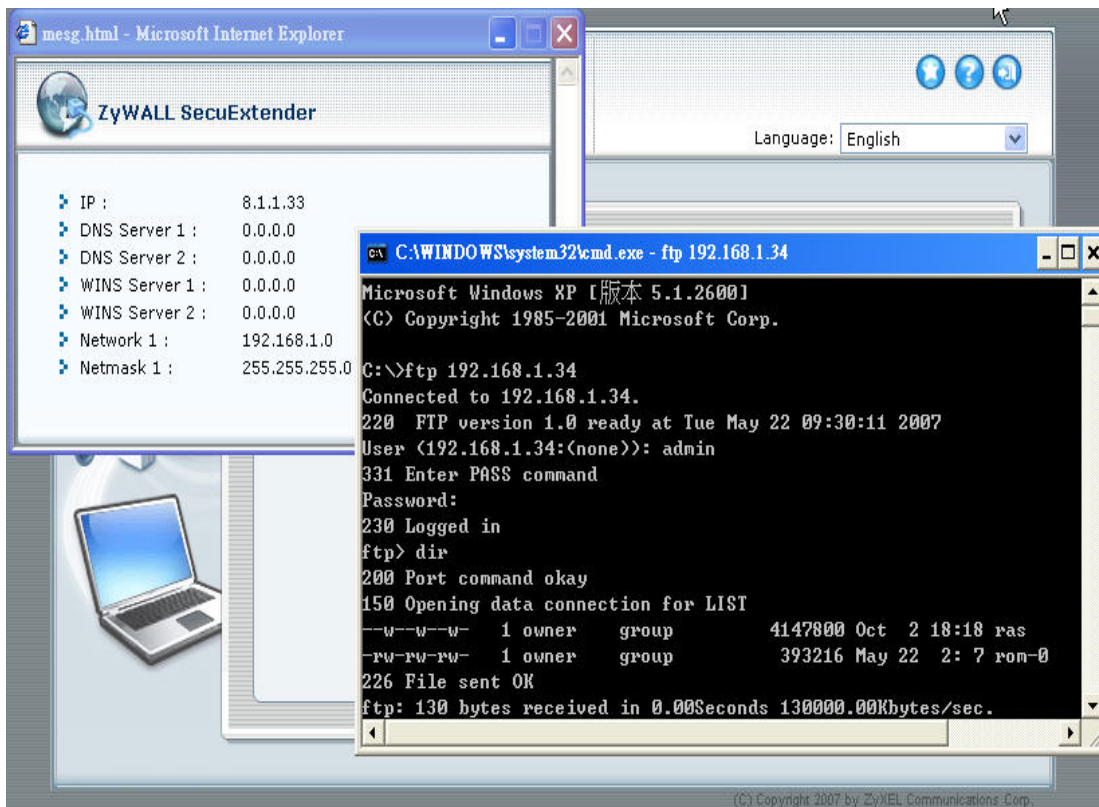


You will see the routing information accordingly as below by typing 'route print'.

Network	Destination	Netmask	Gateway	Interface	Metric
	8.1.1.33	255.255.255.255	127.0.0.1	127.0.0.1	50
	192.168.1.0	255.255.255.0	192.168.200.1	8.1.1.33	2

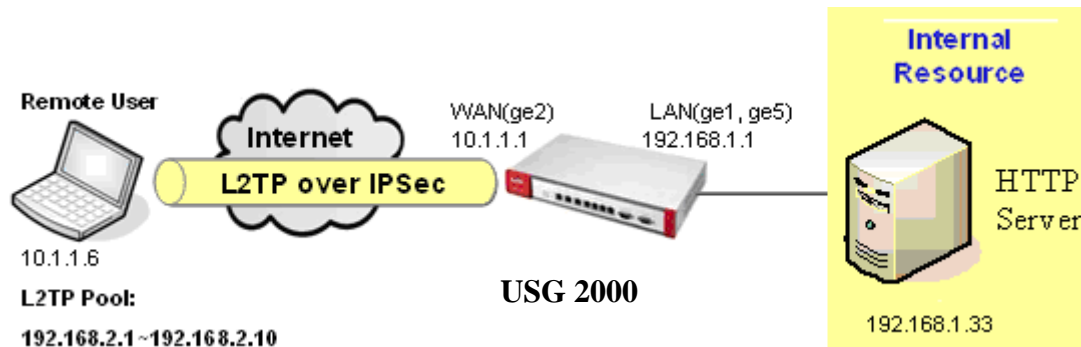
Step 6. Still try to connect the ZW\_http link. You should be able to access the ZyWALL login page then.

Step 7. Try to ftp the device and see if you can access the ZyNOS ZyWALL by FTP tool. If so, that means you have successfully established the network extension and aren't limited just by the available application list.



### 1.3.4 L2TP over IPSec Application

#### 1.3.4.1 Scenario topology



#### 1.3.4.2 Configuration flow

- **Create object**
- **Configure the default L2TP rule in IPSec VPN Gateway**
- **Configure the default L2TP rule in IPSec VPN Connection**
- **Configure the L2TP rule**
- **Configure Policy Route for L2TP**
- **Remote PC/NB L2TP Setup on WinXP or Win2K**

#### 1.3.4.3 Configuration Procedure

##### Create Object

Step 1. Switch to menu **Object > Address**, create two object for further VPN connection setting.

L2TP\_IFACE, HOST, 10.1.1.1

L2TP\_HOST, HOST, 0.0.0.0

L2TP\_Pool, Range, 192.168.2.1 ~ 192.168.2.10

Step 2. Switch to menu **Object > User/Group**, create one object for L2TP application.

L2TP\_user/1234, Local user

### Configure the default L2TP rule in IPsec VPN Gateway

Step 1. Go to menu **VPN > IPsec VPN > VPN Gateway**, click the **Default\_L2TP\_VPN\_GW** entry's **Edit** icon.

#	Name	My address	Secure Gateway	VPN Connection	
1	Default_L2TP_VPN_GW	ge2	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection	

Step 2. Ensure the My Address is configured with Interface ge2 with WAN IP address, 10.1.1.1. And the pre-shared key is 12345678. Click the **OK** button.

**General Settings**

VPN Gateway Name: Default\_L2TP\_VPN\_GW

**Gateway Settings**

My Address: ☒ Interface ☐ Domain Name / IP

Peer Gateway Address: ☐ Static Address ☒ Dynamic Address

1. 0.0.0.0

2. 0.0.0.0

**Authentication** Advanced

☒ Pre-Shared Key: 12345678

☐ Certificate: default (See [My Certificates](#))

**Phase 1 Settings** Advanced

SA Life Time: 86400 (180 - 3000000 Seconds)

Step 3. Enable the rule by clicking the **enable** icon.

VPN Connection | **VPN Gateway** | Concentrator | SA Monitor

**Configuration**

Total Connection:1 30 connection per page Page: 1 of 1

#	Name	My address	Secure Gateway	VPN Connection	
1	Default_L2TP_VPN_GW	ge2	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection	

Apply Reset

### Configure the default L2TP rule in IPSec VPN Connection

Step1. Switch to menu **VPN > IPSec VPN > VPN Connection**, click the **Default\_L2TP\_VPN\_GW** entry's **Edit** icon.

VPN Connection | VPN Gateway | Concentrator | SA Monitor

**Global Setting**

☐ Use Policy Route to control dynamic IPSec rules  
☐ Ignore "Don't Fragment" setting in packet header

**Configuration**

Total Connection:1 30 connection per page Page: 1 of 1

#	Name	VPN Gateway	Encapsulation	Algorithm	Policy	
1	Default_L2TP_VPN_Connection	Default_L2TP_VPN_GW	TRANSPORT	3DES/SHA 3DES/MD5 DES/SHA	/	

Apply Reset

Step 2. Especially configure the policy enforcement as below. Click **OK** button.

**Policy** Basic

Local policy L2TP\_IFACE HOST, 10.1.1.1

Remote policy L2TP\_HOST HOST, 0.0.0.0

☒ Policy Enforcement

Step 3. Enable the rule by clicking the **enable** icon.

**VPN Connection** | VPN Gateway | Concentrator | SA Monitor

**Global Setting**

☐ Use Policy Route to control dynamic IPsec rules

☐ Ignore "Don't Fragment" setting in packet header

**Configuration**

Total Connection: 1 | 30 connection per page | Page: 1 of 1

#	Name	VPN Gateway	Encapsulation	Algorithm	Policy
1	Default_L2TP_VPN_Connection	Default_L2TP_VPN_GW	TRANSPORT	3DES/SHA 3DES/MD5 DES/SHA	/

Apply Reset

### Configure the L2TP rule

Step 1. Go to menu **VPN > L2TP VPN**, configure it as follows.

**L2TP VPN** | Session Monitor

**General Setup**

☒ Enable L2TP Over IPsec

VPN Connection: Default\_L2TP\_VPN\_Connection

IP Address Pool: L2TP\_Pool

Authentication Method: default

Allowed User: L2TP\_user

Keep Alive Timer: 60 (1-180 seconds)

First DNS Server (Optional): Custom Defined

Second DNS Server (Optional): Custom Defined

First WINS Server (Optional):

Second WINS Server (Optional):

Apply Reset

### Configure Policy Route for L2TP

Step 1. Go to menu **Network > Routing > Policy Route**, configure it as follows.

Configuration							
<input checked="" type="checkbox"/> Enable							
Description	for_L2TP (Optional)						
Criteria							
User	any						
Incoming	Interface / any <span>Change...</span>						
Source Address	LAN_SUBNET						
Destination Address	L2TP_POOL						
Schedule	none						
Service	any						
Next-Hop							
Type	VPN Tunnel						
VPN Tunnel	Default_L2TP_VPN_Connection						
<input type="checkbox"/> Auto Destination Address							
Port Triggering	<table border="1"> <thead> <tr> <th>#</th> <th>Incoming Service</th> <th>Trigger Service</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table>	#	Incoming Service	Trigger Service			
#	Incoming Service	Trigger Service					

## Remote PC/NB L2TP Setup on WinXP or Win2K

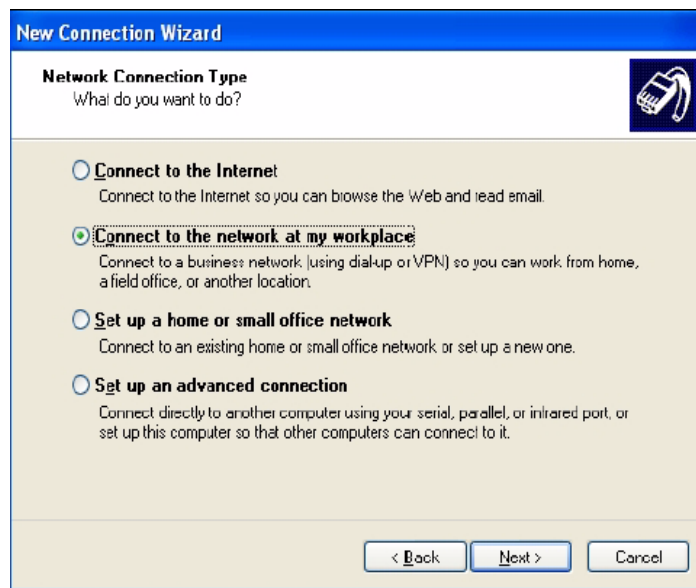
*Note: Please ensure your computer is using Windows XP and Windows 2000 for the follow settings.*

Before you configure the client, issue one of the following commands from the Windows command prompt to make sure the computer is running the Microsoft IPsec service. Make sure you include the quotes.

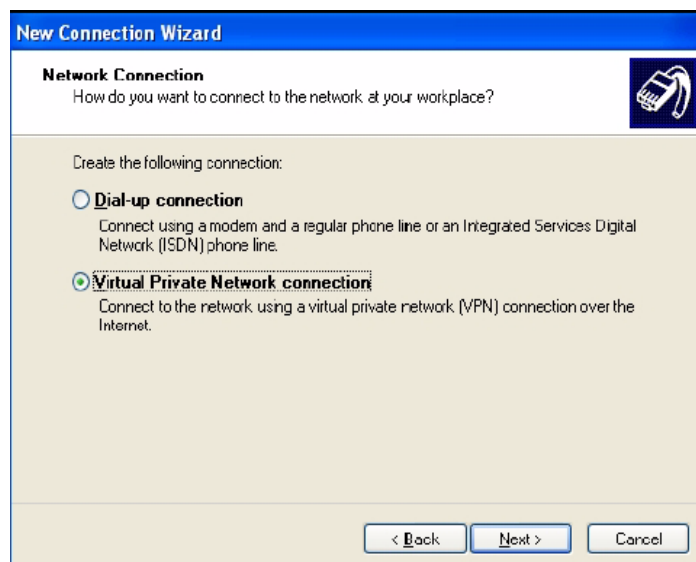
- For Windows XP, use net start "ipsec services".
- For Windows 2000, use net start "ipsec policy agent".

In Windows XP do the following to establish an L2TP VPN connection.

- Step 1** Click **Start > Control Panel > Network Connections > New Connection Wizard**.
- Step 2** Click **Next** in the **Welcome** screen.
- Step 3** Select **Connect to the network at my workplace** and click **Next**.

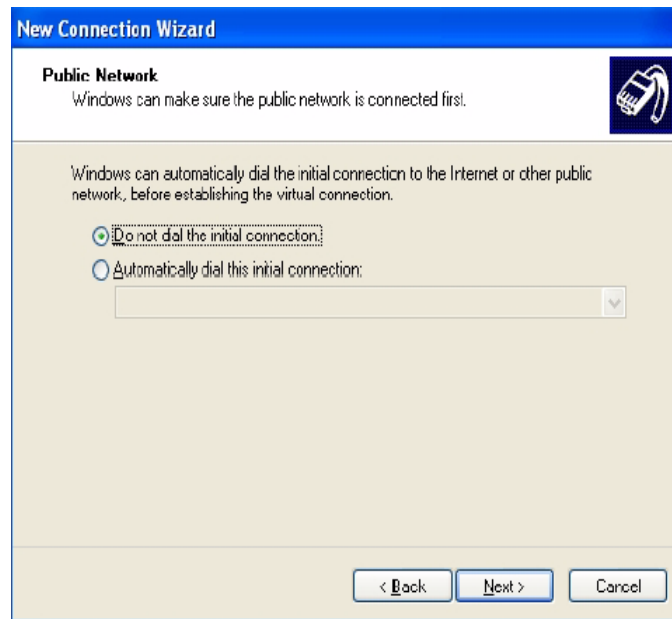


**Step 4** Select **Virtual Private Network connection** and click **Next**.

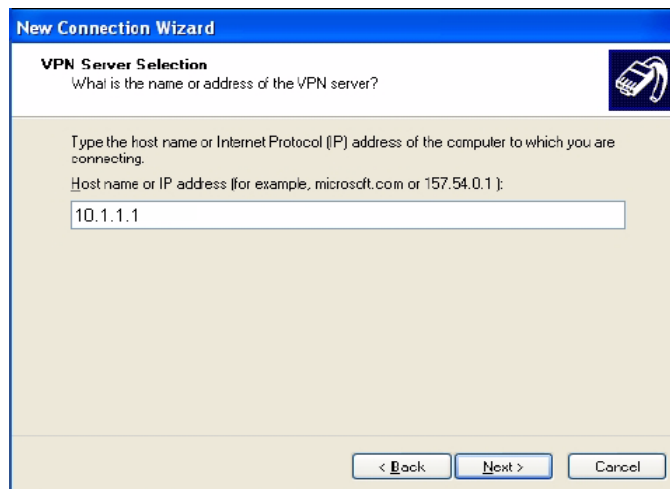


**Step 5** Type **L2TP to ZyWALL** as the **Company Name**.

**Step 6** Select **Do not dial the initial connection** and click **Next**.



- Step 7** Enter the domain name or WAN IP address configured as the **My Address** in the VPN gateway configuration that the ZyWALL is using for L2TP VPN (10.1.1.1 in this example). Click **Next**.



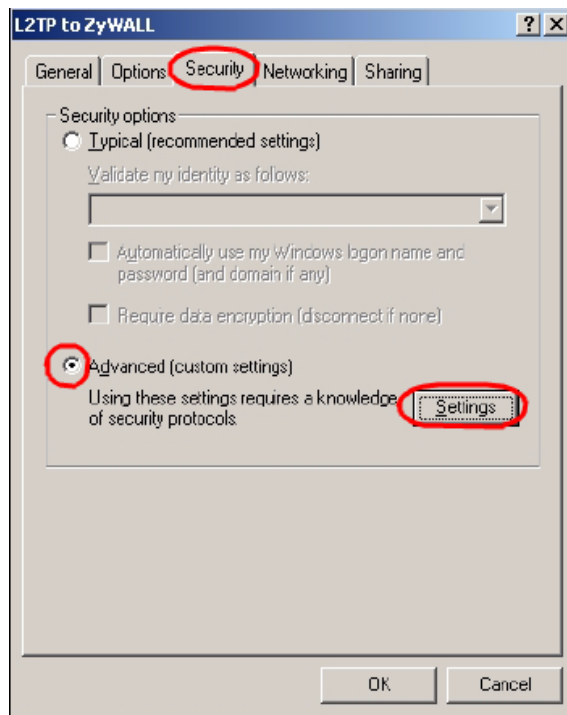
- Step 8** Click **Finish**.



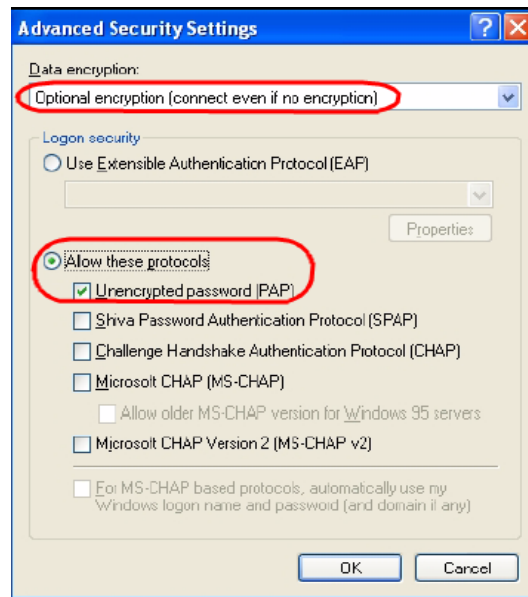
**Step 9** The **Connect L2TP to ZyWALL** screen appears. Click **Properties > Security**.



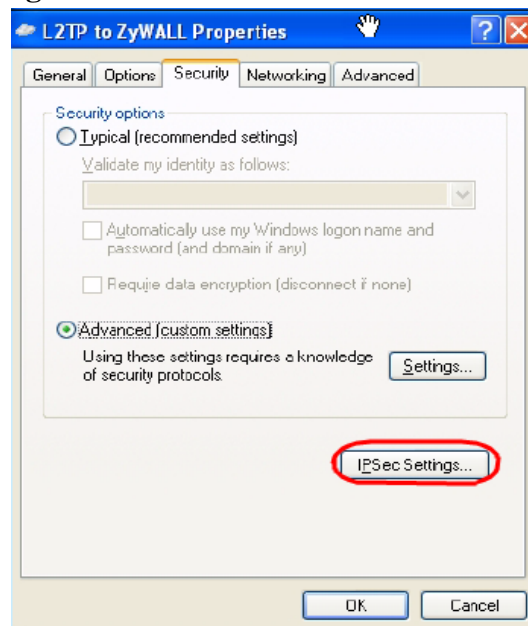
**Step 10** Click **Security**, select **Advanced (custom settings)**, and click **Settings**.



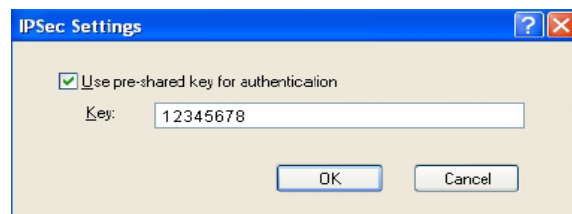
**Step 11** Select **Optional encryption allowed (connect even if no encryption)** and the **Allow these protocols** radio button. Select **Unencrypted password (PAP)** and clear all of the other check boxes. Click **OK**.



**Step 12** Click **IPSec Settings**.



**Step 13** Select the **Use pre-shared key for authentication** check box and enter the pre-shared key used in the VPN gateway configuration that the ZyWALL is using for L2TP VPN. Click **OK**.

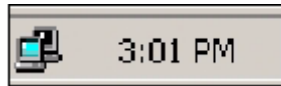


**Step 14** Click **Networking**. Select **L2TP IPSec VPN** as the **Type of VPN**. Click **OK**.

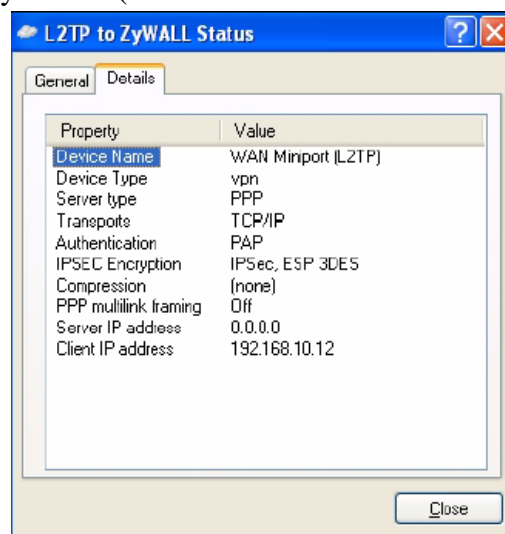
**Step 15** Enter the user name and password of your ZyWALL account. Click **Connect**.

**Step 16** A window appears while the user name and password are verified.

**Step 17** A ZyWALL-L2TP icon displays in your system tray. Double-click it to open a status screen.



**Step 18** Click **Details** to see the address that you received is from the L2TP range you specified on the ZyWALL (192.168.10.10-192.168.10.20).



**Step 19** Access the HTTP server behind the ZyWALL USG 2000 to make sure your access works.

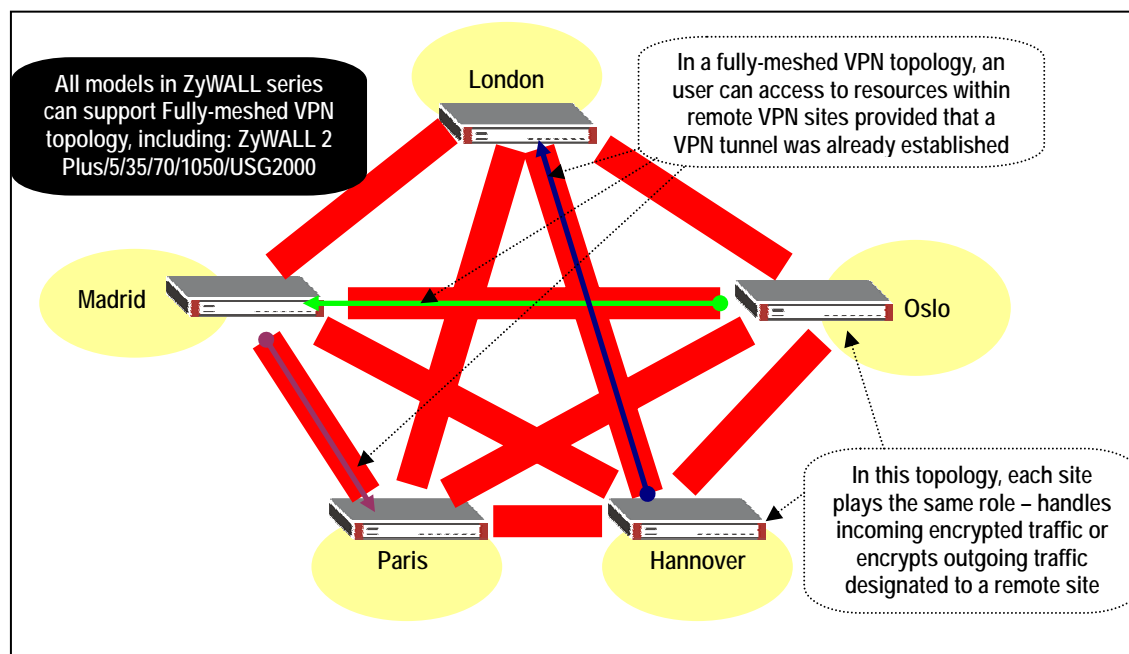


## 1.4 Large-scale VPN Deployment

With the business growing, network administrator will face the more and more complicated VPN topology and applications. ZyWALL USG2000 supports various types of VPN topology that can meet the needs of the organizations of any size.

ZyWALL USG2000 VPN Topology supports fully meshed topology that can be deployed when the total number of remote site is small. Star topology is recommended when the total number of remote sites is high, Even more flexible design, Star and Mesh mixed topology (cascading topology) can be applied for a global distributed environment.

### 1.4.1 Fully Meshed Topology



- 1) In order to achieve the VPN connectivity of all sites in the fully meshed VPN topology, all the sites must be directly connected with VPN tunnels to all the remote sites. The network administrator has to pay huge establishment and maintenance effort with the new remote site joining. This VPN topology is suitable for only a few sites connected with VPN.
- 2) For example, to complete the above topology, administrator needs to repeat the same steps at least five times and totally needs to establish 10 VPN tunnels. The tunnels list follows:

**Tunnel 1: London  $\leftarrow$ VPN  $\rightarrow$ Madrid**

**Tunnel 2: London ←VPN →Paris**

**Tunnel 3: London ←VPN →Hannover**

**Tunnel 4: London ←VPN →Oslo**

**Tunnel 5: Madrid ←VPN → Paris**

**Tunnel 6: Madrid ←VPN → Hannover**

**Tunnel 7: Madrid ←VPN → Oslo**

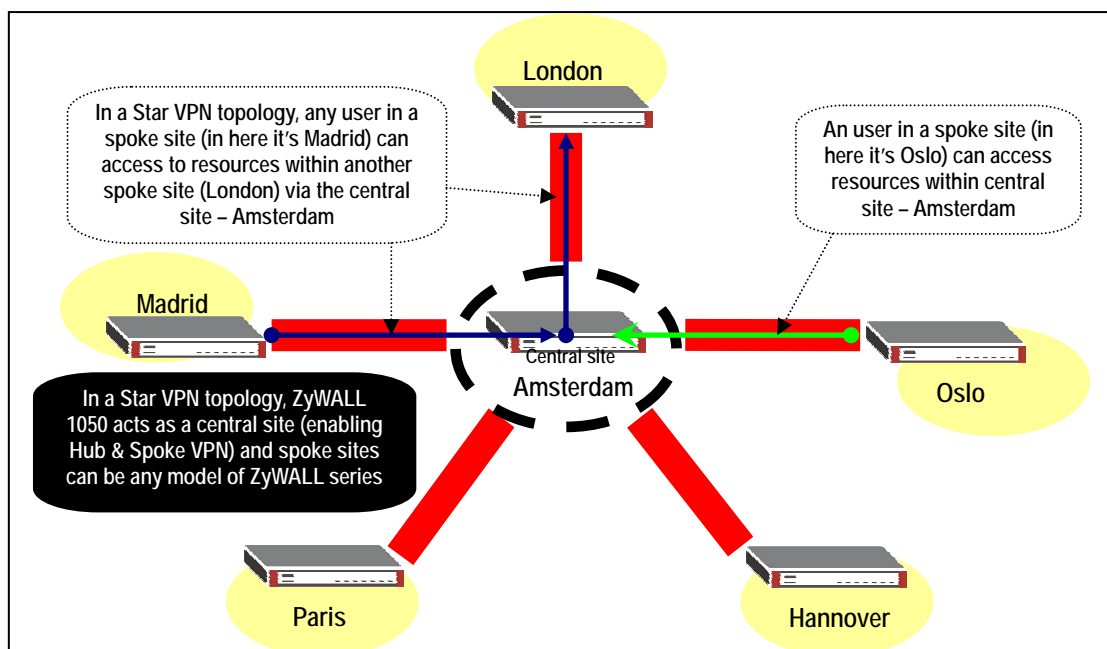
**Tunnel 8: Paris ←VPN → Hannover**

**Tunnel 9: Paris ←VPN → Oslo**

**Tunnel 10: Hannover ←VPN → Oslo**

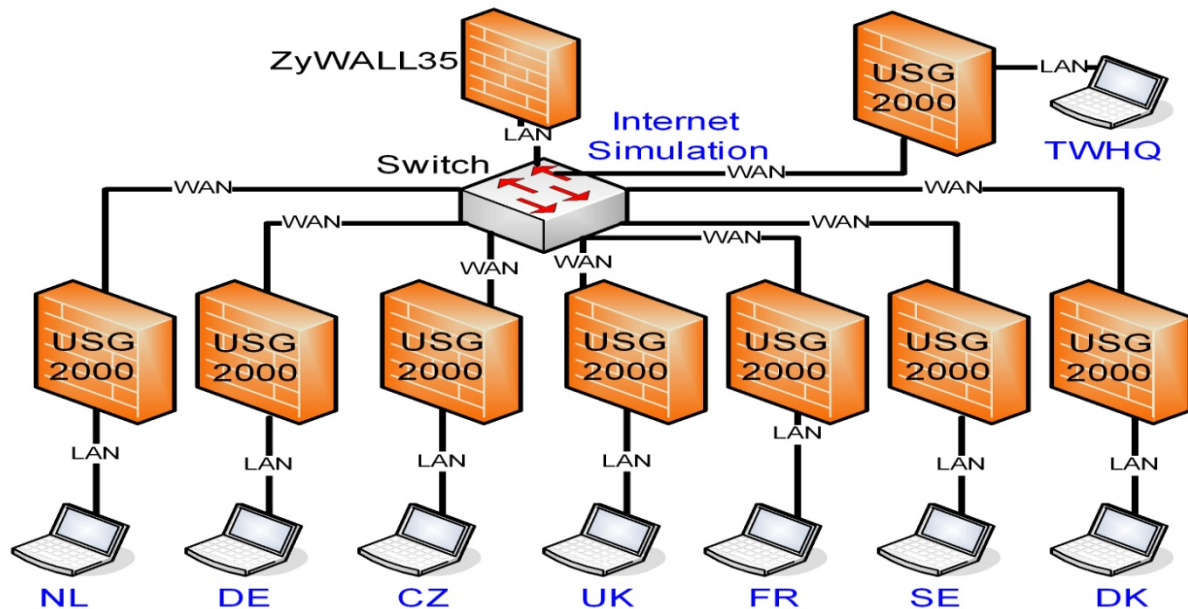
- 3) For help on building up the 10 tunnels, please refer to the section ZyWALL USG2000 to ZyWALL USG2000 VPN tunnel configuration steps . We will introduce the configuration steps for a VPN concentrator that will greatly help to reduce the total number of tunnels.

### 1.4.2 Star Topology



The ZyWALL USG2000 supports Star topology via the VPN concentrator feature. The VPN concentrator can help to reduce the VPN tunnel numbers and allows centralized VPN tunnel management.

The topology used for our VPN concentrator guide.



This topology is designed to simulate a global VPN network deployment. The company has a global headquarters in Taiwan and other offices around the world.

This company decided to build up a VPN concentrator to let all the offices' internal network to be shared and interconnected based on a security link.

We will separate each group as a member of each office and build up the VPN tunnel with headquarter and then to route the VPN traffic across the HQ to the destination office's internal network.

#### The VPN configuration parameter

Remote Office	HQ
WAN: 10.59.1.11	WAN: 10.59.1.10
~	LAN: 192.168.100.0/24

WAN: 10.59.1.17 LAN: 192.168.101.0/24 ~ LAN: 192.168.119.0/24	
Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1	Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1
Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None	Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None

### Setup VPN tunnel between each remote office and HQ

We used the Netherland site (NL) as an example to show how to setup tunnel between **NL** and **HQ**. Please refer the above VPN parameter table to setup the VPN gateway and connection as I don't list the detail configuration steps here,.

Configure the **NL** site address object for each remote office subnet

Address

Address Group

Configuration

#	Name	Type	Address	
1	HQ_SUBNET	SUBNET	192.168.100.0/24	
2	VPN_REMOTE_SUBNET	SUBNET	192.168.1.0/24	
3	DMZ_SUBNET	SUBNET	192.168.200.0/24	
4	VPN_visitor_pc	HOST	192.168.1.33	
5	Trainer_PC	HOST	10.59.1.18	
6	LAN_SUBNET	SUBNET	192.168.101.0/24	
7	DE_SUBNET	SUBNET	192.168.102.0/24	
8	CZ_SUBNET	SUBNET	192.168.103.0/24	
9	UK_SUBNET	SUBNET	192.168.104.0/24	
10	FR_SUBNET	SUBNET	192.168.105.0/24	
11	SE_SUBNET	SUBNET	192.168.106.0/24	
12	DK_SUBNET	SUBNET	192.168.107.0/24	



Setup NL site address group that includes all the remote office subnets; the address object group is used as a policy route destination criterion.

**Group Members**

Name: RemoteOfficeVPN

Description:

**Member List**

Available:

- === Object ===
- DMZ1\_SUBNET
- DMZ2\_SUBNET
- L2TP\_HOST
- L2TP\_IFACE
- L2TP\_POOL
- LAN\_SUBNET
- === Group ===

Member:

- === Object ===
- CZ\_SUBNET
- DE\_SUBNET
- DK\_SUBNET
- FR\_SUBNET
- HQ\_SUBNET
- SE\_SUBNET
- UK\_SUBNET
- === Group ===

OK Cancel

The screenshot below is the NL site VPN Gateway status page.

VPN Connection | **VPN Gateway** | Concentrator | SA Monitor

**Configuration**

Total Connection: 2 | 30 connection per page | Page: 1 of 1

#	Name	My address	Secure Gateway	VPN Connection	
1	Default_L2TP_VPN_GW	ge2	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection	
2	NL_HQ	ge2	10.59.1.1, 10.59.1.1	NL_HQ_tunnel	

Apply Reset

NL site VPN Connection status page

VPN Connection
VPN Gateway
Concentrator
SA Monitor

Global Setting

☐ Use Policy Route to control dynamic IPSec rules  
☐ Ignore "Don't Fragment" setting in packet header

Configuration

Total Connection:2
30 connection per page
Page: 1 of 1

#	Name	VPN Gateway	Encapsulation	Algorithm	Policy	
1	Default_L2TP_VPN_Connection	Default_L2TP_VPN_GW	TUNNEL	DES/SHA	LAN_SUBNET/LAN_SUBNET	
2	NL_HQ_tunnel	NL_HQ	TUNNEL	DES/SHA	LAN_SUBNET/HQ_SUBNET	

Apply
Reset

NL site policy route for VPN traffic, this policy route is used to indicate that the ZyWALL 1050 sends the packets to the VPN tunnel.

Policy Route
Static Route
RIP
OSPF

BWM Global Setting

☐ Enable BWM

Configuration

Total Connection:4
30 connection per page
Page: 1 of 1

#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM	
1	any	none	any	LAN_SUBNET	RemoteOfficeVPN	any	NL_HQ_tunnel	none	0	
2	any	none	ge1	LAN_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0	
3	any	none	ge4	DMZ1_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0	
4	any	none	ge5	DMZ2_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0	

Apply
Reset

### HQ VPN concentrator configuration steps:

Here are step by step instructions on how to setup the VPN **concentrator** in HQ to route all the remote sites' VPN traffic.

The amount of tunnels needed to be configured in HQ ZyWALL1050 is the amount of the remote sites.

This means that if we want HQ to route 5 remote sites VPN traffic, we need to configure 5 VPN tunnels from remote office to HQ.

For the HQ VPN tunnel setting, please refer to the table below.

Remote Office	HQ
WAN: 10.59.1.11	WAN: 10.59.1.10

~ WAN: 10.59.1.17 LAN: 192.168.101.0/24 ~ LAN: 192.168.119.0/24	LAN: 192.168.100.0/24
Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1	Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1
Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None	Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None

Setup the remote offices' subnets address objects for the further VPN configuring.

















Policy Route
Static Route
RIP
OSPF

BWM Global Setting

☐ Enable BWM

Configuration

Total Connection:4
30 connection per page
Page: 1 of 1

#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM	
1	any	none	any	LAN_SUBNET	RemoteOfficeVPN	any	NL_HQ_tunnel	none	0	   
2	any	none	ge1	LAN_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0	   
3	any	none	ge4	DMZ1_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0	   
4	any	none	ge5	DMZ2_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0	   




























Apply
Reset

Setup the HQ VPN Gateway for all the remote sites

VPN Connection **VPN Gateway** Concentrator SA Monitor

**Configuration**

Total Connection:9 30 connection per page Page: 1 of 1

#	Name	My address	Secure Gateway	VPN Connection	
1	Default_L2TP_VPN_GW	ge2	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection	  
2	NL_HQ	ge2	10.59.1.1, 10.59.1.1	NL_HQ_tunnel	  
3	HQ_NL	ge2	10.59.1.11, 10.58.1.11	HQ_NL_tunnel	  
4	HQ_DE	ge2	10.59.1.12, 10.58.1.12	HQ_DE_tunnel	  
5	HQ_CZ	ge2	10.59.1.13, 10.58.1.13	HQ_CZ_tunnel	  
6	HQ_UK	ge2	10.59.1.14, 10.58.1.14	HQ_UK_tunnel	  
7	HQ_FR	ge2	10.59.1.15, 10.58.1.15	HQ_FR_tunnel	  
8	HQ_SE	ge2	10.59.1.16, 10.58.1.16	HQ_SE_tunnel	  
9	HQ_DK	ge2	10.59.1.17, 10.58.1.17	HQ_DK_tunnel	  


Apply Reset

Setup the HQ VPN connection for all the remote sites

VPN Connection **VPN Gateway** Concentrator SA Monitor





































**Global Setting**

☐ Use Policy Route to control dynamic IPSec rules

☐ Ignore "Don't Fragment" setting in packet header 

**Configuration**

Total Connection:9 30 connection per page Page: 1 of 1

#	Name	VPN Gateway	Encapsulation	Algorithm	Policy	
1	Default_L2TP_VPN_Connection	Default_L2TP_VPN_GW	TUNNEL	DES/SHA	LAN_SUBNET/LAN_SUBNET	   
2	NL_HQ_tunnel	NL_HQ	TUNNEL	DES/SHA	LAN_SUBNET/HQ_SUBNET	   
3	HQ_NL_tunnel	HQ_NL	TUNNEL	DES/SHA	LAN_SUBNET/NL_SUBNET	   
4	HQ_DE_tunnel	HQ_DE	TUNNEL	DES/SHA	LAN_SUBNET/DE_SUBNET	   
5	HQ_CZ_tunnel	HQ_CZ	TUNNEL	DES/SHA	LAN_SUBNET/CZ_SUBNET	   
6	HQ_UK_tunnel	HQ_UK	TUNNEL	DES/SHA	LAN_SUBNET/UK_SUBNET	   
7	HQ_FR_tunnel	HQ_FR	TUNNEL	DES/SHA	LAN_SUBNET/FR_SUBNET	   
8	HQ_SE_tunnel	HQ_SE	TUNNEL	DES/SHA	LAN_SUBNET/SE_SUBNET	   
9	HQ_DK_tunnel	HQ_DK	TUNNEL	DES/SHA	LAN_SUBNET/DK_SUBNET	   

Apply Reset

The next step is the most important one. We need to build up a VPN concentrator and join all the remote sites' VPN traffic to it.

Switch to ZyWALL USG2000 > Configuration > Network > IPSec VPN > Concentrator and then click the add icon to add a new concentrator.















On the concentrator edit page, click the add icon to add VPN connection to this concentrator.

The VPN traffic can be routed by HQ once the VPN connection has been added to the

concentrator. If this tunnel is already included in the concentrator, user doesn't need to add any policy route to the VPN tunnel.

**Group Members**

Name
RemoteOfficeConcentrator

#	Member	
1	IPSEC / HQ_CZ_tunnel	 
2	IPSEC / HQ_DE_tunnel	 
3	IPSEC / HQ_DK_tunnel	 
4	IPSEC / HQ_FR_tunnel	 
5	IPSEC / HQ_NL_tunnel	 
6	IPSEC / HQ_SE_tunnel	 
7	IPSEC / HQ_UK_tunnel	 

OK
Cancel

Now after the VPN concentrator setup, all the remote VPN tunnels have been linked to the HQ concentrator and remote sites can reach other remote sites via HQ.

The VPN concentrator is designed to route the remote sites' VPN traffic. However, user still needs to setup the policy route for local subnet VPN traffic. For example, if we setup the VPN concentrator only for HQ and remote sites A & B, then the A subnet can connect to B subnet but HQ subnet can't connect to neither A nor B subnet.

Thus, this depends on how customers want to deploy their Global VPN network.

We can add the following policy route to allow the HQ subnet to connect with all the concentrator's remote subnets.









































**Policy Route**
Static Route
RIP
OSPF

**BWM Global Setting**

☐ Enable BWM

**Configuration**

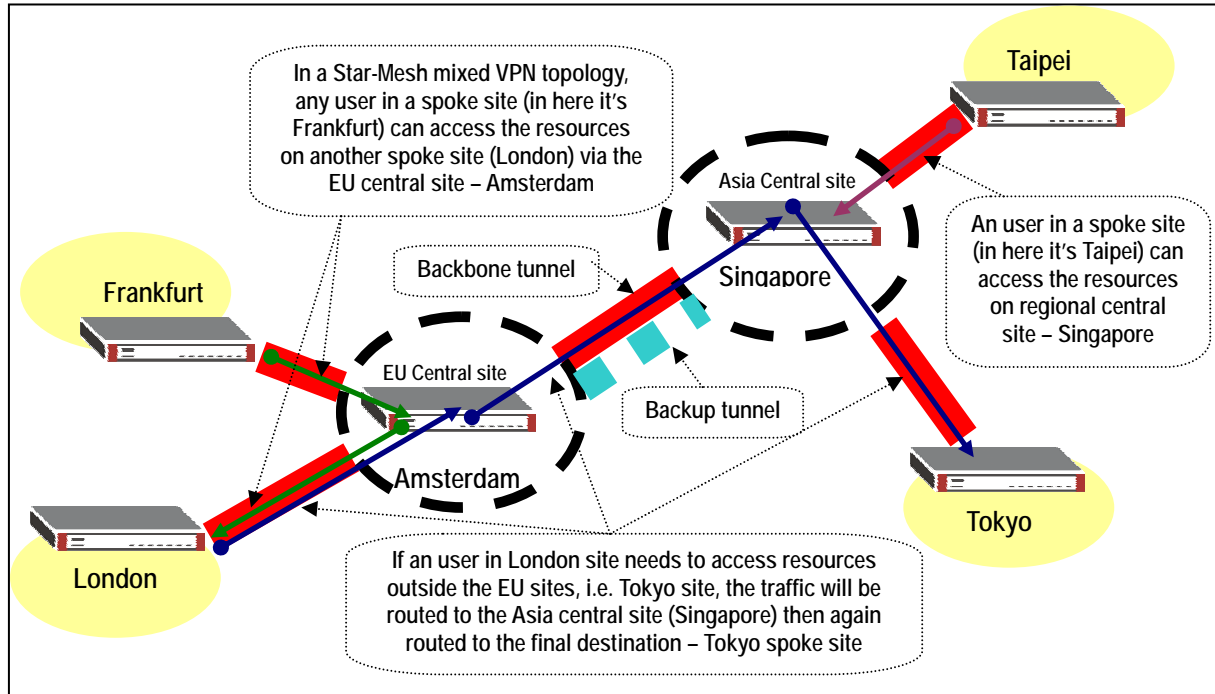
Total Connection:10
30 connection per page
Page: 1 of 1

#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM	
1	any	none	any	LAN_SUBNET	UK_SUBNET	any	HQ_UK_tunnel	none	0	   
2	any	none	any	LAN_SUBNET	NL_SUBNET	any	HQ_NL_tunnel	none	0	   
3	any	none	any	LAN_SUBNET	FR_SUBNET	any	HQ_FR_tunnel	none	0	   
4	any	none	any	LAN_SUBNET	CZ_SUBNET	any	HQ_CZ_tunnel	none	0	   
5	any	none	any	LAN_SUBNET	DE_SUBNET	any	HQ_DE_tunnel	none	0	   
6	any	none	any	LAN_SUBNET	SE_SUBNET	any	HQ_SE_tunnel	none	0	   
7	any	none	any	LAN_SUBNET	DK_SUBNET	any	HQ_DK_tunnel	none	0	   
8	any	none	ge1	LAN_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0	   
9	any	none	ge4	DMZ1_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0	   
10	any	none	ge5	DMZ2_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0	   

Apply
Reset

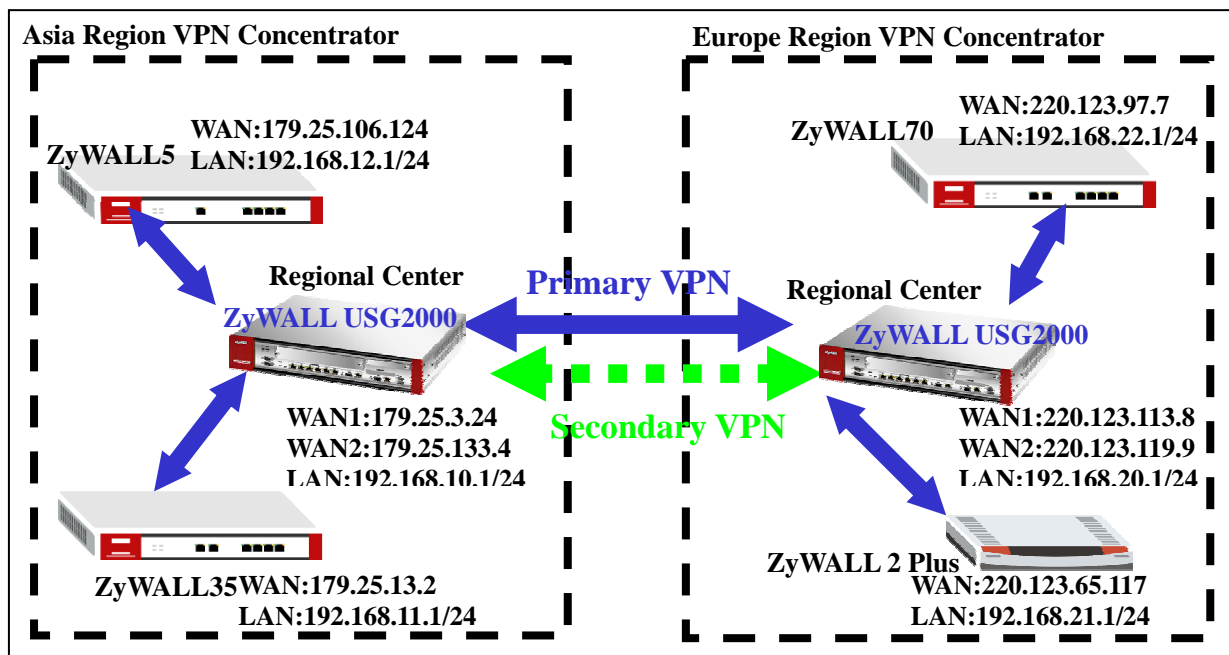


### 1.4.3 Star-Mesh Mixed Topology



In a Star-mesh mixed VPN topology, ZyWALL USG2000 acts as a regional central site (enabling Hub & Spoke VPN) and spoke sites can be any model of ZyWALL series. The Star – Mesh Mixed Topology is well suited for an enterprise having a regional operation center acting as a regional hub and spoke VPN network in the area. The connection between each regional operation center will be backbone VPN tunnel. To ensure the communication continuity, we can use VPN HA (secondary security gateway) to configure a backup VPN tunnel in case the primary VPN connection failure.

We use the below presented network topology to explain how to configure Star-Mesh Mixed Topology between all the ZyWALL series devices. The ZyWALL USG2000 act as a Regional Center devices whereas ZyWALL 2 Plus, 5, 35 and 70 are the regional remote sites' devices which are building VPN tunnel back to the Regional Center and provide connection with the other area remote nodes via the VPN tunnel between the two Regional Centers.



### Configuration Steps for Asia Region VPN Concentrator

ZyWALL5 and ZyWALL35 interface and VPN setting

Please configure the ZyWALL5 WAN and LAN interface as the topology diagram shown above. We can check the status page to confirm the correctness. Please refer to ZyWALL5 user guide for detail interface setting steps.

Network Status					
Interface	Status	IP Address	Subnet Mask	IP Assignment	Renew
WAN	100M/Full	179.25.106.124	255.255.0.0	Static	N/A
Dial Backup	Down	0.0.0.0	0.0.0.0	N/A	<input type="button" value="Dial"/>
<input checked="" type="checkbox"/> LAN	100M/Full	192.168.12.1	255.255.255.0	DHCP server	N/A
WLAN	Down	N/A	N/A	N/A	N/A
<input checked="" type="checkbox"/> DMZ	100M/Full	0.0.0.0	0.0.0.0	Static	N/A

### The VPN configuration parameters in Asia Region

Regional Remote Sites	Regional Center
ZyWALL5 WAN: 179.25.106.124 Local Policy: 192.168.12.0/24	WAN: 179.25.3.24 Local Policy: 192.168.0.0/16



Remote Policy: 192.168.0.0/16 ZyWALL35 WAN: 179.25.13.2 Local Policy: 192.168.11.0/24 Remote Policy: 192.168.0.0/16	Remote Policy: 192.168.12.0/16  Local Policy: 192.168.0.0/16  Remote Policy: 192.168.11.0/16
Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1	Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1
Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None	Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None

The next step is to configure the VPN tunnel setting. Following the ZyWALL5 VPN design logic, we have to define the local and remote policies to force the traffic going through the VPN tunnel to the remote site. For example, the traffic from ZyWALL5 will be sent to all the remote sites' devices like ZyWALL35 (LAN subnet: 192.168.11.x), local center's ZyWALL USG2000 (LAN subnet: 192.168.21.x), remote center's ZyWALL USG2000 (LAN subnet: 192.168.20.x), ZyWALL 2 Plus (LAN subnet: 192.168.21.x) and ZyWALL70 (LAN subnet: 192.168.22.x) by building one VPN tunnel with local center ZyWALL USG2000. Thus a separate VPN tunnel to each remote site is not needed. We will use a class B subnet (192.168.0.0/255.255.0.0) as remote policy in order to include all ranges of the remote policies requirements.

The Local Policy is the local subnet 192.168.12.0/24 and Remote Policy is 192.168.0.0/16 for the tunnel between ZyWALL5 and local center ZyWALL USG2000. Please switch to menu Security > VPN > Global Setting and activate the "VPN rules skip applying to the overlap range of local and remote IP addresses" option because the local and remote policies are in the overlap range in this application. If this feature is not activated, you will fail to access device because of triggering VPN tunnels.

**VPN**

**VPN Rules (IKE)   VPN Rules (Manual)   SA Monitor   Global Setting**

**IPSec Global Setting**

Output Idle Timer: 120 (120~3600 sec)

Input Idle Timer: 0 (30~3600 sec, 0 means timer disabled)

Gateway Domain Name Update Timer: 5 (2~60 min, 0 means timer disabled)

Adjust TCP Maximum Segment Size: Auto 0

☒ VPN rules skip applying to the overlap range of local and remote IP addresses.  
 (Warning: When this checkbox is not checked, you may not access device because of triggering VPN tunnels)

Apply   Reset

Based on the VPN configuration parameter table to finish the VPN tunnel configuration and the VPN status page will brief list the VPN tunnel information like following screen shot after the VPN setting. The VPN can't be dialed up for testing because the remote ZyWALL USG2000 didn't setup the corresponding VPN tunnel until now. The test and debug can start only after both sites' VPN setup is done. Please refer to the ZyWALL5 user guide for detail VPN setting steps.

**VPN**

**VPN Rules (IKE)   VPN Rules (Manual)   SA Monitor   Global Setting**

**VPN Rules**

Local Network — My ZyWALL — Internet VPN Tunnel — Remote Gateway — Remote Network

#	VPN Rules				
1	zw1050	179.25.106.124	179.25.3.24		
	zw1050VPN	192.168.12.1 / 255.255.255.0	192.168.0.0 / 255.255.0.0		

There are similar configuration steps for the ZyWALL35 interface and the VPN setup. The ZyWALL35 WAN and LAN interface are set as follow.

Network Status					
Interface	Status	IP Address	Subnet Mask	IP Assignment	Renew
WAN 1	100M/Full	179.25.13.2	255.255.0.0	Static	
WAN 2	Down	0.0.0.0	0.0.0.0	DHCP client	<a href="#">Renew</a>
Dial Backup	Down	0.0.0.0	0.0.0.0	N/A	<a href="#">Dial</a>
<a href="#">+</a> LAN	100M/Full	192.168.11.1	255.255.255.0	DHCP server	N/A
WLAN	Down	N/A	N/A	N/A	N/A
<a href="#">+</a> DMZ	100M/Full	0.0.0.0	0.0.0.0	Static	N/A

[Show Statistics](#)
[Show DHCP Table](#)
[VPN Status](#)

Please make sure to activate the “VPN rules skip applying to the overlap range of local and remote IP addresses” option before starting to setup the VPN tunnel.

VPN

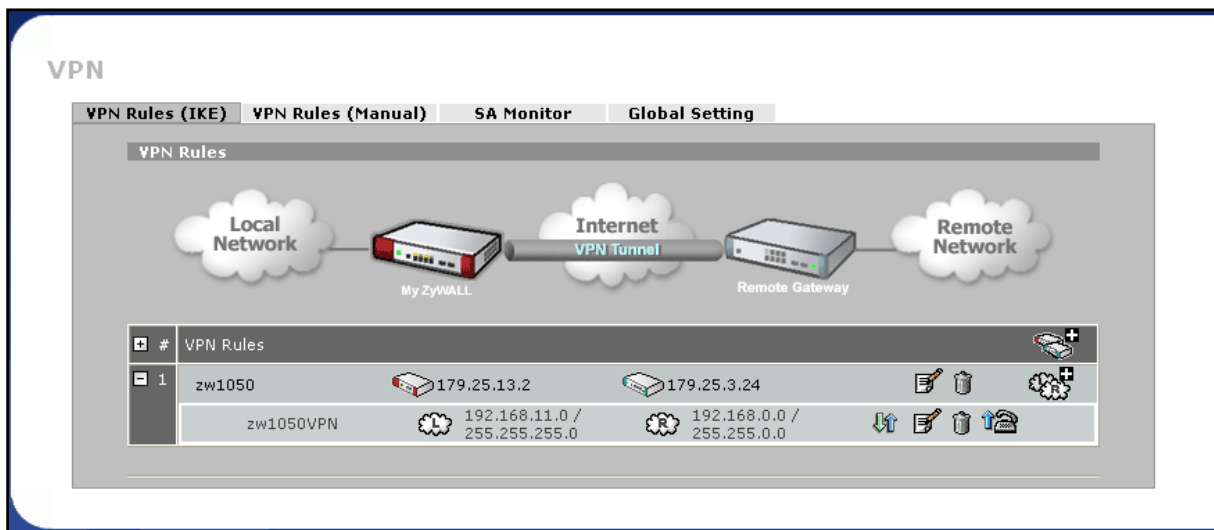
VPN Rules (IKE)
VPN Rules (Manual)
SA Monitor
Global Setting

IPSec Global Setting

Output Idle Timer: 120 (120~3600 sec)  
Input Idle Timer: 0 (30~3600 sec, 0 means timer disabled)  
Gateway Domain Name Update Timer: 5 (2~60 min, 0 means timer disabled)  
Adjust TCP Maximum Segment Size: Auto 0  
☒ VPN rules skip applying to the overlap range of local and remote IP addresses.  
(Warning: When this checkbox is not checked, you may not access device because of triggering VPN tunnels)

[Apply](#)
[Reset](#)

The VPN tunnel status page after configured the local center ZyWALL USG2000 tunnel.



As soon as we finish the configuration of ZyWALL5 and ZyWALL35, we can move to ZyWALL USG2000's configuration.

























Asia Regional Center ZyWALL USG2000 interface and VPN concentrator setting

**The VPN configuration parameter for Asia and Europe regional Center ZyWALL USG2000**

Asia Regional Center ZyWALL USG2000	Europe Regional Center ZyWALL USG2000
WAN1:179.25.3.24 WAN2:179.25.133.4 LAN:192.168.10.1/24	WAN1:220.123.113.8 WAN2:220.123.119.9 LAN:192.168.20.1/24
Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1	Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1
Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None	Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None

Please refer to the application topology to setup the ZyWALL USG2000 interface first. We can move to next steps only after setting up the interface. We use ge1 as LAN interface and IP

address is 192.168.10.1/255.255.255.0. The ge2 and ge3 are WAN1 and WAN2 interfaces and IP address are 179.25.3.24/255.255.0.0 and 179.25.133.4/255.255.0.0.

















Interface Summary		Ethernet	Port Grouping	VLAN	Bridge	PPPoE/PPTP	Auxiliary	Trunk
Configuration								
#	Name	IP Address	Mask	Modify				
1	ge1	STATIC -- 192.168.10.1	255.255.255.0	  				
2	ge2	STATIC -- 179.25.3.24	255.255.0.0	  				
3	ge3	STATIC -- 179.25.133.4	255.255.0.0	  				
4	ge4	STATIC -- 192.168.2.1	255.255.255.0	  				
5	ge5	STATIC -- 192.168.3.1	255.255.255.0	  				
6	ge6	STATIC -- 0.0.0.0	0.0.0.0	  				
7	ge7	STATIC -- 0.0.0.0	0.0.0.0	  				
8	ge8	STATIC -- 59.124.163.154	255.255.255.224	  				
<div><div>Apply</div><div>Reset</div></div>								

We have to pre-configure some address objects for the later VPN configuration requirements. The needed address objects list is as follows:

Address

Address Group

Configuration

#	Name	Type	Address	 
1	LAN_SUBNET	SUBNET	192.168.10.0/24	 
2	zw5VPN_LAN	SUBNET	192.168.12.0/24	 
3	Global_subnet	SUBNET	192.168.0.0/16	 
4	zw35VPN_LAN	SUBNET	192.168.11.0/24	 
5	remote_zw1050_LAN	SUBNET	192.168.20.0/24	 
6	AsiaRegion	RANGE	192.168.10.0-192.168.15.0	 
7	EuropeRegion	RANGE	192.168.20.0-192.168.25.0	 

The address object AsiaRegion (192.168.10.0 – 192.168.15.0) and EuropeRegion (192.168.20.0 – 192.168.25.0) are used for the two regional center VPN concentrators employed. When Asia region site like ZyWALL5 (192.168.12.0) tries to access the other region's remote site like ZyWALL70 (192.168.22.0) it will match these two addresses' object ranges and ZyWALL USG2000 can do next processing.

This ZyWALL USG2000 is the local center of Asia region. We need to setup the VPN tunnel between local sites ZyWALL5 and ZyWALL35 and Europe region center ZyWALL USG2000.

Follow the VPN parameter tables to setup the three VPN gateways (IKE / IPsec Phase1). For detail steps please refer to the ZyWALL USG2000 user guide. We have to configure a secondary security gateway for the VPN gateway between both of the regional centers' ZyWALL USG2000s. The VPN connection can fail over to secondary gateway in case the parameter gateway fails.

**General Settings**

VPN Gateway Name: usg2000

**Gateway Settings**

My Address: ☐ Interface: ge2 Static -- 179.25.3.24/255.255.0.0  
☐ Domain Name / IP

Peer Gateway Address: ☐ Static Address  
 1. 220.123.113.8  
 2. 220.123.119.9  
☐ Dynamic Address

**Authentication** [Advanced](#)

☒ Pre-Shared Key: default (See [My Certificates](#))  
☐ Certificate

**Phase 1 Settings** [Advanced](#)

SA Life Time: 86400 (180 - 3000000 Seconds)

[More Settings](#)

After configuration, there will be three VPN gateways listed in the VPN Gateway status page.

VPN Connection VPN Gateway Concentrator SA Monitor					
Configuration					
Total Connection:4		30 connection per page	Page: 1 of 1		
#	Name	My address	Secure Gateway	VPN Connection	
1	Default_L2TP_VPN_GW	ge2	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection	
2	zw5	ge2	179.25.106.124, 0.0.0.0	zw5VPN	
3	zw35	ge2	179.25.13.2, 0.0.0.0	zw35VPN	
4	usg2000	ge2	220.123.113.8, 220.123.119.9	usg2000VPN	
<div> <a href="#">Apply</a> <a href="#">Reset</a> </div>					

The next step is to create the VPN connection (IPSec / IPSec Phase2). Make sure the parameters are configured correctly, otherwise the VPN will fail to dial. Below is the VPN connection global page.

**VPN Connection** | VPN Gateway | Concentrator | SA Monitor

**Global Setting**

☐ Use Policy Route to control dynamic IPSec rules

☐ Ignore "Don't Fragment" setting in packet header

**Configuration**

Total Connection:4 | 30 connection per page | Page: 1 of 1

#	Name	VPN Gateway	Encapsulation	Algorithm	Policy	Icons
1	Default_L2TP_VPN_Connection	Default_L2TP_VPN_GW	TUNNEL	DES/SHA	LAN_SUBNET/LAN_SUBNET	[Icons]
2	zw5VPN	zw5	TUNNEL	DES/SHA	Global_subnet/zw5VPN_LAN	[Icons]
3	zw35VPN	zw35	TUNNEL	DES/SHA	Global_subnet/zw35VPN_LAN	[Icons]
4	usg2000VPN	usg2000	TUNNEL	DES/SHA	AsiaRegion/EuropeRegion	[Icons]

Apply Reset

Now, we have already successfully added three VPN connection rules and we can start to edit our regional VPN concentrator. Switch to Concentrator sub menu and click the Add icon to add a new concentrator.

**VPN Connection** | VPN Gateway | **Concentrator** | SA Monitor

**Configuration**

Name

[Add Icon]

Give a name to this concentrator and then click add icon to make the existing VPN connection become a member of this concentrator.

**Group Members**

Name 1. AsiaRegion

#	Member	
1	IPSEC / usg2000VPN	<span style="border: 1px solid red; padding: 2px;">2. +</span>
2	IPSEC / zw35VPN	
3	IPSEC / zw5VPN	

3. OK Cancel

The remote regional center ZyWALL USG2000 VPN connection is also treated as a member of this concentrator and the packets will be sent to the remote center first and then following the remote concentrator setting will be routed to the destination sites where the traffic destination is the site allocated under remote VPN concentrator.

We had finished all settings of the Asia Region VPN concentrator. Now you can test the local VPN concentrator link. Later on, we can test the connection of both concentrators. This will be after we setup the Europe Region VPN concentrator.

### Configuration Steps for Europe Region VPN Concentrator

ZyWALL 2 Plus and ZyWALL70 interface and VPN setting

ZyWALL 2 Plus WAN and LAN interface setting

**Network Status**

Interface	Status	IP Address	Subnet Mask	IP Assignment	Renew
WAN	100M/Full	220.123.65.117	255.255.0.0	Static	N/A
Dial Backup	Down	0.0.0.0	0.0.0.0	N/A	<span style="border: 1px solid gray; padding: 2px;">Dial</span>
<span style="border: 1px solid gray; padding: 2px;">+</span> LAN	100M/Full	192.168.21.1	255.255.255.0	DHCP server	N/A

Show Statistics
Show DHCP Table
VPN Status

### The VPN configuration parameters in Europe Region

Regional Remote Sites	Regional Center
ZyWALL 2 Plus WAN: 220.123.65.117 Local Policy: 192.168.21.0/24 Remote Policy: 192.168.0.0/16	WAN: 220.123.113.8 Local Policy: 192.168.0.0/16  Remote Policy: 192.168.21.0/16



ZyWALL70 WAN: 220.123.97.7 Local Policy: 192.168.22.0/24 Remote Policy: 192.168.0.0/16	Local Policy: 192.168.0.0/16 Remote Policy: 192.168.22.0/16
Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1	Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1
Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None	Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None

Remember to activate “VPN rules skip applying to the overlap range of local and remote IP addresses” option before configuring the VPN tunnel.

VPN

VPN Rules (IKE) | VPN Rules (Manual) | SA Monitor | Global Setting

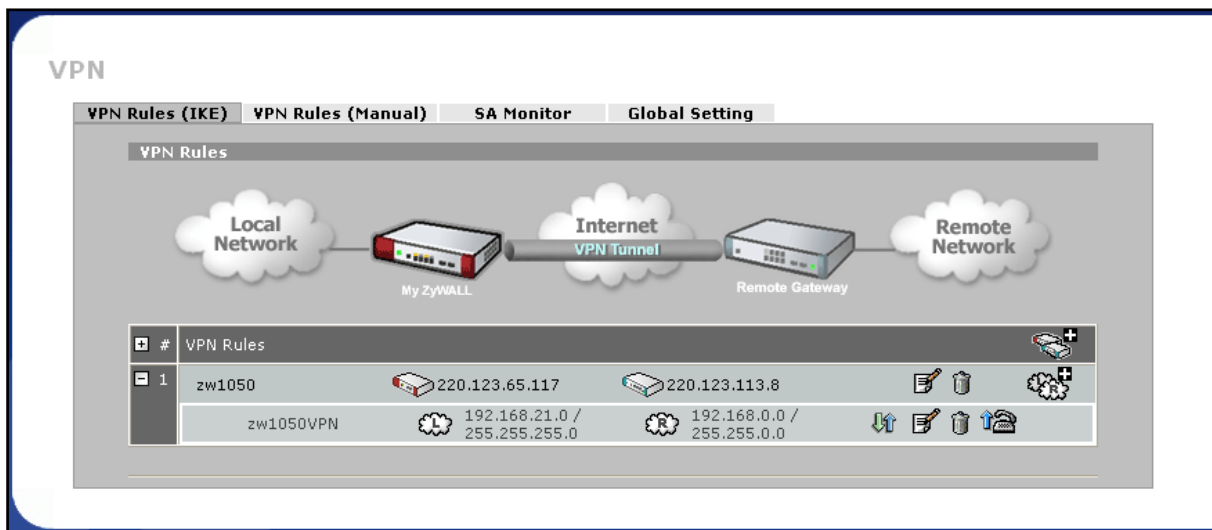
IPSec Global Setting

Output Idle Timer 120 (120~3600 sec)  
Input Idle Timer 0 (30~3600 sec, 0 means timer disabled)  
Gateway Domain Name Update Timer 5 (2~60 min, 0 means timer disabled)  
Adjust TCP Maximum Segment Size Auto 0

☒ VPN rules skip applying to the overlap range of local and remote IP addresses.  
(Warning: When this checkbox is not checked, you may not access device because of triggering VPN tunnels)

Apply Reset

Follow the VPN parameter table to configure the VPN tunnel.

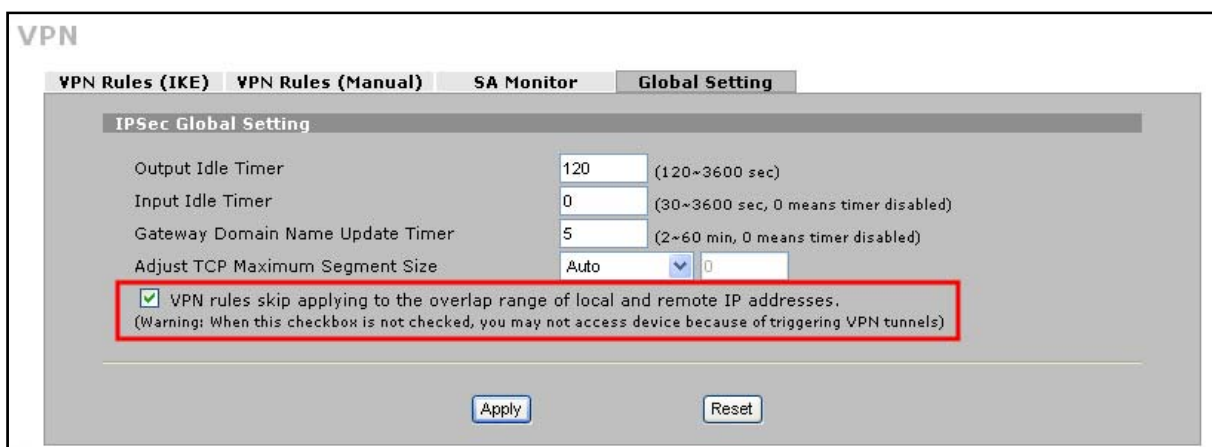


ZyWALL70 WAN and LAN interface setting.

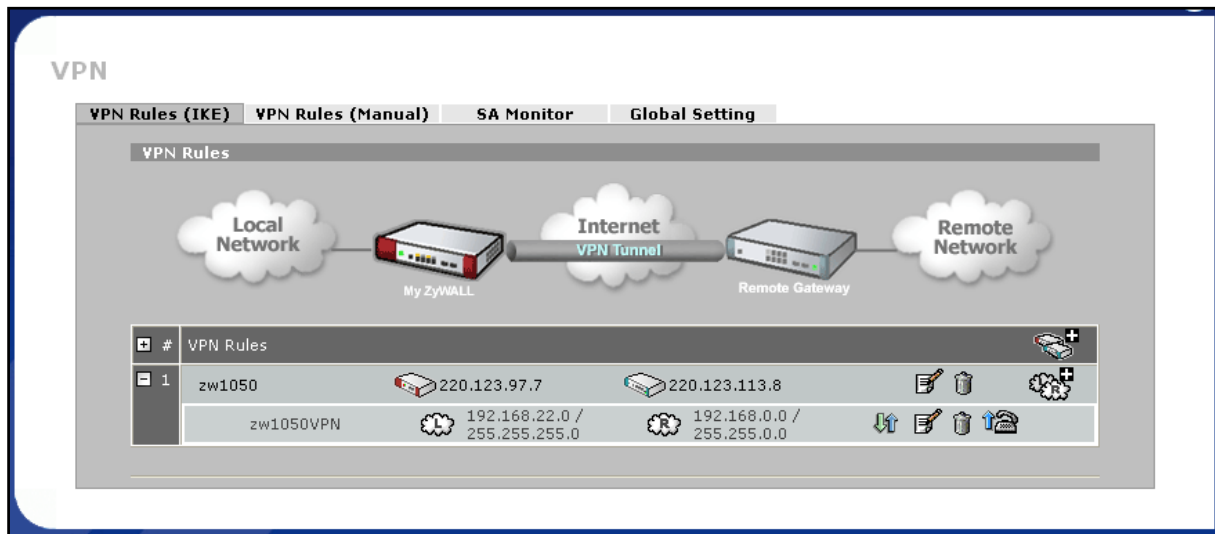
Network Status					
Interface	Status	IP Address	Subnet Mask	IP Assignment	Renew
WAN 1	100M/Full	220.123.97.7	255.255.0.0	Static	
WAN 2	Down	0.0.0.0	0.0.0.0	DHCP client	<button>Renew</button>
Dial Backup	Down	0.0.0.0	0.0.0.0	N/A	<button>Dial</button>
<b>+</b> LAN	100M/Full	192.168.22.1	255.255.255.0	DHCP server	N/A
WLAN	Down	N/A	N/A	N/A	N/A
<b>+</b> DMZ	100M/Full	0.0.0.0	0.0.0.0	Static	N/A

Show Statistics
Show DHCP Table
VPN Status

Remember to activate “VPN rules skip applying to the overlap range of local and remote IP addresses” option before configuring the VPN tunnel.



Follow the VPN parameter table to configure the VPN tunnel.



After we finish the configuration of ZyWALL 2 Plus and ZyWALL70, we can move to ZyWALL USG2000's configuration.

Europe Regional Center ZyWALL USG2000 interface and VPN concentrator setting

**The VPN configuration parameter for Asia and Europe regional Center ZyWALL USG2000**

Asia Regional Center ZyAWLL USG2000	Europe Regional Center ZyAWLL USG2000
WAN1:179.25.3.24 WAN2:179.25.133.4 LAN:192.168.10.1/24	WAN1:220.123.113.8 WAN2:220.123.119.9 LAN:192.168.20.1/24
Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1	Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1
Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None	Phase2 Encapsulation: Tunnel Active Protocol: ESP Encryption: DES Authentication: SHA1 Perfect Forward Secrecy (PFS): None

Please refer to the application topology to setup the ZyWALL USG2000 interface first. Then we can move to setting the VPN.

#	Name	IP Address	Mask	Modify
1	ge1	STATIC -- 192.168.20.1	255.255.255.0	
2	ge2	STATIC -- 220.123.113.8	255.255.0.0	
3	ge3	STATIC -- 220.123.119.9	255.255.0.0	
4	ge4	STATIC -- 192.168.2.1	255.255.255.0	
5	ge5	STATIC -- 192.168.3.1	255.255.255.0	
6	ge6	STATIC -- 0.0.0.0	0.0.0.0	
7	ge7	STATIC -- 0.0.0.0	0.0.0.0	
8	ge8	STATIC -- 59.124.163.154	255.255.255.224	

We have to pre-configure some address objects for the later VPN configuration requirements. The needed address objects list is as follows.

#	Name	Type	Address	
1	LAN_SUBNET	SUBNET	192.168.20.0/24	
2	zw70VPN_LAN	SUBNET	192.168.22.0/24	
3	zw2PlusVPN_LAN	SUBNET	192.168.21.0/24	
4	Global_subnet	SUBNET	192.168.0.0/16	
5	remote_zw1050_LAN	SUBNET	192.168.10.0/24	
6	EuropeRegion	RANGE	192.168.20.0-192.168.25.0	
7	AsiaRegion	RANGE	192.168.10.0-192.168.15.0	

This ZyWALL USG2000 is the local center of Europe region. We need to setup the VPN tunnel between local sites ZyWALL 2 Plus and ZyWALL70 and Asia region center ZyWALL USG2000. Follow the VPN parameter tables to setup the three VPN gateways (IKE / IPSec Phase1). We have to configure a secondary security gateway for the VPN gateway between both regional centers' ZyWALL USG2000s.

General Settings

VPN Gateway Name

usg2000

Gateway Settings

My Address

☒ Interface

ge2

Static -- 220.123.113.8/255.255.0.0

☐ Domain Name / IP

Peer Gateway Address

☒ Static Address

1. 179.25.3.24  
2. 179.25.133.4

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

12345678

☐ Certificate

default

(See [My Certificates](#))

Phase 1 Settings













SA Life Time

86400

(180 - 3000000 Seconds)

More Settings

After configuration, there will be three VPN gateways listed in the VPN Gateway status page.

VPN Connection VPN Gateway Concentrator SA Monitor					
Configuration					
Total Connection:4		30	connection per page		Page: 1 of 1
#	Name	My address	Secure Gateway	VPN Connection	
1	Default_L2TP_VPN_GW	ge2	0.0.0.0, 0.0.0.0	Default_L2TP_VPN_Connection	  
2	usg2000	ge2	179.25.3.24, 179.25.133.4	usg2000VPN	  
3	zw2Plus	ge2	220.123.65.117, 0.0.0.0	zw2PlusVPN	  
4	zw70	ge2	220.123.97.7, 0.0.0.0	zy70VPN	  
<div>Apply</div> <div>Reset</div>					

The next step is to create the VPN connection (IPSec / IPSec Phase2). Make sure the parameters are correctly configured; otherwise the VPN will fail to dial. Below is the VPN connection global page.

**VPN Connection** | VPN Gateway | Concentrator | SA Monitor

**Global Setting**

☐ Use Policy Route to control dynamic IPSec rules

☐ Ignore "Don't Fragment" setting in packet header

**Configuration**

Total Connection: 4 | 30 connection per page | Page: 1 of 1

#	Name	VPN Gateway	Encapsulation	Algorithm	Policy	Icons
1	Default_L2TP_VPN_Connection	Default_L2TP_VPN_GW	TUNNEL	DES/SHA	LAN_SUBNET/LAN_SUBNET	[Icons]
2	usg2000VPN	usg2000	TUNNEL	DES/SHA	AsiaRegion/EuropeRegion	[Icons]
3	zw2PlusVPN	zw2Plus	TUNNEL	DES/SHA	Global_subnet/zw2PlusVPN_LAN	[Icons]
4	zy70VPN	zw70	TUNNEL	DES/SHA	Global_subnet/zw70VPN_LAN	[Icons]

Apply Reset

Now, we already successfully added the three VPN connection rules and we can start to edit our regional VPN concentrator. Switch to the Concentrator sub menu and click the Add icon to add a new concentrator.

**VPN Connection** | **VPN Gateway** | **Concentrator** | SA Monitor

**Configuration**

Name	Icons
	[Add Icon]

Assign a name to this concentrator and then click the add icon to make the existing VPN become the member of this concentrator.

**Group Members**

Name: 1 EuropeRegion

#	Member	Icons
1	IPSEC / usg2000VPN	[Icons]
2	IPSEC / zw2PlusVPN	[Icons]
3	IPSEC / zy70VPN	[Icons]

2 [Add Icon]

3 OK Cancel

The remote regional center ZyWALL USG2000 VPN connection is also treated as a member of this concentrator and the packets will be sent to the remote center first and then

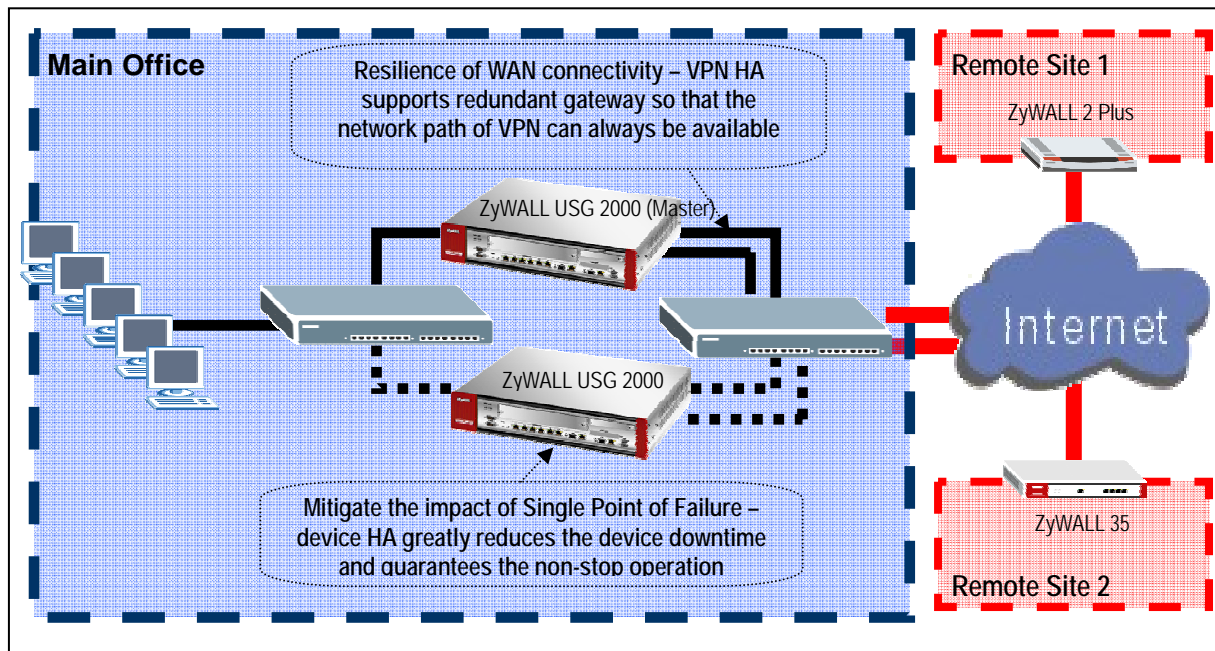
following the remote concentrator setting will be routed to the destination sites where the traffic destination is the site allocated under remote VPN concentrator.

We have finished all the Star-Mesh Mixed VPN topology setting. Now you can test the local VPN concentrator link. Also, you can try the connection between both concentrators' site.

## 1.5 Device HA

In the Global or multi-site Enterprise network deployment, reliability is another major concern while planning a VPN deployment.

**ZyWALL USG 2000 provides advanced features to support the following scenarios to achieve high availability of the VPN infrastructure.**



The benefits for the customer are:

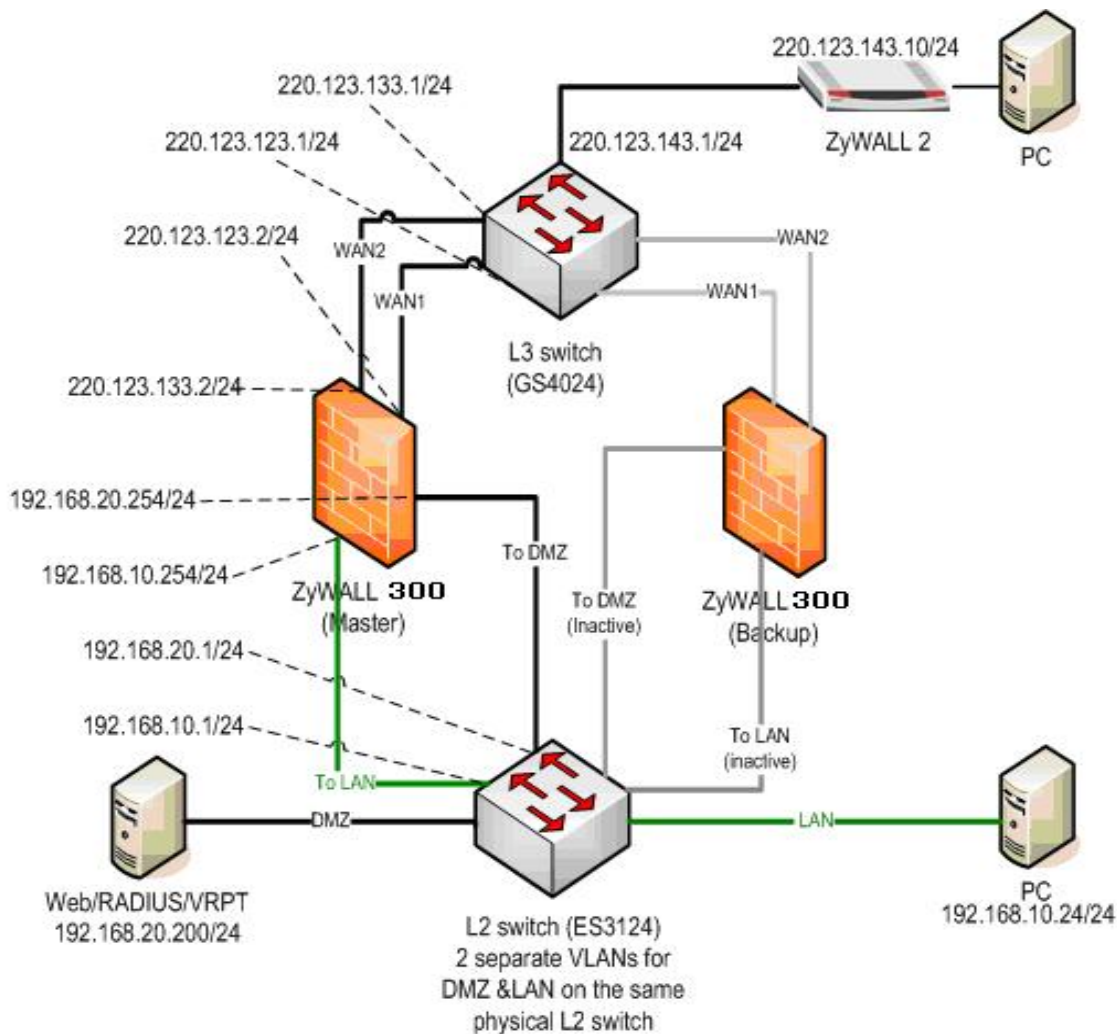
- Dealing with the impact of unreliable WAN connectivity
- Mitigates the impact of Single Point of Failure

Below is the Application topology. The L3 switch is configured to three VLANs to simulate the internet environment, and the traffic can be routed between each VLAN.



### 1.5.1 Device HA

Here is the example, we are going to demonstrate the device high available provided by ZyWALL USG 2000.



#### 1.5.1.1 Configuration procedure

- **Setup Master ZyWALL USG 2000 and the configuration will auto sync with Backup ZyWALL USG 2000 via the device HA setting.**
- **Configure the interface to correspond Zone**
- **Setup the routing**
- **Setup Device HA (Activate-Passive)**

## Steps:

Setup Master ZyWALL USG 2000 and the configuration will auto sync with Backup ZyWALL USG 2000 via the device HA setting.

### 1. Interface setup

The default LAN subnet is combined with ge1 and default IP is 192.168.1.1. Please connect to LAN port and ZyWALL USG 2000 will dispatch an IP for your PC. Then we can start to setup the basic interface and routing setting.

Step1. Login to device and check the device status

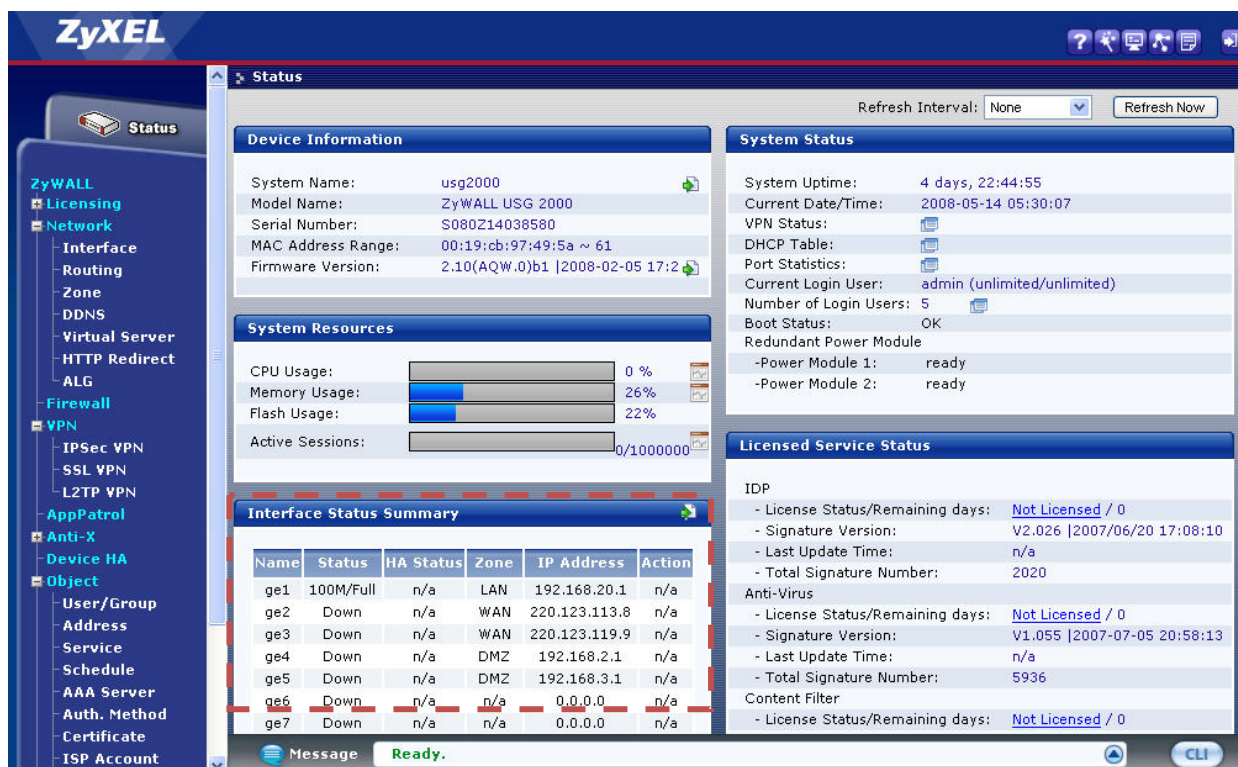
The screenshot shows the ZyWALL USG 2000 web management interface. The left sidebar contains a navigation menu with options like Status, Licensing, Network, Interface, Routing, Zone, DDNS, Virtual Server, HTTP Redirect, ALG, Firewall, VPN, AppPatrol, Anti-X, Device HA, and Object. The main content area is titled 'Status' and includes several sections:

- Device Information:**
  - System Name: usg2000
  - Model Name: ZyWALL USG 2000
  - Serial Number: S080Z14038580
  - MAC Address Range: 00:19:cb:97:49:5a ~ 61
  - Firmware Version: 2.10(AQW.0)b1 | 2008-02-05 17:2
- System Resources:**
  - CPU Usage: 0 %
  - Memory Usage: 26 %
  - Flash Usage: 22 %
  - Active Sessions: 0/1000000
- Interface Status Summary:**

Name	Status	HA Status	Zone	IP Address	Action
ge1	100M/Full	n/a	LAN	192.168.20.1	n/a
ge2	Down	n/a	WAN	220.123.113.8	n/a
ge3	Down	n/a	WAN	220.123.119.9	n/a
ge4	Down	n/a	DMZ	192.168.2.1	n/a
ge5	Down	n/a	DMZ	192.168.3.1	n/a
ge6	Down	n/a	n/a	0.0.0.0	n/a
ge7	Down	n/a	n/a	0.0.0.0	n/a
- System Status:**
  - System Uptime: 4 days, 22:44:55
  - Current Date/Time: 2008-05-14 05:30:07
  - VPN Status: [Icon]
  - DHCP Table: [Icon]
  - Port Statistics: [Icon]
  - Current Login User: admin (unlimited/unlimited)
  - Number of Login Users: 5
  - Boot Status: OK
  - Redundant Power Module:
    - Power Module 1: ready
    - Power Module 2: ready
- Licensed Service Status:**
  - IDP:
    - License Status/Remaining days: Not Licensed / 0
    - Signature Version: V2.026 | 2007/06/20 17:08:10
    - Last Update Time: n/a
    - Total Signature Number: 2020
  - Anti-Virus:
    - License Status/Remaining days: Not Licensed / 0
    - Signature Version: V1.055 | 2007-07-05 20:58:13
    - Last Update Time: n/a
    - Total Signature Number: 5936
  - Content Filter:
    - License Status/Remaining days: Not Licensed / 0

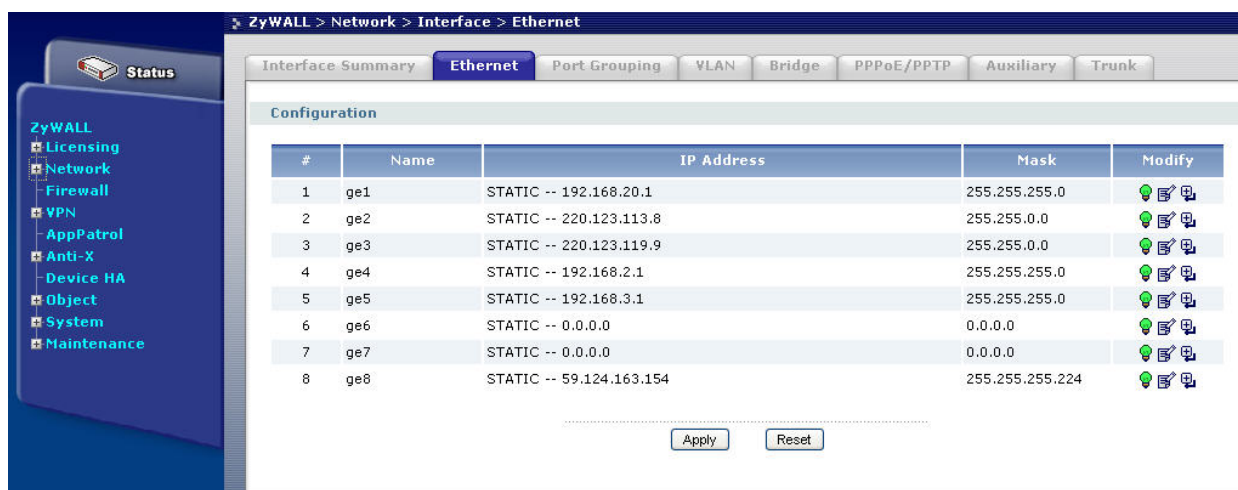
At the bottom, there is a 'Message' box showing 'Ready.' and a 'CLI' button.

Step2. We can check all the interface information on the Status display page.



Step3. Setup ge2 as WAN1, ge3 as WAN2, ge1 as LAN, ge4 as DMZ interface and the IP parameters as in the demo topology.

The default interface configuration is as follows. We will configure ge2, ge3, ge1 and ge4 in turn. User needs to click the “Edit” icon to modify the setting.



Step 3.1: ge2(WAN1 interface) Fix IP: 220.123.123.2/255.255.255.0 Gateway: 220.123.123.1( ZyWALL > Network > Interface > Edit > ge2)

**ZyWALL > Network > Interface > Edit > ge2**

---

**Interface Properties**

☒ Enable Interface

Interface Name: ge2

MAC Address: 00:19:CB:97:49:5B

Description:  (Optional)

---

**IP Address Assignment**

☐ Get Automatically

☒ Use Fixed IP Address

IP Address: 220.123.123.2

Subnet Mask: 255.255.255.0

Gateway: 220.123.123.1 (Optional)

Metric: 0 (0-15)

---

**Interface Parameters**

Upstream Bandwidth: 1048576 Kbps

Downstream Bandwidth: 1048576 Kbps

MTU: 1500 Bytes

---

**RIP Setting**

☐ Enable RIP

Direction: BiDir

Step 3.2: ge3(WAN2 interface) Fix IP: 220.123.133.2/255.255.255.0 Gateway: 220.123.133.1(ZyWALL > Network > Interface > Edit > ge3)

**ZyWALL > Network > Interface > Edit > ge3**

---

**Interface Properties**

☒ Enable Interface

Interface Name: ge3

MAC Address: 00:19:CB:97:49:5C

Description:  (Optional)

---

**IP Address Assignment**

☐ Get Automatically

☒ Use Fixed IP Address

IP Address: 220.123.133.2

Subnet Mask: 255.255.255.0

Gateway: 220.123.133.1 (Optional)

Metric: 0 (0-15)

---

**Interface Parameters**

Upstream Bandwidth: 1048576 Kbps

Downstream Bandwidth: 1048576 Kbps

MTU: 1500 Bytes

---

**RIP Setting**

☐ Enable RIP

Direction: BiDir

Step 3.3: ge4(DMZ interface) Fix IP: 192.168.20.254/255.255.255.0 DHCP server (ZyWALL > Network > Interface > Edit > ge4)

**ZyWALL > Network > Interface > Edit > ge4**

Interface Properties	
<input checked="" type="checkbox"/> Enable Interface	
Interface Name	ge4
MAC Address	00:19:CB:97:49:5D
Description	<input type="text"/> (Optional)

IP Address Assignment	
<input type="radio"/> Get Automatically	<input type="text"/>
<input checked="" type="radio"/> Use Fixed IP Address	
IP Address	192.168.20.254
Subnet Mask	255.255.255.0
Gateway	<input type="text"/> (Optional)
Metric	0 (0-15)

Interface Parameters	
Upstream Bandwidth	1048576 Kbps
Downstream Bandwidth	1048576 Kbps
MTU	1500 Bytes

RIP Setting	
<input type="checkbox"/> Enable RIP	
Direction	BiDir

Step 3.4: ge1(LAN1 interface) Fix IP: 192.168.10.254/255.255.255.0 DHCP server (ZyWALL > Network > Interface > Edit > ge1)

**ZyWALL > Network > Interface > Edit > ge1**

---

**Interface Properties**

☒ Enable Interface

Interface Name: **ge1**

MAC Address: **00:19:CB:97:49:5A**

Description:  (Optional)

---

**IP Address Assignment**

☐ Get Automatically

☒ Use Fixed IP Address

IP Address: **192.168.10.254**

Subnet Mask: **255.255.255.0**

Gateway:  (Optional)

Metric: **0** (0-15)

---

**Interface Parameters**

Upstream Bandwidth: **1048576** Kbps

Downstream Bandwidth: **1048576** Kbps

MTU: **1500** Bytes

---

**RIP Setting**

☐ Enable RIP

Direction: **Bidir**

User's pc network connection will disconnect and get the new IP address from ZyWALL USG 2000 after applying the ge1's new setting.







### Configure the interface to correspond Zone

Step1. Switch to ZyWALL > Network > Zone and click the "Edit" icon to modify the setting.

**ZyWALL > Network > Zone**

---

**Configuration**

Name	Block Intra-zone	Member	
LAN	No	ge1	 
WAN	Yes	ge2, ge3	 
DMZ	Yes	ge4, ge5	 

Step2. The default setting of ZyWALL is having three Zones. User can add more Zones or modify the Zone's name if they wish. The main purpose of Zone is to add the security checking between different interfaces. The default interface for LAN zone is binding with ge1, WAN zone is binding with ge2 and ge3, DMZ zone is ge4 and ge5.

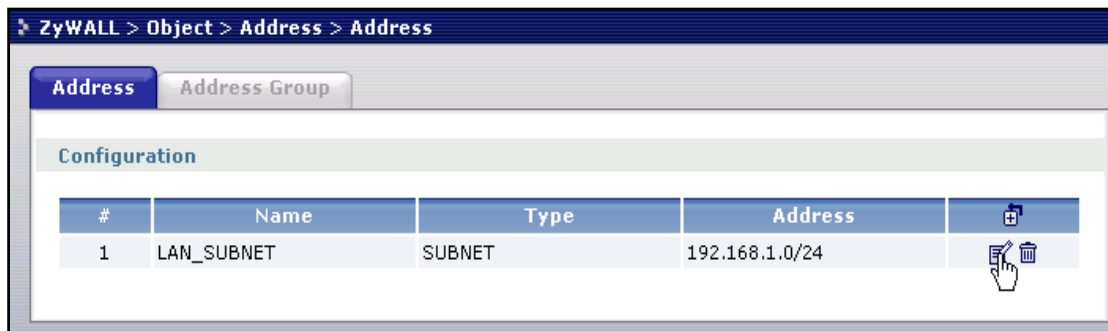
Step3. Check the interface summary page to confirm the settings. (**ZyWALL > Network > Interface > Interface Summary**)



## Setup the routing

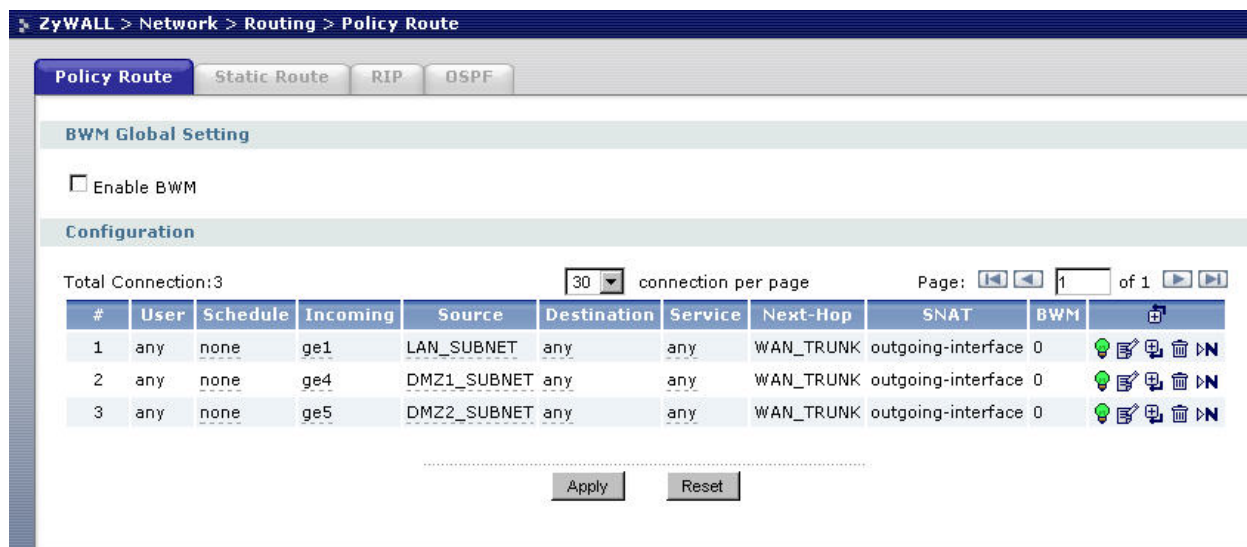
The routing source and destination address options will auto-grant from address object. The policy or static route can't be correctly setup until the corresponding address object is not configured.

Step1. Switch to **ZyWALL > Object > Address > Address** and you will find there exists default LAN\_SUBNET address object.



Step.2 ZyWALL will automatically route the traffic between all connected interfaces. There are default policy routes for LAN and DMZ zone traffic going out to the network behind WAN.

Switch to **ZyWALL > Network > Routing > Policy Route or Static Route** to check the routing settings.



User can click the “Edit” icon to check the detail settings

**ZyWALL > Network > Routing > Policy Route > Edit > #1**

---

**Configuration**

☒ Enable  
 Description  (Optional)

**Criteria**

User   
 Incoming    
 Source Address   
 Destination Address   
 Schedule   
 Service

**Next-Hop**

Type   
 Trunk

**Address Translation**

Source Network Address Translation

Port Triggering

#	Incoming Service	Trigger Service

**Bandwidth Shaping**

Step4. After applying all the routing settings, the PC in ZyWALL LAN subnet can communicate with the ZyWALL 2.

```

C:\CAWINDOWS\system32\cmd.exe

C:\>ping 220.123.143.10

Pinging 220.123.143.10 with 32 bytes of data:

Reply from 220.123.143.10: bytes=32 time=9ms TTL=252
Reply from 220.123.143.10: bytes=32 time=2ms TTL=252
Reply from 220.123.143.10: bytes=32 time=2ms TTL=252
Reply from 220.123.143.10: bytes=32 time=3ms TTL=252

Ping statistics for 220.123.143.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 9ms, Average = 4ms

C:\>
  
```

### Setup Device HA (Activate-Passive)

We will configure the Device HA setting on master ZyWALL USG 2000 first. Then we can connect the Backup ZyWALL cables to L3 and L2 switch and then synchronize the configuration from Master. The Device HA will be ready after this and Backup ZyWALL



would take over when Master ZyWALL fails.

Step1. Navigate to **ZyWALL > Device HA > General**. Check the “Enable Device HA.”

**ZyWALL > Device HA > General**

**General** | Active-Passive Mode | Legacy Mode

**General Settings**

☒ Enable Device HA

Device HA Mode: Active-Passive Mode ([Switch to Legacy Mode page](#))

**Monitored Interface Summary**

Interface	Virtual Router IP / Netmask	Management IP / Netmask	Link Status	HA Status

Apply Reset

Secondly, click the “add” icon to add a new VRRP GROUP in **ZyWALL > Device HA > Active-Passive Mode**.

**ZyWALL > Device HA > Active-Passive Mode**

**General** | **Active-Passive Mode** | Legacy Mode

**General Settings**

Device Role: ☒ Master ☐ Backup

**Cluster Settings** [Advanced](#)

Cluster ID:  (1-16)

**Monitored Interface Summary**

Interface	Virtual Router IP/Netmask	Management IP/Netmask	Link Status	Modify
ge1	192.168.10.254 / 255.255.255.0	/	Up	
ge2	220.123.123.2 / 255.255.255.0	/	Down	
ge3	220.123.133.2 / 255.255.255.0	/	Down	
ge4	192.168.20.254 / 255.255.255.0	/	Up	
ge5	192.168.3.1 / 255.255.255.0	/	Down	
ge6	/	/	Down	
ge7	/	/	Down	
ge8	59.124.163.154 / 255.255.255.224	/	Up	

**Synchronization**

Server Address: 192.168.10.254, 220.123.123.2, 220.123.133.2, 192.168.20.254, 192.168.3.1, 59.124.163.154

Server Port: 21 ([Configure](#))

Password:

Remark: With the latest design in ZLD 2.0x, when one of the VRRP interface’s link in the master ZyWALL is down, the Device HA status of the failed interface will remain “*active*” but Device HA status of the reset of not-failed interface will turn into “*fault*”. This design will

guarantees the backup ZyWALL can correctly detect the failure event from the master ZyWALL.

As for setting group of HA, you can refer to use guide to do detailed configuration to build LAN HA, WAN1 HA group, WAN2 HA group, DMZ HA group.

Step2. Connect the PC to Backup ZyWALL USG 2000 ge1 and the PC should be dispatched an IP address from the device. User can login to the Backup ZyWALL USG 2000 and configure the Backup Device HA setting. We have to set the ge1 interface IP setting as Master ge1 IP address. Then we can setup the Backup ZyWALL USG 2000 management IP address in the same LAN subnet.

The screenshot displays the 'ZyWALL > Network > Interface > Edit > ge1' configuration page. It is divided into four main sections:

- Interface Properties:** Includes a checked 'Enable Interface' box. The 'Interface Name' is 'ge1', the 'MAC Address' is '00:19:CB:97:49:5A', and there is an empty 'Description' field with '(Optional)' text.
- IP Address Assignment:** Features two radio buttons: 'Get Automatically' (unchecked) and 'Use Fixed IP Address' (checked). Under 'Use Fixed IP Address', there are input fields for 'IP Address' (192.168.10.254), 'Subnet Mask' (255.255.255.0), 'Gateway' (empty, with '(Optional)' text), and 'Metric' (0, with '(0-15)' text).
- Interface Parameters:** Contains input fields for 'Upstream Bandwidth' (1048576 Kbps), 'Downstream Bandwidth' (1048576 Kbps), and 'MTU' (1500 Bytes).
- RIP Setting:** Includes an unchecked 'Enable RIP' box and a 'Direction' dropdown menu currently set to 'BiDir'.

Step3. PC will get a new IP address after updating the lan1 interface setting. Login to the Backup ZyWALL and navigate to active the Device HA in **ZyWALL > Device HA > General**. Afterwards, click on “add” to create a **Backup Device HA** group in **ZyWALL > Device HA > Active-Passive Mode**. The detail parameter should be referred to the topology.

General
Active-Passive Mode
Legacy Mode

**General Settings**

Device Role
☐ Master
☒ Backup
Priority
 (1-254)
☐ Enable Preemption

**Cluster Settings**

Cluster ID
 (1-16)

**Monitored Interface Summary**

Interface	Virtual Router IP/Netmask	Management IP/Netmask	Link Status	Modify
ge1	192.168.10.254 / 255.255.255.0	/	Up	
ge2	220.123.123.2 / 255.255.255.0	/	Down	
ge3	220.123.133.2 / 255.255.255.0	/	Down	
ge4	192.168.20.254 / 255.255.255.0	/	Up	
ge5	192.168.4.1 / 255.255.255.0	/	Down	
ge6	/	/	Down	
ge7	/	/	Down	
ge8	59.124.163.154 / 255.255.255.224	/	Up	

**Synchronization**
Server Address
 (IP or FQDN)
Server Port

Between Master and Backup Role, the difference in settings is the Management IP configuration. The Backup ZyWALL will copy all the settings from the Master Device so we need a management IP to access and configure the Backup Device.

ZyWALL > Device HA > Monitored Interface > Edit > #1

**Monitored Interface Configuration**
☒ Enable Monitored Interface
Interface Name
ge1
Virtual Router IP(VRIP) / Subnet Mask
192.168.10.254 / 255.255.255.0
Manage IP
Subnet Mask

Step4. Unplug the PC cable from Backup ZyWALL wan1 and plug it back to L2 switch LAN segment. Connect all the cables from L2 and L3 switches to the Backup ZyWALL as on the network topology diagram shown on the index page. Login to the Backup ZyWALL via the management IP. Now we can synchronize the configuration from the Master to the Backup. Switch to **ZyWALL > Device HA > Active-Passive Mode > Synchronize** and enter the Master ZyWALL admin account password. Input the LAN IP address of the Master ZyWALL

in the “Synchronize from” option and set the auto synchronize interval. Then click the “Apply” button to save the configuration.

**Synchronization**

Server Address: 167.35.4.3, 10.59.1.45, 192.168.1.1, 10.59.0.1, 192.168.2.1

Server Port: 21 (Configure)

Password:

Note: Backup device's configuration can synchronize with master device's.

Apply Reset

Switch to **ZyWALL > Maintenance > Log > View Log** to check the log record.

**View Log** Log Setting

Logs

Show Filter

Display: All Logs Email Log Now Refresh Clear Log

Total logging entries: 143 30 entries per page Page 1/5

#	Time	Priority	Category	Message	Source	Destination	Note
1	2006-01-25 11:48:38	notice	Device HA	Device HA syncing from 192.168.10.254 Successfully			Device HA
2	2006-01-25 11:48:38	notice	Policy Route	Policy-route rule 1 was modified.			CONFIG CHANGE
3	2006-01-25 11:48:38	notice	Policy Route	Policy-route rule 1 was appended.			CONFIG CHANGE
4	2006-01-25 11:48:38	notice	Firewall	Firewall global rule 6 was modified.			CONFIG CHANGE
5	2006-01-25 11:48:38	notice	Firewall	Firewall global rule 5 was modified.			CONFIG CHANGE
6	2006-01-25 11:48:38	notice	Firewall	Firewall global rule 4 was modified.			CONFIG CHANGE
7	2006-01-25 11:48:38	notice	Firewall	Firewall global rule 3 was modified.			CONFIG CHANGE
8	2006-01-25 11:48:38	notice	Firewall	Firewall global rule 2 was modified.			CONFIG CHANGE
9	2006-01-25 11:48:38	notice	Firewall	Firewall global rule 1 was modified.			CONFIG CHANGE
10	2006-01-25	info	System	DHCP Server executed with cautious mode.			DHCP

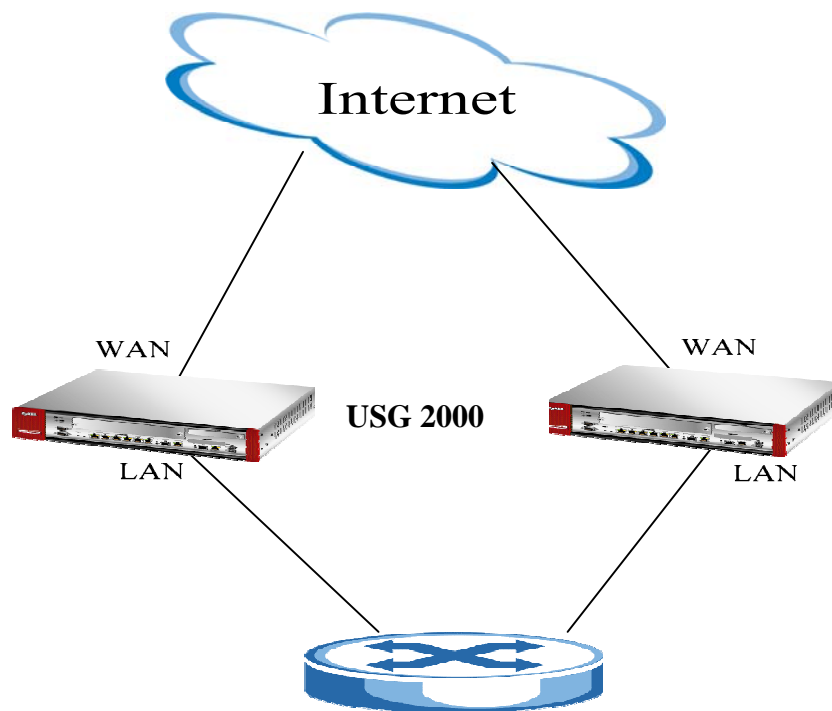
Step6. Check the system status page. You will see that the Master ZyWALL USG 2000's configuration has been synchronized to Backup ZyWALL USG 2000 and we can continue to setup the remaining setting HA group in Backup HA, you can refer to use guide to do detailed configuration.

After these steps, the Device HA configuration is done.

### 1.5.2 Device High Availability (HA) Active-Passive mode

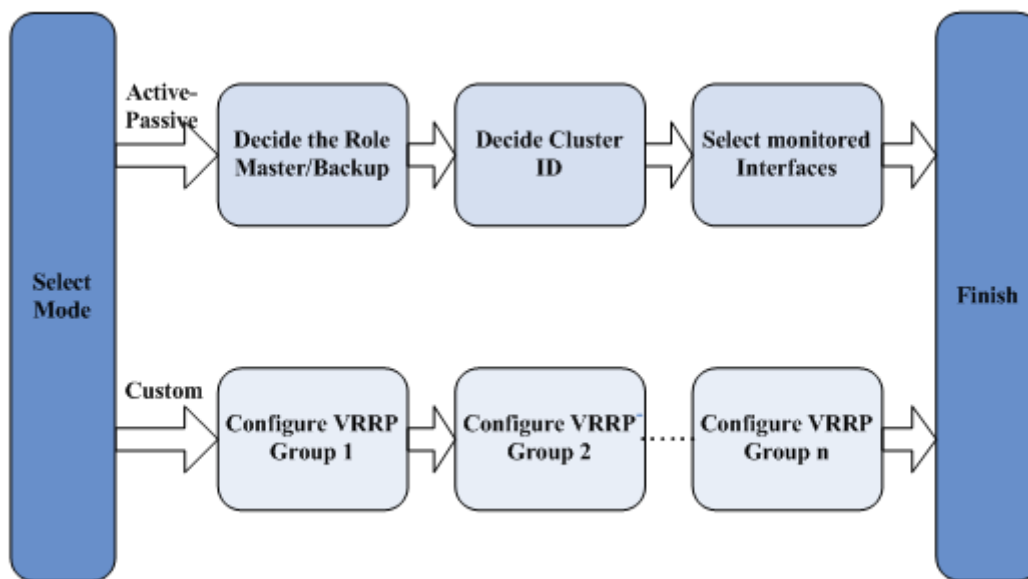
Device HA provides the benefit of network reliability. It prevents the unavailability of the whole network due to the failure of single point. Here, we use Virtual Router Redundancy Protocol (VRRP) to implement this purpose. VRRP allows you to create redundant backup gateways to ensure that default gateway is always available.

#### 1.5.2.1 Scenario Topology



#### 1.5.2.2 Configuration Flow

ZyXEL ZyWALL runs VRRP v2. Hence, you can only set up device HA with other ZyWALLs of the same model running the same firmware version. In this example, there are two gateways with the following configuration. You first configure a gateway as master one and then configure another one as backup gateway.



### 1.5.2.3 Configuration procedure

- Configuring master USG
- Activating Device HA on the master USG
- Configuring Manage IP for the LAN Interface on the master USG
- Configuring LAN interface in master USG
- Configure Device HA on the Backup USG
- Activating Device HA on the backup USG
- Configuring Manage IP for the LAN Interface on the backup USG
- Interconnecting the Master and the Backup
- Test: Unplug the WAN cable on the Master

In this example, the network parameters will be the same as following table.

**The configuration on the Master**

WAN= 59.124.163.155

WAN Manage IP= 59.124.163.150

LAN= 192.168.1.1

LAN Manage IP = 192.168.1.2

**The configuration on the Backup**

WAN= 59.124.163.155

WAN Manage IP = 59.124.163.151

LAN= 192.168.1.1

LAN Manage IP =192.168.1.3

### 1.5.2.4 Steps to configure

In this figure, it shows that current setting of interface in WAN1 and LAN1. You will need the information to use in the configuration of device HA.

Interface Summary								
Interface Summary								
Name	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Renew/Dial	
ge1	100M/Full	n/a	LAN	192.168.10.254 / 255.255.255.0	Static	n/a	n/a	
ge2	Down	n/a	WAN	220.123.123.2 / 255.255.255.0	Static	n/a	n/a	
ge3	Down	n/a	WAN	220.123.133.2 / 255.255.255.0	Static	n/a	n/a	
ge4	100M/Full	n/a	DMZ	192.168.20.254 / 255.255.255.0	Static	n/a	n/a	
ge5	Down	n/a	DMZ	192.168.4.1 / 255.255.255.0	Static	n/a	n/a	
ge6	Down	n/a	n/a	0.0.0.0 / 0.0.0.0	Static	n/a	n/a	
ge7	Down	n/a	n/a	0.0.0.0 / 0.0.0.0	Static	n/a	n/a	
ge8	1000M/Full	n/a	n/a	59.124.163.154 / 255.255.255.224	Static	n/a	n/a	
aux	Inactive	n/a	n/a	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a	

### Configuration on the Master

First, we decide one gateway as master router. Therefore, you enable the Device HA and then configure it as master router in the tab of “Active-Passive mode (AP mode)”



**ZyWALL > Device HA > General**

General Active-Passive Mode Legacy Mode

**General Settings**

☒ Enable Device HA  
Device HA Mode Active-Passive Mode ([Switch to Legacy Mode page](#))

**Monitored Interface Summary**

Interface	Virtual Router IP / Netmask	Management IP / Netmask	Link Status	HA Status

Apply Reset

### Enable Device HA on the Master

This figure shows that the configuration in the mode of Active-Passive mode.

**ZyWALL > Device HA > Active-Passive Mode**

General Active-Passive Mode Legacy Mode

**General Settings**

Device Role ☒ Master ☐ Backup

**Cluster Settings** [Advanced](#)

Cluster ID  (1-16)

**Monitored Interface Summary**

Interface	Virtual Router IP/Netmask	Management IP/Netmask	Link Status	Modify
ge1	192.168.10.254 / 255.255.255.0	/	Up	
ge2	220.123.123.2 / 255.255.255.0	/	Up	
ge3	220.123.133.2 / 255.255.255.0	/	Down	
ge4	192.168.20.254 / 255.255.255.0	/	Down	
ge5	192.168.4.1 / 255.255.255.0	/	Down	
ge6	/	/	Down	
ge7	/	/	Down	
ge8	59.124.163.154 / 255.255.255.224	/	Up	

**Synchronization**

Active-Passive mode (AP mode) configuration

### Configuring Manage IP for the WAN Interface on the Master

After setting up the virtual router IP, we need to configure the management IP and its corresponding subnet for this master router.



**ZyWALL > Device HA > Monitored Interface > Edit > #2**

**Monitored Interface Configuration**

☒ Enable Monitored Interface

Interface Name: ge2

Virtual Router IP(VRIP) / Subnet Mask: 220.123.123.2 / 255.255.255.0

Manage IP: 220.123.123.5

Subnet Mask: 255.255.255.0

OK Cancel

Configuring Manage IP for the WAN Interface on the Master

After finishing the setting of WAN, you need to configure the setting of LAN for this master gateway.

**ZyWALL > Device HA > Active-Passive Mode**

General Active-Passive Mode Legacy Mode

















**General Settings**

Device Role: ☒ Master ☐ Backup

**Cluster Settings** [Advanced](#)

Cluster ID: 1 (1-16)

**Monitored Interface Summary**

Interface	Virtual Router IP/Netmask	Management IP/Netmask	Link Status	Modify
ge1	192.168.10.254 / 255.255.255.0	/	Up	 
ge2	220.123.123.2 / 255.255.255.0	/	Up	 
ge3	220.123.133.2 / 255.255.255.0	/	Down	 
ge4	192.168.20.254 / 255.255.255.0	/	Down	 
ge5	192.168.4.1 / 255.255.255.0	/	Down	 
ge6	/	/	Down	 
ge7	/	/	Down	 
ge8	59.124.163.154 / 255.255.255.224	/	Up	 

### Configuring LAN interface

In this figure, it shows that you need to set the parameters of LAN for master gateway. IN this example, we type ge1 Manage IP as 192.168.10.250.

**ZyWALL > Device HA > Monitored Interface > Edit > #1**

---

**Monitored Interface Configuration**

☒ Enable Monitored Interface

Interface Name ge1

Virtual Router IP(VRIP) / Subnet Mask 192.168.10.254 / 255.255.255.0

Manage IP 192.168.10.250

Subnet Mask 255.255.255.0

### Configure Device HA on the Backup

Make sure the network settings are same with the Master

Since these two gateways will be backup each other. For end nodes in this network, they will know only one gateway. Hence, you must confirm the setting of interface of WAN and LAN in backup gateway are the same as the ones in master gateway.

Interface Status Summary					
Name	Status	HA Status	Zone	IP Address	Action
ge1	100M/Full	n/a	LAN	192.168.10.254	n/a
ge2	100M/Full	n/a	WAN	220.123.123.2	n/a
ge3	Down	n/a	WAN	220.123.133.2	n/a
ge4	Down	n/a	DMZ	192.168.20.254	n/a
ge5	Down	n/a	DMZ	192.168.4.1	n/a
ge6	Down	n/a	n/a	0.0.0.0	n/a
ge7	Down	n/a	n/a	0.0.0.0	n/a
ge8	1000M/Full	n/a	n/a	59.124.163.154	n/a
aux	Inactive	n/a	n/a	0.0.0.0	n/a

Then, you first activate the function of “Device HA.”

ZyWALL > Device HA > General

General
Active-Passive Mode
Legacy Mode

#### General Settings

☒ Enable Device HA  
Device HA Mode

Active-Passive Mode ([Switch to Legacy Mode page](#))

#### Monitored Interface Summary

Interface	Virtual Router IP / Netmask	Management IP / Netmask	Link Status	HA Status
<div> Apply Reset </div>				

Enable Device HA on the backup

At the same time, configure this gateway as backup one.

The screenshot shows the configuration interface for the ZyWALL USG 2000. The 'Active-Passive Mode' tab is selected. In the 'General Settings' section, the 'Device Role' is set to 'Backup' (highlighted with a red box). The 'Priority' is set to 1. In the 'Cluster Settings' section, the 'Cluster ID' is set to 1. The 'Monitored Interface Summary' table lists interfaces ge1 through ge8 with their respective IP addresses, netmasks, and link statuses. The 'Modify' column for ge2 is highlighted with a red box.

Interface	Virtual Router IP/Netmask	Management IP/Netmask	Link Status	Modify
ge1	192.168.10.254 / 255.255.255.0	/	Up	
ge2	220.123.123.2 / 255.255.255.0	/	Up	
ge3	220.123.133.2 / 255.255.255.0	/	Down	
ge4	192.168.20.254 / 255.255.255.0	/	Down	
ge5	192.168.4.1 / 255.255.255.0	/	Down	
ge6	/	/	Down	
ge7	/	/	Down	
ge8	59.124.163.154 / 255.255.255.224	/	Up	

Selecting the device role and monitored interfaces

In the following figure, it shows the setting of ge2 in backup gateway.

The screenshot shows the 'Monitored Interface Configuration' dialog box for interface ge2. The 'Enable Monitored Interface' checkbox is checked. The 'Interface Name' is ge2. The 'Virtual Router IP(VRIP) / Subnet Mask' is 220.123.123.2 / 255.255.255.0. The 'Manage IP' is 220.123.123.10 and the 'Subnet Mask' is 255.255.255.0. The 'OK' and 'Cancel' buttons are at the bottom.

Assign a manage IP to the WAN Interface on the Backup

Next, we set the parameters in LAN for backup gateway.

**ZyWALL > Device HA > Active-Passive Mode**

General **Active-Passive Mode** Legacy Mode









**General Settings**

Device Role ☐ Master ☒ Backup  
 Priority  (1-254)  
☐ Enable Preemption

**Cluster Settings** [Advanced](#)

Cluster ID  (1-16)

**Monitored Interface Summary**

Interface	Virtual Router IP/Netmask	Management IP/Netmask	Link Status	Modify
ge1	192.168.10.254 / 255.255.255.0	/	Up	
ge2	220.123.123.2 / 255.255.255.0	/	Up	
ge3	220.123.133.2 / 255.255.255.0	/	Down	
ge4	192.168.20.254 / 255.255.255.0	/	Down	
ge5	192.168.4.1 / 255.255.255.0	/	Down	
ge6	/	/	Down	
ge7	/	/	Down	
ge8	59.124.163.154 / 255.255.255.224 /	/	Up	

**Synchronization**

Assign a manage IP to the LAN Interface on the Backup

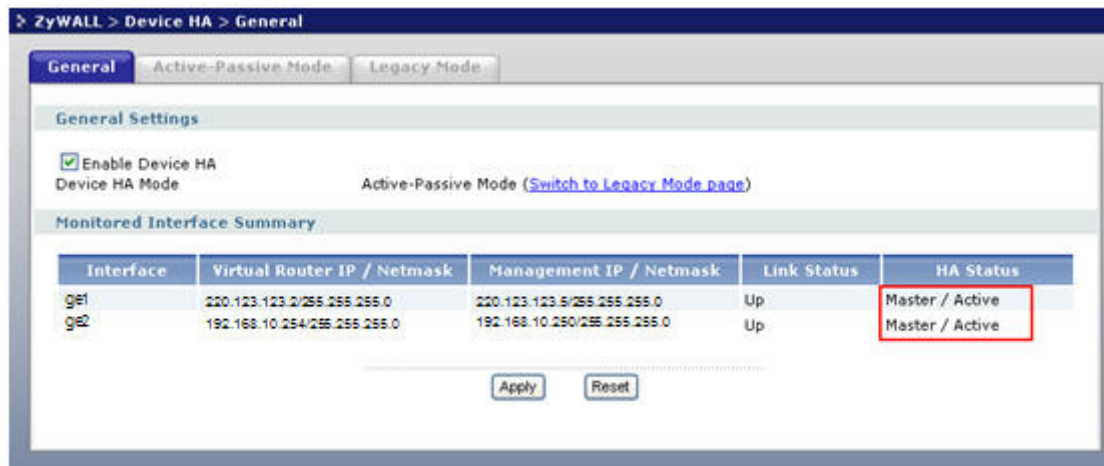
**ZyWALL > Device HA > Monitored Interface > Edit > #1**

**Monitored Interface Configuration**

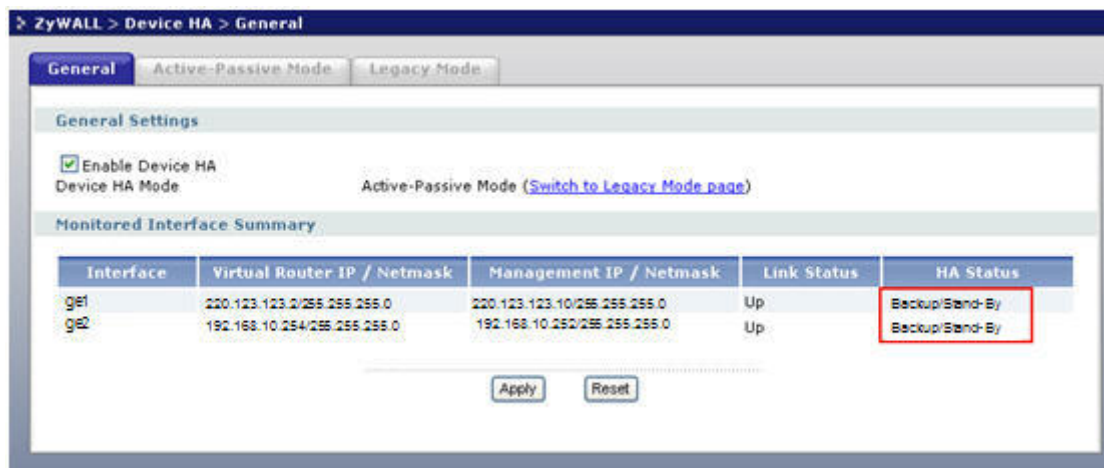
☒ Enable Monitored Interface  
 Interface Name   
 Virtual Router IP(VRIP) / Subnet Mask   
 Manage IP   
 Subnet Mask

## Connect the Master and the Backup

After confirming the setting in both of gateway, we link these two gateways. You should see the corresponding role shown in HA status. Master management IP is 192.168.1.2.



In this figure, you can find that backup server is alive and is in the status of Stand-by because master gateway is working well. (Backup management IP: 192.168.1.3)



Afterwards, you need to synchronize the information in both of gateways. Please provide another password for this procedure. This is not the same as the administrator's password. The default is the password in FTP service.

















It is recommended to use LAN to synchronize the configuration in both of devices.

**ZyWALL > Device HA > Active-Passive Mode**

**Cluster Settings** Advanced

Cluster ID  (1-16)

**Monitored Interface Summary**


Interface	Virtual Router IP/Netmask	Management IP/Netmask	Link Status	Modify
ge1	192.168.10.254 / 255.255.255.0	/	Up	 
ge2	220.123.123.2 / 255.255.255.0	/	Up	 
ge3	220.123.133.2 / 255.255.255.0	/	Down	 
ge4	192.168.20.254 / 255.255.255.0	/	Down	 
ge5	192.168.4.1 / 255.255.255.0	/	Down	 
ge6	/	/	Down	 
ge7	/	/	Down	 
ge8	59.124.163.154 / 255.255.255.224	/	Up	 

**Synchronization**

Server Address 192.168.10.254, 220.123.123.2, 220.123.133.2, 192.168.20.254, 192.168.4.1, 59.124.163.154

Server Port 21 [\(Configure\)](#)

Password

 Note:  
Backup device's configuration can synchronize with master device's.

Enter the password for synchronization on the Master

### Test: Unplug the WAN cable on the Master

Next, we do a test to see whether the function of “Device HA” work. You can simply un-plug the WAN cable connected in the master gateway to simulate the link failure in the network.

In this figure, you can see the master router goes down based on the information shown in HA status. You can see that HA status will change to fault on the Master and the Backup will go Active

**ZyWALL > Device HA > General**

**General** Active-Passive Mode Legacy Mode

**General Settings**

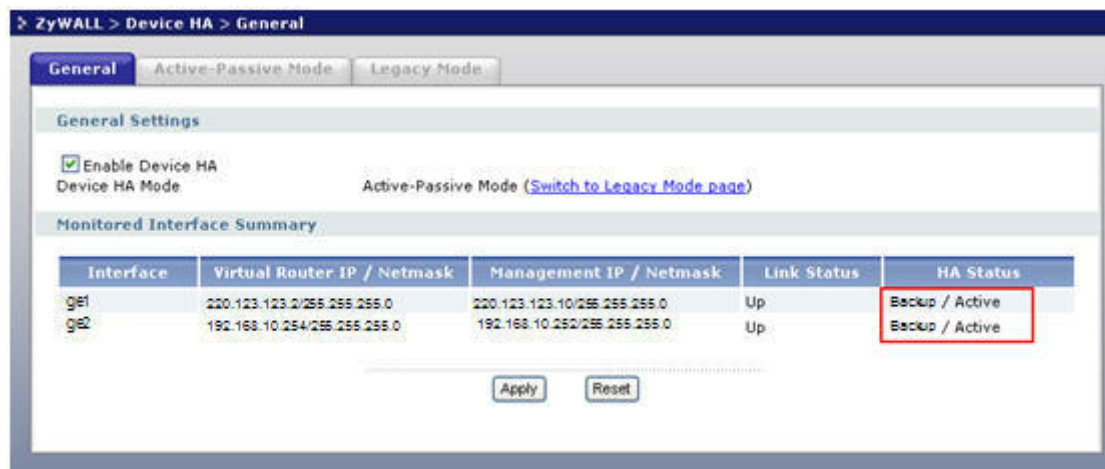
☒ Enable Device HA

Device HA Mode Active-Passive Mode ([Switch to Legacy Mode page](#))

**Monitored Interface Summary**

Interface	Virtual Router IP / Netmask	Management IP / Netmask	Link Status	HA Status
ge1	220.123.123.2/255.255.255.0	220.123.123.5/255.255.255.0	Up	Master / Fault
ge2	192.168.10.254/255.255.255.0	192.168.10.250/255.255.255.0	Up	Master / Fault

In this figure, you can find that backup server is alive and is in the status of “Active” because master gateway is down now. Hence, the backup server is handling all traffic.





## 2. Security Policy Enforcement

### **What is a security policy?**

Security policy, in the context of information security, defines an individual or an object's access privilege to information assets which are very important for the company. If the security policy is not considered and deployed well, the impact on the company will be massive. We can say that it is a mandatory process to protect the information assets.

For example, ZyCompany doesn't want their guests or vendors to be able to access their internal network but allows them to access Internet in case they have to get some information from outside, i.e. access their company's email. Therefore, ZyCompany defines a security policy - outsider can use 'guest/guest1234' to access Internet through wireless access, but it is forbidden for them to access company's Internal resource, like talk to LAN PC, access the DMZ servers, or access the branch office's data through VPN's environment.

### **What your business can benefit from deployment of security policy?**

Deploy security policy well can not only protect company information assets, but also increase overall productivity, mitigate the impact of malicious application or misuse, and support regulatory compliance.

## 2.1 Managing IM/P2P Applications

### **2.1.1 Why bother with managing IM/P2P applications?**

Because some virus/exploits which may cause security breaches are transmitted via IM/P2P applications, managing IM/P2P application well can mitigate security breaches. Besides, restricting access to IM/P2P applications can help employees focusing on his/her job to increase productivity and reduce misuse of network resources, e.g. bandwidth.

### **2.1.2 What does ZyWALL USG 2000 provide for managing IM/P2P**

#### **applications?**

ZyWALL provides best solution to solve the rigidity of the “all-or-nothing” approach and can meet customer’s expectation.

1. Application patrol: it can “recognize” IM/P2P applications and IT administrators can leverage it to restrict access to IM/P2P applications
2. Access granularity: combined with access granularity, IT admin can enforce flexible policy against IM/P2P applications.

ZyWALL USG 2000’s access granularity for controlling hazardous IM/P2P applications:

- By User/Group
- By Time of access
- By Bandwidth

### **2.1.3 Configuration Example**

Application patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, http and ftp) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application’s individual features (like text messaging, voice, video conferencing, and file transfers). Application patrol also has powerful bandwidth management including traffic prioritization to enhance the performance of delay-sensitive applications like voice and video.

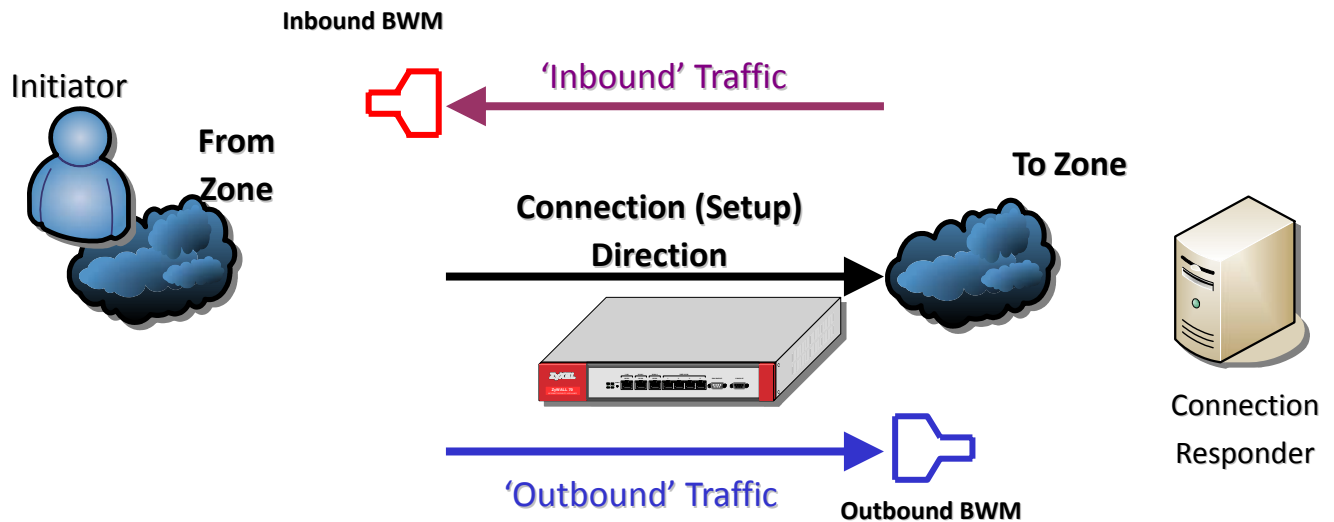
#### **Zone Design is Now Available**

Zone design is now supported in ZLD 2.x 2000. The major enhancement in ZLD2.x 2000 solutions enables the ZyWALL to correctly differentiate the traffic from different sources.

With ZLD1.0x the ZyWALL can decide whether the specific traffic can be forwarded or not, but it does not differentiate the traffic from different sources. As a result, it may accidentally drop the packet. For example, both the malicious/suspicious packets from WAN to LAN

(known as a attack) and the traffic coming from DMZ to LAN (normal traffic) will be treated as an attack.

### Inbound Traffic vs. Outbound Traffic



A connection has an outbound and inbound packet flow. The ZyWALL controls the bandwidth of traffic of both flows as it is going out through an interface or VPN tunnel.

- Outbound traffic flows from the connection initiator to the connection responder.
- Inbound traffic flows from the connection responder to the connection initiator.

For example, a LAN to WAN connection is initiated from the LAN and goes to the WAN.

- Outbound traffic goes from a LAN zone device to a WAN zone device. Bandwidth management is applied before sending the packets out a WAN zone interface on the ZyWALL.
- Inbound traffic comes back from the WAN zone device to the LAN zone device. Bandwidth management is applied before sending the traffic out a LAN zone interface.

Bandwidth management is very useful when applications are competing for limited bandwidth. Here is an example of what the rules need to accomplish. See the following sections for more details.

For proper network usage, the IT manager requires the network administrator to configure ZyWALL AppPatrol according to company IT policy as:

- Boss: Can use any internet application without access control and bandwidth limitation.
- Sales: Can use instant messaging application (MSN) for text message and file transfer

purpose. Application allowed during certain period of time between 8:00~18:00 with bandwidth limitation 500K bps.

- RD: Allows instant messaging chat but file transfer within period 8:00~20:00. Bandwidth limited to 200K bps.

To fulfill the requirement, the network administrator needs to configure the ZyWALL according to the following setting:

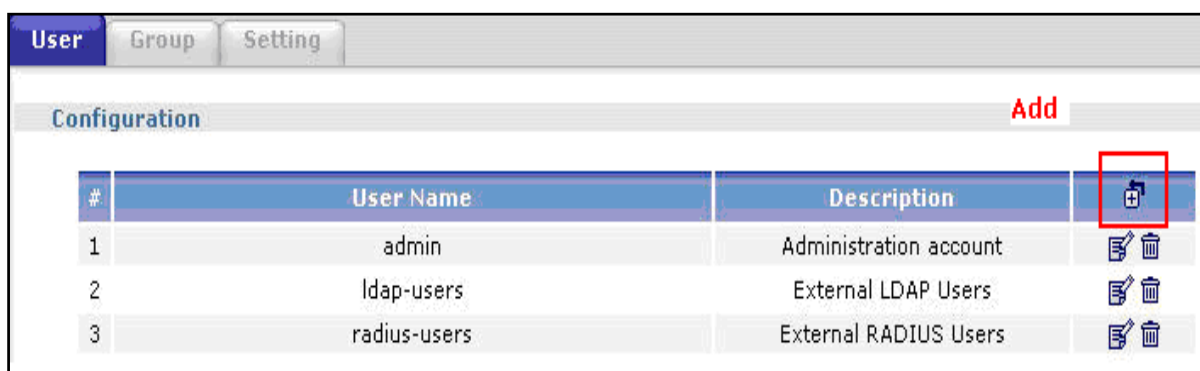
1. Create the required user/group object
2. Define AppPatrol (application type/access control/bandwidth limitation) according to IT policy
3. Application Policy Configuration

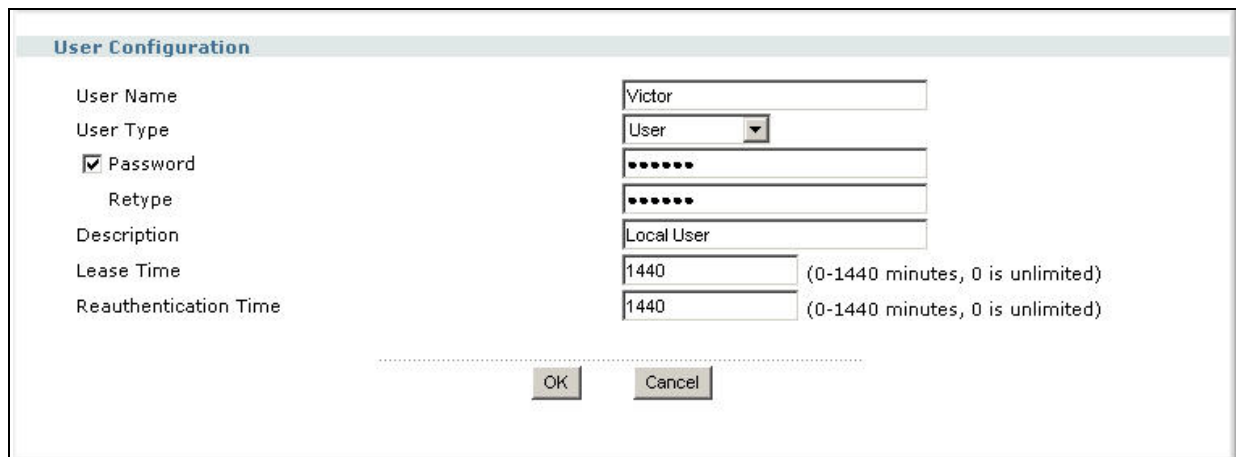
### STEP 1: Create the Required User and Group Object

1. We are going to create several users for different groups.

User	Group	IM Access	File Transfer	Access Allowed	Bandwidth
Victor	Manager	Yes	Yes	All	Unlimited
Peter	Sales	Yes	Yes	08:00-18:00	500k
John	RD	Yes	No	08:00-20:00	No
Guest	Guest	No	No	No	No

2. Navigate to **ZyWALL > Object > User/Group > User tab** and add the user 'Victor' as the screen dump.





**User Configuration**

User Name: Victor

User Type: User

☒ Password: .....

Retype: .....

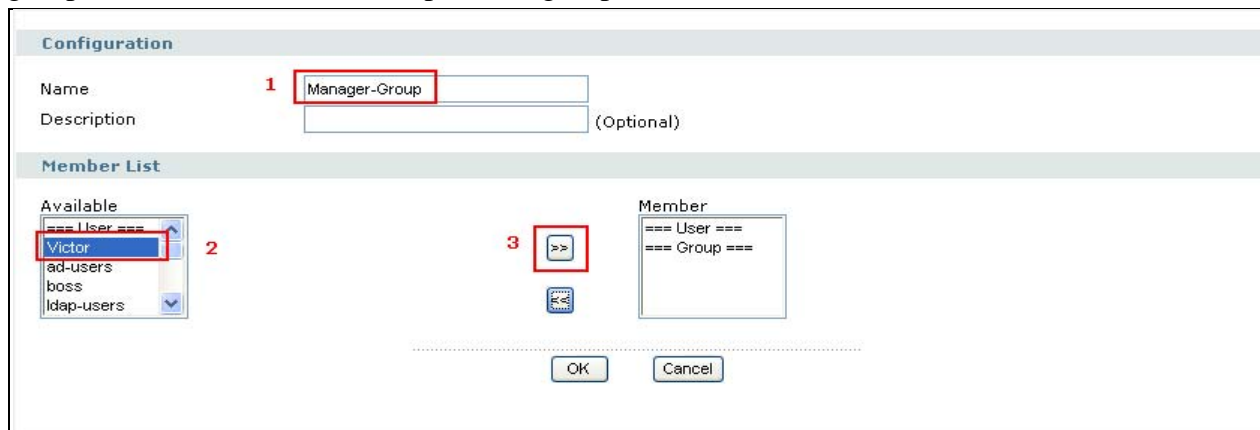
Description: Local User

Lease Time: 1440 (0-1440 minutes, 0 is unlimited)

Reauthentication Time: 1440 (0-1440 minutes, 0 is unlimited)

OK Cancel

3. Switch to Group tab, create a group named 'Manager' and add 'Victor' to the manager group. Press 'OK' button to complete the group creation.



**Configuration**

Name: 1 Manager-Group

Description: (Optional)

**Member List**

Available: 2 Victor

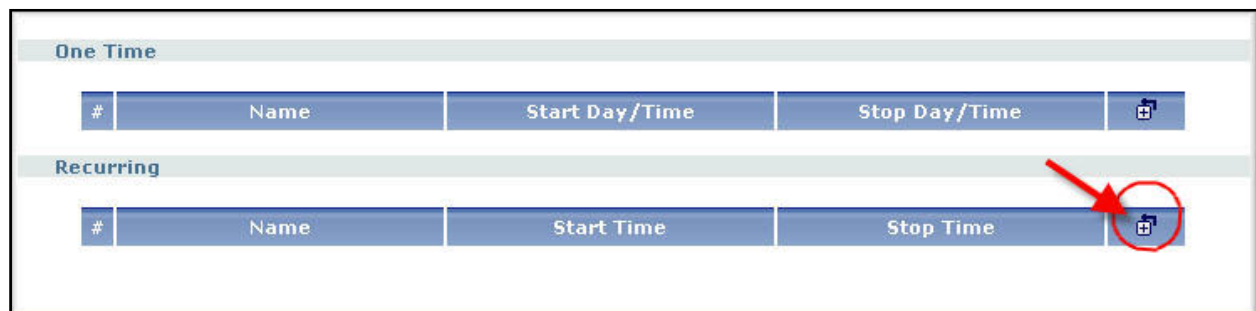
Member: 3 >>

OK Cancel

4. Create three more groups called 'Sales-Group', 'RD-Group' and 'Guest-Group'. Add 'Peter' into the Sales group and add 'John' into RD group.

## STEP 2: Create Schedule Object as Required

Go to menu **ZyWALL > Object > Schedule**, click Add button from the Recurring schedule to create a new schedule as following.



**One Time**

#	Name	Start Day/Time	Stop Day/Time	

**Recurring**

#	Name	Start Time	Stop Time	

A red arrow points to the Add button (plus icon) in the Recurring table.

Configuration						
Name	<input type="text" value="IM_For_Sales"/>					
Day Time						
Item #	Date			Time		
	Year	Month	Day	Hour	Minute	
Start	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="08"/>	<input type="text" value="00"/>	
Stop	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="18"/>	<input type="text" value="00"/>	
Weekly						
Week Days	<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday	<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input type="checkbox"/> Saturday
	<input type="checkbox"/> Sunday					
<input type="button" value="OK"/> <input type="button" value="Cancel"/>						

Click 'OK' button to complete this settings and repeat the above steps to create a new schedule for RD-Group.

Configuration						
Name	<input type="text" value="IM_FOR_RD"/>					
Day Time						
Item #	Date			Time		
	Year	Month	Day	Hour	Minute	
Start	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="08"/>	<input type="text" value="00"/>	
Stop	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text" value="22"/>	<input type="text" value="00"/>	
Weekly						
Week Days	<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday	<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input type="checkbox"/> Saturday
	<input type="checkbox"/> Sunday					
<input type="button" value="OK"/> <input type="button" value="Cancel"/>						

### STEP 3: AppPatrol Configuration

1. Navigate to **ZyWALL > AppPatrol > General** and check 'Enable Application Patrol'.

**General** Common Instant Messenger Peer to Peer VoIP Streaming Other Statistics

**General Setup**

☒ Enable Application Patrol

**BWM Global Setting**

☐ Enable BWM

**Registration**

Registration Status: **Licensed**  
 Registration Type: **Trial**  
[Apply New Registration](#)

**Signature Information**

Current Version: **2.020**  
 Released Date: **2007/05/10 21:19:58**  
[Update Signatures](#)

Apply Reset

2. Go to Instant Messenger tab and click 'Modify' button on MSN for further configuration.

General Common **Instant Messenger** Peer to Peer VoIP Streaming Other Statistics

**Configuration**

#	Service	Default Access	Modify
1	web-msn	forward	
2	yahoo	forward	
3	aol-icq	forward	
4	qq	forward	
5	jabber	forward	
6	odigo	forward	
7	rediff	forward	
8	msn	forward	

Apply Reset

3. Enable the service.

**Service**

☒ Enable Service

**Service Identification**

Name: **msn**  
 Classification: ☒ Auto ☐ Service Ports

**Policy**

#	Port	Schedule	User	From	To	Source	Destination	Access	BWM In/Out/Pri	Log	Modify
Default 0	none	any	any	any	any	any	any	reject	N/A	no	

OK Cancel

#### STEP 4: Application Policy Configuration

1. Click 'Edit' to edit the 'Default' policy

**Service**

☒ Enable Service

**Service Identification**

Name:

Classification: ☒ Auto ☐ Service Ports

**Policy**

#	Port	Schedule	User	From	To	Source	Destination	Access	BWM In/Out/Pri	Log	
Default 0		none	any	any	any	any	any	reject	N/A	no	

OK Cancel

2. Change the default access to 'Reject' and then click 'OK'

**Configuration**

Access: Reject ▼

Action Block: ☐ Login ☐ Message ☐ Audio ☐ Video ☐ File-Transfer

Bandwidth Management: Inbound:  kbps Outbound:  kbps (0 : disabled)

Priority:

☐ Maximize Bandwidth Usage

Log: no ▼

OK Cancel

3. Create a new application policy rule by clicking '+' icon and fill out the setting as the figure shown below.



### Application Policy for Manager-Group

Configuration	
<input checked="" type="checkbox"/> Enable Policy	
Port	0 (0 : any)
Schedule	none
User	Manager-Group
From	any
To	any
Source	any
Destination	any
Access	forward
Action Block	<input type="checkbox"/> Login <input type="checkbox"/> Message <input type="checkbox"/> Audio <input type="checkbox"/> Video <input type="checkbox"/> File-Transfer
Bandwidth Management	Inbound: 0 kbps Outbound: 0 kbps (0 : disabled)
	Priority 1
	<input type="checkbox"/> Maximize Bandwidth Usage
Log	no
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

### Application Policy for Sales-Group

Configuration	
<input checked="" type="checkbox"/> Enable Policy	
Port	0 (0 : any)
Schedule	IM_FOR_Sales
User	Sales-Group
From	any
To	any
Source	any
Destination	any
Access	forward
Action Block	<input type="checkbox"/> Login <input type="checkbox"/> Message <input type="checkbox"/> Audio <input type="checkbox"/> Video <input type="checkbox"/> File-Transfer
Bandwidth Management	Inbound: 0 kbps Outbound: 0 kbps (0 : disabled)
	Priority 1
	<input type="checkbox"/> Maximize Bandwidth Usage
Log	no
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

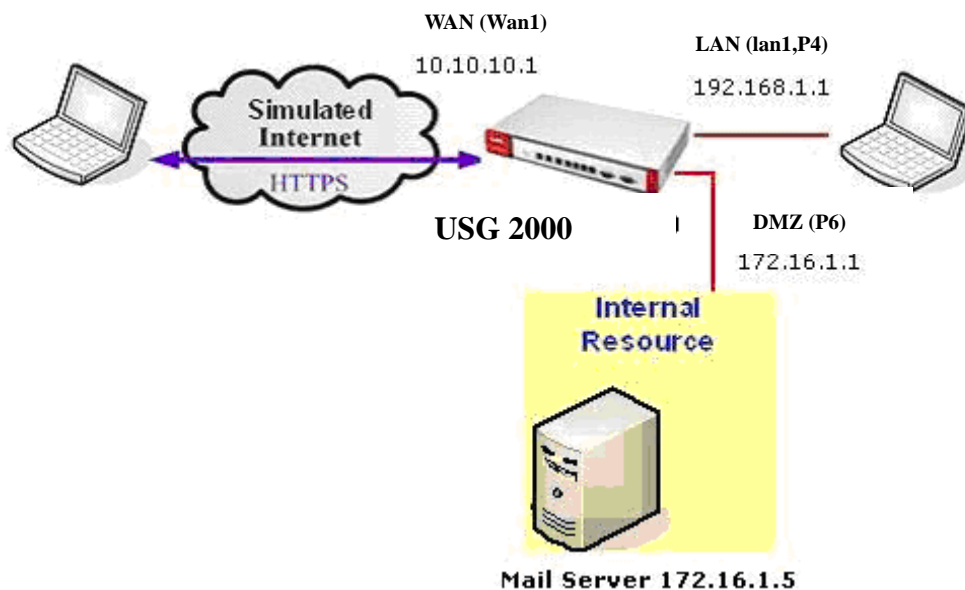
### Application Policy for RD-Group

Configuration	
<input checked="" type="checkbox"/> Enable Policy	
Port	0 (0 : any)
Schedule	IM_FOR_RD
User	RD-Group
From	any
To	any
Source	any
Destination	any
Access	forward
Action Block	<input type="checkbox"/> Login <input type="checkbox"/> Message <input type="checkbox"/> Audio <input type="checkbox"/> Video <input checked="" type="checkbox"/> File-Transfer
Bandwidth Management	Inbound: 0 kbps Outbound: 0 kbps (0 : disabled)
	Priority 1
	<input type="checkbox"/> Maximize Bandwidth Usage
Log	no
<input type="button" value="OK"/> <input type="button" value="Cancel"/>	

4. Press 'OK' button to complete the setting.

## 2.2 Zone-based Anti-Virus Protection

### 2.2.1 Applying Zone-Based Anti-Virus to ZyWALL USG 2000



Priority	From	To	Protocol
1	WAN	LAN	HTTP FTP SMTP POP3 IMAP4
2	WAN	DMZ	SMTP
3	DMZ	LAN	Don't need to check
4	DMZ	WAN	Don't need to check
5	LAN	DMZ	SMTP

In this example, there are 3 zones in total as WAN, LAN and DMZ.

For security, the email server will be placed in the DMZ. Whenever the email is sending in the direction of LAN to DMZ or WAN to DMZ, the Anti-Virus engine always scans the email transaction to ensure the email is not infected. Thus, it is unnecessary to scan every outgoing email from the DMZ again.

Please follow the instruction in order to achieve the result:

- 1) Login the GUI in the ZyWALL USG 2000 and navigate to **Configuration > Network > Interface > Ethernet**. Then, assign wan1 as WAN, P4 as lan1 and P6 as DMZ. Click “edit” to configure WAN1.

**ZyWALL > Network > Interface > Edit > Configuration > wan1**

**General Settings**

☒ Enable Interface

**Interface Properties**

Interface Name: wan1  
 Port: P1  
 Zone: WAN  
 MAC Address: 00:19:CB:7F:30:C1  
 Description: (Optional)

**IP Address Assignment**

☐ Get Automatically  
☒ Use Fixed IP Address

IP Address: 10.10.10.1  
 Subnet Mask: 255.255.255.0  
 Gateway: (Optional)  
 Metric: 0 (0-15)

- 2) Assign IP to wan1 and another to DMZ. Leave the reset of settings as default which will disable the DHCP Server in these two interfaces.

**ZyWALL > Network > Interface > Edit > Configuration > dmz**

**General Settings**

☒ Enable Interface

**Interface Properties**

Interface Name: dmz  
 Port: P6, P7  
 Zone: DMZ  
 MAC Address: 00:19:CB:7F:30:C6  
 Description: (Optional)

**IP Address Assignment**

IP Address: 172.16.1.1  
 Subnet Mask: 255.255.255.0

**Interface Parameters**

Egress Bandwidth: 1048576 Kbps

**DHCP Setting**

DHCP: None

Tips: You do not need a Gateway here since this interface is directly connected to ZyWALL

## USG 2000

- 1) The final summary of the Ethernet Interfaces should look like the example below.

ZyWALL > Network > Interface > Status

Status

Port Role

Ethernet

PPP

Cellular

WLAN

VLAN

Bridge

Auxiliary

Trunk

Interface Status

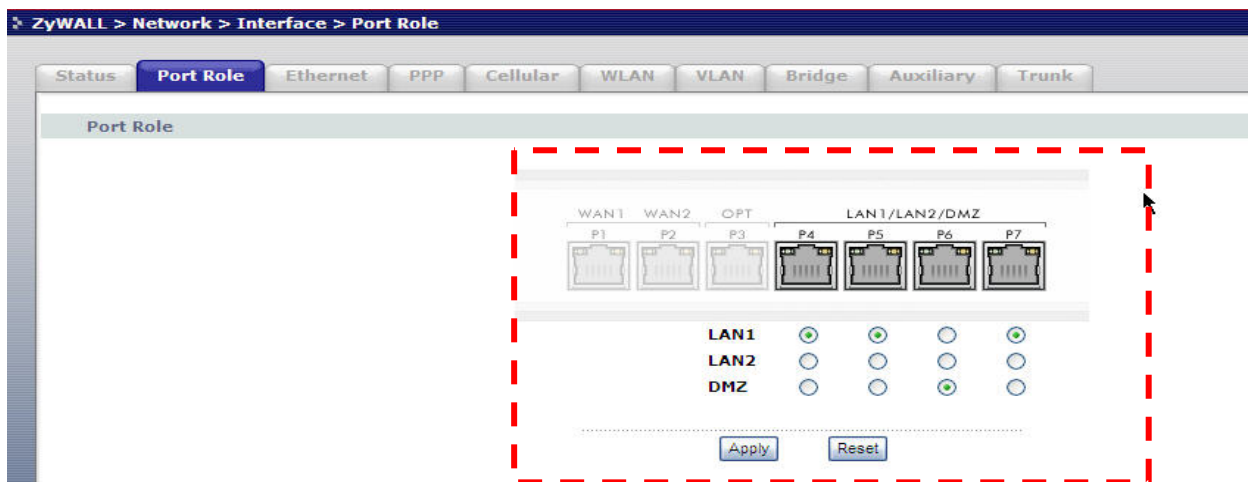
Name	Status	HA Status	Zone	IP Addr/Netmask	IP Assignment	Services	Action
wan1	Down	n/a	WAN	10.10.10.1 / 255.255.255.0	Static	n/a	n/a
wan2	Down	n/a	WAN	10.59.1.45 / 255.255.255.0	Static	n/a	n/a
opt	Down	n/a	OPT	0.0.0.0 / 0.0.0.0	Static	n/a	n/a
lan1	Up	n/a	LAN1	192.168.1.1 / 255.255.255.0	Static	DHCP server	n/a
lan2	Down	n/a	LAN2	192.168.3.1 / 255.255.255.0	Static	n/a	n/a
dmz	Down	n/a	DMZ	172.16.1.1 / 255.255.255.0	Static	n/a	n/a
aux	Inactive	n/a	WAN	0.0.0.0 / 0.0.0.0	Dynamic	n/a	n/a

Interface Statistics

Refresh

Name	Status	TxPkts	RxPkts	Collision	Tx B/s	Rx B/s
wan1	Down	4174	2073	0	0	0
wan2	Down	7114	0	0	0	0
opt	Down	0	0	0	0	0
lan1	Up	158934	156684	0	62046	27163
lan2	Down	0	0	0	0	0
dmz	Down	0	0	0	0	0

- 2) Assign proper ports in to the zone area. You can check ports zone status in **ZyWALL> Network> Interface >Port role**. In this example, we just need P4 as in LAN1 zone, P6 in DMZ zone.



- 3) After assigning specific port in zone area. Navigate to **Network > Zone**. Ensure your lan1 is assigned in LAN zone, WAN1 in WAN zone and the DMZ in DMZ zone.

ZyWALL > Network > Zone

Configuration

Name	Block Intra-zone	Member	Modify
LAN1	No	lan1	
LAN2	No	lan2	
WAN	Yes	wan1, wan2, wan1_ppp, wan2_ppp, aux	
DMZ	Yes	dmz	

- 4) Create 3 policies as WAN to LAN, WAN to DMZ, and LAN to DMZ. Navigate to **Anti-X > Anti-Virus**. In the Policies section, click “Add” button.


➤ ZyWALL > Anti-X > Anti-Virus > General

**General**   Setting   Signature

**General Setup**

☐ Enable Anti-Virus and Anti-Spyware

**Policies**

Priority	From	To	Protocol	
				

**Registration**

Registration Status: **Licensed**  
 Registration Type: **Trial**  
[Apply New Registration](#)

**Signature Information**

Current Version: **1.021**  
 Signature Number: **3200**  
 Released Date: **2007/06/26 00:52:18**  
[Update Signatures](#)

- 5) To create one policy and enable this rule, configure direction from WAN to LAN and select which protocols you want to scan.

**ZyWALL > Anti-X > Anti-Virus > General > Edit > #1**

<b>Configuration</b>				
<input checked="" type="checkbox"/> Enable				
<b>Direction</b>				
From	WAN			
To	LAN			
<b>Protocols to Scan</b>				
<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> FTP	<input checked="" type="checkbox"/> SMTP	<input checked="" type="checkbox"/> POP3	<input checked="" type="checkbox"/> IMAP4
<b>Actions When Matched</b>				
<input checked="" type="checkbox"/> Destroy infected file				
<input checked="" type="checkbox"/> Send windows message				
Log	log			
<b>White List / Black List Checking</b>				
<input type="checkbox"/> Bypass white list checking				
<input type="checkbox"/> Bypass black list checking				
<b>File decompression</b>				
<input checked="" type="checkbox"/> Enable file decompression (ZIP and RAR)				
<input type="checkbox"/> Destroy compressed files that could not be decompressed				

- 6) To create one policy and enable this rule, configure direction from WAN to DMZ and select which protocols you want to scan.

**ZyWALL > Anti-X > Anti-Virus > General > Edit > #1**

<b>Configuration</b>				
<input checked="" type="checkbox"/> Enable				
<b>Direction</b>				
From	WAN			
To	DMZ			
<b>Protocols to Scan</b>				
<input type="checkbox"/> HTTP	<input type="checkbox"/> FTP	<input checked="" type="checkbox"/> SMTP	<input type="checkbox"/> POP3	<input type="checkbox"/> IMAP4
<b>Actions When Matched</b>				
<input checked="" type="checkbox"/> Destroy infected file				
<input checked="" type="checkbox"/> Send windows message				
Log	log			
<b>White List / Black List Checking</b>				
<input type="checkbox"/> Bypass white list checking				
<input type="checkbox"/> Bypass black list checking				
<b>File decompression</b>				
<input checked="" type="checkbox"/> Enable file decompression (ZIP and RAR)				
<input type="checkbox"/> Destroy compressed files that could not be decompressed				

- 7) To create one policy and enable this rule, configure direction from LAN to DMZ and select which protocols you want to scan.

**ZyWALL > Anti-X > Anti-Virus > General > Edit > #1**

**Configuration**

☒ Enable

**Direction**

From: LAN  
To: DMZ

**Protocols to Scan**

☐ HTTP ☐ FTP ☒ SMTP ☐ POP3 ☐ IMAP4

**Actions When Matched**

☒ Destroy infected file  
☒ Send windows message  
Log: log

**White List / Black List Checking**

☐ Bypass white list checking  
☐ Bypass black list checking

**File decompression**

☒ Enable file decompression (ZIP and RAR)  
☐ Destroy compressed files that could not be decompressed

- 8) Reset log by pressing “Clean”. Navigate to **Maintenance > Log** and select **Anti-Virus** from **Display** drop-down list.

**ZyWALL > Maintenance > Log > View Log**

View Log | Log Setting

**Logs**

Show Filter

Display: Anti-Virus

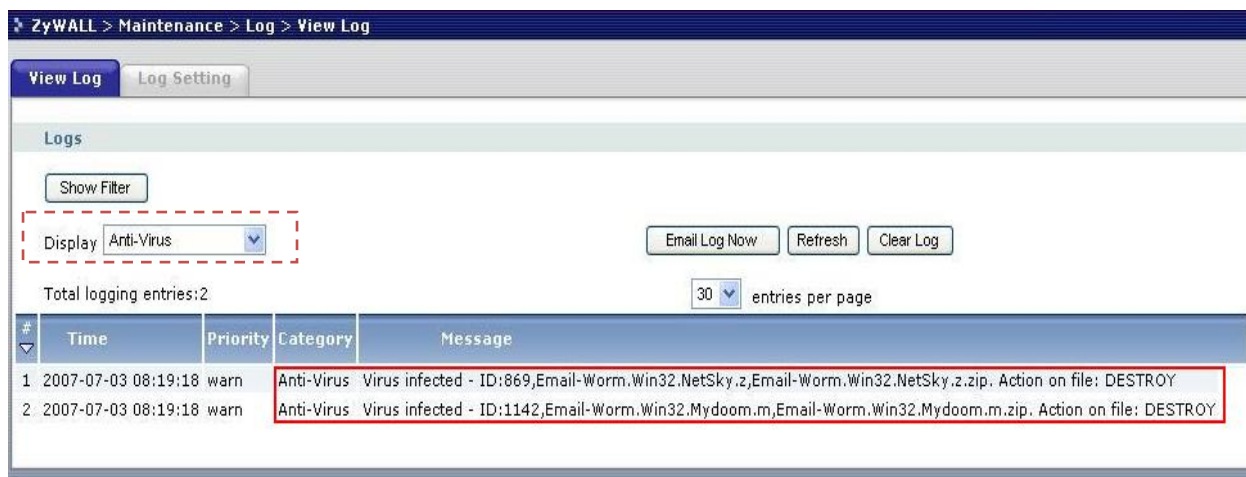
Email Log Now | Refresh | Clear Log

Total logging entries: 0 | 30 entries per page | Page: 1 of 1

#	Time	Priority	Category	Message	Source	Destination	Note
---	------	----------	----------	---------	--------	-------------	------

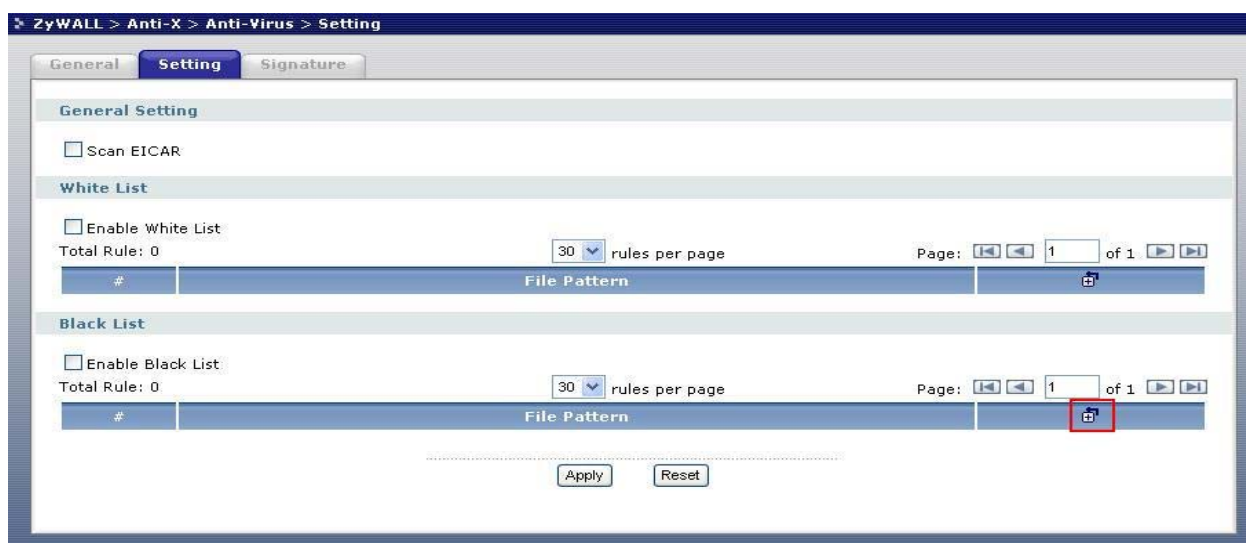
- 9) Test: Send **an email contains virus** from LAN to the mail server in DMZ.
- 10) Check the log file again from **Maintenance > Log**. Sort the log by selecting **Anti-Virus** from **Display** drop-down list. We can see the viruses have been destroyed correctly.



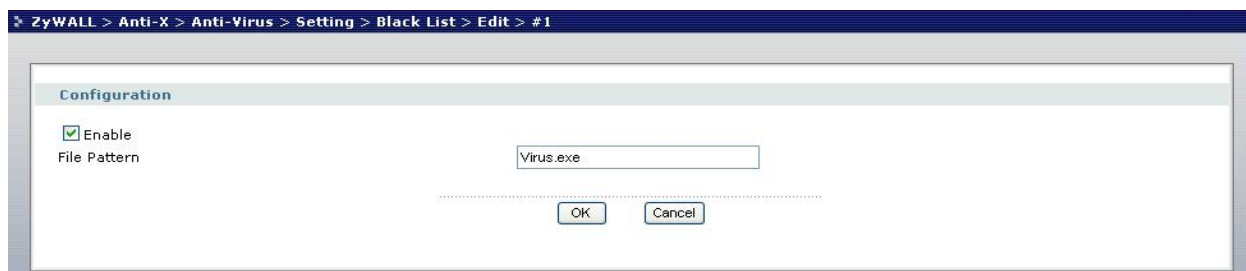


## 2.2.2 Enabling Black and White List

- 1) Add a black list by navigate to **Anti-X > Anti-Virus**, click **Settings** tab then click “**Add**” to create a new black list entry.

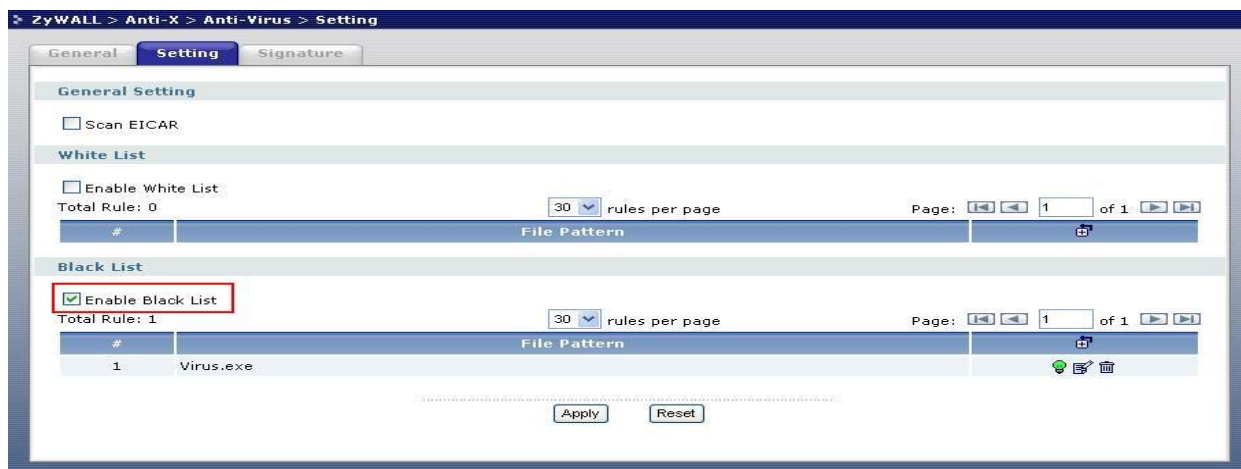


- 2) Check the **Enable** checkbox and enter the file name in **File Pattern** field. In this example, we try to destroy a file that named “Virus.exe” so we enter it in the field.

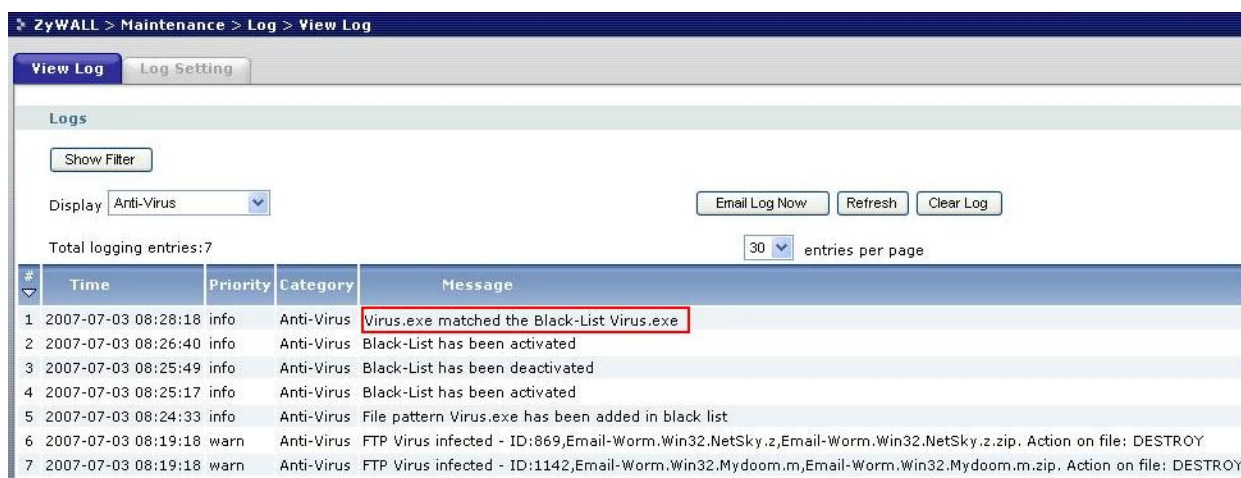


Click “OK” to go return to Setting page.

- 3) Check “Enable the Black List” on the **Setting** page and press “Apply” button.



- 4) Send an email with attached file “Virus.exe” to examinant the functionality of Back List.
- 5) Check the system log from **Maintenance > Log** and select **Anti-Virus** form **Display** drop-down list.



### 2.2.3 Enabling Anti-Virus Statistics Report

- 1) Navigate to **Maintenance > Report**, click the **Anti-Virus** tab and check the **Collect Statistics** checkbox.
- 2) Click **Apply** button.

- 3) Send an email to from the LAN.
- 4) Check the Anti-Virus statistics report from **Anti-Virus tab** by navigate to **Maintenance > Report**.

**Setup**

☒ Collect Statistics Apply Reset

**Summary**

Total Files Scanned: 6  
Infected Files Detected: 6

**Statistics**

Top Entry By: Virus Name

#	Virus Name	Occurrence
1	Email-Worm.Win32.NetSky.z	3
2	Email-Worm.Win32.Mydoom.m	3

Total: 6

## 2.2.4 Dual AV

## 2.3 Configuring ZyWALL USG 2000 as a Wireless Router

ZyWALL USG can also be a wireless router and provides wireless service for network administrator to extend their network topology if you install the PCMCIA-based wireless card. So far, ZyWALL USG only supports one wireless card ZyXELG-170S.

### 2.3.1 Configuration procedure

- Install wireless card
- Setting parameters of WLAN in USG
- Test wireless connection between client and USG

In this example, the following parameters will be applied in ZyWALL USG 200.

**SSID: USG 200**

**DHCP Server: 192.168.77.1**

**IP Pool: 192.168.77.51-60**

**MAC Filter: 00:0E:35:4F:85:15**

**WPA and Pre-shared Key**

First, you must check whether the wireless card is installed in your device and can be detected by ZyWALL USG 2000. In the following figure, you can see the wireless card, ZyXEL G-170S, has been installed and detected by ZyWALL USG 2000.

The screenshot displays the 'Status' page of the ZyWALL USG 2000. It includes sections for System Resources, Interface Status Summary, and Extension Slot. The Extension Slot section shows a PC Card (ZyXEL G-170S) installed in Slot 1.

Name	Status	HA Status	Zone	IP Address	Action
wan1	100M/Full	n/a	WAN	59.124.163.155	n/a
wan2	100M/Full	n/a	WAN	172.23.30.7	Renew
opt	Down	n/a	OPT	0.0.0.0	n/a
lan1	Up	n/a	LAN1	192.168.1.1	n/a
lan2	Down	n/a	LAN2	10.59.0.1	n/a
dmz	Down	n/a	DMZ	192.168.2.1	n/a
aux	Inactive	n/a	WAN	0.0.0.0	n/a

Slot	Device	Status
PC Card	ZyXEL G-170S	
USB 1	none	
USB 2	none	

Next, you need to activate the WLAN service in **ZyWALL> Network> Interface> WLAN**.

The screenshot shows the 'ZyWALL > Network > Interface > Wireless Card' configuration page. The 'WLAN' tab is selected. Under 'WLAN Device Settings', the 'Enable WLAN Device' checkbox is checked. The '802.11 Band' is set to 'b+g' and the 'Channel' is set to '6'. An 'Interface Summary' table is at the bottom, and an 'Edit' icon is highlighted in the table's header row.

#	Name	SSID	IP Address	Mask	Security	

Click the Edit icon to configure the details for WLAN. **Please make a copy of parameters in WLAN.** For instance, SSID, Security setting and IP assignment etc. Those information will

help you to configure wireless card in client side.

The screenshot shows the ZyWALL configuration interface for the WLAN interface. The breadcrumb trail is: ZyWALL > Network > Interface > WLAN > Edit > #1. The interface is divided into several sections:

- General Settings:**
  - ☒ Enable Interface
  - Interface Name: wlan-1
  - Description: (Optional)
  - Zone: LAN1
- Virtual Access Point Settings:**
  - SSID: USG200
  - ☐ Hide SSID Broadcast
  - ☐ Block Intra BSS Traffic
  - Maximum Associations: 255
- WLAN Security Settings:**
  - Security Type: WPA-PSK
  - Pre Shared Key: 12345678
- IP Address Assignment:**
  - IP Address: 192.168.77.1
  - Subnet Mask: 255.255.255.0
- Interface Parameters:**
  - Egress Bandwidth: 1048576 Kbps
- DHCP Setting:**
  - DHCP: DHCP Server
  - IP Pool Start Address (Optional): 192.168.77.51
  - Pool Size: 10
- Related Setting:**
  - ☒ Add a default wlan Policy Route for WAN access.

At the bottom, there is a "More Settings" button and "OK" and "Cancel" buttons.

### 2.3.2 MAC filter in WLAN

In WLAN of ZyXEL USG, you can also specify which MAC address(es) will be allowed or denied to access this WLAN service.

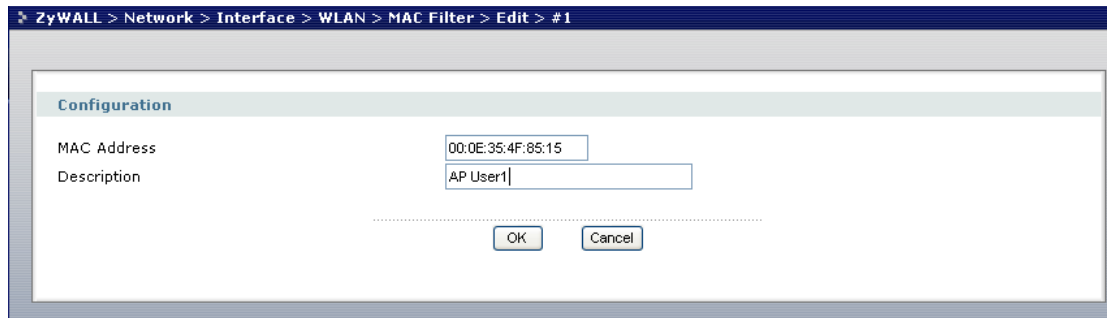
The screenshot shows the ZyWALL configuration interface for the MAC Filter settings. The breadcrumb trail is: ZyWALL > Network > Interface > WLAN > MAC Filter. The interface has tabs for Status, Port Role, Ethernet, PPP, Cellular, WLAN (selected), VLAN, Bridge, Auxiliary, and Trunk. Under the WLAN tab, there are sub-tabs for General, MAC Filter (selected), and Station Monitor.

In the **Configuration** section:

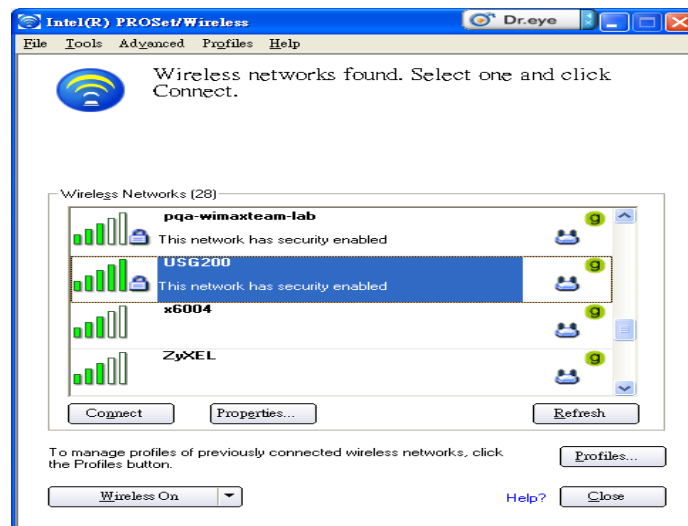
- ☒ Enable MAC Filter
- Association: Allow

Below this is a table with columns: #, MAC Address, and Description. A red box highlights the "Add" button (a plus icon) in the Description column. At the bottom, there are "Apply" and "Reset" buttons.

In this example, you assign a given MAC to **be allowed** to access the WLAN service.



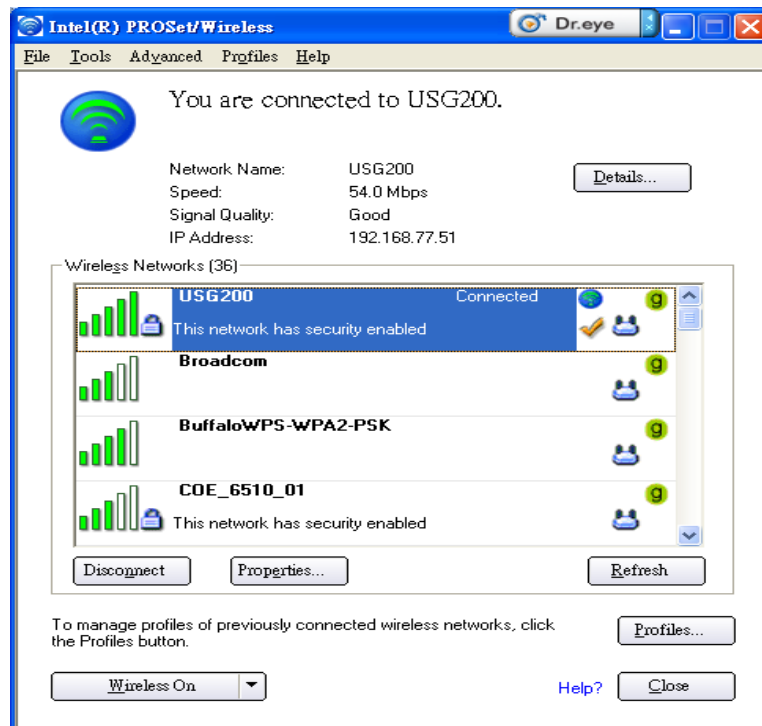
After setting the parameters in MAC filter, you can check it by using a wireless device to access the WLAN of ZyXEL USG. In client's view, you can see there is a WLAN service with SSID shown as USG200.



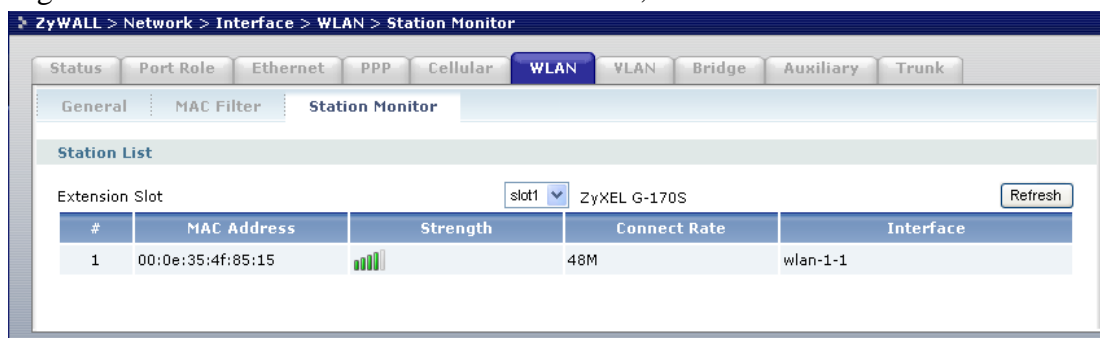
Next, client need to provide password to access this WLAN.



Next, you can see the successful connection information in client.



You can also check the WLAN status in USG to see which client is accessing WLAN by clicking Network>Interface>WLAN>Station Monitor,



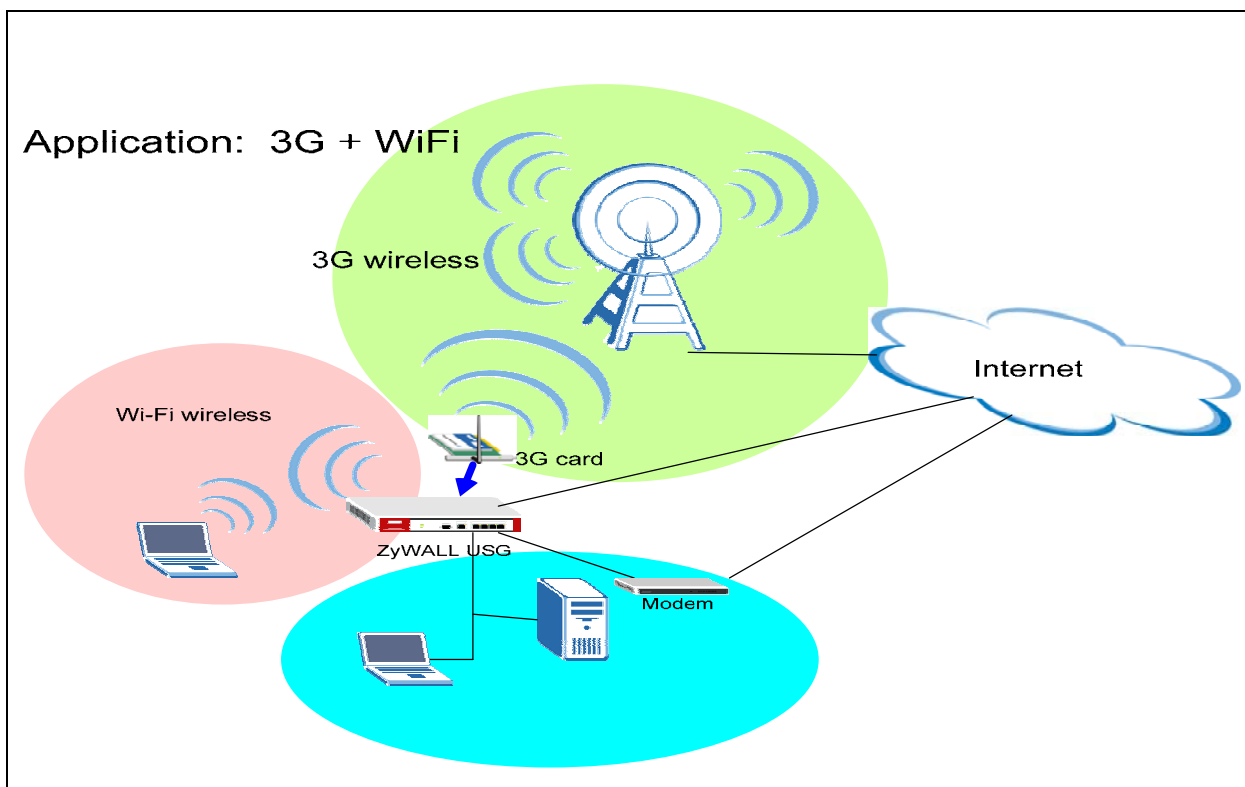
## 2.4 Mobility Internet Access

You may have experienced the need of Internet access in a location where wired connection is difficult to deploy, e.g. in countryside or mountain. Or you are just in a public environment without Internet access, like in a park, on a bus, in a train or metropolitan subway, etc... Or you may temporarily need Internet access when you are in your exhibition booth and need Internet access for some demonstration. ZyWALL USG 2000 is especially designed for the mobility Internet access; it is light to carry everywhere and can utilize a 3G card for dial up to get the Internet access. Besides, you could utilize the embedded wireless card to provide

wireless access for your LAN users.

Not only the mobility, you could also use ZyWALL USG 2000 as your WAN backup in the small office or SOHO. You could further choose a certain load balancing mechanism to perform dual WAN access.

In summery, you could utilize the 3G wireless access for your primary WAN, or backup WAN, or work with your primary WAN(Ethernet or PPP) together as a dual WAN application.



#### **2.4.1 Utilize 3G Wireless for Accessing the Internet**

ZyWALL USG 2000 utilize the benefits of 3G wireless network to combine with the wire WAN links. For small business environment, they can use 3G wireless as their backup WAN link once the wire WAN link encounters disconnection. At that moment, 3G wireless network can be active to take over the function of wire WAN.

We will show you how to configure this function step-by-step.



### 2.4.1.1 Configuration procedure

- Install 3G card
- Setting parameters 3G card in ZyXEL USG 2000

Step 1. Plug the 3G card to ZyWALL USG 2000's card slot before powering on the ZyWALL USG device.

In this figure, it shows the 3G card, Sierra Wireless AC850, has been installed in ZyWALL USG.

Interface Status Summary					
Name	Status	HA Status	Zone	IP Address	Action
wan1	Down	n/a	WAN	0.0.0.0	Renew
wan2	Down	n/a	WAN	0.0.0.0	Renew
opt	Down	n/a	OPT	0.0.0.0	n/a
lan1	Up	n/a	LAN1	192.168.1.1	n/a
lan2	Down	n/a	LAN2	10.59.0.1	n/a
dmz	Down	n/a	DMZ	192.168.2.1	n/a
cellular1	SIM locked-PIN	n/a	n/a	0.0.0.0	Unlock
aux	Inactive	n/a	WAN	0.0.0.0	n/a

Extension Slot		
Slot	Device	Status
PC Card	Sierra Wireless AC 850	
USB 1	none	
USB 2	none	

Step 2. Login the GUI. After the system boots up, you can see the 3G card information on the home page. Make sure there is no "Error" message in "3G Card IMEI" and "SIM Card IMSI" fields. Otherwise, you need to re-install the 3G card and the SIM card and make sure they are properly installed. Please refer to the quick start guide if you need to troubleshoot because of an error message.

Step 3. Click the GUI menu ZyWALL> Network> Interface> Cellular.



Step 4. Then, choose the edit icon to configure the APN, username, password, PIN code, phone number, the authentication type and other settings you have got from your service provider. Click the **Apply** button.

**General Settings**

☒ Enable Interface

**Interface Properties**

Interface Name: cellular1  
Zone: WAN  
Extension Slot: PC Card  
Connected Device: Sierra Wireless AC875  
Description:  (Optional)

**Connectivity**

☐ Nailed-Up  
Idle timeout:  (Seconds)

**ISP Settings**

Profile Selection: ☒ Device ☐ Custom  
Profile 1  
APN:   
Dial String:   
Authentication Type: None

Step 5. Next, you have to enter the PIN code for ZyWALL USG 2000 to dial up the 3G wireless network. Also, you can apply this 3G wireless network as backup WAN link. So, you need to select the checkbox “add this interface to Trunk to allow WAN load balance.”

SIM Card Setting

PIN Code

Interface Parameters
Advanced

Egress Bandwidth
 Kbps

Connectivity Check

☐ Enable Connectivity Check

Check Method

Check Period
 (5-30 seconds)

Check Timeout
 (1-10 seconds)

Check Fail Tolerance
 (1-10)

☒ Check Default Gateway

☐ Check this address
 (Domain Name or IP Address)

Related Setting

☒ Add this interface to [Trunk](#) to allow WAN load balance.

Configure [Policy Route](#)

More Settings

Step 6. Next, click the Trunk tab to edit the WAN\_Trunk detail.




Status
Port Role
Ethernet
PPP
Cellular
WLAN
VLAN
Bridge
Auxiliary
**Trunk**

General Settings

☐ Enable Link Sticking

Timeout  (30-3600 seconds)

Configuration

Name	Algorithm	Modify
WAN_TRUNK	lbf	
WAN_TRUNK2	lbf	
WAN_TRUNK3	lbf	
WAN_TRUNK4	lbf	
WAN_TRUNK5	lbf	

Apply
Reset

Step 7. In this step, you can select the types of load balancing algorithm. Then, edit the content of “aux.”

**ZyWALL > Network > Trunk > Edit > #1**

**Trunk Members**

Name: WAN\_TRUNK  
Load Balancing Algorithm: Least Load First

#	Member	Mode	Ingress Bandwidth	Egress Bandwidth	
1	wan1	Active	1048576 Kbps	1048576 Kbps	
2	wan1_ppp	Active	1048576 Kbps	1048576 Kbps	
3	wan2	Active	1048576 Kbps	1048576 Kbps	
4	wan2_ppp	Active	1048576 Kbps	1048576 Kbps	
5	aux	Passive	1048576 Kbps	0 Kbps	
6	cellular1	Active	1048576 Kbps	1048576 Kbps	

OK Cancel

Step 8. Within this step, you can assign the mode of load balance for the 3G wireless network. Passive mode means that the 3G network will be backup link once the main WAN link fails.

**ZyWALL > Network > Trunk > Edit > #1**

**Trunk Members**

Name: WAN\_TRUNK  
Load Balancing Algorithm: Least Load First

#	Member	Mode	Ingress Bandwidth	Egress Bandwidth	
1	wan1	Active	1048576 Kbps	1048576 Kbps	
2	wan1_ppp	Active	1048576 Kbps	1048576 Kbps	
3	wan2	Active	1048576 Kbps	1048576 Kbps	
4	wan2_ppp	Active	1048576 Kbps	1048576 Kbps	
5	cellular1	Passive	1048576 Kbps	1048576 Kbps	

OK Cancel

Step 9. You can also see more detail status of 3G network by click the icon of “celluar1.” In this figure, it shows the connection status is excellent.



The image shows a screenshot of a web interface titled "Cellular Device Status". It contains a table with two columns: "Item" and "Value". The table lists various cellular network parameters and their current status.

Item	Value
Extension Slot	PC Card
Service Provider	Chunghwa Telecom
Cellular System	UMTS
Signal Strength	-69 dBm
Signal Quality	Excellent 
Device Manufacturer	Sierra Wireless
Device Model	AC875
Device Firmw. 850	H1_0_0_9ACAP
Device IMEI / ESN	352822012857919
SIM Card IMSI	466923101455327

Then the 3G wireless card will be dialed up automatically when WAN1 is not available. If you check the "Nailed-up" option as shown in the figure above, the system will automatically dial up the 3G Internet access even if WAN1 is available. Then you will see the process in logs as following.

Step 10. Now, you can verify whether the backup link work well. By plugging out of WAN link to make link failure and check the WAN status in ZyWALL USG. In the following figure, it shows that both of WAN services are down. Only the cellular network provided by 3G is working.

In the following figure, it presents that WAN service is working before plugging out the main WAN link, WAN1. Then, the WAN1 link fails. There is no ICMP response and get time out. After a while, the backup link, cellular network, take over the WAN link. Hence, ZyWALL USG receives the ICMP responses again.

```
C:\Documents and Settings\Rex Lee>ping 168.95.1.1 -t

Pinging 168.95.1.1 with 32 bytes of data:

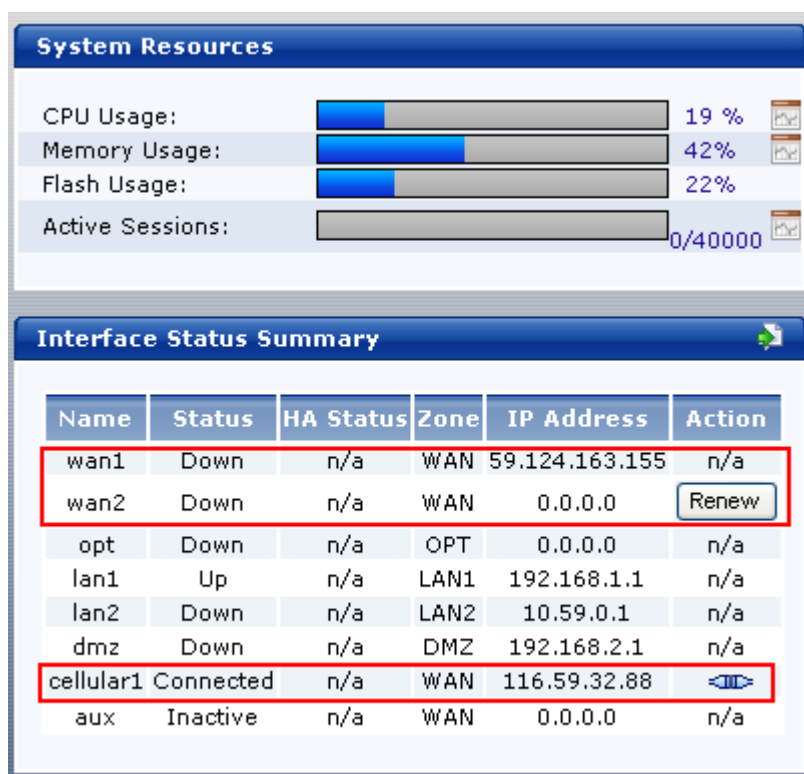
Reply from 168.95.1.1: bytes=32 time=9ms TTL=246
Reply from 168.95.1.1: bytes=32 time=9ms TTL=246
Reply from 168.95.1.1: bytes=32 time=9ms TTL=246
Reply from 168.95.1.1: bytes=32 time=9ms TTL=246
Request timed out.
Request timed out.
Request timed out.
Reply from 168.95.1.1: bytes=32 time=245ms TTL=244
Reply from 168.95.1.1: bytes=32 time=254ms TTL=244
Reply from 168.95.1.1: bytes=32 time=242ms TTL=244
Reply from 168.95.1.1: bytes=32 time=242ms TTL=244
Reply from 168.95.1.1: bytes=32 time=260ms TTL=244
Reply from 168.95.1.1: bytes=32 time=258ms TTL=244
Reply from 168.95.1.1: bytes=32 time=287ms TTL=244
Reply from 168.95.1.1: bytes=32 time=256ms TTL=244
Reply from 168.95.1.1: bytes=32 time=264ms TTL=244
Reply from 168.95.1.1: bytes=32 time=243ms TTL=244
Reply from 168.95.1.1: bytes=32 time=261ms TTL=244

Ping statistics for 168.95.1.1:
    Packets: Sent = 18, Received = 15, Lost = 3 (16% loss),
Approximate round trip times in milli-seconds:
    Minimum = 9ms, Maximum = 287ms, Average = 189ms
Control-C
^C
C:\Documents and Settings\Rex Lee>
```

```
root@nessus:~
login as: admin
Using keyboard-interactive authentication.
Password:
Bad terminal type: "xterm". Will assume vt100.
Router> packet-trace interface cellular1
tcpdump: listening on ppp13
02:42:03.647372 116.59.7.82 > 168.95.1.1: icmp: echo request
02:42:04.925853 168.95.1.1 > 116.59.7.82: icmp: echo reply (DF)
02:42:04.927178 116.59.7.82 > 168.95.1.1: icmp: echo request
02:42:05.255837 168.95.1.1 > 116.59.7.82: icmp: echo reply (DF)
02:42:05.930704 116.59.7.82 > 168.95.1.1: icmp: echo request
02:42:06.175789 168.95.1.1 > 116.59.7.82: icmp: echo reply (DF)
02:42:06.932176 116.59.7.82 > 168.95.1.1: icmp: echo request
02:42:07.215738 168.95.1.1 > 116.59.7.82: icmp: echo reply (DF)

16 packets received by filter
0 packets dropped by kernel
Router> █
```

Step 11. If dialed up successfully, you can see the GUI home page as shown below. You will get the "Cellular1 is connected" and "3G card's signal strength" messages in the latest alerts.



## 3. Seamless Incorporation

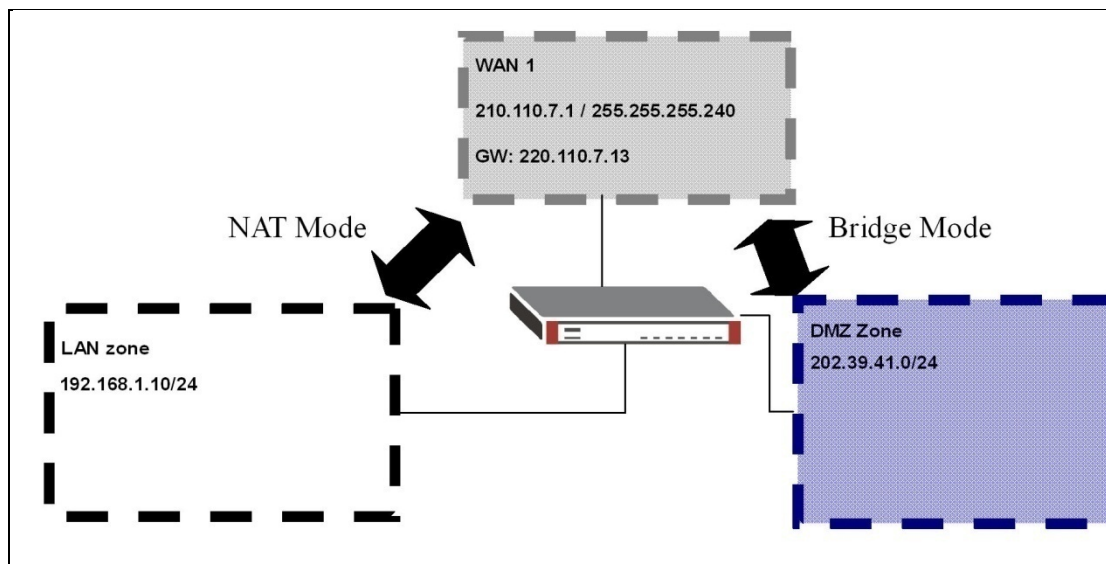
With its robust networking functionalities, ZyWALL USG 2000 is easy to integrate into existing network infrastructure. You can easily implement the following applications. They are “Transparent firewall”, “Transparent IDP” and “Network Partitioning using VLAN”.

### 3.1 Transparent Firewall

With transparent firewall, you do not need to change the IP addressing scheme of your existing network topology. What you need to do is to insert ZyWALL USG 2000 into your existing network environment. Bridge the ports you think that need to be included in this bridge interface. Apply the security policies that you want. And that will be it. Moreover, ZyWALL USG 2000 supports working as bridge mode and router mode at the same time; which means that they can co-exist.

#### 3.1.1 Bridge mode & Router (NAT) mode co-exist

Here is an example:



DMZ and WAN zone can be bridged, so that servers in the DMZ zone can keep using the same public IP address (as those in WAN zone) for effortless IP management. Additionally, IP addressing in LAN zone is private IP segments. Thus, we apply NAT, which is the router mode here. To make this scenario works the follow the configuration steps as stated below:



- 1) Login the ZyWALL USG 2000 GUI and setup the WAN1 interface for internet connection and manually assign a static IP. The configuration path is ZyWALL USG 2000 **ZyWALL > Network > Interface > Edit > Configuration > wan1**.

Please use this same method to assign IP for the LAN and DMZ interface.

**ZyWALL > Network > Interface > Edit > Configuration > wan1**

**Configuration** Wizard

**General Settings**

☒ Enable Interface

**Interface Properties**

Interface Name: wan1  
 Port: P1  
 Zone: WAN  
 MAC Address: 00:19:CB:7F:30:C1  
 Description: (Optional)

**IP Address Assignment**

☐ Get Automatically  
☒ Use Fixed IP Address

IP Address: 210.110.7.1  
 Subnet Mask: 255.255.255.240  
 Gateway: 210.110.7.13 (Optional)  
 Metric: 0 (0-15)

- 2) Switch to **Network > Interface > Bridge**, add a new Bridge Interface. First we enable this interface and give it a name, place the available ports into the member ports and make them become the member of this bridge interface.

**ZyWALL > Network > Interface > Bridge**

Status Port Role Ethernet PPP Cellular WLAN VLAN **Bridge** Auxiliary Trunk

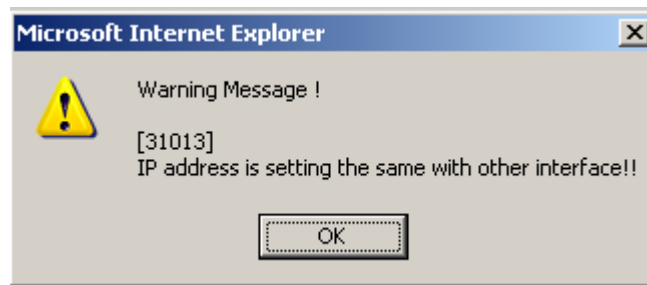
**Configuration**

#	Name	IP Address	Member	

Apply Reset

- 3) Moreover, don't forget to set the WAN IP information here since it is a "Bridge mode & Router (NAT) mode co-exist" example and the NAT mode will need it. Here, the bridge mode looks most likely a routing bridge mode instead of the pure bridge mode. Thus, it needs an IP address. You may use the same IP address that it used in the WAN interface,

however you will get a warning message like below.



If you got more than one IP, you can pick the other one here.

**ZyWALL > Network > Interface > Bridge > Edit > #1**

**General Settings**

☒ Enable Interface

**Interface Properties**

Interface Name: br1  
 Zone: ▼  
 Description:  (Optional)

**Member Configuration**

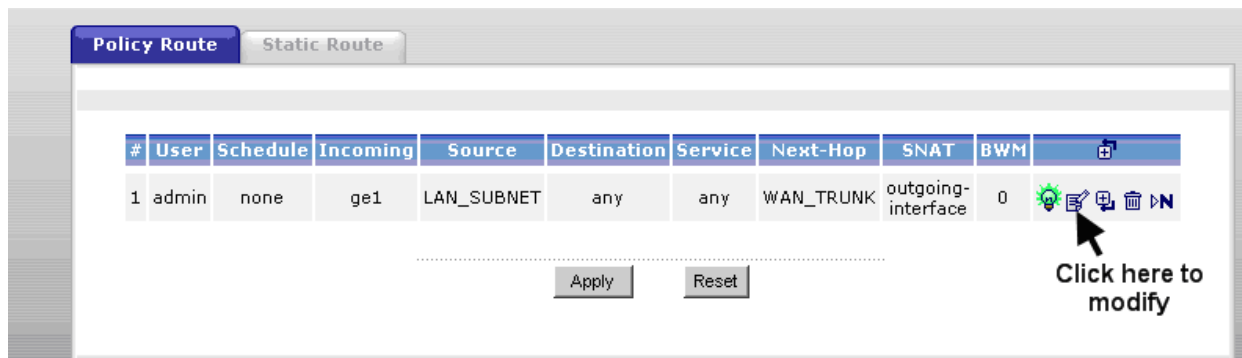
Available: wan2, opt, lan2  
 Member: dmz, lan1, wan1

**IP Address Assignment**

☐ Get Automatically  
☒ Use Fixed IP Address

IP Address:   
 Subnet Mask:   
 Gateway:  (Optional)(Required for transparent mode.)  
 Metric:  (0-15)

3) Switch to **Network > Routing > Policy Route**, to modify the default rule there. The default rule is for the Router Mode (NAT Mode). Since we have two different modes co-existing here, we need to make some adjustments to this rule.



Here we need to modify the “Next-Hop” from “WAN\_TRUNK” to “Interface” of the Bridge interface (br1) that we just created.

Then click “OK” at the bottom to save the changes.

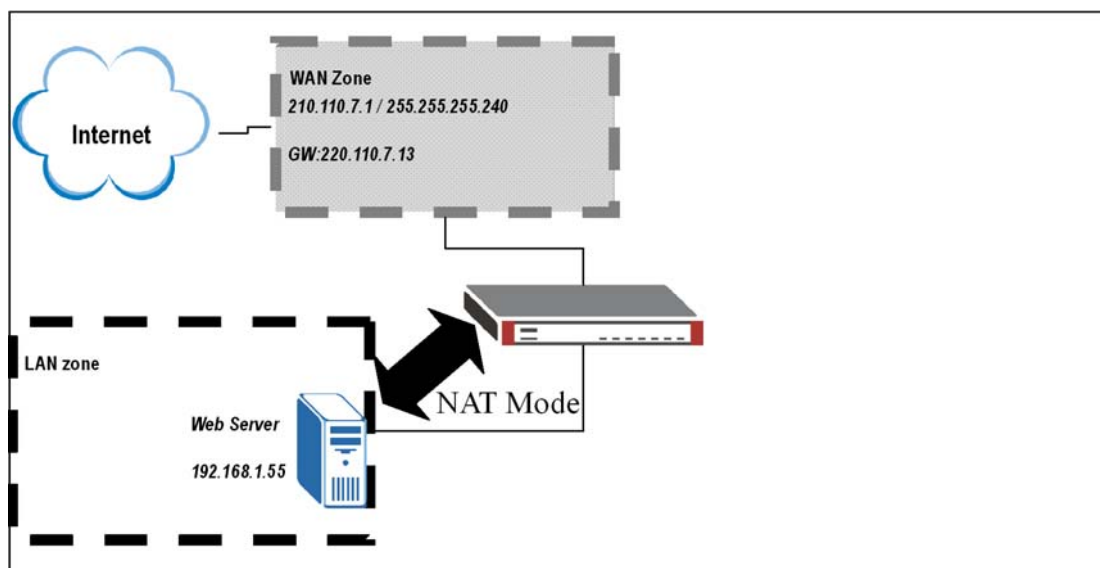
### Tips for application:

Disable the Firewall to test the connectivity.

Every time you make a change, don’t forget to click the “apply” button

### 3.1.2 NAT & Virtual Server

Here is an example:



There is a web server located in the DMZ zone. The virtual Server setting in ZyWALL USG 2000 is required here for people outside of WAN to access the Web pages located on the Web

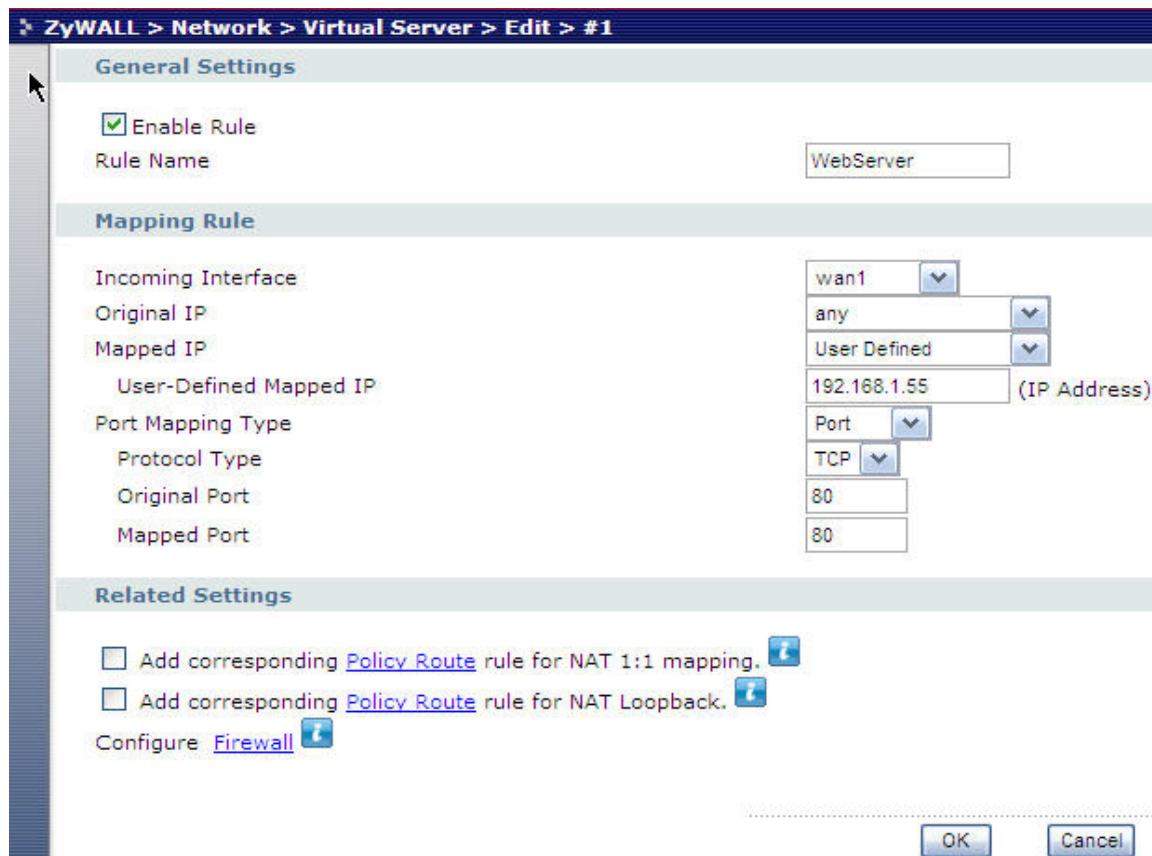
Server in the DMZ zone.

To make this scenario work; follow the configuration steps stated below:

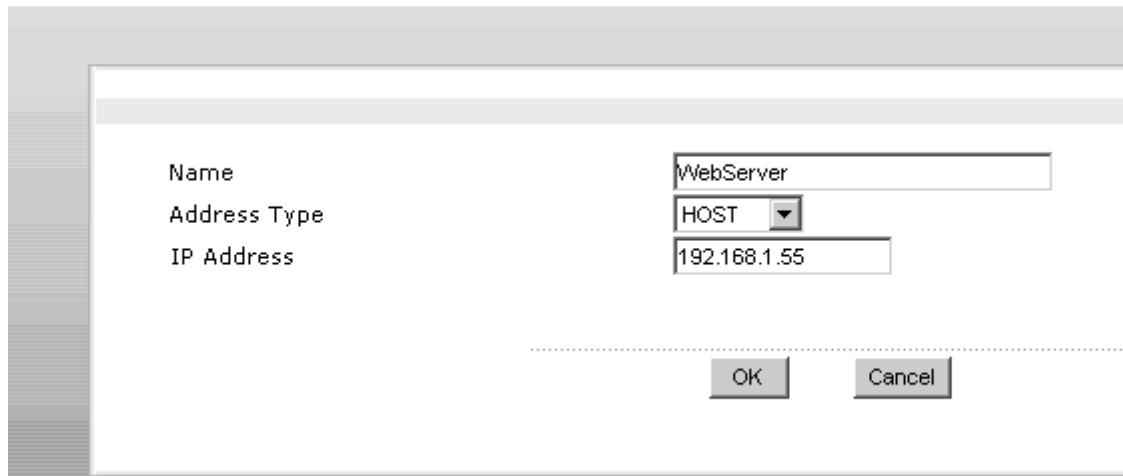
- 1) Login ZyWALL USG 2000 GUI and setup the WAN1 interface for internet connection and manually assign a static IP. Login ZyWALL USG 2000 GUI and go to **Network > Interface > Edit > WAN1**



- 2) Switch to **General > Network > Virtual Server** and add a new Virtual Server. Fill in the mapping information. In our example here, since WAN1 is our WAN port, we are going to map any IP from the WAN port to our internal Web Server, which is 192.168.1.55. And in this case, our web server is running on TCP 80, therefore, we pick TCP 80 for our mapping.



- 4) Switch to **Object > Address**, and add a new address object for your Web server.



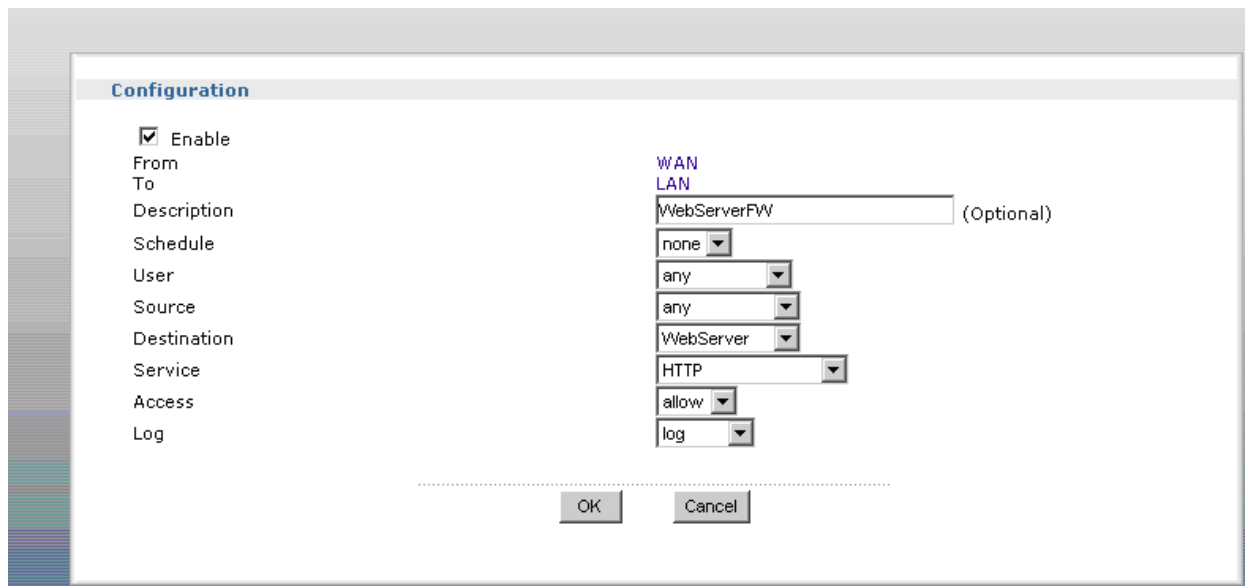
Name: WebServer

Address Type: HOST

IP Address: 192.168.1.55

OK Cancel

- 4) Switch to **Firewall > Firewall Rule**, and add a new firewall rule for your virtual server. Since it is a web server, we choose “HTTP” as the Service and “Allow” for the access action.



**Configuration**

☒ Enable

From: WAN

To: LAN

Description: WebServerFW (Optional)

Schedule: none

User: any

Source: any

Destination: WebServer

Service: HTTP

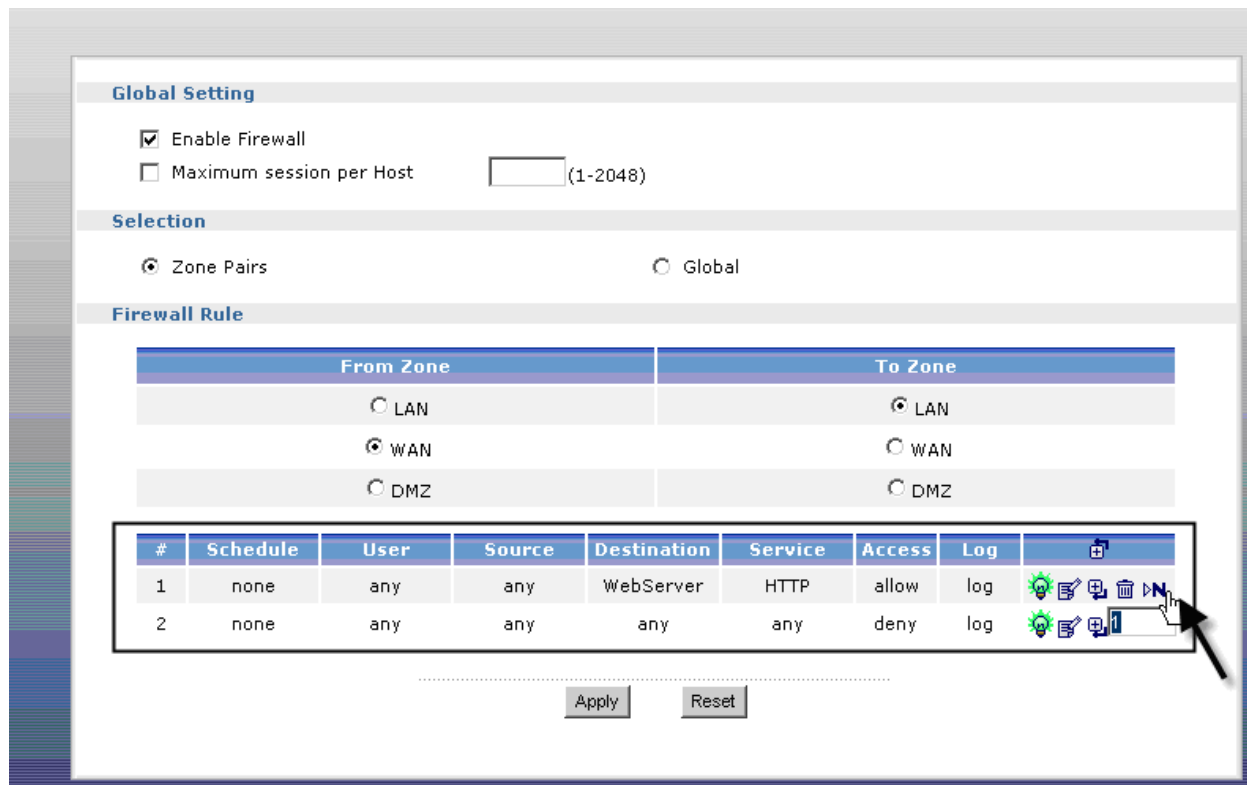
Access: allow

Log: log

OK Cancel

### Tips for application:

Do not forget to place your rule before the default “Deny all” Rule in the **WAN-to-LAN** direction.



**Global Setting**

☒ Enable Firewall



☐ Maximum session per Host  (1-2048)

**Selection**

☒ Zone Pairs ☐ Global

**Firewall Rule**

From Zone		To Zone	
<input type="radio"/> LAN	<input checked="" type="radio"/> LAN		
<input checked="" type="radio"/> WAN	<input type="radio"/> WAN		
<input type="radio"/> DMZ	<input type="radio"/> DMZ		

#	Schedule	User	Source	Destination	Service	Access	Log	
1	none	any	any	WebServer	HTTP	allow	log	
2	none	any	any	any	any	deny	log	

Apply Reset

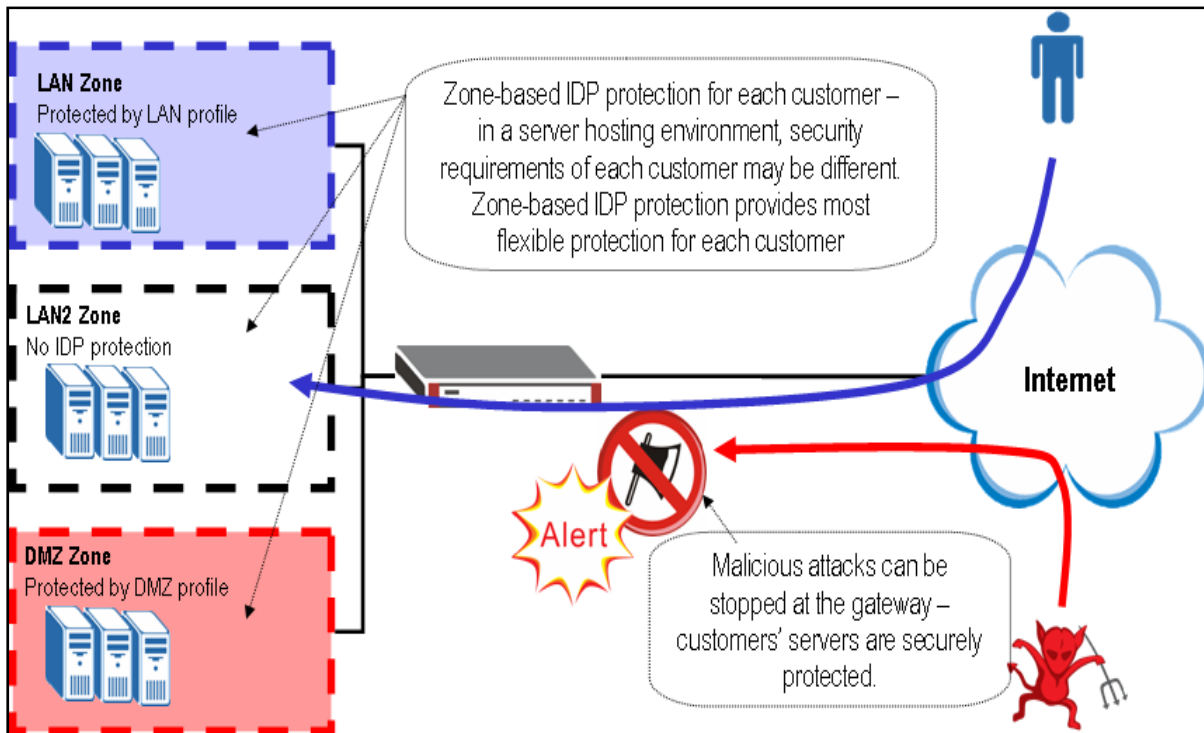
## 3.2 Zone-based IDP Protection

ZyWALL USG 2000 comes with a state of art Intrusion Detection Protection System (IDP) which can provide comprehensive and easy to use protection against current and emerging threats at both the application and network layer. Using industry recognized state of art detection and prevention techniques; With ZyWALL USG 2000 IDP system, IT manager can apply unique protection profile to each network segment or Zone. And it is best for MSP environment since it can effectively identify and stop network and application-level attacks before they inflict any damage, minimizing the time and costs associated with the intrusions.

The ZyWALL USG 2000 Zone-based IDP can be implemented in a server-hosting environment. Usually, in a server hosting environment, security requirements of each customer may be different. As multiple IDP protection profiles can be applied to different Zones for each customer, ZyWALL USG 2000 Zone-based IDP protection provides the most flexible protection for each customer. Malicious attacks can be stopped at the gateway – customers' servers are securely protected and a notification alert can be sent to the involved parties or individuals.

### 3.2.1 Applying Zone-Based IDP to ZyWALL USG 2000

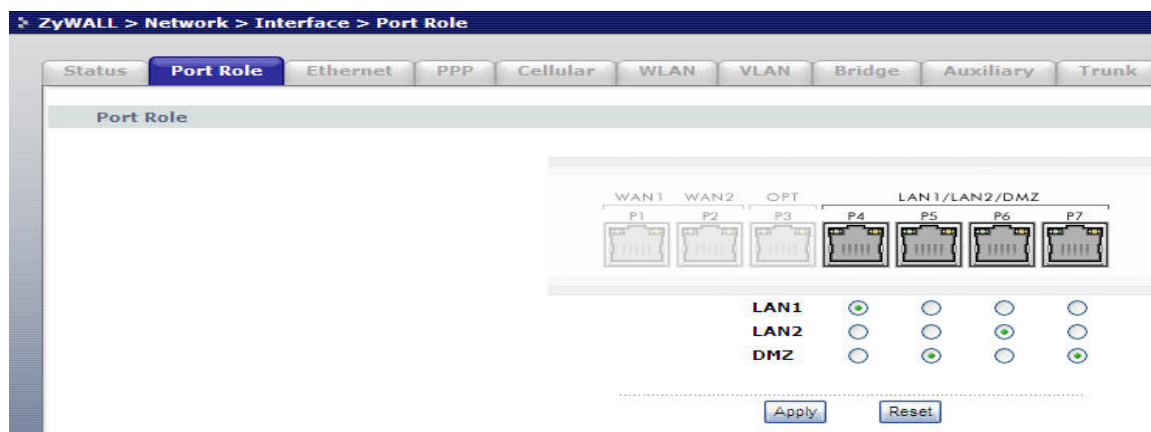
Here is an example:



To fulfill the above scenario, you will need three networks on P4, P5 and P6. Then you can apply different IDP profiles to them.

Here are the steps:

- 1) Login the ZyWALL USG 2000 GUI and go to **Network > Interface > Port Role**. Since we are going to have three intra-networks in our scenario, we will make P5 and P6 another two networks for DMZ and LAN2.



- 2) Go to **Network > Interface > Ethernet** and click the “edit” icon to modify the LAN1 (P4) settings.

**ZyWALL > Network > Zone**

Configuration			
Name	Block Intra-zone	Member	Modify
LAN1	No	lan1	
LAN2	No	lan2	
WAN	Yes	wan1, wan2, wan1_ppp, wan2_ppp, aux	
DMZ	Yes	dmz	
OPT	Yes	opt, opt_ppp	
SSL_VPN	Yes		
IPSec_VPN	Yes		

- 11) Now, we can assign an IP domain to P4 and another one for P5. Other settings are all optional. In this example, we keep the default values which will disable the DHCP Server in these two interfaces.

**ZyWALL > Network > Interface > Edit > Configuration > dmz**

**General Settings**

☒ Enable Interface

**Interface Properties**

Interface Name: dmz  
 Port: P5, P7  
 Zone: DMZ  
 MAC Address: 00:19:CB:7F:30:C6  
 Description:  (Optional)

**IP Address Assignment**

IP Address:   
 Subnet Mask:

**Interface Parameters**

Egress Bandwidth:  Kbps

**DHCP Setting**

DHCP:



**ZyWALL > Network > Interface > Edit > Configuration > lan2**

**General Settings**

☒ Enable Interface

**Interface Properties**

Interface Name: lan2  
 Port: P6  
 Zone: LAN2  
 MAC Address: 00:19:CB:7F:30:C5  
 Description:  (Optional)

**IP Address Assignment**

IP Address: 192.168.3.1  
 Subnet Mask: 255.255.255.0

**Interface Parameters**

Egress Bandwidth: 1048576 Kbps

**DHCP Setting**

DHCP: None

Tips: You do not need a Gateway here since this interface is directly connected to ZyWALL USG 2000.

12) Your final summary of the Ethernet Interfaces should look like the figure below.

**ZyWALL > Network > Interface > Ethernet**

Status Port Role **Ethernet** PPP Cellular WLAN VLAN Bridge Auxiliary Trunk

**Configuration**








#	Name	IP Address	Mask	Modify
1	wan1	STATIC -- 167.35.4.3	255.255.255.0	
2	wan2	STATIC -- 10.59.1.45	255.255.255.0	
3	opt	STATIC -- 0.0.0.0	0.0.0.0	
4	lan1	STATIC -- 192.168.1.1	255.255.255.0	
5	lan2	STATIC -- 10.59.0.1	255.255.255.0	
6	dmz	STATIC -- 192.168.2.1	255.255.255.0	

Apply Reset

13) Now, you will need to setup your DMZ Zone and LAN2 Zone. Go to **Configuration > Network > Zone**.

**ZyWALL > Network > Zone**

Configuration

Name	Block Intra-zone	Member	Modify
LAN1	No	lan1	
LAN2	No	lan2	
WAN	Yes	wan1, wan2, wan1_ppp, wan2_ppp, aux	
DMZ	Yes	dmz	
OPT	Yes	opt, opt_ppp	
SSL_VPN	Yes		
IPSec_VPN	Yes		

14) Although the DMZ Zone is already there, Click the “edit” icon of DMZ Zone and then select the P5 interface as DMZ zone.

**ZyWALL > Network > Zone > Edit > #4**

**Group Members**

Name DMZ

☒ Block Intra-zone Traffic 

**Member List**

Available Interface

>>

<<

Member

INTERFACE / dmz

15) Before you apply the IDP profiles, you need to make sure that the IDP Service on your ZyWALL USG 2000 is licensed.

**ZyXEL**

**Status**

Refresh Interval: None [Refresh Now]

**Device Information**

System Name: zywall-usg-200  
 Model Name: ZyWALL USG 200  
 Serial Number: S080Z05014416  
 MAC Address Range: 00:19:c0:7f:30:c1 ~ c6  
 Firmware Version: 2.10(AQU.0)b3 |2008-01-11 19:0

**System Status**

System Uptime: 00:40:55  
 Current Date/Time: 2008-03-14 03:08:05  
 VPN Status: [OK]  
 DHCP Table: [OK]  
 Port Statistics: [OK]  
 Current Login User: admin (unlimited/00:04:59)  
 Number of Login Users: 1  
 Boot Status: OK

**System Resources**

CPU Usage: 7 %  
 Memory Usage: 42%  
 Flash Usage: 22%  
 Active Sessions: 0/40000

**Interface Status Summary**

Name	Status	HA Status	Zone	IP Address	Action
wan1	Down	n/a	WAN	59.124.163.155	n/a
wan2	Down	n/a	WAN	0.0.0.0	Renew
opt	Down	n/a	OPT	0.0.0.0	n/a
lan1	Up	n/a	LAN1	192.168.1.1	n/a
lan2	Down	n/a	LAN2	10.50.0.1	n/a

**Licensed Service Status**

IDP

- License Status/Remaining days: [Not Licensed](#) / 0
- Signature Version: V2.026 |2007/06/20 17:08:10
- Last Update Time: n/a
- Total Signature Number: 2020

Anti-Virus

- License Status/Remaining days: [Not Licensed](#) / 0
- Signature Version: V1.055 |2007-07-05 20:58:13
- Last Update Time: n/a
- Total Signature Number: 5936

Content Filter

- License Status/Remaining days: [Not Licensed](#) / 0

Message: Ready.

- 16) If your IDP is not licensed, go to the Registration page. You can either login using your existing myZyXEL.com account or apply for a new one. Each ZyWALL USG 2000 comes with a 30 days free trial on IDP Service. Just register your ZyWALL USG 2000 and your ZyWALL USG 2000 will receive the license automatically. Here a page which is already registered is shown.

ZyWALL > Licensing > Registration

Registration
Service

General Settings

This device is not registered to myZyXEL.com. Please enter information below to **register** your device.  
If you don't have myZyXEL.com account, please select "new myZyXEL.com account" below. If you have  
a myZyXEL.com account, but you forget your User Name or Password, please go to [www.myZyXEL.com](http://www.myZyXEL.com)  
for help.

☒ new myZyXEL.com account
☐ existing myZyXEL.com account

User Name
Password
Confirm Password
E-Mail Address
Country Code

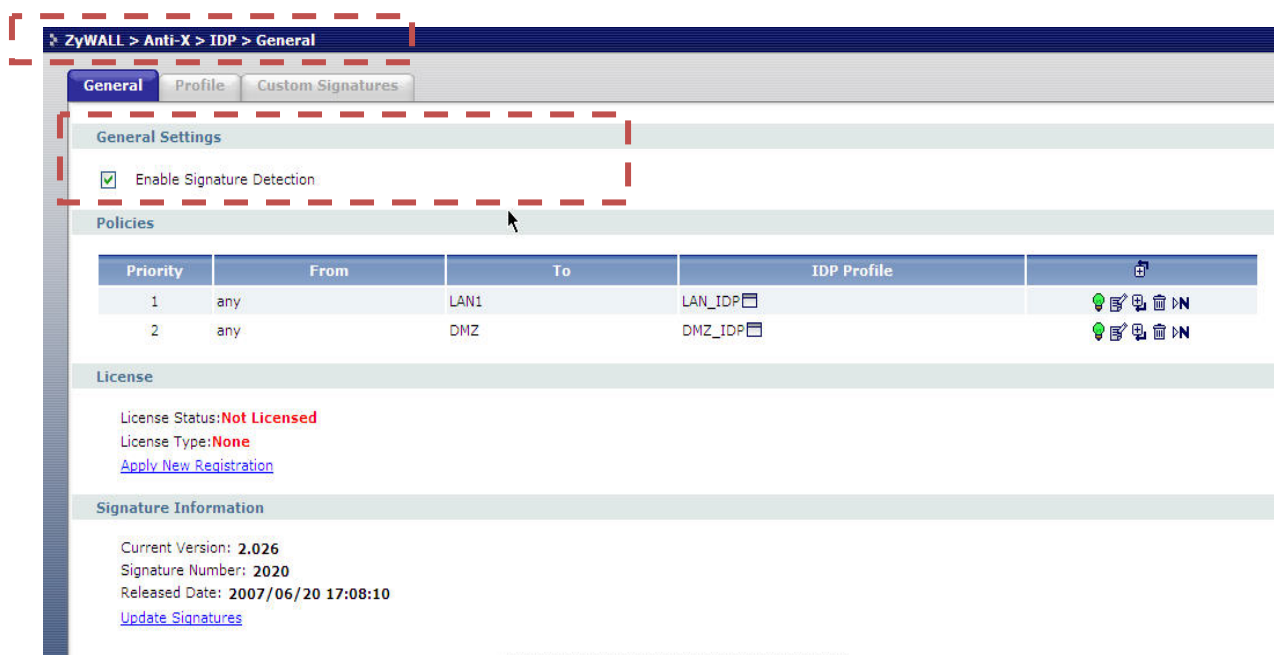
Select

you can click to check if username exists

Trial Service Activation

☐ Anti-Virus Signature Service
☐ ZyXEL ICSA Anti-Virus Engine
☐ Kasperskey Anti-Virus Engine
☐ IDP/AppPatrol Signature Service
☐ Content Filter Category Service

17) Now, go to **Anti- X > IDP**. Enable the IDP check box to activate the IDP service on your ZyWALL USG 2000.



18) Here, all the Zones are shown. As you can see, two of them have IDP enabled by default. According to the scenario, LAN Zone needs a LAN Profile, DMZ Zone needs a DMZ Profile and LAN2 Zone does not need any IDP protection at all. And here is everything you need.

### 3.3 Anti-spam on the ZyWALL USG 2000

Nowadays, electronic mail system brings us many benefits, ex: convenience, low cost, and quickly delivery, to achieve efficient communication. Because of those obvious features, most of individuals and commercial companies are widely applied in our daily life and commercial environment. However, it will be annoying to receive the anonymous or unregistered mails; especially you do not want to receive them. Those kinds of emails are called spamming emails. In commercial appliance, it will consume unnecessary network bandwidth, server loading and labor cost. Hence, anti-spam is a major requirement for business to protect their network environment. Now, this feature is built in ZyWALL 2000.

Anti-spam provides an efficient method for enterprise to restrict flooding spam mails.

### **3.3.1 How Anti-Spam works on ZyWALL USG**

There are two ways to implement the anti-spam function. One is to make black list and white list; the other is to refer the black list from one credited website, this function is called as DNS-based black list (DNSBL)

### **3.3.2 Using DNSBL (DNS-based blacklist)**

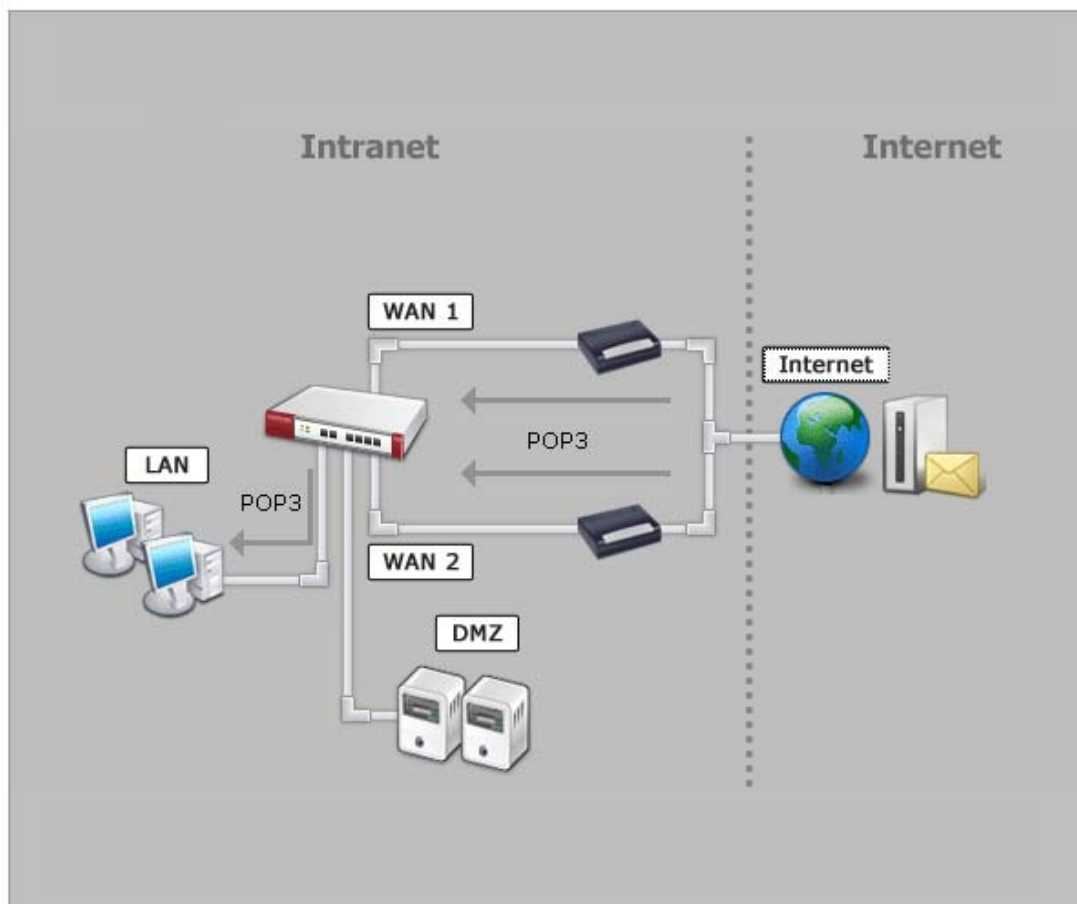
There is another way to avoid receiving spam emails. Currently, there are some websites which are responsible for monitoring and analyzing email server activity in the network. Accordingly, they maintain a list of spam email servers and publish this list. ZyWALL will check the list provided by the DNSBL website to see whether it is listed in blacklist when this function is activated.

#### **3.3.2.1 Application scenario to apply DNSBL**

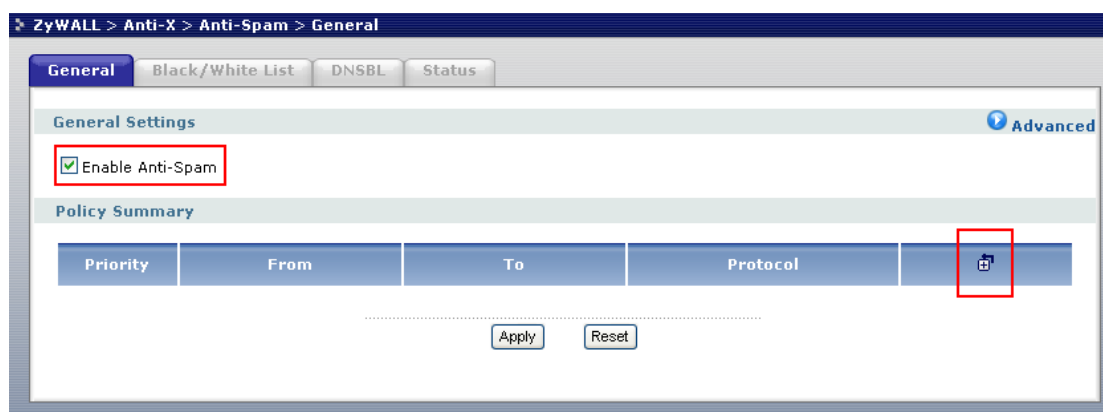
There are two scenarios for demonstrating this function. One is supposed that the company's email server is located in the DMZ and the other presents email server is located in the ISP/Internet.

##### **3.3.2.1.1 Scenario I: Email server is located in the ISP/ Internet**

In this case, the Email server is located at ISP or Internet, which means end user will receive the email through protocol POP3 only. It also means that the location of email server is outside ZyWALL USG.



First, we activate the function of anti-spam. Then, edit the content to choose which protocol we want to scan and will scan all the incoming emails based on the list provided by DNSBL website.



Here, we select “POP3” in the option of “protocol to scan.” Then, choose the check DNSBL checkbox in the option of “scan options.”

**ZyWALL > Anti-X > Anti-Spam > General > Edit > #1**

**General Settings**

☒ Enable Policy  
Log: log

**Email Direction**

From: WAN  
To: LAN1

**Protocols to Scan**

☐ SMTP ☒ POP3

**Scan Options**

☐ Check White List  
☐ Check Black List  
☒ Check DNSBL

**Actions For Spam Mail**

SMTP: forward with tag  
POP3: forward with tag

OK Cancel

Afterwards, we click the DNSBL tab to edit the trusted DNSBL website.

**ZyWALL > Anti-X > Anti-Spam > General**

General Black/White List **DNSBL** Status

**General Settings** Advanced

☒ Enable Anti-Spam

**Policy Summary**

Priority	From	To	Protocol	
1	WAN	LAN1	POP3	⚙️ 📄 🗑️ 🔄

Apply Reset

During this step, we activate the DNSBL checking and then edit the list.

**ZyWALL > Anti-X > Anti-Spam > DNSBL**

General Black/White List **DNSBL** Status

**General Settings** Advanced

☒ Enable DNS Black List (DNSBL) Checking  
DNSBL Spam Tag: [Spam] (Optional)

**Query Timeout Setting**

Actions when Query Timeout:  
SMTP: forward with tag  
POP3: forward with tag  
Timeout Value: 5 (1-10 Seconds)  
Timeout Tag: [DNSBL Timeout] (Optional)

**DNSBL Domain List**

#	DNSBL Domain	
		⚙️

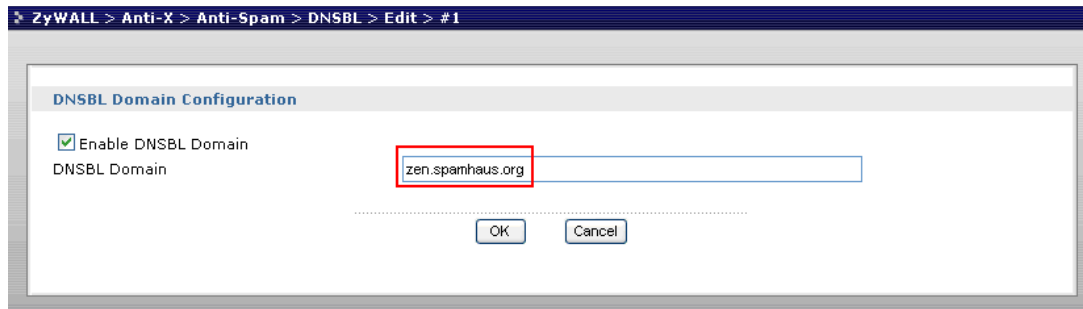
**Note:**  
Each mail relay and sender IP in mail header (under max. number) will be checked against the DNSBL domain servers listed and enabled above.

Apply Reset

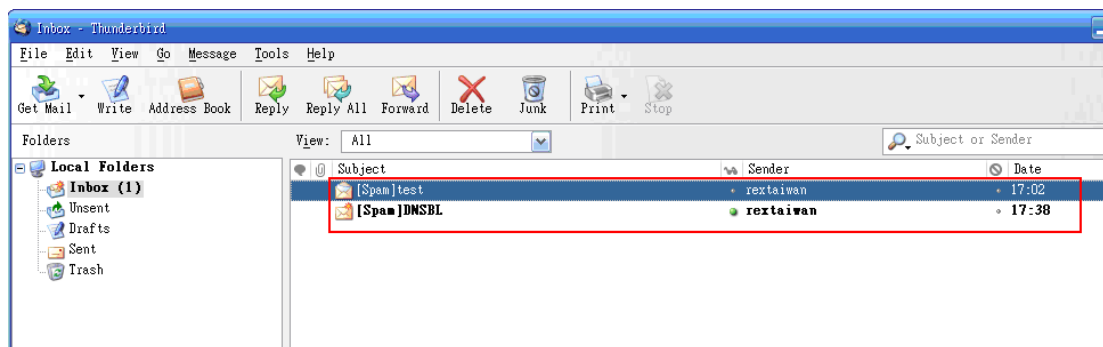
In this step, we type the DNSBL website we will refer. There are many reference DNSBL



websites.

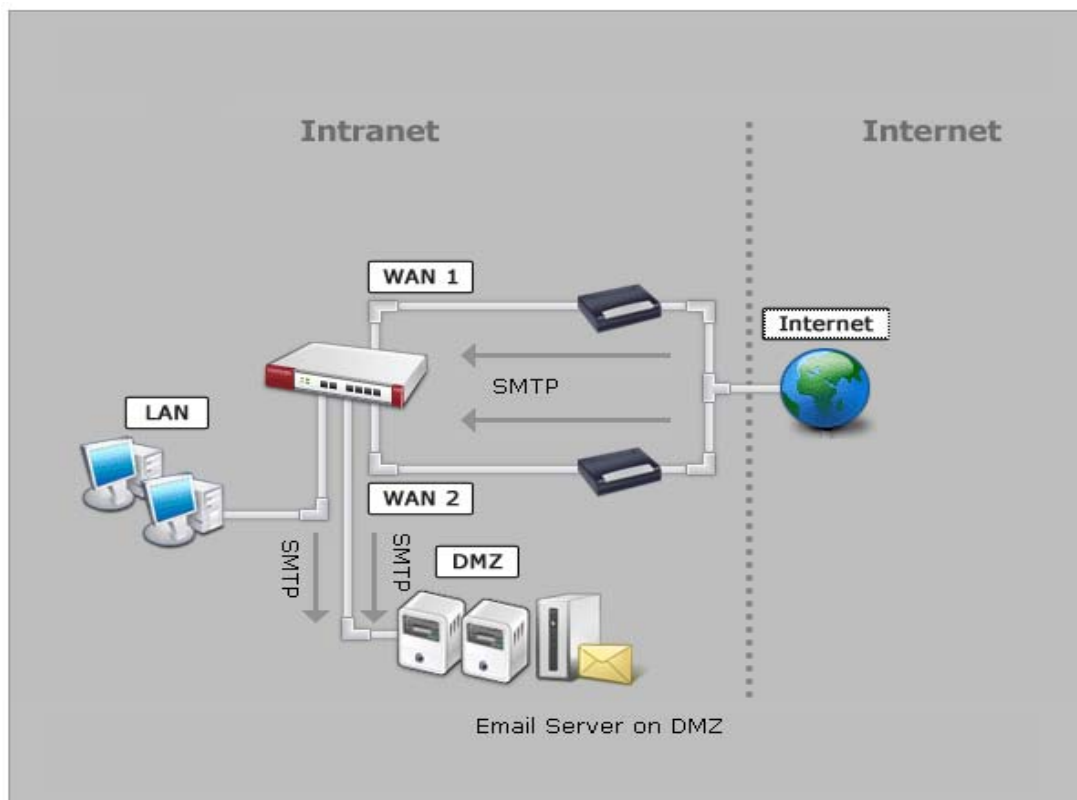


The following figure shows that ZyWALL succeed to identify the spam mail by using DNSBL function and tag the suspected spam emails. There are many DNSBL websites can be referred, for example, zen.spamhaus.org, dul.dnsbl.sorb.net, list.dsbl.org and combined.njabl.org

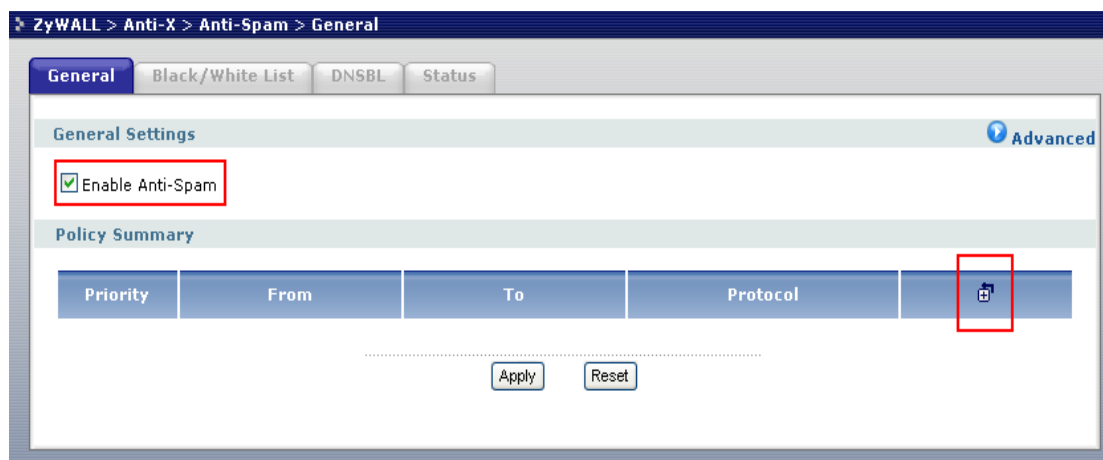


### 3.3.2.1.2 Scenario II: Company's Email server located in the DMZ

The other scenario presents that email server is located inside the intranet. It means that the email server behind the ZyWALL. In this scenario, the better way to filter spam mails is to scan them when outside email want to establish the connection with our email server. In other words, scan all incoming emails before they are received by our email server. Hence, we must scan based on the SMTP protocol and DNSBL.



First, we select the checkbox to enable the anti-spam.



Then, we choose the SMTP and option of DNSBL to be checked.

**ZyWALL > Anti-X > Anti-Spam > General > Edit > #1**

**General Settings**

☒ Enable Policy  
Log: log

**Email Direction**

From: WAN  
To: LAN1

**Protocols to Scan**

☒ SMTP ☐ POP3

**Scan Options**

☐ Check White List  
☐ Check Black List  
☒ Check DNSBL

**Actions For Spam Mail**

SMTP: forward with tag  
POP3: forward with tag

OK Cancel

Next, you select the tab of DNSBL to configure more details.

**ZyWALL > Anti-X > Anti-Spam > General**

General Black/White List **DNSBL** Status

**General Settings** Advanced

☒ Enable Anti-Spam

**Policy Summary**

Priority	From	To	Protocol
1	WAN	LAN1	POP3

Apply Reset

In the tab of DNSBL, we activate the DNSBL checking and then edit the list.

**ZyWALL > Anti-X > Anti-Spam > DNSBL**

General Black/White List **DNSBL** Status

**General Settings** Advanced

☒ Enable DNS Black List (DNSBL) Checking  
DNSBL Spam Tag: [Spam] (Optional)

**Query Timeout Setting**

Actions when Query Timeout:  
SMTP: forward with tag  
POP3: forward with tag  
Timeout Value: 5 (1-10 Seconds)  
Timeout Tag: [DNSBL Timeout] (Optional)

**DNSBL Domain List**

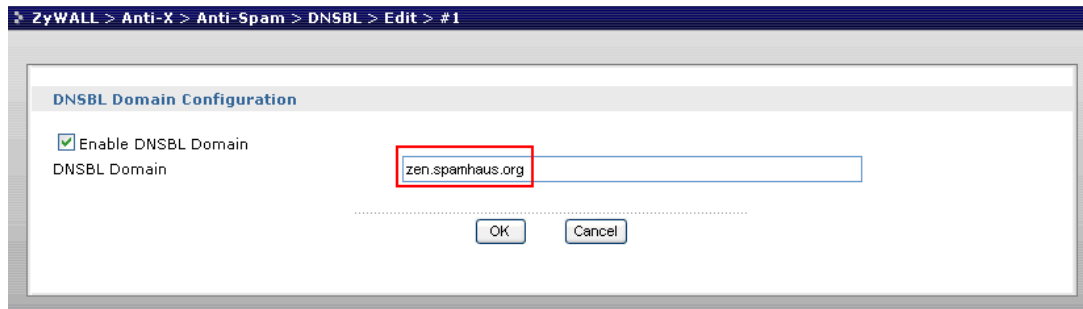
#	DNSBL Domain

**Note:**  
Each mail relay and sender IP in mail header (under max. number) will be checked against the DNSBL domain servers listed and enabled above.

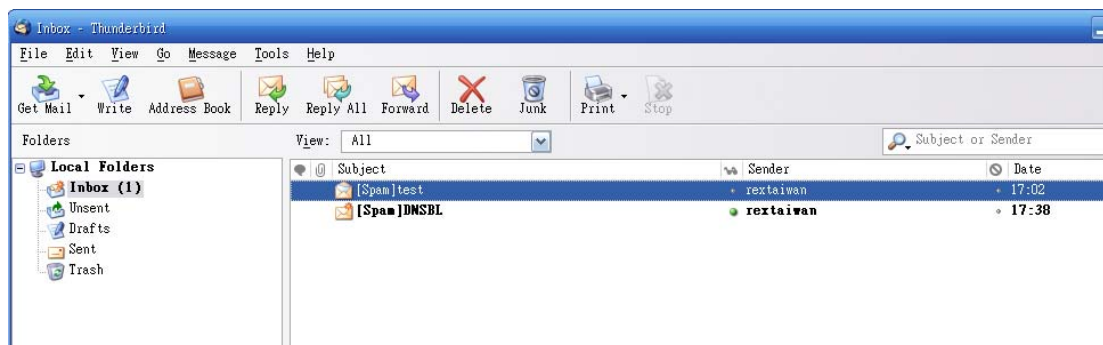
Apply Reset

In this step, we enter the DNSBL website we will refer. Please remember to APPLY the

finishing the DNSBL domain list.



In the following figure, we can see that the anti-spam function is working.



### 3.3.3 Using Black/White list (B/W list)

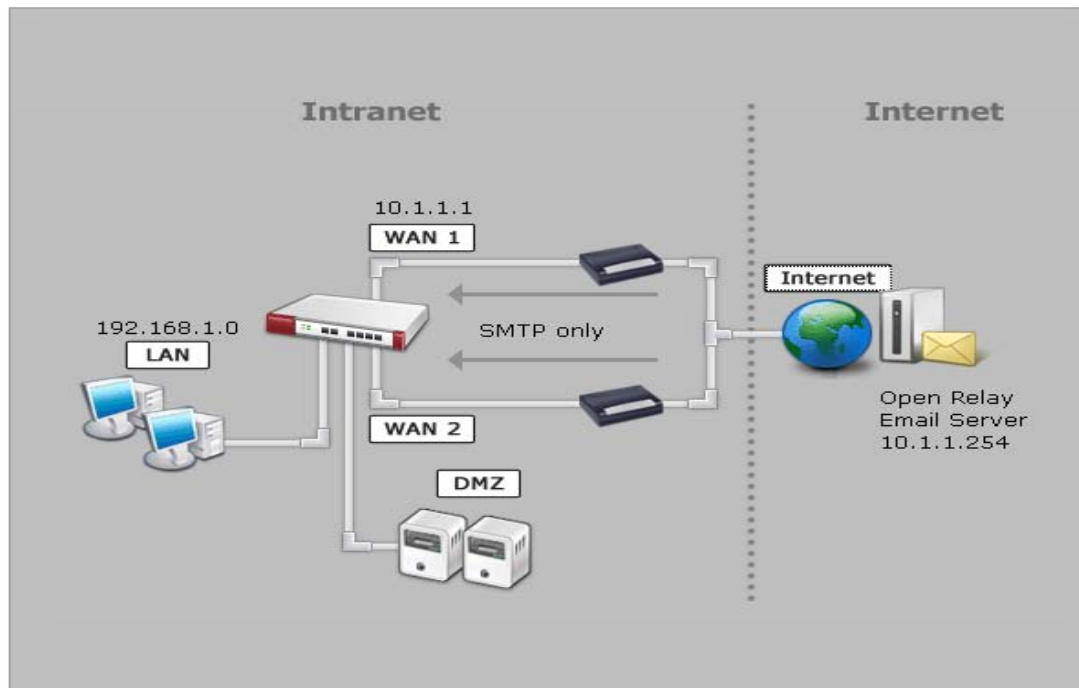
First, we can edit our owned black list and/or white list. Generally speaking, one way of making black list is to edit the address of email server that you do not trust. Additionally, ZyWALL USG also provide other options to filter the spam mails based on subject, source IP address of relay email servers, email address and mail header. In contrast, you can edit the white list based on the information of email subject, source IP address of relay email servers, email address.

#### 3.3.3.1 Configuration procedure

- Enabling Anti-Spam
- Add Policy
- Editing Black/White List
- Click Apply button to apply it
- Test result: the subject of email has been tagged

### 3.3.3.2 Scenario topology

In this example, we consider the SMTP email server is outside the LAN.

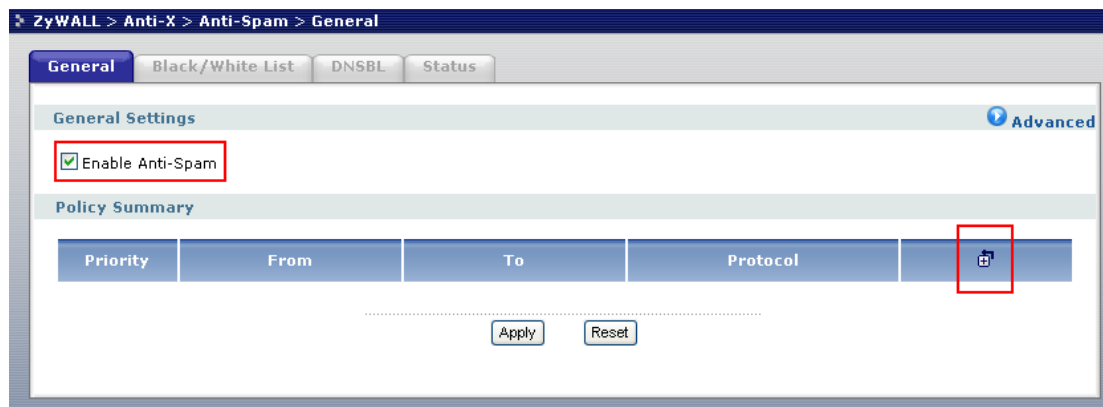


### 3.3.3.3 Steps to configure B/W list

#### Step 1. Enabling Anti-Spam

First, we activate the function of “Anti-Spam”

ZyWALL > Anti-X > Click Add button



## Step 2. Add Policy

Since email server is located outside LAN, and the best way of filtering spam emails is to scan all incoming emails before end users receive them. Therefore, we set the email direction as “From WAN to LAN” in the policy configuration. Additionally, we can choose which kind of list (black list and/or white list) we want to apply.

**ZyWALL > Anti-X > Anti-Spam > General > Edit > #1**

**General Settings**

☒ Enable Policy  
Log: log [icon]

**Email Direction**

From: WAN [icon]  
To: LAN1 [icon]

**Protocols to Scan**

☒ SMTP ☐ POP3

**Scan Options**

☒ Check White List  
☒ Check Black List  
☐ Check DNSBL

**Actions For Spam Mail** [icon]

SMTP: forward with tag [icon]  
POP3: forward with tag [icon]

OK Cancel

## Step 3. Editing Black/White List

You can add an open relay server to the Black List in Anti-spam/ “White/Black List”/ Black list. Here, you need to select the check box and add a special tag in the title of suspected spam emails if you want. Then, we edit our owned black list that displays the relayed email servers we do not trust.

**ZyWALL > Anti-X > Anti-Spam > White/Black List > Black List**

General Black/White List DNSBL Status

**Black List** White List

**General Settings**

☒ Enable Black List Checking  
Black List Spam Tag: [Spam] (Optional)

**Rule Summary**

Total Rule: 0 30 rules per page Page: 1 of 1

#	Type	Content	[icon]

Apply Reset

#### Step 4. Setting rule

In setting the rule, you can specify how to identify the spam mails based on the type of email. In other words, in the field of type, you can specify email subject, sender IP address, sender email address or mail header. In this example, we sue the type of sender or re mail relay IP address to judge whether the mails are spam.

The screenshot shows the 'Rule Configuration' dialog box in the ZyWALL configuration interface. The breadcrumb path at the top is 'ZyWALL > Anti-X > Anti-Spam > White/Black Lists > Black List > Edit > #1'. The dialog has a section titled 'Rule Configuration' with the following fields:

- ☒ Enable Rule
- Type: IP Address (selected from a dropdown menu)
- Sender or Mail Relay IP Address: 10.1.1.254
- Netmask: 255.255.255.0

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

#### Step 5. Apply the setting

In the following figure, we can see the new entry in the black list.

The screenshot shows the 'Black List' tab in the ZyWALL configuration interface. The breadcrumb path at the top is 'ZyWALL > Anti-X > Anti-Spam > White/Black List > Black List'. The interface has tabs for 'General', 'Black/White List', 'DNSBL', and 'Status'. The 'Black List' tab is active, and the 'Black List' sub-tab is selected. The 'General Settings' section shows:

- ☒ Enable Black List Checking
- Black List Spam Tag: [Spam] (Optional)

The 'Rule Summary' section shows 'Total Rule: 1' and '30 rules per page'. Below this is a table with the following data:

#	Type	Content	
1	ip-address	10.1.1.254 / 255.255.255.0	[Icons]

At the bottom of the table are 'Apply' and 'Reset' buttons. The 'Apply' button is highlighted with a red box.

### Step 6. Test result: the subject of email has been tagged

In the result, we can see that the mail from the email server in our black list is tagged as [Spam]. It means that the anti-spam of ZyWALL is working well.



## 3.4 Guaranteed Quality of Service

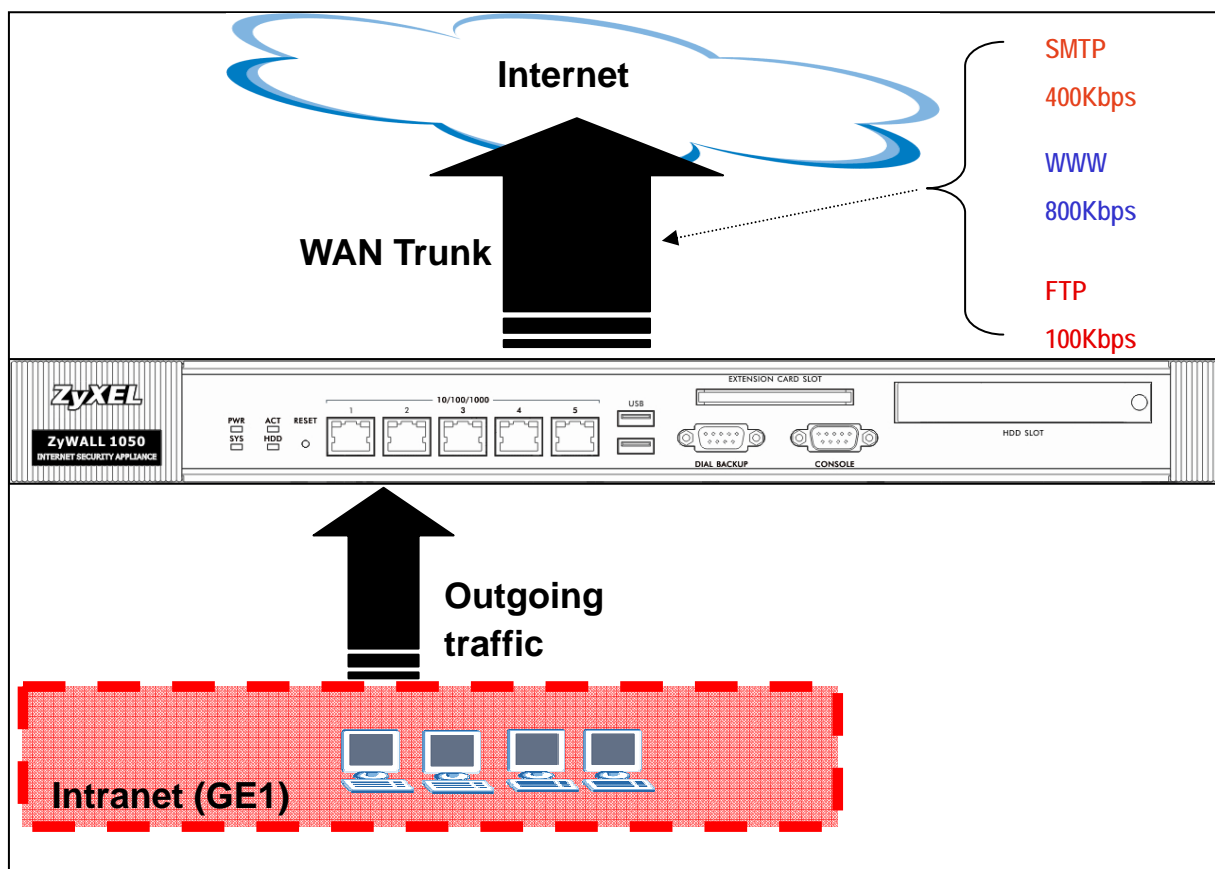
Nowadays if you need a good quality of service, just simply throwing more bandwidth at your network is not the ultimate solution to this problem, because you can't foresee what new bandwidth-hungry applications will be in use in several months. An ill-behaved application can easily bring your network down and potentially shut down your business operation. To gain more effective control of your network, you need to incorporate Quality of Service (QoS). In a QoS-enabled network, you can prioritize network traffic flow, allocate network bandwidth and resources to different applications and users, enforce security to the applications and the users entering your network, and set network behavior according to the business needs. Using QoS approach, an application would request a certain level of service prior to using the network. If bandwidth is expensive in your region, QoS style approach may make more sense than just simply adding more bandwidth. It is assumed that there is insufficient capacity for all users to complete what they want at the same time.



### 3.4.1 Priority & Bandwidth management

ZyWALL 1050 supports both prioritizing and bandwidth management for outgoing traffic. IT administrator can define bandwidth management policies to ensure quality of running services in their network environment. ZyWALL 1050 supports bandwidth management policy based on the type of service, origin of the traffic, user/group to ensure optimized bandwidth utilization. Bandwidth management and prioritization can be done with policy route in ZyWALL 1050.

Here is an example:



To fulfill this scenario; please follow the configuration steps as below:

1) By default, ZyWALL 1050 created a WAN Trunk interface for you. Thus, you don't need to worry about WAN Trunk in this scenario. Now, we will need to create those Bandwidth Management policies for our application. Logon to the ZyWALL 1050 GUI and go to **Configuration > Policy > Route > Policy Route**. Then click the "+" to add a new policy

route at the top of your list.



2) The description of the policy is optional. In this scenario, we will need to make a policy on all the SMTP traffic going out from LAN (GE1) to WAN. Since all the traffic should go out through the WAN Trunk, we need to set our “Incoming” interface to GE1, “Source” subnet to LAN\_subnet, and “Next-Hop” to “Trunk” through the “WAN\_Trunk” Interface. And finally we get to the QoS part of our policy. In this scenario we are going to set 400Kbps for SMTP traffic. We can assign this policy a relatively high priority (like 100) just in case the bandwidth is not enough at all but SMTP service can still get more bandwidth than the other type of network services.

**ZyWALL 1050 > Configuration > Policy > Route > Policy Route > Edit > #1**

**Configuration**

☒ Enable  
 Description  (Optional)

**Criteria**

User   
 Incoming    
 Source Address   
 Destination Address   
 Schedule   
 Service

**Next-Hop**

Type   
 Gateway   
 Interface   
 VPN Tunnel   
 Trunk

**Address Translation**

Source Network Address Translation   
 Port Triggering

#	Incoming Service	Trigger Service

**Bandwidth Shaping**

Maximum Bandwidth  Kbps  
 Bandwidth Priority  (1-1024, 1 is highest priority)

3) Repeat the above steps to create two more policy routes for “WWW” and “FTP” services. In the policy route you can set their Maximum Bandwidth to 800Kbps and 100Kbps along with a priority value. Below is what you should get so far:

**ZyWALL 1050 > Configuration > Policy > Route > Policy Route**

**Policy Route** **Static Route**

#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM	
1	any	none	ge1	LAN_SUBNET	any	SMTP	WAN_TRUNK	outgoing-interface	400	[Icons]
2	any	none	ge1	LAN_SUBNET	any	HTTP	WAN_TRUNK	outgoing-interface	800	[Icons]
3	any	none	ge1	LAN_SUBNET	any	FTP	WAN_TRUNK	outgoing-interface	100	[Icons]
4	any	none	ge1	LAN_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0	[Icons]

**New added Policy Routes**

**The default Policy Route**

**Apply** **Reset**

Tips: Policy Route rules are based on first match, first go. Thus, all your new rules should be placed before the default policy route, which is the last one here.

4) The default policy route makes bandwidth management disabled. In any case if you want to make sure that the bandwidth is guaranteed instead of just metering, you should check whether every rule you have here has the bandwidth control enabled. This must include the default route. Also, the sum of bandwidth in all your rules should not exceed the physical bandwidth of your WAN interfaces(s). Otherwise the Bandwidth Management might not be able to guarantee your bandwidth during a congestion. Let's assume that the max bandwidth of our WAN is 1.5Mbps. Now we already spent 400kbps for SMTP, 800kbps for HTTP, and 100kbps for SMTP. What left over is 200kbps available to us; thus, we can apply it for the remaining traffic, which is our default route.

**ZyWALL 1050 > Configuration > Policy > Route > Policy Route**

**Policy Route** **Static Route**

#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM	
1	any	none	ge1	LAN_SUBNET	any	SMTP	auto	outgoing-interface	400	[Icons]
2	any	none	ge1	LAN_SUBNET	any	HTTP	auto	outgoing-interface	800	[Icons]
3	any	none	ge1	LAN_SUBNET	any	FTP	auto	outgoing-interface	100	[Icons]
4	any	none	ge1	LAN_SUBNET	any	any	WAN_TRUNK	outgoing-interface	0	[Icons]

**Click here to modify the settings of the default route.**

**Apply** **Reset**

5) Modify the values of bandwidth and priority here in the default policy route. Click “OK” to apply.

**ZyWALL 1050 > Configuration > Policy > Route > Policy Route > Edit > #4**

**Configuration**

☒ Enable

Description: NAT (Optional)

**Criteria**

User: any

Incoming: Interface / ge1 (Change...)

Source Address: LAN\_SUBNET

Destination Address: any

Schedule: none

Service: any (New...)

**Next-Hop**

Type: Trunk

Gateway: ge1

VPN Tunnel: ZYWALL2PLUS\_CONN

Trunk: WAN\_TRUNK

**Address Translation**

Source Network Address Translation: outgoing-interface

Port Triggering: # Incoming Service Trigger Service

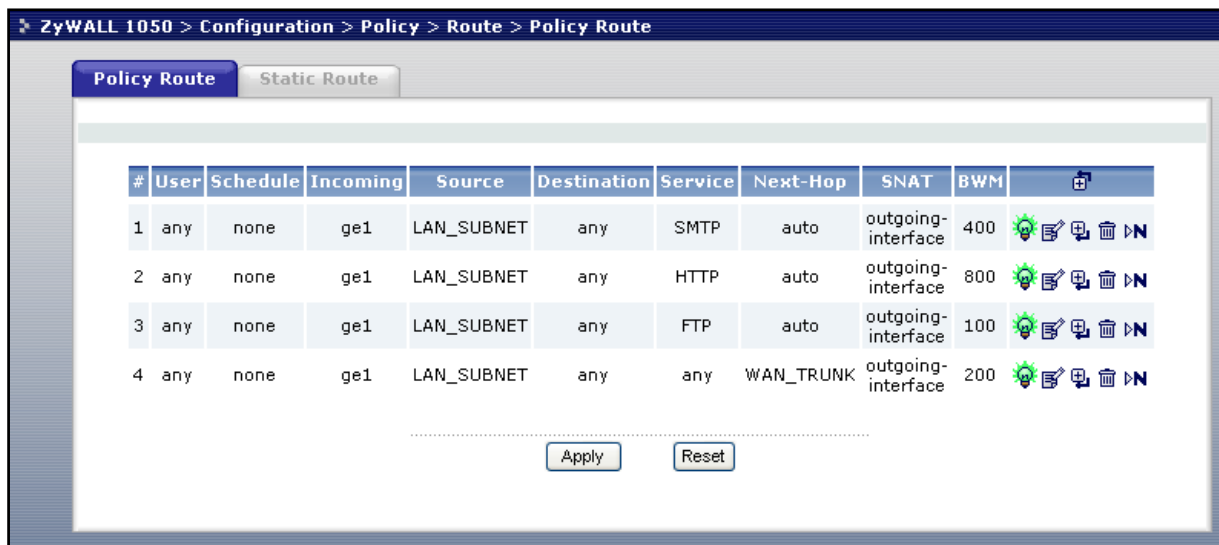
**Bandwidth Shaping**

Maximum Bandwidth: 200 Kbps

Bandwidth Priority: 1024 (1-1024, 1 is highest priority)

OK Cancel

9) Now the final list should look like the one below:



### CLI commands for the first SMTP policy route:

```

[0] policy 1 (the number of your SMTP policy)
[1] no deactivate
[2] description SMTP
[3] no user
[4] interface ge1
[5] source LAN_SUBNET
[6] destination any
[7] no schedule
[8] service SMTP
[9] next-hop trunk WAN_TRUNK
[10] snat outgoing-interface
[11] bandwidth 400 priority 100
[12] exit
  
```

### CLI commands for applying bandwidth and priority to the default policy route:

```

[0] policy 4 (the number of your default policy)
  
```

- [1] no deactivate
- [2] description NAT
- [3] no user
- [4] interface ge1
- [5] source LAN\_SUBNET
- [6] destination any
- [7] no schedule
- [8] service any
- [9] next-hop trunk WAN\_TRUNK
- [10] snat outgoing-interface
- [11] bandwidth 200 priority 1024
- [12] exit

## FAQ

### A. Device Management FAQ

#### **A01. How can I connect to ZyWALL USG 2000 to perform administrator's tasks?**

You can connect your PC to ZyWALL USG 2000 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 2000 for management. The default administration username is “**admin**”, and password is “**1234**”.

#### **A02. Why can't I login into ZyWALL USG 2000?**

There may have several reasons why you can't login to ZyWALL USG 2000:

1. The ZyWALL USG 2000 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 2000'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 2000'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 2000 blocks login from such an IP address for 30 minutes by default.
6. You can be connecting to ZyWALL USG 2000 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 **accept** the access **from 'WAN' or from 'All'**.



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

The screenshot shows the ZyWALL configuration interface for the 'System > WWW' menu. It is divided into two sections: 'HTTPS' and 'HTTP'.

**HTTPS Configuration:**

- ☒ Enable
- Server Port: 443
- ☐ Authenticate Client Certificates (See [Trusted CAs](#))
- Server Certificate: default
- ☒ Redirect HTTP to HTTPS

**Admin Service Control Table:**

#	Zone	Address	Action
1	ALL	ALL	Accept

**User Service Control Table:**

#	Zone	Address	Action
1	ALL	ALL	Accept

**HTTP Configuration:**

- ☒ Enable
- Server Port: 80

**Admin Service Control Table:**

#	Zone	Address	Action
1	ALL	ALL	Accept

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

The screenshot shows the 'ZyWALL > Firewall' configuration page. It includes 'Global Setting' and a 'Firewall rule' table.

**Global Setting:**

- ☒ Enable Firewall
- ☐ Allow Asymmetrical Route
- ☐ Maximum session per Host: (1-8192)

**Firewall rule configuration:**

From Zone: any To Zone: any Refresh

Total rules: 27 30 entries per page Page: 1 of 1

#	Priority	From	To	Schedule	User	Source	Destination	Service	Access	Log
1	1	LAN1	WAN	none	any	any	any	any	allow	no
2	2	LAN1	DMZ	none	any	any	any	any	allow	no
3	3	WAN	LAN1	none	any	any	any	any	deny	log
4	4	WAN	DMZ	none	any	any	any	any	allow	no
5	5	DMZ	LAN1	none	any	any	any	any	deny	log
6	6	DMZ	WAN	none	any	any	any	any	allow	no
7	7	LAN1	ZyWALL	none	any	any	any	any	allow	no
8	8	WAN	ZyWALL	none	any	any	any	VRRP	allow	no
9	9	WAN	ZyWALL	none	any	any	any	ESP	allow	no
10	10	WAN	ZyWALL	none	any	any	any	AH	allow	no
11	11	WAN	ZyWALL	none	any	any	any	NATT	allow	no

**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 2000 redirects me to the login page when I am performing the management tasks in GUI?**

There may be several reasons for ZyWALL USG 2000 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 2000 using other remote management client (telnet or ssh...etc) after you logged in ZyWALL USG 2000 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 2000 restarts?**

There may have two reasons:

1. If you configure ZyWALL USG 2000 from CLI. You must type CLI “**write**” to save the configuration before rebooting. If you configure ZyWALL USG 2000 from GUI, any configuration will be automatically saved.
2. ZyWALL USG 2000 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 2000 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 2000 boots up for a long time as below.

1. It might because you have many configurations on ZyWALL USG 2000. 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 2000’s lan1 port which is with IP address 192.168.1.1 by default.

2. The ZyWALL USG 2000 may get firmware crashed. Generally, it may happen if power off ZyWALL USG 2000 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 2000's lan1 port via an Ethernet cable.
2. [ftp 192.168.1.1](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 2000 automatically.

## **B. Registration FAQ**

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

You must first register ZyWALL USG 2000 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 2000 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 2000 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 2000 manage multiple configuration files?**

From ZyWALL USG 2000 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 2000 system configuration file. When ZyWALL USG 2000 is booting, it will use this configuration file for ZyWALL USG 2000 as system configuration.
2. **system-default.conf:** The system-default.conf is ZyWALL USG 2000 system default configuration file. When you press the reset button, ZyWALL USG 2000 will copy system-default.conf over startup-conf.conf.
3. **lastgood.conf:** The lastgood.conf is created after ZyWALL USG 2000 successfully applies startup-config.conf. And ZyWALL USG 2000 will try to apply lastconfig.conf, if ZyWALL USG 2000 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 2000 through GUI menu **File manager > Shell Script** tab. Some notes as followings.

- Must follow ZyWALL USG 2000 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.

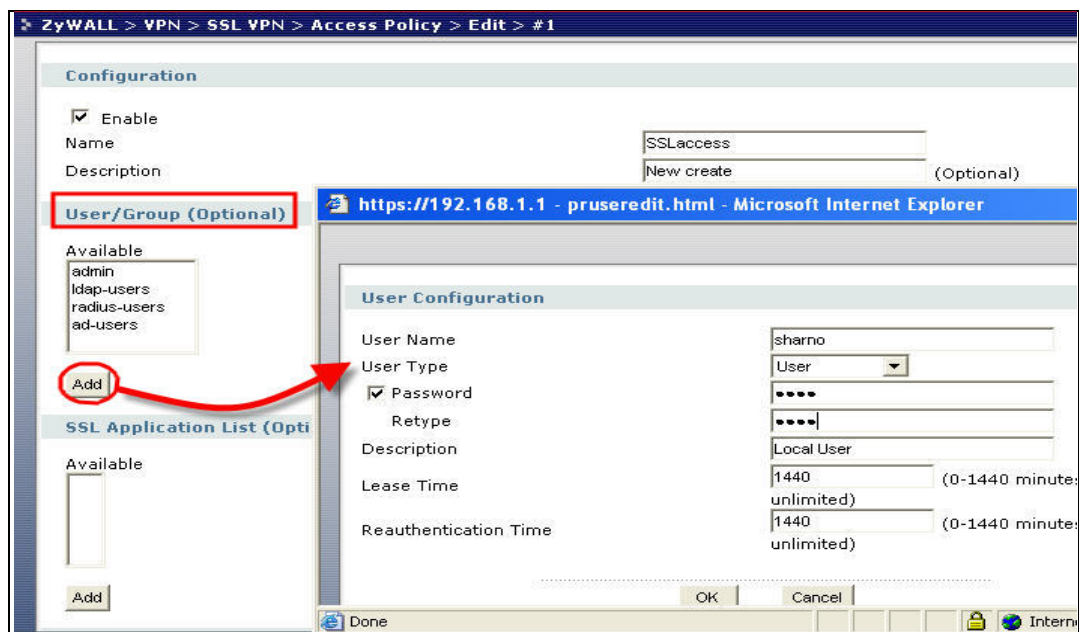
## D. Object FAQ

### D01. Why does ZyWALL USG 2000 use object?

ZyWALL USG 2000 object include address, service, schedule, authentication method, certificate, zone, interface group and ISP account object. The ZyWALL USG 2000 uses object as a basic configuration block. It can simplify the configuration change once you 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.

## **F. Routing and NAT FAQ**

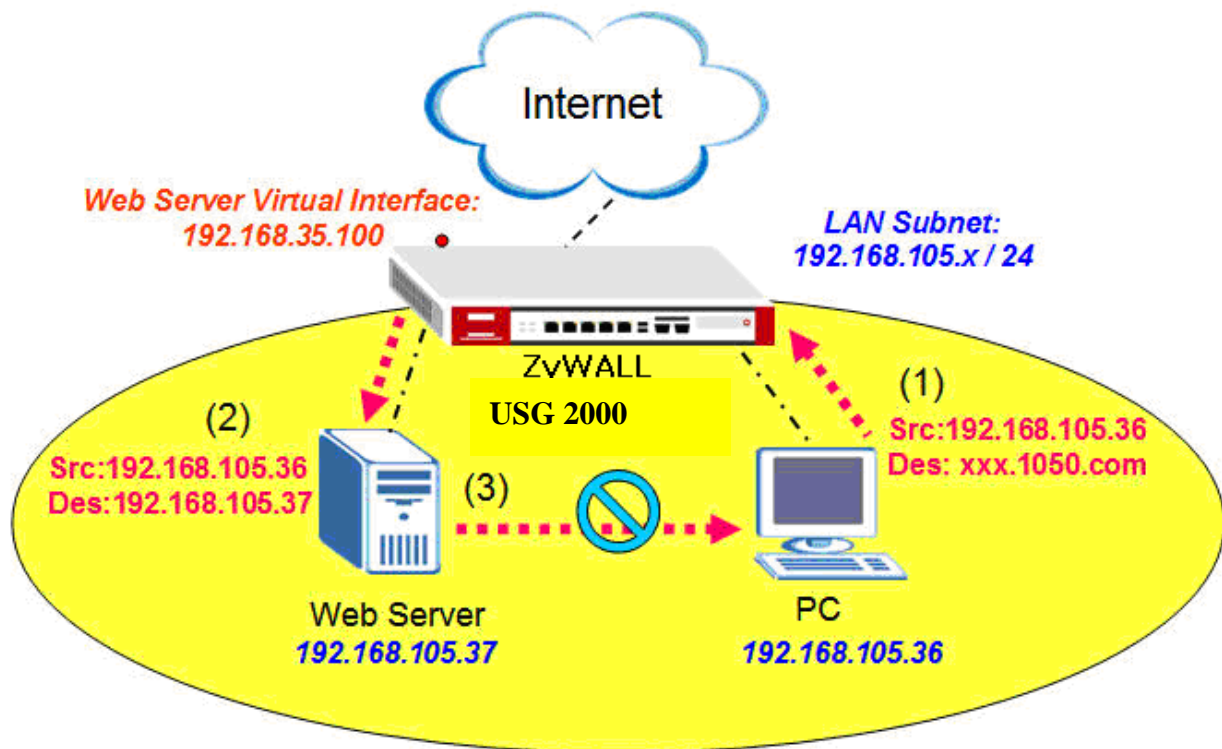
### **F01. How to add a policy route?**

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 2000 will use the route setting to direct the traffic to the next hop.

### **F02. How to configure local loopback in ZyWALL USG 2000?**

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 2000 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 2000 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.

Name: NAT-FTP

Interface: ge2

Original IP: WEB-WAN

Mapped IP: 192.168.105.37

Mapping Type: Port

Protocol Type: Any

Original Port: 80

Mapped Port: 80

\* Please make sure the firewall allows virtual server traffic.  
 \* Please create a corresponding policy route (NAT 1:1) if the virtual server will also establish connections to clients.

OK Cancel

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 2000 is complete.

**Configuration**

☒ Enable

Description: (Optional)

**Criteria**

User: any

Incoming: Interface / any

Source Address: WEB-LAN

Destination Address: any

Schedule: none

Service: any

**Next-Hop**

Type: Trunk

Gateway: ZW\_WAN\_IP

Interface: ge1

VPN Tunnel: Remote-Dialup

Trunk: WAN\_TRUNK

**Address Translation**

Source Network Address Translation: WEB-WAN

### NAT loopback Configuration

In order to run the NAT loopback on ZyWALL USG 2000, 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.

Name: NAT-FTP-IN  
 Interface: ge1  
 Original IP: WEB-WAN  
 Mapped IP: 192.168.105.37  
 Mapping Type: Port  
 Protocol Type: Any  
 Original Port: 80  
 Mapped Port: 80

\* Please make sure the firewall allows virtual server traffic.  
 \* Please create a corresponding policy route (NAT 1:1) if the virtual server will also establish connections to clients.

OK Cancel

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.

Virtual Server

Total Virtual Servers: 2      30 entries per page      Page 1/1

#	Name	Interface	Original IP	Mapped IP	Protocol	Original Port	Mapped Port	
1	NAT-WEB	ge2	WEB-WAN	192.168.105.37	any	80	80	
2	NAT-WEB-IN	ge1	WEB-WAN	192.168.105.37	any	80	80	

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 2000 and avoid the triangle route problem.

**Configuration**

☒ Enable  
Description  (Optional)

**Criteria**

User   
Incoming    
Source Address   
Destination Address   
Schedule   
Service  

**Next-Hop**

Type   
Gateway   
Interface   
VPN Tunnel   
Trunk

**Address Translation**

Source Network Address Translation

#	Incoming Service	Trigger Service
<input type="button" value="Add"/>		

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 2000 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 2000'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 2000 routing database. When routing, ZyWALL USG 2000 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 2000 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 2000. 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 2000 will select this as default route and traffic can't go out from the ZyWALL USG 2000.

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

ZyWALL USG 2000 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 2000 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 2000?**

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?

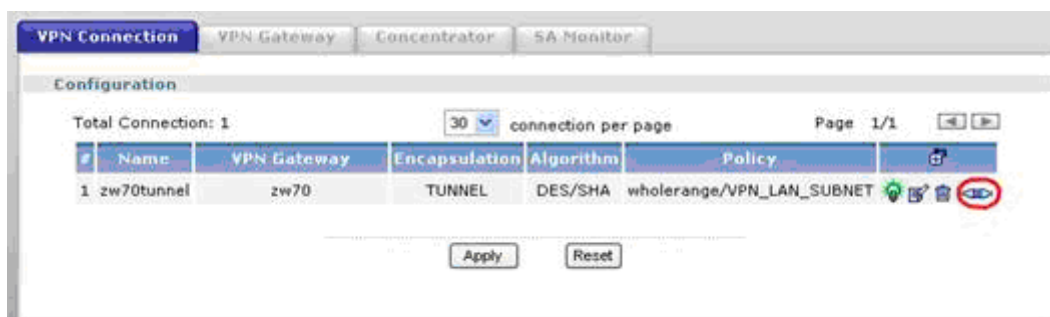
Please check the responder's logs whether the fail occurs in phase 1 or phase 2. If the phase 1 has failed, try to check the VPN gateway configuration, such as proposals or Local/Remote ID. If the phase 2 has failed, try to check the VPN connection configuration, such as whether the policy matches the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

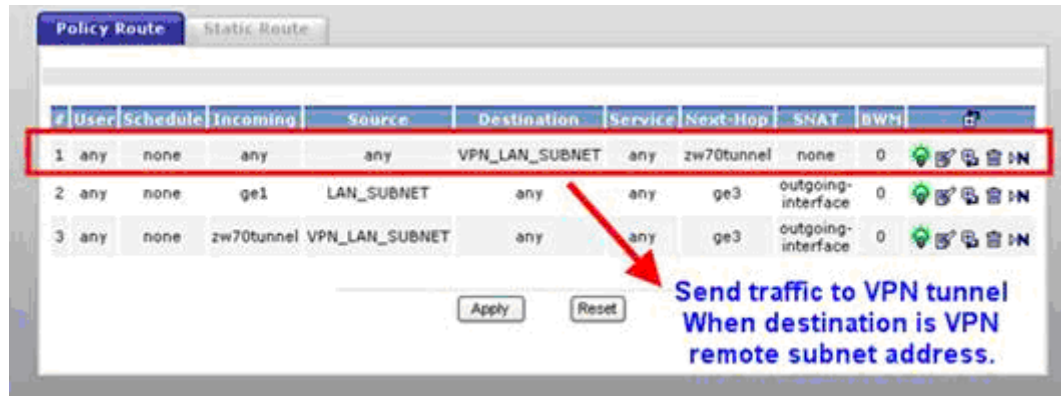
### G03. Why ZyWALL USG 2000 VPN tunnel had been configured correctly and the VPN connection status is connected but the traffic still can not reach the remote VPN subnet?

ZyWALL USG 2000 VPN traffic is the route base VPN, this means we need to configure a policy route rule to guide the ZyWALL USG 2000 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 2000 send the packet to VPN tunnel when the packet's destination address is VPN remote subnet. Please switch to ZyWALL USG

2000 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 2000 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 2000 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

### 103. 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 2000. 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.



**Service**

☒ Enable Service

**Service Identification**

Name: eDonkey

Classification: ☐ Auto ☒ Service Ports

Service Port:

Service Port	
4661	
4662	
4663	
4664	
4665	

**Policy**

#	Port	Schedule	User	From	To	Source	Destination	Access
Default 0		none	any	any	any	any	any	forward

OK Cancel

(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 2000 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 2000 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.

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

**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.

## **K. Content Filtering 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 2000. 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.”

ZyWALL > Device HA > Monitored Interface > Edit > #1

**Monitored Interface Configuration**

☒ Enable Monitored Interface

Interface Name: wan1

Virtual Router IP(VRIP) / Subnet Mask: 167.35.4.3 / 255.255.255.0

Manage IP:

Subnet Mask:

OK Cancel

**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 2000 and backup ZW USG 2000 are activated at the same time?**

Since the ZWUSG 2000 master sends multicast VRRP announcement to backup ZWUSG 2000 periodically, if the backup ZWUSG 2000 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 2000 connect to a switch, the switch MUST forward the VRRP multicast to the backup ZWUSG 2000. 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 "Unknown multicast flooding" 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 2000 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 2000 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 2000, [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?**

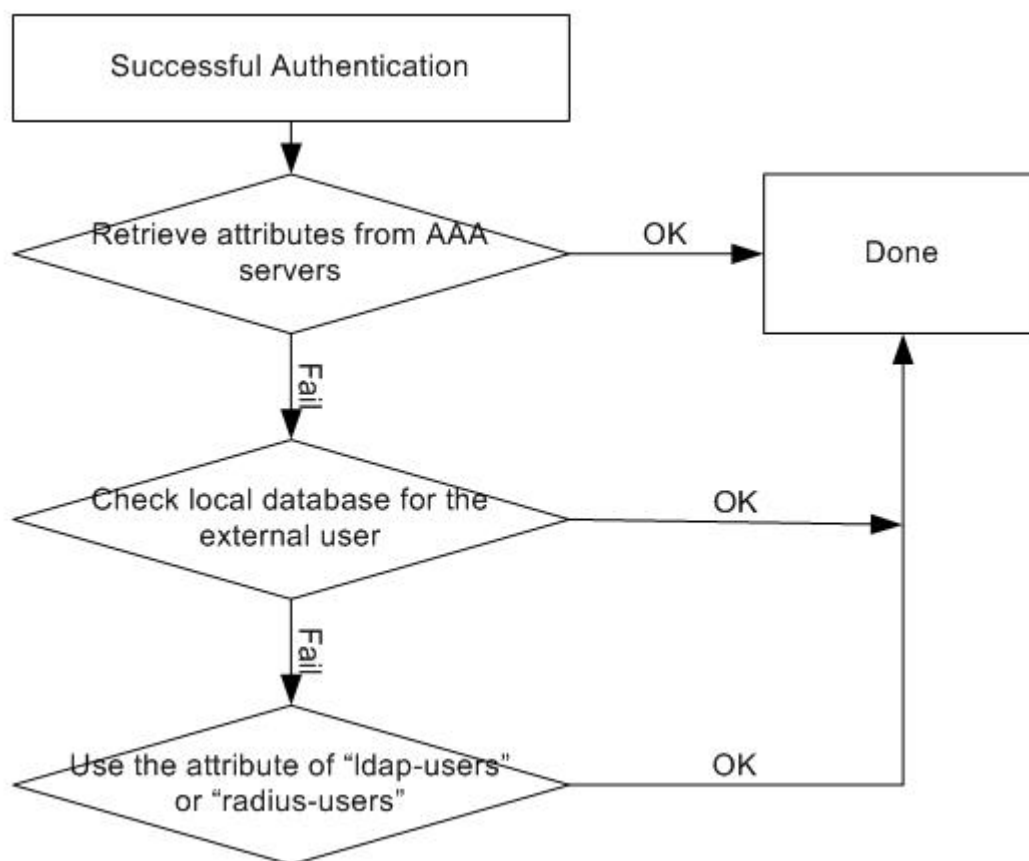
ldap-users/radius-users refer to the users that are authenticated successfully via LDAP/RADIUS server. If you want to perform access control rules or build access policies for the users authenticated via external servers such as LDAP or RADIUS, you can use the ldap-users and radius-users in your access 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 (ldap 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 2000 (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.

User			
Group			
Setting			
Configuration			
#	User Name	Description	
1	admin	Administration account	 
2	ldap-users	External LDAP Users	 
3	radius-users	External RADIUS Users	 

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**

### **001. 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.

### **002. 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.

### **003. 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.

### **004. 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 2000 Anti-Virus engine?**

Due to ZyWALL USG 2000 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 2000 Anti-Virus support compressed file scanning?**

Yes, the ZyWALL USG 2000 Anti-Virus engine supports virus scanning with compression format ZIP, PKZIP, GZIP and RAR.

### **P03. What is the maximum concurrent session of ZyWALL USG 2000 Anti-Virus engine?**

Due to ZyWALL USG 2000 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 2000?**

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 2000 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 2000 to avoid this situation.

**P08. Does ZyWALL USG 2000 Anti-Virus engine support Passive FTP?**

Yes, ZyWALL USG 2000 supports both Active FTP and Passive FTP.

**P09. What kinds of protocol are currently supported on ZyWALL USG 2000 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 2000 will destroy the infected file, log this event and send alert to system administrator. Anti-Virus engine cannot cure the infected file.