



ZyWALL USG Series

Unified Security Gateway

Version 4.10

Edition 1, 05/2014

Application Notes

Table of Contents

Scenario 1 — Connecting your USG to the Internet	4
1.1 Application Scenario	4
1.2 Configuration Guide	4
Scenario 2 — WAN Load Balancing and Customized Usage of WAN	
Connection for Specific Traffic --Dual WAN setting.....	8
2.1 Application Scenario	8
2.2 Configuration Guide	8
Scenario 3 — How to configure NAT if you have Internet-facing public	
servers	13
3.1 Application Scenario	13
3.2 Configuration Guide	13
Scenario 4 — Secure site-to-site connections by using IPSec VPN – IPv4	
with IKEv2 / IPv6	17
4.1 Application Scenario	17
4.2 Configuration Guide	17
Scenario 5 — Connect to USG by using IPSec IKEv2 in Windows 7.....	25
5.1 Application Scenario	25
5.2 Configuration Guide	25
Scenario 6 — GRE over IPSec VPN tunnel –VPN fail over	40
6.1 Application scenario.....	40
6.2 Configuration Guide	40
Scenario 7 - Deploying SSL VPN for Tele-workers to Access Company	
Resources –SSL VPN with Apple Mac OSX.....	54
7.1 Application Scenario	54
7.2 Configuration Guide	54
Scenario 8 — Reserving Highest Bandwidth Management Priority for	
VoIP traffic	58
8.1 Application Scenario	58
8.2 Configuration Guide	58
Scenario 9 - Reserving Highest Bandwidth Management Priority for a	
Superior User and Control Session per Host – BWM Per IP or Per User	60
9.1 Application Scenario	60
9.2 Configuration Guide	60
Scenario 10 - Using USG to Control Popular Applications –APP patrol .	66
10.1 Application Scenario	66
10.2 Configuration Guide	66

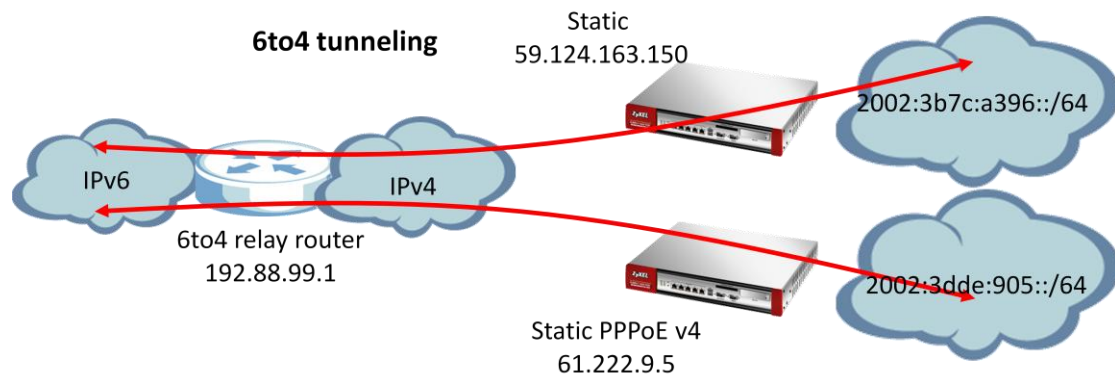
Scenario 11 –configure unified policy (firewall policy + UTM profile).....	70
11.1 Application Scenario	71
11.2 Configuration Guide	71
Scenario 12 – Block HTTPs web site by Content Filter	74
12.1 Application Scenario	74
12.2 Configuration Guide	74
Scenario 13: Single sign-on with USG and Windows platform.....	77
13.1 Application Scenario	77
13.2 Configuration Guide	77
Scenario 14 – WLAN Controller function on USG.....	90
14.1 Application Scenario	90
14.2 Configuration Guide	90
Scenario 15 – Device HA on the USG.....	95
15.1 Application Scenario	95
15.2 Configuration Guide	95

Tutorial 1: How to Set Up Your Network.....	98
1.1 Wizard Overview	98
1.2 How to Configure Interfaces, Port Roles, and Zones	98
1.3 How to Configure a Cellular Interface	101
1.4 How to Set Up a Wireless LAN.....	103
1.6 How to Set Up IPv6 Interfaces For Pure IPv6 Routing.....	108
1.7 How to Set Up an IPv6 6to4 Tunnel.....	113
1.8 How to Set Up an IPv6-in-IPv4 Tunnel	117
Tutorial 2: Protecting Your Network	121
2.1 Firewall	121
2.2 User-aware Access Control.....	122
2.3 Device and Service Registration	123
2.4 Anti-Virus Policy Configuration	124
2.5 IDP Profile Configuration	126
2.6 ADP Profile Configuration	127
2.7 Content Filter Profile Configuration.....	129
2.8 Viewing Content Filter Reports	131
2.9 Anti-Spam Policy Configuration	134
Tutorial 3: Create Secure Connections Across the Internet.....	136
3.1 IPSec VPN.....	136
3.2 VPN Concentrator Example	138
3.3 Hub-and-spoke IPSec VPN Without VPN Concentrator	140
3.4 USG IPSec VPN Client Configuration Provisioning	142
3.5 SSL VPN.....	144
3.6 L2TP VPN with Android, iOS, and Windows.....	145
Tutorial 4: Managing Traffic	159
4.1 How to Configure Bandwidth Management.....	159
4.2 How to Configure a Trunk for WAN Load Balancing	166
4.3 How to Use Multiple Static Public WAN IP Addresses for LAN-to-WAN Traffic	168
4.4 How to Use Device HA to Backup Your USG.....	169
4.5 How to Configure DNS Inbound Load Balancing.....	173
4.6 How to Allow Public Access to a Web Server	189
4.7 How to Manage Voice Traffic	177
4.8 How to Limit Web Surfing and MSN to Specific People.....	197

Scenario 1 — Connecting your USG to the Internet

1.1 Application Scenario

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



1.2 Configuration Guide

Network conditions:

USG:

WAN1: 61.222.9.5(Static PPPoE v4)

Or

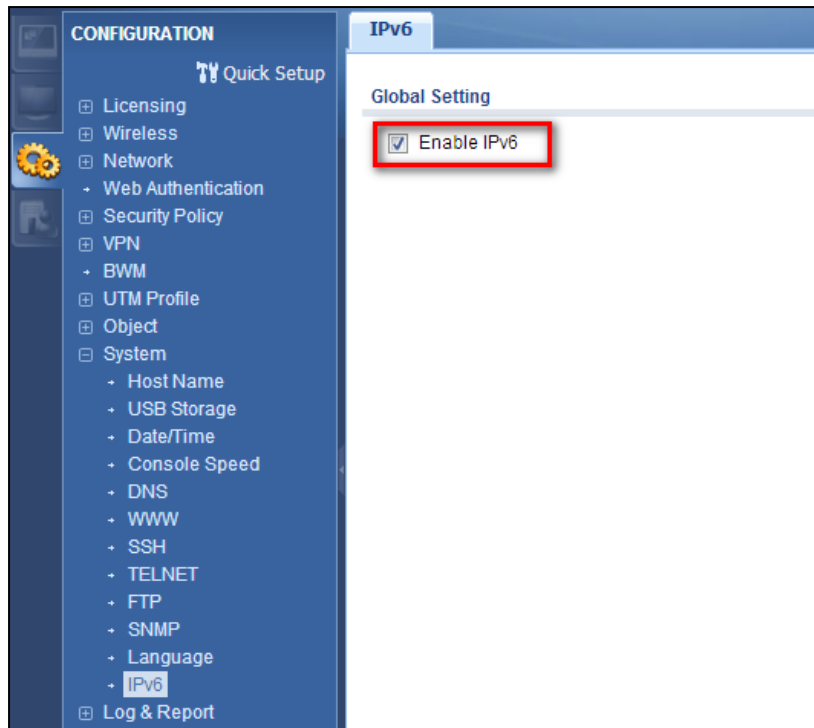
WAN1: 59.124.163.150(Static)

Goal to achieve:

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

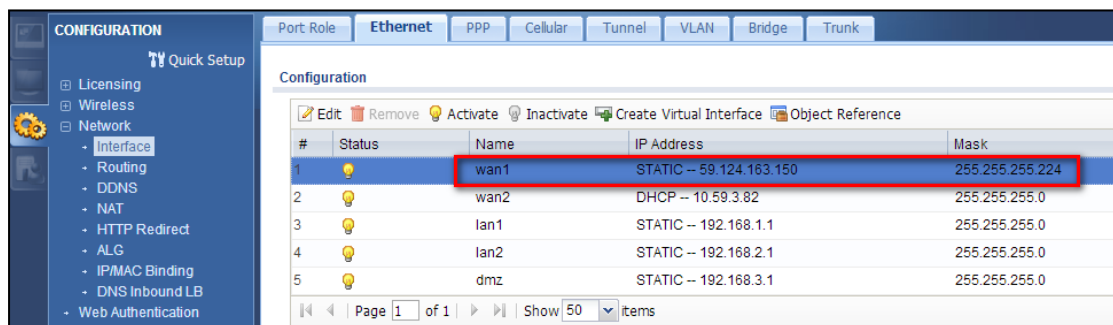
USG configuration

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



Step 2: Setting the static IP on WAN1

Configuration > Interface > Ethernet > double-click on **WAN1** interface and configure with static IP address 59.124.163.150.



Step 3: Setting IPv6 IP address on LAN1

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

Edit Ethernet

IPv6 View ▾ Show Advanced Settings Create new Object

General Settings

☒ Enable Interface

General IPv6 Setting

☒ Enable IPv6 ⓘ

Interface Properties

Interface Type: internal

Interface Name: lan1

Port: P3, P4, P5, P6

Zone: LAN1

MAC Address: B0:B2:DC:70:C1:D8

(2) Convert WAN1 IP address to hexadecimal. 59.124.163.150(Decimal) = 3b7c:a396(Hex). Fill-in **2002:3b7c:a396::1/128** in the prefix table as the LAN interface IPv6 address.

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

Edit Ethernet

IPv6 View ▾ Show Advanced Settings Create new Object

☒ IGMP Downstream

IPv6 Address Assignment

☒ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: fe80::b2b2:dcff:fe70:c1d8/64

IPv6 Address/Prefix Length: 2002:3b7c:a396::1/1 (Optional)

DHCPv6 Setting

DHCPv6: N/A

IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

Router Preference: Medium

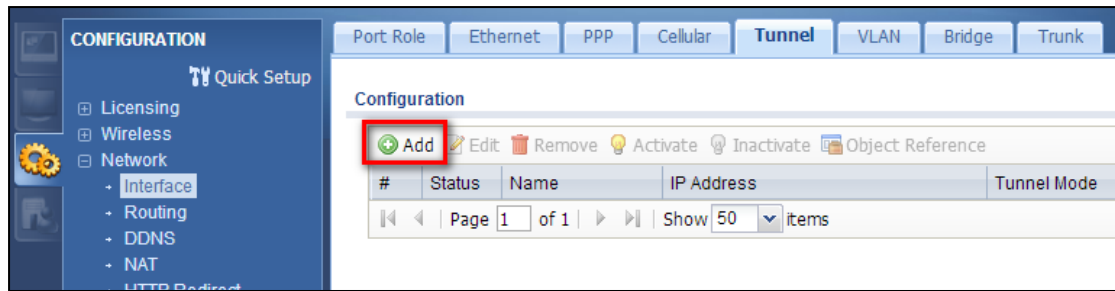
Advertised Prefix Table

#	IPv6 Address/Prefix Length
1	2002:3b7c:a396::/64

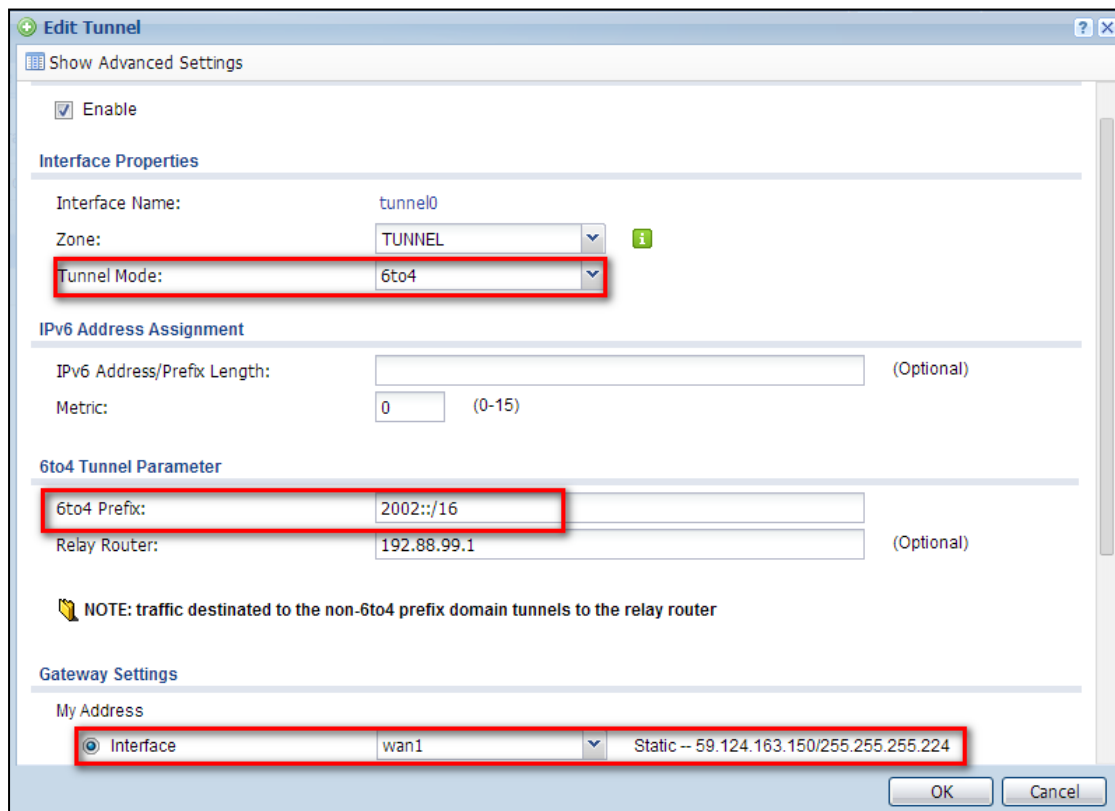
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Step 4: Enable 6 to 4 tunnel.

(1) **Configuration > Interface>Tunnel > Click on the Add button.**



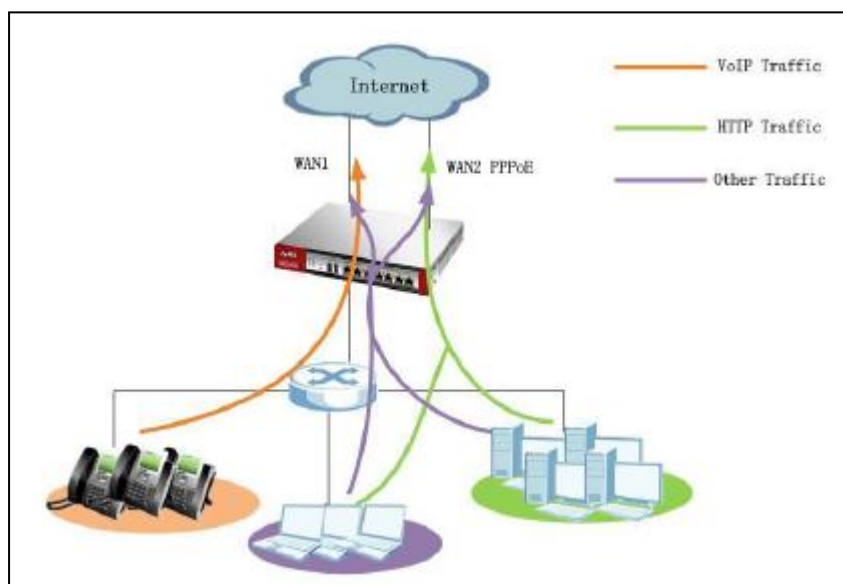
- (2) Select the **6to4** in that **Tunnel Mode**.
- (3) Check the **Prefix** in the **6tp4 tunnel Parameter**.
- (4) Select the **WAN1** interface as the gateway in the **Gateway Setting**.



Scenario 2 — WAN Load Balancing and Customized Usage of WAN Connection for Specific Traffic -- Dual WAN setting

2.1 Application Scenario

The company has two WAN connections for sharing outbound internet traffic. WAN1 uses a static IP address, 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. The 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.



2.2 Configuration Guide

Goals to achieve:

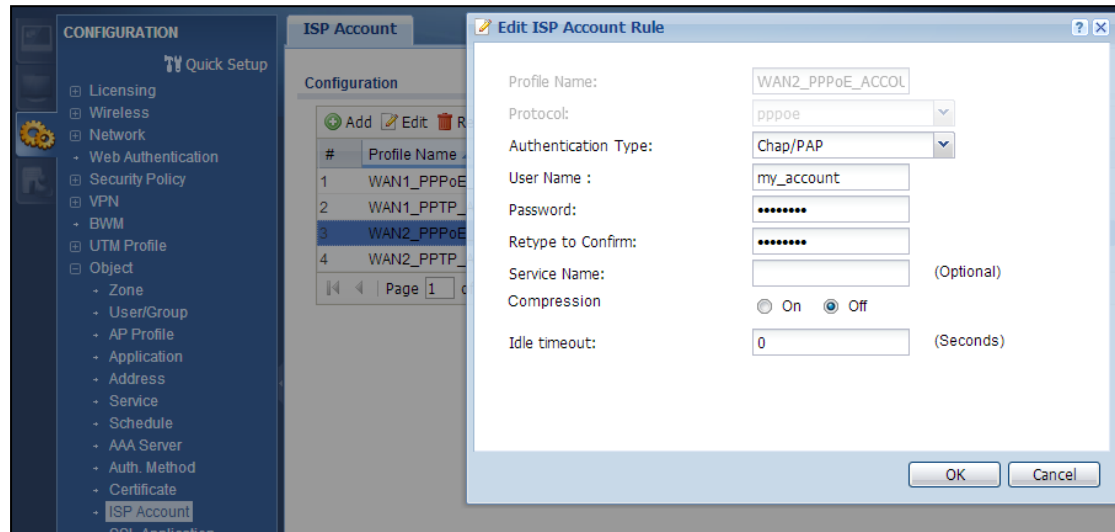
- 1) VoIP traffic goes out primarily through WAN1. In case WAN1 is down, it will go out via WAN2 PPPoE connection.
- 2) HTTP traffic goes out primarily through WAN2 PPPoE connection. In case WAN2 PPPoE is down, it will go out via WAN1.
- 3) All other traffic goes out via WAN trunk performing Load Balancing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

Load Balancing algorithm.

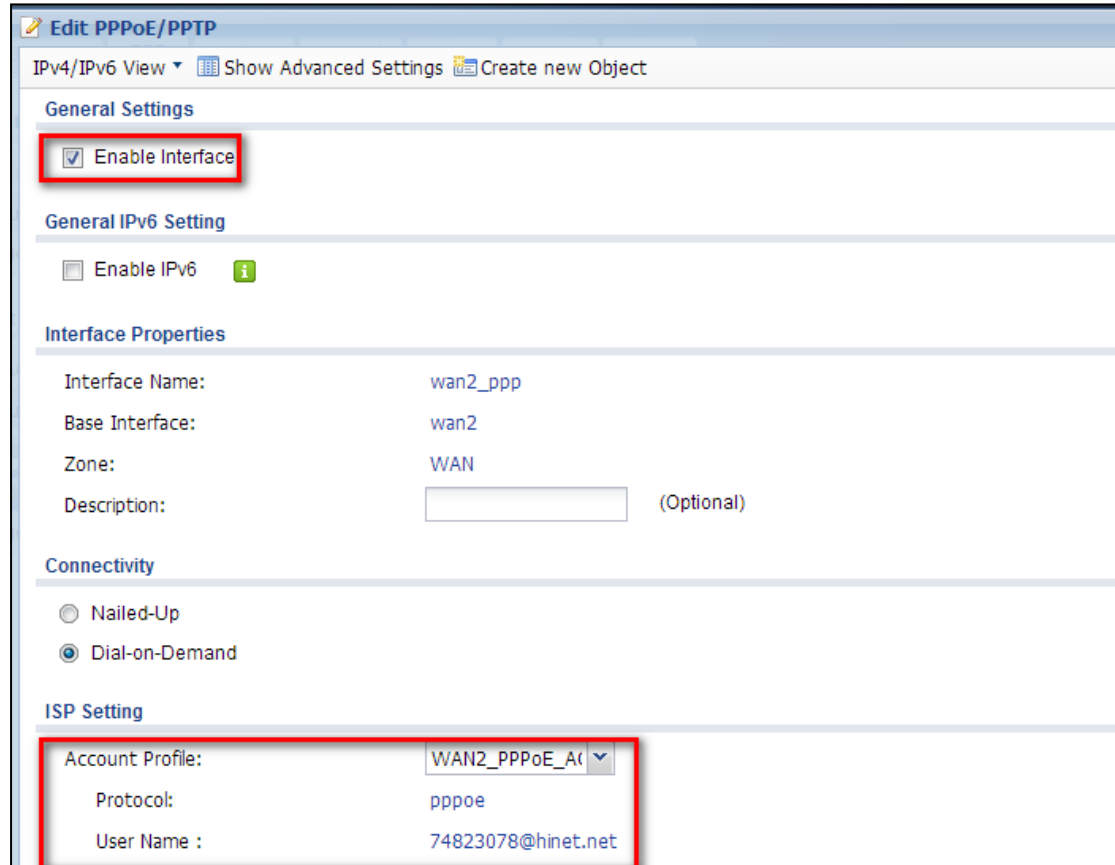
USG configuration

Step 1. Configure a PPPoE account on WAN2 interface.

(1) Go to **CONFIGURATION > Object > ISP Account**, add a PPPoE account:

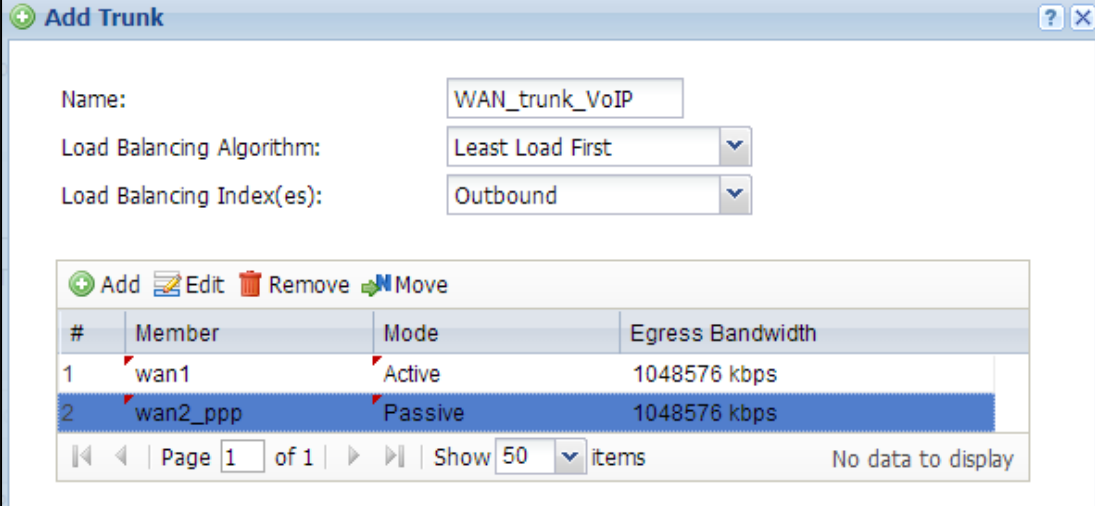


(2) Go to **CONFIGURATION > Network > Interface > PPP**, add a new PPP interface, which is based on WAN 2 interface:



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

- (1) Add WAN trunk for VoIP traffic — Set WAN1 as Active mode, while setting WAN2_ppp as Passive mode.



Add Trunk

Name: WAN_trunk_VoIP

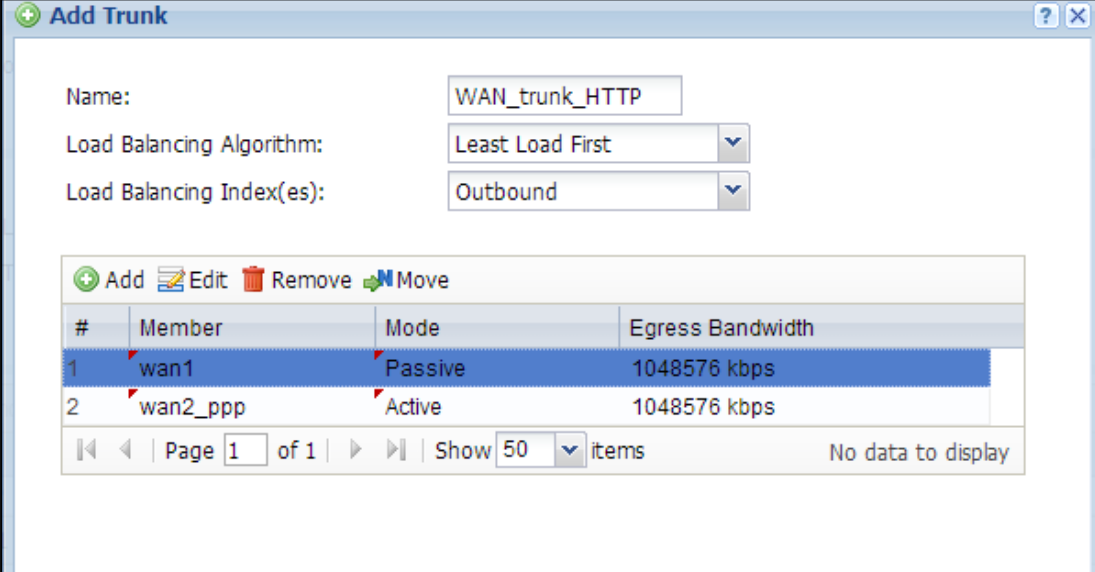
Load Balancing Algorithm: Least Load First

Load Balancing Index(es): Outbound

#	Member	Mode	Egress Bandwidth
1	wan1	Active	1048576 kbps
2	wan2_ppp	Passive	1048576 kbps

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

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



Add Trunk

Name: WAN_trunk_HTTP

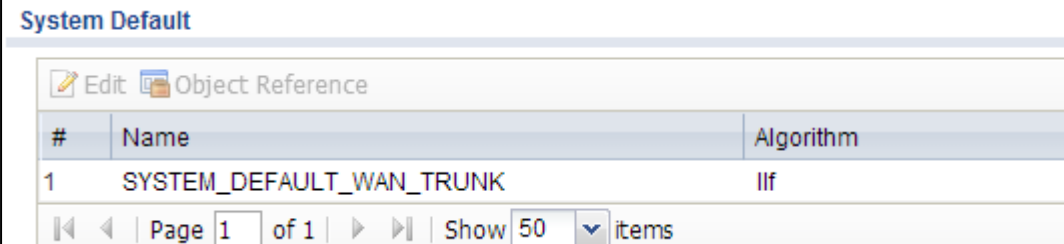
Load Balancing Algorithm: Least Load First

Load Balancing Index(es): Outbound

#	Member	Mode	Egress Bandwidth
1	wan1	Passive	1048576 kbps
2	wan2_ppp	Active	1048576 kbps

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

- (3) Use SYSTEM_DEFAULT_WAN_TRUNK to perform load balancing for all other traffic.



System Default

Edit Object Reference

#	Name	Algorithm
1	SYSTEM_DEFAULT_WAN_TRUNK	lbf

Page 1 of 1 | Show 50 items

Step 3. Go to **CONFIGURATION > Network > Routing > Policy Route**, add policy

routes for VoIP traffic and HTTP traffic.

(1) 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

Add Policy Route

Show Advanced Settings Create new Object

Criteria

User: any

Incoming: any (Excluding ZyWALL)

Source Address: LAN1_SUBNET

Destination Address: any

DSCP Code: any

Schedule: none

Service: SIP

Next-Hop

Type: Trunk

Trunk: WAN_trunk_VoIP

DSCP Marking

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.

CONFIGURATION

Quick Setup

- Licensing
- Wireless
- Network
 - Interface
 - Routing
 - DDNS
 - NAT
 - HTTP Redirect
 - ALG
 - IP/MAC Binding
 - DNS Inbound LB
 - Web Authentication
- Security Policy
- VPN
- BWM
- UTM Profile

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)

☐ Restrict Peer to Peer Signaling Connection

☐ Restrict Peer to Peer Media Connection

SIP Signaling Port :

Add Edit Remove

#	Port
1	5060

(2) 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.

Add Policy Route

Show Advanced Settings Create new Object

Criteria

User: any

Incoming: any (Excluding ZyWALL)

Source Address: LAN1_SUBNET

Destination Address: any

DSCP Code: any

Schedule: none

Service: HTTP

Next-Hop

Type: Trunk

Trunk: WAN_trunk_HTTP

- (3) For all other traffic, use **SYSTEM_DEFAULT_WAN_TRUNK** to perform load balancing. Go to **Configuration > Network > Interface > Trunk**. Click on **Show Advanced Settings**.

CONFIGURATION

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

Quick Setup Show Advanced Settings

Configuration

☒ Disconnect Connections Before Falling Back

Default WAN Trunk

- 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_HTTP

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, the user can configure a NAT mapping rule to forward the traffic from the Internet side to intranet side. This feature does not only ensure service availability, but also helps avoid exposing the server's real IP address from being attacked.

3.2 Configuration Guide

Goal to achieve:

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

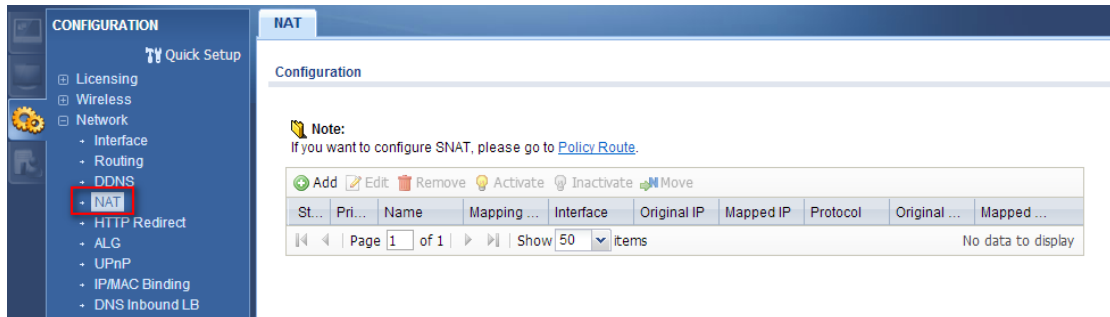
Network Conditions: USG-50:

- WAN IP: 59.124.163.152
- FTP server IP: 192.168.50.33



Configuration

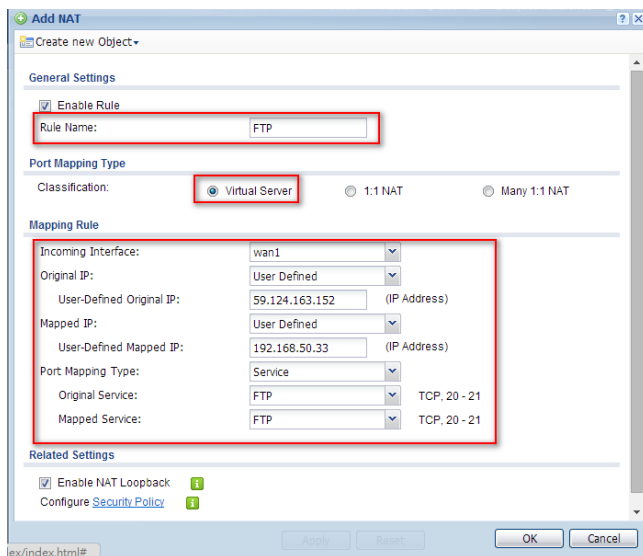
Step 1. Go to **CONFIGURATION > Network > NAT** to open the configuration screen.



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

Step 3. In this page, the user needs to configure:

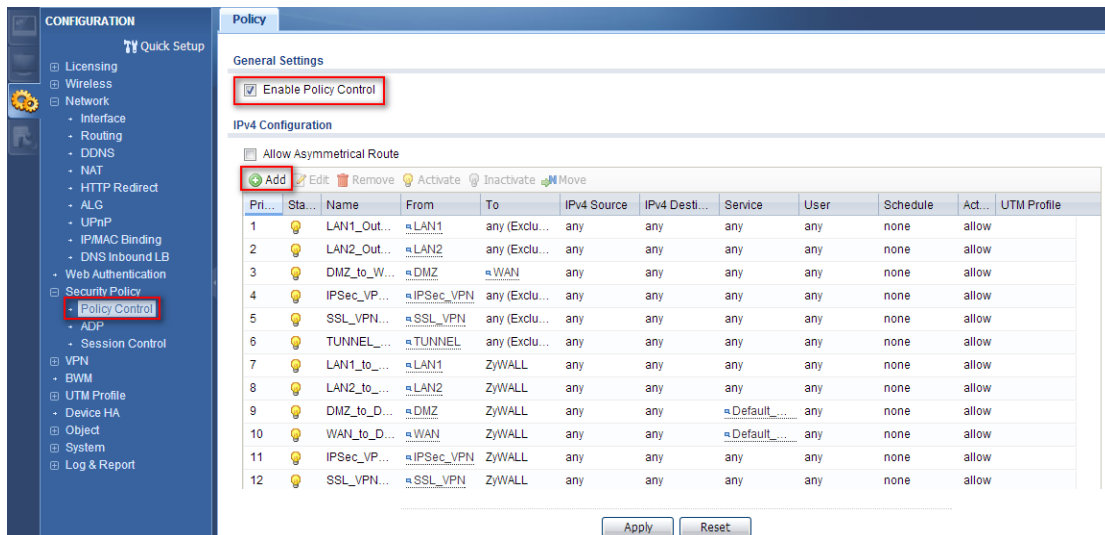
- Rule's name
- Select Virtual Server type to let USG-50 do packet forwarding
- Fill-in the **Original IP** (WAN IP) address
- Fill-in the **Mapped IP** (Internal FTP server IP) address
- Select the **service to be mapped** (FTP); the ports will be selected automatically



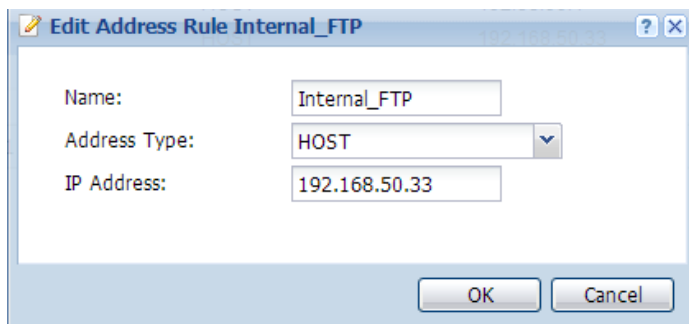
Step 4. Go to **CONFIGURATION > Security Policy > Policy Control** to open the firewall configuration screen.

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

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



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



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

Add corresponding

Create new Object

☒ Enable

Name: For_FTP

Description: (Optional)

From: WAN

To: LAN1

Source: any

Destination: Internal_FTP

Service: FTP

User: any

Schedule: none

Action: allow

Log matched traffic: no

UTM Profile

☐ Application Patrol: none Log: by profile

☐ Content Filter: none Log: by profile

☐ IDP: none Log: by profile

☐ Anti-Virus: none Log: by profile

☐ Anti-Spam: none Log: by profile

☐ SSL Inspection: none Log: by profile

Apply Reset OK Cancel

Step 8: Click on the **OK** button, you will see the rule in policy control.

CONFIGURATION

Quick Setup

- Licensing
- Wireless
- Network
 - Interface
 - Routing
 - DDNS
 - NAT
 - HTTP Redirect
 - ALG
 - UPnP
 - IP/MAC Binding
 - DNS Inbound LB
- Security Policy
 - Policy Control
 - ADP
 - Session Control
- VPN
 - BWM
 - UTM Profile
 - Device HA
 - Object
 - Zone

Policy

General Settings

☒ Enable Policy Control

IPv4 Configuration

☐ Allow Asymmetrical Route

Add Edit Remove Activate Inactivate Move

Pri...	Sta...	Name	From	To	IPv4 Source	IPv4 Desti...	Service	User	Schedule	Act...	UTM Profile
1		For_FTP	WAN	LAN1	any	Internal_...	FTP	any	none	allow	
2		LAN1_Out...	LAN1	any (Exclu...	any	any	any	any	none	allow	
3		LAN2_Out...	LAN2	any (Exclu...	any	any	any	any	none	allow	
4		DMZ_to_W...	DMZ	WAN	any	any	any	any	none	allow	
5		IPSec_VPN...	IPSec_VPN	any (Exclu...	any	any	any	any	none	allow	
6		SSL_VPN...	SSL_VPN	any (Exclu...	any	any	any	any	none	allow	
7		TUNNEL...	TUNNEL	any (Exclu...	any	any	any	any	none	allow	
8		LAN1_to...	LAN1	ZyWALL	any	any	any	any	none	allow	
9		LAN2_to...	LAN2	ZyWALL	any	any	any	any	none	allow	
10		DMZ_to_D...	DMZ	ZyWALL	any	Default_...	any	any	none	allow	

Scenario 4 — Secure Site-to-site Connections using IPSec VPN – IPv4 with IKEv2 / IPv6

4.1 Application Scenario

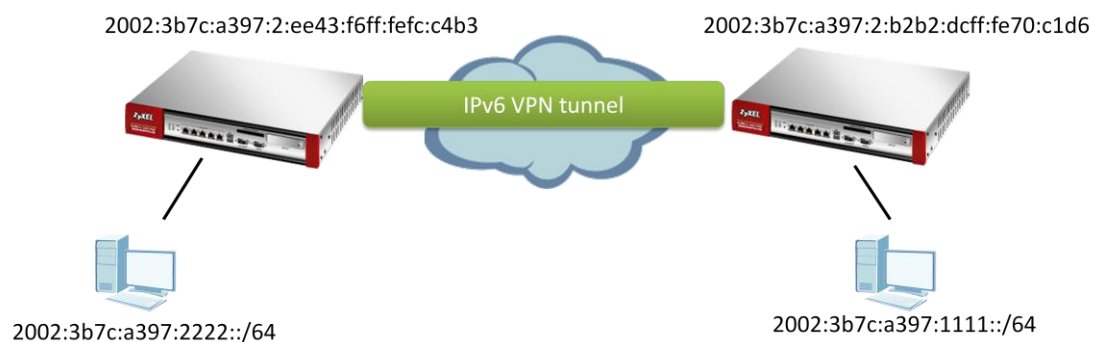
IPv4 with IKEv2

We want to use IKEv2 to establish a VPN tunnel between the HQ and Branch Office.



IPv6 (with IKEv2 only)

ISP has changed the environment to IPv6. We applied for IPv6 address pool for internal use. So we have to change use the IPv6 address to establish an VPN tunnel between the USG.



4.2 Configuration Guide

IPv4

Network Conditions:

USG-40W with static WAN:

- WAN IP: 59.124.163.155
- Local subnet: 192.168.100.0/24

USG-40W with PPPOE WAN:

- PPPOE IP: 220.137.67.76
- Local subnet: 192.168.200.0/24

IPSec VPN Conditions:

Phase 1:	Phase 2:
IKE version: IKEv2	Active Protocol: ESP
Authentication: 1234567890	Encapsulation Mode: Tunnel
Local/Peer ID type: IPv4 0.0.0.0 / Any	Encryption Algorithm: DES
Encryption Algorithm: 3DES	Authentication Algorithm: SHA1
Authentication Algorithm: MD5	Perfect Forward Secrecy: None
Key Group: DH1	

Goal to achieve:

Establish an IPSec VPN tunnel between two USGs with the above configuration.

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

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



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

- VPN gateway name
- Enable IKEv2 protocol
- 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

Add VPN Gateway

Hide Advanced Settings
Create new Object

General Settings

☒ Enable

VPN Gateway Name:

To_PPPOE40W_GW

IKE Version

☐ IKEv1

☒ IKEv2

Gateway Settings

My Address

☒ Interface

wan1

Static -- 59.124.163.155/255.255.255.224

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary

220.137.67.76

Secondary

0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval:

300

(60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

1234567890

☒ unmasked

☐ Certificate

default

(See My Certificates)

Local ID Type:

IPv4

Content:

0.0.0.0

Peer ID Type:

Any

Content:

Phase 1 Settings

SA Life Time:

86400

(180 - 3000000 Seconds)

Proposal

Add Edit Remove

#	Encryption	Authentication
1	3DES	MD5

Key Group:

DH1

Extended Authentication Protocol

☒ Enable Extended Authentication Protocol

Allowed Auth Method:

mschapv2

☒ Server Mode

AAA Method:

default

Allowed User:

any

☐ Client Mode

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

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



Step 6. To configure the phase-2 rule, the 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

Add VPN Connection

Hide Advanced Settings
Create new Object

General Settings

☒ Enable

Connection Name:
To_PPPOE40W_VPN

☐ Nailed-Up

☐ Enable Replay Detection

☐ Enable NetBIOS broadcast over IPsec

MSS Adjustment

☐ Custom Size
0
(200 - 1460 Bytes)

☒ Auto

☒ Narrowed

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway:
To_PPPOE40W_GW
wan1
220.137.67.76, 0.0.0.0

Policy

Local policy:
LAN1_SUBNET
INTERFACE SUBNET, 192.168.100.0/24

Remote policy:
PPPOE40W_LAN
SUBNET, 192.168.200.0/24

☐ Enable GRE over IPsec

☐ Policy Enforcement

Phase 2 Setting

SA Life Time:
86400
(180 - 3000000 Seconds)

Active Protocol:
ESP

Encapsulation:
Tunnel

Proposal

Add Edit Remove

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS):
none

Related Settings

Zone:
IPSec_VPN

Connectivity Check

☐ Enable Connectivity Check

Check Method:
icmp

Check Period:
5
(5-600 Seconds)

Check Timeout:
5
(1-10 Seconds)

Check Fail Tolerance:
(1-10)

☐ Check This Address

☒ Check the First and Last IP Address in the Remote Policy

☐ Log

Inbound/Outbound traffic NAT

Outbound Traffic

☐ Source NAT

Source:
Please select one ...

Destination:
Please select one ...

SNAT:
Please select one ...

Inbound Traffic

☐ Source NAT

Source:
Please select one ...

Destination:
Please select one ...

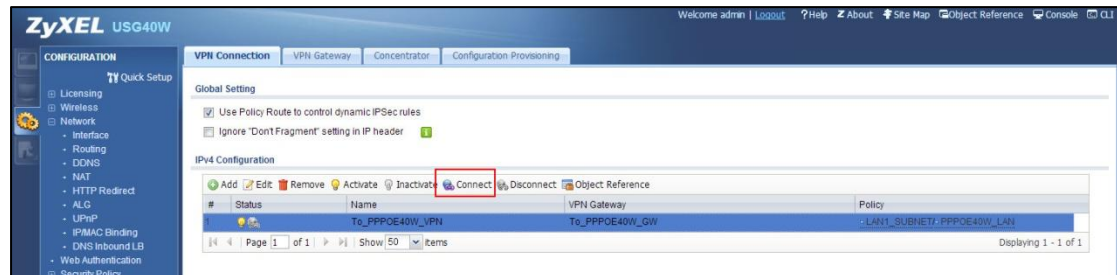
SNAT:
Please select one ...

☐ Destination NAT

Add Edit Remove Move

#	Original IP	Mapped IP	Protocol	Original Port S...	Original Port End	Mapped Port S...	Mapped Port E...
---	-------------	-----------	----------	--------------------	-------------------	------------------	------------------

Step 7. After setting the rule, the user can select the rule and click on 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, the user can find the SA information on **MONITOR > VPN MONITOR > IPSec**.

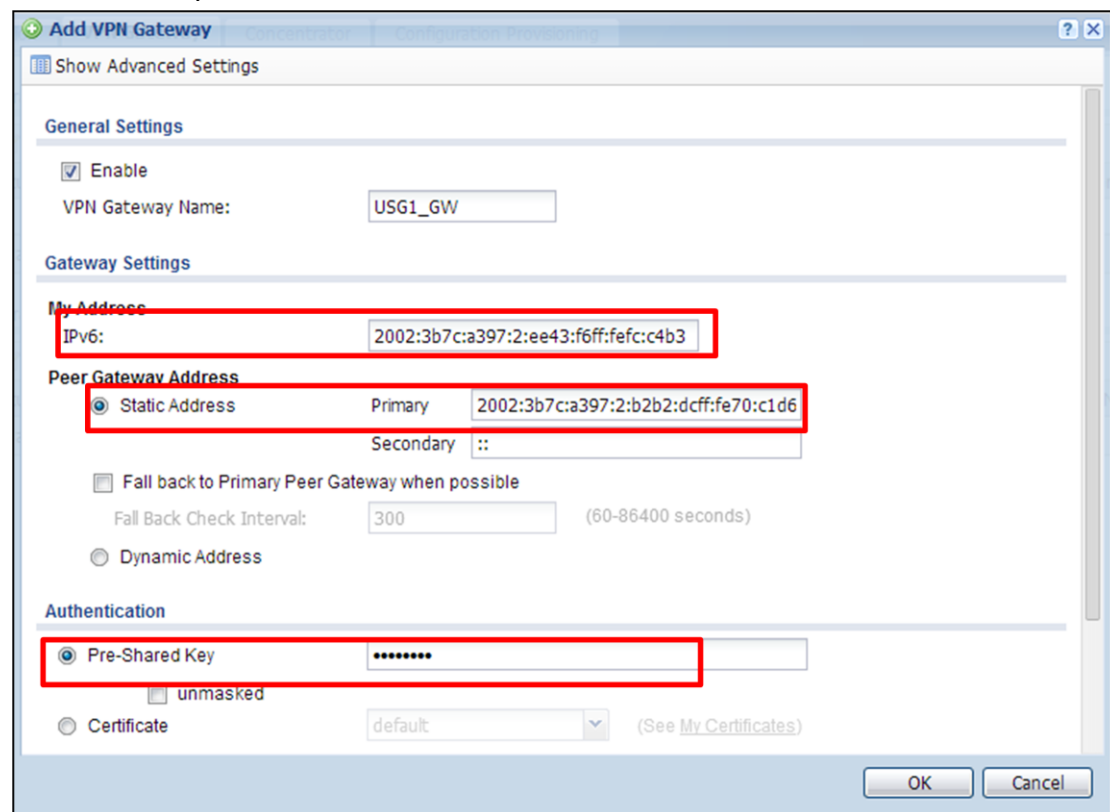
IPv6

Step 1. Add an IPV6 VPN phase I on USG1. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**.

My Address: 2002:3b7c:a397:2:ee43:f6ff:fe70:c4b3

Peer Gateway Address: 2002:3b7c:a397:2:b2b2:dcff:fe70:c1d6

Pre-Shared Key: 12345678



Step 2. Add an IPv6 VPN phase II on USG1. Go to **CONFIGURATION > VPN > IPSec**

VPN > VPN Connection.

VPN Gateway: USG1_GW

Local policy: 2002:3b7c:a397:2222::/64

Remote policy: 2002:3b7c:a397:1111::/64

Step 3. Add an IPV6 VPN phase I on USG2. Go to **CONFIGURATION > VPN > IPSec**

VPN > VPN Gateway.

My Address: 2002:3b7c:a397:2:b2b2:dcff:fe70:c1d6

Peer Gateway Address: 2002:3b7c:a397:2:ee43:f6ff:fefc:c4b3

Pre-Shared Key: 12345678

Step 4. Add an IPV6 VPN phase II on USG2. Go to **CONFIGURATION > VPN > IPSec**

VPN > VPN Connection.

VPN Gateway: USG2_GW

Local policy: 2002:3b7c:a397:1111::/64

Remote policy: 2002:3b7c:a397:2222::/64

Add VPN Connection

Show Advanced Settings Create new Object

General Settings

☒ Enable

Connection Name: USG2_Conn

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: USG2_GW 2002:3b7c:a397:2:b2b2:dcff:fe70:c1d6 2002:3b7c:a397:2:ee43:f6ff:fefc:c4b3, ::

Policy

Local policy: LAN1_SUBNET_DHCPv6 INTERFACE SUBNET, 2002:3b7c:a397:1111::1/64(DHCPv6)

Remote policy: remote_v6 SUBNET, 2002:3b7c:a397:2222::/64

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

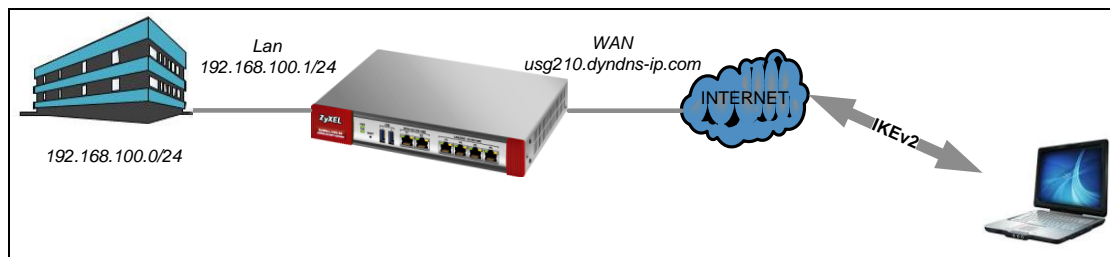
Step 5. When the VPN tunnel is established, the user can find the SA information on

MONITOR > VPN MONITOR > IPSec.

Scenario 5 — Connect to USG using IPSec

IKEv2 in Windows 7

5.1 Application Scenario



Windows 7 supports IPSec IKEv2 with certificate authentication.

This section provides information on how to configure the IKEv2 (Internet Key Exchange) on a Windows 7 PC via certificates.

5.2 Configuration Guide

Network Conditions:

USG 210:

- WAN1 IP: usg210.dyndns-ip.com
- Local subnet: 192.168.100.0/24

USG-210 VPN Conditions:

Phase 1:

- Authentication Method: Certificate
- Local /Peer ID type: DNS / Any
- Encryption and Authentication Algorithm:
3DES/SHA1, AES128/MD5, AES128/SHA1
- Key Group: DH2

Goal to achieve:

Establish an IPSec VPN tunnel from Windows 7 using IKEv2 protocol.

Step 1. Go to **CONFIGURATION > Object > Certificate > My Certificates tab** to add a new certificate for Windows clients.

Add My Certificates

Configuration

Name: CER_For_Windows

Subject Information

☐ Host IP Address

☒ Host Domain Name usg210.dyndns-ip.com **Must select and fill in FQDN**

☐ E-Mail

Organizational Unit: (Optional)

Organization: (Optional)

Town (City): (Optional)

State (Province): (Optional)

Country: (Optional)

Key Type: RSA

Key Length: 2048 bits

Extended Key Usage

☒ Server Authentication

☒ Client Authentication

☒ iKEIntermediate **Must select iKEIntermediate**

☒ Create a self-signed certificate

☐ Create a certification request and save it locally for later manual enrollment

Step 2. Go to **CONFIGURATION > Object > User/Group** to create a user account. Add this account into IKEv2 users group object. This group object will be used in IPsec VPN phase-1 EAP (Extended Authentication Protocol) field.

#	User Name	User Type	Description	Reference
1	admin	admin	Administration account	0
2	ldap-users	ext-user	External LDAP Users	0
3	radius-users	ext-user	External RADIUS Users	0
4	ad-users	ext-user	External AD Users	0
5	spark	user	Local User	0

ZyXEL USG210

Configuration

Group

Configuration

Name: IKEv2_users

Description: (Optional)

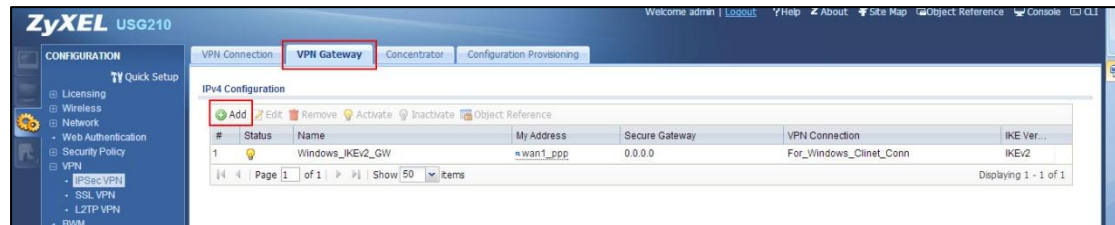
Member List

Available: ad-users, ldap-users, radius-users

Member: spark

Step 3. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** to open the configuration screen.

Step 4. Click on the **Add** button to add a VPN gateway rule.



Step 5. To configure the VPN gateway rule, the user needs to fill-in:

- VPN gateway name:
- IKE Version: IKEv2
- Gateway address: both local (My Address) and peer (Dynamic Address)
- Authentication setting:
 - Certificate
- Phase-1 setting
 - Encryption and Authentication Algorithm:
 - 1) 3DES / SHA1
 - 2) AES128 / MD5
 - 3) AES128 / SHA1
 - 4) Key Group DH2
- Extended Authentication Protocol:
 - Enable Extended Authentication Protocol
 - Server Mode
 - AAA Method: default
 - Allowed User: IKEv2_users

Edit VPN Gateway Windows_IKEv2_GW

Hide Advanced Settings Create new Object

General Settings

☒ Enable

VPN Gateway Name: Windows_IKEv2_GW

IKE Version

☐ IKEv1

☒ IKEv2

Gateway Settings

My Address

☒ Interface wan1_ppp Dynamic -- 111.250.186.198/255.255.255.255

☐ Domain Name / IPv4

Peer Gateway Address

☐ Static Address

Primary 0.0.0.0

Secondary 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

☒ Dynamic Address

Authentication

☐ Pre-Shared Key

☒ Certificate CER_For_Windows (See My Certificates)

Local ID Type: DNS

Content: usg210.dyndns-ip.com

Peer ID Type: Any

Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Proposal

Add Edit Remove

#	Encryption	Authentication
1	3DES	SHA1
2	AES128	MD5
3	AES128	SHA1

Key Group: DH2

Extended Authentication Protocol

☒ Enable Extended Authentication Protocol

Allowed Auth Method: mschapv2

☒ Server Mode

AAA Method: default

Allowed User: IKEv2_users

☐ Client Mode

User Name :

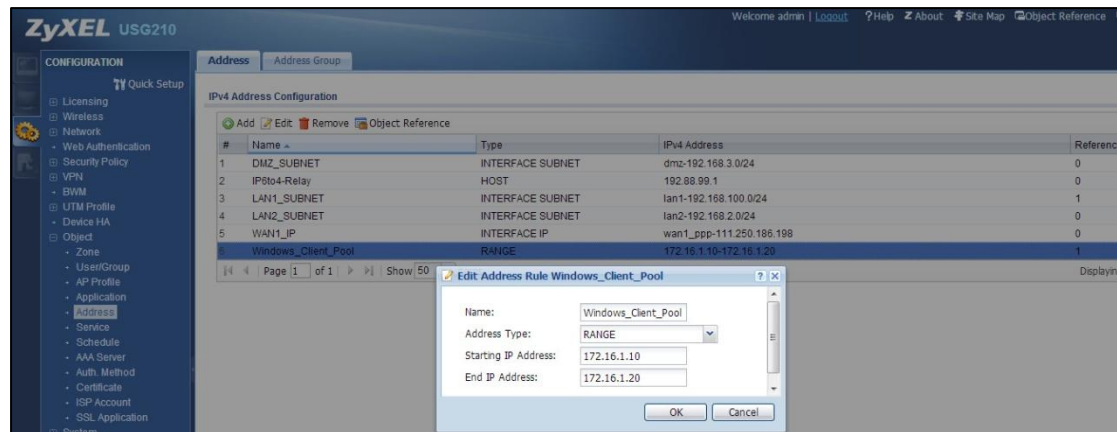
Password:

Retype to Confirm:

Step 6. Go to **CONFIGURATION > Object > Address** to create an address object. This

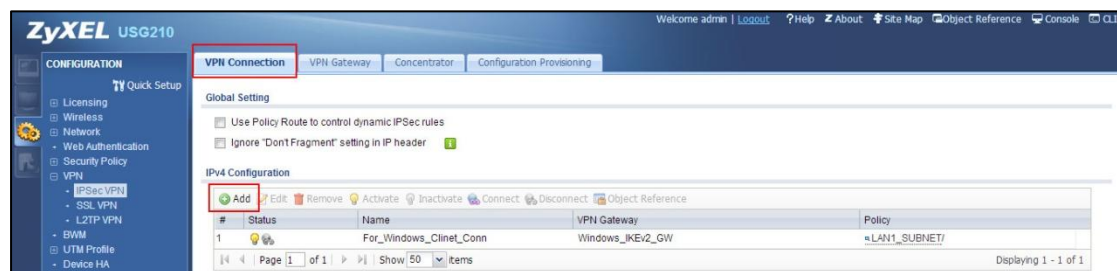
ZyXEL – USG Application Notes

address object's IP address will be assigned to the Windows IKEv2 client's machine.



Step 7. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to open the configuration screen to configure the phase-2 rule.

Step 8. Click on the **Add** button to add a rule.



Step 9. To configure the phase-2 rule, the user needs to fill-in:

- VPN connection name
- VPN gateway selection
- Policy for
 - Local network side
- Configuration Payload
 - Enable Configuration Payload
 - IP Address Pool:
- Phase-2 setting
 - Active protocol
 - Encapsulation mode
 - Encryption algorithm
 - Authentication algorithm
 - Perfect Forward Secrecy

Edit VPN Connection For_Windows_Clinet_Conn
Hide Advanced Settings Create new Object

General Settings

☒ Enable

Connection Name: For_Windows_Clinet_Conn

☐ Nailed-Up

☐ Enable Replay Detection

☐ Enable NetBIOS broadcast over IPSec

MSS Adjustment

☐ Custom Size 0 (200 - 1460 Bytes)

☒ Auto

☒ Narrowed

VPN Gateway

Application Scenario

☐ Site-to-site

☐ Site-to-site with Dynamic Peer

☒ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: Windows_IKEv2_GW wan1_ppp 0.0.0.0, 0.0.0.0

Policy

Local policy: LAN1_SUBNET INTERFACE SUBNET, 192.168.100.0/24

☐ Enable GRE over IPSec

Configuration Payload

☒ Enable Configuration Payload

IP Address Pool: Windows_Client_Pool RANGE, 172.16.1.10-172.16.1.20

First DNS Server (Optional): 1.1.1.1

Second DNS Server (Optional): 2.2.2.2

First WINS Server (Optional): 3.3.3.3

Second WINS Server (Optional): 4.4.4.4

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	3DES	SHA1
2	AES128	SHA256
3	AES256	SHA1

Perfect Forward Secrecy (PFS): none

Related Settings

Zone: IPSec_VPN

Connectivity Check

☐ Enable Connectivity Check

Check Method: icmp

Check Period: (5-600 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: Please select one ...

Destination: Please select one ...

SNAT: Please select one ...

Inbound Traffic

☐ Source NAT

Source: Please select one ...

Destination: Please select one ...

SNAT: Please select one ...

☐ Destination NAT

#	Original IP	Mapped IP	Protocol	Original Port S...	Original Port End	Mapped Port S...	Mapped Port E...
No data to display							

Step 10. Export the certificate, which was generated in step 1, and save it to the Windows 7 machine.

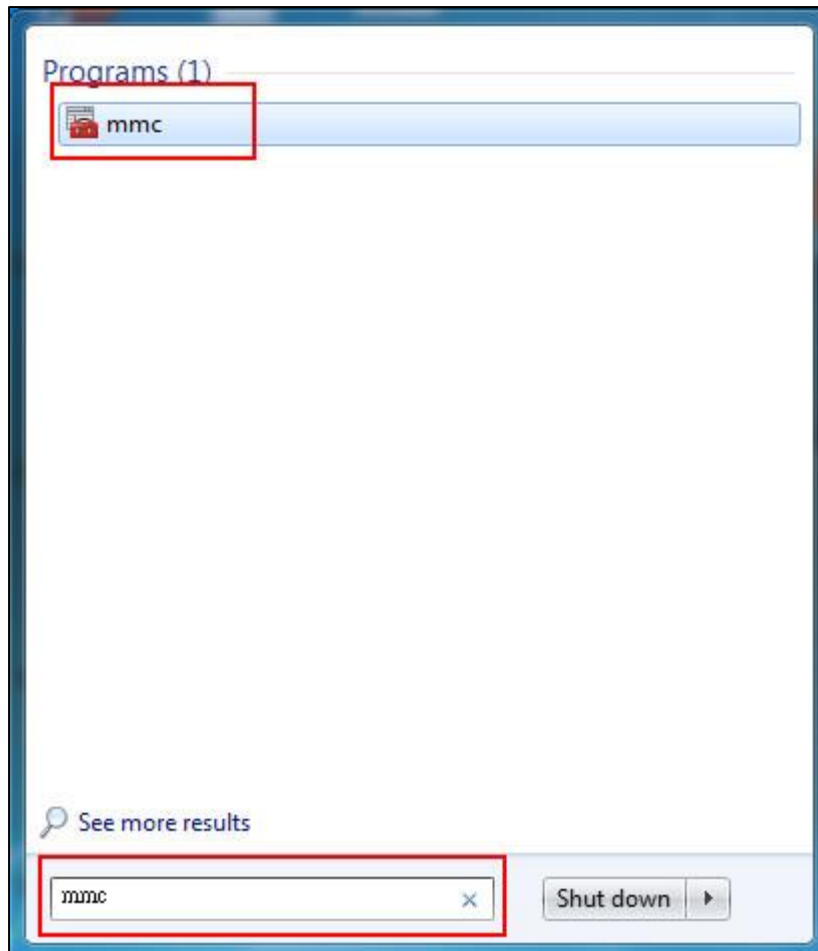
The screenshot shows the 'Edit My Certificates' window with the following sections:

- Configuration:** Name: CER_For_Windows
- Certification Path:** CN=usg210.dyndns-ip.com, Validation Result=self-signed, with a Refresh button.
- Certificate Information:**
 - Type: Self-signed X.509 Certificate
 - Version: V3
 - Serial Number: 1396161402
 - Subject: CN=usg210.dyndns-ip.com
 - Issuer: CN=usg210.dyndns-ip.com
 - Signature Algorithm: rsa-pkcs1-sha1
 - Valid From: 2014-03-30 06:36:42 GMT
 - Valid To: 2017-03-29 06:36:42 GMT
 - Key Algorithm: rsaEncryption (2048 bits)
 - Subject Alternative Name: usg210.dyndns-ip.com
 - Key Usage: DigitalSignature, KeyEncipherment, DataEncipherment, KeyCertSign
 - Extended Key Usage: ServerAuthentication, ClientAuthentication, iKEIntermediate
 - Basic Constraint: Subject Type=CA, Path Length Constraint=1
 - MD5 Fingerprint: eb:1e:f0:f9:e5:ca:04:81:5e:0f:fc:48:d5:8c:e9:34
 - SHA1 Fingerprint: ec:8e:71:ef:ef:66:d9:f1:b2:a6:59:93:e8:ee:a3:93:b5:79:35:44
- Certificate in PEM (Base-64) Encoded Format:**

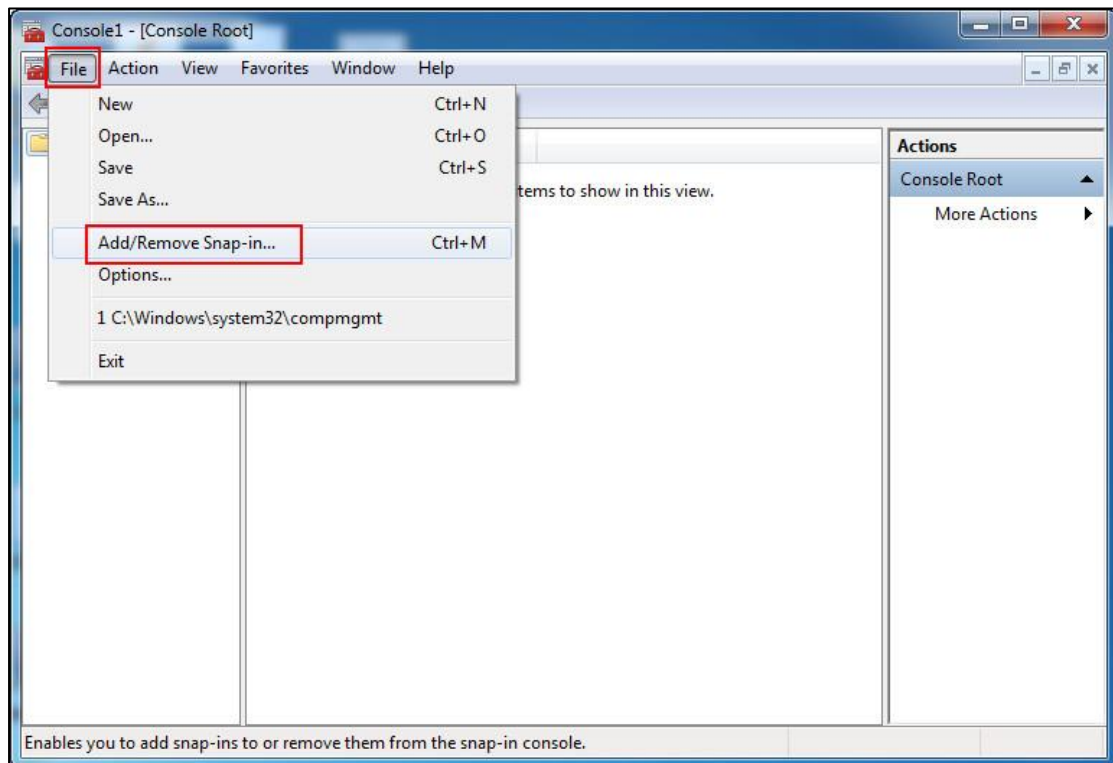
```
-----BEGIN X509 CERTIFICATE-----
MIIDVDCCAjygAwIBAgIEUze7ejANBgkqhkiG9w0BAQUFADAfMR0wGwYDVQQDEXR1
c2cyMTAuZHUZG5zLWlwLmNvbTAeFw0xNDAzMzAwNjM2NDJaFw0xNzAzMjkwNjM2
NDJaMB8xHTAbBgNVBAMTFHVzZzIxMCS5keW5kbmMtaXAuY29tMIIBjANBgkqhkiG

```
- Export Options:**
 - Export Certificate Only (highlighted with a red box)
 - Export Certificate with Private Key

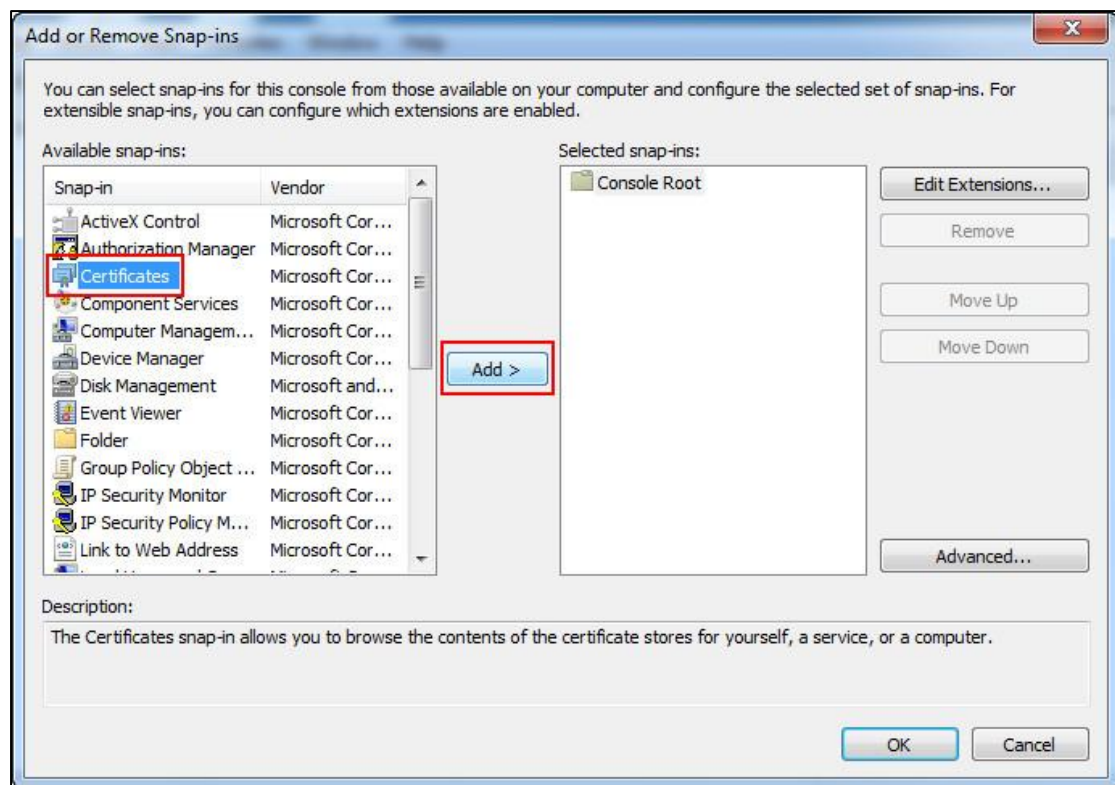
Step 11. In the Windows 7 machine, go to **Start > mmc >**



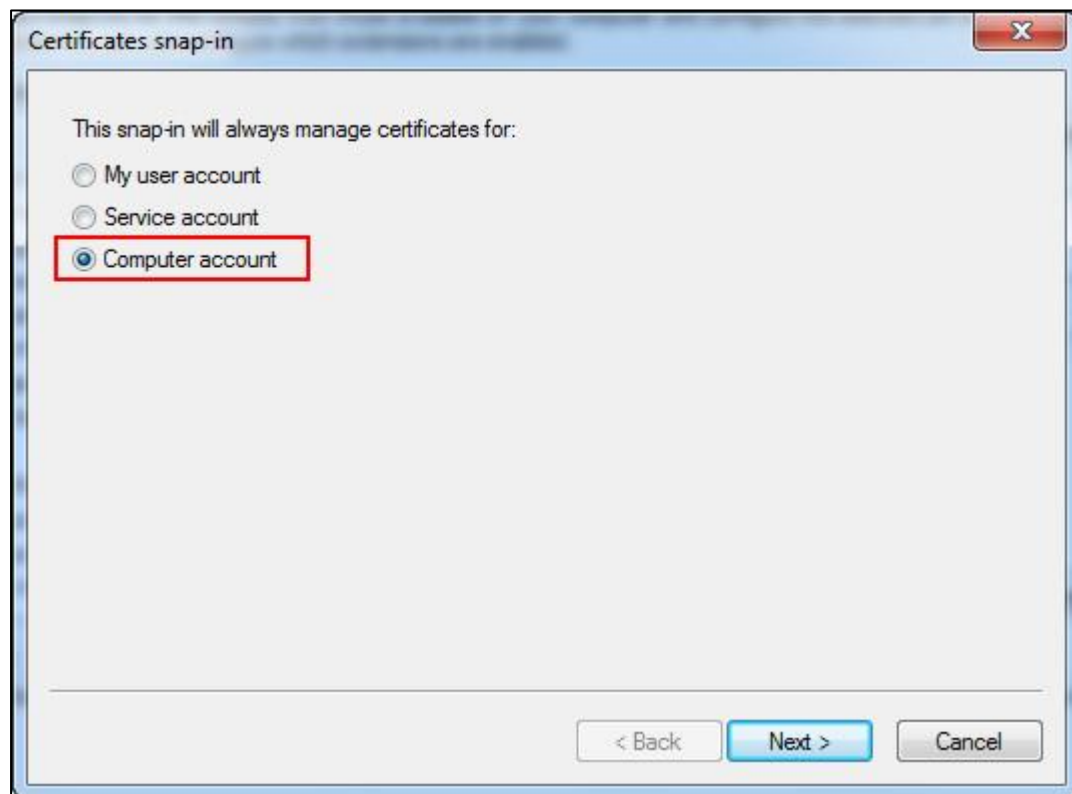
Step 12. In the mmc console, click on **File > Add/Remove Snap-in... >**

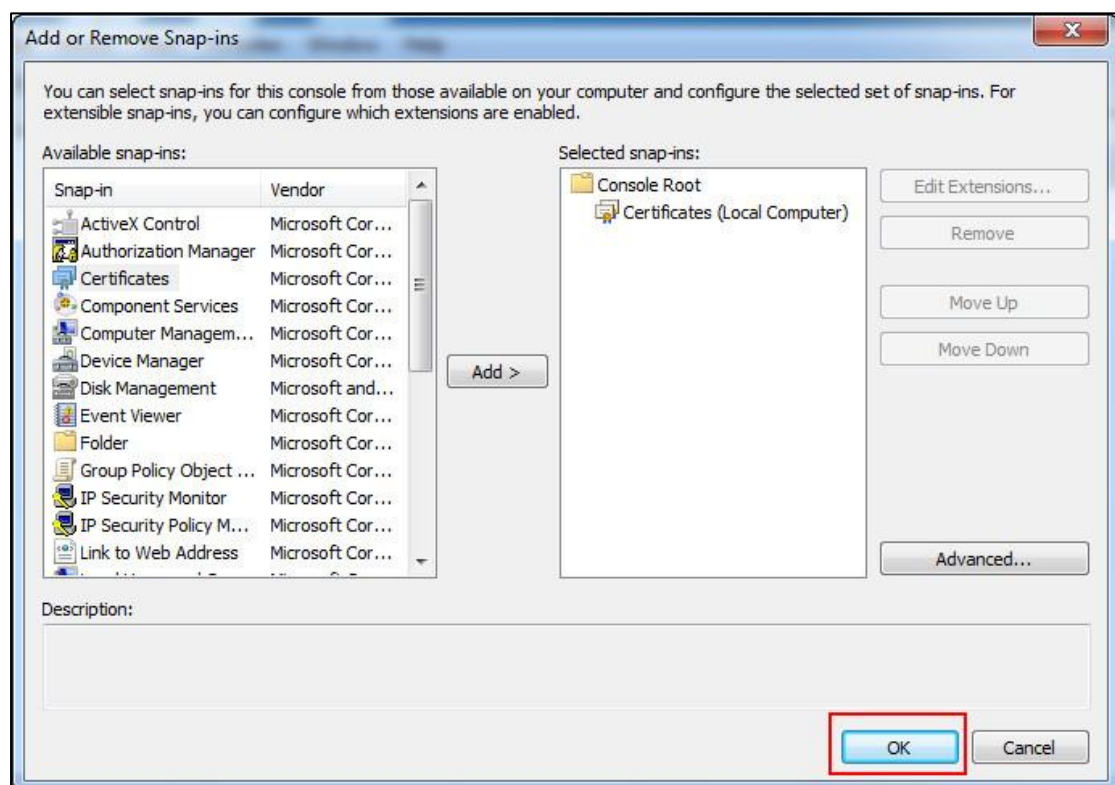
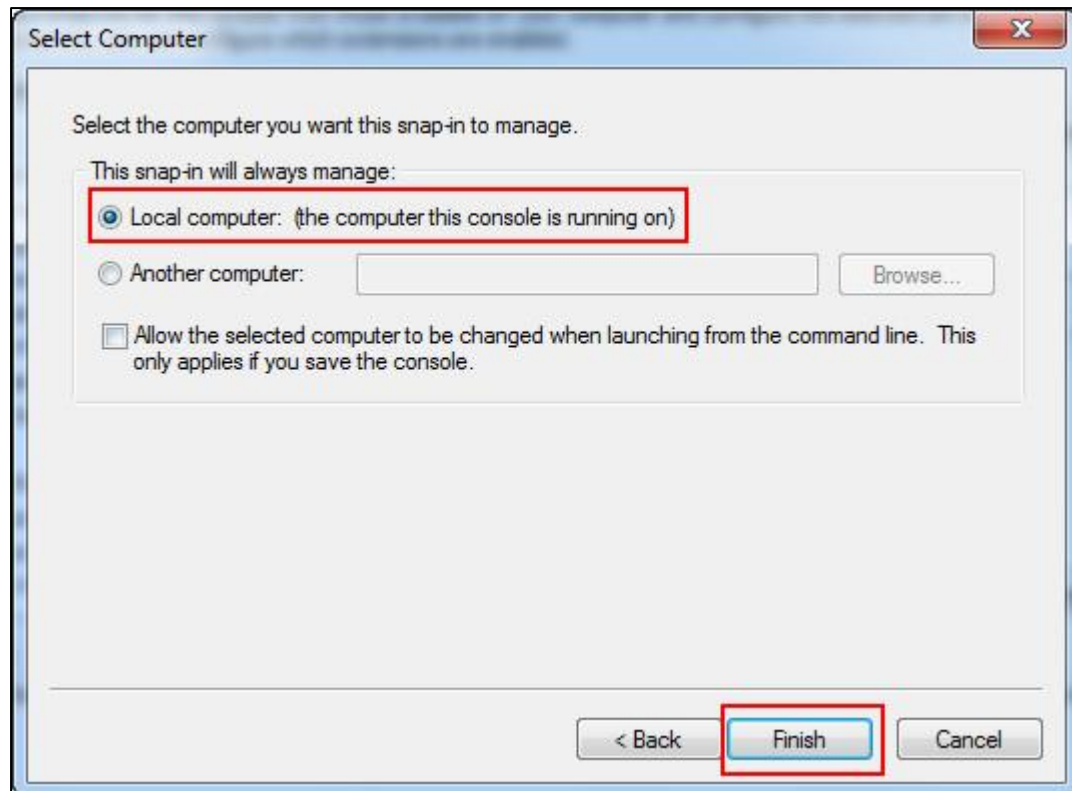


Step 13. In the left panel, select the Certificates and click on the **Add** button.

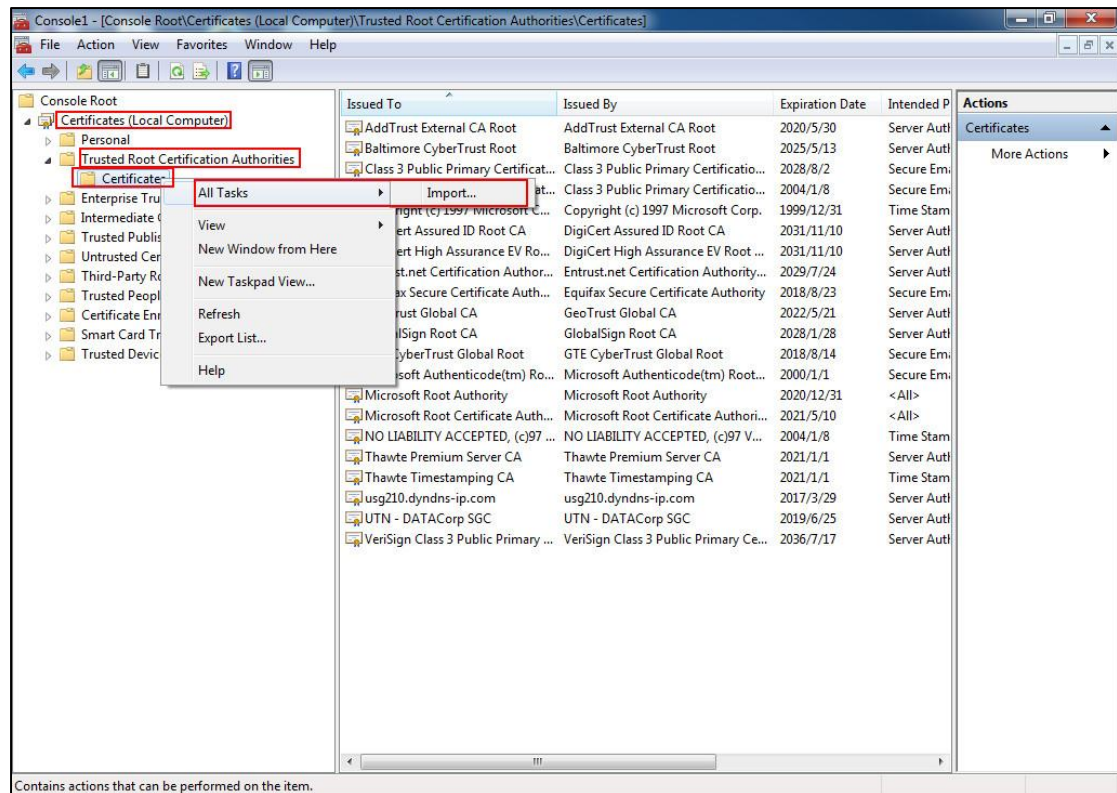


Step 14. Select the **Computer account** > **Next** button > select **Local computer** > **Finish** button > **OK** button.

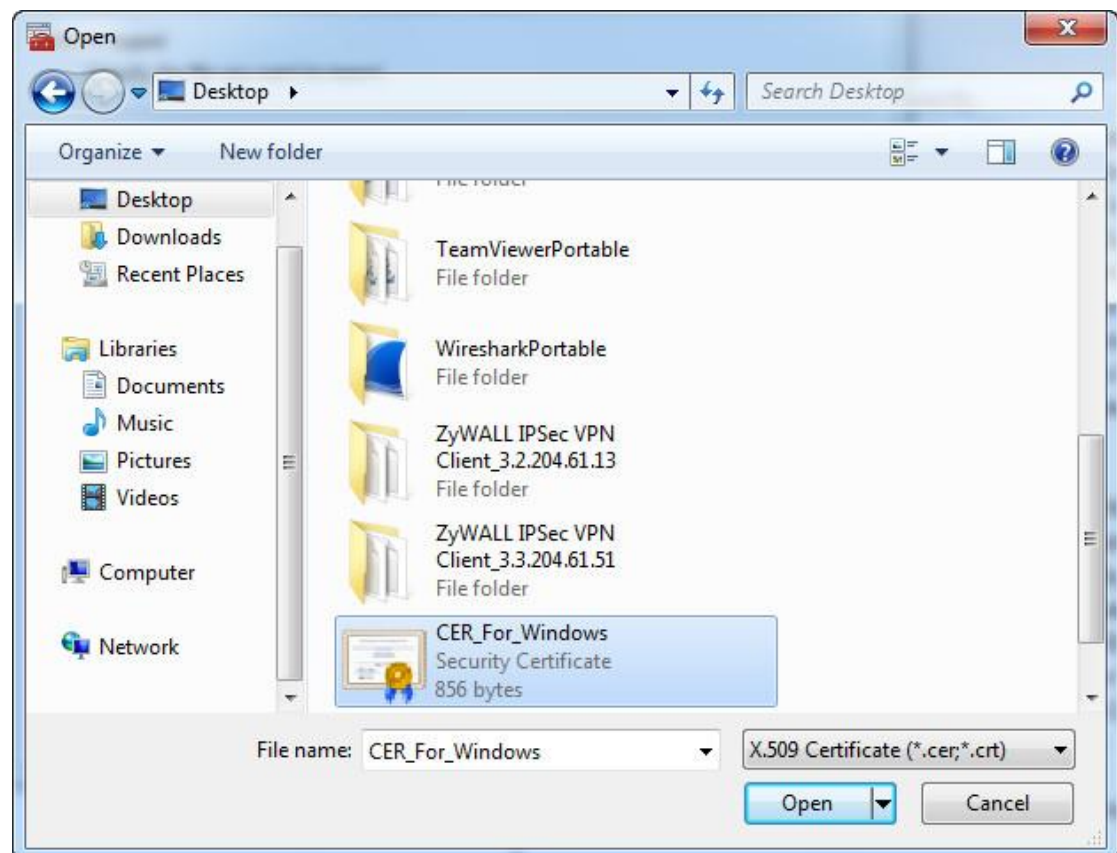




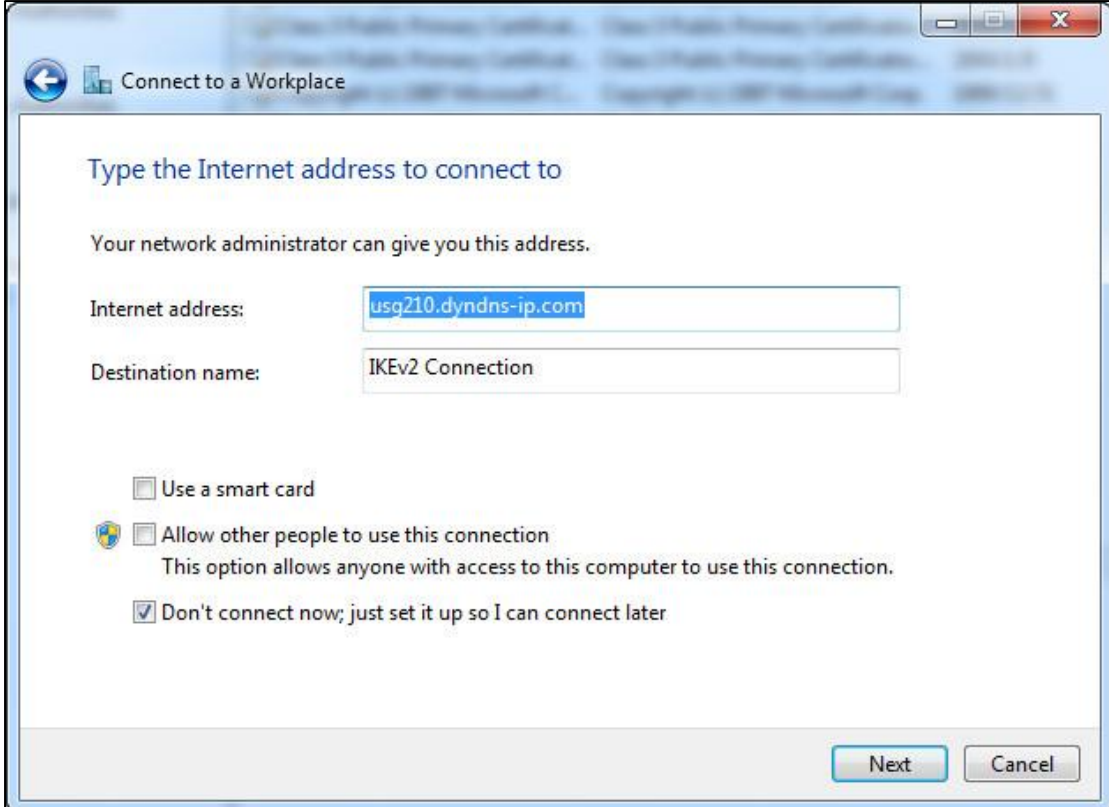
Step 15. Open up the **Certificates (Local Computer) > Trusted Root Certification Authorities > right-click on Certificate > All Tasks > Import.**



Step 16. Select the certificate, which was generated by the USG.



Step 17. Create the Windows IPSec connection profile.



Connect to a Workplace

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address:

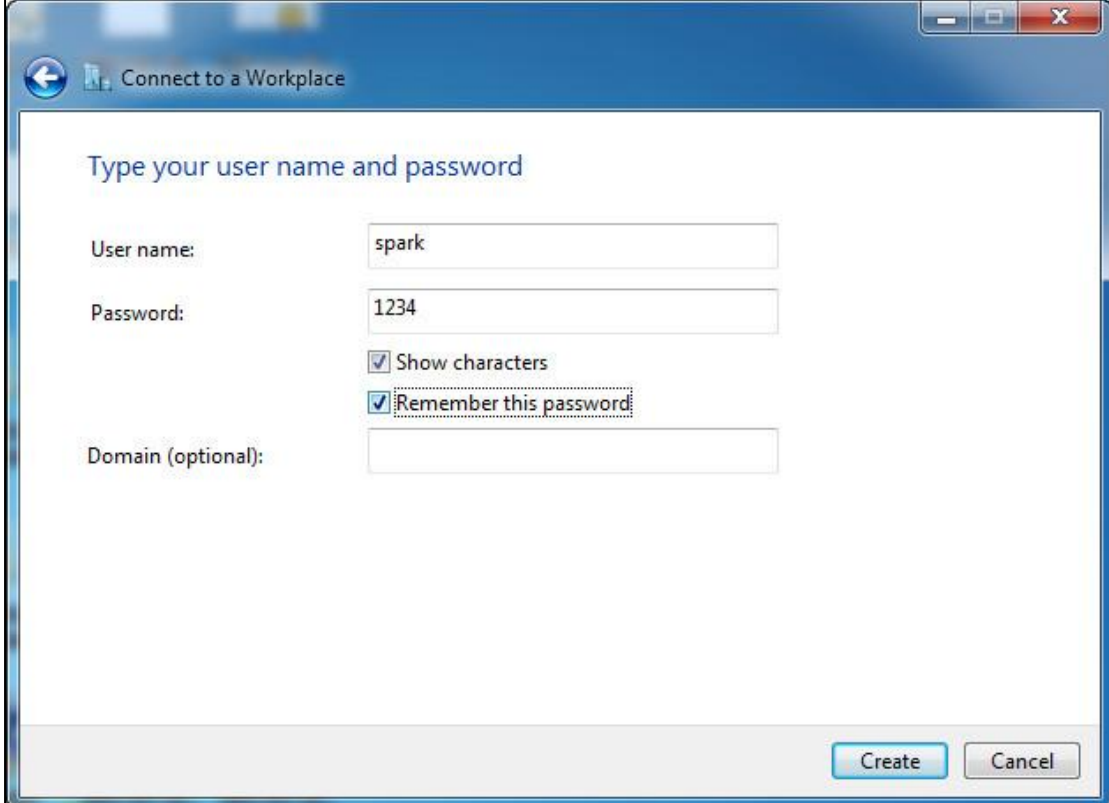
Destination name:

☐ Use a smart card

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☒ Don't connect now; just set it up so I can connect later

Next Cancel



Connect to a Workplace

Type your user name and password

User name:

Password:

☒ Show characters

☒ Remember this password

Domain (optional):

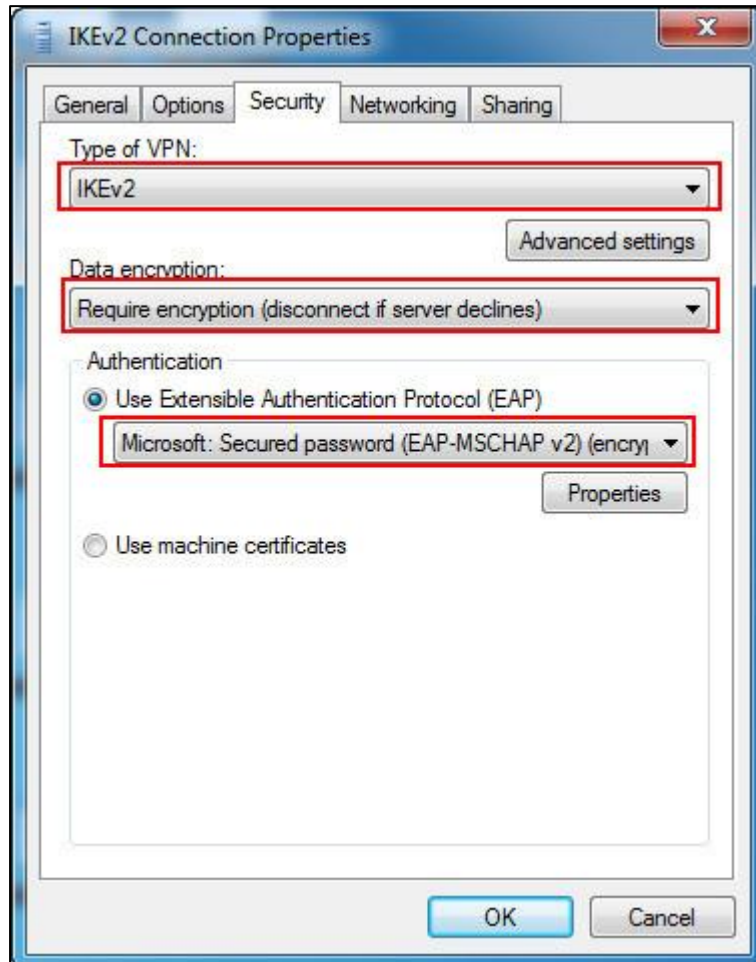
Create Cancel

Step 18. Modify the IPSec connection profile. Go to **Security** >

Type of VPN: IKEv2

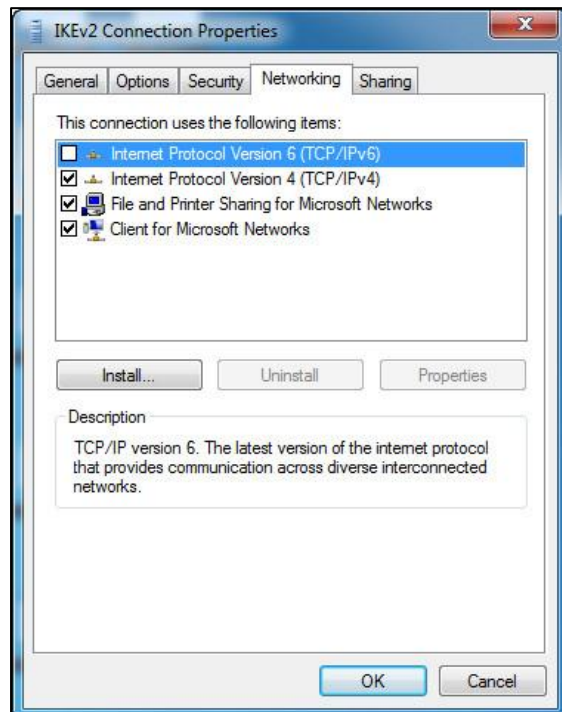
Data encryption: Requires encryption (disconnect if server declines)

Authentication: Use Extensible Authentication Protocol (EAP)

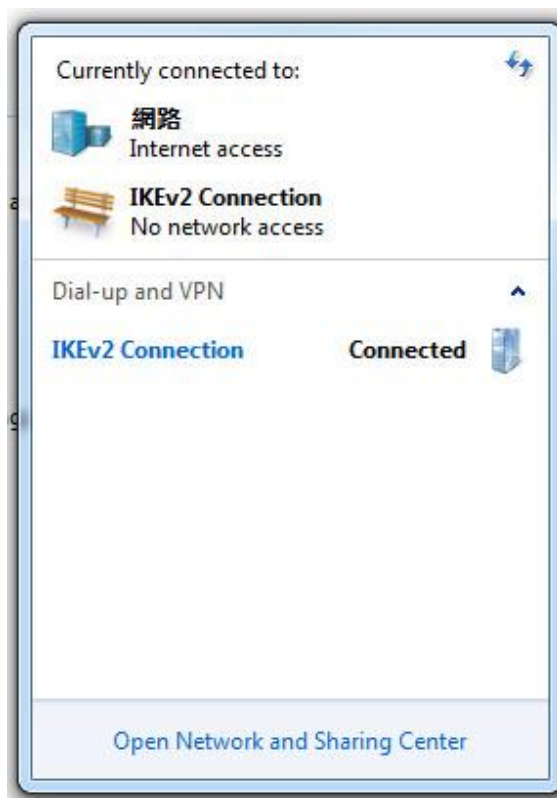


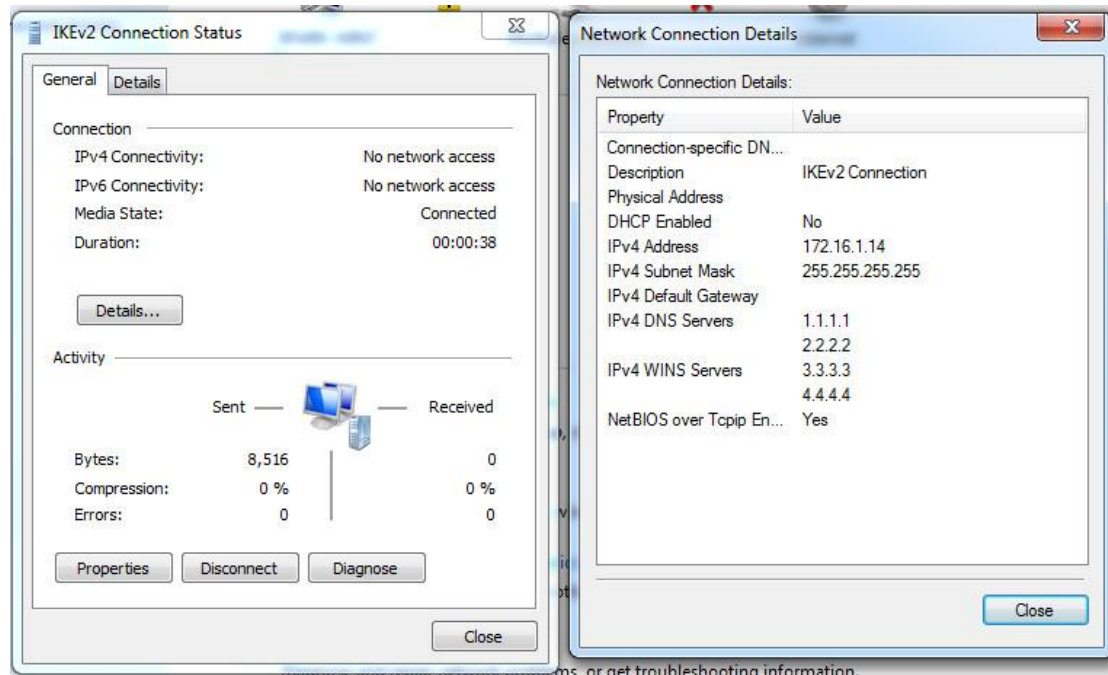
Step 19. Modify IPSec connection profile. Go to **Networking >** and disable the **TCP/IPv6** checkbox.

Note: USG 4.10 firmware does not support multiple proposals. It only supports IPv4 proposal selection.



Step 20. Establish the IPSec tunnel from the Windows 7 machine, and the tunnel will be established successfully.



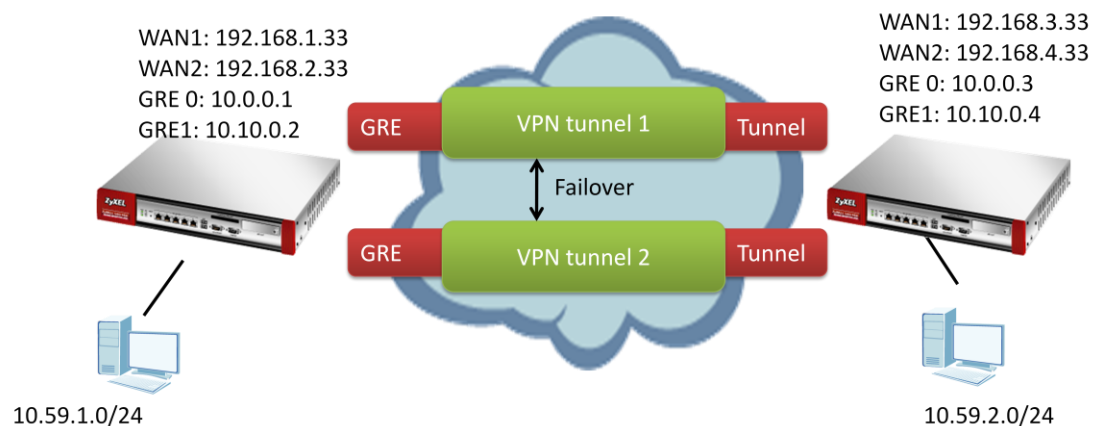


Scenario 6 — GRE over IPsec VPN

Tunnel –VPN Failover

6.1 Application scenario

We want to use VPN tunnels to transfer important files between the branch Office and HQ. To prevent the network from getting disconnected, we configure four WAN interfaces to do redundancy. Now, we want to establish two VPN tunnels between the two USGs to perform failover, to ensure that the transfer will not be interrupted when the first connection encounters a problem. This will create a stable environment for the transfer.



6.2 Configuration Guide

Network conditions:

USG1

- WAN1 IP: 192.168.1.33
- WAN2 IP: 192.168.2.33
- GRE tunnel interface1: 10.0.0.1
- GRE tunnel interface2: 10.10.0.2

USG2

- WAN1 IP: 192.168.3.33
- WAN2 IP: 192.168.4.33
- GRE tunnel interface1: 10.0.0.3
- GRE tunnel interface2: 10.10.0.4

Goals to achieve:

Use GRE over IPsec VPN to perform the VPN fail-over.

USG configuration

Step 1. Add two GRE tunnels on USG1. Go to **CONFIGURATION > Tunnel**.

- a. Add the first tunnel

IP Address: 10.0.0.1, Subnet Mask: 255.255.255.0

My Address: WAN1, Remote Gateway Address: 192.168.3.33

The screenshot shows the 'Edit Tunnel' window with the following settings:

- General Settings:** ☒ Enable
- Interface Properties:**
 - Interface Name: tunnel0
 - Zone: TUNNEL
 - Tunnel Mode: GRE
- IP Address Assignment:**
 - IP Address: 10.0.0.1
 - Subnet Mask: 255.255.255.0
 - Metric: 0 (0-15)
- Gateway Settings:**
 - My Address: ☒ Interface wan1 (DHCP client -- 192.168.1.33/255.255.255.0)
 - ☐ IP Address 0.0.0.0
 - Remote Gateway Address: 192.168.3.33

Place a check in the **Enable Connectivity Check** checkbox. Ensure that the Address is the remote GRE tunnel interface.

The screenshot shows the 'Edit Tunnel' window with the following settings in the 'Connectivity Check' section:

- ☒ Enable Connectivity Check
- Check Method: icmp
- Check Period: 10 (5-600 seconds)
- Check Timeout: 3 (1-10 seconds)
- Check Fail Tolerance: 3 (1-10)
- Check this address: 10.0.0.3 (Domain Name or IP Address)

Below the Connectivity Check section, there are links for 'Related Setting':

- Configure [WAN TRUNK](#)
- Configure [Policy Route](#)

- b. Add the second tunnel

IP Address: 10.10.0.2, Subnet Mask: 255.255.255.0

My Address: WAN2, Remote Gateway Address: 192.168.4.33

Edit Tunnel

Show Advanced Settings

General Settings

☒ Enable

Interface Properties

Interface Name: tunnel1

Zone: TUNNEL

Tunnel Mode: GRE

IP Address Assignment

IP Address: 10.10.0.2

Subnet Mask: 255.255.255.0

Metric: 0 (0-15)

Gateway Settings

My Address

☒ Interface wan2 DHCP client -- 192.168.2.33/255.255.255.0

☐ IP Address 0.0.0.0

Remote Gateway Address: 192.168.4.33

Place a check in the **Enable Connectivity Check** checkbox. Ensure that the Address is the remote GRE tunnel interface.

Edit Tunnel

Show Advanced Settings

Connectivity Check

☒ Enable Connectivity Check

Check Method: icmp

Check Period: 10 (5-600 seconds)

Check Timeout: 3 (1-10 seconds)

Check Fail Tolerance: 3 (1-10)

Check this address: 10.10.0.4 (Domain Name or IP Address)

Related Setting

Configure [WAN TRUNK](#)

Configure [Policy Route](#)

OK Cancel

Step 2. Add a GRE tunnel trunk on USG1. Go to **CONFIGURATION > Network > Interface > Trunk**.
gre_trunk member:
tunnel0: Active
tunnel1: Passive

CONFIGURATION | Port Role | Ethernet | PPP | Cellular | Tunnel | VLAN | Bridge | **Trunk**

Quick Setup | Show Advanced Settings

Configuration

☐ Disconnect Connections Before Falling Back ⓘ

Default WAN Trunk

Default Trunk Selection

☒ SYSTEM_DEFAULT_WAN_TRUNK

☐ User Configured Trunk Please select one ...

User Configuration

➕ Add ✎ Edit 🗑 Remove 🔗 Object Reference

#	Name	Algorithm
1	gre_trunk	

Page 1 of 1 | Show 50 items

Add Trunk

Name:

Load Balancing Algorithm: Least Load First

Load Balancing Index(es): Outbound

➕ Add ✎ Edit 🗑 Remove ↔ Move

#	Member	Mode	Egress Bandwidth
1	tunnel0	Active	1048576 kbps
2	tunnel1	Passive	1048576 kbps

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

Step3. Add two IPSec VPN tunnels on USG1. Go to **CONFIGURATION > VPN > IPSec VPN**.

a. Add two VPN gateway policies.

First VPN Gateway policy (USG1 wan1 to USG2 wan1)

My Address: wan1, Peer Gateway Address: 192.168.3.33

Pre-Shared Key: 12345678

Edit VPN Gateway GRE0_GW

Show Advanced Settings Create new Object ▾

General Settings

☒ Enable

VPN Gateway Name: GRE0_GW

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface wan1 DHCP client -- 192.168.1.33/255.255.255.0

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address Primary 192.168.3.33

Secondary 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

Secondary Gateway policy (USG1 wan2 to USG2 wan2)
 My Address: wan2, Peer Gateway Address: 192.168.4.33
 Pre-Shared Key: 12345678

Edit VPN Gateway GRE1_GW

Show Advanced Settings Create new Object ▾

General Settings

☒ Enable

VPN Gateway Name: GRE1_GW

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface wan2 DHCP client -- 192.168.2.33/255.255.255.0

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address Primary 192.168.4.33

Secondary 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

- b. Add two VPN Connections
- First VPN Connection
- Enable Nailed-Up
- Application Scenario: Site-to-Site
- VPN Gateway: GRE0_GW
- Local policy: 192.168.1.33
- Remote policy: 192.168.3.33

Enable GRE over IPSec

Edit VPN Connection GRE0_Conn

Hide Advanced Settings Create new Object ▾

General Settings

☒ Enable

Connection Name: GRE0_Conn

☒ Nailed-Up

☐ Enable Replay Detection

☐ Enable NetBIOS broadcast over IPSec

MSS Adjustment

☐ Custom Size 0 (200 - 1460 Bytes)

☒ Auto

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: GRE0_GW wan1 192.168.3.33, 0.0.0.0

Edit VPN Connection GRE0_Conn

Hide Advanced Settings Create new Object ▾

Policy

Local policy: local_gre0 HOST, 192.168.1.33

Remote policy: remote_gre0 HOST, 192.168.3.33

☒ Enable GRE over IPSec

☐ Policy Enforcement

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Security (PFS): none

Related Settings

Zone: IPSec_VPN

OK Cancel

Second VPN Connection

Enable Nailed-Up

Application Scenario: Site-to-Site

VPN Gateway: GRE1_GW

Local policy: 192.168.2.33

Remote policy: 192.168.4.33

Enable GRE over IPSec

Edit VPN Connection GRE1_Conn

Hide Advanced Settings Create new Object

General Settings

☒ Enable

Connection Name: GRE1_Conn

☒ Nailed-Up

☐ Enable Replay Detection

☐ Enable NetBIOS broadcast over IPSec

MSS Adjustment

☐ Custom Size 0 (200 - 1460 Bytes)

☒ Auto

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: GRE1_GW wan2 192.168.4.33, 0.0.0.0

Edit VPN Connection GRE1_Conn

Hide Advanced Settings Create new Object

Policy

Local policy: local_gre1 HOST, 192.168.2.33

Remote policy: remote_gre1 HOST, 192.168.4.33

☒ Enable GRE over IPsec

☐ Policy Enforcement

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS): none

Related Settings

Zone: IPSec_VPN

OK Cancel

Step 4. Add a policy routes on USG1. Go to **CONFIGURATION > Network > Routing**.

Source: LAN1_Subnet

Destination: Remote subnet

Next-Hop: gre_trunk

SNAT: none

Add Policy Route [?] [X]

Show Advanced Settings Create new Object ▾

Configuration

☒ Enable

Description: (Optional)

Criteria

User: any ▾

Incoming: any (Excluding ZyWALL) ▾

Source Address: LAN1_SUBNET ▾

Destination Address: remote_11 ▾

DSCP Code: any ▾

Schedule: none ▾

Service: any ▾

Next-Hop

Type: Trunk ▾

Trunk: gre_trunk ▾

OK Cancel

Step5. Add two GRE tunnels on the USG2. **Go to CONFIGURATION > Tunnel.**

a. Add first tunnel

IP Address: 10.0.0.3, Subnet Mask: 255.255.255.0

My Address: WAN1, Remote Gateway Address: 192.168.1.33

Add Tunnel [?] [X]

Show Advanced Settings

General Settings

☒ Enable

Interface Properties

Interface Name: tunnel0

Zone: TUNNEL ▾

Tunnel Mode: GRE ▾

IP Address Assignment

IP Address: 10.0.0.3

Subnet Mask: 255.255.255.0

Metric: 0 (0-15)

Gateway Settings

My Address

☒ Interface wan1 ▾ DHCP client -- 192.168.3.33/255.255.255.0

☐ IP Address 0.0.0.0

Remote Gateway Address: 192.168.1.33

Place a check in the **Enable Connectivity** Check checkbox. Ensure that the Address is the remote GRE tunnel interface.

Add Tunnel [?] [X]

Show Advanced Settings

Egress Bandwidth: 1048576 Kbps

Connectivity Check

☒ Enable Connectivity Check

Check Method: icmp

Check Period: 10 (5-600 seconds)

Check Timeout: 3 (1-10 seconds)

Check Fail Tolerance: 3 (1-10)

Check this address: 10.0.0.1 (Domain Name or IP Address)

Related Setting

Configure [WAN TRUNK](#)

Configure [Policy Route](#)

OK Cancel

b. Add Second tunnel

IP Address: 10.10.0.4, Subnet Mask: 255.255.255.0

My Address: WAN2, Remote Gateway Address: 192.168.2.33

Edit Tunnel [?] [X]

Show Advanced Settings

General Settings

☒ Enable

Interface Properties

Interface Name: tunnel1

Zone: TUNNEL

Tunnel Mode: GRE

IP Address Assignment

IP Address: 10.10.0.4

Subnet Mask: 255.255.255.0

Metric: 0 (0-15)

Gateway Settings

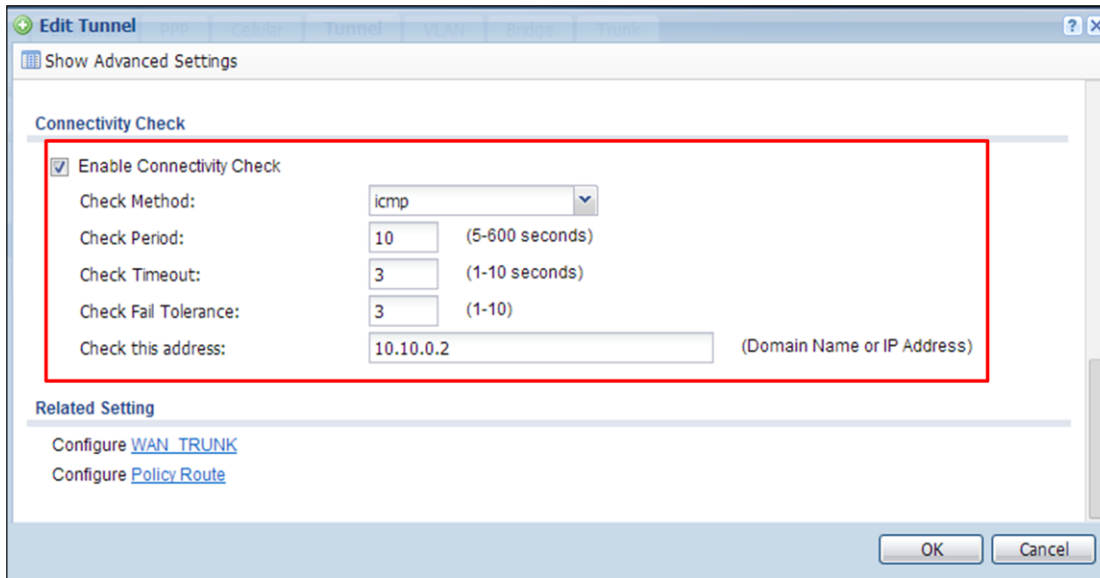
My Address

☒ Interface wan2 DHCP client -- 192.168.4.33/255.255.255.0

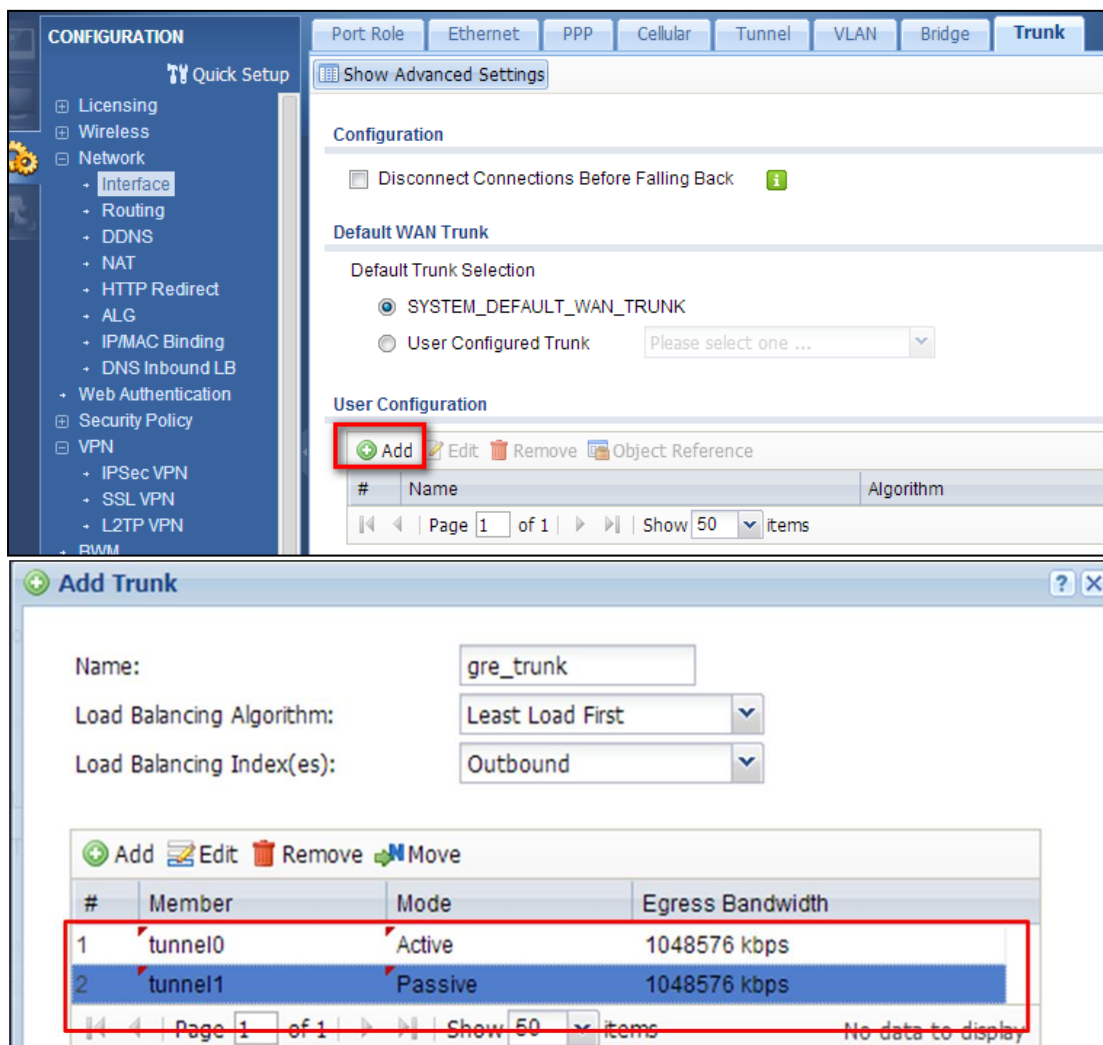
☐ IP Address 0.0.0.0

Remote Gateway Address: 192.168.2.33

Place a check in the **Enable Connectivity** Check checkbox. Ensure that the Address is the remote GRE tunnel interface.



Step6. Add a GRE tunnel trunk on USG2. Go to **CONFIGURATION > Network > Interface > Trunk**.
gre_trunk member:
tunnel0: Active
Tunnel1: Passive



Step 7. Add two IPsec VPN tunnels on USG2. Go to **CONFIGURATION > VPN > IPsec VPN**.

- a. Add two VPN Gateways.

First VPN Gateway

My Address: wan1, Peer Gateway Address: 192.168.1.33

Pre-Shared Key: 12345678

The screenshot shows the 'Add VPN Gateway' configuration window for a gateway named GRE0_GW. The 'Enable' checkbox is checked. Under 'IKE Version', 'IKEv1' is selected. The 'Gateway Settings' section includes 'My Address' set to 'Interface' (wan1) with a DHCP client range of 192.168.3.33/255.255.255.0. The 'Peer Gateway Address' is set to 'Static Address' (Primary) with the value 192.168.1.33. The 'Authentication' section has 'Pre-Shared Key' selected with a masked key. Red boxes highlight the 'My Address', 'Peer Gateway Address', and 'Authentication' sections.

Second VPN Gateway

My Address: wan2, Peer Gateway Address: 192.168.2.33

Pre-Shared Key: 12345678

The screenshot shows the 'Add VPN Gateway' configuration window for a gateway named GRE1_GW. The 'Enable' checkbox is checked. Under 'IKE Version', 'IKEv1' is selected. The 'Gateway Settings' section includes 'My Address' set to 'Interface' (wan2) with a DHCP client range of 192.168.4.33/255.255.255.0. The 'Peer Gateway Address' is set to 'Static Address' (Primary) with the value 192.168.2.33. The 'Authentication' section has 'Pre-Shared Key' selected with a masked key. Red boxes highlight the 'My Address', 'Peer Gateway Address', and 'Authentication' sections.

- b. Add two VPN Connections.

First VPN connection

Application Scenario: Site-to-Site

VPN Gateway: GRE0_GW

Local policy: 192.168.3.33

Remote policy: 192.168.1.33

Enable GRE over IPSec

Edit VPN Connection GRE0_Conn

Hide Advanced Settings Create new Object

General Settings

☒ Enable
Connection Name: GRE0_Conn

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

MSS Adjustment
☐ Custom Size 0 (200 - 1460 Bytes)
☒ Auto

VPN Gateway

Application Scenario
☒ Site-to-site
☐ Site-to-site with Dynamic Peer
☐ Remote Access (Server Role)
☐ Remote Access (Client Role)

VPN Gateway: GRE0_GW wan1 192.168.1.33, 0.0.0.0

Edit VPN Connection GRE0_Conn

Hide Advanced Settings Create new Object

Policy

Local policy: local_gre0 HOST, 192.168.3.33
Remote policy: remote_gre0 HOST, 192.168.1.33

☒ Enable GRE over IPSec
☐ Policy Enforcement

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)
Active Protocol: ESP
Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS): none

Related Settings

Zone: IPSec_VPN

OK Cancel

Second VPN connection

Enable Nailed-Up

Application Scenario: Site-to-Site

VPN Gateway: GRE1_GW

Local policy: 192.168.4.33

Remote policy: 192.168.2.33

Enable GRE over IPSec

Edit VPN Connection GRE1_Conn

Hide Advanced Settings Create new Object

General Settings

☒ Enable

Connection Name: GRE1_Conn

☐ Nailed-Up

☐ Enable Replay Detection

☐ Enable NetBIOS broadcast over IPSec

MSS Adjustment

☐ Custom Size 0 (200 - 1460 Bytes)

☒ Auto

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

VPN Gateway: GRE1_GW wan2 192.168.2.33, 0.0.0.0

Edit VPN Connection GRE1_Conn

Hide Advanced Settings Create new Object

Policy

Local policy: local_gre1 HOST, 192.168.4.33

Remote policy: remote_gre1 HOST, 192.168.2.33

☒ Enable GRE over IPSec

☐ Policy Enforcement

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS): none

Related Settings

Zone: IPSec_VPN

OK Cancel

Step 8. Add a policy routes on USG2. Go to **CONFIGURATION > Network > Routing**.

Source: LAN1_Subnet

Destination: Remote subnet

Next-Hop: gre_trunk

SNAT: none

Add Policy Route [?] [X]

Show Advanced Settings Create new Object ▾

Configuration

☒ Enable

Description: (Optional)

Criteria

User: any ▾

Incoming: any (Excluding ZyWALL) ▾

Source Address: LAN1_SUBNET ▾

Destination Address: remote_10 ▾

DSCP Code: any ▾

Schedule: none ▾

Service: any ▾

Next-Hop

Type: Trunk ▾

Trunk: gre_trunk ▾

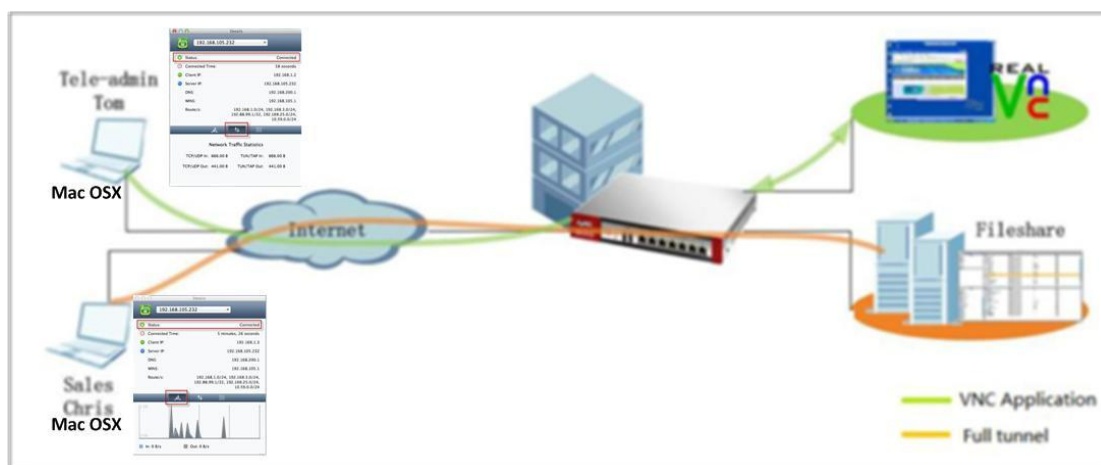
OK Cancel

Scenario 7 - Deploying SSL VPN for Tele-workers to Access Company Resources –SSL VPN with Apple Mac OS X

7.1 Application Scenario

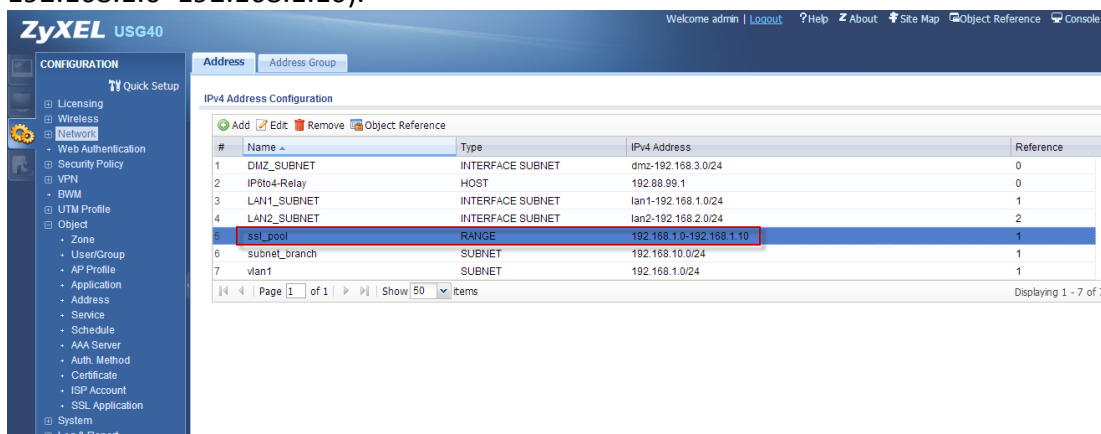
Tele-workers who work away from the office, sometimes need to access company resources in a secured way. USG supports hybrid VPN for client dial-up, and provides an SSL VPN function, which allowing tele-workers to access company resources through a secured VPN tunnel with little effort. All they need on their PC is a browser, and it only requires installation of additional SSL SecuExtender software. Besides, in SSL VPN, the network administrator can define different access rules to allow different users to access different company resources. In the USG 4.10 firmware, we have extended support for SSL VPN with Apple Mac OSX.

For example, the network administrator can configure an SSL VPN rule to allows the administrator to remotely control company servers by RDP or VNC through an SSL VPN tunnel. The administrator can also configure an SSL VPN Full tunnel rule to allow sales people to remotely access company file-share resources to conduct their daily tasks.

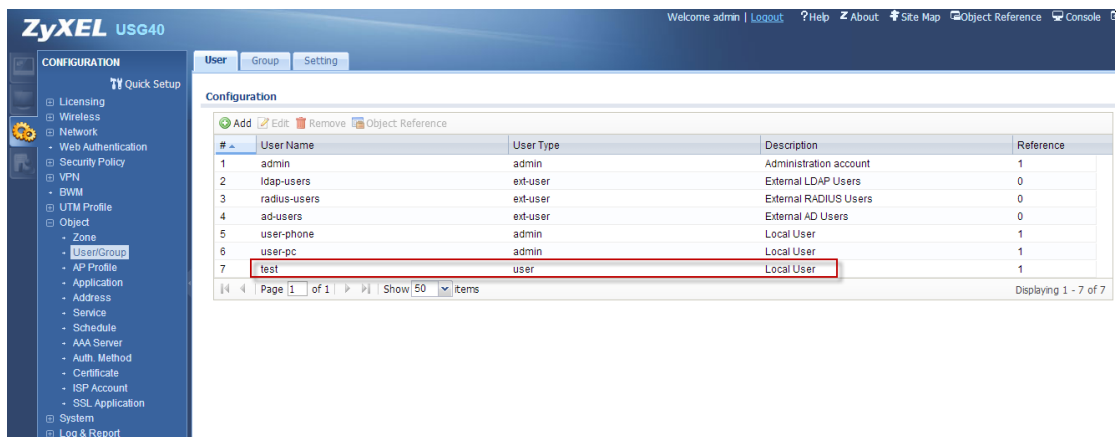


7.2 Configuration Guide

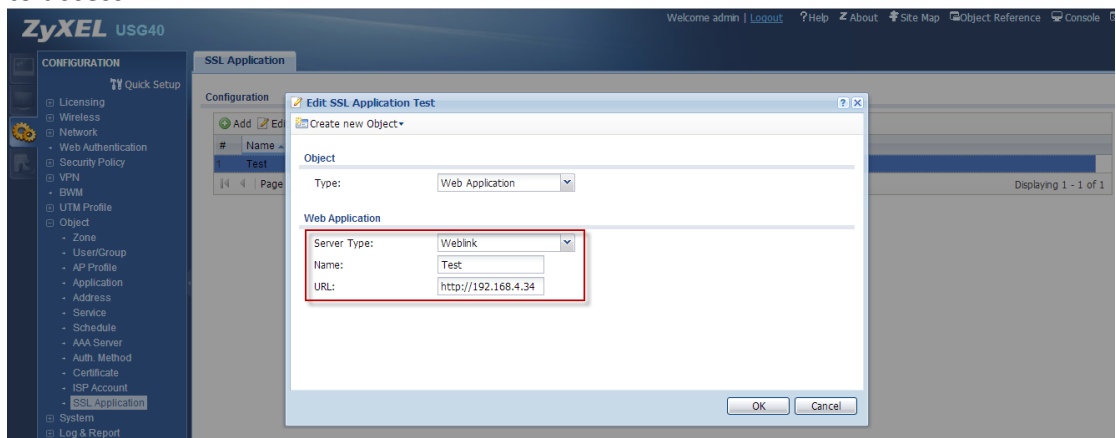
Step 1. Go to **Configuration > Object > Address**, add address object with “ssl_pool” (range 192.168.1.0~192.168.1.10).



Step 2. Go to **Configuration > Object > User/Group**, add an SSL VPN user account, e.g. “test”.

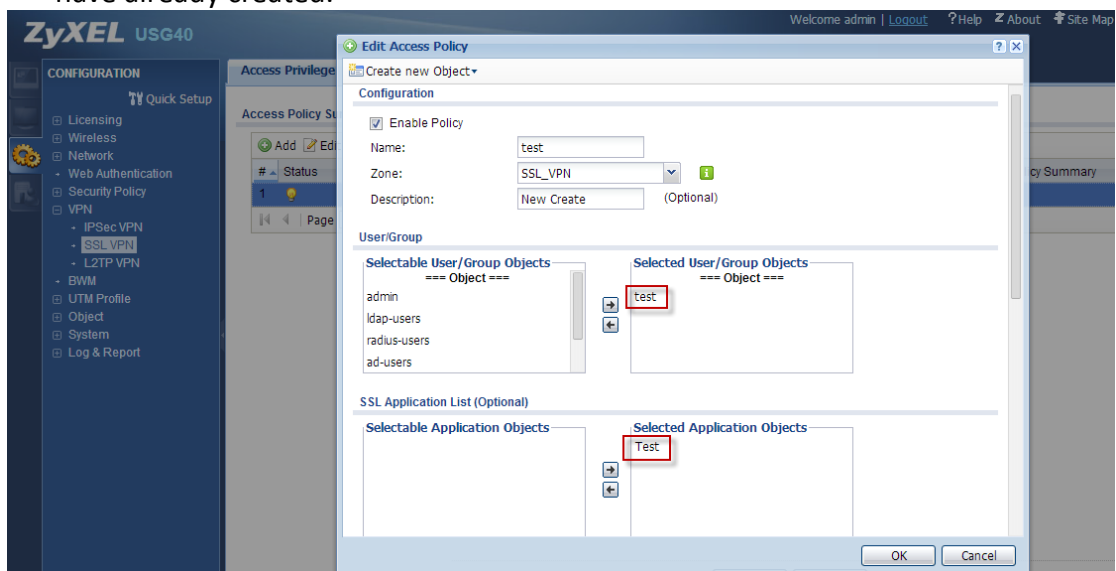


Step 3. Go to **Configuration > Object > SSL Application**, add a web link with the URL for the SSL VPN client to access.



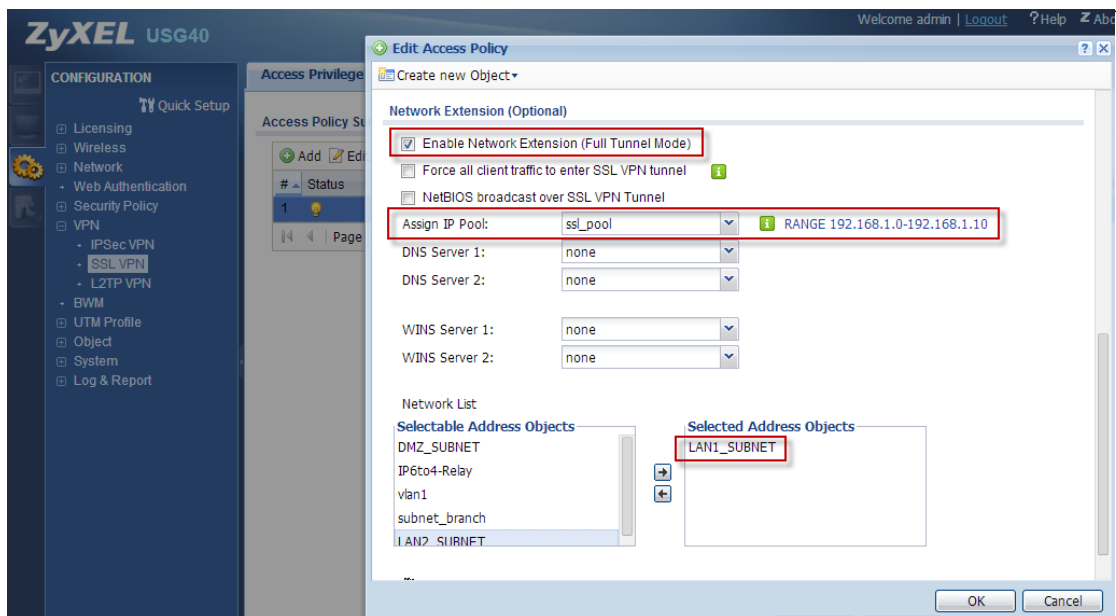
Step 4. Go to **Configuration > VPN > SSL VPN > Access Privilege**

(1) Add one SSL VPN rule and select User/Group Objects with “test” and SSL Application “Test” which you have already created.



(2) Enable **Network Extension (Full Tunnel Mode)**. Choose the **Assign IP pool** with “ssl-pool” which you already create.

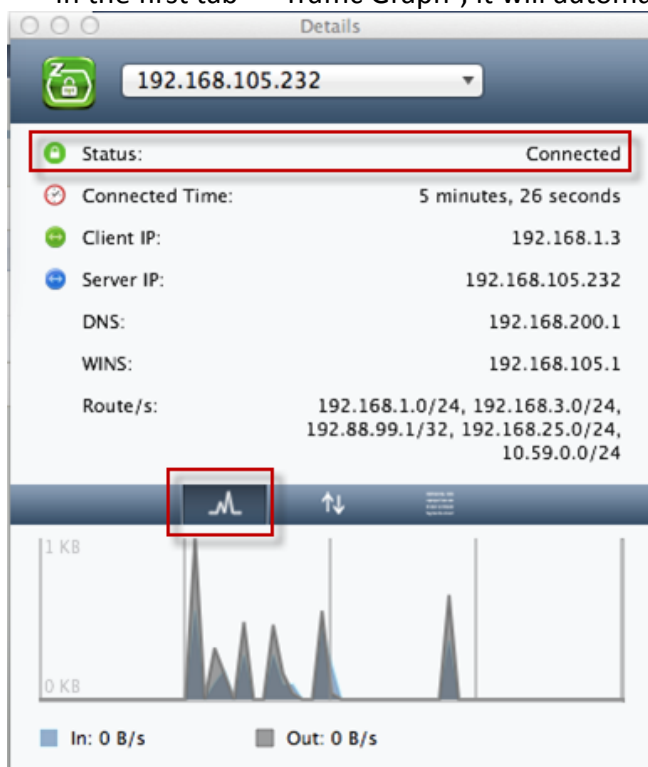
In the **Network List**, selected **LAN1_Subnet**.



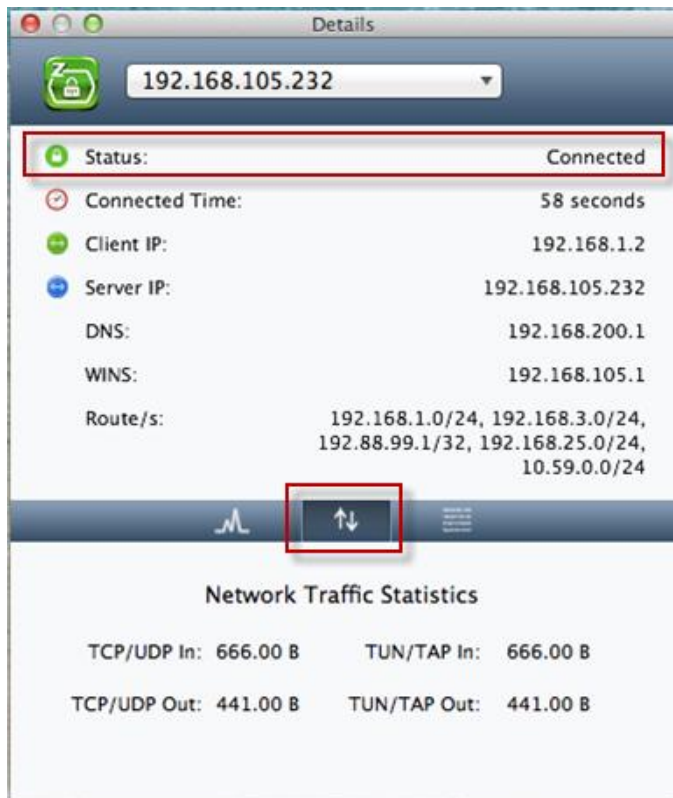
Step 5. Establish an SSL VPN on Apple Mac OS X

- (1) When establishing an SSL VPN on Apple Mac OSX, the Status will become “Connected”, and you can check the IP address information in the details.

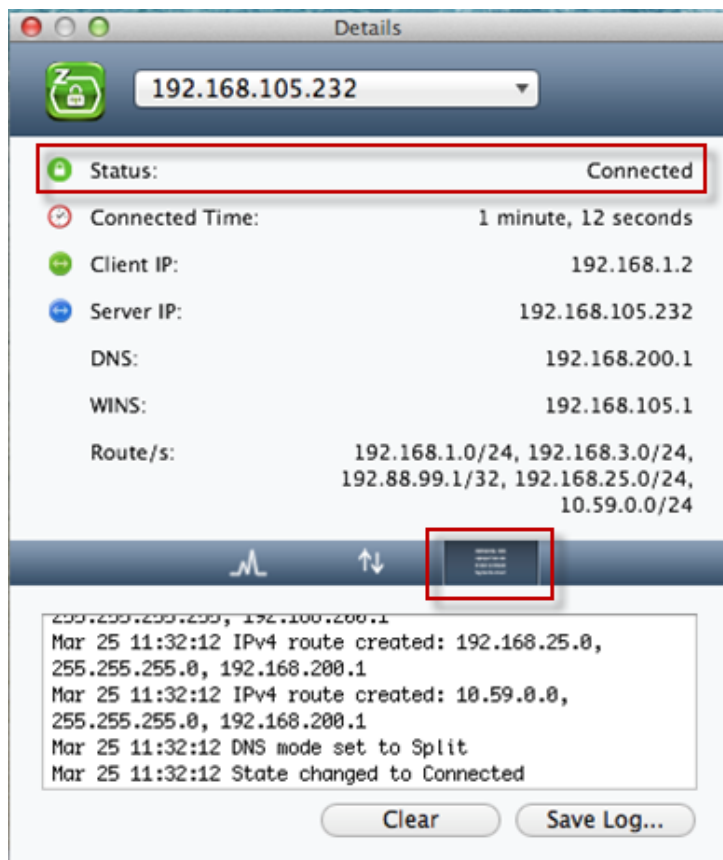
In the first tab – “Traffic Graph”, it will automatically scale to match the maximum traffic rate.



- (2) In the second tab – “Traffic”, lists total data amounts that have passed through the VPN network adapter. These values are reset each time the connection is re-established.



(3) In the third tab – “Log”, the log will contain important information if you are having trouble connecting.

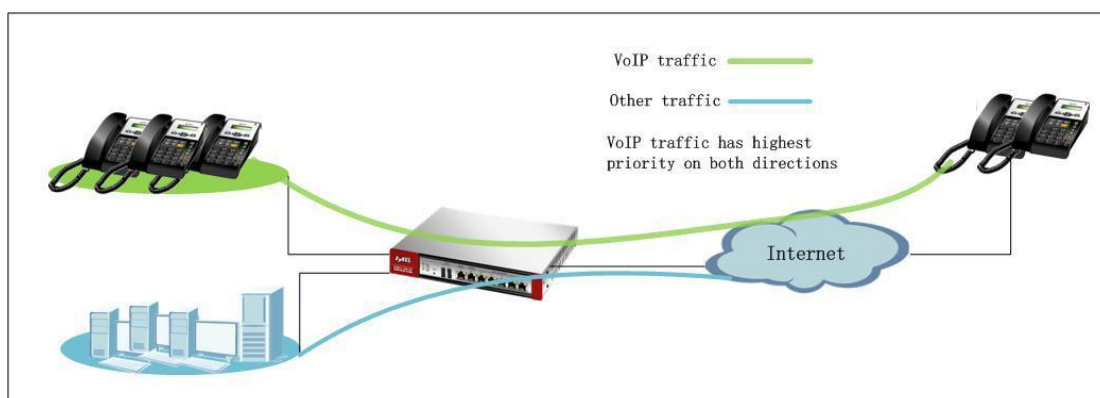


Scenario 8 — Reserving Highest Bandwidth Management Priority for VoIP traffic

8.1 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 USG provides Bandwidth Management (BWM) function to effectively manage bandwidth according to different flexible criteria.

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



8.2 Configuration Guide

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

The screenshot shows the ZyXEL USG40W web interface. The left sidebar contains a 'CONFIGURATION' menu with options like Licensing, Wireless, Network, Interface, Routing, DDNS, NAT, HTTP Redirect, ALG, UPnP, IP/MAC Binding, DNS Inbound LB, Web Authentication, Security Policy, VPN, BWM, UTM Profile, Object, System, and Log & Report. The 'ALG' tab is selected. The main content area shows 'SIP Settings' with the following options:

- ☒ **Enable SIP ALG** (highlighted with a red box)
- ☐ Enable SIP Transformations
- ☒ Enable Configure SIP Inactivity Timeout
 - SIP Media Inactivity Timeout : 120 (seconds)
 - SIP Signaling Inactivity Timeout : 1800 (seconds)
- ☐ Restrict Peer to Peer Signaling Connection
- ☐ Restrict Peer to Peer Media Connection
- SIP Signaling Port :
 - Buttons: Add, Edit, Remove
 - Table:

#	Port
1	5060

Below the SIP Settings, the 'H.323 Settings' section is visible:

- ☐ Enable H.323 ALG
- ☐ Enable H.323 Transformations
- H.323 Signaling Port : 1720 (1025-65535)
- Additional H.323 Signaling Port for Transformations : (1025-65535) (Optional)

Step 2. Go to **Configuration > BWM > enable BWM** and enable **Highest Bandwidth Priority for SIP Traffic > Apply**.

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.

ZyXEL

USG40W

CONFIGURATION

Quick Setup

Licensing

Wireless

Network

Interface

Routing

DDNS

NAT

HTTP Redirect

ALG

UPnP

IP/MAC Binding

DNS Inbound LB

Web Authentication

Security Policy

VPN

BWM

UTM Profile

Object

System

Log & Report

Welcome admin | [Logout](#) | [? Help](#) | [About](#) | [Site Map](#) | [Object Reference](#) | [Console](#) | [CLI](#)

BWM

BWM Global Setting

☒ Enable BWM

☒ Enable Highest Bandwidth Priority for SIP Traffic

Configuration

Add

Edit

Remove

Activate

Inactivate

Move

Status	Prio...	Description	BWM Type	User	Schedule	Incoming Int...	Outgoing Int...	Source	Destination	DSCP...	Service	BWM In/Pri/Out...	DSCP Marking
def...			shared	any	none	any	any	any	any	any	Obj: any	no/7/ino/7	preserve/pr...

Page 1 of 1

Show 50 items

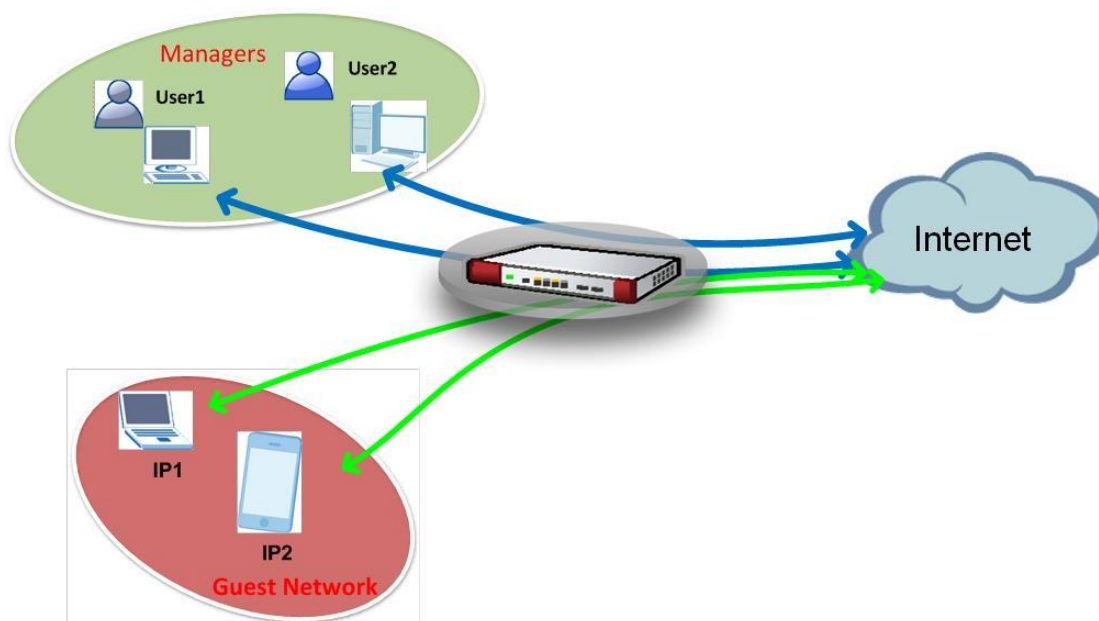
Displaying 1 - 1 of 1

Scenario 9 - Reserving Highest Bandwidth Management Priority for a Superior User and Control Session per Host – BWM Per IP or Per User

9.1 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. Therefore, intelligent bandwidth management for improved productivity becomes a matter of high concern for network administrators. USG provides Bandwidth Management (BWM) function to effectively manage bandwidth according to different flexible criteria.

In the USG 4.10 firmware, we have extended the BWM function for a superior user and control session per host by only adding one rule. Then the USG can control Per IP or Per User to use the limited bandwidth individually. 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 managers need to surf the Internet smoothly to conduct their daily tasks. Therefore, the network administrator should use the bandwidth management function to prioritize the managers' Internet traffic, and guarantee a minimum bandwidth for their own traffic by IP address or by user account.



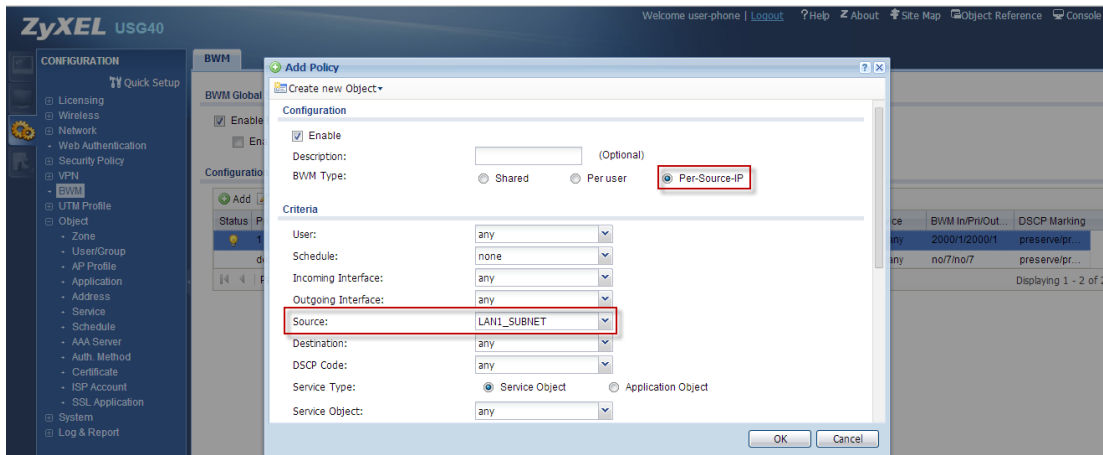
9.2 Configuration Guide

BWM Per IP

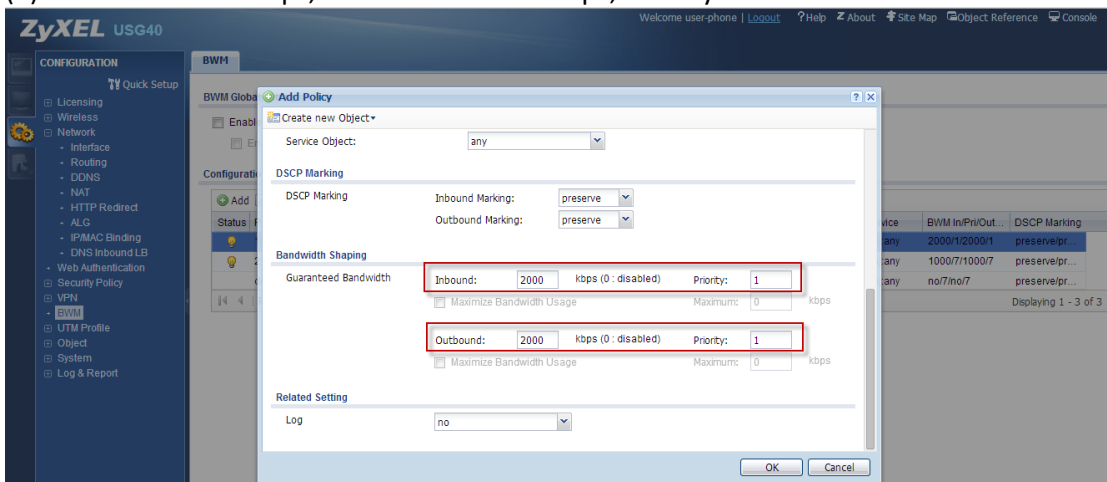
Step 1. Go to **Configuration > BWM** > add the policy to limit the Bandwidth by BWM type –Per-Source-IP.

(1) BWM Type : Per-Source-IP, Source: LAN1_SUBNET

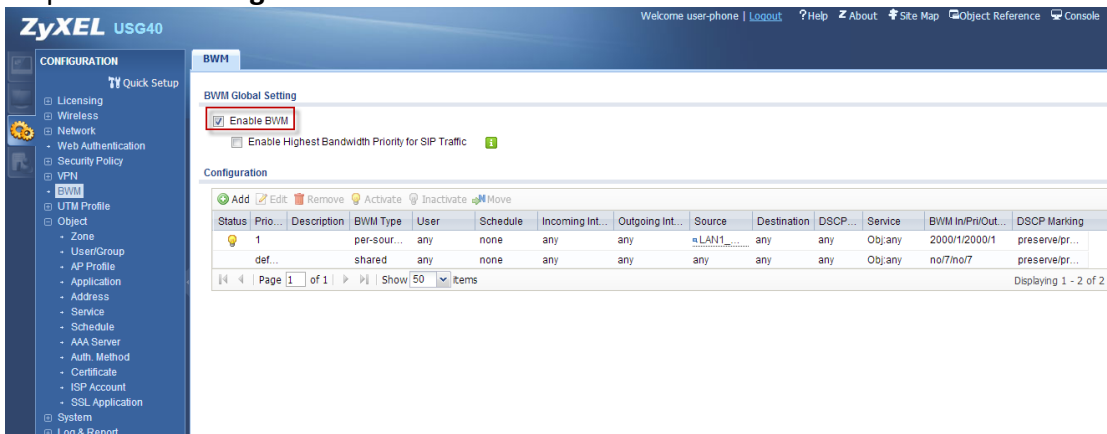
Note: Object source IP address must belong to class C range which amount can't over 256 users.



(2) Inbound = 2000Kbps, Out bound = 2000Kbps, Priority = 1



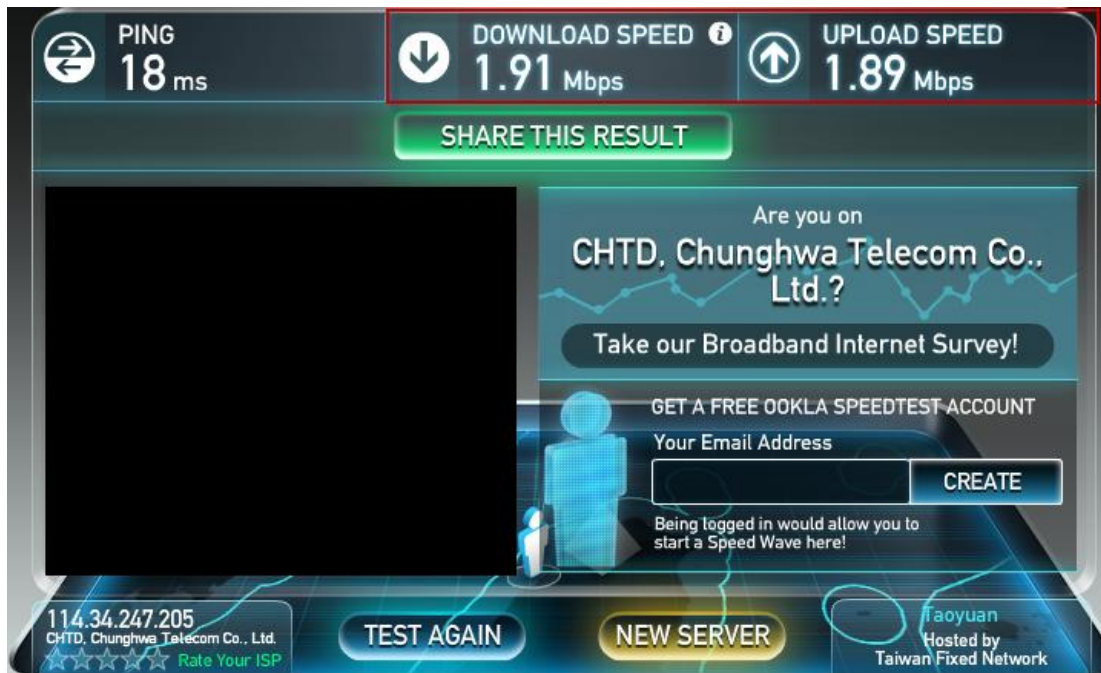
Step 2. Go to **Configuration > BWM > Enable BWM function.**



Step 3. Use the PC's IP address of "192.168.1.33" to connect to the USG.

Visit the website <http://www.speedtest.net/> to test the speed.

The test result is around 2 Mbps, which is the same as our setup to manage per source IP 2 Mbps.



Step 4. Use the PC's IP address of "192.168.1.40" to connect to the USG.

Visit the website <http://www.speedtest.net/> to test the speed.

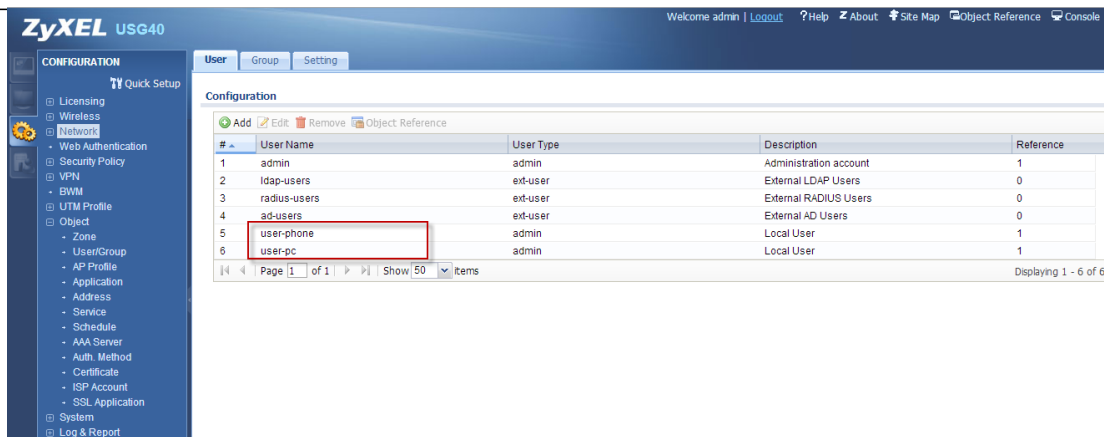
The test result is around 2 Mbps, which is the same as our setup to manage per source IP 2 Mbps.



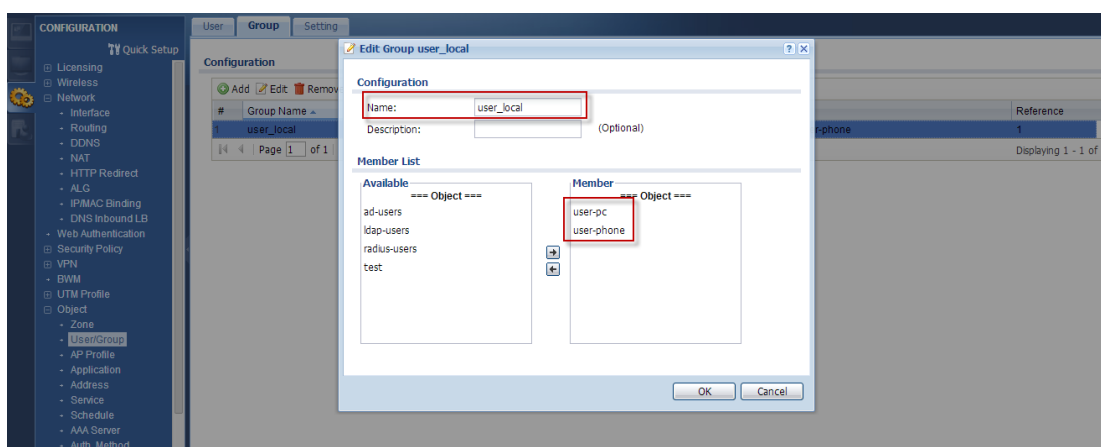
BWM Per User-

Step 1. Go to **Configuration > Object > User/Group**.

(1) Add one user name as "user-phone", and add another user name as "user-pc".

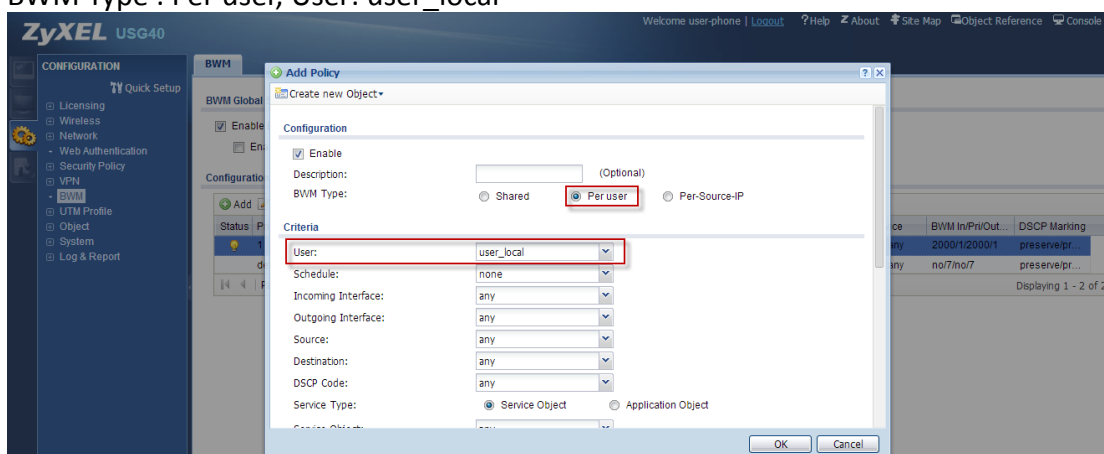


(2) Add these two accounts “user-phone” and “user-pc” into the group as “user_local”.

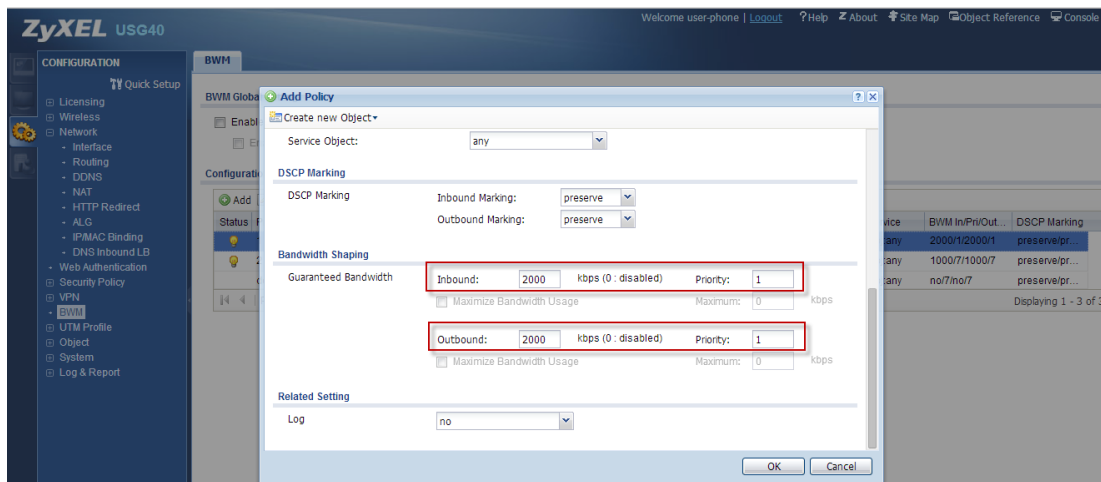


Step 2. Go to **Configuration > BWM > Add the policy to limit the Bandwidth by BWM type – Per user.**

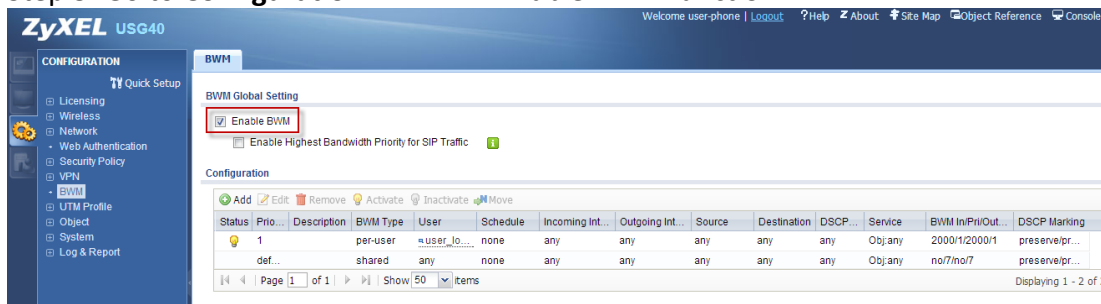
(1) BWM Type : Per user, User: user_local



(2) Inbound=2000Kbps, Out bound=2000Kbps, Priority =1

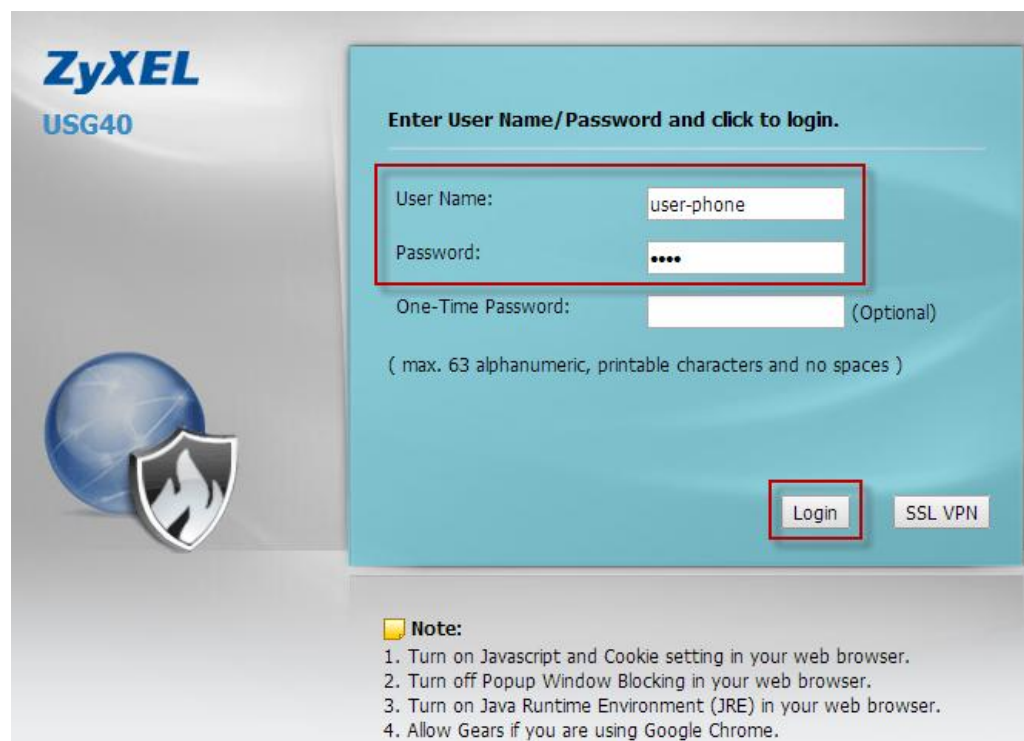


Step 3. Go to **Configuration > BWM > Enable BWM function.**




Step 4. Verify with the “user-phone” account.


(1) Enter the “user-phone” user name and password and Login.



(2) Visit the website “ <http://www.speedtest.net/> ” to test the speed.

The test result is around 2 Mbps, which is the same as our setup to manage per user 2 Mbps.

**PING**
18 ms

**DOWNLOAD SPEED**
1.90 Mbps

**UPLOAD SPEED**
1.90 Mbps

SHARE THIS RESULT

Are you on
CHTD, Chunghwa Telecom Co., Ltd.?

Take our Broadband Internet Survey!

GET A FREE OOKLA SPEEDTEST-ACCOUNT

Your Email Address

CREATE

Being logged in would allow you to start a Speed Wave here!

114.34.247.205
CHTD, Chunghwa Telecom Co., Ltd.
☆☆☆☆☆ Rate Your ISP

TEST AGAIN

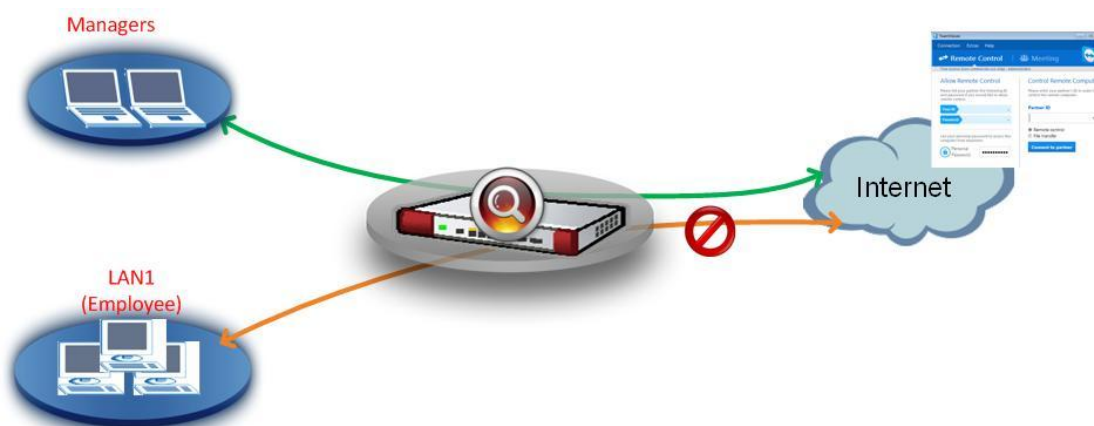
NEW SERVER

Taoyuan
Hosted by
Taiwan Fixed Network

Scenario 10 - Using USG to Control Popular Applications –APP Patrol

10.1 Application Scenario

In the company, the network administrator will need to control access to the Internet for internal managers and employees. The USG's Application Patrol function can take corresponding actions according to the configuration in App Patrol. For example, if the general managers need to execute the Teamviewer application to access the customer's side to conduct their daily work, then the network administrator can use the Firewall to drop other employee that are not allowed to use this type of application, and allow only managers to execute Teamviewer application.

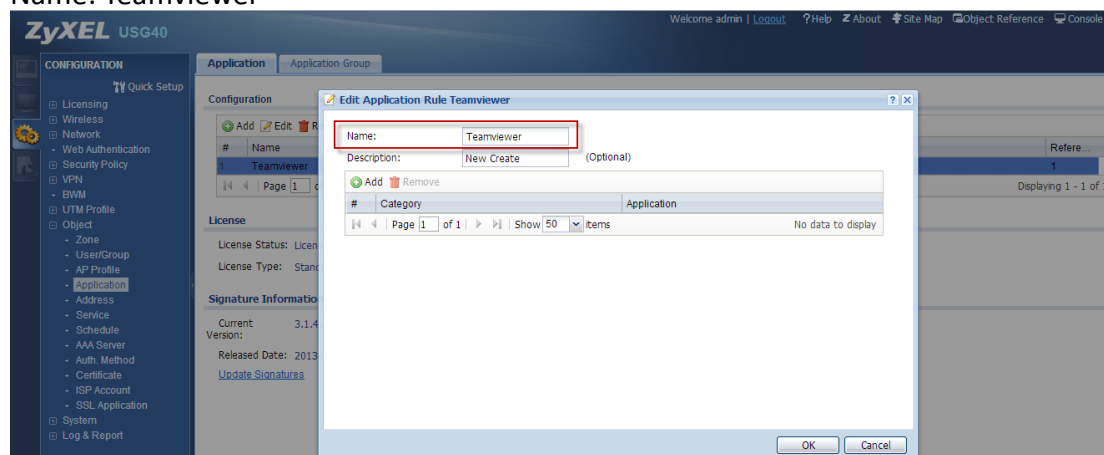


10.2 Configuration Guide

Step 1. Go to **Configuration > Object > Application > Add Application Rule**

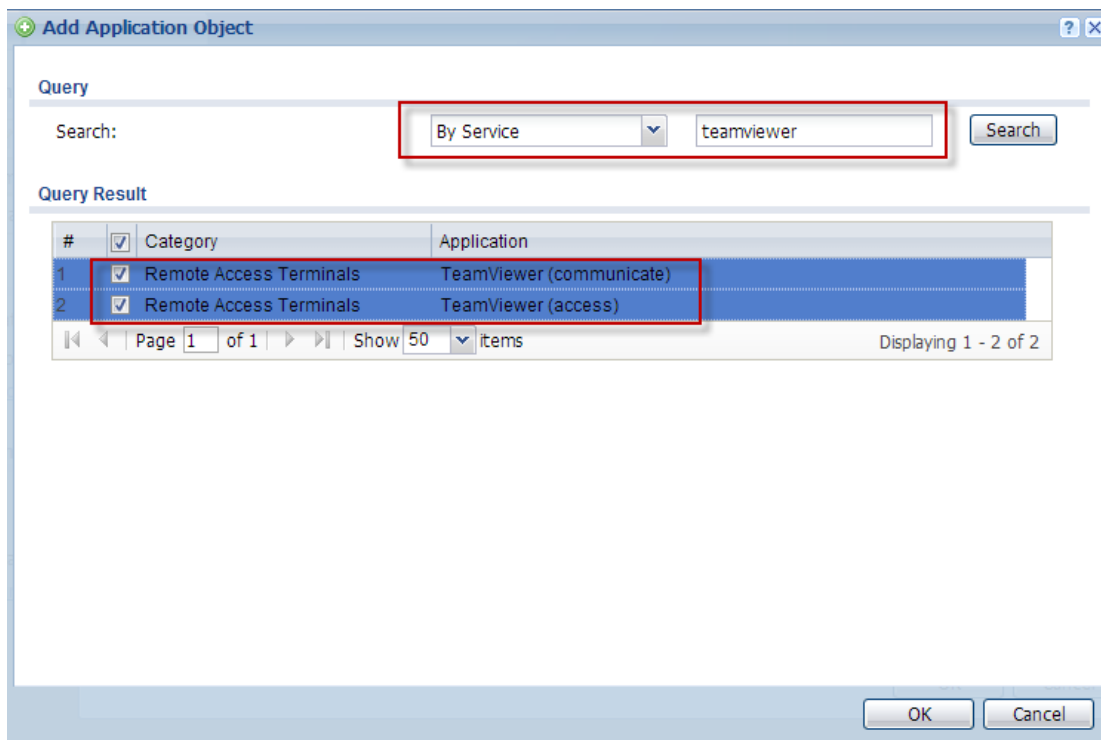
For example

Name: Teamviewer

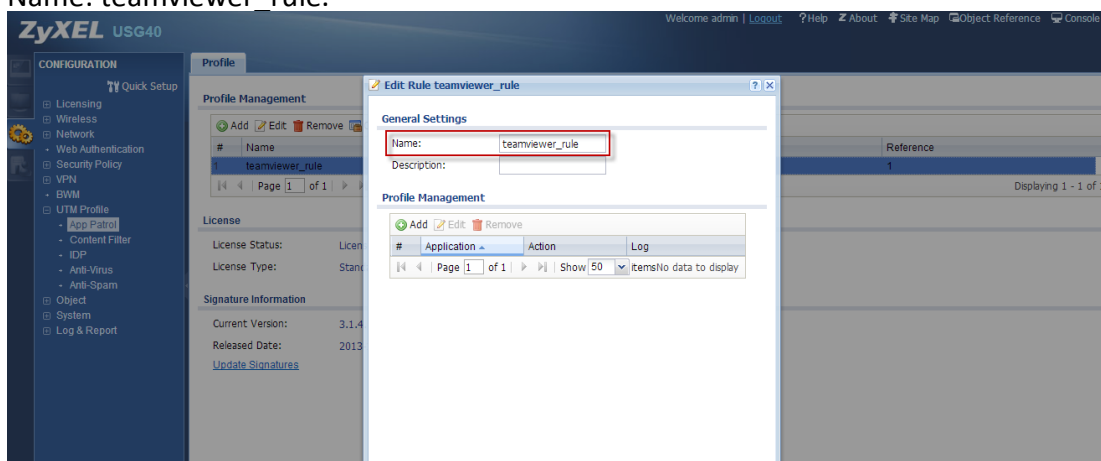


NOTE: You need to register the IDP/App Patrol license to use App Patrol.

Step 2. Please add **Application Object > Search By Service > insert "teamviewer"** > select all to control all teamviewer applications > and then click on the **OK** button.



Step 3. Go to **Configuration > UTM Profile > App Patrol > Profile > Add rule**
 For example
 Name: teamviewer_rule.



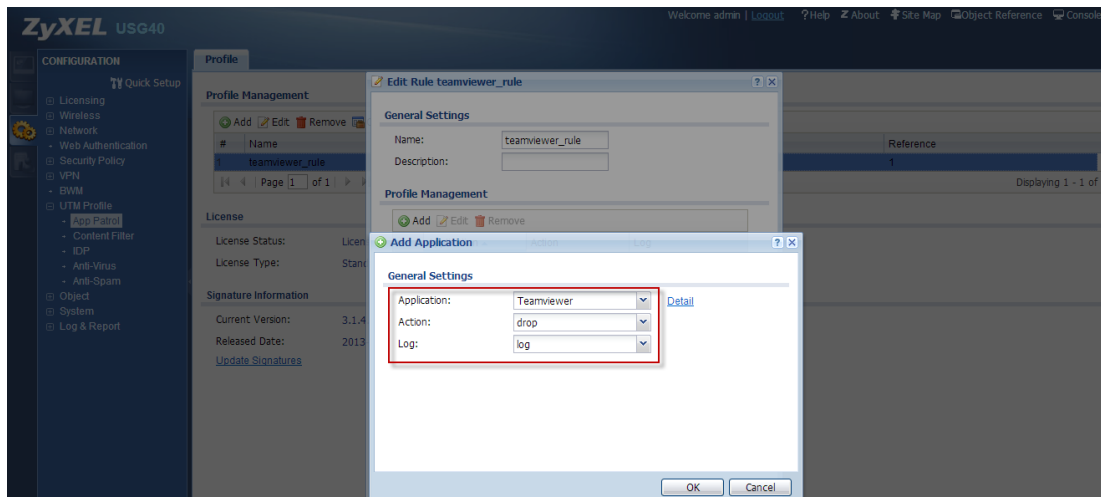
Step 4. Go to **Profile Management > Add Application**

For example

Application: choose the application object of "Teamviewer" which you have already created.

Action: drop

Log: log > ok.



Step 5. Go to **Configuration > Security policy > Policy Control > Policy > Add corresponding > Enable rule**

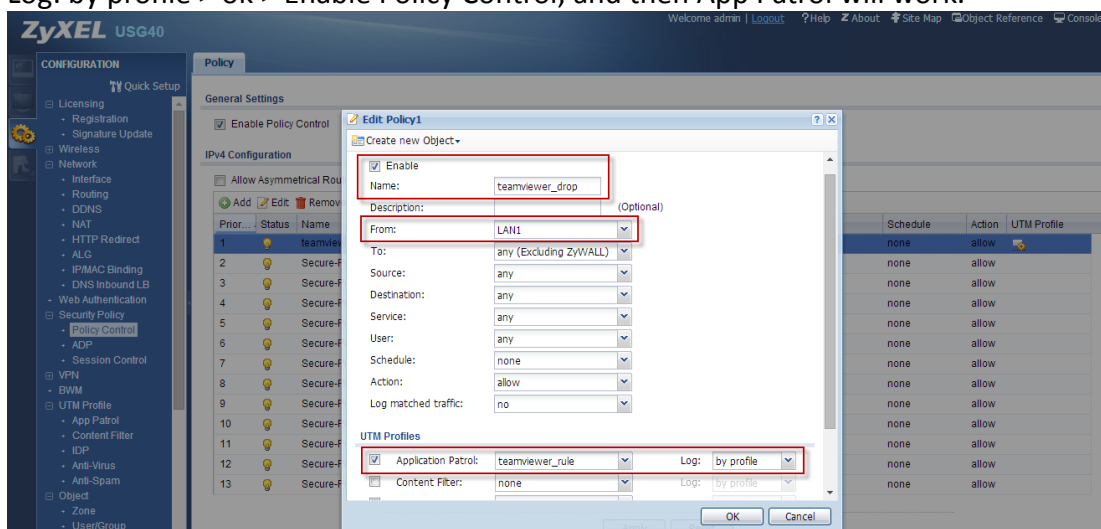
For example

Name: teamviewer_drop

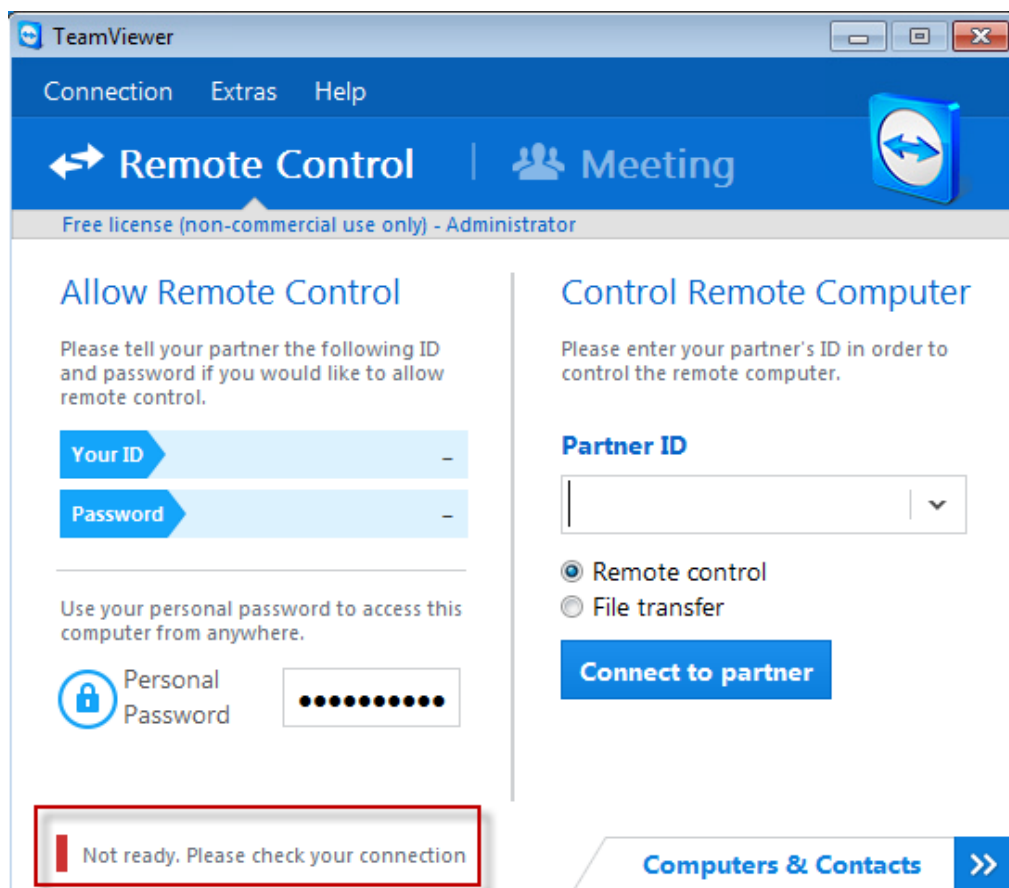
From: LAN1

UTM Profiles: Enable Application Patrol: choose the application profile of “teamviewer_rule” which you have already created.

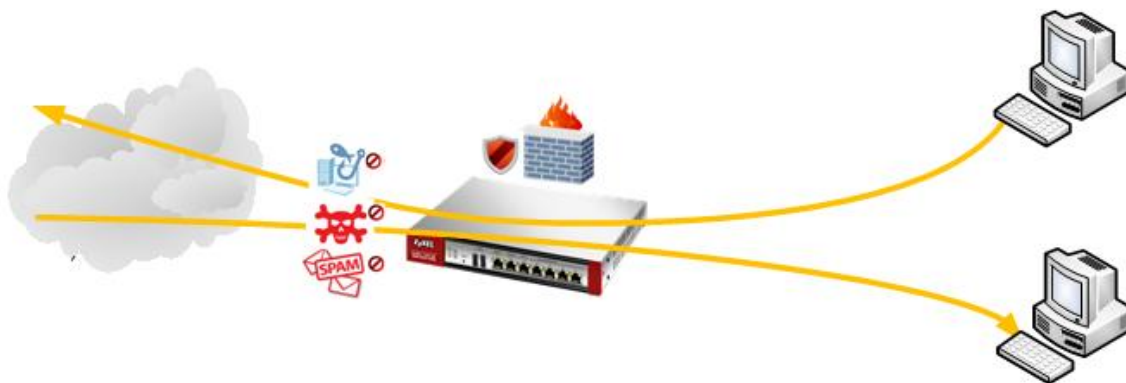
Log: by profile > ok > Enable Policy Control, and then App Patrol will work.



Step 6. Connect to the PC under USG LAN1, then teamviewer application will not open.
But from other interface can, it can open.



Scenario 11 – Configure Unified Policy (Firewall Policy + UTM Profile)



Introduction:

The unified policy is merging with firewall rule and UTM functions. The flow will check the firewall rule first, and then check the UTM function. If the packets are already dropped by the firewall rule, then it will not check the UTM rule any more. The behavior of policy control is to check for the Initiator source IP address. For example, if you would like to block LAN1 users from downloading file from the Internet, then you should block From: LAN, To: WAN, Service: FTP, Action: deny.

If the packets are already dropped by the firewall rule, then it will not check the UTM rule any more.

Add corresponding	
Create new Object	
<input checked="" type="checkbox"/> Enable	
Name:	test
Description:	(Optional)
From:	LAN1
To:	WAN
Source:	any
Destination:	any
Service:	any
User:	any
Schedule:	none
Action:	deny
Log denied traffic:	no

If the packets are allowed by the firewall rule, then you can select the UTM profile to control sessions.

Add corresponding

Create new Object

☒ Enable

Name: test

Description: (Optional)

From: LAN1

To: WAN

Source: any

Destination: any

Service: any

User: any

Schedule: none

Action: allow

Log matched traffic: no

UTM Profile

<input type="checkbox"/> Application Patrol:	none	Log: by profile
<input type="checkbox"/> Content Filter:	none	Log: by profile
<input type="checkbox"/> IDP:	none	Log: by profile
<input type="checkbox"/> Anti-Virus:	none	Log: by profile
<input type="checkbox"/> Anti-Spam:	none	Log: by profile
<input type="checkbox"/> SSL Inspection:	none	Log: by profile

Apply OK Cancel

11.1 Application Scenario

The customer wants to block Skype and all social networks in LAN1.



11.2 Configuration Guide

(1) Add a Skype object in Application.

Go to **Configuration > Object > Application**, and click on the “Add” button.

ZyXEL USG210

Welcome admin | Logout | Help | About | Site Map | Object Reference

CONFIGURATION

Quick Setup

- HTTP Redirect
- ALG
- UPnP
- IP/MAC Binding
- DNS Inbound LB
- Web Authentication
- Security Policy
 - Policy Control
 - ADP
 - Session Control
- VPN
- BWM
- UTM Profile
- Device HA
- Object
 - Zone
 - User/Group
 - AP Profile
 - Application**
 - Address
 - Service
 - Schedule
 - AAA Server
 - Auth. Method
 - Certificate
 - ISP Account
 - SSL Application
- System

Application Application Group

Configuration

Add Edit Remove Object Reference

#	Name	Description
1	skype	New Create

Page 1 of 1 Show 50

License

License Status: Licensed

License Type: Standard

Signature Information

Current: 3.1.4.073

Version:

Released Date: 2014-02-27 09:26:47

Update Signatures

Edit Application Rule skype

Name: skype

Description: New Create (Optional)

Add Remove

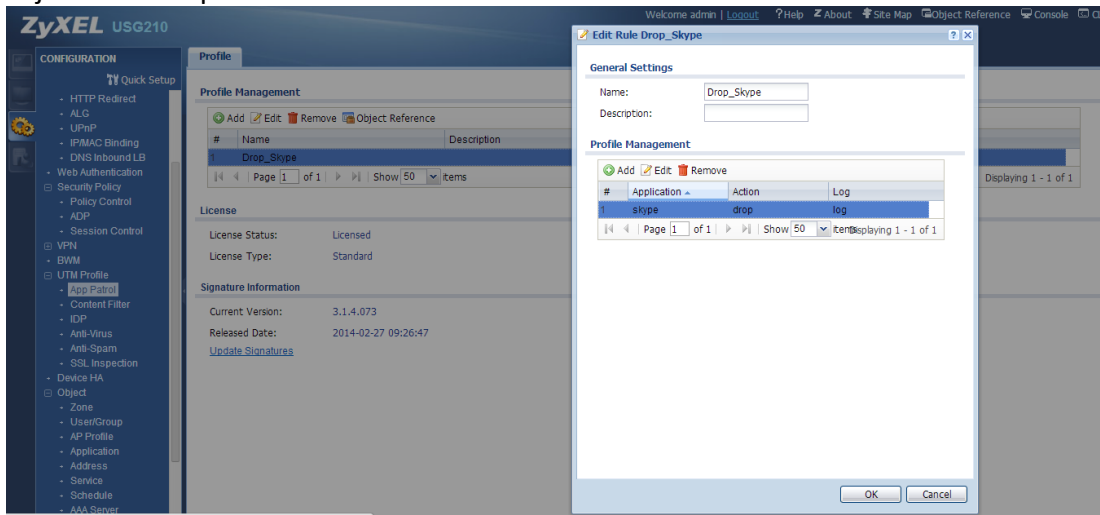
#	Category	Application
1	Voice over IP	Skype (authority)
2	Voice over IP	Skype (media)
3	Voice over IP	Skype (connect)

Page 1 of 1 Show 50 Items Displaying 1 - 3 of 3

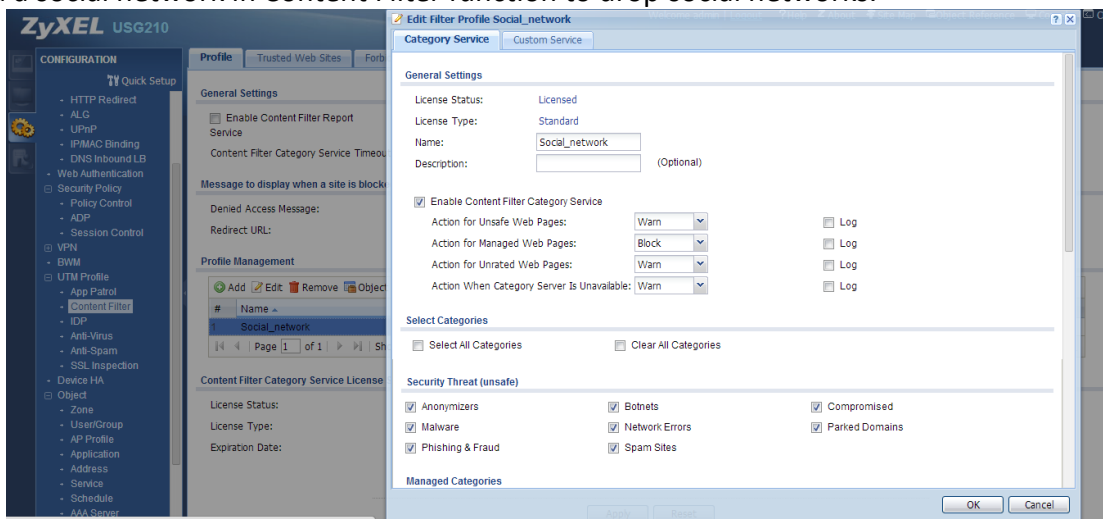
OK Cancel

(2) Add to the App Patrol profile

Go to **Configuration > UTM profile > App Patrol**, and click on the **“Add”** button to add the application object into the profile.

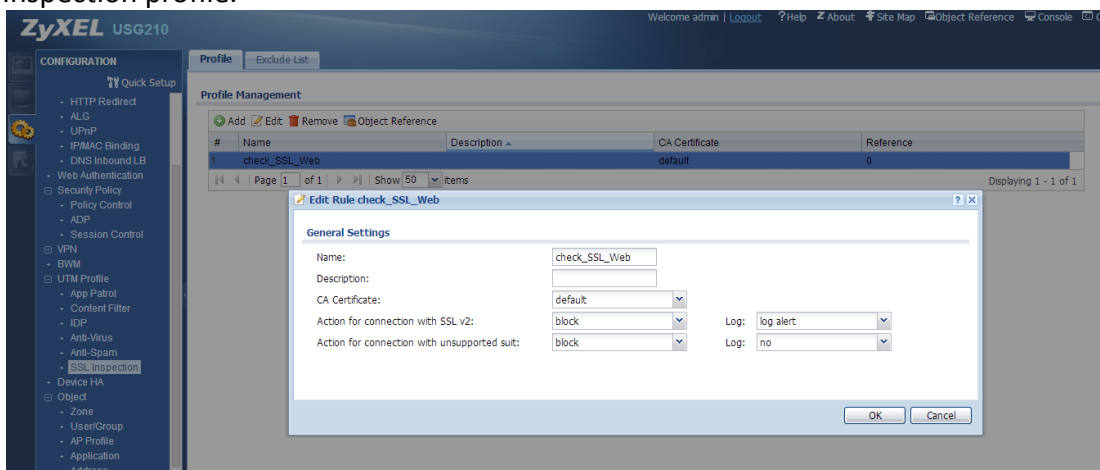


Add a social network in Content Filter function to drop social networks.



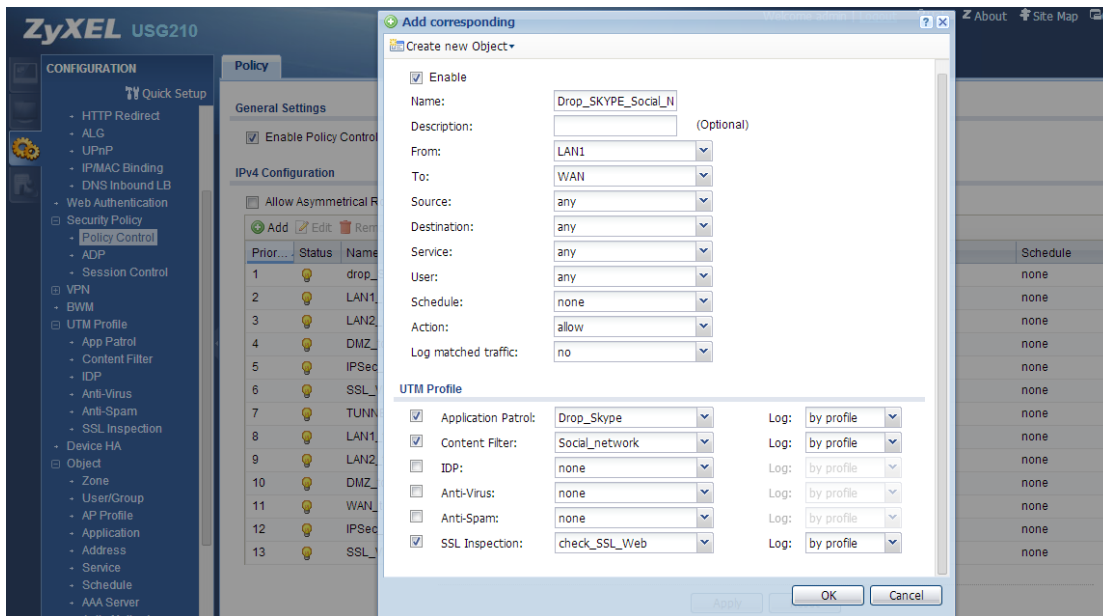
- (3)
(4) Add a SSL inspection rule to drop the SSL web site to access the social network.

Go to **Configuration > UTM Profile > SSL Inspection > Profile**, and click on the **“Add”** button to add a SSL Inspection profile.



- (5) Add the policy control rule to drop Skype and social networks from LAN1 subnet.

Go to **Configuration > Security Policy > Policy control > Policy**, and click on the **“Add”** button to add the rule, and select the objects into this rule.



After configuring these rule, then you can drop Skype and all of the social networks successfully.

Scenario 12 – Block HTTPS Websites by Content Filter

Introduction:

The Content Filter function can distinguish between websites by categories. Since the Content Filter does not know that the traffic has already been encrypted, so the HTTPS websites cannot be detected. But now can we use the “SSL Inspection” function to decrypt the packets, and then to block it.

After enabling the SSL inspection, clients only need to import the certificate generated by the USG, because the USG has become a proxy to help to verify these HTTPS websites, so client only needs to trust the USG.



After using the SSL inspect function, HTTPS traffic can be detected well by the Content Filter function.

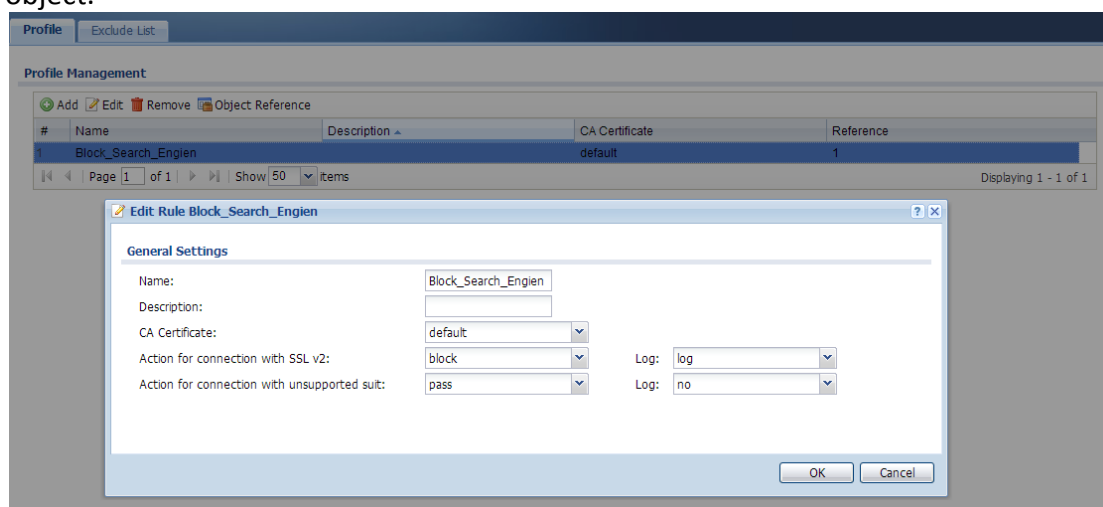
12.1 Application Scenario

Block the search engine in the internal website.

12.2 Configuration Guide

(1) Create an object in SSL inspection function.

Go to **Configuration > UTM Profile > SSL Inspection > Profile**, and click on “**Add**” to add an SSL Inspection object.



(2) Create a Content Filter object on the device.

Go to **Configuration > UTM Profile > Content Filter** and click on “**Add**” to create a Content Filter profile.

The default setting of “Action Managed Web Page” is “Block”.

The screenshot shows the 'Edit Filter Profile Search_Engine' window with the 'Category Service' tab selected. Under 'General Settings', the 'License Status' is 'Licensed', 'License Type' is 'Standard', and 'Name' is 'Search_Engine'. The 'Action for Managed Web Pages' is set to 'Block' and is highlighted with a red box. Other actions are set to 'Warn'. Under 'Select Categories', 'Select All Categories' is checked. Under 'Security Threat (unsafe)', several threats are checked, including Anonymizers, Malware, Phishing & Fraud, Botnets, Network Errors, Spam Sites, Compromised, and Parked Domains.

In the **Managed Categories** select “Search Engines/ Portals” to block the search engine.

The screenshot shows the 'Edit Filter Profile Search_Engine' window with the 'Managed Categories' tab selected. A list of categories is displayed, and 'Search Engines/Portals' is checked and highlighted with a red box. Other categories like Advertisements & Pop-Ups, Business, Forums & Newsgroups, etc., are listed but not checked.

(3) After Create SSL Inspection and Content Filter profiles, then go to the **Policy Control** function to setup the rule.

Go to **Configuration > Security policy > Policy control** and click on the “**Add**” button to add the rule.

After you setup a session orientation, then you can setup the UTM profile.

In this example, after you select the profile that you added in this rule, then the end user will not be able to access the search engine any more.

Edit Policy1

Create new Object

☒ Enable

Name: Block_Search_Engine

Description: (Optional)

From: any

To: any (Excluding ZyWALL)

Source: any

Destination: any

Service: any

User: any

Schedule: none

Action: allow

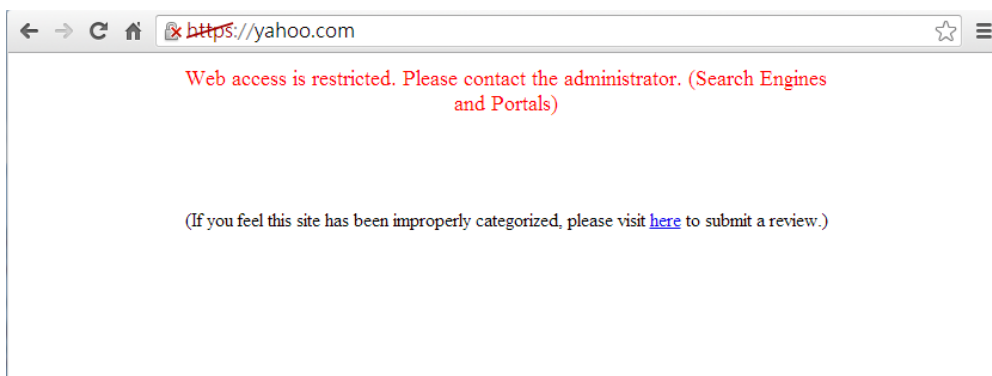
Log matched traffic: no

UTM Profile

<input type="checkbox"/>	Application Patrol:	none	Log: by profile
<input checked="" type="checkbox"/>	Content Filter:	Search_Engine	Log: by profile
<input type="checkbox"/>	IDP:	none	Log: by profile
<input type="checkbox"/>	Anti-Virus:	none	Log: by profile
<input type="checkbox"/>	Anti-Spam:	none	Log: by profile
<input checked="" type="checkbox"/>	SSL Inspection:	Block_Search_Engine	Log: by profile

Apply OK Cancel

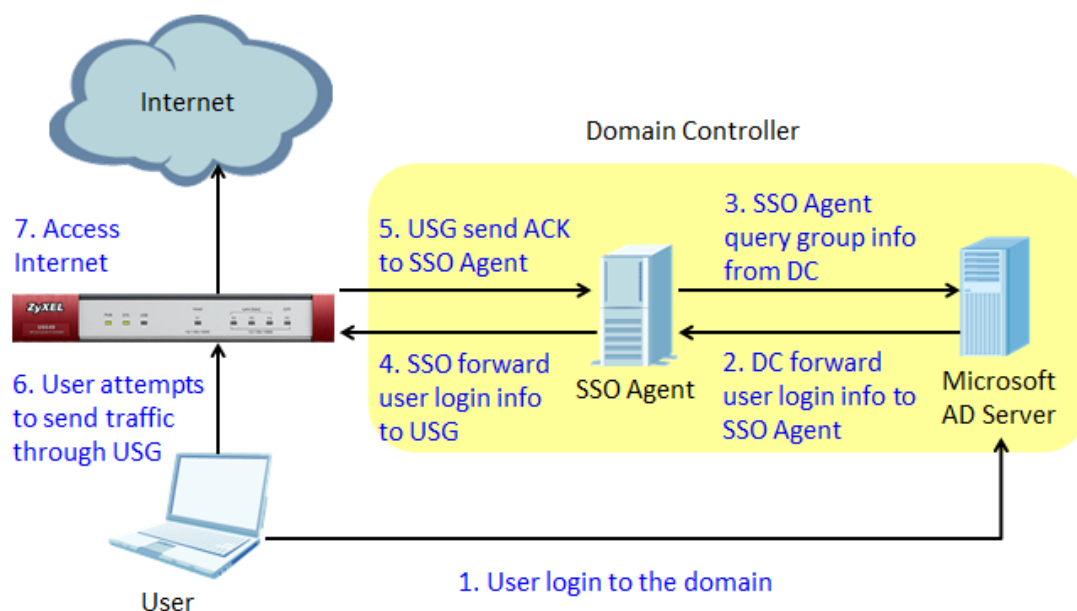
Verification: Access to https:yahoo.com



Scenario 13: Single Sign-on with USG and Windows Platform

13.1 Application Scenario

When the employee's PC is connected to the company's network, usually he needs to login to the domain first, and then login to the USG with the same username and password again, to pass the web authentication before accessing the Internet and the company's resources. With Single Sign-On agent integrated with Microsoft Active Directory, the SSO Agent sends authentication information to the USG to let users automatically get access to permitted resources. Users just need to login to the domain once and have access to the Internet and company internal resources that they are authorized to access directly without being prompted to login again.



13.2 Configuration Guide

Network conditions

WAN: 59.124.163.151

LAN 1: 192.168.1.0/255.255.255.0

Domain Controller (Windows Server 2008 R2): 192.168.1.34

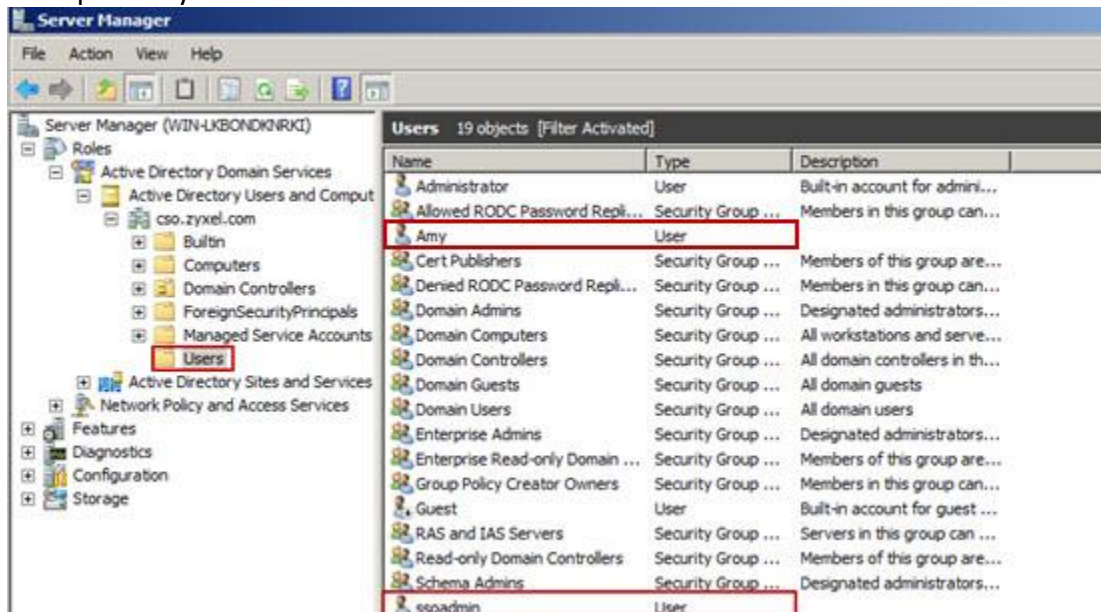
Client's laptop: 192.168.1.33

Goals to achieve

The user logs into the domain once and is able to access the Internet directly without specifying the username and password in the web browser.

Domain Controller Configuration

1. Go to **Active Directory Users and Computers** to create a new domain account and add it to the group of "Domain Admins".
Example: ssoadmin
Create some domain users.
Example: Amy



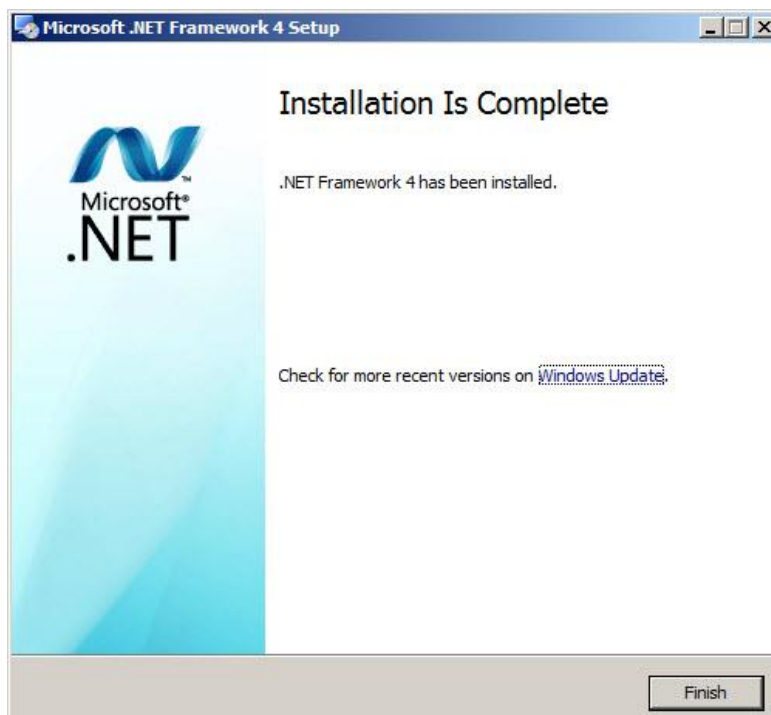
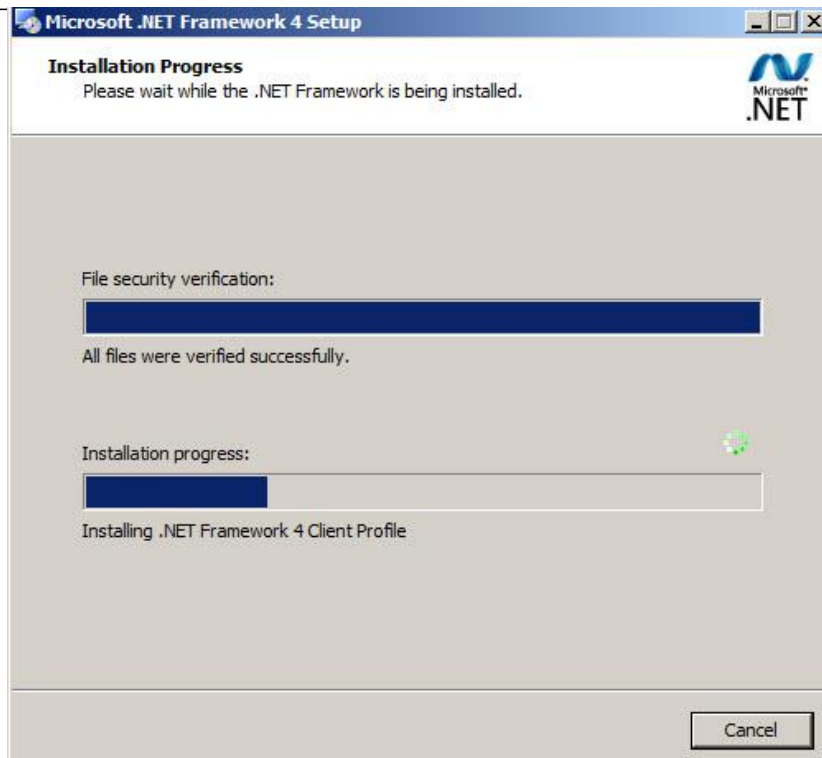
SSO Agent Installation

1. Prepare the package of SSO Agent.
2. Install .NET Framework v4.0.30319 or above version.

DotNetFx40	3/24/2014 2:54 PM	File folder
vcredist_x86	3/24/2014 2:54 PM	File folder
WindowsInstaller3_1	3/24/2014 2:54 PM	File folder

Double click "dotNetFx40_Full_x86_x64.exe".

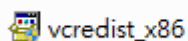
dotNetFx40_Full_x86_x64

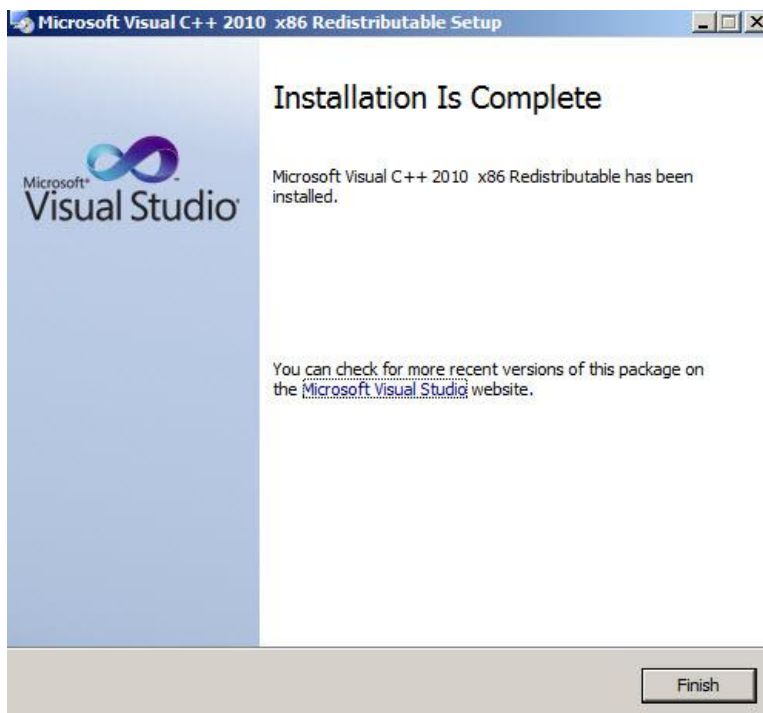
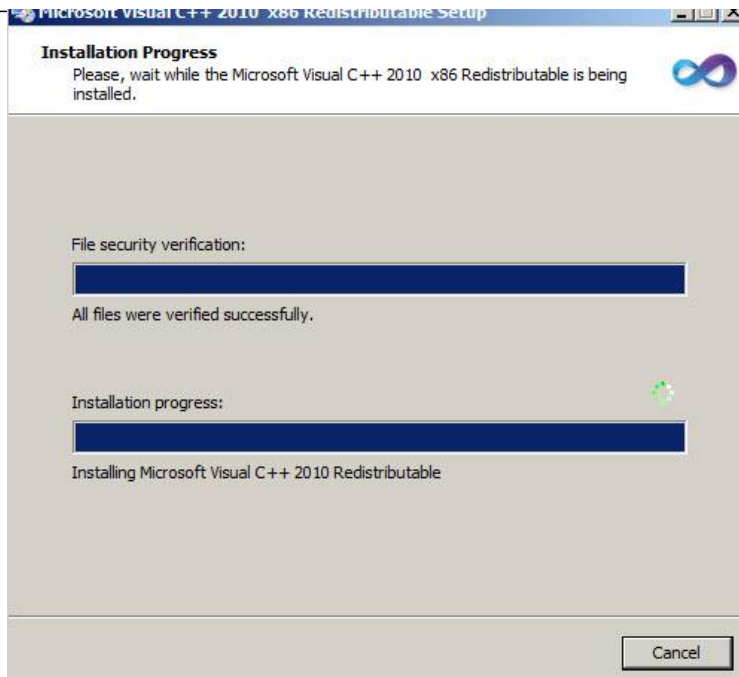


3. Install Visual C++

 DotNetFX40	3/24/2014 2:54 PM	File folder
 vcredist_x86	3/24/2014 2:54 PM	File folder
 WindowsInstaller3_1	3/24/2014 2:54 PM	File folder

Double-click on the "vcredist_x86.exe".





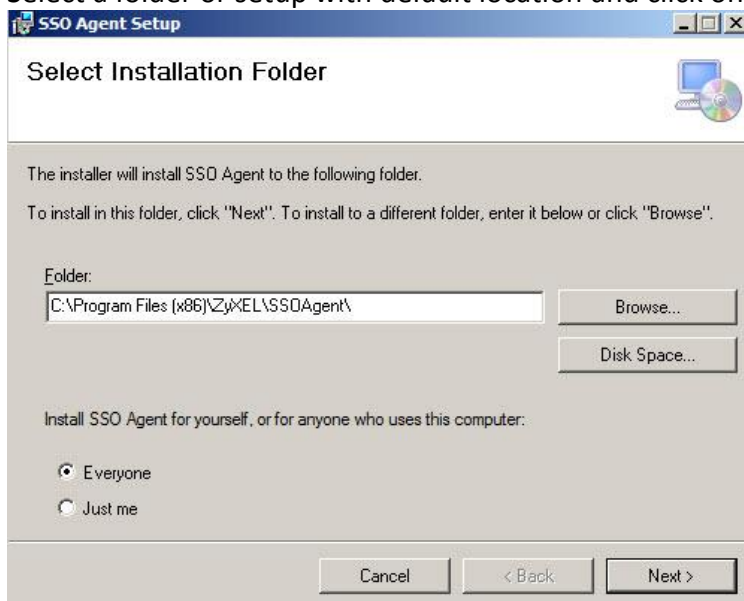
4. Double-click on "SSOAgentInstaller.exe" to install SSO Agent.

DotNetFX40	3/24/2014 2:54 PM	File folder	
vcredist_x86	3/24/2014 2:54 PM	File folder	
WindowsInstaller3_1	3/24/2014 2:54 PM	File folder	
Cleaner	3/12/2014 3:32 PM	Application	12 KB
install	3/24/2014 3:17 PM	Text Document	451 KB
setup	3/21/2014 11:00 AM	Application	418 KB
SSOAgentBoostraper	3/12/2014 2:32 PM	Application	6 KB
SSOAgentInstaller	3/21/2014 12:03 PM	Application	7,414 KB
SSOAgentSetup	3/21/2014 11:00 AM	Windows Installer P...	8,095 KB

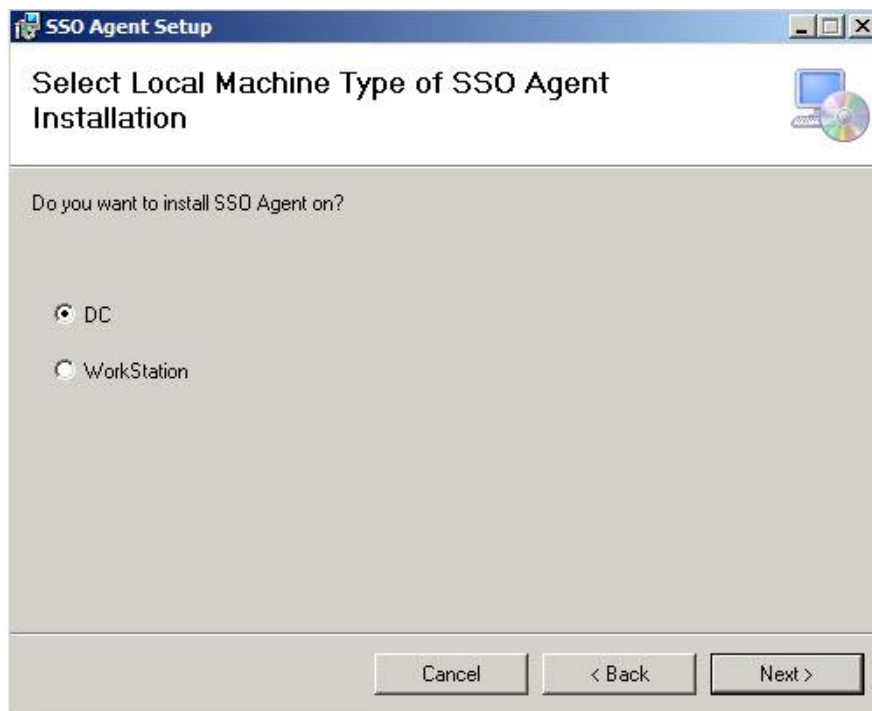
Click on "Next" to proceed.



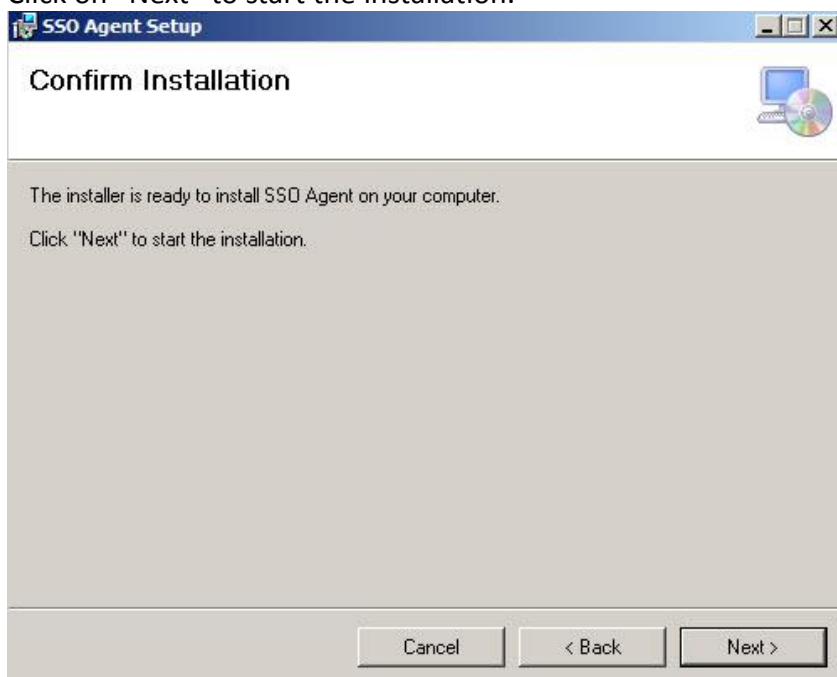
Select a folder or setup with default location and click on “Next”.



In this scenario, SSO Agent is installed on the Domain Controller. Select “DC”.

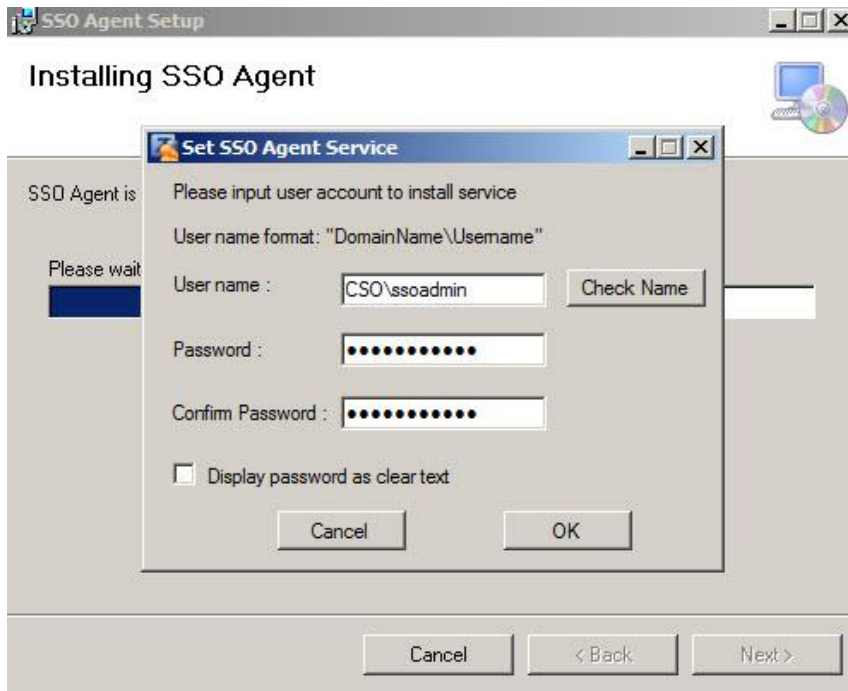


Click on "Next" to start the installation.

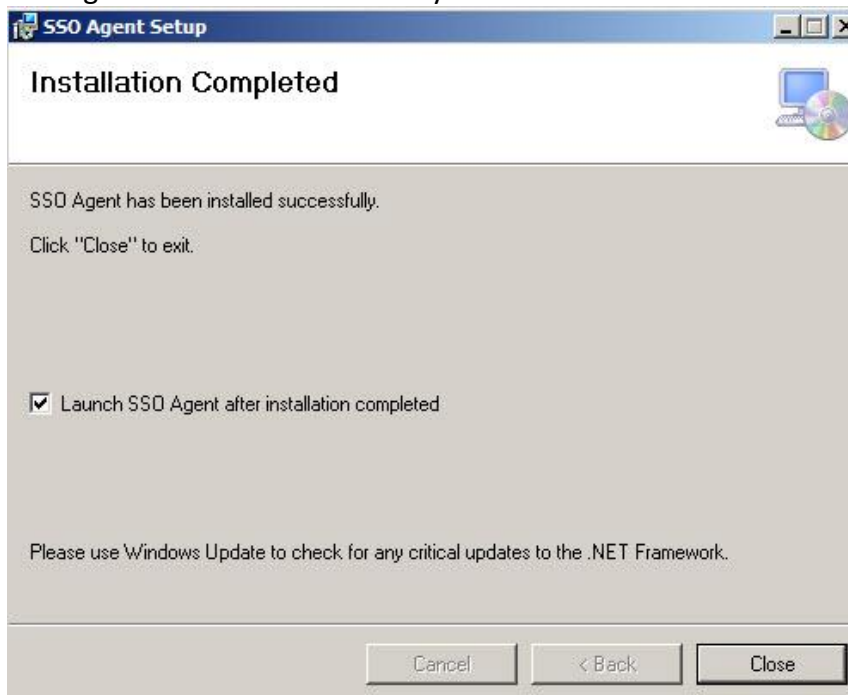


A dialog box called "Set SSO Agent Service" will pop-up.

Enter the Domain\Username and password of the domain account that was created in **Domain Controller configuration**. Click on "OK" to continue.

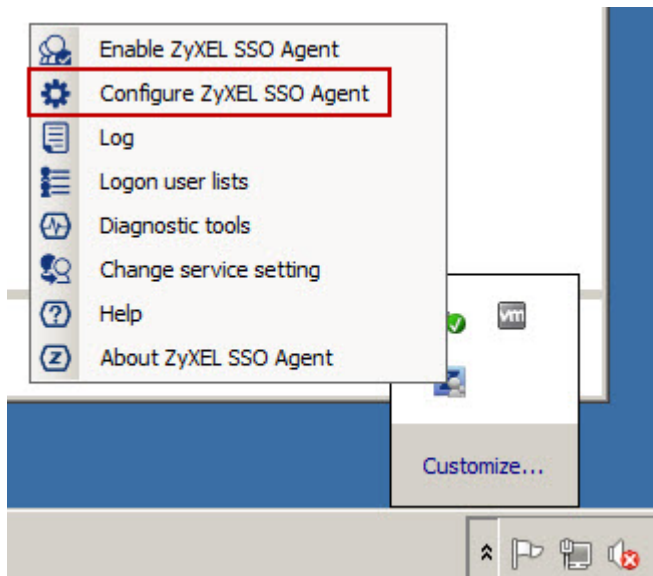


SSO Agent is installed successfully.

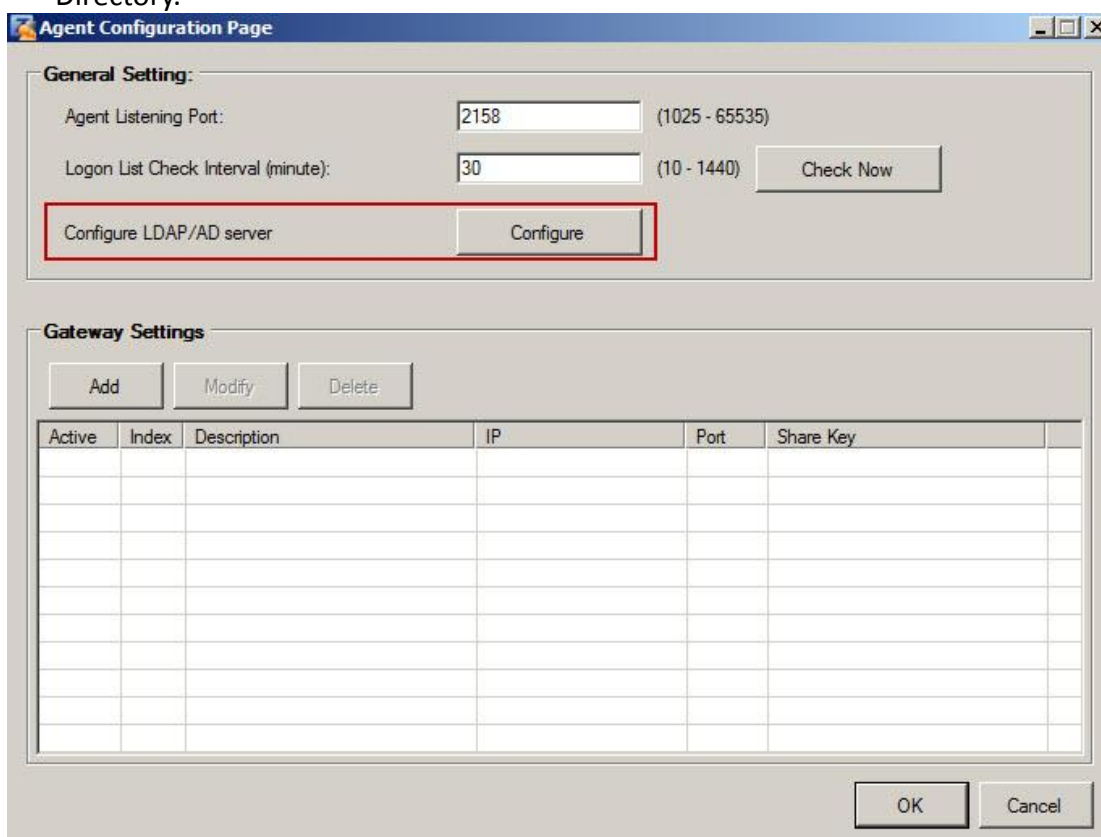


SSO Agent Installation

1. Click on "Configure ZyXEL SSO Agent".



2. Click on “Configure” to configure the LDAP query to get group information of users from the Active Directory.



Configure the IP address of the AD server, Base DN, and Bind DN.

LDAP/AD server configuration

General Settings

Name:

Description:

Server Settings

Server Address:

Backup Server Address:

Port:

Base DN:

☐ Use SSL

Search time limit:

☐ Case-sensitive User names

Server Authentication

Bind DN:

Password:

Retype to Confirm:

User Login Settings

Login Name Attribute:

Alternative Login Name Attribute:

Group Membership Attribute:

Configuration Validation

Please enter the existing user account in this server to validate the above settings

Username:

Under Gateway Settings, click on “Add” to configure the IP address of the USG and the Pre-Shared Key.

Gateway Setting

Gateway IP: IPv4 Address

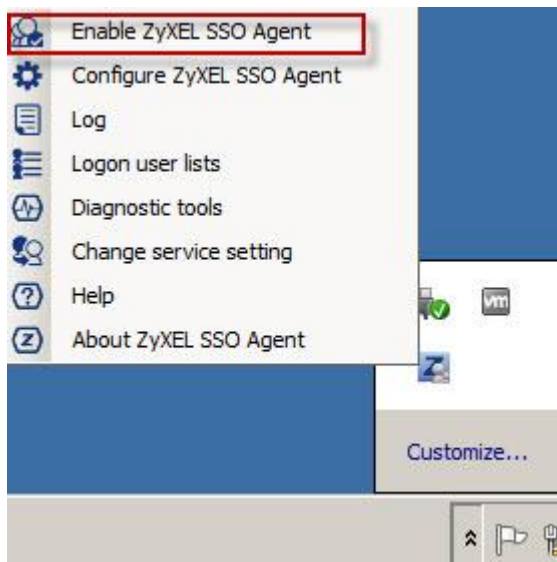
Gateway Port: (1025 - 65535)

Description:

PreShareKey:

☐ Check to show PreShareKey as clear Text

Enable SSO service.



When the SSO service is started successfully, the icon is enabled.



USG Configuration

1. Go to **CONFIGURATION > Object > AAA server > Active Directory > Edit Active Directory**. Configure the AD server that has the same settings as step 2 of “SSO Agent Installation”.

2. Go to **CONFIGURATION > Object > User/Group > User** and add a new ext-group-user. Ex: csosecurity. The domain user “Amy” must belong to this group in the AD.

3. Go to **CONFIGURATION > Object > Auth. Method** and add “group ad” in the default authentication method.

#	Method List
1	group ad
2	local

4. Go to **CONFIGURATION > Web Authentication > SSO**.
Fill-in the Pre-Shared Key which is configured in the **SSO Configuration**.

5. Go to **CONFIGURATION > Web Authentication > Web Authentication Policy Summary** to add a new authentication policy.
Enable the “Single Sign-on” checkbox to be authenticated by the SSO.

Auth. Policy Edit

Create new Object ▾

General Settings

☒ Enable Policy

Description: (Optional)

User Authentication Policy


Source Address: LAN1_SUBNET ▾ INTERFACE SUBNET, 192.168.1.0/24

Destination Address: any ▾








Schedule: none ▾

Authentication: required ▾

☒ Single Sign-on

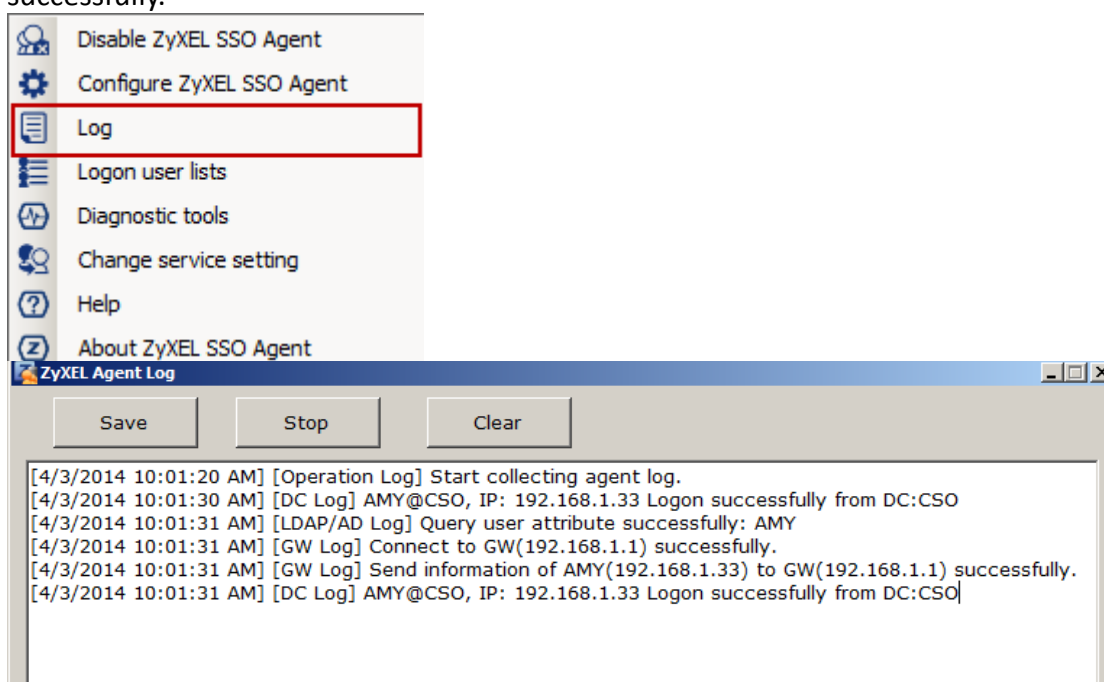
☒ Force User Authentication 

Web Authentication Policy Summary

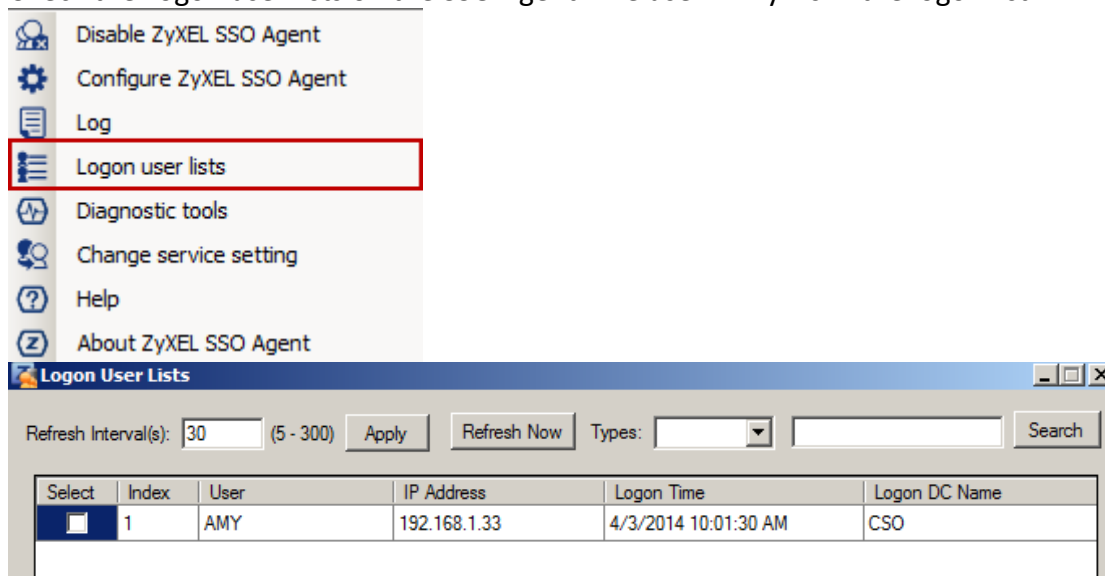
 Add  Edit  Remove  Activate  Inactivate  Move					
Status	Priority	Source	Destination	Schedule	Authentication
	1	LAN1_SUBNET	any	none	SSO/force
	Default	any	any	none	unnecessary
Page 1 of 1 Show 50 items					

Verification

- On the client's laptop, login using the domain account "Amy".
Example: CSO\Amy
Open the browser or application on the client's laptop to trigger traffic to pass to the USG. The client "Amy" can surf the Internet directly without extra authentication.
- Check SSO Agent Log. User login is successful and has sent information to the USG's GW (192.168.1.1) successfully.

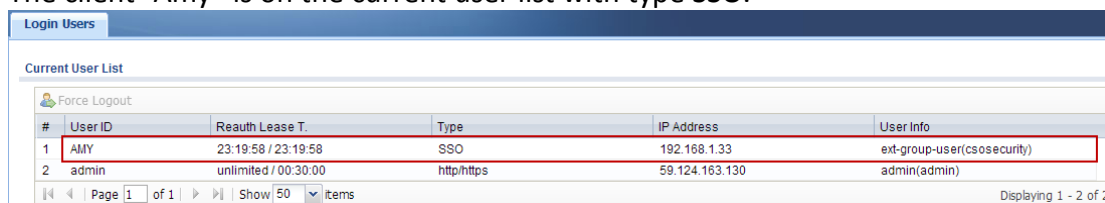


3. Check the Logon user lists on the SSO Agent. The user “Amy” is in the logon list.



4. Go to **MONITOR > System Status > Login Users**.

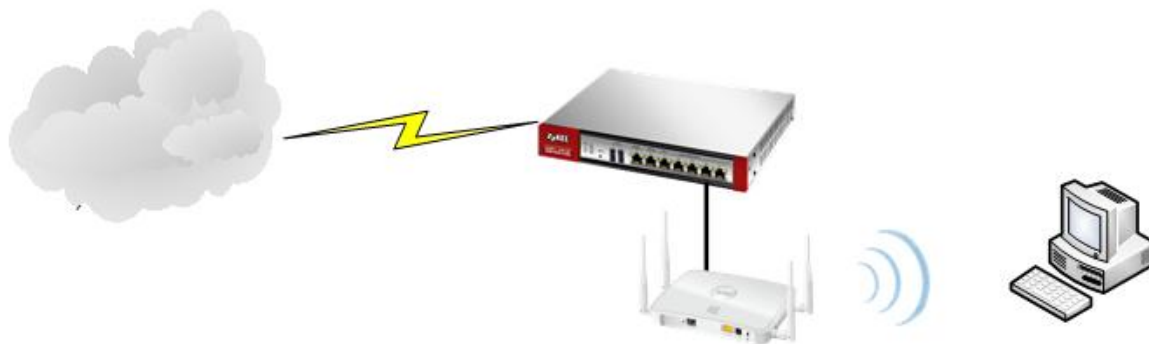
The client “Amy” is on the current user list with type SSO.



Scenario 14 – WLAN Controller Function on USG

14.1 Application Scenario

USG with 4.10 firmware supports the AP controller function. You can follow the steps to control your AP device.

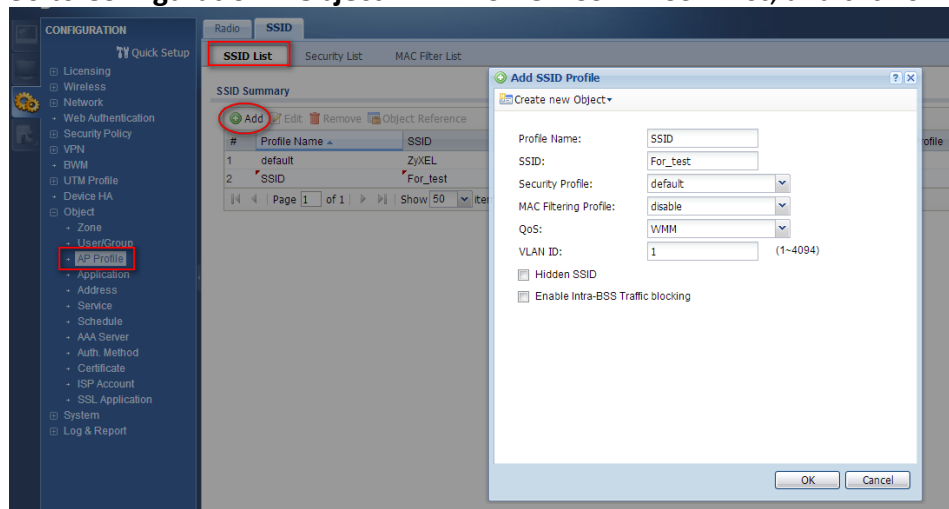


14.2 Configuration Guide

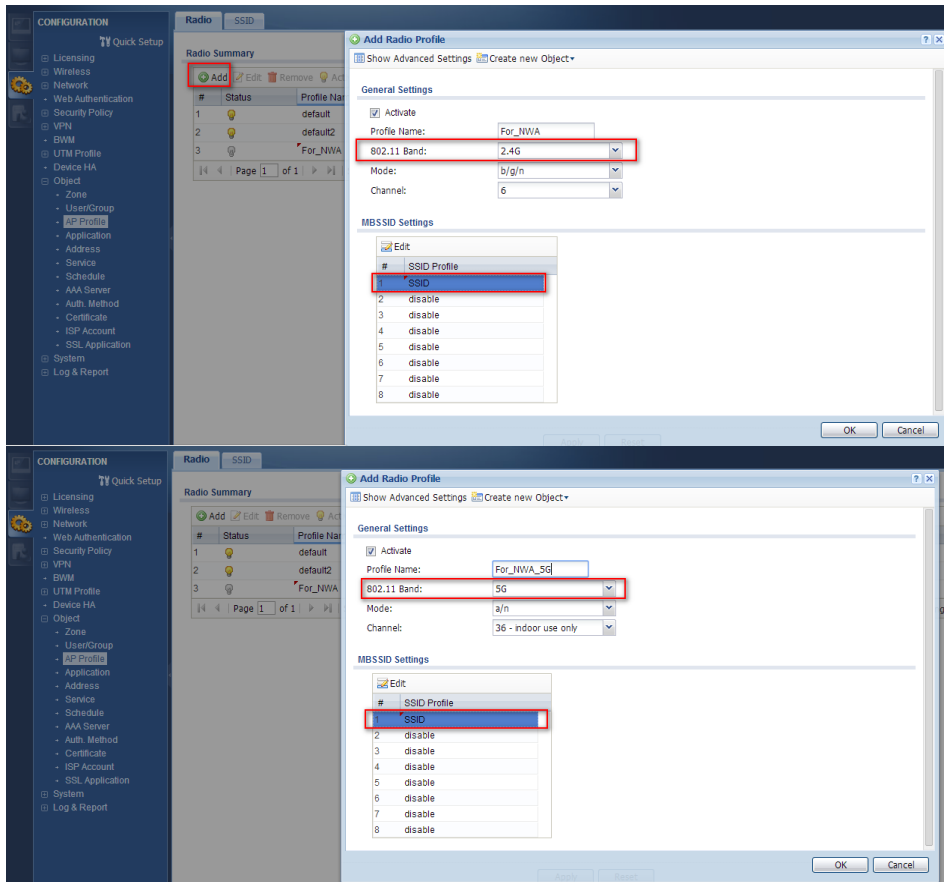
Management of external AP device

(1) Add an SSID object on the device

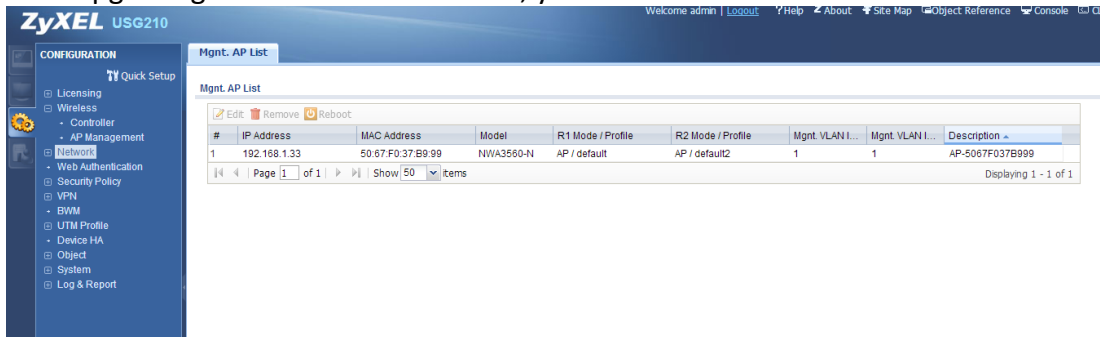
Go to **Configuration > Object > AP Profile > SSID > SSID list**, and click on the “Add” button.



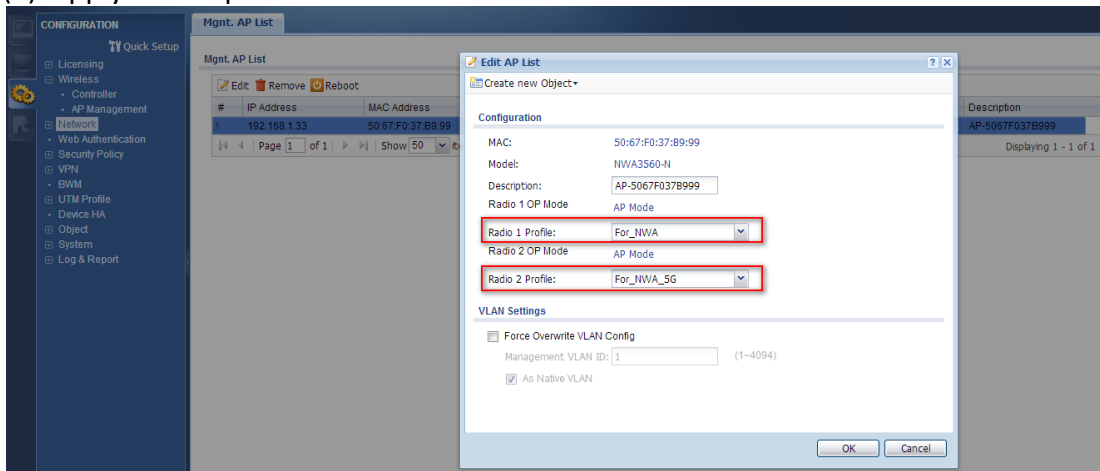
(2) Go to **Configuration > Object > AP Profile > Radio**, and click on the “Add” button to add 2.4G and 5G radio objects, and set the SSID profile to this object.



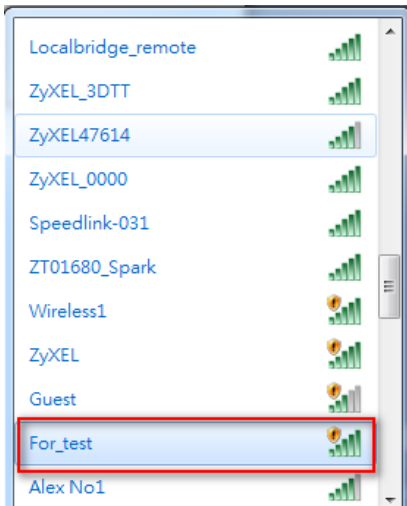
- (3) Connect your AP to the LAN interface (this document is using NWA 3560-N to test).
- The AP must be set as managed mode.
 - After the connection is successful, the NWA will start upgrading the firmware from the USG.
- After upgrading the firmware successful, you will see the MAC address and model name in the GUI.



- (4) Apply the AP profile on the NWA.



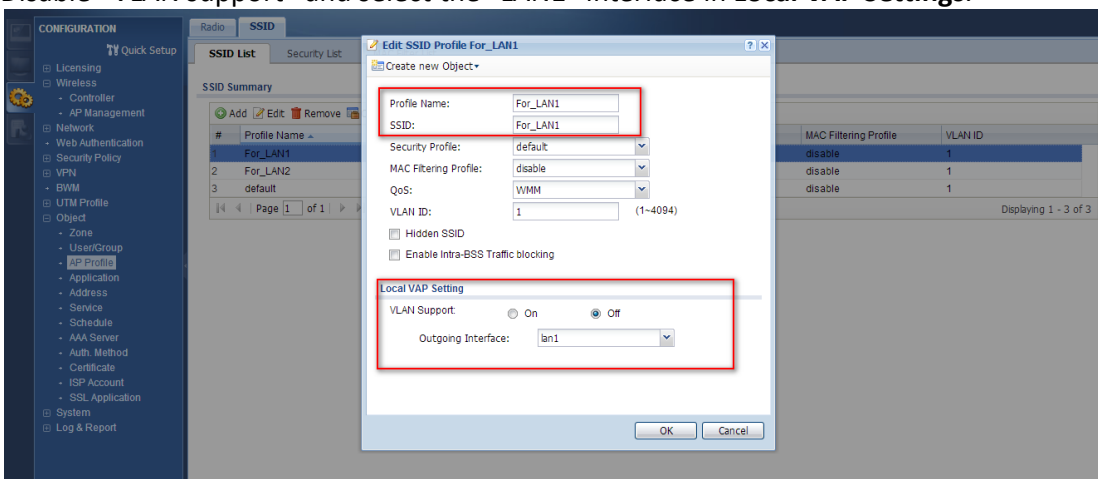
- (5) Verify the SSID on your network (the SSID is "For_test")



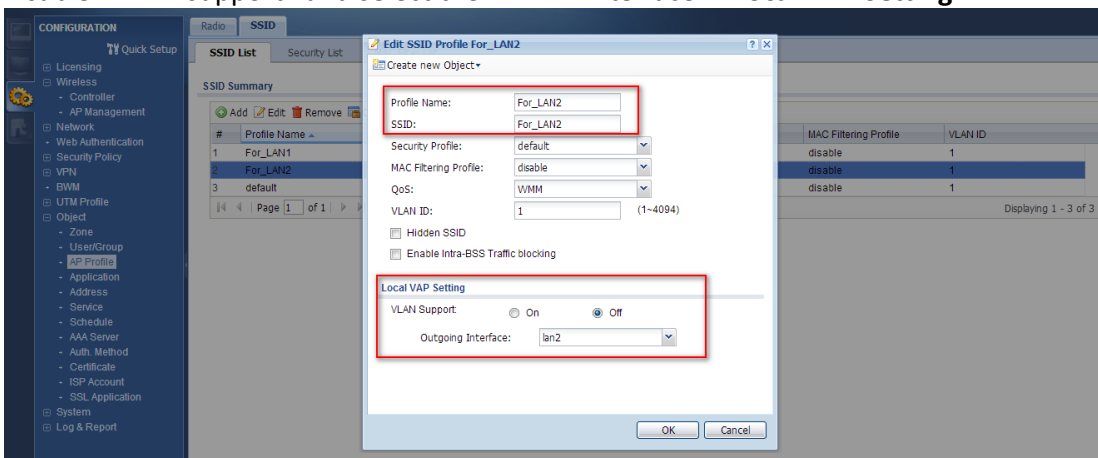
Management of Local AP interface (Only for USG40W & USG60W)

(1) Add 2 SSIDs in the SSID list (LAN1 and LAN2 subnet)

Go to **Configuration > Object > AP Profile > SSID > SSID list** and click on the “Add” button to create SSID object. Disable “VLAN support” and select the “LAN1” interface in **Local VAP Settings**.



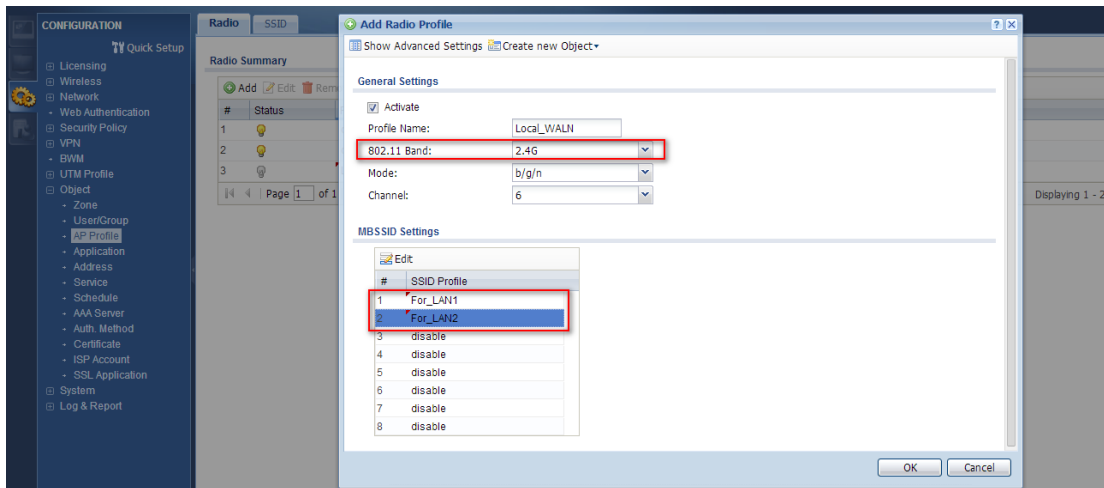
Disable “VLAN support” and select the “LAN2” interface in **Local VAP Setting**.



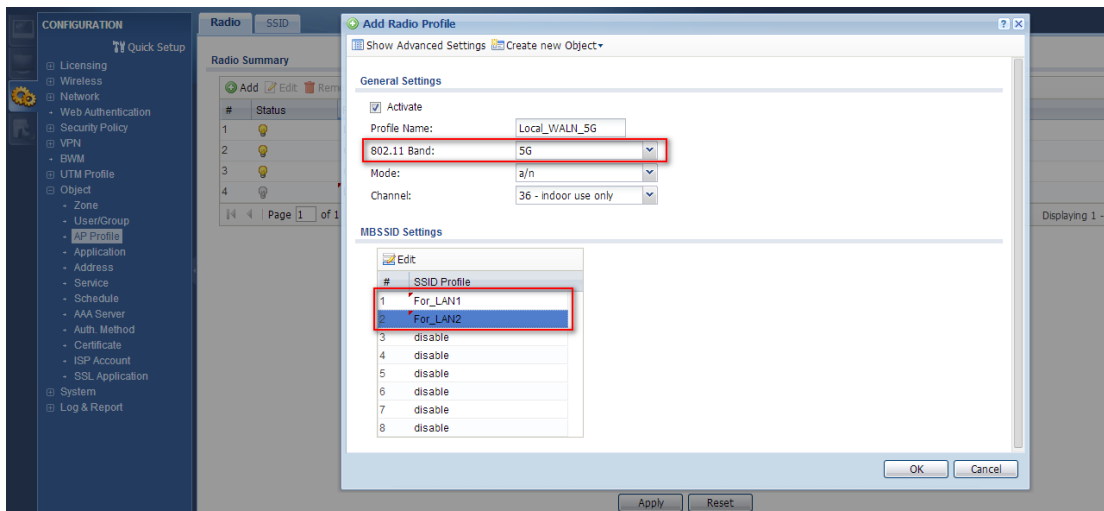
(2) Add AP profiles and select these 2 SSID objects in the rule.

Go to **Configuration > Object > AP Profile > RADIO** and click on the “Add” button to create the AP profile

2.4G Band



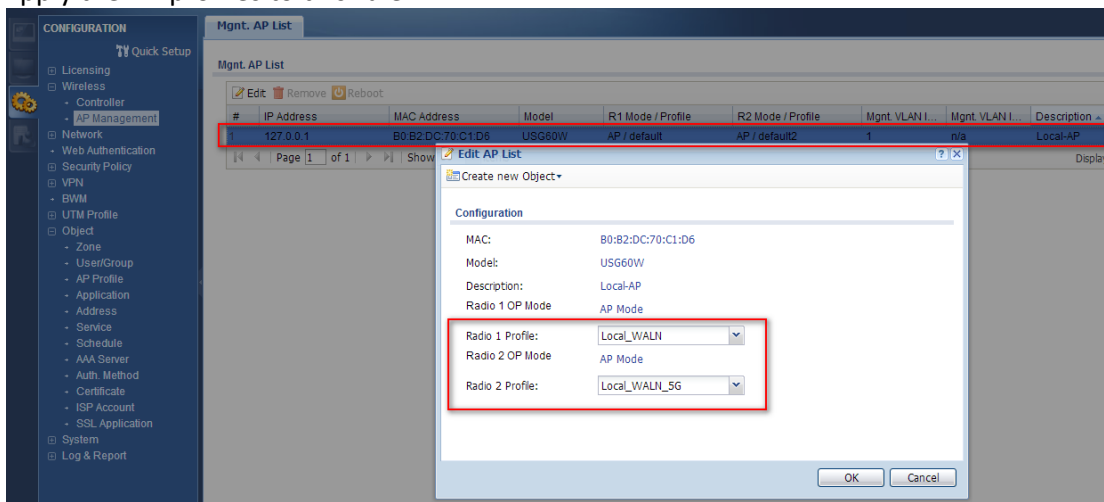
5G Band



(3) Apply AP profiles to the Local AP interface

Go to **Configuration > Wireless > AP Management** and click the local AP (IP address is 172.0.0.1) to edit the rule.

Apply the AP profiles to this rule.



Verification:

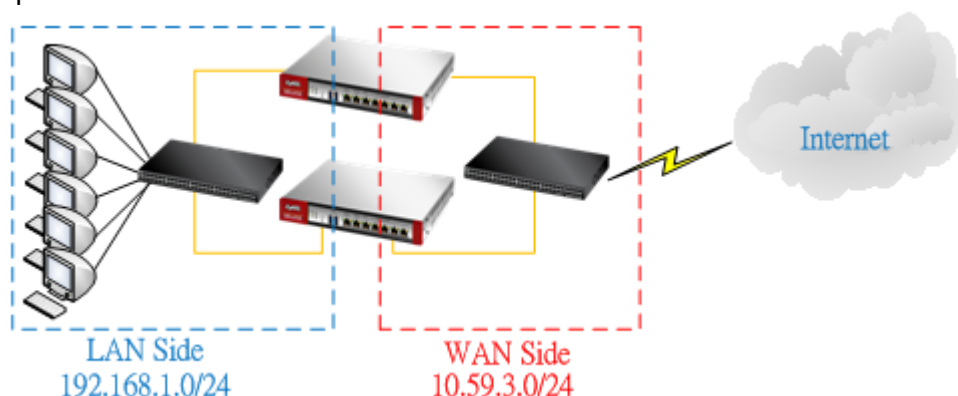
If you have connected to For_LAN1 SSID, then you will get the LAN1 subnet IP address. If you connect to For_LAN2, then you will get the LAN2 subnet IP address.

ZyXEL00036	
VIDEOTRON0048	
CHT6695	
For_LAN1	
Wireless1	
ZyXEL	
ZyXEL_3DTT	
TTNET_ZyXEL_F4YW	
Keenetic-5079	
BBBBBBBBBBBBBBBBBBBB	
For_LAN2	

Scenario 15 – Device HA on the USG

15.1 Application Scenario

Setup the Device HA environment.



	Master device	Backup device
WAN interface IP	10.59.3.100/24	10.59.3.100/24
WAN Management IP	10.59.3.101/24	10.59.3.102/24
LAN1 Interface IP	192.168.1.1/24	192.168.1.1/24
LAN1 Management IP	192.168.1.11/24	192.168.1.12/24
Cluster ID	1	1

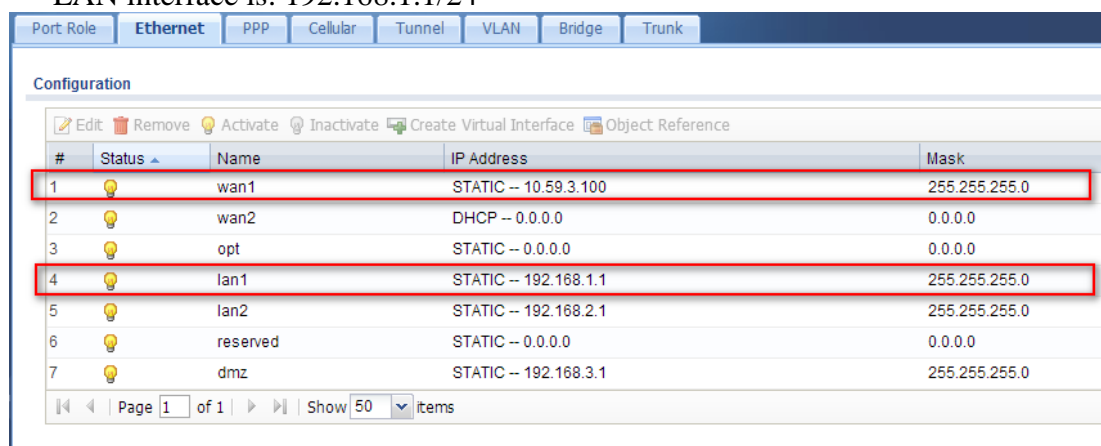
15.2 Configuration Guide

On Master setting:

- (1) Go to **Configuration > Network > Interface > Ethernet** to check the WAN and LAN interface setting.

WAN interface is: 10.59.3.100/24

LAN interface is: 192.168.1.1/24



- (2) Go to **Configuration > Device HA > Activate-Passive Mode** to add the management interface on the master device.

The **Device Role** must be set as “Master”.

WAN management IP address is: 10.59.3.101

LAN management IP address is: 192.168.1.11

General Settings

Device Role: ☒ Master ☐ Backup

Cluster Settings

Cluster ID: 1

Monitored Interface Summary

#	Status	Interface	Virtual Router IP/Netmask	Management IP / Netmask	Link Status
1	Up	wan1	10.59.3.100 / 255.255.255.0	10.59.3.101 / 255.255.255.0	Up
2	Down	wan2	/	/	Down
3	Down	opt	/	/	Down
4	Up	lan1	192.168.1.1 / 255.255.255.0	192.168.1.11 / 255.255.255.0	Up
5	Down	lan2	192.168.2.1 / 255.255.255.0	/ 255.255.255.0	Down
6	Down	reserved	/	/	Down
7	Down	dmz	192.168.3.1 / 255.255.255.0	/ 255.255.255.0	Down

Page 1 of 1 | Show 50 items | Displaying 1 - 7 of 7

- (3) Go to **Configuration > Device HA > General** to enable the Device HA function.

After you have enabled the Device HA function, you will see the interface that was monitored above.

General Settings

☒ Enable Device HA

Device HA Mode: Active-Passive Mode

Monitored Interface Summary

#	Interface	Virtual Router IP/Netmask	Management IP / Netmask	Link Status	HA Status
1	wan1	10.59.3.100 / 255.255.255.0	10.59.3.101 / 255.255.255.0	Up	Master / Active
2	lan1	192.168.1.1 / 255.255.255.0	192.168.1.11 / 255.255.255.0	Up	Master / Active

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

On Backup setting:

- (4) Go to **Configuration > Network > Interface > Ethernet** to check the WAN and LAN interface setting.

WAN interface is: 10.59.3.100/24

LAN interface is: 192.168.1.1/24

Port Role: Ethernet

Configuration

#	Status	Name	IP Address	Mask
1	Up	wan1	STATIC -- 10.59.3.100	255.255.255.0
2	Up	wan2	DHCP -- 0.0.0.0	0.0.0.0
3	Up	opt	STATIC -- 0.0.0.0	0.0.0.0
4	Up	lan1	STATIC -- 192.168.1.1	255.255.255.0
5	Up	lan2	STATIC -- 192.168.2.1	255.255.255.0
6	Up	reserved	STATIC -- 0.0.0.0	0.0.0.0
7	Up	dmz	STATIC -- 192.168.3.1	255.255.255.0

Page 1 of 1 | Show 50 items

- (5) Go to **Configuration > Device HA > Activate-Passive Mode** to add the management interface on the backup device.

The **Device Role** must be set as “Backup”.

WAN management IP address is: 10.59.3.102

LAN management IP address is: 192.168.1.12

General Active-Passive Mode

Show Advanced Settings

General Settings

Device Role: ☐ Master ☒ Backup

Priority: 1 (1-254)

☐ Enable Preemption

Cluster Settings

Cluster ID: 1

Monitored Interface Summary

#	Status	Interface	Virtual Router IP/Netmask	Management IP / Netmask	Link Status
1	Up	wan1	10.59.3.100 / 255.255.255.0	10.59.3.102 / 255.255.255.0	Up
2	Down	wan2	/	/	Down
3	Down	opt	/	/	Down
4	Up	lan1	192.168.1.1 / 255.255.255.0	192.168.1.12 / 255.255.255.0	Up
5	Down	lan2	192.168.2.1 / 255.255.255.0	/ 255.255.255.0	Down
6	Down	reserved	/	/	Down
7	Down	dmz	192.168.3.1 / 255.255.255.0	/ 255.255.255.0	Down

Page 1 of 1 Show 50 items Displaying 1 - 7 of 7

(6) Go to **Configuration > Device HA > General** to enable Device HA function.

After you have enabled the Device HA function, you will see the interface that was monitored above.

General Active-Passive Mode

General Settings

☒ Enable Device HA

Device HA Mode: Active-Passive Mode

Monitored Interface Summary

#	Interface	Virtual Router IP/Netmask	Management IP / Netmask	Link Status	HA Status
1	wan1	10.59.3.100 / 255.255.255.0	10.59.3.102 / 255.255.255.0	Up	Backup / Stand-By
2	lan1	192.168.1.1 / 255.255.255.0	192.168.1.12 / 255.255.255.0	Up	Backup / Stand-By

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

Verification:

You can check the status of the Device HA in the GUI.

The status of the master device will be "Master/Activate".

General Active-Passive Mode

General Settings

☒ Enable Device HA

Device HA Mode: Active-Passive Mode

Monitored Interface Summary

#	Interface	Virtual Router IP/Netmask	Management IP / Netmask	Link Status	HA Status
1	wan1	10.59.3.100 / 255.255.255.0	10.59.3.101 / 255.255.255.0	Up	Master / Active
2	lan1	192.168.1.1 / 255.255.255.0	192.168.1.11 / 255.255.255.0	Up	Master / Active

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

The status of the backup device will be "Backup/Stand-By"

General Active-Passive Mode

General Settings

☒ Enable Device HA

Device HA Mode: Active-Passive Mode

Monitored Interface Summary

#	Interface	Virtual Router IP/Netmask	Management IP / Netmask	Link Status	HA Status
1	wan1	10.59.3.100 / 255.255.255.0	10.59.3.102 / 255.255.255.0	Up	Backup / Stand-By
2	lan1	192.168.1.1 / 255.255.255.0	192.168.1.12 / 255.255.255.0	Up	Backup / Stand-By

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

Tutorial 1: How to Set Up Your Network

Here are examples of using the Web Configurator to set up your network in the USG.

Note: The tutorials featured here require a basic understanding of connecting to and using the Web Configurator. For field descriptions of individual screens, see the Web Configurator Online Help.

1.1 Wizard Overview

Use the wizards to quickly configure Internet connection and VPN settings as well as activate subscription services.

WIZARD	DESCRIPTION
Installation Setup Wizard	Use this wizard the first time log into the Web Configurator to configure WAN connections and register your USG.
Quick Setup	You can find the following wizards in the CONFIGURATION navigation panel.
WAN Interface	Use these wizard screens to quickly configure a WAN interface's encapsulation and IP address settings.
VPN Setup	Use these wizard screens to quickly configure an IPSec VPN or IPSec VPN configuration provisioning.

After you complete a wizard, you can go to the **CONFIGURATION** screens to configure advanced settings.

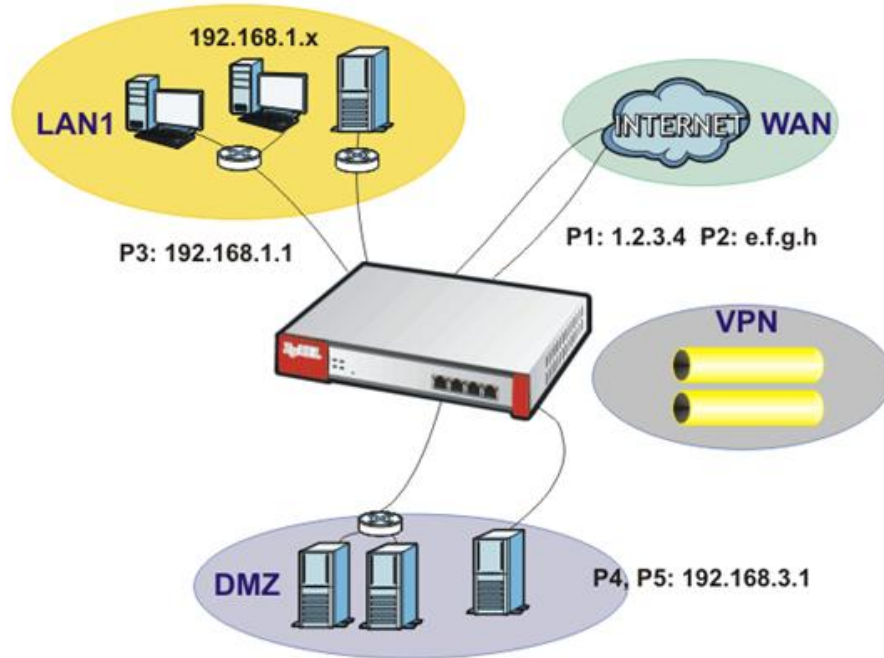
1.2 How to Configure Interfaces, Port Roles, and Zones

This tutorial shows how to configure Ethernet interfaces, port roles, and zones for the following example configuration.

- The **wan1** interface uses a static IP address of 1.2.3.4.

- Add **P5** (lan2) to the DMZ interface (Note: In USG 20/20W, use **P4** (lan2) instead of **P5** in this example). The DMZ interface is used for a protected local network. It uses IP address 192.168.3.1 and serves as a DHCP server by default.
- You want to be able to apply specific security settings for the VPN tunnel created by the **Quick Setup - VPN Setup** wizard (named **WIZ_VPN**). So you create a new zone and add **WIZ_VPN** to it.

Figure 21 Ethernet Interface, Port Roles, and Zone Configuration Example



1.2.1 Configure a WAN Ethernet Interface

You need to assign the USG's **wan1** interface a static IP address of 1.2.3.4.

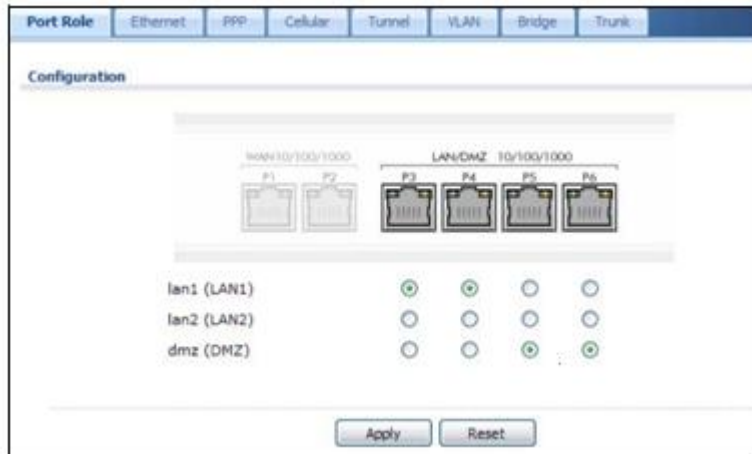
Click **Configuration > Network > Interface > Ethernet** and double-click the **wan1** interface's entry in the **Configuration** section. Select **Use Fixed IP Address** and configure the IP address, subnet mask, and default gateway settings and click **OK**.

1.2.2 Configure Port Roles

Here is how to take the **P5** port from the lan2 interface and add it to the dmz interface.

- 1 Click **Configuration > Network > Interface > Port Role**.

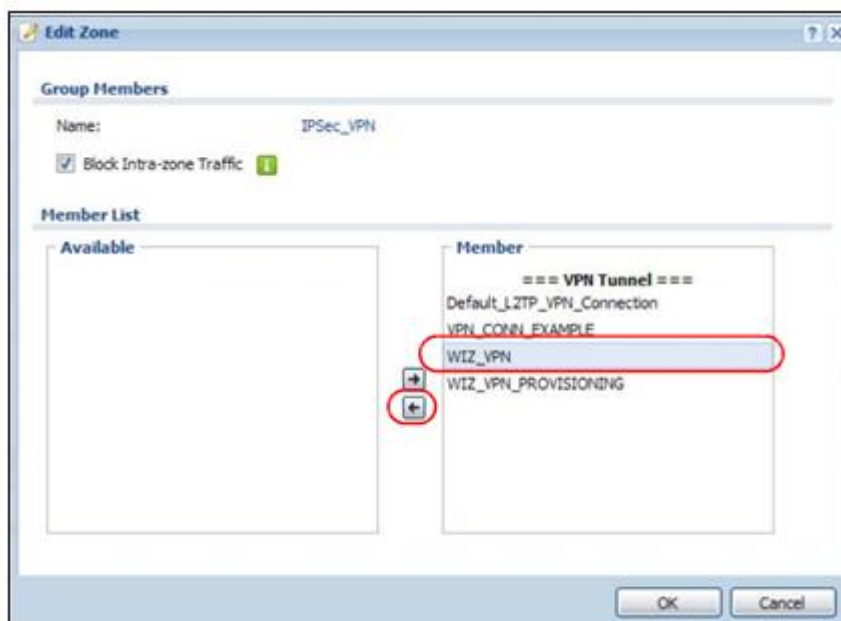
- Under **P5** select the **dmz (DMZ)** radio button and click **Apply**.



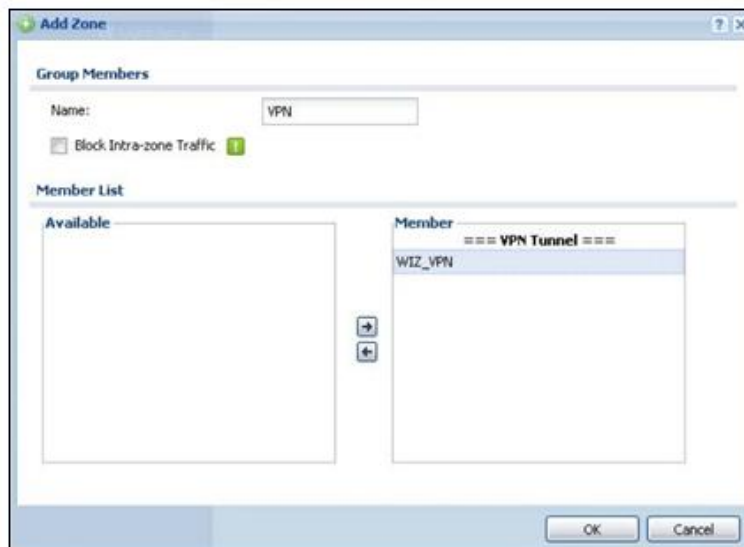
1.2.3 Configure Zones

In this example you have created a **WIZ_VPN** tunnel through the **Quick Setup - VPN Setup** wizard. By default, it is assigned to the **IPSec_VPN** zone. Do the following to move **WIZ_VPN** from the **IPSec_VPN** zone to a new zone.

- Click **Configuration > Network > Zone** and then double-click the **IPSec_VPN** entry.
- Select **WIZ_VPN** and remove it from the **Member** box and click **OK**.



- Back to the **Configuration > Network > Zone** screen and click **Add in the User Configuration** section.
- Enter **VPN** as the new zone's name. Select **WIZ_VPN** and move it to the **Member** box and click **OK**.

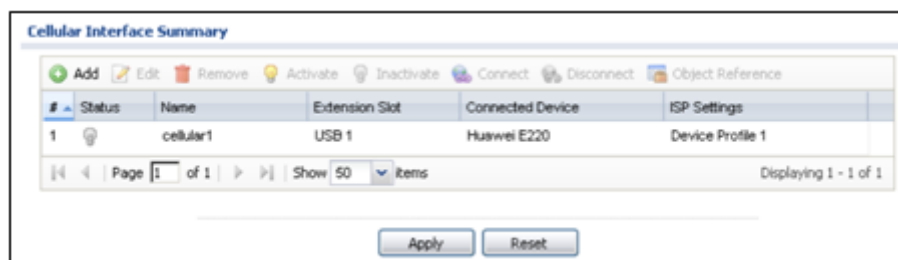


Then you can configure firewall rules to apply specific security settings to this **VPN** zone.

1.3 How to Configure a Cellular Interface

Use 3G cards for cellular WAN (Internet) connections. See www.zyxel.com for a supported 3G card. In this example you connect the 3G USB card before you configure the cellular interfaces but is also possible to reverse the sequence.

- 1 Make sure the 3G device's SIM card is installed.
- 2 Connect the 3G device to one of the USG's USB ports.
- 3 Click **Configuration > Network > Interface > Cellular**. Select the 3G device's entry and click **Edit**.



- 4 Enable the interface and add it to a zone. It is highly recommended that you set the **Zone** to **WAN** to apply your WAN zone security settings to this 3G connection. Leaving **Zone** set to **none** has the USG not apply any security settings to the 3G connection. Enter the **PIN Code** provided by the cellular 3G service provider (0000 in this example).

Edit Cellular configuration

☐ Hide Advanced Settings

General Settings

☒ Enable Interface

Interface Properties

Interface Name: cellular1

Zone: WAN

Extension Slot: USB 1

Connected Device: Huawei E220

Description: (Optional)

Connectivity

☒ Nailed-Up

Idle timeout: 0 seconds

ISP Settings

Profile Selection: ☒ Device ☐ Custom

Profile 1

APN: n/a

Dial String: n/a

SIM Card Setting

PIN Code: ****

Retype to Confirm: ****

OK Cancel

Note: The **Network Selection** is set to **auto** by default. This means that the 3G USB modem may connect to another 3G network when your service provider is not in range or when necessary. Select **Home** to have the 3G device connect only to your home network or local service provider. This prevents you from being charged using the rate of a different ISP.

- Go to the **Dashboard**. The **Interface Status Summary** section should contain a "cellular" entry. When its connection status is **Connected** you can use the 3G connection to access the Internet.

Interface Status Summary

#	Name	Status	Zone	IP Address	Action
1	wan1	Down	WAN	0.0.0.0	n/a
2	wan1_pp	Disconnected	WAN		
3	wan2	Down	WAN	0.0.0.0	Renew
4	lan1	Down	LAN1	192.168.1.1	n/a
5	lan2	100M/Full	LAN2	192.168.2.1	n/a
6	dmz	Down	DMZ	192.168.3.1	n/a
7	cellular1	Connected	n/a		

Page 1 of 1 | Show 50 items | Displaying 1 - 7 of 7

- The USG automatically adds the cellular interface to the system default WAN trunk. If the USG is using a user-configured trunk as its default trunk and you want this cellular interface to be part of it, use the **Trunk** screens to add it.

This way the USG can automatically balance the traffic load amongst the available WAN connections to enhance overall network throughput. Plus, if a WAN connection goes down, the USG still sends traffic through the remaining WAN connections. For a simple test, disconnect all of the USG's wired WAN connections. If you can still access the Internet, your cellular interface is properly configured and your cellular device is working.

1.4 How to Set Up a Wireless LAN

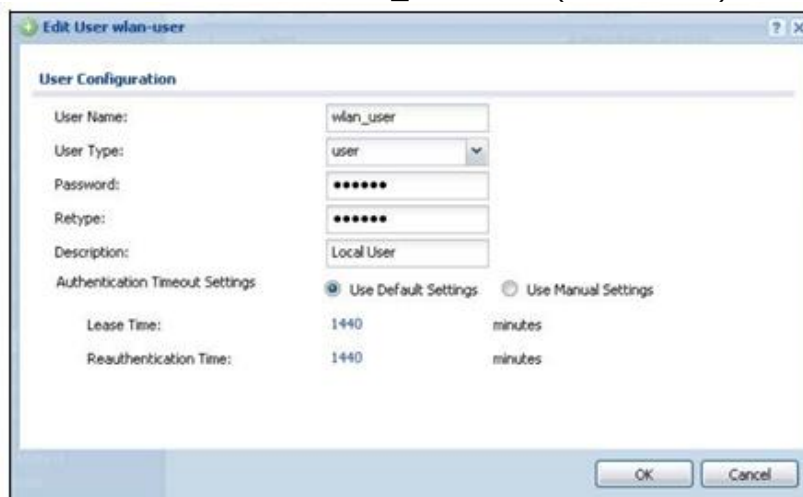
This tutorial applies only to models that include wireless LAN.

You can configure different interfaces to use on the wireless LAN card. This lets you have different wireless LAN networks using different SSIDs. You can configure the WLAN interfaces before or after you install the wireless LAN card. This example shows how to create a WLAN interface that uses WPA or WPA2 security and the USG's local user database for authentication.

1.4.1 Set Up User Accounts

Besides WPA-PSK, the USG also supports TTLS using PAP so you can use the USG's local user database with WPA or WPA2 instead of needing an external RADIUS server. For each WLAN user, set up a user account containing the user name and password the WLAN user needs to enter to connect to the wireless LAN.

- 1 Click **Configuration > Object > User/Group > User** and the **Add** icon.
- 2 Set the **User Name** to **wlan_user**. Enter (and re-enter) the user's password. Click **OK**.



- 3 Use the **Add** icon in the **Configuration > Object > User/Group > User** screen to set up the remaining user accounts in similar fashion.

1.4.2 Create the WLAN Interface

- 1 Click **Configuration > Network > Interface > WLAN > Add** to open the **WLAN Add** screen.
- 2 Edit this screen as follows.

A (internal) name for the WLAN interface displays. You can modify it if you want to.

The USG's security settings are configured by zones. Select to which security zone you want the WLAN interface to belong (the WLAN zone in this example). This determines which security settings the USG applies to the WLAN interface.

Configure the **SSID** (ZYXEL_WPA in this example).

If all of your wireless clients support WPA2, select **WPA2-Enterprise** as the **Security Type**, otherwise select **WPA/WPA-2-Enterprise**. Set the **Authentication Type** to **Auth Method**. The

USG can use its default authentication method (the local user database) and its default certificate to authenticate the users.

Configure the interface's IP address and set it to **DHCP Server**. Click **OK**.

Add WLAN

Show Advanced Settings

General Settings

☒ Enable Interface

Interface Name: wlan-1-2

Description: (Optional)

Zone: Please select one ...

Virtual Access Point Settings

SSID: ZYXEL_WPA

☐ Hide SSID Broadcast

☐ Block Intra BSS Traffic

Maximum Associations: 255

WLAN Security Settings

Security Type: WPA2-Enterprise

Authentication Type: Auth Method

Authentication Method: default

TTLS Certificate: default

IP Address Assignment

IP Address: 10.1.1.1

Subnet Mask: 255.255.0.0

Interface Parameters

Egress Bandwidth: 1048576 Kbps

DHCP Setting

DHCP: DHCP Server

IP Pool Start Address (Optional):

First DNS Server (Optional): Custom Defined

Pool Size:

Apply Reset OK Cancel

2 Turn on the wireless LAN and click **Apply**.

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

General MAC Filter

Show Advanced Settings

WLAN Device Settings

Extension Slot: slot1 ZyXEL G-1705

☒ Enable WLAN Device

802.11 Band: b+g

Channel: 6

Interface Summary

Add Edit Remove Activate Inactivate Object Reference

#	Status	Name	SSID	IP Address	Mask	Security
1	Light Bulb	wlan-1-1	ZyXEL01	10.59.1.1	255.255.255.0	none
2	Light Bulb	wlan-1-2	ZYXEL_WF	10.1.1.1	255.255.0.0	wpa2-aes-eap

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

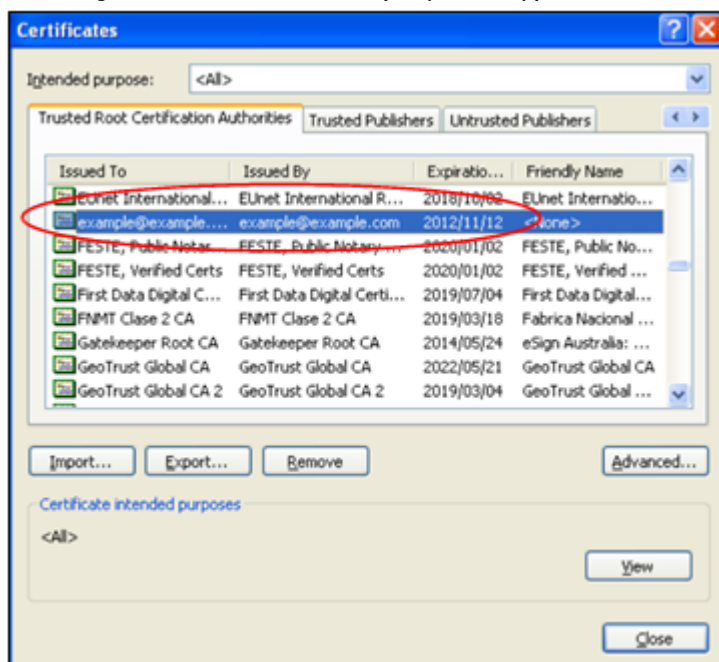
Apply Reset

4 Configure your wireless clients to connect to the wireless network.

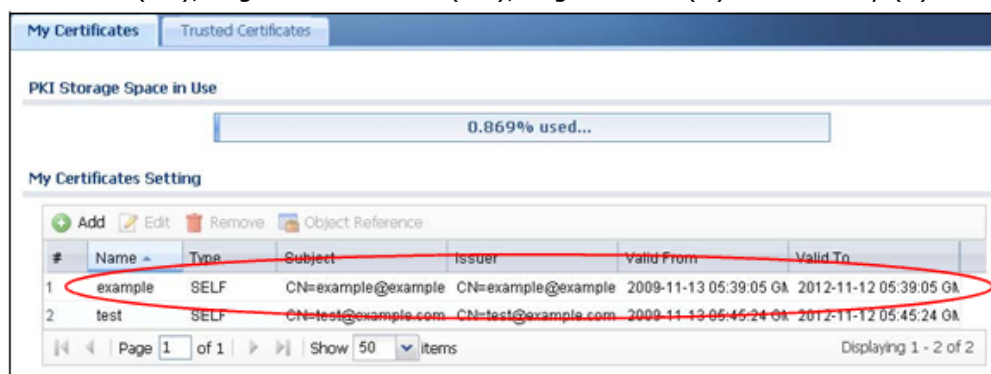
1.4.2.1 Wireless Clients Import the USG's Certificate

You must import the USG's certificate into the wireless clients if they are to validate the USG's certificate. Use the **Configuration > Object > Certificate > Edit** screen to export the certificate the USG is using for the WLAN interface. Then do the following to import the certificate into each wireless client computer:

- 1 In Internet Explorer, click **Tools > Internet Options > Content** and click the **Certificates** button.
- 2 Click **Import**.
- 3 Use the wizard screens to import the certificate. You may need to change the **Files of Type** setting to **All Files** in order to see the certificate file.
- 4 When you get to the **Certificate Store** screen, select the option to automatically select the certificate store based on the type of certificate.
- 5 If you get a security warning screen, click **Yes** to proceed.
- 6 The **Internet Explorer Certificates** screen remains open after the import is done. You can see the newly imported certificate listed in the **Trusted Root Certification Authorities** tab. The values in the **Issued To** and **Issued By** fields should match those in the USG's **My Certificates** screen's **Subject** and **Issuer** fields (respectively).



The **My Certificates** screen indicates what type of information is being displayed, such as Common Name (CN), Organizational Unit (OU), Organization (O) and Country (C).



Repeat the steps to import the certificate into each wireless client computer that is to validate the USG's certificate when using the WLAN interface.

1.4.2.2 Wireless Clients Use the WLAN Interface

Wireless clients enter their username and password when they connect to the wireless network.

1.5 How to Configure Ethernet, PPP, VLAN, Bridge and Policy Routing

The following table describes when to configure the Ethernet, PPP, VLAN, Bridge screens under **Configuration > Network > Interface** and the **Configuration > Network > Routing > Policy Routing** screen.

Table 10 Ethernet, PPP, VLAN, Bridge and Policy Routing Screen Relationships

SCREEN	DESCRIPTION
Ethernet	Configure this if any interface on the USG is connecting to an Ethernet network. Ethernet interfaces are the foundation for defining other interfaces and network policies.
PPP	Configure this if you need your service provider to provide an IP address through PPPoE or PPTP in order to access the Internet or another network.
VLAN	Configure this if you want to divide your physical networks into multiple VLANs, or your service provider or an aggregated network needs the USG to recognize the VLAN tags in the packets flowing through the USG.
Bridge	Configure this if you want the USG to combine two or multiple network segments into one single network. Although the USG is "transparent" in this mode, you can still apply security checking on packets flowing through the USG.
Policy Routing	Configure this if you want to override the USG's default routing behavior in order to send packets through the appropriate interface or VPN tunnel.

Since firmware version 3.00, the USG supports IPv6 configuration in these **Ethernet, PPP, VLAN, Bridge** and **Policy Route** screens under **Configuration > Network > Interface** and **Configuration > Network > Routing**. Basically, these are the same as the ones for IPv4 networks except the following differences:

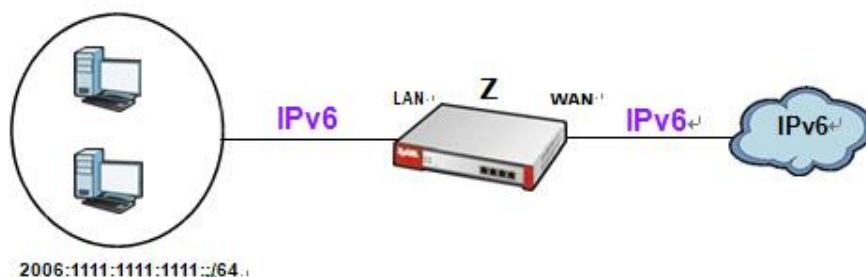
- You have to enable IPv6 globally in the **CONFIGURATION > System > IPv6** screen to make the IPv6 settings work.
- An **Enable IPv6** setting - Select this in the screens listed above to enable the USG to be able to send and receive IPv6 packets through the interface. Otherwise, the USG discards IPv6 packets flowing through the interface.
- **IPv6 Address Assignment** - This section allows you to enable auto-configuration and configure prefix delegation.
- **DHCPv6 Setting** - This section allows you to configure the DHCPv6 role and the corresponding settings for the interface.

1.6 How to Set Up IPv6 Interfaces For Pure IPv6 Routing

This example shows how to configure your USG **Z**'s WAN and LAN interfaces which connects two IPv6 networks. USG **Z** periodically advertises a network prefix of 2006:1111:1111:1111::/64 to the LAN through router advertisements.

Note: Instead of using router advertisement, you can use DHCPv6 to pass the network settings to the computers on the LAN.

Figure 22 Pure IPv6 Network Example



1.6.1 Setting Up the WAN IPv6 Interface

- 1 In the **CONFIGURATION** > **Network** > **Interface** > **Ethernet** screen's **IPv6 Configuration** section, double-click the **wan1**.
- 2 The **Edit Ethernet** screen appears. Select **Enable Interface** and **Enable IPv6**. Select **Enable Auto-Configuration**. Click **OK**.

Note: Your ISP or uplink router should enable router advertisement.

The screenshot shows the "Edit Ethernet" configuration window for the "wan1" interface. The window has a title bar with "Edit Ethernet" and standard window controls. Below the title bar, there are tabs for "IPv6 View" and "Show Advanced Settings", and a "Create new Object" button. The main content area is divided into four sections: "General Settings", "General IPv6 Setting", "Interface Properties", and "IPv6 Address Assignment". In the "General Settings" section, the "Enable Interface" checkbox is checked and circled in red. In the "General IPv6 Setting" section, the "Enable IPv6" checkbox is checked and circled in red. In the "Interface Properties" section, the "Interface Type" is set to "external", "Interface Name" is "wan1", "Port" is "P1", "Zone" is "WAN", "MAC Address" is "00:00:AA:79:73:79", and there is an optional "Description" field. In the "IPv6 Address Assignment" section, the "Enable Auto-configuration" checkbox is checked and circled in red. Below this, the "Link-Local Address" is set to "n/a", and there is an optional "IPv6 Address/Prefix Length" field.

1.6.2 Setting Up the LAN Interface

- 1 In the **CONFIGURATION > Network > Interface > Ethernet** screen, double-click the **lan1** in the **IPv6 Configuration** section.
- 2 The **Edit Ethernet** screen appears. Select **Enable Interface** and **Enable IPv6**.
Select **Enable Router Advertisement** and click **Add** and configure a network prefix for the LAN1 (2006:1111:1111:1111::/64 in this example). Click **OK**.

The screenshot shows the 'Edit Ethernet' configuration window for interface 'lan1'. The window is divided into several sections:

- General Settings:** 'Enable Interface' is checked and highlighted with a red circle.
- General IPv6 Setting:** 'Enable IPv6' is checked and highlighted with a red circle.
- Interface Properties:** Interface Type is 'internal', Interface Name is 'lan1', Port is 'P3, P4', Zone is 'LAN1', MAC Address is '00:00:AA:79:73:75', and Description is empty.
- IPv6 Address Assignment:** 'Enable Auto-configuration' is unchecked. Link-Local Address is 'n/a'. IPv6 Address/Prefix Length is empty.
- DHCPv6 Setting:** DHCPv6 is 'N/A'.
- IPv6 Router Advertisement Setting:** 'Enable Router Advertisement' is checked and highlighted with a red circle. Below this, there is a table for 'Advised Prefix Table' with one entry: '2006:1111:1111:1111::/64'. The 'Add' button is highlighted with a red circle.

You have completed the settings on the USG. But if you want to request a network address prefix from your ISP for your computers on the LAN, you can configure prefix delegation .

1.6.3 Prefix Delegation and Router Advertisement Settings

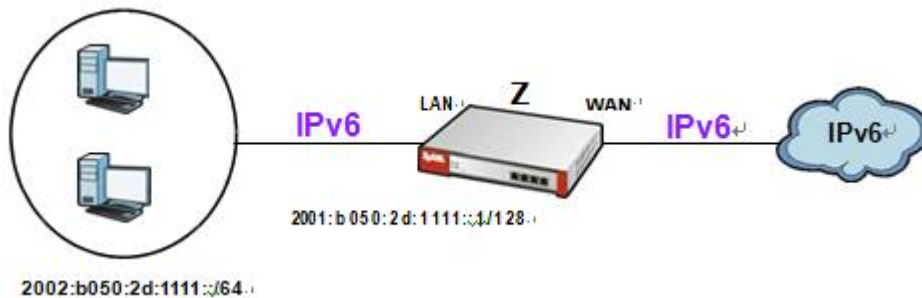
This example shows how to configure prefix delegation on the USG's WAN and router advertisement on the LAN.

1.6.3.1 Apply a Network Prefix From Your ISP

First of all, you have to apply a network prefix from your ISP or the uplink router's administrator. The WAN port's DUID is required when you apply the prefix. You can check the DUID information in the **WAN IPv6 Interface Edit** screen.

This example assumes that you were given a network prefix of 2001:b050:2d::/48 and you decide to divide it and give 2001:b050:2d:1111::/64 to the LAN network. LAN1's IP address is 2001:b050:2d:1111::1/128.

Figure 23 Pure IPv6 Network Example Using Prefix Delegation



1.6.3.2 Setting Up the WAN IPv6 Interface

- 1 In the **Configuration > Network > Interface > Ethernet** screen's **IPv6 Configuration** section, double-click the **wan1**.
- 2 The **Edit Ethernet** screen appears. Select **Enable Interface** and **Enable IPv6**. Click **Create new Object** to add a **DHCPv6 Request** object with the **Prefix Delegation** type. Select **Enable Auto-Configuration**. Select **Client** in the **DHCPv6** field. (WAN1's DUID appears.) Click **Add** in the **DHCPv6 Request Options** table and select the DHCPv6 request object you just created. You cannot see the prefix your ISP gave you in the **Value** field until you click **OK** and then come back to this screen again. It is 2001:b050:2d::/48 in this example.

Note: Your ISP or a DHCPv6 server in the same network as the WAN should assign an IPv6 IP address for the WAN interface.

Edit Ethernet

IPv6 View | Show Advanced Settings | Create new Object

General Settings

- ☒ Enable Interface

General IPv6 Setting

- ☒ Enable IPv6

Interface Properties

Interface Type: external

Interface Name: wan1

Port: P1

Zone: WAN

MAC Address: 00:00:AA:79:73:69

Description: (Optional)

IPv6 Address Assignment

- ☒ Enable Auto-configuration

Link-Local Address: fe80::200:aaff:fe79:7369/64

IPv6 Address/Prefix Length: (Optional)

DHCPv6 Setting

DHCPv6: Client

DUID: 00:03:00:01:00:00:AA:79:73:69

☐ Request Address

DHCPv6 Request Options

Add Remove Object Reference

#	Name	Type	Value
1	Request_WAN1_PD	prefix-delegation	n/a

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

1.6.3.3 Setting Up the LAN Interface

- 1 In the **Configuration > Network > Interface > Ethernet** screen, double-click the **lan1** in the **IPv6 Configuration** section.
- 2 The **Edit Ethernet** screen appears. Click **Show Advanced Settings** to display more settings on this screen.

Select **Enable Interface** and **Enable IPv6**.

In the **Address from DHCPv6 Prefix Delegation** table, click **Add** and select the DHCPv6 request object from the drop-down list, type `::1111:0:0:0:1/128` in the **Suffix Address** field. (The combined address `2001:b050:2d:1111::1/128` will display as LAN1's IPv6 address after you click **OK** and come back to this screen again).

Note: You can configure the IPv6 Address/Prefix Length field instead if the delegated prefix is never changed.

Select **Enable Router Advertisement**.

In the **Advertised Prefix from DHCPv6 Prefix Delegation** table, click **Add** and select the DHCPv6 request object from the drop-down list, type `::1111/64` in the **Suffix Address** field. (The combined prefix `2001:b050:2d:1111::/64` will display for the LAN1's network prefix after you click **OK** and come back to this screen again).

Edit Ethernet

IPv6 View • Hide Advanced Settings Create new Object

General Settings

☒ Enable Interface

General IPv6 Setting

☒ Enable IPv6

Interface Properties

Interface Type: Internal

Interface Name: lan1

Port: P1_14

Zone: (AN)

MAC Address: 00:00:AA:79:23:75

Description: (Optional)

IPv6 Address Assignment

☐ Enable Stateless Address Auto-configuration (SLAAC)

Link Local Address: n/a

IPv6 Address/Prefix Length: (Optional)

Gateway: (Optional)

Metric: (0-255)

Address from DHCPv6 Profile Delegation

#	Delegated Profile	Subnet Address	Address
1	Request_WWW_PD	::1111:0:0:0:128	n/a

Page 1 of 1 Show 50 No data to display

DHCPv6 Setting

DHCPv6: N/A

IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

☐ Advertised Hosts Get Network Configuration from DHCPv6

☐ Advertised Hosts Get Other Configuration from DHCPv6

Router Preference: Medium

MTU: 1480 (1280-1500, 0 is disabled)

Hop Limit: 64 (0-255, 0 is disabled)

Advertised Prefix Table

#	Delegated Profile	Subnet Address	Address
1	Request_WWW_PD	::1111:0:0:0:128	n/a

Page 1 of 1 Show 50 No data to display

Advertised Prefix from DHCPv6 Profile Delegation

#	Delegated Profile	Subnet Address	Address
1	Request_WWW_PD	::1111:0:0:0:128	n/a

Page 1 of 1 Show 50 No data to display

1.6.4 Test

- 1 Connect a computer to the USG's LAN1.

- 2 Enable IPv6 support on your computer.
In Windows XP, you need to use the `IPv6 install` command in a Command Prompt.
In Windows 7, IPv6 is supported by default. You can enable IPv6 in the **Control Panel > Network and Sharing Center > Local Area Connection** screen.
- 3 Your computer should get an IPv6 IP address (starting with 2001:b050:2d:1111: for this example) from the USG.
- 4 Open a web browser and type `http://www.kame.net`. If your IPv6 settings are correct, you can see a dancing turtle in the website.

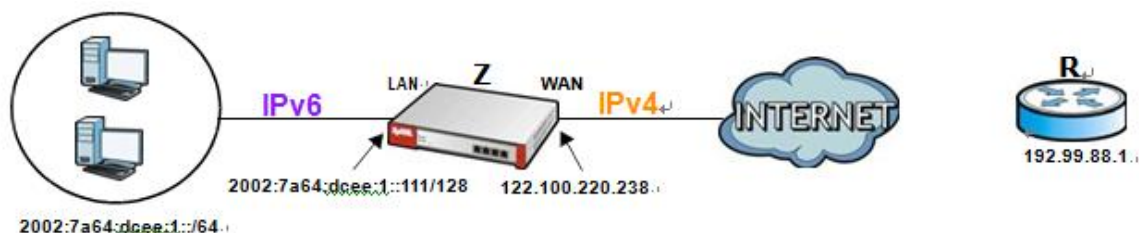
1.6.5 What Can Go Wrong?

- 1 If you forgot to enable **Auto-Configuration** on the WAN1 IPv6 interface, you will not have any default route to forward the LAN's IPv6 packets.
- 2 To use prefix delegation, you must set the WAN interface to a DHCPv6 client, enable router advertisements on the LAN interface as well as configure the **Advertised Prefix from DHCPv6 Prefix Delegation** table.
- 3 If the **Value** field in the WAN1's **DHCPv6 Request Options** table displays **n/a**, contact your ISP for further support.
- 4 In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

1.7 How to Set Up an IPv6 6to4 Tunnel

This example shows how to use the interface configuration screens to create the following 6to4 tunnel.

Figure 24 6to4 Tunnel Example



In this example, the USG (**Z**) acts as a 6to4 router which connects the IPv4 Internet (through WAN1 with an IP address of 122.100.220.238) and an IPv6 intranet network. In the 6to4 tunnel application, you must configure the LAN1 with an IP address starting with 2002:7a64:dcee::/48 if you decide to use the WAN1 IP address to forward 6to4 packets to the IPv4 network. The second and third sets of 16-bit IP address from the left must be converted from 122.100.220.238. It becomes 7a64:dcee in hexadecimal. You are free to use the fourth set of 16-bit IP address from the left in order to allocate different network addresses (prefixes) to IPv6 interfaces. In this example,

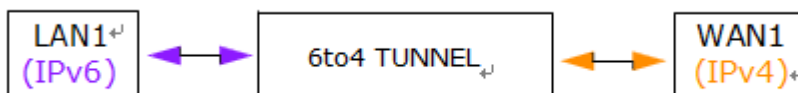
the LAN1 network address is assigned to use 2002:7a64:dcee:1::/64 and the LAN1 IP address is set to 2002:7a64:dcee:1::111/128.

A relay router **R** (192.99.88.1) is used in this example in order to forward 6to4 packets to any unknown IPv6 addresses.

1.7.1 Configuration Concept

After the 6to4 tunnel settings are complete, IPv4 and IPv6 packets transmitted between WAN1 and LAN1 will be handled by the USG through the following flow.

Figure 25 6to4 Tunnel Configuration Concept



1.7.2 Setting Up the LAN IPv6 Interface

- 1 In the **CONFIGURATION > Network > Interface > Ethernet** screen's **IPv6 Configuration** section, double-click the **lan1**.
- 2 The **Edit Ethernet** screen appears. Select **Enable Interface** and **Enable IPv6**.

Type **2002:7a64:dcee:1::111/128** in the **IPv6 Address/Prefix Length** field for the LAN1's IP address.

Enable **Router Advertisement**. Then click **Add** in the **Advertised Prefix Table** to add **2002:7a64:dcee:1::/64**. The LAN1 hosts will get the network prefix through the router advertisement messages sent by the LAN1 IPv6 interface periodically. Click **OK**.

General Settings

☒ Enable Interface

General IPv6 Setting

☒ Enable IPv6

Interface Properties

Interface Type: internal

Interface Name: lan1

Port: P2, P3

Zone: LAN1

MAC Address: 00:00:AA:79:73:6A

Description: (Optional)

IPv6 Address Assignment

☐ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: fe80::200:aaff:fe79:736a/64

IPv6 Address/Prefix Length: 2002:7a64:dcee:1::111 (Optional)

DHCPv6 Setting

DHCPv6: N/A

IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

Router Preference: Medium

Advertised Prefix Table

#	IPv6 Address/Prefix Length
1	2002:7a64:dcee:1::/64

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

1.7.3 Setting Up the 6to4 Tunnel

- 1 Click **Add** in the **CONFIGURATION > Network > Interface > Tunnel** screen.
- 2 The **Add Tunnel** screen appears. Select **Enable**.
Enter **tunnel0** as the **Interface Name** and select **6to4** as the **Tunnel Mode**.
In the **6to4 Tunnel Parameter** section, this example just simply uses the default **6to4 Prefix**, 2002::/16. Enter your relay router's IP address (192.88.99.1 in this example).
Select **wan1** as the gateway. Click **OK**.

Add Tunnel

Show Advanced Settings

General Settings

☒ Enable

Interface Properties

Interface Name: tunnel0

Zone: TUNNEL

Tunnel Mode: 6to4

IPv6 Address Assignment

IPv6 Address/Prefix Length: (Optional)

Metric: 0 (0-15)

6to4 Tunnel Parameter

6to4 Prefix: 2002::/16

Relay Router: 192.88.99.1 (Optional)

NOTE: traffic destined to the non-6to4 prefix domain tunnels to the relay router

Gateway Settings

My Address

☒ Interface wan1 DHCP client -- 122.100.220.238/255.255.255.0

☐ IP Address 0.0.0.0

Remote Gateway Address: Automatic

1.7.4 Testing the 6to4 Tunnel

- 1 Connect a computer to the USG's LAN1.
- 2 Enable IPv6 support on you computer.
In Windows XP, you need to use the `IPv6 install` command in a Command Prompt.
In Windows 7, IPv6 is supported by default. You can enable IPv6 in the **Control Panel > Network and Sharing Center > Local Area Connection** screen.
- 3 You should get an IPv6 IP address starting with 2002:7a64:dcee:1:.
- 4 Type `ping -6 ipv6.google.com` in a Command Prompt to test. You should get a response.

1.7.5 What Can Go Wrong?

- 1 Do not enable Auto-Configuration for the LAN1 IPv6 interface. Enabling it will cause two default routes, however, the USG only needs a default route generated by your relay router setting.
In 6to4, the USG doesn't need a policy route to determine where to forward a 6to4 packet (starting with 2002 in the IPv6 IP address). The next gateway information of where to forward a 6to4 packet can be retrieved from the packet's destination IP address. The USG only forwards a 6to4 packet to the relay router using the default route if the packet's destination is not an IP address starting with 2002.
- 2 You don't need to activate the WAN1 IPv6 interface but make sure you enable the WAN1 IPv4 interface. In 6to4, the USG uses the WAN1 IPv4 interface to forward your 6to4 packets over the IPv4 network.

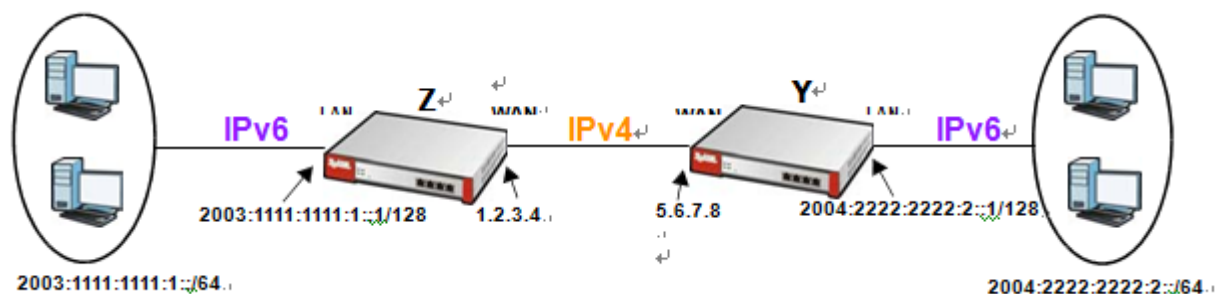
Note: For 6to4, you do not need to enable IPv6 in the wan1 since the IPv6 packets will be redirected into the 6to4 tunnel.

- 3 In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

1.8 How to Set Up an IPv6-in-IPv4 Tunnel

This example shows how to use the interface and policy route configuration screens to create an IPv6-in-IPv4 tunnel.

Figure 26 IPv6-in-IPv4 Tunnel Example



In this example, the USGs (**Z** and **Y**) act as IPv6-in-IPv4 routers which connect the IPv4 Internet and an individual IPv6 network. This configuration example only shows the settings on USG **Z**. You can use similar settings to configure USG **Y**.

Note: In the IPv6-in-IPv4 tunnel application, you must configure the peer gateway's WAN IPv4 address as the remote gateway IP.

1.8.1 Configuration Concept

After the IPv6-in-IPv4 tunnel settings are complete, IPv4 and IPv6 packets transmitted between WAN1 and LAN1 will be handled by the USG through the following flow.

Figure 27 IPv6-in-IPv4 Tunnel Configuration Concept



1.8.2 Setting Up the IPv6-in-IPv4 Tunnel

- 1 Click **Add** in the **CONFIGURATION** > **Network** > **Interface** > **Tunnel** screen.

- 2 The **Edit Tunnel** screen appears. Select **Enable**.
Enter **tunnel0** as the **Interface Name** and select **IPv6-in-IPv4** as the **Tunnel Mode**.
Select **wan1** in the **Interface** field in the **Gateway Settings** section.
Enter **5.6.7.8** as the remote gateway's IP address. Click **OK**.

The screenshot shows the 'Edit Tunnel' configuration window. The 'General Settings' section has the 'Enable' checkbox checked. The 'Interface Properties' section shows 'Interface Name' as 'tunnel0', 'Zone' as 'TUNNEL', and 'Tunnel Mode' as 'IPv6-in-IPv4'. The 'IPv6 Address Assignment' section has 'IPv6 Address/Prefix Length' and 'Metric' (0) fields. The 'Gateway Settings' section has 'My Address' set to 'Interface' (wan1) and 'Remote Gateway Address' set to '5.6.7.8'. Red circles highlight the 'Enable' checkbox, 'tunnel0', 'IPv6-in-IPv4', 'wan1', and '5.6.7.8'.

1.8.3 Setting Up the LAN IPv6 Interface

- 1 Select lan1 in the **IPv6 Configuration** section in the **CONFIGURATION > Network > Interface > Ethernet** screen and click **Edit**.
- 2 The **Edit Ethernet** screen appears. Select **Enable Interface** and **Enable IPv6**.
Type **2003:1111:1111:1::1/128** in the **IPv6 Address/Prefix Length** field for the LAN1's IP address.
Enable **Router Advertisement**. Then click **Add** in the **Advertised Prefix Table** to add **2003:1111:1111:1::/64**. The LAN1 hosts will get the network prefix through router advertisements sent by the LAN1 IPv6 interface periodically. Click **OK**.

Edit Ethernet

IPv6 View | Show Advanced Settings | Create new Object

General Settings

☒ Enable Interface

General IPv6 Setting

☒ Enable IPv6

Interface Properties

Interface Type: internal

Interface Name: lan1

Port: P2, P3

Zone: LAN1

MAC Address: 00:00:AA:79:73:6A

Description: (Optional)

IPv6 Address Assignment

☐ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: fe80::200:aaff:fe:79:736a/64

IPv6 Address/Prefix Length: 2003::1111:1111:1::1/64 (Optional)

DHCPv6 Setting

DHCPv6: N/A

IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

Router Preference: Medium

Advertised Prefix Table

	IPv6 Address/Prefix Length
1	2003:1111:1111:1::/64

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

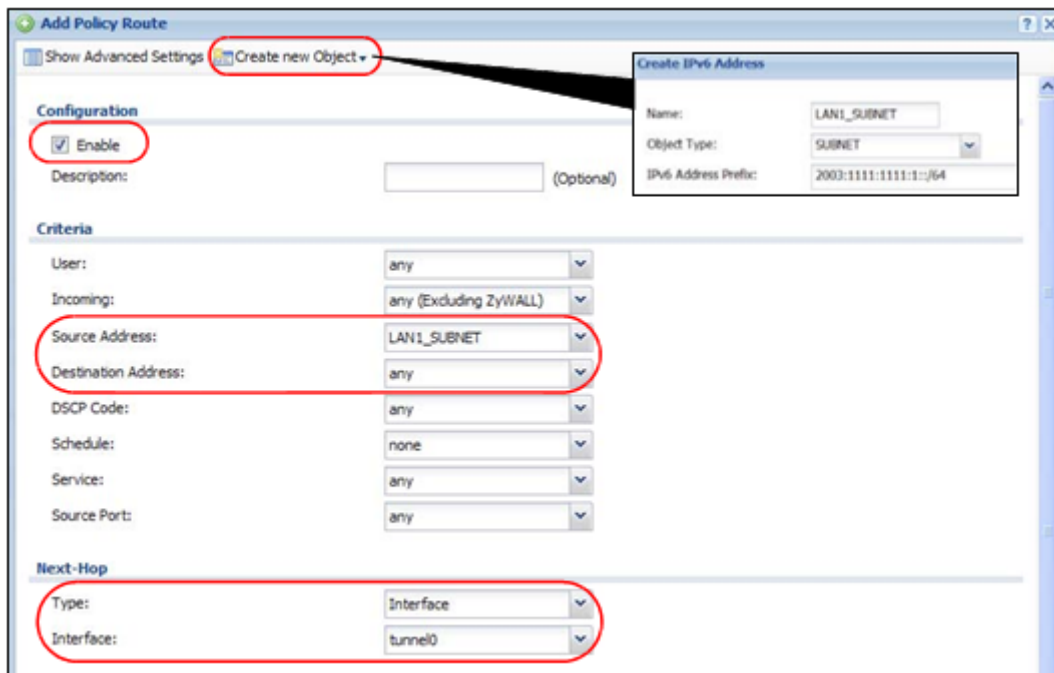
1.8.4 Setting Up the Policy Route

- 1 Go to the **CONFIGURATION > Network > Routing** screen and click **Add** in the **IPv6 Configuration** table.
- 2 The **Add Policy Route** screen appears. Click **Create New Object** to create an IPv6 address object with the address prefix of **2003:1111:1111:1::/64**.
Select **Enable**.

Select the address object you just created in the **Source Address** field.

Select **any** in the **Destination Address** field.

Select **Interface** as the next-hop type and then **tunnel0** as the interface. Click **OK**.



1.8.5 Testing the IPv6-in-IPv4 Tunnel

- 1 Connect a computer to the USG's LAN1.
- 2 Enable IPv6 support on your computer.
In Windows XP, you need to use the `IPv6 install` command in a Command Prompt.
In Windows 7, IPv6 is supported by default. You can enable IPv6 in the **Control Panel > Network and Sharing Center > Local Area Connection** screen.
- 3 You should get an IPv6 IP address starting with `2003:1111:1111:1000::`.
- 4 Use the `ping -6 [IPv6 IP address]` command in a Command Prompt to test whether you can ping a computer behind USG Y. You should get a response.

1.8.6 What Can Go Wrong?

- 1 You don't need to activate the WAN1 IPv6 interface but make sure you enable the WAN1 IPv4 interface. In IPv6-in-IPv4, the USG uses the WAN1 IPv4 interface to forward your 6to4 packets to the IPv4 network.
- 2 In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

Tutorial 2: Protecting Your Network

These sections cover configuring the USG to protect your network.

2.1 Firewall

The firewall controls the travel of traffic between or within zones for services using static port numbers. Use application patrol to control services using flexible/dynamic port numbers. The firewall can also control traffic for NAT (DNAT) and policy routes (SNAT). Firewall rules can use schedule, user, user groups, address, address group, service, and service group objects. To-USG firewall rules control access to the USG itself including management access. By default the firewall allows various types of management from the LAN, HTTPS from the WAN and no management from the DMZ. The firewall also limits the number of user sessions.

This example shows the USG's default firewall behavior for WAN to LAN traffic and how stateful inspection works. A LAN user can initiate a Telnet session from within the LAN zone and the firewall allows the response. However, the firewall blocks Telnet traffic initiated from the WAN zone and destined for the LAN zone. The firewall allows VPN traffic between any of the networks.

Figure 28 Default Firewall Action



2.1.1 What Can Go Wrong

- The USG checks the firewall rules in order and applies the first firewall rule the traffic matches. If traffic is unexpectedly blocked or allowed, make sure the firewall rule you want to apply to the traffic comes before any other rules that the traffic would also match.
- Even if you have configured the firewall to allow access for a management service such as HTTP, you must also enable the service in the service control rules.
- The USG is not applying your firewall rules for certain interfaces. The USG only apply's a zone's rules to the interfaces that belong to the zone. Make sure you assign the interfaces to the appropriate zones. When you create an interface, there is no security applied on it until you assign it to a zone.

2.2 User-aware Access Control

You can configure many policies and security settings for specific users or groups of users. Users can be authenticated locally by the USG or by an external (AD, RADIUS, or LDAP) authentication server. Here is how to have the USG use a RADIUS server to authenticate users before giving them access.

- 1 Set up user accounts in the RADIUS server.
- 2 Set up user accounts and groups on the USG (**Configuration > Object > User/Group**).
- 3 Configure an object for the RADIUS server. Click **Configuration > Object > AAA Server > RADIUS** and double-click the **radius** entry.
- 4 Then, set up the authentication method, Click **Configuration > Object > Auth. Method**. Double-click the **default** entry. Click the **Add** icon.
- 5 Configure the USG's security settings. The USG can use the authentication method in authenticating wireless clients, HTTP and HTTPS clients, IPSec gateways (extended authentication), L2TP VPN, and authentication policy.

2.2.1 What Can Go Wrong

- The USG always authenticates the default **admin** account locally, regardless of the authentication method setting. You cannot have the RADIUS server authenticate the USG's default admin account.
- The authentication attempt will always fail if the USG tries to use the local database to authenticate an **ext-user**. An external server such as AD, LDAP or RADIUS must authenticate the ext-user accounts.
- Attempts to add the admin users to a user group with access users will fail. You cannot put

access users and admin users in the same user group.

- Attempts to add the default admin account to a user group will fail. You cannot put the default **admin** account into any user group.

2.3 Device and Service Registration

This tutorial shows you how to create a myZyXEL.com account and register the USG. You can then activate your service subscription.

- 1 You can directly create a myZyXEL.com account and register the USG on the **Registration** screen. Click **Configuration > Licensing > Registration** to open the following screen. Select **new myZyXEL.com account**. Fill in the fields marked in red in this screen. Click **Apply** to create your account and register the device.

The screenshot shows the 'Registration' screen with two tabs: 'Registration' and 'Service'. Under 'General Settings', there is a message: 'This device is not registered to myZyXEL.com. Please enter information below to register your device. If you don't have myZyXEL.com account, please select "new myZyXEL.com account" below. If you have a myZyXEL.com account, but you forget your User Name or Password, please go to www.myZyXEL.com for help.' Below this, there are two radio buttons: 'new myZyXEL.com account' (selected) and 'existing myZyXEL.com account'. A red box highlights the 'new myZyXEL.com account' radio button and the input fields for 'User Name', 'Password', 'Confirm Password', 'E-Mail Address', and 'Country'. A 'Check' button is next to the 'User Name' field with the text 'you can click to check if username exists'.

- 2 Click the **Service** tab. To activate or extend a standard service subscription enter your iCard's license key in the **License Key** field. The license key can be found on the reverse side of the iCard.

The screenshot shows the 'Service' screen with two tabs: 'Registration' and 'Service'. Under 'License Status', there is a table with the following data:

#	Service	Status	Registration Type	Expiration Date	Count
1	Anti-Virus Signature Service	Not Licensed			N/A
2	IDP/AppPatrol Signature Service	Not Licensed			N/A
3	Anti-Spam Service	Not Licensed			N/A
4	CommTouch Content Filter Service	Not Licensed			N/A
5	BlueCoat Content Filter Service	Not Licensed			N/A
6	SSL VPN Service	Not Licensed			2

Below the table, there is a pagination bar: 'Page 1 of 1', 'Show 50 Items', and 'Displaying 1 - 6 of 6'. Under 'License Activation', there is a 'License Key' input field and an 'Activation' button, both highlighted with a red box. There is also a 'Service License Refresh' button.

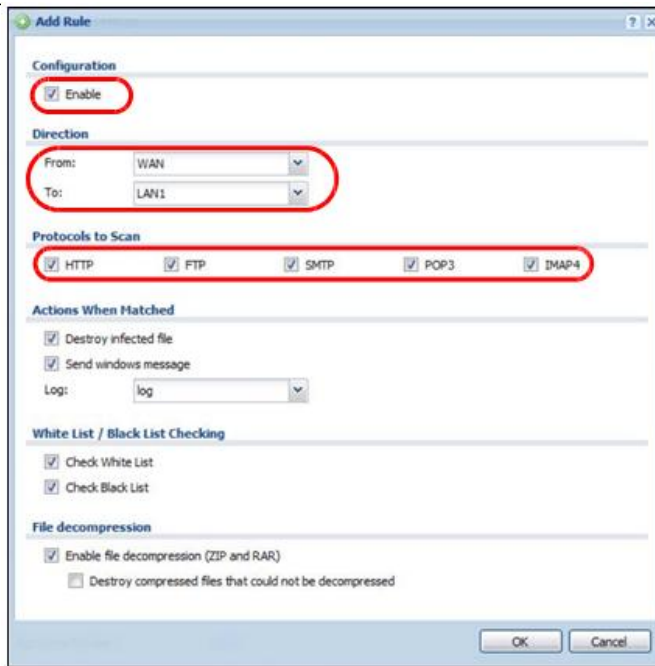


2.4 Anti-Virus Policy Configuration

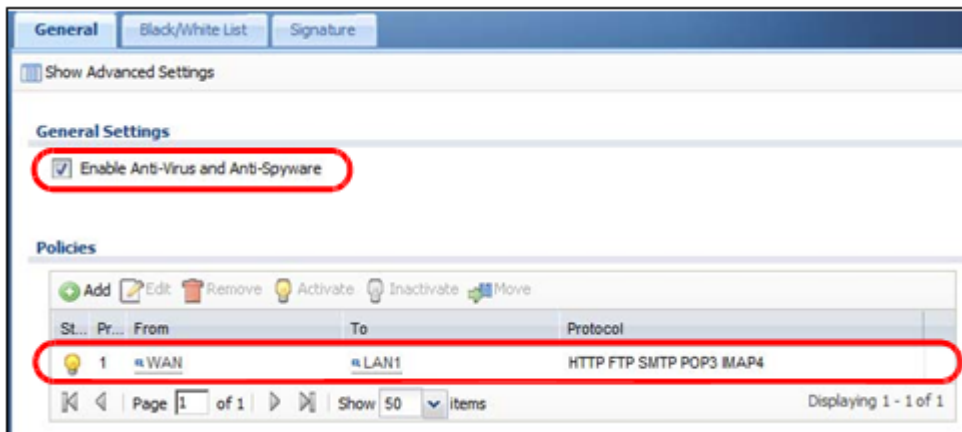
This tutorial shows you how to configure an Anti-Virus policy.

Note: You need to first activate your Anti-Virus service license or trial. See

- 1 Click **Configuration > Anti-X > Anti-Virus** to display the Anti-Virus **General** screen. In the **Policies** section click **Add** to display the **Add Rule** screen. Select **Enable**. In the **Direction** section, you can select the **From** and **To** zones for traffic to scan for viruses. You can also select traffic types to scan for viruses under **Protocols to Scan**. Click **OK**.



- 2 The policy configured in the previous step will display in the **Policies** section. Select **Enable Anti-Virus and Anti-Spyware** and click **Apply**.



2.4.1 What Can Go Wrong

- The USG does not scan the following file/traffic types:
 - Simultaneous downloads of a file using multiple connections. For example, when you use FlashGet to download sections of a file simultaneously.
 - Encrypted traffic. This could be password-protected files or VPN traffic where the USG is not the endpoint (pass-through VPN traffic).
 - Traffic through custom (non-standard) ports. The only exception is FTP traffic. The USG scans whatever port number is specified for FTP in the ALG screen.
 - ZIP file(s) within a ZIP file.

2.5 IDP Profile Configuration

IDP (Intrusion, Detection and Prevention) detects malicious or suspicious packets and protects against network-based intrusions.

Note: You need to first activate your IDP service license or trial.

You may want to create a new profile if not all signatures in a base profile are applicable to your network. In this case you should disable non-applicable signatures so as to improve USG IDP processing efficiency.

You may also find that certain signatures are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the USG. As each network is different, false positives and false negatives are common on initial IDP deployment.

You could create a new 'monitor profile' that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have been reduced to an acceptable level, you could then create an 'inline profile' whereby you configure appropriate actions to be taken when a packet matches a signature.

2.5.1 Procedure To Create a New Profile

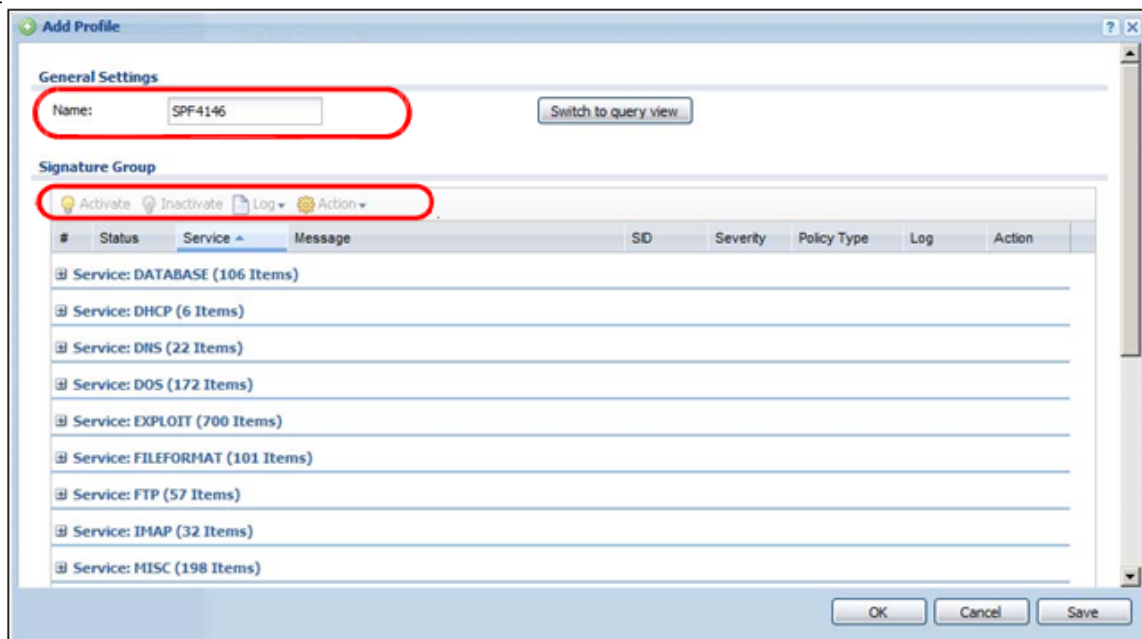
To create a new profile:

- 1 Click **Configuration > Anti-X > IDP > Profile** and in the **Profile Management** section of this screen, click the **Add** icon. A pop-up screen will appear allowing you to choose a base profile. Select a base profile to go to the profile details screen.



Note: If Internet Explorer opens a warning screen about a script making Internet Explorer run slowly and the computer maybe becoming unresponsive, just click **No** to continue.

- 2 Type a new profile **Name**. Enable or disable individual signatures by selecting a row and clicking **Activate** or **Inactivate**. Click **OK**.



- 3 Edit the default log options and actions.

2.6 ADP Profile Configuration

ADP (Anomaly Detection and Prevention) protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal traffic flows such as port scans.

You may want to create a new profile if not all traffic or protocol rules in a base profile are applicable to your network. In this case you should disable non-applicable rules so as to improve USG ADP processing efficiency.

You may also find that certain rules are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the USG. As each network is different, false positives and false negatives are common on initial ADP deployment.

You could create a new 'monitor profile' that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you're satisfied that they have been reduced to an acceptable level, you could then create an 'inline profile' whereby you configure appropriate actions to be taken when a packet matches a detection.

2.6.1 Procedure To Create a New ADP Profile

To create a new profile:

- 1 Click **Configuration > Anti-X > ADP > Profile** and in the **Profile Management** section of this screen, click the **Add** icon. A pop-up screen will appear allowing you to choose a base profile. Select a base profile to go to the profile details screen.



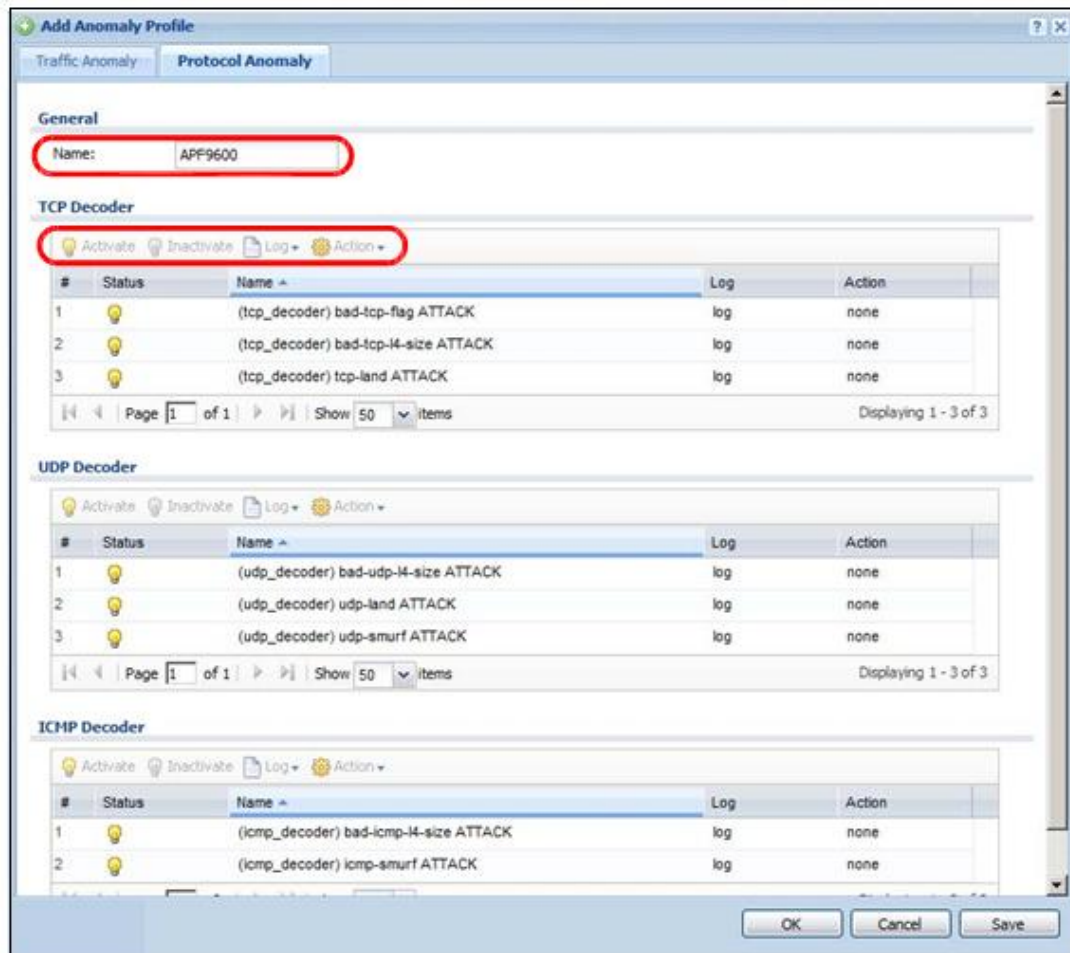
Note: If Internet Explorer opens a warning screen about a script making Internet Explorer run slowly and the computer maybe becoming unresponsive, just click **No** to continue.

- 2 The **Traffic Anomaly** screen will display. Type a new profile **Name**. Enable or disable individual scan or flood types by selecting a row and clicking **Activate** or **Inactivate**. Selecting different levels in the **Sensitivity** drop-down menu adjusts levels for scan thresholds and sample times. Edit the default log options and actions by selecting a row and making a selection in the **Log** or **Action** drop-down menus. Click **OK**.

#	Status	Name	Log	Action
1	⚡	(portscan) TCP Portscan	log	none
2	⚡	(portscan) TCP Portscan Fin	log	none
3	⚡	(portscan) TCP Portscan Syn	log	none
4	⚡	(portscan) UDP Portscan	log	none
5	⚡	(sweep) TCP Port Sweep	log	none

#	Status	Name	Log	Action	Threshold(pkt/sec)
1	⚡	(flood) ICMP Flood	log	none	1000

- 3 Click the **Protocol Anomaly** tab. Type a new profile **Name**. Enable or disable individual rules by selecting a row and clicking **Activate** or **Inactivate**. Edit the default log options and actions by selecting a row and making a selection in the **Log** or **Action** drop-down menus. Click **OK**.



2.7 Content Filter Profile Configuration

Content filter allows you to control access to specific web sites or filter web content by checking against an external database. This tutorial shows you how to configure a Content Filter profile.

Note: You need to first activate your Content Filter service license or trial to use Commtouch or BlueCoat content filtering service.

- 1 You will first configure a content filter profile. Click **Configuration > Anti-X > Content Filter > Filter Profile > Add** to open the following screen. Enter a profile **Name** and select **Enable Content Filter Category Service** and select desired actions for the different web page categories. Then select the categories to include in the profile or select **Select All Categories**. Click **Apply**.

General Settings

License Status: Licensed

License Type: Trial

Name: BlueCoat

☒ Enable Content Filter Category Service

Action for Unsafe Web Pages: Warn ☐ Log

Action for Managed Web Pages: Block ☐ Log

Action for Unrated Web Pages: Warn ☐ Log

Action When Category Server Is Unavailable: Warn ☐ Log

Select Categories

☒ Select All Categories ☐ Clear All Categories

- 2 Click the **General** tab and in the **Policies** section click **Add**. In the **Add Policy** screen that appears, select the **Filter Profile** you created in the previous step. Click **OK**.

Add Policy

Create new Object ▾

☒ Enable Policy

Schedule: none ▾

Address: any ▾

Filter Profile: BlueCoat ▾

User/Group: any ▾

OK Cancel

- 3 In the **General** screen, the configured policy will appear in the **Policies** section. Select **Enable Content Filter** and select **BlueCoat**. Then select **Enable Content Filter Report Service** to collect content filtering statistics for reports. Click **Apply**.

General Filter Profile Trusted Web Sites Forbidden Web Sites

General Settings

☒ Enable Content Filter

☐ Commtouch

☒ BlueCoat

☒ Enable Content Filter Report Service Report Server ⓘ

Content Filter Category Service Timeout: 10 (1~60 Seconds)

Content Filter Port

Add Edit Remove

#	Port
1	80

Policies

☐ Block web access when no policy is applied

Add Edit Remove Activate Inactivate Move

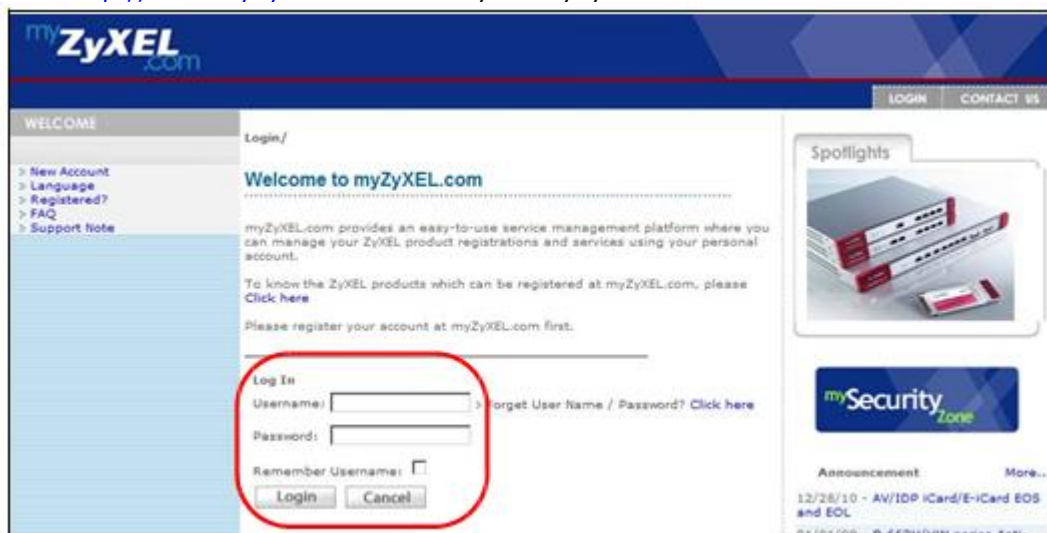
#	Status	Address	Schedule	User	Filter Profile
1	⚡	any	none	any	BlueCoat

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

2.8 Viewing Content Filter Reports

Content filtering reports are generated statistics and charts of access attempts to web sites belonging to the categories you selected in your device content filter screen. You need to register your iCard before you can view content filtering reports. Alternatively, you can also view content filtering reports during the free trial (up to 30 days).

- 1 Go to <http://www.myZyXEL.com>. Fill in your myZyXEL.com account information and click **Login**.



myZyXEL.com

WELCOME

Login/

Welcome to myZyXEL.com

myZyXEL.com provides an easy-to-use service management platform where you can manage your ZyXEL product registrations and services using your personal account.

To know the ZyXEL products which can be registered at myZyXEL.com, please [Click here](#).

Please register your account at myZyXEL.com first.

Log In

Username: [Forgot User Name / Password? Click here](#)

Password:

Remember Username: ☐

Login Cancel

Spotlights

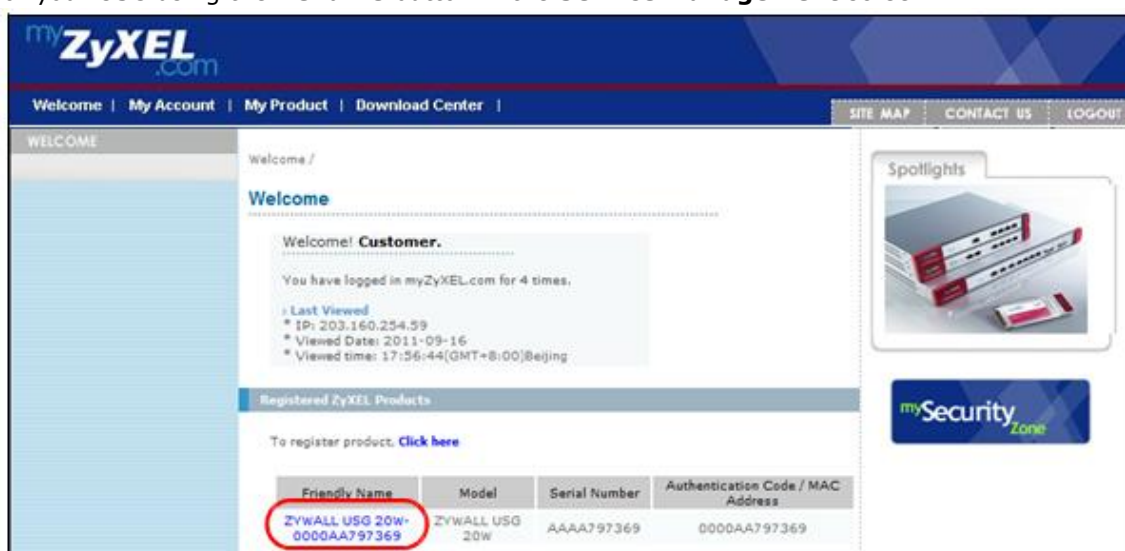
mySecurity Zone

Announcement More...

12/28/10 - AV10P iCard/E-Card EOS and EOL

01/05/09 - B-6674/10W series 801

- 2 A welcome screen displays. Click your USG's model name and/or MAC address under **Registered ZyXEL Products** (the USG 20W is shown as an example here). You can change the descriptive name for your USG using the **Rename** button in the **Service Management** screen.



myZyXEL.com

Welcome | My Account | My Product | Download Center |

SITE MAP CONTACT US LOGOUT

WELCOME

Welcome /

Welcome

Welcome! Customer.

You have logged in myZyXEL.com for 4 times.

Last Viewed

* IP: 203.160.254.59

* Viewed Date: 2011-09-16

* Viewed time: 17:56:44(GMT+8:00)Beijing

Registered ZyXEL Products

To register product, [Click here](#)

Friendly Name	Model	Serial Number	Authentication Code / MAC Address
ZYWALL USG 20W-0000AA797369	ZYWALL USG 20W	AAAA797369	0000AA797369

Spotlights

mySecurity Zone

- 3 In the **Service Management** screen click **Content Filter (BlueCoat)** or **Content Filter (CommTouch)** in the **Service Name** column to open the content filter reports screens.

My Products / Service Activation

Service Management

Product Information

ZYWALL USG 20W-0000AA797369

Serial Number: AAAA797369
Products: ZYWALL USG 20W
Authentication Code / MAC Address: 0000AA797369
Activation Key: N/A

[Edit Reseller Information](#)

Reseller Business Name:
Reseller Email:
Reseller Phone Number:
VAT Number:

Manage Product

Manage this product's registration by clicking on the appropriate buttons below

> ZYWALL USG 20W-0000AA797369 [Rename](#) [Transfer](#)

Available Service List

To enable your service(s), please click "Activate" shown below to enter your license key(s).

	Service Name	Service Activation	Service Type	Status	Expiration Date	Remark
1	Content Filter(BlueCoat)-Applied	Upgrade	Trial	Installed	2011-09-30 extends to 2012-09-30	-
2	Content Filter(CommTouch)	Upgrade	Trial	Installed	2011-09-30 extends to 2012-09-30	-

- 4 In the **Web Filter Home** screen, click **CommTouch Report** or **BlueCoat Report**.

ZyXEL **comintouch** Real Security. In Real Time. **Powered By BlueCoat** [Technical Support](#)

Web Filter Home

Welcome

You're protected by Web Filtering. Web Filtering provides you the ability to control what web sites can be accessed on your home or business PC. Web Filter allows you to modify blocked categories and view reports of Internet activity.

REPORTS:

Track Internet activity by viewing user reports, including site violations.

Click links below to enter CommTouch / BlueCoat reports:

[▶ CommTouch Report](#)

[▶ BlueCoat Report](#)

- 5 Select items under **Global Reports** to view the corresponding reports.

ZyXEL **comintouch** Real Security. In Real Time. **Powered By BlueCoat** [Technical Support](#)

CommTouch Reports

[Report Home](#) | [Global Reports](#)

Report Home

Report Navigation

Global reports provide You with an overview of all your Internet use.

Global Reports

[Allowed/Blocked](#)

[Categories](#)

[URLs](#)

- 6 Select a time period in the **Date Range** field, either **Allowed** or **Blocked** in the **Action Taken** field and a category (or enter the user name if you want to view single user reports) and click **Run Report**.

The screens vary according to the report type you selected in the **Report Home** screen.

- 7 A chart and/or list of requested web site categories display in the lower half of the screen.



- 8 You can click a category in the **Categories** report or click **URLs** in the **Report Home** screen to see the URLs that were requested.

ZyXEL **comintouch** **BlueCoat** **Technical Support**

Global Reports - URLs

This report displays allowed or blocked URLs requested within a specific category.

Date Range: Last 24 Hours
Action taken: Allowed
Category: Email
Run Report

URLs Requested for category: Email

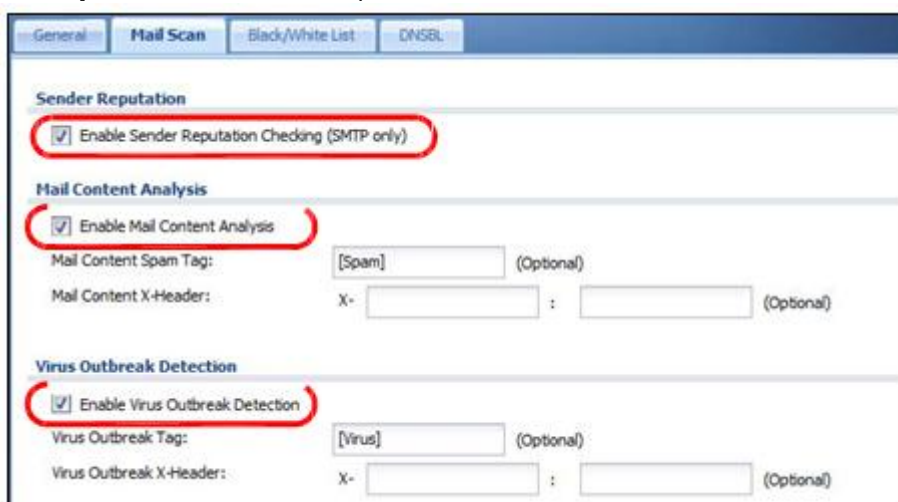
Item #	URL	Number of Requests	Open Web Page
1	www.mail.yahoo.com/	10	
2	mail.yahoo.com/	10	
3	mail.google.com/a/stam.com.my/	10	
4	mail.google.com/mail/	9	
5	mail.google.com/mail/?ui=2&view=bs&over=1qyapcunrkyv	9	

2.9 Anti-Spam Policy Configuration

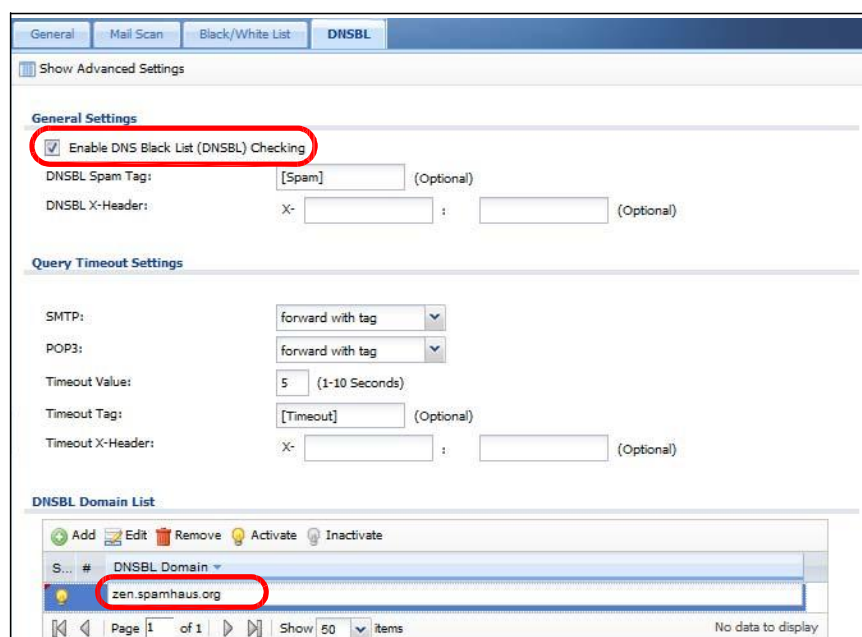
This tutorial shows you how to configure an Anti-Spam policy with Mail Scan functions and DNS Black List (DNSBL).

Note: You need to first activate your Anti-Spam service license or trial to use the Mail Scan functions (Sender Reputation, Mail Content Analysis and Virus Outbreak Detection).

- 1 To use the Mail Scan functions (Sender Reputation, Mail Content Analysis and Virus Outbreak Detection) you need to enable them in the **Mail Scan** screen. Click **Configuration > Anti-X > Anti-Spam > Mail Scan** to open this screen. Enable the desired Mail Scan functions. Click **Apply**.



- 2 To configure DNS Black List (DNSBL), click the **DNSBL** tab. Select **Enable DNS Black List (DNSBL) Checking**. In the **DNSBL Domain** section click **Add**. Enter the **DNSBL Domain** for a DNSBL service. In this example, **zen.spamhaus.org** is used. Click **Apply**.



- 3 Click the **General** tab. In the **Policy Summary** section, click **Add** to display the **Add rule** screen. Select from the list of available **Scan Options** and click **OK** to return to the **General** screen.

Add rule

General Settings

☒ Enable Policy

Log: i

Email Direction

From:

To:

Protocols to Scan

☒ SMTP ☒ POP3

Scan Options

☒ Check White List

☒ Check Black List

☒ Check IP Reputation (SMTP only)

☒ Check Mail Content

☒ Check Virus Outbreak

☒ Check DNSBL

Actions For Spam Mail i

SMTP:

POP3:

OK Cancel

- 4 In the **General** screen, the policy configured in the previous step will display in the **Policy Summary** section. Select **Enable Anti-Spam** and click **Apply**.

General Mail Scan Black/White List DNSBL

Show Advanced Settings

General Settings

☒ Enable Anti-Spam

Policy Summary

+ Add E Edit X Remove i Activate i Inactivate M Move

St...	Pri...	From	To	Protocol	Scan Options
i	1	any	any	smtp, pop3	WL, BL, IP Reputation, Mail Content, Virus Outbre...

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

Tutorial 3: Create Secure Connections Across the Internet

These sections cover using VPN to create secure connections across the Internet.

3.1 IPSec VPN

Besides using the VPN quick setup wizard to configure settings for an IPSec VPN tunnel, you can use the **Configuration > VPN > IPSec VPN** screens to configure and activate or deactivate VPN gateway and IPSec VPN connection policies. You can also connect or disconnect IPSec VPN connections.

- Use the **VPN Gateway** screens to manage the USG's VPN gateways. A VPN gateway specifies the IPSec routers at either end of a VPN tunnel and the IKE SA settings (phase 1 settings). You can also activate or deactivate each VPN gateway.
- Use the **VPN Connection** screens to specify which IPSec VPN gateway an IPSec VPN connection policy uses, which devices behind the IPSec routers can use the VPN tunnel, and the IPSec SA settings (phase 2 settings). You can also activate or deactivate and connect or disconnect each VPN connection (each IPSec SA).

3.1.1 Test the VPN Connection

After you configure the VPN gateway and VPN connection settings, set up the VPN settings on the peer IPsec router and try to establish the VPN tunnel. To trigger the VPN, either try to connect to a device on the peer IPsec router's LAN or click **Configuration > VPN > IPsec VPN > VPN Connection** and use the VPN connection screen's **Connect** icon.

3.1.2 Configure Security Policies for the VPN Tunnel

You configure security policies based on zones. The new VPN connection was assigned to the IPsec_VPN zone. By default, there are no security restrictions on the IPsec_VPN zone, so, next, you should set up security policies that apply to the IPsec_VPN zone.

3.1.3 What Can Go Wrong

If the IPsec tunnel does not build properly, the problem is likely a configuration error at one of the IPsec routers. Log into both IPsec routers and check the settings in each field methodically and slowly. Make sure both the USG and remote IPsec router have the same security settings for the VPN tunnel. It may help to display the settings for both routers side-by-side.

Here are some general suggestions.

- The system log can often help to identify a configuration problem.
- If you enable NAT traversal, the remote IPsec device must also have NAT traversal enabled.
- Both routers must use the same authentication method to establish the IKE SA.
- Both routers must use the same negotiation mode, encryption algorithm, authentication algorithm, and DH key group.
- When using manual keys, both routers must use the same encryption key and authentication key.
- When using pre-shared keys, both routers must use the same pre-shared key.
- The USG's local and peer ID type and content must match the remote IPsec router's peer and local ID type and content, respectively.
- Both routers must use the same active protocol, encapsulation, and SPI.
- If the sites are/were previously connected using a leased line or ISDN router, physically disconnect these devices from the network before testing your new VPN connection. The old route may have been learnt by RIP and would take priority over the new VPN connection.
- To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other.
Before doing so, ensure that both computers have Internet access (via the IPsec routers).
- It is also helpful to have a way to look at the packets that are being sent and received by the USG and remote IPsec router (for example, by using a packet analyzer such as Wireshark). Check

the configuration for the following USG features.

- Make sure the To-USG firewall rules allow IPsec VPN traffic to the USG. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- The USG supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the To-USG firewall rules allow UDP port 4500 too.
- Make sure regular firewall rules allow traffic between the VPN tunnel and the rest of the network. Regular firewall rules check packets the USG sends before the USG encrypts them and check packets the USG receives after the USG decrypts them. This depends on the zone to which you assign the VPN tunnel and the zone from which and to which traffic may be routed.
- If you set up a VPN tunnel across the Internet, make sure your ISP supports AH or ESP (whichever you are using).
- If you have the USG and remote IPsec router use certificates to authenticate each other, You must set up the certificates for the USG and remote IPsec router first and make sure they trust each other's certificates. If the USG's certificate is self-signed, import it into the remote IPsec router. If it is signed by a CA, make sure the remote IPsec router trusts that CA. The USG uses one of its **Trusted Certificates** to authenticate the remote IPsec router's certificate. The trusted certificate can be the remote IPsec router's self-signed certificate or that of a trusted CA that signed the

remote IPSec router's certificate.

- Multiple SAs connecting through a secure gateway must have the same negotiation mode.

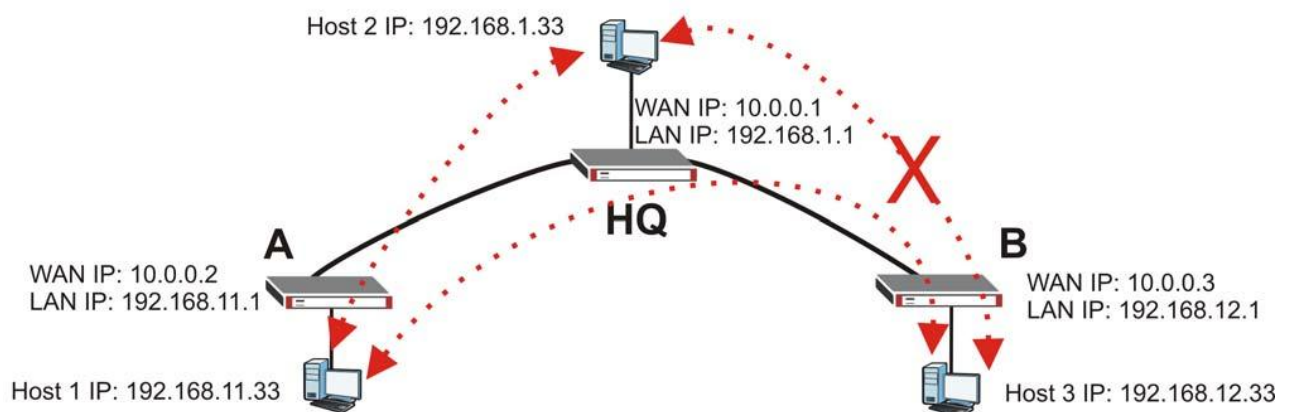
If you have the **Configuration > VPN > IPSec VPN > VPN Connection** screen's **Use Policy Route to control dynamic IPSec rules option** enabled and the VPN connection is up but VPN traffic cannot be transmitted through the VPN tunnel, check the routing policies to see if they are sending traffic elsewhere instead of through the VPN tunnels.

3.2 VPN Concentrator Example

A VPN concentrator uses hub-and-spoke VPN topology to combine multiple IPSec VPN connections into one secure network. The hub routes VPN traffic between the spoke routers and itself. This reduces the number of VPN connections to set up and maintain. Here a VPN concentrator connects ZLD-based USGs at headquarters (HQ) and branch offices A and B in one secure network.

- Branch A's USG uses one VPN rule to access both the headquarters (HQ) network and branch B's network.
- Branch B's USG uses one VPN rule to access branch A's network only. Branch B is not permitted to access the headquarters network.

Figure 29 IPSec VPN Concentrator Example



This IPSec VPN concentrator example uses the following settings.

Branch Office A

VPN Gateway (VPN Tunnel 1):

- My Address: 10.0.0.2
- Peer Gateway Address: 10.0.0.1

VPN Connection (VPN Tunnel 1):

- Local Policy: 192.168.11.0/255.255.255.0
- Remote Policy: 192.168.1.0/255.255.255.0
- Disable Policy Enforcement

Policy Route

- Source: 192.168.11.0

- Destination: 192.168.12.0
- Next Hop: VPN Tunnel 1

Headquarters

VPN Gateway (VPN Tunnel 1):

- My Address: 10.0.0.1
- Peer Gateway Address: 10.0.0.2

VPN Connection (VPN Tunnel 1):

- Local Policy: 192.168.1.0/255.255.255.0
- Remote Policy: 192.168.11.0/255.255.255.0
- Disable Policy Enforcement

VPN Gateway (VPN Tunnel 2):

- My Address: 10.0.0.1
- Peer Gateway Address: 10.0.0.3

VPN Connection (VPN Tunnel 2):

- Local Policy: 192.168.1.0/255.255.255.0
- Remote Policy: 192.168.12.0/255.255.255.0
- Disable Policy Enforcement

Concentrator

- Add VPN tunnel 1 and VPN tunnel 2 to an IPSec VPN concentrator.

Firewall

- Block traffic from VPN tunnel 2 from accessing the LAN.

Branch Office B

VPN Gateway (VPN Tunnel 2):

- My Address: 10.0.0.3
- Peer Gateway Address: 10.0.0.1

VPN Connection (VPN Tunnel 2):

- Local Policy: 192.168.12.0/255.255.255.0
- Remote Policy: 192.168.1.0/255.255.255.0
- Disable Policy Enforcement

Policy Route

- Source: 192.168.12.0
- Destination: 192.168.11.0
- Next Hop: VPN Tunnel 2

3.2.1 What Can Go Wrong

Consider the following when using the VPN concentrator:

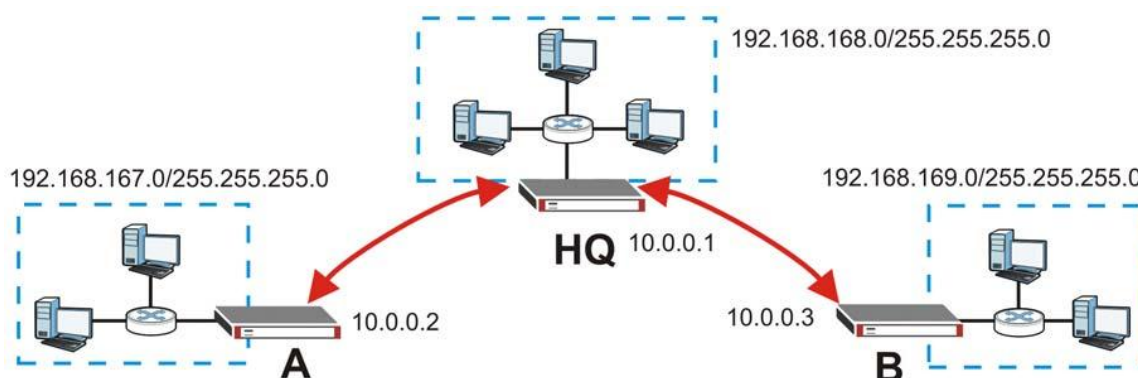
- The local IP addresses configured in the VPN rules should not overlap.
- The concentrator must have at least one separate VPN rule for each spoke. In the local policy, specify the IP addresses of the networks with which the spoke is to be able to have a VPN tunnel. This may require you to use more than one VPN rule for each spoke.
- To have all Internet access from the spoke routers go through the VPN tunnel, set the VPN rules in the spoke routers to use 0.0.0.0 (any) as the remote IP address.
- Your firewall rules can still block VPN packets.
- If on a USG USG or USG 1050 the concentrator's VPN tunnels are members of a single zone, make sure it is not set to block intra-zone traffic.

3.3 Hub-and-spoke IPSec VPN Without VPN Concentrator

Here is an example of a hub-and-spoke VPN that does not use the USG's VPN concentrator feature. Here branch office A has a ZyNOS-based USG and headquarters (HQ) and branch office B have ZLD-based USGs.

- Branch A's USG uses one VPN rule to access both the headquarters (HQ) network and branch B's network.
- Branch B's USG uses one VPN rule to access both the headquarters and branch A's networks.

Figure 30 Hub-and-spoke VPN Example



This hub-and-spoke VPN example uses the following settings.

Branch Office A (ZyNOS-based USG):

Gateway Policy (Phase 1):

- My Address: 10.0.0.2
- Primary Remote Gateway: 10.0.0.1

Network Policy (Phase 2): Local Network: 192.168.167.0/255.255.255.0; Remote Network: 192.168.168.0~192.168.169.255

Headquarters (ZLD-based USG):

VPN Gateway (VPN Tunnel 1):

- My Address: 10.0.0.1
- Peer Gateway Address: 10.0.0.2

VPN Connection (VPN Tunnel 1):

- Local Policy: 192.168.168.0~192.168.169.255
- Remote Policy: 192.168.167.0/255.255.255.0
- Disable Policy Enforcement

VPN Gateway (VPN Tunnel 2):

- My Address: 10.0.0.1
- Peer Gateway Address: 10.0.0.3

VPN Connection (VPN Tunnel 2):

- Local Policy: 192.168.167.0~192.168.168.255
- Remote Policy: 192.168.169.0/255.255.255.0
- Disable Policy Enforcement

Branch Office B (ZLD-based USG):

VPN Gateway:

- My Address: 10.0.0.3
- Peer Gateway Address: 10.0.0.1

VPN Connection:

- Local Policy: 192.168.169.0/255.255.255.0
- Remote Policy: 192.168.167.0~192.168.168.255
- Disable Policy Enforcement

3.3.1 What Can Go Wrong

Consider the following when implementing a hub-and-spoke VPN.

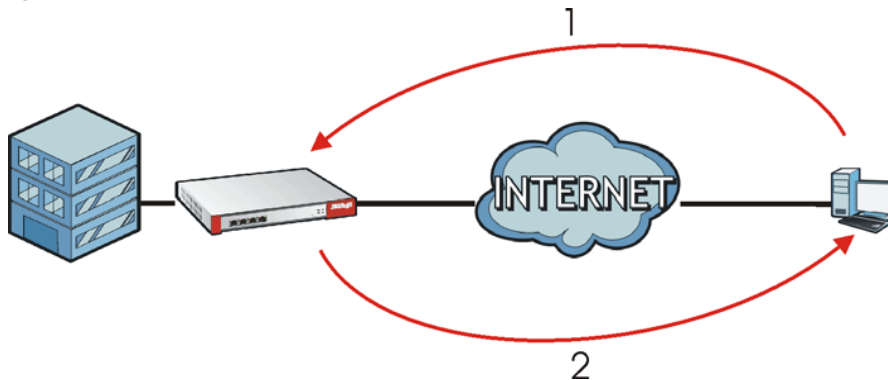
- This example uses a wide range for the ZyNOS-based USG's remote network, to use a narrower range.
- The local IP addresses configured in the VPN rules should not overlap.
- The hub router must have at least one separate VPN rule for each spoke. In the local policy, specify the IP addresses of the hub-and-spoke networks with which the spoke is to be able to have a VPN tunnel. This may require you to use more than one VPN rule.
- To have all Internet access from the spoke routers to go through the VPN tunnel, set the VPN rules in the spoke routers to use 0.0.0.0 (any) as the remote IP address.
- Your firewall rules can still block VPN packets.
- If the ZLD-based USGs' VPN tunnels are members of a single zone, make sure it is not set to block intra-zone traffic.
- The ZyNOS based USGs don't have user-configured policy routes so the only way to get traffic destined for another spoke router to go through the ZyNOS USG's VPN tunnel is to make the remote policy cover both tunnels.
- Since the ZLD-based USGs automatically handle the routing for VPN tunnels, if a ZLD-based USG is a hub router and the local policy covers both tunnels, the automatic routing takes care of it without needing a VPN concentrator.

- If a Zynos-based USG's remote network setting overlaps with its local network settings, set `ipsec swSkipOverlapIp` to `on` to send traffic destined to A's local network to A's local network instead of through the VPN tunnel.

3.4 USG IPsec VPN Client Configuration Provisioning

VPN configuration provisioning gives USG IPsec VPN Client users VPN rule settings automatically.

Figure 31 IPsec VPN Configuration Provisioning Process



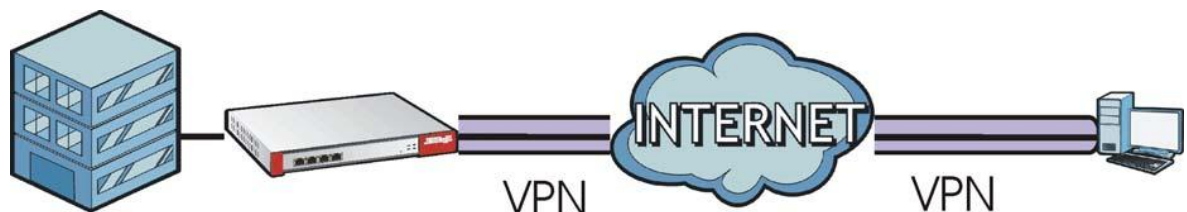
- 1 User Charlotte with the USG IPsec VPN Client sends her user name and password to the USG.
- 2 The USG sends the settings for the matching VPN rule.

3.4.1 Overview of What to Do

- 1 Create a VPN rule on the USG using the VPN Configuration Provisioning wizard.
- 2 Configure a username and password for the rule on the USG.
- 3 On a computer, use the USG IPsec VPN Client to get the VPN rule configuration.

Now user Charlotte can access the network behind the USG through the VPN tunnel.

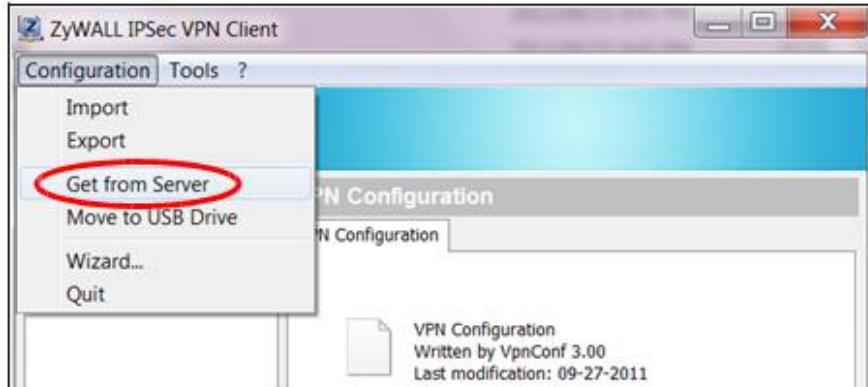
Figure 32 USG IPsec VPN Client with VPN Tunnel Connected



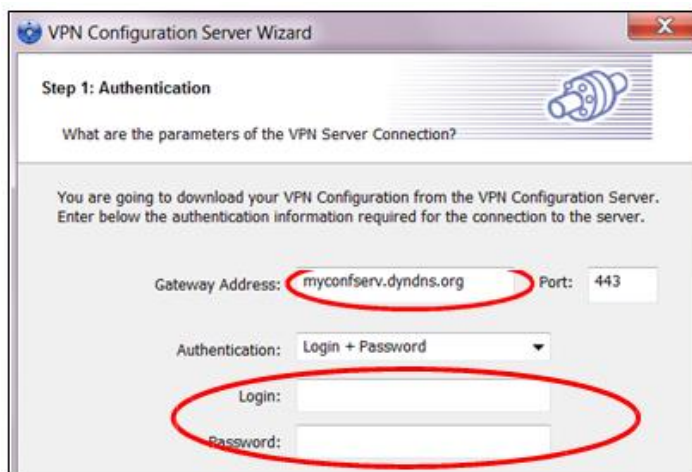
3.4.2 Configuration Steps

- 1 In the USG **Quick Setup** wizard, use the **VPN Settings for Configuration Provisioning** wizard to create a VPN rule that can be used with the USG IPsec VPN Client.

- 2 Click **Configuration > Object > User/Group** and create a user account for the USG IPSec VPN Client user.
- 3 Then, enable **Configuration Provisioning** in **Configuration > VPN > IPSec VPN > Configuration Provisioning** and configure it to allow the newly created user to retrieve this rule's settings using the USG IPSec VPN Client.
- 4 On the USG IPSec VPN Client, select **Configuration > Get From Server**.



- 5 Enter the WAN IP address or URL for the USG. If you changed the default HTTPS port on the USG, then enter the new one here. Enter the user name (**Login**) and password exactly as configured on the USG or external authentication server. Click **Next**.



- 6 Click **OK**. The rule settings are now imported from the USG into the USG IPSec VPN Client.

3.4.3 What Can Go Wrong

- VPN rule settings violate the the USG IPSec VPN Client restrictions:
 Check that the rule does not contain **AH** active protocol, **NULL** encryption, **SHA512** authentication, or a subnet/range remote policy.
 The USG IPSec VPN Client can also indicate rule violations. Check its warning screen.
 Although the rule settings may be valid, whether the tunnel actually works depends on the network environment. For example, a remote policy IP address for a server may be valid, but the server may be down or have an actual different IP address.
- There is a login problem:
 Reenter the user name (**Login**) and password in the USG IPSec VPN Client exactly as configured on the USG or the external authentication server.
 Check that the client authentication method selected on the USG is where the user name and password are configured . For example, if the user name and password are configured on the USG, then the configured authentication method should be **Local**.
- There's a network connectivity problem between the USG and the USG IPSec VPN Client:

Check that the correct USG IP address and HTTPS port (if the default port was changed) was entered.

Ping the USG from the computer on which the USG IPsec VPN Client is installed. If there is no reply, check that the computer has Internet access.

If the computer has Internet access, contact the USG administrator.

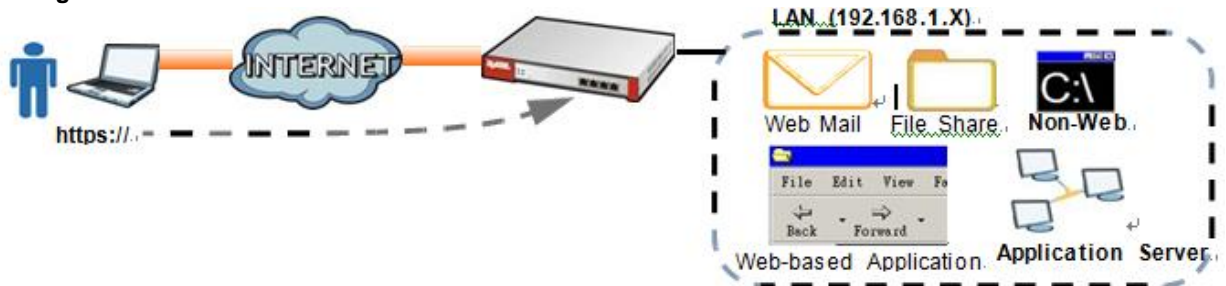
- The entry is not activated:

Make sure that both **Enable Configuration Provisioning** in **Configuration > VPN > IPsec VPN > Configuration Provisioning** is selected and that the entry has a yellow **Status** icon.

3.5 SSL VPN

SSL VPN uses remote users' web browsers to provide the easiest-to-use of the USG's VPN solutions. A user just types the USG's web address and enters his user name and password to securely access the USG's network. Here a user uses his browser to securely connect to network resources in the same way as if he were part of the internal network.

Figure 33 SSL VPN



- Click **Configuration > Object > SSL Application** and configure an SSL application object to specify the type of application and the address of the local computer, server, or web site SSL users are to be able to access.
- Click **Configuration > VPN > SSL VPN > Access Privilege** to configure SSL access policies.
- Use the **Configuration > VPN > SSL VPN > Global Setting** screen to set the IP address of the USG (or a gateway device) on your network for full tunnel mode access, enter access messages or upload a custom logo to be displayed on the remote user screen.

Remote users can access resources on the local network using one of the following methods:

- Using a supported web browser
Once you have successfully logged in through the USG, you can access intranet sites, web-based applications, or web-based e-mails using one of the supported web browsers.
- Using the USG SecuExtender client
Once you have successfully logged into the USG, if the SSL VPN access policy has network extension enabled the USG automatically loads the USG SecuExtender client program to your computer. With the USG SecuExtender, you can access network resources, remote desktops and manage files as if you were on the local network.

3.5.1 What Can Go Wrong

- If you uploaded a logo to show in the SSL VPN user screens but it does not display properly, check that the logo graphic is in GIF, JPG, or PNG format. The graphic should use a resolution of

103 x 29 pixels to avoid distortion when displayed. The USG automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.

- If users can log into the SSL VPN but cannot see some of the resource links check the SSL application object's configuration.
- If the user account is not included in an SSL VPN access policy, the USG redirects the user to the user aware screen.
- Operating system and browser requirements for the remote user's computer:
 - Windows 7 (32 or 64-bit), Vista (32 or 64-bit), 2003 (32-bit), XP (32-bit), or 2000 (32-bit)
 - Internet Explorer 7 and above or Firefox 1.5 and above
 - Using RDP requires Internet Explorer
 - Sun's Runtime Environment (JRE) version 1.6 or later installed and enabled.
- Changing the HTTP/HTTPS configuration disconnects SSL VPN network extension sessions. Users need to re-connect if this happens.

3.6 L2TP VPN with Android, iOS, and Windows

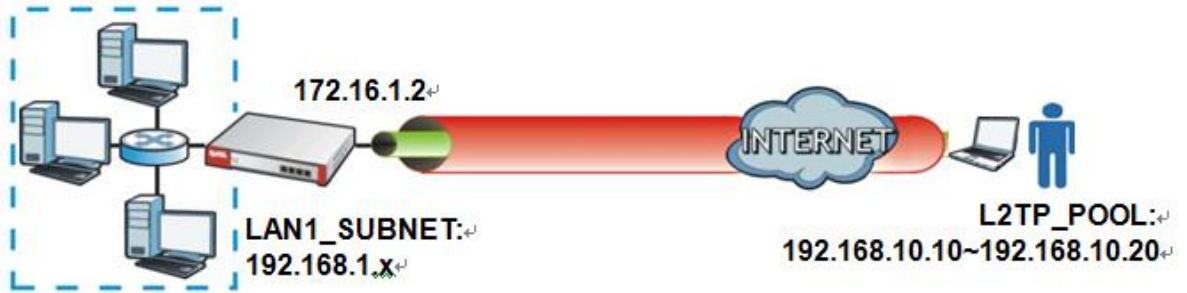
L2TP VPN uses the L2TP and IPSec client software included in remote users' Android, iOS, or Windows operating systems for secure connections to the network behind the USG.

- 1 L2TP VPN uses one of the USG's IPSec VPN connections. Edit **Default_L2TP_VPN_GW** as follows:
 - Set **My Address** to the WAN interface domain name or IP address you want to use.
 - Replace the default **Pre-Shared Key**.
- 2 Create a host-type address object containing the **My Address** IP address configured in the **Default_L2TP_VPN_GW** and set the **Default_L2TP_VPN_Connection's Local Policy** to use it.
- 3 In **Configuration > VPN > L2TP VPN** enable the connection and set the VPN connection L2TP VPN uses, the L2TP client IP address pool, the authentication method, and the allowed users.
- 4 Configure a policy route to let remote users access resources on the network behind the USG.
 - Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN1_SUBNET** in the following example).
 - Set the **Destination Address** to the IP address pool that the USG assigns to the remote users (**L2TP_POOL** in the following example).
 - Set the next hop to be the VPN tunnel you are using for L2TP.

3.6.1 L2TP VPN Example

Here a sales representative uses a laptop to securely connect to the USG's network.

Figure 34 L2TP VPN Example



- The USG has a WAN interface with a static IP address of 172.16.1.2.
- The remote user has a dynamic public IP address and connects through the Internet.
- You configure an IP address pool object named **L2TP_POOL** to assign the remote users IP addresses from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel.
- The VPN rule allows the remote user to access the **LAN1_SUBNET** (the 192.168.1.x subnet). Do

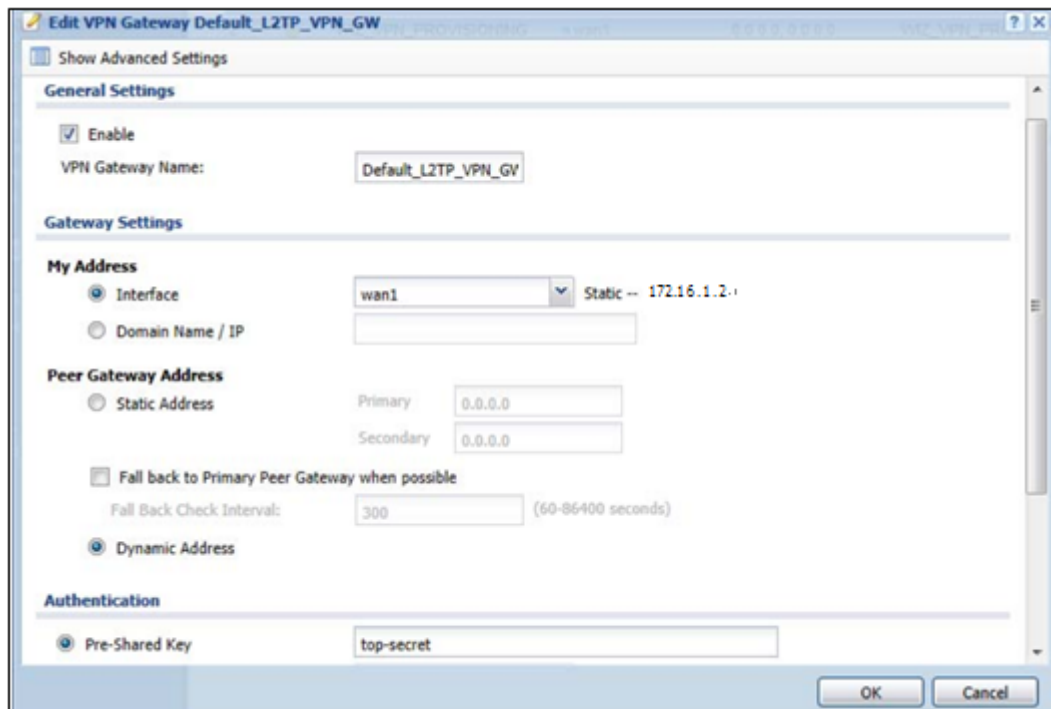
the following to configure the L2TP VPN example:

- 1 Click **Configuration > VPN > IPsec VPN > VPN Gateway** and double-click the **Default_L2TP_VPN_GW** entry.

Select **Enable**.

Set **My Address**. This example uses a WAN interface with static IP address 172.16.1.2.

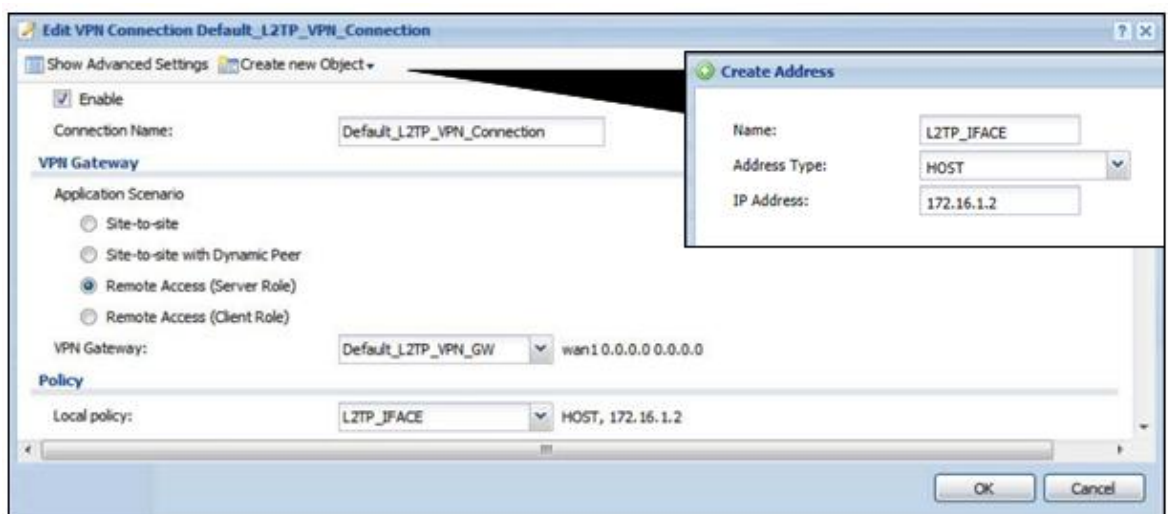
Set **Authentication** to **Pre-Shared Key** and configure a password. This example uses **top-secret**. Click **OK**.



- 2 Click the **VPN Connection** tab and double-click the **Default_L2TP_VPN_Connection** entry.

Click **Create New Object > Address** and create a host type address object that contains the **My Address** IP address you configured in the **Default_L2TP_VPN_GW**. The address object in this example uses the WAN interface's IP address (172.16.1.2) and is named **L2TP_IFACE**.

Select **Enable**, set **Application Scenario** to **Remote Access** and **Local Policy** to **L2TP_IFACE**, and click **OK**.



- Click **Configuration > VPN > L2TP VPN** and then **Create New Object > Address** to create an IP address pool for the L2TP VPN clients. This example uses **L2TP_POOL** with a range of 192.168.10.10 to 192.168.10.20. Click **Create New Object > User/Group** to create a user object for the users allowed to use the tunnel. This example uses a user object named **L2TP-test**.

Enable the connection.

Set **VPN Connection** to **Default_L2TP_VPN_Connection**.

Set **IP Address Pool** to **L2TP_POOL**.

Select the authentication method (default in this example), and select the users that can use the tunnel (**L2TP-test** in this example).

The image shows the L2TP VPN configuration interface. The main window is titled 'L2TP VPN' and has a 'General Settings' tab. The 'Enable L2TP Over IPsec' checkbox is checked. The 'VPN Connection' dropdown is set to 'Default_L2TP_VPN_Conne'. The 'IP Address Pool' dropdown is set to 'L2TP_POOL'. The 'Authentication Method' dropdown is set to 'default'. The 'Allowed User' dropdown is set to 'L2TP-test'. There are 'Apply' and 'Reset' buttons at the bottom. Two dialog boxes are overlaid on the main window. The 'Create Address' dialog box has fields for 'Name' (L2TP_POOL), 'Address Type' (RANGE), 'Starting IP Address' (192.168.10.10), and 'End IP Address' (192.168.10.20). The 'Add User' dialog box has fields for 'User Name' (L2TP-test), 'User Type' (user), 'Password' (****), and 'Retype' (****).

3.6.2 Configuring Policy Routing

You must also configure a policy route to let remote users access resources on the network behind the USG.

- Set the policy route's **Source Address** to the address object that you want to allow the remote users to access (**LAN_1SUBNET** in this example).
- Set the **Destination Address** to the IP address pool that the USG assigns to the remote users (**L2TP_POOL** in this example)).
- Set the next hop to be the VPN tunnel that you are using for L2TP VPN.

The image shows the 'Add Policy Route' dialog box. It has a 'Configuration' tab. The 'Enable' checkbox is checked. The 'Description' field is set to 'L2TP_VPN' (Optional). The 'Criteria' section has dropdowns for 'User' (any), 'Incoming' (any (Excluding ZyWALL)), 'Source Address' (LAN1_SUBNET), 'Destination Address' (L2TP_POOL), 'DSCP Code' (any), 'Schedule' (none), and 'Service' (any). The 'Next-Hop' section has dropdowns for 'Type' (VPN Tunnel) and 'VPN Tunnel' (Default_L2TP_VPN_Conne).

USG's return traffic back through the L2TP VPN tunnel.

- Set **Incoming** to **USG**.
- Set **Destination Address** to the L2TP address pool.
- Set the next hop to be the VPN tunnel that you are using for L2TP.

Add Policy Route

Show Advanced Settings Create new Object ▾

Configuration

☒ Enable

Description: Remote Management (Optional)

Criteria

User: admin ▾

Incoming: ZyWALL ▾

Source Address: any ▾

Destination Address: L2TP_POOL ▾

DSCP Code: any ▾

Schedule: none ▾

Service: any ▾

Next-Hop

Type: VPN Tunnel ▾

VPN Tunnel: Default_L2TP_VPN_Conne ▾

If some of the traffic from the L2TP clients needs to go to the Internet, create a policy route to send traffic from the L2TP tunnels out through a WAN trunk.

- Set **Incoming** to **Tunnel** and select your L2TP VPN connection.
- Set the **Source Address** to the L2TP address pool.
- Set the **Next-Hop Type** to **Trunk** and select the appropriate WAN trunk.

Edit Policy Route

Show Advanced Settings Create new Object ▾

Configuration

☒ Enable

Description: L2TP VPN to Internet (Optional)

Criteria

User: L2TP-test ▾

Incoming: Tunnel ▾

Please select one member: Default_L2TP_VPN_Conne ▾

Source Address: L2TP_POOL ▾

Destination Address: any ▾

DSCP Code: any ▾

Schedule: none ▾

Service: any ▾

Next-Hop

Type: Trunk ▾

Trunk: SYSTEM_DEFAULT_WAN_ ▾

3.6.3

To configure L2TP VPN in an Android device, go to **Menu > Settings > Wireless & networks > VPN settings > Add VPN > Add L2TP/IPSec PSK VPN** and configure as follows..

- **VPN name** is for the user to identify the VPN configuration.
- **Set VPN server** is the USG's WAN IP address.
- **Set IPsec pre-shared key** is the pre-shared key of the IPsec VPN gateway the USG uses for L2TP VPN over IPsec (top-secret in this example).
- **Enable L2TP secret** turn this off.
- **DNS search domain** leave this on.
- When dialing the L2TP VPN, the user will have to enter his account and password.

3.6.4 Configuring L2TP VPN in iOS

To configure L2TP VPN in an iOS device, go to **Settings > VPN > Add VPN Configuration > L2TP** and configure as follows.

- **Description** is for the user to identify the VPN configuration.
- **Server** is the USG's WAN IP address.
- **Account** is the user's account for using the L2TP VPN (L2TP-test in this example).
- **RSA SecurID** leave this off.
- **Password** is the password for the user's account.
- **Secret** is the pre-shared key of the IPsec VPN gateway the USG uses for L2TP VPN over IPsec (top-secret in this example).
- **Send All Traffic** leave this on.
- **Proxy** leave this off.

3.6.5 Configuring L2TP VPN in Windows

The following sections cover how to configure L2TP in remote user computers using Windows 7, Vista, or XP.

3.6.5.1 Configuring L2TP in Windows 7 or Windows Vista

Do the following to establish an L2TP VPN connection.

Create a Connection Object

- 1 Open the **Network and Sharing Center** screen.
Windows 7: click **Start > Control Panel > View network status and tasks > Set up a new connection or network**.
Windows Vista: click **Start > Network > Network and Sharing Center > Set up a connection or network**).
- 2 Select **Connect to a workplace** and click **Next**.
- 3 Select **Use my Internet connection (VPN)**.
- 4 For the **Internet address** enter the **My Address** domain name or WAN IP address of the VPN gateway the USG is using for L2TP VPN (172.16.1.2 in this example).
 - 4a For the **Destination name**, specify a name to identify this VPN (L2TP to USG for example).
 - 4b Select **Don't connect now, just set it up so I can connect later** and click **Next**.

Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: 172.16.1.2

Destination name: L2TP to ZyWALL

☐ Use a smart card

☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

☒ Don't connect now; just set it up so I can connect later

Next Cancel

- 4 Enter your USG user name and password and click **Create**.

Type your user name and password

User name: L2TP-test

Password: ••••••••

☐ Show characters

☐ Remember this password

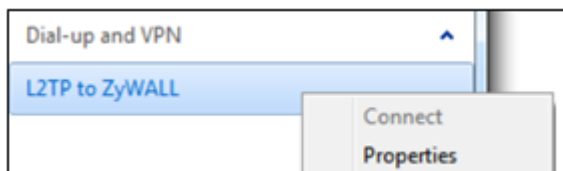
Domain (optional):

Create Cancel

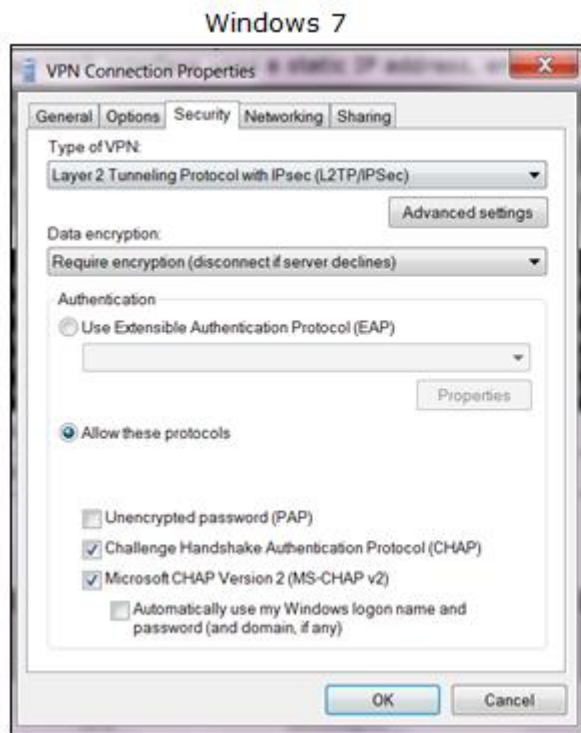
- 6 Click **Close**.

Configure the Connection Object

- 1 In the **Network and Sharing Center** screen, click **Connect to a network**. Right-click the L2TP VPN connection and select **Properties**.



- 2 In Windows 7, click **Security** and set the **Type of VPN** to **Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)**. Then click **Advanced settings**.
In Windows Vista, click **Networking**. Set the **Type of VPN** to **L2TP IPSec VPN** and click **IPSec Settings**.



- 2 Select **Use preshared key for authentication** and enter the pre-shared key of the VPN gateway entry the USG is using for L2TP VPN (top-secret in this example). Click **OK** to save your changes and close the **Advanced Properties** screen. Then click **OK** again to close the **Properties** window.



- 4 If a warning screen about data encryption not occurring if PAP or CHAP is negotiated, click **Yes**. When you use L2TP VPN to connect to the USG, the USG establishes an encrypted IPsec VPN tunnel first and then builds an L2TP tunnel inside it. The L2TP tunnel itself does not need encryption since it is inside the encrypted IPsec VPN tunnel.



Connect Using L2TP VPN

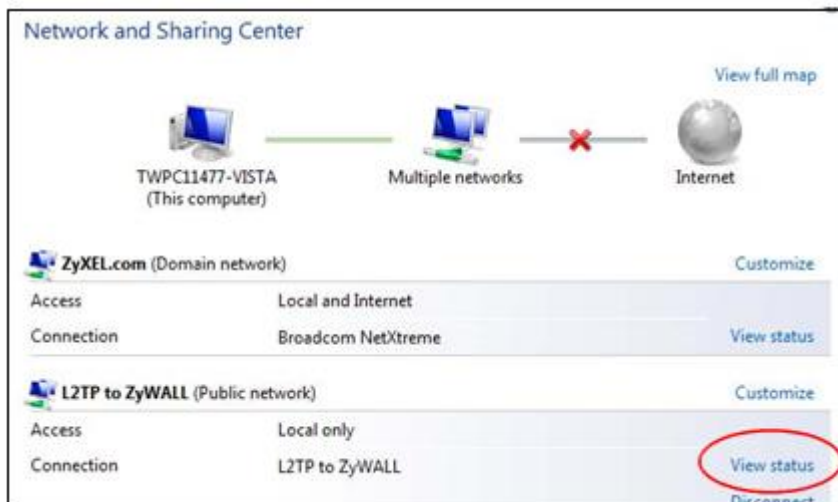
- 1 In the **Network and Sharing Center** screen, click **Connect to a network**, select the L2TP VPN connection and click **Connect** to display a login screen. Enter the user name and password of your USG user account and click **Connect**.



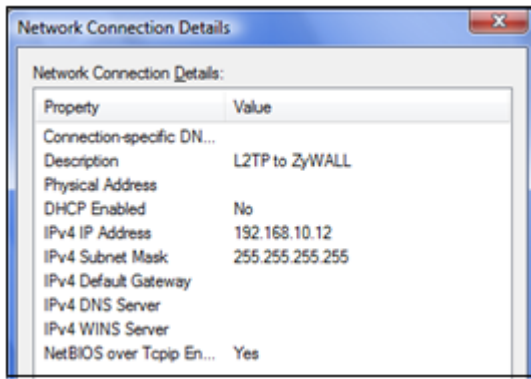
- 2 A window appears while the user name and password are verified. The **Connect to a network** screen shows **Connected** after the L2TP over IPsec VPN tunnel is built.



- 3 After the connection is up a connection icon displays in your system tray. Click it and then the L2TP connection to open a status screen.
- 4 Click the L2TP connection's **View status** link to open a status screen.



- 5 Click **Details** to see the address that you received is from the L2TP range you specified on the USG (192.168.10.10-192.168.10.20 in the example).



- 6 Access a server or other network resource behind the USG to make sure your access works.

3.6.5.2 Configuring L2TP in Windows XP

In Windows XP, first issue the following command from the Windows command prompt (including the quotes) to make sure the computer is running the Microsoft IPsec service.

```
net start "ipsec services".
```

Then do the following to establish an L2TP VPN connection.

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



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



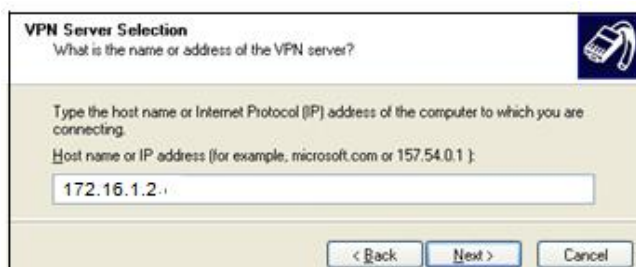
- 5 Type **L2TP to USG** as the **Company Name**.



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



- 7 Enter the domain name or WAN IP address configured as the **My Address** in the VPN gateway configuration that the USG is using for L2TP VPN (172.16.1.2 in this example).



- 8 Click **Finish**.

- 9 The **Connect L2TP to USG** screen appears. Click **Properties > Security**.



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



- 11 Select **Optional encryption (connect even if no encryption)** and the **Allow these protocols**

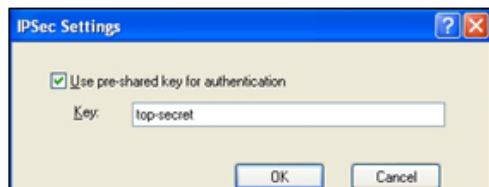
radio button. Select **Unencrypted password (PAP)** and clear all of the other check boxes. Click **OK**.



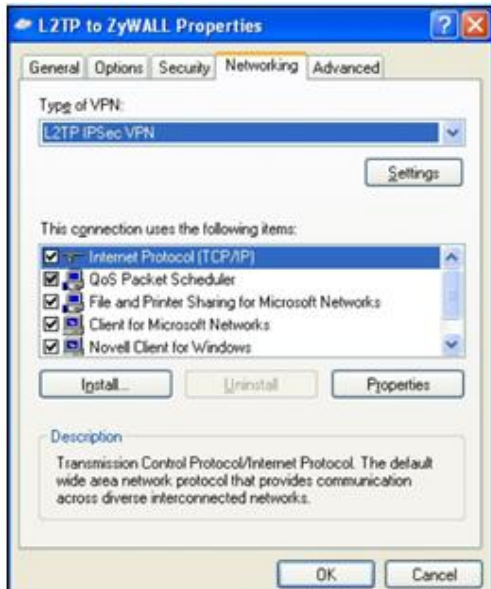
12 Click **IPSec Settings**.



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



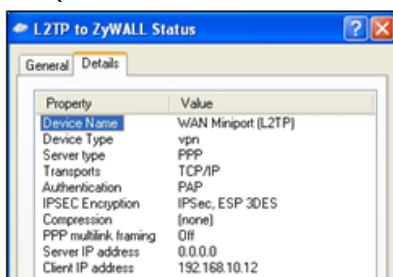
14 Click **Networking**. Select **L2TP IPSec VPN** as the **Type of VPN**. Click **OK**.



- 15 Enter the user name and password of your USG account. Click **Connect**.



- 16 A window appears while the user name and password are verified.
 17 A USG-L2TP icon displays in your system tray. Double-click it to open a status screen.
 18 Click **Details** to see the address that you received from the L2TP range you specified on the USG (192.168.10.10-192.168.10.20).



- 19 Access a server or other network resource behind the USG to make sure your access works.

3.6.6 What Can Go Wrong

The IPsec VPN connection must:

- Be enabled
- Use transport mode
- Not be a manual key VPN connection

- Use **Pre-Shared Key** authentication
- Use a VPN gateway with the **Secure Gateway** set to **0.0.0.0** if you need to allow L2TP VPN clients to connect from more than one IP address.

Disconnect any existing L2TP VPN sessions before modifying L2TP VPN settings. The remote users must make any needed matching configuration changes and re-establish the sessions using the new settings.

Tutorial 4: Managing Traffic

These sections cover controlling the traffic going through the USG.

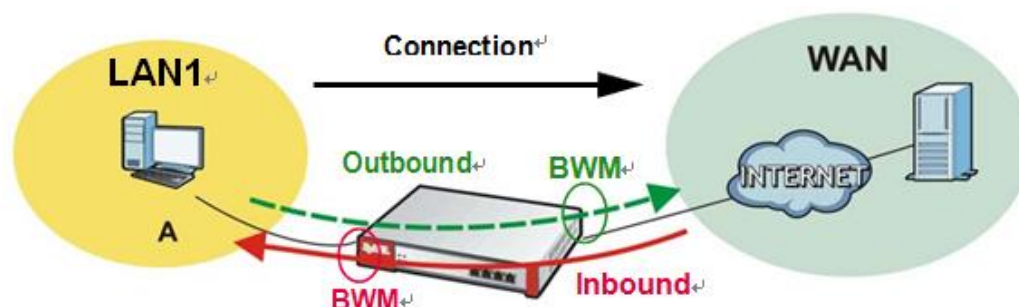
4.1 How to Configure Bandwidth Management

Bandwidth management is very useful when applications are competing for limited bandwidth.

Connection and Packet Directions

Bandwidth management looks at the connection's direction from the interface it was initiated on to the interface it goes out. The connection initiator sends outbound traffic and receives inbound traffic. The USG controls each flow's bandwidth as it goes out through an interface or VPN tunnel. For example, a LAN1 to WAN connection is initiated from LAN1 and goes to the WAN.

Figure 36 LAN1 to WAN Connection and Packet Directions



- Outbound traffic goes from a LAN1 device to the WAN. The USG applies bandwidth management before sending the packets out a WAN interface.
- Inbound traffic comes back from the WAN to the LAN1 device. The USG applies bandwidth management before sending the traffic out a LAN1 interface.

You can set outbound and inbound guaranteed and maximum bandwidths for an application.

4.1.1 Bandwidth Allocation Example

Say a 10-person office has WAN1 connected to a 50 Mbps downstream and 5 Mbps upstream VDSL line and you want to allocate bandwidth for the following:

- SIP: Up to 10 simultaneous 100 Kbps calls guaranteed
- Video conferencing: Up to 10 simultaneous 128 Kbps Skype video calls guaranteed
- Video streaming: up to 10 simultaneous 256 Kbps sessions
- HTTP: Internet access including downloading files for 10 users
- SMTP: 10 users sending email
- POP3: 10 users receiving email
- FTP: 10 users uploading and downloading files

Here is an example of allocating the any to WAN connection's inbound and outbound packet flows. Enable Maximize Bandwidth Usage (Max B.U.) on a packet flow to set no limit on it and let it use any available bandwidth on the out-going interface.

Table 11 50 Mbps / 5 Mbps Connection Any to WAN Bandwidth Allocation Example

PRIORITY AND APPLICATION		GUARANTEED K / MAXIMUM K OR MAX B.U.	
		INBOUND	OUTBOUND
1	SIP	1000/2000	1000/2000
2	Video conferencing	1280/3840	1280/3840
3	Video streaming	2560/3584	*
4	HTTP	10240/46080	*
4	SMTP	*	2048/Max B.U.
4	POP3	10240/Max B.U.	*
5	FTP	10240/46080	792/3072
Total guaranteed bandwidth:		35560 Kbps	5120 Kbps

* This application does not usually generate enough traffic in this direction to require management.

4.1.2 Setting the Interface's Bandwidth

Use the **Configuration > Interface** screens to set the WAN1 interface's upstream (egress) bandwidth to be equal to (or slightly less than) what the connected device can support. This example uses 5120 Kbps.

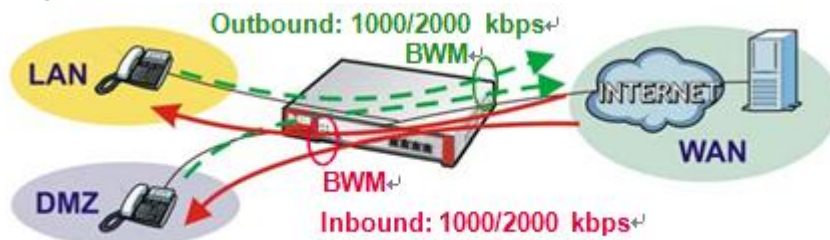
4.1.3 SIP Bandwidth Management

The most effective way to ensure the quality of SIP calls is to go to the **Configuration > BWM** screen and enable BWM and select **Enable Highest Bandwidth Priority for SIP Traffic**. See the following section if you prefer to configure specific bandwidth management rules for SIP instead.

4.1.4 SIP Any-to-WAN and WAN-to-Any Bandwidth Management Example

- Manage SIP traffic going to WAN1 from users on the LAN or DMZ.
- Inbound and outbound traffic are both guaranteed 1000 kbps and limited to 2000 kbps.

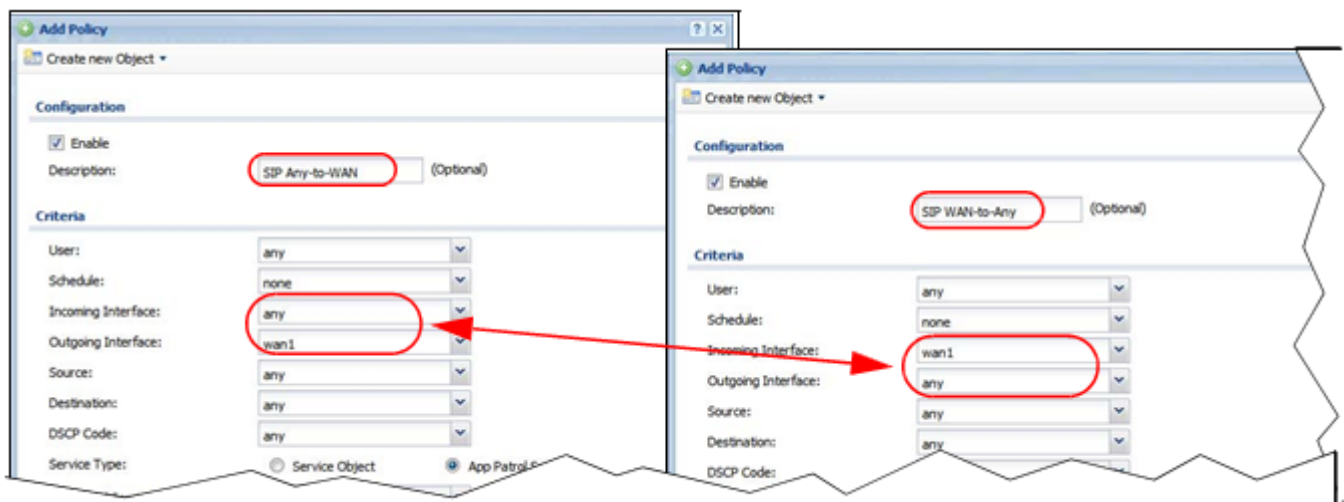
Figure 37 SIP Any-to-WAN Guaranteed / Maximum Bandwidths Example



- 1 In the **Configuration > BWM** screen, click **Add**.
- 2 In the **Add Policy** screen, select **Enable** and type **SIP Any-to-WAN** as the policy's name. Leave the incoming interface to **any** and select **wan1** as the outgoing interface. Select **App Patrol Service** and **sip** as the service type. Set the inbound and outbound guaranteed bandwidth to **1000** (kbps) and maximum bandwidth to **2000** kbps and priority **1**. Click **OK**.

Note: Use **App Patrol Service** for the services classified by the USG's IDP packet inspection signatures. Use **Service Object** for pre-defined services.

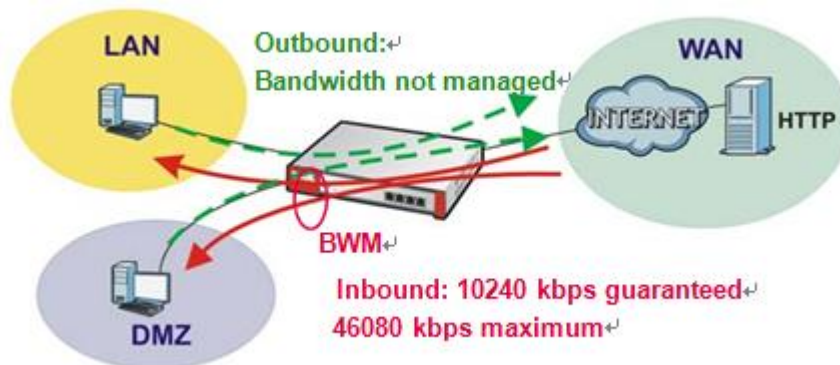
- 2 Repeat the steps above to create another policy named **SIP WAN-to-Any** for calls coming in from the SIP server on the WAN. It is the same as the **SIP Any-to-WAN** policy, but with the directions reversed (WAN-to-Any instead of Any-to-WAN).



4.1.5 HTTP Any-to-WAN Bandwidth Management Example

- Set inbound guaranteed and maximum rates as the local users on the LAN and DMZ will probably download more than they upload to the Internet.
- Set fourth highest priority (4) for the HTTP traffic in both directions.

Figure 38 HTTP Any-to-WAN Bandwidth Management Example



- 1 In the **Configuration > BWM** screen, click **Add**.
- 2 In the **Add Policy** screen, select **Enable** and type **HTTP Any-to-WAN** as the policy's name. Leave the incoming interface to **any** and select **wan1** as the outgoing interface. Select **App Patrol Service** and **http** as the service type. Set the guaranteed inbound bandwidth to **10240** (kbps) and set priority **4**. Set the maximum to **46080** (kbps). Set the outbound priority to **4**. Click **OK**.

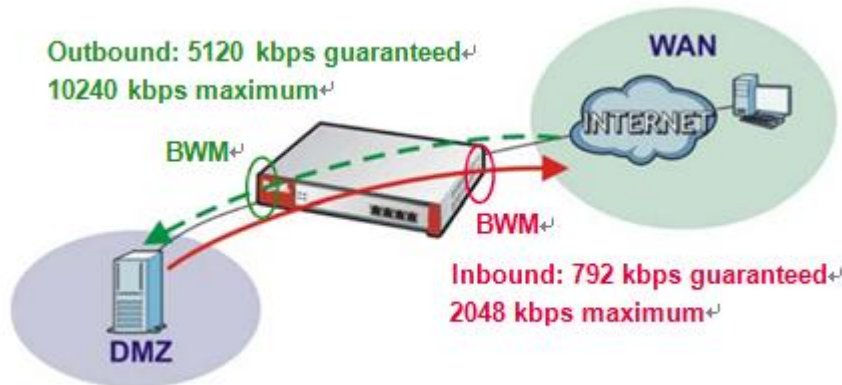
The screenshot shows the 'Add Policy' configuration window. The 'Configuration' section has 'Enable' checked and 'HTTP Any-to-WAN' as the description. The 'Criteria' section has 'Incoming Interface' set to 'any' and 'Outgoing Interface' set to 'wan1'. The 'Service Type' is set to 'App Patrol Service' with 'http' as the service. The 'Bandwidth Shaping' section has 'Inbound' bandwidth set to 10240 kbps with priority 4, and 'Outbound' bandwidth set to 0 kbps with priority 4.

4.1.6 FTP WAN-to-DMZ Bandwidth Management Example

Suppose the office has an FTP server on the DMZ. Here is how to limit WAN1 to DMZ FTP traffic so it does not interfere with SIP and HTTP traffic.

- Allow remote users only 2048 kbps inbound for downloading from the DMZ FTP server but up to 10240 kbps outbound for uploading to the DMZ FTP server.
- Set the fifth highest priority (5) for the FTP traffic.

Figure 39 FTP WAN-to-DMZ Bandwidth Management Example



- 1 In the **Configuration** > **BWM** screen, click **Add**.
- 2 In the **Add Policy** screen, select **Enable** and type **FTP WAN-to-DMZ** as the policy's name. Select **wan1** as the incoming interface and **dmz** as the outgoing interface. Select **App Patrol Service** and **ftp** as the service type. Set inbound guaranteed bandwidth to **792** kbps, priority **5**, and maximum **2048** kbps. Set outbound guaranteed bandwidth to **5120** kbps, priority **5**, and maximum **10240** kbps. Click **OK**.

Add Policy

Create new Object ▾

Configuration

☒ Enable

Description: FTP WAN-to-DMZ (Optional)

Criteria

User: any

Schedule: none

Incoming Interface: wan1

Outgoing Interface: dmz

Source: any

Destination: any

DSCP Code: any

Service Type: ☐ Service Object ☒ App Patrol Service

App Patrol Service: ftp

DSCP Marking

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth

Inbound: 792 kbps (0 : disabled) Priority: 5

☐ Maximize Bandwidth Usage Maximum: 2048 kbps

Outbound: 5120 kbps (0 : disabled) Priority: 5

☐ Maximize Bandwidth Usage Maximum: 2048 kbps

Related Setting

Log: no

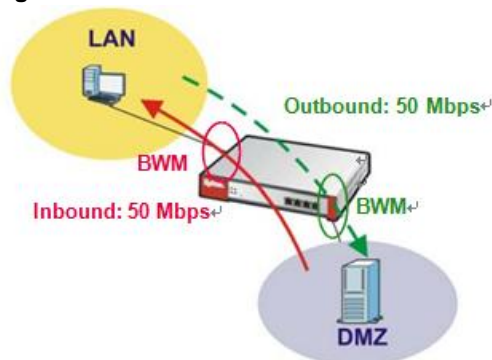
OK Cancel

4.1.7 FTP LAN-to-DMZ Bandwidth Management Example

FTP traffic from the LAN1 to the DMZ can use more bandwidth since the interfaces support up to 1 Gbps connections, but give it lower priority and limit it to avoid interference with other traffic.

- Limit both outbound and inbound traffic to 50 Mbps.
- Set fifth highest priority (5) for the FTP traffic.

Figure 40 FTP LAN-to-DMZ Bandwidth Management Example



- 1 In the **Configuration > BWM** screen, click **Add**.
- 2 In the **Add Policy** screen, select **Enable** and type **FTP LAN-to-DMZ** as the policy's name.

Select **lan1** as the incoming interface and **dmz** as the outgoing interface.

Select **App Patrol Service** and **ftp** as the service type.

Type **10240** (kbps) with priority **5** for both the inbound and outbound guaranteed bandwidth. Do not select the **Maximize Bandwidth Usage**. Set the maximum to **51200** (kbps). Click **OK**.

Add Policy

Create new Object ▾

Configuration

☒ Enable

Description: FTP LAN-to-DMZ (Optional)

Criteria

User: any

Schedule: none

Incoming Interface: lan1

Outgoing Interface: dmz

Source: any

Destination: any

DSCP Code: any

Service Type: ☒ Service Object ☒ App Patrol Service

App Patrol Service: ftp

DSCP Marking

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth

Inbound: 10240 kbps (0 : disabled) Priority: 5

☐ Maximize Bandwidth Usage Maximum: 51200 kbps

Outbound: 10240 kbps (0 : disabled) Priority: 5

☐ Maximize Bandwidth Usage Maximum: 51200 kbps

Finally, in the **BWM** screen, select **Enable BWM**. Click **Apply**.

BWM

BWM Global Setting

☒ Enable BWM

☒ Enable Highest Bandwidth Priority for SIP Traffic

Configuration

Add Edit Remove Activate Inactivate Move

Status	Priority	Description	User	Schedule	Incoming I...	Outgoing I...	Source	Destina...	DSC...	Service	BWM In/PrO...	DSCP M...
1	1	FTP LAN-to-DMZ	any	none	lan1	dmz	any	any	any	App=ftp	10240/5/102...	preserv...
2	2	FTP WAN-to-DMZ	any	none	wan1	dmz	any	any	any	App=ftp	792/5/5120/5	preserv...
3	3	HTTP Any-to-WAN	any	none	any	wan1	any	any	any	App=h...	10240/4/1024	preserv...
4	4	SIP Any-to-WAN	any	none	any	wan1	any	any	any	App=sip	1000/1/1000/1	preserv...
5	5	SIP WAN-to-Any	any	none	wan1	any	any	any	any	App=sip	1000/1/1000/1	preserv...
6	6	FTP LAN-to-DMZ	any	none	lan1	dmz	any	any	any	Objany	10000/5/100...	preserv...
default			any	none	any	any	any	any	any	Objany	no/7/1024/7	preserv...

Page 1 of 1 Show 50 items Displaying 1 - 7 of 7

Apply Reset

4.1.8 What Can Go Wrong?

- The "outbound" in the guaranteed bandwidth settings apply to traffic going from the connection initiator to the outgoing interface. The "inbound" refers to the reverse direction.
- Make sure you have registered the IDP/App.Patrol service on the USG to use **App Patrol Service** as the service type in the bandwidth management rules. The application patrol service uses the

4.2 How to Configure a Trunk for WAN Load Balancing

These examples show how to configure a trunk for two WAN connections to the Internet. The available bandwidth for the connections is 1 Mbps (**wan1**) and 512 Kbps (**wan2 or cellular1**) respectively. As these connections have different bandwidth, use the **Weighted Round Robin** algorithm to send traffic to wan1 and wan2 (or cellular1) in a 2:1 ratio.

Figure 41 Trunk Example For Dual WANs

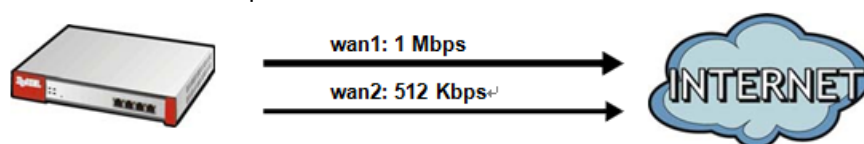
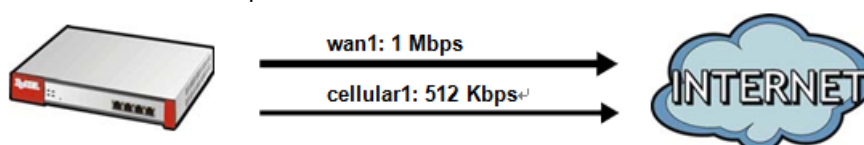


Figure 42 Trunk Example For WAN and 3G Interface



You do not have to change many of the USG's settings from the defaults to set up this trunk. You only have to set up the outgoing bandwidth on each of the WAN interfaces and configure the WAN_TRUNK trunk's load balancing settings.

4.2.1 Set Up Available Bandwidth on Ethernet Interfaces

Here is how to set a limit on how much traffic the USG tries to send out through each WAN interface.

- 1 Click **Configuration > Network > Interface > Ethernet** and double-click the **wan1** entry. Enter the available bandwidth (1000 kbps) in the **Egress Bandwidth** field. Click **OK**.

Edit Ethernet

IPv4 View Show Advanced Settings Create new Object

General Settings

☒ Enable Interface

Interface Properties

Interface Type: external

Interface Name: wan1

Port: P1

Zone: WAN

MAC Address: 00:00:AA:79:73:79

Description: (Optional)

IP Address Assignment

☐ Get Automatically

☒ Use Fixed IP Address

IP Address: 1.2.3.4

Subnet Mask: 255.255.255.0

Gateway: 1.2.3.254 (Optional)

Metric: 0 (0-15)

Interface Parameters

Egress Bandwidth: 1000 Kbps

Connectivity Check

☐ Enable Connectivity Check

OK Cancel

- 2 Repeat the process to set the egress bandwidth for **wan2** to 512 Kbps.
- 3 For 3G interface settings, go to **Configuration > Network > Interface > Cellular**. Double-click the **cellular1** entry and set the egress bandwidth for **cellular1** to 512 Kbps.

4.2.2 Configure the WAN Trunk

- 1 Click **Configuration > Network > Interface > Trunk**. Click the **Add** icon.
- 2 Name the trunk and set the **Load Balancing Algorithm** field to **Weighted Round Robin**.
Add **wan1** and enter 2 in the **Weight** column.
Add **wan2 (or cellular1)** and enter 1 in the **Weight** column.
Click **OK**.

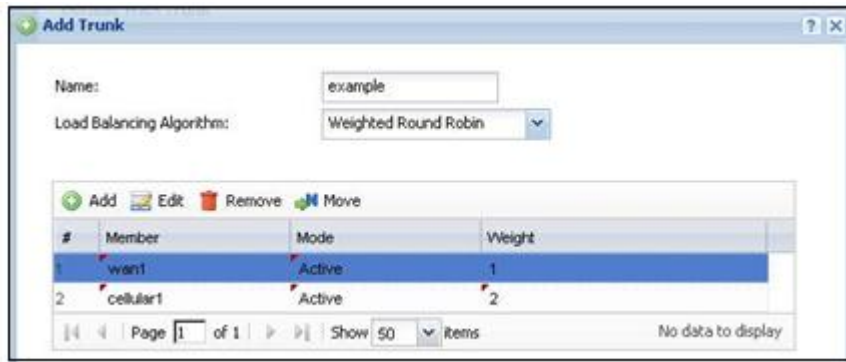
Add Trunk

Name: example

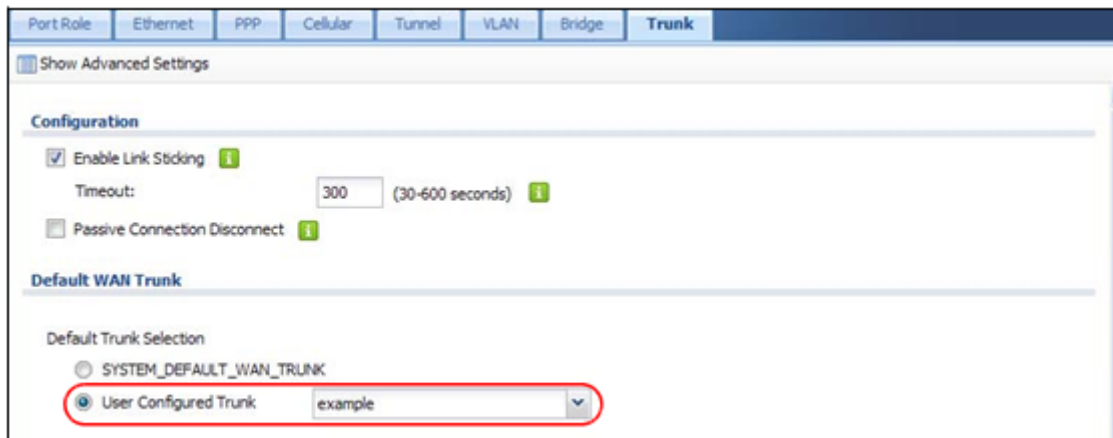
Load Balancing Algorithm: Weighted Round Robin

#	Member	Mode	Weight
1	wan1	Active	2
2	wan2	Active	1

Page 1 of 1 Show 50 Items No data to display



- 2 Select the trunk as the default trunk and click **Apply**.



4.3 How to Use Multiple Static Public WAN IP Addresses for LAN-to-WAN Traffic

If your ISP gave you a range of static public IP addresses, this example shows how to configure a policy route to have the USG use them for traffic it sends out from the LAN.

4.3.1 Create the Public IP Address Range Object

Click **Configuration > Object > Address > Add** (in **IPv4 Address Configuration**) to create the address object that represents the range of static public IP addresses. In this example you name it **Public-IPs** and it goes from 1.1.1.10 to 1.1.1.17.



4.3.2 Configure the Policy Route

Now you need to configure a policy route that has the USG use the range of public IP addresses as the source address for WAN to LAN traffic.

Click **Configuration > Network > Routing > Policy Route > Add** (in **IPv4 Configuration**). It

is recommended to add a description. This example uses **LAN-to-WAN-Range**.

Specifying a **Source Address** is also recommended. This example uses **LAN1_SUBNET**.

Set the **Source Network Address Translation** to **Public-IPs** and click **OK**.

The screenshot shows the 'Add Policy Route' configuration window. The 'Configuration' section has 'Enable' checked and 'Description' set to 'LAN-to-WAN-Range (Optional)'. The 'Criteria' section has 'User' set to 'any', 'Incoming' set to 'any (Excluding ZyWALL)', 'Source Address' set to 'LAN1_SUBNET', 'Destination Address' set to 'any', 'DSCP Code' set to 'any', 'Schedule' set to 'none', and 'Service' set to 'any'. The 'Next-Hop' section has 'Type' set to 'Auto'. The 'DSCP Marking' section has 'DSCP Marking' set to 'preserve'. The 'Address Translation' section has 'Source Network Address Translation' set to 'Public-IPs'. The 'OK' and 'Cancel' buttons are at the bottom right.

4.4 How to Use Device HA to Backup Your USG

Use device high availability (HA) to set up an additional USG as a backup gateway to ensure the default gateway is always available for the network.

Active-Passive Mode and Legacy Mode

Active-passive mode has a backup USG take over if the master USG fails and is recommended for general device failover deployments. Use legacy mode if you need a more complex relationship between the master and backup USGs, such as having both USGs active or using different USGs as the master for individual interfaces. The USGs must all use the same device HA mode (either

active-passive or legacy).

Management Access IP Addresses

For each interface you can configure an IP address in the same subnet as the interface IP address to use to manage the USG whether it is the master or the backup.

Synchronization

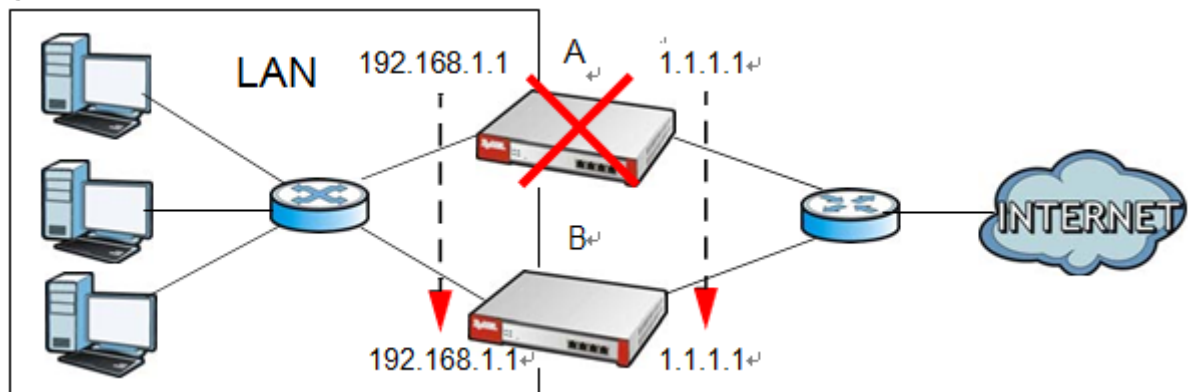
Synchronize USGs of the same model and firmware version to copy the master USG's configuration, signatures (anti-virus, IDP/application patrol, and system protect), and certificates to the backup USG so you do not need to do it manually.

4.4.1 Active-Passive Mode Device HA Example

Here active-passive mode device HA has backup USG **B** automatically takes over all of master USG **A**'s functions if **A** fails or loses its LAN or WAN connection.

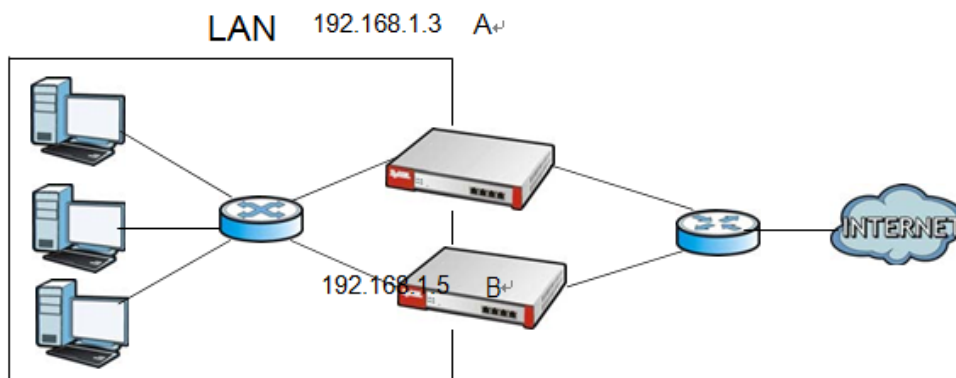
An Ethernet switch connects both USGs' LAN interfaces to the LAN. Whichever USG is functioning as the master uses the default gateway IP address of the LAN computers (192.168.1.1) for its LAN interface and the static public IP address (1.1.1.1) for its WAN interface. If USG **A** recovers (has both its LAN and WAN interfaces connected), it resumes its role as the master and takes over all of its functions again.

Figure 43 Device HA: Master Fails and Backup Takes Over



Each USG's LAN interface also has a separate management IP address that stays the same whether the USG functions as the master or a backup. USG **A**'s management IP address is 192.168.1.3 and USG **B**'s is 192.168.1.5.

Figure 44 Device HA: Management IP Addresses



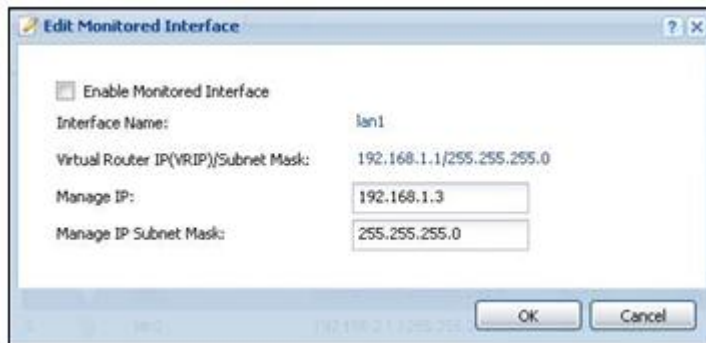
4.4.2 Before You Start

USG **A** should already be configured. You will use device HA to copy USG **A**'s settings to **B** later. To

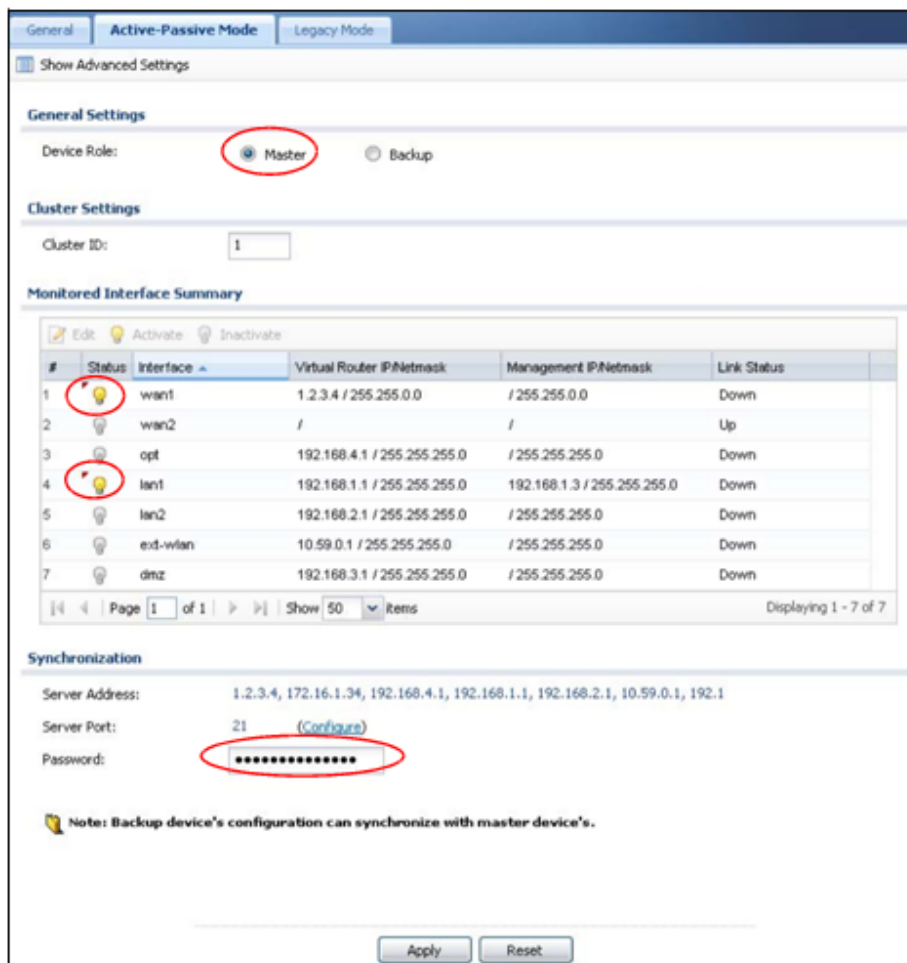
avoid an IP address conflict, do not connect USG **B** to the LAN subnet until after you configure its device HA settings and the instructions tell you to deploy it.

4.4.3 Configure Device HA on the Master USG

- 1 Log into USG **A** (the master) and click **Configuration > Device HA > Active-Passive Mode**. Double-click the LAN interface's entry.
- 2 Configure 192.168.1.3 as the **Manage IP** and 255.255.255.0 as the **Manage IP Subnet Mask**. Click **OK**.



- 3 Set the **Device Role** to **Master**. This example focuses on the connection from the LAN to the Internet through the WAN interface, so select the LAN and WAN interfaces and click **Activate**. Enter a **Synchronization Password** ("mySyncPassword" in this example). Retype the password and click **Apply**.



#	Status	Interface	Virtual Router IP/Netmask	Management IP/Netmask	Link Status
1	Lightbulb icon	wan1	1.2.3.4 / 255.255.0.0	/ 255.255.0.0	Down
2	Lightbulb icon	wan2	/	/	Up
3	Lightbulb icon	opt	192.168.4.1 / 255.255.255.0	/ 255.255.255.0	Down
4	Lightbulb icon	lan1	192.168.1.1 / 255.255.255.0	192.168.1.3 / 255.255.255.0	Down
5	Lightbulb icon	lan2	192.168.2.1 / 255.255.255.0	/ 255.255.255.0	Down
6	Lightbulb icon	ext-wlan	10.59.0.1 / 255.255.255.0	/ 255.255.255.0	Down
7	Lightbulb icon	dmz	192.168.3.1 / 255.255.255.0	/ 255.255.255.0	Down

- 4 Click the **General** tab, enable device HA, and click **Apply**.

General Settings

☒ Enable Device HA

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

4.4.4 Configure the Backup USG

- 1 Connect a computer to USG **B**'s LAN interface and log into its Web Configurator. Connect USG **B** to the Internet and subscribe it to the same subscription services (like content filtering and anti-virus) to which USG **A** is subscribed. See the **Registration** screens for more on the subscription services.
- 2 In USG **B** click **Configuration > Device HA > Active-Passive Mode** and the LAN interface **Edit** icon.
- 3 Configure 192.168.1.5 as the **Manage IP** and 255.255.255.0 as the **Subnet Mask**. Click **OK**.

Edit Monitored Interface

☒ Enable Monitored Interface

Interface Name: lan1

Virtual Router IP(VRIP)/Subnet Mask: 192.168.1.1/255.255.255.0

Manage IP: 192.168.1.5

Manage IP Subnet Mask: 255.255.255.0

OK Cancel

- 4 Set the **Device Role** to **Backup**. Activate monitoring for the LAN and WAN interfaces. Set the **Synchronization Server Address** to 192.168.1.1, the **Port** to 21, and the **Password** to "mySyncPassword". Retype the password, select **Auto Synchronize**, and set the **Interval** to 60. Click **Apply**.

General Settings

Device Role: ☐ Master ☒ Backup

Priority: 1 (1-254)

☐ Enable Preemption

Cluster Settings

Cluster ID: 1

Monitored Interface Summary

#	Status	Interface	Virtual Router IP/Netmask	Management IP/Netmask	Link Status
1		wan1	1.2.3.4 / 255.255.0.0	/ 255.255.0.0	Down
2		wan2	/	/	Up
3		opt	192.168.4.1 / 255.255.255.0	/ 255.255.255.0	Down
4		lan1	192.168.1.1 / 255.255.255.0	192.168.1.5 / 255.255.255.0	Down
5		lan2	192.168.2.1 / 255.255.255.0	/ 255.255.255.0	Down
6		ext-wlan	10.59.0.1 / 255.255.255.0	/ 255.255.255.0	Down
7		dmz	192.168.3.1 / 255.255.255.0	/ 255.255.255.0	Down

Synchronization

Server Address: 192.168.1.1 (IP or FQDN)

Server Port: 21

Password: mySyncPassword

☒ Auto Synchronize

Interval: 60 minutes (5-1440)

- 5 In the **General** tab enable device HA and click **Apply**.



4.4.5 Deploy the Backup USG

Connect USG **B**'s LAN interface to the LAN network. Connect USG **B**'s WAN interface to the same router that USG **A**'s WAN interface uses for Internet access. USG **B** copies **A**'s configuration (and re-synchronizes with **A** every hour). If USG **A** fails or loses its LAN or WAN connection, USG **B** functions as the master.

4.4.6 Check Your Device HA Setup

- 1 To make sure USG **B** copied USG **A**'s settings, you can log into USG **B**'s management IP address (192.168.1.5) and check the configuration. You can use the **Maintenance > File Manager > Configuration File** screen to save copies of the USGs' configuration files that you can compare.
- 2 To test your device HA configuration, disconnect USG **A**'s LAN or WAN interface. Computers on LAN should still be able to access the Internet. If they cannot, check your connections and device HA configuration.

Congratulations! Now that you have configured device HA for LAN, you can use the same process for any of the USG's other local networks. For example, enable device HA monitoring on the DMZ interfaces and use an Ethernet switch to connect both USGs' DMZ interfaces to your publicly available servers.

4.5 How to Configure DNS Inbound Load Balancing

This example shows you how to configure the USG to respond to DNS query messages with the least loaded interface's IP address. The DNS query senders will then transmit packets to that interface instead of an interface that has a heavy load.

This example assumes that your company's domain name is www.example.com. You want your USG's WAN1 (202.1.2.3) and WAN2 (202.5.6.7) to use DNS inbound load balancing to balance traffic loading coming from the Internet.

- 1 In the **CONFIGURATION > Network > Inbound LB** screen, select **Enable DNS Load Balancing**. Click **Apply**.



- 2 Click **Add** in the **Configuration** table. The following screen appears.
Select **Enable**, enter ***.example.com** as the **Query Domain Name**.
Enter **300** in the **Time to Live** field to have DNS query senders keep the resolved DNS entries on

their computers for 5 minutes.

Select **any** in the **IP Address** field and **WAN** in the **Zone** field to apply this rule for all DNS query messages the WAN zone receives.

Select **Least Load - Total** as the load balancing algorithm.

Click **Add** to add WAN1 and WAN2 as the member interfaces. Click **OK**.

The screenshot shows the 'Add DNS Load Balancing' configuration window. The 'General Settings' section has 'Enable' checked. The 'DNS Setting' section has 'Query Domain Name' set to '*.example.com' and 'Time to Live' set to 300. The 'Query From Setting' section has 'IP Address' set to 'any' and 'Zone' set to 'WAN'. The 'Load Balancing Member' section has 'Load Balancing Algorithm' set to 'Least Load - Total' and 'Failover IP Address' set to '0.0.0.0'. Below this is a table with two members: Member 1 with IP 202.1.2.3 and Monitor Interface wan1, and Member 2 with IP 202.5.6.7 and Monitor Interface wan2. Two callout boxes show the 'Load Balancing Member' configuration for each member, confirming the 'Same as Monitor Interface' IP address setting.

Continue to go to the **Configuration > Firewall** and **Configuration > Network > NAT** screens to configure the corresponding firewall rules and NAT virtual server for the inbound service access.

4.5.1 What Can Go Wrong?

- Using a greater TTL value makes DNS inbound load balancing become ineffective, although it can reduce the USG's loading as the DNS request senders does not need to send new queries to the USG that often.
- If you choose **Custom** in the **Load Balancing Member** screen and enter another IP address for a member interface, make sure the entered IP address is configured in the corresponding firewall and NAT virtual server rules.

4.6 How to Allow Public Access to a Web Server

This is an example of making an HTTP (web) server in the DMZ zone accessible from the Internet (the WAN zone). In this example you have public IP address 1.1.1.1 that you will use on the WAN interface and map to the HTTP server's private IP address of 192.168.3.7.

Figure 45 Public Server Example Network Topology



4.6.1 Configure NAT

Create a NAT rule to send HTTP traffic coming to WAN IP address 1.1.1.1 to the HTTP server's private IP address of 192.168.3.7.

- 1 Click **Configuration > Network > NAT > Add > Create New Object > Address** and create an IPv4 host address object named **DMZ_HTTP** for the HTTP server's private IP address of 192.168.3.7. Repeat to create a host address object named **Public_HTTP_Server_IP** for the public WAN IP address 1.1.1.1.

- 2 Configure the NAT rule.

For the **Incoming Interface** select the WAN interface.

Set the **Original IP** to the **Public_HTTP_Server_IP** object and the **Mapped IP** to the **DMZ_HTTP** object.

HTTP traffic and the HTTP server in this example both use TCP port 80. So you set the **Port Mapping Type** to **Port**, the **Protocol Type** to **TCP**, and the original and mapped ports to 80.

Keep **Enable NAT Loopback** selected to allow users connected to other interfaces to access the HTTP server.

The image shows two overlapping configuration windows. The main window is 'Add NAT' with the following settings:

- General Settings:** 'Enable Rule' is checked. 'Rule Name' is 'DMZ_HTTP'.
- Port Mapping Type:** 'Classification' is 'Virtual Server'.
- Mapping Rule:** 'Incoming Interface' is 'wan1', 'Original IP' is 'Public_HTTP_Server_IP', 'Mapped IP' is 'DMZ_HTTP', 'Port Mapping Type' is 'Port', 'Protocol Type' is 'TCP', 'Original Port' is '80', and 'Mapped Port' is '80'.
- Related Settings:** 'Enable NAT Loopback' is checked.

An 'Add Address Rule' window is open over the 'Add NAT' window, showing:

- Name:** 'Public_HTTP_Server_IP'
- Address Type:** 'HOST'
- IP Address:** '1.1.1.1'

4.6.2 Set Up a Firewall Rule

Create a firewall rule to allow the public to send HTTP traffic to IP address 1.1.1.1 in order to access the HTTP server. If a domain name is registered for IP address 1.1.1.1, users can just go to the domain name to access the web server.

Click **Configuration > Firewall > Add**. Set the **From** field as **WAN** and the **To** field as **DMZ**. Set the **Destination** to the HTTP server's DMZ IP address object (**DMZ_HTTP**). **DMZ_HTTP** is the destination because the USG applies NAT to traffic before applying the firewall rule. Set the **Access** field to **allow** and the **Service** to **HTTP**, and click **OK**.

The image shows the 'Add Firewall Rule' configuration window with the following settings:

- Enable:** Checked
- From:** 'WAN' (highlighted with a red circle)
- To:** 'DMZ' (highlighted with a red circle)
- Description:** (Optional)
- Schedule:** 'none'
- User:** 'any'
- Source:** 'any'
- Destination:** 'DMZ_HTTP' (highlighted with a red circle)
- Service:** 'HTTP' (highlighted with a red circle)
- Access:** 'allow' (highlighted with a red circle)
- Log:** 'no'

4.6.3 What Can Go Wrong

- The USG checks the firewall rules in order and applies the first firewall rule the traffic matches. If traffic matches a rule that comes earlier in the list, it may be unexpectedly blocked.
- The USG does not apply the firewall rule. The USG only apply's a zone's rules to the interfaces that belong to the zone. Make sure the WAN interface is assigned to WAN zone.

4.7 How to Manage Voice Traffic

Here are examples of allowing H.323 and SIP traffic through the USG.

4.7.1 How to Allow Incoming H.323 Peer-to-peer Calls

Suppose you have a H.323 device on the LAN for VoIP calls and you want it to be able to receive peer-to-peer calls from the WAN. Here is an example of how to configure NAT and the firewall to have the USG forward H.323 traffic destined for WAN IP address 10.0.0.8 to a H.323 device located on the LAN and using IP address 192.168.1.56.

Figure 46 WAN to LAN H.323 Peer-to-peer Calls Example



4.7.1.1 Turn On the ALG

Click **Configuration > Network > ALG**. Select **Enable H.323 ALG** and **Enable H.323 transformations** and click **Apply**.

Figure 47 Configuration > Network > ALG

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 :

H.323 Settings

- ☒ **Enable H.323 ALG**
- ☒ Enable H.323 Transformations
- H.323 Signaling Port : 1720 (1025-65535)
- Additional H.323 Signaling Port for Transformations : (1025-65535) (Optional)

4.7.1.2 Set Up a NAT Policy For H.323

In this example, you need a NAT policy to forward H.323 (TCP port 1720) traffic received on the

- 1 Click **Configuration > Network > NAT > Add > Create New Object > Address** and create an IPv4 host address object for the public WAN IP address (called WAN_IP-for-H323 here). Repeat to create an address object for the H.323 device's private LAN IP address (called LAN_H323 here).

Configure a name for the rule (WAN-LAN_H323 here).

You want the LAN H.323 device to receive peer-to-peer calls from the WAN and also be able to initiate calls to the WAN so you set the **Classification** to **NAT 1:1**.

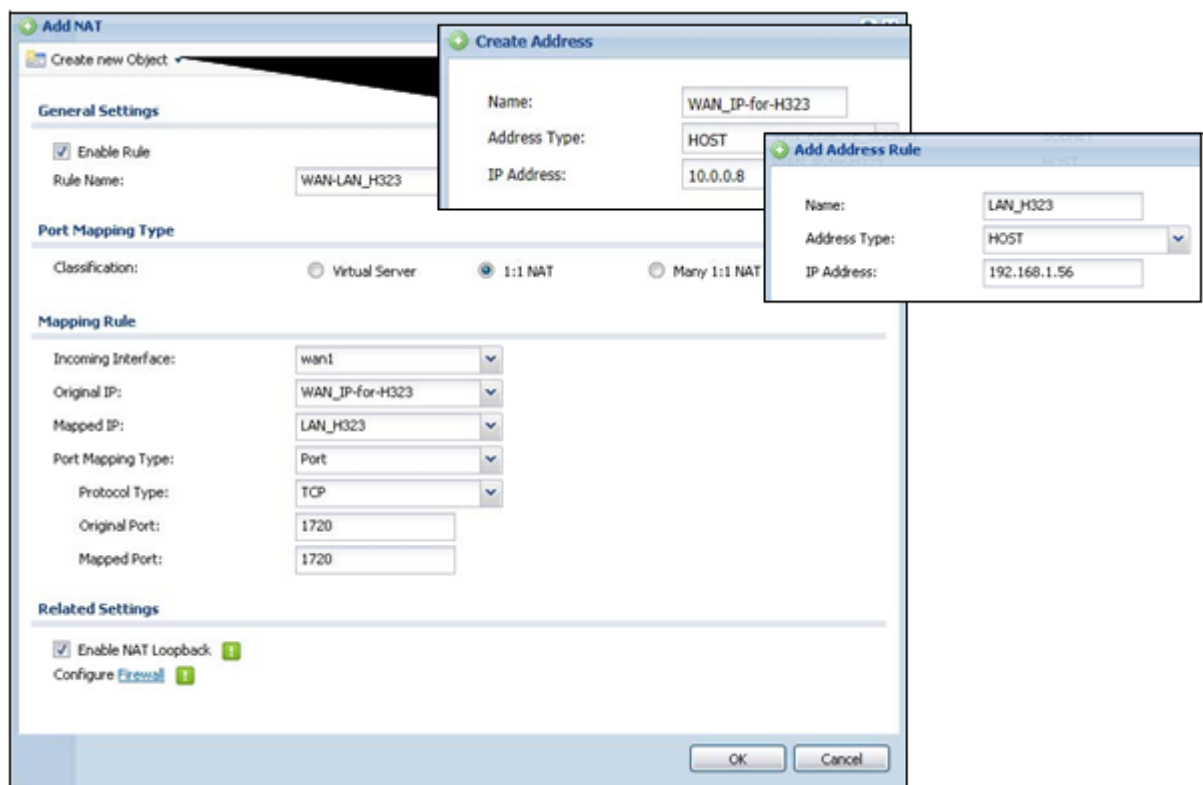
Set the **Incoming Interface** to the WAN interface.

Set the **Original IP** to the WAN address object (**WAN_IP-for-H323**).

Set the **Mapped IP** to the H.323 device's LAN IP address object (**LAN_H323**).

Set the **Port Mapping Type** to **Port**, the **Protocol Type** to **TCP** and the original and mapped ports to 1720.

Click **OK**.



4.7.1.3 Set Up a Firewall Rule For H.323

Configure a firewall rule to allow H.323 (TCP port 1720) traffic received on the WAN_IP-for-H323 IP address to go to LAN IP address 192.168.1.56.

- 1 Click **Configuration > Firewall > Add**.

In the **From** field select WAN.

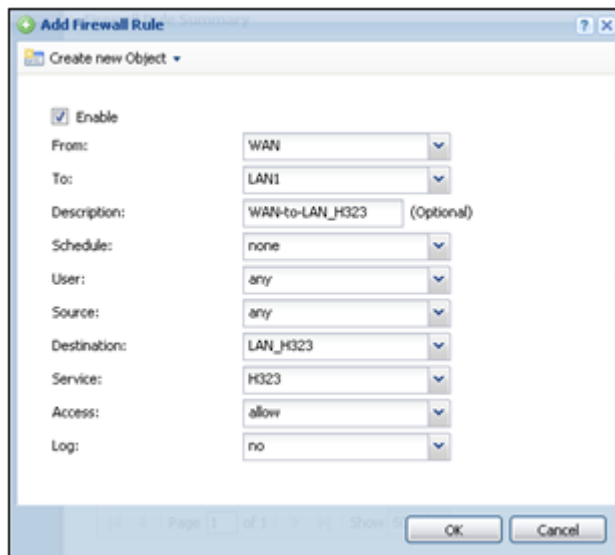
In the **To** field select LAN1.

Configure a name for the rule (WAN-to-LAN_H323 here).

Set the **Destination** to the H.323 device's LAN1 IP address object (**LAN_H323**). **LAN_H323** is the destination because the USG applies NAT to traffic before applying the firewall rule.

Set the **Service** to **H.323**.

Click **OK**.



4.7.2 How to Use an IPPBX on the DMZ

This is an example of making an IPPBX x6004 using SIP in the DMZ zone accessible from the Internet (the WAN zone). In this example you have public IP address 1.1.1.2 that you will use on the WAN interface and map to the IPPBX's private IP address of 192.168.3.9. The local SIP clients are on the LAN.

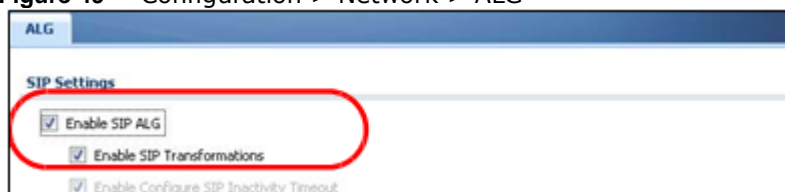
Figure 48 IPPBX Example Network Topology



4.7.2.1 Turn On the ALG

Click **Configuration > Network > ALG**. Select **Enable SIP ALG** and **Enable SIP Transformations** and click **Apply**.

Figure 49 Configuration > Network > ALG



4.7.2.2 Set Up a NAT Policy for the IPPBX

Click **Configuration > Network > NAT > Add > Create New Object > Address** and create an IPv4 host address object for the IPPBX's private DMZ IP address of 192.168.3.9. Repeat to create a host address object named IPPBX-Public for the public WAN IP address 1.1.1.2.

- Configure a name for the rule (WAN-DMZ_IPPBX here).
- You want the IPPBX to receive calls from the WAN and also be able to send calls to the WAN so you set the **Classification** to **NAT 1:1**.

- Set the **Incoming Interface** to use the WAN interface.
- Set the **Original IP** to the WAN address object (**IPPBX-Public**). If a domain name is registered for IP address 1.1.1.2, users can use it to connect to for making SIP calls.
- Set the **Mapped IP** to the IPPBX's DMZ IP address object (**IPPBX-DMZ**).
- Set the **Port Mapping Type** to **Port**, the **Protocol Type** to **UDP** and the original and mapped ports to 5060.
- Keep **Enable NAT Loopback** selected to allow the LAN users to use the IPPBX.
- Click **OK**.

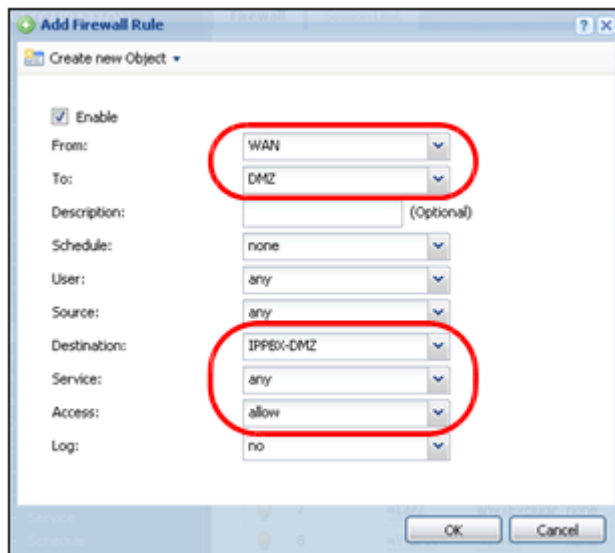
Figure 50 Configuration > Network > NAT > Add

The screenshot shows the 'Add NAT' configuration window. The 'General Settings' section has 'Enable Rule' checked and 'Rule Name' set to 'WAN-DMZ_IPPBX'. The 'Port Mapping Type' section has 'Classification' set to '1:1 NAT'. The 'Mapping Rule' section has 'Incoming Interface' set to 'wan1', 'Original IP' set to 'IPPBX-Public', 'Mapped IP' set to 'IPPBX-DMZ', 'Port Mapping Type' set to 'Port', 'Protocol Type' set to 'UDP', 'Original Port' set to '5060', and 'Mapped Port' set to '5060'. The 'Related Settings' section has 'Enable NAT Loopback' checked. Two 'Add Address Rule' sub-windows are overlaid. The top one has 'Name' set to 'IPPBX-DMZ', 'Address Type' set to 'HOST', and 'IP Address' set to '192.168.3.9'. The bottom one has 'Name' set to 'IPPBX-Public', 'Address Type' set to 'HOST', and 'IP Address' set to '1.1.1.2'.

4.7.2.3 Set Up a WAN to DMZ Firewall Rule for SIP

The firewall blocks traffic from the WAN zone to the DMZ zone by default so you need to create a firewall rule to allow the public to send SIP traffic to the IPPBX. If a domain name is registered for IP address 1.1.1.2, users can use it to connect to for making SIP calls.

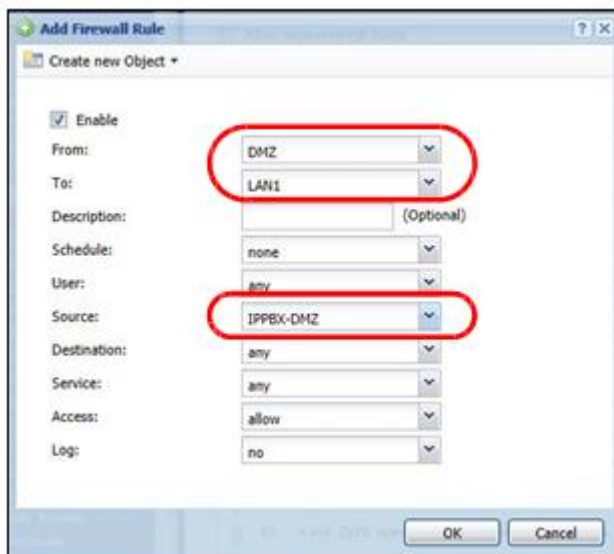
Click **Configuration > Firewall > Add**. Set the **From** field as **WAN** and the **To** field as **DMZ**. Set the **Destination** to the IPPBX's DMZ IP address object (**DMZ_SIP**). **IPPBX_DMZ** is the destination because the USG applies NAT to traffic before applying the firewall rule. Set the **Access** field to **allow** and click **OK**.



4.7.2.4 Set Up a DMZ to LAN Firewall Rule for SIP

The firewall blocks traffic from the DMZ zone to the LAN1 zone by default so you need to create a firewall rule to allow the IPPBX to send SIP traffic to the SIP clients on the LAN.

- 1 Click **Configuration > Firewall > Add**. Set the **From** field as **DMZ** and the **To** field as **LAN1**. Set the **Destination** to the IPPBX's DMZ IP address object (**DMZ_SIP**). Set the **Source** to **IPPBX_DMZ**. Leave the **Access** field to **allow** and click **OK**.



4.7.3 What Can Go Wrong

- The USG checks the firewall rules in order and applies the first firewall rule the traffic matches. If traffic matches a rule that comes earlier in the list, it may be unexpectedly blocked.
- The USG does not apply the firewall rule. The USG only apply's a zone's rules to the interfaces that belong to the zone. Make sure the WAN interface is assigned to WAN zone.

4.8 How to Limit Web Surfing and MSN to Specific People

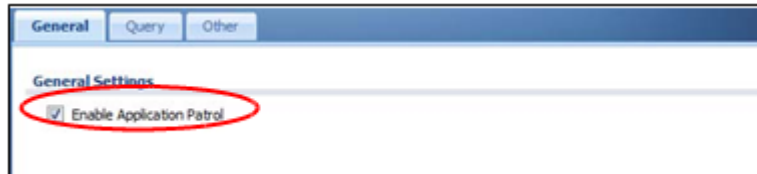
The following is an example of using application patrol (AppPatrol) to enforce web surfing and MSN

policies for the sales department of a company.

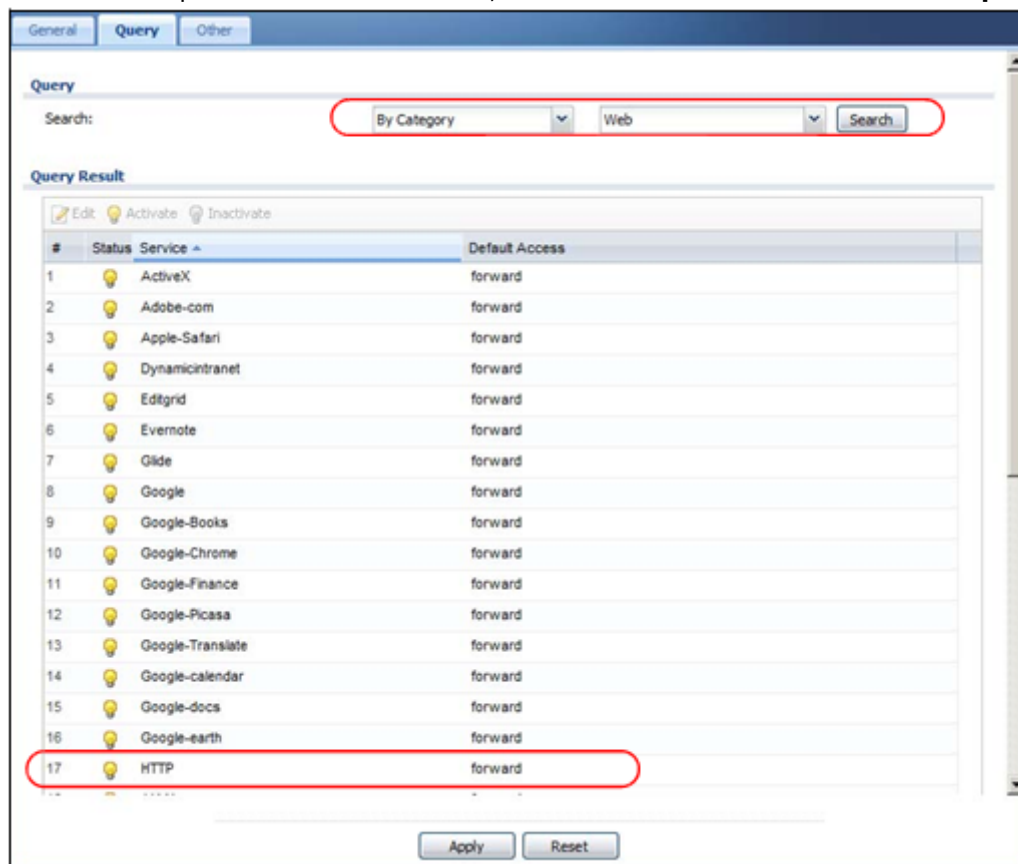
4.8.1 Set Up Web Surfing Policies

Before you configure any policies, you must have already subscribed for the application patrol service. You can subscribe using the **Configuration > Licensing > Registration** screens or using one of the wizards.

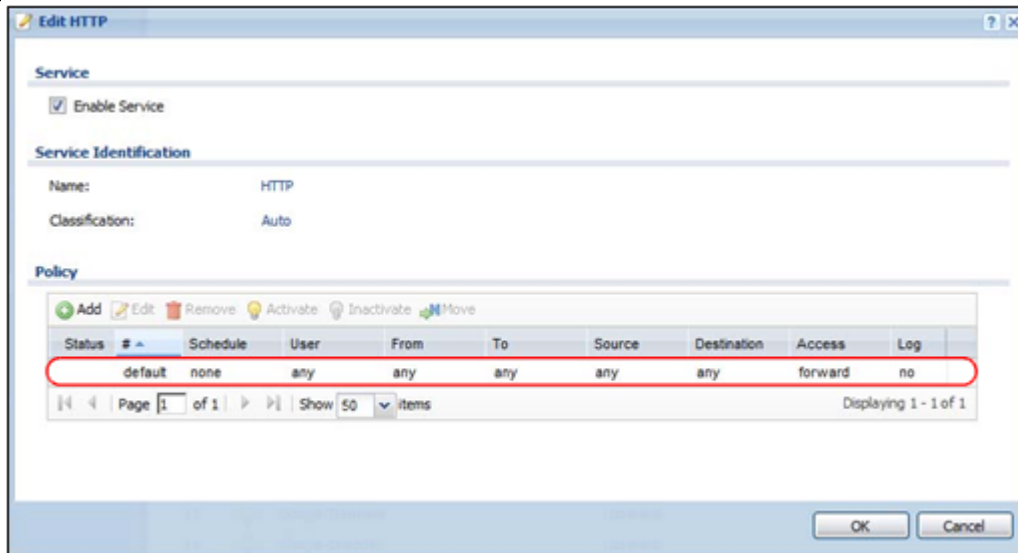
- 1 Click **Configuration > AppPatrol**. If application patrol is not enabled, enable it, and click **Apply**.



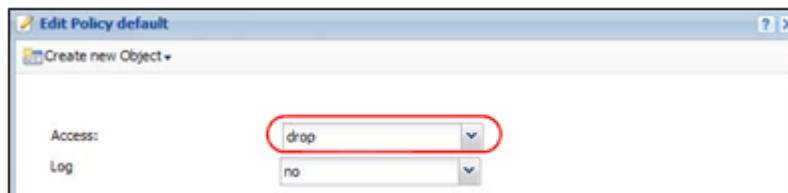
- 2 Click **Configuration > AppPatrol > Query**. In the first drop down menu select **By Category** and in the second drop down menu select **Web**, then click **Search**. Double-click the **http** entry to edit it.



- 3 Double-click the **Default** policy.



- 4 Change the access to **Drop** because you do not want anyone except authorized user groups to browse the web. Click **OK**.



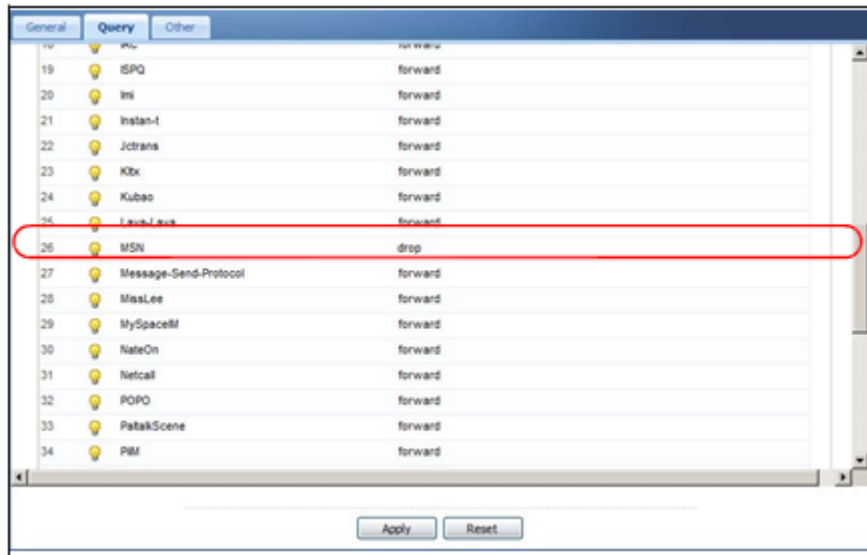
- 5 Click the **Add** icon in the policy list. In the new policy, select **Sales** as the user group allowed to browse the web. (The user group should be set in the **Configuration > Object > User/Group > Group > Add** screen.) Click **OK**.



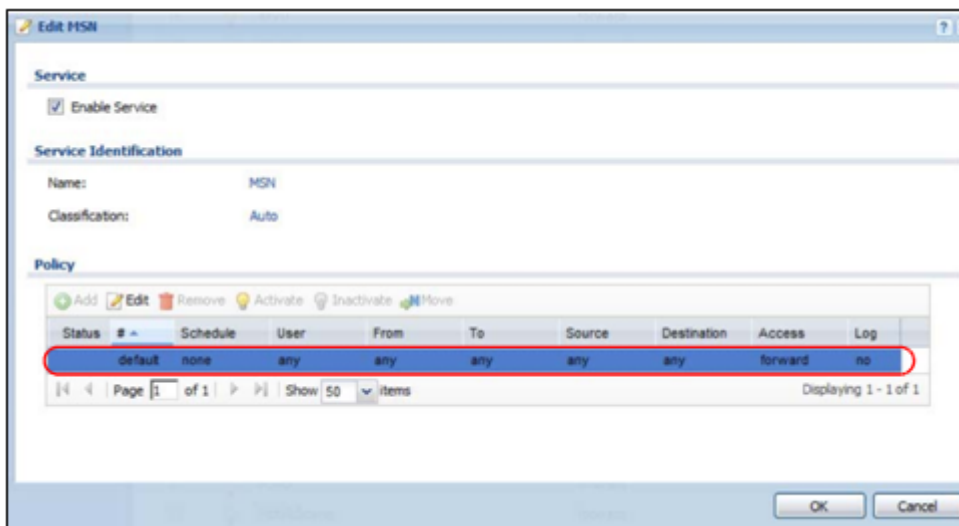
4.8.2 Set Up MSN Policies

In this part of the tutorial, you can set up a recurring schedule and apply it to the MSN application patrol rule so that only the sales department is allowed to use MSN during work hours on weekdays.

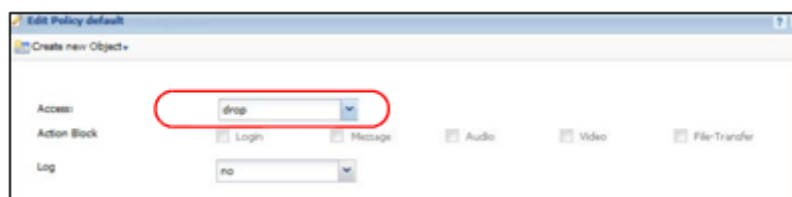
- 1 Click **Configuration > AppPatrol > Query**, and in the second dropdown menu, select **Instant Messenger**, and click **Search**. Then, double-click the **msn** entry to edit it.



2 Double-click the **Default** policy.



3 Change the access to **Drop** because you do not want anyone except the authorized user group (sales) to use MSN. Click **OK**.



4 Now you will need to set up a recurring schedule object first. Click **Configuration > Object > Schedule**. Click the **Add** icon for recurring schedules.

5 Give the schedule a descriptive name such as **WorkHours**. Set up the days (Monday through Friday) and the times (08:00 - 17:30) when the sales group is allowed to use MSN. Click **OK**.

Add Schedule Recurring Rule

Configuration

Name: WorkHours

Day Time

Start Time: 08:00

Stop Time: 17:30

Weekly

Week Days: ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☐ Saturday ☐ Sunday

- 6 Click **Configuration > AppPatrol > Query**, and in the second dropdown menu, select **Instant Messenger**, and click **Search**. Then, double-click the **msn** entry to edit it.

Protocol	Access	
19	ISPO	forward
20	Im	forward
21	Instant	forward
22	Jctrans	forward
23	Kbx	forward
24	Kubao	forward
25	Love-Love	forward
26	MSN	drop
27	Message-Send-Protocol	forward
28	MissLee	forward
29	MySpaceIM	forward
30	NateOn	forward
31	Netcall	forward
32	POPO	forward
33	PatakiScene	forward
34	PIM	forward

- 7 Click the **Add** icon in the policy list. In the new policy, select **WorkHours** as the schedule and **Sales** as the user group that is allowed to use MSN at the appointed schedule. Then select **forward** in the **Access** field. Click **OK to finish the setup**.

Edit Policy 1

Create new Object

☒ Enable Policy

Port: 0 (0 : any)

Schedule: WorkHours

User: Sales

From: any

To: any

Source: any

Destination: any

Access: forward

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

Log: no

OK Cancel

Now only the sales group may use MSN during work hours on week days.

4.8.3 What Can Go Wrong

If you have not already subscribed for the application patrol service, you will not be able to configure any policies. You can do so by using the **Configuration > Licensing > Registration** screens or using one of the wizards.