

Internet Security Appliance



Version 1.00 June. 2006



All contents copyright (c) 2006 ZyXEL Communications Corporation.

## INDEX

1. VPN concentr	ator
1.1 Extende	ed Intranets
1.1.1 \$	Site to Site VPN solutions:
1.2 Deploy	ment of Extranet 10
1.2.1	Site to site VPN solutions (ZyWALL1050 to ZyWALL70)11
1.2.2	Interoperability – VPN with other vendors
1	2.2.1 ZyWALL with FortiGate VPN Tunneling
1	2.2.2 ZyWALL with NetScreen VPN Tunneling
1	2.2.3 ZyWALL with SonicWall VPN Tunneling
1.3 Replaci	ng Costly RAS Dial-in
1.3.1	Remote Access VPN
1.4 Large-s	cale VPN Deployment
1.4.1	Fully Meshed Topology
1.4.2	Star Topology
1.5 Internet	Access via Central Gateway
1.5.1	VPN Tunnel to Central Side (ZyWALL 70 to ZyWALL 1050) 60
2. Security Polic	y Enforcement
2.1 Managi	ng IM/P2P Application67
2.1.1	Why bother to manage IM/P2P applications?
2.1.2	What does ZyWALL 1050 provide for managing IM/P2P applications? 68
2.1.3	Configuration Example
2.2 Managi	ng WLAN79
2.2.1	Why the wireless networks need to be managed?79
2.2.2	What can we do against wireless insecurity?79
3. Seamless Inco	prporation91
3.1 Transpa	rent Firewall91
3.1.1	Bridge mode & Router (NAT) mode co-exist
3.1.2	NAT & Virtual Server96

# **1. VPN concentrator**

VPN (Virtual Private Network) allows you to establish a virtual direct connection to remote locations or for 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 are easy to troubleshoot.



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



All contents copyright (c) 2006 ZyXEL Communications Corporation.

Now, VPN connection management is made easy with the VPN concentrator. The VPN concentrator routes VPN traffics across multiple remote sites without complex settings, thus reducing configuration overhead and the possibility of improper configuration. The VPN concentrator is also a centralize management tool for administrators because all traffic sent between remote sites had to go through the central office first and administrators can set up different access control rules based on the source address, remote address, user and schedule to enhance VPN security. To help 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 easy troubleshooting and further 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 ability.



For SMB customer, ZyXEL provide total VPN solution from personal client to 500+ people firewall and all of them 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 consider a part of main office internet thus user behind branch office also can use the internal network resource as in main office. User will have LAN-like user experience across the internet through the VPN connection. Use of a VPN for smaller branch offices, franchise sites, and remote workers provides nearly the same level of connectivity and reliability as a private network. The remote connection cost also can decrease by leveraging the Internet connections to replace expensive leased lines.



#### 1.1.1 Site to Site VPN solutions:

Site to Site VPN is the basic VPN solution between local and remote gateway. We used this type of VPN connection to extend and join both site's local network as an internet over internet. There are two kinds of connection interface such as static IP, and Dynamic DNS.

Configure ZyWALL1050 with Static IP address:

ZyWALL1050 uses the static IP address for VPN connection. The topology is as following figure.



User need to configure the static IP address and then apply to VPN Gateway configuration page. The configuration steps as follow;

- Login ZyWALL1050 GUI and setup the ge2 interface for internet connection and manually assign a static IP. The configuration path is at ZyWALL 1050 menu Configuration > Network > Interface > Edit > ge2
- 2) Switch to Configuration > Network > IPSec VPN > VPN Gateway, and select interface ge2 as My Address and then set remote gateway IP 167.35.4.3 in Security Gateway Address field. 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 Remote ZyWALL1050. The **Local ID Type** & content and **Peer ID Type** & content are reverse to Local ZyWALL1050.

Ethernet Interface Properties	
✓ Enable Interface Name Description	ge2 (Optional)
IP Address Assignment	
<ul> <li>Get Automatically</li> <li>Use Fixed IP Address</li> </ul>	
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	<pre>x &gt; IPSec ¥PN &gt; ¥PN Gateway &gt; Edit &gt; #1</pre>
1 1050 > Configuration > Network > 1	PSec VPN > VPN Gatemax > Edit > #5	RemoteSite
VPN Gateway		
VPN Gateway Name	LocalSite	Main 💌
IKE Phase 1		# Encryption Authentication
Negotiation Mode Proposal	Main 🔽	1 DES MDS 🗹 🗑
	1 DES V MD5 V III	66400 <180 - 3000000>
Key Group		
SA Life Time (Seconds)	86400 <180 - 3000000>	
🔲 NAT Traversal		
🔽 Dead Peer Detection (DPD)		
Property		ge2 Static 167.35.4.3/255.255.250.240
My Address		
Interface	ge2 Static 210.110.7.1/255.255.255.240	1. 210.110.7.1
C Domain Name		2. 0.0.0
Secure Gateway Address	1. 167.35.4.3	
	2, 0.0.0.0	
Authentication Method		123456/89
• Pre-Shared Key	123456789	
C Certificate	(See My Certificates)	167.35.4.3
Local ID Type	IP 🔻	P 🗴
Content	210.110.7.1	210.110.7.1
Peer ID Type	IP V	
Content	167 35 4 3	

- 4) User can refer to the user guide to complete the rest settings for VPN tunnel.
- 5) The ZyWALL1050 VPN is the 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 local subnet to remote subnet after configured the VPN gateway and connection (phase1 and phase2). The purpose for this policy route is to tell the ZyWALL1050 send the traffic to VPN tunnel when traffic from local subnet and destination is remote subnet. Switch to ZyWALL 1050 > 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 VPN tunnel and then choose the corresponding VPN connection rule from VPN tunnel drop down menu. After all, the VPN tunnel and routing had built up and user can start to test in field.

ZyWALL 1050 > Configuration > Policy > Route	> Policy Route > Edit > #1
Configuration	
	<b>b</b>
Description	VPN_route (Optional)
Uriteria	
User	any 💌
Incoming	Interface / ge1 Change
Source Address	LAN_SUBNET 💌
Destination Address	Remote_Subnet 🗸
Schedule	none 💌
Service	any 🔽 New
Next-Hop	
Туре	VPN Tuppel
Gateway	WAN Gateway
Interface	ge1 🗸
VPN Tunnel	RemoteTunnel 🗸
Trunk	WAN_TRUNK 🗸
Bandwidth Shaping	
Neulinum Bergleichte	
Maximum Bandwidth	U Kbps
Bandwidth Priority	0 (1-1024, 1 is highest priority)
	OK Cancel

#### The CLI command 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 local and remote gateway.
- 2. Make sure the IKE & IPSec proposal is the same in local and remote gateway.
- 3. Select the correct **interface** for VPN connection.
- 4. The Local and Peer ID type and content must opposite not in the same content.
- 5. Make sure the **VPN policy route** had been setup in ZyWALL1050.

### **1.2 Deployment of Extranet**

The VPN provides the access to extranets which can provide the security path over internet to improve the client service, vendor support and company communications. The different and flexible business models have been development base on the global VPN extranet architecture. For example, customers can order equipment over the VPN and Suppliers also can check the orders electronically. The other general application is the employees across different branches can collaborate on project documents and share the different site's internal resource to complete the project.



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 more...

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

The exciting ZyWALL35 or 70 users can replace their central office gateway to ZyWALL1050 and move the ZyWALL35 or 70 to remote office. The ZyWALL1050 can provide higher VPN throughput and deal with multiple VPN tunnels at the same time. We used ZyWALL70 as an example to show how to build tunnel between ZyWALL5/35/70 and ZyWALL1050.



 Login ZyWALL1050 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 Description	ge2 (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 interface ge2 as My Address and then set remote gateway IP 167.35.4.3 in Security Gateway Address field. 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 ZyWALL1050. The My Address and Remote Gateway Address are ZyWALL70 and ZyWALL1050 WAN IP address. The Pre-Shared Key configured in both sides must exactly the same. The Local ID Type & content and Peer ID Type & content are reverse to Local ZyWALL1050.
- 4) The IKE Proposal is very important setting when configuring the VPN tunnel. The proposal includes Negotiation Mode, Encryption and Authentication Algorithm and.... Please make sure the IKE proposal parameters must the same in both sides.

WALL 1050 > Configuration > Network > :	IPSec YPN > YPN Gateway > Edit > #5	Negotiation Mode Encryption Algorithm Authentication Algorithm SA Life Time (Seconds) Key Group Enable Multiple Proposals Associated Network Poliries	Man V DES V MO5 V 28000 DHT V
VPN Gateway Name 2	LocalSite	Inspecial and including Foncies	
IKE Phase 1		/PN - GATEWAY POLICY - EE	DIT
Negotiation Mode Proposal	Main V # Encryption Authentication 1 DES V MD5 V	Property Name	Bandoffee
Kev Group	DH1 V	NAT Traversal	<b>_</b>
SA Life Time (Seconds)           NAT Traversal           Dead Peer Detection (DPD)	86400 <180 - 3000000>	Gateway Policy Information	
		NY THE	107.05.4.2
Property		My Address     My Demain Name	(Dr.30.4.3 (Domain Name or IP Address)
My Address Interface	ge2 Y Static 210.110.7.1/255.255.25	Remote Gateway Address	210.110.7.1
ODOMAIN NAME Secure Gateway Address	1, 167.35.4.3	Authentication Key	
	2. 00.0.0	• Pre-Shared Key	123456789
Authentication Method		O Certificate	auto_generaled_self_signed_cert 🔽 (See <u>My Certificates</u> )
Pre-Shared Key	123456789	Local ID Type	
O Certificate	(See My Certificates)	Content Description	16/.30.4.3
Local ID Type	P V	Peer ID Tipe	210 110 7 1
Content	210.110.7.1		210.110.1.1]
Peer ID Type	P 💌	Extended Authentication	
Content	167.35.4.3	Enable Extended Authentication	
		O Server Mode	(Search Local User first then RADIUS)
		<ul> <li>Client Mode</li> </ul>	
		User Name	
		Password	

- 5) Switch to Configuration > Network > IPSec VPN > VPN Connection, add a new VPN connection (IPSec phase2). Please setup the Phase2 proposal and local and remote policies in turn. The phase2 proposal chosen must the same as remote site ZyWALL70.
- 6) In ZyWALL70, VPN is the rule based VPN; this means the traffic going to tunnel or not

will depends 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 reverse to the ZyWALL70's setting, otherwise the tunnel will fail to buildup.

7) Please confirm the **IPSec proposal** in both sites is the same and the configuration is done in both sites.



8) The ZyWALL1050 VPN is the 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 local subnet to remote subnet after configured the VPN gateway and connection (phase1 and phase2). The purpose for this policy route is to tell the ZyWALL1050 send the traffic to VPN tunnel when traffic from local subnet and destination is 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 VPN tunnel and then choose the corresponding

VPN connection rule from VPN tunnel drop down menu. After all, the VPN tunnel and routing had built up and user can start to test in field.

<u> </u>	ALL 1030 > Configuration > Poinc	y > Route > Fully Route > Eult > #1
	Configuration	
	🗹 Enable	8
	Description	VPN_route (Optional)
	Criteria	
	User	any 💙
	Incoming	Interface / ge1 Change
	Source Address	
	Destination Address	Remote_Subnet 🗸
	Schedule	none
	Service	any 💉 New
	Next-Hop	
	Туре	VPN Tunnel
	Gateway	WAN Gateway
	Interface	ge1 🗸
	VPN Tunnel	RemoteTunnel
	Trunk	WAN_TRUNK 🗸
	Bandwidth Shaping	
	Maximum Bandwidth	
	Bandwidth Priority	0 (1-1024, 1 is highest priority)
		OK Cancel

- 9) After configured both sides VPN setting, we can click the Dial up VPN tunnel icon to test the VPN connectivity.
- 10) The tunnel had been successful dialed up message.



#### The CLI command for application:

```
ZyWALL1050 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
```

```
ZyWALL1050 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 local and remote gateway.
- 2. Make sure the IKE & IPSec proposal is the same in local and remote gateway.
- 3. Select the correct **interface** for VPN connection.
- 4. The Local and Peer ID type and content must opposite not in the same content.
- 5. Make sure the **VPN policy route** had been setup in ZyWALL1050.

#### 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 the figure shown below, the tunnel between Central and Remote offices ensures the packet flows 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 ZyWALL1050's interface and VPN setting retain the same setting as pervious example; if you are first jumping this section please refer to page8 ZyWALL1050 to ZYWALL70 VPN tunnel setting:

I made a list to briefly show the VPN phase1 and phase2 configuration parameter as below.

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

All contents copyright (c) 2006 ZyXEL Communications Corporation.

- Please configure the ZyWALL1050 's VPN gateway and VPN connection as the list and please remember to configure the policy route for VPN traffic routing. User can refer to pervious scenario or user guide to setup the ZyWALL1050 VPN setting.
- Login to FortiGate GUI and switch to System > Network > Interface and setup the wan1 interface as 167.35.4.3 and internal interface as 192.168.2.1/255.255.255.0.

	<u>Interface</u> Zone	Options			
✓ System	Create New 2				
Status	Greateriten				
Network	Name	IP / Netmask	Access	Status	
DHCP	dmz1	10.10.10.1 / 255.255.255.0	HTTPS,PING	O Bring Down	2
	dmz2	1	PING	O Bring Down	2
Admin	internal	192.168.2.1 / 255.255.255.0	HTTPS,PING,HTTP	O Bring Down	2
- Maintananna	wan1	167.35.4.3 / 255.255.255.0	HTTPS,PING,HTTP	O Bring Down	2
	wan2	1	PING	O Bring Down	2

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

 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.

		<u>Auto Key (IKE)</u> Manual Key	Concentrator Monitor	
	System	Create Phase 1) Create Phase	2)	3
Þ	Router	Phase 1	Phase 2	Interface Binding
Þ	Firewall			
-	VPN			
	IPSEC			
	PPTP			
	SSL			
	Certificates			

4) Fill-in the VPN phase1 setting according to the table listed. We don't have to setup the ID type and content because FortiGate accept any peer ID. Make sure the pre-share key and proposal is the same as the ZyWALL1050.

o Key (IKE)	Manual Key Conce	entrator Monitor		
		New Phase 1		
	Name	ZyWALL		
	Remote Gateway	Static IP Address 💌		
	IP Address	210.110.7.1		
	Local Interface	wan1 💌		
	Mode	O Aggressive 💿 Main (ID protection)		
	Authentication Method	Preshared Key 💌		
	Pre-shared Key	•••••		
	Peer Options			
		<ul> <li>Accept any peer ID</li> </ul>		
	Advanced	(XAUTH, Nat Traversal, DPD)		
	Enable IDPec Interface Mede			
	Local Galeway IP			
	D1 Dreposal	O specify 0.0.0.0		
	PIProposal			
	DU Crave			
	DH Group			
	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) Back to the VPN configuration page again and click **Create Phase 2** button to add a new Phase2 policy.

	Auto Key (IKE) Manual Key	Concentrator Monitor			
System	(Create Phase 1) (Create Phase 2)				
Router	Phase 1	Phase 2	Interface Binding		
Firewall		Tunnel Mode:			
	ZyWALL		wan1	💼 🌌	
- VPN					
>IPSEC					
PPTP					
SSL					
Certificates					

6) Select the "ZyWALL"(configured in step 4) policy from 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 ZyWALL1050 phase 2.

Auto Key (IKE)	Manual Key 💦 🤇	Concentrator	Monitor
			6
		Ne	ew Phase 2
	Name	Z	yWALL_PH2
	Phase 1	Z	ZyWALL
	Advanced	)	
	P2 Proposal	1-Encryption:	DES 💌 Authentication: SHA1 💌 🗉
		🗹 Enable repla	ay detection
		🔲 Enable perf	ect forward secrecy(PFS).
		DH Group	1 0 2 5 0
	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 add	dress 192.168.1.0/255.255.255.0
		Destination por	t 0
		Protocol	0
	(	ок	Cancel

7) We finished the VPN tunnel configuration and the VPN IPSec page will show the VPN phase 1 and phase 2 rules under Auto Key (IKE) tab.

Contour.	<u>Auto Key (IKE)</u> Manual Key	Concentrator Monitor		
System	Create Phase 1 Create Phase	2		7
Router	Phase 1	Phase 2	Interface Binding	
Firewall		Tunnel Mode:		
	ZyWALL		wan1	2
- VPN		ZyWALL_PH2		💼 🎽
IPSEC				

8) We need to setup the firewall rule 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 "Creat New" button to creat new address object.

	<u>Address</u> Group		
> System	Create New		8
Router	Name	Address / FQDN	
🗕 Firewall	▼ IP/Mask		
Policy	Fortinet	192.168.2.0/255.255.255.0	2
Address	Zynet	192.168.1.0/255.255.255.0	2
Service	all	0.0.0/0.0.0.0	2
Service			

 Switch to Firewall > Policy and click "Insert Policy Before" icon to add new policy for VPN traffic from FortiGate to ZyWALL.

Policy						
Create New						<b>Q</b>
ID Source	Dest	Schedule	Service	Action	Enable	
▼ internal -> wan1 (1)						
1 <u>all</u>	all	always	ANY	ACCEPT		💼 🎽 🐳 🗟
	Policy       Create New       ID     Source       internal -> wan1 (1)       1     all	Policy       Create New       ID     Source       internal -> wan1 (1)       1     all	Policy       Create New       ID     Source       internal -> wan1 (1)       1     all       all	Policy       Create New       ID     Source       D     Source       Dest     Schedule       Schedule     Service       internal -> wan1 (1)     I       1     all       all     always	Policy       Create New       ID     Source       D     Source       D     Source       Internal -> wan1 (1)       1     all       all     always   ANY ACCEPT	Policy       Create New       ID     Source       D     Source       Dest     Schedule       Service     Action       Enable       internal -> wan1 (1)       1     all       always     ANY

All contents copyright (c) 2006 ZyXEL Communications Corporation.

10) We 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 all kind of traffic can pass through VPN tunnel at any time. There are three kinds of Action available for user to configure, because the traffic sends 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 ZyWALL tunnel.

		New Po	licy	
Source	Interface/Zone	internal		*
	Address Name	Fortinet	~	
Destination	Interface/Zone	wan1		~
	Address Name	Zynet	~	
	Schedule	always		~
	Service	ANY		~
	Action	IPSEC		~
VPN Tunnel		ZyWALL		*
🗹 Allow inł	oound (	Inbound NAT		
🗹 Allow ou	tbound (	Outbound NAT		
🗌 Protecti	on Profile	unfiltered		~
🗌 Loa Alla	wed Traffic			
Traffic S	haping			
Comments	(maximum 63 cha	aracters)		
				<u>^</u>
				·
	<u> </u>		Cancel	

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

	System	C	reate New 💦							11	LÌ	
I	Router	IC	) Source	Dest	Schedule	Service	Action	Enable				
	Firewall	🔻 int	ternal -> wan1 (2)									
ľ	Policy	2	Fortinet	Zynet	always	ANY	ENCRYPT		ŵ	2 🗄	<b>I</b> 6	4
	Address	1	all	all	always	ANY	ACCEPT		Û	2 -	3	•

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 Address name is Fortinet

(192.168.2.0/255.255.255.0 address object). Schedule and service type are always and ANY to ensure all kind of traffic can pass through VPN tunnel at any time. We only

select "ACCEPT" as action this time because the traffic send from wan to internal must be decrypted first then can be transmitted. Don't select the IPSec as the **Action** in this VPN traffic flow direction.

				12
		New Policy	/	
Source	Interface/Zone	wan1		<b>~</b>
	Address Name	Zynet	~	
Destination	Interface/Zone	internal		<b>~</b>
	Address Name	Fortinet	~	
	Schedule	always		<b>~</b>
	Service	ANY		~
	Action	ACCEPT		~
		Dynamic IP Pool Fixed Port		
🗌 Protectio	n Profile	unfiltered		<b>~</b>
📃 Log Allow	/ed Traffic			
Authentic	ation	Firewall		×
🗌 Traffic Sh	aping			
Comments (r	naximum 63 cha	aracters)		
		ок	Cancel	

13) The overall firewall policy shows in follow figure and the VPN tunnel between ZyWALL and FortiGate had been successfully setup.

	Po	olicy										
System		Cre	ate New							1	.3	j
Router		ID	Source	Dest	Schedule	Service	Action	Enable				
🗕 Firewall	🔹 i	nter	nal -> wan1 (2)									
Policy		2	<u>Fortinet</u>	Zynet	always	ANY	ENCRYPT		ŵ	2	1	4
Address		1	<u>all</u>	<u>all</u>	always	ANY	ACCEPT		â	2	1	
Service	• •	want	l -> internal (1)									
Schedule		3	Zynet	Fortinet	always	ANY	ACCEPT		Î	2	-	

#### **Tips for application:**

- 1. Make sure the **Pre-Shared Key** is the same in local and remote gateway.
- 2. Make sure both IKE and IPSec proposal are the same in local and remote gateway.
- 3. Make sure the **VPN policy route** had been setup in ZyWALL1050.
- 4. Make sure the **Firewall rule** had been setup in FortiGate.

#### 1.2.2.2 ZyWALL with NetScreen VPN Tunneling

This page guides how to setup a VPN connection between the ZyWALL 1050 and NetScreen 5GT.

As the figure shown below, the tunnel between Central and Remote offices ensures the packet flows 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 NetScreen are explained in the following sections.



The central office gateway ZyWALL1050's interface and VPN setting retain the same setting as pervious example; if you are first jumping this section please refer to page8 ZyWALL1050 to ZYWALL70 VPN tunnel setting:

I made a list to briefly show the VPN phase1 and phase2 configuration parameter as below.

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

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

- Please configure the ZyWALL1050 's VPN gateway and VPN connection as the list and please remember to configure the policy route for VPN traffic routing. User can refer to pervious scenario or user guide to setup the ZyWALL1050 VPN setting.
- 2) Using a web browser, login NetScreen by giving the LAN IP address of NetScreen in URL field. The default username and password is netscreen/netscreen.
- 3) Switch to menu Network > Inetrfaces and configure the WAN/LAN IP address to WAN: 167.35.4.3 LAN: 192.168.2.0/24. The trust interface is stand for LAN, the untrust interface is stand for WAN.

			Network	< > I	Routing > Routing I	Entries						5gt	?
	- <u>E</u> N	Ι	List 20	*	per page						3		_
	NET SCREEN <sup>.</sup>		List rou	te e	entries for All virtua	l routers 🐱					trust-vr	*	New
	TREND SECURE												
	NS5GT	•		tri	ust-vr								
	Update Admin	^			IP/Netmask	Gateway	Interface	Protocol	Metric	Vsys	Configure		
	Auth			*	0.0.0.0/0	167.35.4.1	untrust	s	1	Root	<u>Remove</u>		
	Port Mode			*	167.35.4.0/24	0.0.0.0	untrust	с	0	Root	-		
	Report Settings			*	192.168.2.0/24	0.0.0.0	trust	с	0	Root	-		
$\Gamma \vdash$	Binding	≡	* ۵	ctiv	/e route C Conne	cted I Impo	orted	eB EBGP (	O OSPF	E1 OSP	F external typ	be 1	
	DNS				S Static	A Auto	-Exported	ib Ibgp f	R RIP	E2 OSP	F external typ	)e 2	
	Zones Interfaces												
	DHCP	_											
	PPPoE												

Note: About 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 setup a static IP address for untrust interface, please switch to Network -> Routing -> Routing Entries to edit a default Gateway IP address. In this example, my Gateway IP address is 167.35.4.1.

( - Yeni	Networ	rk > Ro	outing > Routing Entri	es					ns
NETSCREEN' List route entries for All virtual routes The trust-virtual									
NS5GT		tru	ist-vr						
			IP/Netmask	Gateway	Interface	Protocol	Metric	Vsys	Configure
- Home +- Configuration		*	192.168.1.0/24	0.0.0.0	trust	с	0	Root	-
Network		*	167.35.4.0/24	0.0.0.0	untrust	С	0	Root	-
- Binding - DNS		*	0.0.0.0/0	167.35.4.1	untrust	s	1	Root	Remove
- Zones			* Active route C Co	nnected I Im	ported	eB EBGP O C	OSPF E1	OSPF ext	ternal type 1
<ul> <li>Interfaces</li> </ul>			SSt	atic A Au	to-Exported	IB IBGP R F	UP E2	OSPF ext	ternal type 2
- PPPoE									
E Routing									
<ul> <li>Routing Entries</li> <li>Source Routing</li> </ul>									
Virtual Routers									

5) To edit the IPSec rule, the sequence is building the gateway policy first and then edit the IKE policy. Please switch to VPNs > AutoKey Advanced > Gateway, and then press New button.

	VPNs > Auto	Key Advar	nced > Gateway			ns5gt 💡
					ļ	5 New
TREND SECURE						
NS5GT	Name	Туре	Address/ID/User Group	Local ID	Security Level	Configure
A			No entry av	vailable		
- Home						
- Network						
- Binding						
_ Zones						
- DHCP						
- PPPoE						
Routing						
Source Routing						
Virtual Routers						
Untrust Failover						
±- Screening						
- VPNs						
- AutoKey IKE						
AutoKey Advanced						
D1 Proposal						
– P2 Proposal						
- XAuth Settings						
- VPN Groups						
+ L2TP						

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

Gateway Name	ToZyWALL					6
Security Level	🔘 Standard	🔘 Compa	tible	🔘 Basic	⊙ Custom	
Remote Gateway Type						
Static IP Address		IP .	Addres	s/Hostname	210.110.7.1	
O Dynamic IP Address				Peer IC		
🔿 Dialup User				User	None 🗸	
🔿 Dialup User Group				Group	None 🖌	
				. –	1	
Preshared Key	•••••		Use	As Seed 📃		
Local ID		(optior	nal)			
Outgoing Interface	untrust 🐱					
	ОК	Cancel	A	dvanced		

7) On Security Level settings, we can set up phase 1 proposal. In this example, 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 O Standard O Co User Defined O Custom	ompatible	O Basic
Phase 1 Proposal		
pre-g1-des-md5	None	<u> </u>
None	None	~
Mode (Initiator	) 💿 Main	(ID Protection) O Aggressive
Enable NAT-Traversal UDP Checksum	n 🗖	
Keepalive Frequency	<b>/</b> 5	Seconds (0~300 Sec)
Heartbeat		
Hello	0	Seconds (0~3600 Sec)
Reconnec	t O	Seconds (60~9999 Sec)
Threshold	15	
<ul> <li>None</li> <li>XAuth Server</li> <li>Use Default</li> </ul>		

8) We can see an IKE rule on the page after the pervious settings.

Э	Configure	Security Level	Local ID	Address/ID/User Group	Туре	Name
ve	Edit Remov	Custom	-	210.110.7.1	Static	ToZyWALL
nc	Edit Ren	Custom	-	210.110.7.1	Static	ToZyWALL

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

	١	/PNs > AutoKey Ik	(E			ns5gt 👔
NetScreen.						<b>9</b>
NS5GT		Name	<u>Gateway</u>	Security	Monitor	Configure
Home				No entry available		

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

VPN Name	ToZyWALL IPSec			10
Security Level 🔾	Standard 🛛 🔿 Compa	atible 🔘 Basic	⊙ Custom	
Remote Gateway 📀	Predefined	ToZyWA	Ш 🗸	
0	Create a Simple Gatev	vay		
	Gateway Name			
	Туре	⊙ Static IP Ad	dress/Hostname	
		🔘 Dynamic IP	Peer ID	
		🔘 Dialup User	User Nome 🗸	
		🔿 Dialup Group	Group None 🗸	
	Local ID		optional)	
	Preshared Key		Use As Seed	
	Security Level	💿 Standard 💦 🤇	🔾 Compatible 💦 🔘 Ba	asic
	Outgoing Interface	untrust 🐱		
	ОК Са	ancel Advanc		

11) On Security Level settings, choose User Defined option, 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, thus you can monitor your VPN tunnels. Then, press Return button, and press OK button on next page to save the settings.

Security Level					
Predefined (	🔵 Standard  🔘	Comp	oatible 🔘 Bas	ic	
User Defined (	● Custom				11
	Phase 2 Proposa	al			
	nopfs-esp-des-sha	*	None	~	
	None	¥	None	~	
			L		
Replay Protection [					
Transport Mode [	🗌 (For L2TP-over	-IPS	ec only)		
	<b></b>				
Bind to (	• None				
C	UTunnel Interfac	3			none 🗸
C	) Tunnel Zone				Untrust-Iun 👻
Proxy-ID	<b>•</b>				
Local IP / Netmask	192.168.2.0	1	24		
Remote IP / Netmask	192.168.1.0	1	24		
Service	ANY		~		
VPN Group 1	None 👻				Weight 0
VPN Monitor	<b>~</b>				
Source Interface	default 🐱				
Destination IP	0.0.0.0				
Optimized [					
Rekey [					
	Return Cano	el			

12) After the settings, the VPN IKE page will show an IPSec rule on the page.

Name	<u>Gateway</u>	Security	Monitor	Configure	12
ToZyWALL IPSec	ToZyWALL	Custom	On	Edit	-

13) Switch to Policies to set up policy rules for VPN traffic. To choose From to Trust, and To to Untrust (it means from LAN to WAN), and then press New button to edit the policy rules.

	Poli	cies (From 1	rust To Untrust)							nst	igt	?
- EN	List	20 🔽 per	page							13	Sear	ch
NETSCREEN"	Fro	rom Trost V Go New										
UTREND SECURE		From Trust To Listaust, total policy: 1										
NS5GT	FI FI	om Trust To	o Ontrust, total	policy: 1	1							_
	I	O Source	Destination	Service	Action	Options		Config	jure	Enable	Move	
+ Configuration	1	. Any	Any	ANY			<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	2	φ 👐	-
+ Network + Screening Policies - VPNs												-

14) Give a name for this policy, for example "VPN". On Source Address, you should set up Local LAN IP addresses. In this example, select New Address option, and type 192.168.2.0 / 255.255.255.0 on the text box. On Destination Address, you should set up remote IP addresses. In this example, select New Address option, and type 192.168.1.0 / 255.255.255.0 on the text box. Select Action to Tunnel, and select ToZyWALLIPSecVPN rule. Check Modify matching bidirectional VPN policy check box, it means that you can create/modify the VPN policy for the opposite direction. Then, press OK button to save your settings.



15) After the settings, the new policy rules will display in the **Policies** page.

	Po	licies (From All zones To All z	cones)					ns	5gt	?
NETSCREEN DITREND SECURE	Lis Fro	t 20 v per page om All zones v	T	To All zone	s 🔽 (	Go	15 Search New			
NS567	Promitrust to ontrust, total pointy. 2									
Home	ID	Source	Destination	Service	Action	Options		Config	jure	Enable
+ Configuration	1	Any	Any	ANY	<b>V</b>		<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	
▪ Network ▪ Screening	з	192.168.2.0/255.255.255.0	192.168.1.0/255.255.255.0	ANY	< <b>ii</b> >		<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	•
- Policies	Fro	m Untrust To Trust, total po	licy: 2							
±-Objects	ID	Source	Destination	Service	Action	Options		Config	jure	Enable
+ Reports + Wizards	2	Any	Any	ANY	Ø		<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	N
÷ Help Logout	4	192.168.1.0/255.255.255.0	192.168.2.0/255.255.255.0	ANY	< <b>8</b>		<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	V

16) Move the add policy rules to top, thus the VPN policies will be checked first.

Pol	icies (From All zones To All z	rones)					ns	5gt	?	
Lis Fro	t 20 vperpage om All zones v	Т	o All zone	s 🔽 🤇	Go		<b>16</b>	Sear	ch Jew	
Fro	From Trust To Untrust, total policy: 2									
ID	Source	Destination	Service	Action	Options		Config	jure	Enable	
	192.168.2.0/255.255.255.0	192.168.1.0/255.255.255.0	ANY	¢ <b>8</b> \$		<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	•	
1	Any	Any	ΑΝΥ	<b>Ø</b>		<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	•	
Fro	m Untrust To Trust, total po	licy: 2			,					
ID	Source	Destination	Service	Action	Options		Config	lure	Enable	
	192.168.1.0/255.255.255.0	192.168.2.0/255.255.255.0	ANY	¢ <b>8</b> \$		<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	•	
2	Any	Any	ΑΝΥ	Ø		<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	~	

17) Ping the remote host and switch to VPNs > Monitor Status to check the VPN link status; if the **Link** status is Up means the VPN tunnel between ZyWALL and NetScreen had been successfully built-up.

	VPNs > Monitor Status					nst	igt ?
	List 🙎 🖌 per page				17	Show Al	I Filter
NS5GT	VPN Name	SA ID	Policy ID	Peer Gateway IP	Туре	SA Status	Link
Hama	ToZyWALL IPSec	00000006	4/3	210.110.7.1	AutoIKE	Active	Up
Configuration Network Screening Policies VPNs AutoKey IKE AutoKey KE AutoKey KE Manual Key LIZP Monitor Status							

#### 1.2.2.3 ZyWALL with SonicWall VPN Tunneling

This page guides how to setup a VPN connection between the ZyWALL 1050 and SonicWall TZ170.

As the figure shown below, the tunnel between Central and Remote offices ensures the packet flows 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 SonicWall are explained in the following sections.



The central office gateway ZyWALL1050's interface and VPN setting retain the same setting as pervious example; if you are first jumping this section please refer to page8 ZyWALL1050 to ZYWALL70 VPN tunnel setting:

I made a list to briefly show the VPN phase1 and phase2 configuration parameter as below.

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

All contents copyright (c) 2006 ZyXEL Communications Corporation.

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

- 1) Please configure the ZyWALL1050 's VPN gateway and VPN connection as the list and please remember to configure the policy route for VPN traffic routing. User can refer to pervious scenario or user guide to setup the ZyWALL1050 VPN setting.
- Using a web browser, login SonicWall by giving the LAN IP address of SonicWall in URL field. The default username and password is admin/password.
- Switch to menu Network > Inetrfaces and configure the WAN/LAN IP address to WAN: 167.35.4.3 LAN: 192.168.2.1/24.

SONICWALL	1.	COMPREHENSIVE INTI	ERNET SECURITY*					3
System Network	Network	> Interfaces				Setup Wizard.	. Clear Sta	atistics ?
🕿 Interfaces 🖿 WAN Failover & LB	Interface	Settings						
💼 Zones	Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
DNS	LAN	LAN	192.168.2.1	255.255.255.0	Static	100 Mbps full-du	plex Default LAN	20
Address Objects	WAN	WAN	167.35.4.3	255.255.255.0	Static	100 Mbps full-du	plex Default WAN	Ň
NAT Policies	OPT	Unassigned	0.0.0.0	0.0.0.0	N/A	No link		20
🖿 ARP								
DHCP Server								
🛅 IP Helper								

 Switch to VPN > Settings, check Enable VPN check box, and then press Add button, it will bring up for VPN settings. (Note: The VPN Policy Wizard is an alternative way to set up VPN rules as well.)

System						
Network	VPN > Settings			VPN Policy Wizard	Apply	Cancel ?
SonicPoint						
Firewall	VPN Global Settings					<b>_</b>
VoIP VPN	Enable VPN					-
🕿 Settinas	Unique Firewall Identifier: 0006B10418D	8				
Advanced					_	
DHCP over VPN	VPN Policies				Items 1	to 2 (of 2) 🕅 🗸 🕨 🕄
L2TP Server						
	📕 # Name	Gateway	Destinations	Crypto Suite	Enable	Configure
	1 WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)		۵ 🗑 😼
	2 WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)		۵ 🗑 🎸
	Add Delete					Delete All
	Site To Site Policies: 0 Policies Defined, 0	Policies Enable	d, 2 Maximum Poli	icies Allowed		

5) Click General tab, on Security Policy settings, give a name to this policy. In this example, type ToZyWALL. IPSec Primary Gateway Name or Address is the ZyWALL's WAN IP Address (remote gateway IP address). In this example, please type 210.110.7.1 on IPSec Primary Gateway Name or Address text box. Then, enter the key string 123456789 on Shared Secret text box.

General	Network	Proposals	Advanced				
Security Po	olicy						5
IPSec Keying N	Node:		IKE using F	Preshared Sec	cret 💌		
Name:			ToZyWALL				
IPSec Primary Gateway Name or Address:			210.110.7.1				
IPSec Second:	ary Gateway Nam	ne or Address:					
Shared Secret	:		123456789				
Local IKE ID (o	ptional):	IP Address	~				
Peer IKE ID (oj	ptional):	IP Address	~				
Roady							
Reduy			_				
				OK	Cancel	Н	elp

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, thus we have to create a new address object from remote network drop down list and the new address object window will popup.

General Network Proposals Advanced
Local Networks 6
<ul> <li>Choose local network from list LAN Subnets</li> <li>Local network obtains IP addresses using DHCP through this VPN Tunnel</li> <li>Any address P</li> </ul> Destination Networks <ul> <li>Use this VPN Tunnel as default route for all Internet traffic</li> </ul>
<ul> <li>Destination network obtains IP addresses using DHCP through this VPN Tunnel</li> <li>Choose destination network from list         <ul> <li>Select Remote Network</li> <li>Create new address object</li> <li>Create new address group</li> </ul> </li> </ul>
Ready
OK Cancel Help

7) The name for this object can be "Remote\_Subnet"; the Network IP Address and Subnet Mask are remote site LAN subnet. In this example, please type 192.168.1.0 on Network text box and then type 255.255.255.0 on Subnet Mask text box, and then press OK button. We can select the new address object "Remote\_Subnet" from destination network drop down list after the address object successfully setup.
| 🚰 http://167.35.4.3 - Add Address Object - Mi 📃 🗖 🔀 |               |  |
|---|---------------|--|
|   | - 7           |  |
| Name:   | Remote_Subnet |  |
| Zone Assignment:                                    | VPN 💌         |  |
| Туре:   | Network 💌     |  |
| Network:  | 192.168.1.0   |  |
| Netmask:  | 255.255.255.0 |  |
|   |               |  |
| Ready   |               |  |
|   | OK Cancel     |  |

8) Switch to Proposals tab, on IKE (Phase1) proposal settings, select Main mode, DH Group to Group1, Encryption to DES and Authentication to MD5. On IPSec (Phase2) proposal settings, select ESP Protocol, Encryption to DES and Authentication to SHA1. Then, press OK button on this page.

General Network P	oposals Advanced				
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 Secrec					
DH Group:	Group 2				
Life Time (seconds):	28800				
Ready					
	OK Cancel Help				

 Switch to Advanced tab, on VPN policy bound to setting, select Interface WAN. Then, press OK button on this page.

General	Network	Proposals	Advanced			
Advanced	Advanced Settings					9
🗌 Enable Ke	Enable Keep Alive					
📃 Suppress	automatic Acces	ss Rules creatio	n for VPN Policy			
📃 Require a	uthentication of V	/PN clients by XA	UTH			
User grou	p for XAUTH use	rs:Select	a user group	~		
📃 Enable Wi	ndows Networki	ng (NetBIOS) Bro	padcast			
📃 Enable Mu	Ilticast					
📃 Apply NAT	Apply NAT Policies					
Translated	d Local Network:	Select	Translated Loca	al Network	~	
Translated	d Remote Netwo	rk:Select	Translated Rem	ote Network-		
Management v	ia this SA:		P 🗌 HTTPS			
User login via t	this SA:		P 🗌 HTTPS			
Default LAN G	ateway (optional)	):				
VPN Policy bou	und to:	Interfac	e WAN 🔽			
Ready						
			_			
				OK	Cancel	Help

10) The VPN status page will show a new VPN rule and please make sure the rule had been enabled.

VPN Policies			Items 1	to 3 (of 3)	10
🔳 # Name	Gateway	Destinations	Crypto Suite	Enable	Configure
1 WAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)		🏷 🗑 🖗
2 WLAN GroupVPN			ESP 3DES HMAC SHA1 (IKE)		۵ 🗑 🎸
3 ToZWVALL	210.110.7.1	192.168.1.1 - 192.168.1.255	ESP DES HMAC SHA1 (IKE)		6 🎸
Add Delete					Delete All

11) Ping the remote host to dial up the tunnel. We can check the connected VPN status in the VPN status page. The VPN tunnel should be appeared in the Currently Active VPN Tunnels page and it indicated the tunnel had been successfully built-up.

VPN Policies				Items 1	to 3 (of 3)	K A D K
🔳 # Name	Gateway	Destinations	Crypto Suite		Enable	- 11 comigare
1 WAN GroupVPN			ESP 3DES HMAC SH	A1 (IKE)		👌 🗑 🖗
2 WLAN GroupVPN			ESP 3DES HMAC SH	A1 (IKE)		🏼 🥹 🗑 🔗
3 ToZyWALL	210.110.7.1 🤇	192.168.1.1 - 192.168.1.255	ESP DES HMAC SHA	1 (IKE)	<b>~</b>	80 🕅
Add Delet	te					Delete .
Site To Site Policies: 1 Policie GroupVPN Policies: 2 Policies	s Defined, 1 Policies Enabled s Defined, 0 Policies Enabled,	, 2 Maximum Policies Allowed 6 Maximum Policies Allowed				
Currently Active VPN	Tunnels			Items 1	to 1 (of 1)	
# Name Lo	ocal	Remote	Gateway			
1 ToZyWALL 19	2.168.2.1 - 192.168.2.255	192.168.1.1 - 192.168.1.25	5 210.110.7.1	Renego	tiate	₩ ⇔
1 Currently Active VPN Tunnels	3					

# **1.3 Replacing Costly RAS Dial-in**

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

The most often applications scenario will like; an employee on the road, aka teleworker, can gain full network access simply by tapping into an Internet connection and this connection also provide the confidentiality during data transmitting between remote and host (Data transferring in VPN tunnel with encryption).

The other genius solution like "Mobile office" enabler: teleworker or home & SOHO employee can work at airport, cyber café, hot spots, hotel or home. The office building scope can be eliminated and the one global office can fully utilize the global resource.

### 1.3.1 Remote Access VPN

In this scenario, we assume the ZyWALL1050 admin configure VPN setting to allow teleworkers access internal network resource through remote access VPN. Since we don't know which IP address will be at the remote teleworker's PC/notebook, so we will use 0.0.0.0 which represents "any IPs" for ZyWALL1050's remote gateway setting. On the other hands, the teleworkers use ZyWALL VPN client on his notebook to establish IPSec VPN with main office.



So we are going to complete following tasks.

- Create object 'address' for local and remote network on ZyWALL1050
- Configure a VPN gateway and the VPN connection setting on ZyWALL1050
- Configure the corresponding VPN setting in ZyWALL VPN client

ZyWALL 1050	ZyWALL VPN Client
My address: ge2(10.59.1.45)	My address: Any
Secure gateway address: 0.0.0.0	Secure gateway address: 10.59.1.45
Local: 192.168.2.0/24	Local: Any
Remote: 0.0.0/24	Remote: 192.168.2.0/24
Phase 1	Phase 1
Negotiation Mode : Main	Negotiation Mode : Main
Pre-share key: 123456789	Pre-share key: 123456789
Encryption :DES	Encryption :DES
Authentication :MD5	Authentication :MD5
Key Group :DH1	Key Group :DH1

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

See configuration step by step as following.

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

Name	subnet2
Address Type	SUBNET 💌
Network	192.168.2.0
Netmask	255.255.255.0
	OK Cancel

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

Name	VPNclient
Address Type	HOST 🔽
IP Address	0.0.0

3) Go to **Configuration** > **Network** > **IPSec VPN** > **VPN Gateway** to create gateway for remote VPN client. Because this kind of VPN is initialed from remote user, the **Secure Gateway** should be put as dynamic one which is 0.0.0.0. Also VPN peers should keep consistence with each other for other parameter, such as Pre-Shared Key, ID Type, Encryption and Authentication proposal and so on.

VPN Gateway Name	remoteaccess
IKE Phase 1	
Negotiation Mode Proposal	Main 🔽
· · · F · · · ·	# Encryption Authentication 🖻
	1 DES 💙 MD5 💙 💼
Key Group	DH1 🗸
SA Life Time (Seconds)	86400 <180 - 3000000 >
NAT Traversal	
Dead Peer Detection (DPD)	
Duran autor	
Property	
My Address	
<ul> <li>Interface</li> </ul>	ge2 M DHCP client 10.59.1.45/255.255.255.0
🔿 Domain Name	
Secure Gateway Address	1. 0.0.0.0
	<b>2.</b> 0.0.0.0
Authentication Method	
● Pre-Shared Key	123456789
○ Certificate	(See <u>My Certificates</u> )
Local ID Type	
Content	0.0.0.0
Peer ID Type	Any 💌
Content	
Extended Authentication	
Enable Extended Authentication	
-	
age Ready	

4) Go to **Configuration** > **Network** > **IPSec VPN** > **VPN Connection**, to create a VPN rule. Put **Policy** as those defined in step 1 and step2. Remote policy should be dynamic host address. We put **VPN Gateway** as dynamic which has been defined in step3.

VPN Connection		
Connection Name	remoteaccess	
VPN Gateway		
Name	remoteaccess Add New VPN Gateway	
Phase 2		
Active Protocol Encapsulation Proposal	ESP 💌 Tunnel 💌	_
FICHUSAI	#     Encryption     Authentication       1     DES     MD5     V	€
SA Life Time (Seconds) Perfect Forward Secrecy (PFS	86400 (180 - 3000000)	
Policy		
Policy Enforcement		
Local policy	subnet2 Y SUBNET, 192.168.2.0/24	
Remote policy	VPNclient Y HOST, 0.0.0.0	
Property		
Nailed-Up Enable Replay Detection Enable NetBIOS broadcast	over IPSec	
Inbound/Outbound traffic Na	Т	
Outbound Traffic Source NAT So De	irce 💙	
age Ready.		

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

Security Policy Editor - ZyWALL VPN Cl	ient 🔲 🗖 🔀
File Edit Options Help	
Network Security Policy Network Security Policy My Connection New Connection Security Policy New Connection Security Policy New Connection Security Policy Ny Identity Security Policy Proposal 1 Security Proposal 1 S	Connection Security Secure Non-secure Block Remote Party Identity and Addressing ID Type IP Address Range From: 192.168.2.05 To: 192.168.2.255 Protocol All Port Vuse Secure Gateway Tunnel Conly Connect Manually Conly Connect Manu
	Click here to find out about program add-ons.

Under **My Identity** we select local **ID type** as Any.

File Edit Options Help		
Network Security Policy  My Connections  My Identity  Security Policy  Authentication (Phase 1)  Proposal 1  Key Exchange (Phase 2)  Proposal 1  Other Connections	My Identity Select Certificate None ID Type IP Address Any Secure Interface Configuration Virtual Adapter	Pre-Shared Key

Also please do not forget to enter Pre-Shared Key by clicking **Pre-Shared Key** button.

Z Security Policy	y Editor - ZyWAL	L VPN Client	×
File Edit Options	Help		
			ZR
Network Security F	Policy		
	Pre-Shared Key	Enter Pre-Shared Key (at least 8 characters) This key is used during Authentication Phase if the Authentication Method Pronosal is "Pre-Shared key"	re-Shared Key
Other Conr		OK Cancel	
		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, VPN connection should be initialed from this host site.

Security Policy Editor - ZyWALL VPN Clin File Edit Options Help	ent 🔲 🗆 🔀
File Edit Options Help Network Security Policy My Connection New Connection My Identity Security Policy Authentication (Phase 1) Proposal 1 Connections Proposal 1 Other Connections	Authentication Method and Algorithms          Authentication Method         Pre-Shared Key         Encrypt Alg         DES         Hash Alg         MD5         Seconds         SA Life         Seconds         Key Group         Diffie-Hellman Group 1
Connections	Authentication Method         Pre-Shared Key         Encryption and Data Integrity Algorithms         Encrypt Alg         DES         Hash Alg         MD5         SA Life         Seconds         Key Group         Diffie-Hellman Group 1

■ × I III Network Security Policy	ZS
My Connections     My Connection     My Identity     Security Policy     Authentication (Phase 1)     Proposal 1     Key Exchange (Phase 2)     Proposal 1     Other Connections	IPSec Protocols Seconds KBytes SA Life Seconds 28800 Compression None Encrypt Alg DES Hash Alg MD5 Encapsulation Tunnel
	Authentication Protocol (AH) Hash Alg SHA-1 Encapsulation Tunnel

The CLI command 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 VPN connection.
- 4. The Local and Peer ID type and content must opposite not in the same content.
- 5. The Local Policy of ZyWALL 1050 should be 'dynamic single host with the value
- 0.0.0.0. And VPN tunnel should be initialed from 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 type of VPN topology which can meet the needs of organizations of any size.

ZyWALL1050 VPN Topology supported fully meshed topology that can be deployed when the total number of remote site is few. Star topology is recommended when the total number of remote site is huge and even more flexible design; Star and Mesh mixed topology (cascading topology) can be deployed while in a global distributed environment.



### 1.4.1 Fully Meshed Topology

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

Tunnel 1: London ←VPN →Madrid

Tunnel 2: London ←VPN →Paris

Tunnel 3: London ←VPN →Hannover

Tunnel 4: London ←VPN →Oslo

Tunnel 5: Madrid  $\leftarrow$  VPN  $\rightarrow$  Paris

Tunnel 6: Madrid  $\leftarrow$  VPN  $\rightarrow$  Hannover

Tunnel 7: Madrid  $\leftarrow$  VPN  $\rightarrow$  Oslo

Tunnel 8: Paris ←VPN → Hannover

Tunnel 9: Paris  $\leftarrow$  VPN  $\rightarrow$  Oslo

Tunnel 10: Hannover  $\leftarrow$  VPN  $\rightarrow$  Oslo

3) Please refer to the section ZyWALL1050 to ZyWALL1050 VPN tunnel configuration steps to build up the 10 tunnels in turn. We will introduce the configuration steps for VPN concentrator that will greatly help to reduce the total number of tunnel.

### 1.4.2 Star Topology



The ZyWALL1050 support Star topology via the VPN concentrator feature. The VPN concentrator can help to reduce the VPN tunnel numbers and 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 headquarter in Taiwan and other office around the world.

This company decided to build up a VPN concentrator let all office's internal network to share and connecting to each other 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 destination office's internal network.

Remote Office	HQ	
WAN: 10.59.1.11		
~		
WAN: 10.59.1.17	WAN: 10.59.1.10	
LAN: 192.168.101.0/24	LAN: 192.168.100.0/24	
~		
LAN: 192.168.119.0/24		
	WAN	52

WAN

#### The VPN configuration parameter

All contents copyright (c) 2006 ZyXEL Communications Corporation.

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

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

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

onfigur	ation			
#	Name	Туре	Address	Ð
1	HQ_SUBNET	SUBNET	192.168.100.0/24	<b>B</b> 🗇
2	VPN_REMOTE_SUBNET	SUBNET	192.168.1.0/24	BÝ 🖻
3	DMZ_SUBNET	SUBNET	192.168.200.0/24	e in the second s
4	VPN_visitor_pc	HOST	192.168.1.33	e de la companya de l
5	Trainer_PC	HOST	10.59.1.18	e de la companya de l
6	LAN_SUBNET	SUBNET	192.168.101.0/24	e de la companya de l
7	DE_SUBNET	SUBNET	192.168.102.0/24	BÝ 🖻
8	CZ_SUBNET	SUBNET	192.168.103.0/24	BÝ 🖻
9	UK_SUBNET	SUBNET	192.168.104.0/24	BÝ 🖻
10	FR_SUBNET	SUBNET	192.168.105.0/24	e de la companya de l
11	SE_SUBNET	SUBNET	192.168.106.0/24	e în
12	DK_SUBNET	SUBNET	192.168.107.0/24	<b>B</b> Ý 🛍

Configure the NL site address object for each remote office subnet

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

Group Members		
Name	RemoteOfficeVPN	
Description		
#	Member	÷
1	Object/UK_SUBNET 🗖	🖳 🗇
2	Object/DE_SUBNET	🔁 💼
3	Object/CZ_SUBNET 🗖	🔁 🖮
4	Object/HQ_SUBNET 🗖	<b>₽</b> 💼
5	Object/DK_SUBNET 🗖	🔁 🗰
6	Object/FR_SUBNET 🗖	🖳 💼
7	Object/SE_SUBNET	🖳 💼
	OK Cancel	

The screen shot below is the NL site VPN Gateway status page.

#         Name         My address         Secure Gateway         VPN Connection           1         ZyWALL2PLUS_VPN         0.0.0.0         10.60.1.10, 0.0.0.0         ZyWALL2PLUS_CONN	VPN Connection VPN Gateway Concentrator SA Monitor Configuration						
1         ZyWALL2PLUS_VPN         0.0.0.0         10.60.1.10, 0.0.0.0         ZyWALL2PLUS_CONN         凌 ☞           2         NL_HQ         0.0.0.0         10.59.1.10, 10.58.1.10         NL_HQ_tunnel         豪 ☞	#	Name	My address	Secure Gateway	¥PN Connection	T	
2 NL_HQ 0.0.0 10.59.1.10, NL_HQ_tunnel 🕸 🗊 💼	1	ZyWALL2PLUS_VPN	0.0.0	10.60.1.10, 0.0.0.0	ZyWALL2PLUS_CONN	🖗 🗊 🖻	
	2	NL_HQ	0.0.0	10.59.1.10, 10.58.1.10	NL_HQ_tunnel	÷ 10	
Apply Reset							

### NL site VPN Connection status page

	Configuration						
	Total Connection: 2	2	30 💌 со	nnection per	page	Page 1/1	
#	Name	¥PN Gateway	Encapsulation	Algorithm	Polic	/	÷ <b>r</b>
1	ZyWALL2PLUS_CONN	ZyWALL2PLUS_VPN	TUNNEL	DES/SHA	LAN_SUBNET/VPN_R	EMOTE_SUBNET	🖗 <b>5</b> ° 🗊 - 300
2	NL_HQ_tunnel	NL_HQ	TUNNEL	DES/SHA	LAN_SUBNET/H	Q_SUBNET	🖗 <b>5</b> ° 🖻 -0=D-
Apply Reset							

NL site policy route for VPN traffic, this policy route is used to indicate the ZyWALL1050

send the packet to VPN tunnel.

) z	yWALL 1	050 > Con	figuration	> Policy > Ro	ute > Policy Route					
	Policy Ro	ute St	atic Route	1						
									_	
#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM	
1	any	none	any	LAN_SUBNET	RemoteOfficeVPN	any	NL_HQ_tunnel	none	0	🥸 🗗 🖳 🛅 🖻 N
2	Guest	none	any	any	any	any	WAN_TRUNK	outgoing- interface	100	🥸 🗗 🖳 🛅 🖻 N
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	🏘 🗗 🛱 🕷
					Apply	Reset				
								~		

#### HQ VPN concentrator configuration steps:

The next steps are introduced how to setup the VPN **concentrator** in HQ to route all remote site VPN traffic

The tunnel need to setup in HQ ZyWALL1050 is the amount of the remote sites.

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

Please refer to below table for the HQ VPN tunnel setting

Remote Office	HQ
WAN: 10.59.1.11	
~	
WAN: 10.59.1.17	WAN: 10.59.1.10
LAN: 192.168.101.0/24	LAN: 192.168.100.0/24
~	
LAN: 192.168.119.0/24	
Phase 1	Phase 1
Negotiation Mode : Main	Negotiation Mode : Main
Pre-share key: 123456789	Pre-share key: 123456789
Encryption :DES	Encryption :DES
Authentication :MD5	Authentication :MD5

All contents copyright (c) 2006 ZyXEL Communications Corporation.

Key Group :DH1	Key Group :DH1
Phase2	Phase2
Encapsulation: Tunnel	Encapsulation: Tunnel
Active Protocol: ESP	Active Protocol: ESP
Encryption: DES	Encryption: DES
Authentication: SHA1	Authentication: SHA1
Perfect Forward Secrecy (PFS): None	Perfect Forward Secrecy (PFS): None

Setup the remote office subnets address objects for the further VPN setting.

Configur	ation			
#	Name	Туре	Address	÷
1	LAN_SUBNET	SUBNET	192.168.100.0/24	e de la companya de l
2	VPN_REMOTE_SUBNET	SUBNET	192.168.1.0/24	e de la companya de l
3	DMZ_SUBNET	SUBNET	192.168.200.0/24	e de la companya de l
4	VPN_visitor_pc	HOST	192.168.1.33	<b>e</b>
5	Trainer_PC	HOST	10.59.1.18	e e e e e e e e e e e e e e e e e e e
6	NL_SUBNET	SUBNET	192.168.101.0/24	e di se di s
7	DE_SUBNET	SUBNET	192.168.102.0/24	<b>B</b> 🗇
8	CZ_SUBNET	SUBNET	192.168.103.0/24	<b>B</b> 🗇
9	UK_SUBNET	SUBNET	192.168.104.0/24	<b>B</b> 🖬
10	FR_SUBNET	SUBNET	192.168.105.0/24	<b>B</b> 🗇
11	SE_SUBNET	SUBNET	192.168.106.0/24	<b>B</b> 🗇
12	DK_SUBNET	SUBNET	192.168.107.0/24	<b>B</b> 🗇

Setup the HQ VPN Gateway for all remote sites

#	Name	My address	Secure Gateway	VPN Connection	đ
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, 10.58.1.11	HQ_NL_tunnel	÷5° 🖻
3	HQ_DE	0.0.0.0	10.59.1.12, 10.58.1.12	HQ_DE_tunnel	÷ 1
4	HQ_CZ	0.0.0.0	10.59.1.13, 10.58.1.13	HQ_CZ_tunnel	÷ 1
5	HQ_UK	0.0.0.0	10.59.1.14, 10.58.1.14	HQ_UK_tunnel	÷ 1
6	HQ_FR	0.0.0.0	10.59.1.15, 10.58.1.15	HQ_FR_tunnel	÷ 1
7	HQ_SE	0.0.0.0	10.59.1.16, 10.58.1.16	HQ_SE_tunnel	÷ 1
8	HQ_DK	0.0.0.0	10.59.1.17, 10.58.1.17	HQ_DK_tunnel	÷ 10
					-

Setup the HQ VPN connection for all remote sites

	Total Connection: 8	3	30 💌 co	Innection per	rpage Page 1/1	
#	Name	VPN Gateway	Encapsulation	Algorithm	Policy	Ē
1	ZyWALL2PLUS_CONN	ZyWALL2PLUS_VPN	TUNNEL	DES/SHA	LAN_SUBNET/VPN_REMOTE_SUBNET	🥸 <b>5</b> ° 🖻 -0=D
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	🖗 <b>5</b> ° 🖻 -0=0
6	HQ_FR_tunnel	HQ_FR	TUNNEL	DES/SHA	LAN_SUBNET/FR_SUBNET	🖗 <b>5</b> ° 🖻 -0=0
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	∲§∕ @ ⊲•D

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

Switch to ZyWALL 1050 > Configuration > Network > IPSec VPN > Concentrator and then click the add icon to add a new concentrator.

Under concentrator edit page click the add icon to add VPN connection to join this concentrator. The VPN traffic can be routed by HQ once the VPN connection had been

added to the concentrator. User doesn't need to add any policy route to the VPN tunnel when this tunnel already included in the concentrator.

Group Members		
Name	RemotOfficeConcentrator	
#	Member	
1	IPSEC/HQ_DK_tunnel	<b>1</b>
2	IPSEC/HQ_SE_tunnel	₽ 🖮
3	IPSEC/HQ_FR_tunnel 🗖	₽ 面
4	IPSEC/HQ_UK_tunnel	₽ 面
5	IPSEC/HQ_CZ_tunnel	🖳 🏛
6	IPSEC/HQ_DE_tunnel 🗖	₽ 面
7	IPSEC/HQ_NL_tunnel	🔁 💼
	OK Cancel	

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

The VPN concentrator is design to route the remote site VPN traffic; user still need to setup the policy route for local subnet VPN traffic. For example, we only setup the VPN concentrator for HQ and remote site A & B then the A subnet can connect to B subnet but HQ subnet can't connect either A nor B subnet.

Thus, this depends on how customers want to deploy their Global VPN network. We can add follow policy route to let HQ subnet also can connect with all concentrator's remote subnet.

> Zy	WALL 1	050 > Conf	iguration :	> Policy > Ro	ute > Policy Route					
P	olicy Rou	ute Sta	tic Route							
#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM	ŧ,
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	👰 🗗 🔁 🖬 🖻 N
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	ару	none	ne1	IAN SUBNET	алх	арх	WAN TRUNK	outgoing-	n	ἅ≓∕⊞⇔⊾
	Messag	e Ready								

# **1.5 Internet Access via Central Gateway**

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

The scenario is to direct all outgoing traffic originated from branch office to main office so that network admin and control traffic or apply additional secure access control or inspection.



Main office – ZyWALL 1050	<b>Branch office – ZyWALL 70</b>
My Address: ge2, 10.59.1.55	My Address: 10.59.1.69
Security Gateway Address: 10.59.1.69	Security Gateway Address: 10.59.1.55

All contents copyright (c) 2006 ZyXEL Communications Corporation.

Local ID Type: IP, 1.1.1.1 Peer ID Type: IP, Any Local: Range, 0.0.0.0-255.255.255 Remote: Subnet, 192.168.1.0/24

> Phase 1 Negotiation Mode : Main Pre-share key: 123456789 Encryption :DES Authentication :MD5 Key Group :DH1

Phase2 Encapsulation: Tunnel Active Protocol: ESP

Encryption: DES

Authentication: SHA1

Perfect Forward Secrecy (PFS): None

Local ID Type: IP, 1.1.1.1 Peer ID Type: IP, 1.1.1.1 Local network: Subnet, 192.168.1.0/24 Remote network: Range, 0.0.0.0-255.255.255.255 Phase 1 Negotiation Mode : Main Pre-share key: 123456789 **Encryption** :DES Authentication :MD5 Key Group :DH1 Phase2 Encapsulation: Tunnel Active Protocol: ESP **Encryption: DES** Authentication: SHA1 Perfect Forward Secrecy (PFS): None

Thus, we are going to complete the tasks:

- Create object 'Address' for remote network ranging from 0.0.0.0 to 255.255.255 on ZyWALL1050
- Configure VPN gateway and connection setting on ZyWALL1050
- Configure the corresponding VPN setting on ZyWALL70

See the configuration step-by-step as following.

 Login ZyWALL 1050 GUI and go to Configuration > Object >Address to create an address object for all incoming traffic.

Name	wholerange	
Address Type	RANGE 💙	
Starting IP Address	0.0.0	
End IP Address	255.255.255.255	

All contents copyright (c) 2006 ZyXEL Communications Corporation.

2) Switch to Configuration > Network > IPSec VPN > VPN Connection > VPN Gateway to set VPN Gateway. Here we select 'ge2' as My Address. We put 10.59.1.69 for Security Gateway Address and 123456789 for Pre-Shared Key .Also IP with value 1.1.1.1 for ID Type. For other parameters, we remain them as default. There's no special settings for these parameters and the main concern is to let VPN peer match each other.

VPN Gateway	
VPN Gateway Name	remotesite
IKE Phase 1	
Negotiation Mode Proposal	Main # Encryption Authentication
Key Group SA Life Time (Seconds) □ NAT Traversal ☑ Dead Peer Detection (DPD)	DH1 V 86400 <180 - 3000000>
Property	
My Address ③ Interface ○ Domain Name Secure Gateway Address	ge2 Static 10.59.1.55/255.0.0.0 1. 10.59.1.69 2. 0.0.0.0
Authentication Method	
<ul> <li>Pre-Shared Key</li> <li>Certificate</li> <li>Local ID Type</li> <li>Content</li> <li>Peer ID Type</li> <li>Content</li> </ul>	123456789 (See <u>My Certificates</u> ) P 1.1.1.1 Any

3) Go back to **Configuration** > **Network** > **IPSec VPN** >**VPN Connection** to set VPN Connection. Here we choose the gateway which has been configured in the step2 as VPN gateway. Because such VPN tunnel is used for central site, we should specify **Local policy** as a range of 0.0.0.0-255.255.255.255. This range has been predefined in step1. So here we just select it in the drop down list. Here we suppose peer subnet as 192.168.1.x and select the default address object 'LAN\_SUBNET' to meet our requirement.

centralVPN		
remotesite V Add New VF ge2 centralVPN	'N Gateway	
ESP V Tunnel V		
# Encryption	Authentication	Ð
86400 (180 - 3000000) none 💌		
wholerange 🛛 RANGE, 0.0.0	.0 - 255.255.255.255	
LAN_SUBNET 💙 SUBNET, 192	.168.1.0/24	
r IPSec	hand	
	centralVPN         remotesite       Add New VF         ge2       centralVPN         ESP       Tunnel         #       Encryption         1       DES         86400       (180 - 3000000)         none       RANGE, 0.0.0         LAN_SUBNET       SUBNET, 192         r IPSec       IPSec	centralVPN         remotesite       Add New VPN Gateway         ge2 centralVPN         ESP         Tunnel         #       Encryption         Authentication         1       DES         86400       (180 - 3000000)         none       RANGE, 0.0.0.0 - 255.255.255.255         LAN_SUBNET       SUBNET, 192.168.1.0/24

			JU 🎽 connec	tion per pag	e Page	1/1
# 1	Name	¥PN Gateway	Encapsulation	Algorithm	Policy	€
1 ce	ntralVPN	remotesite	TUNNEL	DES/MD5	wholerange/LAN_SUBNET	Ţ <mark>ġ</mark> ₿°₫⊲₽⊳

The CLI command for application:

Address Object:

[0] address-object wholerange 0.0.0.0-255.255.255.255

```
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 10.59.1.69 0.0.0.0
[8] authentication pre-share
[9] keystring 123456789
[10] local-id type ip 1.1.1.1
[11] peer-id type any
```

```
[12] xauth type server default deactivate
[13] group1
VPN Connection:
[0] crypto map centralVPN
[1] ipsec-isakmp remotesite
[2] encapsulation tunnel
[3] transform-set esp-des-md5
[4] set security-association lifetime seconds 86400
[5] set pfs none
[6] policy-enforcement
[7] local-policy wholerange
[8] remote-policy 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
```

4) Go to GUI of ZyWALL 70 to configure VPN rule.

Go to Security >VPN to set IKE rules. We put 10.59.1.69 for My Address and 10.59.1.55

for Remote Gateway Address also 123456789 for Pre-Shared Key.

For other parameter we let them match those in the ZyWALL 1050.

Property		
Name	Central	1
Gateway Policy Information		
My Zy₩ALL		
<ul> <li>My Address</li> </ul>	10.59.1.69	(Domain Name or IP Address)
🔘 My Domain Name	None 🔽 (See DDNS)	
😡 Remote Gateway Address	10.59.1.55	
· ·		
Authentication Key		
Pre-Shared Key	123456789	
🔘 Certificate	auto_generated_self_signed_cert	(See <u>My Certificates</u> )
Local ID Type	IP 💌	
Content	1.1.1.1	
Peer ID Type	P	
Content	1.1.1.1	
Future de di Autobio esti esti esti		
Extended Authentication		
Enable Extended Authentication		
🔘 Server Mode	(Search <u>Local User</u> first then <u>RA</u>	IDIUS)
<ul> <li>Client Mode</li> </ul>		
User Name		
Password		
IKC PTOPOSal		

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

Property	
M Antina	
Name	central1
Protocol	
	<u> </u>
Allow NetBIOS Traffic Through IPSe	ec Tunnel
Check IPSec Tunnel Connectivity	Log
Ping this Address	0.0.0.0
Gateway Policy Information	
🐶 😪 Gateway Policy	Central 💌
Local Network	
C Address Type	Subpet Address 👽
Starting IP Address	
Ending IP Address / Subnet Mask	255 . 255 . 255 . 0
Local Port	Start 0 End 0
Remote Network	
ER3 Address Type	Range Address 💟
Starting IP Address	0.0.0.0
Ending IP Address / Subnet Mask	255 . 255 . 255 . 255
Remote Port	Start <sup>0</sup> End <sup>0</sup>
TDSec Dronosal	
Encapsulation Mode	Tunnel 💌
Active Protocol	ESP 💌
Encryption Algorithm	DES 💌
Authentication Algorithm	MD5 💌
SA Life Time (Seconds)	28800

### **Tips for application:**

- 1. Make sure the **Pre-Shared Key** is the same in local and remote gateway.
- 2. Make sure the **IKE proposal** is the same in local and remote gateway.
- 3. Select the correct Interface for VPN connection on ZyWALL1050.
- 4. The Local and Peer ID type and content must opposite not in the same content.
- 5. The **Local Policy** of ZyWALL1050 should be the range of 0.0.0.0-255.255.255.255 then

it can take the role as central center to control all the outgoing traffic from branch.

# 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 is very important for company and it will impact company a lot if the security policy didn't be considered and deployed well. We could say that it is a mandatory process to protect information assets.

For example, ZyCompany doesn't want their guest or vendor to be able to access their internal network but allow them to access Internet in case they have to get some information outside like access their company's email. So ZyCompany defines a security policy--outsider could use 'guess/guess1234'to access Internet through wireless access, but it's forbidden for them to access company's Internal resource, like talk to LAN PC, access with DMZ servers, or access to branch office's data through VPN's environment.

What your business can be benefited from deployment of security policy?

Deploy security policy well could not only protect company information asset, but also increase overall productivity, mitigate the impact of malicious application or misuse, and compliant with regulatory.

# 2.1 Managing IM/P2P Application

### 2.1.1 Why bother to manage IM/P2P applications?

Because some virus/exploits which may cause security breaches are transmitted via IM/P2P applications, manage IM/P2P application well could 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.

ZyWALL1050'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 cannot use P2P/IM while some employees are not allowed to use P2P all the time but could 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 over 200k. Besides, both 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

Let's see how to configure in ZW1050 step by step as following.

#### Step1. Create user/group object

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

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

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

fi	gure.	

User Group	Setting	Click '+' to add new user	
Configuration			
#	User Name	Description	
1	admin	Administration account	E to
2	Idap-users	External LDAP Users	<b>e b</b>
3	radius-users	External RADIUS Users	<b>B</b> 🗇

lser Name	Victor	
Jser Type	User	
🗸 Password	•••••	
Retype	•••••	
escription	Local User	
ease Time	1440	(0-1440 minutes, 0 is unlimited)
leauthentication Time	1440	(0-1440 minutes, 0 is unlimited)

Corresponding CLI commends 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 Group tab, create group 'Manager' and add member 'Victor' to it as the

following figure.

	anager		
ription Ma	anager group	Optional)	$\sim$
	Member	K	( 🗄 )
	User/Idap-use		<b>1</b>
n: 1 🔻 Page	1/2 D	-	
	OK	Cancel	
Group/exten	d		
User/John			
User/Peter			
User/Victor			
User/John User/Peter User/Victor			

4. Then press 'OK' button to complete the group creation.

Name	Manager		
Description	Manager group	(Optional)	
#	Me	mber	Ť
1	User/ <sup>1</sup>	Victor 🗖	<b>₽ m</b>

Corresponding CLI commends for your reference

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

5. Create two more group 'Engineer1' and Engineer2' to add 'Peter' and 'John' in through similar configuration.

Step2. Create schedule object

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

#	Name	Start Day/Time	Stop Day/Time	7
ecurring				~
#	Name	Start Time	Stop Time	<b>7</b> )

Configuration					
Name	IM_for_Engineer2				
Day Time					
Itom #	Day		Time		
item *	Year	Month	Day	Hour	minute
Start				18	00
Stop				22	00
Weekly					
Week Days	🗹 Monday 🛛 🗹 Ti 🗋 Sunday	uesday 🔽 Wedne	esday 🔽 Thur:	sday 🔽 Friday	🗆 🗆 Saturd

Corresponding CLI commends 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 perform further configuration.
| Conf | 050 > C<br>figurati | onfiguration            | > Policy > Ar | oplication Pat | rol > Configu | ration     |     |            |
|------|---------------------|-------------------------|---------------|----------------|---------------|------------|-----|------------|
| Ge   | eneral S            | etup<br>ble Application | Patrol        |                |               |            |     |            |
| Ge   | eneral P            | rotocols                |               |                |               |            |     |            |
|      | #                   | Service                 | Access        | Classify       | Exception     | BWM / kbps | Log | Modify     |
|      | 1                   | ftp                     | forward       | portless       | drop          | no         | no  | <b>* *</b> |
|      | 2                   | smtp                    | forward       | portless       | drop          | no         | no  | <b>*</b>   |
|      | 3                   | рор3                    | forward       | portless       | drop          | no         | no  | <b>*</b>   |
|      | 4                   | irc                     | forward       | portless       | drop          | no         | no  | <b>*</b>   |
|      | 5                   | http                    | drop          | portless       | forward       | no         | no  | <b>* *</b> |
| In   | stant M             | essenger                |               |                |               |            |     |            |
|      | #                   | Service                 | Access        | Classify       | Exception     | BWM / kbps | Log | Modify     |
|      | 1                   | msn                     | forward       | portless       | drop          | no         | no  | V B        |
|      | 2                   | aol-icq                 | forward       | portless       | drop          | no         | no  | 10 B       |
|      | 3                   | yahoo                   | forward       | portless       | drop          | no         | no  | <b>*</b>   |
|      | 4                   | 99                      | forward       | portless       | drop          | no         | no  | <b>*</b>   |

- 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 become 'Forward' automatically.
- 7. Click '+' to add two exceptions rules for 2 groups, Engineer2 and Manager, as the figure shown below.

Servi	ce						
◄	Enable Service						
Servio	ce Identification						
Nam Clas	ne ssification	msn @ Po	rt-less C Port-base	8			
Defau	Ilt Policy						
Acce Log Excep	ess Enable Bandwidth S <b>otion Policy</b>	Drop no haping 1	kbps				
Allo	w Port		Allow Port	Ē			
Acti	on: Forwa	ard					
#	Schedule	User	Source	ĺ.	estination	Log	Ð
1	IM_for_Engineer2	Engineer2	LAN_SUBNET	💌 any		🔹 no 💌	🔁 💼 🕅
2	none	Manager 💌	LAN_SUBNET	💌 any		• no •	⊕ m ⊳N
			ок	Cancel			

Corresponding CLI commends 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 in Policy Route

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

- 2. Create a new policy route rule by clicking '+' icon. And fill out the setting as the figure shown below.
- 3. Note that:

we choose user the group 'Engineer2' source from LAN subnet Schedule as what we just created named 'IM\_for\_Engineer2' From Next-Hop, choose 'Trunk' and choose 'WAN\_Trunk' from Trunk field. Input the maximum bandwidth is 100Kbps.

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

Configuration	
✓ Enable Description	M_access_by_Engineer2 (Optional)
Criteria	
User	Engineer2
Incoming	Interface / any Change
Source Address	LAN_SUBNET
Destination Address	any
Schedule	IM_for_Engineer2 💌
Service	any New
Next-Hop	
Туре	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)
	OK Cancel

Corresponding CLI commends 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 group 'Manager'. You will get the result as below after both rules are done.

P	olicy Rout	e Static Rout	e							
#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM	Ē
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 in IDP

- 1. First of all, make sure that you've registered and enable IDP function from menu Registration.
- 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.

eneral Prof	le Custom Signatures	Update			
acket Inspecti	on Traffic Anomaly	Protocol Anom	ialy		
Name	IM_P2P			Swit	tch to query view
gnature Group					
	Service 🛆		Activation	Log	Action
⊕ web_php			ø	log 💌	none 💌
• WEB_MISC	2		ଡ	orignal setting 💌	none
~~~~	~~~~~	$\sim\sim\sim\sim$	$\sim$	~~~~	~~~~
⊕ P2P			ø	log 💌	reject-both 💌
		the contract or show that	ø	log 💌	none
→ → → → → → → → → → → → → → → → → → →	~~~~~	~~~~	ୢୄୄ	orignal setting 💌	none 💌
			*	log 💌	reject-both 🔻
⊕ім					
⊕ IM ⊕ ICMP			ୁ ଜ	orignal setting 💌	none 💌
⊕ IM ⊕ ICMP ⊕ FTP			କ କ	orignal setting 💌	none 💌
<ul> <li>⊕ IM</li> <li>⊕ ICMP</li> <li>⊕ FTP</li> <li>⊕ FINGER</li> </ul>			ୁ କ କ	orignal setting	none

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

General Profile Custom Sign	atures Update			
General Setup				
🔽 Enable IDP				
Bindings				
Protected Zone	IDP Profile	.1	Activation 2	
LAN	LAN_IDP 🗖		🧟 🖌 💾	8
WAN	non	P	( @ <b>)</b>	
DMZ	DMZ_IDP	GoTo: 1 🔻	Page 1/2 🚺 D	
VPN_LAN	IDP_VPN_L		Duofilo	
VPN_DMZ	IDP_VPN_D	Please select one IDP	Prome.	
Registration Status		DMZ_ IDP VP	_IDP N DMZ	
Please go to the <u>Registration</u> page.		IDP_VP	N_LAN	
Registration Status: Licensed Registration Type: Trial			IDP	
4	Apply	ОК	Cancel	

# 2.2 Managing WLAN

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

Wireless network 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, it might be harmful under certain condition:

- People misuse People who you don't know might probe your AP and break you're your network without your permission. We usually called it "Wardriving". When you are using wireless link to transfer confidential data, those important data might be eavesdropped by the temper guy.
- 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 to allow outsides by pass the company's security checking and to access the company's confidential information or even use tools to damage the company's network service.

## 2.2.2 What can we do against wireless insecurity?

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



So we are going to complete following setting.

- 1. Create a VLAN interface dedicate 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 access granted

Step1. Create a VLAN interface dedicate for wireless access

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

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

Leave other fields as default and press 'ok' button	

☑ Enable Interface Name Port	vlan10 ge5
Virtual LAN Tag	10 (1-4094)
Description	VLAN10 for wireless zone (Optional)
P Address Assignment	
C Get Automatically	
O Use Fixed IP Address	
IP Address	192.168.10.1
Subnet Mask	255.255.255.0
Gateway	(Optional)
Metric	0 (0-15)
nterface Parameters	
Upstream Bandwidth	1048576 Kbps
Downstream Bandwidth	1048576 Kbps
МТО	1500 Bytes
HCP Setting	
DHCP	None
ing 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
C Ping this address	(Domain Name or IP Address)

## Step2. Define WLAN zones

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

ame	Wireless_Zone	
🗌 Block Intra-zone T	raffic	1-1
#	Member	Ē
1	IFACE/vlan10 🗖	🖳 💼
	OK Cancel	

Corresponding CLI commends 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**, to 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 packets from wireless network will be redirected to the authentication page.

11 725			-	
User Type		User		
Lease Time		1440	(0-1440 minutes, 0	is unlimited)
Reauthentication Time		1440	(0-1440 minutes, 0	is unlimited)
Jser Logon Setting				
Limit the number of simult	aneous logons for admin	istration account		
Maximum number per adm	inistration account	1	(1-1024)	
Limit the number of simult	aneous logons for access	s account		
Maximum number per acce	ss account	1	(1-1024)	
Icon Lockout Cotting				
_				
🗹 Enable logon retry limit			(10)	
Maximum retry count		5	(1-99)	
Lockout period		30	(1-65535 minutes)	
Jser Miscellaneous Settings				
Allow renewing lease time	automatically			
Enable user idle detection	,			
User idle timeout		3	(1-60 minutes)	
orce User Authentication Po	нсу			
Total Policy: 1	30 💌 F	olicy per page	Page 1/1	
# Schedule	Source	Destination	Authenticate	÷
1 none	Wireless	any	force 🧔	≸ 🖳 🗇 ▷N
/	Apply	Reset		
Configuration				
Configuration		wireless force author	(Option-II)	
Configuration		wireless_force_auther	) (Optional)	
Configuration Enable Description Authentication		wireless_force_auther	) (Optional)	
Configuration Enable Description Authentication Criteria		wireless_force_auther	) (Optional)	
Configuration Enable Description Authentication Friteria Source Address		wireless_force_auther force 💌	) (Optional)	
Configuration Enable Description Authentication Criteria Source Address Destination Address		wireless_force_auther force 💌 Wireless 💌 any 💌	) (Optional)	
Configuration Enable Description Authentication Fiteria Source Address Destination Address Schedule		wireless_force_auther force 💌 Wireless 💌 any 💌 none	) (Optional)	

Step4. Configure LDAP server information.

 Go to menu Object >> AAA server >> LDAP tab >> Default, configure the IP address, port and other necessary information. Click Apply button then.

onfiguration		
Host	192.168.105.155	(IP or FQDN)
Port	389 (165535)	
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		
	Apply	least 1

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

```
Corresponding CLI commends 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.



User	Group Setting		
Config	juration		1
#	User Name	Description	÷ l
1	admin	Administration account	B
2	Idap-users	External LDAP Users	B D
3	radius-users	External RADIUS Users	E D

4. For security concern, 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.

Jser Name	ldap-users	
User Type	Ext-User	<b>*</b>
Description	External LDA	PUsers
Lease Time	30	(0-1440 minutes, 0 is unlimited)
Reputhentication Time	30	(0-1440 minutes 0 is unlimited)

Corresponding CLI commends 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
```

Iser Name	ldap-employee
Jser Type	Ext-User
Description	External User
ease 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.

Name	default	
#	Method List	đ
1	group Idap	<b>9</b> m
2	local	₽ 亩
	OK Cancel	

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

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

C Authent Server Cert	: ticate Client Certificates tificate xt HTTP to HTTPS	443 (See <u>Trusted CAs</u> ) default ▼ (See <u>Mγ Ce</u>	ertificates)	
Admin Service	Control			
#	Zone	Address	Action	Ē
1	ALL	ALL	Accept	<b>ਡ ₽ ₪ №</b>
Jser Service C	Control			
#	Zone	Address	Action	Ē
1	ALL	ALL	Accept	🛒 🔁 🛍 🕅 🔊
Server Port		00		
Server Port Admin Service	Control	Address	Action	ħ
Server Port Admin Service # 1	Control Zone	Address	Action Accept	± F°⊈ mi⊳N
Server Port Admin Service # 1	Control Zone LAN Control	Address ALL	Action Accept	∄ डिं⊈ े №
Server Port Admin Service # 1 Jser Service C	Control Zone LAN Control Zone Zone	Address ALL Address	Action Accept Action	EF ∰ m ⊳N
Server Port Admin Service 1 Jser Service C # 1	Control Zone LAN Control Zone ALL	Address ALL Address ALL	Action Accept Action Accept	E° ⊈ m ⊳N E° ⊈ m ⊳N
Server Port Admin Service # Jser Service C # 1 thentication	Control Zone LAN Control Zone ALL	Address ALL Address ALL	Action Accept Action Accept	EF ∰ m DN EF ∰ m DN EF ∰ m DN
Server Port Admin Service 1 Jser Service C # 1 thentication Client Author	Control Zone LAN Control Zone ALL entication Method	Address ALL Address ALL default	Action Accept Action Accept	EF 및 m >N EF 및 m >N EF 및 m >N

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

- 1. Go to menu Network >> Firewall
- 2. Enable firewall and choose from zone "Wireless\_Zone" which 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
<ul> <li>Through-ZyWALL rules</li> <li>Zone Pairs</li> <li>All rules</li> <li>To-ZyWALL rules</li> </ul>
From Zone To Zone
O LAN O LAN
C DMZ O DMZ
Wireless_Zone     O Wireless_Zone
# Priority Schedule User Source Destination Service Access Log
Apply Reset Add

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

🗹 Enable		
From To	Wireless_Zone WAN	
Description	allow-employee-access (Opt	ional)
Schedule	none	
User	Idap-employee 💌	
Source	Wireless	
Destination	any	
Service	any	
Access	allow 💌	
Log	no	

Corresponding CLI commends for your reference

[0]	firewall 8
[1]	no schedule
[2]	user ldap-employee
[3]	sourceip Wireless
F / 1	no dogtinotionin

less [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 non-employee access from source "wireless network" to "any" in WAN.

6. After setting, you will see the result as the figure below. Click Apply button.

а 🟹 1	Enable Fire	wall symmetrical	Route						
M 🗌	Maximum s	session per H	lost 🔽	(1-81	.92)				
rewa	ill rule								
• т	Through-Z	yWALL rules							
(	🖲 Zone Pa	airs							
(	O All rule:	5							
СТ	Γo-Zy₩ALL	_ rules							
		Fron	n Zone				To Zone		
		С	LAN				O LAN		
		c o	LAN WAN				⊂ LAN ⊙ WAN		
		0 0	LAN WAN DMZ				C LAN		
		C C C Wire	LAN WAN DMZ less_Zone			с	C LAN ⊙ WAN C DMZ Wireless_	Zone	
#	Priority	C C C Wire Schedule	LAN WAN DMZ less_Zone User	Source	Destination	C Service	C LAN wAN C DMZ Wireless_ Access	Zone Log	
#	Priority 8	C C C Wire Schedule none	LAN WAN DMZ less_Zone User Idap- employee	Source Wireless	Destination any	C Service any	C LAN wAN C DMZ wireless_ Access allow	Zone Log no	±

Corresponding CLI commends 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 following figures.

C WAN			
C DMZ			
Ē			
\$\$ <b>€</b> ⊕ @ №			
e og			

9	C C Wire Schedule none From	LAN WAN DMZ less_Zone User Idap- employee	Source Wireless Apply	Destination any Reset	C Service any	C LAN C WAN C DMZ Wireless_ Access allow	Zone Log no	± 
9	C © Wire Schedule none Fron	WAN DMZ less_Zone User Idap- employee	Source Wireless Apply	Destination any Reset	C Service any	C WAN C DMZ Wireless_ Access allow	Zone Log no	± 7 7 7 8 7 9 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
ority 9	C © Wire Schedule none From	DMZ less_Zone User Idap- employee	Source Wireless Apply	Destination any Reset	C Service any	© DMZ Wireless_ Access allow	Zone Log no	∄ ∲€°⊉ ₪ ▷N
9	© Wire Schedule none Fron	less_Zone User Idap- employee n Zone	Source Wireless Apply	Destination any Reset	C Service any	Wireless Access allow	Zone Log no	∲ ぼ 型 前 い
9	Schedule none Fron	User Idap- employee	Source Wireless Apply	Destination any Reset	Service any	Access allow To Zone	Log no	₽ ©®® ₽ ₪ ₪
9	none From	Idap- employee	Wireless Apply	any Reset	any	allow	no	∲®°₽ ₪ №
_	From	n Zone	Apply	Reset		To Zo <u>ne</u>		
	C	(				100 A 100 A 100 A		
	Fron	n Zone				To Zo <u>ne</u>		
		1 0 M				Q L AN		
C WAN					O WAN			
	C					С рмz		
	• Wire	less Zone			c	Wireless	Zone	
		-		-				
prity	Schedule	User	Source	Destination	Service	Access	Log	
.0	none	employee	Wireless	any	any	allow	no	🧐 🗊 🛱 🛍 🕅 🔊
.C	rity )	C © Wire rity Schedule ) none	C DMZ C Wireless_Zone C Schedule User D none	C DMZ      Wireless_Zone      Schedule User Source      none Idap-     employee Wireless	C DMZ C Wireless_Zone C Wireless_Zone C Wireless_Zone C Volume Vo	C DMZ         • Wireless_Zone       •         • Schedule       User       Source       Destination       Service         • none       Idap- employee       Wireless       any       any	C DMZ       C DMZ         Image: Wireless_Zone       Image: Wireless_Zone       Image: Wireless_Zone         Schedule       User       Source       Destination       Service       Access         Image: Wireless       Image: Wireless       any       allow	C DMZ       C DMZ         Image: Wireless_Zone       Image: Wireless_Zone         Schedule       User       Source       Destination       Service       Access       Log         Image: Monee       Idap- employee       Wireless       any       any       allow       no

All contents copyright (c) 2006 ZyXEL Communications Corporation.

# 3. Seamless Incorporation

With robust networking functionalities in place, 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 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 on 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 play the rule 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 below:

1) Login ZyWALL1050 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)

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

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.

Microsoft	: Internet Explorer	x
1	Warning Message ! [31013] IP address is setting the same with other interface	!!
	(ОК	

All contents copyright (c) 2006 ZyXEL Communications Corporation.

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



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 Router Mode (NAT Mode). Since we have two different modes co-existing here, we need to make some adjustments to this rule.

Zy₩/	ALL	10	50 > C	onfigurati	on > Policy	y > Route > F	olicy Route					
	Pol	icy	Route	Stati	Route							
		#	User	Schedule	Incoming	Source	Destination	Service	Next-Hop	SNAT	BWM	T
		1	admin	none	ge1	LAN_SUBNET	any	any	WAN_TRUNK	outgoing- interface	0	🥸 🛐 🗒 🕅 🔊 N
												R
							Apply	Reset				Click here to modify

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

WALL 1050 > Configuration > Policy > R	Route > Policy Route > Edit > #1
Configuration	
Enable	
Description	(Optional)
Criteria	
User	admin
Incoming	Interface / ge1 Change
Source Address	
Destination Address	any
Schedule	none 💌
Service	any New
Next-Hop	
Туре	
Gateway	
Interface	br1 💌
VPN Tunnel	
Trunk	WAN_TRUNK

Then please 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.

Each time you make a change, never 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 outsider from WAN to access the Web pages locating on the Web Server in the DMZ zone.

To make this scenario works; the follow the configuration steps as below:

1) Login ZyWALL1050 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** 



≥ Zy₩	ALL 1050 > Configuration > I	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
		OK Cancel

## **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						
		192 168 1 55						
	IF Address	132.100.1.33						
		Cancer						

### CLI to create an address object

### [0] address-object WebServer 192.168.1.55

4)Switch to Configuration > Policy > Firewall > Firewall Rule, add a new firewall rule

for your virtual server. Since it is an web server, so we choose "HTTP" as the Service. And "Allow" for the access action.

> ZyWALL 1050 > Configu	ration > Policy > Firewall > Firewall Rule > Edit > #1
Configuration.	
Configuration	
🗹 Enable	
From	WAN
То	LAN
Description	WebServerFW (Optional)
Schedule	none 💌
User	any
Source	any
Destination	WebServer
Service	НТТР
Access	allow 💌
Log	log 🔽
	OK Cancel

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.

ALL 1	1050 >	Configuratio	n > Policy > f	firewall					
G	lobal 9	Setting							
	🔽 En	able Firewall							
	🗖 Ma	aximum session	per Host		1-2048)				
S	electio	in							
	Θzα	one Pairs			O Glob	al			
Fi	rewall	Rule							
			From Zone				To Zon	e	
			O LAN				🖸 LAP	V	
			💿 wan				O WA	N	
			O DMZ				O DM	z	
Г	#	Schedule	User	Source	Destination	Service	Access	Log	ŧ
	1	none	any	any	WebServer	НТТР	allow	log	🖗 🗊 🖳 🛍 DN
	2	none	any	any	any	any	deny	log	∲₿°₽ <mark>∎</mark> _~
					Apply Res	et			