ZyWALL USG Series

Unified Security Gateway

Version 4.20
Edition 1, 08/2016

Application Notes

Table of Contents

Scenario 1 — How to Configure NAT if you have Internet-facing Public Servers

1.1 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.

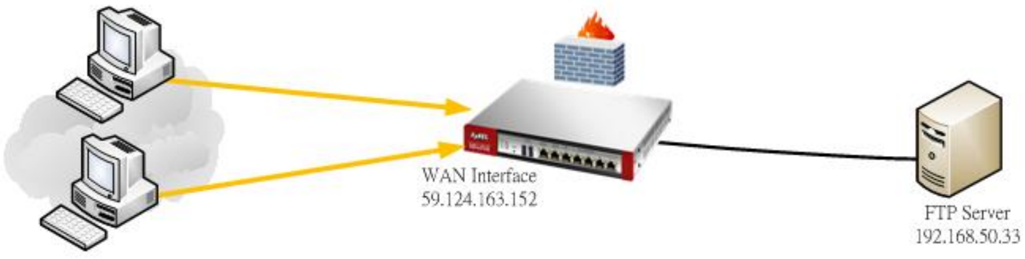
1.2 Configuration Guide

Goal to achieve:

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

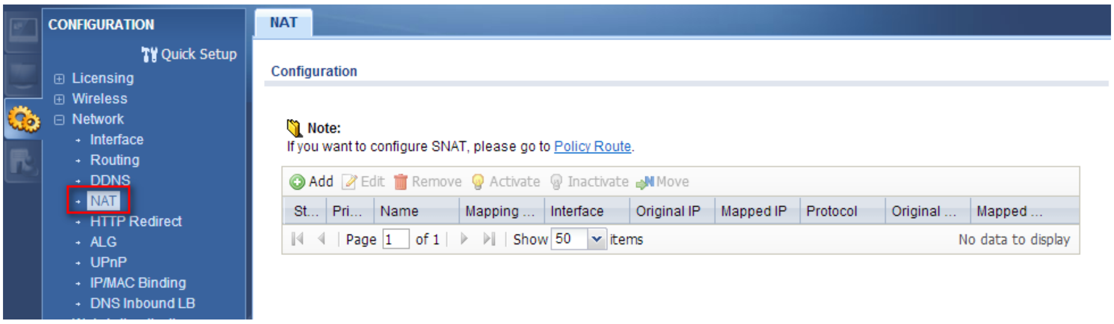
Network Conditions: USG-50:

- 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.

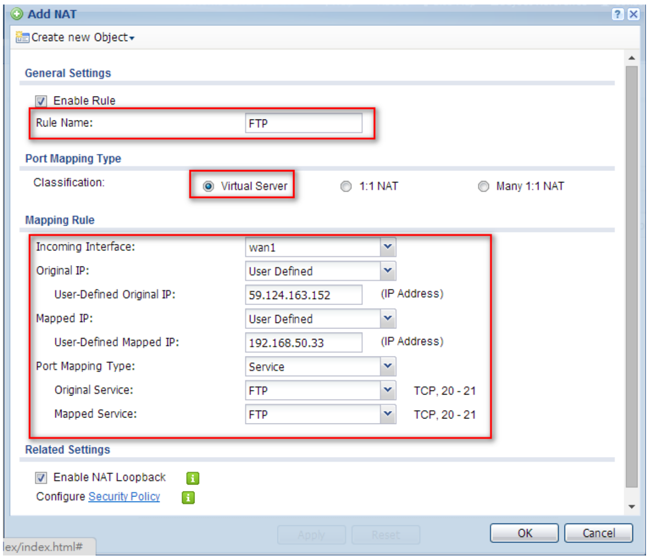


Note:
If you want to configure SNAT, please go to Policy Route.

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



☑ Enable Rule

Rule Name: FTP

Classification: ● Virtual Server ○ 1:1 NAT ○ Many 1:1 NAT

Incoming Interface:	wan1	
Original IP:	User Defined	
User-Defined Original IP:	59.124.163.152	(IP Address)
Mapped IP:	User Defined	
User-Defined Mapped IP:	192.168.50.33	(IP Address)
Port Mapping Type:	Service	
Original Service:	FTP	TCP, 20 - 21
Mapped Service:	FTP	TCP, 20 - 21

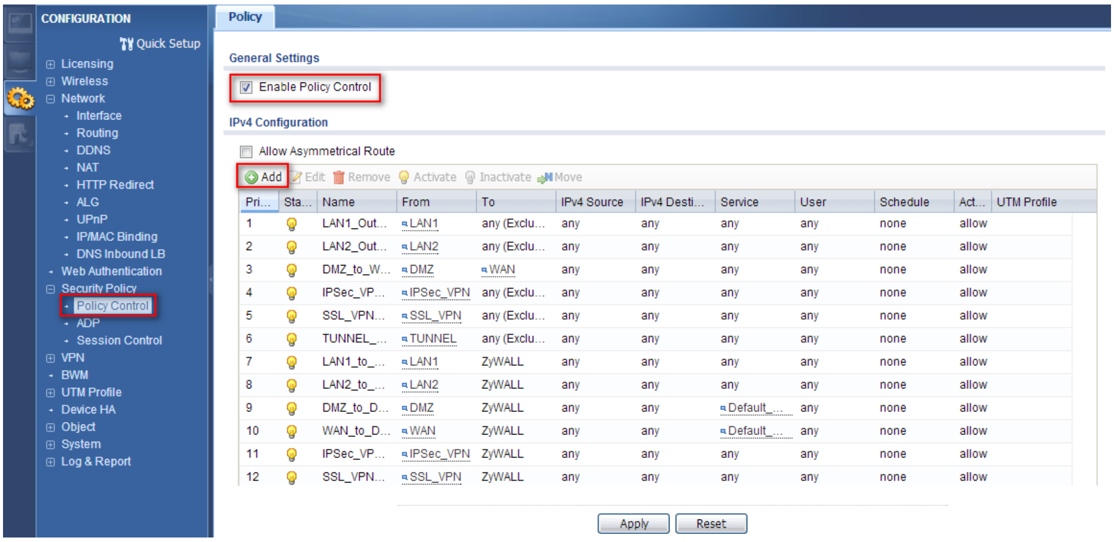
☑ Enable NAT Loopback

Configure Security Policy

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.



General Settings

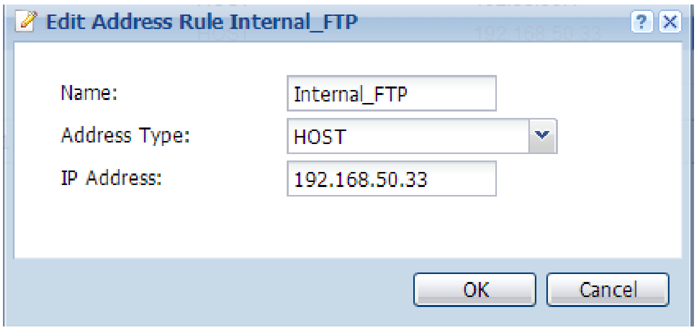
☑ Enable Policy Control

IPv4 Configuration

□ Allow Asymmetrical Route

Pri...	Sta...	Name	From	To	IPv4 Source	IPv4 Desti...	Service	User	Schedule	Act...	UTM Profile
1	●	LAN1_Out...	LAN1	any (Exclu...	any	any	any	any	none	allow	
2	●	LAN2_Out...	LAN2	any (Exclu...	any	any	any	any	none	allow	
3	●	DMZ_to_W...	DMZ	WAN	any	any	any	any	none	allow	
4	●	IPSec_VP...	IPSec_VPN	any (Exclu...	any	any	any	any	none	allow	
5	●	SSL_VPN...	SSL_VPN	any (Exclu...	any	any	any	any	none	allow	
6	●	TUNNEL_...	TUNNEL	any (Exclu...	any	any	any	any	none	allow	
7	●	LAN1_to_...	LAN1	ZyWALL	any	any	any	any	none	allow	
8	●	LAN2_to_...	LAN2	ZyWALL	any	any	any	any	none	allow	
9	●	DMZ_to_D...	DMZ	ZyWALL	any	any	Default_...	any	none	allow	
10	●	WAN_to_D...	WAN	ZyWALL	any	any	Default_...	any	none	allow	
11	●	IPSec_VP...	IPSec_VPN	ZyWALL	any	any	any	any	none	allow	
12	●	SSL_VPN...	SSL_VPN	ZyWALL	any	any	any	any	none	allow	

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.



Edit Address Rule Internal_FTP

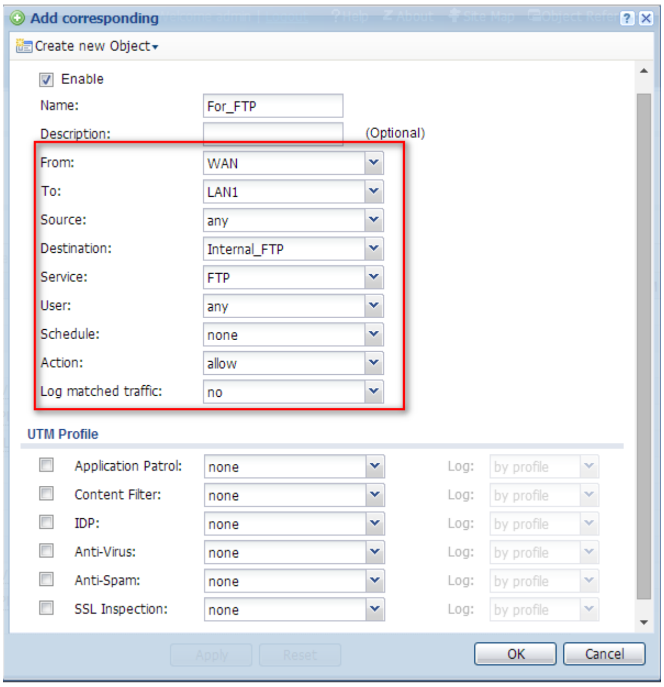
Name: Internal_FTP

Address Type: HOST

IP Address: 192.168.50.33

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

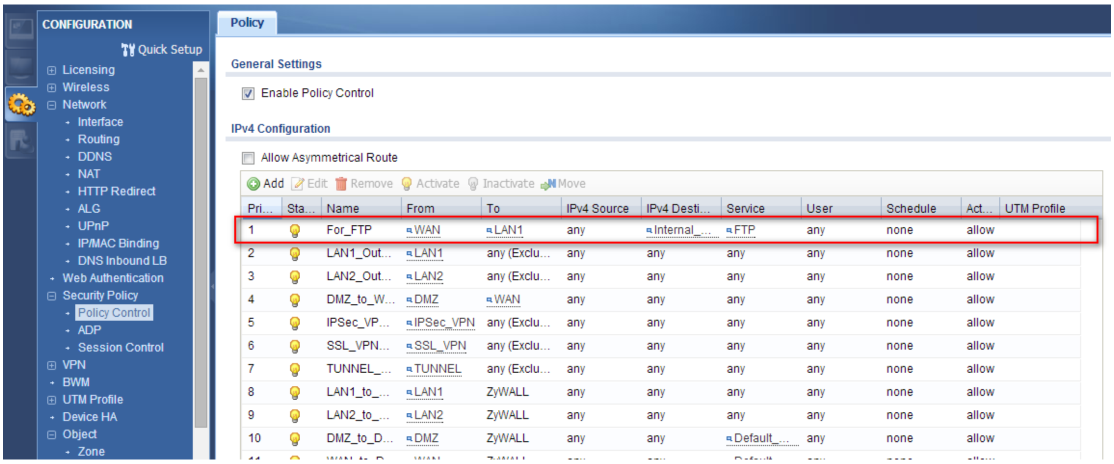


☑ Enable

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

□ 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

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



General Settings

☑ Enable Policy Control

IPv4 Configuration

□ Allow Asymmetrical Route

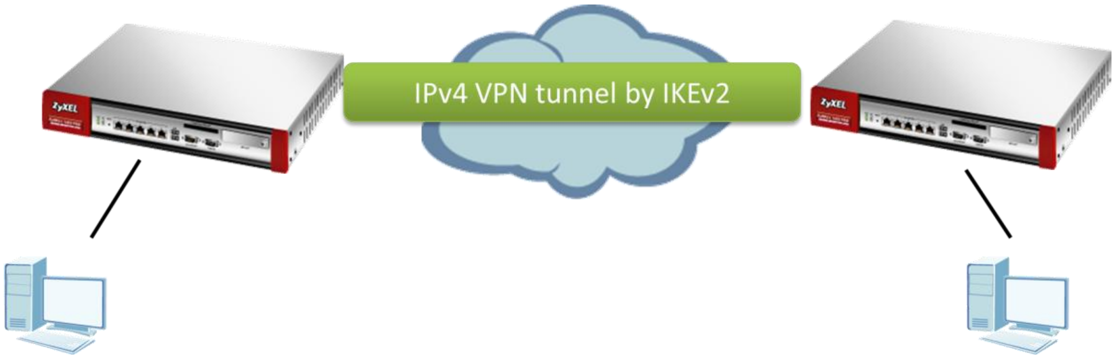
Pri...	Sta...	Name	From	To	IPv4 Source	IPv4 Desti...	Service	User	Schedule	Act...	UTM Profile
1	💡	For_FTP	WAN	LAN1	any	Internal_...	FTP	any	none	allow	
2	💡	LAN1_Out...	LAN1	any (Exclu...	any	any	any	any	none	allow	
3	💡	LAN2_Out...	LAN2	any (Exclu...	any	any	any	any	none	allow	
4	💡	DMZ_to_W...	DMZ	WAN	any	any	any	any	none	allow	
5	💡	IPSec_VP...	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	any	Default_...	any	none	allow	

Scenario 2 — Secure Site-to-site Connections using IPSec VPN – IPv4 with IKEv2 / IPv6

2.1 Application Scenario

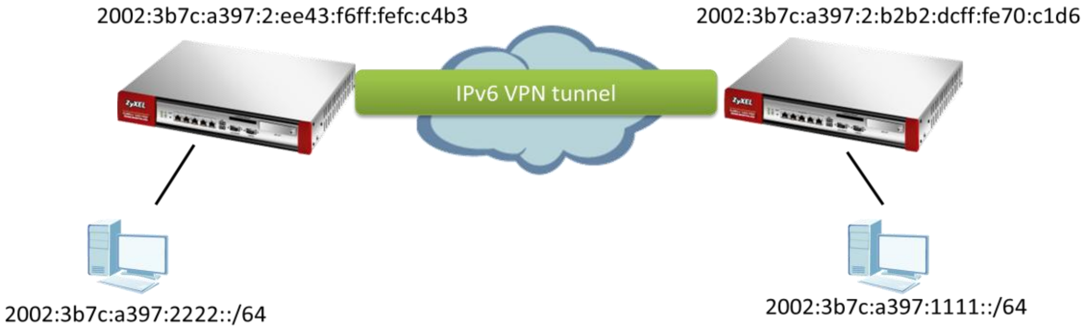
IPv4 with IKEv2

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.


2002:3b7c:a397:2:ee43:f6ff:fefc:c4b3
2002:3b7c:a397:2:b2b2:dcff:fe70:c1d6
IPv6 VPN tunnel
2002:3b7c:a397:2222::/64
2002:3b7c:a397:1111::/64

2.2 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:

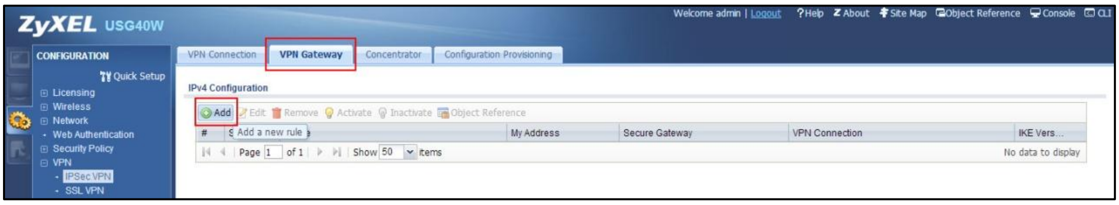
Phase 1:	**Phase 2:**
IKE version: IKEv2	Active Protocol: ESP
Authentication: 1234567890	Encapsulation Mode: Tunnel
Local/Peer ID type: IPv4 0.0.0.0 / Any	Encryption Algorithm: DES
Encryption Algorithm: 3DES	Authentication Algorithm: SHA1
Authentication Algorithm: MD5	Perfect Forward Secrecy: None
Key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

Goal to achieve:

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

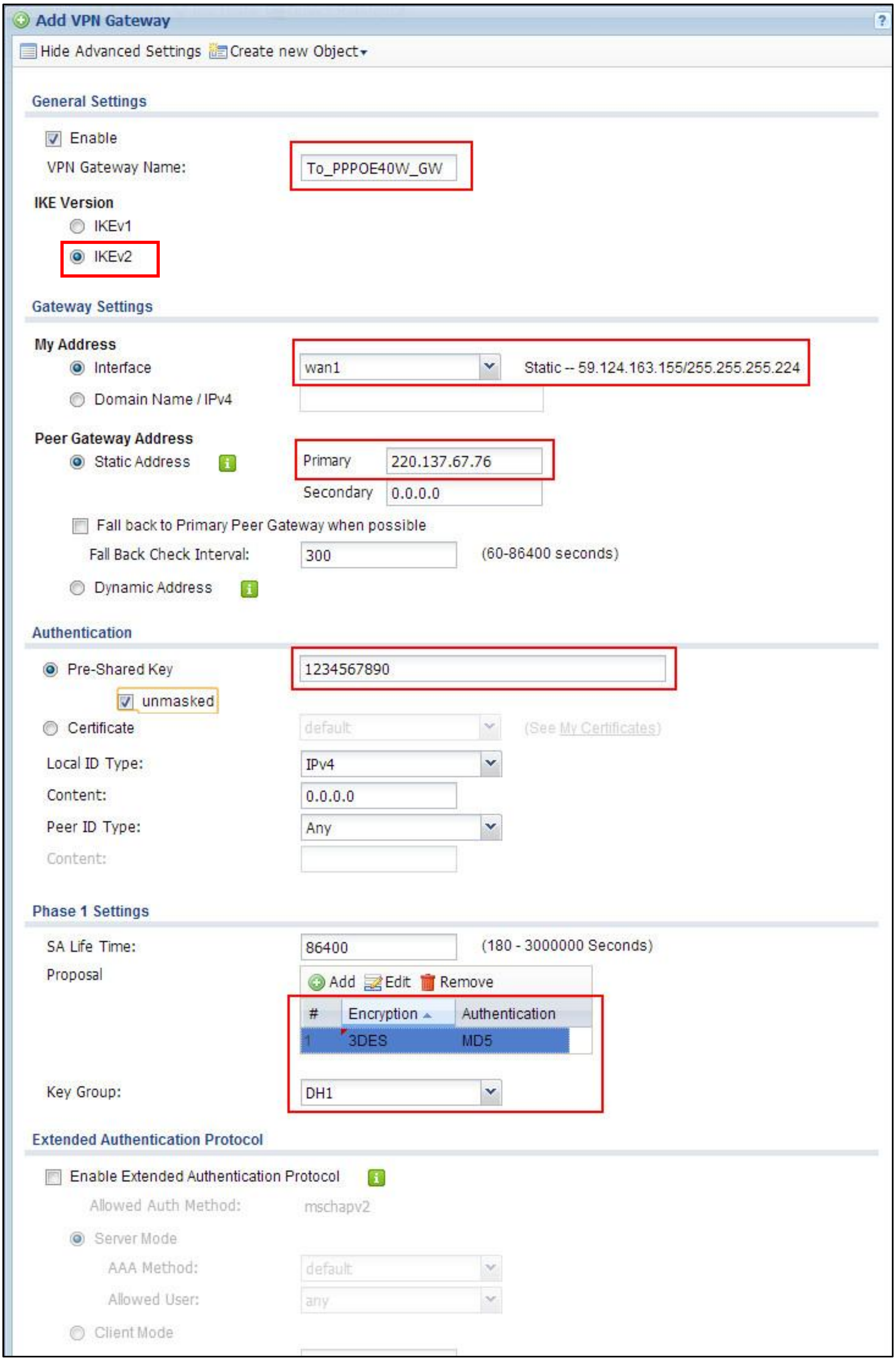
Step 1. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** to open the configuration screen.

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

#	Encryption	Authentication
1	3DES	MD5

Key Group: DH1

Extended Authentication Protocol

□ Enable Extended Authentication Protocol

Allowed Auth Method: mschapv2

● Server Mode

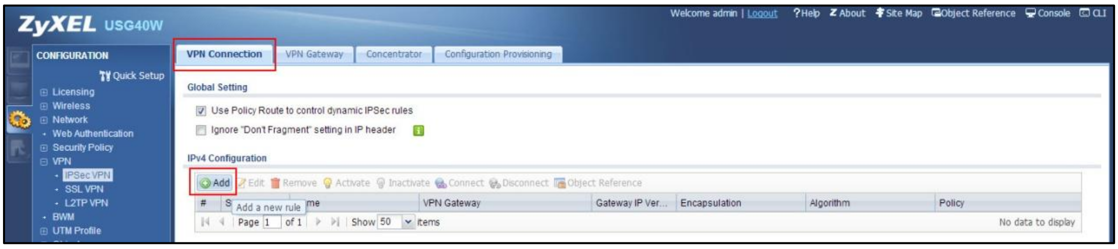
AAA Method: default

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.



☑ Use Policy Route to control dynamic IPSec rules

□ Ignore "Don't Fragment" setting in IP header

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

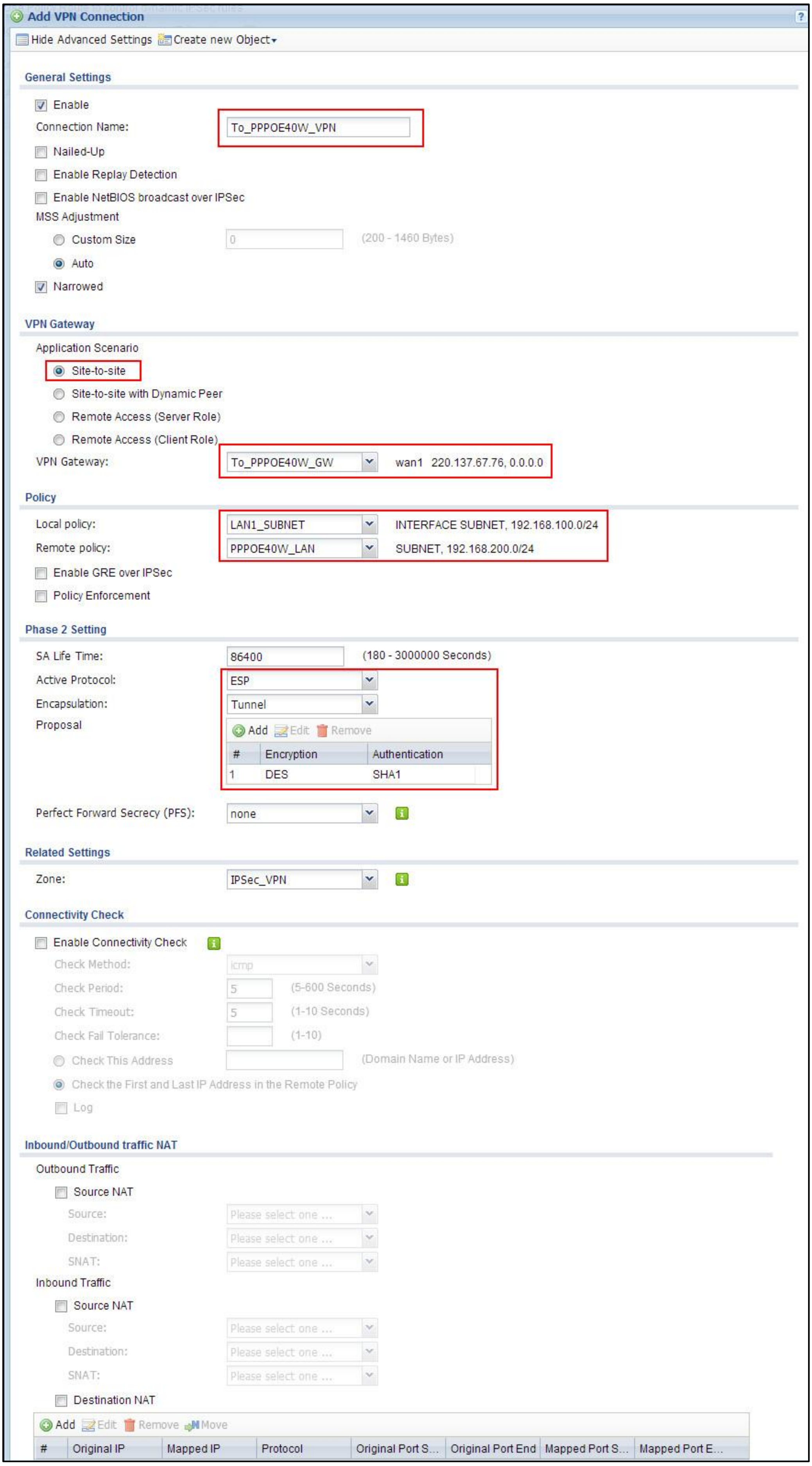
- VPN connection name
- VPN gateway selection

-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 (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 ...

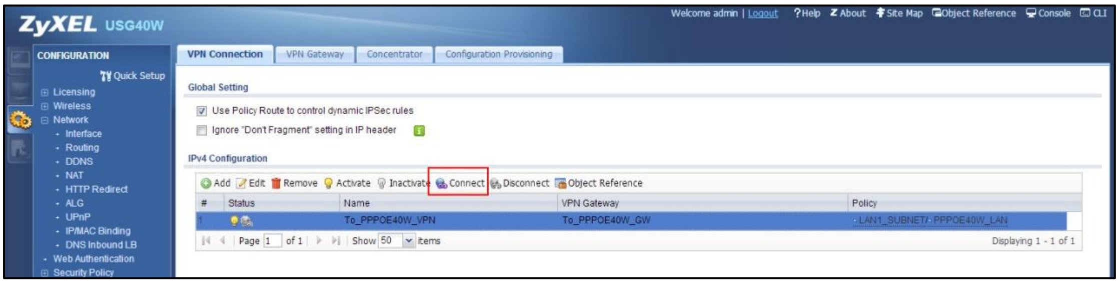
SNAT: Please select one ...

☐ Destination NAT

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.



Global Setting

☑ Use Policy Route to control dynamic IPSec rules

□ Ignore "Don't Fragment" setting in IP header

IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1		To_PPPOE40W_VPN	To_PPPOE40W_GW	LAN1_SUBNET/ PPPOE40W_LAN

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

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

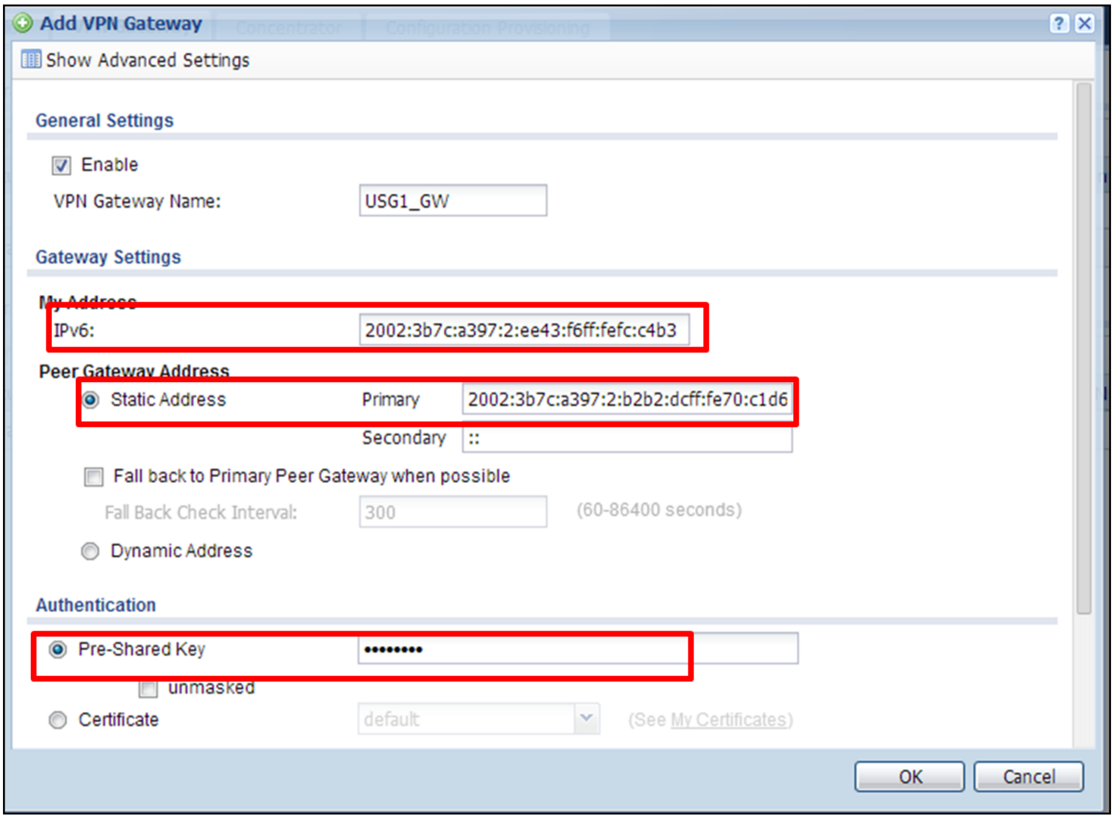
IPv6

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:fefc:c4b3

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

Pre-Shared Key: 12345678



General Settings

☑ Enable

VPN Gateway Name: USG1_GW

Gateway Settings

My Address

IPv6: 2002:3b7c:a397:2:ee43:f6ff:fefc:c4b3

Peer Gateway Address

● Static Address Primary 2002:3b7c:a397:2:b2b2:dcff:fe70:c1d6

Secondary ::

□ Fall back to Primary Peer Gateway when possible

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

○ Dynamic Address

Authentication

● Pre-Shared Key ••••••••

□ unmasked

○ Certificate default (See My Certificates)

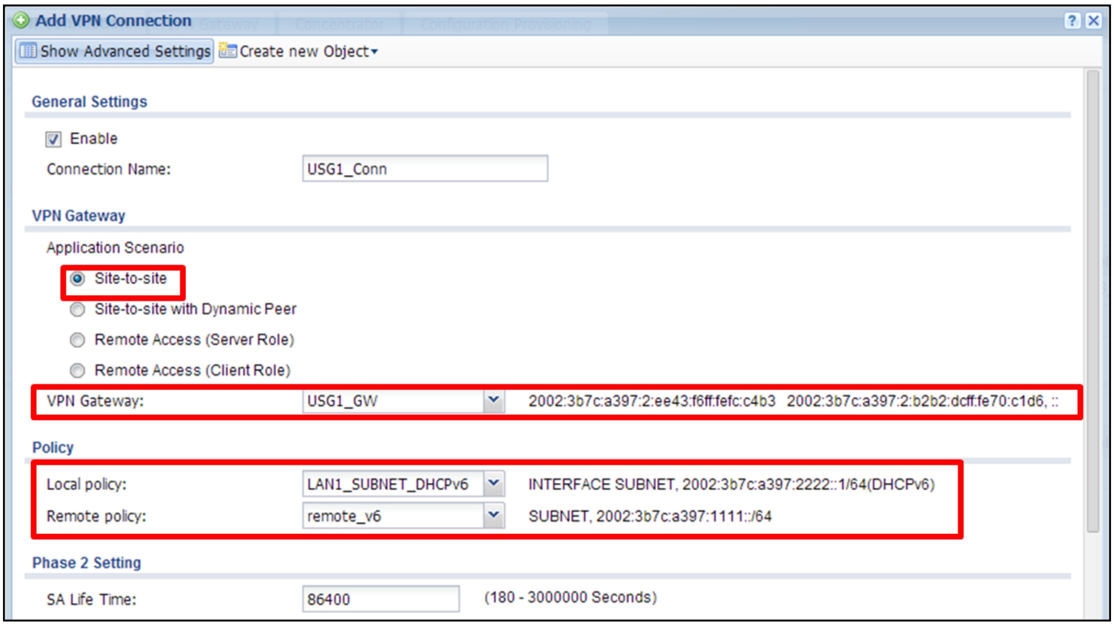
Step 2. Add an IPv6 VPN phase II on USG1. Go to **CONFIGURATION >**

VPN > IPSec VPN > VPN Connection.

VPN Gateway: USG1_GW

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

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



Add VPN Connection

Show Advanced Settings | Create new Object▾

General Settings

☑ Enable

Connection Name: USG1_Conn

VPN Gateway

Application Scenario

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

VPN Gateway: USG1_GW 2002:3b7c:a397:2:ee43:f6ff:fefc:c4b3 2002:3b7c:a397:2:b2b2:dcff:fe70:c1d6, ::

Policy

Local policy: LAN1_SUBNET_DHCPv6 INTERFACE SUBNET, 2002:3b7c:a397:2222::1/64(DHCPv6)

Remote policy: remote_v6 SUBNET, 2002:3b7c:a397:1111::/64

Phase 2 Setting

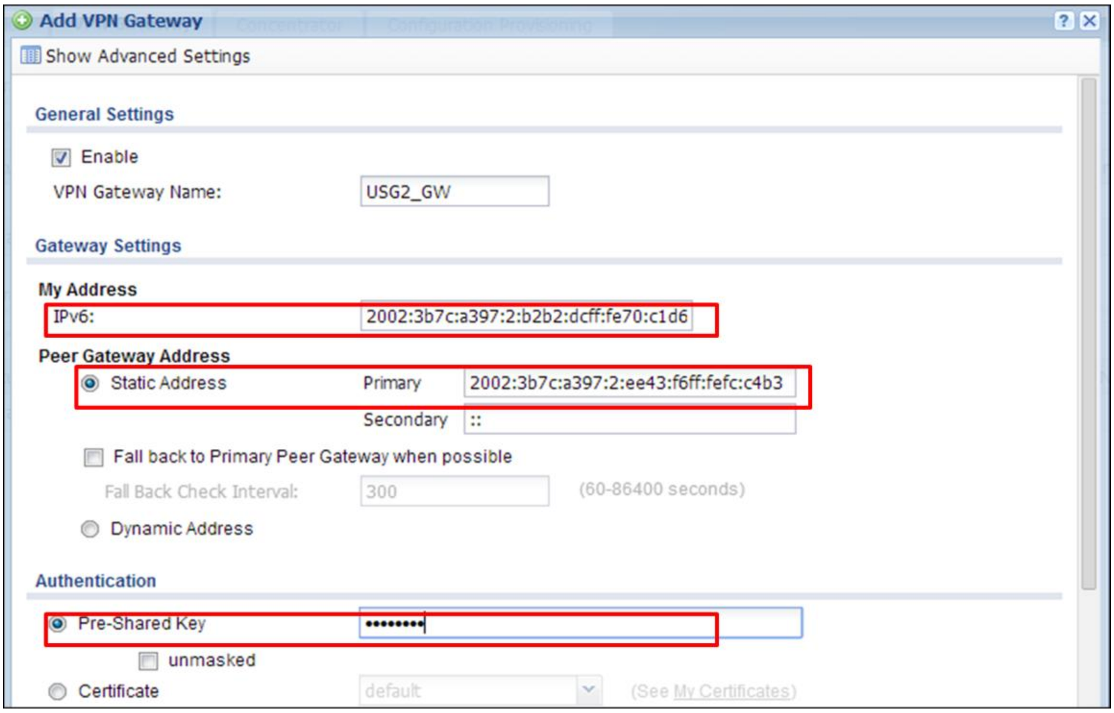
SA Life Time: 86400 (180 - 3000000 Seconds)

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



Add VPN Gateway

Show Advanced Settings

General Settings

☑ Enable

VPN Gateway Name: USG2_GW

Gateway Settings

My Address

IPv6: 2002:3b7c:a397:2:b2b2:dcff:fe70:c1d6

Peer Gateway Address

● Static Address Primary 2002:3b7c:a397:2:ee43:f6ff:fefc:c4b3

Secondary ::

□ Fall back to Primary Peer Gateway when possible

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

○ Dynamic Address

Authentication

● Pre-Shared Key ••••••••

□ unmasked

○ Certificate default (See My Certificates)

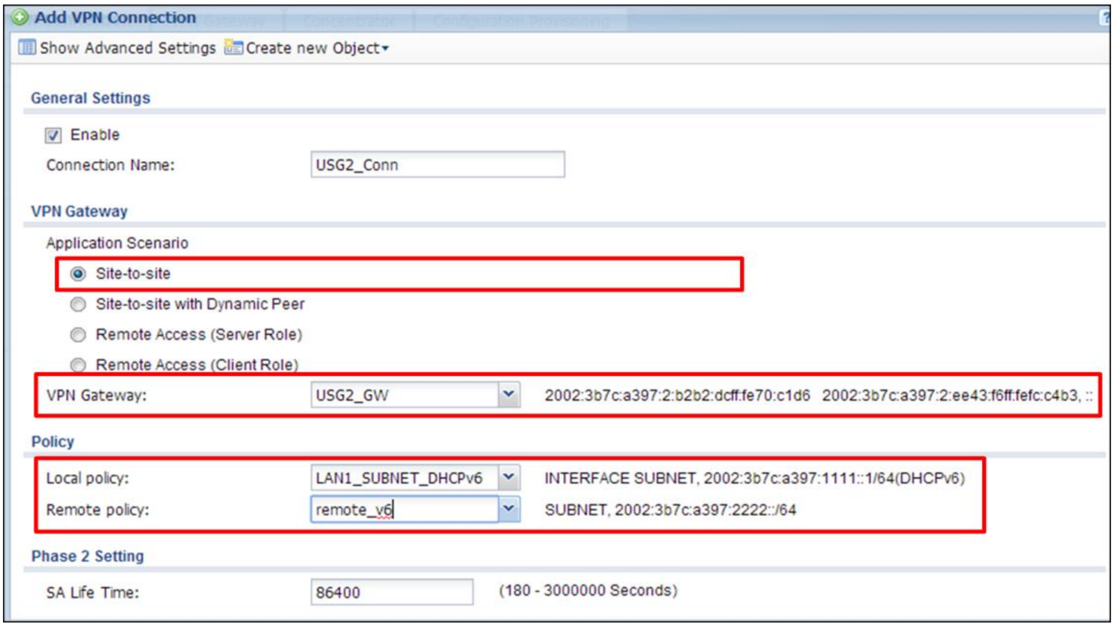
Step 4. Add an IPV6 VPN phase II on USG2. Go to **CONFIGURATION >**

VPN > IPSec VPN > VPN Connection.

VPN Gateway: USG2_GW

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

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



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

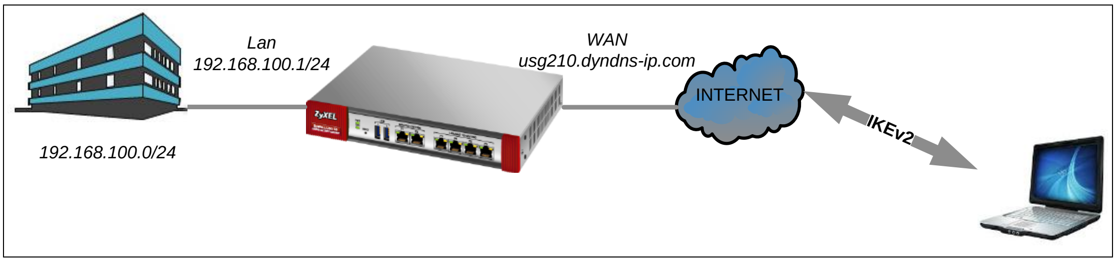
SA Life Time: 86400 (180 - 3000000 Seconds)

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

MONITOR > VPN MONITOR > IPSec.

Scenario 3 — Connect to USG using IPSec IKEv2 in Windows 7

3.1 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.

3.2 Configuration Guide

Network Conditions:

<u>USG 210:</u>

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

USG-210 VPN Conditions:

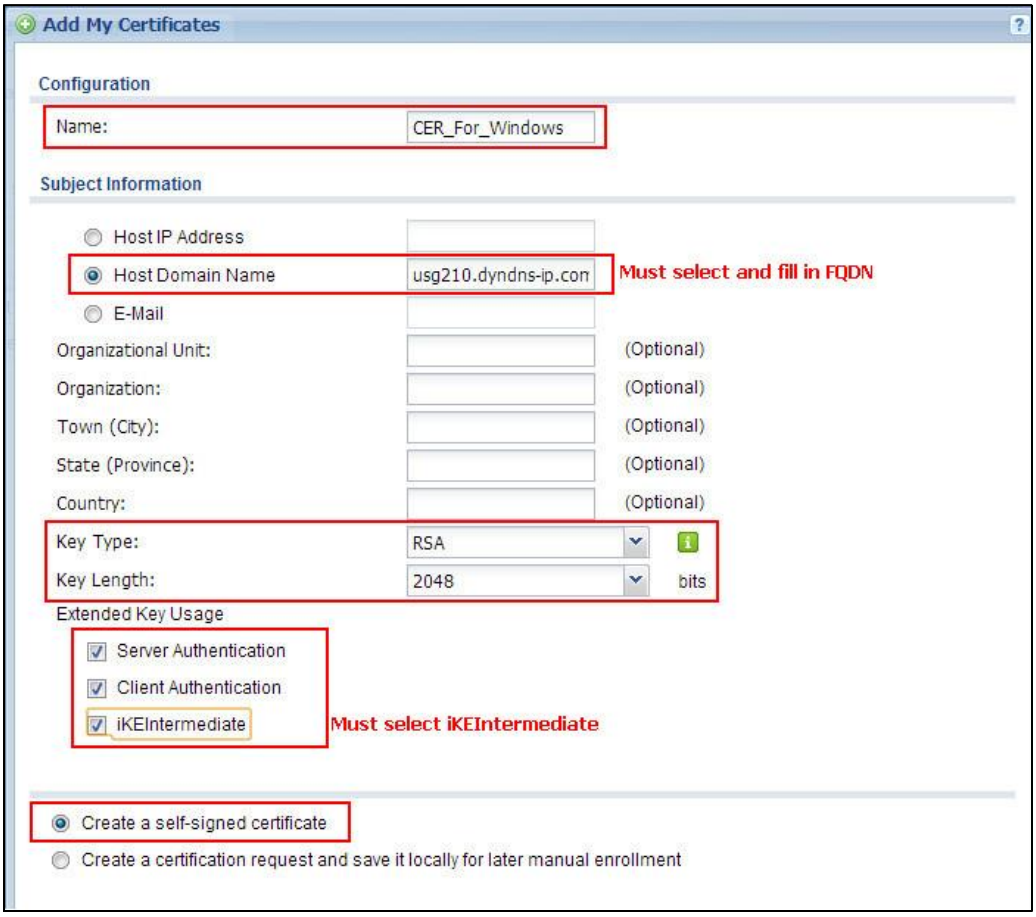
<u>Phase 1:</u>

- 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

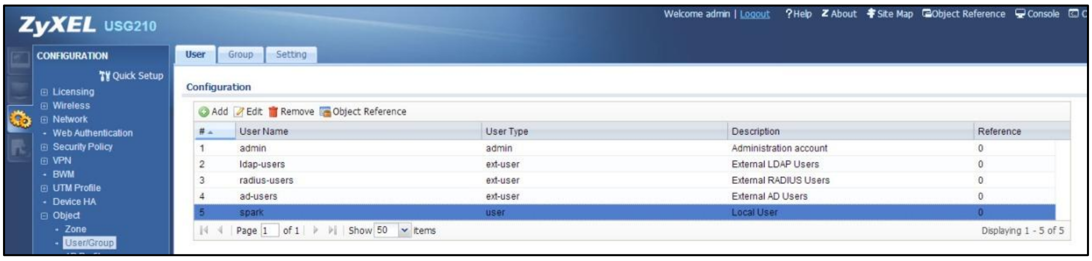
☑ iKEIntermediate

Must select iKEIntermediate

● Create a self-signed certificate

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

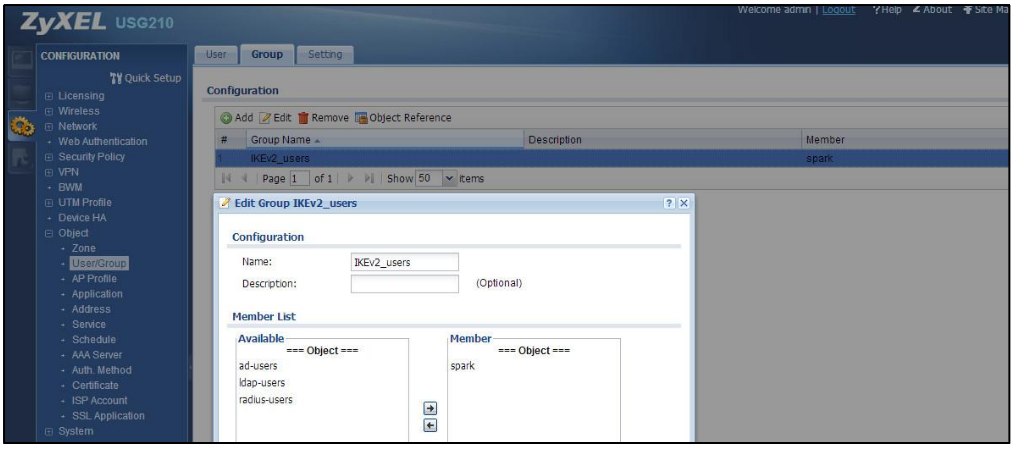
Step 2. Go to **CONFIGURATION > Object > User/Group** to create a user account. Add this account into IKEv2 users group object. This group object will be used in IPSec VPN phase-1 EAP (Extended Authentication Protocol) field.



Configuration

#	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

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



Configuration

#	Group Name	Description	Member
1	IKEv2_users		spark

Edit Group IKEv2_users

Configuration

Name: IKEv2_users

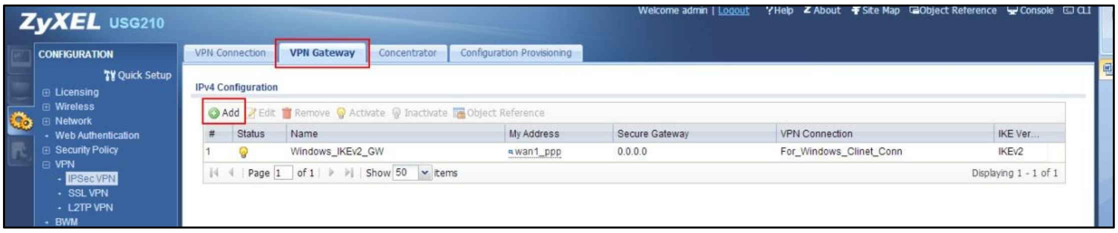
Description: (Optional)

Member List

Available	Member
=== Object ===	=== Object ===
ad-users	spark
ldap-users	
radius-users	

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.



IPv4 Configuration

#	Status	Name	My Address	Secure Gateway	VPN Connection	IKE Ver...
1		Windows_IKEv2_GW	wan1_ppp	0.0.0.0	For_Windows_Clinet_Conn	IKEv2

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

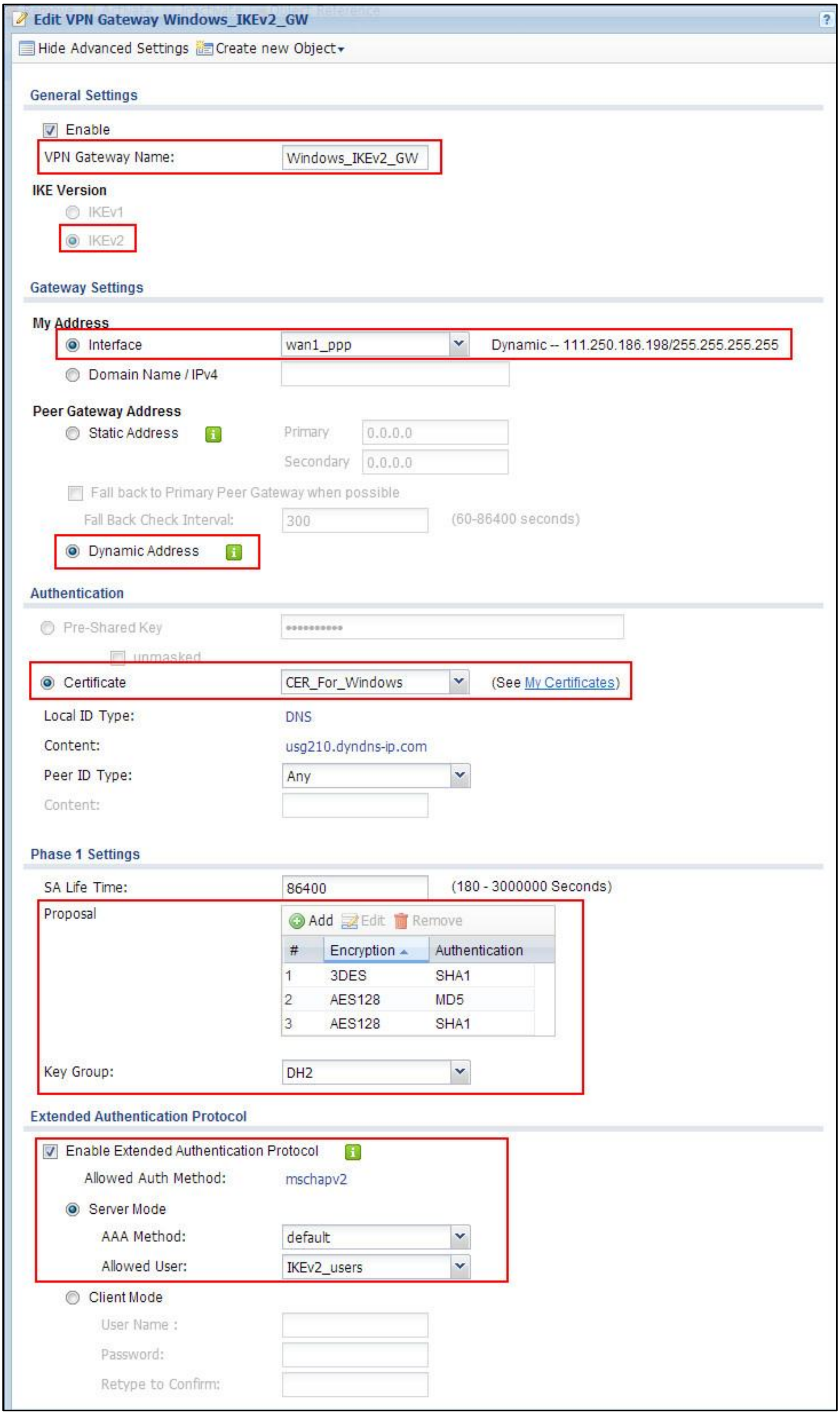
- Extended Authentication Protocol:

■ 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: ••••••••••

□ unmasked

● 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

#	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

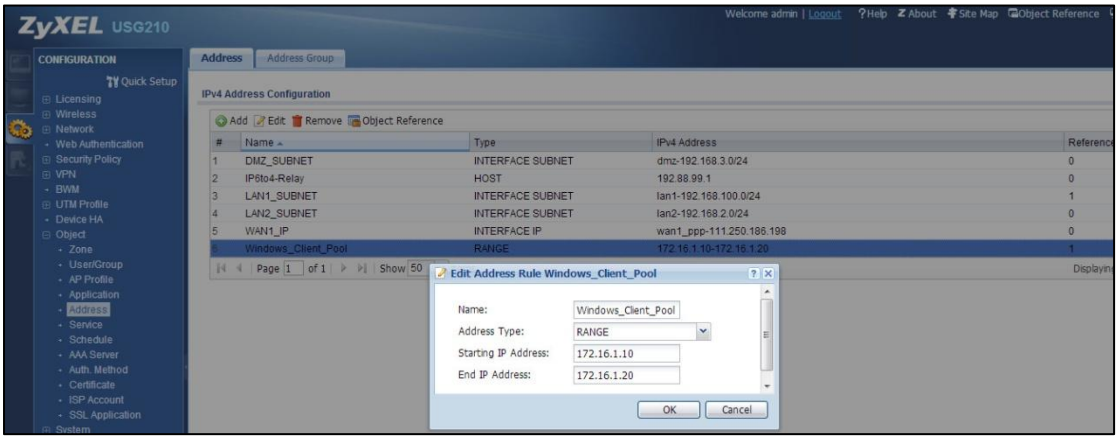
○ Client Mode

User Name :

Password:

Retype to Confirm:

Step 6. Go to **CONFIGURATION > Object > Address** to create an address object. This address object's IP address will be assigned to the Windows IKEv2 client's machine.



IPv4 Address Configuration

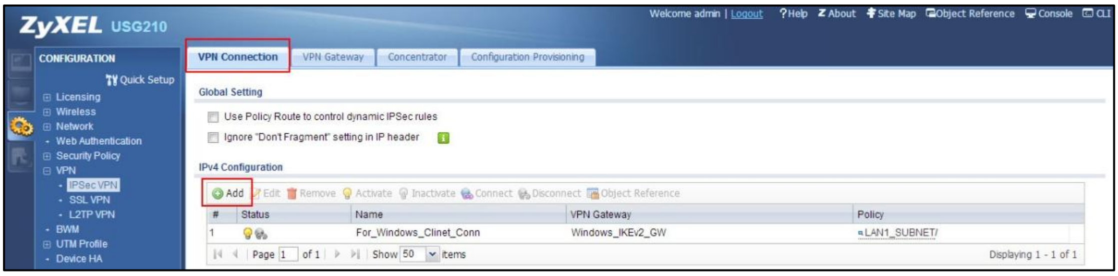
#	Name	Type	IPv4 Address	Reference
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24	0
2	IP6to4-Relay	HOST	192.88.99.1	0
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.100.0/24	1
4	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24	0
5	WAN1_IP	INTERFACE IP	wan1_ppp-111.250.186.198	0
6	Windows_Client_Pool	RANGE	172.16.1.10-172.16.1.20	1

Edit Address Rule Windows_Client_Pool

Name: Windows_Client_Pool
Address Type: RANGE
Starting IP Address: 172.16.1.10
End IP Address: 172.16.1.20

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.



Global Setting

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

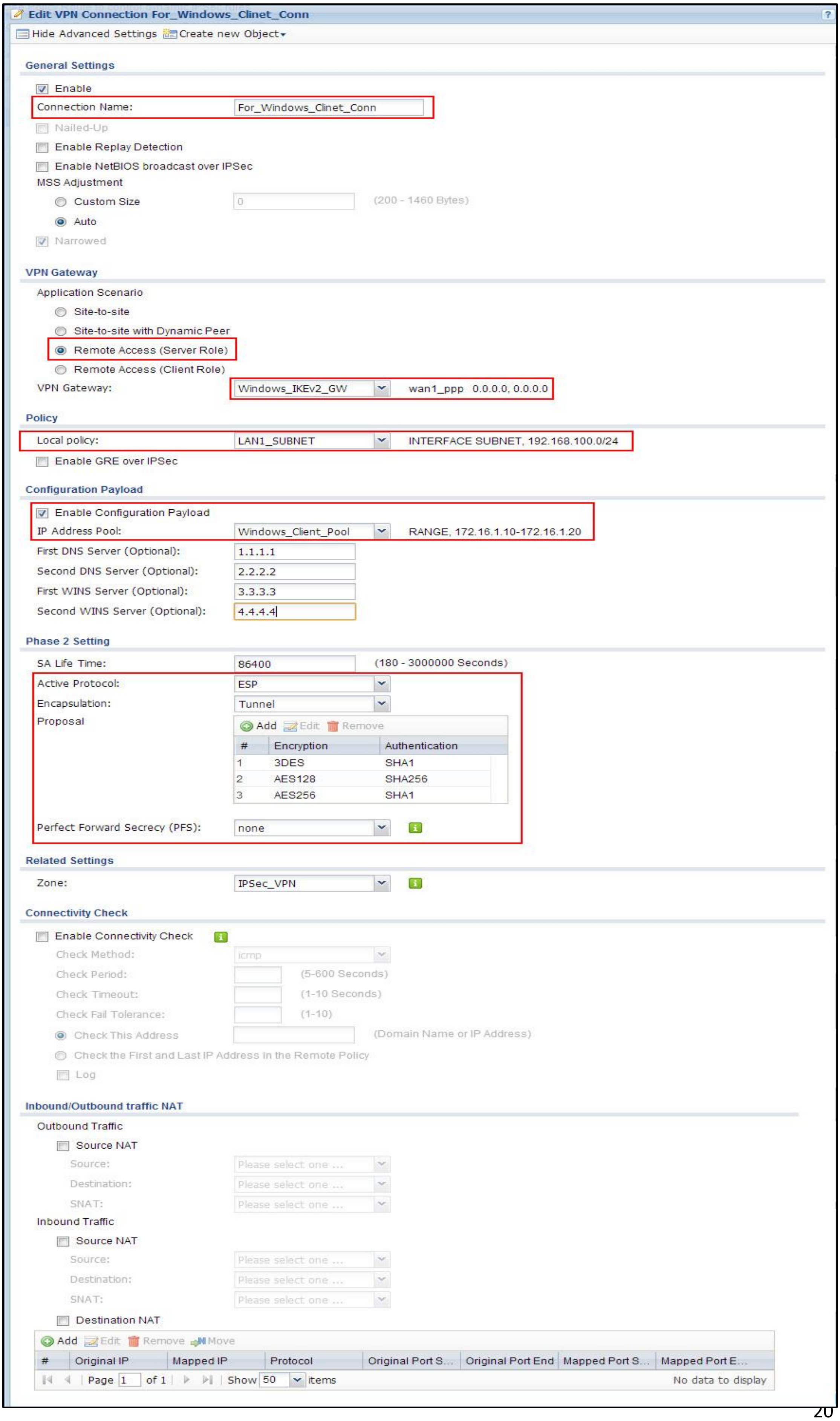
IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1		For_Windows_Clinet_Conn	Windows_IKEv2_GW	LAN1_SUBNET/

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

Add | Edit | Remove

#	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 ...

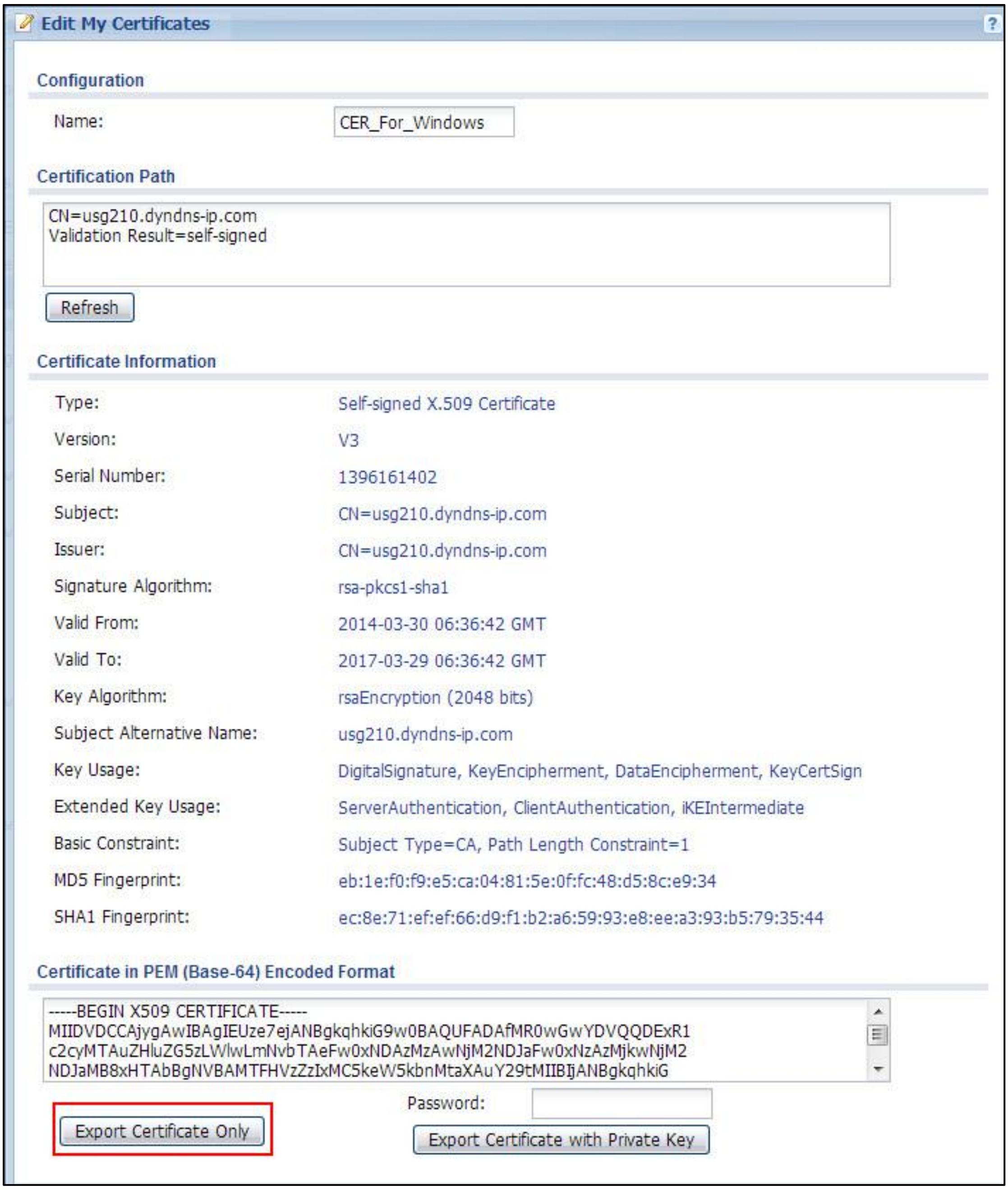
□ Destination NAT

Add | Edit | Remove | Move

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

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

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



Configuration

Name: CER_For_Windows

Certification Path

CN=usg210.dyndns-ip.com
Validation Result=self-signed

Certificate Information

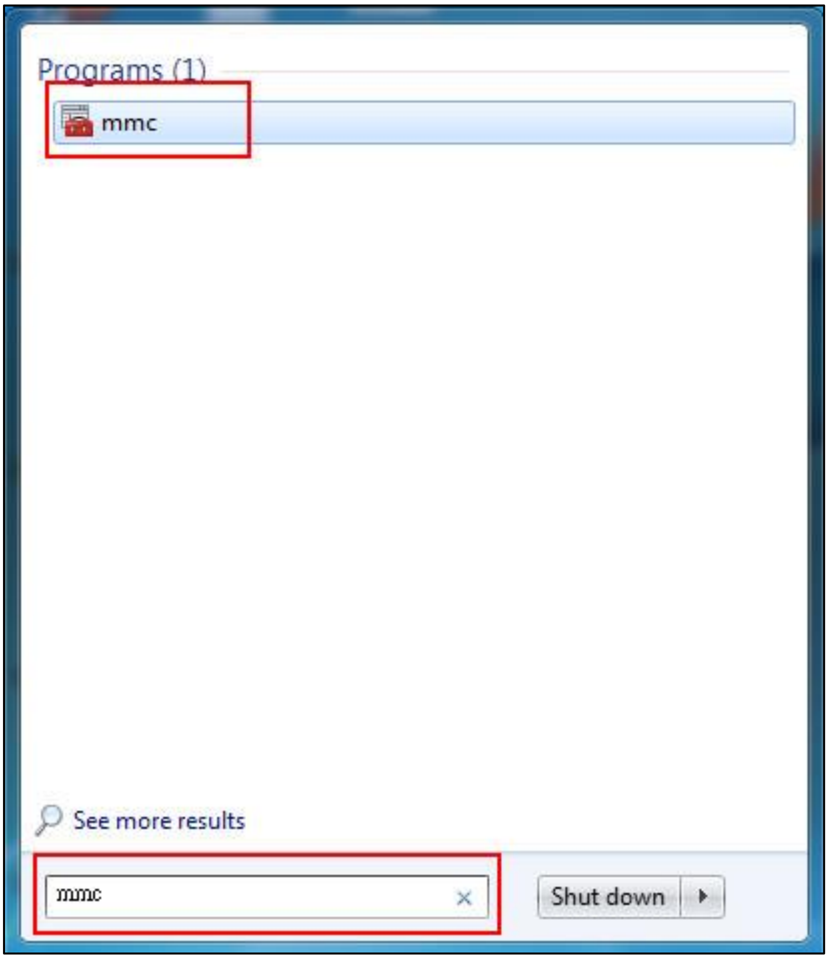
Type:	Self-signed X.509 Certificate
Version:	V3
Serial Number:	1396161402
Subject:	CN=usg210.dyndns-ip.com
Issuer:	CN=usg210.dyndns-ip.com
Signature Algorithm:	rsa-pkcs1-sha1
Valid From:	2014-03-30 06:36:42 GMT
Valid To:	2017-03-29 06:36:42 GMT
Key Algorithm:	rsaEncryption (2048 bits)
Subject Alternative 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

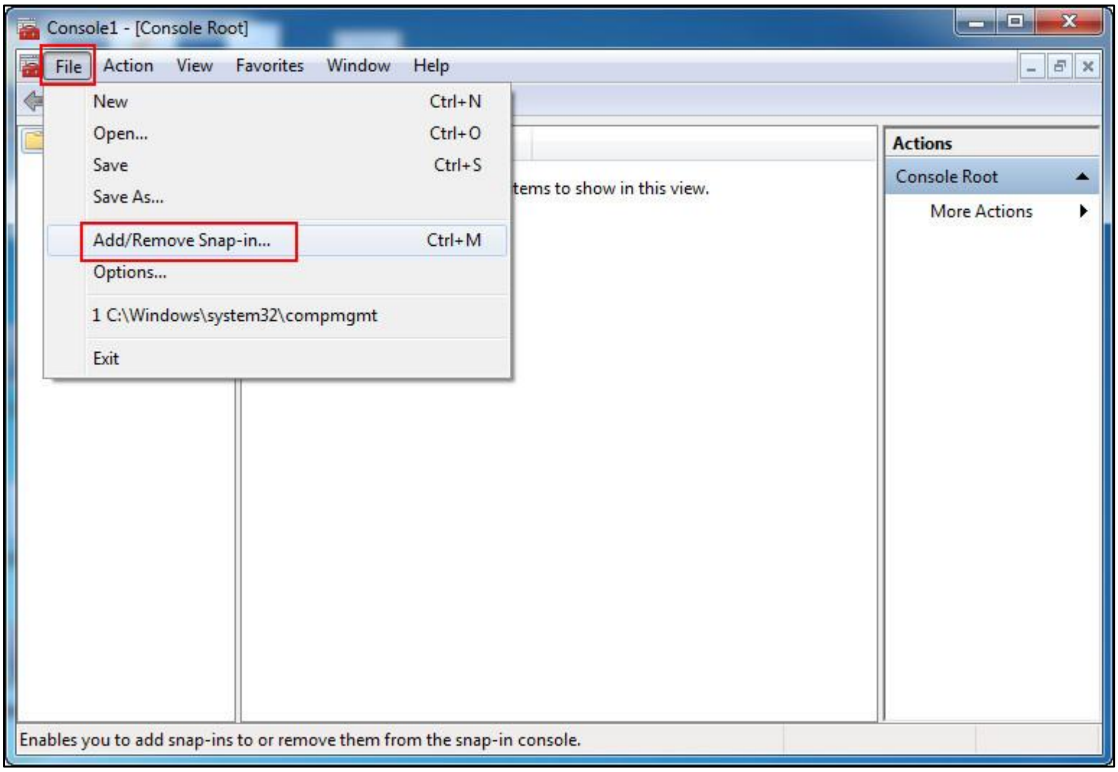
```
-----BEGIN X509 CERTIFICATE-----
MIIDVDCCAjygAwIBAgIEUze7ejANBgkqhkiG9w0BAQUFADAfMR0wGwYDVQQDExR1
c2cyMTAuZHluZG5zLWlwLmNvbTAeFw0xNDAzMzAwNjM2NDJaFw0xNzAzMjkwNjM2
NDJaMB8xHTAbBgNVBAMTFHVzZzIxMC5keW5kbnMtaXAuY29tMIIBIjANBgkqhkiG
```

Password:

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

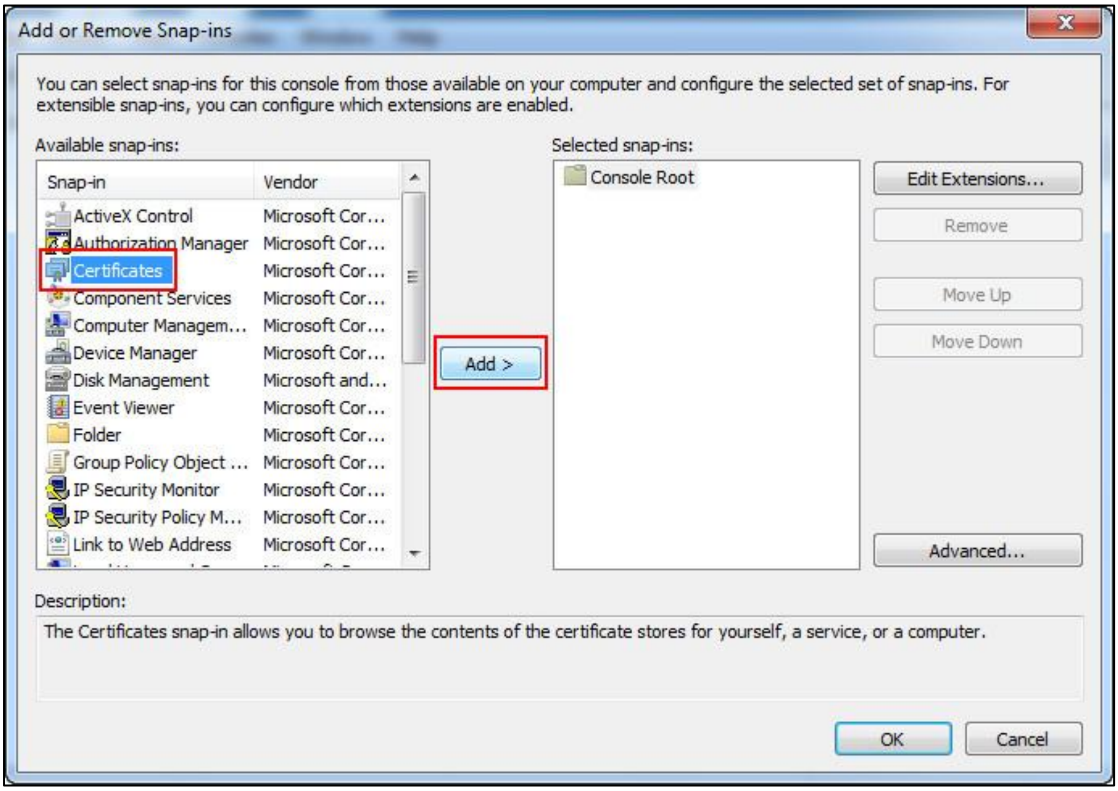


Step 12. In the mmc console, click on **File > Add/Remove Snap-in... >**



Enables you to add snap-ins to or remove them from the snap-in console.

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



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

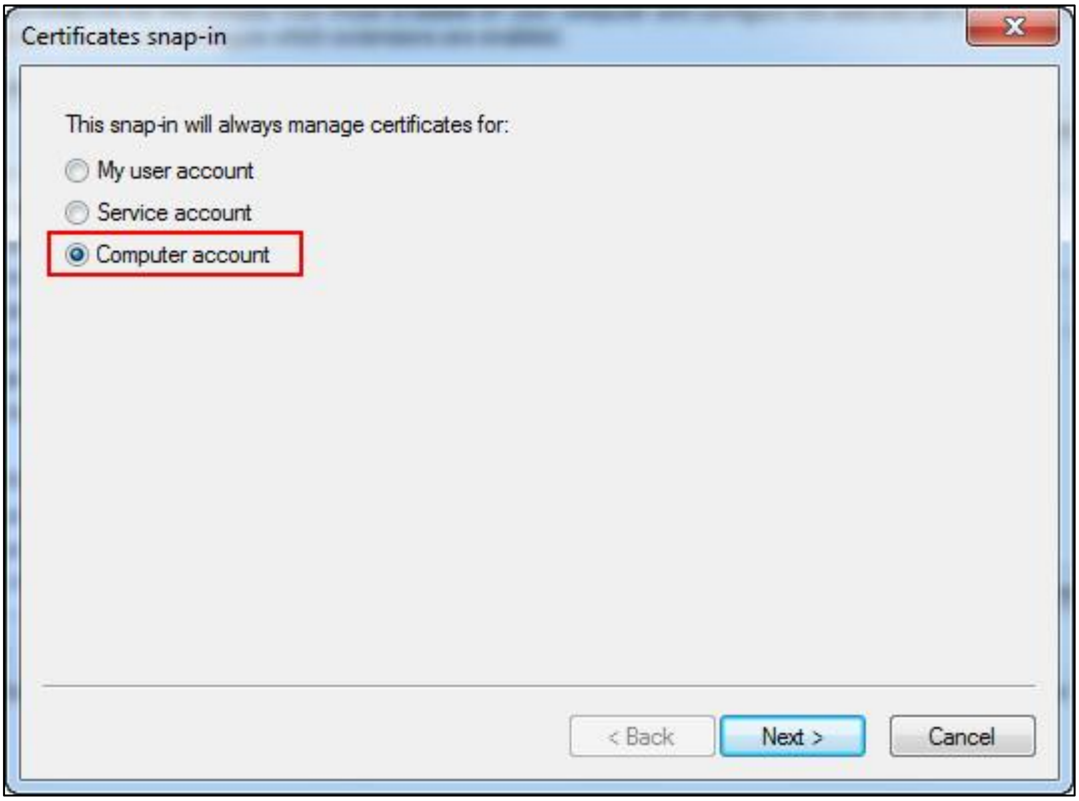
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

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



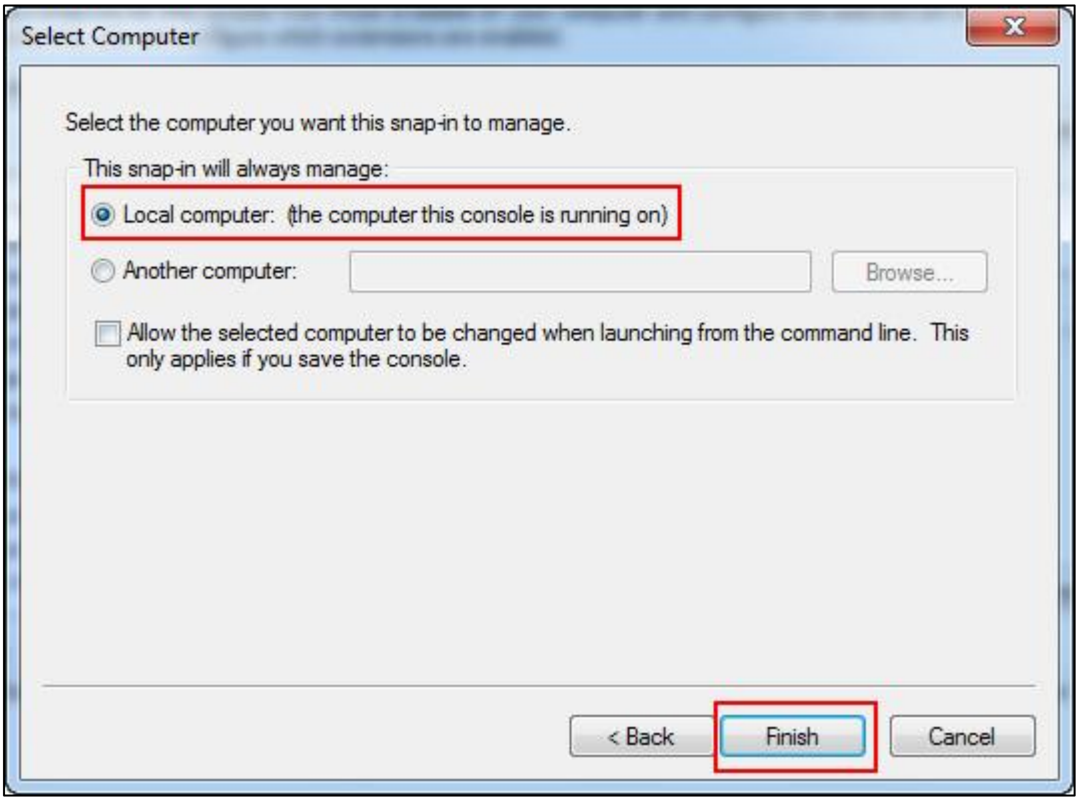
Certificates snap-in

This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account



Select Computer

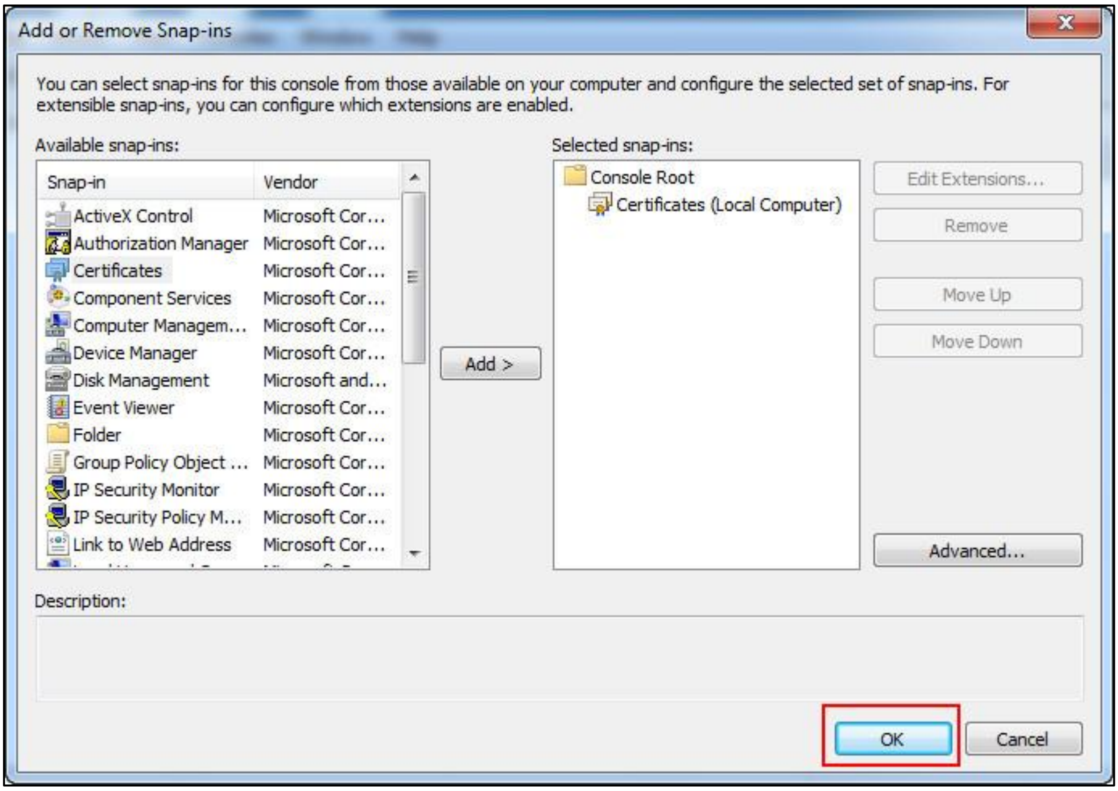
Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

○ Another computer:

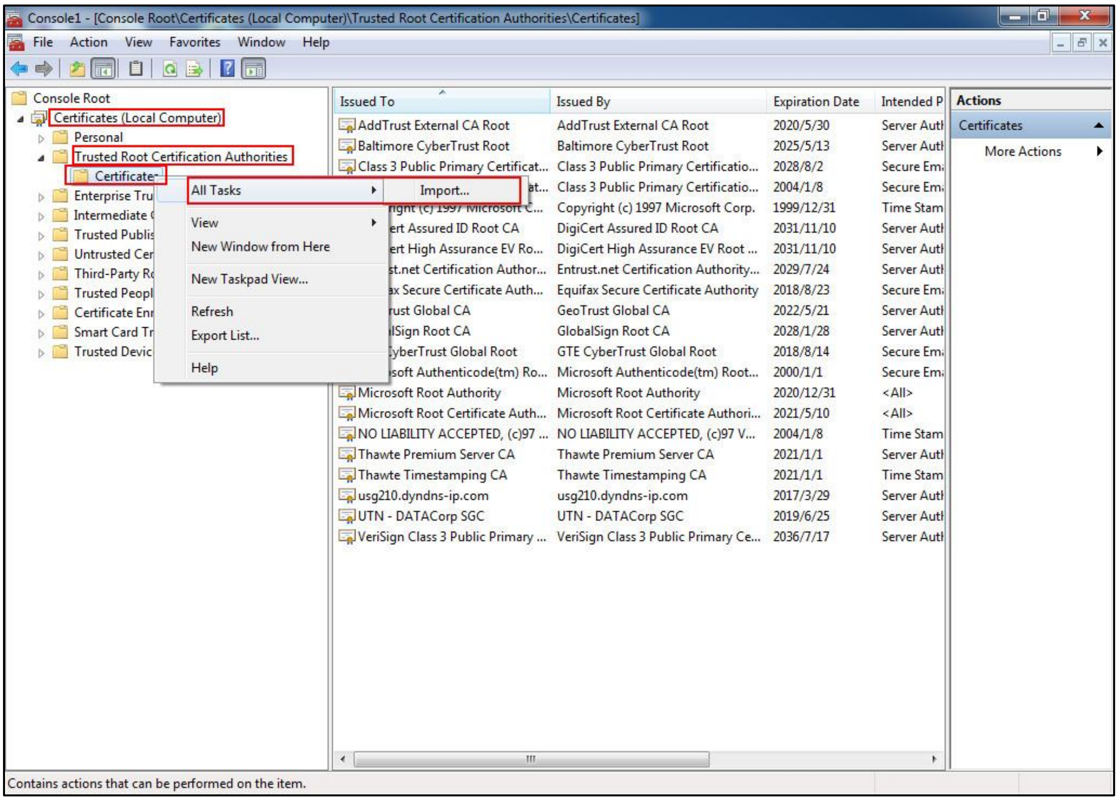
□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.



You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

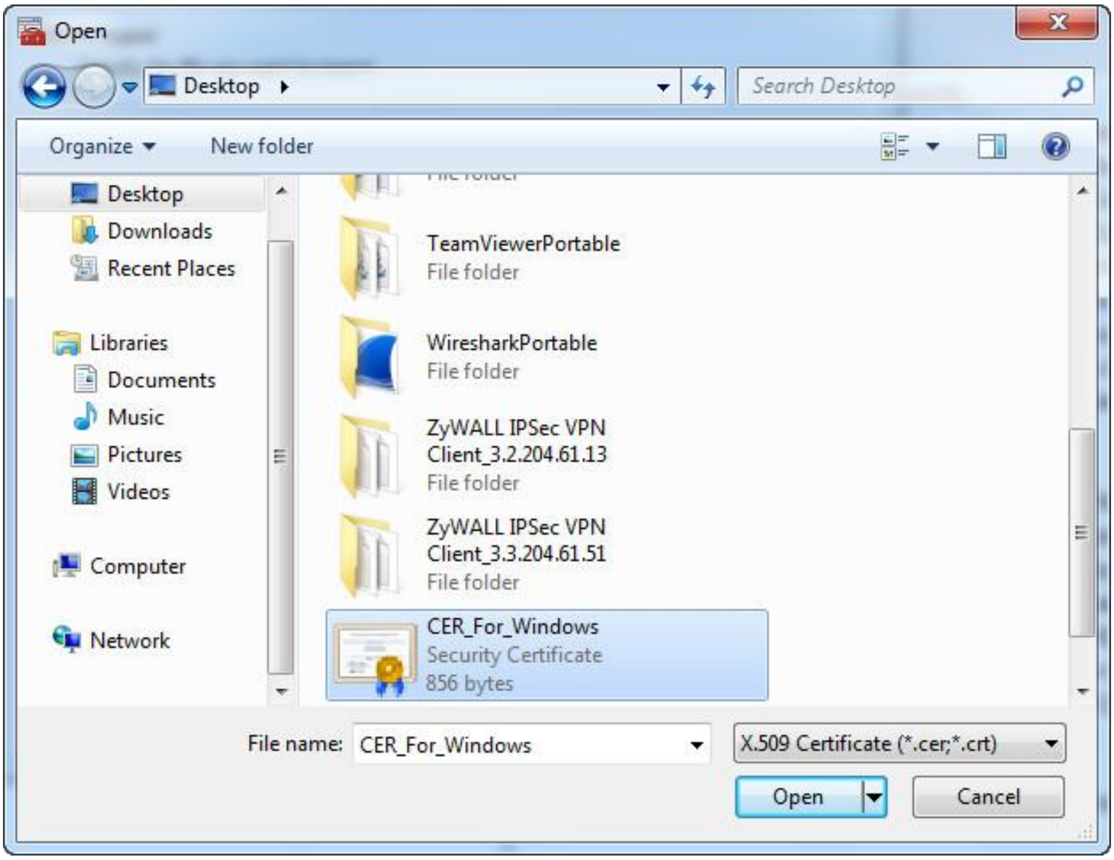
Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy M...	Microsoft Cor...
Link to Web Address	Microsoft Cor...

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



Issued To	Issued By	Expiration Date	Intended P
AddTrust External CA Root	AddTrust External CA Root	2020/5/30	Server Auth
Baltimore CyberTrust Root	Baltimore CyberTrust Root	2025/5/13	Server Auth
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	2028/8/2	Secure Ema
at...	Class 3 Public Primary Certificatio...	2004/1/8	Secure Ema
...right (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	1999/12/31	Time Stam
ert Assured ID Root CA	DigiCert Assured ID Root CA	2031/11/10	Server Auth
ert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	2031/11/10	Server Auth
st.net Certification Author...	Entrust.net Certification Authority...	2029/7/24	Server Auth
ax Secure Certificate Auth...	Equifax Secure Certificate Authority	2018/8/23	Secure Ema
rust Global CA	GeoTrust Global CA	2022/5/21	Server Auth
lSign Root CA	GlobalSign Root CA	2028/1/28	Server Auth
yberTrust Global Root	GTE CyberTrust Global Root	2018/8/14	Secure Ema
soft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	2000/1/1	Secure Ema
Microsoft Root Authority	Microsoft Root Authority	2020/12/31	<All>
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	2021/5/10	<All>
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	2004/1/8	Time Stam
Thawte Premium Server CA	Thawte Premium Server CA	2021/1/1	Server Auth
Thawte Timestamping CA	Thawte Timestamping CA	2021/1/1	Time Stam
usg210.dyndns-ip.com	usg210.dyndns-ip.com	2017/3/29	Server Auth
UTN - DATACorp SGC	UTN - DATACorp SGC	2019/6/25	Server Auth
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	2036/7/17	Server Auth

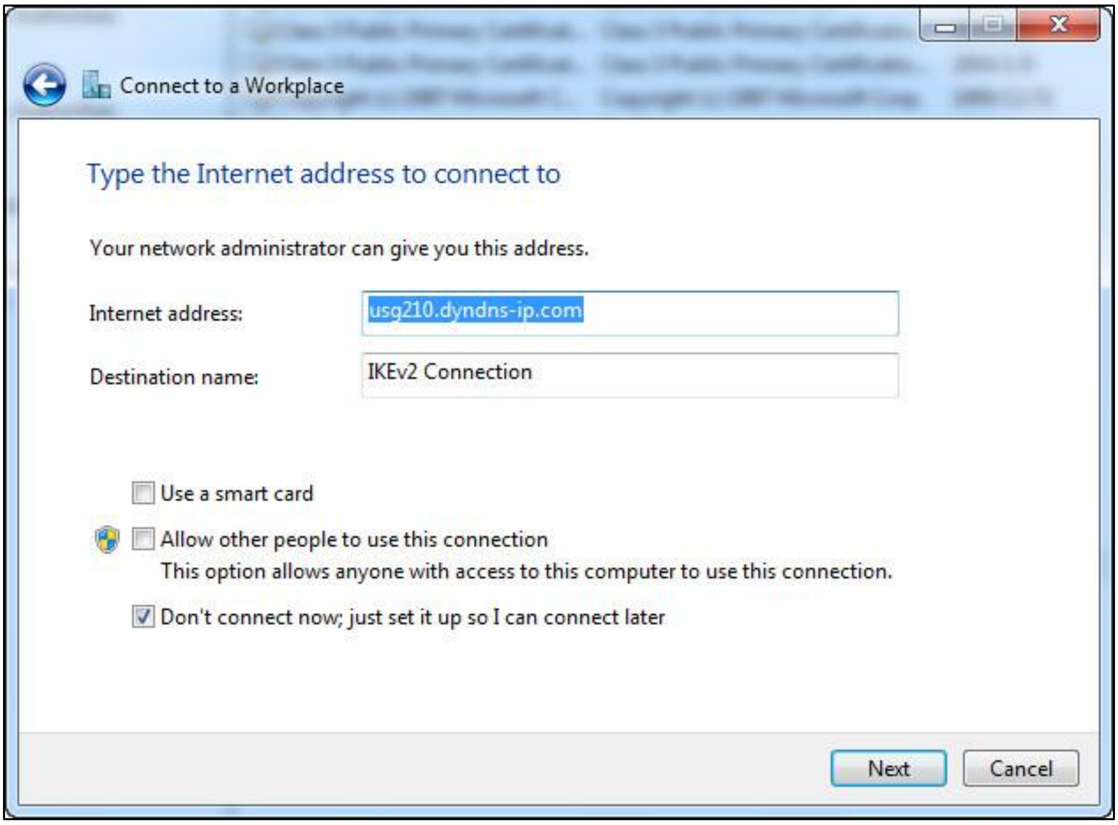
Step 16. Select the certificate, which was generated by the USG.



File name: CER_For_Windows

X.509 Certificate (*.cer;*.crt)

Step 17. Create the Windows IPSec connection profile.



Type the Internet address to connect to

Your network administrator can give you this address.

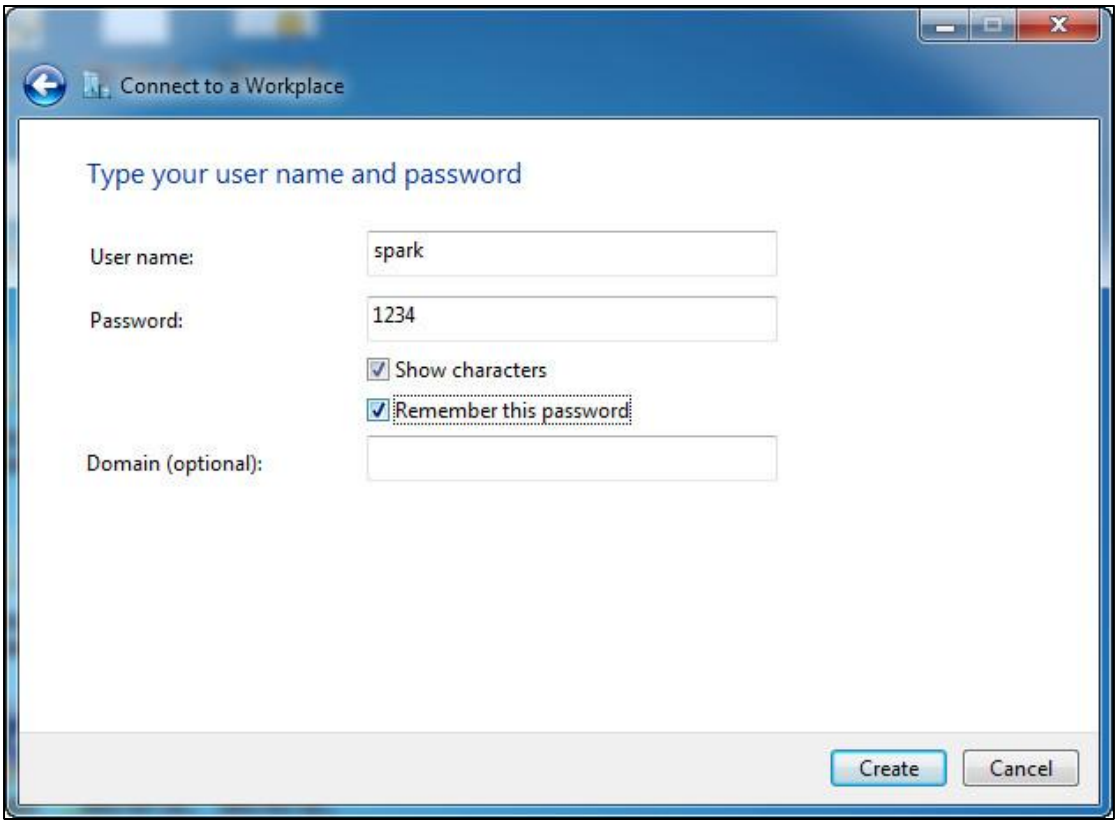
Internet address: usg210.dyndns-ip.com

Destination name: IKEv2 Connection

□ 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



Connect to a Workplace

Type your user name and password

User name: spark

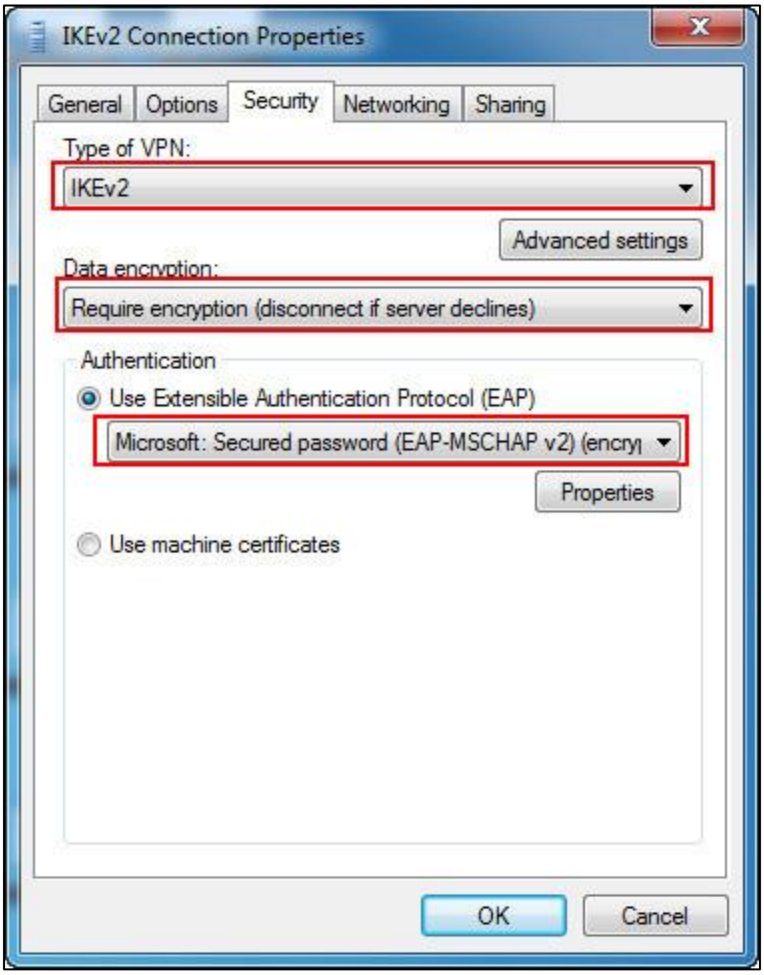
Password: 1234

☑ Show characters

☑ Remember this password

Domain (optional):

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)



IKEv2 Connection Properties

Type of VPN: IKEv2

Data encryption: Require encryption (disconnect if server declines)

Authentication

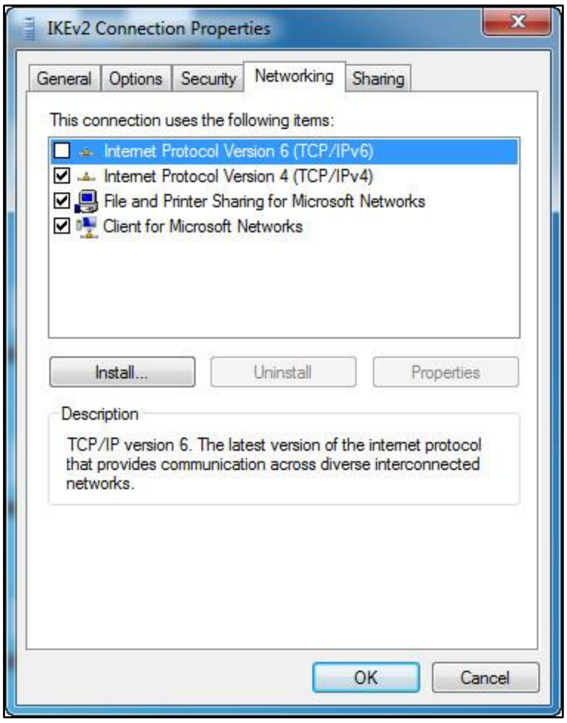
● Use Extensible Authentication Protocol (EAP)

Microsoft: Secured password (EAP-MSCHAP v2) (encry

○ Use machine certificates

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.



IKEv2 Connection Properties

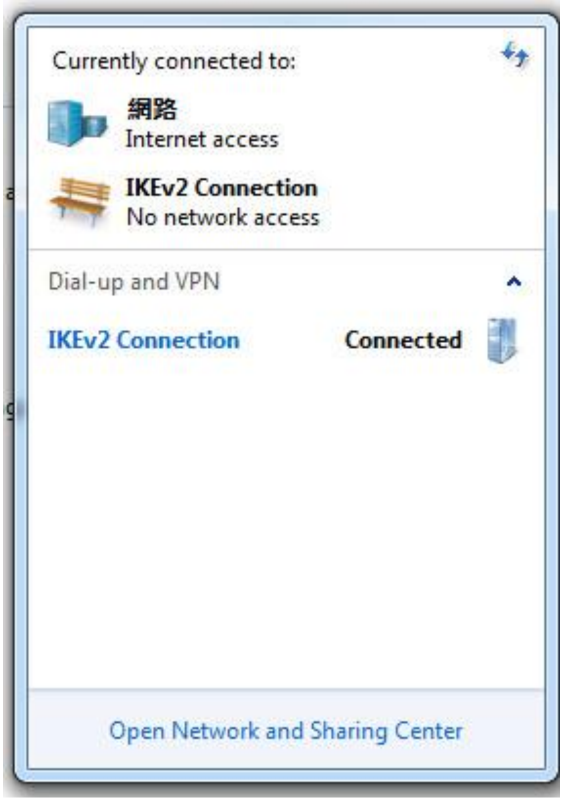
This connection uses the following items:

- □ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Client for Microsoft Networks

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

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



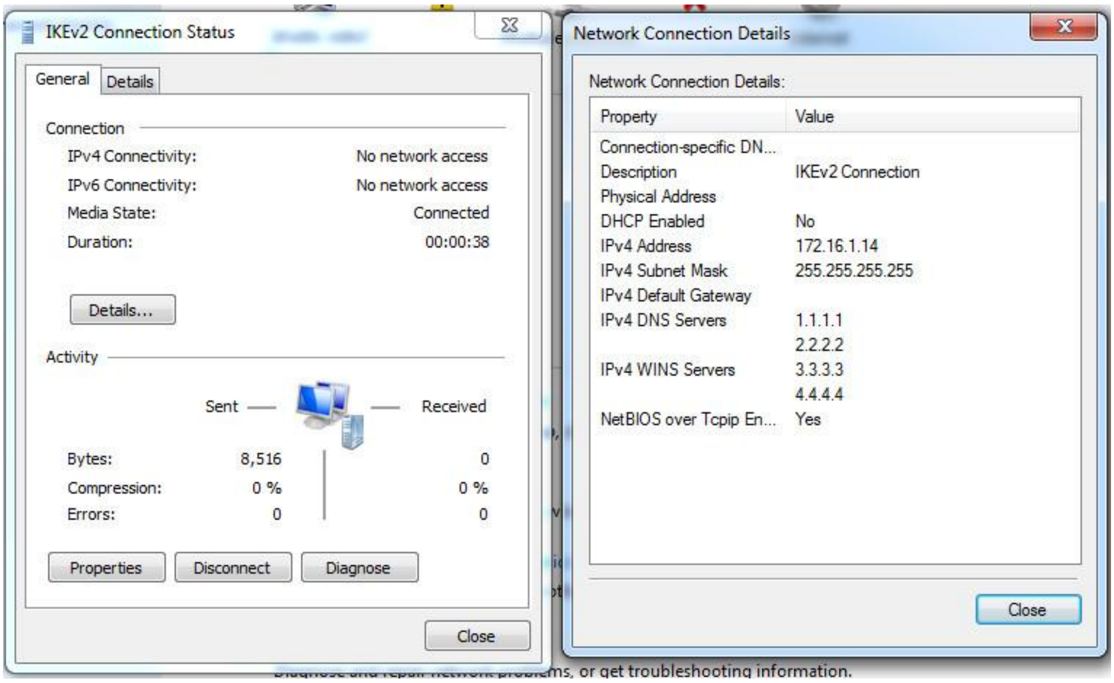
Currently connected to:

網路
Internet access

IKEv2 Connection
No network access

Dial-up and VPN

IKEv2 Connection Connected



Connection

IPv4 Connectivity:	No network access
IPv6 Connectivity:	No network access
Media State:	Connected
Duration:	00:00:38

Activity

	Sent	Received
Bytes:	8,516	0
Compression:	0 %	0 %
Errors:	0	0

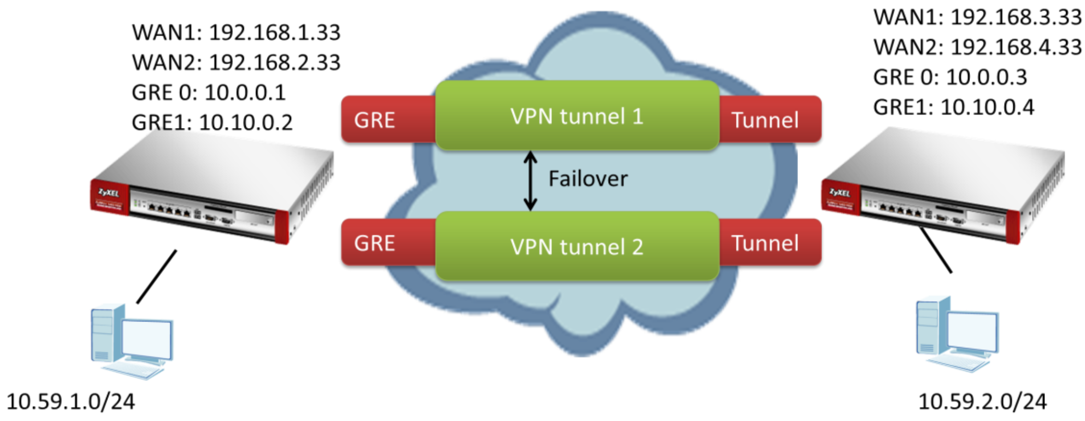
Network Connection Details:

Property	Value
Connection-specific DN...	
Description	IKEv2 Connection
Physical Address	
DHCP Enabled	No
IPv4 Address	172.16.1.14
IPv4 Subnet Mask	255.255.255.255
IPv4 Default Gateway	
IPv4 DNS Servers	1.1.1.1 2.2.2.2
IPv4 WINS Servers	3.3.3.3 4.4.4.4
NetBIOS over Tcpip En...	Yes

Scenario 4 — GRE over IPSec VPN Tunnel –VPN Failover

4.1 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.



4.2 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.

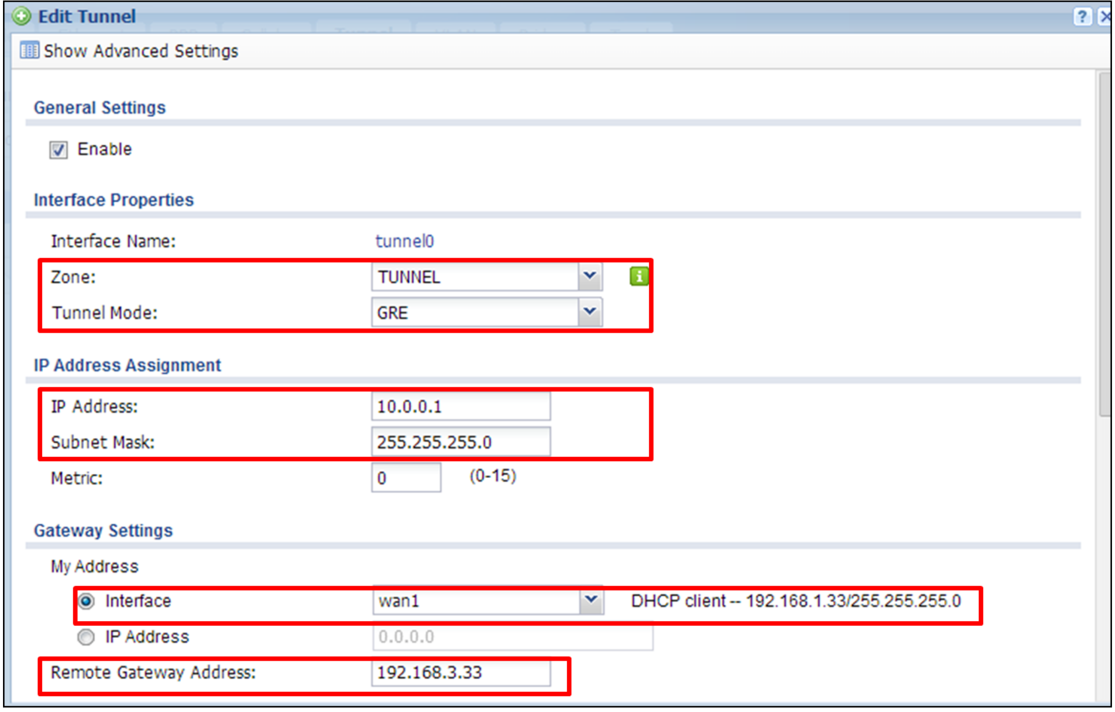
USG configuration

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



Edit Tunnel

Show Advanced 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

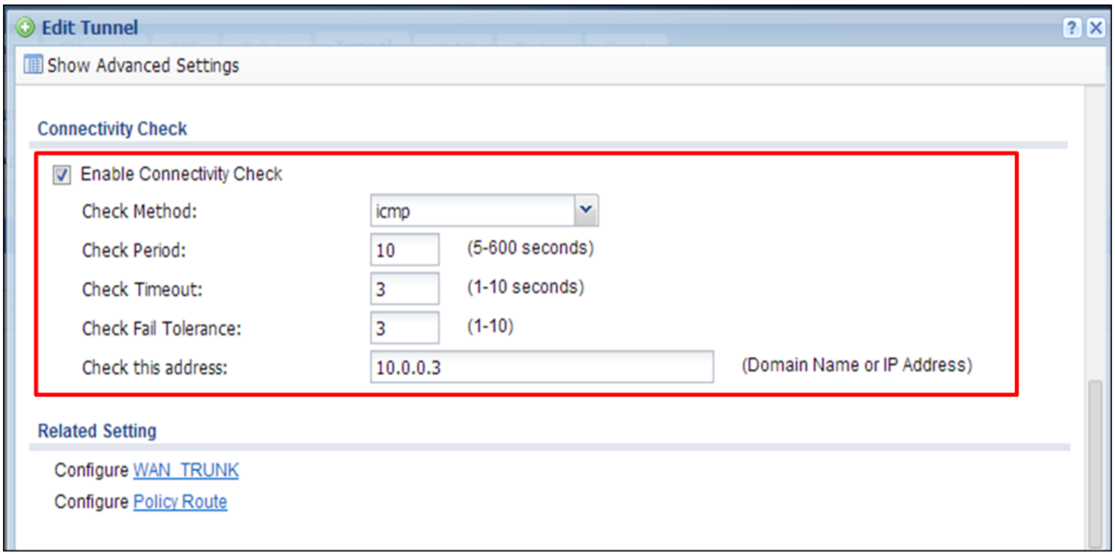
My Address

● 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.



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: 10.0.0.3 (Domain Name or IP Address)

Related Setting

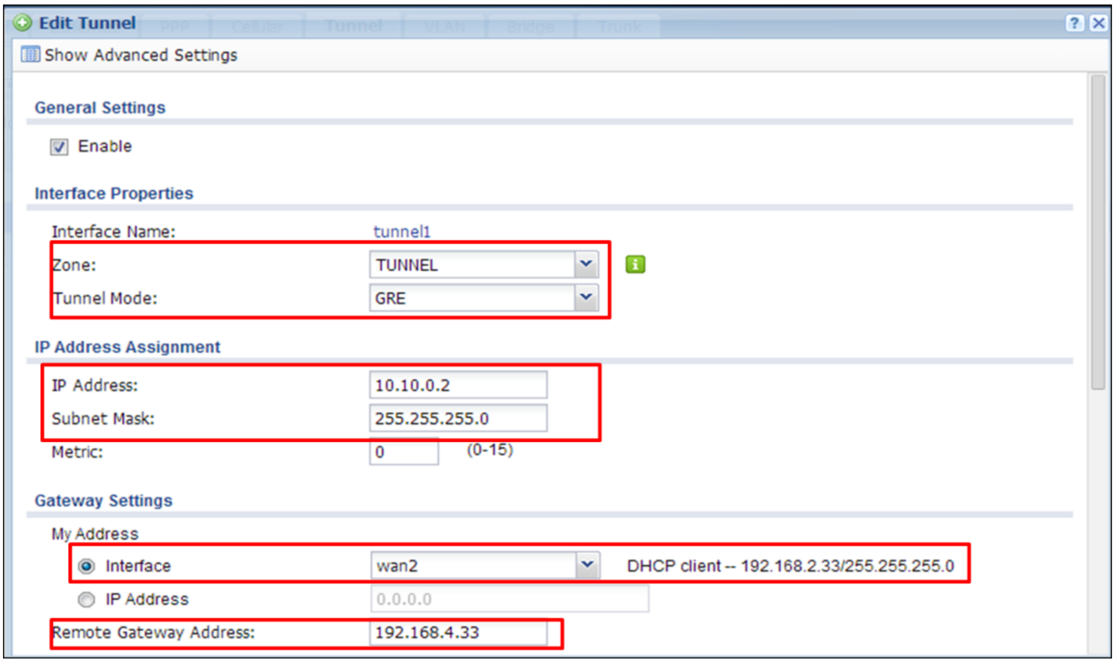
Configure WAN_TRUNK

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

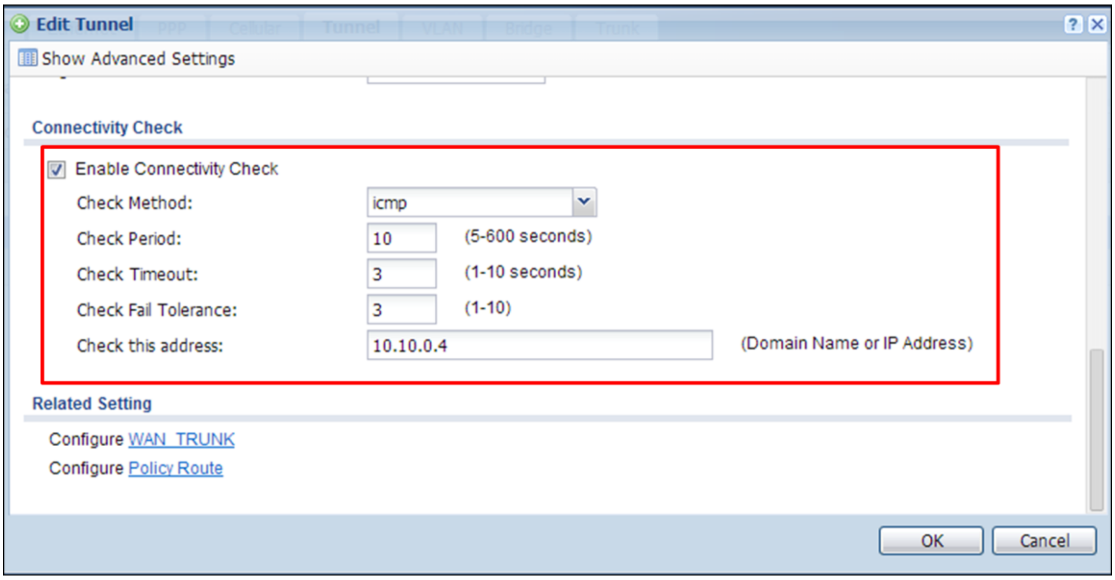
My Address

● 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)

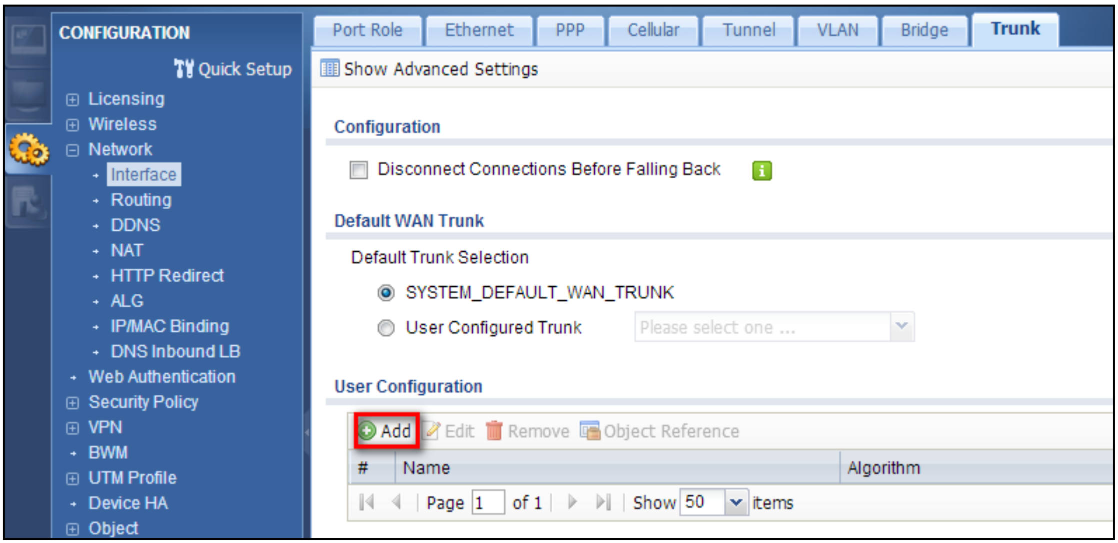
Related Setting

Configure WAN_TRUNK

Configure Policy Route

Step 2. Add a GRE tunnel trunk on USG1. Go to **CONFIGURATION > Network > Interface > Trunk.**

gre_trunk member:
tunnel0: Active
tunnel1: Passive



Configuration

□ Disconnect Connections Before Falling Back

Default WAN Trunk

Default Trunk Selection

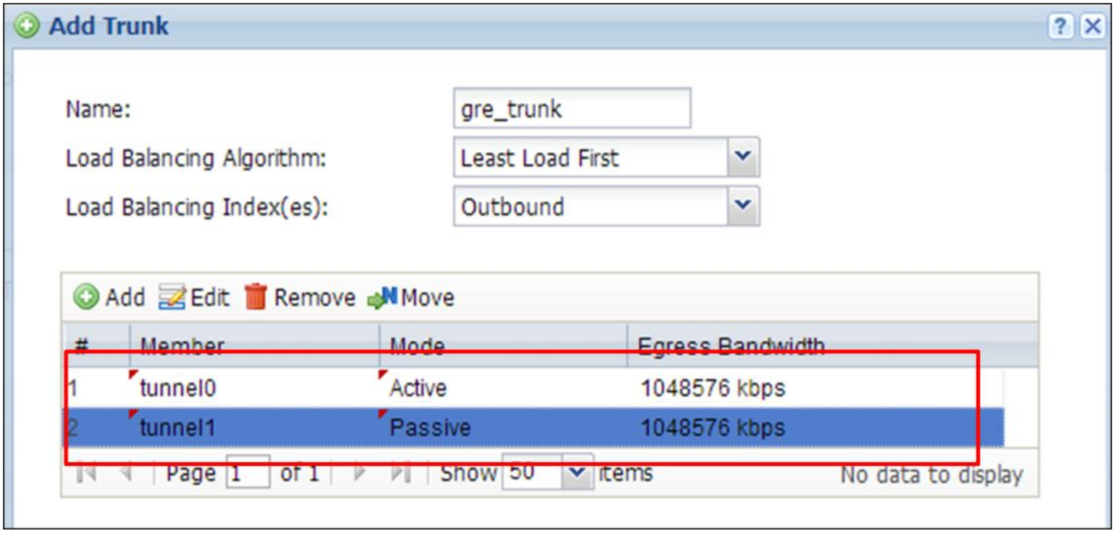
● SYSTEM_DEFAULT_WAN_TRUNK

○ User Configured Trunk Please select one ...

User Configuration

#	Name	Algorithm

Page 1 of 1 | Show 50 items



Name: gre_trunk

Load Balancing Algorithm: Least Load First

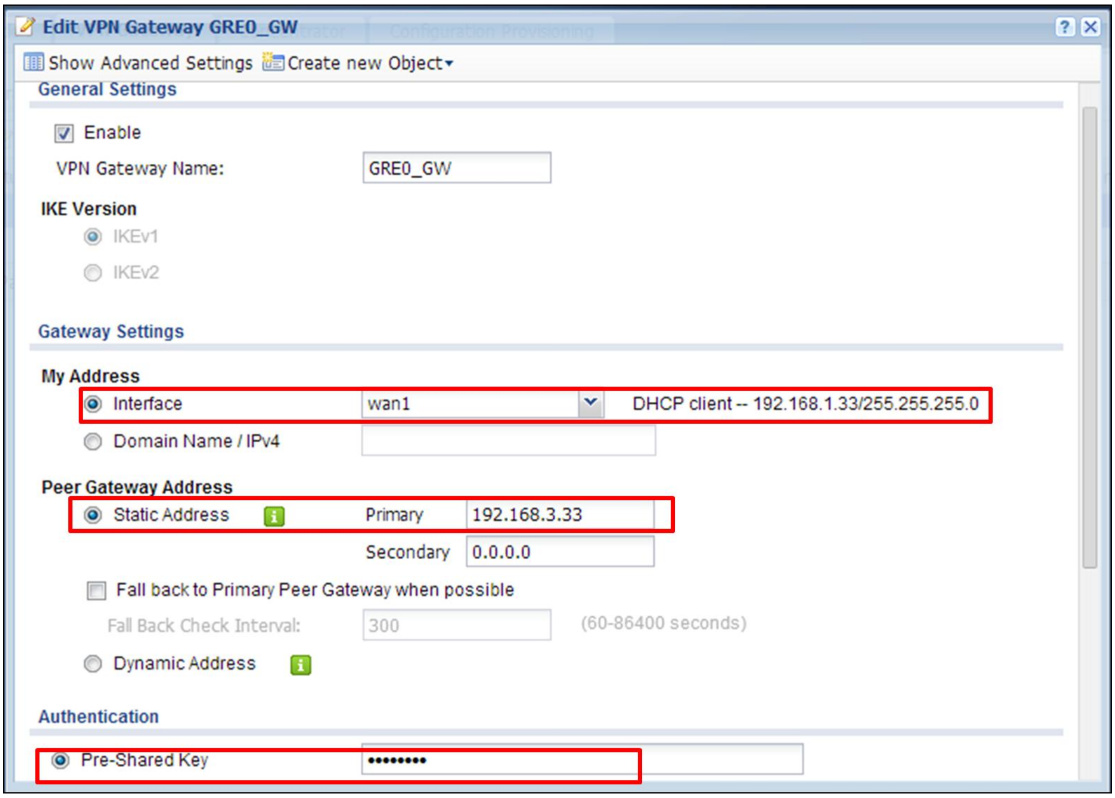
Load Balancing Index(es): Outbound

#	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

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

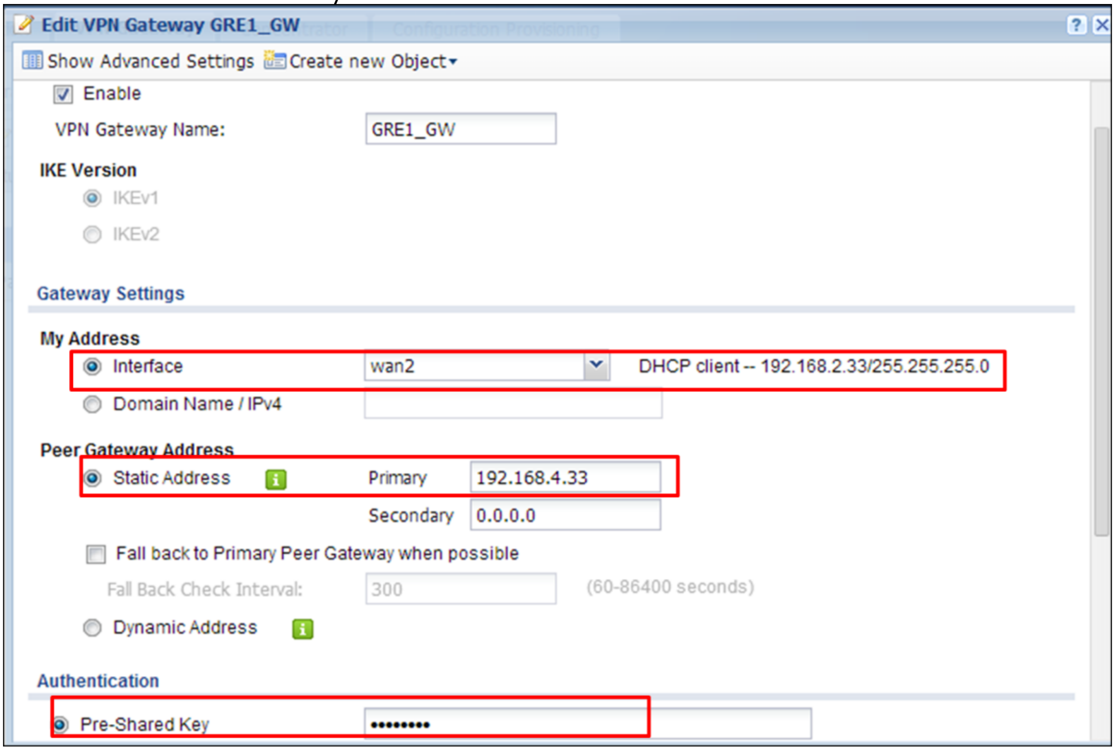
Fall Back Check Interval: 300 (60-86400 seconds)

○ 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

☑ 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

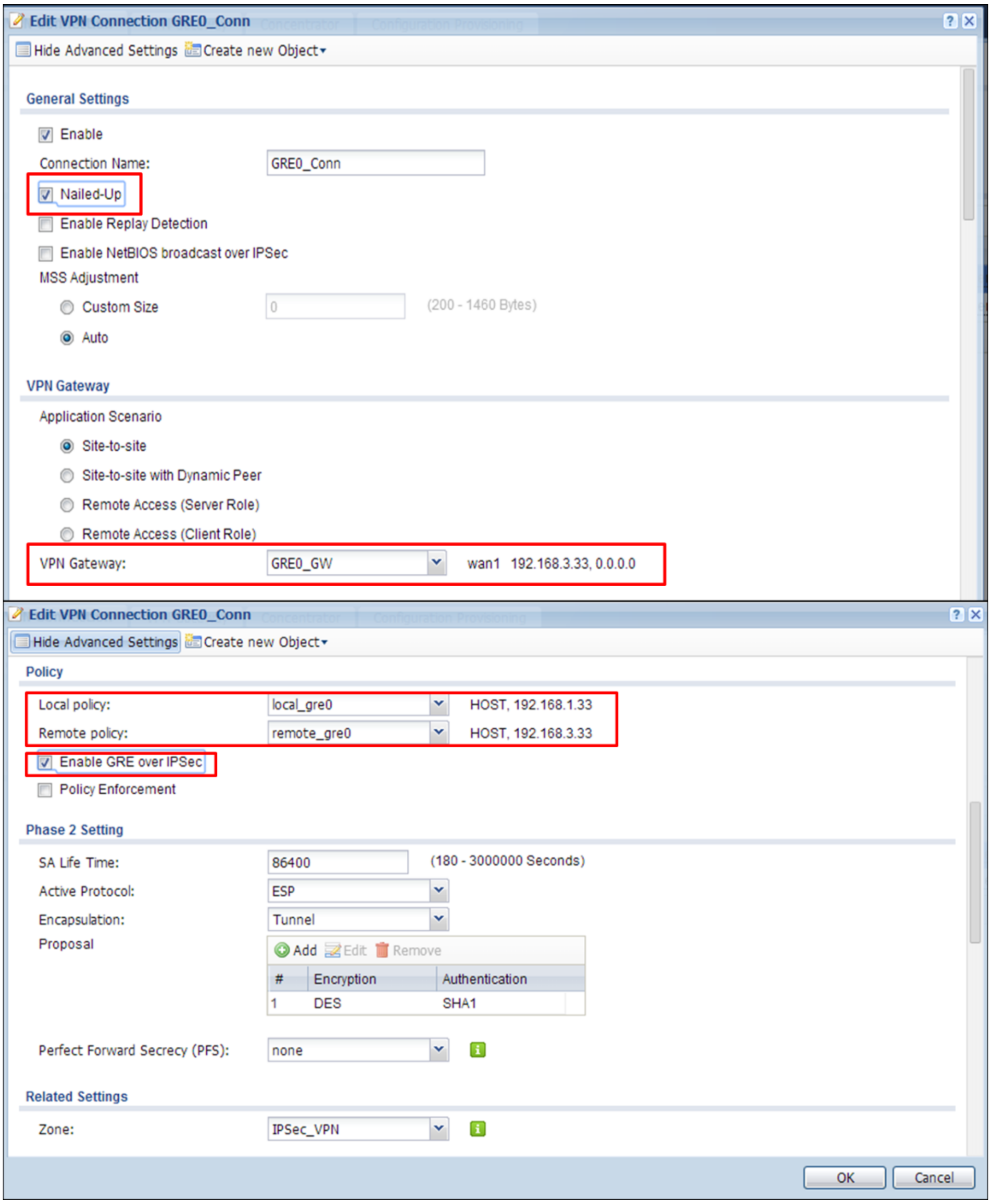
Fall Back Check Interval: 300 (60-86400 seconds)

○ 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



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

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

Add Edit Remove

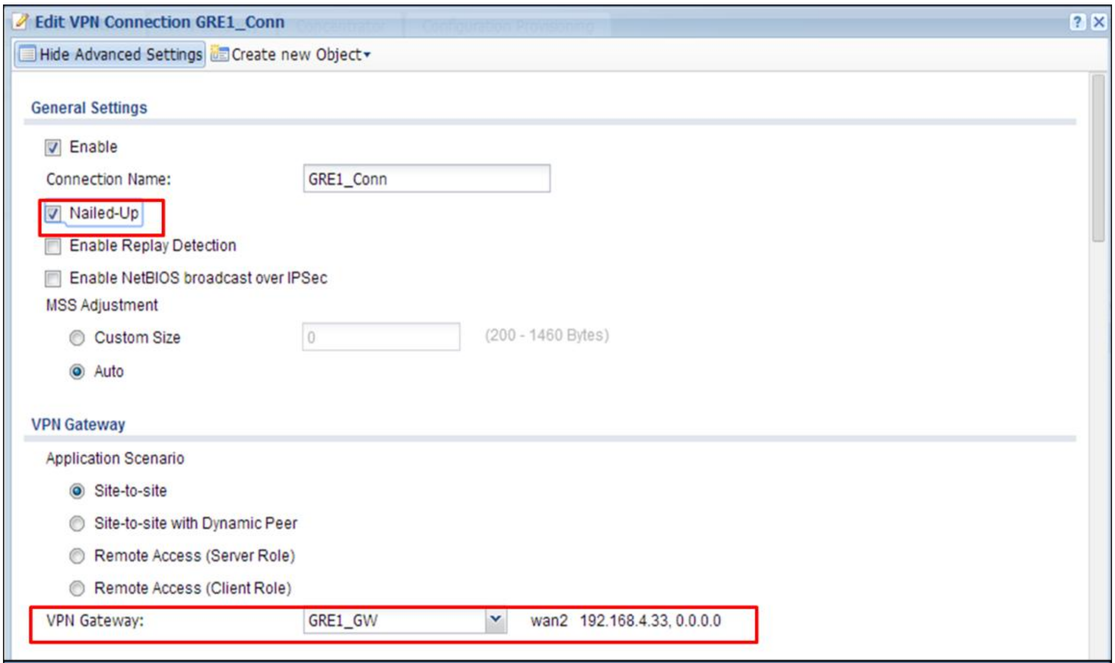
#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS): none

Related Settings

Zone: IPSec_VPN

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



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

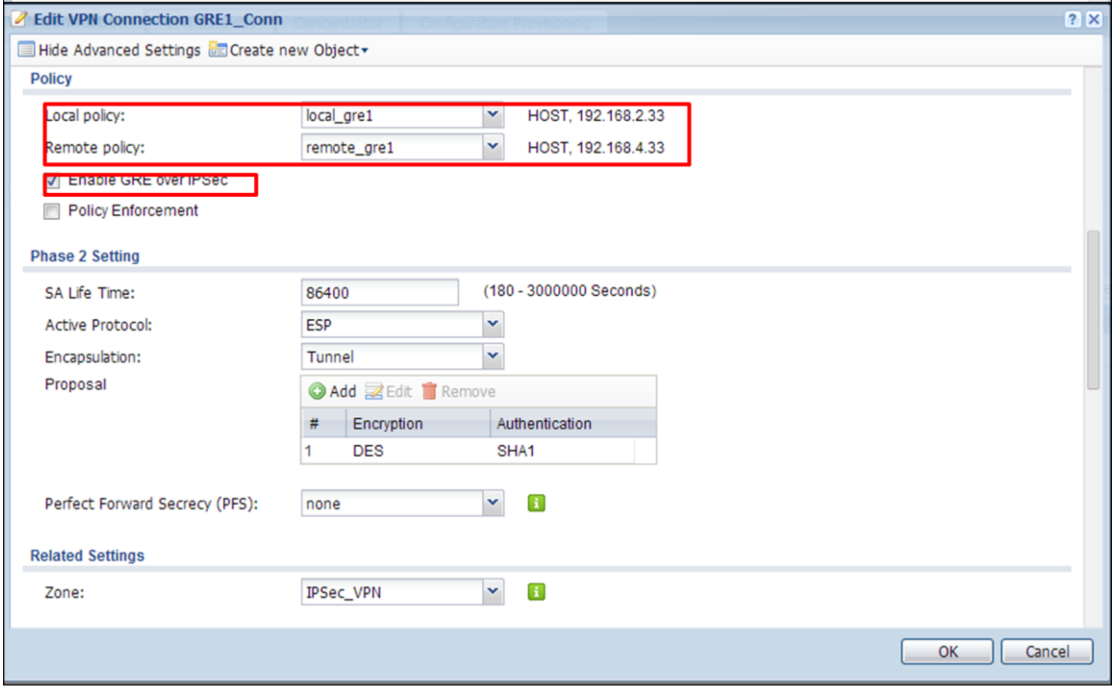
● Site-to-site

○ 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



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

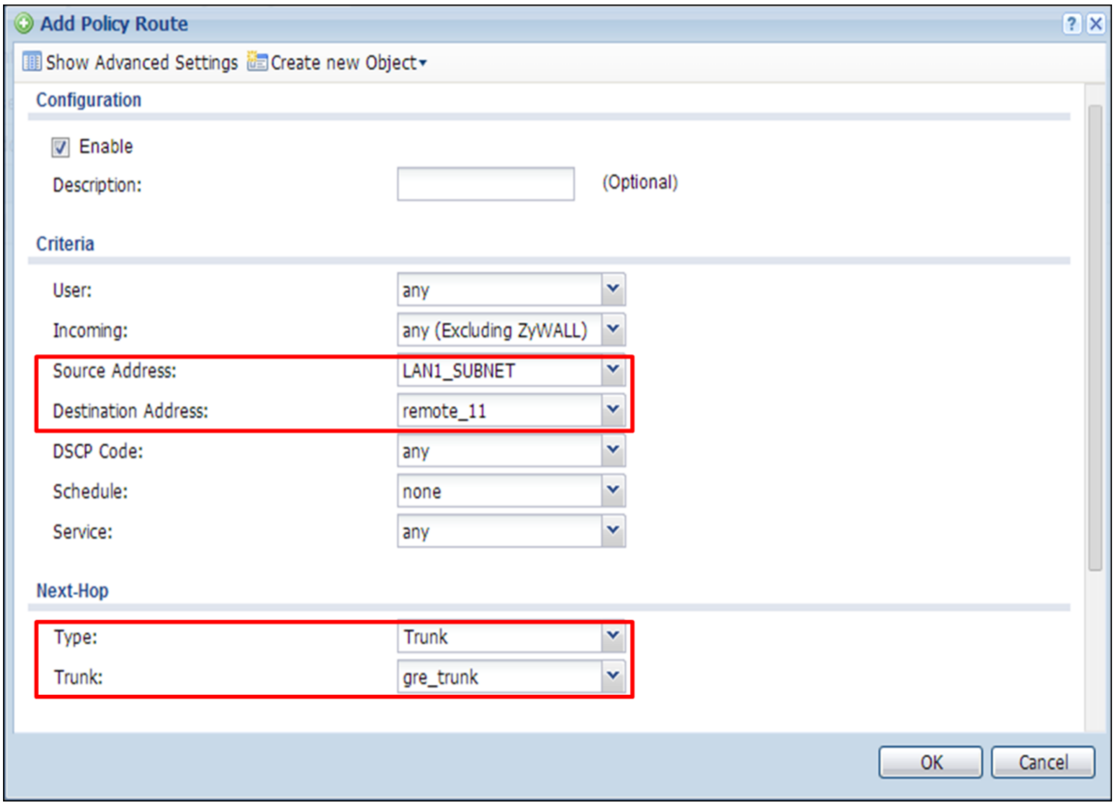
Perfect Forward Secrecy (PFS): none

Related Settings

Zone: IPSec_VPN

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

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

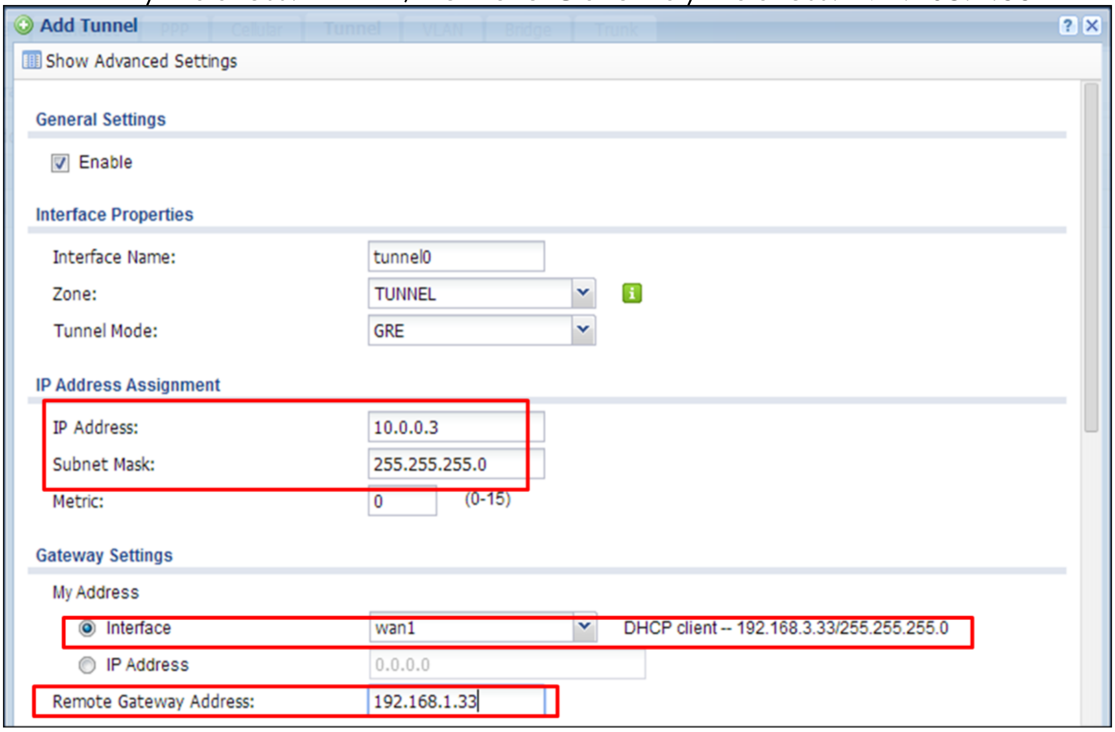
Next-Hop

Type: Trunk

Trunk: gre_trunk

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

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

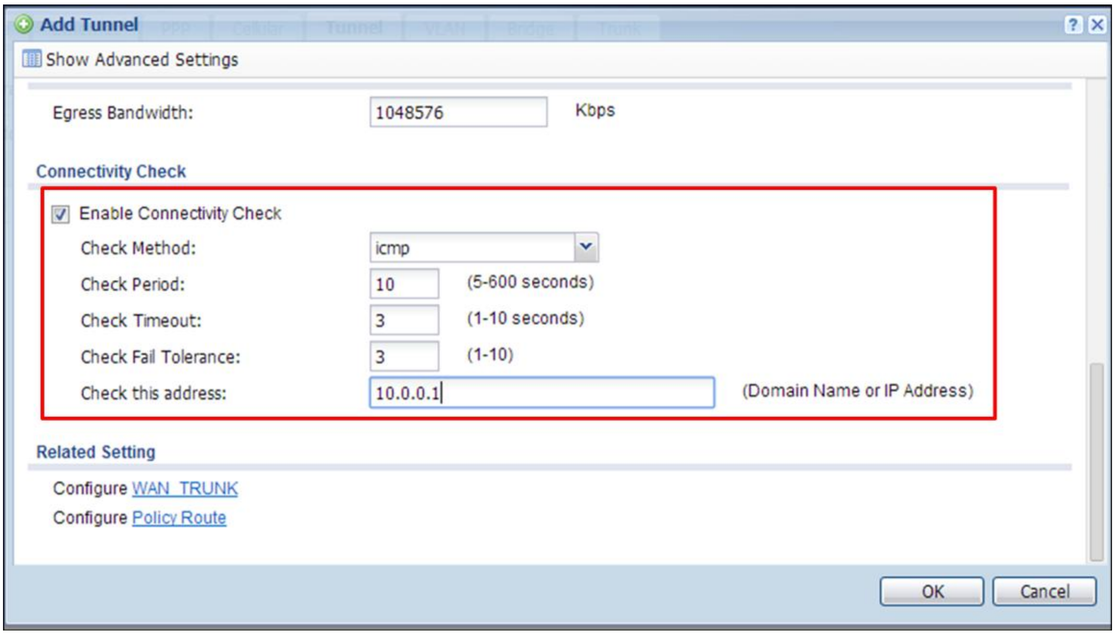
My Address

● 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

Show Advanced Settings

Egress Bandwidth: 1048576 Kbps

Connectivity Check

☑ Enable Connectivity Check

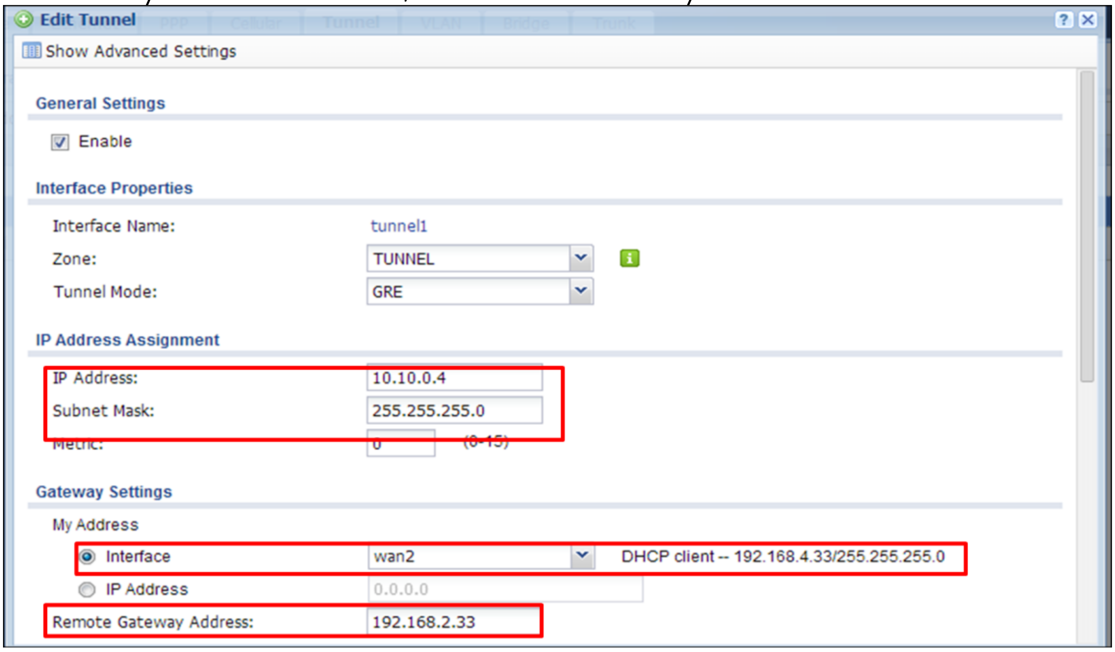
Check Method:	icmp	
Check Period:	10	(5-600 seconds)
Check Timeout:	3	(1-10 seconds)
Check Fail Tolerance:	3	(1-10)
Check this address:	10.0.0.1	(Domain Name or IP Address)

Related Setting

Configure WAN TRUNK

Configure Policy Route

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

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

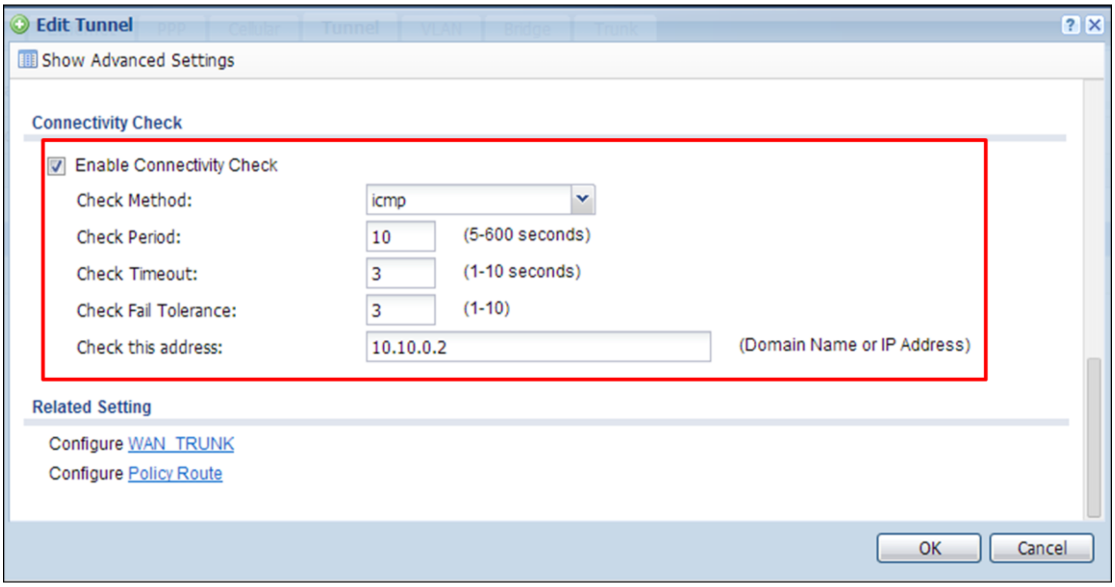
My Address

● 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.



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:	10.10.0.2	(Domain Name or IP Address)

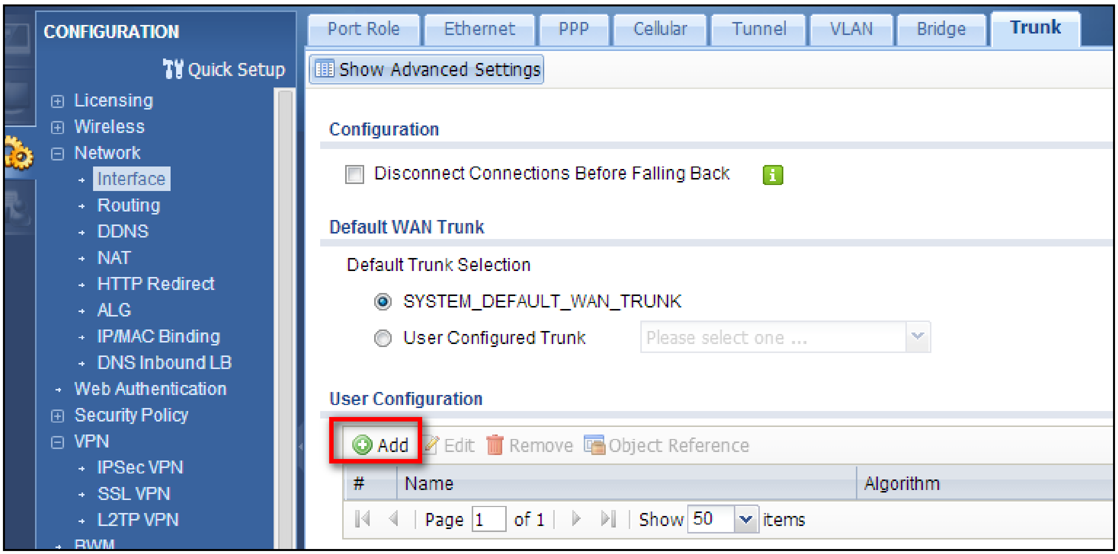
Related Setting

Configure WAN_TRUNK

Configure Policy Route

Step6. Add a GRE tunnel trunk on USG2. **Go to CONFIGURATION > Network > Interface > Trunk.**

gre_trunk member:
tunnel0: Active
Tunnel1: Passive



Configuration

□ Disconnect Connections Before Falling Back

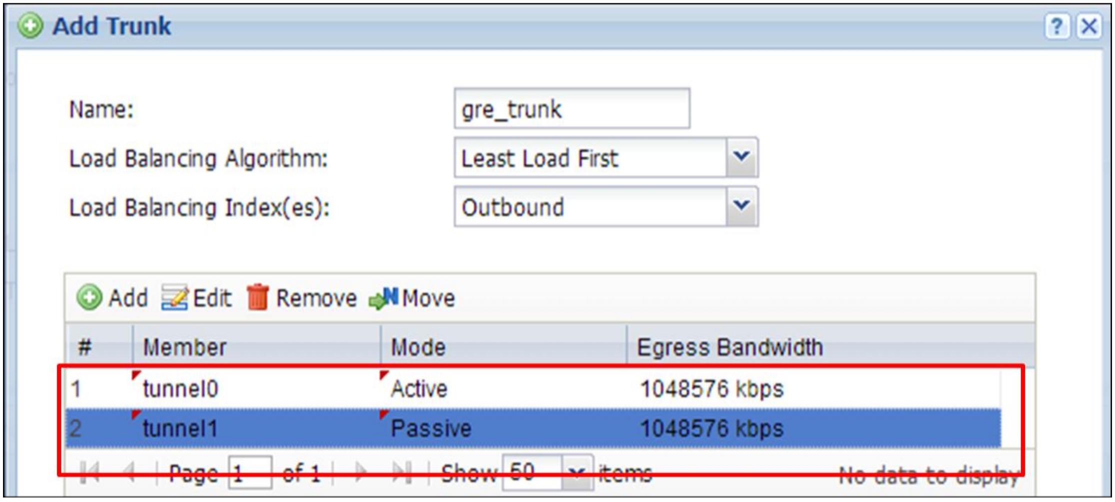
Default WAN Trunk

Default Trunk Selection

● SYSTEM_DEFAULT_WAN_TRUNK

○ User Configured Trunk Please select one ...

User Configuration

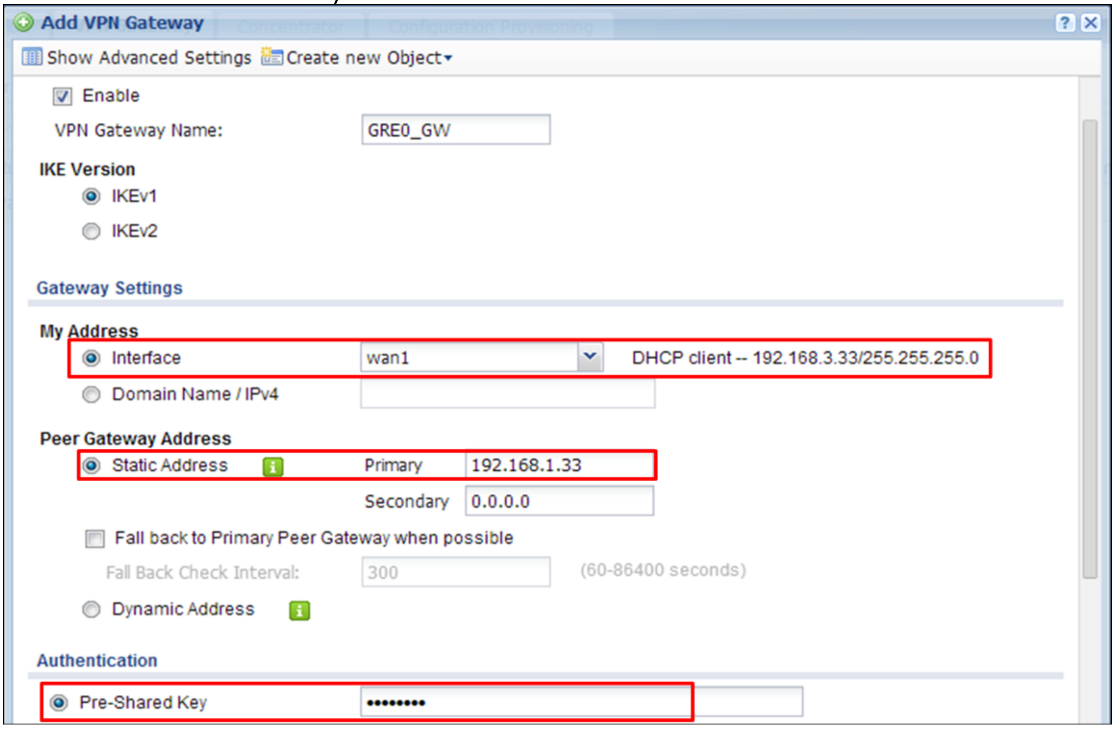


Name:	gre_trunk
Load Balancing Algorithm:	Least Load First
Load Balancing Index(es):	Outbound

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

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



Add VPN Gateway

Show Advanced Settings | Create new Object

☑ Enable

VPN Gateway Name: GRE0_GW

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface wan1 DHCP client -- 192.168.3.33/255.255.255.0

○ Domain Name / IPv4

Peer Gateway Address

● Static Address Primary 192.168.1.33

Secondary 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

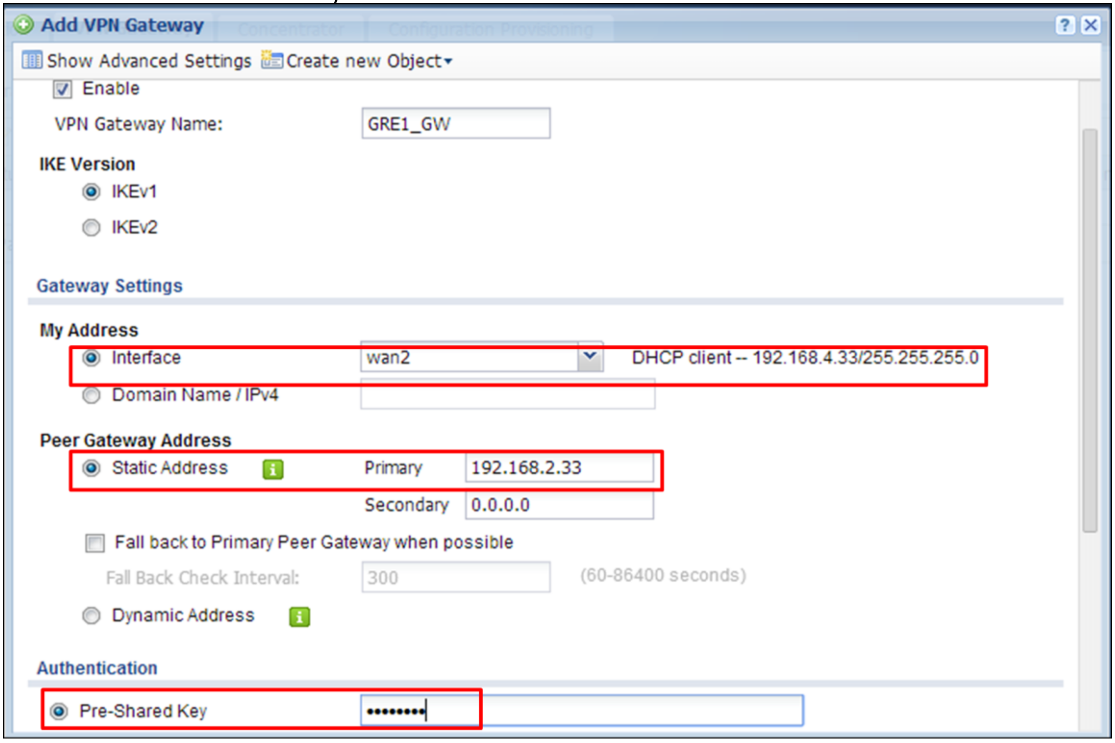
Fall Back Check Interval: 300 (60-86400 seconds)

○ Dynamic Address

Authentication

● Pre-Shared Key ••••••••

   Second VPN Gateway
   My Address: wan2, Peer Gateway Address: 192.168.2.33
   Pre-Shared Key: 12345678



Add VPN Gateway

Show Advanced Settings | Create new Object

☑ Enable

VPN Gateway Name: GRE1_GW

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface wan2 DHCP client -- 192.168.4.33/255.255.255.0

○ Domain Name / IPv4

Peer Gateway Address

● Static Address Primary 192.168.2.33

Secondary 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

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

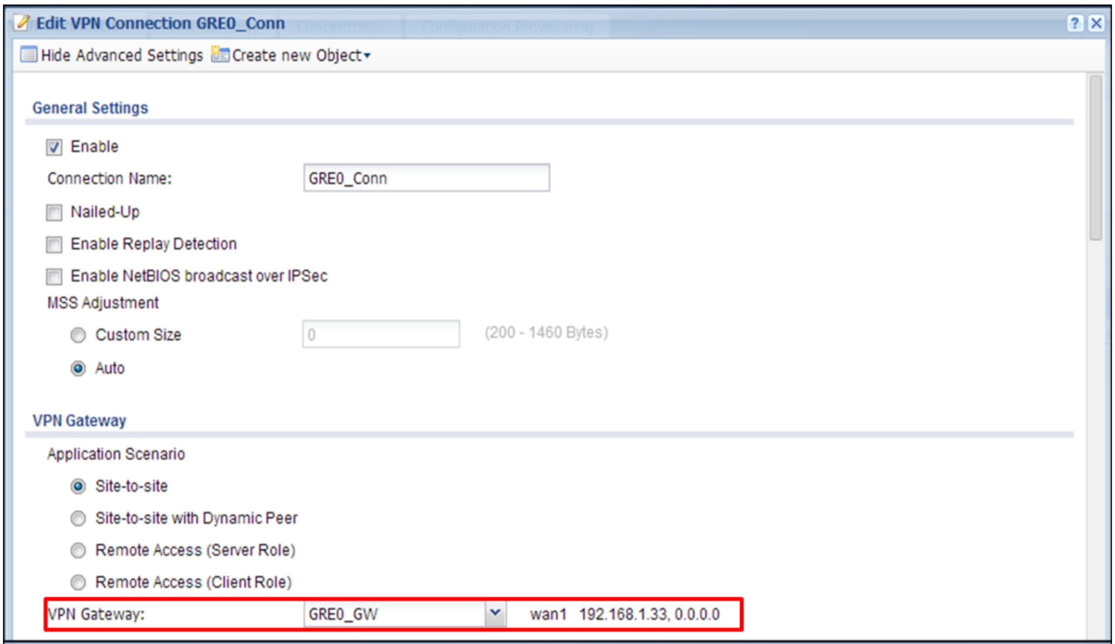
○ Dynamic Address

Authentication

● Pre-Shared Key ••••••••

b. Add two VPN Connections.
   First VPN connection
   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

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

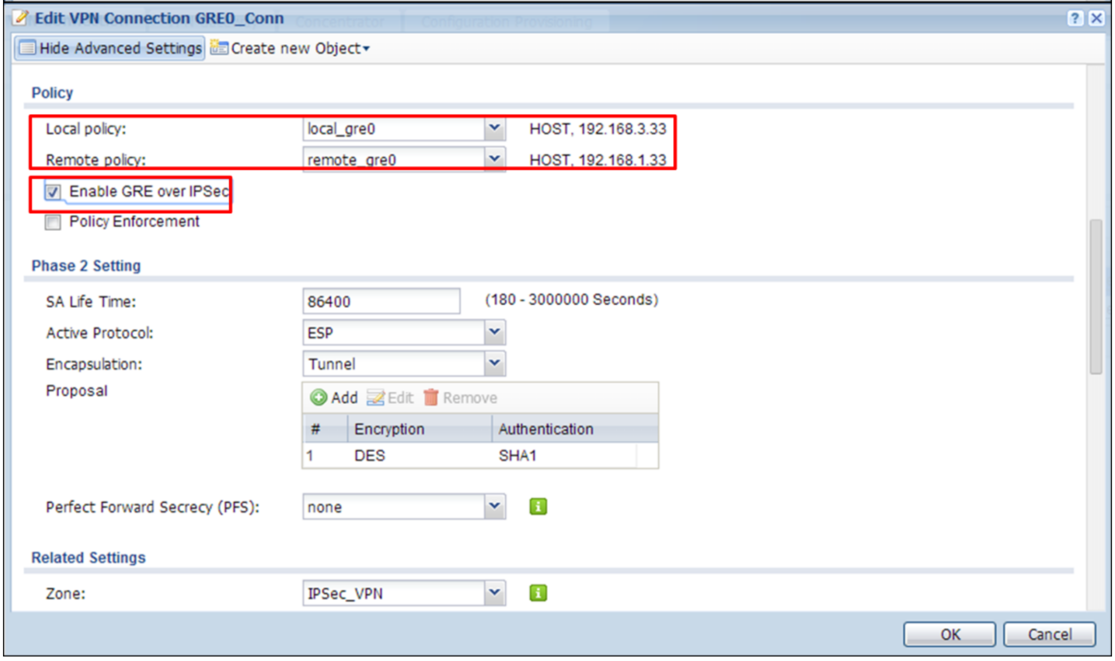
● Site-to-site

○ 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

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

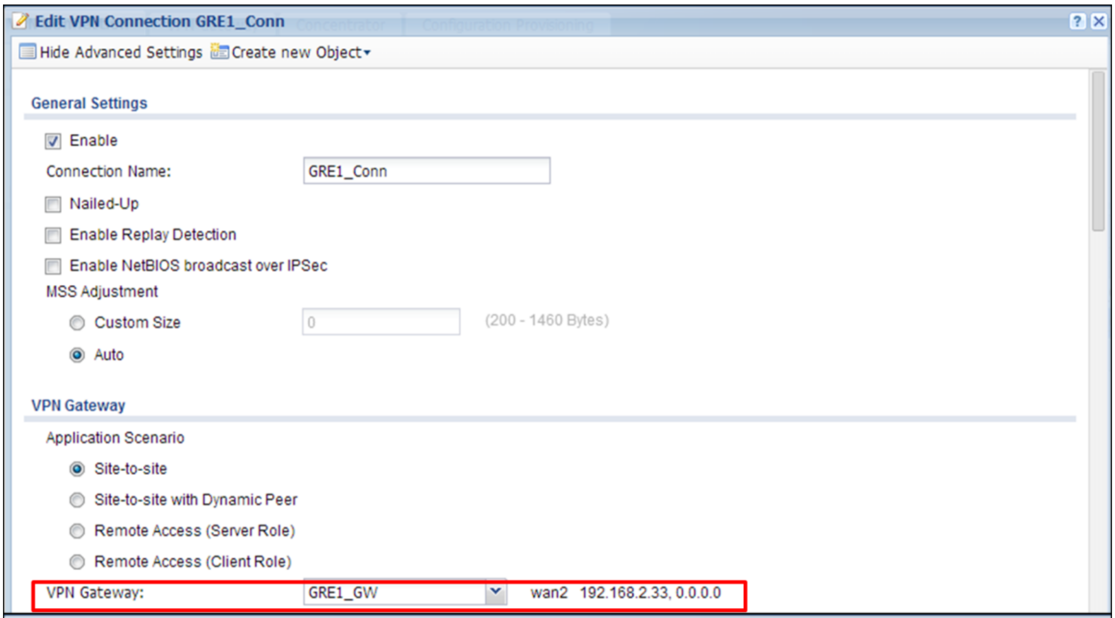
#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS): none

Related Settings

Zone: IPSec_VPN

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

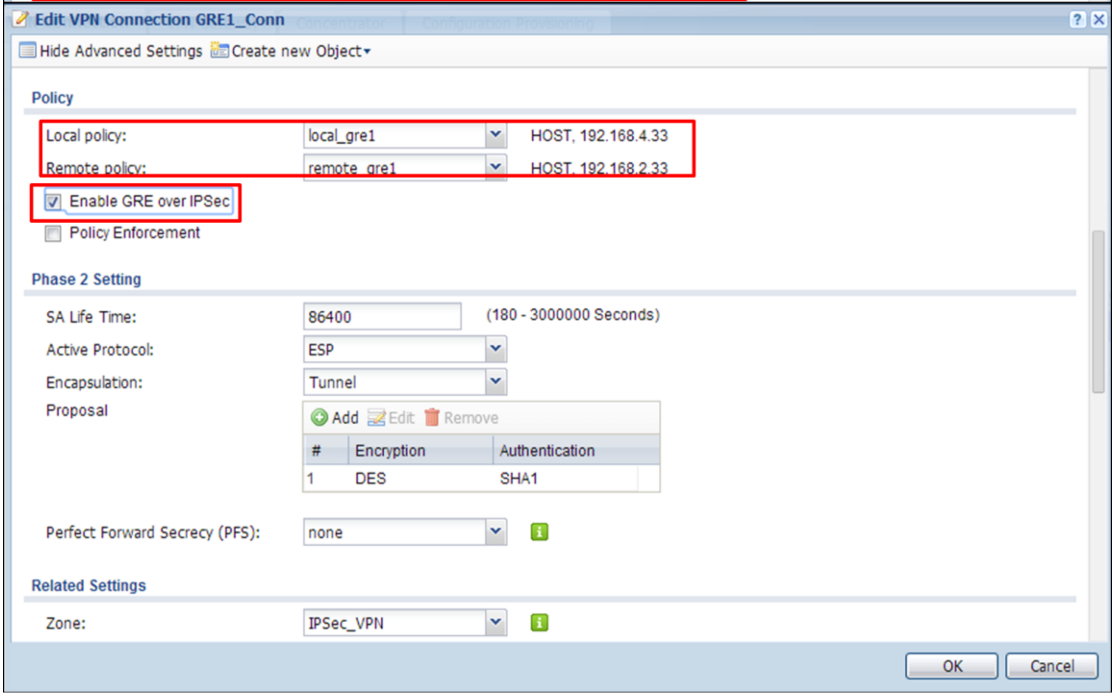
● Site-to-site

○ 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

Add | Edit | Remove

#	Encryption	Authentication
1	DES	SHA1

Perfect Forward Secrecy (PFS): none

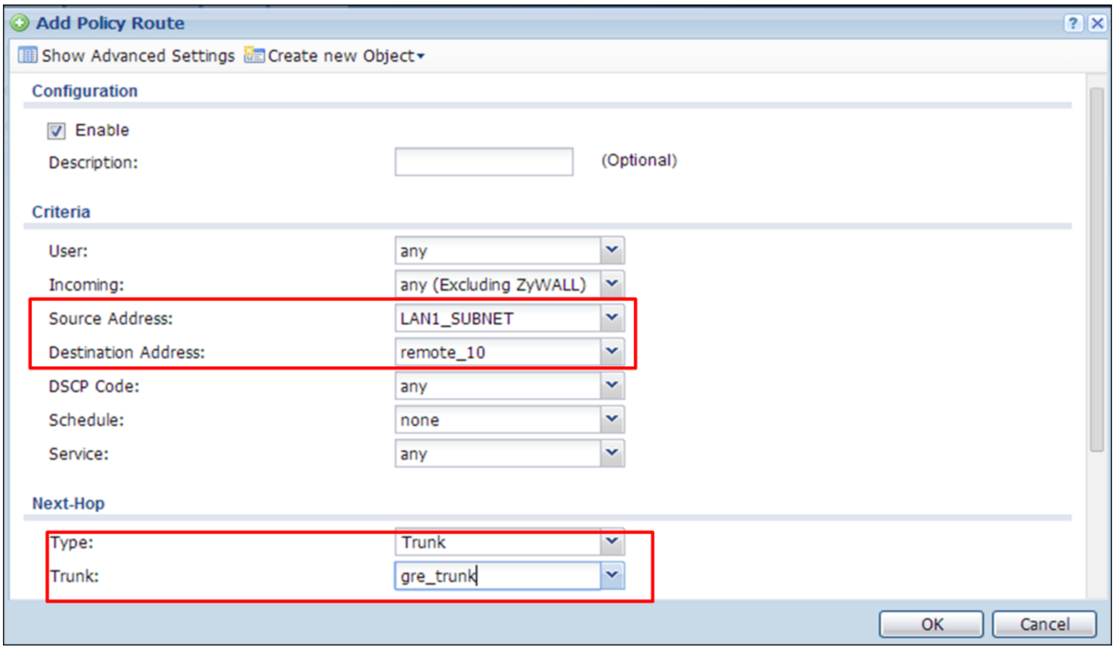
Related Settings

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

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

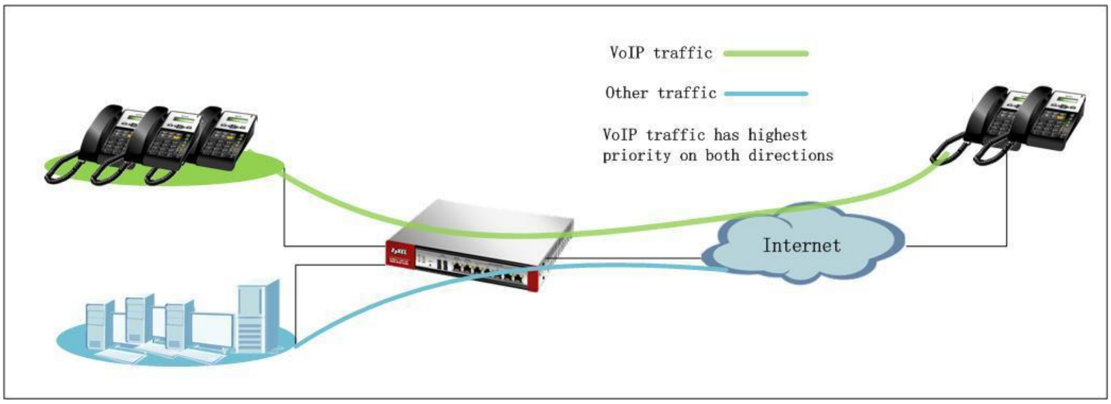
Trunk: gre_trunk

Scenario 5 — Reserving Highest Bandwidth Management Priority for VoIP traffic

5.1 Application Scenario

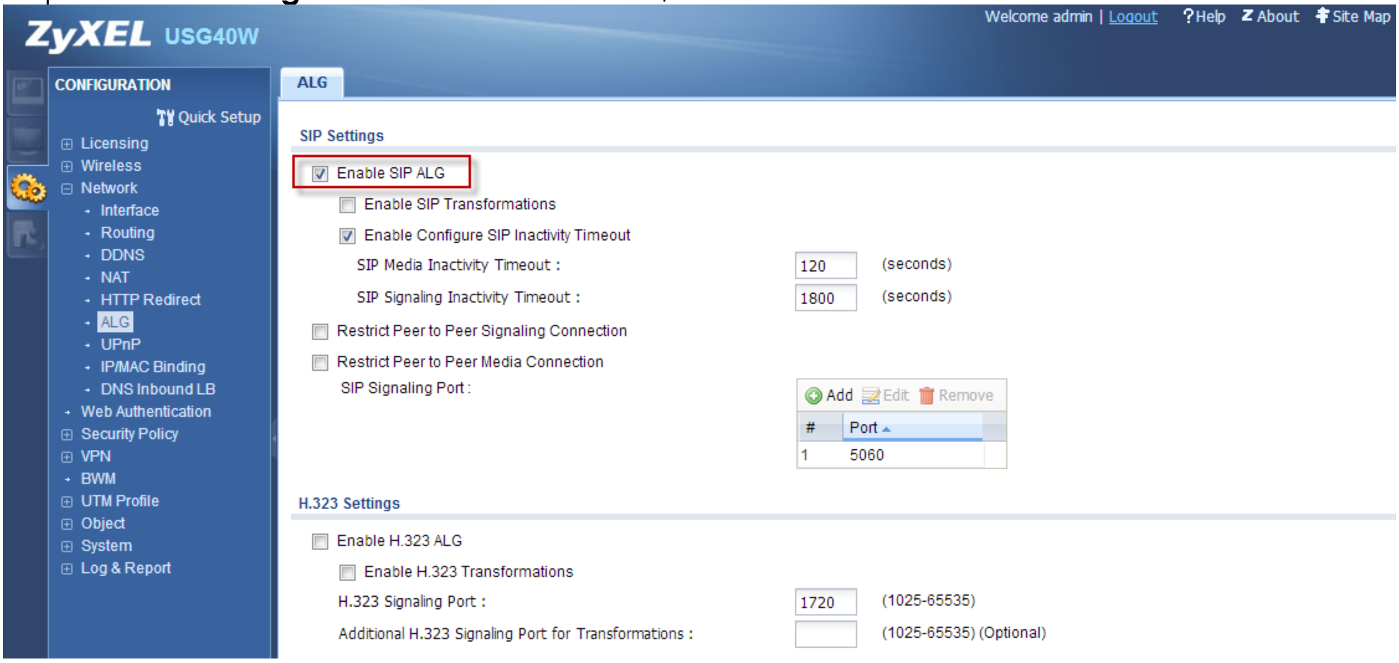
In an enterprise network, there are various types of traffic. But the company Internet connection bandwidth is limited to a specific value. All this traffic will contend to use the limited bandwidth, which may result in some important traffic, for example, VoIP traffic getting slow or even starved. Therefore, 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.



5.2 Configuration Guide

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



SIP Settings

☑ Enable SIP ALG

☐ Enable SIP Transformations

☑ Enable Configure SIP Inactivity Timeout

SIP Media Inactivity Timeout : 120 (seconds)

SIP Signaling Inactivity Timeout : 1800 (seconds)

☐ Restrict Peer to Peer Signaling Connection

☐ Restrict Peer to Peer Media Connection

SIP Signaling Port :

#	Port
1	5060

H.323 Settings

☐ Enable H.323 ALG

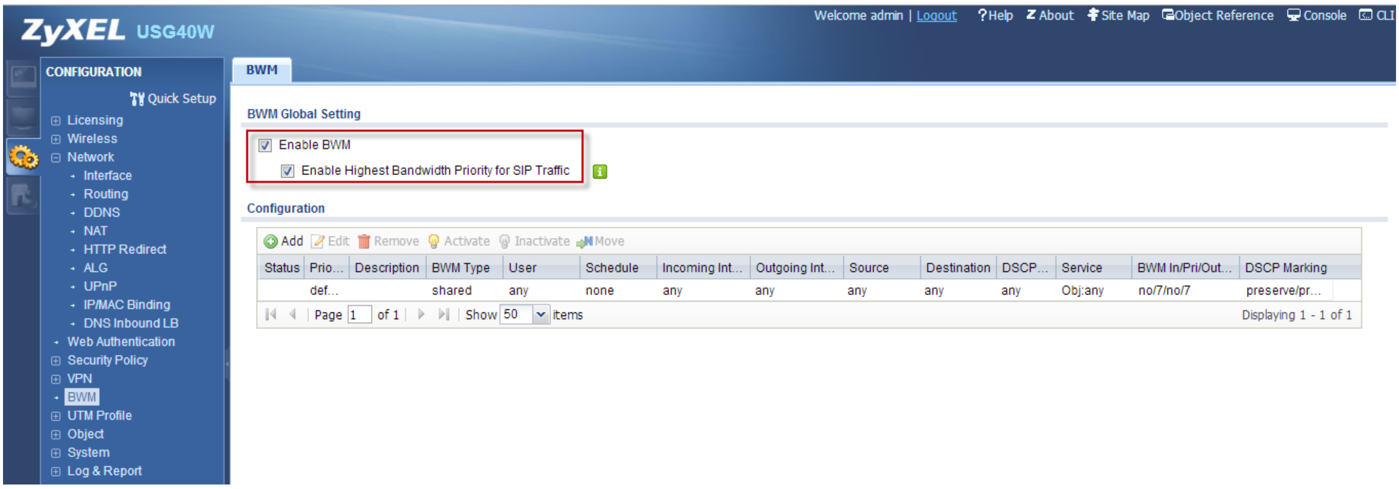
☐ Enable H.323 Transformations

H.323 Signaling Port : 1720 (1025-65535)

Additional H.323 Signaling Port for Transformations : (1025-65535) (Optional)

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.



BWM Global Setting

☑ Enable BWM

☑ Enable Highest Bandwidth Priority for SIP Traffic

Configuration

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/no/7	preserve/pr...

Page 1 of 1 | Show 50 items

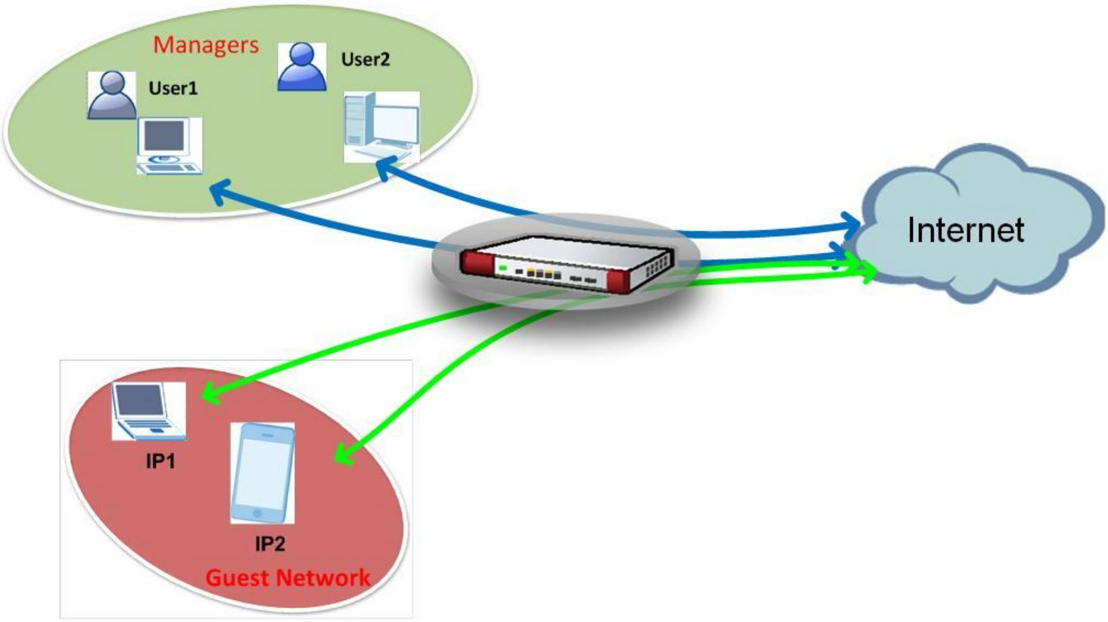
Displaying 1 - 1 of 1

Scenario 6 - Reserving Highest Bandwidth Management Priority for a Superior User and Control Session per Host – BWM Per IP or Per User

6.1 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 a 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.



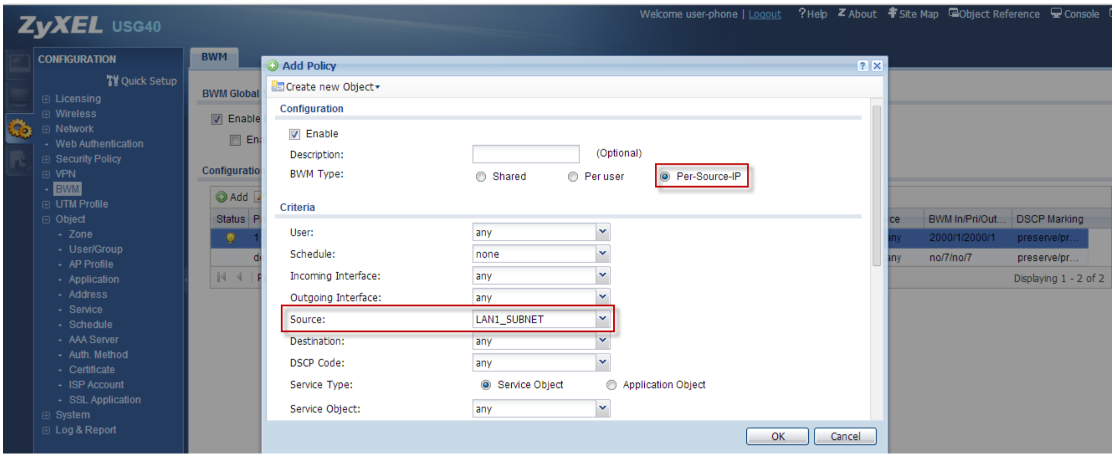
6.2 Configuration Guide

BWM Per IP

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



Configuration

☑ Enable

Description: (Optional)

BWM Type: ○ Shared ○ Per user ● Per-Source-IP

Criteria

User: any

Schedule: none

Incoming Interface: any

Outgoing Interface: any

Source: LAN1_SUBNET

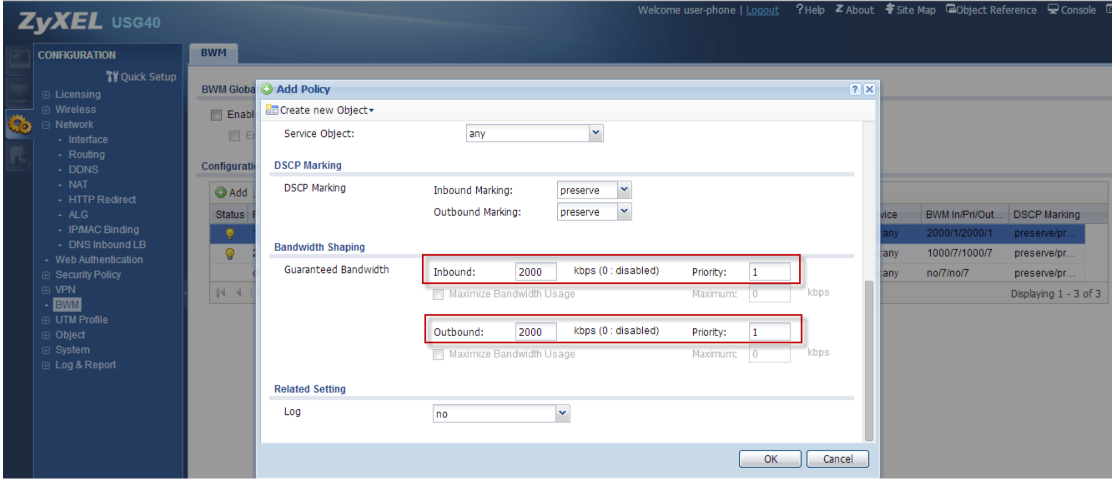
Destination: any

DSCP Code: any

Service Type: ● Service Object ○ Application Object

Service Object: any

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



Service Object: any

DSCP Marking

DSCP Marking Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth Inbound: 2000 kbps (0 : disabled) Priority: 1

□ Maximize Bandwidth Usage Maximum: 0 kbps

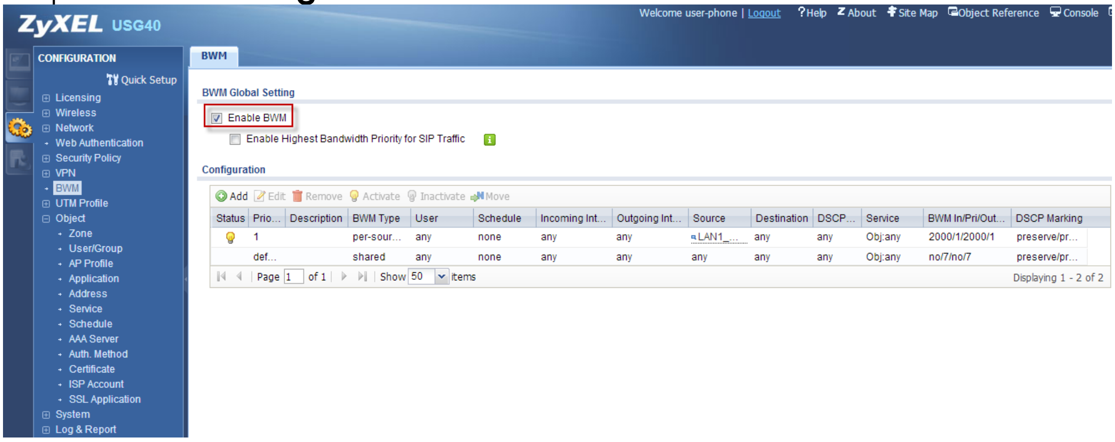
Outbound: 2000 kbps (0 : disabled) Priority: 1

□ Maximize Bandwidth Usage Maximum: 0 kbps

Related Setting

Log: no

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



BWM Global Setting

☑ Enable BWM

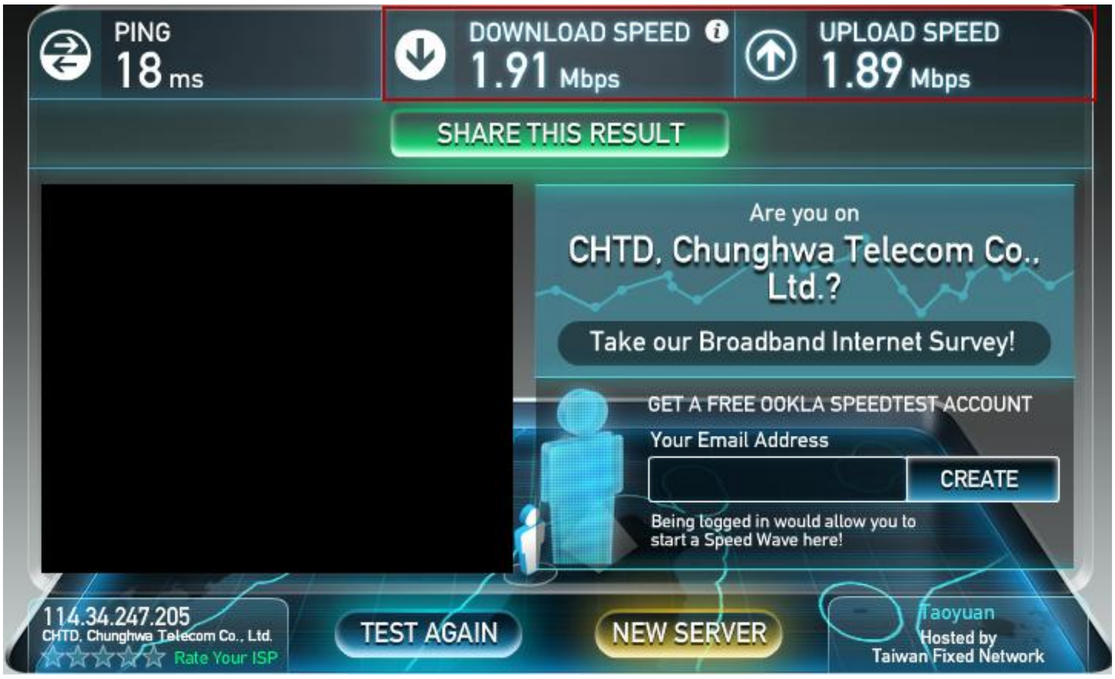
□ Enable Highest Bandwidth Priority for SIP Traffic

Configuration

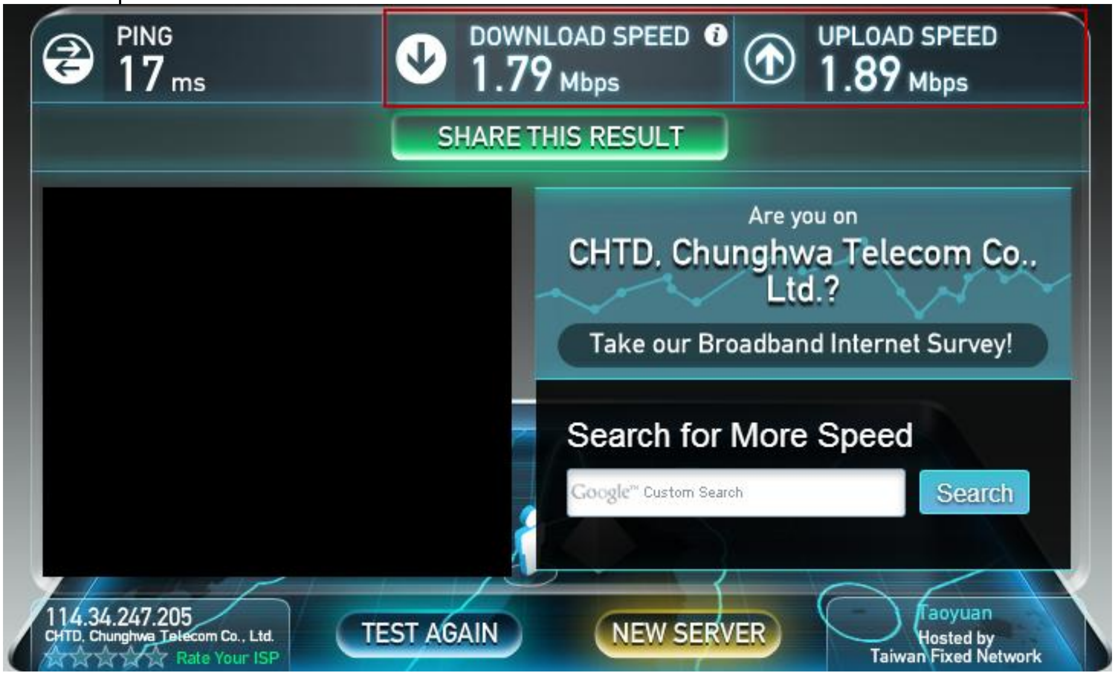
Status	Prio...	Description	BWM Type	User	Schedule	Incoming Int...	Outgoing Int...	Source	Destination	DSCP...	Service	BWM In/Pri/Out...	DSCP Marking
💡	1		per-sour...	any	none	any	any	LAN1_...	any	any	Obj:any	2000/1/2000/1	preserve/pr...
	def...		shared	any	none	any	any	any	any	any	Obj:any	no/7/no/7	preserve/pr...

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

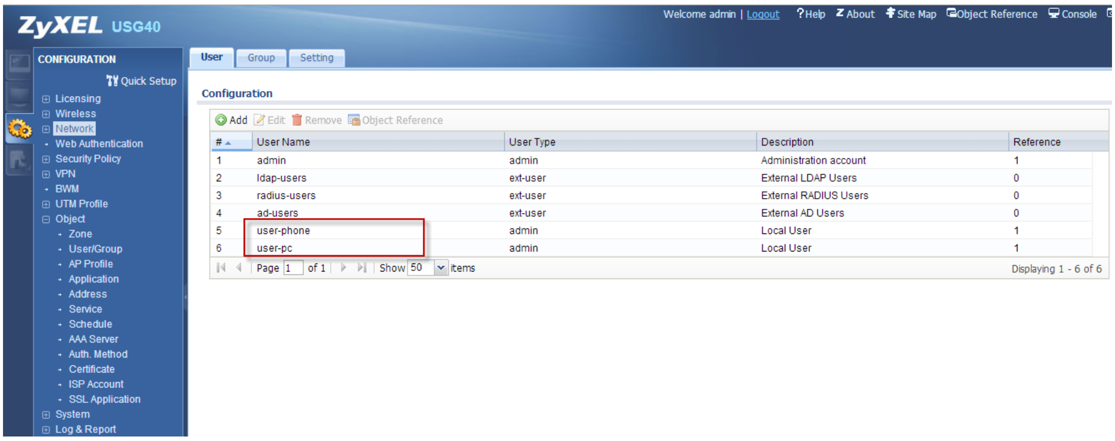
Step 3. Use the PC's IP address of "192.168.1.33" to connect to the USG.
Visit the website http://www.speedtest.net/ to test the speed.
The test result is around 2 Mbps, which is the same as our setup to manage per source IP 2 Mbps.


PING
18 ms
DOWNLOAD SPEED
1.91 Mbps
UPLOAD SPEED
1.89 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

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.



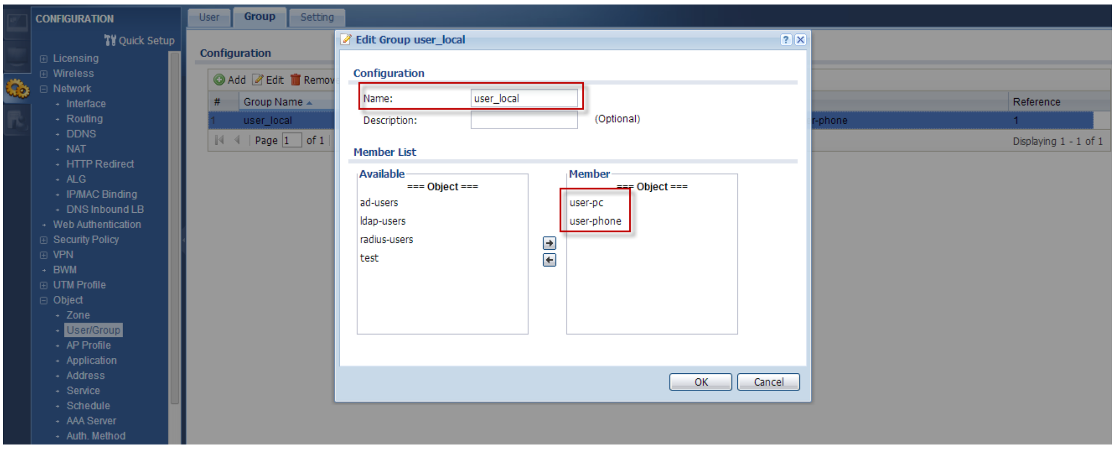
BWM Per User-
Step 1. Go to **Configuration > Object > User/Group**.
(1) Add one user name as "user-phone", and add another user name as "user-pc".



#	User Name	User Type	Description	Reference
1	admin	admin	Administration account	1
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	user-phone	admin	Local User	1
6	user-pc	admin	Local User	1

Page 1 of 1 | Show 50 items | Displaying 1 - 6 of 6

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



Configuration

Name: user_local

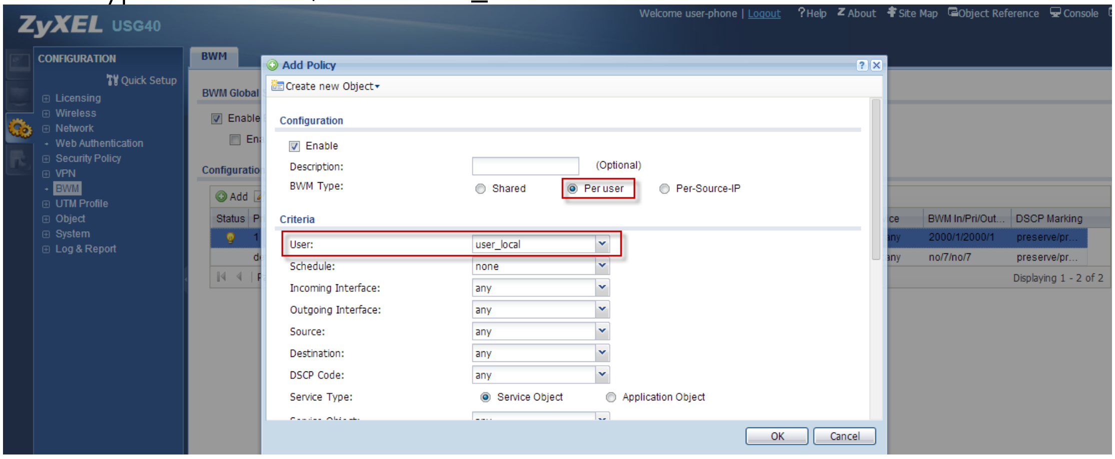
Description: (Optional)

Member List

Available	Member
=== Object ===	=== Object ===
ad-users	user-pc
ldap-users	user-phone
radius-users	
test	

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



Configuration

☑ Enable

Description: (Optional)

BWM Type: ○ Shared ● Per user ○ Per-Source-IP

Criteria

User: user_local

Schedule: none

Incoming Interface: any

Outgoing Interface: any

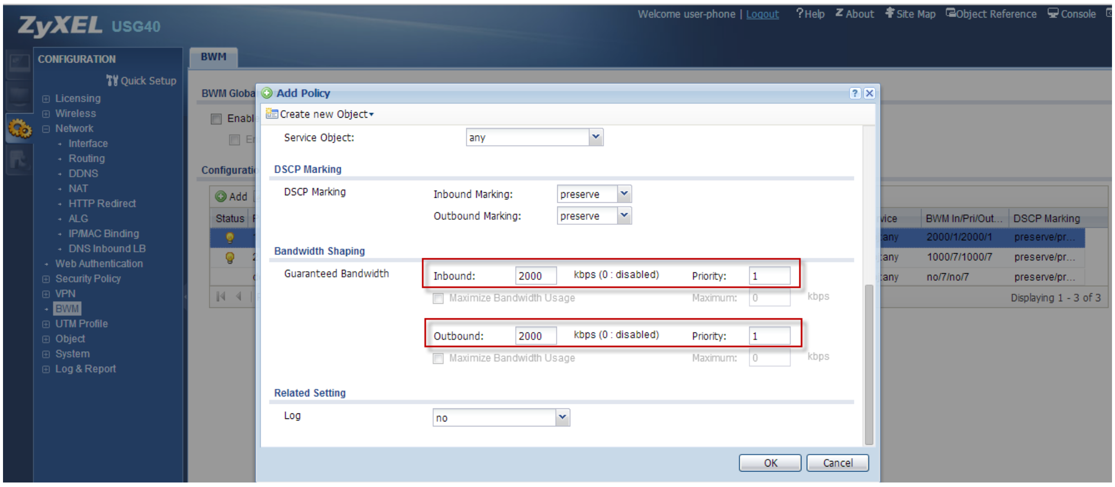
Source: any

Destination: any

DSCP Code: any

Service Type: ● Service Object ○ Application Object

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



Add Policy

Create new Object▾

Service Object: any

DSCP Marking

DSCP Marking — Inbound Marking: preserve; Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth — Inbound: 2000 kbps (0 : disabled) Priority: 1

□ Maximize Bandwidth Usage Maximum: 0 kbps

Outbound: 2000 kbps (0 : disabled) Priority: 1

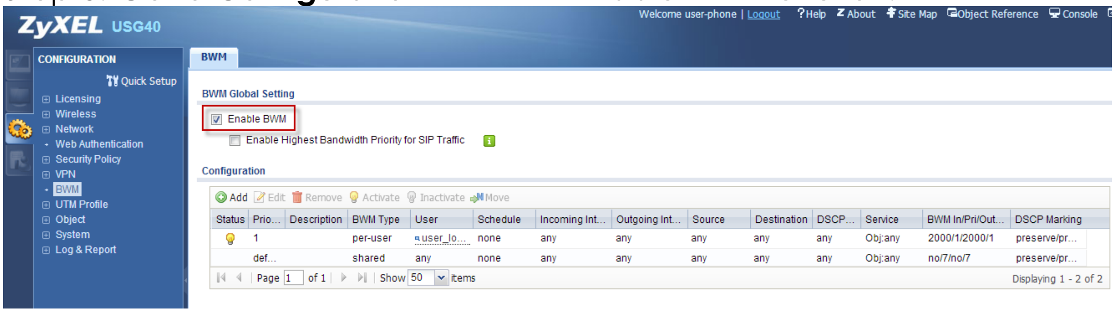
□ Maximize Bandwidth Usage Maximum: 0 kbps

Related Setting

Log: no

OK Cancel

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



BWM Global Setting

☑ Enable BWM

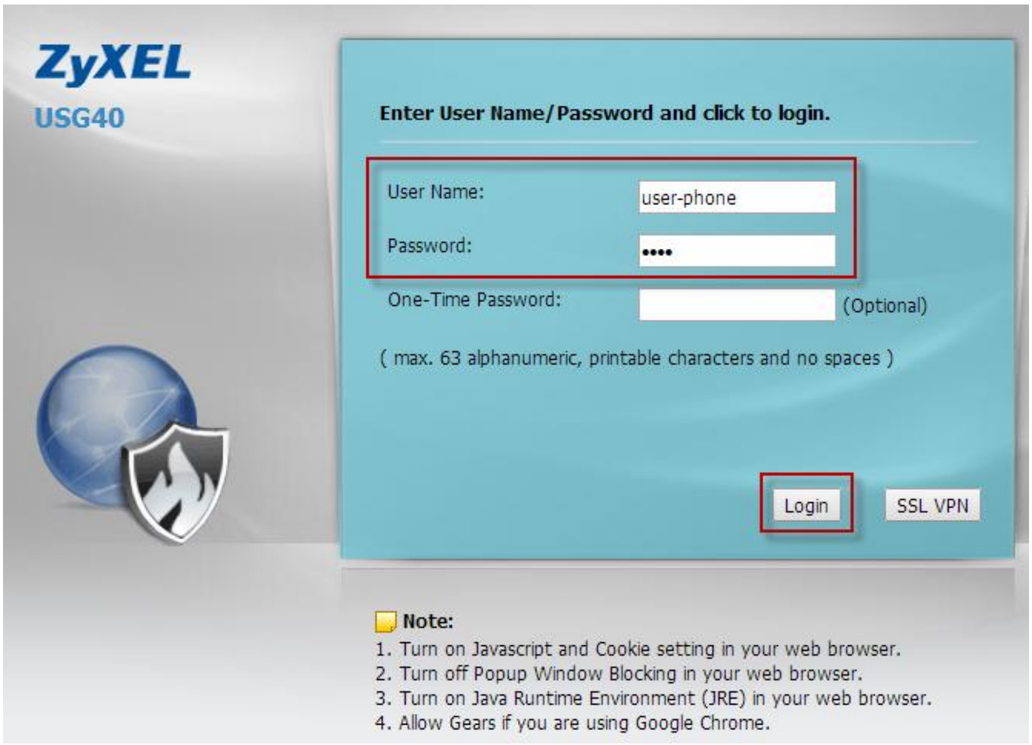
□ Enable Highest Bandwidth Priority for SIP Traffic

Configuration

Status	Prio...	Description	BWM Type	User	Schedule	Incoming Int...	Outgoing Int...	Source	Destination	DSCP...	Service	BWM In/Pri/Out...	DSCP Marking
💡	1		per-user	user_lo...	none	any	any	any	any	any	Obj:any	2000/1/2000/1	preserve/pr...
	def...		shared	any	none	any	any	any	any	any	Obj:any	no/7/no/7	preserve/pr...

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

Step 4. Verify with the "user-phone" account.
(1) Enter the "user-phone" user name and password and Login.



Enter User Name/Password and click to login.

User Name: user-phone

Password: ••••

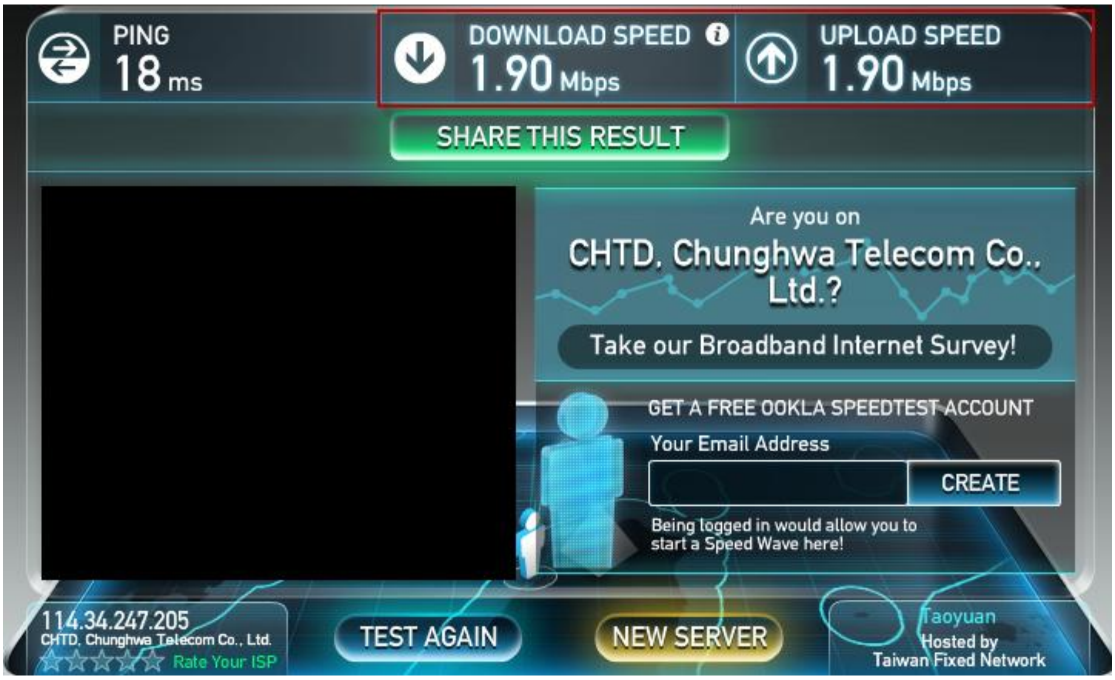
One-Time Password: (Optional)

(max. 63 alphanumeric, printable characters and no spaces)

Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.

(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

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

Take our Broadband Internet Survey!

GET A FREE OOKLA SPEEDTEST ACCOUNT

Your Email Address

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

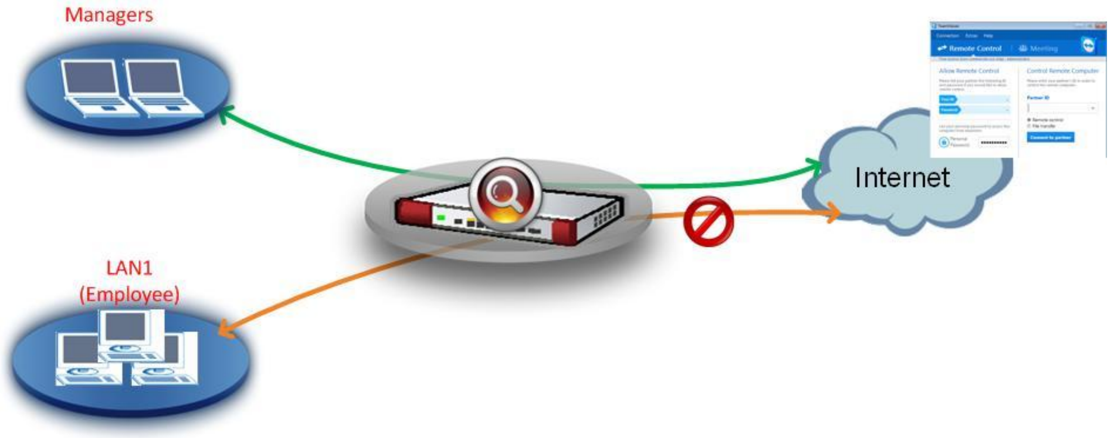
114.34.247.205
CHTD. Chunghwa Telecom Co., Ltd.

Taoyuan
Hosted by
Taiwan Fixed Network

Scenario 7 - Using USG to Control Popular Applications –APP Patrol

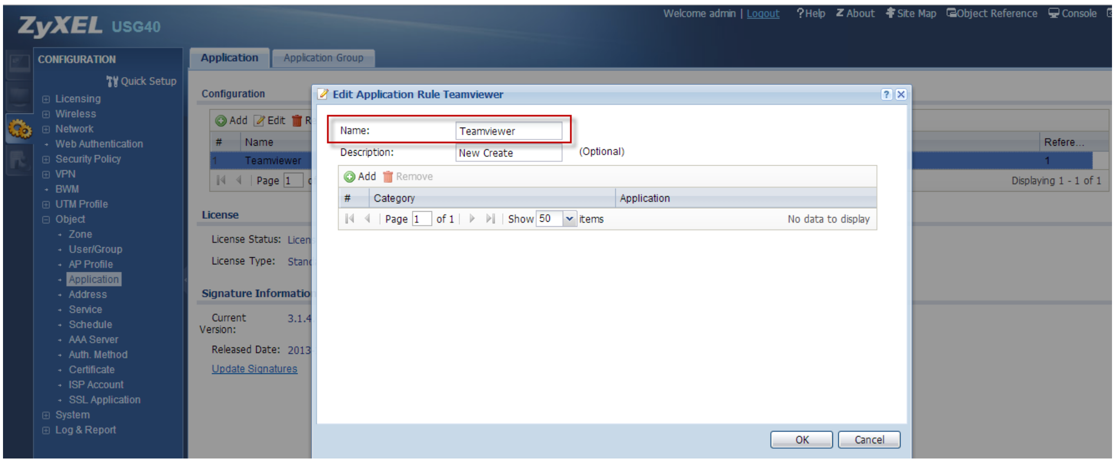
7.1 Application Scenario

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.



7.2 Configuration Guide

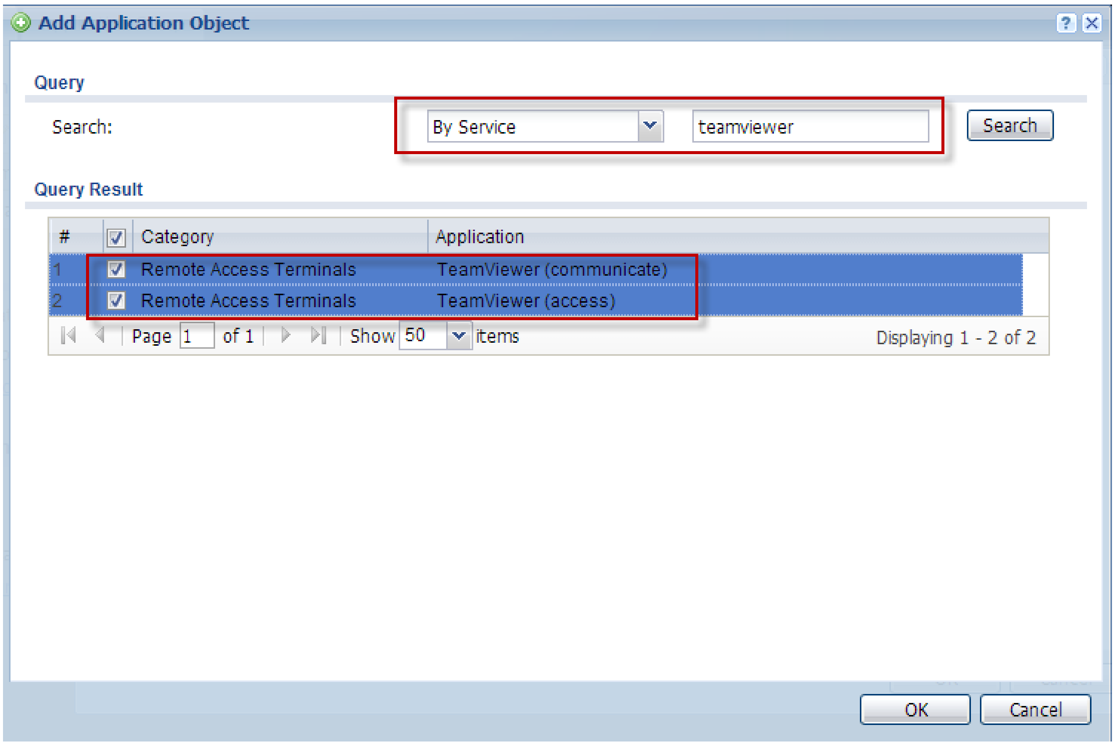
Step 1. Go to **Configuration > Object > Application > Add Application Rule**
For example
Name: Teamviewer


Edit Application Rule Teamviewer

Name: Teamviewer
Description: New Create (Optional)

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.



Add Application Object

Query

Search: By Service | teamviewer | Search

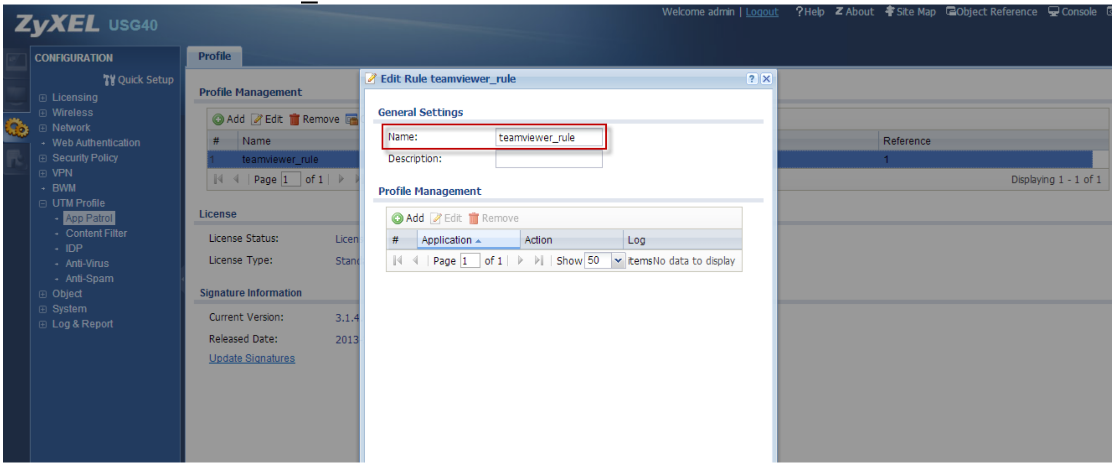
Query Result

#	☑	Category	Application
1	☑	Remote Access Terminals	TeamViewer (communicate)
2	☑	Remote Access Terminals	TeamViewer (access)

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

OK | Cancel

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



Profile Management

Add | Edit | Remove

#	Name	Reference
1	teamviewer_rule	1

Page 1 of 1 | Displaying 1 - 1 of 1

License

License Status: Licen

License Type: Stan

Signature Information

Current Version: 3.1.4

Released Date: 2013

Update Signatures

Edit Rule teamviewer_rule

General Settings

Name: teamviewer_rule

Description:

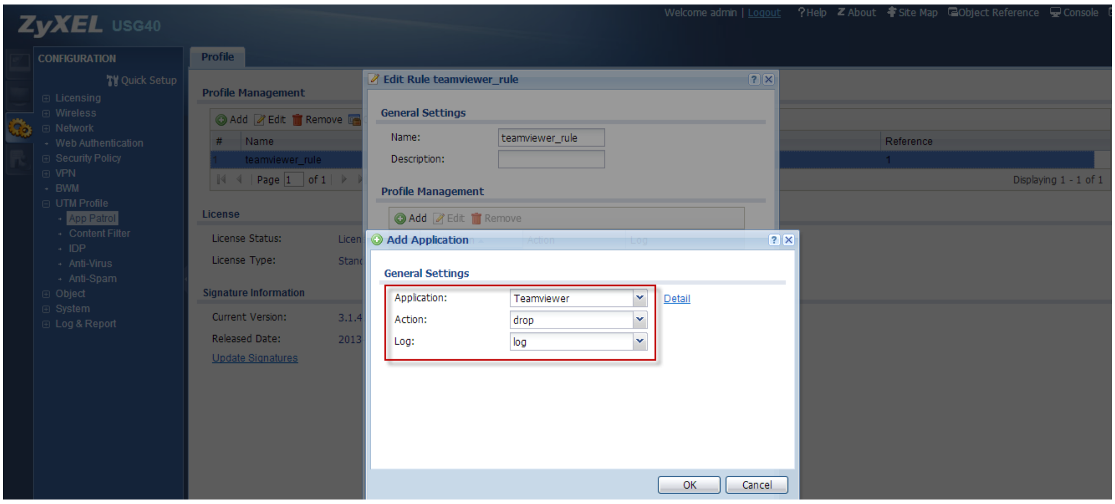
Profile Management

Add | Edit | Remove

#	Application	Action	Log

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

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.



Edit Rule teamviewer_rule

General Settings

Name: teamviewer_rule

Description:

Profile Management

Add Application

General Settings

Application: Teamviewer

Action: drop

Log: log

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

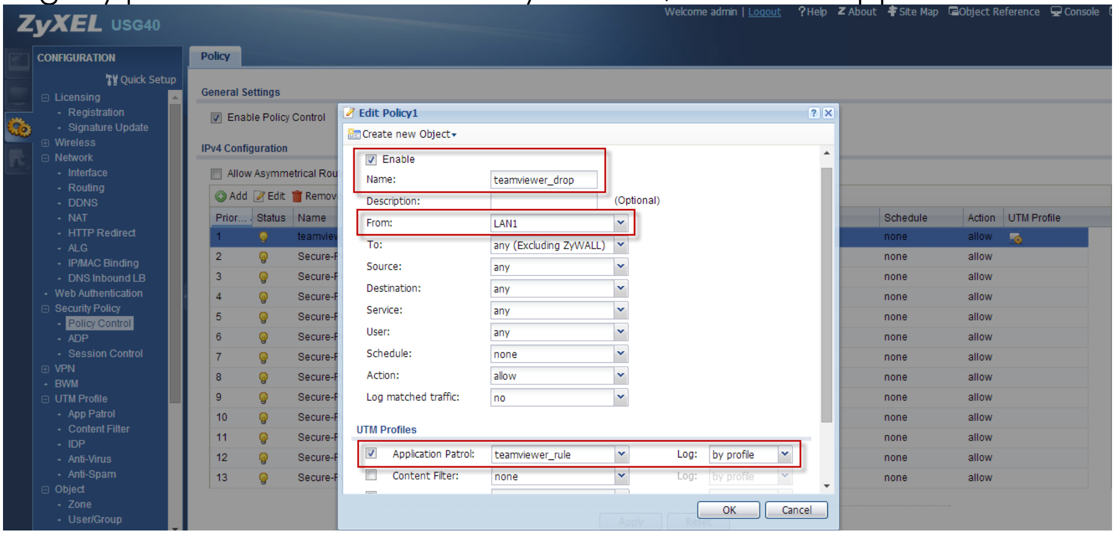
For example

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.



Edit Policy1

☑ Enable

Name: teamviewer_drop

Description: (Optional)

From: LAN1

To: any (Excluding ZyWALL)

Source: any

Destination: any

Service: any

User: any

Schedule: none

Action: allow

Log matched traffic: no

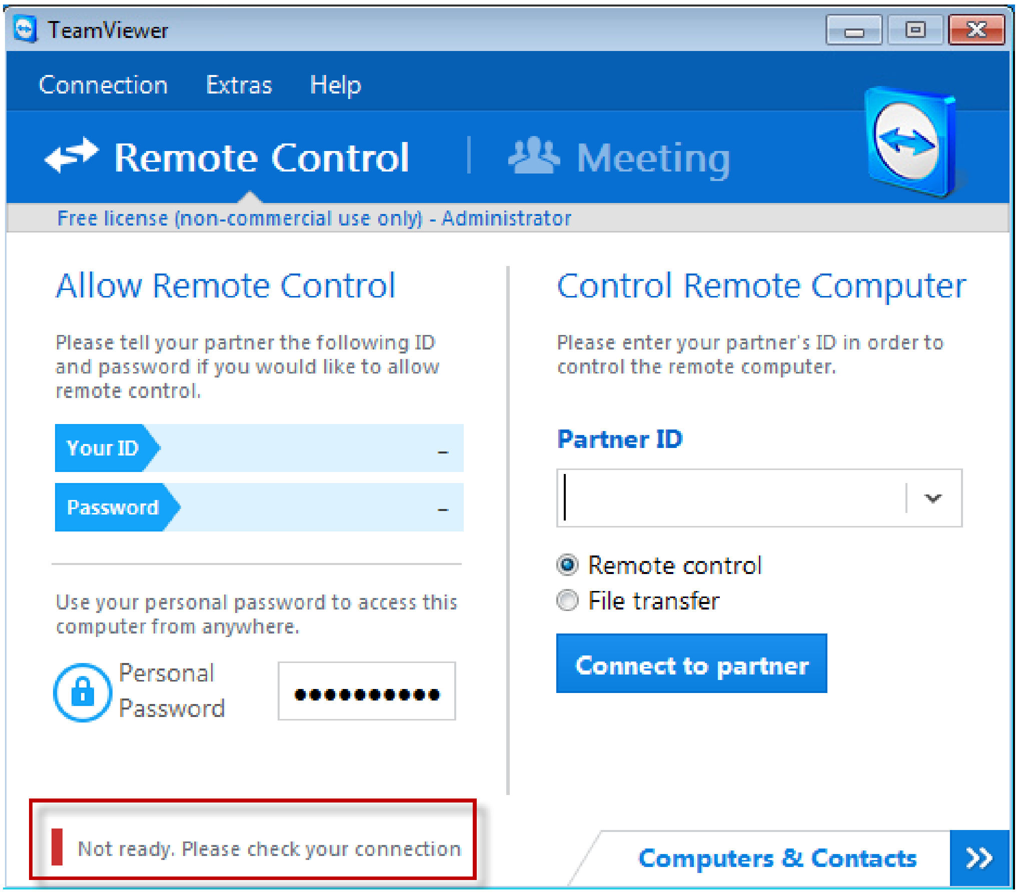
UTM Profiles

☑ Application Patrol: teamviewer_rule Log: by profile

□ Content Filter: none Log: by profile

Step 6. Connect to the PC under USG LAN1, then teamviewer application will not open.

But from other interface can, it can open.



Free license (non-commercial use only) - Administrator

Allow Remote Control

Please tell your partner the following ID and password if you would like to allow remote control.

Your ID –

Password –

Use your personal password to access this computer from anywhere.

Personal Password ●●●●●●●●●●●

Control Remote Computer

Please enter your partner's ID in order to control the remote computer.

Partner ID

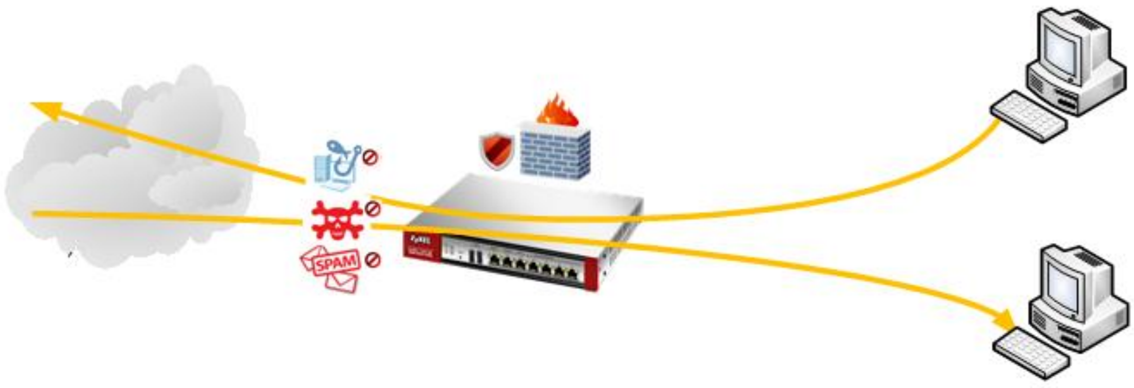
● Remote control

○ File transfer

Connect to partner

Not ready. Please check your connection

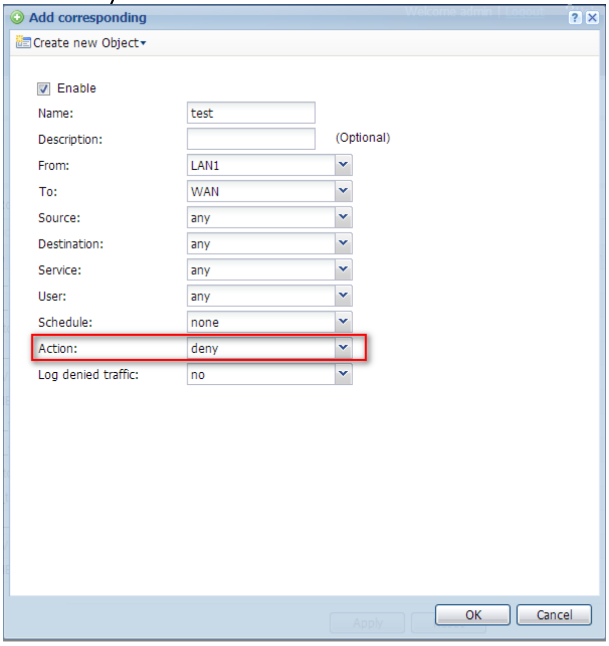
Scenario 8 – Configure Unified Policy (Firewall Policy + UTM Profile)



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.

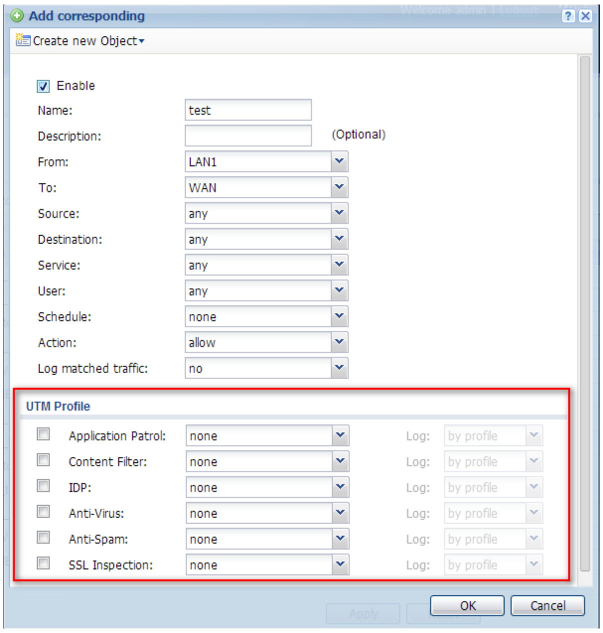
If the packets are already dropped by the firewall rule, then it will not check the UTM rule any more.



☑ 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.



☑ Enable

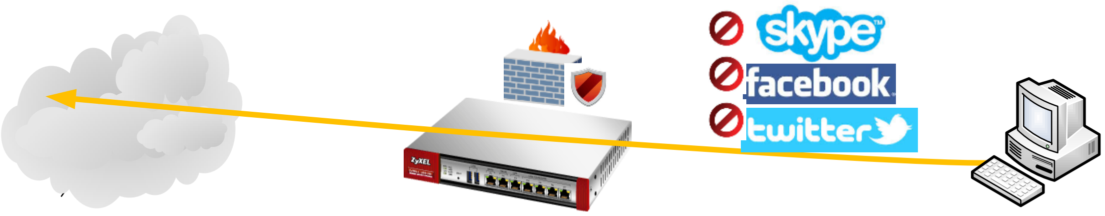
Name:	test
Description:	(Optional)
From:	LAN1
To:	WAN
Source:	any
Destination:	any
Service:	any
User:	any
Schedule:	none
Action:	allow
Log matched traffic:	no

UTM Profile

□	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

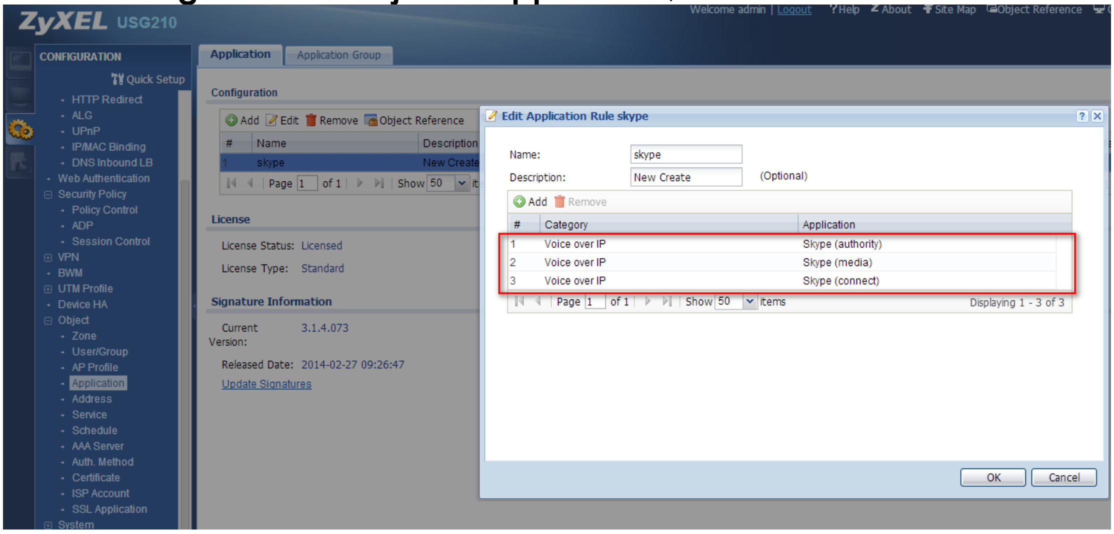
8.1 Application Scenario

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



8.2 Configuration Guide

(1) Add a Skype object in Application.
Go to **Configuration** > **Object** > **Application**, and click on the "**Add**" button.



#	Name	Description
1	skype	New Create

License

License Status: Licensed

License Type: Standard

Signature Information

Current Version: 3.1.4.073

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

Edit Application Rule skype

Name: skype

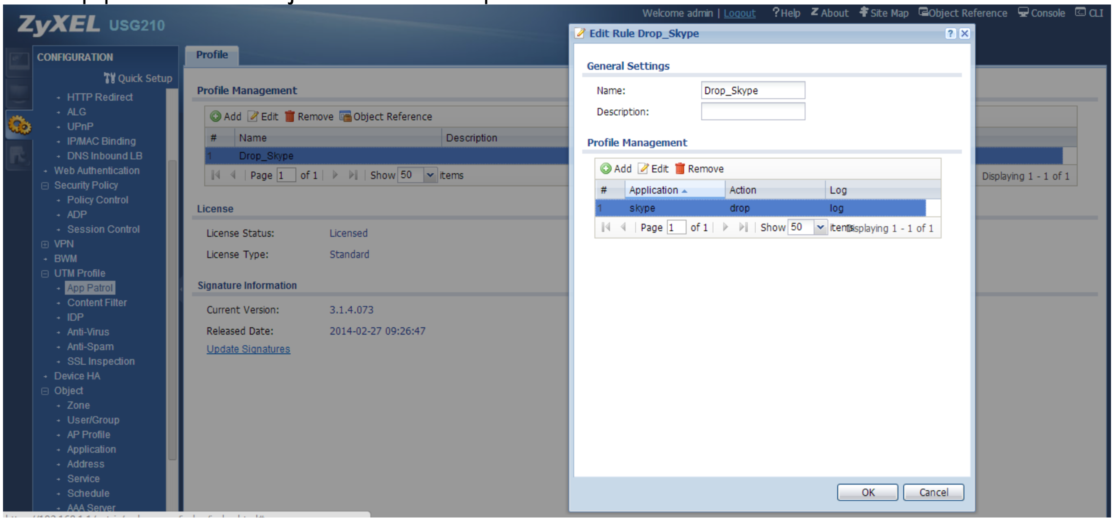
Description: New Create (Optional)

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

Displaying 1 - 3 of 3

(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.



Edit Rule Drop_Skype

General Settings

Name: Drop_Skype

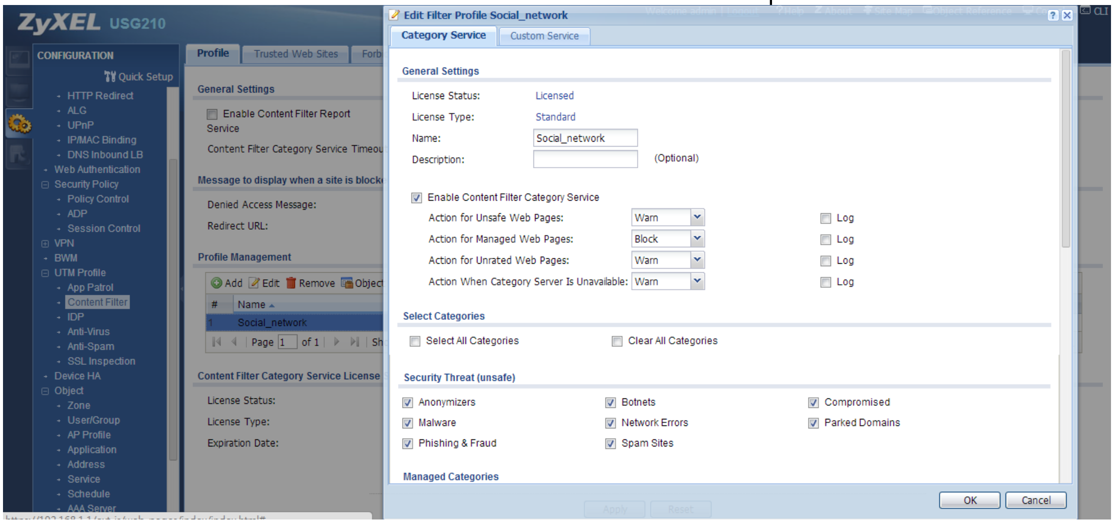
Description:

Profile Management

#	Application	Action	Log
1	skype	drop	log

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

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



Edit Filter Profile Social_network

Category Service | Custom Service

General Settings

License Status: Licensed

License Type: Standard

Name: Social_network

Description: (Optional)

☑ 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

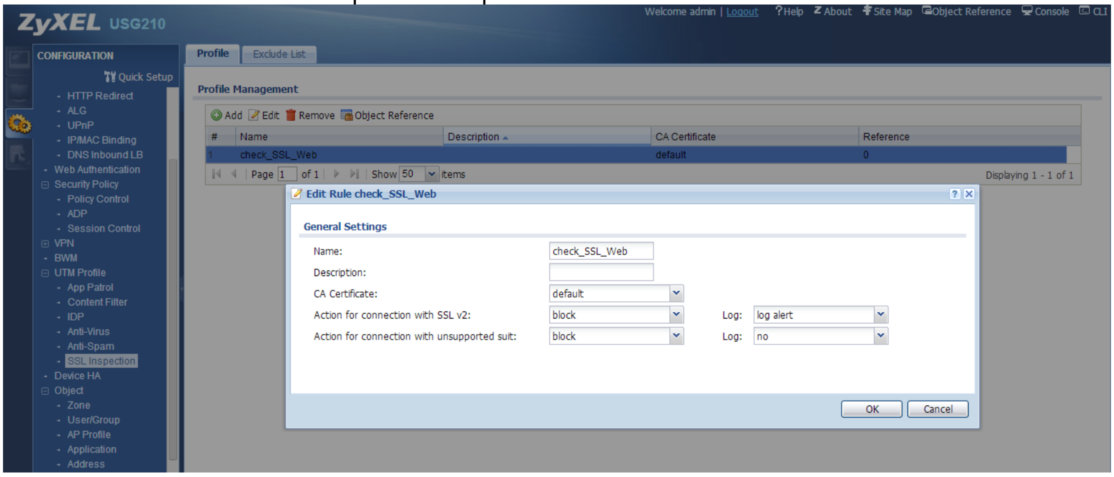
Security Threat (unsafe)

☑ Anonymizers	☑ Botnets	☑ Compromised
☑ Malware	☑ Network Errors	☑ Parked Domains
☑ Phishing & Fraud	☑ Spam Sites	

Managed Categories

(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.



Profile Management

#	Name	Description	CA Certificate	Reference
1	check_SSL_Web		default	0

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

Edit Rule check_SSL_Web

General Settings

Name: check_SSL_Web

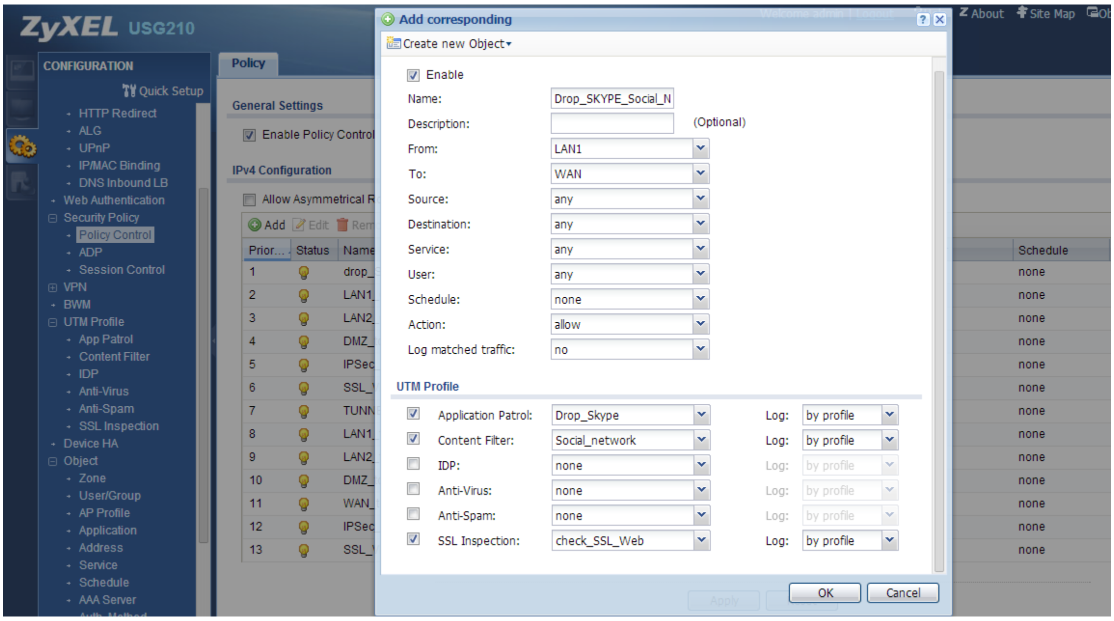
Description:

CA Certificate: default

Action for connection with SSL v2: block Log: log alert

Action for connection with unsupported suit: block Log: no

(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.



Add corresponding

☑ Enable

Name: Drop_SKYPE_Social_N

Description: (Optional)

From: LAN1

To: WAN

Source: any

Destination: any

Service: any

User: any

Schedule: none

Action: allow

Log matched traffic: no

UTM Profile

☑	Application Patrol:	Drop_Skype	Log:	by profile
☑	Content Filter:	Social_network	Log:	by profile
□	IDP:	none	Log:	by profile
□	Anti-Virus:	none	Log:	by profile
□	Anti-Spam:	none	Log:	by profile
☑	SSL Inspection:	check_SSL_Web	Log:	by profile

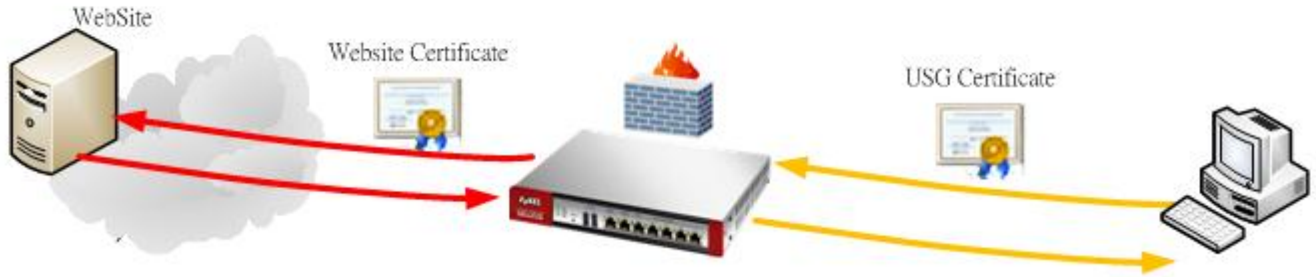
After configuring these rule, then you can drop Skype and all of the social networks successfully.

Scenario 9 – 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.



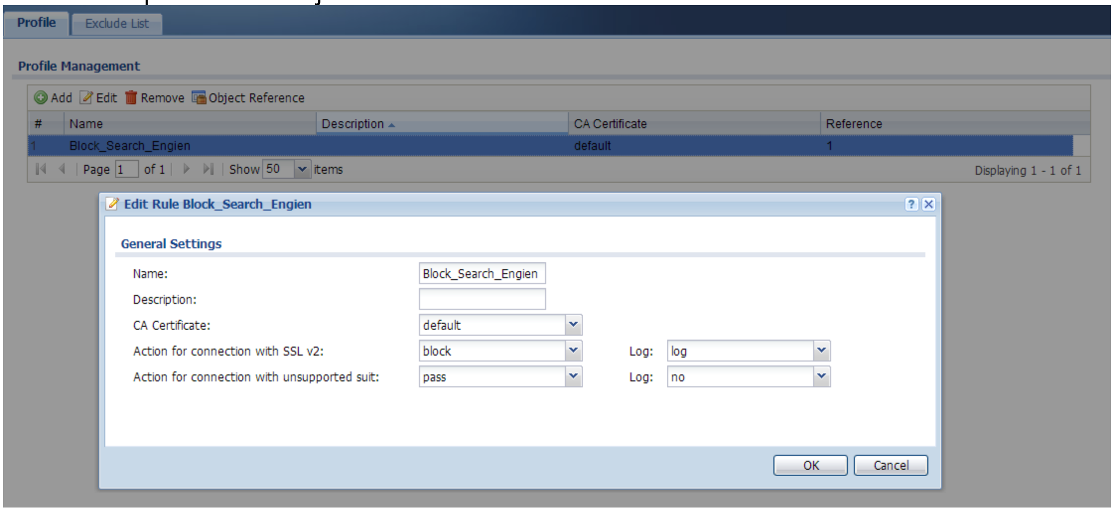
After using the SSL inspect function, HTTPs traffic can detect it well by the Content Filter function.

9.1 Application Scenario

Block the search engine in the internal website.

9.2 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.



Profile Management

#	Name	Description	CA Certificate	Reference
1	Block_Search_Engien		default	1

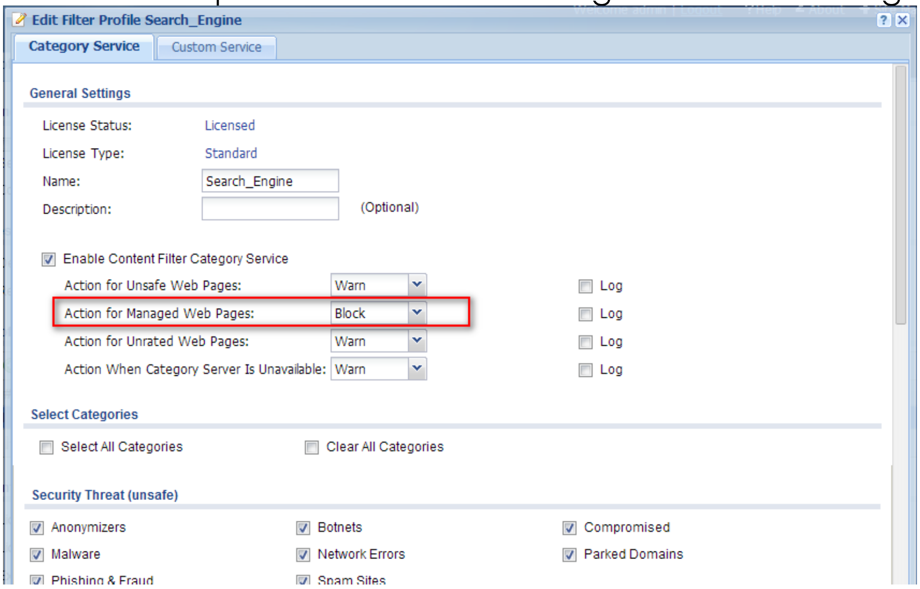
Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Edit Rule Block_Search_Engien

General Settings

Name: Block_Search_Engien
Description:
CA Certificate: default
Action for connection with SSL v2: block Log: log
Action for connection with unsupported suit: pass Log: no

(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".



Edit Filter Profile Search_Engine

General Settings

License Status: Licensed
License Type: Standard
Name: Search_Engine
Description: (Optional)

☑ 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

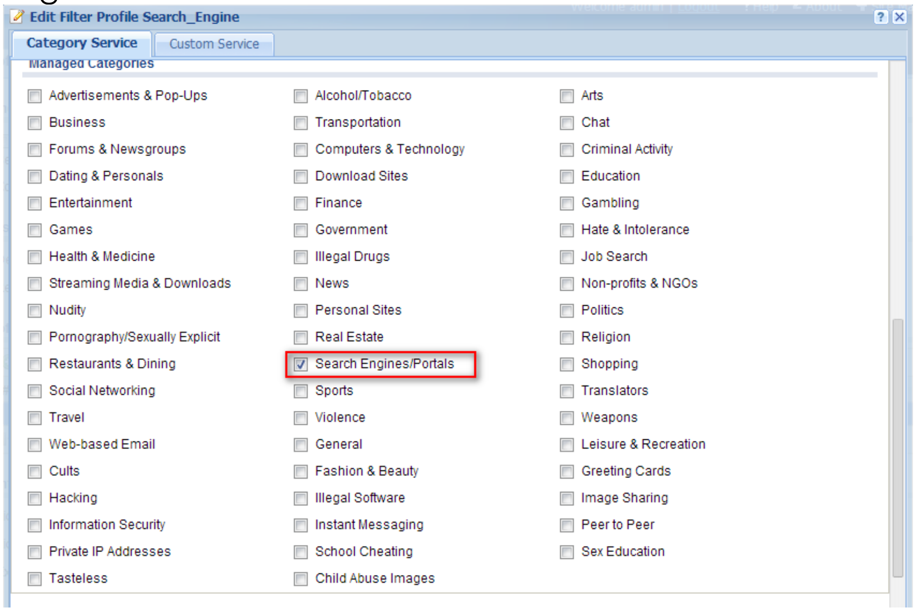
Select Categories

□ Select All Categories □ Clear All Categories

Security Threat (unsafe)

☑ Anonymizers ☑ Botnets ☑ Compromised
☑ Malware ☑ Network Errors ☑ Parked Domains
☑ Phishing & Fraud ☑ Spam Sites

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



Edit Filter Profile Search_Engine

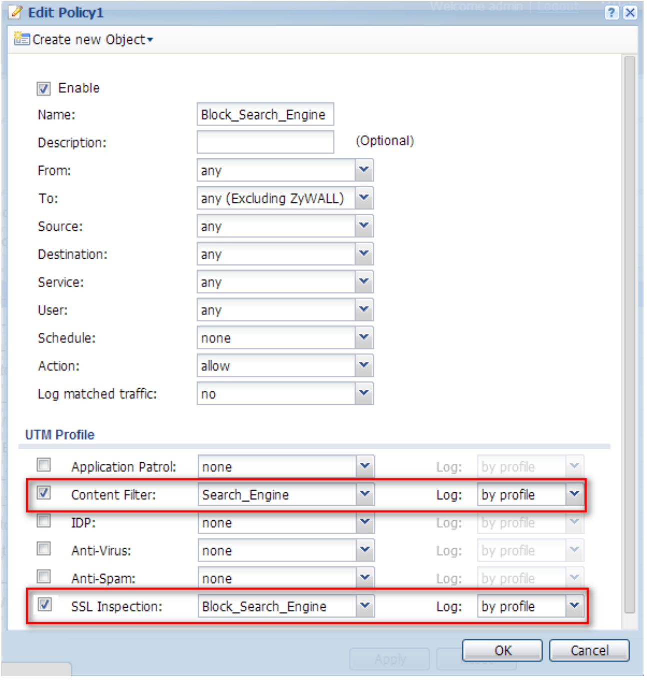
Managed Categories

□ Advertisements & Pop-Ups
□ Business
□ Forums & Newsgroups
□ Dating & Personals
□ Entertainment
□ Games
□ Health & Medicine
□ Streaming Media & Downloads
□ Nudity
□ Pornography/Sexually Explicit
□ Restaurants & Dining
□ Social Networking
□ Travel
□ Web-based Email
□ Cults
□ Hacking
□ Information Security
□ Private IP Addresses
□ Tasteless

□ Alcohol/Tobacco
□ Transportation
□ Computers & Technology
□ Download Sites
□ Finance
□ Government
□ Illegal Drugs
□ News
□ Personal Sites
□ Real Estate
☑ Search Engines/Portals
□ Sports
□ Violence
□ General
□ Fashion & Beauty
□ Illegal Software
□ Instant Messaging
□ School Cheating
□ Child Abuse Images

□ Arts
□ Chat
□ Criminal Activity
□ Education
□ Gambling
□ Hate & Intolerance
□ Job Search
□ Non-profits & NGOs
□ Politics
□ Religion
□ Shopping
□ Translators
□ Weapons
□ Leisure & Recreation
□ Greeting Cards
□ Image Sharing
□ Peer to Peer
□ Sex Education

(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

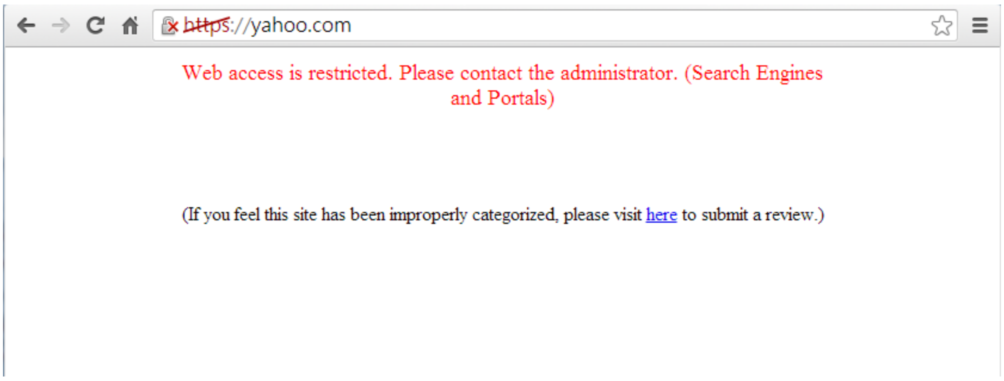
Action: allow

Log matched traffic: no

UTM Profile

□ Application Patrol:	none	Log:	by profile
☑ Content Filter:	Search_Engine	Log:	by profile
□ IDP:	none	Log:	by profile
□ Anti-Virus:	none	Log:	by profile
□ Anti-Spam:	none	Log:	by profile
☑ SSL Inspection:	Block_Search_Engine	Log:	by profile

Verification: Access to https:yahoo.com



~~https~~://yahoo.com

Web access is restricted. Please contact the administrator. (Search Engines and Portals)

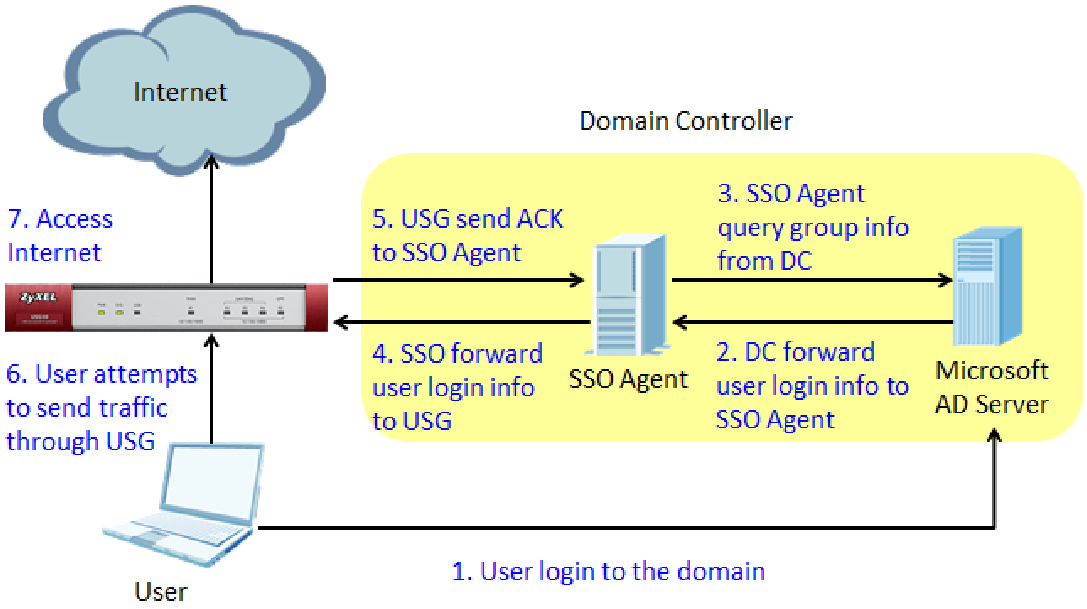
(If you feel this site has been improperly categorized, please visit here to submit a review.)

Scenario 10: Single Sign-on with USG and Windows

Platform

10.1 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. (SSO function support for USG110,210,310,1100 and 1900)


Internet
Domain Controller
7. Access Internet
5. USG send ACK to SSO Agent
3. SSO Agent query group info from DC
4. SSO forward user login info to USG
SSO Agent
2. DC forward user login info to SSO Agent
Microsoft AD Server
6. User attempts to send traffic through USG
User
1. User login to the domain

10.2 Configuration Guide

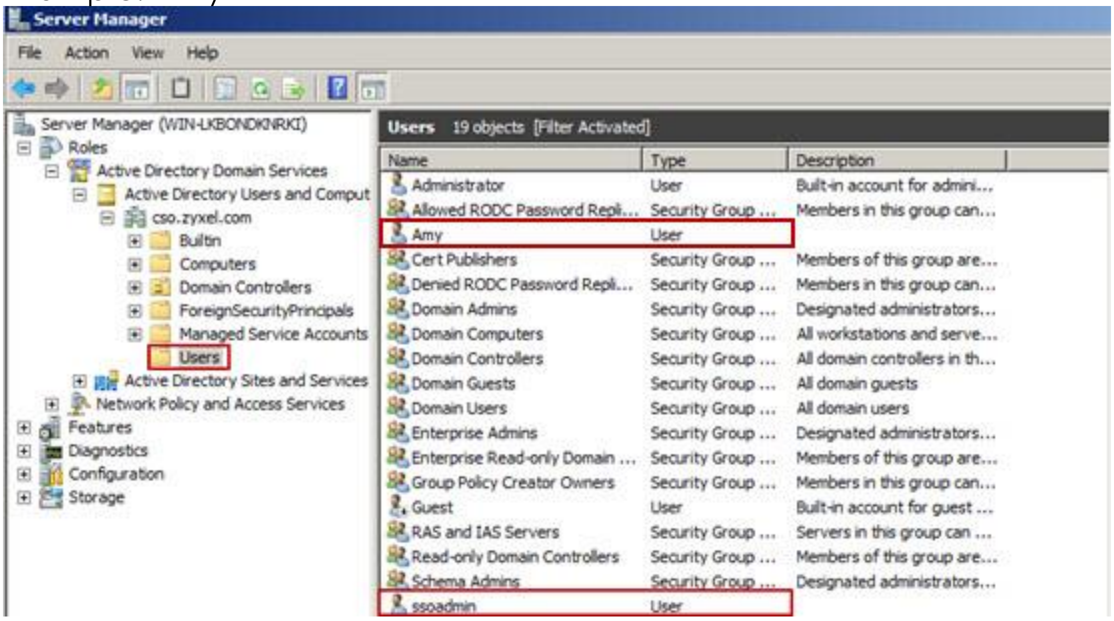
Network conditions
WAN: 59.124.163.151
LAN 1: 192.168.1.0/255.255.255.0
Domain Controller (Windows Server 2008 R2): 192.168.1.34
Client's laptop: 192.168.1.33

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

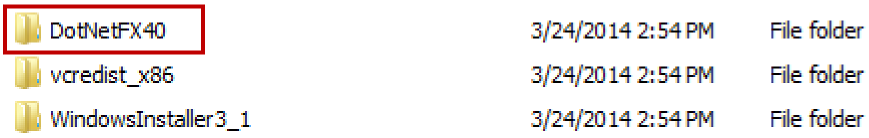

Server Manager
File
Action
View
Help
Server Manager (WIN-LKBONDKNRKI)
Roles
Active Directory Domain Services
Active Directory Users and Comput
cso.zyxel.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users
Active Directory Sites and Services
Network Policy and Access Services
Features
Diagnostics
Configuration
Storage

Users 19 objects [Filter Activated]

Name	Type	Description
Administrator	User	Built-in account for admini...
Allowed RODC Password Repli...	Security Group ...	Members in this group can...
Amy	User	
Cert Publishers	Security Group ...	Members of this group are...
Denied RODC Password Repli...	Security Group ...	Members in this group can...
Domain Admins	Security Group ...	Designated administrators...
Domain Computers	Security Group ...	All workstations and serve...
Domain Controllers	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Admins	Security Group ...	Designated administrators...
Enterprise Read-only Domain ...	Security Group ...	Members of this group are...
Group Policy Creator Owners	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
RAS and IAS Servers	Security Group ...	Servers in this group can ...
Read-only Domain Controllers	Security Group ...	Members of this group are...
Schema Admins	Security Group ...	Designated administrators...
ssoadmin	User	

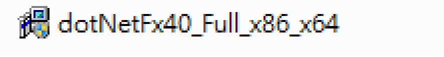
SSO Agent Installation

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

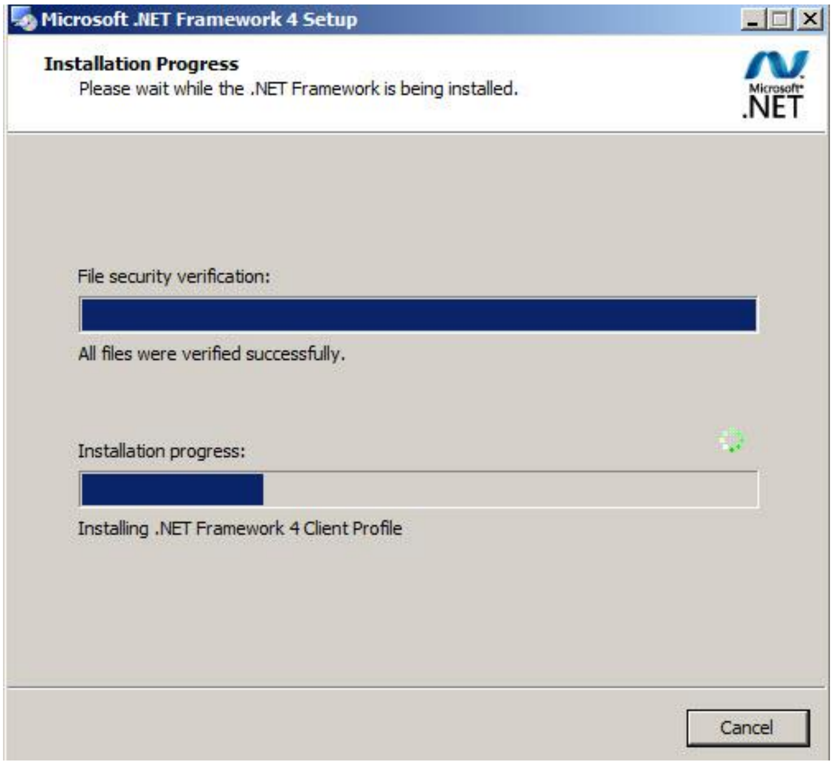


DotNetFX40	3/24/2014 2:54 PM	File folder
vcredist_x86	3/24/2014 2:54 PM	File folder
WindowsInstaller3_1	3/24/2014 2:54 PM	File folder

   Double click “dotNetFx40_Full_x86_x64.exe”.



dotNetFx40_Full_x86_x64



Installation Progress

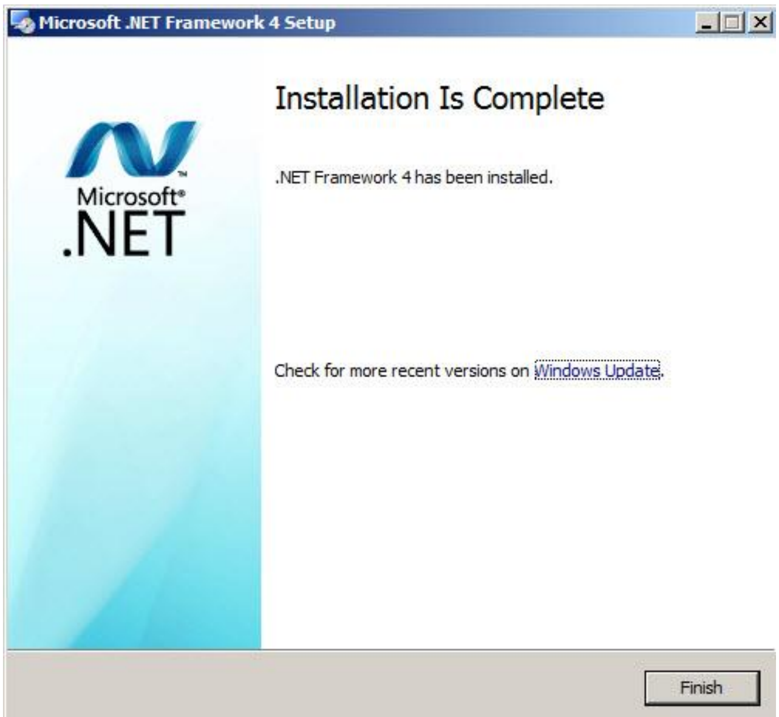
Please wait while the .NET Framework is being installed.

File security verification:

All files were verified successfully.

Installation progress:

Installing .NET Framework 4 Client Profile

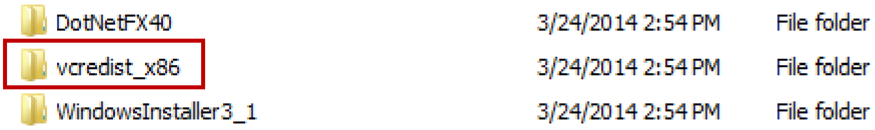


Installation Is Complete

.NET Framework 4 has been installed.

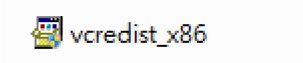
Check for more recent versions on Windows Update.

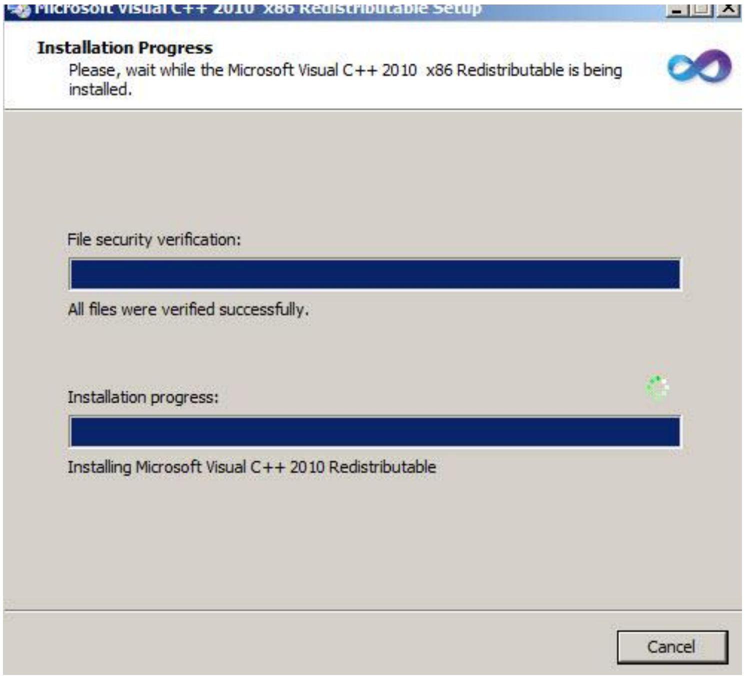
3. Install Visual C++



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”.




Microsoft Visual C++ 2010 x86 Redistributable Setup

Installation Progress

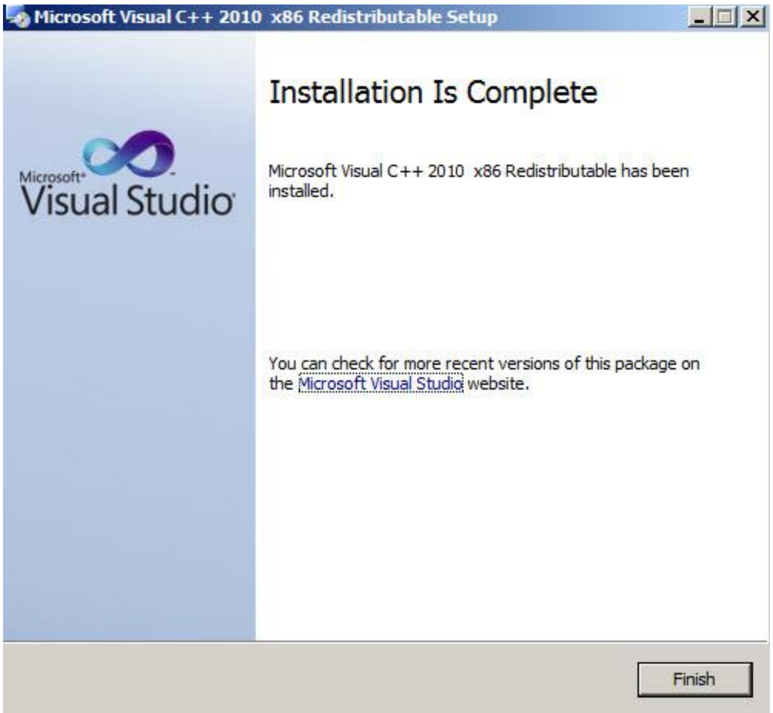
Please, wait while the Microsoft Visual C++ 2010 x86 Redistributable is being installed.

File security verification:

All files were verified successfully.

Installation progress:

Installing Microsoft Visual C++ 2010 Redistributable

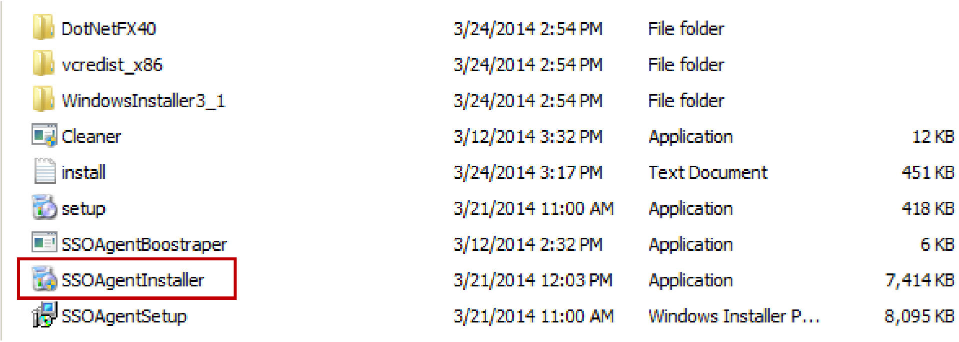

Microsoft Visual C++ 2010 x86 Redistributable Setup

Installation Is Complete

Microsoft Visual C++ 2010 x86 Redistributable has been installed.

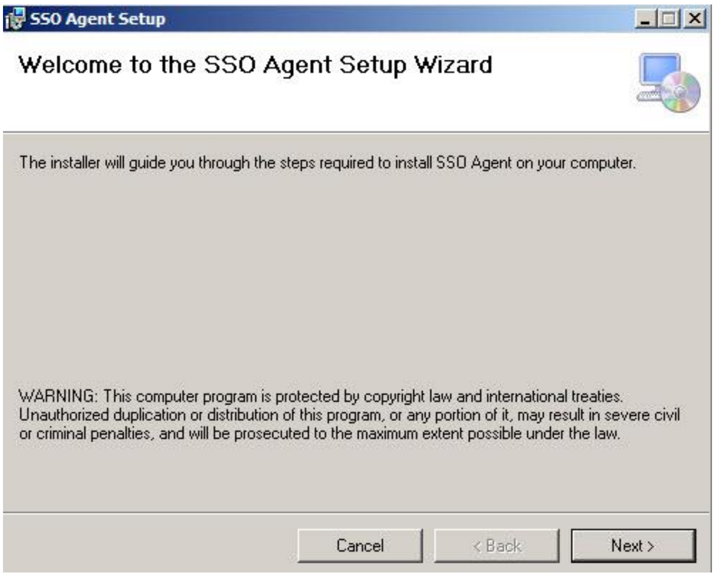
You can check for more recent versions of this package on the Microsoft Visual Studio website.

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.



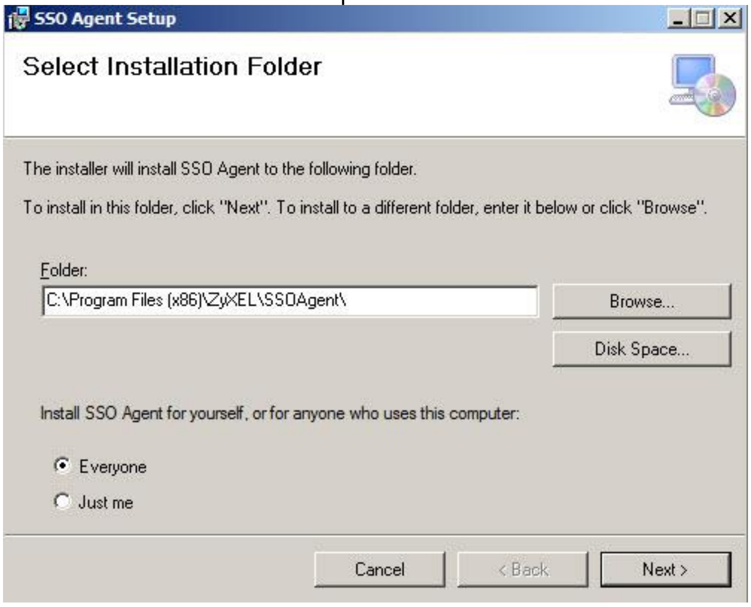
SSO Agent Setup

Welcome to the SSO Agent Setup Wizard

The installer will guide you through the steps required to install SSO Agent on your computer.

WARNING: This computer program is protected by copyright law and international treaties. Unauthorized duplication or distribution of this program, or any portion of it, may result in severe civil or criminal penalties, and will be prosecuted to the maximum extent possible under the law.

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



SSO Agent Setup

Select Installation Folder

The installer will install SSO Agent to the following folder.

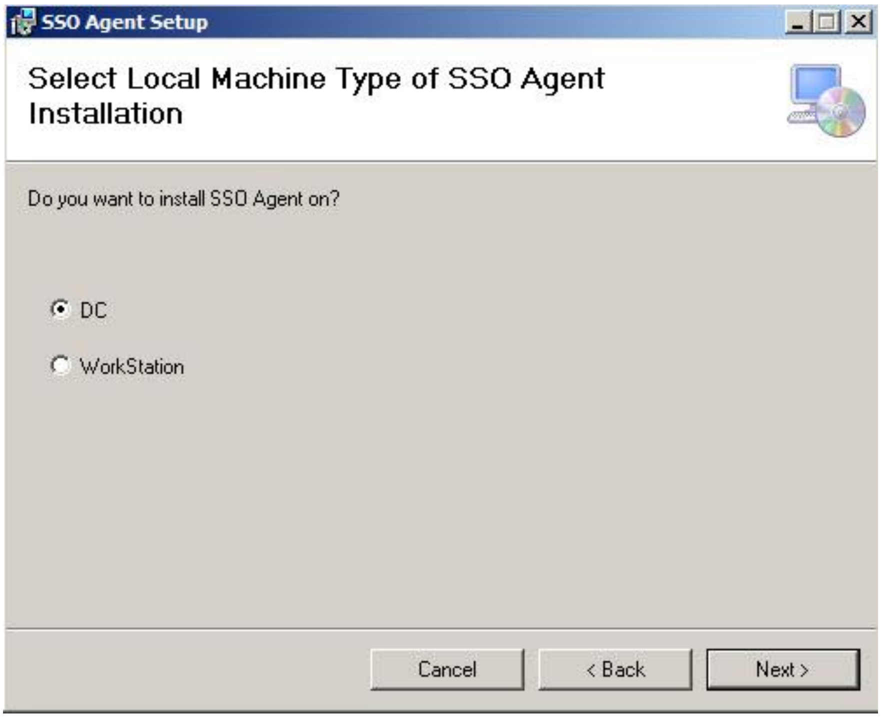
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder: C:\Program Files (x86)\ZyXEL\SSOAgent\

Install SSO Agent for yourself, or for anyone who uses this computer:

● Everyone
○ Just me

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



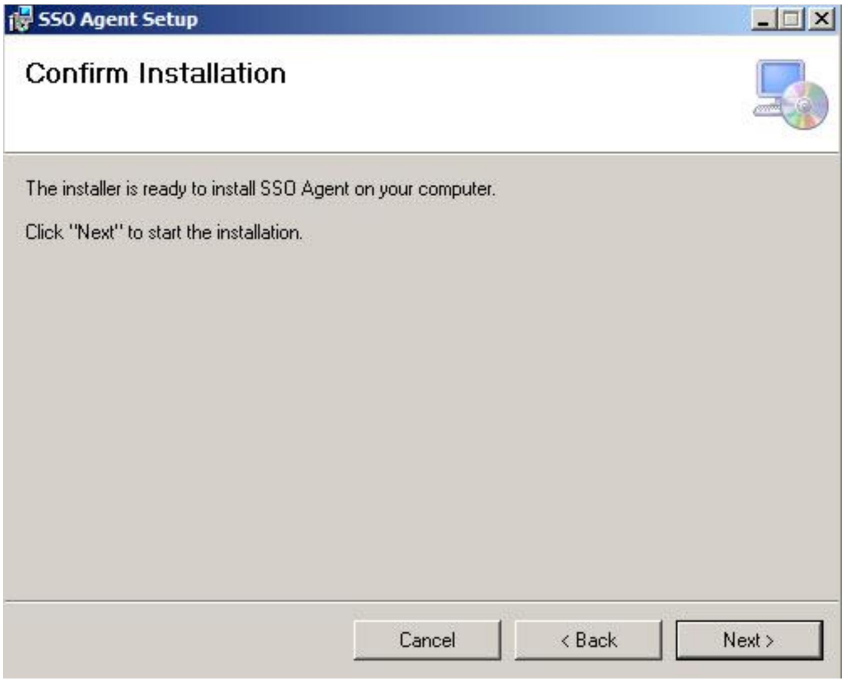
Select Local Machine Type of SSO Agent Installation

Do you want to install SSO Agent on?

● DC

○ WorkStation

Click on “Next” to start the installation.

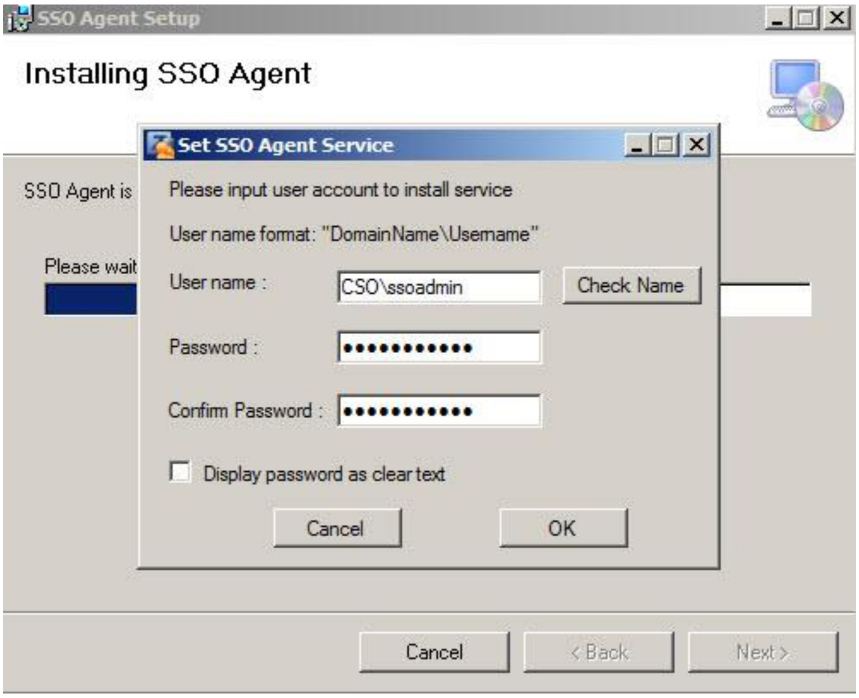


Confirm Installation

The installer is ready to install SSO Agent on your computer.

Click "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.



Please input user account to install service

User name format: "DomainName\Username"

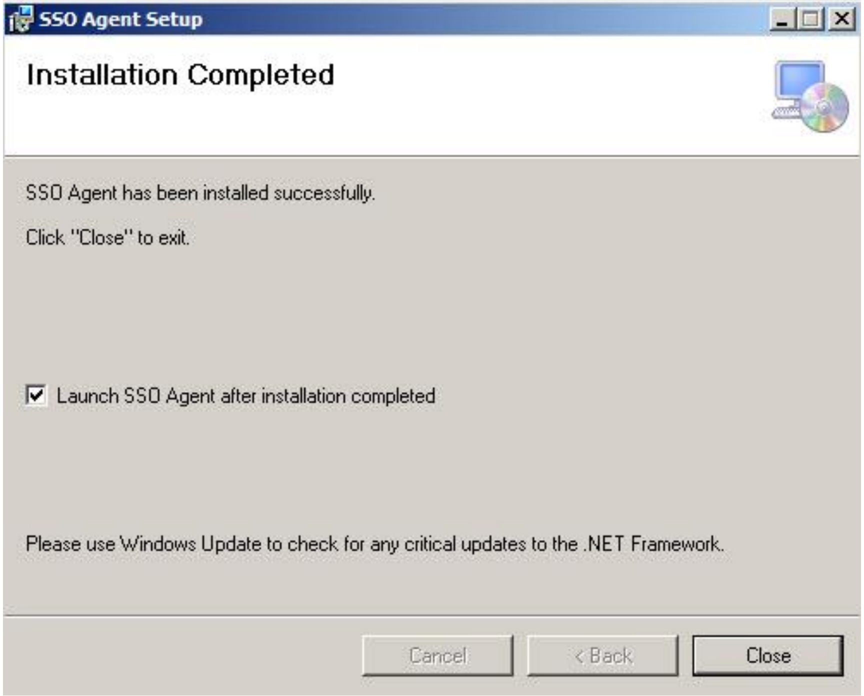
User name : CSO\ssoadmin

Password : ●●●●●●●●●●●

Confirm Password : ●●●●●●●●●●●

□ Display password as clear text

SSO Agent is installed successfully.



SSO Agent has been installed successfully.

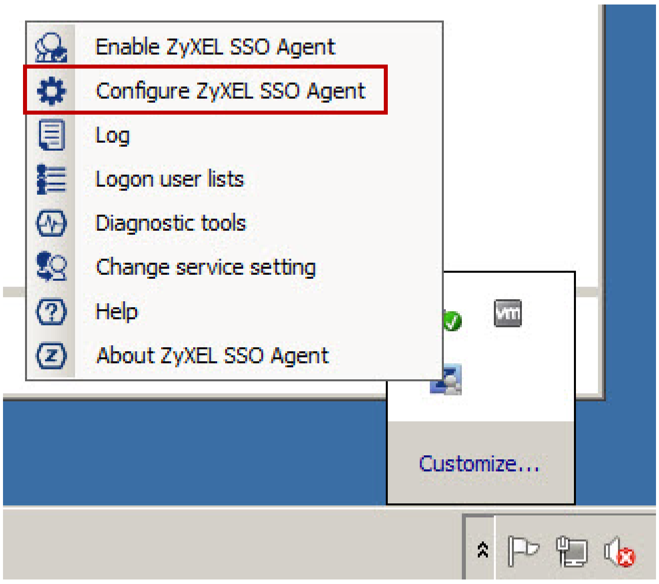
Click "Close" to exit.

☑ Launch SSO Agent after installation completed

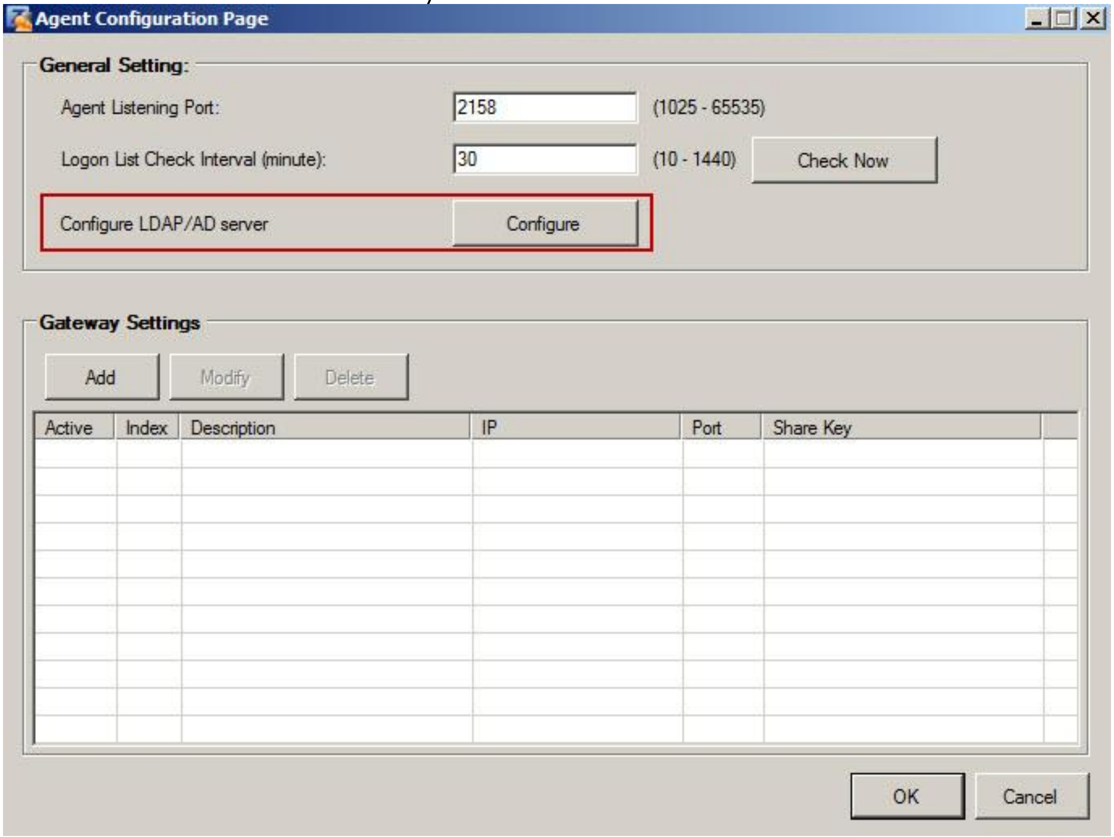
Please use Windows Update to check for any critical updates to the .NET Framework.

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.


Agent Configuration Page

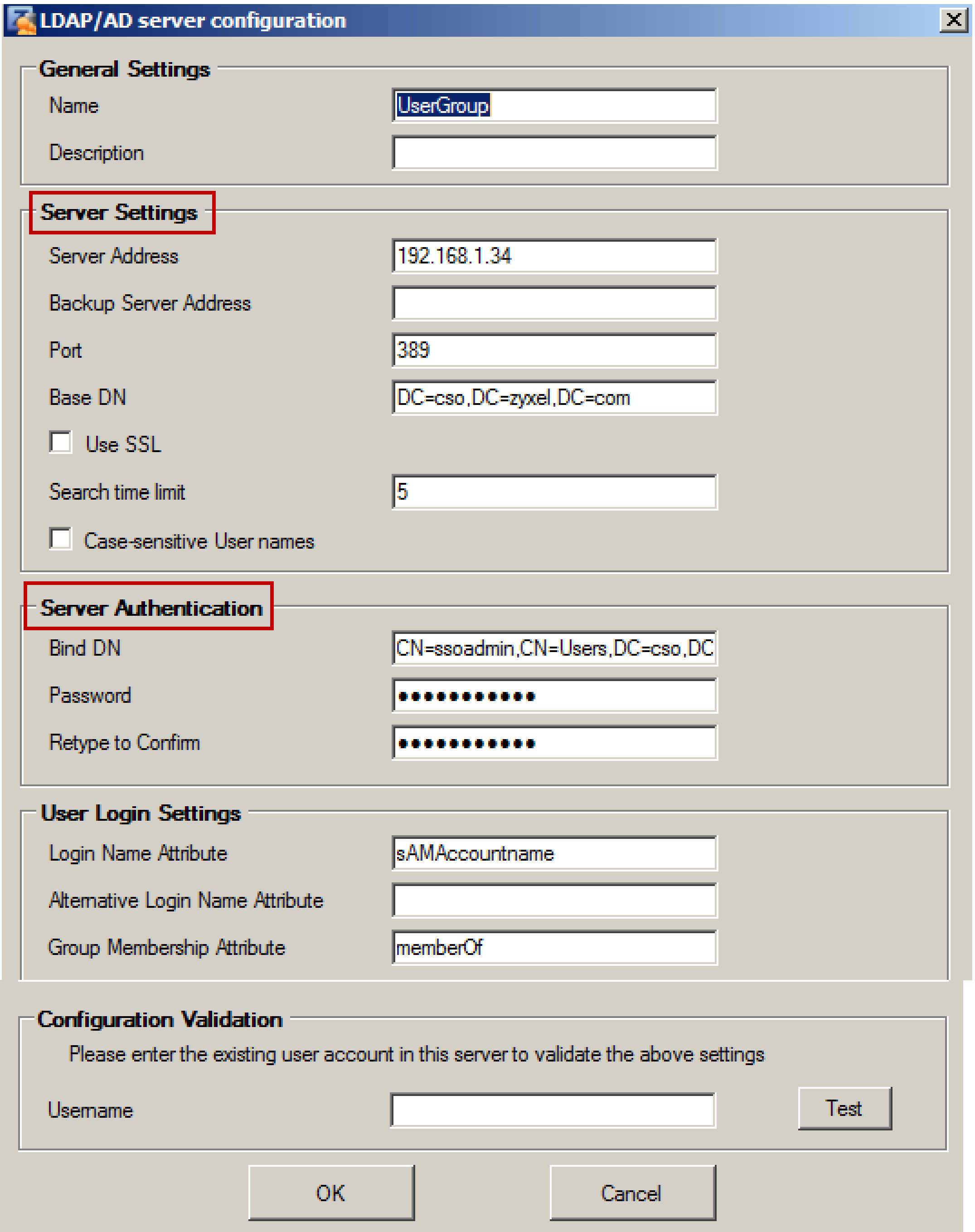
General Setting:

Agent Listening Port: 2158 (1025 - 65535)

Logon List Check Interval (minute): 30 (10 - 1440)

Active	Index	Description	IP	Port	Share Key

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



LDAP/AD server configuration

General Settings

Name: UserGroup

Description:

Server Settings

Server Address: 192.168.1.34

Backup Server Address:

Port: 389

Base DN: DC=cso,DC=zyxel,DC=com

☐ Use SSL

Search time limit: 5

☐ Case-sensitive User names

Server Authentication

Bind DN: CN=ssoadmin,CN=Users,DC=cso,DC

Password: ●●●●●●●●●●●

Retype to Confirm: ●●●●●●●●●●●

User Login Settings

Login Name Attribute: sAMAccountname

Alternative Login Name Attribute:

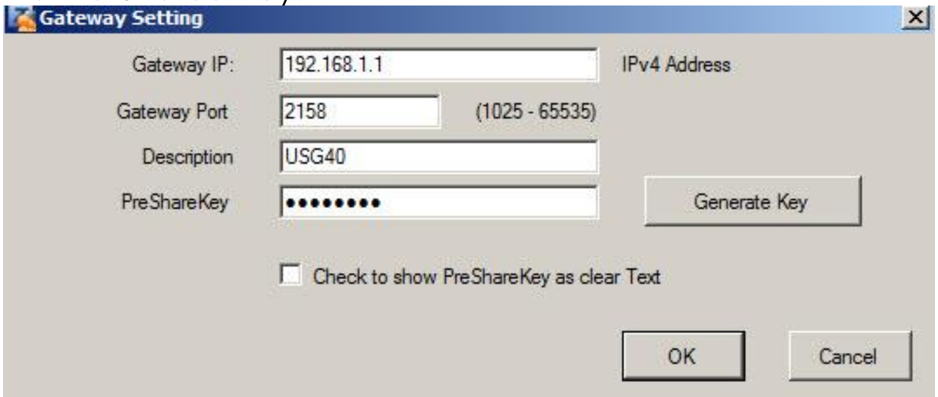
Group Membership Attribute: memberOf

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: 192.168.1.1 IPv4 Address

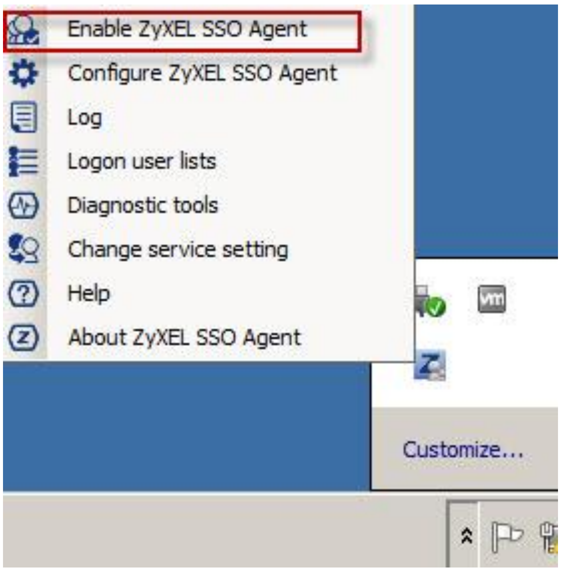
Gateway Port: 2158 (1025 - 65535)

Description: USG40

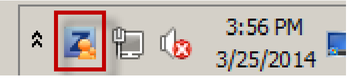
PreShareKey: ●●●●●●●●

☐ Check to show PreShareKey as clear Text

Enable SSO service.

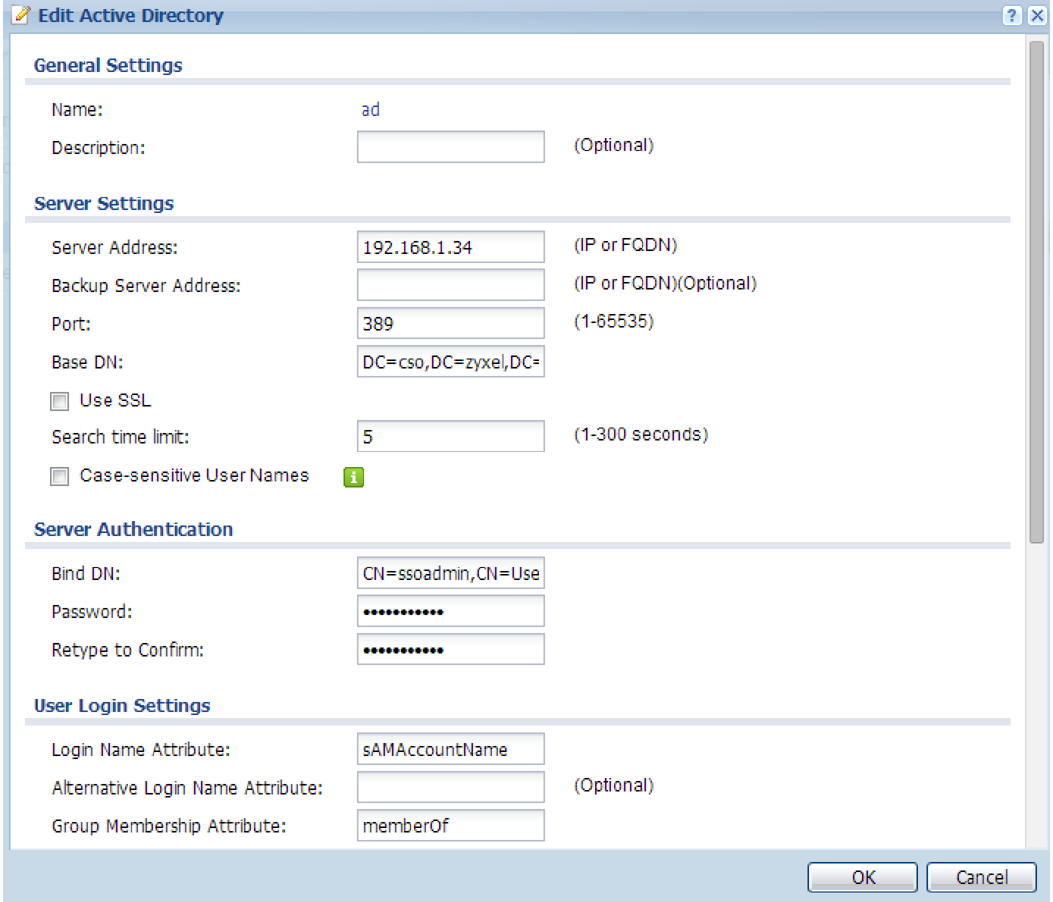


When the SSO service is started successfully, the icon is enabled.



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**".



Edit Active Directory

General Settings

Name:	ad	
Description:		(Optional)

Server Settings

Server Address:	192.168.1.34	(IP or FQDN)
Backup Server Address:		(IP or FQDN)(Optional)
Port:	389	(1-65535)
Base DN:	DC=cso,DC=zyxel,DC=	
□ Use SSL		
Search time limit:	5	(1-300 seconds)
□ Case-sensitive User Names		

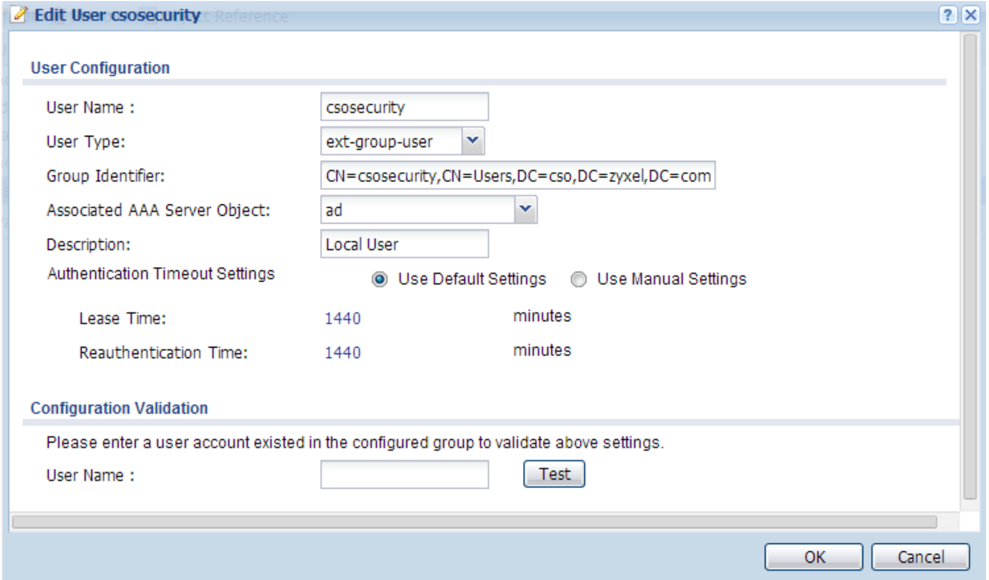
Server Authentication

Bind DN:	CN=ssoadmin,CN=Use
Password:	•••••••••••
Retype to Confirm:	•••••••••••

User Login Settings

Login Name Attribute:	sAMAccountName	
Alternative Login Name Attribute:		(Optional)
Group Membership Attribute:	memberOf	

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.



Edit User csosecurity

User Configuration

User Name :	csosecurity
User Type:	ext-group-user
Group Identifier:	CN=csosecurity,CN=Users,DC=cso,DC=zyxel,DC=com
Associated AAA Server Object:	ad
Description:	Local User
Authentication Timeout Settings	● Use Default Settings ○ Use Manual Settings
Lease Time:	1440 minutes
Reauthentication Time:	1440 minutes

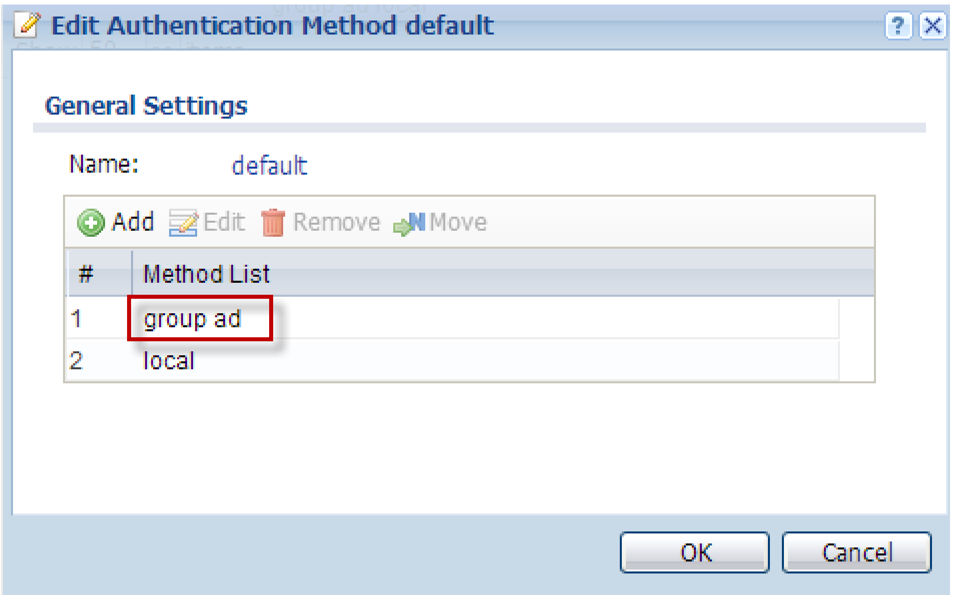
Configuration Validation

Please enter a user account existed in the configured group to validate above settings.

User Name : Test

OK Cancel

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



Edit Authentication Method default

General Settings

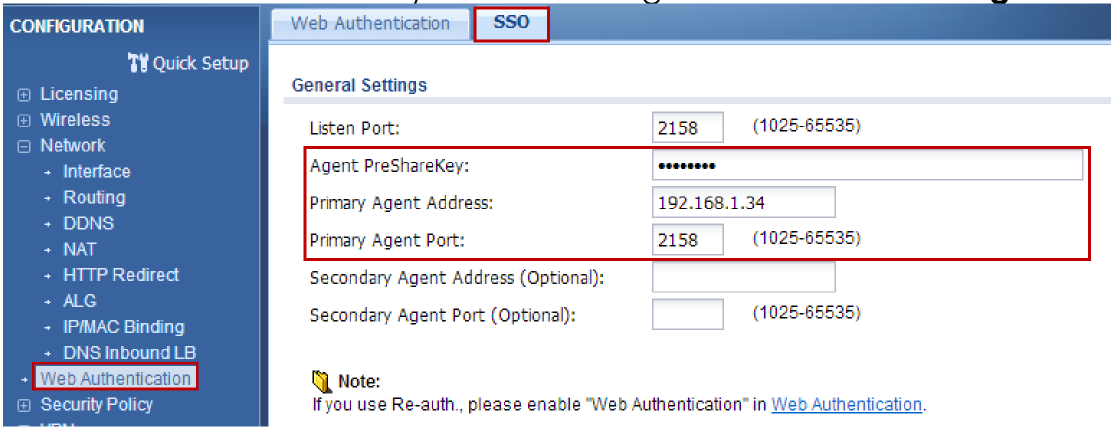
Name: default

Add Edit Remove Move

#	Method List
1	group ad
2	local

OK Cancel

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

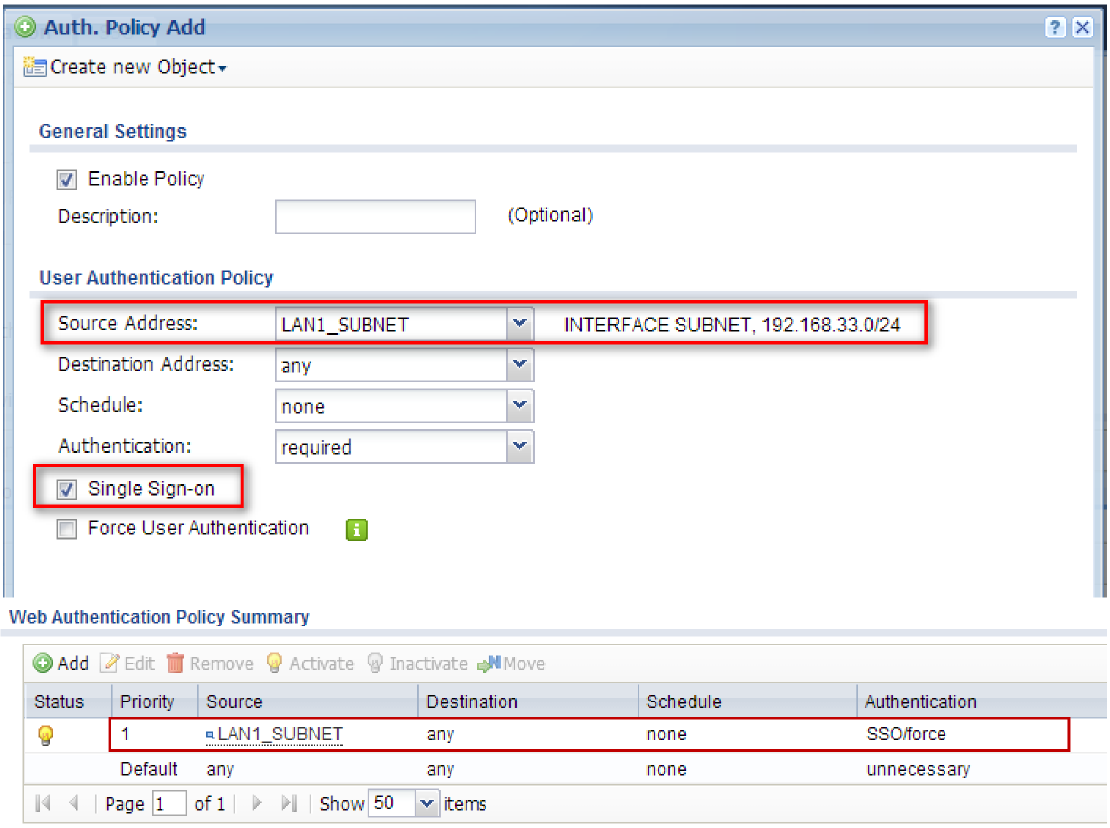


General Settings

Listen Port:	2158	(1025-65535)
Agent PreShareKey:	••••••••	
Primary Agent Address:	192.168.1.34	
Primary Agent Port:	2158	(1025-65535)
Secondary Agent Address (Optional):		
Secondary Agent Port (Optional):		(1025-65535)

Note:
If you use Re-auth., please enable "Web Authentication" in Web Authentication.

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 Add

General Settings

☑ Enable Policy

Description: (Optional)

User Authentication Policy

Source Address: LAN1_SUBNET INTERFACE SUBNET, 192.168.33.0/24

Destination Address: any

Schedule: none

Authentication: required

☑ Single Sign-on

□ Force User Authentication

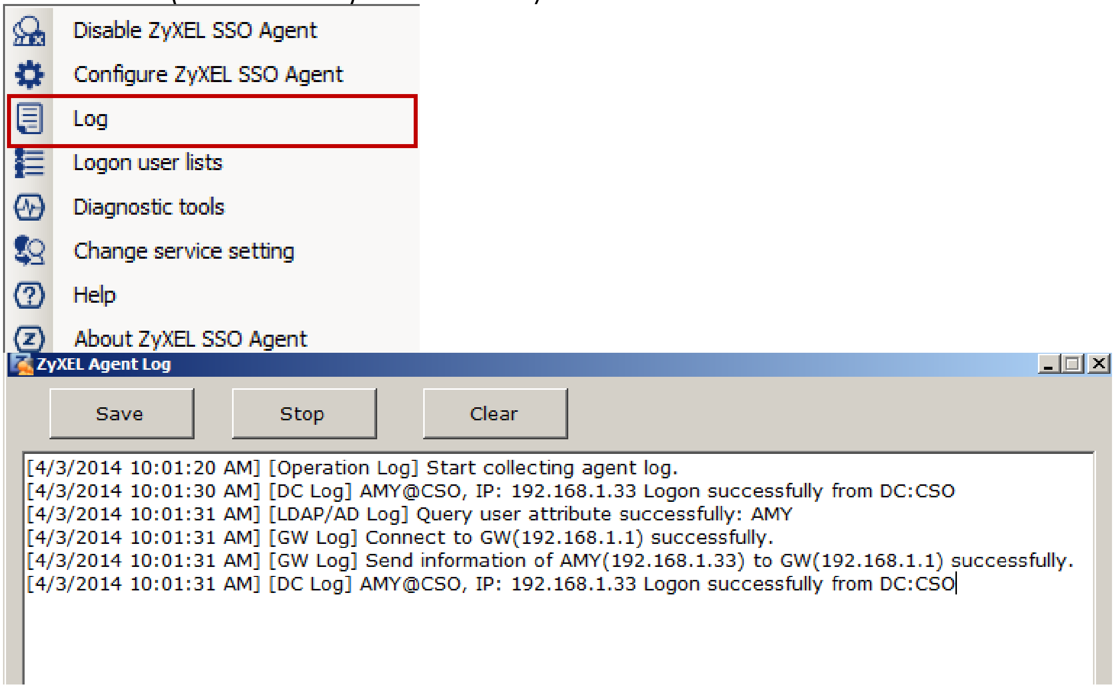
Web Authentication Policy Summary

Status	Priority	Source	Destination	Schedule	Authentication
💡	1	LAN1_SUBNET	any	none	SSO/force
	Default	any	any	none	unnecessary

Verification

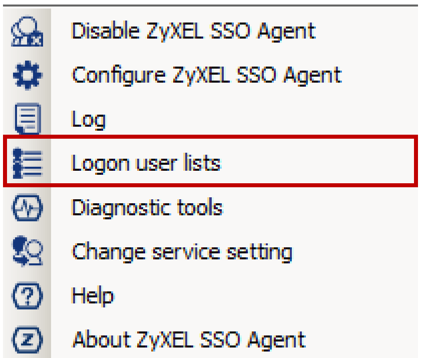
1. On the client's laptop, login using the domain account "Amy".
   Example: CSO\Amy
   Open the browser or application on the client's laptop to trigger traffic to pass to the USG. The client “Amy” can surf the Internet directly without extra authentication.

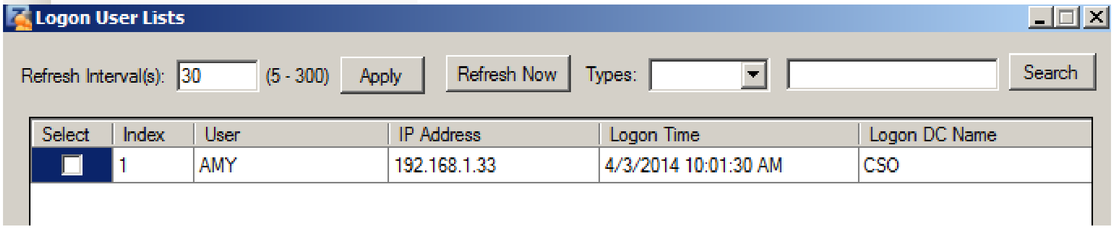
2. Check SSO Agent Log. User login is successful and has sent information to the USG’s GW (192.168.1.1) successfully.



```
[4/3/2014 10:01:20 AM] [Operation Log] Start collecting agent log.
[4/3/2014 10:01:30 AM] [DC Log] AMY@CSO, IP: 192.168.1.33 Logon successfully from DC:CSO
[4/3/2014 10:01:31 AM] [LDAP/AD Log] Query user attribute successfully: AMY
[4/3/2014 10:01:31 AM] [GW Log] Connect to GW(192.168.1.1) successfully.
[4/3/2014 10:01:31 AM] [GW Log] Send information of AMY(192.168.1.33) to GW(192.168.1.1) successfully.
[4/3/2014 10:01:31 AM] [DC Log] AMY@CSO, IP: 192.168.1.33 Logon successfully from DC:CSO
```

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

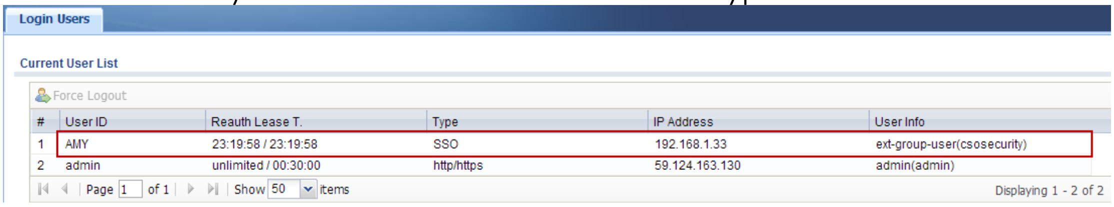




Refresh Interval(s): 30 (5 - 300) Types:

Select	Index	User	IP Address	Logon Time	Logon DC Name
□	1	AMY	192.168.1.33	4/3/2014 10:01:30 AM	CSO

4. Go to **MONITOR > System Status > Login Users**.
   The client "Amy" is on the current user list with type SSO.



Current User List

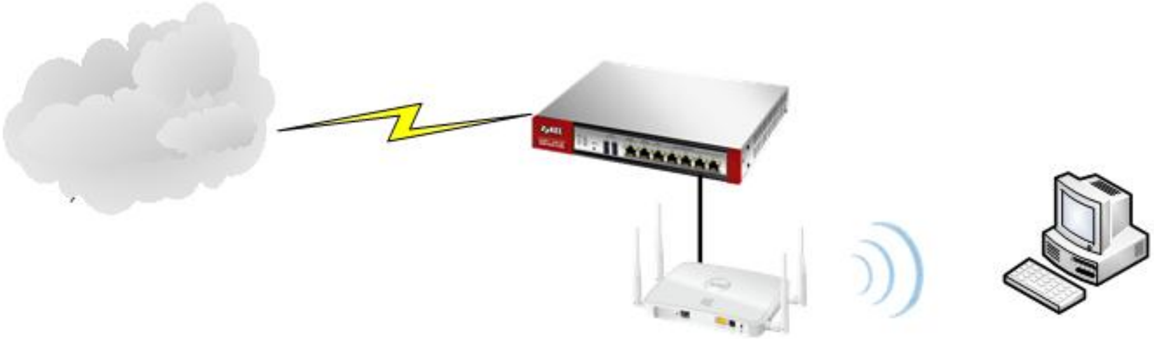
#	User ID	Reauth Lease T.	Type	IP Address	User Info
1	AMY	23:19:58 / 23:19:58	SSO	192.168.1.33	ext-group-user(csosecurity)
2	admin	unlimited / 00:30:00	http/https	59.124.163.130	admin(admin)

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

Scenario 11 – WLAN Controller Function on USG

11.1 Application Scenario

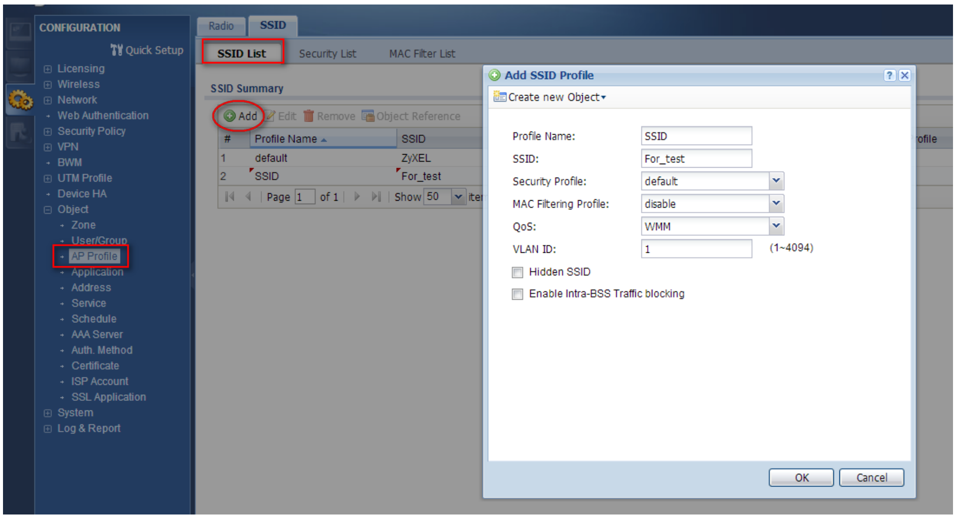
USG with 4.10 firmware supports the AP controller function.
You can follow the steps to control your AP device.



11.2 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.



SSID Summary

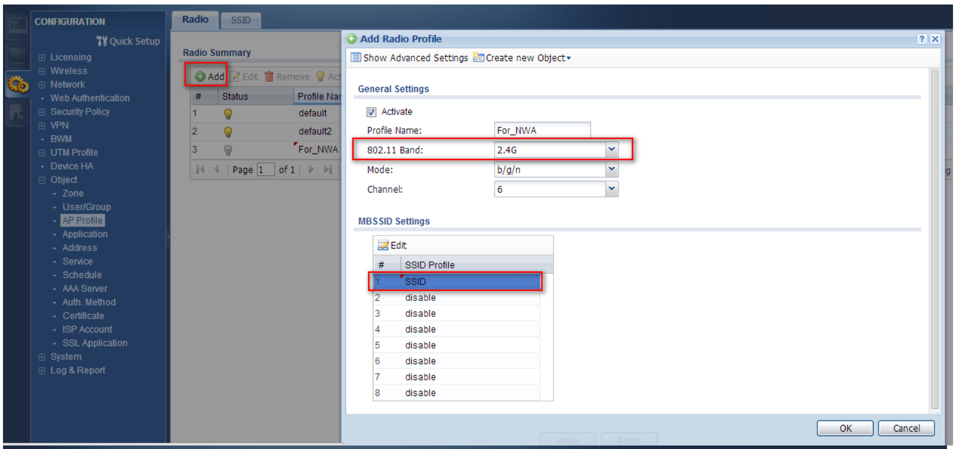
#	Profile Name	SSID
1	default	ZyXEL
2	SSID	For_test

Page 1 of 1 | Show 50 items

Add SSID Profile

Profile Name: SSID
SSID: For_test
Security Profile: default
MAC Filtering Profile: disable
QoS: WMM
VLAN ID: 1 (1~4094)
□ Hidden SSID
□ Enable Intra-BSS Traffic blocking

(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.



Add Radio Profile

General Settings

☑ Activate

Profile Name: For_NWA

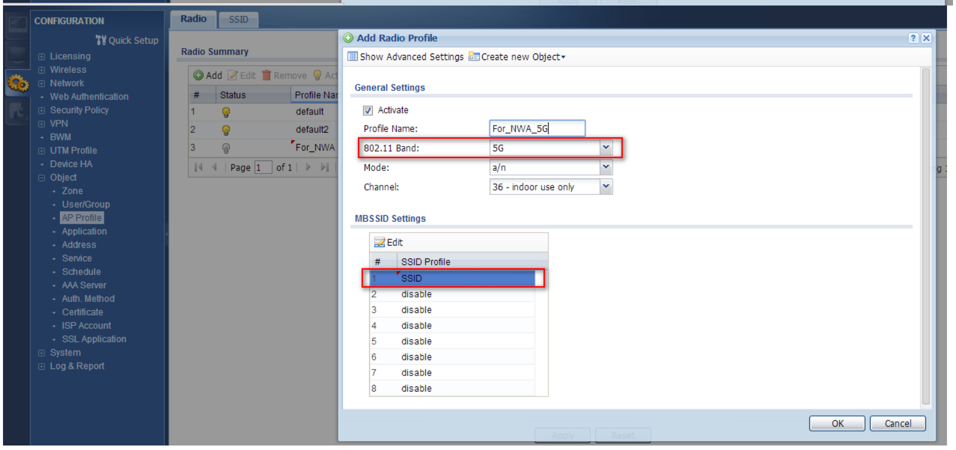
802.11 Band: 2.4G

Mode: b/g/n

Channel: 6

MBSSID Settings

#	SSID Profile
1	SSID
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable



Add Radio Profile

General Settings

☑ Activate

Profile Name: For_NWA_5G

802.11 Band: 5G

Mode: a/n

Channel: 36 - indoor use only

MBSSID Settings

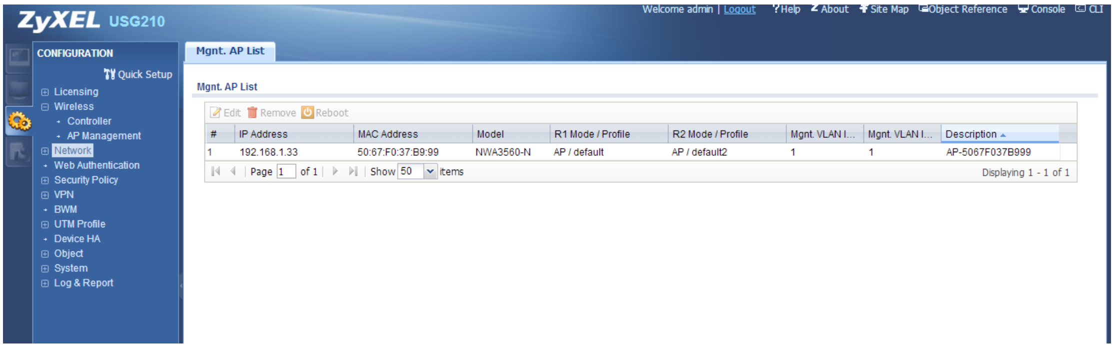
#	SSID Profile
1	SSID
2	disable
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

(3) Connect your AP to the LAN interface (this document is using NWA 3560-N to test).

a. The AP must be set as managed mode.

b. 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.

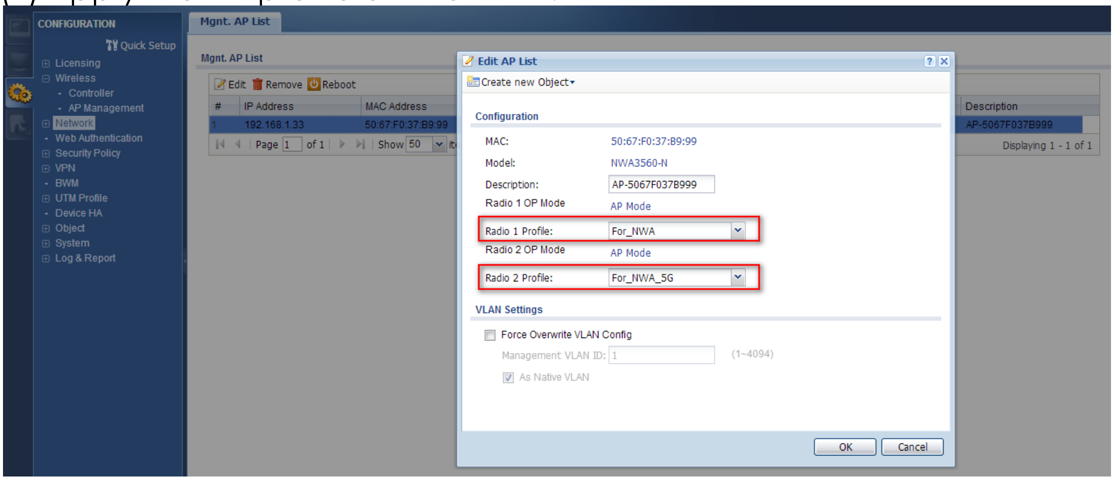


Mgnt. AP List

#	IP Address	MAC Address	Model	R1 Mode / Profile	R2 Mode / Profile	Mgnt. VLAN I...	Mgnt. VLAN I...	Description
1	192.168.1.33	50:67:F0:37:B9:99	NWA3560-N	AP / default	AP / default2	1	1	AP-5067F037B999

Displaying 1 - 1 of 1

(4) Apply the AP profile on the NWA.



Edit AP List

Configuration

MAC: 50:67:F0:37:B9:99

Model: NWA3560-N

Description: AP-5067F037B999

Radio 1 OP Mode: AP Mode

Radio 1 Profile: For_NWA

Radio 2 OP Mode: AP Mode

Radio 2 Profile: For_NWA_5G

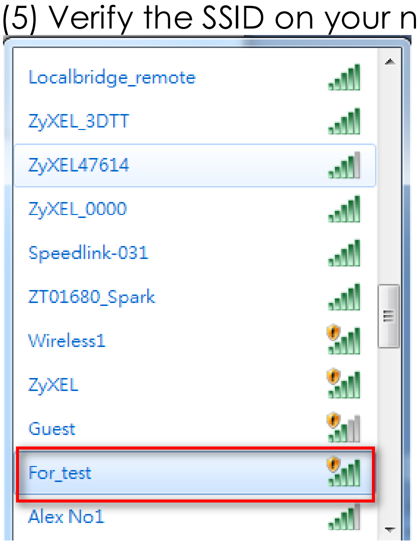
VLAN Settings

□ Force Overwrite VLAN Config

Management VLAN ID: 1 (1~4094)

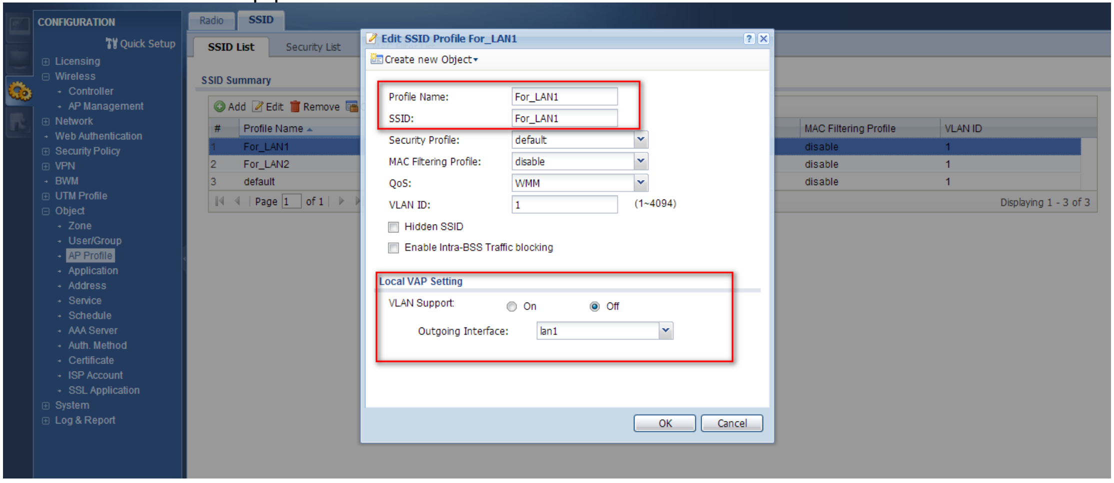
☑ As Native VLAN

(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**.



Edit SSID Profile For_LAN1

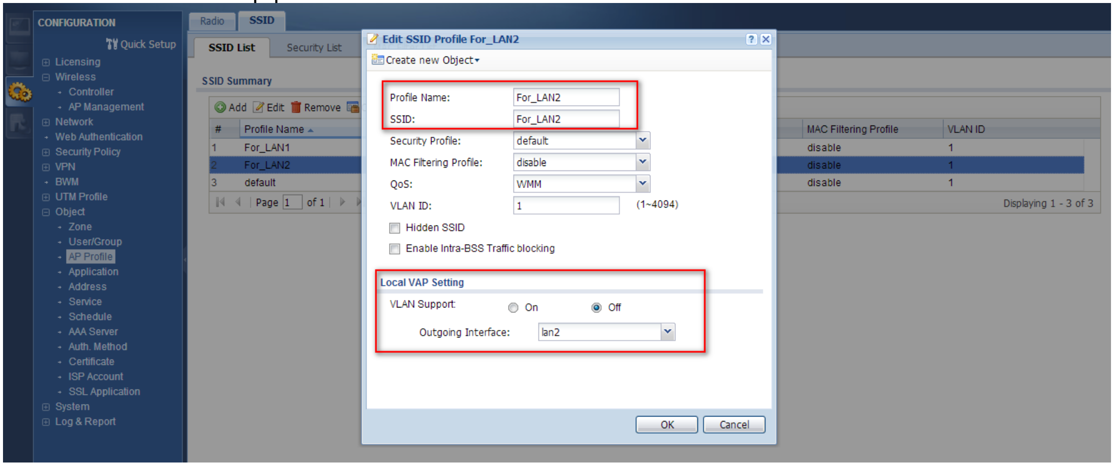
#	Profile Name	MAC Filtering Profile	VLAN ID
1	For_LAN1	disable	1
2	For_LAN2	disable	1
3	default	disable	1

Page 1 of 1 · Displaying 1 - 3 of 3

Profile Name: For_LAN1
SSID: For_LAN1
Security Profile: default
MAC Filtering Profile: disable
QoS: WMM
VLAN ID: 1 (1~4094)
□ Hidden SSID
□ Enable Intra-BSS Traffic blocking

Local VAP Setting
VLAN Support: ○ On ● Off
Outgoing Interface: lan1

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



Edit SSID Profile For_LAN2

#	Profile Name	MAC Filtering Profile	VLAN ID
1	For_LAN1	disable	1
2	For_LAN2	disable	1
3	default	disable	1

Page 1 of 1 · Displaying 1 - 3 of 3

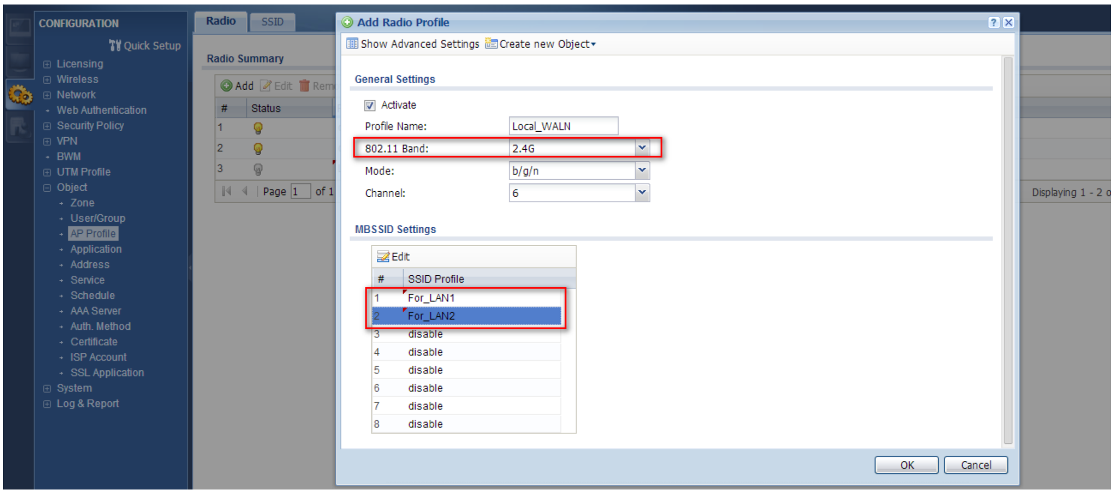
Profile Name: For_LAN2
SSID: For_LAN2
Security Profile: default
MAC Filtering Profile: disable
QoS: WMM
VLAN ID: 1 (1~4094)
□ Hidden SSID
□ Enable Intra-BSS Traffic blocking

Local VAP Setting
VLAN Support: ○ On ● Off
Outgoing Interface: lan2

(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



Add Radio Profile

General Settings

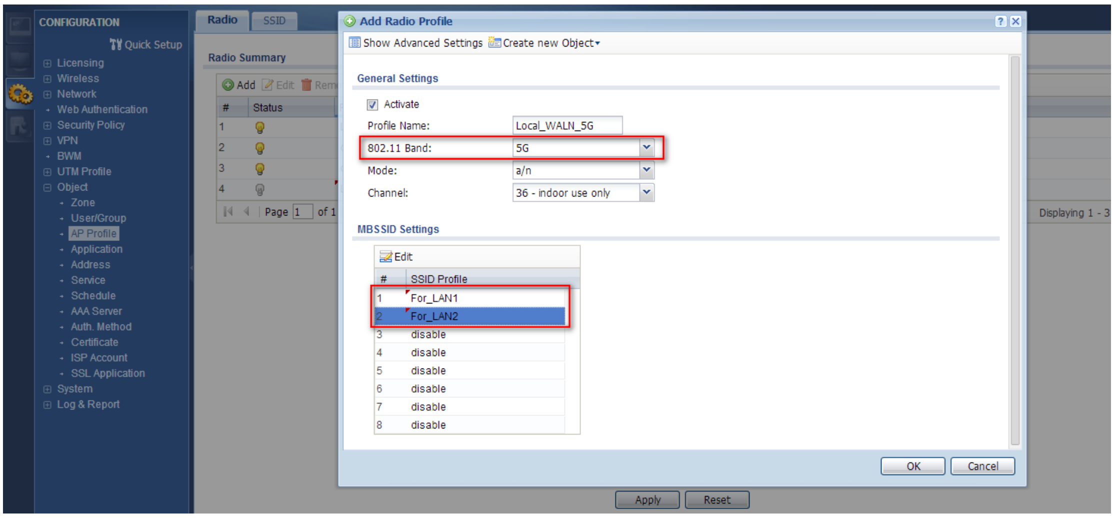
☑ Activate

Profile Name:	Local_WALN
802.11 Band:	2.4G
Mode:	b/g/n
Channel:	6

MBSSID Settings

#	SSID Profile
1	For_LAN1
2	For_LAN2
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

5G Band



Add Radio Profile

General Settings

☑ Activate

Profile Name:	Local_WALN_5G
802.11 Band:	5G
Mode:	a/n
Channel:	36 - indoor use only

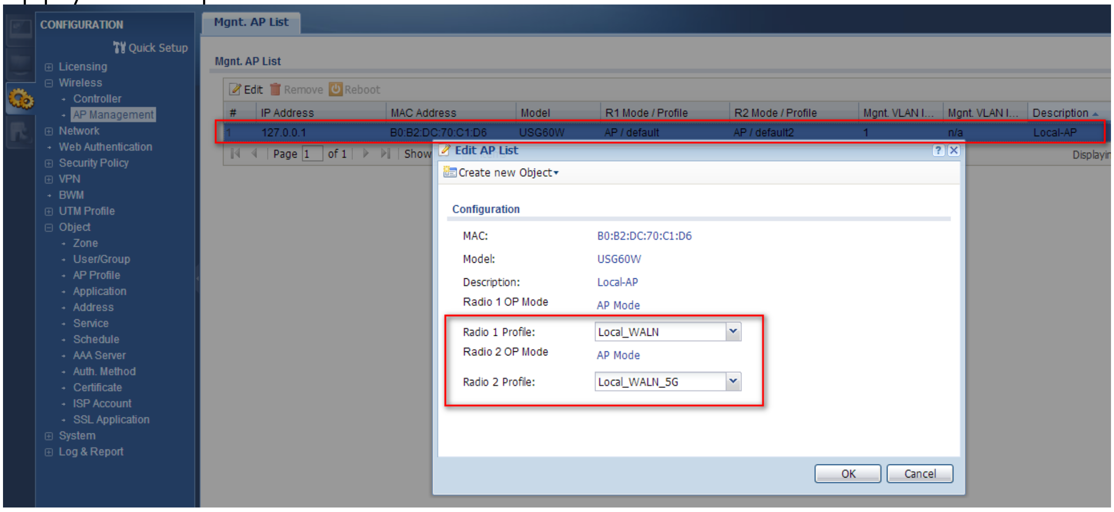
MBSSID Settings

#	SSID Profile
1	For_LAN1
2	For_LAN2
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

(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.



Mgnt. AP List

#	IP Address	MAC Address	Model	R1 Mode / Profile	R2 Mode / Profile	Mgnt. VLAN I...	Mgnt. VLAN I...	Description
1	127.0.0.1	B0:B2:DC:70:C1:D6	USG60W	AP / default	AP / default2	1	n/a	Local-AP

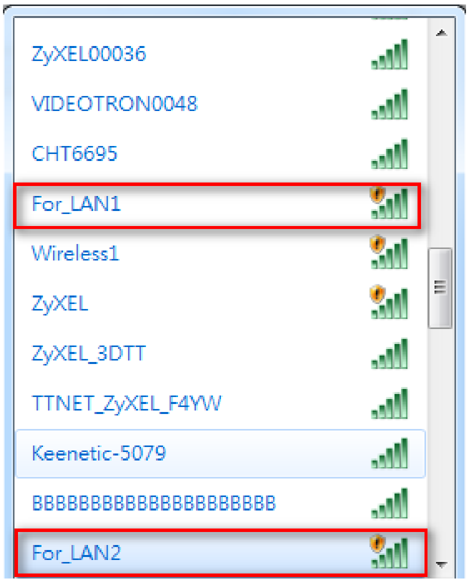
Edit AP List

Configuration

MAC:	B0:B2:DC:70:C1:D6
Model:	USG60W
Description:	Local-AP
Radio 1 OP Mode	AP Mode
Radio 1 Profile:	Local_WALN
Radio 2 OP Mode	AP Mode
Radio 2 Profile:	Local_WALN_5G

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

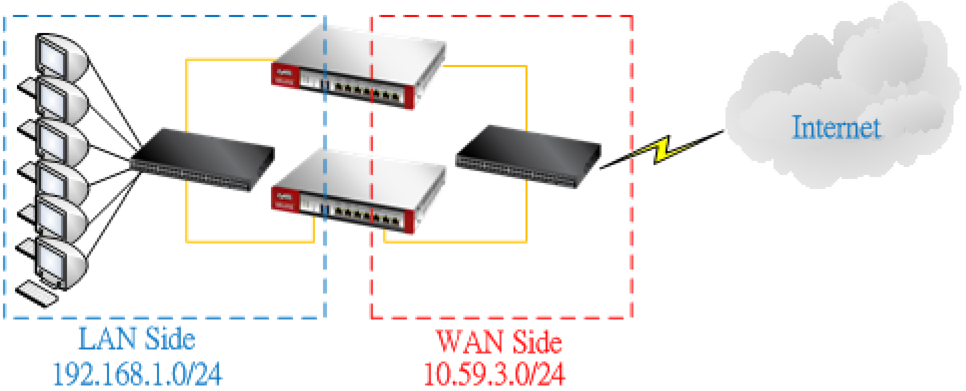
BBBBBBBBBBBBBBBBBBBB

For_LAN2

Scenario 12 – Device HA on the USG

12.1 Application Scenario

Setup the Device HA environment.

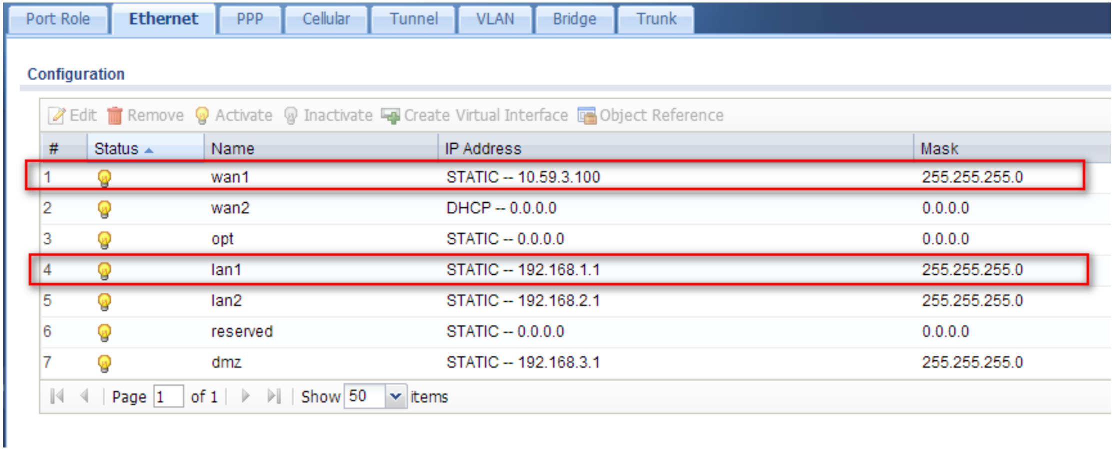


	Master device	Backup device
WAN interface IP	10.59.3.100/24	10.59.3.100/24
WAN Management IP	10.59.3.101/24	10.59.3.102/24
LAN1 Interface IP	192.168.1.1/24	192.168.1.1/24
LAN1 Management IP	192.168.1.11/24	192.168.1.12/24
Cluster ID	1	1

12.2 Configuration Guide

On Master setting:

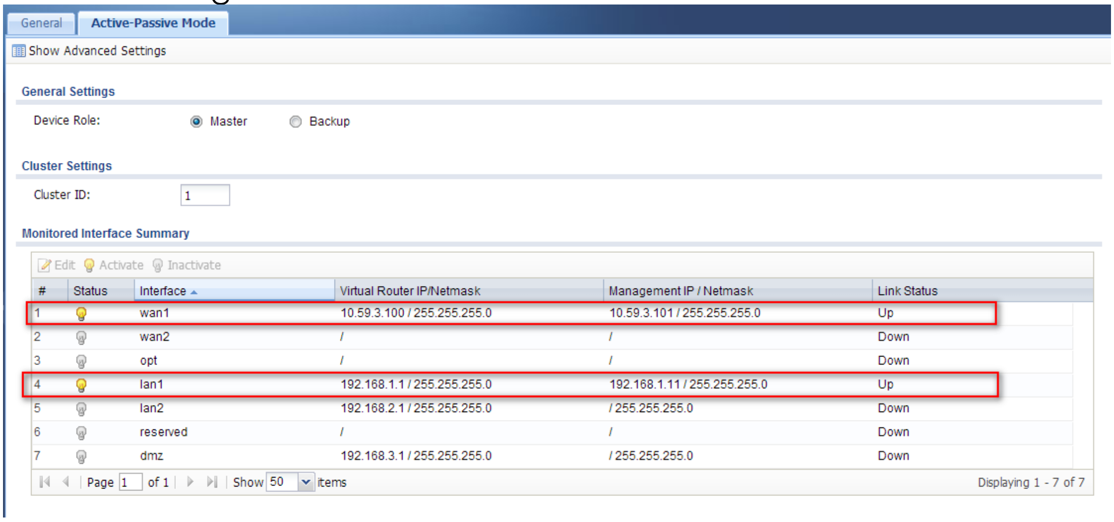
(1) Go to **Configuration** > **Network** > **Interface** > **Ethernet** to check the WAN and LAN interface setting.
WAN interface is: 10.59.3.100/24
LAN interface is: 192.168.1.1/24



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

(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

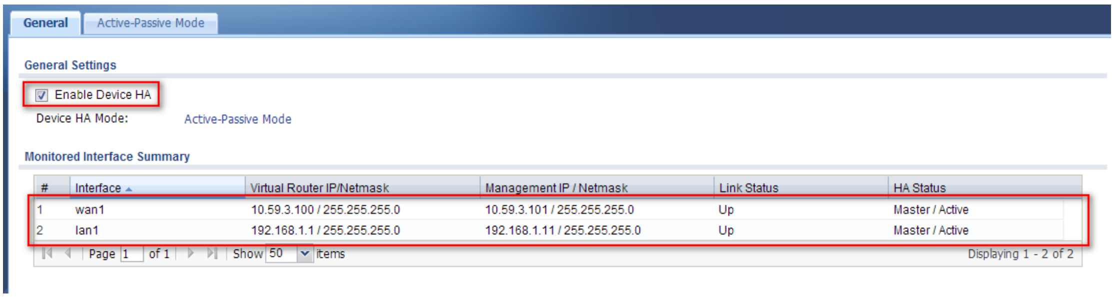
Cluster ID: 1

Monitored Interface Summary

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

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

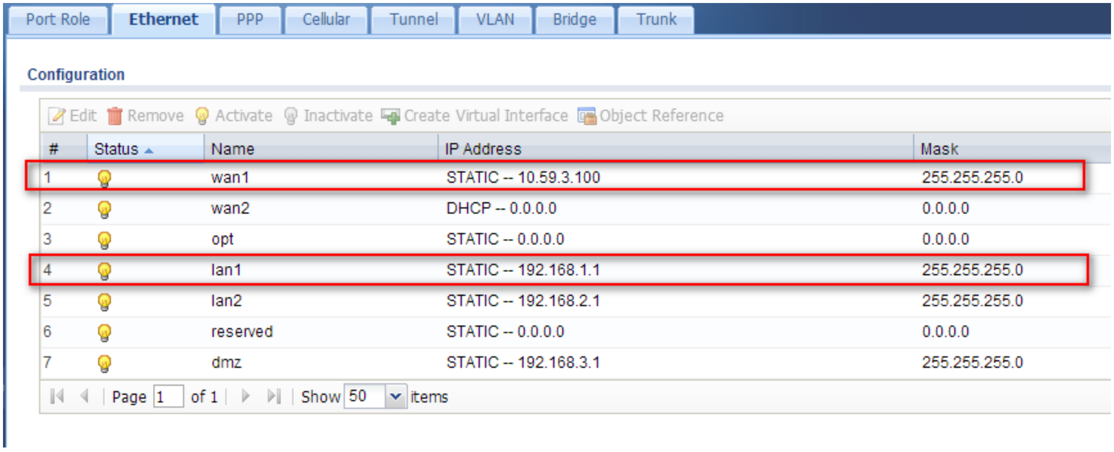
Monitored Interface Summary

#	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

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
PPP
Cellular
Tunnel
VLAN
Bridge
Trunk

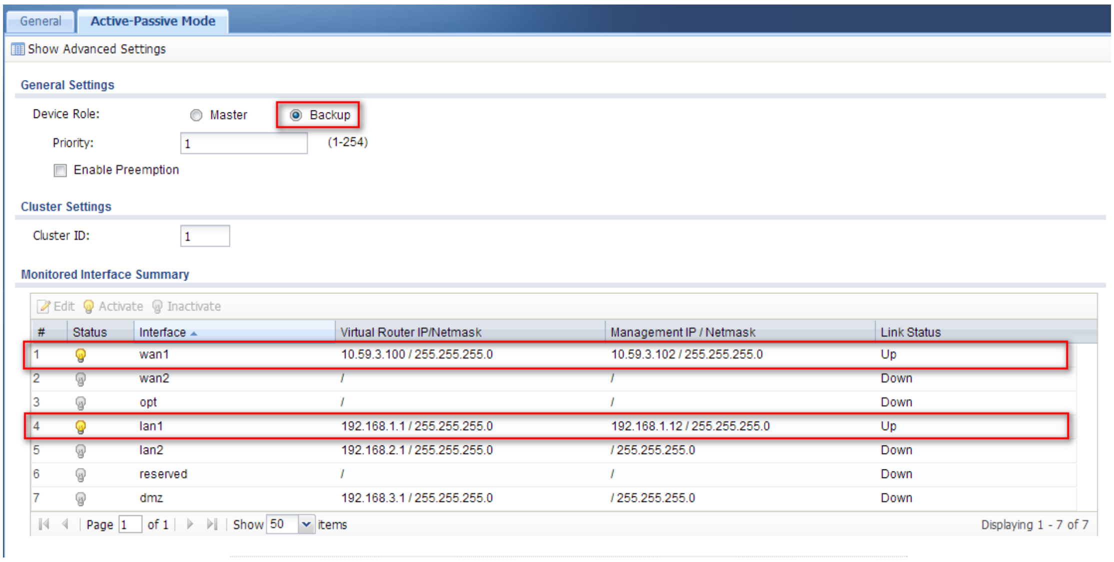
Configuration

Edit Remove Activate Inactivate Create Virtual Interface Object Reference

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

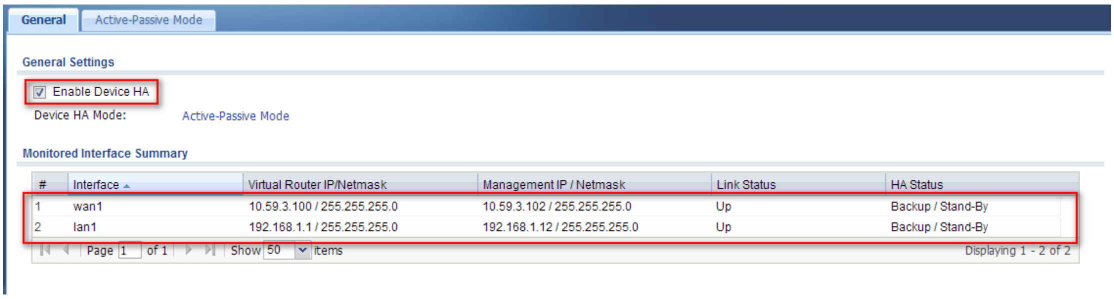
Monitored Interface Summary

Edit Activate Inactivate

#	Status	Interface	Virtual Router IP/Netmask	Management IP / Netmask	Link Status
1	●	wan1	10.59.3.100 / 255.255.255.0	10.59.3.102 / 255.255.255.0	Up
2	○	wan2	/	/	Down
3	○	opt	/	/	Down
4	●	lan1	192.168.1.1 / 255.255.255.0	192.168.1.12 / 255.255.255.0	Up
5	○	lan2	192.168.2.1 / 255.255.255.0	/ 255.255.255.0	Down
6	○	reserved	/	/	Down
7	○	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 saw the interface that was monitored above.



General | Active-Passive Mode

General Settings

☑ Enable Device HA

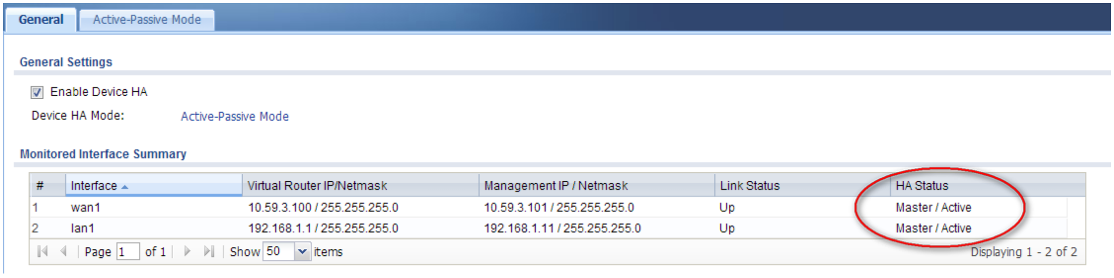
Device HA Mode: Active-Passive Mode

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

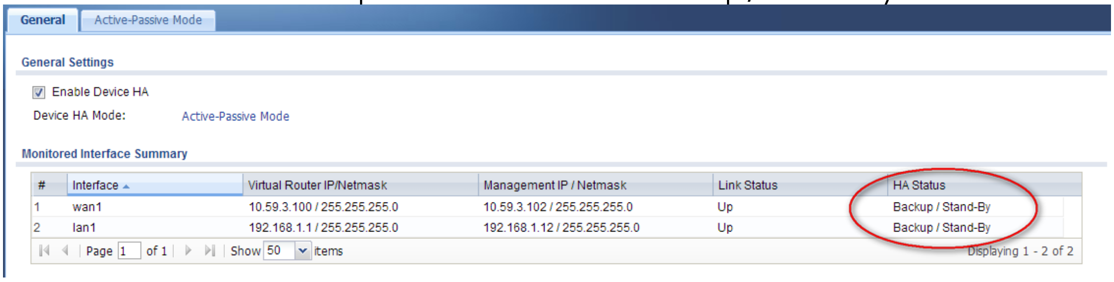
Device HA Mode: Active-Passive Mode

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

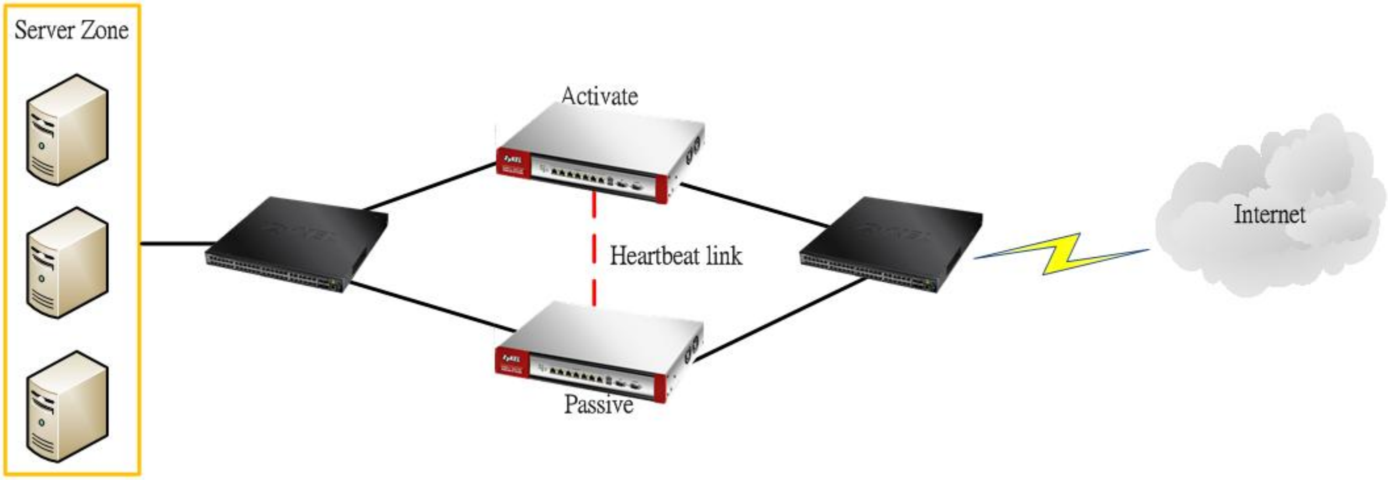
#	Interface	Virtual Router IP/Netmask	Management IP / Netmask	Link Status	HA Status
1	wan1	10.59.3.100 / 255.255.255.0	10.59.3.102 / 255.255.255.0	Up	Backup / Stand-By
2	lan1	192.168.1.1 / 255.255.255.0	192.168.1.12 / 255.255.255.0	Up	Backup / Stand-By

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

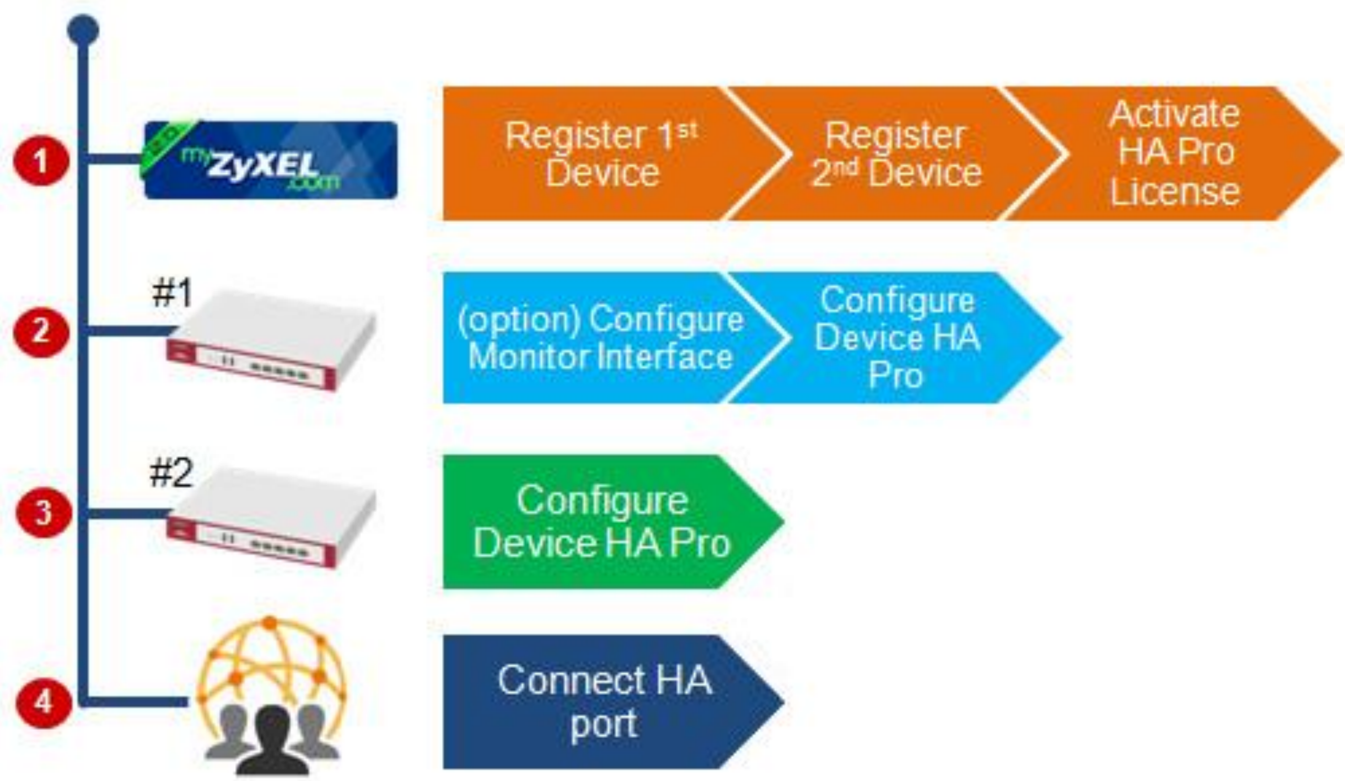
Scenario 13 – Activating Device HA Pro

13.1 How to Enable Device HA Pro

The Device HA feature acts as a failover when one of the devices in the network is dead or can't access the Internet. Therefore, this is a popular feature for network environments. In the previous firmware version, the USG supports AP (Activate-Passive/Master-Backup) mode. In V4.20, the Device HA feature is enhanced and named **Device HA Pro**.

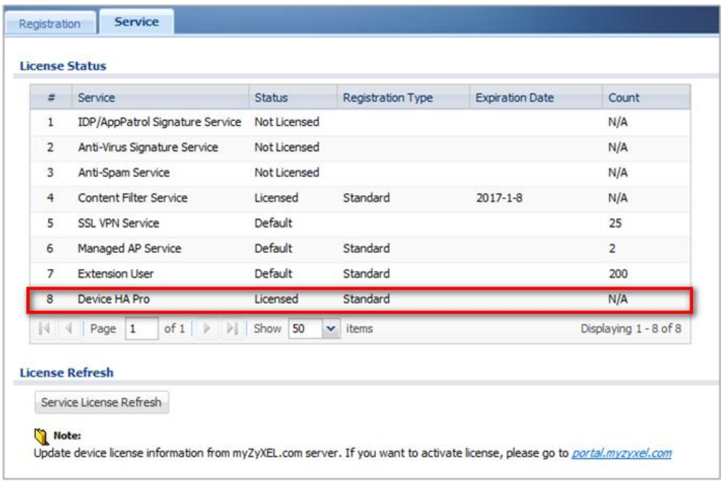


In Device HA Pro, a "heartbeat link" is added for monitoring the interface status and synchronizing settings. Follow the steps below to deploy the Device HA Pro feature in your network environment.



Device HA Pro License

1. The Device HA Pro feature is license required. You must register both of your devices on the **myZyXEL.com** server first. Then make sure the Device HA Pro license is available on both of your devices.



License Status

#	Service	Status	Registration Type	Expiration Date	Count
1	IDP/AppPatrol Signature Service	Not Licensed			N/A
2	Anti-Virus Signature Service	Not Licensed			N/A
3	Anti-Spam Service	Not Licensed			N/A
4	Content Filter Service	Licensed	Standard	2017-1-8	N/A
5	SSL VPN Service	Default			25
6	Managed AP Service	Default	Standard		2
7	Extension User	Default	Standard		200
8	Device HA Pro	Licensed	Standard		N/A

Page 1 of 1 | Show 50 items | Displaying 1 - 8 of 8

License Refresh

Note:
Update device license information from myZyXEL.com server. If you want to activate license, please go to portal.myzyxel.com

Behavior of the Device HA Pro

The behavior of the Device HA Pro includes a heartbeat link to monitor the "activate" device's interface status. If one of the monitored interfaces is dead or fails, the "passive" device's status will became "activate". (This means only 1 device's status can be "activate" at a time.)

Be aware that the Device HA status of the devices might constantly change due to the network environment situation. In the current firmware design, Device HA Pro will not fallback when the primary device interface is working normally again.

Device-HA Pro Settings:

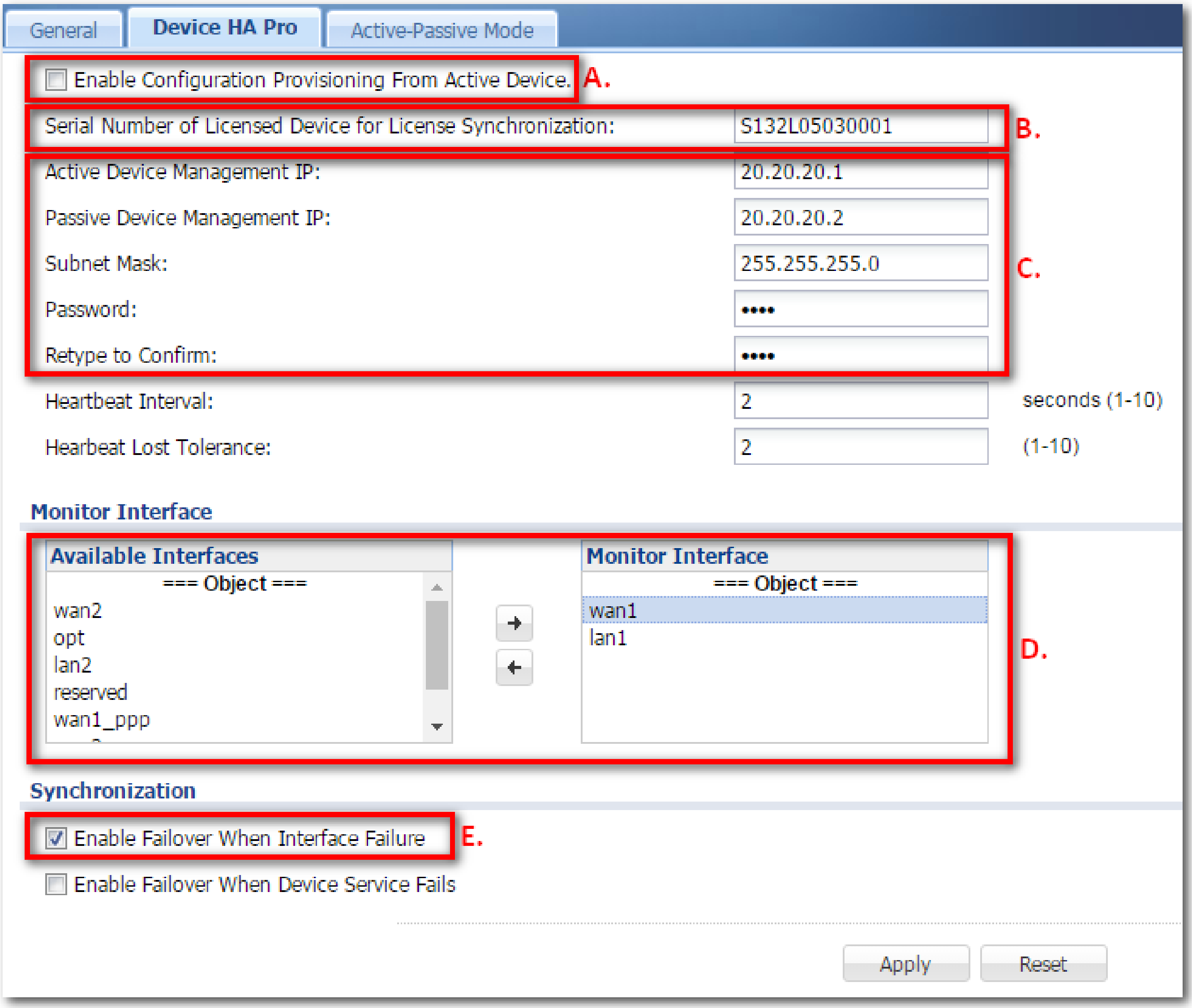
A. ***Enable configuration provisioning on the activated device***
--This function is for the secondary device. If you are configuring the primary device, this function is unnecessary.

B. ***Serial number of the licensed device for license synchronization***
--Entering the serial number of license from the **myZyXEL.com** server.

C. ***Configure the Device HA Pro interface***
-- Enter the management IP address of the active and passive devices. Also, enter the password for synchronizing configuration with each other.

D. ***Monitoring Interfaces***
--Select the interfaces which you would like to monitor.

E. ***Synchronization***
-- Enable failover when one of the interfaces fails.



□ Enable Configuration Provisioning From Active Device.

Serial Number of Licensed Device for License Synchronization: S132L05030001

Active Device Management IP: 20.20.20.1

Passive Device Management IP: 20.20.20.2

Subnet Mask: 255.255.255.0

Password: ••••

Retype to Confirm: ••••

Heartbeat Interval: 2 seconds (1-10)

Hearbeat Lost Tolerance: 2 (1-10)

Monitor Interface

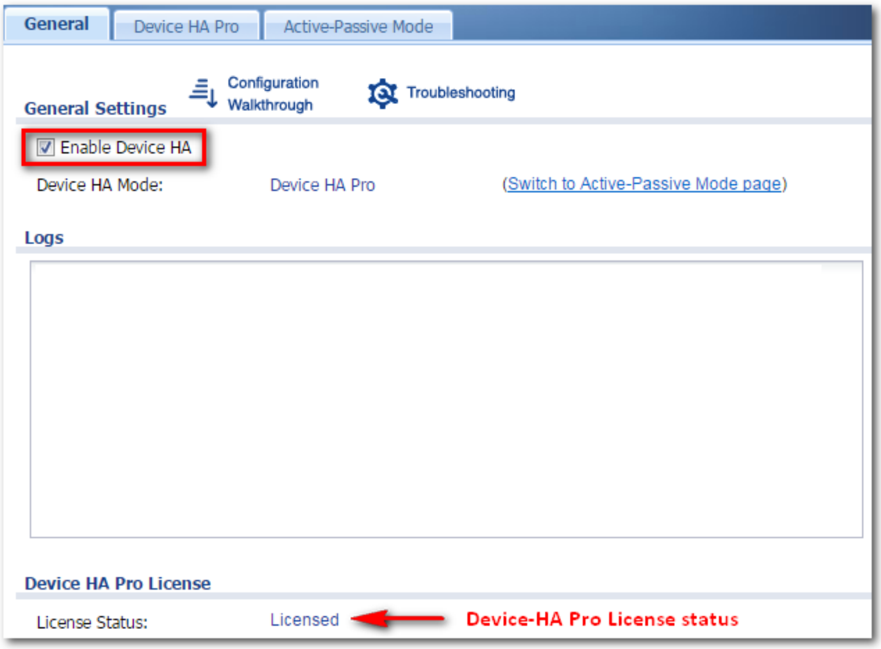
Available Interfaces	Monitor Interface
=== Object ===	=== Object ===
wan2	wan1
opt	lan1
lan2	
reserved	
wan1_ppp	

Synchronization

☑ Enable Failover When Interface Failure

□ Enable Failover When Device Service Fails

The Main Function of the Device HA Pro



General Settings

☑ Enable Device HA

Device HA Mode: Device HA Pro (Switch to Active-Passive Mode page)

Logs

Device HA Pro License

License Status: Licensed

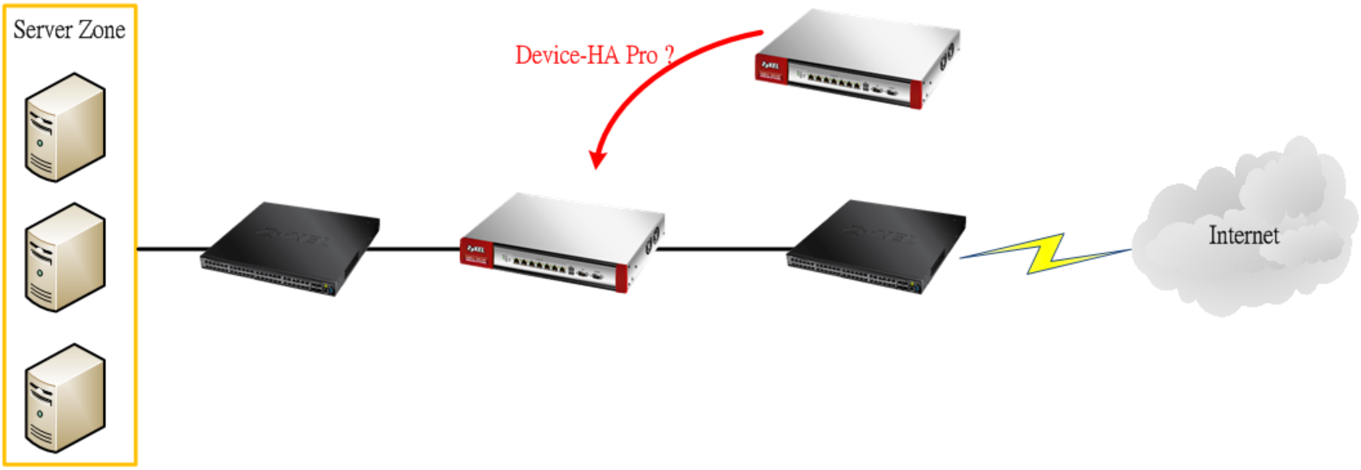
Heartbeat Link

The heartbeat port is a new physical port on the device.
After you have enabled Device HA Pro, the devices will transmit multicast packets (UDP 694) to check each device's status.
When the passive device is working properly, the system LED light will be on. Only the heartbeat port's LED light can be on.

Suggestions

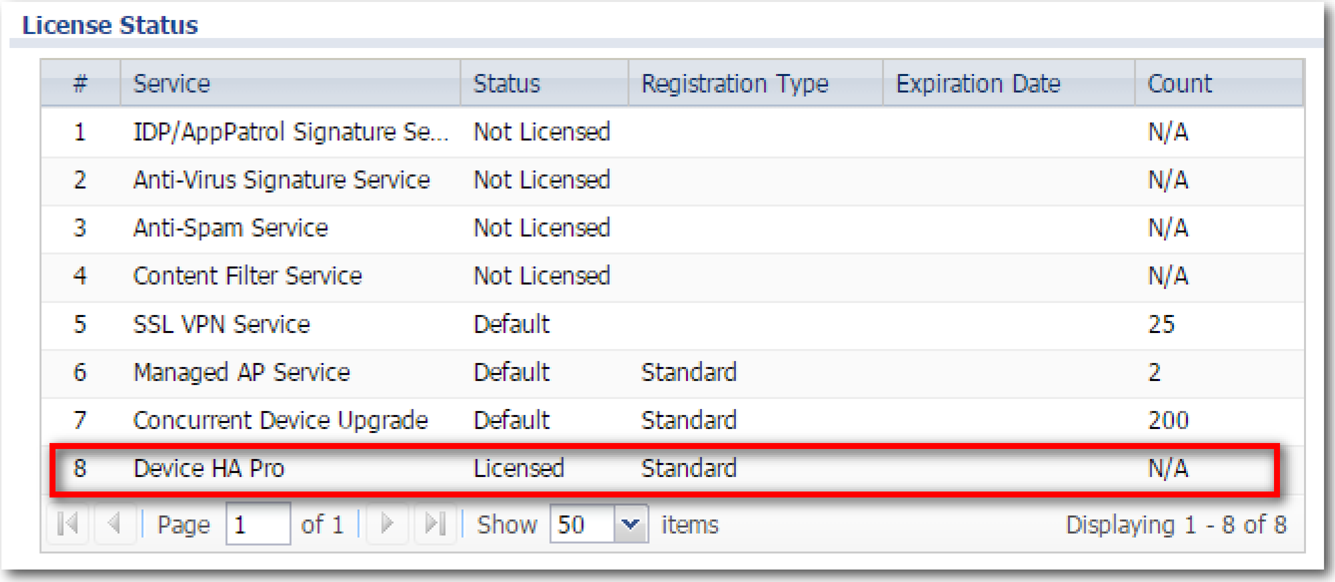
(1) Transfer all of the licenses to the primary device. This helps to avoid the system from recounting licenses every time.
(2) Enable the connectivity check function on the monitored interfaces. When an interface doesn't receive any response from the remote server for a certain period of time, the device will consider the interface status as fail. Then the Device HA Pro feature will change the status of the interface.

13.2 How do I Configure Device HA Pro in My Current Environment?



1. License

The Device HA Pro feature is license required. Please go to register both of your devices on **myZyXEL.com** and make sure the devices have the license after syncing with the **myZyXEL.com** server.

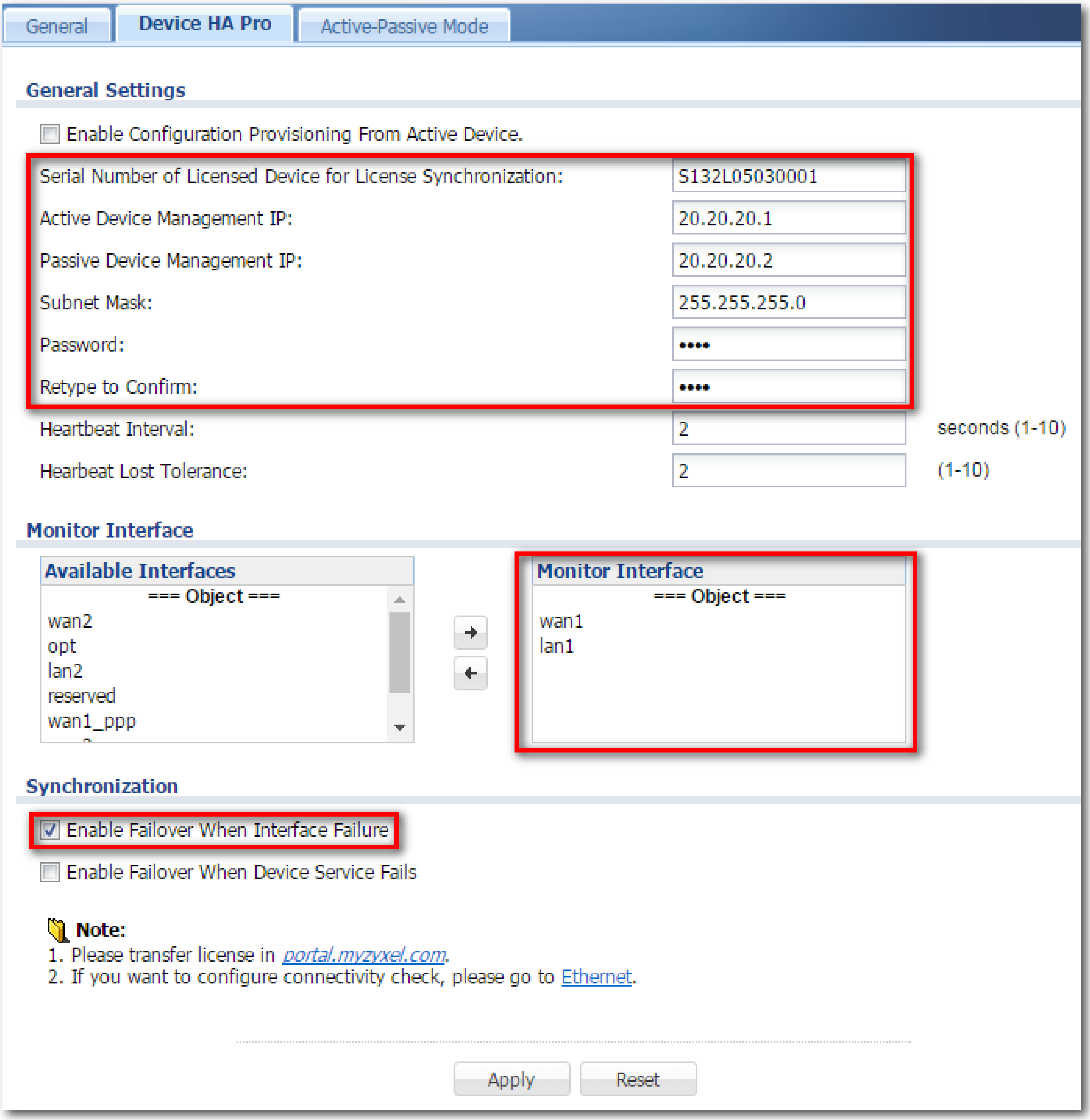


License Status

#	Service	Status	Registration Type	Expiration Date	Count
1	IDP/AppPatrol Signature Se...	Not Licensed			N/A
2	Anti-Virus Signature Service	Not Licensed			N/A
3	Anti-Spam Service	Not Licensed			N/A
4	Content Filter Service	Not Licensed			N/A
5	SSL VPN Service	Default			25
6	Managed AP Service	Default	Standard		2
7	Concurrent Device Upgrade	Default	Standard		200
8	Device HA Pro	Licensed	Standard		N/A

2. Configurations on the Primary Device

Go to the **Configuration** > **Device HA** > **Device HA Pro** screen.
-Enter the device's license serial number from the **myZyXEL.com** server.
-Enter the management IP address after enabling the Device HA Pro feature.
-Select the interfaces which you would like to monitor.
-Enable failover when an interface fails.
-Click **Apply**.



General Settings

□ Enable Configuration Provisioning From Active Device.

Serial Number of Licensed Device for License Synchronization:	S132L05030001	
Active Device Management IP:	20.20.20.1	
Passive Device Management IP:	20.20.20.2	
Subnet Mask:	255.255.255.0	
Password:	••••	
Retype to Confirm:	••••	
Heartbeat Interval:	2	seconds (1-10)
Hearbeat Lost Tolerance:	2	(1-10)

Monitor Interface

Available Interfaces
=== Object ===
wan2
opt
lan2
reserved
wan1_ppp

Monitor Interface
=== Object ===
wan1
lan1

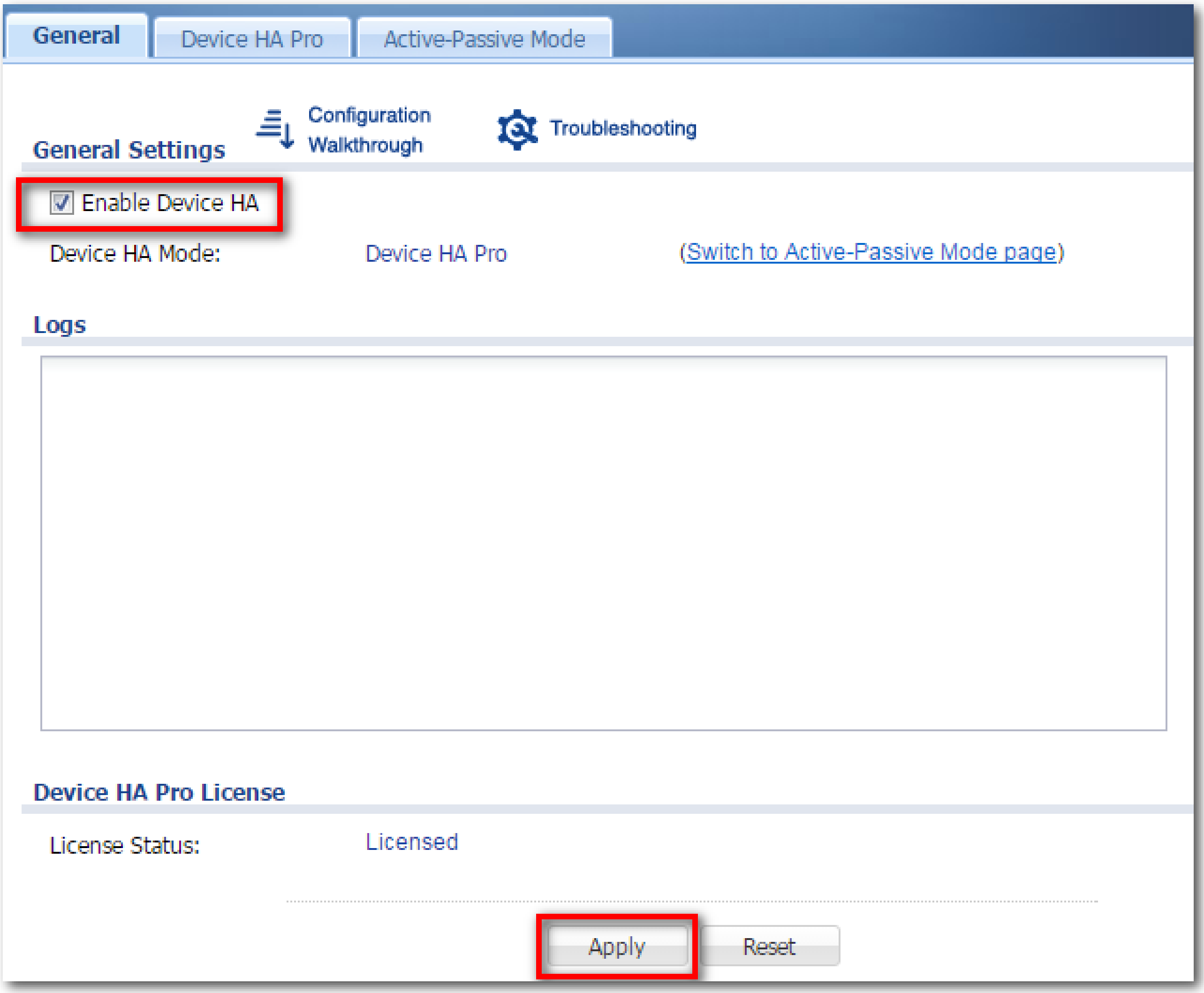
Synchronization

☑ Enable Failover When Interface Failure

□ Enable Failover When Device Service Fails

Note:
1. Please transfer license in portal.myzyxel.com.
2. If you want to configure connectivity check, please go to Ethernet.

Go to the **Configuration** > **Device HA** > **General** screen.
- Select **Enable Device HA** and click **Apply** to enable Device HA Pro.



General Settings

☑ Enable Device HA

Device HA Mode: Device HA Pro (Switch to Active-Passive Mode page)

Logs

Device HA Pro License

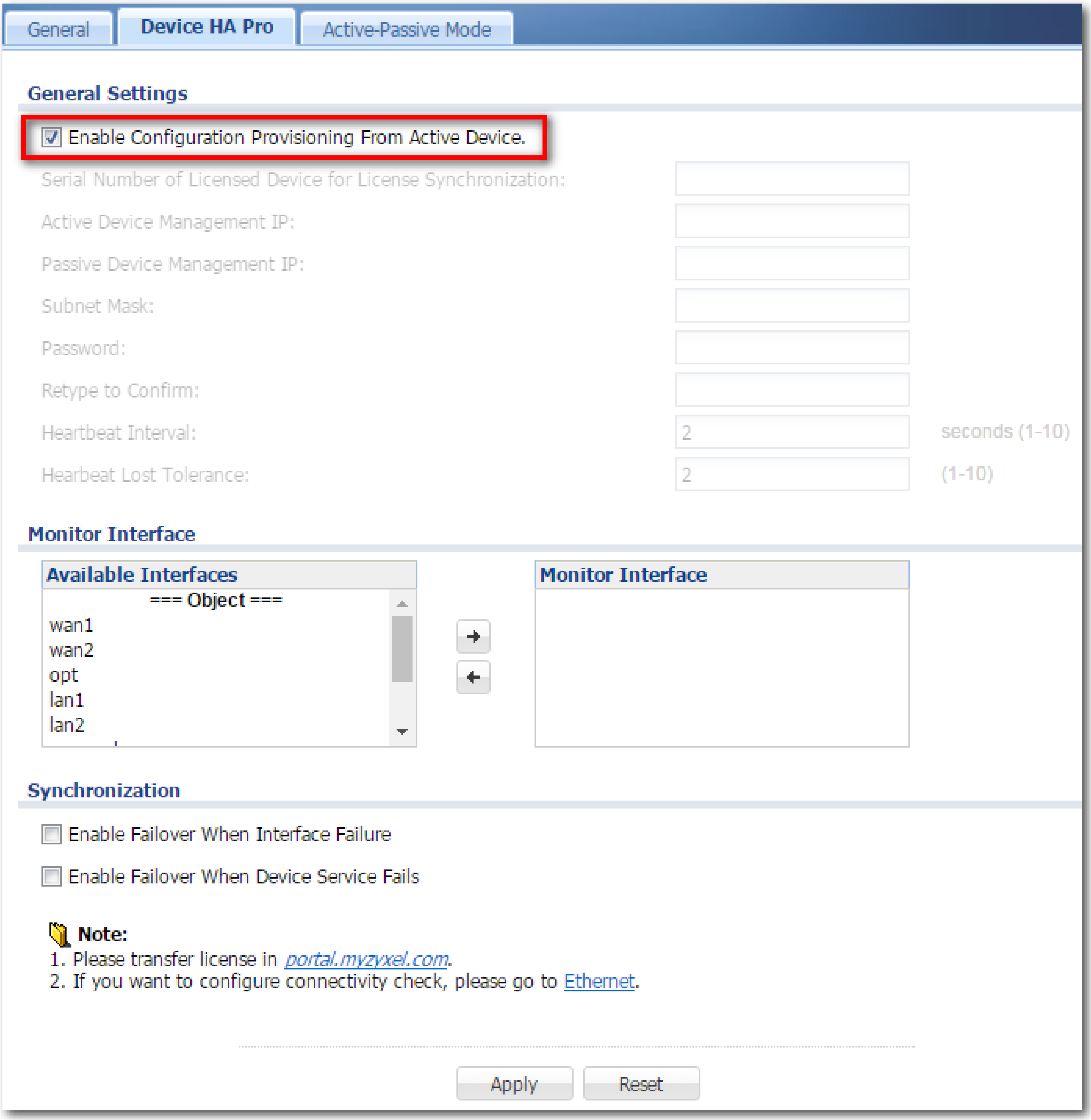
License Status: Licensed

3. Configurations on the Secondary Device

Go to the **Configuration** > **Device HA** > **Device-HA Pro** screen.

-Select **Enable Configuration Provisioning From Active Device**.

-Click **Apply**.



General Settings

☑ Enable Configuration Provisioning From Active Device.

Serial Number of Licensed Device for License Synchronization:		
Active Device Management IP:		
Passive Device Management IP:		
Subnet Mask:		
Password:		
Retype to Confirm:		
Heartbeat Interval:	2	seconds (1-10)
Hearbeat Lost Tolerance:	2	(1-10)

Monitor Interface

Available Interfaces	Monitor Interface
=== Object === wan1 wan2 opt lan1 lan2	

Synchronization

☐ Enable Failover When Interface Failure

☐ Enable Failover When Device Service Fails

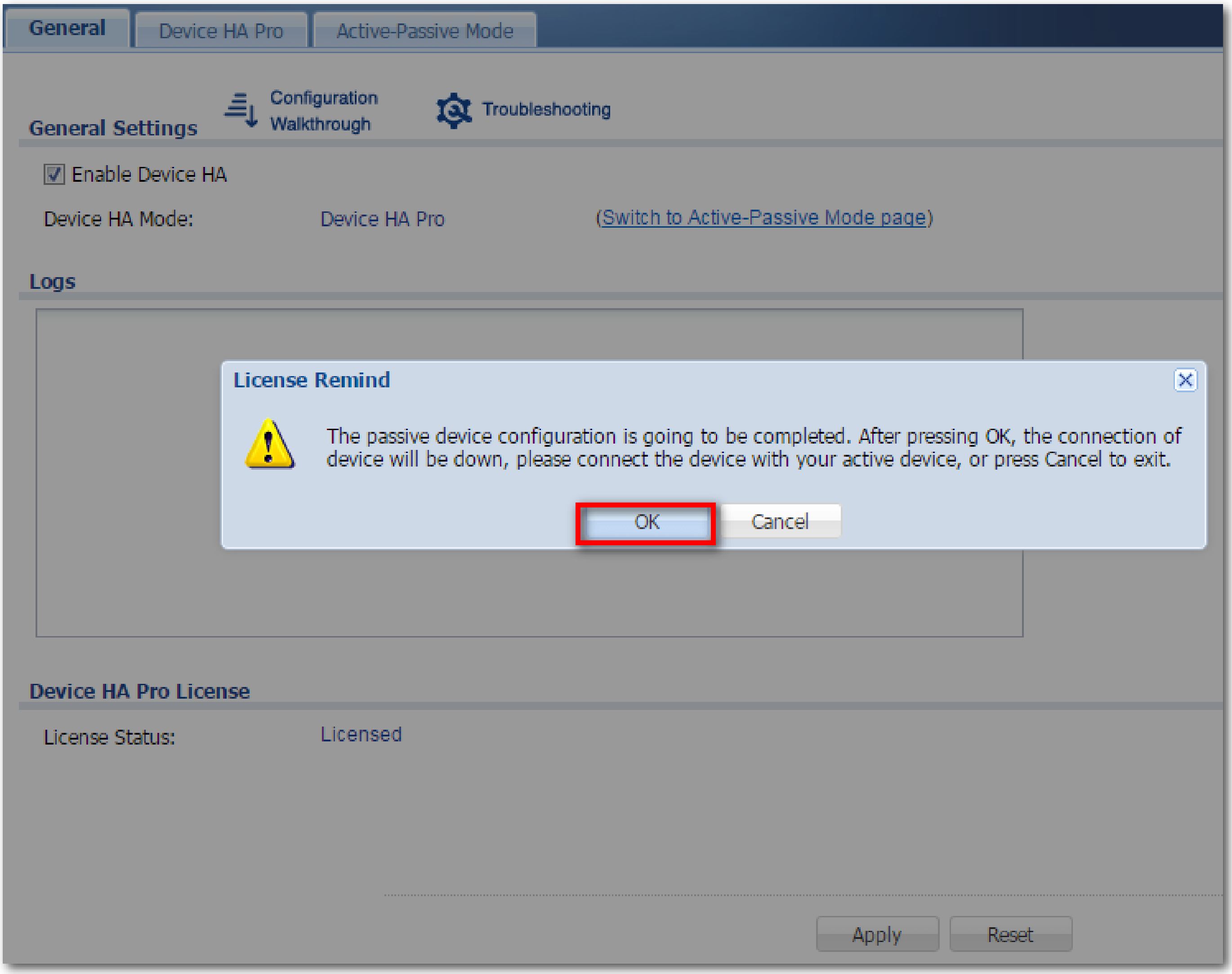
Note:

1. Please transfer license in *portal.myzyxel.com*.
2. If you want to configure connectivity check, please go to Ethernet.

Go to the **Configuration** > **Device HA** > **General** screen.

-Select **Enable Device HA** and click **Apply**.

-Before the Device HA Pro feature is enabled on the secondary device, a **warning message** will pop-up for you to confirm. Click **OK** to enable it.



☑ Enable Device HA

Device HA Mode: Device HA Pro (Switch to Active-Passive Mode page)

License Remind

The passive device configuration is going to be completed. After pressing OK, the connection of device will be down, please connect the device with your active device, or press Cancel to exit.

OK Cancel

License Status: Licensed

4. **Connecting the Device HA Pro Port**

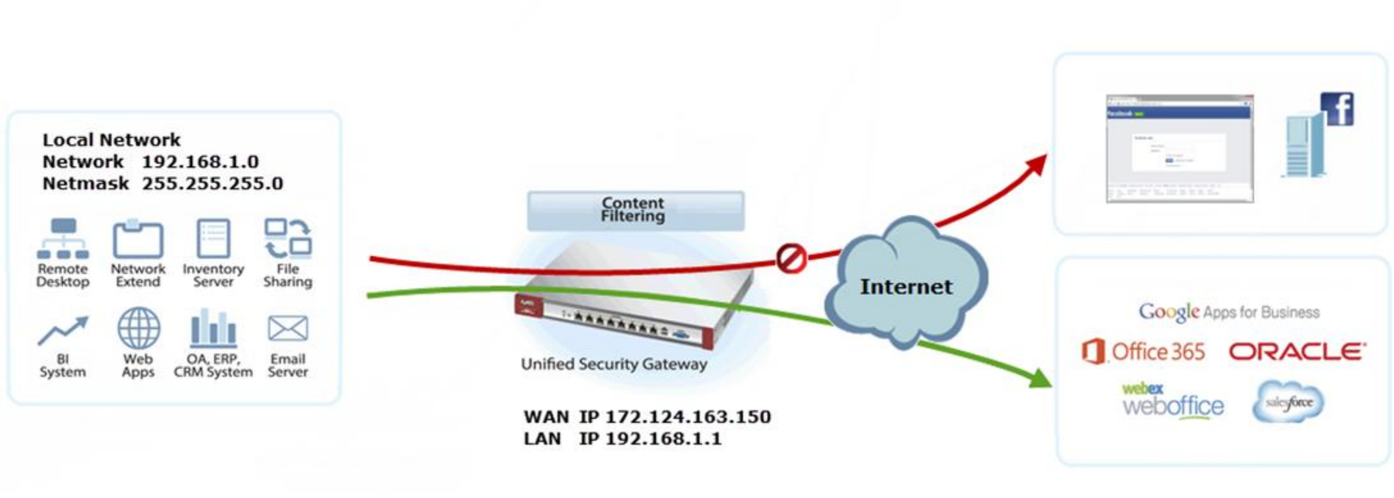
   The Device HA Pro port is a new physical port on the DUT. You can use a cable to connect the devices with each other.

Scenario 14 — Content Filter 2.0 - HTTPs Domain Filter

14.1 Application Scenario

The Content Filter 2.0 - HTTPs Domain Filter allows you to block HTTPs websites by category service without SSL-Inspection. The filtering feature is based on 64 categories built in ZyWALL/USG such as pornography, gambling, hacking, etc.

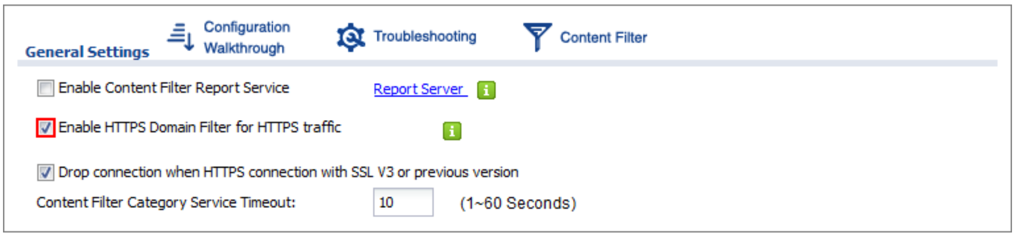
When user makes HTTPS request, the information contains a Server Name Indication (SNI) extension fields in server FQDN. Using the SNI to query category from local cache then cloud database, then take action when it matches the block category in Content Filter profile.



14.2 Configuration Guide

Set Up the Content Filter on the ZyWALL/USG

1. Go to **CONFIGURATION > UTM Profile> Content Filter > Profile > General Settings**. Select **Enable HTTPS Domain Filter for HTTPS traffic.**



General Settings

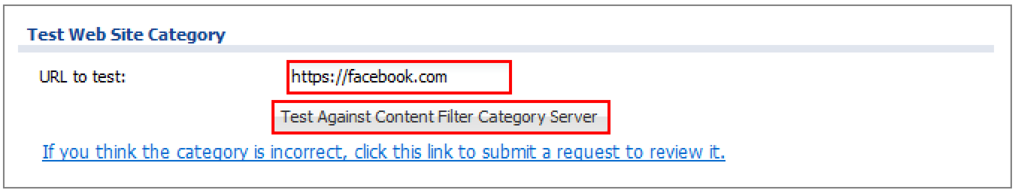
☐ Enable Content Filter Report Service Report Server

☑ Enable HTTPS Domain Filter for HTTPS traffic

☑ Drop connection when HTTPS connection with SSL V3 or previous version

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

2. Go to **CONFIGURATION > UTM Profile> Content Filter > Profile Management > Add Filter Profile > Test Web Site Category**. Type URL to test the category and click **Test Against Content Filter Category Server.**

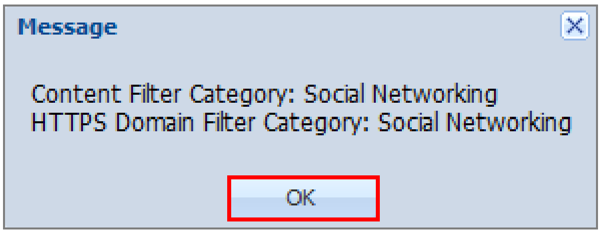


Test Web Site Category

URL to test: https://facebook.com

If you think the category is incorrect, click this link to submit a request to review it.

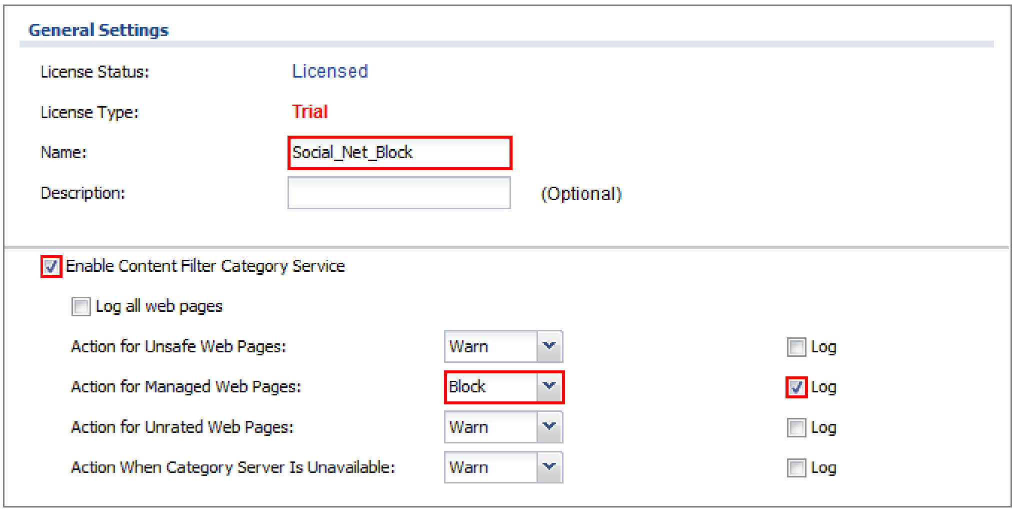
3. You will see the category recorded in the external content filter server's database for both HTTP and HTTPS Domain you specified.



Message

Content Filter Category: Social Networking
HTTPS Domain Filter Category: Social Networking

4. Go to **CONFIGURATION > UTM Profile> Content Filter > Profile Management > Add Filter File > Custom Service**. Configure a **Name** for you to identify the **Content Filter Profile** and select **Enable Content Filter Category Service**. Select **Block** to prevent users from accessing web pages that match the managed categories that you select below. Select **Log** to record attempts to access web pages that match the unsafe categories that you select below.



General Settings

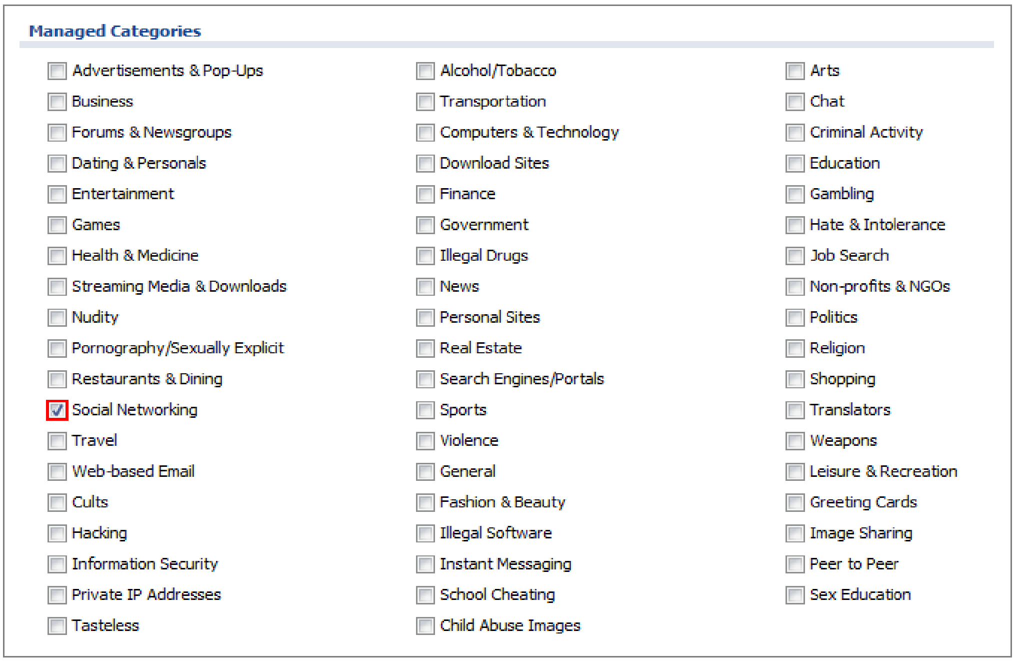
License Status: Licensed
License Type: Trial
Name: Social_Net_Block
Description: (Optional)

☑ Enable Content Filter Category Service

□ Log all web pages

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

5. Scroll down to the **Managed Categories** section, select categories in this section to control access to specific types of Internet content. You must have the Content Filtering license to filter these categories.



Managed Categories

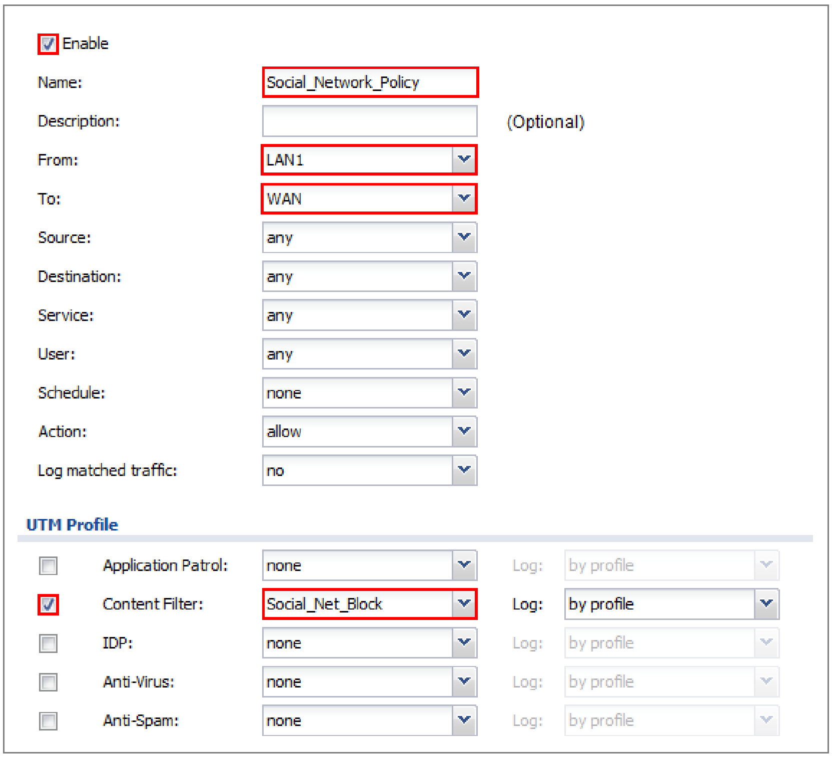
□ Advertisements & Pop-Ups
□ Business
□ Forums & Newsgroups
□ Dating & Personals
□ Entertainment
□ Games
□ Health & Medicine
□ Streaming Media & Downloads
□ Nudity
□ Pornography/Sexually Explicit
□ Restaurants & Dining
☑ Social Networking
□ Travel
□ Web-based Email
□ Cults
□ Hacking
□ Information Security
□ Private IP Addresses
□ Tasteless

□ Alcohol/Tobacco
□ Transportation
□ Computers & Technology
□ Download Sites
□ Finance
□ Government
□ Illegal Drugs
□ News
□ Personal Sites
□ Real Estate
□ Search Engines/Portals
□ Sports
□ Violence
□ General
□ Fashion & Beauty
□ Illegal Software
□ Instant Messaging
□ School Cheating
□ Child Abuse Images

□ Arts
□ Chat
□ Criminal Activity
□ Education
□ Gambling
□ Hate & Intolerance
□ Job Search
□ Non-profits & NGOs
□ Politics
□ Religion
□ Shopping
□ Translators
□ Weapons
□ Leisure & Recreation
□ Greeting Cards
□ Image Sharing
□ Peer to Peer
□ Sex Education

Set Up the Security Policy on the ZyWALL/USG

1. Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Social_Net_Block in this example).



☑ Enable

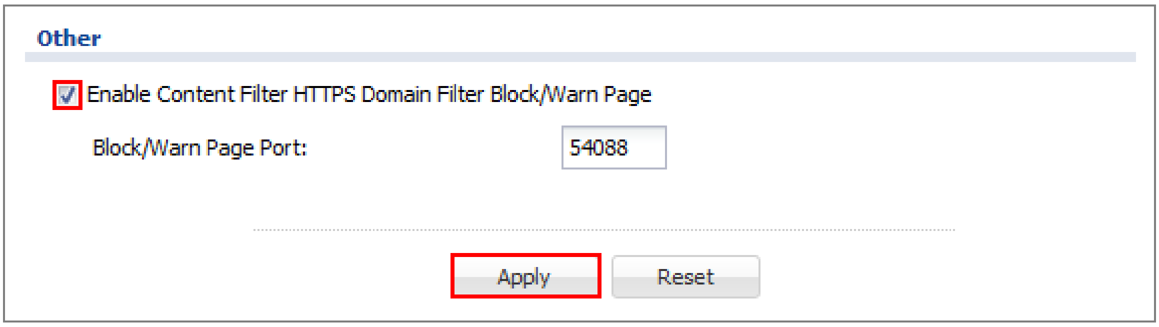
Name:	Social_Network_Policy	
Description:		(Optional)
From:	LAN1	
To:	WAN	
Source:	any	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	no	

UTM Profile

□	Application Patrol:	none	Log:	by profile
☑	Content Filter:	Social_Net_Block	Log:	by profile
□	IDP:	none	Log:	by profile
□	Anti-Virus:	none	Log:	by profile
□	Anti-Spam:	none	Log:	by profile

Set Up the System Policy on the ZyWALL/USG

1. Go to **CONFIGURATION** > **System** > **WWW** > **Show Advanced Settings** > **Other**, click **Enable Content Filter HTTPS Domain Filter Block/Warn Page**.



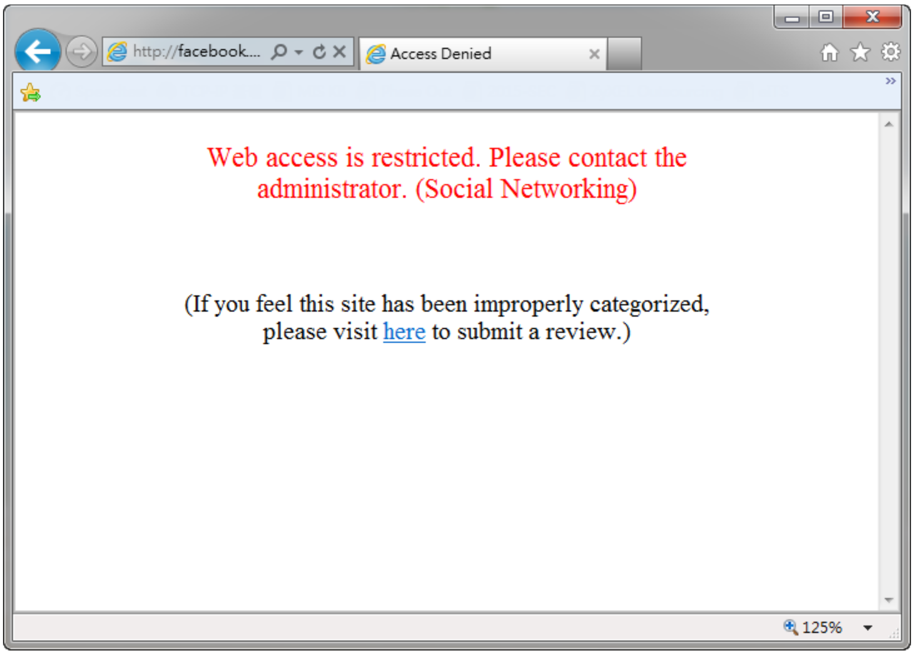
Other

☑ Enable Content Filter HTTPS Domain Filter Block/Warn Page

Block/Warn Page Port: 54088

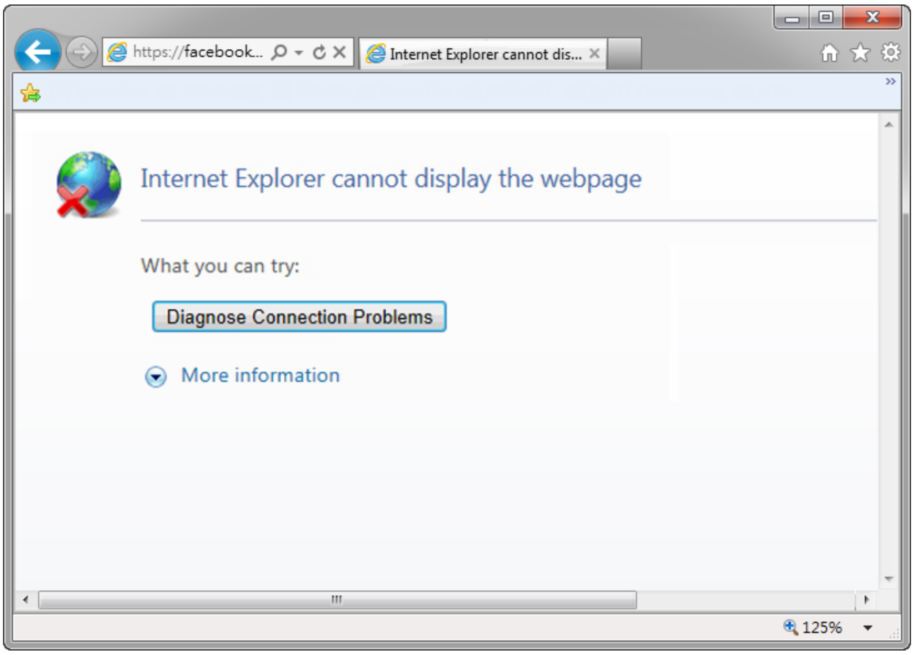
Test the Result

1. Type http://www.facebook.com/ or https://www.facebook.com/ into the browser, the error message occurs.



Web access is restricted. Please contact the administrator. (Social Networking)

(If you feel this site has been improperly categorized, please visit here to submit a review.)

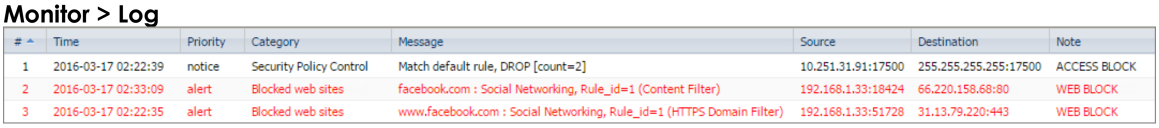


Internet Explorer cannot display the webpage

What you can try:

2. Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below. HTTP traffic log matches (Content Filter) and HTTPS traffic log matches (HTTPS Domain Filter) in message field.

Monitor > Log



#	Time	Priority	Category	Message	Source	Destination	Note
1	2016-03-17 02:22:39	notice	Security Policy Control	Match default rule, DROP [count=2]	10.251.31.91:17500	255.255.255.255:17500	ACCESS BLOCK
2	2016-03-17 02:33:09	alert	Blocked web sites	facebook.com : Social Networking, Rule_id=1 (Content Filter)	192.168.1.33:18424	66.220.158.68:80	WEB BLOCK
3	2016-03-17 02:22:35	alert	Blocked web sites	www.facebook.com : Social Networking, Rule_id=1 (HTTPS Domain Filter)	192.168.1.33:51728	31.13.79.220:443	WEB BLOCK

Scenario 15 — Content Filter 2.0 - Geo IP Blocking

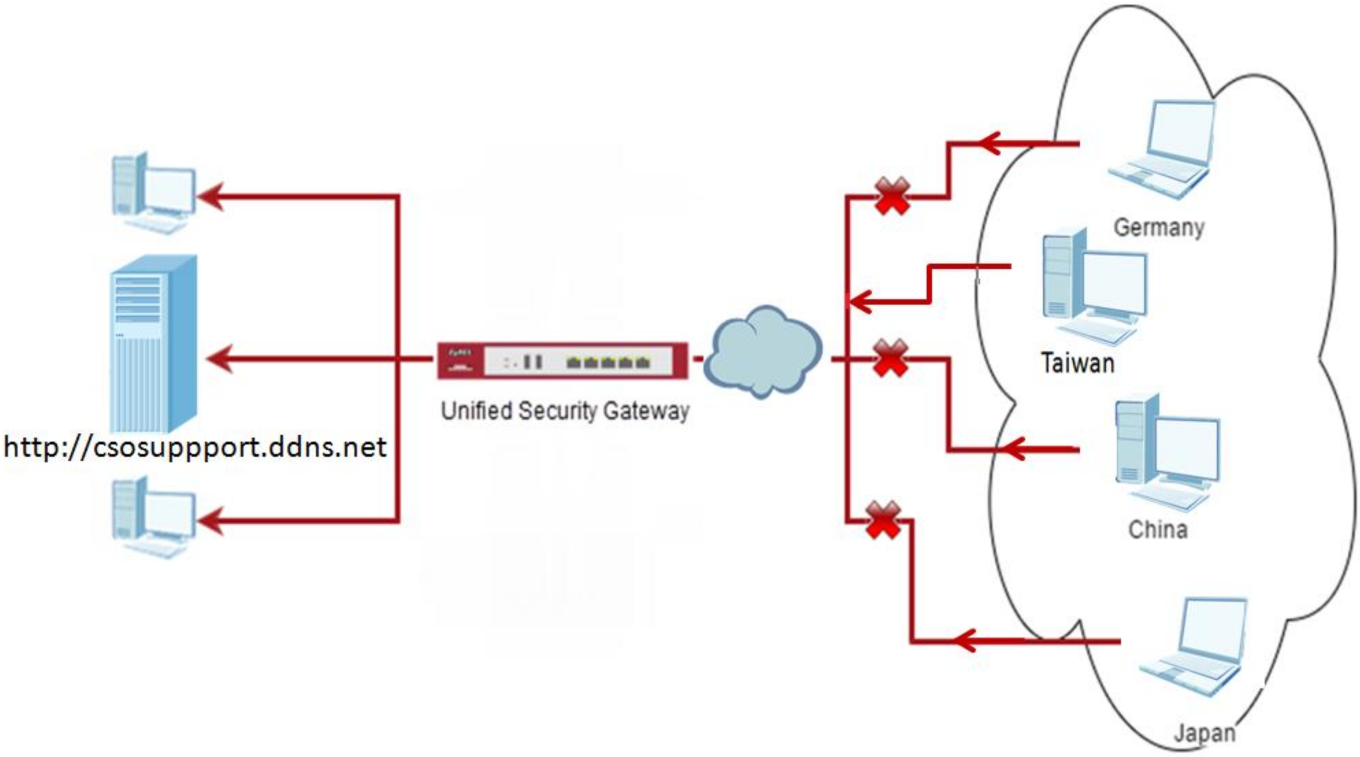
15.1 Application Scenario

The Content Filter 2.0 - Geo IP blocking offers identify the country based on IP address, it allows you to block the client accessing to certain country based on organizational policy.

When user makes HTTP or HTTPS request, ZyWALL/USG query IP address from MaxMind database, then take action when it matches the block country in Content Filter profile.

If you have a local web site and your primary market is local people, then there is no need to let any other countries index or waste bandwidth on your server.

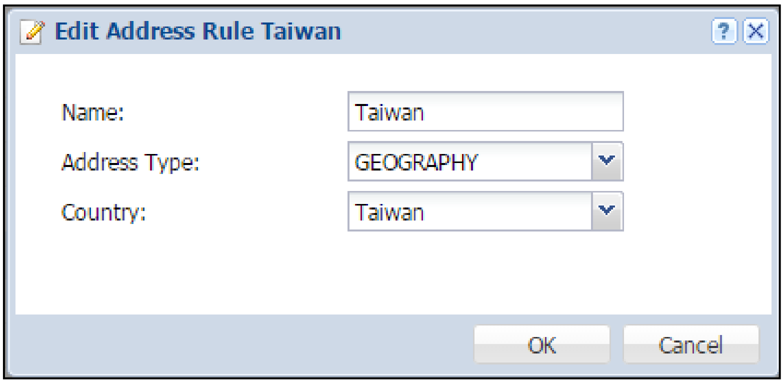
Also this feature offer an easy and effective way to prevent bogus, bots, brute force hacks, vulnerability scanners, and web crawlers from other countries.



15.2 Configuration Guide

Set Up the Address Objet with Geo IP on the ZyWALL/USG

1. Go to **CONFIGURATION > Object > Address/Geo IP > Address > Add Address Rule**.



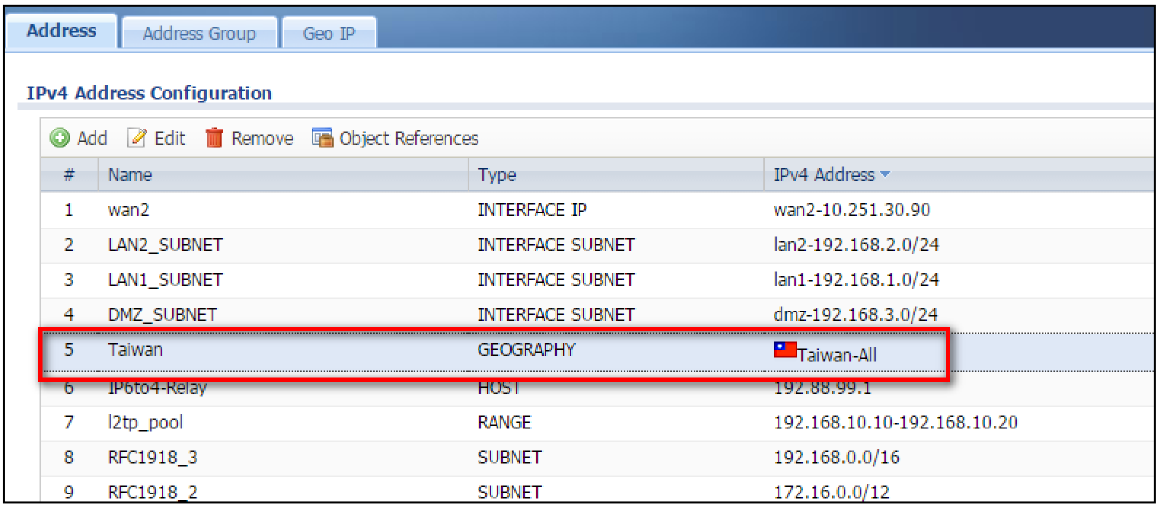
Edit Address Rule Taiwan

Name: Taiwan

Address Type: GEOGRAPHY

Country: Taiwan

2. Go to **CONFIGURATION > Object > Address/Geo IP > Address**, you can see the customized GEOGRAPHY address.

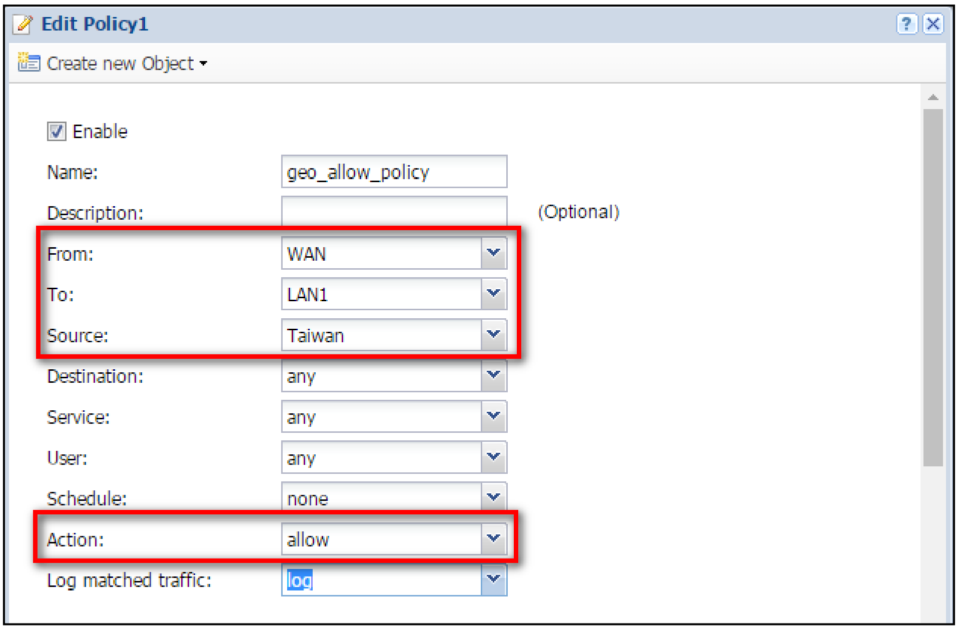


IPv4 Address Configuration

#	Name	Type	IPv4 Address
1	wan2	INTERFACE IP	wan2-10.251.30.90
2	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
4	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
5	Taiwan	GEOGRAPHY	Taiwan-All
6	IP6to4-Relay	HOST	192.88.99.1
7	l2tp_pool	RANGE	192.168.10.10-192.168.10.20
8	RFC1918_3	SUBNET	192.168.0.0/16
9	RFC1918_2	SUBNET	172.16.0.0/12

Set Up the Security Policy on the ZyWALL/USG

1. Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set Geo IP traffic from WAN to LAN allow source from local country (geo_allow_policy in this example).

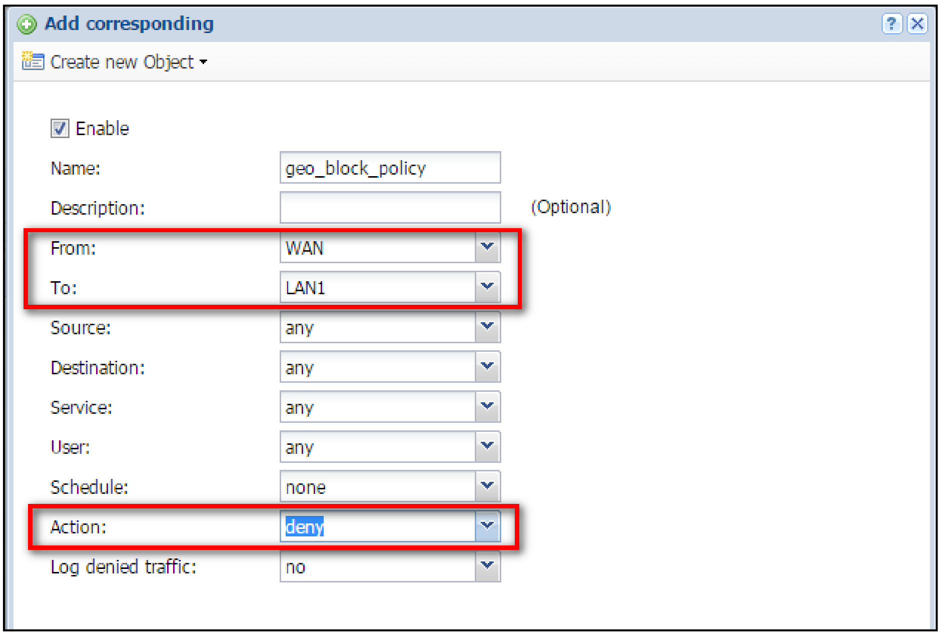


Edit Policy1

☑ Enable

Name:	geo_allow_policy	
Description:		(Optional)
From:	WAN	
To:	LAN1	
Source:	Taiwan	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	log	

2. Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set traffic from WAN to LAN deny (geo_block_policy in this example).



Add corresponding

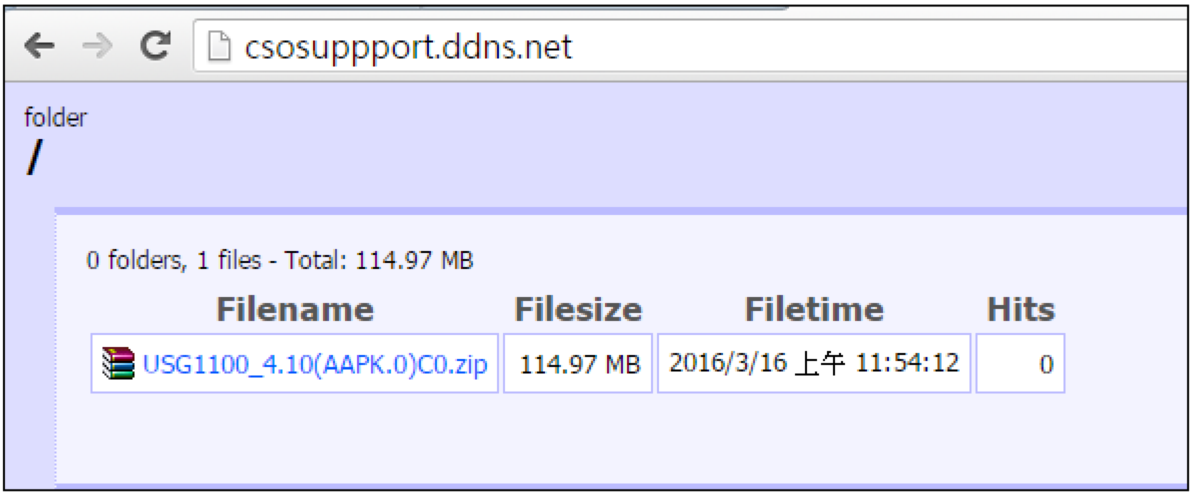
Create new Object

☑ Enable

Name:	geo_block_policy
Description:	(Optional)
From:	WAN
To:	LAN1
Source:	any
Destination:	any
Service:	any
User:	any
Schedule:	none
Action:	deny
Log denied traffic:	no

Test the Result

1. Type http://csosuppport.ddns.net/ into the browser, and the http can be reached.



csosuppport.ddns.net

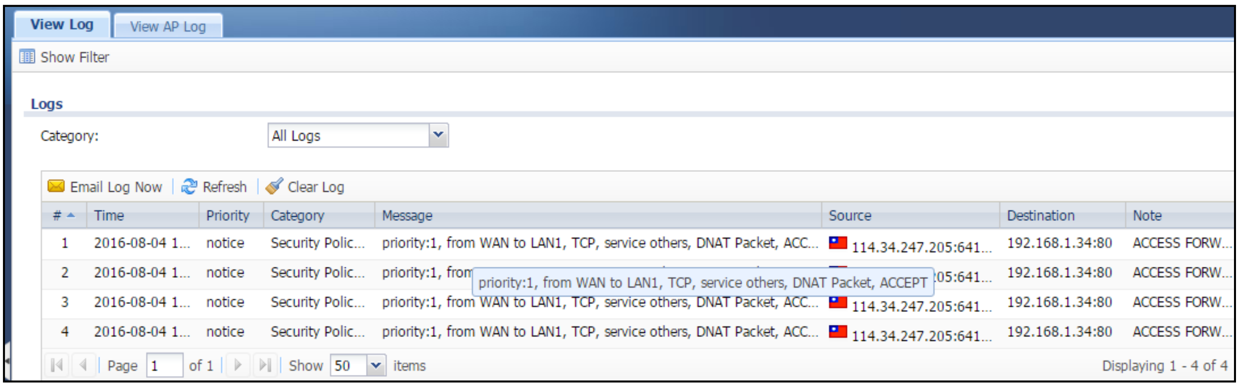
folder

/

0 folders, 1 files - Total: 114.97 MB

Filename	Filesize	Filetime	Hits
USG1100_4.10(AAPK.0)C0.zip	114.97 MB	2016/3/16 上午 11:54:12	0

2. Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] log message such as below. Traffic matches Geo IP policy will be blocked and shows in message field.



Category: All Logs

#	Time	Priority	Category	Message	Source	Destination	Note
1	2016-08-04 1...	notice	Security Polic...	priority:1, from WAN to LAN1, TCP, service others, DNAT Packet, ACC...	114.34.247.205:641...	192.168.1.34:80	ACCESS FORW...
2	2016-08-04 1...	notice	Security Polic...	priority:1, from	05:641...	192.168.1.34:80	ACCESS FORW...
3	2016-08-04 1...	notice	Security Polic...	priority:1, from WAN to LAN1, TCP, service others, DNAT Packet, ACC...	114.34.247.205:641...	192.168.1.34:80	ACCESS FORW...
4	2016-08-04 1...	notice	Security Polic...	priority:1, from WAN to LAN1, TCP, service others, DNAT Packet, ACC...	114.34.247.205:641...	192.168.1.34:80	ACCESS FORW...

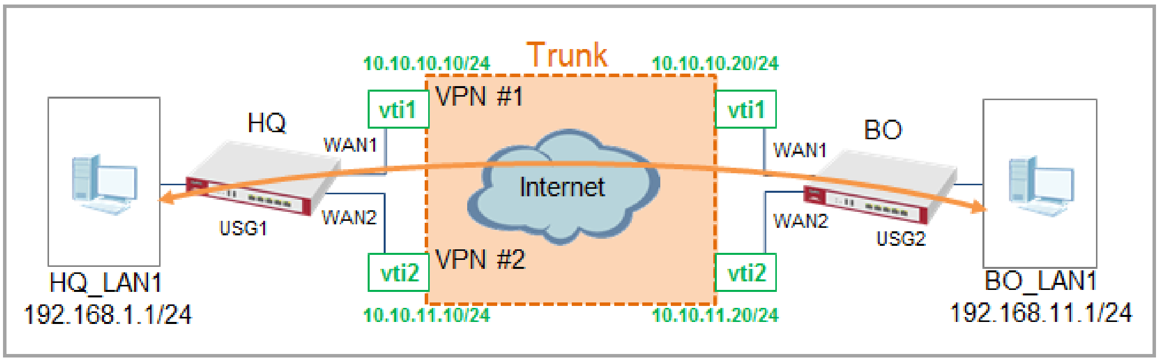
priority:1, from WAN to LAN1, TCP, service others, DNAT Packet, ACCEPT

Page 1 of 1 | Show 50 items | Displaying 1 - 4 of 4

Scenario 16 — VPN Failover with VTI

16.1 How to Create a VTI for VPN Tunnel

With VTI (Virtual Tunnel Interface), the user can create an interface for the VPN tunnel. Through VTI, the VPN tunnel can be managed as an interface with more flexibility. It allows the user to configure a trunk with VTI to achieve VPN load balancing. Besides, the user can configure a policy route or static route by selecting the VTI as the next-hop. Furthermore, it allows the user to configure the BWM rule with a VTI object. This example illustrates how to create a VTI object and configure a policy route with the VTI. Furthermore, it applies the VTI to the WAN trunk to achieve VPN load balancing.



VTI Deployment Flow

1 Configure the VPN gateways.

2. Configure a VPN tunnel for each VPN gateway with the application scenario **VPN Tunnel Interface**.
3. Create a VTI for each VPN tunnel.
4. Create a trunk with the VTIs.
5. Configure a policy route.
6. Connect the VPN tunnels.

Configuration Guide

Network Conditions

USG1
- WAN1 IP: 10.251.31.114
- WAN2 IP: 10.251.31.167
- VTI 1: 10.10.10.10
- VTI 2: 10.10.11.10
- LAN1: 192.168.1.0/24

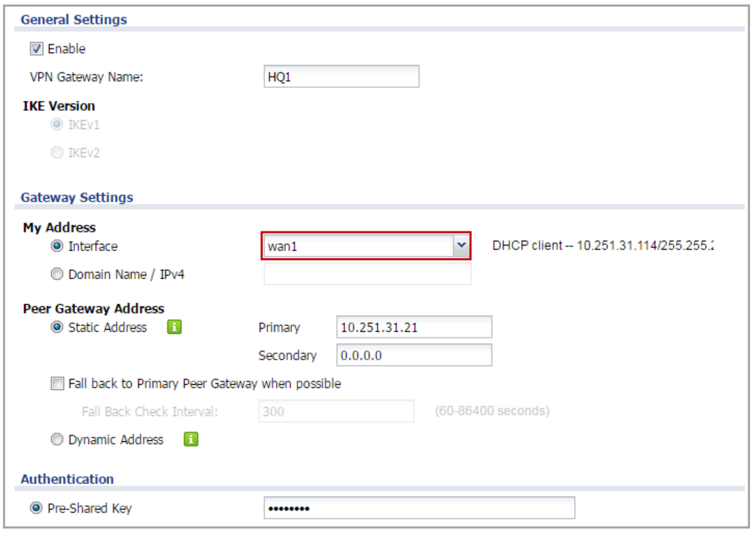
USG2
- WAN1 IP: 10.251.31.21
- WAN2 IP: 10.251.31.107
- VTI 1: 10.10.10.20
- VTI 2: 10.10.11.10
- LAN1: 192.168.11.0/24

On **USG1**:

(1) Configure the VPN gateways

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add**.

Create the VPN gateway **HQ1** with **wan1**.



General Settings

☑ Enable

VPN Gateway Name: HQ1

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface: wan1 — DHCP client -- 10.251.31.114/255.255.:

○ Domain Name / IPv4

Peer Gateway Address

● Static Address — Primary: 10.251.31.21 — Secondary: 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

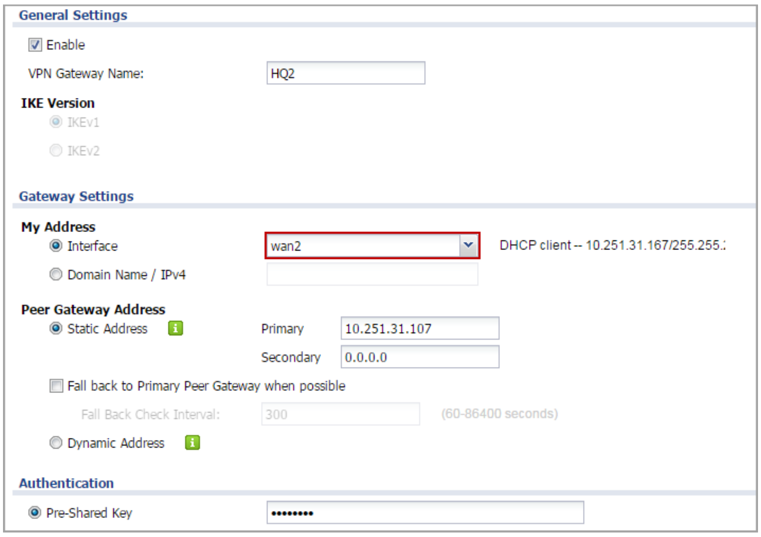
Fall Back Check Interval: 300 (60-86400 seconds)

○ Dynamic Address

Authentication

● Pre-Shared Key: ••••••••

In the same screen, create the VPN gateway **HQ2** with **wan2**.



General Settings

☑ Enable

VPN Gateway Name: HQ2

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface: wan2 — DHCP client -- 10.251.31.167/255.255.:

○ Domain Name / IPv4

Peer Gateway Address

● Static Address — Primary: 10.251.31.107 — Secondary: 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

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

○ Dynamic Address

Authentication

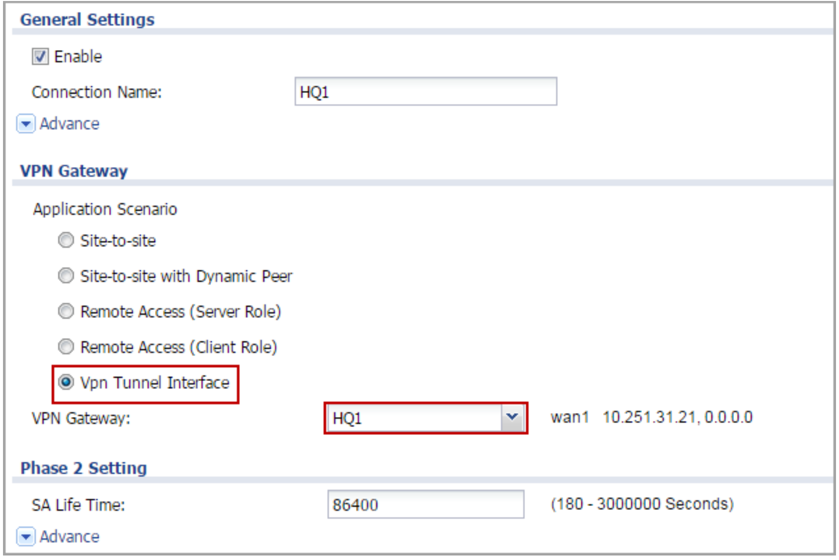
● Pre-Shared Key: ••••••••

(2) Configure the VPN tunnels

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add**.

Create a VPN tunnel for the VPN gateway **HQ1**.

Select **VPN Tunnel Interface** as the application scenario.



General Settings

☑ Enable

Connection Name: HQ1

Advance

VPN Gateway

Application Scenario

○ Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

● Vpn Tunnel Interface

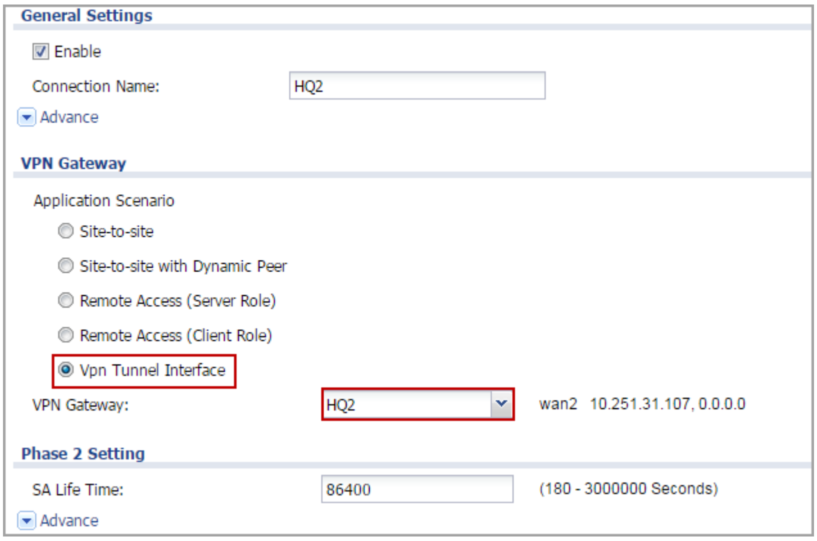
VPN Gateway: HQ1 wan1 10.251.31.21, 0.0.0.0

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

Advance

In the same screen, create a VPN tunnel for the VPN gateway **HQ2**. Select **VPN tunnel Interface** as the application scenario.



General Settings

☑ Enable

Connection Name: HQ2

Advance

VPN Gateway

Application Scenario

○ Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

● Vpn Tunnel Interface

VPN Gateway: HQ2 wan2 10.251.31.107, 0.0.0.0

Phase 2 Setting

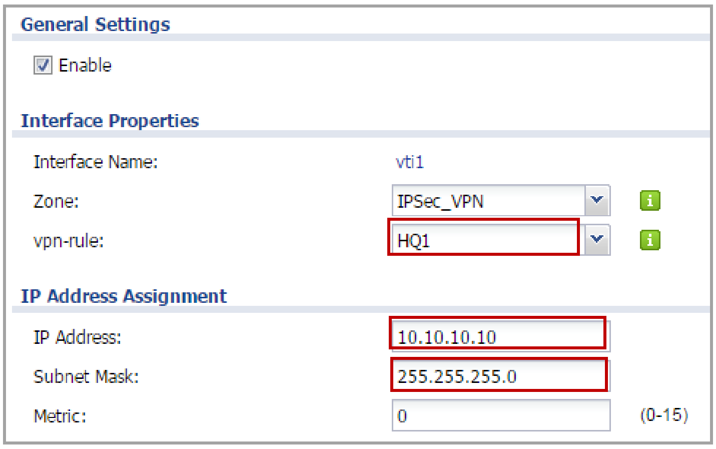
SA Life Time: 86400 (180 - 3000000 Seconds)

Advance

(3) Create VTIs

Go to **CONFIGURATION > Network > Interface > VTI > Add.**

Create a VTI for the VPN tunnel **HQ1**.



General Settings

☑ Enable

Interface Properties

Interface Name: vti1

Zone: IPSec_VPN

vpn-rule: HQ1

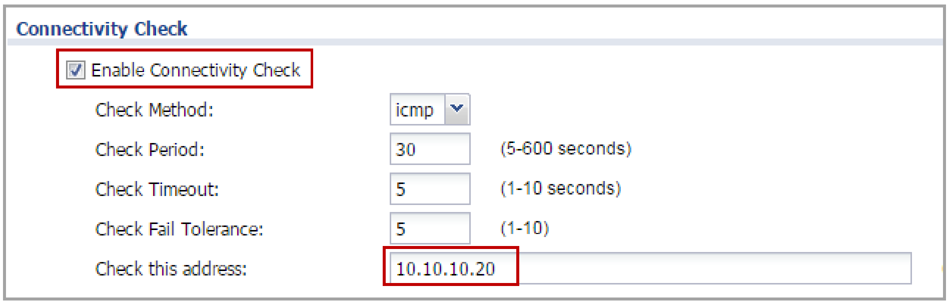
IP Address Assignment

IP Address: 10.10.10.10

Subnet Mask: 255.255.255.0

Metric: 0 (0-15)

Enable the connectivity check. Enter the IP address of **vti1**, which is configured on **USG2**.

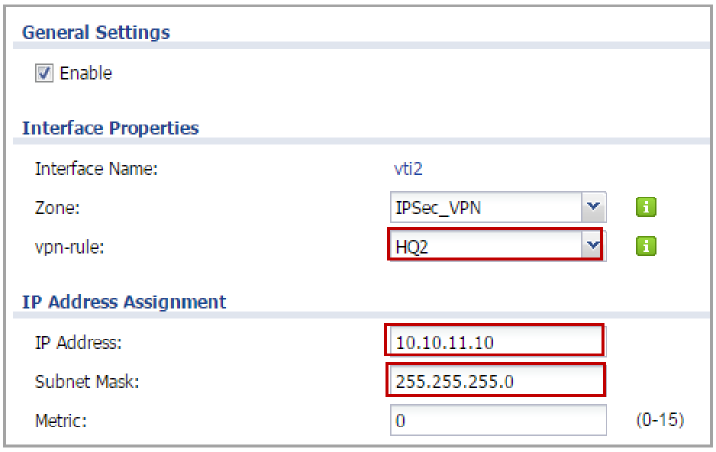


Connectivity Check

☑ Enable Connectivity Check

Check Method:	icmp	
Check Period:	30	(5-600 seconds)
Check Timeout:	5	(1-10 seconds)
Check Fail Tolerance:	5	(1-10)
Check this address:	10.10.10.20	

In the same screen, create a VTI for the VPN tunnel **HQ2**.



General Settings

☑ Enable

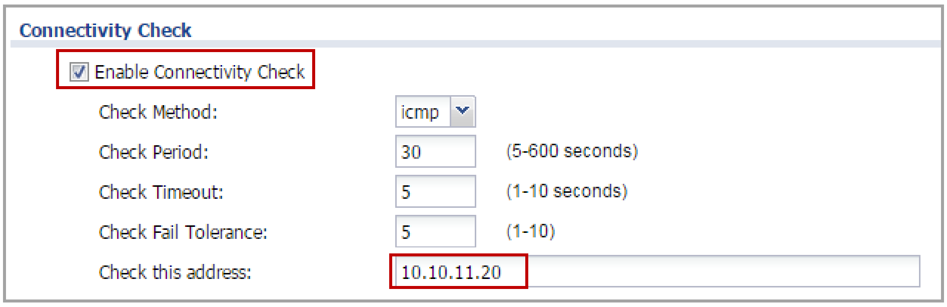
Interface Properties

Interface Name:	vti2	
Zone:	IPSec_VPN	
vpn-rule:	HQ2	

IP Address Assignment

IP Address:	10.10.11.10	
Subnet Mask:	255.255.255.0	
Metric:	0	(0-15)

Enable the connectivity check. Enter the IP address of **vti2**, which is configured on **USG2**.



Connectivity Check

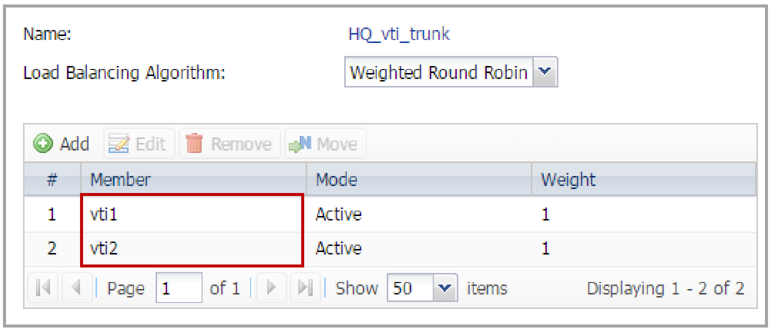
☑ Enable Connectivity Check

Check Method:	icmp	
Check Period:	30	(5-600 seconds)
Check Timeout:	5	(1-10 seconds)
Check Fail Tolerance:	5	(1-10)
Check this address:	10.10.11.20	

(4) Create a new trunk

Go to **CONFIGURATION > Network > Interface > Trunk > User Configuration > Add**.

Add **vti1** and **vti2** to the new trunk.



Name:	HQ_vti_trunk
Load Balancing Algorithm:	Weighted Round Robin

#	Member	Mode	Weight
1	vti1	Active	1
2	vti2	Active	1

(5) Configure a policy route

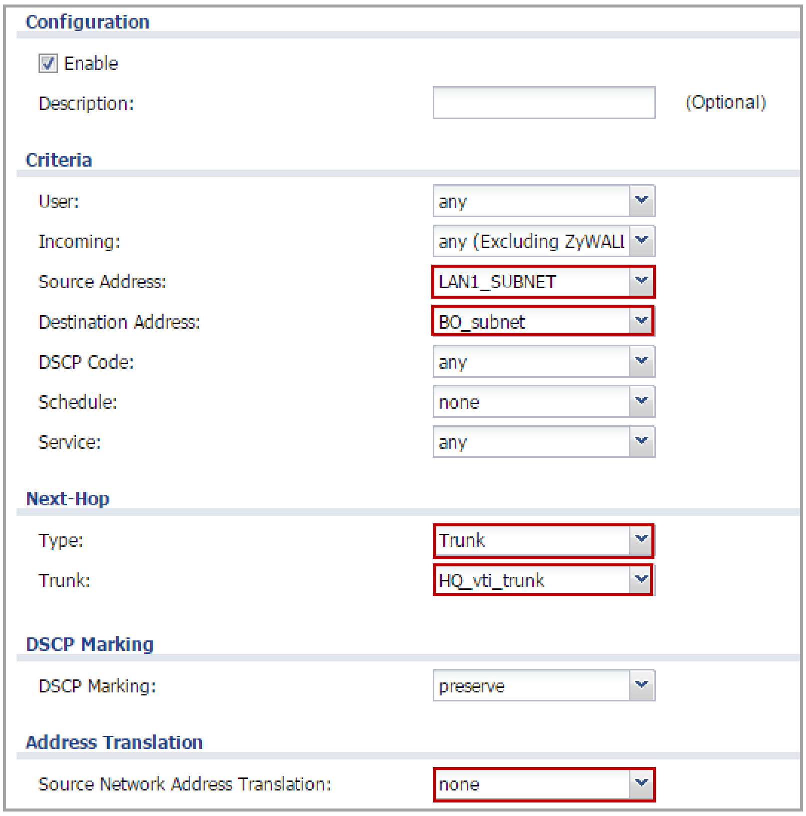
Go to **CONFIGURATION > Network > Routing > Policy Route > Add** and enter the following parameters.

Source Address: LAN1_SUBNET (192.168.1.0/24)

Destination Address: BO_subnet (192.168.11.0/24)

Next-Hop: HQ_vti_trunk

SNAT: none



Configuration

☑ Enable

Description:		(Optional)

Criteria

User:	any
Incoming:	any (Excluding ZyWALL
Source Address:	LAN1_SUBNET
Destination Address:	BO_subnet
DSCP Code:	any
Schedule:	none
Service:	any

Next-Hop

Type:	Trunk
Trunk:	HQ_vti_trunk

DSCP Marking

DSCP Marking:	preserve

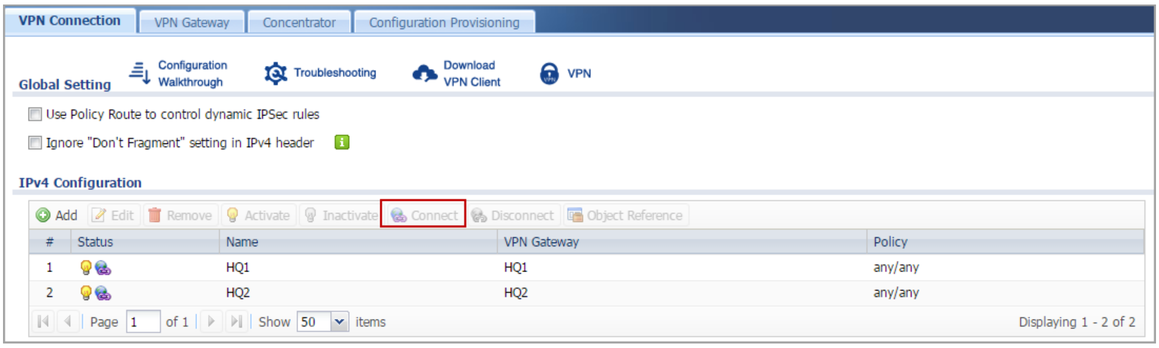
Address Translation

Source Network Address Translation:	none

(6) Connect the VPN tunnels

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection**.

Connect the VPN tunnels when the VTIs are ready.



Global Setting

□ Use Policy Route to control dynamic IPSec rules

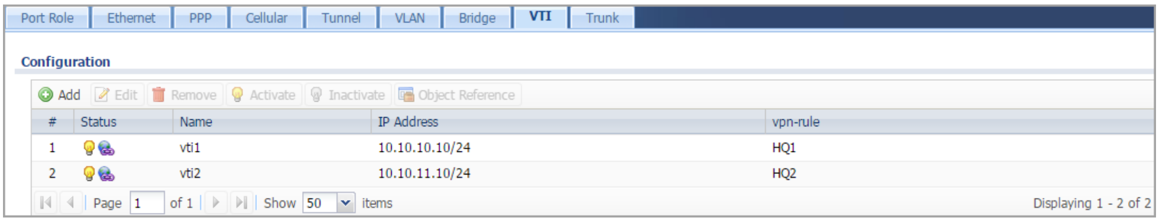
□ Ignore "Don't Fragment" setting in IPv4 header

IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1		HQ1	HQ1	any/any
2		HQ2	HQ2	any/any

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

In the **CONFIGURATION > Network > Interface > VTI** screen, you should be able to see that the status of the VTI is up when the corresponding VPN tunnel is established.



Configuration

#	Status	Name	IP Address	vpn-rule
1		vti1	10.10.10.10/24	HQ1
2		vti2	10.10.11.10/24	HQ2

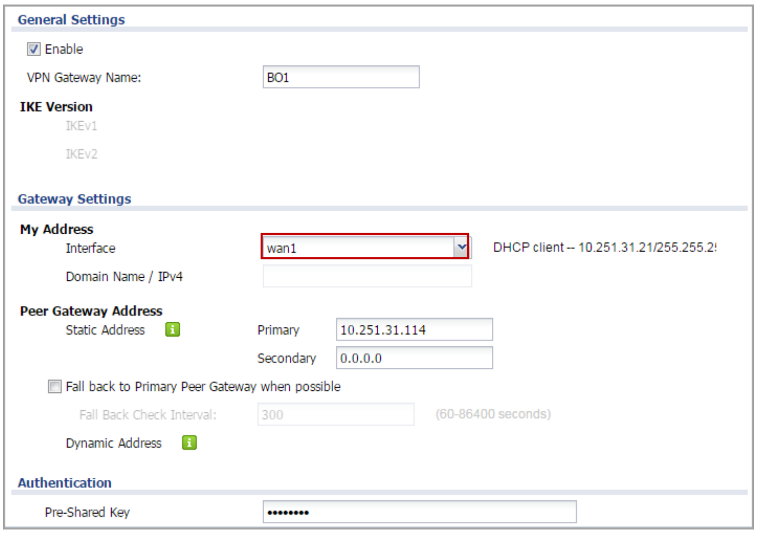
Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

On **USG2**:

(1) Configure the VPN gateways

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add**.

Create the VPN gateway **BO1** with **wan1**.



General Settings

☑ Enable

VPN Gateway Name: BO1

IKE Version

IKEv1

IKEv2

Gateway Settings

My Address

Interface wan1 DHCP client -- 10.251.31.21/255.255.2

Domain Name / IPv4

Peer Gateway Address

Static Address Primary 10.251.31.114

Secondary 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

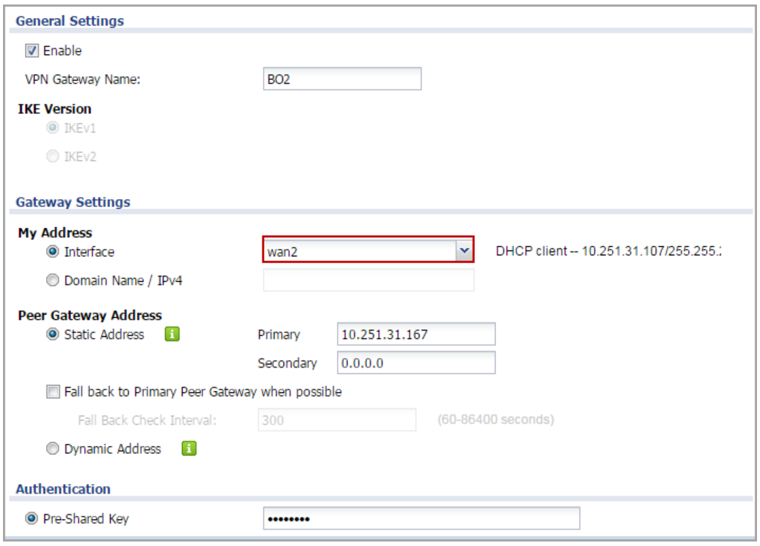
Fall Back Check Interval: 300 (60-86400 seconds)

Dynamic Address

Authentication

Pre-Shared Key ••••••••

In the same screen, create the VPN gateway **BO2** with **wan2**.



General Settings

☑ Enable

VPN Gateway Name: BO2

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface wan2 DHCP client -- 10.251.31.107/255.255.

○ Domain Name / IPv4

Peer Gateway Address

● Static Address Primary 10.251.31.167

Secondary 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

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

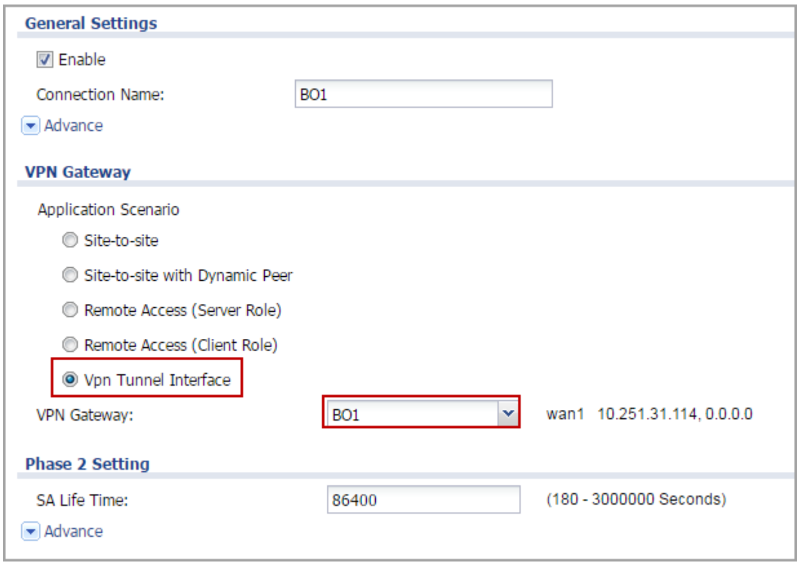
○ Dynamic Address

Authentication

● Pre-Shared Key ••••••••

(2) Configure the VPN tunnels

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add**.
Create a VPN tunnel for the VPN gateway **BO1**.
Select **VPN tunnel Interface** as the application scenario.



General Settings

☑ Enable

Connection Name: BO1

Advance

VPN Gateway

Application Scenario

○ Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

● Vpn Tunnel Interface

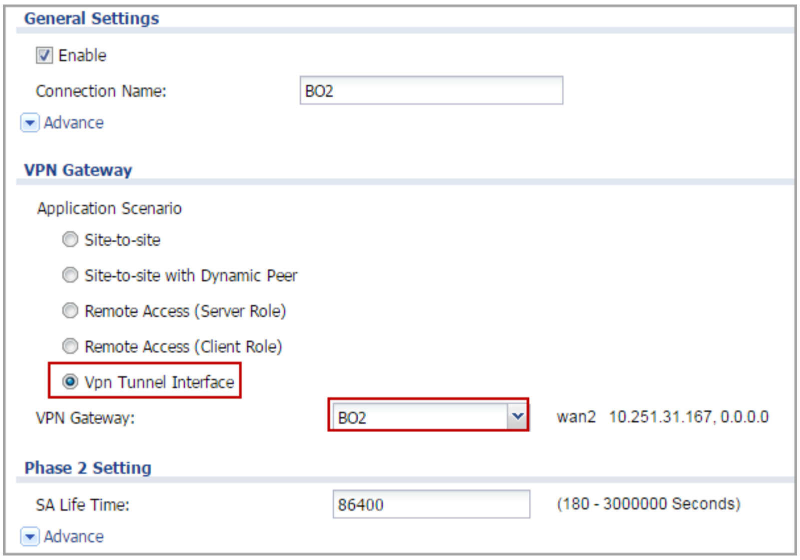
VPN Gateway: BO1 wan1 10.251.31.114, 0.0.0.0

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

Advance

In the same screen, create a VPN tunnel for the VPN gateway **BO2**.
Select **VPN tunnel Interface** as the application scenario.



General Settings

☑ Enable

Connection Name: BO2

Advance

VPN Gateway

Application Scenario

○ Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

● Vpn Tunnel Interface

VPN Gateway: BO2 wan2 10.251.31.167, 0.0.0.0

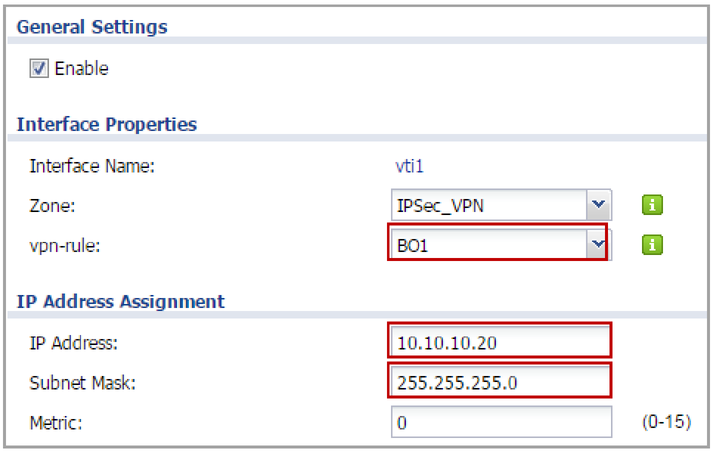
Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

Advance

(3) Create VTIs

Create a VTI for the VPN tunnel **BO1** in the **CONFIGURATION > Network > Interface > VTI > Add** screen.
Be aware that the IP address of this VTI must be in the same subnet as **vti1** on **USG1**. In this example, the IP address and subnet mask of **vti1** on **USG1** is **10.10.10.10** and **255.255.255.0** respectively. The IP address of **vti1** on **USG2** must be in the subnet of **10.10.10.0/24**.



General Settings

☑ Enable

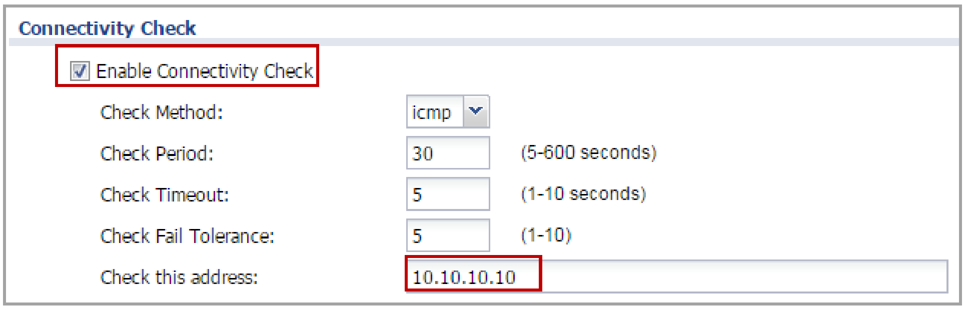
Interface Properties

Interface Name:	vti1
Zone:	IPSec_VPN
vpn-rule:	BO1

IP Address Assignment

IP Address:	10.10.10.20	
Subnet Mask:	255.255.255.0	
Metric:	0	(0-15)

Enable the connectivity check. Enter the IP address of **vti1**, which is configured on **USG1**.

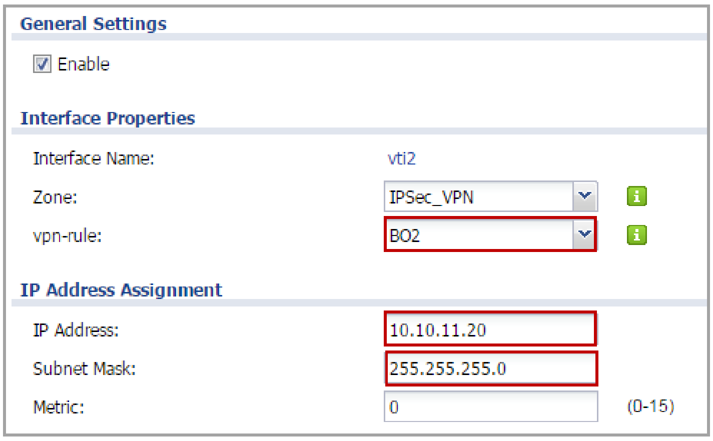


Connectivity Check

☑ Enable Connectivity Check

Check Method:	icmp	
Check Period:	30	(5-600 seconds)
Check Timeout:	5	(1-10 seconds)
Check Fail Tolerance:	5	(1-10)
Check this address:	10.10.10.10	

In the same screen, create a VTI for the VPN tunnel **BO2**.
Be aware that the IP address of this VTI must be in the same subnet as **vti2** on **USG1**. In this example, the IP address and subnet mask of **vti2** on **USG1** is **10.10.11.10** and **255.255.255.0** respectively. The IP address of **vti2** on **USG2** must be in the subnet of **10.10.11.0/24**.



General Settings

☑ Enable

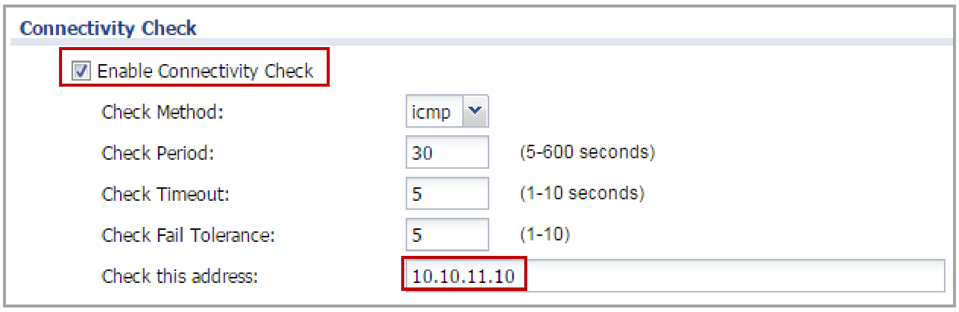
Interface Properties

Interface Name:	vti2
Zone:	IPSec_VPN
vpn-rule:	BO2

IP Address Assignment

IP Address:	10.10.11.20	
Subnet Mask:	255.255.255.0	
Metric:	0	(0-15)

Enable the connectivity check. Enter the IP address of **vti2**, which is configured on **USG1**.



Connectivity Check

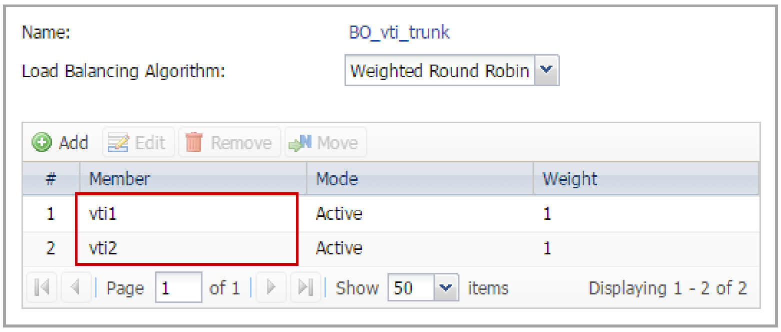
☑ Enable Connectivity Check

Check Method:	icmp	
Check Period:	30	(5-600 seconds)
Check Timeout:	5	(1-10 seconds)
Check Fail Tolerance:	5	(1-10)
Check this address:	10.10.11.10	

(4) Create a new trunk

Go to **CONFIGURATION** > **Network** > **Interface** > **Trunk** > **User Configuration** > **Add**.

Add **vti1** and **vti2** to the new trunk.



Name: BO_vti_trunk

Load Balancing Algorithm: Weighted Round Robin

#	Member	Mode	Weight
1	vti1	Active	1
2	vti2	Active	1

(5) Configure a policy route

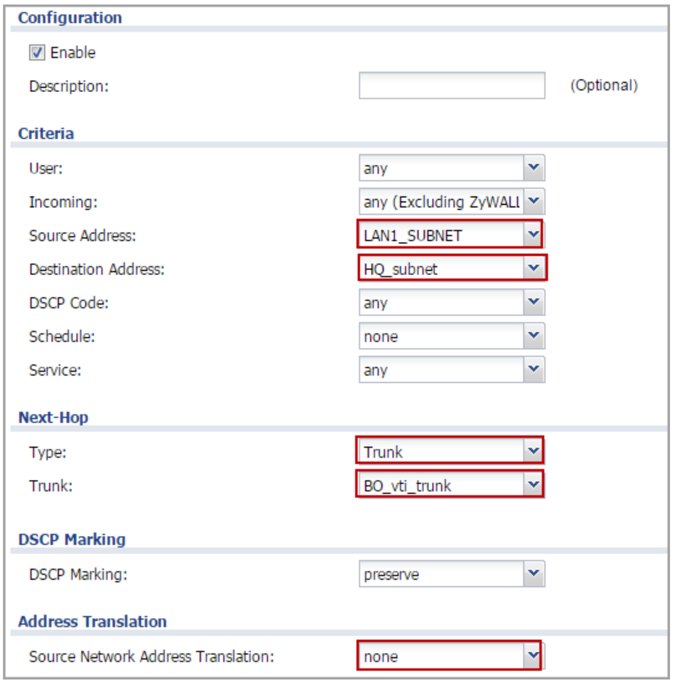
Go to **CONFIGURATION** > **Network** > **Routing** > **Policy Route** > **Add** and enter the following parameters.

Source Address: LAN1_SUBNET (192.168.11.0/24)

Destination Address: HQ_subnet (192.168.1.0/24)

Next-Hop: BO_vti_trunk

SNAT: none



Configuration

☑ Enable

Description: (Optional)

Criteria

User:	any
Incoming:	any (Excluding ZyWALL
Source Address:	LAN1_SUBNET
Destination Address:	HQ_subnet
DSCP Code:	any
Schedule:	none
Service:	any

Next-Hop

Type:	Trunk
Trunk:	BO_vti_trunk

DSCP Marking

DSCP Marking: preserve

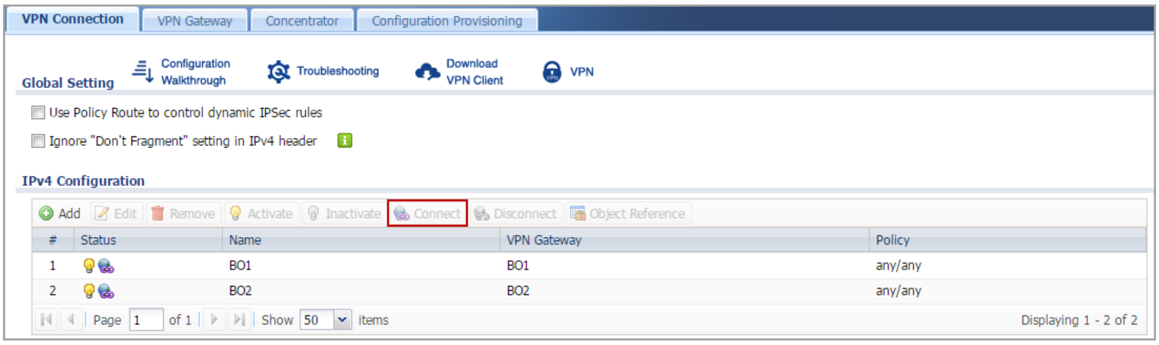
Address Translation

Source Network Address Translation: none

(6) Connect the VPN tunnels

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection**.

Connect the VPN tunnels when the VTIs are ready.



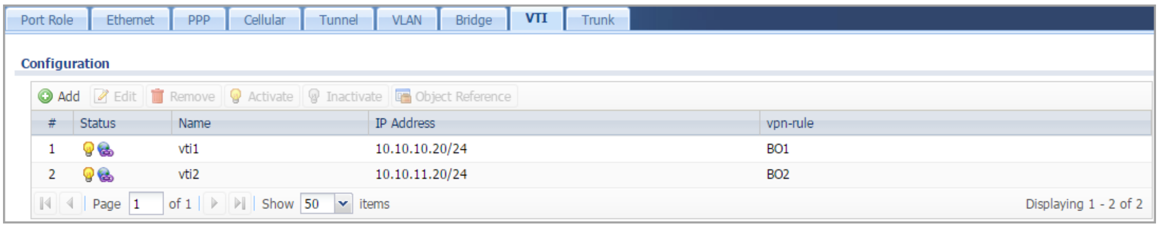
□ Use Policy Route to control dynamic IPSec rules

□ Ignore "Don't Fragment" setting in IPv4 header

#	Status	Name	VPN Gateway	Policy
1		BO1	BO1	any/any
2		BO2	BO2	any/any

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

Go to **CONFIGURATION > Network > Interface > VTI**. You will see that the status of the VTI is up when the corresponding VPN tunnel is established.



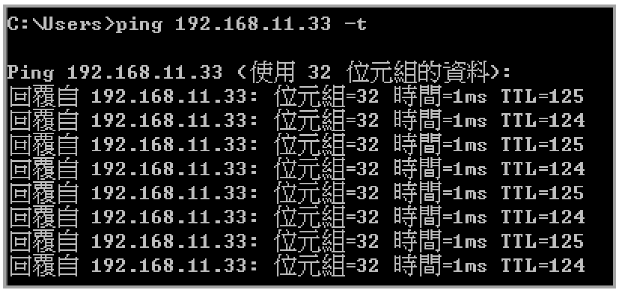
#	Status	Name	IP Address	vpn-rule
1		vti1	10.10.10.20/24	BO1
2		vti2	10.10.11.20/24	BO2

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

16.2 Verification

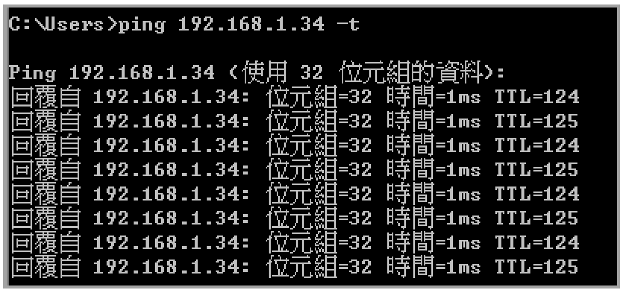
Task 1: The PC in LAN1 of **USG1** is able to ping the PC in LAN1 of **USG2** and vice versa.

PC of **USG1**: 192.168.1.34



```
C:\Users>ping 192.168.11.33 -t

Ping 192.168.11.33 (使用 32 位元組的資料):
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
```

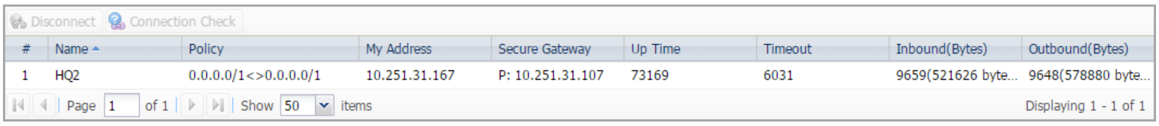
PC of **USG2**: 192.168.11.33



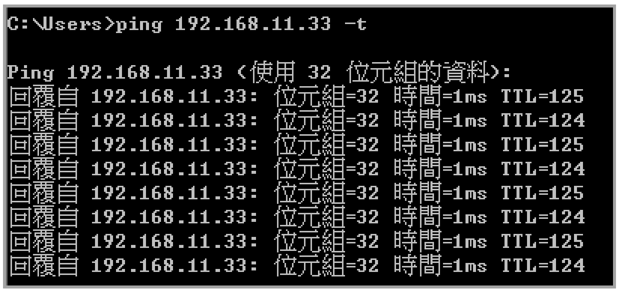
```
C:\Users>ping 192.168.1.34 -t

Ping 192.168.1.34 (使用 32 位元組的資料):
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
```

Task 2: Unplug **wan1** of **USG1**. The PC in LAN1 of **USG1** is still able to ping the PC in LAN1 of **USG2** and vice versa because the VTI trunk is used as the next-hop in the policy route.

Check the status of the **USG1** PC (192.168.1.34) in the **MONITOR > VPN Monitor > IPSec** screen.

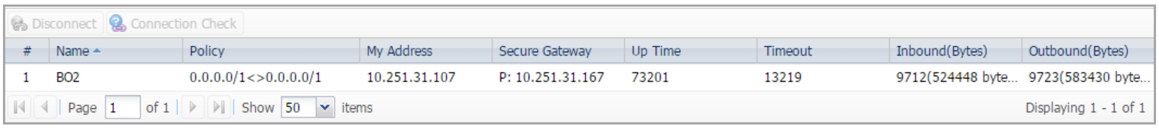


#	Name	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound(Bytes)	Outbound(Bytes)
1	HQ2	0.0.0.0/1<>0.0.0.0/1	10.251.31.167	P: 10.251.31.107	73169	6031	9659(521626 byte...	9648(578880 byte...

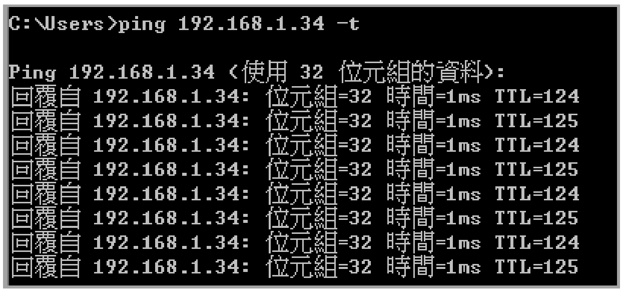


```
C:\Users>ping 192.168.11.33 -t

Ping 192.168.11.33 (使用 32 位元組的資料):
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
```

Check the status of the **USG2** PC (192.168.11.33) in the **MONITOR > VPN Monitor > IPSec** screen.



#	Name	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound(Bytes)	Outbound(Bytes)
1	BO2	0.0.0.0/1<>0.0.0.0/1	10.251.31.107	P: 10.251.31.167	73201	13219	9712(524448 byte...	9723(583430 byte...

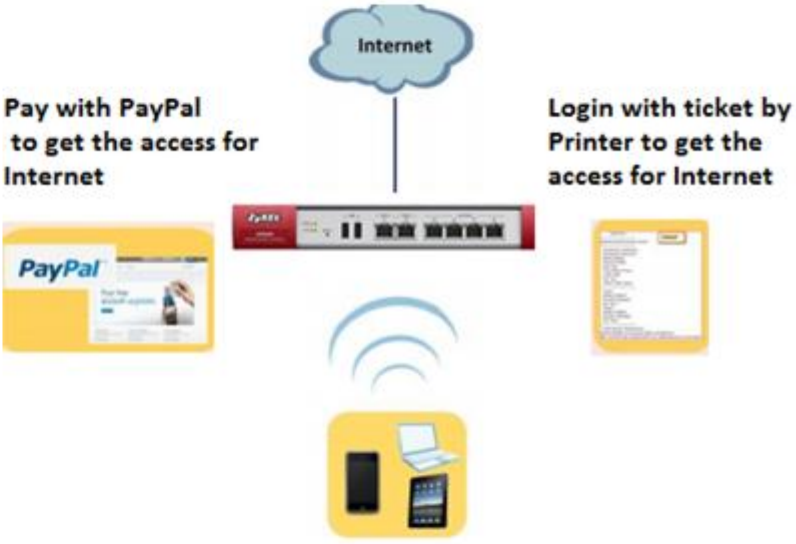


```
C:\Users>ping 192.168.1.34 -t

Ping 192.168.1.34 (使用 32 位元組的資料):
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
```

Scenario 17 – How to Activate a Paid Access Hotspot

17.1 Application Scenario

In this scenario, many customers need to access the Internet via a paid hotspot. The USG1100 can manage access to the Internet effectively. There are two ways to achieve this on the USG1100; one method is to use a printer, and the other is to use the PayPal payment service. Customers who use the PayPal payment service can pay with their PayPal account to access the Internet. As for the printer, customers can purchase tickets that are generated by a thermal printer from the store or hotel's reception desk. By using the account and password information on the tickets, customers can access the Internet with a web browser.


Internet
Pay with PayPal to get the access for Internet
Login with ticket by Printer to get the access for Internet
PayPal

17.2 Configuration Guide

Network Conditions

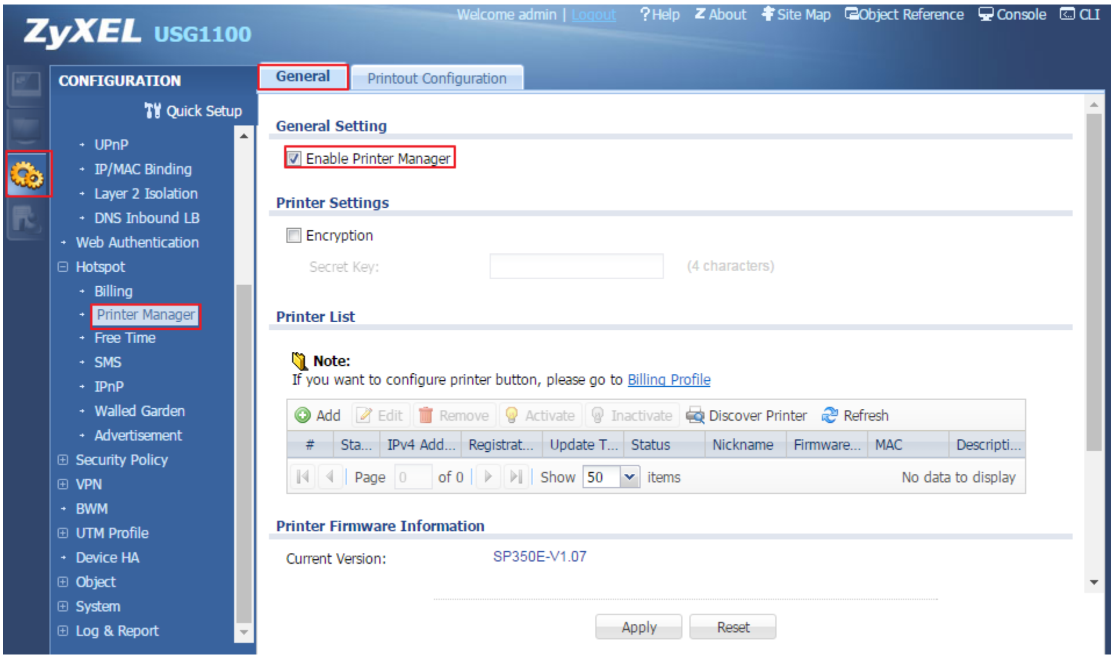
- SP350E:
- Default IP address (DHCP): 192.168.2.4
- User name: admin
- Password: 1234
- Port number: 9100

Printing a Ticket for Accessing the Internet

Configurations on the USG1100:

1. Configure the **Printer Manager** screen settings on the USG1100.

   (1) Go to **Configuration** > **Printer Manager** > **General**.



General Setting

☑ Enable Printer Manager

Printer Settings

☐ Encryption

Secret Key: (4 characters)

Printer List

Note:
If you want to configure printer button, please go to Billing Profile

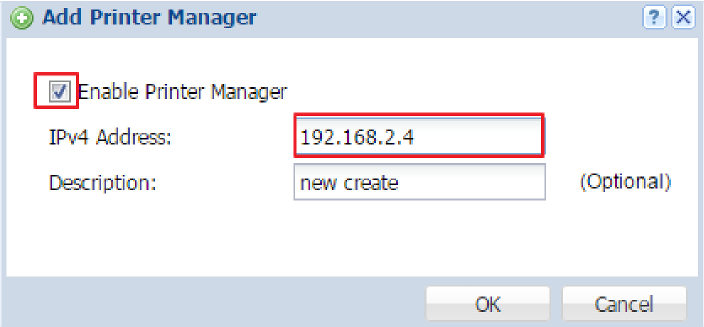
#	Sta...	IPv4 Add...	Registrat...	Update T...	Status	Nickname	Firmware...	MAC	Descripti...

Page 0 of 0 | Show 50 items | No data to display

Printer Firmware Information

Current Version: SP350E-V1.07

   (2) Enable the printer manager and add the printer by entering its IP address. Click **OK**.

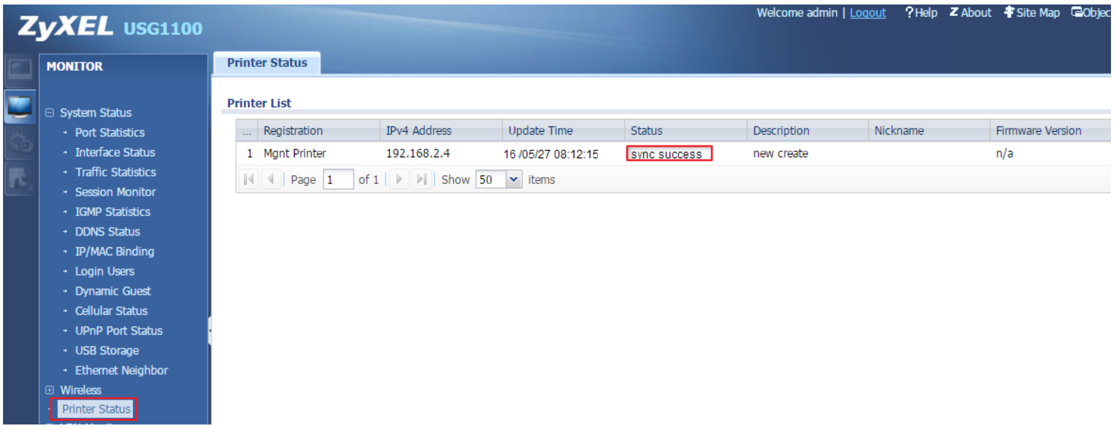


☑ Enable Printer Manager

IPv4 Address: 192.168.2.4

Description: new create (Optional)

2. Go to **Configuration** > **Monitor** > **Printer Status**. Check if the status of the printer shows “sync success“.

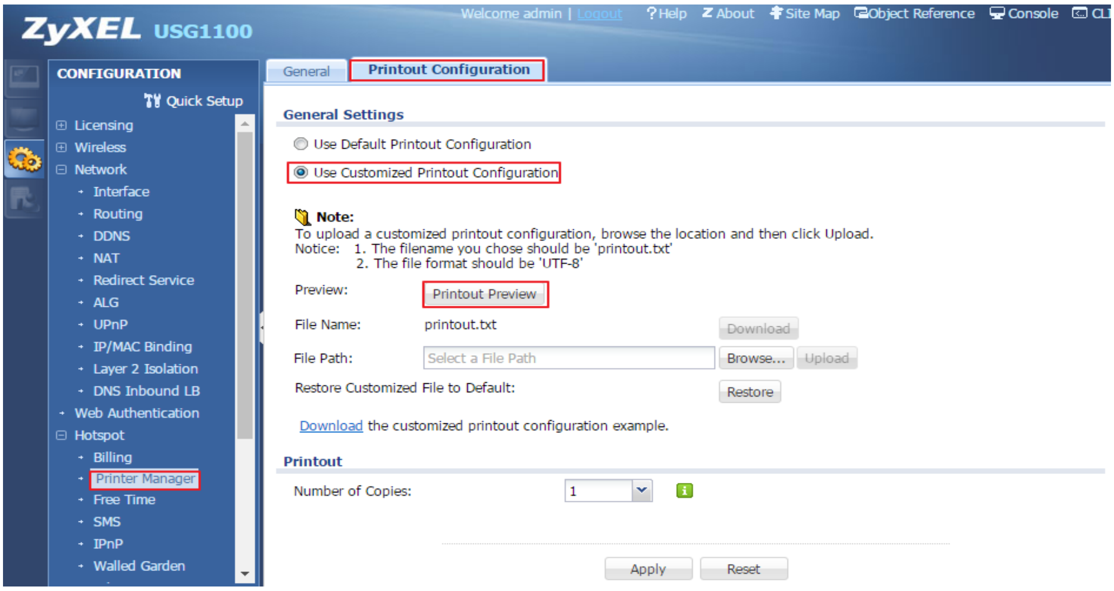


Printer List

...	Registration	IPv4 Address	Update Time	Status	Description	Nickname	Firmware Version
1	Mgnt Printer	192.168.2.4	16 /05/27 08:12:15	sync success	new create		n/a

Page 1 of 1 | Show 50 items

3. Go to **Configuration** > **Printer Manager** > **Printout Configuration**. In this screen, you can choose whether you want to use the default printout configuration or a customized one. If you choose **Use Customized Printout Configuration**, you can customize the ticket information by downloading the example and modifying the ticket. Then upload the customized printout configuration to the system.



General Settings

○ Use Default Printout Configuration

● Use Customized Printout Configuration

Note:
To upload a customized printout configuration, browse the location and then click Upload.
Notice: 1. The filename you chose should be 'printout.txt'
2. The file format should be 'UTF-8'

Preview: Printout Preview

File Name: printout.txt

File Path: Select a File Path

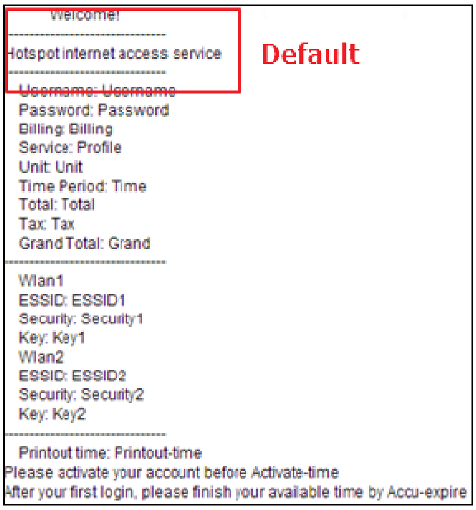
Restore Customized File to Default:

Download the customized printout configuration example.

Printout

Number of Copies: 1

4. Click **Printout Preview** to display a pop-up preview window of the default or customized printout configuration ticket format.



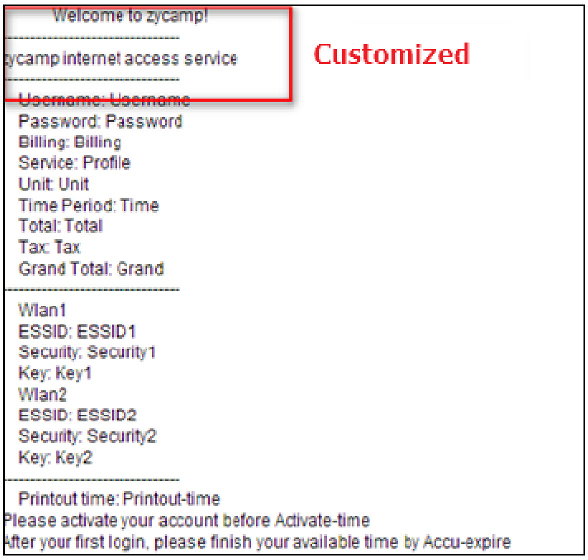
Welcome!

Hotspot internet access service

Username: Username
Password: Password
Billing: Billing
Service: Profile
Unit: Unit
Time Period: Time
Total: Total
Tax: Tax
Grand Total: Grand

Wlan1
ESSID: ESSID1
Security: Security1
Key: Key1
Wlan2
ESSID: ESSID2
Security: Security2
Key: Key2

Printout time: Printout-time
Please activate your account before Activate-time
After your first login, please finish your available time by Accu-expire



Welcome to zycamp!

zycamp internet access service

Username: Username
Password: Password
Billing: Billing
Service: Profile
Unit: Unit
Time Period: Time
Total: Total
Tax: Tax
Grand Total: Grand

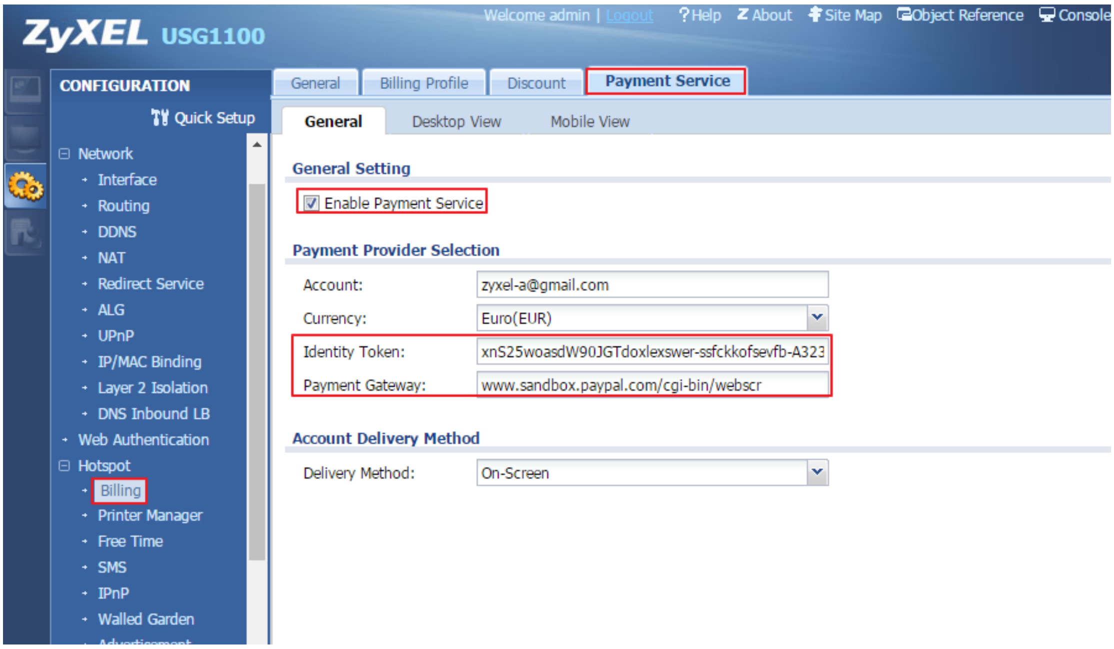
Wlan1
ESSID: ESSID1
Security: Security1
Key: Key1
Wlan2
ESSID: ESSID2
Security: Security2
Key: Key2

Printout time: Printout-time
Please activate your account before Activate-time
After your first login, please finish your available time by Accu-expire

Using the PayPal Payment Service to Access the Internet

Configurations on the USG1100

1. Go to **Configuration** > **Billing** > **Payment Service**. Select **Enable Payment Service** and enter the payment provider's information, which should be provided to you by PayPal after successfully applying for your PayPal account.



General Setting

☑ Enable Payment Service

Payment Provider Selection

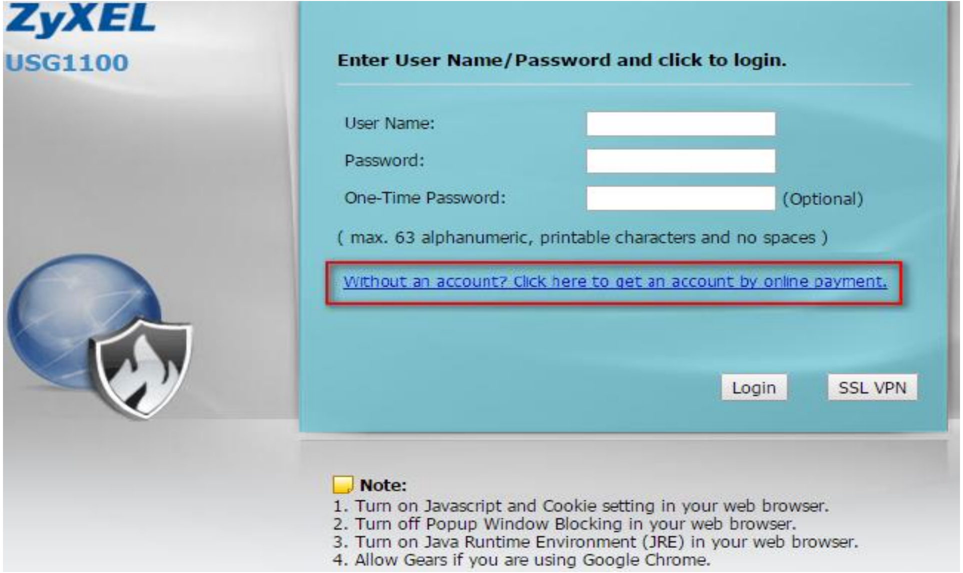
Account:	zyxel-a@gmail.com
Currency:	Euro(EUR)
Identity Token:	xnS25woasdW90JGTdoxlexswer-ssfckkofsevfb-A323
Payment Gateway:	www.sandbox.paypal.com/cgi-bin/webscr

Account Delivery Method

Delivery Method:	On-Screen

2. Test the dynamic account to pay the bill by using the payment function.

   (1) Open the **Login** screen after enabling the payment function. You will see a link to create an account. Click it to be redirected to the billing profile screen.



Enter User Name/Password and click to login.

User Name:

Password:

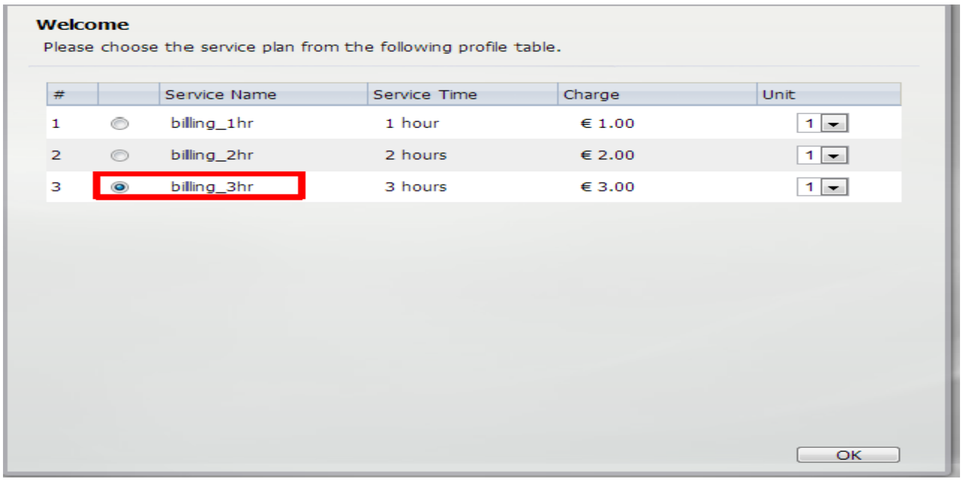
One-Time Password: (Optional)

(max. 63 alphanumeric, printable characters and no spaces)

Without an account? Click here to get an account by online payment.

Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.

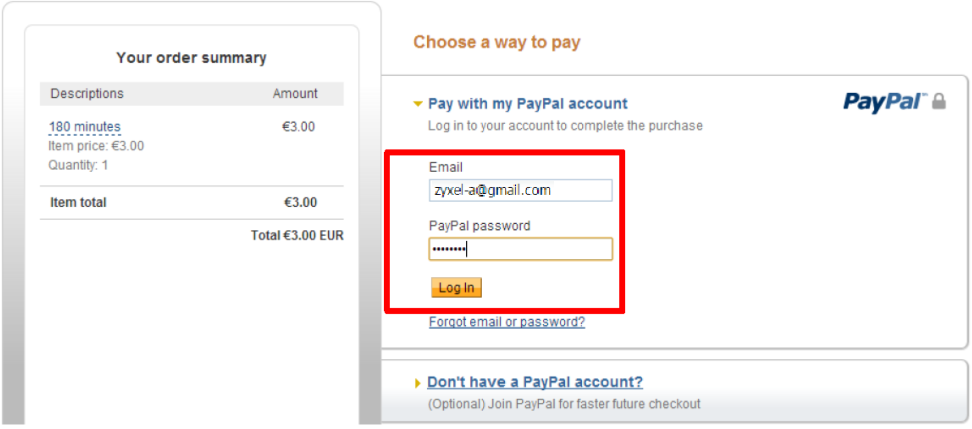
(2) As a test, select the **billing_3hr** billing profile and click **OK**. You will be redirected to the PayPal authentication screen.



Welcome

Please choose the service plan from the following profile table.

#		Service Name	Service Time	Charge	Unit
1	○	billing_1hr	1 hour	€ 1.00	1
2	○	billing_2hr	2 hours	€ 2.00	1
3	●	billing_3hr	3 hours	€ 3.00	1



Your order summary

Descriptions	Amount
180 minutes Item price: €3.00 Quantity: 1	€3.00
Item total	€3.00
	Total €3.00 EUR

Choose a way to pay

Pay with my PayPal account

Log in to your account to complete the purchase

Email: zyxel-a@gmail.com

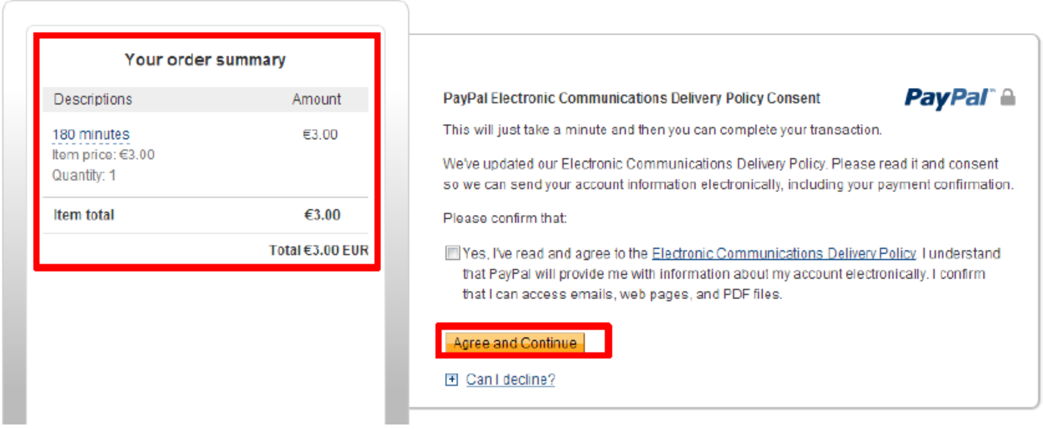
PayPal password: ••••••••

Forgot email or password?

Don't have a PayPal account?

(Optional) Join PayPal for faster future checkout

(4) Log into the PayPal screen to check your order.



Your order summary

Descriptions	Amount
180 minutes Item price: €3.00 Quantity: 1	€3.00
Item total	€3.00
	Total €3.00 EUR

PayPal Electronic Communications Delivery Policy Consent

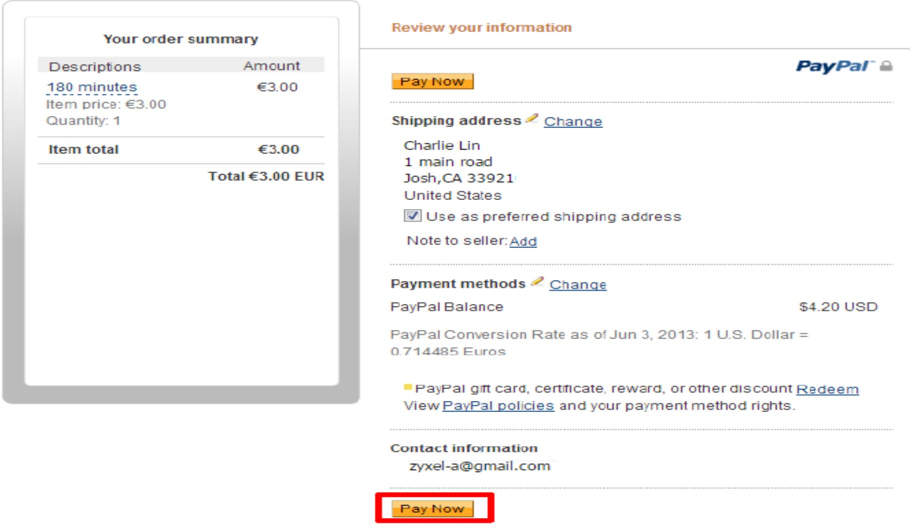
This will just take a minute and then you can complete your transaction.

We've updated our Electronic Communications Delivery Policy. Please read it and consent so we can send your account information electronically, including your payment confirmation.

Please confirm that:

□ Yes, I've read and agree to the Electronic Communications Delivery Policy. I understand that PayPal will provide me with information about my account electronically. I confirm that I can access emails, web pages, and PDF files.

(5) After clicking the **Agree and Continue** button, you can click **Pay Now** to pay the bill.



Your order summary

Descriptions	Amount
180 minutes Item price: €3.00 Quantity: 1	€3.00
Item total	€3.00
	Total €3.00 EUR

Review your information

Shipping address Change

Charlie Lin
1 main road
Josh,CA 33921
United States

☑ Use as preferred shipping address

Note to seller: Add

Payment methods Change

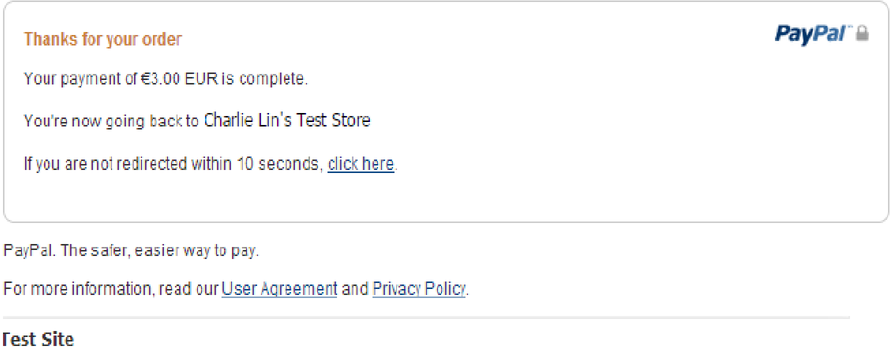
PayPal Balance $4.20 USD

PayPal Conversion Rate as of Jun 3, 2013: 1 U.S. Dollar = 0.714485 Euros

PayPal gift card, certificate, reward, or other discount Redeem
View PayPal policies and your payment method rights.

Contact information
zyxel-a@gmail.com

(6) After clicking the **Pay Now** button, PayPal will display a pop-up window as shown below. After 10 seconds, you will be redirected to the hotspot's login information.



Thanks for your order

Your payment of €3.00 EUR is complete.

You're now going back to Charlie Lin's Test Store

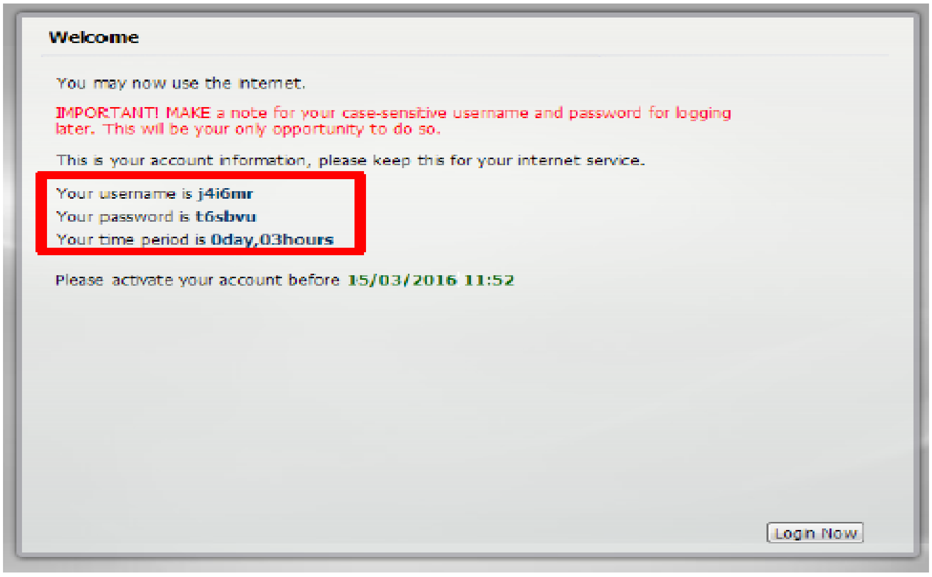
If you are not redirected within 10 seconds, click here.

PayPal. The safer, easier way to pay.

For more information, read our User Agreement and Privacy Policy.

Test Site

(7) Now you can see the login username and password for the hotspot.



Welcome

You may now use the internet.

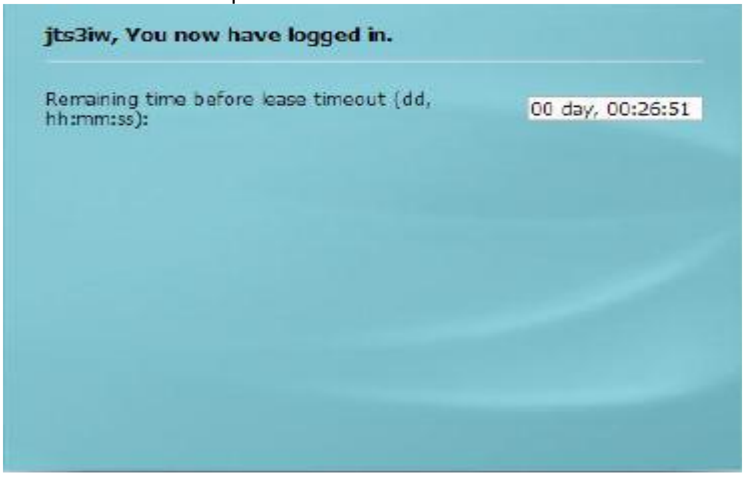
IMPORTANT! MAKE a note for your case-sensitive username and password for logging later. This will be your only opportunity to do so.

This is your account information, please keep this for your internet service.

Your username is **j4i6mr**
Your password is **t6sbvu**
Your time period is **0day,03hours**

Please activate your account before **15/03/2016 11:52**

(8) You can log into the device with the provided username and password during the allocated time period.



jts3iw, You now have logged in.

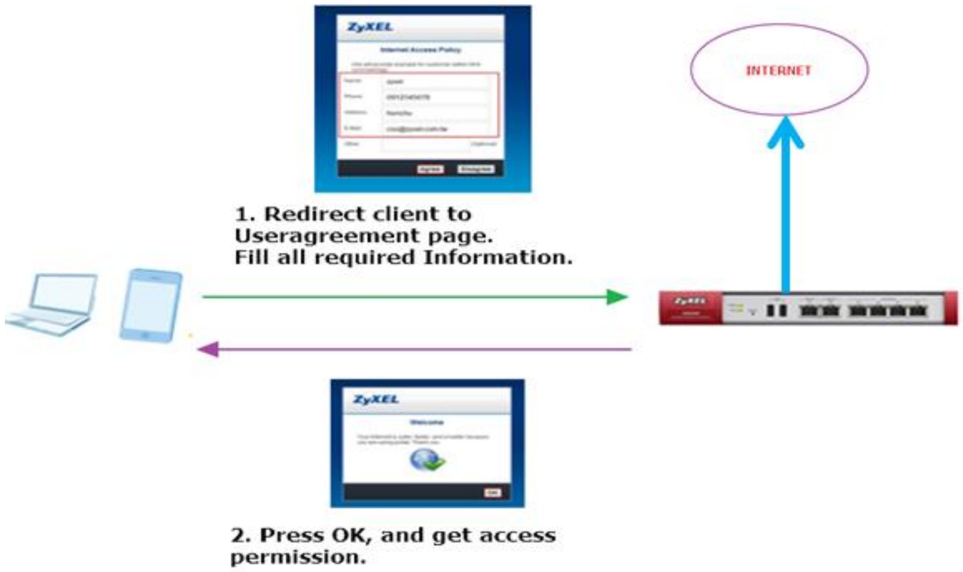
Remaining time before lease timeout (dd, hh:mm:ss): 00 day, 00:26:51

Scenario 18 – How to Activate a Free Access Hotspot

18.1 Application Scenario

Some hotels need to provide free Internet services to hundreds of guests on a daily basis, and managing the Internet access for so many people can be very complicated without the right equipment. With web authentication methods such as user agreement and web portal, hotel guests are redirected to a web-based authentication portal upon the first attempt to access the network. In some countries, the law requires the identification and tracking of users who use public Internet access. The USG1100 can authenticate people by forcing them to receive an authentication code via SMS on their phone. In this way, the USG1100 can authorize the user's Internet access via their mobile phone number and keep track of the device in case of illegal activities via the hotspot. Guests can get free access to the Internet in a matter of seconds simply by entering all required personal contact information and agreeing to the policy of user agreement. If a user that does not have a guest account wants to access the free Internet for a specified period of time, his or her mobile phone number must be entered to receive the guest account information by SMS.

User Agreement



18.2 Configuration Guide

Network Conditions

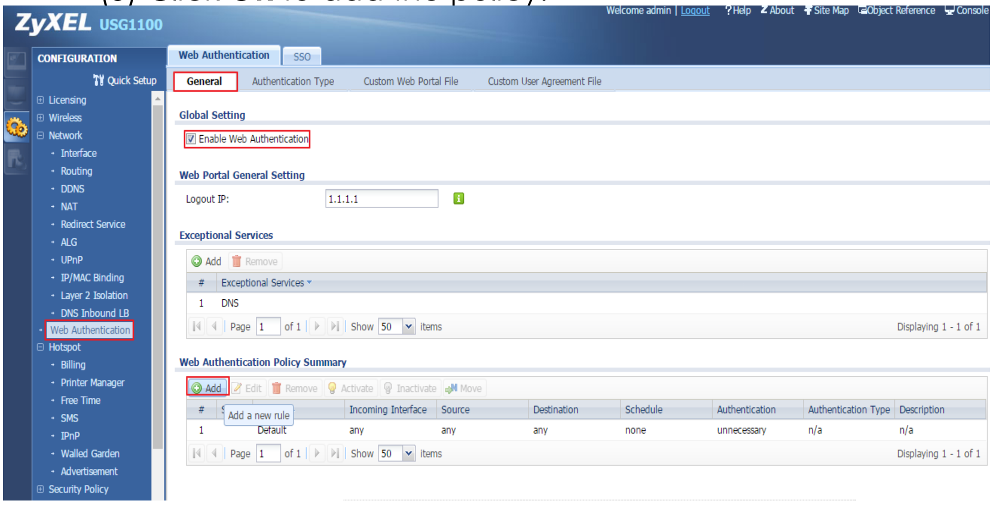
- WAN: 10.251.31.112
- LAN 1: 192.168.1.1/255.255.255.0
- User's laptop: 192.168.1.33

Configurations on the USG1100

The user agreement of this feature allows clients to access the Internet without a guest account. An advertisement webpage is used as the first page when an authenticated user attempts to access the Internet.

1. On the USG1100, go to **Configuration** > **Web Authentication** > **General**. Select **Enable Web Authentication** and click **Add** in the **Web Authentication Policy Summary** section.

   (1) Select **Enable Policy**.
   (2) Select **default-user-agreement** as the **Authentication Type**.
   (3) Click **OK** to add the policy.



Global Setting

☑ Enable Web Authentication

Web Portal General Setting

Logout IP: 1.1.1.1

Exceptional Services

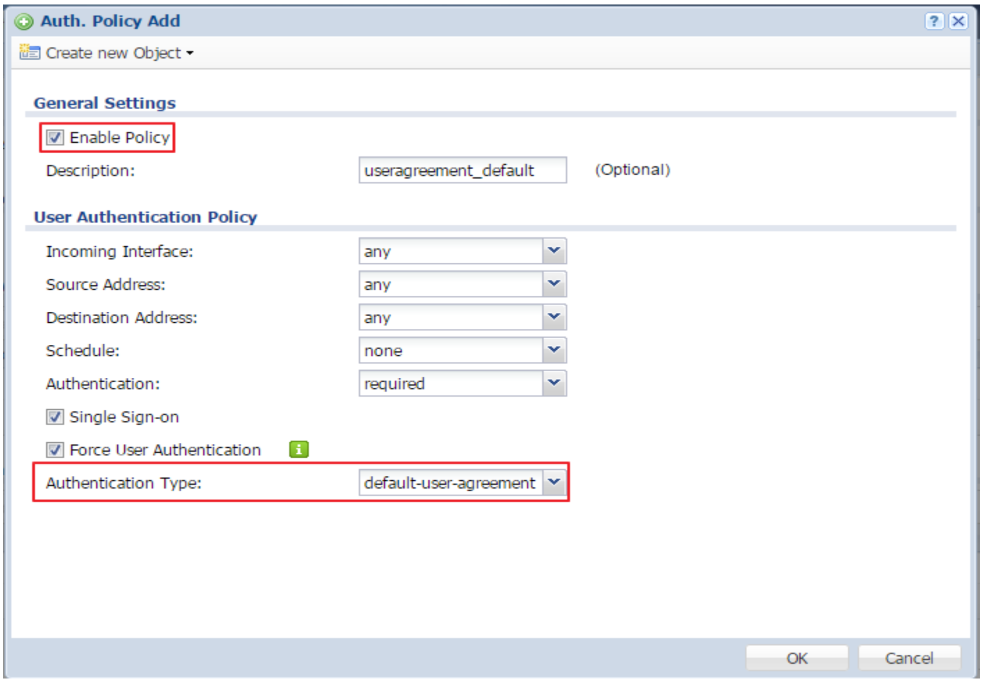
#	Exceptional Services
1	DNS

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

Web Authentication Policy Summary

#		Incoming Interface	Source	Destination	Schedule	Authentication	Authentication Type	Description
1	Default	any	any	any	none	unnecessary	n/a	n/a

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



General Settings

☑ Enable Policy

Description: useragreement_default (Optional)

User Authentication Policy

Incoming Interface: any

Source Address: any

Destination Address: any

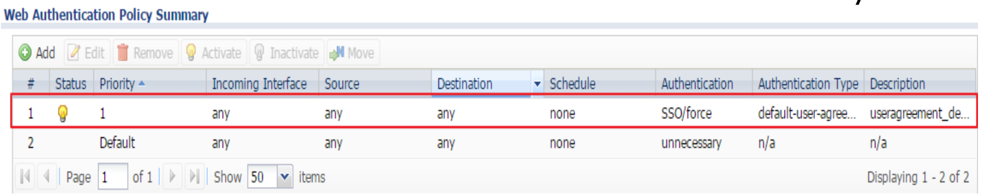
Schedule: none

Authentication: required

☑ Single Sign-on

☑ Force User Authentication

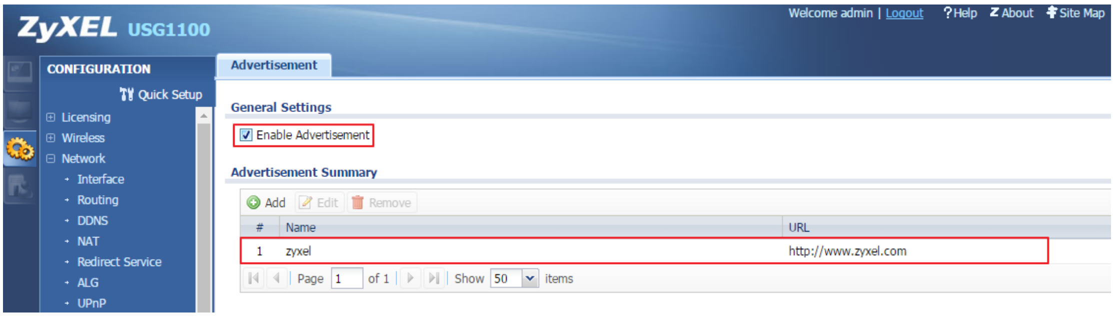
Authentication Type: default-user-agreement


Web Authentication Policy Summary

#	Status	Priority	Incoming Interface	Source	Destination	Schedule	Authentication	Authentication Type	Description
1		1	any	any	any	none	SSO/force	default-user-agree...	useragreement_de...
2		Default	any	any	any	none	unnecessary	n/a	n/a

2. Go to **Configuration** > **Hotspot** > **Advertisement**.

   (1) Select **Enable Advertisement**.
   (2) Add the URL of the website that you want to advertise.



General Settings

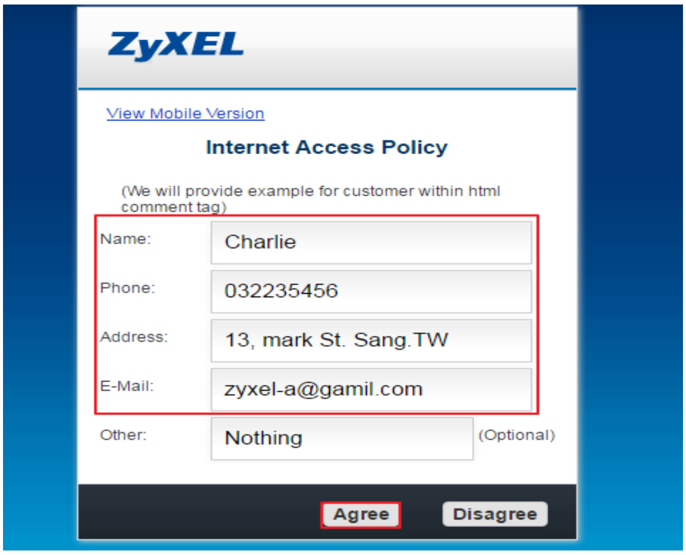
☑ Enable Advertisement

Advertisement Summary

#	Name	URL
1	zyxel	http://www.zyxel.com

Verification

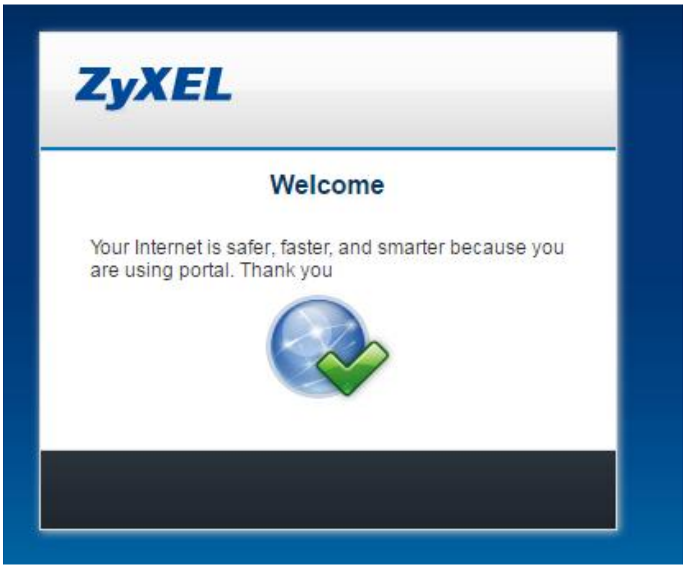
1. When a client attempts to access the Internet via a browser, he/she will be redirected to the user agreement page.



Internet Access Policy

(We will provide example for customer within html comment tag)

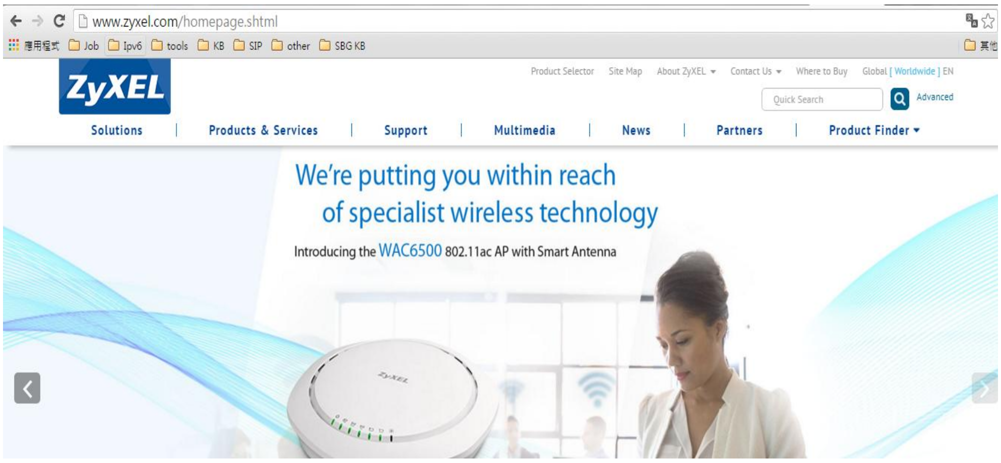
Name:	Charlie
Phone:	032235456
Address:	13, mark St. Sang.TW
E-Mail:	zyxel-a@gamil.com
Other:	Nothing (Optional)



Welcome

Your Internet is safer, faster, and smarter because you are using portal. Thank you

2. The advertisement webpage will be displayed in a new window and it is the first page that appears whenever the user connects to the Internet.

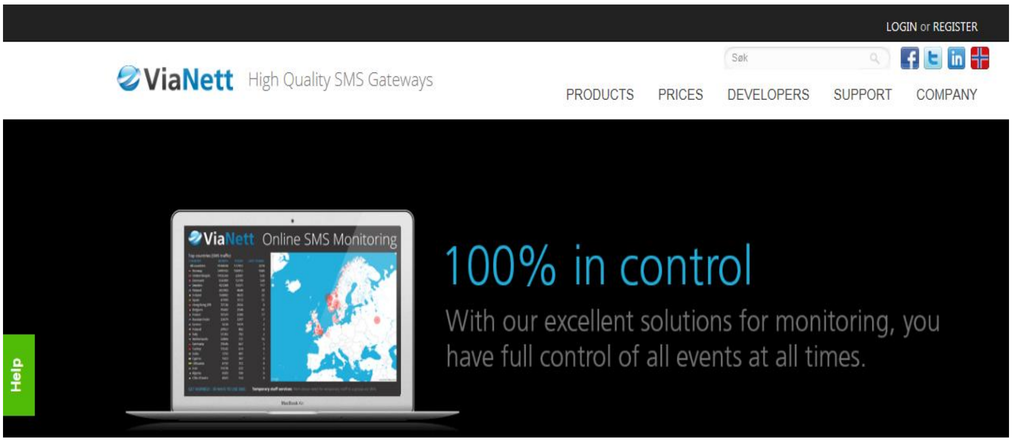


Enable the Free Time Feature

Configurations on the USG1100

On the USG1100, you need to enable the SMS service and select **SMS** as the delivery method in the **Free Time** feature.

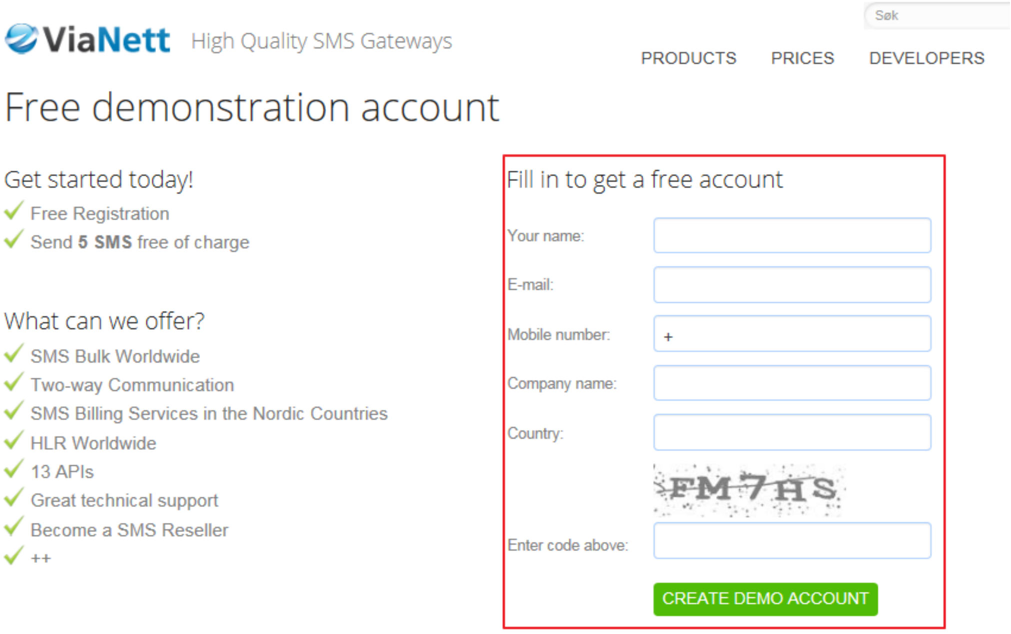
1. Register for a ViaNett account at http://www.vianett.com.


LOGIN or REGISTER
Søk
ViaNett High Quality SMS Gateways
PRODUCTS
PRICES
DEVELOPERS
SUPPORT
COMPANY
ViaNett Online SMS Monitoring
Help

100% in control

With our excellent solutions for monitoring, you have full control of all events at all times.

2. Enter all the required information.



Free demonstration account

Get started today!

- ✓ Free Registration
- ✓ Send **5 SMS** free of charge

What can we offer?

- ✓ SMS Bulk Worldwide
- ✓ Two-way Communication
- ✓ SMS Billing Services in the Nordic Countries
- ✓ HLR Worldwide
- ✓ 13 APIs
- ✓ Great technical support
- ✓ Become a SMS Reseller
- ✓ ++

Fill in to get a free account

Your name:

E-mail:

Mobile number: +

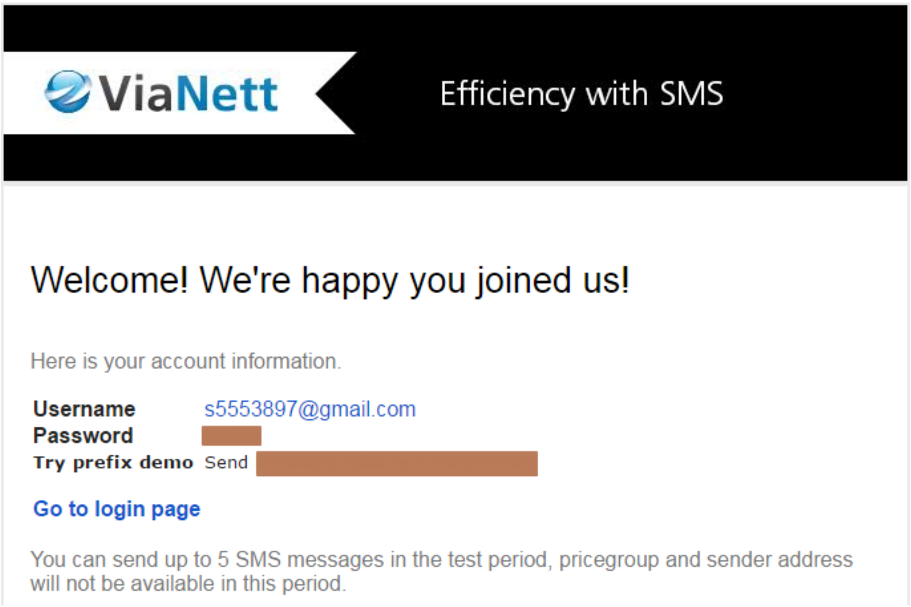
Company name:

Country:

FM7HS

Enter code above:

3. After the form has been submitted, the account information will be sent to your E-mail address.



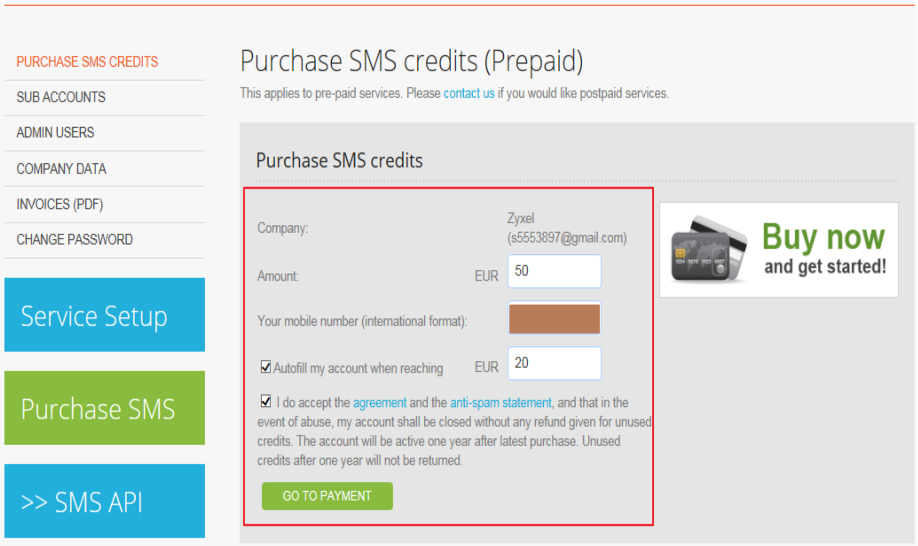
Welcome! We're happy you joined us!

Here is your account information.

Username s5553897@gmail.com
Password [redacted]
Try prefix demo Send [redacted]

Go to login page

You can send up to 5 SMS messages in the test period, pricegroup and sender address will not be available in this period.



Purchase SMS credits (Prepaid)

This applies to pre-paid services. Please contact us if you would like postpaid services.

Purchase SMS credits

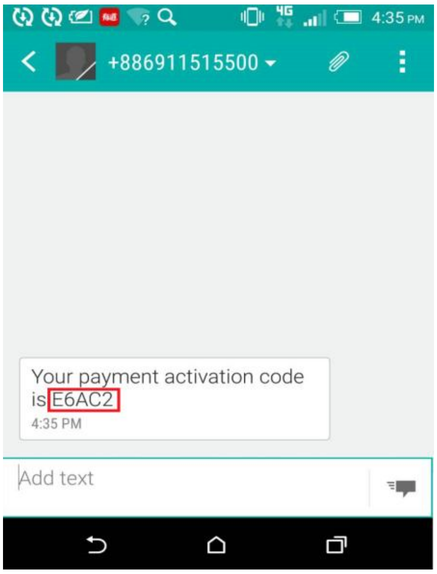
Company: Zyxel (s5553897@gmail.com)

Amount: EUR 50

Your mobile number (international format): [redacted]

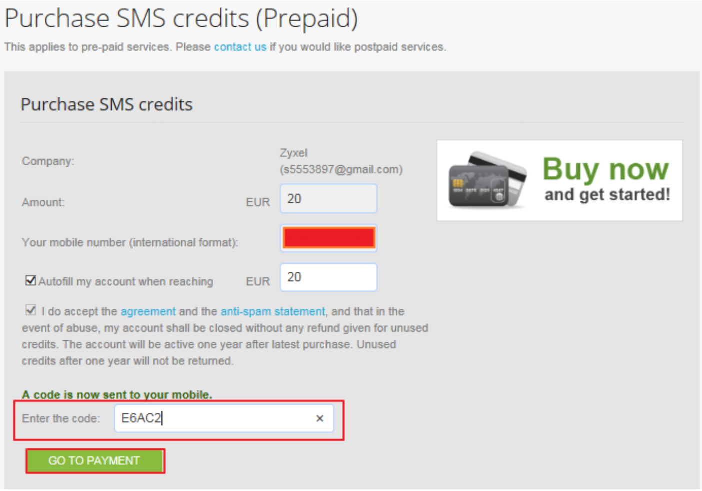
☑ Autofill my account when reaching EUR 20

☑ I do accept the agreement and the anti-spam statement, and that in the event of abuse, my account shall be closed without any refund given for unused credits. The account will be active one year after latest purchase. Unused credits after one year will not be returned.



Your payment activation code is E6AC2
4:35 PM

4. Enter the activation code and proceed to make the payment.



Purchase SMS credits (Prepaid)

This applies to pre-paid services. Please contact us if you would like postpaid services.

Purchase SMS credits

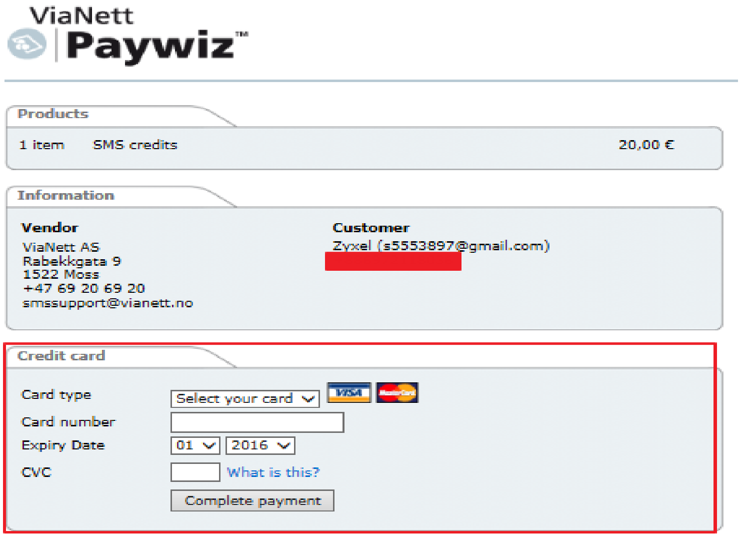
Company:	Zyxel (s5553897@gmail.com)
Amount:	EUR 20
Your mobile number (international format):	[redacted]
☑ Autofill my account when reaching	EUR 20

☑ I do accept the agreement and the anti-spam statement, and that in the event of abuse, my account shall be closed without any refund given for unused credits. The account will be active one year after latest purchase. Unused credits after one year will not be returned.

A code is now sent to your mobile.

Enter the code: E6AC2

5. Fill-in the credit card information to complete the payment.



ViaNett Paywiz™

Products

1 item	SMS credits	20,00 €

Information

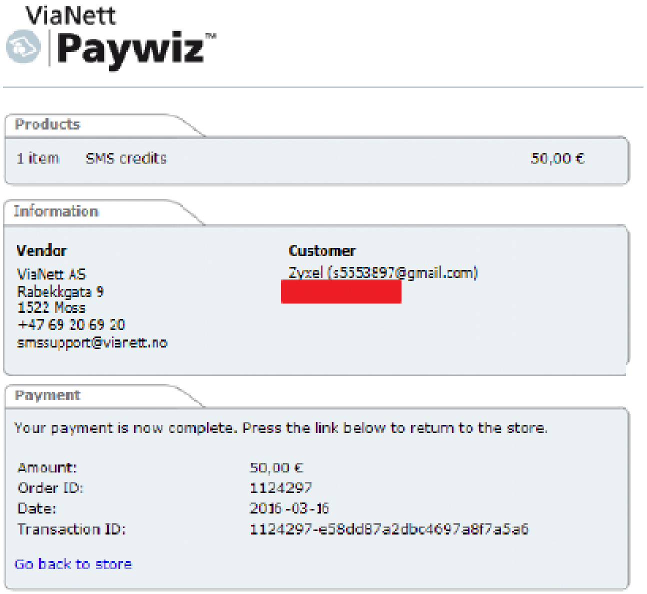
Vendor
ViaNett AS
Rabekkgata 9
1522 Moss
+47 69 20 69 20
smssupport@vianett.no

Customer
Zyxel (s5553897@gmail.com)
[redacted]

Credit card

Card type	Select your card
Card number	
Expiry Date	01 2016
CVC	What is this?

The payment is complete.



ViaNett Paywiz™

Products

1 item	SMS credits	50,00 €

Information

Vendor
ViaNett AS
Rabekkgata 9
1522 Moss
+47 69 20 69 20
smssupport@vianett.no

Customer
Zyxel (s5553897@gmail.com)
[redacted]

Payment

Your payment is now complete. Press the link below to return to the store.

Amount:	50,00 €
Order ID:	1124297
Date:	2016-03-16
Transaction ID:	1124297-e58dd87a2dbc4697a8f7a5a6

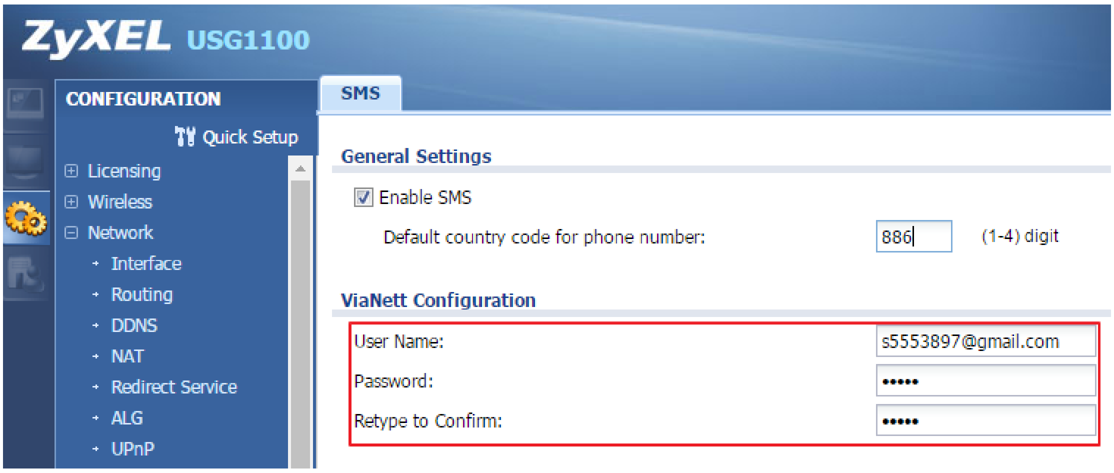
Go back to store

6. After the ViaNett account is ready, go to the USG1100's **Configuration** > **Hotspot** > **SMS** screen.

   (1)Enable SMS.

   (2)Fill-in your local phone country code as the default country code.

   (3) Add authentication policy for every source.



General Settings

☑ Enable SMS

Default country code for phone number: 886 (1-4) digit

ViaNett Configuration

User Name: s5553897@gmail.com

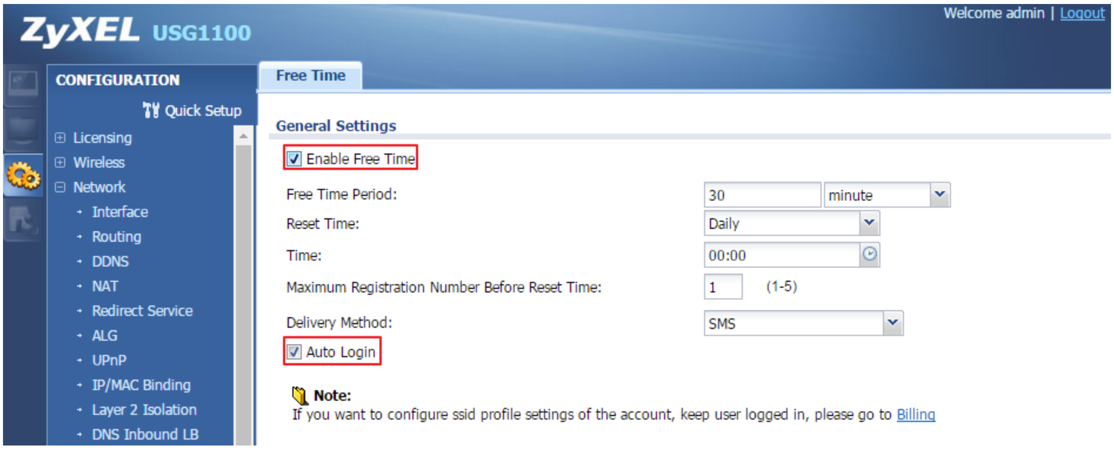
Password: •••••

Retype to Confirm: •••••

7. Go to **Configuration** > **Hotspot** > **Free Time**.

   (1) Select **Enable Free Time** and set up the free time period. By default, the **Reset Time** is at AM 00:00. You can also set up how many times a MAC address can access the Internet.

   (2) Select **SMS** as the method to deliver the login information to the mobile phone.



General Settings

☑ Enable Free Time

Free Time Period: 30 minute

Reset Time: Daily

Time: 00:00

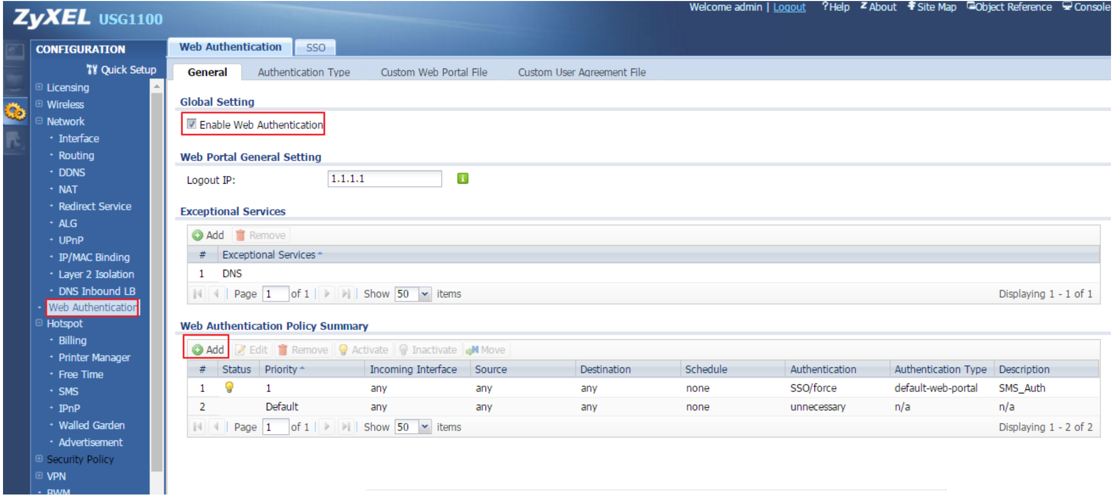
Maximum Registration Number Before Reset Time: 1 (1-5)

Delivery Method: SMS

☑ Auto Login

Note:
If you want to configure ssid profile settings of the account, keep user logged in, please go to Billing

8. Go to **Configuration** > **Web Authentication**. Select **Enable Web Authentication** and click **Add** in the **Web Authentication Policy Summary** section.



Global Setting

☑ Enable Web Authentication

Web Portal General Setting

Logout IP: 1.1.1.1

Exceptional Services

#	Exceptional Services
1	DNS

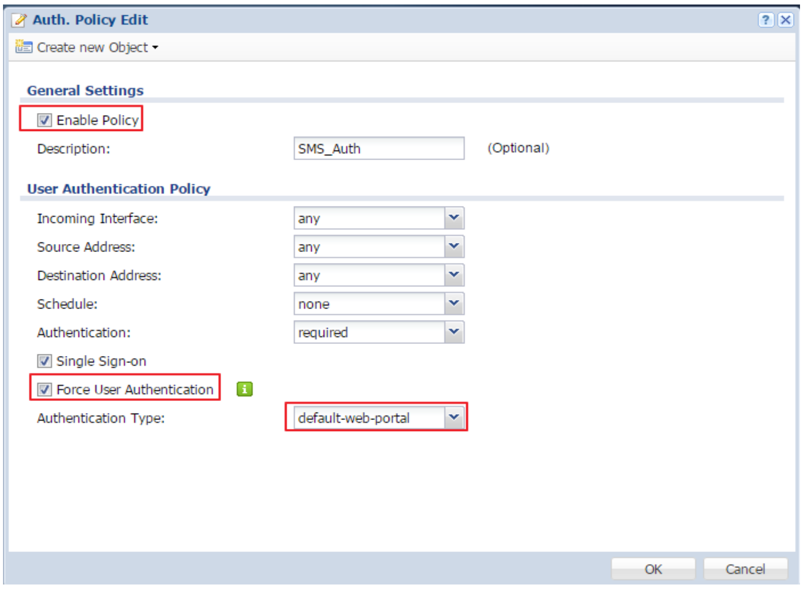
Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

Web Authentication Policy Summary

#	Status	Priority	Incoming Interface	Source	Destination	Schedule	Authentication	Authentication Type	Description
1	💡	1	any	any	any	none	SSO/force	default-web-portal	SMS_Auth
2		Default	any	any	any	none	unnecessary	n/a	n/a

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

9. Select **Enable Policy**, **Force User Authentication**, and then select **default-web-portal** as the **Authentication Type**.



General Settings

☑ Enable Policy

Description: SMS_Auth (Optional)

User Authentication Policy

Incoming Interface: any

Source Address: any

Destination Address: any

Schedule: none

Authentication: required

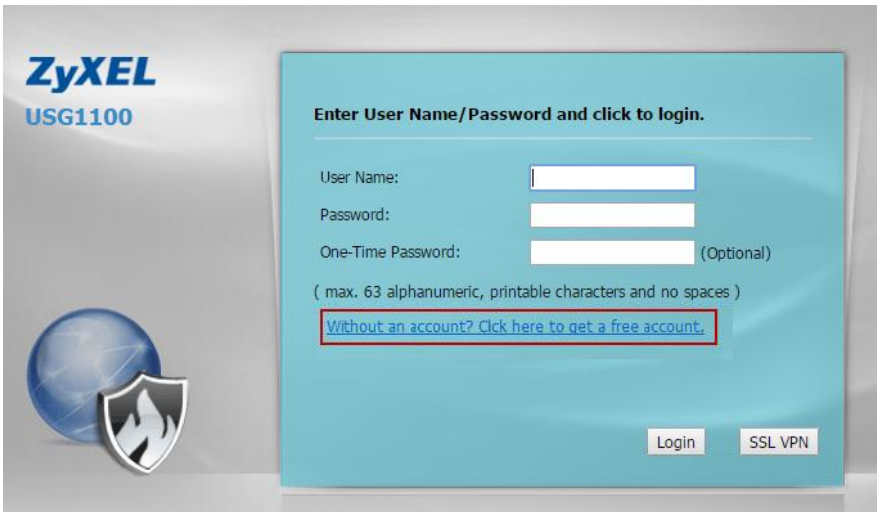
☑ Single Sign-on

☑ Force User Authentication

Authentication Type: default-web-portal

Verification

1. The user will be redirected to the **Login** screen before he/she is permitted to access the Internet. Click on the link to get a free account.



Enter User Name/Password and click to login.

User Name:

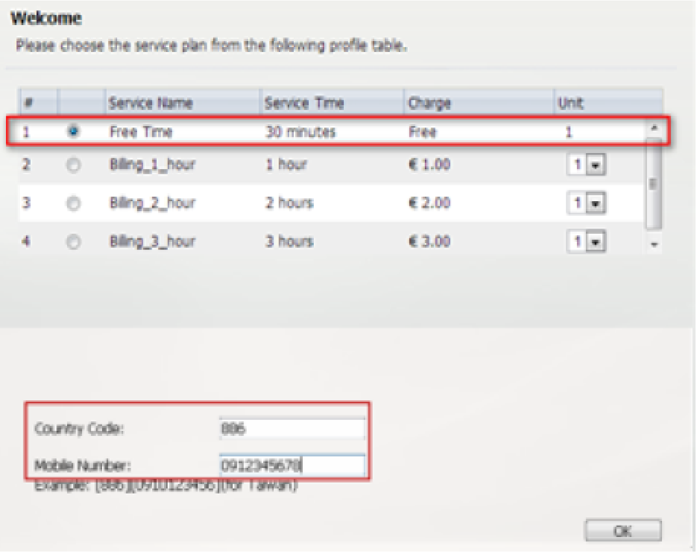
Password:

One-Time Password: (Optional)

(max. 63 alphanumeric, printable characters and no spaces)

Without an account? Click here to get a free account.

2. Select **Free Time** as the service plan. Then submit your country code and mobile phone number.



Welcome

Please choose the service plan from the following profile table.

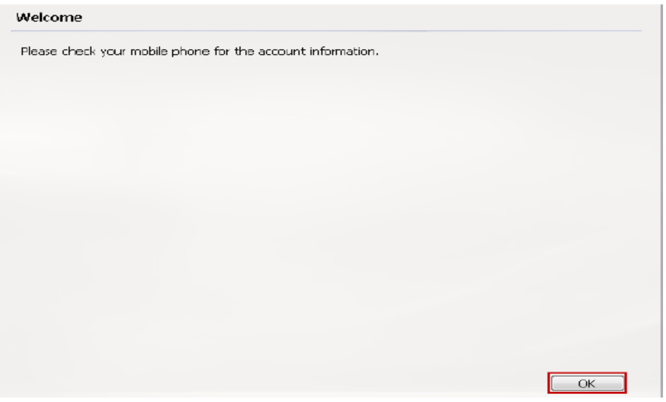
#		Service Name	Service Time	Charge	Unit
1	●	Free Time	30 minutes	Free	1
2	○	Billing_1_hour	1 hour	€ 1.00	1
3	○	Billing_2_hour	2 hours	€ 2.00	1
4	○	Billing_3_hour	3 hours	€ 3.00	1

Country Code: 886

Mobile Number: 0912345678

Example: [886][0910123456](for Taiwan)

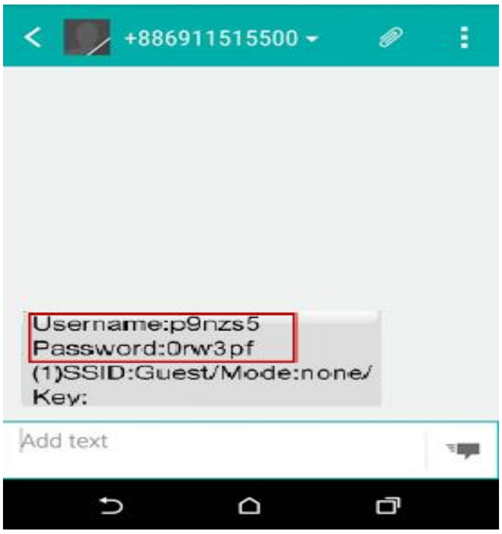
3. The account and password will be sent to your mobile phone.



Welcome

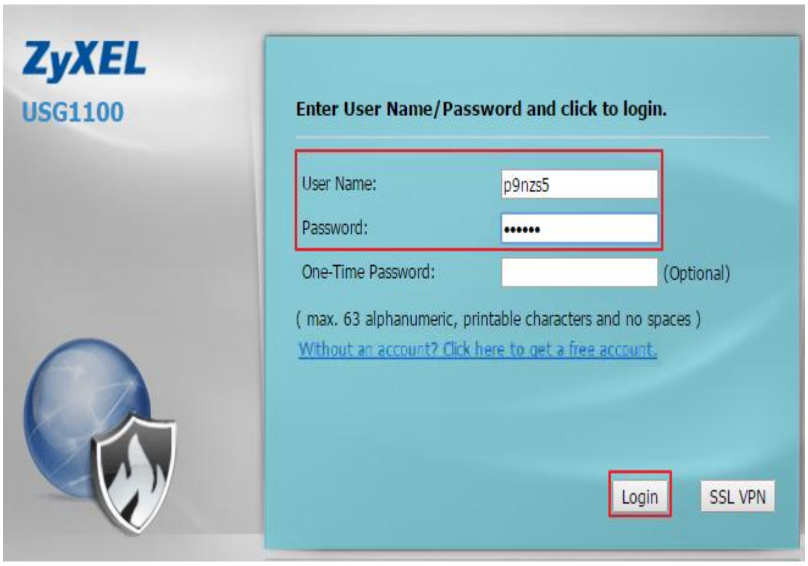
Please check your mobile phone for the account information.

4. Check your account information.



Username:p9nzs5
Password:0rw3pf
(1)SSID:Guest/Mode:none/
Key:

5. Fill-in the account information received on your mobile phone and click **Login**.



Enter User Name/Password and click to login.

User Name: p9nzs5

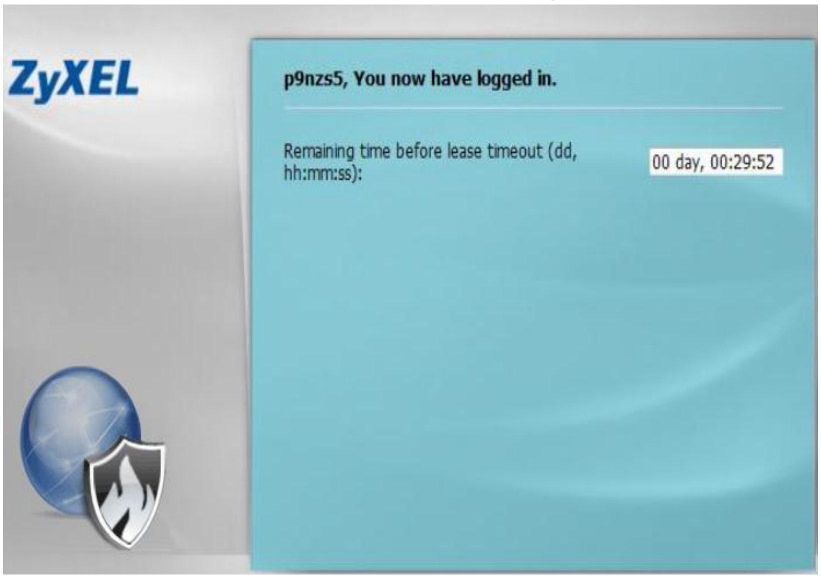
Password: ••••••

One-Time Password: (Optional)

(max. 63 alphanumeric, printable characters and no spaces)

Without an account? Click here to get a free account.

6. Now the client can start accessing the Internet.



p9nzs5, You now have logged in.

Remaining time before lease timeout (dd, hh:mm:ss): 00 day, 00:29:52

Scenario 19 – Link Aggregation Group (LAG)

19.1 Application Scenario

A Link Aggregation Group (LAG) allows you to combine a number of physical ports together to create a single high bandwidth data path. It helps to implement the traffic to perform load balancing or failover features, depending on the situation of the actual case.

Before you begin:

LAG interface supported models: ZyWALL 310/1100/1900, USG 310/1100/1900

The link aggregation supported models have Active-backup, 802.3ad (LACP), and Balance-alb modes.

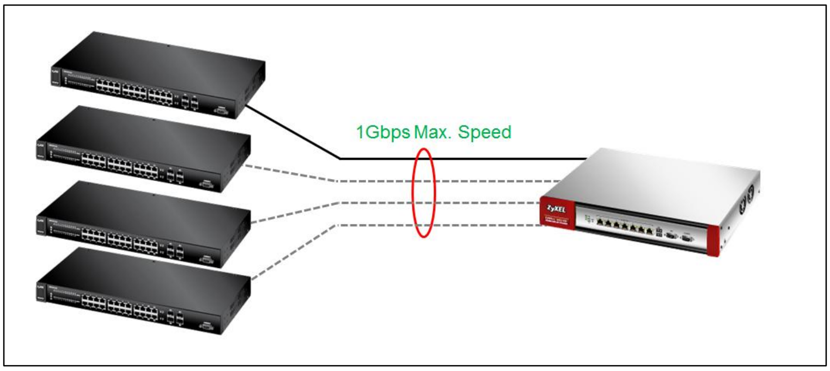
Link aggregation supports IPSec tunnel, VLAN, and bridge interface.

Device HA Pro is supported on the LAG interface but Device HA is not.

19.2 Configuration Guide

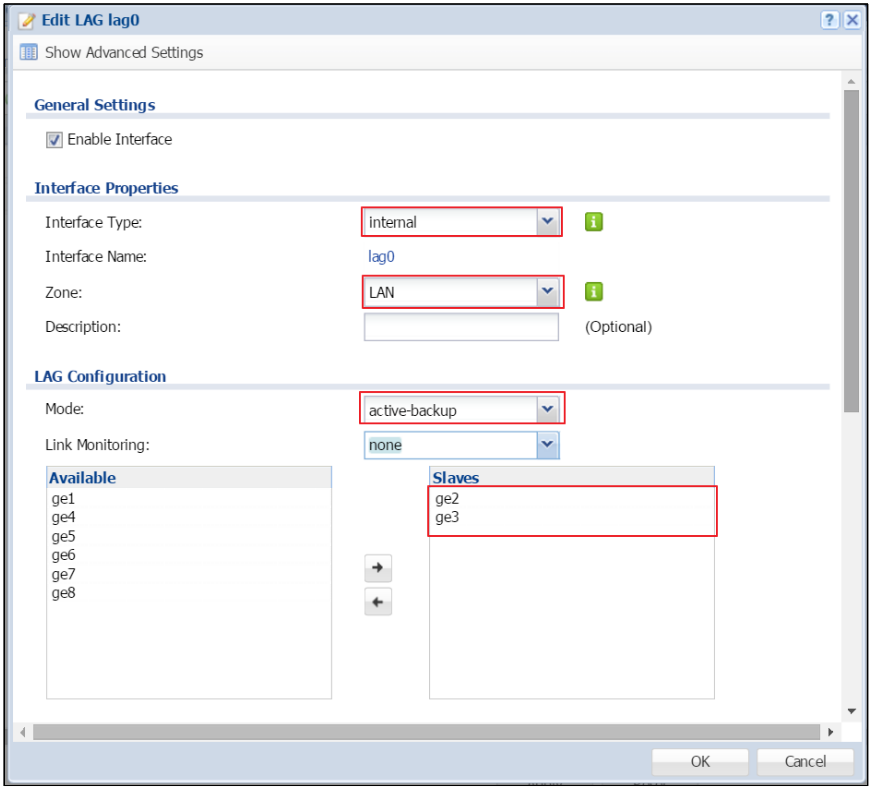
- **LAG Application Scenario: Active-backup, 802.3ad, Balance-alb**

Active-backup Mode:
(Does not require switch configuration and one or multiple switches can be used.)



Only the USG needs to be configured. You do not need to change any settings on the switch.

On the USG, go to **Configuration > Network > Interface > LAG**.
Choose the proper interface type and zone depending on the case. Also, select the slave ports that will be added in the LAG interface.
The interface format will be **lagx** (x = 0~3).



Edit LAG lag0

Show Advanced Settings

General Settings

☑ Enable Interface

Interface Properties

Interface Type: internal

Interface Name: lag0

Zone: LAN

Description: (Optional)

LAG Configuration

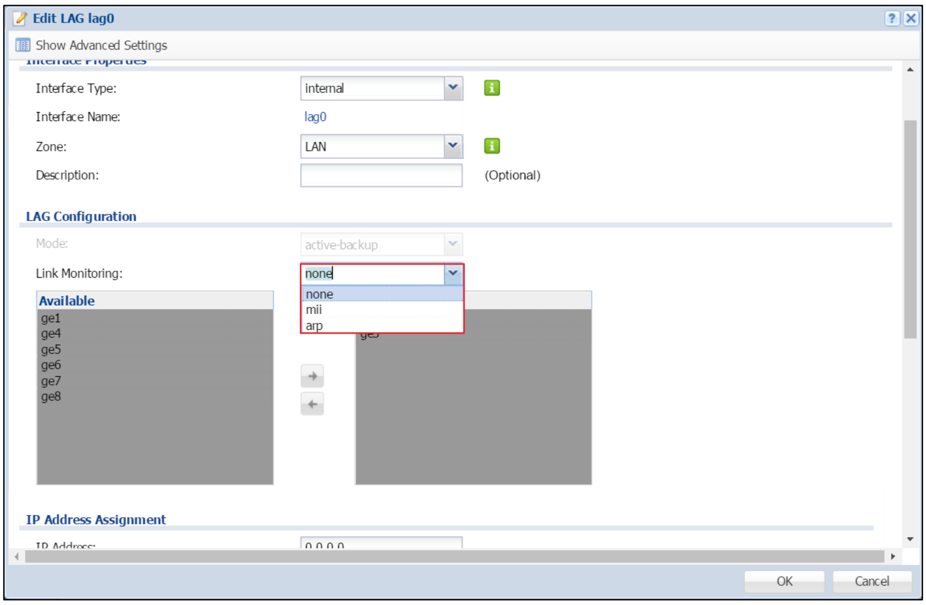
Mode: active-backup

Link Monitoring: none

Available	Slaves
ge1	ge2
ge4	ge3
ge5	
ge6	
ge7	
ge8	

Link Monitoring:

You can choose link up/down detection (specify the MII link monitoring frequency or ARP interval time).



Edit LAG lag0

Show Advanced Settings

Interface Properties

Interface Type: internal

Interface Name: lag0

Zone: LAN

Description: (Optional)

LAG Configuration

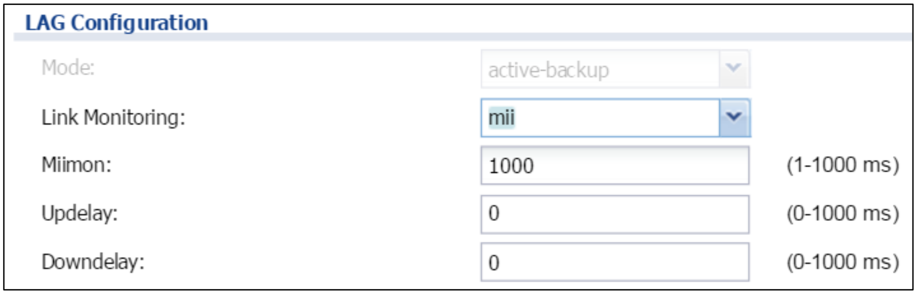
Mode: active-backup

Link Monitoring: none

Available
ge1
ge4
ge5
ge6
ge7
ge8

IP Address Assignment

IP Address: 0.0.0.0

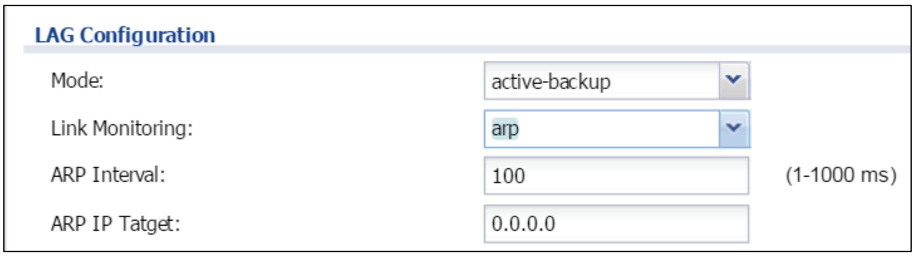


LAG Configuration

Mode:	active-backup	
Link Monitoring:	mii	
Miimon:	1000	(1-1000 ms)
Updelay:	0	(0-1000 ms)
Downdelay:	0	(0-1000 ms)

Updelay is the time to wait to enable the slave port after the device detects the link recovery.

Downdelay is the time to wait to disable the slave port after the device detects the link failure.



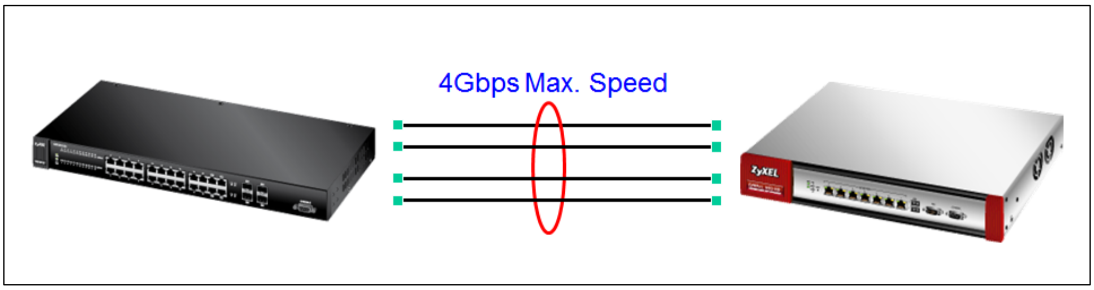
LAG Configuration

Mode:	active-backup	
Link Monitoring:	arp	
ARP Interval:	100	(1-1000 ms)
ARP IP Tatget:	0.0.0.0	

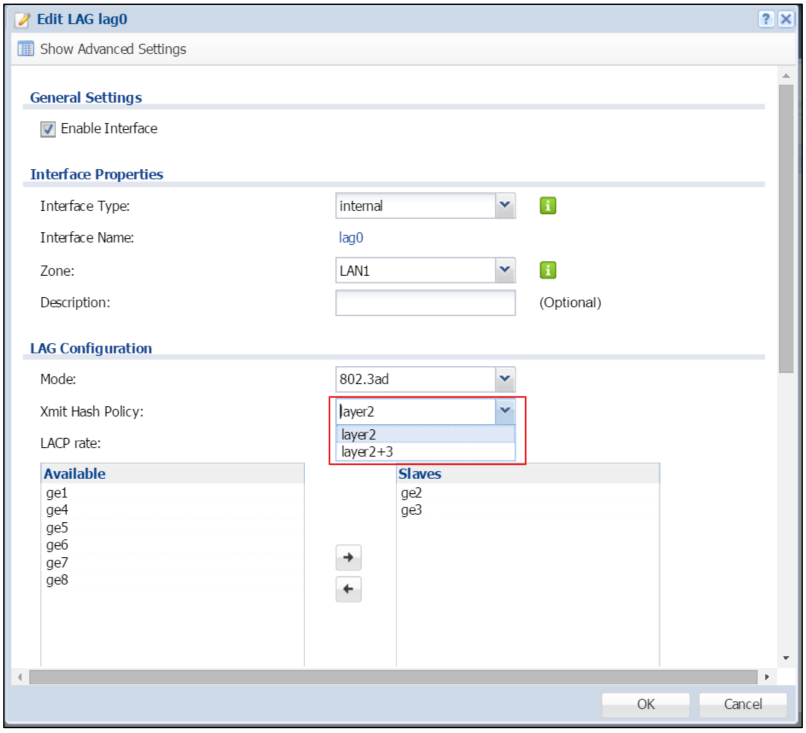
The taget IP can be the Layer 3 device or the host IP, can be reachable by the USG.

802.3ad (LACP) Mode:

(Both devices need to be configured. Only one switch can be used. The port speed and duplex must be the same.)



The USG should be connected to only one switch and its settings should be the same as the switch. This utilizes all slave network interfaces in the active aggregator group according to the 802.3ad specification.



Edit LAG lag0

General Settings

☑ Enable Interface

Interface Properties

Interface Type: internal

Interface Name: lag0

Zone: LAN1

Description: (Optional)

LAG Configuration

Mode: 802.3ad

Xmit Hash Policy: layer2

LACP rate:

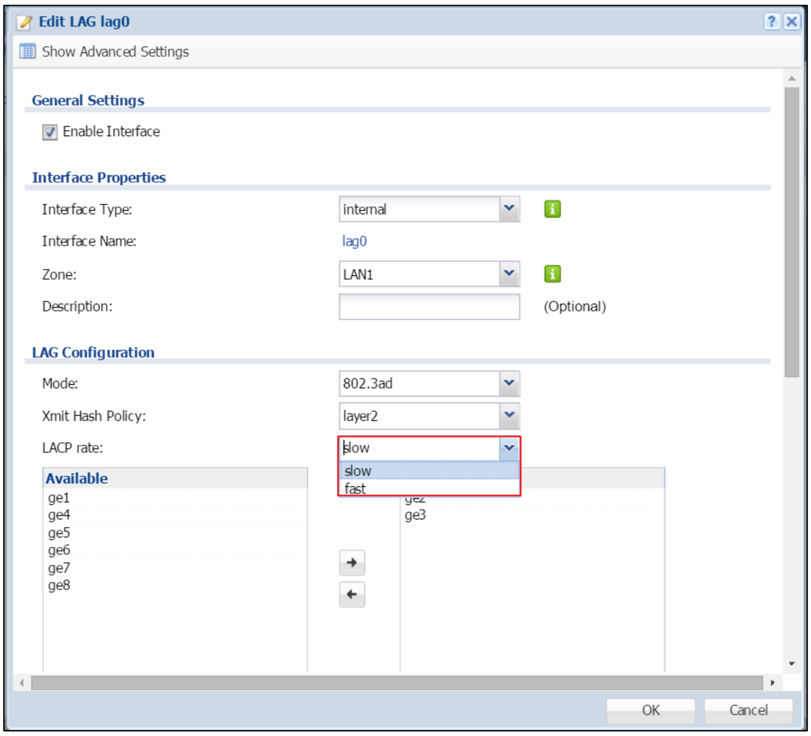
Available	Slaves
ge1 ge4 ge5 ge6 ge7 ge8	ge2 ge3

Xmit Hash Policy:

Xmit Hash policy: Select **layer2** or **layer2+3**.

Select **layer 2** if the LAG interface is connect to a layer 2 subnet.

Select **layer 2+3** if the LAG interface is connect to a network with a router or a L3 switch.



Edit LAG lag0

General Settings

☑ Enable Interface

Interface Properties

Interface Type: internal

Interface Name: lag0

Zone: LAN1

Description: (Optional)

LAG Configuration

Mode: 802.3ad

Xmit Hash Policy: layer2

LACP rate: slow

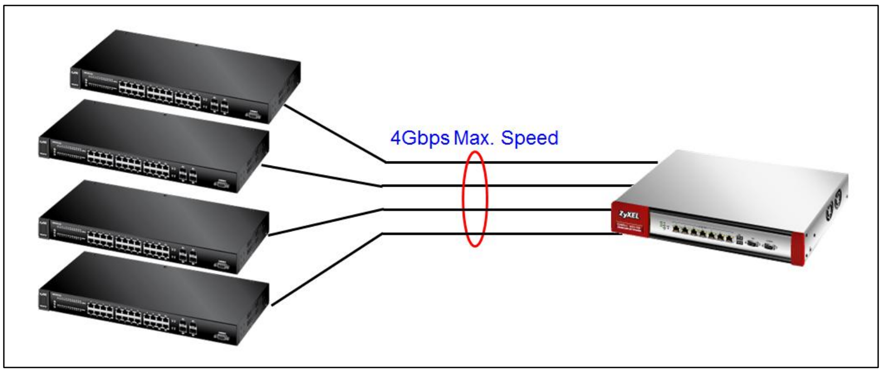
Available	
ge1 ge4 ge5 ge6 ge7 ge8	ge2 ge3

LACP rate:

The interval can be fast (every second) or slow (every 30 seconds).

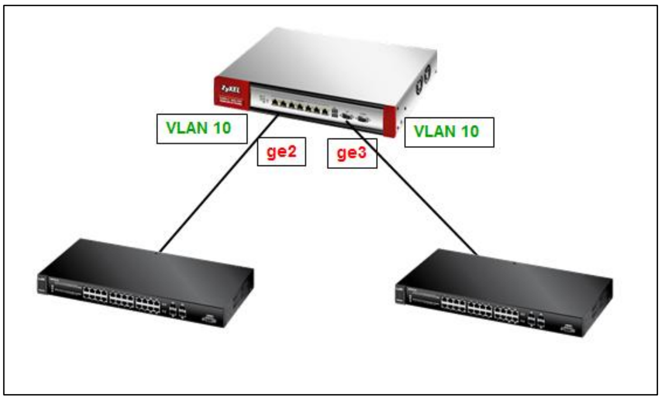
Balance-alb Mode:

(Does not require configuration on the switch and one or multiple switches can be used.)

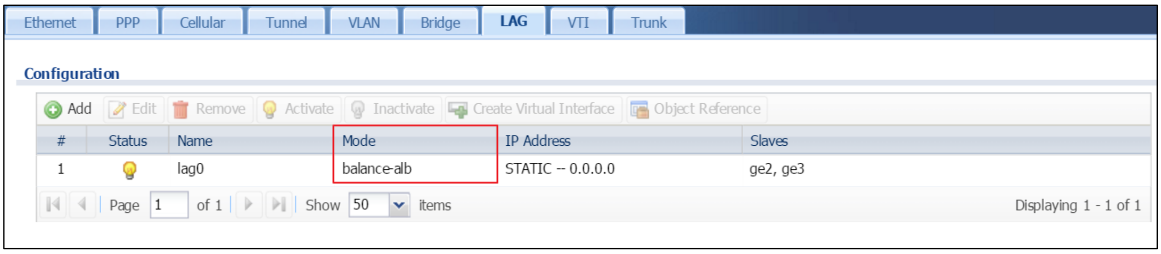


The settings are the same as the active-backup mode.

The VLAN interface is cross-connected to different switches and the link statuses on both switches are active.

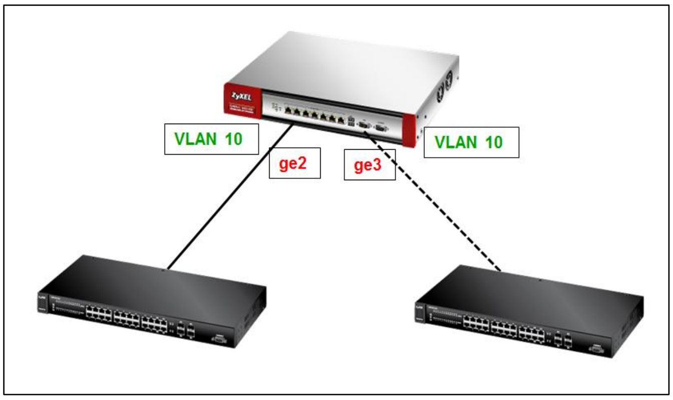


In this case, the LAG interface mode must be set to **Balance-alb**.

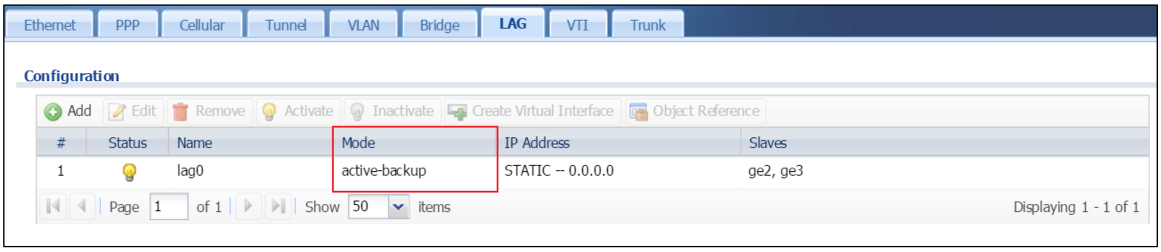


#	Status	Name	Mode	IP Address	Slaves
1	💡	lag0	balance-alb	STATIC -- 0.0.0.0	ge2, ge3

The VLAN interface is cross-connected to different switches (fault tolerance).



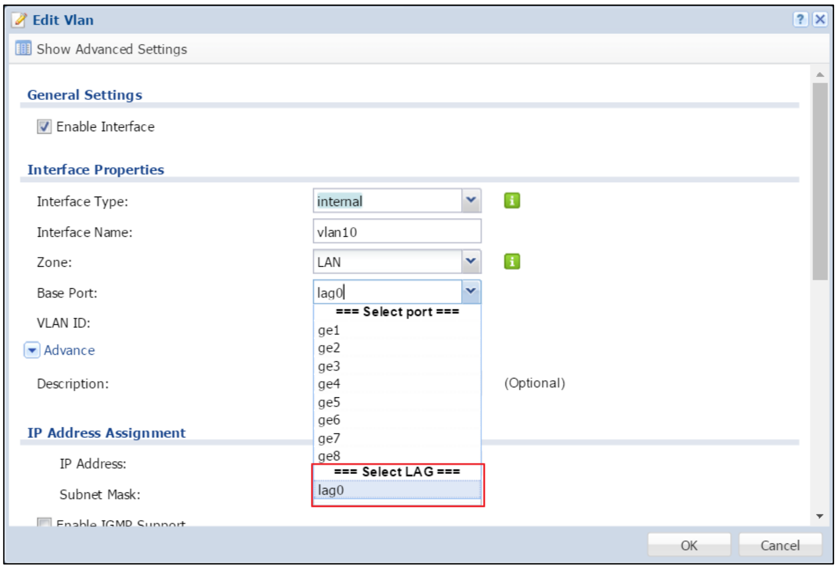
Only one link connection is up and the other is down. In this case, you will need to use the **active-backup** mode.



Configuration

#	Status	Name	Mode	IP Address	Slaves
1	💡	lag0	active-backup	STATIC -- 0.0.0.0	ge2, ge3

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



Edit Vlan

General Settings

☑ Enable Interface

Interface Properties

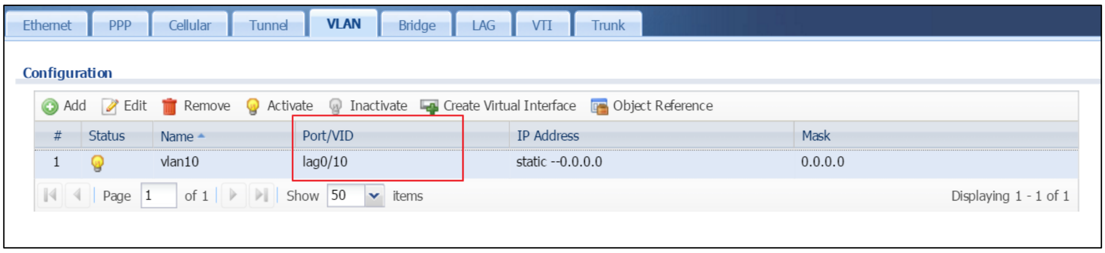
Interface Type:	internal
Interface Name:	vlan10
Zone:	LAN
Base Port:	lag0
VLAN ID:	
Description:	(Optional)

IP Address Assignment

IP Address:	
Subnet Mask:	

□ Enable IGMP Support

You can find the LAG interface in the VLAN interface..



Configuration

#	Status	Name ▲	Port/VID	IP Address	Mask
1	💡	vlan10	lag0/10	static --0.0.0.0	0.0.0.0

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