

ZyWALL USG 20/20W/50

ZLD 2.21 Support Notes

Revision 1.00

August, 2010

Written by CSO



Table of Contents

- Scenario 1 — Connecting your USG to the Internet 4
 - 1.1 Application Scenario 4
 - 1.2 Configuration Guide 5
- Scenario 2 — WAN Load Balancing and Customized Usage of WAN Connection for Specific Traffic (USG 50 only) 12
 - 2.1 WAN Load Balancing 12
 - 2.1.1 Load Balancing Algorithm 12
 - 2.2 Customized Usage of WAN Connection for Specific Traffic Type 14
 - 2.3 Application Scenario 15
 - 2.4 Configuration Guide 16
- Scenario 3 — How to configure NAT if you have Internet-facing public servers 22
 - 3.1 Application Scenario 22
 - 3.2 Configuration Guide 23
- Scenario 4 — Secure site-to-site connections using IPSec VPN 27
 - 4.1 Application Scenario 27
 - 4.2 Configuration Guide 28
- Scenario 5 — Secure client-to-site connections using IPSec VPN 35
 - 5.1 Application Scenario 35
 - 5.2 Configuration Guide 36
- Scenario 6 — Deploying SSL VPN for Tele-workers to Access Company Resources (USG 50 only) 45
 - 6.1 Application Scenario 45
 - 6.2 Configuration Guide 46
- Scenario 7 — Reserving Highest Bandwidth Management Priority for VoIP Traffic 55
 - 7.1 Application Scenario 55
 - 7.2 Configuration Guide 56

- Scenario 8 — Reserving Highest Bandwidth Management Priority for a Superior User and Control Session per Host..... 61
 - 8.1 Application Scenario 61
 - 8.2 Configuration Guide 62
- Scenario 9 — Using ZyWALL to Control Popular P2P Applications (USG 50 only) 71
 - 9.1 Application Scenario 71
 - 9.2 Configuration Guide 72
- Scenario 10 — Deploying Content Filtering to Manage Employee Browsing Behavior 77
 - 10.1 Introduction to ZSB (ZyXEL Safe Browsing) 78
 - 10.2 Application Scenario 78
 - 10.3 Configuration Guide 79
- Scenario 11 — Quick Setup for Allowing WLAN Users to Access LAN Services (USG 20W only) 86
 - 11.1 Application Scenario 86
 - 11.2 Configuration Guide 87

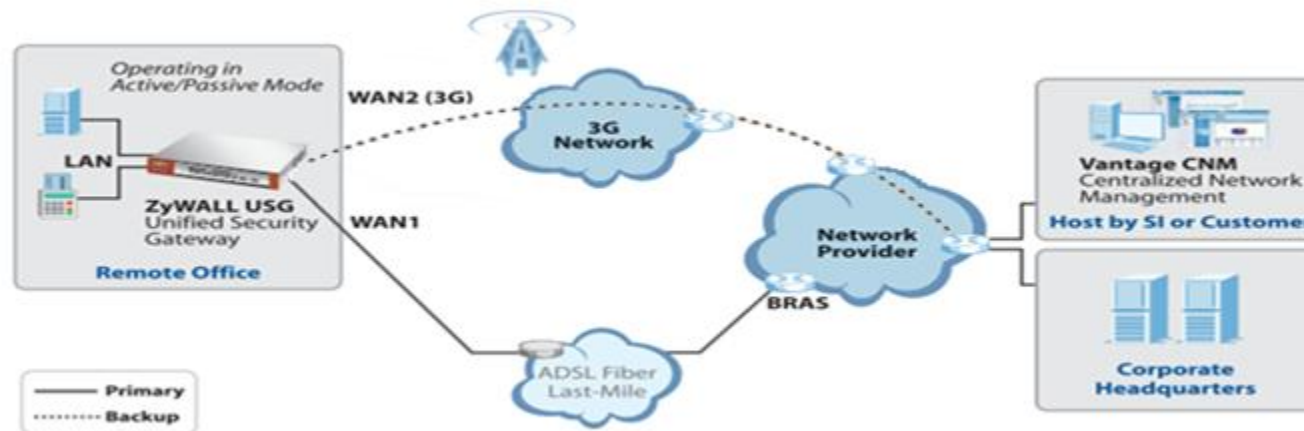
Scenario 1 — Connecting your USG to the Internet

1.1 Application Scenario

A WAN (Wide Area Network) connection is an outside connection to another network or the Internet. It connects your private network such as LAN (Local Area Network) and other networks, so that a computer in one location can communicate with computers in other locations.

The USG has a multiple WAN feature which enables you to link your network with up to two ISPs or other networks via Ethernet, PPPoE or 3G connections. User can either use trunks for WAN traffic load balancing to increase overall network throughput (“active-active” load sharing mode) or as a backup to enhance network reliability (“active-passive” failover mode).

Load balancing will be described further in Scenario 2. In the figure below we first show the scenario for non-stop Internet access with the PPPoE as primary WAN and 3G backup through USB. This means that the USG will normally use the PPPoE interface for Internet access, and it will only resort to the 3G interface when the PPPoE interface’s connection fails.



1.2 Configuration Guide

Network Conditions:

USG-50:

- WAN1_PPP: PPP over Ethernet
- Cellular1: 3G

ZyWALL-5 UTM:

- WAN1: PPP over Ethernet
- WAN2: 3G

Goal to achieve:

Use the PPPoE interface as device's primary WAN connection and switch to the 3G interface automatically when the PPPoE interface's connection fails.

ZLD configuration

Step 1. Click **CONFIGURATION > Object > ISP Account** to create an ISP account first.

#	Profile Name	Protocol	Authentication Type	User Name
1	WAN1_PPPoE_ACCOUNT	pppoe	chap-pap	
2	WAN1_PPTP_ACCOUNT	pptp	chap-pap	
3	WAN2_PPPoE_ACCOUNT	pppoe	chap-pap	
4	WAN2_PPTP_ACCOUNT	pptp	chap-pap	

ZyNOS configuration

Step 1. Click **Network > WAN > WAN1** to open the configuration screen.

ISP Parameters for Internet Access

Encapsulation: **PPP over Ethernet**

Service Name: (Optional)

User Name: 85111279@hinet.net

Password: [REDACTED]

Retype to Confirm: [REDACTED]

Authentication Type: **CHAP/PAP**

Nailed-Up

Idle Timeout: 0 (Seconds)

WAN IP Address Assignment

Get Automatically from ISP

Use Fixed IP Address

My WAN IP Address: 0 . 0 . 0 . 0

Step 2. Fill in the PPPoE user name and password.

Edit ISP Account Rule

Profile Name: WAN1_PPPoE_ACCOUNT

Protocol: pppoe

Authentication Type: Chap/PAP

User Name: 85111279@hinet.net

Password: ●●●●●●

Retype to confirm: ●●●●●●

Service Name: (Optional)

Compression: On Off

Idle timeout: 0 (Seconds)

OK Cancel

Step 3. Click **CONFIGURATION > Network > Interface > PPP** to open the configuration page. User can click the system default rule and edit it.

CONFIGURATION

Port Role: Ethernet **PPP** Cellular VLAN Bridge Trunk

User Configuration

#	Status	Name	Base Interface	Account Profile
1	●	wan1_ppp	wan1	WAN1_PPPoE_ACCOUNT
2	●	wan2_ppp	wan2	WAN2_PPPoE_ACCOUNT

Page 1 of 1 | Show 50 items | No data to display

System Default

#	Status	Name	Base Interface	Account Profile
1	●	wan1_ppp	wan1	WAN1_PPPoE_ACCOUNT
2	●	wan2_ppp	wan2	WAN2_PPPoE_ACCOUNT

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

Step 2. Fill in the PPPoE parameters:

- Select **PPP over Ethernet** encapsulation mode
- User name
- Password

Step 3. Click the **Apply** button to save and apply the setting.

WAN

WAN 1 | 3G (WAN 2) | Traffic Redirect | Dial Backup

ISP Parameters for Internet Access

Encapsulation: **PPP over Ethernet**

Service Name: (Optional)

User Name: 85111279@hinet.net

Password: ●●●●●●

Retype to Confirm: ●●●●●●

Authentication Type: CHAP/PAP

Nailed-Up

Idle Timeout: 0 (Seconds)

WAN IP Address Assignment

Get Automatically from ISP

Use Fixed IP Address

My WAN IP Address: 0 . 0 . 0 . 0

Advanced Setup

Enable NAT (Network Address Translation)

RIP Direction: None

RIP Version: RIP-1

Enable Multicast

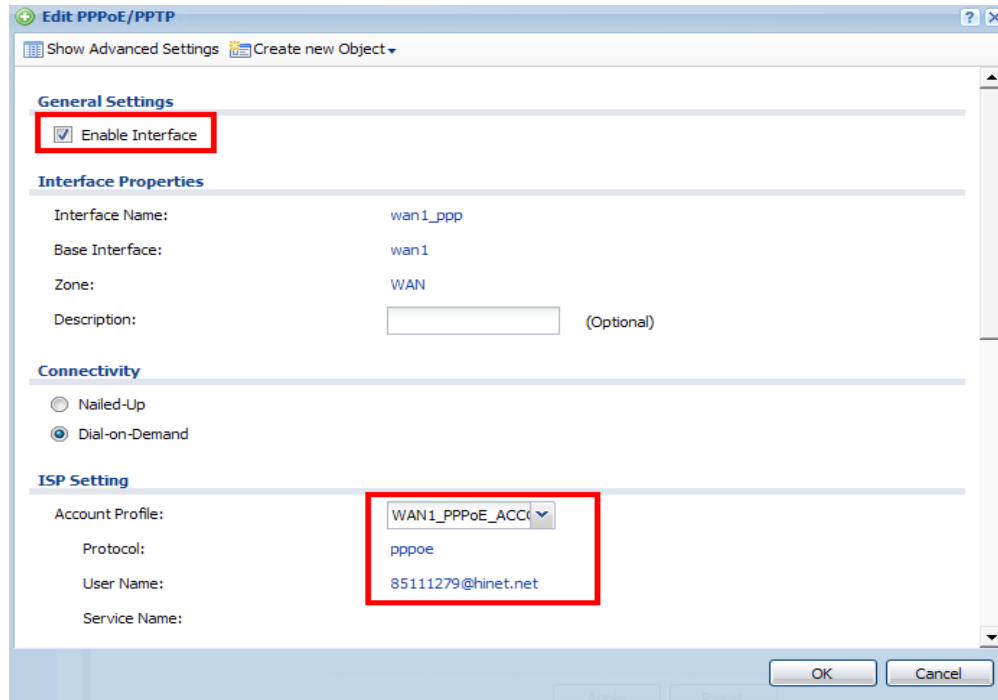
Multicast Version: IGMP-v1

Spoof WAN MAC Address from LAN

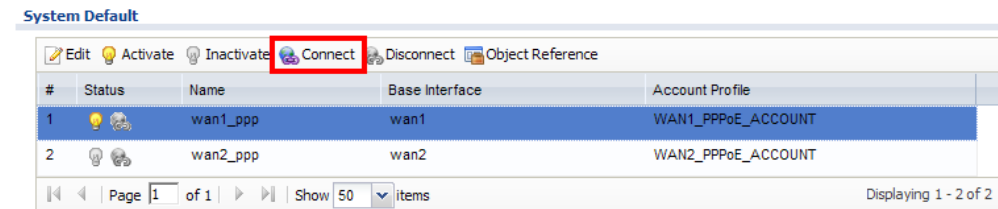
Clone the computer's MAC address - IP Address: 0 . 0 . 0 . 0

Apply Reset

Step 4. Enable the interface and select the pre-configured ISP account to activate the PPPoE rule.



Step 5. When the configuration is done, click the **Connect** button to enable the PPPoE link. Once the connection is established, the *connected* icon will be displayed in front of the rule.



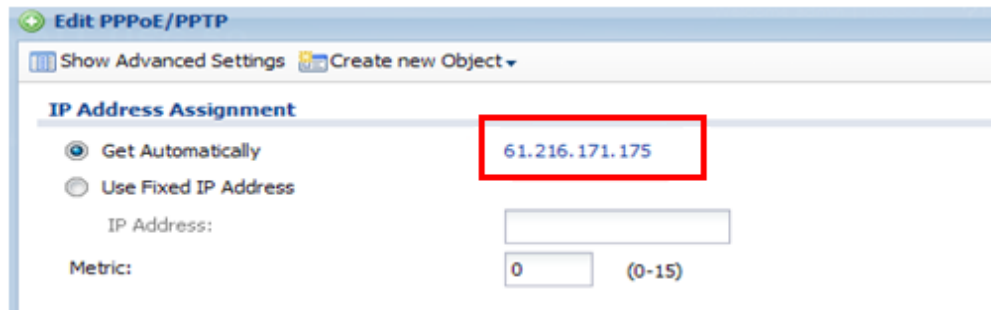
Step 4. Check the connection status on the dashboard.



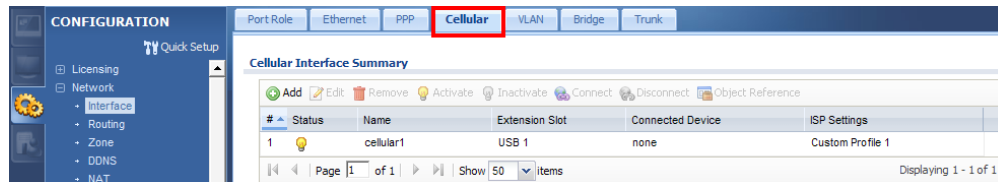
Step 5. Click **Network > WAN > 3G (WAN2)** to open the configuration screen.



Step 6. To check the PPPoE IP address, click the PPPoE rule and check the IP address part for the information.

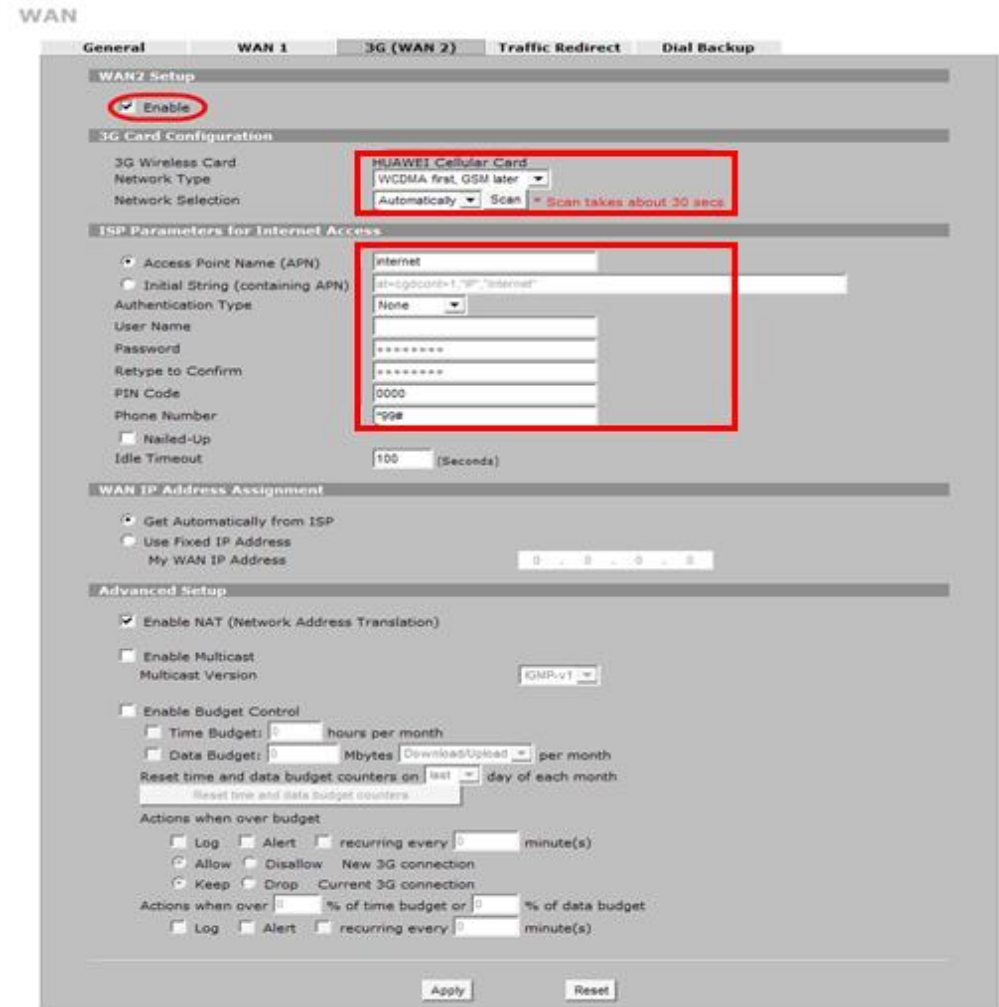


Step 7. Click **CONFIGURATION > Network > Interface > Cellular** to open the configuration page.



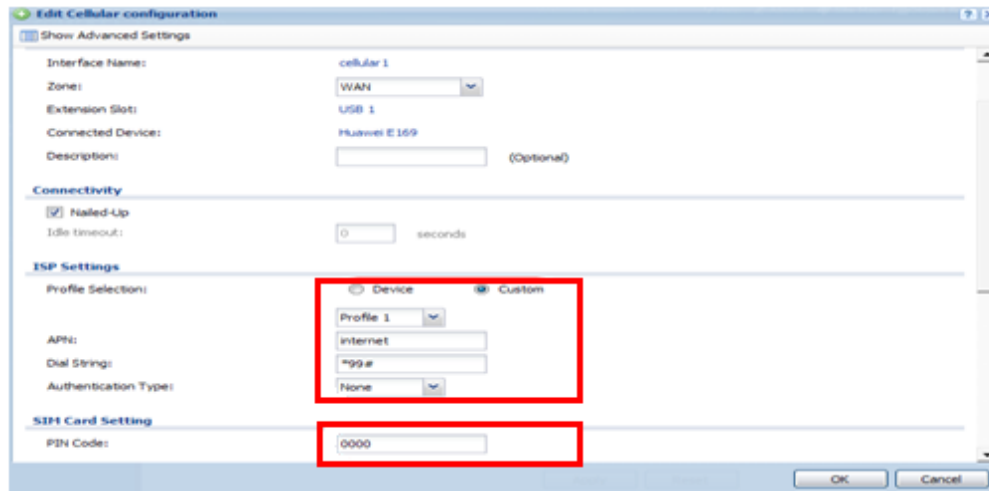
Step 6. Fill in the 3G connection parameters:

- The card information will be detected by device automatically
- Internet Access setting
 - Access Point Name (APN)
 - PIN code
 - Phone number (enter *99# if not sure what number to fill in)

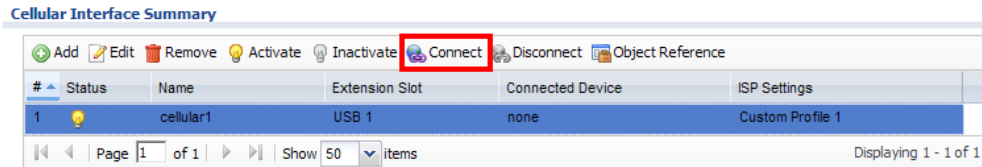


Step 8. Fill in the 3G connection parameters:

- The card information will be detected by device automatically
- ISP Settings
 - APN name
 - Dial String
- PIN code



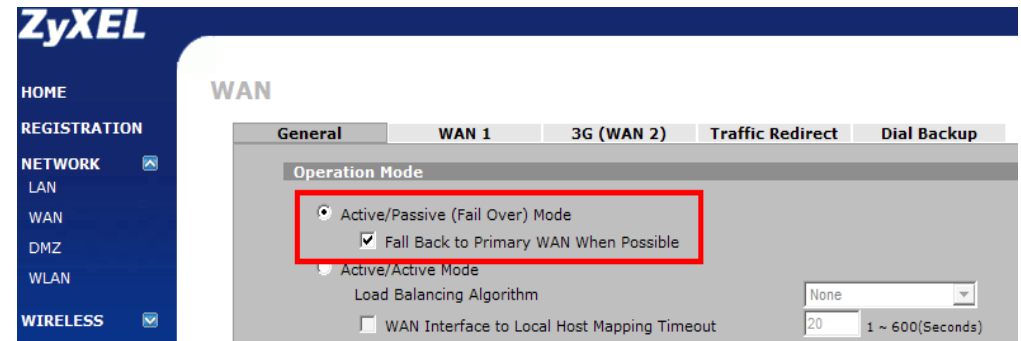
Step 9. After the configuration is done, click **Activate** to enable the rule. And then click Connect button to enable the 3G connection.



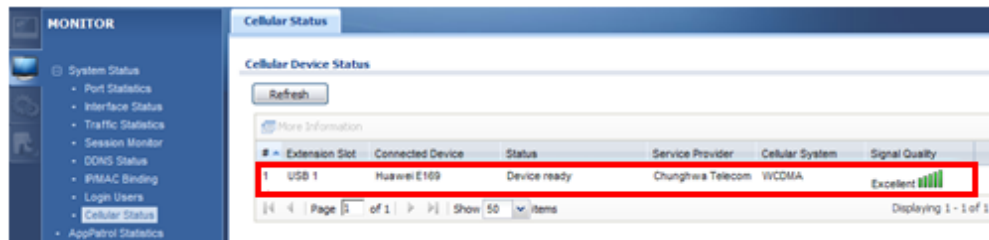
Step 7. Go to the dashboard and click the **Dial** button to trigger the rule. User can check the 3G WAN interface status to get the 3G modem detail information.



Step 8. Now the both PPPoE and 3G connection are UP. Click on **Network > WAN > General** page to select the **Active/Passive Mode** to achieve the backup mechanism.

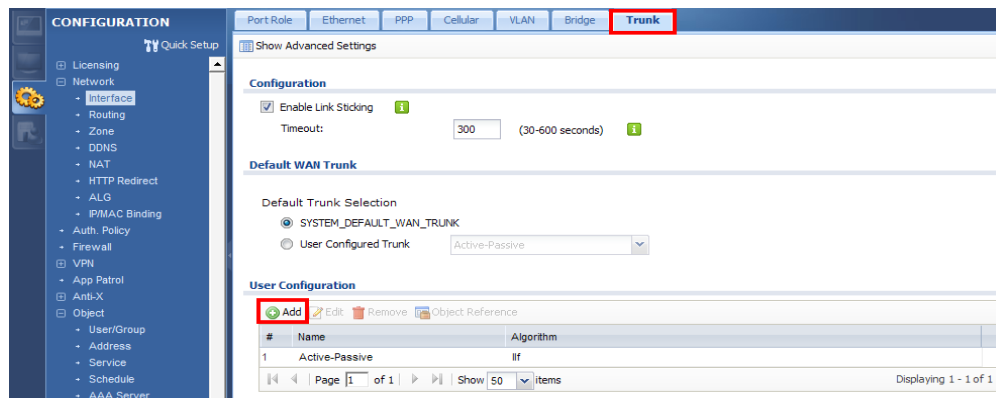


Step 10. User can check the 3G connection status on **MONITOR > System Status > Cellular Status** screen.

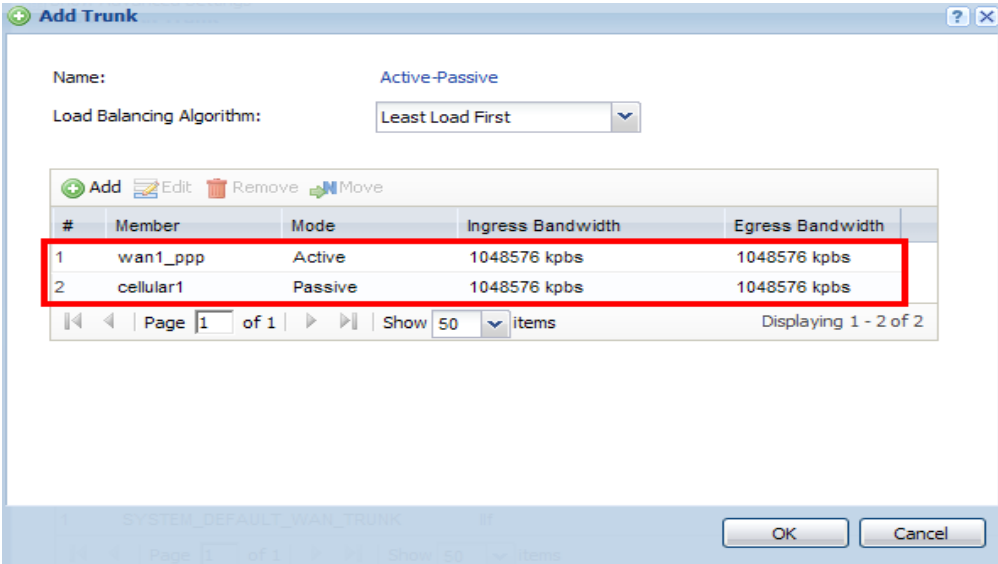


Step 11. Now both the PPPoE and 3G connection are UP. Click on **CONFIGURATION > Network > Interface > Trunk** to open the configuration screen.

Step 12. Click the **Add** button to add a User Configuration rule.



Step 13. Configure the **trunk name** and add the two interfaces: PPPoE for Active and 3G for Passive mode.



Step 14. Select the **User Configured Trunk** rule as the default WAN trunk. Then it will work using PPPoE as primary and 3G as a backup connection.

Default WAN Trunk

Default Trunk Selection

SYSTEM_DEFAULT_WAN_TRUNK

User Configured Trunk Active-Passive

User Configuration

#	Name	Algorithm
1	Active-Passive	lbf

Scenario 2 — WAN Load Balancing and Customized Usage of WAN Connection for Specific Traffic (USG 50 only)

2.1 WAN Load Balancing

As an enterprise network gateway, the USG ZyWALL often has more than one WAN connection to share the company network traffic load. Without WAN load balancing, a single WAN connection may get too congested, causing the Internet traffic to become slow or even get lost.

USG ZyWALL provides network administrators with flexible ways of implementing WAN load balancing according to their demands. The outbound traffic is shared among multiple internet connections. Therefore, Internet traffic can get passed through the USG ZyWALL smoothly, improving your service quality and ensuring the Internet connections get effectively utilized.

2.1.1 Load Balancing Algorithm

WRR — Weighted Round Robin

We can assign different weights to different internet connections according to their bandwidth. The outbound traffic sessions will be sent out among the multiple WAN connections in turn; sessions will be assigned to different connections according to their proportional weights. Take the following for example:

WAN1 bandwidth: 1 Mbps.

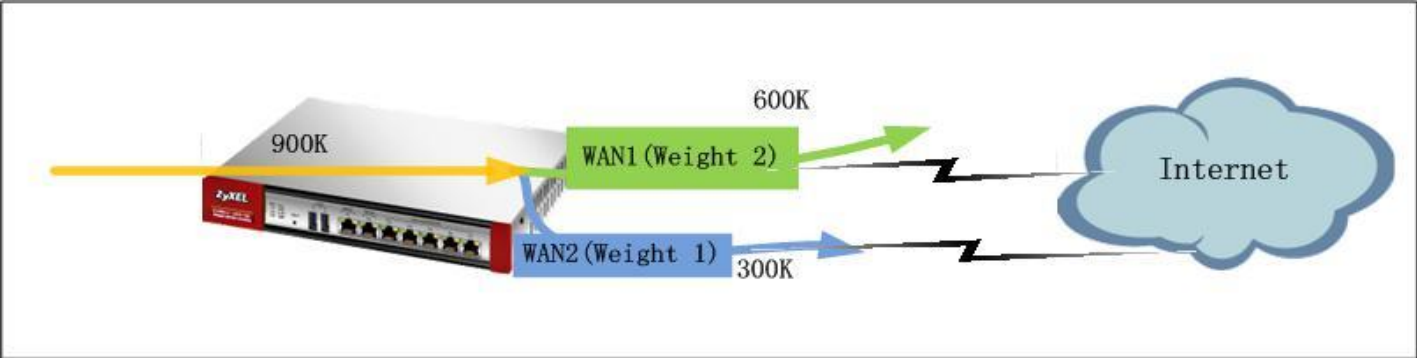
WAN2 bandwidth: 512 Kbps.

Since WAN1 has a bandwidth about twice that of WAN2, we can assign the weights to WAN1 and WAN2 as follows:

WAN1 Weight: 2

WAN2 Weight: 1

The outbound traffic sessions will be assigned to WAN1 and WAN2 according to their proportional weights. E.g., when there's total outbound traffic of 900K, 600K will be sent out over WAN1 and 300K will be sent out over WAN2.



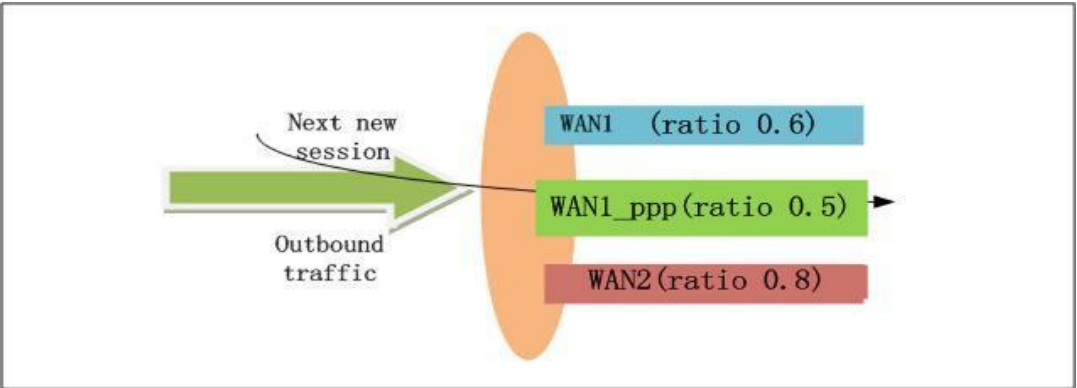
LLF — Least Load First

When choosing LLF as the load balancing algorithm, the USG will calculate each WAN interface’s current outbound traffic utilization against the interface’s available bandwidth. Then it will use each interface’s traffic utilization ratio as the index to decide via which WAN interface it will send the next new session. The interface with the least outbound traffic utilization ratio will be used to send the next new session.

Take the following for example:

Interface	Available Bandwidth	Current measured Traffic	Utilization Ratio
WAN1	1M	600K	0.6
WAN1_ppp	512K	256K	0.5
WAN2	2M	1.6M	0.8

The next outbound new session will be sent over WAN1_ppp.



Spill-over

When choosing the Spill-over load balancing algorithm, the USG will send outbound traffic to the first interface member in the WAN trunk until its maximum allowable bandwidth is reached. Then the USG will send the excess outbound traffic to the second interface member in the WAN trunk.

This algorithm is used when the first WAN connection is free or has a lower billing rate than the second WAN connection. The company can use this load balancing algorithm to reduce Internet fees while avoiding congestion on the first WAN connection.

See the example below:

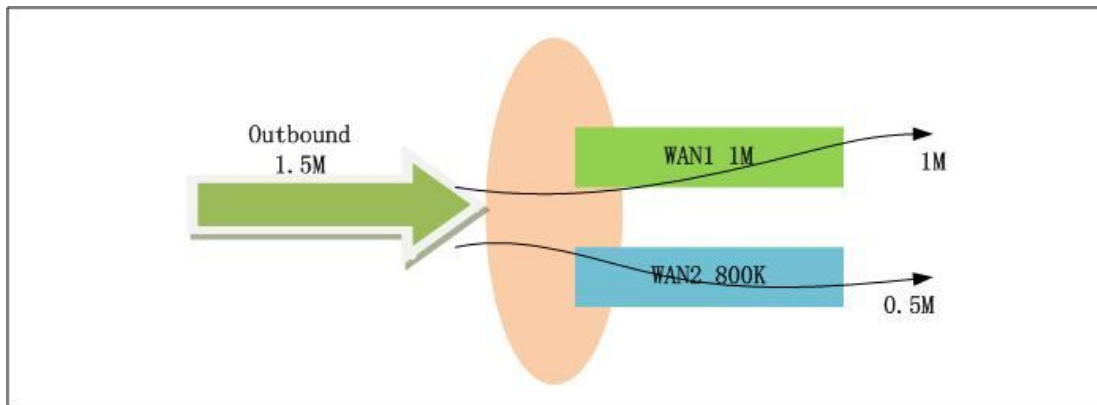
WAN1 (free connection) bandwidth: 1M

WAN2 (billing connection) bandwidth: 800K

Total outbound traffic is 1.5M. The traffic distribution among the two connections:

WAN1: 1M

WAN2: 0.5M



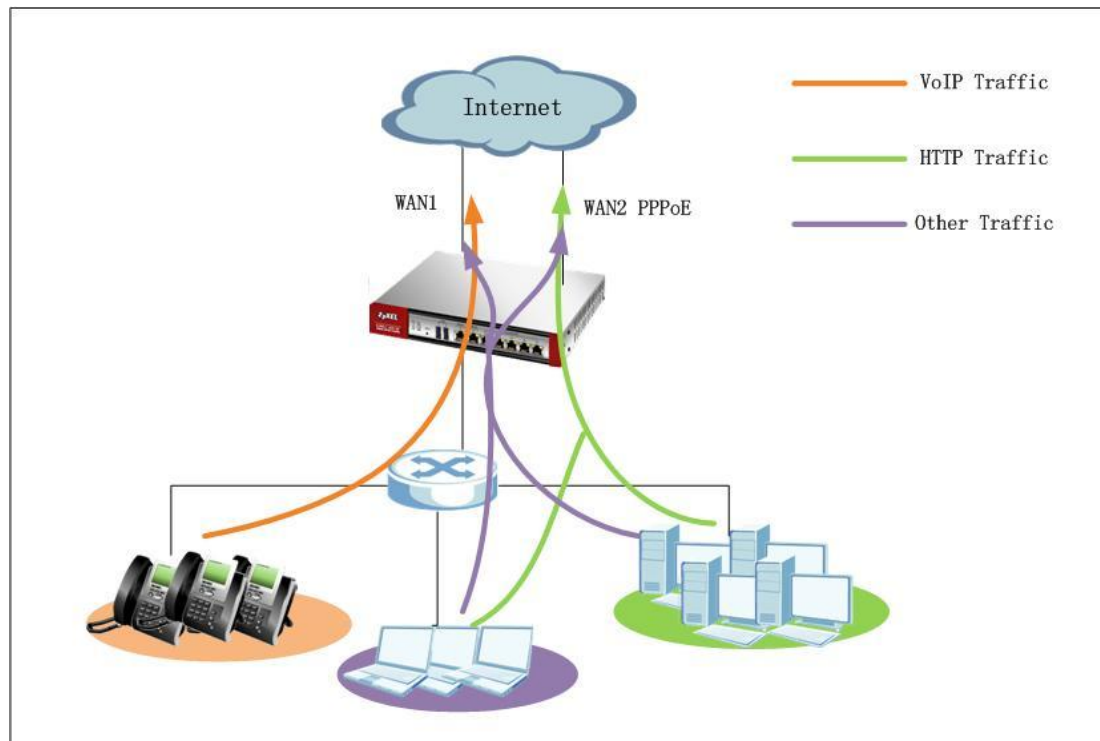
2.2 Customized Usage of WAN Connection for Specific Traffic Type

In some cases, the network administrator may prefer to send out some specific type of traffic over a specific WAN connection. For example, the ISP for WAN1 connection is also the company's ITSP (VoIP provider). Therefore, network administrator can set the gateway to send VoIP traffic out over WAN1.

Both ZyNOS ZyWALL and USG ZyWALL can achieve this application by Policy Route.

2.3 Application Scenario

The company has two WAN connections for sharing outbound internet traffic. WAN1 uses static IP, and WAN2 uses a PPPoE connection. Since WAN1 ISP is also the company's VoIP provider, the network administrator wants VoIP traffic primarily sent out over WAN1. In case WAN1 is down, the VoIP traffic can still go out over WAN2 PPPoE connection. Network administrator also wants HTTP traffic sent over WAN2 PPPoE connection primarily. In case WAN2 PPPoE is down, LAN users can still surf internet over WAN1. For all other types of traffic, administrator needs the two WAN connections to share the outbound traffic load, performing load balancing.



2.4 Configuration Guide

Network Conditions:

- LAN subnet: 192.168.1.0/24
- WAN1 IP: 200.0.0.1
- WAN2 PPPoE IP: Dynamic
- WAN1 download bandwidth: 2M
- WAN2 download bandwidth: 2M

Goals to achieve:

- 1) VoIP traffic goes out primarily through WAN1. In case WAN1 is down, it will go out via WAN2 PPPoE connection.
- 2) HTTP traffic goes out primarily through WAN2 PPPoE connection. In case WAN2 PPPoE is down, it will go out via WAN1.
- 3) All other traffic goes out via WAN trunk performing Load Balancing with Least Load Balancing algorithm.

ZLD configuration

Step 1. Configure a PPPoE account on WAN2 interface.

- a. Go to **CONFIGURATION > Object > ISP Account**, add a PPPoE account:

The screenshot shows the 'Add ISP Account Rule' dialog box with the following configuration:

- Profile Name: wan2_ppp
- Protocol: pppoe
- Authentication Type: Chap/PAP
- User Name: my_account
- Password: [masked]
- Retype to confirm: [masked]
- Service Name: [empty] (Optional)
- Compression: On Off
- Idle timeout: 0 (Seconds)

ZyNOS configuration

Step 1. Go to **Advanced > Policy Route**, add policy route to route VoIP traffic out primarily from WAN1, and WAN2 as backup.

Criteria:

Application: SIP

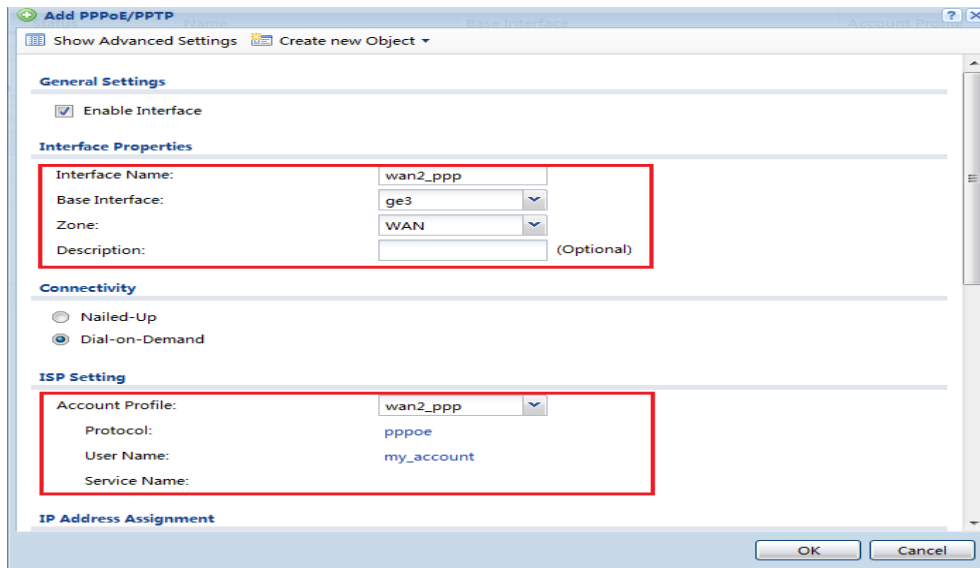
Source: Choose LAN interface. Address range: 192.168.1.0~192.168.1.255

Destination: Any.

Action Applies to: Matched packets.

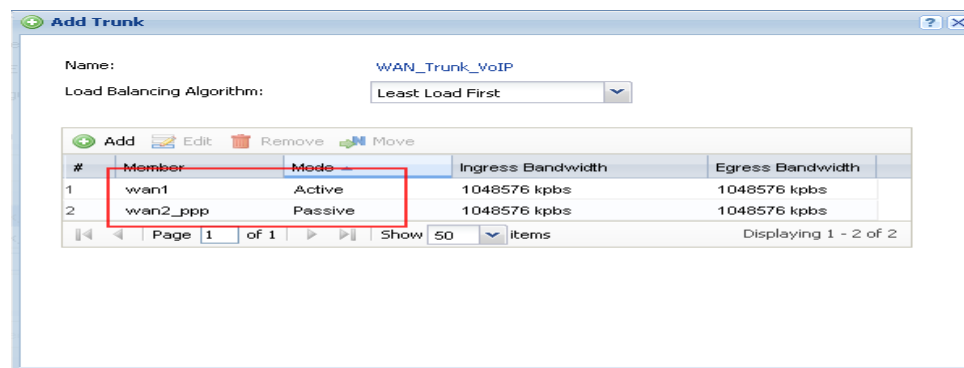
Routing Action:

b. Go to **CONFIGURATION > Network > Interface > PPP**, add a new PPP interface which is based on WAN 2(ge3) interface:

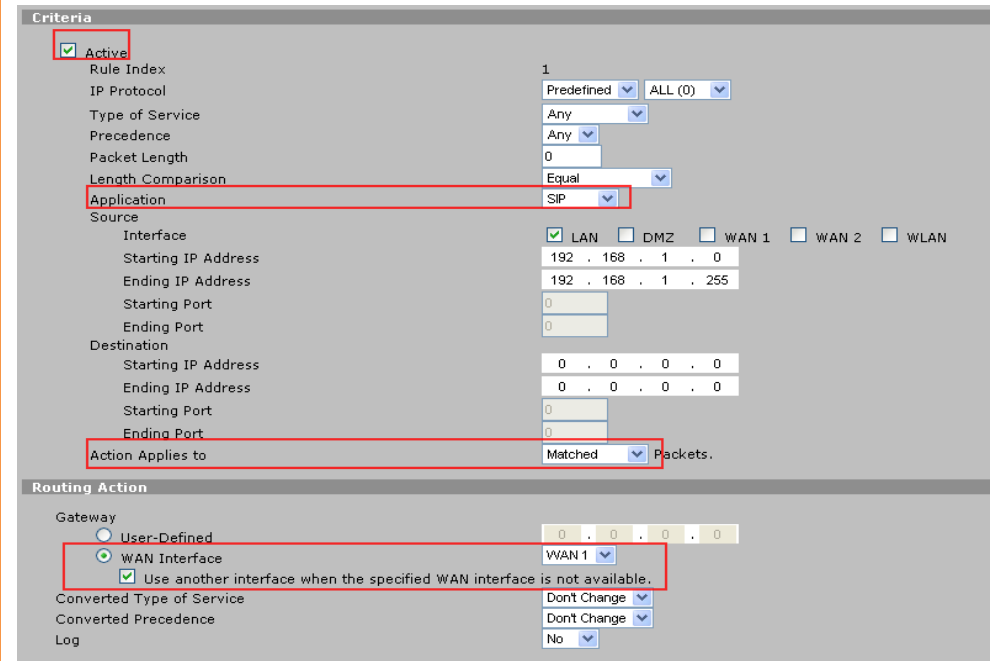


Step 2. Go to **CONFIGURATION > Network > Interface > Trunk**. Add WAN Trunks.

a. Add WAN trunk for VoIP traffic — Set WAN1 as Active mode, while setting WAN2_ppp as Passive mode.

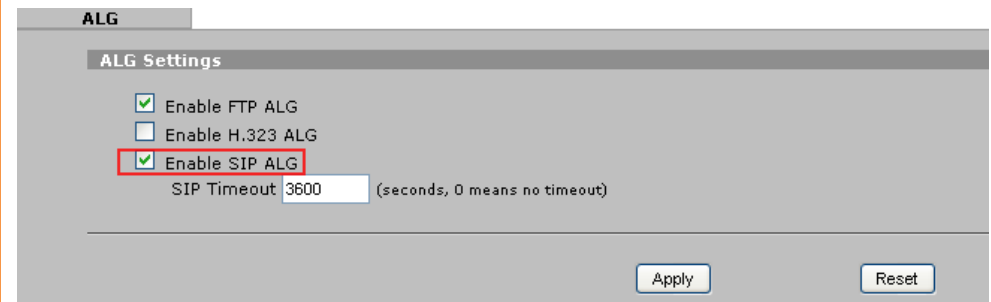


Choose WAN interface WAN1, and enable **Use another interface when the specified WAN interface is not available**.

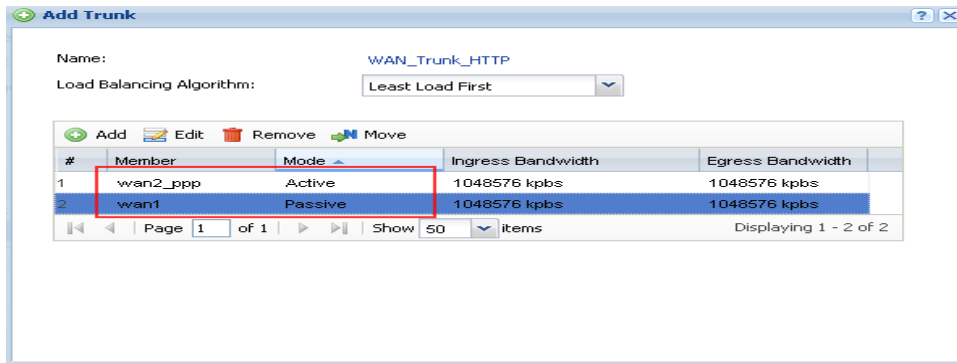


Please enable **SIP ALG** to let this policy route apply to all VoIP traffic including both SIP signaling and RTP (voice data).

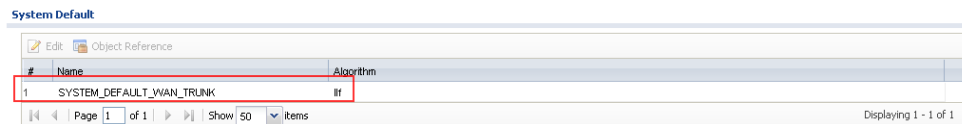
Go to **Advanced > ALG**, enable SIP ALG.



- b. Add WAN trunk for HTTP traffic — Set WAN2_ppp as Active mode, while setting WAN1 as Passive mode.



- c. Use SYSTEM_DEFAULT_WAN_TRUNK to do load balancing for all other traffic.



Step 2. Go to **Advanced > Policy Route**, add a policy route to route HTTP traffic out primarily through WAN2, leaving WAN1 as backup.

Criteria:

IP Protocol: TCP (6)

Application: Custom

Source IP: Choose interface LAN. Address range: 192.168.1.0~192.168.1.255

Source port: Any

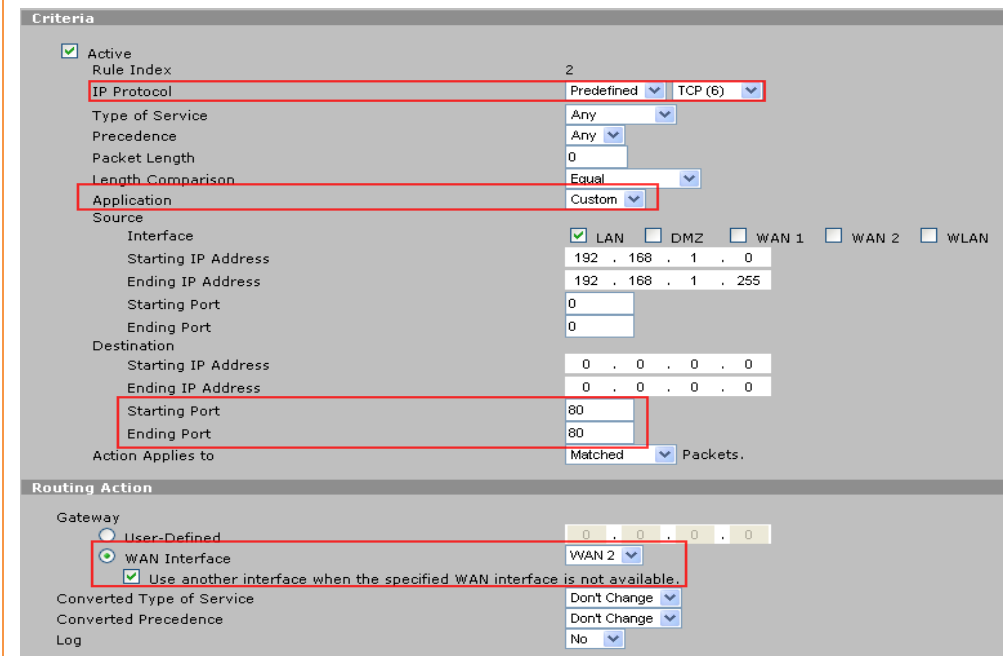
Destination IP: Any

Destination Port: 80

Action Applies to: Matched packets.

Routing Action:

Choose WAN interface WAN2, and enable **Use another interface when the specified WAN interface is not available.**



Step 3. Go to **CONFIGURATION > Network > Routing > Policy Route**, add policy routes for VoIP traffic and HTTP traffic.

a. Add a policy route for VoIP traffic:

Source: LAN1_subnet

Destination: Any

Service: SIP

Next Hop: select the newly created WAN trunk WAN_Trunk_VoIP

Enable
Description: (Optional)

Criteria

User: any
Incoming: any
Source Address: LAN1_SUBNET
Destination Address: any
DSCP Code: any
Schedule: none
Service: SIP

Next-Hop

Type: Trunk
Trunk: WAN_Trunk_VoIP

Auto-Disable

Please note that to make sure this policy route applies to all VoIP traffic, including both the SIP signaling and RTP (voice data), we need to enable **SIP ALG**. Go to **Configuration > Network > ALG**, enable SIP ALG.

SIP Settings

Enable SIP ALG

Enable SIP Transformations

Enable Configure SIP Inactivity Timeout

SIP Media Inactivity Timeout : 120 (seconds)

SIP Signaling Inactivity Timeout : 1800 (seconds)

SIP Signaling Port :

#	Port
1	5060

Step 3. For all other traffic, we use the two WAN connections to perform load balancing. Go to **Network > WAN > General**.

Choose Active/Active Mode.

Set the **Load Balancing Algorithm** to Least Load First.

To avoid the situation where traffic from the same LAN host may be sent over different WAN interfaces, which may cause servers to refuse the connection due to a different source IP, we enable and set “**WAN Interface to Local Host Mapping Timeout**” to a specific time period.

For Load Balancing Index (es), we choose **Outbound Only**.

Set the available outbound bandwidth for the two WAN connections according to the bandwidth obtained from each ISP.

Operation Mode

Active/Passive (Fail Over) Mode
 Fall Back to Primary WAN When Possible

Active/Active Mode

Load Balancing Algorithm: Least Load First

WAN Interface to Local Host Mapping Timeout

Time Frame: 10 (10(Seconds) ~ 600(Seconds))

Load Balancing Index(es): Outbound Only

Interface	Available Inbound Bandwidth	Available Outbound Bandwidth
WAN 1	0 Kbps	1000 Kbps
WAN 2	0 Kbps	512 Kbps

b. Add a policy route for HTTP traffic:

Source: LAN1_subnet

Destination: Any

Service: HTTP

Next Hop: Select the newly created WAN trunk WAN_Trunk_HTTP.

Criteria

User:	any
Incoming:	any
Source Address:	LAN1_SUBNET
Destination Address:	any
DSCP Code:	any
Schedule:	none
Service:	HTTP

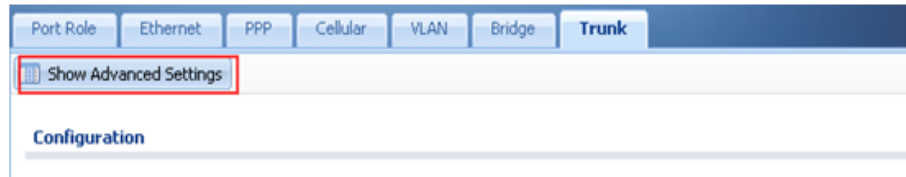
Next-Hop

Type:	Trunk
Trunk:	WAN_Trunk_HTTP

Auto-Disable

- c. For all other traffic, use **SYSTEM_DEFAULT_WAN_TRUNK** to do load balancing.

Go to **Configuration > Network > Interface > Trunk**. Click Show Advanced Settings.



Make sure **Default SNAT** is enabled. Select **SYSTEM_DEFAULT_WAN_TRUNK** in Default Trunk Selection.

Default WAN Trunk

Enable Default SNAT

Default Trunk Selection

SYSTEM_DEFAULT_WAN_TRUNK

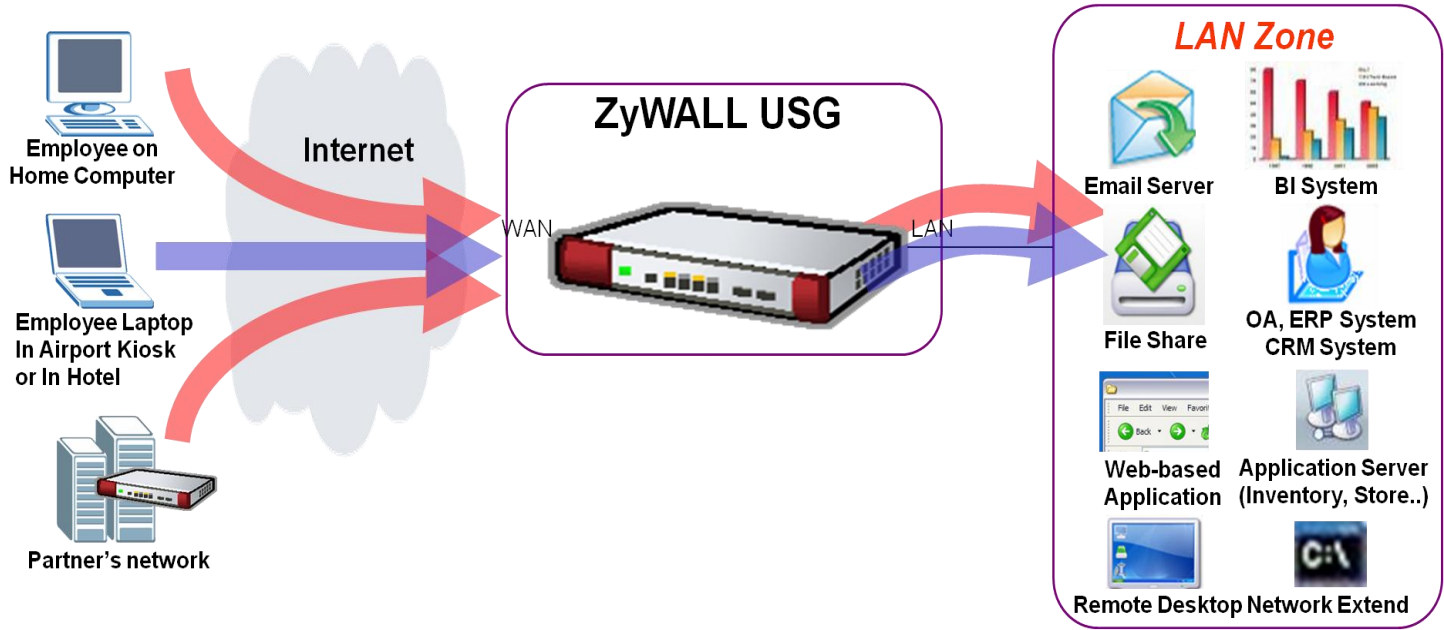
User Configured Trunk

WAN_Trunk_VoIP

Scenario 3 — How to configure NAT if you have Internet-facing public servers

3.1 Application Scenario

It is a common practice to place company servers behind the USG’s protection; while at the same time letting WAN side clients/servers access the intranet servers. To give an example, the company may have an internal FTP server, which needs to be accessible from the Internet as well. To fulfill this requirement, user can configure a NAT mapping rule to forward the traffic from Internet side to intranet side. This feature can not only ensure service availability but also helps avoid exposing the server’s real IP address to be attacked.



3.2 Configuration Guide

Network Conditions:

USG-50:


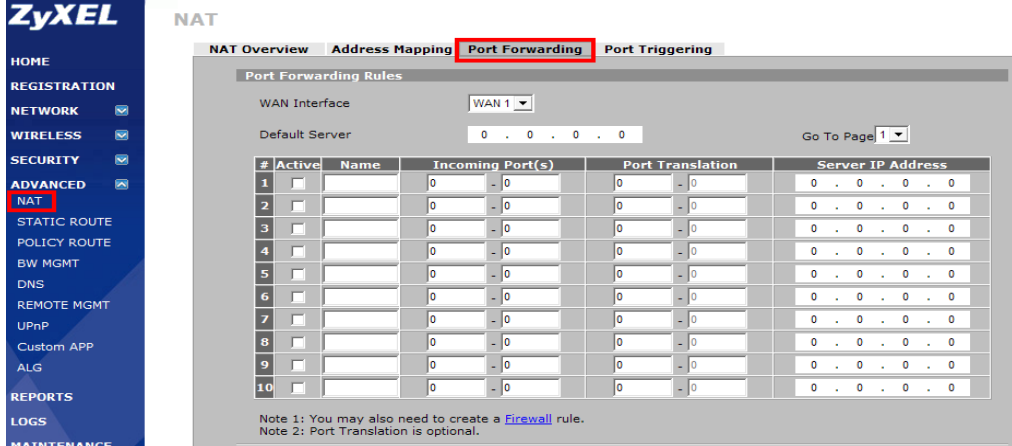
- WAN IP: 59.124.163.152
- FTP server IP:192.168.50.33

ZyWALL-5 UTM:

- WAN IP: 10.59.1.50
- FTP server IP: 192.168.5.33

Goal to achieve:

User Tom can access the internal FTP server by accessing the Internet-facing WAN IP address.

ZLD configuration	ZyNOS configuration
<p>Step 1. Click CONFIGURATION > Network > NAT to open the configuration screen.</p> 	<p>Step 1. Click ADVANCED > NAT > Port Forwarding to open the configuration screen.</p> 

Step 2. Click the **Add** button to create a mapping rule.

Step 3. In this page user needs to configure:

- Rule's name
- Select Virtual Server type to let USG-50 do packet forwarding
- Fill in the **Original IP** (WAN IP) address
- Fill in the **Mapped IP** (Internal FTP server IP) address
- Select the **service to be mapped** (FTP); the ports will be selected automatically

Step 2. Configure the mapping rule. User needs to select the WAN interface for the incoming access, choosing the WAN IP for users to access.

Step 3. Then configure the incoming ports, translation ports and the internal FTP server IP address.

In this case, when the user accesses the WAN IP address with the port 20/21, the ZyWALL-5 UTM will forward the request to the FTP server, 192.168.5.33, with the port 20/21. Thus, user can access the internal FTP server without problem.

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	FTP	20 - 21	20 - 21	192 . 168 . 5 . 33

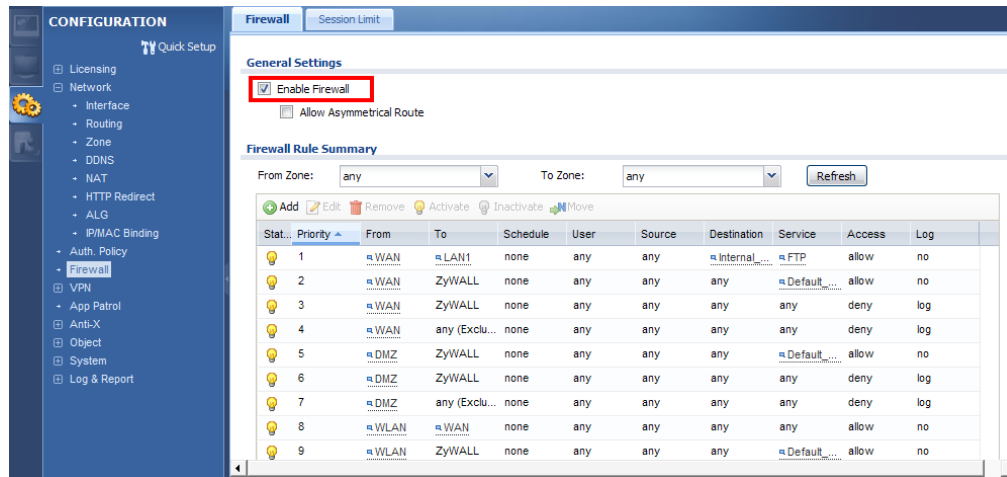
Step 4. The port forwarding rule enables delivery of the access request from WAN to the internal network, but the user still needs to configure access privileges by adjusting the firewall rule. By default all WAN to LAN access is dropped.

FIREWALL

From	To	LAN	WAN1	WAN2	DMZ	WLAN	VPN
LAN		0 Rules Permit	0 Rules Permit	0 Rules Permit	0 Rules Permit	0 Rules Permit	0 Rules Permit
WAN1		3 Rules Drop	1 Rules Permit	0 Rules Drop	0 Rules Permit	0 Rules Drop	0 Rules Permit

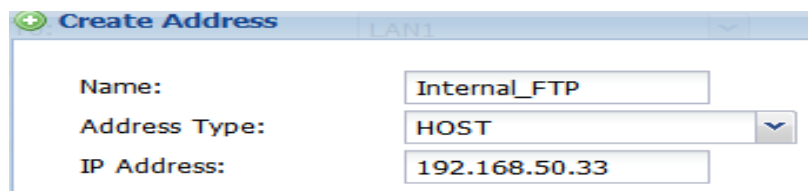
Step 4. Click **CONFIGURATION > Network > Firewall** to open the firewall configuration screen.

Here assume the user already assigned the WAN interface to WAN zone and LAN interface to LAN1 zone.



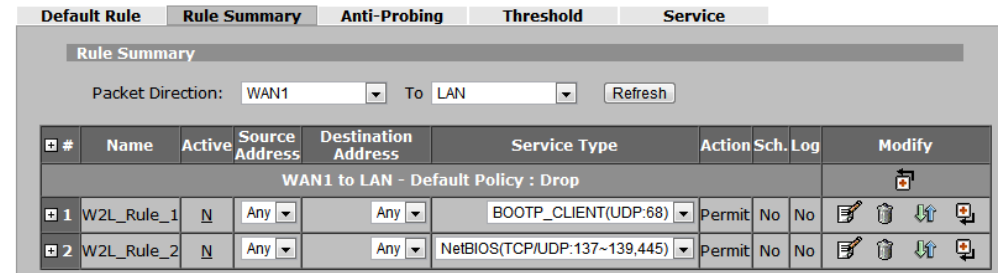
Step 5. Click the Add button to create a firewall rule to enable the FTP service to pass from WAN to LAN1.

Step 6. User can create an address object for the internal FTP server for further configuration usage. Click **Create new Object** for this function.



Step 5. Click **Rule Summary** to customize the setup. The default is to drop all packets.

FIREWALL



Step 6. Configure the firewall rule to enable the FTP service to pass from WAN1 to LAN.

- **Source IP address** is not specific
- **Destination IP address** is the FTP server’s address
- Select **FTP service** (with port 20/21) to be enabled
- Select the **Permit** action for matched packets

After this configuration, user can access the FTP server from WAN side.

Step 7. Configure the rule to:

- **Allow access** from WAN to LAN1
- **Source IP address** is not specific
- **Destination IP address** is the FTP server’s address
- Select **FTP service** (with port 20/21) to be enabled
- Select the **allow** action for matched packets

After this configuration, user can access the FTP server from WAN side.

Add Firewall Rule

Create new Object ▾

Enable

From: **WAN** ▾

To: **LAN1** ▾

Description: allow FTP service (Optional)

Schedule: none ▾

User: any ▾

Source: any ▾

Destination: **Internal_FTP** ▾

Service: **FTP** ▾

Access: **allow** ▾

Log: no ▾

OK Cancel

FIREWALL - EDIT RULE

Rule Name: **FTP**

Edit Source Address

Address Editor: Any Address ▾

Address Type: Any Address ▾

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Source Address(es): Any

Add Modify Delete

Edit Destination Address

Address Editor: Any Address ▾

Address Type: Any Address ▾

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Destination Address(es): **192.168.5.33**

Add Modify Delete

Edit Service

Available Services (See Service)

- *ECHO_REPLY(ICMP.Type:0/Code:0)
- *ECHO_REQUEST(ICMP.Type:8/Code:0)
- *VPN_NAT_T(UDP:4500)
- Any(All)
- Any(TCP)
- Any(UDP)
- Any(ICMP)
- AIM/NEW_ICQ(TCP:5190)
- AUTH(TCP:113)
- BGP(TCP:179)
- BOOTP_CLIENT(UDP:68)
- BOOTP_SERVER(UDP:67)
- CJ-SEEME(TCP/UDP:7648,24032)
- DNS(TCP/UDP:53)
- FINGER(TCP:79)

Selected Service(s): **FTP(TCP:20,21)**

<< >>

Edit Schedule

Day to Apply:

Sun Mon Tue Wed Thu Fri Sat

Time of Day to Apply: (24-Hour Format)

All day

Start: 0 (Hour) 0 (Minute) End: 0 (Hour) 0 (Minute)

Actions When Matched

Log Packet Information When Matched

Send Alert Message to Administrator When Matched

Action for Matched Packets: **Permit** ▾

Apply Cancel

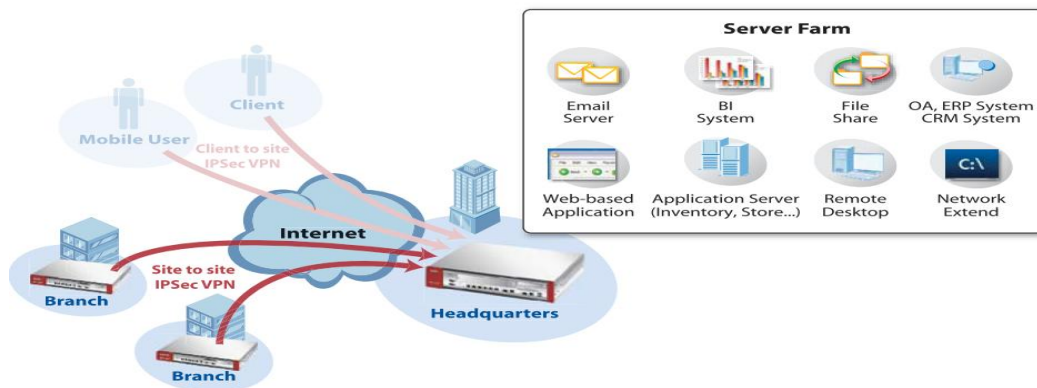
Scenario 4 — Secure site-to-site connections using IPSec VPN

4.1 Application Scenario

A virtual private network (VPN) provides secure communications between sites without the expense of leased site-to-site lines. A secure VPN is a combination of tunneling, encryption, authentication, access control and auditing. It is used to transport traffic over the Internet or any insecure network that uses TCP/IP for communication.

Internet Protocol Security (IPSec) offers standards-based VPN solutions that enable flexible scenarios for secure data communications across a public network like the Internet. An IPSec VPN tunnel is usually established in two phases. Each phase establishes a security association (SA), a contract indicating what security parameters the ZyWALL and the remote IPSec router will use. The first phase establishes an Internet Key Exchange (IKE) SA between the ZyWALL and a remote IPSec router. The second phase uses the IKE SA to securely establish an IPSec SA through which the ZyWALL and remote IPSec router can send data between computers on the local network and remote network.

The USG can provide secure site-to-site access between remote locations and corporate resources through the Internet. Using IPSec VPN, companies can secure connections to branch offices, partners and headquarters as the illustration below.



4.2 Configuration Guide

Network Conditions:

USG-50:

- WAN IP: 59.124.163.152
- Local subnet: 192.168.50.0/24

ZyWALL-5 UTM:

- WAN IP: 10.59.1.50
- Local subnet: 192.168.5.0/24

IPSec VPN Conditions:

Phase 1:

- Authentication: 1234567890
- Local/Peer ID type: IP 0.0.0.0
- Negotiation: Main mode
- Encryption Algorithm: 3DES
- Authentication Algorithm: MD5
- Key Group: DH1

Phase 2:

- Encapsulation Mode: Tunnel
- Active Protocol: ESP
- Encryption Algorithm: DES
- Authentication Algorithm: SHA1
- Perfect Forward Secrecy: None

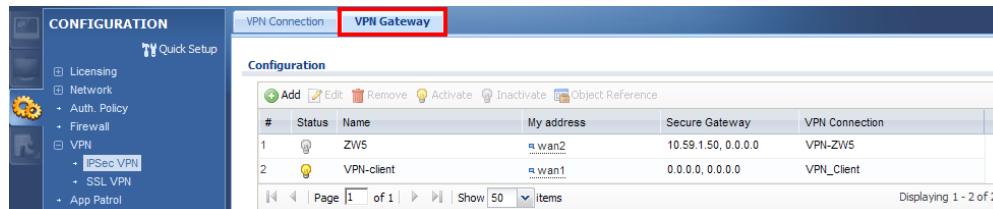
Goal to achieve:

Build up the IPSec VPN tunnel between USG-50 and ZyWALL-5 UTM with the above configuration.

ZLD configuration

Step 1. Click **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** to open the configuration screen.

Step 2. Click the **Add** button to add a VPN gateway rule.



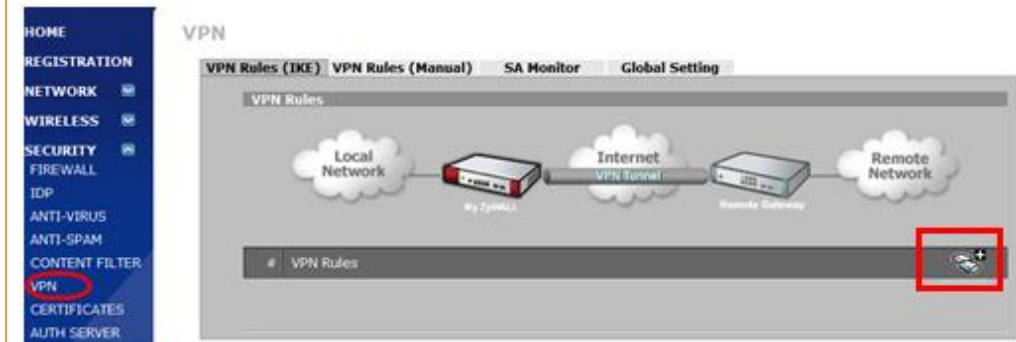
Step 3. To configure the VPN gateway rule, user needs to fill in:

- VPN gateway name
- Gateway address; both local (My Address) and peer (Peer GW Address)
- Authentication setting
 - Pre-Shared Key
 - ID Type setting (Local and Peer side)
- Phase-1 setting
 - Negotiation mode
 - Encryption algorithm
 - Authentication algorithm
 - Key Group

ZyNOS configuration

Step 1. Click **SECURITY > VPN > VPN RULES (IKE)** to open the configuration screen.

Step 2. Click the **Add** button to add a gateway policy.



Step 3. To configure the gateway policy, user needs to fill in:

- Policy name
- Gateway information; both local (My ZyWALL) and peer (Remote GW)
- Authentication setting
 - Pre-Shared Key
 - ID Type setting (Local and Peer side)
- Configure the IKE proposal
 - Negotiation mode
 - Encryption algorithm
 - Authentication algorithm
 - Key Group

Edit VPN Gateway ZW5

Hide Advanced Settings

General Settings

Enable

VPN Gateway Name:

Gateway Settings

My Address

Interface

Domain Name / IP

Peer Gateway Address

Static Address

Primary

Secondary

Dynamic Address

Authentication

Pre-Shared Key

Certificate (See My Certificates)

Local ID Type:

Content:

Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)

Negotiation Mode:

Proposal

#	Encryption	Authentication
1	3DES	MD5

Key Group:

NAT Traversal

Dead Peer Detection (DPD)

Extended Authentication

Enable Extended Authentication

Server Mode

Client Mode

User Name:

Password:

VPN - GATEWAY POLICY - EDIT

Property

Name

NAT Traversal

Gateway Policy Information

My ZyWALL

My Address (Domain Name or IP Address)

My Domain Name (See DDNS)

Primary Remote Gateway (Domain Name or IP Address)

Enable IPsec High Availability

Redundant Remote Gateway (Domain Name or IP Address)

Fall back to Primary Remote Gateway when possible

Fall Back Check Interval* (180~86400 seconds)

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

Authentication Key

Pre-Shared Key

Certificate (See My Certificates)

Local ID Type

Content

Peer ID Type

Content

Extended Authentication

Enable Extended Authentication

Server Mode (Search Local User first then RADIUS)

Client Mode

User Name

Password

IKE Proposal

Negotiation Mode

Encryption Algorithm

Authentication Algorithm

SA Life Time (Seconds)

Key Group

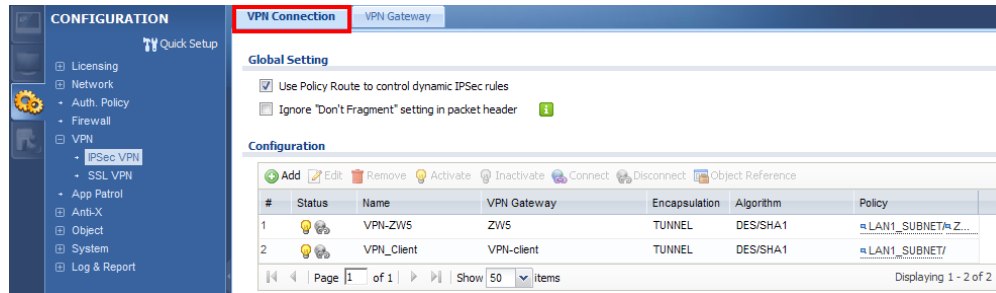
Enable Multiple Proposals

Associated Network Policies

#	Name	Local Network	Remote Network
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>			

Step 4. Click **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to open the configuration screen to configure the phase-2 rule.

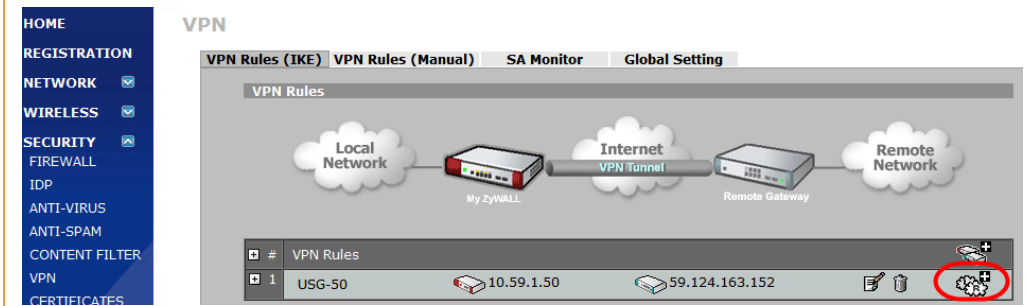
Step 5. Click the **Add** button to add a rule.



Step 6. To configure the phase-2 rule, user needs to fill in:

- VPN connection name
- VPN gateway selection
- Policy for
 - Local network side
 - Remote network side
- Phase-2 settings
 - Active protocol
 - Encapsulation mode
 - Encryption algorithm
 - Authentication algorithm
 - Perfect Forward Secrecy

Step 4. Go back to the previous page to see the newly created IKE rule. Click the **Add** button to add a Network policy.



Step 5. To configure the network policy, user needs to fill in:

- Policy name
- The gateway rule it is applied to
- Tunnel policy for
 - Local network side
 - Remote network side
- Configure the IPSec proposal
 - Encapsulation mode
 - Active protocol
 - Encryption algorithm
 - Authentication algorithm
 - Perfect Forward Secrecy

Edit VPN Connection VPN-ZW5

Hide Advanced Settings Create new Object

General Settings

Enable

Connection Name: **VPN-ZW5**

Nailed-Up

Enable Replay Detection

Enable NetBIOS broadcast over IPSec

VPN Gateway

Application Scenario

Site-to-site

Site-to-site with Dynamic Peer

Remote Access (Server Role)

Remote Access (Client Role)

VPN Gateway: **ZW5** wan2 10.59.1.50 0.0.0.0

Manual Key

Manual Key

My Address:

Secure Gateway Address:

SPI: (256 - 4095)

Encapsulation Mode: Tunnel

Policy

Local policy: **LAN1_SUBNET** INTERFACE SUBNET, 192.168.50.0/24

Remote policy: **ZW5-LAN** SUBNET, 192.168.5.0/24

Policy Enforcement

Phase 2 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS): none

VPN - NETWORK POLICY - EDIT

Property

Active

Name: **VPN-USG50**

Protocol: 0

Nailed-Up

Allow NetBIOS broadcast Traffic Through IPSec Tunnel

Check IPSec Tunnel Connectivity Log

Ping this Address: 0 . 0 . 0 . 0

Gateway Policy Information

Gateway Policy: **USG-50**

Virtual Address Mapping Rule:

Active

Virtual Address Mapping Rule: Port Forwarding Rules

Type: One-to-One

Private Starting IP Address: 0 . 0 . 0 . 0

Private Ending IP Address: 0 . 0 . 0 . 0

Virtual Starting IP Address: 0 . 0 . 0 . 0

Virtual Ending IP Address: 0 . 0 . 0 . 0

Local Network

Address Type: Subnet Address

Starting IP Address: 192 . 168 . 5 . 0

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

Local Port: Start 0 End 0

Remote Network

Address Type: Subnet Address

Starting IP Address: 192 . 168 . 50 . 0

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

Remote Port: Start 0 End 0

IPSec Proposal

Encapsulation Mode: Tunnel

Active Protocol: ESP

Encryption Algorithm: DES

Authentication Algorithm: SHA1

SA Life Time (Seconds): 28800

Perfect Forward Secrecy (PFS): NONE

Enable Replay Detection

Enable Multiple Proposals

Apply Cancel

Connectivity Check

Enable Connectivity Check i

Check Method:

Check Period: (5-30 Seconds)

Check Timeout: (1-10 Seconds)

Check Fail Tolerance: (1-10)

Check This Address Domain Name or IP Address

Check the First and Last IP Address in the Remote Policy

Log

Inbound/Outbound traffic NAT

Outbound Traffic

Source NAT

Source:

Destination:

SNAT:

Inbound Traffic

Source NAT

Source:

Destination:

SNAT:

Destination NAT

#	Original IP	Mapped IP	Protocol	Original ...	Original ...	Mapped ...	Mapped ...
No data to display							

Step 6. After saving the network policy, user can see the IPSec VPN configuration is complete. Click the **Connect** button to enable the VPN tunnel.

VPN

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

VPN Rules

#	VPN Rules	Local Network	Remote Network	Actions
1	USG-50	10.59.1.50	59.124.163.152	[Edit] [Delete] [Refresh] [Connect]
	Y VPN-USG50	192.168.5.0 / 255.255.255.0	192.168.50.0 / 255.255.255.0	[Up] [Down] [Refresh] [Connect]

Step 7. After the VPN tunnel is established, user can find the SA information on **SECURITY > VPN > SA Monitor**.

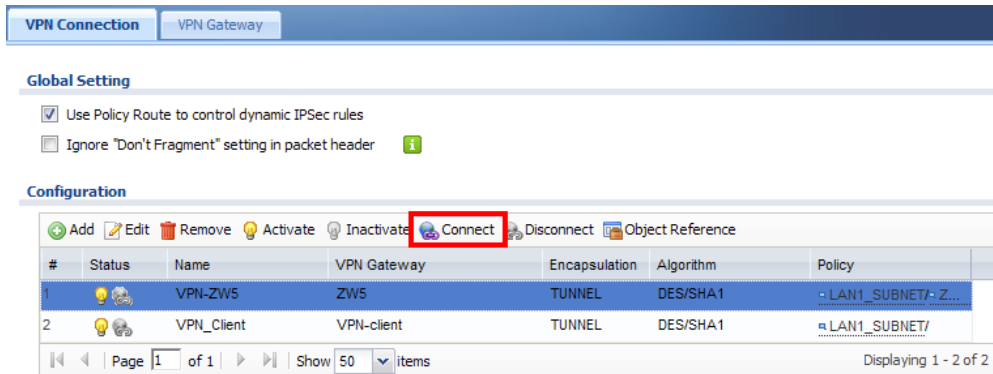
VPN

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

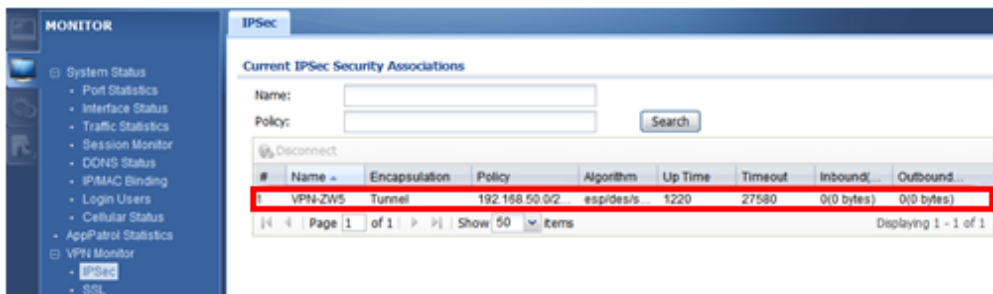
Security Associations Table

#	Name	Local Network	Remote Network	Encapsulation	IPSec Algorithm
1	VPN-USG50	192.168.5.0 / 255.255.255.0	192.168.50.0 / 255.255.255.0	Tunnel	ESP DES--SHA1

Step 7. After setting the rule, user can select the rule and click the **Connect** button to establish the VPN link. Once the tunnel is established, a **connected** icon will be displayed in front of the rule.



Step 8. When the VPN tunnel is established, user can find the SA information on **MONITOR > VPN MONITOR > IPSec**.

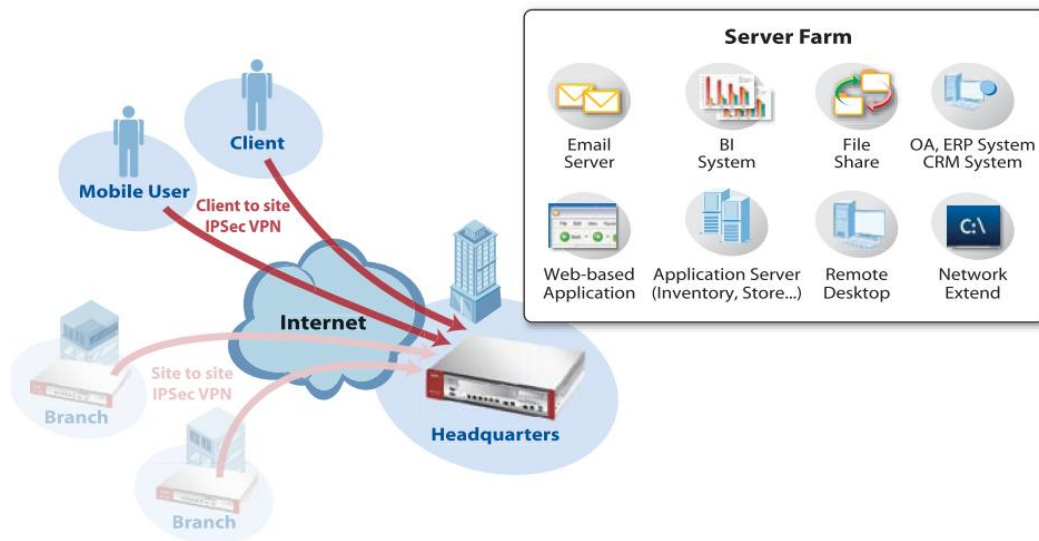


Scenario 5 — Secure client-to-site connections using IPSec VPN

5.1 Application Scenario

The ZyWALL USG Series can provide secure access between remote locations and corporate resources through the Internet for organizations of any size. Using IPSec VPN, companies can secure connections to branch offices, partners and headquarters.

Road warriors and telecommuters can use SSL or L2TP VPN to safely access the company network without having to install VPN software. ZyWALL USG Series provides a flexible and easy way to enable mobile employees, vendors and partners to confidentially access your network resource for better efficiency.



5.2 Configuration Guide

Network Conditions:

USG-50:

- WAN IP: 10.59.1.39
- Local subnet: 192.168.50.0/24

ZyWALL-5 UTM:

- WAN IP: 10.59.1.50
- Local subnet: 192.168.5.0/24

IPSec VPN Conditions:

Phase 1:

- Authentication: 1234567890
- Local/Peer ID type: IP 0.0.0.0
- Negotiation: Main mode
- Encryption Algorithm: 3DES
- Authentication Algorithm: MD5
- Key Group: DH1

Phase 2:

- Encapsulation Mode: Tunnel
- Active Protocol: ESP
- Encryption Algorithm: DES
- Authentication Algorithm: SHA1
- Perfect Forward Secrecy: None

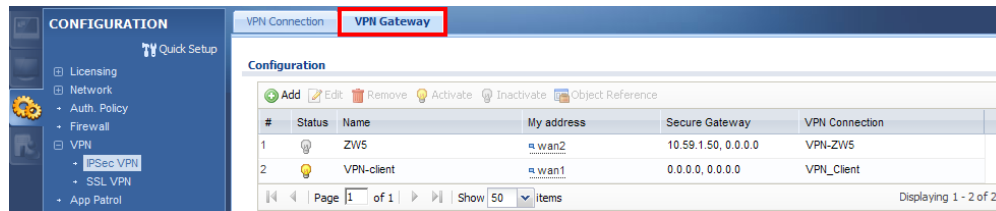
Goal to achieve:

Build up an IPSec VPN tunnel for mobile user's dynamic access to USG-50 or ZyWALL-5 UTM with the above configuration.

ZLD configuration

Step 1. Click **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** to open the configuration screen.

Step 2. Click the **Add** button to add a VPN gateway rule.



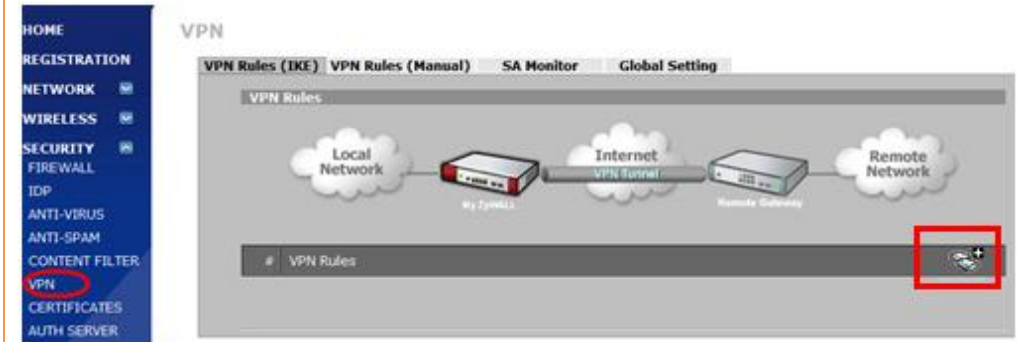
Step 3. To configure the VPN gateway rule, user needs to fill in:

- VPN gateway name
- Gateway address; both local (My Address) and peer (Dynamic Address)
- Authentication setting
 - Pre-Shared Key
 - ID Type setting (Local and Peer side)
- Phase-1 setting
 - Negotiation mode
 - Encryption algorithm
 - Authentication algorithm
 - Key Group

ZyNOS configuration

Step 1. Click **SECURITY > VPN > VPN RULES (IKE)** to open the configuration screen.

Step 2. Click the **Add** button to add a gateway policy.



Step 3. To configure the gateway policy, user needs to fill in:

- Policy name
- Gateway information; both local (My ZyWALL) and peer ("0.0.0.0" for dynamic access)
- Authentication setting
 - Pre-Shared Key
 - ID Type setting (Local and Peer side)
- Configure the IKE proposal
 - Negotiation mode
 - Encryption algorithm
 - Authentication algorithm
 - Key Group

Edit VPN Gateway VPN-client

Hide Advanced Settings

General Settings

Enable
VPN Gateway Name:

Gateway Settings

My Address

Interface: DHCP client -- 10.59.1.61/255.255.255.0
 Domain Name / IP:

Peer Gateway Address

Static Address
Primary:
Secondary:
 Dynamic Address

Authentication

Pre-Shared Key:
 Certificate: (See My Certificates)
Local ID Type:
Content:

Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)
Negotiation Mode:
Proposal:

#	Encryption	Authentication
1	3DES	MD5

Key Group:
 NAT Traversal
 Dead Peer Detection (DPD)

Extended Authentication

Enable Extended Authentication
 Server Mode:
 Client Mode
User Name:
Password:

VPN - GATEWAY POLICY - EDIT

Property

Name:
 NAT Traversal

Gateway Policy Information

My ZyWALL
 My Address: (Domain Name or IP Address)
 My Domain Name: (See DDNS)
 Primary Remote Gateway: (Domain Name or IP Address)
 Enable IPsec High Availability
 Redundant Remote Gateway: (Domain Name or IP Address)
 Fall back to Primary Remote Gateway when possible
Fall Back Check Interval*: (180~86400 seconds)

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

Authentication Key

Pre-Shared Key:
 Certificate: (See My Certificates)
Local ID Type:
Content:
Peer ID Type:
Content:

Extended Authentication

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

IKE Proposal

Negotiation Mode:
Encryption Algorithm:
Authentication Algorithm:
SA Life Time (Seconds):
Key Group:
 Enable Multiple Proposals

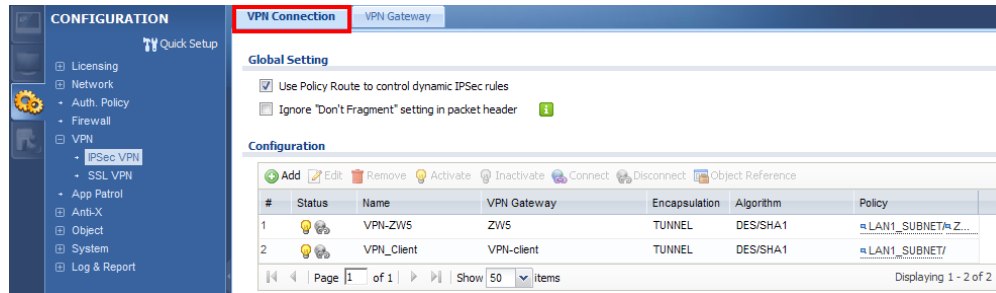
Associated Network Policies

#	Name	Local Network	Remote Network
---	------	---------------	----------------

Apply Cancel

Step 4. Click **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to open the configuration screen to configure the phase-2 rule.

Step 5. Click **Add** button to add a rule.

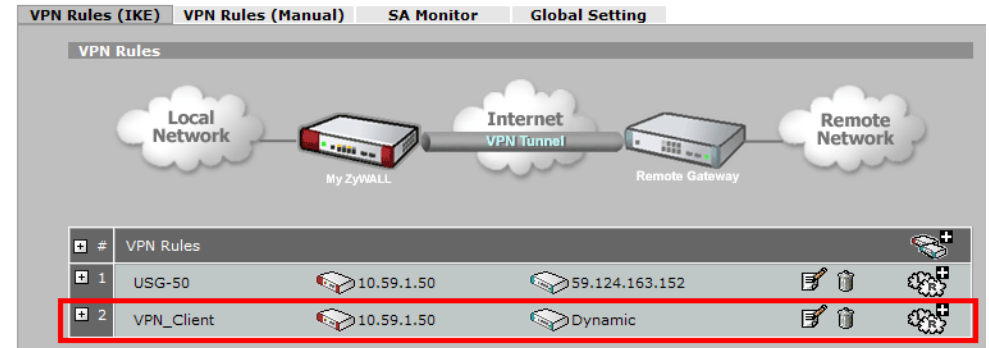


Step 6. To configure the phase-2 rule, user needs to fill in:

- VPN connection name
- VPN gateway selection
- Policy for
 - Local network side
 - Remote network side
- Phase-2 setting
 - Active protocol
 - Encapsulation mode
 - Encryption algorithm
 - Authentication algorithm
 - Perfect Forward Secrecy

Step 4. Go back to the previous page, to see the newly created IKE rule with the destination **Dynamic**. Click the **Add** button to add a Network policy.

VPN



Step 5. To configure the network policy, user needs to fill in:

- Policy name
- The gateway rule it is applied to
- Tunnel policy for
 - Local network side
 - Remote network side; "0.0.0.0" means for dynamic access
- Configure the IPSec proposal
 - Encapsulation mode
 - Active protocol
 - Encryption algorithm
 - Authentication algorithm
 - Perfect Forward Secrecy

Edit VPN Connection VPN_Client

Hide Advanced Settings | Create new Object

General Settings

Enable

Connection Name: **VPN_Client**

Nailed-Up

Enable Replay Detection

Enable NetBIOS broadcast over IPsec

VPN Gateway

Application Scenario

Site-to-site

Site-to-site with Dynamic Peer

Remote Access (Server Role)

Remote Access (Client Role)

VPN Gateway: **VPN-client** wan1 0.0.0.0 0.0.0.0

Manual Key

Manual Key

My Address:

Secure Gateway Address:

SPI: (256 - 4095)

Active Protocol:

Encryption Algorithm:

Authentication Algorithm:

Encryption Key:

Authentication Key:

Policy

Local policy: **LAN1_SUBNET** INTERFACE SUBNET, 192.168.50.0/24

Policy Enforcement

Phase 2 Settings

SA Life Time: (180 - 3000000 Seconds)

Active Protocol:

Encapsulation:

Proposal

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS):

VPN - NETWORK POLICY - EDIT

Property

Active

Name: **Mobile_User**

Protocol:

Nailed-Up

Allow NetBIOS broadcast Traffic Through IPsec Tunnel

Check IPsec Tunnel Connectivity Log

Ping this Address:

Gateway Policy Information

Gateway Policy: **VPN_Client**

Virtual Address Mapping Rule:

Active

Virtual Address Mapping Rule:

Type:

Private Starting IP Address:

Private Ending IP Address:

Virtual Starting IP Address:

Virtual Ending IP Address:

Local Network

Address Type:

Starting IP Address:

Ending IP Address / Subnet Mask:

Local Port: Start End

Remote Network

Address Type:

Starting IP Address:

Ending IP Address / Subnet Mask:

Remote Port: Start End

IPsec Proposal

Encapsulation Mode:

Active Protocol:

Encryption Algorithm:

Authentication Algorithm:

SA Life Time (Seconds):

Perfect Forward Secrecy (PFS):

Enable Replay Detection

Enable Multiple Proposals

Connectivity Check

Enable Connectivity Check i

Check Method:

Check Period: (5-30 Seconds)

Check Timeout: (1-10 Seconds)

Check Fail Tolerance: (1-10)

Check This Address Domain Name or IP Address

Check the First and Last IP Address in the Remote Policy

Log

Inbound/Outbound traffic NAT

Outbound Traffic

Source NAT

Source:

Destination:

SNAT:

Inbound Traffic

Source NAT

Source:

Destination:

SNAT:

Destination NAT

#	Original IP	Mapped IP	Protocol	Original ...	Original ...	Mapped ...	Mapped ...
No data to display							

Page 1 of 1 | Show 50 items

Step 6. After setting up the network policy, user can see the IPsec VPN configuration is complete. Note that the destination is **Any**.

VPN

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

VPN Rules

#	VPN Rules	Local IP	Remote IP	Remote Policy
1	USG-50	10.59.1.50	59.124.163.152	
2	VPN_Client	10.59.1.50	Dynamic	Any

Step 7. Start the ZyXEL IPsec VPN Client. Fill in the Phase-1 configuration.

ZyWALL IPsec VPN Client

File | VPN Configuration | View | Tools | ?

ZyXEL

Console | Parameters | Connections

Phase1 (Authentication)

Name:

Interface:

Remote Gateway:

Preshared Key

Confirm:

Certificate

IKE

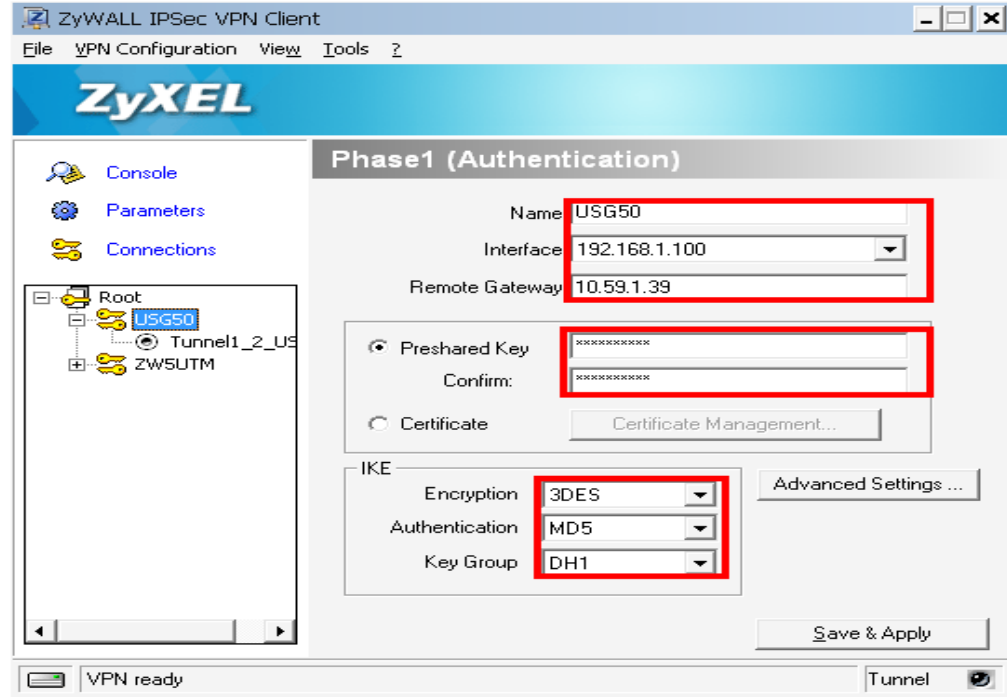
Encryption:

Authentication:

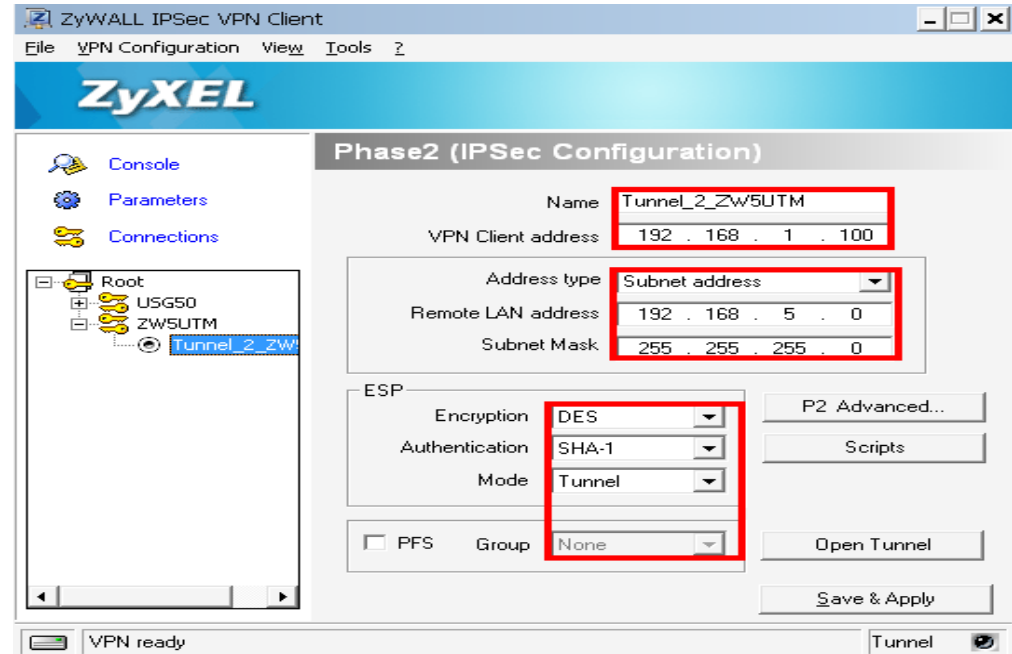
Key Group:

VPN ready | Tunnel

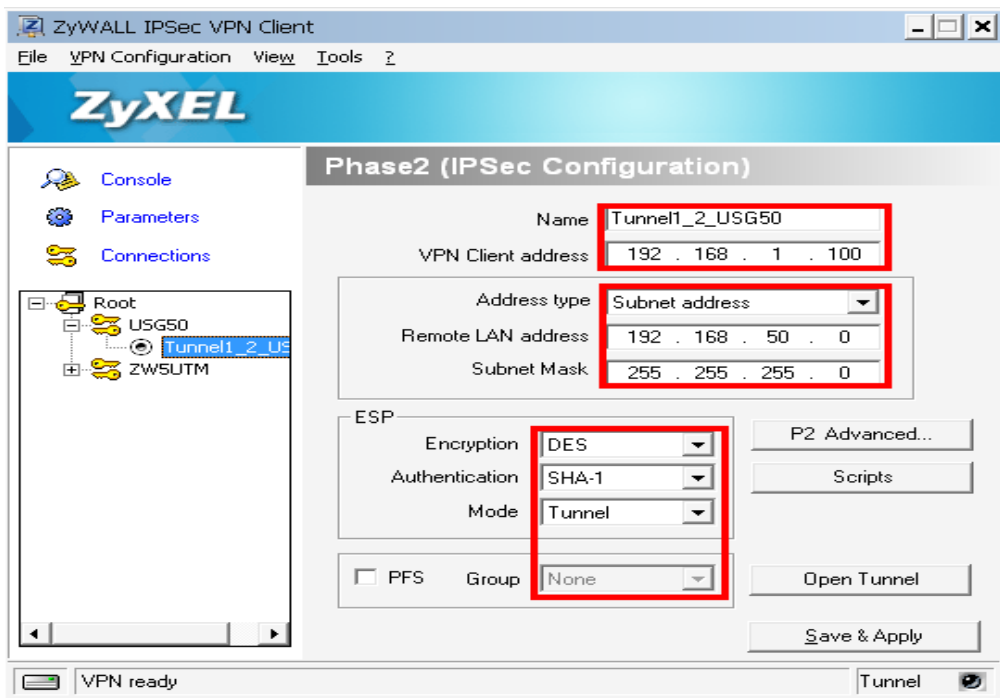
Step 7. Start the ZyXEL IPsec VPN Client. Fill in the Phase-1 configuration. Note that the USG series does not support the “Config Mode” in phase-1 advanced setting, thus users must avoid selecting it when performing configuration.



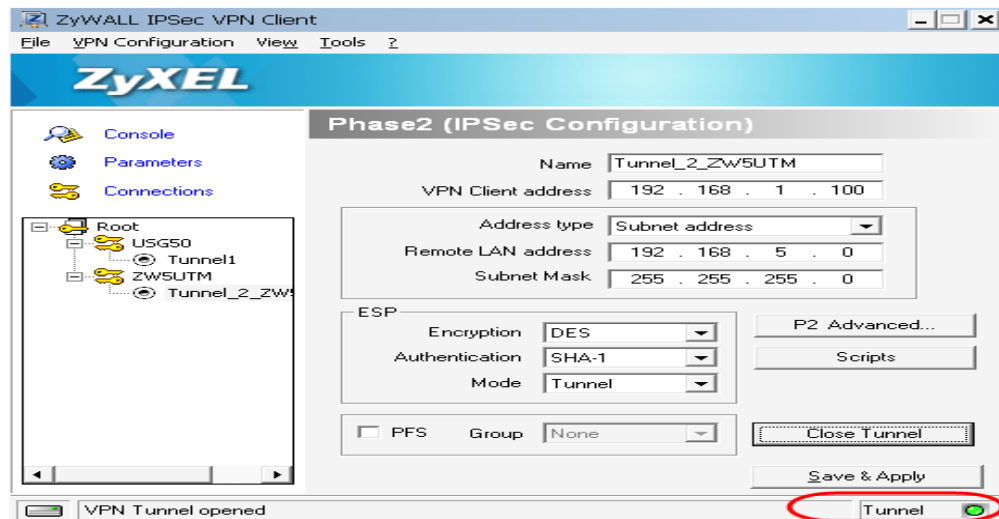
Step 8. Configure the phase-2 parameters.



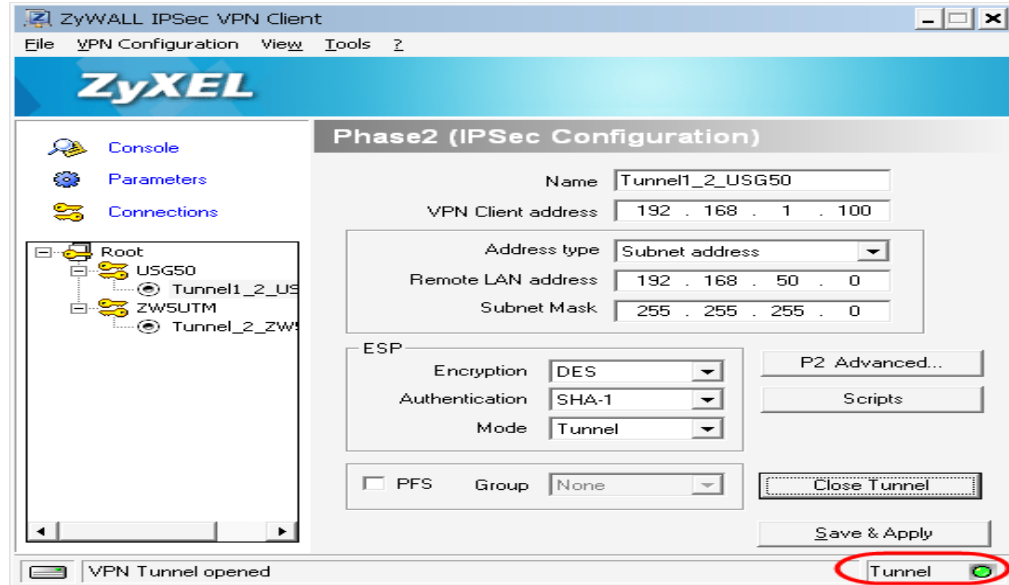
Step 8. Configure the phase-2 parameters.



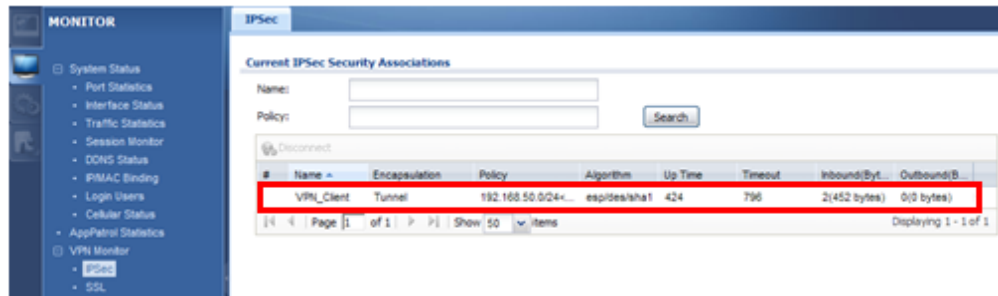
Step 9. Because it is a dynamic rule, user MUST enable it from the VPN client. Click **Open Tunnel** to enable it. The icon will change to green if established successfully.



Step 9. Because it is a dynamic rule, user **MUST** enable it from the VPN client. Click **Open Tunnel** to enable it. The icon will change to green if established successfully.



Step 10. When the VPN tunnel is established, user can find the SA information on **MONITOR > VPN MONITOR > IPsec**.

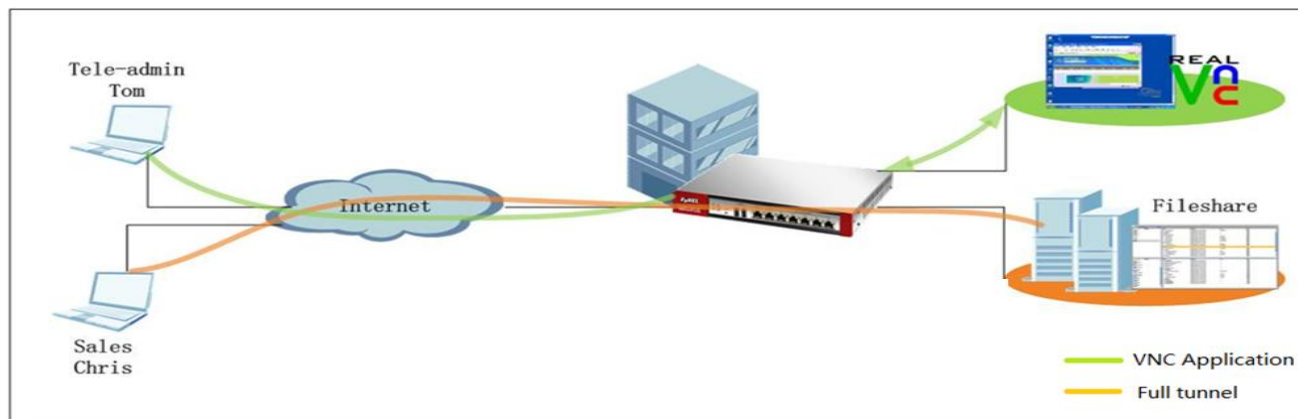


Scenario 6 — Deploying SSL VPN for Tele-workers to Access Company Resources (USG 50 only)

6.1 Application Scenario

Tele-workers who work out of the office sometimes need to access company resources by a secured way. While building an IPSec tunnel to the company gateway is an option, the Windows VPN client configuration is too complicated, and for an easier way to configure IPSec VPN, it requires installation of additional IPSec VPN client software. The USG ZyWALL provides an SSL VPN function, which enables teleworkers to access company resources through a secured VPN tunnel with little effort. All they need on their PC is a browser. Besides, in SSL VPN, the network administrator can define different access rules to allow different users to access different company resources.

For example, the network administrator can set up an SSL VPN rule to allow administrator Tom remotely control company servers by RDP or VNC through SSL VPN tunnel. He can also set up an SSL VPN Full tunnel rule to allow sales Chris to remotely access company file-share resources to conduct his important daily job.



NOTE: USG 50 supports RDP, VNC, WEB link application and SSL VPN full tunnel, but doesn't support SSL VPN file-share and OWA applications so far. If the remote clients want to use file-share and OWA through SSL VPN, they can use SSL VPN full tunnel mode (Security Extender) as a workaround.

6.2 Configuration Guide

Network Conditions:

- WAN IP: 172.25.27.62
- LAN subnet: 192.168.1.0/24
- VNC server IP: 192.168.1.5

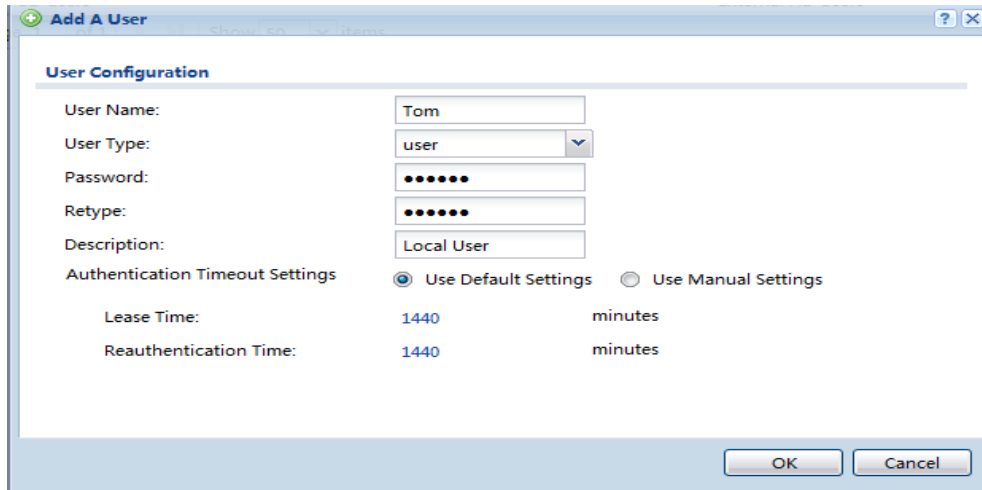
Goals to achieve:

- 1) Tom in tele-admin group can VNC to the internal server 192.168.1.5 by SSL VPN application.
- 2) Chris in sales group can access company fileshare resources in the LAN subnet through SSL VPN full tunnel.

ZLD configuration

Step 1. Create two local user accounts for Tom and Chris on USG50.

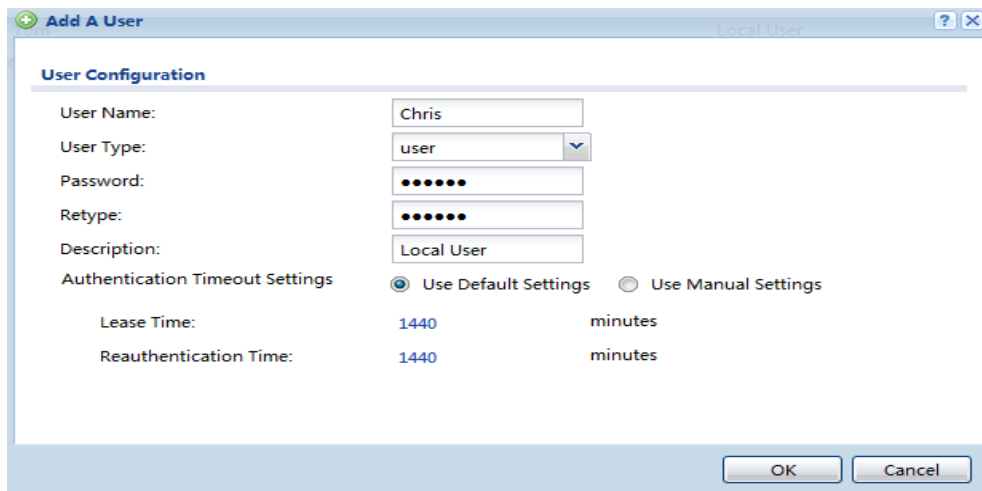
Go to **Configuration > Object > User/Group**, add two local user accounts for Tom and Chris:



The screenshot shows the 'Add A User' dialog box with the following configuration:

- User Name: Tom
- User Type: user
- Password: [masked]
- Retype: [masked]
- Description: Local User
- Authentication Timeout Settings:
 - Use Default Settings
 - Use Manual Settings
- Lease Time: 1440 minutes
- Reauthentication Time: 1440 minutes

Buttons: OK, Cancel



The screenshot shows the 'Add A User' dialog box with the following configuration:

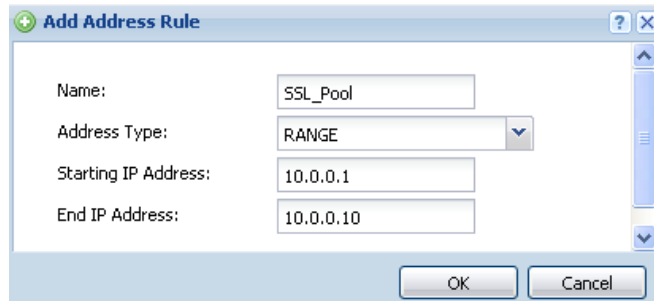
- User Name: Chris
- User Type: user
- Password: [masked]
- Retype: [masked]
- Description: Local User
- Authentication Timeout Settings:
 - Use Default Settings
 - Use Manual Settings
- Lease Time: 1440 minutes
- Reauthentication Time: 1440 minutes

Buttons: OK, Cancel

ZyNOS configuration

ZyNOS ZyWALL does not support SSL VPN.

Step 2. Go to **Configuration > Object > Address**. Add an IP address pool for the SSL VPN full tunnel mode access (Security Extender).

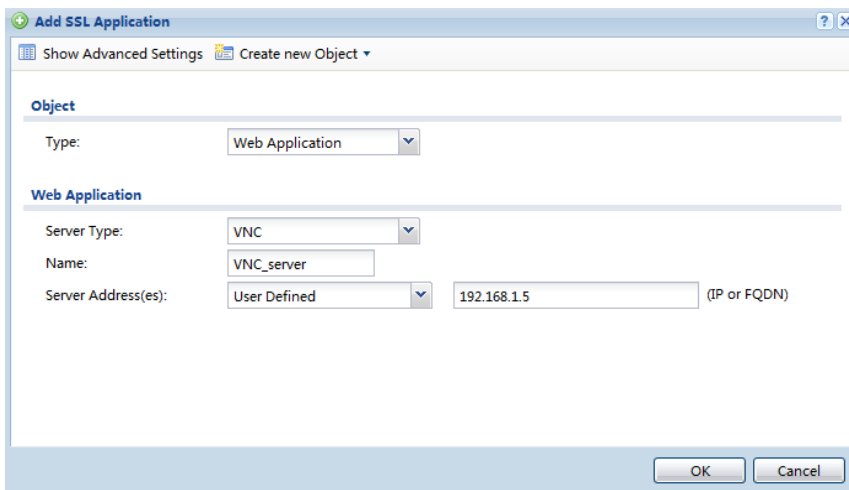


The screenshot shows the 'Add Address Rule' dialog box. It contains the following fields:

- Name: SSL_Pool
- Address Type: RANGE
- Starting IP Address: 10.0.0.1
- End IP Address: 10.0.0.10

Buttons: OK, Cancel

Step 3. Go to **Configuration > Object > SSL Application**. Create an SSL application object for the VNC server.



The screenshot shows the 'Add SSL Application' dialog box. It contains the following fields:

- Object Type: Web Application
- Web Application Server Type: VNC
- Name: VNC_server
- Server Address(es): User Defined, 192.168.1.5 (IP or FQDN)

Buttons: OK, Cancel

Step4. Go to **Configuration > VPN > SSL VPN**. Add an SSL VPN rule for Tom to access.

- Allow the user “Tom” to access this rule.
- Add the VNC application to SSL Application.

Add Access Policy

Create new Object ▾

Configuration

Enable Policy

Name: For_Tom

Description: New Create (Optional)

Clean browser cache when user logs out ⓘ

User/Group

Selectable User/Group Objects

- admin
- ldap-users
- radius-users
- ad-users
- Chris

Selected User/Group Objects

=== Object ===

- Tom

Endpoint Security (EPS)

Enable EPS Checking

Periodical checking time 1 (1-1440 minutes)

Selectable EPS Objects

Selected EPS Objects

Endpoint needs to match at least one EPS object.

SSL Application List (Optional)

Selectable Application Objects

Selected Application Objects

- VNC_server

OK Cancel

Step5. Go to **Configuration > VPN > SSL VPN**. Add an SSL VPN rule for Chris to access.

- Allow the user “Chris” to access this rule.
- Enable Network Extension, assign the address pool for SSL VPN clients, and select the USG internal network to allow SSL VPN clients to access.

Add Access Policy

Create new Object ▾

Configuration

Enable Policy

Name: For_Chris

Description: New Create (Optional)

Clean browser cache when user logs out ⓘ

User/Group

Selectable User/Group Objects

- admin
- Idap-users
- radius-users
- ad-users
- Tom

Selected User/Group Objects

==== Object ====

- Chris

Endpoint Security (EPS)

Network Extension (Optional)

Enable Network Extension

Assign IP Pool: SSL_Pool RANGE 10.0.0.1-10.0.0.10

DNS Server 1: none

DNS Server 2: none

WINS Server 1: none

WINS Server 2: none

Network List

Selectable Address Objects

- DMZ1_SUBNET
- DMZ2_SUBNET
- WIZ_VPN_LOCAL
- WIZ_VPN_REMOTE
- manager_IP

Selected Address Objects

- LAN1_SUBNET

OK Cancel

Check the created policies as below:

Access Policy Summary

Add
 Edit
 Remove
 Activate
 Inactivate
 Move
 Object Reference

#	Status	Name	User/Group	Access Policy Summary
1		For_Chris	Chris	
2		For_Tom	Tom	VNC_server


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

Scenario Verification

a. Log in with user “Tom”:

Open the USG login page. Make sure Java is installed and enabled in your browser. Use user “Tom” to log into SSL VPN.

NOTE: To use the SSL VPN RDP application, user must use IE.



ZyXEL
ZyWALL USG 1000

Enter User Name/Password and click to login.

User Name:

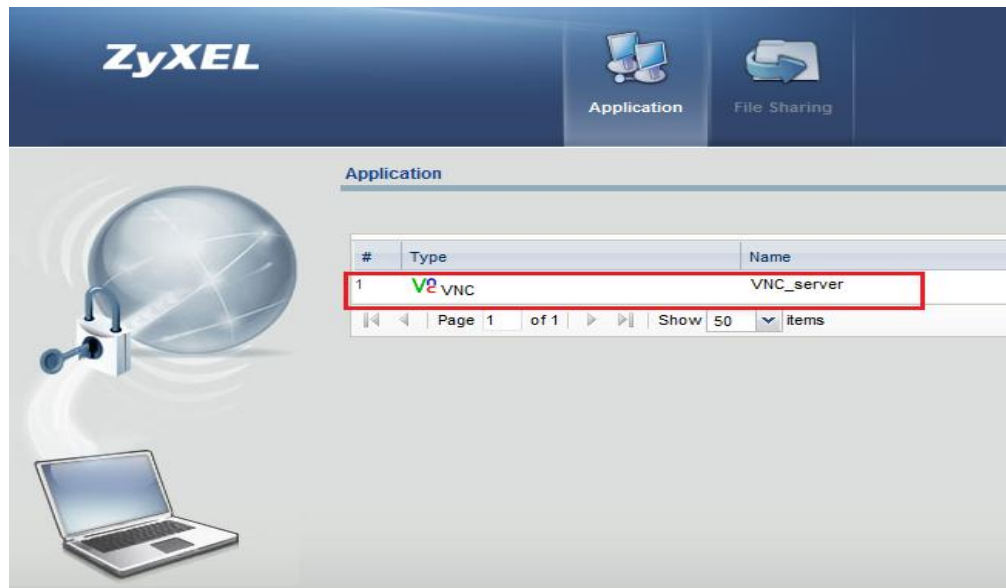
Password:

One-Time Password: (Optional)
(max. 63 alphanumeric, printable characters and no spaces)

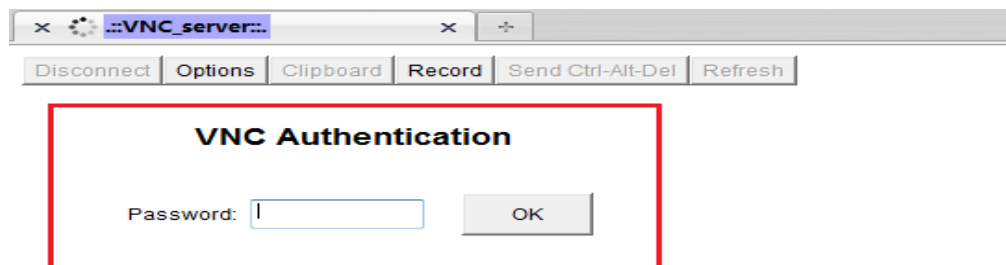
Note:

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

SSL VPN is established. You can see the VNC server on the VPN portal.



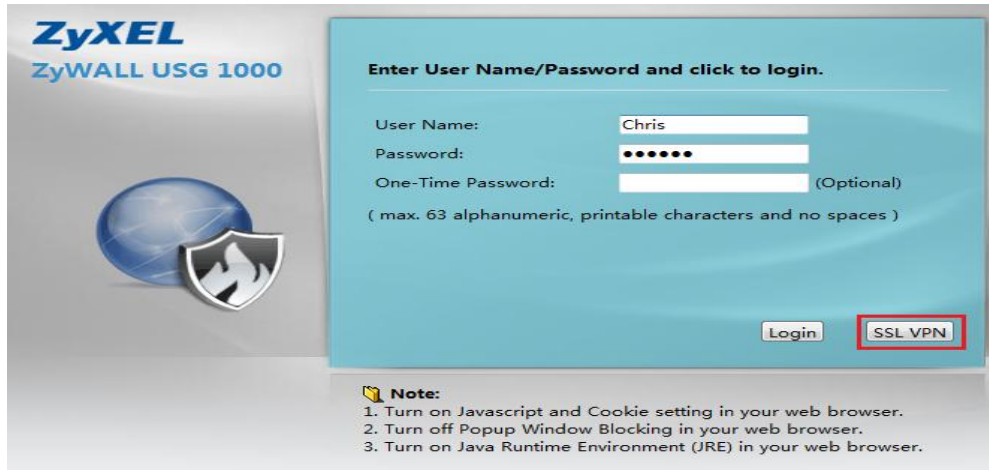
User can just click on the VNC application and access the VNC server.



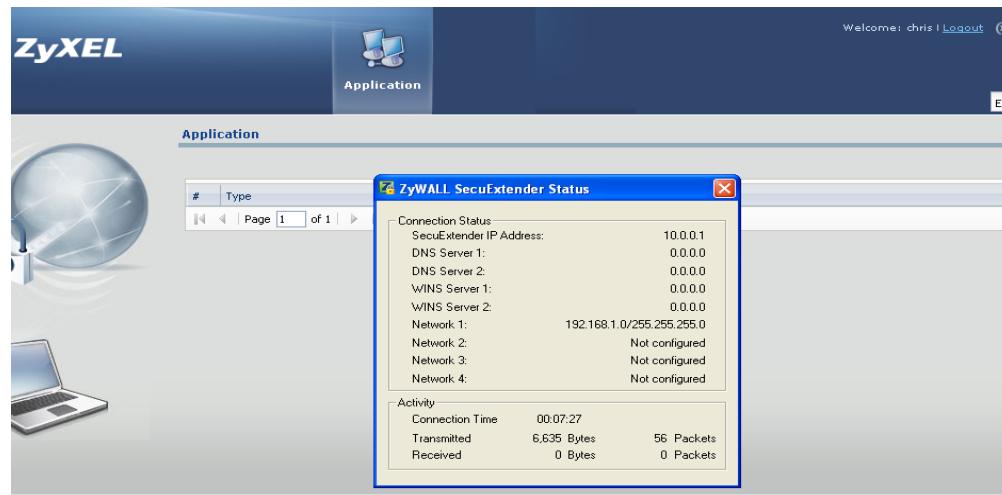
Input the correct password for VNC login, and click OK, the VNC connection will be established.

b. Log in with user “Chris”:

Open the USG login page. Make sure Java is installed and enabled in your browser. Use user “Chris” to log into SSL VPN.



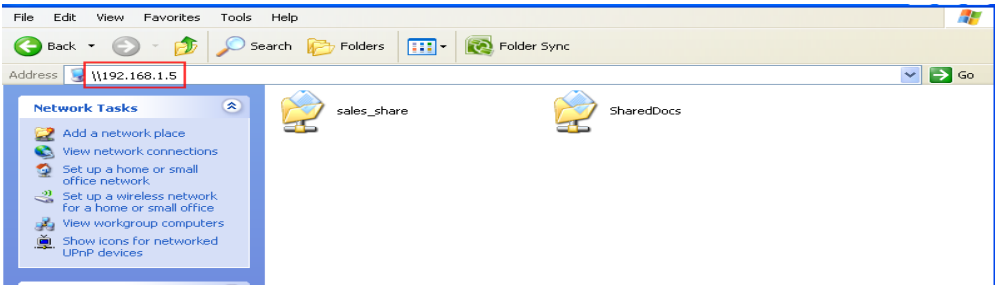
Full tunnel SSL VPN (Security Extender) will be established.



You can check the client’s routing table after the full tunnel is established.

```
C:\Documents and Settings\Administrator>route print
=====
Interface List
0x1 ..... MS TCP Loopback interface
0x2 ...00 1b 78 86 b6 89 ..... Realtek RTL8169/8110 Family Gigabit Ethernet NI
- Packet Scheduler Miniport
0x40004 ...00 53 45 00 00 00 ..... WAN (PPP/SLIP) Interface
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                    0.0.0.0          172.25.27.252   172.25.27.35     2
0.0.0.0                    0.0.0.0          172.25.27.254   172.25.27.35     20
10.0.0.1                   255.255.255.255  127.0.0.1      127.0.0.1        50
10.255.255.255             255.255.255.255  10.0.0.1       10.0.0.1         50
127.0.0.0                  255.0.0.0        127.0.0.1      127.0.0.1        1
172.20.0.0                 255.255.0.0      172.25.27.254  172.25.27.35     2
172.23.0.0                 255.255.0.0      172.25.27.254  172.25.27.35     2
172.25.0.0                 255.255.0.0      172.25.27.254  172.25.27.35     2
172.25.5.0                 255.255.255.0    172.25.27.254  172.25.27.35     2
172.25.27.0                255.255.255.0    172.25.27.35   172.25.27.35     20
172.25.27.35               255.255.255.255  127.0.0.1      127.0.0.1        20
172.25.255.255             255.255.255.255  172.25.27.35   172.25.27.35     20
192.168.1.0                255.255.255.0    192.168.200.1  10.0.0.1         1
192.168.200.1              255.255.255.255  10.0.0.1       10.0.0.1         1
224.0.0.0                  240.0.0.0        10.0.0.1       10.0.0.1         50
224.0.0.0                  240.0.0.0        172.25.27.35   172.25.27.35     20
255.255.255.255           255.255.255.255  10.0.0.1       10.0.0.1         1
255.255.255.255           255.255.255.255  172.25.27.35   172.25.27.35     20
```

The client can access the LAN resources by their private IP’s as if he were in the same local network with the LAN hosts. In this example, the user can access the file share server in USG LAN subnet.

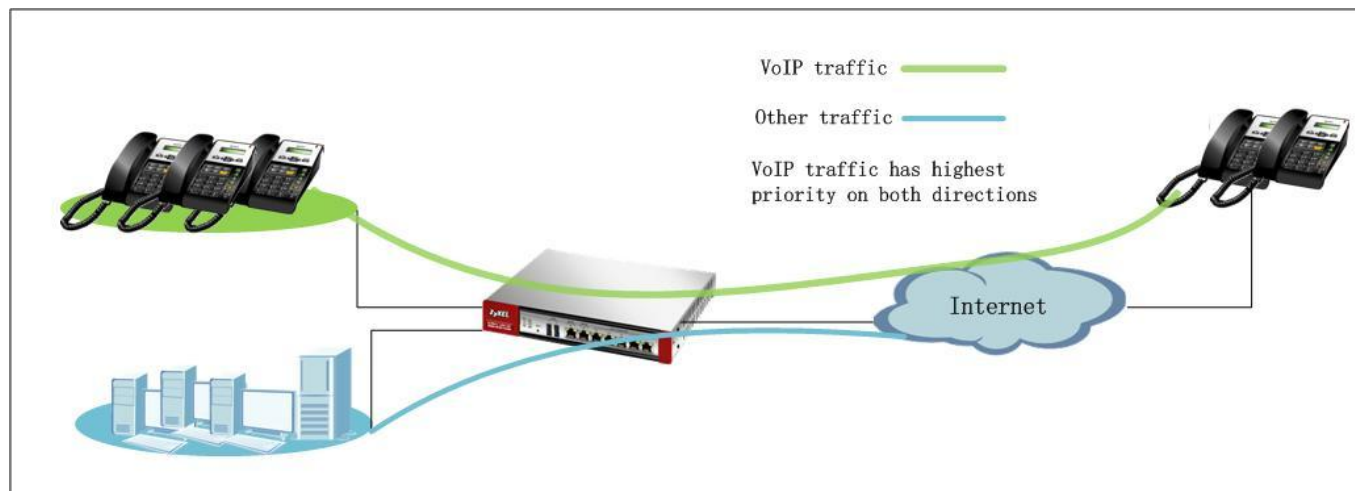


Scenario 7 — Reserving Highest Bandwidth Management Priority for VoIP Traffic

7.1 Application Scenario

In an enterprise network, there are various types of traffic. But the company Internet connection bandwidth is limited to a specific value. All this traffic will contend to use the limited bandwidth, which may result in some important traffic, for example, VoIP traffic getting slow or even starved. Therefore, intelligent bandwidth management for improved productivity becomes a matter of high concern for network administrators. ZyXEL ZyWALL provides Bandwidth Management (BWM) function to effectively manage bandwidth according to different flexible criteria.

VoIP traffic is quite sensitive to delay and jitter. Therefore, in an enterprise company, VoIP traffic should usually be awarded the highest priority over all other types of traffic.



7.2 Configuration Guide

Network Conditions:

- WAN download bandwidth: 2M
- WAN upload bandwidth: 1M

Goal to achieve:

Make sure VoIP traffic has the highest priority over all other traffic.

ZLD configuration

<< ZyWALL USG50 configuration steps >>

Step 1. Go to **Configuration > Network > ALG**, enable SIP ALG.

SIP Settings

Enable SIP ALG

Enable SIP Transformations

Enable Configure SIP Inactivity Timeout

SIP Media Inactivity Timeout : (seconds)

SIP Signaling Inactivity Timeout : (seconds)

SIP Signaling Port :

#	Port
1	5060

ZyNOS configuration

Step 1. Go to **Advanced > ALG**, enable SIP ALG.

(If you want to use BWM to manage VoIP traffic, SIP ALG must be enabled.)

ALG

ALG Settings

Enable FTP ALG

Enable H.323 ALG

Enable SIP ALG

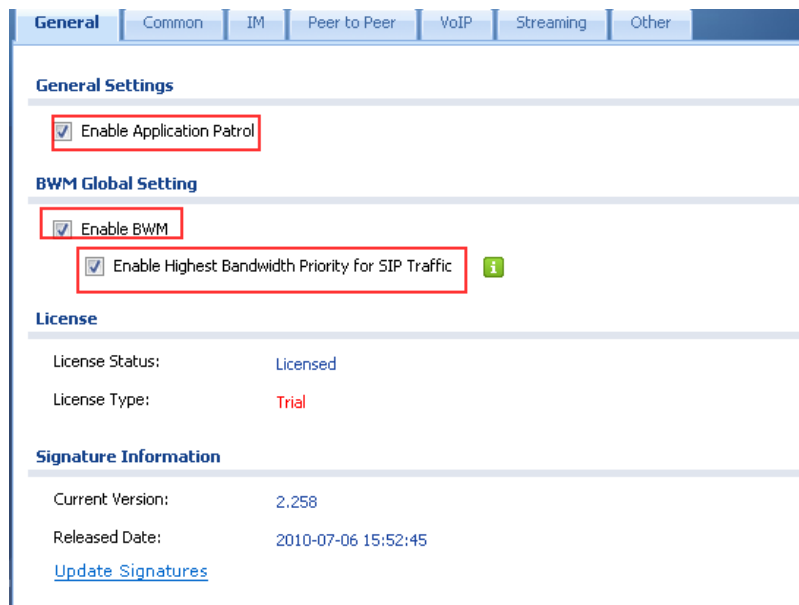
SIP Timeout (seconds, 0 means no timeout)

Apply

Reset

Step 2. Go to **Configuration > App Patrol > General**, enable **Application Patrol**, enable **BWM** and enable **Highest Bandwidth Priority for SIP Traffic**.

Enabling **Highest Bandwidth Priority for SIP Traffic** forces the device to give SIP traffic the highest bandwidth priority. When this option is enabled the system ignores the bandwidth management settings of all application patrol rules for SIP traffic and does not record SIP traffic bandwidth usage statistics.



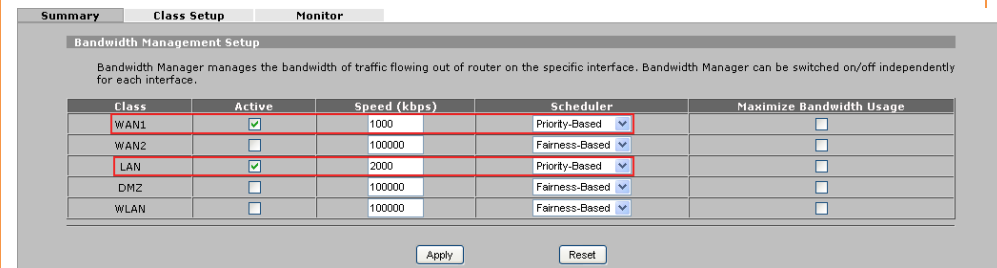
NOTE: You need to register IDP/App Patrol license to use App Patrol.

Step 2. Go to **Advanced > BW Management > Summary**.

Enable WAN1 interface. Since ISP upload speed is 1 Mbps, set WAN1 speed to 1000 kbps.

Choose **Priority-Based Scheduler**.

Enable LAN interface. Since ISP download speed is 2 Mbps, set LAN speed to 2000 kbps.



Step3. Go to **Advanced > BW Management > Class Setup**.

Add Sub-Class under interface WAN1 to manage upload traffic.



<< ZyWALL USG20/20W configuration steps >>

Step 1. Go to **Configuration > Network > ALG**, enable **SIP ALG**.

SIP Settings

Enable SIP ALG

Enable SIP Transformations

Enable Configure SIP Inactivity Timeout

SIP Media Inactivity Timeout : (seconds)

SIP Signaling Inactivity Timeout : (seconds)

SIP Signaling Port :

+ Add		✎ Edit		✖ Remove	
#	Port				
1	5060				

Step 2. Go to **Configuration > BWM**, enable **BWM**.

CONFIGURATION | **BWM**

BWM Global Setting

Enable BWM

Configuration

St...	#	Destin...	Sched...	User	From	To	Source	Desti...	DSCP Marking In/...	BWM In/OutPri
d...	0	none	any	any	any	any	any	any	preserve/preserve	no/no/7

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

Upload bandwidth budget: 300kbps.

Priority: 7.

(Priority order: 7~1 — Highest ~ Lowest)

Enable Bandwidth Filter.

Service: SIP

Destination: Any

Source: LAN subnet

Class Configuration

Class Name: VoIP_upload

Bandwidth Budget: 300 (Kbps)

Priority: 7 (0-7)

Borrow bandwidth from parent class

Filter Configuration

Enable Bandwidth Filter

Service: SIP

Destination Address Type: Single Address

Destination IP Address: 0 . 0 . 0 . 0

Destination End Address / Subnet Mask: 0 . 0 . 0 . 0

Destination Port: Start 0 End 0

Source Address Type: Subnet Address

Source IP Address: 192 . 168 . 1 . 0

Source End Address / Subnet Mask: 255 . 255 . 255 . 0

Source Port: Start 0 End 0

Protocol ID: 0

Summary | **Class Setup** | **Monitor**

Class Tree View

Interface: WAN1

Bandwidth Management: Active

- Root Class: 1000 kbps
- VoIP_upload: 300 kbps, priority: 7, borrow

Buttons: Add Sub-Class, Edit, Delete, Statistics

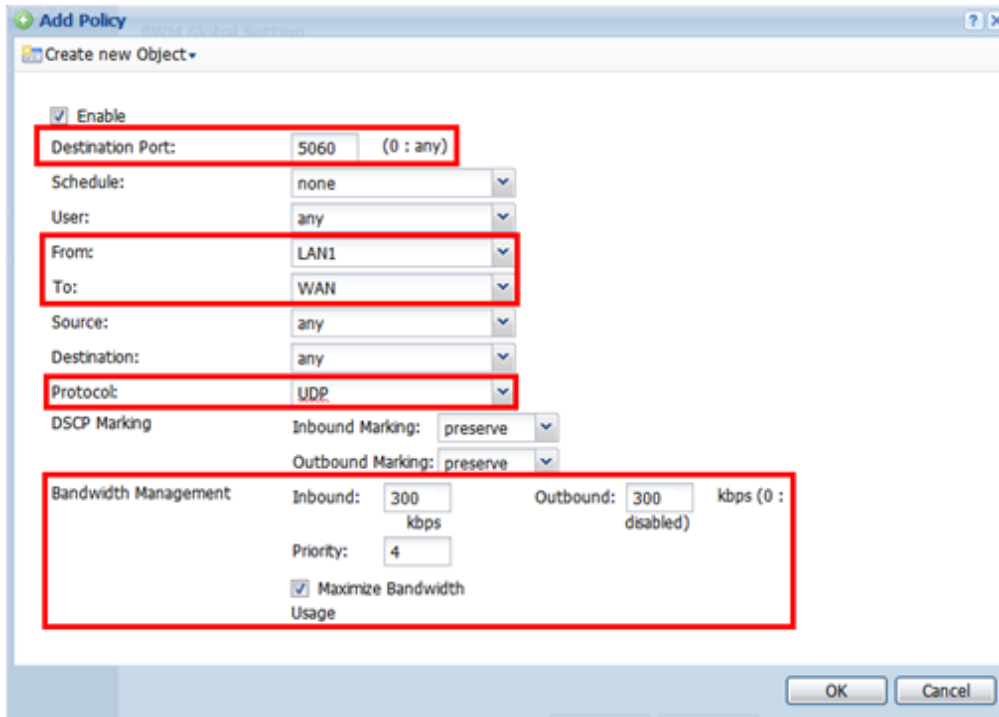
Enabled classes Search Order

Search Order	Class Name	Service	Destination IP Address	Destination Port	Source IP Address	Source Port	Protocol ID
1	VoIP_upload	SIP	0.0.0.0	0	192.168.1.0/24	0	0

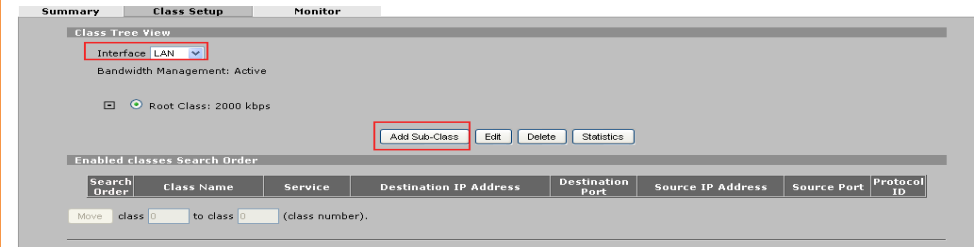
Move class 0 to class 0 (class number).

Step3. Create a bandwidth management rule and configure

- **Destination port** 5060 for SIP application
- Configure the rule as **from LAN1 to WAN**
- Select the **UDP** protocol
- Allocate 300kbps for both inbound/outbound bandwidths.



Add Sub-Class under interface LAN to manage download traffic.



To guarantee voice quality, the bandwidth for VoIP traffic with should be at least 300Kbps in both download and upload directions.

Download bandwidth budget: 300kbps.

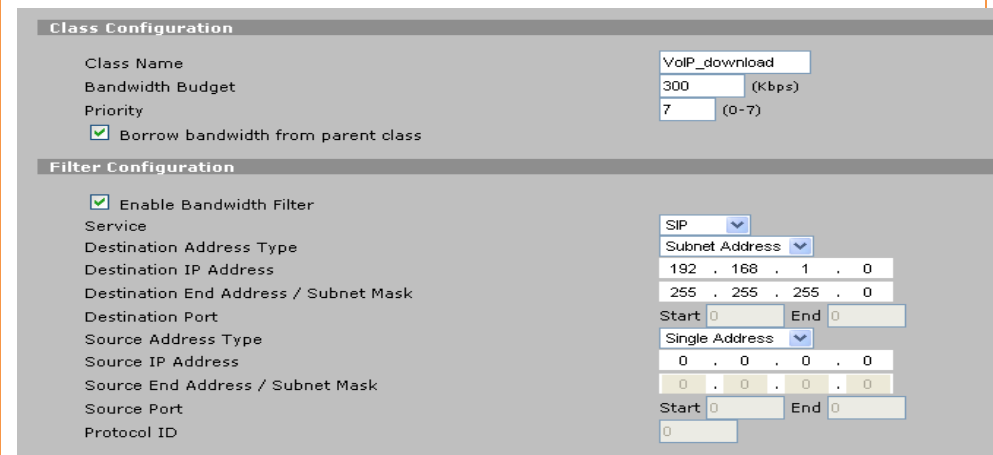
Priority: 7. (Priority order: 7~1 — Highest ~ Lowest)

Enable Bandwidth Filter.

Service: SIP

Destination: LAN subnet

Source: Any



Step4. Create a bandwidth management rule and configure

- Configure the rule as **from WAN to LAN1**
- Configure the rest identically to the above rule

Add Policy Help Close

Create new Object

Enable

Destination Port: 5060 (0 : any)

Schedule: none

User: any

From: WAN

To: LAN1

Source: any

Destination: any

Protocol: UDP

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Management

Inbound: 300 kbps

Outbound: 300 kbps (0 : disabled)

Priority: 4

Maximize Bandwidth Usage

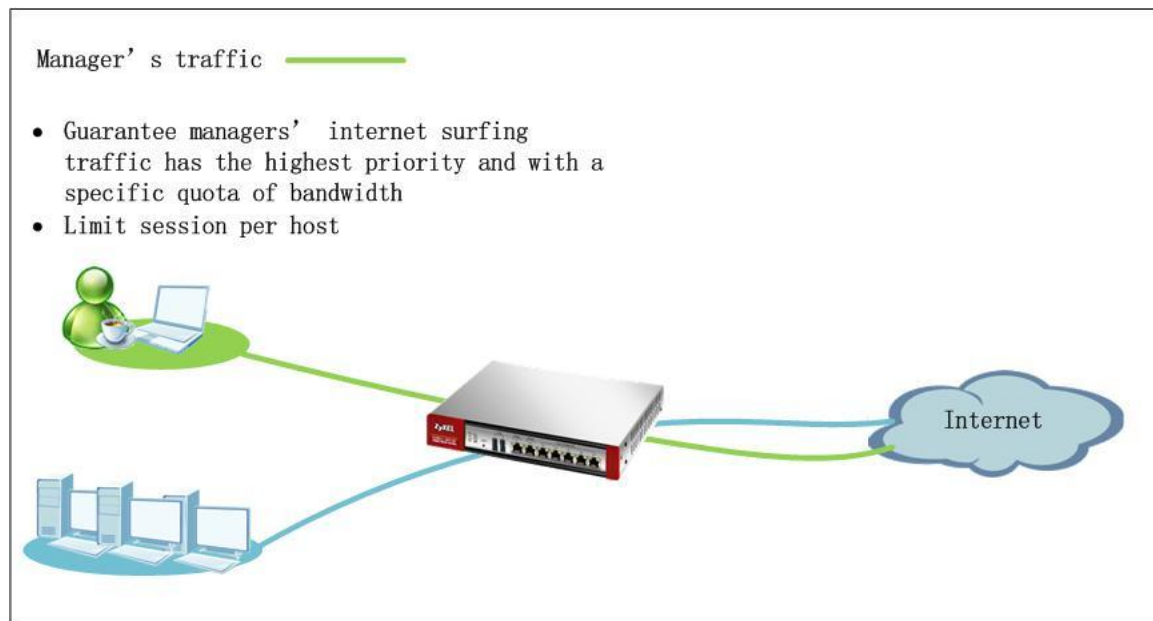
OK Cancel

Scenario 8 — Reserving Highest Bandwidth Management Priority for a Superior User and Control Session per Host

8.1 Application Scenario

Among all the traffic in the company network, sometimes we need to assign higher priority to some superior users to keep their important work going on smoothly. For example, the general manager needs to surf Internet smoothly to conduct his daily important work. Therefore, the network administrator should use the bandwidth management function to prioritize the manager's Internet traffic, and guarantee a minimum bandwidth for his traffic.

During the office hours, to prevent any user consuming too much of the company's bandwidth, the network administrator should limit the number of sessions each user may use.



8.2 Configuration Guide

Network Conditions:

- WAN download bandwidth: 2M
- WAN upload bandwidth: 1M
- Manager’s PC IP: 192.168.1.50

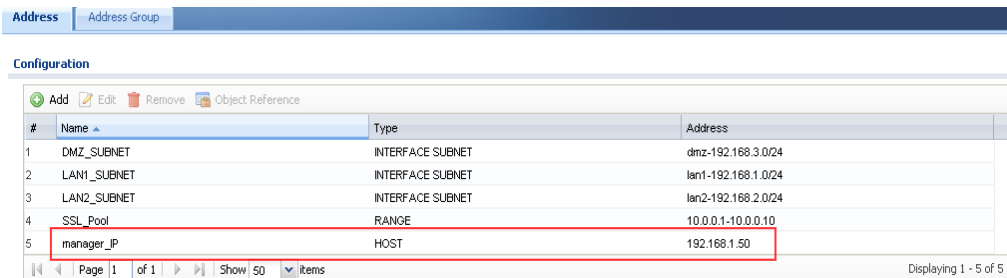
Goal to achieve:

Guarantee manager’s internet surfing traffic going smoothly. Limit each user’s session numbers to prevent any user from using up too many sessions.

ZLD configuration

<< ZyWALL USG50 configuration steps >>

Step 1. Go to **Configuration > Object > Address**, add an address object for the manager. manager_IP: 192.168.1.50

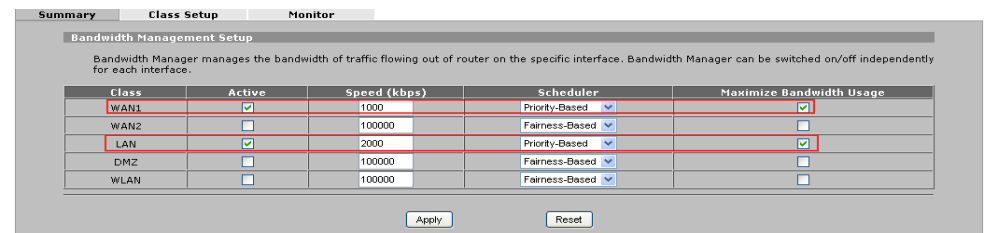


ZyNOS configuration

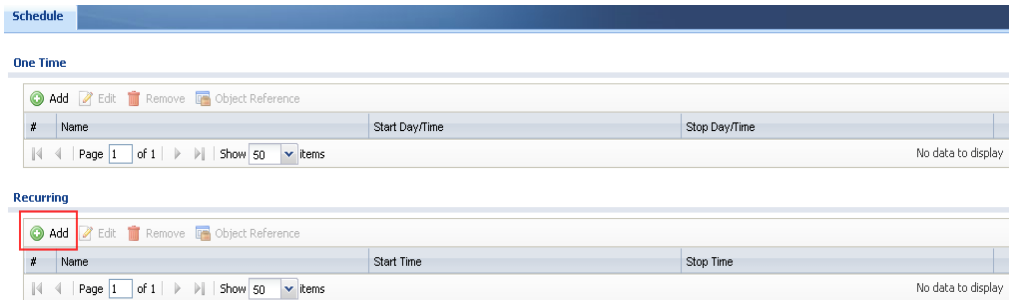
Step 1. Go to **ADVANCED > BW MGMT > Summary**.

Enable **BWM** on WAN1. Set the **speed** to 1000kbps (upload bandwidth). Set the scheduler to **Priority-Based**. Enable **Maximize Bandwidth Usage**.

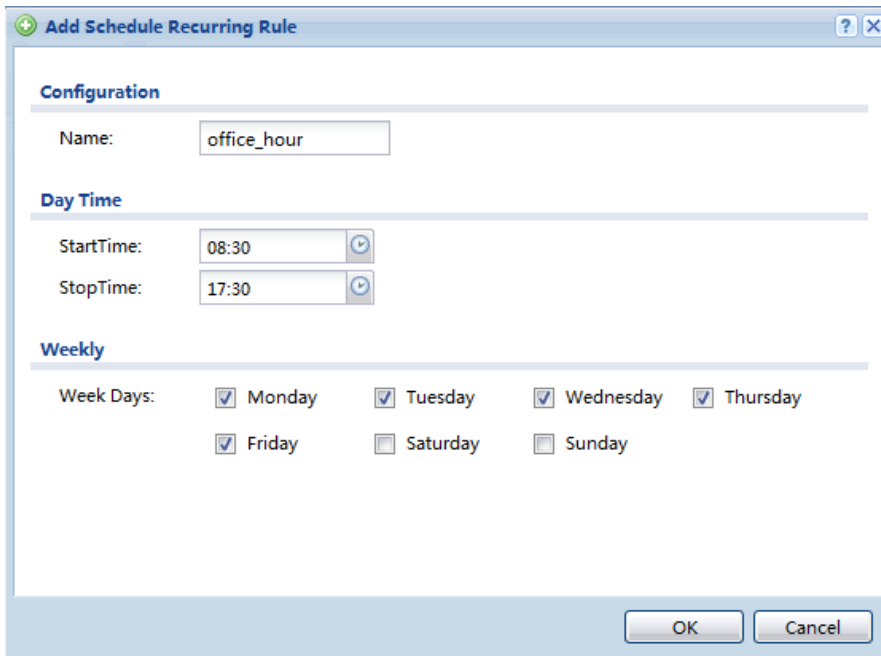
Enable **BWM** on LAN. Set **speed** to 2000kbps (download bandwidth). Set the scheduler to **Priority-Based**. Enable **Maximize Bandwidth Usage**.



Step 2. Go to **Configuration > Object > Schedule**. Add one recurring schedule object.



Input **Start Time** and **Stop Time**, and choose the **weekdays**.



Step 2. Go to **ADVANCED > BW MGMT > Class Setup**. Choose WAN1 to configure upload bandwidth management. Add a Sub-Class.



Bandwidth Budget: Allocate 100kbps for the manager's http upload traffic.

Priority: Assign the highest priority 7.

Enable **Borrow bandwidth from parent class**.

Enable **Bandwidth Filter**

Service: choose **Custom**

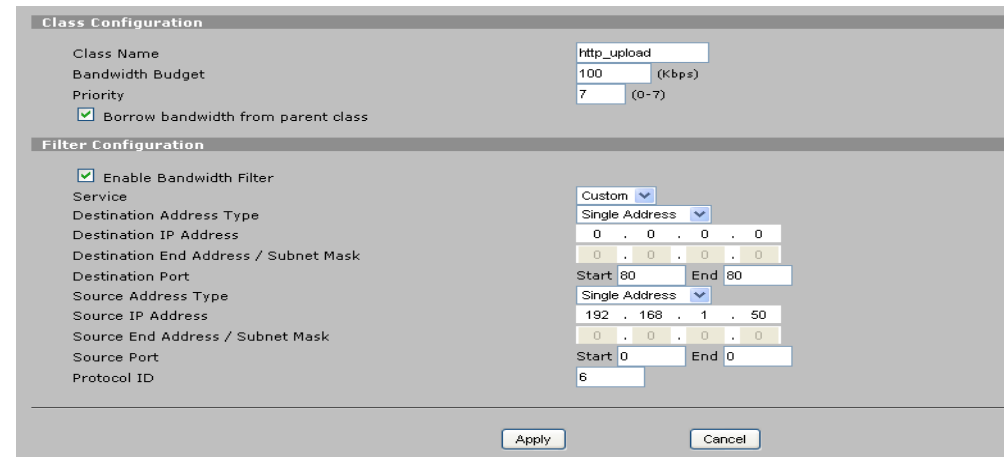
Destination Address: **Any**

Destination Port: **80(HTTP)**

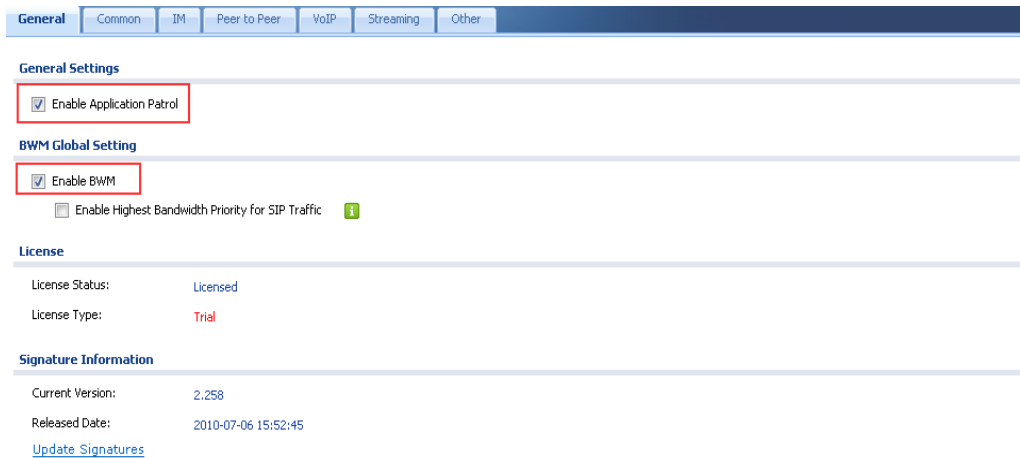
Source Address: **manager's IP 192.168.1.50**

Source Port: **Any**

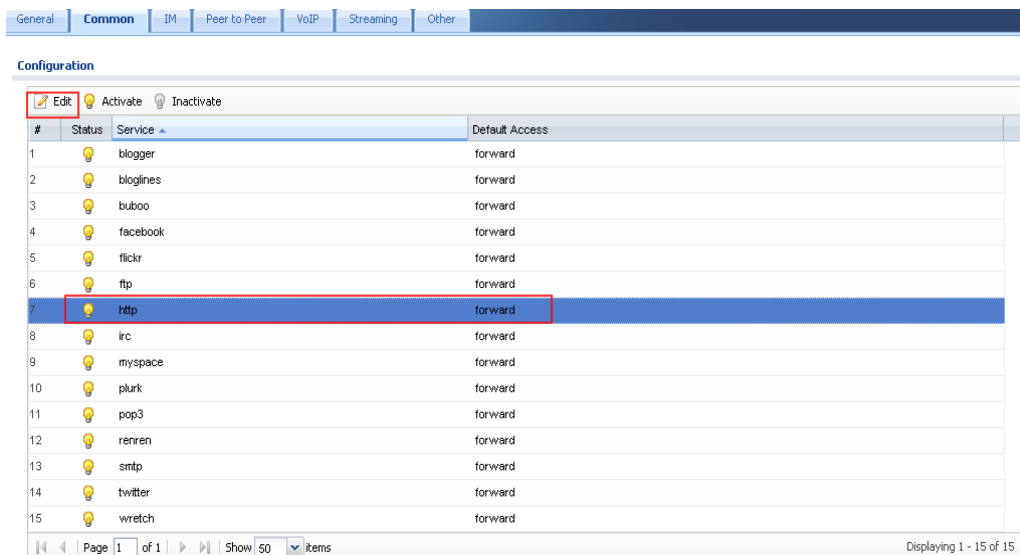
Protocol ID: **6(TCP)**



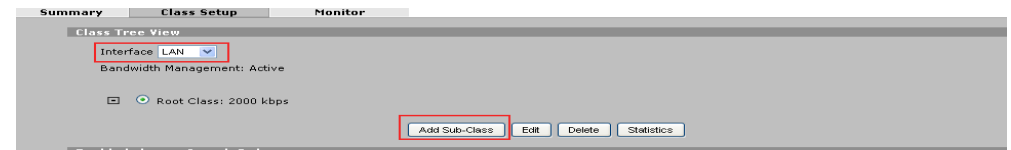
Step3. Go to **Configuration > App Patrol > General**. Enable Application Patrol, and enable BWM.



Step4. **Configuration > App Patrol > Common**. Edit the application “http”.



Step3. Go to **ADVANCED > BW MGMT > Class Setup**. Choose LAN to configure download bandwidth management. Add a Sub-Class.



Bandwidth Budget: Allocate 300kbps for the manager’s http download traffic.

Priority: Assign the highest priority 7.

Enable **Borrow bandwidth from parent class**.

Enable **Bandwidth Filter**

Service: choose **Custom**

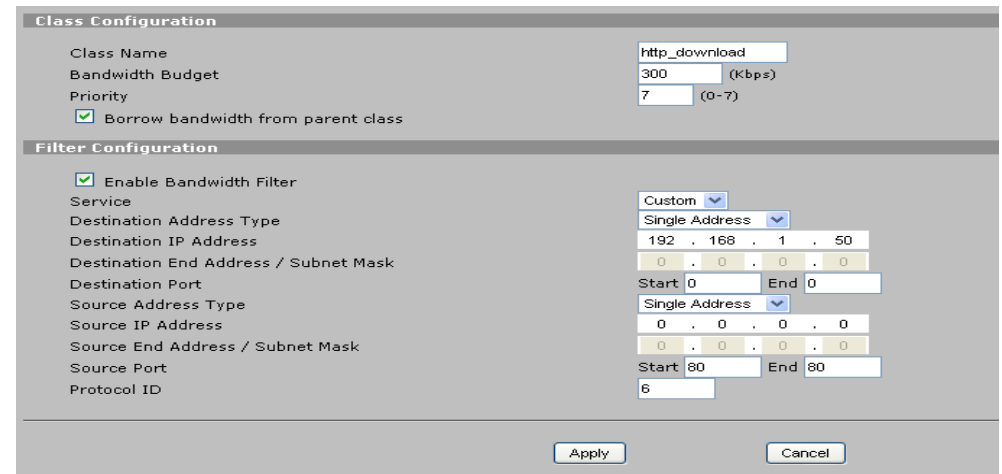
Destination Address: **manager’s IP 192.168.1.50**

Destination Port: **Any**

Source Address: **Any**

Source Port: **80(HTTP)**

Protocol ID: **6(TCP)**



Add a policy to manage the manager’s http traffic bandwidth.

Direction: from LAN to Any.

Source: manager_IP

Destination: any

Bandwidth Management: To guarantee the manager can surf internet smoothly, we can assign a bandwidth of 300kbps for inbound traffic (download), and assign a bandwidth of 100kbps for outbound traffic (upload).

For the definition of Inbound and Outbound, please refer to the [App Patrol BWM Direction NOTE](#) below.

Set priority as the highest —1.

Enable **Maximize Bandwidth Usage**.

Create new Object

Enable Policy

Port: 0 (0 : any)

Schedule: none

User: any

From: LAN1

To: any

Source: manager_IP

Destination: any

Access: forward

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Management

Inbound: 300 kbps

Outbound: 100 kbps (0 : disabled)

Priority: 1

Maximize Bandwidth Usage

Log: no

OK Cancel

Limit each user’s number of sessions

To prevent any user from consuming too many sessions, we can limit each user’s sessions to a specific number. Go to ADVANCED > NAT > NAT Overview. Set Max. Concurrent Sessions Per Host to 1000. Administrator can adjust this value according to his real network environment.

NAT Overview Address Mapping Port Forwarding Port Triggering

Global Settings

Max. Concurrent Sessions 6000

Max. Concurrent Sessions Per Host 1000 (Historical high since last startup: 8)

WAN Operation Mode Active/Passive Fail Over

WAN 1

Enable NAT

Address Mapping Rules

SUA

Full Feature 2/30

Port Forwarding Rules 0/30 Copy to WAN 2

Port Triggering Rules 0/12 Copy to WAN 2

WAN 2

Enable NAT

Address Mapping Rules

SUA

Full Feature 2/30

Port Forwarding Rules 0/30 Copy to WAN 1

Port Triggering Rules 0/12 Copy to WAN 1

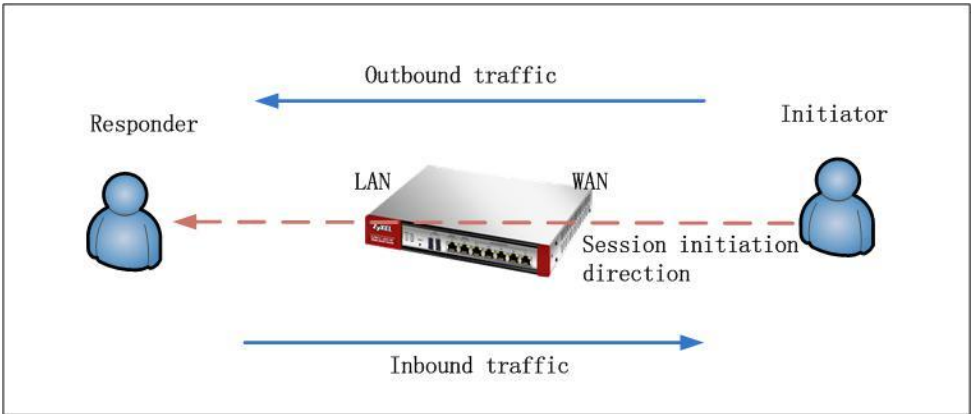
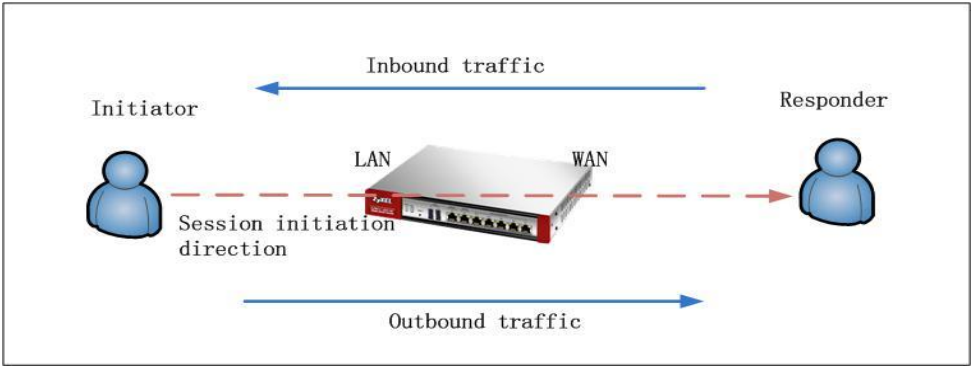
App Patrol BWM Direction NOTE

To use App Patrol to manage bandwidth correctly, users must understand the direction Inbound and Outbound.

The direction Inbound and Outbound are determined with the traffic session initiation direction as reference.

Inbound: From session responder to session initiator

Outbound: From session initiator to session responder.



Limit each user's session number

To prevent any user from using up too many sessions, we can limit each user's sessions to a specific number. Go to **Configuration > Firewall > Session Limit**.

Enable **Session Limit**, and set **Default Session per Host** to 1000. Administrator can adjust this value according to his real network environment.

The screenshot shows the 'Session Limit' configuration page. Under 'General Settings', the 'Enable Session Limit' checkbox is checked, and the 'Default Session per Host' is set to 1000. Below this is a 'Rule Summary' table with columns for Status, #, User, Address, Description, and Limit. The table is currently empty, showing 'Page 1 of 1' and 'No data to display'.

Status	#	User	Address	Description	Limit
--------	---	------	---------	-------------	-------

<< ZyWALL USG20/20W configuration steps >>

Step 1. Go to **Configuration > Object > Address**, Add an address object for the manager.

manager_IP: 192.168.1.50

Address | Address Group

Configuration

Add Edit Remove Object Reference

#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
3	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
4	SSL_Pool	RANGE	10.0.0.1-10.0.0.10
5	manager_IP	HOST	192.168.1.50

Page 1 of 1 | Show 50 items | Displaying 1 - 5 of 5

Step 2. Go to **Configuration > Object > Schedule**. Add one recurring schedule object.

Schedule

One Time

Add Edit Remove Object Reference

#	Name	Start Day/Time	Stop Day/Time
No data to display			

Page 1 of 1 | Show 50 items

Recurring

Add Edit Remove Object Reference

#	Name	Start Time	Stop Time
No data to display			

Page 1 of 1 | Show 50 items

Input **Start Time** and **Stop Time**, and choose the **weekdays**.

Add Schedule Recurring Rule

Configuration

Name:

Day Time

StartTime:

StopTime:

Weekly

Week Days: Monday Tuesday Wednesday Thursday
 Friday Saturday Sunday

OK Cancel

Step3. Go to **Configuration > BWM**.

Add a policy to manage the manager's http traffic bandwidth.

BWM

BWM Global Setting

Enable BWM

Configuration

Stat...	#	Destinati...	Schedule	User	From	To	Source	Destinati...	DSCP Marking In/Out	BWM In/C
def...	0		none	any	any	any	any	any	preserve/preserve	no/no/7

Page 1 of 1 | Show 50 items

Destination Port: 80

Schedule: the recurring schedule object configured in step2.

Direction: from LAN1 to WAN.

Source: manager_IP

Destination: any

Protocol: TCP

Bandwidth Management: To guarantee the manager can surf internet smoothly, we can assign a bandwidth of 300kbps for inbound traffic (download), and assign a bandwidth of 100kbps for outbound traffic (upload). Set priority as the highest 1.

Enable **Maximize Bandwidth Usage**.

Add Policy

Create new Object

Enable

Destination Port: 80 (0 : any)

Schedule: office_hour

User: any

From: LAN1

To: WAN

Source: manager_IP

Destination: any

Protocol: TCP

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Management

Inbound: 300 kbps

Outbound: 100 kbps (0 : disabled)

Priority: 1

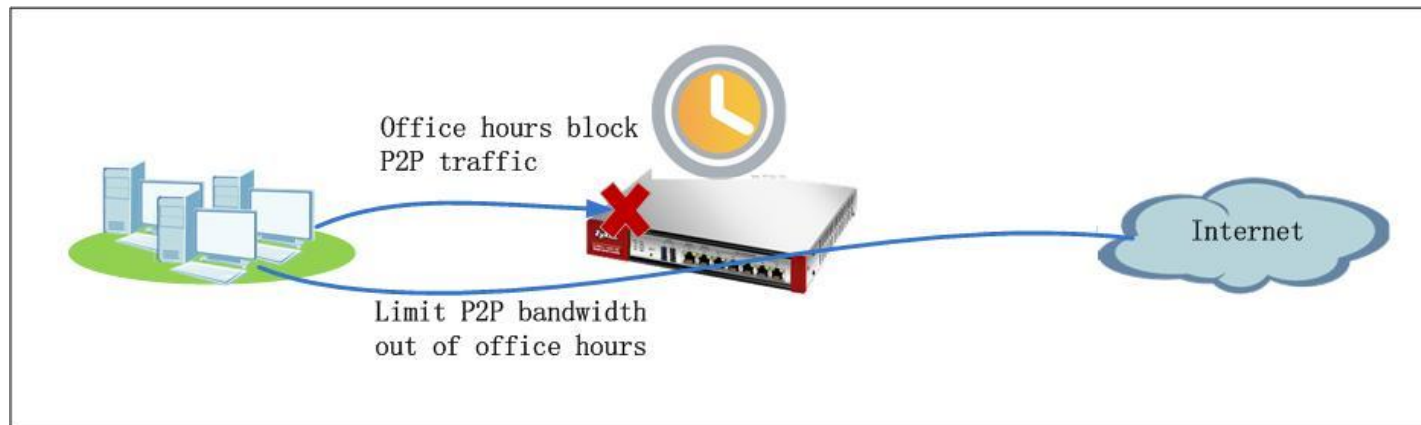
Maximize Bandwidth Usage

OK Cancel

Scenario 9 — Using ZyWALL to Control Popular P2P Applications (USG 50 only)

9.1 Application Scenario

Peer to Peer applications, with their massive numbers of concurrent sessions and fast traffic transmission speed, can consume much of a company's limited bandwidth. This will slow down other normal productive traffic speed and affect productivity, lowering company productivity profit. USG ZyWALL's Application Patrol function can examine passing traffic in real time, detect traffic service type, and take corresponding actions according to the configuration in App Patrol. For example, to improve network productivity efficiency, network administrator can set App Patrol to block P2P traffic in office hours, and limit its speed with bandwidth management out of office hours.



9.2 Configuration Guide

Network Conditions:

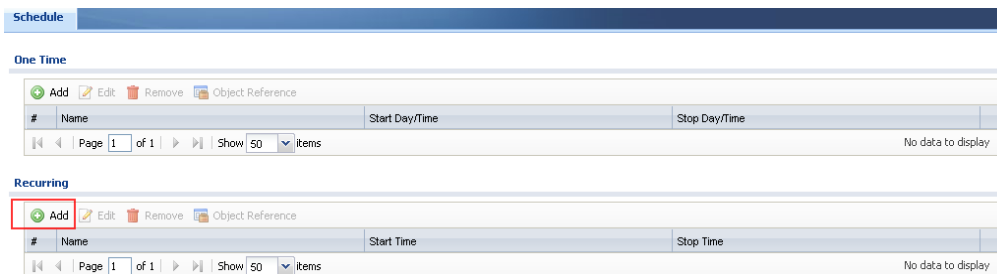
- LAN subnet: 192.168.1.0/24

Goals to achieve:

- 1) Block P2P traffic during office hours (8:30~17:30)
- 2) Allow P2P traffic out of office hours but limit its bandwidth to 100kbps.

ZLD configuration

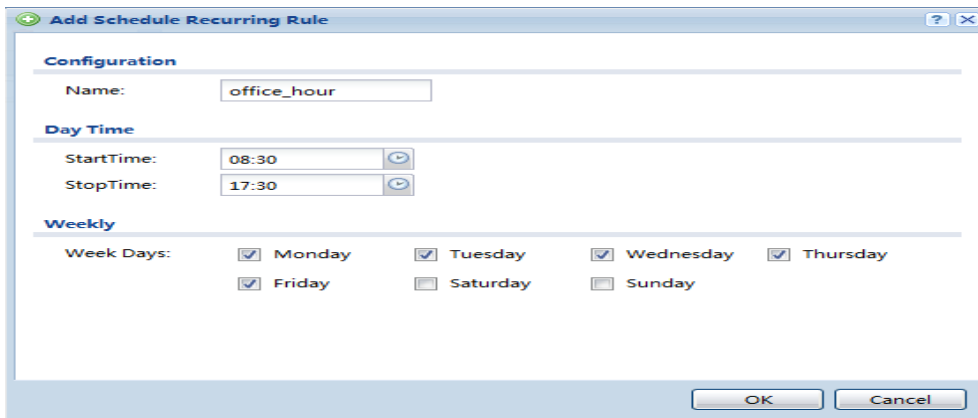
Step 1. Go to **Configuration > Object > Schedule**, add a Recurring schedule object for the office hours.



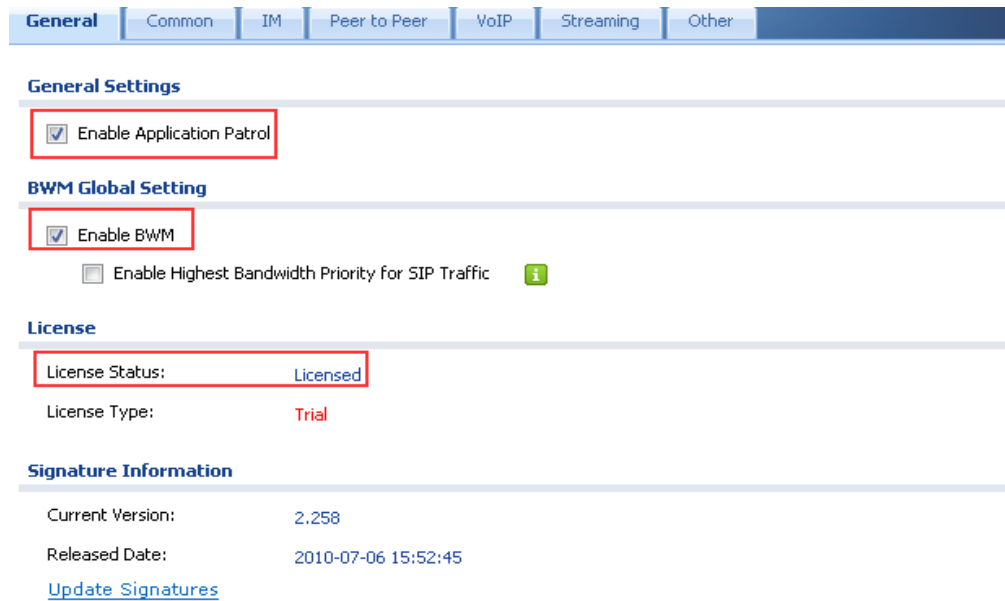
ZyNOS configuration

Step 1. IDP Common Setting.

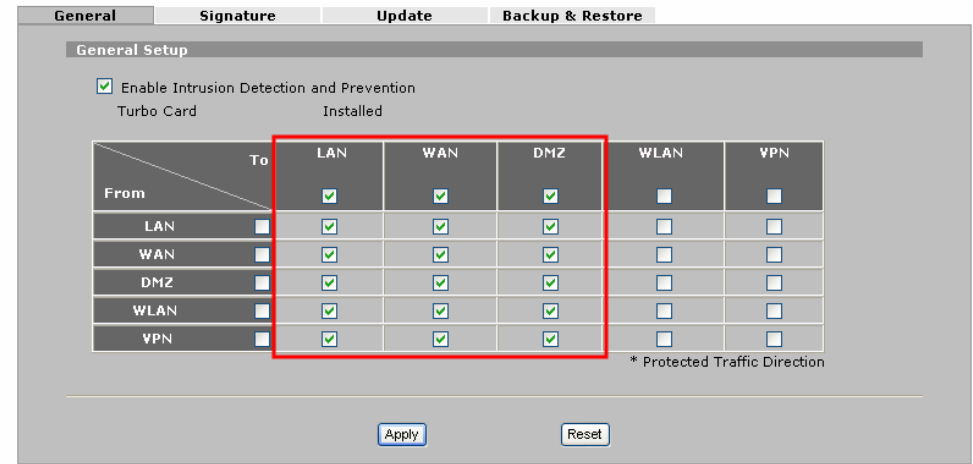
- a. In **IDP->General**, check the **Enable Intrusion Detection and Prevention** check box to enable IDP function.
- b. In **Active** option, check all the traffic to LAN, DMZ and WAN check boxes to have the IM/P2P traffic between LAN zone users and the remote users under control.
- c. Click the **Apply** button to save the above settings.



Step 2. Go to **Configuration > App Patrol > General**. First of all, please make sure you have activated your IDP/App Patrol license. Enable **Application Patrol**, and enable **BWM**.

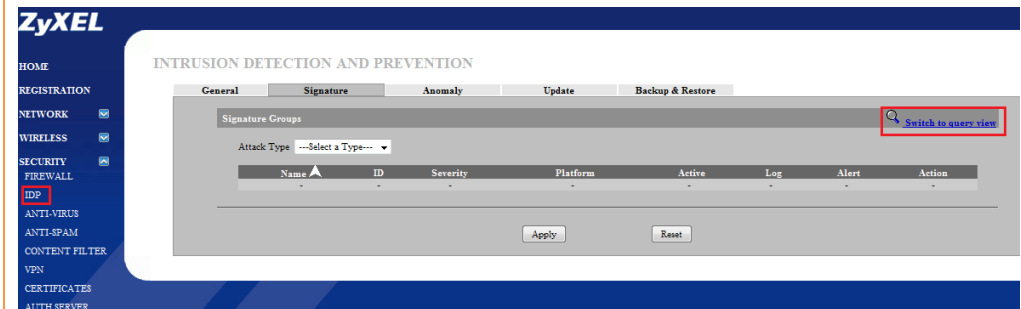


INTRUSION DETECTION AND PREVENTION



Step 2. Control Thunder application.

- a. In IDP->**Signature**, click on **Switch to query view** to search for the specified signatures and set them up optionally.



Step3. Switch to **Configuration > App Patrol > Peer to Peer**. Edit the P2P services you need to control. In this example, we will edit the thunder application.

Configuration

#	Status	Service	Default Access
1	🔆	ares	forward
2	🔆	bittorrent	forward
3	🔆	clubbox	forward
4	🔆	edonkey	forward
5	🔆	ezpeer	forward
6	🔆	fasttrack	forward
7	🔆	gnutella	forward
8	🔆	imesh	forward
9	🔆	poco	forward
10	🔆	soulseek	forward
11	🔆	teamviewer	forward
12	🔆	thunder	forward
13	🔆	ultrasurf	forward

Page 1 of 1 | Show 50 items | Displaying 1 - 13 of 13

b. Use the “Thunder” keyword to search for and list any signatures related to “thunder”.

INTRUSION DETECTION AND PREVENTION

General | Signature | Anomaly | Update | Backup & Restore

Query Signatures

Signature Search By Name

Signature Search by Attributes.

Hold 'Ctrl' to make multiple selection on items in the lists:

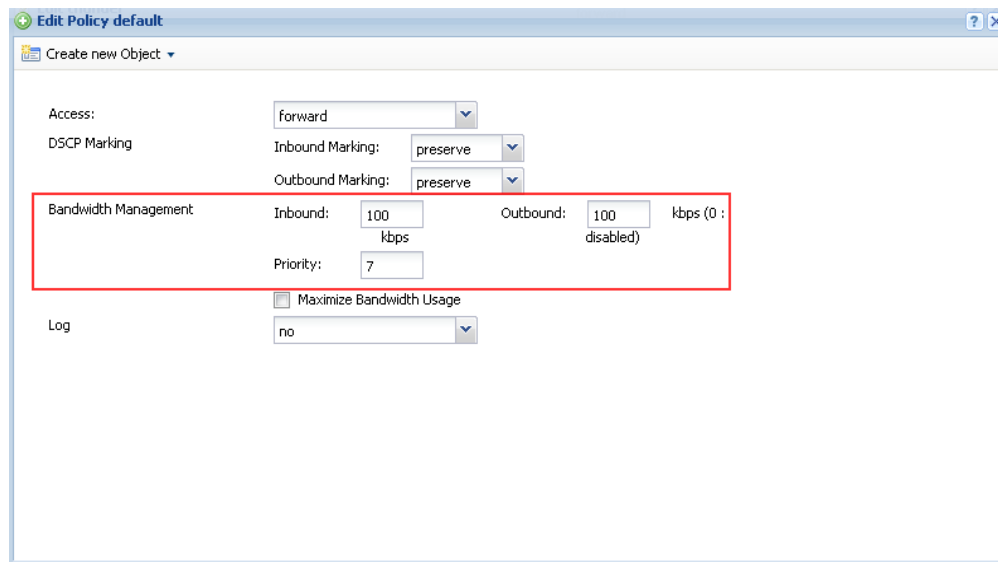
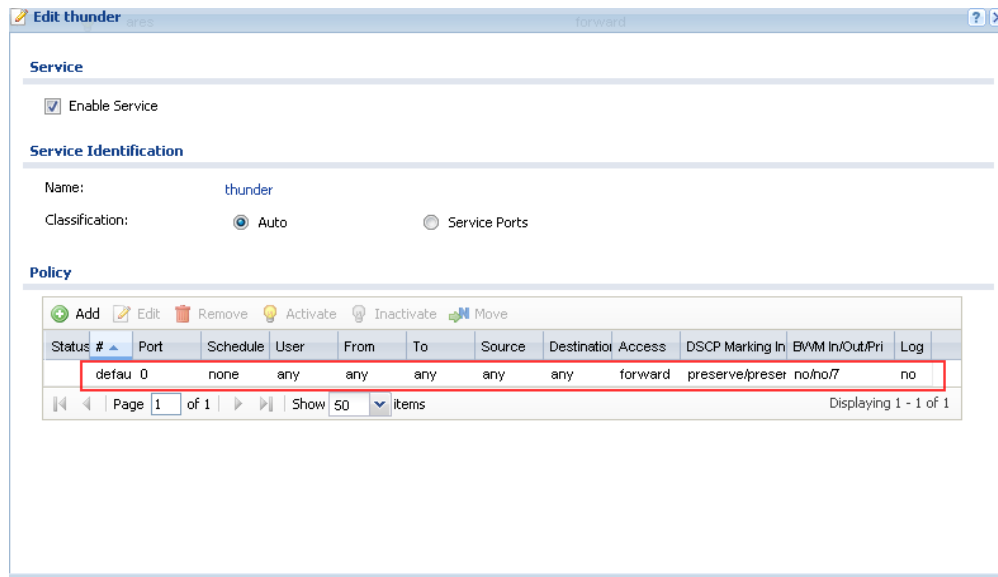
Severity	Type	Platform	Active	Log	Alert
Any	Any	Any	Any	Any	Any
Severe	AccessControl	Windows	Active	Log	Alert
High	Backdoor/Trojan	Linux/Unix	Inactive	No Log	No Alert
Medium	BufferOverflow	Network device			
Low	DDOS				

Search

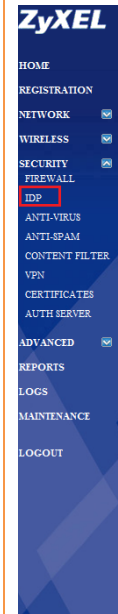
Configure Signatures

Name	ID	Severity	Type	Platform	Active
Xunlei Thunder PPLAYER DLL ActiveX exploit	8009057	Medium	BufferOverflow		<input checked="" type="checkbox"/>
P2P Thunder user agent	8800155	Very Low	P2P		<input type="checkbox"/>
P2P Thunder user agent mode2	8800232	Very Low	P2P		<input type="checkbox"/>
P2P Thunder resource query	8800149	Very Low	P2P		<input type="checkbox"/>
P2P Thunder http request	8800142	Very Low	P2P		<input type="checkbox"/>
P2P Thunder dns query	8800235	Very Low	P2P		<input type="checkbox"/>
P2P Thunder Try to connect to client size:93	8800386	Very Low	P2P		<input type="checkbox"/>
P2P Thunder Try to connect to client size:109	8800387	Very Low	P2P		<input type="checkbox"/>
P2P Thunder TCP info data	8800393	Very Low	P2P		<input type="checkbox"/>

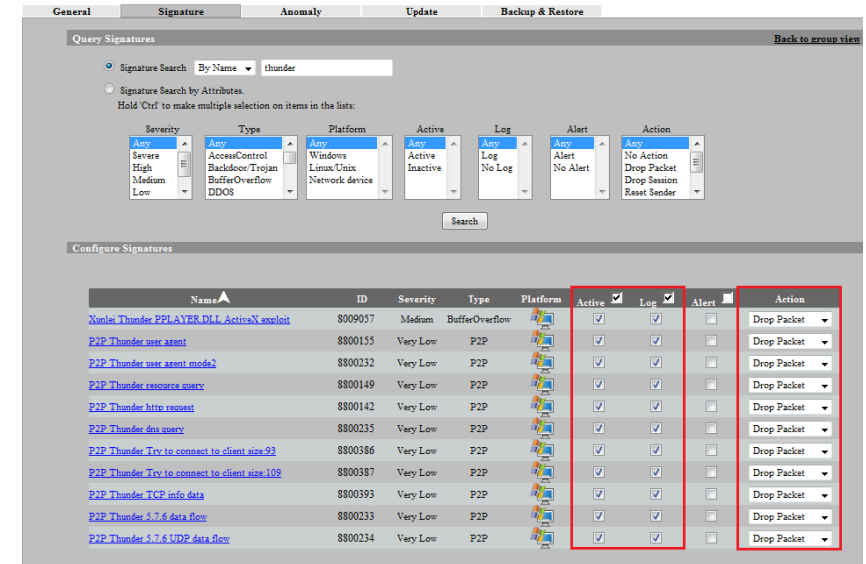
Edit the default policy. Limit its bandwidth to 100kbps for both inbound and outbound traffic. Assign the lowest priority —7 for it.



- c. IT staff can log all Thunder traffic by checking the Log check box and blocking the Thunder packets by selecting **Drop Packet** in the Action field. Also remember to check the **Active** check box to activate the signatures.



INTRUSION DETECTION AND PREVENTION



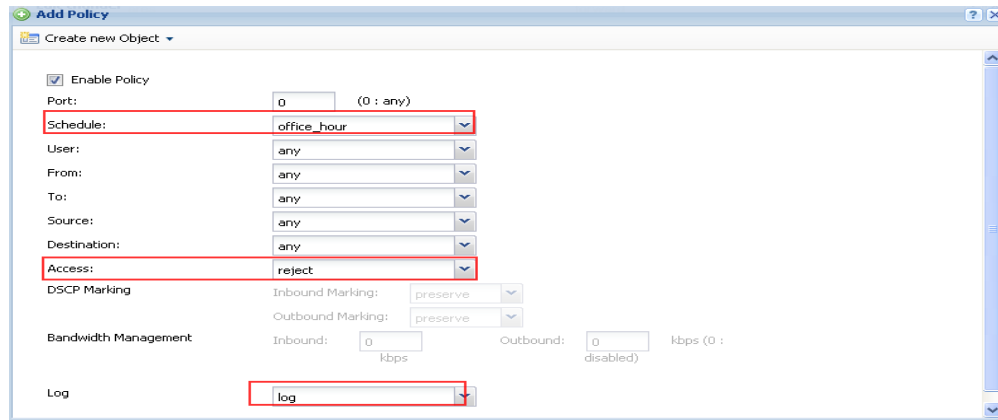
Add a policy to block thunder traffic during office hours.

Schedule: Choose the object **office_hour**

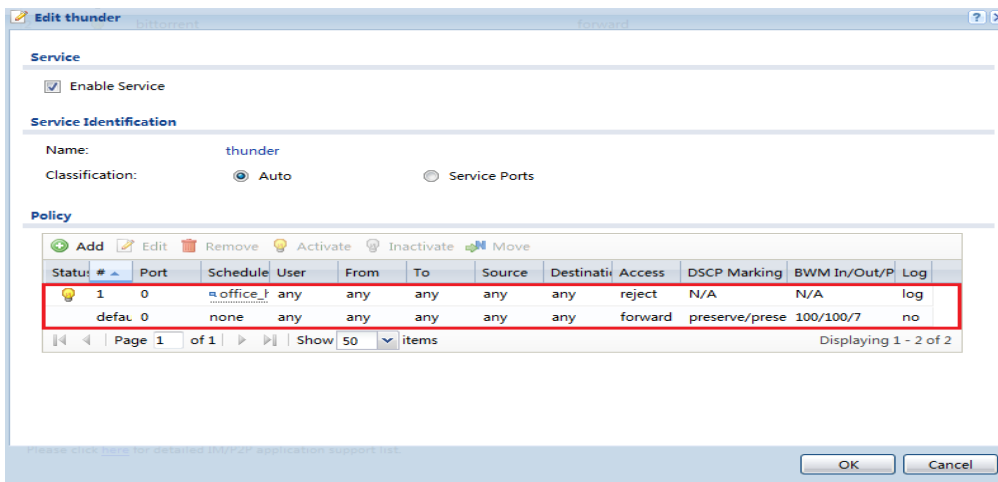
Session direction: from Any to Any

Access: Reject

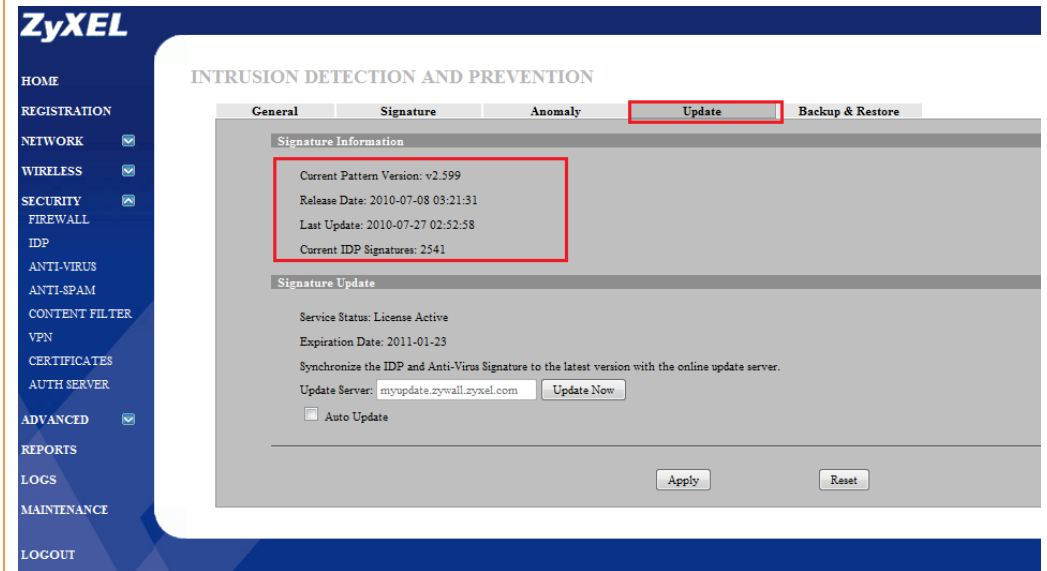
We can enable Log to check which user tries to violate the rule.



Check the created policies. Make sure their order lists as below:



Step 3. IDP signature update. To keep the ZyWALL IDP engine performing at its best, make sure the IDP signatures are kept updated (The **update** procedure can be done manually or automatically.)

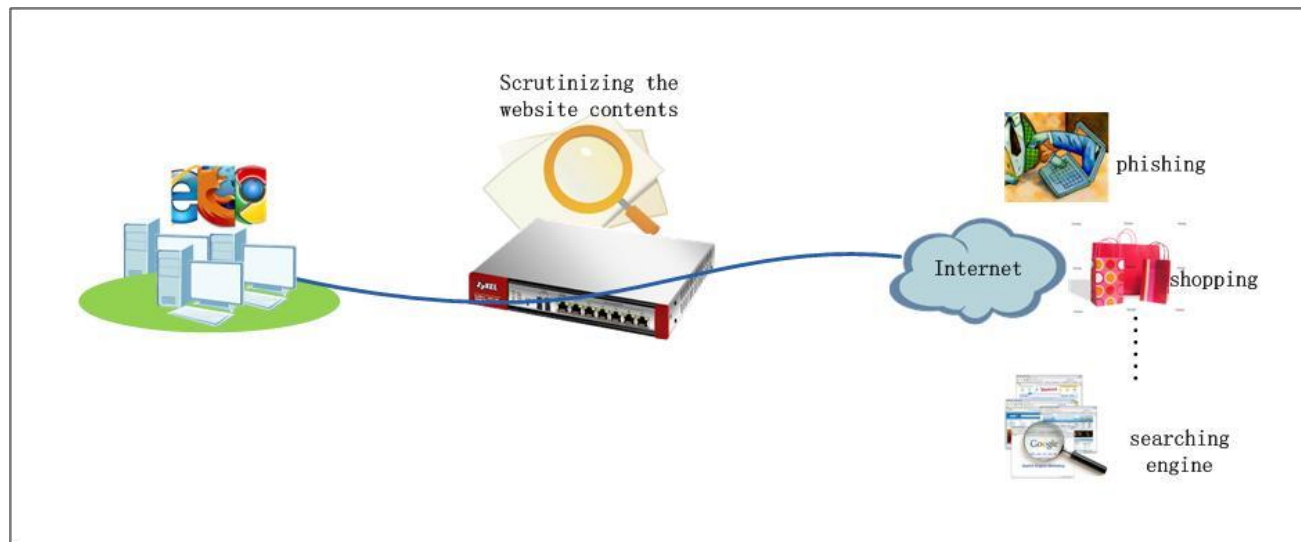


NOTE: You need to register an IDP license to use the IDP function.

Scenario 10 — Deploying Content Filtering to Manage Employee Browsing Behavior

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

ZyXEL Content Filtering service, including its Safe Browsing service, is tailored to help network administrator to handle these requirements.



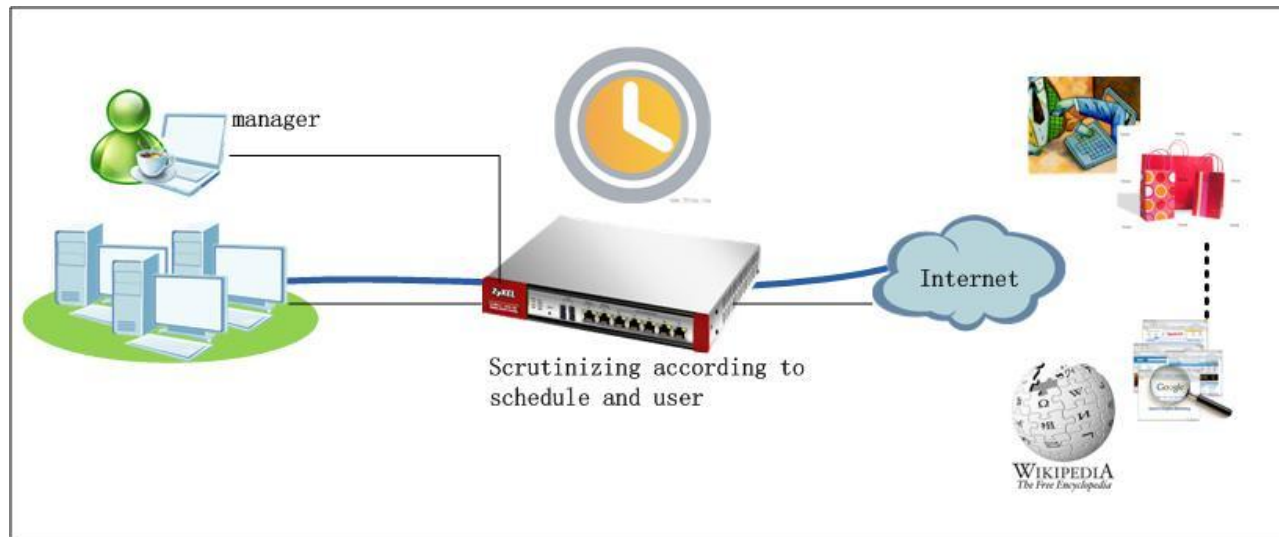
10.1 Introduction to ZSB (ZyXEL Safe Browsing)

ZSB stands for ZyXEL Safe Browsing.

As suggested by its name, this function enhances web browsing safety. With the Internet becoming more and more popular, an increasing number of threats are injected into web pages. Some web pages may be phishing web sites where the visitors may be enticed to release their confidential information, other web pages may contain malware intended to infect the visitor's PC with viruses or even to corrupt the visitor's PC. Additionally, some web pages may contain spyware sources. ZSB has been added to ZyWALL to help protect users from such unsafe web sites.

10.2 Application Scenario

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



10.3 Configuration Guide

Network Conditions:

- LAN subnet: 192.168.1.0/24
- Manager IP: 192.168.1.50

Goals to achieve:

- 1) The manager can access all websites at any time.
- 2) During office hours, other employees should be restricted from accessing websites that are irrelevant to their work.
- 3) All employees may access any websites outside of office hours.

ZLD configuration

Step 1. Go to **Configuration > Object > User/Group**. Add an address object for the manager's IP.

#	Name	Type	Address
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
2	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
3	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
4	SSL_Pool	RANGE	10.0.0.1-10.0.0.10
5	manager_IP	HOST	192.168.1.50

ZyNOS configuration

Step 1. Go to **SECURITY > CONTENT FILTER > General**.

First of all, please make sure Content Filter service is licensed.

Enable Content Filter.

Enable **External Database Content Filtering** and set the action for matched web pages to **“Block and Log”**.

Enter **the message to display when a website is blocked**. E.g. “This website is restricted. Please contact administrator.”

Step 2. Go to **Configuration > Object > Schedule**. Add a Recurring schedule for office hours.

Schedule

One Time

Recurring

#	Name	Start Time	Stop Time
1	office_hour	09:30	17:30

Step 3. Go to **Configuration > Anti-X > Content Filter > Filter Profile**. Add a profile.

Filter Profile

Profile Management

Add Edit Remove

#	Filter Profile Name

Policy

General Setup

Enable Content Filter

External Database Service General Setup

Enable External Database Content Filtering

Block Log Matched Web Pages

Block Log Unrated Web Pages

Block Log When Content Filter Server Is Unavailable

Content Filter Server Unavailable Timeout: 10 (1-30 seconds)

External Database Service License Status

License Status: Trial Active

Expiration Date: 2011-01-15

Message to display when a site is blocked

Denied Access Message: This website is restricted. Please contact administrator

Redirect URL

Apply Reset

Step 2. Go to **SECURITY > CONTENT FILTER > Policy**. Insert an access policy.

Policy

Resource Usage

Content Filter Storage Space in Use

0% 1% 100%

Policy Summary

#	Name	Active	Group Address	Modify
	new rule before rule 1			

Insert new rule before rule 1 (policy number)

Move policy 1 to policy 1 (policy number)

Add a profile which allows users to serf all websites.

Enable Content Filter Category Service.

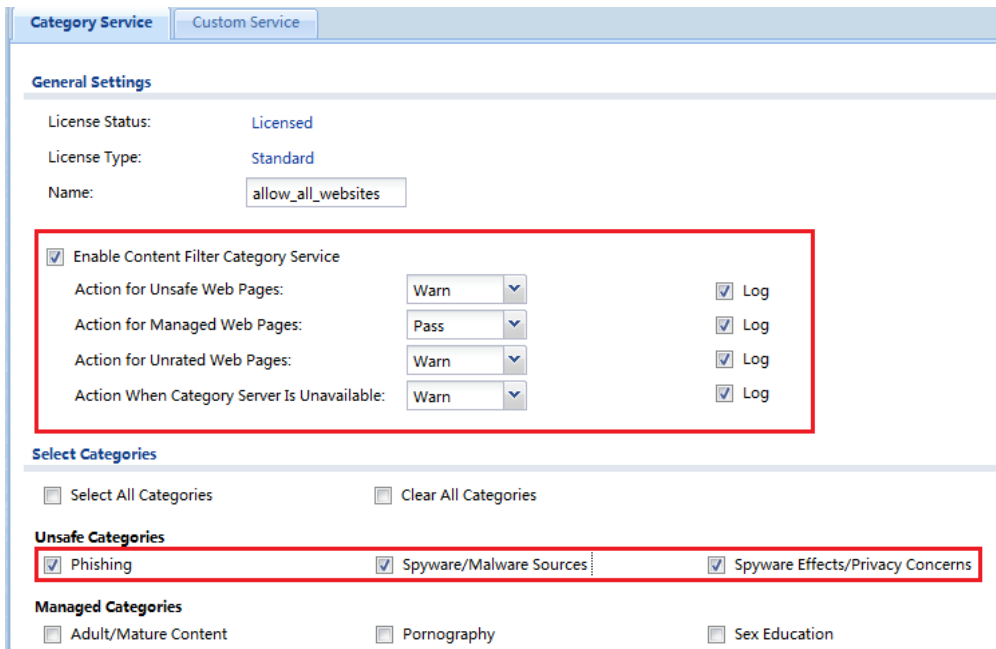
Set action for Unsafe Web Pages to “Warn and Log”.

Set action for Managed Web Pages to “Pass”.

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

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

Check all the unsafe categories, and leave all the managed categories as unchecked.

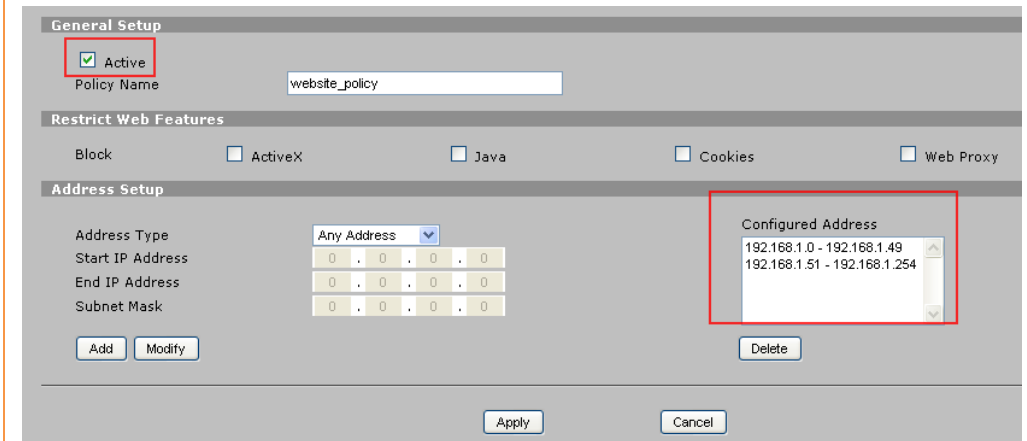


Add a policy to meet the requirement that during office hours, employees should be prevented from accessing some websites, and that the manager (192.168.1.50) is not restricted.

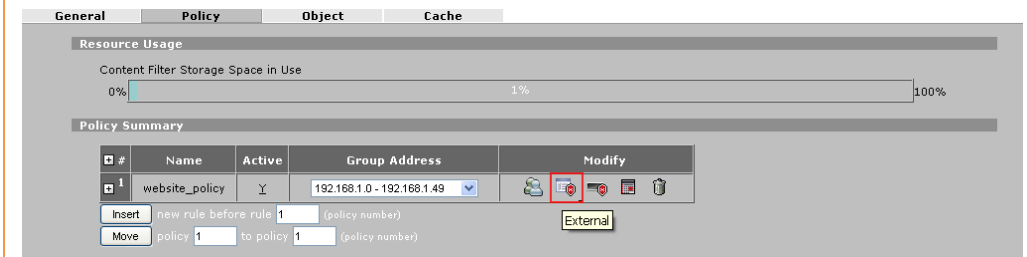
Address Setup: Add two address ranges to Configured Address.

192.168.1.0~192.168.1.49

192.168.1.51~192.168.1.254



Click the External icon to edit the external categories.



Add a profile for employees to surf only allowed websites.

Enable Content Filter Category Service.

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

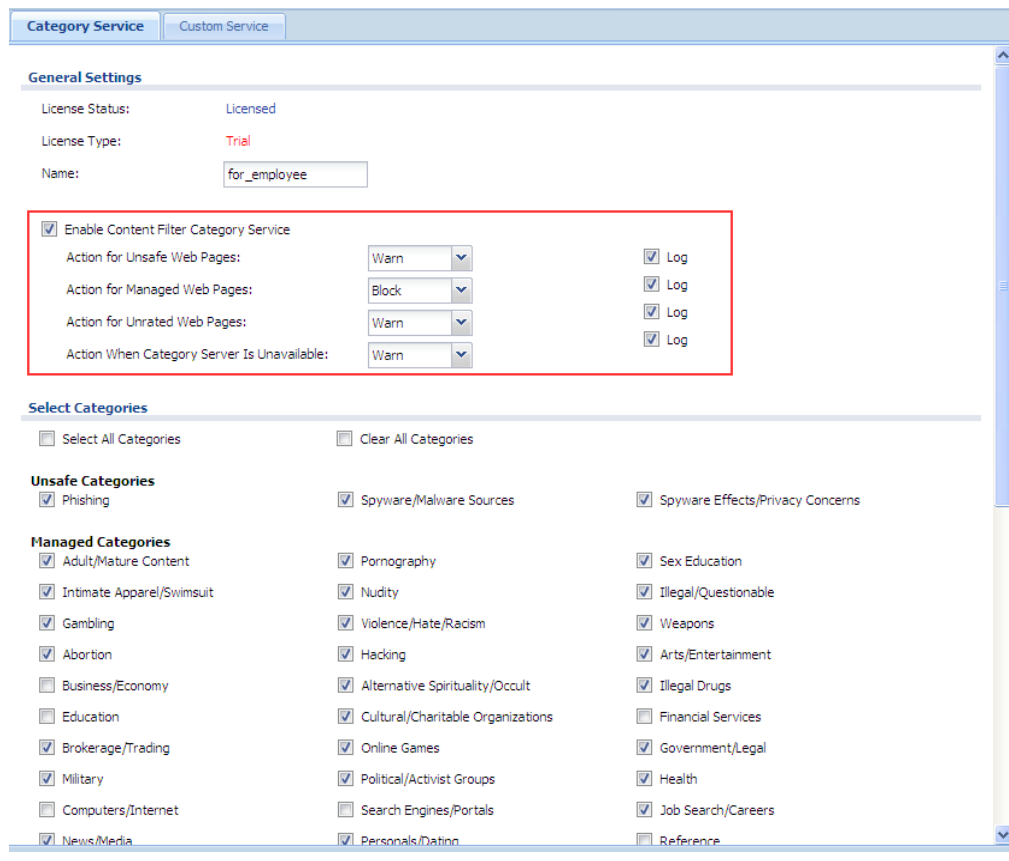
Set action for Managed Web Pages to “Block and Log”.

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

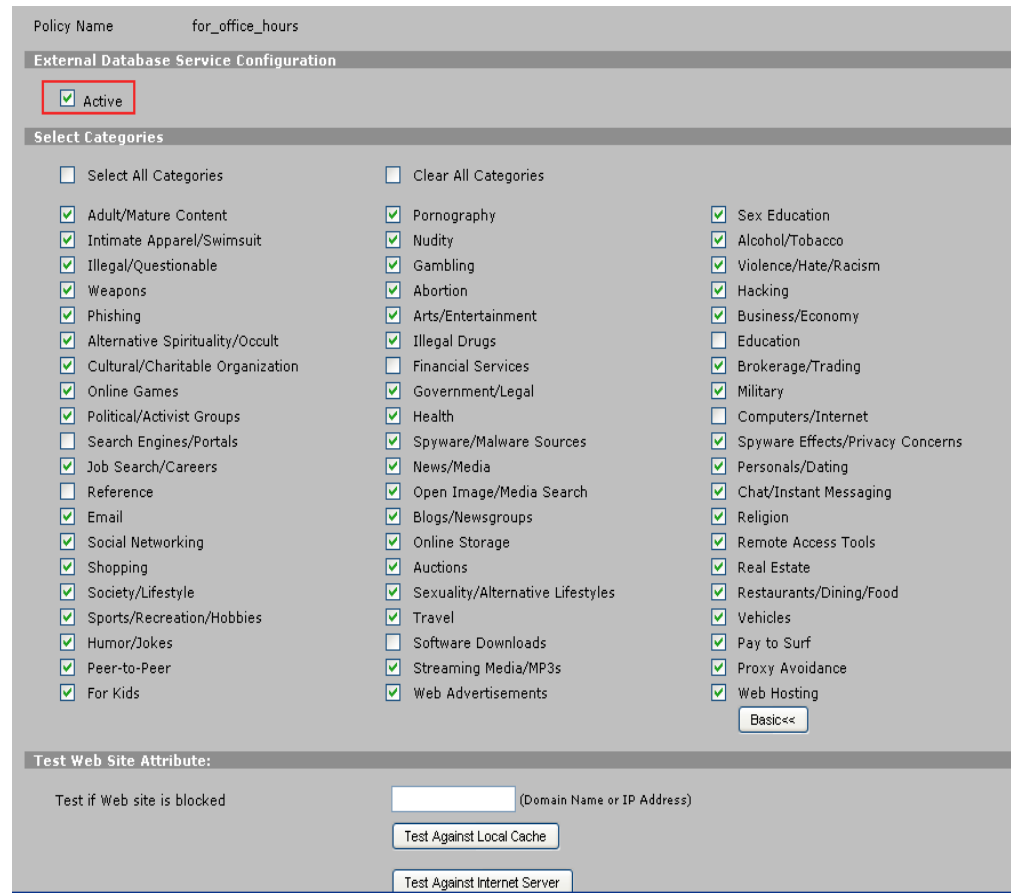
Set action When Category Server is Unavailable to “Warn and Log”.

Check all the unsafe categories.

Check the managed categories that you don’t want employees to surf during office hours.



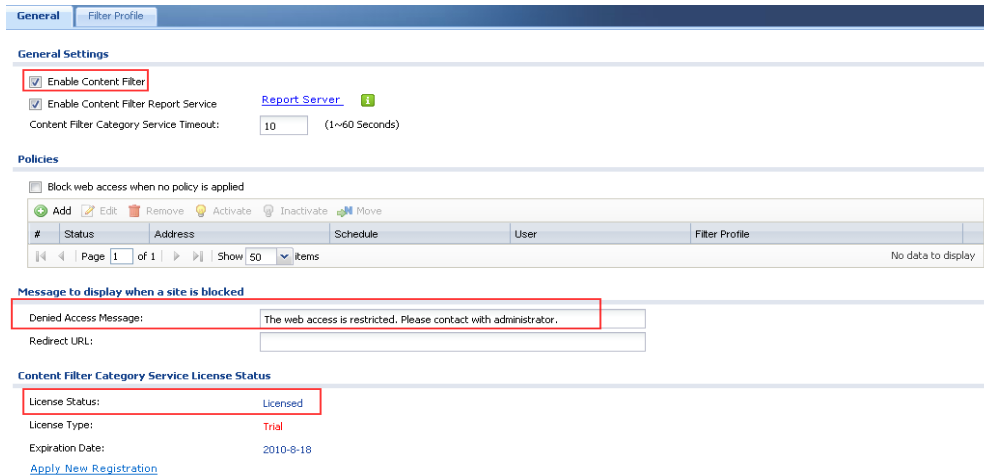
Activate the **External Database Service**. Select managed websites that you want to prevent the employees from accessing during office hours.



Step 4. Switch to **Configuration > Anti-X > Content Filter > General**. Enable **Content Filter**.

You can edit the **Denied Access Message**.

Make sure the Content Filter service is licensed.



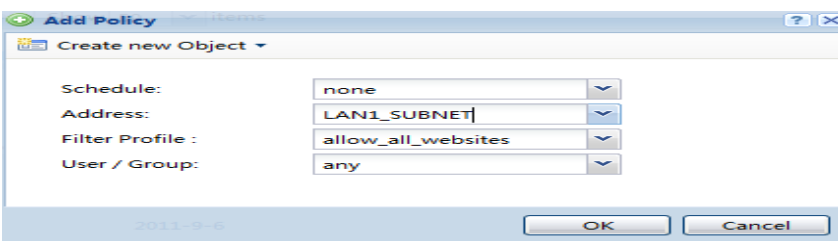
Add an access policy for all the crew outside of office hours.

Schedule: none.

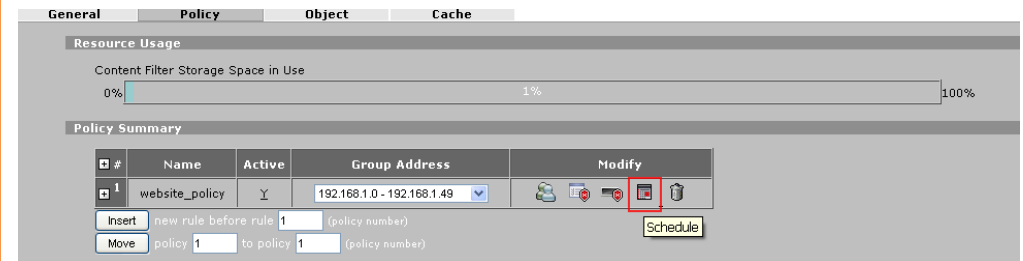
Address: select the address object LAN subnet.

Filter Profile: select the profile “**allow_all_websites**” created in the Profile page.

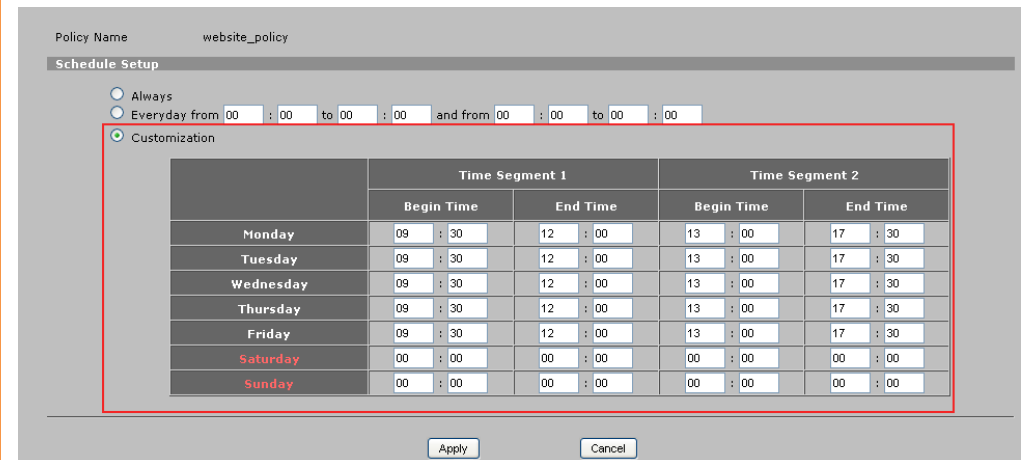
User/Group: Any



Click on the **Schedule** icon to edit the schedule.



Choose **Customization**, and define your office hours.



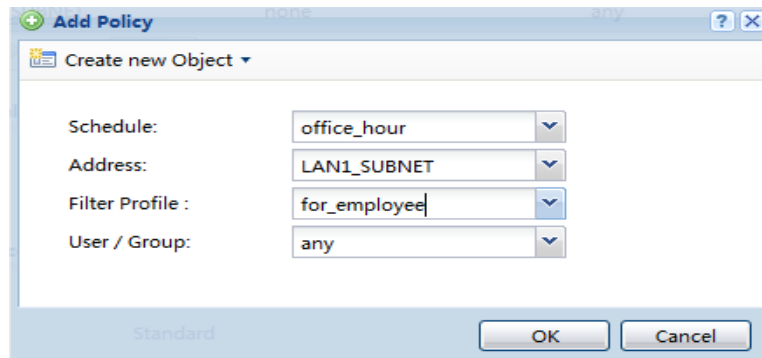
Add an access policy for the employees during office hours.

Schedule: select the “office_hour” object

Address: select the LAN subnet address object.

Filter Profile: select the “for_employee” profile created in the Profile page.

User/Group: Any

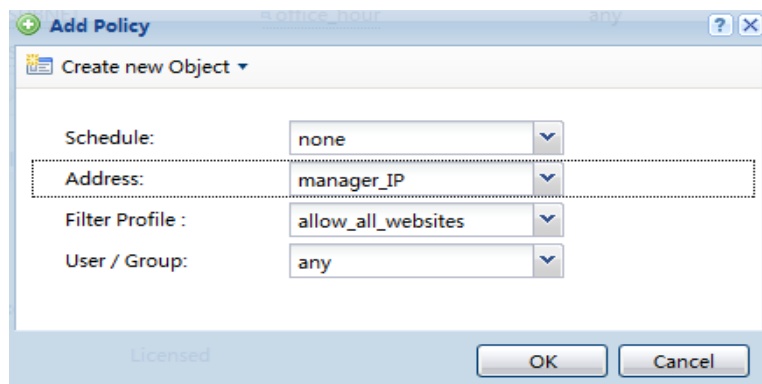


Add an access policy for the manager.

Schedule: none (all the time)

Address: manager’s IP address

Filter Profile: select the profile “allow_all_websites” created in Profile page.



Check the created policies. Make sure their order lists as below:

⊕ Add ✎ Edit 🗑 Remove 💡 Activate ⚪ Inactivate ↻ Move

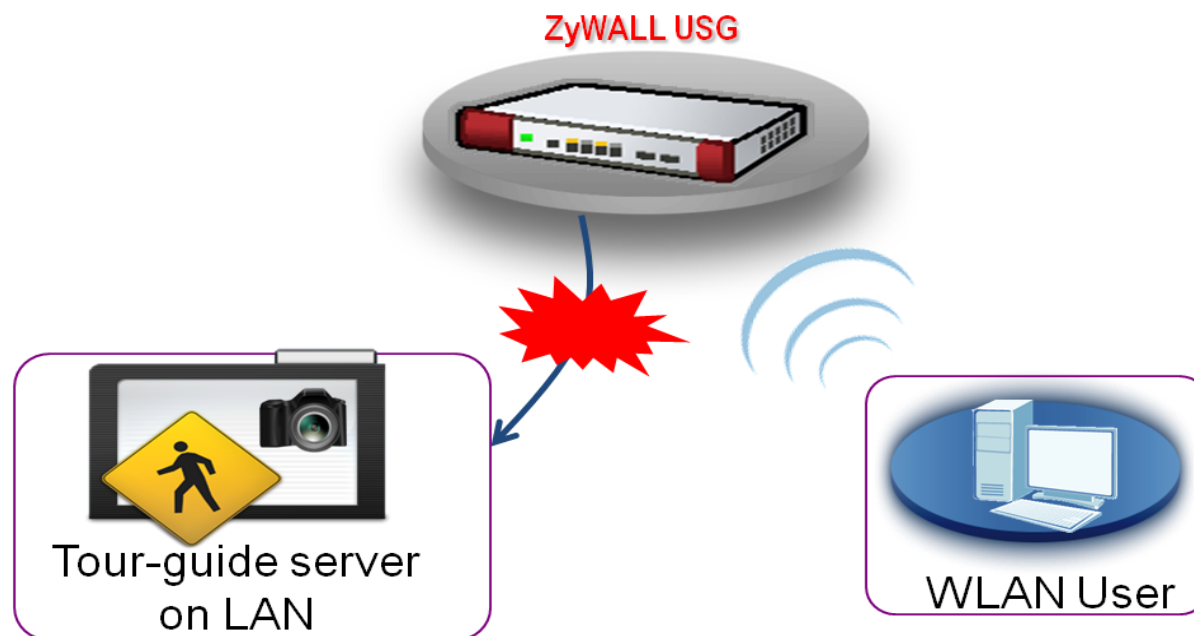
#	Status	Address	Schedule	User	Filter Profile
1	💡	manager_IP	none	any	allow_all_websites
2	💡	LAN1_SUBNET	office_hour	any	for_employee
3	💡	LAN1_SUBNET	none	any	allow_all_websites

⏪ ⏩ Page 1 of 1 Show 50 items

Scenario 11 — Quick Setup for Allowing WLAN Users to Access LAN Services (USG 20W only)

11.1 Application Scenario

To provide rich and helpful tour information to customers, most hotels have a tour guide server to present the message. However, due to the security protection design, WLAN users cannot access the server on LAN side by default. To enable this, the system administrator needs to configure the firewall policy to allow access from WLAN to LAN and also from LAN to WLAN. To streamline the configuration process, the administrator can simply relocate the WLAN users and the server on LAN side into the same security group to give them identical properties. The steps below will show you how to realize this.



11.2 Configuration Guide

Goal to achieve:

A quick setup to allow users connected by WLAN access the service in the LAN zone.

ZLD configuration

Step 1. Click **CONFIGURATION** > **Network** > **Interface** > **WLAN** to open the configuration screen.

The screenshot shows the ZyXEL ZyWALL USG 20W configuration interface. The 'WLAN' tab is selected in the top navigation bar. The 'General' tab is active, showing the 'Enable WLAN Device' checkbox checked. The '802.11 Band' is set to 'b+g+n' and the 'Channel' is set to '6'. The 'Interface Summary' table shows one entry for 'wlan-1-1'.

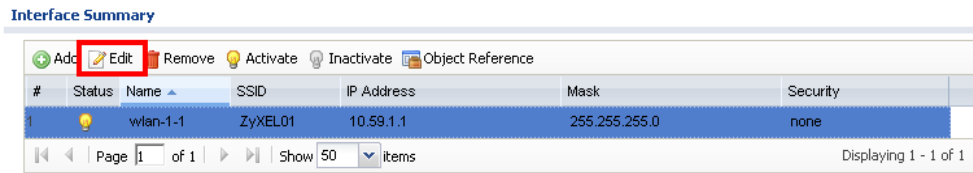
#	Status	Name	SSID	IP Address	Mask	Security
1	🔦	wlan-1-1	ZyXEL-20W	192.168.20.1	255.255.255.0	wep-64

ZyNOS configuration

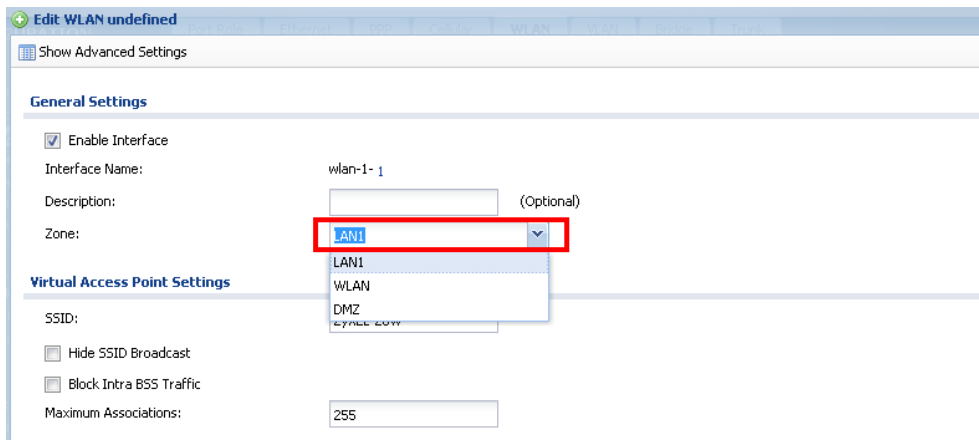
Step 1. Click **WIRELESS** > **Wi-Fi** > **Wireless Card** to open the configuration screen.

The screenshot shows the ZyXEL ZyNOS configuration interface. The 'Wireless Card' tab is selected in the top navigation bar. The 'Wireless Card Setting' section shows the 'Enable Wireless Card' checkbox checked. The 'Bridge to' is set to 'wLAN' and the '802.11 Mode' is set to '802.11b+g'. The 'Choose Channel ID' is set to 'Channel-006 2437MHz'.

Step 2. You can add a new rule by clicking the **Add** button or edit the pre-configured rule by clicking the **Edit** button.



Step 3. Configure this SSID to belong to the LAN zone. With both the WLAN users and the LAN server belonging to the same security zone, the WLAN users will be able to access the LAN service even without modifying the firewall policy.



Step 2. Configure the WLAN bridge to the LAN zone. This will give the WLAN users the same security properties with the LAN server.

Wi-Fi

