# ZyWALL 1050

Internet Security Appliance

# Support Notes

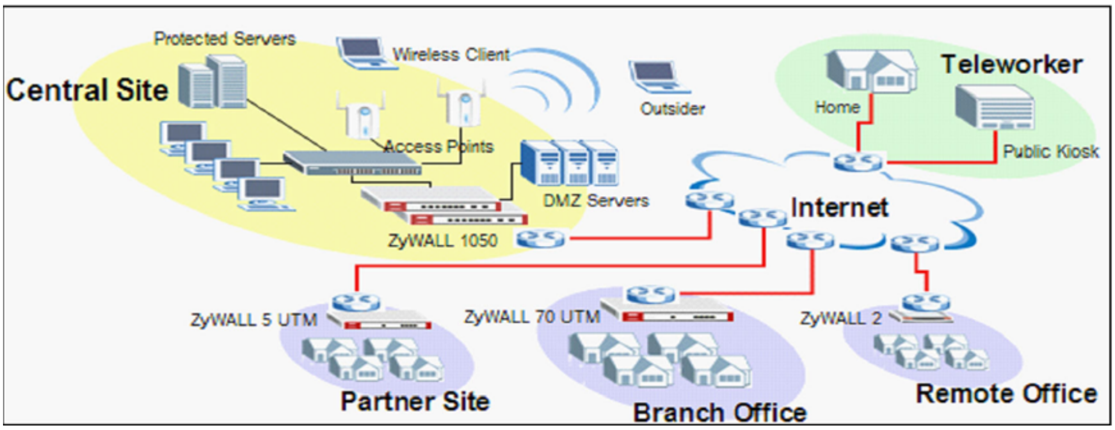
Revision 2.01

August. 2006

# INDEX

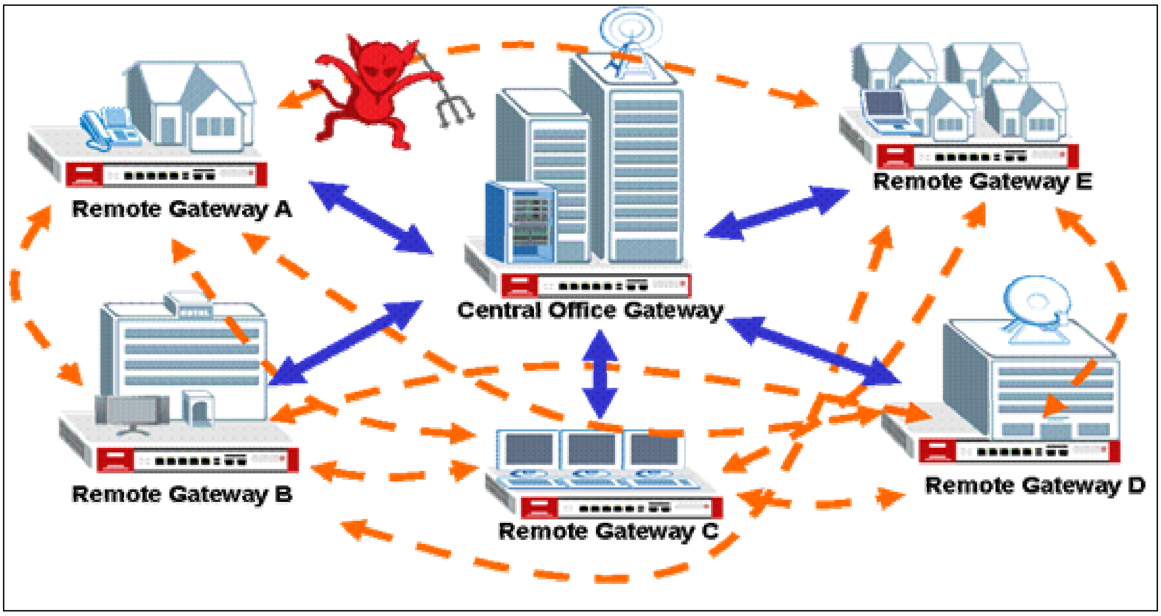
# 1. Deploying VPN

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.



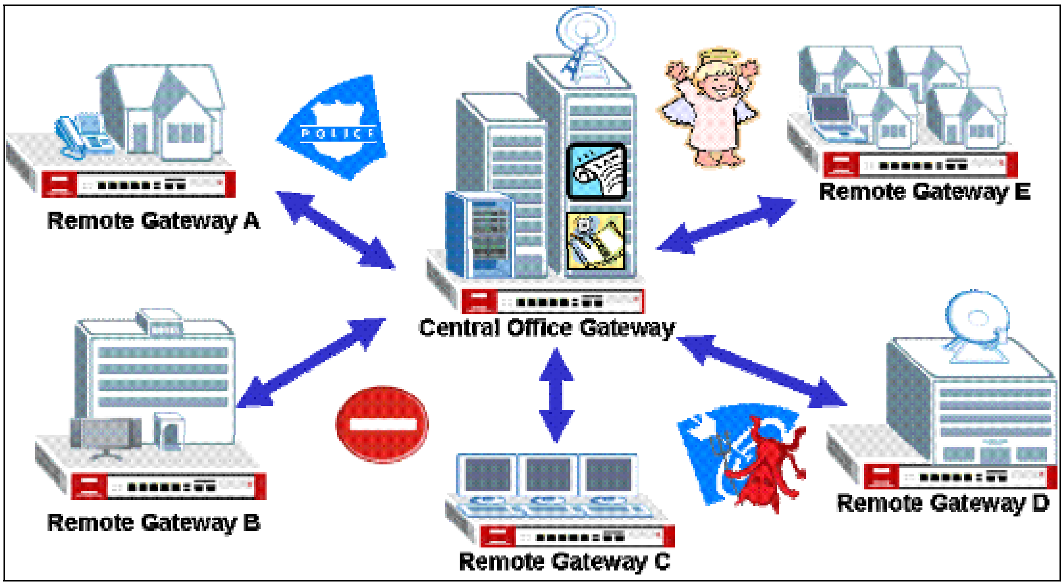
VPN gives you site-to-site connection flexibility. However, with multiple VPN connections between sites, it can become more difficult to maintain. Typically, an administrator has to configure many site-to-site VPN connections to allow a truly global VPN network.

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.

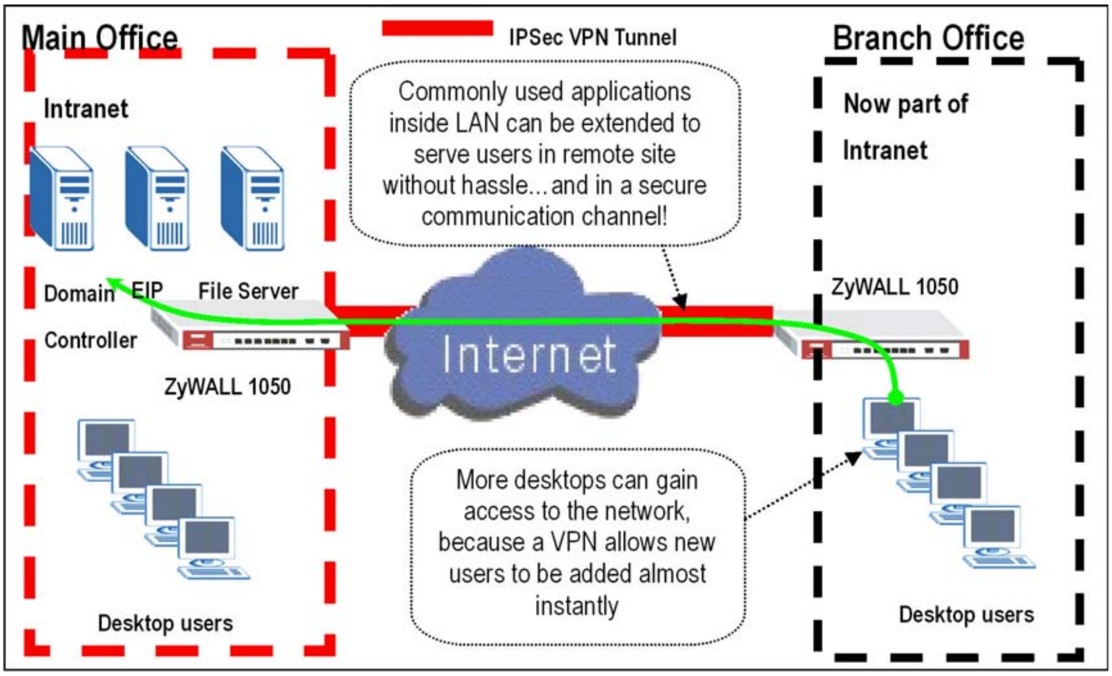


For SMB customer, ZyXEL provides a total VPN solution from a personal client to a 500+ people firewall where all of these devices have the VPN connection ability.

- 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.

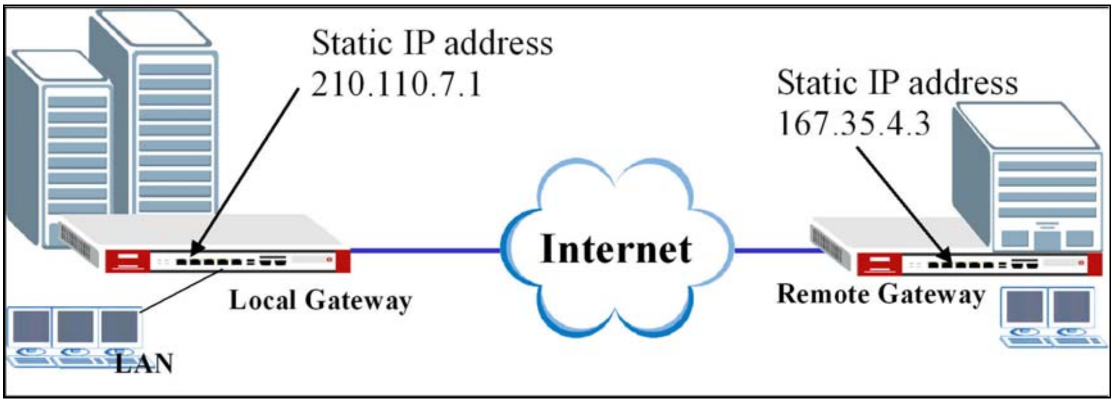

Main Office
IPSec VPN Tunnel
Branch Office
Intranet
Commonly used applications inside LAN can be extended to serve users in remote site without hassle...and in a secure communication channel!
Now part of Intranet
Domain Controller
EIP
File Server
ZyWALL 1050
Internet
ZyWALL 1050
More desktops can gain access to the network, because a VPN allows new users to be added almost instantly
Desktop users
Desktop users

### 1.1.1 Site to Site VPN solutions

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.

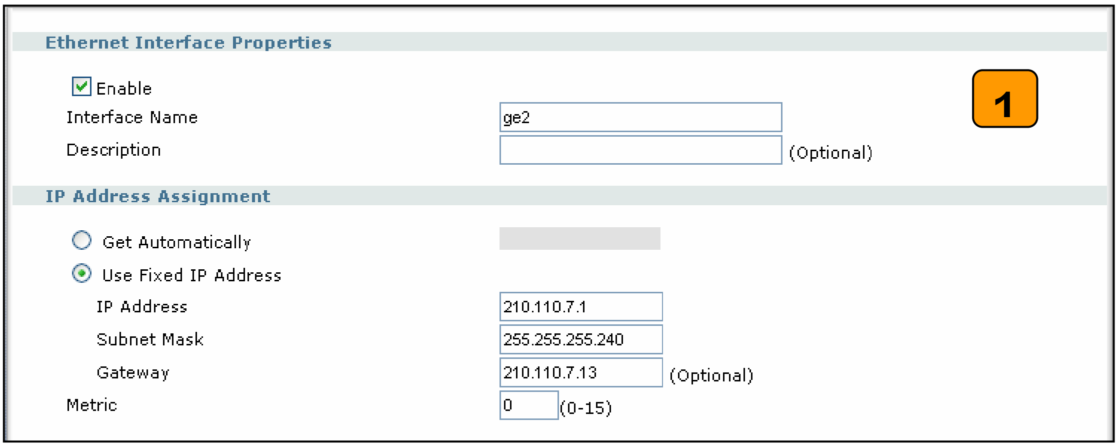
Configure ZyWALL 1050 with Static IP address:

ZyWALL 1050 uses the static IP address for VPN connection. The topology is shown at 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 menu is **Configuration** > **Network** > **Interface** > **Edit** > **ge2**
2) Switch to **Configuration** > **Network** > **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) Repeat the step1 & 2 to configure the Remote ZyWALL 1050. The **Local ID Type** & content and **Peer ID Type** & content are reverse to the Local ZyWALL 1050.



Ethernet Interface Properties

☑ Enable

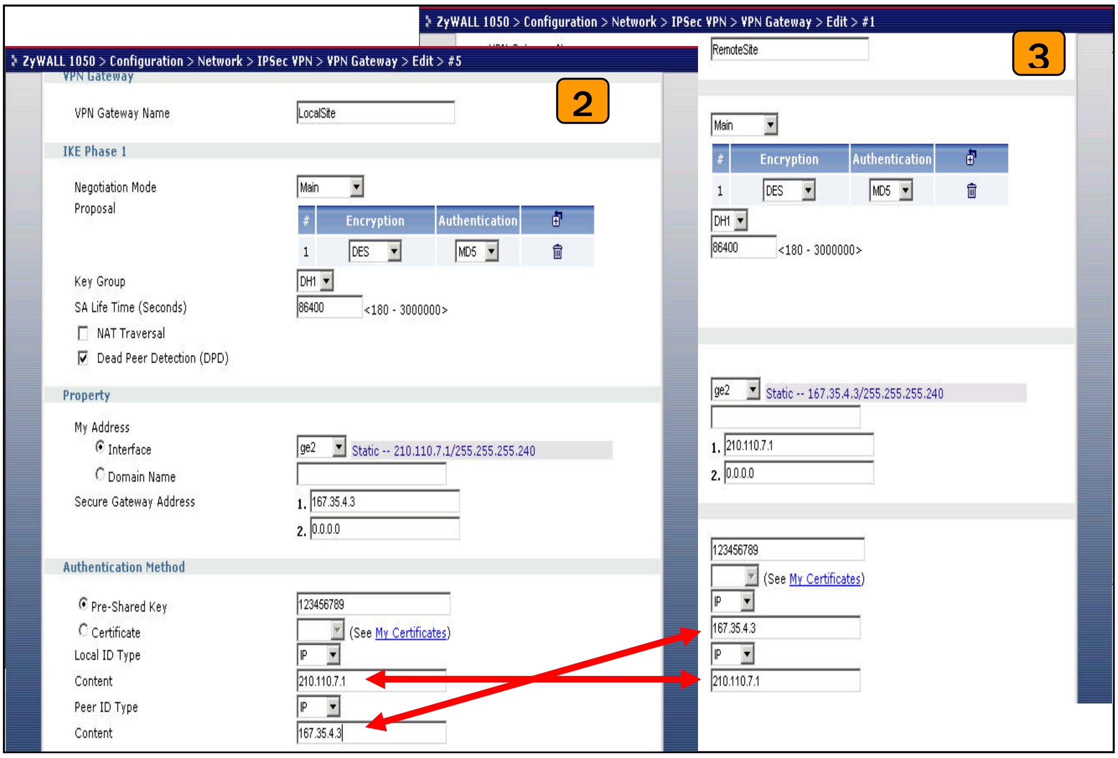
| | |
|---|---|
| Interface Name | ge2 |
| Description | (Optional) |

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) |



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway > Edit > #5

VPN Gateway

VPN Gateway Name: LocalSite

IKE Phase 1

Negotiation Mode: Main

Proposal:

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | MD5 |

Key Group: DH1

SA Life Time (Seconds): 86400 <180 - 3000000>

☐ NAT Traversal

☑ Dead Peer Detection (DPD)

Property

My Address

● Interface: ge2 Static -- 210.110.7.1/255.255.255.240

○ Domain Name:

Secure Gateway Address: 1. 167.35.4.3 2. 0.0.0.0

Authentication Method

● Pre-Shared Key: 123456789

○ Certificate: (See My Certificates)

Local ID Type: IP

Content: 210.110.7.1

Peer ID Type: IP

Content: 167.35.4.3

ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway > Edit > #1

RemoteSite

Main

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | MD5 |

DH1

86400 <180 - 3000000>

ge2 Static -- 167.35.4.3/255.255.255.240

1. 210.110.7.1
2. 0.0.0.0

123456789

(See My Certificates)

IP

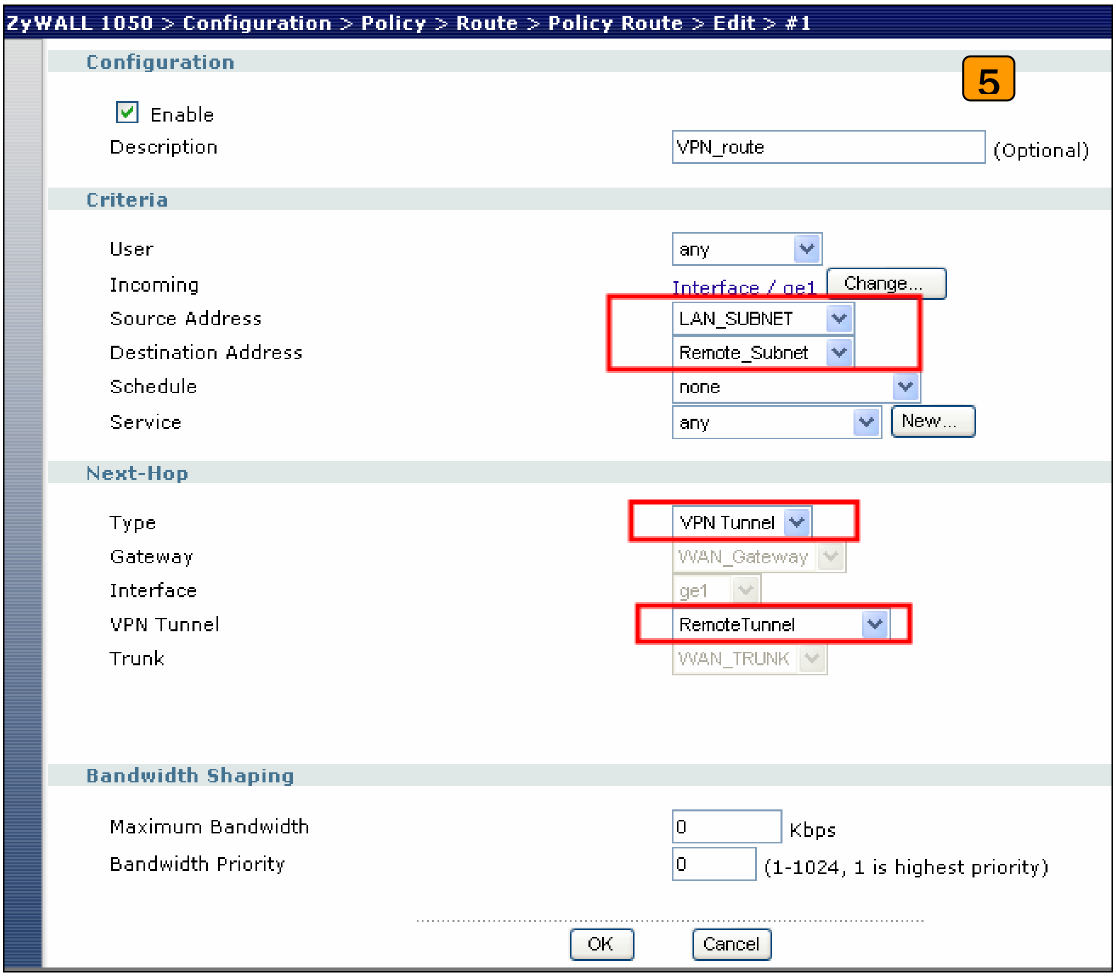
167.35.4.3

IP

210.110.7.1

4) User can refer to the user guide to complete the rest of the settings for VPN tunnel.

5) The ZyWALL1050 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 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 > Configuration > Policy > Route > 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 1050 > Configuration > Policy > Route > Policy Route > Edit > #1

**Configuration**

☑ Enable

Description: VPN_route (Optional)

**Criteria**

User: any

Incoming: Interface / ge1 [Change...]

Source Address: LAN_SUBNET

Destination Address: Remote_Subnet

Schedule: none

Service: any [New...]

**Next-Hop**

Type: VPN Tunnel

Gateway: WAN_Gateway

Interface: ge1

VPN Tunnel: RemoteTunnel

Trunk: WAN_TRUNK

**Bandwidth Shaping**

Maximum Bandwidth: 0 Kbps

Bandwidth Priority: 0 (1-1024, 1 is highest priority)

[OK] [Cancel]

**The CLI commands for application:**

Local Gateway:

```
[0] isakmp policy rename RemoteSite LocalSite
[1] isakmp policy LocalSite
[2] mode main
[3] transform-set des-md5
[4] lifetime 86400
[5] no natt
[6] dpd
[7] local-ip interface ge2
[8] peer-ip 167.35.4.3 0.0.0.0
[9] authentication pre-share
[10] keystring 123456789
[11] local-id type ip 210.110.7.1
[12] peer-id type ip 167.35.4.3
[13] peer-id type ip 167.35.4.3
[14] xauth type server default deactivate
[15] group1
[16] exit
```

Remote Gateway:

```
[0] isakmp policy RemoteSite
[1] mode main
[2] transform-set des-md5
[3] lifetime 86400
[4] no natt
[5] dpd
[6] local-ip interface ge2
[7] peer-ip 210.110.7.1 0.0.0.0
[8] authentication pre-share
[9] keystring 123456789
[10] local-id type ip 167.35.4.3
[11] peer-id type ip 210.110.7.1
[12] peer-id type ip 210.110.7.1
[13] xauth type server default deactivate
[14] group1
[15] exit
```

Policy Route for VPN traffic:

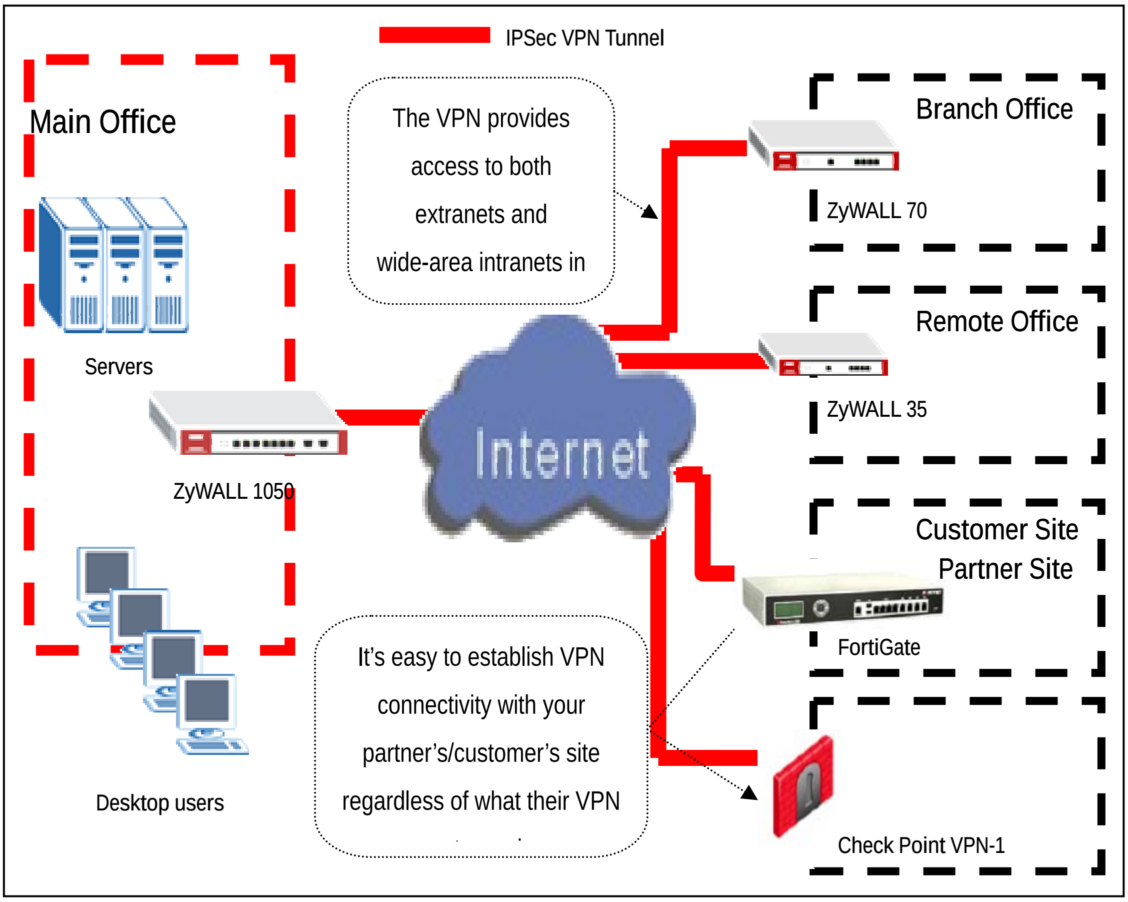
```
[0] policy 1
[1] no deactivate
[2] no description
[3] no user
[4] interface ge1
[5] source LAN_SUBNET
[6] destination Remote_Subnet
[7] no schedule
[8] service any
[9] no snat
[10] next-hop tunnel RemoteTunnel
[11] no bandwidth
[12] exit
```

**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 the opposite and contain the same.
5. Make sure the **VPN policy route** has been configured in ZyWALL1050.

## 1.2 Extranet Deployment

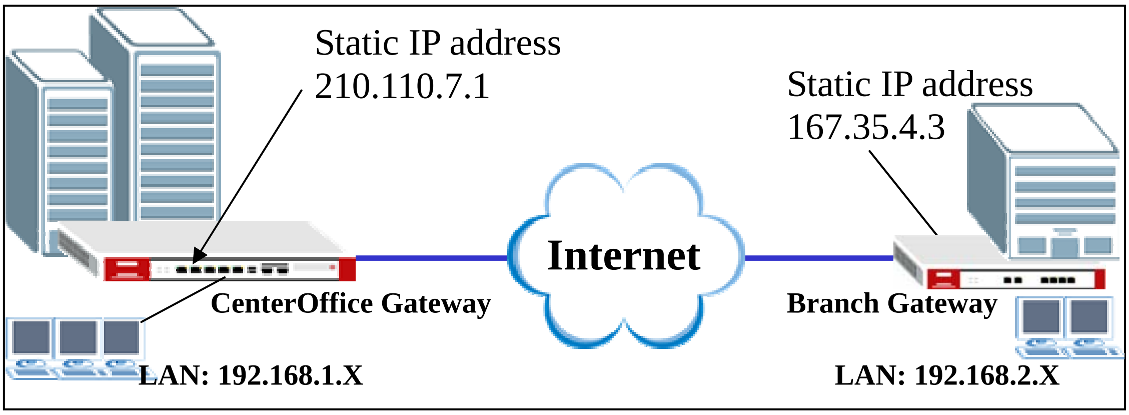
The VPN provides the access to extranets which can provide the security path over internet to improve the client service, vendor support and company communication. Different flexible business models have been developed based on the global VPN extranet architecture. For example, customers can order equipment 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.


IPSec VPN Tunnel
Main Office
Servers
ZyWALL 1050
Desktop users
The VPN provides access to both extranets and wide-area intranets in
Internet
It's easy to establish VPN connectivity with your partner's/customer's site regardless of what their VPN
Branch Office
ZyWALL 70
Remote Office
ZyWALL 35
Customer Site
Partner Site
FortiGate
Check Point VPN-1

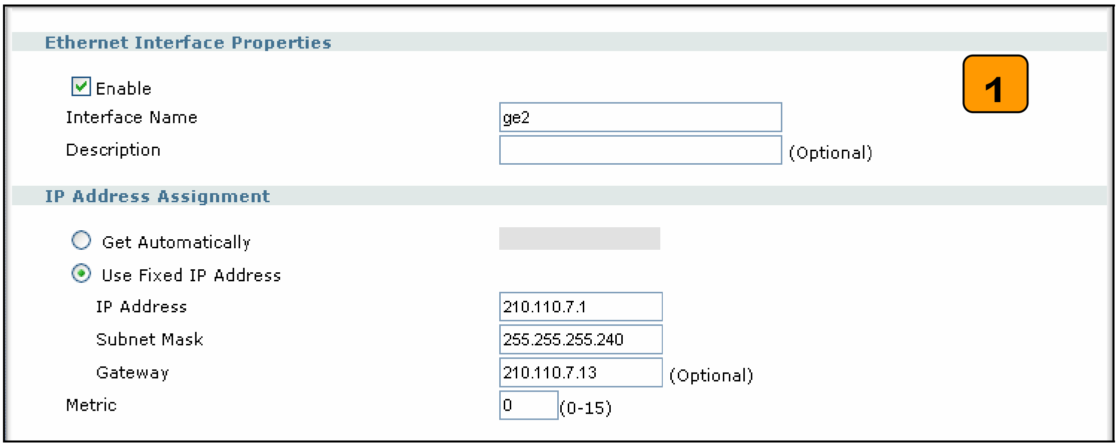
The ZyWALL 1050 can be placed as a VPN gateway in the central site. It can communicate with other ZyXEL's VPN-capable products as well as VPN products from other major vendors in the network device industry, e.g. Cisco PIX/IOS VPN products, Check Point VPN Pro, Juniper NetScreen series and others…

### 1.2.1 Site to site VPN solutions (ZyWALL1050 to ZyWALL70)

The exciting ZyWALL35 or 70 in central office gateway can be replaced by ZyWALL 1050, and the ZyWALL35 or 70 moved to a remote office. The ZyWALL 1050 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 1050 we used ZyWALL 70 as an example.



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



Ethernet Interface Properties

☑ Enable

| | |
|---|---|
| Interface Name | ge2 |
| Description | (Optional) |

IP Address Assignment

○ Get Automatically

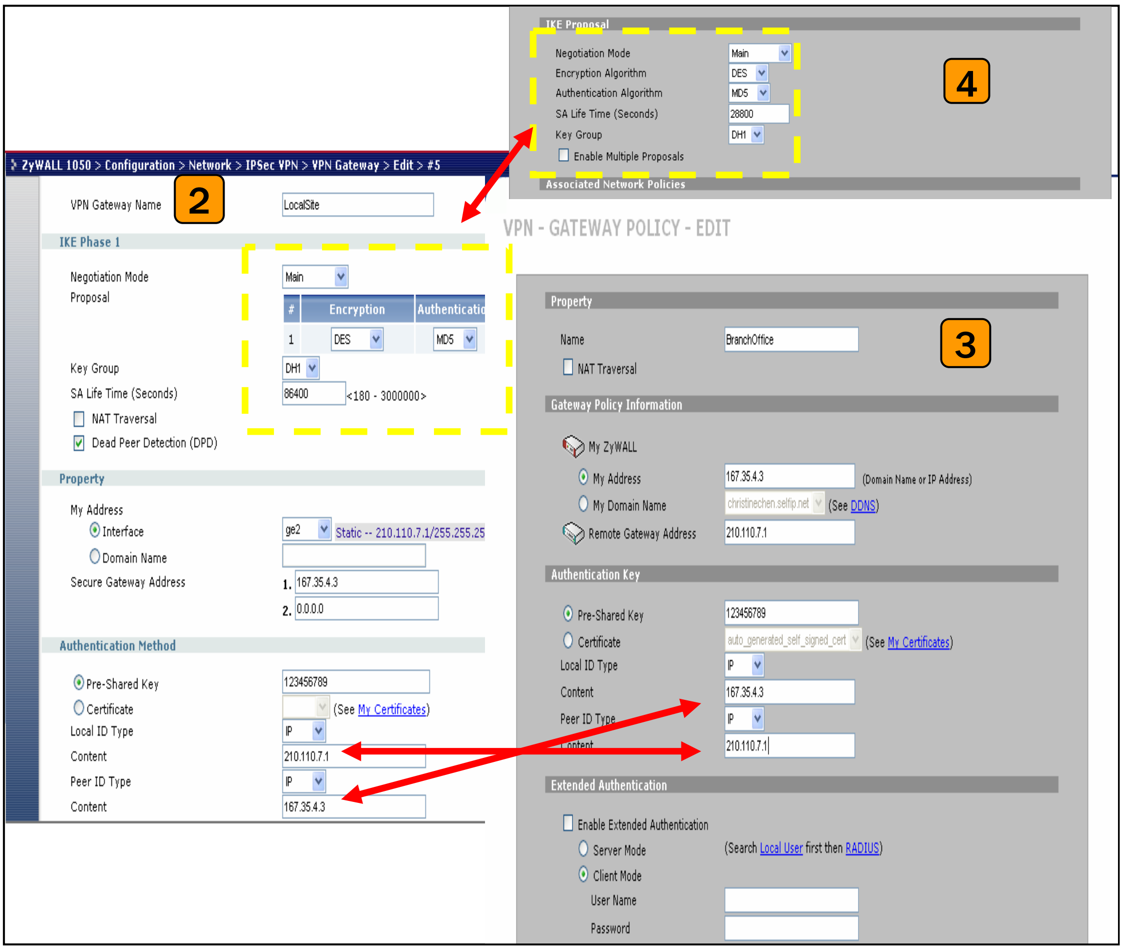
● Use Fixed IP Address

| | |
|---|---|
| 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 **Configuration** > **Network** > **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 1050. **My Address** and **Remote Gateway Address** are ZyWALL70 and ZyWALL 1050 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 1050.

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.



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway > Edit > #5

VPN Gateway Name: LocalSite

IKE Phase 1

Negotiation Mode: Main

Proposal:

| # | Encryption | Authenticatio |
|---|---|---|
| 1 | DES | MD5 |

Key Group: DH1

SA Life Time (Seconds): 86400 <180 - 3000000>

☐ NAT Traversal

☑ Dead Peer Detection (DPD)

Property

My Address
● Interface: ge2 Static -- 210.110.7.1/255.255.25
○ Domain Name

Secure Gateway Address: 1. 167.35.4.3 2. 0.0.0.0

Authentication Method

● Pre-Shared Key: 123456789
○ Certificate (See My Certificates)
Local ID Type: IP
Content: 210.110.7.1
Peer ID Type: IP
Content: 167.35.4.3

IKE Proposal

Negotiation Mode: Main
Encryption Algorithm: DES
Authentication Algorithm: MD5
SA Life Time (Seconds): 28800
Key Group: DH1
☐ Enable Multiple Proposals

Associated Network Policies

VPN - GATEWAY POLICY - EDIT

Property

Name: BranchOffice
☐ NAT Traversal

Gateway Policy Information

My ZyWALL
● My Address: 167.35.4.3 (Domain Name or IP Address)
○ My Domain Name: christinechen.selfip.net (See DDNS)
Remote Gateway Address: 210.110.7.1

Authentication Key

● Pre-Shared Key: 123456789
○ Certificate: auto_generated_self_signed_cert (See My Certificates)
Local ID Type: IP
Content: 167.35.4.3
Peer ID Type: IP
Content: 210.110.7.1

Extended Authentication

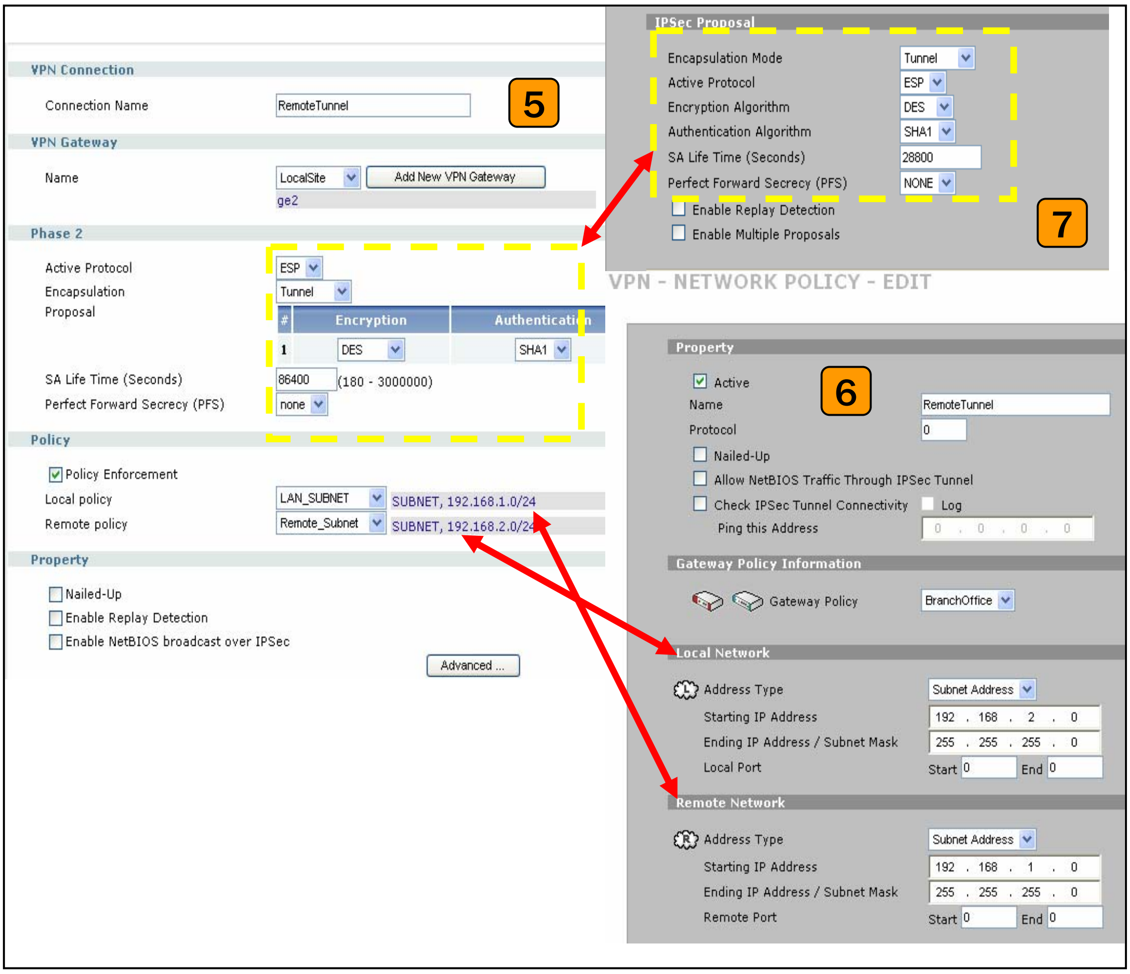
☐ Enable Extended Authentication
○ Server Mode (Search Local User first then RADIUS)
● Client Mode
User Name:
Password:

5) Switch to **Configuration** > **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 ZyWALL1050 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.



VPN Connection

Connection Name: RemoteTunnel

VPN Gateway

Name: LocalSite [Add New VPN Gateway]
ge2

Phase 2

Active Protocol: ESP
Encapsulation: Tunnel
Proposal:

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | SHA1 |

SA Life Time (Seconds): 86400 (180 - 3000000)
Perfect Forward Secrecy (PFS): none

Policy

☑ Policy Enforcement
Local policy: LAN_SUBNET SUBNET, 192.168.1.0/24
Remote policy: Remote_Subnet SUBNET, 192.168.2.0/24

Property

□ Nailed-Up
□ Enable Replay Detection
□ Enable NetBIOS broadcast over IPSec

[Advanced ...]

IPSec Proposal

Encapsulation Mode: Tunnel
Active Protocol: ESP
Encryption Algorithm: DES
Authentication Algorithm: SHA1
SA Life Time (Seconds): 28800
Perfect Forward Secrecy (PFS): NONE
□ Enable Replay Detection
□ Enable Multiple Proposals

VPN - NETWORK POLICY - EDIT

Property

☑ Active
Name: RemoteTunnel
Protocol: 0
□ Nailed-Up
□ Allow NetBIOS Traffic Through IPSec Tunnel
□ Check IPSec Tunnel Connectivity □ Log
Ping this Address: 0 . 0 . 0 . 0

Gateway Policy Information

Gateway Policy: BranchOffice

Local Network

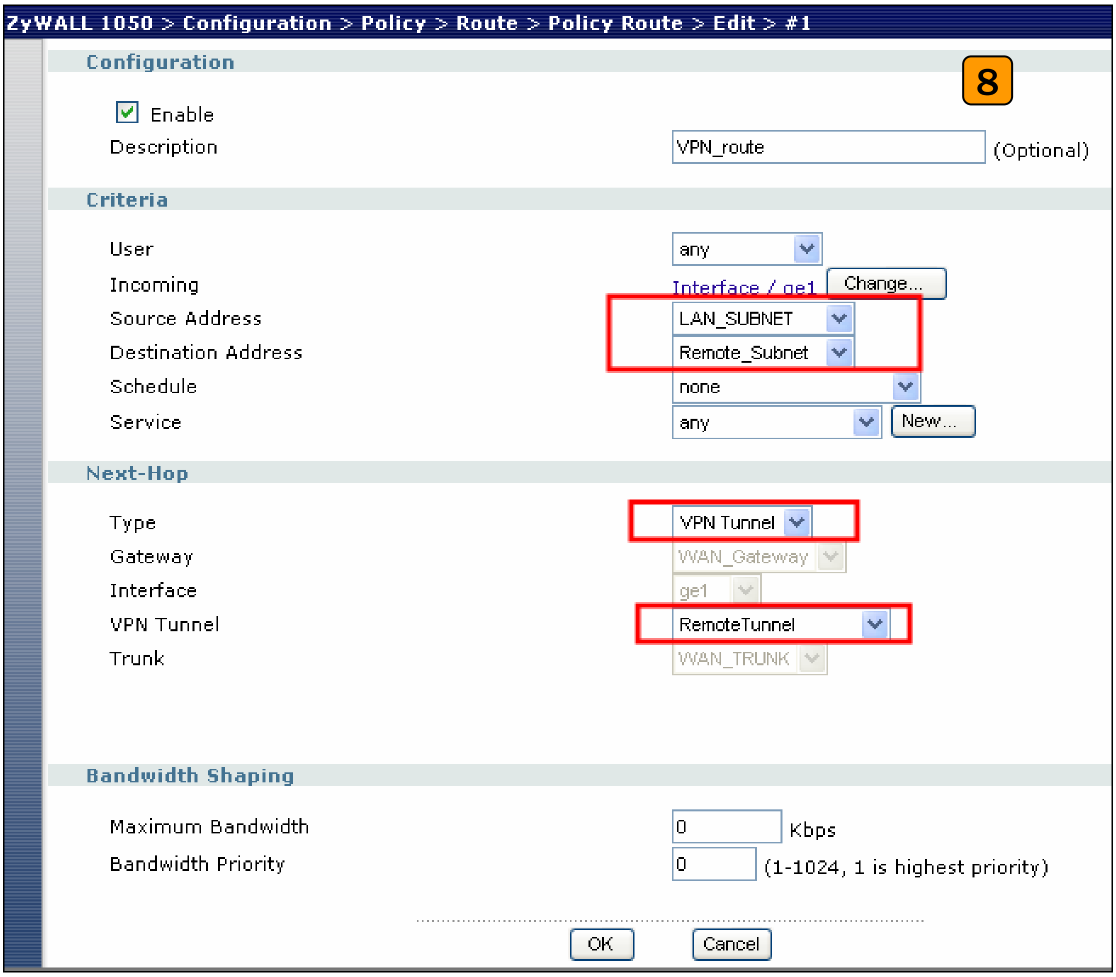
Address Type: Subnet Address
Starting IP Address: 192 . 168 . 2 . 0
Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0
Local Port: Start 0 End 0

Remote Network

Address Type: Subnet Address
Starting IP Address: 192 . 168 . 1 . 0
Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0
Remote Port: Start 0 End 0

8) The ZyWALL1050 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 ZyWALL1050 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 **Configuration** > **Policy** > **Route** > **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 1050 > Configuration > Policy > Route > Policy Route > Edit > #1

**Configuration**

☑ Enable

Description: VPN_route (Optional)

**Criteria**

| | |
|---|---|
| User | any |
| Incoming | Interface / ge1 |
| Source Address | LAN_SUBNET |
| Destination Address | Remote_Subnet |
| Schedule | none |
| Service | any |

**Next-Hop**

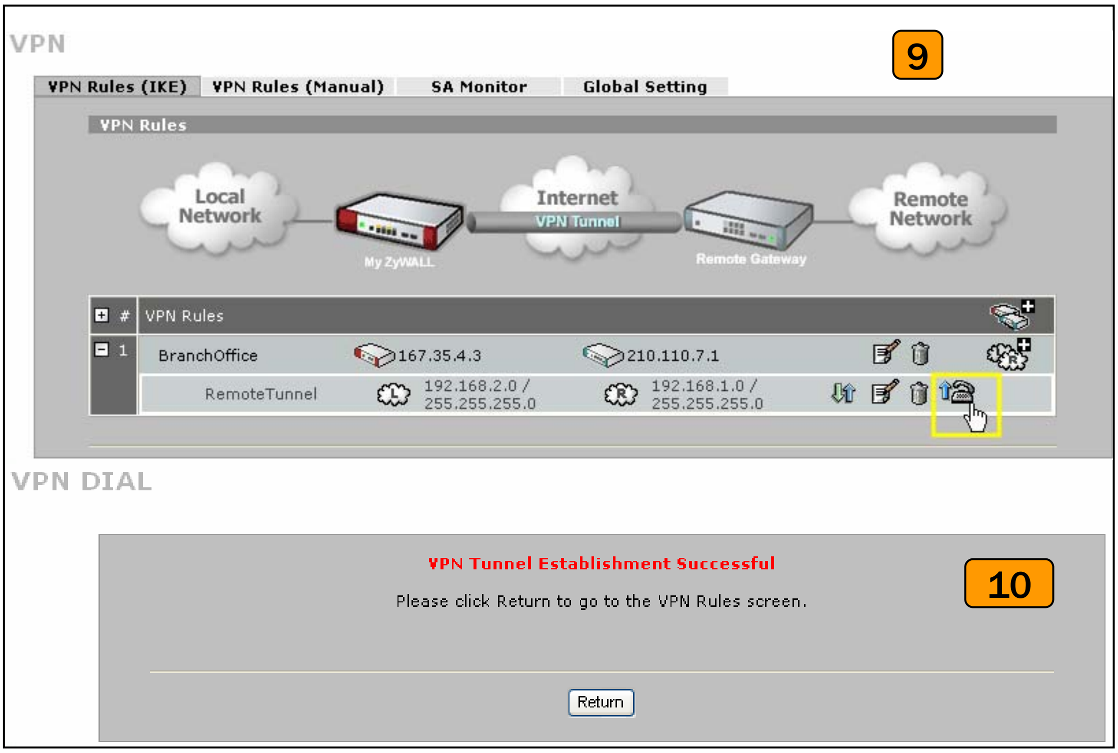
| | |
|---|---|
| Type | VPN Tunnel |
| Gateway | WAN_Gateway |
| Interface | ge1 |
| VPN Tunnel | RemoteTunnel |
| Trunk | WAN_TRUNK |

**Bandwidth Shaping**

| | |
|---|---|
| Maximum Bandwidth | 0 Kbps |
| Bandwidth Priority | 0 (1-1024, 1 is highest priority) |

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

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



| # | VPN Rules | | |
|---|---|---|---|
| 1 | BranchOffice | 167.35.4.3 | 210.110.7.1 |
| | RemoteTunnel | 192.168.2.0 / 255.255.255.0 | 192.168.1.0 / 255.255.255.0 |

VPN Tunnel Establishment Successful

Please click Return to go to the VPN Rules screen.

**The CLI command for application:**

ZyWALL 1050 VPN Gateway:

```
[0] isakmp policy LocalSite
[1] mode main
[2] transform-set des-md5
[3] lifetime 86400
[4] no natt
[5] dpd
[6] local-ip interface ge2
[7] peer-ip 167.35.4.3 0.0.0.0
[8] authentication pre-share
[9] keystring 123456789
[10] local-id type ip 210.110.7.1
[11] peer-id type ip 167.35.4.3
[12] peer-id type ip 167.35.4.3
[13] xauth type server default deactivate
[14] group1
[15] exit
```

ZyWALL 1050 VPN Connection:

```
[0] crypto map RemoteTunnel
[1] ipsec-isakmp LocalSite
[2] encapsulation tunnel
[3] transform-set esp-des-sha
[4] set security-association lifetime seconds 86400
```

```
[5] set pfs none
[6] policy-enforcement
[7] local-policy LAN_SUBNET
[8] remote-policy Remote_Subnet
[9] no nail-up
[10] no replay-detection
[11] no netbios-broadcast
[12] no out-snat activate
[13] no in-snat activate
[14] no in-dnat activate
[15] exit
```

Policy Route for VPN traffic:

```
[0] policy 1
[1] no deactivate
[2] no description
[3] no user
[4] interface ge1
[5] source LAN_SUBNET
[6] destination Remote_Subnet
[7] no schedule
[8] service any
[9] no snat
[10] next-hop tunnel RemoteTunnel
[11] no bandwidth
[12] exit
```

**Tips for application:**

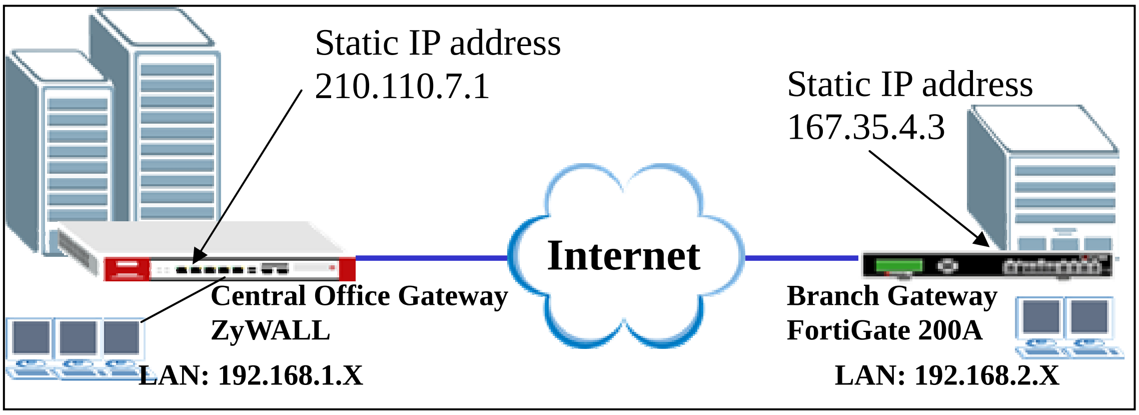
1. Make sure the **presharekey** is the same in both the local and the remote gateways.
2. Make sure the **IKE & IPSec proposal** is the same in both the local and the remote gateways.
3. Select the correct **interface** for the VPN connection.
4. The **Local** and **Peer** ID type and content must be the opposite and not of the same content.
5. Make sure the **VPN policy route** had been setup in ZyWALL 1050.

### 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 1050 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.

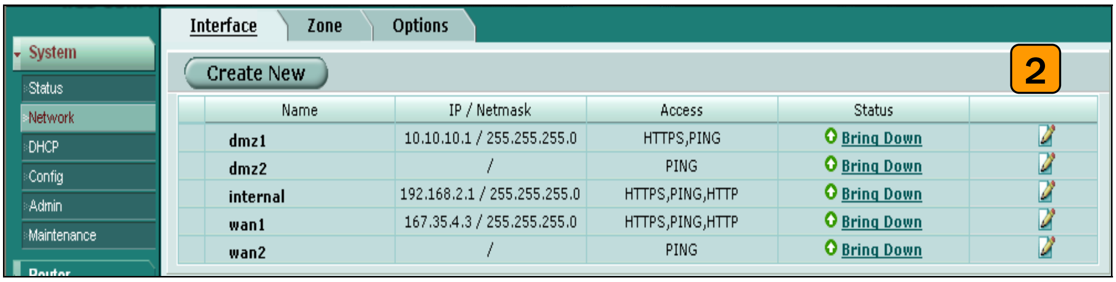


The central office gateway ZyWALL 1050's interface and VPN setting retain the same setting as in the previous example. If you jumped this section first, please refer to 'ZyWALL 1050 to ZYWALL70 VPN tunnel setting' on page 8.
This list below is to briefly show the VPN phase1 and phase2 configuration parameters:

| ZyWALL | FortiGate |
|---|---|
| WAN: 210.110.7.1<br>LAN: 192.168.1.0/24 | WAN: 167.35.4.3<br>LAN:   192.168.2.0/24 |
| Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES | Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES |

| | |
|---|---|
| Authentication :MD5<br>Key Group :DH1 | Authentication :MD5<br>Key Group :DH1 |
| Phase2<br>Encapsulation: Tunnel<br>Active Protocol: ESP<br>Encryption: DES<br>Authentication: SHA1<br>Perfect Forward Secrecy (PFS): None | Phase2<br>Encapsulation: Tunnel<br>Active Protocol: ESP<br>Encryption: DES<br>Authentication: SHA1<br>Perfect Forward Secrecy (PFS): None |

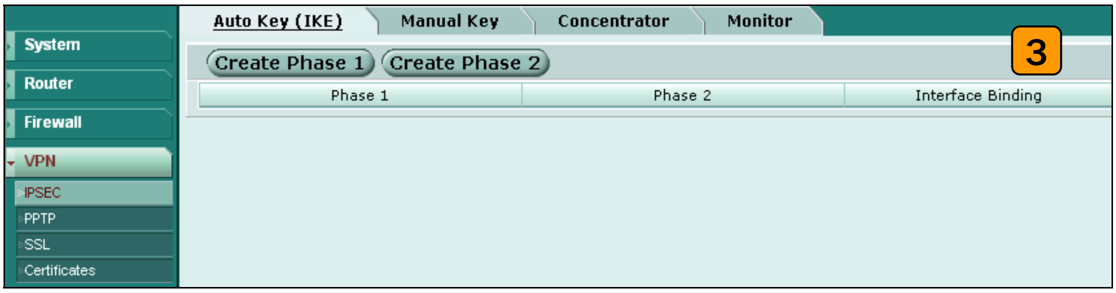
1) Configure the ZyWALL1050 ‘s VPN gateway and VPN connection as on the list. Also, remember to configure the policy route for the VPN traffic routing. Refer to the previous scenario or user guide to find help on setting the ZyWALL1050 VPN.
2) Login to the FortiGate GUI and switch to System > Network > Interface and set the wan1 interface to 167.35.4.3 and internal interface to 192.168.2.1/255.255.255.0.



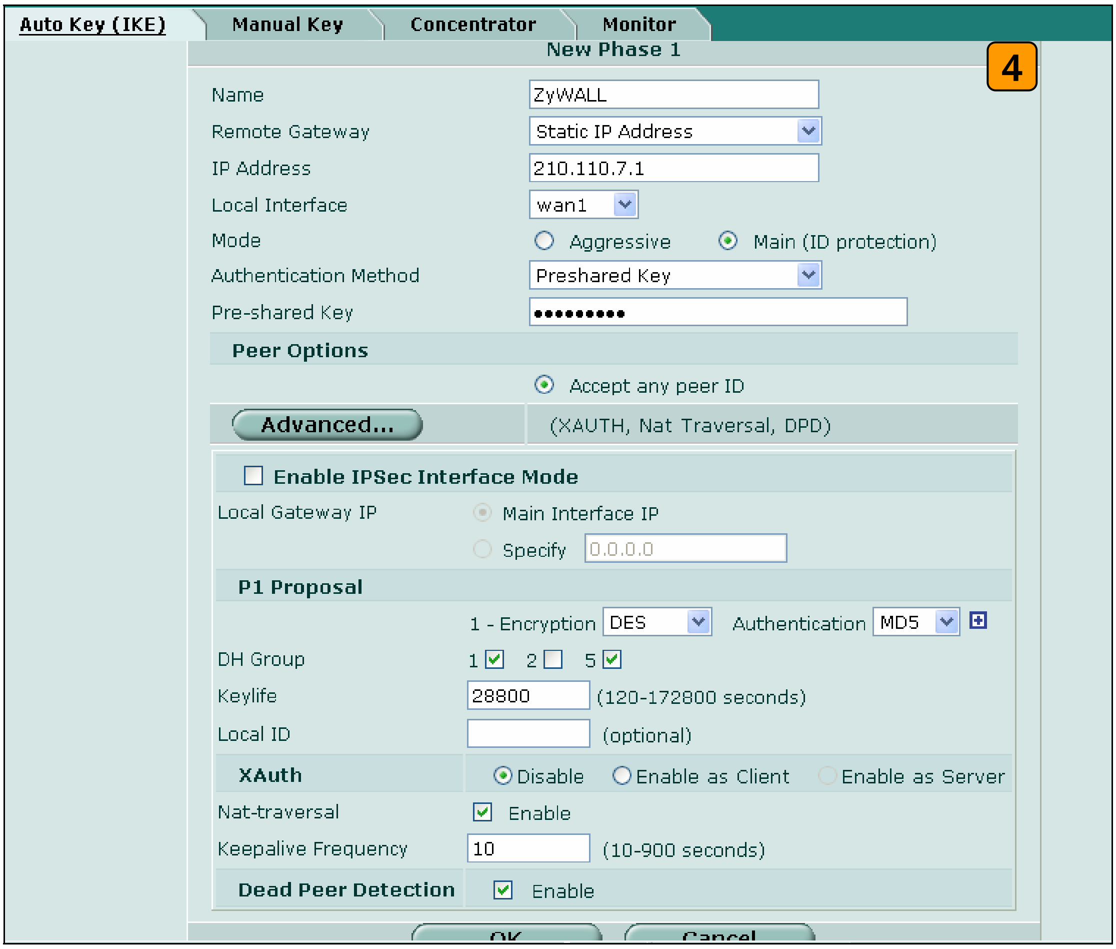
| Name | IP / Netmask | Access | Status |
|---|---|---|---|
| dmz1 | 10.10.10.1 / 255.255.255.0 | HTTPS,PING | Bring Down |
| dmz2 | / | PING | Bring Down |
| internal | 192.168.2.1 / 255.255.255.0 | HTTPS,PING,HTTP | Bring Down |
| wan1 | 167.35.4.3 / 255.255.255.0 | HTTPS,PING,HTTP | Bring Down |
|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



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 ZyWALL1050.



New Phase 1

| | |
|---|---|
| Name | ZyWALL |
| Remote Gateway | Static IP Address |
| IP Address | 210.110.7.1 |
| Local Interface | wan1 |
| Mode | ○ Aggressive ● Main (ID protection) |
| Authentication Method | Preshared Key |
| Pre-shared Key | ●●●●●●●●● |

Peer Options

● Accept any peer ID

Advanced... (XAUTH, Nat Traversal, DPD)

□ Enable IPSec Interface Mode

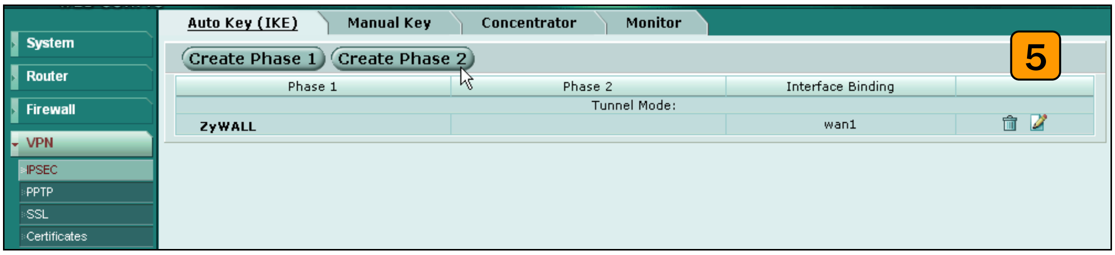
| | |
|---|---|
| Local Gateway IP | ● Main Interface IP<br>○ Specify 0.0.0.0 |

P1 Proposal

| | |
|---|---|
| | 1 - Encryption DES Authentication MD5 |
| DH Group | 1 ☑ 2 □ 5 ☑ |
| Keylife | 28800 (120-172800 seconds) |
| Local ID | (optional) |
| XAuth | ● Disable ○ Enable as Client ○ Enable as Server |
| Nat-traversal | ☑ Enable |
| Keepalive Frequency | 10 (10-900 seconds) |
| Dead Peer Detection | ☑ Enable |

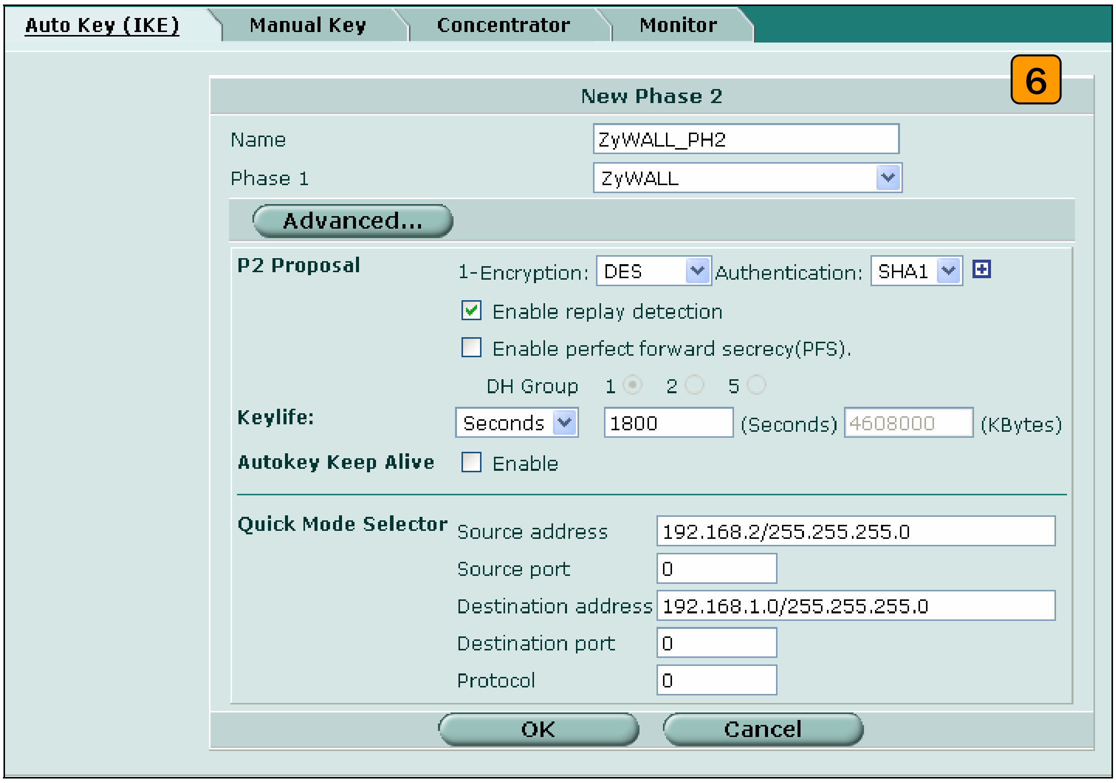
OK Cancel

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



| Phase 1 | Phase 2 | Interface Binding |
|---|---|---|
| | Tunnel Mode: | |
| ZyWALL | | wan1 |

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 1050 phase 2.



New Phase 2

Name: ZyWALL_PH2

Phase 1: ZyWALL

P2 Proposal: 1-Encryption: DES Authentication: SHA1

☑ Enable replay detection

☐ Enable perfect forward secrecy(PFS).

DH Group 1 ● 2 ○ 5 ○

Keylife: Seconds 1800 (Seconds) 4608000 (KBytes)

Autokey Keep Alive: ☐ Enable

Quick Mode Selector

Source address: 192.168.2/255.255.255.0

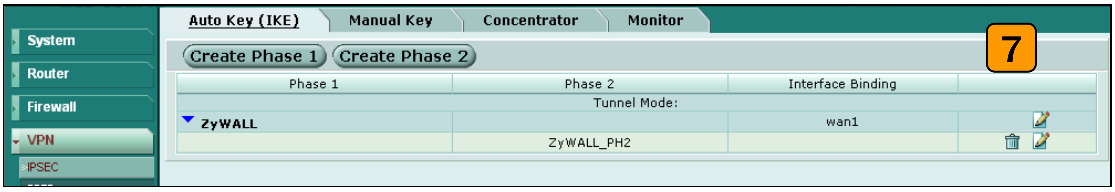
Source port: 0

Destination address: 192.168.1.0/255.255.255.0

Destination port: 0

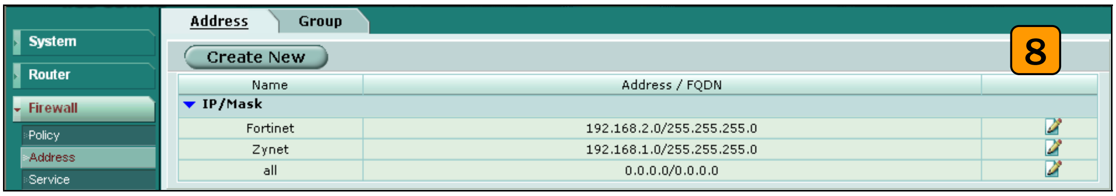
Protocol: 0

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.



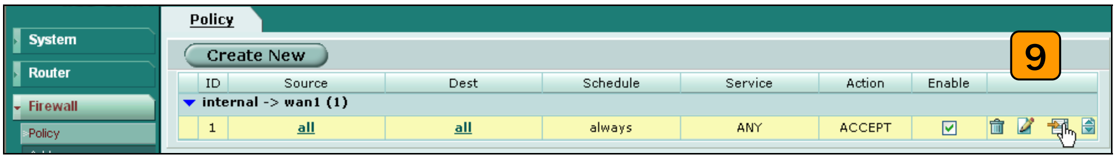
| Phase 1 | Phase 2 | Interface Binding |
|---|---|---|
| | Tunnel Mode: | |
| ZyWALL | | wan1 |
| | ZyWALL_PH2 | |

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 objects which stand for ZyWALL LAN subnet and FortiGate LAN subnet. Using the “**Create New**” button to create a new address object.



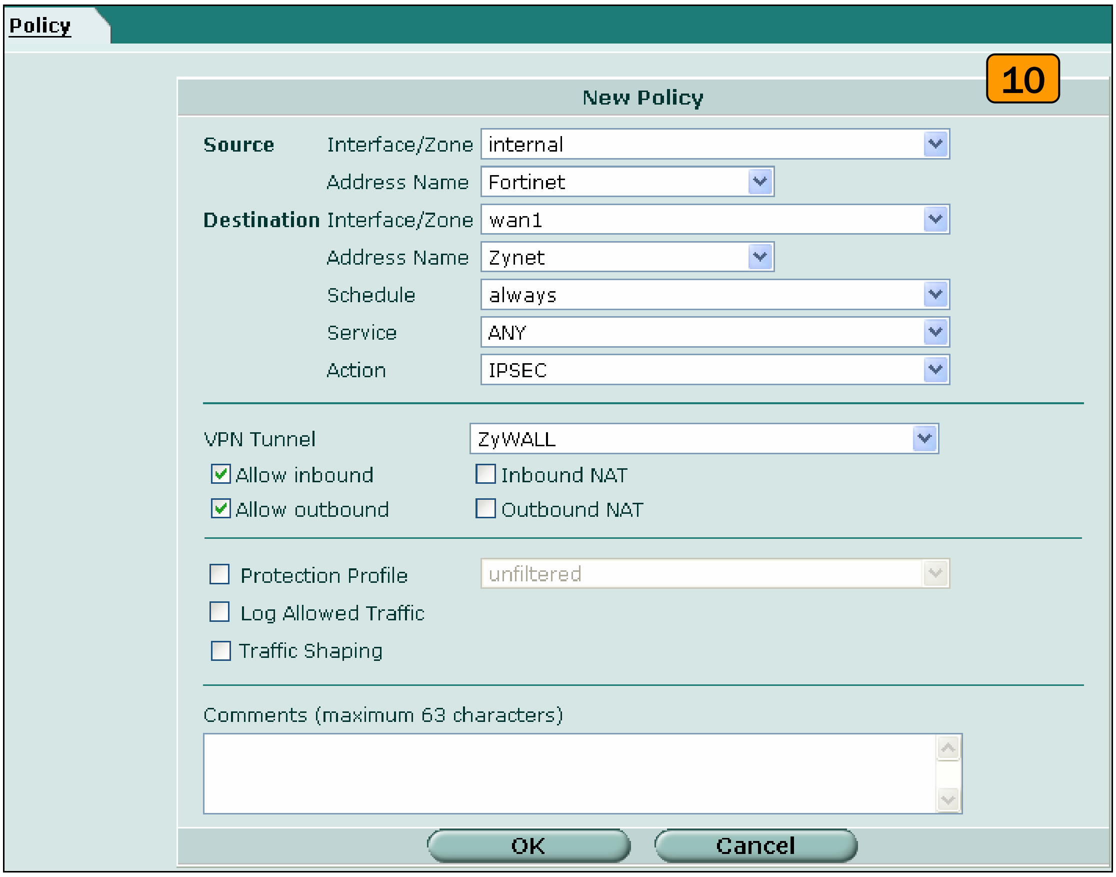
| Name | Address / FQDN |
|---|---|
| IP/Mask | |
| Fortinet | 192.168.2.0/255.255.255.0 |
| Zynet | 192.168.1.0/255.255.255.0 |
| all | 0.0.0.0/0.0.0.0 |

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



| ID | Source | Dest | Schedule | Service | Action | Enable |
|---|---|---|---|---|---|---|
| internal -> wan1 (1) | | | | | | |
| 1 | all | all | always | ANY | ACCEPT | ☑ |

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.



New Policy

| | | |
|---|---|---|
| Source | Interface/Zone | internal |
| | Address Name | Fortinet |
| Destination | Interface/Zone | wan1 |
| | Address Name | Zynet |
| | Schedule | always |
| | Service | ANY |
| | Action | IPSEC |

VPN Tunnel: ZyWALL

☑ Allow inbound ☐ Inbound NAT

☑ Allow outbound ☐ Outbound NAT

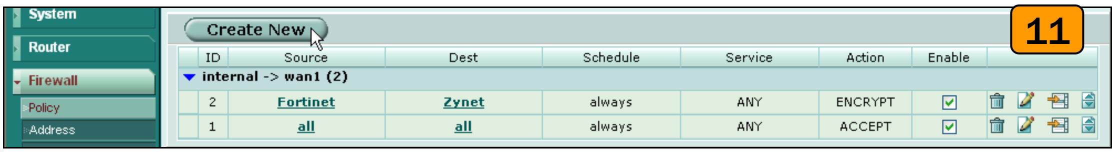
☐ Protection Profile: unfiltered

☐ Log Allowed Traffic

☐ Traffic Shaping

Comments (maximum 63 characters)

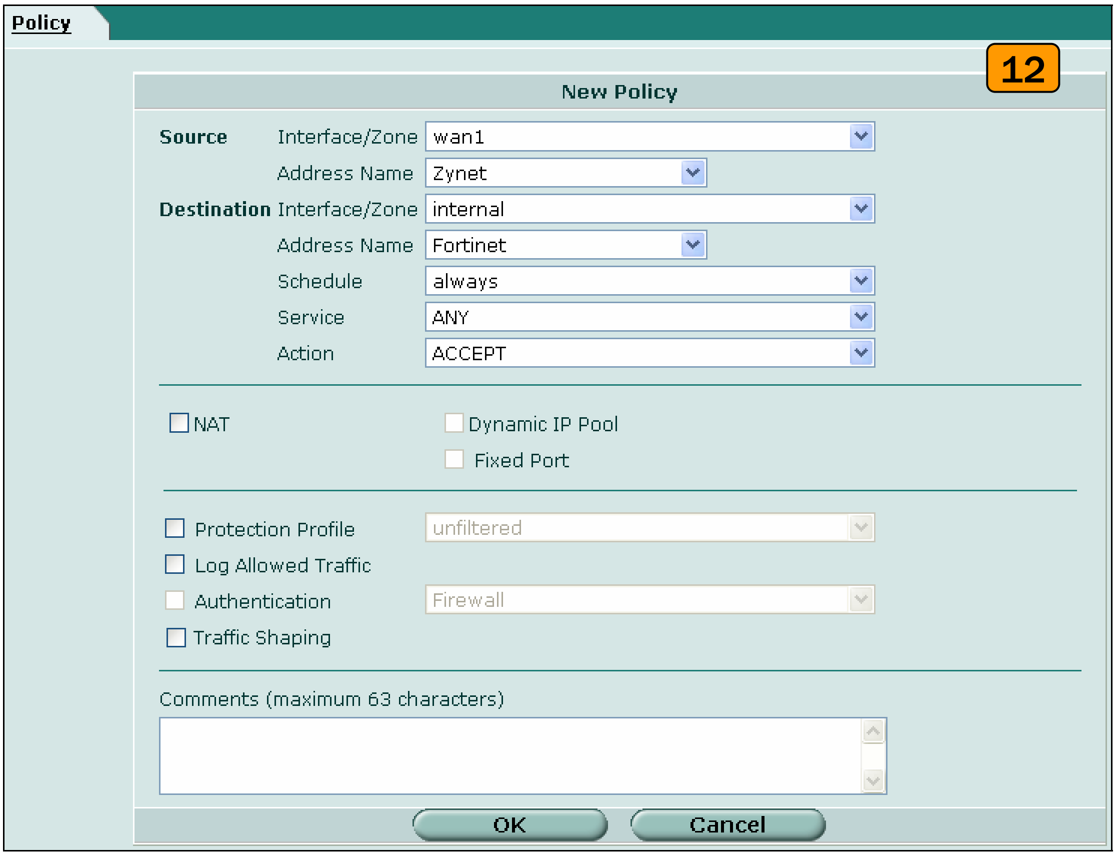
11) Switch to **Firewall** > **Policy** and click “Create New” button to add new policy for the VPN traffic from ZyWALL to FortiGate.



| ID | Source | Dest | Schedule | Service | Action | Enable |
|---|---|---|---|---|---|---|
| internal -> wan1 (2) | | | | | | |
| 2 | Fortinet | Zynet | always | ANY | ENCRYPT | ☑ |
| 1 | all | all | always | ANY | ACCEPT | ☑ |

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.



| | | |
|---|---|---|
| **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

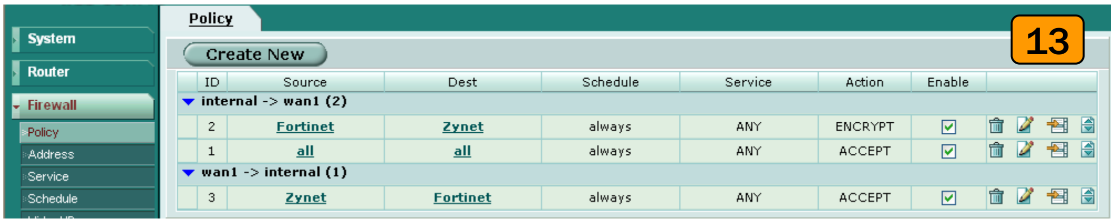
□ Log Allowed Traffic

□ Authentication　Firewall

□ Traffic Shaping

Comments (maximum 63 characters)

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



| ID | Source | Dest | Schedule | Service | Action | Enable |
|---|---|---|---|---|---|---|
| internal -> wan1 (2) | | | | | | |
| 2 | Fortinet | Zynet | always | ANY | ENCRYPT | ☑ |
| 1 | all | all | always | ANY | ACCEPT | ☑ |
| wan1 -> internal (1) | | | | | | |
| 3 | Zynet | Fortinet | always | ANY | ACCEPT | ☑ |

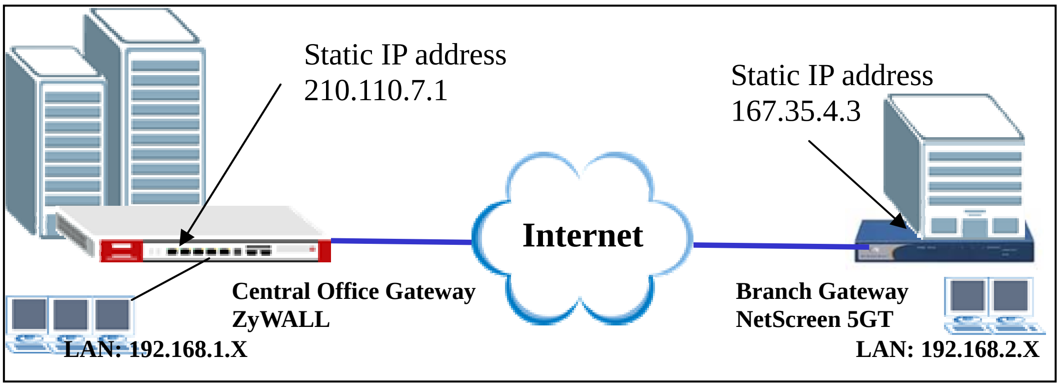
## Tips for application:

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 ZyWALL1050.
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 1050 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.



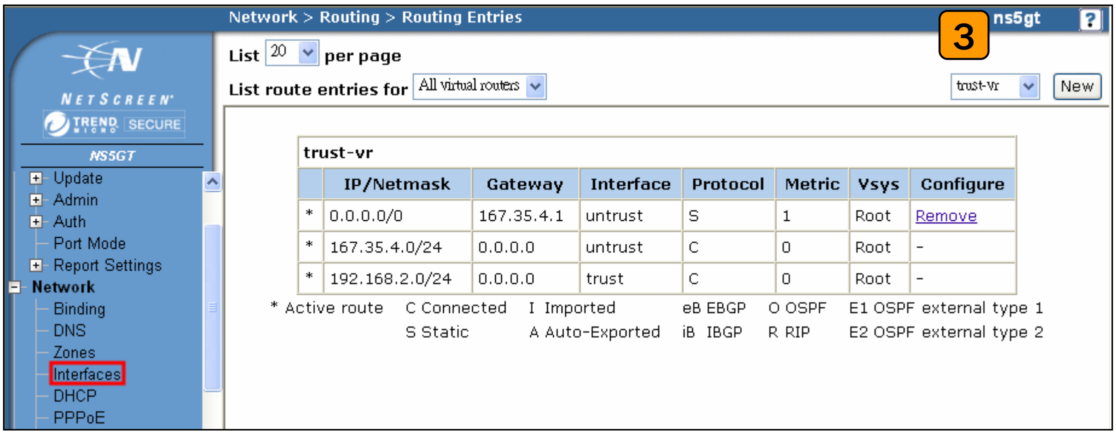
The central office gateway ZyWALL 1050's interface and VPN setting retain the same settings as in the previous example. If you jumped to this section first, please refer to 'ZyWALL1050 to ZYWALL70 VPN tunnel setting' on the page 8.

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

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

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

1) Configure the ZyWALL1050 ‘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 1050 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

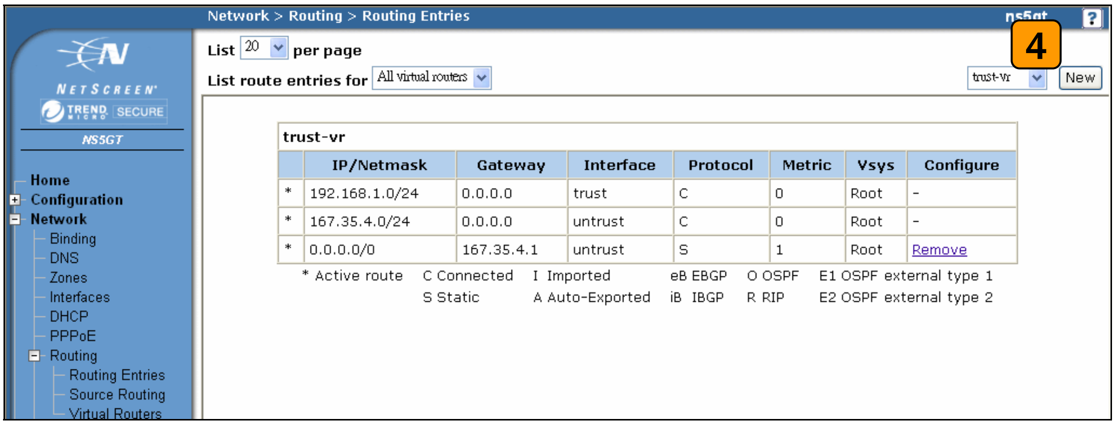
trust-vr

| | IP/Netmask | Gateway | Interface | Protocol | Metric | Vsys | Configure |
|---|---|---|---|---|---|---|---|
| * | 0.0.0.0/0 | 167.35.4.1 | untrust | S | 1 | Root | Remove |
| * | 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.



Network > Routing > Routing Entries

List 20 per page

List route entries for All virtual routers

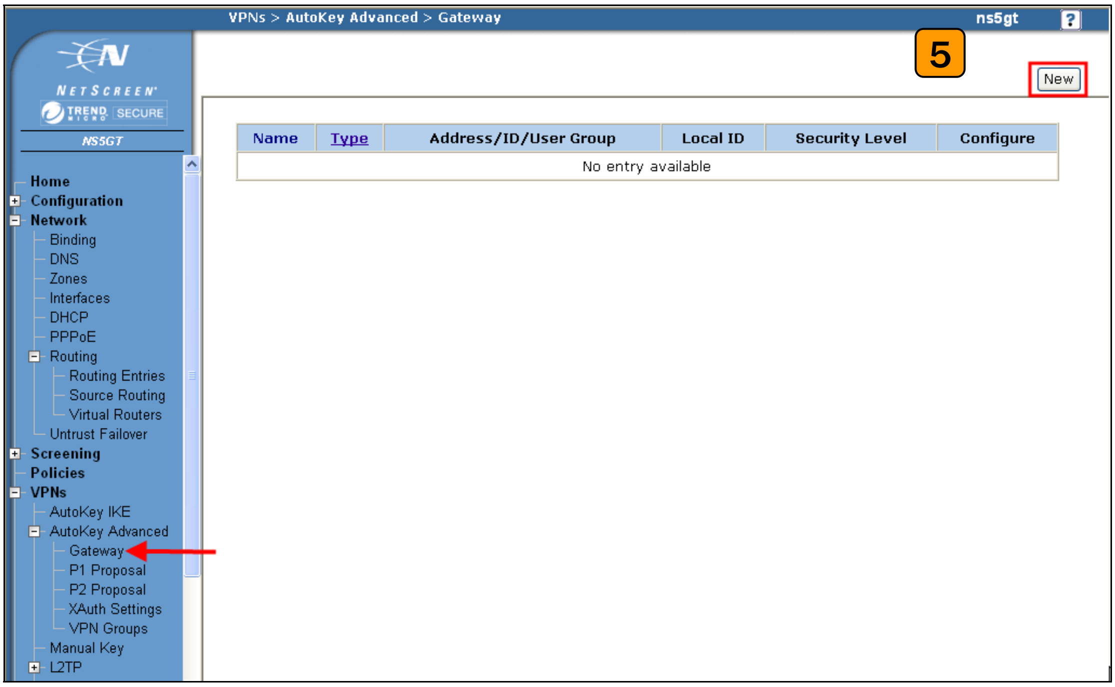
trust-vr New

trust-vr

|  | IP/Netmask | Gateway | Interface | Protocol | Metric | Vsys | Configure |
|---|---|---|---|---|---|---|---|
| * | 192.168.1.0/24 | 0.0.0.0 | trust | C | 0 | Root | - |
| * | 167.35.4.0/24 | 0.0.0.0 | untrust | C | 0 | Root | - |
| * | 0.0.0.0/0 | 167.35.4.1 | untrust | S | 1 | Root | Remove |

```
* 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
```

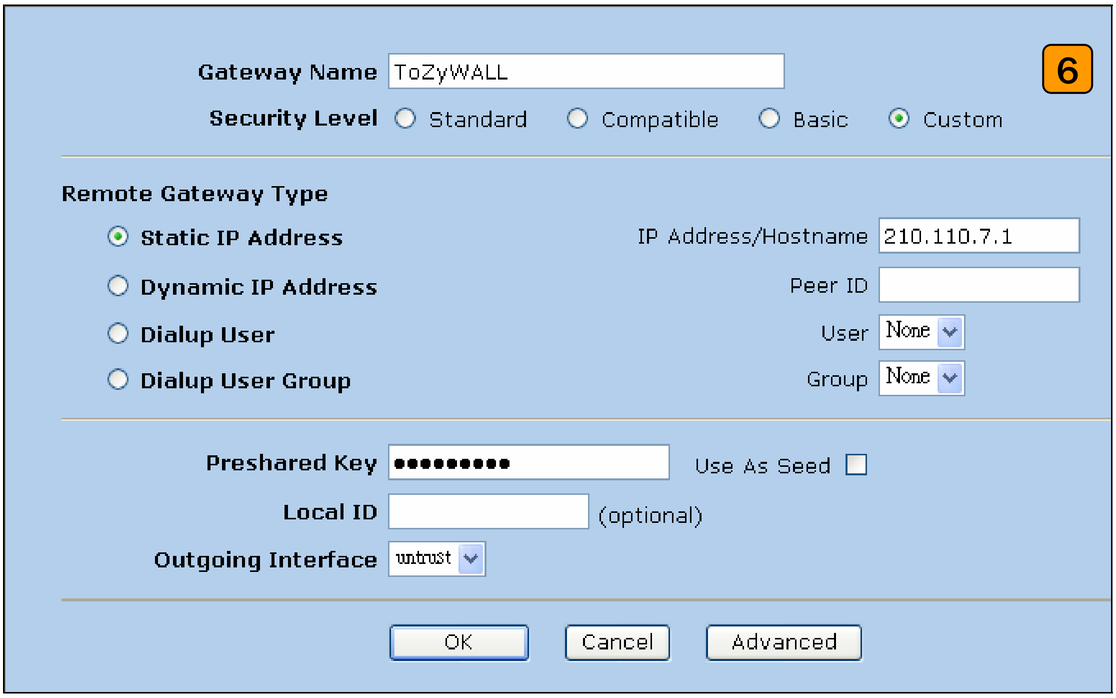
5) To edit the IPSec rule, first set the gateway policy and then edit the IKE policy. Switch to **VPNs** > **AutoKey Advanced > Gateway**, and then press the **New** button.



VPNs > AutoKey Advanced > Gateway

| Name | Type | Address/ID/User Group | Local ID | Security Level | Configure |
|---|---|---|---|---|---|
| No entry available |  |  |  |  |  |

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.



Gateway Name: ToZyWALL

Security Level: ○ Standard ○ Compatible ○ Basic ● Custom

Remote Gateway Type

● Static IP Address — IP Address/Hostname: 210.110.7.1

○ Dynamic IP Address — Peer ID:

○ Dialup User — User: None

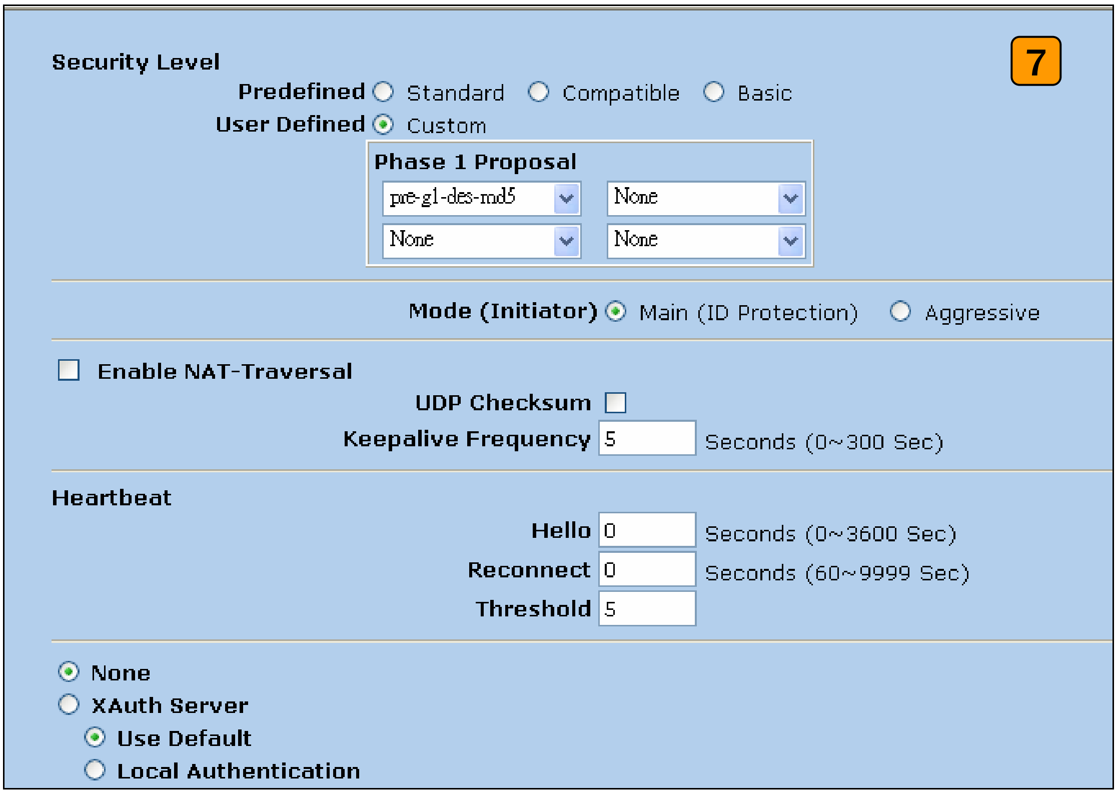
○ Dialup User Group — Group: None

Preshared Key: ●●●●●●●●●● Use As Seed □

Local ID: (optional)

Outgoing Interface: untrust

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.



Security Level

Predefined ○ Standard ○ Compatible ○ Basic

User Defined ● Custom

Phase 1 Proposal

| | |
|---|---|
| pre-g1-des-md5 | None |
| None | None |

Mode (Initiator) ● Main (ID Protection) ○ Aggressive

□ Enable NAT-Traversal

UDP Checksum □

Keepalive Frequency 5 Seconds (0~300 Sec)

Heartbeat

Hello 0 Seconds (0~3600 Sec)

Reconnect 0 Seconds (60~9999 Sec)

Threshold 5

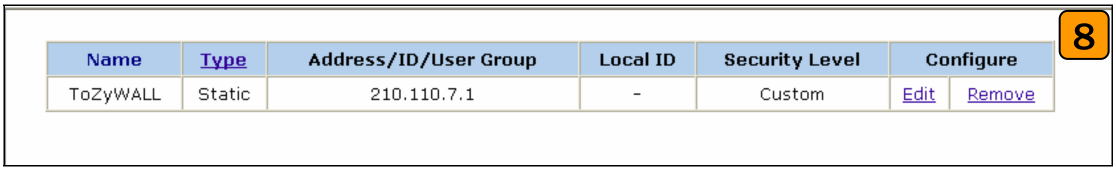
● None

○ XAuth Server

● Use Default

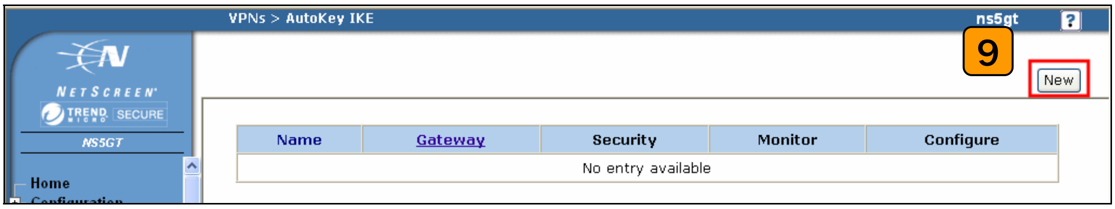
○ Local Authentication

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



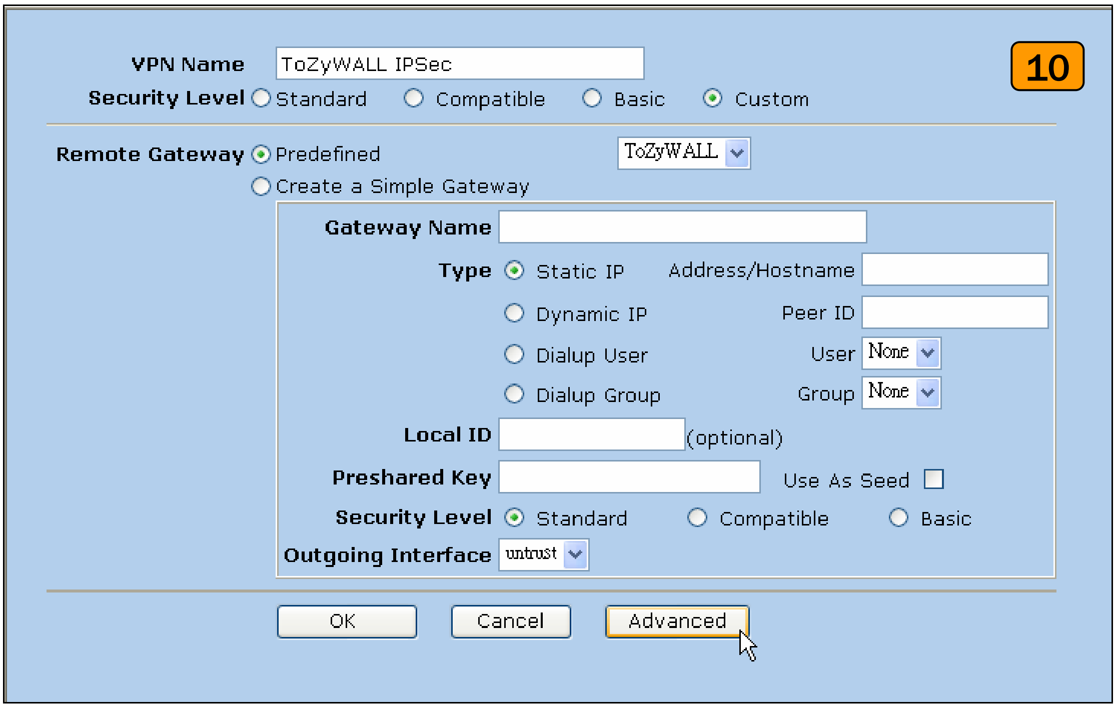
| Name | Type | Address/ID/User Group | Local ID | Security Level | Configure | |
|---|---|---|---|---|---|---|
| ToZyWALL | Static | 210.110.7.1 | - | Custom | Edit | Remove |

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



| Name | Gateway | Security | Monitor | Configure |
|---|---|---|---|---|
| No entry available | | | | |

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.



VPN Name: ToZyWALL IPSec

Security Level: ○ Standard ○ Compatible ○ Basic ● Custom

Remote Gateway: ● Predefined ToZyWALL

○ Create a Simple Gateway

Gateway Name:

Type: ● Static IP Address/Hostname:

○ Dynamic IP Peer ID:

○ Dialup User User: None

○ Dialup Group Group: None

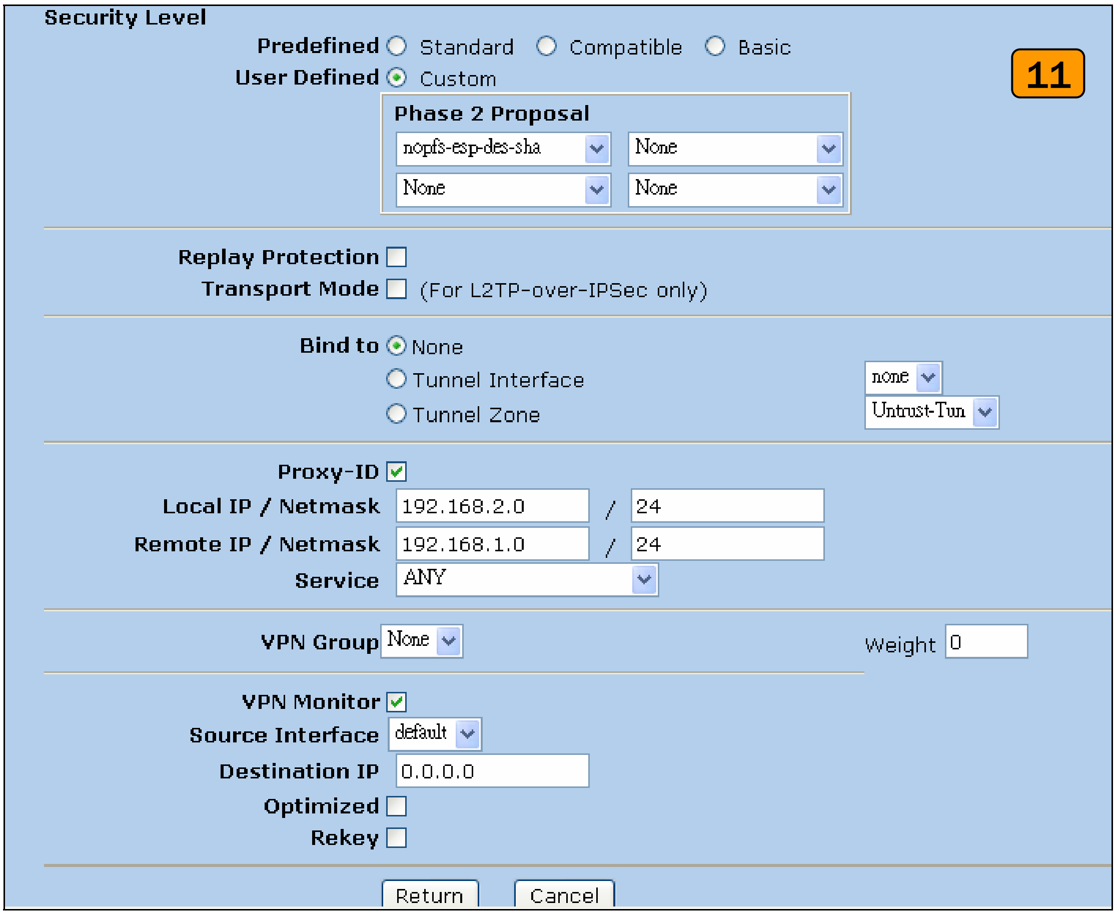
Local ID: (optional)

Preshared Key: Use As Seed □

Security Level: ● Standard ○ Compatible ○ Basic

Outgoing Interface: untrust

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 |

Replay Protection □

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

Bind to ● None

○ Tunnel Interface — none

○ Tunnel Zone — 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 ☑

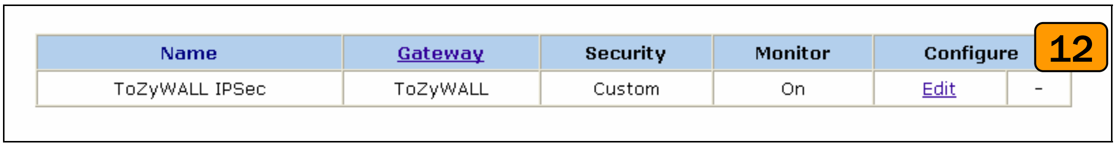
Source Interface default

Destination IP 0.0.0.0

Optimized □

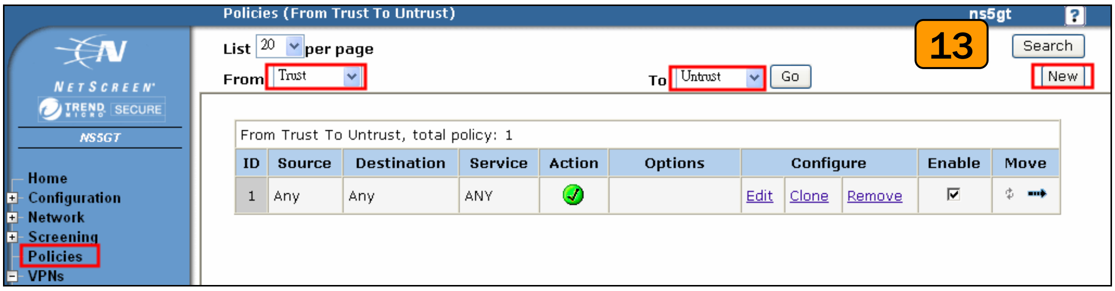
Rekey □

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 | Edit | - |

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.



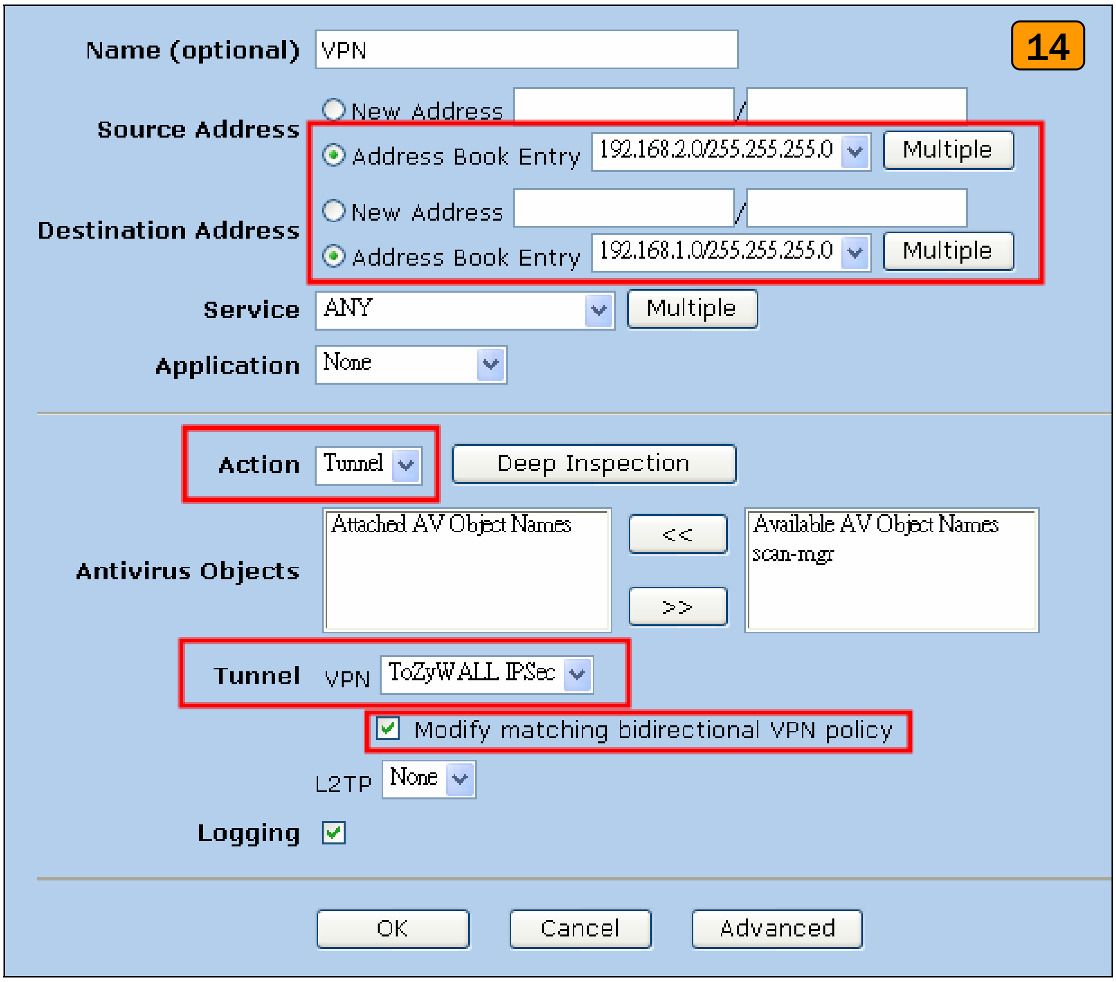
List 20 per page

From Trust — To Untrust

From Trust To Untrust, total policy: 1

| 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.


14

Name (optional): VPN

Source Address: ○ New Address / ● Address Book Entry 192.168.2.0/255.255.255.0 Multiple

Destination Address: ○ New Address / ● Address Book Entry 192.168.1.0/255.255.255.0 Multiple

Service: ANY Multiple

Application: None

Action: Tunnel Deep Inspection

Antivirus Objects: Attached AV Object Names << >> Available AV Object Names scan-mgr

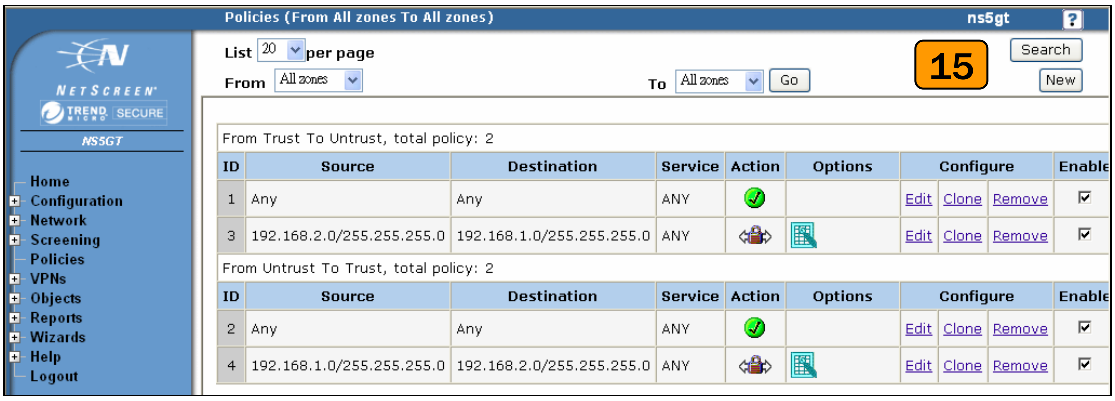
Tunnel: VPN ToZyWALL IPSec

☑ Modify matching bidirectional VPN policy

L2TP None

Logging ☑

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



List 20 per page

From All zones To All zones

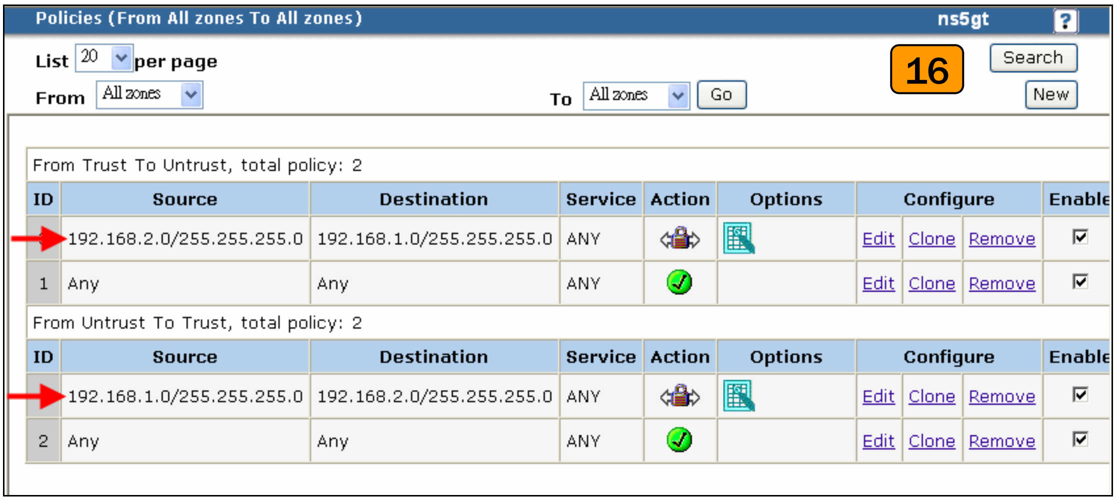
From Trust To Untrust, total policy: 2

| ID | Source | Destination | Service | Action | Options | Configure | | | Enable |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Any | Any | ANY | ✓ | | Edit | Clone | Remove | ☑ |
| 3 | 192.168.2.0/255.255.255.0 | 192.168.1.0/255.255.255.255.0 | 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.



List 20 per page

From All zones To All zones

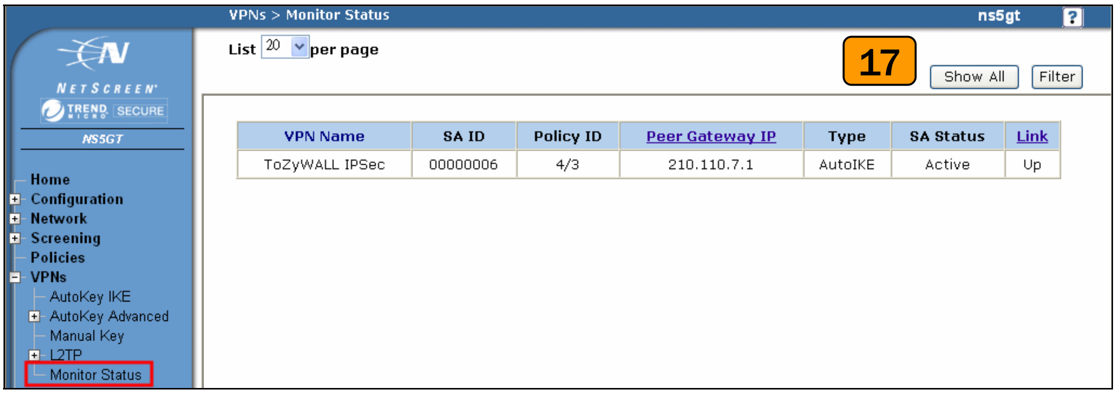
From Trust To Untrust, total policy: 2

| ID | Source | Destination | Service | Action | Options | Configure | | | Enable |
|---|---|---|---|---|---|---|---|---|---|
| | 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 |
|---|---|---|---|---|---|---|---|---|---|
| | 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.



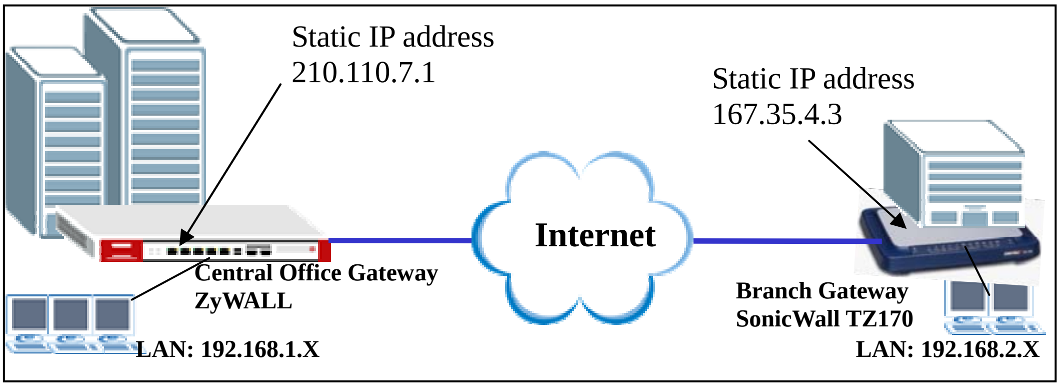
List 20 per page

| VPN Name | SA ID | Policy ID | Peer Gateway IP | Type | SA Status | Link |
|---|---|---|---|---|---|---|
| ToZyWALL IPSec | 00000006 | 4/3 | 210.110.7.1 | AutoIKE | Active | Up |

### *1.2.2.3 ZyWALL with SonicWall VPN Tunneling*

This section guides how to setup a VPN connection between the ZyWALL 1050 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.



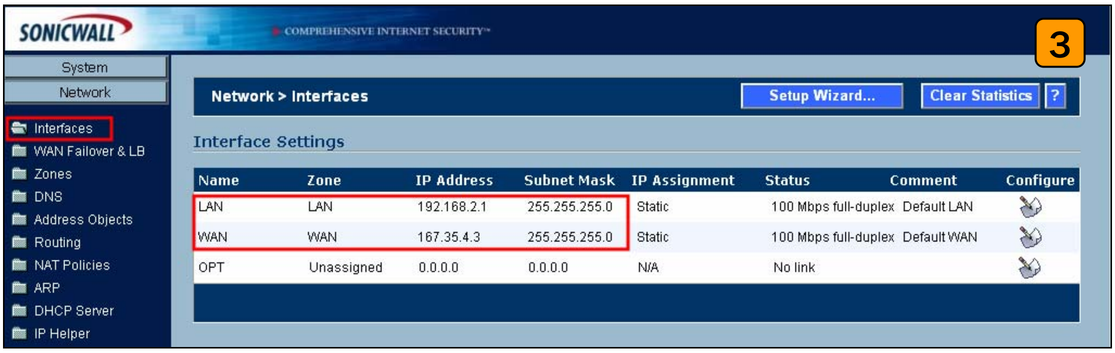
The central office gateway ZyWALL 1050's interface and VPN setting retain the same settings as in the previous example. If you jumped to this section first, please refer to 'ZyWALL1050 to ZYWALL70 VPN tunnel setting' on the page 8.

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

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

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

1) Configure the ZyWALL1050 ‘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 ZyWALL1050 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.

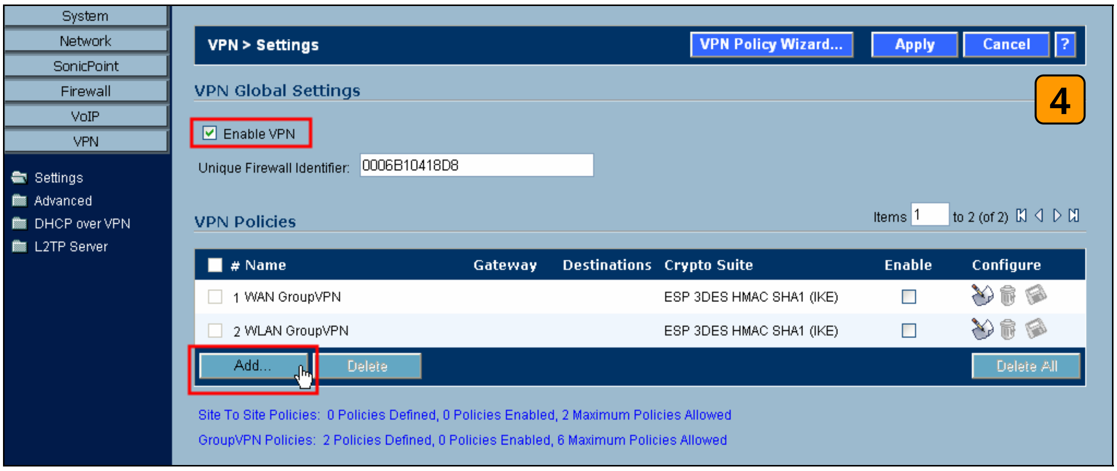


Interface Settings

| Name | Zone | IP Address | Subnet Mask | IP Assignment | Status | Comment | Configure |
|---|---|---|---|---|---|---|---|
| LAN | LAN | 192.168.2.1 | 255.255.255.0 | Static | 100 Mbps full-duplex | Default LAN | |
| WAN | WAN | 167.35.4.3 | 255.255.255.0 | Static | 100 Mbps full-duplex | Default WAN | |
| OPT | Unassigned | 0.0.0.0 | 0.0.0.0 | N/A | No link | | |

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 Global Settings

☑ Enable VPN

Unique Firewall Identifier: 0006B10418D8

VPN Policies

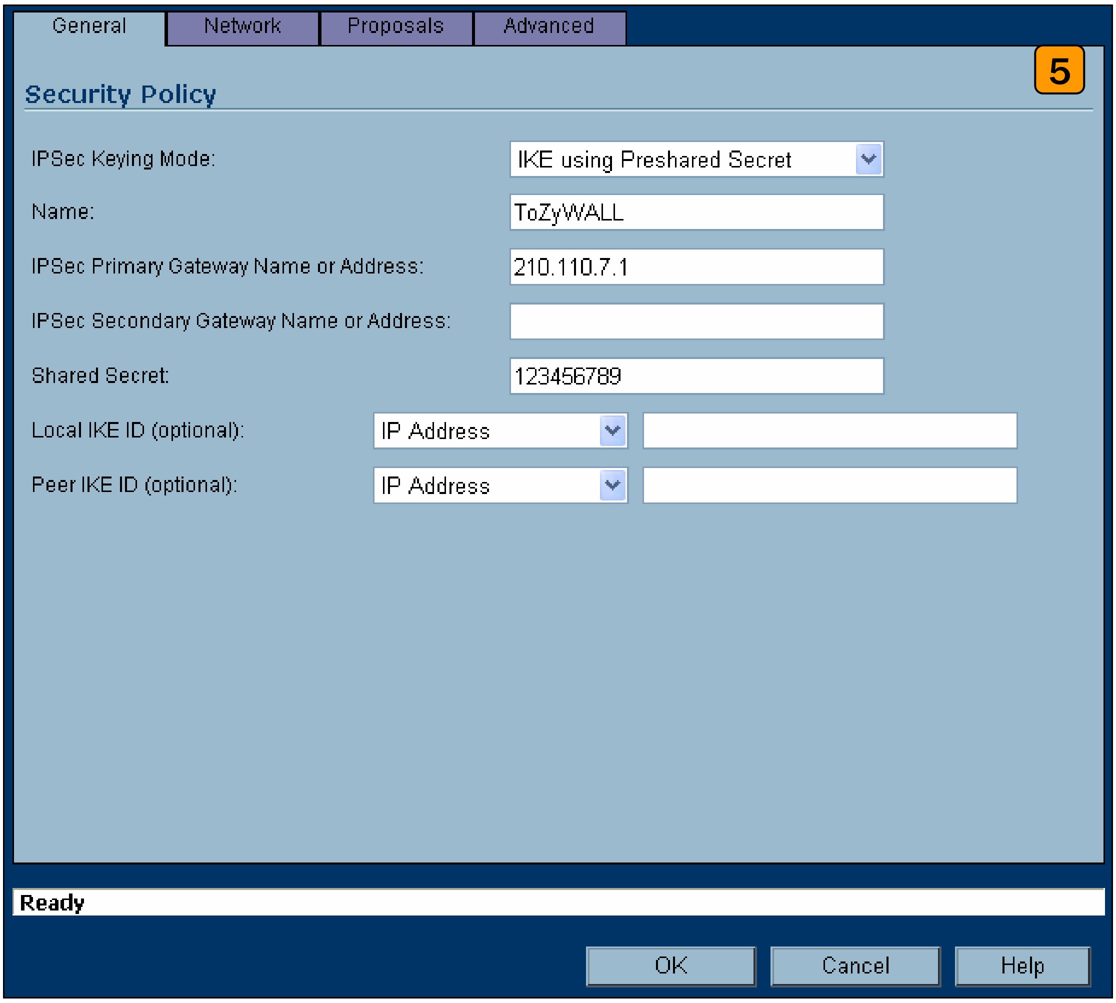
Items 1 to 2 (of 2)

| □ | # Name | Gateway | Destinations | Crypto Suite | Enable | Configure |
|---|---|---|---|---|---|---|
| □ | 1 WAN GroupVPN | | | ESP 3DES HMAC SHA1 (IKE) | □ | |
| □ | 2 WLAN GroupVPN | | | ESP 3DES HMAC SHA1 (IKE) | □ | |

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**.



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:

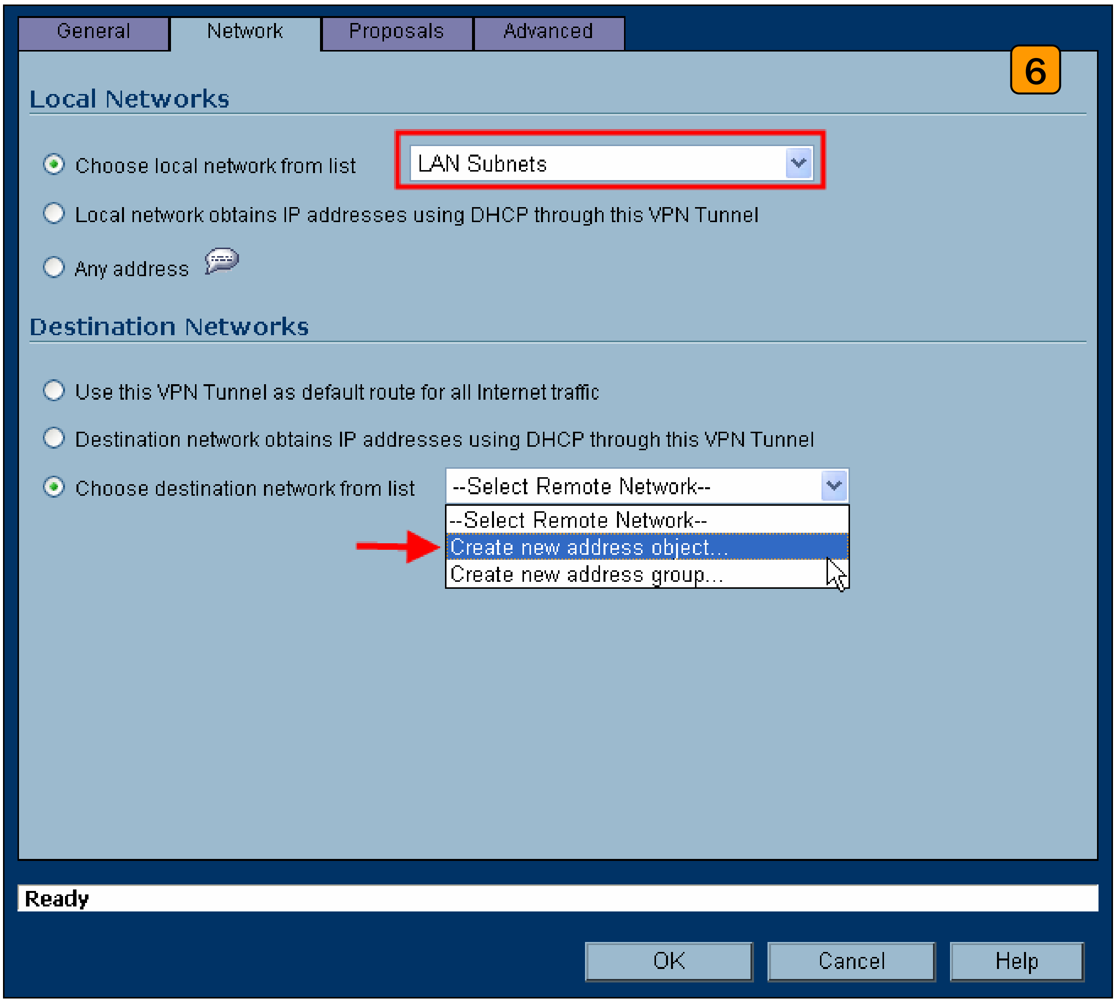
Shared Secret: 123456789

Local IKE ID (optional): IP Address

Peer IKE ID (optional): IP Address

Ready

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.



Local Networks

● Choose local network from list: LAN Subnets

○ Local network obtains IP addresses using DHCP through this VPN Tunnel

○ Any address

Destination Networks

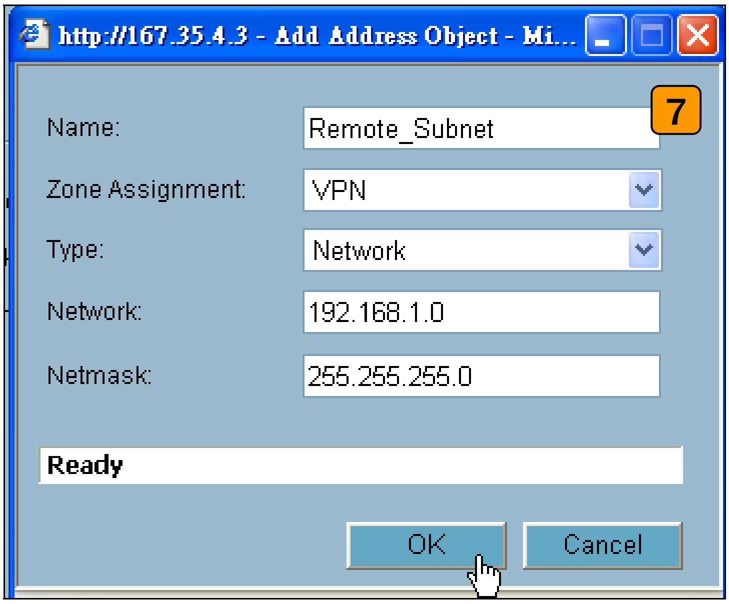
○ Use this VPN Tunnel as default route for all Internet traffic

○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Choose destination network from list: --Select Remote Network--

--Select Remote Network--
Create new address object...
Create new address group...
Ready
OK
Cancel
Help

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.



http://167.35.4.3 - Add Address Object - Mi...

Name: Remote_Subnet

Zone Assignment: VPN

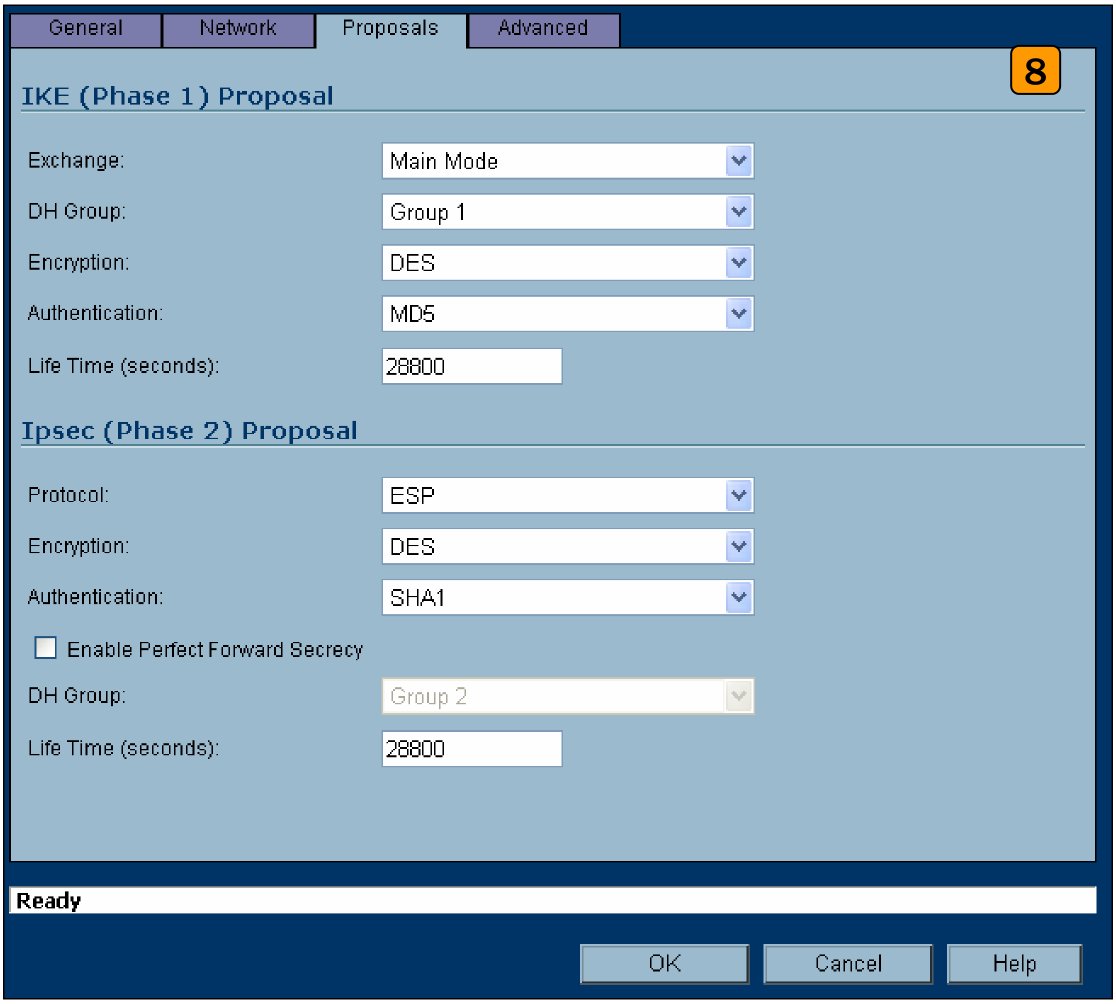
Type: Network

Network: 192.168.1.0

Netmask: 255.255.255.0

Ready

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.



IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 1

Encryption: DES

Authentication: MD5

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: DES

Authentication: SHA1

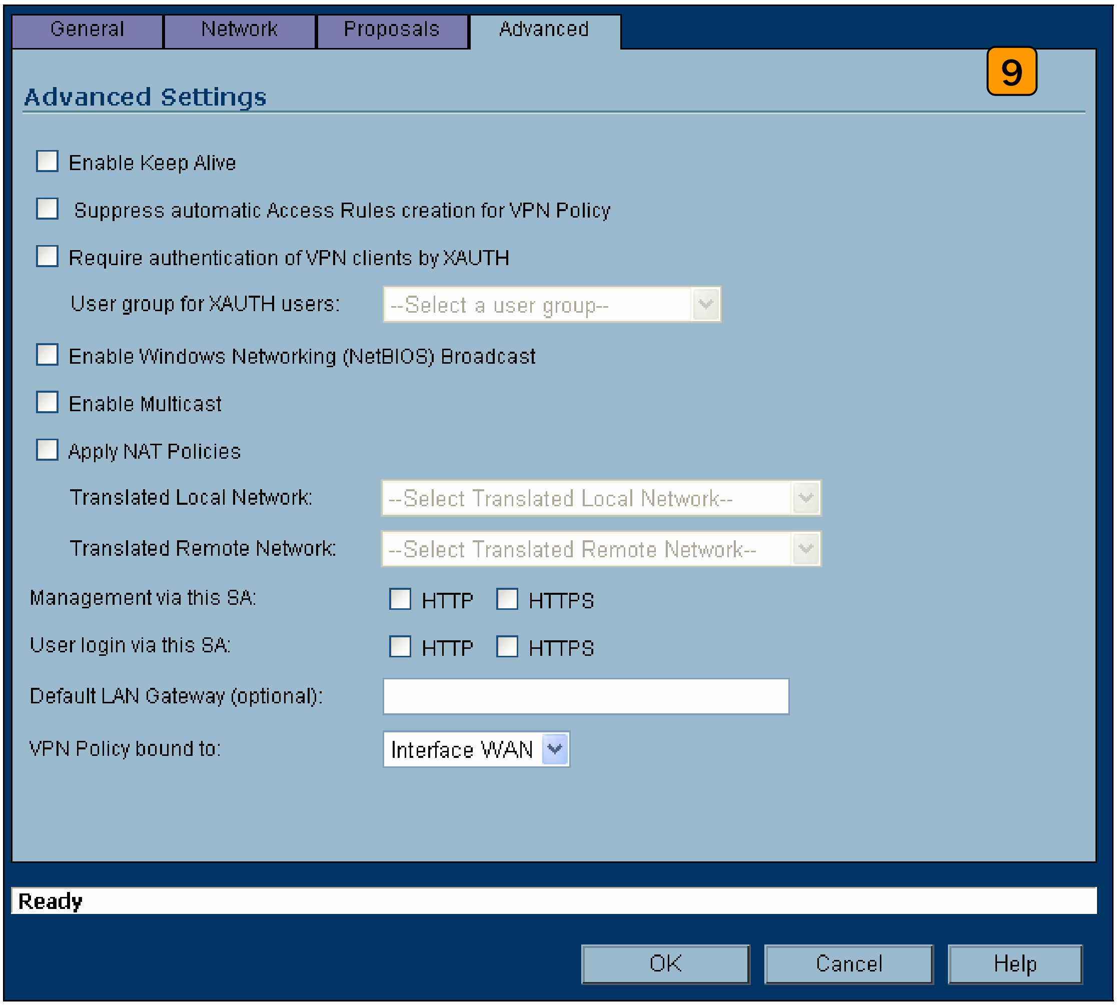
□ Enable Perfect Forward Secrecy

DH Group: Group 2

Life Time (seconds): 28800

Ready

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

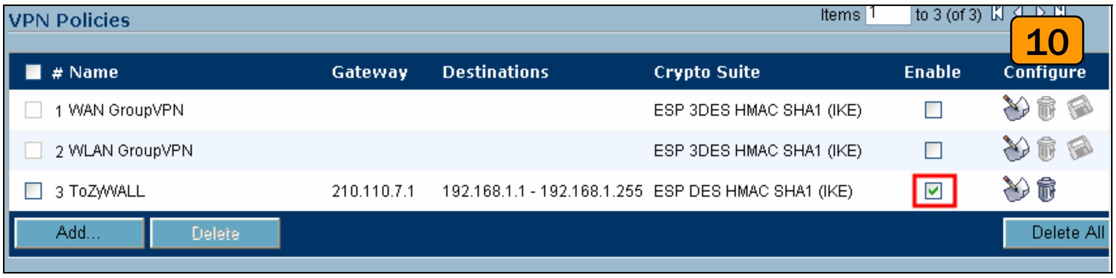
User login via this SA: ☐ HTTP ☐ HTTPS

Default LAN Gateway (optional):

VPN Policy bound to: Interface WAN

Ready

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

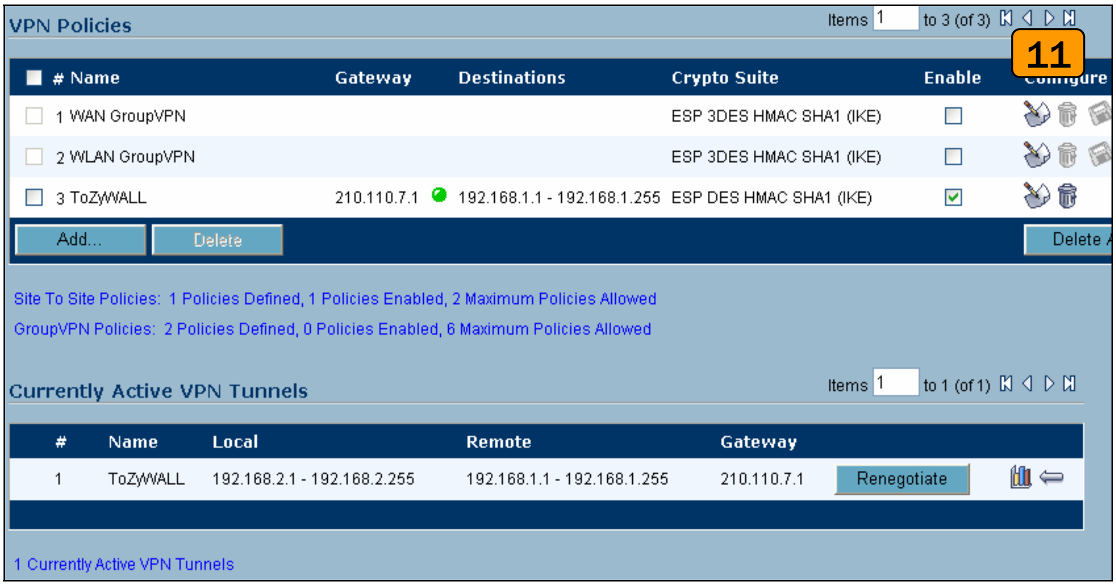


VPN Policies

Items 1 to 3 (of 3)

| ☐ | # Name | Gateway | Destinations | Crypto Suite | Enable | Configure |
|---|---|---|---|---|---|---|
| ☐ | 1 WAN GroupVPN | | | ESP 3DES HMAC SHA1 (IKE) | ☐ | |
| ☐ | 2 WLAN GroupVPN | | | ESP 3DES HMAC SHA1 (IKE) | ☐ | |
| ☐ | 3 ToZyWALL | 210.110.7.1 | 192.168.1.1 - 192.168.1.255 | ESP DES HMAC SHA1 (IKE) | ☑ | |

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

| ☐ # Name | Gateway | Destinations | Crypto Suite | Enable | Configure |
|---|---|---|---|---|---|
| ☐ 1 WAN GroupVPN | | | ESP 3DES HMAC SHA1 (IKE) | ☐ | |
| ☐ 2 WLAN GroupVPN | | | ESP 3DES HMAC SHA1 (IKE) | ☐ | |
| ☐ 3 ToZyWALL | 210.110.7.1 ● | 192.168.1.1 - 192.168.1.255 | ESP DES HMAC SHA1 (IKE) | ☑ | |

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

| # | 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

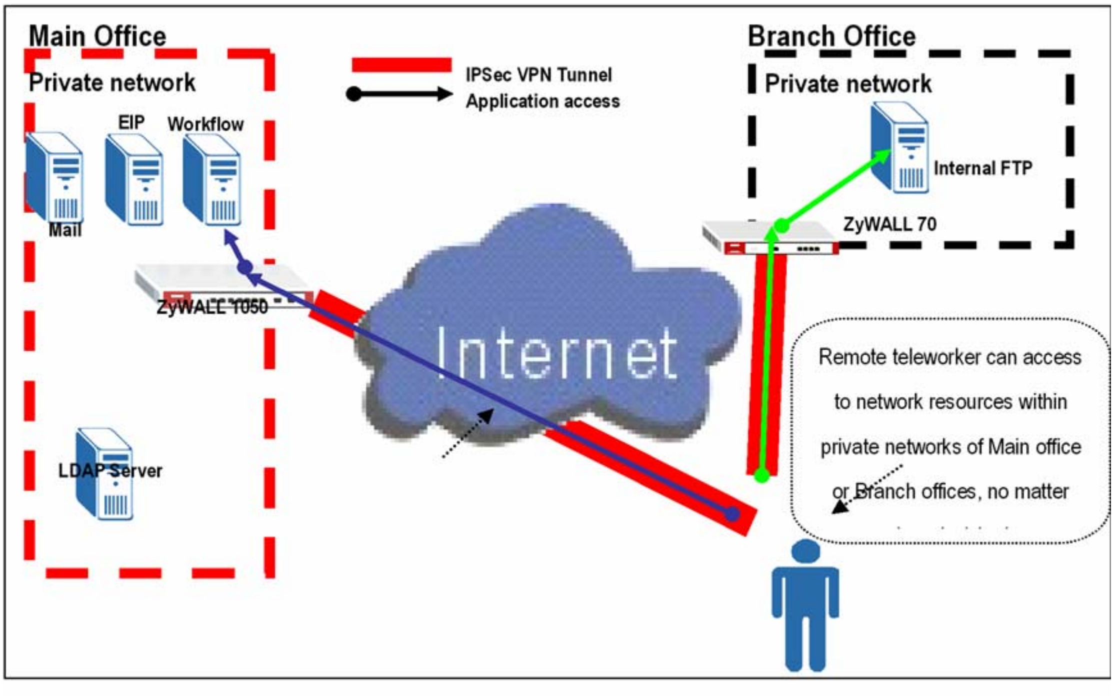
Remote Access VPN provides a cost-effective alternative to standard dial-in remote access to a company network. The users can connect to the network via the Internet, eliminating the expensive long-distance or the toll-free dial-in costs.

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.

## 1.3.1 Remote Access VPN

In this scenario, we assume the ZyWALL1050 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 ZyWALL1050’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.

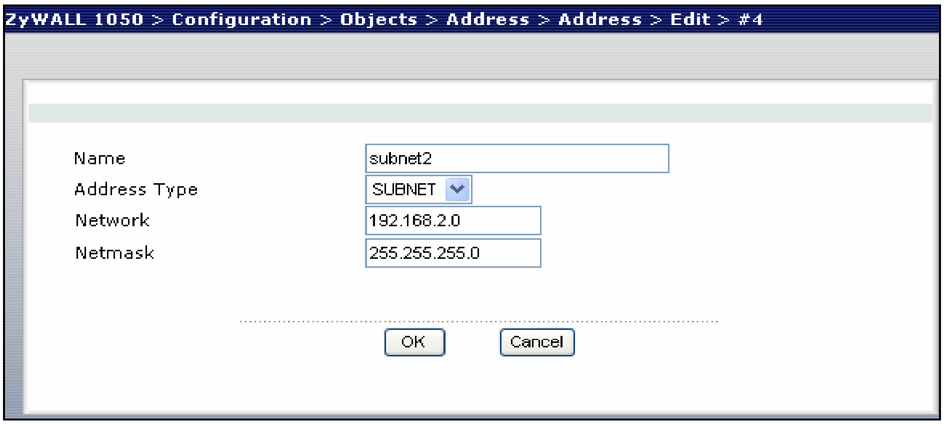
- In ZyWALL1050 create object ‘address’ for both local and remote networks
- In ZyWALL1050 configure a VPN gateway and the VPN connection setting
- In ZyWALL VPN client configure the corresponding VPN setting in ZyWALL VPN client

| **ZyWALL 1050** | **ZyWALL VPN Client** |
|---|---|
| My address: **ge2(10.59.1.45)**<br>Secure gateway address: **0.0.0.0**<br>Local: **192.168.2.0/24**<br>Remote: **0.0.0.0/24** | My address: **Any**<br>Secure gateway address: **10.59.1.45**<br>Local: **Any**<br>Remote: **192.168.2.0/24** |
| Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 | Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 |

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

Below is a step by step configuration:

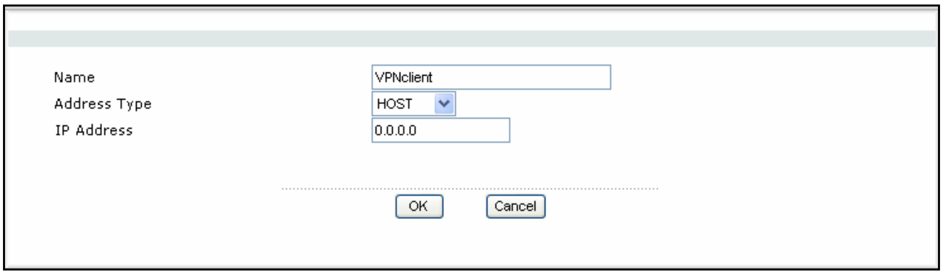
1) Login ZyWALL 1050 GUI and go to **Configuration** > **Objects** > **Address** to create an address object (local subnet) for remote access.



ZyWALL 1050 > Configuration > Objects > Address > Address > Edit > #4

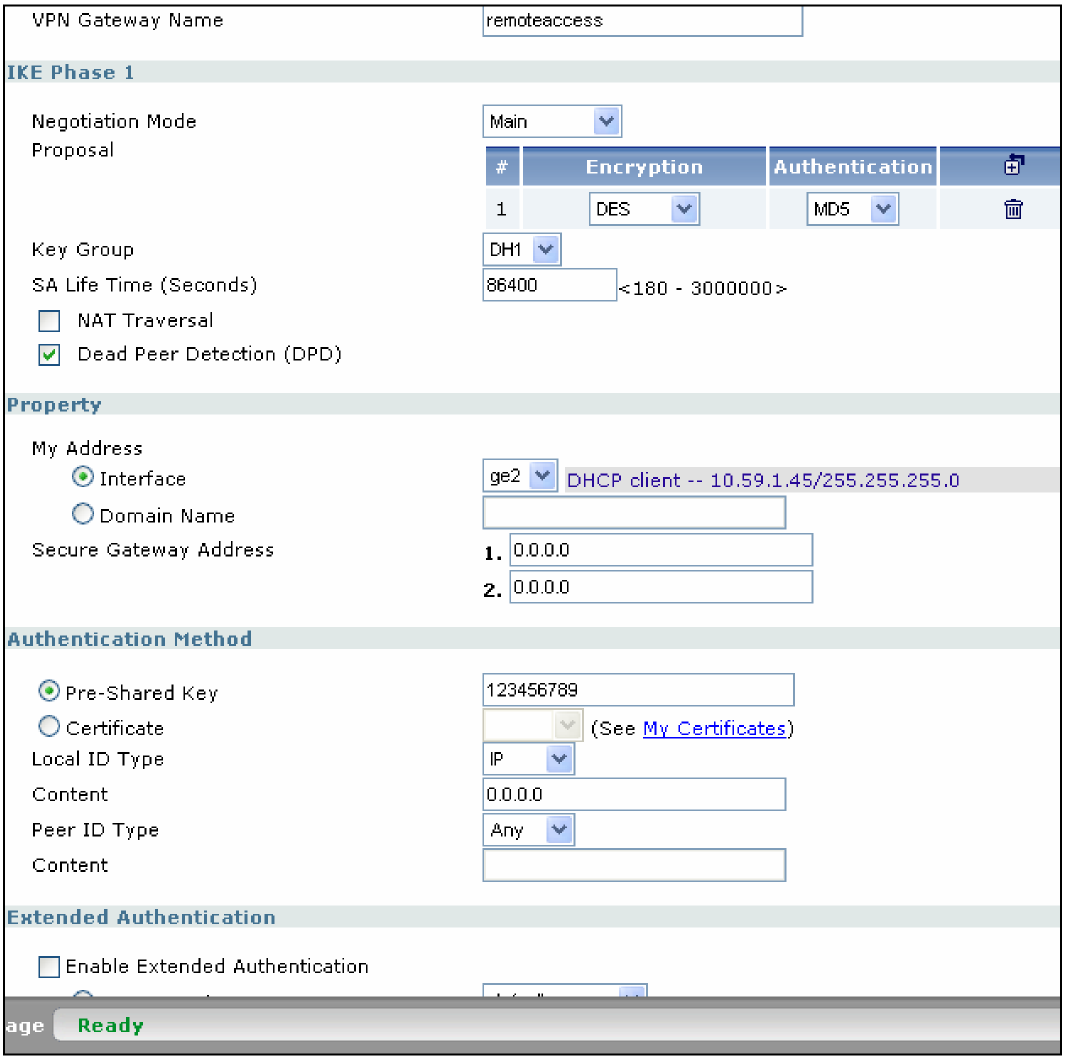
Name: subnet2
Address Type: SUBNET
Network: 192.168.2.0
Netmask: 255.255.255.0

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.



Name: VPNclient
Address Type: HOST
IP Address: 0.0.0.0

3) Go to **Configuration** > **Network** > **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.



VPN Gateway Name: remoteaccess

**IKE Phase 1**

Negotiation Mode: Main

Proposal

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | MD5 |

Key Group: DH1

SA Life Time (Seconds): 86400 <180 - 3000000>

□ NAT Traversal

☑ Dead Peer Detection (DPD)

**Property**

My Address

● Interface: ge2 DHCP client -- 10.59.1.45/255.255.255.0

○ Domain Name

Secure Gateway Address

1. 0.0.0.0
2. 0.0.0.0

**Authentication Method**

● Pre-Shared Key: 123456789

○ Certificate (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

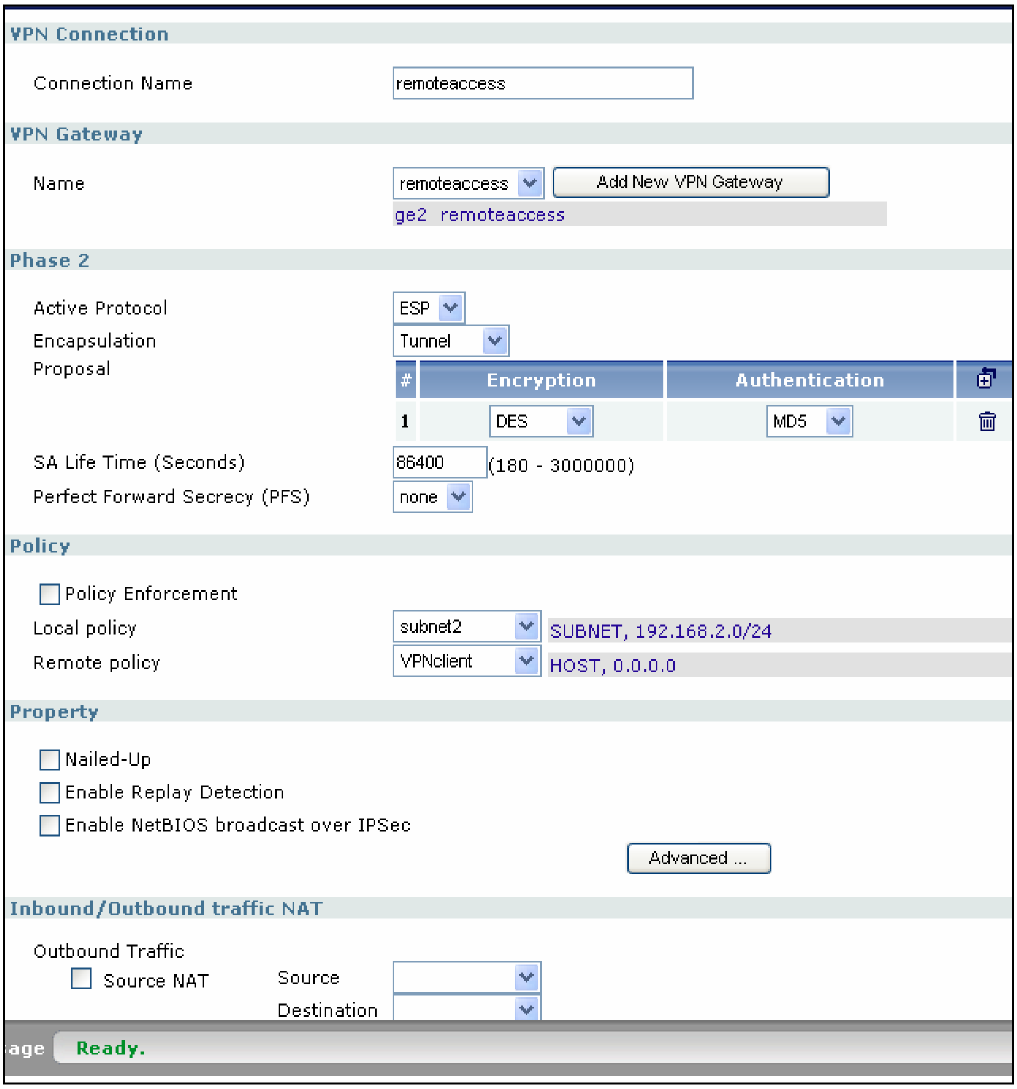
Peer ID Type: Any

Content:

**Extended Authentication**

□ Enable Extended Authentication

4) To create a VPN rule, go to **Configuration** > **Network** > **IPSec VPN** > **VPN Connection**. Set **Policy** 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.



**VPN Connection**

| | |
|---|---|
| Connection Name | remoteaccess |

**VPN Gateway**

| | |
|---|---|
| Name | remoteaccess ▾ [Add New VPN Gateway]<br>ge2 remoteaccess |

**Phase 2**

| | |
|---|---|
| Active Protocol | ESP ▾ |
| Encapsulation | Tunnel ▾ |
| Proposal | |

| # | Encryption | Authentication | |
|---|---|---|---|
| 1 | DES ▾ | MD5 ▾ | |

| | |
|---|---|
| SA Life Time (Seconds) | 86400 (180 - 3000000) |
| Perfect Forward Secrecy (PFS) | none ▾ |

**Policy**

☐ Policy Enforcement

| | | |
|---|---|---|
| Local policy | subnet2 ▾ | SUBNET, 192.168.2.0/24 |
| Remote policy | VPNclient ▾ | HOST, 0.0.0.0 |

**Property**

☐ Nailed-Up
☐ Enable Replay Detection
☐ Enable NetBIOS broadcast over IPSec

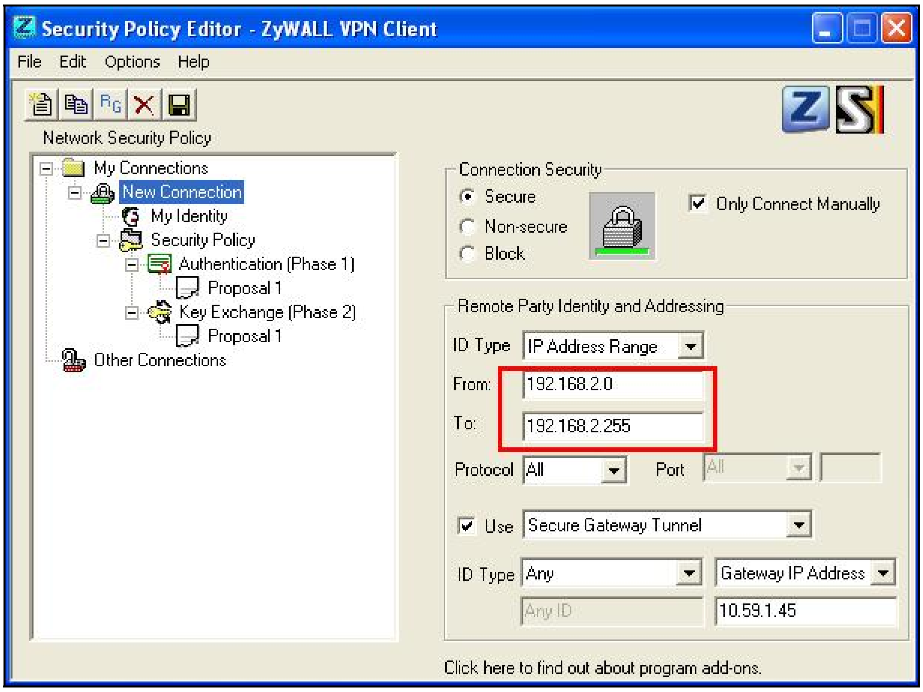
[Advanced ...]

**Inbound/Outbound traffic NAT**

Outbound Traffic
☐ Source NAT    Source ▾
Destination ▾

age Ready.

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



Connection Security: ● Secure ○ Non-secure ○ Block ☑ Only Connect Manually

Remote Party Identity and Addressing

ID Type: IP Address Range

From: 192.168.2.0

To: 192.168.2.255

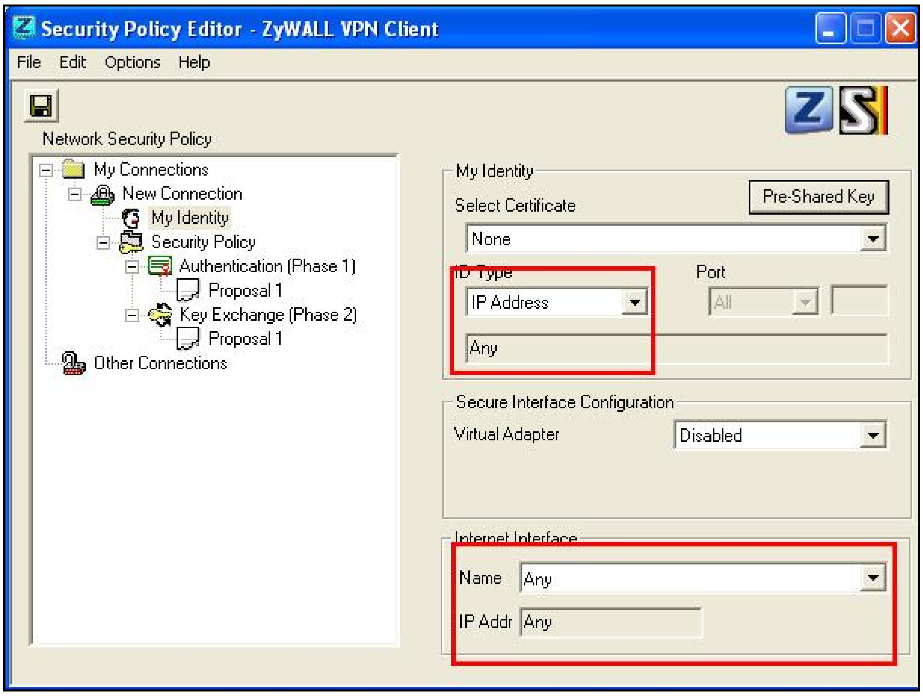
Protocol: All Port: All

☑ Use Secure Gateway Tunnel

ID Type: Any | Gateway IP Address

Any ID | 10.59.1.45

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



My Identity

Select Certificate: None

ID Type: IP Address Port: All

Any

Secure Interface Configuration

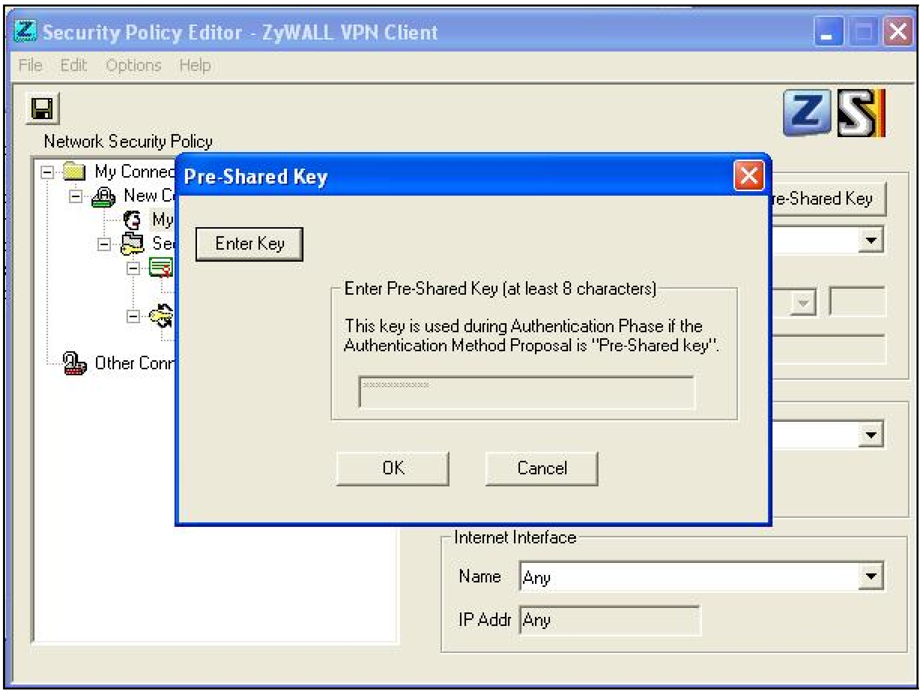
Virtual Adapter: Disabled

Internet Interface

Name: Any

IP Addr: Any

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



Enter Pre-Shared Key (at least 8 characters)

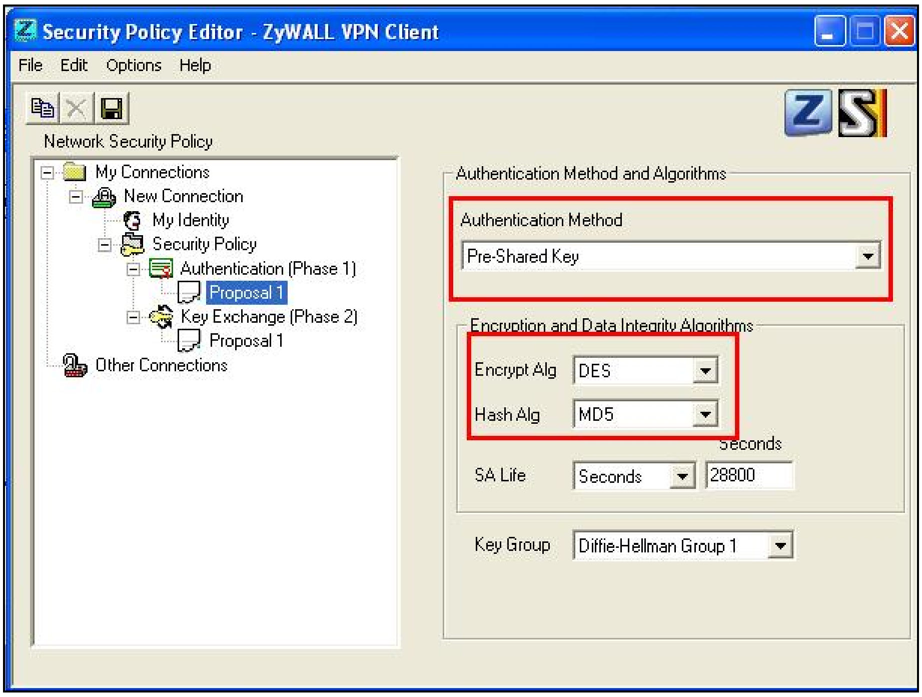
This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".

Internet Interface

Name: Any

IP Addr: Any

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.



Authentication Method and Algorithms

Authentication Method: Pre-Shared Key

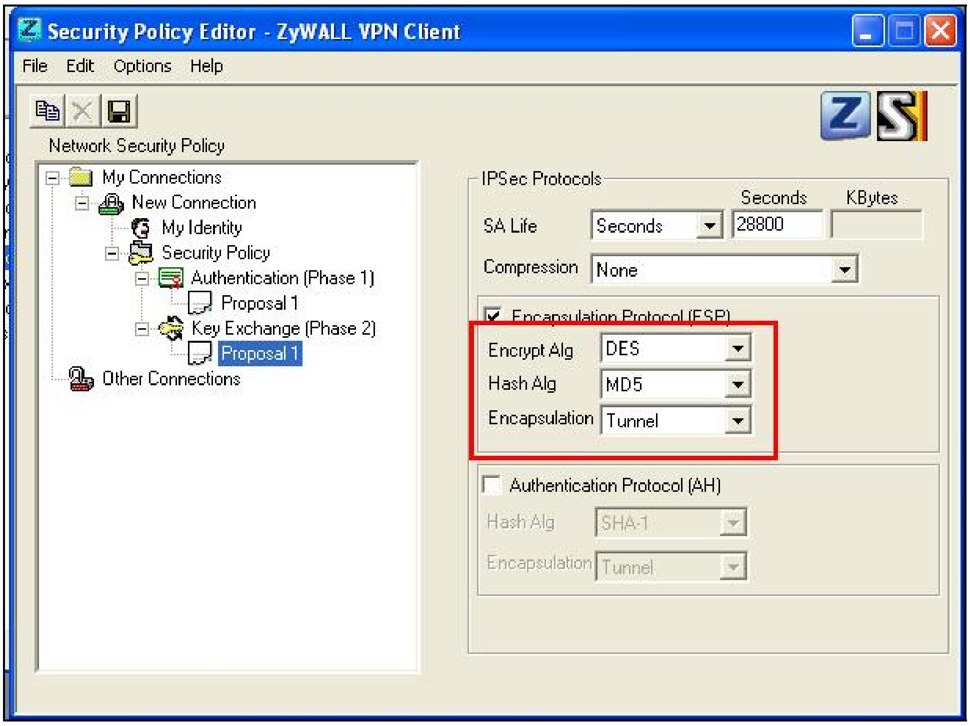
Encryption and Data Integrity Algorithms

Encrypt Alg: DES

Hash Alg: MD5

SA Life: Seconds 28800

Key Group: Diffie-Hellman Group 1



SA Life: Seconds — Seconds 28800, KBytes

Compression: None

☑ Encapsulation Protocol (ESP)

Encrypt Alg: DES

Hash Alg: MD5

Encapsulation: Tunnel

□ Authentication Protocol (AH)

Hash Alg: SHA-1

Encapsulation: Tunnel

The CLI commands for application:

Address Object for local subnet:

```
[0] address-object subnet2 192.168.2.0 255.255.255.0
```

Address Object for remote host:

```
[0] address-object VPNclient 0.0.0.0
```

Remote Gateway:

```
[0] isakmp policy remoteaccess
[1] mode main
[2] transform-set des-md5
[3] lifetime 86400
[4] no natt
[5] dpd
[6] local-ip interface ge2
[7] peer-ip 0.0.0.0 0.0.0.0
[8] authentication pre-share
[9] keystring 123456789
[10] local-id type ip 0.0.0.0
[11] peer-id type any
[12] xauth type server default deactivate
[13] group1
```

VPN Connection:

```
[0] crypto map remoteaccess
[1] ipsec-isakmp remoteaccess
[2] encapsulation tunnel
[3] transform-set esp-des-md5
[4] set security-association lifetime seconds 86400
[5] set pfs none
[6] no policy-enforcement
[7] local-policy subnet2
[8] remote-policy VPNclient
[9] no nail-up
[10] no replay-detection
[11] no netbios-broadcast
[12] no out-snat activate
[13] no in-snat activate
[14] no in-dnat activate
```

**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 the opposite and not of the same content.

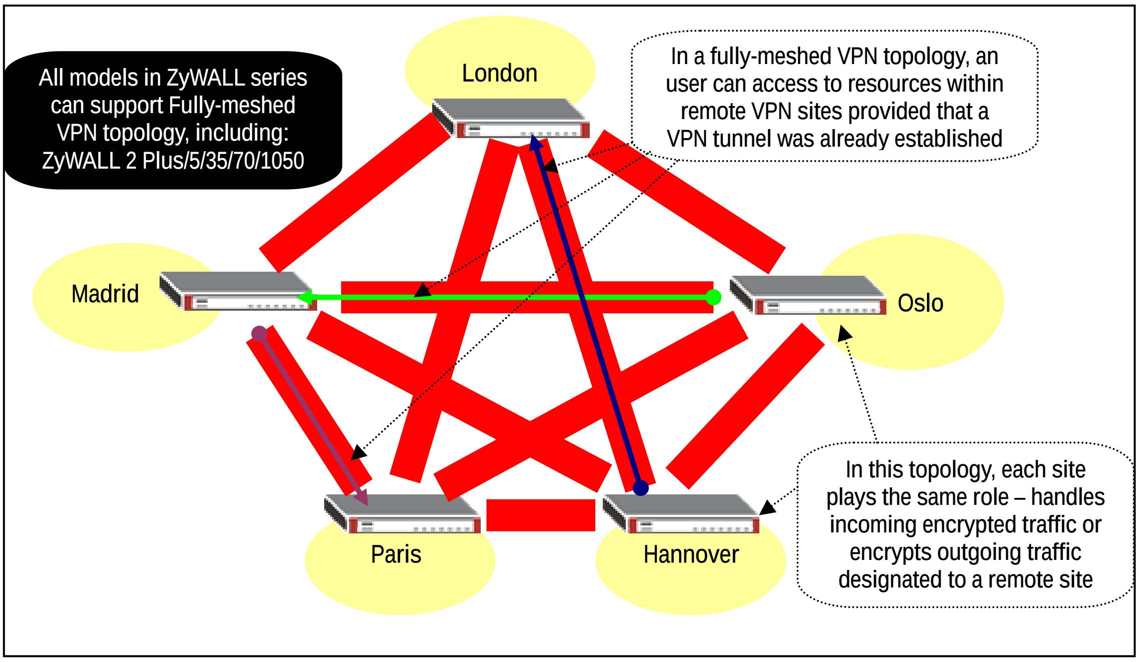
5. The **Local Policy** of ZyWALL 1050 should be ‘dynamic single host with the value 0.0.0.0’. The VPN tunnel should be initialed from the remote host site.

## 1.4 Large-scale VPN Deployment

With the business growing, network administrator will face the more and more complicated VPN topology and applications. ZyWALL 1050 supports various types of VPN topology that can meet the needs of the organizations of any size.

ZyWALL1050 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



All models in ZyWALL series can support Fully-meshed VPN topology, including: ZyWALL 2 Plus/5/35/70/1050

In a fully-meshed VPN topology, an user can access to resources within remote VPN sites provided that a VPN tunnel was already established

In this topology, each site plays the same role – handles incoming encrypted traffic or encrypts outgoing traffic designated to a remote site

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 ←VPN →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**

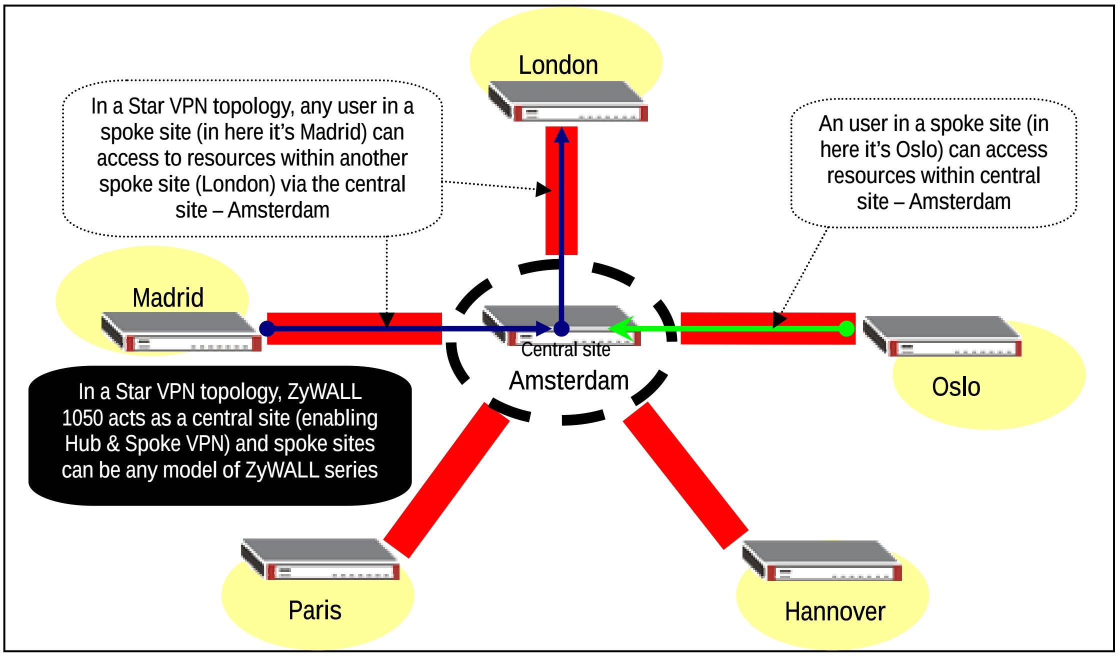
**Tunnel 8: Paris ←VPN → Hannover**

**Tunnel 9: Paris ←VPN → Oslo**

**Tunnel 10: Hannover ←VPN → Oslo**

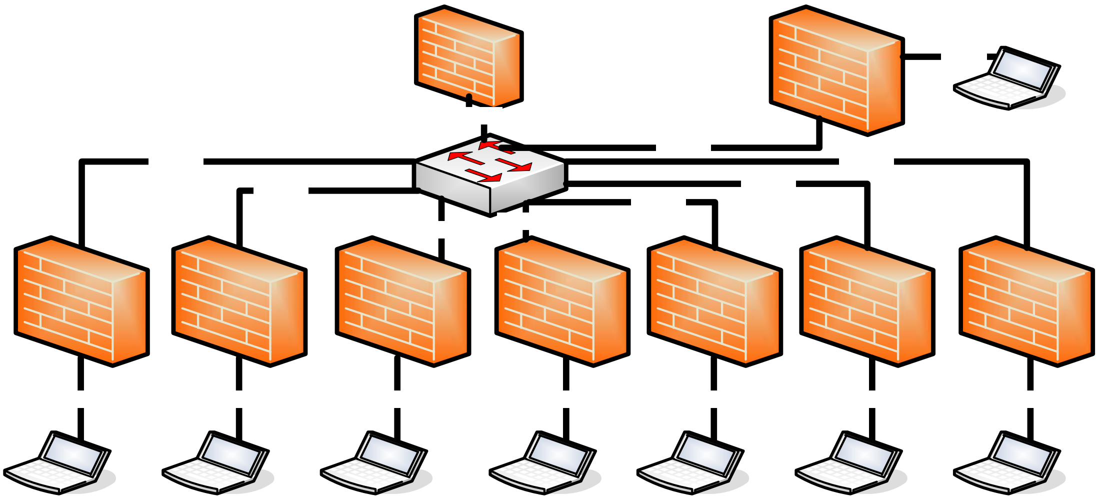
3) For help on building up the 10 tunnels, please refer to the section ZyWALL1050 to ZyWALL1050 VPN tunnel configuration steps . We will introduce the configuration steps for a VPN concentrator that will greatly help to reduce the total number of tunnels.

### 1.4.2 Star Topology


London
In a Star VPN topology, any user in a spoke site (in here it's Madrid) can access to resources within another spoke site (London) via the central site – Amsterdam
An user in a spoke site (in here it's Oslo) can access resources within central site – Amsterdam
Madrid
Central site
Amsterdam
Oslo
In a Star VPN topology, ZyWALL 1050 acts as a central site (enabling Hub & Spoke VPN) and spoke sites can be any model of ZyWALL series
Paris
Hannover

The ZyWALL1050 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.

ZyWA

**The VPN configuration parameter**

| Remote Office | HQ |
|---|---|
| WAN: 10.59.1.11<br>~<br>WAN: 10.59.1.17<br>LAN: 192.168.101.0/24 | WAN: 10.59.1.10<br>LAN: 192.168.100.0/24 |

WAN

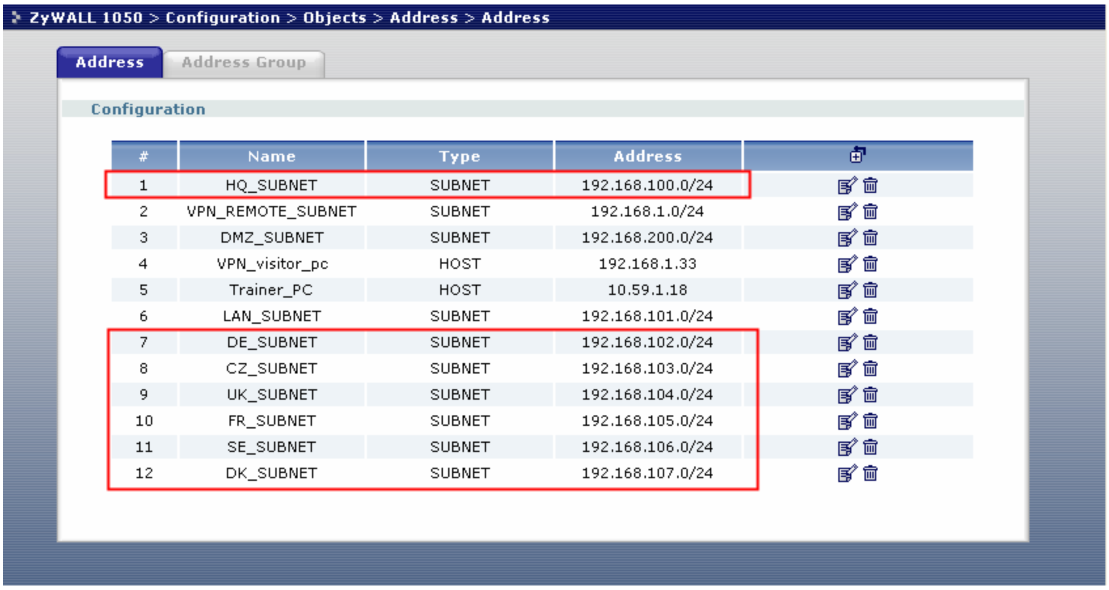
WAN

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

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

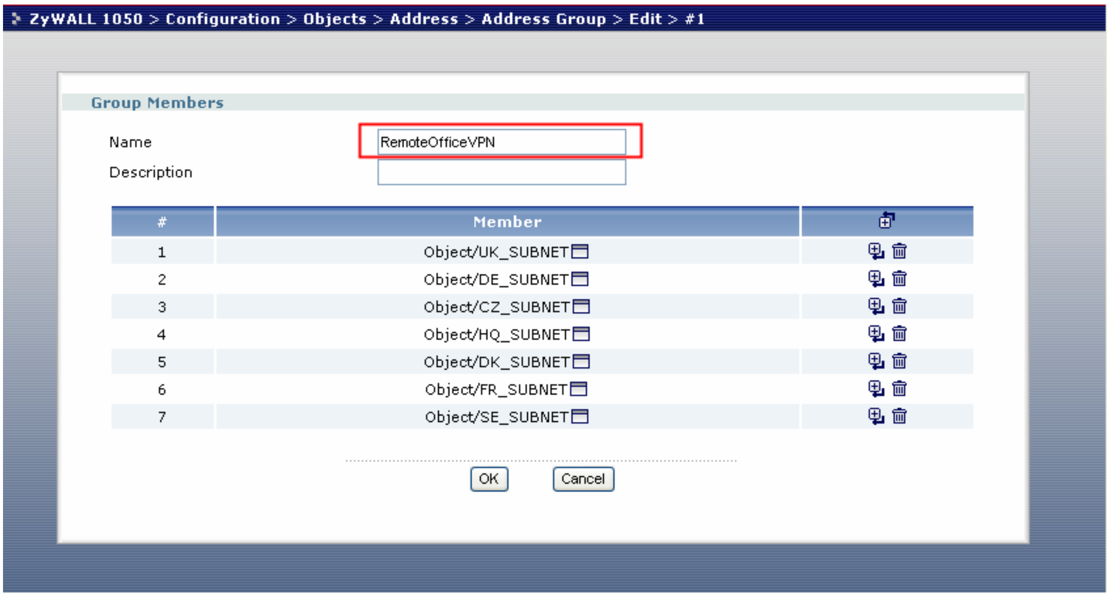
We used the Netherland site (NL) as an example to show how to setup tunnel between **NL** and **HQ. P**lease refer the above VPN parameter table to setup the VPN gateway and connection as I don't list the detail configuration steps here,.

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



| # | 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.



ZyWALL 1050 > Configuration > Objects > Address > Address Group > Edit > #1

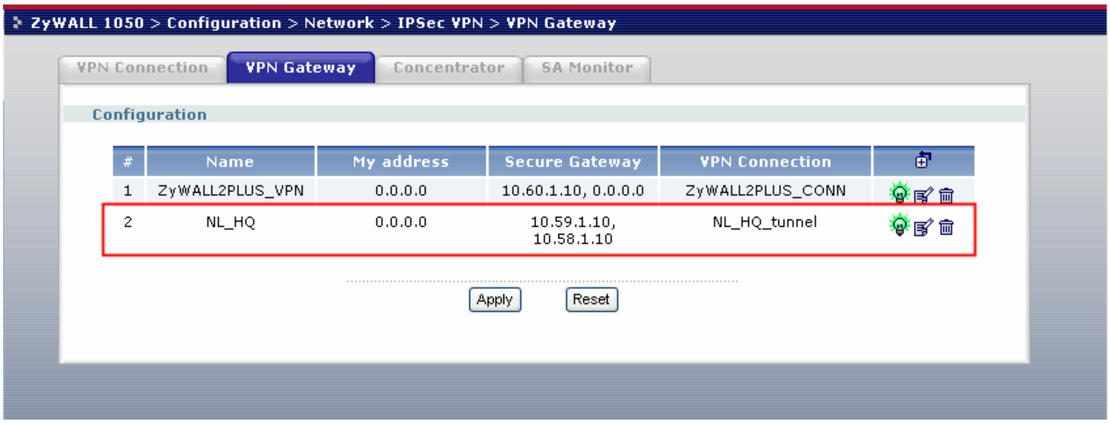
Group Members

Name: RemoteOfficeVPN

Description:

| # | Member |
|---|---|
| 1 | Object/UK_SUBNET |
| 2 | Object/DE_SUBNET |
| 3 | Object/CZ_SUBNET |
| 4 | Object/HQ_SUBNET |
| 5 | Object/DK_SUBNET |
| 6 | Object/FR_SUBNET |
| 7 | Object/SE_SUBNET |

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

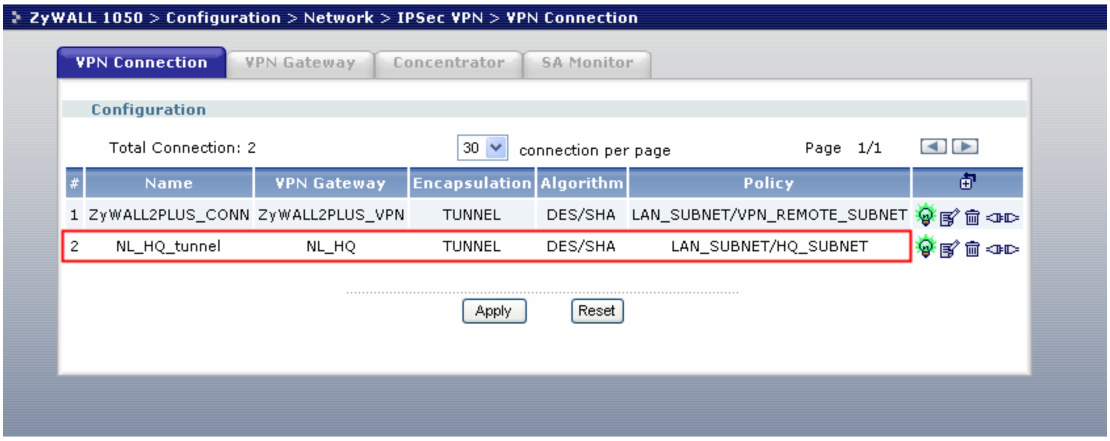


ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway

Configuration

| # | Name | My address | Secure Gateway | VPN Connection |
|---|---|---|---|---|
| 1 | ZyWALL2PLUS_VPN | 0.0.0.0 | 10.60.1.10, 0.0.0.0 | ZyWALL2PLUS_CONN |
| 2 | NL_HQ | 0.0.0.0 | 10.59.1.10,<br>10.58.1.10 | NL_HQ_tunnel |

**NL** site VPN Connection status page



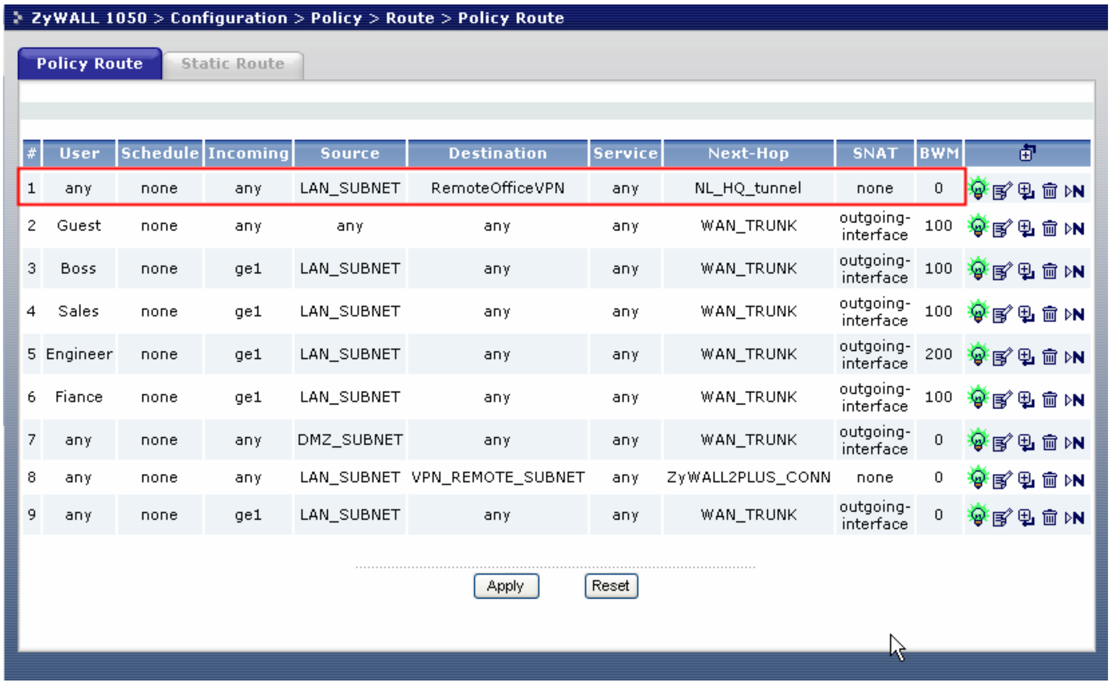
ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Connection

Configuration

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

| # | Name | VPN Gateway | Encapsulation | Algorithm | Policy |
|---|---|---|---|---|---|
| 1 | ZyWALL2PLUS_CONN | ZyWALL2PLUS_VPN | TUNNEL | DES/SHA | LAN_SUBNET/VPN_REMOTE_SUBNET |
| 2 | NL_HQ_tunnel | NL_HQ | TUNNEL | DES/SHA | LAN_SUBNET/HQ_SUBNET |

**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.



ZyWALL 1050 > Configuration > Policy > Route > Policy Route

| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM |
|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | any | LAN_SUBNET | RemoteOfficeVPN | any | NL_HQ_tunnel | none | 0 |
| 2 | Guest | none | any | any | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 3 | Boss | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 4 | Sales | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 5 | Engineer | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 200 |
| 6 | Fiance | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 7 | any | none | any | DMZ_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 0 |
| 8 | any | none | any | LAN_SUBNET | VPN_REMOTE_SUBNET | any | ZyWALL2PLUS_CONN | none | 0 |
| 9 | any | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 0 |

**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.

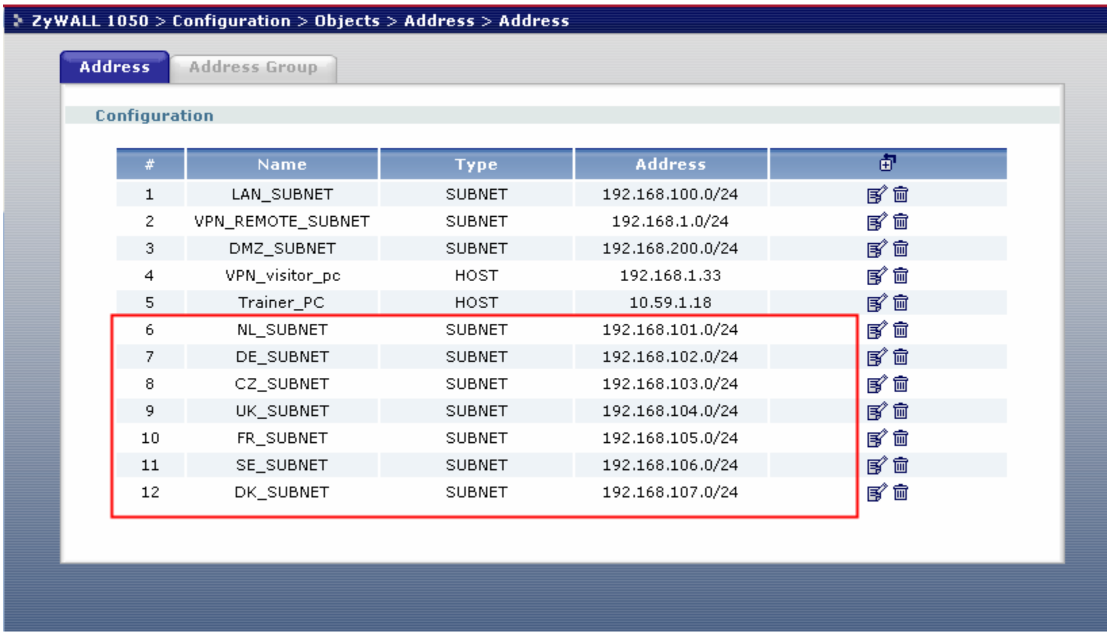
This means that if we want HQ to route 5 remote sites VPN traffic, we need to configure 5 VPN tunnels from remote office to HQ.

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

| **Remote Office** | **HQ** |
|---|---|
| WAN: 10.59.1.11<br>~<br>WAN: 10.59.1.17<br>LAN: 192.168.101.0/24<br>~<br>LAN: 192.168.119.0/24 | WAN: 10.59.1.10<br>LAN: 192.168.100.0/24 |
| Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789 | Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789 |

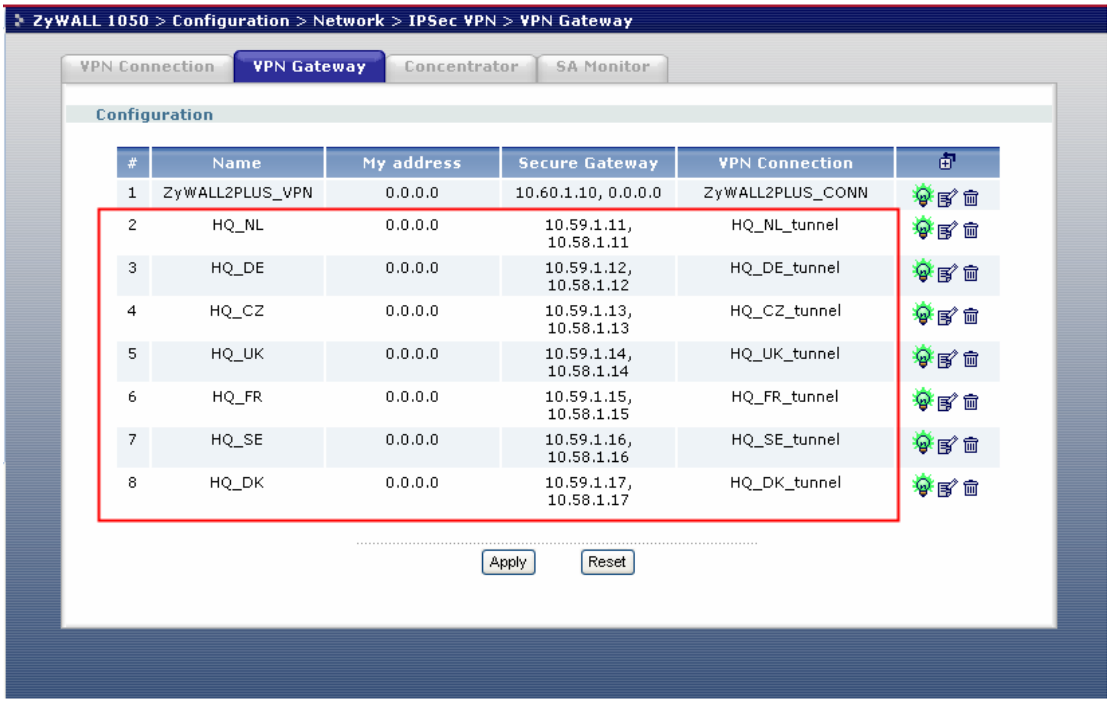
| | |
|---|---|
| Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 | Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 |
| Phase2<br>Encapsulation: Tunnel<br>Active Protocol: ESP<br>Encryption: DES<br>Authentication: SHA1<br>Perfect Forward Secrecy (PFS): None | Phase2<br>Encapsulation: Tunnel<br>Active Protocol: ESP<br>Encryption: DES<br>Authentication: SHA1<br>Perfect Forward Secrecy (PFS): None |

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



| # | Name | Type | Address |
|---|---|---|---|
| 1 | LAN_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 | NL_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 |

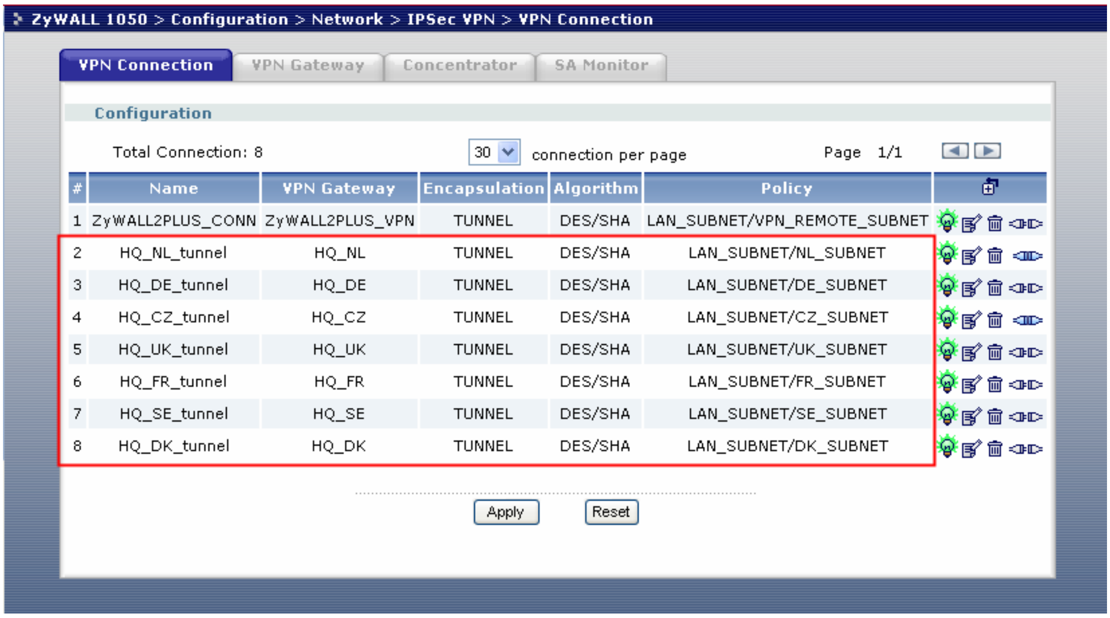
Setup the HQ VPN Gateway for all the remote sites



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway

| # | Name | My address | Secure Gateway | VPN Connection |
|---|---|---|---|---|
| 1 | ZyWALL2PLUS_VPN | 0.0.0.0 | 10.60.1.10, 0.0.0.0 | ZyWALL2PLUS_CONN |
| 2 | HQ_NL | 0.0.0.0 | 10.59.1.11,<br>10.58.1.11 | HQ_NL_tunnel |
| 3 | HQ_DE | 0.0.0.0 | 10.59.1.12,<br>10.58.1.12 | HQ_DE_tunnel |
| 4 | HQ_CZ | 0.0.0.0 | 10.59.1.13,<br>10.58.1.13 | HQ_CZ_tunnel |
| 5 | HQ_UK | 0.0.0.0 | 10.59.1.14,<br>10.58.1.14 | HQ_UK_tunnel |
| 6 | HQ_FR | 0.0.0.0 | 10.59.1.15,<br>10.58.1.15 | HQ_FR_tunnel |
| 7 | HQ_SE | 0.0.0.0 | 10.59.1.16,<br>10.58.1.16 | HQ_SE_tunnel |
| 8 | HQ_DK | 0.0.0.0 | 10.59.1.17,<br>10.58.1.17 | HQ_DK_tunnel |

Setup the HQ VPN connection for all the remote sites



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Connection

Total Connection: 8 — 30 connection per page — Page 1/1

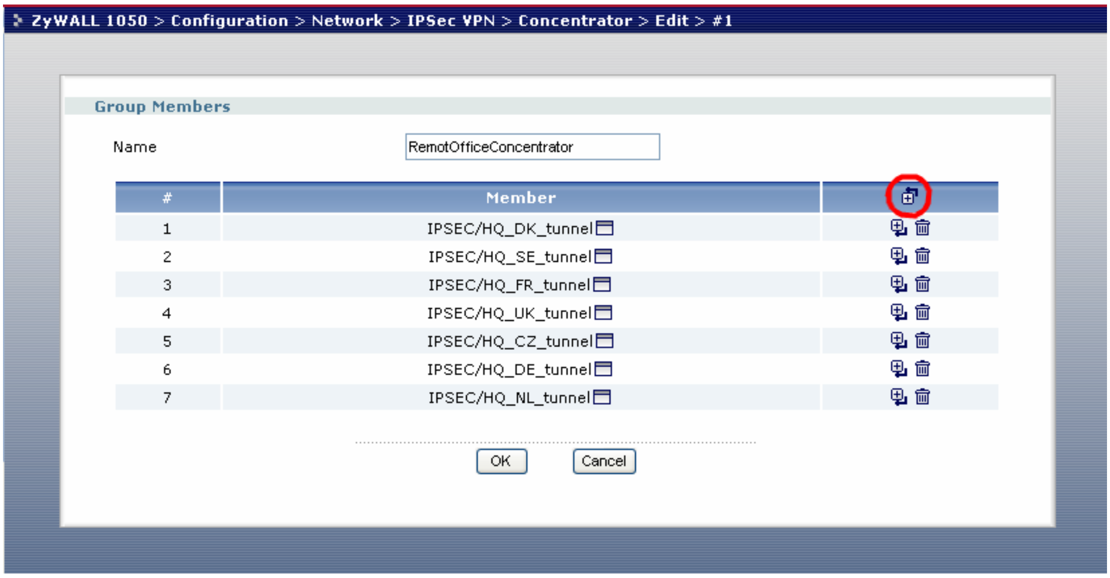
| # | Name | VPN Gateway | Encapsulation | Algorithm | Policy |
|---|---|---|---|---|---|
| 1 | ZyWALL2PLUS_CONN | ZyWALL2PLUS_VPN | TUNNEL | DES/SHA | LAN_SUBNET/VPN_REMOTE_SUBNET |
| 2 | HQ_NL_tunnel | HQ_NL | TUNNEL | DES/SHA | LAN_SUBNET/NL_SUBNET |
| 3 | HQ_DE_tunnel | HQ_DE | TUNNEL | DES/SHA | LAN_SUBNET/DE_SUBNET |
| 4 | HQ_CZ_tunnel | HQ_CZ | TUNNEL | DES/SHA | LAN_SUBNET/CZ_SUBNET |
| 5 | HQ_UK_tunnel | HQ_UK | TUNNEL | DES/SHA | LAN_SUBNET/UK_SUBNET |
| 6 | HQ_FR_tunnel | HQ_FR | TUNNEL | DES/SHA | LAN_SUBNET/FR_SUBNET |
| 7 | HQ_SE_tunnel | HQ_SE | TUNNEL | DES/SHA | LAN_SUBNET/SE_SUBNET |
| 8 | HQ_DK_tunnel | HQ_DK | TUNNEL | DES/SHA | LAN_SUBNET/DK_SUBNET |

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 1050 > 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.



ZyWALL 1050 > Configuration > Network > IPSec VPN > Concentrator > Edit > #1

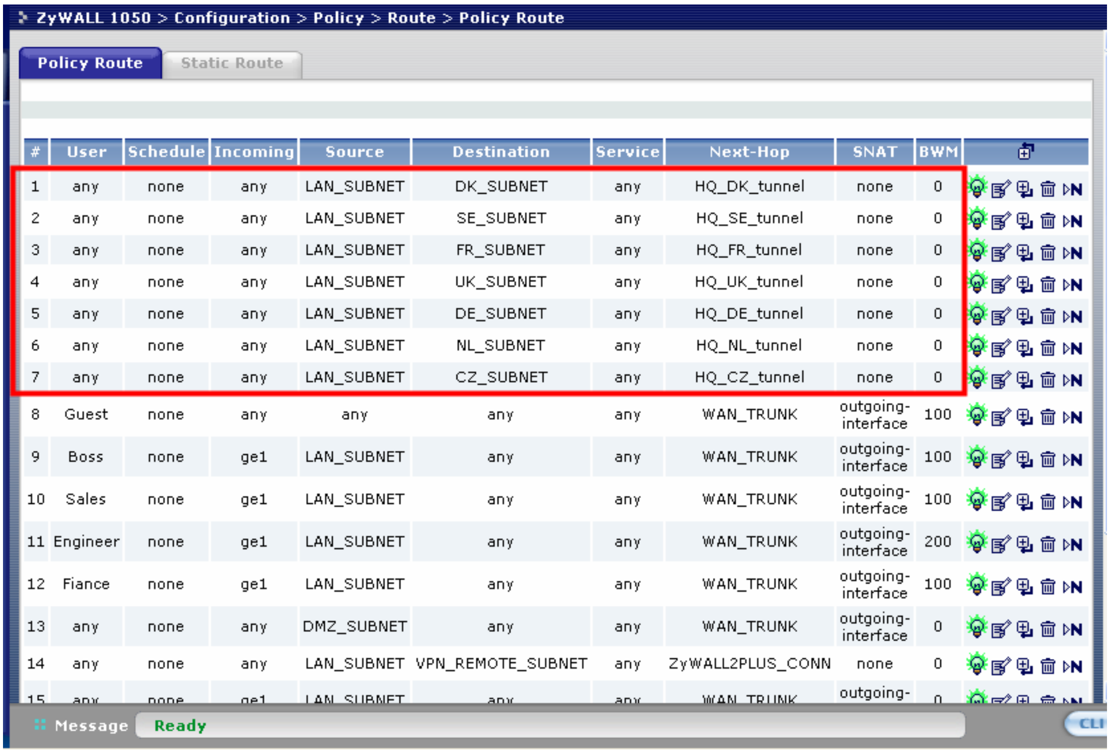
Group Members

Name: RemotOfficeConcentrator

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

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.

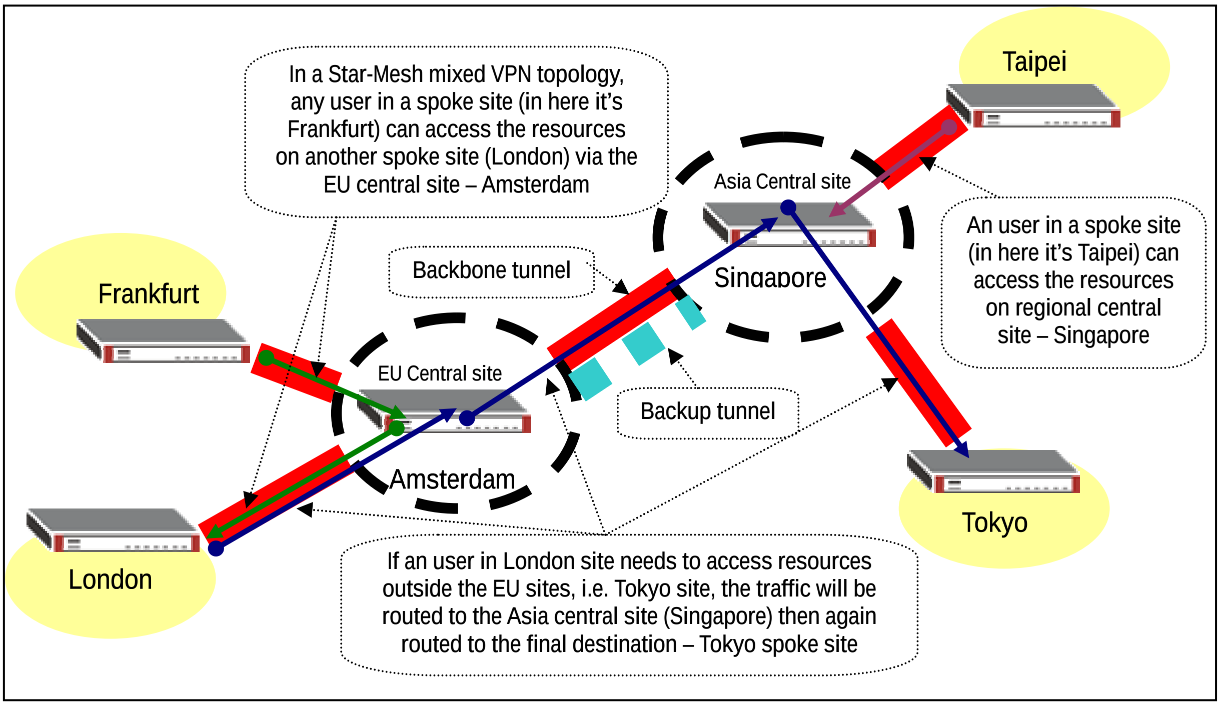
The VPN concentrator is designed to route the remote sites' VPN traffic. However, user still needs to setup the policy route for local subnet VPN traffic. For example, if we setup the VPN concentrator only for HQ and remote sites A & B, then the A subnet can connect to B subnet but HQ subnet can't connect 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.



ZyWALL 1050 > Configuration > Policy > Route > Policy Route

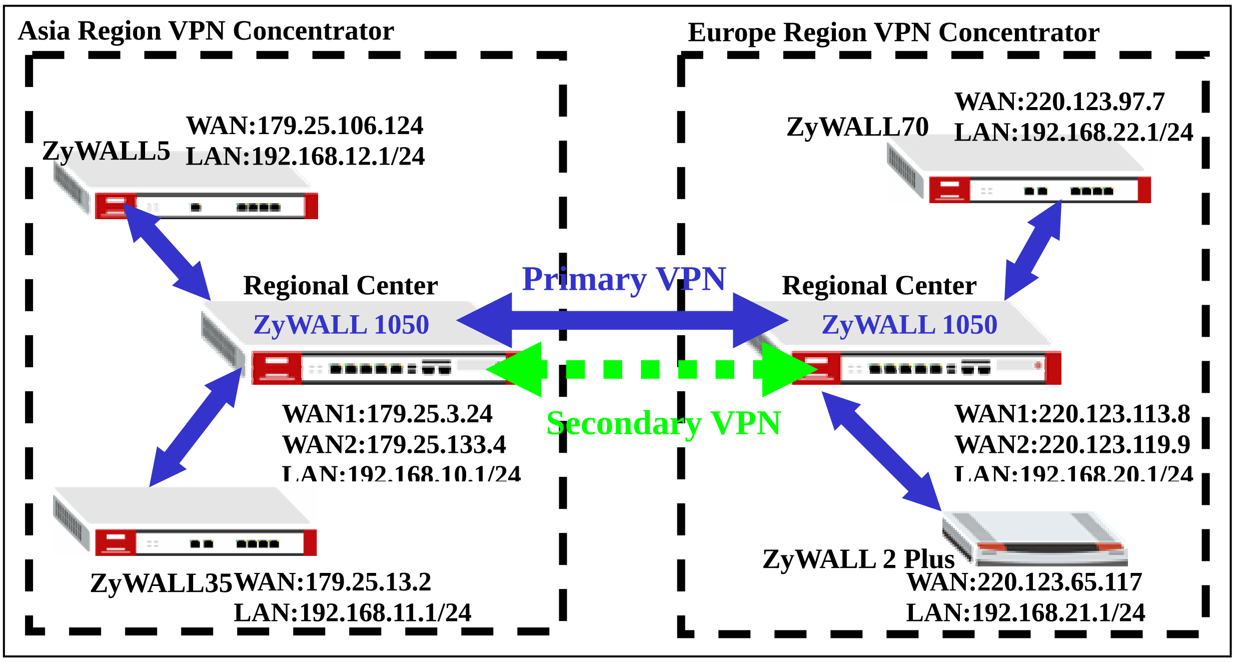
| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM |
|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | any | LAN_SUBNET | DK_SUBNET | any | HQ_DK_tunnel | none | 0 |
| 2 | any | none | any | LAN_SUBNET | SE_SUBNET | any | HQ_SE_tunnel | none | 0 |
| 3 | any | none | any | LAN_SUBNET | FR_SUBNET | any | HQ_FR_tunnel | none | 0 |
| 4 | any | none | any | LAN_SUBNET | UK_SUBNET | any | HQ_UK_tunnel | none | 0 |
| 5 | any | none | any | LAN_SUBNET | DE_SUBNET | any | HQ_DE_tunnel | none | 0 |
| 6 | any | none | any | LAN_SUBNET | NL_SUBNET | any | HQ_NL_tunnel | none | 0 |
| 7 | any | none | any | LAN_SUBNET | CZ_SUBNET | any | HQ_CZ_tunnel | none | 0 |
| 8 | Guest | none | any | any | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 9 | Boss | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 10 | Sales | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 11 | Engineer | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 200 |
| 12 | Fiance | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 13 | any | none | any | DMZ_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 0 |
| 14 | any | none | any | LAN_SUBNET | VPN_REMOTE_SUBNET | any | ZyWALL2PLUS_CONN | none | 0 |
| 15 | any | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing- | 0 |

### 1.4.3 Star-Mesh Mixed Topology


Taipei
In a Star-Mesh mixed VPN topology, any user in a spoke site (in here it's Frankfurt) can access the resources on another spoke site (London) via the EU central site – Amsterdam
Asia Central site
Singapore
Frankfurt
Backbone tunnel
An user in a spoke site (in here it's Taipei) can access the resources on regional central site – Singapore
EU Central site
Amsterdam
Backup tunnel
Tokyo
London
If an user in London site needs to access resources outside the EU sites, i.e. Tokyo site, the traffic will be routed to the Asia central site (Singapore) then again routed to the final destination – Tokyo spoke site

In a Star-mesh mixed VPN topology, ZyWALL 1050 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.

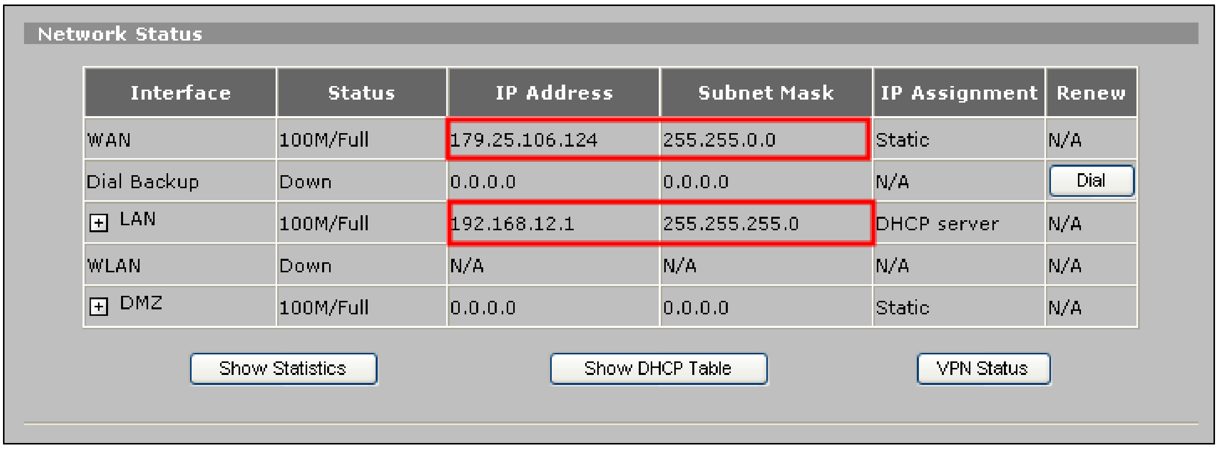
We use the below presented network topology to explain how to configure Star-Mesh Mixed Topology between all the ZyWALL series devices. The ZyWALL 1050s act as a Regional Center devices whereas ZyWALL 2 Plus, 5, 35 and 70 are the regional remote sites' devices which are building VPN tunnel back to the 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 | Dial |
| ⊞ 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 |
| ⊞ DMZ | 100M/Full | 0.0.0.0 | 0.0.0.0 | Static | N/A |

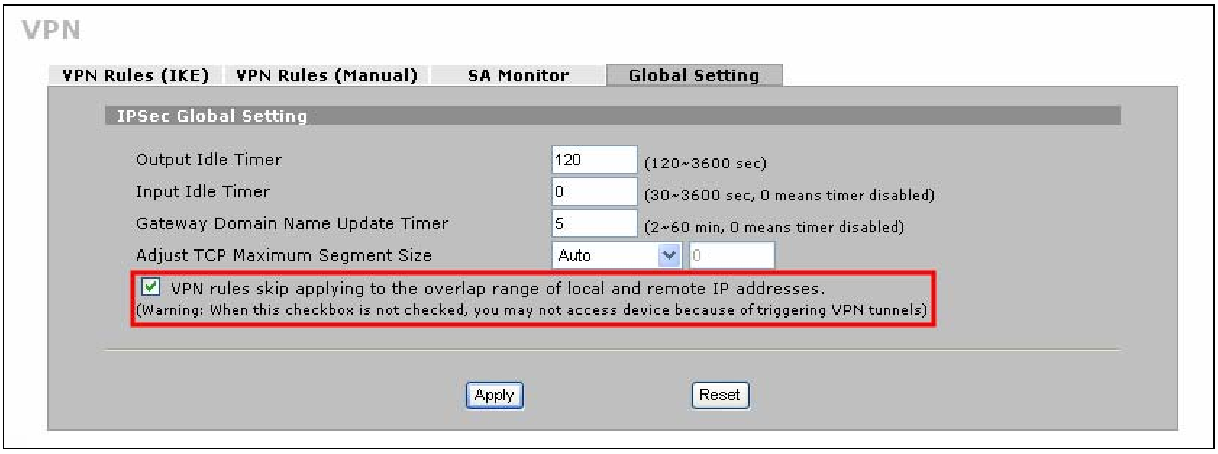
## The VPN configuration parameters in Asia Region

| Regional Remote Sites | Regional Center |
|---|---|
| ZyWALL5 WAN: 179.25.106.124<br>Local Policy: 192.168.12.0/24 | WAN: 179.25.3.24<br>Local Policy: 192.168.0.0/16 |

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

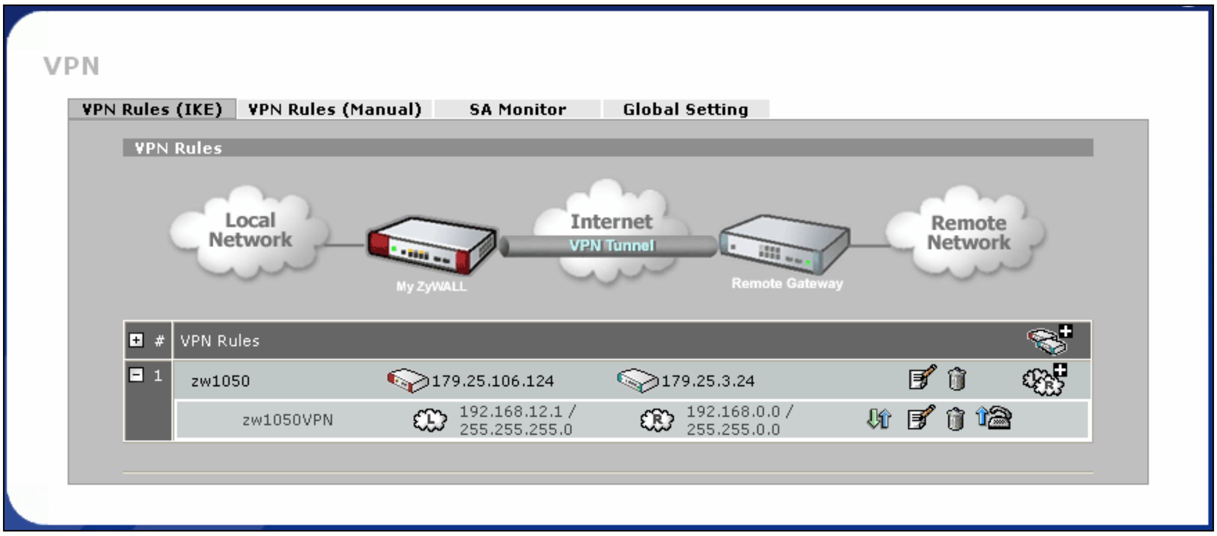
The next step is to configure the VPN tunnel setting. Following the ZyWALL5 VPN design logic, we have to define the local and remote policies to force the traffic going through the VPN tunnel to the remote site. For example, the traffic from ZyWALL5 will be sent to all the remote sites' devices like ZyWALL35 (LAN subnet: 192.168.11.x), local center's ZyWALL 1050 (LAN subnet: 192.168.21.x), remote center's ZyWALL 1050 (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 1050. 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 1050. 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.



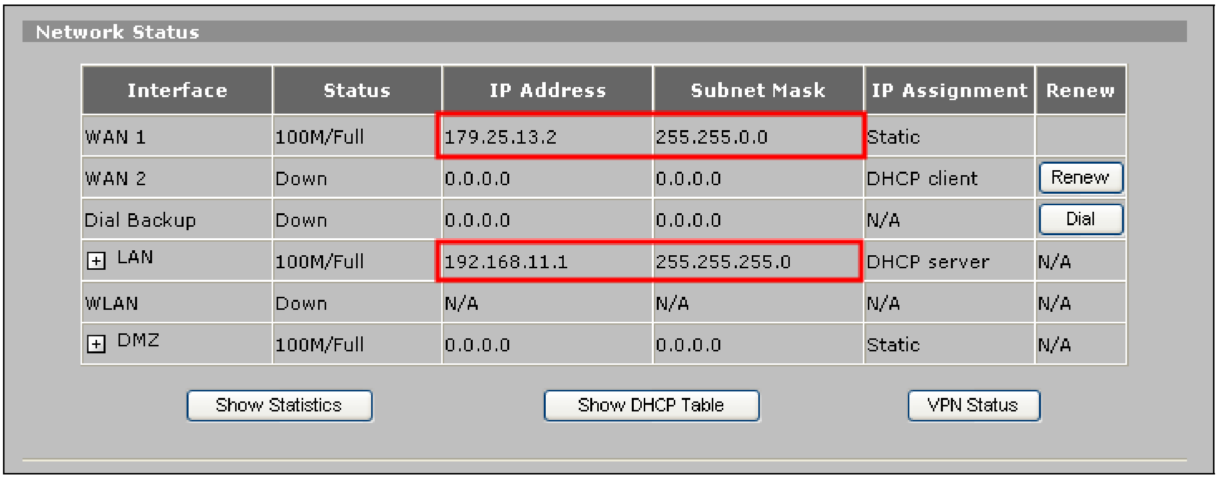
Output Idle Timer 120 (120~3600 sec)
Input Idle Timer 0 (30~3600 sec, 0 means timer disabled)
Gateway Domain Name Update Timer 5 (2~60 min, 0 means timer disabled)
Adjust TCP Maximum Segment Size Auto 0
☑ VPN rules skip applying to the overlap range of local and remote IP addresses.
(Warning: When this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

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 1050 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 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 |

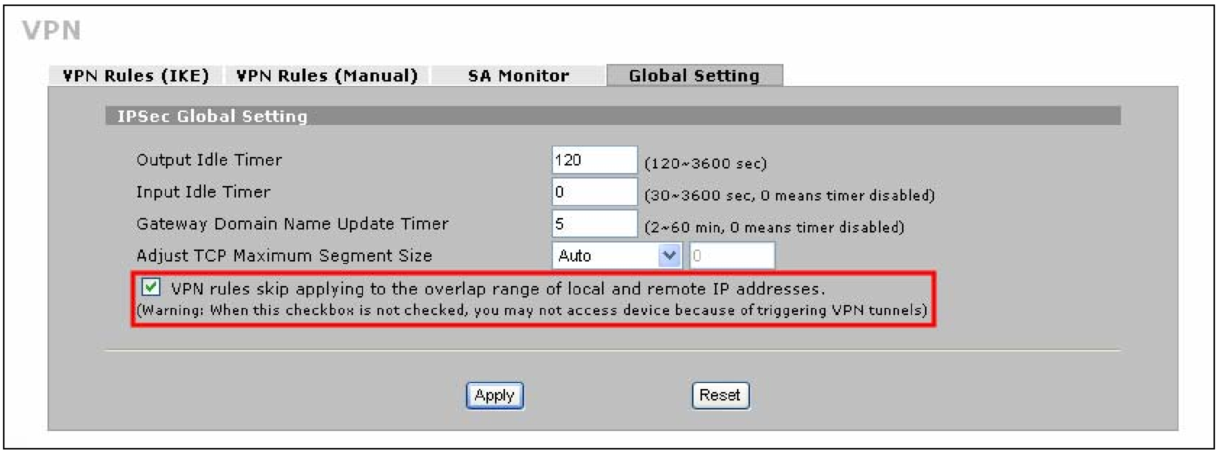
There are similar configuration steps for the ZyWALL35 interface and the VPN setup. The ZyWALL35 WAN and LAN interface are set as follow.



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 | Renew |
| Dial Backup | Down | 0.0.0.0 | 0.0.0.0 | N/A | Dial |
| ⊞ 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 |
| ⊞ DMZ | 100M/Full | 0.0.0.0 | 0.0.0.0 | Static | N/A |

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.

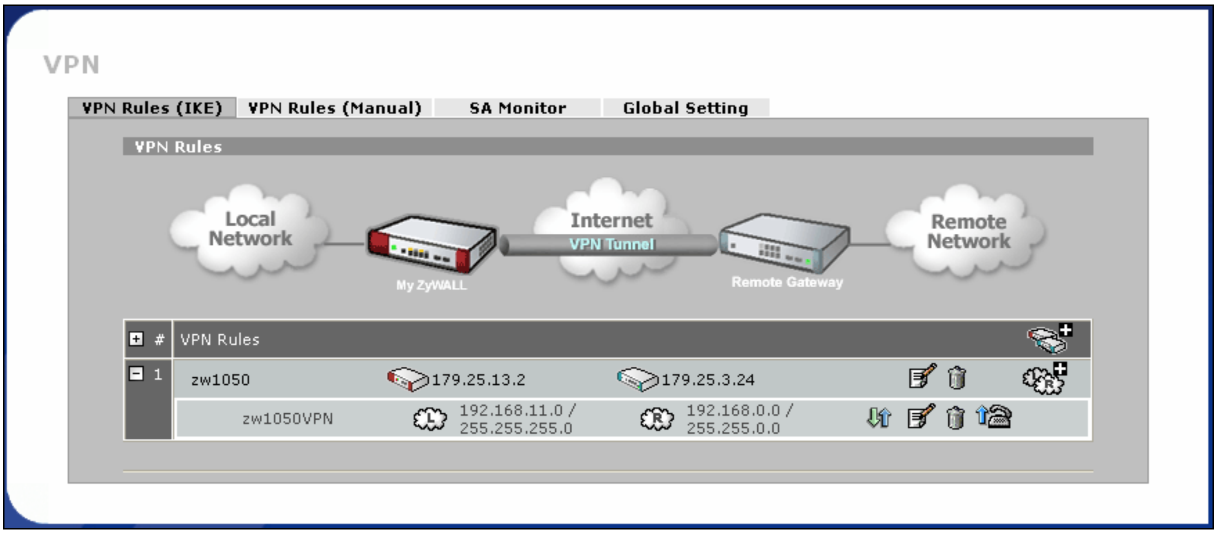


IPSec Global Setting

| | | |
|---|---|---|
| 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)

The VPN tunnel status page after configured the local center ZyWALL 1050 tunnel.



| ⊞ | # | VPN Rules | | |
|---|---|---|---|---|
| ⊟ | 1 | zw1050 | 179.25.13.2 | 179.25.3.24 |
| | | zw1050VPN | 192.168.11.0 / 255.255.255.0 | 192.168.0.0 / 255.255.0.0 |

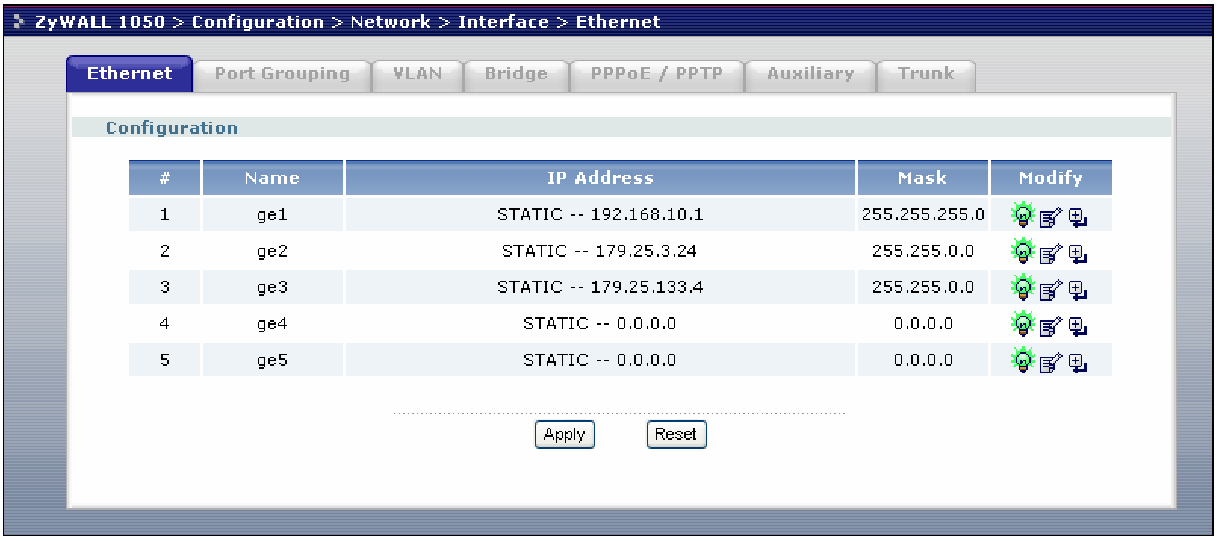
As soon as we finish the configuration of ZyWALL5 and ZyWALL35, we can move to ZyWALL 1050's configuration.

Asia Regional Center ZyWALL 1050 interface and VPN concentrator setting

**The VPN configuration parameter for Asia and Europe regional Center ZyWALL 1050**

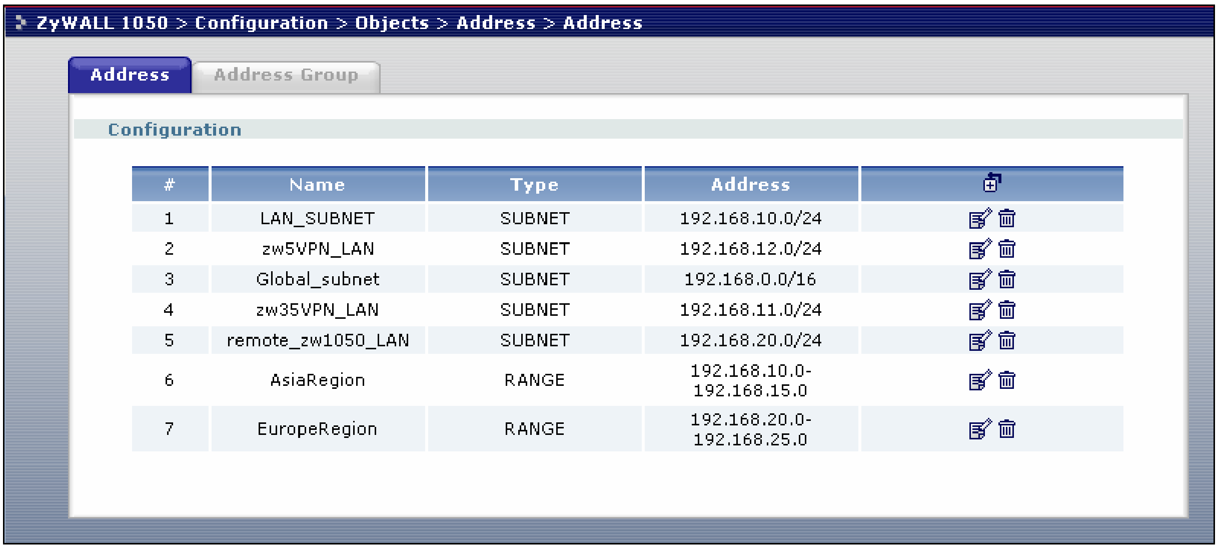
| Asia Regional Center ZyAWLL1050 | Europe Regional Center ZyAWLL1050 |
|---|---|
| WAN1:179.25.3.24<br>WAN2:179.25.133.4<br>LAN:192.168.10.1/24 | WAN1:220.123.113.8<br>WAN2:220.123.119.9<br>LAN:192.168.20.1/24 |
| Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 | Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 |
| Phase2<br>Encapsulation: Tunnel<br>Active Protocol: ESP<br>Encryption: DES<br>Authentication: SHA1<br>Perfect Forward Secrecy (PFS): None | Phase2<br>Encapsulation: Tunnel<br>Active Protocol: ESP<br>Encryption: DES<br>Authentication: SHA1<br>Perfect Forward Secrecy (PFS): None |

Please refer to the application topology to setup the ZyWALL 1050 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.



| # | 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 -- 0.0.0.0 | 0.0.0.0 | |
| 5 | ge5 | STATIC -- 0.0.0.0 | 0.0.0.0 | |

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

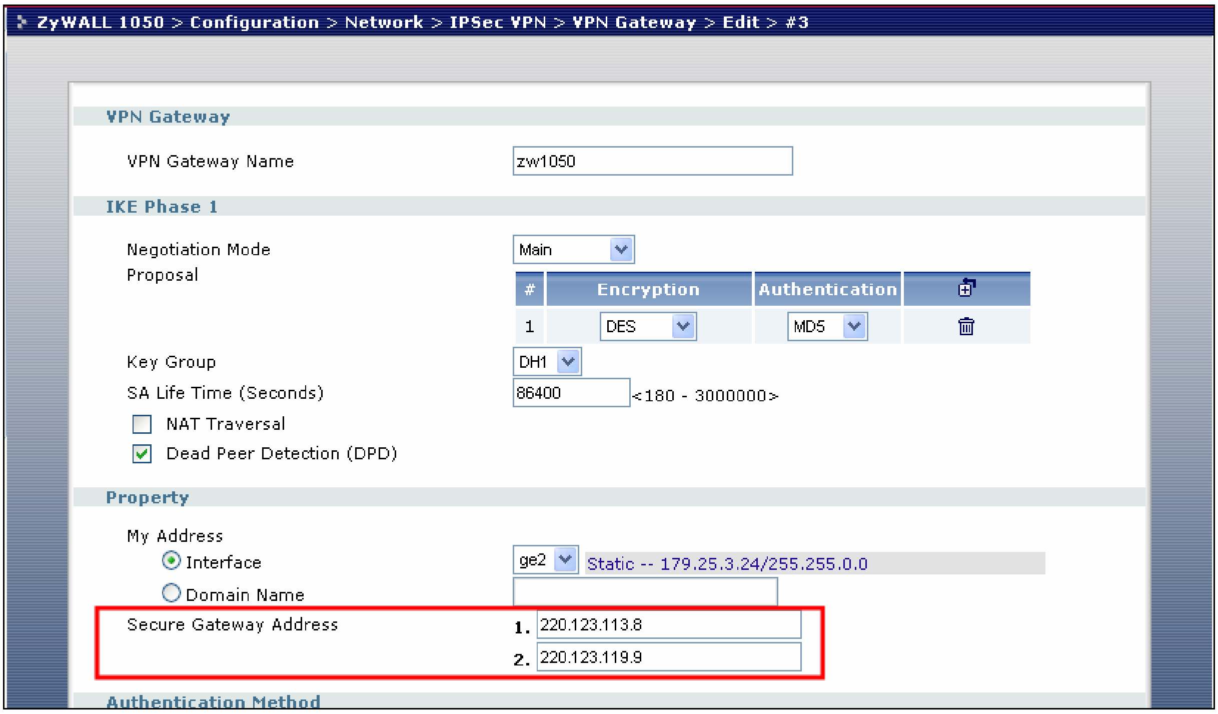


| # | Name | Type | Address | |
|---|---|---|---|---|
| 1 | LAN_SUBNET | SUBNET | 192.168.10.0/24 | |
| 2 | zw5VPN_LAN | SUBNET | 192.168.12.0/24 | |
| 3 | Global_subnet | SUBNET | 192.168.0.0/16 | |
| 4 | zw35VPN_LAN | SUBNET | 192.168.11.0/24 | |
| 5 | remote_zw1050_LAN | SUBNET | 192.168.20.0/24 | |
| 6 | AsiaRegion | RANGE | 192.168.10.0-<br>192.168.15.0 | |
| 7 | EuropeRegion | RANGE | 192.168.20.0-<br>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 1050 can do next processing.

This ZyWALL 1050 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 1050.

Follow the VPN parameter tables to setup the three VPN gateways (IKE / IPSec Phase1). For detail steps please refer to the ZyWALL 1050 user guide. We have to configure a secondary security gateway for the VPN gateway between both of the regional centers' ZyWALL 1050s. The VPN connection can fail over to secondary gateway in case the parameter gateway fails.



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway > Edit > #3

VPN Gateway

VPN Gateway Name: zw1050

IKE Phase 1

Negotiation Mode: Main

Proposal

| # | Encryption | Authentication | |
|---|---|---|---|
| 1 | DES | MD5 | |

Key Group: DH1

SA Life Time (Seconds): 86400 <180 - 3000000>

□ NAT Traversal

☑ Dead Peer Detection (DPD)

Property

My Address

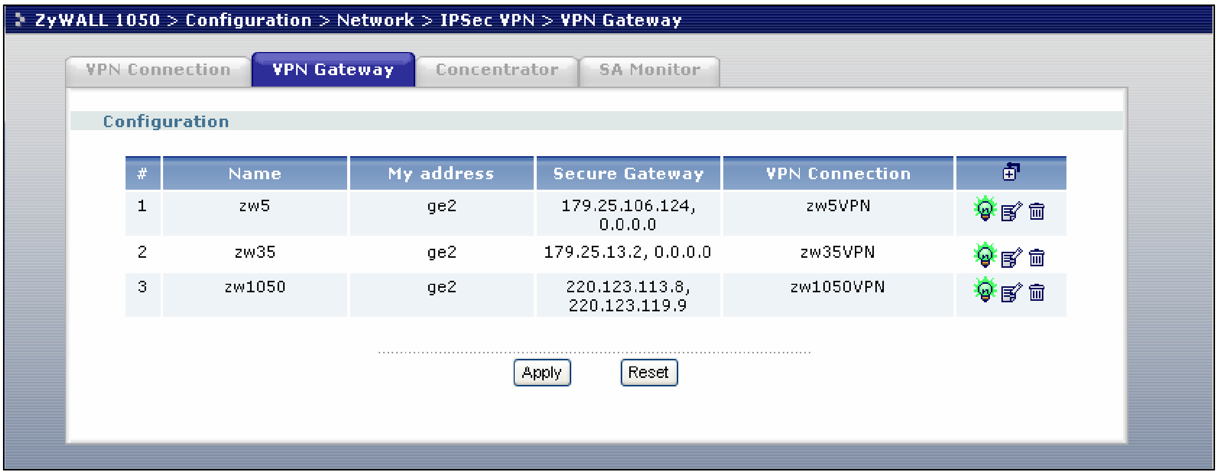
● Interface: ge2 Static -- 179.25.3.24/255.255.0.0

○ Domain Name

Secure Gateway Address: 1. 220.123.113.8 2. 220.123.119.9

Authentication Method

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

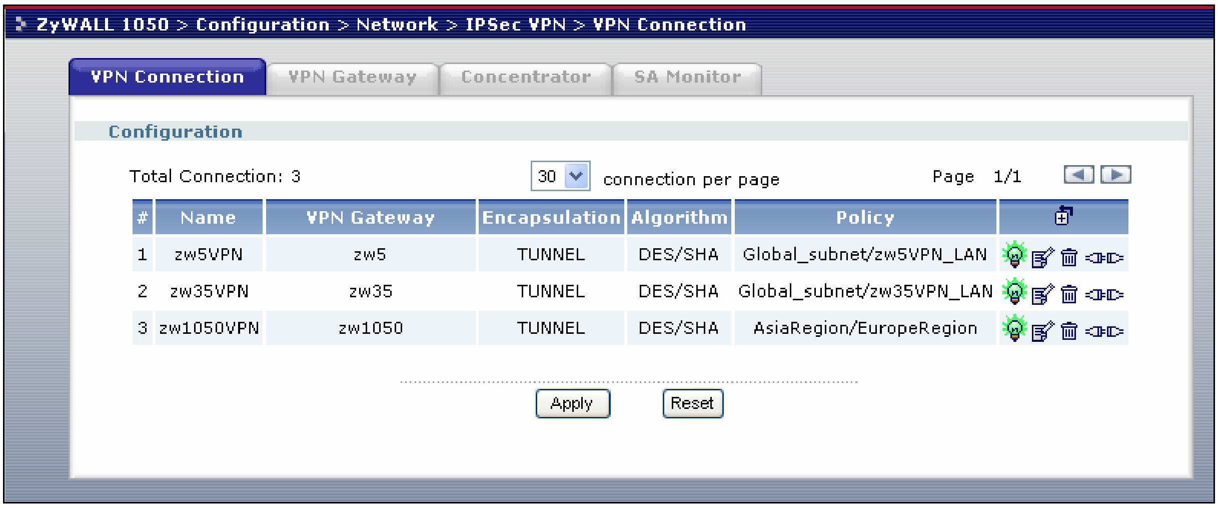


ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway

Configuration

| # | Name | My address | Secure Gateway | VPN Connection | |
|---|---|---|---|---|---|
| 1 | zw5 | ge2 | 179.25.106.124, 0.0.0.0 | zw5VPN | |
| 2 | zw35 | ge2 | 179.25.13.2, 0.0.0.0 | zw35VPN | |
| 3 | zw1050 | ge2 | 220.123.113.8, 220.123.119.9 | zw1050VPN | |

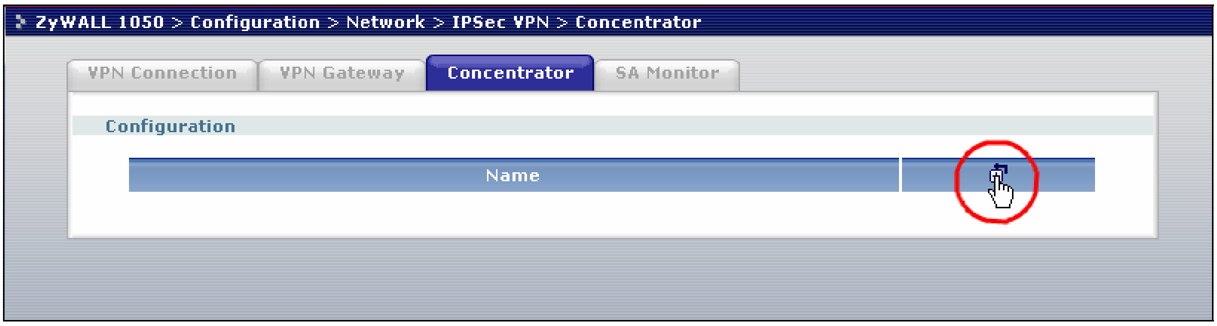
The next step is to create the VPN connection (IPSec / IPSec Phase2). Make sure the parameters are configured correctly, otherwise the VPN will fail to dial. Below is the VPN connection global page.



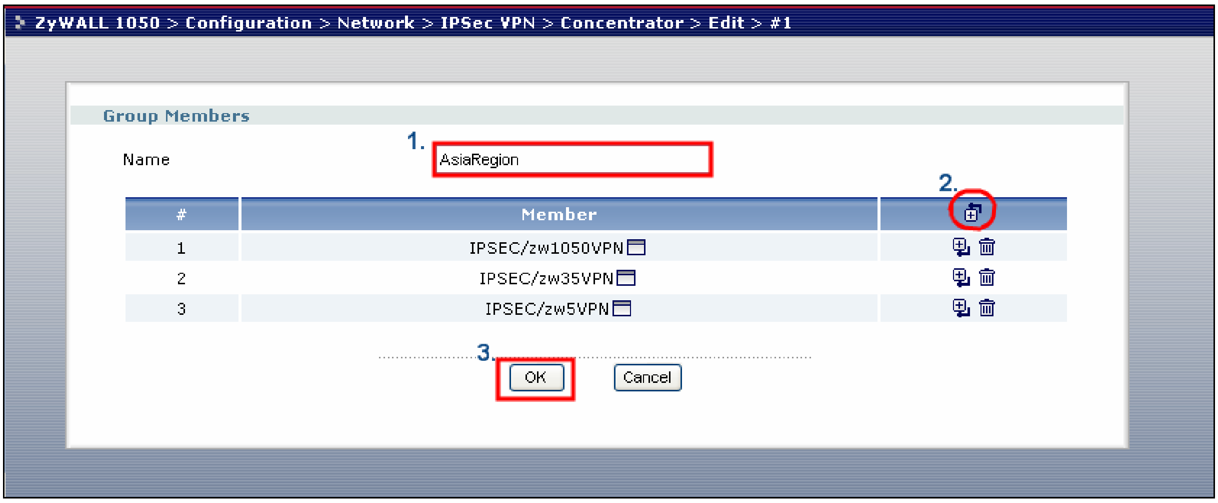
Total Connection: 3 30 connection per page Page 1/1

| # | Name | VPN Gateway | Encapsulation | Algorithm | Policy | |
|---|---|---|---|---|---|---|
| 1 | zw5VPN | zw5 | TUNNEL | DES/SHA | Global_subnet/zw5VPN_LAN | |
| 2 | zw35VPN | zw35 | TUNNEL | DES/SHA | Global_subnet/zw35VPN_LAN | |
| 3 | zw1050VPN | zw1050 | TUNNEL | DES/SHA | AsiaRegion/EuropeRegion | |

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.


ZyWALL 1050 > Configuration > Network > IPSec VPN > Concentrator
VPN Connection
VPN Gateway
Concentrator
SA Monitor
Configuration
Name

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


ZyWALL 1050 > Configuration > Network > IPSec VPN > Concentrator > Edit > #1
Group Members
1.
2.
3.
OK
Cancel

Name AsiaRegion

| # | Member | |
|---|---|---|
| 1 | IPSEC/zw1050VPN | |
| 2 | IPSEC/zw35VPN | |
| 3 | IPSEC/zw5VPN | |

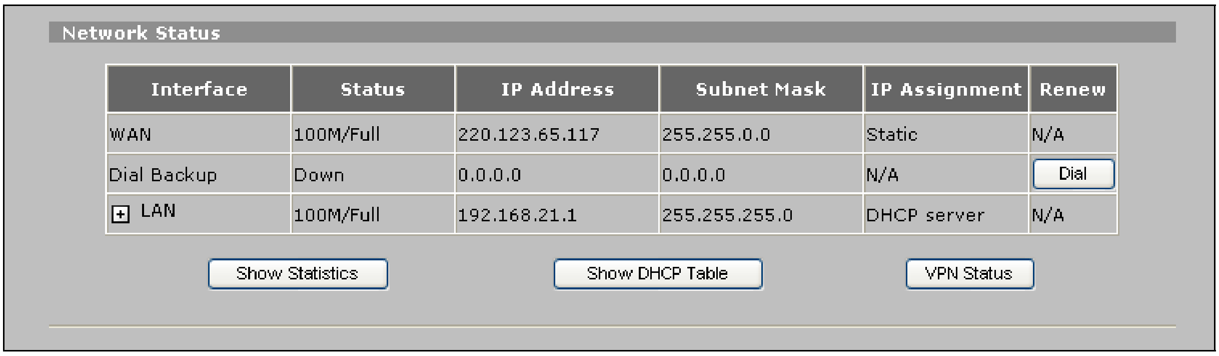
The remote regional center ZyWALL 1050 VPN connection is also treated as a member of this concentrator and the packets will be sent to the remote center first and then following the remote concentrator setting will be routed to the destination sites where the traffic destination is the site allocated 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

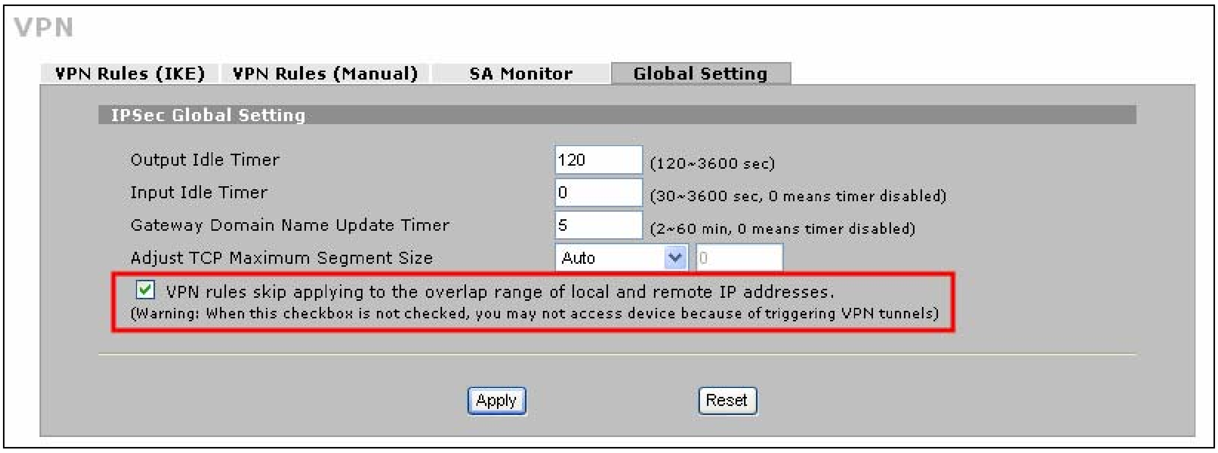
| Interface | Status | IP Address | Subnet Mask | IP Assignment | Renew |
|---|---|---|---|---|---|
| WAN | 100M/Full | 220.123.65.117 | 255.255.0.0 | Static | N/A |
| Dial Backup | Down | 0.0.0.0 | 0.0.0.0 | N/A | Dial |
| ⊞ LAN | 100M/Full | 192.168.21.1 | 255.255.255.0 | DHCP server | N/A |

**The VPN configuration parameters in Europe Region**

| Regional Remote Sites | Regional Center |
|---|---|
| ZyWALL 2 Plus WAN: 220.123.65.117<br>Local Policy: 192.168.21.0/24<br>Remote Policy: 192.168.0.0/16<br>ZyWALL70 WAN: 220.123.97.7<br>Local Policy: 192.168.22.0/24<br>Remote Policy: 192.168.0.0/16 | WAN: 220.123.113.8<br>Local Policy: 192.168.0.0/16<br>Remote Policy: 192.168.21.0/16<br>Local Policy: 192.168.0.0/16<br>Remote Policy: 192.168.22.0/16 |
| Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 | Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 |

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

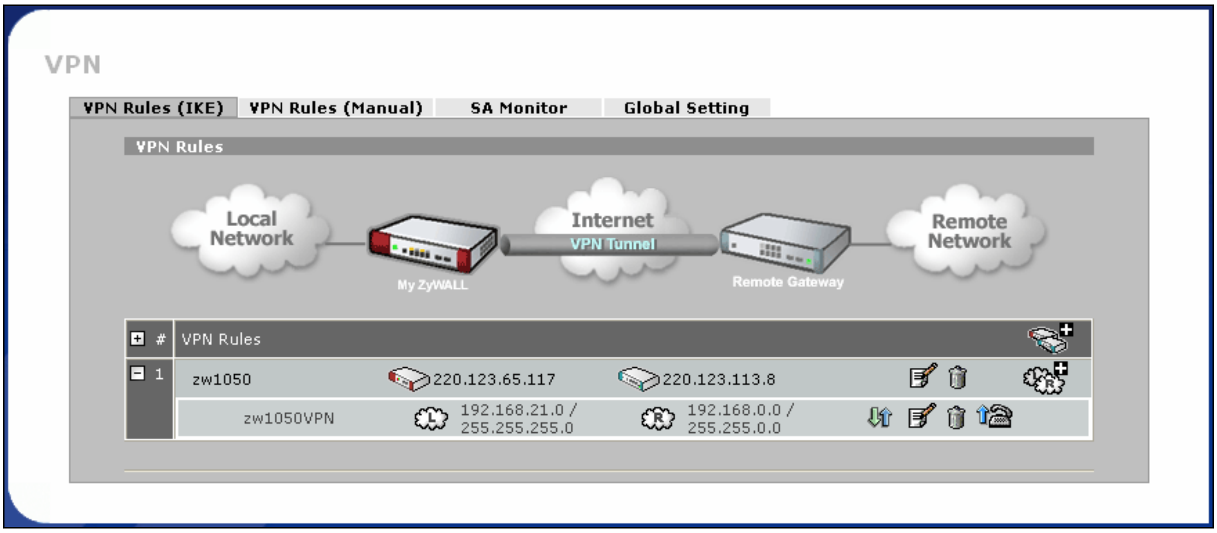


IPSec Global Setting

| | | |
|---|---|---|
| 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 |

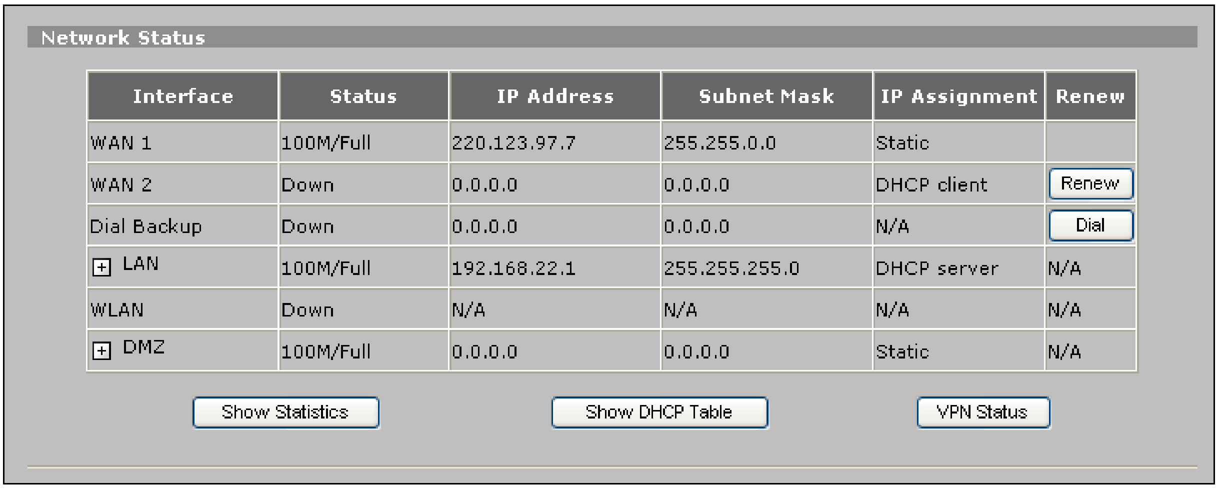
☑ VPN rules skip applying to the overlap range of local and remote IP addresses.
(Warning: When this checkbox is not checked, you may not access device because of triggering VPN tunnels)

Follow the VPN parameter table to configure the VPN tunnel.



| # | VPN Rules | | |
|---|---|---|---|
| 1 | zw1050 | 220.123.65.117 | 220.123.113.8 |
| | zw1050VPN | 192.168.21.0 / 255.255.255.0 | 192.168.0.0 / 255.255.0.0 |

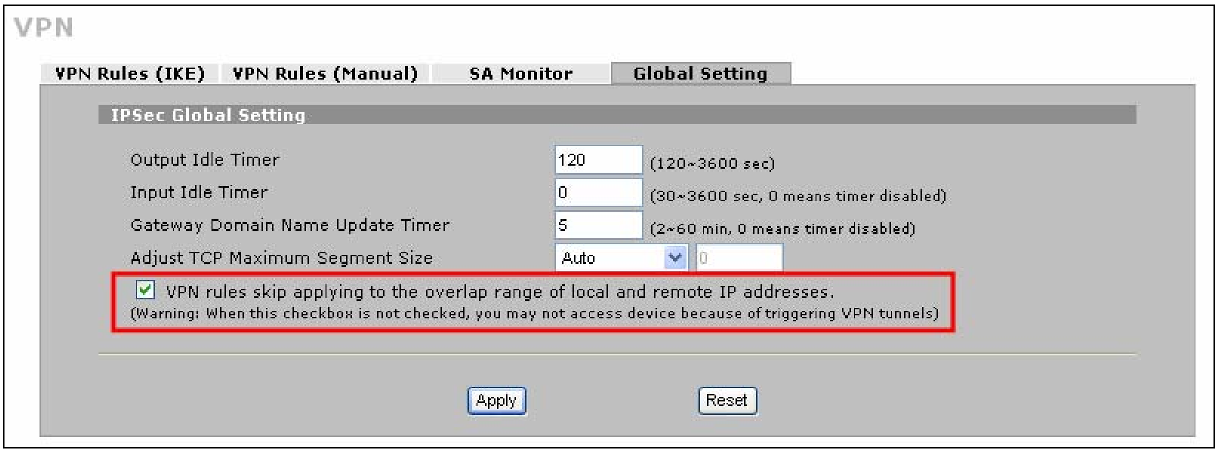
ZyWALL70 WAN and LAN interface setting.



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 | Renew |
| Dial Backup | Down | 0.0.0.0 | 0.0.0.0 | N/A | Dial |
| + 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 |
| + DMZ | 100M/Full | 0.0.0.0 | 0.0.0.0 | Static | N/A |

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



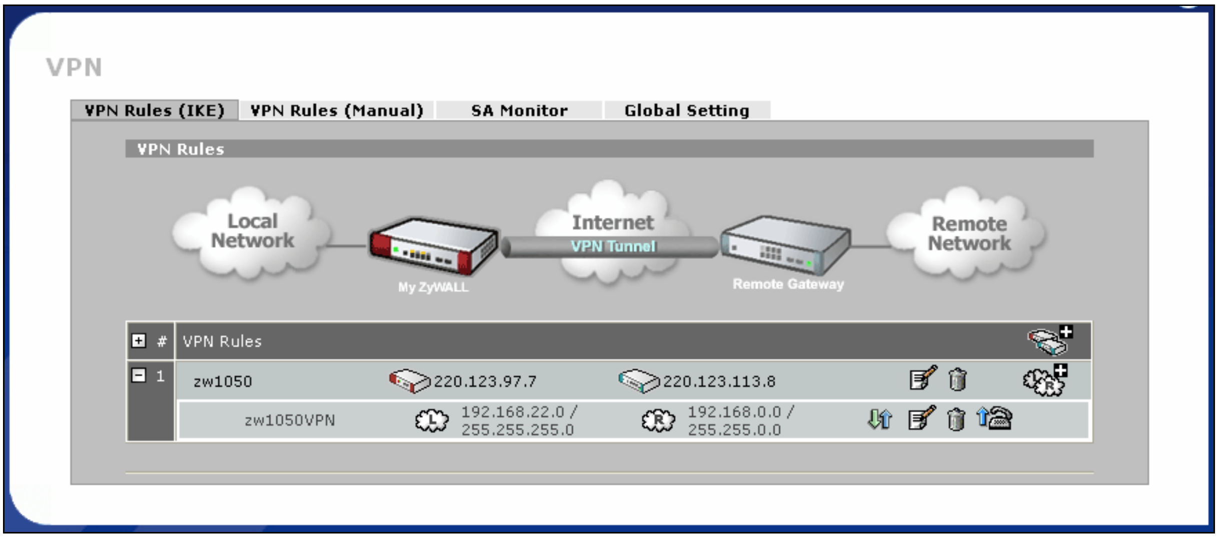
VPN

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)

Follow the VPN parameter table to configure the VPN tunnel.



VPN

| # | VPN Rules | | |
|---|---|---|---|
| 1 | zw1050 | 220.123.97.7 | 220.123.113.8 |
| | zw1050VPN | 192.168.22.0 / 255.255.255.0 | 192.168.0.0 / 255.255.0.0 |

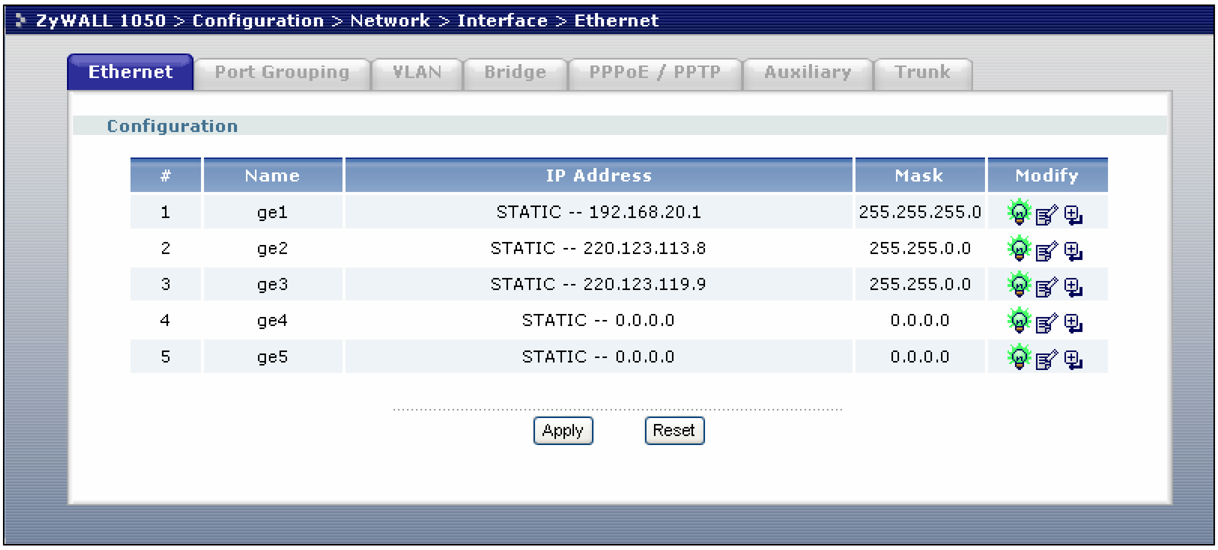
After we finish the configuration of ZyWALL 2 Plus and ZyWALL70, we can move to ZyWALL 1050's configuration.

Europe Regional Center ZyWALL 1050 interface and VPN concentrator setting

**The VPN configuration parameter for Asia and Europe regional Center ZyWALL 1050**

| Asia Regional Center ZyAWLL1050 | Europe Regional Center ZyAWLL1050 |
|---|---|
| WAN1:179.25.3.24<br>WAN2:179.25.133.4<br>LAN:192.168.10.1/24 | WAN1:220.123.113.8<br>WAN2:220.123.119.9<br>LAN:192.168.20.1/24 |
| Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 | Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 |
| Phase2<br>Encapsulation: Tunnel<br>Active Protocol: ESP<br>Encryption: DES<br>Authentication: SHA1<br>Perfect Forward Secrecy (PFS): None | Phase2<br>Encapsulation: Tunnel<br>Active Protocol: ESP<br>Encryption: DES<br>Authentication: SHA1<br>Perfect Forward Secrecy (PFS): None |

Please refer to the application topology to setup the ZyWALL 1050 interface first. Then we can move to setting the VPN.

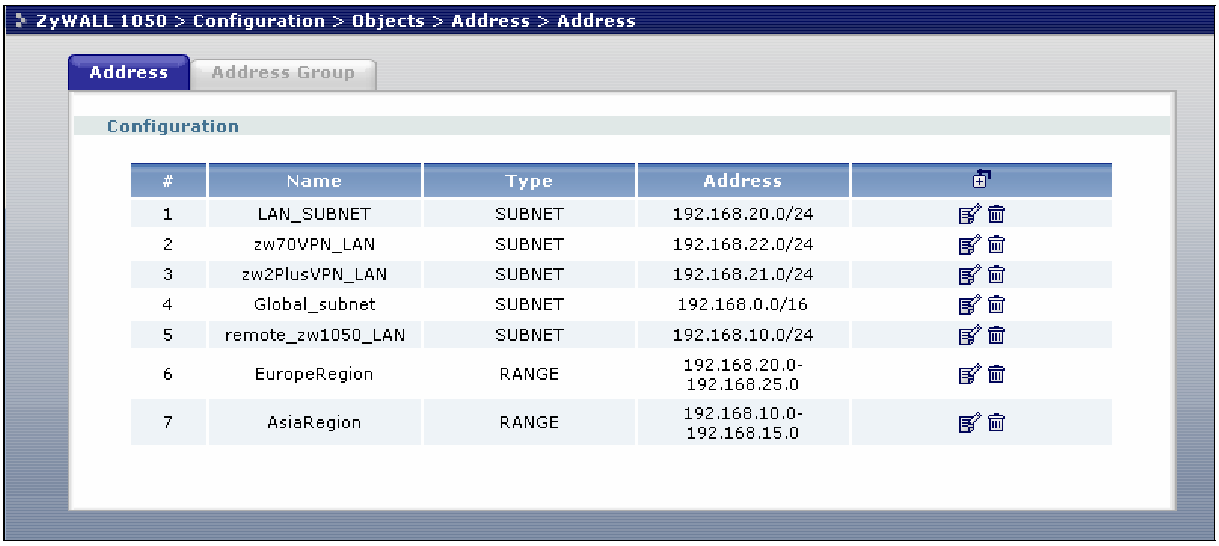


ZyWALL 1050 > Configuration > Network > Interface > Ethernet

Configuration

| # | 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 -- 0.0.0.0 | 0.0.0.0 | |
| 5 | ge5 | STATIC -- 0.0.0.0 | 0.0.0.0 | |

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

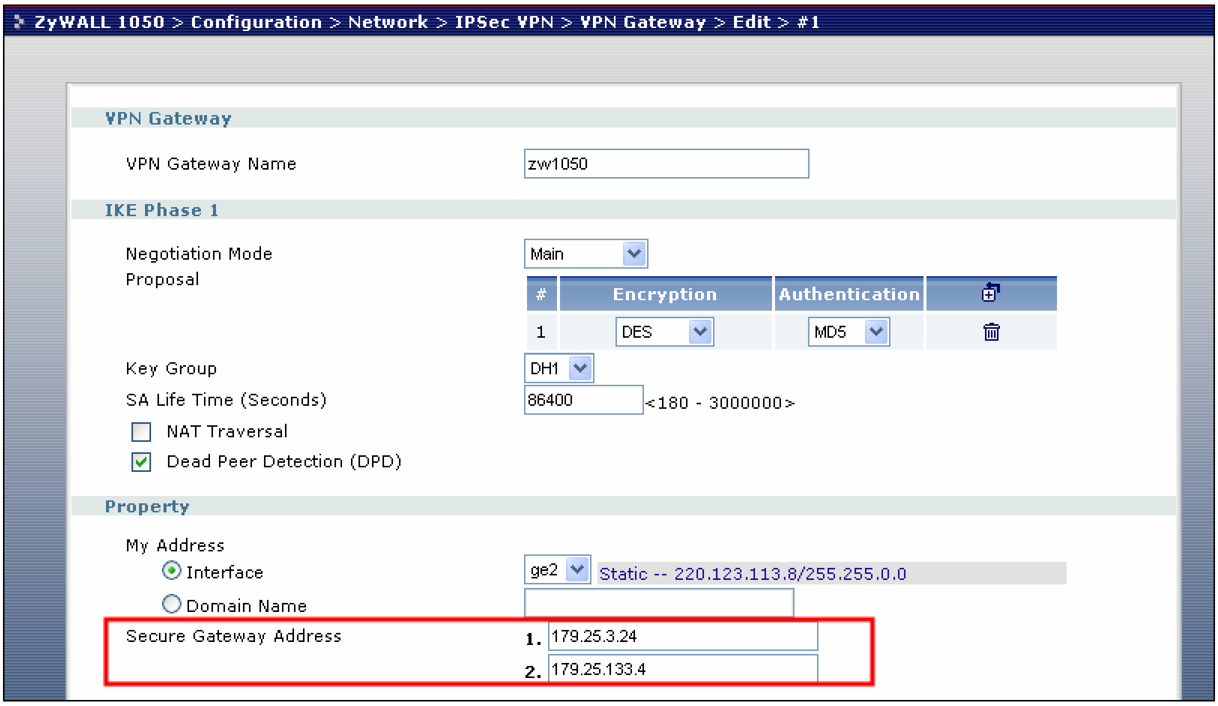


ZyWALL 1050 > Configuration > Objects > Address > Address

Configuration

| # | 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-<br>192.168.25.0 |
| 7 | AsiaRegion | RANGE | 192.168.10.0-<br>192.168.15.0 |

This ZyWALL 1050 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 1050. 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 1050s.



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway > Edit > #1

VPN Gateway

VPN Gateway Name: zw1050

IKE Phase 1

Negotiation Mode: Main

Proposal

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | MD5 |

Key Group: DH1

SA Life Time (Seconds): 86400 <180 - 3000000>

□ NAT Traversal

☑ Dead Peer Detection (DPD)

Property

My Address

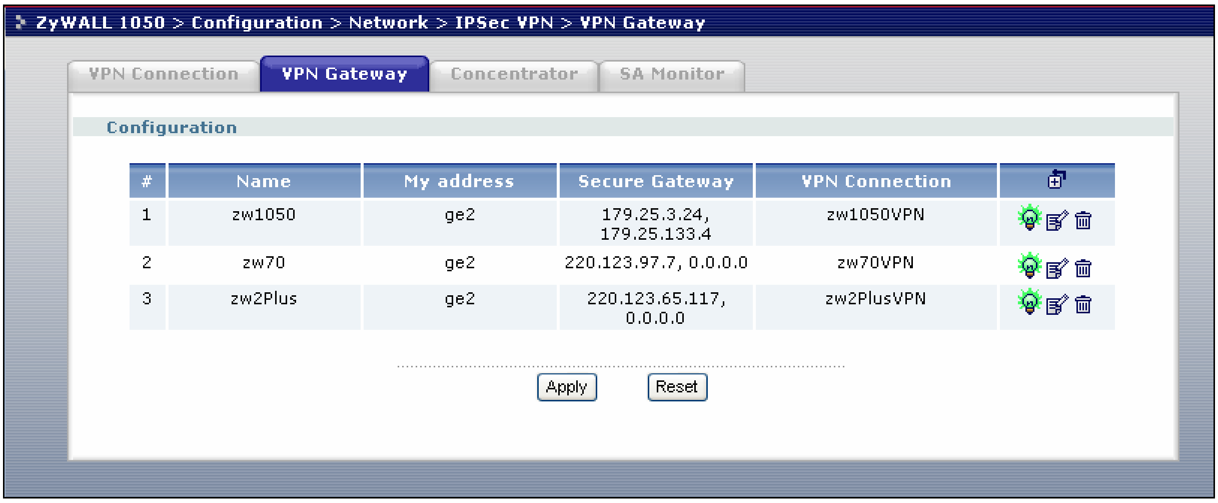
● Interface: ge2 Static -- 220.123.113.8/255.255.0.0

○ Domain Name

Secure Gateway Address 1. 179.25.3.24

2. 179.25.133.4

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

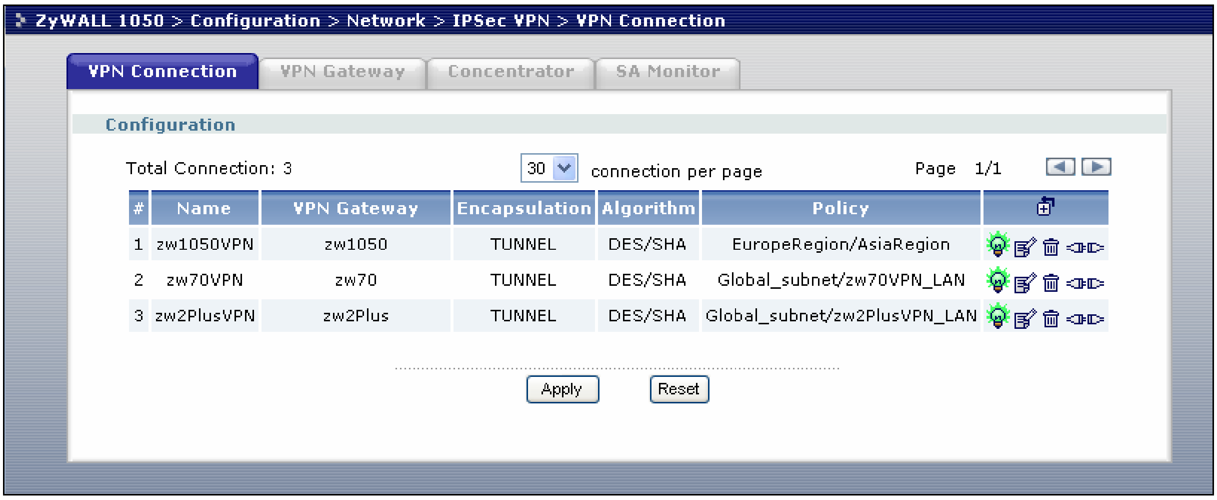


ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway

Configuration

| # | Name | My address | Secure Gateway | VPN Connection |
|---|---|---|---|---|
| 1 | zw1050 | ge2 | 179.25.3.24, 179.25.133.4 | zw1050VPN |
| 2 | zw70 | ge2 | 220.123.97.7, 0.0.0.0 | zw70VPN |
| 3 | zw2Plus | ge2 | 220.123.65.117, 0.0.0.0 | zw2PlusVPN |

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.



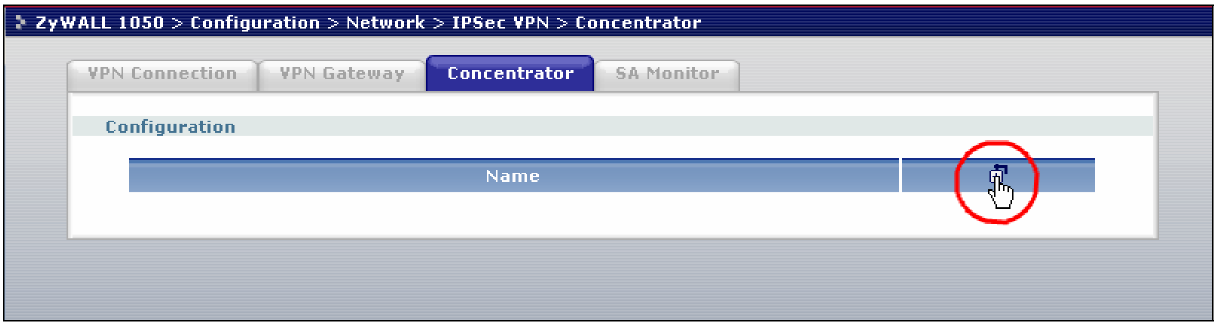
ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Connection

Configuration

Total Connection: 3    30 connection per page    Page 1/1

| # | Name | VPN Gateway | Encapsulation | Algorithm | Policy |
|---|---|---|---|---|---|
| 1 | zw1050VPN | zw1050 | TUNNEL | DES/SHA | EuropeRegion/AsiaRegion |
| 2 | zw70VPN | zw70 | TUNNEL | DES/SHA | Global_subnet/zw70VPN_LAN |
| 3 | zw2PlusVPN | zw2Plus | TUNNEL | DES/SHA | Global_subnet/zw2PlusVPN_LAN |

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.

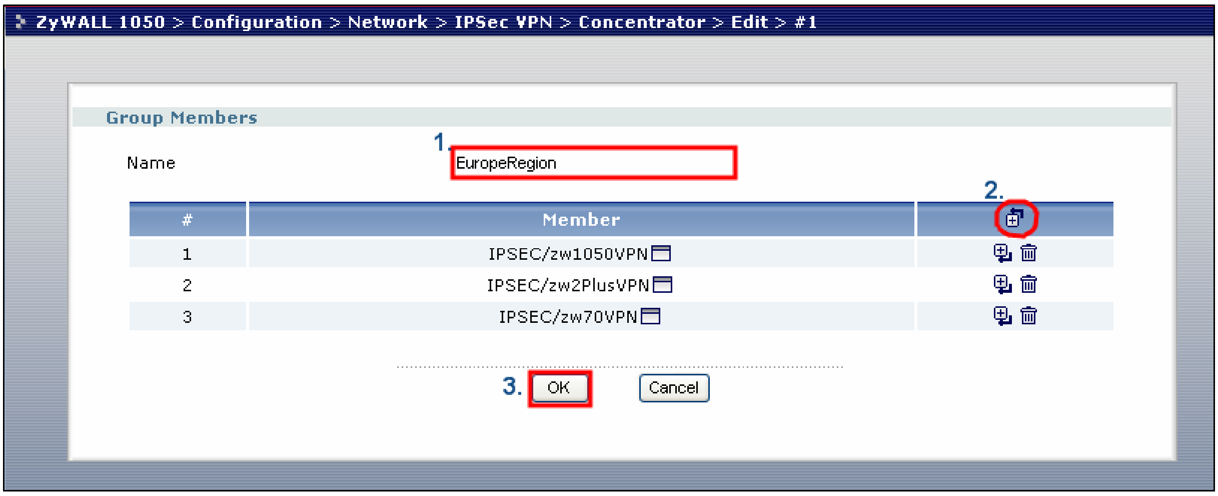


ZyWALL 1050 > Configuration > Network > IPSec VPN > Concentrator

Configuration

| Name | |
|---|---|

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



ZyWALL 1050 > Configuration > Network > IPSec VPN > Concentrator > Edit > #1

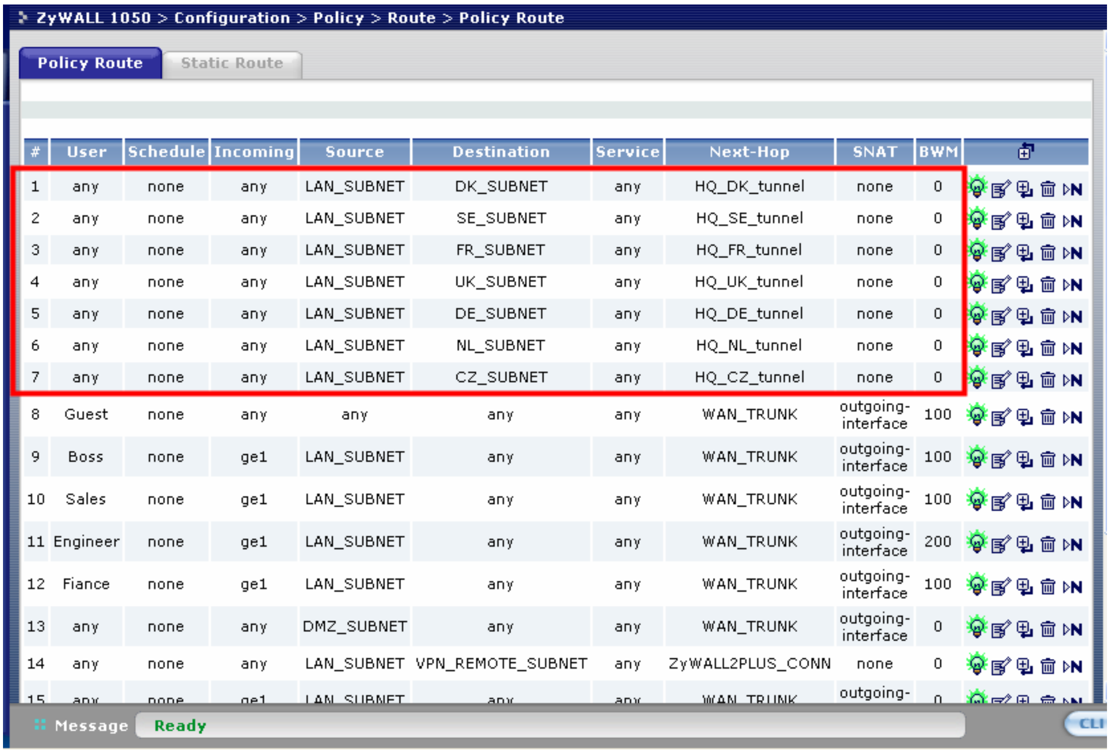
Group Members

Name: EuropeRegion

| # | Member | |
|---|---|---|
| 1 | IPSEC/zw1050VPN | |
| 2 | IPSEC/zw2PlusVPN | |
| 3 | IPSEC/zw70VPN | |

The remote regional center ZyWALL 1050 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.



ZyWALL 1050 > Configuration > Policy > Route > Policy Route

Policy Route | Static Route

| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM |
|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | any | LAN_SUBNET | DK_SUBNET | any | HQ_DK_tunnel | none | 0 |
| 2 | any | none | any | LAN_SUBNET | SE_SUBNET | any | HQ_SE_tunnel | none | 0 |
| 3 | any | none | any | LAN_SUBNET | FR_SUBNET | any | HQ_FR_tunnel | none | 0 |
| 4 | any | none | any | LAN_SUBNET | UK_SUBNET | any | HQ_UK_tunnel | none | 0 |
| 5 | any | none | any | LAN_SUBNET | DE_SUBNET | any | HQ_DE_tunnel | none | 0 |
| 6 | any | none | any | LAN_SUBNET | NL_SUBNET | any | HQ_NL_tunnel | none | 0 |
| 7 | any | none | any | LAN_SUBNET | CZ_SUBNET | any | HQ_CZ_tunnel | none | 0 |
| 8 | Guest | none | any | any | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 9 | Boss | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 10 | Sales | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 11 | Engineer | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 200 |
| 12 | Fiance | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 100 |
| 13 | any | none | any | DMZ_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 0 |
| 14 | any | none | any | LAN_SUBNET | VPN_REMOTE_SUBNET | any | ZyWALL2PLUS_CONN | none | 0 |
| 15 | any | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing- | 0 |

Message Ready

# 1.5 Access via Central Site

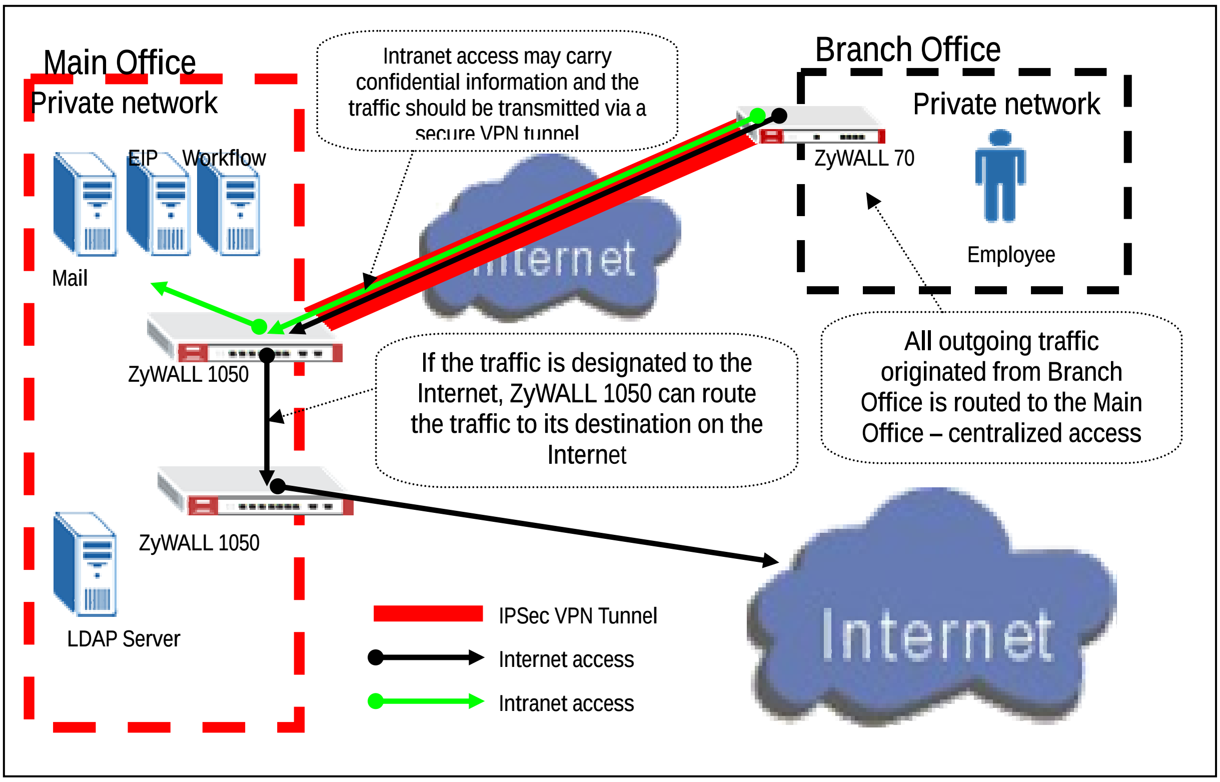
## 1.5.1 VPN Tunnel to Central Site (ZyWALL 70 to ZyWALL 1050)

The idea of this scenario is to redirect all the outgoing traffic originated from the branch office to the main office via the VPN tunnel so that the network administrator can manage and control the traffic or apply additional secure access control or inspection.

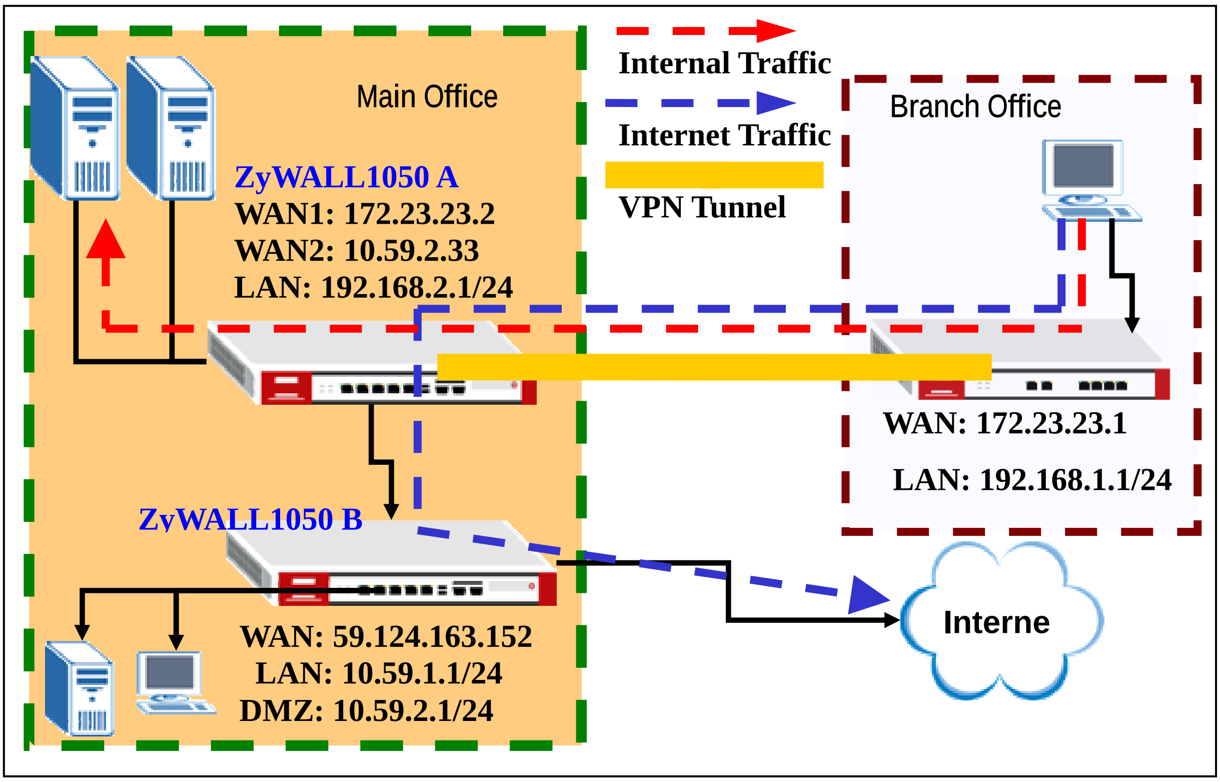
What is the benefit for deploying ZyWALL1050 in this kind of application?

- **Insecurity of Internet connectivity**
  - Virus, Bots, spyware, exploits and other forms of attacks are all coming in from the Internet
  - As a result, Internet connectivity needs to be securely managed & watched
  - “Avoid multiple Internet connections in a corporate network” is a common security practice
- **What there is a multi-site, distributed corporate network?**
  - Through network planning, centralized Internet connectivity can be achieved
  - ZyWALL 1050 helps you to easily achieve this goal

For the enterprise security and performance consideration, we can also separate the VPN and internet connection loading and send it through different security gateways. Thus, all VPNs connected to the VPN gateway can apply the VPN concentrator role; the internet connection gateway will focus on the internet connection and perform all layer7 security inspection. By doing this, we can achieve good level of security while the total network throughput and performance remains high.


Main Office
Private network
EIP
Workflow
Mail
ZyWALL 1050
ZyWALL 1050
LDAP Server
Intranet access may carry confidential information and the traffic should be transmitted via a secure VPN tunnel
Internet
Branch Office
Private network
ZyWALL 70
Employee
If the traffic is designated to the Internet, ZyWALL 1050 can route the traffic to its destination on the Internet
All outgoing traffic originated from Branch Office is routed to the Main Office – centralized access
IPSec VPN Tunnel
Internet access
Intranet access
Internet

The network topology below is used to illustrate this application. We used ZyWALL70 as branch office gateway which is connected to the main office’s ZyWALL1050 A. All the outgoing traffic from the branch office including the internet traffic and the remote subnet traffic will be send to the VPN tunnel and handled by ZyWALL1050 A. ZyWALL1050 uses WAN1 to establish VPN connection with ZyWALL70 in remote office and WAN2 as an uplink to the ZyWALL1050 B which is the internet connection gateway of main office. Thus, ZyWALL1050 A will route the traffic from the VPN tunnel and send it to the appropriate place of the packet destination.



**VPN configuration table**

| Main office – ZyWALL 1050 A | Branch office – ZyWALL 70 |
|---|---|
| My Address: ge2, 10.59.1.55<br>Security Gateway Address: 10.59.1.69<br>Local: Range, 0.0.0.0-255.255.255.255<br>Remote: Subnet, 192.168.1.0/24 | My Address: 10.59.1.69<br>Security Gateway Address: 10.59.1.55<br>Local network: Subnet, 192.168.1.0/24<br>Remote network: Range, 0.0.0.0-255.255.255.255 |
| Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 | Phase 1<br>Negotiation Mode : Main<br>Pre-share key: 123456789<br>Encryption :DES<br>Authentication :MD5<br>Key Group :DH1 |

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

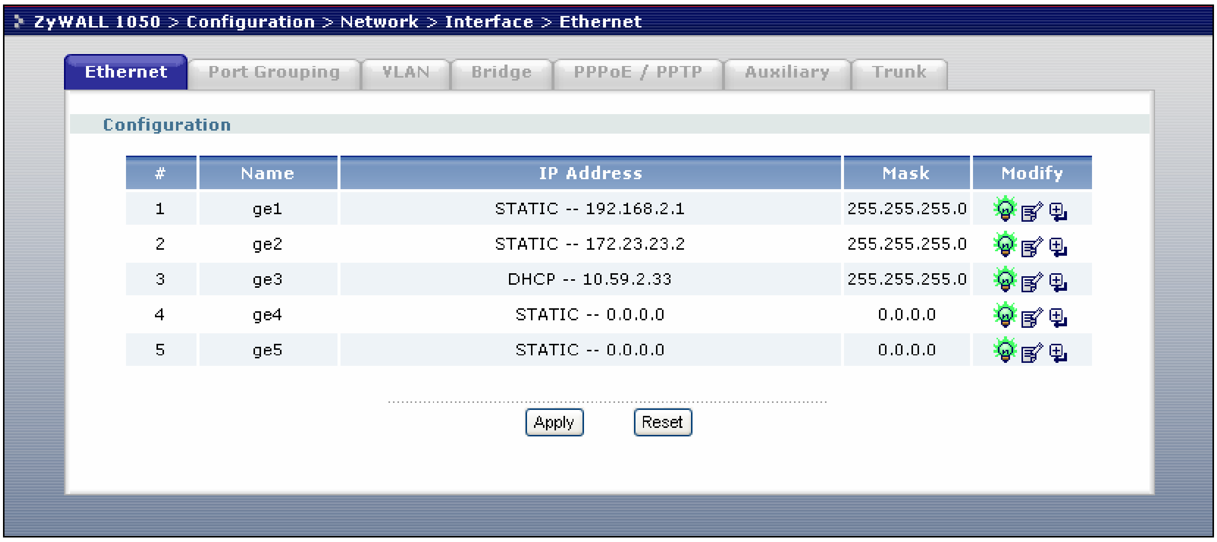
To achieve this, we have to complete the following tasks:

- On ZyWALL1050, create the object 'Address' for remote network ranging from 0.0.0.0 to 255.255.255.255
- On ZyWALL1050, configure VPN gateway and connection settings
- On ZyWALL70, configure the corresponding VPN settings

See the following step-by-step configuration.

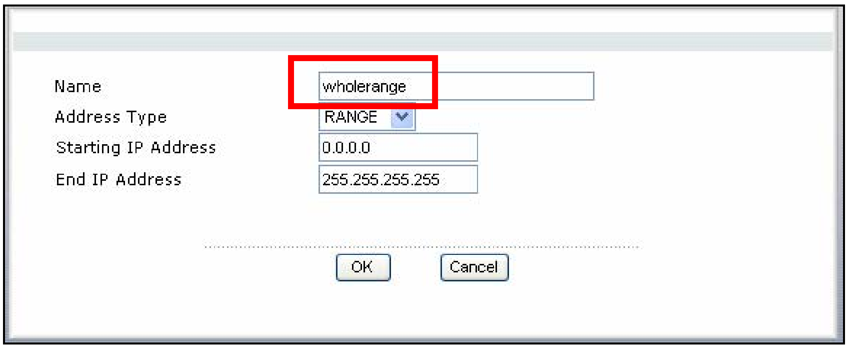
## ZyWALL1050 A configuration

1) Login ZyWALL1050 A GUI and go to **Configuration** > **Network** > **Interface** > **Ethernet** and configure the IP setting as shown in the topology.



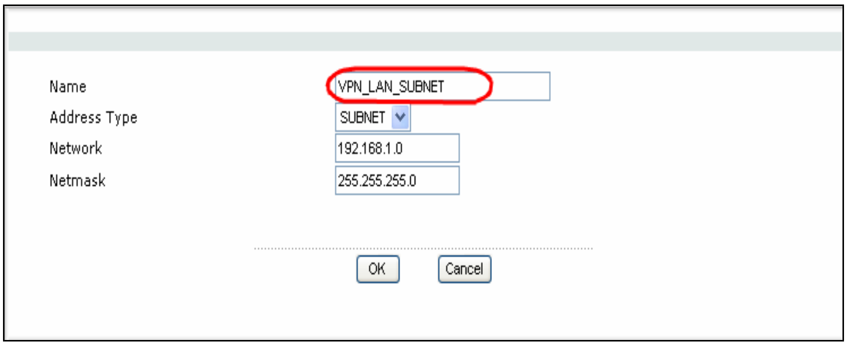
| # | Name | IP Address | Mask | Modify |
|---|---|---|---|---|
| 1 | ge1 | STATIC -- 192.168.2.1 | 255.255.255.0 | |
| 2 | ge2 | STATIC -- 172.23.23.2 | 255.255.255.0 | |
| 3 | ge3 | DHCP -- 10.59.2.33 | 255.255.255.0 | |
| 4 | ge4 | STATIC -- 0.0.0.0 | 0.0.0.0 | |
| 5 | ge5 | STATIC -- 0.0.0.0 | 0.0.0.0 | |

2) Go to **Configuration** > **Object** >**Address** to create an address object for all the incoming traffic.



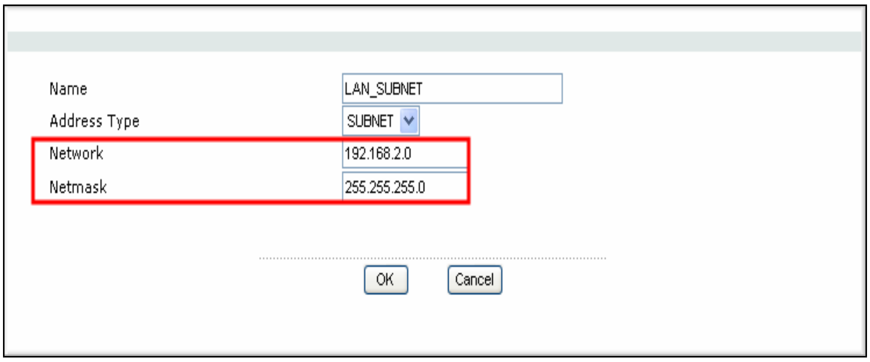
| | |
|---|---|
| Name | wholerange |
| Address Type | RANGE |
| Starting IP Address | 0.0.0.0 |
| End IP Address | 255.255.255.255 |

Configure the other address object VPN_LAN_SUBNET for the VPN remote network usage.



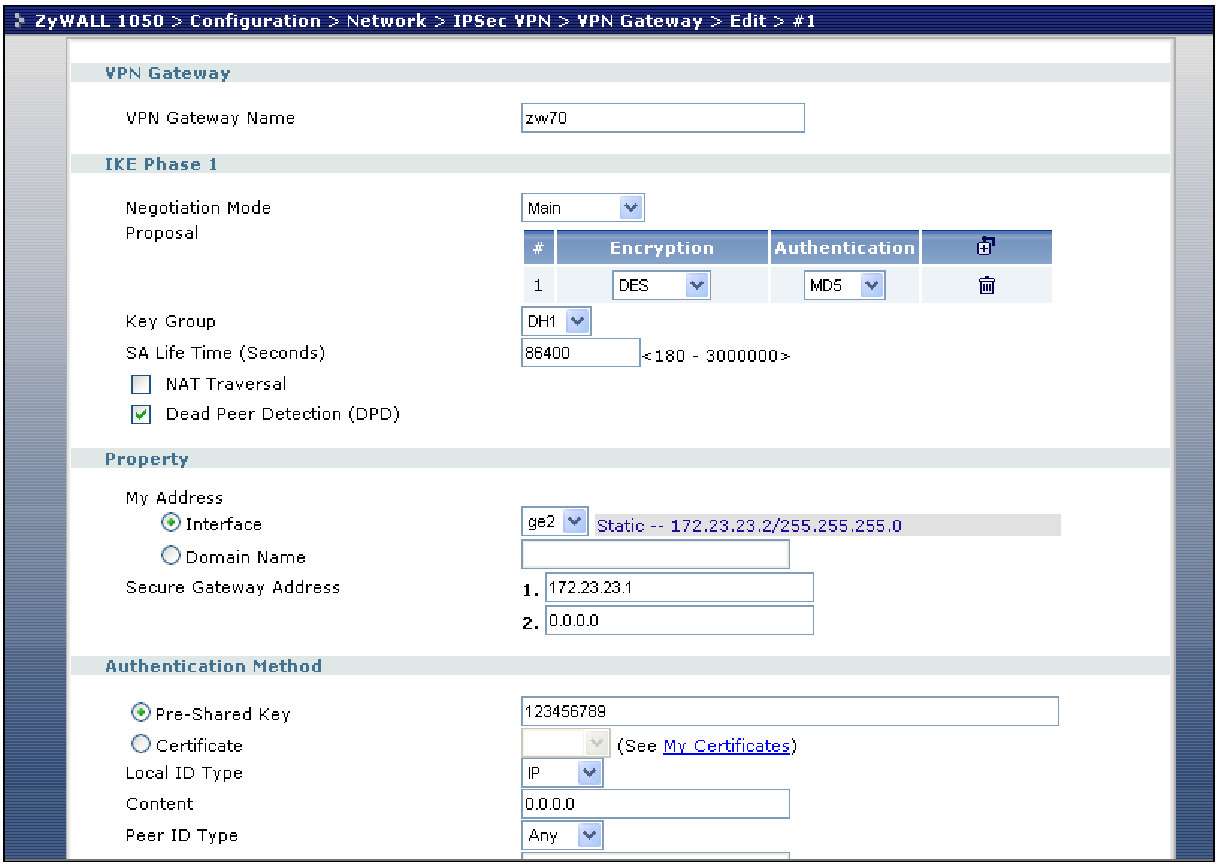
| | |
|---|---|
| Name | VPN_LAN_SUBNET |
| Address Type | SUBNET |
| Network | 192.168.1.0 |
| Netmask | 255.255.255.0 |

Modify the LAN_SUBNET address to 192.168.2.0 as used in our topology.



| | |
|---|---|
| Name | LAN_SUBNET |
| Address Type | SUBNET |
| Network | 192.168.2.0 |
| Netmask | 255.255.255.0 |

3) Switch to **Configuration** > **Network** > **IPSec VPN** > **VPN Connection** > **VPN Gateway** to set the VPN Gateway. Here we select ‘ge2’ as **My Address**. We put 172.23.23.2 as the **Security Gateway Address** and 123456789 as the **Pre-Shared Key.** For other parameters, we leave them as default. There are no special settings for these parameters and the main concern is to let the VPN peers match each other.



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway > Edit > #1

**VPN Gateway**

| | |
|---|---|
| VPN Gateway Name | zw70 |

**IKE Phase 1**

| | |
|---|---|
| Negotiation Mode | Main |
| Proposal | |

| # | Encryption | Authentication | |
|---|---|---|---|
| 1 | DES | MD5 | |

| | |
|---|---|
| Key Group | DH1 |
| SA Life Time (Seconds) | 86400 <180 - 3000000> |

□ NAT Traversal

☑ Dead Peer Detection (DPD)

**Property**

My Address

● Interface: ge2 Static -- 172.23.23.2/255.255.255.0

○ Domain Name

Secure Gateway Address: 1. 172.23.23.1 2. 0.0.0.0

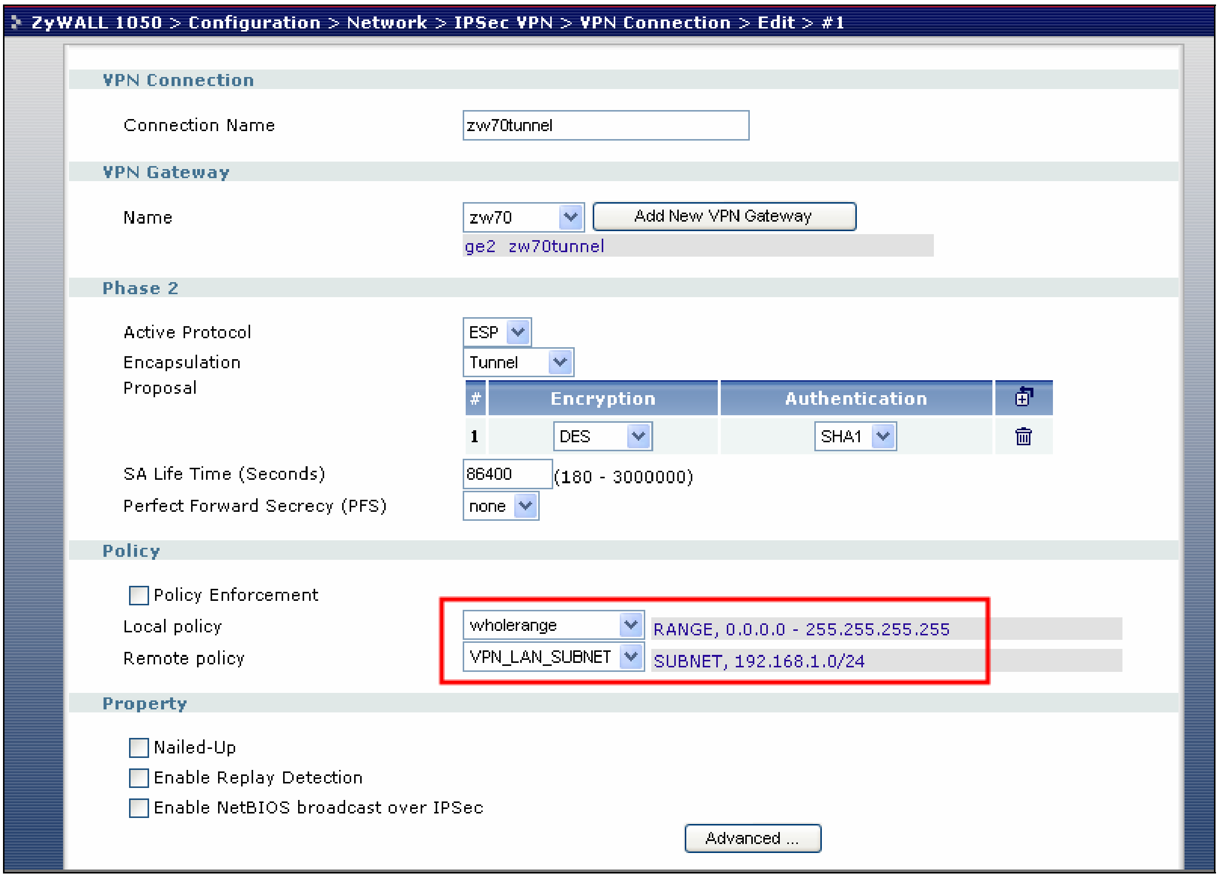
**Authentication Method**

● Pre-Shared Key: 123456789

○ Certificate (See My Certificates)

| | |
|---|---|
| Local ID Type | IP |
| Content | 0.0.0.0 |
| Peer ID Type | Any |

4) Go to **Configuration** > **Network** > **IPSec VPN** >**VPN Connection** to set the VPN Connection. Here we choose the gateway which has been configured in the step2 as the VPN gateway. Because such VPN tunnel is used for central site, we should specify the **Local policy** as a range of 0.0.0.0-255.255.255.255. This range has been pre-defined in the step1 and we just need to select it in the drop down list. Here, we assume the peer subnet is 192.168.1.x and select the default address object 'VPN_LAN_SUBNET' to meet our requirements.



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Connection > Edit > #1

**VPN Connection**

Connection Name: zw70tunnel

**VPN Gateway**

Name: zw70 [Add New VPN Gateway]
ge2 zw70tunnel

**Phase 2**

Active Protocol: ESP
Encapsulation: Tunnel
Proposal:

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | SHA1 |

SA Life Time (Seconds): 86400 (180 - 3000000)
Perfect Forward Secrecy (PFS): none

**Policy**

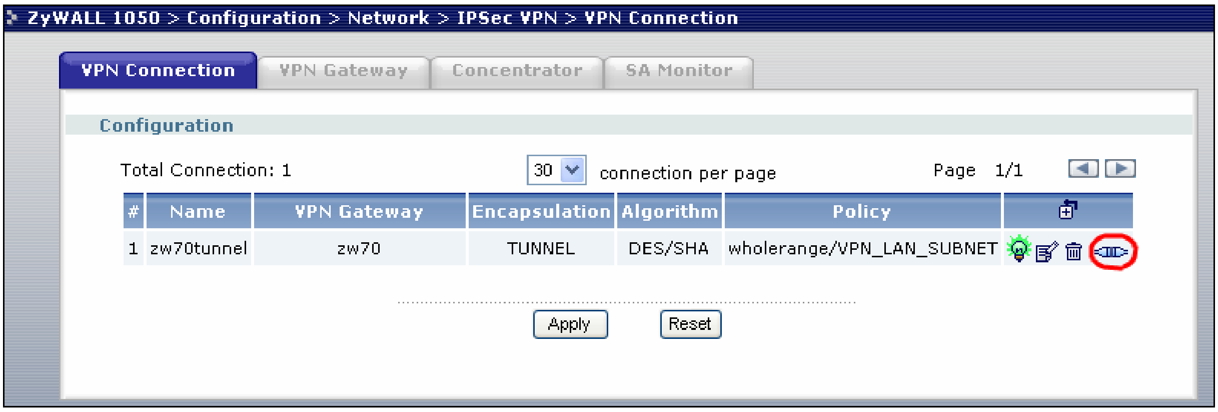
☐ Policy Enforcement
Local policy: wholerange RANGE, 0.0.0.0 - 255.255.255.255
Remote policy: VPN_LAN_SUBNET SUBNET, 192.168.1.0/24

**Property**

☐ Nailed-Up
☐ Enable Replay Detection
☐ Enable NetBIOS broadcast over IPSec

[Advanced ...]

Try to click the connect icon to confirm the VPN configuration correctness.



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Connection

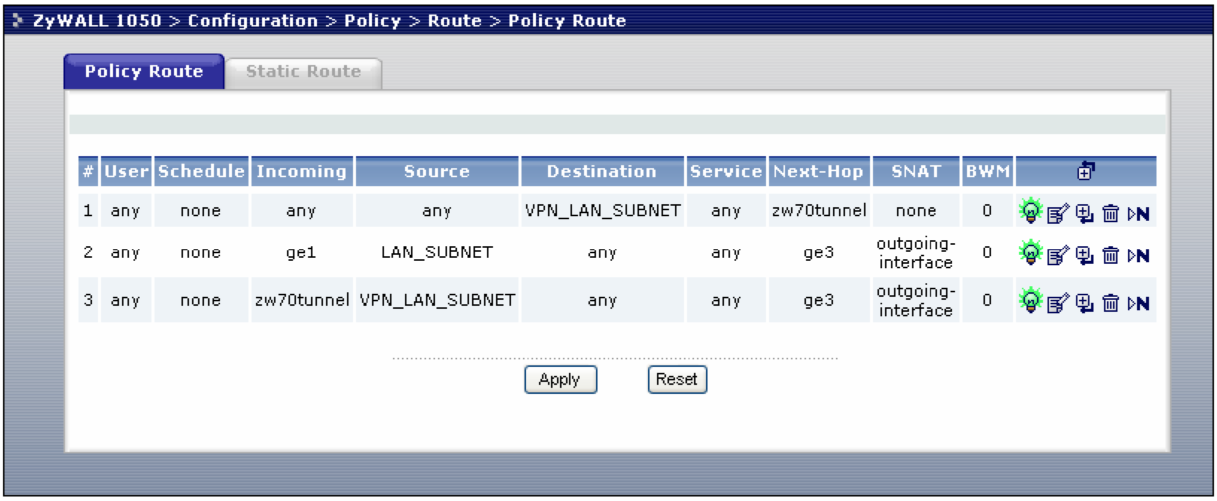
**Configuration**

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

| # | Name | VPN Gateway | Encapsulation | Algorithm | Policy |
|---|---|---|---|---|---|
| 1 | zw70tunnel | zw70 | TUNNEL | DES/SHA | wholerange/VPN_LAN_SUBNET |

[Apply] [Reset]

5) The next step is to configure the policy route. We need three policy routes to fulfill our application. **First policy route rule** is to route the traffic destination of which is the host located in a VPN remote subnet and the next-hop will be VPN tunnel. **Second policy route rule** is for LAN host to internet, thus the next-hop will be ge3 that is connected to the internet gateway ZyWALL 1050 B. **The third rule** is for the traffic coming from the VPN tunnel and the destination is the internet. Then next-hop will be ge3.



| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM |
|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | any | any | VPN_LAN_SUBNET | any | zw70tunnel | none | 0 |
| 2 | any | none | ge1 | LAN_SUBNET | any | any | ge3 | outgoing-interface | 0 |
| 3 | any | none | zw70tunnel | VPN_LAN_SUBNET | any | any | ge3 | outgoing-interface | 0 |

The CLI commands for application:

Address Object:

```
[0] address-object wholerange 0.0.0.0-255.255.255.255
[0] address-object VPN_LAN_SUBNET 192.168.1.0 255.255.255.0
[0] address-object LAN_SUBNET 192.168.2.0 255.255.255.0
```

VPN Gateway:

```
[0] isakmp policy zw70
[1] mode main
[2] transform-set des-md5
[3] lifetime 86400
[4] no natt
[5] dpd
[6] local-ip interface ge2
[7] peer-ip 172.23.23.1 0.0.0.0
[8] authentication pre-share
[9] keystring 123456789
[10] local-id type ip 0.0.0.0
[11] peer-id type any
[12] xauth type server default deactivate
[13] group1
[14] exit
```

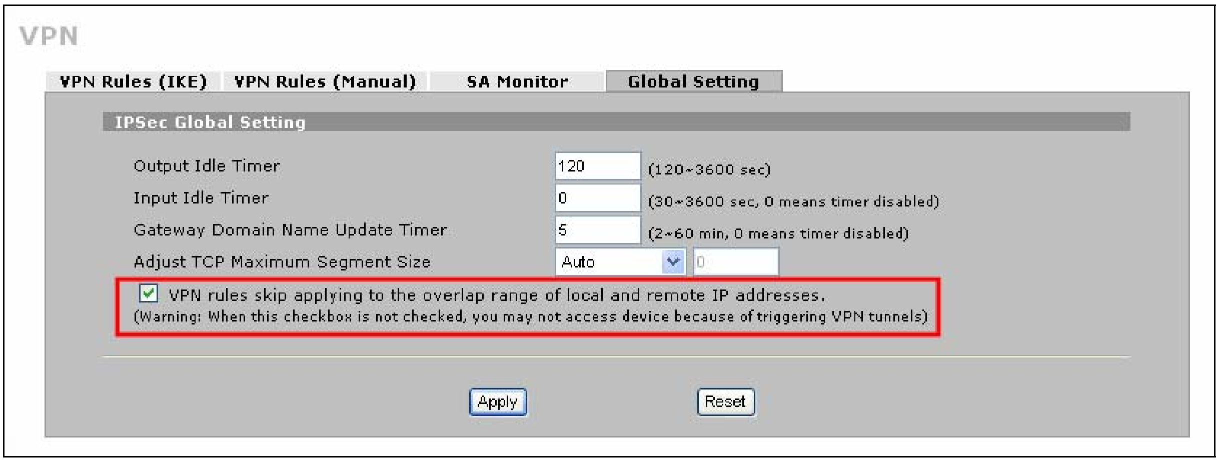
VPN Connection:

```
[0] crypto map zw70tunnel
[1] ipsec-isakmp zw70
[2] encapsulation tunnel
[3] transform-set esp-des-sha
[4] set security-association lifetime seconds 86400
[5] set pfs none
[6] no policy-enforcement
[7] local-policy wholerange
[8] remote-policy VPN_LAN_SUBNET
```

```
[9] no nail-up
[10] no replay-detection
[11] no netbios-broadcast
[12] no out-snat activate
[13] no in-snat activate
[14] no in-dnat activate
[15] exit
```

ZyWALL70 configuration

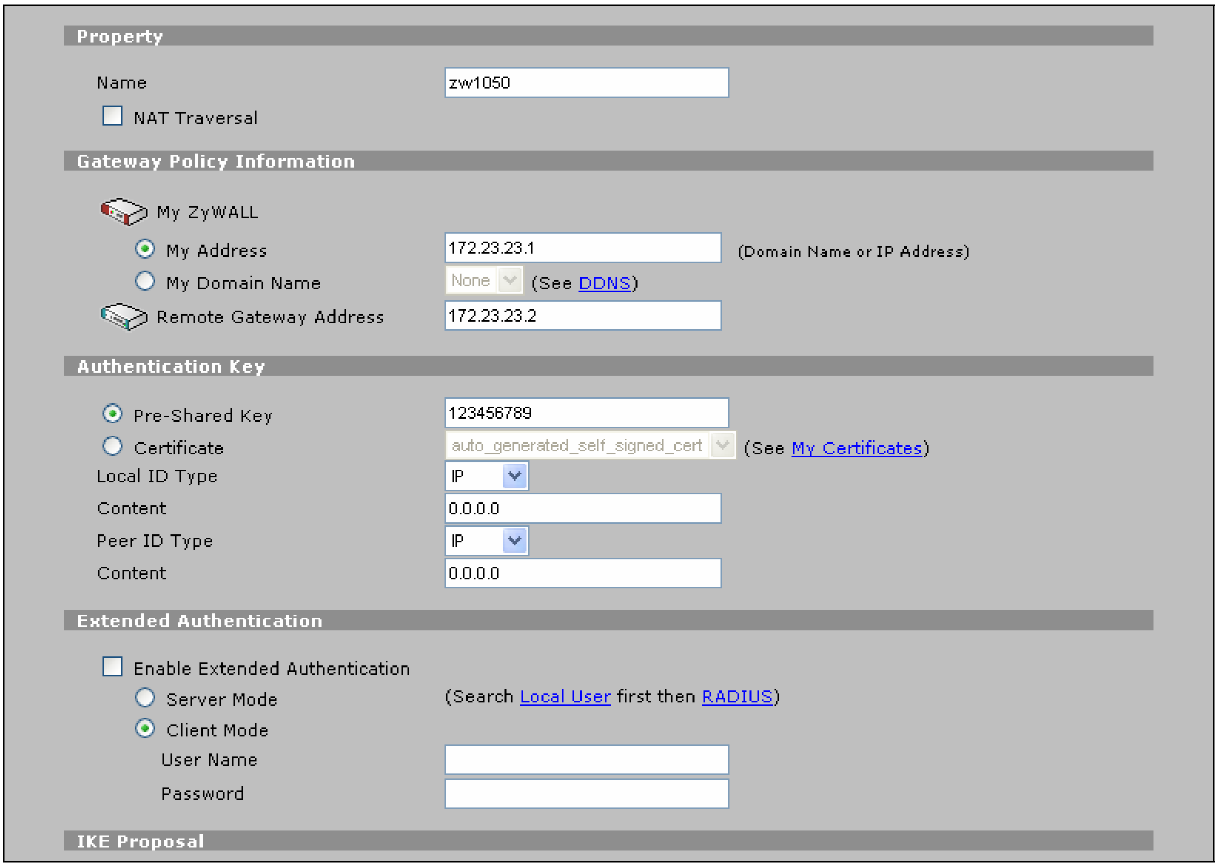
1) Go to the GUI of ZyWALL70 > VPN Global Setting page to configure the VPN rules. The remote subnet range will be 0.0.0.0 to 255.255.255.255. This range also includes ZyWALL70's local network 192.168.1.0. Thus, we have to activate the option of VPN rules skip applying to the overlap range of local and remote IP addresses. The ZyWALL70 management IP 192.168.1.1 and other internal subnet resources will become unreachable if the user forgot to activate this option.



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)

**2)** Go to **Security** >**VPN** to set the IKE rules. We put 172.23.23.1 as **My Address,** 172.23.23.2 as the **Remote Gateway** address and 123456789 as the **Pre-Shared Key.** For other parameters, we set them to match those set in the ZyWALL1050 A.



**Property**

| | |
|---|---|
| Name | zw1050 |
| □ NAT Traversal | |

**Gateway Policy Information**

| | | |
|---|---|---|
| My ZyWALL | | |
| ● My Address | 172.23.23.1 | (Domain Name or IP Address) |
| ○ My Domain Name | None | (See DDNS) |
| Remote Gateway Address | 172.23.23.2 | |

**Authentication Key**

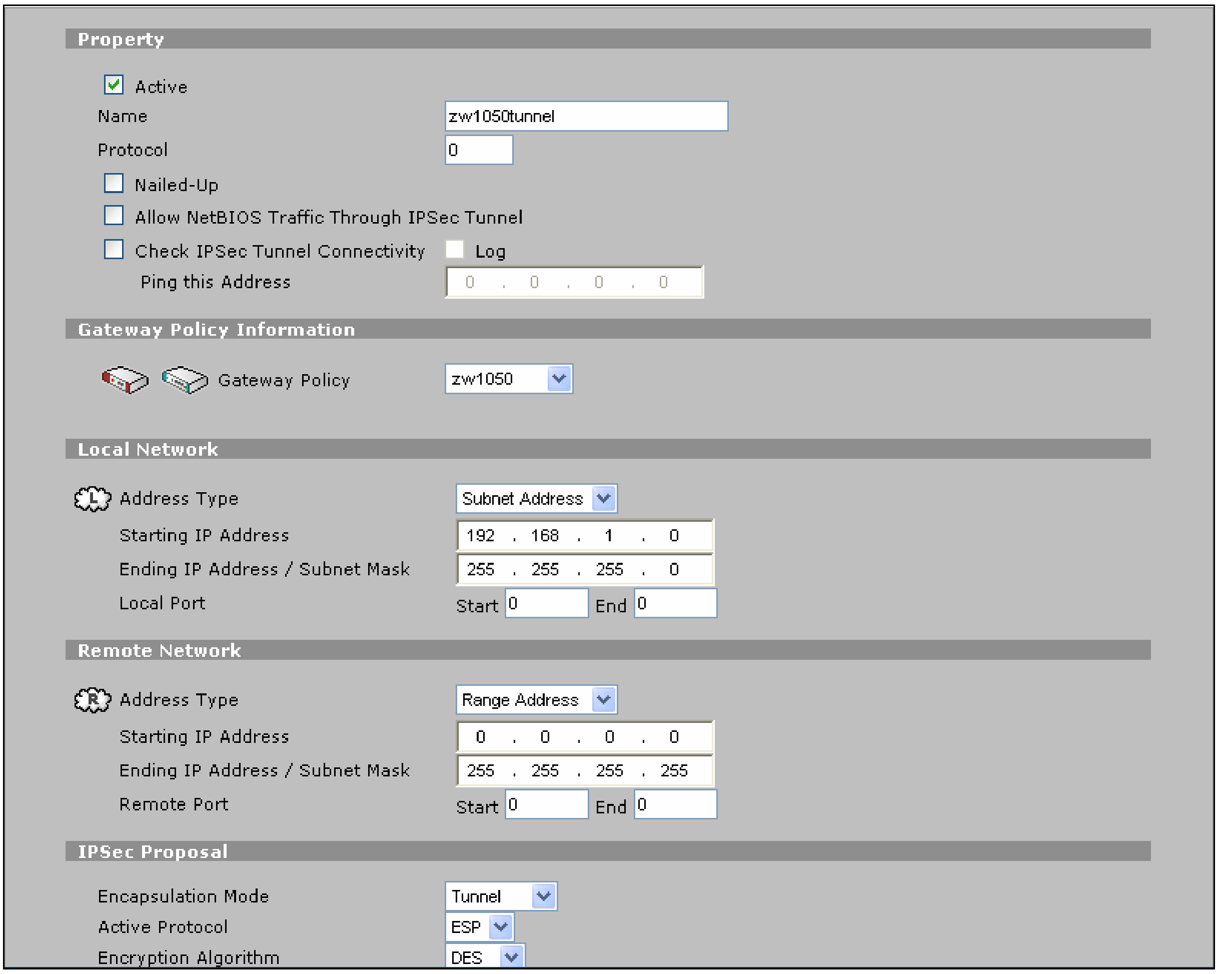
| | | |
|---|---|---|
| ● Pre-Shared Key | 123456789 | |
| ○ Certificate | auto_generated_self_signed_cert | (See My Certificates) |
| Local ID Type | IP | |
| Content | 0.0.0.0 | |
| Peer ID Type | IP | |
| Content | 0.0.0.0 | |

**Extended Authentication**

| | |
|---|---|
| □ Enable Extended Authentication | |
| ○ Server Mode | (Search Local User first then RADIUS) |
| ● Client Mode | |
| User Name | |
| Password | |

**IKE Proposal**

Go to the **Associated Network Policies** of this rule to configure the IPSec rule. Please note that the Remote Network should be within 0.0.0.0-255.255.255.255 range.



**Property**

☑ Active

Name: zw1050tunnel

Protocol: 0

□ Nailed-Up

□ Allow NetBIOS Traffic Through IPSec Tunnel

□ Check IPSec Tunnel Connectivity □ Log

Ping this Address: 0 . 0 . 0 . 0

**Gateway Policy Information**

Gateway Policy: zw1050

**Local Network**

Address Type: Subnet Address

Starting IP Address: 192 . 168 . 1 . 0

Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Local Port: Start 0 End 0

**Remote Network**

Address Type: Range Address

Starting IP Address: 0 . 0 . 0 . 0

Ending IP Address / Subnet Mask: 255 . 255 . 255 . 255

Remote Port: Start 0 End 0

**IPSec Proposal**

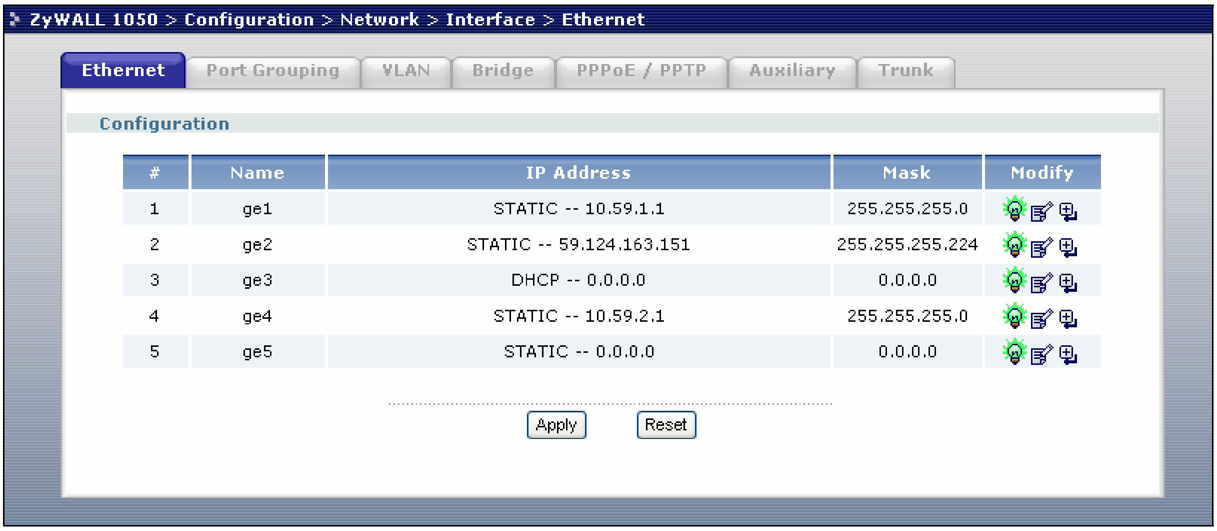
Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

## ZyWALL1050 B configuration

1) Login the ZyWALL1050 A GUI and go to **Configuration** > **Network** > **Interface** > **Ethernet** and configure the IP settings as shown in the topology.



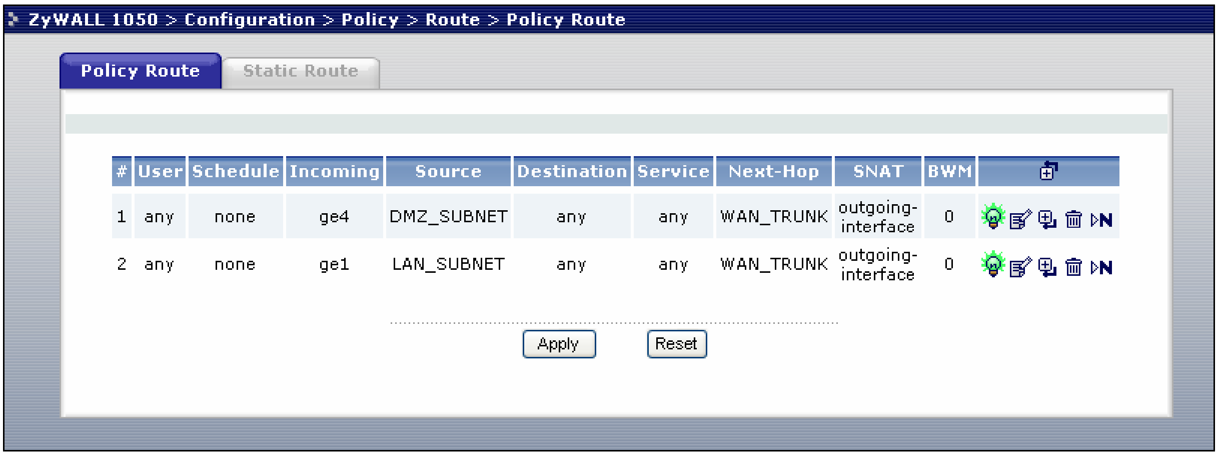
ZyWALL 1050 > Configuration > Network > Interface > Ethernet

Configuration

| # | Name | IP Address | Mask | Modify |
|---|---|---|---|---|
| 1 | ge1 | STATIC -- 10.59.1.1 | 255.255.255.0 | |
| 2 | ge2 | STATIC -- 59.124.163.151 | 255.255.255.224 | |
| 3 | ge3 | DHCP -- 0.0.0.0 | 0.0.0.0 | |
| 4 | ge4 | STATIC -- 10.59.2.1 | 255.255.255.0 | |
| 5 | ge5 | STATIC -- 0.0.0.0 | 0.0.0.0 | |

2) We have to add one more policy route for the traffic from DMZ (ge4) to internet

(WAN_TRUNK).



| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM |
|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | ge4 | DMZ_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 0 |
| 2 | any | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 0 |

After we finish the setting in ZyWALL 70 and ZyWALL 1050 A and B, the setup is complete.

The CLI commands for application:

Policy Route:

```
[0] policy 1
[1] no deactivate
[2] no description
[3] no user
[4] interface ge4
[5] source DMZ_SUBNET
[6] destination any
[7] no schedule
[8] service any
[9] next-hop trunk WAN_TRUNK
[10] snat outgoing-interface
[11] no bandwidth
[12] exit
```

**Tips for application:**

1. Make sure the **Pre-Shared Key** is the same in both local and remote gateways.
2. Make sure the **IKE proposal** is the same in both local and remote gateways.
3. Select the correct **Interface** for VPN connection on ZyWALL1050.
4. The **Local** and the **Peer ID type** and content must the opposite and not of the same content.
5. The **Local Policy** of ZyWALL 1050 should be within the range of 0.0.0.0-255.255.255.255. Then it can take the role of a central controller of all the outgoing traffic from a branch.

# 1.6 Multiple Entry Point (MEP)

To ensure high reliability and high availability of Headquarters' network access for branch office or teleworker, ZyWALL 1050 supports multiple entry points application to bring the following benefits:

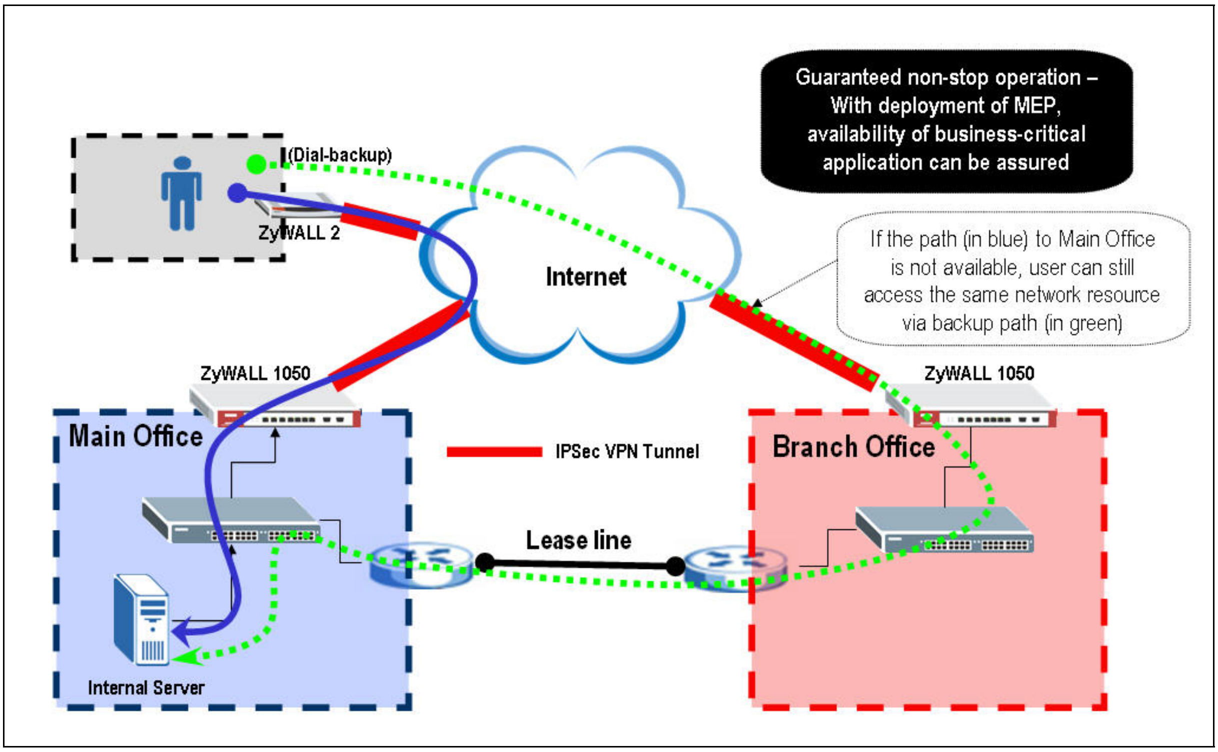
1. Ensuring the network path is always available － if the use of the primary network path fails, user can access the same resources via a backup path
2. Easy to maintain － does not require complex configuration
3. Affordable － does not require investments in excessive/expensive equipment

There are some perquisites for using ZyWALL1050:

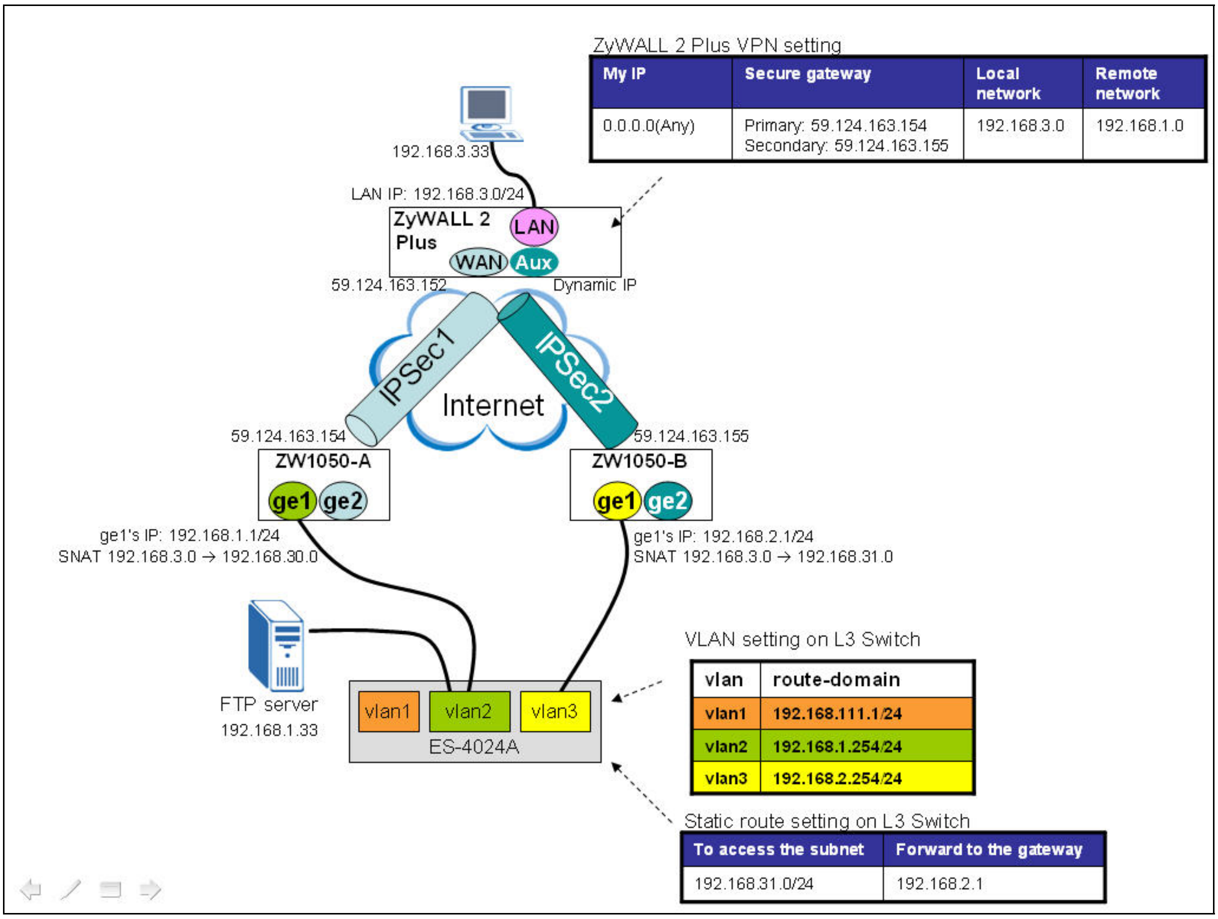
1. Remote VPN gateway must support redundant VPN gateway (VPN HA)
2. Routing mechanism must be well-designed to prevent asymmetric routing from happening in the Intranet

## 1.6.1 Deploying MEP

Assume a teleworker is out of office and needs to access the internal server in the main office. In case the primary WAN access is unavailable, he configures a secondary secure gateway to access the server through another branch office which has a lease line to connect to the main office.


Guaranteed non-stop operation – With deployment of MEP, availability of business-critical application can be assured
(Dial-backup)
ZyWALL 2
Internet
If the path (in blue) to Main Office is not available, user can still access the same network resource via backup path (in green)
ZyWALL 1050
ZyWALL 1050
Main Office
IPSec VPN Tunnel
Branch Office
Lease line
Internal Server

Here, we simulate the topology as on the following picture. It shows a simple use of ZyWALL 2 Plus which supports VPN HA and Dial Backup functions. When the primary WAN access to the VPN tunnel is down, ZyWALL1050 will trigger the dialup backup and establish a VPN tunnel with second secure gateway of another ZyWALL1050 located at the branch office.



ZyWALL 2 Plus VPN setting

| My IP | Secure gateway | Local network | Remote network |
|---|---|---|---|
| 0.0.0.0(Any) | Primary: 59.124.163.154<br>Secondary: 59.124.163.155 | 192.168.3.0 | 192.168.1.0 |

VLAN setting on L3 Switch

| vlan | route-domain |
|---|---|
| vlan1 | 192.168.111.1/24 |
| vlan2 | 192.168.1.254/24 |
| vlan3 | 192.168.2.254/24 |

Static route setting on L3 Switch

| To access the subnet | Forward to the gateway |
|---|---|
| 192.168.31.0/24 | 192.168.2.1 |

For this scenario, we need the following devices:

- One ZyWALL 2 Plus
- Two ZyWALL 1050
- One ES-4024A
- One modem connecting to ZyWALL 2 Plus's AUX port (ex. ZyXEL omni.lite com+)
- One FTP server
- One PC behind ZyWALL 2 Plus

Now, we are going to complete the following main tasks:

1. Configure Dynamic VPN setting with SNAT on ZyWALL 1050_A
2. Configure Dynamic VPN setting with SNAT on ZyWALL 1050_B
3. Configure the VPN setting corresponding with VPN HA on ZyWALL 2 Plus and enable ping check to detect the whether the WAN connection is down so that the switch can dial backup connection immediately.
4. Configure VLAN setting on ES-4024A. And once the PC is able to access the FTP server through the second VPN tunnel, an static route on ES-4024A is required to direct the

traffic to go back through the original path(FTP server → ES-4024A → ZyWALL 1050-B → ZyWALL 2 Plus → PC).

5. Test either when primary or secondary VPN tunnel is on, the PC behind ZyWALL 2 Plus should be able to reach the FTP server by ping.

The IP addresses and configuration of the VPN setting on the three devices are as shown below.

| | Main office<br>ZyWALL 1050-A | ZyWALL 2 Plus | Branch office<br>ZyWALL 1050-B |
|---|---|---|---|
| My Address | ge2, 59.124.163.154 | 0.0.0.0 | ge2, 59.124.163.155 |
| Security Gateway Address | 0.0.0.0 | Primary: 59.124.163.154<br>Secondary: 59.124.163.155<br>Fail back check: Enable<br>Fail back check Interval: 180sec | 0.0.0.0 |
| Local ID Type | IP, 0.0.0.0 | IP, 0.0.0.0 | IP, 0.0.0.0 |
| Peer ID Type | Any | IP, 0.0.0.0 | Any |
| Local | Subnet, 192.168.1.0 | Subnet, 192.168.3.0 | Subnet, 192.168.2.0 |
| Remote | Subnet, 192.168.3.0 | Subnet, 192.168.1.0 | Subnet, 192.168.3.0 |
| SNAT | Change<br>192.168.3.0 →<br>192.168.1.0<br>to<br>192.168.30.0 →<br>192.168.1.0 | N/A | Change<br>192.168.3.0 →<br>192.168.1.0<br>to<br>192.168.31.0 →<br>192.168.1.0 |
| Phase1 | | | |
| Negotiation Mode | Main | Main | Main |
| Pre-share key | 123456789 | 123456789 | 123456789 |
| Encryption | DES | DES | DES |
| Authentication | MD5 | MD5 | MD5 |
| Key Group | DH1 | DH1 | DH1 |
| Phase2 | | | |

| | | | |
|---|---|---|---|
| Encapsulation | Tunnel | Tunnel | Tunnel |
| Active Protocol | ESP | ESP | ESP |
| Encryption | DES | DES | DES |
| Authentication | SHA1 | SHA1 | SHA1 |
| PFS | NONE | NONE | NONE |

See the following step-by-step configuration:

### *1. Configuration on ZyWALL 1050-A*

**(1) LAN/WAN Network Setting**

Login ZyWALL 1050-A's GUI, go to menu **Configuration** > **Network** > **Interface**. Modify ge2's IP address to 59.124.163.154 with subnet 255.255.255.224 and gateway 59.124.163.129. Secondly, modify interface "ge1" to be as LAN network. Here we keep to use the default IP address "192.168.1.0" with subnet 255.255.255.0. Moreover, configure the DHCP setting as a DHCP server with the IP poor starting address, pool size accordingly and the proper DNS server IP address which will apply to LAN PCs automatically. (By default, the "first DNS server" is configured as "from ISP". Since we configure the static IP address for ge2(WAN), it won't automatically get any DNS setting from ISP. So we have to change it to "Custom Defined" and enter a proper DNS server's IP address.)

**(2). Dynamic VPN Setting with SNAT**

Step1. Create Address Objects for further configuration

1. Go to menu **Configuration** > **Network** > **Object** > **Address**
2. Create one address for the local VPN network by clicking '+' icon
    Name: Local_192_168_1
    Subnet, 192.168.1.0/255.255.255.0
3. Create another one for the remote VPN network
    Name: Remote_192_168_3
    Subnet, 192.168.3.0/255.255.255.0
4. Create another one for the network behind ZyWALL1050-A performing SNAT
    Name: Local_192_168_30
    Subnet, 192.168.30.0/255.255.255.0

5. Create another one for the network for traffic which wants to go to the branch office's subnet, that is ZyWALL1050-B's LAN site.

Name: Local_192_168_31

Subnet, 192.168.31.0/255.255.255.0

6. Create another one for dynamic remote network.

Name: Remote_ANY

Subnet, 0.0.0.0/0.0.0.0

7. Create another one for the IP domain interface on ES-4024A's VLAN2.

Name: HOST_192_168_1_254

Host, 192.168.1.254/255.255.255.255

8. Create another one to indicate ZyWALL 2 Plus's WAN IP address for the Firewall rule usage which will allow the pingcheck traffic of ZyWALL 2 Plus can ping ZyWALL 1050-A's ge2(WAN) interface.

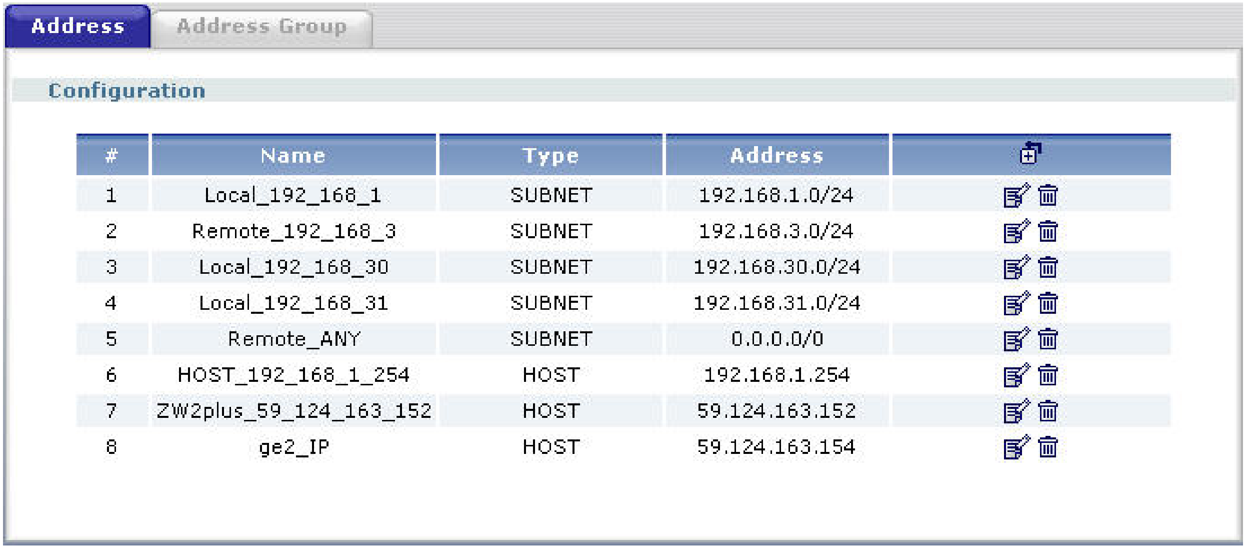
Name: ZW2plus_59_124_163_152

Host, 59.124.163.152/255.255.255.255

9. Create one more still to indicate ZyWALL 1050-A's ge2(WAN) IP address for Firewall rule usage which will allow ZyWALL 1050-A's ge2 to be ping from ZyWALL 2 plus and also can response to the ping.

Name: ge2_IP

Host, 59.124.163.154/255.255.255.255



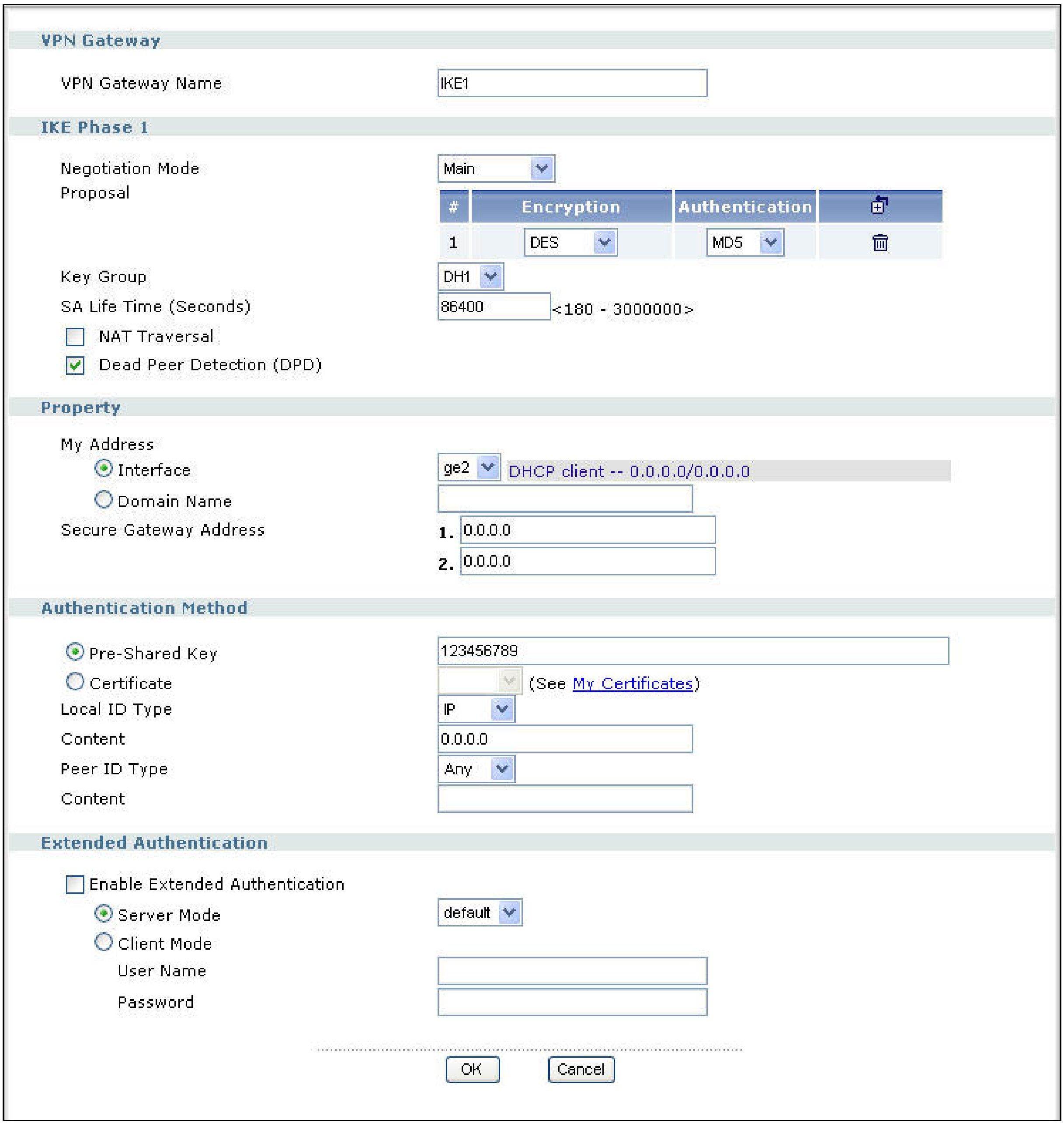
| # | Name | Type | Address | |
|---|---|---|---|---|
| 1 | Local_192_168_1 | SUBNET | 192.168.1.0/24 | |
| 2 | Remote_192_168_3 | SUBNET | 192.168.3.0/24 | |
| 3 | Local_192_168_30 | SUBNET | 192.168.30.0/24 | |
| 4 | Local_192_168_31 | SUBNET | 192.168.31.0/24 | |
| 5 | Remote_ANY | SUBNET | 0.0.0.0/0 | |
| 6 | HOST_192_168_1_254 | HOST | 192.168.1.254 | |
| 7 | ZW2plus_59_124_163_152 | HOST | 59.124.163.152 | |
| 8 | ge2_IP | HOST | 59.124.163.154 | |

CLI command for reference:

```
[0] address-object Local_192_168_1 192.168.1.0 255.255.255.0
[1] address-object Remote_192_168_3 192.168.3.0 255.255.255.0
[2] address-object Local_192_168_30 192.168.30.0 255.255.255.0
[3] address-object Local_192_168_31 192.168.31.0 255.255.255.0
[4] address-object Remote_ANY 0.0.0.0 0.0.0.0
[5] address-object HOST_192_168_1_254 192.168.1.254
255.255.255.255
[6] address-object ZW2plus_59_124_163_152 59.124.163.152
255.255.255.255
[7] address-object ge2_IP 59.124.163.154 255.255.255.255
```

Step2. Create an IKE rule

1. Go to menu **Configuration** > **Network** > **IPSec VPN**, switch to '**VPN Gateway**'
2. Create a new IKE by clicking '+' icon
3. Fill out the fields as following.



**VPN Gateway**

| | |
|---|---|
| VPN Gateway Name | IKE1 |

**IKE Phase 1**

| | |
|---|---|
| Negotiation Mode | Main |
| Proposal | |

| # | Encryption | Authentication | |
|---|---|---|---|
| 1 | DES | MD5 | |

| | |
|---|---|
| Key Group | DH1 |
| SA Life Time (Seconds) | 86400 <180 - 3000000> |
| □ NAT Traversal | |
| ☑ Dead Peer Detection (DPD) | |

**Property**

| | |
|---|---|
| My Address | |
| ● Interface | ge2 DHCP client -- 0.0.0.0/0.0.0.0 |
| ○ Domain Name | |
| Secure Gateway Address | 1. 0.0.0.0 |
| | 2. 0.0.0.0 |

**Authentication Method**

| | |
|---|---|
| ● Pre-Shared Key | 123456789 |
| ○ Certificate | (See My Certificates) |
| Local ID Type | IP |
| Content | 0.0.0.0 |
| Peer ID Type | Any |
| Content | |

**Extended Authentication**

| | |
|---|---|
| □ Enable Extended Authentication | |
| ● Server Mode | default |
| ○ Client Mode | |
| User Name | |
| Password | |

CLI commands for reference:

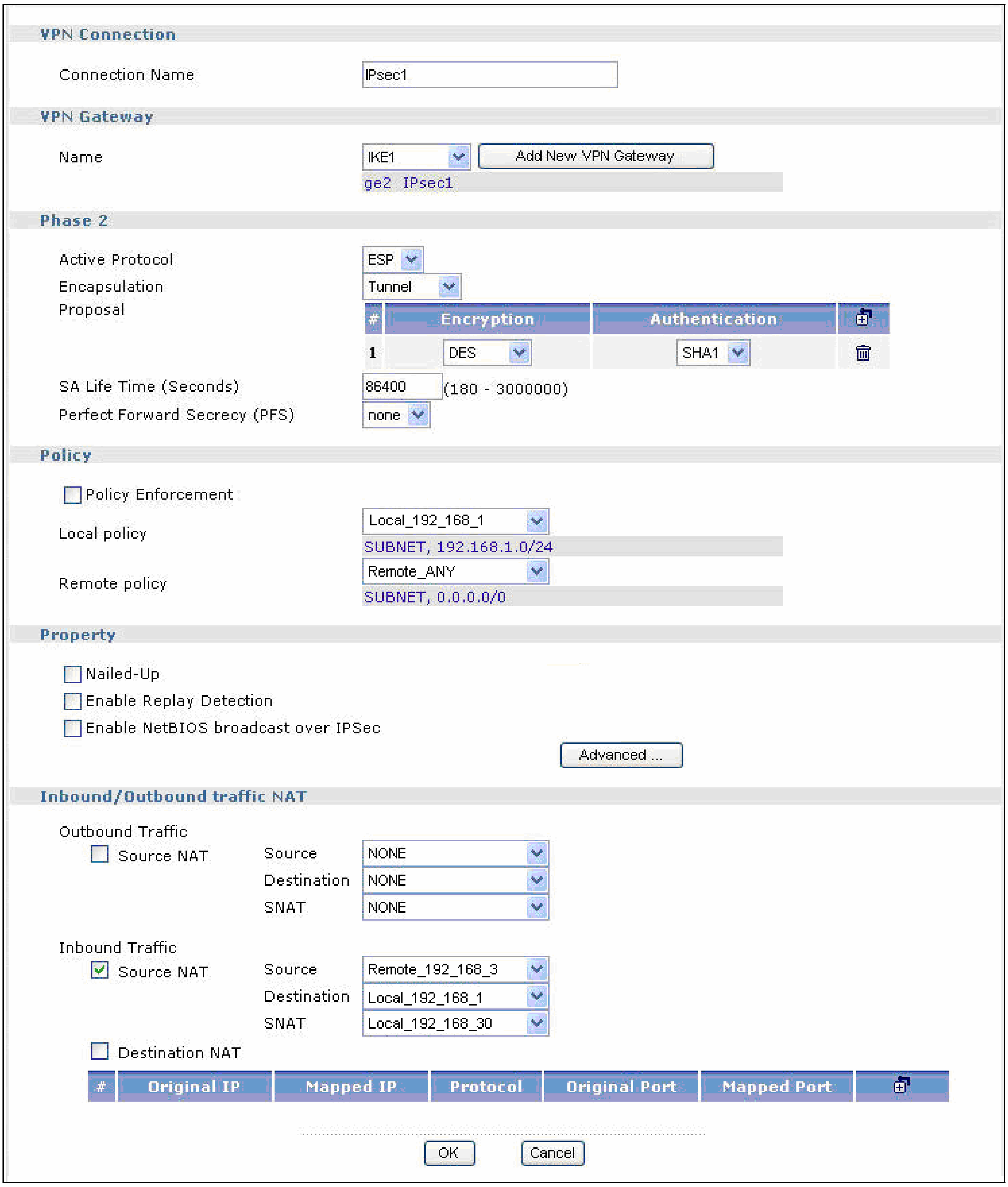
```
[0] isakmp policy IKE1
[1] mode main
[2] transform-set des-md5
[3] lifetime 86400
[4] no natt
[5] dpd
[6] local-ip interface ge2
[7] peer-ip 0.0.0.0 0.0.0.0
```

```
[8] authentication pre-share
[9] keystring 123456789
[10] local-id type ip 0.0.0.0
[11] peer-id type any
[12] xauth type server default deactivate
[13] group1
```

---

Step3. Configure the IPSec rule

1. Go to menu **Configuration** > **Network** > **IPSec VPN**, switch to '**VPN Connection**'
2. Create a new IPSec by clicking '+' icon
3. Configure the VPN setting as shown below.



VPN Connection

| | |
|---|---|
| Connection Name | IPsec1 |

VPN Gateway

| | |
|---|---|
| Name | IKE1 |
| | ge2 IPsec1 |

Phase 2

| | |
|---|---|
| Active Protocol | ESP |
| Encapsulation | Tunnel |

Proposal

| # | Encryption | Authentication | |
|---|---|---|---|
| 1 | DES | SHA1 | |

| | |
|---|---|
| SA Life Time (Seconds) | 86400 (180 - 3000000) |
| Perfect Forward Secrecy (PFS) | none |

Policy

□ Policy Enforcement

| | |
|---|---|
| Local policy | Local_192_168_1 |
| | SUBNET, 192.168.1.0/24 |
| Remote policy | Remote_ANY |
| | SUBNET, 0.0.0.0/0 |

Property

□ Nailed-Up
□ Enable Replay Detection
□ Enable NetBIOS broadcast over IPSec

Inbound/Outbound traffic NAT

Outbound Traffic

| | | |
|---|---|---|
| □ Source NAT | Source | NONE |
| | Destination | NONE |
| | SNAT | NONE |

Inbound Traffic

| | | |
|---|---|---|
| ☑ Source NAT | Source | Remote_192_168_3 |
| | Destination | Local_192_168_1 |
| | SNAT | Local_192_168_30 |

□ Destination NAT

| # | Original IP | Mapped IP | Protocol | Original Port | Mapped Port | |
|---|---|---|---|---|---|---|

***Note:*** In ZyWALL 1050-A, we use “Source NAT” to change the VPN traffic from 192.168.3.0 network which will go to 192.168.1.0 network to 192.168.30.0 network. And we will also configure ZyWALL 1050-B to change the VPN traffic from 192.168.3.0 network which will go to 192.168.2.0 network to 192.168.31.0 network later.

CLI commands for reference

```
[0] crypto map IPsec1
[1] ipsec-isakmp IKE1
[2] encapsulation tunnel
[3] transform-set esp-des-sha
[4] set security-association lifetime seconds 86400
[5] set pfs none
[6] no policy-enforcement
[7] local-policy Local_192_168_1
[8] remote-policy Remote_ANY
[9] no nail-up
[10] no replay-detection
[11] no netbios-broadcast
[12] no out-snat activate
[13] in-snat activate
[14] in-snat source Remote_192_168_3 destination Local_192_168_1
snat Local_192_168_30
[15] no in-dnat activate
```

---

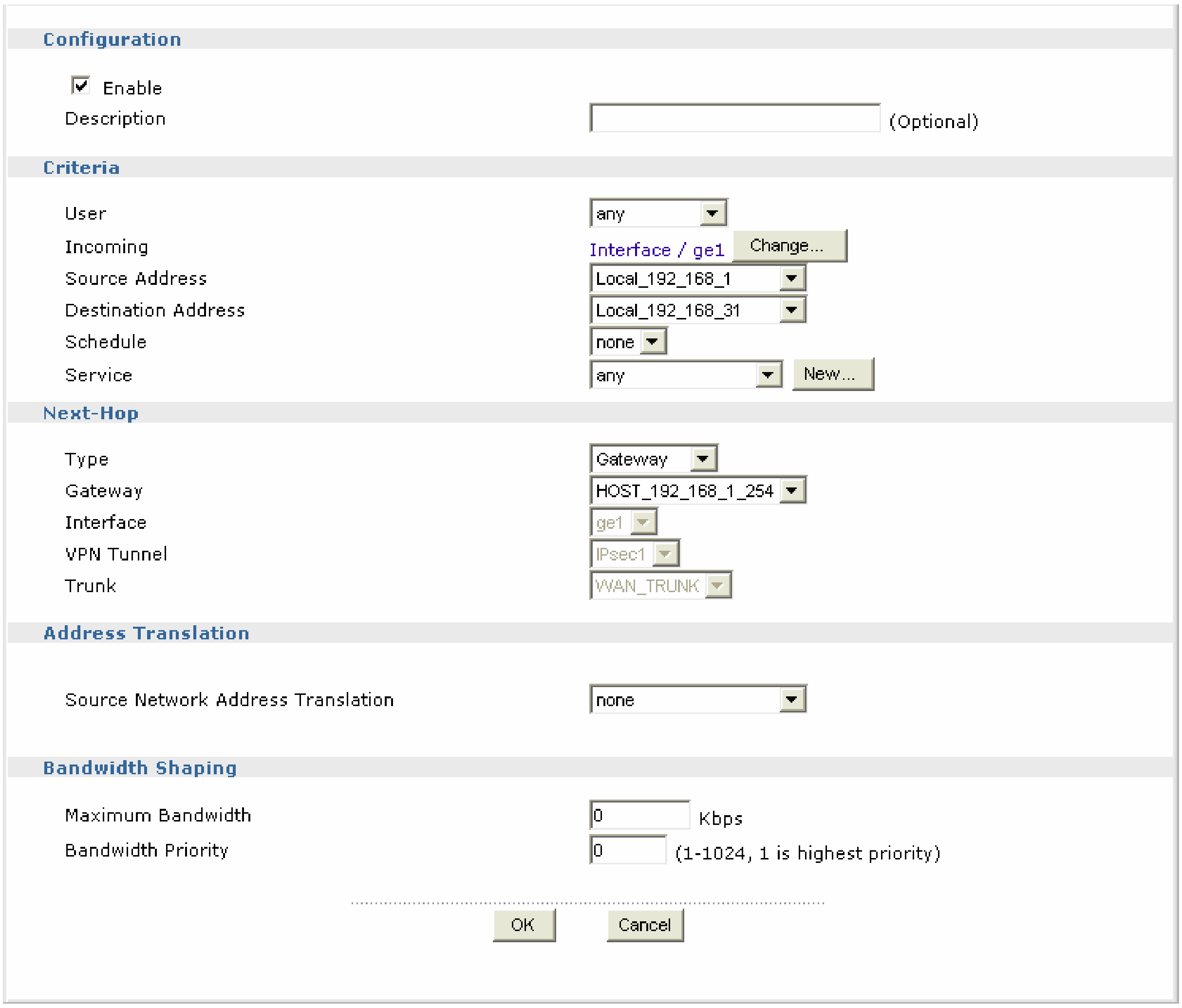
**(3) Add a policy route**

**1.** Go to GUI menu **Configuration** > **Policy** > **Route > Policy Route** tab

**2.** By default, there is one policy route already to indicate all packets which is sent from LAN to any network will be passed through WAN_TRUNK. This is also to direct IKE packet to WAN and trigger the VPN tunnel then.

**3.** Click the '+' icon to add another new policy route which will be used to route traffic from ZyWALL 1050-B to return via original path.

4. Define that all the traffic from 192.168.1.0 network that wants to go to 192.168.31.0 routed by the gateway, the host of 192.168.1.254. The configuration is as shown below.



**Configuration**

| | |
|---|---|
| ☑ Enable | |
| Description | (Optional) |

**Criteria**

| | |
|---|---|
| User | any |
| Incoming | Interface / ge1 Change... |
| Source Address | Local_192_168_1 |
| Destination Address | Local_192_168_31 |
| Schedule | none |
| Service | any New... |

**Next-Hop**

| | |
|---|---|
| Type | Gateway |
| Gateway | HOST_192_168_1_254 |
| Interface | ge1 |
| VPN Tunnel | IPsec1 |
| Trunk | WAN_TRUNK |

**Address Translation**

| | |
|---|---|
| Source Network Address Translation | none |

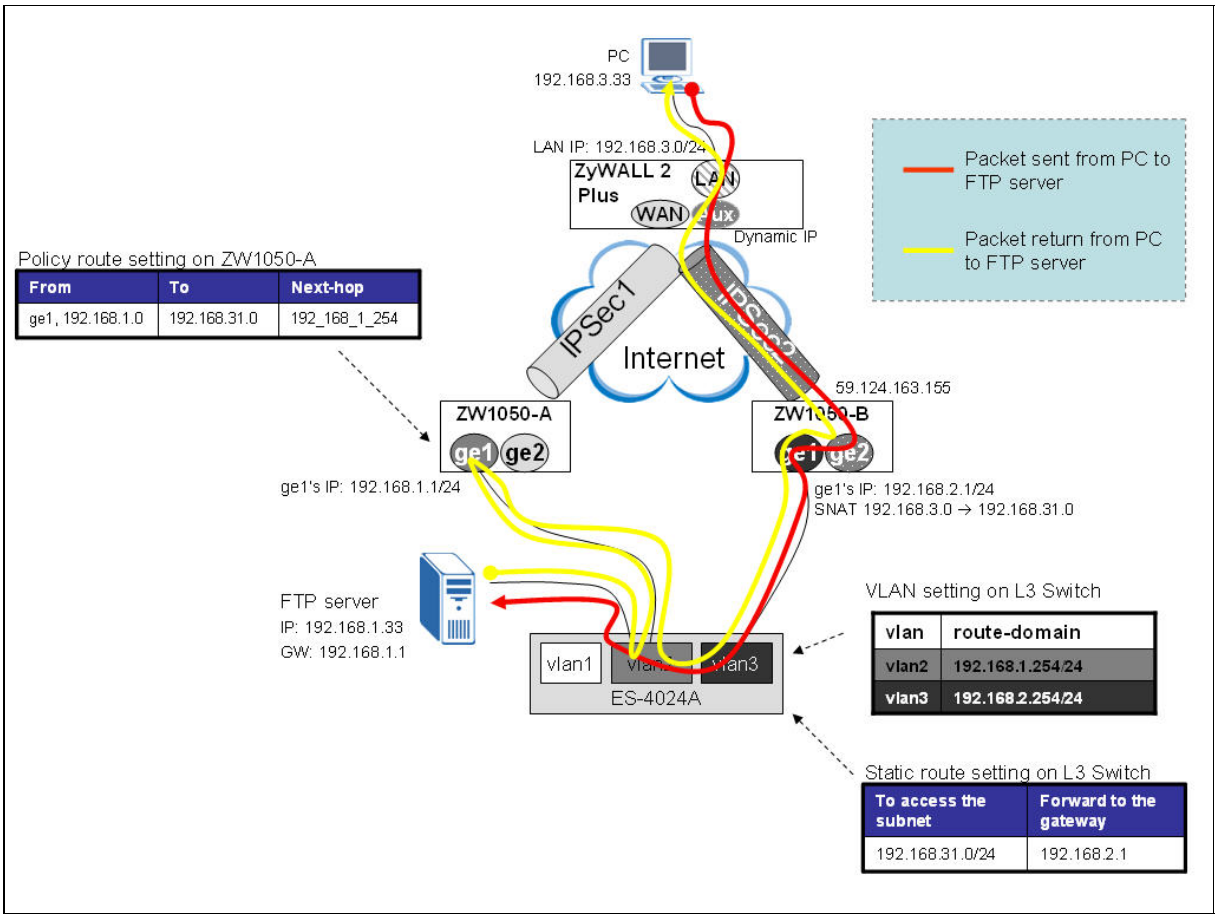
**Bandwidth Shaping**

| | |
|---|---|
| Maximum Bandwidth | 0 Kbps |
| Bandwidth Priority | 0 (1-1024, 1 is highest priority) |

**Note**: The purpose of this policy route is to direct the traffic from 192.168.3.0 which is sent through the secondary VPN path to be redirected to 192.168.31.0 network and returned through the original path.

For example, think about when primary VPN tunnel is down, the traffic would go from PC → ZyWALL 2 Plus → ZyWALL 1050-B (change source IP to 192.168.31.0) → ES-4024A → to FTP server (now the packet is with source 192.168.31.0 to destination 192.168.1.33).

The FTP server's gateway is ZyWALL 1050-A's ge2 applied via DHCP or manually configured. So when traffic would return, it will be flowed from FTP server →ZyWALL 1050-A's ge2 (which will redirect the traffic to another host ) →192.168.1.254 (which is ES-4024A's VLAN3 route-domain IP address) → ZyWALL1050-B → ZyWALL 2 Plus → to the PC behind ZyWALL 2 Plus.



Policy route setting on ZW1050-A

| From | To | Next-hop |
|---|---|---|
| ge1, 192.168.1.0 | 192.168.31.0 | 192_168_1_254 |

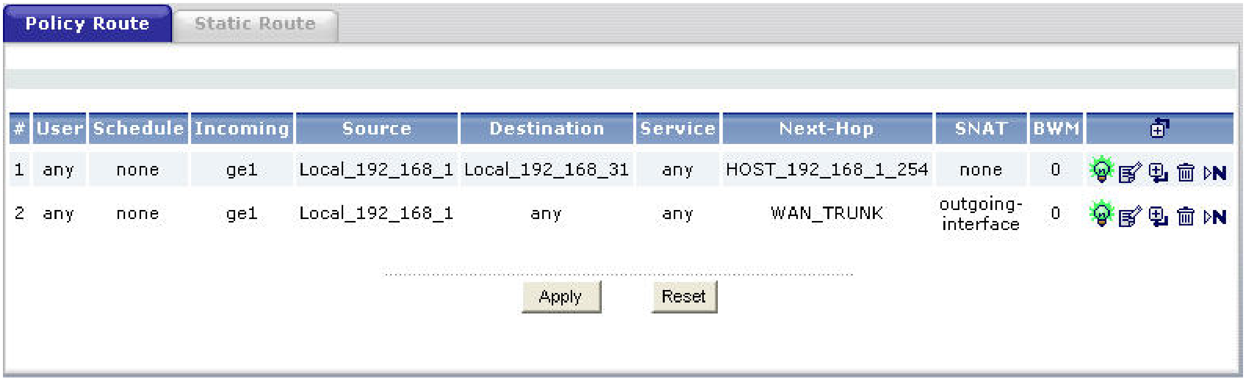
VLAN setting on L3 Switch

| vlan | route-domain |
|---|---|
| vlan2 | 192.168.1.254/24 |
| vlan3 | 192.168.2.254/24 |

Static route setting on L3 Switch

| To access the subnet | Forward to the gateway |
|---|---|
| 192.168.31.0/24 | 192.168.2.1 |

After the configuration is down, you will see two policy routes as shown below.



| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | ge1 | Local_192_168_1 | Local_192_168_31 | any | HOST_192_168_1_254 | none | 0 | |
| 2 | any | none | ge1 | Local_192_168_1 | any | any | WAN_TRUNK | outgoing-interface | 0 | |

CLI commands for reference:

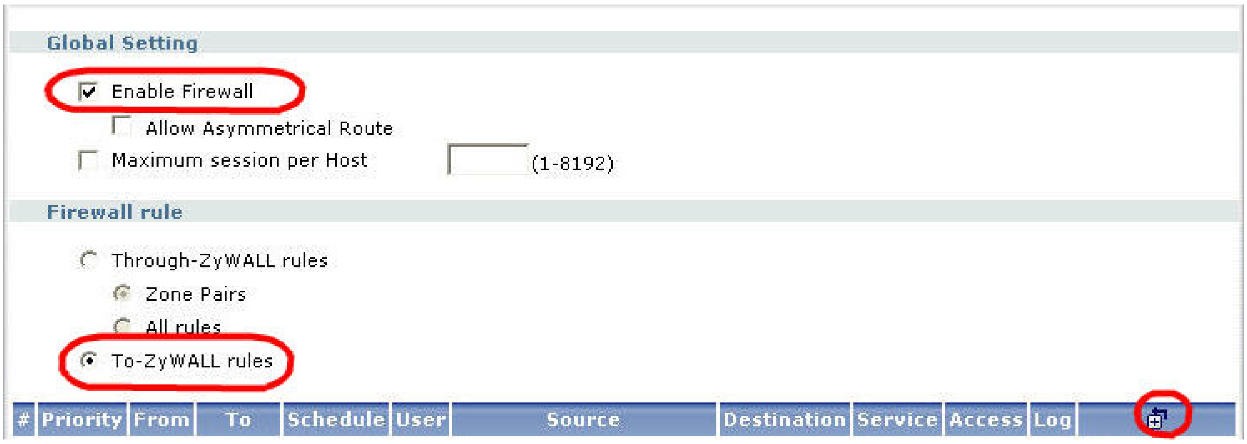
```
[0] policy 1
[1] no deactivate
[2] no description
[3] no user
[4] interface ge1
```

```
[5] source Local_192_168_1
[6] destination Local_192_168_31
[7] no schedule
[8] service any
[9] next-hop gateway HOST_192_168_1_254
[10] no snat
[11] no bandwidth
[12] exit
```

---

**(4) Enable Firewall and create one Firewall policy rule for ZyWALL 2 Plus to be able to ping ZyWALL 1050-A's ge2(WAN)**

1. Go to GUI menu **Security** > **Firewall**
2. **Enable Firewall**: On
3. Choose **To-ZyWALL rules** and click "+" at the right site to add a new rule.



Global Setting

☑ Enable Firewall

□ Allow Asymmetrical Route

□ Maximum session per Host [ ] (1-8192)

Firewall rule

○ Through-ZyWALL rules

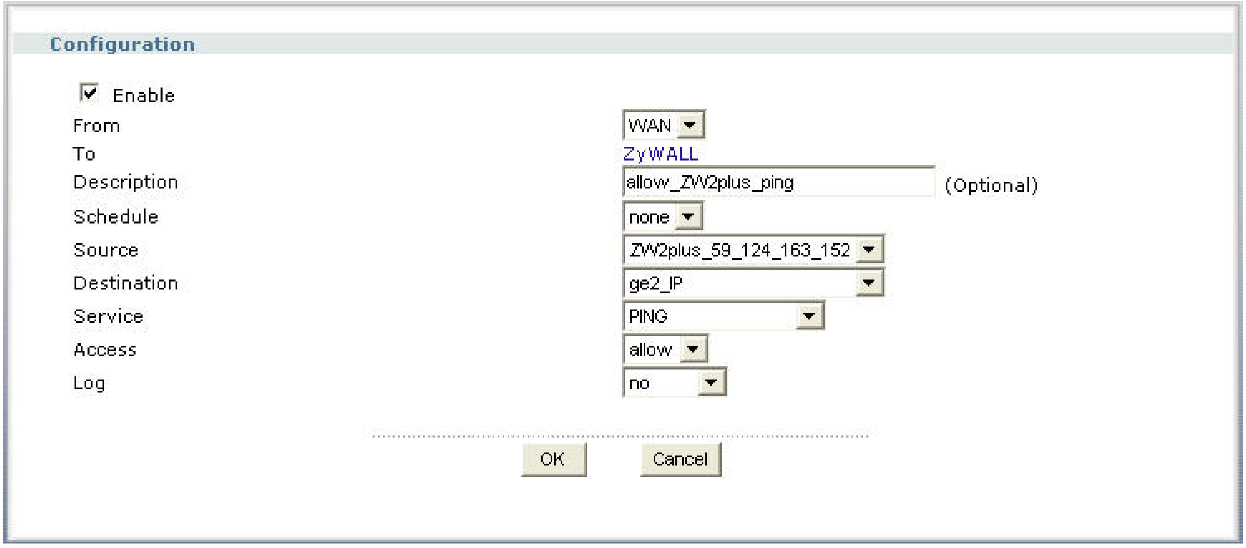
● Zone Pairs

○ All rules

● To-ZyWALL rules

| # | Priority | From | To | Schedule | User | Source | Destination | Service | Access | Log | |
|---|---|---|---|---|---|---|---|---|---|---|---|

4. Fill out the information as following and click "apply" button then.

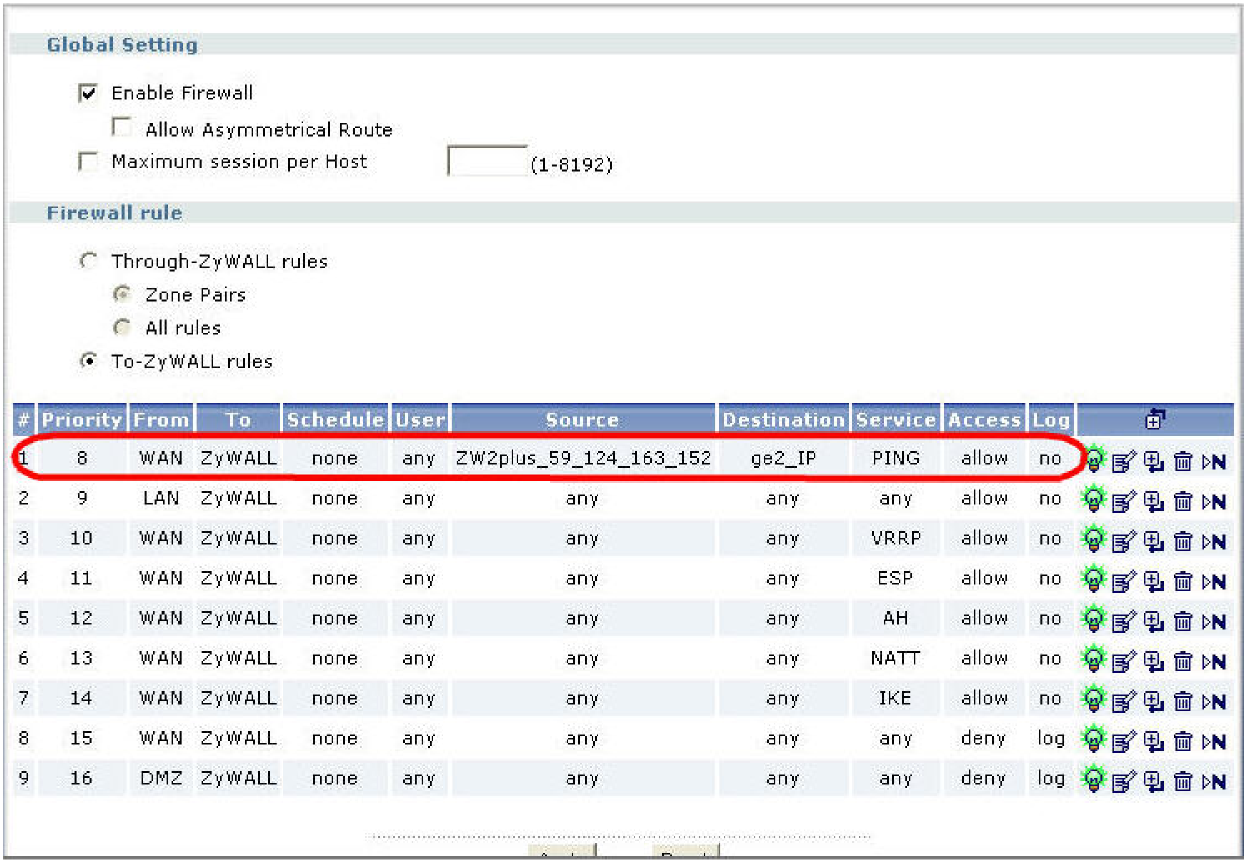


**Configuration**

☑ Enable

| | |
|---|---|
| From | WAN |
| To | ZyWALL |
| Description | allow_ZW2plus_ping (Optional) |
| Schedule | none |
| Source | ZW2plus_59_124_163_152 |
| Destination | ge2_IP |
| Service | PING |
| Access | allow |
| Log | no |

5. The new firewall rule is available as shown below.



**Global Setting**

☑ Enable Firewall

□ Allow Asymmetrical Route

□ Maximum session per Host (1-8192)

**Firewall rule**

○ Through-ZyWALL rules

● Zone Pairs

○ All rules

● To-ZyWALL rules

| # | Priority | From | To | Schedule | User | Source | Destination | Service | Access | Log |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 8 | WAN | ZyWALL | none | any | ZW2plus_59_124_163_152 | ge2_IP | PING | allow | no |
| 2 | 9 | LAN | ZyWALL | none | any | any | any | any | allow | no |
| 3 | 10 | WAN | ZyWALL | none | any | any | any | VRRP | allow | no |
| 4 | 11 | WAN | ZyWALL | none | any | any | any | ESP | allow | no |
| 5 | 12 | WAN | ZyWALL | none | any | any | any | AH | allow | no |
| 6 | 13 | WAN | ZyWALL | none | any | any | any | NATT | allow | no |
| 7 | 14 | WAN | ZyWALL | none | any | any | any | IKE | allow | no |
| 8 | 15 | WAN | ZyWALL | none | any | any | any | any | deny | log |
| 9 | 16 | DMZ | ZyWALL | none | any | any | any | any | deny | log |

### 2. Configuration on ZyWALL 1050-B

**(1). LAN/WAN Network Setting**

Login ZyWALL 1050-A's GUI, go to menu **Configuration** > **Network** > **Interface**. Modify ge2's(WAN) IP address to 59.124.163.155 with subnet 255.255.255.224 and gateway 59.124.163.129. Secondly, modify ge1's(LAN) IP address to 192.168.2.1 with subnet 255.255.255.0 and configure it as a DHCP server with the IP poor starting address and pool size accordingly. Besides, also input the proper DNS server which will apply to LAN PCs automatically. (By default, the first DNS server is configured as "from ISP". Since we configure the static IP address for ge2(WAN), it won't automatically get any DNS setting from ISP. So we have to change it to "Custom Defined" and give it a proper DNS server's IP address.)

**(2). Dynamic VPN Setting with SNAT**

Step1. Create Address Objects for further configuration.

1. Go to menu **Configuration** > **Network** > **Object** > **Address**
2. Create a new address object for local network by clicking '+' icon
   Name: Local_192_168_2
   Subnet, 192.168.2.0/255.255.255.0
3. Create another one for remote network
   Name: Remote_192_168_3
   Subnet, 192.168.3.0/255.255.255.0
4. Create another one for the network behind ZyWALL1050-B performing SNAT
   Name: Local_192_168_31
   Subnet, 192.168.31.0/255.255.255.0
5. Create another one for dynamic remote network.
   Name: Remote_ANY
   Subnet, 0.0.0.0/0.0.0.0
6. Create still one more for the IP domain interface on ES-4024A's VLAN3.
   Name: HOST_192_168_2_254
   Host, 192.168.2.254/255.255.255.255

CLI commands for reference:

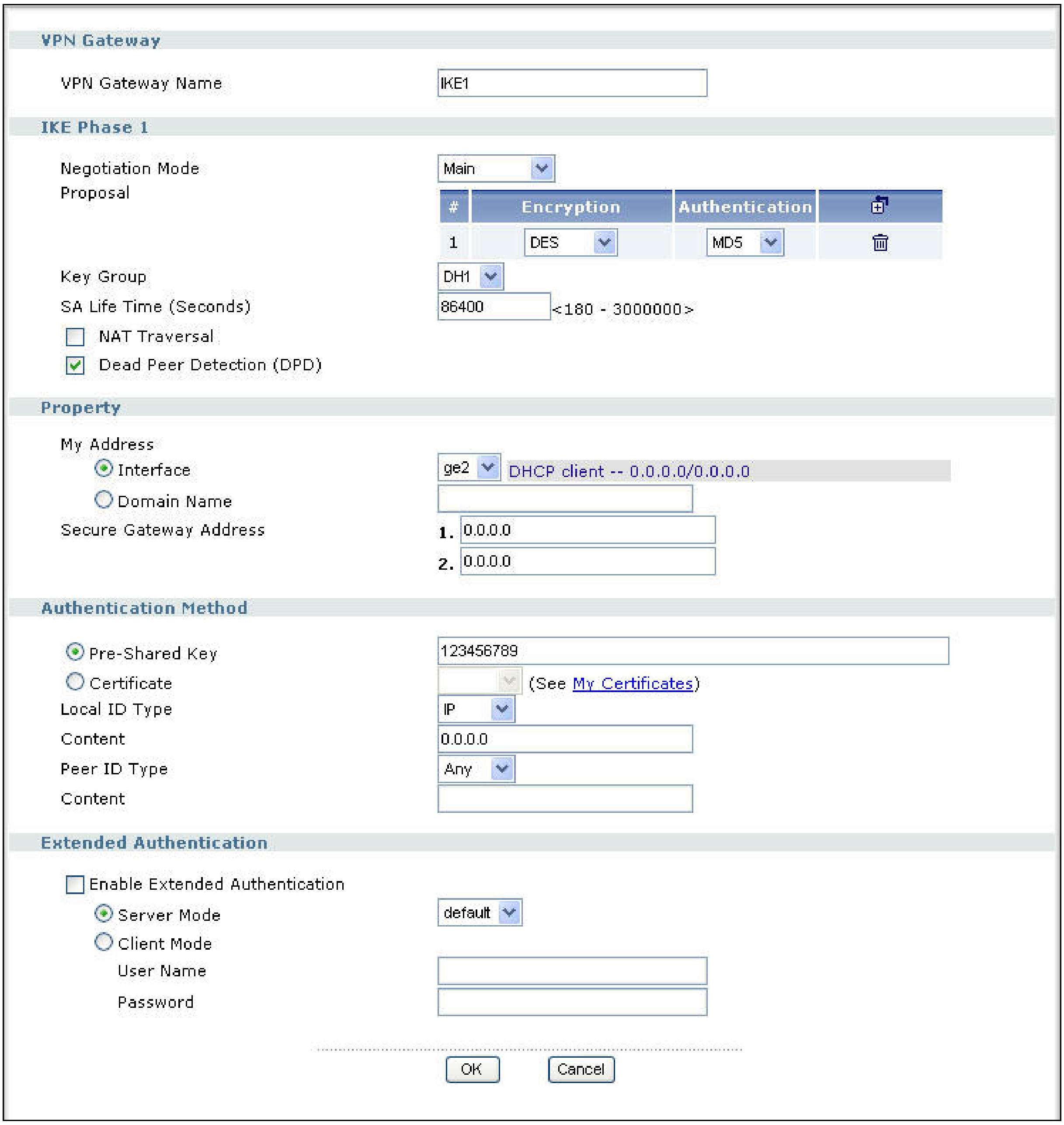
```
[0] address-object Local_192_168_2 192.168.2.0 255.255.255.0
```

```
[1] address-object Remote_192_168_3 192.168.3.0 255.255.255.0
[2] address-object Local_192_168_31 192.168.31.0 255.255.255.0
[3] address-object Remote_ANY 0.0.0.0 0.0.0.0
[4] address-object HOST_192_168_2_254 192.168.2.254
255.255.255.255
```

---

Step2. Create an IKE rule

1. Go to menu **Configuration** > **Network** > **IPSec VPN**, switch to '**VPN Gateway**'
2. Create a new IKE by clicking '+' icon
3. Fill out the fields as following.



**VPN Gateway**

VPN Gateway Name: IKE1

**IKE Phase 1**

Negotiation Mode: Main

Proposal

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | MD5 |

Key Group: DH1

SA Life Time (Seconds): 86400 <180 - 3000000>

□ NAT Traversal

☑ Dead Peer Detection (DPD)

**Property**

My Address

● Interface: ge2 DHCP client -- 0.0.0.0/0.0.0.0

○ Domain Name

Secure Gateway Address: 1. 0.0.0.0 2. 0.0.0.0

**Authentication Method**

● Pre-Shared Key: 123456789

○ Certificate (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: Any

Content:

**Extended Authentication**

□ Enable Extended Authentication

● Server Mode: default

○ Client Mode

User Name

Password

CLI commands for reference:

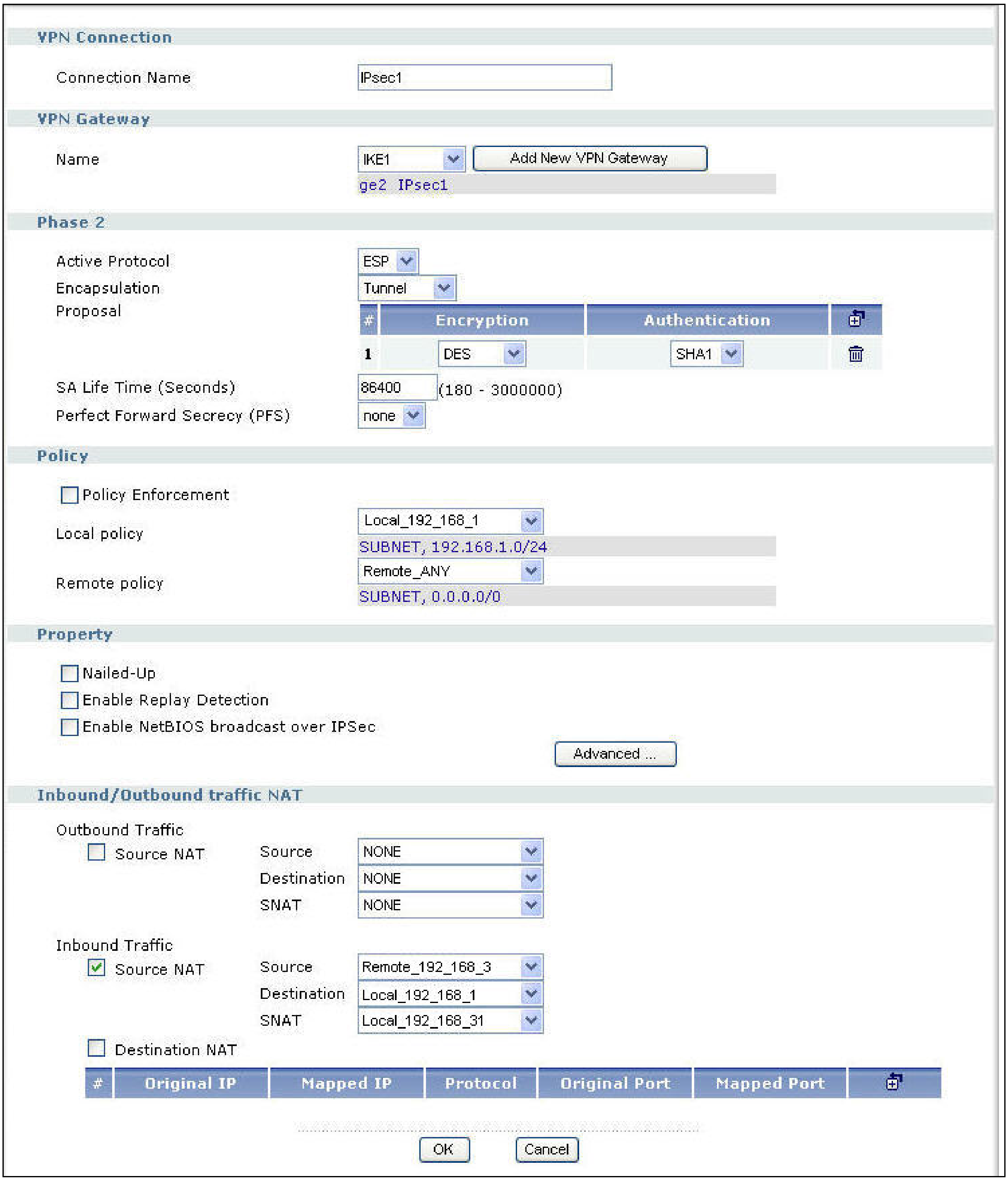
```
[0] isakmp policy IKE1
[1] mode main
[2] transform-set des-md5
[3] lifetime 86400
[4] no natt
[5] dpd
[6] local-ip interface ge2
[7] peer-ip 0.0.0.0 0.0.0.0
```

```
[8] authentication pre-share
[9] keystring 123456789
[10] local-id type ip 0.0.0.0
[11] peer-id type any
[12] xauth type server default deactivate
[13] group1
```

---

Step3. Configure the IPSec rule

1. Go to menu **Configuration** > **Network** > **IPSec VPN**, switch to '**VPN Connection**'
2. Create a new IPSec by click '+' icon
3. Fill out the fields as following



**VPN Connection**

Connection Name: IPsec1

**VPN Gateway**

Name: IKE1 [Add New VPN Gateway]
ge2 IPsec1

**Phase 2**

Active Protocol: ESP
Encapsulation: Tunnel
Proposal:

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | SHA1 |

SA Life Time (Seconds): 86400 (180 - 3000000)
Perfect Forward Secrecy (PFS): none

**Policy**

□ Policy Enforcement
Local policy: Local_192_168_1
SUBNET, 192.168.1.0/24
Remote policy: Remote_ANY
SUBNET, 0.0.0.0/0

**Property**

□ Nailed-Up
□ Enable Replay Detection
□ Enable NetBIOS broadcast over IPSec
[Advanced ...]

**Inbound/Outbound traffic NAT**

Outbound Traffic
□ Source NAT
Source: NONE
Destination: NONE
SNAT: NONE

Inbound Traffic
☑ Source NAT
Source: Remote_192_168_3
Destination: Local_192_168_1
SNAT: Local_192_168_31

□ Destination NAT

| # | Original IP | Mapped IP | Protocol | Original Port | Mapped Port |
|---|---|---|---|---|---|

[OK] [Cancel]

.

Note that we use Source NAT to change the VPN traffic from 192.168.3.0 which will goes to 192.168.1.0 network and to 192.168.31.0 network.

CLI commands for reference

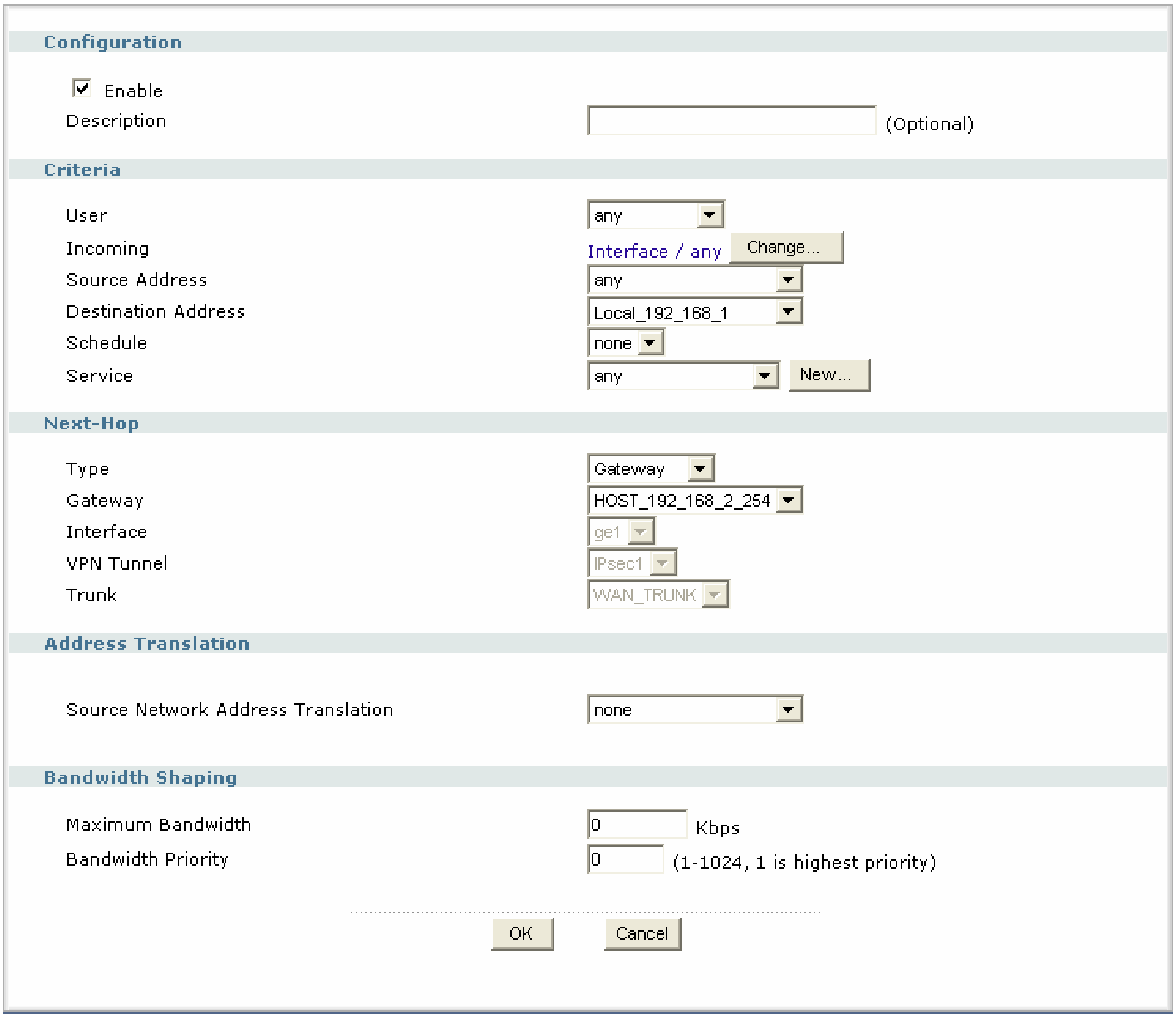
```
[0] crypto map IPsec1
[1] ipsec-isakmp IKE1
```

```
[2] encapsulation tunnel
[3] transform-set esp-des-sha
[4] set security-association lifetime seconds 86400
[5] set pfs none
[6] no policy-enforcement
[7] local-policy Local_192_168_1
[8] remote-policy Remote_ANY
[9] no nail-up
[10] no replay-detection
[11] no netbios-broadcast
[12] no out-snat activate
[13] in-snat activate
[14] in-snat source Remote_192_168_3 destination Local_192_168_1
snat Local_192_168_31
[15] no in-dnat activate
```

---

**(3) Add a policy route**

1. Go to GUI menu **Configuration** > **Policy** > **Route > Policy Route** tab
2. By default, there is one policy route already to indicate all packets which is sent from LAN to any network will be passed through WAN_TRUNK. This is also to direct IKE packet to WAN and trigger the VPN tunnel then.
3. Click the '+' icon to add another policy route which indicates where all the traffic which wants to go to the ZyWALL 1050-A's LAN network will be routed to.
4. Define that all the traffic that wants to go to 192.168.1.0 network will be routed by the gateway, the host of 192.168.2.254. The configuration is as shown below.



**Configuration**

☑ Enable

| | |
|---|---|
| Description | (Optional) |

**Criteria**

| | |
|---|---|
| User | any |
| Incoming | Interface / any [Change...] |
| Source Address | any |
| Destination Address | Local_192_168_1 |
| Schedule | none |
| Service | any [New...] |

**Next-Hop**

| | |
|---|---|
| Type | Gateway |
| Gateway | HOST_192_168_2_254 |
| Interface | ge1 |
| VPN Tunnel | IPsec1 |
| Trunk | WAN_TRUNK |

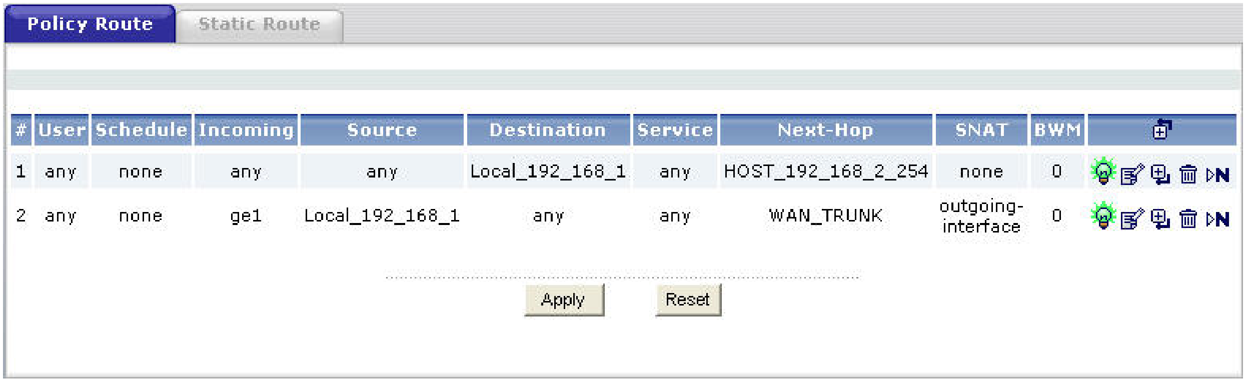
**Address Translation**

| | |
|---|---|
| Source Network Address Translation | none |

**Bandwidth Shaping**

| | |
|---|---|
| Maximum Bandwidth | 0 Kbps |
| Bandwidth Priority | 0 (1-1024, 1 is highest priority) |

After the configuration is down, you will see two policy routes as shown below.



| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | any | any | Local_192_168_1 | any | HOST_192_168_2_254 | none | 0 | |
| 2 | any | none | ge1 | Local_192_168_1 | any | any | WAN_TRUNK | outgoing-interface | 0 | |

CLI commands for reference:

```
[0] policy 1
[1] no deactivate
```

```
[2] no description
[3] no user
[4] no interface
[5] no tunnel
[6] source any
[7] destination Local_192_168_1
[8] no schedule
[9] service any
[10] next-hop gateway HOST_192_168_2_254
[11] no snat
[12] no bandwidth
[13] exit
```

### *3. Configuration on ZyWALL 2 Plus*

**(1). LAN Network Setting**

1. Login ZyWALL 2 Plus GUI and go to menu **Network** > **LAN**, change the IP address to 192.168.3.1/24 and DHCP IP pool starting address from 192.168.3.33. Then release the original IP address on your PC and get the new IP address in 192.168.3.0/24 subnet assigned by DHCP.

**(2). WAN Network Setting**

1. Switch to GUI menu **Network** > **WAN**, change the IP address to 59.124.163.152 with subnet 255.255.255.224 and gateway 59.124.163.129 in this example. Other setting leaves as default value.

***Reminder:*** Please remember to configure the public DNS server at GUI menu **Advanced** > **DNS** > **System** tab, to insert the correct DNS server accordingly at **Name Server Record**.

**(3). Dial Backup Setting**

1. Switch to GUI menu **Network** > **WAN** > **Dial Backup** tab
   - Enable Dial Backup: enable
   - Fill out the login name, password, phone number and dial backup port speed according to your modem dial up settings.
   - Click the **Apply** button

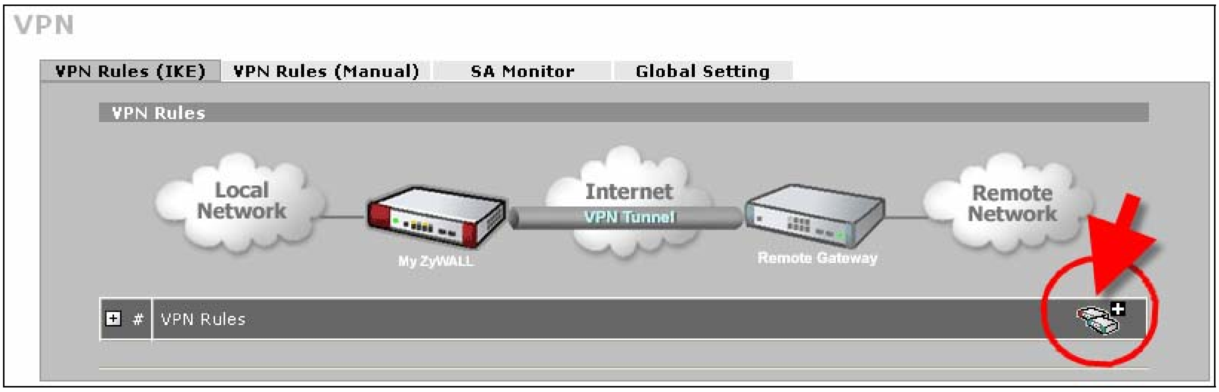
2. Telnet or login ZyWALL 2 Plus console and switch to menu 24.8 to enable the pingcheck to detect the WAN connection availability.
   - Execute the CLI command: **sys rn pingcheck 1**

3. Add the CLI to **autoexec.net** to make it always enabled even after device reboot.

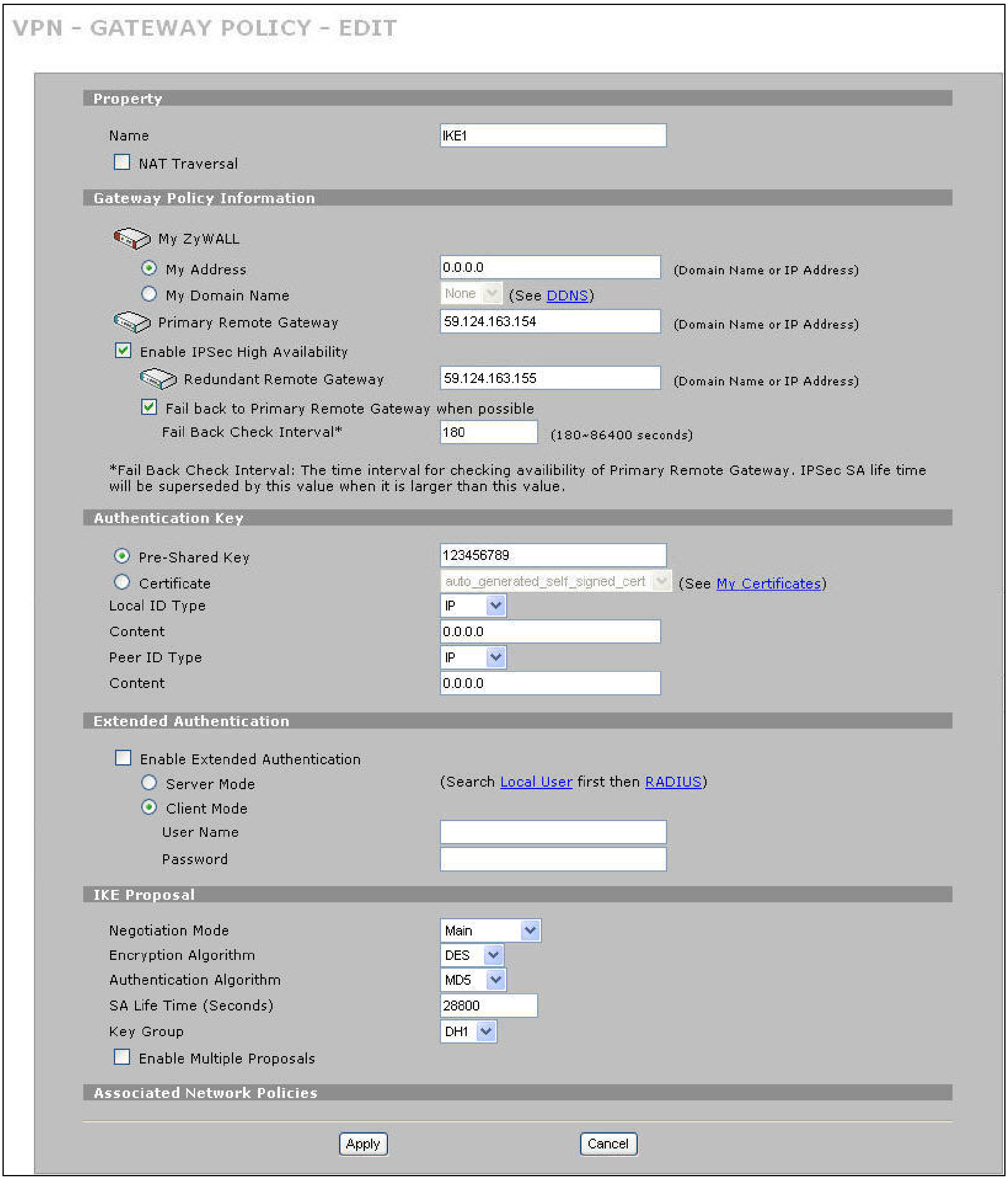
```
ras> sys edit autoexec.net
EDIT cmd: q(uit) x(save & exit) i(nsert after) d(elete) r(eplace) n(ext)
ip nat loopback on
bridge mode 1
: sys rn pingcheck 1        ← enter ‘i’ to insert the command, enter ‘x’ to save and exit then.
ras >
```

## (4) VPN Setting

1. Switch to GUI menu **Security** > **VPN**, click the ‘+’ icon as following to add a VPN-IKE rule.



2. Configure VPN-IKE setting on ZyWALL 2 Plus as following.



VPN - GATEWAY POLICY - EDIT

Property

Name: IKE1

□ NAT Traversal

Gateway Policy Information

My ZyWALL

● My Address: 0.0.0.0 (Domain Name or IP Address)

○ My Domain Name: None (See DDNS)

Primary Remote Gateway: 59.124.163.154 (Domain Name or IP Address)

☑ Enable IPSec High Availability

Redundant Remote Gateway: 59.124.163.155 (Domain Name or IP Address)

☑ Fail back to Primary Remote Gateway when possible

Fail Back Check Interval*: 180 (180~86400 seconds)

*Fail Back Check Interval: The time interval for checking availibility of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.

Authentication Key

● Pre-Shared Key: 123456789

○ Certificate: auto_generated_self_signed_cert (See My Certificates)

Local ID Type: IP

Content: 0.0.0.0

Peer ID Type: IP

Content: 0.0.0.0

Extended Authentication

□ Enable Extended Authentication

○ Server Mode (Search Local User first then RADIUS)

● Client Mode

User Name:

Password:

IKE Proposal

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

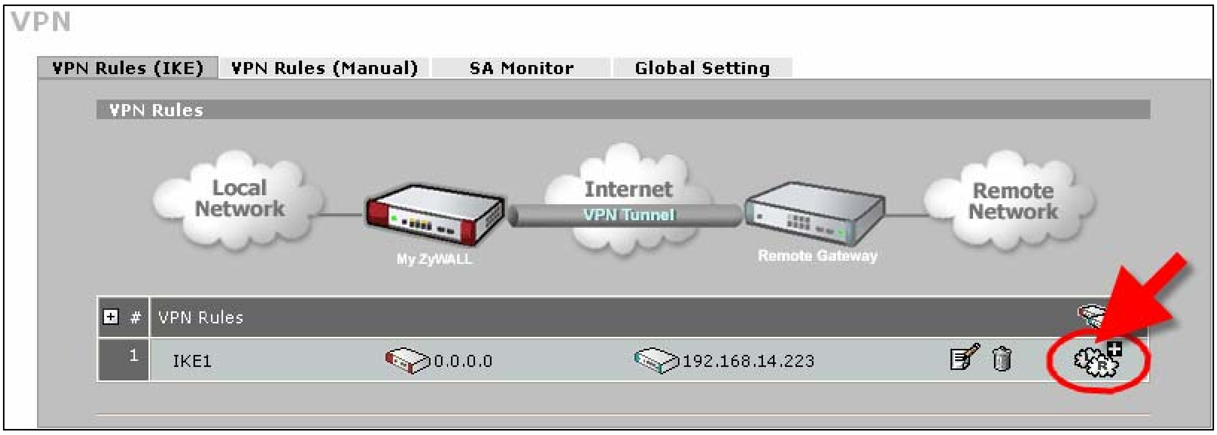
SA Life Time (Seconds): 28800

Key Group: DH1

□ Enable Multiple Proposals

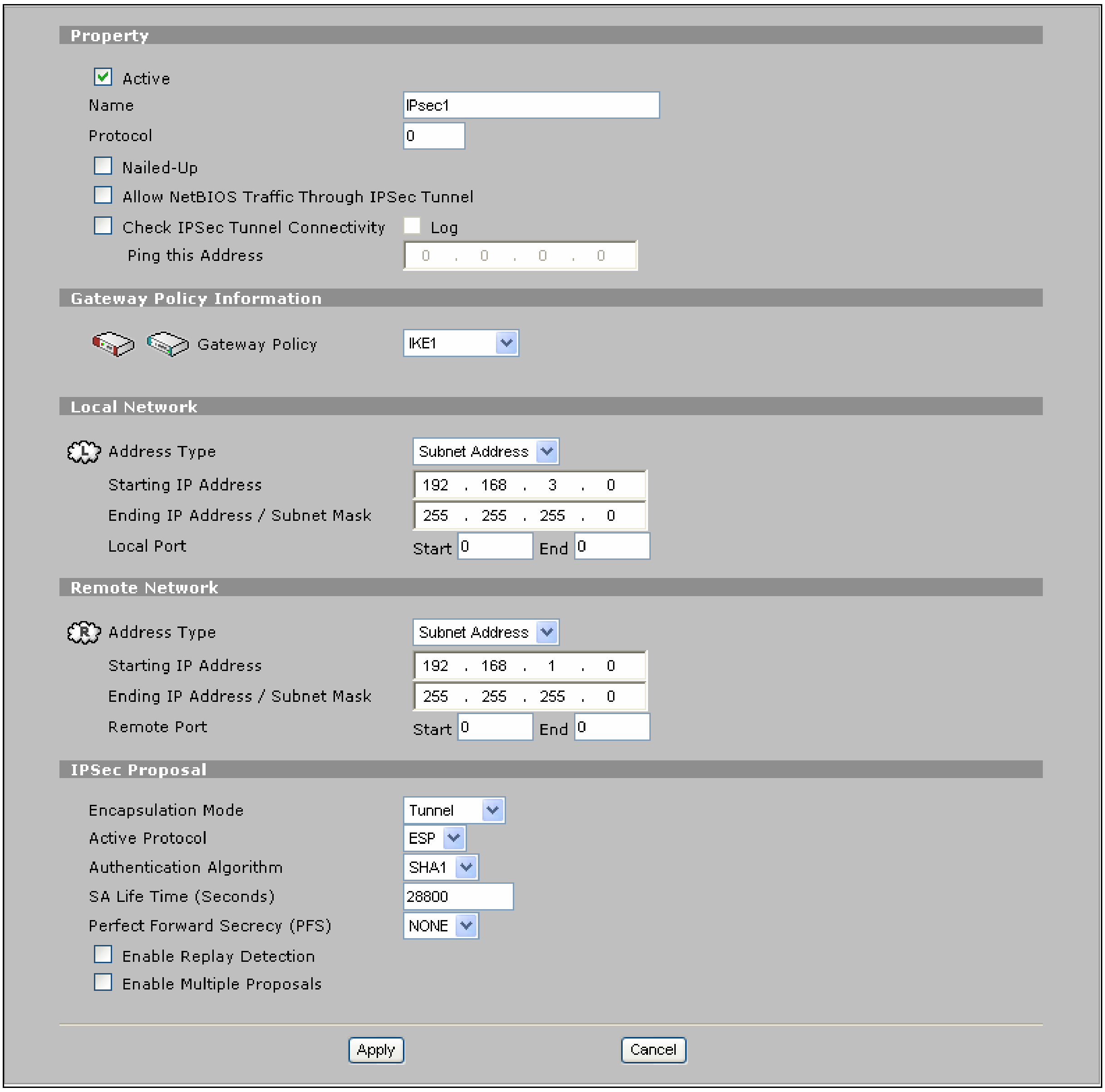
Associated Network Policies

3. At the same page of menu **Security** > **VPN**, click the icon to add a VPN-IPSec rule.



| # | VPN Rules | | | |
|---|---|---|---|---|
| 1 | IKE1 | 0.0.0.0 | 192.168.14.223 | |

4. Configure the IPSec rule as following.



**Property**

☑ Active

Name: IPsec1

Protocol: 0

□ Nailed-Up

□ Allow NetBIOS Traffic Through IPSec Tunnel

□ Check IPSec Tunnel Connectivity □ Log

Ping this Address: 0 . 0 . 0 . 0

**Gateway Policy Information**

Gateway Policy: IKE1

**Local Network**

Address Type: Subnet Address

Starting IP Address: 192 . 168 . 3 . 0

Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Local Port: Start 0 End 0

**Remote Network**

Address Type: Subnet Address

Starting IP Address: 192 . 168 . 1 . 0

Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Remote Port: Start 0 End 0

**IPSec Proposal**

Encapsulation Mode: Tunnel

Active Protocol: ESP

Authentication Algorithm: SHA1

SA Life Time (Seconds): 28800

Perfect Forward Secrecy (PFS): NONE

□ Enable Replay Detection

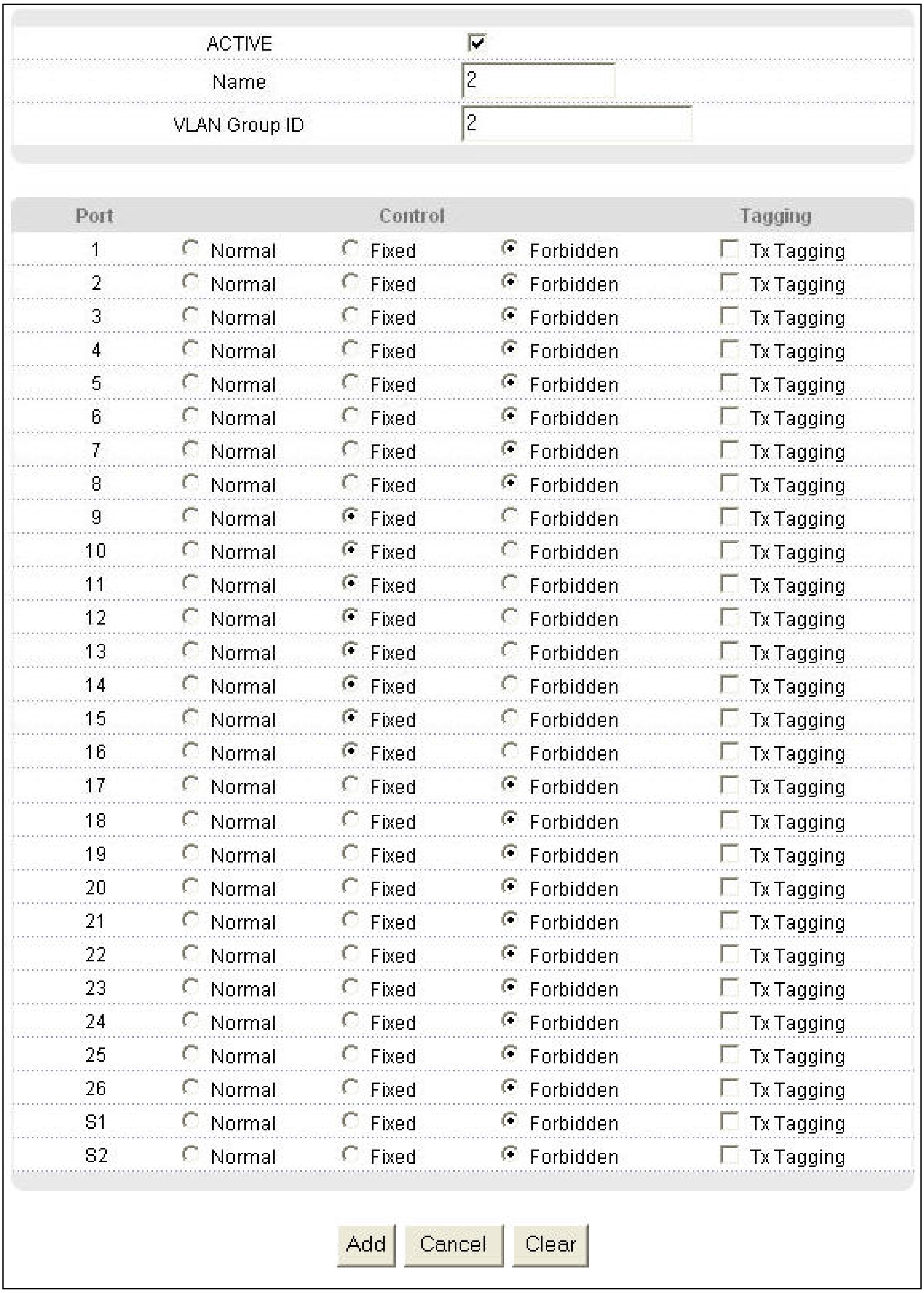
□ Enable Multiple Proposals

### *4. Configuration on ES-4024A*

**(1). Create Two VLANs**

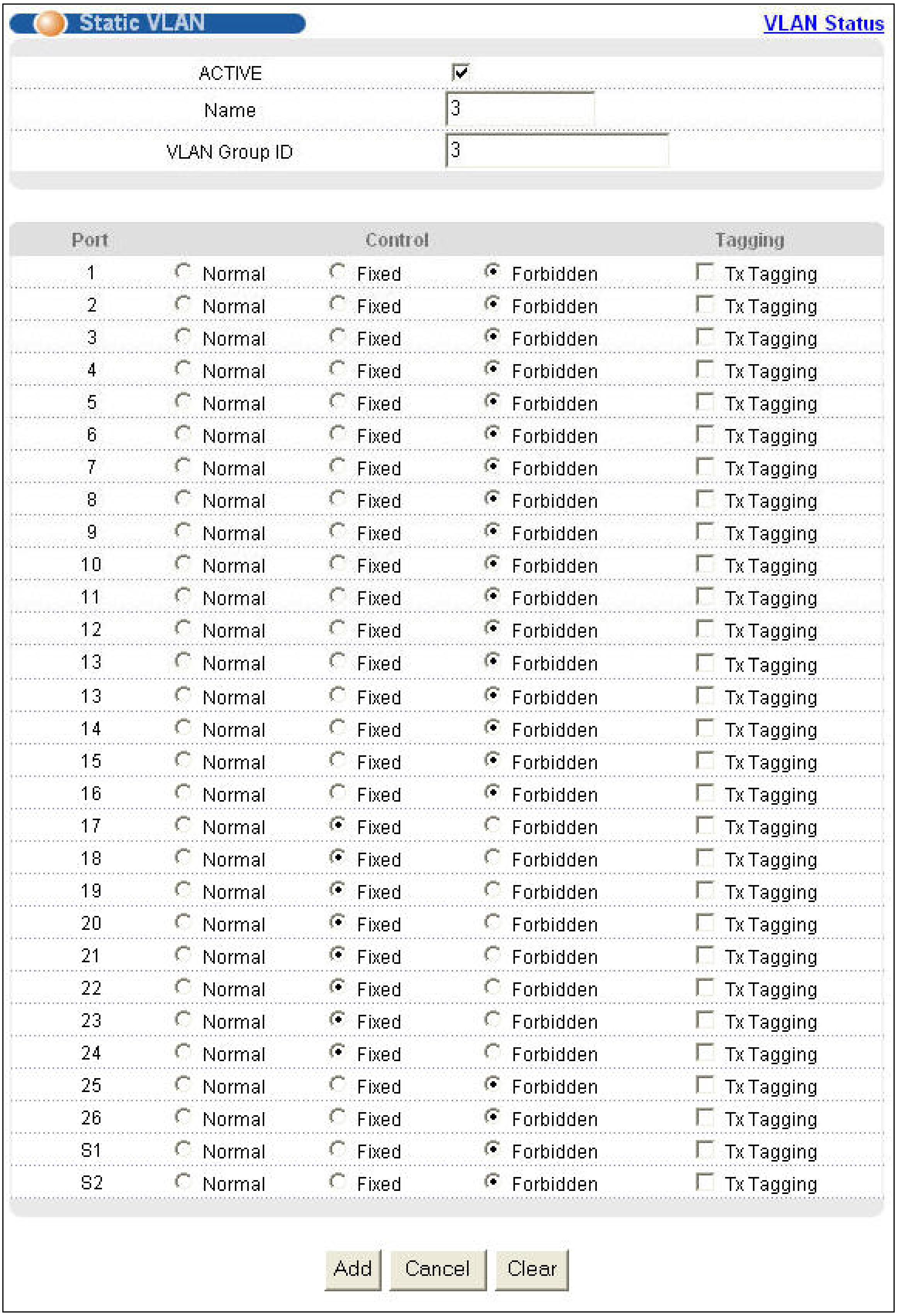
First of all, we need to create two VLANs (vlan2 & vlan3) for 192.168.1.0 and 192.168.2.0 subnet.

1. Login to ES-4024A's GUI menu **Advanced Application** > **VLAN > Static VLAN link**.
2. Add vlan2 (including port 9-16, Fixed, Untag when Egress process) and vlan3 (including port 17-24, Fixed, Untag when Egress process). Then click the **Add** button.



| | |
|---|---|
| ACTIVE | ☑ |
| Name | 2 |
| VLAN Group ID | 2 |

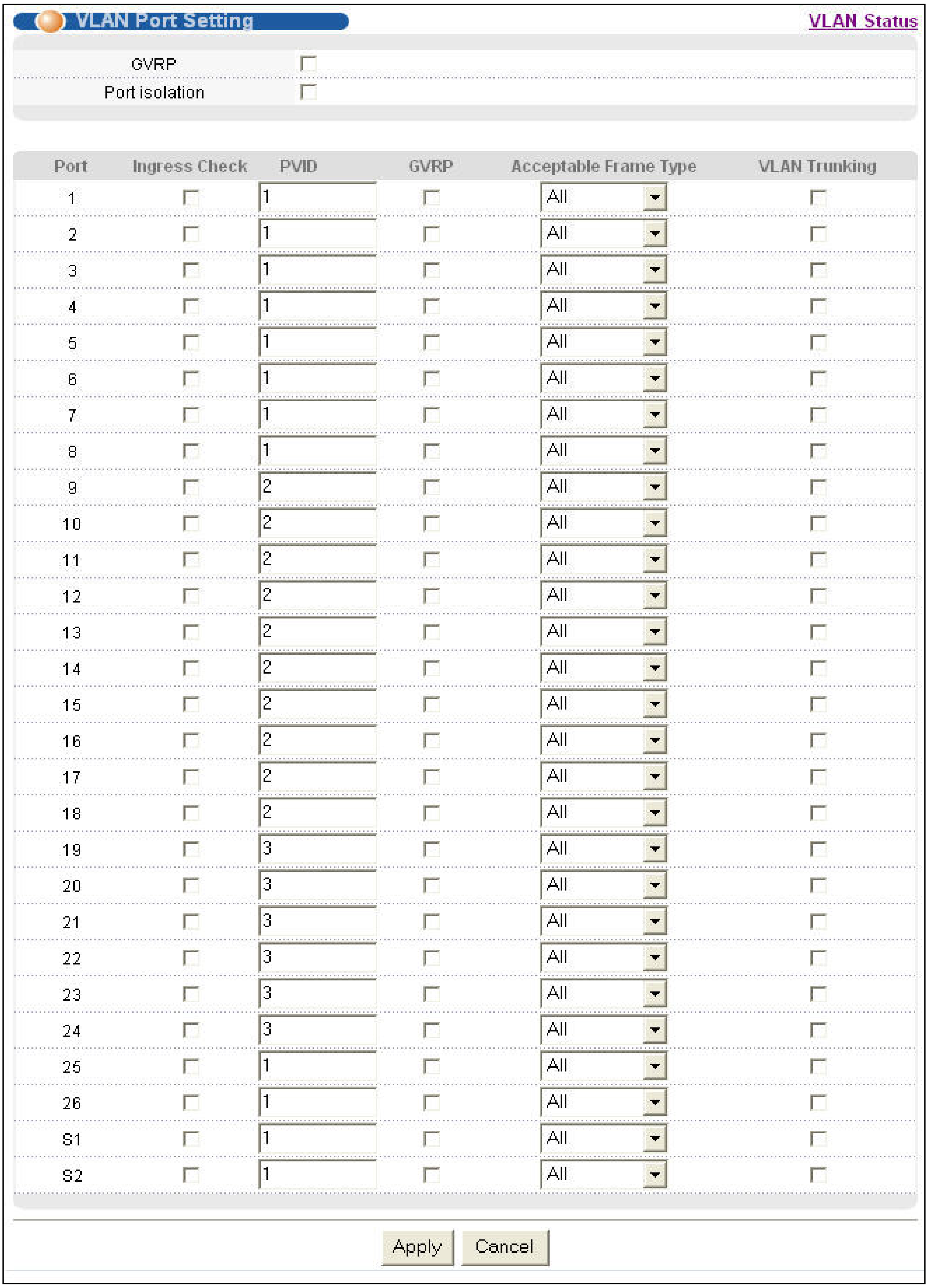
| Port | Control | | | Tagging |
|---|---|---|---|---|
| 1 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 2 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 3 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 4 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 5 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 6 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 7 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 8 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 9 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 10 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 11 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 12 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 13 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 14 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 15 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 16 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 17 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 18 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 19 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 20 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 21 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 22 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 23 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 24 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 25 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 26 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| S1 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| S2 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |



|  |  |
|---|---|
| ACTIVE | ☑ |
| Name | 3 |
| VLAN Group ID | 3 |

| Port | Control |  |  | Tagging |
|---|---|---|---|---|
| 1 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 2 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 3 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 4 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 5 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 6 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 7 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 8 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 9 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 10 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 11 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 12 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 13 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 13 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 14 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 15 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 16 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 17 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 18 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 19 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 20 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 21 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 22 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 23 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 24 | ○ Normal | ● Fixed | ○ Forbidden | □ Tx Tagging |
| 25 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| 26 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| S1 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |
| S2 | ○ Normal | ○ Fixed | ● Forbidden | □ Tx Tagging |

3. Switch to menu **Advanced Application** > **VLAN > VLAN Port Setting link**. Configure PVID equal to 2 for port 9 ~16 and PVID equal to 3 for port 17~24 as shown below. Then click the **Apply** button.



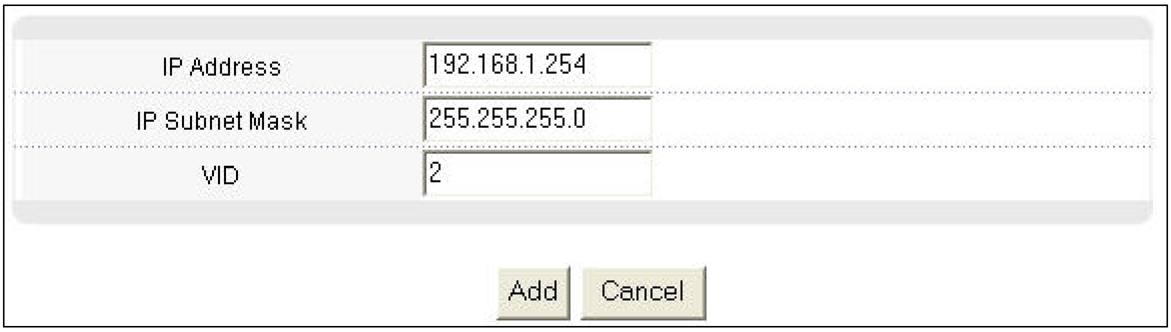
GVRP □

Port isolation □

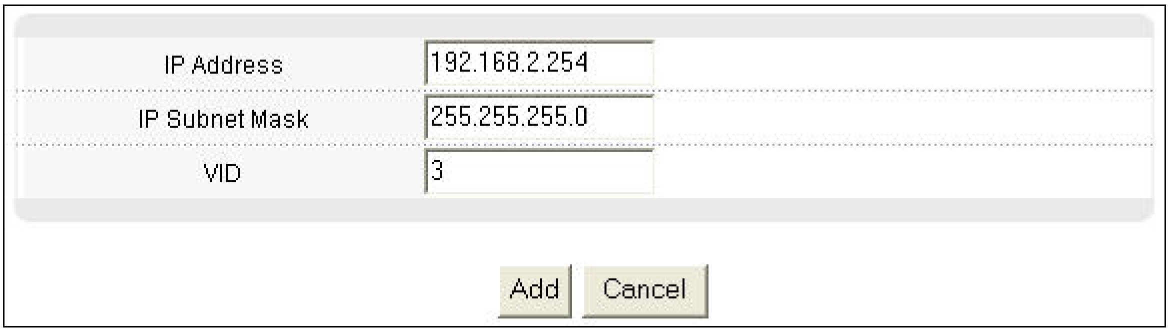
| Port | Ingress Check | PVID | GVRP | Acceptable Frame Type | VLAN Trunking |
|---|---|---|---|---|---|
| 1 | □ | 1 | □ | All | □ |
| 2 | □ | 1 | □ | All | □ |
| 3 | □ | 1 | □ | All | □ |
| 4 | □ | 1 | □ | All | □ |
| 5 | □ | 1 | □ | All | □ |
| 6 | □ | 1 | □ | All | □ |
| 7 | □ | 1 | □ | All | □ |
| 8 | □ | 1 | □ | All | □ |
| 9 | □ | 2 | □ | All | □ |
| 10 | □ | 2 | □ | All | □ |
| 11 | □ | 2 | □ | All | □ |
| 12 | □ | 2 | □ | All | □ |
| 13 | □ | 2 | □ | All | □ |
| 14 | □ | 2 | □ | All | □ |
| 15 | □ | 2 | □ | All | □ |
| 16 | □ | 2 | □ | All | □ |
| 17 | □ | 2 | □ | All | □ |
| 18 | □ | 2 | □ | All | □ |
| 19 | □ | 3 | □ | All | □ |
| 20 | □ | 3 | □ | All | □ |
| 21 | □ | 3 | □ | All | □ |
| 22 | □ | 3 | □ | All | □ |
| 23 | □ | 3 | □ | All | □ |
| 24 | □ | 3 | □ | All | □ |
| 25 | □ | 1 | □ | All | □ |
| 26 | □ | 1 | □ | All | □ |
| S1 | □ | 1 | □ | All | □ |
| S2 | □ | 1 | □ | All | □ |

### (2). Create Two Routing Domains

Switch to menu Basic Setting > IP Setup, create two IP routing domain using menu **Basic setting** > **IP Setup** as shown below. Then click the **Add** button.



| | |
|---|---|
| IP Address | 192.168.1.254 |
| IP Subnet Mask | 255.255.255.0 |
| VID | 2 |



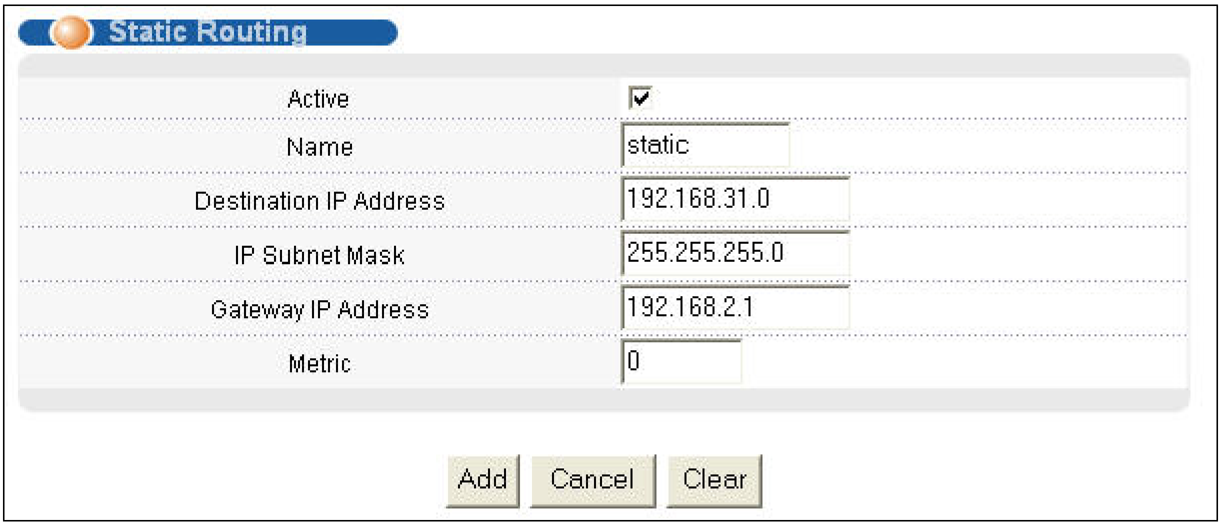
| | |
|---|---|
| IP Address | 192.168.2.254 |
| IP Subnet Mask | 255.255.255.0 |
| VID | 3 |

---

### (3). Create One Static Route

Add the static route for the packets returning from the 192.168.1.0 network to the 192.168.31.0 network if the traffic is from 192.168.3.0 through the secondary VPN gateway, ZyWALL 1050-B.

1. Enter the ES4024A's GUI, go to menu **Routing Protocol** > **Static Routing**.
2. Define that the traffic that wants to go to the 192.168.31.0/24 network will be routed by the gateway, 192.168.2.1. The configuration is as shown below.



Static Routing

| | |
|---|---|
| Active | ☑ |
| Name | static |
| Destination IP Address | 192.168.31.0 |
| IP Subnet Mask | 255.255.255.0 |
| Gateway IP Address | 192.168.2.1 |
| Metric | 0 |

CLI commands for reference:

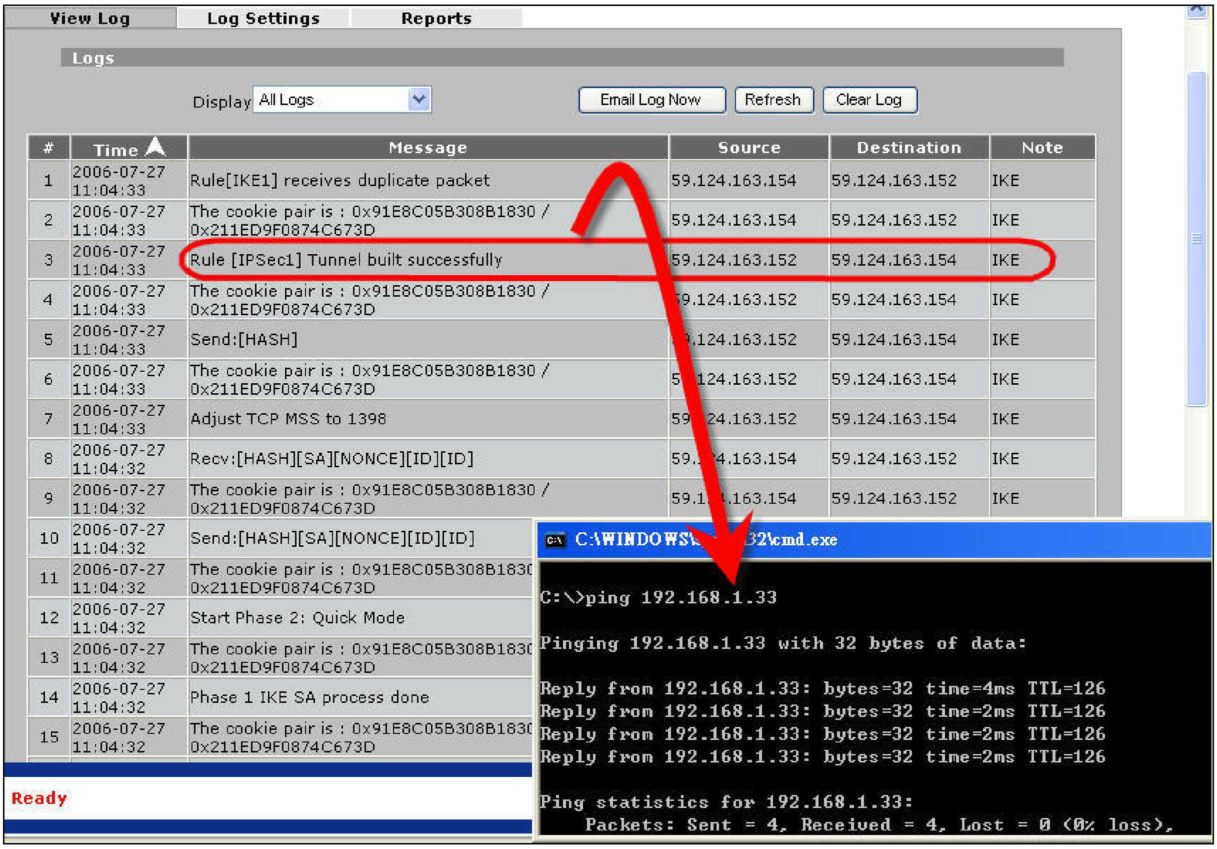
```
vlan 2
name 2
normal ""
fixed 9-16
forbidden 1-8,17-28
untagged 1-28
ip address 192.168.1.254 255.255.255.0
exit
vlan 3
name 3
normal ""
fixed 17-24
forbidden 1-16,25-28
untagged 1-28
ip address 192.168.2.254 255.255.255.0
exit
interface port-channel 9
pvid 2
exit
interface port-channel 10
pvid 2
exit
interface port-channel 11
pvid 2
```

```
exit
interface port-channel 12
pvid 2
exit
interface port-channel 13
pvid 2
exit
interface port-channel 14
pvid 2
exit
interface port-channel 15
pvid 2
exit
interface port-channel 16
pvid 2
exit
interface port-channel 17
pvid 3
exit
interface port-channel 18
pvid 3
exit
interface port-channel 19
pvid 3
exit
interface port-channel 20
pvid 3
exit
interface port-channel 21
pvid 3
exit
interface port-channel 22
pvid 3
exit
interface port-channel 23
pvid 3
exit
```

```
interface port-channel 24
pvid 3
exit
interface route-domain 192.168.1.254/24
exit
interface route-domain 192.168.2.254/24
exit
interface route-domain 192.168.111.1/24
exit
ip route 192.168.31.0 255.255.255.0 192.168.2.1 metric 0 name
LAN_31
exit
```

### *5. Test*

(1). Trigger the Primary VPN tunnel up
Keeping Ping from the PC(ex. IP with 192.168.3.33) behind ZyWALL2 Plus to the FTP server(ex. IP with 192.168.1.33), it will be reachable after the primary VPN tunnel is on. See the screen capture of ZyWALL 2 Plus's log as shown below.

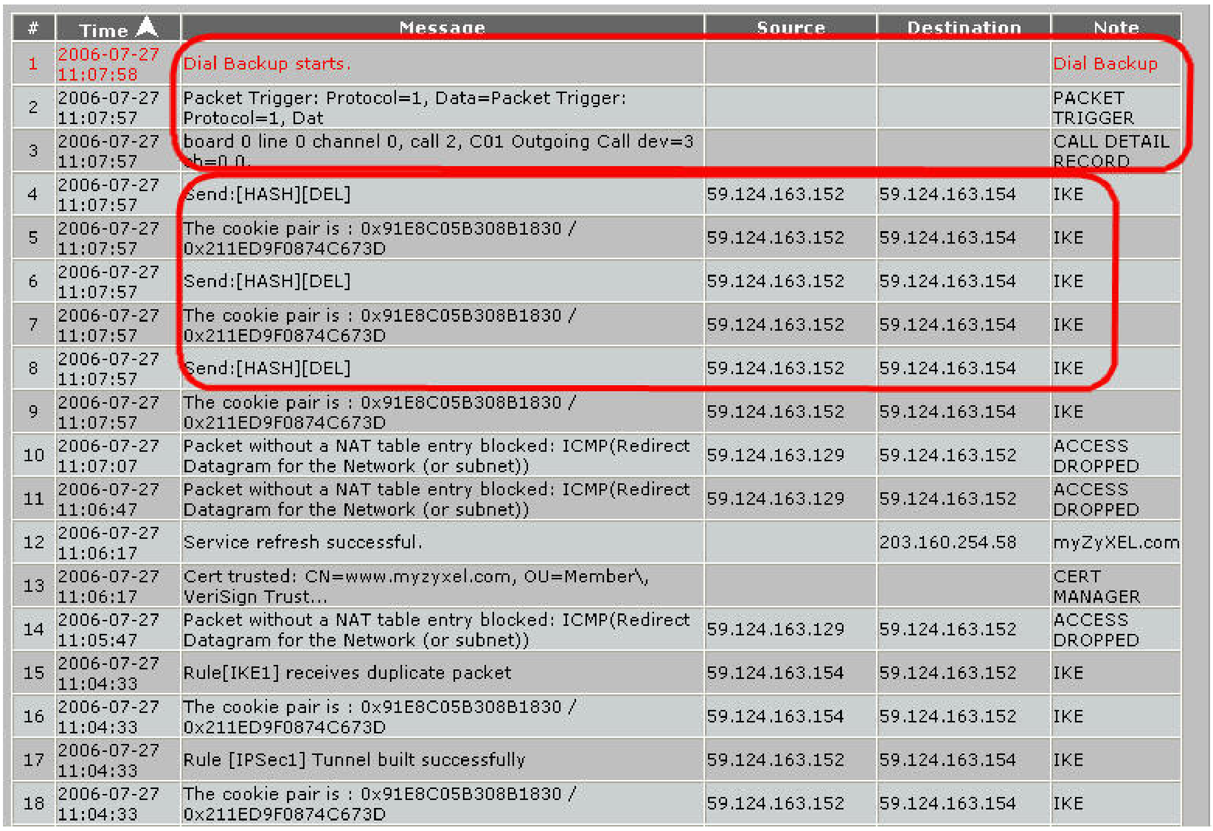


| # | Time | Message | Source | Destination | Note |
|---|---|---|---|---|---|
| 1 | 2006-07-27 11:04:33 | Rule[IKE1] receives duplicate packet | 59.124.163.154 | 59.124.163.152 | IKE |
| 2 | 2006-07-27 11:04:33 | The cookie pair is : 0x91E8C05B308B1830 / 0x211ED9F0874C673D | 59.124.163.154 | 59.124.163.152 | IKE |
| 3 | 2006-07-27 11:04:33 | Rule [IPSec1] Tunnel built successfully | 59.124.163.152 | 59.124.163.154 | IKE |
| 4 | 2006-07-27 11:04:33 | The cookie pair is : 0x91E8C05B308B1830 / 0x211ED9F0874C673D | 9.124.163.152 | 59.124.163.154 | IKE |
| 5 | 2006-07-27 11:04:33 | Send:[HASH] | .124.163.152 | 59.124.163.154 | IKE |
| 6 | 2006-07-27 11:04:33 | The cookie pair is : 0x91E8C05B308B1830 / 0x211ED9F0874C673D | 5 124.163.152 | 59.124.163.154 | IKE |
| 7 | 2006-07-27 11:04:33 | Adjust TCP MSS to 1398 | 59 24.163.152 | 59.124.163.154 | IKE |
| 8 | 2006-07-27 11:04:32 | Recv:[HASH][SA][NONCE][ID][ID] | 59. 4.163.154 | 59.124.163.152 | IKE |
| 9 | 2006-07-27 11:04:32 | The cookie pair is : 0x91E8C05B308B1830 / 0x211ED9F0874C673D | 59.1 .163.154 | 59.124.163.152 | IKE |
| 10 | 2006-07-27 11:04:32 | Send:[HASH][SA][NONCE][ID][ID] | | | |
| 11 | 2006-07-27 11:04:32 | The cookie pair is : 0x91E8C05B308B183( 0x211ED9F0874C673D | | | |
| 12 | 2006-07-27 11:04:32 | Start Phase 2: Quick Mode | | | |
| 13 | 2006-07-27 11:04:32 | The cookie pair is : 0x91E8C05B308B183( 0x211ED9F0874C673D | | | |
| 14 | 2006-07-27 11:04:32 | Phase 1 IKE SA process done | | | |
| 15 | 2006-07-27 11:04:32 | The cookie pair is : 0x91E8C05B308B183( 0x211ED9F0874C673D | | | |

```
C:\>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=4ms TTL=126
Reply from 192.168.1.33: bytes=32 time=2ms TTL=126
Reply from 192.168.1.33: bytes=32 time=2ms TTL=126
Reply from 192.168.1.33: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

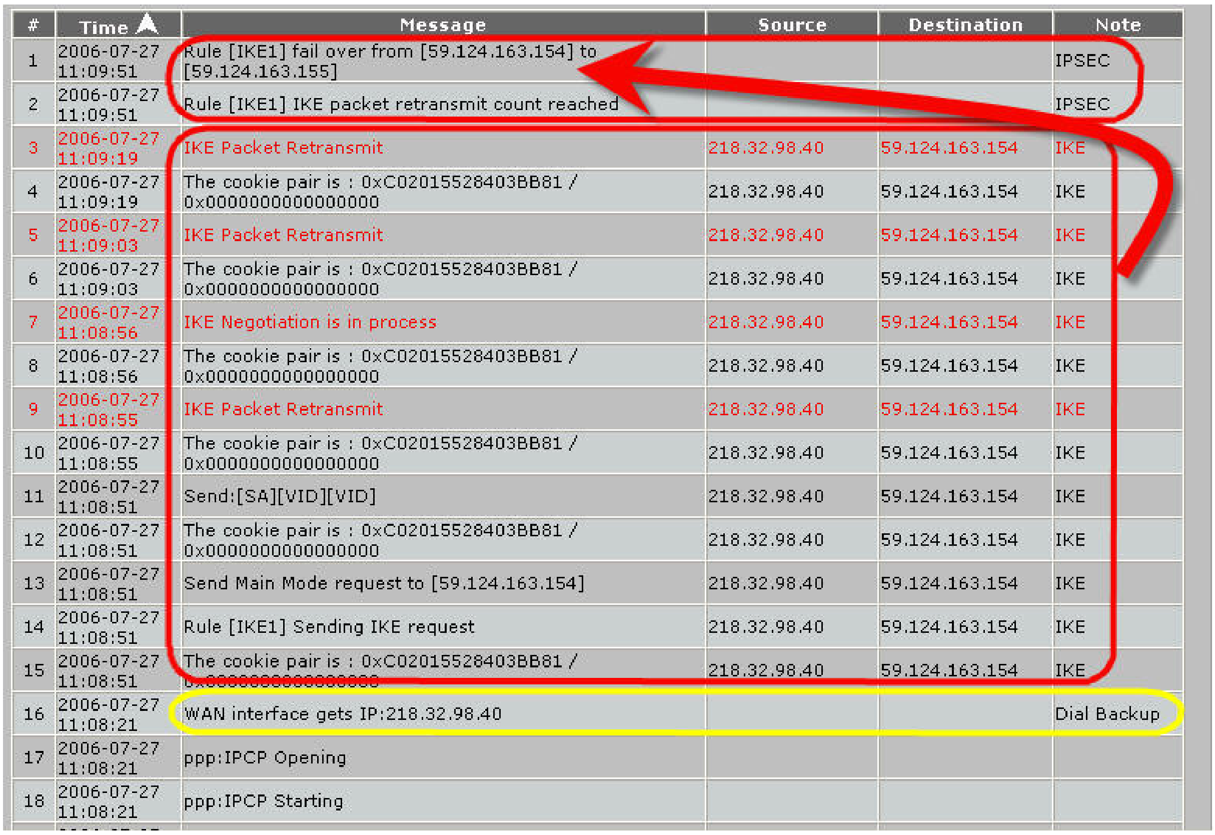
(2). Simulate the WAN connection of ZyWALL2 Plus is down
Unplug both ZyWALL2 Plus's WAN connection and ZyWALL 1050-A's WAN connection at the same time, the PC behind ZyWALL 2 Plus should be able to reach the FTP server by ping after both dial backup and secondary VPN tunnel are on.

See the screen capture of the progress as shown below at this step. The ZyWALL 2 Plus's IKE detect the tunnel is down and send HASH-DEL packet out. (However, since the Internet access is down, so ZyWALL 1050-A won't receive those HASH-DEL packets.) The dial backup starts right away then.



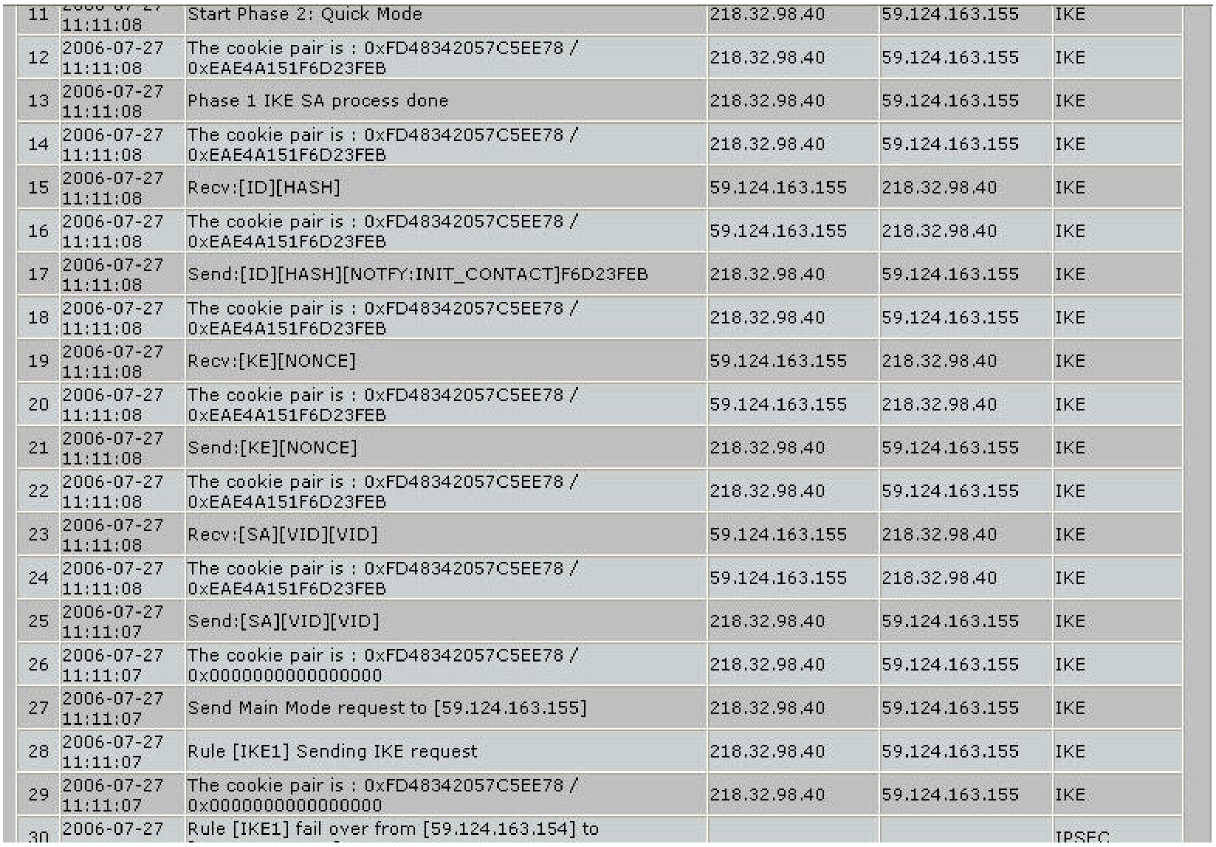
| # | Time | Message | Source | Destination | Note |
|---|---|---|---|---|---|
| 1 | 2006-07-27 11:07:58 | Dial Backup starts. | | | Dial Backup |
| 2 | 2006-07-27 11:07:57 | Packet Trigger: Protocol=1, Data=Packet Trigger: Protocol=1, Dat | | | PACKET TRIGGER |
| 3 | 2006-07-27 11:07:57 | board 0 line 0 channel 0, call 2, C01 Outgoing Call dev=3 ch=0 0. | | | CALL DETAIL RECORD |
| 4 | 2006-07-27 11:07:57 | Send:[HASH][DEL] | 59.124.163.152 | 59.124.163.154 | IKE |
| 5 | 2006-07-27 11:07:57 | The cookie pair is : 0x91E8C05B308B1830 / 0x211ED9F0874C673D | 59.124.163.152 | 59.124.163.154 | IKE |
| 6 | 2006-07-27 11:07:57 | Send:[HASH][DEL] | 59.124.163.152 | 59.124.163.154 | IKE |
| 7 | 2006-07-27 11:07:57 | The cookie pair is : 0x91E8C05B308B1830 / 0x211ED9F0874C673D | 59.124.163.152 | 59.124.163.154 | IKE |
| 8 | 2006-07-27 11:07:57 | Send:[HASH][DEL] | 59.124.163.152 | 59.124.163.154 | IKE |
| 9 | 2006-07-27 11:07:57 | The cookie pair is : 0x91E8C05B308B1830 / 0x211ED9F0874C673D | 59.124.163.152 | 59.124.163.154 | IKE |
| 10 | 2006-07-27 11:07:07 | Packet without a NAT table entry blocked: ICMP(Redirect Datagram for the Network (or subnet)) | 59.124.163.129 | 59.124.163.152 | ACCESS DROPPED |
| 11 | 2006-07-27 11:06:47 | Packet without a NAT table entry blocked: ICMP(Redirect Datagram for the Network (or subnet)) | 59.124.163.129 | 59.124.163.152 | ACCESS DROPPED |
| 12 | 2006-07-27 11:06:17 | Service refresh successful. | | 203.160.254.58 | myZyXEL.com |
| 13 | 2006-07-27 11:06:17 | Cert trusted: CN=www.myzyxel.com, OU=Member\, VeriSign Trust... | | | CERT MANAGER |
| 14 | 2006-07-27 11:05:47 | Packet without a NAT table entry blocked: ICMP(Redirect Datagram for the Network (or subnet)) | 59.124.163.129 | 59.124.163.152 | ACCESS DROPPED |
| 15 | 2006-07-27 11:04:33 | Rule[IKE1] receives duplicate packet | 59.124.163.154 | 59.124.163.152 | IKE |
| 16 | 2006-07-27 11:04:33 | The cookie pair is : 0x91E8C05B308B1830 / 0x211ED9F0874C673D | 59.124.163.154 | 59.124.163.152 | IKE |
| 17 | 2006-07-27 11:04:33 | Rule [IPSec1] Tunnel built successfully | 59.124.163.152 | 59.124.163.154 | IKE |
| 18 | 2006-07-27 11:04:33 | The cookie pair is : 0x91E8C05B308B1830 / 0x211ED9F0874C673D | 59.124.163.152 | 59.124.163.154 | IKE |

The screen capture below shows you the dial backup gets dynamic IP 218.32.98.40. And the IPSec HA take action after several IKE packets sent without any packet returned.



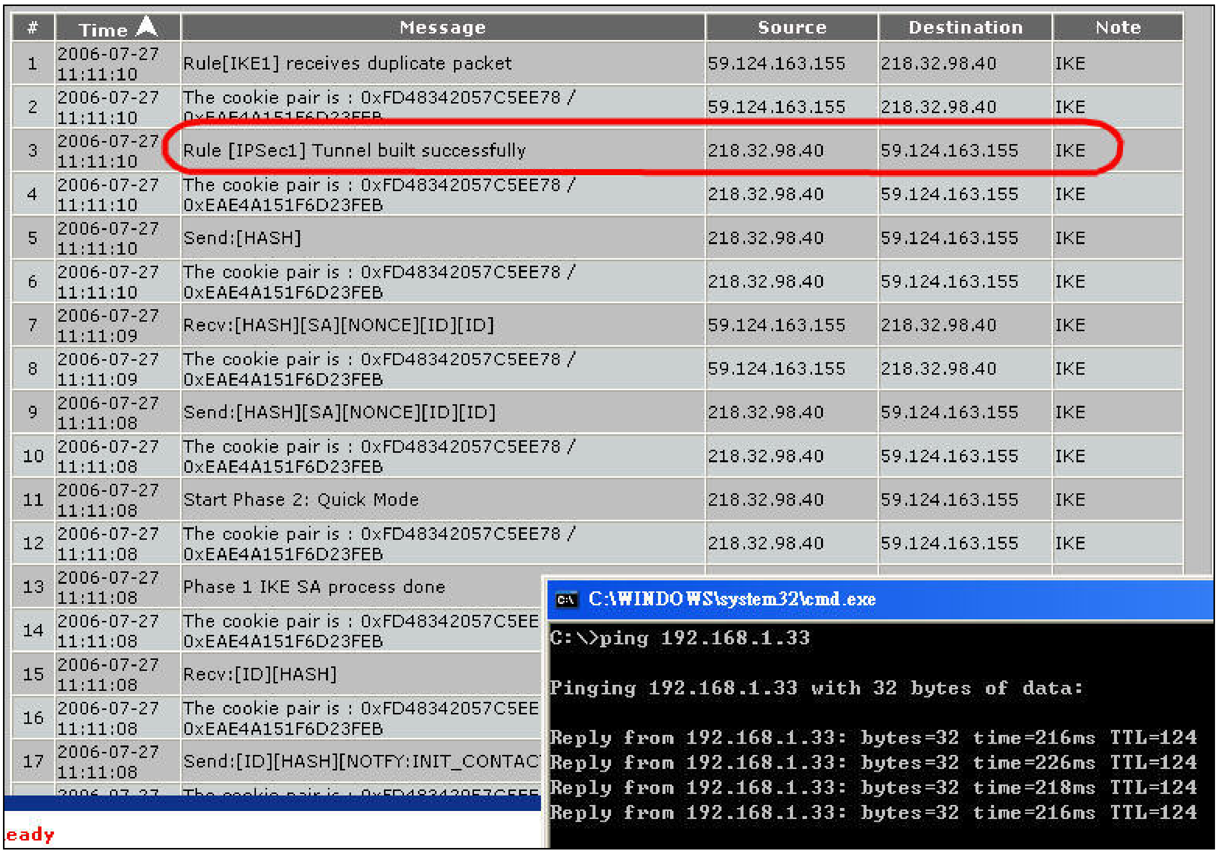
| # | Time | Message | Source | Destination | Note |
|---|---|---|---|---|---|
| 1 | 2006-07-27 11:09:51 | Rule [IKE1] fail over from [59.124.163.154] to [59.124.163.155] | | | IPSEC |
| 2 | 2006-07-27 11:09:51 | Rule [IKE1] IKE packet retransmit count reached | | | IPSEC |
| 3 | 2006-07-27 11:09:19 | IKE Packet Retransmit | 218.32.98.40 | 59.124.163.154 | IKE |
| 4 | 2006-07-27 11:09:19 | The cookie pair is : 0xC02015528403BB81 / 0x0000000000000000 | 218.32.98.40 | 59.124.163.154 | IKE |
| 5 | 2006-07-27 11:09:03 | IKE Packet Retransmit | 218.32.98.40 | 59.124.163.154 | IKE |
| 6 | 2006-07-27 11:09:03 | The cookie pair is : 0xC02015528403BB81 / 0x0000000000000000 | 218.32.98.40 | 59.124.163.154 | IKE |
| 7 | 2006-07-27 11:08:56 | IKE Negotiation is in process | 218.32.98.40 | 59.124.163.154 | IKE |
| 8 | 2006-07-27 11:08:56 | The cookie pair is : 0xC02015528403BB81 / 0x0000000000000000 | 218.32.98.40 | 59.124.163.154 | IKE |
| 9 | 2006-07-27 11:08:55 | IKE Packet Retransmit | 218.32.98.40 | 59.124.163.154 | IKE |
| 10 | 2006-07-27 11:08:55 | The cookie pair is : 0xC02015528403BB81 / 0x0000000000000000 | 218.32.98.40 | 59.124.163.154 | IKE |
| 11 | 2006-07-27 11:08:51 | Send:[SA][VID][VID] | 218.32.98.40 | 59.124.163.154 | IKE |
| 12 | 2006-07-27 11:08:51 | The cookie pair is : 0xC02015528403BB81 / 0x0000000000000000 | 218.32.98.40 | 59.124.163.154 | IKE |
| 13 | 2006-07-27 11:08:51 | Send Main Mode request to [59.124.163.154] | 218.32.98.40 | 59.124.163.154 | IKE |
| 14 | 2006-07-27 11:08:51 | Rule [IKE1] Sending IKE request | 218.32.98.40 | 59.124.163.154 | IKE |
| 15 | 2006-07-27 11:08:51 | The cookie pair is : 0xC02015528403BB81 / 0x0000000000000000 | 218.32.98.40 | 59.124.163.154 | IKE |
| 16 | 2006-07-27 11:08:21 | WAN interface gets IP:218.32.98.40 | | | Dial Backup |
| 17 | 2006-07-27 11:08:21 | ppp:IPCP Opening | | | |
| 18 | 2006-07-27 11:08:21 | ppp:IPCP Starting | | | |

Then ZyWALL 2 Plus tries to establish VPN tunnel with ZyWALL 1050-B (59.124.163.155).



| # | Time | Message | Source | Destination | Note |
|---|---|---|---|---|---|
| 11 | 11:11:08 | Start Phase 2: Quick Mode | 218.32.98.40 | 59.124.163.155 | IKE |
| 12 | 2006-07-27 11:11:08 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 218.32.98.40 | 59.124.163.155 | IKE |
| 13 | 2006-07-27 11:11:08 | Phase 1 IKE SA process done | 218.32.98.40 | 59.124.163.155 | IKE |
| 14 | 2006-07-27 11:11:08 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 218.32.98.40 | 59.124.163.155 | IKE |
| 15 | 2006-07-27 11:11:08 | Recv:[ID][HASH] | 59.124.163.155 | 218.32.98.40 | IKE |
| 16 | 2006-07-27 11:11:08 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 59.124.163.155 | 218.32.98.40 | IKE |
| 17 | 2006-07-27 11:11:08 | Send:[ID][HASH][NOTFY:INIT_CONTACT]F6D23FEB | 218.32.98.40 | 59.124.163.155 | IKE |
| 18 | 2006-07-27 11:11:08 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 218.32.98.40 | 59.124.163.155 | IKE |
| 19 | 2006-07-27 11:11:08 | Recv:[KE][NONCE] | 59.124.163.155 | 218.32.98.40 | IKE |
| 20 | 2006-07-27 11:11:08 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 59.124.163.155 | 218.32.98.40 | IKE |
| 21 | 2006-07-27 11:11:08 | Send:[KE][NONCE] | 218.32.98.40 | 59.124.163.155 | IKE |
| 22 | 2006-07-27 11:11:08 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 218.32.98.40 | 59.124.163.155 | IKE |
| 23 | 2006-07-27 11:11:08 | Recv:[SA][VID][VID] | 59.124.163.155 | 218.32.98.40 | IKE |
| 24 | 2006-07-27 11:11:08 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 59.124.163.155 | 218.32.98.40 | IKE |
| 25 | 2006-07-27 11:11:07 | Send:[SA][VID][VID] | 218.32.98.40 | 59.124.163.155 | IKE |
| 26 | 2006-07-27 11:11:07 | The cookie pair is : 0xFD48342057C5EE78 / 0x0000000000000000 | 218.32.98.40 | 59.124.163.155 | IKE |
| 27 | 2006-07-27 11:11:07 | Send Main Mode request to [59.124.163.155] | 218.32.98.40 | 59.124.163.155 | IKE |
| 28 | 2006-07-27 11:11:07 | Rule [IKE1] Sending IKE request | 218.32.98.40 | 59.124.163.155 | IKE |
| 29 | 2006-07-27 11:11:07 | The cookie pair is : 0xFD48342057C5EE78 / 0x0000000000000000 | 218.32.98.40 | 59.124.163.155 | IKE |
| 30 | 2006-07-27 | Rule [IKE1] fail over from [59.124.163.154] to | | | IPSEC |

Finally, the VPN tunnel has been successfully established with ZyWALL 1050-B. And the PC behind ZyWALL 2 Plus can ping the FTP server then. See the screen capture shown below.



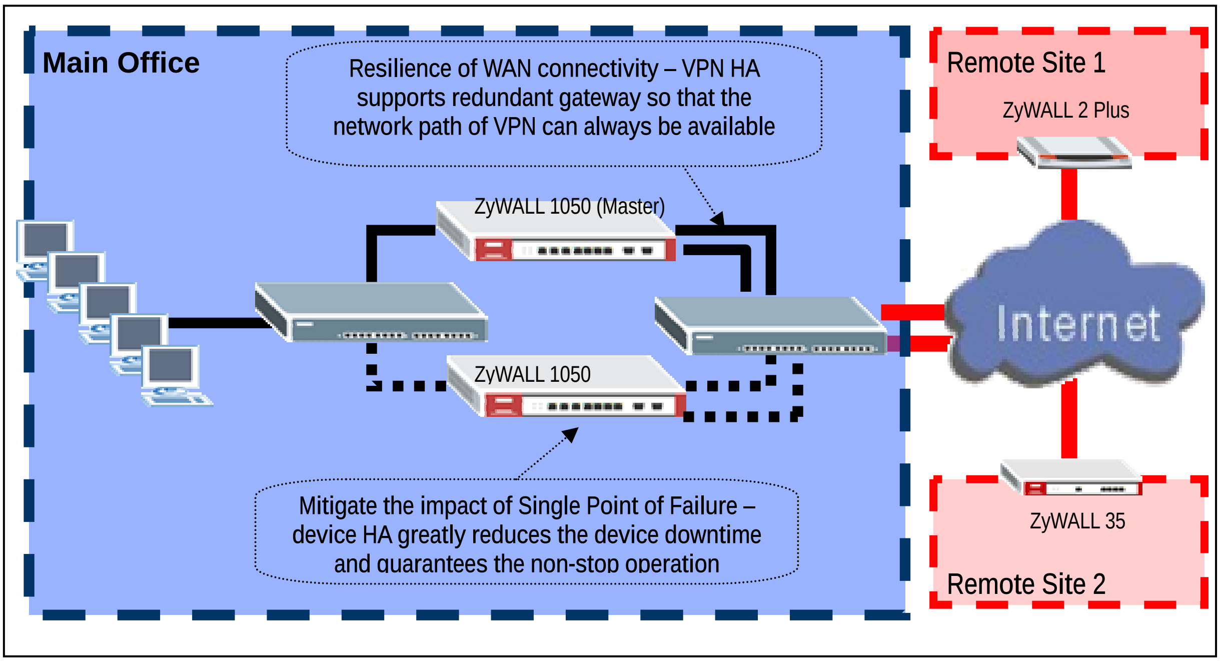
| # | Time | Message | Source | Destination | Note |
|---|---|---|---|---|---|
| 1 | 2006-07-27 11:11:10 | Rule[IKE1] receives duplicate packet | 59.124.163.155 | 218.32.98.40 | IKE |
| 2 | 2006-07-27 11:11:10 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 59.124.163.155 | 218.32.98.40 | IKE |
| 3 | 2006-07-27 11:11:10 | Rule [IPSec1] Tunnel built successfully | 218.32.98.40 | 59.124.163.155 | IKE |
| 4 | 2006-07-27 11:11:10 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 218.32.98.40 | 59.124.163.155 | IKE |
| 5 | 2006-07-27 11:11:10 | Send:[HASH] | 218.32.98.40 | 59.124.163.155 | IKE |
| 6 | 2006-07-27 11:11:10 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 218.32.98.40 | 59.124.163.155 | IKE |
| 7 | 2006-07-27 11:11:09 | Recv:[HASH][SA][NONCE][ID][ID] | 59.124.163.155 | 218.32.98.40 | IKE |
| 8 | 2006-07-27 11:11:09 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 59.124.163.155 | 218.32.98.40 | IKE |
| 9 | 2006-07-27 11:11:08 | Send:[HASH][SA][NONCE][ID][ID] | 218.32.98.40 | 59.124.163.155 | IKE |
| 10 | 2006-07-27 11:11:08 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 218.32.98.40 | 59.124.163.155 | IKE |
| 11 | 2006-07-27 11:11:08 | Start Phase 2: Quick Mode | 218.32.98.40 | 59.124.163.155 | IKE |
| 12 | 2006-07-27 11:11:08 | The cookie pair is : 0xFD48342057C5EE78 / 0xEAE4A151F6D23FEB | 218.32.98.40 | 59.124.163.155 | IKE |
| 13 | 2006-07-27 11:11:08 | Phase 1 IKE SA process done | | | |
| 14 | 2006-07-27 11:11:08 | The cookie pair is : 0xFD48342057C5EE<br>0xEAE4A151F6D23FEB | | | |
| 15 | 2006-07-27 11:11:08 | Recv:[ID][HASH] | | | |
| 16 | 2006-07-27 11:11:08 | The cookie pair is : 0xFD48342057C5EE<br>0xEAE4A151F6D23FEB | | | |
| 17 | 2006-07-27 11:11:08 | Send:[ID][HASH][NOTFY:INIT_CONTAC | | | |
| | 2006-07-27 | The cookie pair is : 0xFD48342057C5EE | | | |

eady

C:\WINDOWS\system32\cmd.exe

```
C:\>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=216ms TTL=124
Reply from 192.168.1.33: bytes=32 time=226ms TTL=124
Reply from 192.168.1.33: bytes=32 time=218ms TTL=124
Reply from 192.168.1.33: bytes=32 time=216ms TTL=124
```

## 1.7 Device High Availability


Main Office
Resilience of WAN connectivity – VPN HA supports redundant gateway so that the network path of VPN can always be available
ZyWALL 1050 (Master)
ZyWALL 1050
Mitigate the impact of Single Point of Failure – device HA greatly reduces the device downtime and guarantees the non-stop operation
Remote Site 1
ZyWALL 2 Plus
Internet
ZyWALL 35
Remote Site 2

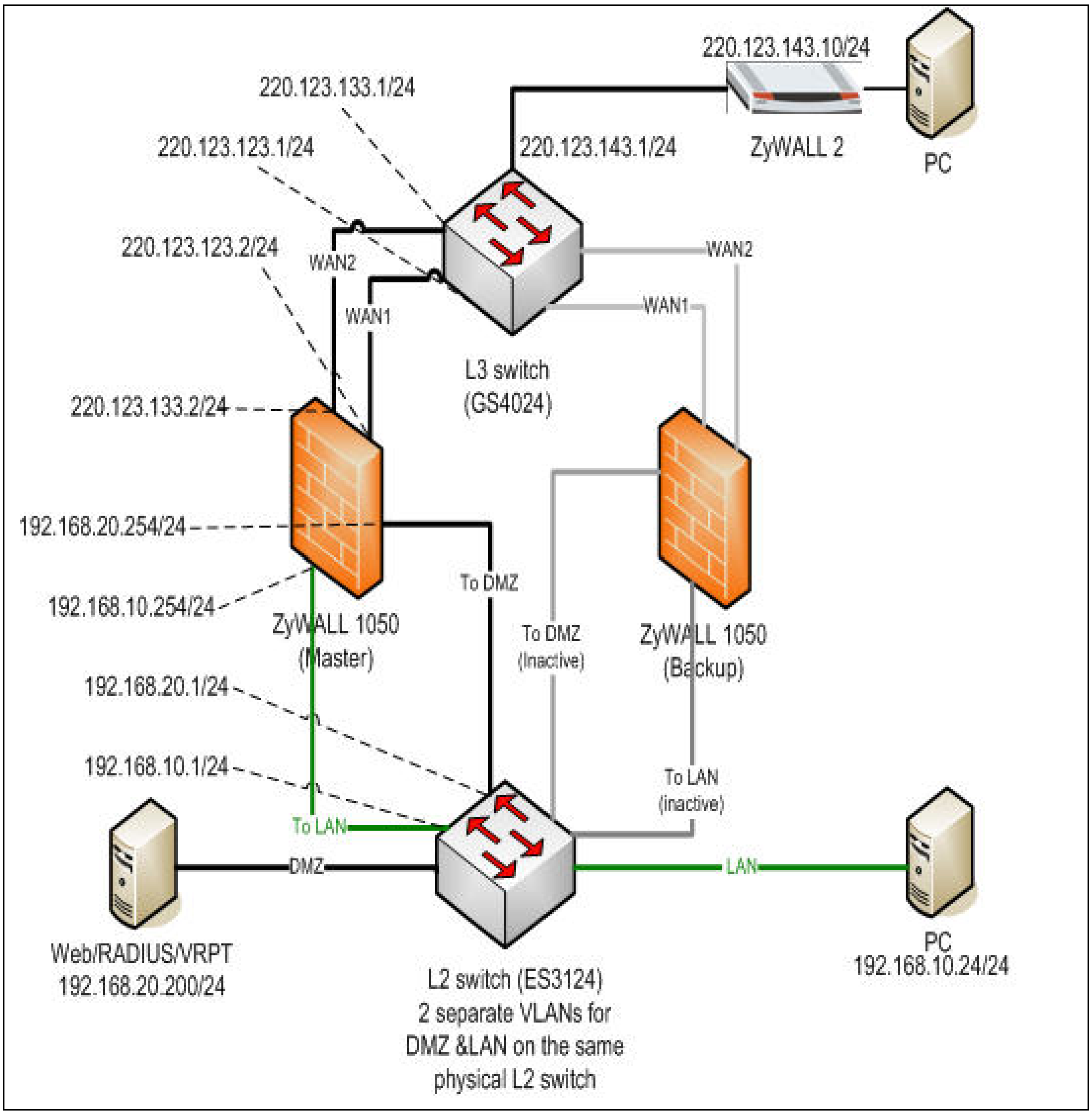
In the Global or multi-site Enterprise network deployment, reliability is another major concern while planning a VPN deployment.

**ZyWALL 1050 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.



## Step by step configuration

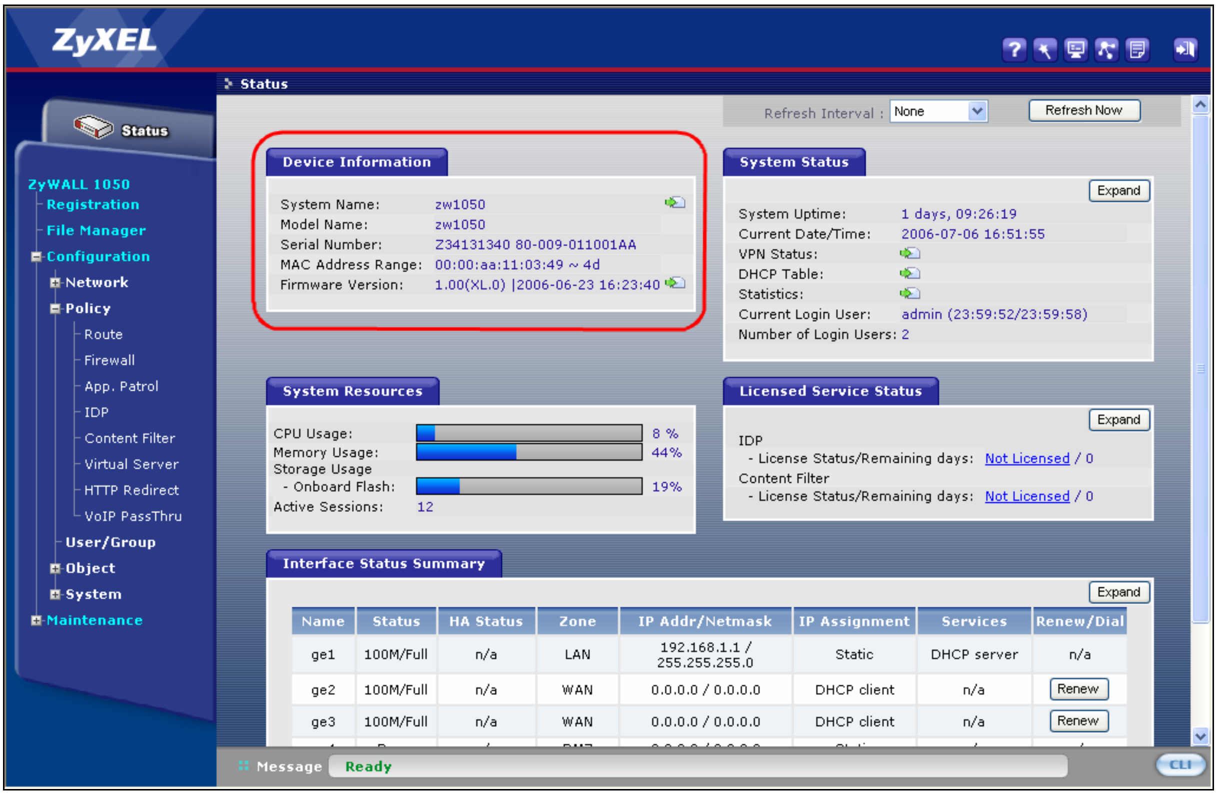
### 1.7.1 Device HA

**1. Setup Master ZyWALL 1050 and the configuration will auto sync with Backup ZyWALL 1050 via the device HA setting.**

**1.1. Interface setup**

The default LAN subnet is combined with ge1 and default IP is 192.168.1.1. Please connect to ge1 and ZyWALL 1050 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



Status

Device Information

System Name: zw1050
Model Name: zw1050
Serial Number: Z34131340 80-009-011001AA
MAC Address Range: 00:00:aa:11:03:49 ~ 4d
Firmware Version: 1.00(XL.0) |2006-06-23 16:23:40

System Status

System Uptime: 1 days, 09:26:19
Current Date/Time: 2006-07-06 16:51:55
VPN Status:
DHCP Table:
Statistics:
Current Login User: admin (23:59:52/23:59:58)
Number of Login Users: 2

System Resources

CPU Usage: 8 %
Memory Usage: 44%
Storage Usage
- Onboard Flash: 19%
Active Sessions: 12

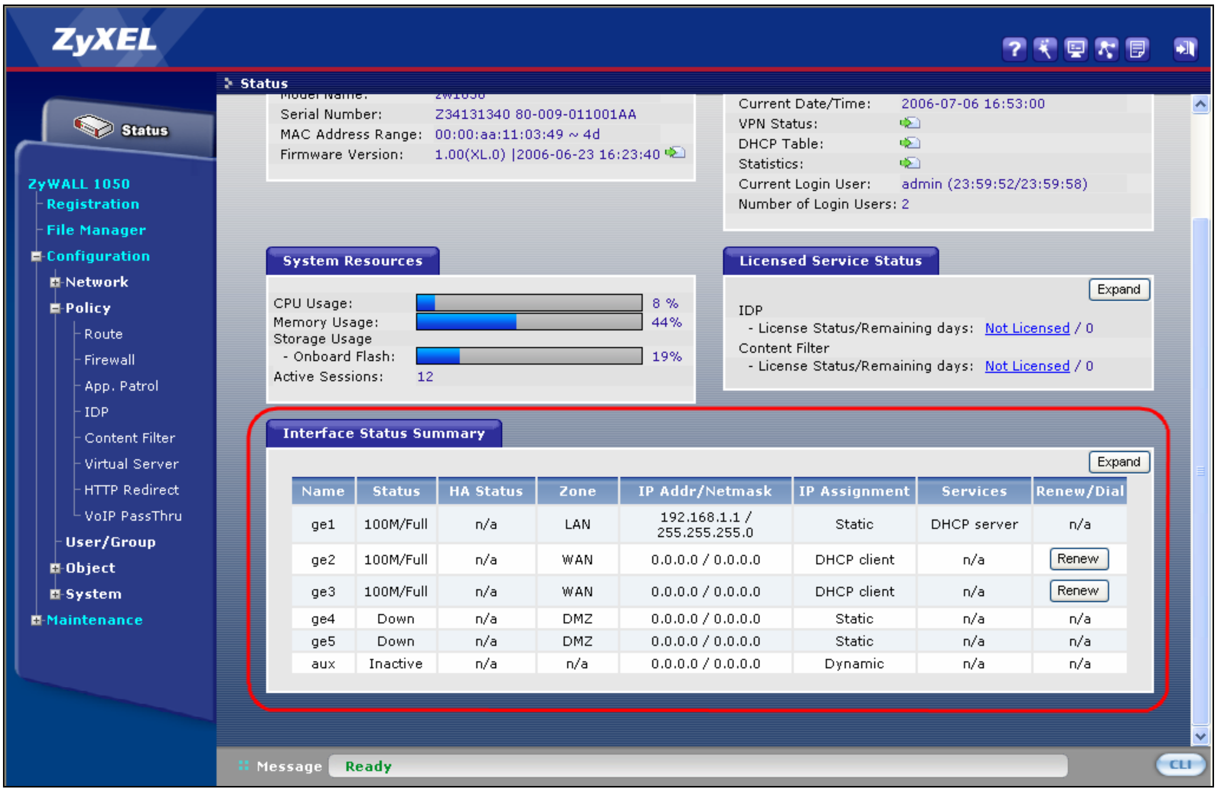
Licensed Service Status

IDP
- License Status/Remaining days: Not Licensed / 0
Content Filter
- License Status/Remaining days: Not Licensed / 0

Interface Status Summary

| Name | Status | HA Status | Zone | IP Addr/Netmask | IP Assignment | Services | Renew/Dial |
|---|---|---|---|---|---|---|---|
| ge1 | 100M/Full | n/a | LAN | 192.168.1.1 / 255.255.255.0 | Static | DHCP server | n/a |
| ge2 | 100M/Full | n/a | WAN | 0.0.0.0 / 0.0.0.0 | DHCP client | n/a | Renew |
| ge3 | 100M/Full | n/a | WAN | 0.0.0.0 / 0.0.0.0 | DHCP client | n/a | Renew |

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



Status

Serial Number: Z34131340 80-009-011001AA
MAC Address Range: 00:00:aa:11:03:49 ~ 4d
Firmware Version: 1.00(XL.0) |2006-06-23 16:23:40

Current Date/Time: 2006-07-06 16:53:00
VPN Status:
DHCP Table:
Statistics:
Current Login User: admin (23:59:52/23:59:58)
Number of Login Users: 2

System Resources

CPU Usage: 8 %
Memory Usage: 44%
Storage Usage
- Onboard Flash: 19%
Active Sessions: 12

Licensed Service Status

IDP
- License Status/Remaining days: Not Licensed / 0
Content Filter
- License Status/Remaining days: Not Licensed / 0

Interface Status Summary

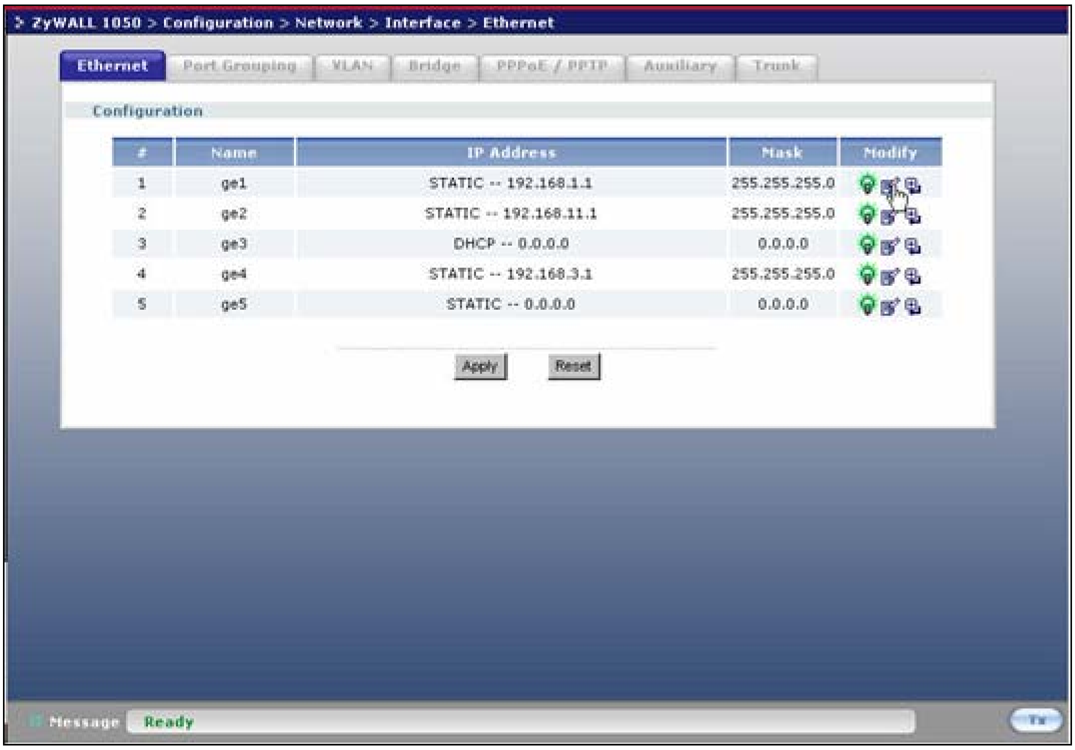
| Name | Status | HA Status | Zone | IP Addr/Netmask | IP Assignment | Services | Renew/Dial |
|---|---|---|---|---|---|---|---|
| ge1 | 100M/Full | n/a | LAN | 192.168.1.1 / 255.255.255.0 | Static | DHCP server | n/a |
| ge2 | 100M/Full | n/a | WAN | 0.0.0.0 / 0.0.0.0 | DHCP client | n/a | Renew |
| ge3 | 100M/Full | n/a | WAN | 0.0.0.0 / 0.0.0.0 | DHCP client | n/a | Renew |
| ge4 | Down | n/a | DMZ | 0.0.0.0 / 0.0.0.0 | Static | n/a | n/a |
| ge5 | Down | n/a | DMZ | 0.0.0.0 / 0.0.0.0 | Static | n/a | n/a |
| aux | Inactive | n/a | n/a | 0.0.0.0 / 0.0.0.0 | Dynamic | n/a | n/a |

Step3. Setup WAN1, WAN2, LAN and DMZ interface IP parameters as in the demo

topology.

| ge1 | ge2 | ge3 | ge4 | ge5 |
|---|---|---|---|---|
| LAN | WAN1 | WAN2 | DMZ | Reserved |

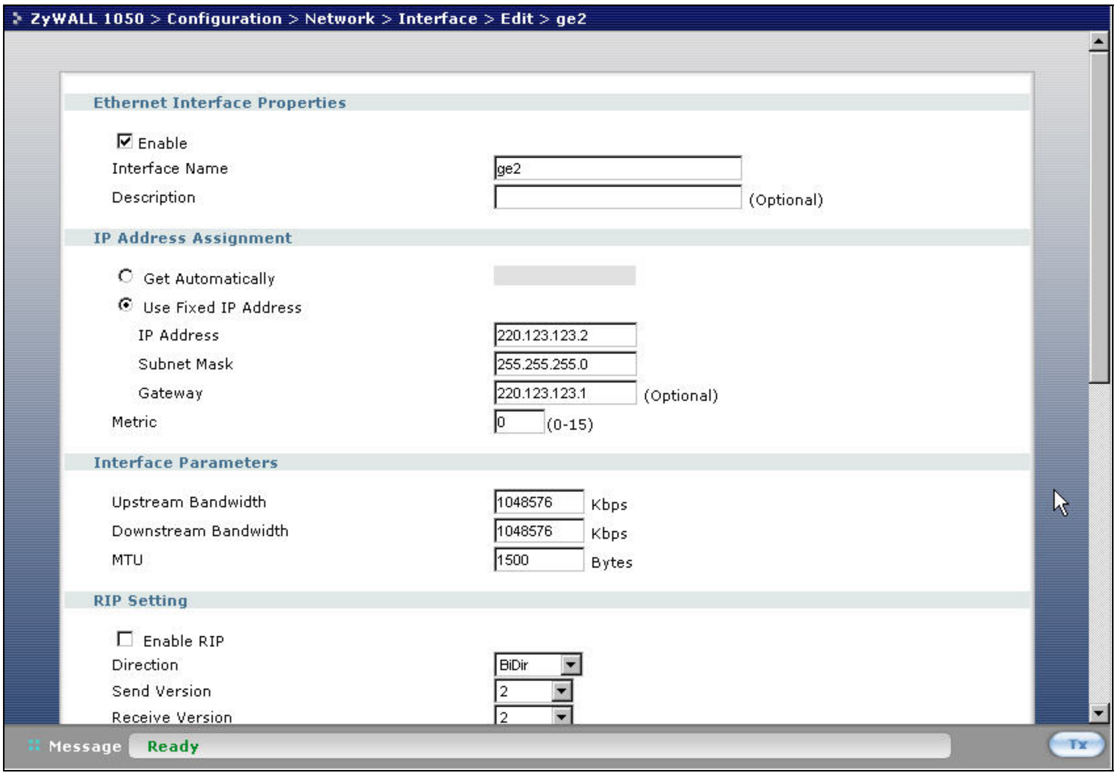
The default interface configuration is as follows. We will configure ge2, ge3, ge4 and ge1 in turn. User needs to click the “Edit” icon to modify the setting.



Configuration

| # | Name | IP Address | Mask | Modify |
|---|---|---|---|---|
| 1 | ge1 | STATIC -- 192.168.1.1 | 255.255.255.0 | |
| 2 | ge2 | STATIC -- 192.168.11.1 | 255.255.255.0 | |
| 3 | ge3 | DHCP -- 0.0.0.0 | 0.0.0.0 | |
| 4 | ge4 | STATIC -- 192.168.3.1 | 255.255.255.0 | |
| 5 | ge5 | STATIC -- 0.0.0.0 | 0.0.0.0 | |

ge2 Fix IP: 220.123.123.2/255.255.255.0 Gateway: 220.123.123.1



ZyWALL 1050 > Configuration > Network > Interface > Edit > ge2

Ethernet Interface Properties

☑ Enable

Interface Name: ge2

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

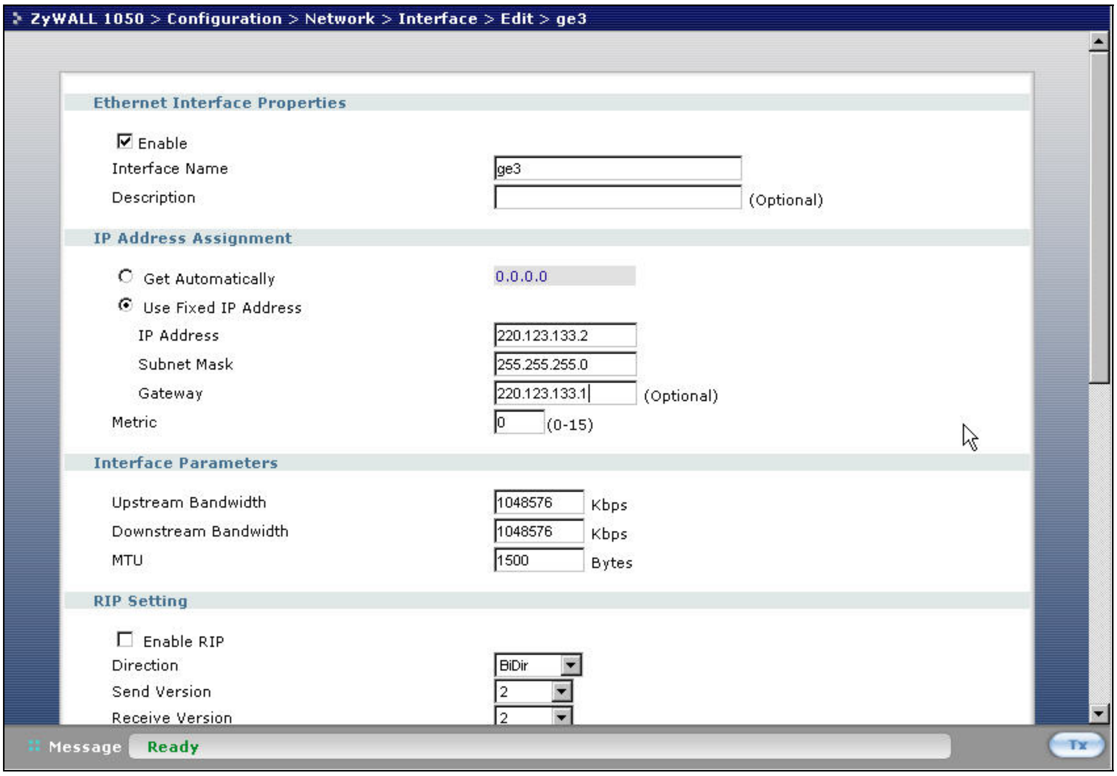
Direction: BiDir

Send Version: 2

Receive Version: 2

Message: Ready

ge3 Fix IP: 220.123.133.2/255.255.255.0 Gateway: 220.123.133.1



ZyWALL 1050 > Configuration > Network > Interface > Edit > ge3

Ethernet Interface Properties

☑ Enable

Interface Name: ge3

Description: (Optional)

IP Address Assignment

○ Get Automatically: 0.0.0.0

● 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

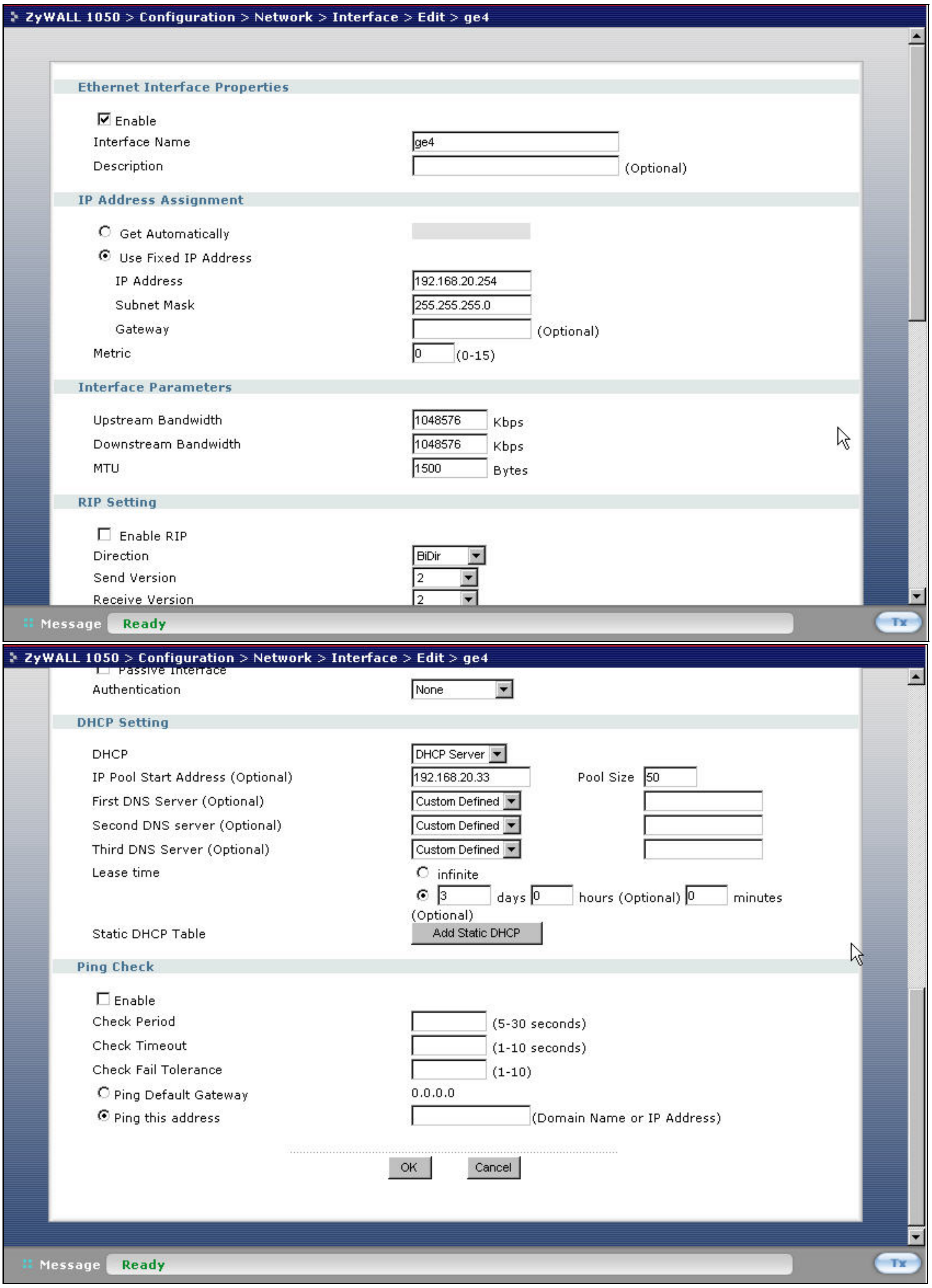
Direction: BiDir

Send Version: 2

Receive Version: 2

Message: Ready

ge4 Fix IP: 192.168.20.254/255.255.255.0 DHCP server



ZyWALL 1050 > Configuration > Network > Interface > Edit > ge4

**Ethernet Interface Properties**

☑ Enable

Interface Name: ge4

Description: (Optional)

**IP Address Assignment**

○ Get Automatically

● Use Fixed IP Address

IP Address: 192.168.20.254

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

Send Version: 2

Receive Version: 2

Message Ready

ZyWALL 1050 > Configuration > Network > Interface > Edit > ge4

□ Passive Interface

Authentication: None

**DHCP Setting**

DHCP: DHCP Server

IP Pool Start Address (Optional): 192.168.20.33 Pool Size: 50

First DNS Server (Optional): Custom Defined

Second DNS server (Optional): Custom Defined

Third DNS Server (Optional): Custom Defined

Lease time: ○ infinite ● 3 days 0 hours (Optional) 0 minutes (Optional)

Static DHCP Table: Add Static DHCP

**Ping Check**

□ Enable

Check Period: (5-30 seconds)

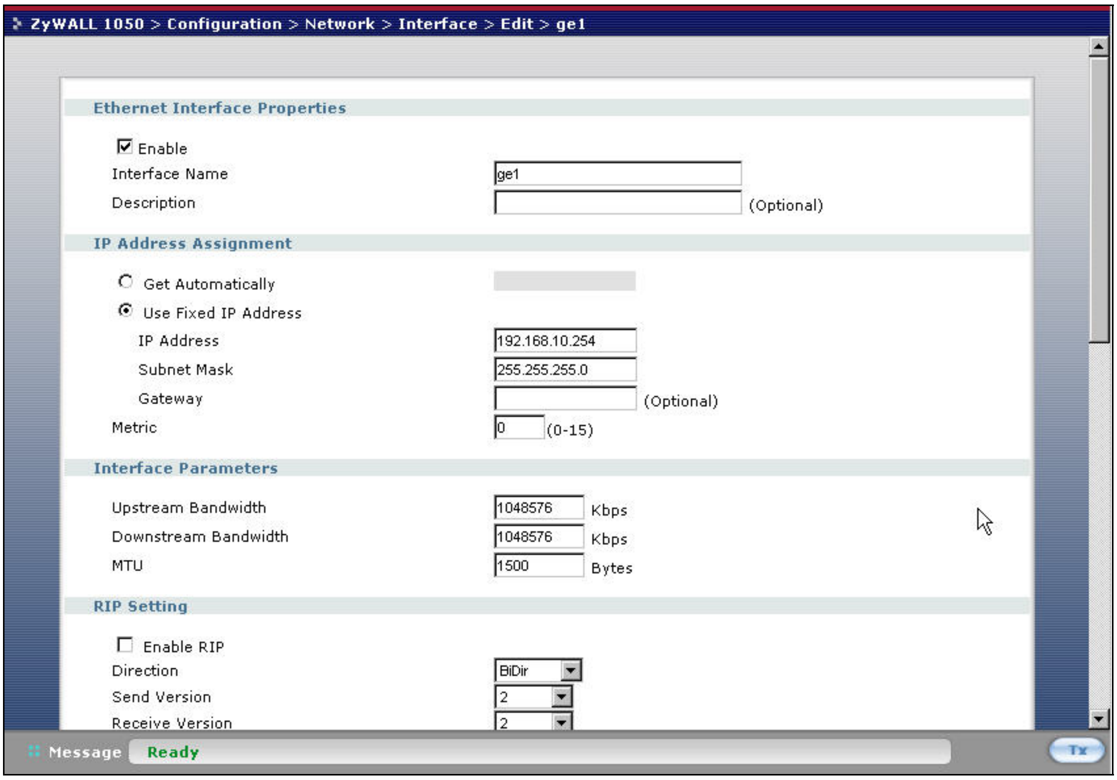
Check Timeout: (1-10 seconds)

Check Fail Tolerance: (1-10)

○ Ping Default Gateway 0.0.0.0

● Ping this address (Domain Name or IP Address)

ge1 Fix IP: 192.168.10.254/255.255.255.0 DHCP server



ZyWALL 1050 > Configuration > Network > Interface > Edit > ge1

**Ethernet Interface Properties**

☑ Enable

Interface Name: ge1

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**

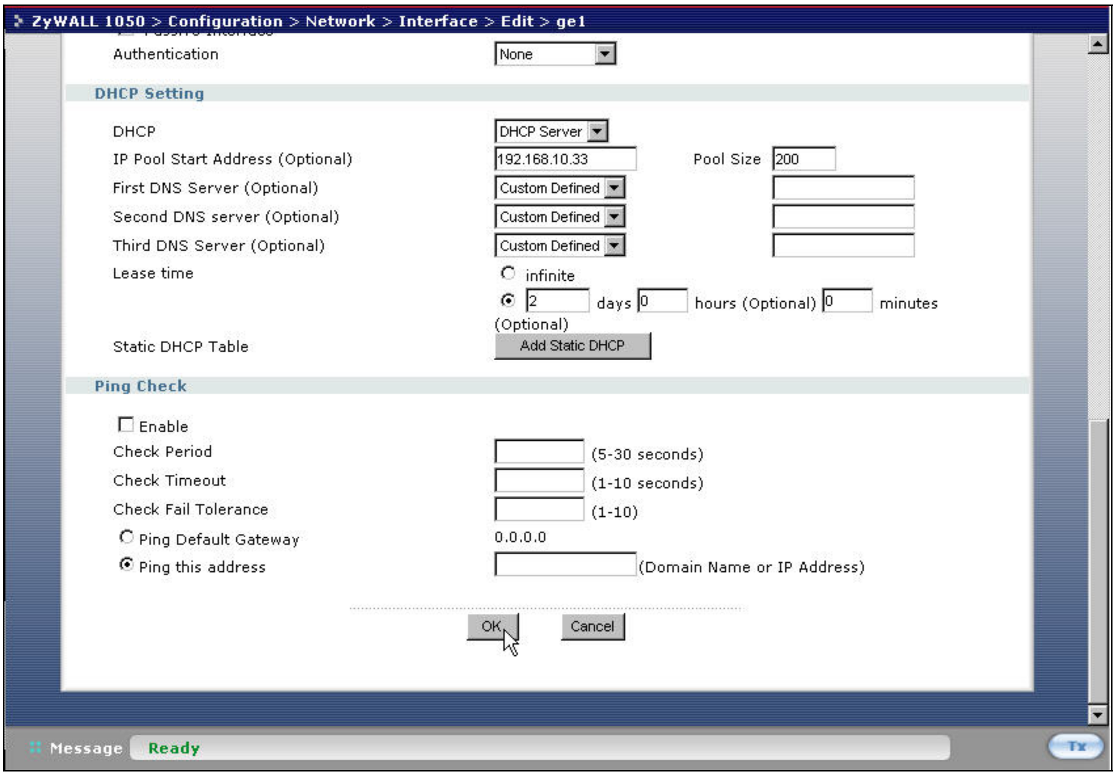
□ Enable RIP

Direction: BiDir

Send Version: 2

Receive Version: 2

Message: Ready



ZyWALL 1050 > Configuration > Network > Interface > Edit > ge1

Authentication: None

**DHCP Setting**

DHCP: DHCP Server

IP Pool Start Address (Optional): 192.168.10.33 Pool Size: 200

First DNS Server (Optional): Custom Defined

Second DNS server (Optional): Custom Defined

Third DNS server (Optional): Custom Defined

Lease time: ○ infinite

● 2 days 0 hours (Optional) 0 minutes (Optional)

Static DHCP Table: Add Static DHCP

**Ping Check**

□ Enable

Check Period: (5-30 seconds)

Check Timeout: (1-10 seconds)

Check Fail Tolerance: (1-10)

○ Ping Default Gateway 0.0.0.0

● Ping this address (Domain Name or IP Address)

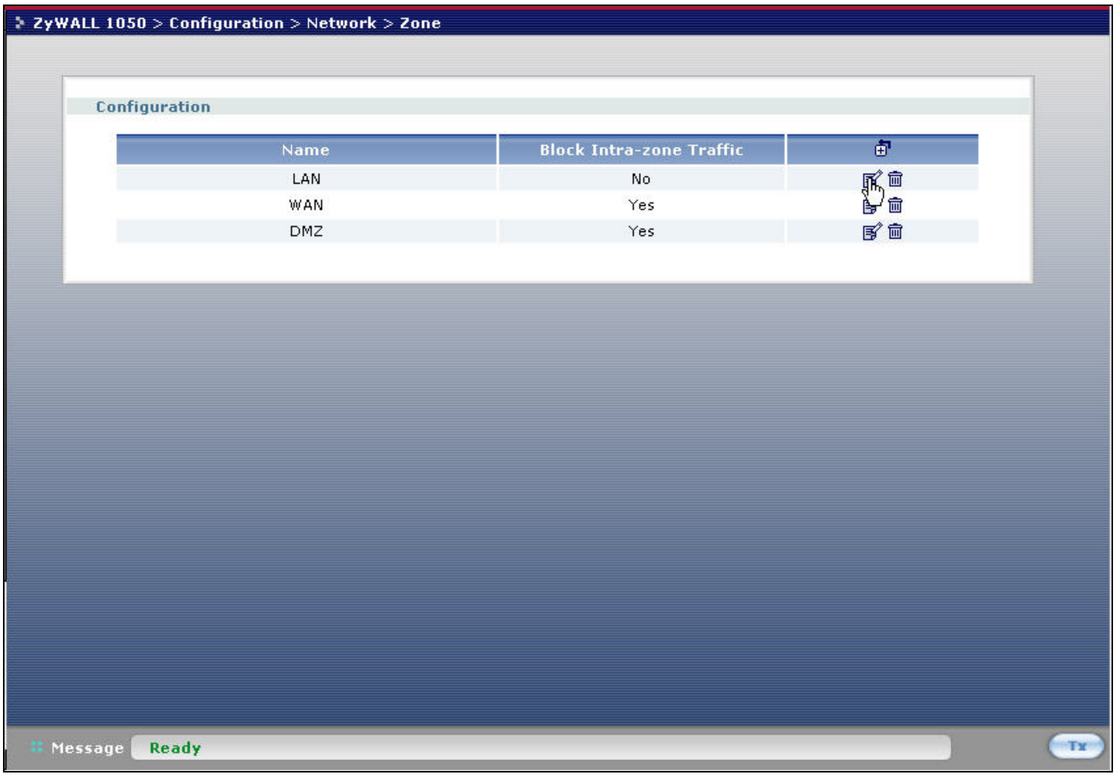
OK Cancel

Message: Ready

User’s pc network connection will disconnect and get the new IP address from ZyWALL 1050 after applying ge1’s new setting.

## 1.2. Configure the interface to correspond Zone

Step1. Switch to ZyWALL 1050 > Configuration > Network > Zone and click the "Edit" icon to modify the setting.



ZyWALL 1050 > Configuration > Network > Zone

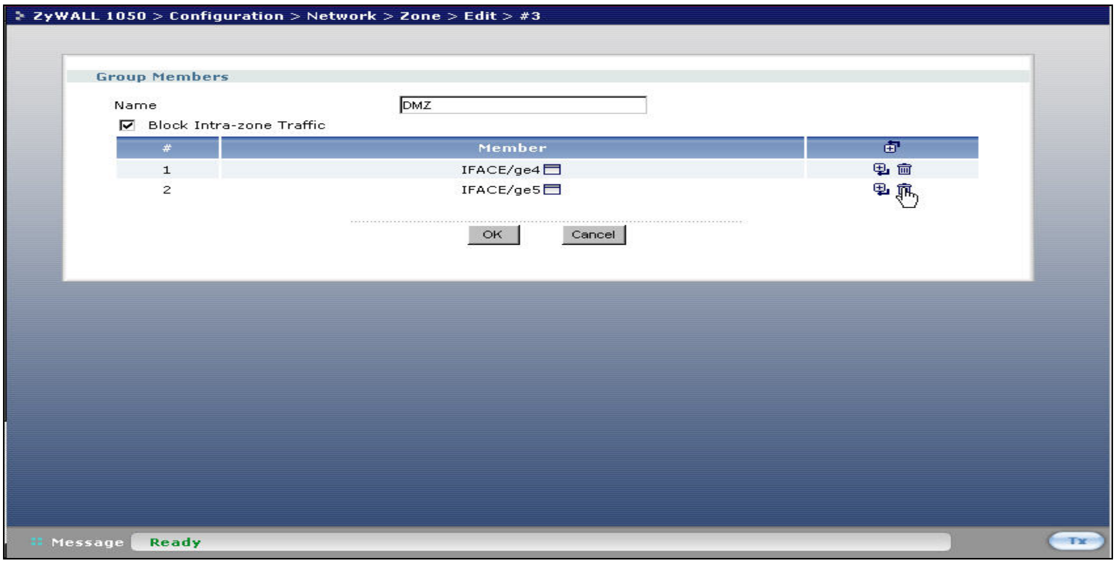
Configuration

| Name | Block Intra-zone Traffic |  |
|---|---|---|
| LAN | No |  |
| WAN | Yes |  |
| DMZ | Yes |  |

Message Ready

Step2. The default setting of ZyWALL 1050 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 binding ge4 and ge5. Thus, we only need to modify the DMZ zone to bind the ge4 only. This is an optional setting that won't affect the whole application.

Click the "Remove" icon to delete ge5 under the DMZ zone.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #3

Group Members

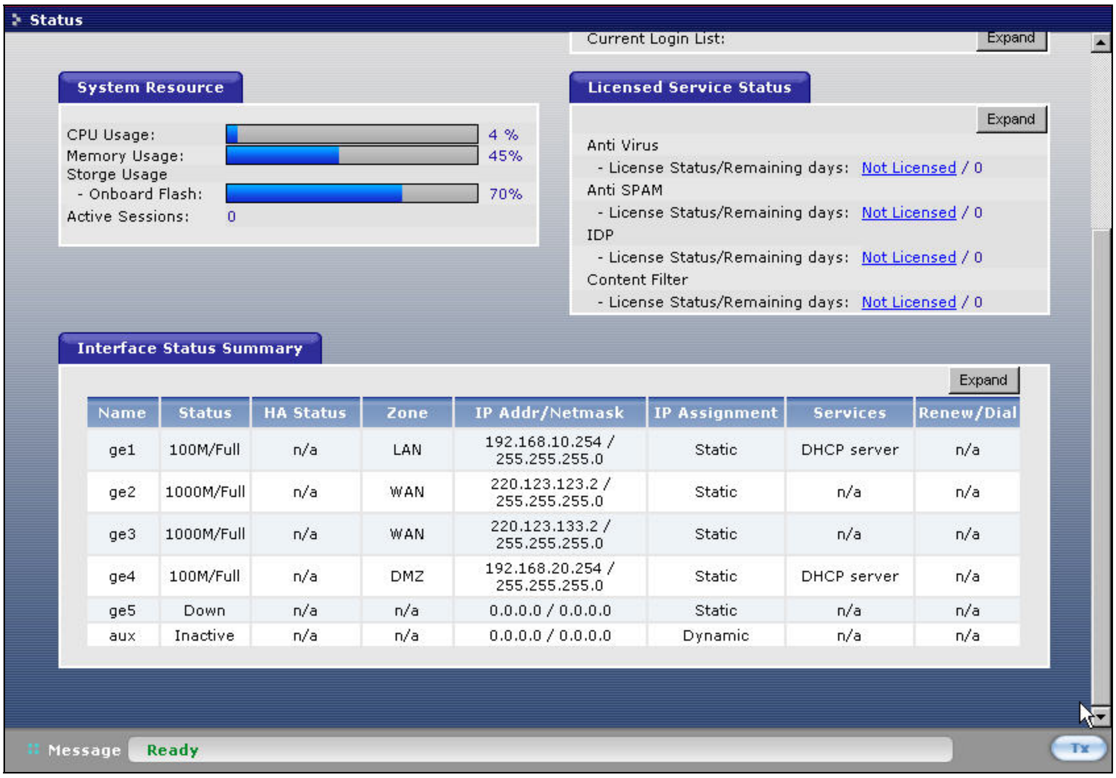
Name DMZ

☑ Block Intra-zone Traffic

| # | Member |  |
|---|---|---|
| 1 | IFACE/ge4 |  |
| 2 | IFACE/ge5 |  |

Message Ready

Step3. Check the interface overview table on the Status page to confirm the settings.



CPU Usage: 4 %
Memory Usage: 45%
Storge Usage
- Onboard Flash: 70%
Active Sessions: 0

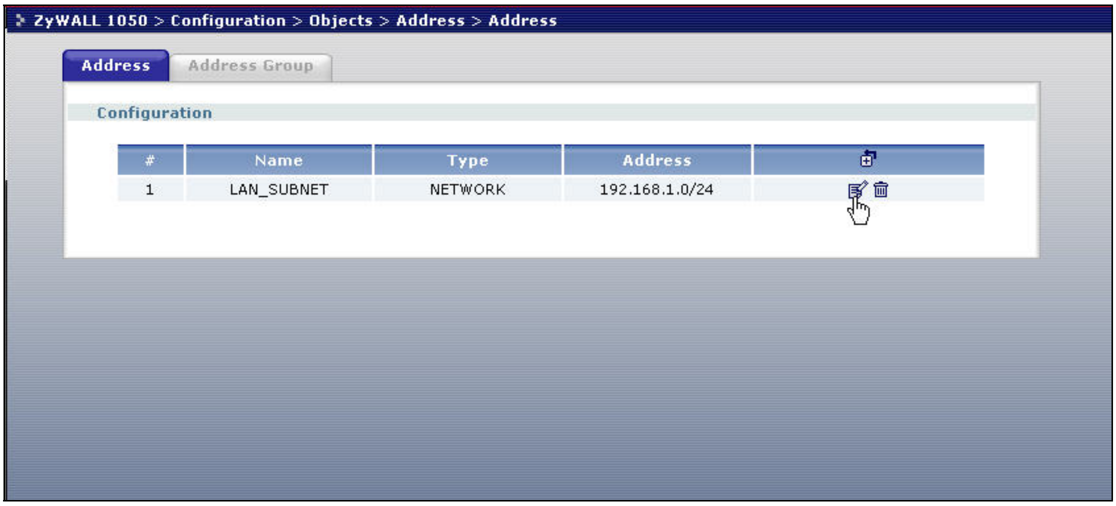
Anti Virus
- License Status/Remaining days: Not Licensed / 0
Anti SPAM
- License Status/Remaining days: Not Licensed / 0
IDP
- License Status/Remaining days: Not Licensed / 0
Content Filter
- License Status/Remaining days: Not Licensed / 0

| 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 | DHCP server | n/a |
| ge2 | 1000M/Full | n/a | WAN | 220.123.123.2 / 255.255.255.0 | Static | n/a | n/a |
| ge3 | 1000M/Full | 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 | DHCP server | n/a |
| ge5 | Down | n/a | n/a | 0.0.0.0 / 0.0.0.0 | Static | n/a | n/a |
| aux | Inactive | n/a | n/a | 0.0.0.0 / 0.0.0.0 | Dynamic | n/a | n/a |

## 1.3. 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 while the corresponding address object is not configured.

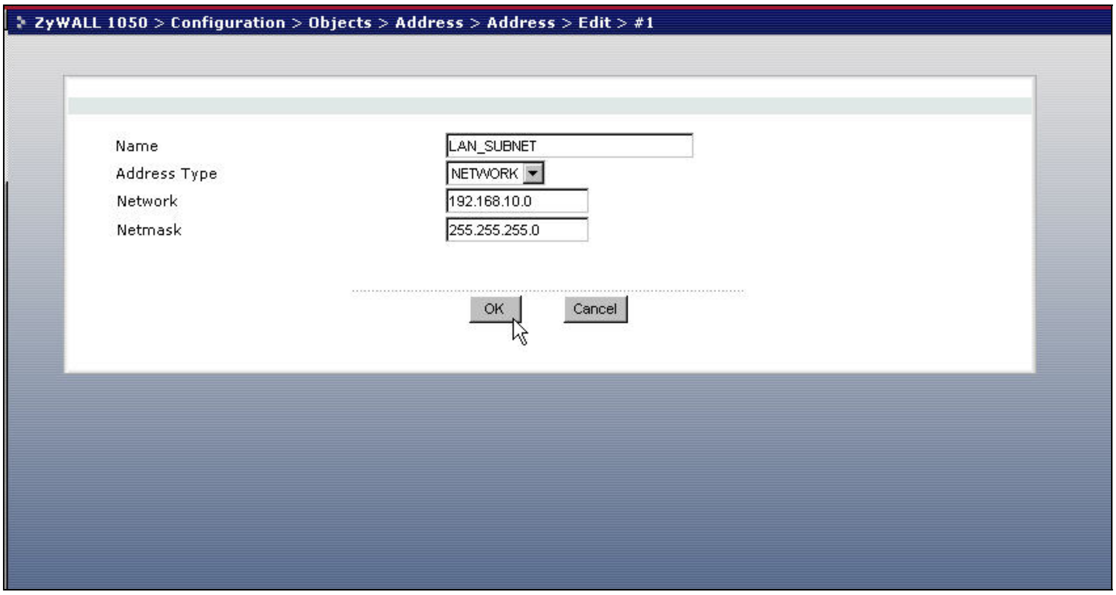
Step1. Switch to ZyWALL 1050 > Configuration > Objects > Address > Address and we will find there is one default LAN_SUBNET address object.



| # | Name | Type | Address | |
|---|---|---|---|---|
| 1 | LAN_SUBNET | NETWORK | 192.168.1.0/24 | |

Change the address from 192.168.1.0 to 192.168.10.0 to configure the new LAN IP. The routing won't work if user changes the default LAN IP address and forgets to modify the

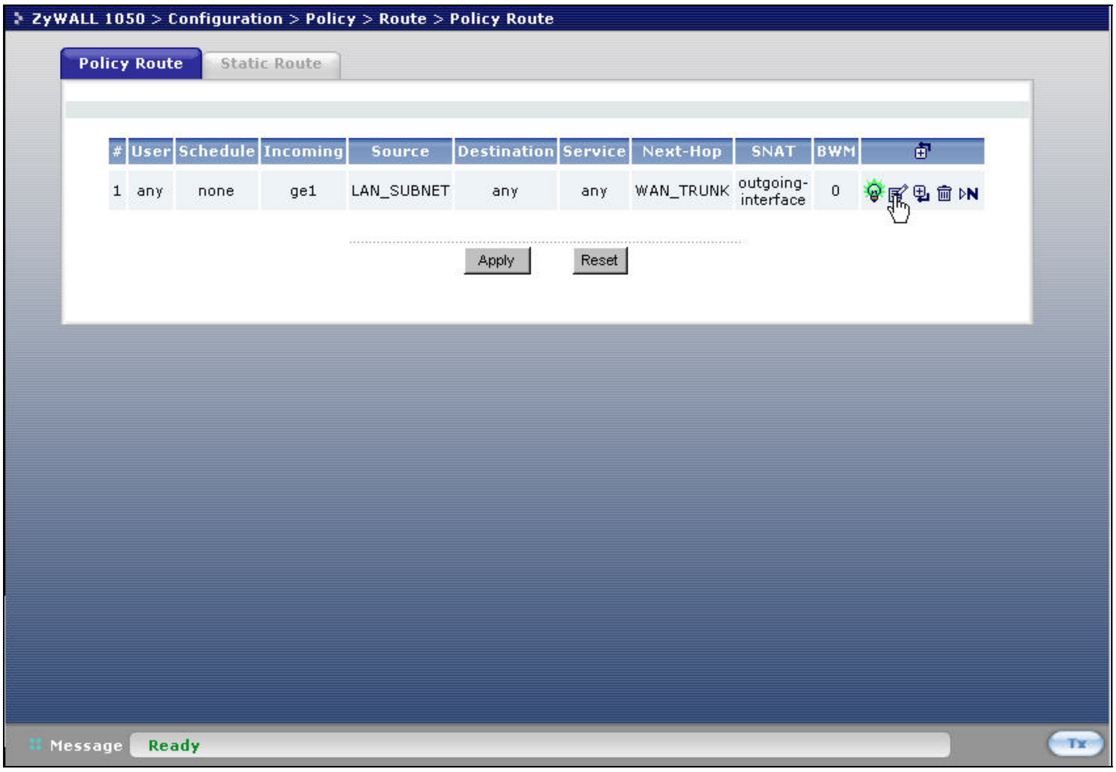
LAN_SUBNET.


ZyWALL 1050 > Configuration > Objects > Address > Address > Edit > #1

| | |
|---|---|
| Name | LAN_SUBNET |
| Address Type | NETWORK |
| Network | 192.168.10.0 |
| Netmask | 255.255.255.0 |

Step.2 ZyWALL 1050 will automatically route the traffic between all connected interfaces. There is one default policy route form LAN for the traffic outgoing to the network behind WAN.

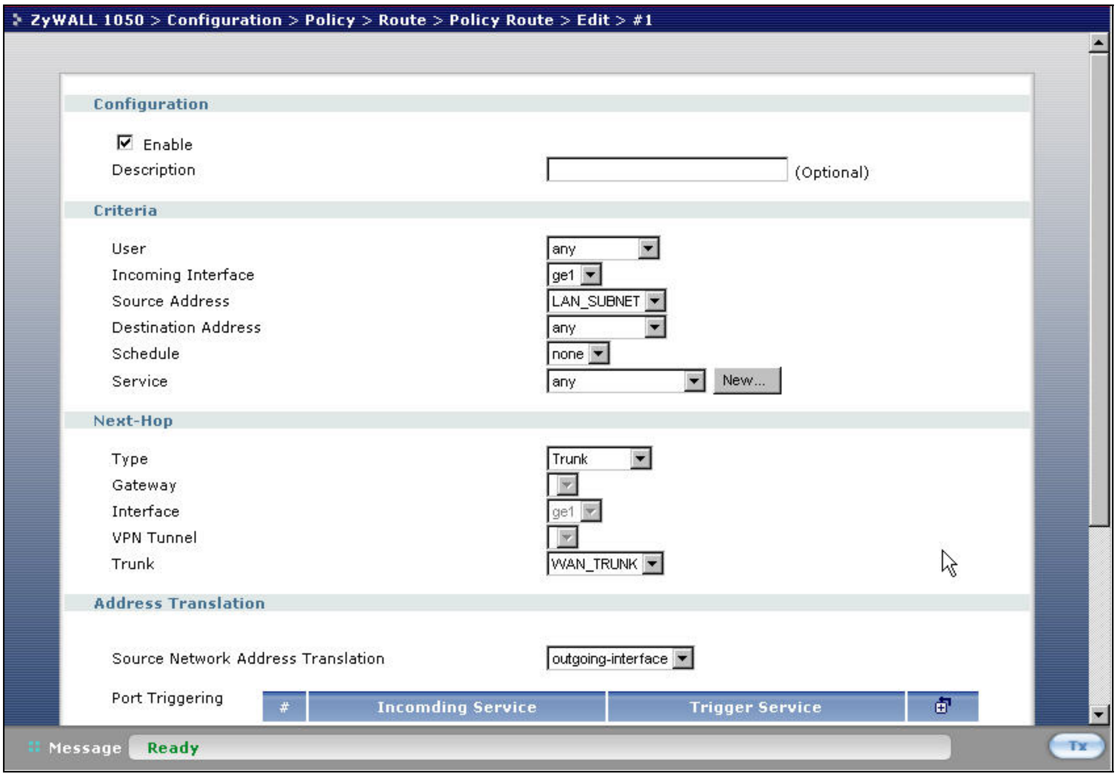
Switch to ZyWALL 1050 > Configuration > Policy > Route > Policy Route or Static Route to check the routing settings.


ZyWALL 1050 > Configuration > Policy > Route > Policy Route

| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 0 | |

Message Ready

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



ZyWALL 1050 > Configuration > Policy > Route > Policy Route > Edit > #1

Configuration

☑ Enable

Description (Optional)

Criteria

|  |  |
|---|---|
| User | any |
| Incoming Interface | ge1 |
| Source Address | LAN_SUBNET |
| Destination Address | any |
| Schedule | none |
| Service | any |

Next-Hop

|  |  |
|---|---|
| Type | Trunk |
| Gateway |  |
| Interface | ge1 |
| VPN Tunnel |  |
| Trunk | WAN_TRUNK |

Address Translation

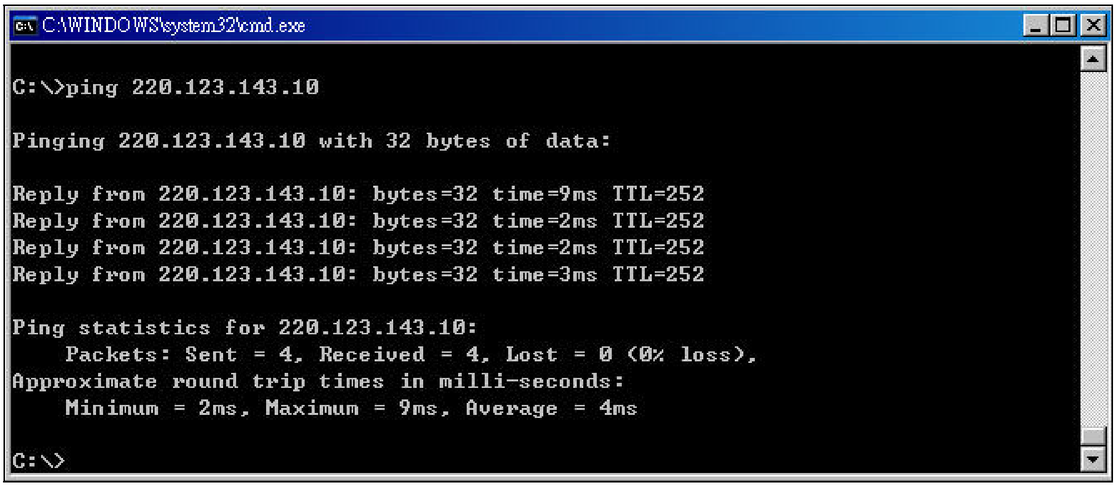
|  |  |
|---|---|
| Source Network Address Translation | outgoing-interface |

Port Triggering

| # | Incomding Service | Trigger Service |  |
|---|---|---|---|

Message Ready

Step4. The PC in ZyWALL 1050 LAN subnet can communicate with the ZyWALL 2 after applying all the routing settings.



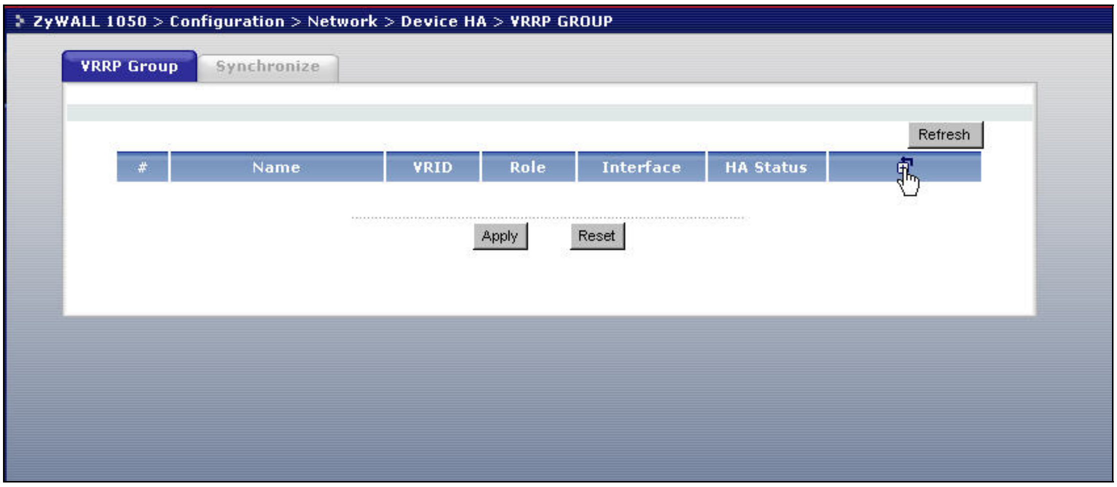
C:\WINDOWS\system32\cmd.exe

```
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:\>
```

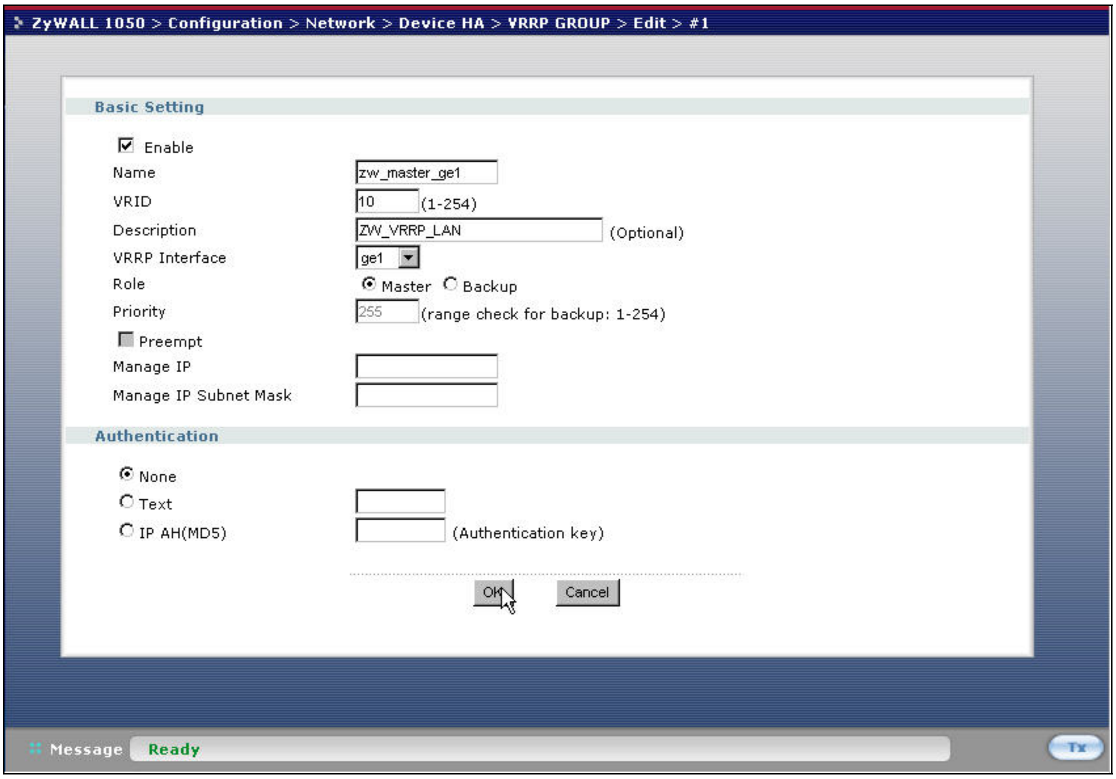
### 1.4. Setup Device HA (Activate-Passive)

We will configure the Device HA setting on master ZyWALL 1050 first. Then we can connect the Backup ZyWALL 1050 cables to L3 and L2 switch and then synchronize the configuration from Master. The Device HA will be ready after this and Backup ZyWALL 1050 will take over when Master ZyWALL 1050 fails.

Step1.Switch to ZyWALL 1050 > Configuration > Network > Device HA > VRRP GROUP and click the “add” icon to add a new VRRP GROUP



Setup the ge1 (LAN) VRRP group


ZyWALL 1050 > Configuration > Network > Device HA > VRRP GROUP > Edit > #1
OK
Cancel
Message
Ready

Basic Setting

☑ Enable

| | |
|---|---|
| Name | zw_master_ge1 |
| VRID | 10 (1-254) |
| Description | ZW_VRRP_LAN (Optional) |
| VRRP Interface | ge1 |
| Role | ● Master ○ Backup |
| Priority | 255 (range check for backup: 1-254) |

□ Preempt

| | |
|---|---|
| Manage IP | |
| Manage IP Subnet Mask | |

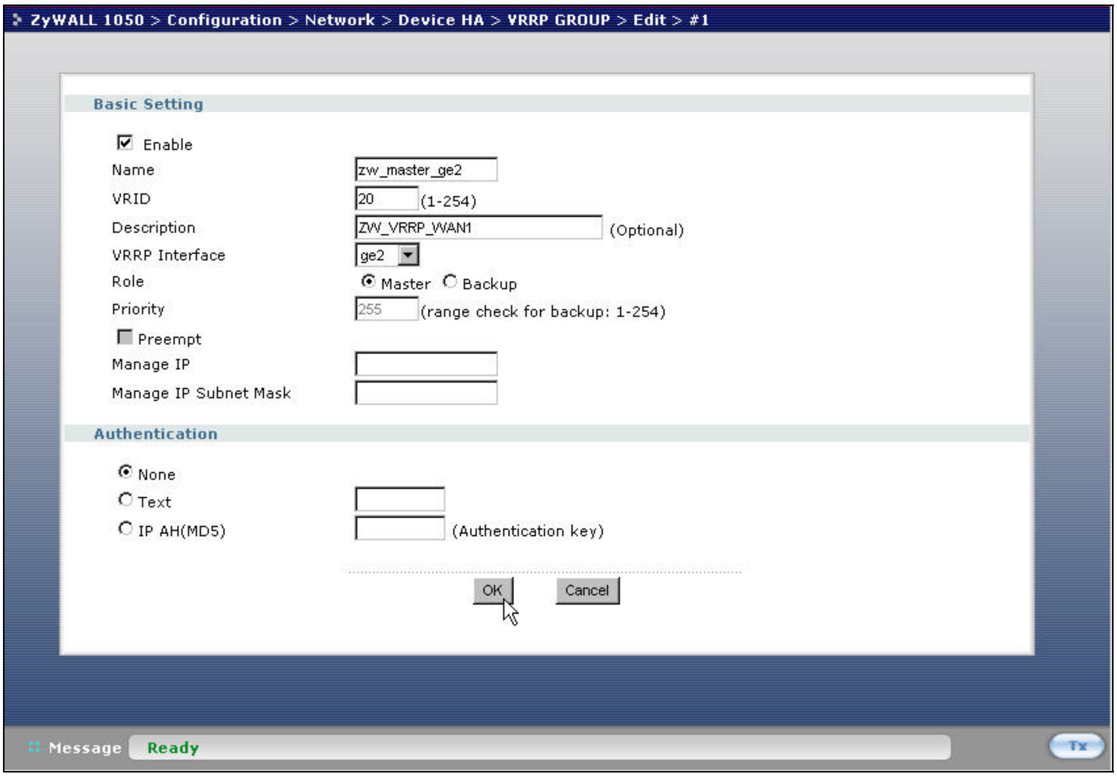
Authentication

● None

○ Text

○ IP AH(MD5) (Authentication key)

Setup the ge2 (WAN1) VRRP group



ZyWALL 1050 > Configuration > Network > Device HA > VRRP GROUP > Edit > #1

**Basic Setting**

☑ Enable

| | |
|---|---|
| Name | zw_master_ge2 |
| VRID | 20 (1-254) |
| Description | ZW_VRRP_WAN1 (Optional) |
| VRRP Interface | ge2 |
| Role | ● Master ○ Backup |
| Priority | 255 (range check for backup: 1-254) |
| □ Preempt | |
| Manage IP | |
| Manage IP Subnet Mask | |

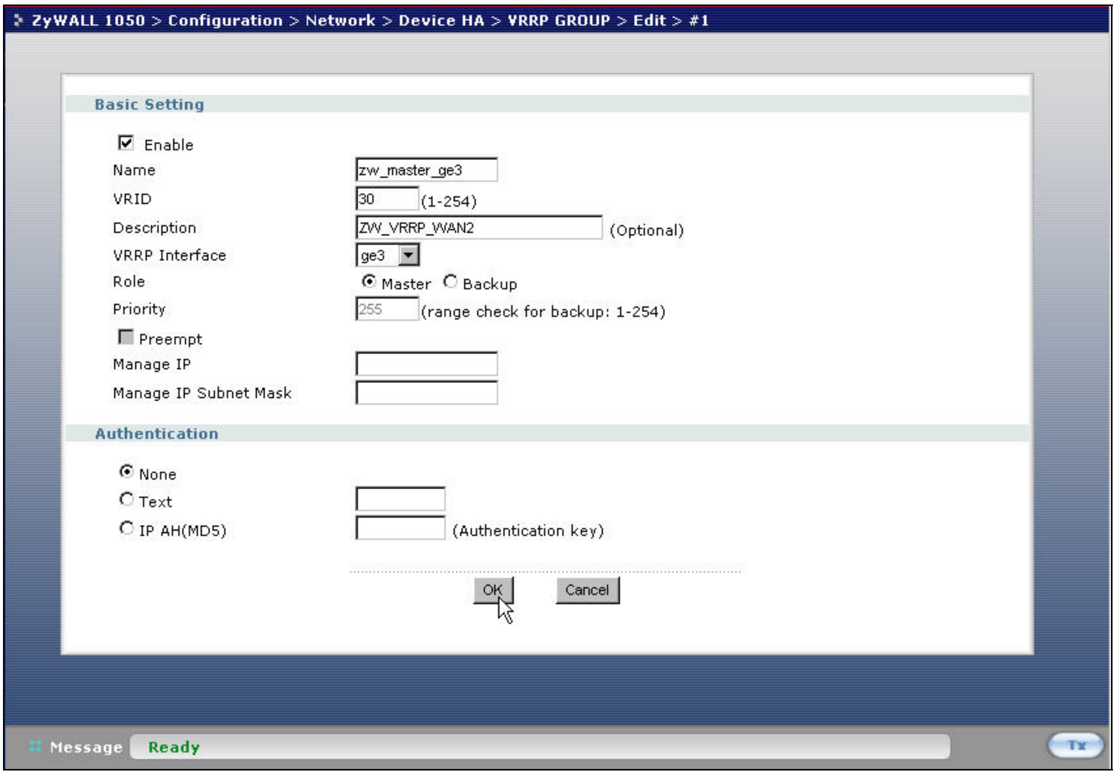
**Authentication**

● None

○ Text

○ IP AH(MD5) (Authentication key)

Setup the ge3 (WAN2) VRRP group



ZyWALL 1050 > Configuration > Network > Device HA > VRRP GROUP > Edit > #1

**Basic Setting**

☑ Enable

| | |
|---|---|
| Name | zw_master_ge3 |
| VRID | 30 (1-254) |
| Description | ZW_VRRP_WAN2 (Optional) |
| VRRP Interface | ge3 |
| Role | ● Master ○ Backup |
| Priority | 255 (range check for backup: 1-254) |
| □ Preempt | |
| Manage IP | |
| Manage IP Subnet Mask | |

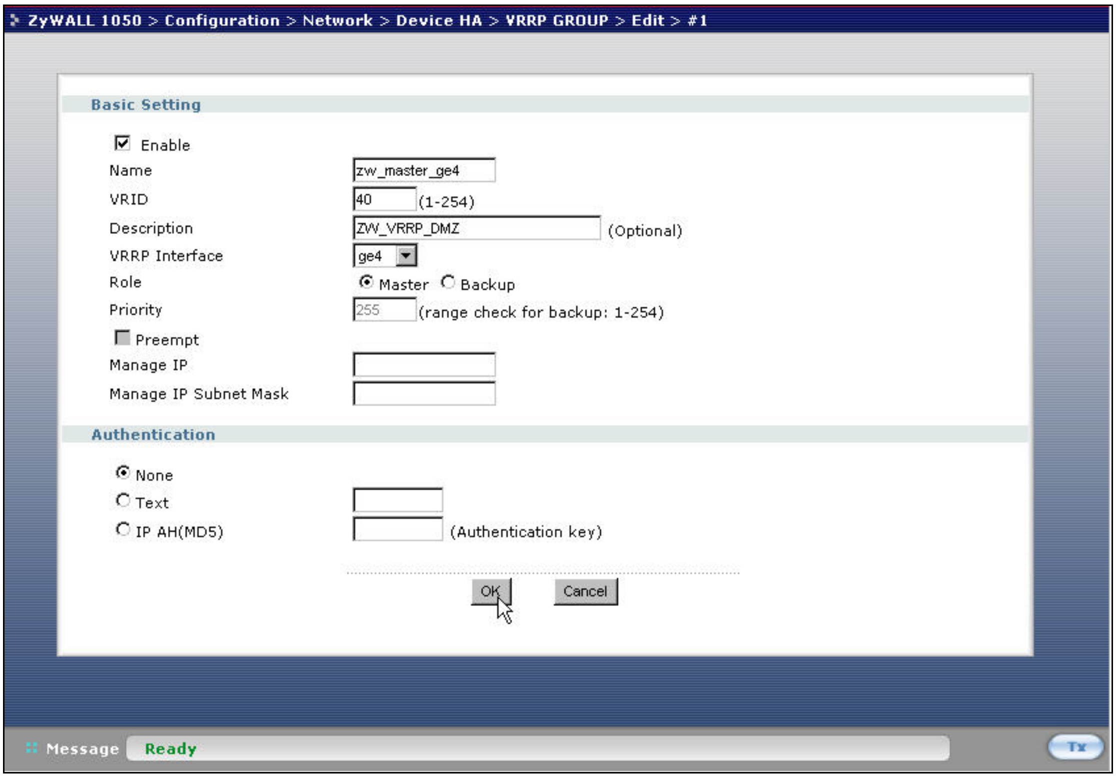
**Authentication**

● None

○ Text

○ IP AH(MD5) (Authentication key)

Setup the ge4 (DMZ) VRRP group



ZyWALL 1050 > Configuration > Network > Device HA > VRRP GROUP > Edit > #1

Basic Setting

☑ Enable

| | |
|---|---|
| Name | zw_master_ge4 |
| VRID | 40 (1-254) |
| Description | ZW_VRRP_DMZ (Optional) |
| VRRP Interface | ge4 |
| Role | ● Master ○ Backup |
| Priority | 255 (range check for backup: 1-254) |

□ Preempt

| | |
|---|---|
| Manage IP | |
| Manage IP Subnet Mask | |

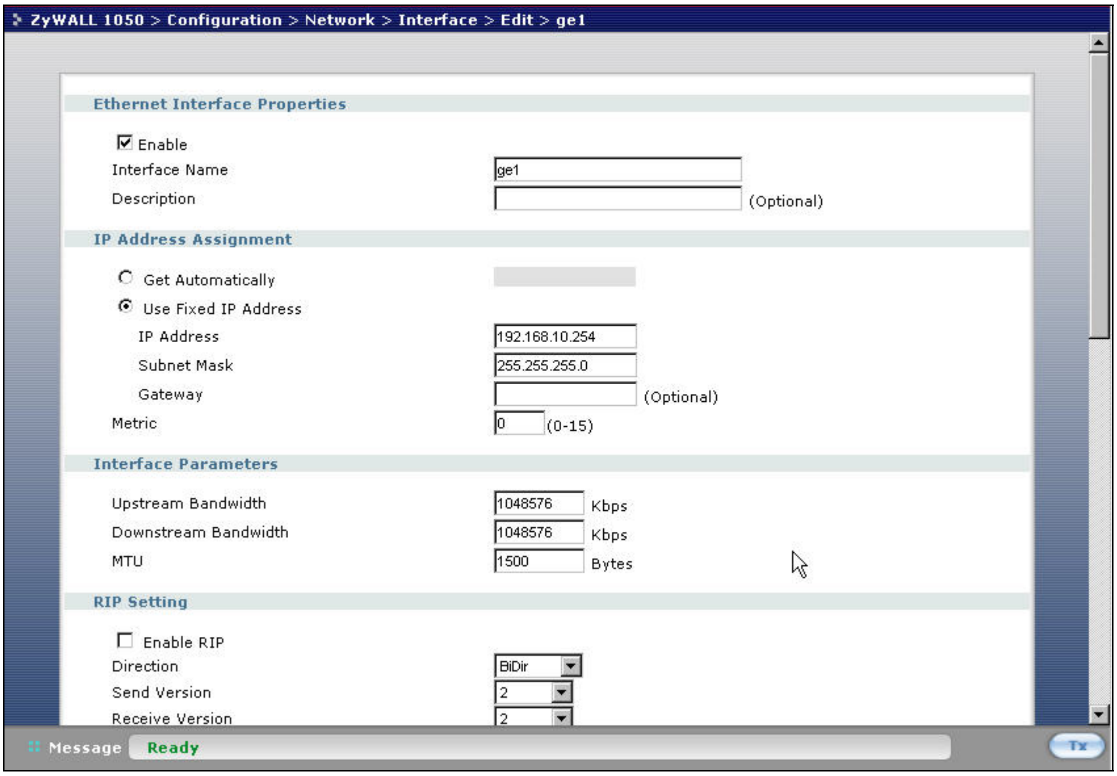
Authentication

● None

○ Text

○ IP AH(MD5) (Authentication key)

Step2. Connect the PC to Backup ZyWALL 1050 ge1 and the PC should be dispatched an IP address from the device. User can login to the Backup ZyWALL 1050 and configure the Backup Device HA setting. We have to set the ge1 interface IP setting as Master ZyWALL 1050 ge1. Then we can setup the Backup ZyWALL 1050 management IP address in the same LAN subnet.



ZyWALL 1050 > Configuration > Network > Interface > Edit > ge1

Ethernet Interface Properties

☑ Enable

Interface Name: ge1

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

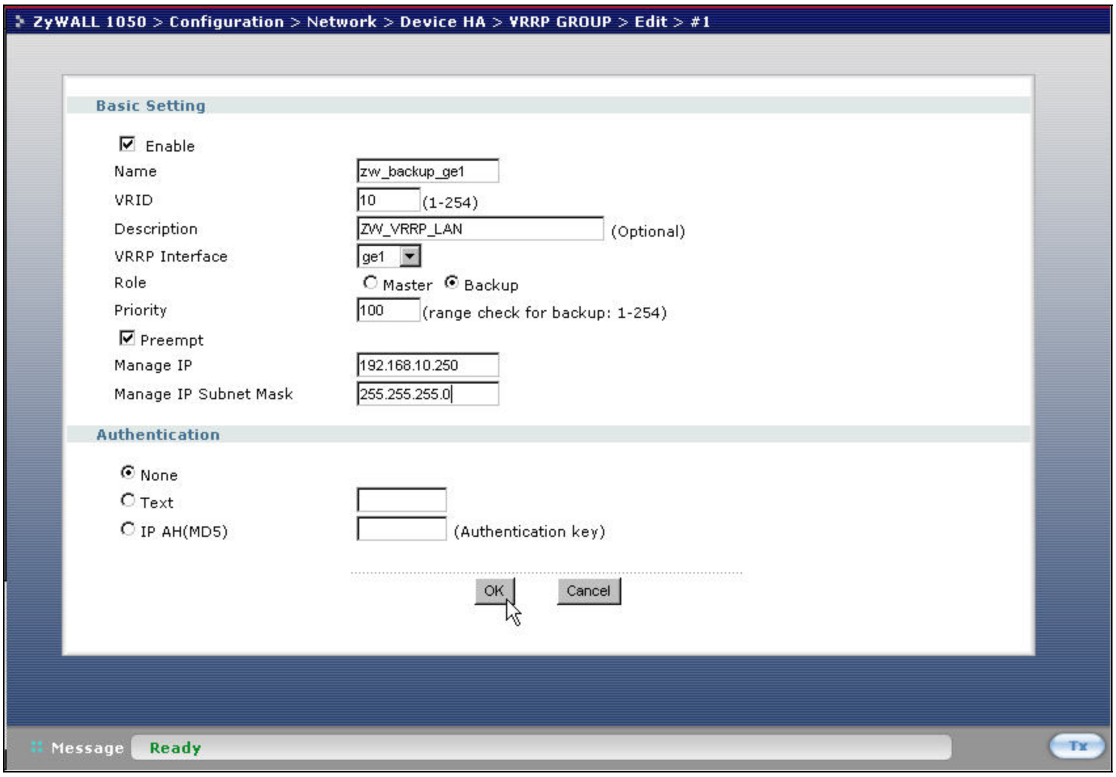
Direction: BiDir

Send Version: 2

Receive Version: 2

Message: Ready

Step3. PC will get a new IP address after updating the ge1 interface setting. Login to the Backup ZyWALL 1050 and switch to ZyWALL 1050 > Configuration > Network > Device HA > VRRP GROUP. Then click the ”add” icon to add a VRRP group. Between Master and Backup Role, the difference in settings is the Management IP configuration. The Backup ZyWALL 1050 will copy all settings from the Master one so we need a management IP to access and configure the Backup ZyWALL 1050.



ZyWALL 1050 > Configuration > Network > Device HA > VRRP GROUP > Edit > #1

**Basic Setting**

☑ Enable

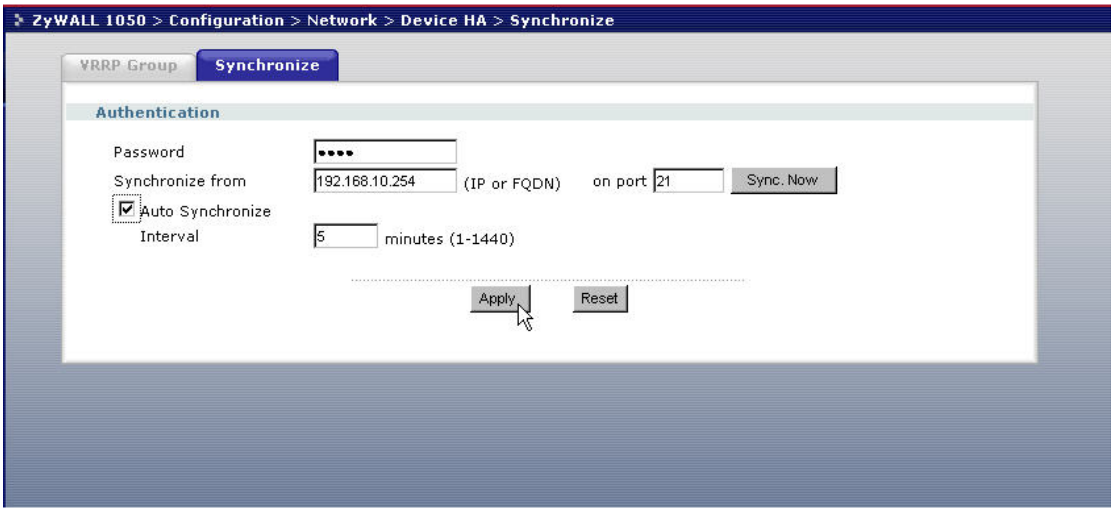
| | |
|---|---|
| Name | zw_backup_ge1 |
| VRID | 10 (1-254) |
| Description | ZW_VRRP_LAN (Optional) |
| VRRP Interface | ge1 |
| Role | ○ Master ● Backup |
| Priority | 100 (range check for backup: 1-254) |
| ☑ Preempt | |
| Manage IP | 192.168.10.250 |
| Manage IP Subnet Mask | 255.255.255.0 |

**Authentication**

● None
○ Text
○ IP AH(MD5) (Authentication key)

Step4. Unplug the PC cable from Backup ZyWALL 1050 ge1 and plug it back to L2 switch LAN segment. Connect all the cables from L2 and L3 switches to the Backup ZyWALL 1050 as on the network topology diagram shown on the index page. Login to Backup ZyWALL 1050 via management IP. Now we can synchronize the configuration from the Master to the Backup.

Switch to ZyWALL 1050 > Configuration > Network > Device HA > Synchronize and enter the Master ZyWALL 1050 admin account password..Input the LAN IP address of the Master ZyWALL 1050 in the “Synchronize from” option and set the auto synchronize interval. Then click the “Apply” button to save the configuration.



ZyWALL 1050 > Configuration > Network > Device HA > Synchronize

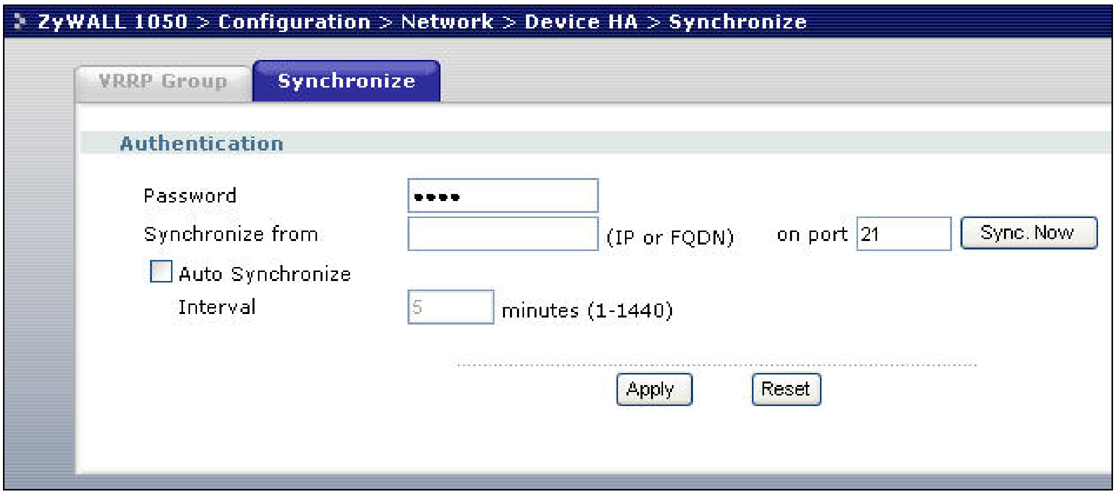
**Authentication**

| | |
|---|---|
| Password | •••• |
| Synchronize from | 192.168.10.254 (IP or FQDN) on port 21 |
| ☑ Auto Synchronize Interval | 5 minutes (1-1440) |

Step5. Switch to “Synchronize” page again and click the “Sync. NOW” button to

synchronize the configuration from the Master to the Backup.

Note: Don't check the "Auto Synchronize" since there is a bug related.



ZyWALL 1050 > Configuration > Network > Device HA > Synchronize

Authentication

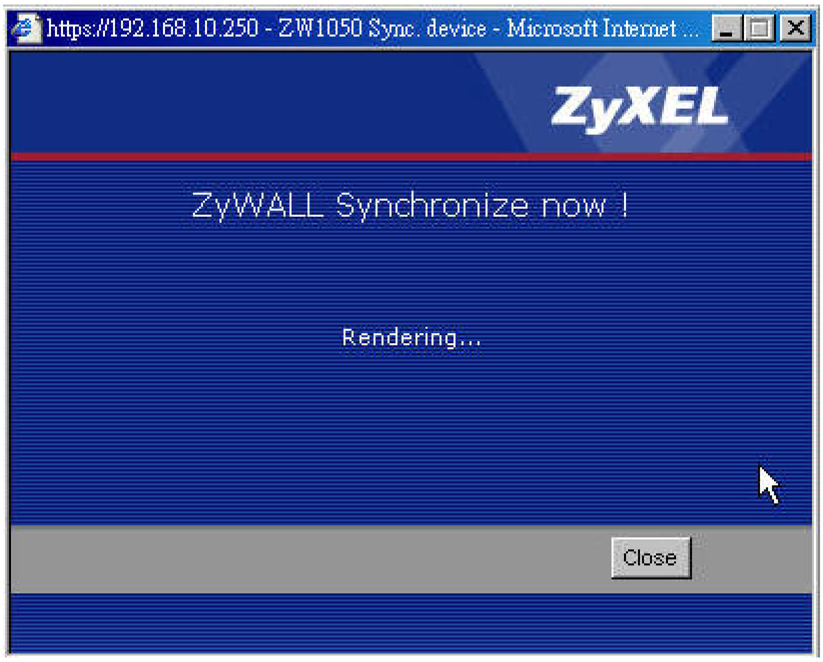
Password: ••••

Synchronize from: (IP or FQDN) on port 21

□ Auto Synchronize

Interval: 5 minutes (1-1440)

Sync process in action

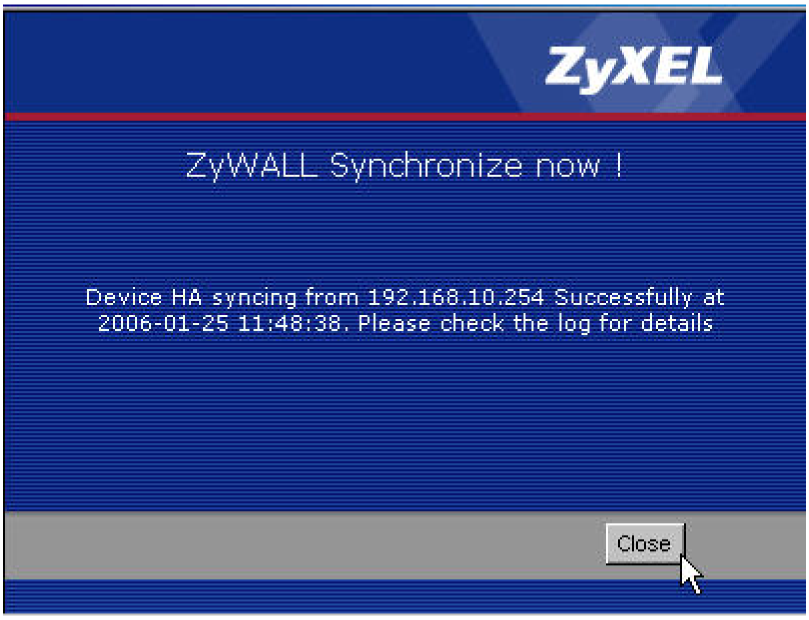


https://192.168.10.250 - ZW1050 Sync. device - Microsoft Internet ...

ZyWALL Synchronize now !

Rendering...

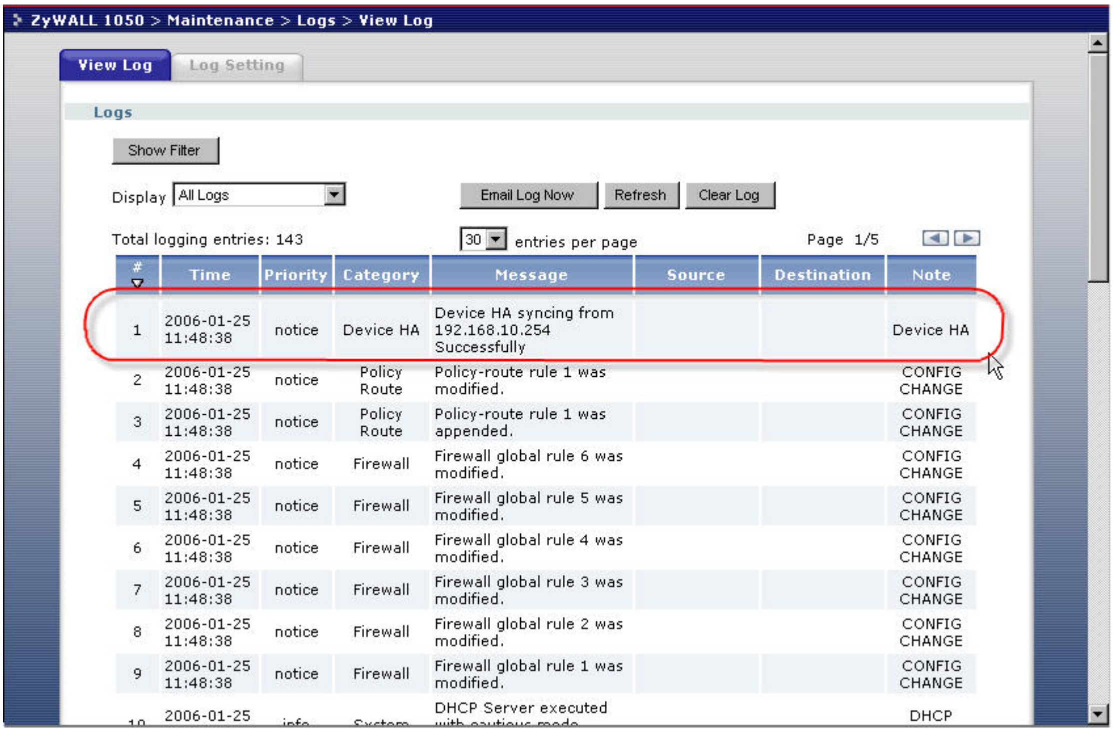
Sync successful notification window



ZyWALL Synchronize now !

Device HA syncing from 192.168.10.254 Successfully at 2006-01-25 11:48:38. Please check the log for details

Switch to ZyWALL 1050 > Maintenance > Logs > View Log to check the log record.



Display All Logs

Total logging entries: 143

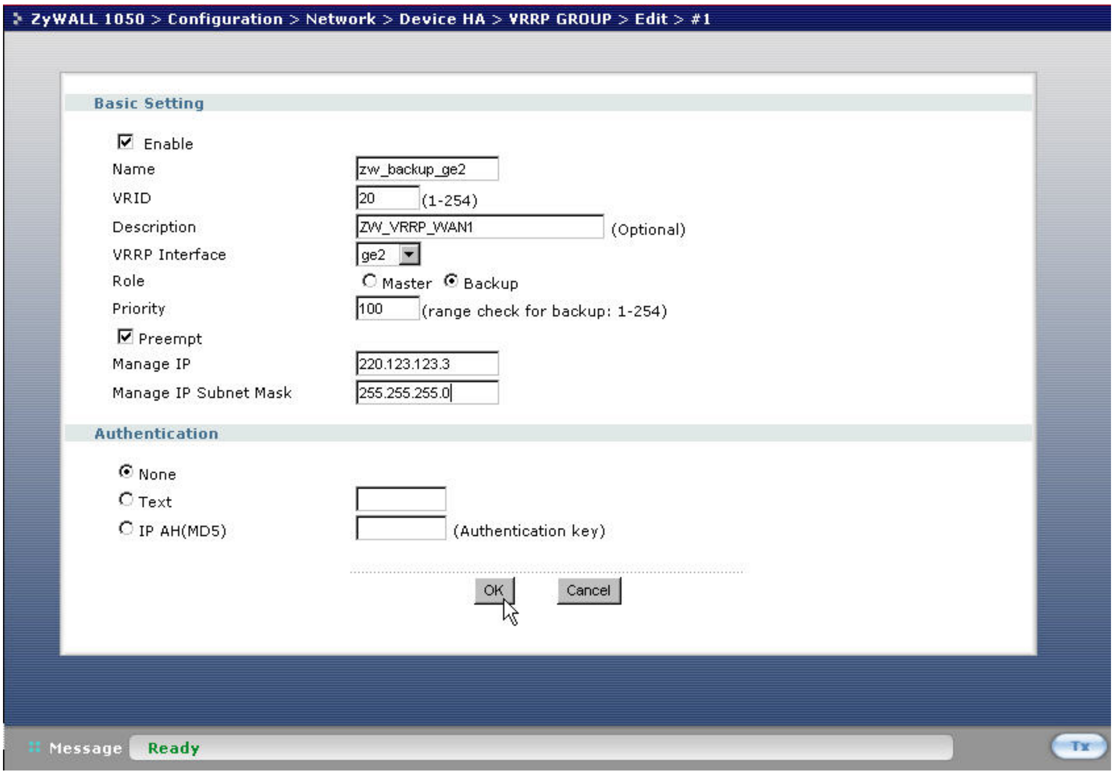
30 entries per page

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 1050's configuration has been synchronized to Backup ZyWALL 1050 and we can continue to setup the rest three VRRP group.

Setup the ge2 (WAN1) VRRP group



ZyWALL 1050 > Configuration > Network > Device HA > VRRP GROUP > Edit > #1

**Basic Setting**

☑ Enable

| | |
|---|---|
| Name | zw_backup_ge2 |
| VRID | 20 (1-254) |
| Description | ZW_VRRP_WAN1 (Optional) |
| VRRP Interface | ge2 |
| Role | ○ Master ● Backup |
| Priority | 100 (range check for backup: 1-254) |

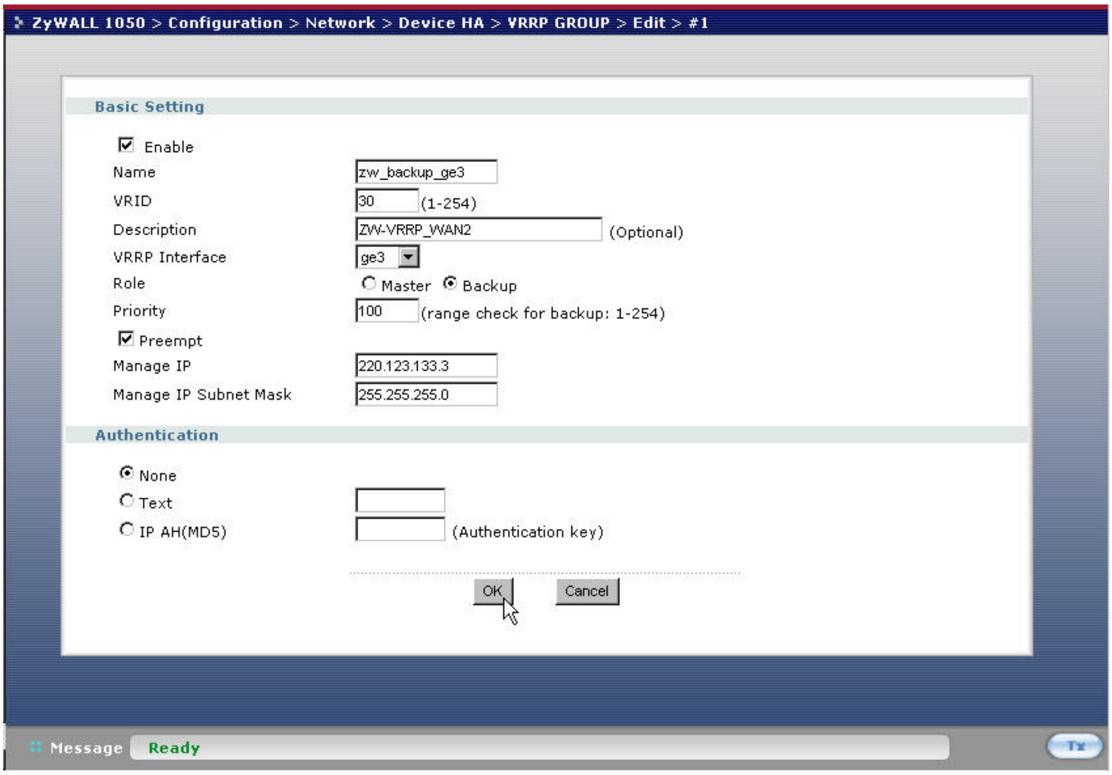
☑ Preempt

| | |
|---|---|
| Manage IP | 220.123.123.3 |
| Manage IP Subnet Mask | 255.255.255.0 |

**Authentication**

● None
○ Text
○ IP AH(MD5) (Authentication key)

Setup the ge3 (WAN2) VRRP group



ZyWALL 1050 > Configuration > Network > Device HA > VRRP GROUP > Edit > #1

**Basic Setting**

☑ Enable

| | |
|---|---|
| Name | zw_backup_ge3 |
| VRID | 30 (1-254) |
| Description | ZW-VRRP_WAN2 (Optional) |
| VRRP Interface | ge3 |
| Role | ○ Master ● Backup |
| Priority | 100 (range check for backup: 1-254) |

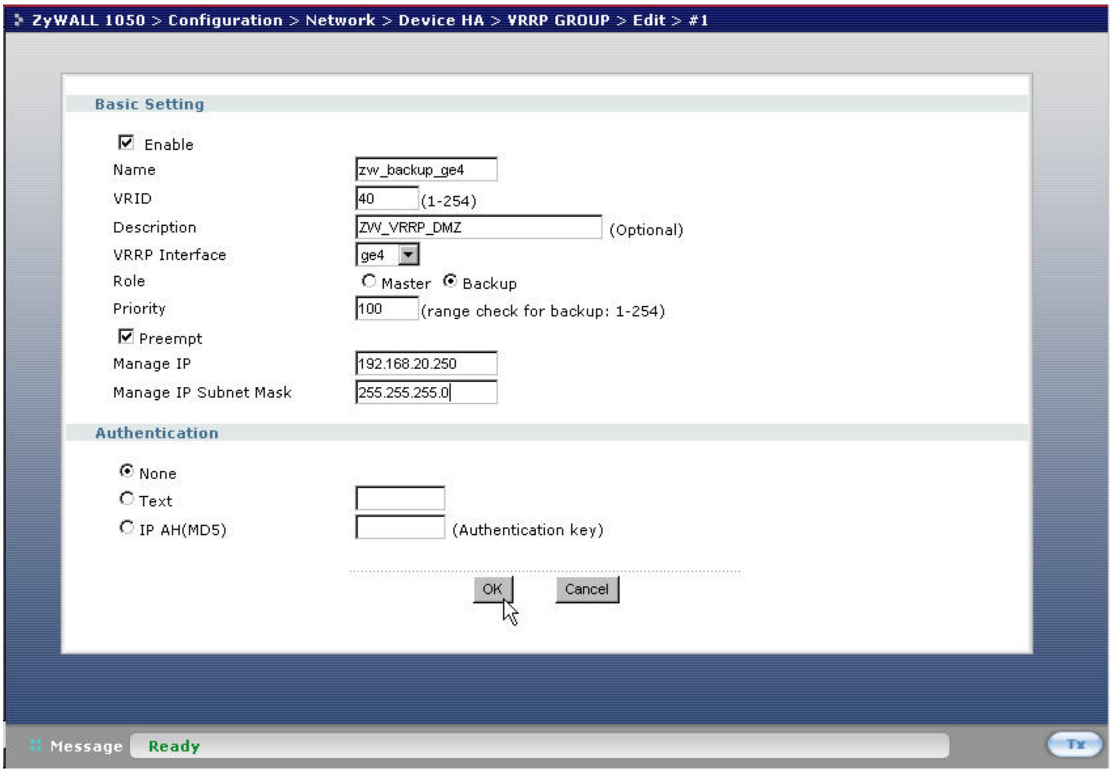
☑ Preempt

| | |
|---|---|
| Manage IP | 220.123.133.3 |
| Manage IP Subnet Mask | 255.255.255.0 |

**Authentication**

● None
○ Text
○ IP AH(MD5) (Authentication key)

Setup the ge4 (DMZ) VRRP group



ZyWALL 1050 > Configuration > Network > Device HA > VRRP GROUP > Edit > #1

Basic Setting

☑ Enable

| | |
|---|---|
| Name | zw_backup_ge4 |
| VRID | 40 (1-254) |
| Description | ZW_VRRP_DMZ (Optional) |
| VRRP Interface | ge4 |
| Role | ○ Master ● Backup |
| Priority | 100 (range check for backup: 1-254) |
| ☑ Preempt | |
| Manage IP | 192.168.20.250 |
| Manage IP Subnet Mask | 255.255.255.0 |

Authentication

● None
○ Text
○ IP AH(MD5) (Authentication key)

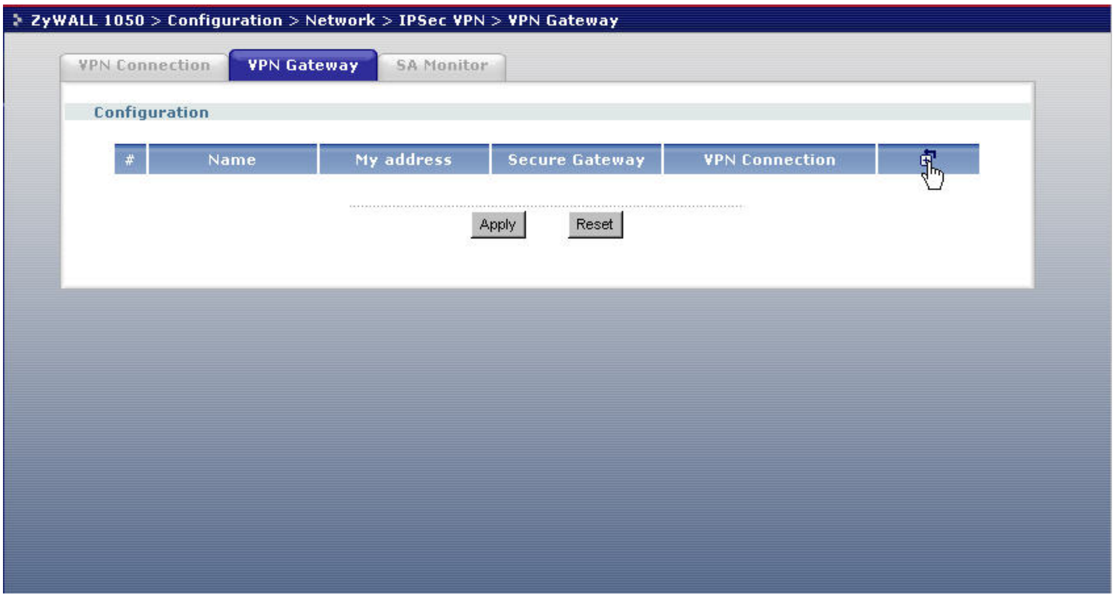
After these steps, the Device HA configuration is done.

### 1.7.2 VPN HA

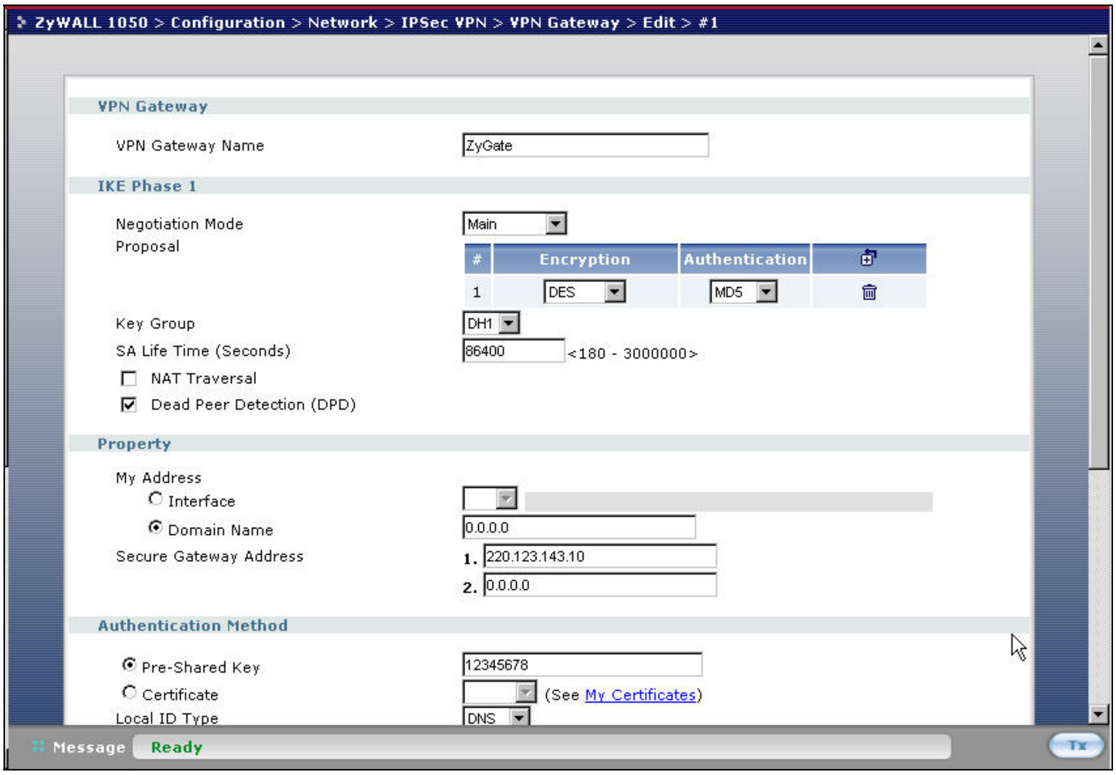
The VPN HA can ensure the availability of VPN demanded. A redundant remote gateway option is added to achieve the goal of availability. It means the device will try connecting to the redundant gateway if the connection to the primary remote gateway is unreachable.

Step1. Setup the VPN at Master ZyWALL 1050

Switch to ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway and click the “Add” icon to add a VPN gateway.



Step2. Setup the VPN Gateway. The ZyWALL 2 VPN parameter configuration has to match the setting shown here. As My Address, we use Domain Name 0.0.0.0 defining a dynamic source as this VPN gateway will be accepting the traffic from ge2 (WAN1) and ge3 (WAN2).


ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway > Edit > #1

VPN Gateway

VPN Gateway Name: ZyGate

IKE Phase 1

Negotiation Mode: Main

Proposal:

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | MD5 |

Key Group: DH1

SA Life Time (Seconds): 86400 <180 - 3000000>

☐ NAT Traversal

☑ Dead Peer Detection (DPD)

Property

My Address
○ Interface
● Domain Name: 0.0.0.0

Secure Gateway Address: 1. 220.123.143.10 2. 0.0.0.0

Authentication Method

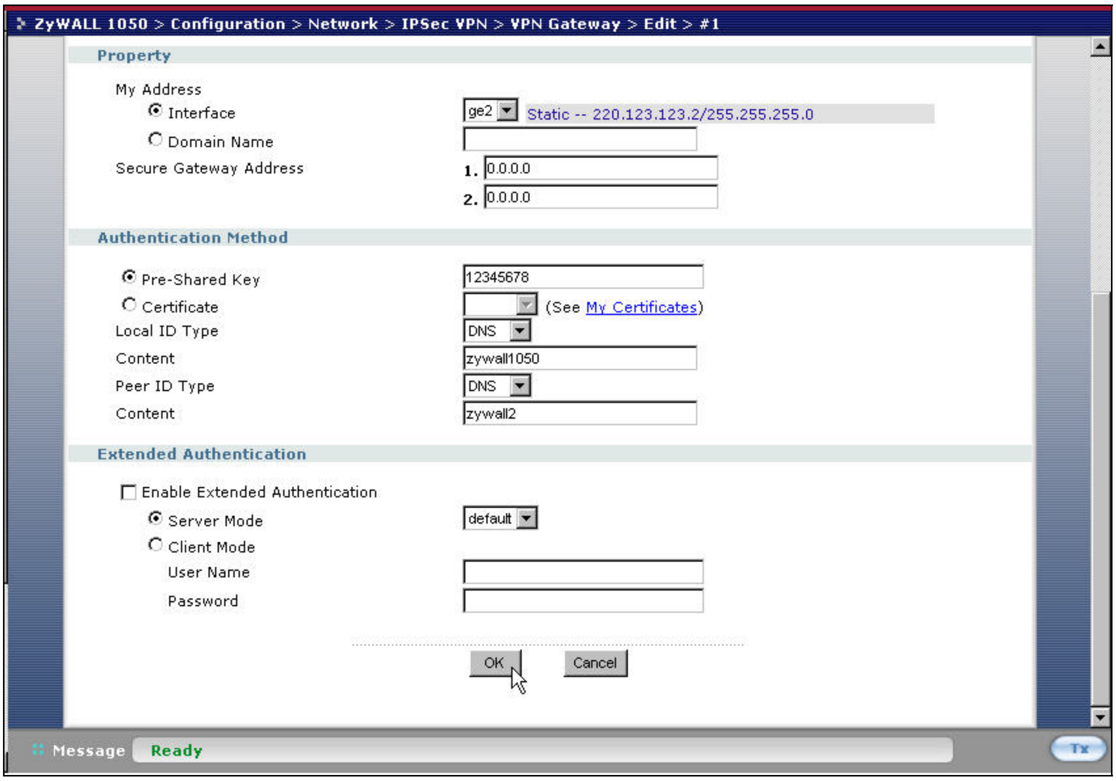
● Pre-Shared Key: 12345678

○ Certificate (See My Certificates)

Local ID Type: DNS

Message: Ready

Setup the DNS ”ZyWALL 1050” and “ZyWALL 2”as Local and Peer ID type.



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway > Edit > #1

**Property**

My Address
● Interface: ge2 — Static -- 220.123.123.2/255.255.255.0
○ Domain Name:
Secure Gateway Address: 1. 0.0.0.0 2. 0.0.0.0

**Authentication Method**

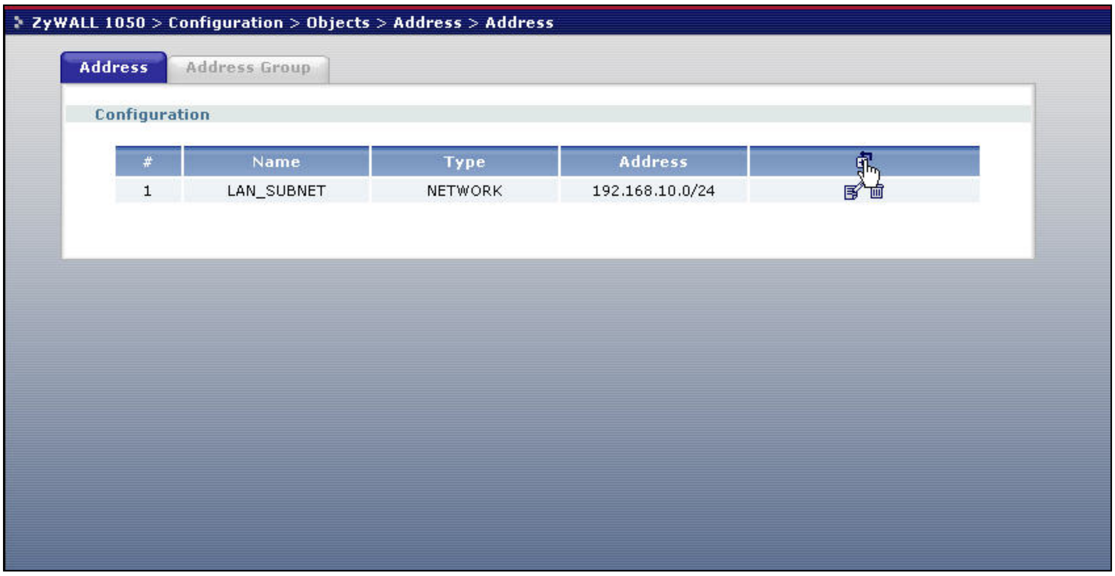
● Pre-Shared Key: 12345678
○ Certificate: (See My Certificates)
Local ID Type: DNS
Content: zywall1050
Peer ID Type: DNS
Content: zywall2

**Extended Authentication**

□ Enable Extended Authentication
● Server Mode: default
○ Client Mode
User Name:
Password:

Step3. We have to add the local and remote address policy in the address **object** first. Then we can configure these address objects in VPN connection settings. We will use the LAN subnet and the DMZ subnet as a VPN local policy and we also need to add the address object for a remote subnet.

Switch to ZyWALL 1050 > Configuration > Objects > Address > Address and we will find the LAN subnet already setup and we need to click the “Add” icon to add one more address object.

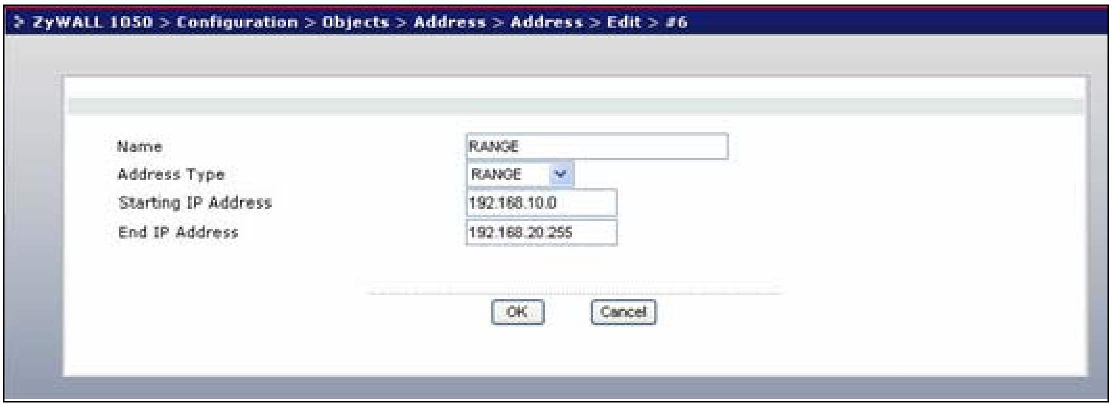


ZyWALL 1050 > Configuration > Objects > Address > Address

**Configuration**

| # | Name | Type | Address | |
|---|---|---|---|---|
| 1 | LAN_SUBNET | NETWORK | 192.168.10.0/24 | |

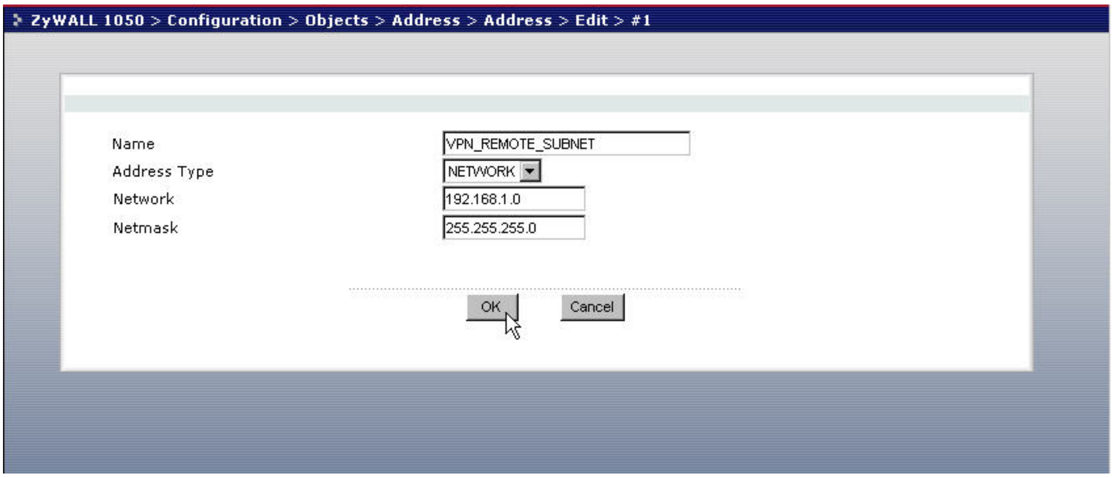
Set the range to 192.168.10.0 ~ 192.168.20.255 including LAN and DMZ subnets as ‘RANGE’ address objects.



ZyWALL 1050 > Configuration > Objects > Address > Address > Edit > #6

| | |
|---|---|
| Name | RANGE |
| Address Type | RANGE |
| Starting IP Address | 192.168.10.0 |
| End IP Address | 192.168.20.255 |

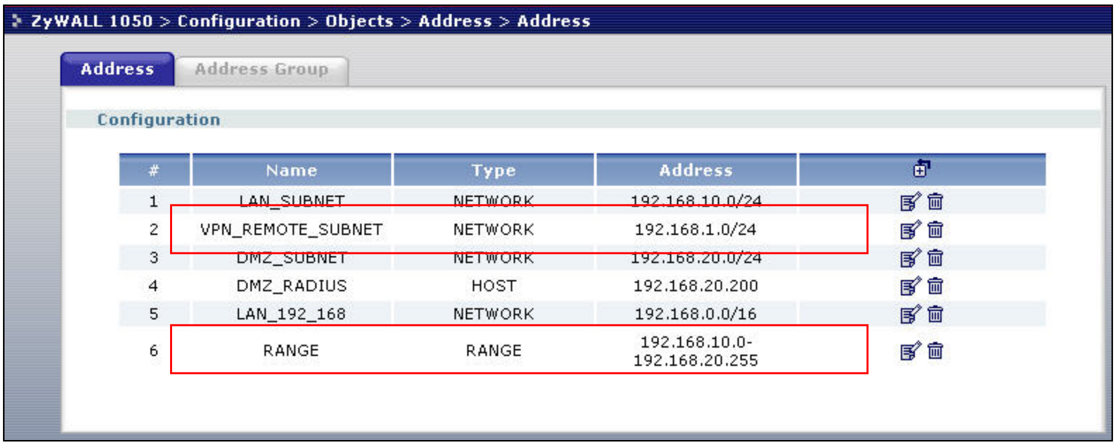
Set the 192.168.1.0 subnet as the remote address object.



ZyWALL 1050 > Configuration > Objects > Address > Address > Edit > #1

| | |
|---|---|
| Name | VPN_REMOTE_SUBNET |
| Address Type | NETWORK |
| Network | 192.168.1.0 |
| Netmask | 255.255.255.0 |

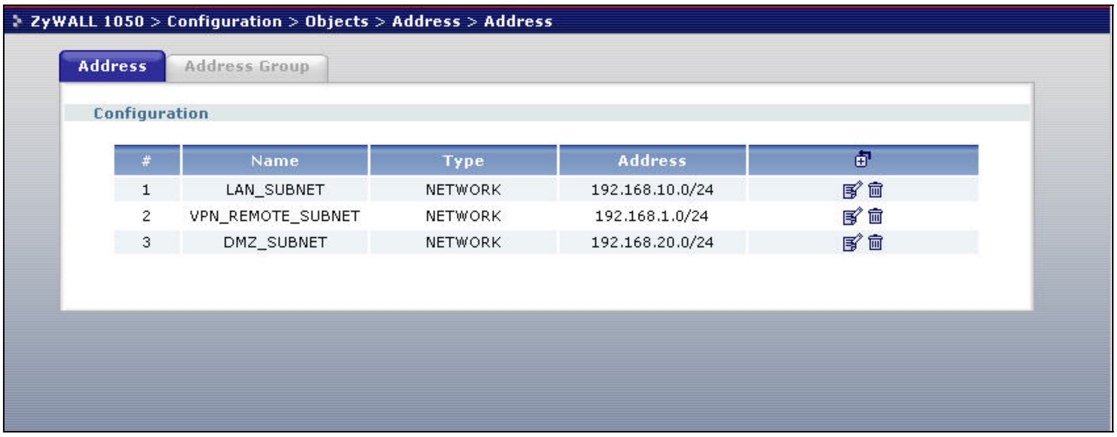
Get back to the overview of the address object page. You can see that three address object R and VPN REMOTE has already been set up.



ZyWALL 1050 > Configuration > Objects > Address > Address

Configuration

| # | Name | Type | Address |
|---|---|---|---|
| 1 | LAN_SUBNET | NETWORK | 192.168.10.0/24 |
| 2 | VPN_REMOTE_SUBNET | NETWORK | 192.168.1.0/24 |
| 3 | DMZ_SUBNET | NETWORK | 192.168.20.0/24 |
| 4 | DMZ_RADIUS | HOST | 192.168.20.200 |
| 5 | LAN_192_168 | NETWORK | 192.168.0.0/16 |
| 6 | RANGE | RANGE | 192.168.10.0-<br>192.168.20.255 |



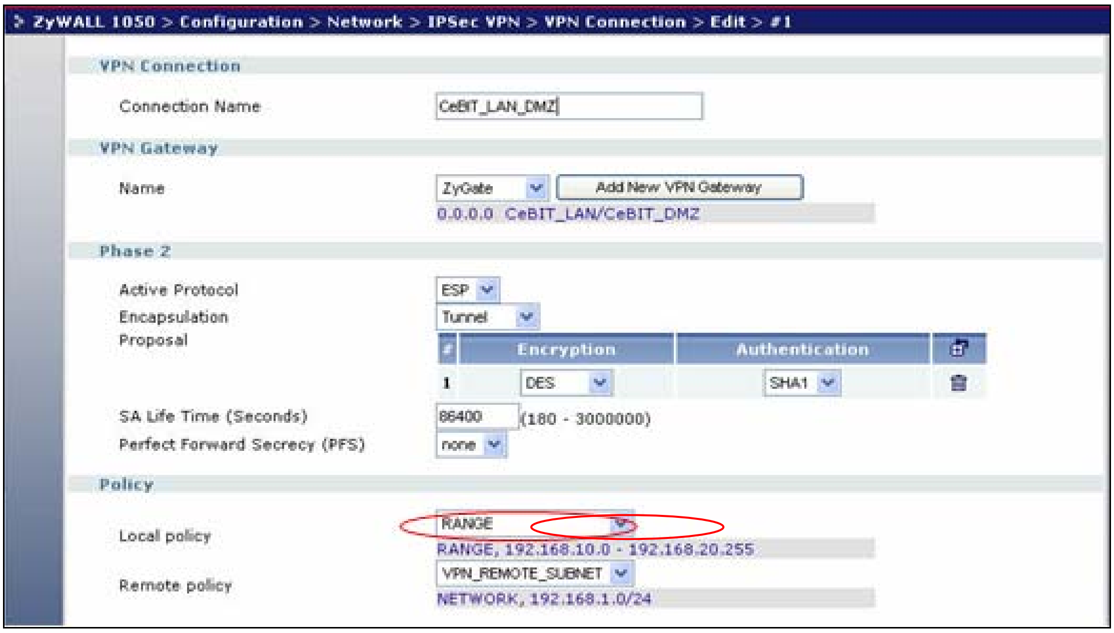
ZyWALL 1050 > Configuration > Objects > Address > Address

Configuration

| # | Name | Type | Address | |
|---|---|---|---|---|
| 1 | LAN_SUBNET | NETWORK | 192.168.10.0/24 | |
| 2 | VPN_REMOTE_SUBNET | NETWORK | 192.168.1.0/24 | |
| 3 | DMZ_SUBNET | NETWORK | 192.168.20.0/24 | |

Step4. Setup the VPN connection.

Setup the VPN connection for RANGE (LAN and DMZ) subnet access.



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Connection > Edit > #1

VPN Connection

Connection Name: CeBIT_LAN_DMZ

VPN Gateway

Name: ZyGate

0.0.0.0 CeBIT_LAN/CeBIT_DMZ

Phase 2

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | SHA1 |

SA Life Time (Seconds): 86400 (180 - 3000000)

Perfect Forward Secrecy (PFS): none

Policy

Local policy: RANGE

RANGE, 192.168.10.0 - 192.168.20.255

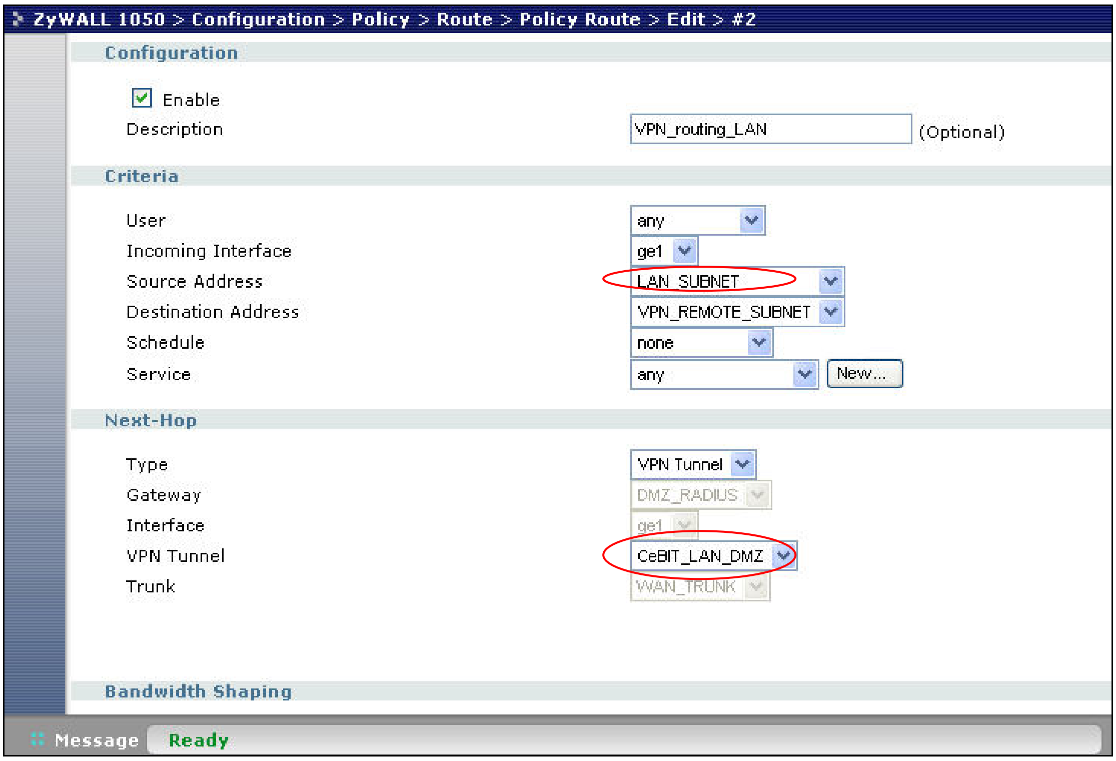
Remote policy: VPN_REMOTE_SUBNET

NETWORK, 192.168.1.0/24

Step5. Policy route for VPN traffic routing.

We have to setup the policy route for the VPN traffic routing to LAN and DMZ.

Switch to ZyWALL 1050 > Configuration > Policy > Route > Policy Route and add the policy route for the VPN traffic to LAN and DMZ.



ZyWALL 1050 > Configuration > Policy > Route > Policy Route > Edit > #2

Configuration

☑ Enable

Description: VPN_routing_LAN (Optional)

Criteria

User: any

Incoming Interface: ge1

Source Address: LAN_SUBNET

Destination Address: VPN_REMOTE_SUBNET

Schedule: none

Service: any

Next-Hop

Type: VPN Tunnel

Gateway: DMZ_RADIUS

Interface: ge1

VPN Tunnel: CeBIT_LAN_DMZ

Trunk: WAN_TRUNK

Bandwidth Shaping

Message: Ready

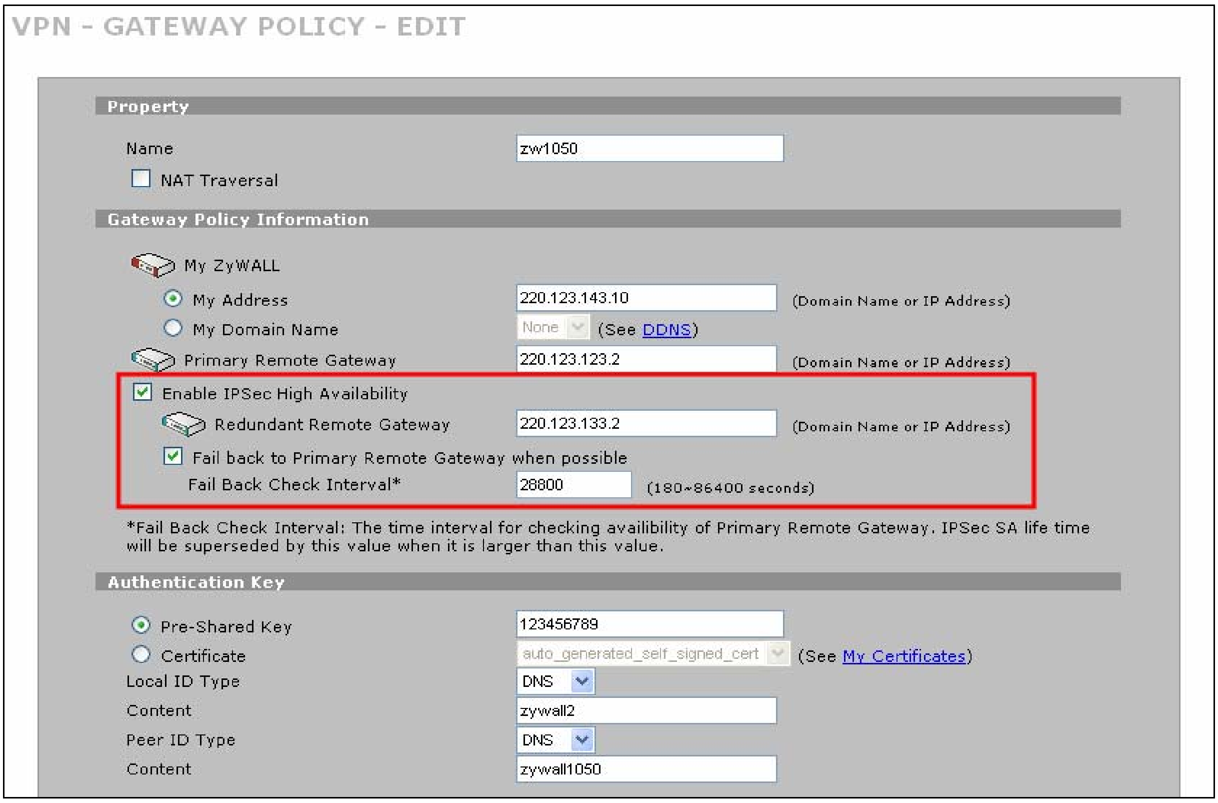
Step6. Connect the PC to ZyWALL 2 Plus and set the VPN settings.

In this step, we have to configure two VPN policies for remote ZyWALL 1050 LAN subnet and DMZ subnet. Login ZyWALL 2 Plus and switch to the VPN configuration page.

Fill in the WAN IP in My Address field and put remote 1050 WAN1 and WAN2 IP as Primary and Redundant remote Gateway. Activate the “Fail back to Primary Remote Gateway when possible” option and set the checking interval.

Setup the DNS domain name “ZyWALL 2”and “ZyWALL 1050” as Local and Peer ID type.

Click Apply to save the configuration.



VPN - GATEWAY POLICY - EDIT

**Property**

Name: zw1050

□ NAT Traversal

**Gateway Policy Information**

My ZyWALL

● My Address: 220.123.143.10 (Domain Name or IP Address)

○ My Domain Name: None (See DDNS)

Primary Remote Gateway: 220.123.123.2 (Domain Name or IP Address)

☑ Enable IPSec High Availability

Redundant Remote Gateway: 220.123.133.2 (Domain Name or IP Address)

☑ Fail back to Primary Remote Gateway when possible

Fail Back Check Interval*: 28800 (180~86400 seconds)

*Fail Back Check Interval: The time interval for checking availibility of Primary Remote Gateway. IPSec SA life time will be superseded by this value when it is larger than this value.

**Authentication Key**

● Pre-Shared Key: 123456789

○ Certificate: auto_generated_self_signed_cert (See My Certificates)

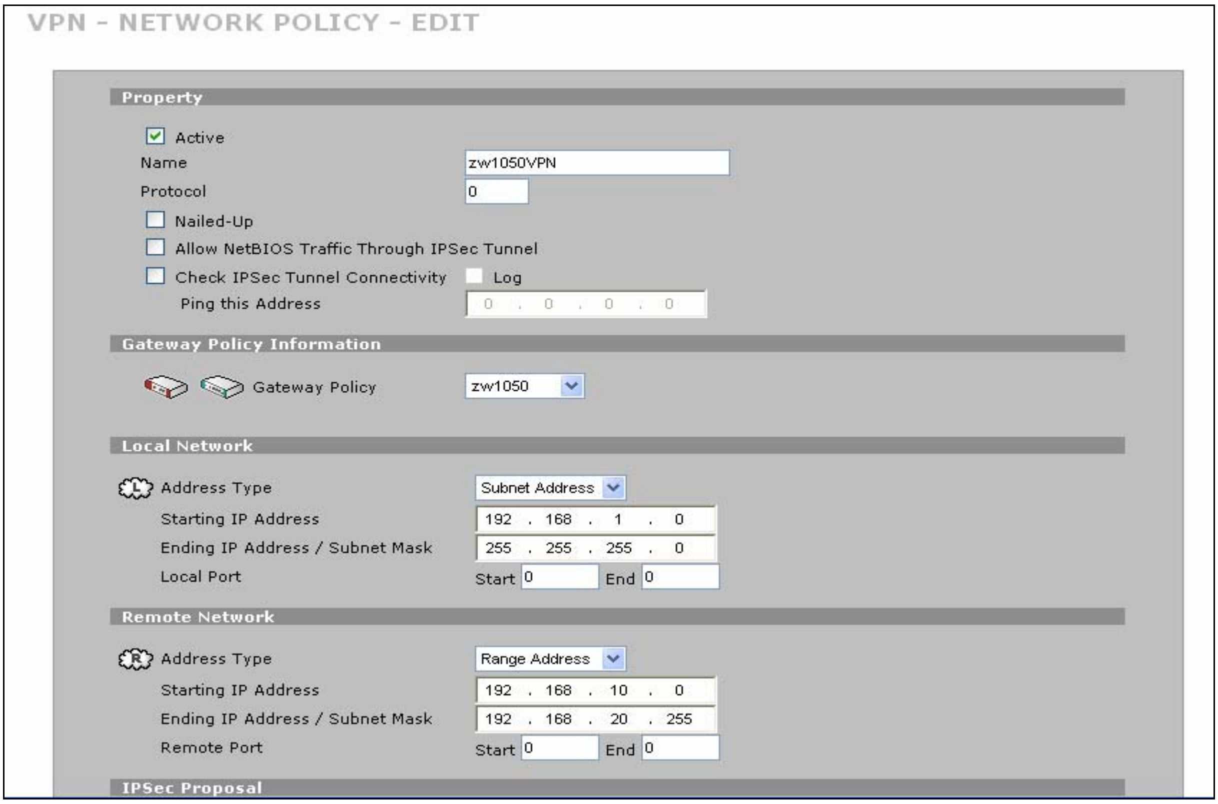
Local ID Type: DNS

Content: zywall2

Peer ID Type: DNS

Content: zywall1050

Click the Add icon to edit the VPN Network Policy. Setup the VPN policy for local LAN subnet (192.168.1.0/24) and Remote address type set to “Range Address” and IP is from 192.168.10.0 to 192.168.20.255. Click Apply to save the configuration.



VPN - NETWORK POLICY - EDIT

**Property**

☑ Active

Name: zw1050VPN

Protocol: 0

□ Nailed-Up

□ Allow NetBIOS Traffic Through IPSec Tunnel

□ Check IPSec Tunnel Connectivity □ Log

Ping this Address: 0 . 0 . 0 . 0

**Gateway Policy Information**

Gateway Policy: zw1050

**Local Network**

Address Type: Subnet Address

Starting IP Address: 192 . 168 . 1 . 0

Ending IP Address / Subnet Mask: 255 . 255 . 255 . 0

Local Port: Start 0 End 0

**Remote Network**

Address Type: Range Address

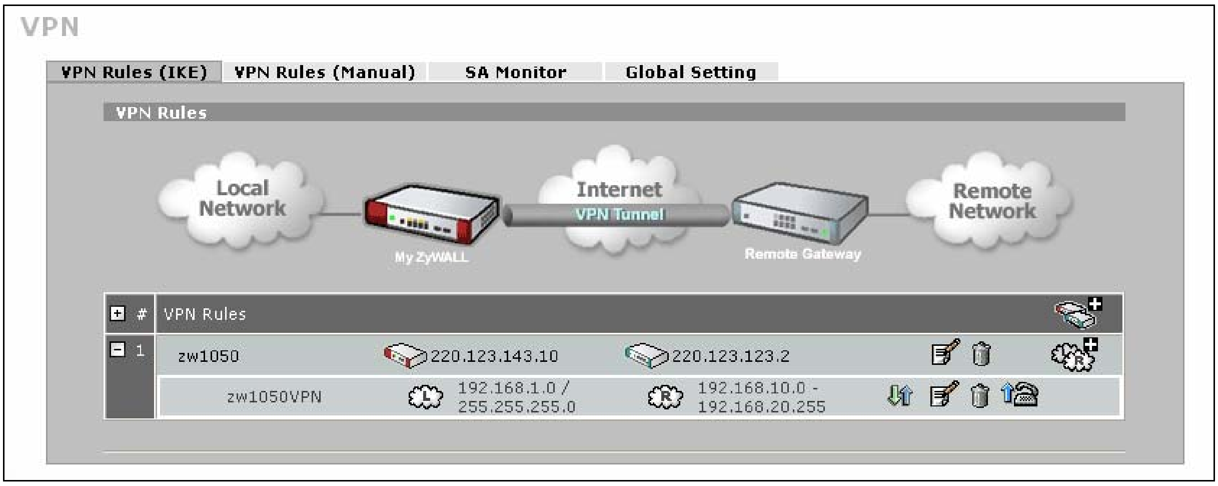
Starting IP Address: 192 . 168 . 10 . 0

Ending IP Address / Subnet Mask: 192 . 168 . 20 . 255

Remote Port: Start 0 End 0

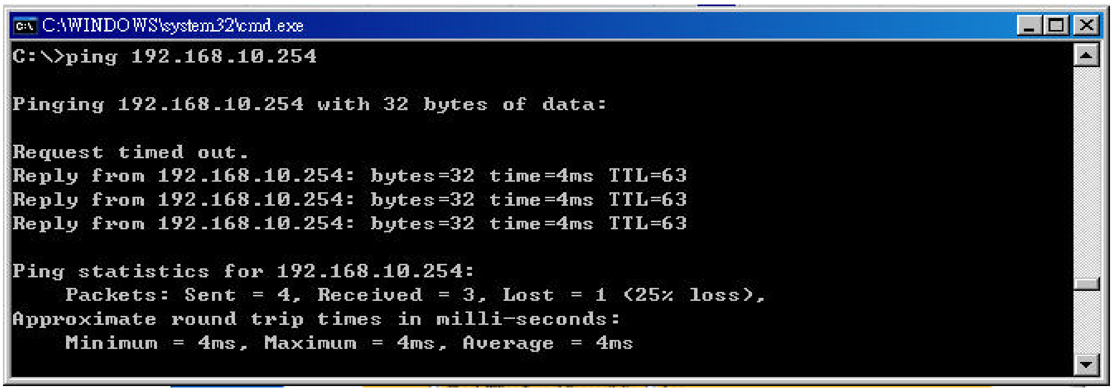
**IPSec Proposal**

We will see the new VPN tunnel listed on the VPN status page after configuring the VPN tunnel.



| # | VPN Rules | | |
|---|---|---|---|
| 1 | zw1050 | 220.123.143.10 | 220.123.123.2 |
| | zw1050VPN | 192.168.1.0 / 255.255.255.0 | 192.168.10.0 - 192.168.20.255 |

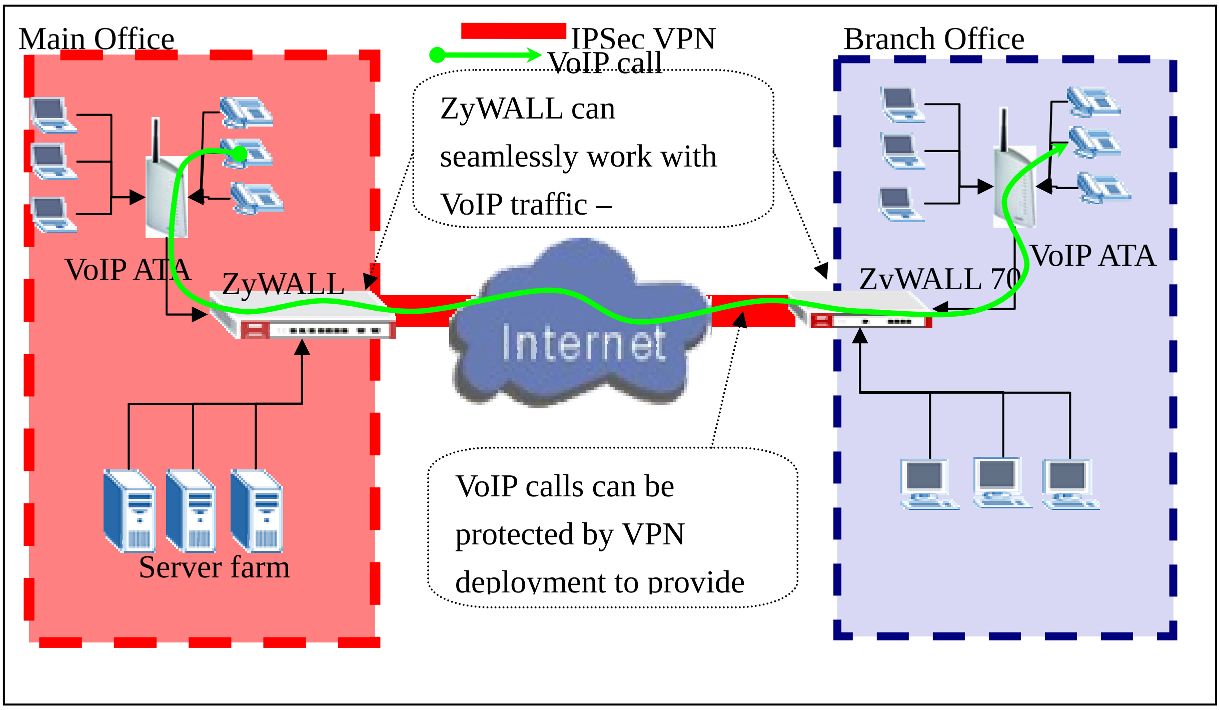
Ping the remote subnet to trigger the VPN tunnel.



```
C:\>ping 192.168.10.254

Pinging 192.168.10.254 with 32 bytes of data:

Request timed out.
Reply from 192.168.10.254: bytes=32 time=4ms TTL=63
Reply from 192.168.10.254: bytes=32 time=4ms TTL=63
Reply from 192.168.10.254: bytes=32 time=4ms TTL=63

Ping statistics for 192.168.10.254:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 4ms, Average = 4ms
```

User can unplug the WAN1 connection cable and test the VPN HA functionality now! Supposedly the VPN connection will switch to WAN2 connection in several seconds.

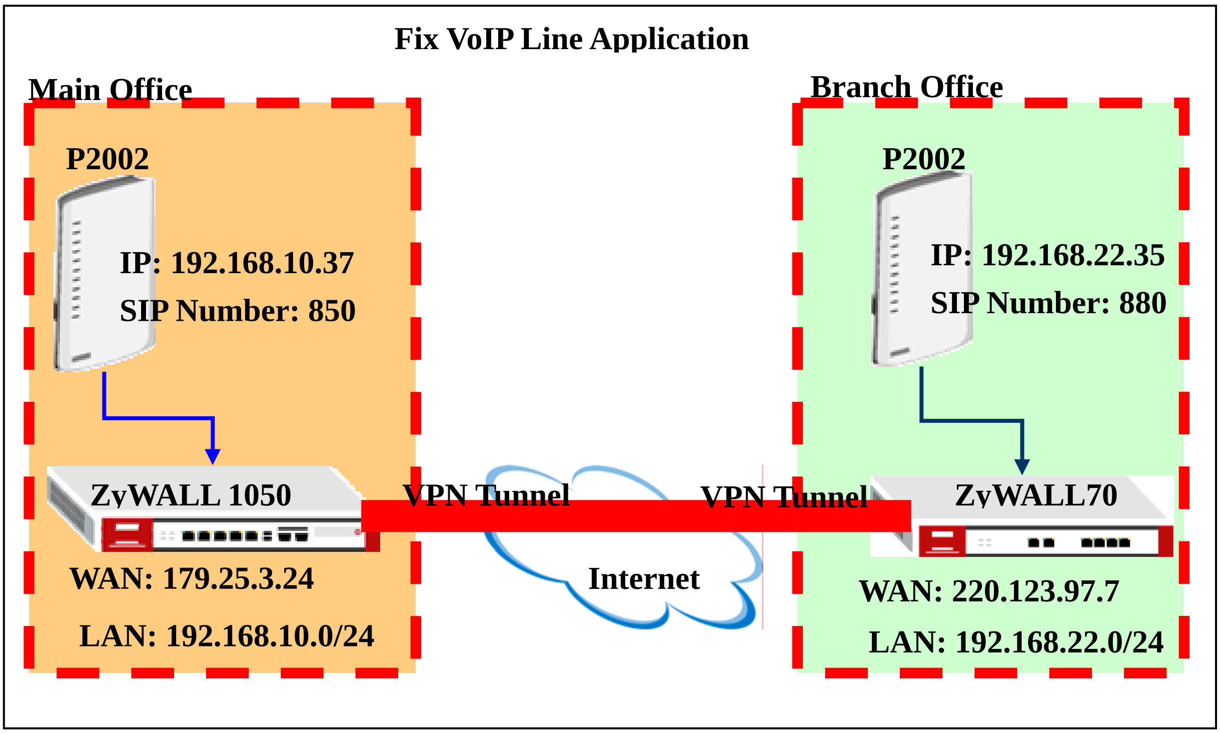
## 1.8 VoIP over VPN



The VoIP line deployment between different offices is more and more popular. This application can help enterprise to reduce the operation cost especially saving on long distance communication fee. The security issues also rise due to the VoIP public network transmission character. The common VoIP Security issues like call hijacking, identity theft and denial of service. Thus ZyWALL 1050 can protect the VoIP line security by employing advanced VPN technology.

- **What's the benefit of using ZyWALL to protect converged network?**
    - Prevent from call hijacking (VoIP over VPN)
    - Prevent from identity theft (VoIP over VPN)
    - Mitigate impact of denial of service

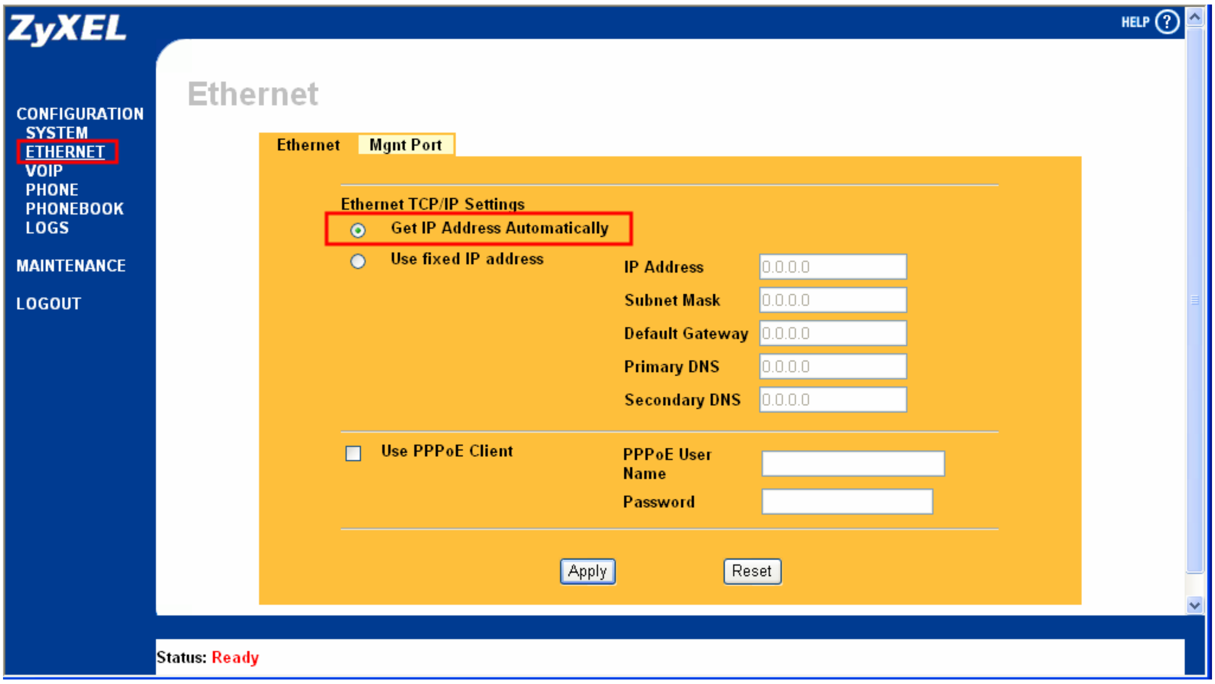
We use a simple topology to illustrate and show how ZyWALL 1050 can protect the VoIP line step by step in the following notes.



We used two VoIP ATA (ZyXEL P2002 series) connected to office gateway. Each of the VoIP ATA has a SIP number for remote ATA dialing. This kind of application is called Fix VoIP Line application. User only needs to install and configure VoIP ATA device and doesn't need to register with an external SIP server. We will use VPN tunnel for VoIP traffic transmission to ensure the VoIP security.

**VoIP ATA P2002 Configuration:**

The default management IP for P2002 is 192.168.5.1. Login to the P2002 GUI and switch to the Ethernet menu. Set the Ethernet IP setting to "Get IP address Automatically".



Ethernet

Ethernet TCP/IP Settings

● Get IP Address Automatically

○ Use fixed IP address

| | |
|---|---|
| IP Address | 0.0.0.0 |
| Subnet Mask | 0.0.0.0 |
| Default Gateway | 0.0.0.0 |
| Primary DNS | 0.0.0.0 |
| Secondary DNS | 0.0.0.0 |

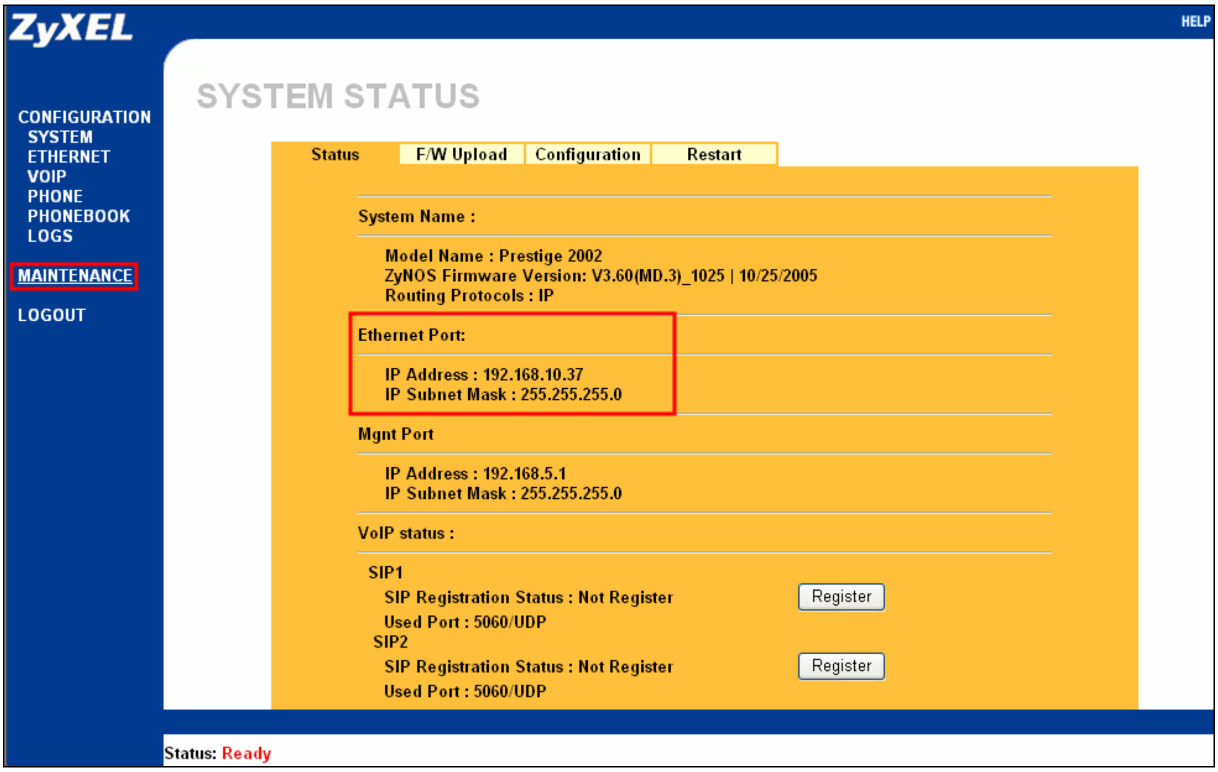
□ Use PPPoE Client

PPPoE User Name

Password

Status: Ready

Switch to the Maintenance menu and check what IP address was granted from ZyWALL 1050.



SYSTEM STATUS

System Name :

Model Name : Prestige 2002
ZyNOS Firmware Version: V3.60(MD.3)_1025 | 10/25/2005
Routing Protocols : IP

Ethernet Port:

IP Address : 192.168.10.37
IP Subnet Mask : 255.255.255.0

Mgnt Port

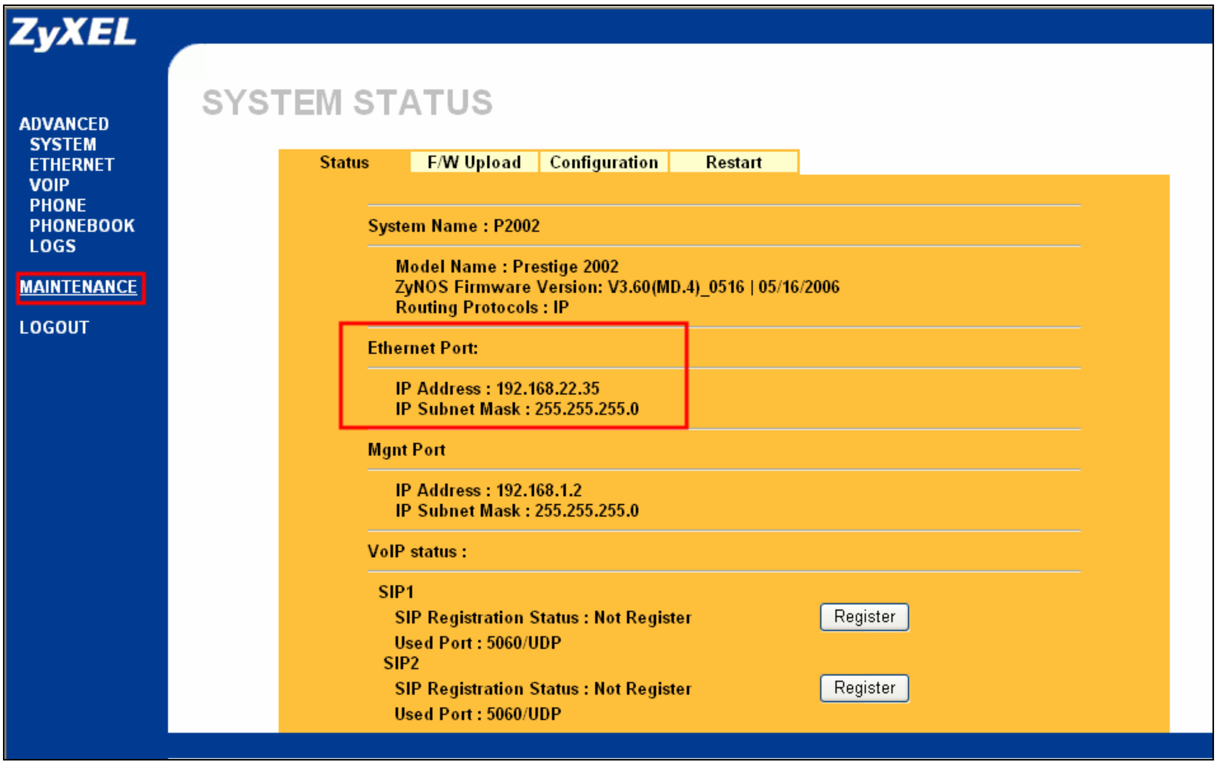
IP Address : 192.168.5.1
IP Subnet Mask : 255.255.255.0

VoIP status :

SIP1
SIP Registration Status : Not Register
Used Port : 5060/UDP
SIP2
SIP Registration Status : Not Register
Used Port : 5060/UDP

Status: Ready

Connect to the other P2002 GUI and repeat the same steps to find out the IP address.



SYSTEM STATUS

System Name : P2002

Model Name : Prestige 2002
ZyNOS Firmware Version: V3.60(MD.4)_0516 | 05/16/2006
Routing Protocols : IP

Ethernet Port:

IP Address : 192.168.22.35
IP Subnet Mask : 255.255.255.0

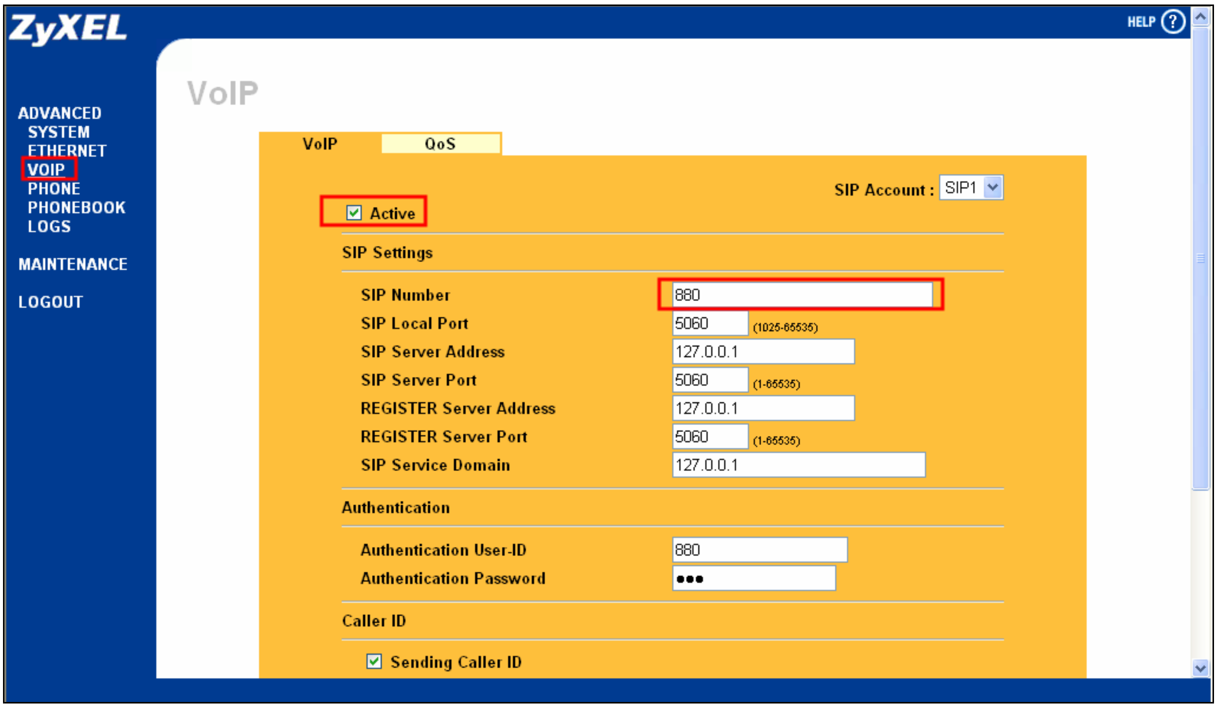
Mgnt Port

IP Address : 192.168.1.2
IP Subnet Mask : 255.255.255.0

VoIP status :

SIP1
SIP Registration Status : Not Register
Used Port : 5060/UDP
SIP2
SIP Registration Status : Not Register
Used Port : 5060/UDP

1. Setup the SIP Number in the Branch Office.



VoIP

SIP Account : SIP1

☑ Active

SIP Settings

| | |
|---|---|
| SIP Number | 880 |
| SIP Local Port | 5060 (1025-65535) |
| SIP Server Address | 127.0.0.1 |
| SIP Server Port | 5060 (1-65535) |
| REGISTER Server Address | 127.0.0.1 |
| REGISTER Server Port | 5060 (1-65535) |
| SIP Service Domain | 127.0.0.1 |

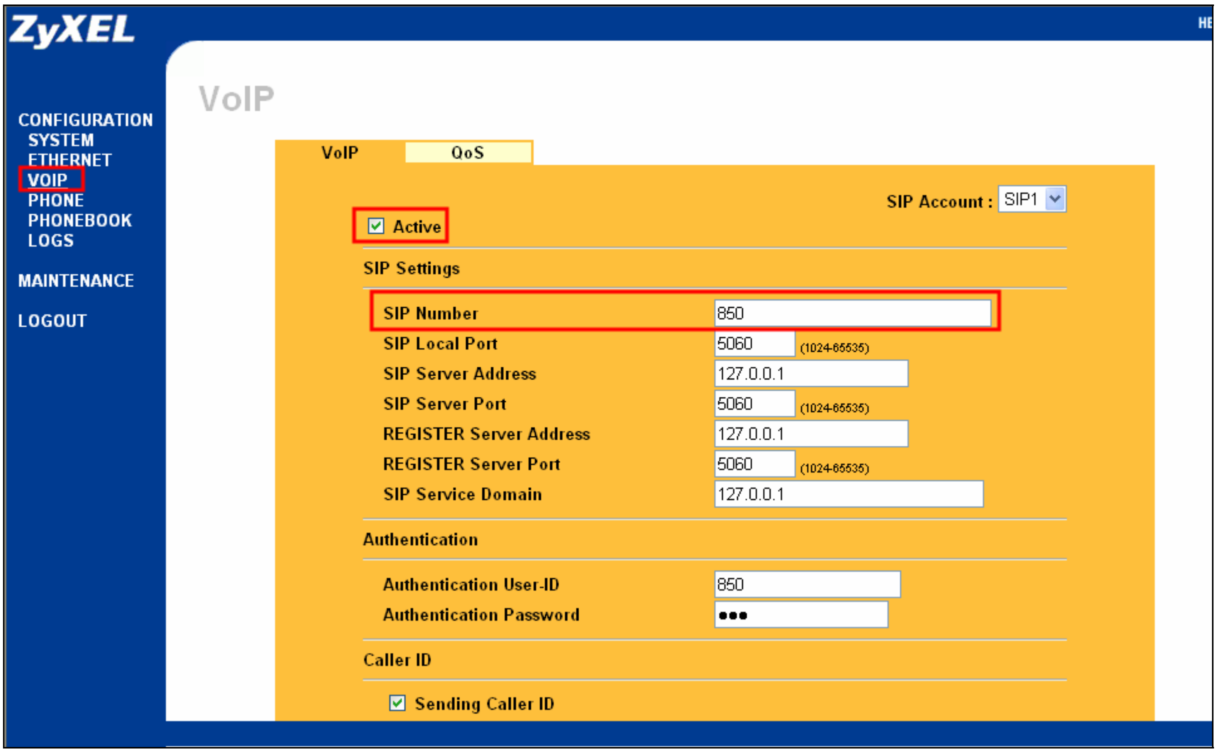
Authentication

| | |
|---|---|
| Authentication User-ID | 880 |
| Authentication Password | ●●● |

Caller ID

☑ Sending Caller ID

2. Setup the SIP Number in the Main Office.



SIP Account : SIP1

☑ Active

SIP Settings

| | |
|---|---|
| SIP Number | 850 |
| SIP Local Port | 5060 (1024-65535) |
| SIP Server Address | 127.0.0.1 |
| SIP Server Port | 5060 (1024-65535) |
| REGISTER Server Address | 127.0.0.1 |
| REGISTER Server Port | 5060 (1024-65535) |
| SIP Service Domain | 127.0.0.1 |

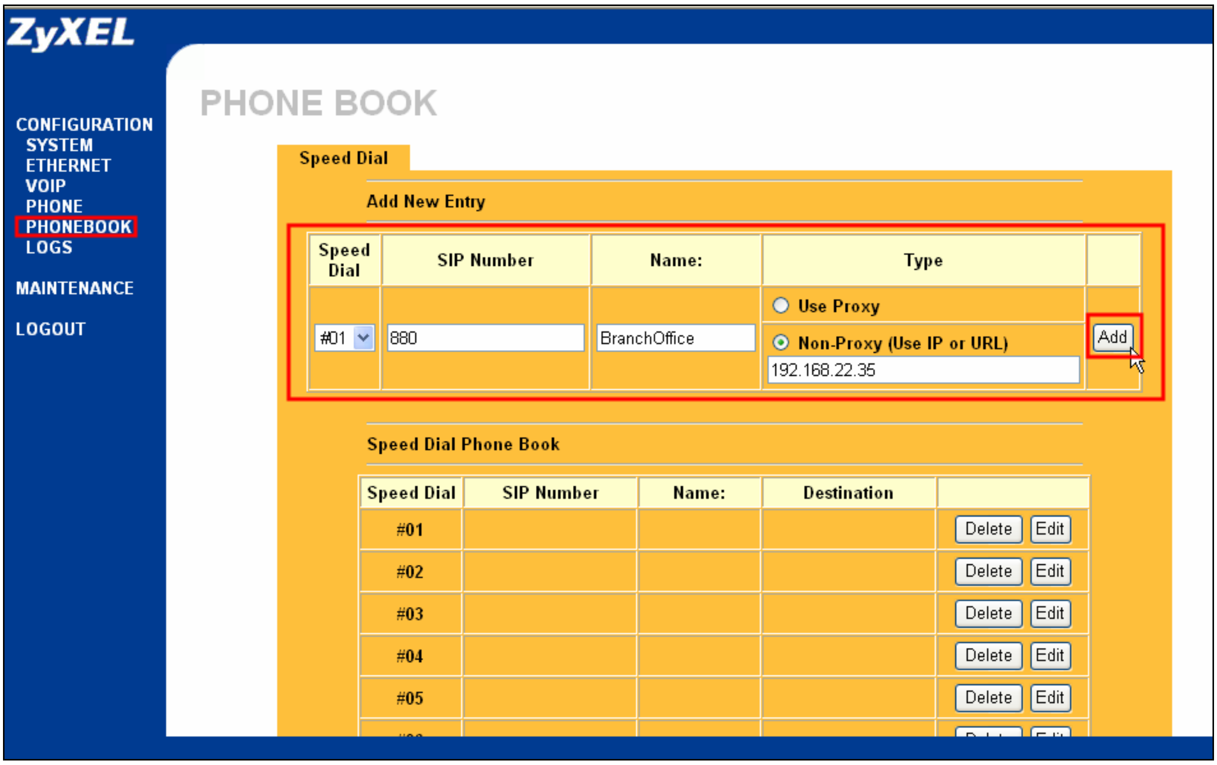
Authentication

| | |
|---|---|
| Authentication User-ID | 850 |
| Authentication Password | ●●● |

Caller ID

☑ Sending Caller ID

3. Setup the Branch Office SIP number and the IP address in the Main Office's P2002's **PHONEBOOK** menu. Fill in the SIP number and the IP address for the branch office VoIP ATA and then click the Add button to add this record in the Speed Dial Phone Book.



Add New Entry

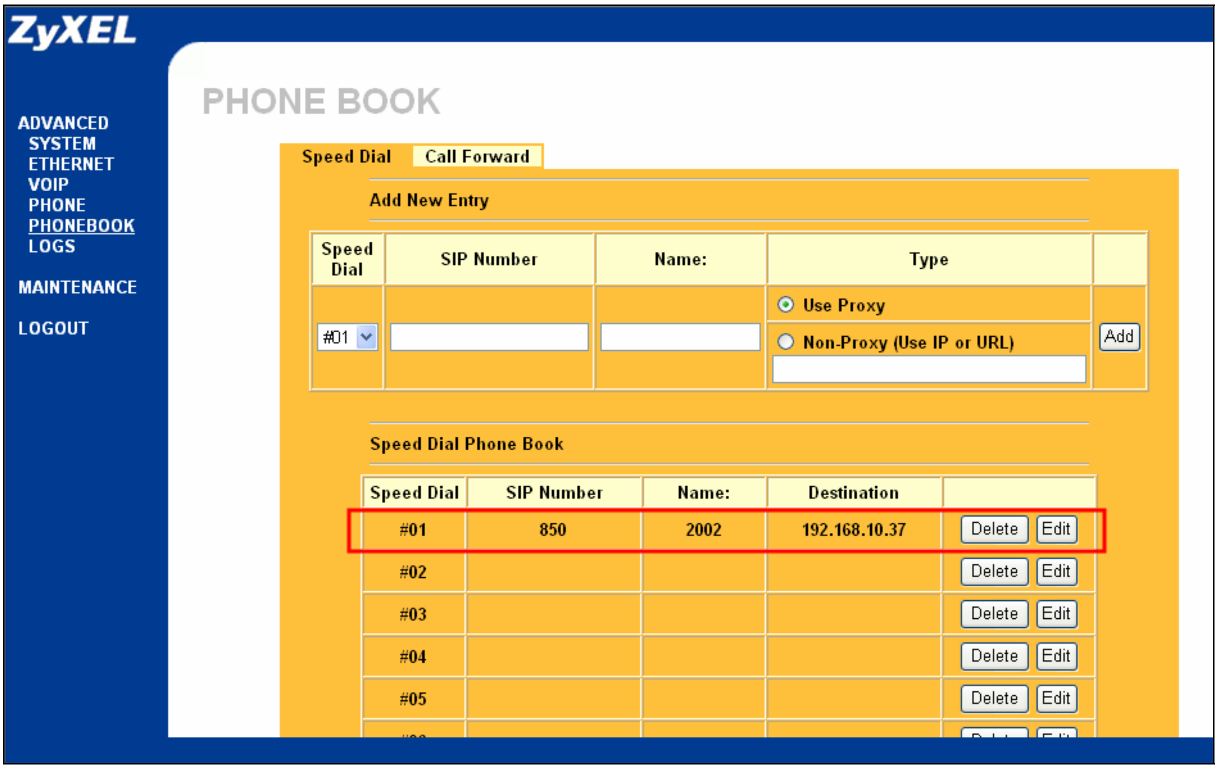
| Speed Dial | SIP Number | Name: | Type | |
|---|---|---|---|---|
| #01 | 880 | BranchOffice | ○ Use Proxy<br>● Non-Proxy (Use IP or URL)<br>192.168.22.35 | Add |

Speed Dial Phone Book

| Speed Dial | SIP Number | Name: | Destination | |
|---|---|---|---|---|
| #01 | | | | Delete Edit |
| #02 | | | | Delete Edit |
| #03 | | | | Delete Edit |
| #04 | | | | Delete Edit |
| #05 | | | | Delete Edit |

4. Setup the Main Office SIP number and the IP address in the Branch Office's P2002's PHONEBOOK menu. The remote office SIP info will show up in Speed Dial Phone Book

after adding this record.



| Speed Dial | SIP Number | Name: | Type |  |
|---|---|---|---|---|
| #01 |  |  | ● Use Proxy<br>○ Non-Proxy (Use IP or URL) | Add |

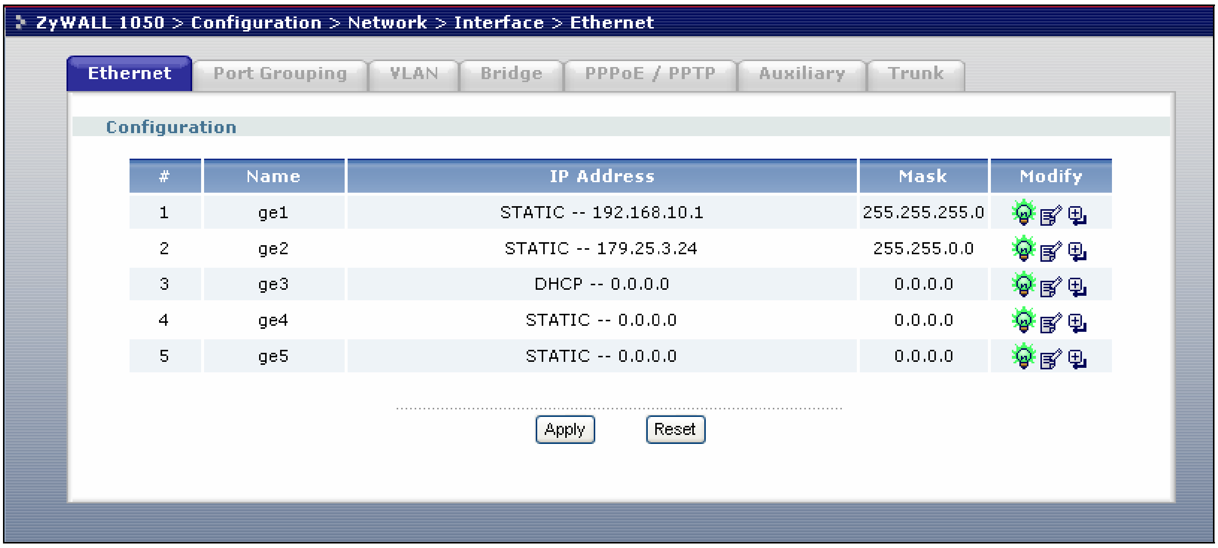
Speed Dial Phone Book

| Speed Dial | SIP Number | Name: | Destination |  |
|---|---|---|---|---|
| #01 | 850 | 2002 | 192.168.10.37 | Delete Edit |
| #02 |  |  |  | Delete Edit |
| #03 |  |  |  | Delete Edit |
| #04 |  |  |  | Delete Edit |
| #05 |  |  |  | Delete Edit |

We have finished the configuration of VoIP ATA on both sites and we can move to the next section, to setup the security gateway on both sites.

**Main Office ZyWALL 1050 Configuration:**

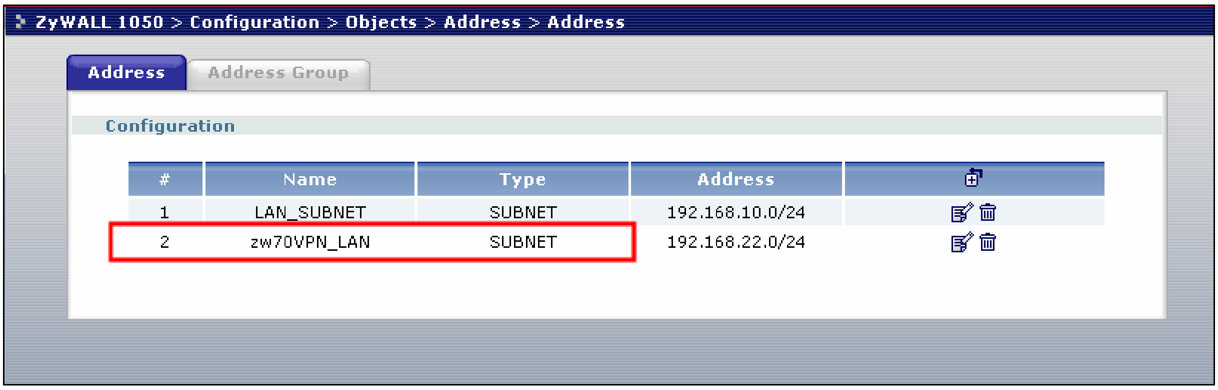
1. Login to the ZyWALL 1050 Web GUI and setup the ZyWALL 1050 WAN and LAN interface as shown on the previous topology diagram.



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 | DHCP -- 0.0.0.0 | 0.0.0.0 |  |
| 4 | ge4 | STATIC -- 0.0.0.0 | 0.0.0.0 |  |
| 5 | ge5 | STATIC -- 0.0.0.0 | 0.0.0.0 |  |

2. Setup the remote subnet address object for the subnet behind the remote office ZyWALL70.

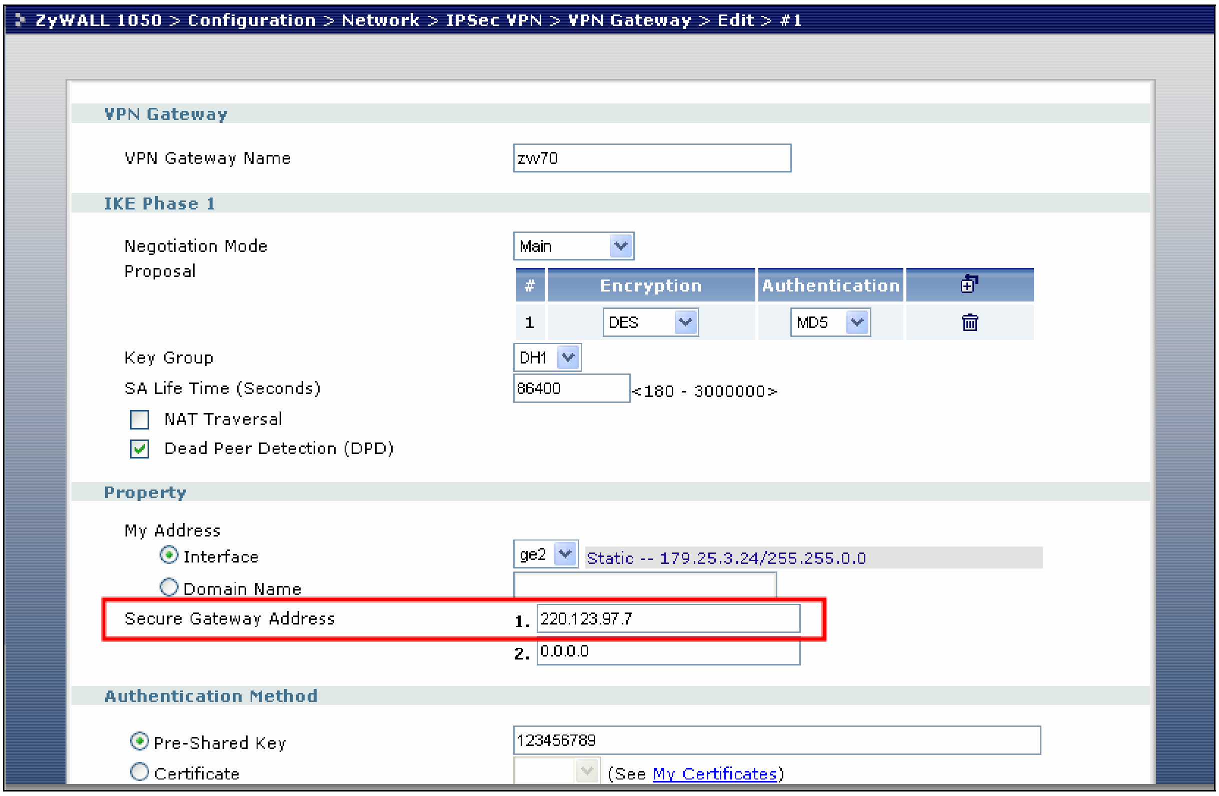


ZyWALL 1050 > Configuration > Objects > Address > Address

Configuration

| # | Name | Type | Address |
|---|---|---|---|
| 1 | LAN_SUBNET | SUBNET | 192.168.10.0/24 |
| 2 | zw70VPN_LAN | SUBNET | 192.168.22.0/24 |

3. Setup the VPN tunnel to force the VoIP traffic going through the VPN tunnel to Branch Office. Switch to ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway and add a new VPN gateway rule.



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Gateway > Edit > #1

VPN Gateway

VPN Gateway Name: zw70

IKE Phase 1

Negotiation Mode: Main

Proposal

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | MD5 |

Key Group: DH1

SA Life Time (Seconds): 86400 <180 - 3000000>

□ NAT Traversal

☑ Dead Peer Detection (DPD)

Property

My Address

● Interface: ge2 Static -- 179.25.3.24/255.255.0.0

○ Domain Name

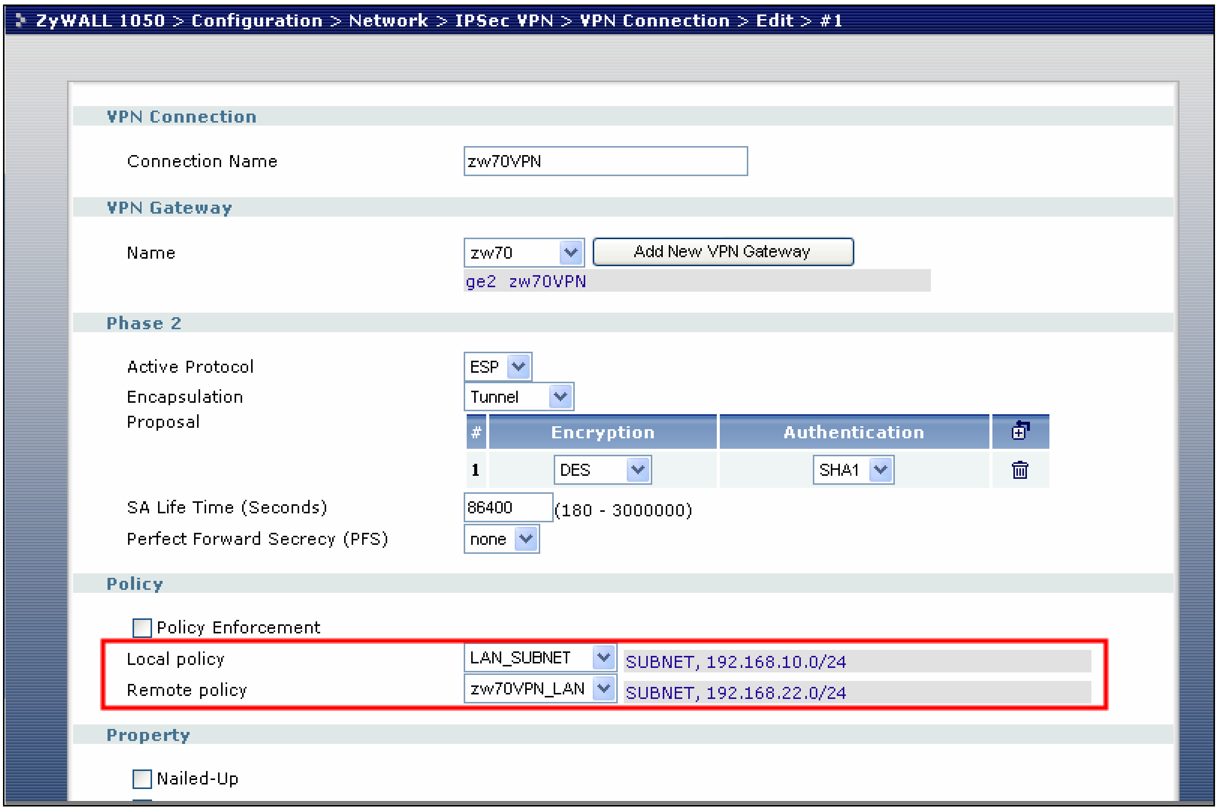
Secure Gateway Address: 1. 220.123.97.7 2. 0.0.0.0

Authentication Method

● Pre-Shared Key: 123456789

○ Certificate (See My Certificates)

4. Switch to ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Connection and add a new VPN connection. The local and remote policy are the Address objects LAN_SUBNET and zw70VPN_LAN.



ZyWALL 1050 > Configuration > Network > IPSec VPN > VPN Connection > Edit > #1

VPN Connection

Connection Name: zw70VPN

VPN Gateway

Name: zw70 [Add New VPN Gateway]
ge2 zw70VPN

Phase 2

Active Protocol: ESP
Encapsulation: Tunnel
Proposal:

| # | Encryption | Authentication |
|---|---|---|
| 1 | DES | SHA1 |

SA Life Time (Seconds): 86400 (180 - 3000000)
Perfect Forward Secrecy (PFS): none

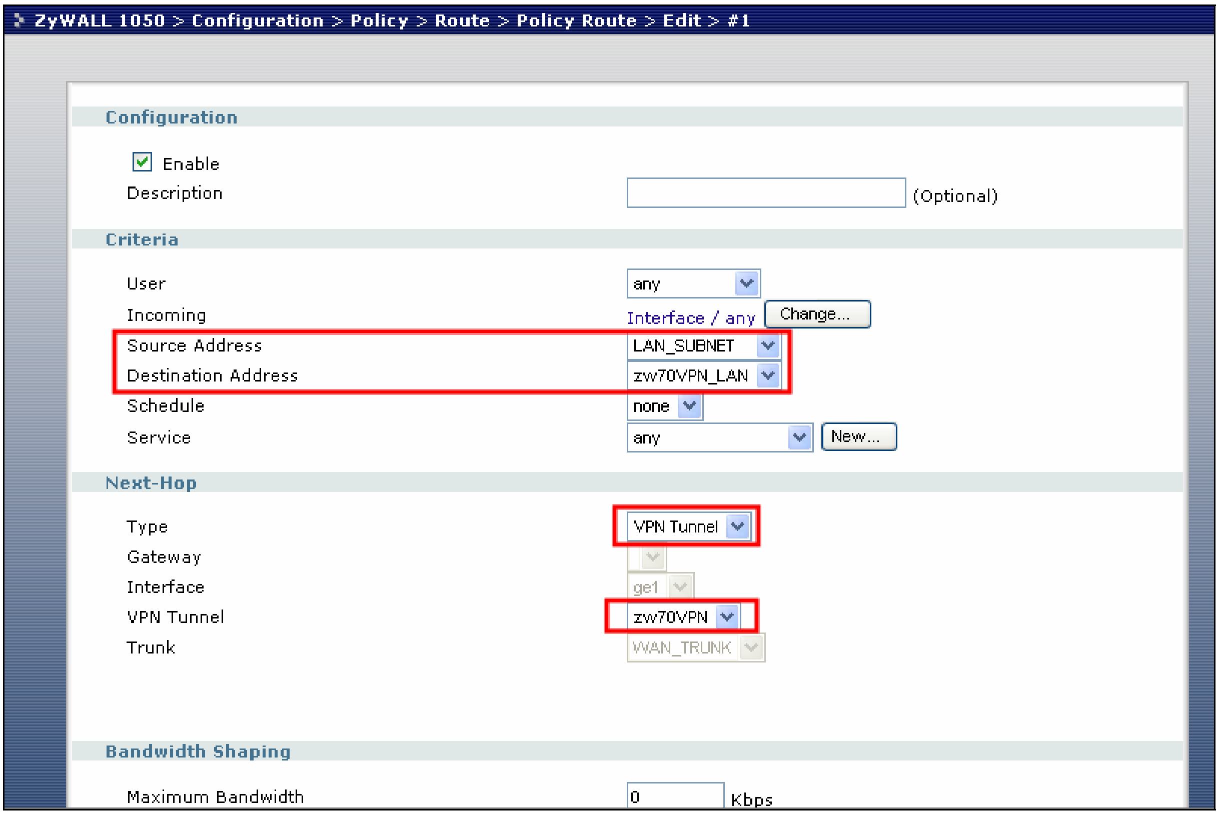
Policy

□ Policy Enforcement
Local policy: LAN_SUBNET SUBNET, 192.168.10.0/24
Remote policy: zw70VPN_LAN SUBNET, 192.168.22.0/24

Property

□ Nailed-Up

5. Switch to ZyWALL 1050 > Configuration > Policy > Route > Policy Route to add a policy route for routing the local subnet traffic to the remote branch office subnet via the tunnel - zw70VPN.



ZyWALL 1050 > Configuration > Policy > Route > Policy Route > Edit > #1

Configuration

☑ Enable
Description: (Optional)

Criteria

User: any
Incoming: Interface / any [Change...]
Source Address: LAN_SUBNET
Destination Address: zw70VPN_LAN
Schedule: none
Service: any [New...]

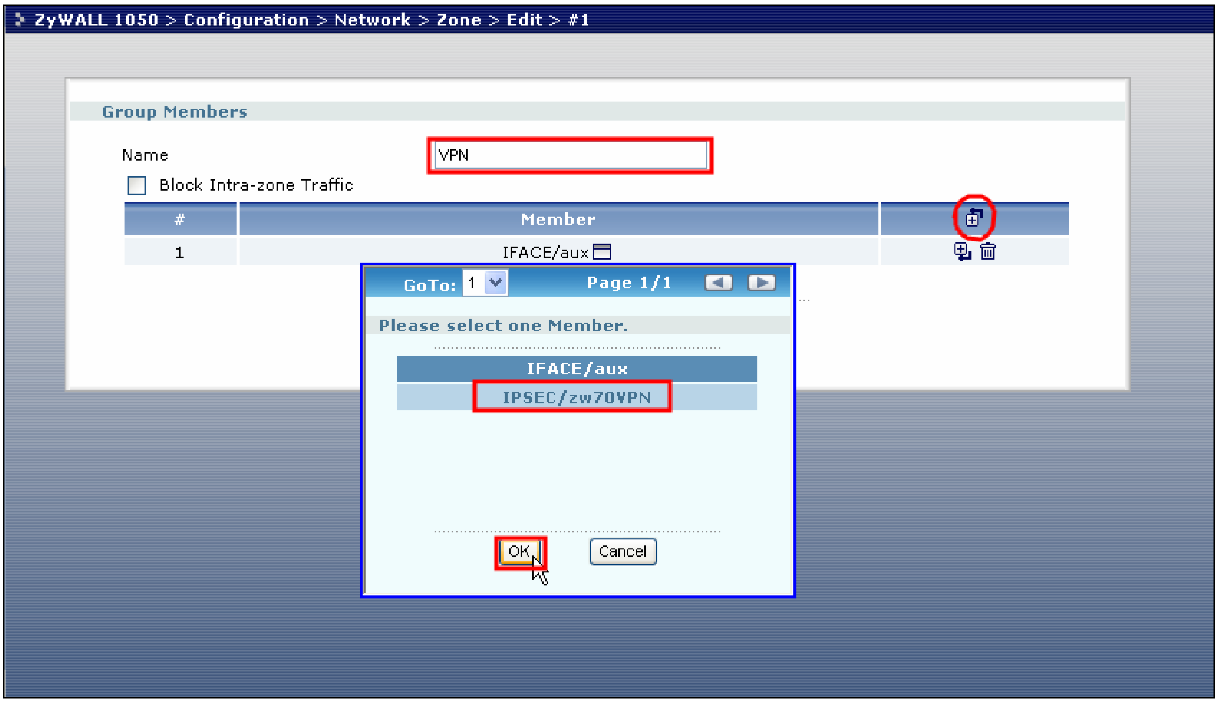
Next-Hop

Type: VPN Tunnel
Gateway:
Interface: ge1
VPN Tunnel: zw70VPN
Trunk: WAN_TRUNK

Bandwidth Shaping

Maximum Bandwidth: 0 Kbps

6. We have finished the VPN connection and routing configuration. Now we can start to setup the security checking rule over this VPN tunnel. Switch to ZyWALL 1050 > Configuration > Network > Zone and add a new Zone for VPN.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #1

Group Members

Name: VPN

□ Block Intra-zone Traffic

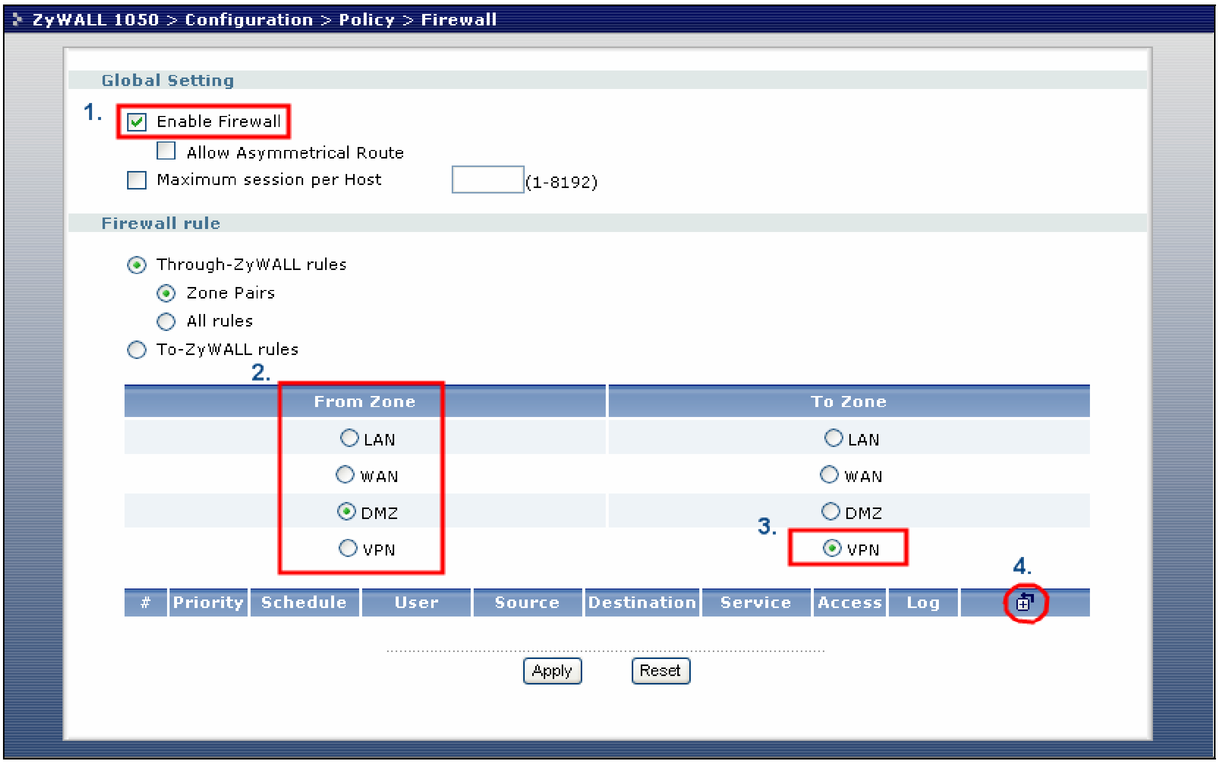
| # | Member |
|---|---|
| 1 | IFACE/aux |

GoTo: 1 Page 1/1

Please select one Member.

IFACE/aux
IPSEC/zw70VPN

7. First, we can configure the firewall rule to prevent the unauthorized access from other zones and we also can add more granular access control rules. Criteria can be different users, sources or services.



ZyWALL 1050 > Configuration > Policy > Firewall

Global Setting

1. ☑ Enable Firewall

□ Allow Asymmetrical Route

□ Maximum session per Host (1-8192)

Firewall rule

● Through-ZyWALL rules

● Zone Pairs

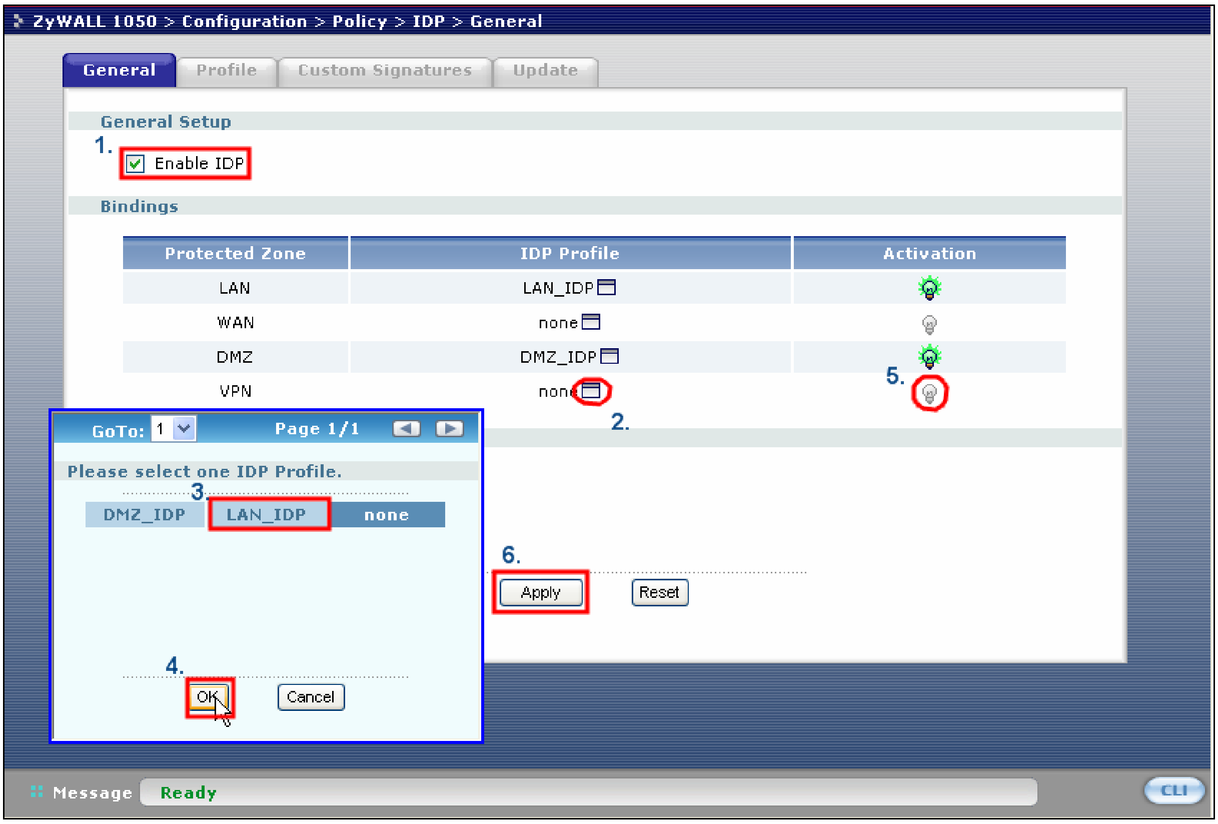
○ All rules

○ To-ZyWALL rules

| 2. From Zone | 3. To Zone |
|---|---|
| ○ LAN | ○ LAN |
| ○ WAN | ○ WAN |
| ● DMZ | ○ DMZ |
| ○ VPN | ● VPN |

| # | Priority | Schedule | User | Source | Destination | Service | Access | Log | 4. |
|---|---|---|---|---|---|---|---|---|---|

8. We also can use IDP to detect and intercept the intrusion in the VPN tunnel. Switch to ZyWALL 1050 > Configuration > Policy > IDP and follow the steps shown on the diagram below to add the IDP protection to the VPN zone.



ZyWALL 1050 > Configuration > Policy > IDP > General

General | Profile | Custom Signatures | Update

General Setup

1. ☑ Enable IDP

Bindings

| Protected Zone | IDP Profile | Activation |
|---|---|---|
| LAN | LAN_IDP | ● |
| WAN | none | ○ |
| DMZ | DMZ_IDP | ● |
| VPN | none | ○ |

GoTo: 1 Page 1/1

Please select one IDP Profile.

3. DMZ_IDP | LAN_IDP | none

4. OK Cancel

6. Apply Reset

Message Ready

9. We have finished the VPN tunnel configuration and security policy enforcement over the VPN tunnel. The VoIP traffic transmitted via the VPN tunnel is well protected now.

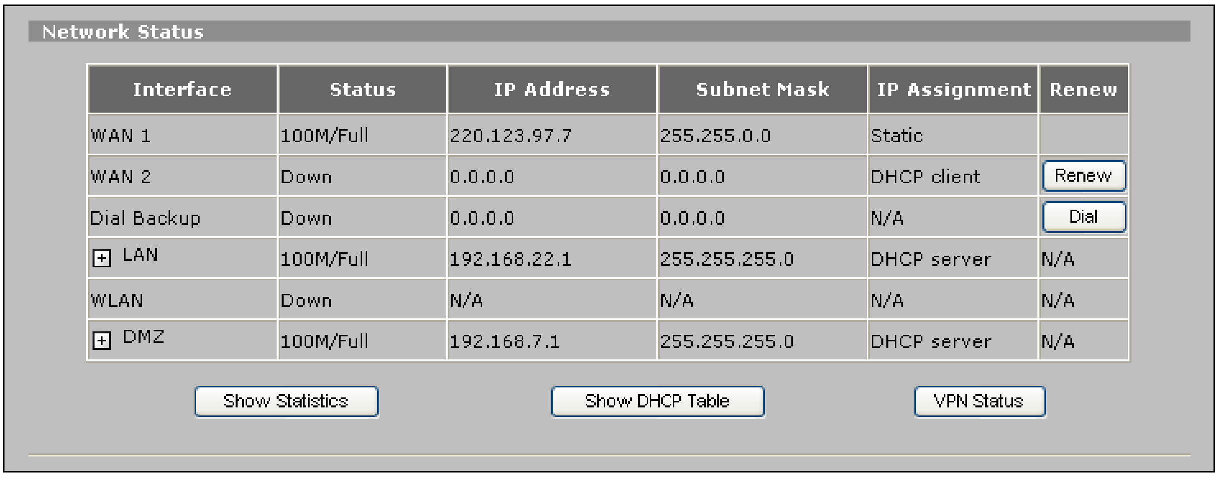
CLI commands for IDP activation and Profile binding:

```
[0] idp activate
[1] idp zone LAN activate
[2] no idp zone WAN activate
[3] idp zone DMZ activate
[4] idp bind VPN profile LAN_IDP
[5] idp zone VPN activate
[6] show idp bindings
[7] show idp profiles
[8] show service-register status idp
[9] show idp activation
```

**Branch Office ZyWALL70 Configuration:**

1. Login to the ZyWALL70 Web GUI and setup the ZyWALL70 WAN and LAN interface as

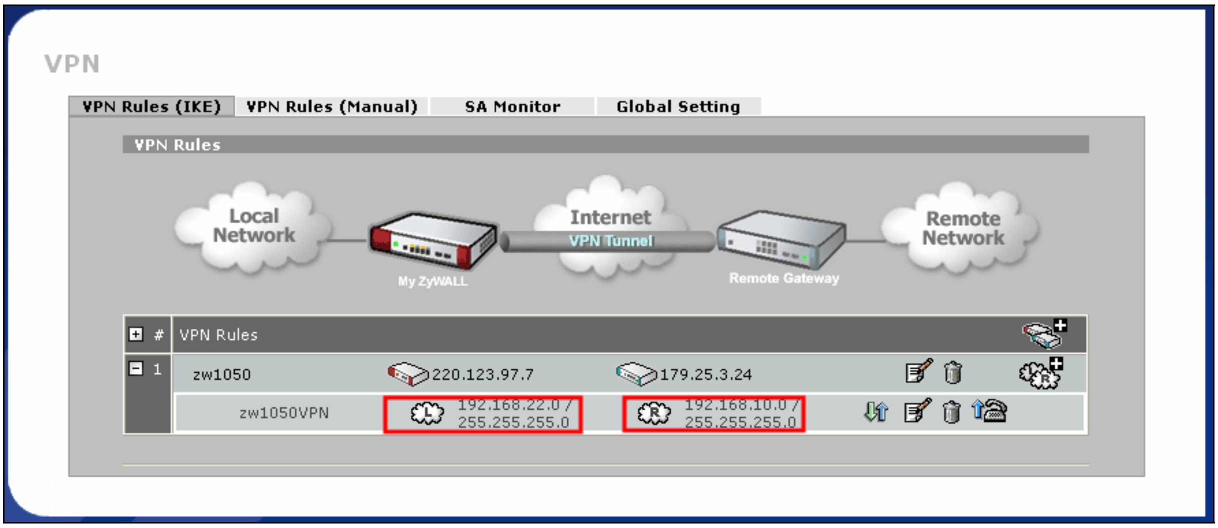
shown in the previous topology diagram.



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 | Renew |
| Dial Backup | Down | 0.0.0.0 | 0.0.0.0 | N/A | Dial |
| ⊞ 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 |
| ⊞ DMZ | 100M/Full | 192.168.7.1 | 255.255.255.0 | DHCP server | N/A |

2. Configure the VPN tunnel for connecting with ZyWALL 1050.



VPN

| ⊞ | # | VPN Rules | | | |
|---|---|---|---|---|---|
| ⊟ | 1 | zw1050 | 220.123.97.7 | 179.25.3.24 | |
| | | zw1050VPN | 192.168.22.0 / 255.255.255.0 | 192.168.10.0 / 255.255.255.0 | |

We can start to enjoy the VoIP Phone Line convenience and cost saving without security issues after the VPN connection and security policy enforcement have been deployed in the network environment.

# 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 1050 provide for managing IM/P2P applications?

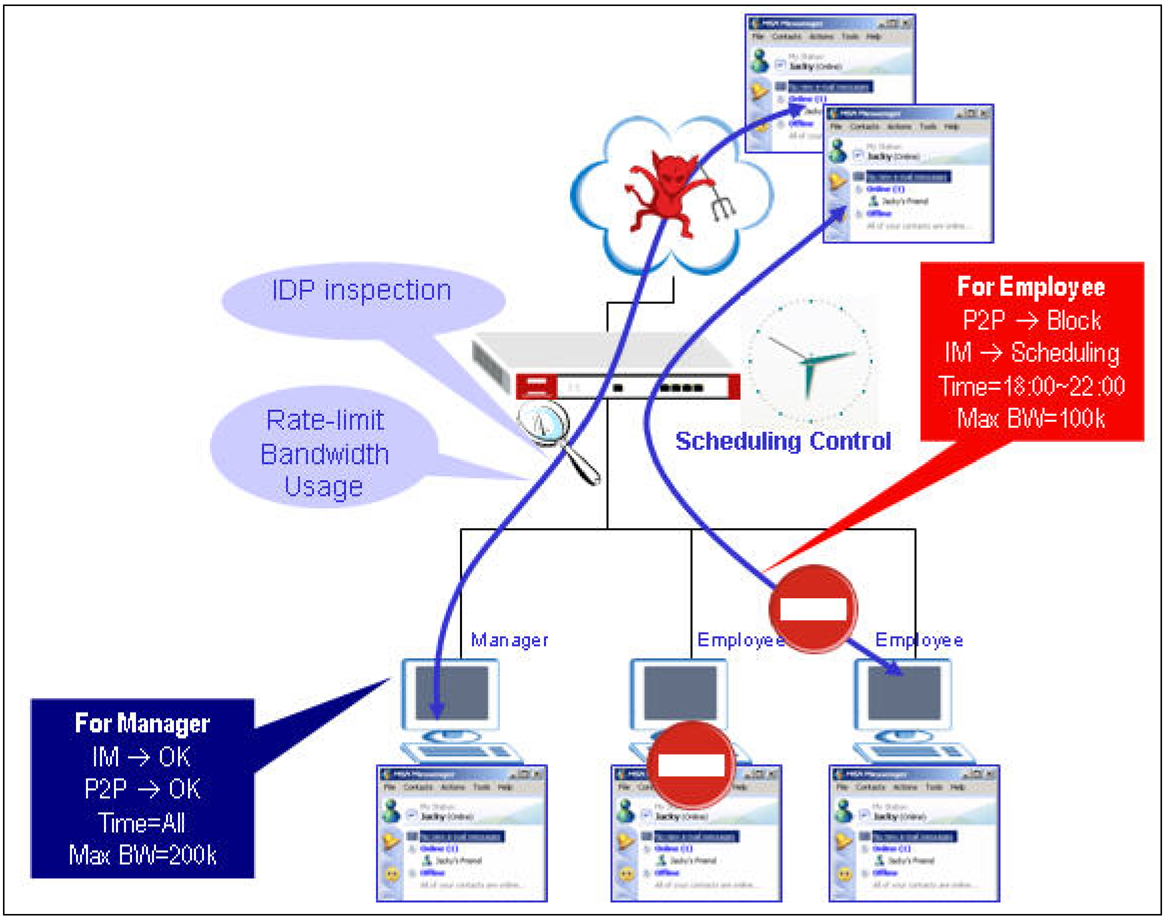
ZyWALL provides best solution to solve the rigidity of the “all-or-nothing” approach and can meet customer’s expectation.

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 1050’s access granularity for controlling hazardous IM/P2P applications:
   - By User/Group
   - By Time of access
   - By Bandwidth

### 2.1.3 Configuration Example



Here we show you an example. ZyCompany has rule to define some employees who cannot use P2P/IM at all while some employees are also not allowed to use P2P, but they can use IM after work during 18:00 ~ 22:00 and the max bandwidth could be used is 100k. For managers, company's policy allows them to use IM and P2P applications all the time but max bandwidth for them is still controlled not to get over 200k. Besides, traffic will be inspected by IDP and be monitored by bandwidth usage to prevent security threats from Internet through the applications.

We are going to complete following setting.

1. Create user/group object
2. Create schedule object
3. Configure layer 7 application control -- App Patrol
4. Configure Policy Route
5. Configure IDP

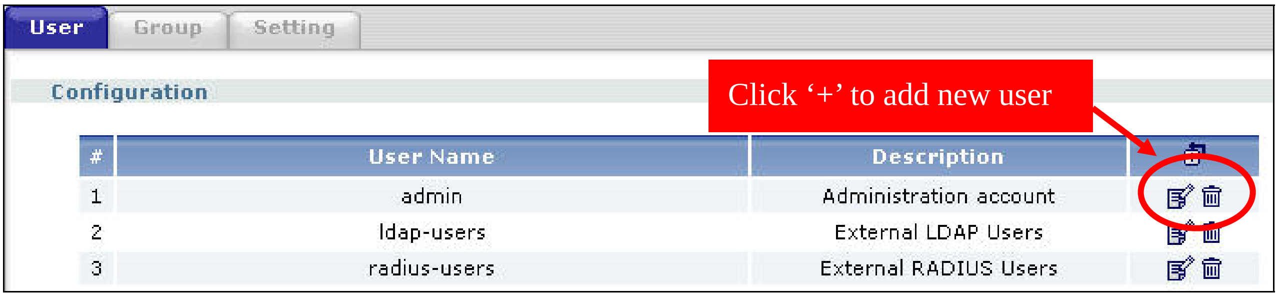
Step by step configuration of ZW1050 is as follows:

**Step1.** Create user/group object

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

| user | group | P2P access | IM access | Time for access | Bandwidth |
|---|---|---|---|---|---|
| **Victor** | **Manager** | ok | ok | IM+P2P(all the time) | IM+P2P <=200k |
| **Peter** | **Engineer1** | X | X | N/A | N/A |
| **John** | **Engineer2** | X | ok | IM-(18:00 ~ 22:00) | IM <=100K |

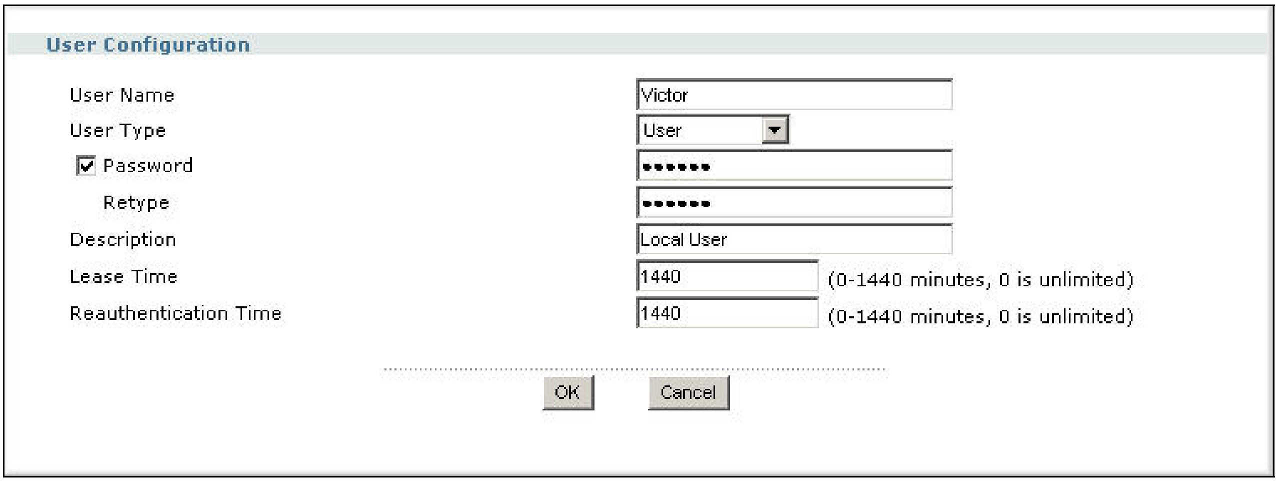
2. Go to menu **Configuration** > **User/Group** > **User tab**, add user 'Victor' as following figure.



Click '+' to add new user

| # | User Name | Description | |
|---|---|---|---|
| 1 | admin | Administration account | |
| 2 | ldap-users | External LDAP Users | |
| 3 | radius-users | External RADIUS Users | |

.

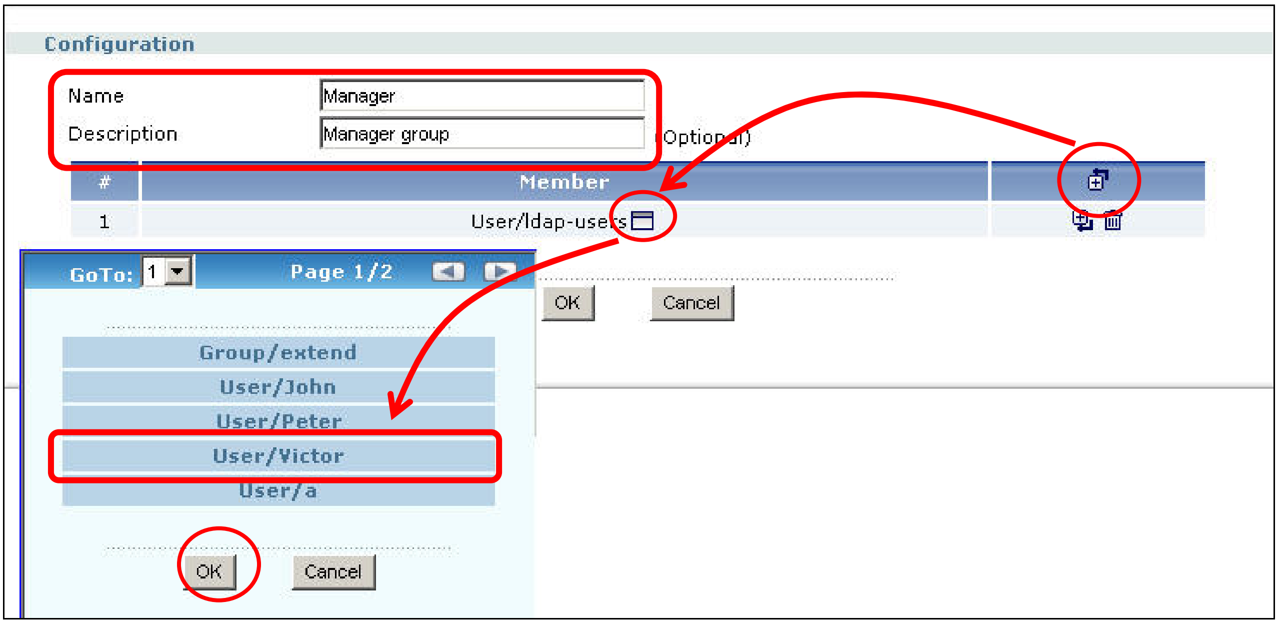

**User Configuration**

| | | |
|---|---|---|
| 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) |

Corresponding CLI commands for your reference

```
[0] username Victor password 1234 user-type user
[1] username Victor description Local User
[2] username Victor logon-lease-time 1440
[3] username Victor logon-re-auth-time 1440
```

3. Switch to the Group tab, create group 'Manager' and add member 'Victor' to it on the following figure.



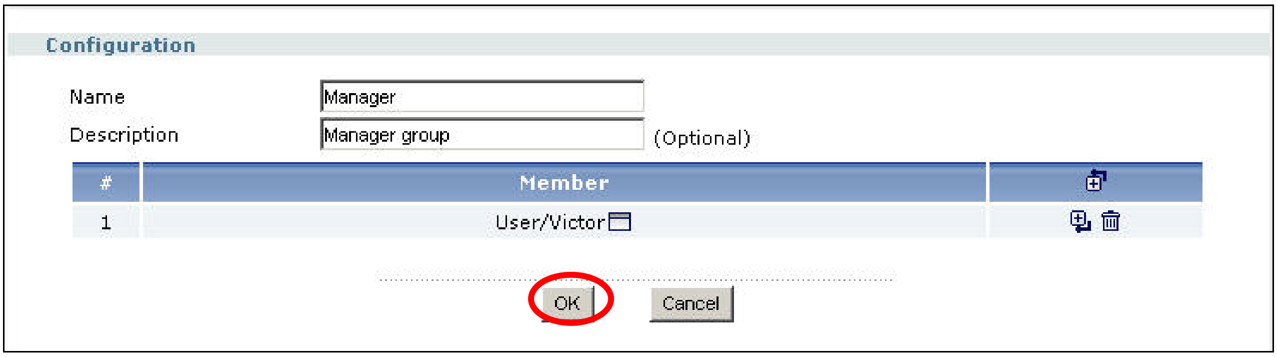
Configuration

Name: Manager

Description: Manager group (Optional)

| # | Member |
|---|---|
| 1 | User/ldap-users |

4. Then press ‘OK’ button to complete the group creation.



Configuration

Name: Manager

Description: Manager group (Optional)

| # | Member |
|---|---|
| 1 | User/Victor |

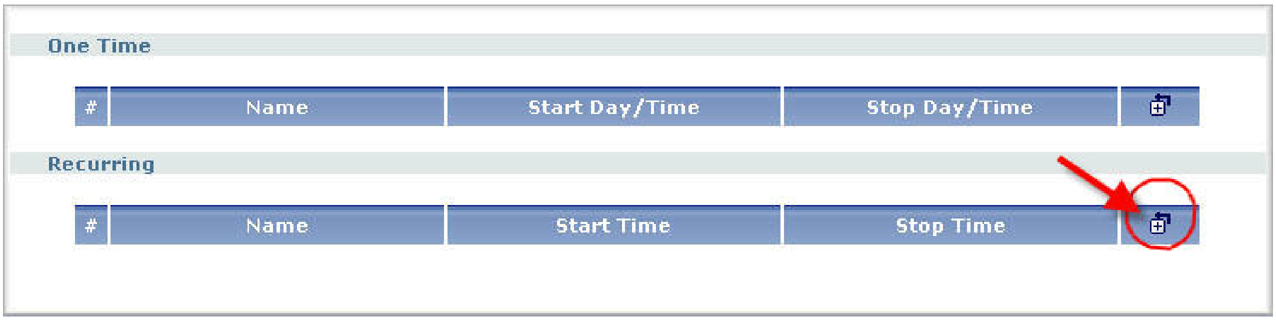
Corresponding CLI commands for your reference

```
[0] groupname Manager
[1] description Manager group
[2] user Victor
[3] exit
```

5. Create two more group ‘Engineer1’ and Engineer2’ to and add ‘Peter’ and ‘John’ in similarly.

**Step2.** Create schedule object

1. Go to menu **Object** > **Schedule**, click the “+” from the Recurring schedule to create a new schedule as following figures.

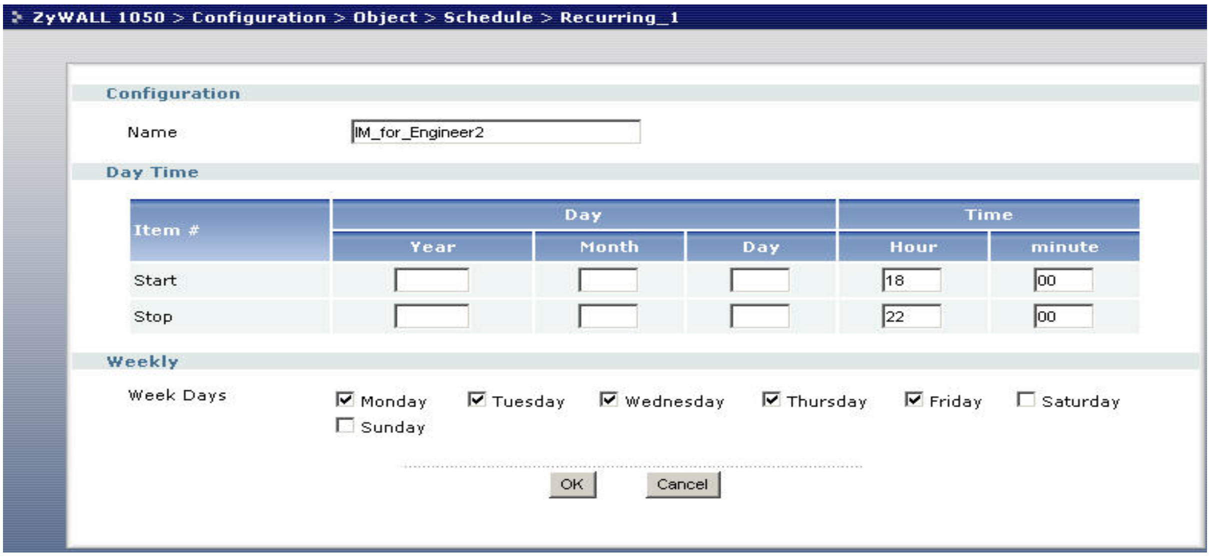


One Time

| # | Name | Start Day/Time | Stop Day/Time | ⊞ |
|---|---|---|---|---|

Recurring

| # | Name | Start Time | Stop Time | ⊞ |
|---|---|---|---|---|



ZyWALL 1050 > Configuration > Object > Schedule > Recurring_1

Configuration

Name: IM_for_Engineer2

Day Time

| Item # | Day | | | Time | |
|---|---|---|---|---|---|
| | Year | Month | Day | Hour | minute |
| Start | | | | 18 | 00 |
| Stop | | | | 22 | 00 |

Weekly

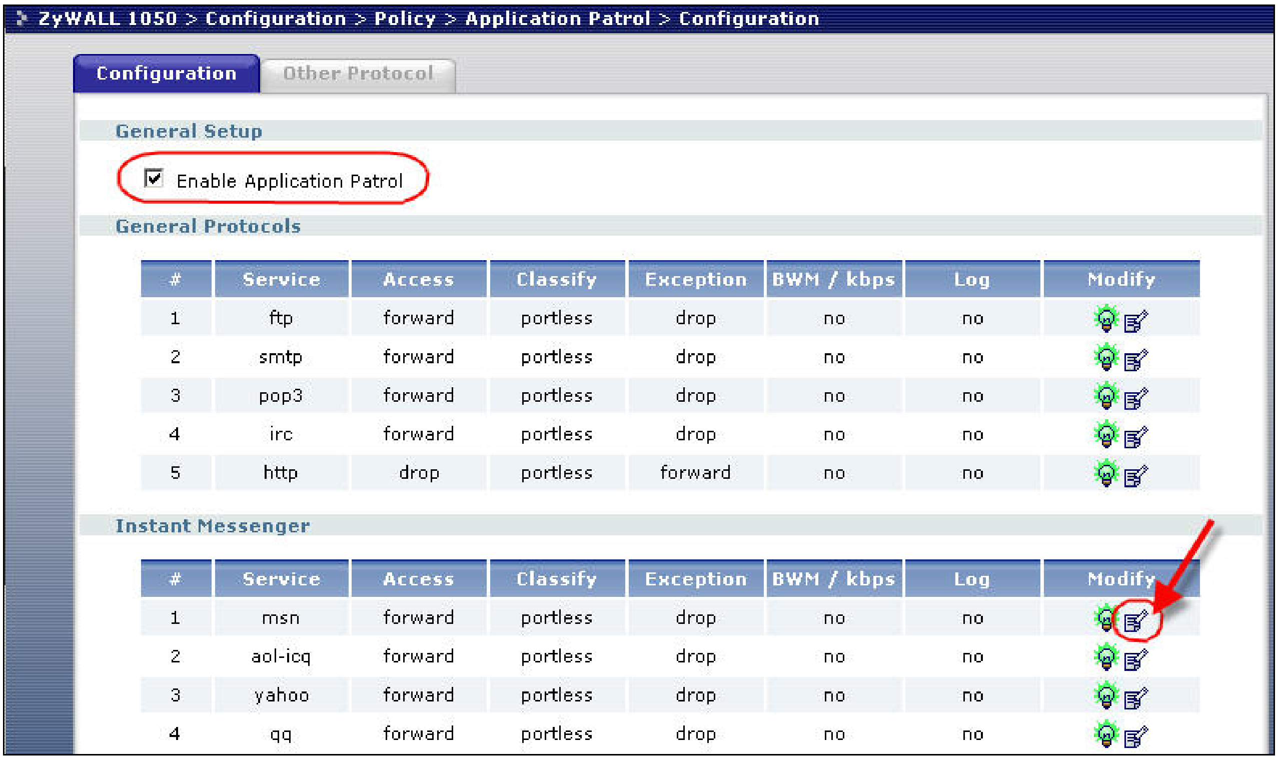
Week Days: ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday □ Saturday □ Sunday

- Corresponding CLI commands for your reference

```
[0] schedule-object IM_for_Engineer2 18:00 22:00 mon tue wed thu
fri
```

**Step3.** Configuration in L7 application control -- App Patrol

1. Go to menu **Configuration** > **Policy** > **APP. Patrol**
2. Enable the application patrol.
3. Choose the application to define further setting. In Instant Messenger and Peer-to-Peer category, there are several applications allowed to be configured. We take ‘MSN’ for example. Click the modify icon to get to the further configuration.



ZyWALL 1050 > Configuration > Policy > Application Patrol > Configuration
Configuration
Other Protocol

General Setup

☑ Enable Application Patrol

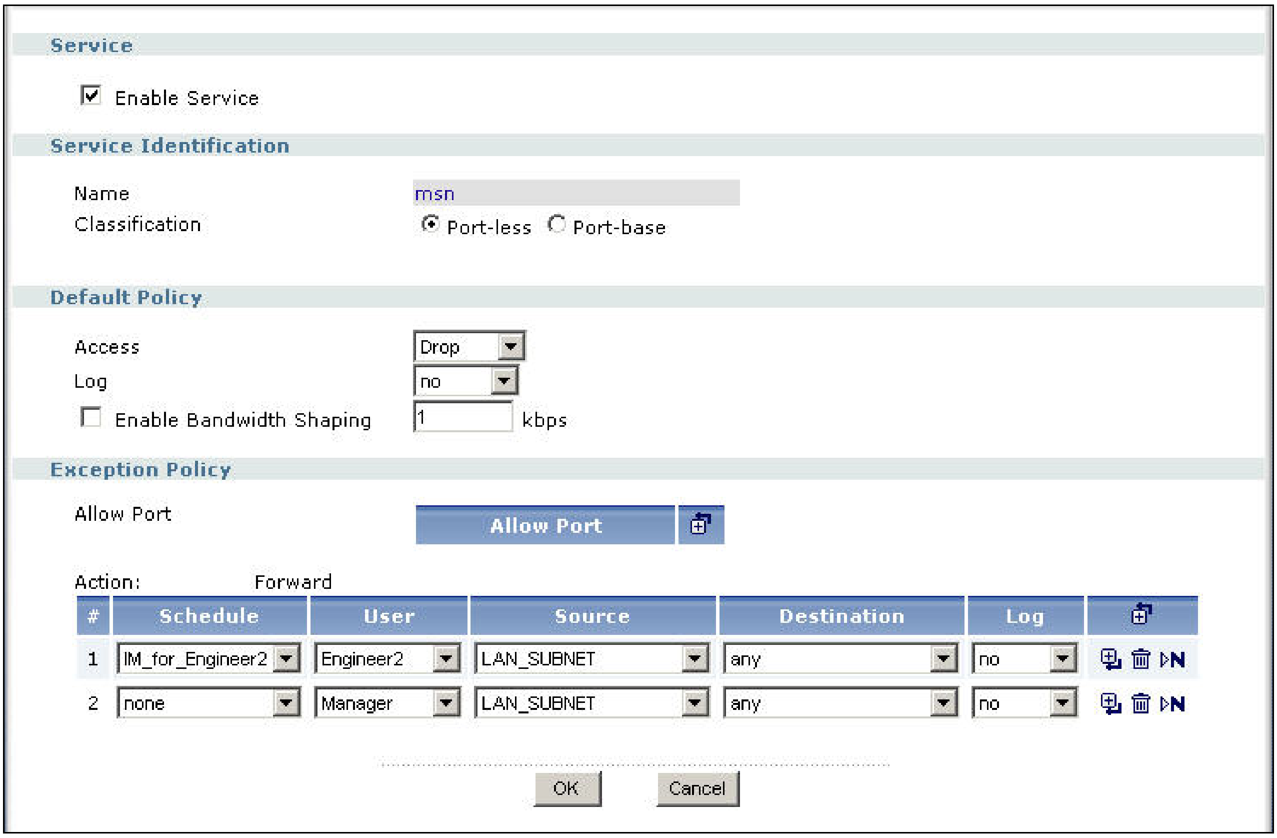
General Protocols

| # | Service | Access | Classify | Exception | BWM / kbps | Log | Modify |
|---|---|---|---|---|---|---|---|
| 1 | ftp | forward | portless | drop | no | no | |
| 2 | smtp | forward | portless | drop | no | no | |
| 3 | pop3 | forward | portless | drop | no | no | |
| 4 | irc | forward | portless | drop | no | no | |
| 5 | http | drop | portless | forward | no | no | |

Instant Messenger

| # | Service | Access | Classify | Exception | BWM / kbps | Log | Modify |
|---|---|---|---|---|---|---|---|
| 1 | msn | forward | portless | drop | no | no | |
| 2 | aol-icq | forward | portless | drop | no | no | |
| 3 | yahoo | forward | portless | drop | no | no | |
| 4 | qq | forward | portless | drop | no | no | |

4. Enable the service
5. Choose the classification ‘Port-less’ to enable layer 7 packet inspection.
6. Choose access ‘Drop’, then the action in the exception policy will change to ‘Forward’ automatically.
7. Click ‘+’ to add two exception rules for 2 groups, Engineer2 and Manager, as on the figure shown below.



**Service**

☑ Enable Service

**Service Identification**

Name: msn

Classification: ● Port-less ○ Port-base

**Default Policy**

Access: Drop

Log: no

□ Enable Bandwidth Shaping: 1 kbps

**Exception Policy**

Allow Port: Allow Port

Action: Forward

| # | Schedule | User | Source | Destination | Log |
|---|---|---|---|---|---|
| 1 | IM_for_Engineer2 | Engineer2 | LAN_SUBNET | any | no |
| 2 | none | Manager | LAN_SUBNET | any | no |

Corresponding CLI commands for your reference

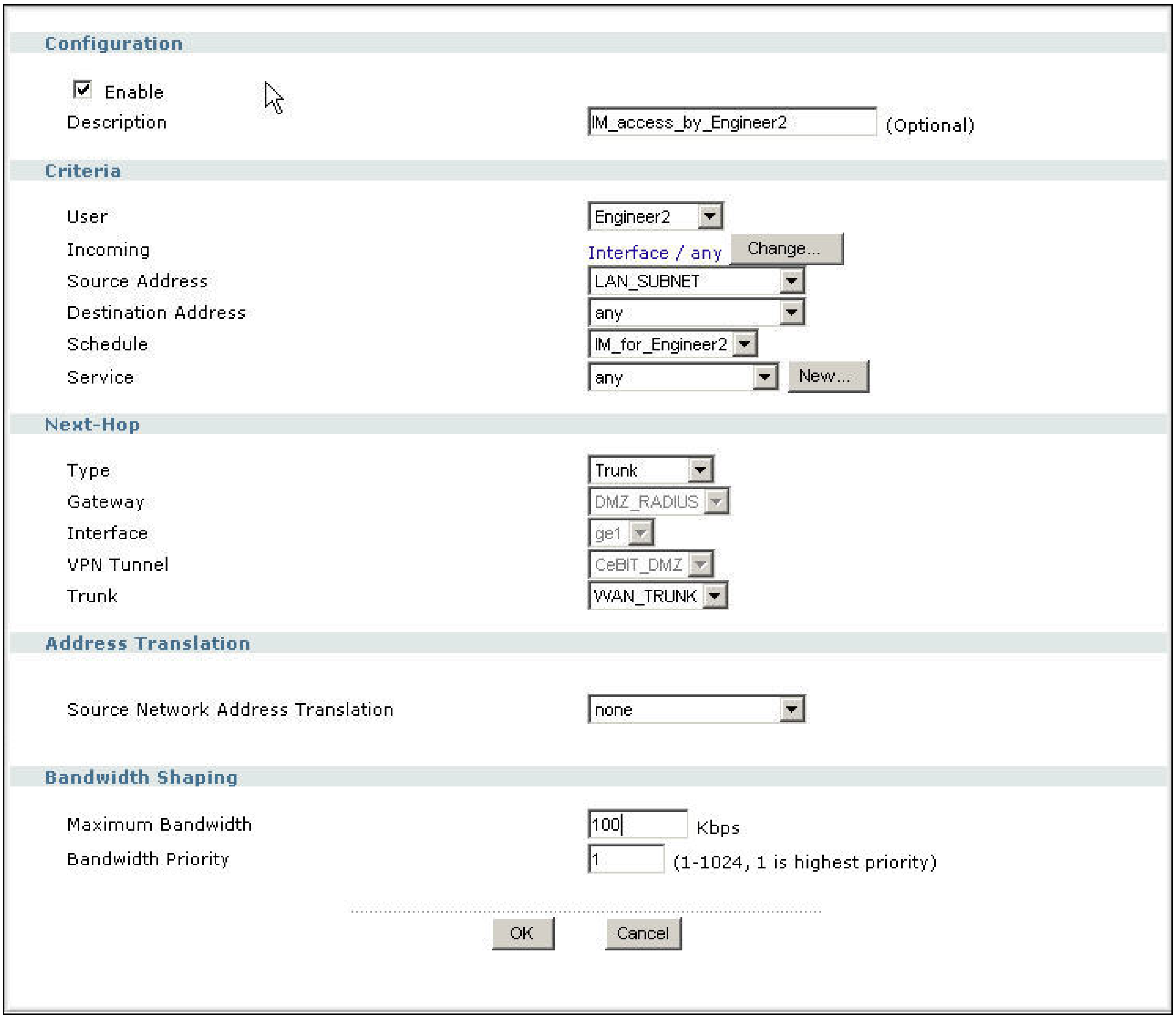
```
[0] app msn drop exception forward
[1] no app msn log
[2] app msn activate
[3] app msn mode portless
[4] no app msn bwm
[5] app msn bandwidth 1
[6] app msn exception 1
[7] schedule IM_for_Engineer2
[8] user Engineer2
[9] source LAN_SUBNET
[10] no destination
[11] no log
[12] exit
[13] app msn exception 2
[14] no schedule
[15] user Manager
[16] source LAN_SUBNET
[17] no destination
[18] no log
[19] exit
```

**Step4.** Configuration of the Policy Route

1. Got to menu **Configuration** > **Policy** > **Route**

2. Create a new policy route rule by clicking the '+' icon. Fill out the settings as on the figure shown below.
3. Note that:
   We choose user the group 'Engineer2'.
   Source is a LAN subnet
   Schedule is what we just created and named 'IM_for_Engineer2'
   From Next-Hop, choose 'Trunk' and choose 'WAN_Trunk' from the Trunk field.
   Enter the maximum bandwidth 100Kbps.

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



Configuration

☑ Enable

Description: IM_access_by_Engineer2 (Optional)

Criteria

User: Engineer2

Incoming: Interface / any

Source Address: LAN_SUBNET

Destination Address: any

Schedule: IM_for_Engineer2

Service: any

Next-Hop

Type: Trunk

Gateway: DMZ_RADIUS

Interface: ge1

VPN Tunnel: CeBIT_DMZ

Trunk: WAN_TRUNK

Address Translation

Source Network Address Translation: none

Bandwidth Shaping

Maximum Bandwidth: 100 Kbps

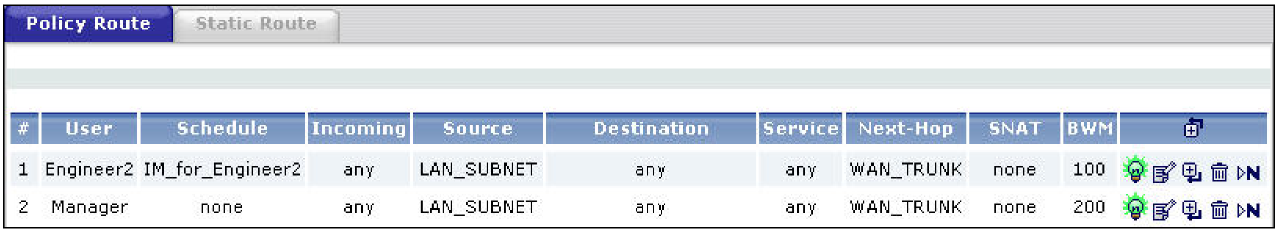
Bandwidth Priority: 1 (1-1024, 1 is highest priority)

Corresponding CLI commands for your reference

```
[0] policy 1
[1] no deactivate
[2] description IM_access_by_Engineer2
[3] user Engineer2
[4] no interface
```

```
[5] no tunnel
[6] source LAN_SUBNET
[7] destination any
[8] schedule IM_for_Engineer2
[9] service any
[10] next-hop trunk WAN_TRUNK
[11] no snat
[12] bandwidth 100 priority 1
[13] exit
```

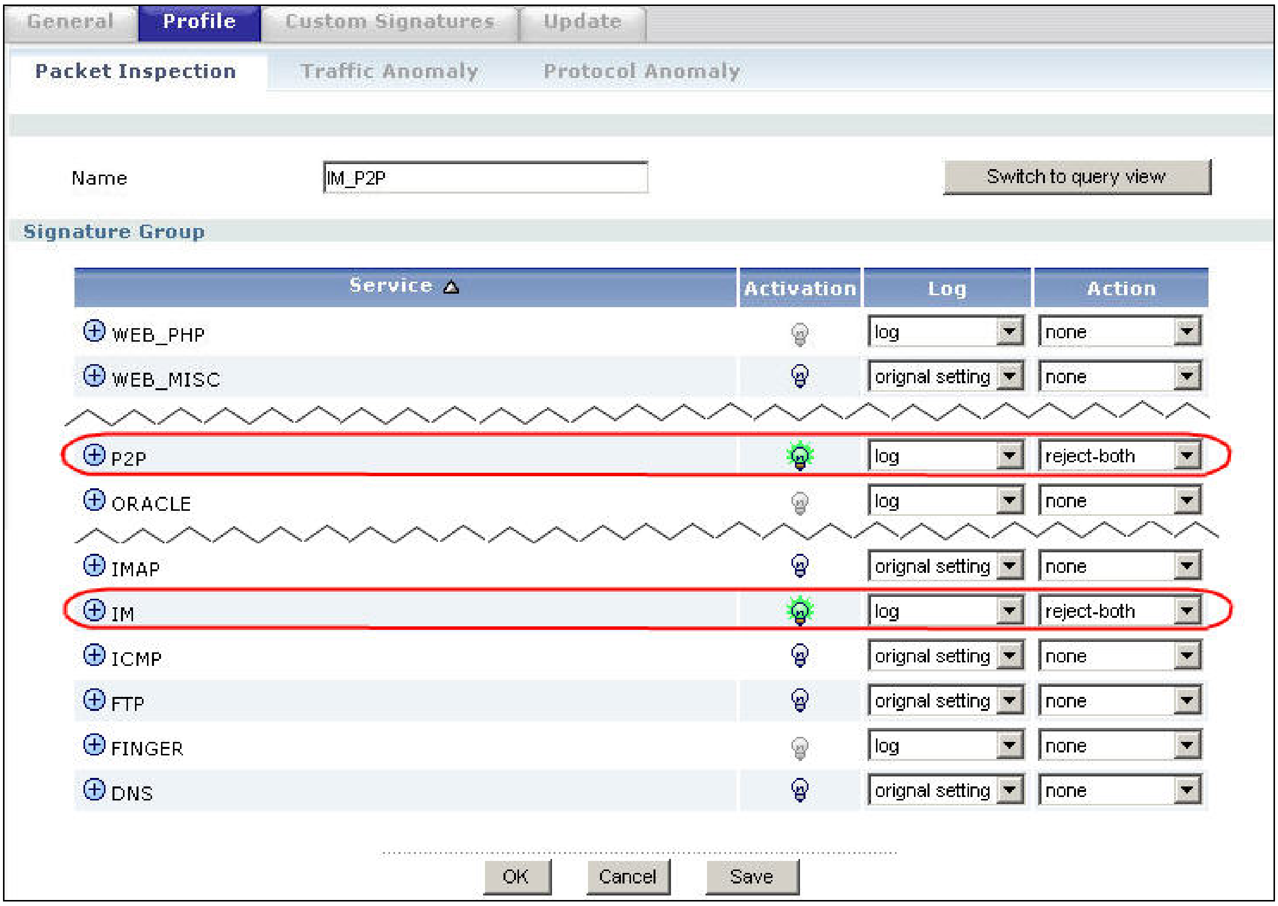
6. Then create another policy route rule for the group ‘Manager’. You will get the result as below after both rules are done.



| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM |
|---|---|---|---|---|---|---|---|---|---|
| 1 | Engineer2 | IM_for_Engineer2 | any | LAN_SUBNET | any | any | WAN_TRUNK | none | 100 |
| 2 | Manager | none | any | LAN_SUBNET | any | any | WAN_TRUNK | none | 200 |

**Step5.** Configuration of the IDP

1. First of all, make sure that you’ve registered and enabled IDP function from the GUI menu **Registration**.
2. Then create an IDP profile by going to the menu **Policy** > **IDP** > **Profile tab** > **Packet inspection tab**.
3. Name it as ‘IM_P2P’ and enable IM and P2P from application list.
4. Click **Ok** button then.

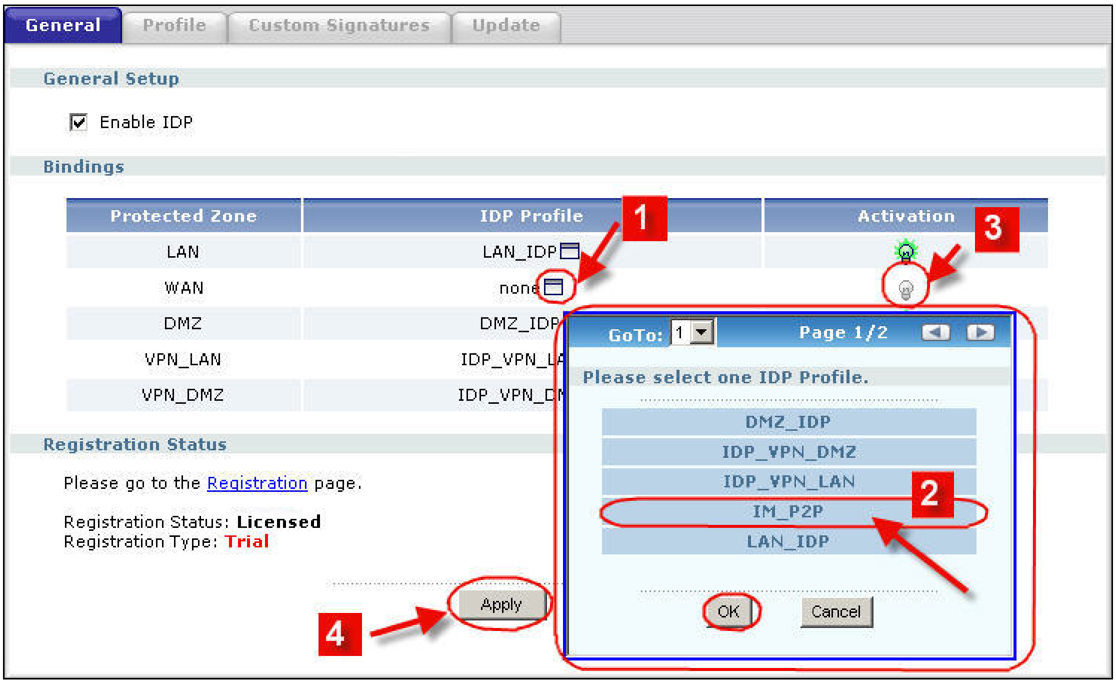


Name: IM_P2P

Signature Group

| Service | Activation | Log | Action |
|---|---|---|---|
| ⊕ WEB_PHP | ○ | log | none |
| ⊕ WEB_MISC | ◐ | orignal setting | none |
| ⊕ P2P | ● | log | reject-both |
| ⊕ ORACLE | ○ | log | none |
| ⊕ IMAP | ◐ | orignal setting | none |
| ⊕ IM | ● | log | reject-both |
| ⊕ ICMP | ◐ | orignal setting | none |
| ⊕ FTP | ◐ | orignal setting | none |
| ⊕ FINGER | ○ | log | none |
| ⊕ DNS | ◐ | orignal setting | none |

5. Back to **IDP** > **General**, choose the IDP profile we just created for WAN zone as on the figure below.
6. Enable it and click **Apply** button then.



General Setup

☑ Enable IDP

Bindings

| Protected Zone | IDP Profile | Activation |
|---|---|---|
| LAN | LAN_IDP | |
| WAN | none | |
| DMZ | DMZ_IDP | |
| VPN_LAN | IDP_VPN_LA | |
| VPN_DMZ | IDP_VPN_DI | |

Registration Status

Please go to the Registration page.

Registration Status: **Licensed**
Registration Type: **Trial**

Apply

GoTo: 1 Page 1/2

Please select one IDP Profile.

- DMZ_IDP
- IDP_VPN_DMZ
- IDP_VPN_LAN
- IM_P2P
- LAN_IDP

OK Cancel

## 2.2 Managing WLAN

### 2.2.1 Why the wireless networks need to be managed?

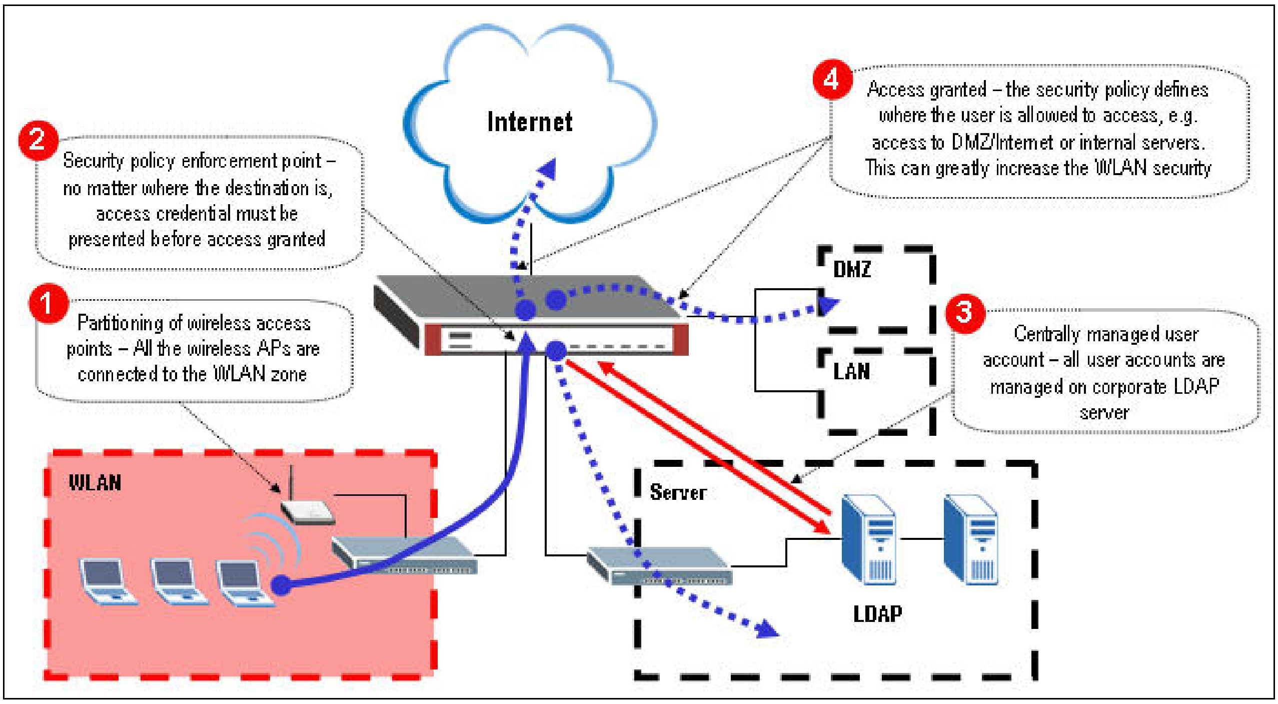
Wireless networks reduce the cost of wired cabling and brings convenience to people to access anytime and anywhere like in the office or in a community. However, they might be harmful under certain conditions.

1. People misuse － People who you don't know might probe your AP and break in your network without your permission. It is usually called "Wardriving". When you are using wireless link to transfer confidential data, these important data might be eavesdropped by somebody.

2. People mis-configuration － In company, it's MIS's headache to control the "Rogue APs". Employees might connect an AP with non-security-mechanism or weak WEP/WAP passphrase to company's network without informing MIS people. It will create a security hole allowing outsiders to bypass the company's security checking and to access the company's confidential information or even use some tools to damage the company's network service.

### 2.2.2 What can we do against the wireless insecurity?

We recommend that Wireless AP must be isolated from your Intranet. Also, there must be a mechanism to centrally manage access privileges and access credentials regardless of whether the clients are wired or wireless.


Internet
2 Security policy enforcement point – no matter where the destination is, access credential must be presented before access granted
1 Partitioning of wireless access points – All the wireless APs are connected to the WLAN zone
4 Access granted – the security policy defines where the user is allowed to access, e.g. access to DMZ/Internet or internal servers. This can greatly increase the WLAN security
3 Centrally managed user account – all user accounts are managed on corporate LDAP server
DMZ
LAN
WLAN
Server
LDAP

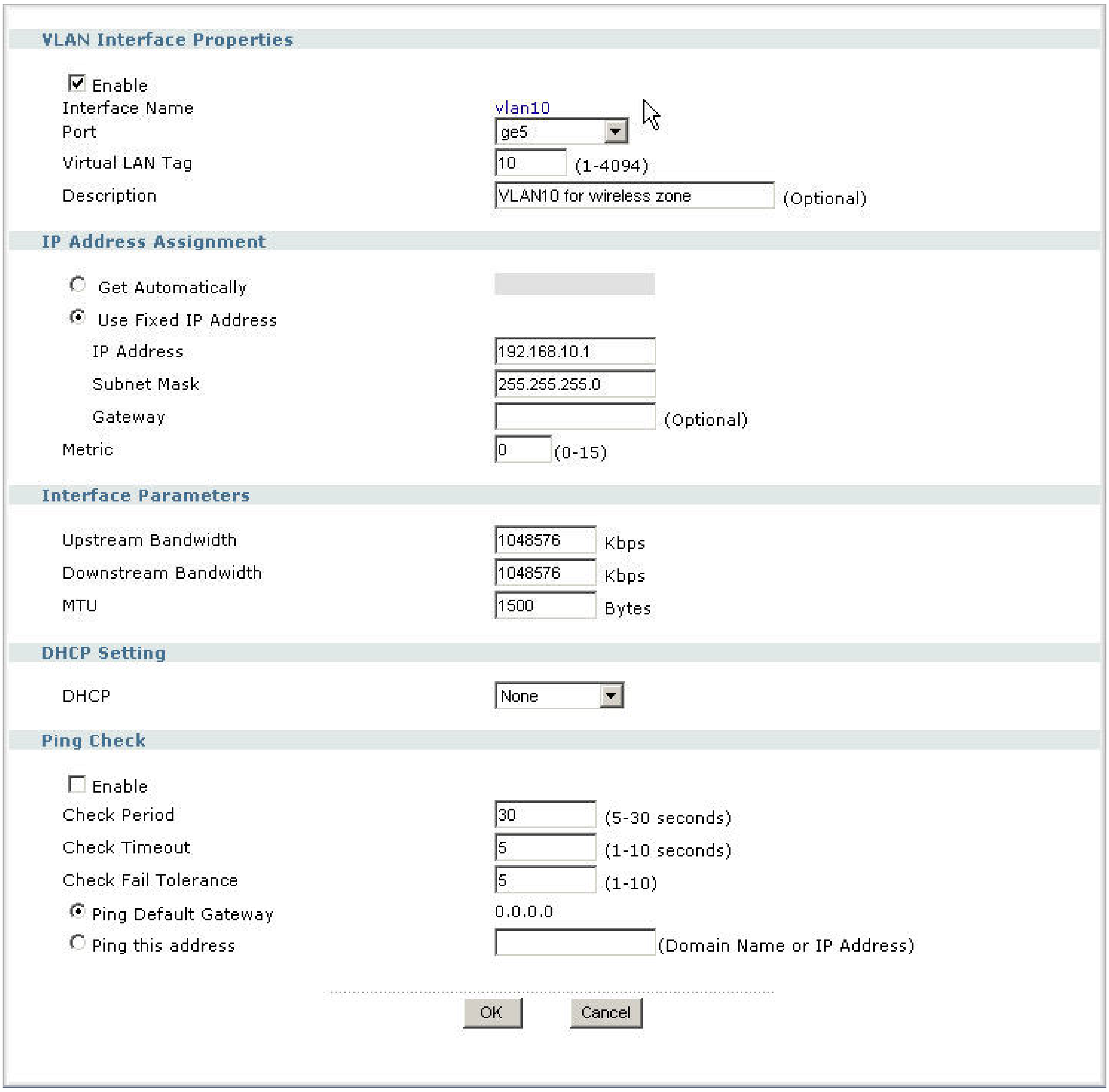
We are going to complete the following setting.

1. Create a VLAN interface dedicated for wireless access
2. Define WLAN zones
3. Enable Force Authentication Page Redirect
4. Configure LDAP server information.
5. Configure WWW Authentication Method
6. Define user/group to have different kind of access granted

**Step1.** Create a VLAN interface dedicated for wireless access
In this example, all the employees or visitors can access Internet through wireless network. For visitors, we want them to limit their access to Internet only while the employees can access all including LAN/DMZ zones. Through packet with VLAN tag added, this will be controlled by ZyWALL acting as a security guide which door(route) to open for packets according to LDAP server's authentication.

1. Go to menu **Network** > **Interface** > **VLAN**.
2. Create a VLAN interface binds with interface ge5 for wireless network. Here, we define:
   Interface name is vlan10 (same as the vlan tag id for its not being confusing).
   Choose 'ge5' for physical port interface that we want to bind with.
   Virtual VLAN Tag is 10.
   Give it a clear description.
   Use the fixed IP address with 192.168.10.1/24.

Leave other fields as default and press 'ok' button



**VLAN Interface Properties**

| | |
|---|---|
| ☑ Enable | |
| Interface Name | vlan10 |
| Port | ge5 |
| Virtual LAN Tag | 10 (1-4094) |
| Description | VLAN10 for wireless zone (Optional) |

**IP Address Assignment**

| | |
|---|---|
| ○ Get Automatically | |
| ● Use Fixed IP Address | |
| IP Address | 192.168.10.1 |
| 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 |

**DHCP Setting**

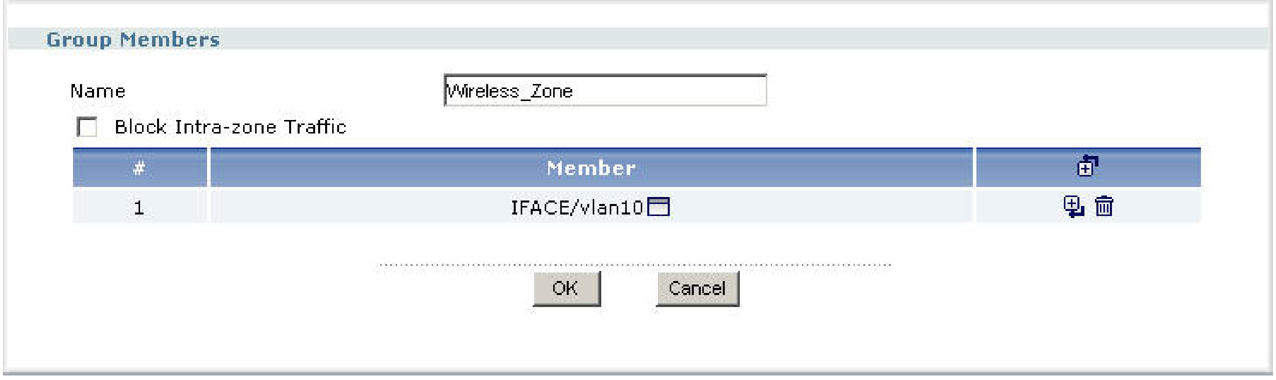
| | |
|---|---|
| DHCP | None |

**Ping Check**

| | |
|---|---|
| □ Enable | |
| Check Period | 30 (5-30 seconds) |
| Check Timeout | 5 (1-10 seconds) |
| Check Fail Tolerance | 5 (1-10) |
| ● Ping Default Gateway | 0.0.0.0 |
| ○ Ping this address | (Domain Name or IP Address) |

**Step2.** Define WLAN zones

Go to menu **Network** > **Zone**. Define a zone for wireless and bind it to interface "vlan10".



Group Members

| | |
|---|---|
| Name | Wireless_Zone |
| □ Block Intra-zone Traffic | |

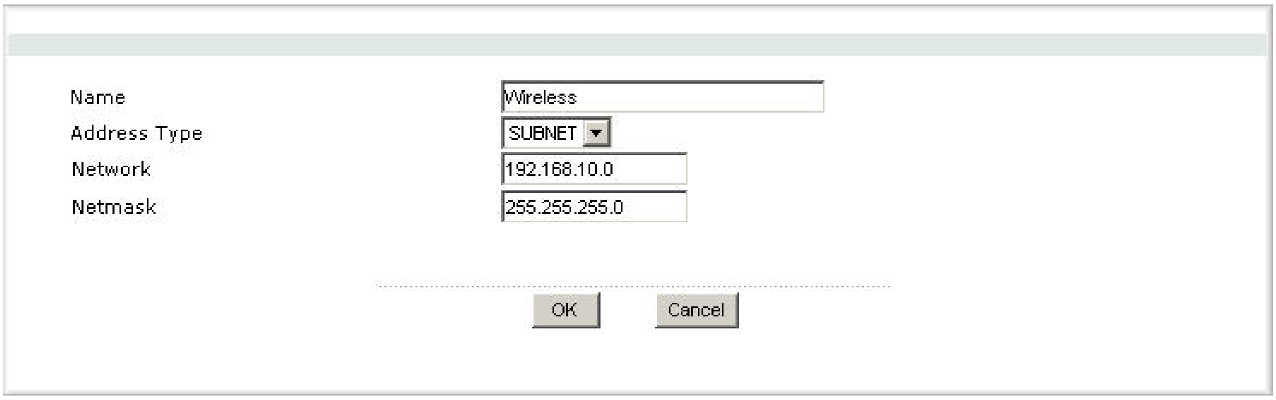
| # | Member | |
|---|---|---|
| 1 | IFACE/vlan10 | |

Corresponding CLI commands for your reference

```
[0] zone Wireless_Zone
[1] no block
[2] interface vlan10
[3] exit
```

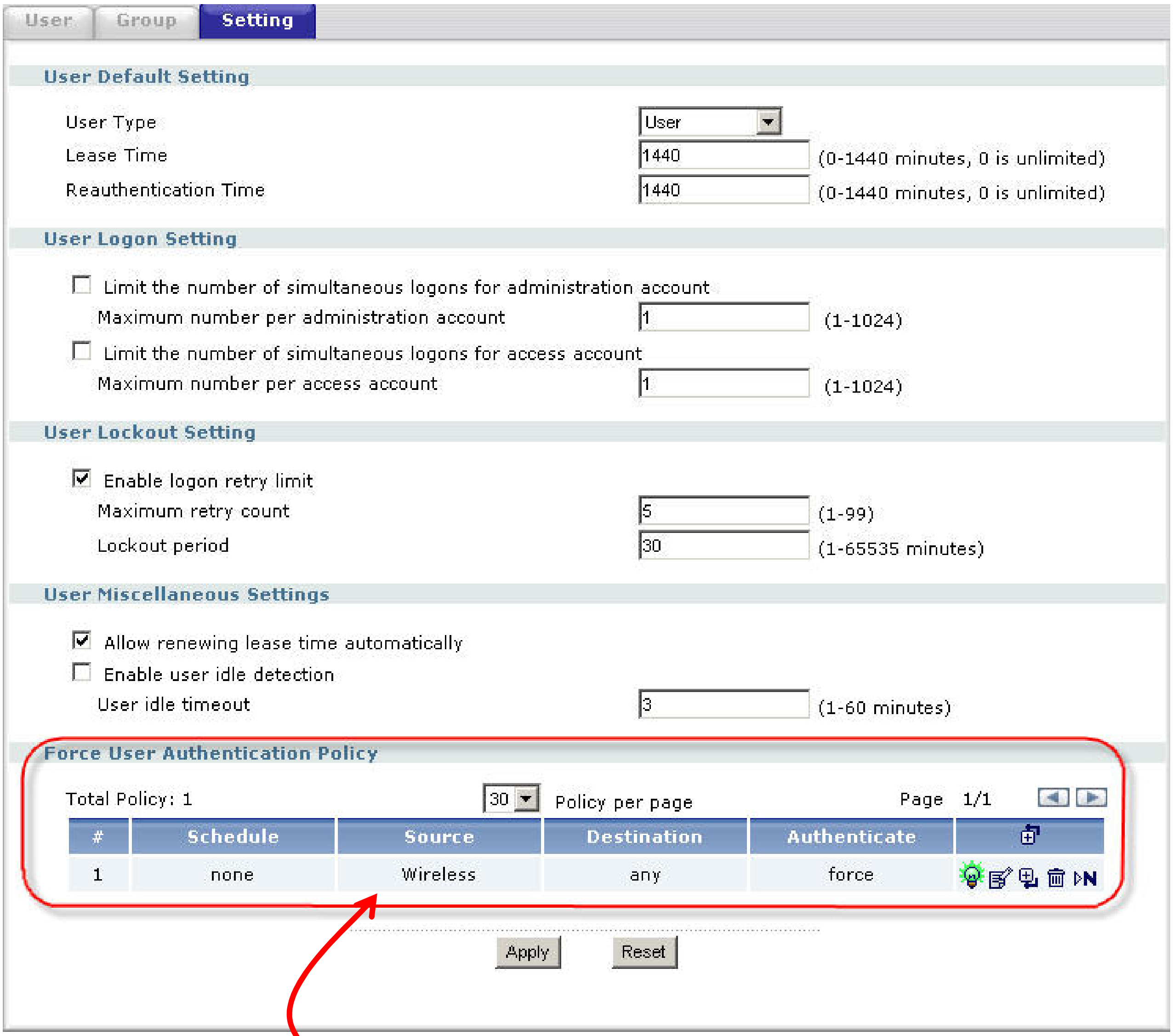
**Step3.** Enable Force Authentication Page Redirect

1. Go to menu **Object** > **Address**, and create a subnet for wireless network. Name it ‘Wireless’ for further configuration use.



| | |
|---|---|
| Name | Wireless |
| Address Type | SUBNET |
| Network | 192.168.10.0 |
| Netmask | 255.255.255.0 |

2. Go to menu **User/Group** > **Setting** > **Force User Authentication Policy**, click ‘+’ to force all the packets from wireless network to be redirected to the authentication page.



**User Default Setting**

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

**User Logon Setting**

☐ Limit the number of simultaneous logons for administration account
Maximum number per administration account: 1 (1-1024)
☐ Limit the number of simultaneous logons for access account
Maximum number per access account: 1 (1-1024)

**User Lockout Setting**

☑ Enable logon retry limit
Maximum retry count: 5 (1-99)
Lockout period: 30 (1-65535 minutes)

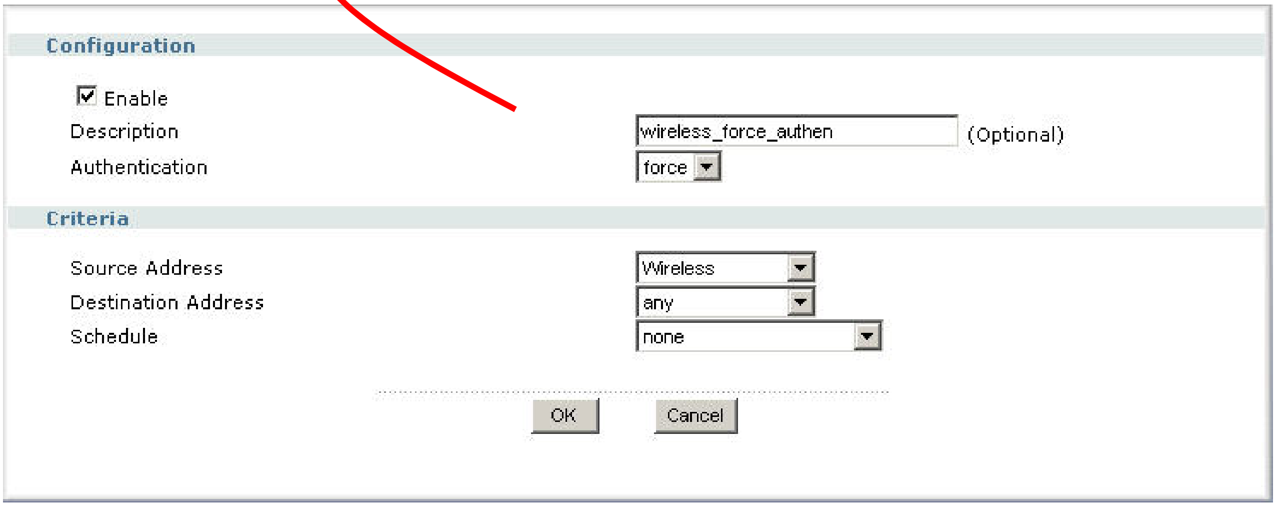
**User Miscellaneous Settings**

☑ Allow renewing lease time automatically
☐ Enable user idle detection
User idle timeout: 3 (1-60 minutes)

**Force User Authentication Policy**

Total Policy: 1 | 30 Policy per page | Page 1/1

| # | Schedule | Source | Destination | Authenticate |
|---|---|---|---|---|
| 1 | none | Wireless | any | force |



**Configuration**

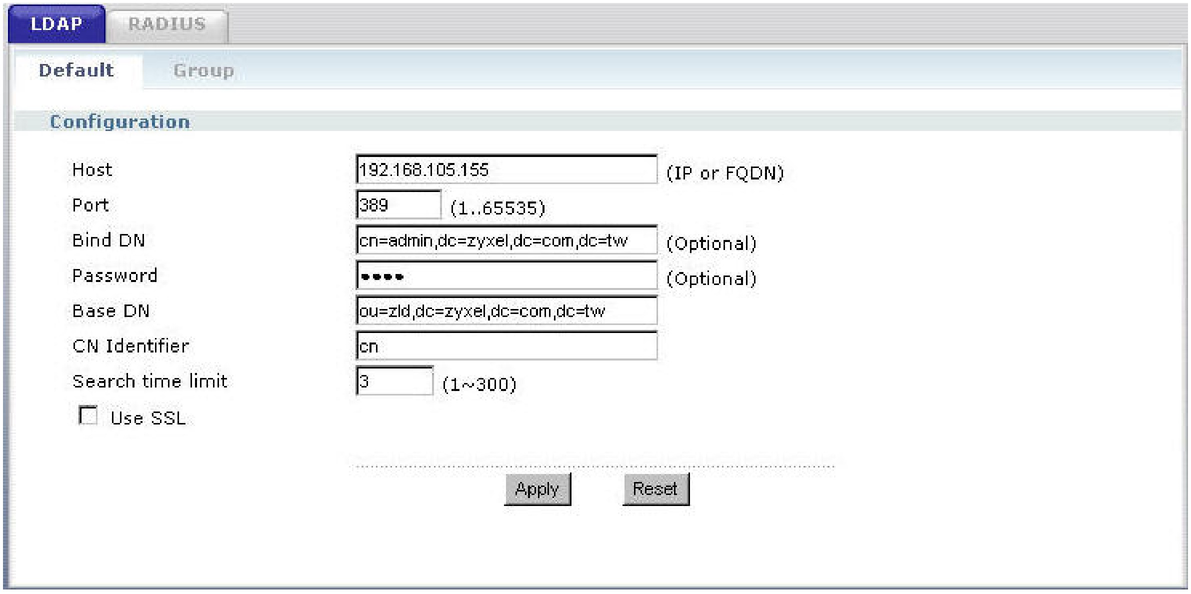
☑ Enable
Description: wireless_force_authen (Optional)
Authentication: force

**Criteria**

Source Address: Wireless
Destination Address: any
Schedule: none

**Step4.** Configure the LDAP server information.

1. Go to menu **Object** > **AAA server** > **LDAP tab** > **Default**, configure the IP address, port and other necessary information. Then click the **Apply** button.



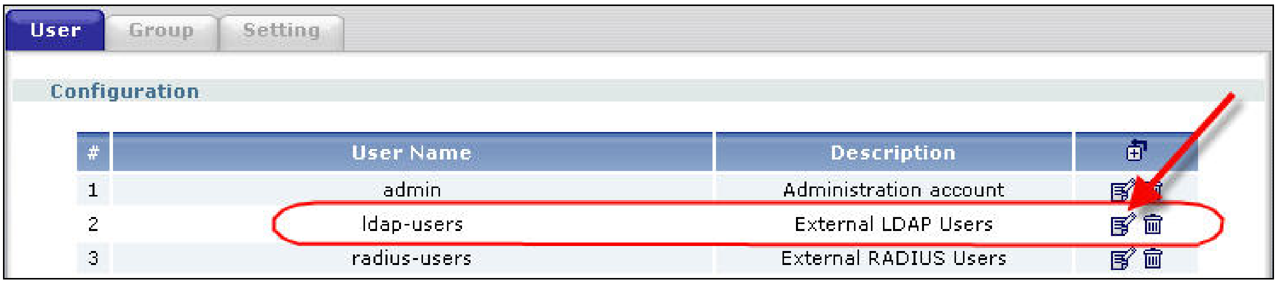
Host 192.168.105.155 (IP or FQDN)
Port 389 (1..65535)
Bind DN cn=admin,dc=zyxel,dc=com,dc=tw (Optional)
Password •••• (Optional)
Base DN ou=zld,dc=zyxel,dc=com,dc=tw
CN Identifier cn
Search time limit 3 (1~300)
□ Use SSL

***Note:*** Please consult your LDAP server admin to configure this part since LDAP has special setting than RADIUS server.

Corresponding CLI commands for your reference

```
[0] ldap-server host 192.168.105.155
[1] no ldap-server ssl
[2] ldap-server port 389
[3] ldap-server password 1234
[4] ldap-server basedn ou=ald,dc=zyxel,dc=com,dc=tw
[5] ldap-server binddn cn=admin,dc=zyxel,dc=com,dc=tw
[6] ldap-server search-time-limit 3
[7] ldap-server cn-identifier cn
```

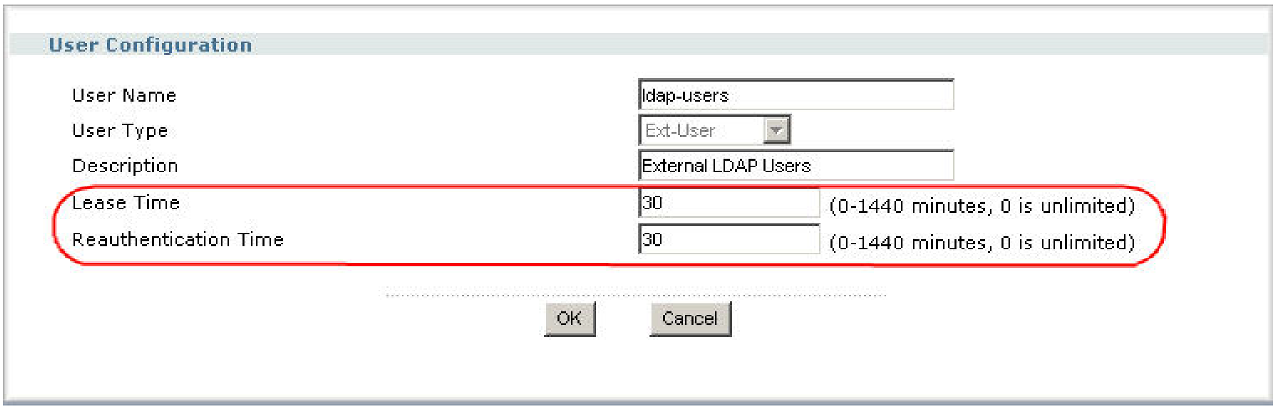
2. Co-work with LDAP server admin to create user/groups with lease time / re-authentication time attributes configured.
3. Go to menu **User/Group** > **User**, configure user “ldap-users” for “non-employees” by clicking the modify icon.



Configuration

| # | User Name | Description | |
|---|---|---|---|
| 1 | admin | Administration account | |
| 2 | ldap-users | External LDAP Users | |
| 3 | radius-users | External RADIUS Users | |

4. For security reasons, those user's attributes which cannot be found in LDAP server will get shorter lease and re-authentication time. Here we use 30 minutes for example.

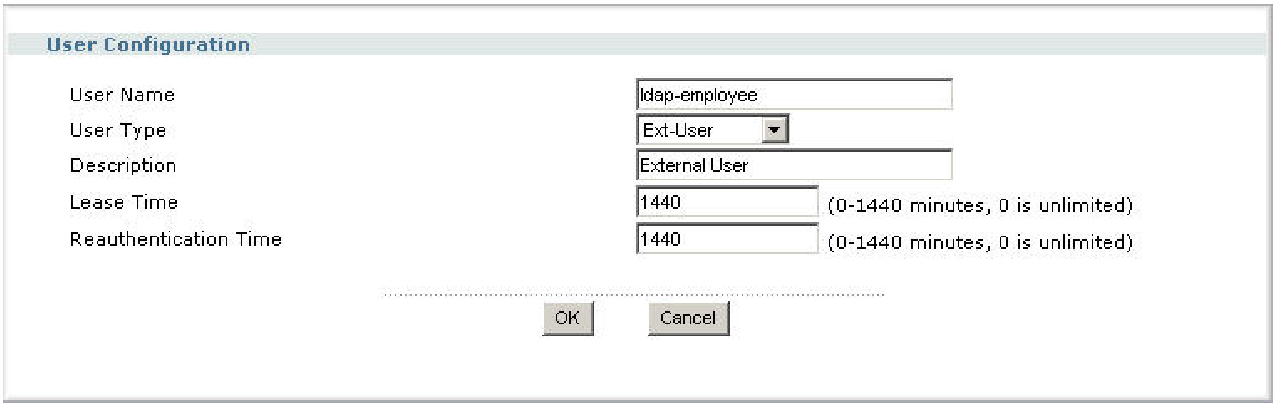


User Configuration

| | | |
|---|---|---|
| User Name | ldap-users | |
| User Type | Ext-User | |
| Description | External LDAP Users | |
| Lease Time | 30 | (0-1440 minutes, 0 is unlimited) |
| Reauthentication Time | 30 | (0-1440 minutes, 0 is unlimited) |

Corresponding CLI commands for your reference

```
[0] username ldap-users user-type ext-user
[1] username ldap-users description External LDAP Users
[2] username ldap-users logon-lease-time 30
[3] username ldap-users logon-re-auth-time 30
```



User Configuration

| | | |
|---|---|---|
| User Name | ldap-employee | |
| User Type | Ext-User | |
| Description | External User | |
| Lease Time | 1440 | (0-1440 minutes, 0 is unlimited) |
| Reauthentication Time | 1440 | (0-1440 minutes, 0 is unlimited) |

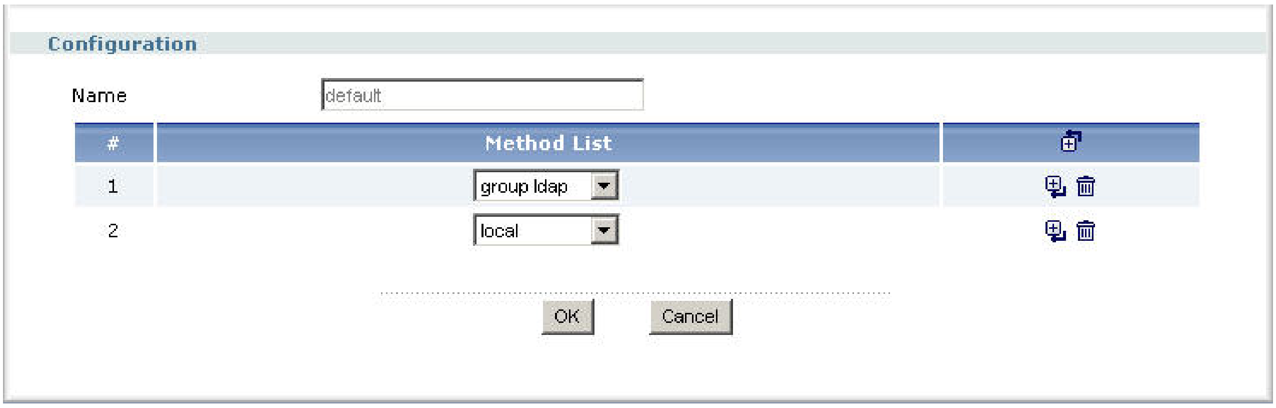
Corresponding CLI commends for your reference

```
[0] username ldap-employee user-type ext-user
[1] username ldap-employee description External User
[2] username ldap-employee logon-lease-time 1440
[3] username ldap-employee logon-re-auth-time 1440
```

**Step5.** Configure WWW Authentication Method

1. Go to menu **Object** > **AAA server**, modify the 'default' profile.
2. Configure the profile as following to be authenticated by LDAP server then local database in ZyWALL.

*Note:* The "group ldap" shown in the figure below will use the settings in **LDAP** > **Default**, rather than **LDAP** >**Group**.

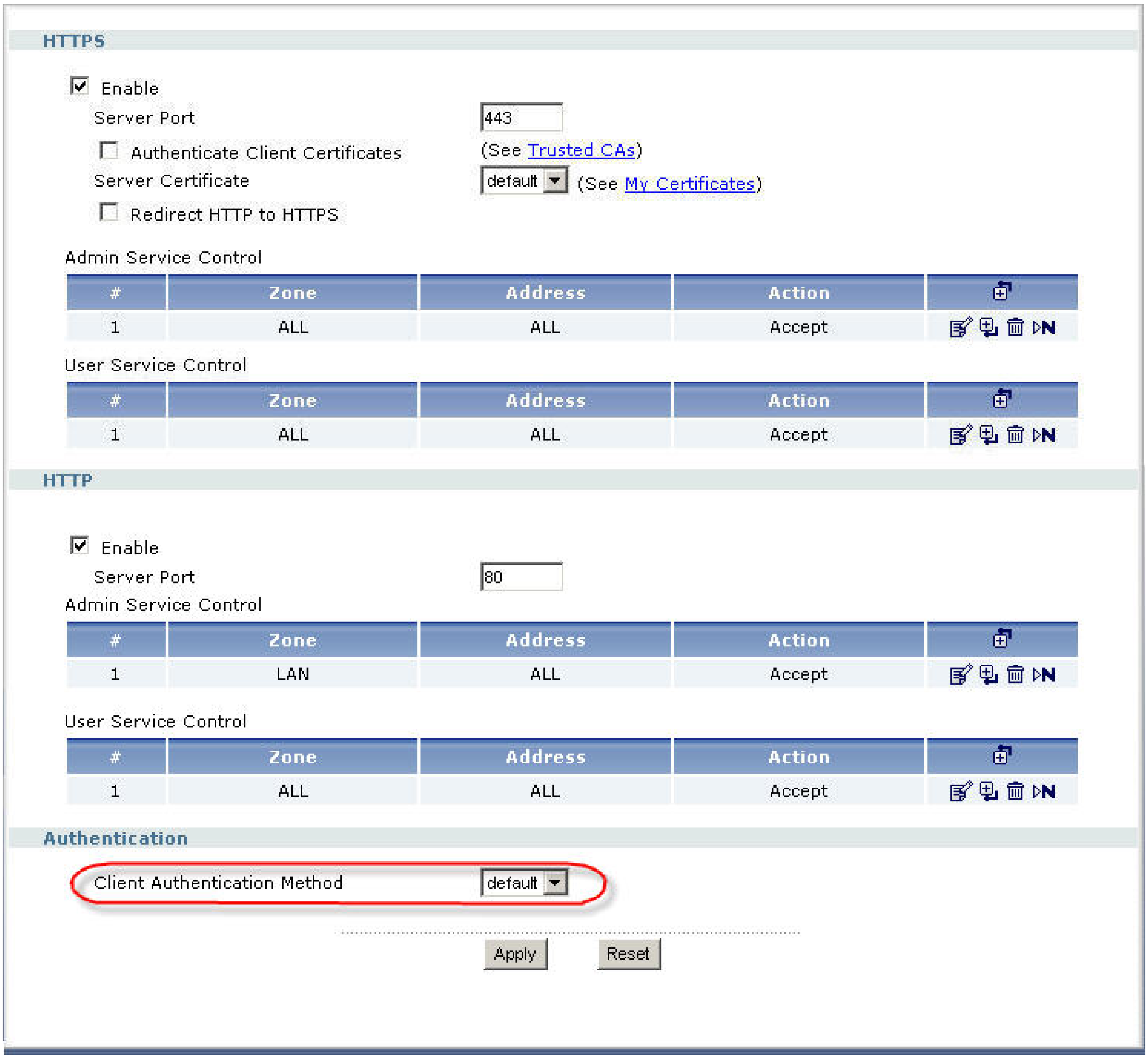


Configuration

Name default

| # | Method List | |
|---|---|---|
| 1 | group ldap | |
| 2 | local | |

3. Go to menu **System** > **WWW**, make sure the authentication method is the profile we just modified. (That is, if I just have created another profile which is not named as 'default', then here we have to choose it.)



HTTPS

☑ Enable

Server Port 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate default (See My Certificates)

☐ Redirect HTTP to HTTPS

Admin Service Control

| # | Zone | Address | Action |
|---|---|---|---|
| 1 | ALL | ALL | Accept |

User Service Control

| # | Zone | Address | Action |
|---|---|---|---|
| 1 | ALL | ALL | Accept |

HTTP

☑ Enable

Server Port 80

Admin Service Control

| # | Zone | Address | Action |
|---|---|---|---|
| 1 | LAN | ALL | Accept |

User Service Control

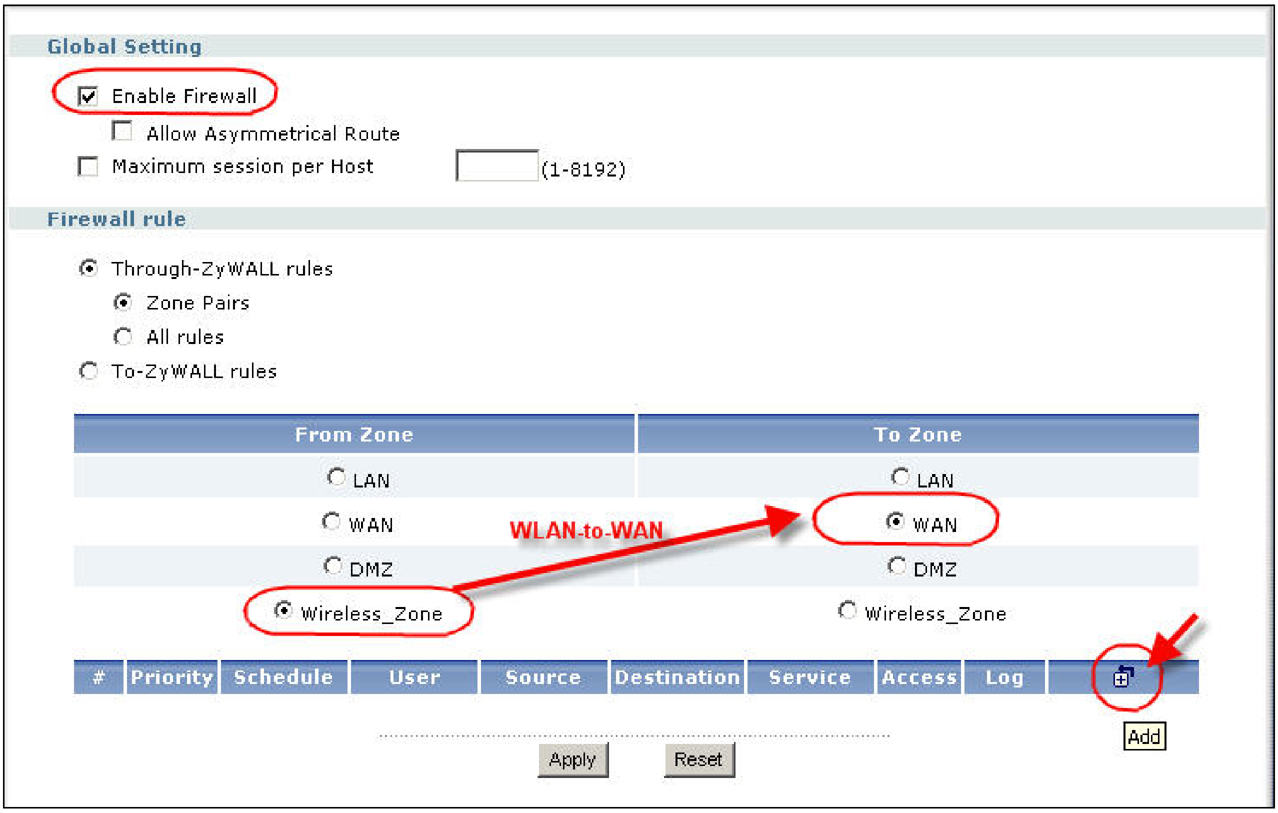
| # | Zone | Address | Action |
|---|---|---|---|
| 1 | ALL | ALL | Accept |

Authentication

Client Authentication Method default

**Step6.** Define firewall ACL rule for different kinds of access granted

1. Go to menu **Network** > **Firewall**
2. Enable firewall and choose from the zone “Wireless_Zone” that we just created and to each zone. Here we configure to zone “WAN” first.
3. Click ‘+’ to add rules.



Global Setting

☑ Enable Firewall

□ Allow Asymmetrical Route

□ Maximum session per Host (1-8192)

Firewall rule

● Through-ZyWALL rules

● Zone Pairs

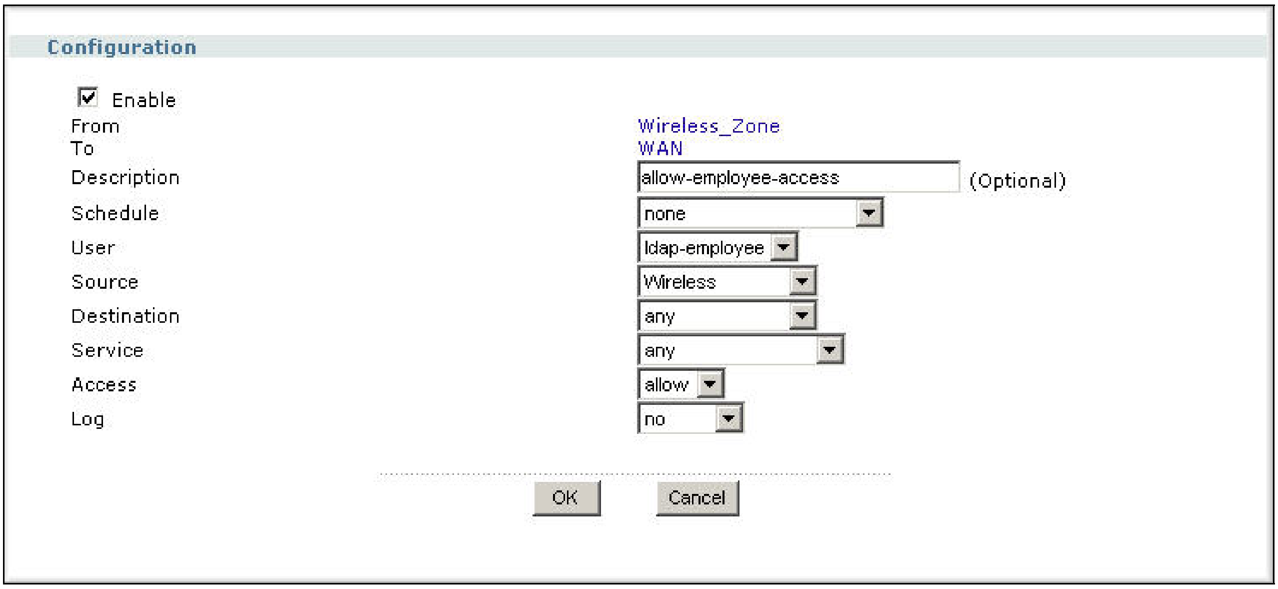
○ All rules

○ To-ZyWALL rules

| From Zone | To Zone |
|---|---|
| ○ LAN | ○ LAN |
| ○ WAN | ● WAN |
| ○ DMZ | ○ DMZ |
| ● Wireless_Zone | ○ Wireless_Zone |

WLAN-to-WAN
# Priority Schedule User Source Destination Service Access Log
Add
Apply
Reset

4. Configure a rule to allow employee access from the source “wireless network” to “any” in WAN.



Configuration

☑ Enable

| | |
|---|---|
| From | Wireless_Zone |
| To | WAN |
| Description | allow-employee-access (Optional) |
| Schedule | none |
| User | ldap-employee |
| Source | Wireless |
| Destination | any |
| Service | any |
| Access | allow |
| Log | no |

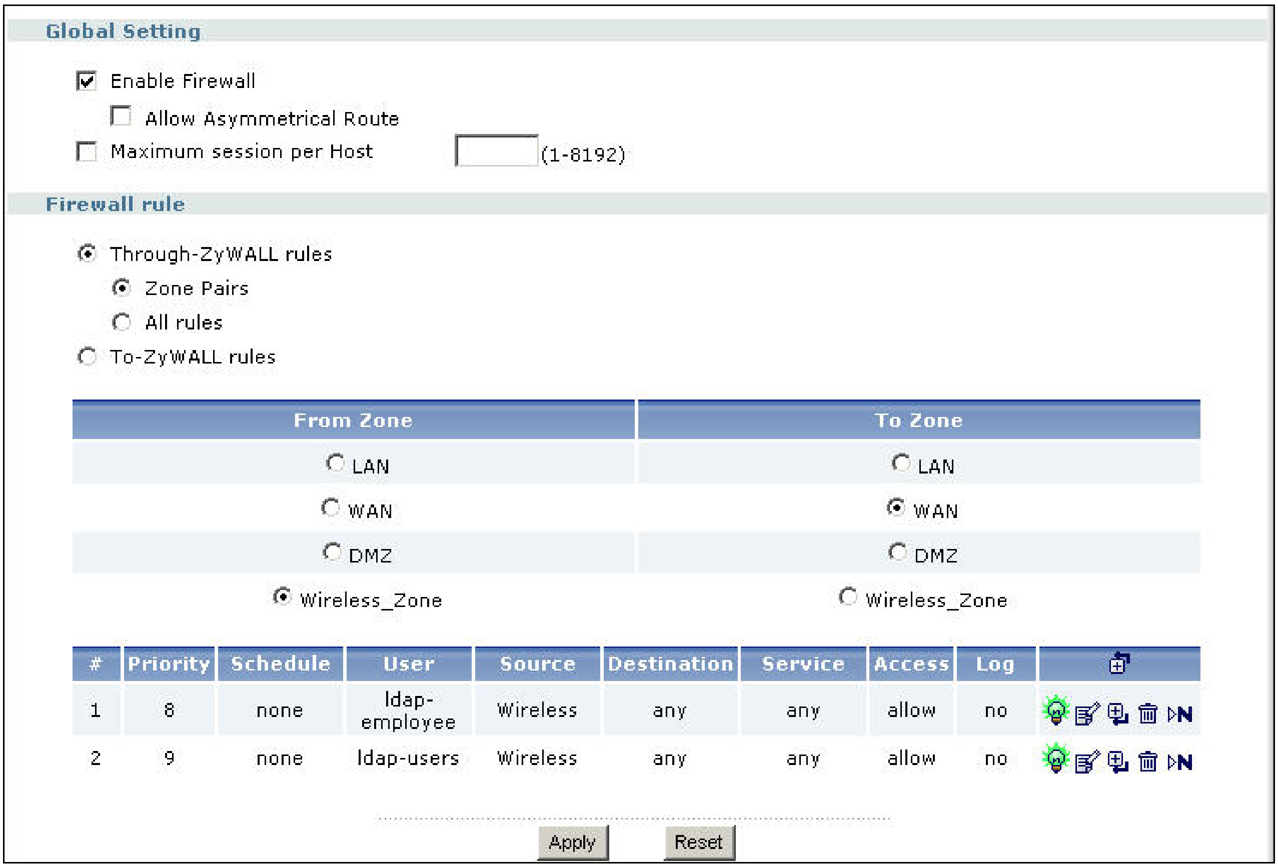
Corresponding CLI commands for your reference

```
[0] firewall 8
[1] no schedule
[2] user ldap-employee
[3] sourceip Wireless
[4] no destinationip
```

```
[5] no service
[6] action allow
[7] from Wireless_Zone
[8] to WAN
[9] no log
[10] activate
[11] description allow-employee-access
[12] exit
```

5. Configure another rule to allow a non-employee access from the source “wireless network” to “any” in WAN.

6. After this, you will see the results as on the figure below. Click Apply button.



Global Setting

☑ Enable Firewall

□ Allow Asymmetrical Route

□ Maximum session per Host [ ] (1-8192)

Firewall rule

● Through-ZyWALL rules

● Zone Pairs

○ All rules

○ To-ZyWALL rules

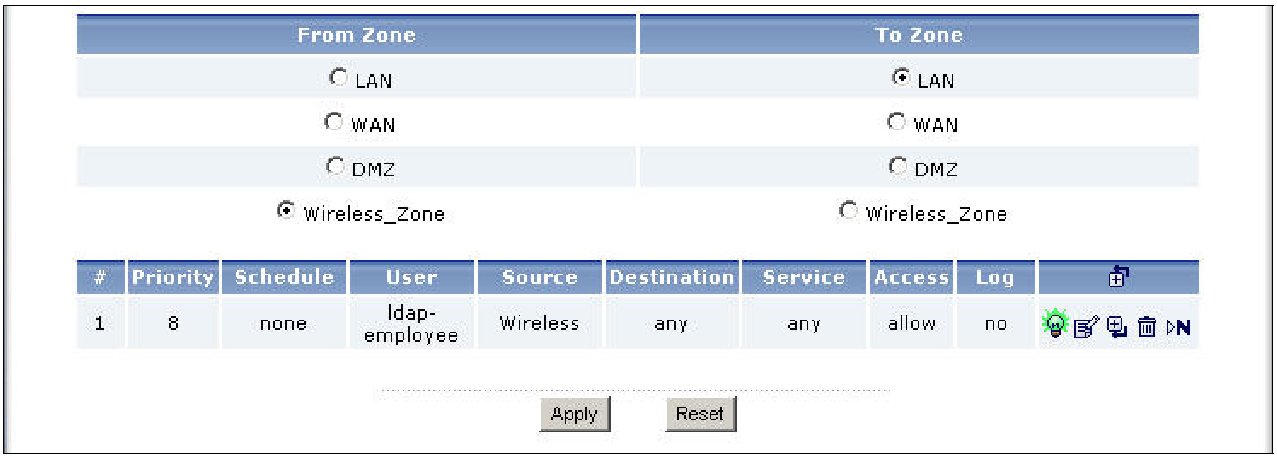
| From Zone | To Zone |
|---|---|
| ○ LAN | ○ LAN |
| ○ WAN | ● WAN |
| ○ DMZ | ○ DMZ |
| ● Wireless_Zone | ○ Wireless_Zone |

| # | Priority | Schedule | User | Source | Destination | Service | Access | Log | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 8 | none | ldap-employee | Wireless | any | any | allow | no | |
| 2 | 9 | none | ldap-users | Wireless | any | any | allow | no | |

Corresponding CLI commands for your reference

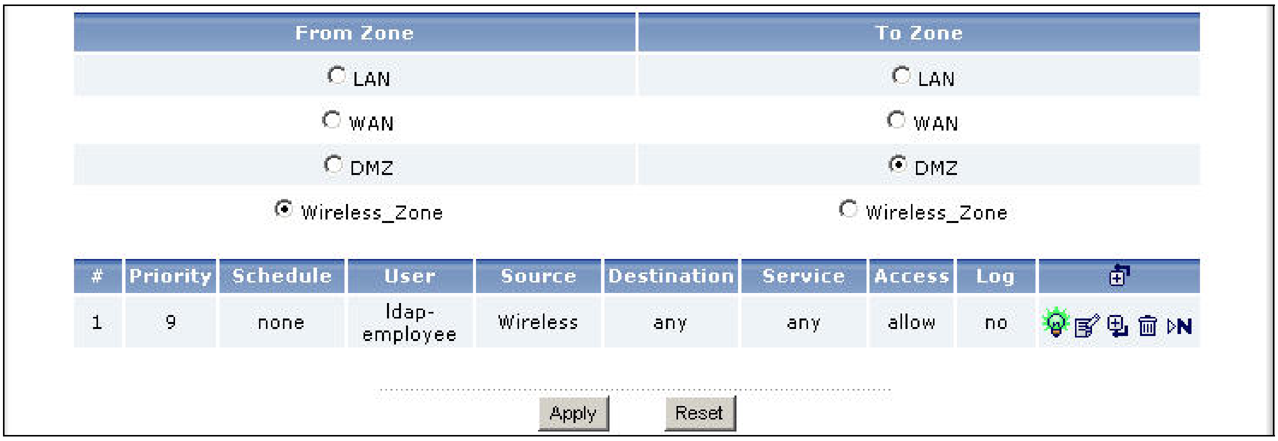
```
[0] firewall activate
[1] no firewall asymmetrical-route activate
[2] firewall 8
[3] activate
[4] exit
[5] firewall 9
[6] activate
[7] exit
```

7. Continue to configure **WLAN-to-LAN**, **WLAN-to-DMZ**, **WLAN-to-WLAN**. Those are accessible for employees only. See the following figures.



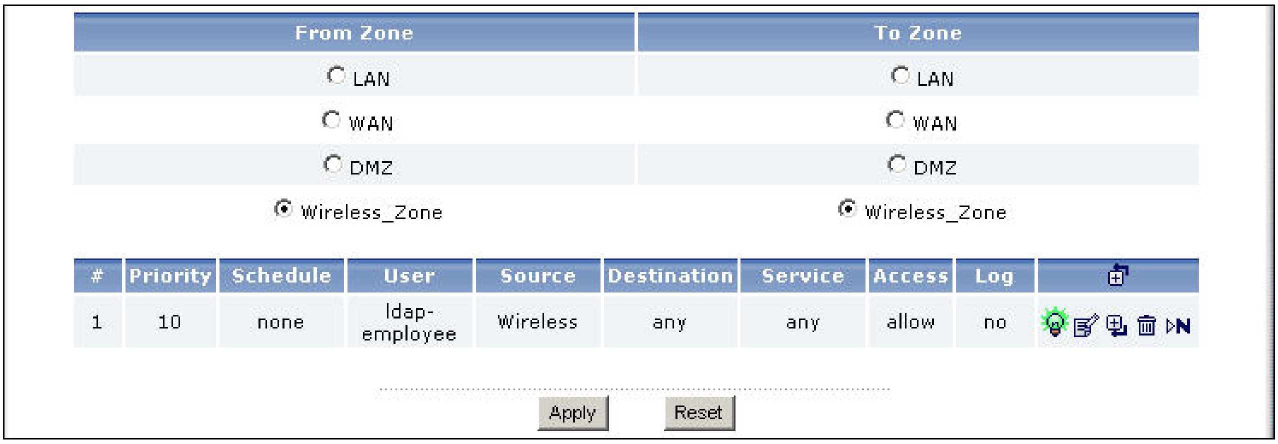
| From Zone | To Zone |
|---|---|
| ○ LAN | ● LAN |
| ○ WAN | ○ WAN |
| ○ DMZ | ○ DMZ |
| ● Wireless_Zone | ○ Wireless_Zone |

| # | Priority | Schedule | User | Source | Destination | Service | Access | Log | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 8 | none | ldap-employee | Wireless | any | any | allow | no | |



| From Zone | To Zone |
|---|---|
| ○ LAN | ○ LAN |
| ○ WAN | ○ WAN |
| ○ DMZ | ● DMZ |
| ● Wireless_Zone | ○ Wireless_Zone |

| # | Priority | Schedule | User | Source | Destination | Service | Access | Log | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 9 | none | ldap-employee | Wireless | any | any | allow | no | |



| From Zone | To Zone |
|---|---|
| ○ LAN | ○ LAN |
| ○ WAN | ○ WAN |
| ○ DMZ | ○ DMZ |
| ● Wireless_Zone | ● Wireless_Zone |

| # | Priority | Schedule | User | Source | Destination | Service | Access | Log | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 10 | none | ldap-employee | Wireless | any | any | allow | no | |

# 2.3 Employee Internet Management (EIM)

## 2.3.1 Benefits of deploying Employee Internet Management

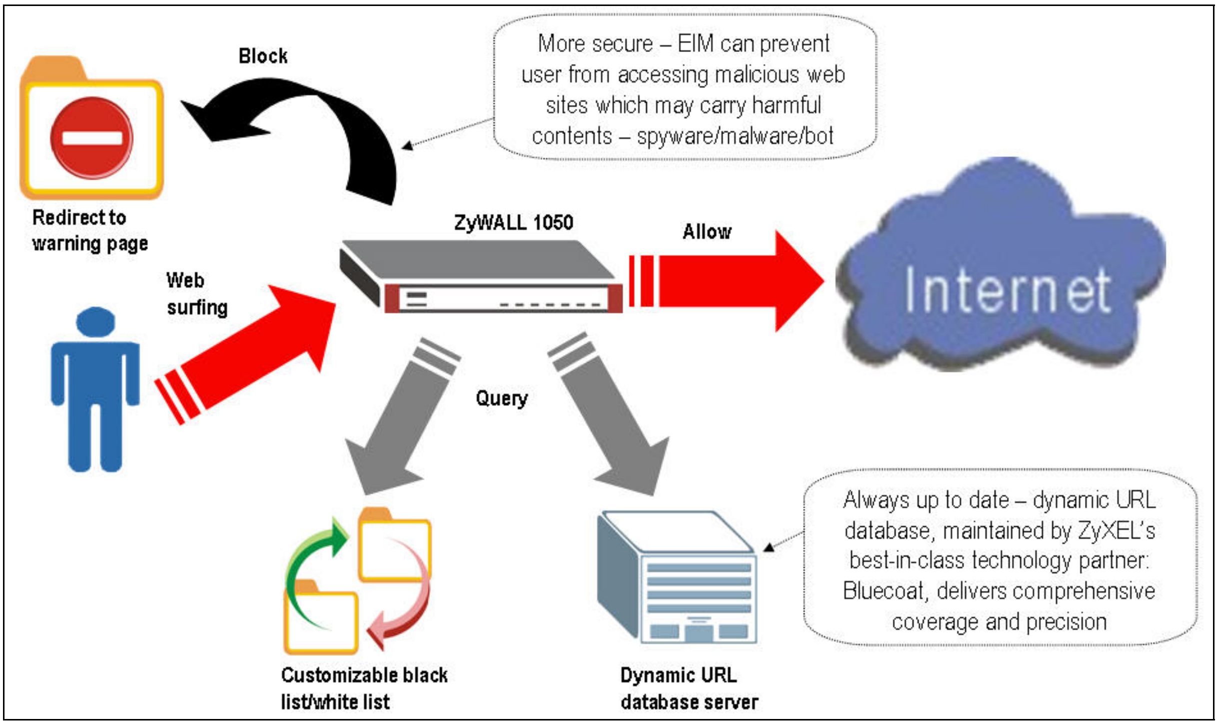
Employer always cares about how to increase company's overall productivity. Some activities like employees' surfing the Internet, downloading files occupying a lot of bandwidth, talking to friends that are not related to the actual job during working hours would decrease the productivity. Through good management of employee behavior, this can be achieved:

- Increased productivity
- Reduced misuse of corporate resources in terms of bandwidth
- Regulatory compliance – get rid of porn/violent web contents that may bring legal issues

## 2.3.2 EIM on ZyWALL 1050

ZyWALL 1050 supports EIM through the following features.

- Flexible access policy: provides the Enforce Access policy with granularity
- Always up to date: query dynamically updated URL database
- Customizable: Keyword blocking/Black list/White list
- In-depth Inspection: can control access of Java/ActiveX/Cookie/embedded proxy links



More secure – EIM can prevent user from accessing malicious web sites which may carry harmful contents – spyware/malware/bot

Always up to date – dynamic URL database, maintained by ZyXEL's best-in-class technology partner: Bluecoat, delivers comprehensive coverage and precision

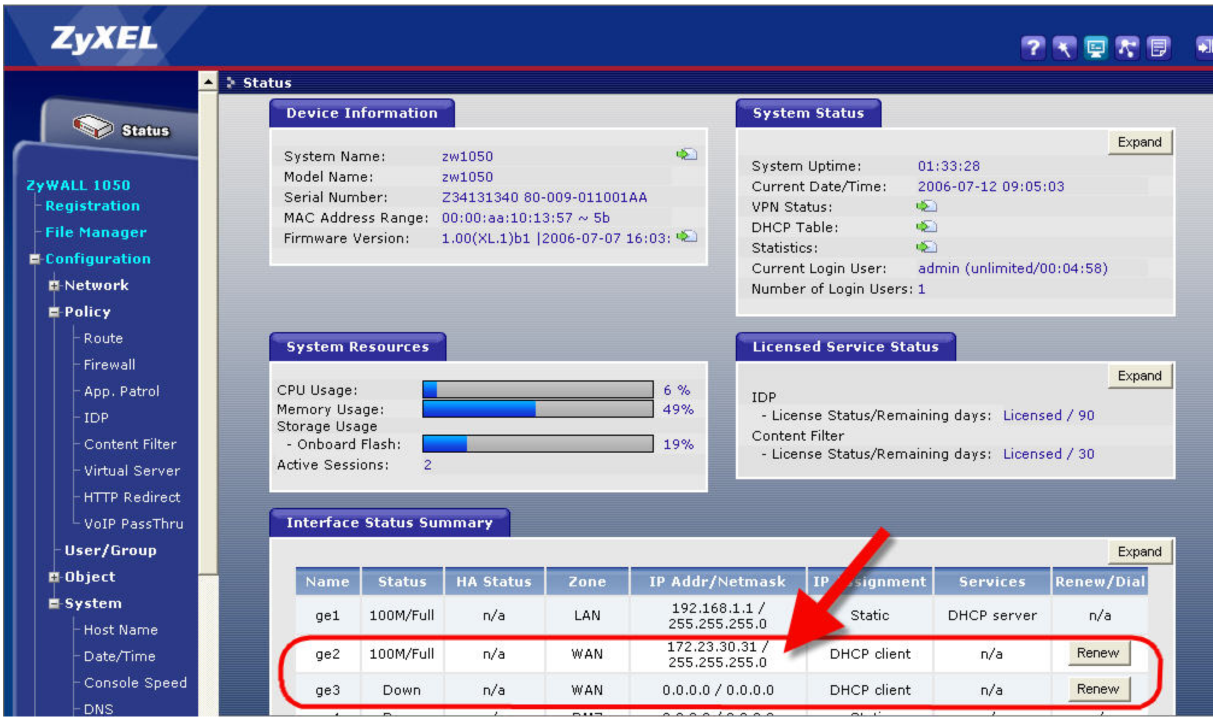
So we are going to complete the following settings.

1. Verify that the Internet access of ZyWALL 1050 is ok
2. Complete user/product/service registrations to activate the Content Filter service
3. Create Address objects for different user groups
4. Enable and configure the Content Filter feature on ZyWALL 1050
   (1) Create two different filtering profiles for Sales and for Engineer departments
   - Enable external dynamic server
   - Configure Black and White lists
   - Control access of Java/ActiveX/Cookie/embedded proxy links
   - Define filtering profiles for different user group
   - Configure the warning message or warning page redirected when user access the forbidden website

Configure ZyWALL 1050 step by step as described below.

**Step1.** Make sure the Internet access has been configured well from PC behind ZyWALL 1050.

By default, ge2 and ge3 of ZyWALL 1050's WAN ports will get the IP address from the ISP or the DHCP server in front of ZyWALL 1050. Connect an Ethernet cable to ZyWALL 1050's ge2 or ge3 and on the GUI Home page check whether ZyWALL 1050 gets the IP address.



**Device Information**

System Name: zw1050
Model Name: zw1050
Serial Number: Z34131340 80-009-011001AA
MAC Address Range: 00:00:aa:10:13:57 ~ 5b
Firmware Version: 1.00(XL.1)b1 |2006-07-07 16:03:

**System Status**

System Uptime: 01:33:28
Current Date/Time: 2006-07-12 09:05:03
VPN Status:
DHCP Table:
Statistics:
Current Login User: admin (unlimited/00:04:58)
Number of Login Users: 1

**System Resources**

CPU Usage: 6 %
Memory Usage: 49%
Storage Usage
- Onboard Flash: 19%
Active Sessions: 2

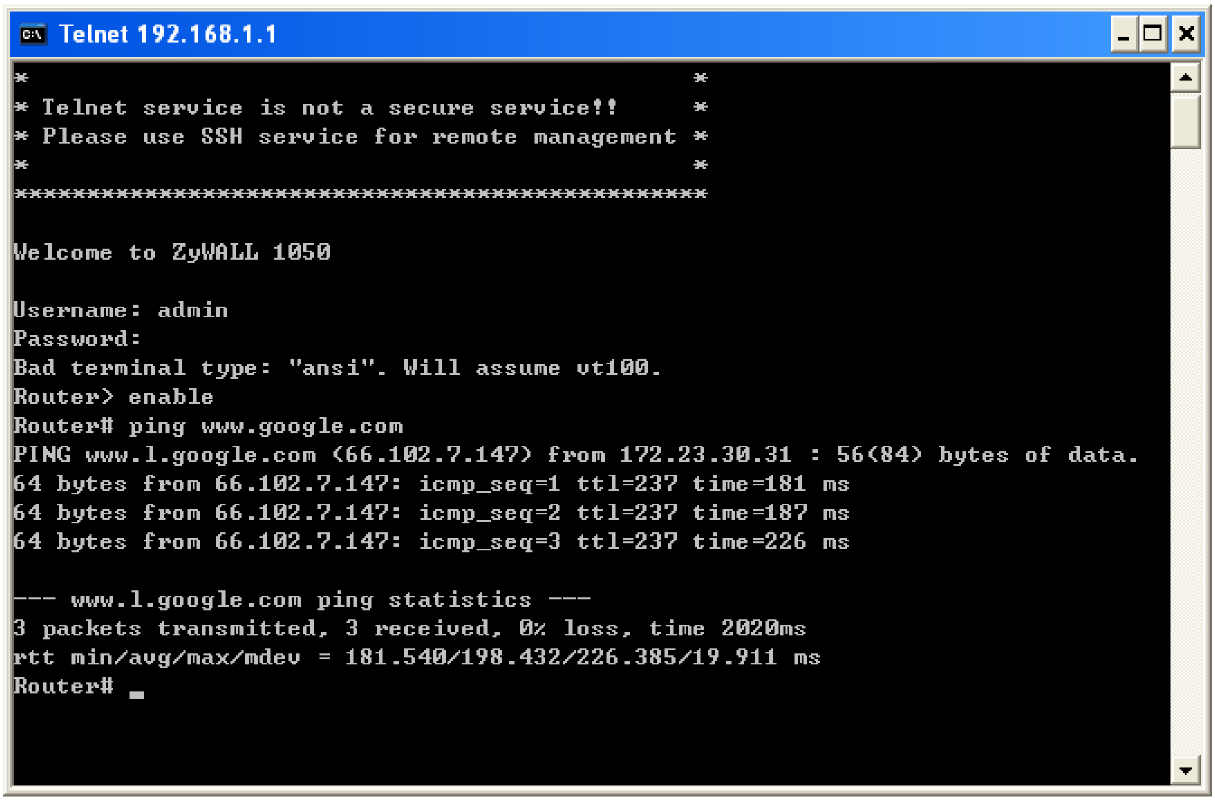
**Licensed Service Status**

IDP
- License Status/Remaining days: Licensed / 90
Content Filter
- License Status/Remaining days: Licensed / 30

**Interface Status Summary**

| Name | Status | HA Status | Zone | IP Addr/Netmask | IP Assignment | Services | Renew/Dial |
|---|---|---|---|---|---|---|---|
| ge1 | 100M/Full | n/a | LAN | 192.168.1.1 / 255.255.255.0 | Static | DHCP server | n/a |
| ge2 | 100M/Full | n/a | WAN | 172.23.30.31 / 255.255.255.0 | DHCP client | n/a | Renew |
| ge3 | Down | n/a | WAN | 0.0.0.0 / 0.0.0.0 | DHCP client | n/a | Renew |

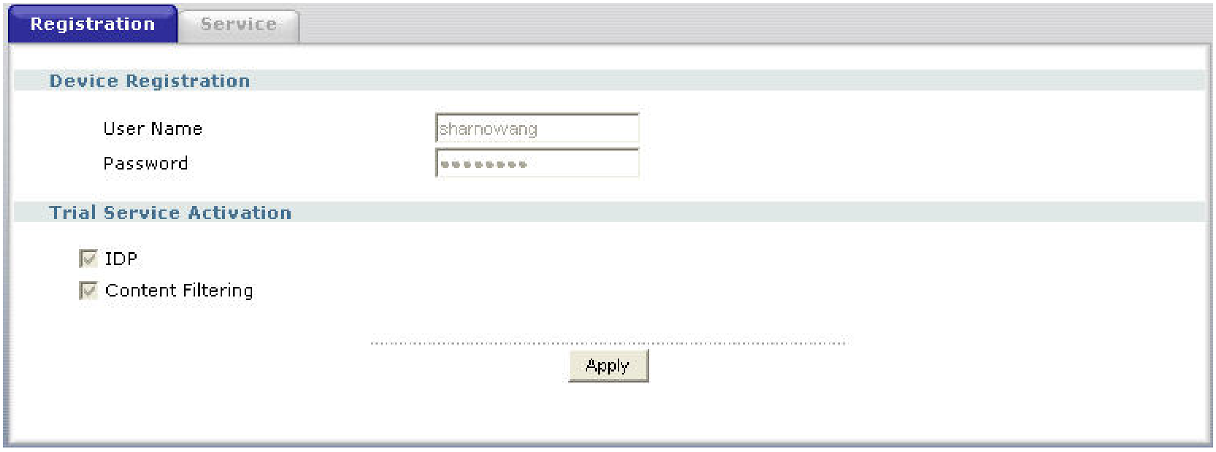
Make sure ZyWALL 1050 can access the Internet using CLI commands via console or telnet. See the example shown below.



```
*                                               *
* Telnet service is not a secure service!!      *
* Please use SSH service for remote management *
*                                               *
************************************************

Welcome to ZyWALL 1050

Username: admin
Password:
Bad terminal type: "ansi". Will assume vt100.
Router> enable
Router# ping www.google.com
PING www.l.google.com (66.102.7.147) from 172.23.30.31 : 56(84) bytes of data.
64 bytes from 66.102.7.147: icmp_seq=1 ttl=237 time=181 ms
64 bytes from 66.102.7.147: icmp_seq=2 ttl=237 time=187 ms
64 bytes from 66.102.7.147: icmp_seq=3 ttl=237 time=226 ms

--- www.l.google.com ping statistics ---
3 packets transmitted, 3 received, 0% loss, time 2020ms
rtt min/avg/max/mdev = 181.540/198.432/226.385/19.911 ms
Router# _
```

**Step2.** Login the ZyWALL 1050's GUI, Go to menu **Registration.** Complete the user, product, and Content Filter service registration on myZyXEL.com.

Here the Content Filter service enabling by activating the trial period is shown. If you are new to myZyXEL.com registration, choose 'Create a new user'. Choose 'Existing user' to enter the username and the password. Check the 'Content Filtering' service activation. Click the **Apply** button to complete the registration process.



Device Registration

User Name sharnowang

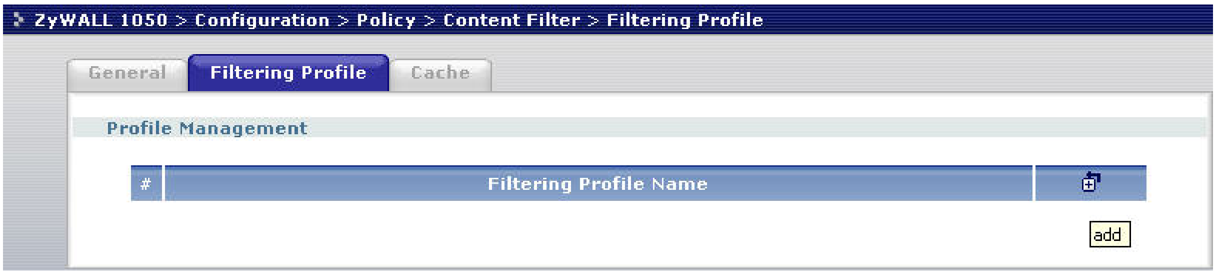
Password ••••••••

Trial Service Activation

☑ IDP

☑ Content Filtering

**Step3.** Switch to menu **Configuration** > **Policy** > **Content Filter** > **Filtering Profile** tab, click the '+' icon to add a new filtering profile.

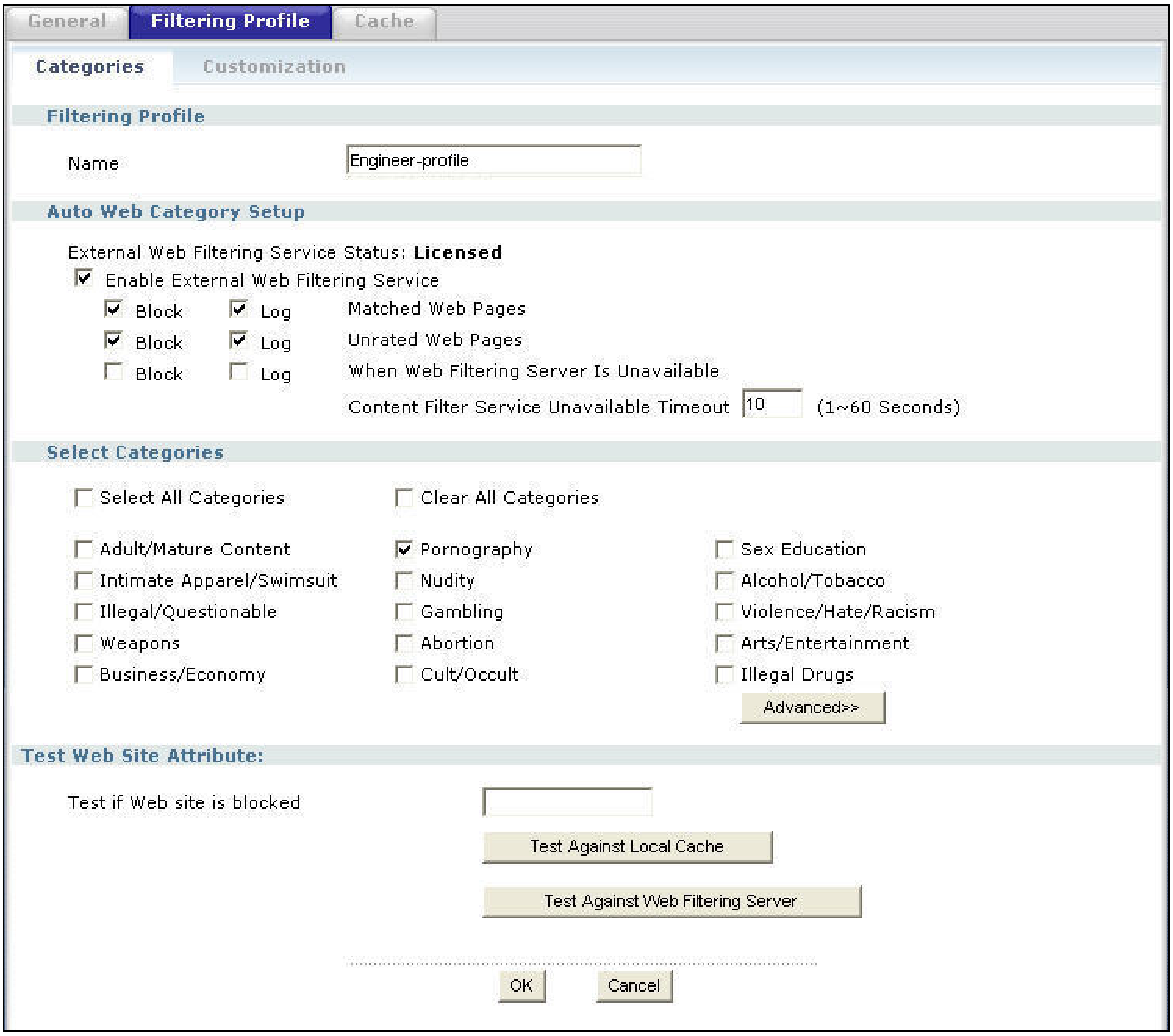


ZyWALL 1050 > Configuration > Policy > Content Filter > Filtering Profile

Profile Management

| # | Filtering Profile Name | |
|---|---|---|

Under the **Categories** tab, enter the profile name and enable the external web filtering service. Define all matched and unrated web pages that should be blocked and logged. Here, we choose to apply the block action to **Pornography** category. Click the **OK** button.



Filtering Profile

Name: Engineer-profile

Auto Web Category Setup

External Web Filtering Service Status: **Licensed**

☑ Enable External Web Filtering Service

☑ Block ☑ Log Matched Web Pages

☑ Block ☑ Log Unrated Web Pages

□ Block □ Log When Web Filtering Server Is Unavailable

Content Filter Service Unavailable Timeout 10 (1~60 Seconds)

Select Categories

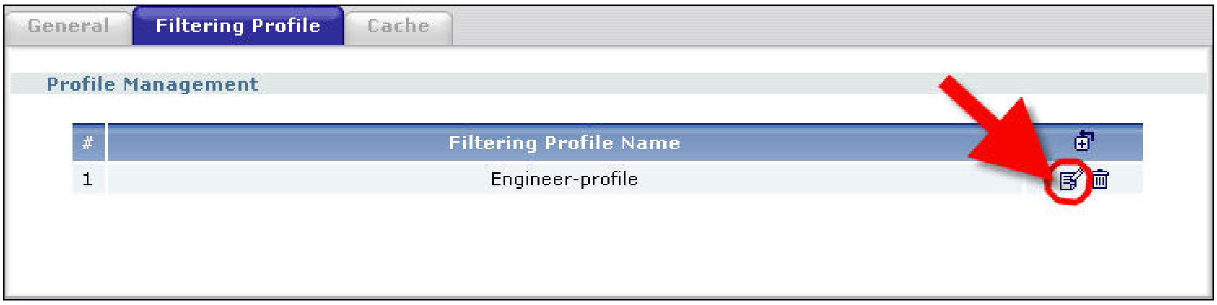
□ Select All Categories □ Clear All Categories

| | | |
|---|---|---|
| □ Adult/Mature Content | ☑ Pornography | □ Sex Education |
| □ Intimate Apparel/Swimsuit | □ Nudity | □ Alcohol/Tobacco |
| □ Illegal/Questionable | □ Gambling | □ Violence/Hate/Racism |
| □ Weapons | □ Abortion | □ Arts/Entertainment |
| □ Business/Economy | □ Cult/Occult | □ Illegal Drugs |

Test Web Site Attribute:

Test if Web site is blocked

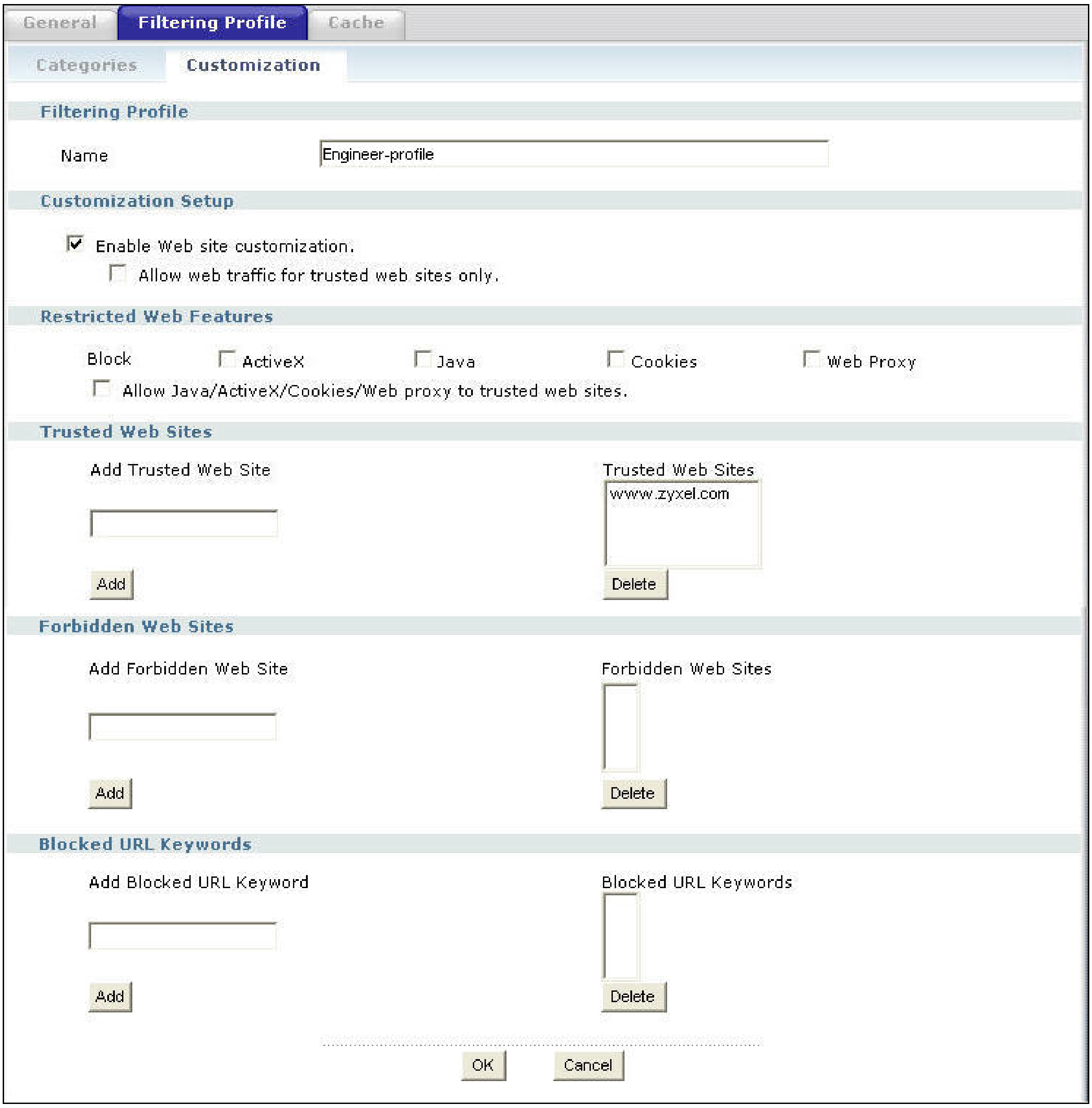
Click the modify icon to configure the trusted website list.



Profile Management

| # | Filtering Profile Name |
|---|---|
| 1 | Engineer-profile |

Switch to **Customization** tab, enable the web site customization. Add the website, www.zyxel.com for example, to the trusted websites. Click **OK** button.



**Filtering Profile**

Name: Engineer-profile

**Customization Setup**

☑ Enable Web site customization.

□ Allow web traffic for trusted web sites only.

**Restricted Web Features**

Block □ ActiveX □ Java □ Cookies □ Web Proxy

□ Allow Java/ActiveX/Cookies/Web proxy to trusted web sites.

**Trusted Web Sites**

Add Trusted Web Site

Trusted Web Sites: www.zyxel.com

**Forbidden Web Sites**

Add Forbidden Web Site

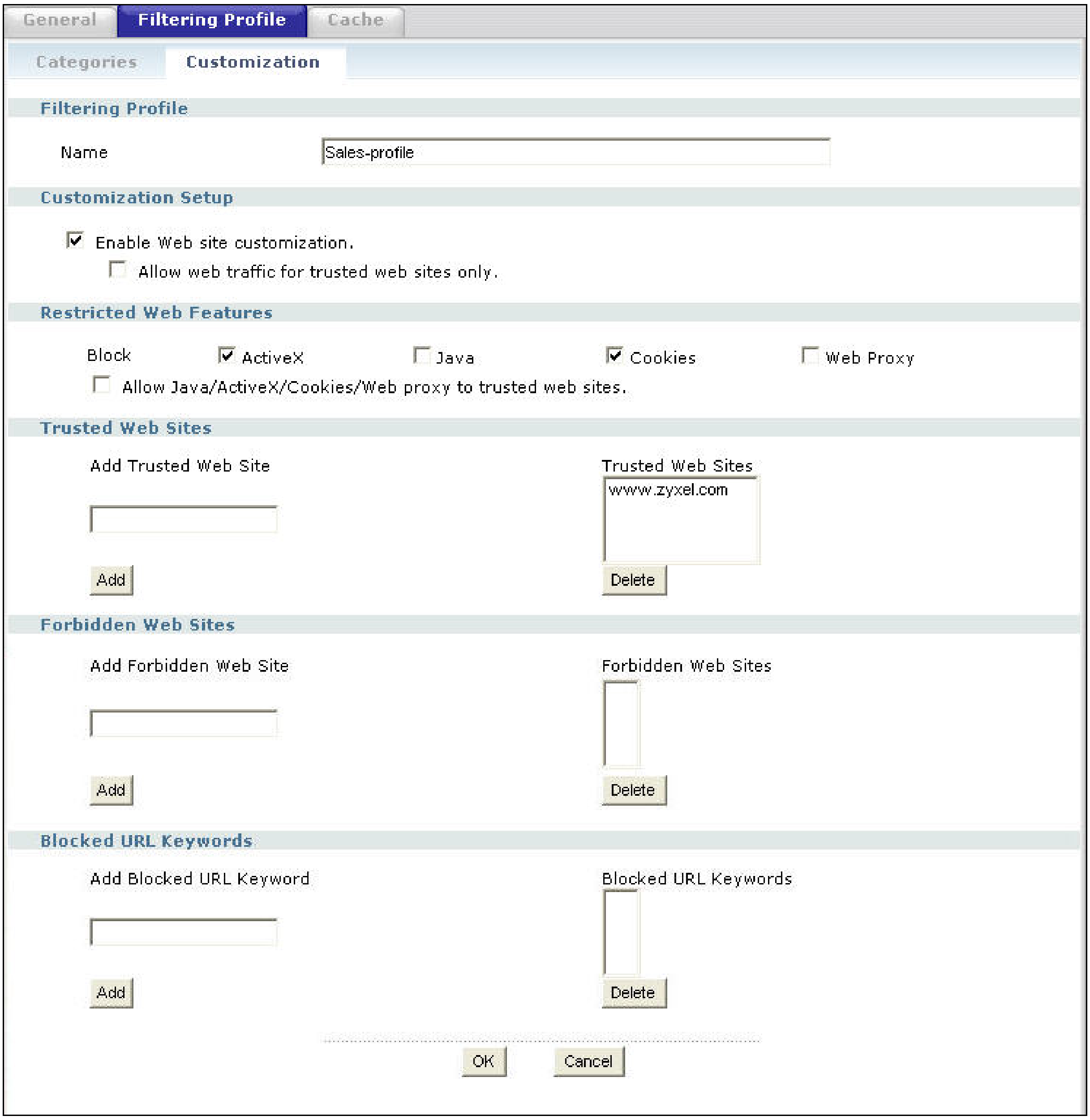
Forbidden Web Sites

**Blocked URL Keywords**

Add Blocked URL Keyword

Blocked URL Keywords

Then follow the similar configuration to create another filtering profile for Sales department. For example, we add an extra access restriction to the websites with ActiveX and Cookies features as configured on the figure below. Click **OK** button.



Filtering Profile

Name: Sales-profile

Customization Setup

☑ Enable Web site customization.

□ Allow web traffic for trusted web sites only.

Restricted Web Features

Block ☑ ActiveX □ Java ☑ Cookies □ Web Proxy

□ Allow Java/ActiveX/Cookies/Web proxy to trusted web sites.

Trusted Web Sites

Add Trusted Web Site

Trusted Web Sites: www.zyxel.com

Forbidden Web Sites

Add Forbidden Web Site

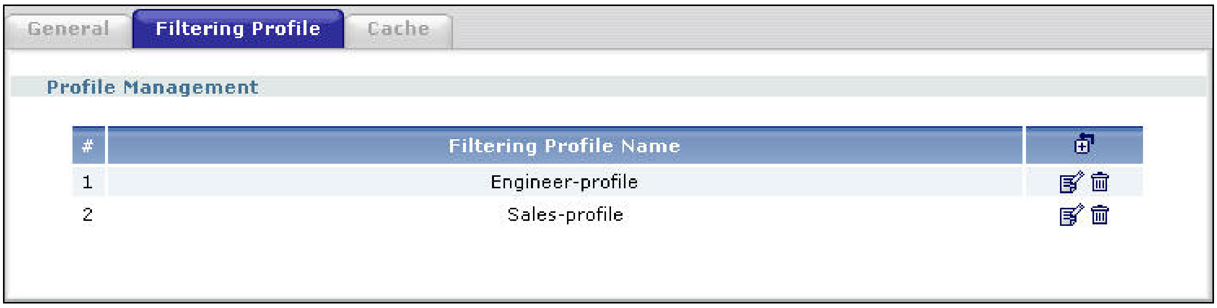
Forbidden Web Sites

Blocked URL Keywords

Add Blocked URL Keyword

Blocked URL Keywords

After it’s done, you will see two profiles as shown below.



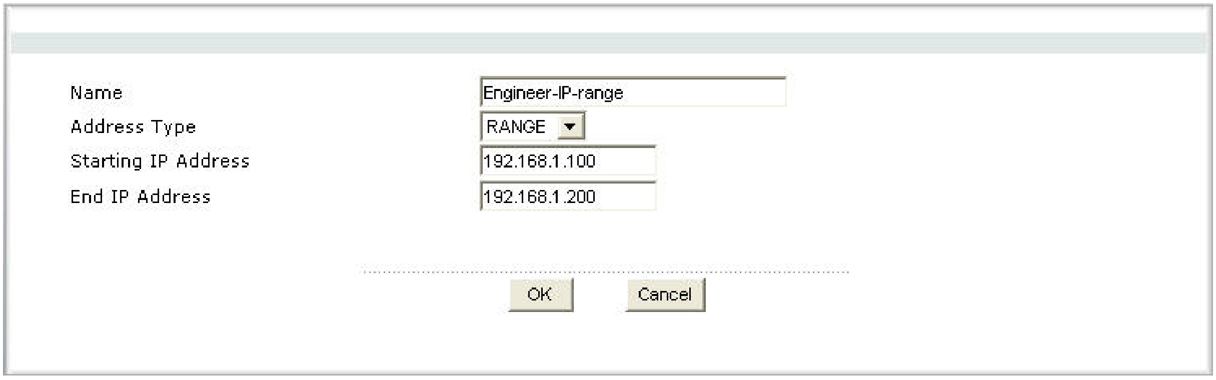
Profile Management

| # | Filtering Profile Name |
|---|---|
| 1 | Engineer-profile |
| 2 | Sales-profile |

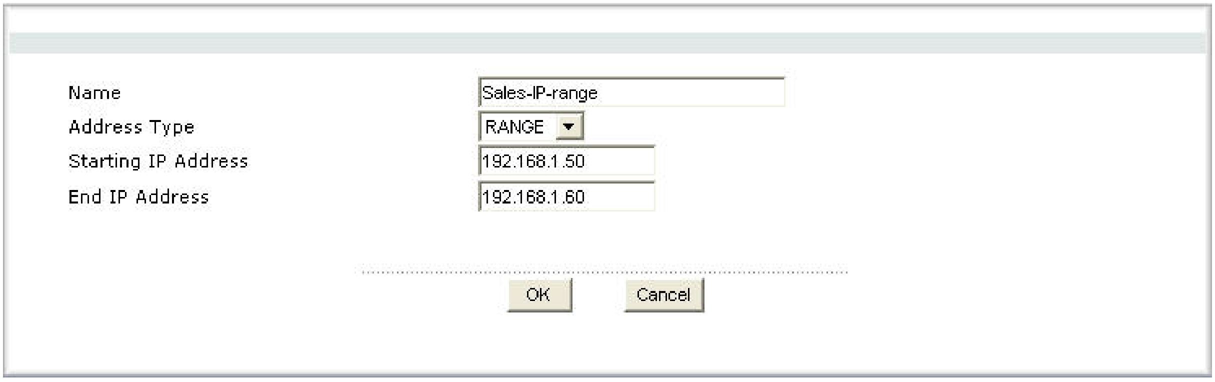
CLI commands for reference:

```
[0] content-filter profile Engineer-profile
[1] content-filter profile Engineer-profile url url-server
[2] content-filter profile Engineer-profile url match block
[3] content-filter profile Engineer-profile url match log
[4] content-filter profile Engineer-profile url unrate block
[5] content-filter profile Engineer-profile url unrate log
[6] content-filter service-timeout 10
[7] content-filter profile Engineer-profile url category 1
[8] content-filter profile Engineer-profile custom
[9] content-filter profile Engineer-profile custom trust
www.zyxel.com
[10] content-filter profile Sales-profile custom
[11] content-filter profile Sales-profile custom activex
[12] content-filter profile Sales-profile custom cookie
[13] content-filter profile Sales-profile custom trust
www.zyxel.com
```

**Step4**. Switch to menu **Configuration** > **Object** > **Address**, create two Address Objects to define the IP address range for the Engineer and the Sales department.



| | |
|---|---|
| Name | Engineer-IP-range |
| Address Type | RANGE |
| Starting IP Address | 192.168.1.100 |
| End IP Address | 192.168.1.200 |

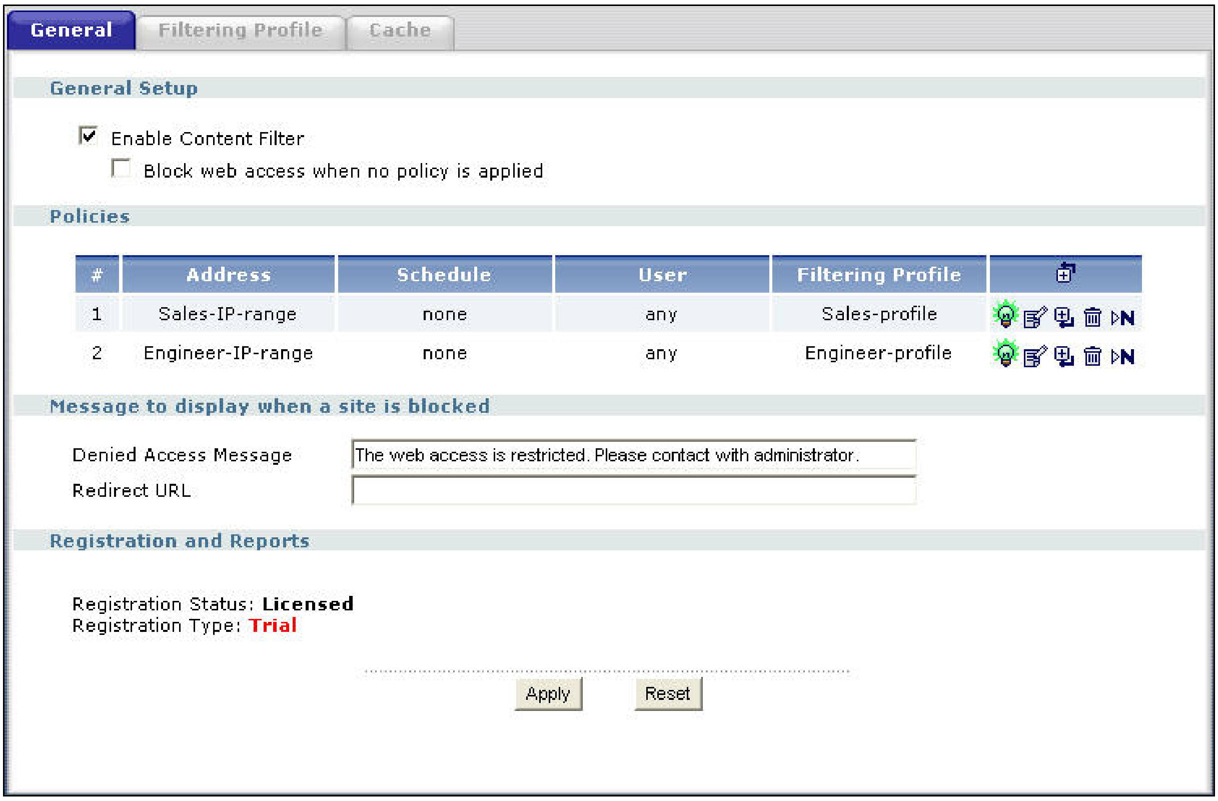


| | |
|---|---|
| Name | Sales-IP-range |
| Address Type | RANGE |
| Starting IP Address | 192.168.1.50 |
| End IP Address | 192.168.1.60 |

CLI commands for reference:

```
[0] address-object Engineer-IP-range 192.168.1.100-192.168.1.200
[0] address-object Sales-IP-range 192.168.1.50-192.168.1.60
```

**Step5**. Switch to **Content Filter** > **General** tab, enable the Content Filter. Add two filtering profiles as shown below.



General Setup

☑ Enable Content Filter

□ Block web access when no policy is applied

Policies

| # | Address | Schedule | User | Filtering Profile |
|---|---|---|---|---|
| 1 | Sales-IP-range | none | any | Sales-profile |
| 2 | Engineer-IP-range | none | any | Engineer-profile |

Message to display when a site is blocked

Denied Access Message: The web access is restricted. Please contact with administrator.

Redirect URL:

Registration and Reports

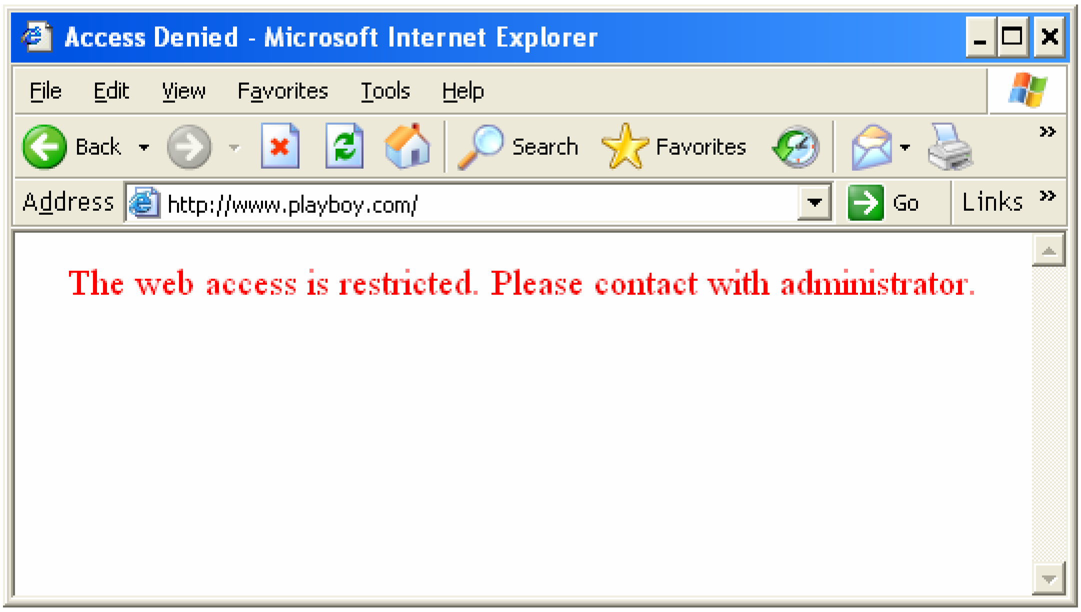
Registration Status: **Licensed**
Registration Type: **Trial**

CLI commands for reference:

```
[0] content-filter block message The web access is restricted.
Please contact with administrator.
[1] content-filter policy insert 1 none any Engineer-IP-range
Engineer-profile
[2] content-filter policy insert 1 none any Sales-IP-range
Sales-profile
[3] content-filter activate
```

Then when Engineers try to surf Interface behind ZyWALL 1050, the HTTP requests will be inspected by the Engineer filter profile whereas Sales' Internet access will be inspected by the Sales filter profile.

For example, if an engineer with PC's IP address 192.168.1.101 is trying to access http://www.playboy.com, it will return the warning message on the browser.


Access Denied - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.playboy.com/ Go Links

The web access is restricted. Please contact with administrator.

On the other hand, a Sales department employee with PC IP address 192.168.1.57 accesses the same website, he is allowed the browsing without any warning message returned.

# 3. Seamless Incorporation

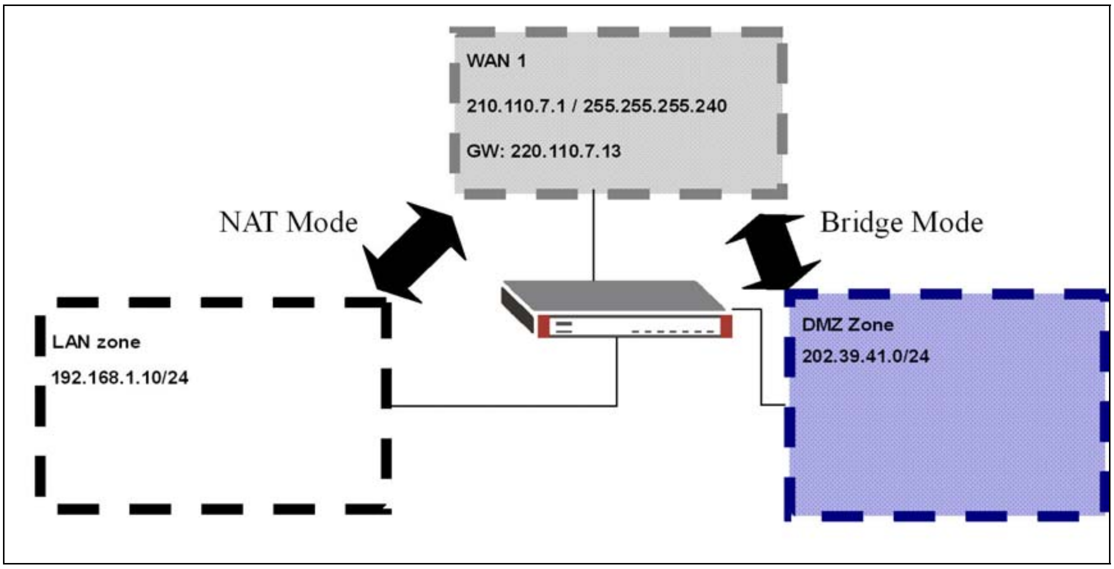
With its robust networking functionalities, ZyWALL 1050 is easy to integrate into existing network infrastructure. You can easily implement the following applications. They are “Transparent firewall”, “Transparent IDP” and “Network Partitioning using VLAN”.

## 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 1050 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 1050 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

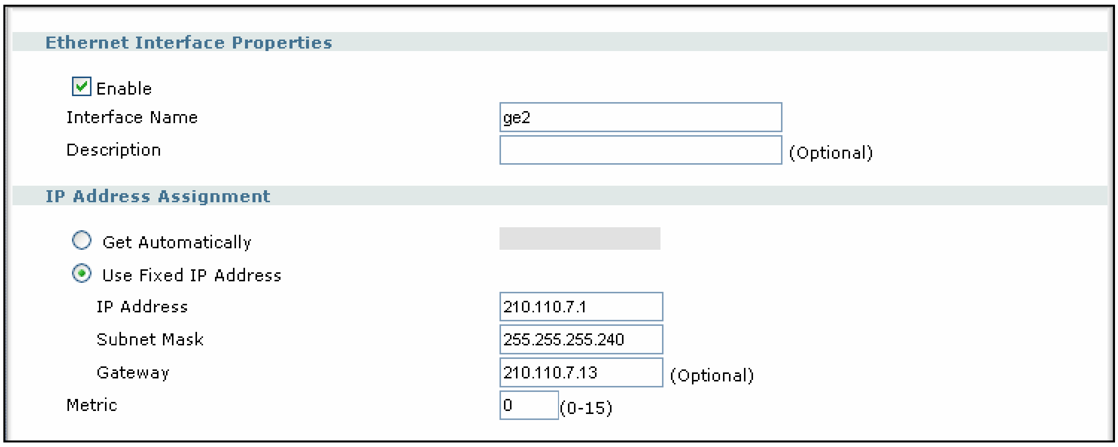
Here is an example:



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. IP addressing in LAN zone is private IP segments. Thus, we need NAT, which is the router mode here. In our example, ge1 acts as LAN, ge2 and ge3 stands for WAN, ge4 and ge5 stands for DMZ.

To make this scenario works the follow the configuration steps as stated below:

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



Ethernet Interface Properties

☑ Enable

Interface Name: ge2

Description: (Optional)

IP Address Assignment

○ Get Automatically

● Use Fixed IP Address

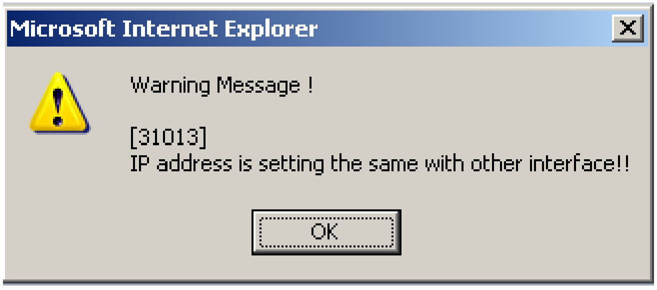
IP Address: 210.110.7.1

Subnet Mask: 255.255.255.240

Gateway: 210.110.7.13 (Optional)

Metric: 0 (0-15)

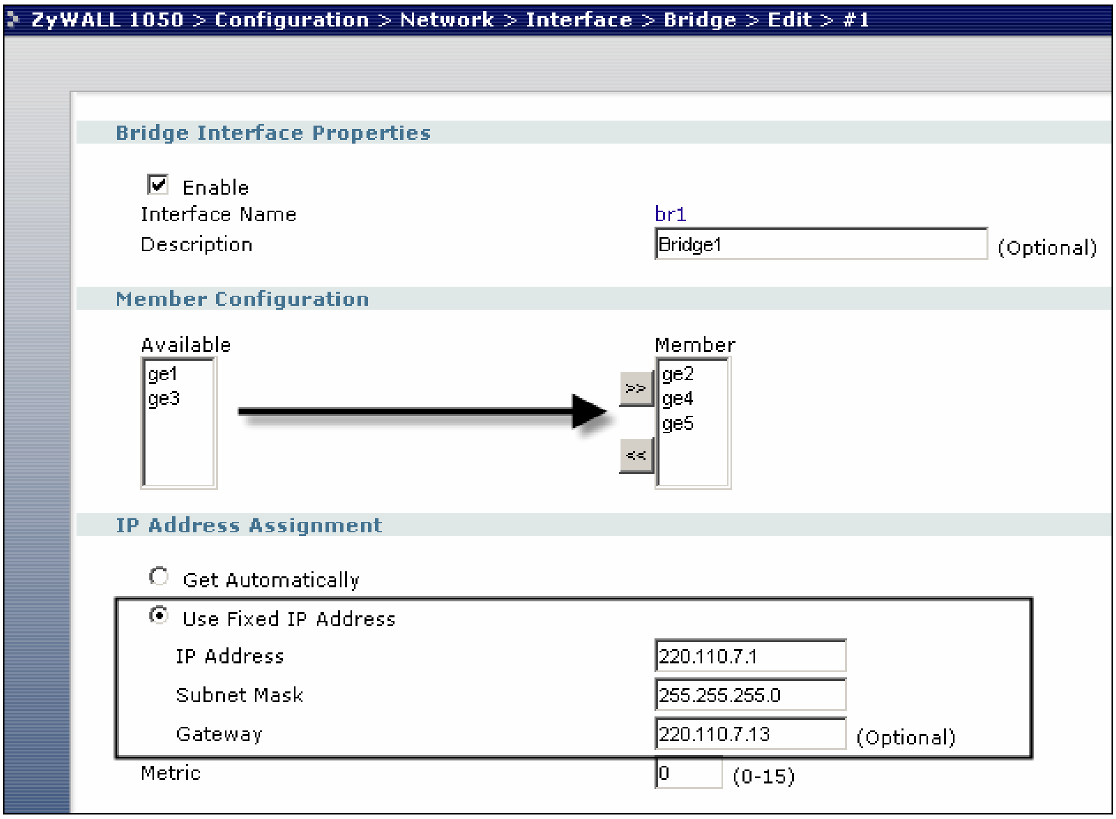
2) Switch to **Configuration** > **Network** > **Interface** > **Bridge**, add a new Bridge Interface. First we enable this interface and give it a name, place the available ports into the member ports and make them become the member of this bridge interface. Moreover, don’t forget to set the WAN IP 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.



Warning Message !

[31013]
IP address is setting the same with other interface!!

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



ZyWALL 1050 > Configuration > Network > Interface > Bridge > Edit > #1

Bridge Interface Properties

☑ Enable

Interface Name: br1

Description: Bridge1 (Optional)

Member Configuration

Available: ge1, ge3

Member: ge2, ge4, ge5

IP Address Assignment

○ Get Automatically

● Use Fixed IP Address

IP Address: 220.110.7.1

Subnet Mask: 255.255.255.0

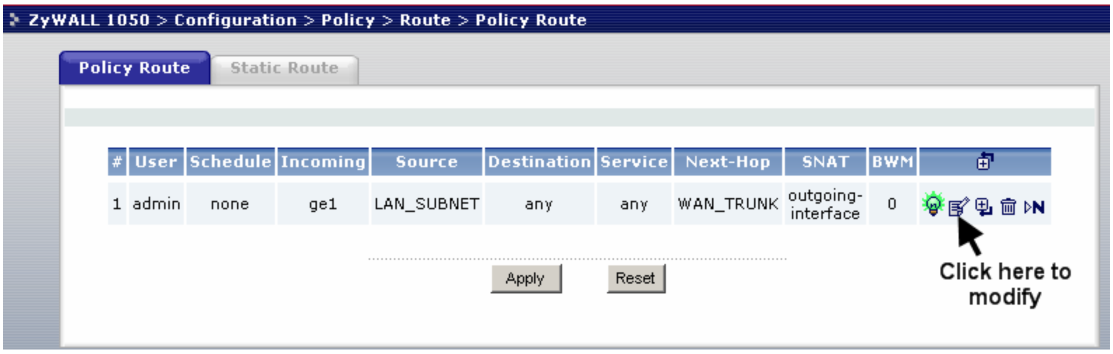
Gateway: 220.110.7.13 (Optional)

Metric: 0 (0-15)

**CLI to create this bridge interface:**

```
[0] interface br1
[1] no join ge2
[2] no join ge4
[3] no join ge5
[4] join ge2
[5] join ge4
[6] join ge5
[7] ip address 220.110.7.1 255.255.255.0
[8] ip gateway 220.110.7.13 metric 0
[9] exit
```

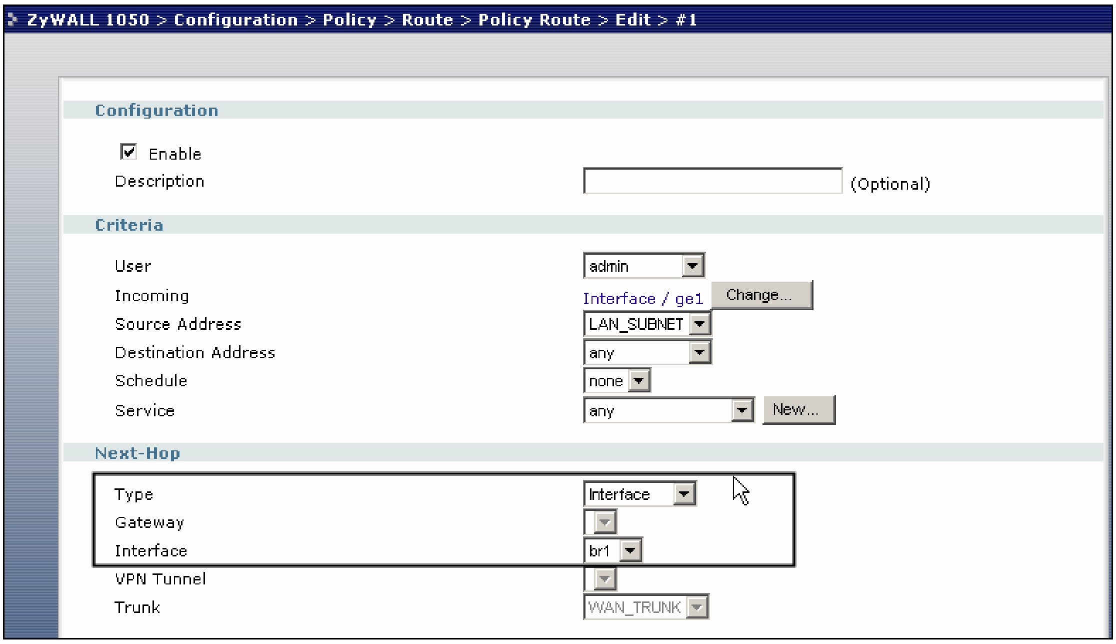
3) Switch to **Configuration** > **Policy > Route** > **Policy Route**, to modify the default rule there. The default rule is for the Router Mode (NAT Mode). Since we have two different modes co-existing here, we need to make some adjustments to this rule.



ZyWALL 1050 > Configuration > Policy > Route > Policy Route

| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM |  |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | admin | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 0 |  |

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



ZyWALL 1050 > Configuration > Policy > Route > Policy Route > Edit > #1

Configuration

☑ Enable

Description ____ (Optional)

Criteria

User admin
Incoming: Interface / ge1
Source Address: LAN_SUBNET
Destination Address: any
Schedule: none
Service: any

Next-Hop

Type: Interface
Gateway:
Interface: br1
VPN Tunnel:
Trunk: WAN_TRUNK

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

**The CLI to create this rule:**

```
[0] policy 1
[1] no deactivate
[2] no description
[3] user admin
[4] interface ge1
[5] source LAN_SUBNET
[6] destination any
[7] no schedule
[8] service any
[9] next-hop interface br1
[10] snat outgoing-interface
[11] no bandwidth
```

```
[12] exit
```

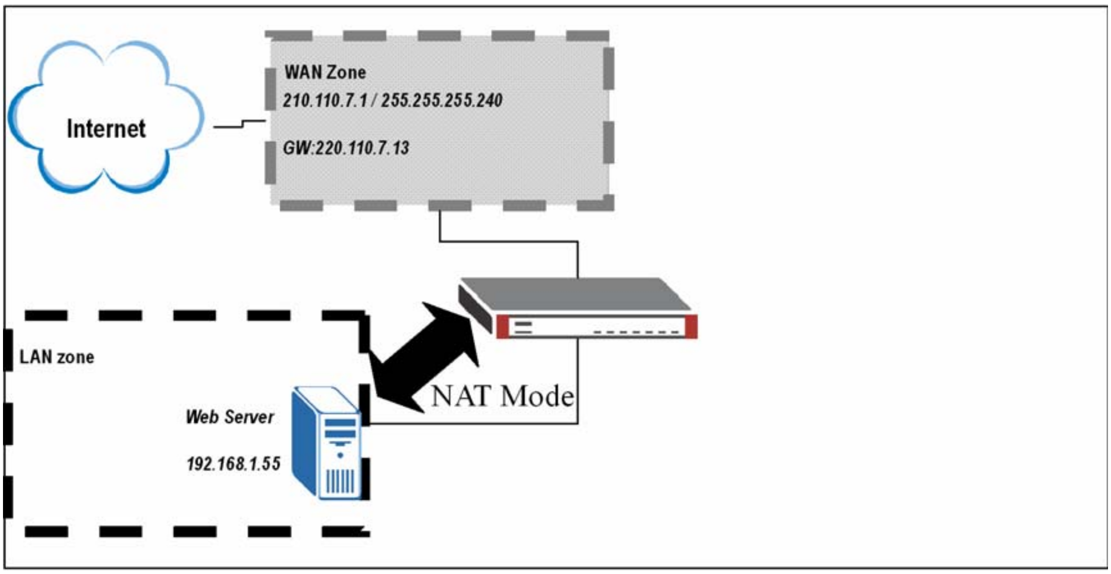
**Tips for application:**

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

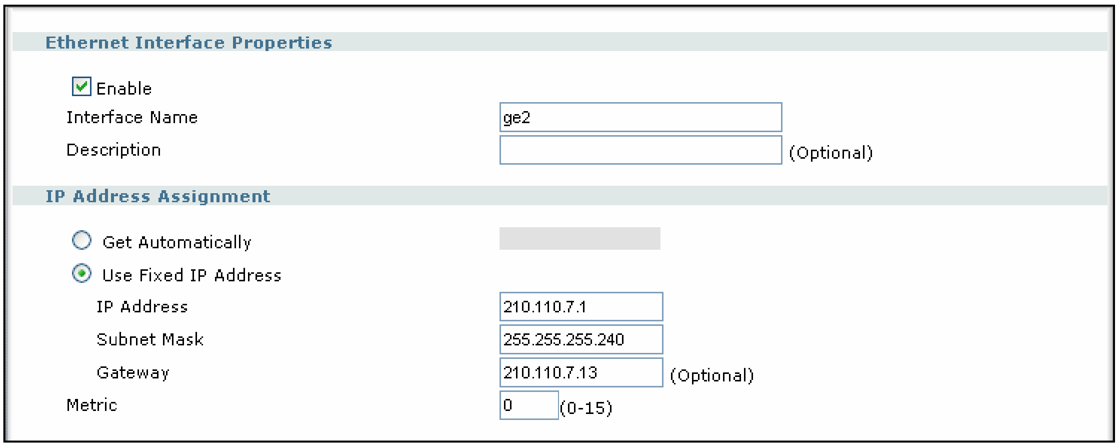
Here is an example:



There is a web server located in the DMZ zone. The virtual Server setting in ZyWALL1050 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 1050 GUI and setup the ge2 interface for internet connection and manually assign a static IP. Login ZyWALL 1050 GUI and go to **Configuration** > **Network** > **Interface** > **Edit** > **ge2**



Ethernet Interface Properties

☑ Enable

| | |
|---|---|
| Interface Name | ge2 |
| Description | (Optional) |

IP Address Assignment

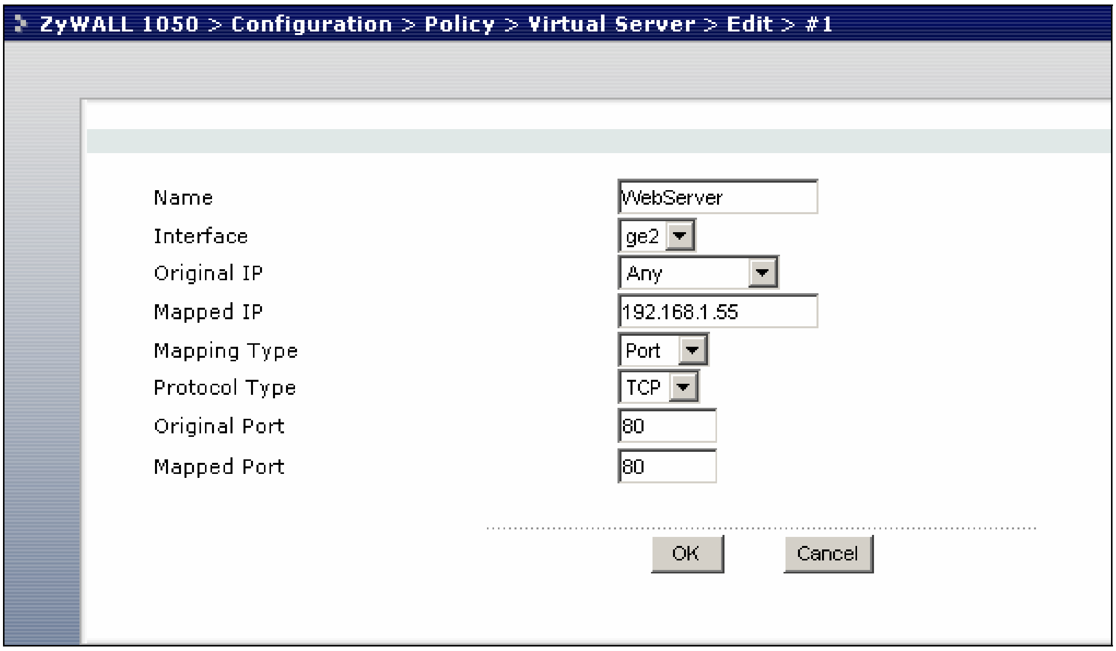
○ Get Automatically

● 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 **Configuration** > **Policy** > **Virtual Server** and add a new Virtual Server. Fill in the mapping information. In our example here, since ge2 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.

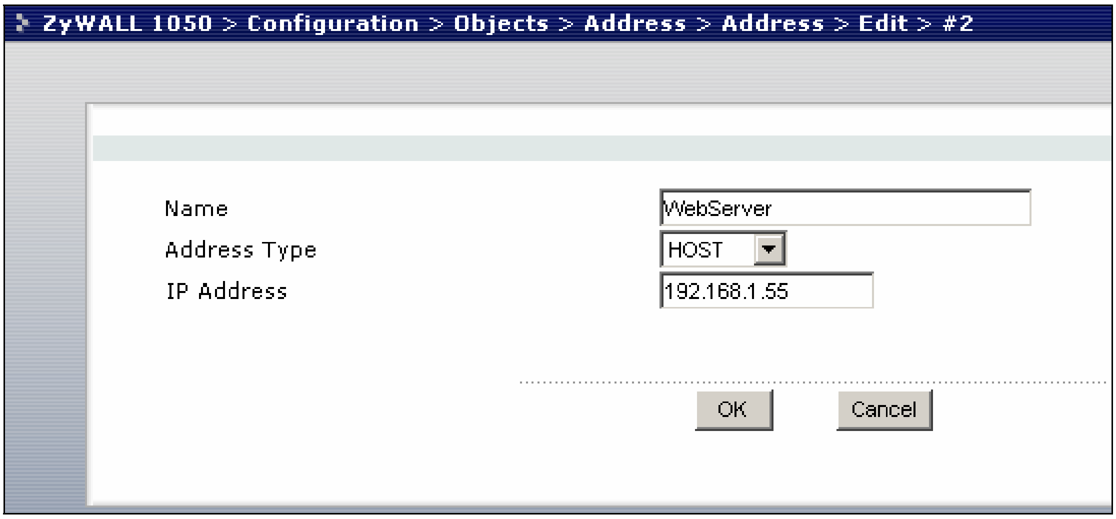

ZyWALL 1050 > Configuration > Policy > Virtual Server > Edit > #1

| | |
|---|---|
| Name | WebServer |
| Interface | ge2 |
| Original IP | Any |
| Mapped IP | 192.168.1.55 |
| Mapping Type | Port |
| Protocol Type | TCP |
| Original Port | 80 |
| Mapped Port | 80 |

**CLI to create a Virtual Server Mapping**

```
[0] ip virtual-server WebServer interface ge2 original-ip any
map-to 192.168.1.55 map-type port protocol tcp original-port 80
mapped-port 80
```

3)Switch to **Configuration** > **Objects** > **Address**, and add a new address object for your Web server.

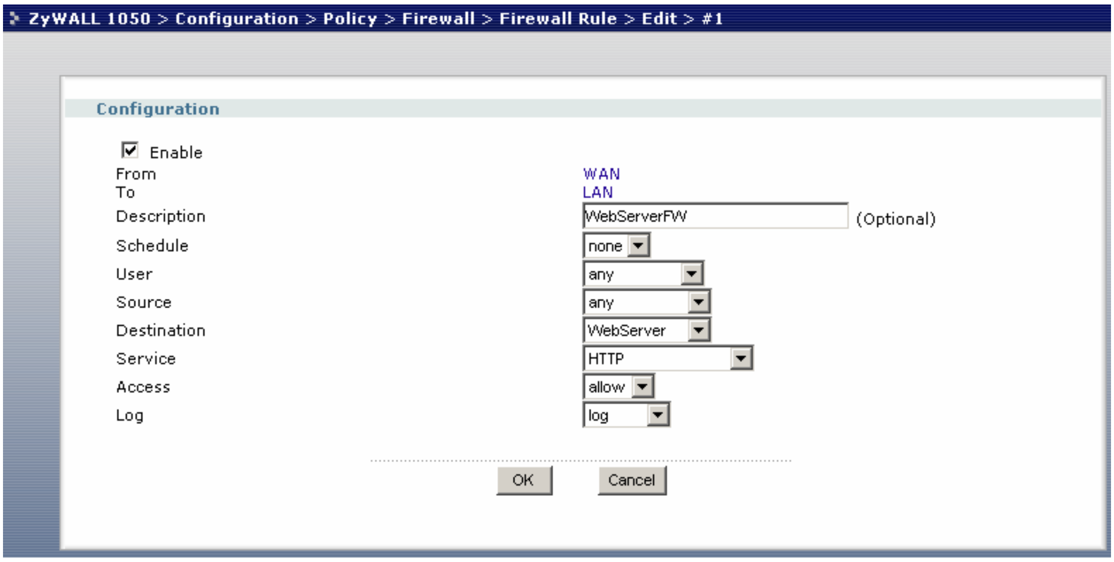

ZyWALL 1050 > Configuration > Objects > Address > Address > Edit > #2

| | |
|---|---|
| Name | WebServer |
| Address Type | HOST |
| IP Address | 192.168.1.55 |

**CLI to create an address object**

```
[0] address-object WebServer 192.168.1.55
```

4) Switch to **Configuration** > **Policy** > **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.


ZyWALL 1050 > Configuration > Policy > Firewall > Firewall Rule > Edit > #1
Configuration
OK
Cancel

☑ Enable

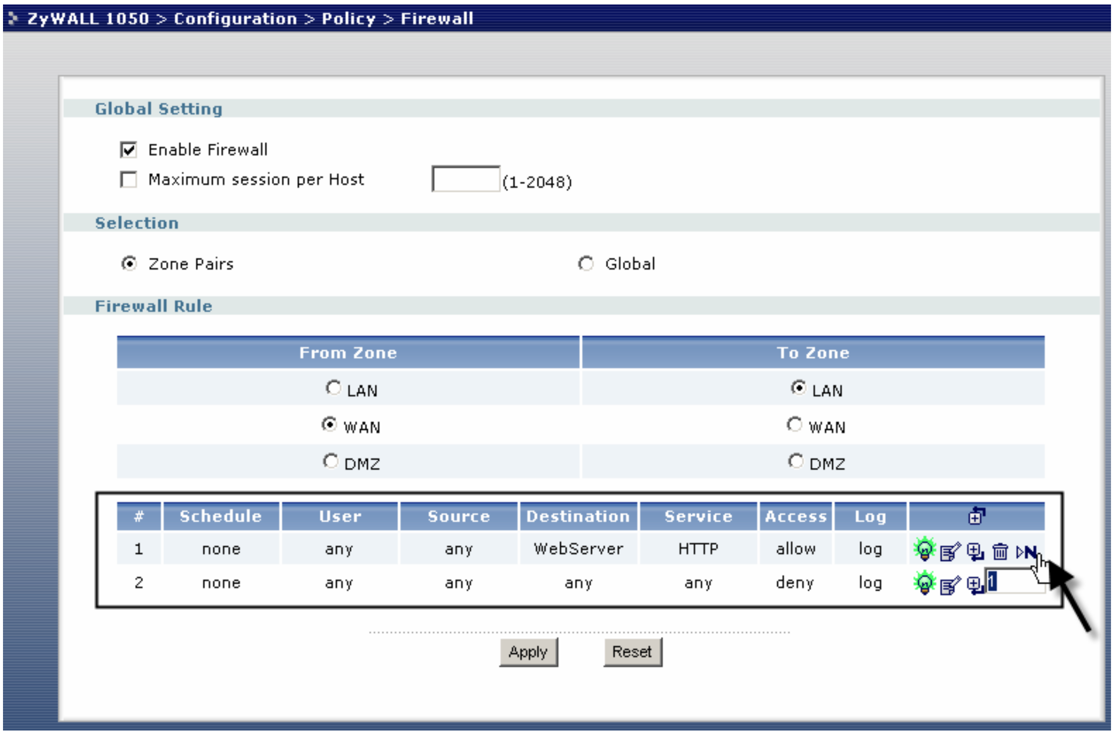
|   |   |
|---|---|
| From | WAN |
| To | LAN |
| Description | WebServerFW (Optional) |
| Schedule | none |
| User | any |
| Source | any |
| Destination | WebServer |
| Service | HTTP |
| Access | allow |
| Log | log |

**CLI to create a firewall rule**

```
[0] firewall 6
[1] no schedule
[2] no user
[3] no sourceip
[4] destinationip WebServer
[5] service HTTP
[6] action allow
[7] from WAN
[8] to LAN
[9] log
[10] activate
[11] description WebServerFW
[12] exit
```

**Tips for application:**

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



ZyWALL 1050 > Configuration > Policy > Firewall

**Global Setting**

☑ Enable Firewall

□ Maximum session per Host (1-2048)

**Selection**

● Zone Pairs ○ Global

**Firewall Rule**

| From Zone | To Zone |
|---|---|
| ○ LAN | ● LAN |
| ● WAN | ○ WAN |
| ○ DMZ | ○ DMZ |

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

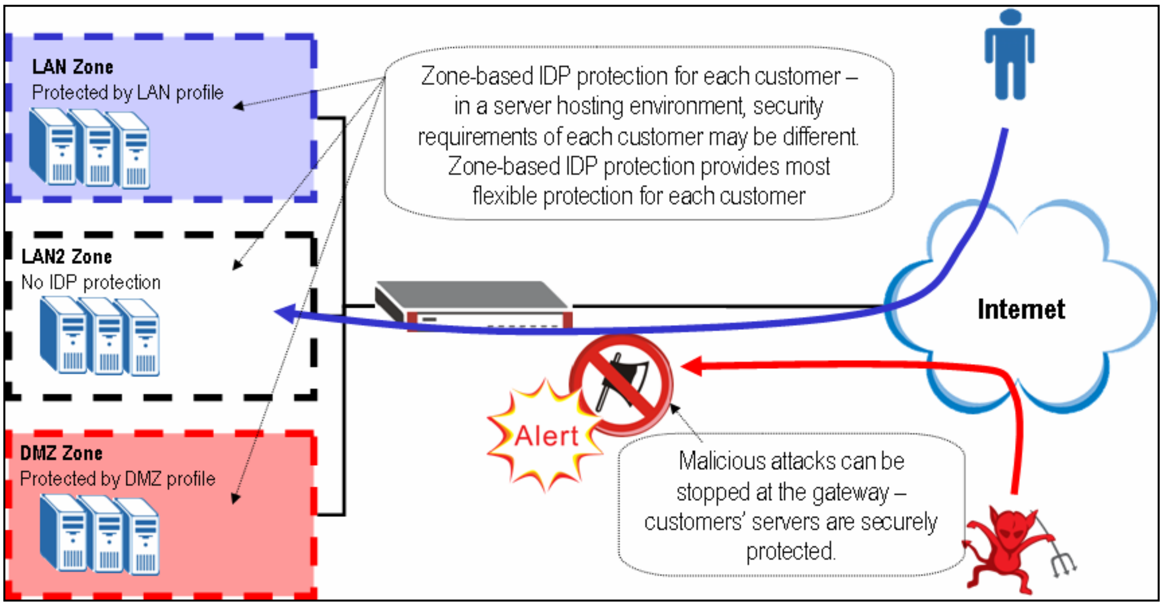
## 3.2 Zone-based IDP Protection

ZyWALL 1050 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 1050 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 1050 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 1050 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 1050

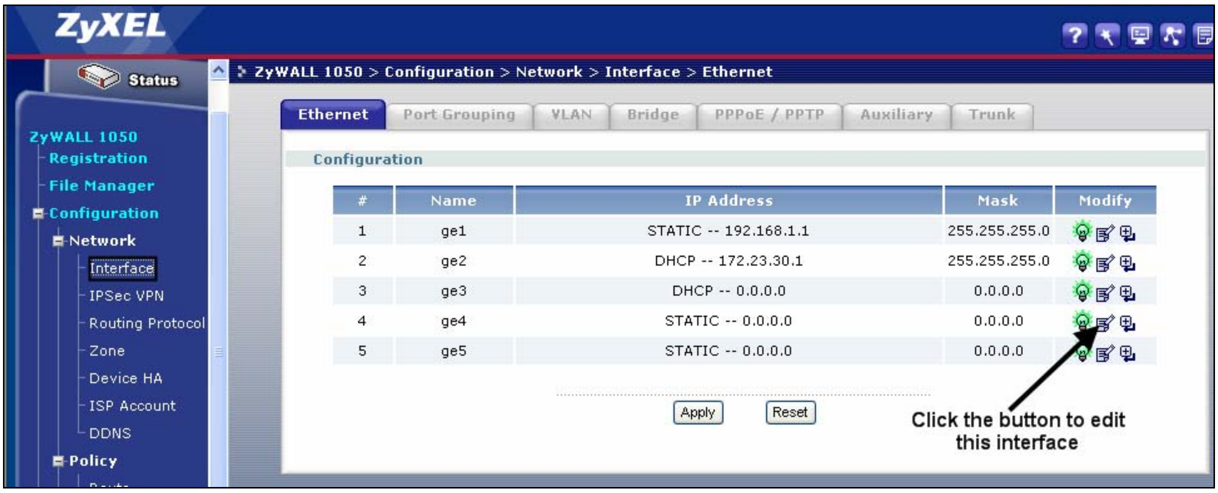
Here is an example:


LAN Zone
Protected by LAN profile
LAN2 Zone
No IDP protection
DMZ Zone
Protected by DMZ profile
Zone-based IDP protection for each customer – in a server hosting environment, security requirements of each customer may be different. Zone-based IDP protection provides most flexible protection for each customer
Internet
Alert
Malicious attacks can be stopped at the gateway – customers' servers are securely protected.

To fulfill the above scenario, you will need three networks on GE1, GE4 and GE5. Then you can apply different IDP profiles to them.

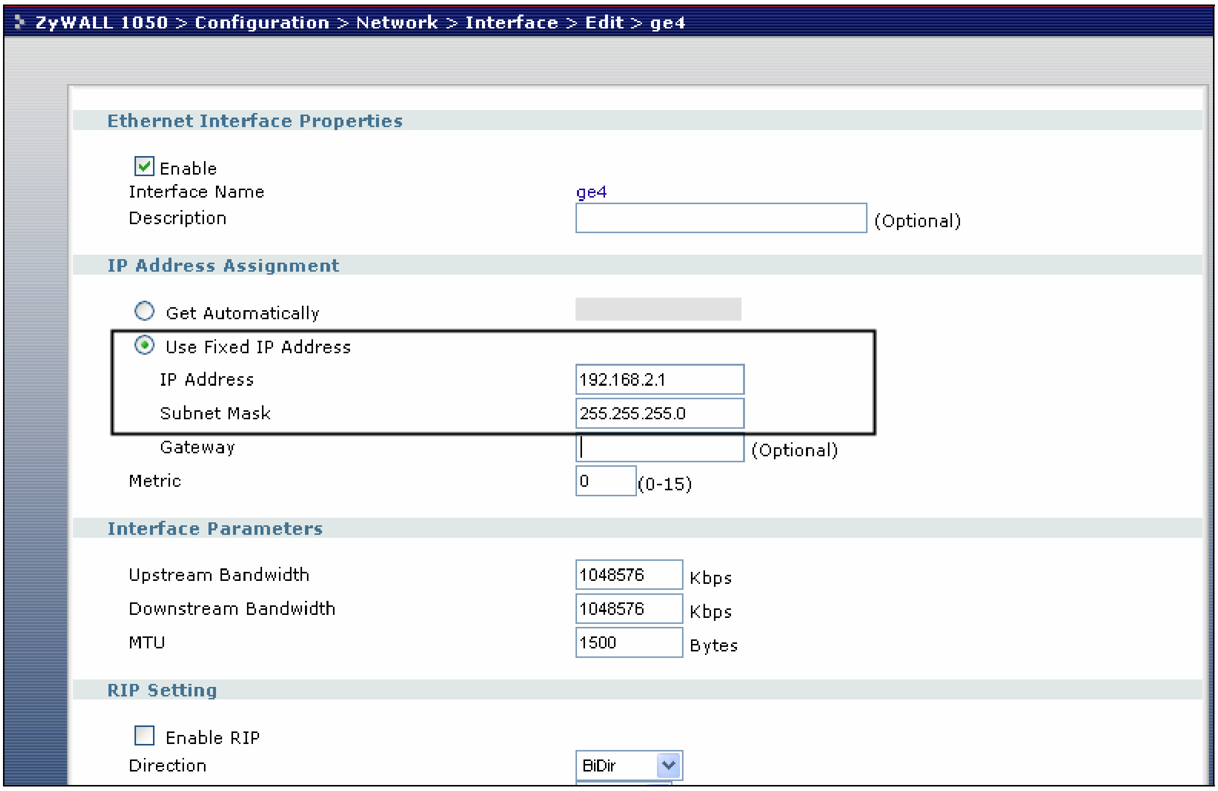
Here are the steps:

1) Login the ZyWALL 1050 GUI and go to **Configuration** > **Network** > **Interface** > **Ethernet.** Since we are going to have three intra-networks in our scenario, we will make GE4 and GE5 another two networks for DMZ and LAN2. First of all, click the “edit” icon which belonging to the GE4 settings.



| # | Name | IP Address | Mask | Modify |
|---|---|---|---|---|
| 1 | ge1 | STATIC -- 192.168.1.1 | 255.255.255.0 | |
| 2 | ge2 | DHCP -- 172.23.30.1 | 255.255.255.0 | |
| 3 | ge3 | DHCP -- 0.0.0.0 | 0.0.0.0 | |
| 4 | ge4 | STATIC -- 0.0.0.0 | 0.0.0.0 | |
| 5 | ge5 | STATIC -- 0.0.0.0 | 0.0.0.0 | |

1) Now we can assign an IP domain to GE4 and another one for GE5. Other settings are all optional. In this example, we keep the default values which will disable the DHCP Server in these two interfaces.



ZyWALL 1050 > Configuration > Network > Interface > Edit > ge4

**Ethernet Interface Properties**

☑ Enable

| | |
|---|---|
| Interface Name | ge4 |
| Description | (Optional) |

**IP Address Assignment**

○ Get Automatically

● Use Fixed IP Address

| | |
|---|---|
| IP Address | 192.168.2.1 |
| Subnet Mask | 255.255.255.0 |
| Gateway | (Optional) |
| Metric | 0 (0-15) |

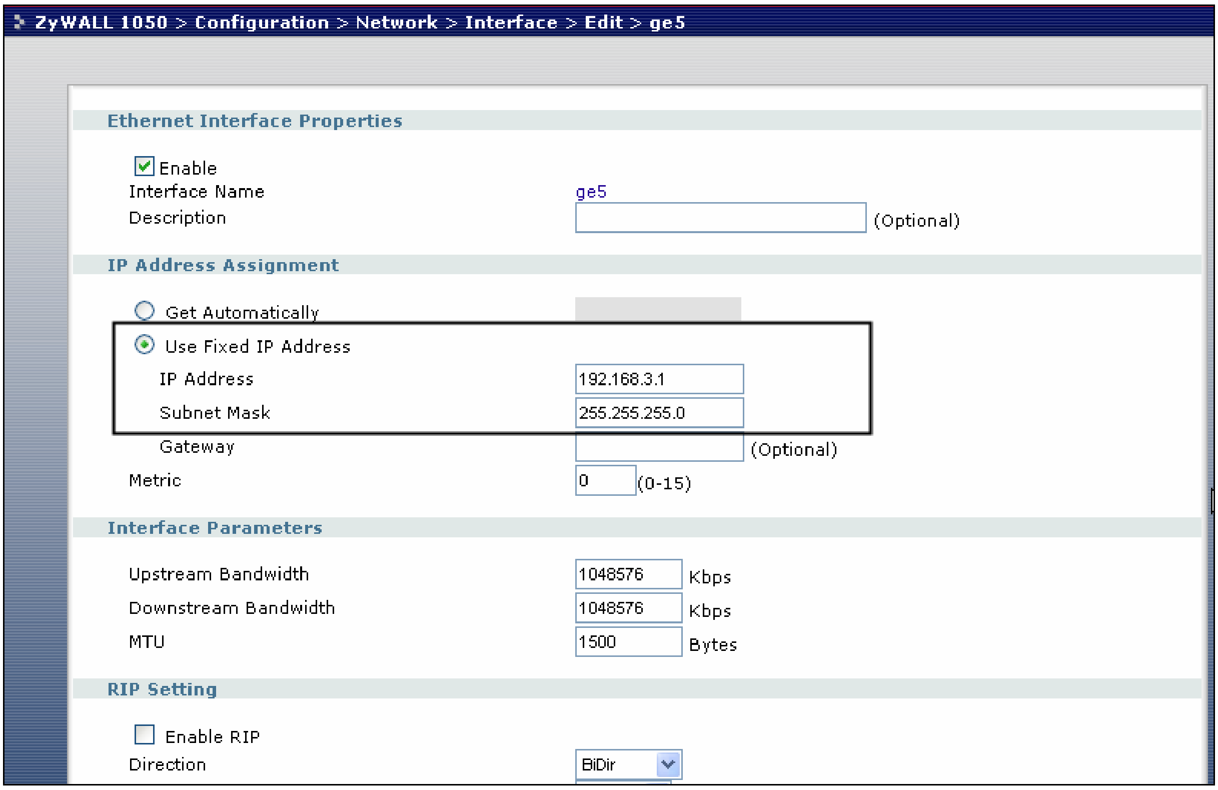
**Interface Parameters**

| | |
|---|---|
| Upstream Bandwidth | 1048576 Kbps |
| Downstream Bandwidth | 1048576 Kbps |
| MTU | 1500 Bytes |

**RIP Setting**

□ Enable RIP

| | |
|---|---|
| Direction | BiDir |



ZyWALL 1050 > Configuration > Network > Interface > Edit > ge5

**Ethernet Interface Properties**

☑ Enable

| | |
|---|---|
| Interface Name | ge5 |
| Description | (Optional) |

**IP Address Assignment**

○ Get Automatically

● Use Fixed IP Address

| | |
|---|---|
| IP Address | 192.168.3.1 |
| 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 |

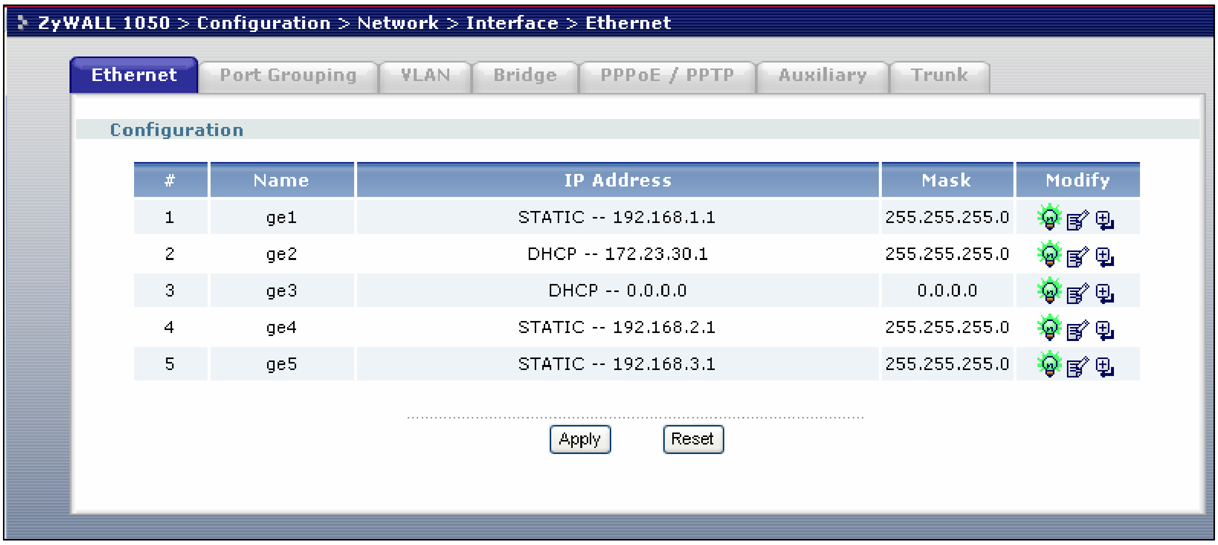
**RIP Setting**

□ Enable RIP

| | |
|---|---|
| Direction | BiDir |

Tips: You do not need a Gateway here since this interface is directly connected to ZyWALL 1050.

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

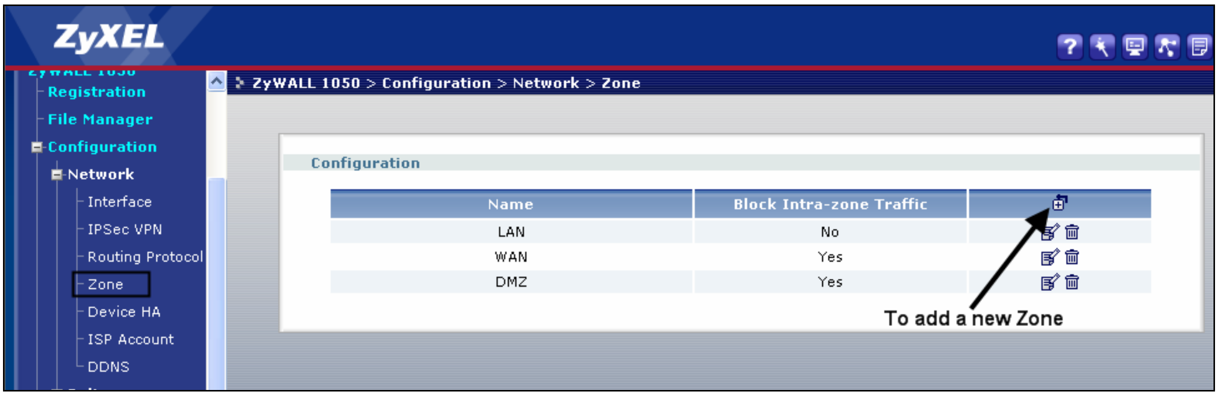


ZyWALL 1050 > Configuration > Network > Interface > Ethernet

Configuration

| # | Name | IP Address | Mask | Modify |
|---|---|---|---|---|
| 1 | ge1 | STATIC -- 192.168.1.1 | 255.255.255.0 | ● ✎ ⊕ |
| 2 | ge2 | DHCP -- 172.23.30.1 | 255.255.255.0 | ● ✎ ⊕ |
| 3 | ge3 | DHCP -- 0.0.0.0 | 0.0.0.0 | ● ✎ ⊕ |
| 4 | ge4 | STATIC -- 192.168.2.1 | 255.255.255.0 | ● ✎ ⊕ |
| 5 | ge5 | STATIC -- 192.168.3.1 | 255.255.255.0 | ● ✎ ⊕ |

3) Now, you will need to setup your DMZ Zone and LAN2 Zone. Go to **Configuration** > **Network** > **Zone.** Click on the "+" icon to add a new Zone.



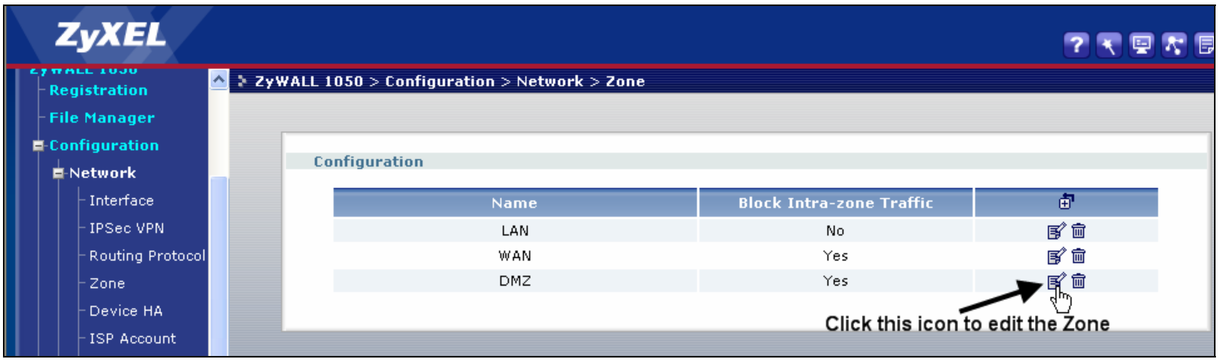
ZyWALL 1050 > Configuration > Network > Zone

Configuration

| Name | Block Intra-zone Traffic | ⊕ |
|---|---|---|
| LAN | No | ✎ 🗑 |
| WAN | Yes | ✎ 🗑 |
| DMZ | Yes | ✎ 🗑 |

To add a new Zone

4) Although the DMZ Zone is already there, by default it includes both GE4 and GE5 as its interfaces. Since we need GE5 for our LAN2 Zone, we will need to remove the interface GE5 from the DMZ Zone. Click the "edit" icon of DMZ Zone and then click on the "remove" icon of the GE5 interface.

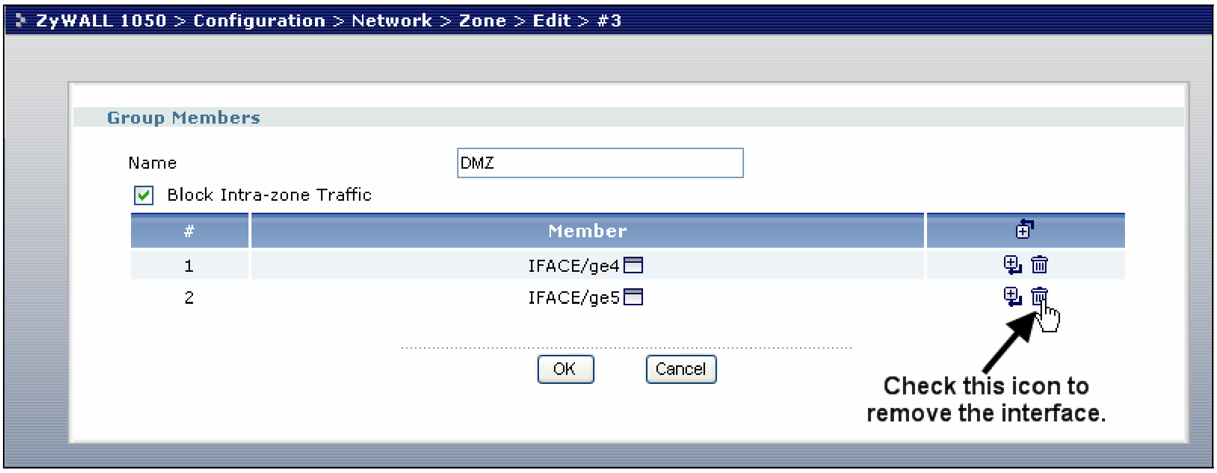


ZyWALL 1050 > Configuration > Network > Zone

Configuration

| Name | Block Intra-zone Traffic | |
|---|---|---|
| LAN | No | |
| WAN | Yes | |
| DMZ | Yes | |

Click this icon to edit the Zone



ZyWALL 1050 > Configuration > Network > Zone > Edit > #3

Group Members

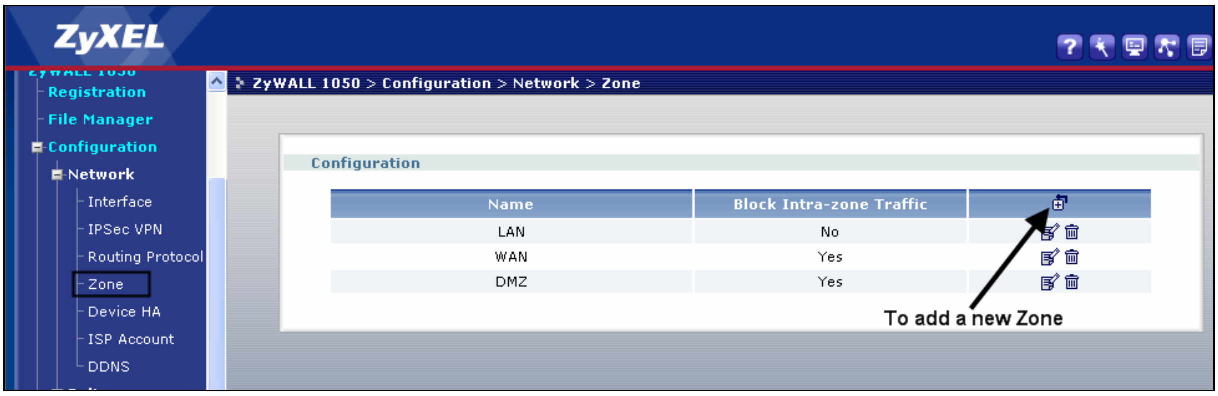
Name: DMZ

☑ Block Intra-zone Traffic

| # | Member | |
|---|---|---|
| 1 | IFACE/ge4 | |
| 2 | IFACE/ge5 | |

Check this icon to remove the interface.

5) Now go back to the Zone page and click the “+” icon to create the LAN2 Zone (for GE5)



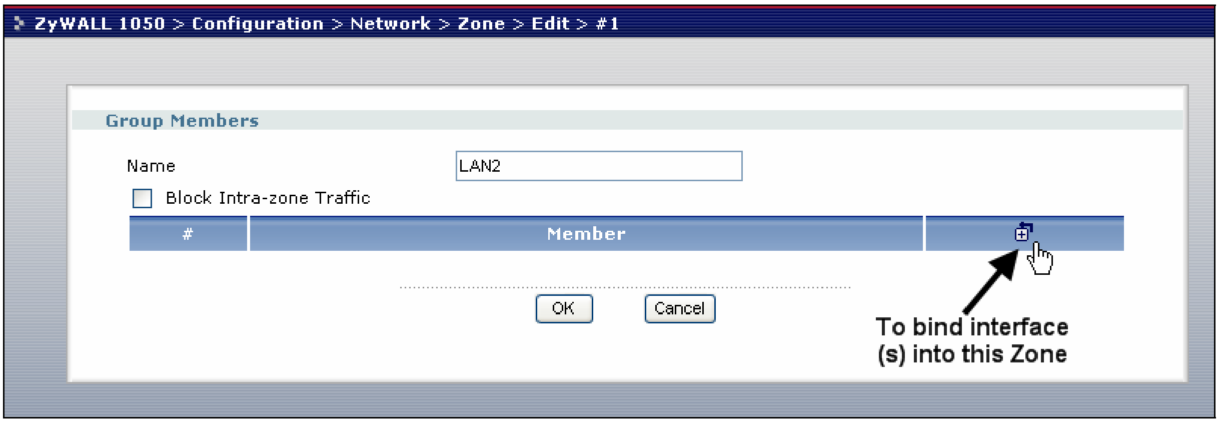
ZyWALL 1050 > Configuration > Network > Zone

Configuration

| Name | Block Intra-zone Traffic | |
|---|---|---|
| LAN | No | |
| WAN | Yes | |
| DMZ | Yes | |

To add a new Zone

6) Put the name “LAN2” and click the “+” icon again to bind the interface to this Zone. Now we only have one interface in this Zone. It is not necessary to care about any Intra-zone traffic.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #1

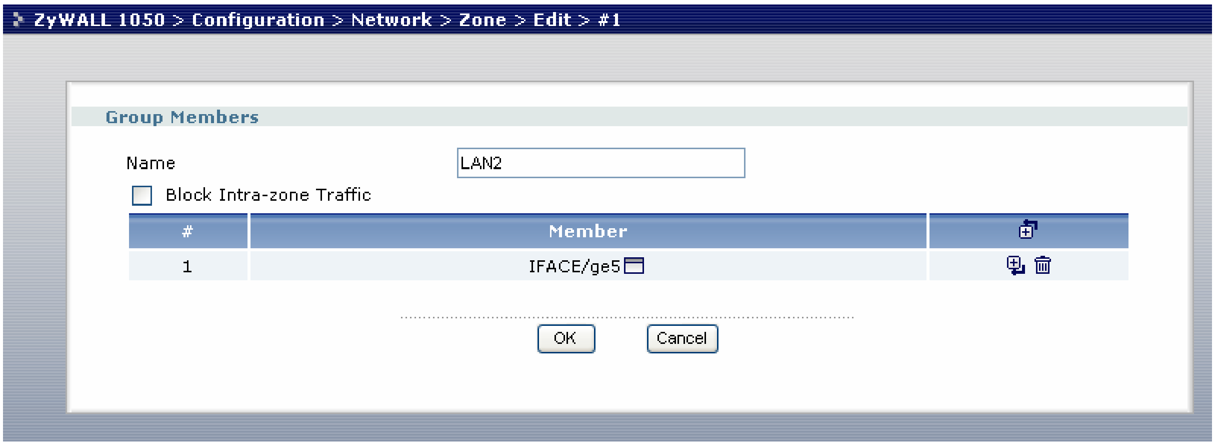
Group Members

Name: LAN2

□ Block Intra-zone Traffic

| # | Member | |
|---|---|---|

7) Since GE5 is the only interface left, GE5 will be automatically selected. Finally click "OK" to apply the new setting.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #1

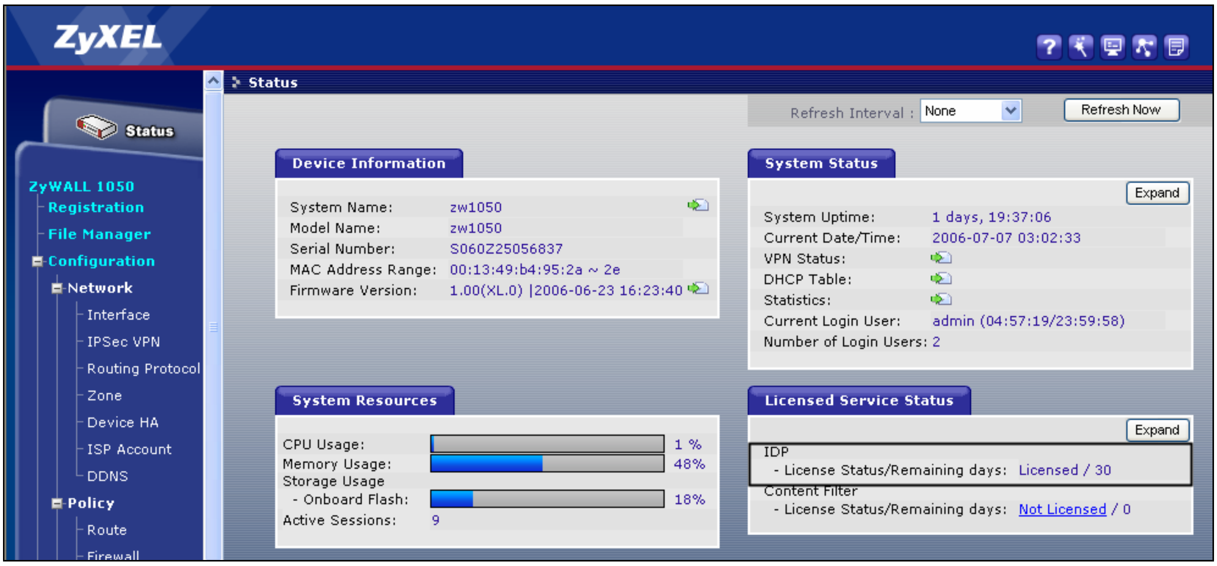
Group Members

Name: LAN2

□ Block Intra-zone Traffic

| # | Member | |
|---|---|---|
| 1 | IFACE/ge5 | |

8) Before you apply the IDP profiles, you need to make sure that the IDP Service on your ZyWALL 1050 is licensed.



Status

Refresh Interval : None

Device Information

System Name: zw1050
Model Name: zw1050
Serial Number: S060Z25056837
MAC Address Range: 00:13:49:b4:95:2a ~ 2e
Firmware Version: 1.00(XL.0) |2006-06-23 16:23:40

System Status

System Uptime: 1 days, 19:37:06
Current Date/Time: 2006-07-07 03:02:33
VPN Status:
DHCP Table:
Statistics:
Current Login User: admin (04:57:19/23:59:58)
Number of Login Users: 2

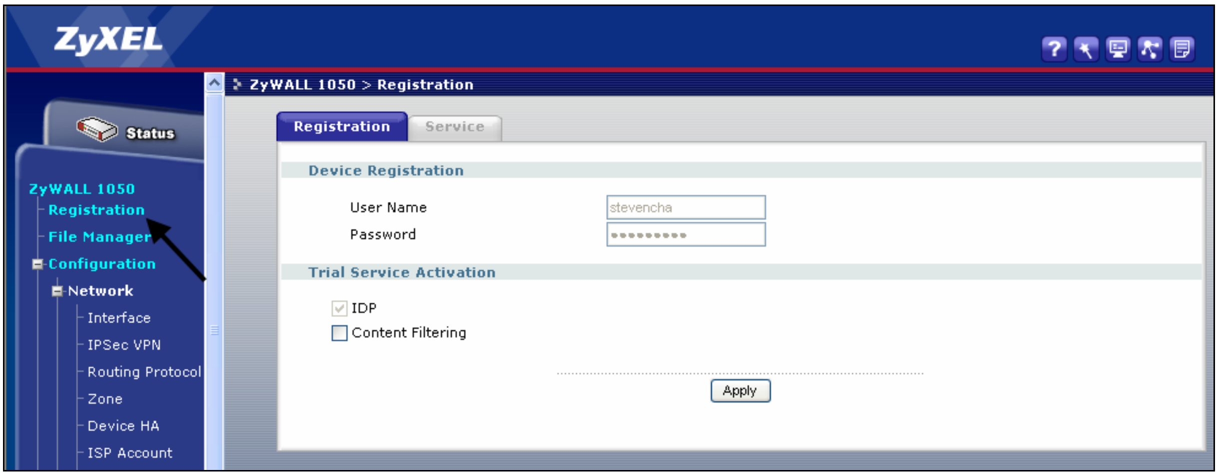
System Resources

CPU Usage: 1 %
Memory Usage: 48%
Storage Usage
- Onboard Flash: 18%
Active Sessions: 9

Licensed Service Status

IDP
- License Status/Remaining days: Licensed / 30
Content Filter
- License Status/Remaining days: Not Licensed / 0

9) 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 1050 comes with a 30 days free trial on IDP Service. Just register your ZyWALL 1050 and your ZyWALL 1050 will receive the license automatically. Here a page which is already registered is shown.



ZyWALL 1050 > Registration

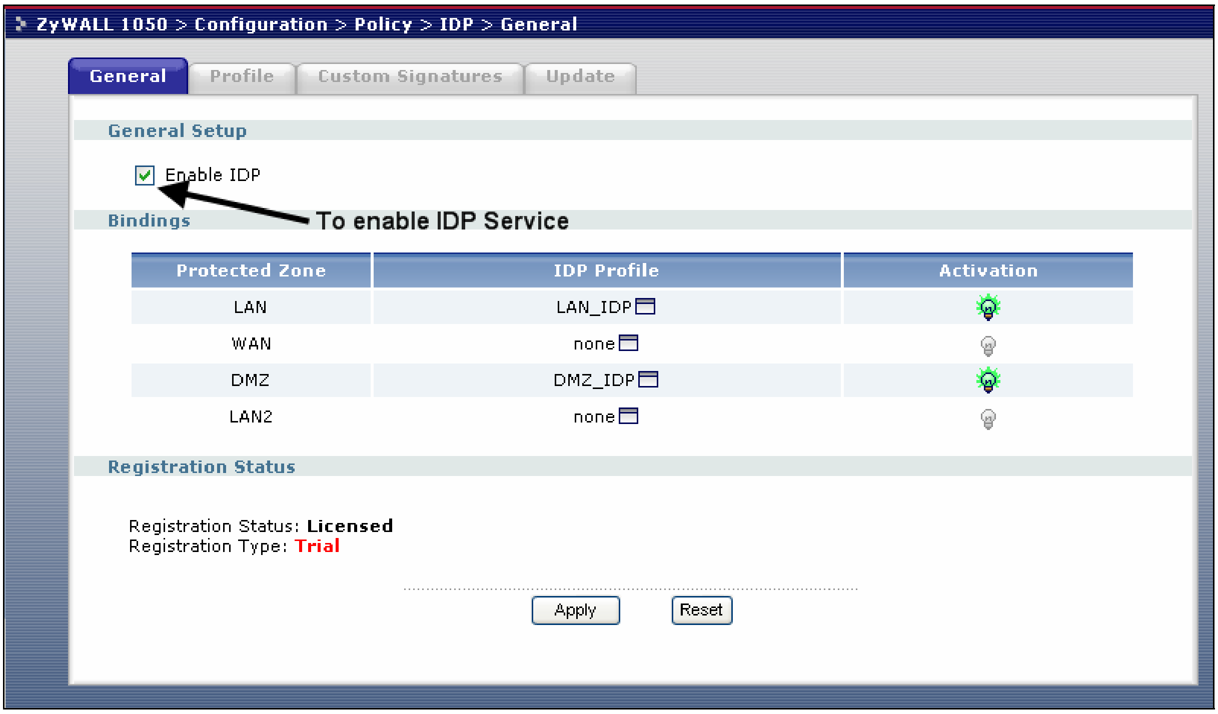
Device Registration

User Name: stevencha
Password: ●●●●●●●●●

Trial Service Activation

☑ IDP
□ Content Filtering

10) Now, go to **Configuration** > **Policy** > **IDP**. Enable the IDP check box to activate the IDP service on your ZyWALL 1050.



General Setup

☑ Enable IDP

To enable IDP Service

Bindings

| Protected Zone | IDP Profile | Activation |
|---|---|---|
| LAN | LAN_IDP | ● |
| WAN | none | ○ |
| DMZ | DMZ_IDP | ● |
| LAN2 | none | ○ |

Registration Status

Registration Status: **Licensed**
Registration Type: **Trial**

11) 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.

**CLI commands to create an IP Domain 192.168.2.0/24 on GE4:**

[0] interface ge4

[1] ip address 192.168.2.1 255.255.255.0

[2] ping-check default-gateway

[3] ping-check default-gateway period 30

[4] ping-check default-gateway timeout 5

[5] ping-check default-gateway fail-tolerance 5

[6] no ping-check activate

[7] exit

[8] router rip

[9] exit

```
[10] router ospf
[11] exit
```

**CLI commands to create an IP Domain 192.168.3.0/24 on GE5:**

```
[0] interface ge5
[1] ip address 192.168.3.1 255.255.255.0
[2] ping-check default-gateway
[3] ping-check default-gateway period 30
[4] ping-check default-gateway timeout 5
[5] ping-check default-gateway fail-tolerance 5
[6] no ping-check activate
[7] exit
[8] router rip
[9] exit
[10] router ospf
[11] exit
```

**CLI commands for removing GE5 from the DMZ Zone:**

```
[0] zone DMZ
[1] block
[2] no interface ge4
[3] no interface ge5
[4] interface ge4
[5] exit
```

**CLI commands for creating the LAN2 Zone:**

```
[0] zone LAN2
[1] no block
```

```
[2] interface ge5

[3] exit
```

**CLI commands for activating the IDP service:**

```
[0] idp activate

[1] idp zone LAN activate

[2] no idp zone WAN activate

[3] idp zone DMZ activate

[4] no idp zone LAN2 activate
```

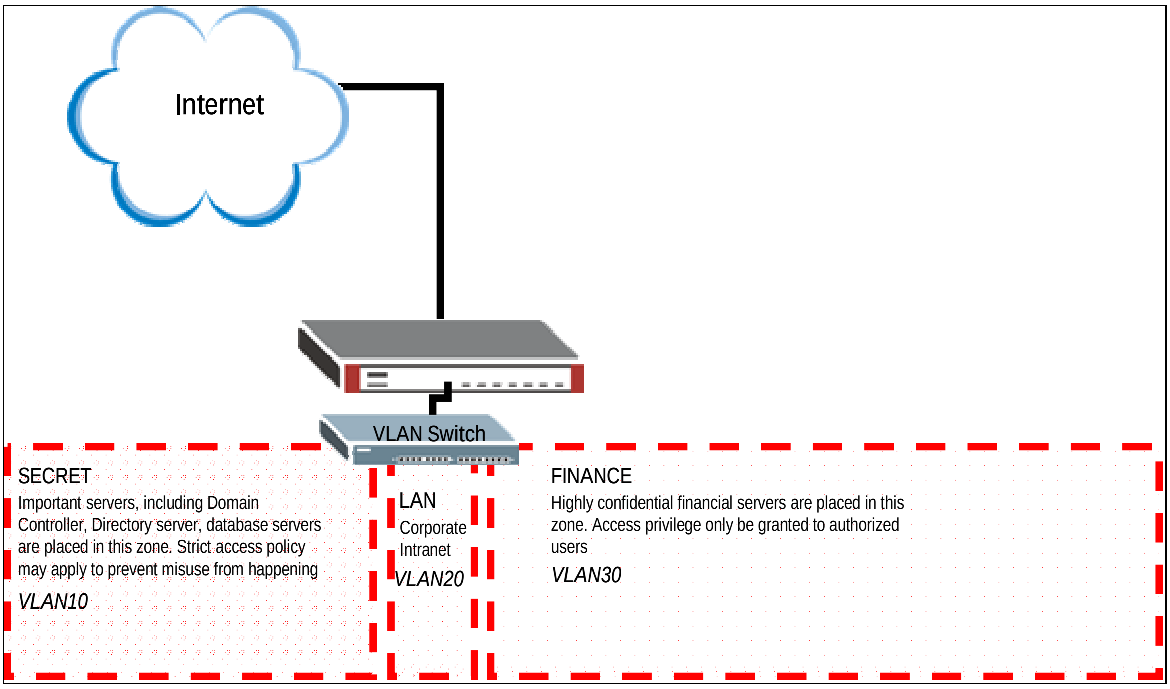
## 3.3 Networking Partitioning Using VLAN

Although ZyWALL 1050 has only five physical ports, you can still partition your networking with more than five interfaces. ZyWALL 1050 is VLAN aware and it supports virtual interface as well. With ZyWALL 1050, you can run a maximum number of thirty two VLANs. As a result, it makes networking partitioning very easy. However, a VLAN-capable L2 switch is required to create the VLAN tags in front of ZyWALL 1050.

When you conduct a network planning, it is always a good idea to aggregate all the similar security level of devices into the same security zone. And different security level of devices should be placed in different security zone. Finally you can apply different access policy enforcements to different security zones to make your network more secure. By combing VLAN and customizable zones, IT managers can construct necessary security infrastructure without hassle and reduce the management burden.

### 3.3.1 Creating VLAN virtual interfaces

Here is an example

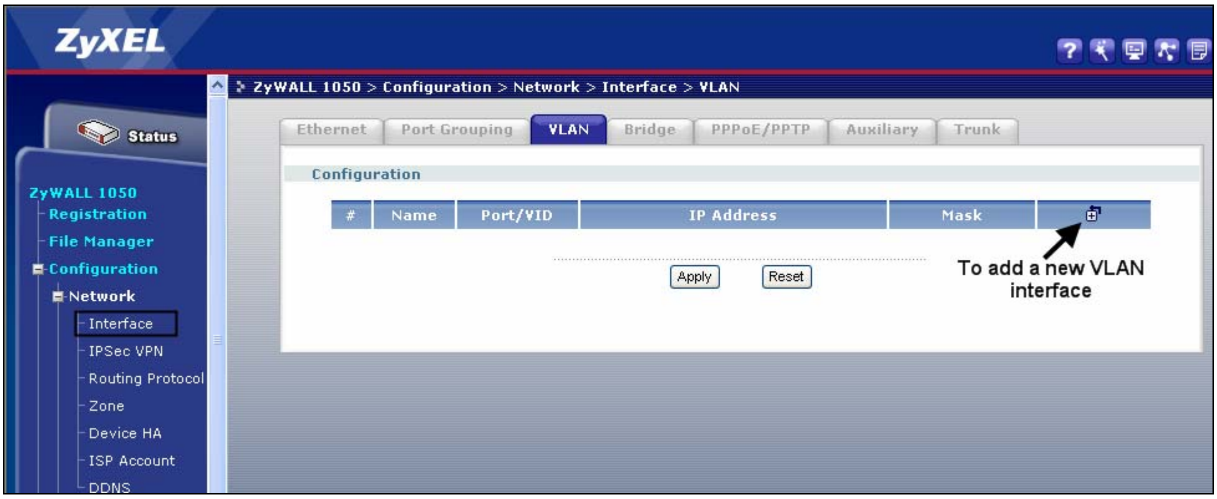

Internet
VLAN Switch
SECRET
Important servers, including Domain Controller, Directory server, database servers are placed in this zone. Strict access policy may apply to prevent misuse from happening
VLAN10
LAN
Corporate Intranet
VLAN20
FINANCE
Highly confidential financial servers are placed in this zone. Access privilege only be granted to authorized users
VLAN30

**VLAN-capable L2 switch is required to create VLAN tags*

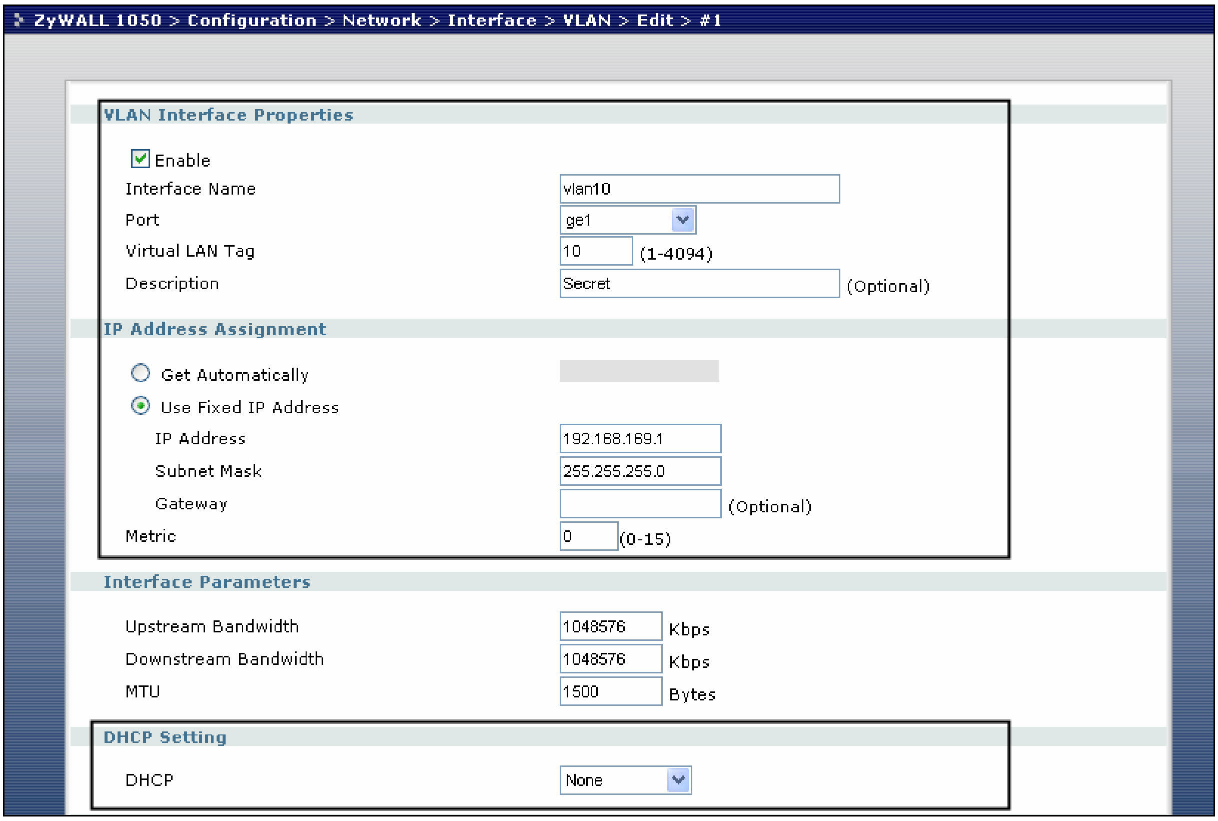
Let’s assume we run WAN on port 2 and LAN on port 1. Now we need to create three VLAN virtual interfaces on port 1. These are VLAN10, VLAN 20 and VLAN30. In this scenario, the VLAN aware Switch will need to apply VLAN10, VLAN20 and VLAN30 802.1q tags to the corresponding packets and send all the packets to the ZyWALL 1050 port 1 through a single physical RJ45 cable.

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

1) Login ZyWALL 1050 GUI and go to **Configuration** > **Network** > **Interface** > **VLAN.** Then click on “+” to add a new VLAN interface.



2) Fill in the information like Interface name, port, VLAN tag and Description. Also, you can choose either getting an IP automatically for this interface or assigning a static one to it. ZyWALL 1050 also supports DHCP Server or Relay per VLAN interface. You can change it in the DHCP Setting section.



ZyWALL 1050 > Configuration > Network > Interface > VLAN > Edit > #1

**VLAN Interface Properties**

☑ Enable

| | |
|---|---|
| Interface Name | vlan10 |
| Port | ge1 |
| Virtual LAN Tag | 10 (1-4094) |
| Description | Secret (Optional) |

**IP Address Assignment**

○ Get Automatically

● Use Fixed IP Address

| | |
|---|---|
| IP Address | 192.168.169.1 |
| Subnet Mask | 255.255.255.0 |
| Gateway | (Optional) |
| Metric | 0 (0-15) |

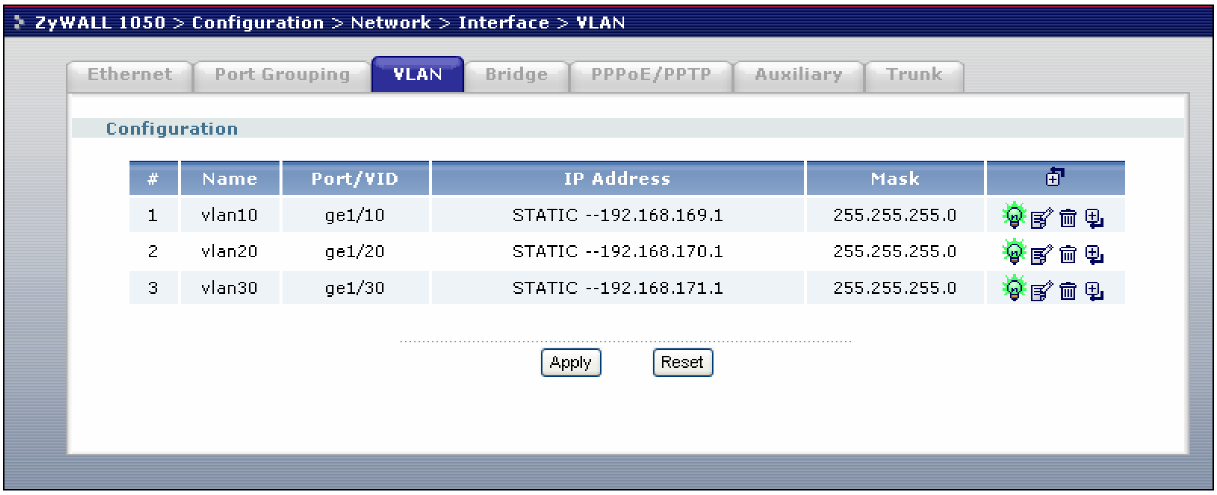
**Interface Parameters**

| | |
|---|---|
| Upstream Bandwidth | 1048576 Kbps |
| Downstream Bandwidth | 1048576 Kbps |
| MTU | 1500 Bytes |

**DHCP Setting**

| | |
|---|---|
| DHCP | None |

3) By following the above steps you can create another two VLAN interfaces. (VLAN20 and VLAN30).



ZyWALL 1050 > Configuration > Network > Interface > VLAN

**Configuration**

| # | Name | Port/VID | IP Address | Mask | |
|---|---|---|---|---|---|
| 1 | vlan10 | ge1/10 | STATIC --192.168.169.1 | 255.255.255.0 | |
| 2 | vlan20 | ge1/20 | STATIC --192.168.170.1 | 255.255.255.0 | |
| 3 | vlan30 | ge1/30 | STATIC --192.168.171.1 | 255.255.255.0 | |

**The CLI commands to create the above VLAN10:**

[0] interface vlan10

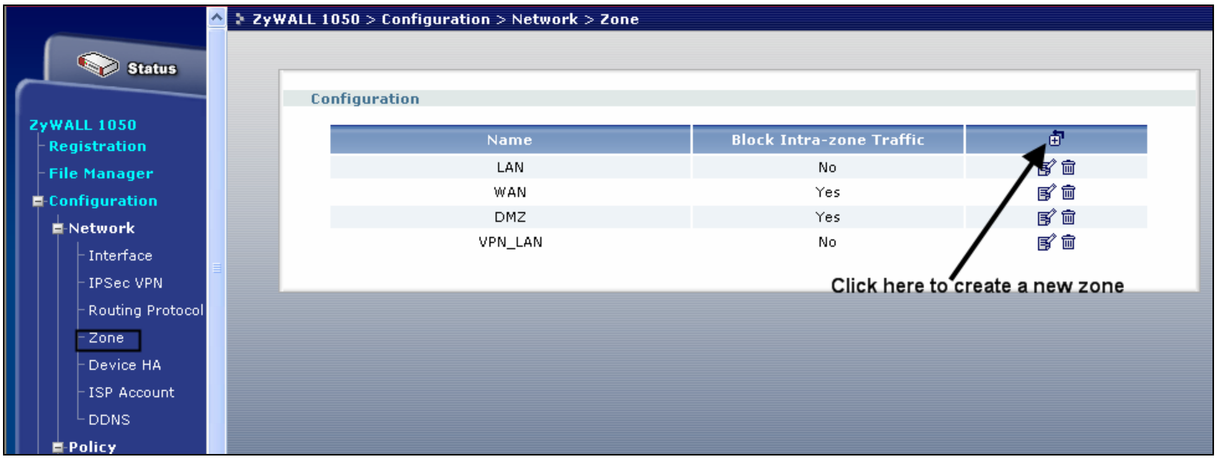
```
[1] no shutdown
[2] port ge1
[3] vlan-id 10
[4] description Secret
[5] upstream 1048576
[6] downstream 1048576
[7] mtu 1500
[8] ip address 192.168.169.1 255.255.255.0
[9] ping-check default-gateway
[10] ping-check default-gateway period 30
[11] ping-check default-gateway timeout 5
[12] ping-check default-gateway fail-tolerance 5
[13] no ping-check activate
[14] exit
```

### 3.3.2 Adding VLAN virtual interfaces to the Zone

Now, since the security policy cannot be applied between interfaces but between zones, it is necessary to add the VLAN virtual interfaces into different zones. Here we are going to create three new zones for the three VLANs.

To create these zones, please follow the configuration steps as below:

1) Login ZyWALL 1050 GUI and go to **Configuration** > **Network** > **Zone.** Then click the "+" to create a new zone.



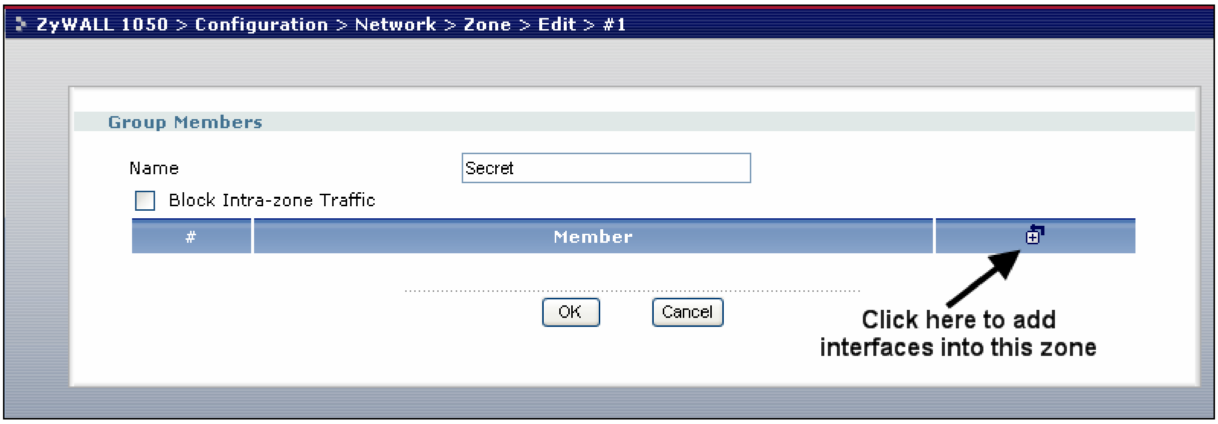
ZyWALL 1050 > Configuration > Network > Zone

Configuration

| Name | Block Intra-zone Traffic | |
|---|---|---|
| LAN | No | |
| WAN | Yes | |
| DMZ | Yes | |
| VPN_LAN | No | |

Click here to create a new zone

2) Give this zone whatever name you can understand later. Check the option “Block Intra-zone Traffic” if you do not want the traffic between different interfaces included in this zone to be allowed. And again click on the “+” icon to make interfaces join this zone.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #1

Group Members

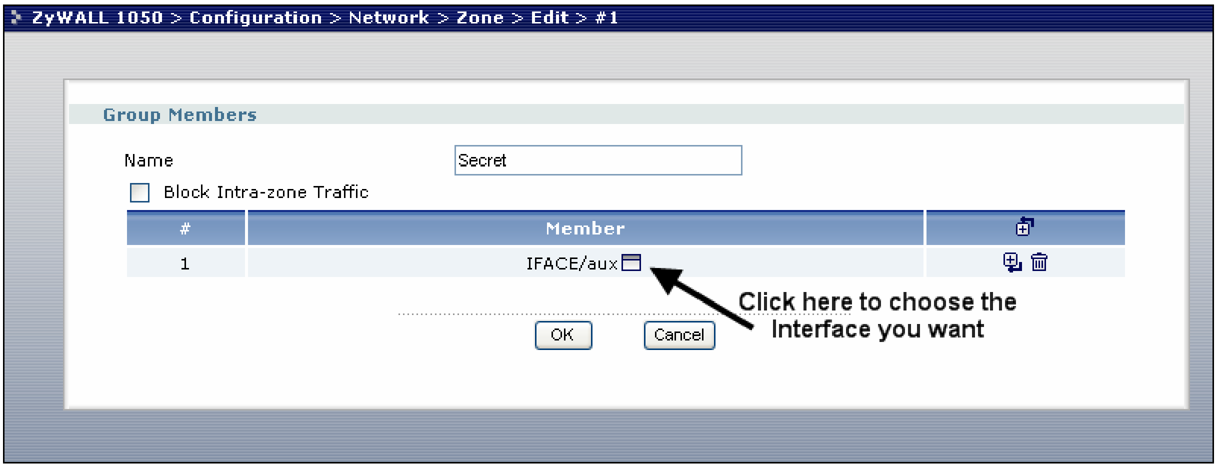
Name: Secret

□ Block Intra-zone Traffic

| # | Member | |
|---|---|---|

Click here to add interfaces into this zone

3) Right after you click on the “+” icon, you will see an interface added to your zone automatically. However, it may not be the one that you have been looking for. Thus, you will need to click on the box of the interface and choose the one that you are looking for.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #1

Group Members

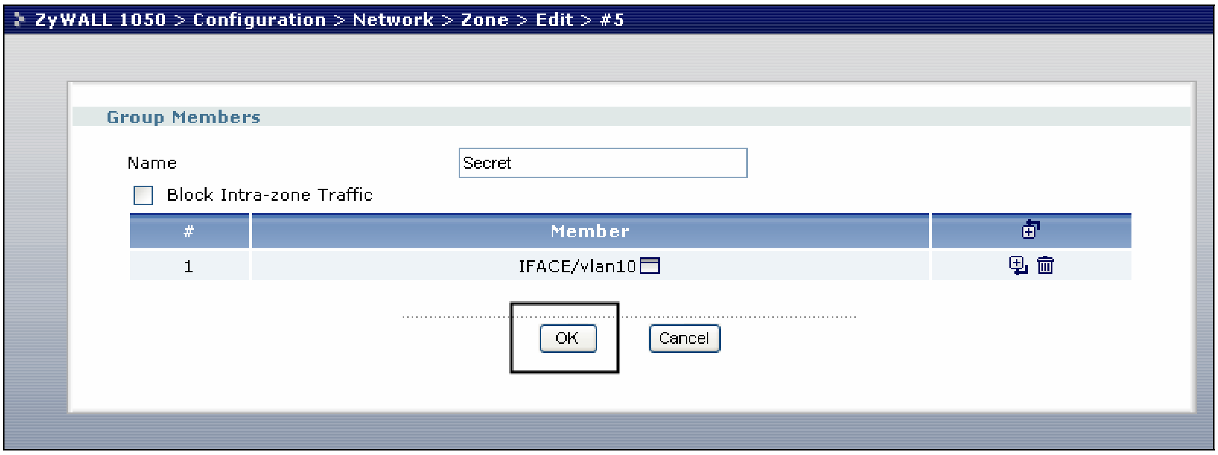
Name: Secret

□ Block Intra-zone Traffic

| # | Member | |
|---|---|---|
| 1 | IFACE/aux | |

Click here to choose the Interface you want

4) Finally, click “OK” to apply your settings.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #5

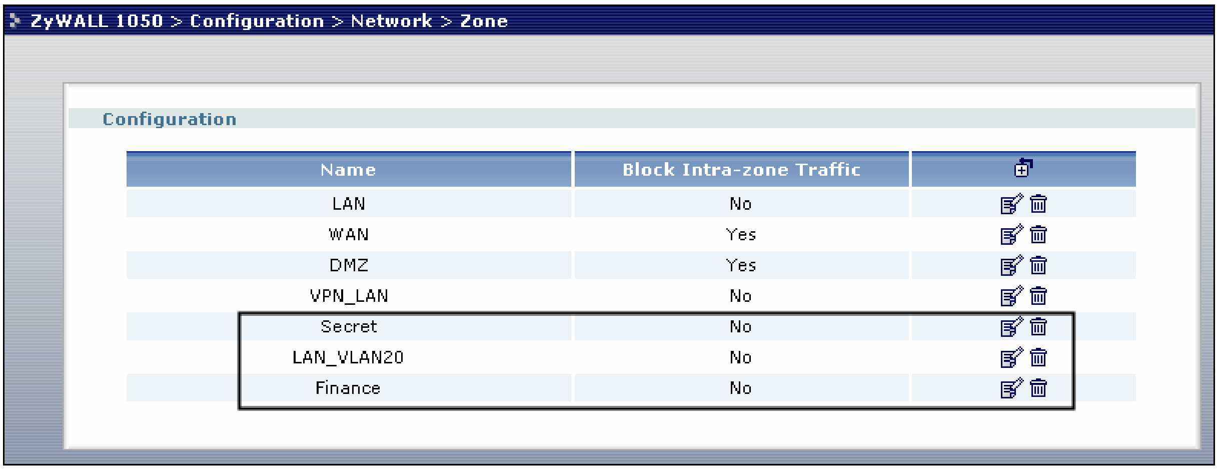
Group Members

Name: Secret

□ Block Intra-zone Traffic

| # | Member | |
|---|---|---|
| 1 | IFACE/vlan10 | |

4) Repeat the above steps to create the other two Zones for VLAN20 and VLAN30.



ZyWALL 1050 > Configuration > Network > Zone

Configuration

| Name | Block Intra-zone Traffic | |
|---|---|---|
| LAN | No | |
| WAN | Yes | |
| DMZ | Yes | |
| VPN_LAN | No | |
| Secret | No | |
| LAN_VLAN20 | No | |
| Finance | No | |

**The CLI commands to join VLAN10 to the Zone:**

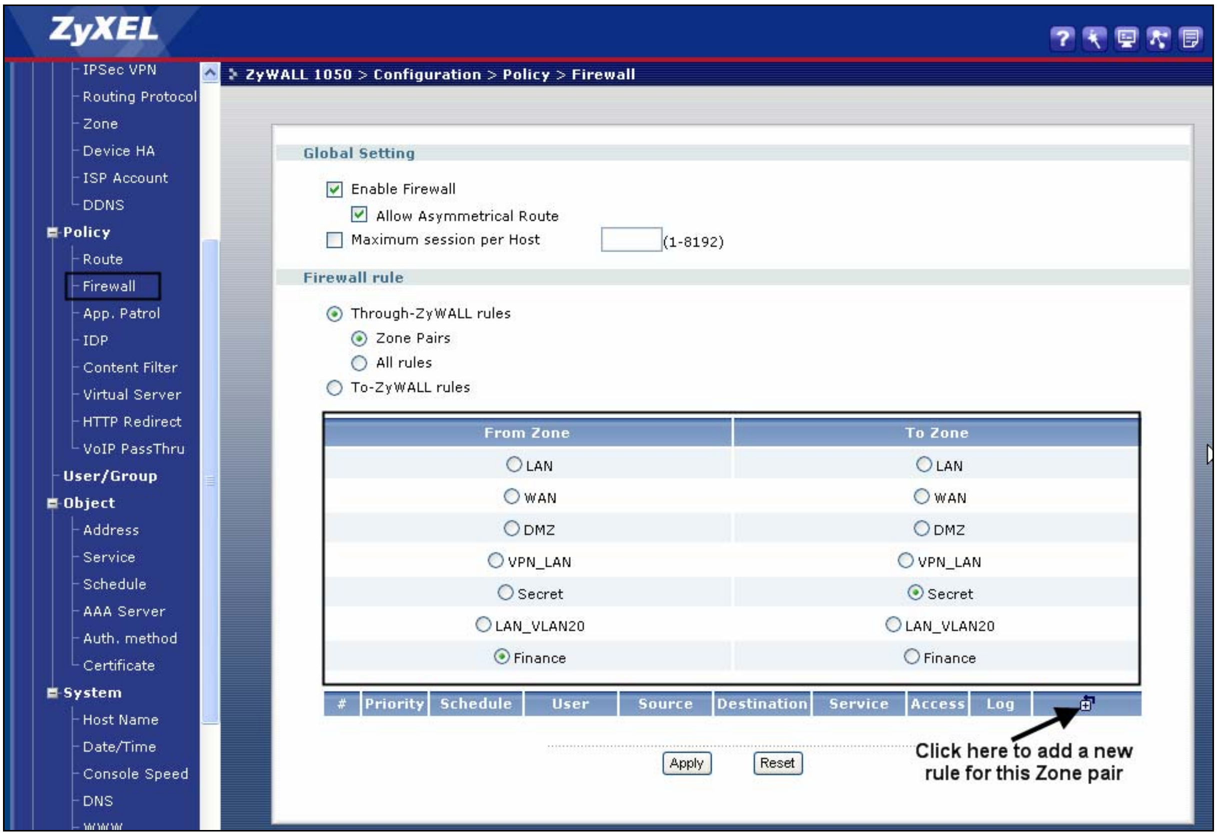
```
[0] zone Secret
[1] no block
[2] interface vlan10
[3] exit
```

### 3.3.3 Applying firewall policy to the Zone of VLANs

Security policy can be enforced between Zones in ZyWALL 1050. Since we have just created three new Zones on port GE1, we can apply some security policies between these Zones. For example, if you do not allow users in the Finance Zone to have an access to users or devices in the Secret Zone, you can apply a firewall rule to do so. Moreover, if you want to allow users in Secret Zone to access users or devices located in the LAN_VLAN20 Zone, you can apply another firewall rule to do so.

To create those two rules, please follow the configuration steps as stated below:

1) Login the ZyWALL 1050 GUI and go to **Configuration** > **Policy** > **Firewall.** Check "Enable Firewall" to activate your Firewall. Then pick your Zone pairs and click the "+" icon to create a new firewall rule especially for your selected pair. For example, first we want to block the access from Finance Zone to Secret Zone, we pick Finance Zone on the left and Secret Zone on the right.



ZyWALL 1050 > Configuration > Policy > Firewall

Global Setting

☑ Enable Firewall

☑ Allow Asymmetrical Route

□ Maximum session per Host (1-8192)

Firewall rule

● Through-ZyWALL rules

● Zone Pairs

○ All rules

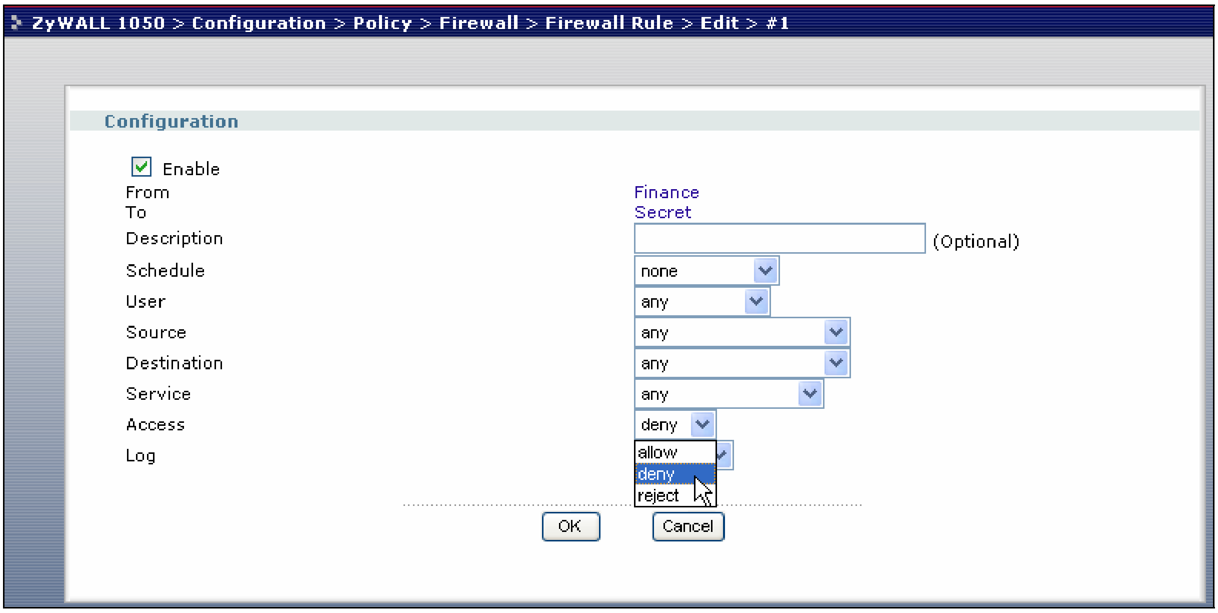
○ To-ZyWALL rules

| From Zone | To Zone |
|---|---|
| ○ LAN | ○ LAN |
| ○ WAN | ○ WAN |
| ○ DMZ | ○ DMZ |
| ○ VPN_LAN | ○ VPN_LAN |
| ○ Secret | ● Secret |
| ○ LAN_VLAN20 | ○ LAN_VLAN20 |
| ● Finance | ○ Finance |

| # | Priority | Schedule | User | Source | Destination | Service | Access | Log | |
|---|---|---|---|---|---|---|---|---|---|

Click here to add a new rule for this Zone pair

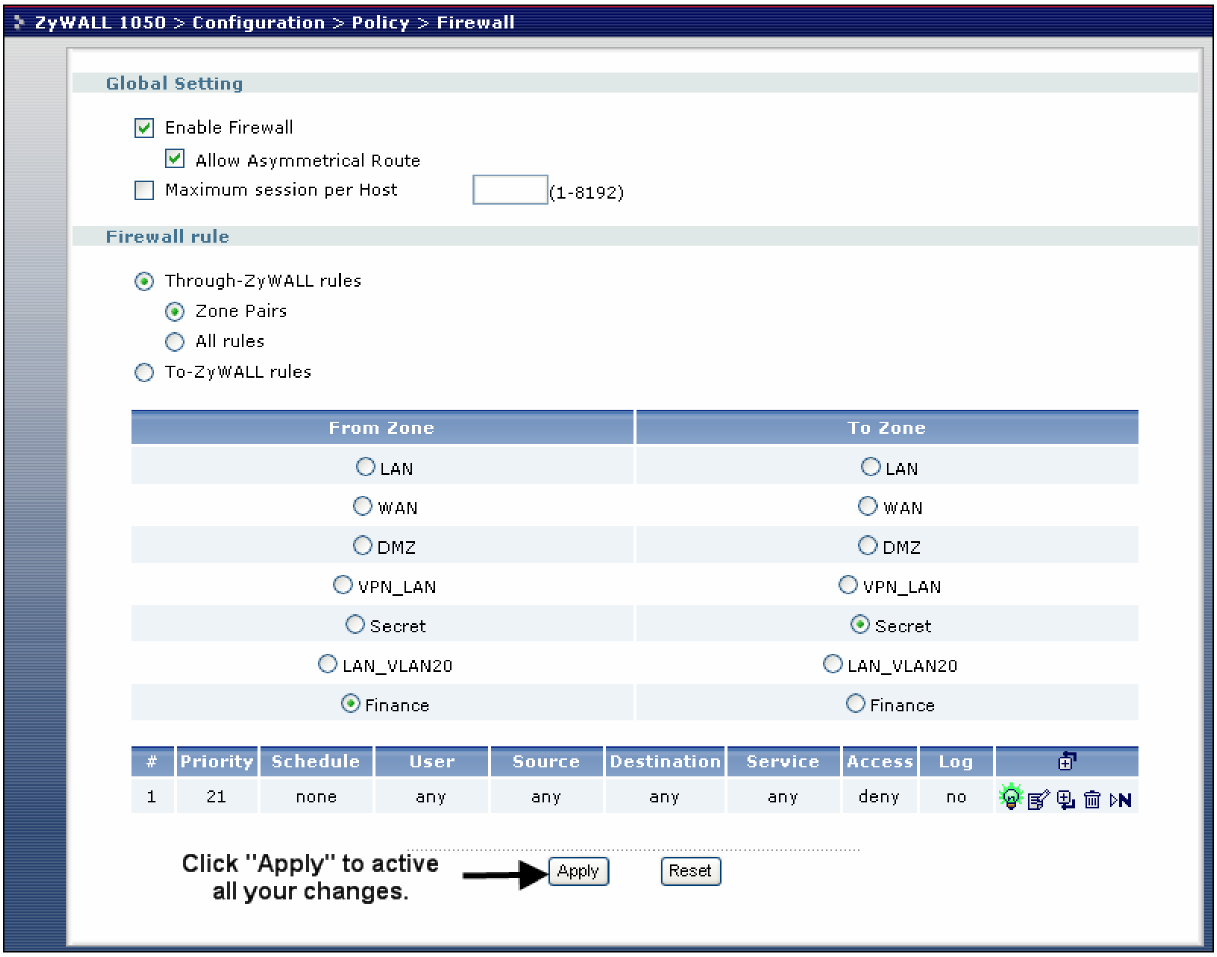
12) It is optional to give this rule a description. If you want to allow anything or block anything, just simply choose “allow” or “deny” as the option of “Access”. Option “Reject” means dropping the packets that match with this rule silently.


ZyWALL 1050 > Configuration > Policy > Firewall > Firewall Rule > Edit > #1

Configuration

|  |  |
|---|---|
| ☑ Enable | |
| From | Finance |
| To | Secret |
| Description | (Optional) |
| Schedule | none |
| User | any |
| Source | any |
| Destination | any |
| Service | any |
| Access | deny |
| Log | |

3) Finally, click “Apply” to activate all your changes on this screen.



ZyWALL 1050 > Configuration > Policy > Firewall

Global Setting

☑ Enable Firewall

☑ Allow Asymmetrical Route

□ Maximum session per Host (1-8192)

Firewall rule

● Through-ZyWALL rules

● Zone Pairs

○ All rules

○ To-ZyWALL rules

| From Zone | To Zone |
|---|---|
| ○ LAN | ○ LAN |
| ○ WAN | ○ WAN |
| ○ DMZ | ○ DMZ |
| ○ VPN_LAN | ○ VPN_LAN |
| ○ Secret | ● Secret |
| ○ LAN_VLAN20 | ○ LAN_VLAN20 |
| ● Finance | ○ Finance |

| # | Priority | Schedule | User | Source | Destination | Service | Access | Log | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 21 | none | any | any | any | any | deny | no | |

Click "Apply" to active all your changes.

4) Repeat the above steps to make another firewall rule to “allow” everything from “Secret” Zone to “LAN_VLAN20” Zone.

**The CLI commands for the above actions:**

[0] firewall Finance Secret insert 1

[1] no schedule

[2] no user

[3] no sourceip

[4] no destinationip

[5] no service

[6] action deny

[7] from Finance

[8] to Secret

[9] no log

[10] activate

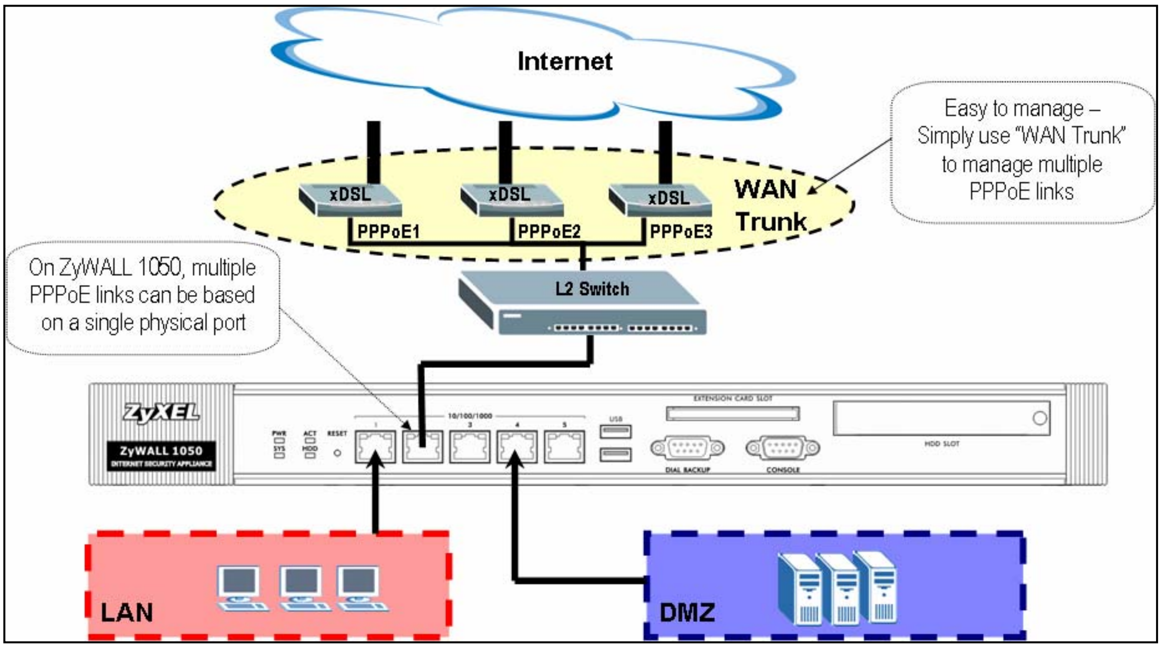
[11] exit

## 3.4 Connecting Multiple ISP Links

The standard option for increasing the bandwidth of your WAN link is to upgrade the capacity of the existing link. However, usually this option will come at a high price in both time and money. And sometimes it may not be available at all. Thus, ZyWALL 1050 comes with another solution which gives more flexibility on upgrading your WAN Link. Basically, ZyWALL 1050 can build up to 12 PPPoE WAN links via one single port or having multiple fixed links over four physical ports. Moreover, ZyWALL 1050 supports an easy management feature for all your WAN Links. It will create a "WAN Trunk" interface for you to manage all of your WAN links. You can manage it like a single WAN link. Users are allowed to choose a load balancing algorithm they wish in order to optimize the utilization of the WAN Links as well as the fault tolerance to increase reliability.

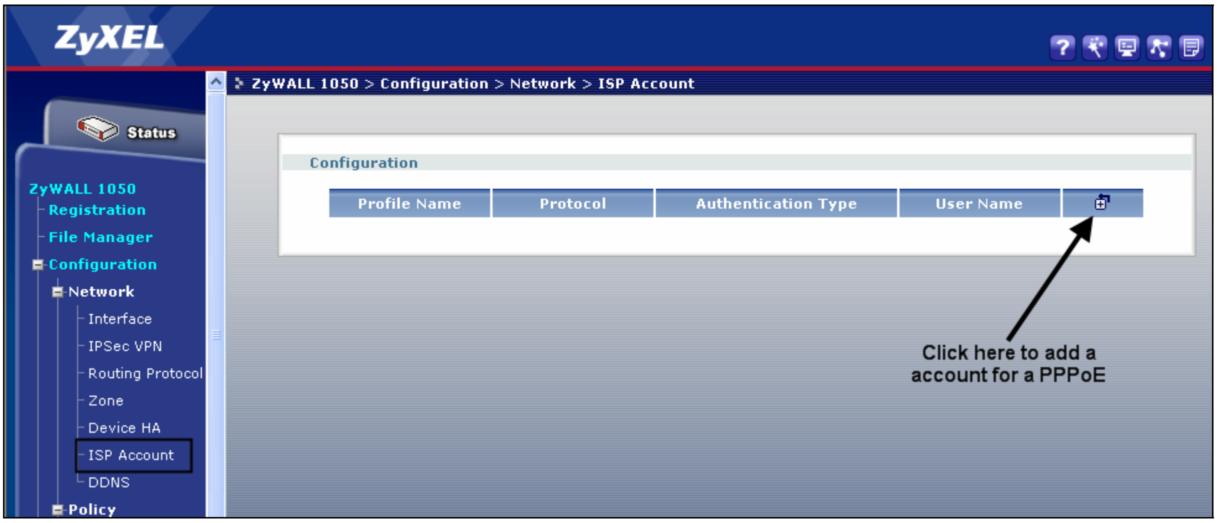
### 3.4.1 Multiple PPPoE links

Multiple PPPoE Links are supported on ZyWALL 1050, with a L2 Switch it will only take one of your physical ports. Here is an example.


Internet
xDSL
xDSL
xDSL
PPPoE1
PPPoE2
PPPoE3
WAN Trunk
Easy to manage – Simply use "WAN Trunk" to manage multiple PPPoE links
On ZyWALL 1050, multiple PPPoE links can be based on a single physical port
L2 Switch
ZyXEL
ZyWALL 1050
LAN
DMZ

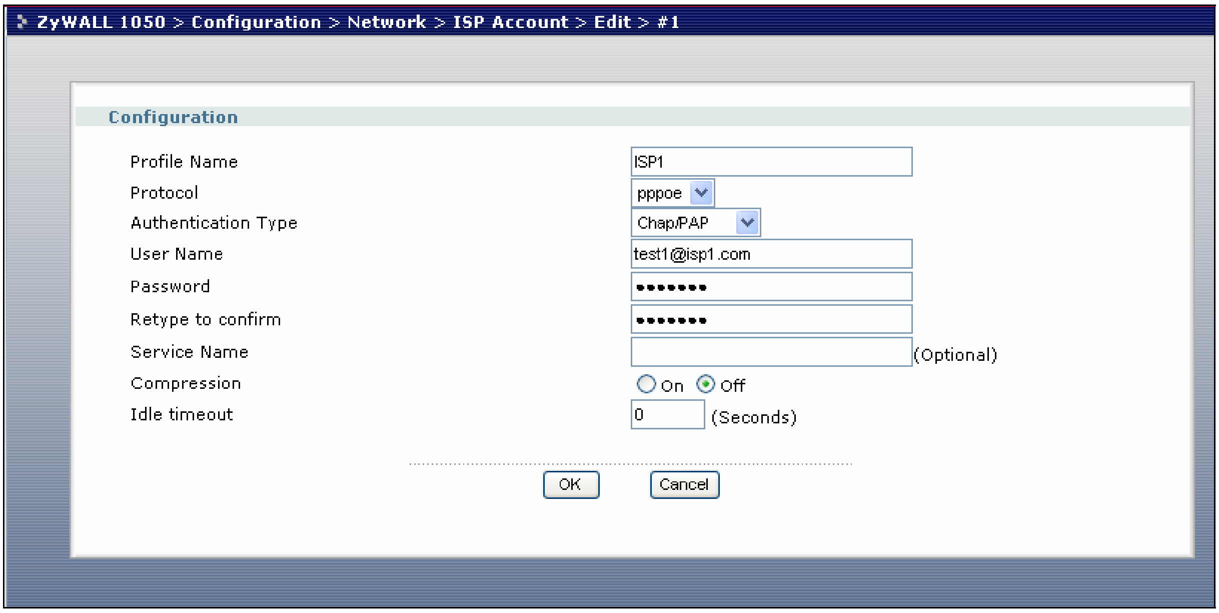
To create three PPPoE links and manage them with the Wan Trunk interface, please follow the configuration steps as stated below:

1) Login ZyWALL 1050 GUI and go to **Configuration** > **Network** > **ISP Account.** Then click the "+" to create a new account for a PPPoE connection.



Click here to add a account for a PPPoE

2) Now, on the screen, you can give a name to this profile. Select the protocol as PPPoE. Please set the Idle timeout to 0 if you do not want this link to be a subject to timeout. All other parameters including the username and the password should be based on your ISP's requirements. Finally, click "OK" to add this account.

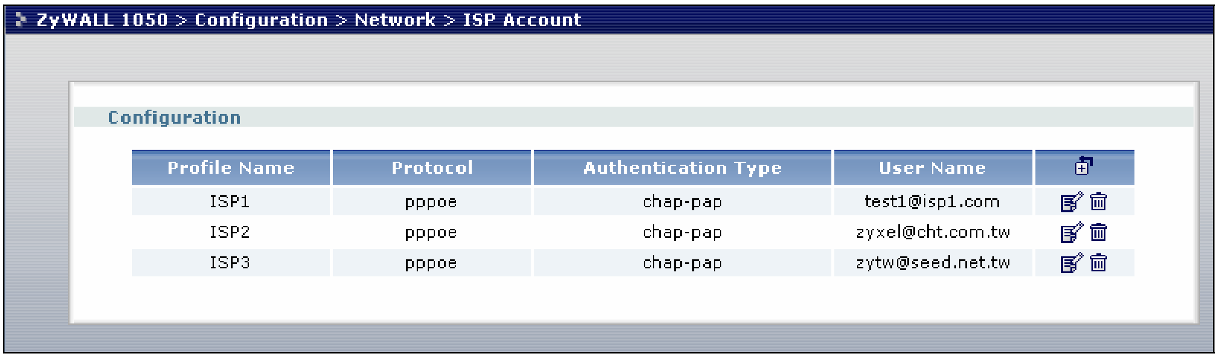

ZyWALL 1050 > Configuration > Network > ISP Account > Edit > #1
OK
Cancel

Configuration

| | |
|---|---|
| Profile Name | ISP1 |
| Protocol | pppoe |
| Authentication Type | Chap/PAP |
| User Name | test1@isp1.com |
| Password | ••••••• |
| Retype to confirm | ••••••• |
| Service Name | (Optional) |
| Compression | ○ On ● Off |
| Idle timeout | 0 (Seconds) |

3) Since we will have three PPPoE links in our scenario, you will need two additional PPPoE

accounts here as well. Repeat the above steps to create all the other accounts. Your final PPPoE account summary screen should look like this.

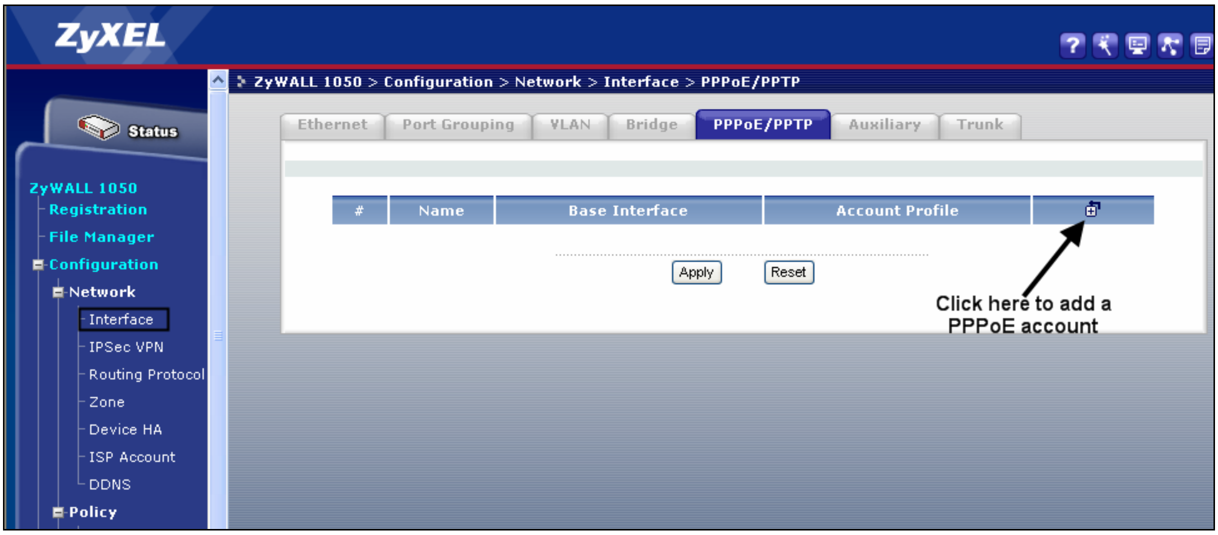


ZyWALL 1050 > Configuration > Network > ISP Account

Configuration

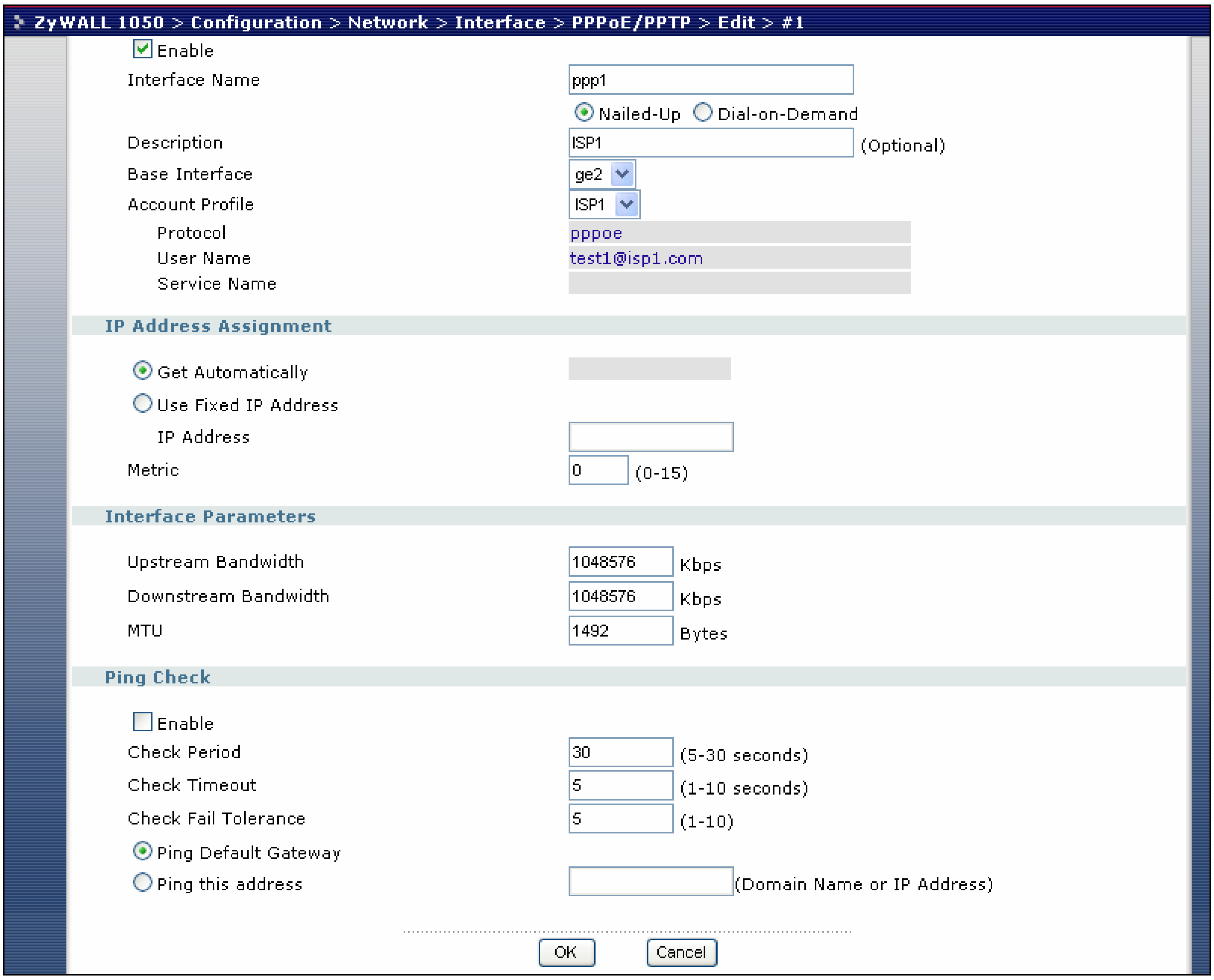
| Profile Name | Protocol | Authentication Type | User Name | |
|---|---|---|---|---|
| ISP1 | pppoe | chap-pap | test1@isp1.com | |
| ISP2 | pppoe | chap-pap | zyxel@cht.com.tw | |
| ISP3 | pppoe | chap-pap | zytw@seed.net.tw | |

4) Now, all the PPPoE accounts are created. Our next task will be creating the PPPoE Interfaces. Go to **Configuration > Network > Interface > PPPoE/PPTP.** Then click the "+" to create a new account.



Click here to add a PPPoE account

5) Your first action is to check the box "Enable" to enable this PPPoE interface, then give the interface a name. It has to be in the format of ppp(0~11). Choose if you want this PPPoE connection to be a forever link up connection or a Dial-on-Demand connection. Based on our scenario, all the PPPoE connections are coming from GE2. Thus, we pick GE2 as our base interface. Pick the account profile that you want to apply for this PPPoE interface. All other remaining settings are either optional or depending on the requirements of your ISP.



ZyWALL 1050 > Configuration > Network > Interface > PPPoE/PPTP > Edit > #1

☑ Enable

| | |
|---|---|
| Interface Name | ppp1 |
| | ● Nailed-Up ○ Dial-on-Demand |
| Description | ISP1 (Optional) |
| Base Interface | ge2 |
| Account Profile | ISP1 |
| Protocol | pppoe |
| User Name | test1@isp1.com |
| Service Name | |

**IP Address Assignment**

| | |
|---|---|
| ● Get Automatically | |
| ○ Use Fixed IP Address | |
| IP Address | |
| Metric | 0 (0-15) |

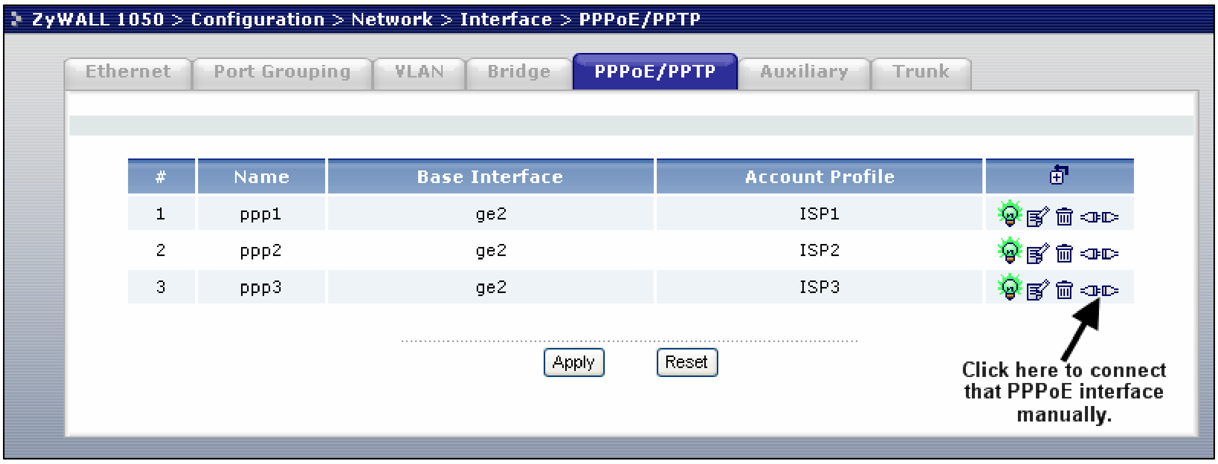
**Interface Parameters**

| | |
|---|---|
| Upstream Bandwidth | 1048576 Kbps |
| Downstream Bandwidth | 1048576 Kbps |
| MTU | 1492 Bytes |

**Ping Check**

| | |
|---|---|
| □ Enable | |
| Check Period | 30 (5-30 seconds) |
| Check Timeout | 5 (1-10 seconds) |
| Check Fail Tolerance | 5 (1-10) |
| ● Ping Default Gateway | |
| ○ Ping this address | (Domain Name or IP Address) |

6) Repeat the above steps to create the other two PPPoE Interfaces. Then you should get a screen looking like this. Also, in a case you want to connect your PPPoE interface manually, click on ⊲⊐⊏⊳ as demonstrated below.



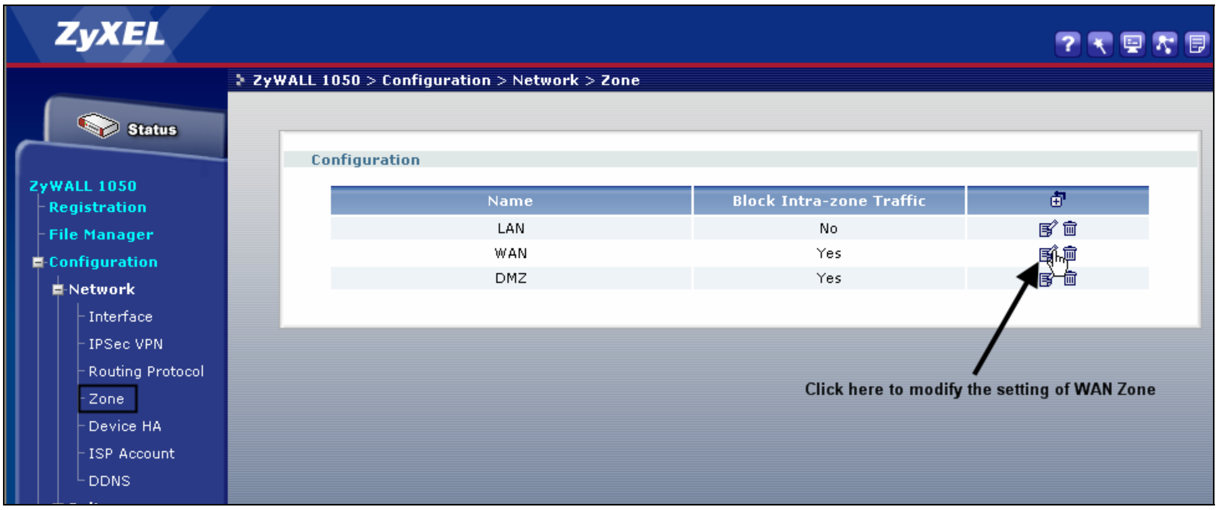
ZyWALL 1050 > Configuration > Network > Interface > PPPoE/PPTP

| # | Name | Base Interface | Account Profile | |
|---|---|---|---|---|
| 1 | ppp1 | ge2 | ISP1 | |
| 2 | ppp2 | ge2 | ISP2 | |
| 3 | ppp3 | ge2 | ISP3 | |

Click here to connect that PPPoE interface manually.

7) Now all the PPPoE interfaces are created. And all of them are desired to be added to the WAN Zone as well. Go to **Configuration** > **Network** > **Zone** to click on the modify icon

of the WAN Zone.



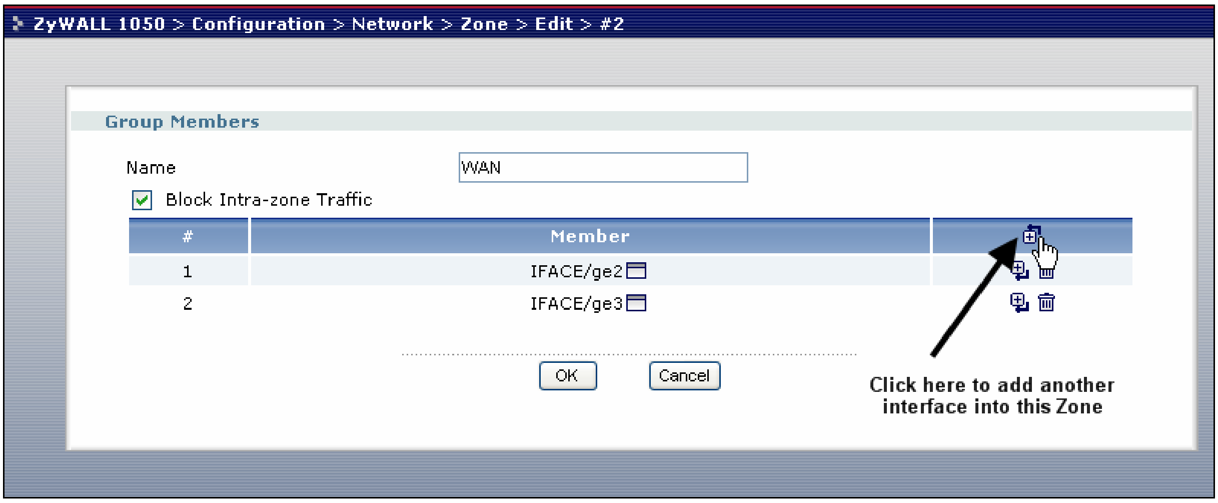
ZyWALL 1050 > Configuration > Network > Zone

Configuration

| Name | Block Intra-zone Traffic | |
|---|---|---|
| LAN | No | |
| WAN | Yes | |
| DMZ | Yes | |

Click here to modify the setting of WAN Zone

8) Click the “+” icon to have a new interface to join this Zone.


ZyWALL 1050 > Configuration > Network > Zone > Edit > #2

Group Members

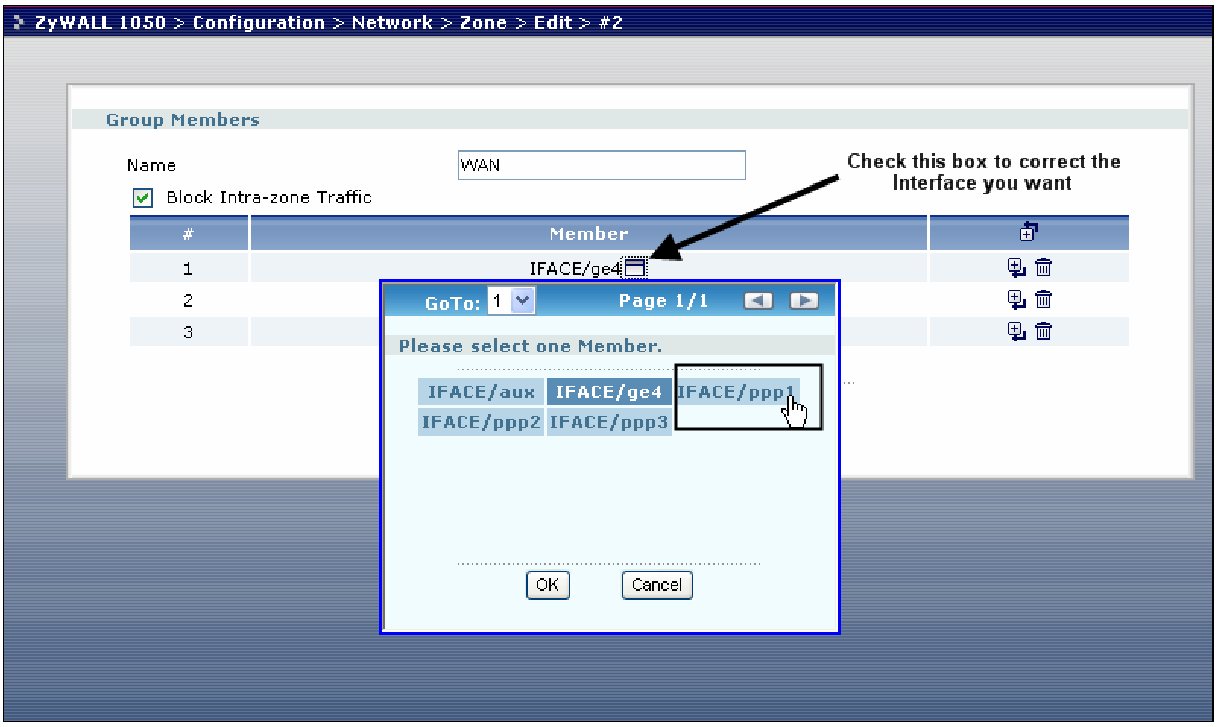
Name: WAN

☑ Block Intra-zone Traffic

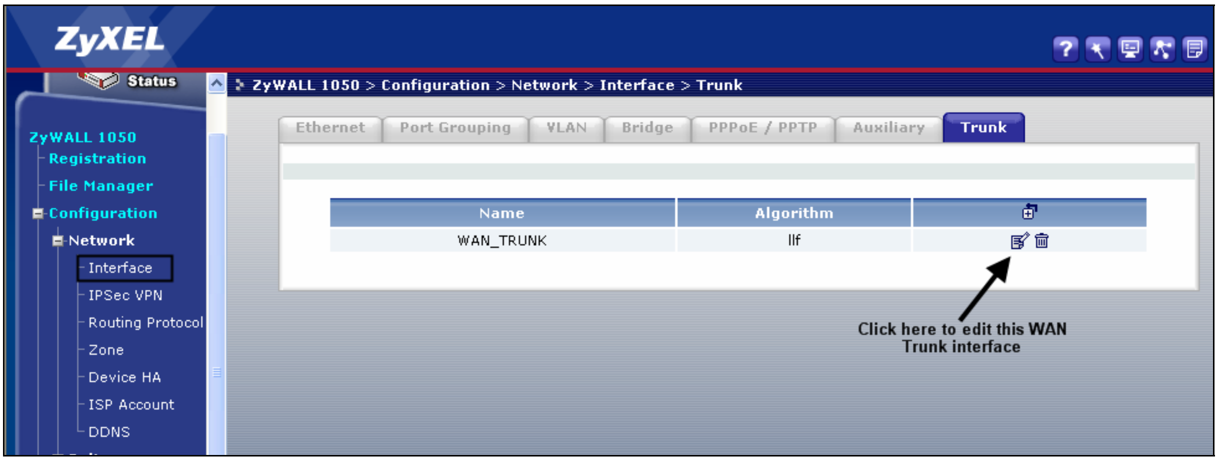
| # | Member | |
|---|---|---|
| 1 | IFACE/ge2 | |
| 2 | IFACE/ge3 | |

Click here to add another interface into this Zone

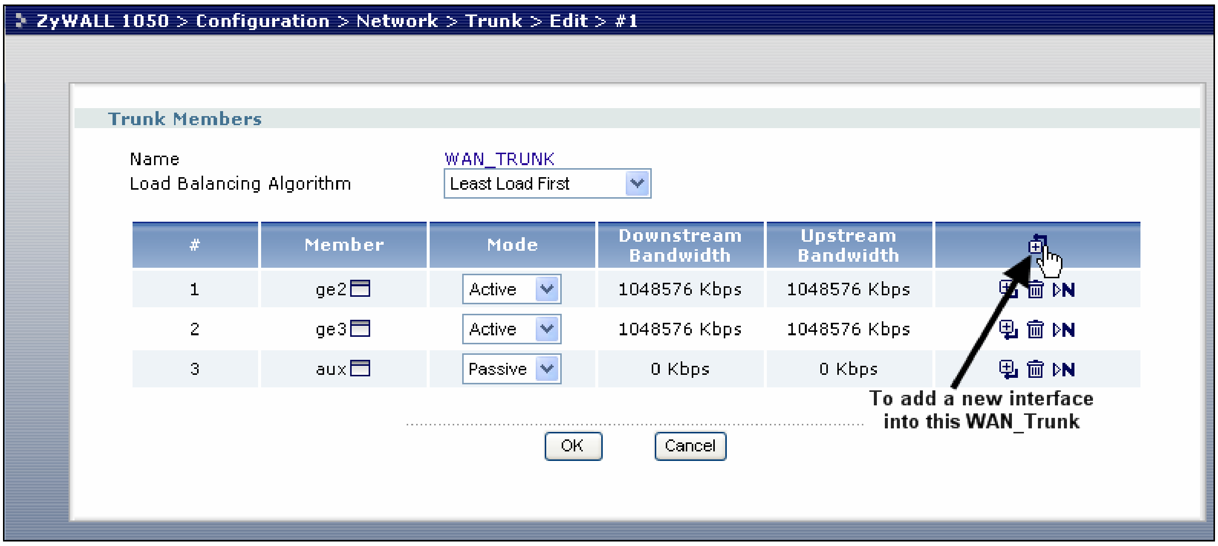
9) Now check the box below to pick PPP1 as the Interface to join the WAN Zone. Repeat the above steps to add PPP2 and PPP3 into the WAN Zone as well.


ZyWALL 1050 > Configuration > Network > Zone > Edit > #2
Group Members
Name
WAN
☑ Block Intra-zone Traffic
#
Member
1
IFACE/ge4
2
3
GoTo: 1
Page 1/1
Please select one Member.
IFACE/aux
IFACE/ge4
IFACE/ppp1
IFACE/ppp2
IFACE/ppp3
OK
Cancel
Check this box to correct the Interface you want

10) Second, we will need to add all three of our PPPoE Interfaces into the WAN Trunk interface. Please go to **Configuration** > **Network** > **Interface** > **Trunk**



11) Click on the “+” icon to add a new interface into this WAN_Trunk interface.



ZyWALL 1050 > Configuration > Network > Trunk > Edit > #1

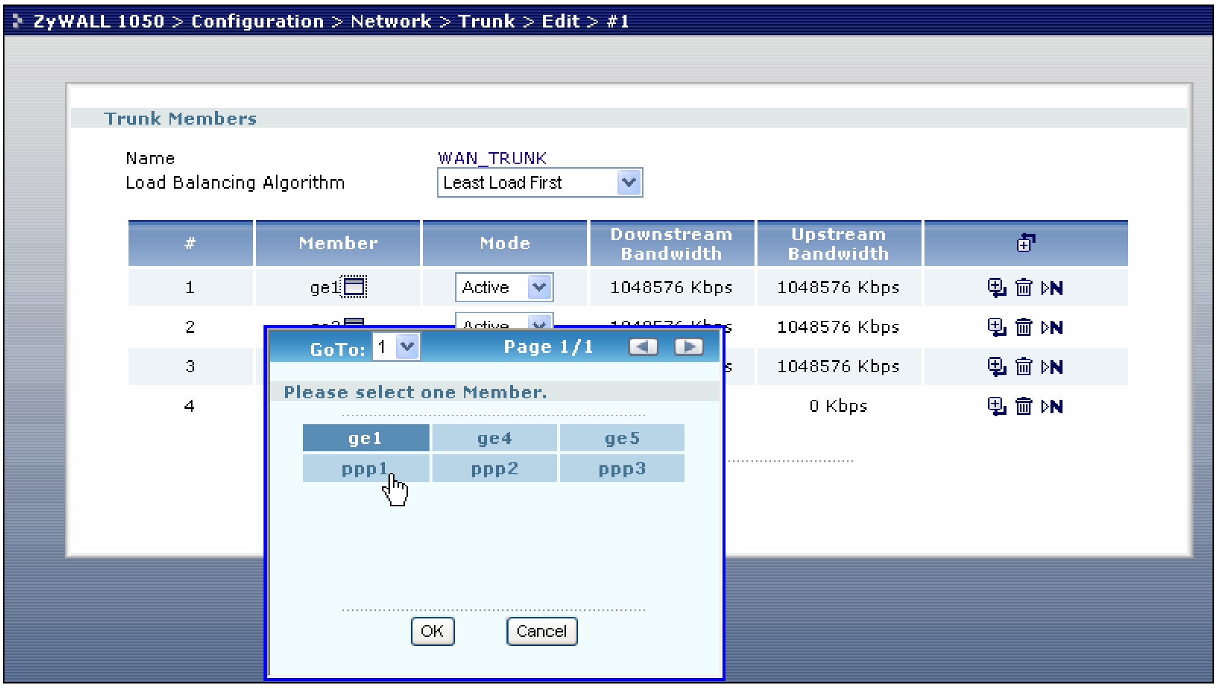
Trunk Members

Name WAN_TRUNK
Load Balancing Algorithm Least Load First

| # | Member | Mode | Downstream Bandwidth | Upstream Bandwidth |
|---|---|---|---|---|
| 1 | ge2 | Active | 1048576 Kbps | 1048576 Kbps |
| 2 | ge3 | Active | 1048576 Kbps | 1048576 Kbps |
| 3 | aux | Passive | 0 Kbps | 0 Kbps |

To add a new interface into this WAN_Trunk

12) Click on the ▭ to pick the right PPPoE interface. Also, for the "Mode" of the Interface, if it is a "nail-up" connection, we can choose Active here; if it is a "dial-on-demand" connection, we can pick "Passive" here. The "Downstream Bandwidth" and the "Upstream Bandwidth" here are the values used for reference of the Load Balancing Algorithm.



ZyWALL 1050 > Configuration > Network > Trunk > Edit > #1

Trunk Members

Name WAN_TRUNK
Load Balancing Algorithm Least Load First

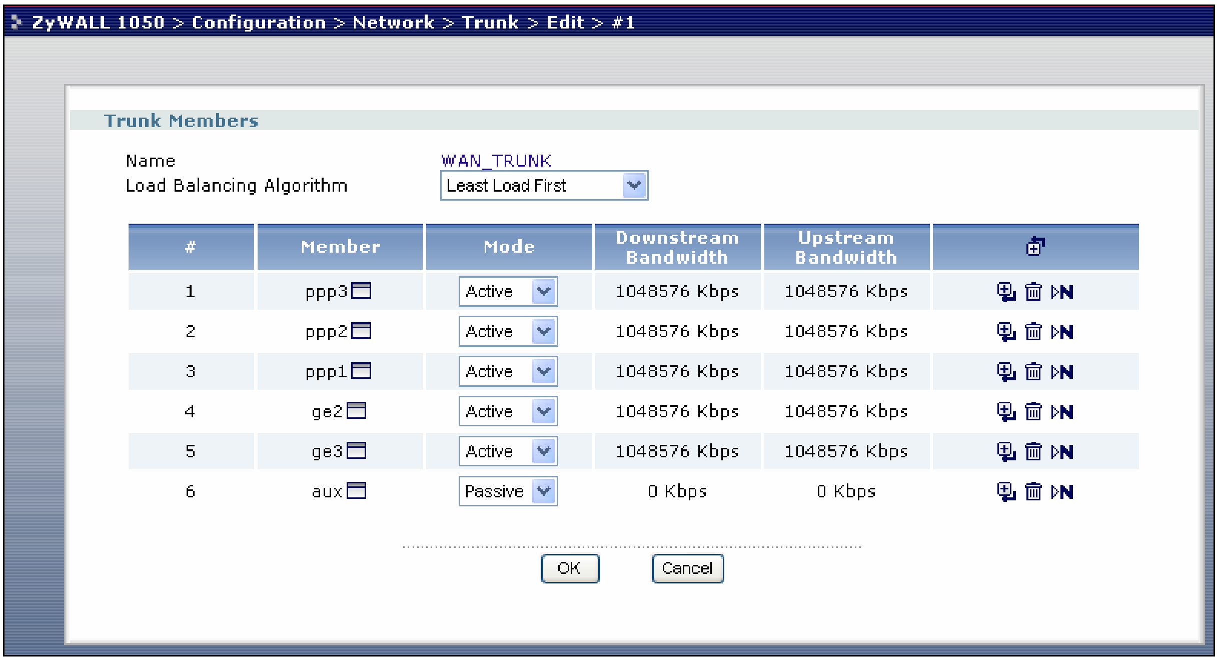
| # | Member | Mode | Downstream Bandwidth | Upstream Bandwidth |
|---|---|---|---|---|
| 1 | ge1 | Active | 1048576 Kbps | 1048576 Kbps |
| 2 | | Active | | 1048576 Kbps |
| 3 | | | | 1048576 Kbps |
| 4 | | | | 0 Kbps |

GoTo: 1 Page 1/1

Please select one Member.

| | | |
|---|---|---|
| ge1 | ge4 | ge5 |
| ppp1 | ppp2 | ppp3 |

13) Repeat the above steps until all three PPPoE interfaces are added into this WAN_Trunk interface. Remove the fixed links on GE2 and/GE3 if you want.



ZyWALL 1050 > Configuration > Network > Trunk > Edit > #1

Trunk Members

Name WAN_TRUNK
Load Balancing Algorithm Least Load First

| # | Member | Mode | Downstream Bandwidth | Upstream Bandwidth |
|---|---|---|---|---|
| 1 | ppp3 | Active | 1048576 Kbps | 1048576 Kbps |
| 2 | ppp2 | Active | 1048576 Kbps | 1048576 Kbps |
| 3 | ppp1 | Active | 1048576 Kbps | 1048576 Kbps |
| 4 | ge2 | Active | 1048576 Kbps | 1048576 Kbps |
| 5 | ge3 | Active | 1048576 Kbps | 1048576 Kbps |
| 6 | aux | Passive | 0 Kbps | 0 Kbps |

## CLI commands to create a PPPoE account

[0] account pppoe ISP1

[1] user test1@isp1.com

[2] password abcdefg

[3] authentication chap-pap

[4] compression no

[5] idle 0

[6] exit

## CLI commands to create a PPPoE interface

[0] interface ppp1

[1] no shutdown

[2] description ISP1

[3] mtu 1492

[4] upstream 1048576

[5] downstream 1048576

```
[6] account ISP1

[7] connectivity nail-up

[8] bind ge2

[9] metric 0

[10] ping-check default-gateway

[11] ping-check default-gateway period 30

[12] ping-check default-gateway timeout 5

[13] ping-check default-gateway fail-tolerance 5

[14] no ping-check activate

[15] exit
```

**CLI commands to add all the PPPoE interfaces into the WAN Zone:**

```
[0] zone WAN

[1] block

[2] no interface ge2

[3] no interface ge3

[4] interface ppp3

[5] interface ppp2

[6] interface ppp1

[7] interface ge2

[8] interface ge3

[9] exit
```

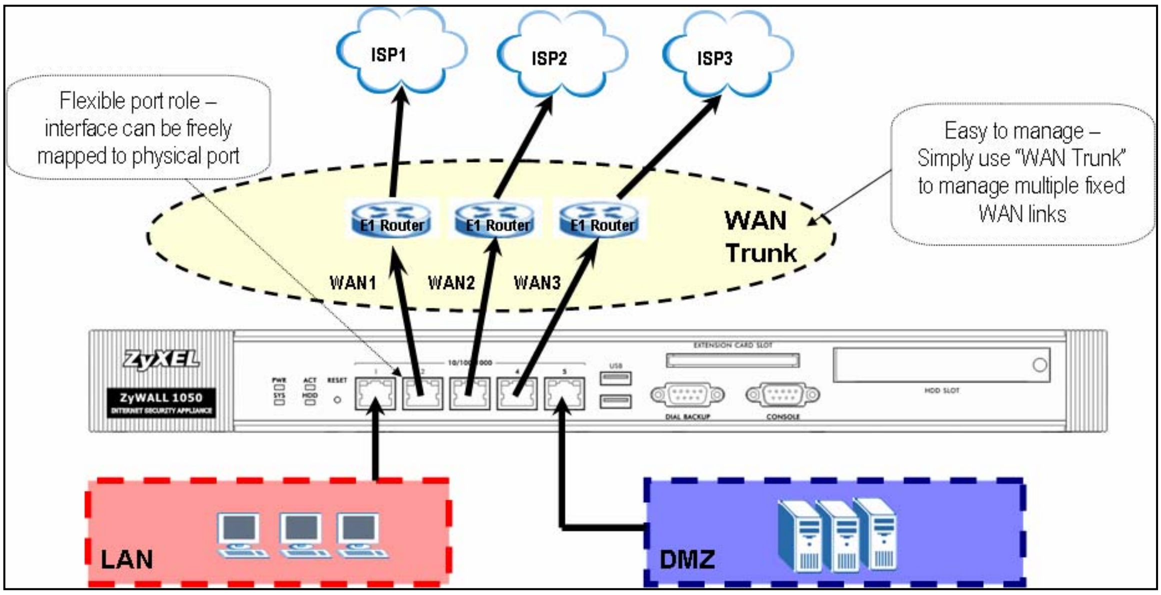
**CLI commands to add those three PPPoE interfaces into the WAN_Trunk interface**

```
[0] interface-group WAN_TRUNK

[1] mode trunk

[2] algorithm llf

[3] no interface ge2
```

```
[4] no interface ge3
[5] no interface aux
[6] interface 1 ppp3
[7] interface 2 ppp2
[8] interface 3 ppp1
[9] interface 4 ge2
[10] interface 5 ge3
[11] interface 6 aux passive
[12] exit
```

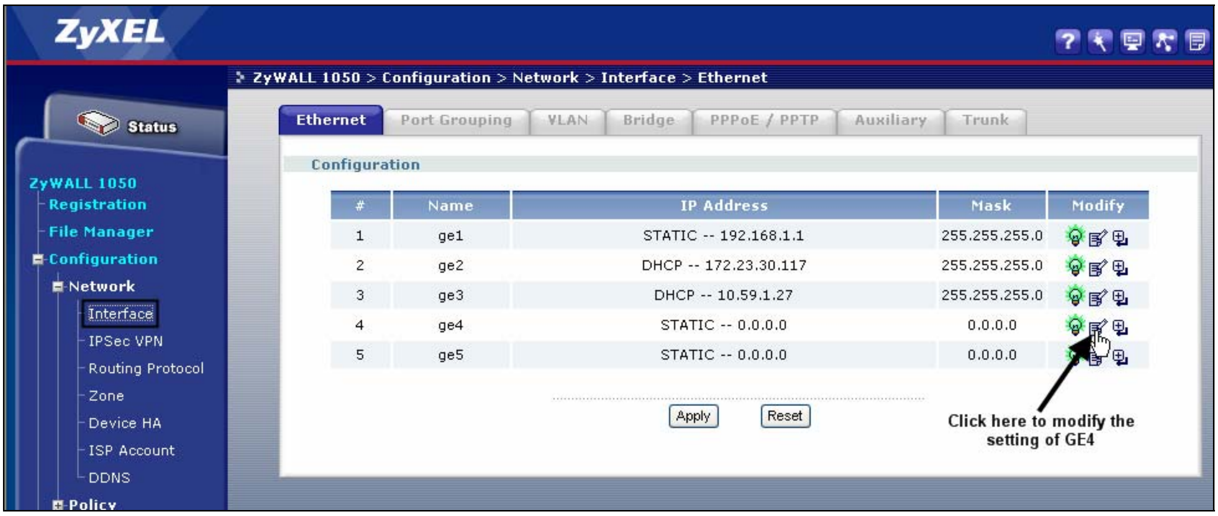
### 3.4.2 Multiple fixed WAN links

Besides multiple PPPoE links, fixed links are also supported on ZyWALL 1050. With ZyWALL 1050, you can have at most 4 fixed links for a WAN. Here is an example with 2 fixed links on GE2, GE3 and GE4.


ISP1
ISP2
ISP3
Flexible port role – interface can be freely mapped to physical port
Easy to manage – Simply use "WAN Trunk" to manage multiple fixed WAN links
E1 Router
E1 Router
E1 Router
WAN Trunk
WAN1
WAN2
WAN3
ZyWALL 1050
LAN
DMZ

Both of the E1 Routers of ISP1 and ISP 2 will have the DHCP Server enabled in this scenario. By default, GE2 and GE3 are set as the DHCP Clients and joined to the WAN_Trunk interface. Therefore, the task is to create another Fixed link with a static IP on GE4 and join it to the WAN_Trunk as well.

1) Login ZyWALL 1050 GUI and go to **Configuration** > **Network** > **Interface** > **Ethernet.** The default setting of GE2 and GE3 is already good for our scenario. Thus, we only need to modify the settings of GE4 in this case.

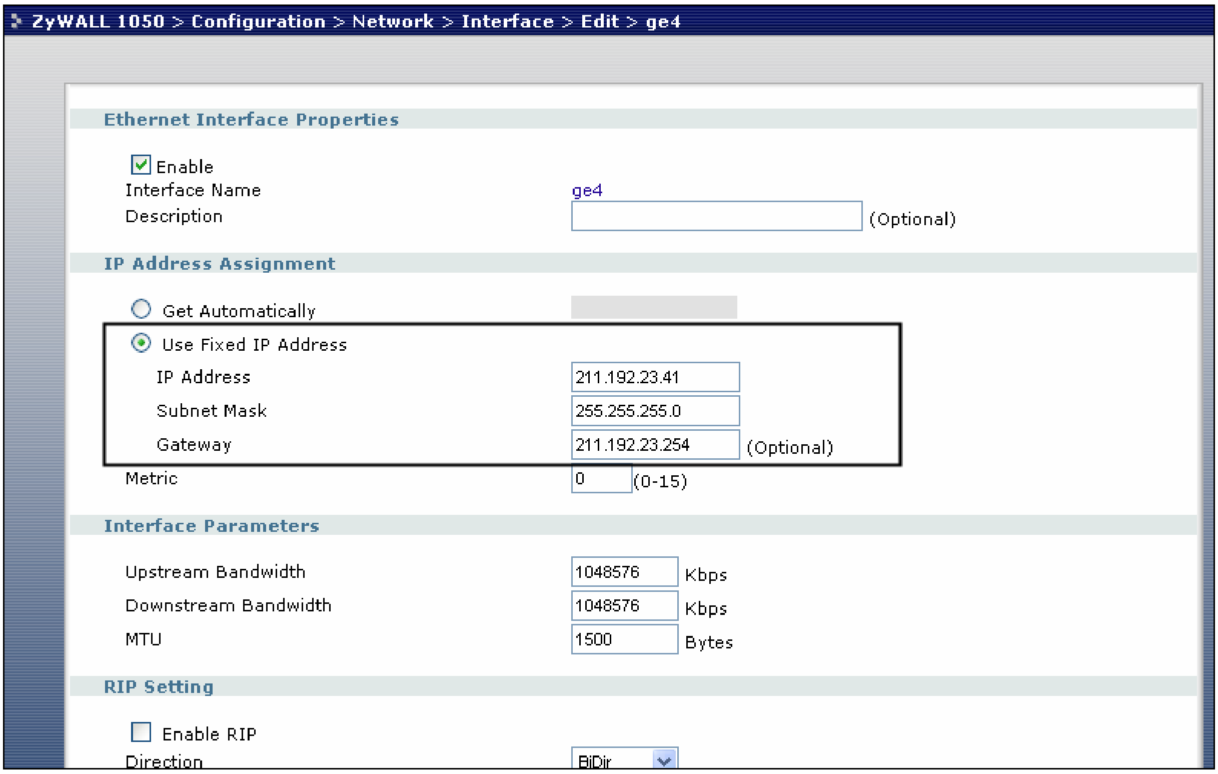


ZyWALL 1050 > Configuration > Network > Interface > Ethernet

| # | Name | IP Address | Mask | Modify |
|---|---|---|---|---|
| 1 | ge1 | STATIC -- 192.168.1.1 | 255.255.255.0 | |
| 2 | ge2 | DHCP -- 172.23.30.117 | 255.255.255.0 | |
| 3 | ge3 | DHCP -- 10.59.1.27 | 255.255.255.0 | |
| 4 | ge4 | STATIC -- 0.0.0.0 | 0.0.0.0 | |
| 5 | ge5 | STATIC -- 0.0.0.0 | 0.0.0.0 | |

Click here to modify the setting of GE4

2) Since we are going to run static IP on GE4, we will file the IP information into GE4 manually. The bandwidth parameters here do not necessarily need to be modified.



ZyWALL 1050 > Configuration > Network > Interface > Edit > ge4

Ethernet Interface Properties

☑ Enable
Interface Name: ge4
Description: (Optional)

IP Address Assignment

○ Get Automatically
● Use Fixed IP Address
IP Address: 211.192.23.41
Subnet Mask: 255.255.255.0
Gateway: 211.192.23.254 (Optional)
Metric: 0 (0-15)

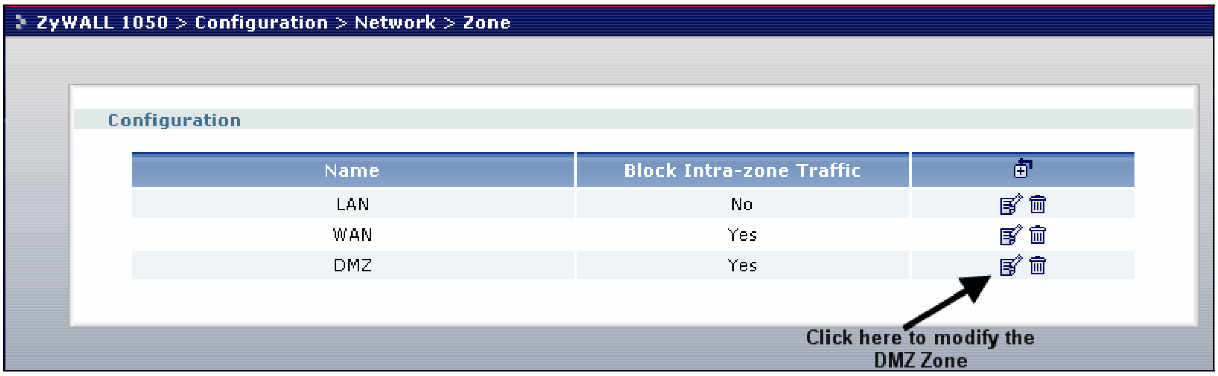
Interface Parameters

Upstream Bandwidth: 1048576 Kbps
Downstream Bandwidth: 1048576 Kbps
MTU: 1500 Bytes

RIP Setting

□ Enable RIP
Direction: BiDir

3) Now since GE4 is in the DMZ Zone by default, we will need to release it for us to use. Go to **Configuration** > **Network** > **Zone** and click on the modify icon of DMZ.



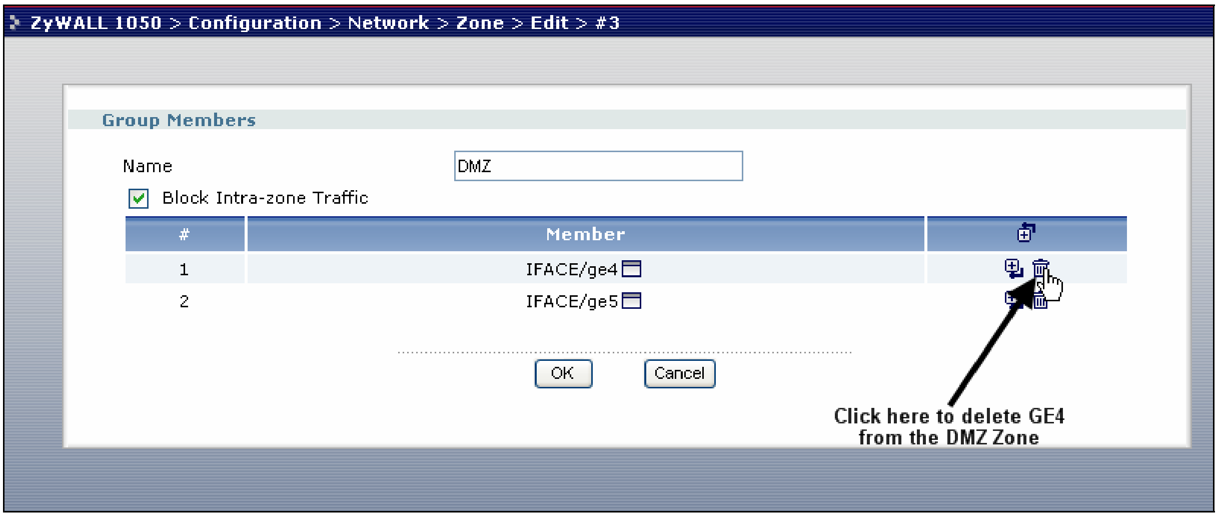
ZyWALL 1050 > Configuration > Network > Zone

Configuration

| Name | Block Intra-zone Traffic | |
|---|---|---|
| LAN | No | |
| WAN | Yes | |
| DMZ | Yes | |

Click here to modify the DMZ Zone

4) Delete GE4 from the DMZ Zone by clicking the remove icon.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #3

Group Members

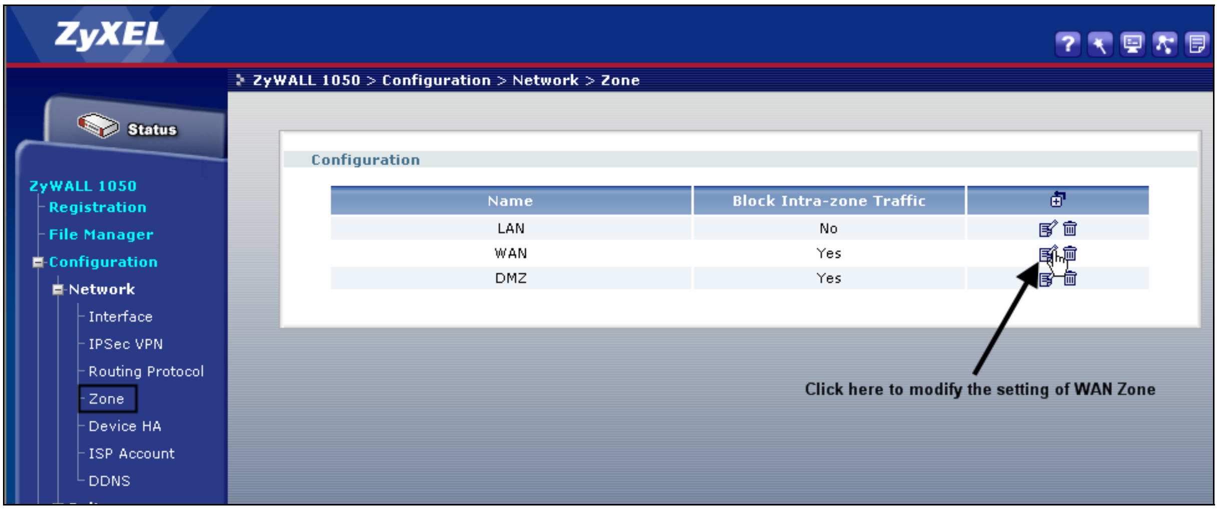
Name: DMZ

☑ Block Intra-zone Traffic

| # | Member | |
|---|---|---|
| 1 | IFACE/ge4 | |
| 2 | IFACE/ge5 | |

Click here to delete GE4 from the DMZ Zone

5) Next, we will need GE4 to join the WAN Zone in order for us to be able to apply a single WAN policy on ZyWALL 1050. Go to **Configuration** > **Network** > **Zone** and click on the modify icon of WAN Zone.



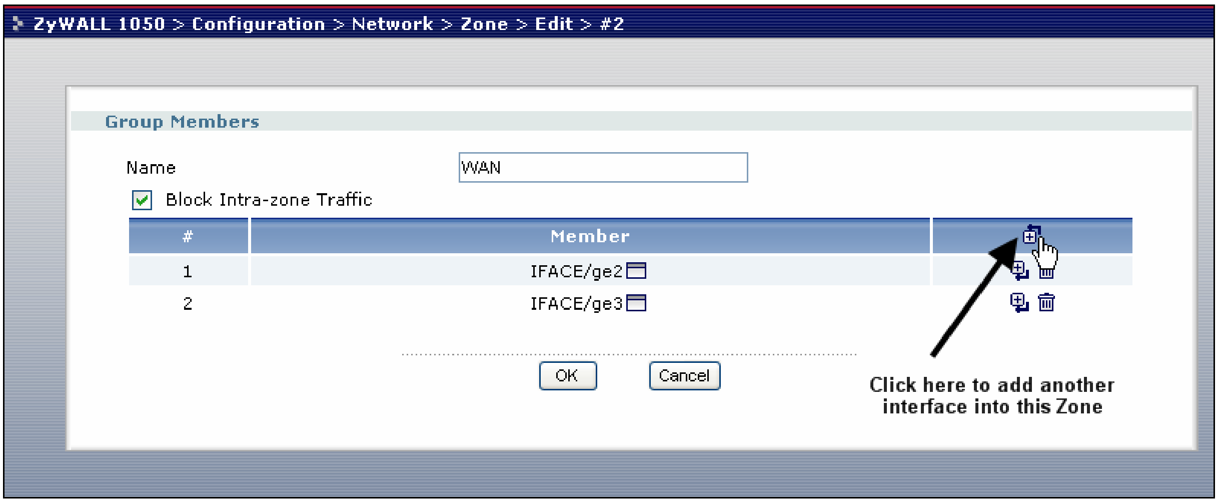
ZyWALL 1050 > Configuration > Network > Zone

Configuration

| Name | Block Intra-zone Traffic | |
|---|---|---|
| LAN | No | |
| WAN | Yes | |
| DMZ | Yes | |

Click here to modify the setting of WAN Zone

6) Click the "+" icon again to make the new interface to join this Zone.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #2

Group Members

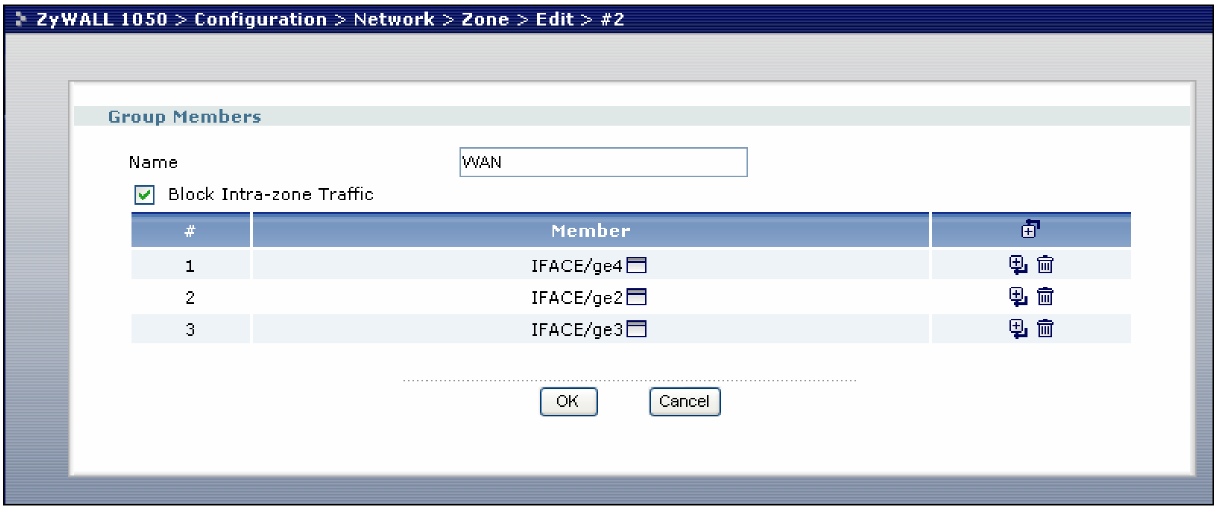
Name: WAN

☑ Block Intra-zone Traffic

| # | Member | |
|---|---|---|
| 1 | IFACE/ge2 | |
| 2 | IFACE/ge3 | |

Click here to add another interface into this Zone

7) Since GE4 is the only free interface here, it will be selected automatically.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #2

Group Members

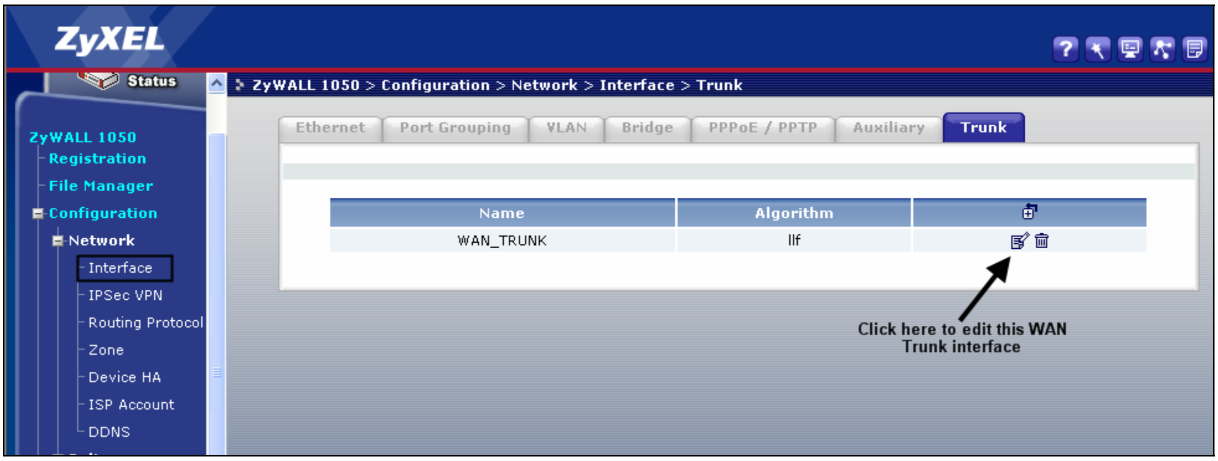
Name: WAN

☑ Block Intra-zone Traffic

| # | Member |
|---|---|
| 1 | IFACE/ge4 |
| 2 | IFACE/ge2 |
| 3 | IFACE/ge3 |

OK Cancel

8) After the Zone, we need to add GE4 into the WAN_Trunk Interface as well. Go to **Configuration** > **Network** > **Interface** > **Trunk** and click on ✎ to modify the settings of the WAN_Trunk.

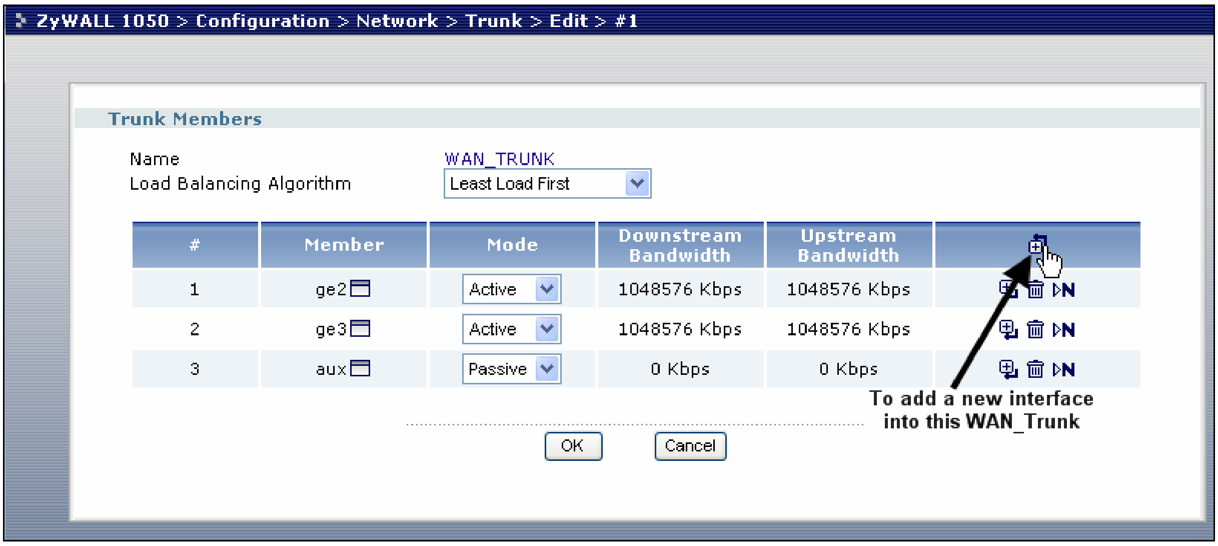


ZyWALL 1050 > Configuration > Network > Interface > Trunk

| Name | Algorithm |
|---|---|
| WAN_TRUNK | llf |

Click here to edit this WAN Trunk interface

9) Click on the "+" icon to add a new interface into this WAN_Trunk interface.



ZyWALL 1050 > Configuration > Network > Trunk > Edit > #1

Trunk Members

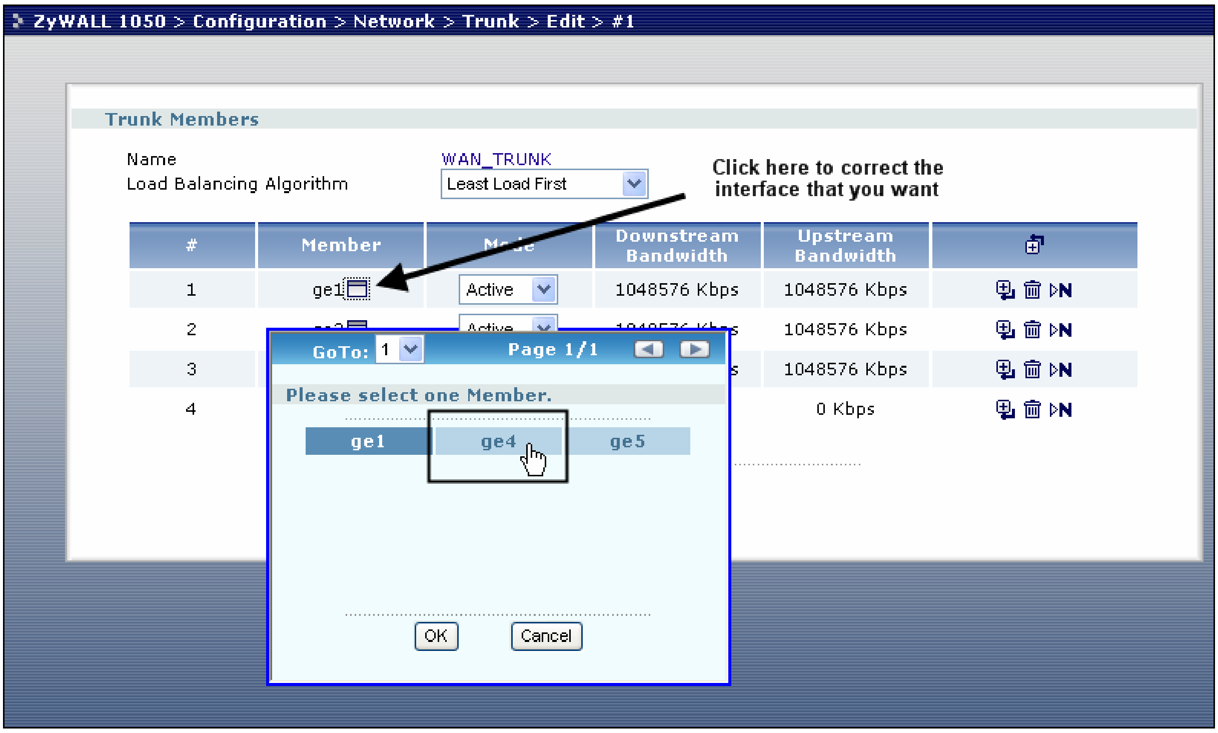
Name: WAN_TRUNK

Load Balancing Algorithm: Least Load First

| # | Member | Mode | Downstream Bandwidth | Upstream Bandwidth | |
|---|---|---|---|---|---|
| 1 | ge2 | Active | 1048576 Kbps | 1048576 Kbps | |
| 2 | ge3 | Active | 1048576 Kbps | 1048576 Kbps | |
| 3 | aux | Passive | 0 Kbps | 0 Kbps | |

To add a new interface into this WAN_Trunk

10) Click the box below to switch the interface from GE1 to GE4. Click OK and to complete the setup of this scenario.



ZyWALL 1050 > Configuration > Network > Trunk > Edit > #1

Trunk Members

Name: WAN_TRUNK

Load Balancing Algorithm: Least Load First

Click here to correct the interface that you want

| # | Member | Mode | Downstream Bandwidth | Upstream Bandwidth | |
|---|---|---|---|---|---|
| 1 | ge1 | Active | 1048576 Kbps | 1048576 Kbps | |
| 2 | | Active | | 1048576 Kbps | |
| 3 | | | | 1048576 Kbps | |
| 4 | | | | 0 Kbps | |

GoTo: 1 Page 1/1

Please select one Member.

## CLI commands to configure the IP information on GE4:

```
[0] interface ge4
```

```
[1] ip address 211.192.23.41 255.255.255.0
[2] ip gateway 211.192.23.254 metric 0
[3] ping-check default-gateway
[4] ping-check default-gateway period 30
[5] ping-check default-gateway timeout 5
[6] ping-check default-gateway fail-tolerance 5
[7] no ping-check activate
[8] exit
[9] router rip
[10] exit
[11] router ospf
[12] exit
```

**CLI commands to remove GE4 from the DMZ Zone:**

```
[0] zone DMZ
[1] block
[2] no interface ge4
[3] no interface ge5
[4] interface ge5
[5] exit
```

**CLI commands to join GE4 to the WAN Zone:**

```
[0] zone WAN
[1] block
[2] no interface ge2
[3] no interface ge3
[4] interface ge4
[5] interface ge2
```

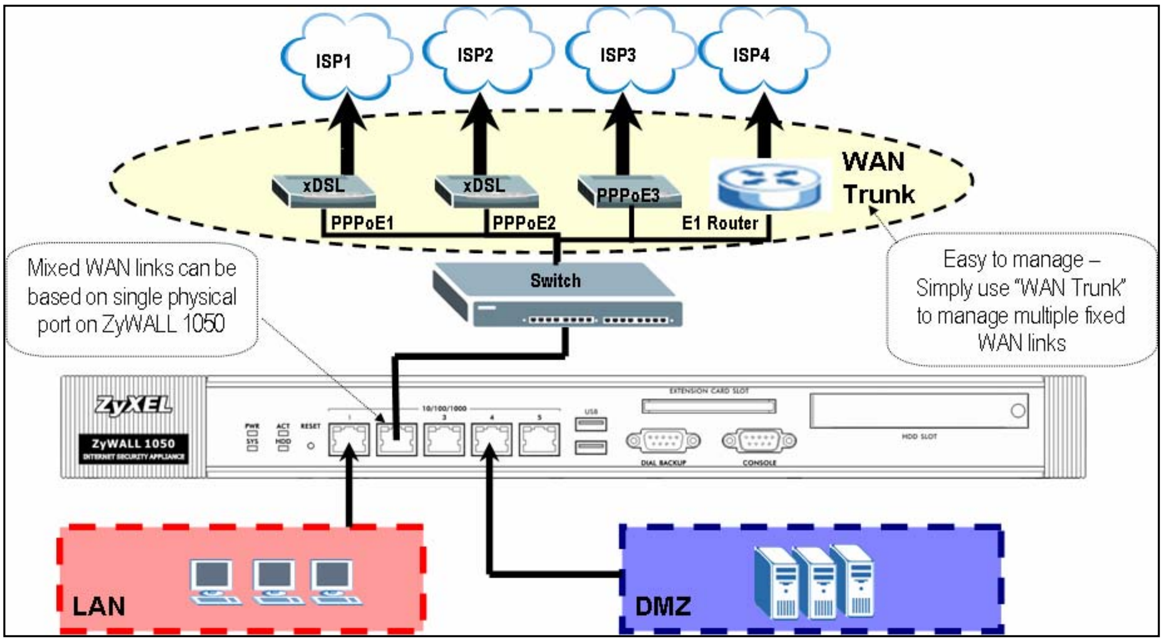
```
[6] interface ge3
[7] exit
```

**CLI commands to join GE4 to the WAN_Trunk:**

```
[0] interface-group WAN_TRUNK
[1] mode trunk
[2] algorithm llf
[3] no interface ge2
[4] no interface ge3
[5] no interface aux
[6] interface 1 ge4
[7] interface 2 ge2
[8] interface 3 ge3
[9] interface 4 aux passive
[10] exit
```

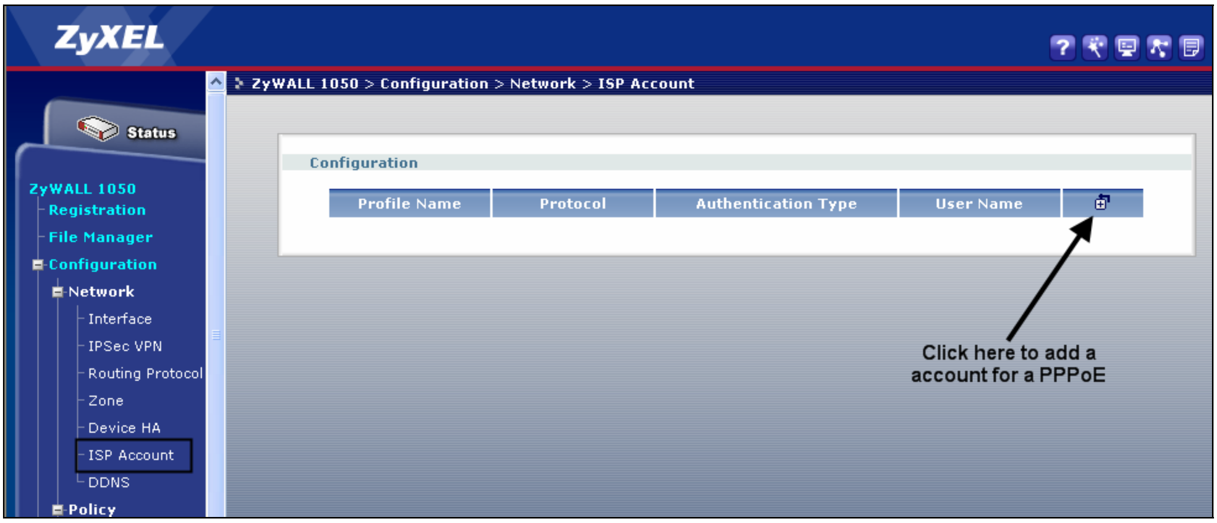
### 3.4.3 Mixed types of WAN links

Mixed types of WAN links are also supported by ZyWALL 1050. You can have multiple PPPoE links together with a fixed link through one single physical port. Besides, you can have multiple PPPoE links and multiple fixed links put together, however, it will occupy more physical ports on the ZyWALL 1050. Here is an example.


ISP1
ISP2
ISP3
ISP4
WAN Trunk
xDSL
xDSL
PPPoE3
PPPoE1
PPPoE2
E1 Router
Switch
Mixed WAN links can be based on single physical port on ZyWALL 1050
Easy to manage – Simply use "WAN Trunk" to manage multiple fixed WAN links
ZyXEL
ZyWALL 1050
LAN
DMZ

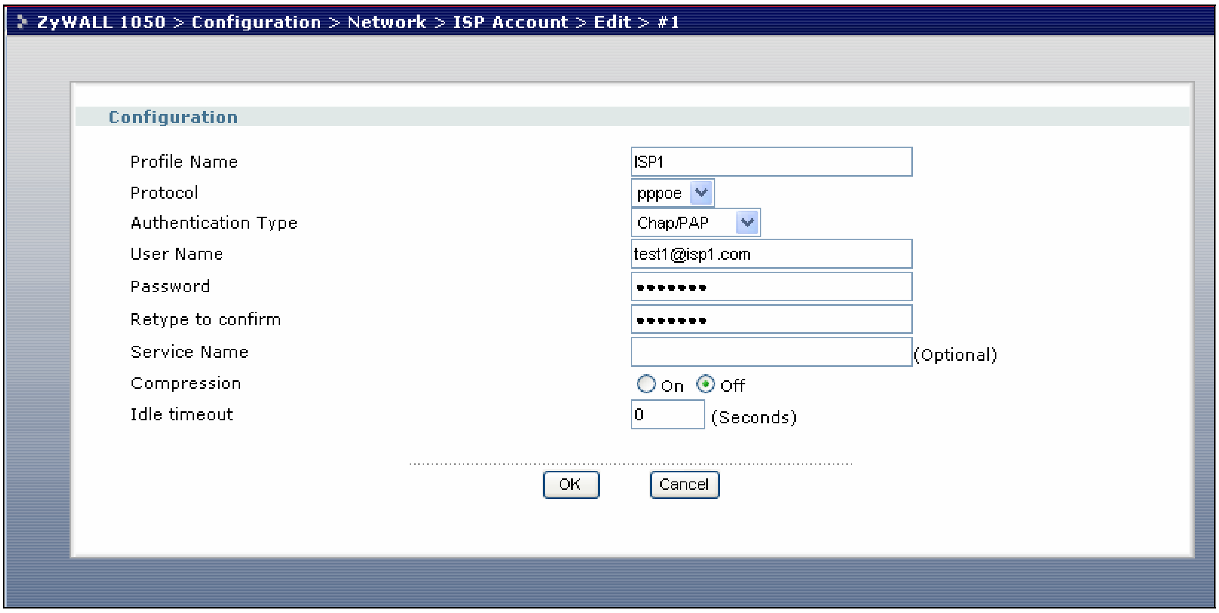
First of all, we are going to configure three PPPoE links on ZyWALL 1050. Also, we will assign GE2 to connect with the enabled DHCP Client as a Fix link, since DHCP Server is enabled on the E1 Router.

1) Login the ZyWALL 1050 GUI and go to **Configuration** > **Network** > **ISP Account.** Then click on "+" to create a new account for a PPPoE connection.



Click here to add a account for a PPPoE

2 On this screen, you can set a name for this profile. Select the protocol as PPPoE. Please set the Idle timeout to 0 if you do not want this link to be a subject to timeout. All other parameters including the username and password should be based on your ISP's requirements. Finally click "OK" to add this account.

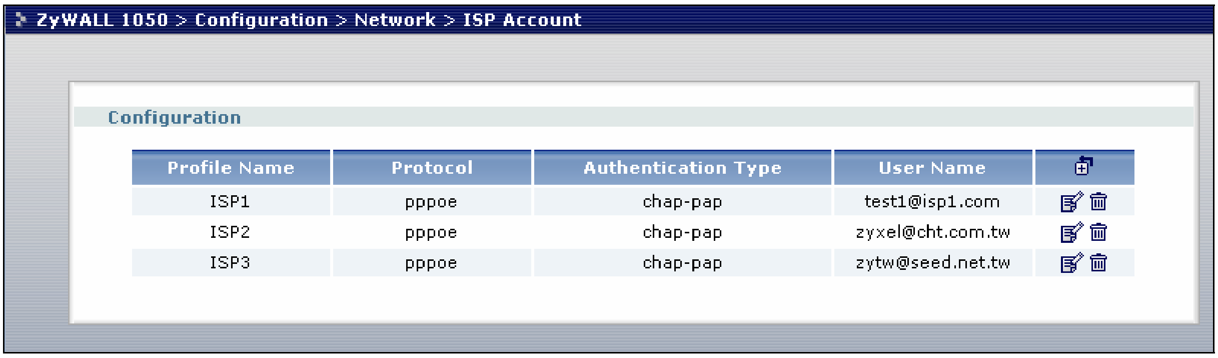


ZyWALL 1050 > Configuration > Network > ISP Account > Edit > #1

Configuration

| | |
|---|---|
| Profile Name | ISP1 |
| Protocol | pppoe |
| Authentication Type | Chap/PAP |
| User Name | test1@isp1.com |
| Password | ••••••• |
| Retype to confirm | ••••••• |
| Service Name | (Optional) |
| Compression | ○ On ● Off |
| Idle timeout | 0 (Seconds) |

3) Since we have three PPPoE links in our scenario, you will need two additional PPPoE accounts here as well. Repeat the above steps to create all the other accounts. Your final PPPoE account summary screen should look like this.

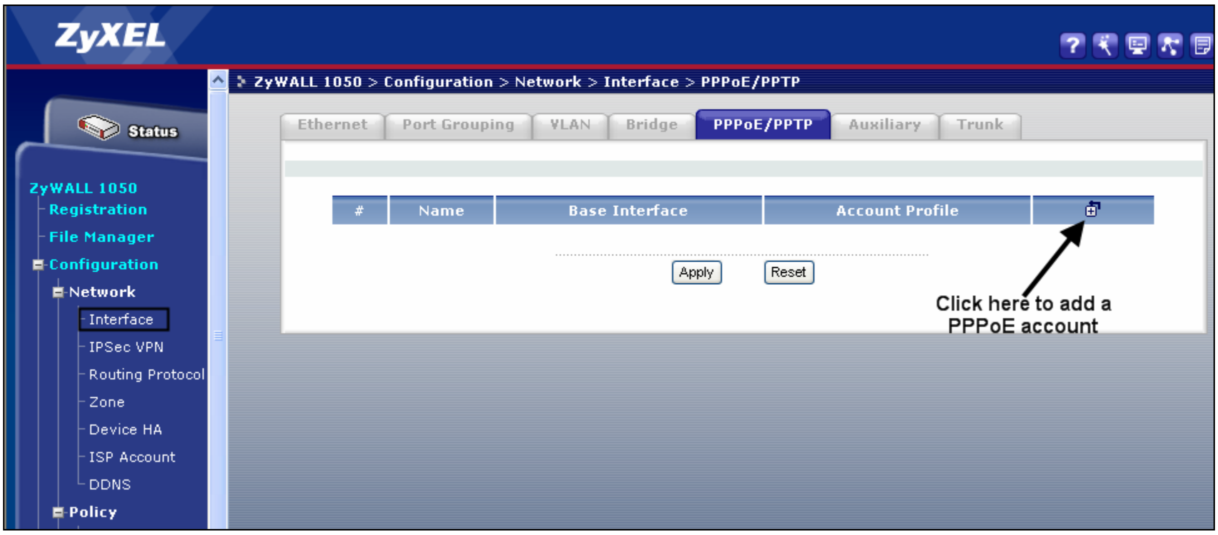


ZyWALL 1050 > Configuration > Network > ISP Account

Configuration

| Profile Name | Protocol | Authentication Type | User Name | |
|---|---|---|---|---|
| ISP1 | pppoe | chap-pap | test1@isp1.com | |
| ISP2 | pppoe | chap-pap | zyxel@cht.com.tw | |
| ISP3 | pppoe | chap-pap | zytw@seed.net.tw | |

4) Now, all the PPPoE accounts are created. Our next task will be creating the PPPoE Interfaces. Go to **Configuration > Network > Interface > PPPoE/PPTP.** Then click the "+" to create a new account.

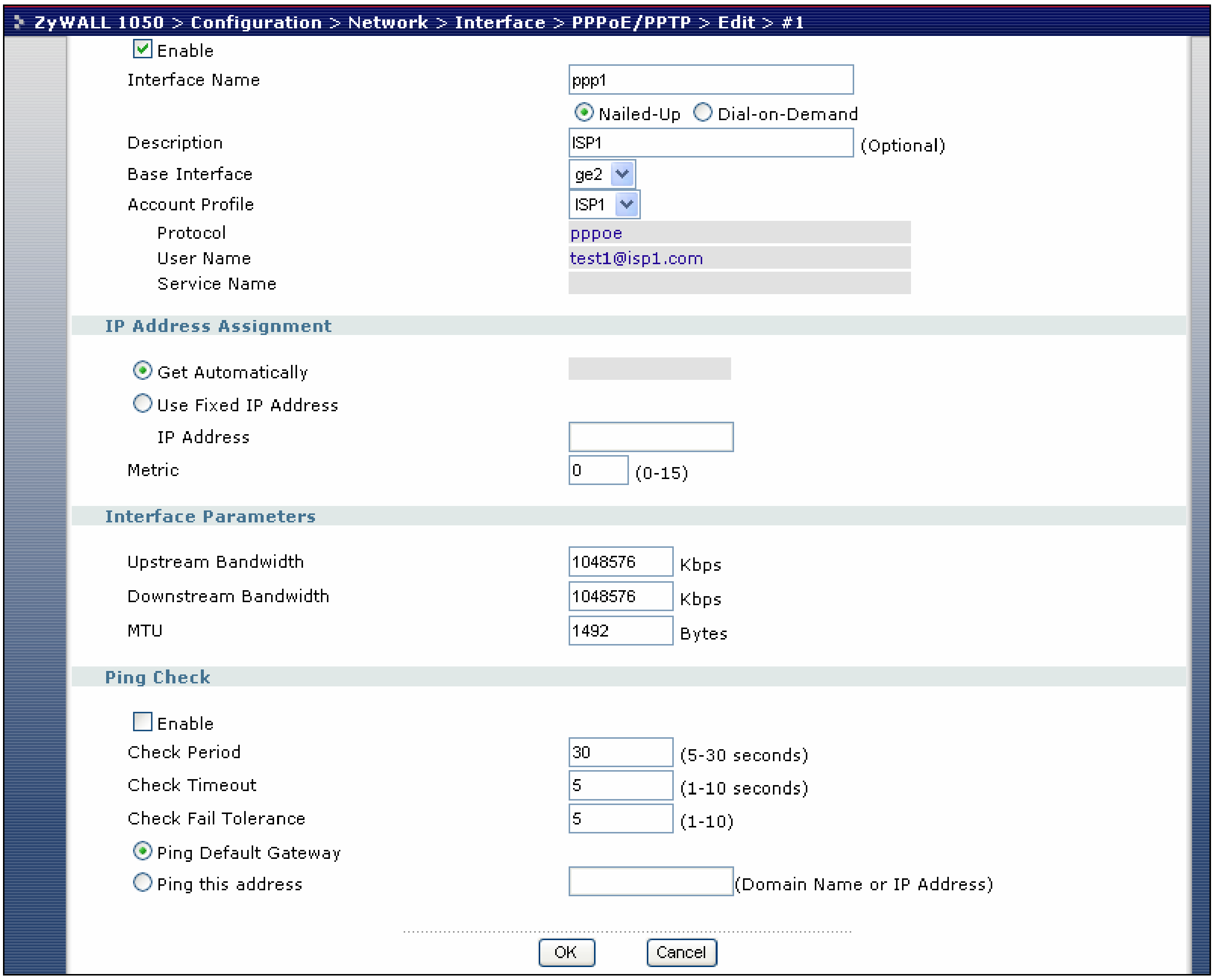


ZyWALL 1050 > Configuration > Network > Interface > PPPoE/PPTP

| # | Name | Base Interface | Account Profile | |
|---|---|---|---|---|

Click here to add a PPPoE account

5) Check the box "Enable" to enable this PPPoE interface, then give the interface a name. The name has to be in the format of ppp(0~11). Choose if you want this PPPoE connection to be a forever link up connection or a Dial-on-Demand connection. According to our scenario, all the PPPoE connections are coming from GE2. Thus, we pick GE2 as our base interface. Pick the account profile that you want to apply for this PPPoE interface; all other remaining settings are either optional or depending on the requirements of your ISP.



ZyWALL 1050 > Configuration > Network > Interface > PPPoE/PPTP > Edit > #1

☑ Enable

| | |
|---|---|
| Interface Name | ppp1 |
| | ● Nailed-Up ○ Dial-on-Demand |
| Description | ISP1 (Optional) |
| Base Interface | ge2 |
| Account Profile | ISP1 |
| Protocol | pppoe |
| User Name | test1@isp1.com |
| Service Name | |

**IP Address Assignment**

| | |
|---|---|
| ● Get Automatically | |
| ○ Use Fixed IP Address | |
| IP Address | |
| Metric | 0 (0-15) |

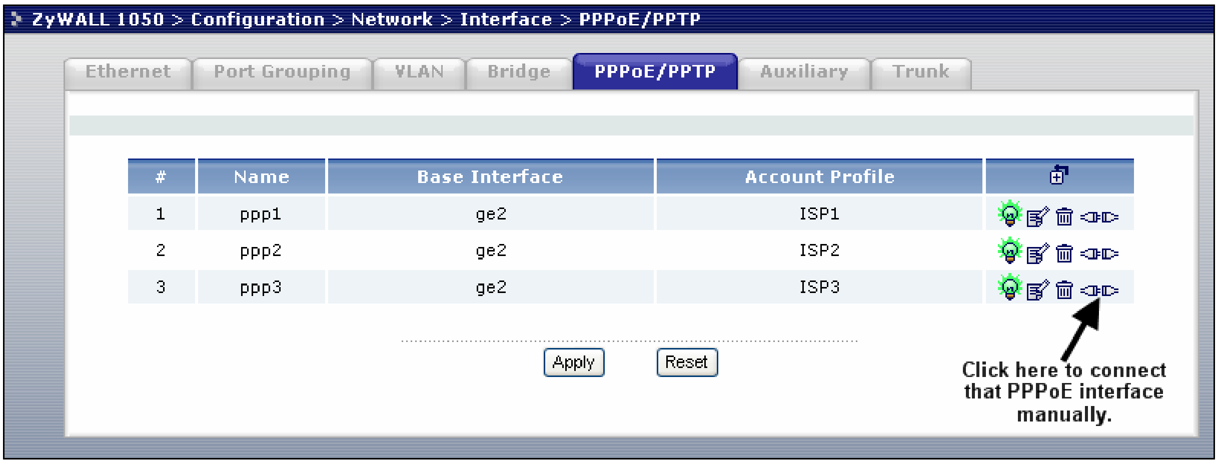
**Interface Parameters**

| | |
|---|---|
| Upstream Bandwidth | 1048576 Kbps |
| Downstream Bandwidth | 1048576 Kbps |
| MTU | 1492 Bytes |

**Ping Check**

| | |
|---|---|
| □ Enable | |
| Check Period | 30 (5-30 seconds) |
| Check Timeout | 5 (1-10 seconds) |
| Check Fail Tolerance | 5 (1-10) |
| ● Ping Default Gateway | |
| ○ Ping this address | (Domain Name or IP Address) |

6) Repeat the above steps to create the other two PPPoE Interfaces. Then you should get a screen that looks like this. If you want to connect your PPPoE interface manually, click on the ⊲⊐⊏⊳ icon below.

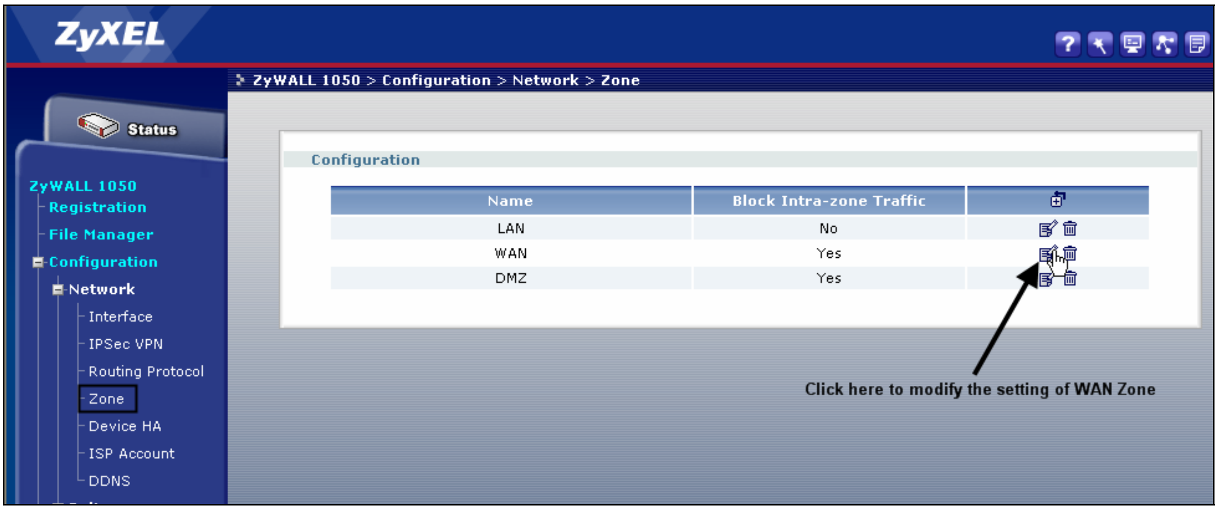


ZyWALL 1050 > Configuration > Network > Interface > PPPoE/PPTP

| # | Name | Base Interface | Account Profile | |
|---|---|---|---|---|
| 1 | ppp1 | ge2 | ISP1 | |
| 2 | ppp2 | ge2 | ISP2 | |
| 3 | ppp3 | ge2 | ISP3 | |

Click here to connect that PPPoE interface manually.

7) Now all the PPPoE interfaces are created. But all of need to be added to the WAN Zone too. Go to **Configuration** > **Network** > **Zone** to click the modify icon of the WAN Zone.



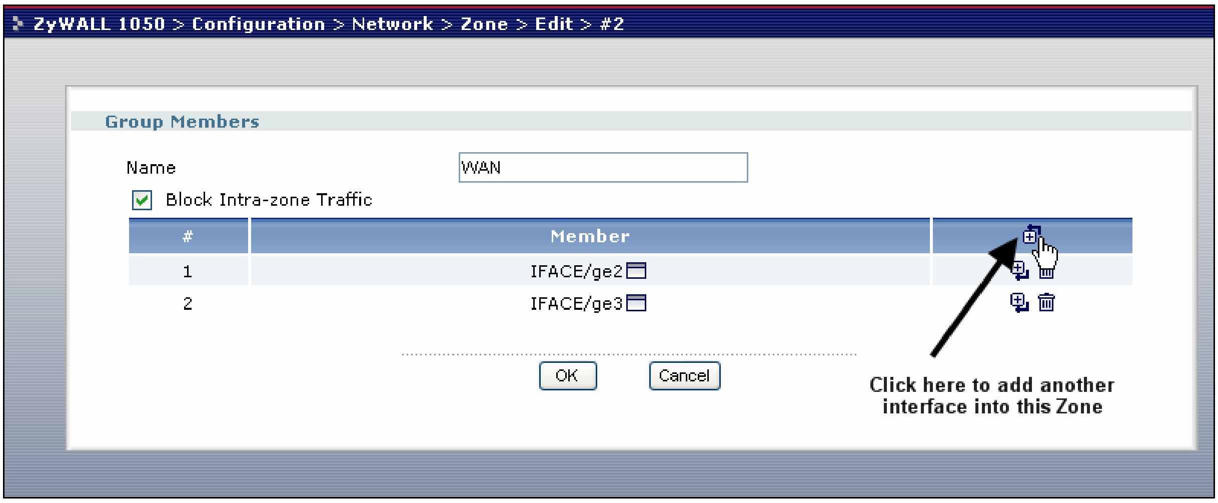
ZyWALL 1050 > Configuration > Network > Zone

Configuration

| Name | Block Intra-zone Traffic | |
|---|---|---|
| LAN | No | |
| WAN | Yes | |
| DMZ | Yes | |

Click here to modify the setting of WAN Zone

8) Click the “+” icon to make a new interface join this Zone.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #2

Group Members

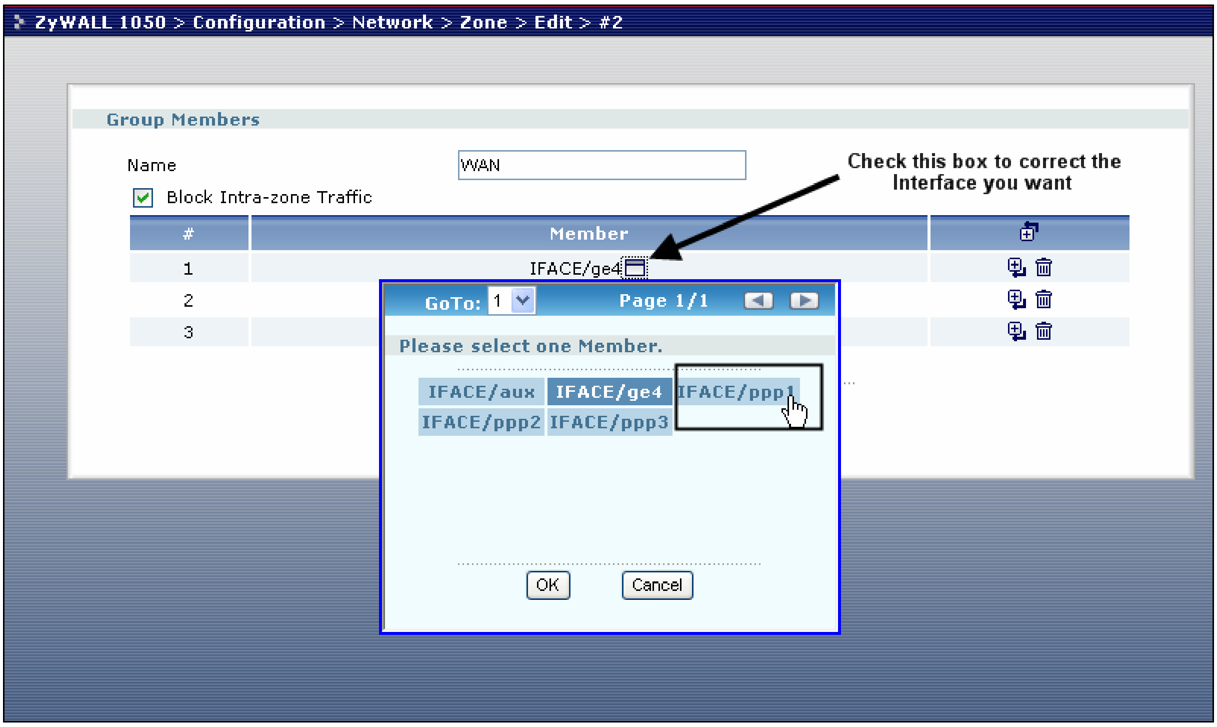
Name: WAN

☑ Block Intra-zone Traffic

| # | Member | |
|---|---|---|
| 1 | IFACE/ge2 | |
| 2 | IFACE/ge3 | |

Click here to add another interface into this Zone

9) Now check the box below to pick PPP1 as the Interface to join the WAN Zone. Repeat the above steps to add PPP2 and PPP3 into the WAN Zone as well.



ZyWALL 1050 > Configuration > Network > Zone > Edit > #2

Group Members

Name: WAN

☑ Block Intra-zone Traffic

| # | Member |
|---|---|
| 1 | IFACE/ge4 |
| 2 | |
| 3 | |

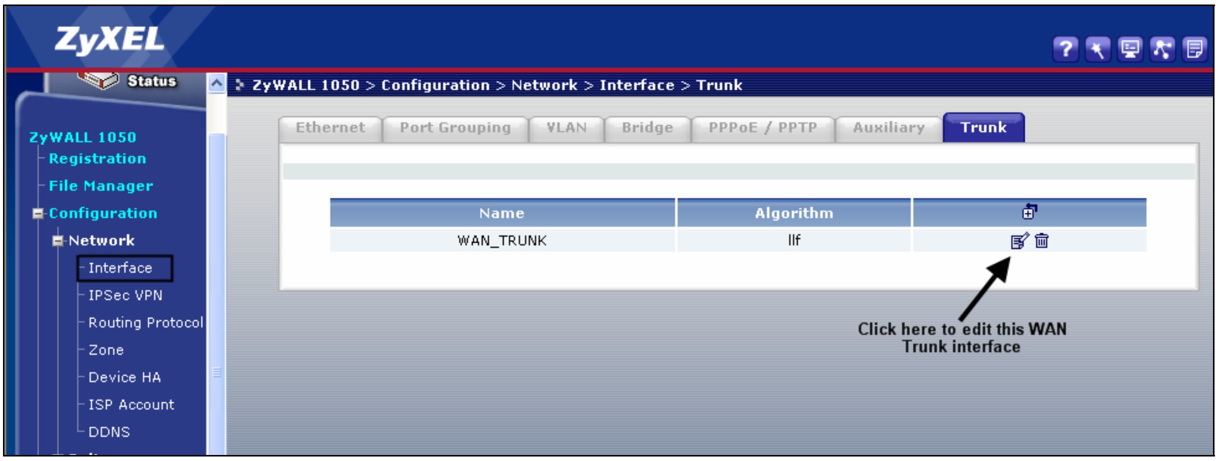
GoTo: 1 Page 1/1

Please select one Member.

| | | |
|---|---|---|
| IFACE/aux | IFACE/ge4 | IFACE/ppp1 |
| IFACE/ppp2 | IFACE/ppp3 | |

Check this box to correct the Interface you want

10) Second, we will need to add all three of our PPPoE Interfaces into the WAN Trunk interface. Please go to **Configuration** > **Network** > **Interface** > **Trunk**

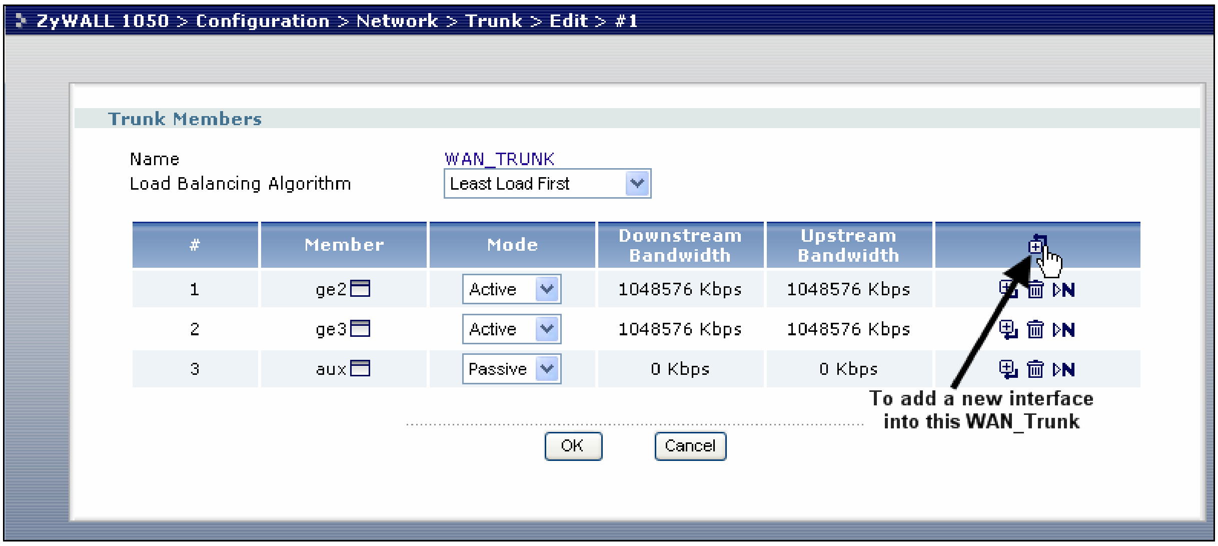


ZyWALL 1050 > Configuration > Network > Interface > Trunk

| Name | Algorithm |
|---|---|
| WAN_TRUNK | llf |

Click here to edit this WAN Trunk interface

11) Click on the "+" icon to add a new interface into this WAN_Trunk interface.



ZyWALL 1050 > Configuration > Network > Trunk > Edit > #1

Trunk Members

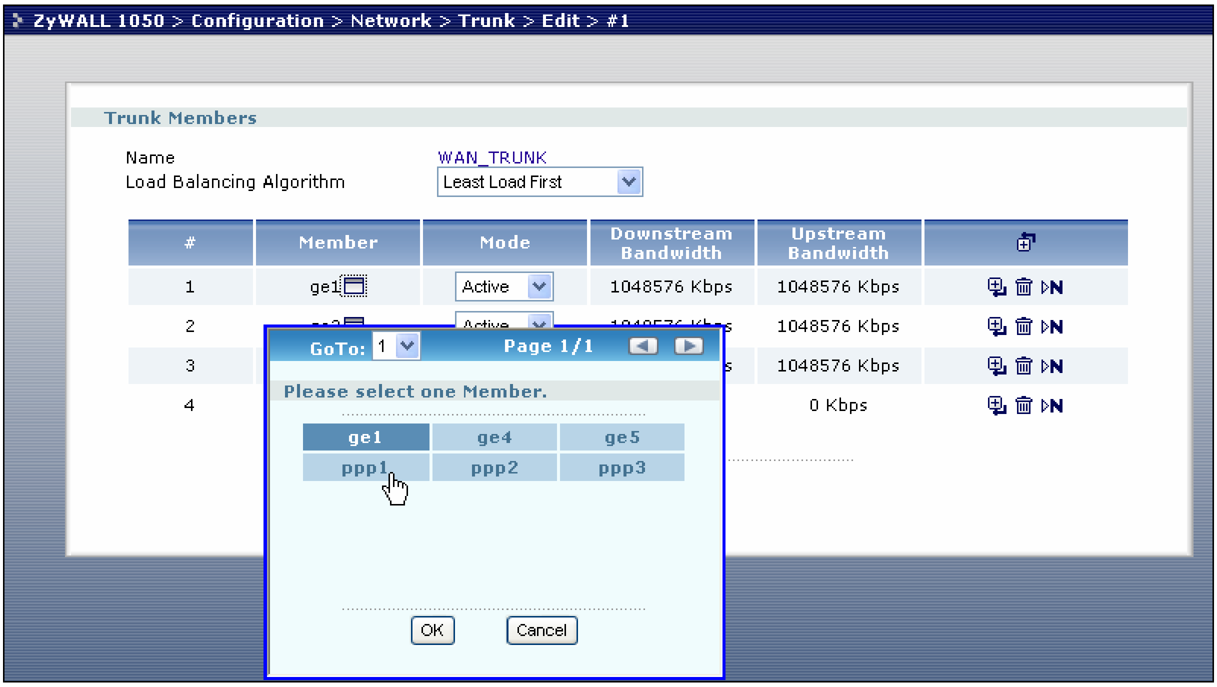
Name WAN_TRUNK

Load Balancing Algorithm Least Load First

| # | Member | Mode | Downstream Bandwidth | Upstream Bandwidth | |
|---|---|---|---|---|---|
| 1 | ge2 | Active | 1048576 Kbps | 1048576 Kbps | |
| 2 | ge3 | Active | 1048576 Kbps | 1048576 Kbps | |
| 3 | aux | Passive | 0 Kbps | 0 Kbps | |

To add a new interface into this WAN_Trunk

12) Click on the ☐ icon to pick the right PPPoE interface. Also, for the “Mode” of the Interface, if it is a “nail-up” connection, choose Active here and if it is a “dial-on-demand” connection, select “Passive” here. The “Downstream Bandwidth” and the “Upstream Bandwidth” are the values used for reference of the Load Balancing Algorithm.



ZyWALL 1050 > Configuration > Network > Trunk > Edit > #1

Trunk Members

Name WAN_TRUNK

Load Balancing Algorithm Least Load First

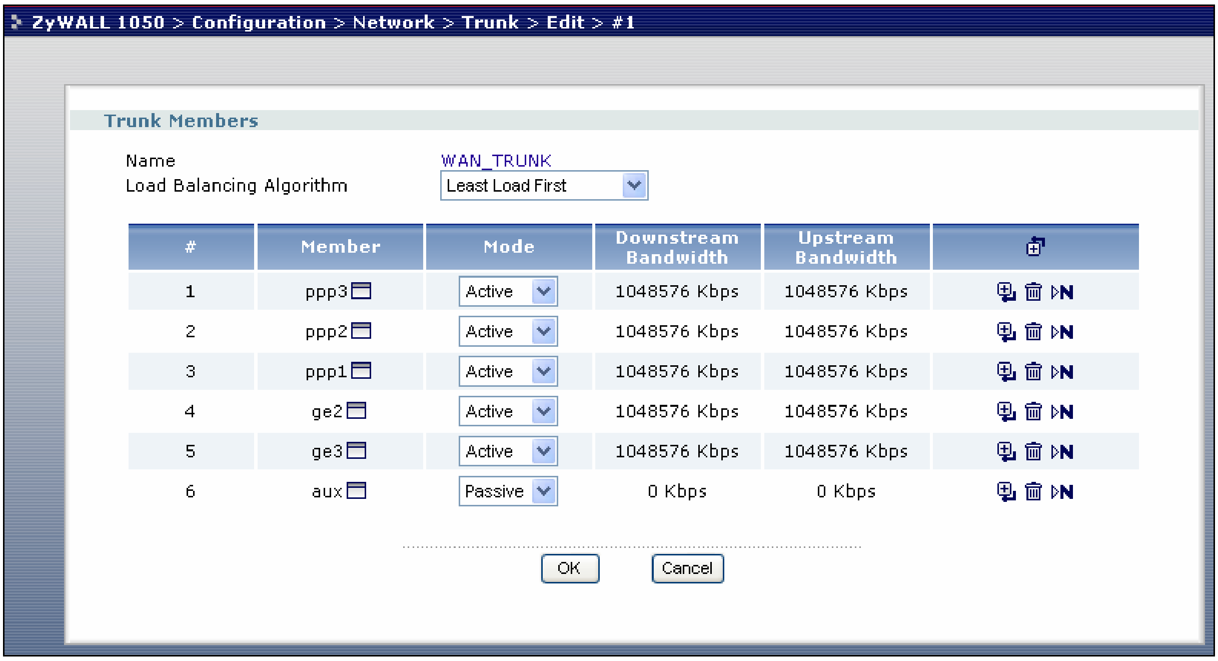
| # | Member | Mode | Downstream Bandwidth | Upstream Bandwidth | |
|---|---|---|---|---|---|
| 1 | ge1 | Active | 1048576 Kbps | 1048576 Kbps | |
| 2 | | Active | 1048576 Kbps | 1048576 Kbps | |
| 3 | | | s | 1048576 Kbps | |
| 4 | | | | 0 Kbps | |

GoTo: 1 Page 1/1

Please select one Member.

| | | |
|---|---|---|
| ge1 | ge4 | ge5 |
| ppp1 | ppp2 | ppp3 |

13) Repeat the above steps until all the three PPPoE interfaces are added into this WAN_Trunk interface.



Trunk Members

Name WAN_TRUNK

Load Balancing Algorithm Least Load First

| # | Member | Mode | Downstream Bandwidth | Upstream Bandwidth |
|---|---|---|---|---|
| 1 | ppp3 | Active | 1048576 Kbps | 1048576 Kbps |
| 2 | ppp2 | Active | 1048576 Kbps | 1048576 Kbps |
| 3 | ppp1 | Active | 1048576 Kbps | 1048576 Kbps |
| 4 | ge2 | Active | 1048576 Kbps | 1048576 Kbps |
| 5 | ge3 | Active | 1048576 Kbps | 1048576 Kbps |
| 6 | aux | Passive | 0 Kbps | 0 Kbps |

14) By default, GE2 and GE3 were already in the WAN_Trunk. And GE2 is set to get the IP automatically from the DHCP Server, thus, the only thing you may need to modify is the bandwidth value. However, this step is not mandatory.

**CLI commands to create a PPPoE account**

[0] account pppoe ISP1

[1] user test1@isp1.com

[2] password abcdefg

[3] authentication chap-pap

[4] compression no

[5] idle 0

[6] exit

**CLI commands to create a PPPoE interface**

[0] interface ppp1

[1] no shutdown

```
[2] description ISP1
[3] mtu 1492
[4] upstream 1048576
[5] downstream 1048576
[6] account ISP1
[7] connectivity nail-up
[8] bind ge2
[9] metric 0
[10] ping-check default-gateway
[11] ping-check default-gateway period 30
[12] ping-check default-gateway timeout 5
[13] ping-check default-gateway fail-tolerance 5
[14] no ping-check activate
[15] exit
```

**CLI commands to add all the PPPoE interfaces into the WAN Zone:**

```
[0] zone WAN
[1] block
[2] no interface ge2
[3] no interface ge3
[4] interface ppp3
[5] interface ppp2
[6] interface ppp1
[7] interface ge2
[8] interface ge3
[9] exit
```

**CLI commands to bind all the WAN Links (PPPoE + Fixed) into the WAN_Trunk interface**

```
[0] interface-group WAN_TRUNK
[1] mode trunk
[2] algorithm llf
[3] no interface ge2
[4] no interface ge3
[5] no interface aux
[6] interface 1 ppp3
[7] interface 2 ppp2
[8] interface 3 ppp1
[9] interface 4 ge2
[10] interface 5 ge3
[11] interface 6 aux passive
[12] exit
```

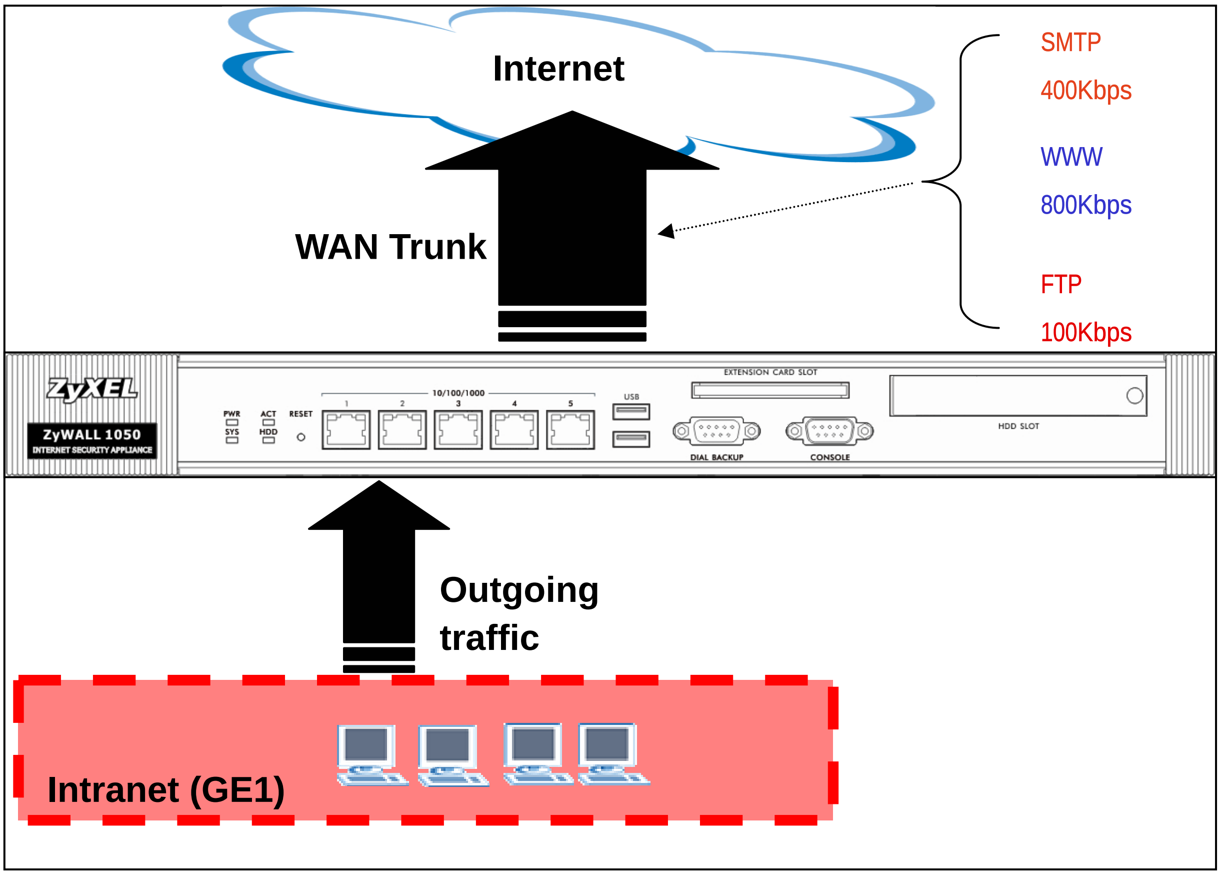
## 3.5 Guaranteed Quality of Service

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.

### 3.5.1 Priority & Bandwidth management

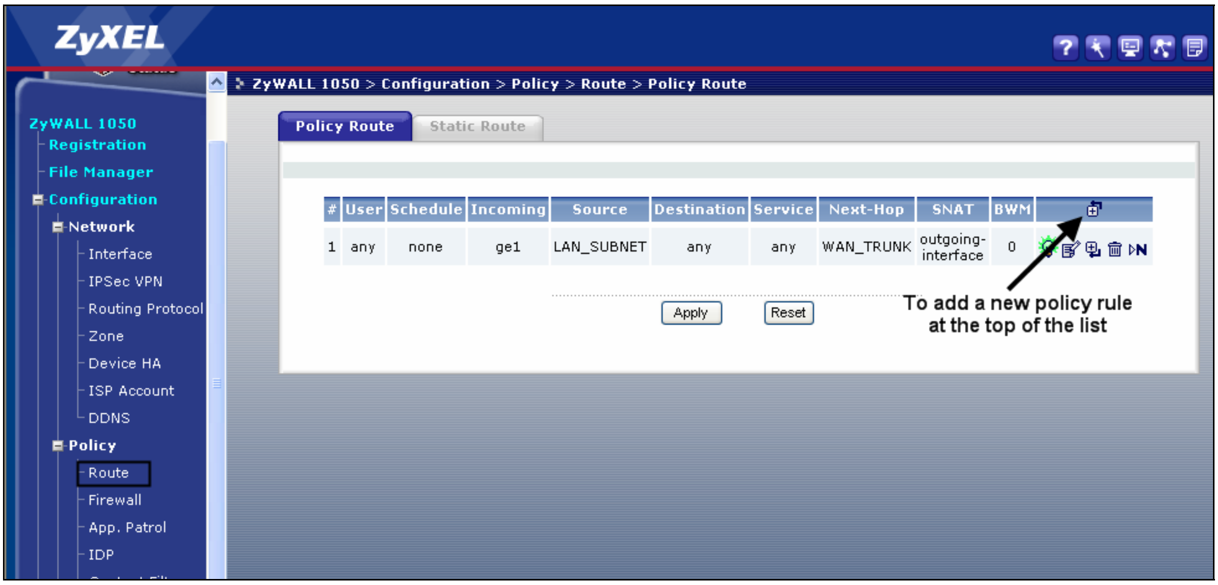
ZyWALL 1050 supports both prioritizing and bandwidth management for outgoing traffic. IT administrator can define bandwidth management policies to ensure quality of running services in their network environment. ZyWALL 1050 supports bandwidth management policy based on the type of service, origin of 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:

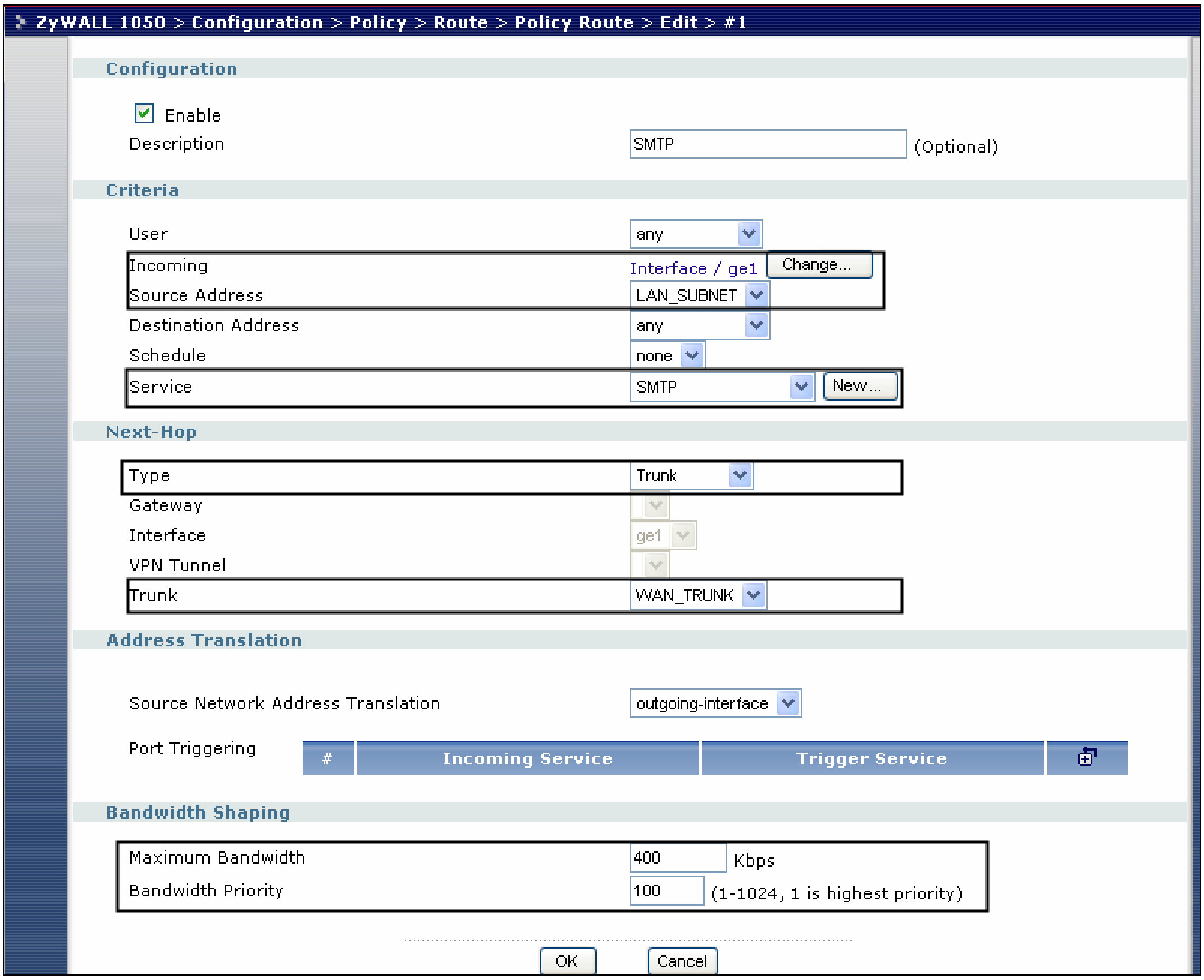
1) By default, ZyWALL 1050 created a WAN Trunk interface for you. Thus, you don’t need to worry about WAN Trunk in this scenario. Now, we will need to create those Bandwidth Management policies for our application. Logon to the ZyWALL 1050 GUI and go to **Configuration** > **Policy** > **Route** > **Policy Route.** Then click the “+” to add a new policy route at the top of your list.



| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM | |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 0 | |

To add a new policy rule at the top of the 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: SMTP (Optional)

**Criteria**

| | |
|---|---|
| User | any |
| Incoming | Interface / ge1 [Change...] |
| Source Address | LAN_SUBNET |
| Destination Address | any |
| Schedule | none |
| Service | SMTP [New...] |

**Next-Hop**

| | |
|---|---|
| Type | Trunk |
| Gateway | |
| Interface | ge1 |
| VPN Tunnel | |
| Trunk | WAN_TRUNK |

**Address Translation**

Source Network Address Translation: outgoing-interface

Port Triggering

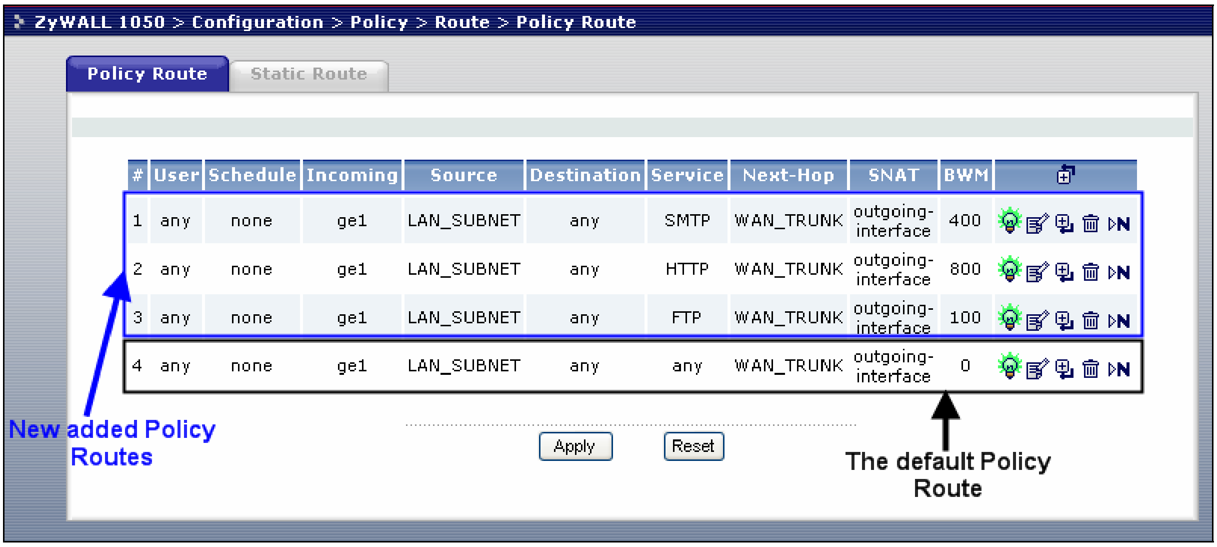
| # | Incoming Service | Trigger Service |
|---|---|---|

**Bandwidth Shaping**

Maximum Bandwidth: 400 Kbps

Bandwidth Priority: 100 (1-1024, 1 is highest priority)

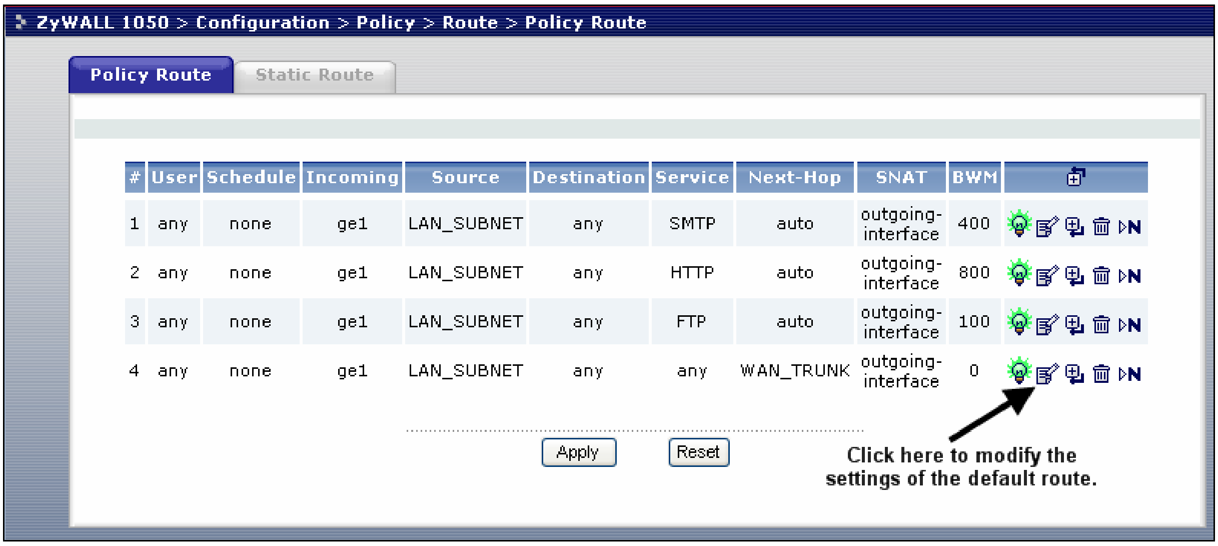
3) Repeat the above steps to create two more policy routes for “WWW” and “FTP” services. In the policy route you can set their Maximum Bandwidth to 800Kbps and 100Kbps along with a priority value. Below is what you should get so far:



| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM |
|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | ge1 | LAN_SUBNET | any | SMTP | WAN_TRUNK | outgoing-interface | 400 |
| 2 | any | none | ge1 | LAN_SUBNET | any | HTTP | WAN_TRUNK | outgoing-interface | 800 |
| 3 | any | none | ge1 | LAN_SUBNET | any | FTP | WAN_TRUNK | outgoing-interface | 100 |
| 4 | any | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 0 |

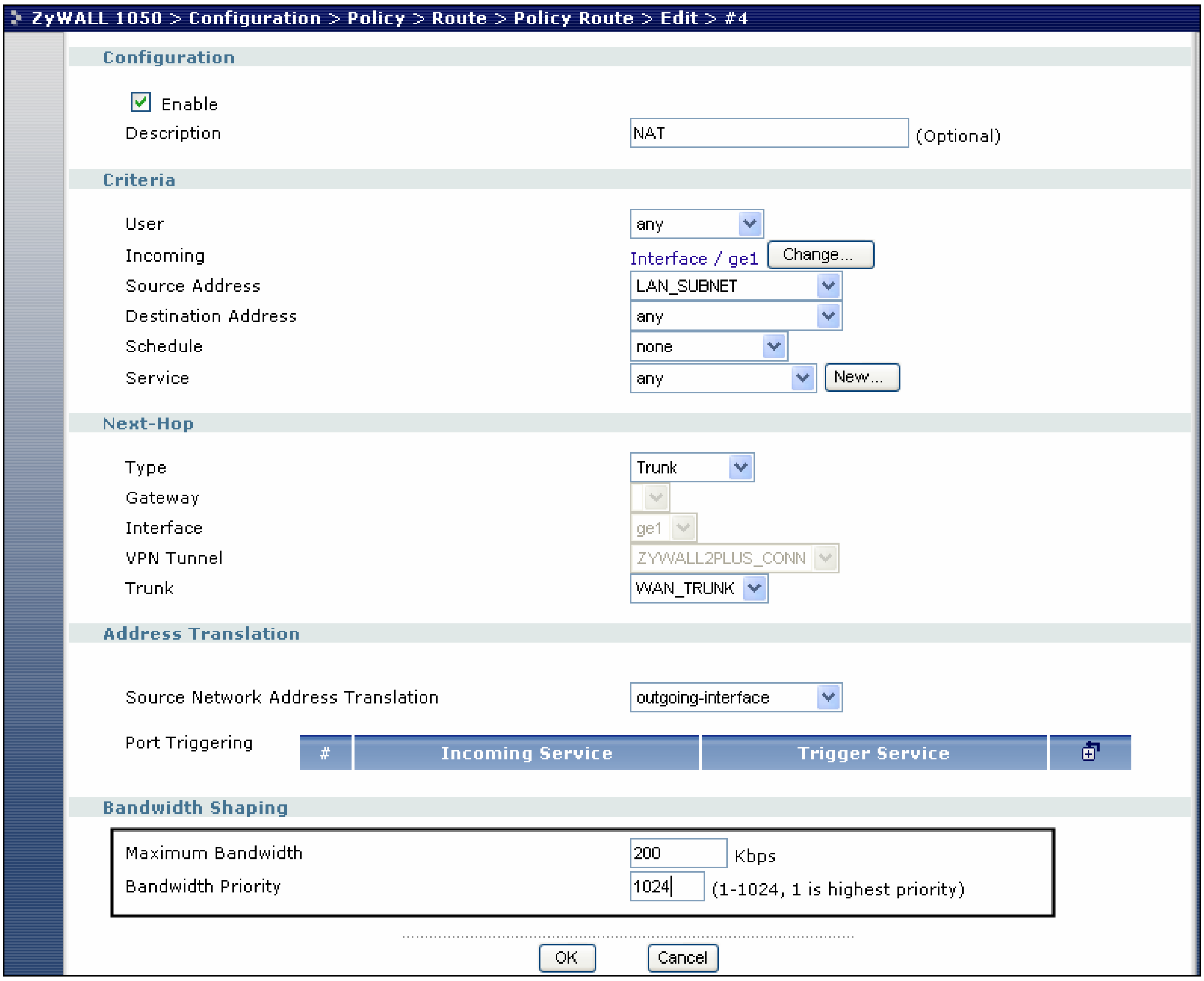
Tips: Policy Route rules are based on first match, first go. Thus, all your new rules should be placed before the default policy route, which is the last one here.

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
Apply
Reset
Click here to modify the settings of the default route.

| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM |
|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | ge1 | LAN_SUBNET | any | SMTP | auto | outgoing-interface | 400 |
| 2 | any | none | ge1 | LAN_SUBNET | any | HTTP | auto | outgoing-interface | 800 |
| 3 | any | none | ge1 | LAN_SUBNET | any | FTP | auto | outgoing-interface | 100 |
| 4 | any | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 0 |

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:

Interface: ge1

VPN Tunnel: ZYWALL2PLUS_CONN

Trunk: WAN_TRUNK

**Address Translation**

Source Network Address Translation: outgoing-interface

Port Triggering

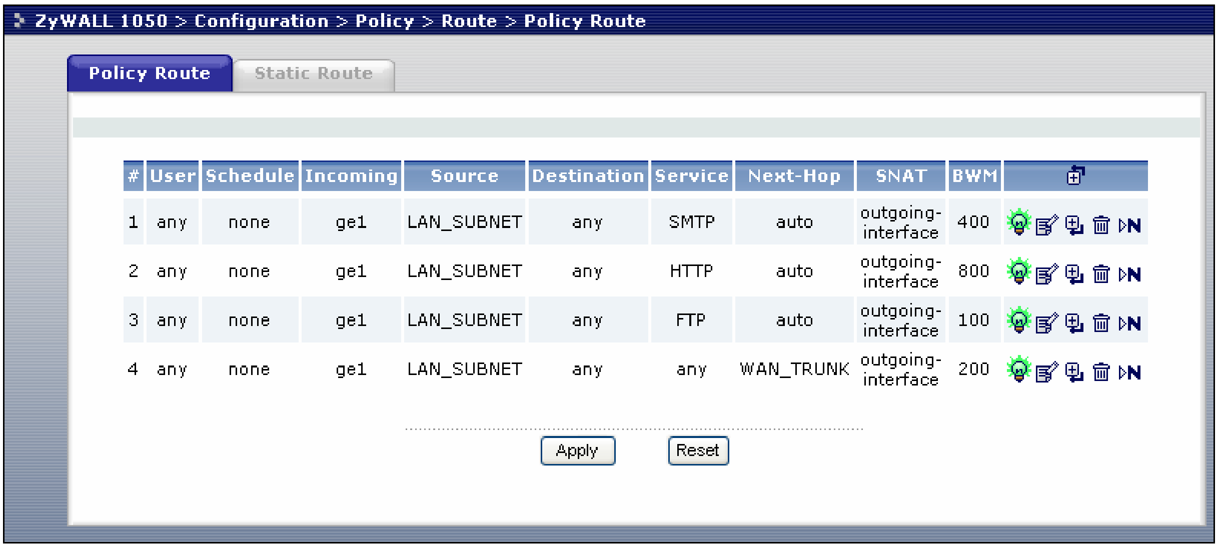
| # | Incoming Service | Trigger Service |
|---|---|---|

**Bandwidth Shaping**

Maximum Bandwidth: 200 Kbps

Bandwidth Priority: 1024 (1-1024, 1 is highest priority)

6) Now the final list should look like the one below:



| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM |
|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | ge1 | LAN_SUBNET | any | SMTP | auto | outgoing-interface | 400 |
| 2 | any | none | ge1 | LAN_SUBNET | any | HTTP | auto | outgoing-interface | 800 |
| 3 | any | none | ge1 | LAN_SUBNET | any | FTP | auto | outgoing-interface | 100 |
| 4 | any | none | ge1 | LAN_SUBNET | any | any | WAN_TRUNK | outgoing-interface | 200 |

**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 1050 to perform administrator's tasks?

You can connect your PC to ZyWALL 1050 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 1050 for management. The default administration username is "**admin**", and password is "**1234**".

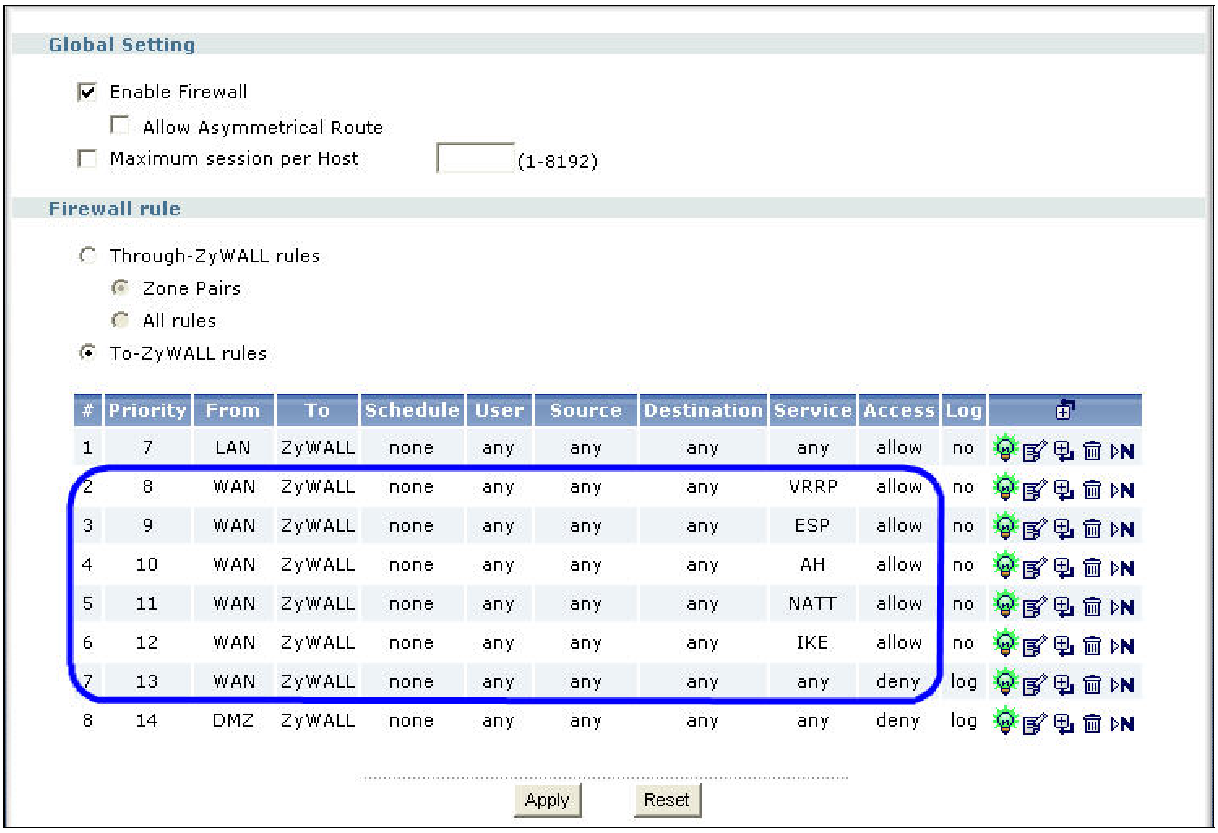
### A02. Why can't I login into ZyWALL 1050?

There may have several reasons why you can't login to ZyWALL 1050:

1. The ZyWALL 1050 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 1050'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 1050'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 1050 blocks login from such an IP address for 30 minutes by default.
6. You can be connecting to ZyWALL 1050 from a WAN interface which is blocked by default. If you don't want this block rule, go to GUI menu Configuration > System > WWW to set to accept the access from 'WAN' or from 'All'.

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

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



Global Setting

☑ Enable Firewall

□ Allow Asymmetrical Route

□ Maximum session per Host (1-8192)

Firewall rule

○ Through-ZyWALL rules

● Zone Pairs

○ All rules

● To-ZyWALL rules

| # | Priority | From | To | Schedule | User | Source | Destination | Service | Access | Log |
|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 7 | LAN | ZyWALL | none | any | any | any | any | allow | no |
| 2 | 8 | WAN | ZyWALL | none | any | any | any | VRRP | allow | no |
| 3 | 9 | WAN | ZyWALL | none | any | any | any | ESP | allow | no |
| 4 | 10 | WAN | ZyWALL | none | any | any | any | AH | allow | no |
| 5 | 11 | WAN | ZyWALL | none | any | any | any | NATT | allow | no |
| 6 | 12 | WAN | ZyWALL | none | any | any | any | IKE | allow | no |
| 7 | 13 | WAN | ZyWALL | none | any | any | any | any | deny | log |
| 8 | 14 | DMZ | ZyWALL | none | any | any | any | any | deny | log |

### A03. What's difference between "Admin Service Control" and "User Service Control" configuration in GUI menu Configuration > 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 1050 redirects me to the login page when I am performing the

**management tasks in GUI?**

There may be several reasons for ZyWALL 1050 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 1050 using other remote management client (telnet or ssh…etc) after you logged in ZyWALL 1050 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 1050 restarts?

There may have two reasons:

1. If you configure ZyWALL 1050 from CLI. You must type CLI “**write**” to save the configuration before rebooting. If you configure ZyWALL 1050 from GUI, any configuration will be automatically saved.
2. ZyWALL 1050 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 1050 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?

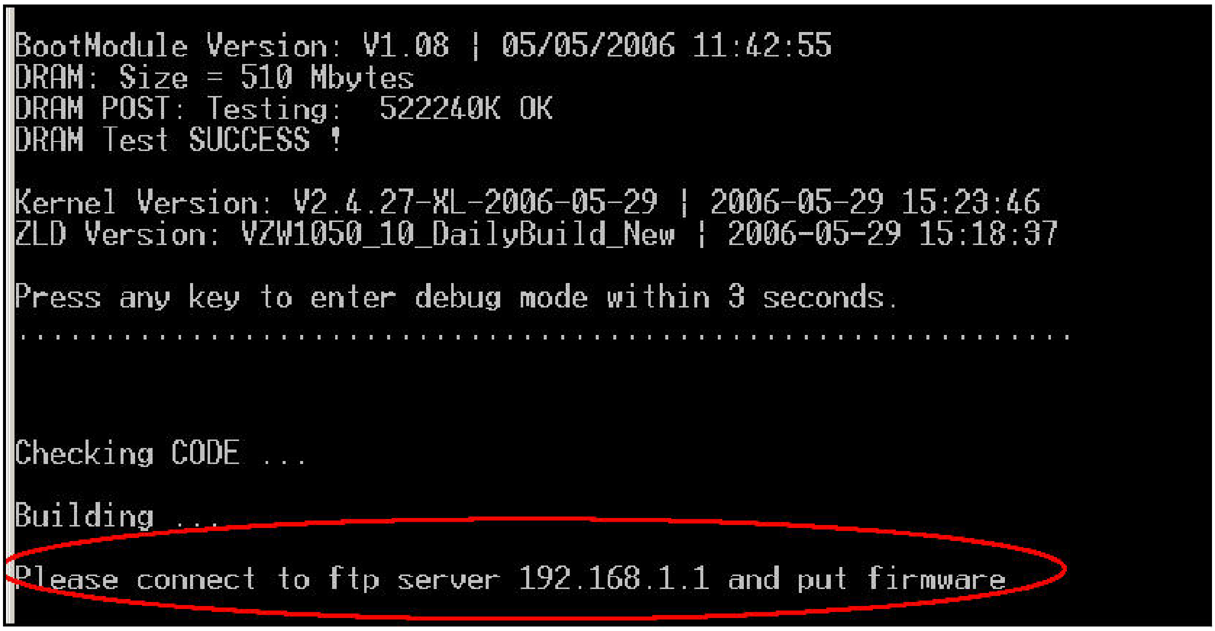
There are two reasons if your ZyWALL 1050 boots up for a long time as below.

1. It might because you have many configuration on ZyWALL 1050. 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 1050’s ge1 port which is with IP address 192.168.1.1 by default.

2. The ZyWALL 1050 may get firmware crashed. Generally, it may happen if power off ZyWALL 1050 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).



```
BootModule Version: V1.08 | 05/05/2006 11:42:55
DRAM: Size = 510 Mbytes
DRAM POST: Testing:  522240K OK
DRAM Test SUCCESS !

Kernel Version: V2.4.27-XL-2006-05-29 | 2006-05-29 15:23:46
ZLD Version: VZW1050_10_DailyBuild_New | 2006-05-29 15:18:37

Press any key to enter debug mode within 3 seconds.
............................................................


Checking CODE ...

Building ...

Please connect to ftp server 192.168.1.1 and put firmware
```

If you do see the message, please start the firmware recovery procedure as following steps.

(1). Connect a PC with ZyWALL 1050's ge1 port via an Ethernet cable.

(2). ftp 192.168.1.1 from your FTP client or MS-DOS mode

(3). Set the transfer mode to binary (use "bin" in the Windows command prompt).

(4). Reload the firmware. (ex. use command "put 1.00(XL.1)C0.bin" to upload firmware file)

(5). Wait the FTP uploading completed and it will restart the ZyWALL 1050 automatically.

# B. Registration FAQ

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

You must first register ZyWALL 1050 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 1050 device with myZyXEL.com server through GUI menu **Registration** page.

### B04. Does the device registration information reset after I reset ZyWALL 1050 to system default?

No. The device and service registration information are NOT stored in flash which is temporary memory. So it will not be erased after ZyWALL 1050 is reset to system defaults.

# C. File Manager FAQ

### C01. How can ZyWALL 1050 manage multiple configuration files?

From ZyWALL 1050 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 1050 system configuration file. When ZyWALL 1050 is booting, it will use this configuration file for ZyWALL 1050 as system configuration.
2. **system-default.conf**: The system-default.conf is ZyWALL 1050 system default configuration file. When you press the reset button, ZyWALL 1050 will copy system-default.conf over startup-conf.conf.
3. **lastgood.conf**: The lastgood.conf is created after ZyWALL 1050 successfully applies startup-config.conf. And ZyWALL 1050 will try to apply lastconfig.conf, if ZyWALL 1050 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 1050 through GUI menu **File manager** > **Shell Script** tab. Some notes as followings.

- Must follow ZyWALL 1050 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 1050 use objects?

ZyWALL 1050 objects include address, service, schedule, authentication method, certificate, zone, interface group and ISP account objects. The ZyWALL 1050 uses objects as a basic configuration block. It can simplify the configuration change once your have some change in the network topology.

For example, User can first create a zone object WAN_ZONE with the ge2 interface and later add the ge3 interface into WAN_ZONE. All security features that use the WAN_ZONE will change their configuration immediately according to zone object WAN_ZONE change.

### 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 ge1. click the “+” icon from the interface ge1 row, and fill out the necessary fields. It will create the virtual interface, ge1:1.

### 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.

### E06. What is the port grouping used for in ZyWALL 1050?

We can group two or more ports (up to five) together to form up a port grouping. For example, we group port1 and port2 together and the representative port is port1. The interface binding on port1 now also can be reached by host connected from port2 but the interface which bind in port2 previously will non-functional until port2 separate from this group.

Basically, port grouping provides an embedded layer-2 switching capability and each physical port can only join one port group. Packets transmit inside the port group are forwarded by hardware switch controller based on the destination MAC address without security checks (such as firewall, IDP…).

# 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 1050 will use the route setting to direct the traffic to the next hop.

## F02. How to configure a NAT?

Unlike ZyNOS ZyWALL, the NAT setting in ZyWALL 1050 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 objects 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 1050's DMZ zone, you need to configure virtual server to forward <Original IP(ex. ge2's IP):8080> to <Internal server IP:8080>.

## F03. 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.

### F03. How to limit some application (for example, FTP) bandwidth usage?

You need to add a policy route and configure service matching FTP object. Then edit the maximum bandwidth to FTP up-bound limitation. Please note that ZyWALL 1050 only support traffic shaping on WAN upstream direction.

### F04. What's the routing order of policy route, dynamic route, static route and direct connect subnet table?

All these routing information create the ZyWALL 1050 routing database. When routing, ZyWALL 1050 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.

### F05. Why can't ZyWALL 1050 ping to 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 1050. 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 1050 will select this as default route and traffic can’t go out from the ZyWALL 1050.

### F06. Why can’t I ping to the, Internet, after I shutdown the primary WAN interface?

ZyWALL 1050 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 1050 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.

### F07. Why don't the virtual server or port trigger 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.

### F08. Why don't the port trigger 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.

### F09. How do I use the traffic redirect feature in ZyWALL 1050?

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.

### F10. 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?

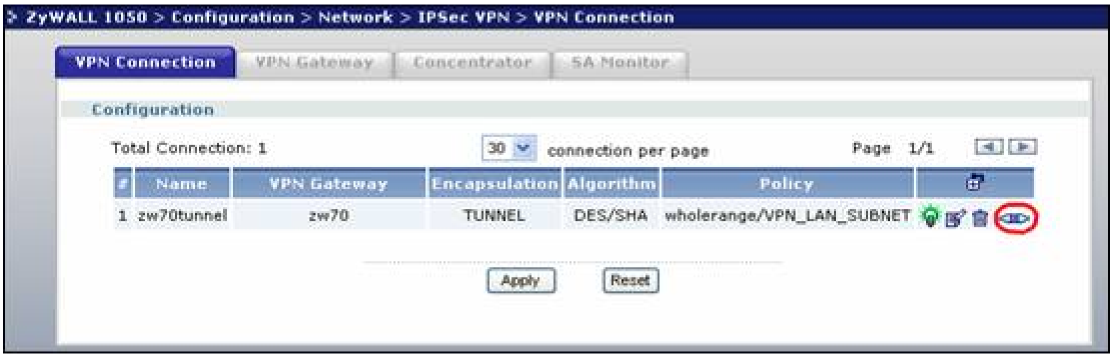
Please check the responder’s logs whether the fail occurs in phase 1 or phase 2. If the phase 1 has failed, try to check the VPN gateway configuration, such as proposals or Local/Remote ID. If the phase 2 has failed, try to check the VPN connection configuration, such as whether the policy matches the 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 1050 VPN tunnel had been configured correctly and the VPN connection status is connected but the traffic still can not reach the remote VPN subnet?

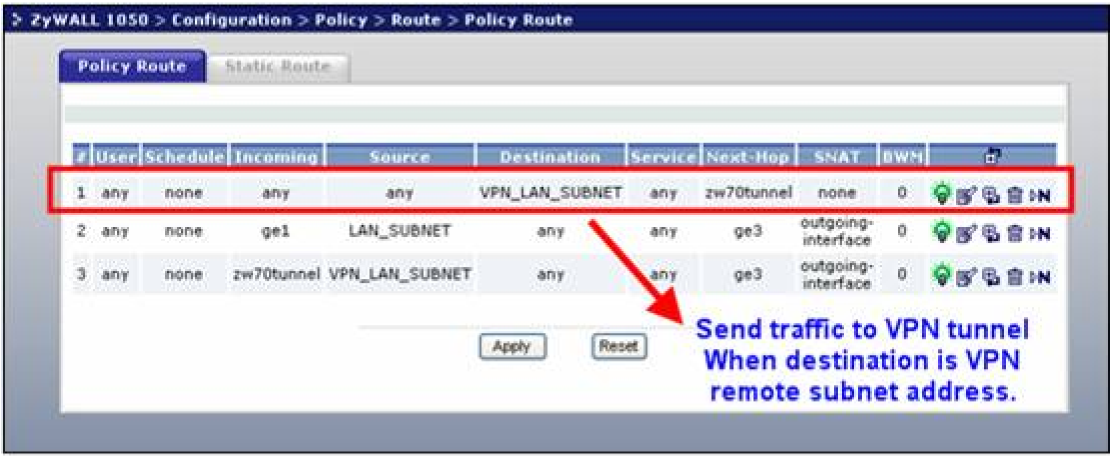
ZyWALL 1050 VPN traffic is the route base VPN, this means we need to configure a policy route rule to guide the ZyWALL 1050 how to route the VPN traffic to the VPN remote subnet. We can check if our VPN parameter setting is working by clicking connect icon after VPN tunnel has configured in both gateway. The VPN connection status showed below is connected.



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

| # | Name | VPN Gateway | Encapsulation | Algorithm | Policy |
|---|---|---|---|---|---|
| 1 | zw70tunnel | zw70 | TUNNEL | DES/SHA | wholerange/VPN_LAN_SUBNET |

We need a policy route to notify the ZyWALL 1050 send the packet to VPN tunnel when the packet’s destination address is VPN remote subnet. Please switch to ZyWALL 1050 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.


> ZyWALL 1050 > Configuration > Policy > Route > Policy Route
Policy Route
Static Route
Apply
Reset

| # | User | Schedule | Incoming | Source | Destination | Service | Next-Hop | SNAT | BWM |
|---|---|---|---|---|---|---|---|---|---|
| 1 | any | none | any | any | VPN_LAN_SUBNET | any | zw70tunnel | none | 0 |
| 2 | any | none | ge1 | LAN_SUBNET | any | any | ge3 | outgoing-interface | 0 |
| 3 | any | none | zw70tunnel | VPN_LAN_SUBNET | any | any | ge3 | outgoing-interface | 0 |

Send traffic to VPN tunnel When destination is VPN remote subnet address.

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

### G03. 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 1050 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?

The Application Patrol on ZyWALL 1050 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).

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

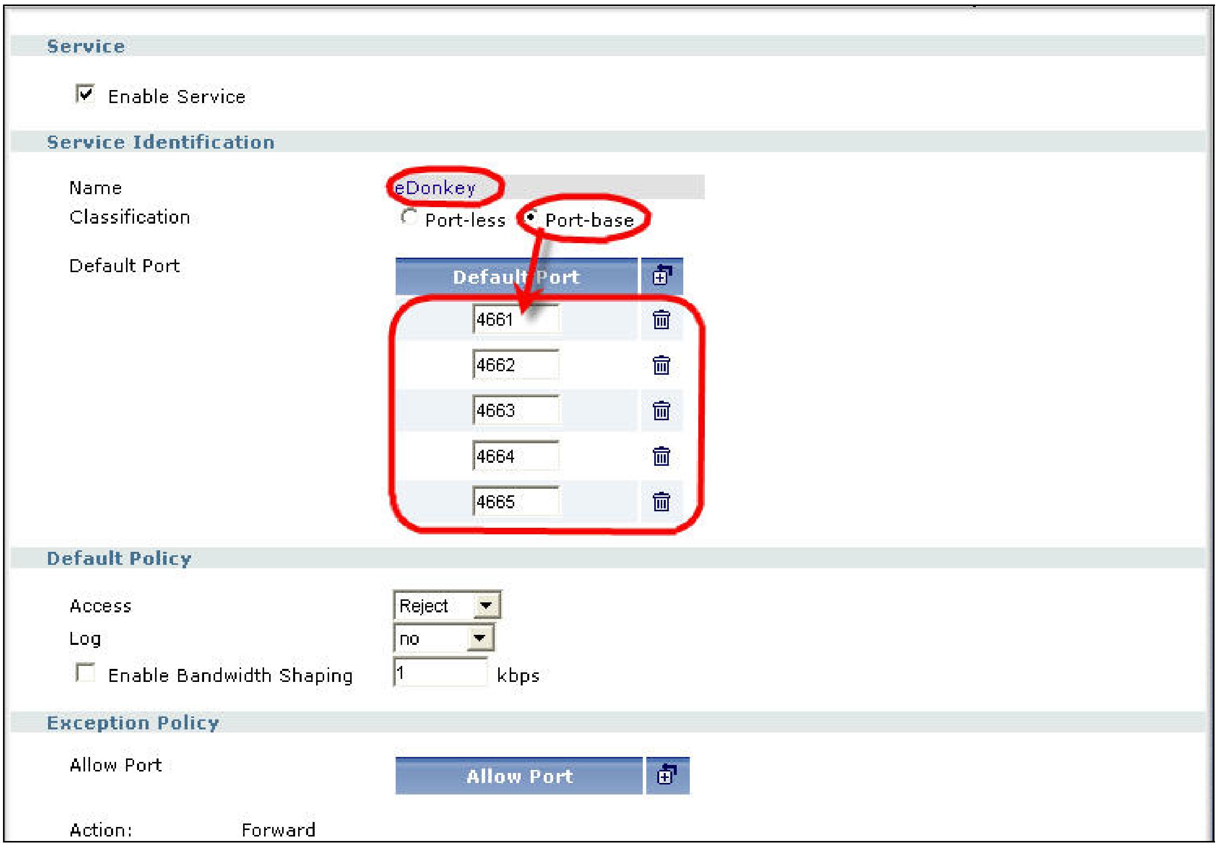
There are two possible reasons for this problem. One is that this application version is not supported by the Application Patrol (please refer to Application Patrol Support List). The other is that the Application Patrol needs several session packets for the application identification. After the session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

## I04. What is the difference for Portless and Port-based settings in the

### Application Patrol configuration page?

The portless setting functions as OSL layer 7 inspection while Port-based functions only up to layer 4 inspection. By default, portless base will be selected when an application patrol rule is enabled. To use Port-based option, it could help:

(1) Provide a clear port lists which is pre-defined in ZyWALL 1050. For example, it could help user to know the eDonkey service is defined the take action on port 4661 ~ 4665 as shown below.



Service

☑ Enable Service

Service Identification

Name: eDonkey

Classification: ○ Port-less ● Port-base

Default Port

| Default Port |
|---|
| 4661 |
| 4662 |
| 4663 |
| 4664 |
| 4665 |

Default Policy

Access: Reject

Log: no

□ Enable Bandwidth Shaping: 1 kbps

Exception Policy

Allow Port

Action: Forward

(2) It could be used when user want to apply bandwidth control for a certain allowed or rejected application (which is in Application Patrol support list). See the picture above. There is a field of “Enable Bandwidth Shaping”.

(3) Since the port-base performs up to OSI layer 4 inspection, so the system performance would be better than the port-less inspection (layer 7). Therefore, if user concern more about system performance or user’s network environment is simple, the port-base setting could be the choice.

# 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 1050 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 1050 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”.

# 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.

# 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 1050 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 1050 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 ZyWALL1050, 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.

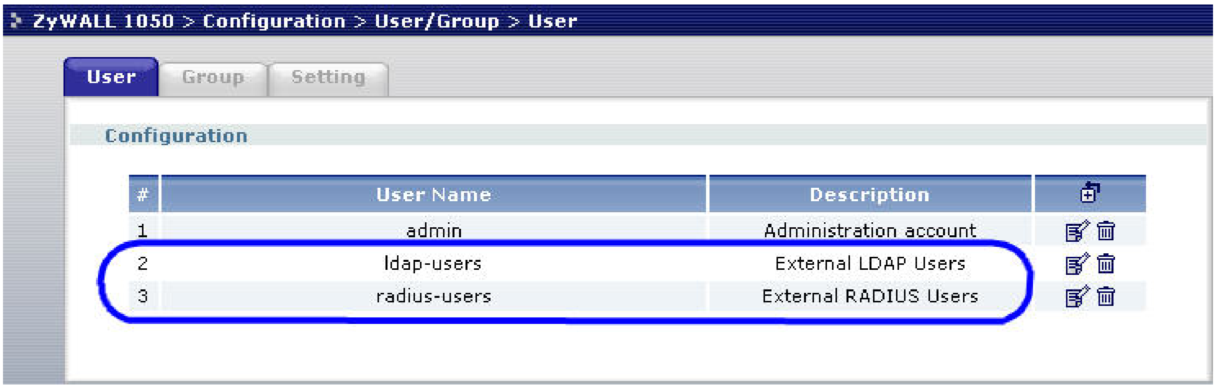
### M05. What are ldap-users and radius-users used for?

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.

### M06. What privileges will be given for ldap-users and radius-users?

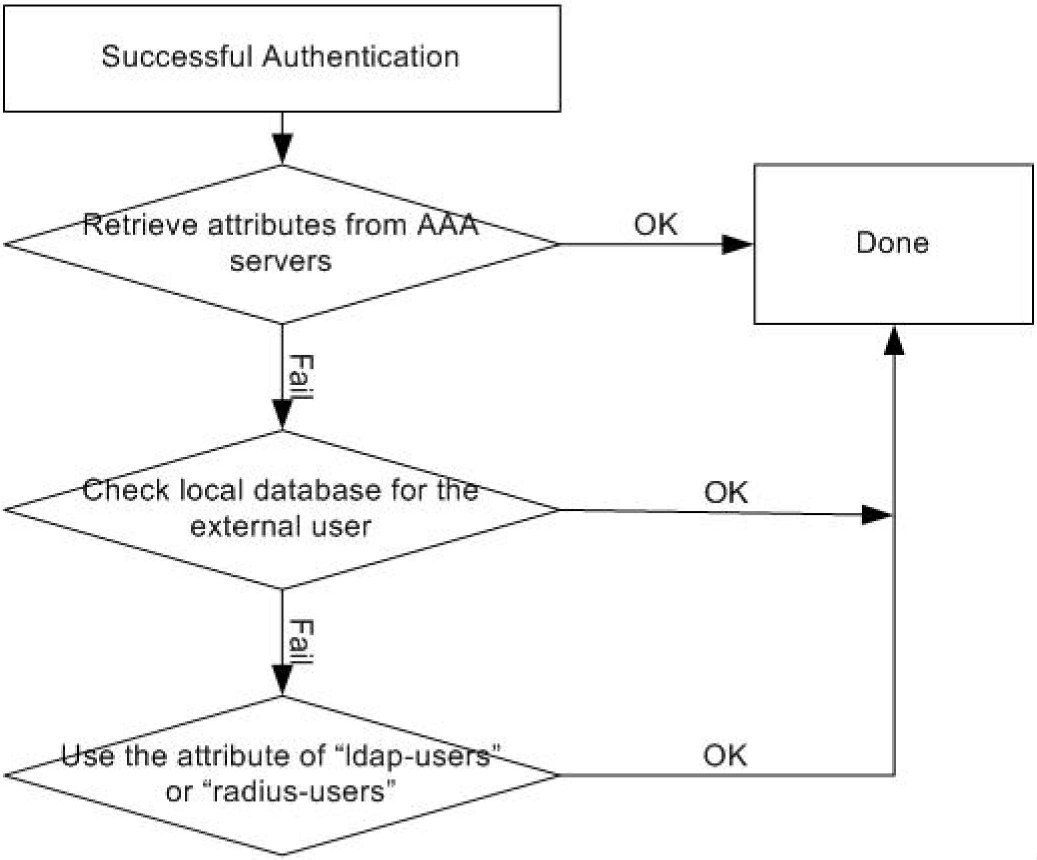
When a user has been authenticated by external database (ladp or radius server), it will retrieve the user’s attributes (like lease timeout and re-auth timeout value) from the external server. If the external server doesn’t define the user’s attributes, it will try to check local database on ZyWALL 1050 (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 Name | Description |  |
|---|---|---|---|
| 1 | admin | Administration account |  |
| 2 | ldap-users | External LDAP Users |  |
| 3 | radius-users | External RADIUS Users |  |

See the flow as shown below.



Successful Authentication
Retrieve attributes from AAA servers
OK
Done
Fail
Check local database for the external user
OK
Fail
Use the attribute of "ldap-users" or "radius-users"
OK

# 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 all the required field filled. Why can’t I receive the log mail?

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

# O. Traffic Statistics FAQ

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

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

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

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

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

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

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

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