www.zyxel.com

ATP/USG FLEX/VPN Series

ATP100 / ATP100W / ATP200 / ATP500/ ATP700/ ATP800

USG FLEX 50 / USG FLEX 50W/ USG FLEX 100
USG FLEX 100W / USG FLEX 200 / USG FLEX 500
USG FLEX 700

VPN50 / VPN100 /VPN300 /VPN1000

USG20-VPN/ USG20W-VPN

Security Firewalls

Firmware Version 5.31
07/2022

Handbook

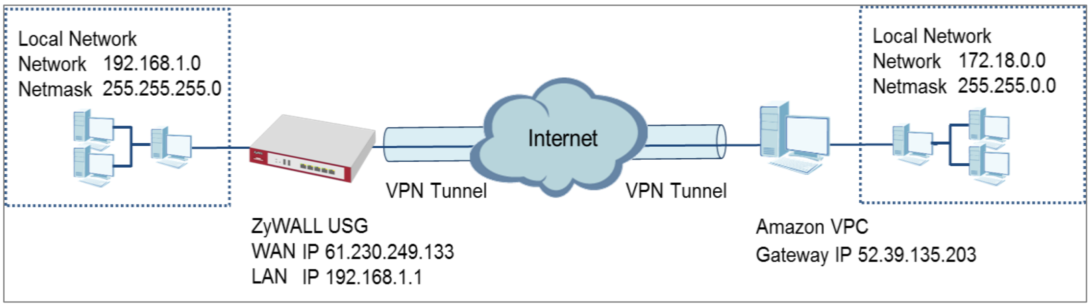
Default Login Details	
LAN Port IP Address	https://192.168.1.1
User Name	admin
Password	1234

Table of Content

Chapter 1- VPN

How to Configure Site-to-site IPSec VPN with Amazon VPC

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZyWALL/USG and an Amazon VPC platform. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



ZyWALL/USG Site-to-site IPSec VPN with Amazon VPC

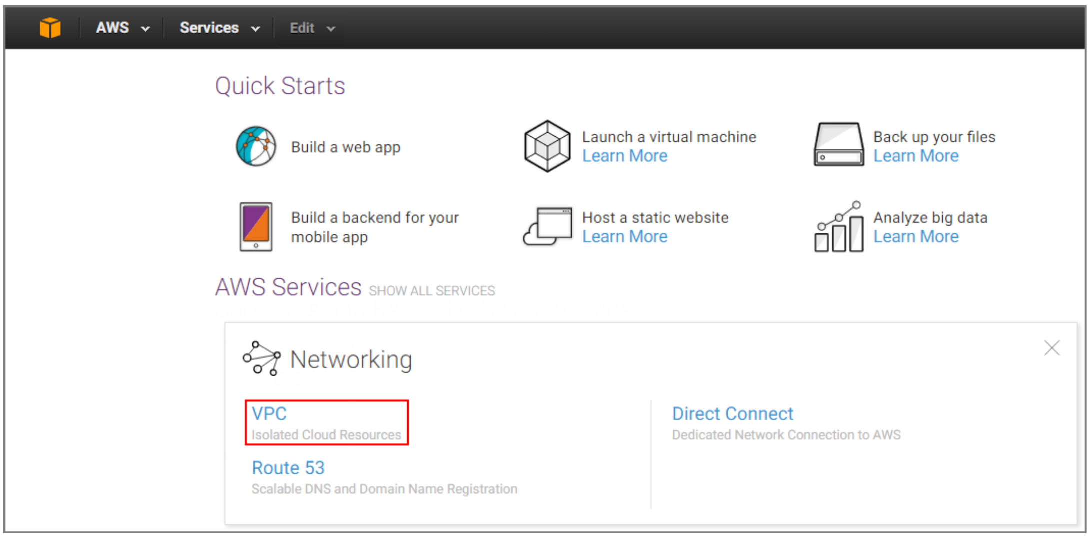
Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25) and Amazon VPC (June, 2016).

Set Up the IPSec VPN Tunnel on the Amazon VPC

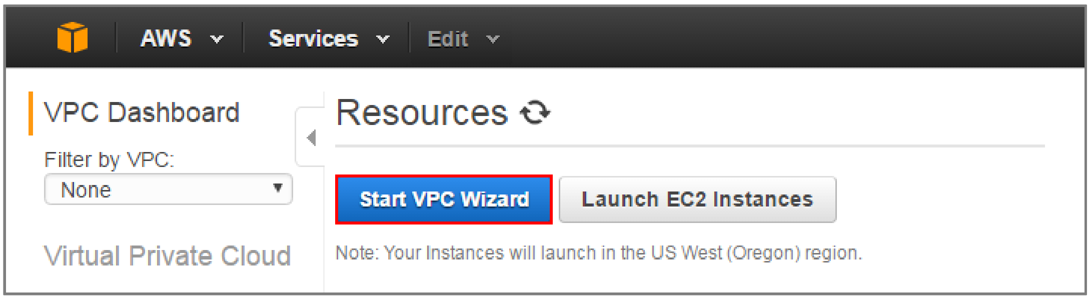
1 Sign into the Amazon AWS Management Console. Go to Networking > VPC.

Amazon AWS Management Console > Networking > VPC



2 In the upper left-hand of the screen, click **Start VPC Wizard**.

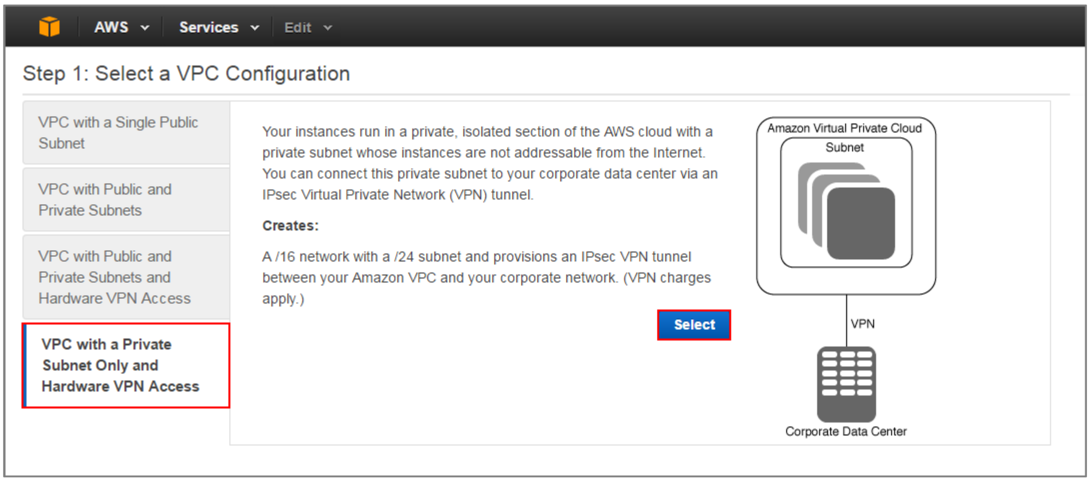
Amazon VPC Management Console > Networking > VPC > Start VPC Wizard



Note: Your Instances will launch in the US West (Oregon) region.

3 Select a VPC Configuration, select VPC with a Private Subnet Only and Hardware VPN Access, and then click Select.

Select a VPC Configuration > VPC with a Private Subnet Only and Hardware VPN Access


AWS
Services
Edit
VPC with a Single Public Subnet
VPC with Public and Private Subnets
VPC with Public and Private Subnets and Hardware VPN Access
VPC with a Private Subnet Only and Hardware VPN Access
Select
Amazon Virtual Private Cloud
Subnet
VPN
Corporate Data Center

Step 1: Select a VPC Configuration

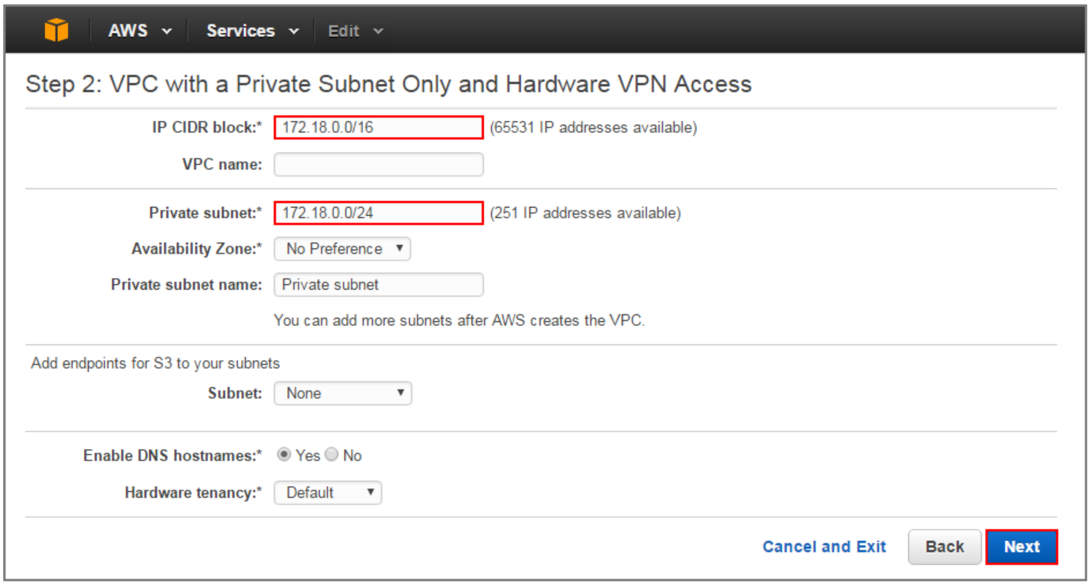
Your instances run in a private, isolated section of the AWS cloud with a private subnet whose instances are not addressable from the Internet. You can connect this private subnet to your corporate data center via an IPsec Virtual Private Network (VPN) tunnel.

Creates:

A /16 network with a /24 subnet and provisions an IPsec VPN tunnel between your Amazon VPC and your corporate network. (VPN charges apply.)

4 VPC with a Private Subnet Only and Hardware VPN, add your **IP CIDR block** and **Private subnet**. Click **Next**.

VPC with a Private Subnet Only and Hardware VPN



Step 2: VPC with a Private Subnet Only and Hardware VPN Access

IP CIDR block:* 172.18.0.0/16 (65531 IP addresses available)

VPC name:

Private subnet:* 172.18.0.0/24 (251 IP addresses available)

Availability Zone:* No Preference

Private subnet name: Private subnet

You can add more subnets after AWS creates the VPC.

Add endpoints for S3 to your subnets

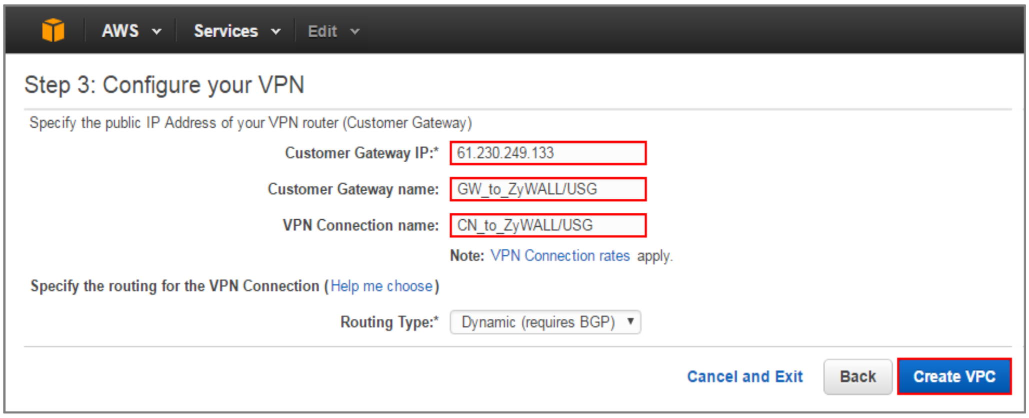
Subnet: None

Enable DNS hostnames:* ● Yes ○ No

Hardware tenancy:* Default

5 Configure your VPN, add your ZyWALL/USG public IP address into **Customer Gateway IP**. Name your **Customer Gateway name** and **VPN Connection name**. Click **Create VPC** at the bottom of the blade.

Configure your VPN



Step 3: Configure your VPN

Specify the public IP Address of your VPN router (Customer Gateway)

Customer Gateway IP:* 61.230.249.133

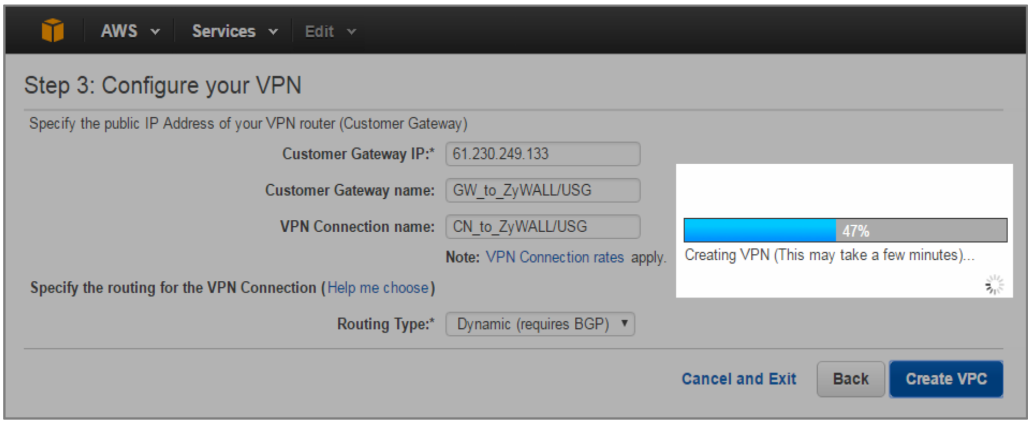
Customer Gateway name: GW_to_ZyWALL/USG

VPN Connection name: CN_to_ZyWALL/USG

Note: VPN Connection rates apply.

Specify the routing for the VPN Connection (Help me choose)

Routing Type:* Dynamic (requires BGP)



Step 3: Configure your VPN

Specify the public IP Address of your VPN router (Customer Gateway)

Customer Gateway IP:* 61.230.249.133

Customer Gateway name: GW_to_ZyWALL/USG

VPN Connection name: CN_to_ZyWALL/USG

Note: VPN Connection rates apply.

Specify the routing for the VPN Connection (Help me choose)

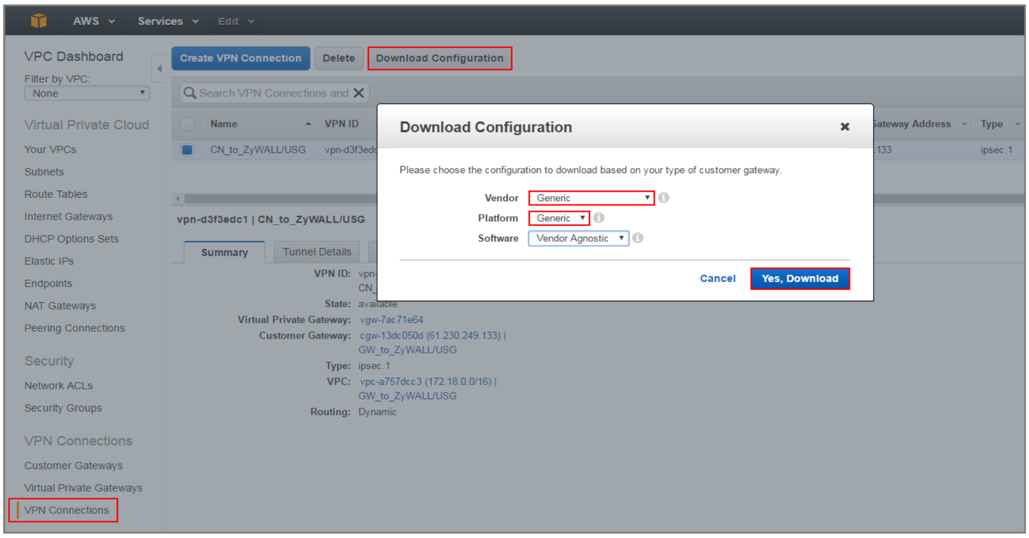
Routing Type:* Dynamic (requires BGP)

47%

Creating VPN (This may take a few minutes)...

6 In the VPC Dashboard, go to VPN Connections. Select Download Configuration from the upper bar. Select Vendor and Platform to be Generic. Click Yes, Download.

VPC Dashboard > VPN Connections



VPN ID: vpn-
CN_

State: available

Virtual Private Gateway: vgw-7ac71e64

Customer Gateway: cgw-13dc050d (61.230.249.133) | GW_to_ZyWALL/USG

Type: ipsec.1

VPC: vpc-a757dcc3 (172.18.0.0/16) | GW_to_ZyWALL/USG

Routing: Dynamic

Download Configuration

Please choose the configuration to download based on your type of customer gateway.

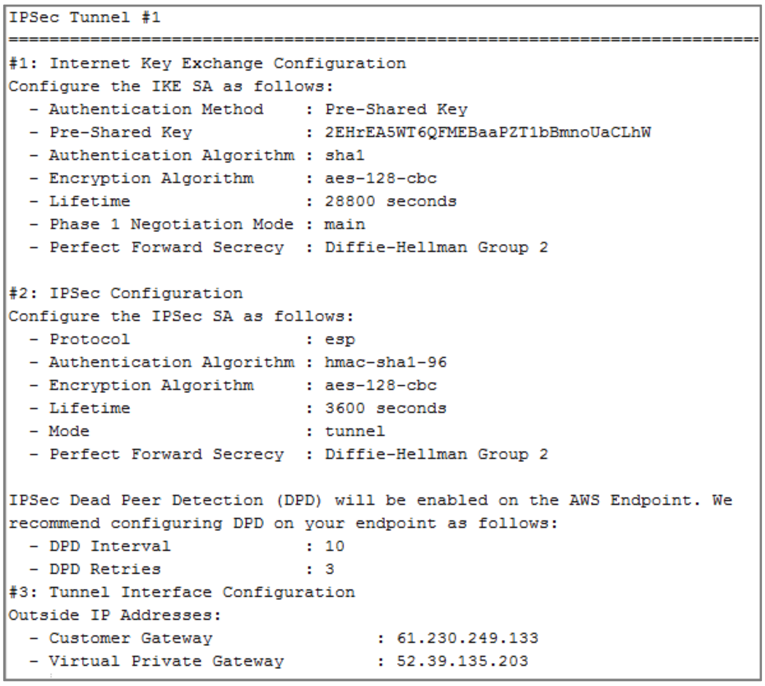
Vendor: Generic

Platform: Generic

Software: Vendor Agnostic

7 Open the downloaded configuration txt. file, it displays IKE SA, IPSec SA and Gateway IP address. Please make sure all the settings match your ZyWALL/USG's setting.

Configuration txt. File

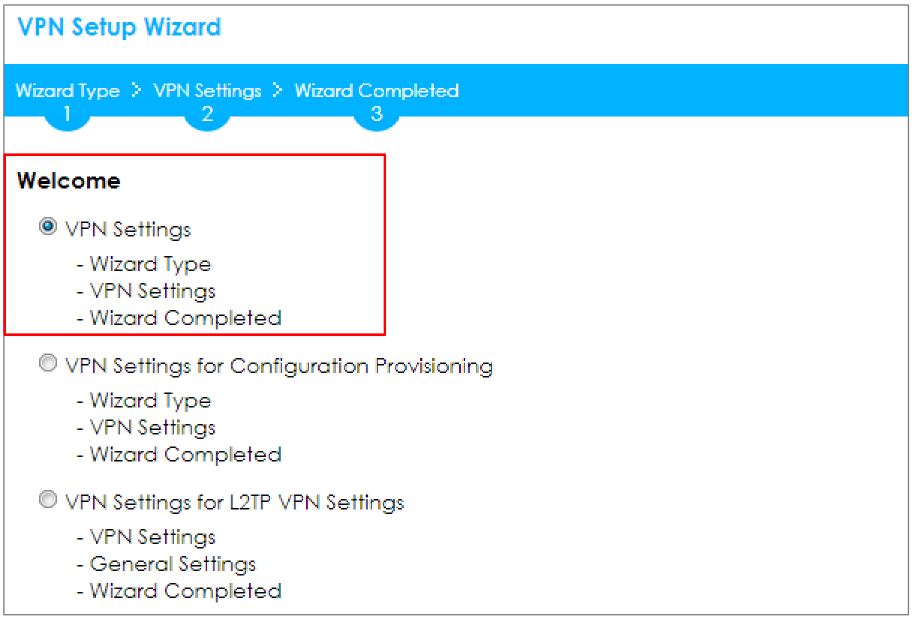


```
IPSec Tunnel #1
==========================================================================
#1: Internet Key Exchange Configuration
Configure the IKE SA as follows:
  - Authentication Method    : Pre-Shared Key
  - Pre-Shared Key           : 2EHrEA5WT6QFMEBaaPZT1bBmnoUaCLhW
  - Authentication Algorithm : sha1
  - Encryption Algorithm     : aes-128-cbc
  - Lifetime                 : 28800 seconds
  - Phase 1 Negotiation Mode : main
  - Perfect Forward Secrecy  : Diffie-Hellman Group 2

#2: IPSec Configuration
Configure the IPSec SA as follows:
  - Protocol                 : esp
  - Authentication Algorithm : hmac-sha1-96
  - Encryption Algorithm     : aes-128-cbc
  - Lifetime                 : 3600 seconds
  - Mode                     : tunnel
  - Perfect Forward Secrecy  : Diffie-Hellman Group 2

IPSec Dead Peer Detection (DPD) will be enabled on the AWS Endpoint. We
recommend configuring DPD on your endpoint as follows:
  - DPD Interval             : 10
  - DPD Retries              : 3
#3: Tunnel Interface Configuration
Outside IP Addresses:
  - Customer Gateway                : 61.230.249.133
  - Virtual Private Gateway         : 52.39.135.203
```

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the Amazon VPC. Click **Next**.

Quick Setup **> VPN Setup Wizard > Welcome**



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Welcome

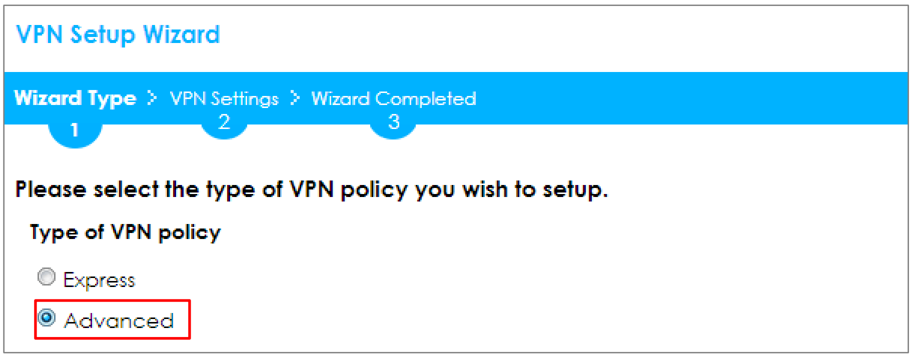
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



VPN Setup Wizard

Please select the type of VPN policy you wish to setup.

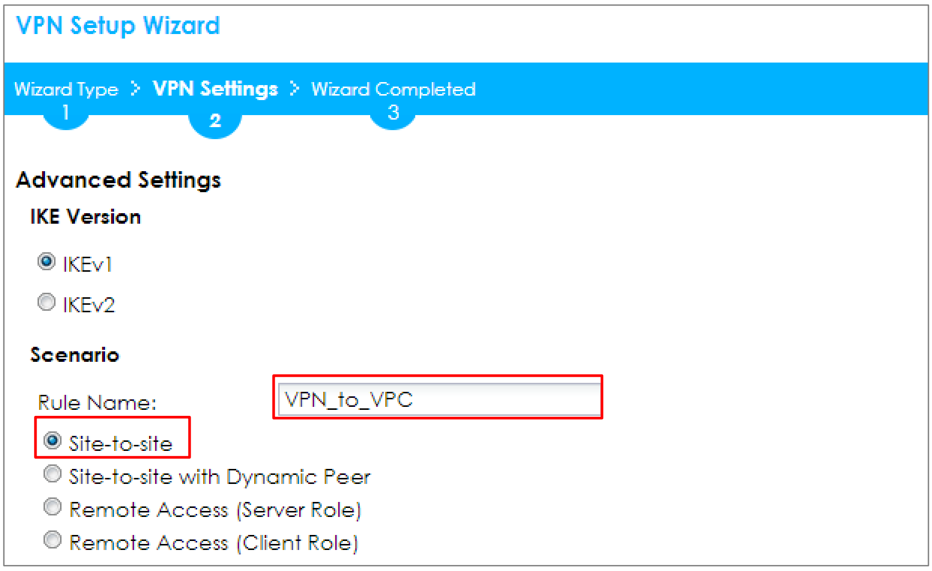
Type of VPN policy

○ Express

● Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup **> VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)**



VPN Setup Wizard

Advanced Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: VPN_to_VPC

● Site-to-site

○ Site-to-site with Dynamic Peer

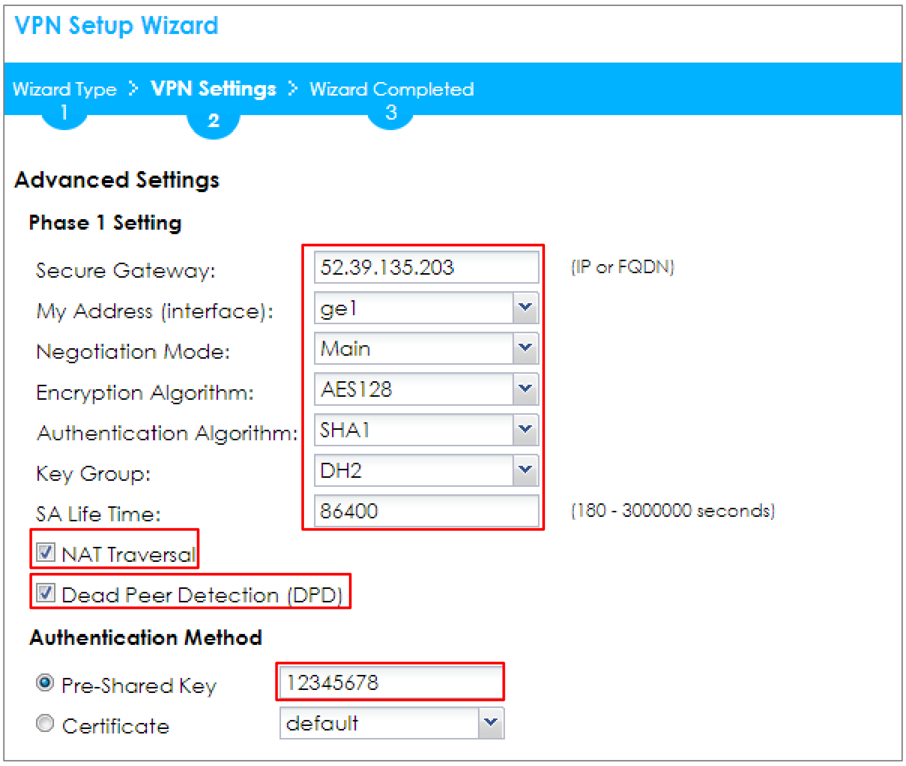
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the peer Amazon VPC's Gateway IP address (in the example, 52.39.135.203); select **My Address** to be the interface connected to the Internet.

Set the **Negotiation**, **Encryption**, **Authentication**, **Key Group** and **SA Life Time** which Amazon VPC supports. Type a secure **Pre-Shared Key**.

Quick Setup **> VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 1 Setting)**



Advanced Settings

Phase 1 Setting

Secure Gateway:	52.39.135.203	(IP or FQDN)
My Address (interface):	ge1	
Negotiation Mode:	Main	
Encryption Algorithm:	AES128	
Authentication Algorithm:	SHA1	
Key Group:	DH2	
SA Life Time:	86400	(180 - 3000000 seconds)

☑ NAT Traversal

☑ Dead Peer Detection (DPD)

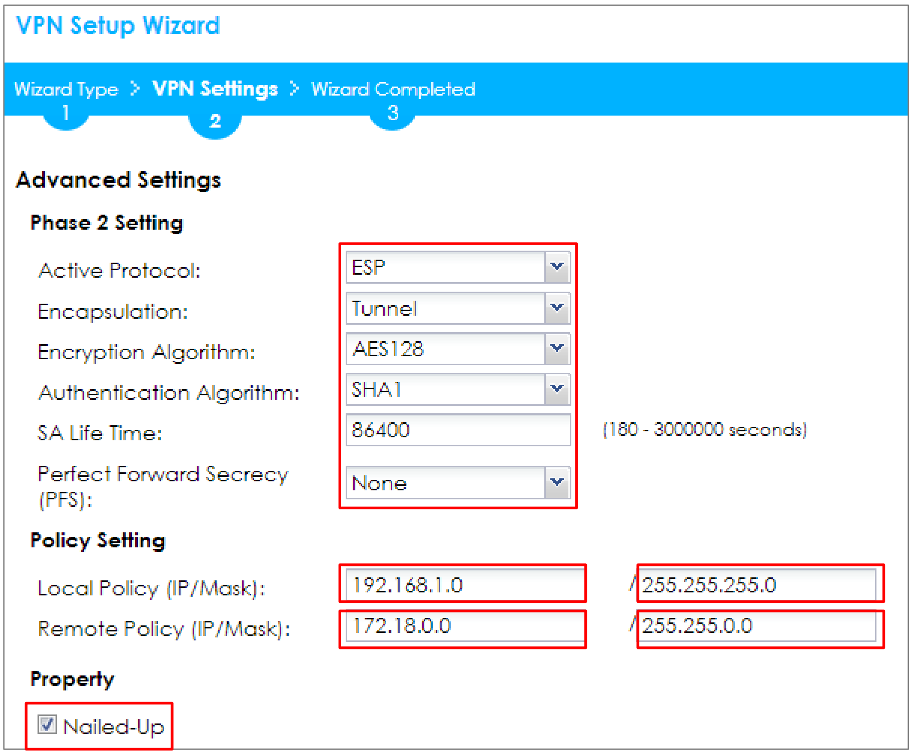
Authentication Method

● Pre-Shared Key 12345678

○ Certificate default

Continue to Phase 2 Settings to select the **Encapsulation**, **Encryption**, **Authentication**, and **SA Life Time** settings which Amazon VPC supports. Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the Amazon VPC. Click **OK**.

Quick Setup **> VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 2 Setting)**



VPN Setup Wizard

Wizard Type 1 > **VPN Settings 2** > Wizard Completed 3

Advanced Settings

Phase 2 Setting

Active Protocol:	ESP	
Encapsulation:	Tunnel	
Encryption Algorithm:	AES128	
Authentication Algorithm:	SHA1	
SA Life Time:	86400	(180 - 3000000 seconds)
Perfect Forward Secrecy (PFS):	None	

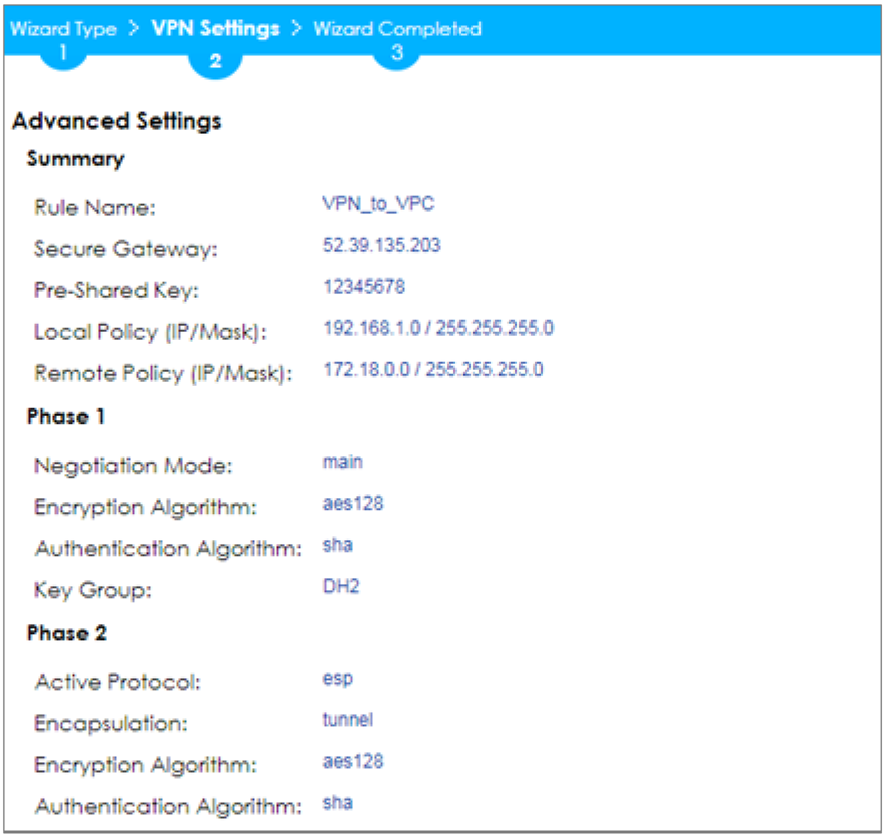
Policy Setting

Local Policy (IP/Mask):	192.168.1.0	/ 255.255.255.0
Remote Policy (IP/Mask):	172.18.0.0	/ 255.255.0.0

Property

☑ Nailed-Up

Quick Setup **> VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)**



Advanced Settings

Summary

Rule Name: VPN_to_VPC

Secure Gateway: 52.39.135.203

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 172.18.0.0 / 255.255.255.0

Phase 1

Negotiation Mode: main

Encryption Algorithm: aes128

Authentication Algorithm: sha

Key Group: DH2

Phase 2

Active Protocol: esp

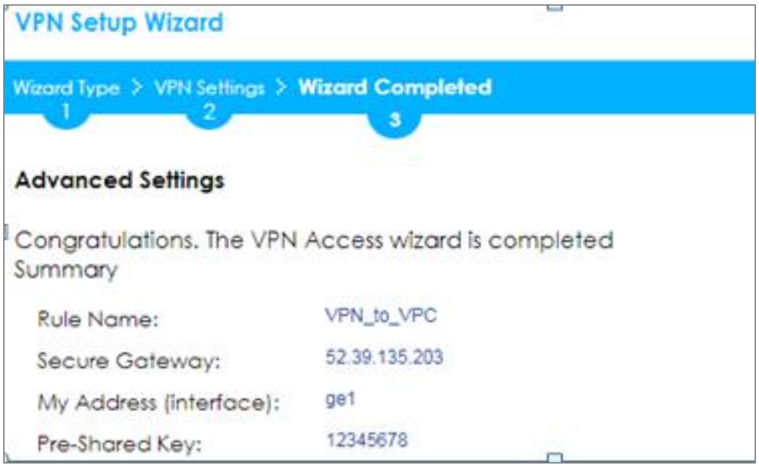
Encapsulation: tunnel

Encryption Algorithm: aes128

Authentication Algorithm: sha

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup **> VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed**



Advanced Settings

Congratulations. The VPN Access wizard is completed

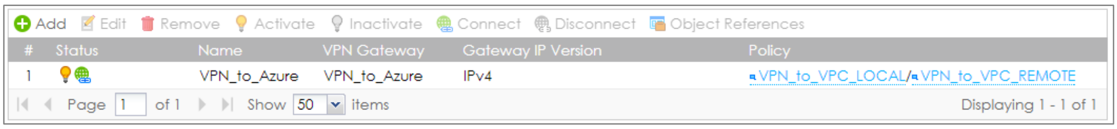
Summary

Rule Name:	VPN_to_VPC
Secure Gateway:	52.39.135.203
My Address (interface):	ge1
Pre-Shared Key:	12345678

Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

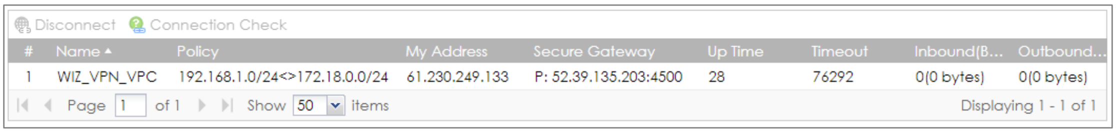


Add Edit Remove Activate Inactivate Connect Disconnect Object References
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

#	Status	Name	VPN Gateway	Gateway IP Version	Policy
1	💡●	VPN_to_Azure	VPN_to_Azure	IPv4	VPN_to_VPC_LOCAL/VPN_to_VPC_REMOTE

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec

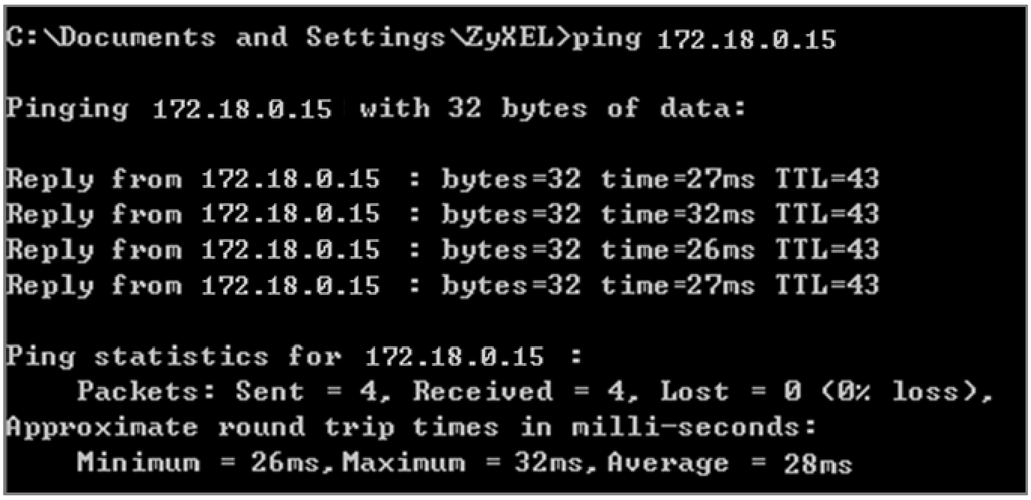


Disconnect Connection Check
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

#	Name ▲	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound(B...	Outbound...
1	WIZ_VPN_VPC	192.168.1.0/24<>172.18.0.0/24	61.230.249.133	P: 52.39.135.203:4500	28	76292	0(0 bytes)	0(0 bytes)

To test whether or not a tunnel is working, ping from a Local LAN to AWS VPC private Subnet for verification. Ensure that both computers have Internet access.

Ping from Local LAN to AWS VPC private Subnet for verification:

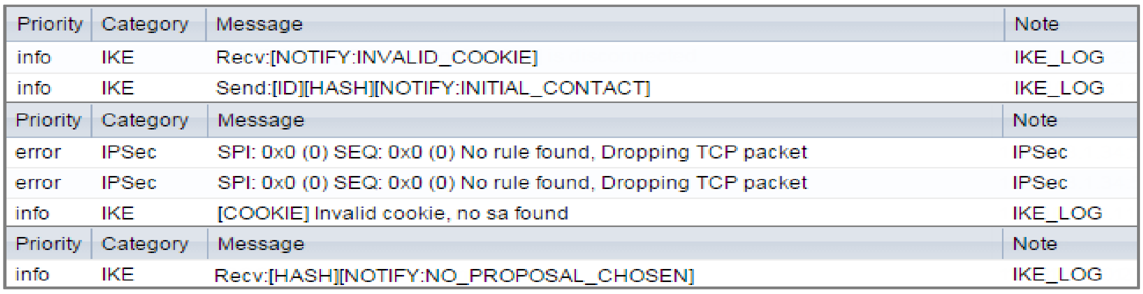


```
C:\Documents and Settings\ZyXEL>ping 172.18.0.15

Pinging 172.18.0.15 with 32 bytes of data:

Reply from 172.18.0.15 : bytes=32 time=27ms TTL=43
Reply from 172.18.0.15 : bytes=32 time=32ms TTL=43
Reply from 172.18.0.15 : bytes=32 time=26ms TTL=43
Reply from 172.18.0.15 : bytes=32 time=27ms TTL=43

Ping statistics for 172.18.0.15 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Make sure your ZyWALL/USG Phase 1 Settings are supported in the Amazon VPC IKE Phase 1 setup list.

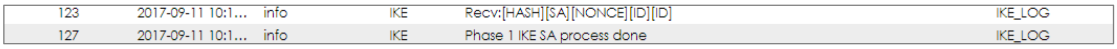
MONITOR > Log



Priority	Category	Message	Note
info	IKE	Recv:[NOTIFY:INVALID_COOKIE]	IKE_LOG
info	IKE	Send:[ID][HASH][NOTIFY:INITIAL_CONTACT]	IKE_LOG
Priority	Category	Message	Note
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
info	IKE	[COOKIE] Invalid cookie, no sa found	IKE_LOG
Priority	Category	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Make sure your ZyWALL/USG Phase 2 Settings are supported in the Amazon VPC IKE Phase 2 setup list.

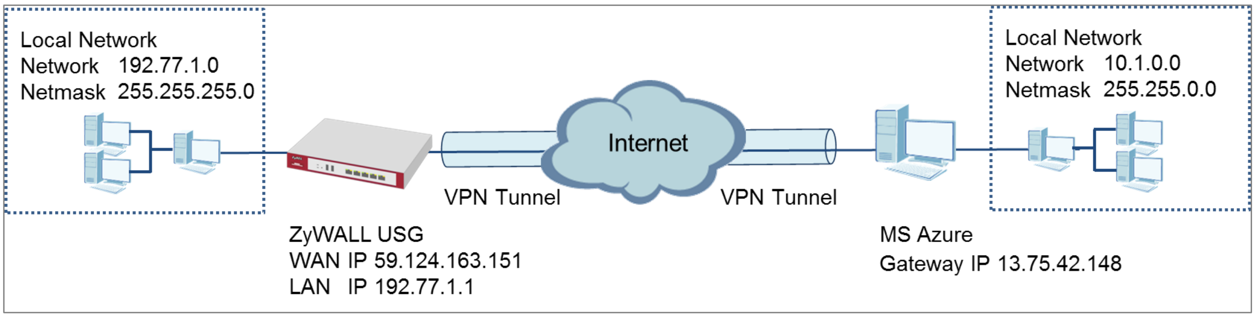
MONITOR > Log



123	2017-09-11 10:1...	info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
127	2017-09-11 10:1...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

How to Configure Site-to-site IPSec VPN with Microsoft (MS) Azure

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZyWALL/USG and a Microsoft (MS) Azure platform. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



ZyWALL Site-to-site IPSec VPN with Microsoft (MS) Azure

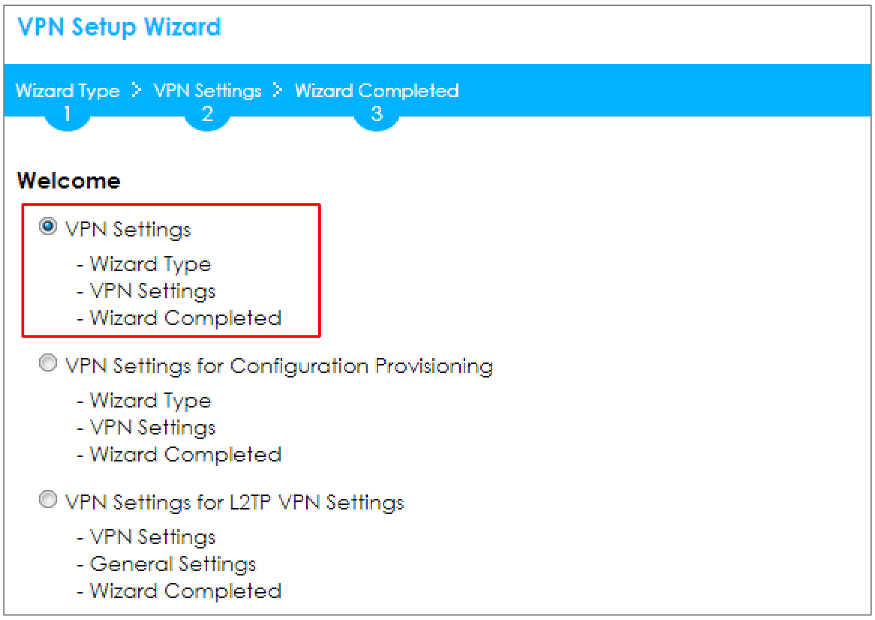
Note:

1. All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG40 (Firmware Version: ZLD 4.25) and MS Azure (April, 2016).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the MS Azure. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Welcome

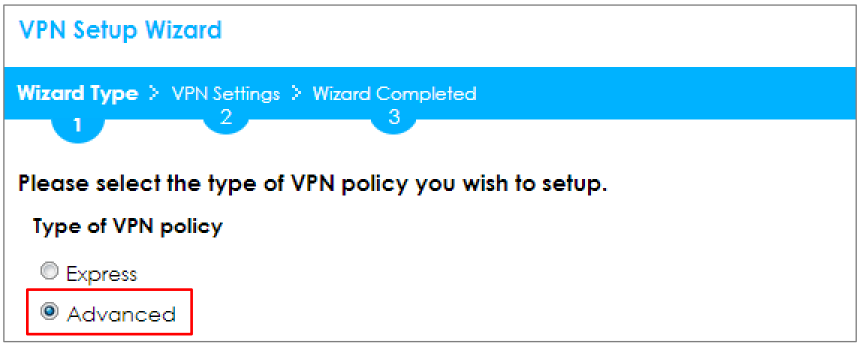
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Please select the type of VPN policy you wish to setup.

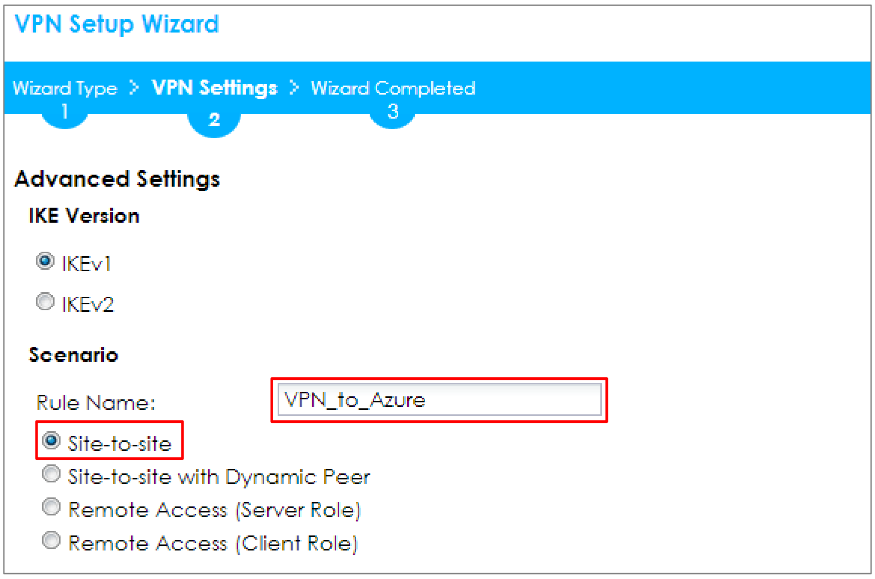
Type of VPN policy

○ Express

● Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Advanced Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: VPN_to_Azure

● Site-to-site

○ Site-to-site with Dynamic Peer

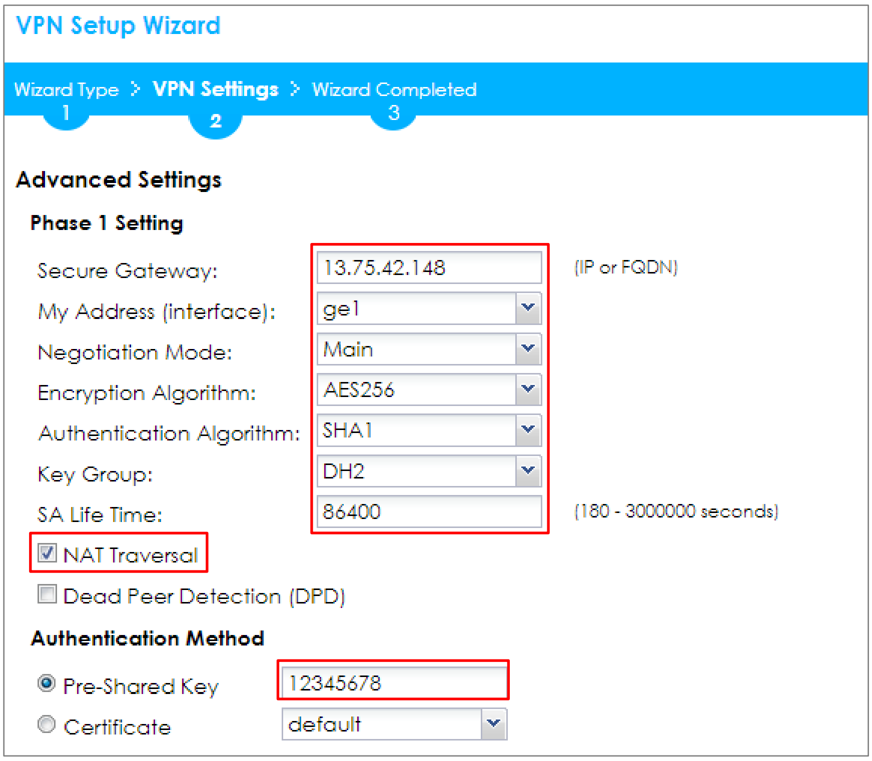
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the peer MS Azure's Gateway IP address (in the example, 13.75.42.148); select **My Address** to be the interface connected to the Internet.

Set the **Negotiation**, **Encryption**, **Authentication**, **Key Group** and **SA Life Time** which MS Azure supports. Please make sure you disable **Dead Peer Detection (DPD)** which is not supported in the MS Azure IKEv1 Policy-based. Type a secure **Pre-Shared Key**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 1 Setting)



VPN Setup Wizard

Advanced Settings

Phase 1 Setting

Secure Gateway:	13.75.42.148	(IP or FQDN)
My Address (interface):	ge1	
Negotiation Mode:	Main	
Encryption Algorithm:	AES256	
Authentication Algorithm:	SHA1	
Key Group:	DH2	
SA Life Time:	86400	(180 - 3000000 seconds)

☑ NAT Traversal

□ Dead Peer Detection (DPD)

Authentication Method

● Pre-Shared Key 12345678

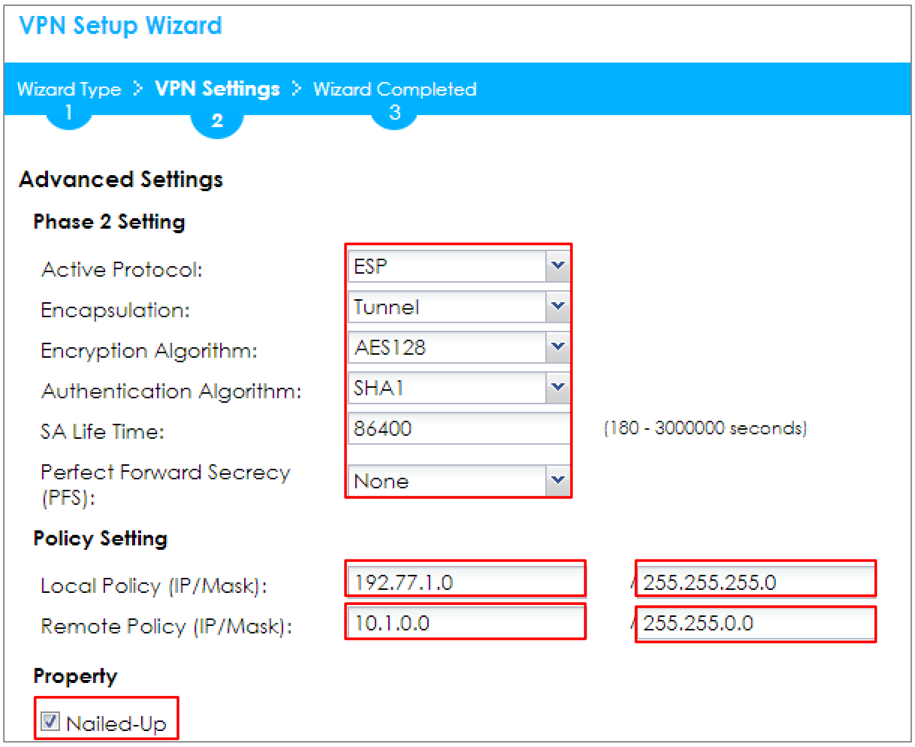
○ Certificate default

Note: For more information about the IPsec Parameters supported in MS Azure, see the Microsoft Azure Documentation **About VPN devices** for Site-to-Site VPN Gateway connections.

Continue to Phase 2 Settings to select the **Encapsulation**, **Encryption**, **Authentication**, and **SA Life Time** settings which MS Azure supports.

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the MS Azure. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 2 Setting)



Advanced Settings

Phase 2 Setting

Active Protocol:	ESP	
Encapsulation:	Tunnel	
Encryption Algorithm:	AES128	
Authentication Algorithm:	SHA1	
SA Life Time:	86400	(180 - 3000000 seconds)
Perfect Forward Secrecy (PFS):	None	

Policy Setting

Local Policy (IP/Mask):	192.77.1.0	/ 255.255.255.0
Remote Policy (IP/Mask):	10.1.0.0	/ 255.255.0.0

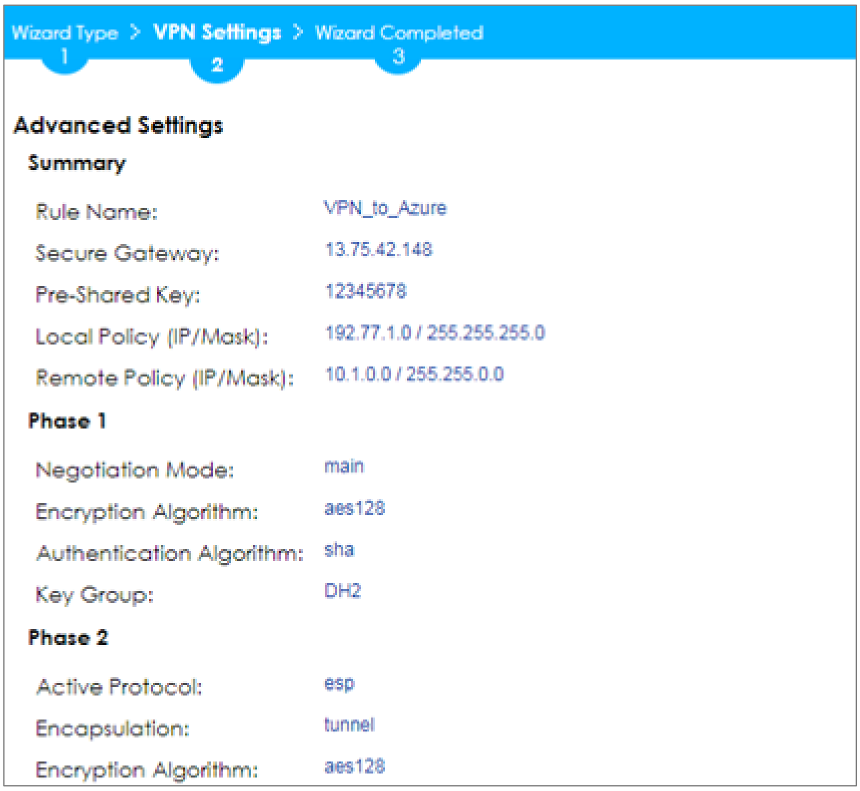
Property

☑ Nailed-Up

Note: For more information about the IPsec Parameters supported in MS Azure, see the Microsoft Azure Documentation [About VPN devices](#) for Site-to-Site VPN Gateway connections.

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



Advanced Settings

Summary

Rule Name:	VPN_to_Azure
Secure Gateway:	13.75.42.148
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.77.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	10.1.0.0 / 255.255.0.0

Phase 1

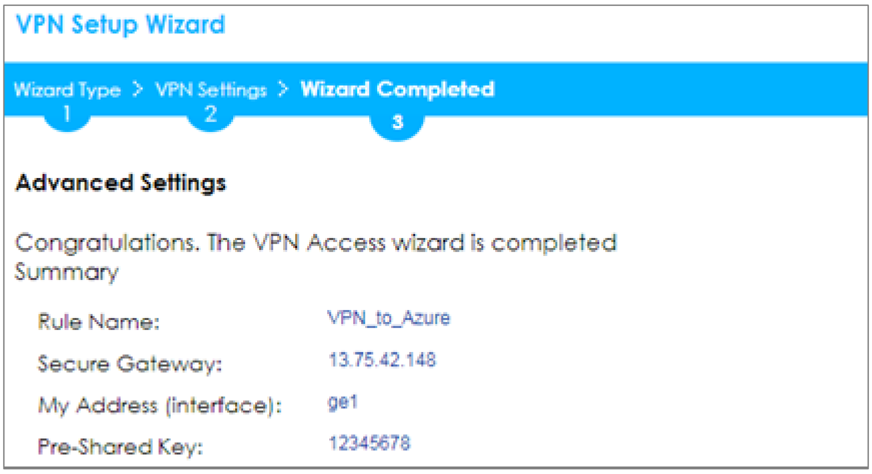
Negotiation Mode:	main
Encryption Algorithm:	aes128
Authentication Algorithm:	sha
Key Group:	DH2

Phase 2

Active Protocol:	esp
Encapsulation:	tunnel
Encryption Algorithm:	aes128

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



VPN Setup Wizard

Advanced Settings

Congratulations. The VPN Access wizard is completed

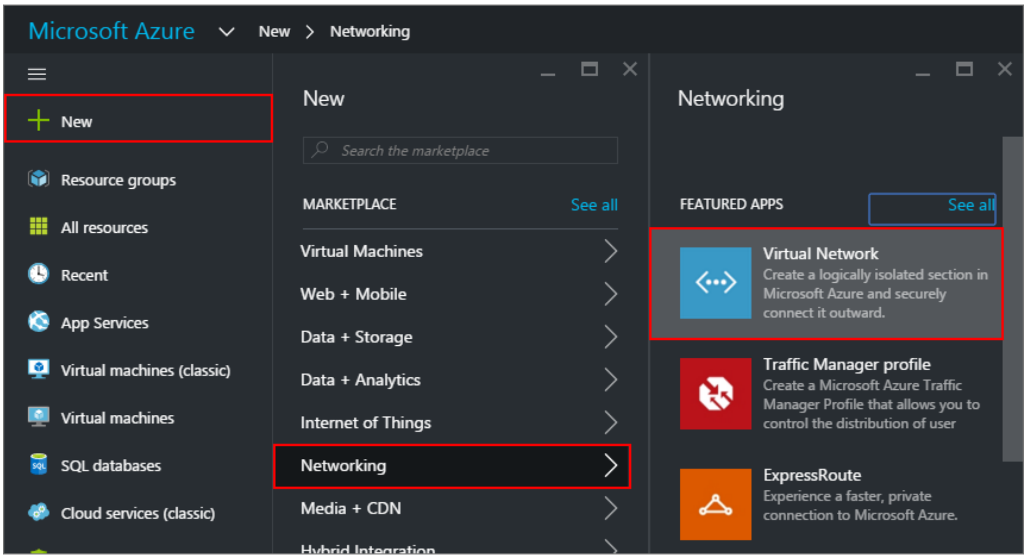
Summary

Rule Name:	VPN_to_Azure
Secure Gateway:	13.75.42.148
My Address (interface):	ge1
Pre-Shared Key:	12345678

Set Up the IPSec VPN Tunnel on the MS Azure

Sign into the **Windows Azure Management Portal**. In the upper left-hand corner of the screen, click **+New > Networking > Virtual Network**.

Azure portal > New > Networking > Virtual Network



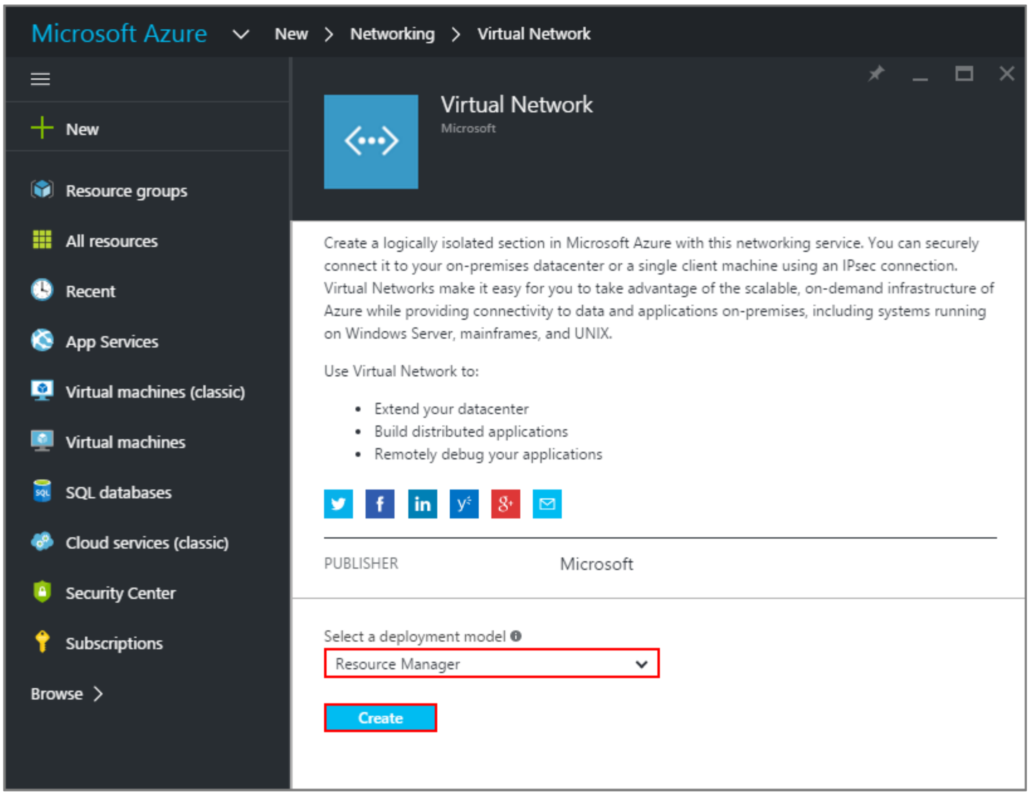
Virtual Network
Create a logically isolated section in Microsoft Azure and securely connect it outward.

Traffic Manager profile
Create a Microsoft Azure Traffic Manager Profile that allows you to control the distribution of user

ExpressRoute
Experience a faster, private connection to Microsoft Azure.

Near the bottom of the **Virtual Network** blade, from the **Select a deployment model** list, select **Resource Manager**, and then click **Create**.

New > Networking > Virtual Network > Select a deployment model



Create a logically isolated section in Microsoft Azure with this networking service. You can securely connect it to your on-premises datacenter or a single client machine using an IPsec connection. Virtual Networks make it easy for you to take advantage of the scalable, on-demand infrastructure of Azure while providing connectivity to data and applications on-premises, including systems running on Windows Server, mainframes, and UNIX.

Use Virtual Network to:

- Extend your datacenter
- Build distributed applications
- Remotely debug your applications

PUBLISHER Microsoft

Select a deployment model: Resource Manager

Create

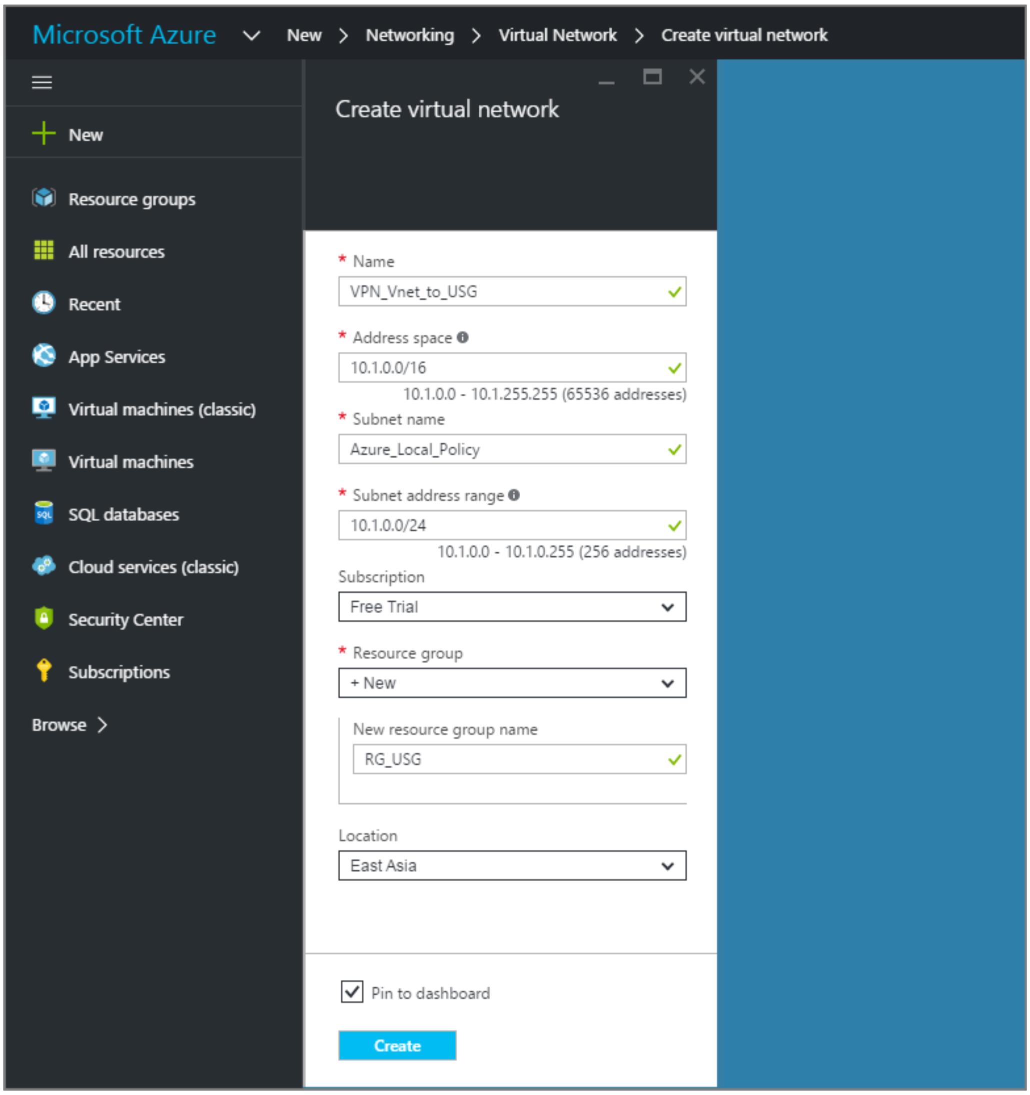
On the **Create virtual network** page, enter the **NAME** for the VPN network. For example, **VPN_Vnet_to_USG**. Add your **Address Space**, **Subnet name** and a single **Subnet address range**.

Click **Resource group** and either select an existing resource group, or create a new one by typing a name for your new resource group. For example, **RG_USG**.

LOCATION is directly related to the physical location (region) where the virtual machines (VMs) reside. The region associated with the virtual network cannot be changed after it has been created.

Then, click the **Create** button. After clicking Create, you will see a tile on your dashboard that will reflect the progress of your VNet. The tile will change as the VNet is being created.

New > Networking > Virtual Network > Create virtual network



Create virtual network

* Name: VPN_Vnet_to_USG ✓

* Address space: 10.1.0.0/16 ✓

10.1.0.0 - 10.1.255.255 (65536 addresses)

* Subnet name: Azure_Local_Policy ✓

* Subnet address range: 10.1.0.0/24 ✓

10.1.0.0 - 10.1.0.255 (256 addresses)

Subscription: Free Trial

* Resource group: + New

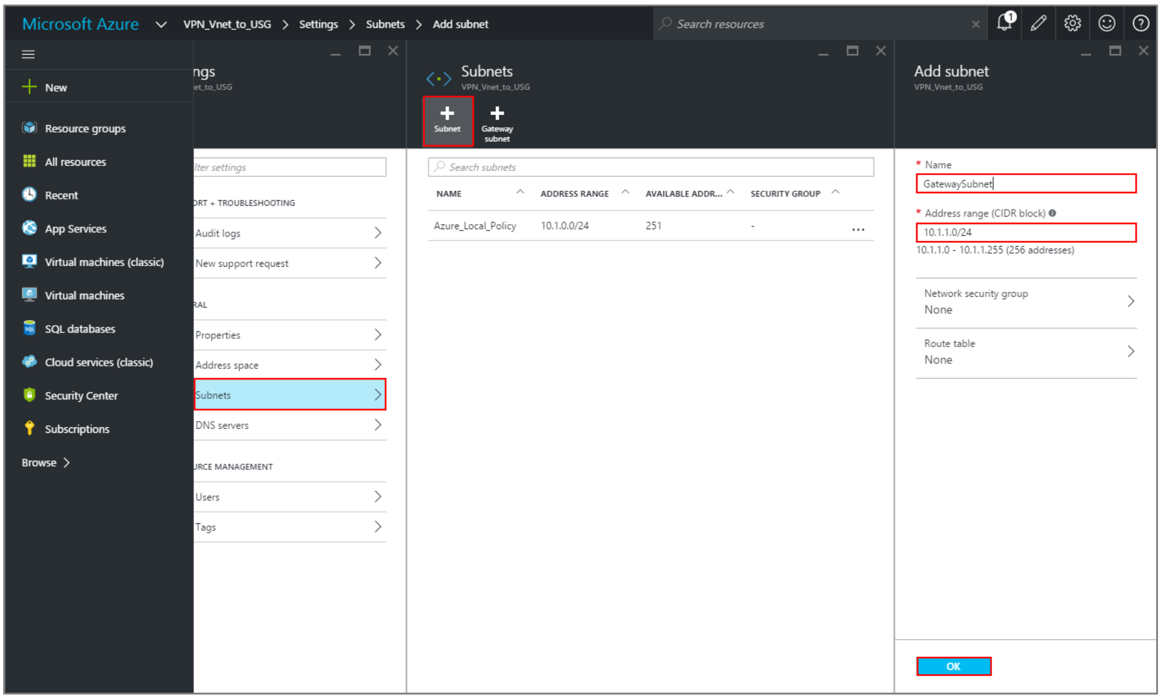
New resource group name: RG_USG ✓

Location: East Asia

☑ Pin to dashboard

In the portal, navigate to the virtual network to which you just created. On the blade for your virtual network, click the **Settings** icon at the top of the blade to expand the Setting blade to **Subnets > Add > Add Subnet**. **Name** your subnet **GatewaySubnet**. You should not name it anything else, or the gateway will not work. Add the IP **Address range** for your gateway. Click **OK** at the bottom of the blade to create the subnet.

VPN Vnet_to_USG > Settings > Subnet > Add subnet



NAME	ADDRESS RANGE	AVAILABLE ADDR...	SECURITY GROUP
Azure_Local_Policy	10.1.0.0/24	251	-

* Name: GatewaySubnet

* Address range (CIDR block): 10.1.1.0/24

10.1.1.0 - 10.1.1.255 (256 addresses)

Network security group: None

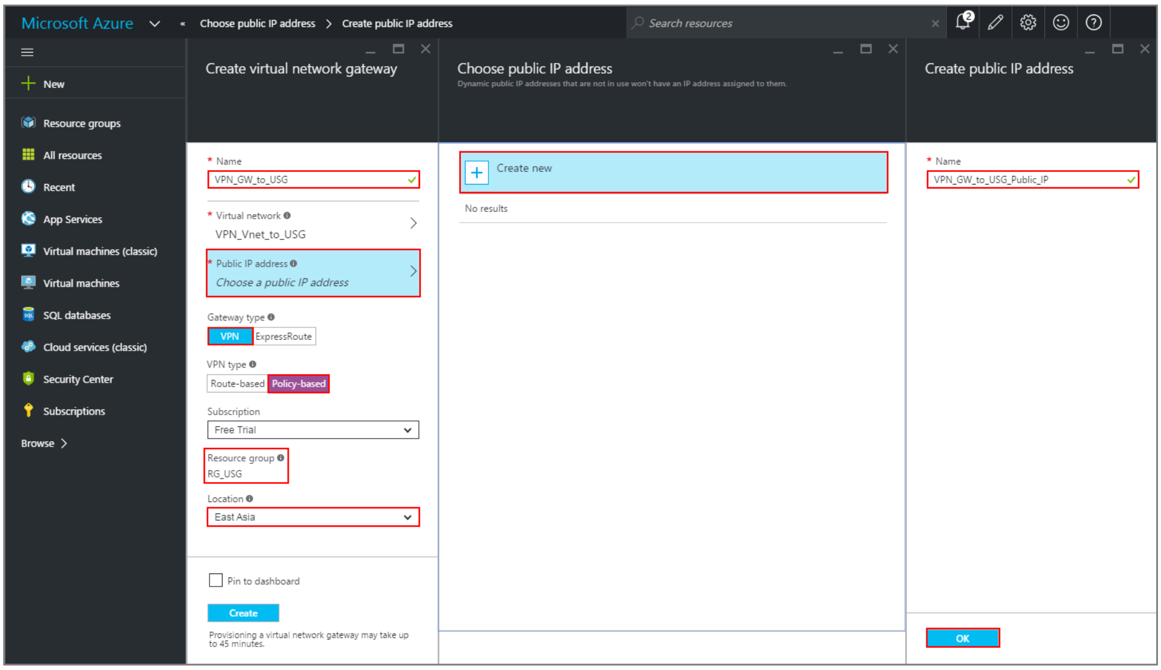
Route table: None

In the portal, go to **New**, then Networking. Select **Virtual network gateway** from the list. On the **Create virtual network gateway** blade **Name** field, name your gateway. Next, choose the **Virtual network** that you want to deploy this gateway to.

Click the arrow (>) to open the **Choose public IP address** blade. Then click **Create New** to open the **Create public IP address** blade. Input a **Name** for your public IP address. Note that this is not asking for an IP address. The IP address will be assigned dynamically. Rather, this is the name of the IP address object that the address will be assigned to. Click **OK** to save your changes.

For **Gateway type**, select **VPN**. For **VPN type**, select **Policy-based**. For **Resource Group**, the resource group is determined by the Virtual Network that you select. For **Location**, make sure it's showing the location that both your Resource Group and VNet exist in.

New > Networking > Create virtual network gateway > Choose public IP address > Create public IP address



Create virtual network gateway

* Name: VPN_GW_to_USG

* Virtual network: VPN_Vnet_to_USG

* Public IP address: *Choose a public IP address*

Gateway type: VPN | ExpressRoute

VPN type: Route-based | Policy-based

Subscription: Free Trial

Resource group: RG_USG

Location: East Asia

□ Pin to dashboard

Create

Provisioning a virtual network gateway may take up to 45 minutes.

Choose public IP address

Dynamic public IP addresses that are not in use won't have an IP address assigned to them.

Create new

No results

Create public IP address

* Name: VPN_GW_to_USG_Public_IP

OK

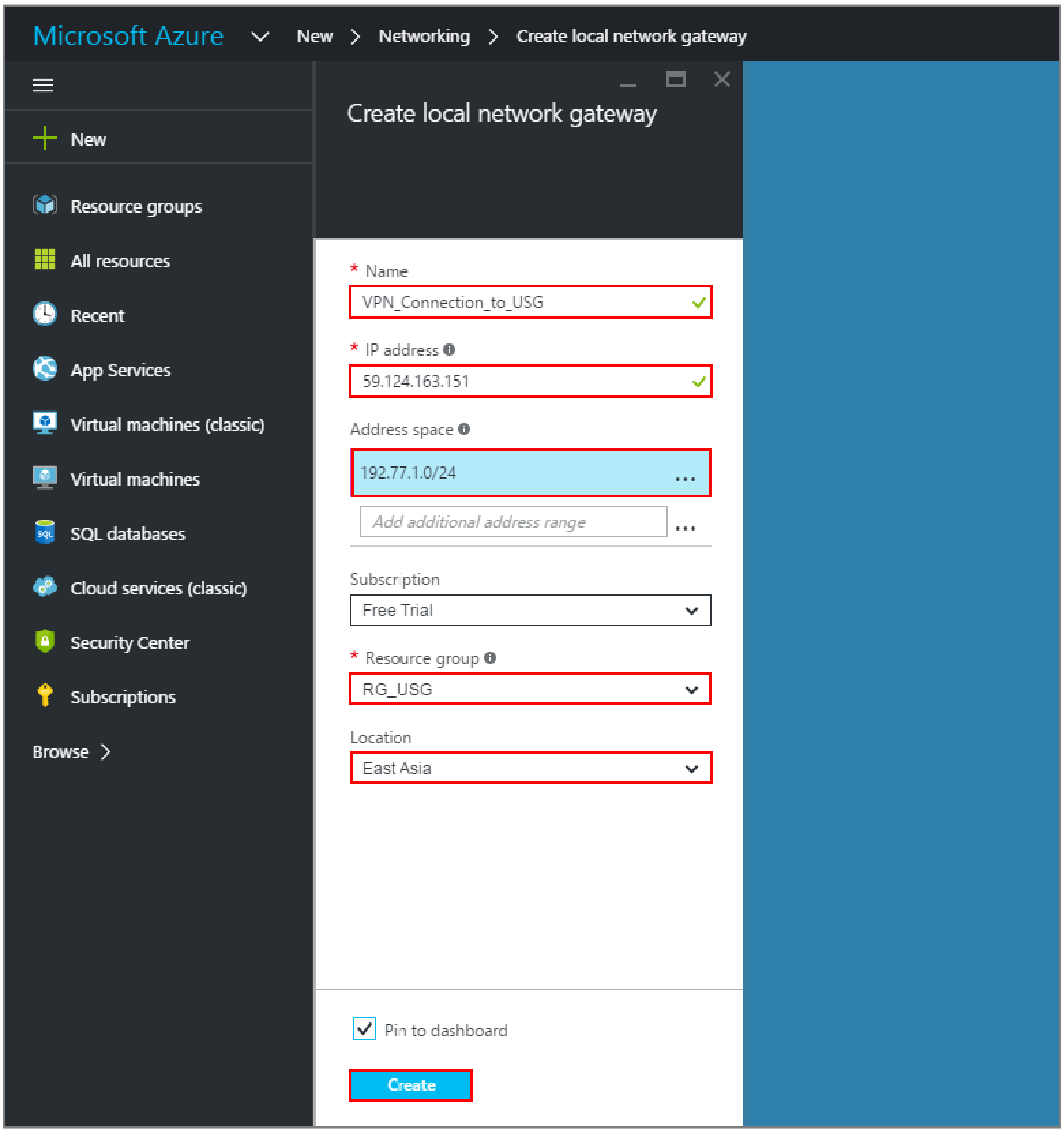
In the Azure Portal, navigate to **New > Networking > Local network gateway**. The local network gateway refers to your ZyWALL/USG public IP and local subnet settings.

On the **Create local network gateway** blade, specify a **Name** for your ZyWALL/USG gateway object.

Specify public IP address of your ZyWALL/USG. It cannot be behind NAT and has to be reachable by Azure. **Address space** refers to the address ranges on your ZyWALL/USG local network. For **Resource Group**, select the resource group that you created before. For **Location**, if you are creating a new local network gateway, you can use the same location as the virtual network gateway. But, this is not required. The local network gateway can be in a different location.

Click **Create** to create the local network gateway.

New > Networking > Local network gateway



* Name: VPN_Connection_to_USG

* IP address: 59.124.163.151

Address space: 192.77.1.0/24

Add additional address range

Subscription: Free Trial

* Resource group: RG_USG

Location: East Asia

☑ Pin to dashboard

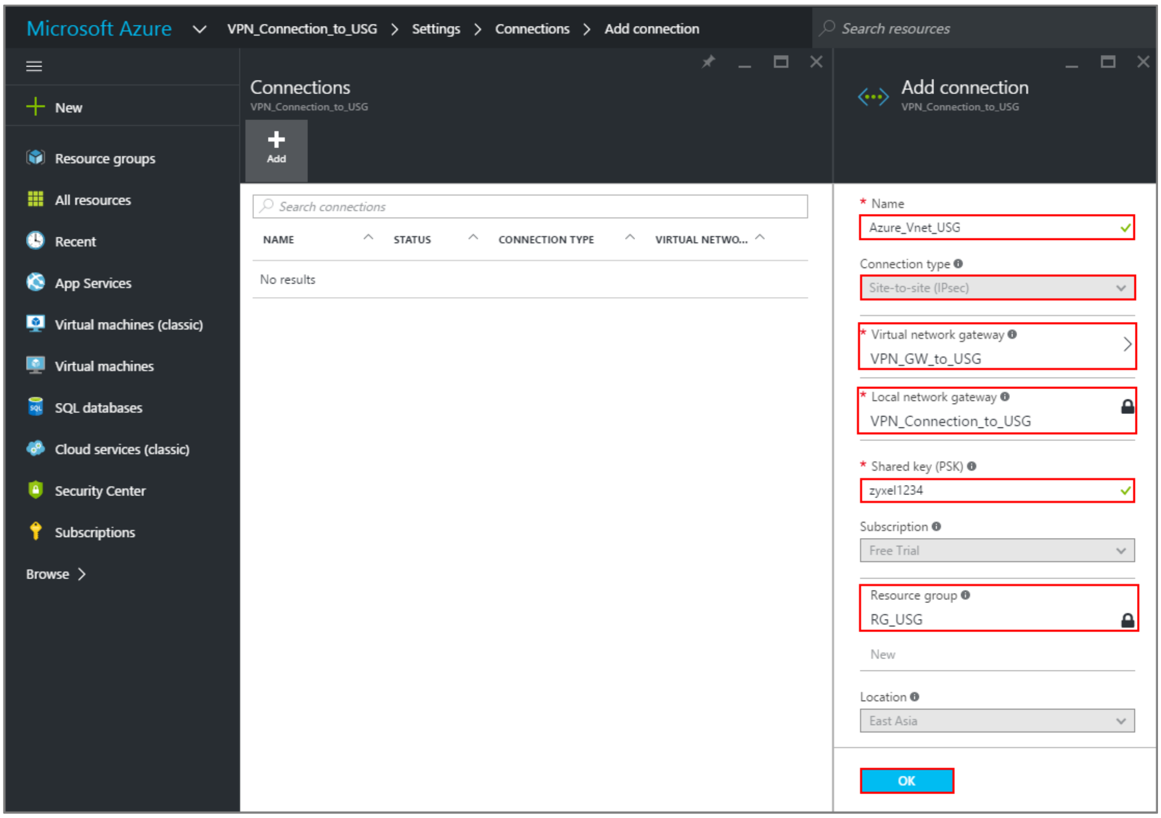
Create

Locate your virtual network gateway (VPN_Connection_to_USG in this example) and click **Settings > Connection > Add connection**, **Name** your connection. For **Connection type**, select **Site-to-site (IPSec)**. For **Virtual network gateway**, the value is fixed because you are connecting from this gateway (VPN_GW_to_USG in this example).

For **Local network gateway**, select the local network gateway that you want to use (VPN_Connection_to_USG in this example).

For **Shared Key (PSK)**, the value here must match the value that you are using for your ZyWALL/USG device. For **Resource Group**, select the resource group that you **created before**. Click **OK** to create your connection.

VPN_Connection_to_USG > Settings > Connections > Add connection



* Name: Azure_Vnet_USG

Connection type: Site-to-site (IPsec)

* Virtual network gateway: VPN_GW_to_USG

* Local network gateway: VPN_Connection_to_USG

* Shared key (PSK): zyxel1234

Subscription: Free Trial

Resource group: RG_USG

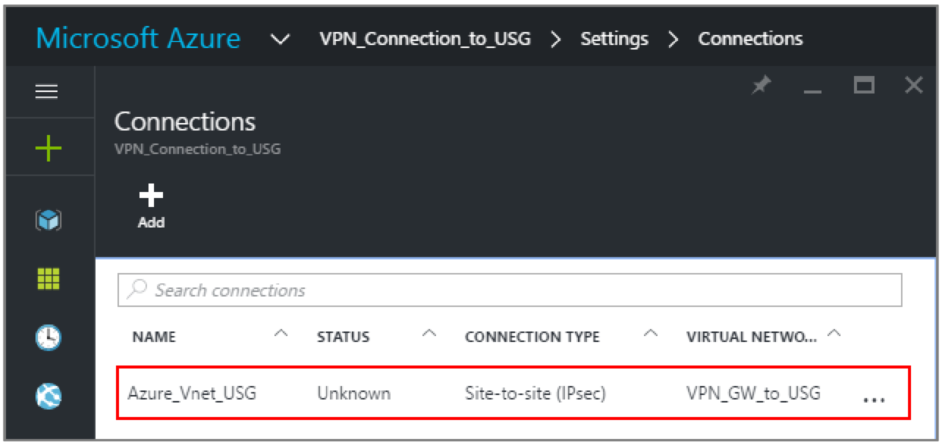
New

Location: East Asia

OK

When the connection is complete, you'll see it appear in the **Connections** blade for your Gateway.

VPN_Connection_to_USG > Settings > Connections

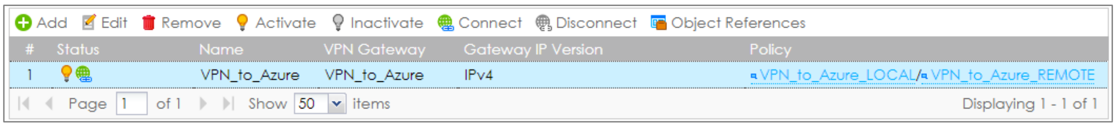


NAME	STATUS	CONNECTION TYPE	VIRTUAL NETWO...	
Azure_Vnet_USG	Unknown	Site-to-site (IPsec)	VPN_GW_to_USG	...

Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

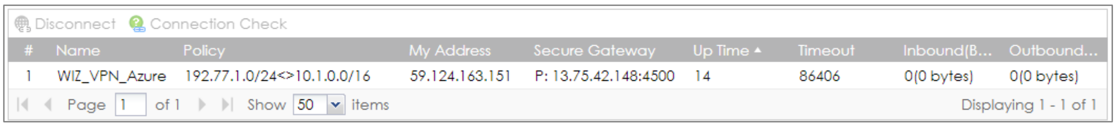
CONFIGURATION > VPN > IPSec VPN > VPN Connection



#	Status	Name	VPN Gateway	Gateway IP Version	Policy
1		VPN_to_Azure	VPN_to_Azure	IPv4	VPN_to_Azure_LOCAL/VPN_to_Azure_REMOTE

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec

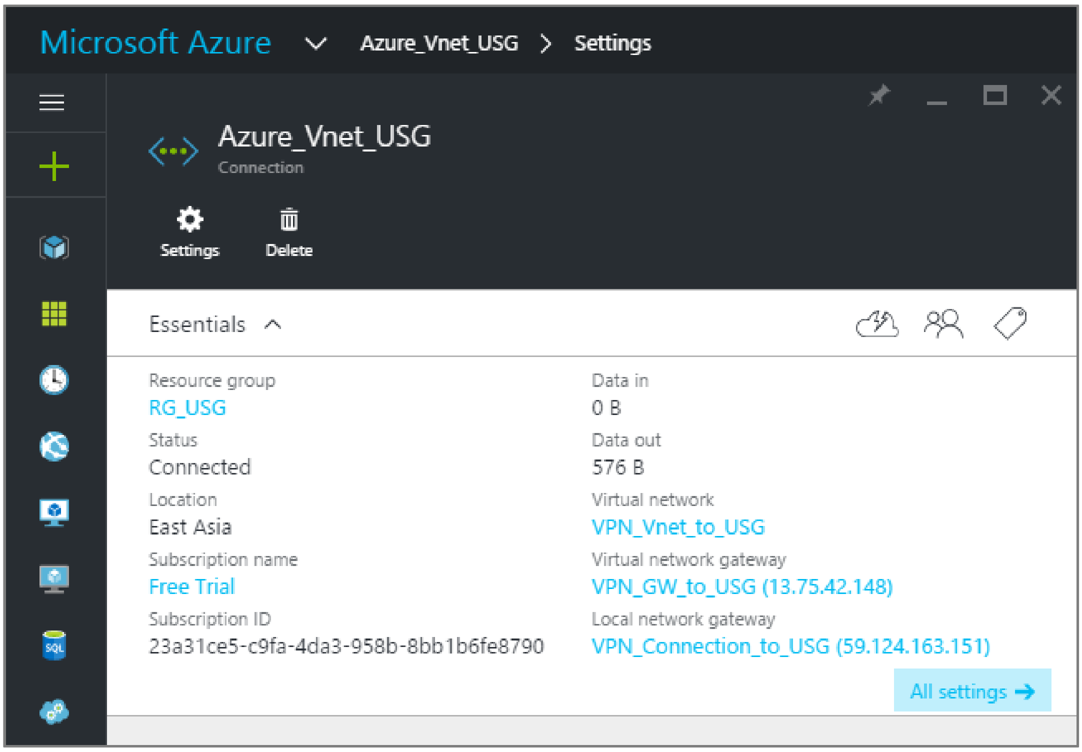


#	Name	Policy	My Address	Secure Gateway	Up Time ▲	Timeout	Inbound(B...	Outbound...
1	WIZ_VPN_Azure	192.77.1.0/24<>10.1.0.0/16	59.124.163.151	P: 13.75.42.148:4500	14	86406	0(0 bytes)	0(0 bytes)

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

Go to **Azure_Vnet_USG > Settings** to check the tunnel **DATA IN** and **DATA OUT**.

VPN > VPN Settings > Currently Active VPN Tunnels



Resource group
RG_USG

Status
Connected

Location
East Asia

Subscription name
Free Trial

Subscription ID
23a31ce5-c9fa-4da3-958b-8bb1b6fe8790

Data in
0 B

Data out
576 B

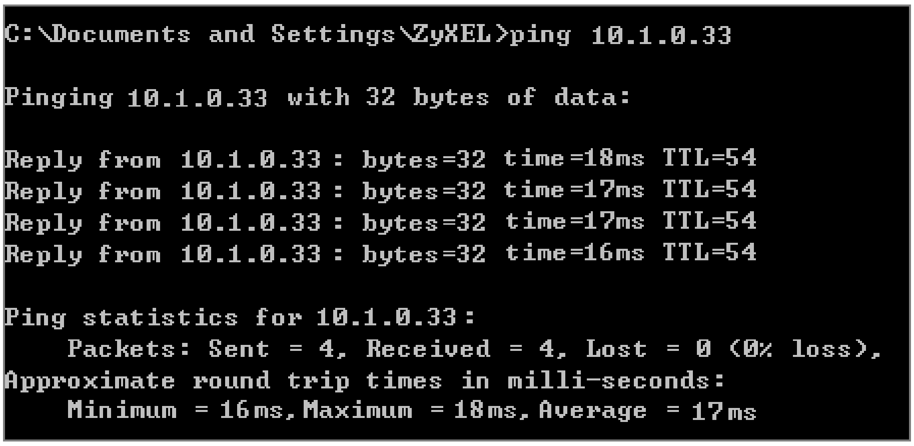
Virtual network
VPN_Vnet_to_USG

Virtual network gateway
VPN_GW_to_USG (13.75.42.148)

Local network gateway
VPN_Connection_to_USG (59.124.163.151)

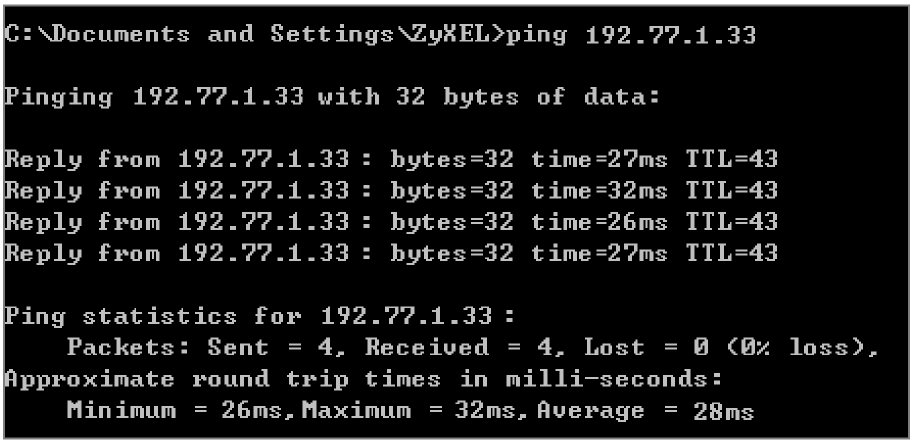
To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access.

PC behind ZyWALL/USG > Window 7 > cmd > ping 10.1.0.33



```
C:\Documents and Settings\ZyXEL>ping 10.1.0.33

Pinging 10.1.0.33 with 32 bytes of data:

Reply from 10.1.0.33 : bytes=32 time=18ms TTL=54
Reply from 10.1.0.33 : bytes=32 time=17ms TTL=54
Reply from 10.1.0.33 : bytes=32 time=17ms TTL=54
Reply from 10.1.0.33 : bytes=32 time=16ms TTL=54

Ping statistics for 10.1.0.33 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC behind MS Azure> Window 7 > cmd > ping 192.77.1.33

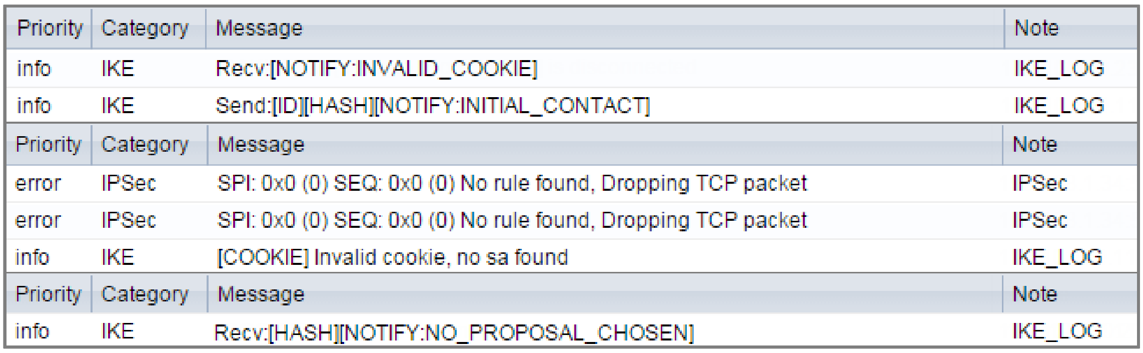


```
C:\Documents and Settings\ZyXEL>ping 192.77.1.33

Pinging 192.77.1.33 with 32 bytes of data:

Reply from 192.77.1.33 : bytes=32 time=27ms TTL=43
Reply from 192.77.1.33 : bytes=32 time=32ms TTL=43
Reply from 192.77.1.33 : bytes=32 time=26ms TTL=43
Reply from 192.77.1.33 : bytes=32 time=27ms TTL=43

Ping statistics for 192.77.1.33 :
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Make sure your ZyWALL/USG Phase 1 Settings are supported in the MS Azure IKE Phase 1 setup list.

MONITOR > Log



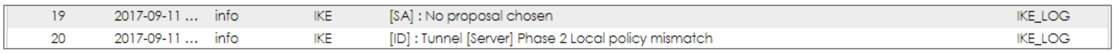
Priority	Category	Message	Note
info	IKE	Recv:[NOTIFY:INVALID_COOKIE]	IKE_LOG
info	IKE	Send:[ID][HASH][NOTIFY:INITIAL_CONTACT]	IKE_LOG

Priority	Category	Message	Note
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
info	IKE	[COOKIE] Invalid cookie, no sa found	IKE_LOG

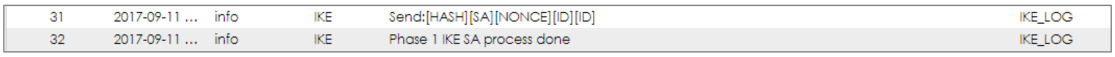
Priority	Category	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Make sure your ZyWALL/USG Phase 2 Settings are supported in the MS Azure IKE Phase 2 setup list.

MONITOR > Log



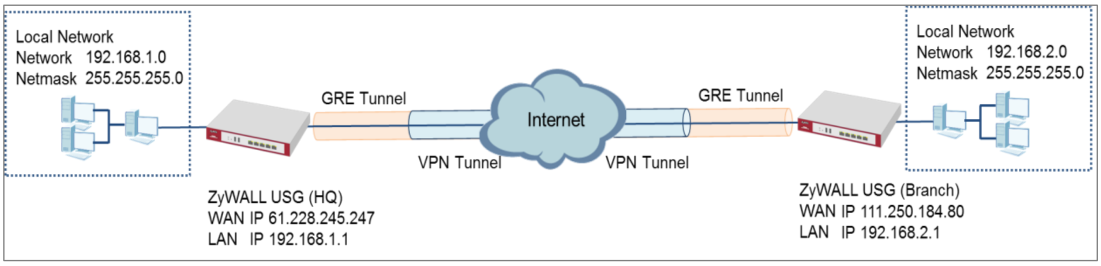
```
19    2017-09-11 ...   info    IKE    [SA] : No proposal chosen                              IKE_LOG
20    2017-09-11 ...   info    IKE    [ID] : Tunnel [Server] Phase 2 Local policy mismatch   IKE_LOG
```



```
31    2017-09-11 ...   info    IKE    Send:[HASH][SA][NONCE][ID][ID]                          IKE_LOG
32    2017-09-11 ...   info    IKE    Phase 1 IKE SA process done                             IKE_LOG
```

How to Configure GRE over IPSec VPN Tunnel

This example shows how to use the VPN Setup Wizard to create a GRE over IPSec VPN tunnel between ZyWALL/USG devices. The example instructs how to configure the VPN tunnel between each site. When the GRE over IPSec VPN tunnel is configured, each site can be accessed securely.



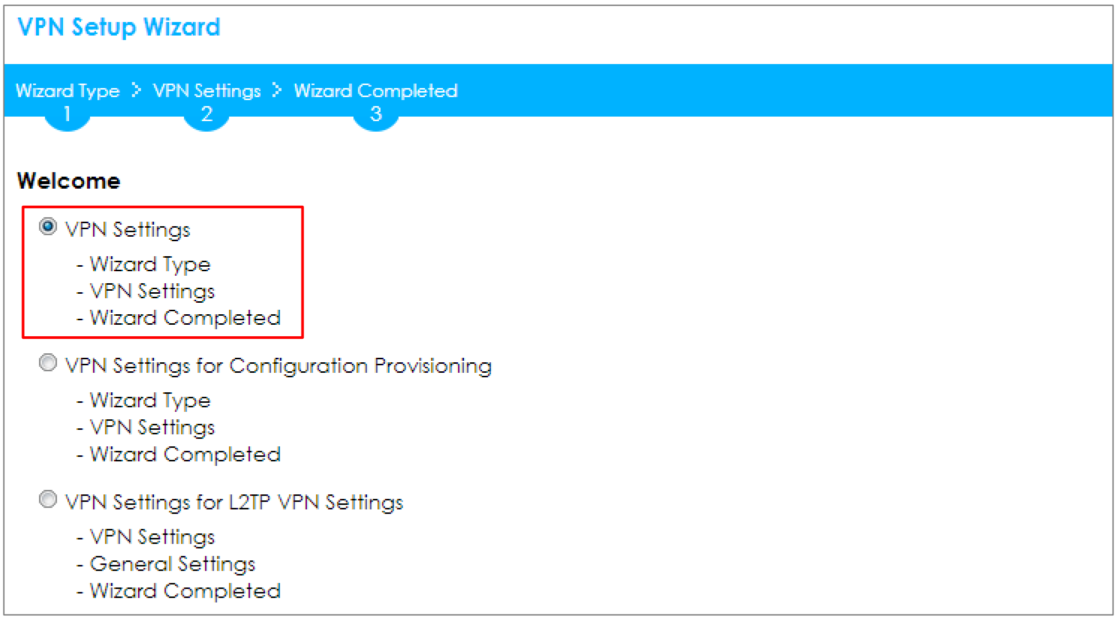
ZyWALL/USG GRE over IPSec VPN

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25) and ZyWALL 310 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG GRE over IPSec VPN Tunnel of Corporate Network (HQ)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup **> VPN Setup Wizard > Welcome**



VPN Setup Wizard

Welcome

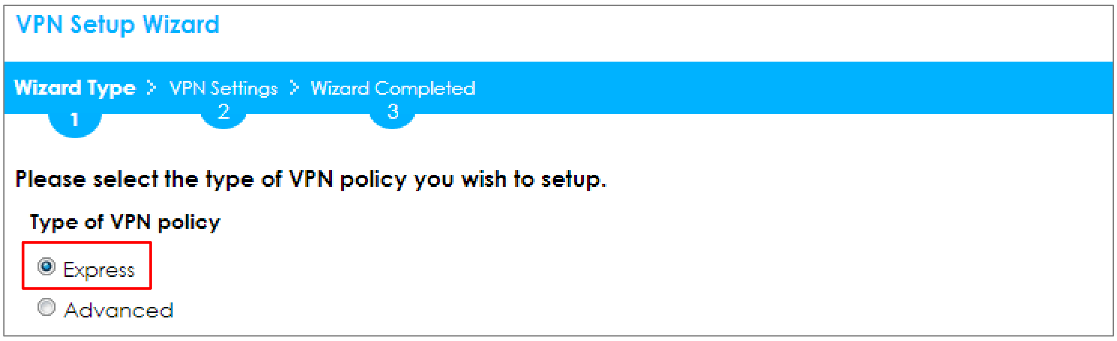
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup **> VPN Setup Wizard > Wizard Type**



VPN Setup Wizard

Please select the type of VPN policy you wish to setup.

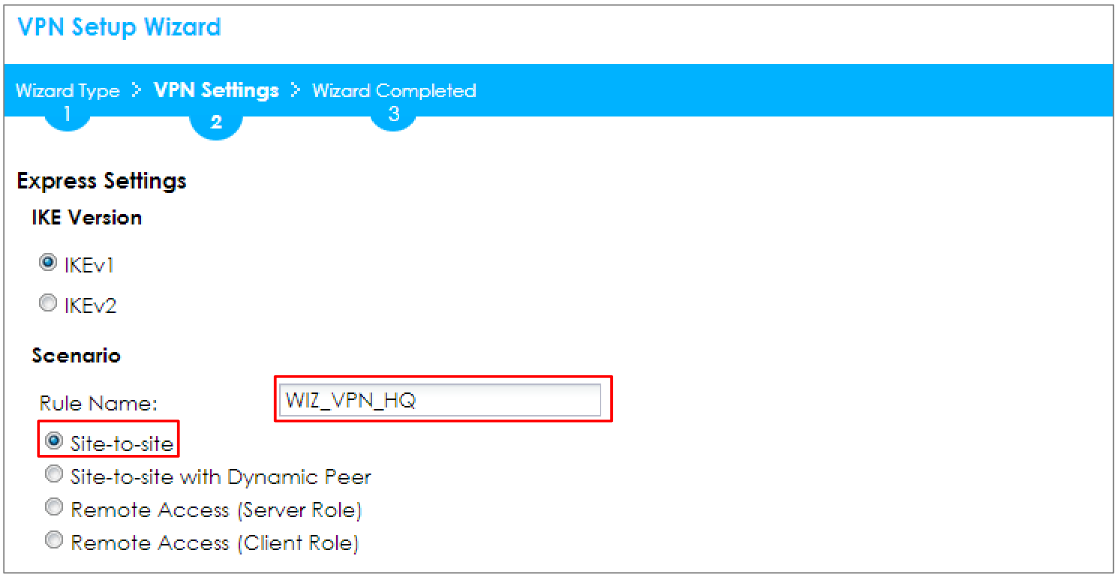
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: WIZ_VPN_HQ

● Site-to-site

○ Site-to-site with Dynamic Peer

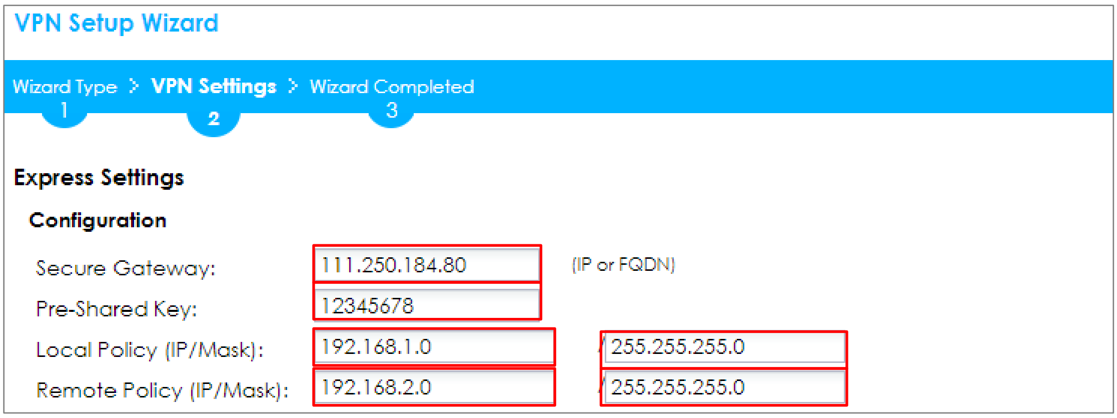
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the Branch's WAN IP address (in the example, 111.250.184.80). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG (HQ) and **Remote Policy** to be the IP address range of the network connected to the ZyWALL/USG (Branch).

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



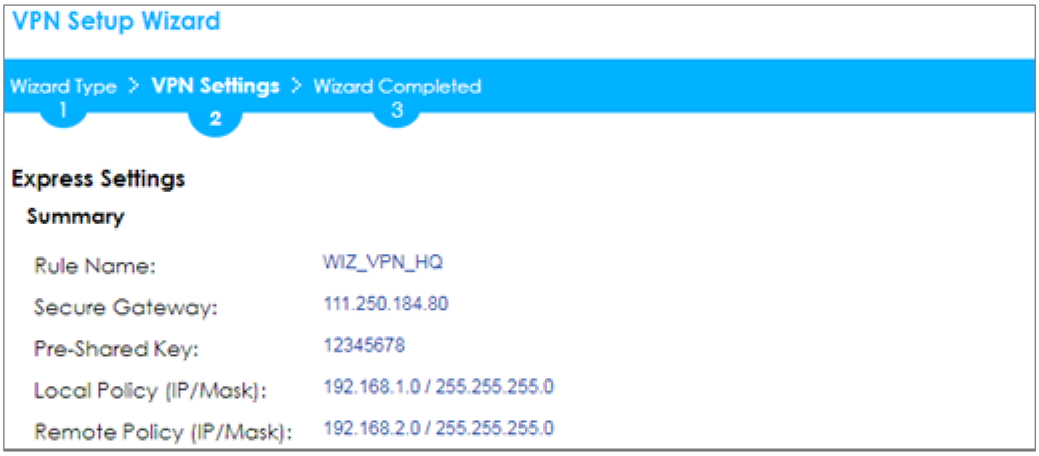
Express Settings

Configuration

Secure Gateway:	111.250.184.80	(IP or FQDN)
Pre-Shared Key:	12345678	
Local Policy (IP/Mask):	192.168.1.0	255.255.255.0
Remote Policy (IP/Mask):	192.168.2.0	255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



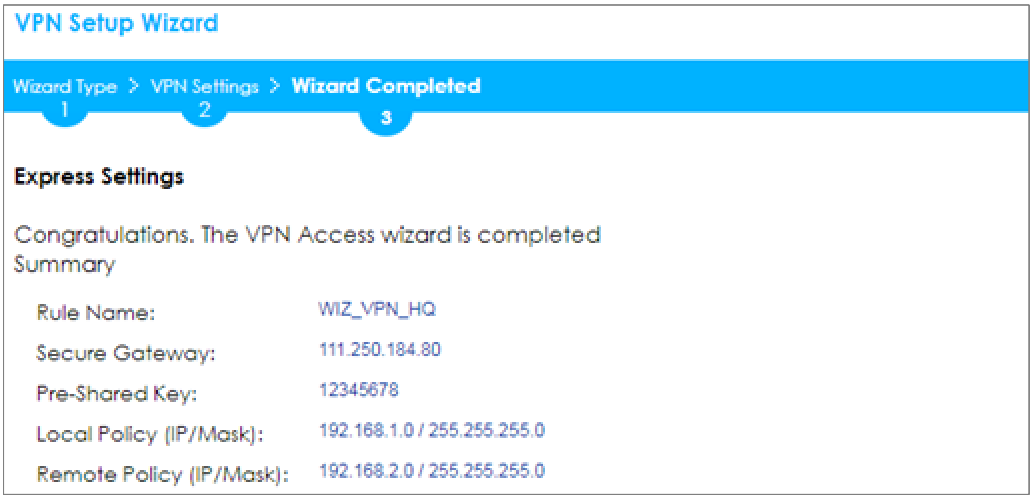
Express Settings

Summary

Rule Name:	WIZ_VPN_HQ
Secure Gateway:	111.250.184.80
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.2.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



Express Settings

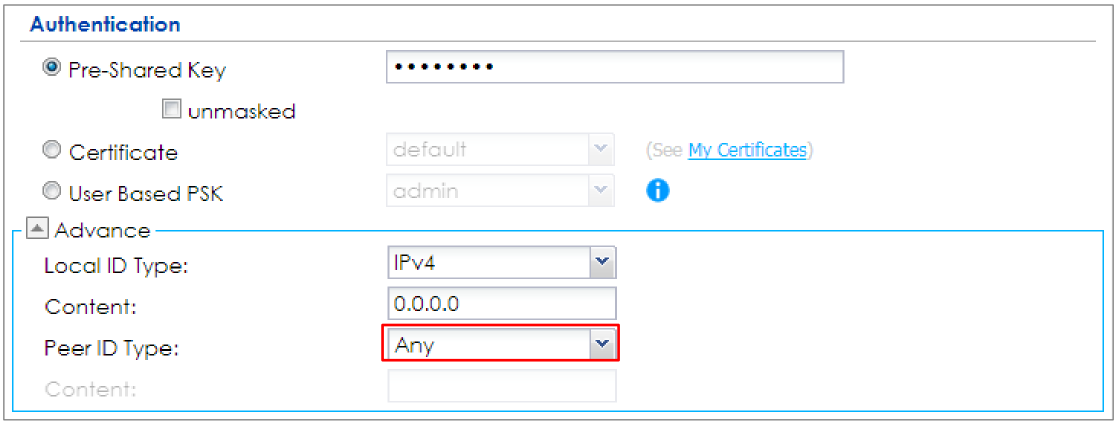
Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_VPN_HQ
Secure Gateway:	111.250.184.80
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.2.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

● Pre-Shared Key: •••••••••

□ unmasked

○ Certificate: default (See My Certificates)

○ User Based PSK: admin

Advance

Local ID Type: IPv4

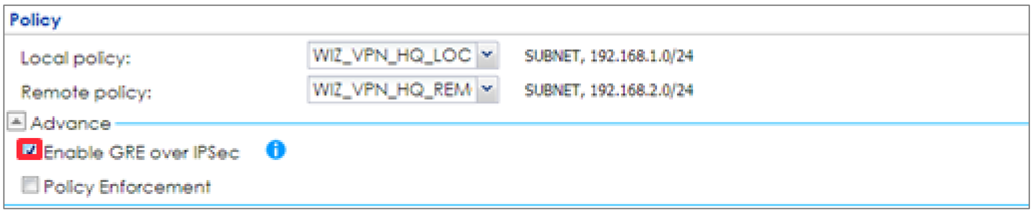
Content: 0.0.0.0

Peer ID Type: Any

Content:

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** > **Show Advanced Settings > Policy**. Select **Enable GRE over IPSec**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Show Advanced Settings > Policy



Policy

Local policy: WIZ_VPN_HQ_LOC SUBNET, 192.168.1.0/24

Remote policy: WIZ_VPN_HQ_REM SUBNET, 192.168.2.0/24

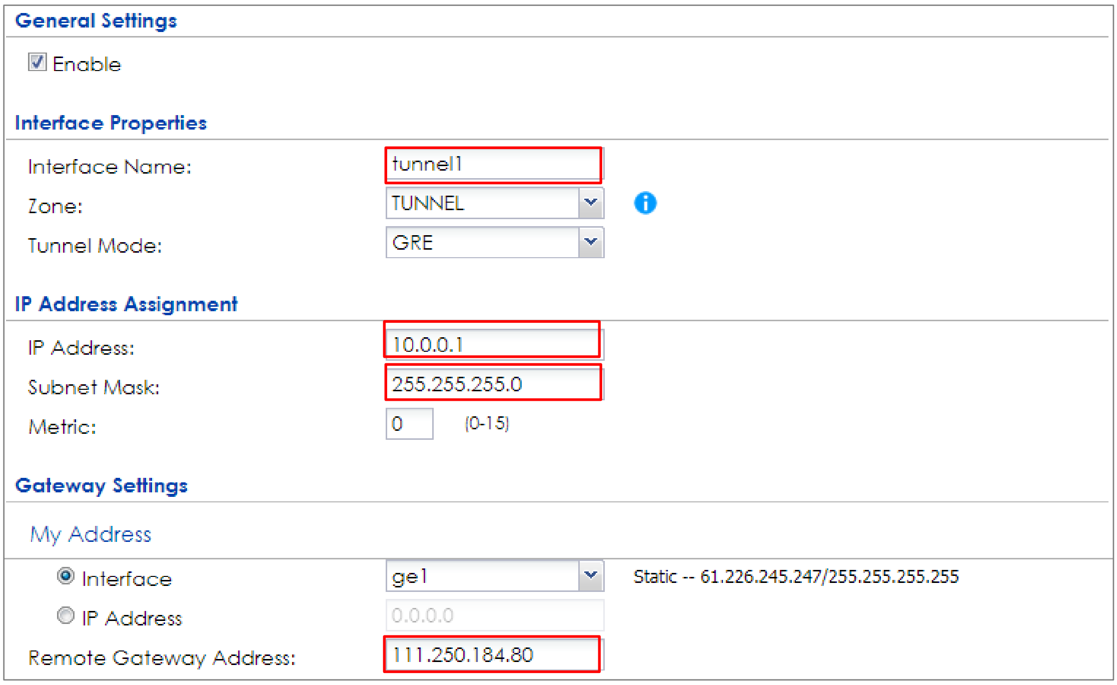
Advance

☑ Enable GRE over IPSec

□ Policy Enforcement

The GRE tunnel runs between the IPsec public interface on the HQ unit and the Branch unit. Go to **CONFIGURATION > Network > Interface > Tunnel > Add**. Enter the **Interface Name** (The format is *tunnelx*, where x is 0 - 3.). Enter the **IP Address** and **Subnet Mask** for this interface. Specify **My Address** to be the interface or IP address to use as the source address for the packets this interface tunnels to the remote gateway. Enter **Remote Gateway Address** to be the IP address or domain name of the remote gateway to this tunnel traffic.

CONFIGURATION > Network > Interface > Tunnel > Add



General Settings

☑ Enable

Interface Properties

Interface Name: tunnel1

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 ge1 Static -- 61.226.245.247/255.255.255.255

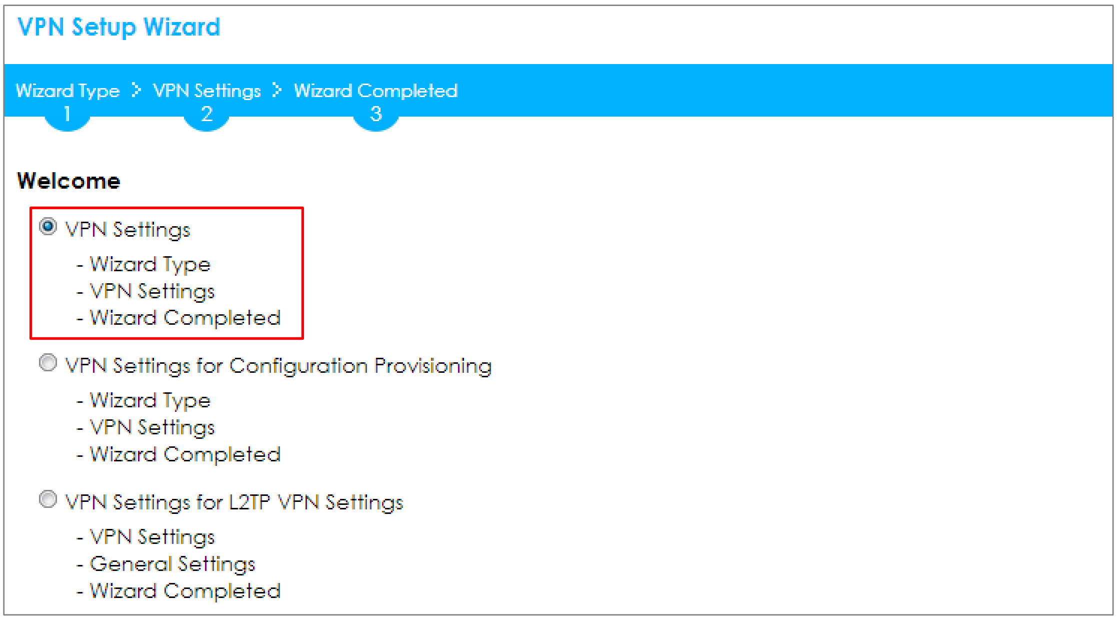
○ IP Address 0.0.0.0

Remote Gateway Address: 111.250.184.80

Set Up the ZyWALL/USG GRE over IPSec VPN Tunnel of Corporate Network (Branch)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Welcome

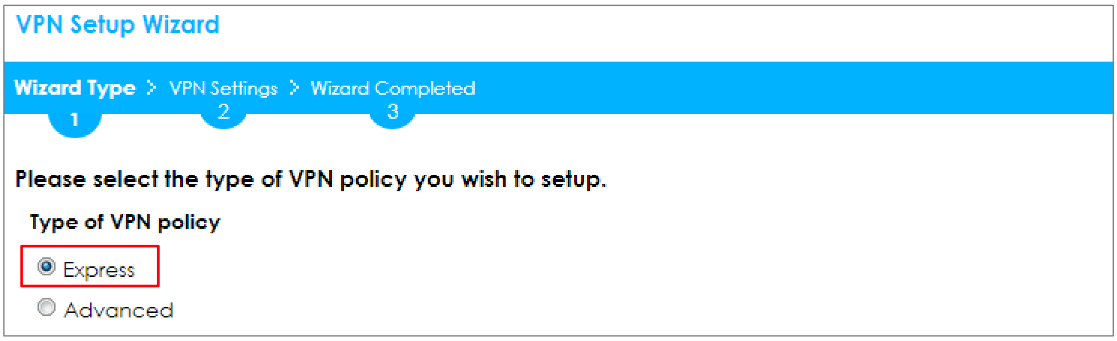
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

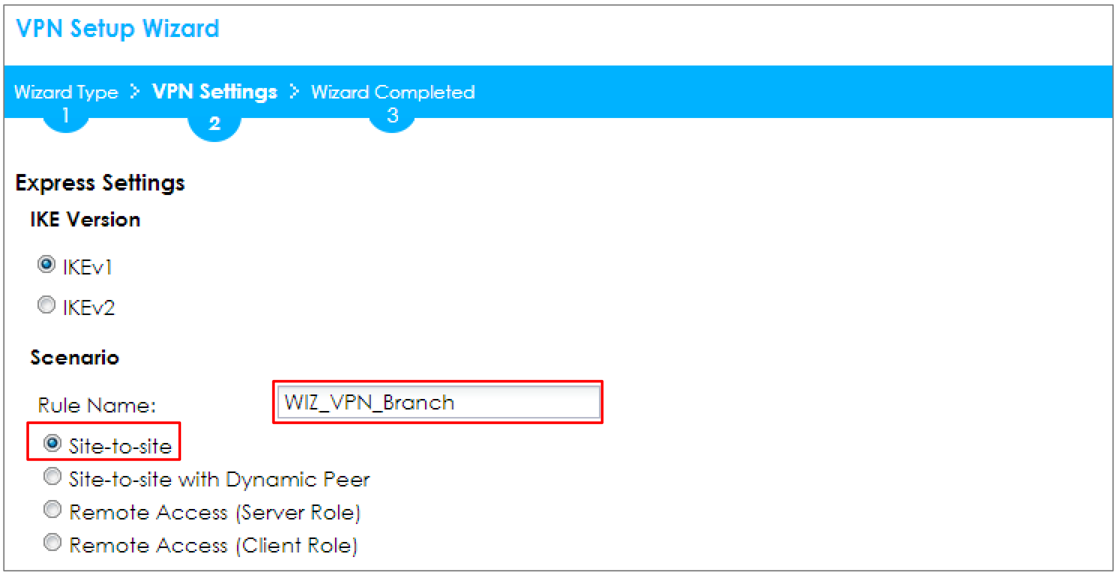
Please select the type of VPN policy you wish to setup.

Type of VPN policy

● Express
○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



Express Settings

IKE Version

● IKEv1
○ IKEv2

Scenario

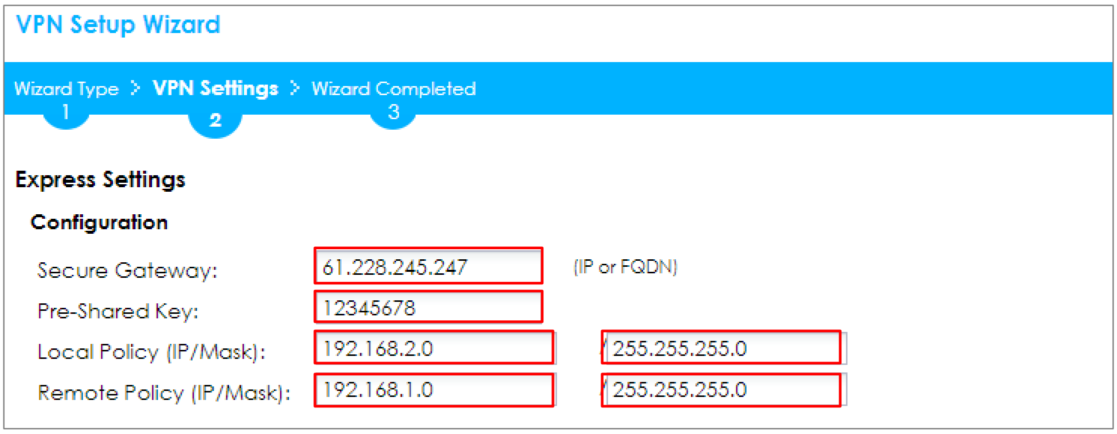
Rule Name: WIZ_VPN_Branch

● Site-to-site
○ Site-to-site with Dynamic Peer
○ Remote Access (Server Role)
○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the HQ's WAN IP address (in the example, 61.228.245.247). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG (Branch) and **Remote Policy** to be the IP address range of the network connected to the ZyWALL/USG (HQ).

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



Express Settings

Configuration

Secure Gateway: 61.228.245.247 (IP or FQDN)

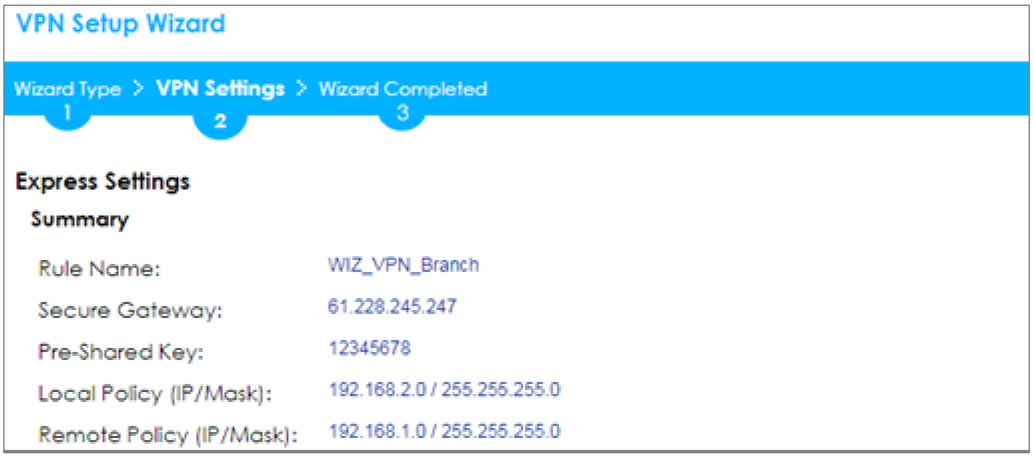
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.2.0 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



VPN Setup Wizard

Express Settings

Summary

Rule Name: WIZ_VPN_Branch

Secure Gateway: 61.228.245.247

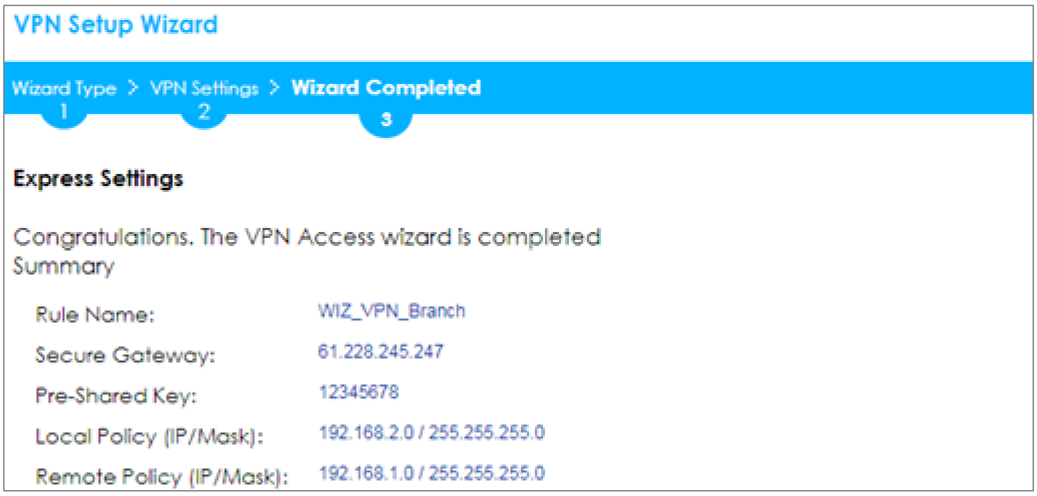
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.2.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



VPN Setup Wizard

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name: WIZ_VPN_Branch

Secure Gateway: 61.228.245.247

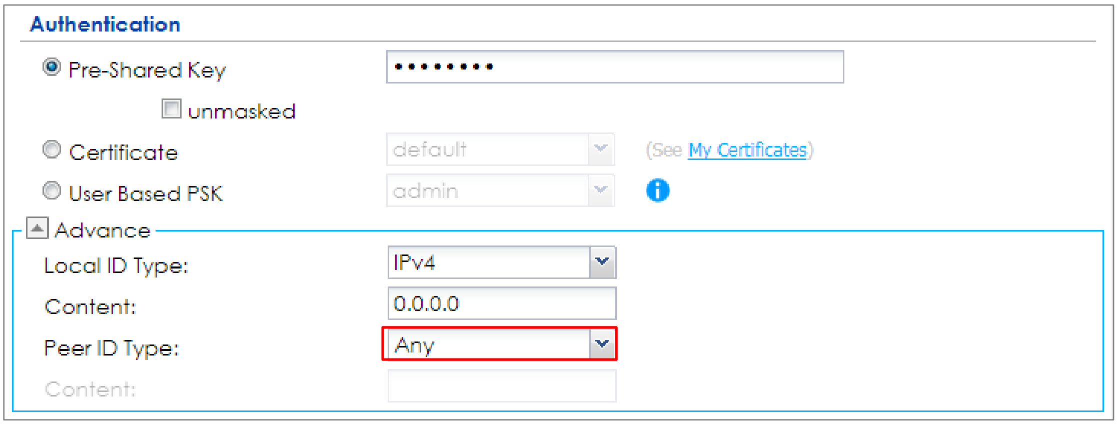
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.2.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

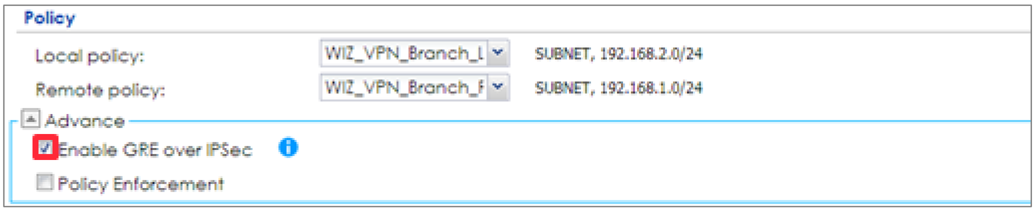
● Pre-Shared Key •••••••••
□ unmasked
○ Certificate default (See My Certificates)
○ User Based PSK admin

Advance

Local ID Type: IPv4
Content: 0.0.0.0
Peer ID Type: Any
Content:

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** > **Show Advanced Settings > Policy**. Select **Enable GRE over IPSec**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Show Advanced Settings > Policy



Policy

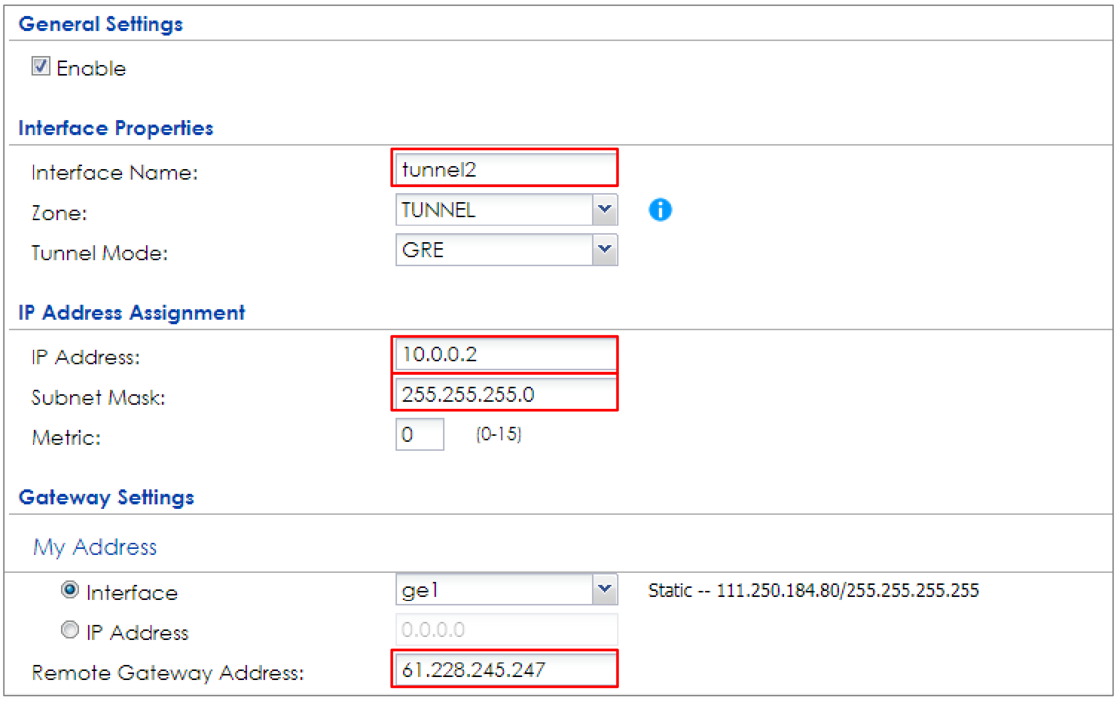
Local policy: WIZ_VPN_Branch_L SUBNET, 192.168.2.0/24
Remote policy: WIZ_VPN_Branch_F SUBNET, 192.168.1.0/24

Advance

☑ Enable GRE over IPSec
□ Policy Enforcement

The GRE tunnel runs between the IPsec public interface on the Branch unit and the HQ unit. Go to **CONFIGURATION > Network > Interface > Tunnel > Add**. Enter the **Interface Name** (The format is *tunnelx*, where x is 0 - 3.). Enter the **IP Address** and **Subnet Mask** for this interface. Specify **My Address** to be the interface or IP address to use as the source address for the packets this interface tunnels to the remote gateway. Enter **Remote Gateway Address** to be the IP address or domain name of the remote gateway to this tunnel traffic.

CONFIGURATION > Network > Interface > Tunnel > Add



General Settings

☑ Enable

Interface Properties

Interface Name:	tunnel2
Zone:	TUNNEL
Tunnel Mode:	GRE

IP Address Assignment

IP Address:	10.0.0.2	
Subnet Mask:	255.255.255.0	
Metric:	0	(0-15)

Gateway Settings

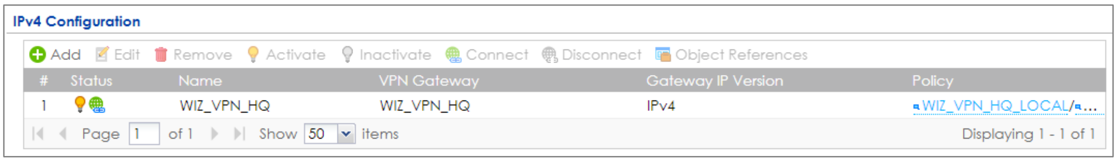
My Address

● Interface	ge1	Static -- 111.250.184.80/255.255.255.255
○ IP Address	0.0.0.0	
Remote Gateway Address:	61.228.245.247	

Test the GRE over IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



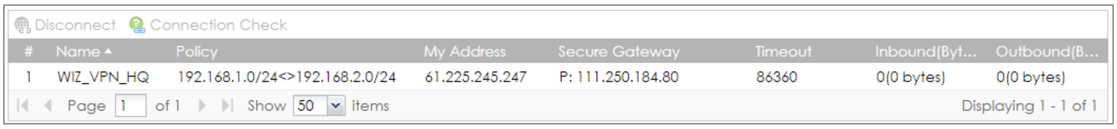
IPv4 Configuration

#	Status	Name	VPN Gateway	Gateway IP Version	Policy
1		WIZ_VPN_HQ	WIZ_VPN_HQ	IPv4	WIZ_VPN_HQ_LOCAL/...

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

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound (Bytes)/Outbound (Bytes)** Traffic.

MONITOR > VPN Monitor > IPSec

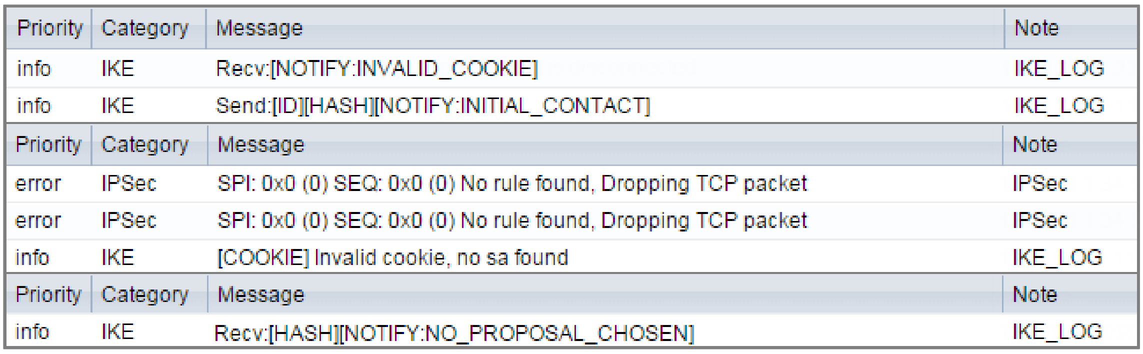


#	Name ▲	Policy	My Address	Secure Gateway	Timeout	Inbound(Byt...	Outbound(B...
1	WIZ_VPN_HQ	192.168.1.0/24<>192.168.2.0/24	61.225.245.247	P: 111.250.184.80	86360	0(0 bytes)	0(0 bytes)

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Make sure your ZyWALL/USG Phase 1 Settings are supported in the Amazon VPC IKE Phase 1 setup list.

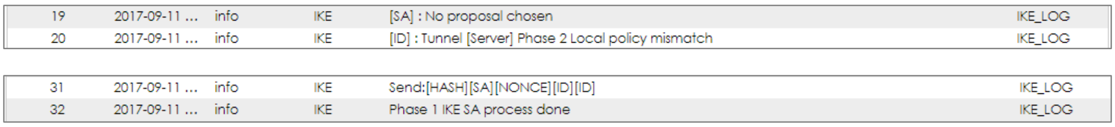
MONITOR > Log



Priority	Category	Message	Note
info	IKE	Recv:[NOTIFY:INVALID_COOKIE]	IKE_LOG
info	IKE	Send:[ID][HASH][NOTIFY:INITIAL_CONTACT]	IKE_LOG
Priority	Category	Message	Note
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
info	IKE	[COOKIE] Invalid cookie, no sa found	IKE_LOG
Priority	Category	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Make sure your ZyWALL/USG Phase 2 Settings are supported in the Amazon VPC IKE Phase 2 setup list.

MONITOR > Log

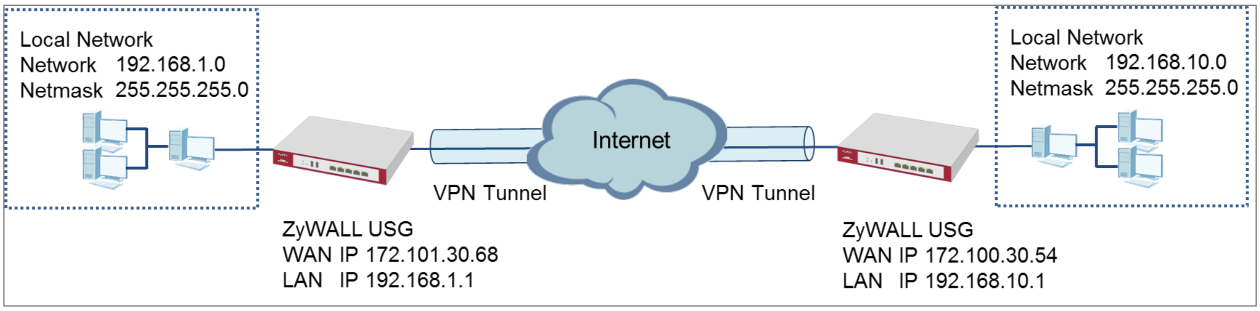


19	2017-09-11 ...	info	IKE	[SA] : No proposal chosen	IKE_LOG
20	2017-09-11 ...	info	IKE	[ID] : Tunnel [Server] Phase 2 Local policy mismatch	IKE_LOG

31	2017-09-11 ...	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

How to Configure Site-to-site IPSec VPN Where the Peer has a Static IP Address

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Static IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.

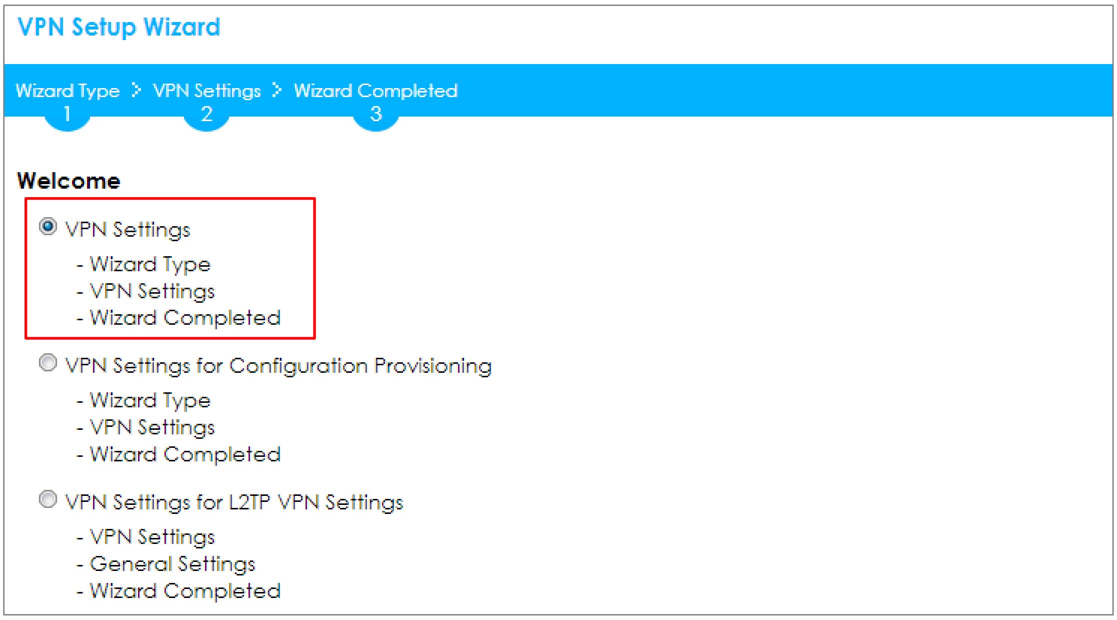


ZyWALL Site-to-site IPSec VPN with a Static IP Address Peer

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (HQ)In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

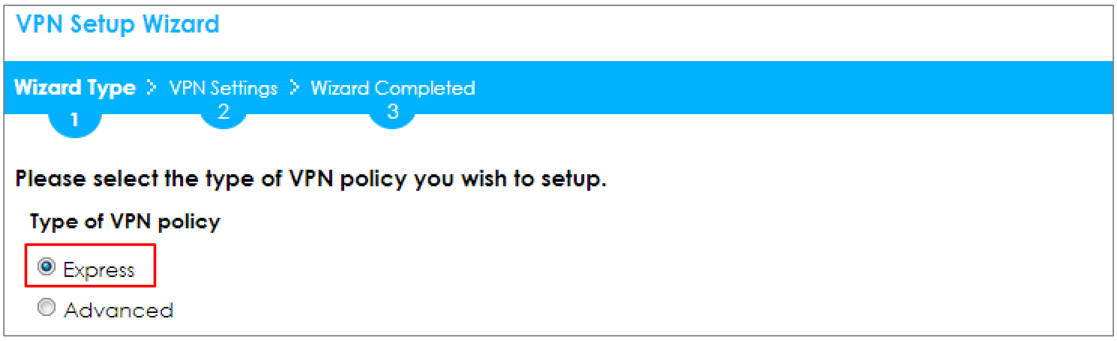
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Please select the type of VPN policy you wish to setup.

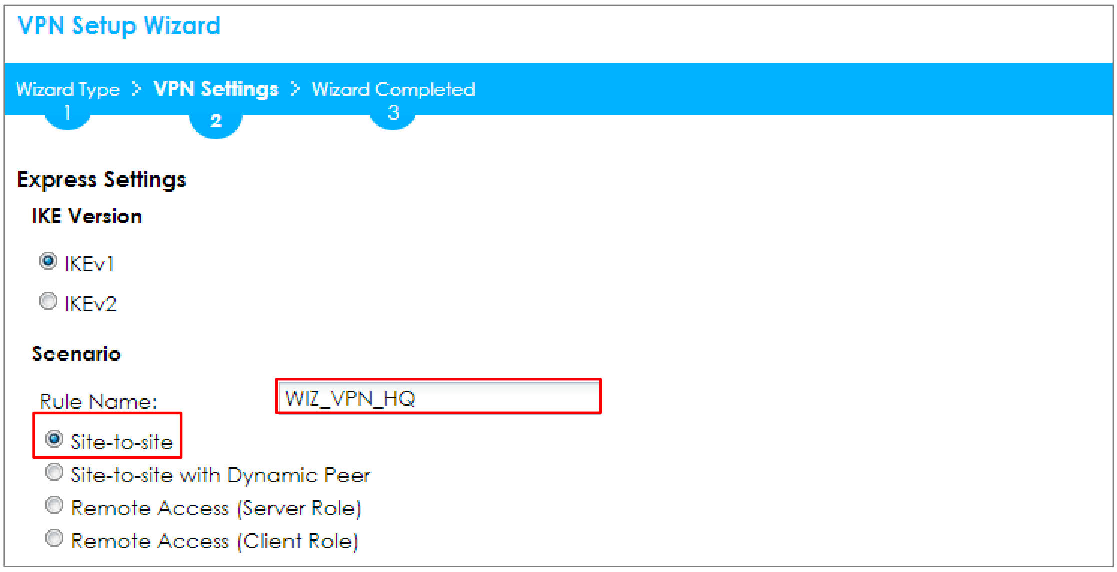
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: WIZ_VPN_HQ

● Site-to-site

○ Site-to-site with Dynamic Peer

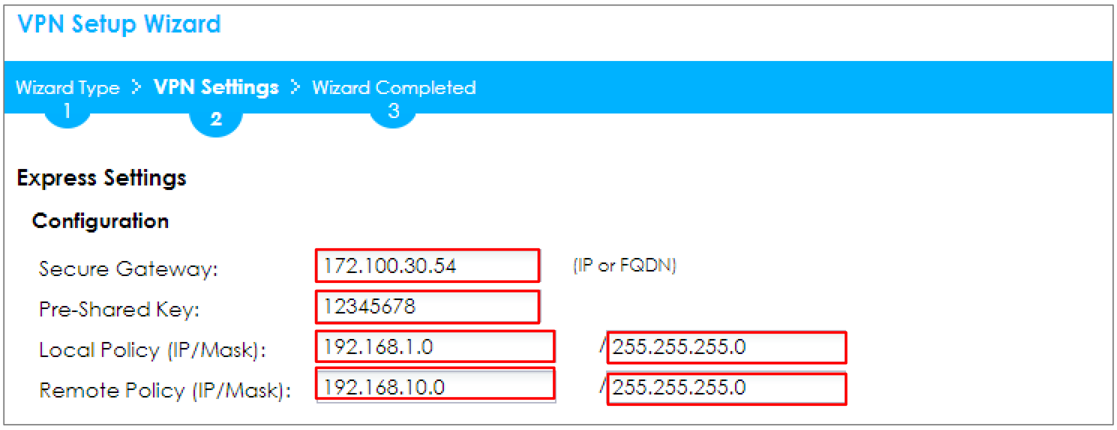
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.100.30.54). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZyWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



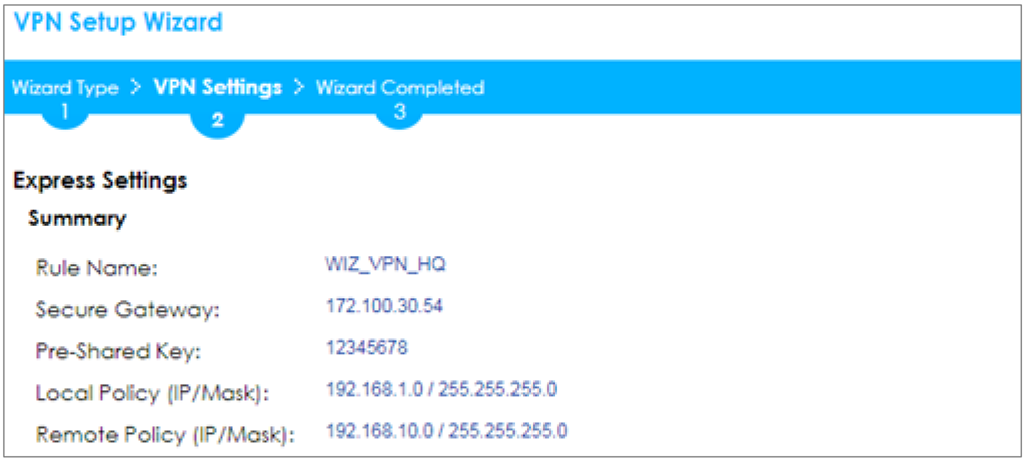
Express Settings

Configuration

Secure Gateway:	172.100.30.54	(IP or FQDN)
Pre-Shared Key:	12345678	
Local Policy (IP/Mask):	192.168.1.0	/ 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0	/ 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



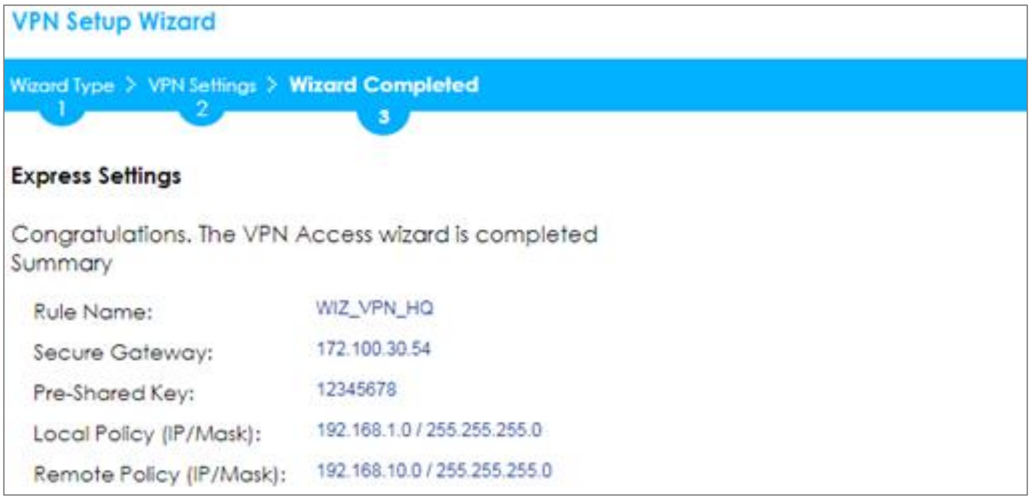
Express Settings

Summary

Rule Name:	WIZ_VPN_HQ
Secure Gateway:	172.100.30.54
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



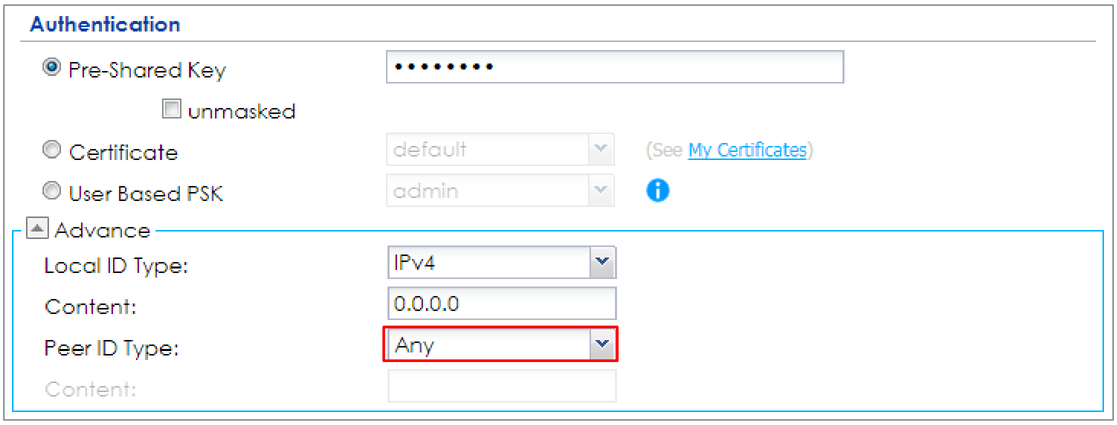
Express Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	WIZ_VPN_HQ
Secure Gateway:	172.100.30.54
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



● Pre-Shared Key: ••••••••

□ unmasked

○ Certificate: default

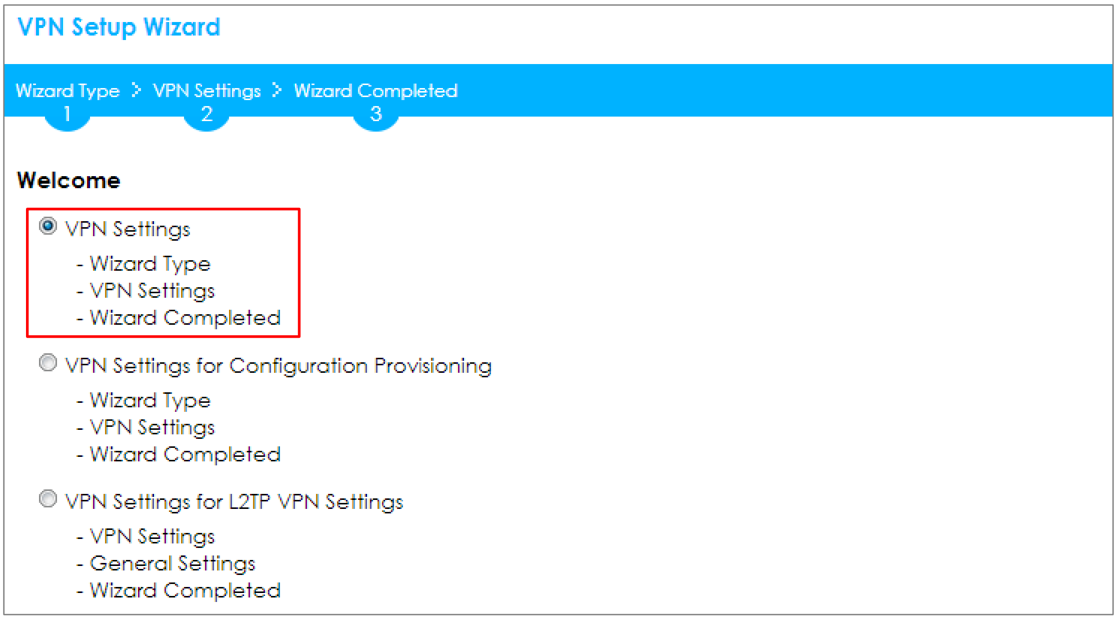
○ User Based PSK: admin

Local ID Type:	IPv4
Content:	0.0.0.0
Peer ID Type:	Any
Content:	

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

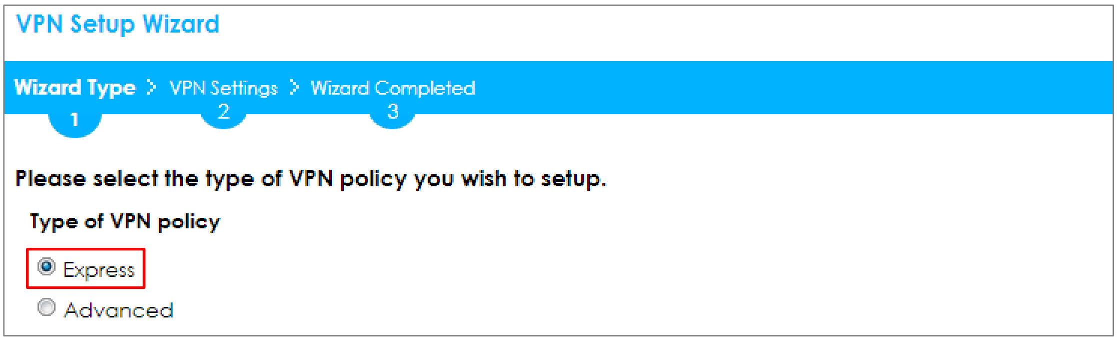
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Please select the type of VPN policy you wish to setup.

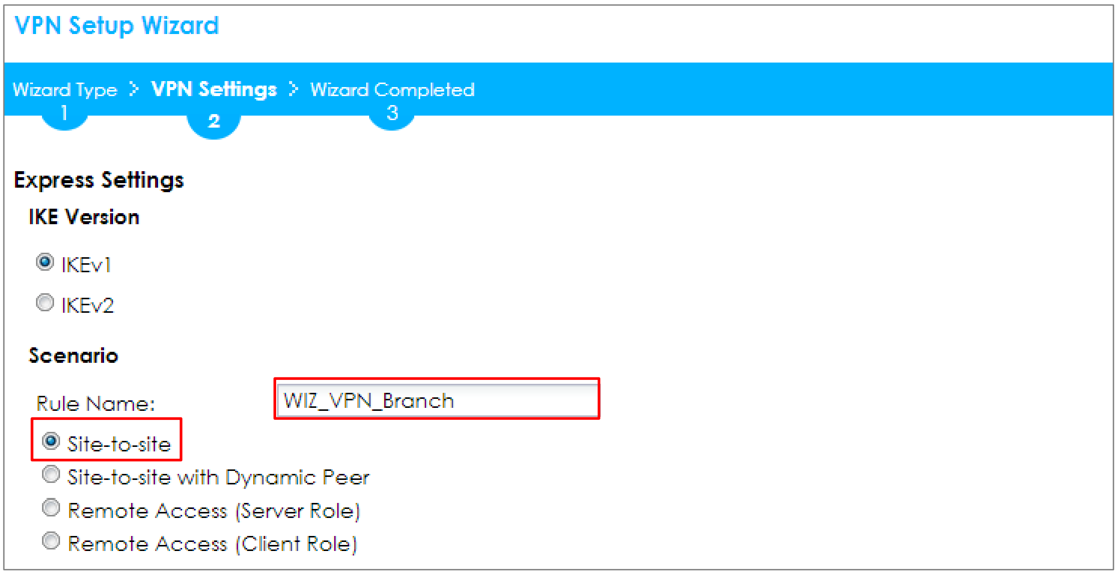
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch

● Site-to-site

○ Site-to-site with Dynamic Peer

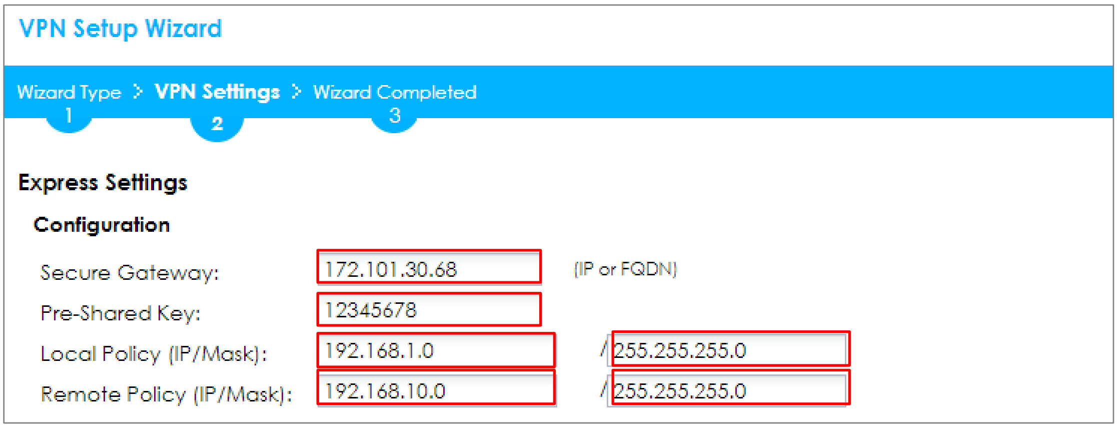
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.101.30.68). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZYWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



Express Settings

Configuration

Secure Gateway: 172.101.30.68 (IP or FQDN)

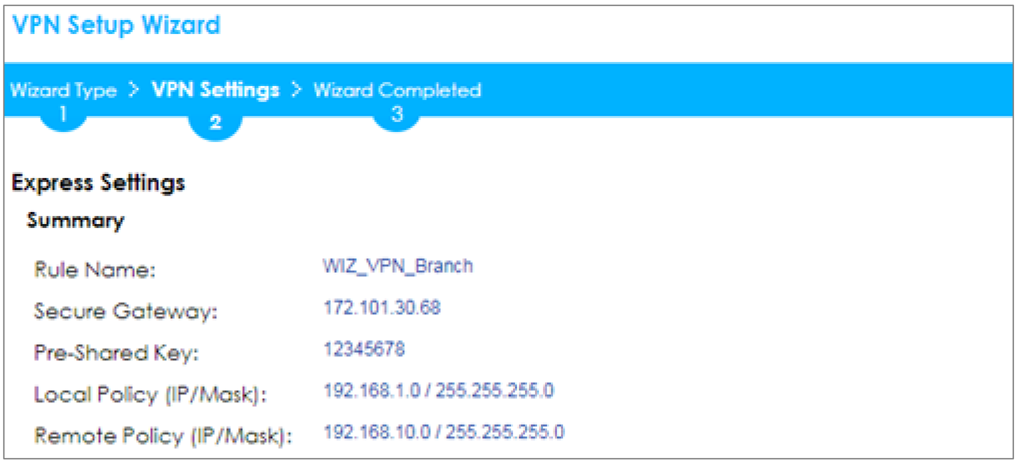
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



Express Settings

Summary

Rule Name: WIZ_VPN_Branch

Secure Gateway: 172.101.30.68

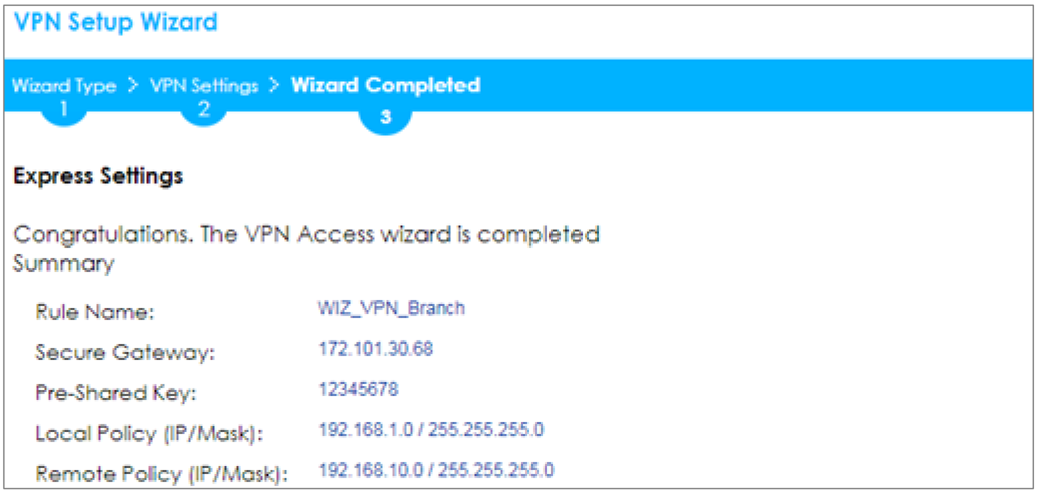
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Express Settings

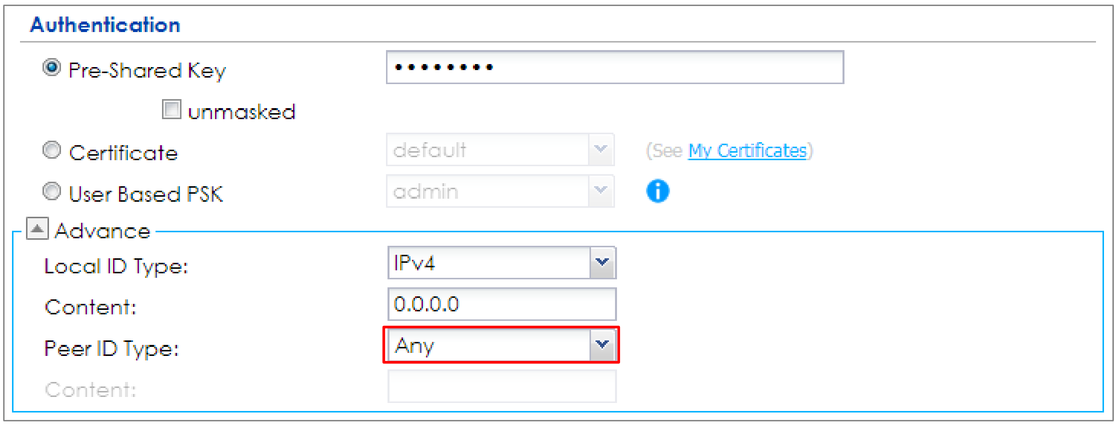
Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_VPN_Branch
Secure Gateway:	172.101.30.68
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. **Configure Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

● Pre-Shared Key: ••••••••

□ unmasked

○ Certificate: default (See My Certificates)

○ User Based PSK: admin

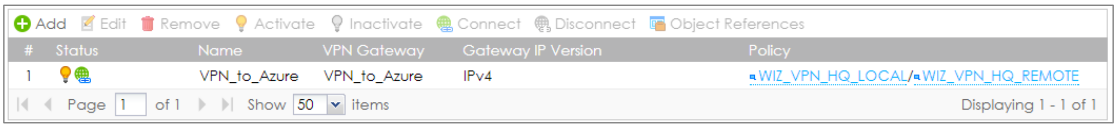
Advance

Local ID Type:	IPv4
Content:	0.0.0.0
Peer ID Type:	Any
Content:	

Test the IPSec VPN Tunnel

Go to ZYWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

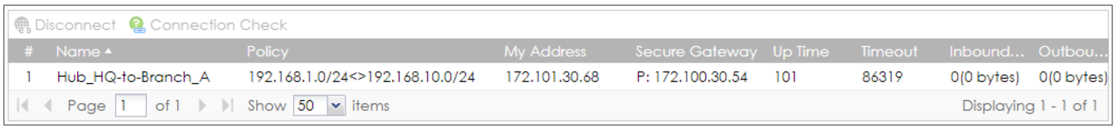
CONFIGURATION > VPN > IPSec VPN > VPN Connection



#	Status	Name	VPN Gateway	Gateway IP Version	Policy
1		VPN_to_Azure	VPN_to_Azure	IPv4	WIZ_VPN_HQ_LOCAL/WIZ_VPN_HQ_REMOTE

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** Traffic.

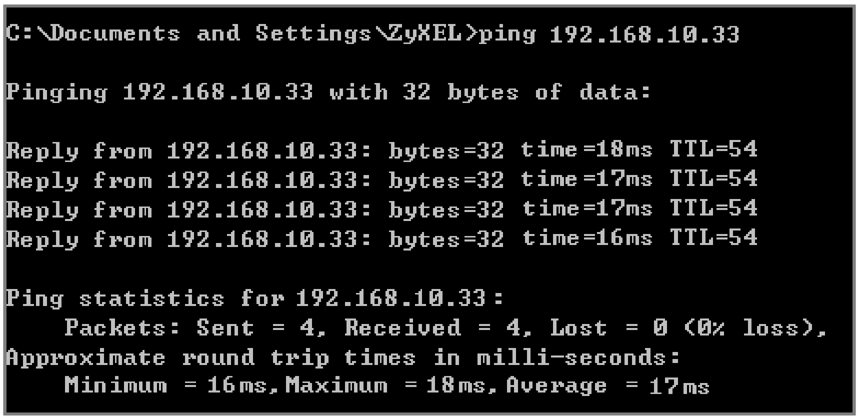
MONITOR > VPN Monitor > IPSec



#	Name ▲	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound...	Outbou...
1	Hub_HQ-to-Branch_A	192.168.1.0/24<>192.168.10.0/24	172.101.30.68	P: 172.100.30.54	101	86319	0(0 bytes)	0(0 bytes)

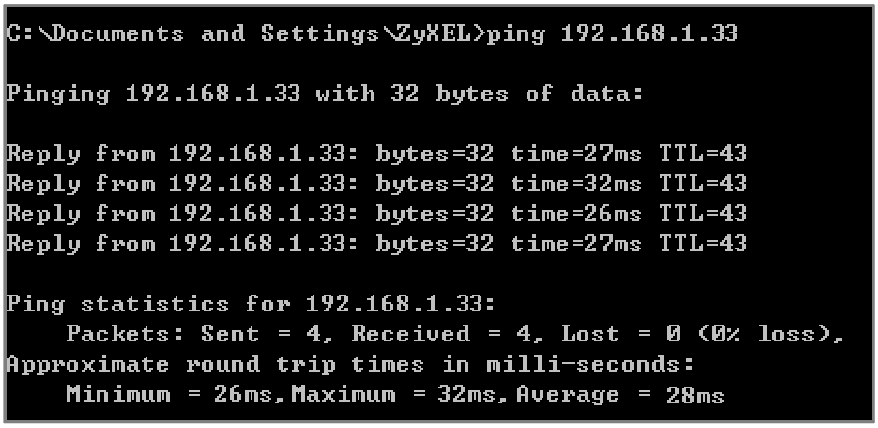
To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC at HQ Office > Window 7 > cmd > ping 192.168.10.33



```
C:\Documents and Settings\ZyXEL>ping 192.168.10.33

Pinging 192.168.10.33 with 32 bytes of data:

Reply from 192.168.10.33: bytes=32 time=18ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.10.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC at Branch Office > Window 7 > cmd > ping 192.168.1.33

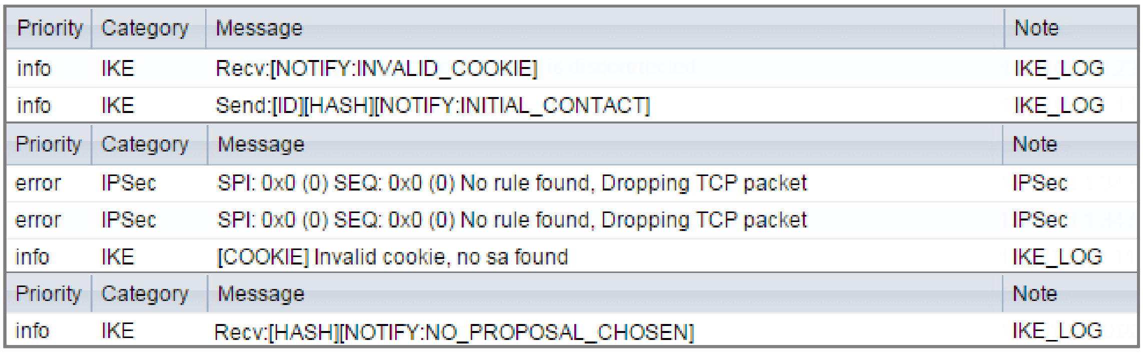


```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

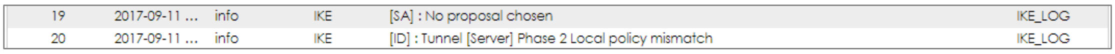
MONITOR > Log



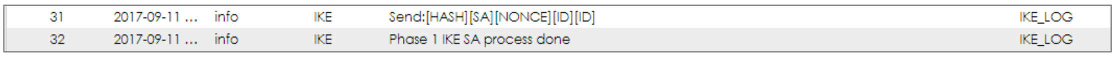
Priority	Category	Message	Note
info	IKE	Recv:[NOTIFY:INVALID_COOKIE]	IKE_LOG
info	IKE	Send:[ID][HASH][NOTIFY:INITIAL_CONTACT]	IKE_LOG
Priority	Category	Message	Note
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
info	IKE	[COOKIE] Invalid cookie, no sa found	IKE_LOG
Priority	Category	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log



```
19    2017-09-11 ...  info    IKE    [SA] : No proposal chosen                                  IKE_LOG
20    2017-09-11 ...  info    IKE    [ID] : Tunnel [Server] Phase 2 Local policy mismatch       IKE_LOG
```



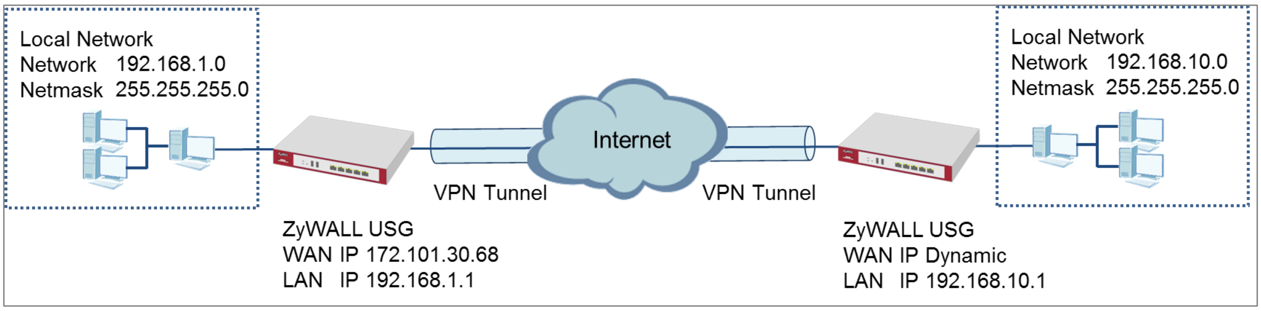
```
31    2017-09-11 ...  info    IKE    Send:[HASH][SA][NONCE][ID][ID]                             IKE_LOG
32    2017-09-11 ...  info    IKE    Phase 1 IKE SA process done                                IKE_LOG
```

Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure Site-to-site IPSec VPN Where the Peer has a Dynamic IP Address

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Dynamic IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



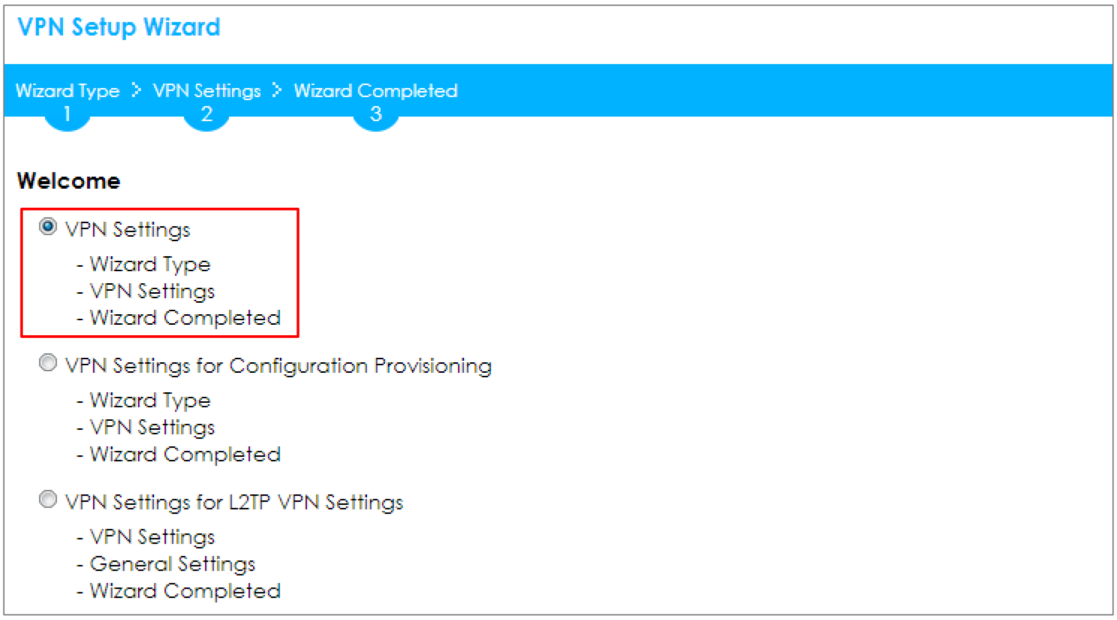
ZyWALL Site-to-site IPSec VPN with a Dynamic IP Address Peer

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (HQ)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

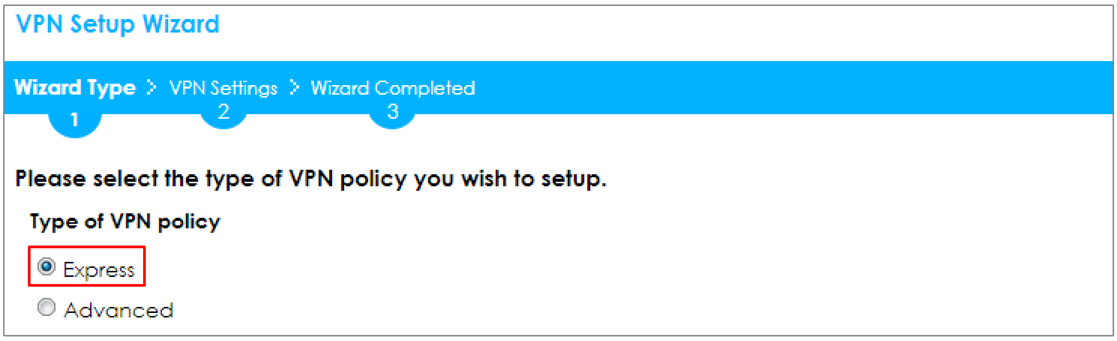
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Please select the type of VPN policy you wish to setup.

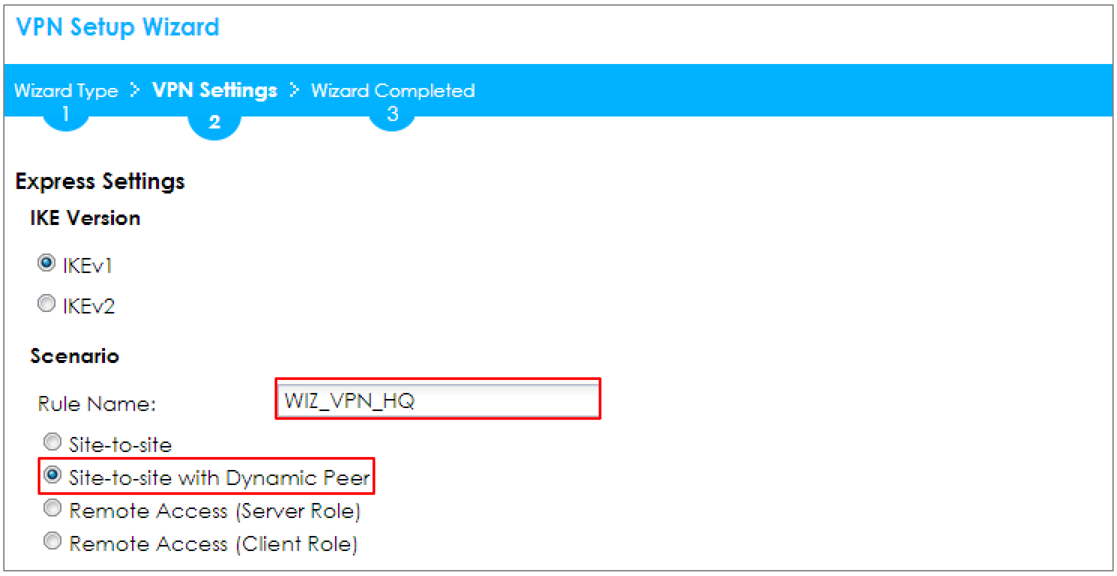
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site with Dynamic Peer**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: WIZ_VPN_HQ

○ Site-to-site

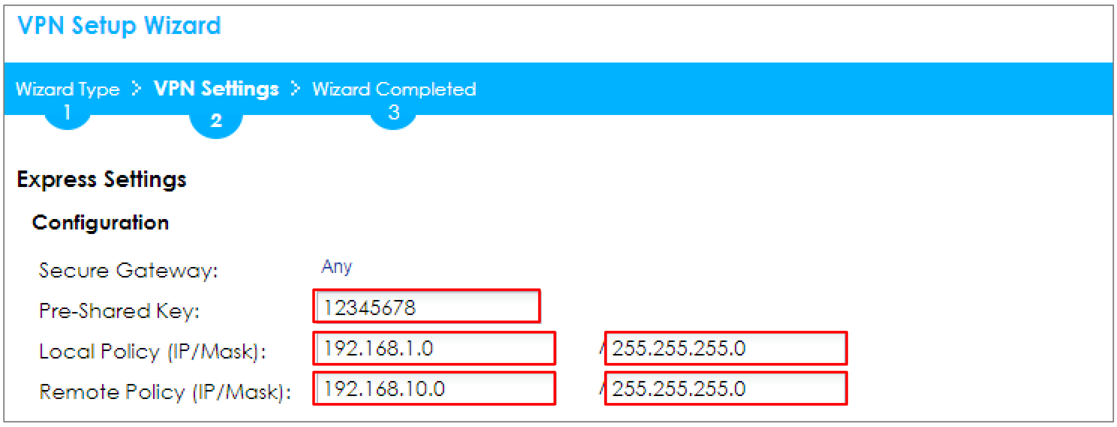
● Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

Type a secure **Pre-Shared Key** (8-32 characters). Then, set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZYWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



VPN Setup Wizard

Express Settings

Configuration

Secure Gateway: Any

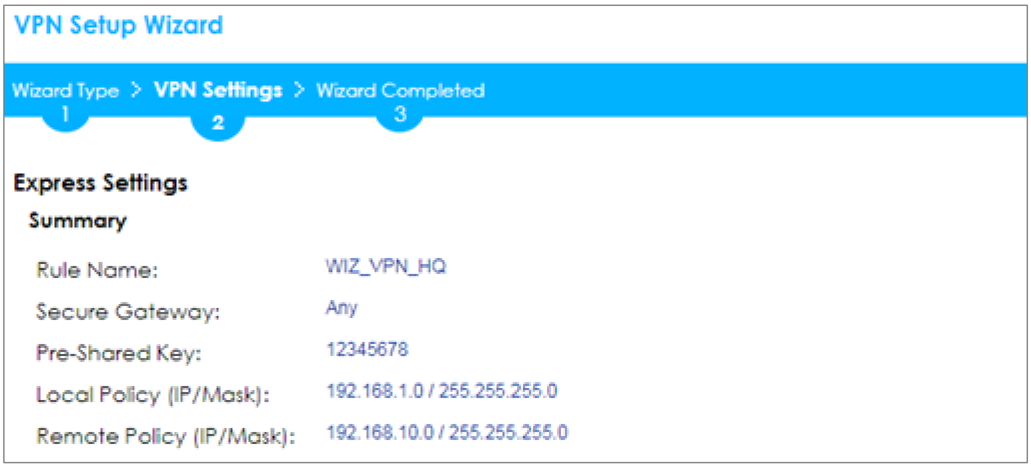
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Summary)



VPN Setup Wizard

Express Settings

Summary

Rule Name: WIZ_VPN_HQ

Secure Gateway: Any

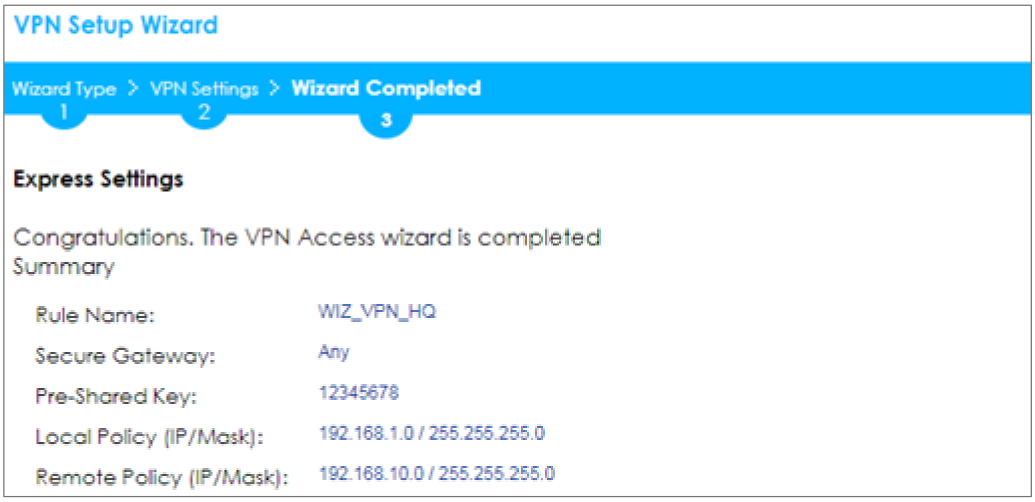
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard completed



VPN Setup Wizard

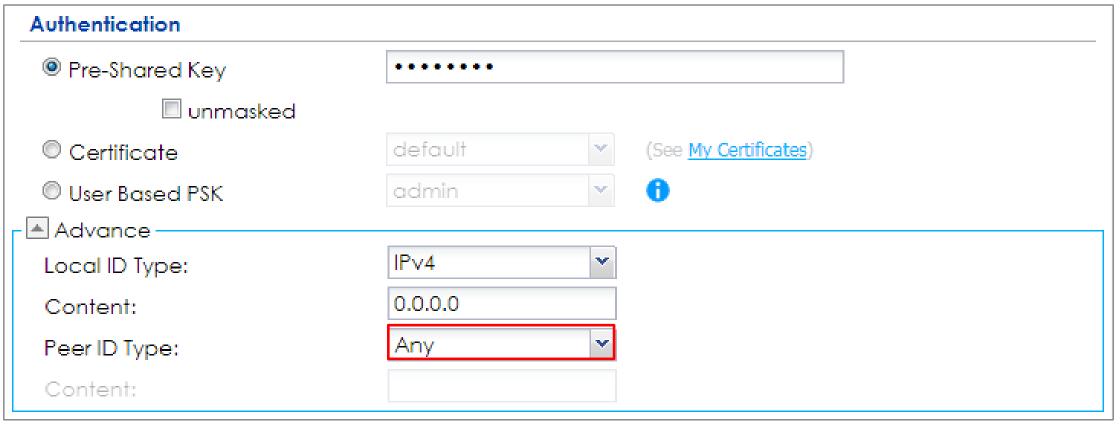
Express Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	WIZ_VPN_HQ
Secure Gateway:	Any
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

● Pre-Shared Key ••••••••

□ unmasked

○ Certificate default (See My Certificates)

○ User Based PSK admin

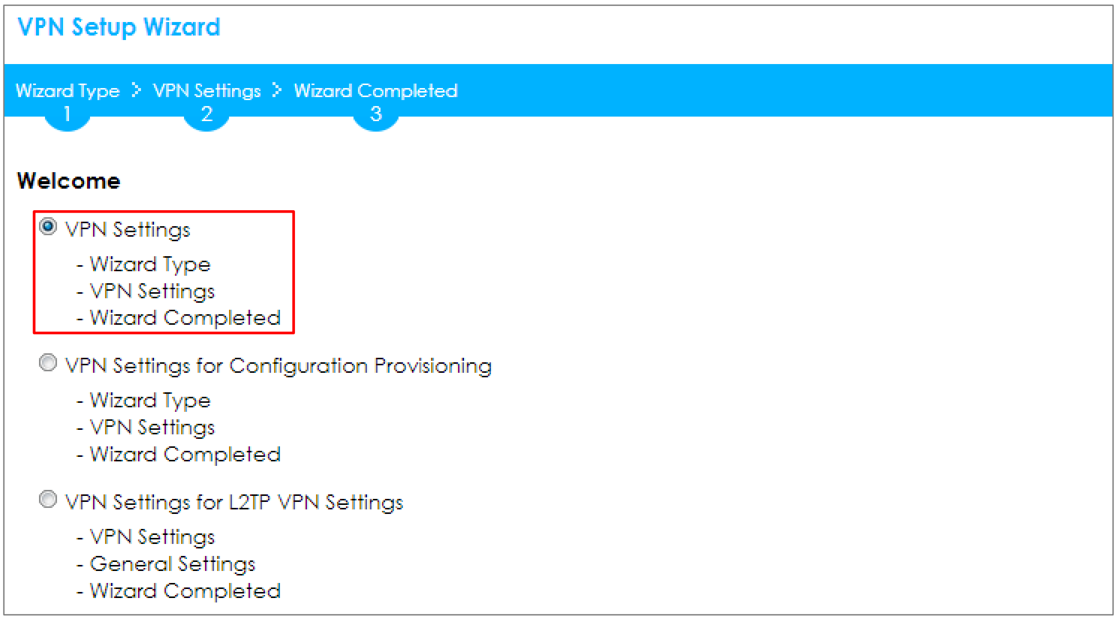
Advance

Local ID Type:	IPv4
Content:	0.0.0.0
Peer ID Type:	Any
Content:	

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch has a Dynamic IP Address)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** to create a **Site-to-site VPN** Rule Name.

Quick Setup > VPN Setup Wizard > WelcomeQuick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Welcome

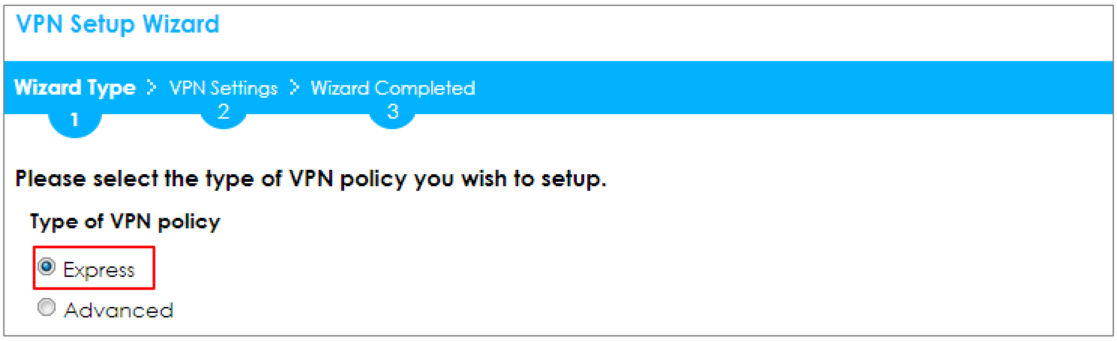
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Please select the type of VPN policy you wish to setup.

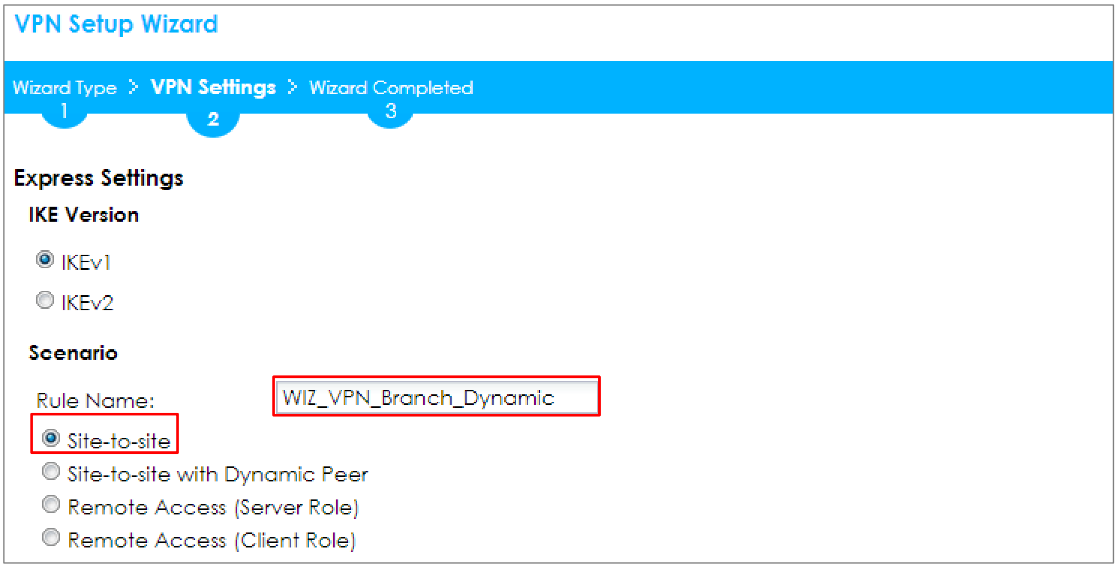
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch_Dynamic

● Site-to-site

○ Site-to-site with Dynamic Peer

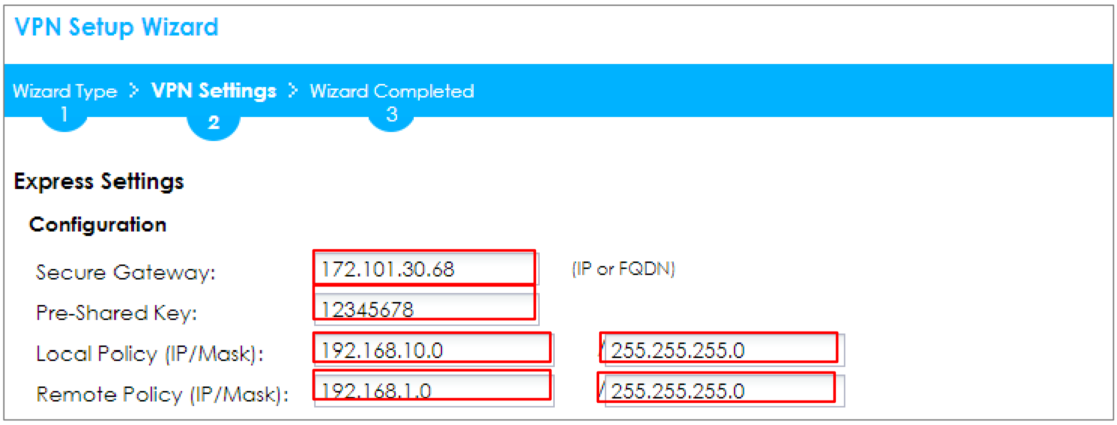
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.101.30.68). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the ZyWALL/USG local IP address that can use the VPN tunnel and set **Remote Policy** to the peer ZyWALL/USG local IP address that can use the VPN tunnel. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



VPN Setup Wizard

Express Settings

Configuration

Secure Gateway: 172.101.30.68 (IP or FQDN)

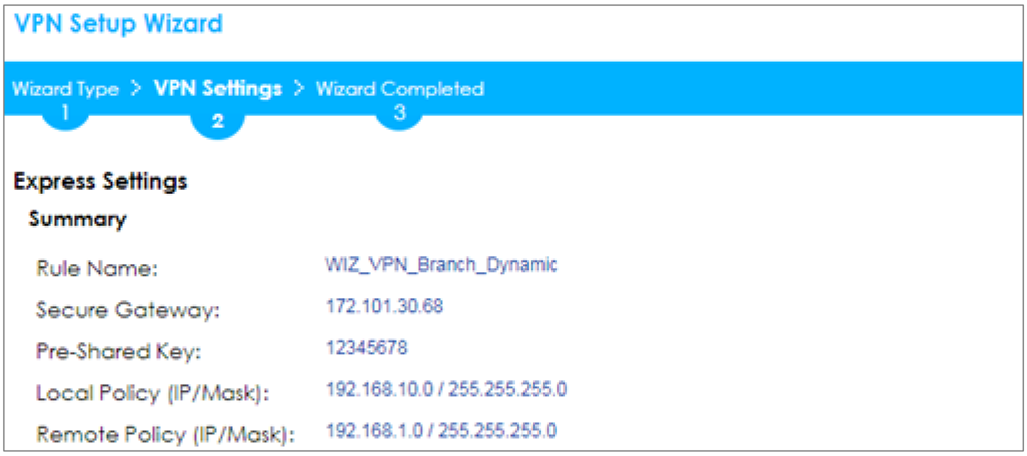
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



VPN Setup Wizard

Express Settings

Summary

Rule Name: WIZ_VPN_Branch_Dynamic

Secure Gateway: 172.101.30.68

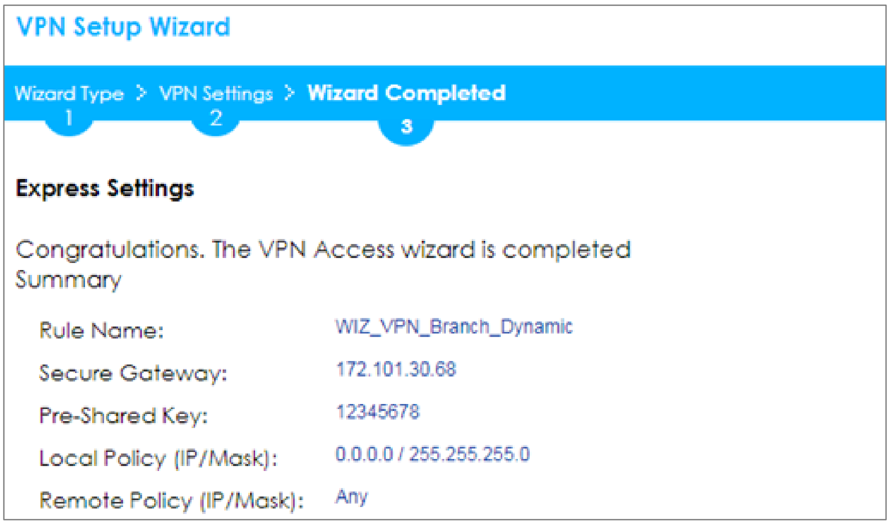
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



VPN Setup Wizard

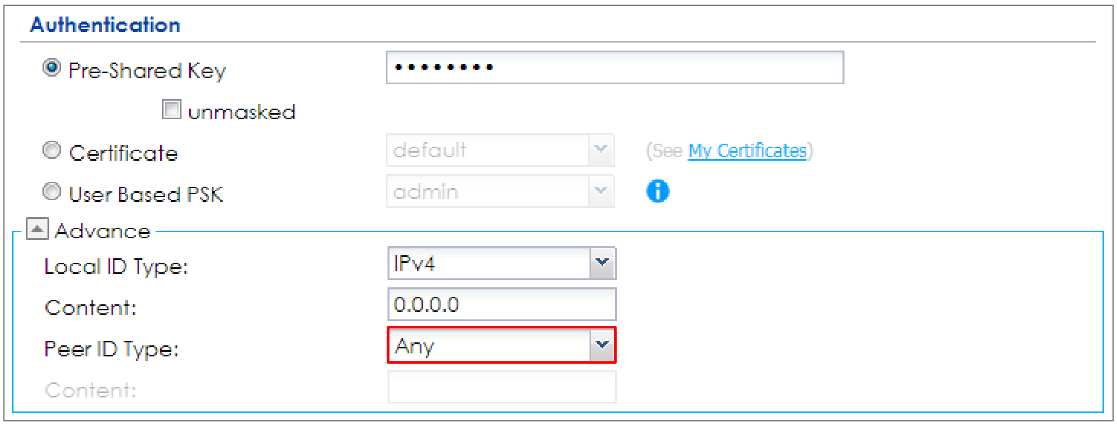
Express Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	WIZ_VPN_Branch_Dynamic
Secure Gateway:	172.101.30.68
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	0.0.0.0 / 255.255.255.0
Remote Policy (IP/Mask):	Any

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. **Configure Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



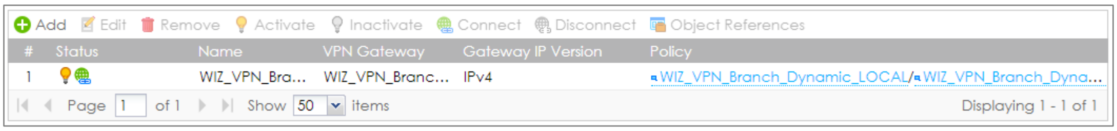
Authentication

● Pre-Shared Key	••••••••
□ unmasked	
○ Certificate	default (See My Certificates)
○ User Based PSK	admin
Advance	
Local ID Type:	IPv4
Content:	0.0.0.0
Peer ID Type:	Any
Content:	

Test the IPSec VPN Tunnel

The Site-to-site VPN with Dynamic Peer can only initiate the VPN tunnel from the peer has a dynamic IP Address. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

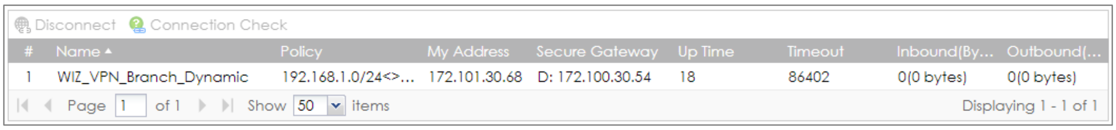
CONFIGURATION > VPN > IPSec VPN > VPN Connection



#	Status	Name	VPN Gateway	Gateway IP Version	Policy
1		WIZ_VPN_Bra...	WIZ_VPN_Branc...	IPv4	WIZ_VPN_Branch_Dynamic_LOCAL/WIZ_VPN_Branch_Dyna...

Go to **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** Traffic.

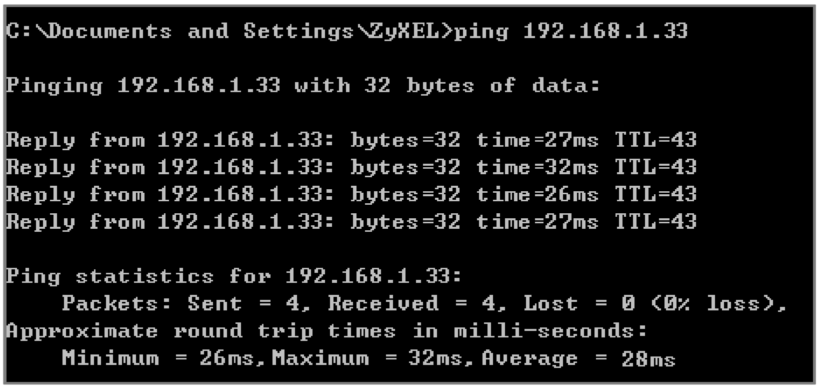
MONITOR > VPN Monitor > IPSec



#	Name	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound(By...	Outbound(...
1	WIZ_VPN_Branch_Dynamic	192.168.1.0/24<>...	172.101.30.68	D: 172.100.30.54	18	86402	0(0 bytes)	0(0 bytes)

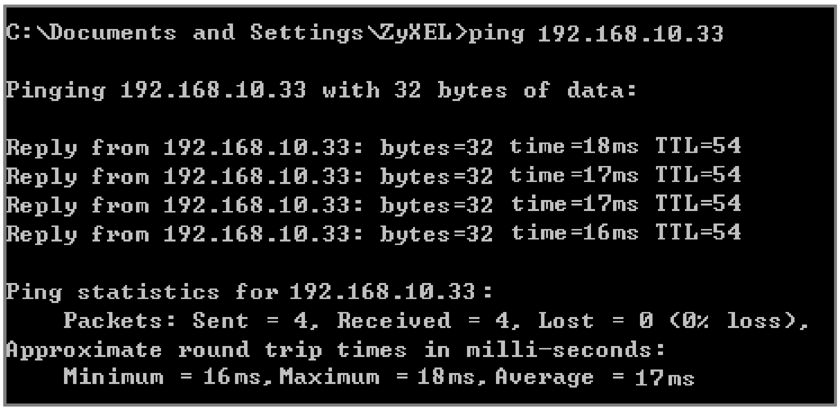
To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC at HQ Office > Window 7 > cmd > ping 192.168.10.33



```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

PC at Branch Office > Window 7 > cmd > ping 192.168.1.33

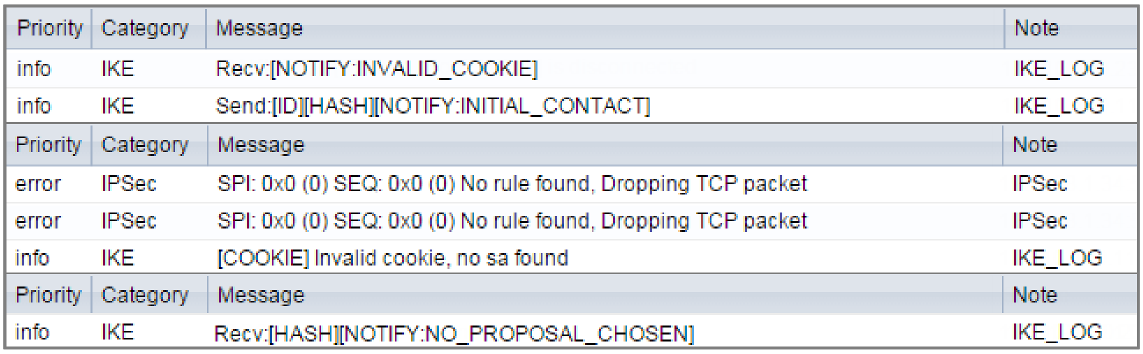


```
C:\Documents and Settings\ZyXEL>ping 192.168.10.33

Pinging 192.168.10.33 with 32 bytes of data:

Reply from 192.168.10.33: bytes=32 time=18ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.10.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

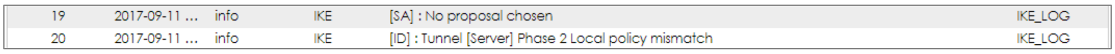
MONITOR > Log



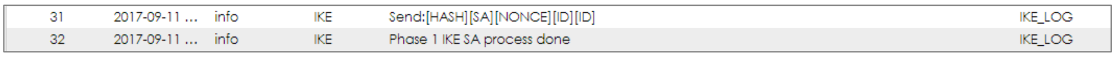
Priority	Category	Message	Note
info	IKE	Recv:[NOTIFY:INVALID_COOKIE]	IKE_LOG
info	IKE	Send:[ID][HASH][NOTIFY:INITIAL_CONTACT]	IKE_LOG
Priority	Category	Message	Note
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
info	IKE	[COOKIE] Invalid cookie, no sa found	IKE_LOG
Priority	Category	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log



```
19   2017-09-11 ...   info   IKE   [SA] : No proposal chosen                              IKE_LOG
20   2017-09-11 ...   info   IKE   [ID] : Tunnel [Server] Phase 2 Local policy mismatch   IKE_LOG
```



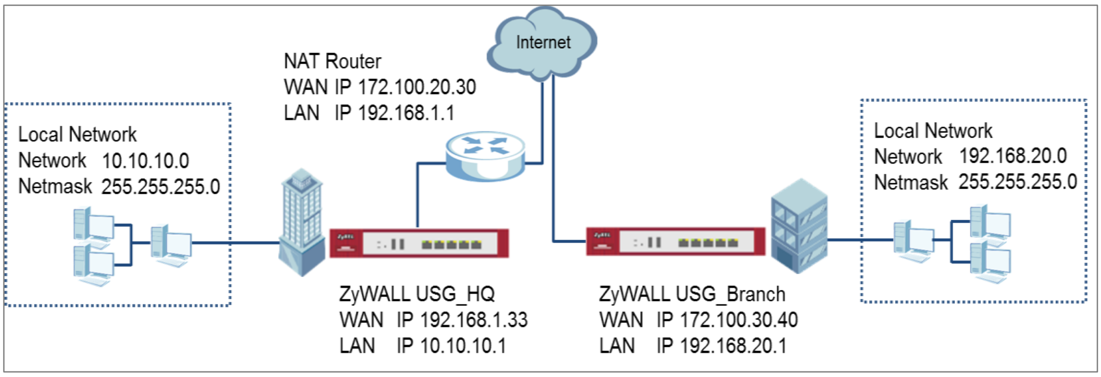
```
31   2017-09-11 ...   info   IKE   Send:[HASH][SA][NONCE][ID][ID]     IKE_LOG
32   2017-09-11 ...   info   IKE   Phase 1 IKE SA process done        IKE_LOG
```

Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure IPSec Site to Site VPN while one Site is behind a NAT router

This example shows how to use the VPN Setup Wizard to create a IPSec Site to Site VPN tunnel between ZyWALL/USG devices. The example instructs how to configure the VPN tunnel between each site while one Site is behind a NAT router. When the IPSec Site to Site VPN tunnel is configured, each site can be accessed securely.



ZyWALL/USG Site to Site VPN while one Site is behind a NAT router

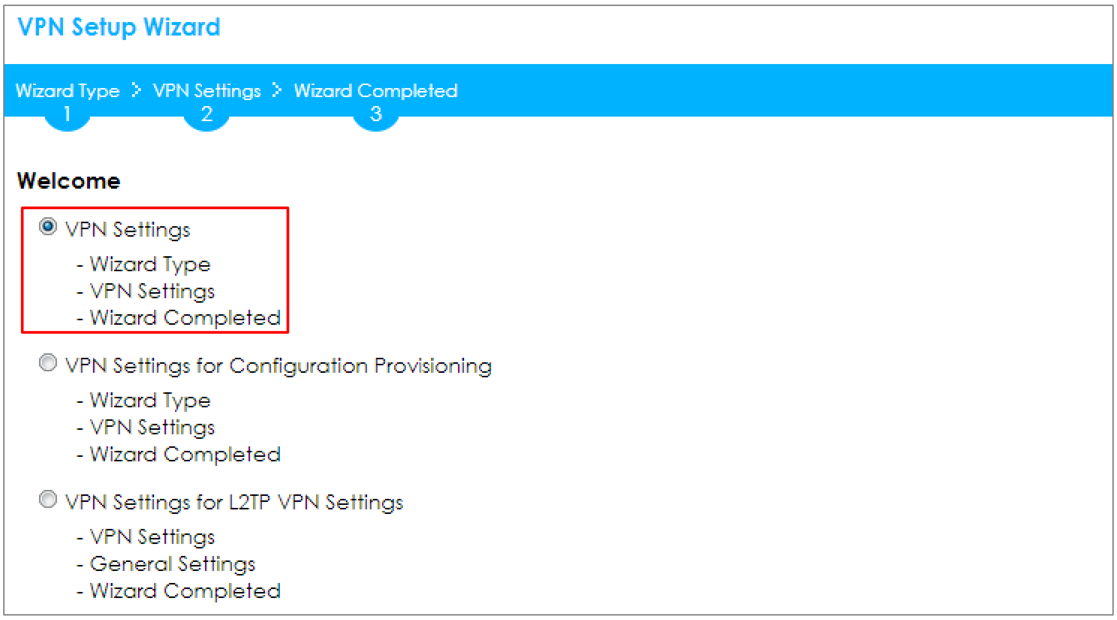
Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25) and ZyWALL 310 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (HQ)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Welcome

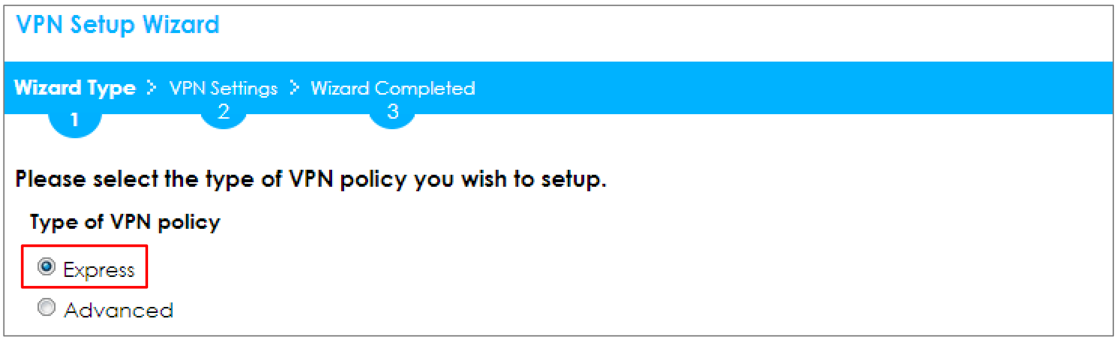
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Please select the type of VPN policy you wish to setup.

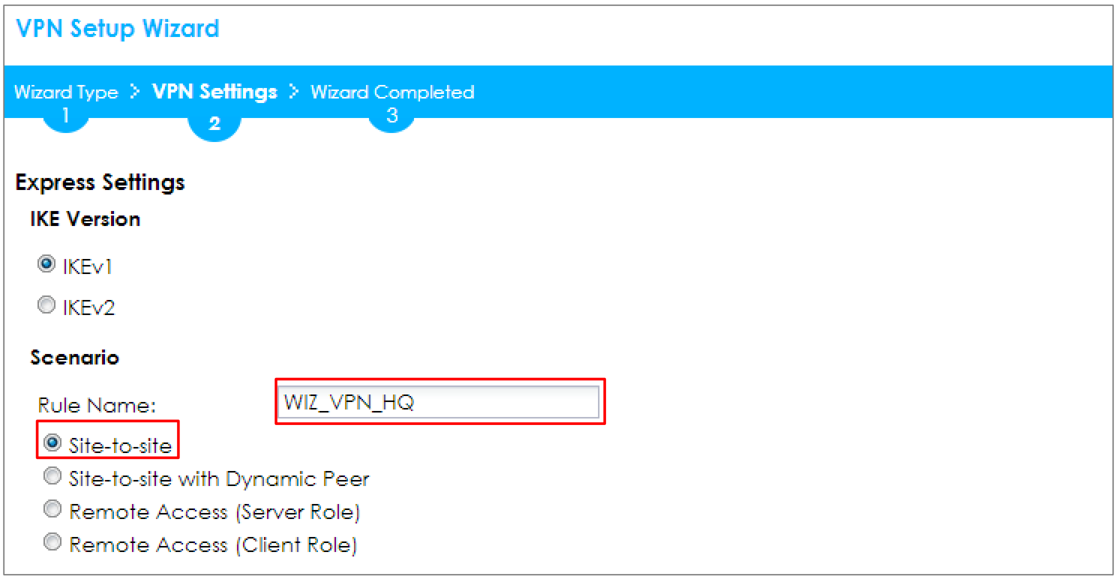
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: WIZ_VPN_HQ

● Site-to-site

○ Site-to-site with Dynamic Peer

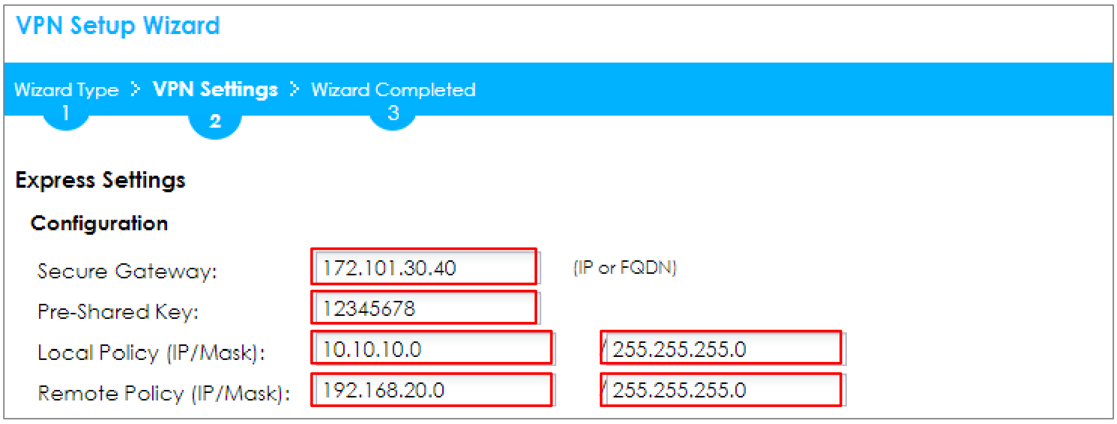
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the Branch's WAN IP address (in the example, 172.100.30.40). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG (HQ) and **Remote Policy** to be the IP address range of the network connected to the ZyWALL/USG (Branch).

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



Express Settings

Configuration

Secure Gateway: 172.101.30.40 (IP or FQDN)

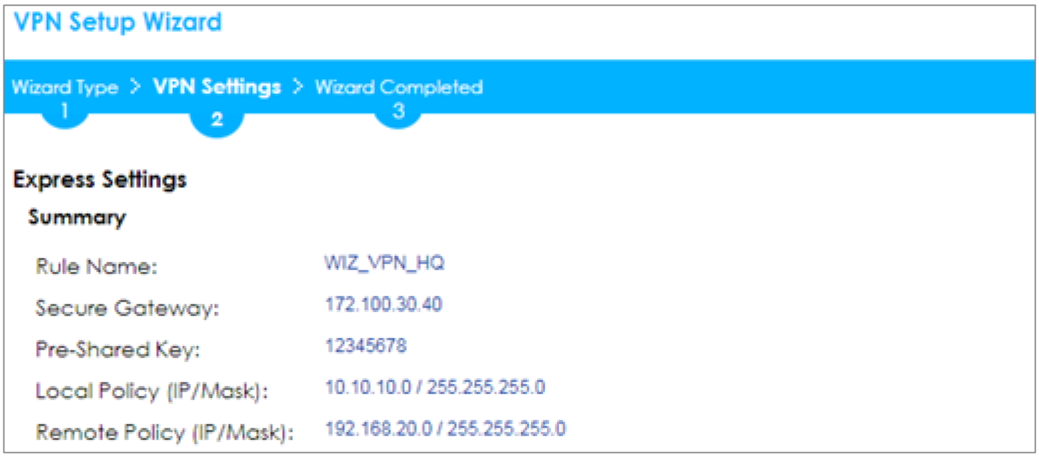
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 10.10.10.0 255.255.255.0

Remote Policy (IP/Mask): 192.168.20.0 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



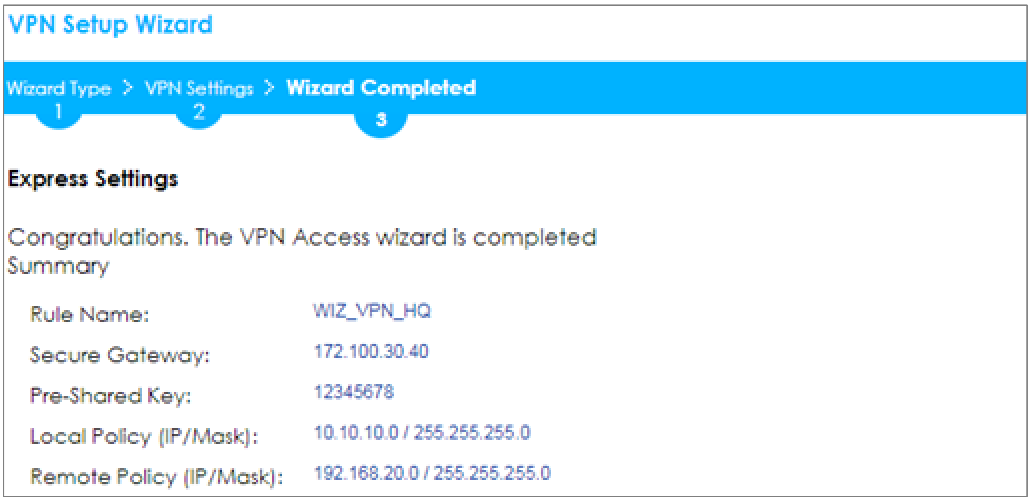
Express Settings

Summary

Rule Name:	WIZ_VPN_HQ
Secure Gateway:	172.100.30.40
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	10.10.10.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.20.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



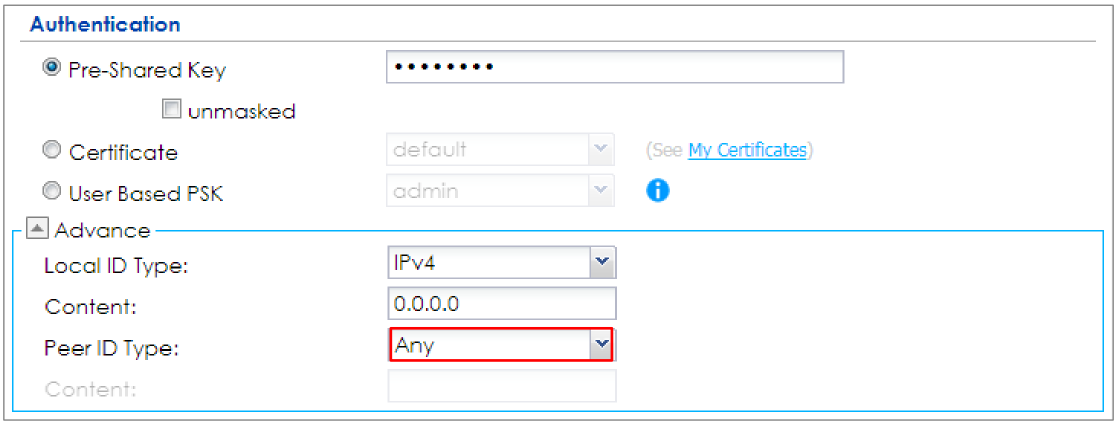
Express Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	WIZ_VPN_HQ
Secure Gateway:	172.100.30.40
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	10.10.10.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.20.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

● Pre-Shared Key •••••••••

□ unmasked

○ Certificate default (See My Certificates)

○ User Based PSK admin

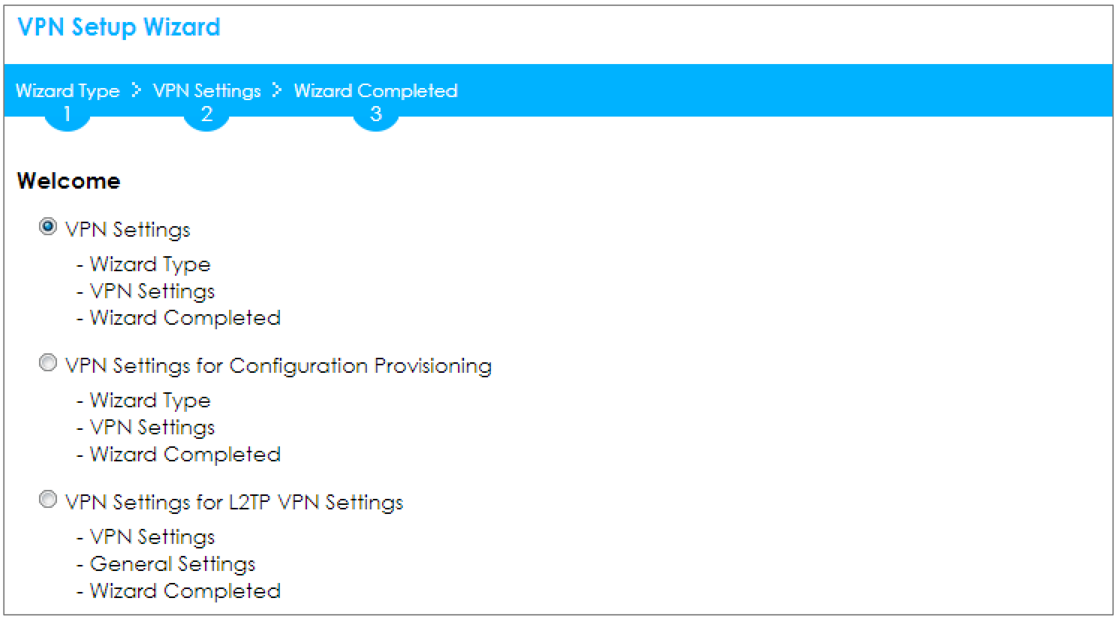
Advance

Local ID Type:	IPv4
Content:	0.0.0.0
Peer ID Type:	Any
Content:	

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

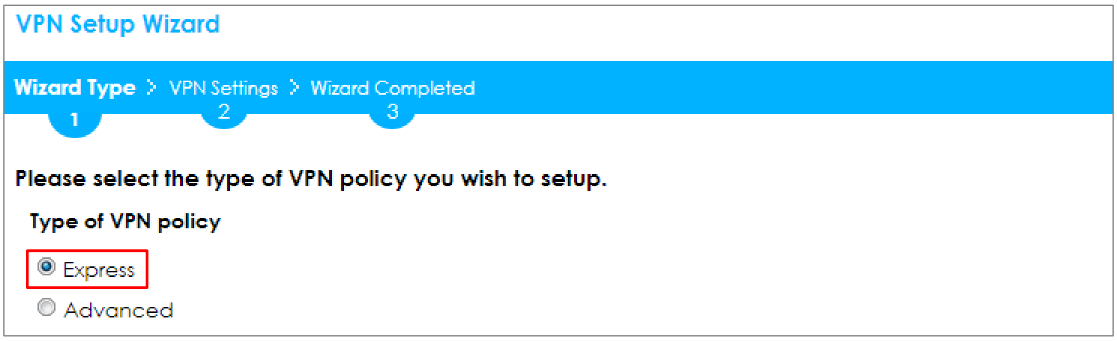
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Please select the type of VPN policy you wish to setup.

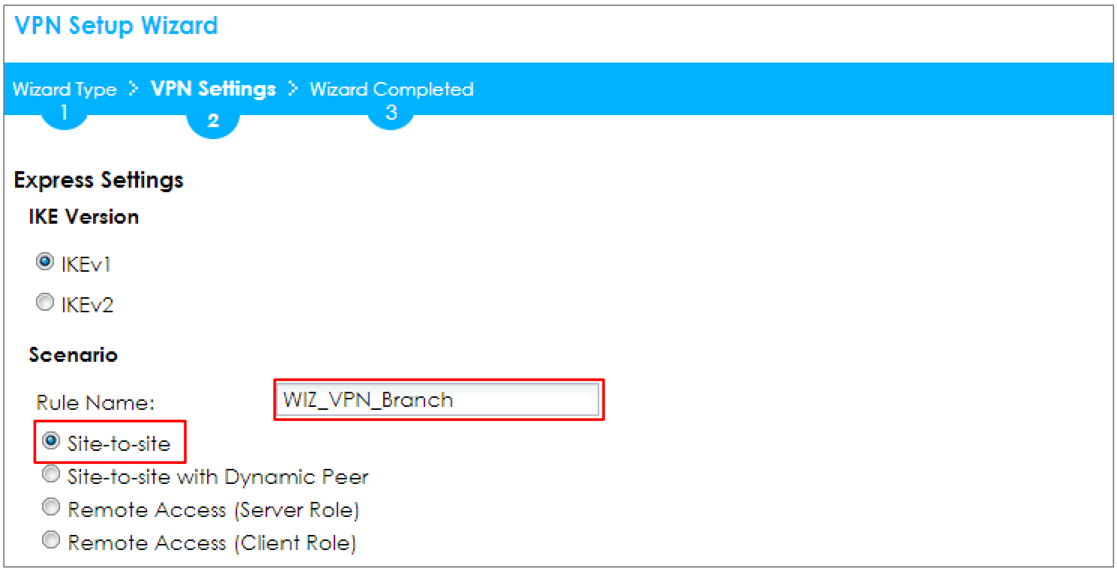
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch

● Site-to-site

○ Site-to-site with Dynamic Peer

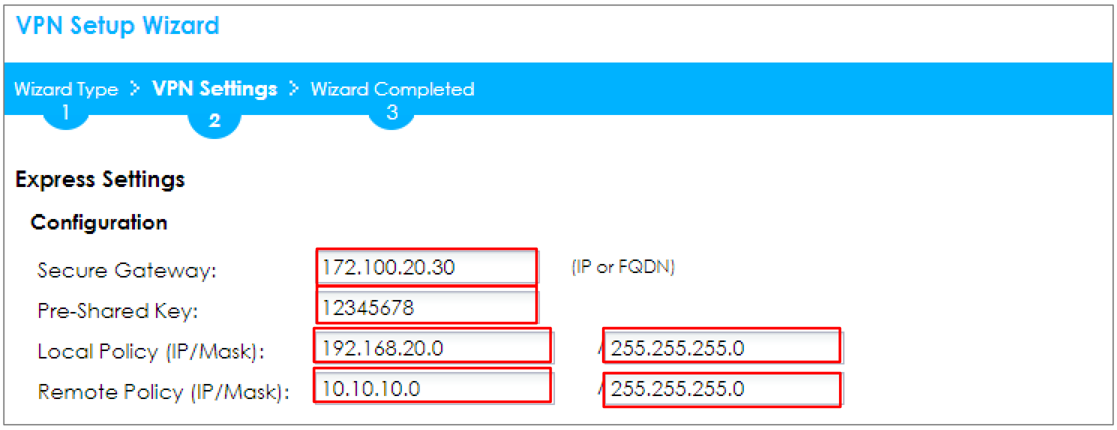
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the Branch's WAN IP address (in the example, 172.100.20.30). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG (HQ) and **Remote Policy** to be the IP address range of the network connected to the ZyWALL/USG (Branch).

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



VPN Setup Wizard

Express Settings

Configuration

Secure Gateway: 172.100.20.30 (IP or FQDN)

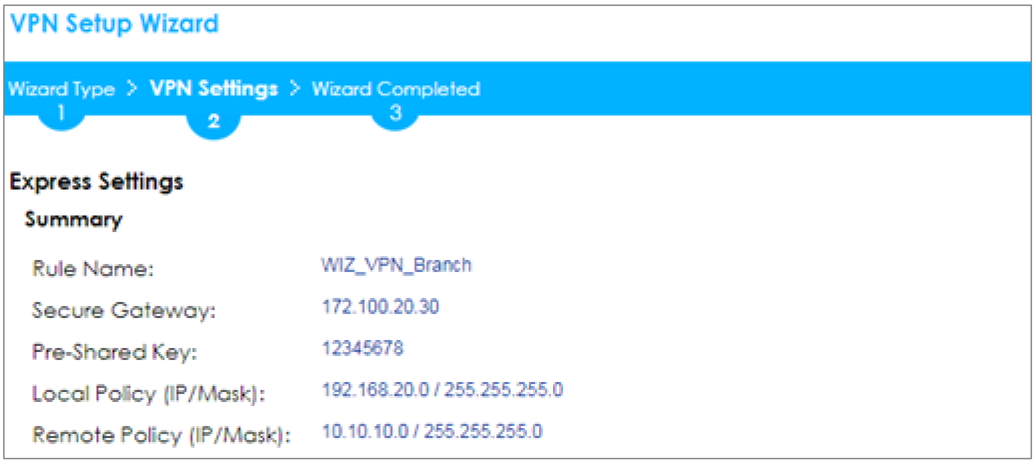
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.20.0 / 255.255.255.0

Remote Policy (IP/Mask): 10.10.10.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



VPN Setup Wizard

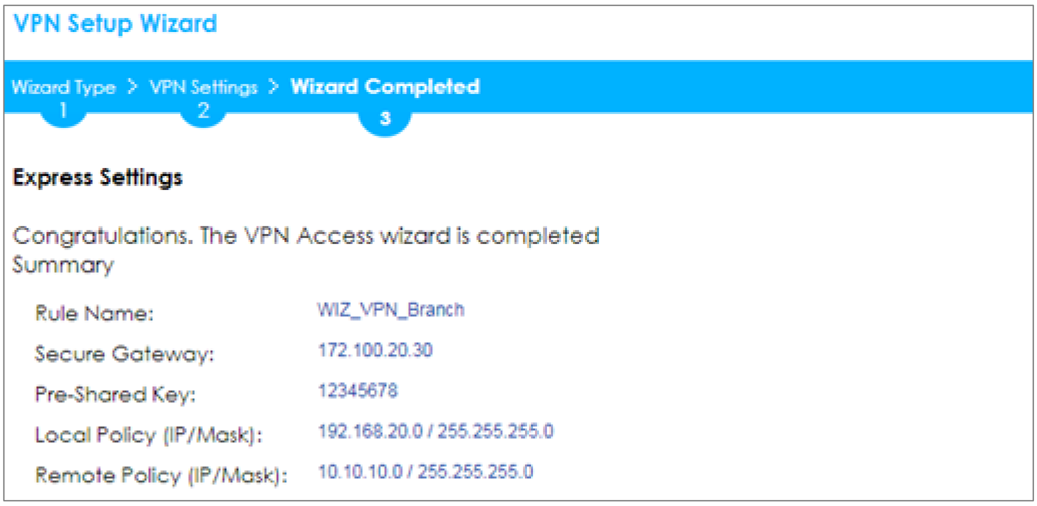
Express Settings

Summary

Rule Name:	WIZ_VPN_Branch
Secure Gateway:	172.100.20.30
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.20.0 / 255.255.255.0
Remote Policy (IP/Mask):	10.10.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



VPN Setup Wizard

Express Settings

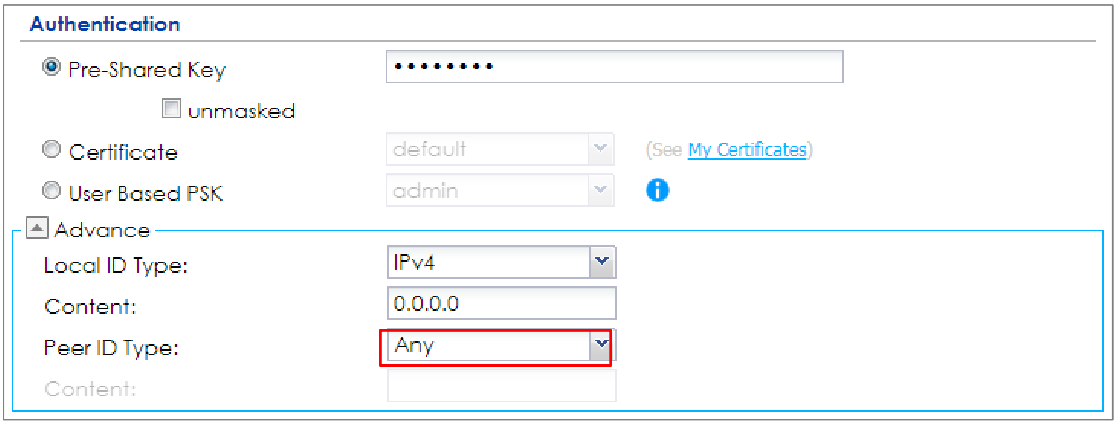
Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_VPN_Branch
Secure Gateway:	172.100.20.30
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.20.0 / 255.255.255.0
Remote Policy (IP/Mask):	10.10.10.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

● Pre-Shared Key: •••••••••
□ unmasked
○ Certificate: default (See My Certificates)
○ User Based PSK: admin

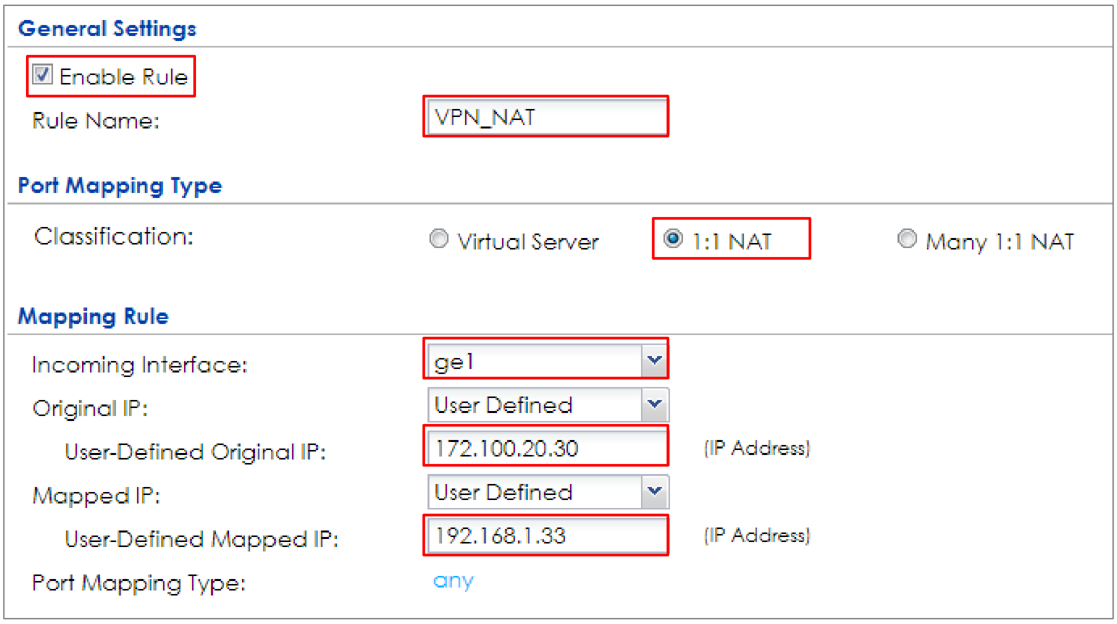
Advance
Local ID Type: IPv4
Content: 0.0.0.0
Peer ID Type: Any
Content:

Set Up the NAT Router (Using ZyWALL USG device in this example)

Go to **CONFIGURATION > Network > NAT > Add**. Select the **Incoming Interface** on which packets for the NAT rule must be received. Specified the **User-**

Defined Original IP field and Type the translated destination IP address that this NAT rule supports.

CONFIGURATION > Network > NAT > Add



General Settings

☑ Enable Rule

Rule Name: VPN_NAT

Port Mapping Type

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

Mapping Rule

Incoming Interface:	ge1	
Original IP:	User Defined	
User-Defined Original IP:	172.100.20.30	(IP Address)
Mapped IP:	User Defined	
User-Defined Mapped IP:	192.168.1.33	(IP Address)
Port Mapping Type:	any	

Go to **CONFIGURATION > Security Policy > Policy Control**. IP forwarding must be enabled at the firewall for the following IP protocols and UDP ports:

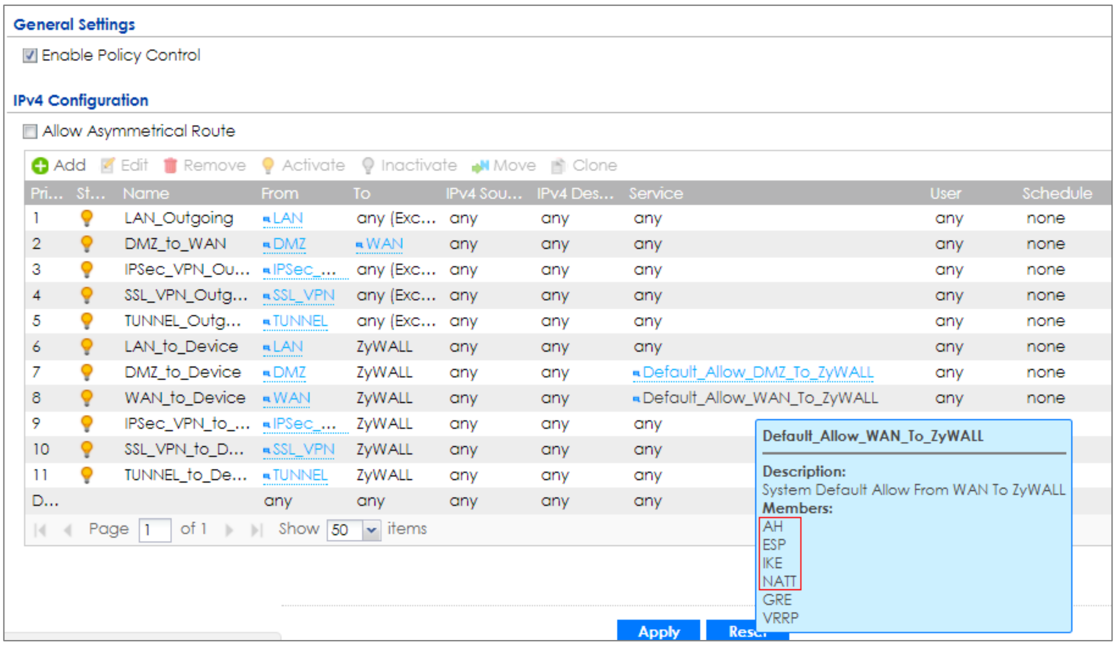
IP protocol = 50 → Used by data path (ESP)

IP protocol = 51 → Used by data path (AH)

UDP Port Number = 500 → Used by IKE (IPSec control path)

UDP Port Number = 4500 → Used by NAT-T (IPsec NAT traversal)

CONFIGURATION > Security Policy > Policy Control



General Settings

☑ Enable Policy Control

IPv4 Configuration

□ Allow Asymmetrical Route

Pri...	St...	Name	From	To	IPv4 Sou...	IPv4 Des...	Service	User	Schedule
1	💡	LAN_Outgoing	LAN	any (Exc...	any	any	any	any	none
2	💡	DMZ_to_WAN	DMZ	WAN	any	any	any	any	none
3	💡	IPSec_VPN_Ou...	IPSec_...	any (Exc...	any	any	any	any	none
4	💡	SSL_VPN_Outg...	SSL_VPN	any (Exc...	any	any	any	any	none
5	💡	TUNNEL_Outg...	TUNNEL	any (Exc...	any	any	any	any	none
6	💡	LAN_to_Device	LAN	ZyWALL	any	any	any	any	none
7	💡	DMZ_to_Device	DMZ	ZyWALL	any	any	Default_Allow_DMZ_To_ZyWALL	any	none
8	💡	WAN_to_Device	WAN	ZyWALL	any	any	Default_Allow_WAN_To_ZyWALL	any	none
9	💡	IPSec_VPN_to_...	IPSec_...	ZyWALL	any	any	any		
10	💡	SSL_VPN_to_D...	SSL_VPN	ZyWALL	any	any	any		
11	💡	TUNNEL_to_De...	TUNNEL	ZyWALL	any	any	any		
D...		any	any	any	any	any			

Page 1 of 1 Show 50 items

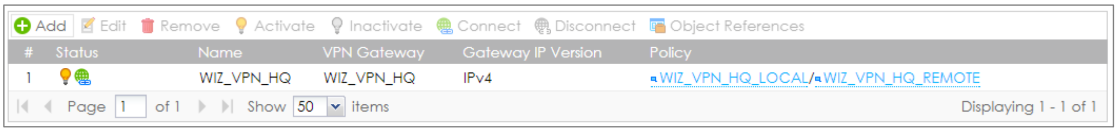
Default_Allow_WAN_To_ZyWALL

Description:
System Default Allow From WAN To ZyWALL
Members:
AH
ESP
IKE
NATT
GRE
VRRP

Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

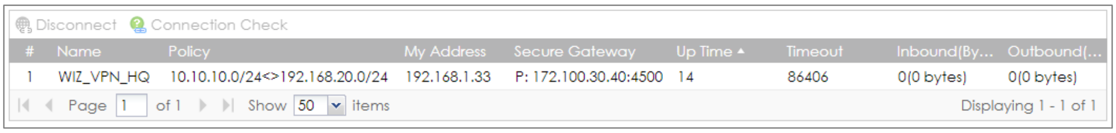


#	Status	Name	VPN Gateway	Gateway IP Version	Policy
1	💡	WIZ_VPN_HQ	WIZ_VPN_HQ	IPv4	WIZ_VPN_HQ_LOCAL/WIZ_VPN_HQ_REMOTE

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

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound (Bytes)/Outbound (Bytes)** Traffic.

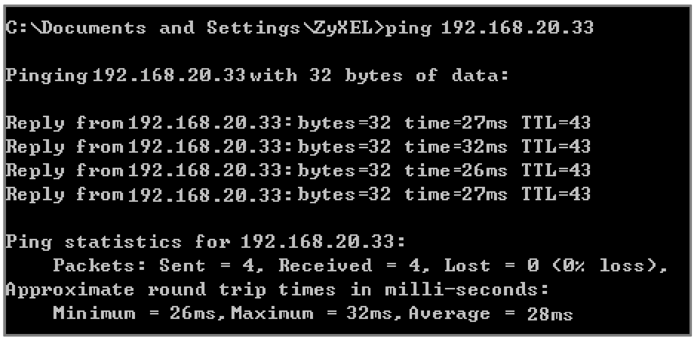
MONITOR > VPN Monitor > IPSec



#	Name	Policy	My Address	Secure Gateway	Up Time ▲	Timeout	Inbound(By...	Outbound(...
1	WIZ_VPN_HQ	10.10.10.0/24<>192.168.20.0/24	192.168.1.33	P: 172.100.30.40:4500	14	86406	0(0 bytes)	0(0 bytes)

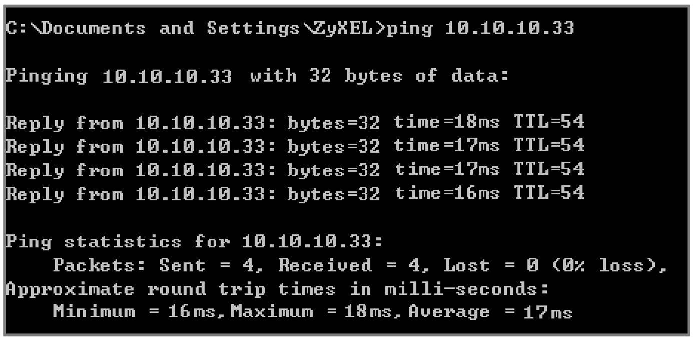
To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC behind ZyWALL/USG (HQ) > Window 7 > cmd > ping 192.168.20.33



```
C:\Documents and Settings\ZyXEL>ping 192.168.20.33

Pinging 192.168.20.33 with 32 bytes of data:

Reply from 192.168.20.33: bytes=32 time=27ms TTL=43
Reply from 192.168.20.33: bytes=32 time=32ms TTL=43
Reply from 192.168.20.33: bytes=32 time=26ms TTL=43
Reply from 192.168.20.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.20.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

PC behind ZyWALL/USG (Branch) > Window 7 > cmd > ping 10.10.10.33

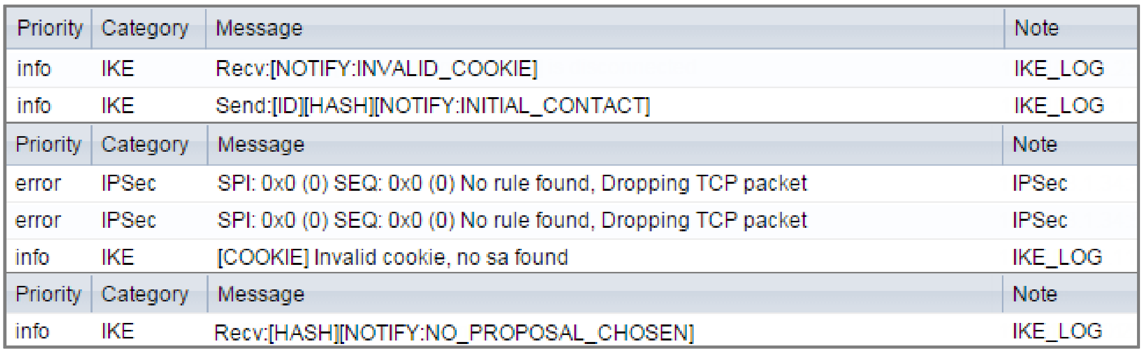


```
C:\Documents and Settings\ZyXEL>ping 10.10.10.33

Pinging 10.10.10.33 with 32 bytes of data:

Reply from 10.10.10.33: bytes=32 time=18ms TTL=54
Reply from 10.10.10.33: bytes=32 time=17ms TTL=54
Reply from 10.10.10.33: bytes=32 time=17ms TTL=54
Reply from 10.10.10.33: bytes=32 time=16ms TTL=54

Ping statistics for 10.10.10.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log



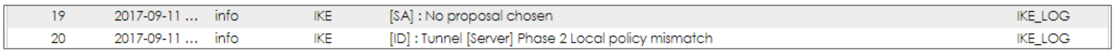
Priority	Category	Message	Note
info	IKE	Recv:[NOTIFY:INVALID_COOKIE]	IKE_LOG
info	IKE	Send:[ID][HASH][NOTIFY:INITIAL_CONTACT]	IKE_LOG

Priority	Category	Message	Note
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
info	IKE	[COOKIE] Invalid cookie, no sa found	IKE_LOG

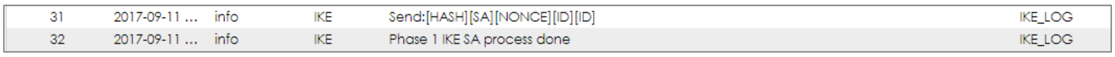
Priority	Category	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log



19	2017-09-11 ...	info	IKE	[SA] : No proposal chosen	IKE_LOG
20	2017-09-11 ...	info	IKE	[ID] : Tunnel [Server] Phase 2 Local policy mismatch	IKE_LOG



31	2017-09-11 ...	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

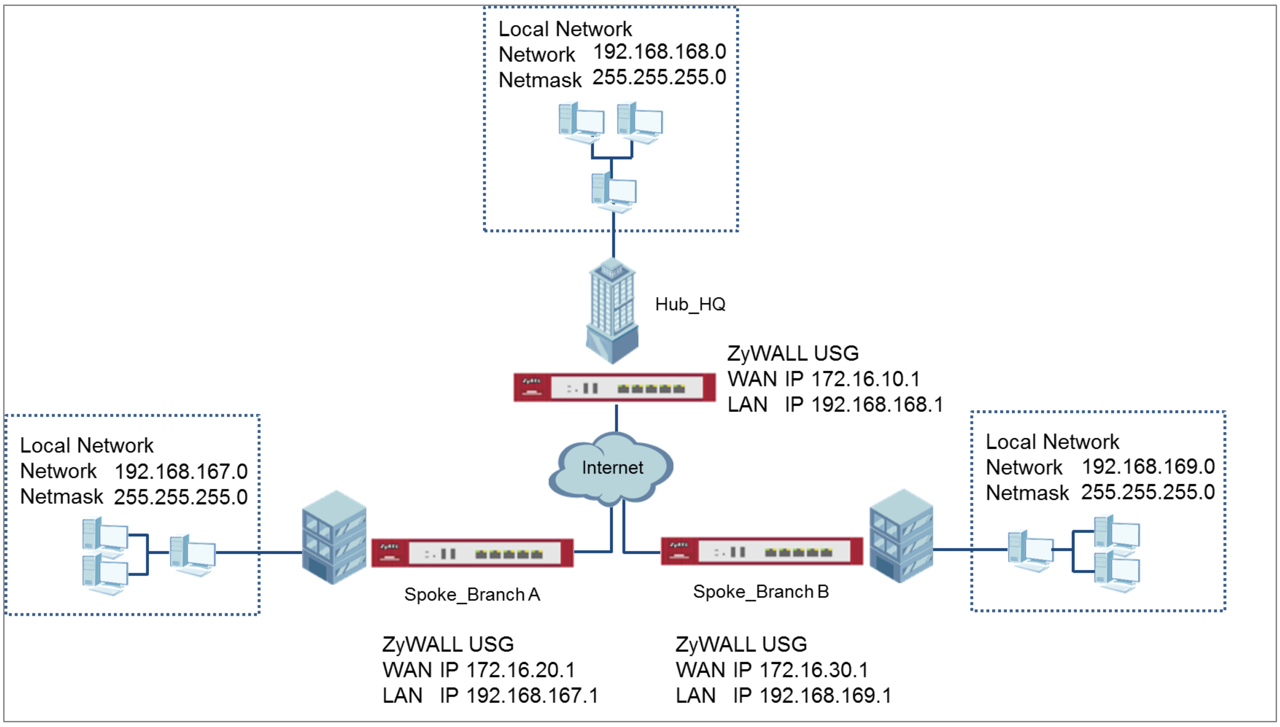
Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure Hub-and-Spoke IPSec VPN

This is an example of a hub-and-spoke VPN with the HQ ZyWALL/USG as the hub and spoke VPNs to Branches A and B. When the VPN tunnel is configured, traffic passes between branches via the hub (HQ). Traffic can also pass between spoke-and-spoke through the hub. Here are two methods to set up hub-and-spoke VPN connections: 1. With VPN Concentrator 2. Without VPN Concentrator. With just two branch offices, you could just manually set up VPN tunnels between HQ and the branches. With many branches it's best to use the VPN Concentrator to set up branch-HQ tunnels automatically.

ZyWALL/USG Hub-and-Spoke VPN Example

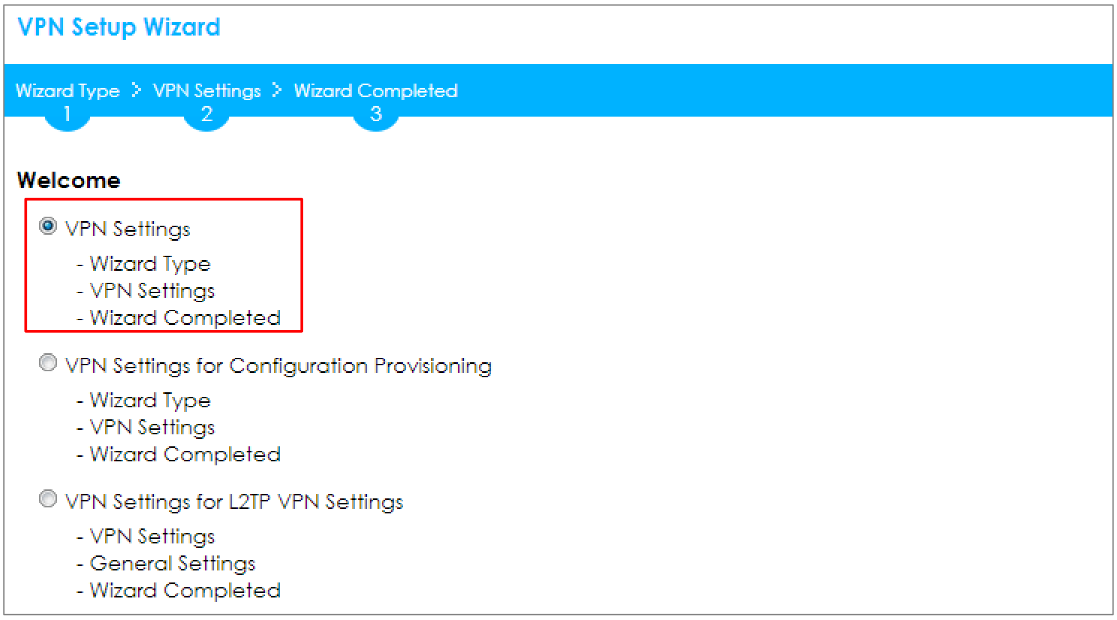


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG by Using VPN Concentrator Hub_HQ-to-Branch_A

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Welcome

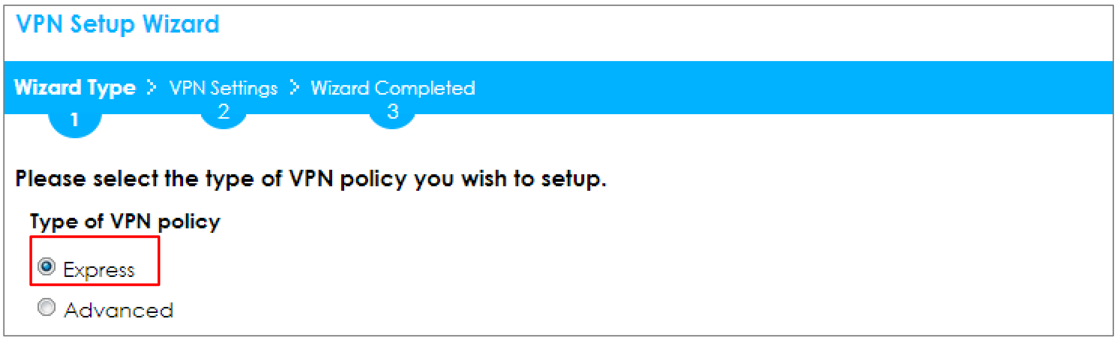
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Please select the type of VPN policy you wish to setup.

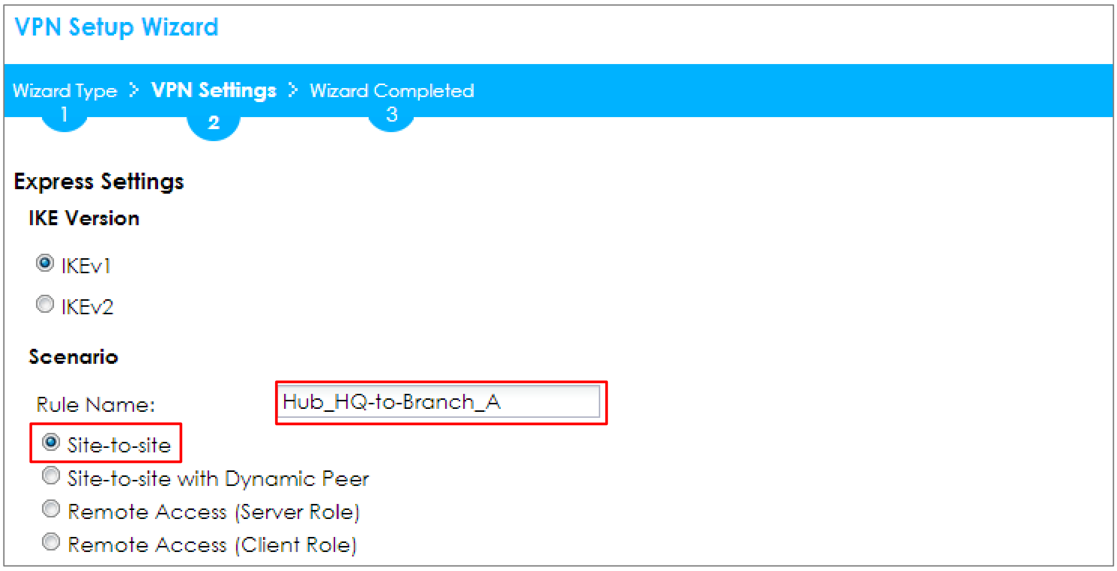
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



Express Settings

IKE Version

● IKEv1
○ IKEv2

Scenario

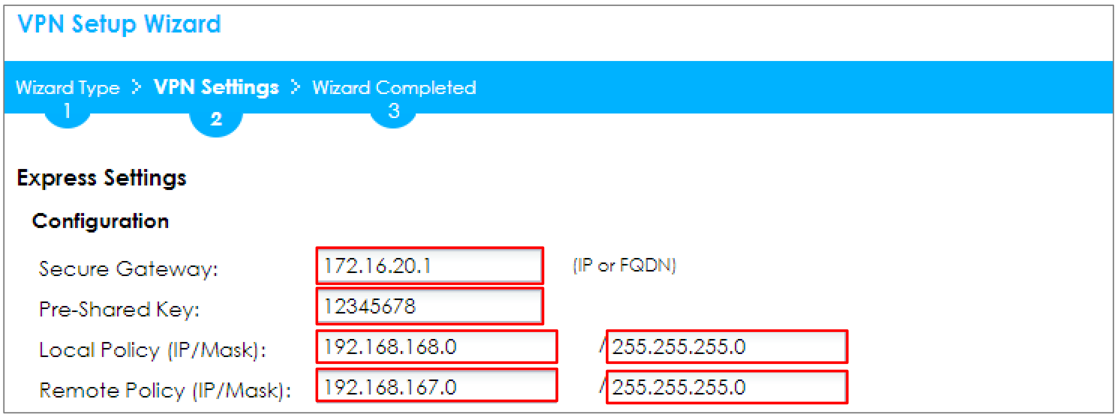
Rule Name: Hub_HQ-to-Branch_A

● Site-to-site
○ Site-to-site with Dynamic Peer
○ Remote Access (Server Role)
○ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the **Branch A**'s Gateway IP address (in the example, 172.16.20.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch A**'s Pre-Shared Key.

Set **Local Policy** to be the IP address range of the network connected to the **Hub_HQ** and **Remote Policy** to be the IP address range of the network connected to the **Branch A**. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



Express Settings

Configuration

Secure Gateway: 172.16.20.1 (IP or FQDN)

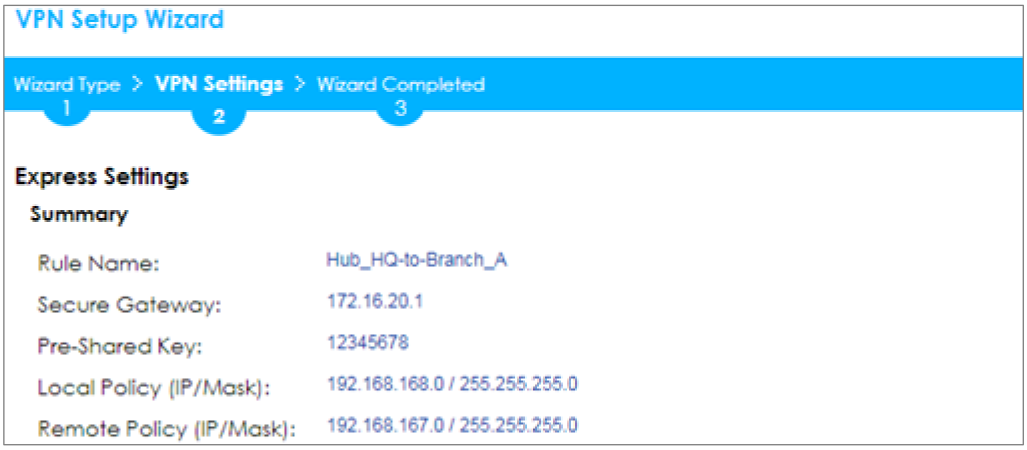
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.167.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Summary)



Express Settings

Summary

Rule Name: Hub_HQ-to-Branch_A

Secure Gateway: 172.16.20.1

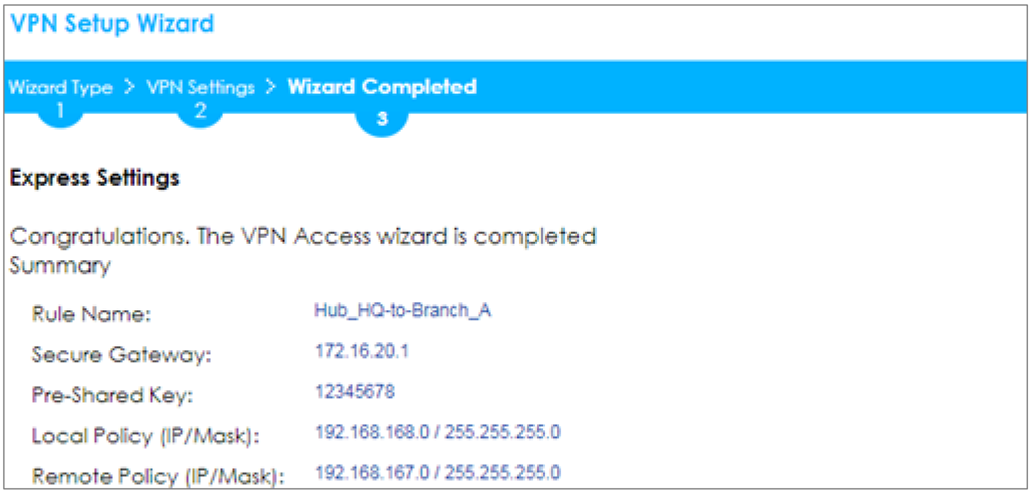
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.167.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard Completed



Express Settings

Congratulations. The VPN Access wizard is completed

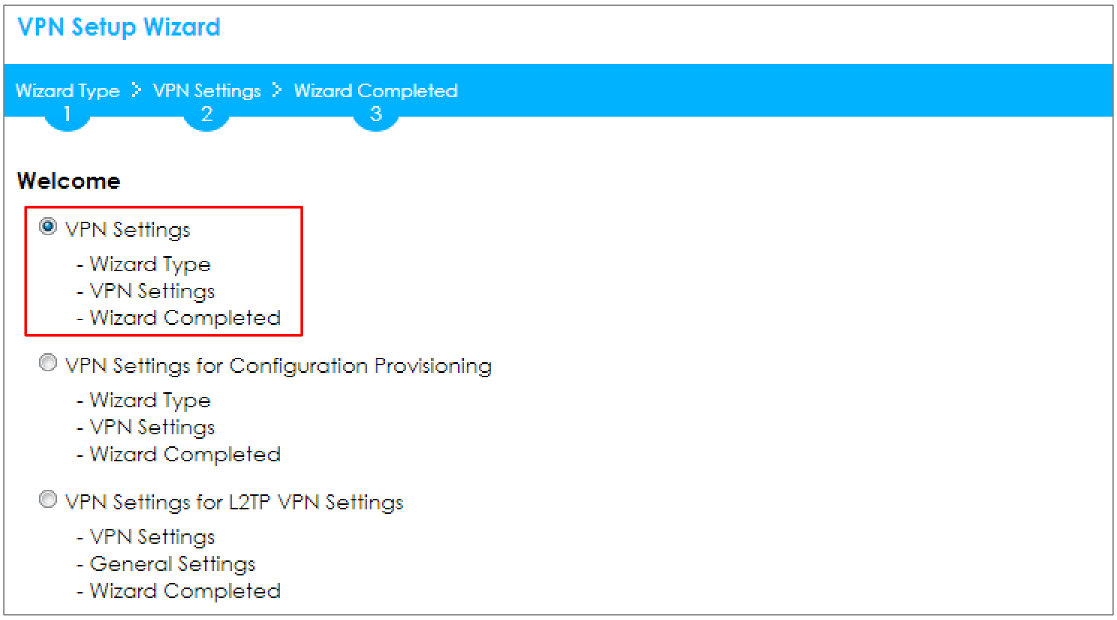
Summary

Rule Name:	Hub_HQ-to-Branch_A
Secure Gateway:	172.16.20.1
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.168.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.167.0 / 255.255.255.0

Hub_HQ-to-Branch_B

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

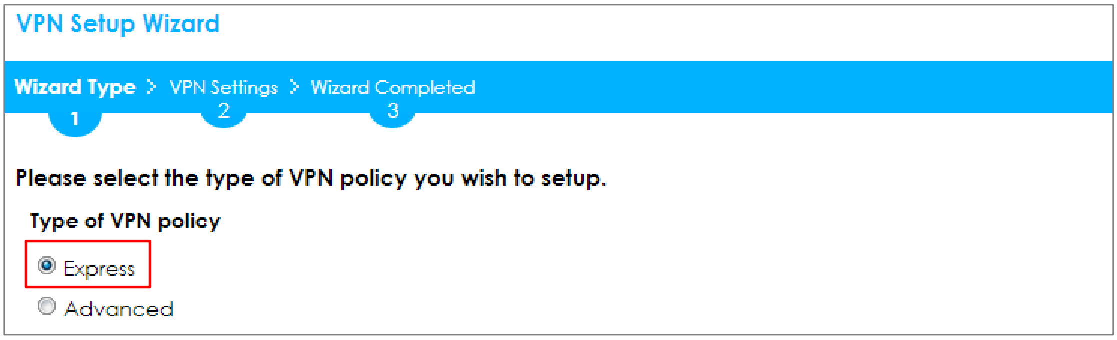
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



VPN Setup Wizard

Please select the type of VPN policy you wish to setup.

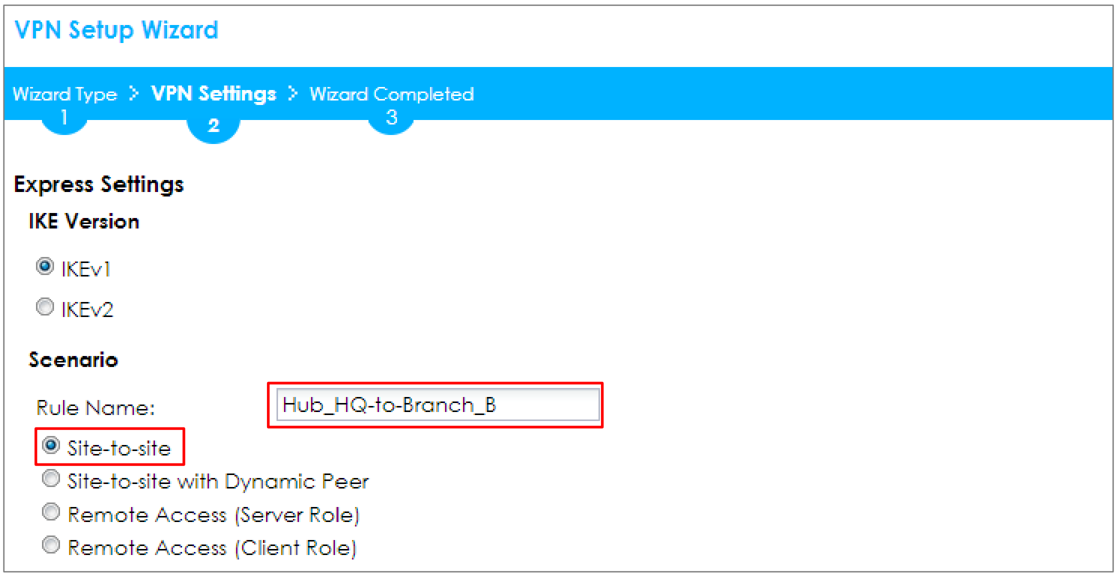
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: Hub_HQ-to-Branch_B

● Site-to-site

○ Site-to-site with Dynamic Peer

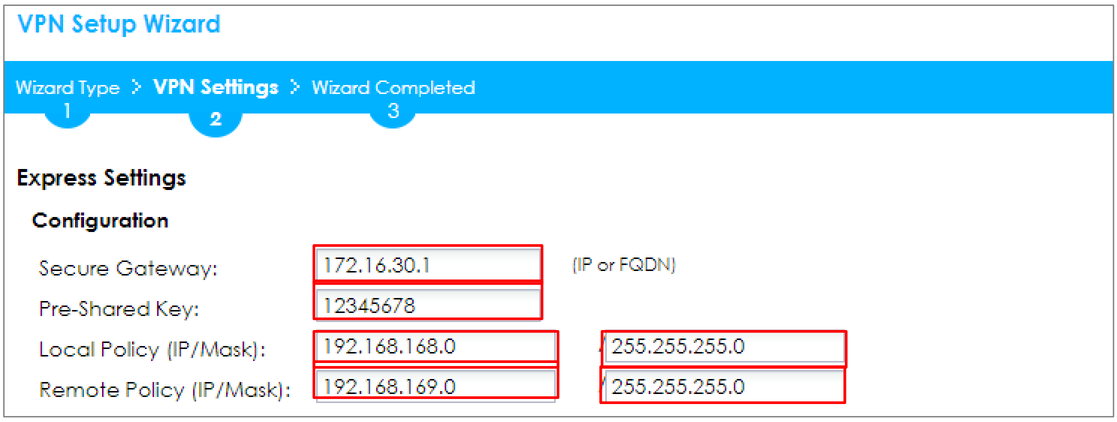
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the **Branch B**'s Gateway IP address (in the example, 172.16.30.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch B**'s Pre-Shared Key.

Set **Local Policy** to be the IP address range of the network connected to the **Hub_HQ** and **Remote Policy** to be the IP address range of the network connected to the **Branch B**. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



Express Settings

Configuration

Secure Gateway: 172.16.30.1 (IP or FQDN)

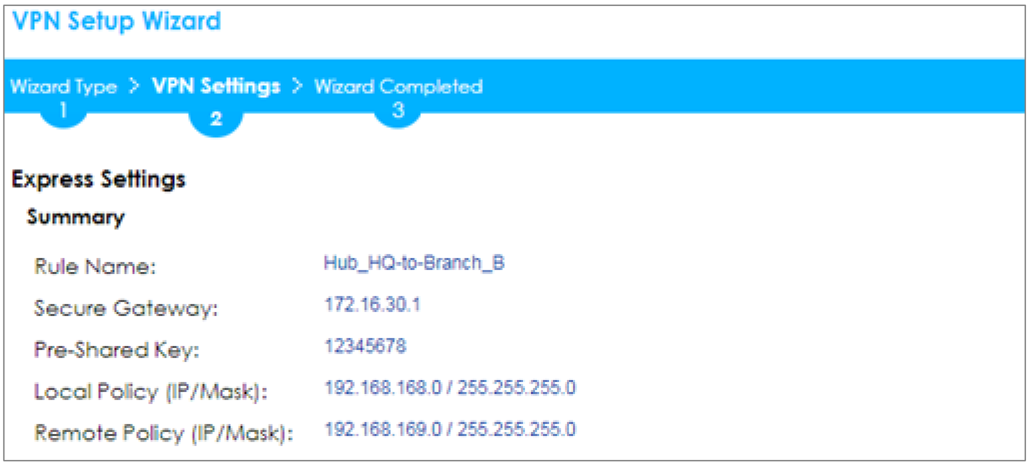
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 255.255.255.0

Remote Policy (IP/Mask): 192.168.169.0 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Summary)



Express Settings

Summary

Rule Name: Hub_HQ-to-Branch_B

Secure Gateway: 172.16.30.1

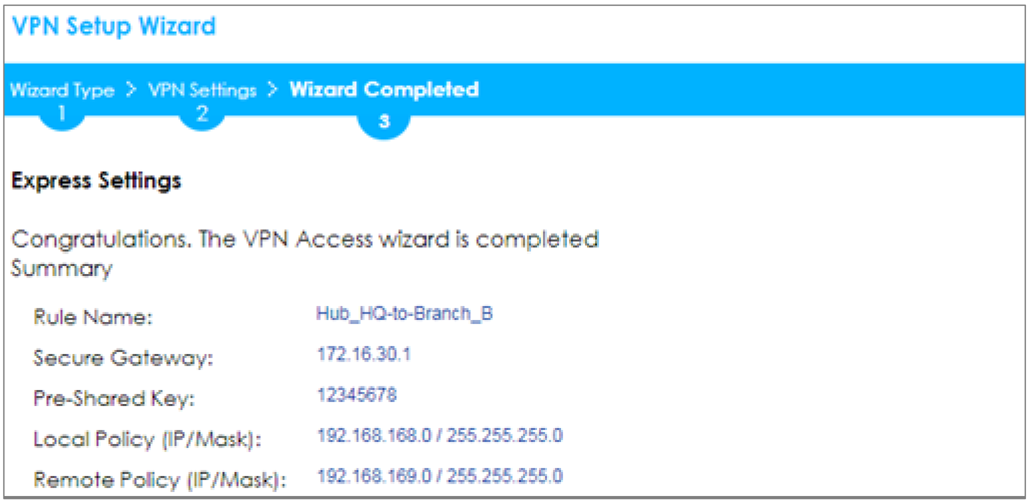
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.169.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard Completed



VPN Setup Wizard

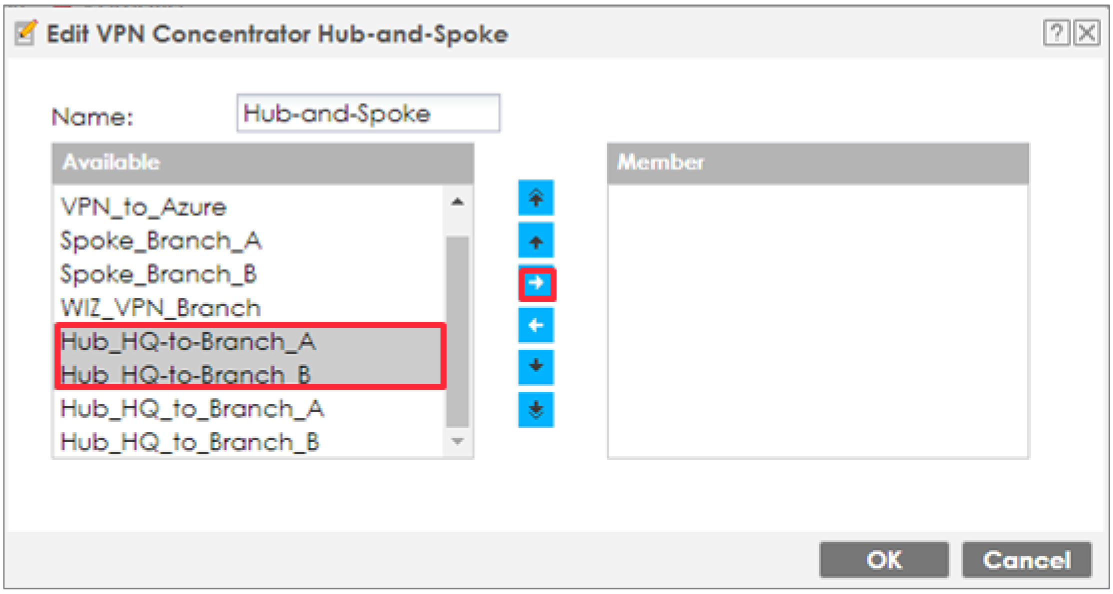
Express Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	Hub_HQ-to-Branch_B
Secure Gateway:	172.16.30.1
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.168.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.169.0 / 255.255.255.0

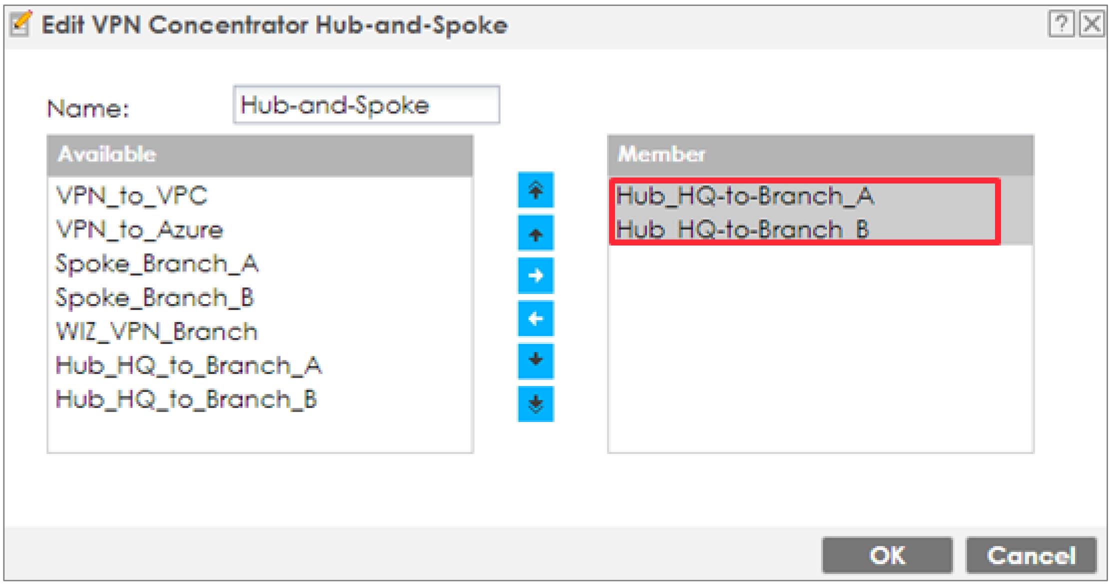
Hub_HQ Concentrator

In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPSec VPN > Concentrator**, add a VPN Concentrator rule. Select VPN tunnels to be in the same member group and click **Save**.



Edit VPN Concentrator Hub-and-Spoke

Name: Hub-and-Spoke



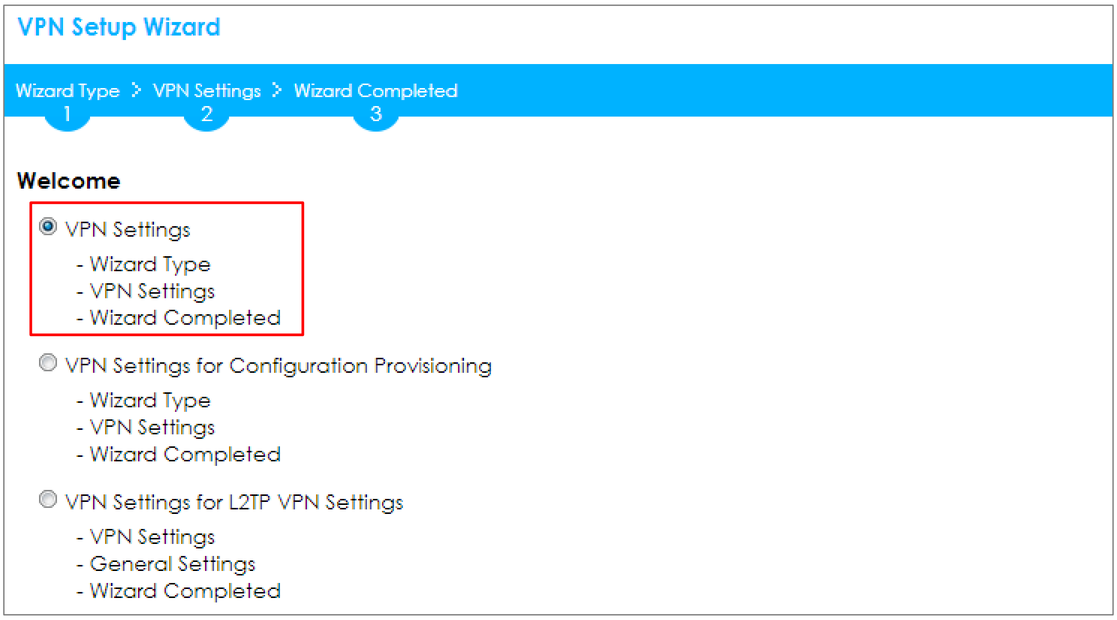
Edit VPN Concentrator Hub-and-Spoke

Name: Hub-and-Spoke

Spoke_Branch_A

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



Welcome

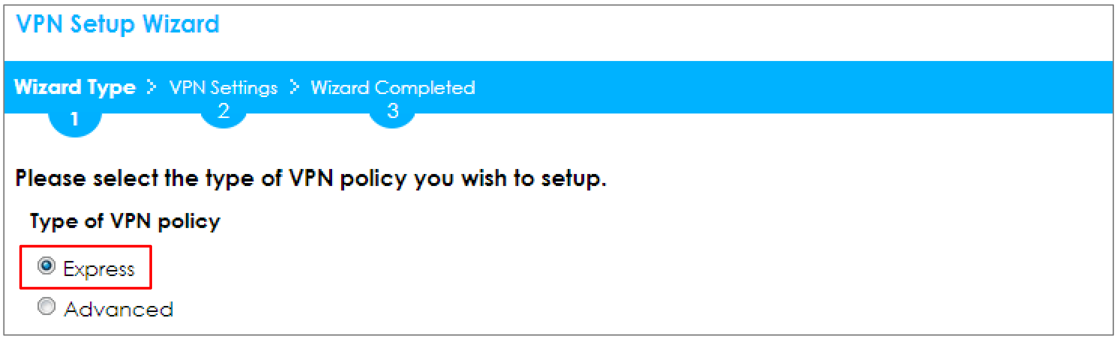
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



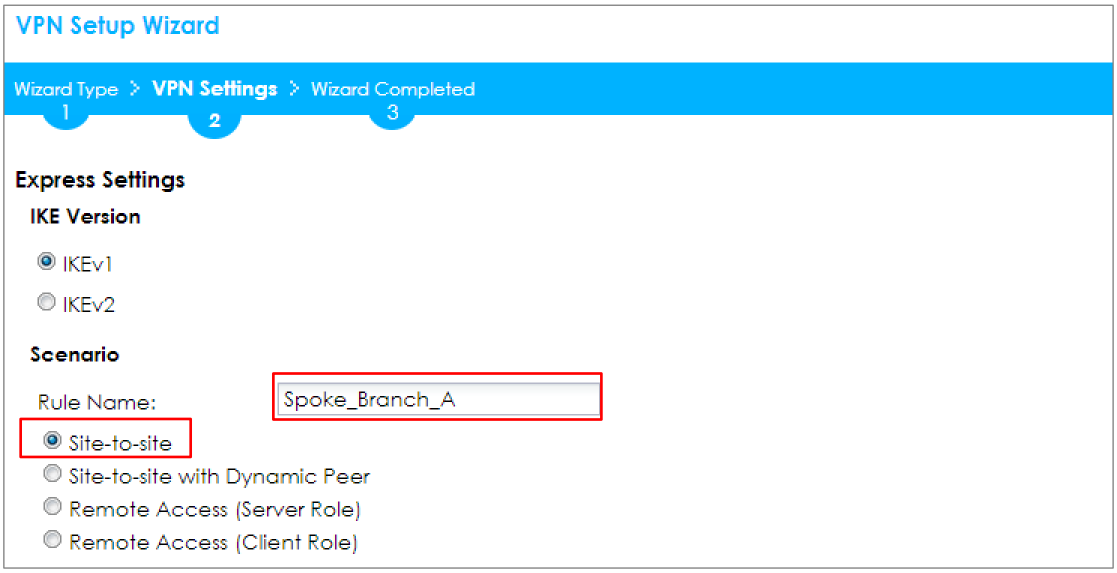
Please select the type of VPN policy you wish to setup.

Type of VPN policy

● Express
○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: Spoke_Branch_A

● Site-to-site

○ Site-to-site with Dynamic Peer

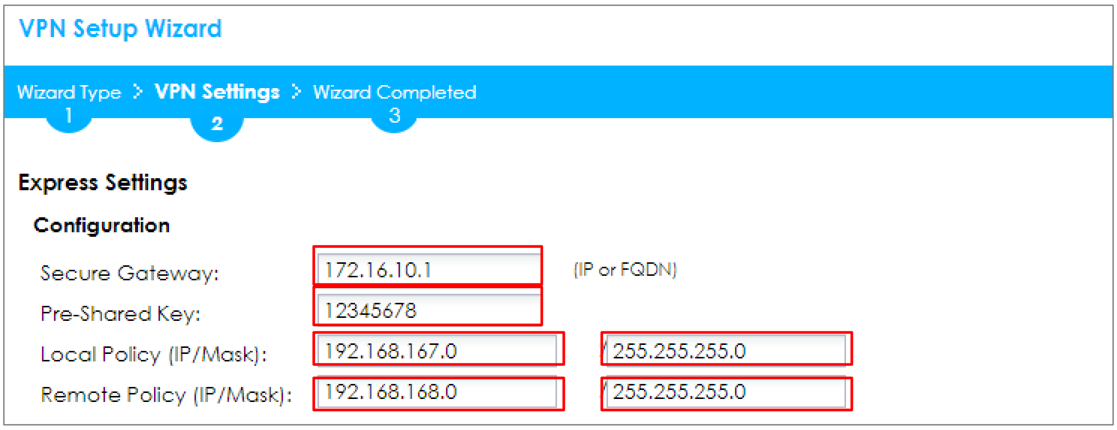
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the **Hub_HQ**'s Gateway IP address (in the example, 172.16.10.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ**'s Pre-Shared Key.

Set **Local Policy** to be the IP address range of the network connected to the **Spoke_Branch_A** and **Remote Policy** to be the IP address range of the network connected to the **Hub_HQ**. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



VPN Setup Wizard

Express Settings

Configuration

Secure Gateway: 172.16.10.1 (IP or FQDN)

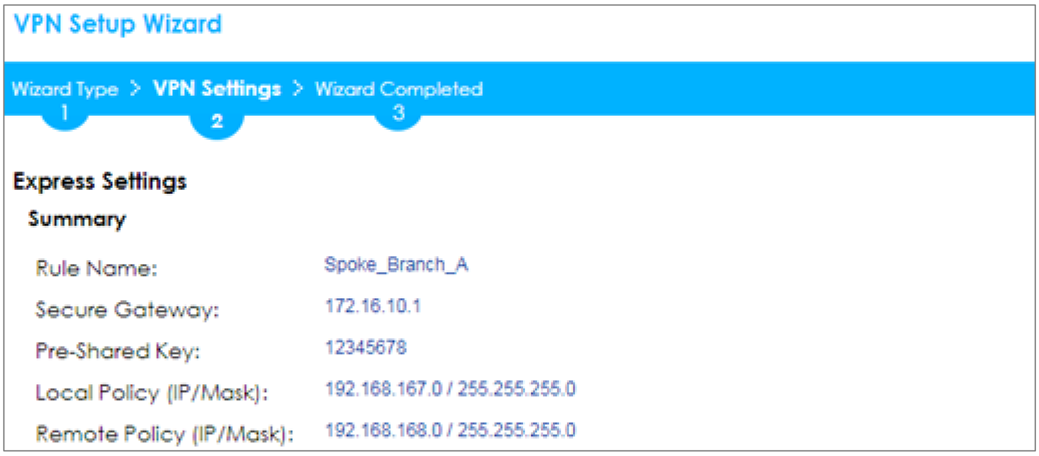
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.167.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Summary)



VPN Setup Wizard

Express Settings

Summary

Rule Name: Spoke_Branch_A

Secure Gateway: 172.16.10.1

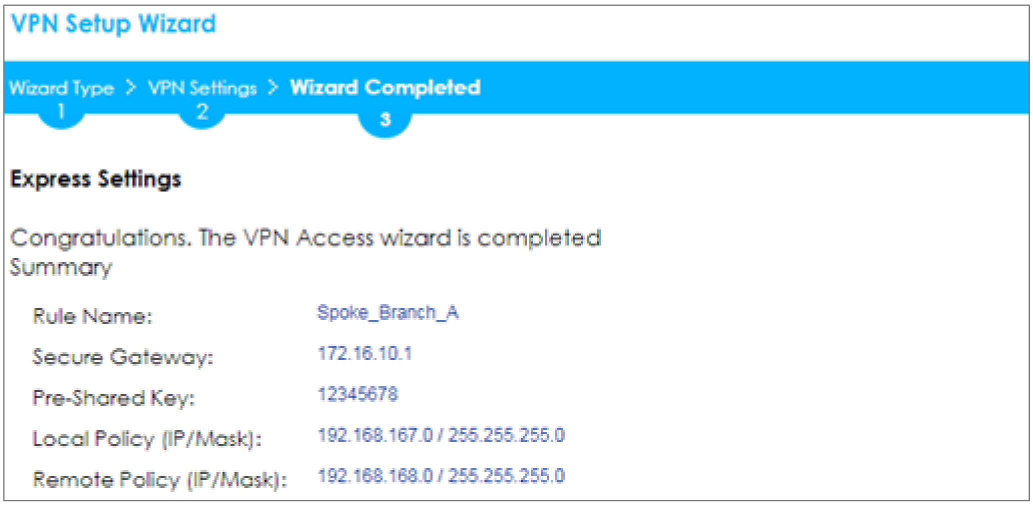
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.167.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard Completed



VPN Setup Wizard

Express Settings

Congratulations. The VPN Access wizard is completed
Summary

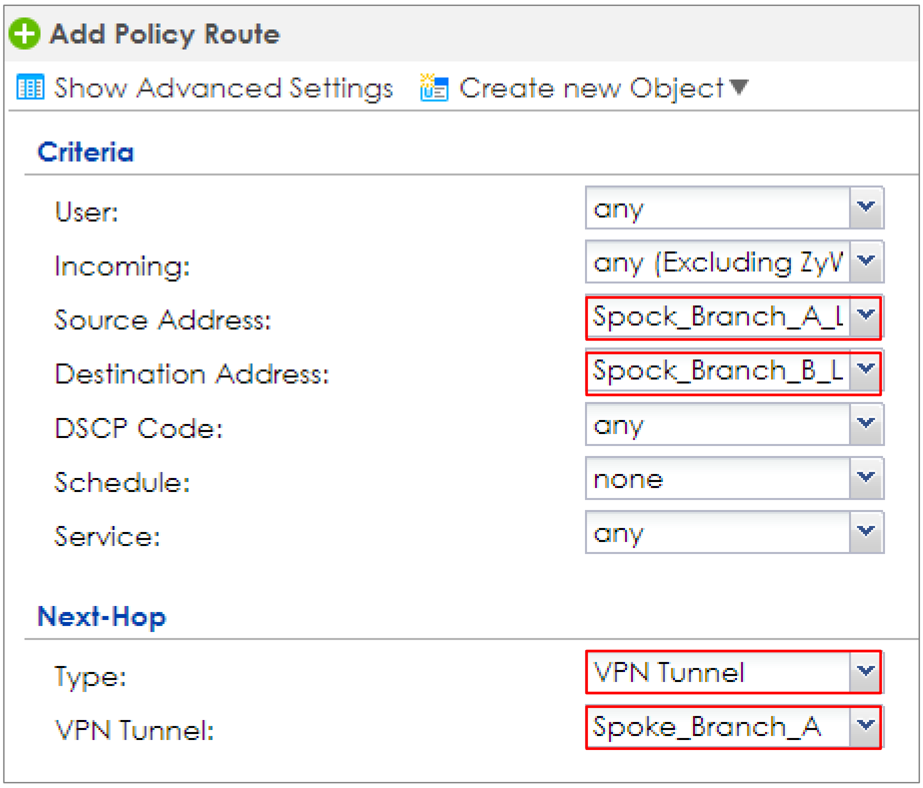
Rule Name:	Spoke_Branch_A
Secure Gateway:	172.16.10.1
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.167.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.168.0 / 255.255.255.0

Go to **Network > Routing > Policy Route** to add a **Policy Route** to allow traffic from **Spoke_Branch_A** to **Spoke_Branch_B**.

Click **Create new Object** and set **Address** to be the local network behind the **Spoke_Branch_B**. Select **Source Address** to be the local network behind the

Spoke_Branch_A. Then, scroll down the **Destination Address** list to choose the newly created **Spoke_Branch_B_LOCAL** address. Click **OK**.

Network > Routing > Policy Route



Criteria

User:	any
Incoming:	any (Excluding ZyW
Source Address:	Spock_Branch_A_L
Destination Address:	Spock_Branch_B_L
DSCP Code:	any
Schedule:	none
Service:	any

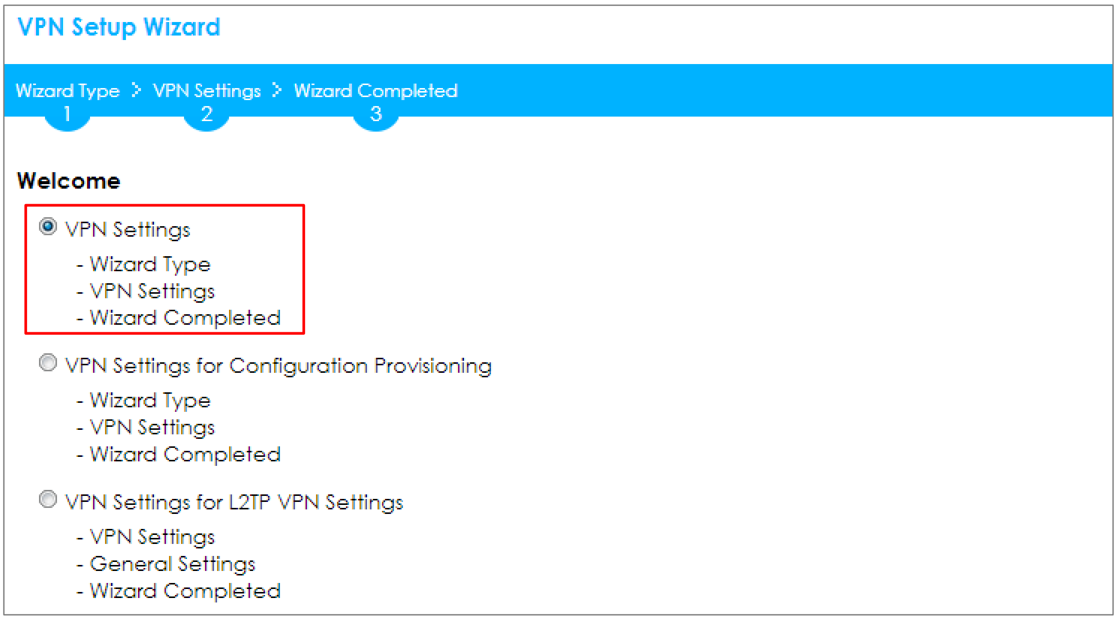
Next-Hop

Type:	VPN Tunnel
VPN Tunnel:	Spoke_Branch_A

Spoke_Branch_B

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

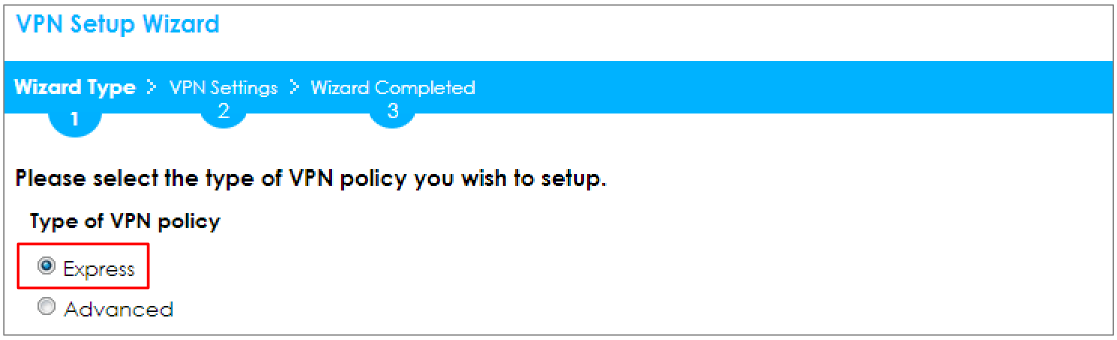
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



VPN Setup Wizard

Please select the type of VPN policy you wish to setup.

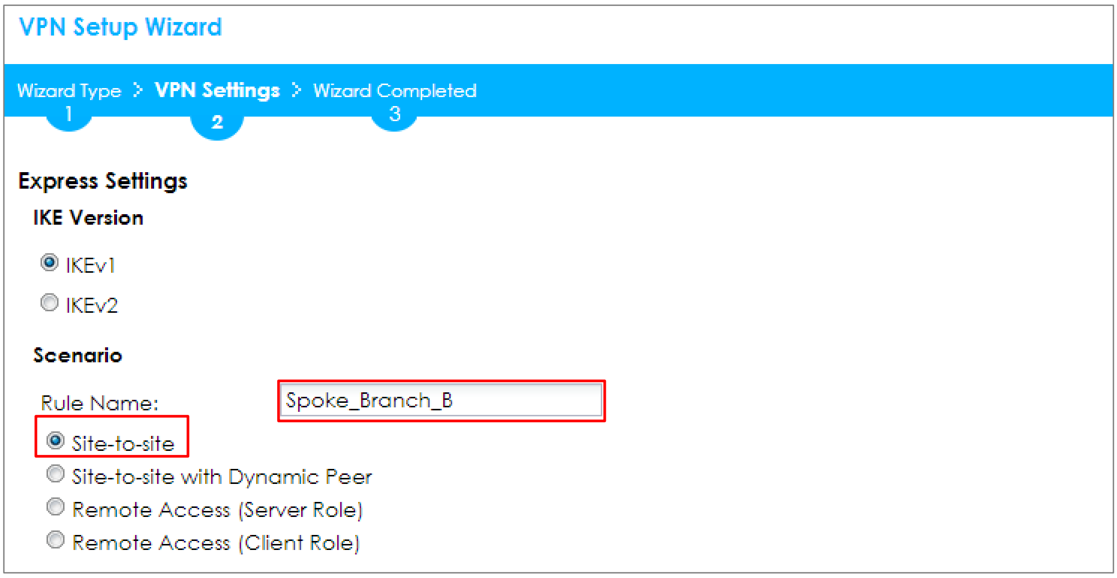
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: Spoke_Branch_B

● Site-to-site

○ Site-to-site with Dynamic Peer

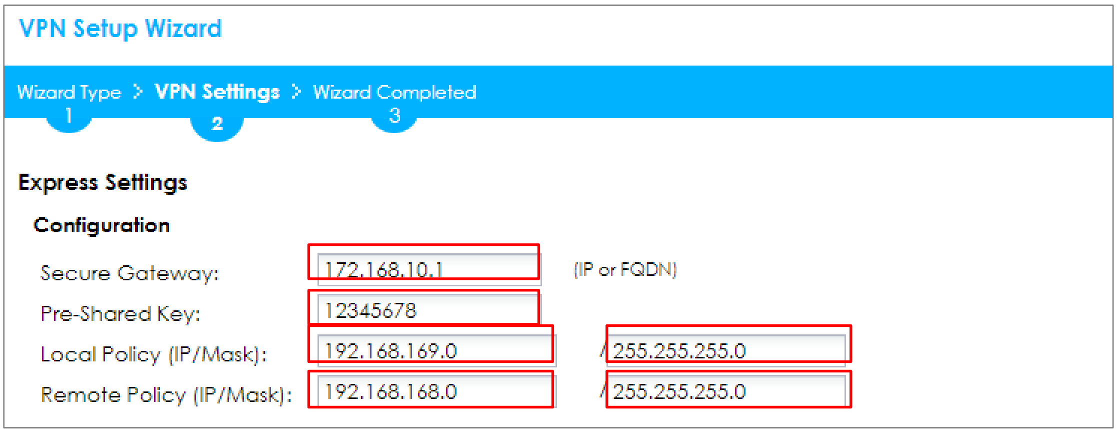
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the **Hub_HQ**'s Gateway IP address (in the example, 172.16.10.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ**'s Pre-Shared Key.

Set **Local Policy** to be the IP address range of the network connected to the **Spoke_Branch_B** and **Remote Policy** to be the IP address range of the network connected to the **Hub_HQ**. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



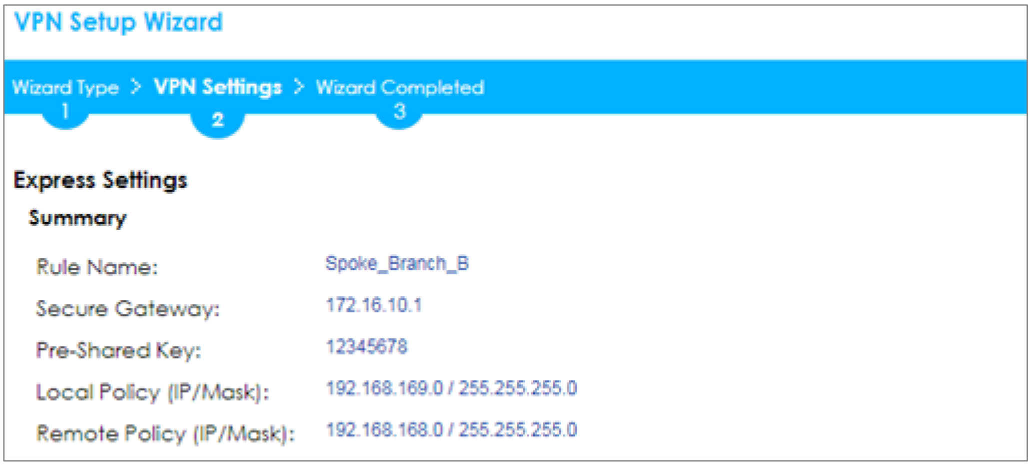
Express Settings

Configuration

Secure Gateway:	172.168.10.1	(IP or FQDN)
Pre-Shared Key:	12345678	
Local Policy (IP/Mask):	192.168.169.0	/ 255.255.255.0
Remote Policy (IP/Mask):	192.168.168.0	/ 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Summary)



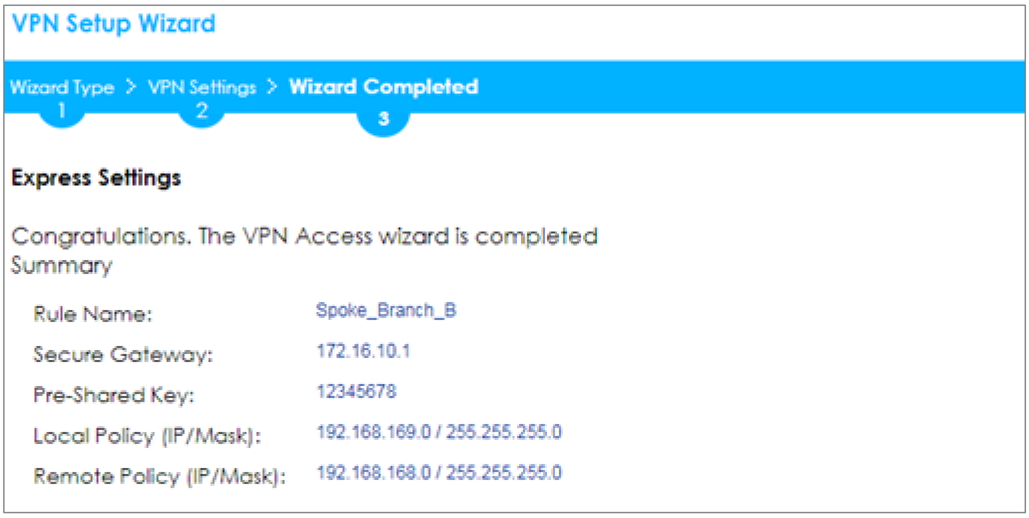
Express Settings

Summary

Rule Name:	Spoke_Branch_B
Secure Gateway:	172.16.10.1
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.169.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.168.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard Completed



Express Settings

Congratulations. The VPN Access wizard is completed
Summary

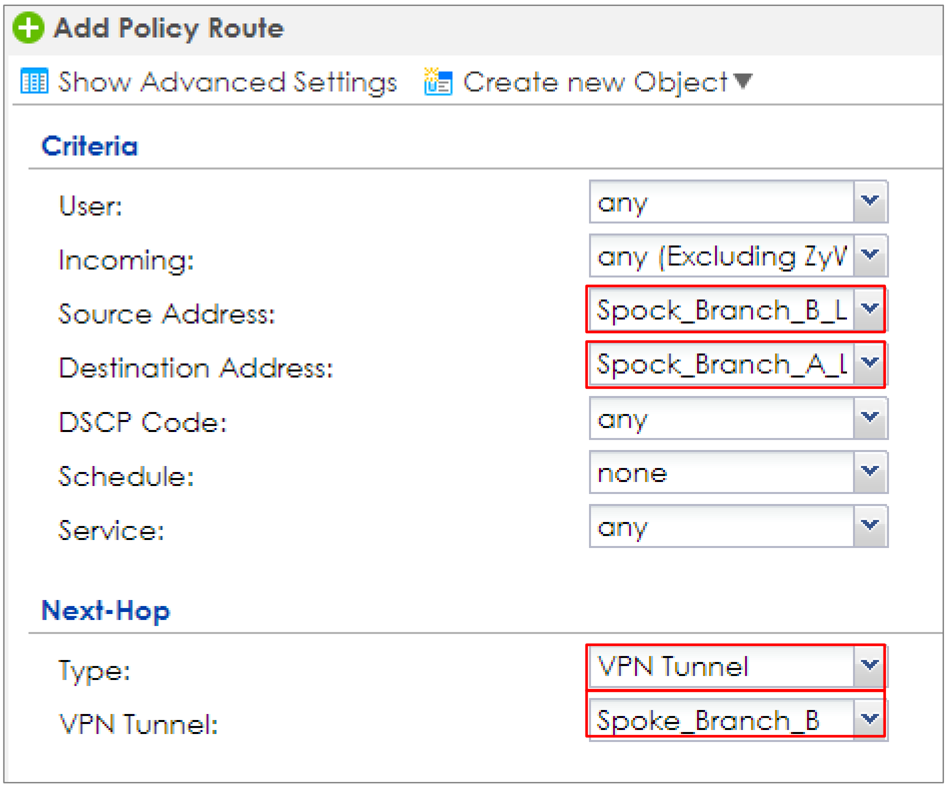
Rule Name:	Spoke_Branch_B
Secure Gateway:	172.16.10.1
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.169.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.168.0 / 255.255.255.0

Go to **Network > Routing > Policy Route** to add a Policy Route to allow traffic from **Spoke_Branch_B** to **Spoke_Branch_A**.

Click **Create new Object** and set **Address** to be the local network behind the **Spoke_Branch_A**. Select **Source Address** to be the local network behind the

Spoke_Branch_B. Then, scroll down the **Destination Address** list to choose the newly created **Spoke_Branch_A_LOCAL** address. Click **OK**.

Network > Routing > Policy Route



Add Policy Route

Criteria

User:	any
Incoming:	any (Excluding ZyW
Source Address:	Spock_Branch_B_L
Destination Address:	Spock_Branch_A_L
DSCP Code:	any
Schedule:	none
Service:	any

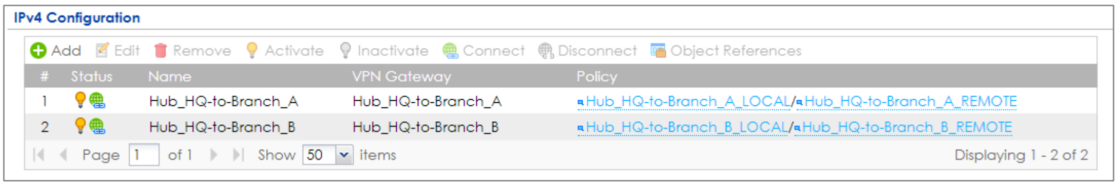
Next-Hop

Type:	VPN Tunnel
VPN Tunnel:	Spoke_Branch_B

Test the IPSec VPN Tunnel

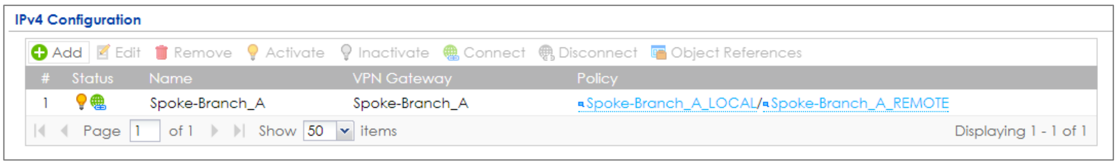
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

Hub_HQ > CONFIGURATION > VPN > IPSec VPN > VPN Connection



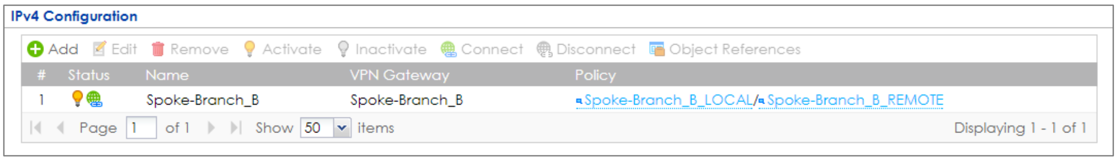
#	Status	Name	VPN Gateway	Policy
1		Hub_HQ-to-Branch_A	Hub_HQ-to-Branch_A	Hub_HQ-to-Branch_A_LOCAL/Hub_HQ-to-Branch_A_REMOTE
2		Hub_HQ-to-Branch_B	Hub_HQ-to-Branch_B	Hub_HQ-to-Branch_B_LOCAL/Hub_HQ-to-Branch_B_REMOTE

Spoke_Branch_A > CONFIGURATION > VPN > IPSec VPN > VPN Connection



#	Status	Name	VPN Gateway	Policy
1		Spoke-Branch_A	Spoke-Branch_A	Spoke-Branch_A_LOCAL/Spoke-Branch_A_REMOTE

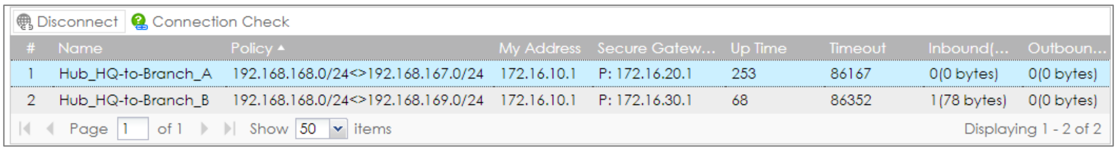
Spoke_Branch_B > CONFIGURATION > VPN > IPSec VPN > VPN Connection



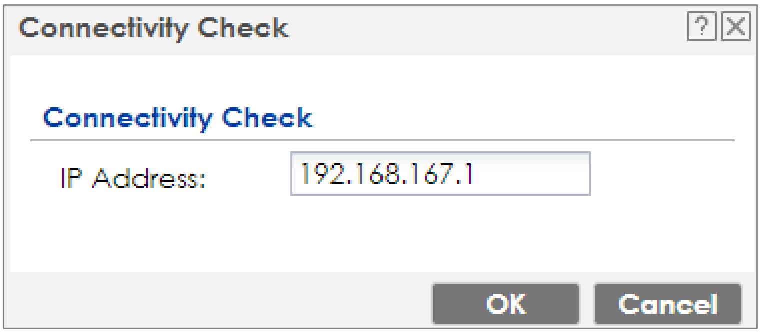
#	Status	Name	VPN Gateway	Policy
1		Spoke-Branch_B	Spoke-Branch_B	Spoke-Branch_B_LOCAL/Spoke-Branch_B_REMOTE

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_A



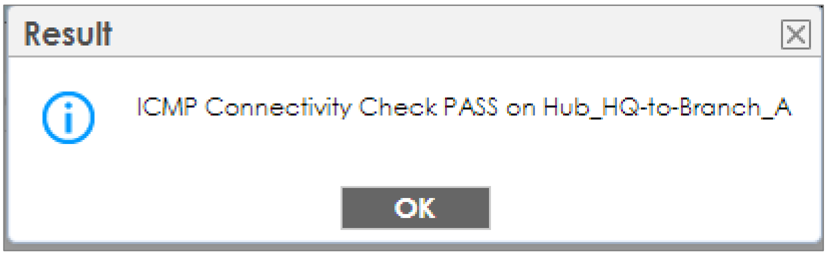
#	Name	Policy ▲	My Address	Secure Gatew...	Up Time	Timeout	Inbound(...	Outboun...
1	Hub_HQ-to-Branch_A	192.168.168.0/24<>192.168.167.0/24	172.16.10.1	P: 172.16.20.1	253	86167	0(0 bytes)	0(0 bytes)
2	Hub_HQ-to-Branch_B	192.168.168.0/24<>192.168.169.0/24	172.16.10.1	P: 172.16.30.1	68	86352	1(78 bytes)	0(0 bytes)



Connectivity Check

Connectivity Check

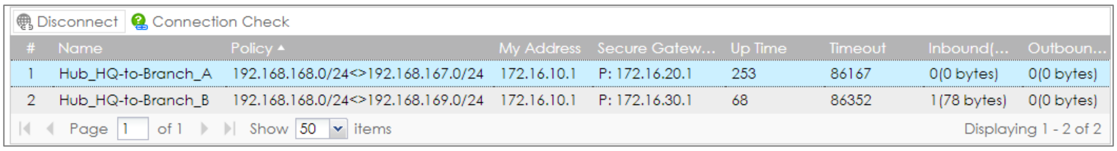
IP Address: 192.168.167.1



Result

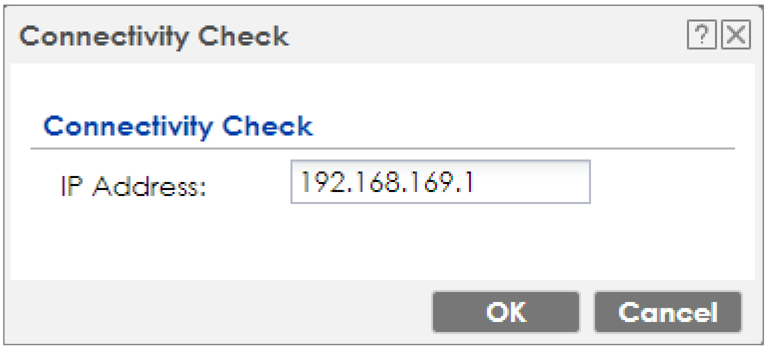
ICMP Connectivity Check PASS on Hub_HQ-to-Branch_A

Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_B



#	Name	Policy ▲	My Address	Secure Gatew...	Up Time	Timeout	Inbound(...	Outboun...
1	Hub_HQ-to-Branch_A	192.168.168.0/24<>192.168.167.0/24	172.16.10.1	P: 172.16.20.1	253	86167	0(0 bytes)	0(0 bytes)
2	Hub_HQ-to-Branch_B	192.168.168.0/24<>192.168.169.0/24	172.16.10.1	P: 172.16.30.1	68	86352	1(78 bytes)	0(0 bytes)

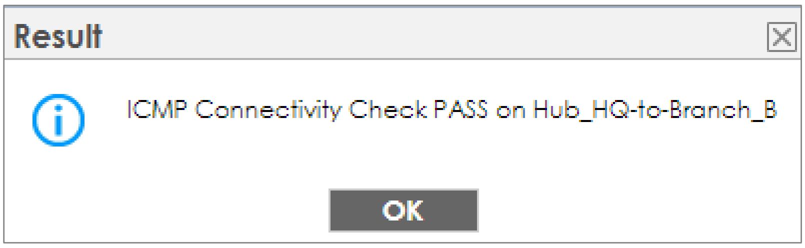
Page 1 of 1 Show 50 items Displaying 1 - 2 of 2



Connectivity Check

Connectivity Check

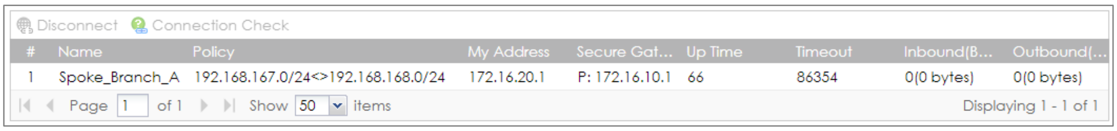
IP Address: 192.168.169.1



Result

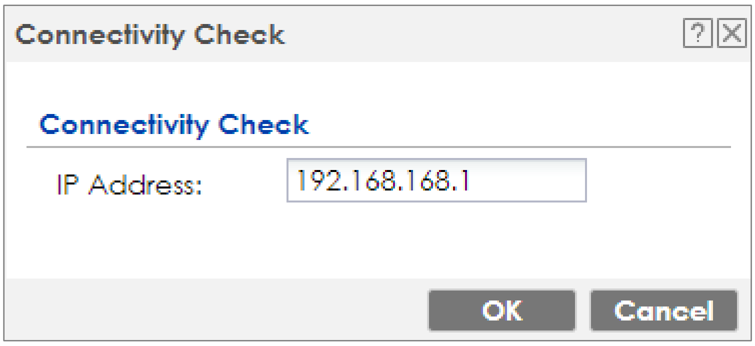
ICMP Connectivity Check PASS on Hub_HQ-to-Branch_B

Spoke_Branch_A > MONITOR > VPN Monitor > IPSec



#	Name	Policy	My Address	Secure Gat...	Up Time	Timeout	Inbound(B...	Outbound(...
1	Spoke_Branch_A	192.168.167.0/24<>192.168.168.0/24	172.16.20.1	P: 172.16.10.1	66	86354	0(0 bytes)	0(0 bytes)

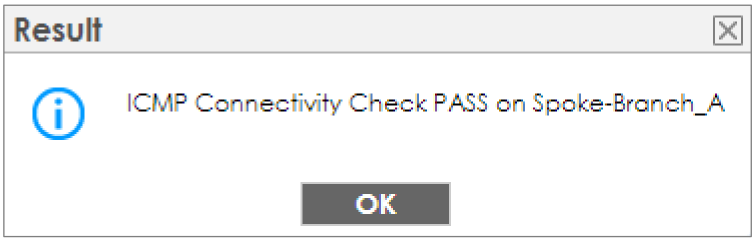
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1



Connectivity Check

Connectivity Check

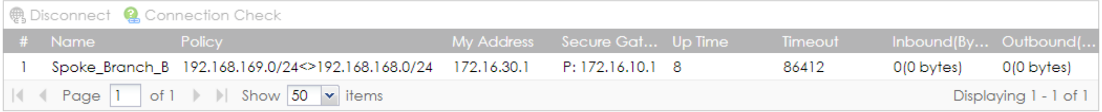
IP Address: 192.168.168.1



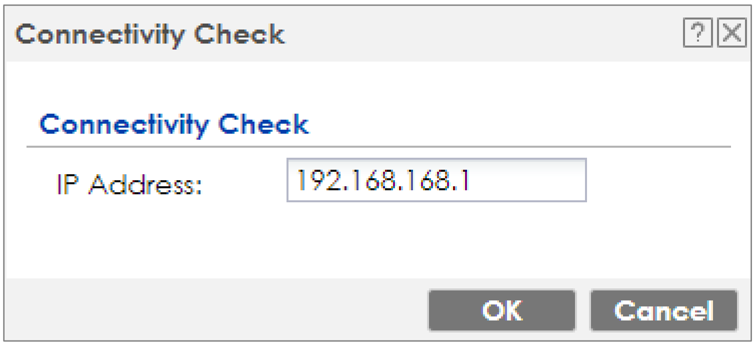
Result

ICMP Connectivity Check PASS on Spoke-Branch_A

Spoke_Branch_B > MONITOR > VPN Monitor > IPSec



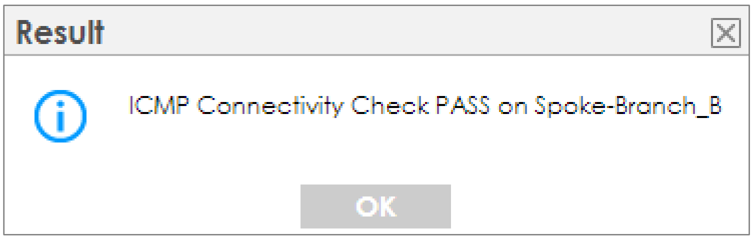
#	Name	Policy	My Address	Secure Gat...	Up Time	Timeout	Inbound(By...	Outbound(...
1	Spoke_Branch_B	192.168.169.0/24<>192.168.168.0/24	172.16.30.1	P: 172.16.10.1	8	86412	0(0 bytes)	0(0 bytes)



Connectivity Check

Connectivity Check

IP Address: 192.168.168.1

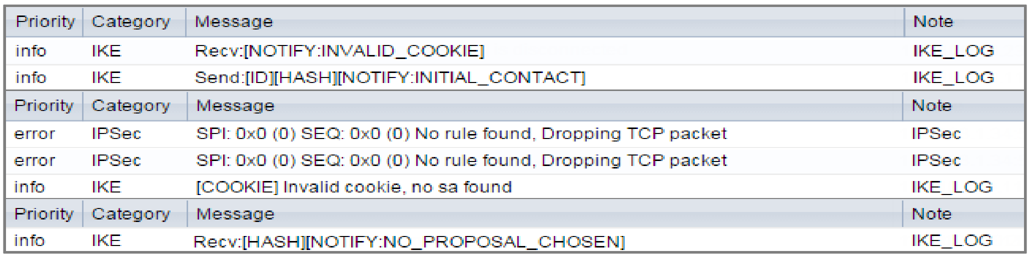


Result

ICMP Connectivity Check PASS on Spoke-Branch_B

What Could Go Wrong?

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. All ZyWALL/USG units must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

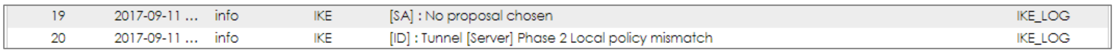


Priority	Category	Message	Note
info	IKE	Recv:[NOTIFY:INVALID_COOKIE]	IKE_LOG
info	IKE	Send:[ID][HASH][NOTIFY:INITIAL_CONTACT]	IKE_LOG

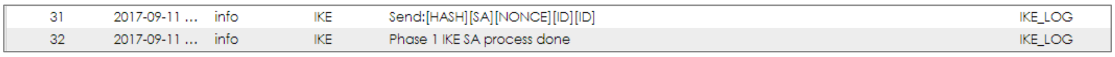
Priority	Category	Message	Note
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
info	IKE	[COOKIE] Invalid cookie, no sa found	IKE_LOG

Priority	Category	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG

If you see that Phase 1 IKE SA process done but still get [info] log message as below, please check ZyWALL/USG and SonicWALL Phase 2 Settings. All ZyWALL/USG units must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.



19	2017-09-11 ...	info	IKE	[SA] : No proposal chosen	IKE_LOG
20	2017-09-11 ...	info	IKE	[ID] : Tunnel [Server] Phase 2 Local policy mismatch	IKE_LOG



31	2017-09-11 ...	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

Make sure the all ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

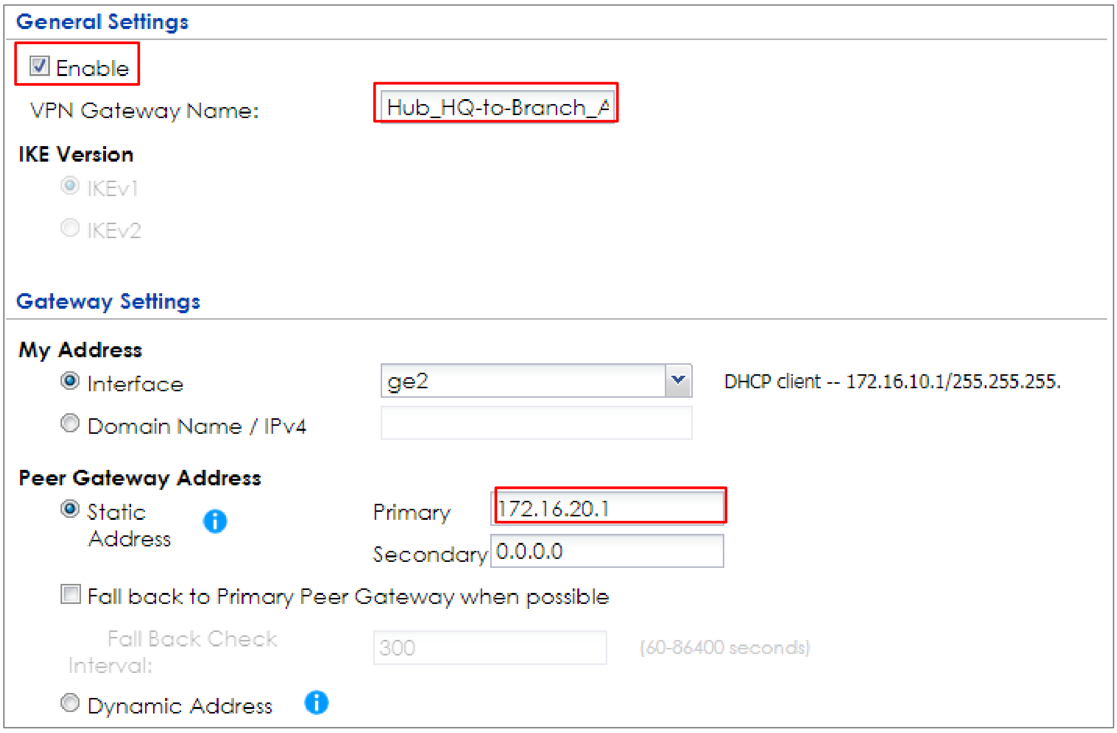
By default, NAT traversal is enabled on ZyWALL/USG, so please make sure the remote IPSec device also has NAT traversal enabled.

Set Up the IPSec VPN Tunnel of ZyWALL/USG without Using VPN Concentrator Hub_HQ-to-Branch_A

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Secure Gateway** IP as the **Branch A**'s Gateway IP address (in the example, 172.16.20.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch A**'s Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway



General Settings

☑ Enable

VPN Gateway Name: Hub_HQ-to-Branch_A

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface ge2 DHCP client -- 172.16.10.1/255.255.255.

○ Domain Name / IPv4

Peer Gateway Address

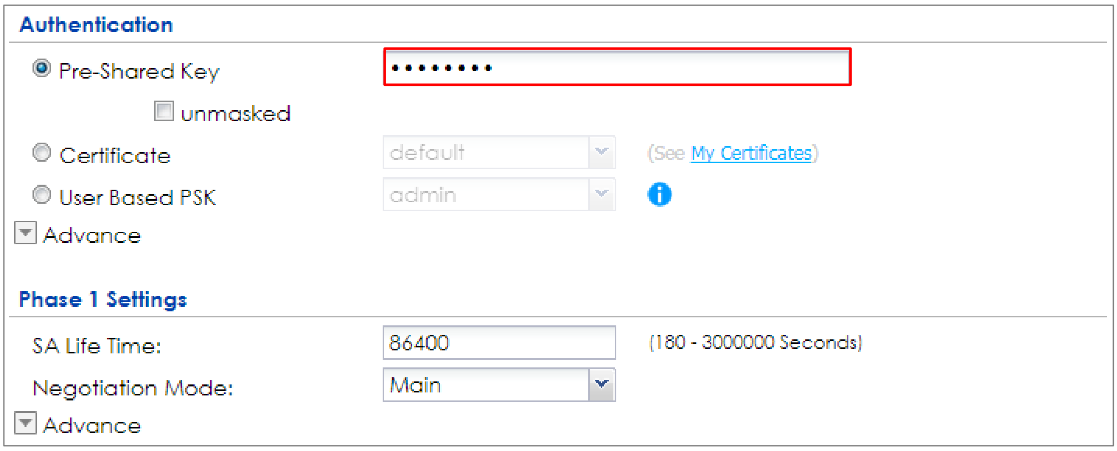
● Static Address Primary 172.16.20.1

Secondary 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

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

○ Dynamic Address



Authentication

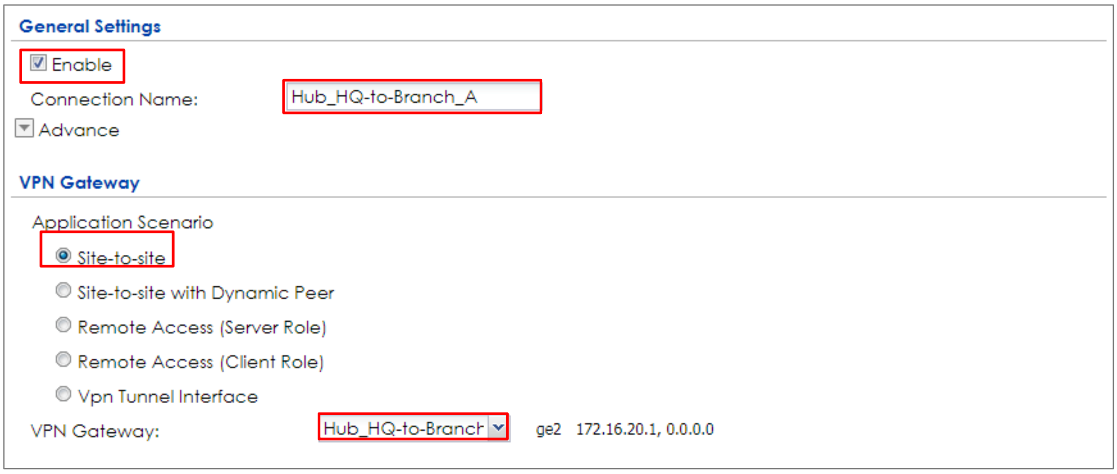
● Pre-Shared Key: •••••••••
□ unmasked
○ Certificate: default (See My Certificates)
○ User Based PSK: admin
Advance

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)
Negotiation Mode: Main
Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



General Settings

☑ Enable
Connection Name: Hub_HQ-to-Branch_A
Advance

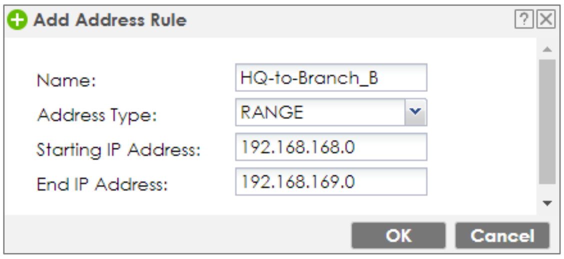
VPN Gateway

Application Scenario
● Site-to-site
○ Site-to-site with Dynamic Peer
○ Remote Access (Server Role)
○ Remote Access (Client Role)
○ Vpn Tunnel Interface
VPN Gateway: Hub_HQ-to-Branch ge2 172.16.20.1, 0.0.0.0

Click **Create new Object** on the upper bar to add the address range of the local network behind **Hub_HQ** to **Branch_B** and an address of local network behind **Branch A**.

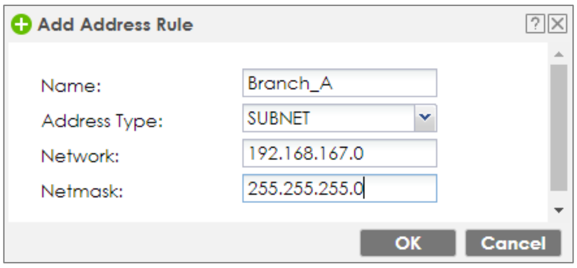
CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy


Add Address Rule

Name: HQ-to-Branch_B
Address Type: RANGE
Starting IP Address: 192.168.168.0
End IP Address: 192.168.169.0

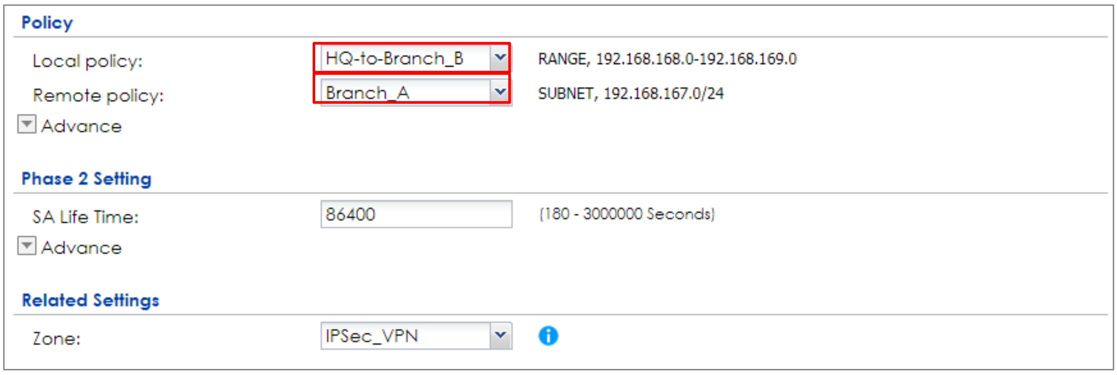
Remote Policy


Add Address Rule

Name: Branch_A
Address Type: SUBNET
Network: 192.168.167.0
Netmask: 255.255.255.0

Set **Local Policy** to be **HQ-to-Branch_B** and **Remote Policy** to **Branch_A** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy


Policy

Local policy: HQ-to-Branch_B RANGE, 192.168.168.0-192.168.169.0
Remote policy: Branch_A SUBNET, 192.168.167.0/24
Advance

Phase 2 Setting

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

Related Settings

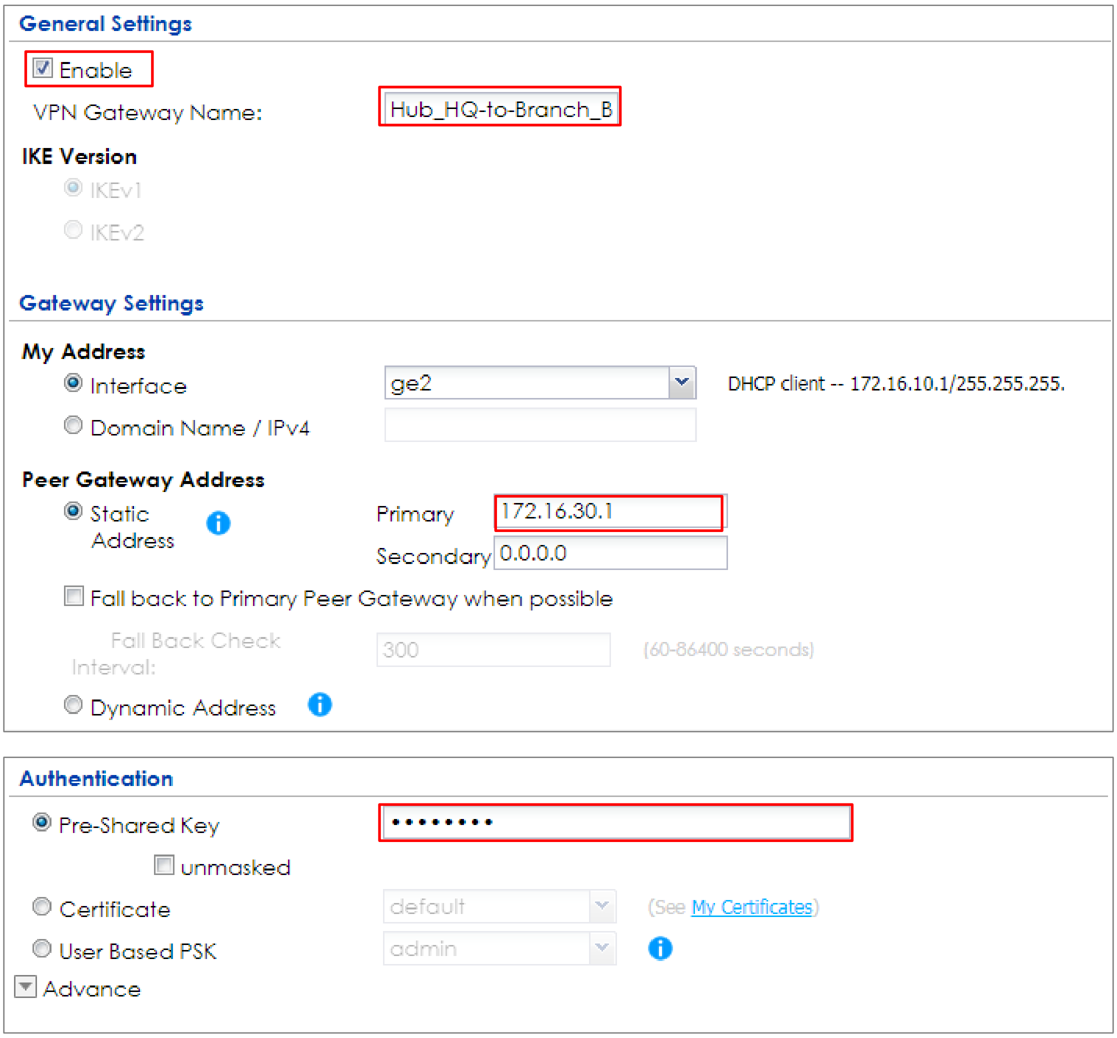
Zone: IPSec_VPN

Hub_HQ-to-Branch_B

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Secure Gateway** IP as the **Branch B**'s Gateway IP address (in the example, 172.16.30.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch B**'s Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway



General Settings

☑ Enable

VPN Gateway Name: Hub_HQ-to-Branch_B

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface: ge2 — DHCP client -- 172.16.10.1/255.255.255.

○ Domain Name / IPv4

Peer Gateway Address

● Static Address — Primary: 172.16.30.1 — 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

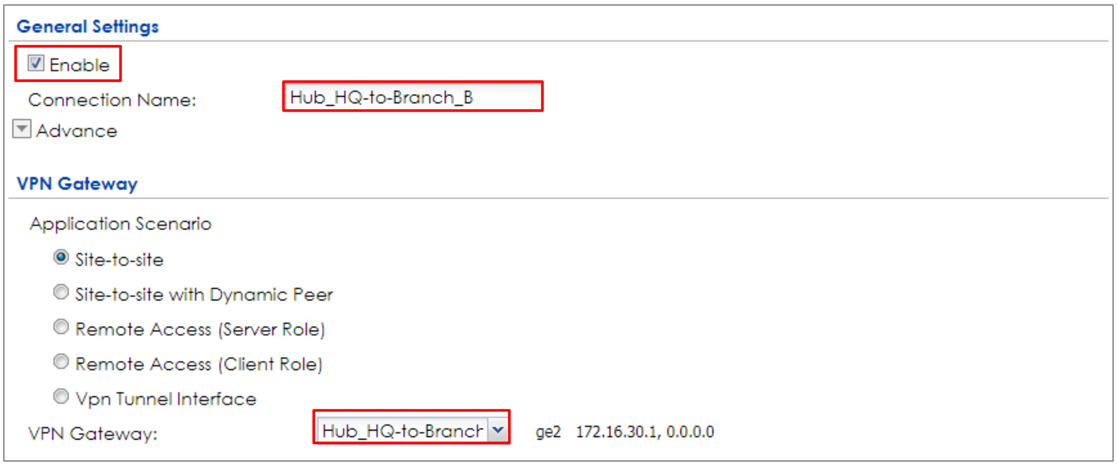
○ Certificate: default (See My Certificates)

○ User Based PSK: admin

Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



General Settings

☑ Enable

Connection Name: Hub_HQ-to-Branch_B

Advance

VPN Gateway

Application Scenario

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

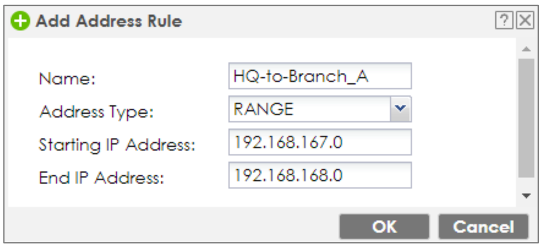
○ Vpn Tunnel Interface

VPN Gateway: Hub_HQ-to-Branch ge2 172.16.30.1, 0.0.0.0

Click **Create new Object** on the upper bar to add the address range of the local network behind **Hub_HQ** to **Branch_A** and an address of local network behind **Branch B**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

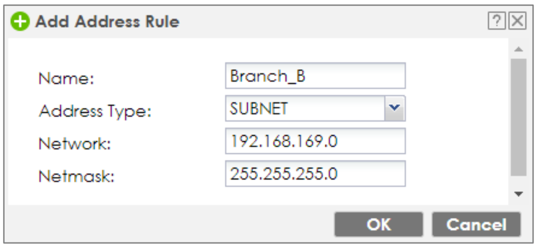
Local Policy



Add Address Rule

Name: HQ-to-Branch_A
Address Type: RANGE
Starting IP Address: 192.168.167.0
End IP Address: 192.168.168.0

Remote Policy

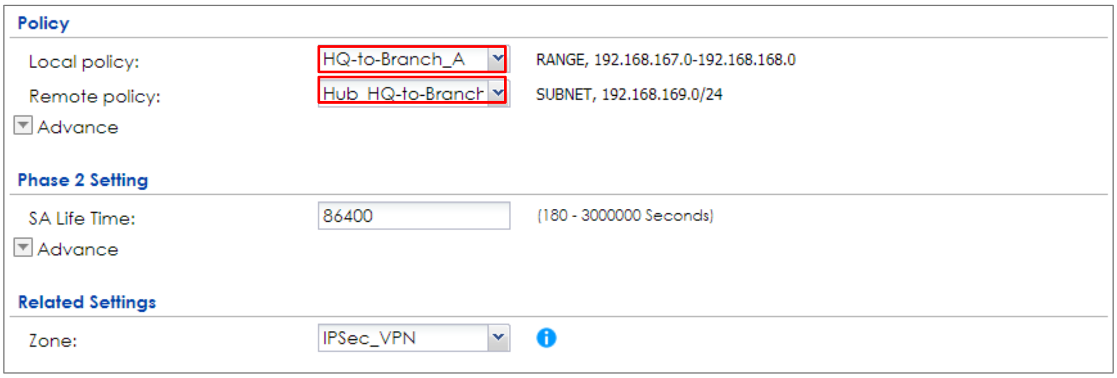


Add Address Rule

Name: Branch_B
Address Type: SUBNET
Network: 192.168.169.0
Netmask: 255.255.255.0

Set **Local Policy** to be **HQ-to-Branch_B** and **Remote Policy** to **Branch_B** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



Policy

Local policy: HQ-to-Branch_A RANGE, 192.168.167.0-192.168.168.0
Remote policy: Hub_HQ-to-Branch SUBNET, 192.168.169.0/24

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

Related Settings

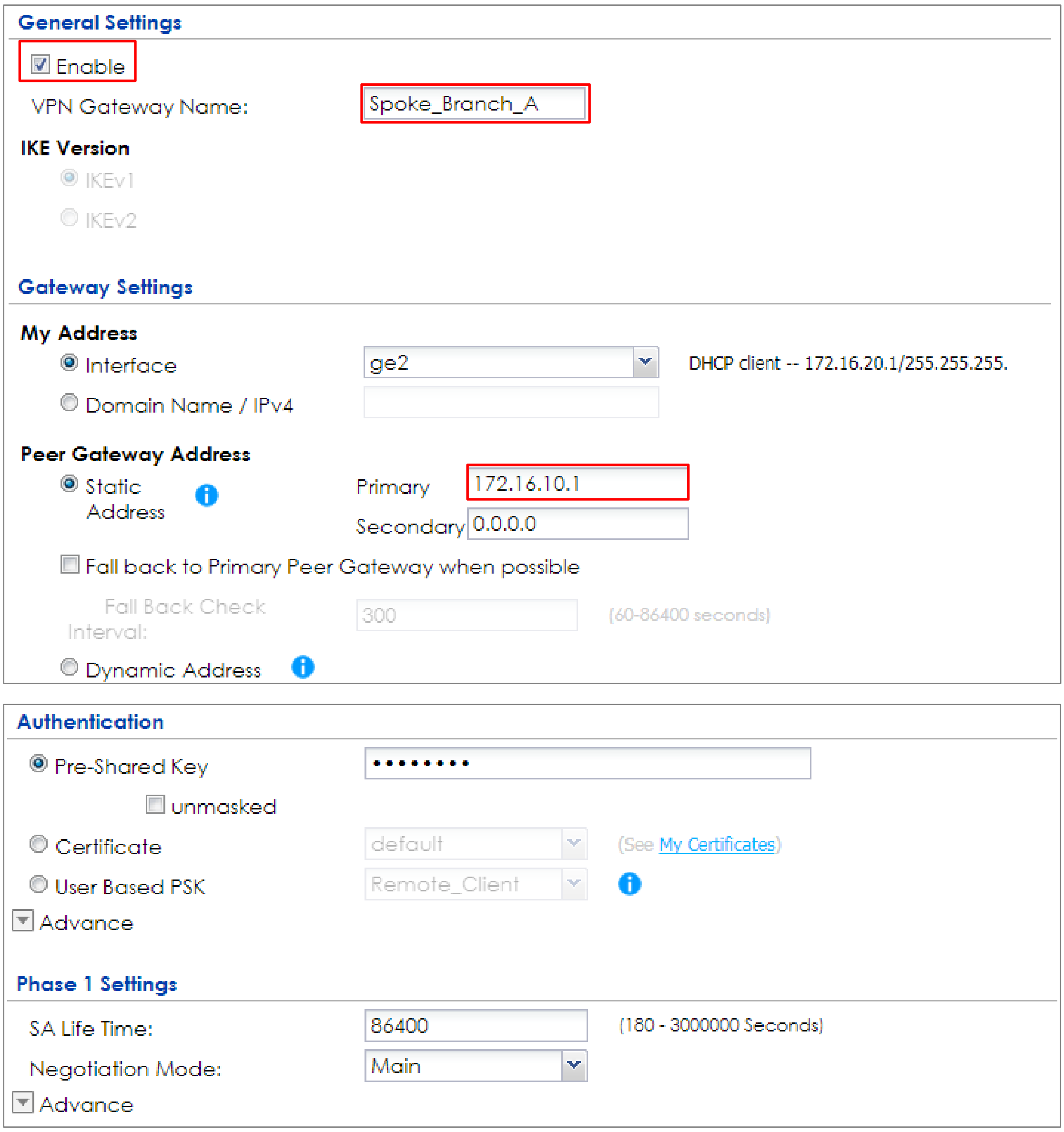
Zone: IPSec_VPN

Spoke_Branch_A

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Secure Gateway** IP as the **Hub_HQ**'s Gateway IP address (in the example, 172.16.10.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ**'s Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway



General Settings

☑ Enable

VPN Gateway Name: Spoke_Branch_A

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface ge2 DHCP client -- 172.16.20.1/255.255.255.

○ Domain Name / IPv4

Peer Gateway Address

● Static Address Primary 172.16.10.1

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 default (See My Certificates)

○ User Based PSK Remote_Client

Advance

Phase 1 Settings

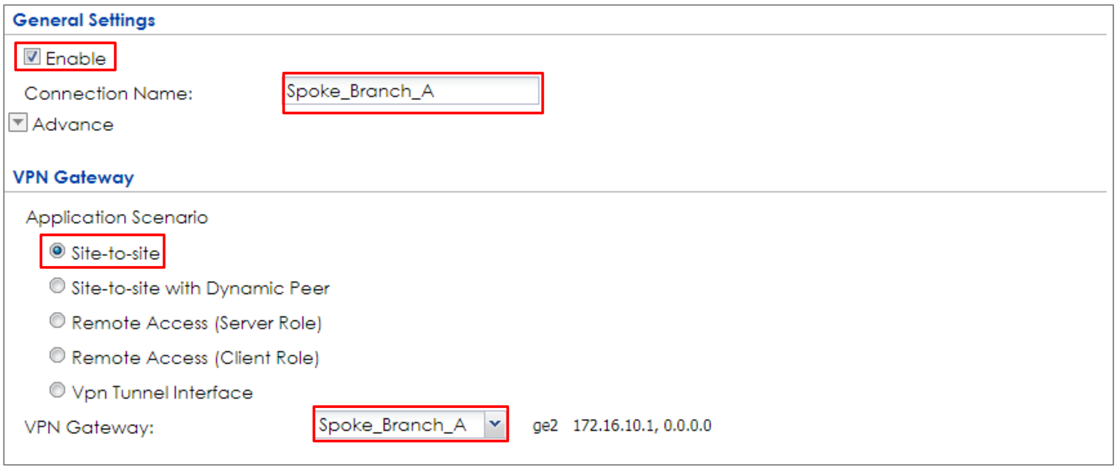
SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



General Settings

☑ Enable

Connection Name: Spoke_Branch_A

Advance

VPN Gateway

Application Scenario

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

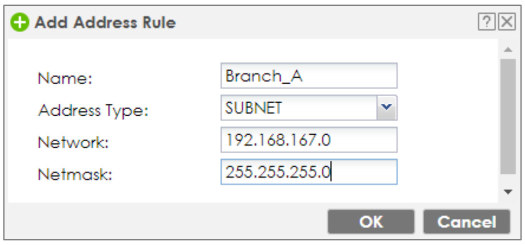
○ Remote Access (Client Role)

○ Vpn Tunnel Interface

VPN Gateway: Spoke_Branch_A ge2 172.16.10.1, 0.0.0.0

Click **Create new Object** on the upper bar to add the address of the local network behind **Branch A** and **the** address range of the local network behind **Hub_HQ** to **Branch_B**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object Local Policy



Add Address Rule

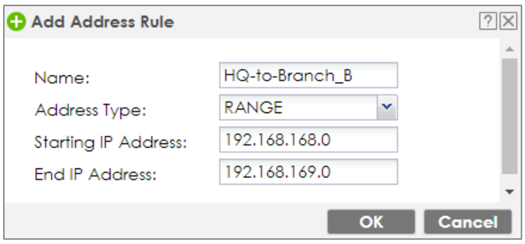
Name: Branch_A

Address Type: SUBNET

Network: 192.168.167.0

Netmask: 255.255.255.0

Remote Policy

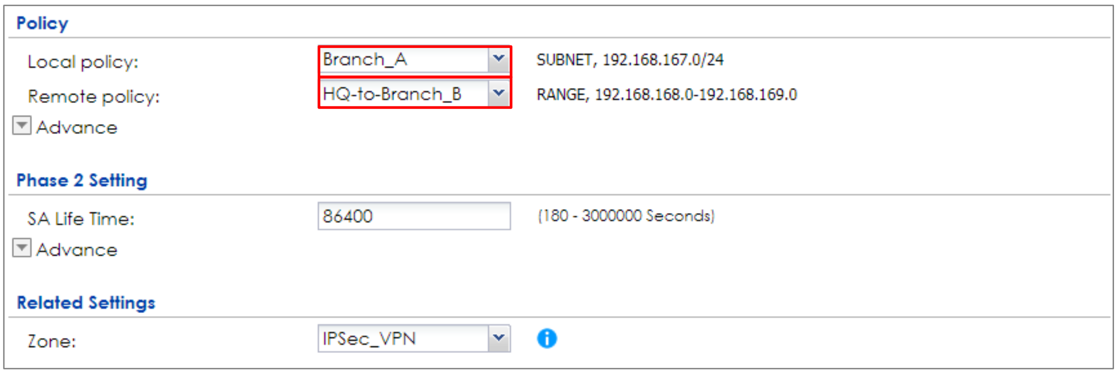


Add Address Rule

Name:	HQ-to-Branch_B
Address Type:	RANGE
Starting IP Address:	192.168.168.0
End IP Address:	192.168.169.0

Set **Local Policy** to be **Branch_A** and **Remote Policy** to **HQ-to-Branch_B** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



Policy

Local policy:	Branch_A	SUBNET, 192.168.167.0/24
Remote policy:	HQ-to-Branch_B	RANGE, 192.168.168.0-192.168.169.0

Phase 2 Setting

SA Life Time:	86400	(180 - 3000000 Seconds)

Related Settings

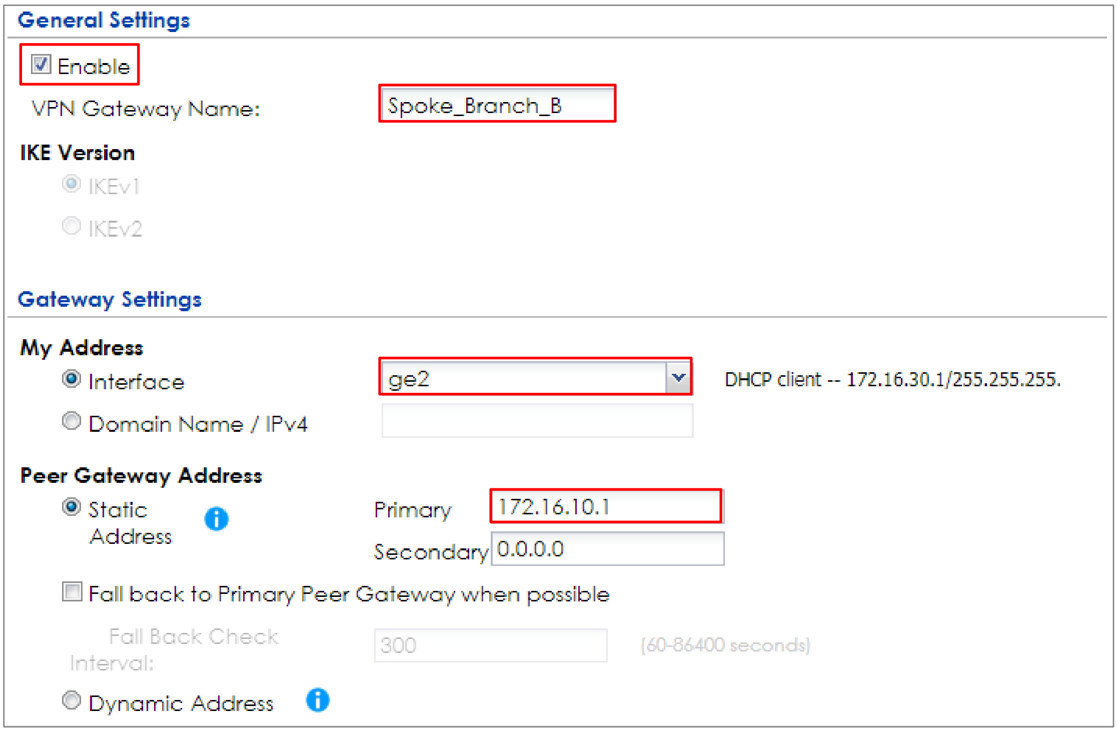
Zone:	IPSec_VPN

Spoke_Branch_B

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Secure Gateway** IP as the **Hub_HQ**'s Gateway IP address (in the example, 172.16.10.1). Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ**'s Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway



General Settings

☑ Enable

VPN Gateway Name: Spoke_Branch_B

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface: ge2 — DHCP client -- 172.16.30.1/255.255.255.

○ Domain Name / IPv4

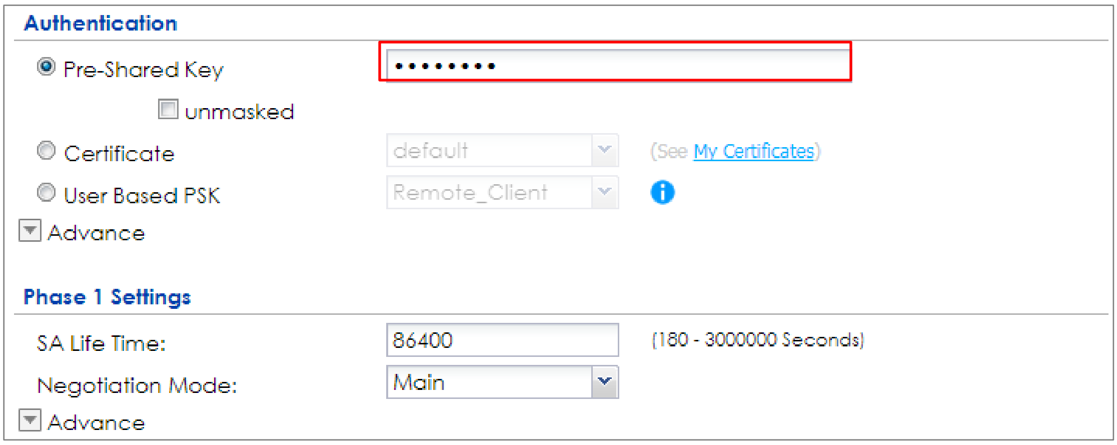
Peer Gateway Address

● Static Address — Primary: 172.16.10.1 — 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: default (See My Certificates)

○ User Based PSK: Remote_Client

Advance

Phase 1 Settings

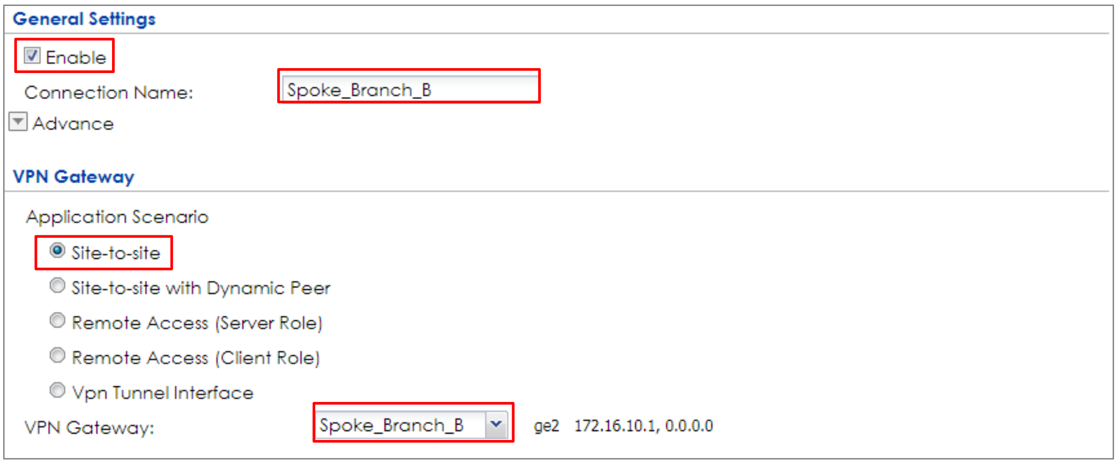
SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



General Settings

☑ Enable

Connection Name: Spoke_Branch_B

Advance

VPN Gateway

Application Scenario

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

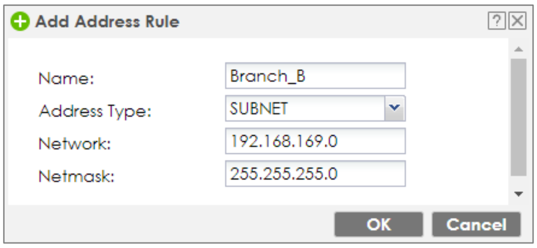
○ Vpn Tunnel Interface

VPN Gateway: Spoke_Branch_B ge2 172.16.10.1, 0.0.0.0

Click **Create new Object** on the upper bar to add the address of local network behind **Branch B** and address range of local network behind **Hub_HQ** to **Branch_A**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy



Add Address Rule

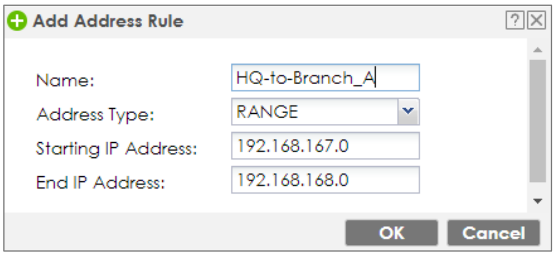
Name: Branch_B

Address Type: SUBNET

Network: 192.168.169.0

Netmask: 255.255.255.0

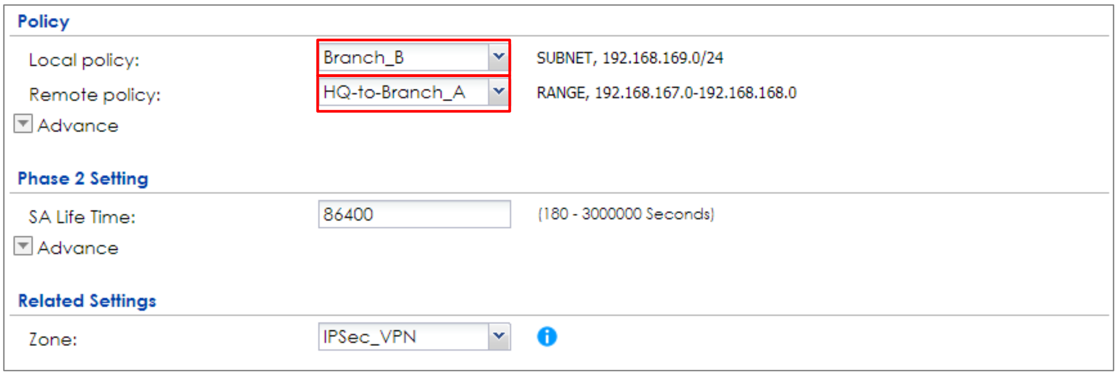
Remote Policy



Name:	HQ-to-Branch_A
Address Type:	RANGE
Starting IP Address:	192.168.167.0
End IP Address:	192.168.168.0

Set **Local Policy** to be **Branch_B** and **Remote Policy** to **HQ-to-Branch_A** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



Policy

Local policy:	Branch_B	SUBNET, 192.168.169.0/24
Remote policy:	HQ-to-Branch_A	RANGE, 192.168.167.0-192.168.168.0

Phase 2 Setting

SA Life Time:	86400	(180 - 3000000 Seconds)

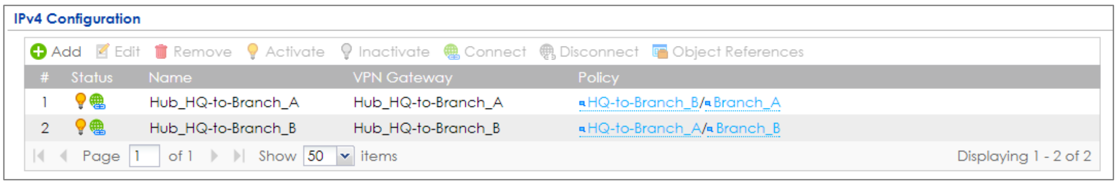
Related Settings

Zone:	IPSec_VPN

Test the IPSec VPN Tunnel

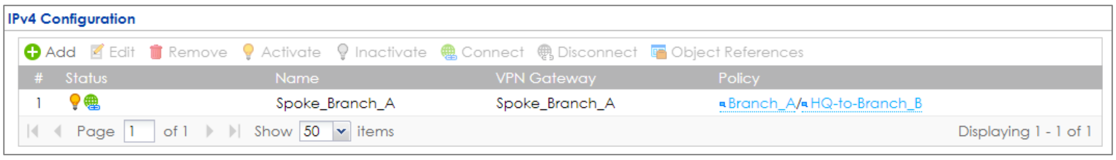
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

Hub_HQ > CONFIGURATION > VPN > IPSec VPN > VPN Connection



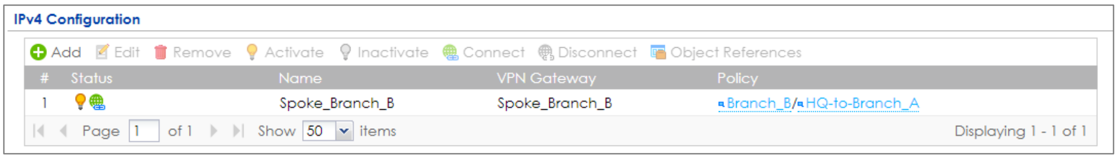
#	Status	Name	VPN Gateway	Policy
1		Hub_HQ-to-Branch_A	Hub_HQ-to-Branch_A	HQ-to-Branch_B/Branch_A
2		Hub_HQ-to-Branch_B	Hub_HQ-to-Branch_B	HQ-to-Branch_A/Branch_B

Spoke_Branch_A > CONFIGURATION > VPN > IPSec VPN > VPN Connection



#	Status	Name	VPN Gateway	Policy
1		Spoke_Branch_A	Spoke_Branch_A	Branch_A/HQ-to-Branch_B

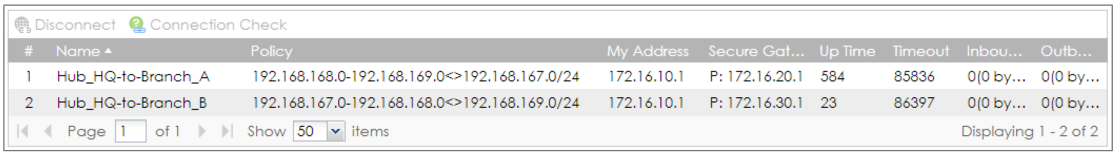
Spoke_Branch_B > CONFIGURATION > VPN > IPSec VPN > VPN Connection



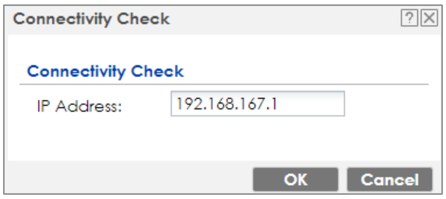
#	Status	Name	VPN Gateway	Policy
1		Spoke_Branch_B	Spoke_Branch_B	Branch_B/HQ-to-Branch_A

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

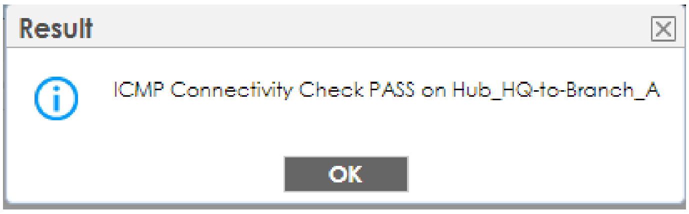
Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_A



#	Name ▲	Policy	My Address	Secure Gat...	Up Time	Timeout	Inbou...	Outb...
1	Hub_HQ-to-Branch_A	192.168.168.0-192.168.169.0<>192.168.167.0/24	172.16.10.1	P: 172.16.20.1	584	85836	0(0 by...	0(0 by...
2	Hub_HQ-to-Branch_B	192.168.167.0-192.168.168.0<>192.168.169.0/24	172.16.10.1	P: 172.16.30.1	23	86397	0(0 by...	0(0 by...



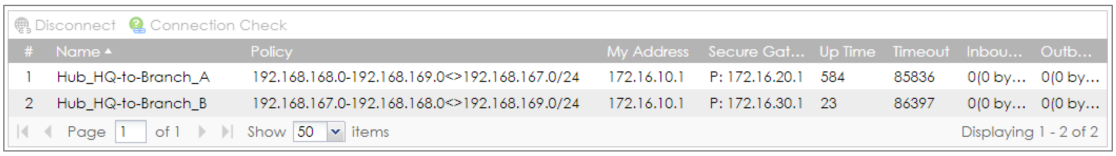
IP Address: 192.168.167.1



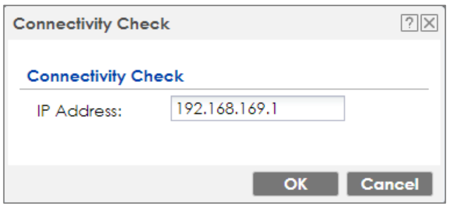
Result

ICMP Connectivity Check PASS on Hub_HQ-to-Branch_A

Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_B



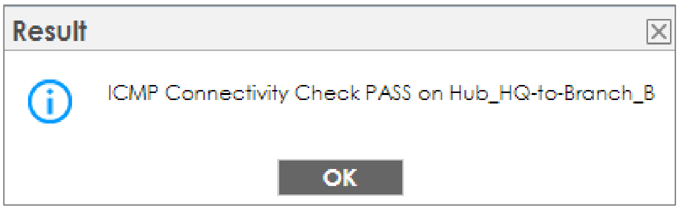
#	Name ▴	Policy	My Address	Secure Gat...	Up Time	Timeout	Inbou...	Outb...
1	Hub_HQ-to-Branch_A	192.168.168.0-192.168.169.0<>192.168.167.0/24	172.16.10.1	P: 172.16.20.1	584	85836	0(0 by...	0(0 by...
2	Hub_HQ-to-Branch_B	192.168.167.0-192.168.168.0<>192.168.169.0/24	172.16.10.1	P: 172.16.30.1	23	86397	0(0 by...	0(0 by...



Connectivity Check

Connectivity Check

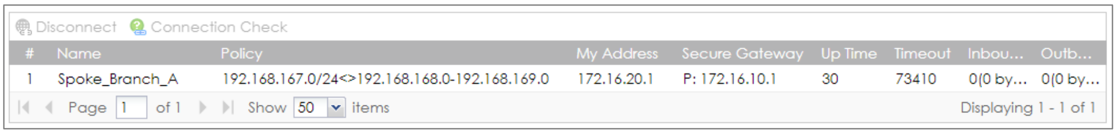
IP Address: 192.168.169.1



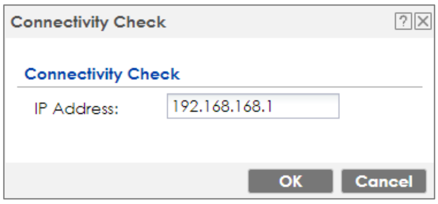
Result

ICMP Connectivity Check PASS on Hub_HQ-to-Branch_B

Spoke_Branch_A > MONITOR > VPN Monitor > IPSec



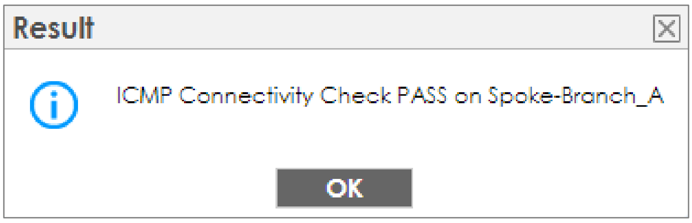
#	Name	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbou...	Outb...
1	Spoke_Branch_A	192.168.167.0/24<>192.168.168.0-192.168.169.0	172.16.20.1	P: 172.16.10.1	30	73410	0(0 by...	0(0 by...



Connectivity Check

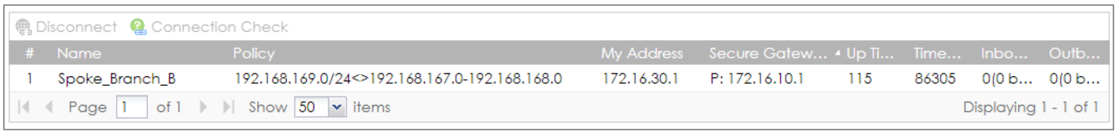
Connectivity Check

IP Address: 192.168.168.1

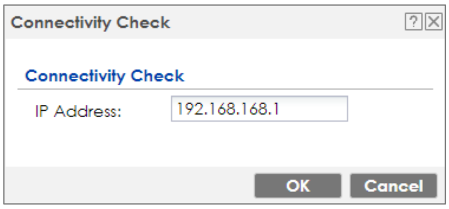


ICMP Connectivity Check PASS on Spoke-Branch_A

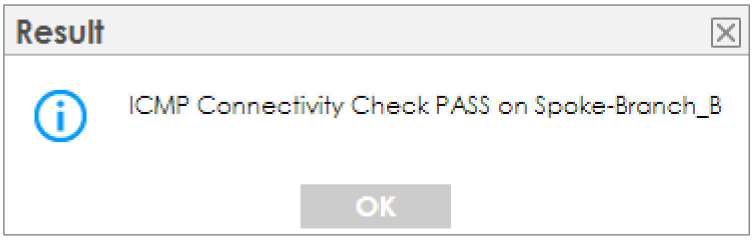
Spoke_Branch_B > MONITOR > VPN Monitor > IPSec



#	Name	Policy	My Address	Secure Gatew...	Up Ti...	Time...	Inbo...	Outb...
1	Spoke_Branch_B	192.168.169.0/24<>192.168.167.0-192.168.168.0	172.16.30.1	P: 172.16.10.1	115	86305	0(0 b...	0(0 b...



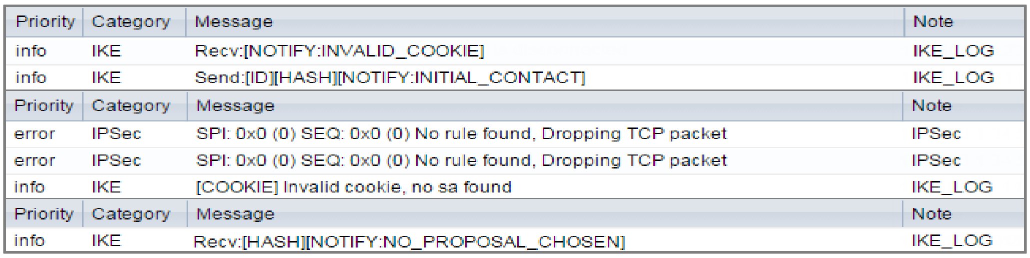
IP Address: 192.168.168.1



ICMP Connectivity Check PASS on Spoke-Branch_B

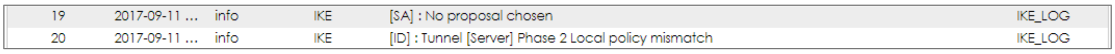
What Could Go Wrong?

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. All ZyWALL/USG units must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

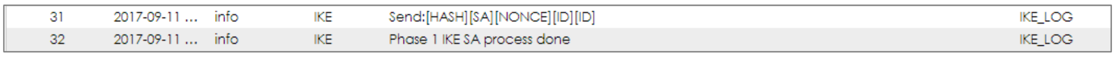


```
Priority  Category  Message                                                      Note
info      IKE       Recv:[NOTIFY:INVALID_COOKIE]                                 IKE_LOG
info      IKE       Send:[ID][HASH][NOTIFY:INITIAL_CONTACT]                      IKE_LOG
Priority  Category  Message                                                      Note
error     IPSec     SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet  IPSec
error     IPSec     SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet  IPSec
info      IKE       [COOKIE] Invalid cookie, no sa found                         IKE_LOG
Priority  Category  Message                                                      Note
info      IKE       Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]                       IKE_LOG
```

If you see that Phase 1 IKE SA process done but still get [info] log message as below, please check ZyWALL/USG and SonicWALL Phase 2 Settings. All ZyWALL/USG units must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.



```
19   2017-09-11 ...   info   IKE   [SA] : No proposal chosen                            IKE_LOG
20   2017-09-11 ...   info   IKE   [ID] : Tunnel [Server] Phase 2 Local policy mismatch  IKE_LOG
```



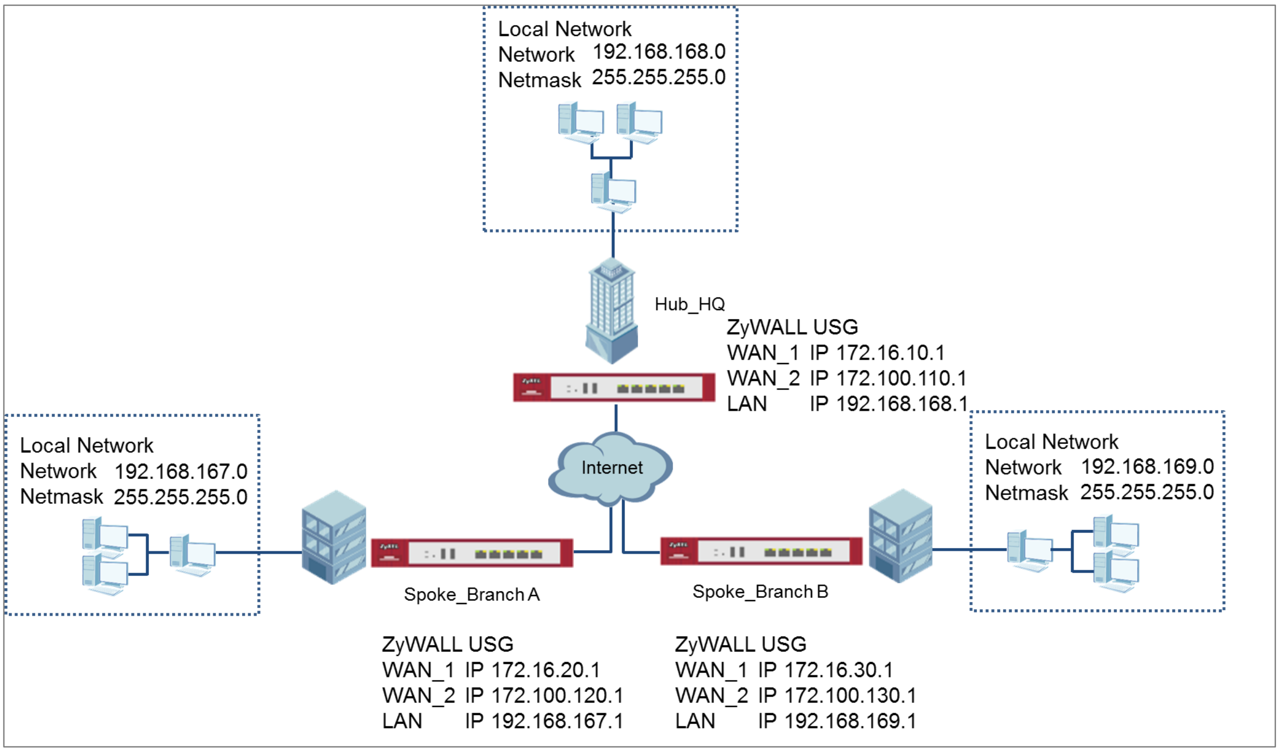
```
31   2017-09-11 ...   info   IKE   Send:[HASH][SA][NONCE][ID][ID]   IKE_LOG
32   2017-09-11 ...   info   IKE   Phase 1 IKE SA process done      IKE_LOG
```

Make sure the all ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

By default, NAT traversal is enabled on ZyWALL/USG, so please make sure the remote IPSec device also has NAT traversal enabled.

How to Use Dual-WAN to Perform Fail-Over on VPN Using the VPN Concentrator

This is an example of using Dual-WAN to perform fail-over on a hub-and-spoke VPN with the HQ ZyWALL/USG as the hub and spoke VPNs to Branches A and B. When the VPN tunnel is configured, traffic passes between branches via the hub (HQ). Traffic can also pass between spoke-and-spoke through the hub. If the primary WAN interface is unavailable, the backup WAN interface will be used. When the primary WAN interface is available again, traffic will use that interface again.



Hub & Spoken VPN Using the VPN Concentrator with Backup WAN

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

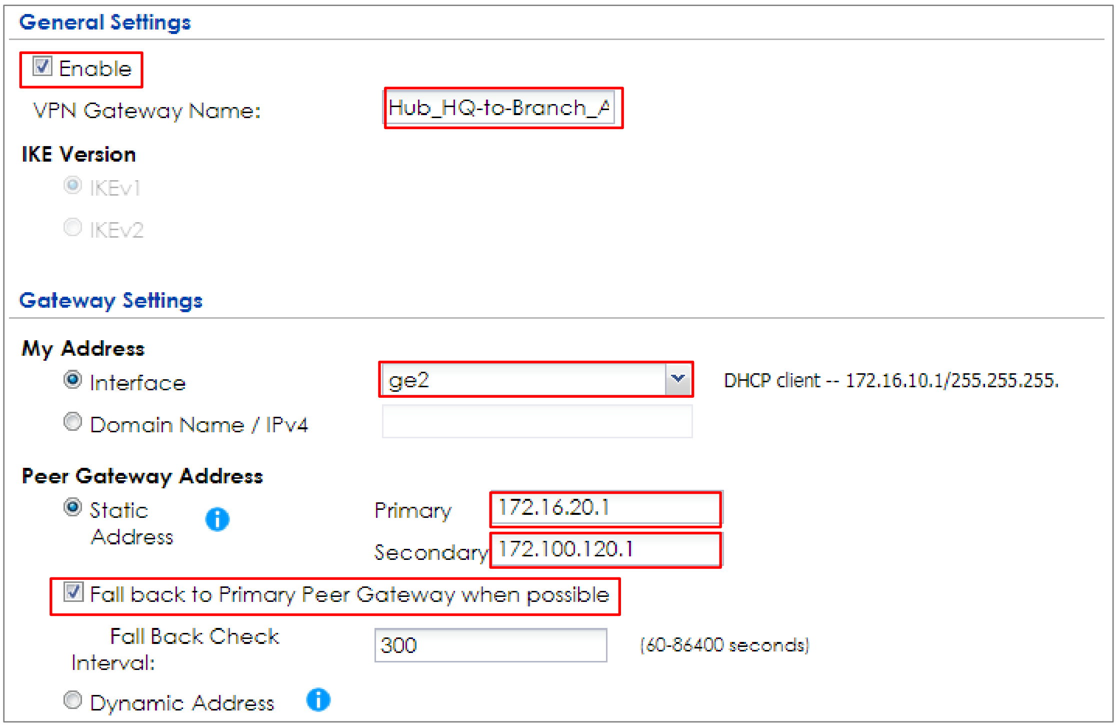
Set Up the IPSec VPN Tunnel on the ZyWALL/USG Hub_HQ-to-Branch_A

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Primary** Gateway IP as the **Branch A**’s **wan1** IP address (in the example, 172.16.20.1) and **Secondary** Gateway IP as the **Branch A**’s **wan2** IP address (in the example, 172.100.120.1). Select **Fall back to Primary Peer Gateway when possible** and set desired **Fall Back Check Interval** time.

Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch A**’s Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway



General Settings

☑ Enable

VPN Gateway Name: Hub_HQ-to-Branch_A

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface: ge2 — DHCP client -- 172.16.10.1/255.255.255.

○ Domain Name / IPv4

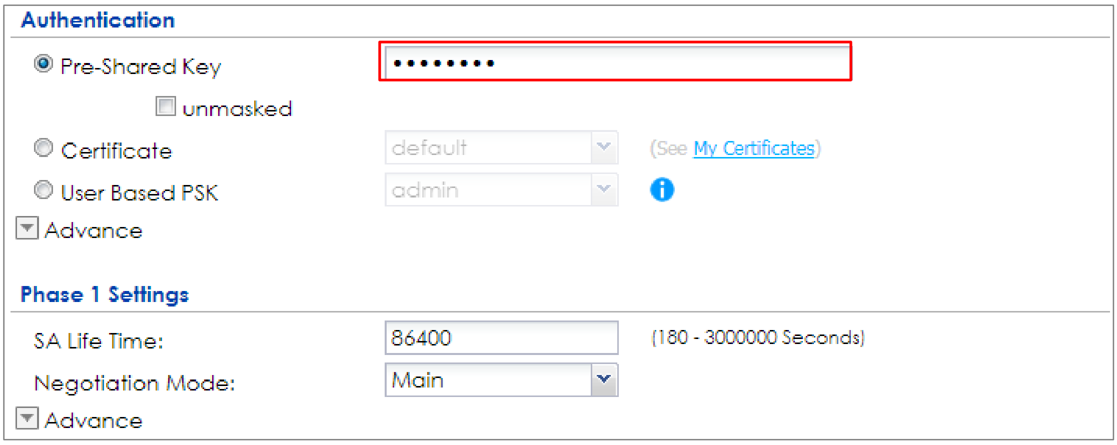
Peer Gateway Address

● Static Address — Primary: 172.16.20.1 — Secondary: 172.100.120.1

☑ 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)

○ User Based PSK admin

Advance

Phase 1 Settings

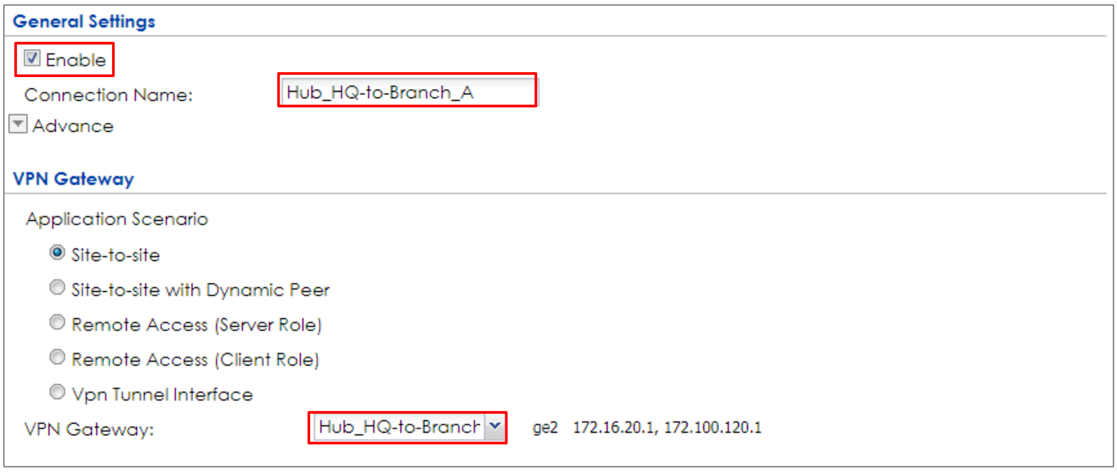
SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



General Settings

☑ Enable

Connection Name: Hub_HQ-to-Branch_A

Advance

VPN Gateway

Application Scenario

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

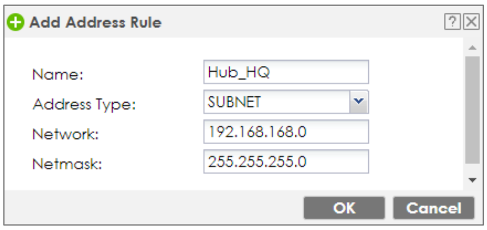
○ Vpn Tunnel Interface

VPN Gateway: Hub_HQ-to-Branch ge2 172.16.20.1, 172.100.120.1

Click **Create new Object** to add the address of local network behind **Hub_HQ** and an address of local network behind **Branch A**.

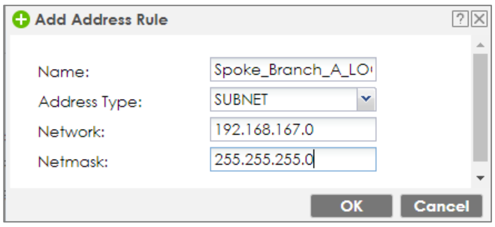
CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy



Name: Hub_HQ
Address Type: SUBNET
Network: 192.168.168.0
Netmask: 255.255.255.0

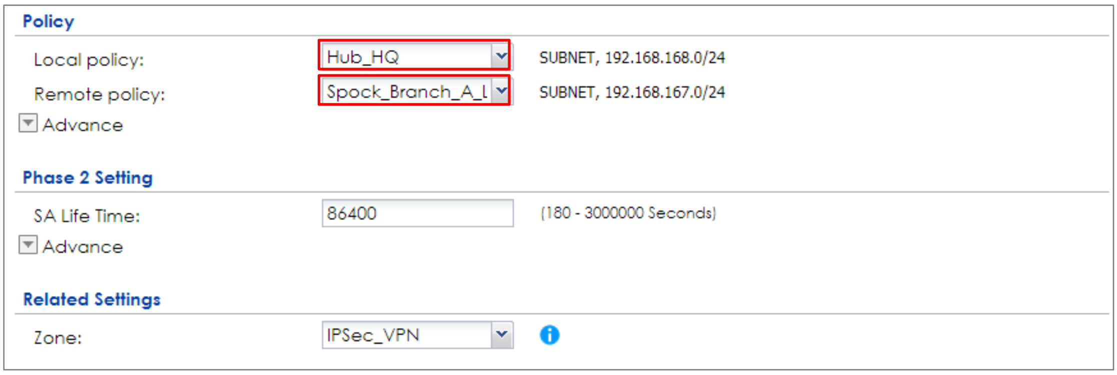
Remote Policy



Name: Spoke_Branch_A_LO
Address Type: SUBNET
Network: 192.168.167.0
Netmask: 255.255.255.0

Set **Local Policy** to be **Hub_HQ** and **Remote Policy** to **Branch_A** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



Policy

Local policy: Hub_HQ SUBNET, 192.168.168.0/24
Remote policy: Spock_Branch_A_L SUBNET, 192.168.167.0/24

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

Related Settings

Zone: IPSec_VPN

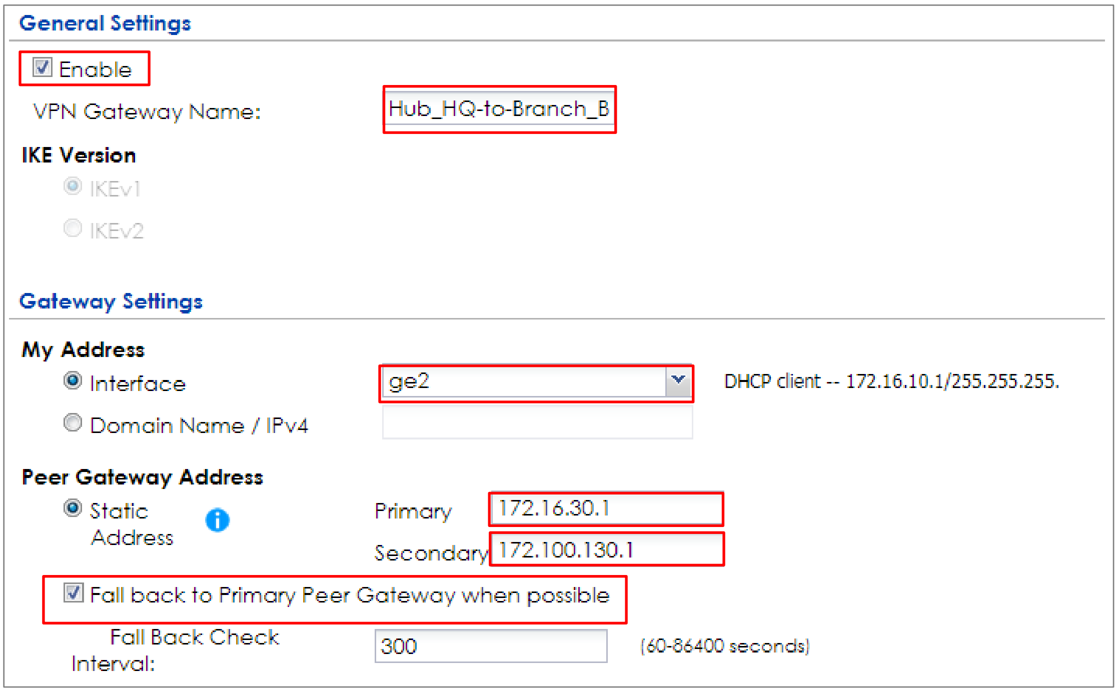
Hub_HQ-to-Branch_B

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Primary** Gateway IP as the **Branch B**'s **wan1** IP address (in the example, 172.16.30.1) and **Secondary** Gateway IP as the **Branch B**'s **wan2** IP address (in the example, 172.100.130.1). Select **Fall back to Primary Peer Gateway when possible** and set desired **Fall Back Check Interval** time.

Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Branch A**'s Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway



General Settings

☑ Enable

VPN Gateway Name: Hub_HQ-to-Branch_B

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface ge2 DHCP client -- 172.16.10.1/255.255.255.

○ Domain Name / IPv4

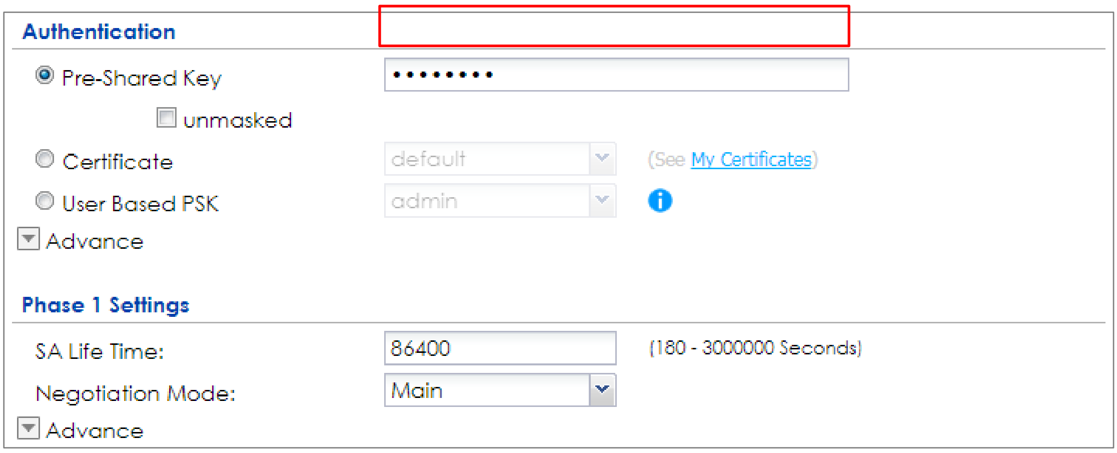
Peer Gateway Address

● Static Address Primary 172.16.30.1

Secondary 172.100.130.1

☑ Fall back to Primary Peer Gateway when possible

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



● Pre-Shared Key ••••••••

□ unmasked

○ Certificate default (See My Certificates)

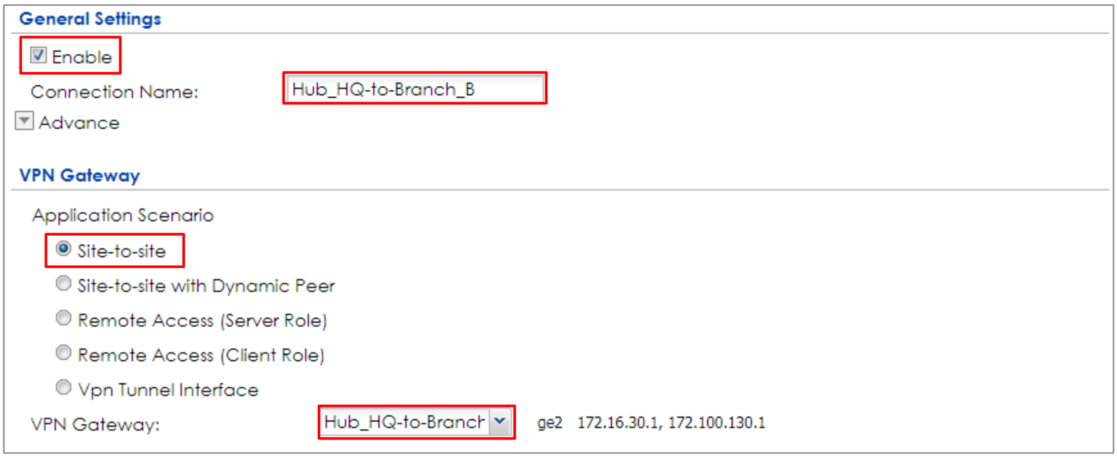
○ User Based PSK admin

SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to enable VPN Connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



☑ Enable

Connection Name: Hub_HQ-to-Branch_B

Application Scenario

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

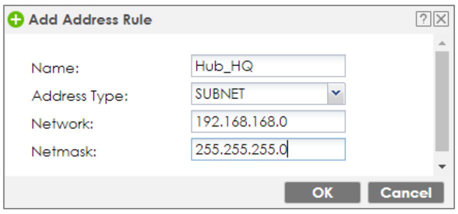
○ Vpn Tunnel Interface

VPN Gateway: Hub_HQ-to-Branch ge2 172.16.30.1, 172.100.130.1

Click **Create new Object** to add an address of local network behind **Hub_HQ** and an address of local network behind **Branch B**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

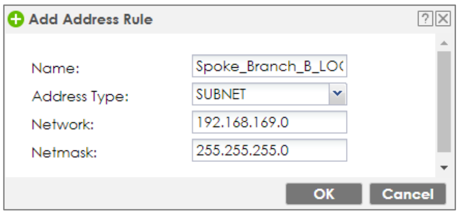
Local Policy



Add Address Rule

Name: Hub_HQ
Address Type: SUBNET
Network: 192.168.168.0
Netmask: 255.255.255.0

Remote Policy

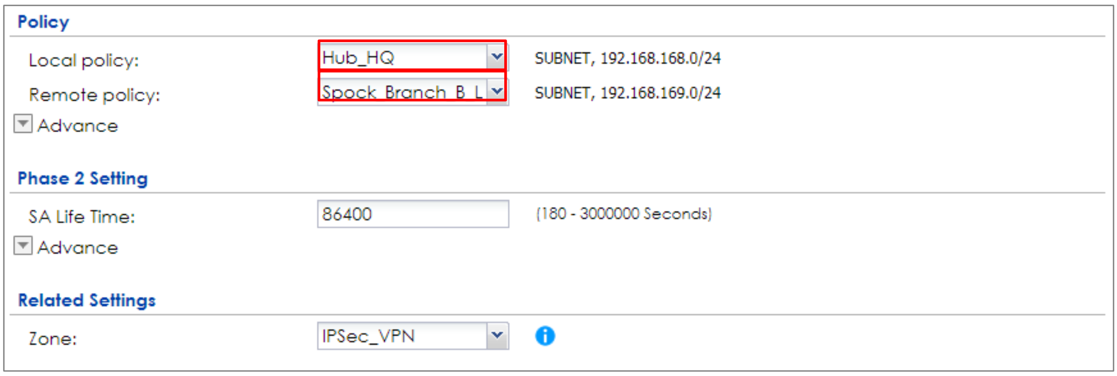


Add Address Rule

Name: Spoke_Branch_B_LO(
Address Type: SUBNET
Network: 192.168.169.0
Netmask: 255.255.255.0

Set **Local Policy** to be **Hub_HQ** and **Remote Policy** to **Branch_B** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



Policy

Local policy: Hub_HQ SUBNET, 192.168.168.0/24
Remote policy: Spock_Branch_B_L SUBNET, 192.168.169.0/24

Phase 2 Setting

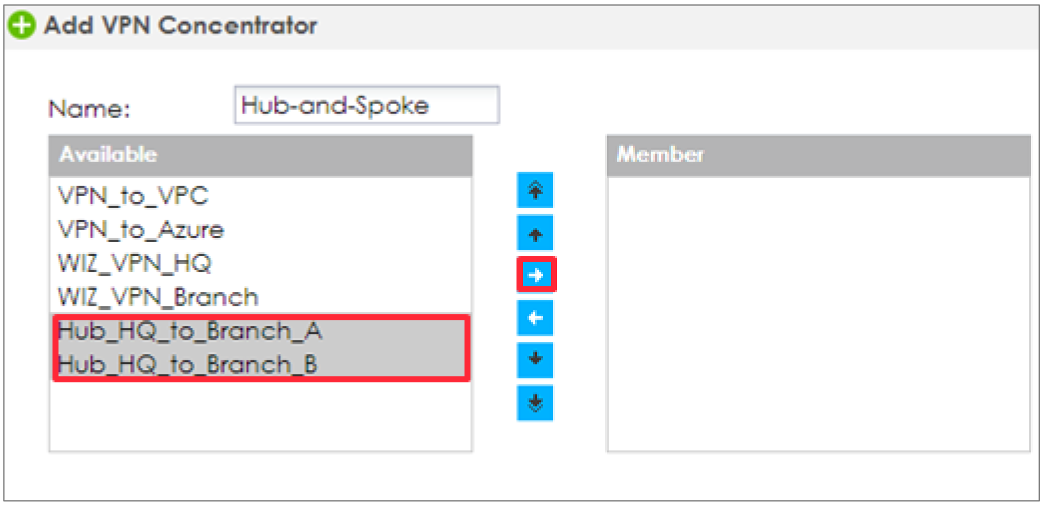
SA Life Time: 86400 (180 - 3000000 Seconds)

Related Settings

Zone: IPSec_VPN

Hub_HQ Concentrator

In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPSec VPN > Concentrator**, add a VPN Concentrator rule. Select VPN tunnels to the same member group and click **Save**.

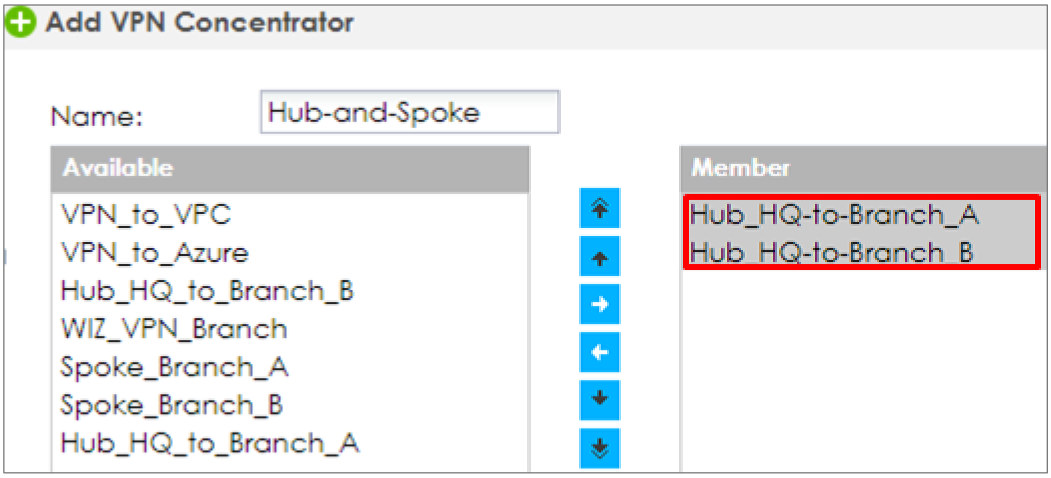


Add VPN Concentrator

Name: Hub-and-Spoke

Available:
VPN_to_VPC
VPN_to_Azure
WIZ_VPN_HQ
WIZ_VPN_Branch
Hub_HQ_to_Branch_A
Hub_HQ_to_Branch_B

Member



Add VPN Concentrator

Name: Hub-and-Spoke

Available:
VPN_to_VPC
VPN_to_Azure
Hub_HQ_to_Branch_B
WIZ_VPN_Branch
Spoke_Branch_A
Spoke_Branch_B
Hub_HQ_to_Branch_A

Member:
Hub_HQ-to-Branch_A
Hub_HQ-to-Branch_B

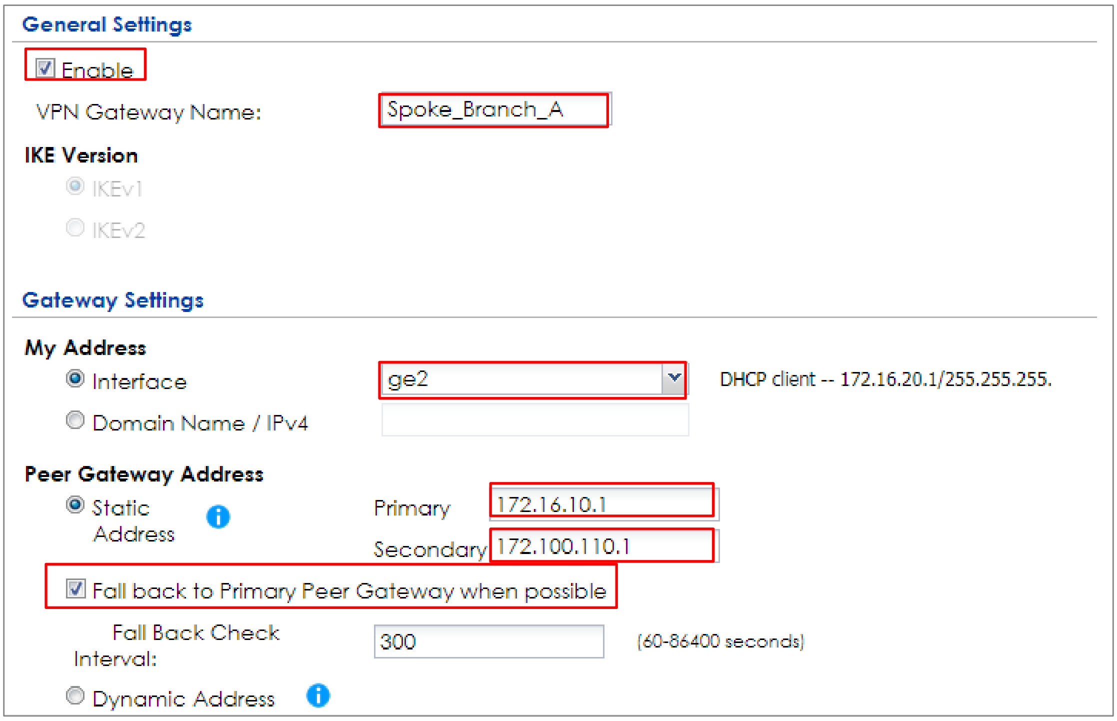
Spoke_Branch_A

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Primary** Gateway IP as the **Hub_HQ**'s **wan1** IP address (in the example, 172.16.10.1) and **Secondary** Gateway IP as the **Hub_HQ**'s **wan2** IP address (in the example, 172.100.110.1). Select **Fall back to Primary Peer Gateway when possible** and set desired **Fall Back Check Interval** time.

Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ**'s Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway



General Settings

☑ Enable

VPN Gateway Name: Spoke_Branch_A

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface ge2 DHCP client -- 172.16.20.1/255.255.255.

○ Domain Name / IPv4

Peer Gateway Address

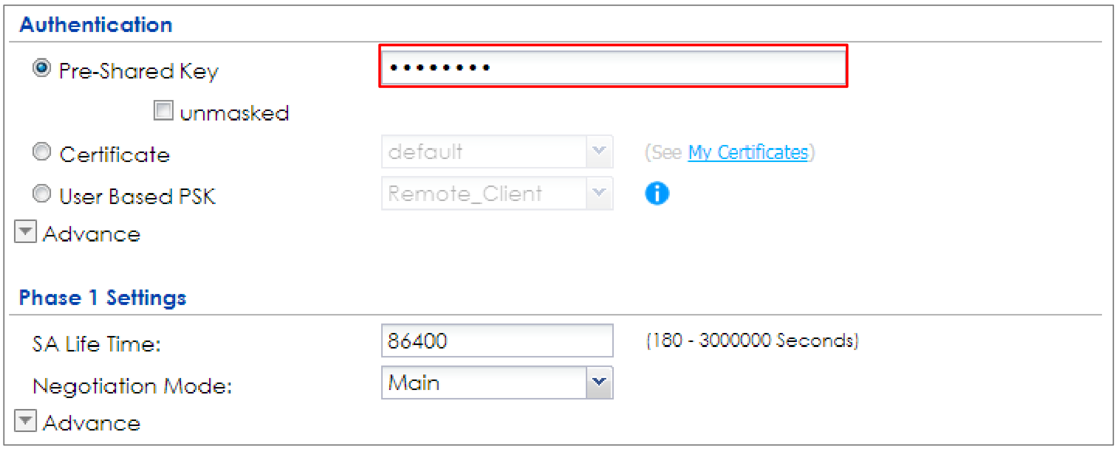
● Static Address Primary 172.16.10.1

Secondary 172.100.110.1

☑ 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)

○ User Based PSK Remote_Client

Advance

Phase 1 Settings

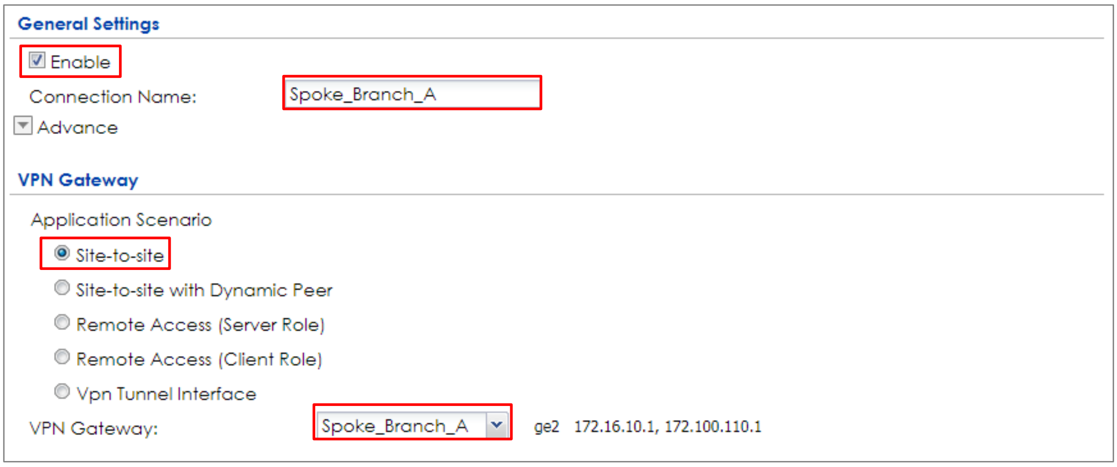
SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



General Settings

☑ Enable

Connection Name: Spoke_Branch_A

Advance

VPN Gateway

Application Scenario

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

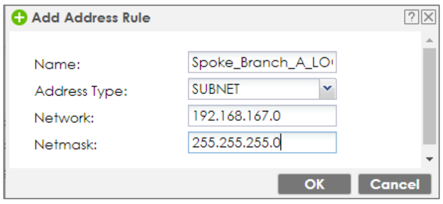
○ Vpn Tunnel Interface

VPN Gateway: Spoke_Branch_A ge2 172.16.10.1, 172.100.110.1

Click **Create new Object** to add the address of local network behind **Branch A** and an address of local network behind **Hub_HQ**

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

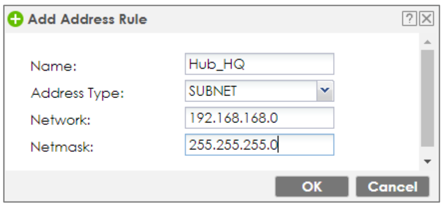
Local Policy



Add Address Rule

Name:	Spoke_Branch_A_LO
Address Type:	SUBNET
Network:	192.168.167.0
Netmask:	255.255.255.0

Remote Policy

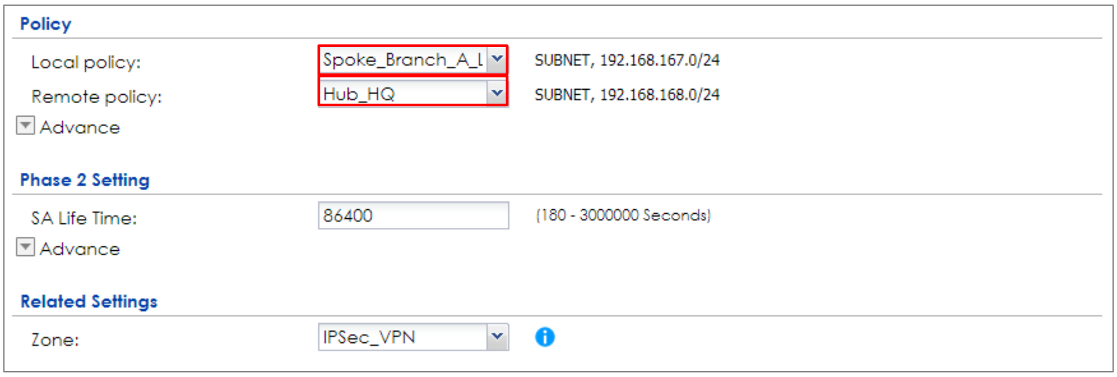


Add Address Rule

Name:	Hub_HQ
Address Type:	SUBNET
Network:	192.168.168.0
Netmask:	255.255.255.0

Set **Local Policy** to be **Spoke_Branch_A_LOCAL** and **Remote Policy** to **Hub_HQ** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



Policy

Local policy:	Spoke_Branch_A_L	SUBNET, 192.168.167.0/24
Remote policy:	Hub_HQ	SUBNET, 192.168.168.0/24

Phase 2 Setting

SA Life Time:	86400	(180 - 3000000 Seconds)

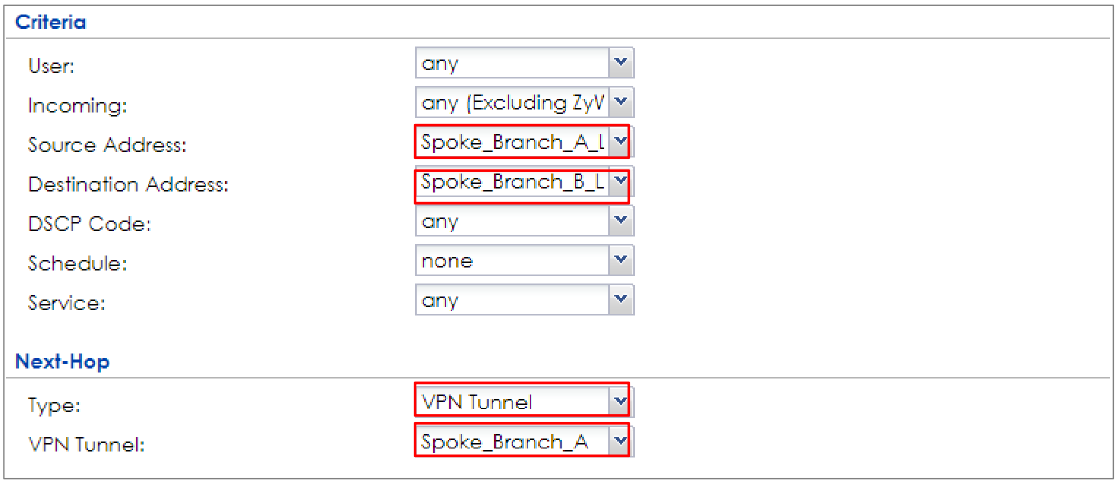
Related Settings

Zone:	IPSec_VPN

Go to **Network > Routing > Policy Route** to add a **Policy Route** to allow traffic from **Spoke_Branch_A** to **Spoke_Branch_B**.

Click **Create new Object** and set the address to be the local network behind the **Spoke_Branch_B**. Select **Source Address** to be the local network behind the **Spoke_Branch_A**. Then, scroll down the **Destination Address** list to choose the newly created **Spoke_Branch_B_LOCAL** address. Click **OK**.

Network > Routing > Policy Route



Criteria

User:	any
Incoming:	any (Excluding ZyW
Source Address:	Spoke_Branch_A_L
Destination Address:	Spoke_Branch_B_L
DSCP Code:	any
Schedule:	none
Service:	any

Next-Hop

Type:	VPN Tunnel
VPN Tunnel:	Spoke_Branch_A

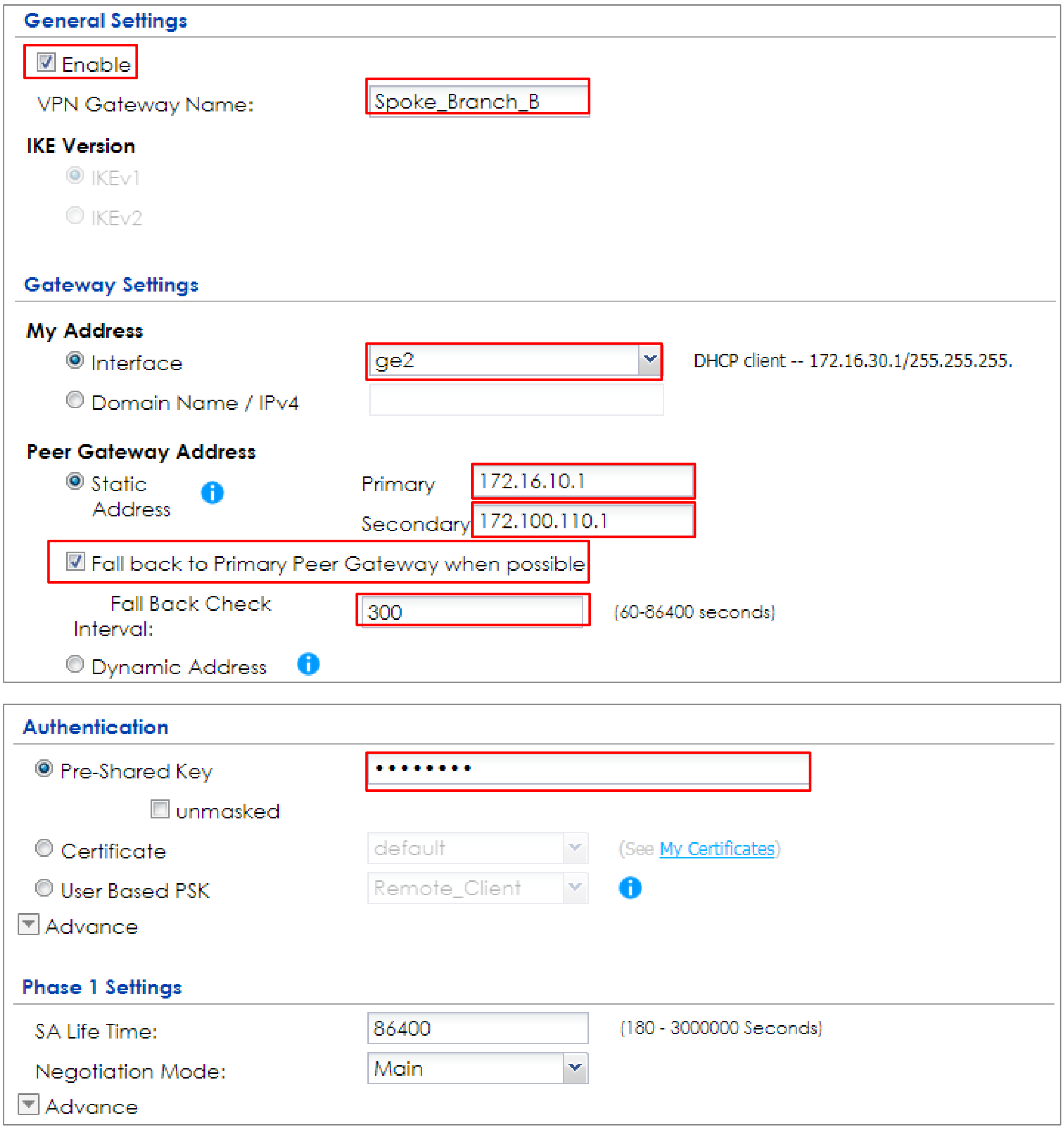
Spoke_Branch_B

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

Then, configure the **Primary** Gateway IP as the **Hub_HQ**'s **wan1** IP address (in the example, 172.16.10.1) and **Secondary** Gateway IP as the **Hub_HQ**'s **wan2** IP address (in the example, 172.100.110.1). Select **Fall back to Primary Peer Gateway when possible** and set desired **Fall Back Check Interval** time.

Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ**'s Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway



General Settings

☑ Enable

VPN Gateway Name: Spoke_Branch_B

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface ge2 DHCP client -- 172.16.30.1/255.255.255.

○ Domain Name / IPv4

Peer Gateway Address

● Static Address Primary 172.16.10.1

Secondary 172.100.110.1

☑ 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)

○ User Based PSK Remote_Client

Advance

Phase 1 Settings

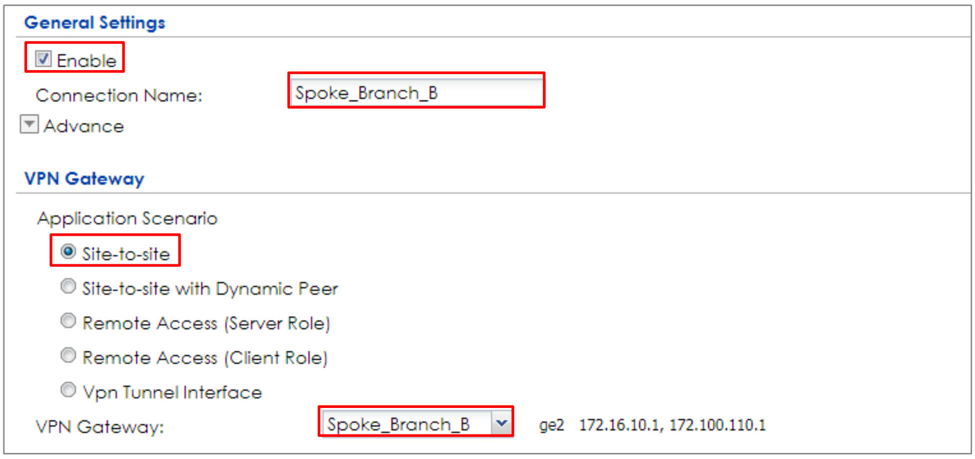
SA Life Time: 86400 (180 - 3000000 Seconds)

Negotiation Mode: Main

Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



General Settings

☑ Enable

Connection Name: Spoke_Branch_B

Advance

VPN Gateway

Application Scenario

● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

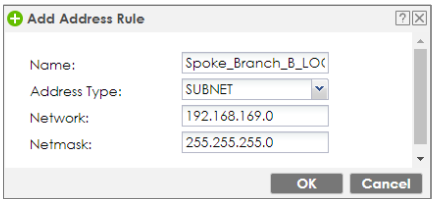
○ Vpn Tunnel Interface

VPN Gateway: Spoke_Branch_B ge2 172.16.10.1, 172.100.110.1

Click **Create new Object** to add the address of local network behind **Branch B** and an address of local network behind **Hub_HQ**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Create new Object

Local Policy



Add Address Rule

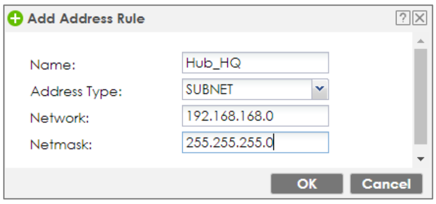
Name: Spoke_Branch_B_LOC

Address Type: SUBNET

Network: 192.168.169.0

Netmask: 255.255.255.0

Remote Policy



Add Address Rule

Name: Hub_HQ

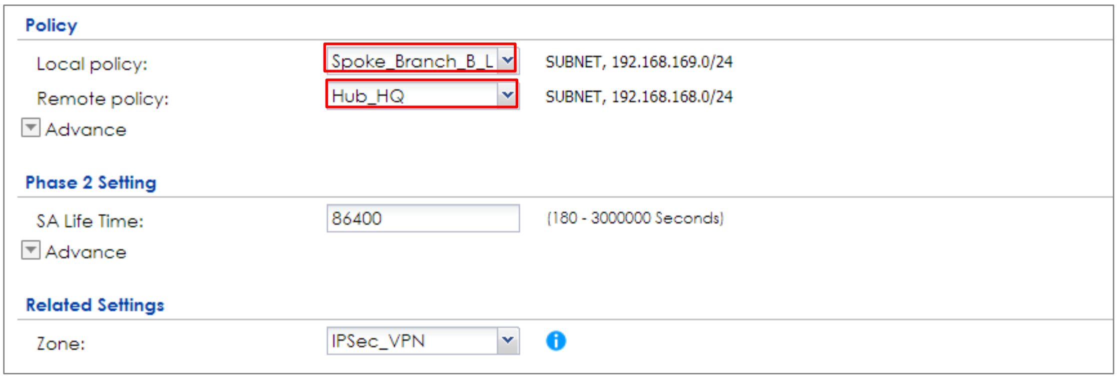
Address Type: SUBNET

Network: 192.168.168.0

Netmask: 255.255.255.0

Set **Local Policy** to be **Spoke_Branch_B_LOCAL** and **Remote Policy** to **Hub_HQ** which are newly created. Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



Policy

Local policy:	Spoke_Branch_B_L	SUBNET, 192.168.169.0/24
Remote policy:	Hub_HQ	SUBNET, 192.168.168.0/24

Phase 2 Setting

SA Life Time:	86400	(180 - 3000000 Seconds)

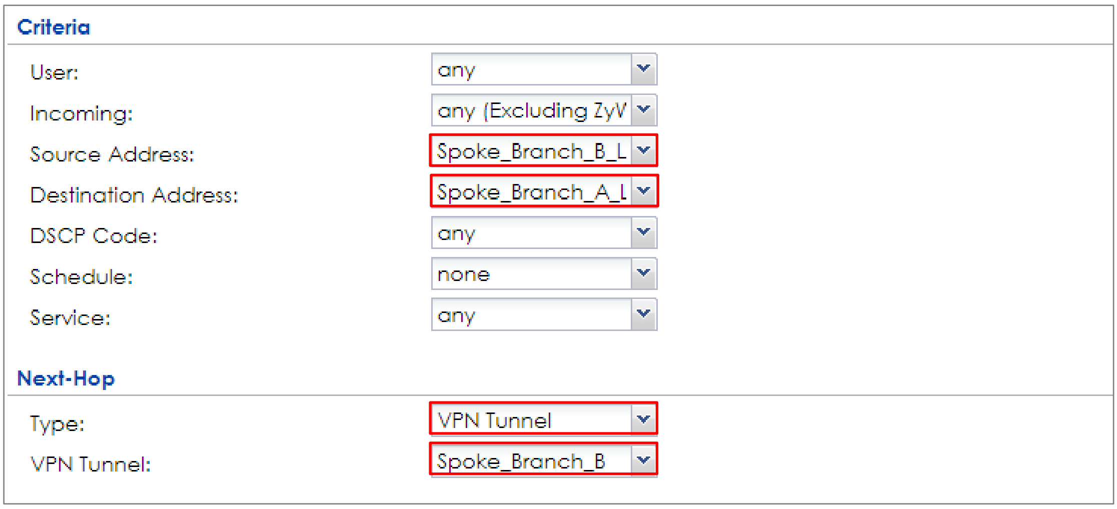
Related Settings

Zone:	IPSec_VPN

Go to **Network > Routing > Policy Route** to add a Policy Route to allow traffic from **Spoke_Branch_B to Spoke_Branch_A**.

Click **Create new Object** and set the address to be the local network behind the **Spoke_Branch_A**. Select **Source Address** to be the local network behind the **Spoke_Branch_B**. Then, scroll down the **Destination Address** list to choose the newly created **Spoke_Branch_A_LOCAL** address. Click **OK**.

Network > Routing > Policy Route



Criteria

User:	any
Incoming:	any (Excluding ZyV
Source Address:	Spoke_Branch_B_L
Destination Address:	Spoke_Branch_A_L
DSCP Code:	any
Schedule:	none
Service:	any

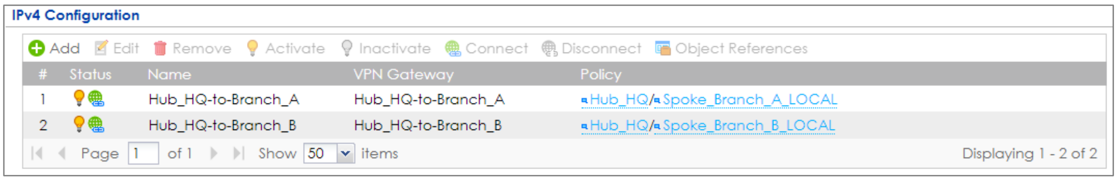
Next-Hop

Type:	VPN Tunnel
VPN Tunnel:	Spoke_Branch_B

Test the IPSec VPN Tunnel

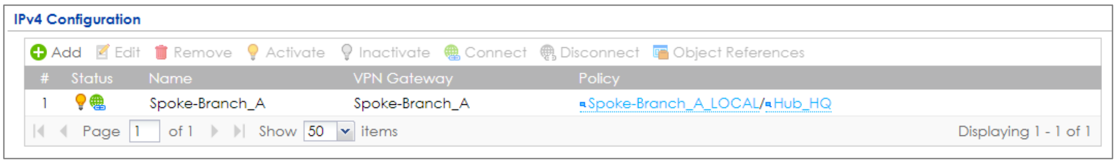
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

Hub_HQ > CONFIGURATION > VPN > IPSec VPN > VPN Connection



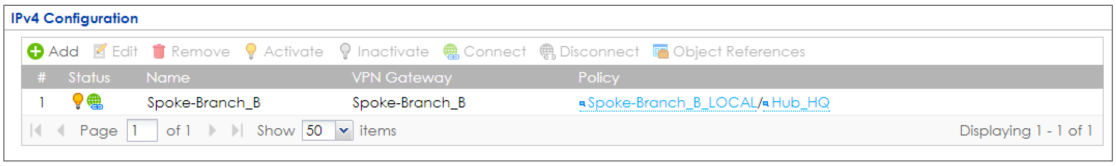
#	Status	Name	VPN Gateway	Policy
1		Hub_HQ-to-Branch_A	Hub_HQ-to-Branch_A	Hub_HQ/Spoke_Branch_A_LOCAL
2		Hub_HQ-to-Branch_B	Hub_HQ-to-Branch_B	Hub_HQ/Spoke_Branch_B_LOCAL

Spoke_Branch_A > CONFIGURATION > VPN > IPSec VPN > VPN Connection



#	Status	Name	VPN Gateway	Policy
1		Spoke-Branch_A	Spoke-Branch_A	Spoke-Branch_A_LOCAL/Hub_HQ

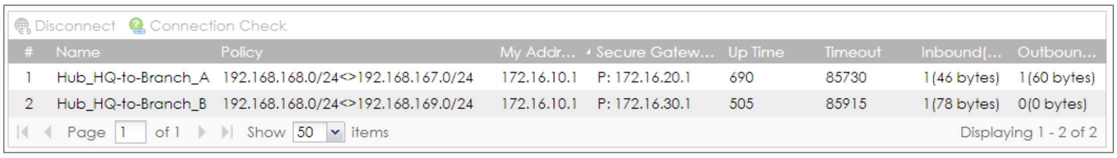
Spoke_Branch_B > CONFIGURATION > VPN > IPSec VPN > VPN Connection



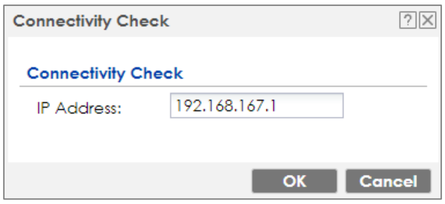
#	Status	Name	VPN Gateway	Policy
1		Spoke-Branch_B	Spoke-Branch_B	Spoke-Branch_B_LOCAL/Hub_HQ

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

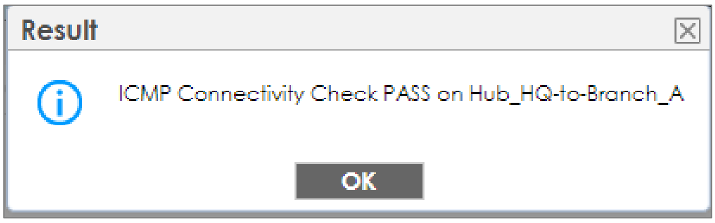
Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_A



#	Name	Policy	My Addr...	Secure Gatew...	Up Time	Timeout	Inbound(...	Outboun...
1	Hub_HQ-to-Branch_A	192.168.168.0/24<>192.168.167.0/24	172.16.10.1	P: 172.16.20.1	690	85730	1(46 bytes)	1(60 bytes)
2	Hub_HQ-to-Branch_B	192.168.168.0/24<>192.168.169.0/24	172.16.10.1	P: 172.16.30.1	505	85915	1(78 bytes)	0(0 bytes)

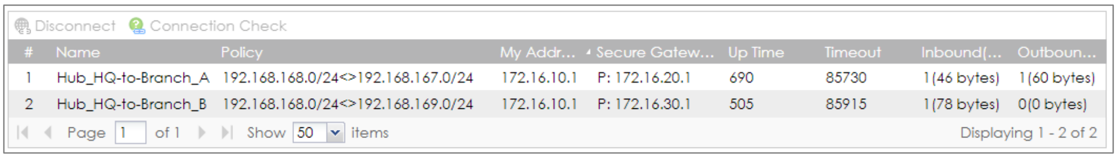


IP Address: 192.168.167.1

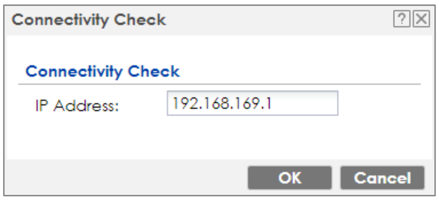


ICMP Connectivity Check PASS on Hub_HQ-to-Branch_A

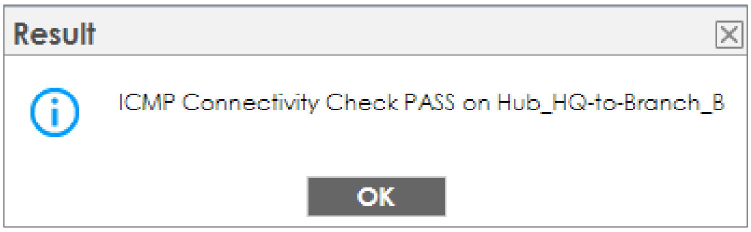
Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_B



#	Name	Policy	My Addr...	Secure Gatew...	Up Time	Timeout	Inbound(...	Outboun...
1	Hub_HQ-to-Branch_A	192.168.168.0/24<>192.168.167.0/24	172.16.10.1	P: 172.16.20.1	690	85730	1(46 bytes)	1(60 bytes)
2	Hub_HQ-to-Branch_B	192.168.168.0/24<>192.168.169.0/24	172.16.10.1	P: 172.16.30.1	505	85915	1(78 bytes)	0(0 bytes)

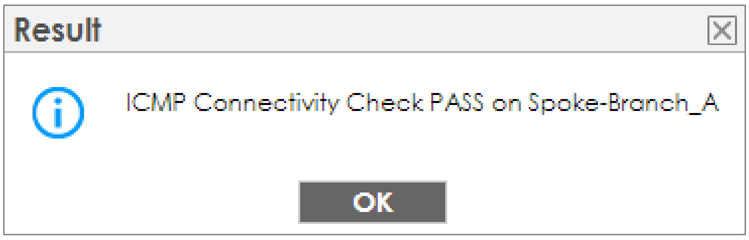


IP Address: 192.168.169.1



ICMP Connectivity Check PASS on Hub_HQ-to-Branch_B

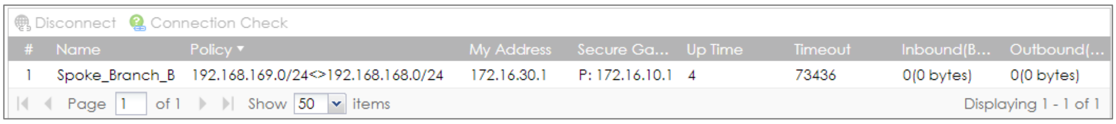
Spoke_Branch_A > MONITOR > VPN Monitor > IPSec



Result

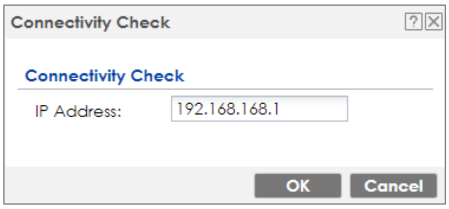
ICMP Connectivity Check PASS on Spoke-Branch_A

Spoke_Branch_B > MONITOR > VPN Monitor > IPSec



#	Name	Policy ▾	My Address	Secure Ga...	Up Time	Timeout	Inbound(B...	Outbound(...
1	Spoke_Branch_B	192.168.169.0/24<>192.168.168.0/24	172.16.30.1	P: 172.16.10.1	4	73436	0(0 bytes)	0(0 bytes)

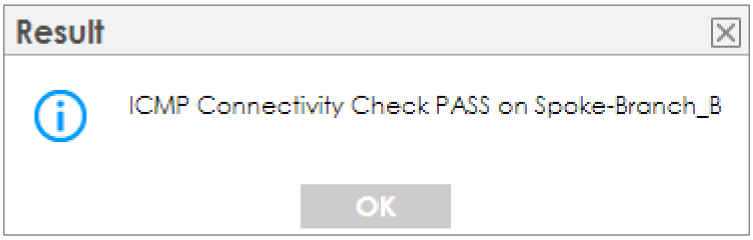
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1



Connectivity Check

Connectivity Check

IP Address: 192.168.168.1

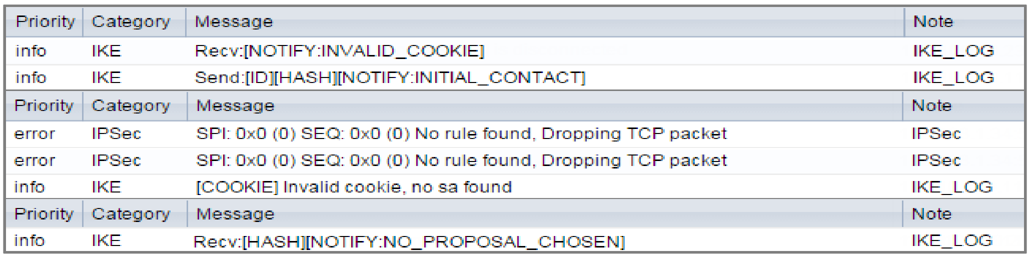


Result

ICMP Connectivity Check PASS on Spoke-Branch_B

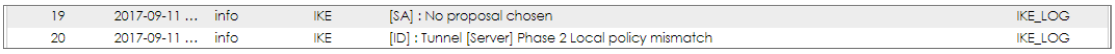
What Could Go Wrong?

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. All ZyWALL/USG units must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

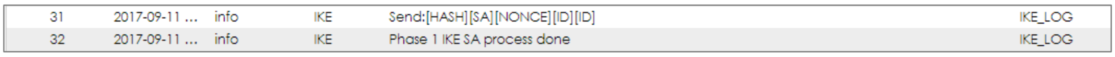


```
Priority  Category  Message                                                        Note
info      IKE       Recv:[NOTIFY:INVALID_COOKIE]                                   IKE_LOG
info      IKE       Send:[ID][HASH][NOTIFY:INITIAL_CONTACT]                        IKE_LOG
Priority  Category  Message                                                        Note
error     IPSec     SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet   IPSec
error     IPSec     SPI: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet   IPSec
info      IKE       [COOKIE] Invalid cookie, no sa found                           IKE_LOG
Priority  Category  Message                                                        Note
info      IKE       Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]                         IKE_LOG
```

If you see that Phase 1 IKE SA process done but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. All ZyWALL/USG units must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.



```
19   2017-09-11 ...   info   IKE   [SA] : No proposal chosen                              IKE_LOG
20   2017-09-11 ...   info   IKE   [ID] : Tunnel [Server] Phase 2 Local policy mismatch   IKE_LOG
```



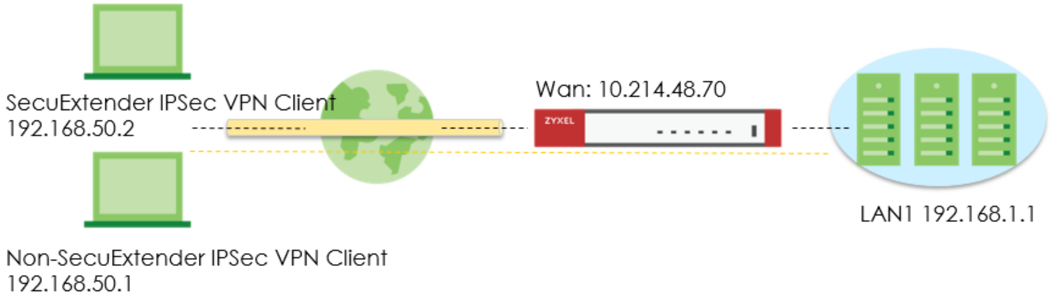
```
31   2017-09-11 ...   info   IKE   Send:[HASH][SA][NONCE][ID][ID]   IKE_LOG
32   2017-09-11 ...   info   IKE   Phase 1 IKE SA process done      IKE_LOG
```

Make sure the all ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

By default, NAT traversal is enabled on ZyWALL/USG, so please make sure the remote IPSec device also has NAT traversal enabled.

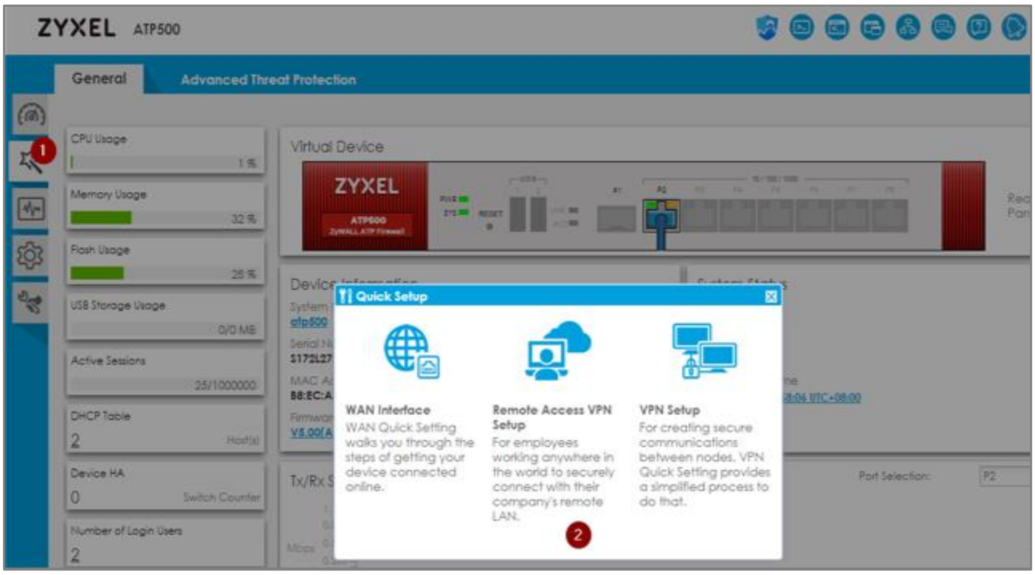
Remote Access VPN Wizard for SecuExtender IPSec and Non-SecuExtender IPSec VPN Clients

With USG FLEX/ ATP you are able to provision predefined settings on your device to SecuExtender IPSec as well as non-SecuExtender IPSec VPN clients. This article will show you how to use **Remote Access VPN Setup** Wizard to quick setup VPN tunnel using IKEv2 with EAP & Certification authentication.


SecuExtender IPSec VPN Client
192.168.50.2
Wan: 10.214.48.70
ZYXEL
LAN1 192.168.1.1
Non-SecuExtender IPSec VPN Client
192.168.50.1

Set up VPN Tunnel on ATP/USG FLEX

1.Log in to the Web GUI of your USG-FLEX/ATP, click **Quick Setup**, then select **Remote Access VPN Setup** to build up VPN tunnel with the Wizard.



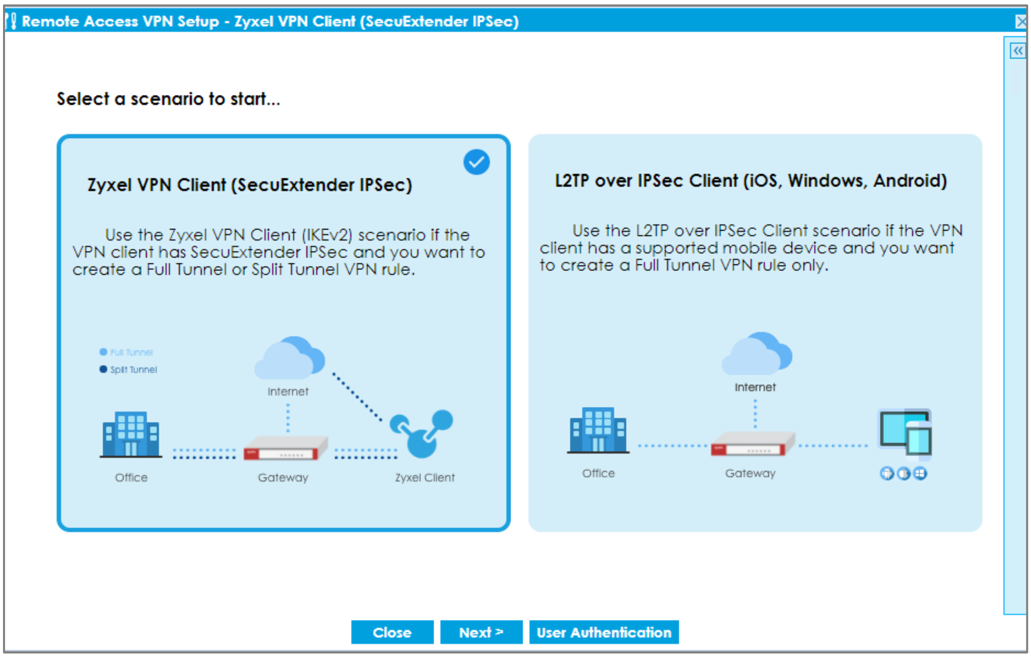
Quick Setup

WAN Interface
WAN Quick Setting walks you through the steps of getting your device connected online.

Remote Access VPN Setup
For employees working anywhere in the world to securely connect with their company's remote LAN.

VPN Setup
For creating secure communications between nodes. VPN Quick Setting provides a simplified process to do that.

2.Select Remote Access VPN Setup, and choose **Zyxel VPN Client (SecuExtender IPSec)**.



Remote Access VPN Setup - Zyxel VPN Client (SecuExtender IPSec)

Select a scenario to start...

Zyxel VPN Client (SecuExtender IPSec)

Use the Zyxel VPN Client (IKEv2) scenario if the VPN client has SecuExtender IPSec and you want to create a Full Tunnel or Split Tunnel VPN rule.

L2TP over IPSec Client (iOS, Windows, Android)

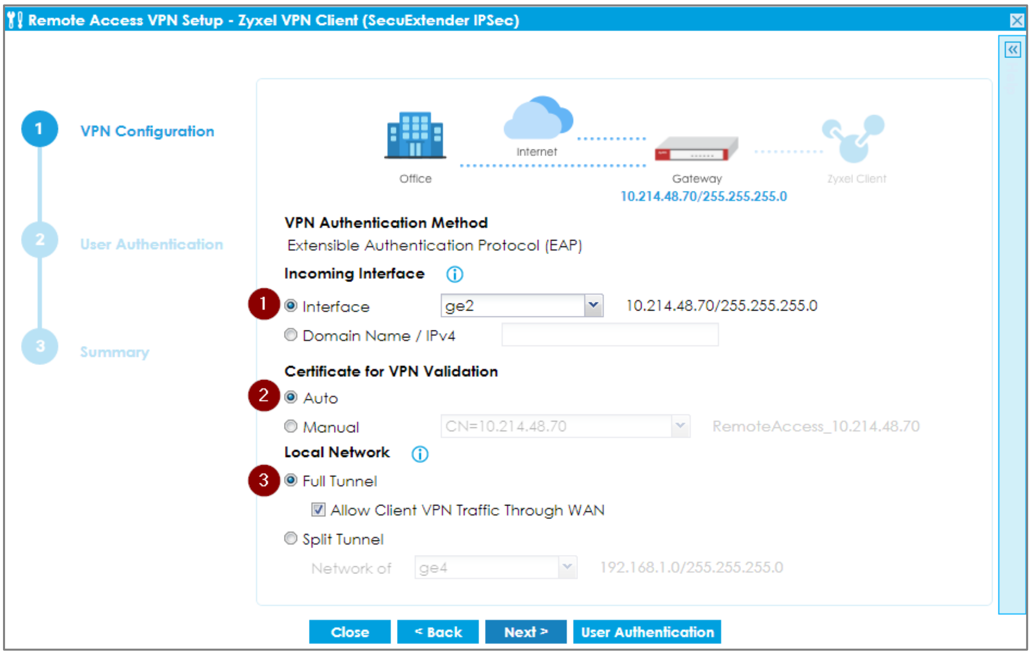
Use the L2TP over IPSec Client scenario if the VPN client has a supported mobile device and you want to create a Full Tunnel VPN rule only.

3.Configure the VPN Authentication Method

(1) Choose Incoming Interface

(2) Choose Certificate for VPN Validation

(3) Select the tunnel type **Full Tunnel** and enable the check box of **Allow Client VPN Traffic Through WAN**.



Remote Access VPN Setup - Zyxel VPN Client (SecuExtender IPSec)

Gateway 10.214.48.70/255.255.255.0

VPN Authentication Method
Extensible Authentication Protocol (EAP)

Incoming Interface
1 ● Interface ge2 10.214.48.70/255.255.255.0
○ Domain Name / IPv4

Certificate for VPN Validation
2 ● Auto
○ Manual CN=10.214.48.70 RemoteAccess_10.214.48.70

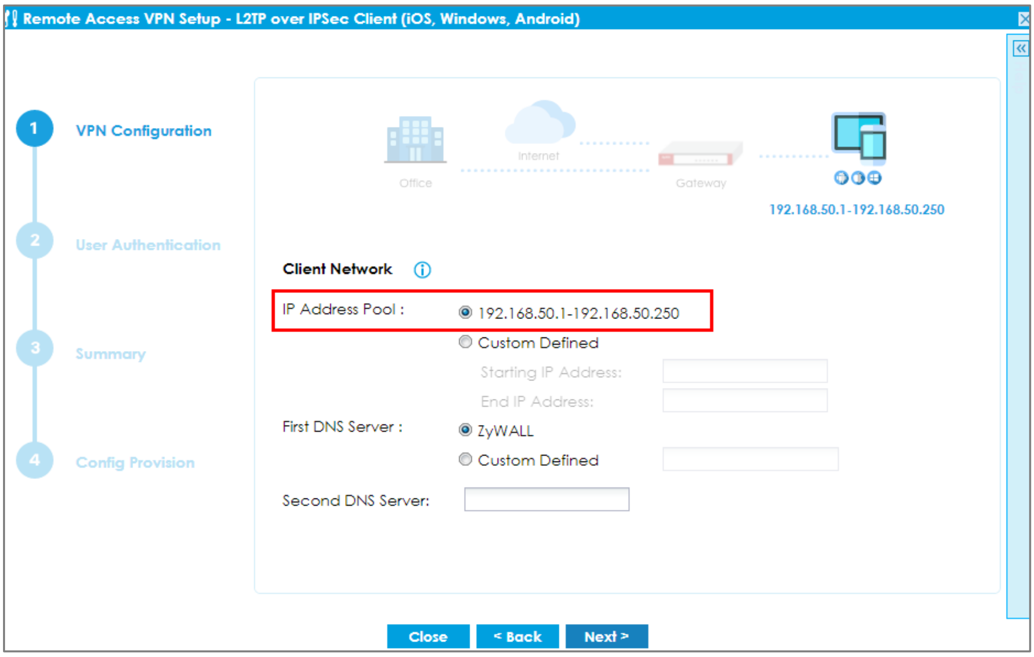
Local Network
3 ● Full Tunnel
☑ Allow Client VPN Traffic Through WAN
○ Split Tunnel
Network of ge4 192.168.1.0/255.255.255.0

4.Configure the IP Address Pool for the client

The IP address pool will auto select non-used subnet on the device to avoid setting up the same subnet on the device. The IP address Pool will begin at 192.168.50.1

If the subnet 192.168.50.1 exists in the gateway settings, the IP address pool will automatically change to 192.168.51.1 subnet.

Note: The gateway only checks overlapped subnets in /24, not check the other subnet mask.



Remote Access VPN Setup - L2TP over IPSec Client (iOS, Windows, Android)

Client Network

IP Address Pool : ● 192.168.50.1-192.168.50.250

○ Custom Defined

Starting IP Address:

End IP Address:

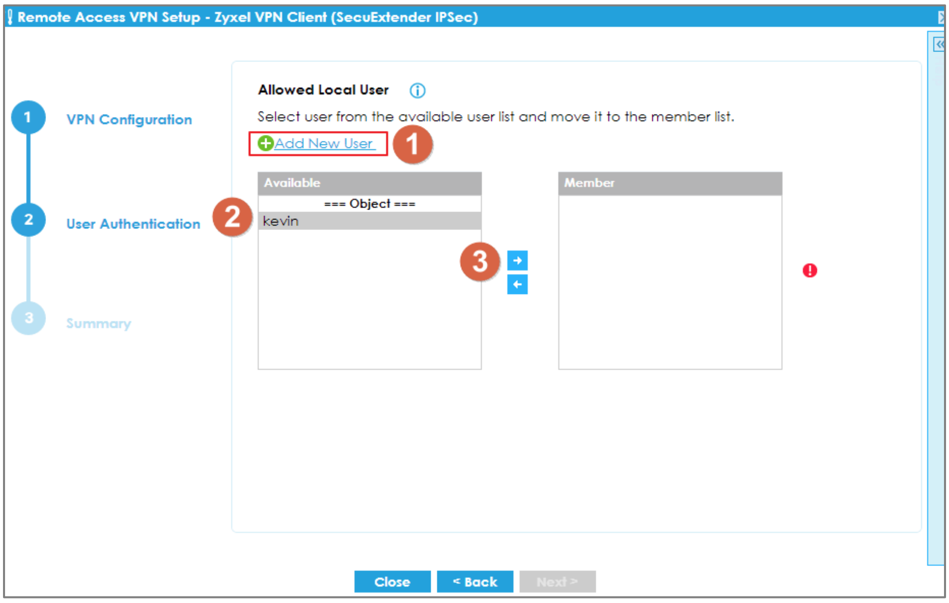
First DNS Server : ● ZyWALL

○ Custom Defined

Second DNS Server:

5. Allow local user to access the device via VPN tunnel

If you have not created the local users for remote VPN access, you can set up the local user here to allow the user to access the network through the VPN tunnel.



Allowed Local User

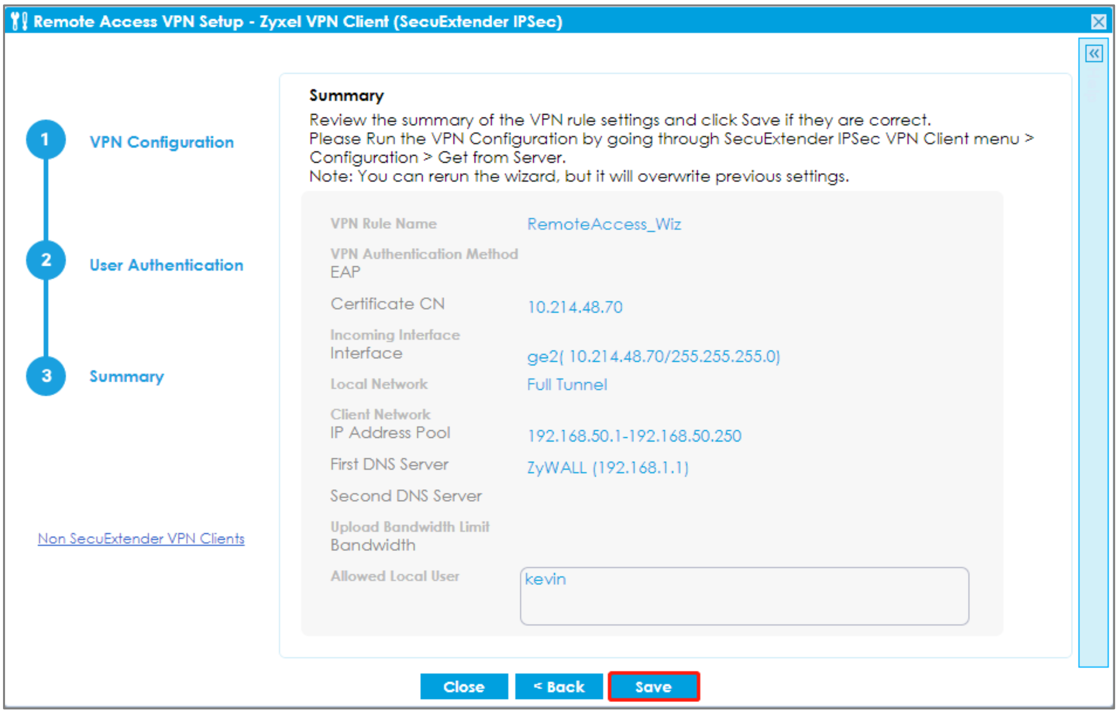
Select user from the available user list and move it to the member list.

Add New User

Available	Member
=== Object ===	
kevin	

6. After done all the steps in the wizard, you can choose using either SecuExtender IPSec or non- SecuExtender IPSec VPN clients (iOS/MacOS, Windows, Strongswan-Android) to provision the VPN settings

- SecuExtender IPSec VPN client: Click Save button to complete the Wizard



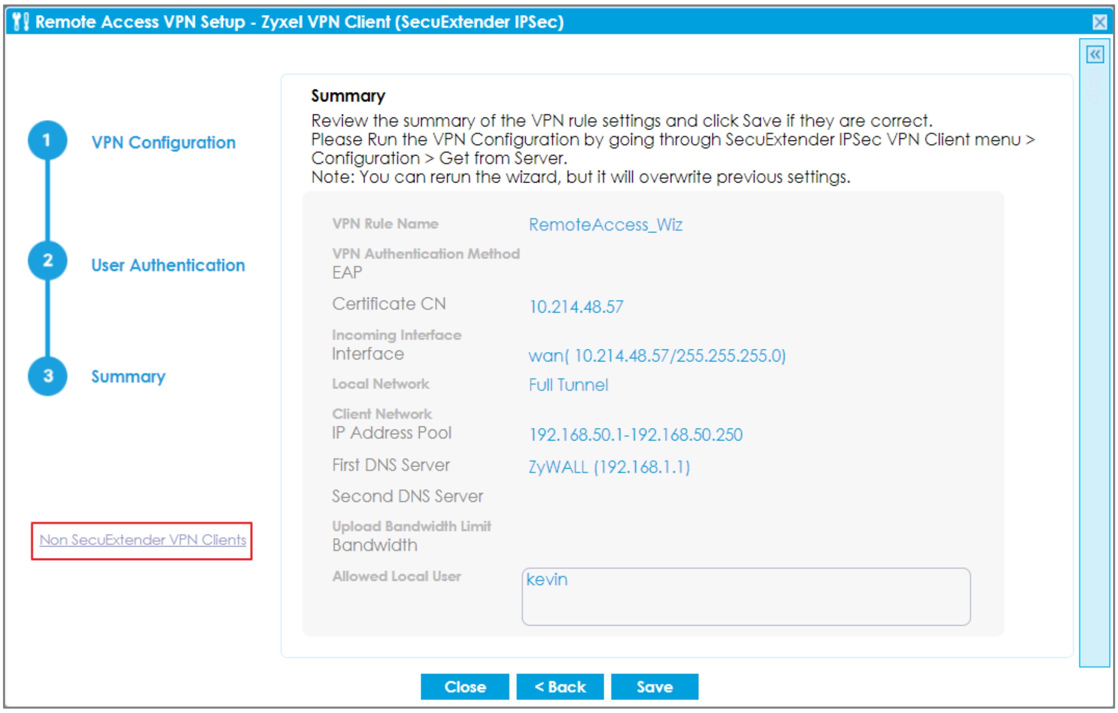
Remote Access VPN Setup - Zyxel VPN Client (SecuExtender IPSec)
1 VPN Configuration
2 User Authentication
3 Summary
Non SecuExtender VPN Clients
Close
< Back
Save

Summary

Review the summary of the VPN rule settings and click Save if they are correct.
Please Run the VPN Configuration by going through SecuExtender IPSec VPN Client menu > Configuration > Get from Server.
Note: You can rerun the wizard, but it will overwrite previous settings.

VPN Rule Name	RemoteAccess_Wiz
VPN Authentication Method EAP	
Certificate CN	10.214.48.70
Incoming Interface Interface	ge2(10.214.48.70/255.255.255.0)
Local Network	Full Tunnel
Client Network IP Address Pool	192.168.50.1-192.168.50.250
First DNS Server	ZyWALL (192.168.1.1)
Second DNS Server	
Upload Bandwidth Limit Bandwidth	
Allowed Local User	kevin

- Non-SecuExtender IPSec VPN client: Click to Non-SecuExtender VPN Client at the left hand side, then choose which device's operating system you want to download the script to install on.



Remote Access VPN Setup - Zyxel VPN Client (SecuExtender IPSec)

1 VPN Configuration

2 User Authentication

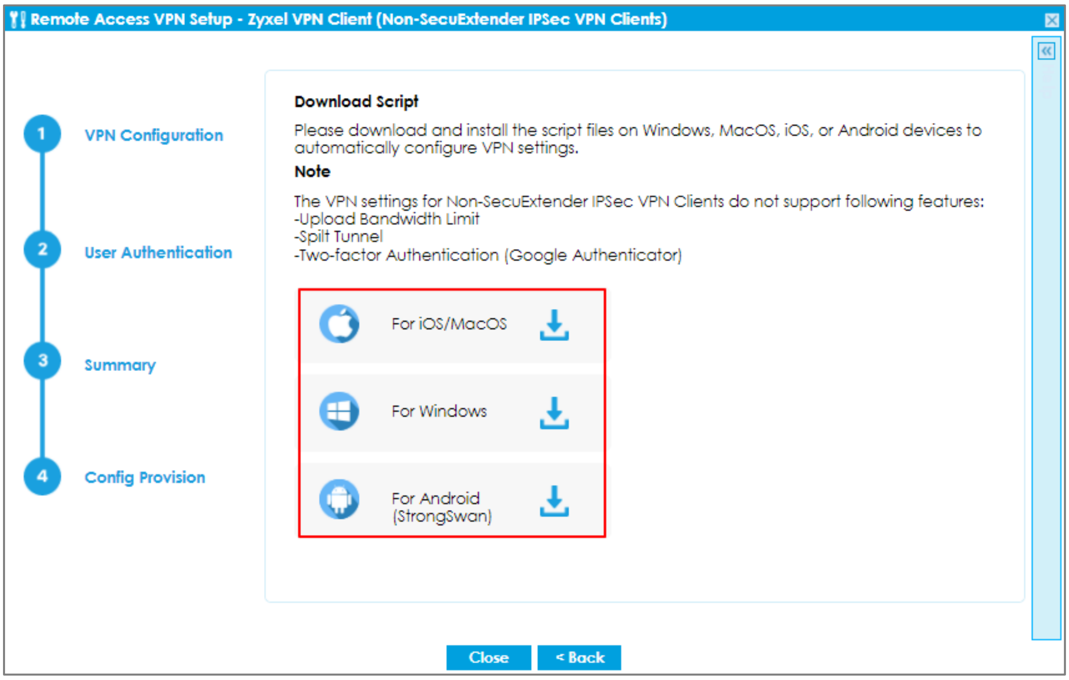
3 Summary

Non SecuExtender VPN Clients

Summary

Review the summary of the VPN rule settings and click Save if they are correct.
Please Run the VPN Configuration by going through SecuExtender IPSec VPN Client menu > Configuration > Get from Server.
Note: You can rerun the wizard, but it will overwrite previous settings.

VPN Rule Name	RemoteAccess_Wiz
VPN Authentication Method EAP	
Certificate CN	10.214.48.57
Incoming Interface Interface	wan(10.214.48.57/255.255.255.0)
Local Network	Full Tunnel
Client Network IP Address Pool	192.168.50.1-192.168.50.250
First DNS Server	ZyWALL (192.168.1.1)
Second DNS Server	
Upload Bandwidth Limit Bandwidth	
Allowed Local User	kevin



Remote Access VPN Setup - Zyxel VPN Client (Non-SecuExtender IPSec VPN Clients)

1 VPN Configuration

2 User Authentication

3 Summary

4 Config Provision

Download Script

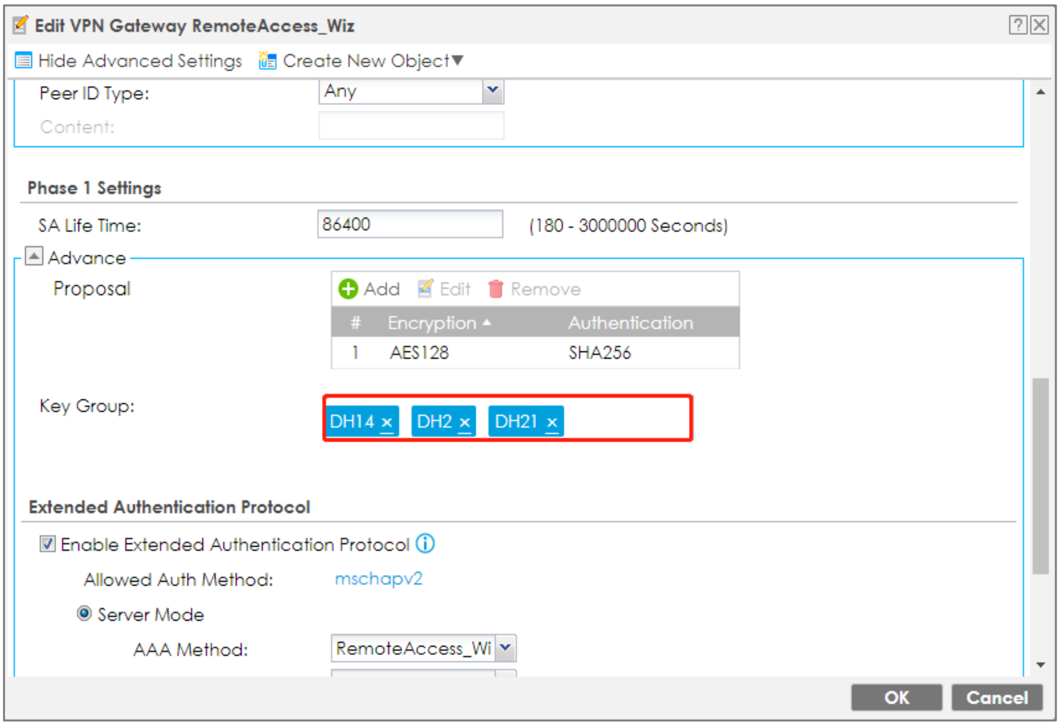
Please download and install the script files on Windows, MacOS, iOS, or Android devices to automatically configure VPN settings.

Note

The VPN settings for Non-SecuExtender IPSec VPN Clients do not support following features:
-Upload Bandwidth Limit
-Spilt Tunnel
-Two-factor Authentication (Google Authenticator)

7. (Optional) Since ZLD5.10, Remote Access VPN Setup Wizard uses DH group 14 for VPN phase 1 setting. If you are using perpetual SecuExtender IPSec VPN client with default DH group 2, you can also manually add more DH group on ATP/USG FLEX to avoid re-provisioning. You can add maximum of 3 DH groups.

- On ATP/USG FLEX Web GUI, go to CONFIGURATION > VPN > IPSec VPN > VPN Gateway, edit the **RemoteAccess_Wiz.** In **Phase 1 Settings**, you can add more **Key Group** (DH)


Edit VPN Gateway RemoteAccess_Wiz

Peer ID Type: Any

Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

⊟ Advance

Proposal

#	Encryption ▲	Authentication
1	AES128	SHA256

Key Group: DH14 × DH2 × DH21 ×

Extended Authentication Protocol

☑ Enable Extended Authentication Protocol

Allowed Auth Method: mschapv2

● Server Mode

AAA Method: RemoteAccess_Wi

Note:

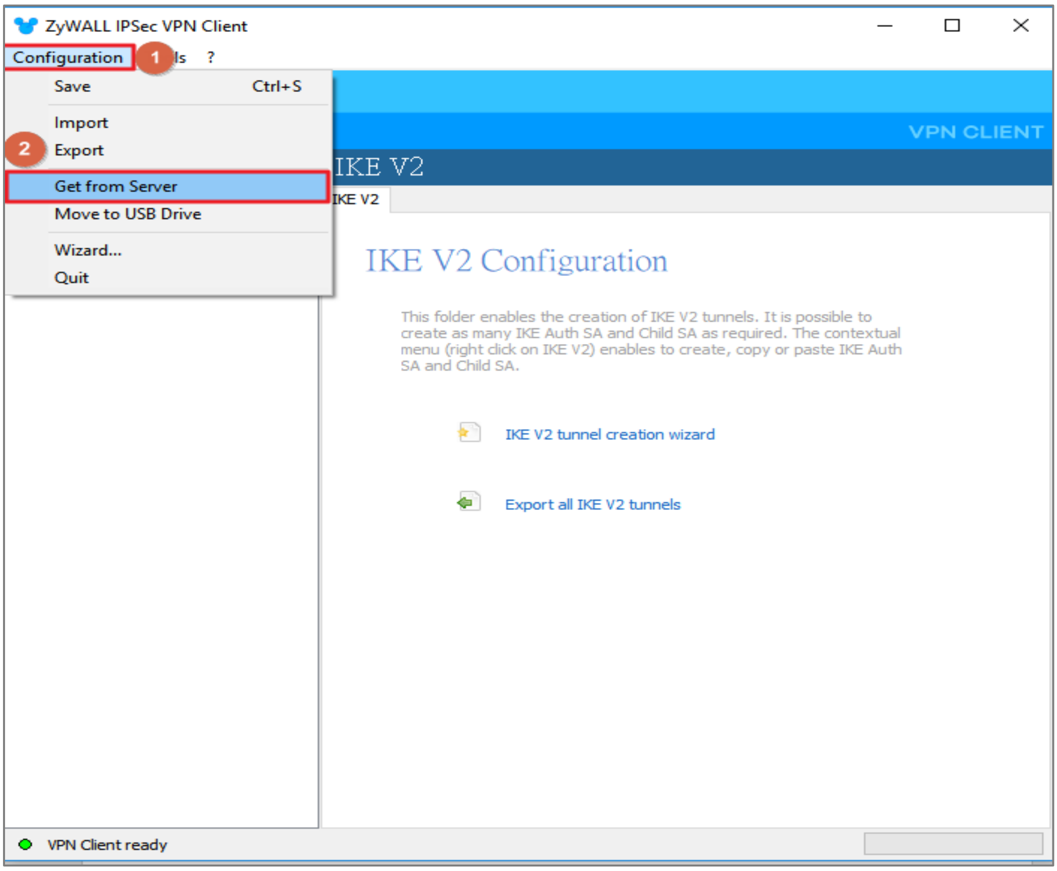
- IKEv2 Remote Access VPN using IKEv2 only supports single proposal (Authentication + Encryption)

- Remote Access VPN client using IKEv2 + EAP/MSCHAPv2 does not support using local-id to differentiate multiple rules. For multiple remote VPN rule, user must to choose different proposal (phase 2 proposal is suggested) to separate.

Test the result

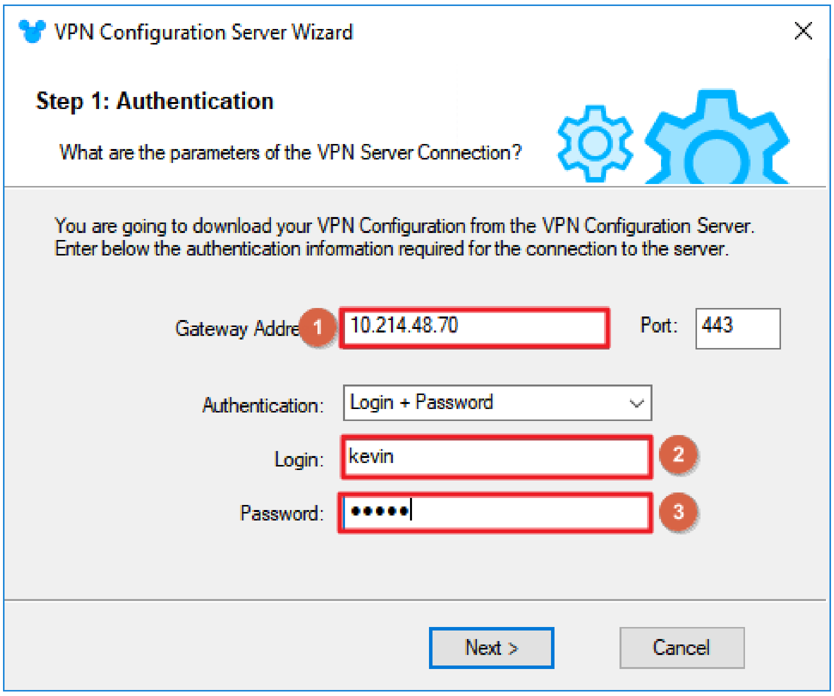
For Windows SecuExtender IPSec VPN client:

1. Go to Configuration tab, and click "Get from Server"



This folder enables the creation of IKE V2 tunnels. It is possible to create as many IKE Auth SA and Child SA as required. The contextual menu (right click on IKE V2) enables to create, copy or paste IKE Auth SA and Child SA.

2. Enter gateway IP and credential to get provision file from gateway.



VPN Configuration Server Wizard

Step 1: Authentication

What are the parameters of the VPN Server Connection?

You are going to download your VPN Configuration from the VPN Configuration Server.
Enter below the authentication information required for the connection to the server.

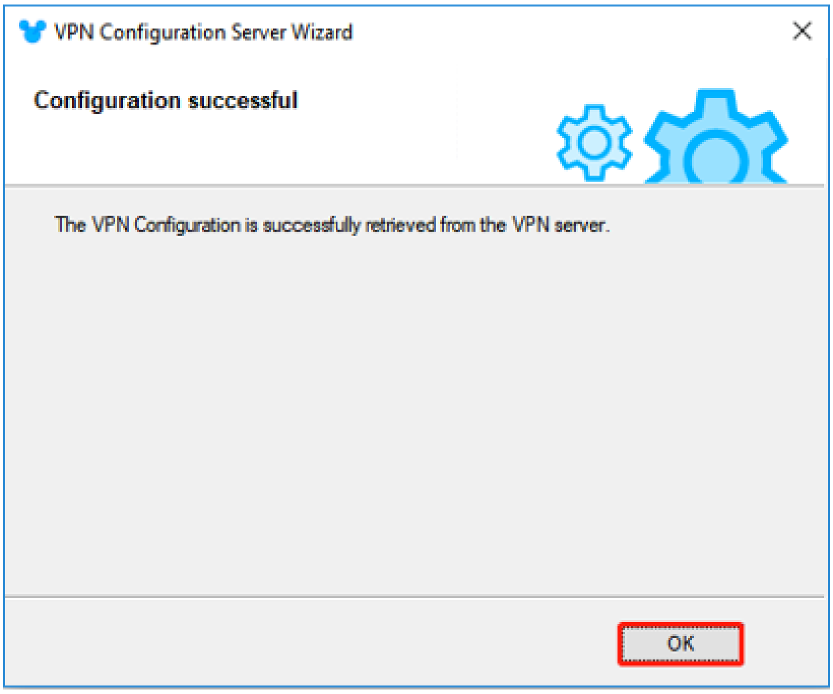
Gateway Address: 10.214.48.70 Port: 443

Authentication: Login + Password

Login: kevin

Password: •••••

Click “OK” to finish.

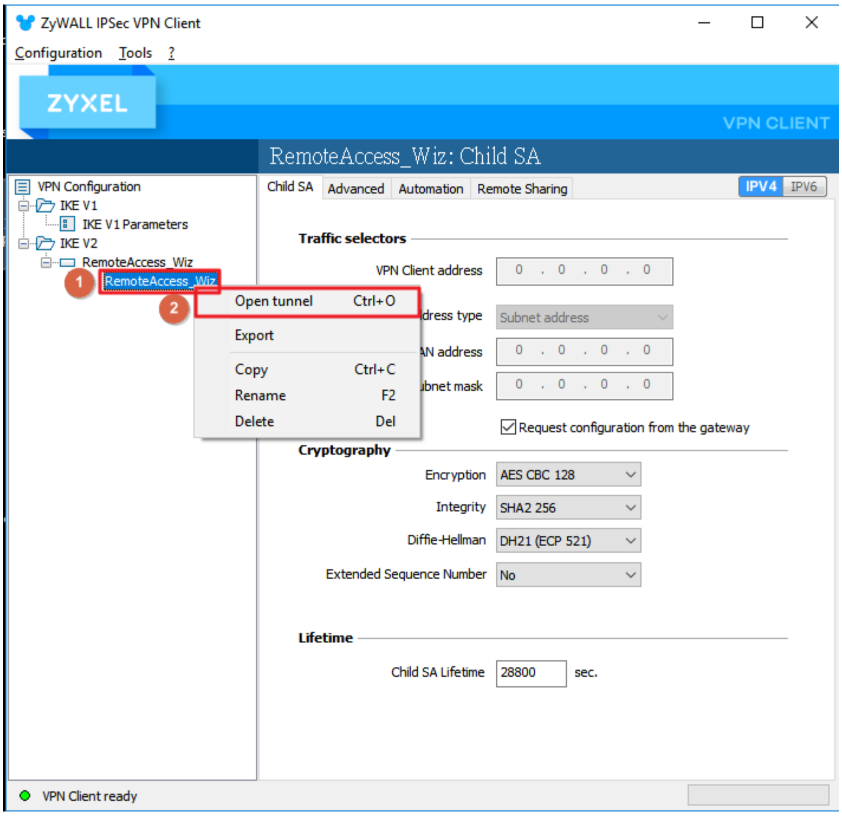


VPN Configuration Server Wizard

Configuration successful

The VPN Configuration is successfully retrieved from the VPN server.

3. Click “Open tunnel” to build up VPN connection.



ZyWALL IPSec VPN Client

RemoteAccess_Wiz: Child SA

Traffic selectors

VPN Client address 0 . 0 . 0 . 0

Address type Subnet address

LAN address 0 . 0 . 0 . 0

Subnet mask 0 . 0 . 0 . 0

☑ Request configuration from the gateway

Cryptography

Encryption AES CBC 128

Integrity SHA2 256

Diffie-Hellman DH21 (ECP 521)

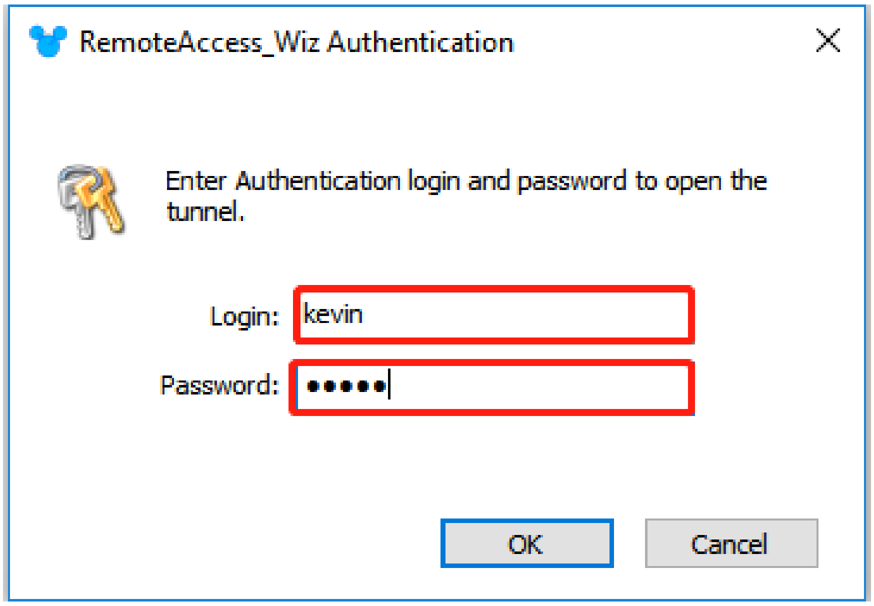
Extended Sequence Number No

Lifetime

Child SA Lifetime 28800 sec.

VPN Client ready

Enter credential and click “OK”.



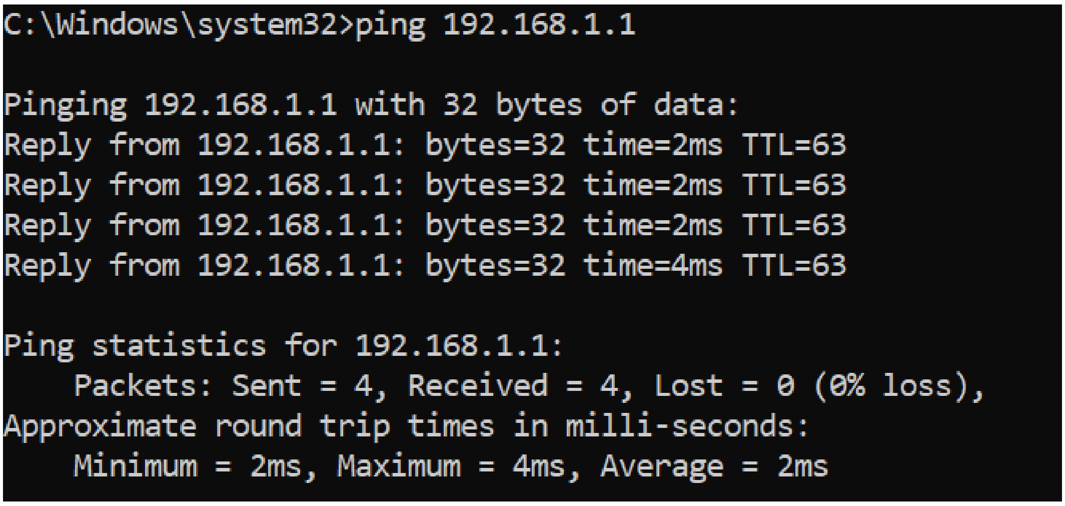
RemoteAccess_Wiz Authentication

Enter Authentication login and password to open the tunnel.

Login: kevin

Password: •••••

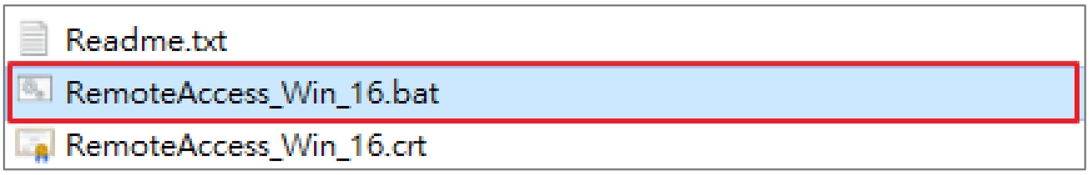
4. The remote user can ping the internal network now.



```
C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=4ms TTL=63

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms
```

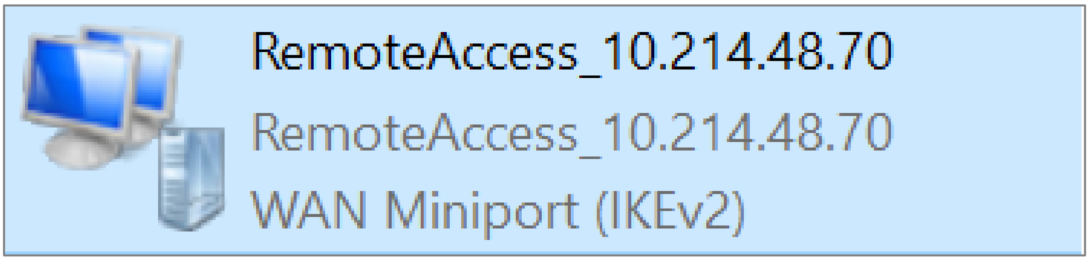
For Windows native IKEv2 client:

1. Extract the Script File, perform the scrip as Administrator.



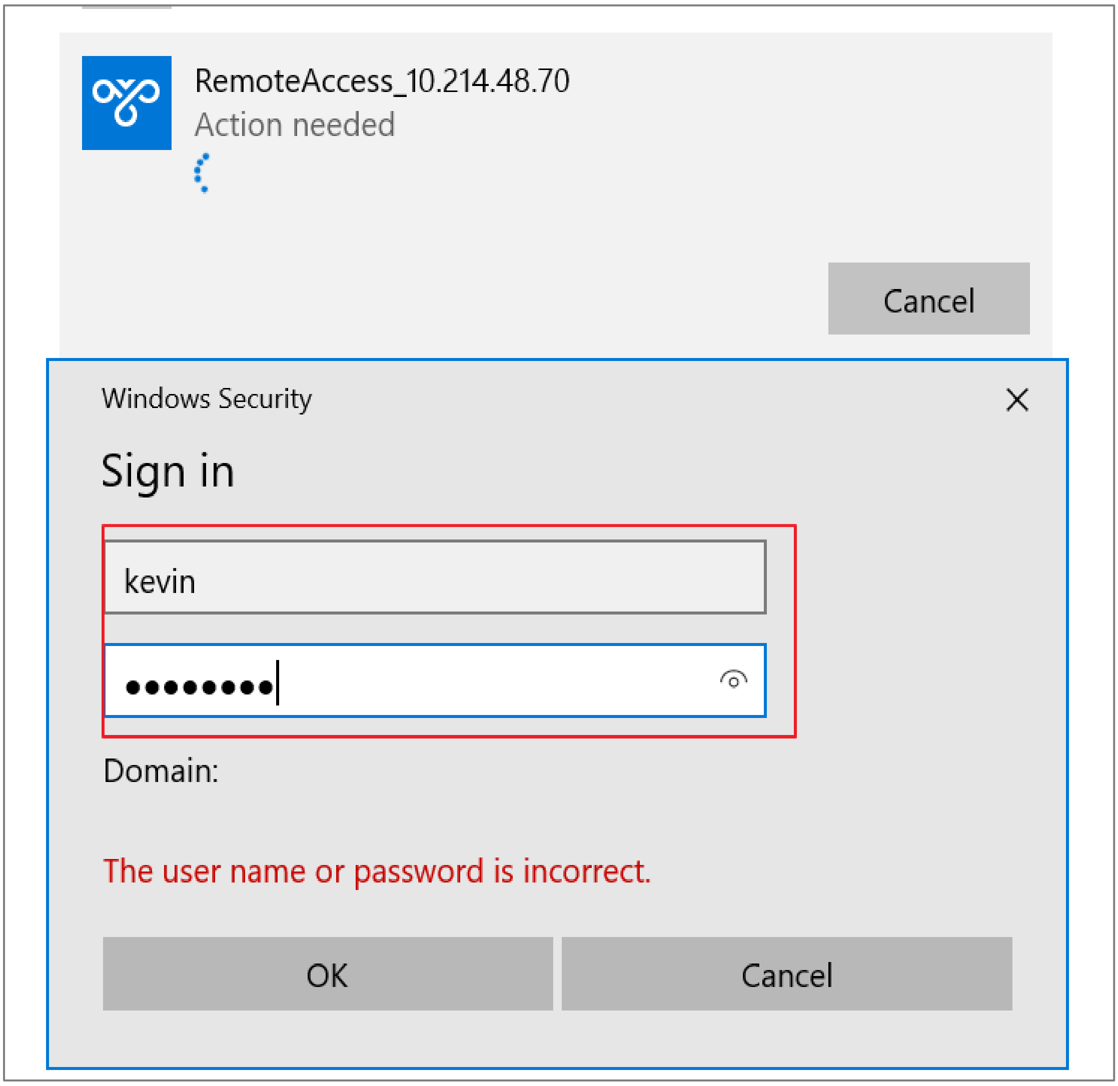
Readme.txt
RemoteAccess_Win_16.bat
RemoteAccess_Win_16.crt

2. VPN for Native IKEV2 is created successfully.

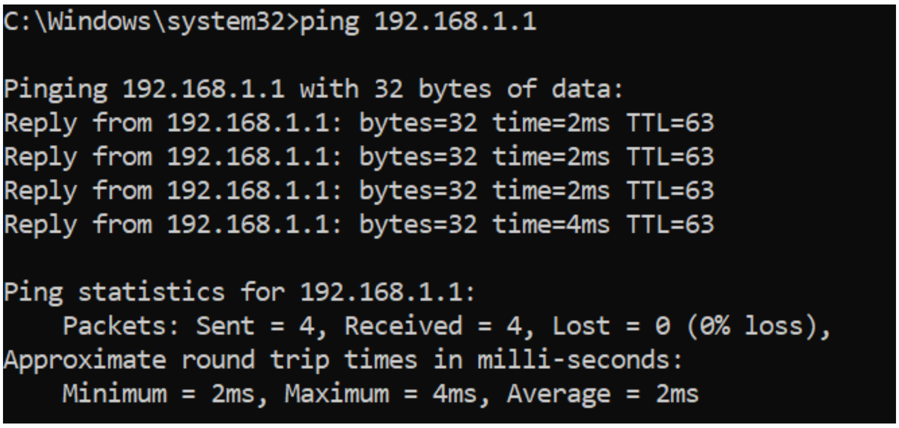


RemoteAccess_10.214.48.70
RemoteAccess_10.214.48.70
WAN Miniport (IKEv2)

3. Enter the VPN credential to complete the connection.



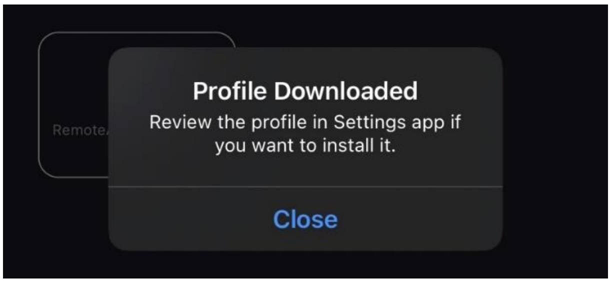
4. The remote user can ping the internal network now.



```
C:\Windows\system32>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=2ms TTL=63
Reply from 192.168.1.1: bytes=32 time=4ms TTL=63

Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 4ms, Average = 2ms
```

For iOS/MacOS:

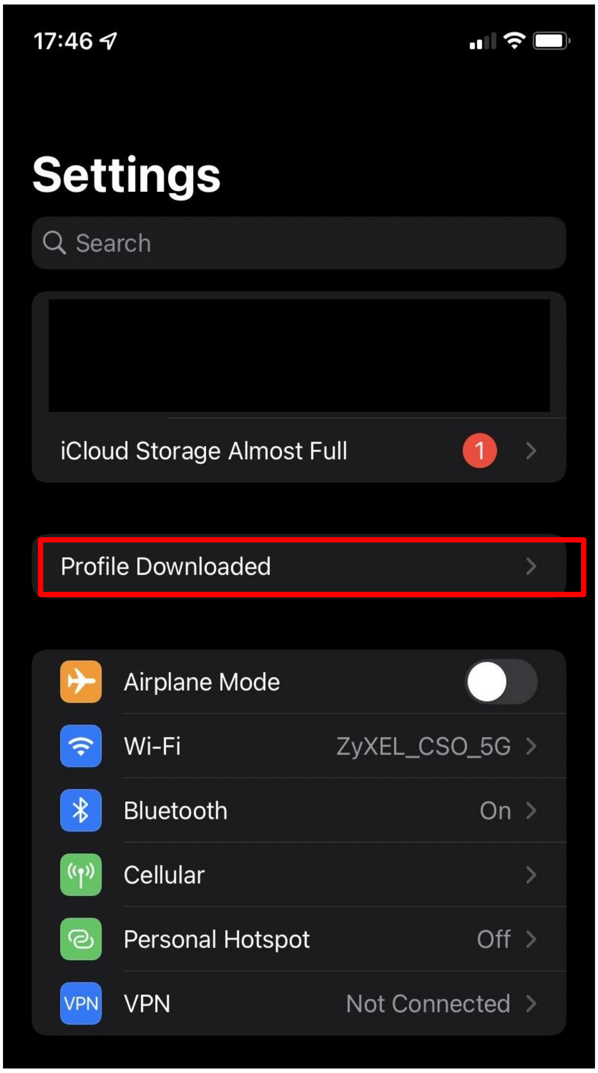
1.Send the Script to Device via email in example, then download the file



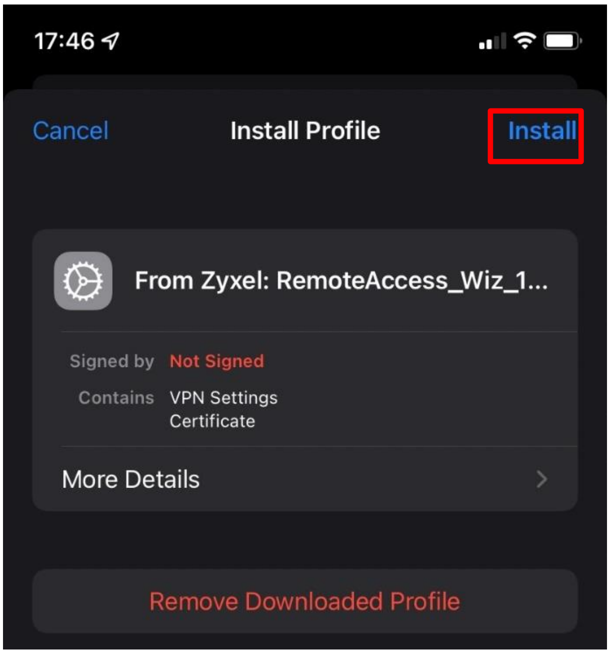
Profile Downloaded

Review the profile in Settings app if you want to install it.

2.Settings->Profile Downloaded



3.Press Install



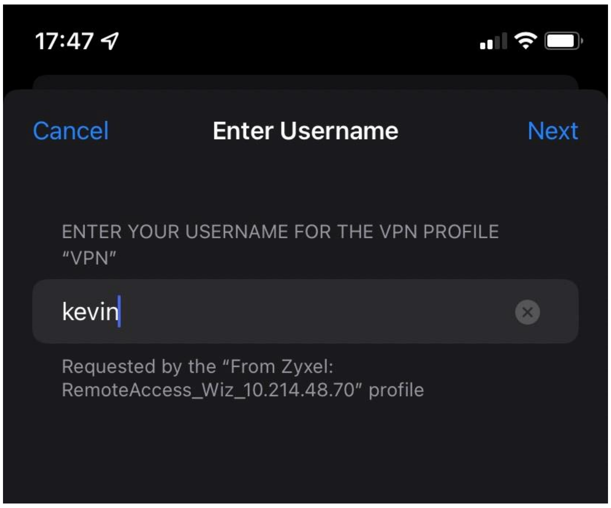
17:46

From Zyxel: RemoteAccess_Wiz_1...

Signed by Not Signed

Contains VPN Settings
Certificate

4.Enter Username and Password

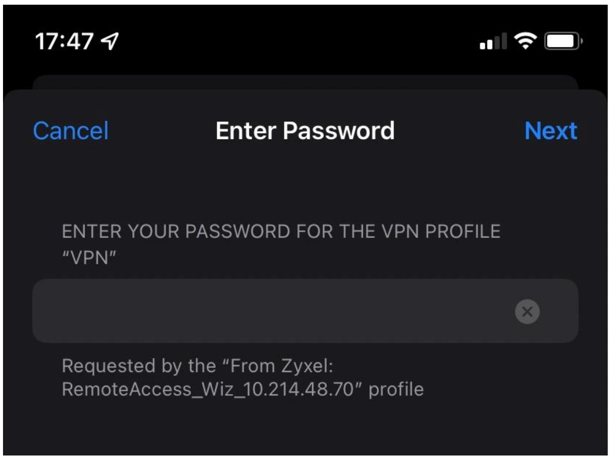


17:47

ENTER YOUR USERNAME FOR THE VPN PROFILE "VPN"

kevin

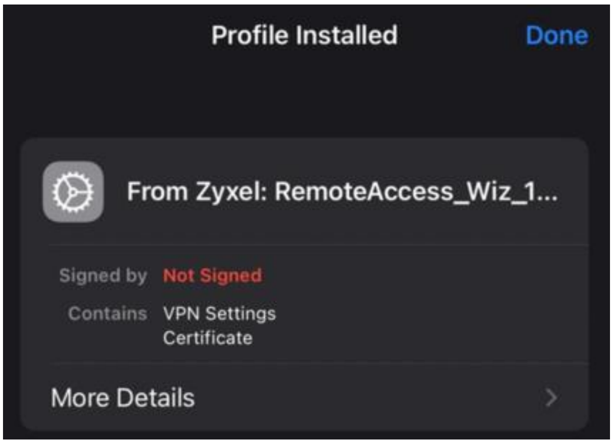
Requested by the "From Zyxel: RemoteAccess_Wiz_10.214.48.70" profile



ENTER YOUR PASSWORD FOR THE VPN PROFILE "VPN"

Requested by the "From Zyxel: RemoteAccess_Wiz_10.214.48.70" profile

5.Profile Installed Done

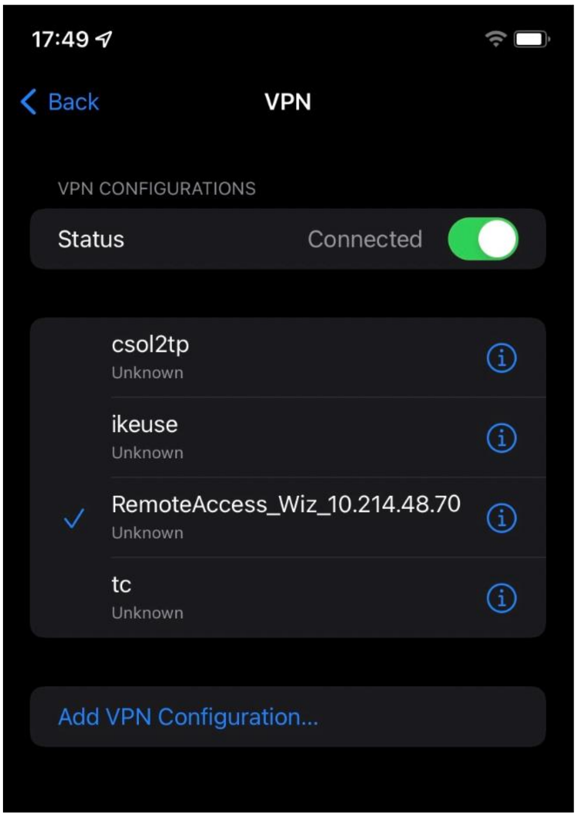


From Zyxel: RemoteAccess_Wiz_1...

Signed by Not Signed

Contains VPN Settings
Certificate

6.Now, it can connect



17:49

Back VPN

VPN CONFIGURATIONS

Status Connected

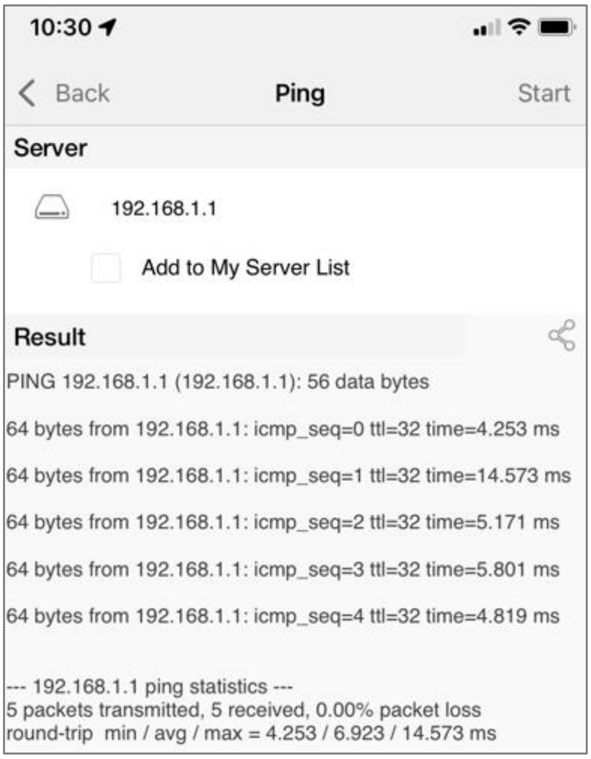
csol2tp
Unknown

ikeuse
Unknown

✓ RemoteAccess_Wiz_10.214.48.70
Unknown

tc
Unknown

Add VPN Configuration...



10:30

Back Ping Start

Server

192.168.1.1

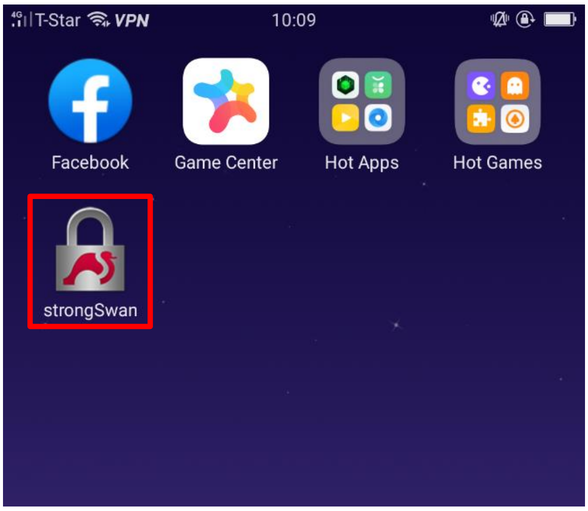
□ Add to My Server List

Result

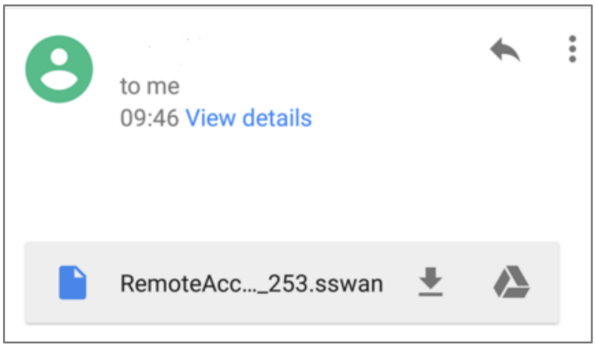
```
PING 192.168.1.1 (192.168.1.1): 56 data bytes
64 bytes from 192.168.1.1: icmp_seq=0 ttl=32 time=4.253 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=32 time=14.573 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=32 time=5.171 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=32 time=5.801 ms
64 bytes from 192.168.1.1: icmp_seq=4 ttl=32 time=4.819 ms

--- 192.168.1.1 ping statistics ---
5 packets transmitted, 5 received, 0.00% packet loss
round-trip  min / avg / max = 4.253 / 6.923 / 14.573 ms
```

For Android:

1.Download strongSwan from Google Play Store

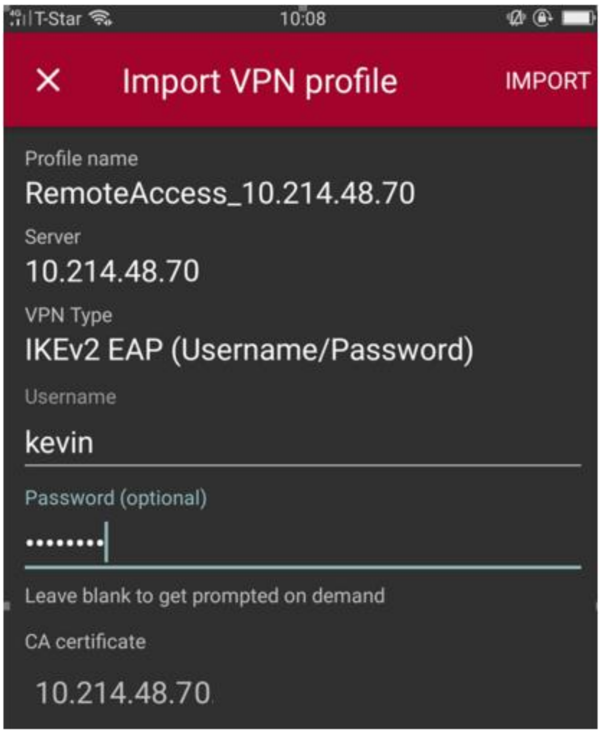


2.Send the Script to Device via email


to me
09:46 View details

RemoteAcc..._253.sswan

3.Import the Script into strongSwan and enter Username, Password



Import VPN profile

Profile name
RemoteAccess_10.214.48.70

Server
10.214.48.70

VPN Type
IKEv2 EAP (Username/Password)

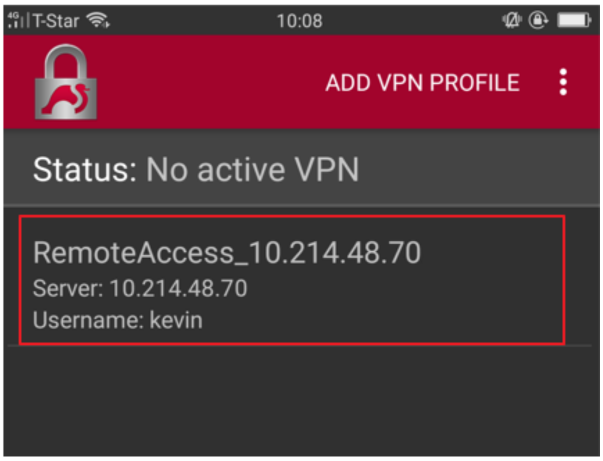
Username
kevin

Password (optional)
••••••••

Leave blank to get prompted on demand

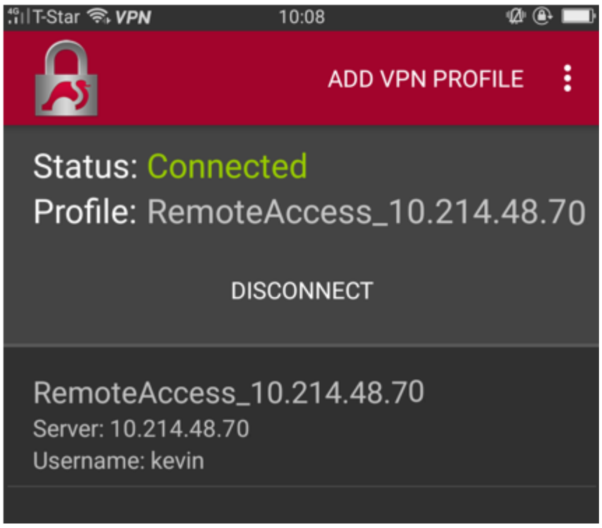
CA certificate
10.214.48.70

4.Now, it can connect.



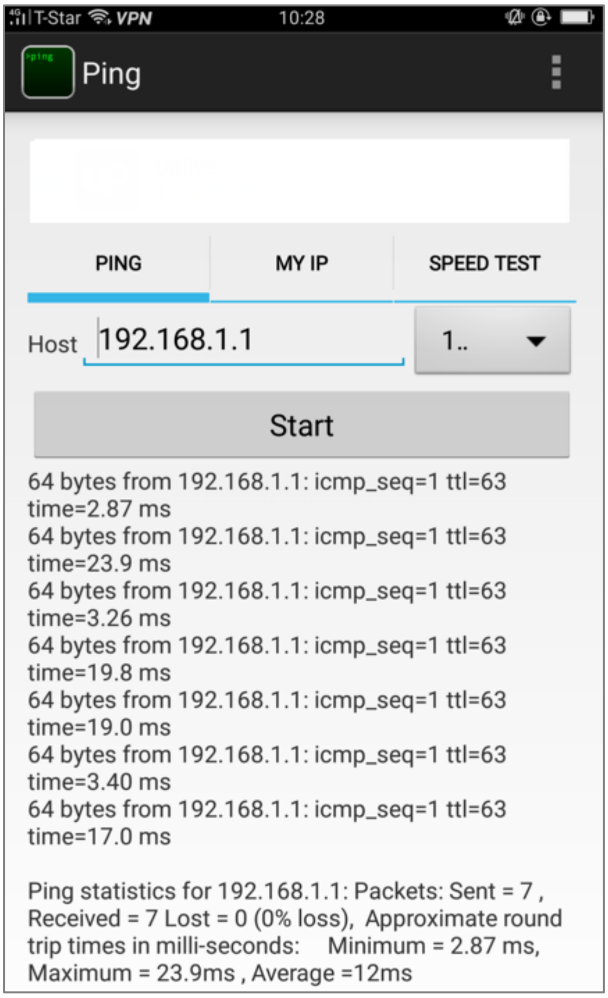
Status: No active VPN

RemoteAccess_10.214.48.70
Server: 10.214.48.70
Username: kevin



Status: Connected
Profile: RemoteAccess_10.214.48.70

RemoteAccess_10.214.48.70
Server: 10.214.48.70
Username: kevin

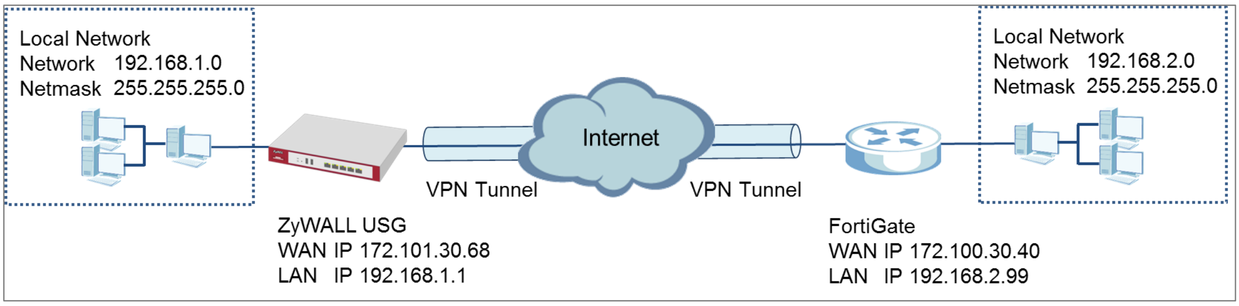


Host 192.168.1.1

```
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63
time=2.87 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63
time=23.9 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63
time=3.26 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63
time=19.8 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63
time=19.0 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63
time=3.40 ms
64 bytes from 192.168.1.1: icmp_seq=1 ttl=63
time=17.0 ms

Ping statistics for 192.168.1.1: Packets: Sent = 7 ,
Received = 7 Lost = 0 (0% loss),  Approximate round
trip times in milli-seconds:     Minimum = 2.87 ms,
Maximum = 23.9ms , Average =12ms
```

How to Configure Site-to-site IPSec VPN with FortiGate

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZYWALL/USG and a FortiGate router. The example instructs how to configure the VPN tunnel between each site. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



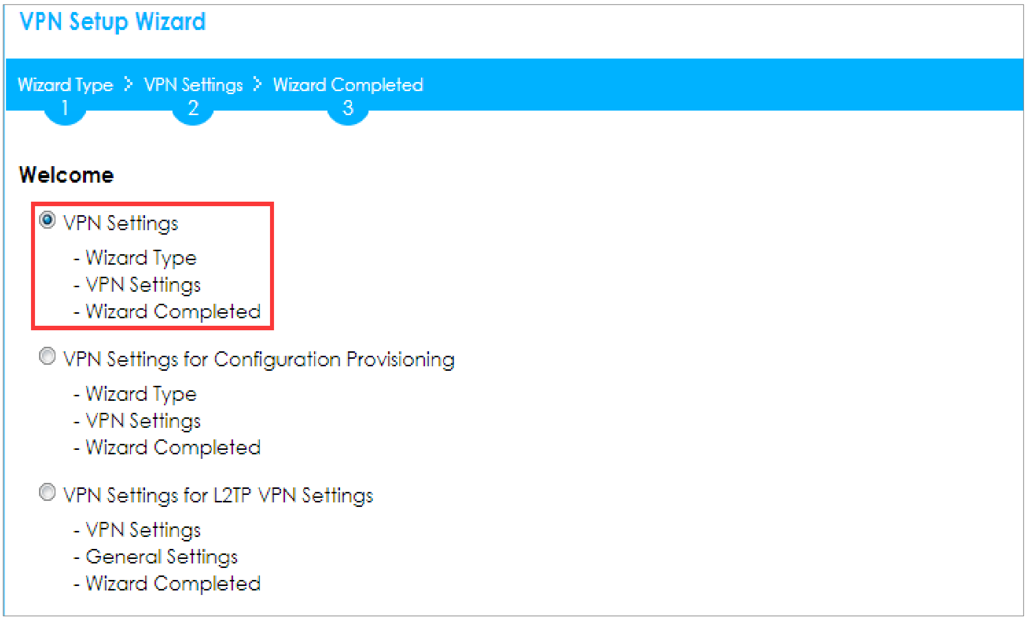
ZyWALL Site-to-site IPSec VPN with FortiGate Connected

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and FortiGate 100D (Firmware Version:

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Welcome

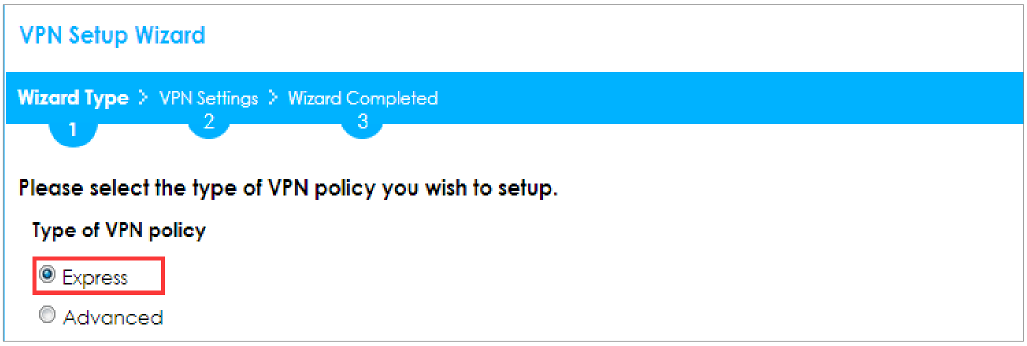
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Please select the type of VPN policy you wish to setup.

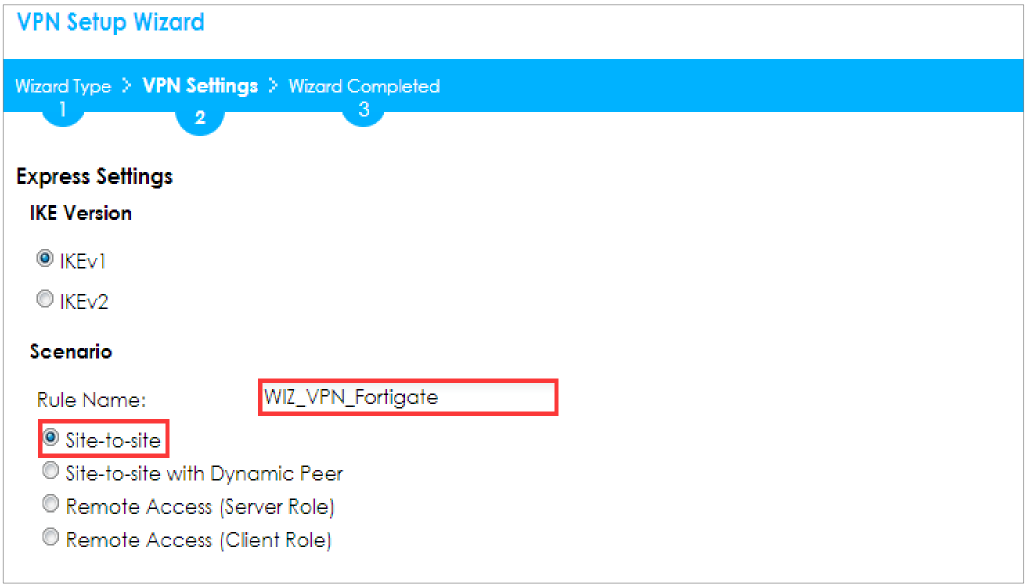
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: WIZ_VPN_Fortigate

● Site-to-site

○ Site-to-site with Dynamic Peer

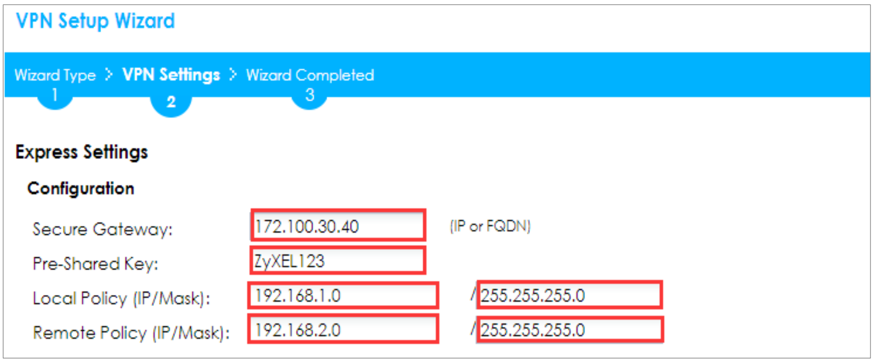
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the FortiGate's WAN IP address (in the example, 172.100.30.40). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the FortiGate.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



Express Settings

Configuration

Secure Gateway: 172.100.30.40 (IP or FQDN)

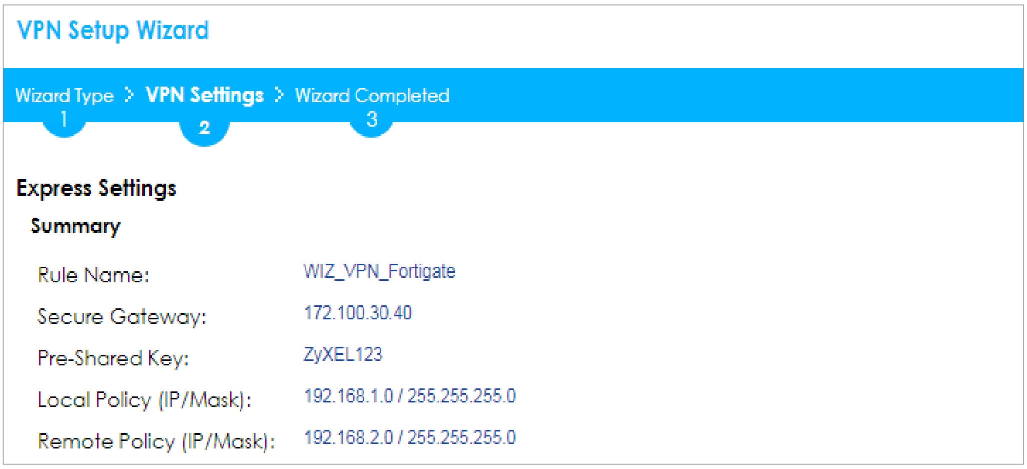
Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.2.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



Express Settings

Summary

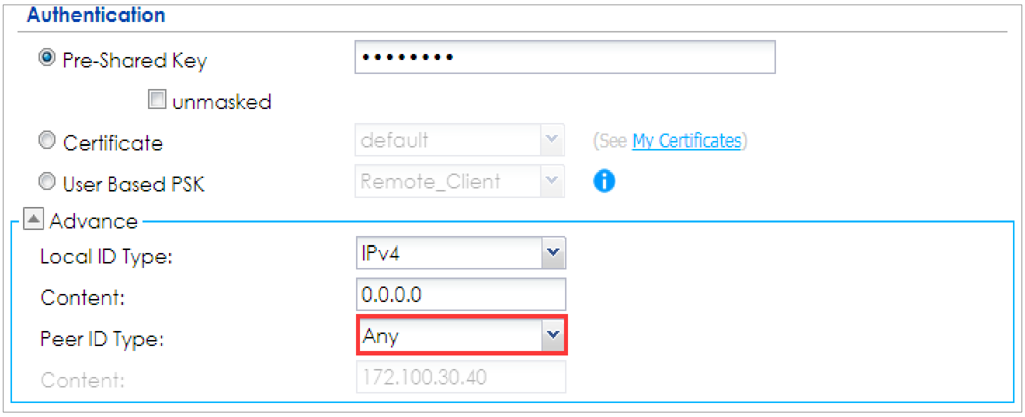
Rule Name:	WIZ_VPN_Fortigate
Secure Gateway:	172.100.30.40
Pre-Shared Key:	ZyXEL123
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.2.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

● Pre-Shared Key: ••••••••

□ unmasked

○ Certificate: default (See My Certificates)

○ User Based PSK: Remote_Client

Advance

Local ID Type: IPv4

Content: 0.0.0.0

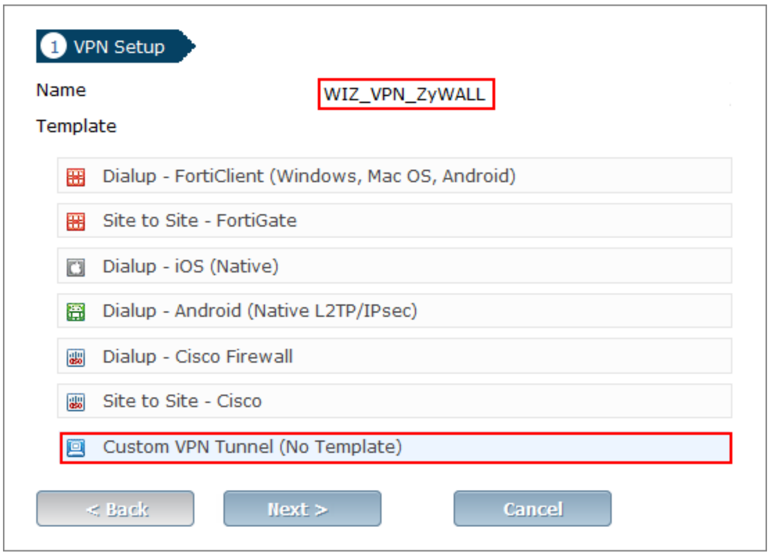
Peer ID Type: Any

Content: 172.100.30.40

Set Up the IPSec VPN Tunnel on the FortiGate

In the FortiGate **VPN > IPsec > Wizard > Custom VPN Tunnel (No Template)**, use the **VPN Setup** to create a **Site-to-site VPN** rule **Name**.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template)



1 VPN Setup

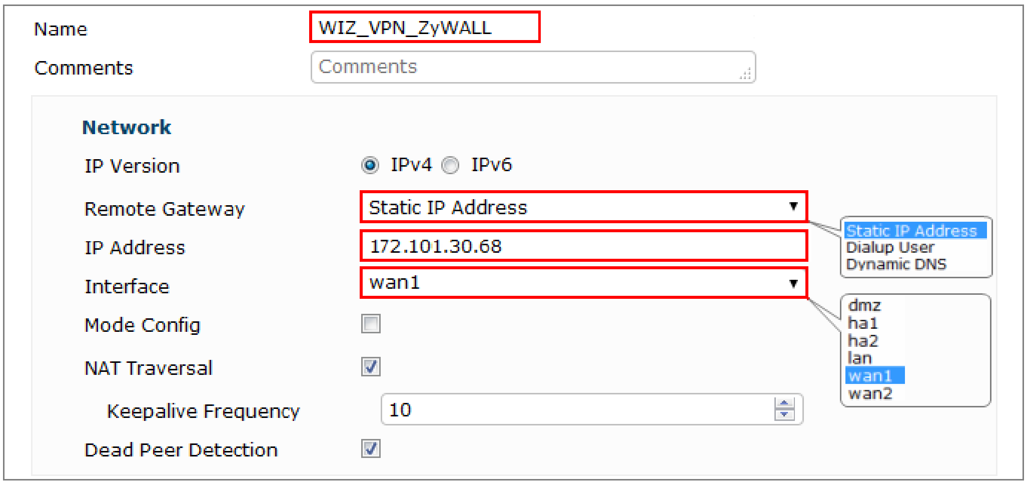
Name: WIZ_VPN_ZyWALL

Template

- Dialup - FortiClient (Windows, Mac OS, Android)
- Site to Site - FortiGate
- Dialup - iOS (Native)
- Dialup - Android (Native L2TP/IPsec)
- Dialup - Cisco Firewall
- Site to Site - Cisco
- Custom VPN Tunnel (No Template)

Type the **Name** used to identify this VPN connection, configure **Remote Gateway** IP as the peer ZyWALL/USG's WAN IP address. Select the **Interface** which is connected to the Internet.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template) > Network



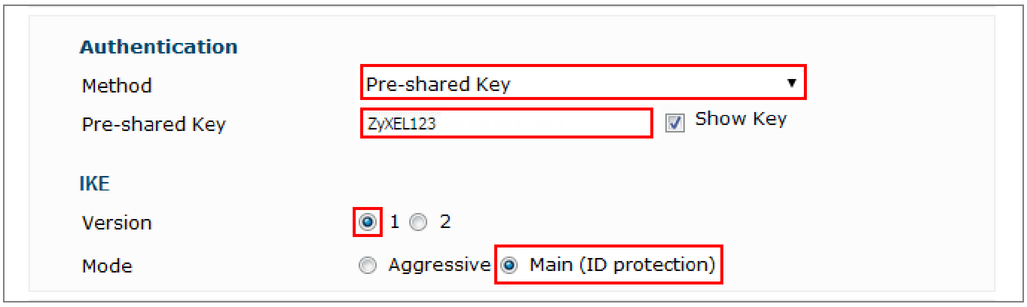
Name	WIZ_VPN_ZyWALL
Comments	Comments

Network

IP Version	● IPv4 ○ IPv6
Remote Gateway	Static IP Address ▾
IP Address	172.101.30.68
Interface	wan1 ▾
Mode Config	□
NAT Traversal	☑
Keepalive Frequency	10
Dead Peer Detection	☑

Go to **Authentication** section, enter **Pre-shared Key** and choose negotiation **Mode** the same as the peer ZyWALL/USG's.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template) > Authentication



Authentication

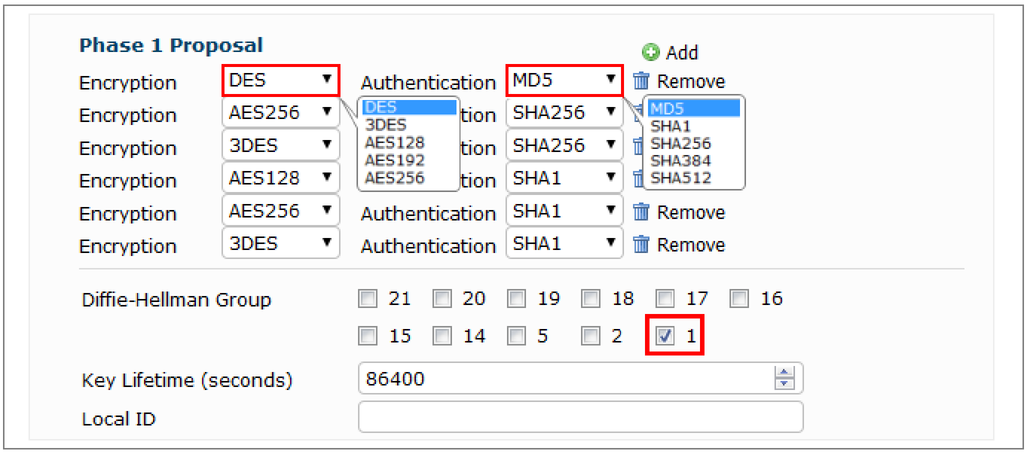
Method	Pre-shared Key ▾
Pre-shared Key	ZyXEL123 ☑ Show Key

IKE

Version	● 1 ○ 2
Mode	○ Aggressive ● Main (ID protection)

Configure Phase 1 Proposal and Diffie-Hellman Group as the peer ZyWALL/USG Advanced Settings' **Phase 1 Settings > Proposal** and **Key Group**.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template) > Phase 1 Proposal



Phase 1 Proposal

Encryption	DES	Authentication	MD5	Remove
Encryption	AES256	Authentication	SHA256	Remove
Encryption	3DES	Authentication	SHA256	Remove
Encryption	AES128	Authentication	SHA1	Remove
Encryption	AES256	Authentication	SHA1	Remove
Encryption	3DES	Authentication	SHA1	Remove

Diffie-Hellman Group □ 21 □ 20 □ 19 □ 18 □ 17 □ 16 □ 15 □ 14 □ 5 □ 2 ☑ 1

Key Lifetime (seconds) 86400

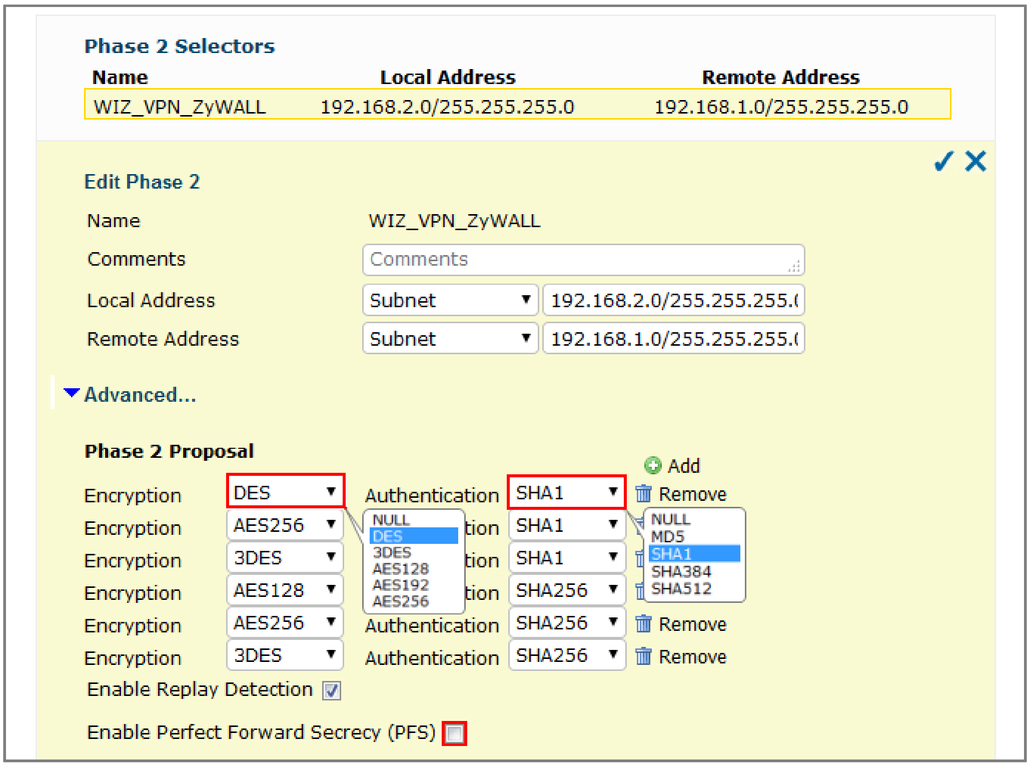
Local ID

Go to **Phase 2 Selectors > Advanced** and configure **Phase 2 Proposal** as the peer ZyWALL/USG Advanced Settings' **Phase 2 Settings > Proposal**.

Set **Local Address** to be the IP address range of the network connected to the FortiGate and **Remote Address** to be the IP address range of the network connected to the ZyWALL/USG.

Make sure you uncheck **Enable Perfect Forward Secrecy (PFS)** if this function is disabled in the peer ZyWALL/USG.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template) > Phase 2 Selectors



Phase 2 Selectors

Name	Local Address	Remote Address
WIZ_VPN_ZyWALL	192.168.2.0/255.255.255.0	192.168.1.0/255.255.255.0

Edit Phase 2

Name	WIZ_VPN_ZyWALL
Comments	Comments
Local Address	Subnet ▾ 192.168.2.0/255.255.255.(
Remote Address	Subnet ▾ 192.168.1.0/255.255.255.(

▾ Advanced...

Phase 2 Proposal

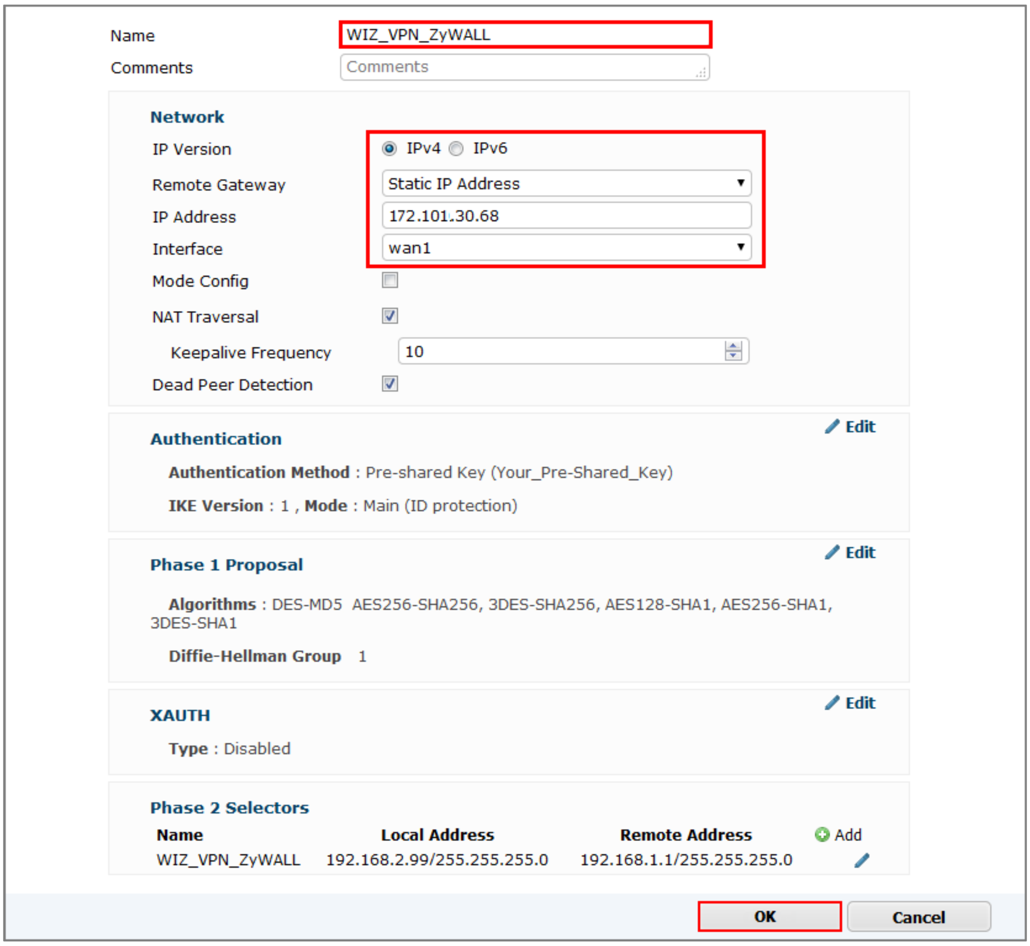
				Add
Encryption	DES ▾	Authentication	SHA1 ▾	Remove
Encryption	AES256 ▾	tion	SHA1 ▾	
Encryption	3DES ▾	tion	SHA1 ▾	
Encryption	AES128 ▾	tion	SHA256 ▾	
Encryption	AES256 ▾	Authentication	SHA256 ▾	Remove
Encryption	3DES ▾	Authentication	SHA256 ▾	Remove

Enable Replay Detection ☑

Enable Perfect Forward Secrecy (PFS) □

This screen provides a summary of the VPN tunnel. Click **OK** to exit the configuration page.

VPN > IPsec > Wizard > Custom VPN Tunnel (No Template)



Name: WIZ_VPN_ZyWALL

Comments: Comments

Network

IP Version: ● IPv4 ○ IPv6

Remote Gateway: Static IP Address

IP Address: 172.101.30.68

Interface: wan1

Mode Config: □

NAT Traversal: ☑

Keepalive Frequency: 10

Dead Peer Detection: ☑

Authentication

Authentication Method : Pre-shared Key (Your_Pre-Shared_Key)

IKE Version : 1 , **Mode** : Main (ID protection)

Phase 1 Proposal

Algorithms : DES-MD5 AES256-SHA256, 3DES-SHA256, AES128-SHA1, AES256-SHA1, 3DES-SHA1

Diffie-Hellman Group 1

XAUTH

Type : Disabled

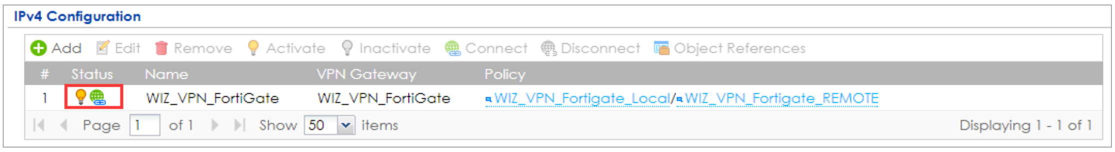
Phase 2 Selectors

Name	Local Address	Remote Address
WIZ_VPN_ZyWALL	192.168.2.99/255.255.255.0	192.168.1.1/255.255.255.0

Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

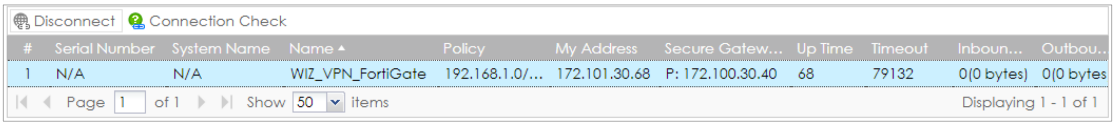
CONFIGURATION > VPN > IPSec VPN > VPN Connection



#	Status	Name	VPN Gateway	Policy
1	💡🌐	WIZ_VPN_FortiGate	WIZ_VPN_FortiGate	WIZ_VPN_Fortigate_Local/WIZ_VPN_Fortigate_REMOTE

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** traffic.

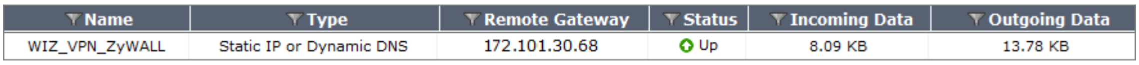
MONITOR > VPN Monitor > IPSec



#	Serial Number	System Name	Name ▲	Policy	My Address	Secure Gatew...	Up Time	Timeout	Inboun...	Outbou..
1	N/A	N/A	WIZ_VPN_FortiGate	192.168.1.0/...	172.101.30.68	P: 172.100.30.40	68	79132	0(0 bytes)	0(0 bytes

Go to FortiGate **VPN > Monitor > IPsec Monitor** and check the tunnel **Status** is up and **Incoming Data/Outgoing Data** traffic.

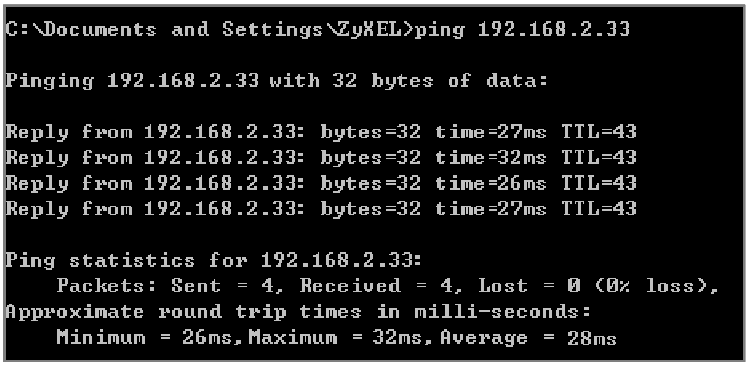
VPN > Monitor > IPsec Monitor



Name	Type	Remote Gateway	Status	Incoming Data	Outgoing Data
WIZ_VPN_ZyWALL	Static IP or Dynamic DNS	172.101.30.68	Up	8.09 KB	13.78 KB

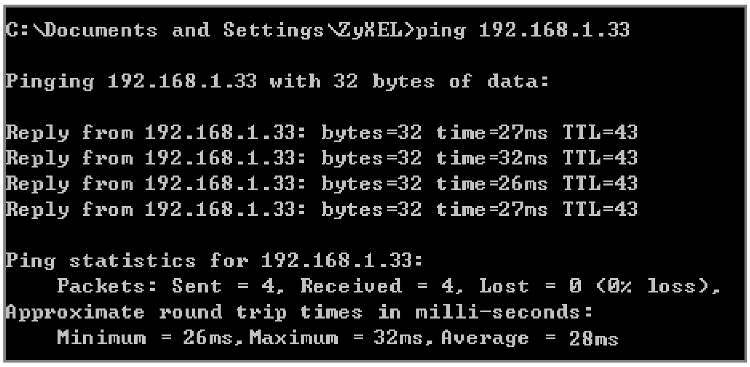
To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC behind ZyWALL/USG > Window 7 > cmd > ping 192.168.2.33



```
C:\Documents and Settings\ZyXEL>ping 192.168.2.33

Pinging 192.168.2.33 with 32 bytes of data:

Reply from 192.168.2.33: bytes=32 time=27ms TTL=43
Reply from 192.168.2.33: bytes=32 time=32ms TTL=43
Reply from 192.168.2.33: bytes=32 time=26ms TTL=43
Reply from 192.168.2.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.2.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

PC behind FortiGate> Window 7 > cmd > ping 192.168.1.33

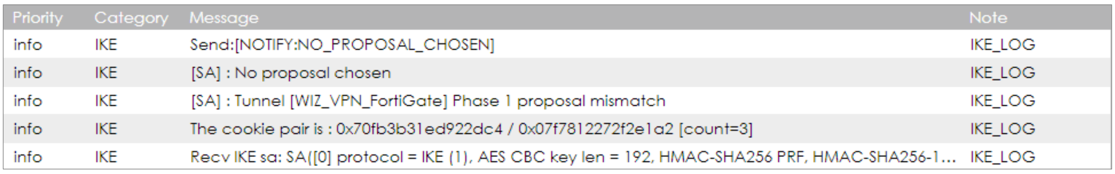


```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG and FortiGate must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

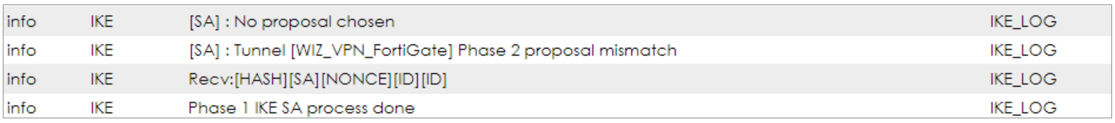
MONITOR > Log



Priority	Category	Message	Note
info	IKE	Send:[NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [WIZ_VPN_FortiGate] Phase 1 proposal mismatch	IKE_LOG
info	IKE	The cookie pair is : 0x70fb3b31ed922dc4 / 0x07f7812272f2e1a2 [count=3]	IKE_LOG
info	IKE	Recv IKE sa: SA([0] protocol = IKE (1), AES CBC key len = 192, HMAC-SHA256 PRF, HMAC-SHA256-1…	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG and FortiGate Phase 2 Settings. Both ZyWALL/USG and FortiGate must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log



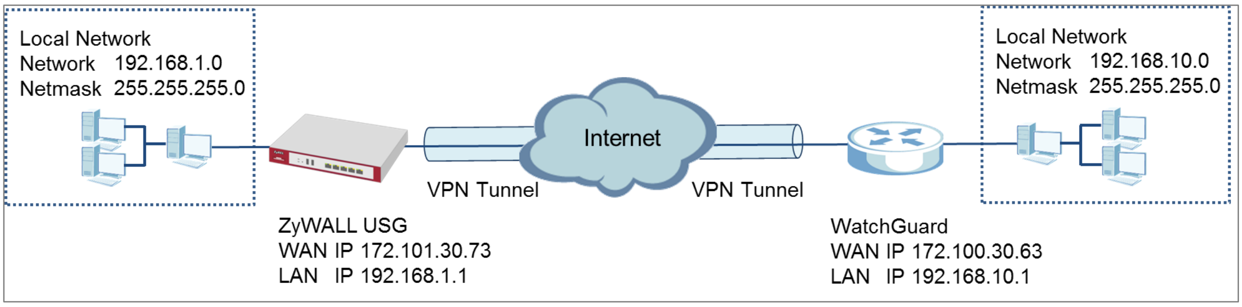
```
info    IKE    [SA] : No proposal chosen                                       IKE_LOG
info    IKE    [SA] : Tunnel [WIZ_VPN_FortiGate] Phase 2 proposal mismatch     IKE_LOG
info    IKE    Recv:[HASH][SA][NONCE][ID][ID]                                  IKE_LOG
info    IKE    Phase 1 IKE SA process done                                     IKE_LOG
```

Make sure the both ZyWALL/USG and FortiGate security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure Site-to-site IPSec VPN with WatchGuard

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZYWALL/USG and a WatchGuard router. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



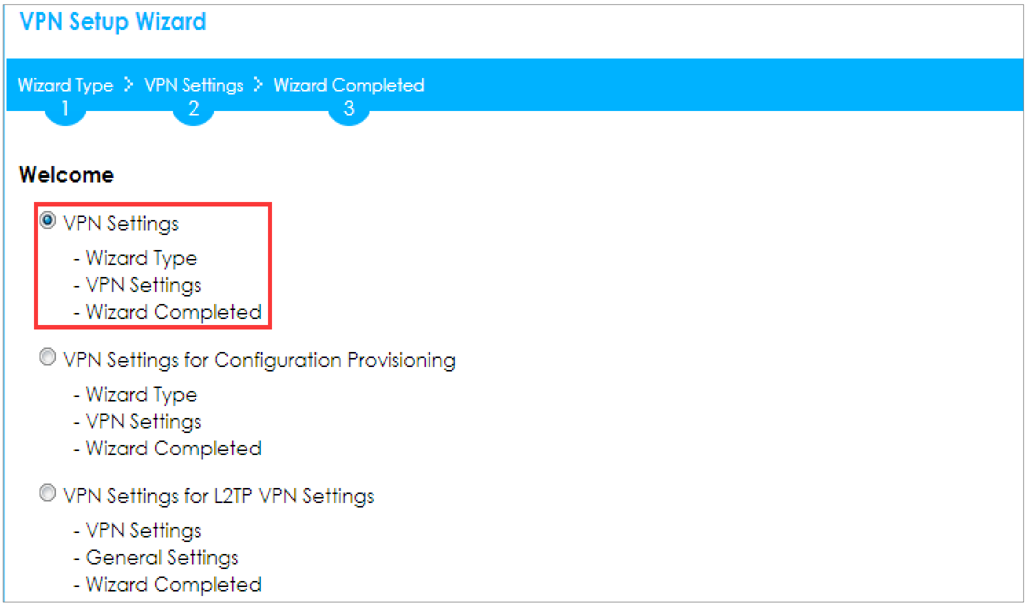
ZyWALL Site-to-site IPSec VPN with WatchGuard Connected

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and WatchGuard XTM 515 (Firmware Version: 11.10.4).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the WatchGuard. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

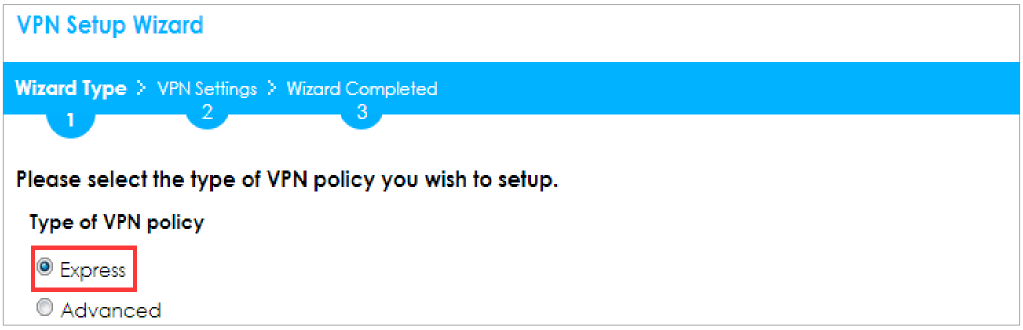
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

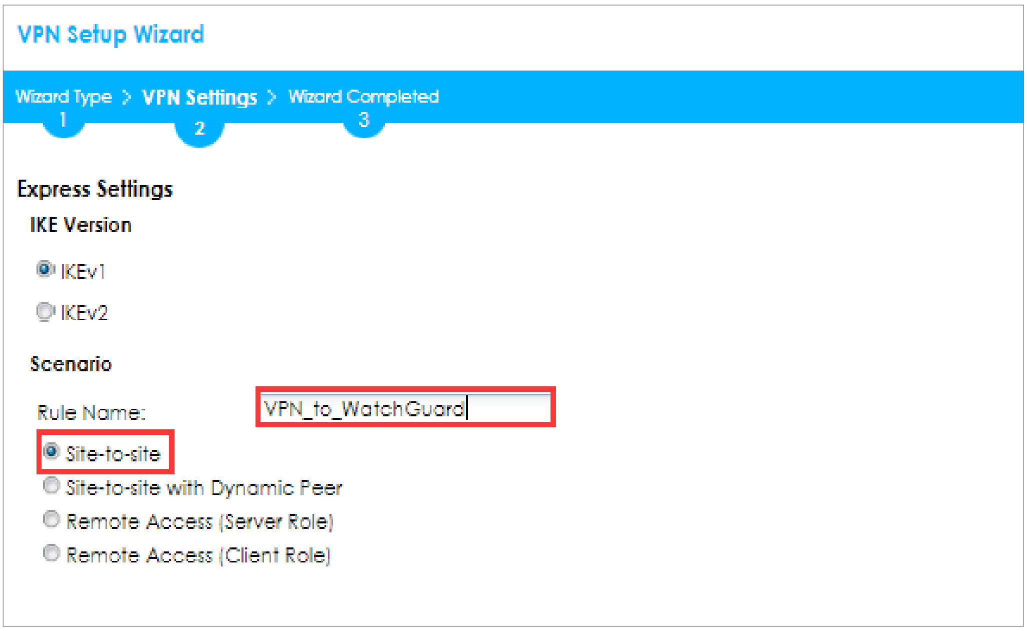
Please select the type of VPN policy you wish to setup.

Type of VPN policy

● Express
○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: VPN_to_WatchGuard

● Site-to-site

○ Site-to-site with Dynamic Peer

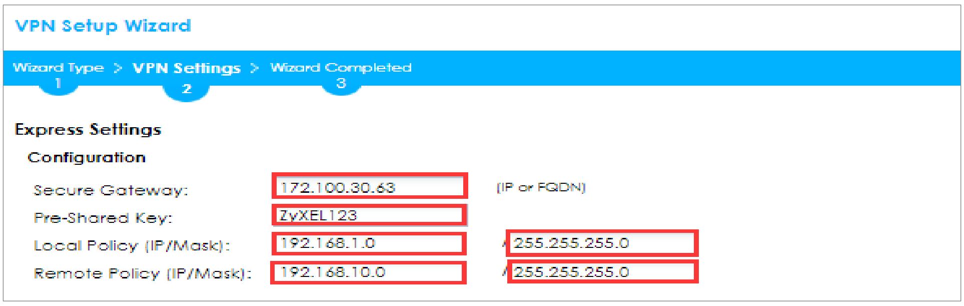
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the WatchGuard's WAN IP address (in the example, 172.100.30.63). Then, type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the WatchGuard. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



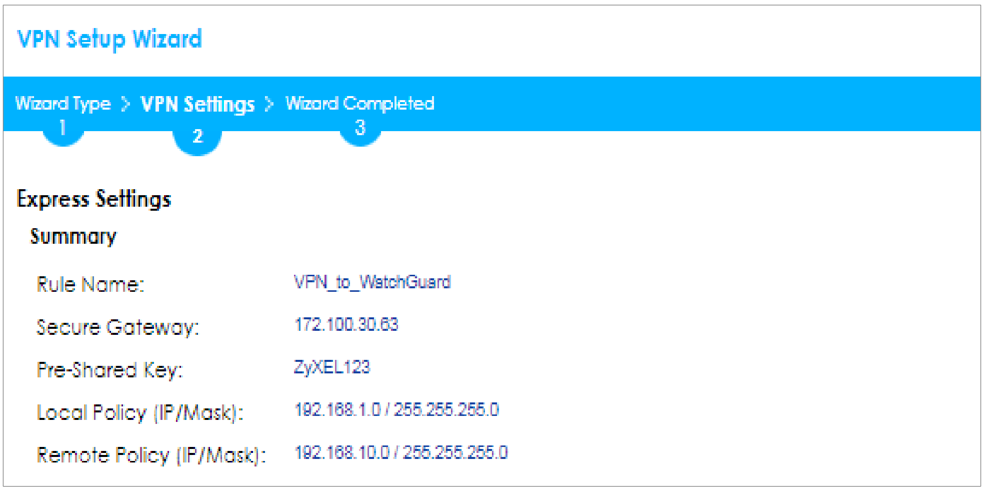
Express Settings

Configuration

Secure Gateway:	172.100.30.63	(IP or FQDN)
Pre-Shared Key:	ZyXEL123	
Local Policy (IP/Mask):	192.168.1.0	/ 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0	/ 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



VPN Setup Wizard

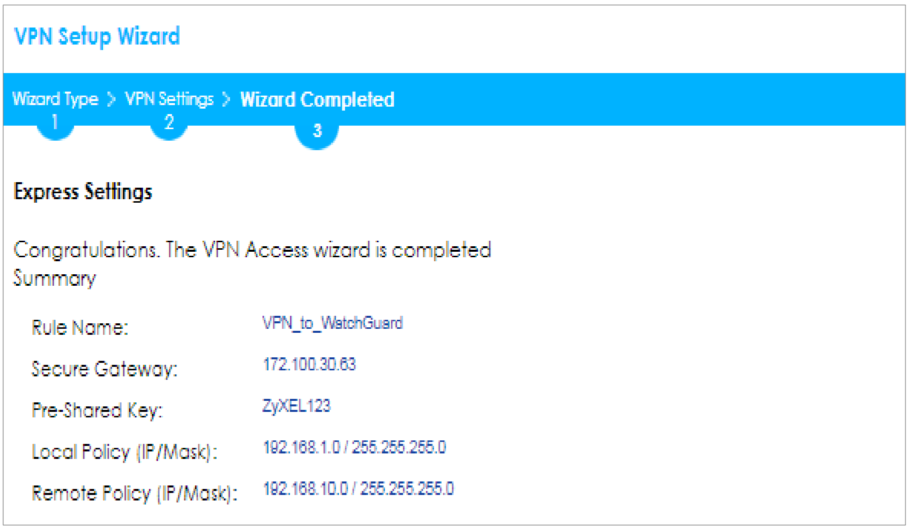
Express Settings

Summary

Rule Name:	VPN_to_WatchGuard
Secure Gateway:	172.100.30.63
Pre-Shared Key:	ZyXEL123
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard completed



VPN Setup Wizard

Express Settings

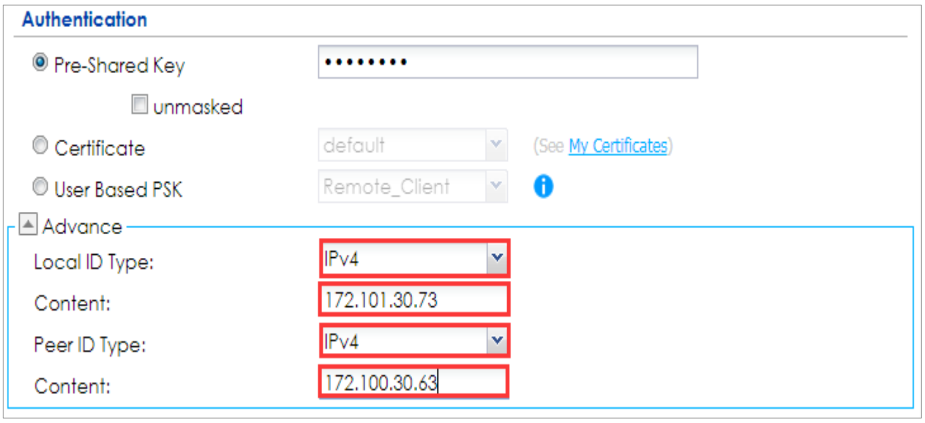
Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	VPN_to_WatchGuard
Secure Gateway:	172.100.30.63
Pre-Shared Key:	ZyXEL123
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, click **Show Advanced Settings**. Configure **Authentication > Local ID Type** as **IPv4** and set the **Content** as your ZyWALL/USG's **WAN IP Address** (in the example, 172.101.30.73). Then, configure **Authentication > Remote ID Type** as **IPv4** and set the **Content** as your WatchGuard's **External IP Address** (in the example, 172.100.30.63). Click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

● Pre-Shared Key: ••••••••

□ unmasked

○ Certificate: default (See My Certificates)

○ User Based PSK: Remote_Client

Advance

Local ID Type: IPv4

Content: 172.101.30.73

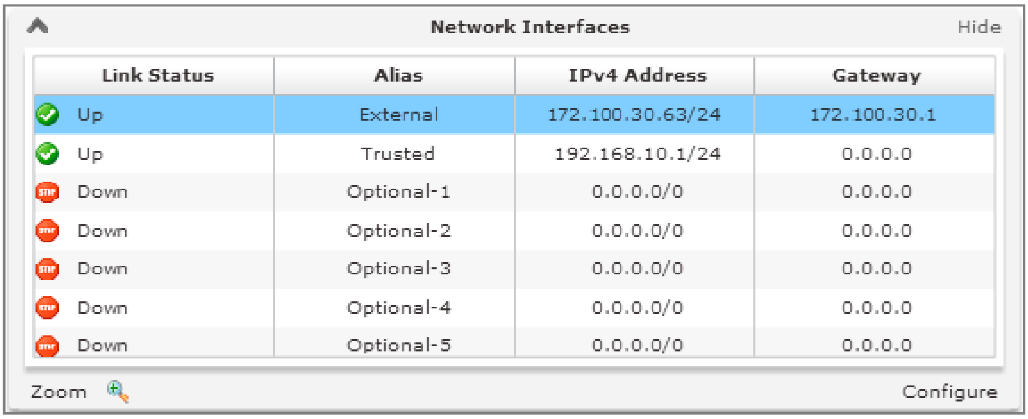
Peer ID Type: IPv4

Content: 172.100.30.63

Set Up the IPSec VPN Tunnel on the WatchGuard

Go to **Dashboard > Network Interfaces** to check your **External IP Address** (the Internet-facing interface) and **Trusted IP Address** (the Local IP address).

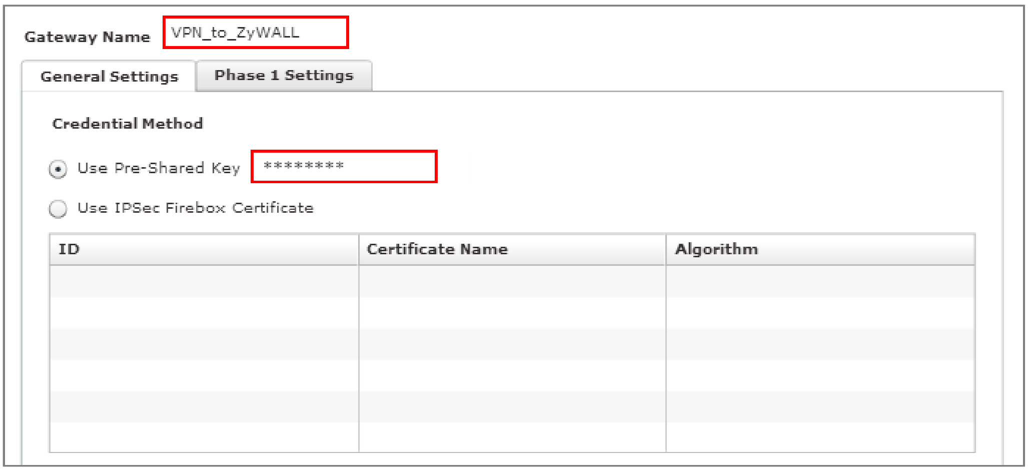
Dashboard > Network Interfaces



Link Status	Alias	IPv4 Address	Gateway
Up	External	172.100.30.63/24	172.100.30.1
Up	Trusted	192.168.10.1/24	0.0.0.0
Down	Optional-1	0.0.0.0/0	0.0.0.0
Down	Optional-2	0.0.0.0/0	0.0.0.0
Down	Optional-3	0.0.0.0/0	0.0.0.0
Down	Optional-4	0.0.0.0/0	0.0.0.0
Down	Optional-5	0.0.0.0/0	0.0.0.0

In the WatchGuard **VPN > Branch Office VPN > Gateway > General Settings** create a Site-to-site VPN **Gateway Name** and set a secure **Pre-Shared Key**.

VPN > Branch Office VPN > Gateway > General Settings > Credential Method



Gateway Name: VPN_to_ZyWALL

Credential Method

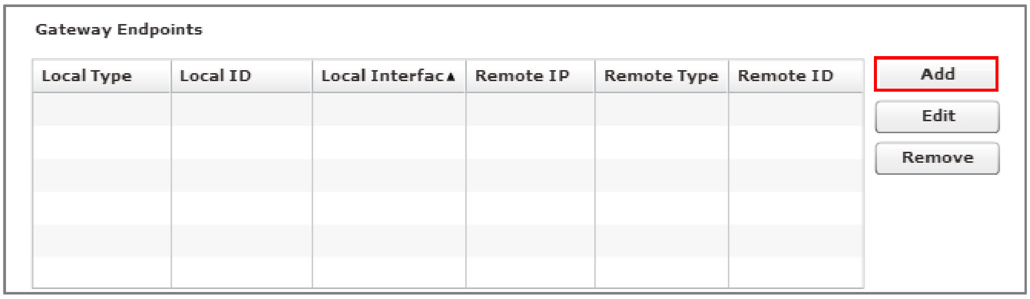
● Use Pre-Shared Key ********

○ Use IPSec Firebox Certificate

ID	Certificate Name	Algorithm

To add a **Gateway Endpoint**, click **Add.**

VPN > Branch Office VPN > Gateway > General Settings > Gateway Endpoints

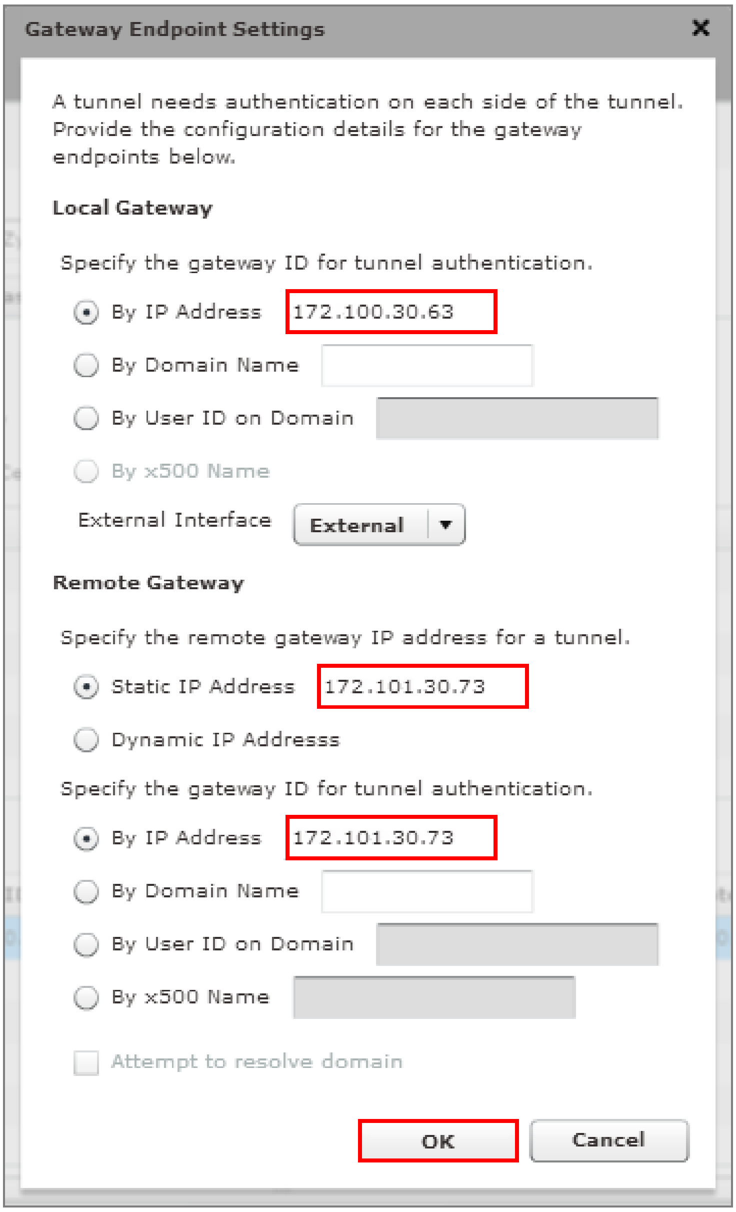


Gateway Endpoints

Local Type	Local ID	Local Interfac▲	Remote IP	Remote Type	Remote ID

The new **Gateway Endpoint** dialog box appears. Configure your **Local Gateway** identity as WatchGuard's **External IP Address** (in the example, 172.100.30.63) and **Remote Gateway** identity as your ZyWALL/USG's **WAN IP Address** (in the example, 172.101.30.73). Click **OK**.

VPN > Branch Office VPN > Gateway > General Settings > Gateway Endpoints



Gateway Endpoint Settings

A tunnel needs authentication on each side of the tunnel. Provide the configuration details for the gateway endpoints below.

Local Gateway

Specify the gateway ID for tunnel authentication.

● By IP Address 172.100.30.63

○ By Domain Name

○ By User ID on Domain

○ By x500 Name

External Interface External

Remote Gateway

Specify the remote gateway IP address for a tunnel.

● Static IP Address 172.101.30.73

○ Dynamic IP Addresss

Specify the gateway ID for tunnel authentication.

● By IP Address 172.101.30.73

○ By Domain Name

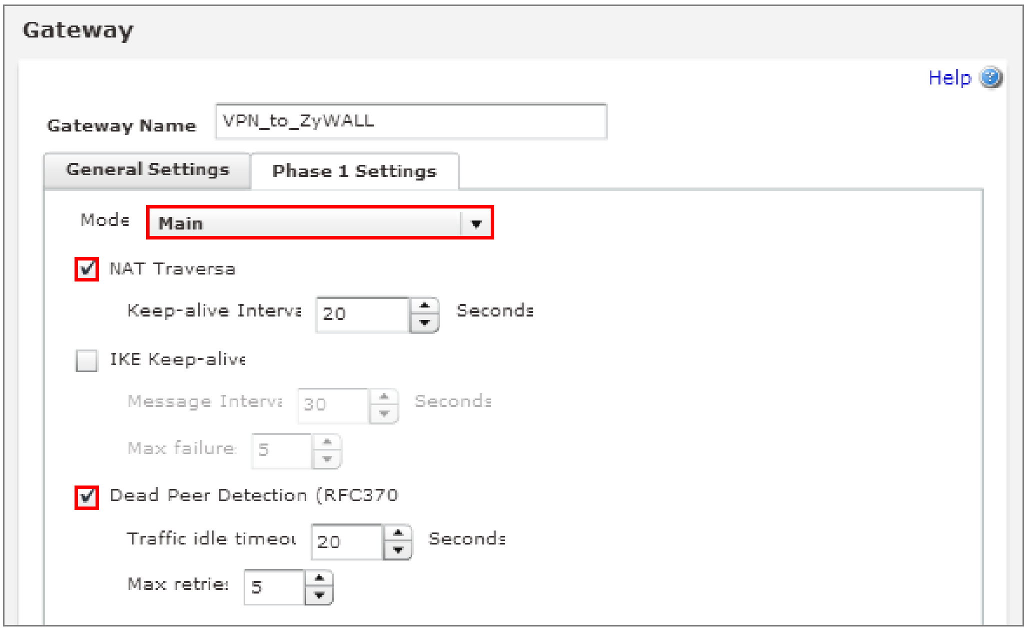
○ By User ID on Domain

○ By x500 Name

□ Attempt to resolve domain

Then, go to **VPN > Branch Office VPN > Gateway > Phase 1 Settings** to select negotiation **Mode** the same as your ZyWALL/USG's Phase 1 Settings. Make sure you enable both **NAT Traversa** and **Dead Peer Detection** options if both options are enabled in the ZyWALL/USG.

VPN > Branch Office VPN > Gateway > Phase 1 Settings



Gateway

Help

Gateway Name: VPN_to_ZyWALL

General Settings | Phase 1 Settings

Mode: Main

☑ NAT Traversa

Keep-alive Interva: 20 Seconds

□ IKE Keep-alive

Message Interva: 30 Seconds

Max failure: 5

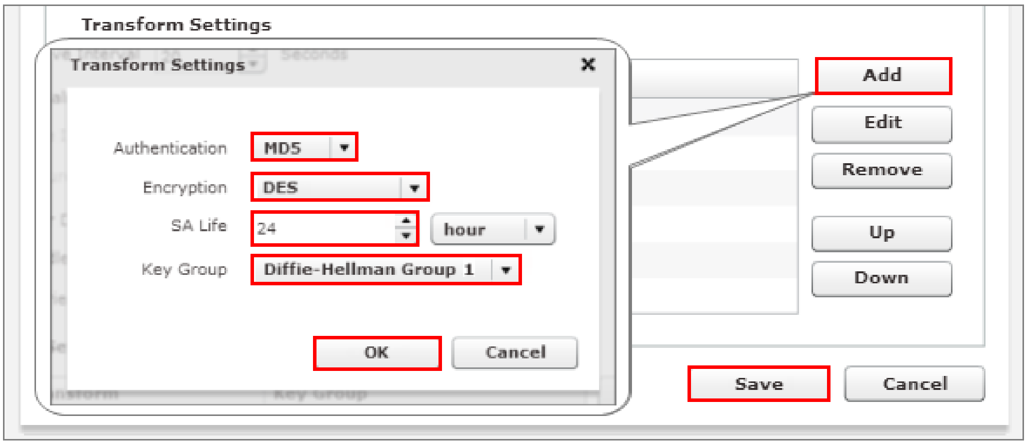
☑ Dead Peer Detection (RFC370

Traffic idle timeou: 20 Seconds

Max retrie: 5

Use **Transform Settings** to create the same security settings as in the ZyWALL/USG Phase 1 settings. Click **OK** and **Save** to exit the **Transform Settings** page.

VPN > Branch Office VPN > Gateway > Phase 1 Settings > Transform Settings



Transform Settings

Transform Settings ×

Authentication: MD5

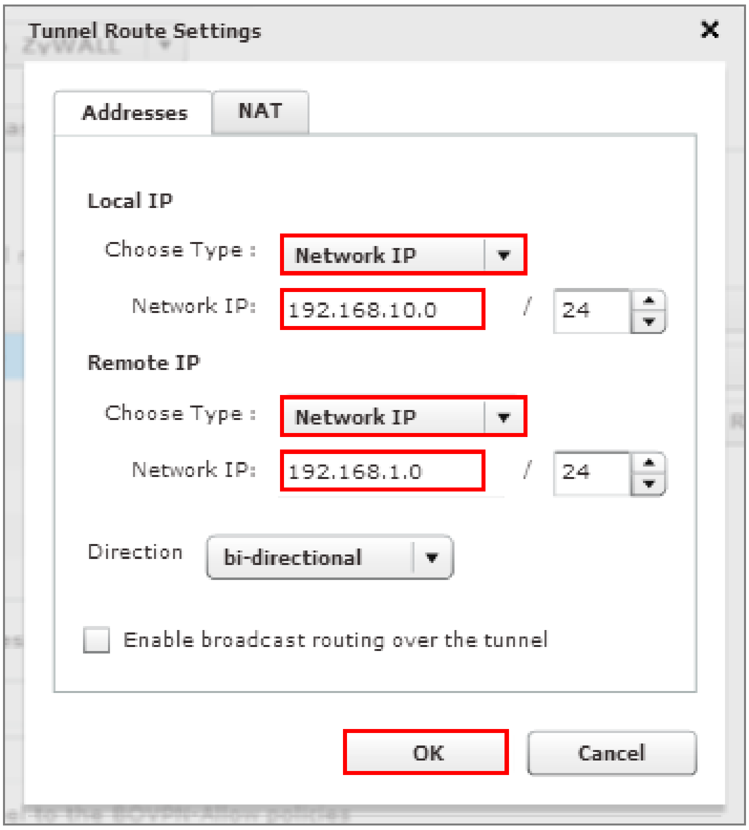
Encryption: DES

SA Life: 24 hour

Key Group: Diffie-Hellman Group 1

Then, go to **VPN > Branch Office VPN > Tunnel** to add a Tunnel Route Settings. In the **Local IP** section, set **the Network IP** to be the IP address range of the network connected to the WatchGuard. In the **Remote IP** section, set **the Network IP** to be the IP address range of the network connected to the ZyWALL/USG. Click **OK**.

VPN > Branch Office VPN > Tunnel > Address



Tunnel Route Settings

Addresses | NAT

Local IP

Choose Type : Network IP

Network IP: 192.168.10.0 / 24

Remote IP

Choose Type : Network IP

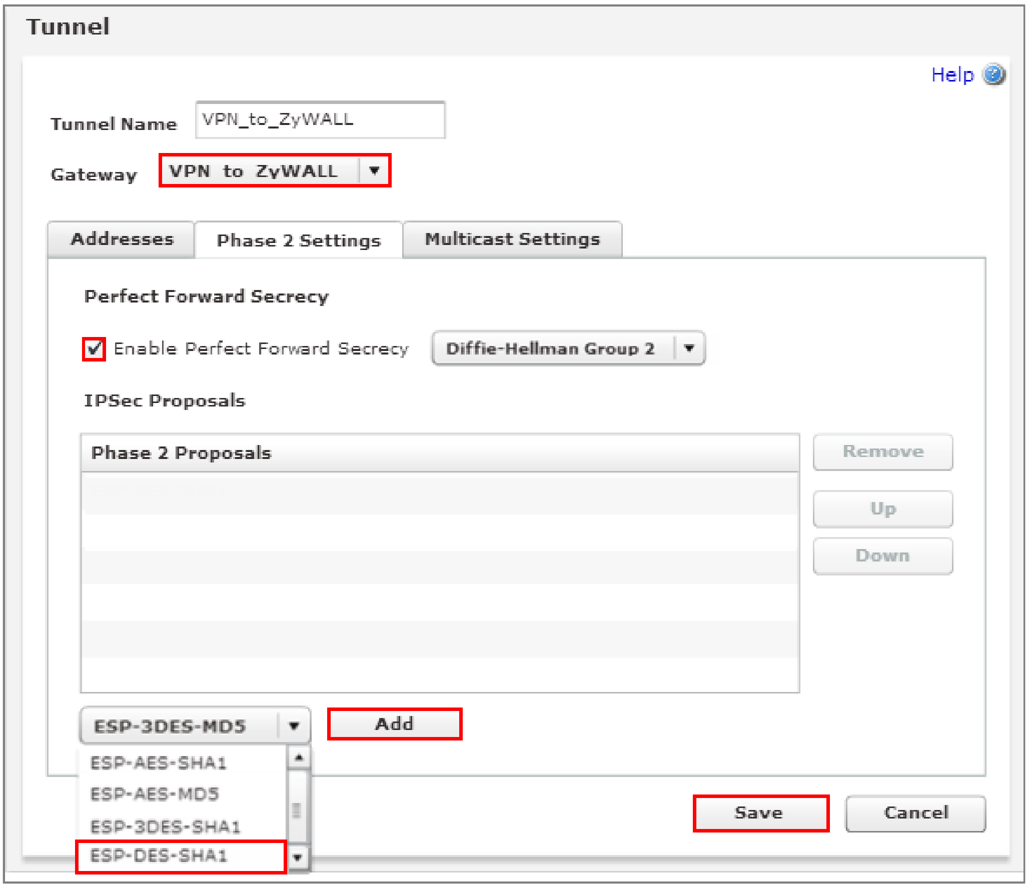
Network IP: 192.168.1.0 / 24

Direction: bi-directional

□ Enable broadcast routing over the tunnel

Go to **VPN > Branch Office VPN > Tunnel > Phase 2 Settings** to create a **Tunnel Name**. Then, select the **Gateway**. Make sure you enable **Perfect Forward Secrecy** and select **Diffie-Hellman Group 2**. Then, scroll down **Phase 2 Proposals** and add the encryption types to match your ZyWALL/USG's **VPN Connection > Phase 2 Settings**. Click **Save**.

VPN > Branch Office VPN > Tunnel > Phase 2 Settings



Tunnel

Tunnel Name: VPN_to_ZyWALL

Gateway: VPN to ZyWALL

Perfect Forward Secrecy

☑ Enable Perfect Forward Secrecy: Diffie-Hellman Group 2

IPSec Proposals

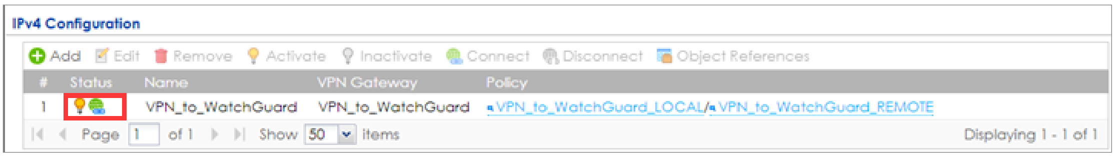
Phase 2 Proposals

ESP-3DES-MD5

Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



IPv4 Configuration

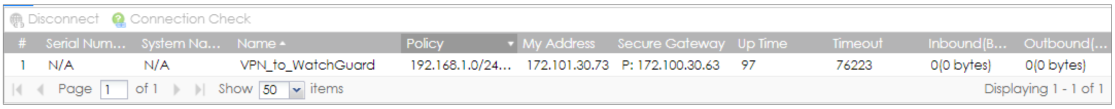
Add Edit Remove Activate Inactivate Connect Disconnect Object References

#	Status	Name	VPN Gateway	Policy
1	●	VPN_to_WatchGuard	VPN_to_WatchGuard	VPN_to_WatchGuard_LOCAL/VPN_to_WatchGuard_REMOTE

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

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec



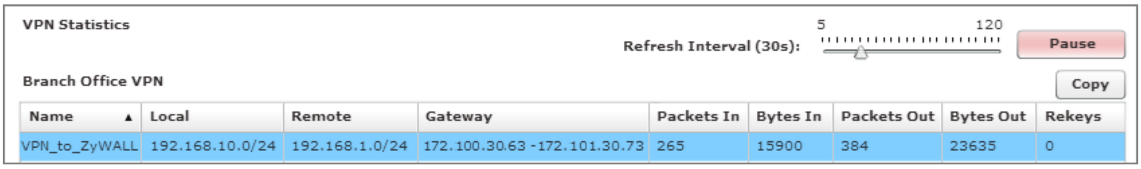
Disconnect Connection Check

#	Serial Num...	System Na...	Name	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound(B...	Outbound(...
1	N/A	N/A	VPN_to_WatchGuard	192.168.1.0/24...	172.101.30.73	P: 172.100.30.63	97	76223	0(0 bytes)	0(0 bytes)

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

Go to WatchGuard **System Status > VPN Statistics > Branch Office VPN** and check the tunnel **Status** is up and **Bytes In** (Incoming Data) and **Bytes Out** (Outgoing Data).

System Status > VPN Statistics > Branch Office



VPN Statistics

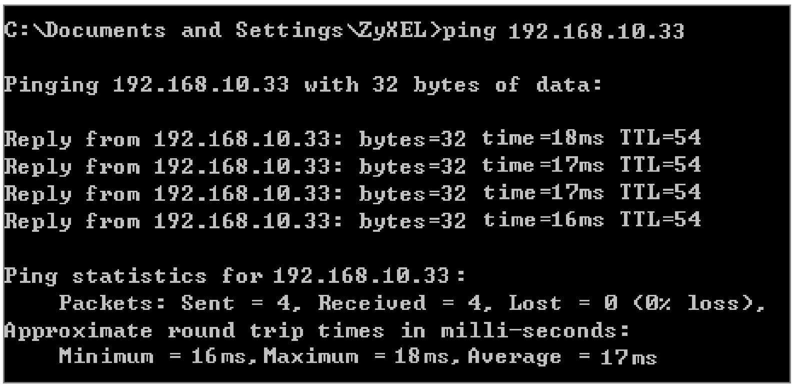
Refresh Interval (30s): 5 120

Branch Office VPN

Name	Local	Remote	Gateway	Packets In	Bytes In	Packets Out	Bytes Out	Rekeys
VPN_to_ZyWALL	192.168.10.0/24	192.168.1.0/24	172.100.30.63 -172.101.30.73	265	15900	384	23635	0

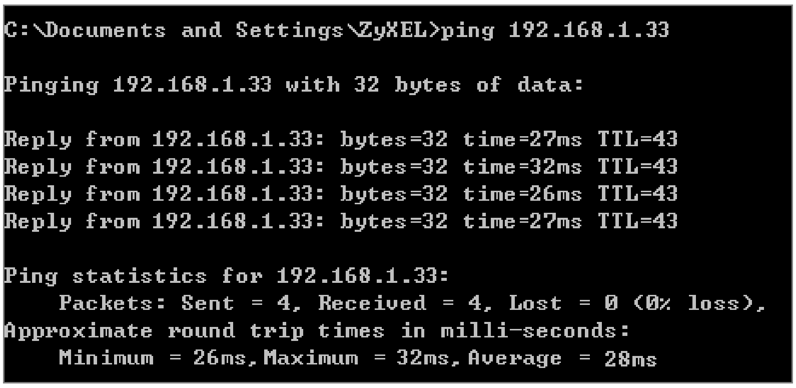
To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC behind ZyWALL/USG > Window 7 > cmd > ping 192.168.10.33



```
C:\Documents and Settings\ZyXEL>ping 192.168.10.33

Pinging 192.168.10.33 with 32 bytes of data:

Reply from 192.168.10.33: bytes=32 time=18ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.10.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC behind WatchGuard> Window 7 > cmd > ping 192.168.1.33

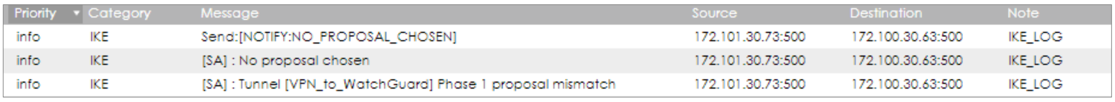


```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG and WatchGuard must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

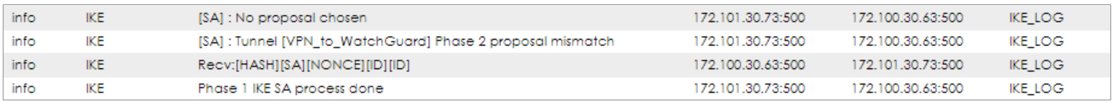
MONITOR > Log



Priority	Category	Message	Source	Destination	Note
info	IKE	Send:[NOTIFY:NO_PROPOSAL_CHOSEN]	172.101.30.73:500	172.100.30.63:500	IKE_LOG
info	IKE	[SA] : No proposal chosen	172.101.30.73:500	172.100.30.63:500	IKE_LOG
info	IKE	[SA] : Tunnel [VPN_to_WatchGuard] Phase 1 proposal mismatch	172.101.30.73:500	172.100.30.63:500	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG and WatchGuard Phase 2 Settings. Both ZyWALL/USG and WatchGuard must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log



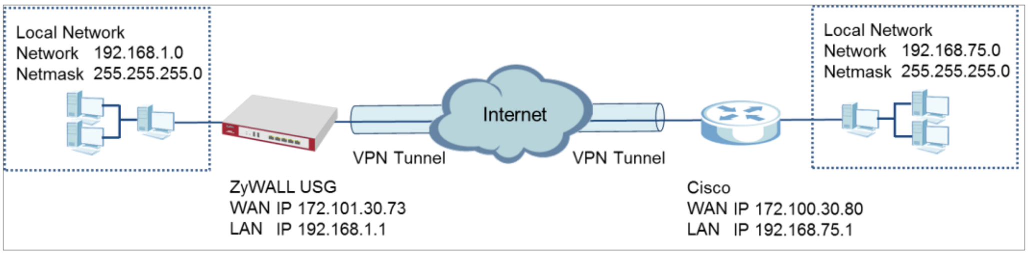
```
info    IKE    [SA] : No proposal chosen                                  172.101.30.73:500    172.100.30.63:500    IKE_LOG
info    IKE    [SA] : Tunnel [VPN_to_WatchGuard] Phase 2 proposal mismatch  172.101.30.73:500    172.100.30.63:500    IKE_LOG
info    IKE    Recv:[HASH][SA][NONCE][ID][ID]                             172.100.30.63:500    172.101.30.73:500    IKE_LOG
info    IKE    Phase 1 IKE SA process done                                172.101.30.73:500    172.100.30.63:500    IKE_LOG
```

Make sure the both ZyWALL/USG and WatchGuard security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure Site-to-site IPSec VPN with Cisco

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZYWALL/USG and a Cisco router. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



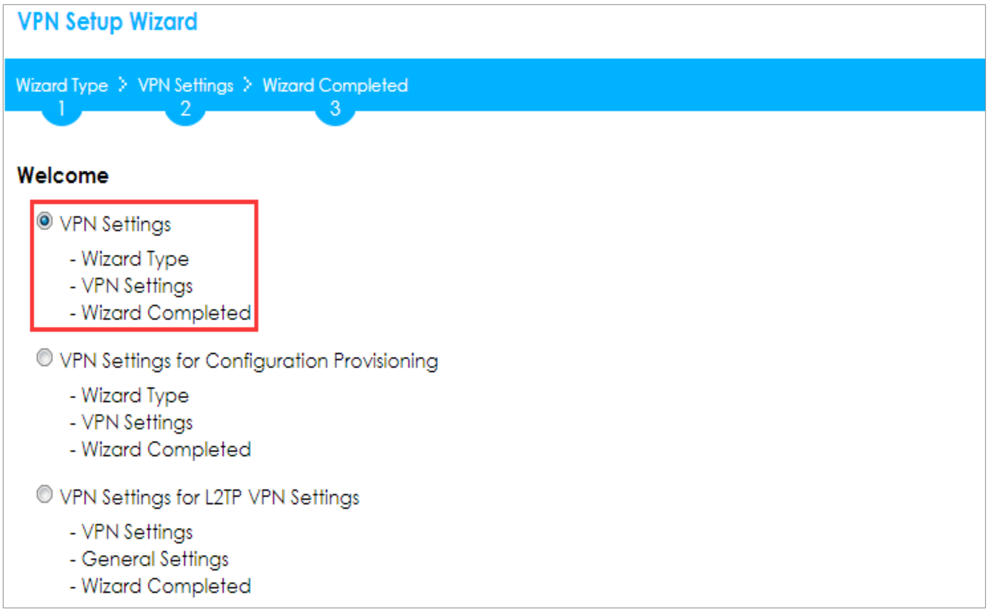
ZyWALL Site-to-site IPSec VPN with Cisco Connected

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and ISA500 (Firmware Version: 1.0.3).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the Cisco. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Welcome

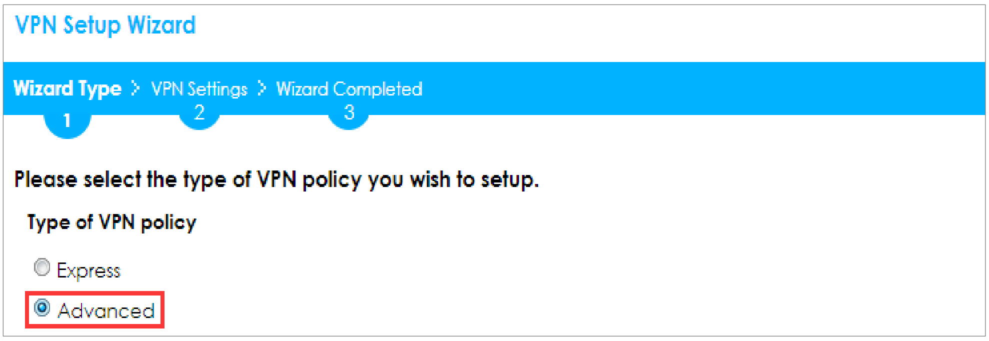
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Please select the type of VPN policy you wish to setup.

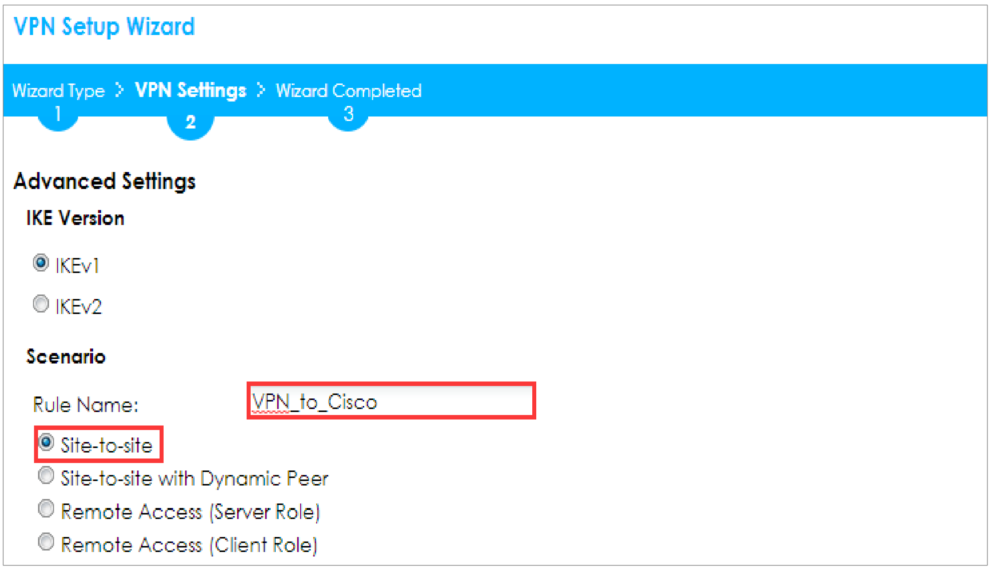
Type of VPN policy

○ Express

● Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



Advanced Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: VPN_to_Cisco

● Site-to-site

○ Site-to-site with Dynamic Peer

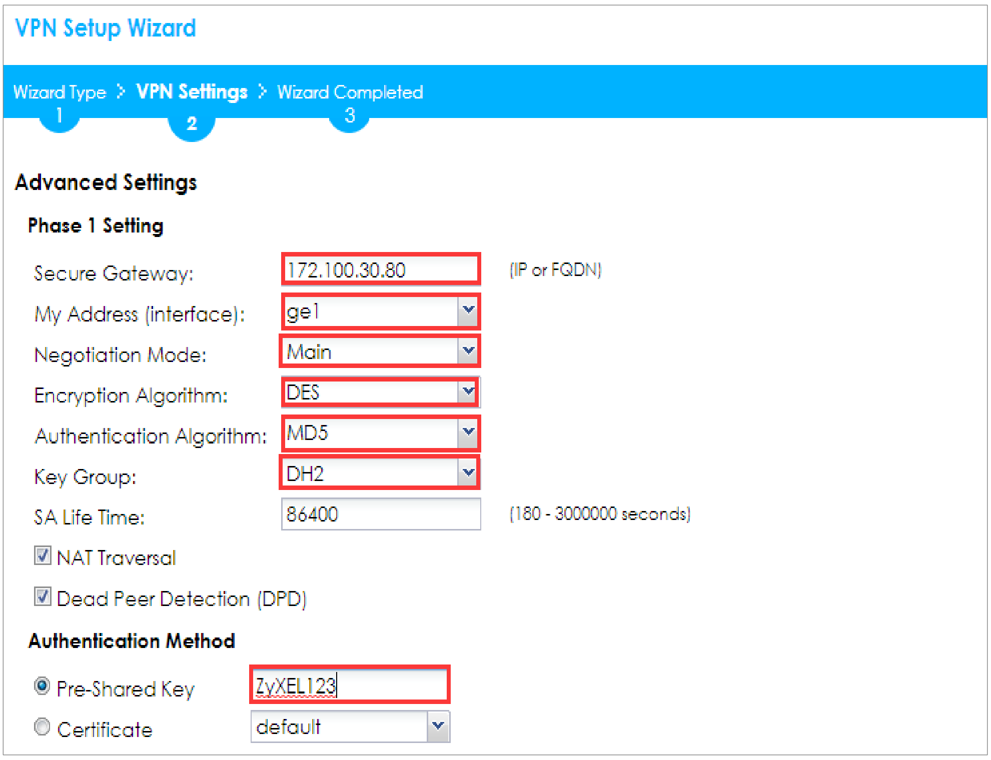
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the Cisco's Gateway IP address (in the example, 172.100.30.80); select **My Address** to be the interface connected to the Internet.

Set the desired **Negotiation**, **Encryption**, **Authentication**, **Key Group** and **SA Life Time** settings. Type a secure **Pre-Shared Key** (8-32 characters) which must match your Cisco **Pre-Shared Key**. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Phase 1 Setting)



Advanced Settings

Phase 1 Setting

Secure Gateway: 172.100.30.80 (IP or FQDN)

My Address (interface): ge1

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

Key Group: DH2

SA Life Time: 86400 (180 - 3000000 seconds)

☑ NAT Traversal

☑ Dead Peer Detection (DPD)

Authentication Method

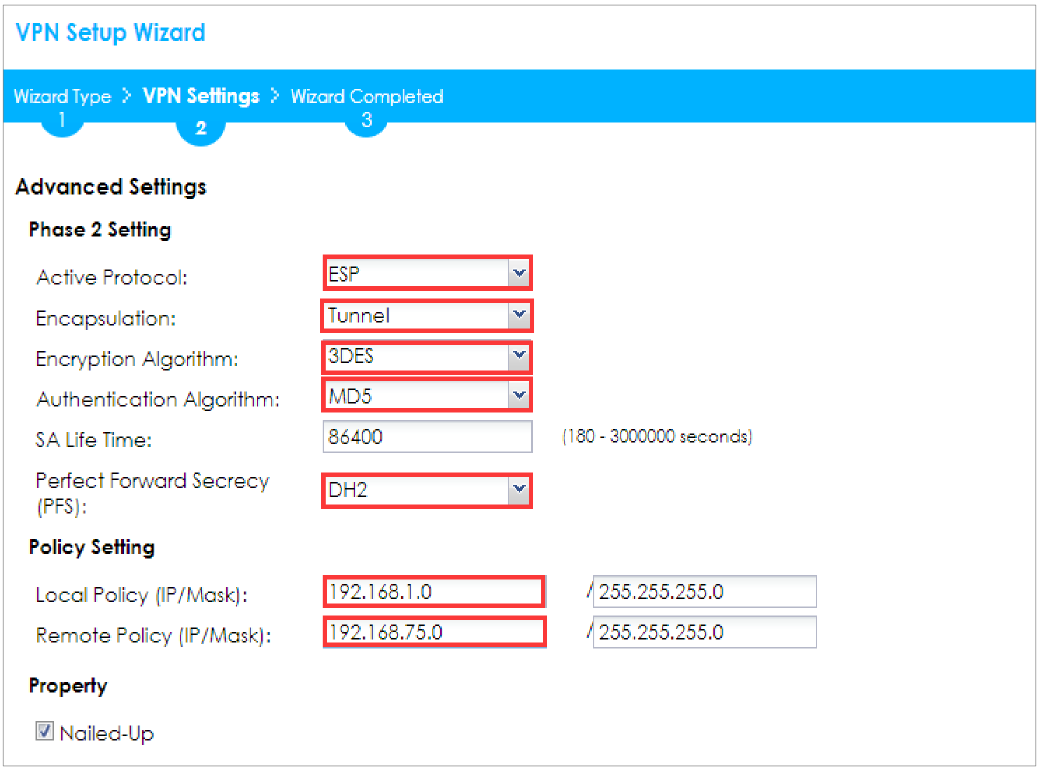
● Pre-Shared Key ZyXEL123

○ Certificate default

Continue to **Phase 2 Settings** to select the desired **Encapsulation**, **Encryption**, **Authentication**, and **Perfect Forward Secrecy (PFS)** settings.

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the Cisco. Click **OK**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Phase 2 Setting)



VPN Setup Wizard

Advanced Settings

Phase 2 Setting

Active Protocol:	ESP	
Encapsulation:	Tunnel	
Encryption Algorithm:	3DES	
Authentication Algorithm:	MD5	
SA Life Time:	86400	(180 - 3000000 seconds)
Perfect Forward Secrecy (PFS):	DH2	

Policy Setting

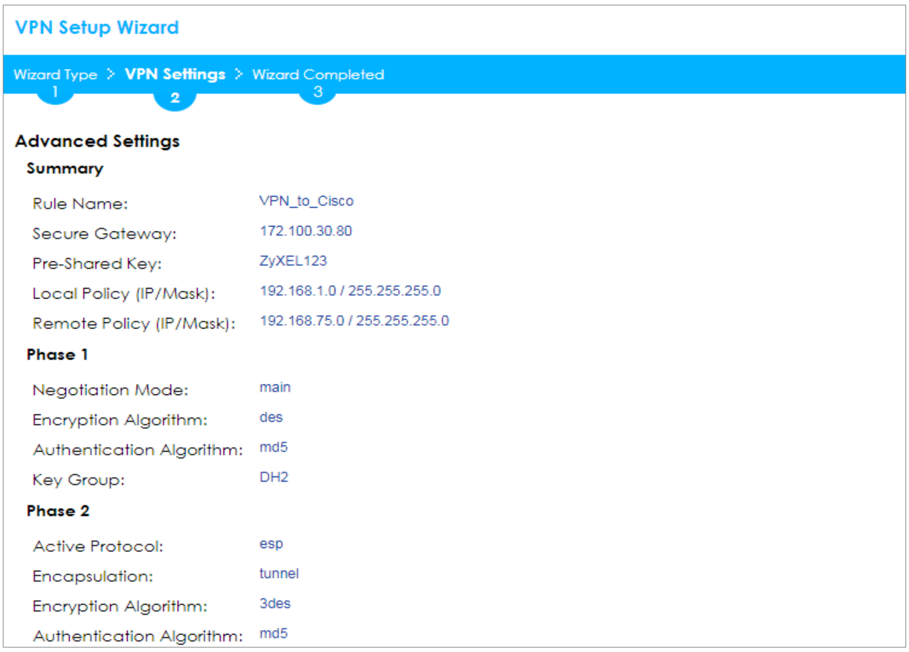
Local Policy (IP/Mask):	192.168.1.0	/ 255.255.255.0
Remote Policy (IP/Mask):	192.168.75.0	/ 255.255.255.0

Property

☑ Nailed-Up

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



VPN Setup Wizard

Advanced Settings

Summary

Rule Name:	VPN_to_Cisco
Secure Gateway:	172.100.30.80
Pre-Shared Key:	ZyXEL123
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.75.0 / 255.255.255.0

Phase 1

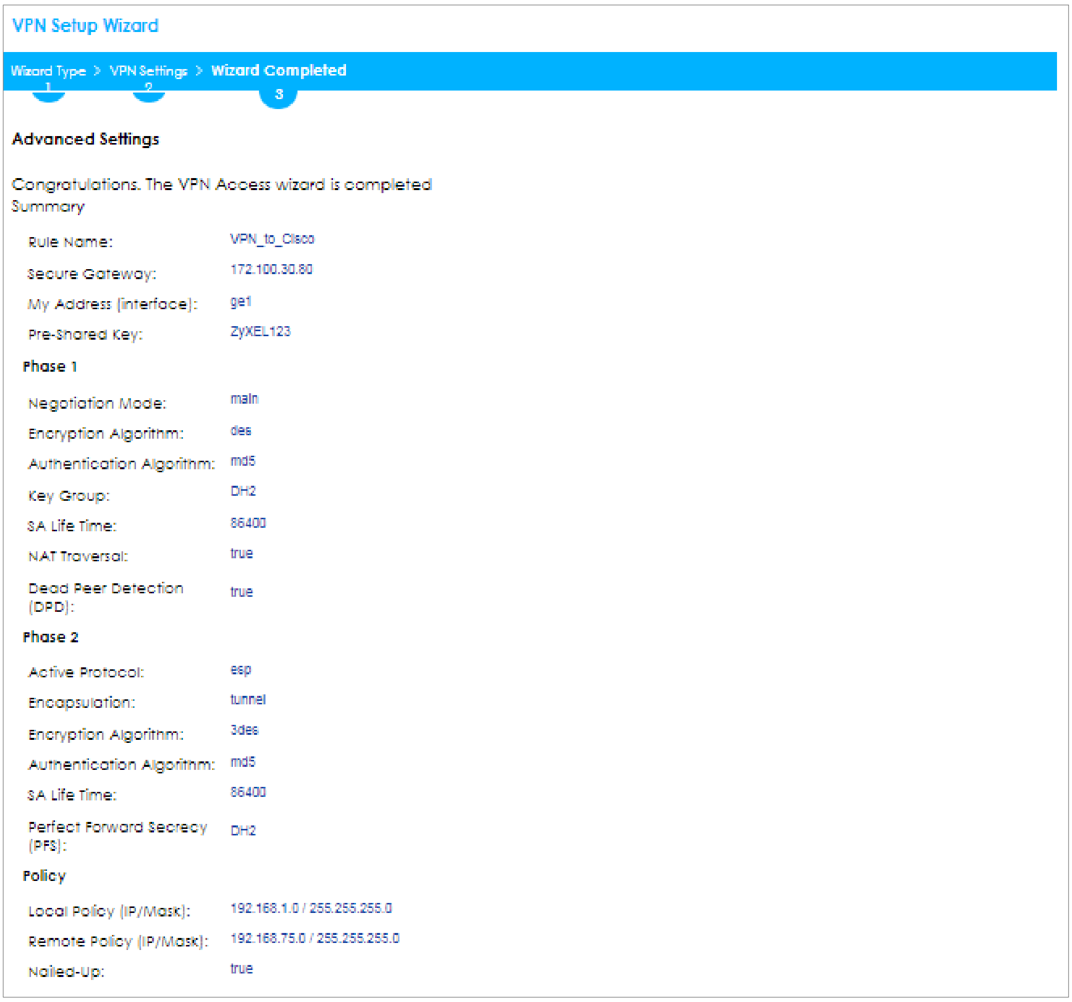
Negotiation Mode:	main
Encryption Algorithm:	des
Authentication Algorithm:	md5
Key Group:	DH2

Phase 2

Active Protocol:	esp
Encapsulation:	tunnel
Encryption Algorithm:	3des
Authentication Algorithm:	md5

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



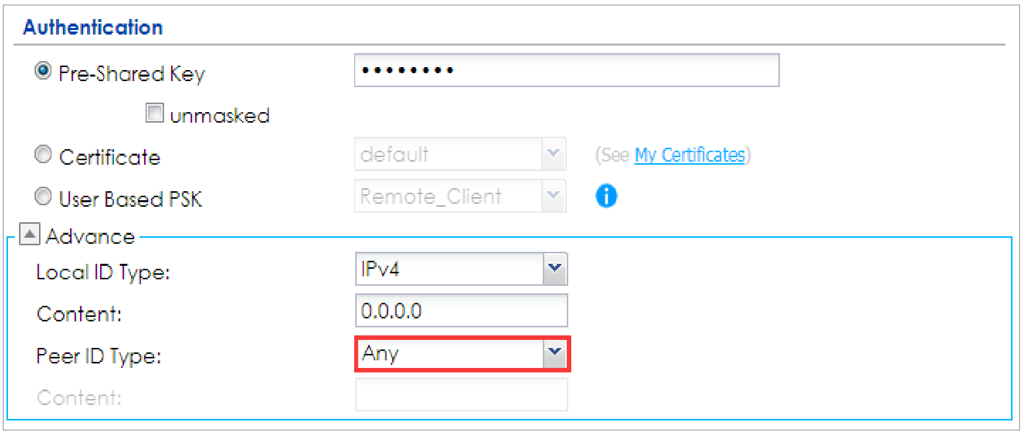
Advanced Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	VPN_to_Cisco
Secure Gateway:	172.100.30.80
My Address (interface):	ge1
Pre-Shared Key:	ZyXEL123
Phase 1	
Negotiation Mode:	main
Encryption Algorithm:	des
Authentication Algorithm:	md5
Key Group:	DH2
SA Life Time:	86400
NAT Traversal:	true
Dead Peer Detection (DPD):	true
Phase 2	
Active Protocol:	esp
Encapsulation:	tunnel
Encryption Algorithm:	3des
Authentication Algorithm:	md5
SA Life Time:	86400
Perfect Forward Secrecy (PFS):	DH2
Policy	
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.75.0 / 255.255.255.0
Nailed-Up:	true

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.



Authentication

● Pre-Shared Key: ••••••••

□ unmasked

○ Certificate: default (See My Certificates)

○ User Based PSK: Remote_Client

Advance

Local ID Type: IPv4

Content: 0.0.0.0

Peer ID Type: Any

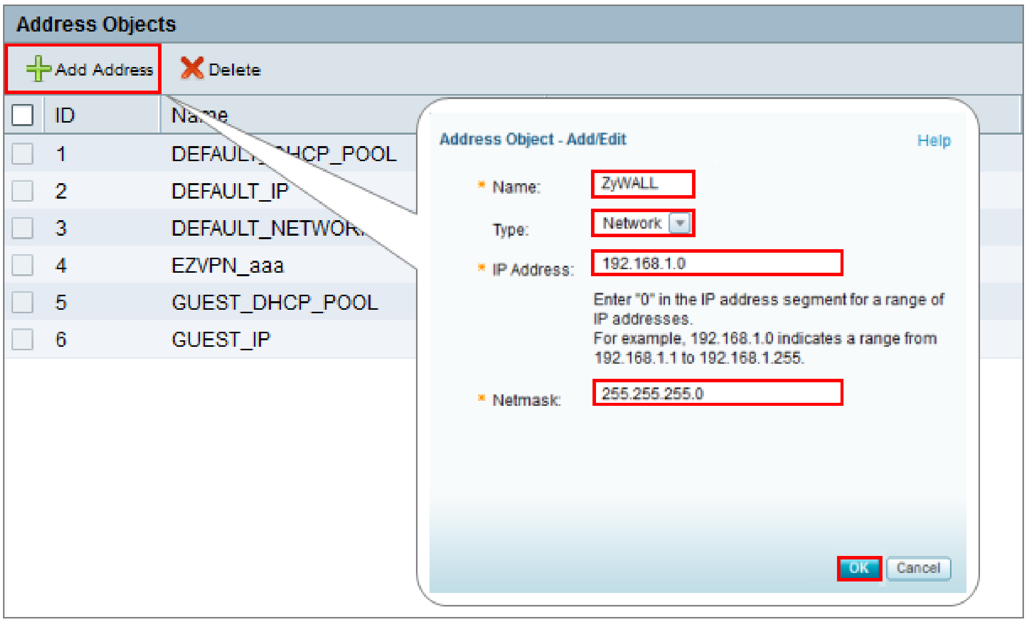
Content:

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

Set Up the IPSec VPN Tunnel on the Cisco

To create an **Address Object Name** of your peer ZyWALL/USG Local IP address, go to **Networking > Address Management > Address Objects** and click **Add Address**. Select **Network** as the **Type**. Configure **IP Address** and **Netmask** to be the IP address range of the network connected to the ZyWALL/USG. Click **OK**.

Networking > Address Management > Address Objects



Address Objects

Add Address | Delete

ID	Name
1	DEFAULT_DHCP_POOL
2	DEFAULT_IP
3	DEFAULT_NETWORK
4	EZVPN_aaa
5	GUEST_DHCP_POOL
6	GUEST_IP

Address Object - Add/Edit

* Name: ZyWALL

Type: Network

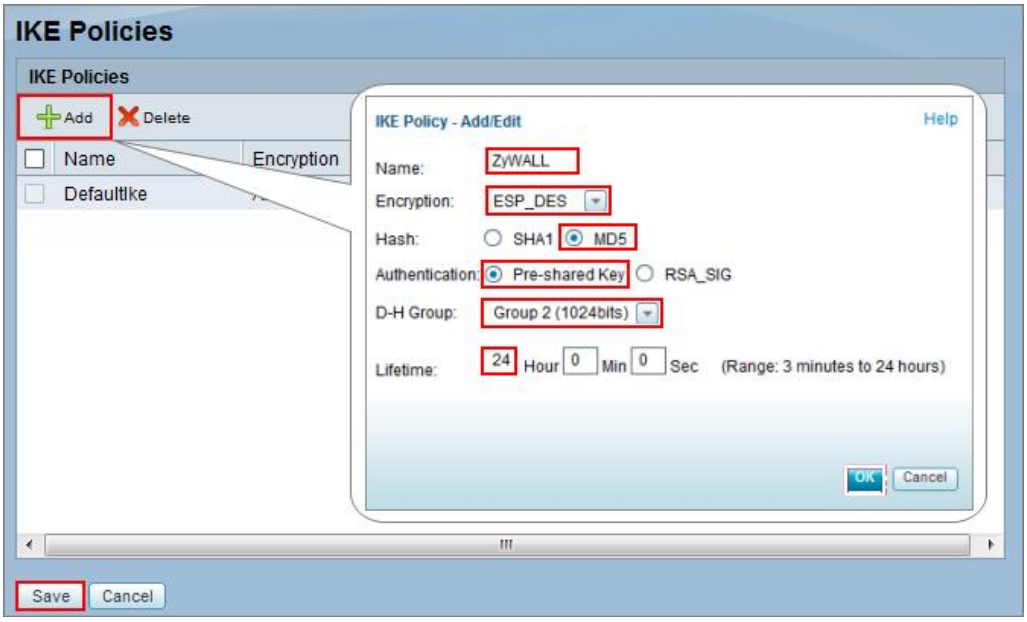
* IP Address: 192.168.1.0

Enter "0" in the IP address segment for a range of IP addresses.
For example, 192.168.1.0 indicates a range from 192.168.1.1 to 192.168.1.255.

* Netmask: 255.255.255.0

Go to **VPN > Site-to-site > IKE Policies**, click **Add** to create a new IKE Policy **Name**. Then, select **Encryption, Hash**, **Pre-shared Key** and **D-H Group** to match your ZyWALL/USG's **VPN Gateway > Phase 1 Settings**. Set **Lifetime** to **24** hours and click **OK** then click **Save** to exit the **IKE Policies** page.

VPN > Site-to-site > IKE Policies



IKE Policies

IKE Policies

Add | Delete

Name	Encryption
DefaultIke	A

IKE Policy - Add/Edit

Name: ZyWALL

Encryption: ESP_DES

Hash: ○ SHA1 ● MD5

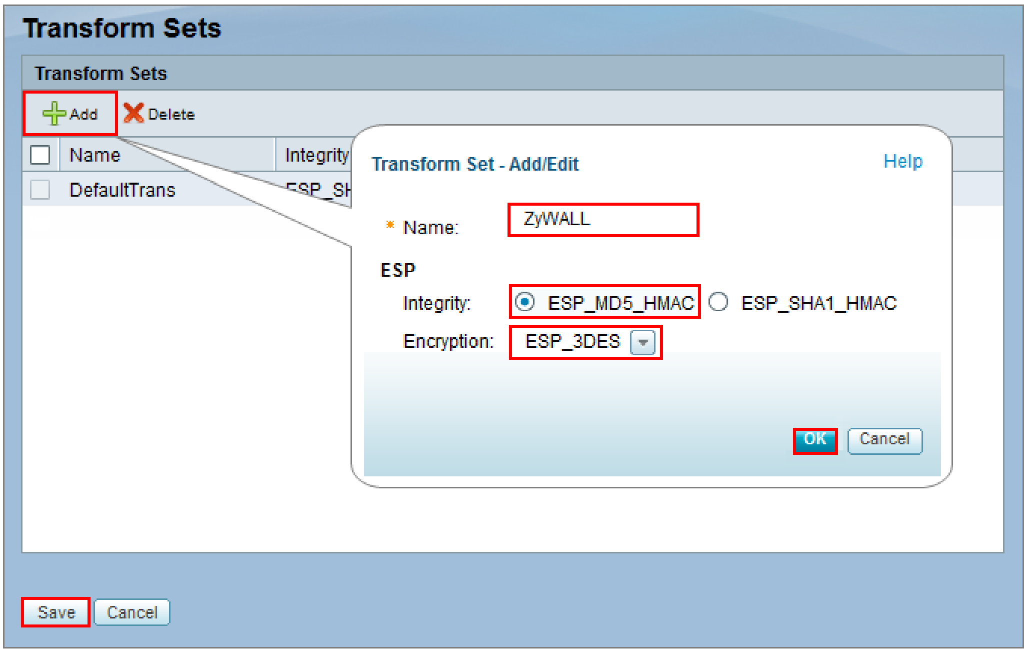
Authentication: ● Pre-shared Key ○ RSA_SIG

D-H Group: Group 2 (1024bits)

Lifetime: 24 Hour 0 Min 0 Sec (Range: 3 minutes to 24 hours)

Go to **VPN > Site-to-site > Transform Sets**, click **Add** to create a new **Transform Set** name. Then, select **Integrity** and **Encryption** to match your ZyWALL/USG's **VPN Connection > Phase 2 Settings**. Click **OK** and click **Save** to exit the **Transform Sets** page.

VPN > Site-to-site > Transform Sets



Transform Sets

Transform Set - Add/Edit

* Name: ZyWALL

ESP

Integrity: ● ESP_MD5_HMAC ○ ESP_SHA1_HMAC

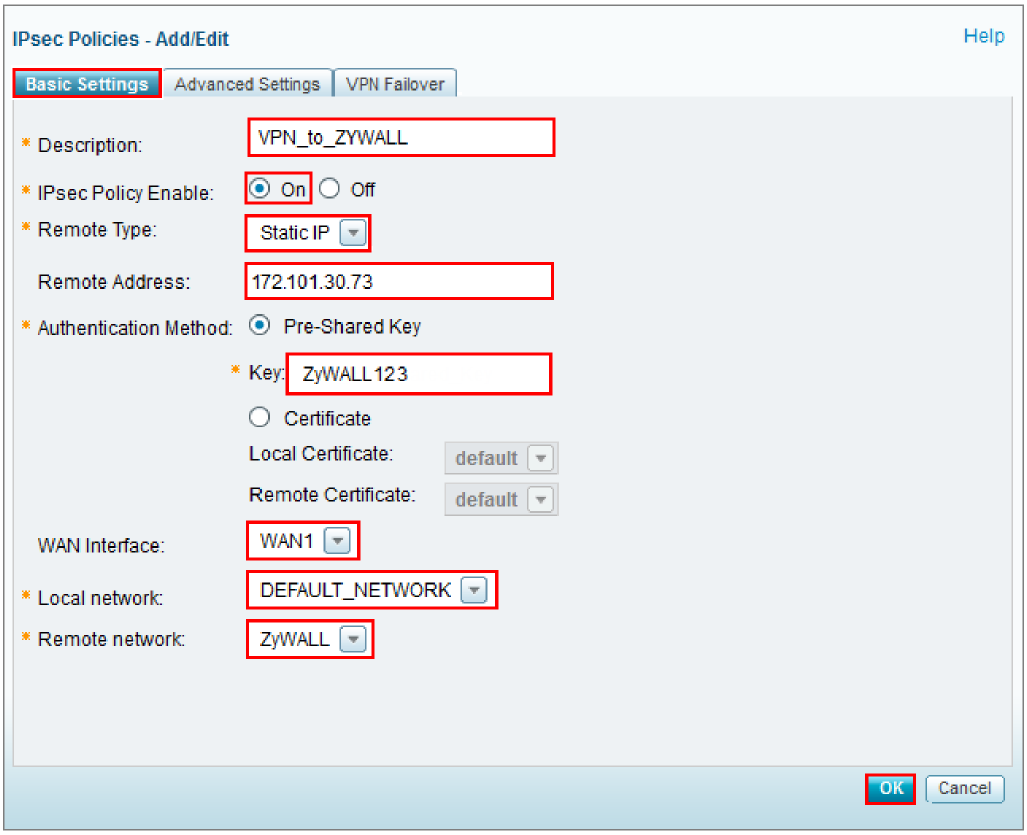
Encryption: ESP_3DES

Go to **VPN > Site-to-site > IPsec Policies** and click **Add**. The new **IPsec Policies** dialog box appears. Go to **Basic Settings,** create IPsec policy **Description** name and click **On** the **IPsec Policy Enable** option.

Select **Static IP** as the **Remote Type**. Set **Remote Address** to be your ZyWALL/USG's WAN IP Address (in the example, 172.101.30.73). Enter the same **Pre-Shared Key** as you created in ZyWALL/USG. Then, set **WAN Interface** to the Internet-facing interface (found under **Status > WAN Interface**).

Select **Local network** to be the IP address range of the network connected to the Cisco (found under **Status > LAN Interface**) and **Remote network** to be the IP address range of the network connected to the ZyWALL/USG (**Address Object** created in Step 1)

VPN > Site-to-site > IPsec Policies > Basic Settings



IPsec Policies - Add/Edit

* Description: VPN_to_ZYWALL

* IPsec Policy Enable: ● On ○ Off

* Remote Type: Static IP

Remote Address: 172.101.30.73

* Authentication Method: ● Pre-Shared Key

* Key: ZyWALL123

○ Certificate

Local Certificate: default

Remote Certificate: default

WAN Interface: WAN1

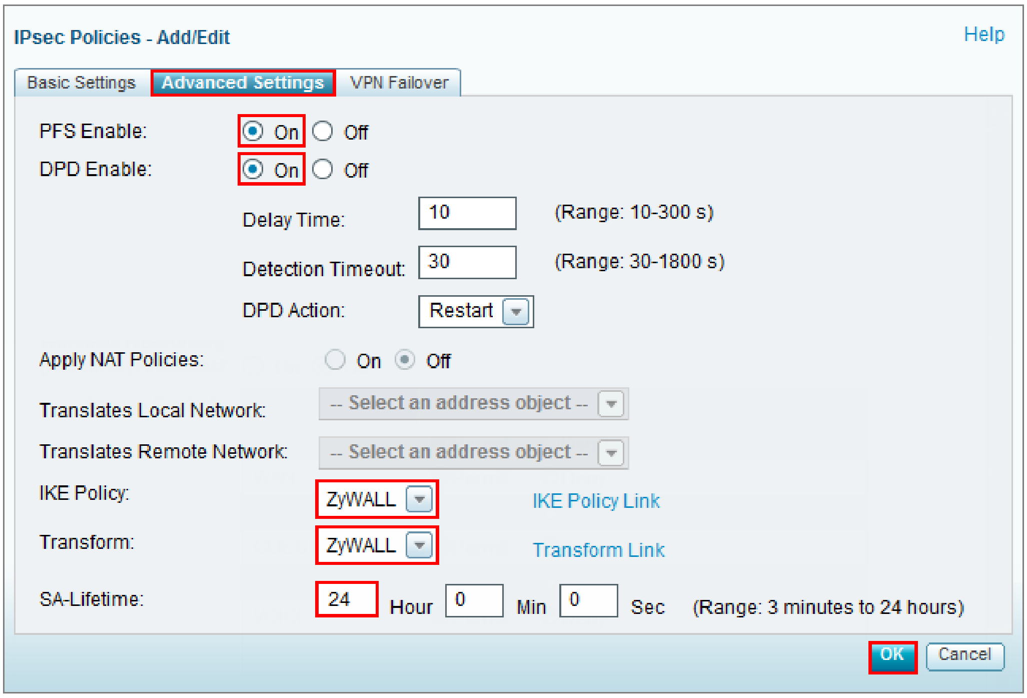
* Local network: DEFAULT_NETWORK

* Remote network: ZyWALL

Then, go to **Advanced Settings** enable **PFS** and **DPD** if you enable both options in the ZyWALL/USG. Set **IKE Policy** to be the **IKE Policy** created in Step 2 (found under **IKE Policy Link**); set **Transform** to be the **Transform Set** created in Step 3 (found under **Transform Link**) and **SA-Lifetime** to be **24** hours.

Click **OK**. The connection active dialog box appears. Click **Activate Connection**.

VPN > Site-to-site > IPsec Policies > Advanced Settings



IPsec Policies - Add/Edit

PFS Enable: ● On ○ Off

DPD Enable: ● On ○ Off

Delay Time: 10 (Range: 10-300 s)

Detection Timeout: 30 (Range: 30-1800 s)

DPD Action: Restart

Apply NAT Policies: ○ On ● Off

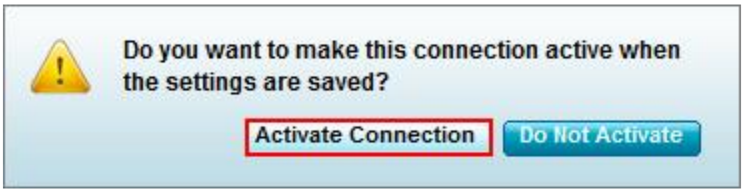
Translates Local Network: -- Select an address object --

Translates Remote Network: -- Select an address object --

IKE Policy: ZyWALL

Transform: ZyWALL

SA-Lifetime: 24 Hour 0 Min 0 Sec (Range: 3 minutes to 24 hours)

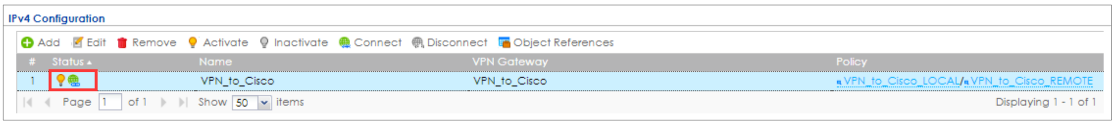


Do you want to make this connection active when the settings are saved?

Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



IPv4 Configuration

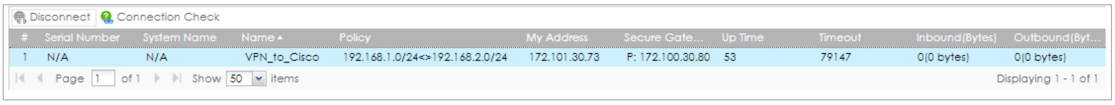
Add | Edit | Remove | Activate | Inactivate | Connect | Disconnect | Object References

#	Status ▴	Name	VPN Gateway	Policy
1		VPN_to_Cisco	VPN_to_Cisco	VPN_to_Cisco_LOCAL/VPN_to_Cisco_REMOTE

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

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec



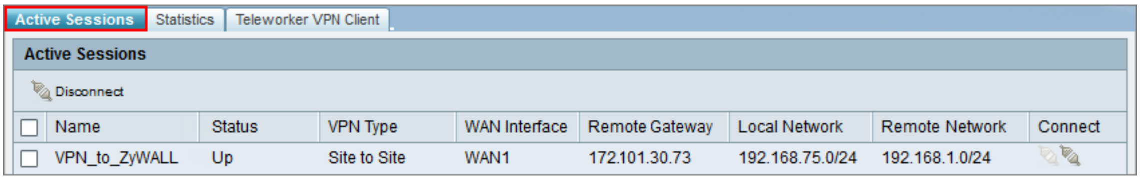
Disconnect | Connection Check

#	Serial Number	System Name	Name ▴	Policy	My Address	Secure Gate...	Up Time	Timeout	Inbound(Bytes)	Outbound(Byt...
1	N/A	N/A	VPN_to_Cisco	192.168.1.0/24<=>192.168.2.0/24	172.101.30.73	P: 172.100.30.80	53	79147	0(0 bytes)	0(0 bytes)

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

Go to Cisco **VPN > VPN Status > IPsec VPN Status > Active Sessions** and check the tunnel **Status** is up.

VPN > VPN Status > IPsec VPN Status > Active Sessions



Active Sessions | Statistics | Teleworker VPN Client

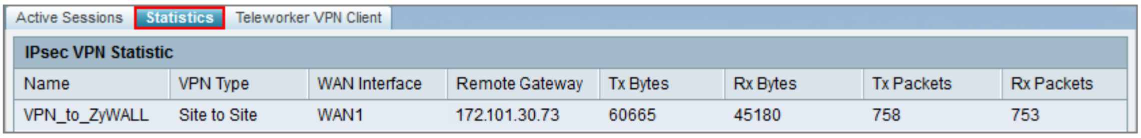
Active Sessions

Disconnect

□	Name	Status	VPN Type	WAN Interface	Remote Gateway	Local Network	Remote Network	Connect
□	VPN_to_ZyWALL	Up	Site to Site	WAN1	172.101.30.73	192.168.75.0/24	192.168.1.0/24	

Go to Cisco **VPN > VPN Status > IPsec VPN Status > Statics** and check the **Tx Packets** (Transmit data) and **Rx Packets** (Receive data).

VPN > VPN Status > IPsec VPN Status > Statistics



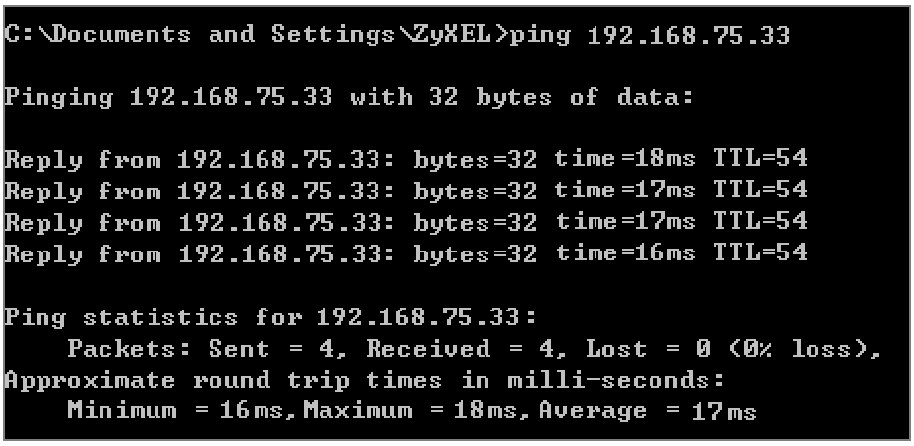
Active Sessions | Statistics | Teleworker VPN Client

IPsec VPN Statistic

Name	VPN Type	WAN Interface	Remote Gateway	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets
VPN_to_ZyWALL	Site to Site	WAN1	172.101.30.73	60665	45180	758	753

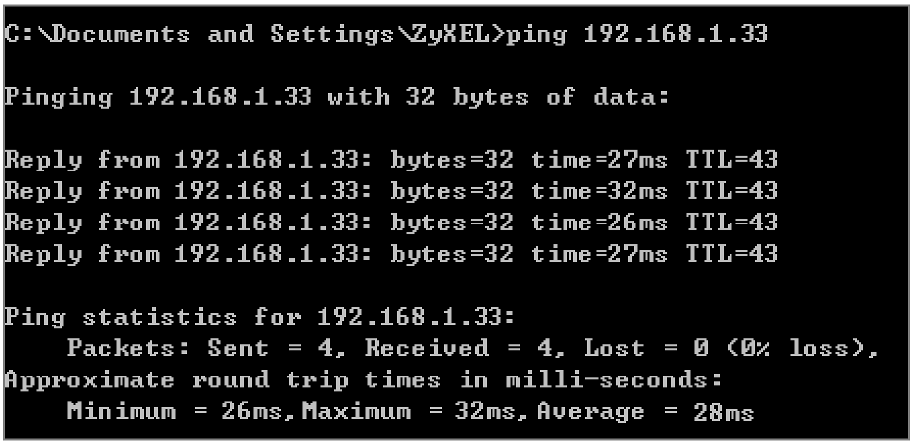
To test whether a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC behind ZyWALL/USG > Window 7 > cmd > ping 192.168.75.33



```
C:\Documents and Settings\ZyXEL>ping 192.168.75.33

Pinging 192.168.75.33 with 32 bytes of data:

Reply from 192.168.75.33: bytes=32 time=18ms TTL=54
Reply from 192.168.75.33: bytes=32 time=17ms TTL=54
Reply from 192.168.75.33: bytes=32 time=17ms TTL=54
Reply from 192.168.75.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.75.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC behind Cisco> Window 7 > cmd > ping 192.168.1.33



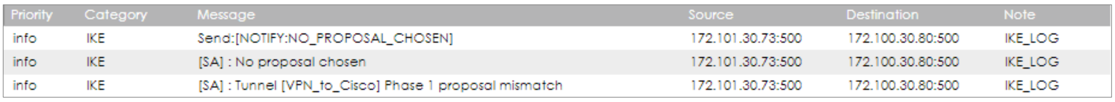
```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG and Cisco must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the

IKE SA.

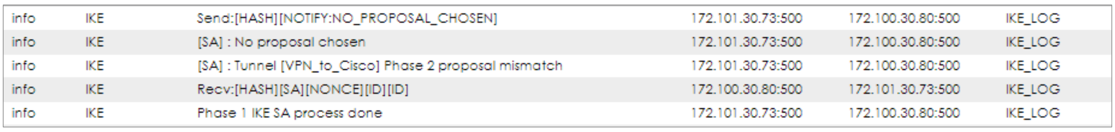
MONITOR > Log



Priority	Category	Message	Source	Destination	Note
info	IKE	Send:[NOTIFY:NO_PROPOSAL_CHOSEN]	172.101.30.73:500	172.100.30.80:500	IKE_LOG
info	IKE	[SA] : No proposal chosen	172.101.30.73:500	172.100.30.80:500	IKE_LOG
info	IKE	[SA] : Tunnel [VPN_to_Cisco] Phase 1 proposal mismatch	172.101.30.73:500	172.100.30.80:500	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG and Cisco Phase 2 Settings. Both ZyWALL/USG and Cisco must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log



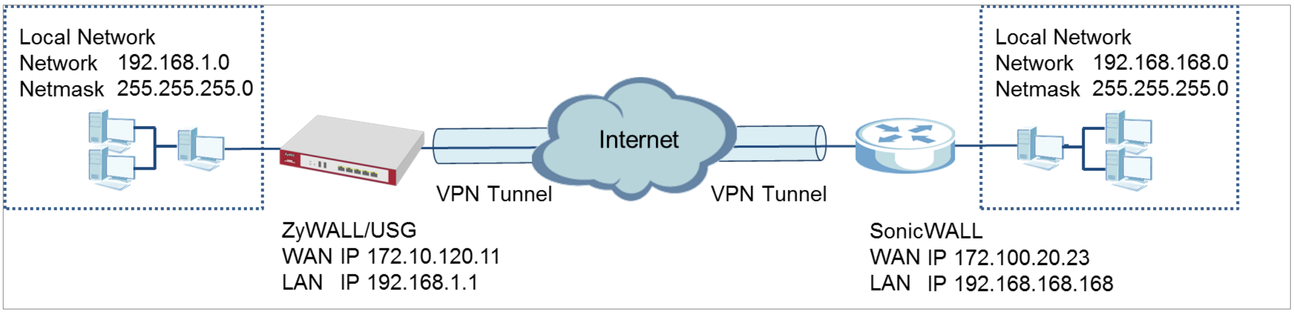
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	172.101.30.73:500	172.100.30.80:500	IKE_LOG
info	IKE	[SA] : No proposal chosen	172.101.30.73:500	172.100.30.80:500	IKE_LOG
info	IKE	[SA] : Tunnel [VPN_to_Cisco] Phase 2 proposal mismatch	172.101.30.73:500	172.100.30.80:500	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	172.100.30.80:500	172.101.30.73:500	IKE_LOG
info	IKE	Phase 1 IKE SA process done	172.101.30.73:500	172.100.30.80:500	IKE_LOG

Make sure the both ZyWALL/USG and Cisco security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure Site-to-site IPSec VPN with a SonicWALL router

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN between a ZYWALL/USG and a SonicWALL router. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



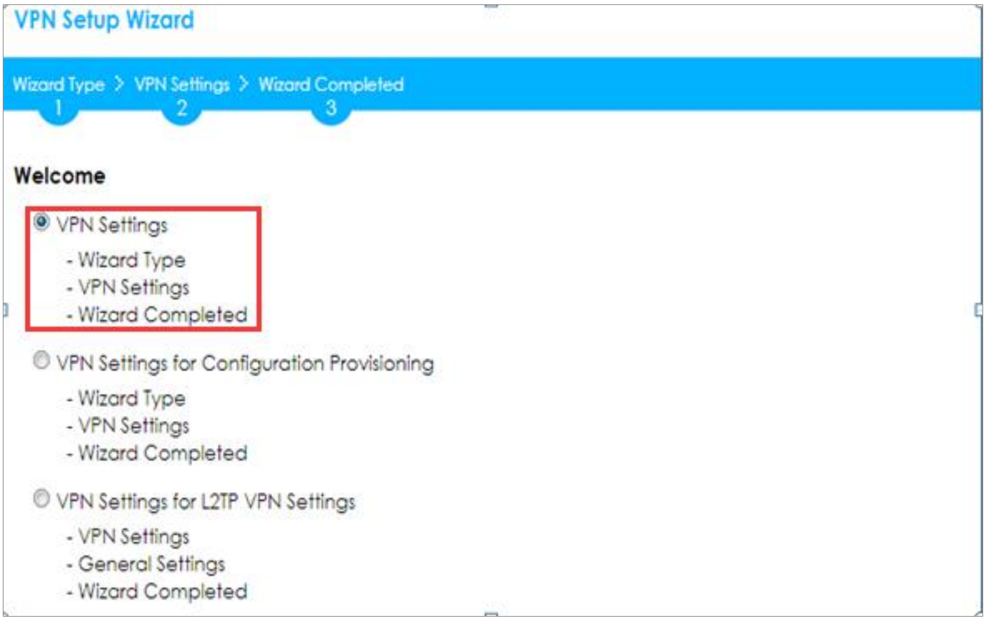
ZyWALL/USG Site-to-site IPSec VPN with SonicWALL

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and NSA240 (Firmware Version: SonicOS Enhanced 5.8.0.1-31o)

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the SonicWALL. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

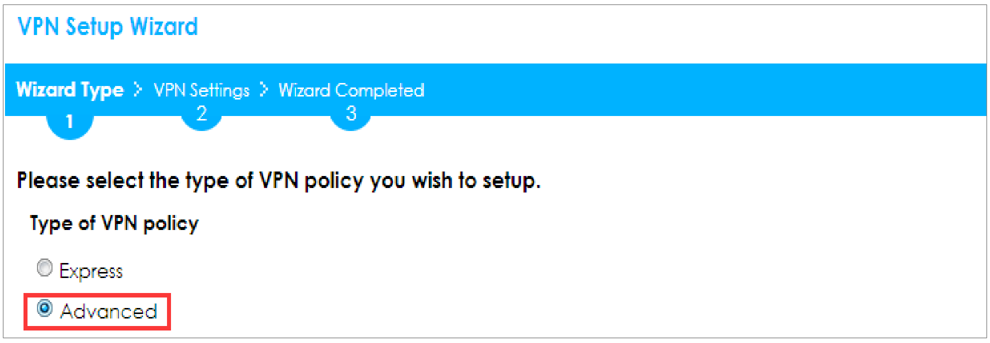
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



VPN Setup Wizard

Please select the type of VPN policy you wish to setup.

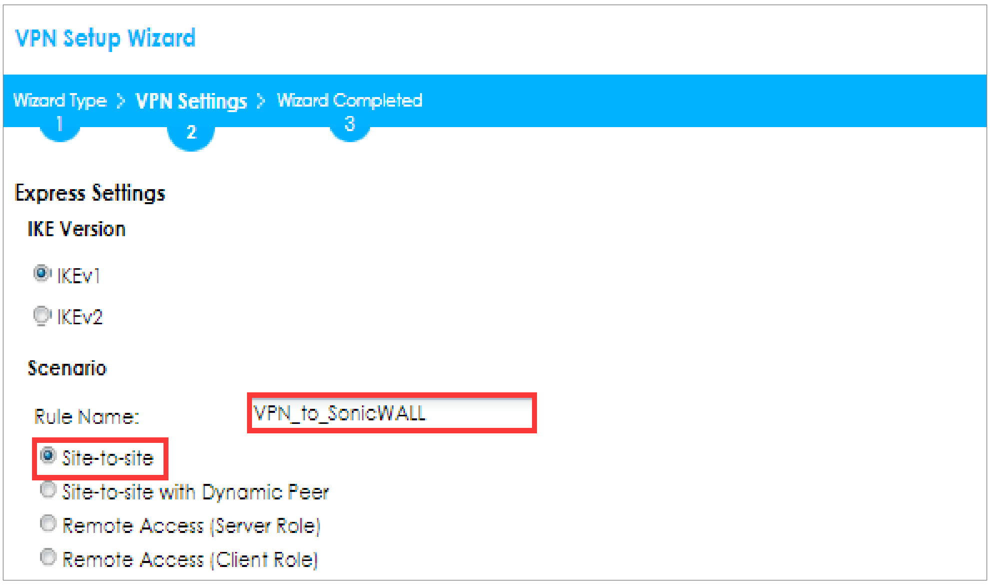
Type of VPN policy

○ Express

● Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



Express Settings

IKE Version

● IKEv1
○ IKEv2

Scenario

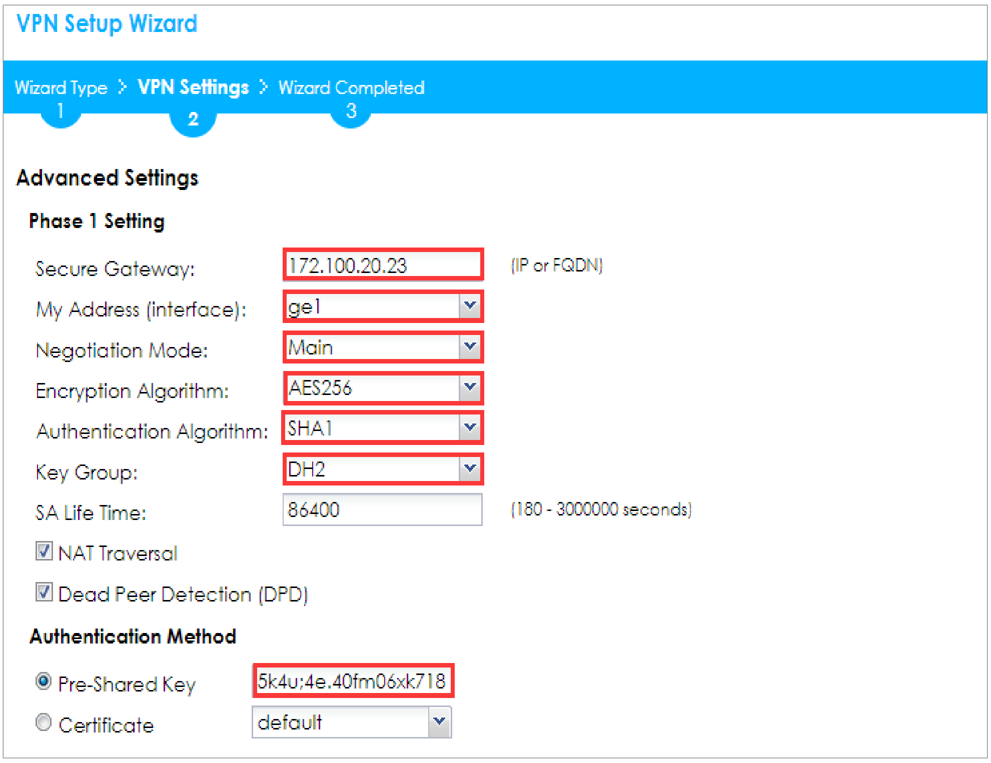
Rule Name: VPN_to_SonicWALL

● Site-to-site
○ Site-to-site with Dynamic Peer
○ Remote Access (Server Role)
○ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the SonicWALL's Gateway IP address (in the example, 172.100.20.23); select **My Address** to be the interface connected to the Internet.

Set the desired **Negotiation**, **Encryption**, **Authentication**, **Key Group** and **SA Life Time** settings. Type a secure **Pre-Shared Key** (8-32 characters) which must match your SonicWALL **Shared Secret**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 1 Setting)



VPN Setup Wizard

Advanced Settings

Phase 1 Setting

Secure Gateway:	172.100.20.23	(IP or FQDN)
My Address (interface):	ge1	
Negotiation Mode:	Main	
Encryption Algorithm:	AES256	
Authentication Algorithm:	SHA1	
Key Group:	DH2	
SA Life Time:	86400	(180 - 3000000 seconds)

☑ NAT Traversal

☑ Dead Peer Detection (DPD)

Authentication Method

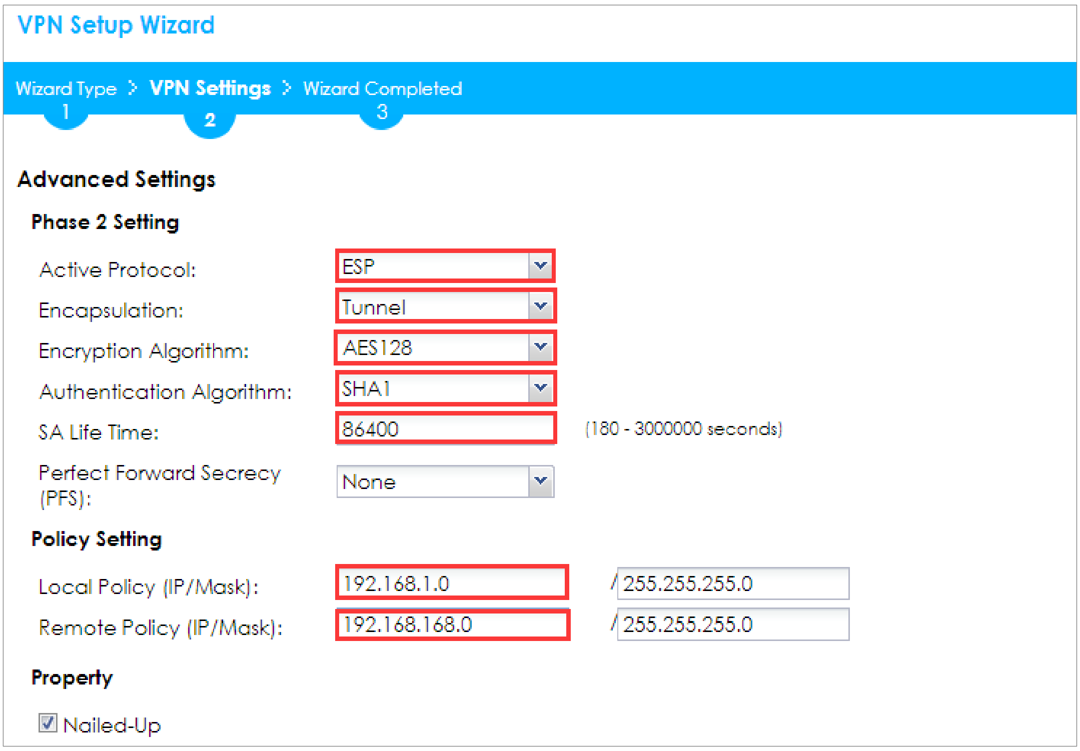
● Pre-Shared Key 5k4u;4e.40fm06xk718

○ Certificate default

Continue to **Phase 2 Settings** to select the desired **Encapsulation**, **Encryption**, **Authentication**, and **SA Life Time** settings.

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the SonicWALL. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 2 Setting)



VPN Setup Wizard

Advanced Settings

Phase 2 Setting

Active Protocol:	ESP	
Encapsulation:	Tunnel	
Encryption Algorithm:	AES128	
Authentication Algorithm:	SHA1	
SA Life Time:	86400	(180 - 3000000 seconds)
Perfect Forward Secrecy (PFS):	None	

Policy Setting

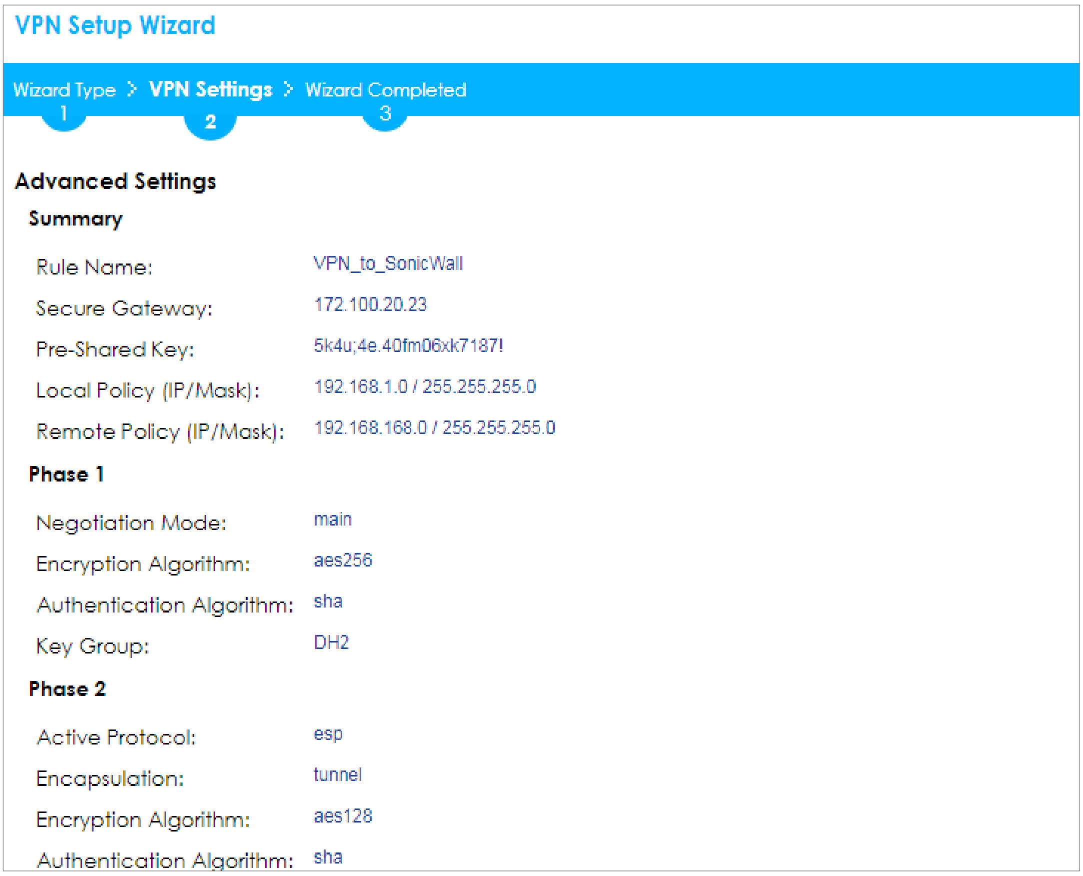
Local Policy (IP/Mask):	192.168.1.0	/ 255.255.255.0
Remote Policy (IP/Mask):	192.168.168.0	/ 255.255.255.0

Property

☑ Nailed-Up

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



VPN Setup Wizard

Advanced Settings

Summary

Rule Name:	VPN_to_SonicWall
Secure Gateway:	172.100.20.23
Pre-Shared Key:	5k4u;4e.40fm06xk7187!
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.168.0 / 255.255.255.0

Phase 1

Negotiation Mode:	main
Encryption Algorithm:	aes256
Authentication Algorithm:	sha
Key Group:	DH2

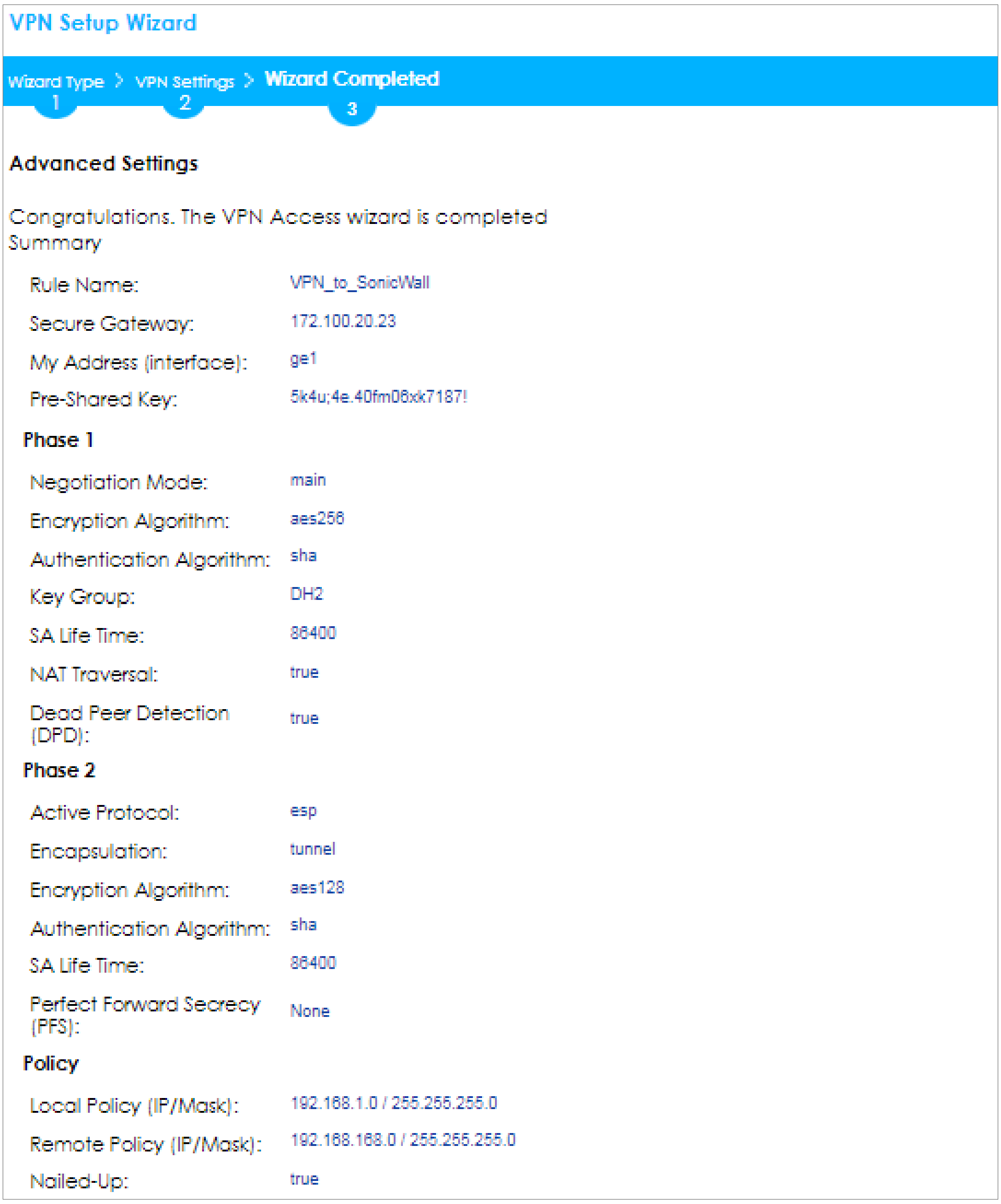
Phase 2

Active Protocol:	esp
Encapsulation:	tunnel
Encryption Algorithm:	aes128
Authentication Algorithm:	sha

Note: The Phase 1 and Phase 2 settings established here must match the Phase 1 and Phase 2 settings configured later in the SonicWALL.

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



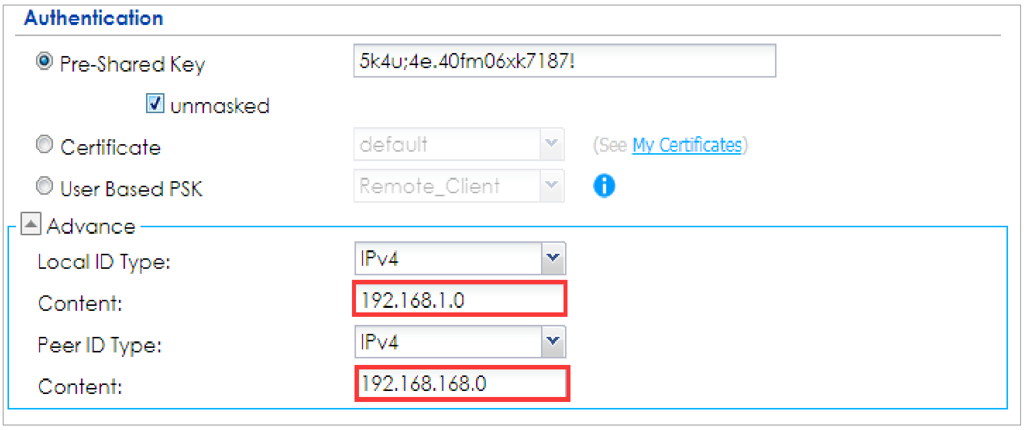
Advanced Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	VPN_to_SonicWall
Secure Gateway:	172.100.20.23
My Address (interface):	ge1
Pre-Shared Key:	5k4u;4e.40fm06xk7187!
Phase 1	
Negotiation Mode:	main
Encryption Algorithm:	aes256
Authentication Algorithm:	sha
Key Group:	DH2
SA Life Time:	86400
NAT Traversal:	true
Dead Peer Detection (DPD):	true
Phase 2	
Active Protocol:	esp
Encapsulation:	tunnel
Encryption Algorithm:	aes128
Authentication Algorithm:	sha
SA Life Time:	86400
Perfect Forward Secrecy (PFS):	None
Policy	
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.168.0 / 255.255.255.0
Nailed-Up:	true

Go to **VPN Gateway > Show Advanced Settings > Authentication** to configure **your Local ID Type** and **Peer ID Type** to match your SonicWALL's **VPN > Settings > VPN Policies > General > IKE Authentication > Local IKE ID** and **Peer IKE ID**.

VPN Gateway > Show Advanced Settings > Authentication



Authentication

● Pre-Shared Key: 5k4u;4e.40fm06xk7187!

☑ unmasked

○ Certificate: default (See My Certificates)

○ User Based PSK: Remote_Client

Advance

Local ID Type: IPv4

Content: 192.168.1.0

Peer ID Type: IPv4

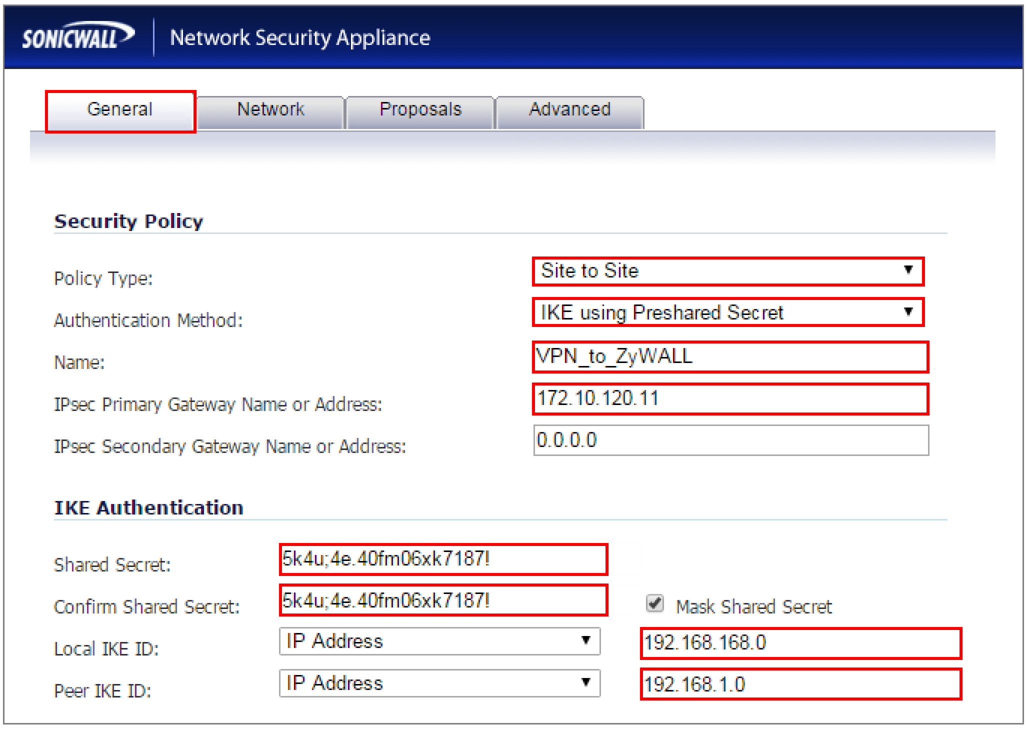
Content: 192.168.168.0

Set Up the IPSec VPN Tunnel on the SonicWALL

In the SonicWALL **VPN > Settings > VPN Policies**, click **Add** to create a new VPN policy. Select **Policy Type** to be the **Site to Site**, select **Authentication Method** to be the **IKE using Preshared Secret**. Type the ZyWALL/USG's WAN IP Address to be the **IPsec Primary Gateway Name or Address** (in the example, 172.10.120.11).

In the **IKE Authentication** section, set the **Shared Secret** to be the same as your ZyWALL/USG's **Pre-Shared Key**. Then, set the **Local IKE ID** and the **Peer IKE ID** to match your ZyWALL/USG's **VPN Gateway > Show Advanced Settings > Authentication > Local ID Type** and **Peer ID Type**.

VPN > Settings > VPN Policies > General



Security Policy

Policy Type:	Site to Site
Authentication Method:	IKE using Preshared Secret
Name:	VPN_to_ZyWALL
IPsec Primary Gateway Name or Address:	172.10.120.11
IPsec Secondary Gateway Name or Address:	0.0.0.0

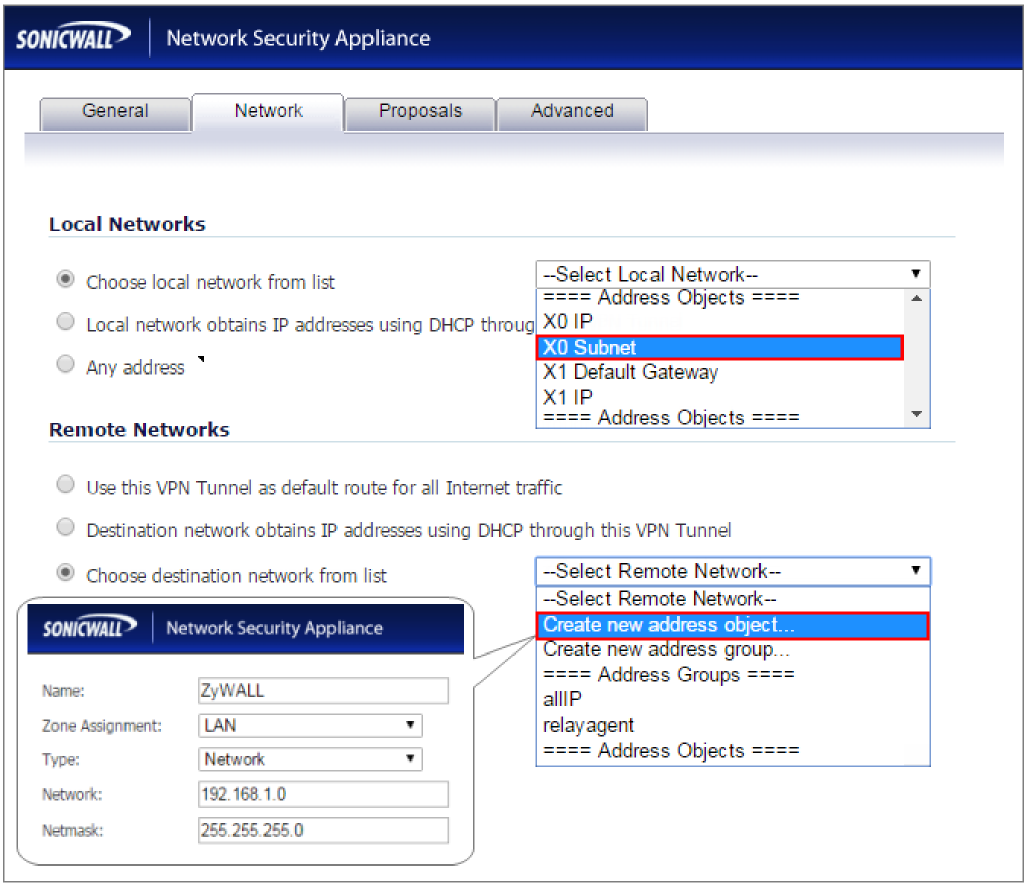
IKE Authentication

Shared Secret:	5k4u;4e.40fm06xk7187!	
Confirm Shared Secret:	5k4u;4e.40fm06xk7187!	☑ Mask Shared Secret
Local IKE ID:	IP Address	192.168.168.0
Peer IKE ID:	IP Address	192.168.1.0

In the SonicWALL **VPN > Settings > VPN Policies > Network**, choose **Local Network** to be the IP address range of the network connected to the **SonicWALL** (found under **SonicWALL > Network > Interfaces > LAN**).

Go to **Remote Network** and create a new address IP address range of the network connected to the ZyWALL/USG. Then, scroll down the list to choose the newly created **Address Object** to be the **Remote Network**.

VPN > Settings > VPN Policies > Network



SONICWALL Network Security Appliance

General | Network | Proposals | Advanced

Local Networks

● Choose local network from list

○ Local network obtains IP addresses using DHCP throug

○ Any address

--Select Local Network--
==== Address Objects ====
X0 IP
X0 Subnet
X1 Default Gateway
X1 IP
==== Address Objects ====

Remote Networks

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

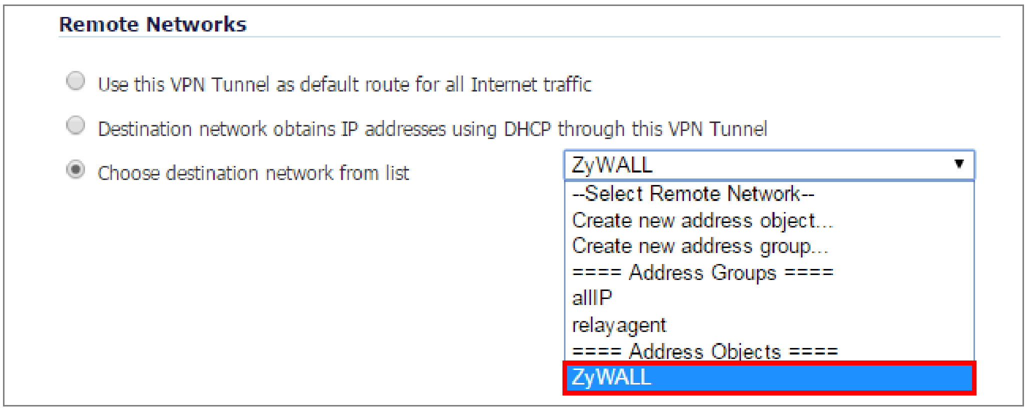
○ Destination network obtains IP addresses using DHCP through this VPN Tunnel

● Choose destination network from list

--Select Remote Network--
--Select Remote Network--
Create new address object...
Create new address group...
==== Address Groups ====
allIP
relayagent
==== Address Objects ====

SONICWALL Network Security Appliance

Name:	ZyWALL
Zone Assignment:	LAN
Type:	Network
Network:	192.168.1.0
Netmask:	255.255.255.0



Remote Networks

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

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

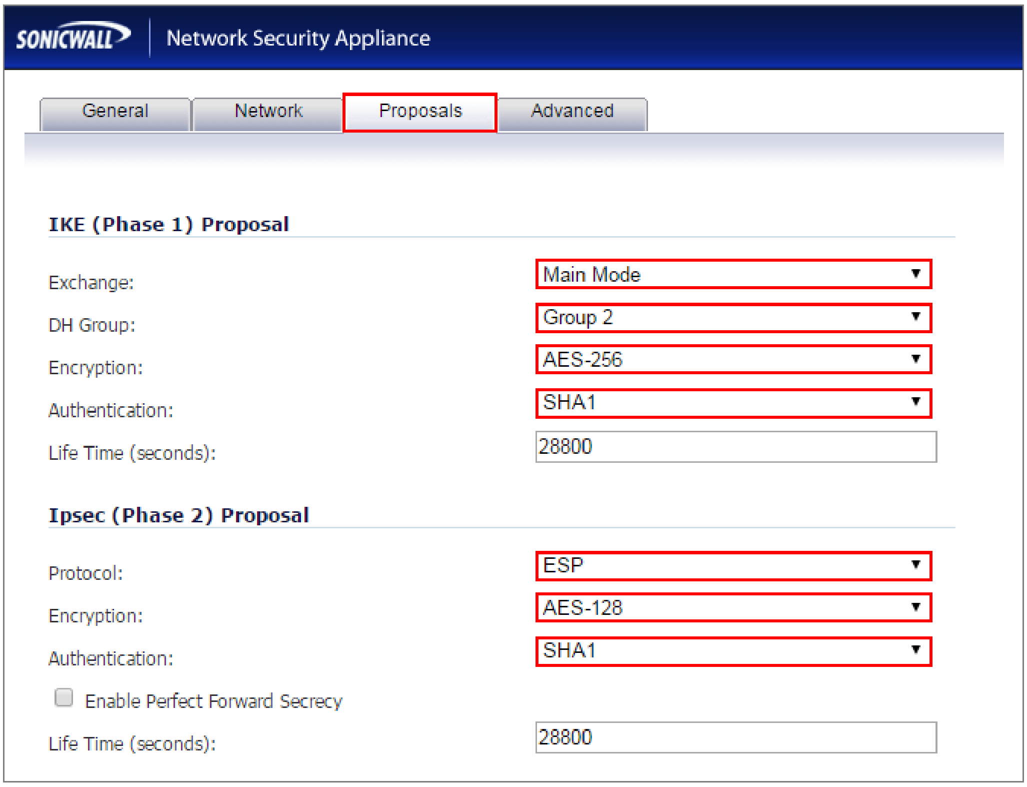
● Choose destination network from list

ZyWALL
--Select Remote Network--
Create new address object...
Create new address group...
==== Address Groups ====
allIP
relayagent
==== Address Objects ====
ZyWALL

In the SonicWALL **VPN > Settings > VPN Policies > Proposals** > **IKE (Phase 1) Proposal** and set **Exchange**, **DH Group**, **Encryption** and **Authentication** to match your ZyWALL/USG's **VPN Gateway > Show Advanced Settings > Phase 1 Settings**.

Go to **IKE (Phase 2) Proposal** and set the **Protocol**, **Encryption** and **Authentication** to match your ZyWALL/USG's **VPN Connection > Show Advanced Settings > Phase 2 Settings**.

VPN > Settings > VPN Policies > Proposals



IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: AES-256

Authentication: SHA1

Life Time (seconds): 28800

Ipsec (Phase 2) Proposal

Protocol: ESP

Encryption: AES-128

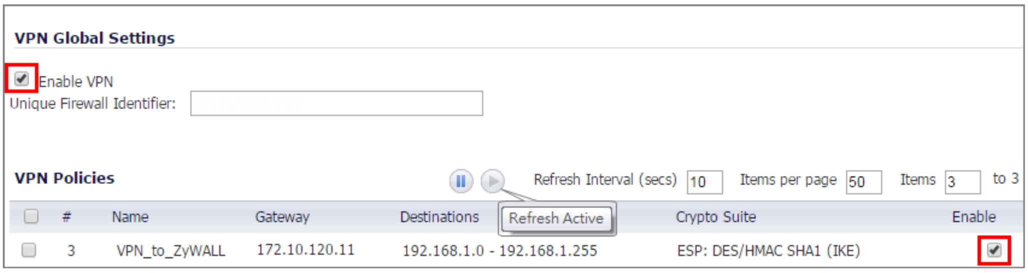
Authentication: SHA1

□ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

Select **Enable VPN** and click **Refresh Active**.

VPN > Settings > VPN Global Settings



VPN Global Settings

☑ Enable VPN

Unique Firewall Identifier:

VPN Policies

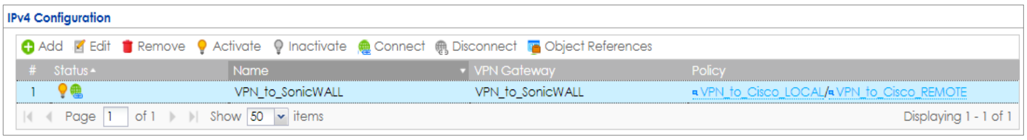
Refresh Interval (secs) 10 Items per page 50 Items 3 to 3

□	#	Name	Gateway	Destinations	Crypto Suite	Enable
□	3	VPN_to_ZyWALL	172.10.120.11	192.168.1.0 - 192.168.1.255	ESP: DES/HMAC SHA1 (IKE)	☑

Test the IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



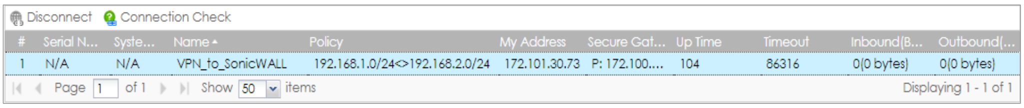
IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1		VPN_to_SonicWALL	VPN_to_SonicWALL	VPN_to_Cisco_LOCAL/VPN_to_Cisco_REMOTE

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

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec

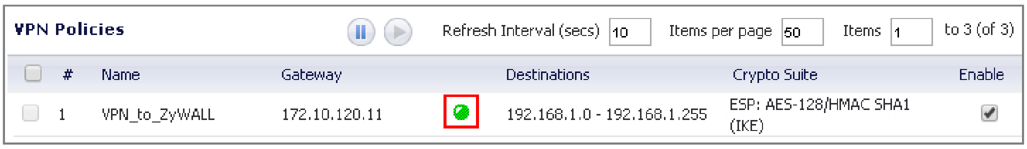


#	Serial N...	Syste...	Name	Policy	My Address	Secure Gat...	Up Time	Timeout	Inbound(B...	Outbound(...
1	N/A	N/A	VPN_to_SonicWALL	192.168.1.0/24<>192.168.2.0/24	172.101.30.73	P: 172.100....	104	86316	0(0 bytes)	0(0 bytes)

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

Go to SonicWALL **VPN > VPN Settings > VPN Policies**, the status green light is on.

VPN > VPN Settings > VPN Policies



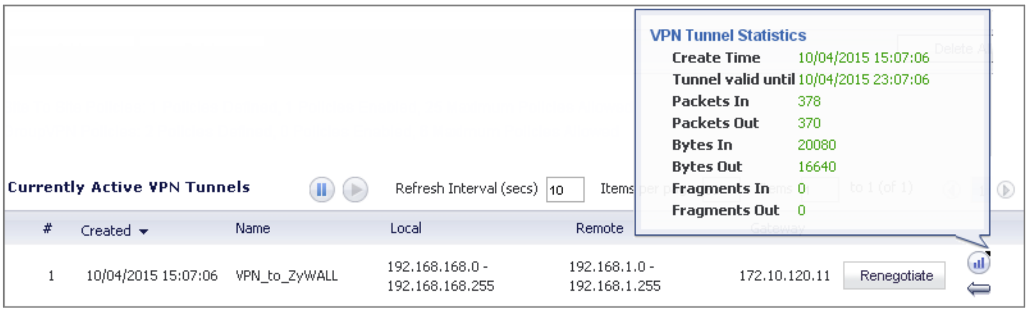
VPN Policies

Refresh Interval (secs) 10 Items per page 50 Items 1 to 3 (of 3)

☐	#	Name	Gateway		Destinations	Crypto Suite	Enable
☐	1	VPN_to_ZyWALL	172.10.120.11	●	192.168.1.0 - 192.168.1.255	ESP: AES-128/HMAC SHA1 (IKE)	☑

Go to SonicWALL **VPN > VPN Settings > Currently Active VPN Tunnels** > **VPN Tunnel Statics** to check **Tunnel valid time**, **Bytes In** (Incoming Data) and **Bytes Out** (Outgoing Data).

VPN > VPN Settings > Currently Active VPN Tunnels



VPN Tunnel Statistics

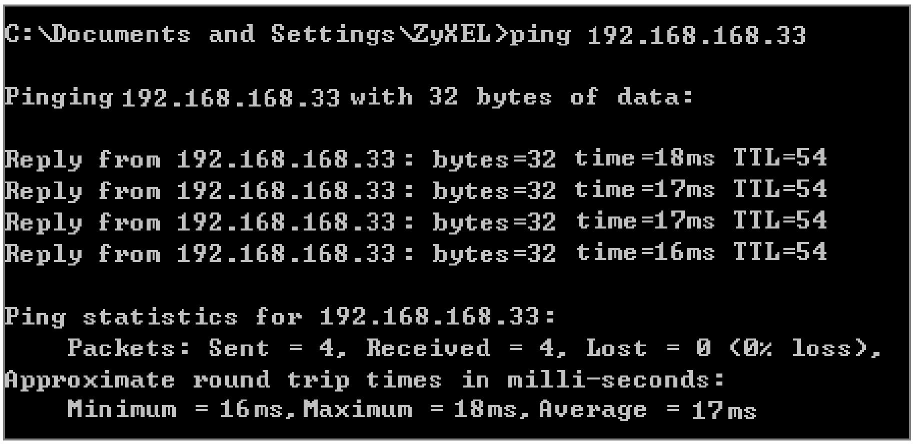
Create Time	10/04/2015 15:07:06
Tunnel valid until	10/04/2015 23:07:06
Packets In	378
Packets Out	370
Bytes In	20080
Bytes Out	16640
Fragments In	0
Fragments Out	0

Currently Active VPN Tunnels Refresh Interval (secs) 10 Items

#	Created	Name	Local	Remote	Gateway	
1	10/04/2015 15:07:06	VPN_to_ZyWALL	192.168.168.0 - 192.168.168.255	192.168.1.0 - 192.168.1.255	172.10.120.11	Renegotiate

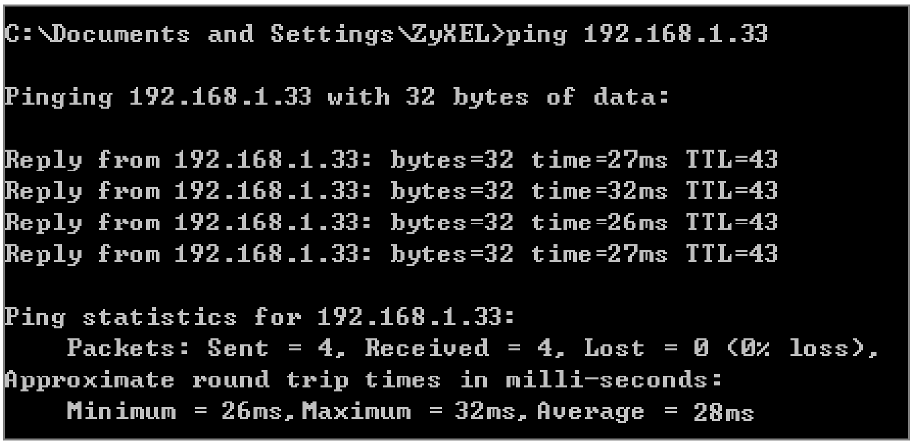
To test whether a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC behind ZyWALL/USG > Window 7 > cmd > ping 192.168.168.33



```
C:\Documents and Settings\ZyXEL>ping 192.168.168.33

Pinging 192.168.168.33 with 32 bytes of data:

Reply from 192.168.168.33: bytes=32 time=18ms TTL=54
Reply from 192.168.168.33: bytes=32 time=17ms TTL=54
Reply from 192.168.168.33: bytes=32 time=17ms TTL=54
Reply from 192.168.168.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.168.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC behind SonicWALL> Window 7 > cmd > ping 192.168.1.33

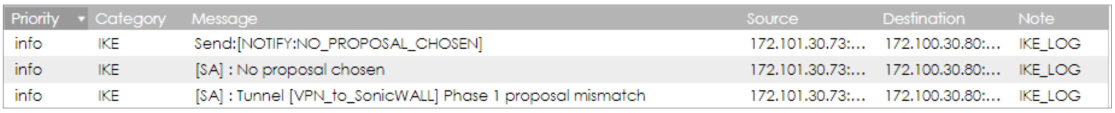


```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG and SonicWALL must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

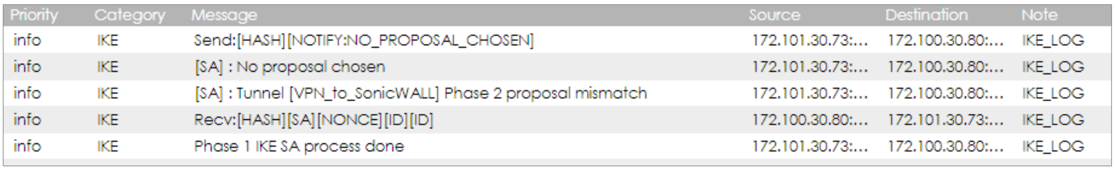
MONITOR > Log



Priority	Category	Message	Source	Destination	Note
info	IKE	Send:[NOTIFY:NO_PROPOSAL_CHOSEN]	172.101.30.73:...	172.100.30.80:...	IKE_LOG
info	IKE	[SA] : No proposal chosen	172.101.30.73:...	172.100.30.80:...	IKE_LOG
info	IKE	[SA] : Tunnel [VPN_to_SonicWALL] Phase 1 proposal mismatch	172.101.30.73:...	172.100.30.80:...	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG and SonicWALL Phase 2 Settings. Both ZyWALL/USG and SonicWALL must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log



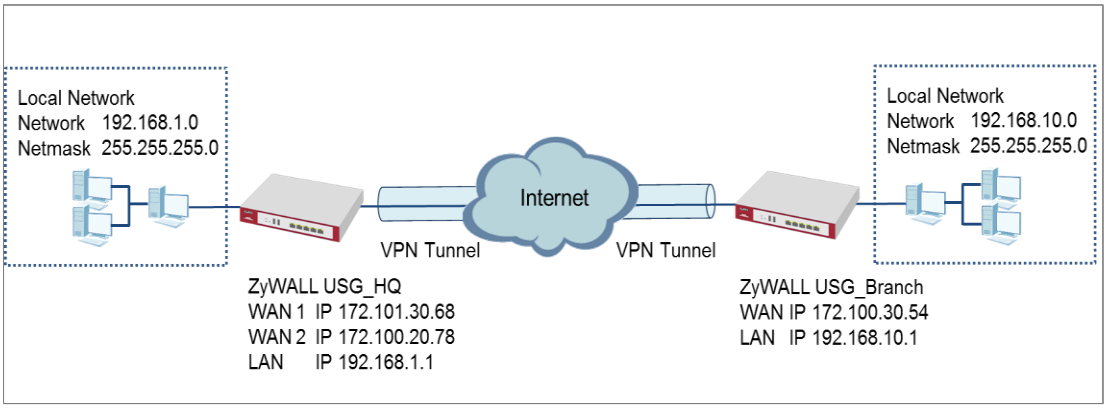
Priority	Category	Message	Source	Destination	Note
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	172.101.30.73:...	172.100.30.80:...	IKE_LOG
info	IKE	[SA] : No proposal chosen	172.101.30.73:...	172.100.30.80:...	IKE_LOG
info	IKE	[SA] : Tunnel [VPN_to_SonicWALL] Phase 2 proposal mismatch	172.101.30.73:...	172.100.30.80:...	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	172.100.30.80:...	172.101.30.73:...	IKE_LOG
info	IKE	Phase 1 IKE SA process done	172.101.30.73:...	172.100.30.80:...	IKE_LOG

Make sure the both ZyWALL/USG and SonicWALL security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure IPSec VPN Failover

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with failover. The example instructs how to configure the VPN tunnel between each site if one site has multi-WAN. When the multi-WAN VPN failover is configured, IPSec VPN tunnels automatically fail over to a backup WAN interface if the primary WAN interface becomes unavailable.



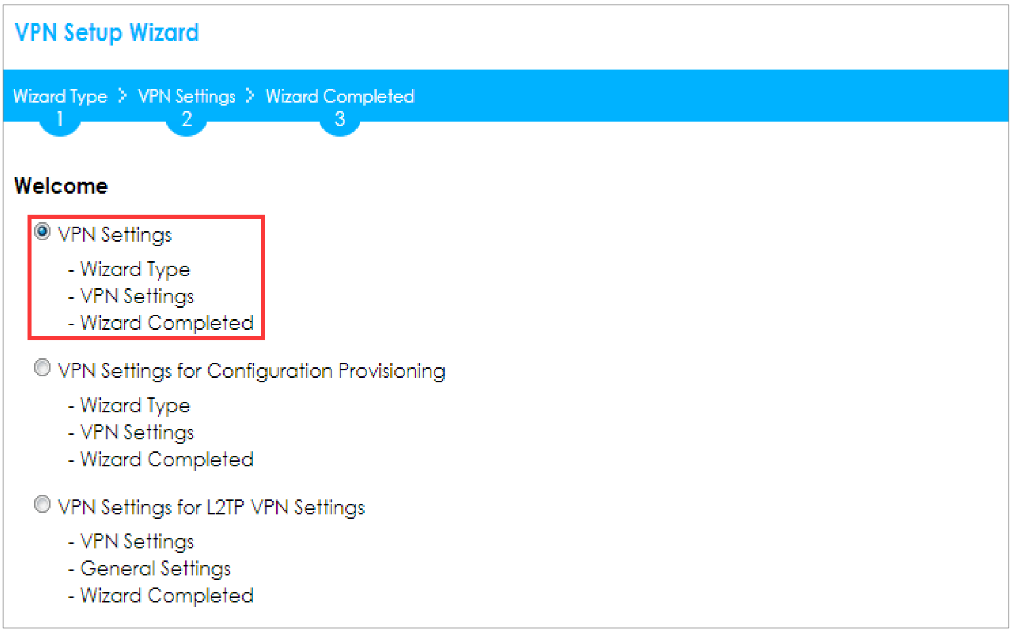
ZyWALL Site-to-site IPSec VPN with multiple WAN failover

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (HQ)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



Welcome

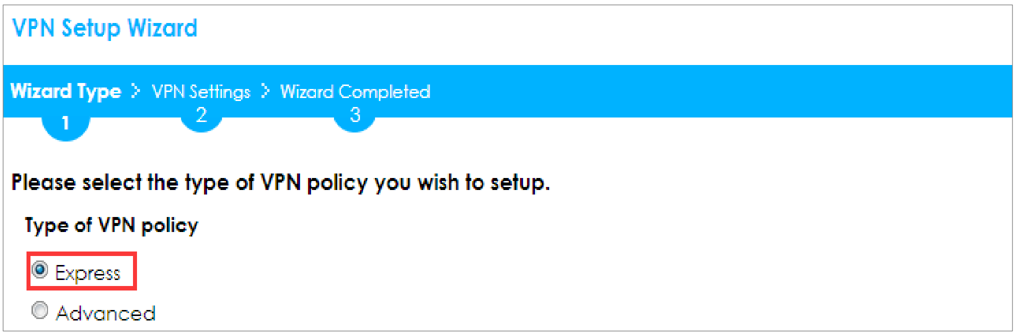
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



Please select the type of VPN policy you wish to setup.

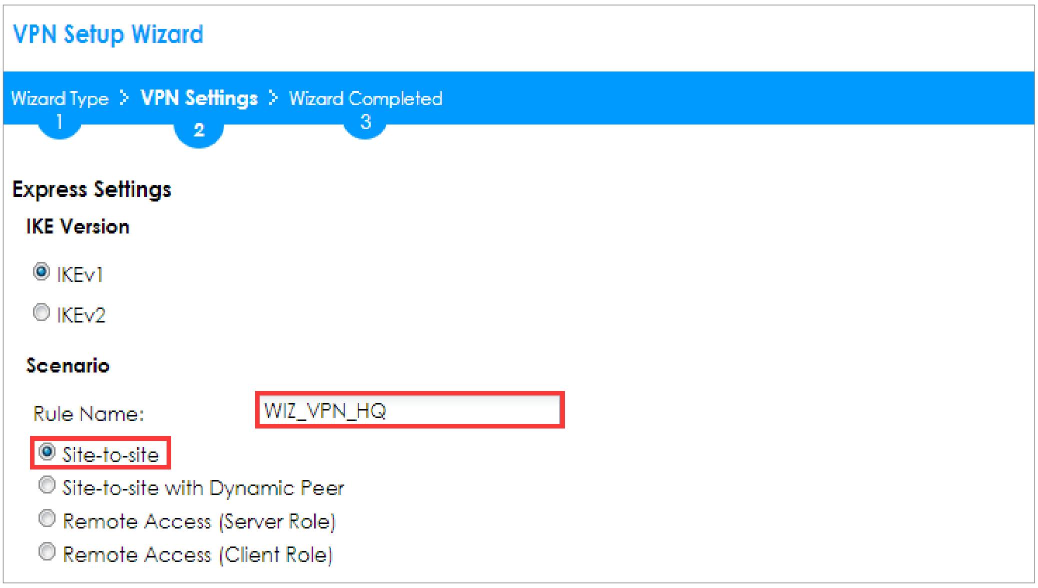
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Express Settings

IKE Version

● IKEv1
○ IKEv2

Scenario

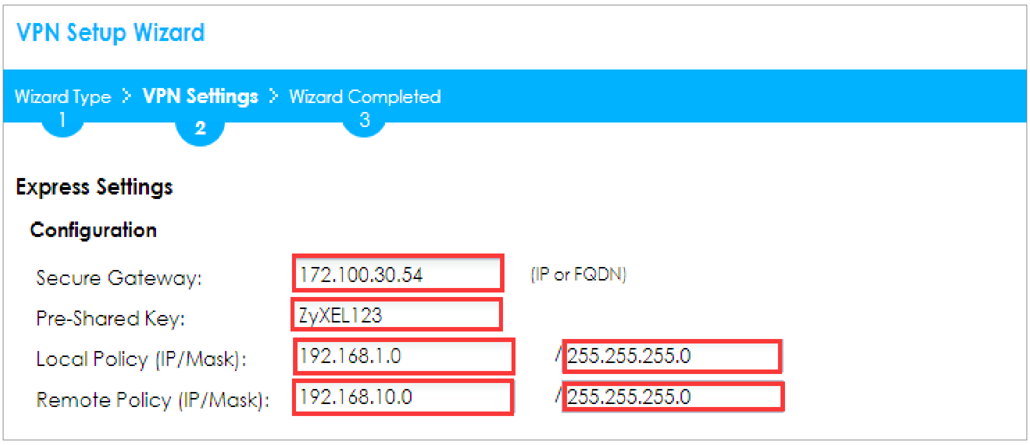
Rule Name: WIZ_VPN_HQ

● Site-to-site
○ Site-to-site with Dynamic Peer
○ Remote Access (Server Role)
○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.100.30.54). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZyWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



VPN Setup Wizard

Express Settings

Configuration

Secure Gateway: 172.100.30.54 (IP or FQDN)

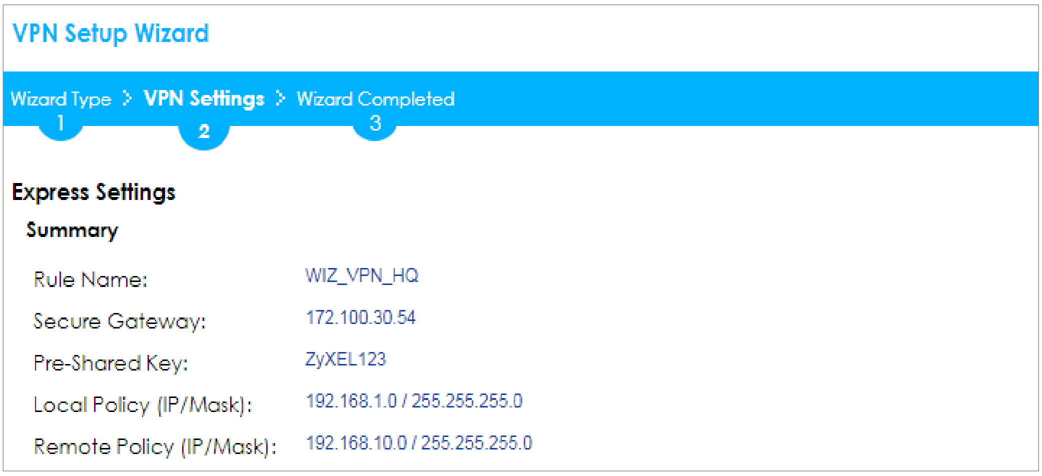
Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



VPN Setup Wizard

Express Settings

Summary

Rule Name: WIZ_VPN_HQ

Secure Gateway: 172.100.30.54

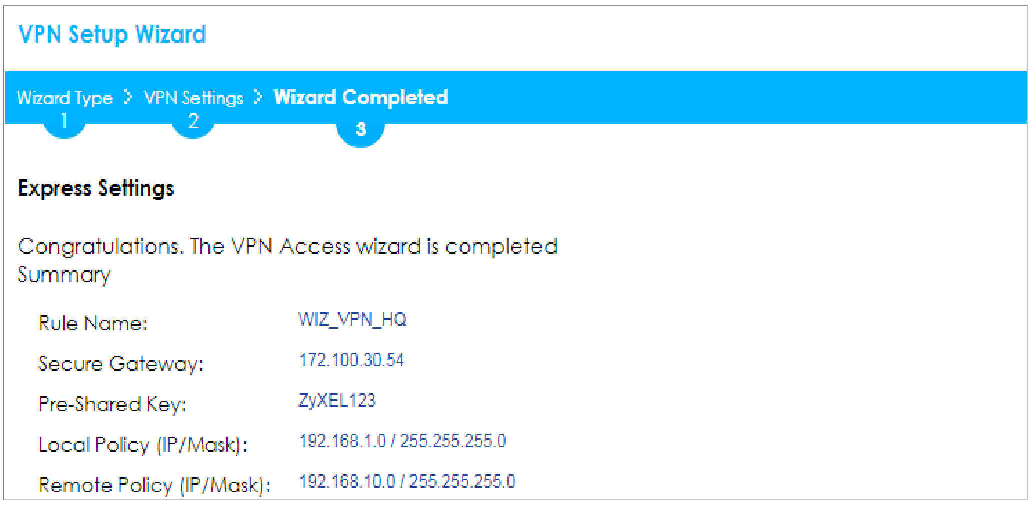
Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

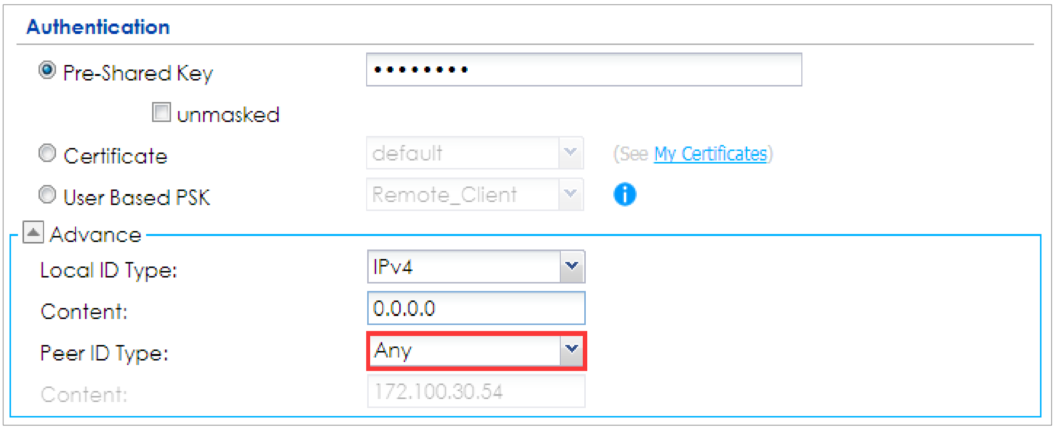
Express Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	WIZ_VPN_HQ
Secure Gateway:	172.100.30.54
Pre-Shared Key:	ZyXEL123
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

● Pre-Shared Key ••••••••

□ unmasked

○ Certificate default (See My Certificates)

○ User Based PSK Remote_Client

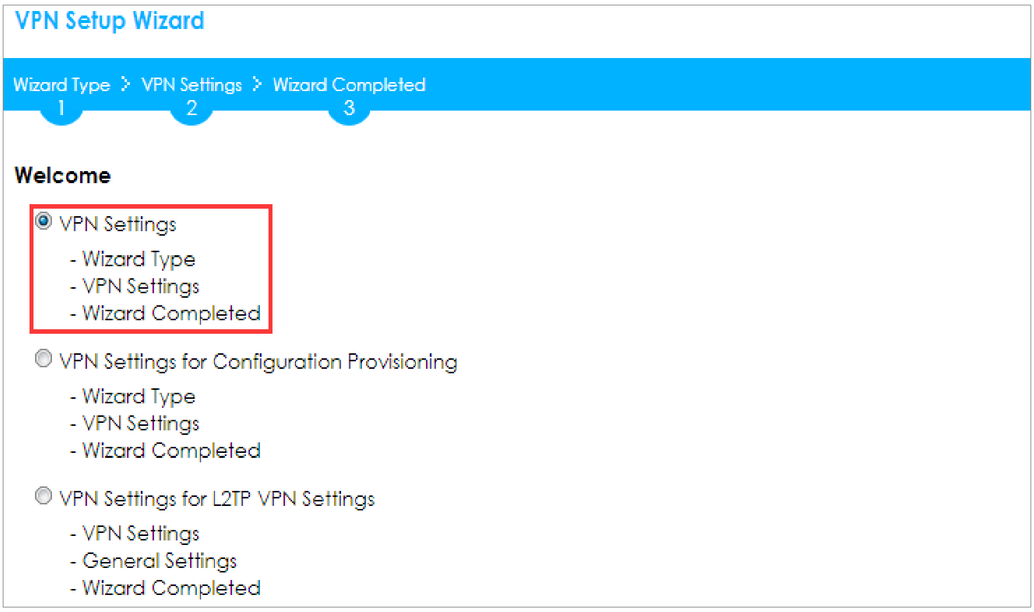
Advance

Local ID Type:	IPv4
Content:	0.0.0.0
Peer ID Type:	Any
Content:	172.100.30.54

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

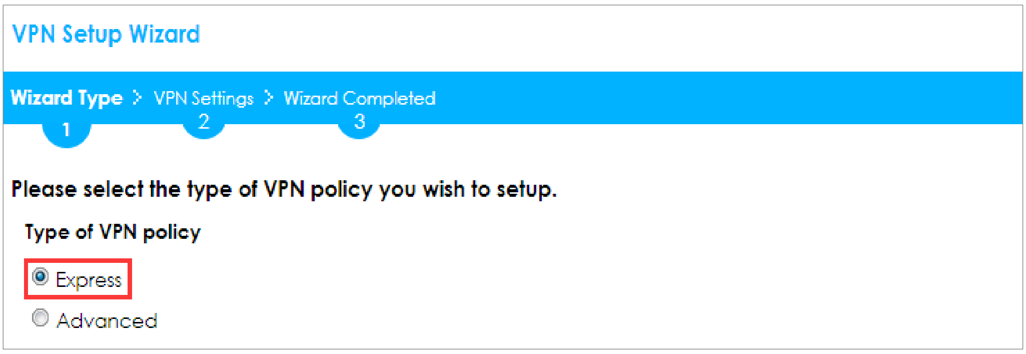
● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Please select the type of VPN policy you wish to setup.

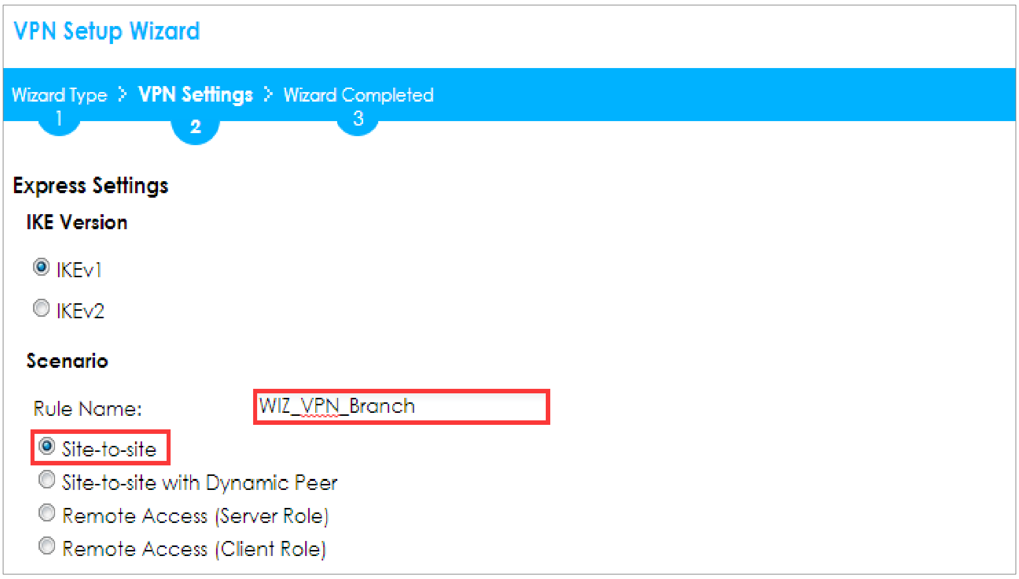
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch

● Site-to-site

○ Site-to-site with Dynamic Peer

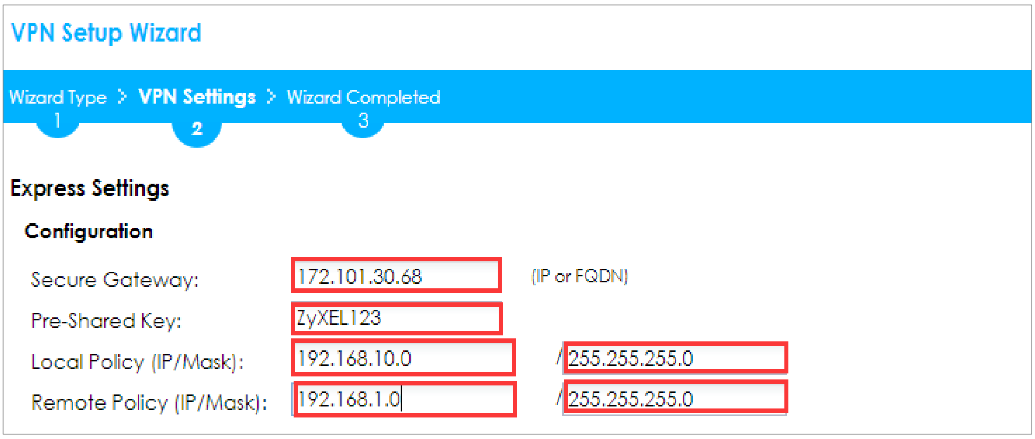
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.101.30.68). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZYWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



VPN Setup Wizard

Express Settings

Configuration

Secure Gateway: 172.101.30.68 (IP or FQDN)

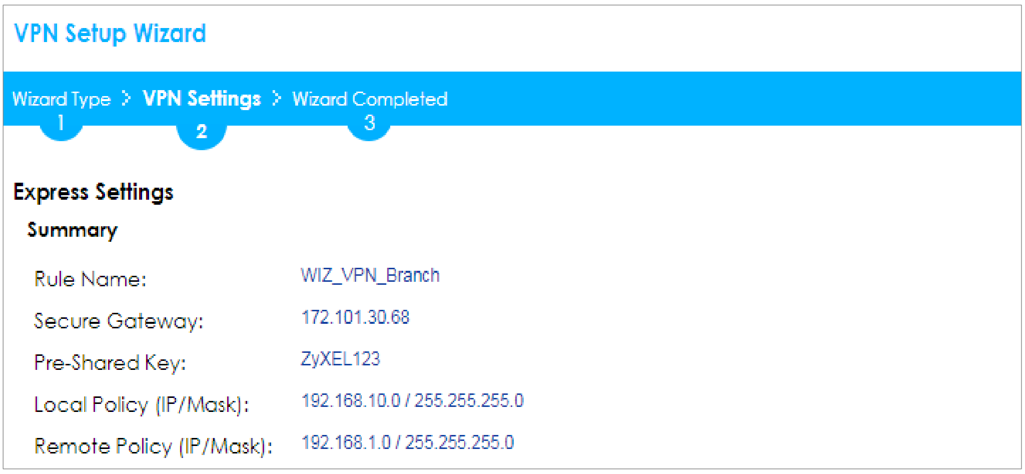
Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



Express Settings

Summary

Rule Name: WIZ_VPN_Branch

Secure Gateway: 172.101.30.68

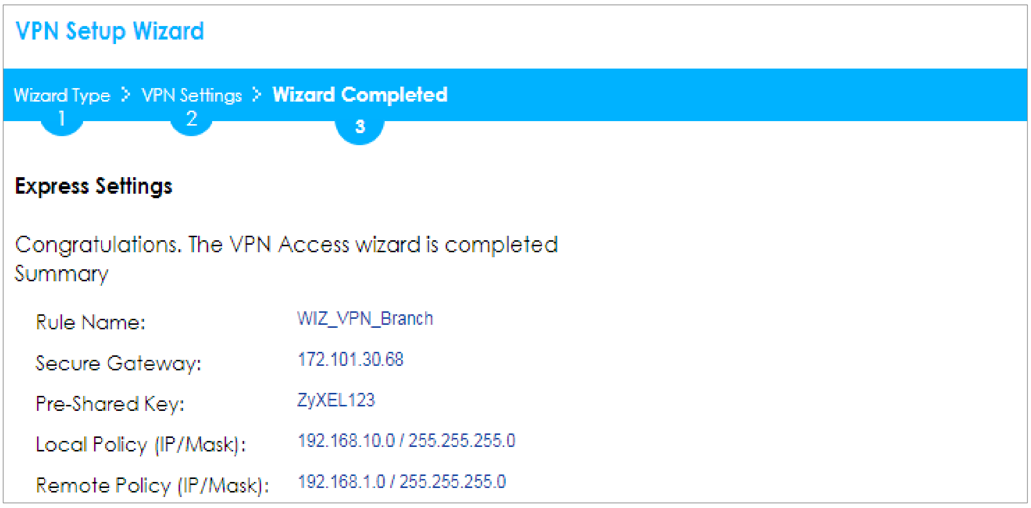
Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name: WIZ_VPN_Branch

Secure Gateway: 172.101.30.68

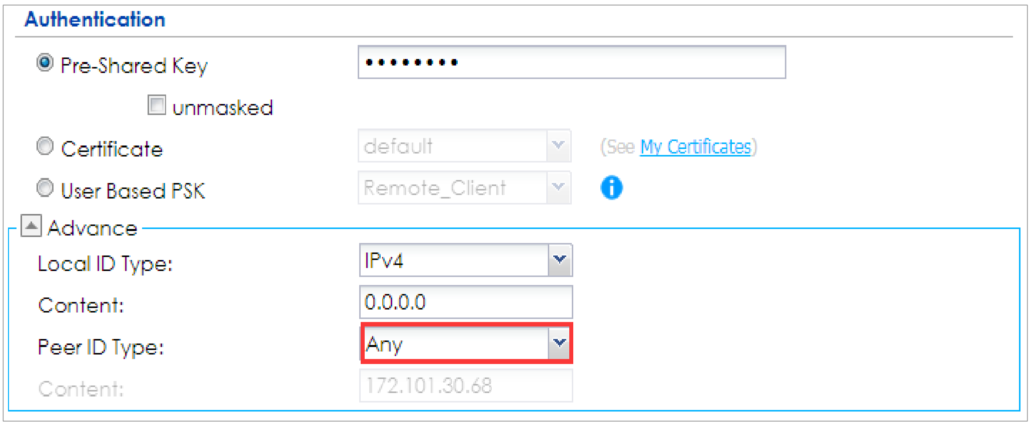
Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings. Configure Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

● Pre-Shared Key: ••••••••

□ unmasked

○ Certificate: default (See My Certificates)

○ User Based PSK: Remote_Client

Advance

Local ID Type: IPv4

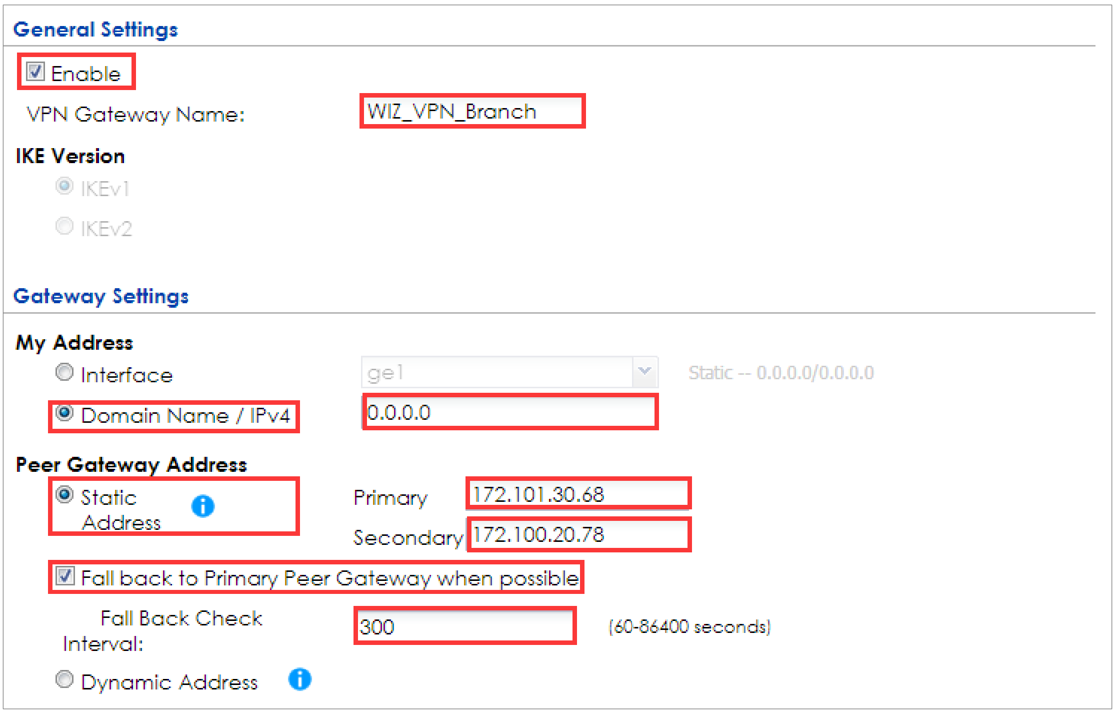
Content: 0.0.0.0

Peer ID Type: Any

Content: 172.101.30.68

Go to **Configuration > VPN > IPSec VPN > VPN Gateway > Gateway Settings**. Set **My Address** to be **Domain Name/IP** "0.0.0.0" (ZyWALL/USG will dial-up with the active WAN interface first). Set **Peer Gateway Address > Static Address > Primary** to be ZyWALL/USG_HQ WAN1 IP address and **Secondary** to be ZyWALL/USG_HQ WAN2 IP address.

Configuration > VPN > IPSec VPN > VPN Gateway > Gateway Settings



General Settings

☑ Enable

VPN Gateway Name: WIZ_VPN_Branch

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

○ Interface: ge1 Static -- 0.0.0.0/0.0.0.0

● Domain Name / IPv4: 0.0.0.0

Peer Gateway Address

● Static Address: Primary 172.101.30.68

Secondary 172.100.20.78

☑ Fall back to Primary Peer Gateway when possible

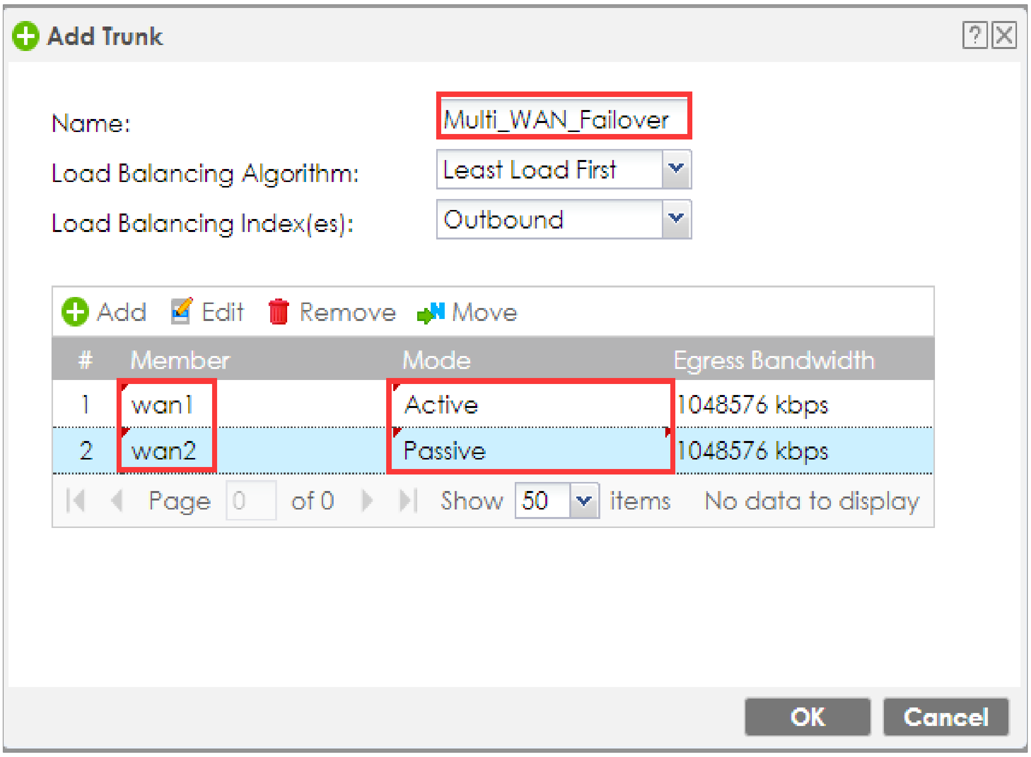
Fall Back Check Interval: 300 (60-86400 seconds)

○ Dynamic Address

Set up the WAN Trunk (ZyWALL/USG_HQ)

Go to **CONFIGURATION > Interface > Trunk > User Configuration > Add**. Select wan1 and wan2 into the trunk **Member** and set wan2 **Mode** to be **Passive**.

CONFIGURATION > Interface > Trunk > User Configuration > Add



Name: Multi_WAN_Failover

Load Balancing Algorithm: Least Load First

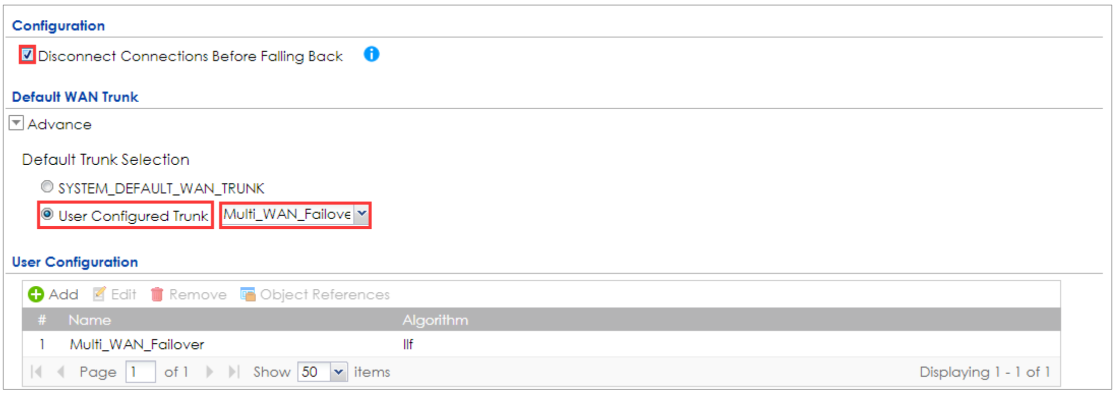
Load Balancing Index(es): Outbound

#	Member	Mode	Egress Bandwidth
1	wan1	Active	1048576 kbps
2	wan2	Passive	1048576 kbps

Page 0 of 0 Show 50 items No data to display

Go to **CONFIGURATION > Interface > Trunk > Configuration**. Select **Disconnect Connection before Falling Back**. In the **Default WAN Trunk**, select **User Configured Trunk** to be the customized WAN trunk added in the previous step (Multi_WAN_Failover in this example).

CONFIGURATION > Interface > Trunk > User Configuration > Add



Configuration

☑ Disconnect Connections Before Falling Back

Default WAN Trunk

Advance

Default Trunk Selection

○ SYSTEM_DEFAULT_WAN_TRUNK

● User Configured Trunk: Multi_WAN_Failove

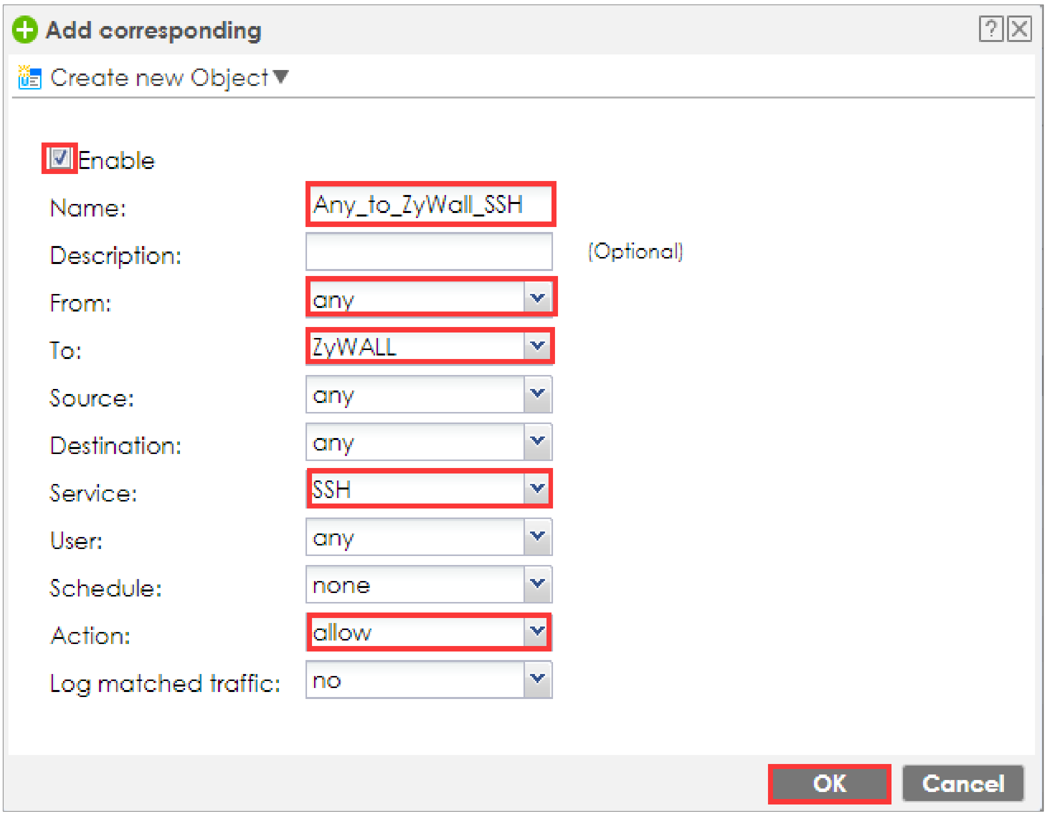
User Configuration

#	Name	Algorithm
1	Multi_WAN_Failover	llf

Set up the Failover Command Line (ZyWALL/USG HQ)

Go to **CONFIGURATION > Security Policy > Policy Control** and add a **To ZyWALL** rule to allow **SSH** service.

CONFIGURATION > Security Policy > Policy Control > Add corresponding



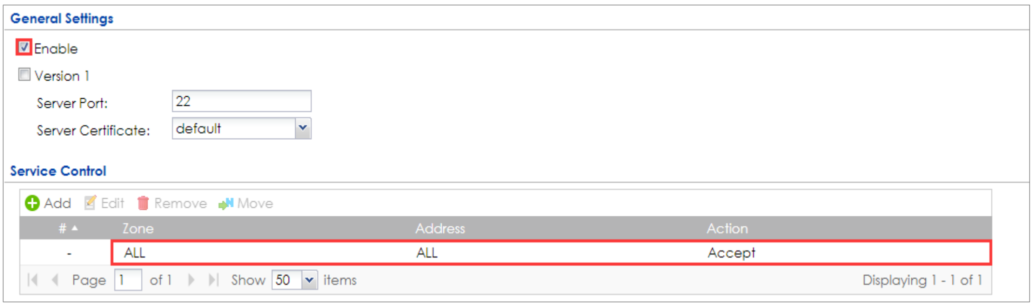
Add corresponding

☑ Enable

Name:	Any_to_ZyWall_SSH
Description:	(Optional)
From:	any
To:	ZyWALL
Source:	any
Destination:	any
Service:	SSH
User:	any
Schedule:	none
Action:	allow
Log matched traffic:	no

If the **Security Policy** is created but still cannot access to ZyWALL, please go to **CONFIGURAITON > System > SSH** to check do you **Enable** the **General Settings** and make sure the **Service Port** is correct and the same in your terminal program. Then, check the **Service Control Action** should be **Accept**.

CONFIGURAITON > System > SSH



General Settings

☑ Enable

☐ Version 1

Server Port: 22

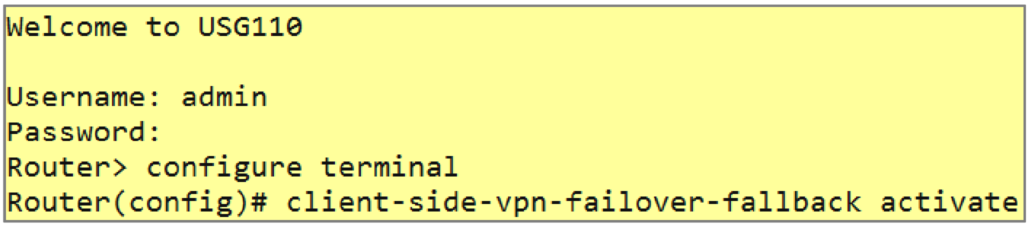
Server Certificate: default

Service Control

#	Zone	Address	Action
-	ALL	ALL	Accept

Enter the command line in terminal mode (Using Tera Term in this example).

Tera Term command

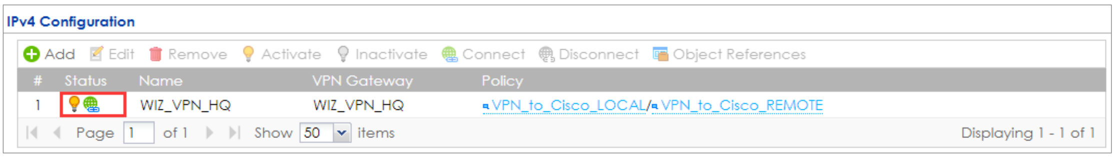


```
Welcome to USG110

Username: admin
Password:
Router> configure terminal
Router(config)# client-side-vpn-failover-fallback activate
```

Test the IPSec VPN Tunnel

8 Go to ZYWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

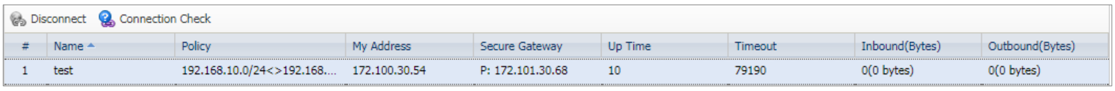


IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1		WIZ_VPN_HQ	WIZ_VPN_HQ	VPN_to_Cisco_LOCAL/VPN_to_Cisco_REMOTE

9 Go to ZyWALL/USG MONITOR > VPN Monitor > IPSec and verify the tunnel Up Time and Inbound(Bytes)/Outbound(Bytes) Traffic.

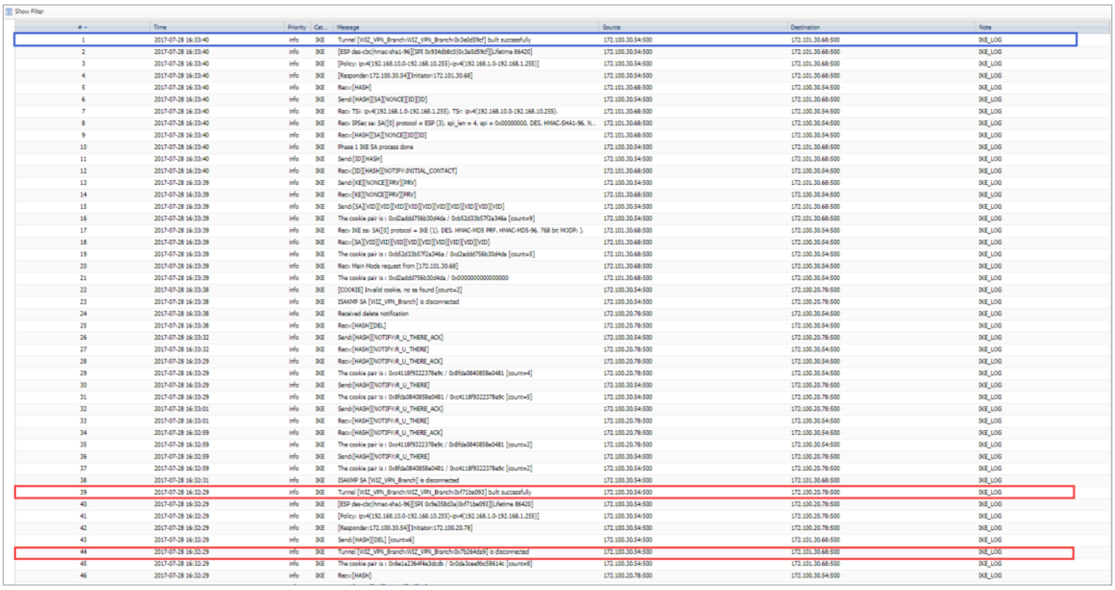
MONITOR > VPN Monitor > IPSec



#	Name ▲	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound(Bytes)	Outbound(Bytes)
1	test	192.168.10.0/24<>192.168....	172.100.30.54	P: 172.101.30.68	10	79190	0(0 bytes)	0(0 bytes)

10 Go to ZyWALL/USG_Branch **MONITOR > Log**. Try to disconnect WAN1 interface (172.1.1.30.68) and you will see the VPN tunnel failover to WAN2 interface (172.100.20.78).

MONITOR > Log

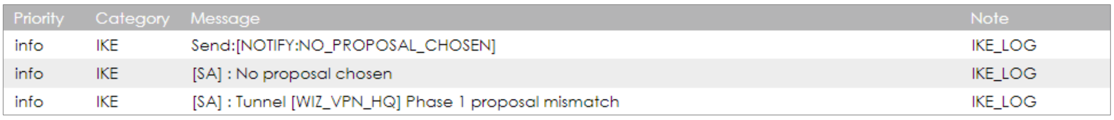


```
# ▲  Time                 Priority  Cat...  Message                                                                                             Source               Destination          Note
1    2017-07-28 16:33:40  info      IKE     Tunnel [WIZ_VPN_Branch:WIZ_VPN_Branch:0x3e0d59cf] built successfully                                172.100.30.54:500    172.101.30.68:500    IKE_LOG
2    2017-07-28 16:33:40  info      IKE     [ESP des-cbc|hmac-sha1-96][SPI 0x934db8c0|0x3e0d59cf][Lifetime 86420]                               172.100.30.54:500    172.101.30.68:500    IKE_LOG
3    2017-07-28 16:33:40  info      IKE     [Policy: ipv4(192.168.10.0-192.168.10.255)-ipv4(192.168.1.0-192.168.1.255)]                         172.100.30.54:500    172.101.30.68:500    IKE_LOG
4    2017-07-28 16:33:40  info      IKE     [Responder:172.100.30.54][Initiator:172.101.30.68]                                                  172.100.30.54:500    172.101.30.68:500    IKE_LOG
5    2017-07-28 16:33:40  info      IKE     Recv:[HASH]                                                                                         172.101.30.68:500    172.100.30.54:500    IKE_LOG
6    2017-07-28 16:33:40  info      IKE     Send:[HASH][SA][NONCE][ID][ID]                                                                      172.100.30.54:500    172.101.30.68:500    IKE_LOG
7    2017-07-28 16:33:40  info      IKE     Recv TSi: ipv4(192.168.1.0-192.168.1.255), TSr: ipv4(192.168.10.0-192.168.10.255).                  172.101.30.68:500    172.100.30.54:500    IKE_LOG
8    2017-07-28 16:33:40  info      IKE     Recv IPSec sa: SA([0] protocol = ESP (3), spi_len = 4, spi = 0x00000000, DES, HMAC-SHA1-96, N...     172.101.30.68:500    172.100.30.54:500    IKE_LOG
9    2017-07-28 16:33:40  info      IKE     Recv:[HASH][SA][NONCE][ID][ID]                                                                      172.101.30.68:500    172.100.30.54:500    IKE_LOG
10   2017-07-28 16:33:40  info      IKE     Phase 1 IKE SA process done                                                                         172.100.30.54:500    172.101.30.68:500    IKE_LOG
11   2017-07-28 16:33:40  info      IKE     Send:[ID][HASH]                                                                                     172.100.30.54:500    172.101.30.68:500    IKE_LOG
12   2017-07-28 16:33:40  info      IKE     Recv:[ID][HASH][NOTIFY:INITIAL_CONTACT]                                                             172.101.30.68:500    172.100.30.54:500    IKE_LOG
13   2017-07-28 16:33:39  info      IKE     Send:[KE][NONCE][PRV][PRV]                                                                          172.100.30.54:500    172.101.30.68:500    IKE_LOG
14   2017-07-28 16:33:39  info      IKE     Recv:[KE][NONCE][PRV][PRV]                                                                          172.101.30.68:500    172.100.30.54:500    IKE_LOG
15   2017-07-28 16:33:39  info      IKE     Send:[SA][VID][VID][VID][VID][VID][VID][VID][VID][VID][VID]                                         172.100.30.54:500    172.101.30.68:500    IKE_LOG
16   2017-07-28 16:33:39  info      IKE     The cookie pair is : 0xd2addd756b30d4da / 0xb52d33b57f2a346a [count=9]                              172.100.30.54:500    172.101.30.68:500    IKE_LOG
17   2017-07-28 16:33:39  info      IKE     Recv IKE sa: SA([0] protocol = IKE (1), DES, HMAC-MD5 PRF, HMAC-MD5-96, 768 bit MODP; ).            172.101.30.68:500    172.100.30.54:500    IKE_LOG
18   2017-07-28 16:33:39  info      IKE     Recv:[SA][VID][VID][VID][VID][VID][VID][VID][VID][VID]                                              172.101.30.68:500    172.100.30.54:500    IKE_LOG
19   2017-07-28 16:33:39  info      IKE     The cookie pair is : 0xb52d33b57f2a346a / 0xd2addd756b30d4da [count=5]                              172.101.30.68:500    172.100.30.54:500    IKE_LOG
20   2017-07-28 16:33:39  info      IKE     Recv Main Mode request from [172.101.30.68]                                                         172.101.30.68:500    172.100.30.54:500    IKE_LOG
21   2017-07-28 16:33:39  info      IKE     The cookie pair is : 0xd2addd756b30d4da / 0x0000000000000000                                        172.101.30.68:500    172.100.30.54:500    IKE_LOG
22   2017-07-28 16:33:38  info      IKE     [COOKIE] Invalid cookie, no sa found [count=2]                                                      172.100.30.54:500    172.100.20.78:500    IKE_LOG
23   2017-07-28 16:33:38  info      IKE     ISAKMP SA [WIZ_VPN_Branch] is disconnected                                                          172.100.30.54:500    172.100.20.78:500    IKE_LOG
24   2017-07-28 16:33:38  info      IKE     Received delete notification                                                                        172.100.20.78:500    172.100.30.54:500    IKE_LOG
25   2017-07-28 16:33:38  info      IKE     Recv:[HASH][DEL]                                                                                    172.100.20.78:500    172.100.30.54:500    IKE_LOG
26   2017-07-28 16:33:32  info      IKE     Send:[HASH][NOTIFY:R_U_THERE_ACK]                                                                   172.100.30.54:500    172.100.20.78:500    IKE_LOG
27   2017-07-28 16:33:32  info      IKE     Recv:[HASH][NOTIFY:R_U_THERE]                                                                       172.100.20.78:500    172.100.30.54:500    IKE_LOG
28   2017-07-28 16:33:29  info      IKE     Recv:[HASH][NOTIFY:R_U_THERE_ACK]                                                                   172.100.20.78:500    172.100.30.54:500    IKE_LOG
29   2017-07-28 16:33:29  info      IKE     The cookie pair is : 0xc4118f9322378a9c / 0x8fda0840858a0481 [count=4]                              172.100.20.78:500    172.100.30.54:500    IKE_LOG
30   2017-07-28 16:33:29  info      IKE     Send:[HASH][NOTIFY:R_U_THERE]                                                                       172.100.30.54:500    172.100.20.78:500    IKE_LOG
31   2017-07-28 16:33:29  info      IKE     The cookie pair is : 0x8fda0840858a0481 / 0xc4118f9322378a9c [count=5]                              172.100.30.54:500    172.100.20.78:500    IKE_LOG
32   2017-07-28 16:33:01  info      IKE     Send:[HASH][NOTIFY:R_U_THERE_ACK]                                                                   172.100.30.54:500    172.100.20.78:500    IKE_LOG
33   2017-07-28 16:33:01  info      IKE     Recv:[HASH][NOTIFY:R_U_THERE]                                                                       172.100.20.78:500    172.100.30.54:500    IKE_LOG
34   2017-07-28 16:32:59  info      IKE     Recv:[HASH][NOTIFY:R_U_THERE_ACK]                                                                   172.100.20.78:500    172.100.30.54:500    IKE_LOG
35   2017-07-28 16:32:59  info      IKE     The cookie pair is : 0xc4118f9322378a9c / 0x8fda0840858a0481 [count=2]                              172.100.20.78:500    172.100.30.54:500    IKE_LOG
36   2017-07-28 16:32:59  info      IKE     Send:[HASH][NOTIFY:R_U_THERE]                                                                       172.100.30.54:500    172.100.20.78:500    IKE_LOG
37   2017-07-28 16:32:59  info      IKE     The cookie pair is : 0x8fda0840858a0481 / 0xc4118f9322378a9c [count=2]                              172.100.30.54:500    172.100.20.78:500    IKE_LOG
38   2017-07-28 16:32:31  info      IKE     ISAKMP SA [WIZ_VPN_Branch] is disconnected                                                          172.100.30.54:500    172.101.30.68:500    IKE_LOG
39   2017-07-28 16:32:29  info      IKE     Tunnel [WIZ_VPN_Branch:WIZ_VPN_Branch:0xf71ba093] built successfully                                172.100.30.54:500    172.100.20.78:500    IKE_LOG
40   2017-07-28 16:32:29  info      IKE     [ESP des-cbc|hmac-sha1-96][SPI 0x9a358d3a|0xf71ba093][Lifetime 86420]                               172.100.30.54:500    172.100.20.78:500    IKE_LOG
41   2017-07-28 16:32:29  info      IKE     [Policy: ipv4(192.168.10.0-192.168.10.255)-ipv4(192.168.1.0-192.168.1.255)]                         172.100.30.54:500    172.100.20.78:500    IKE_LOG
42   2017-07-28 16:32:29  info      IKE     [Responder:172.100.30.54][Initiator:172.100.20.78]                                                  172.100.30.54:500    172.100.20.78:500    IKE_LOG
43   2017-07-28 16:32:29  info      IKE     Send:[HASH][DEL] [count=6]                                                                          172.100.30.54:500    172.101.30.68:500    IKE_LOG
44   2017-07-28 16:32:29  info      IKE     Tunnel [WIZ_VPN_Branch:WIZ_VPN_Branch:0x7b264da9] is disconnected                                   172.100.30.54:500    172.101.30.68:500    IKE_LOG
45   2017-07-28 16:32:29  info      IKE     The cookie pair is : 0x6a1a2364f4a3dcdb / 0x0da3cea9bc58614c [count=8]                              172.100.30.54:500    172.101.30.68:500    IKE_LOG
46   2017-07-28 16:32:29  info      IKE     Recv:[HASH]                                                                                         172.100.20.78:500    172.100.30.54:500    IKE_LOG
```

What Could Go Wrong?

11 If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

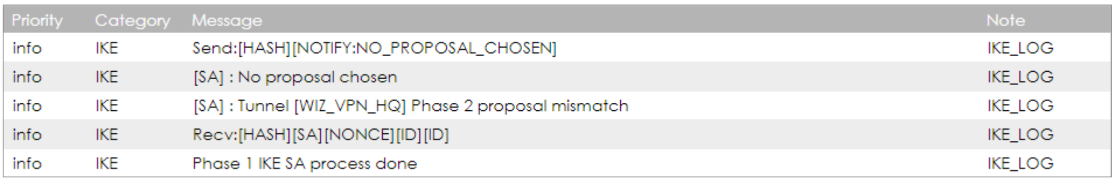
MONITOR > Log



Priority	Category	Message	Note
info	IKE	Send:[NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [WIZ_VPN_HQ] Phase 1 proposal mismatch	IKE_LOG

12 If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log



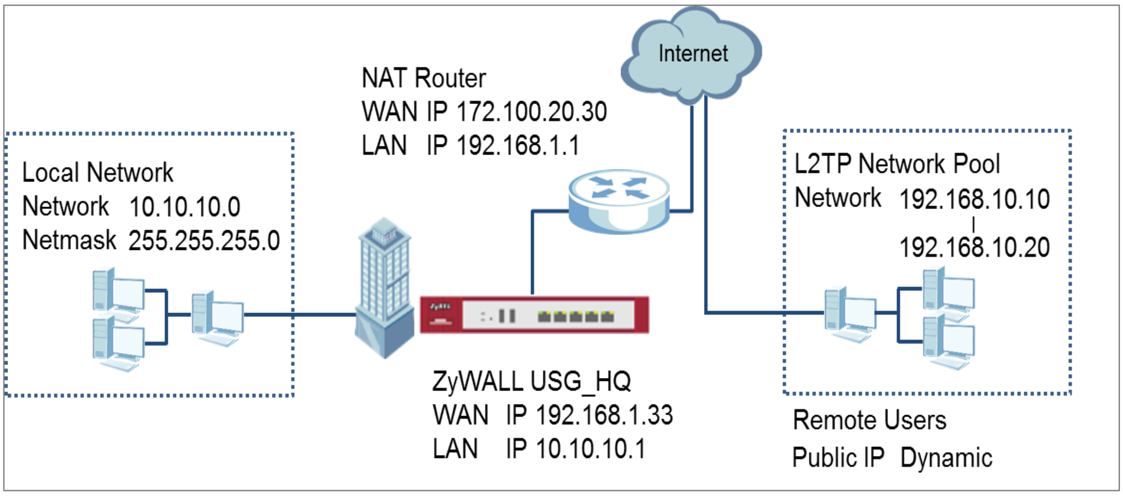
Priority	Category	Message	Note
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [WIZ_VPN_HQ] Phase 2 proposal mismatch	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Phase 1 IKE SA process done	IKE_LOG

13 Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

14 Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Configure L2TP over IPSec VPN while the ZyWALL/USG is behind a NAT router

This example shows how to use the VPN Setup Wizard to create a L2TP over IPSec VPN tunnel between ZyWALL/USG devices. The example instructs how to configure the VPN tunnel between each site while the ZyWALL/USG is behind a NAT router. When the L2TP over IPSec VPN tunnel is configured, each site can be accessed securely.



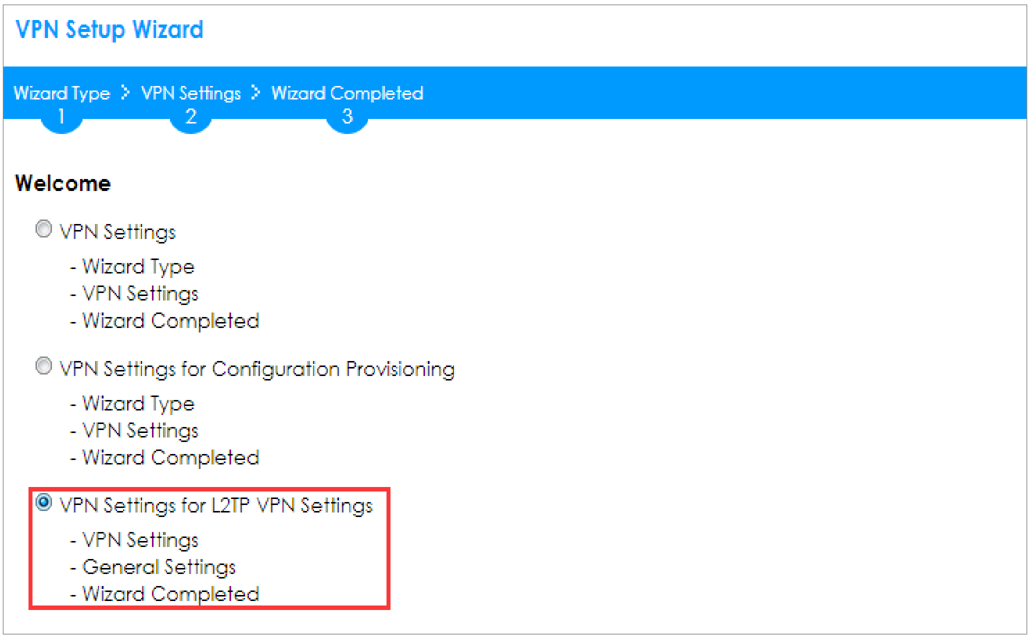
ZyWALL/USG L2TP over IPSec VPN while the ZyWALL/USG is behind a NAT router

Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the L2TP VPN Tunnel on the ZyWALL/USG_HQ

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the remote Android Mobile Devices. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Welcome

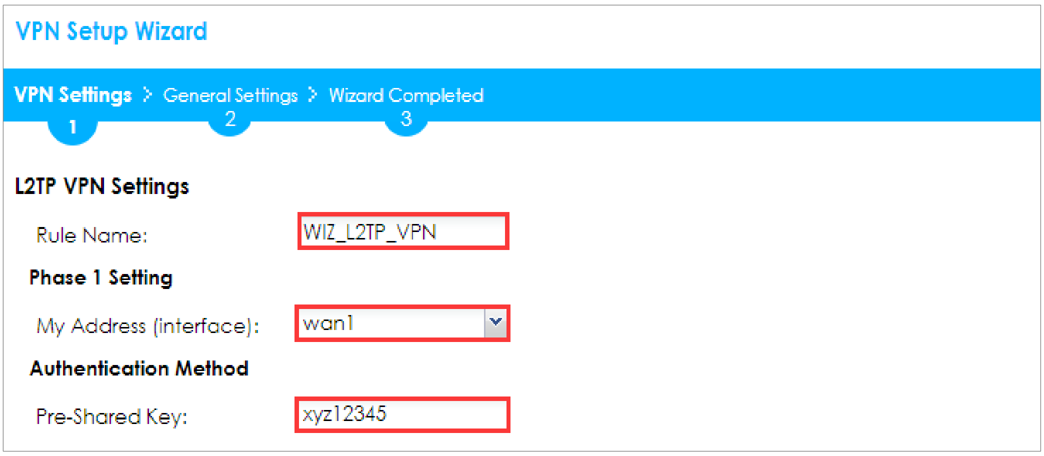
○ VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

● VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



VPN Setup Wizard

VPN Settings 1 > General Settings 2 > Wizard Completed 3

L2TP VPN Settings

Rule Name: WIZ_L2TP_VPN

Phase 1 Setting

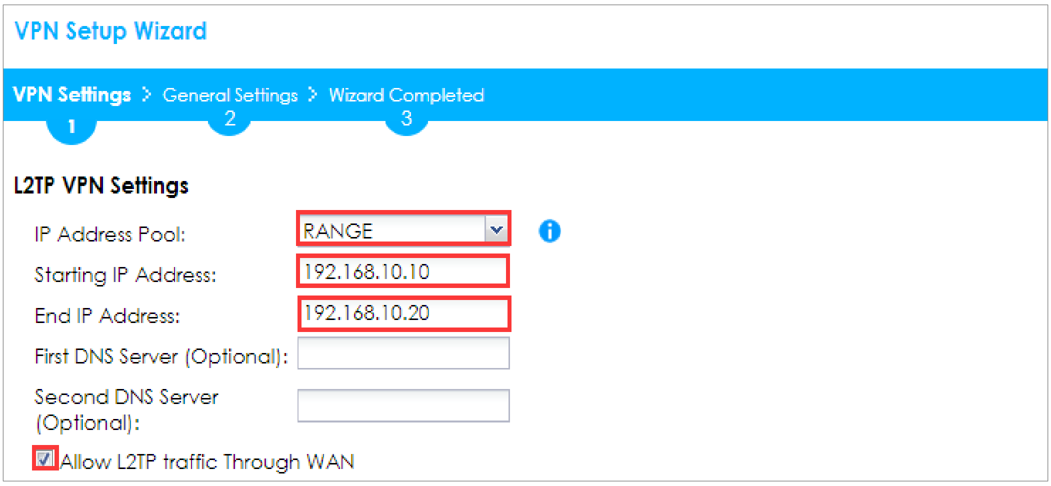
My Address (interface): wan1

Authentication Method

Pre-Shared Key: xyz12345

Assign the remote users IP addresses range from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)



L2TP VPN Settings

IP Address Pool: RANGE

Starting IP Address: 192.168.10.10

End IP Address: 192.168.10.20

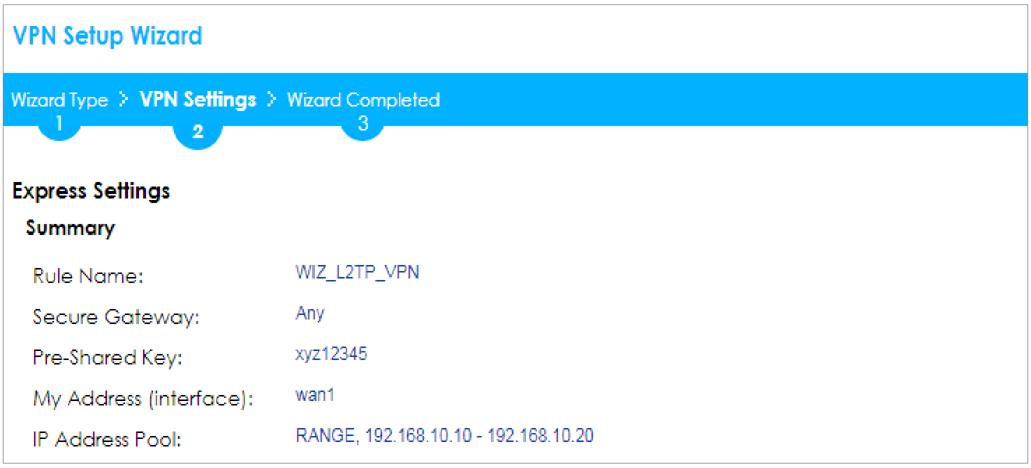
First DNS Server (Optional):

Second DNS Server (Optional):

☑ Allow L2TP traffic Through WAN

15 This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)



Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

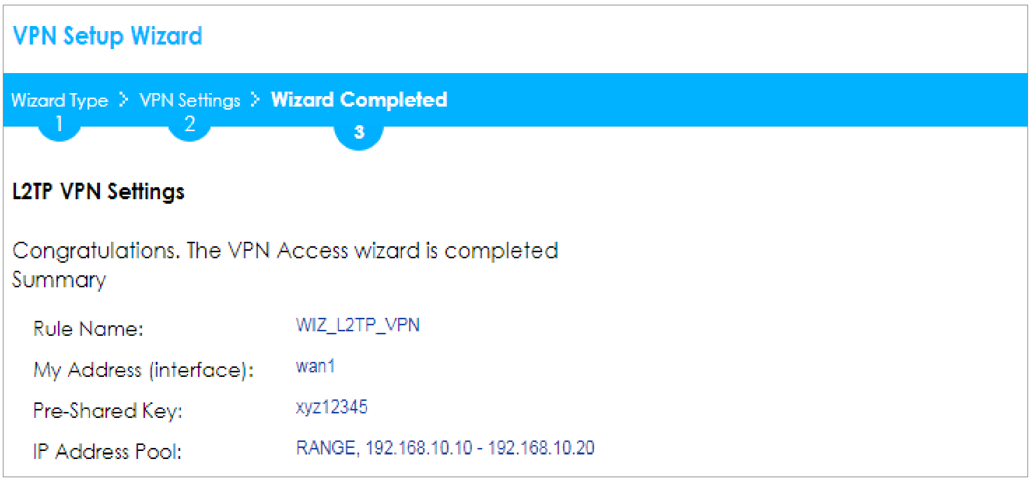
Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Wizard Completed



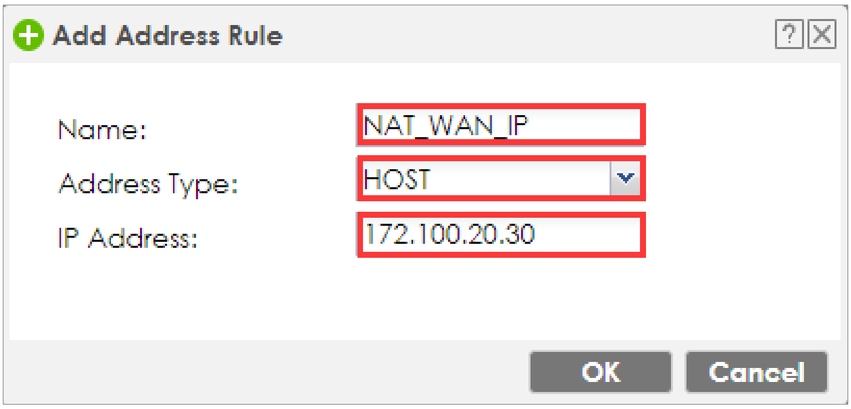
L2TP VPN Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	WIZ_L2TP_VPN
My Address (interface):	wan1
Pre-Shared Key:	xyz12345
IP Address Pool:	RANGE, 192.168.10.10 - 192.168.10.20

Go to **CONFIGURATION > VPN Connection > Create new Object > Create Address**, create an address object as the NAT router's WAN IP address (in the example, 172.100.20.30).

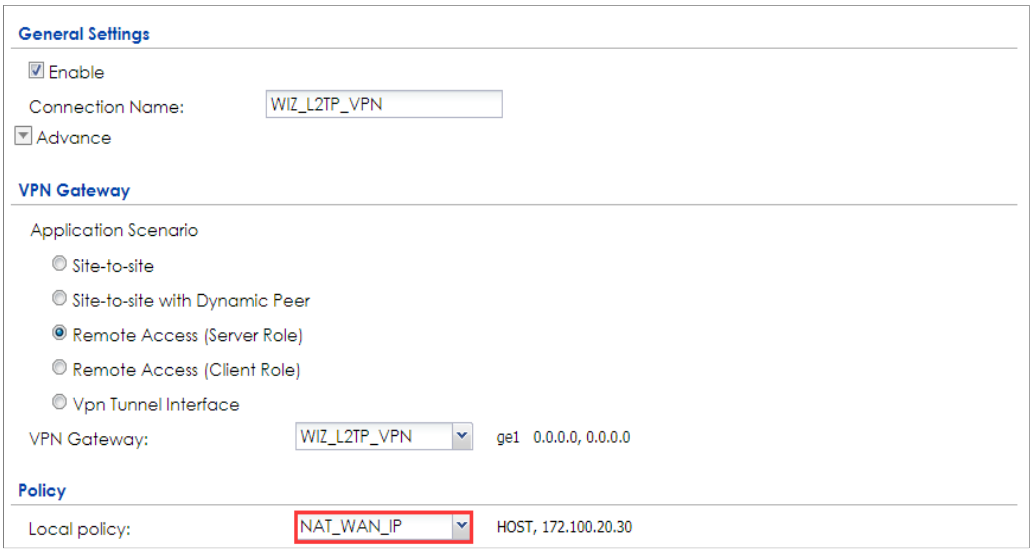
CONFIGURATION > VPN Connection > Create new Object > Create Address



Name:	NAT_WAN_IP
Address Type:	HOST
IP Address:	172.100.20.30

Go to **CONFIGURATION > VPN Connection > Policy > Local Policy**, select it be to the NAT router's WAN IP address (in the example, 172.100.20.30).

CONFIGURATION > VPN Connection > Policy > Local Policy



General Settings

☑ Enable

Connection Name: WIZ_L2TP_VPN

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

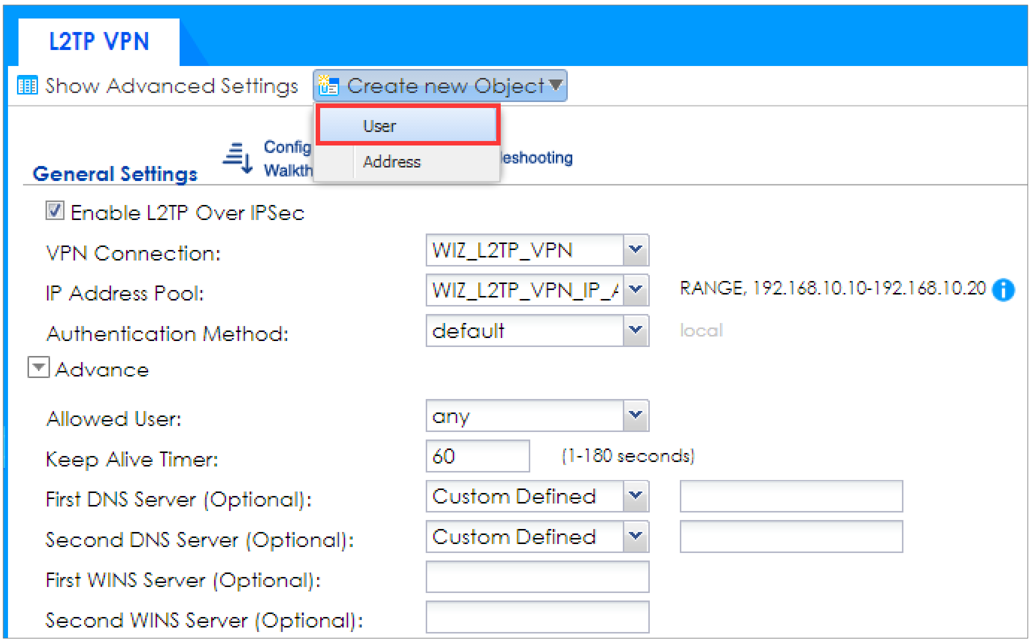
VPN Gateway: WIZ_L2TP_VPN ge1 0.0.0.0, 0.0.0.0

Policy

Local policy: NAT_WAN_IP HOST, 172.100.20.30

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User



☑ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_/ RANGE, 192.168.10.10-192.168.10.20

Authentication Method: default local

Advance

Allowed User: any

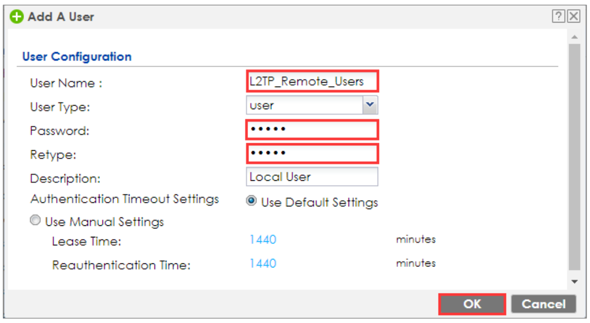
Keep Alive Timer: 60 (1-180 seconds)

First DNS Server (Optional): Custom Defined

Second DNS Server (Optional): Custom Defined

First WINS Server (Optional):

Second WINS Server (Optional):



User Configuration

User Name : L2TP_Remote_Users

User Type: user

Password: •••••

Retype: •••••

Description: Local User

Authentication Timeout Settings ● Use Default Settings

○ Use Manual Settings

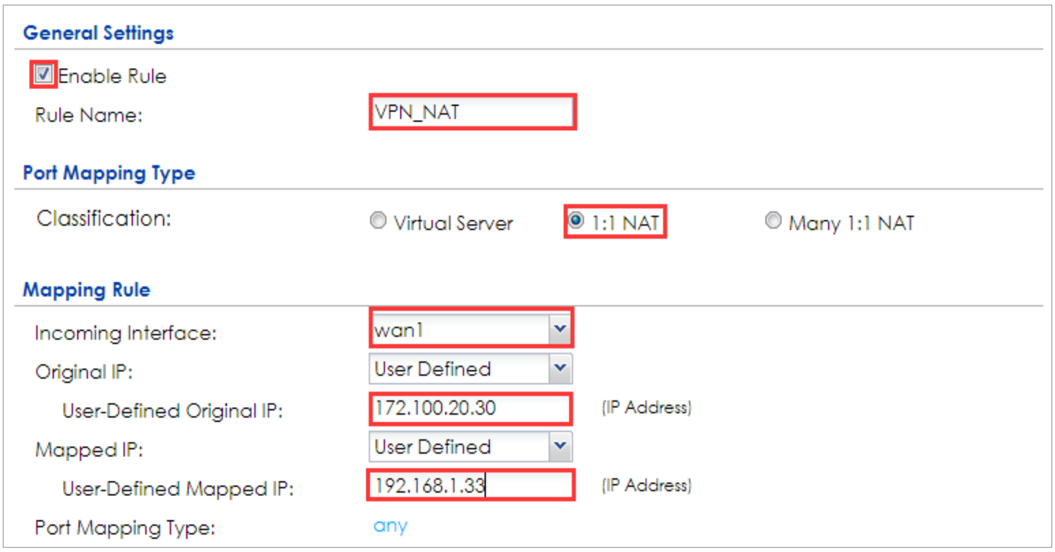
Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Set Up the NAT Router (Using ZyWALL USG device in this example)

Go to **CONFIGURATION > Network > NAT > Add**. Select the **Incoming Interface** on which packets for the NAT rule must be received. Specified the **User-Defined Original IP** field and Type the translated destination IP address that this NAT rule supports.

CONFIGURATION > Network > NAT > Add



General Settings

☑ Enable Rule

Rule Name: VPN_NAT

Port Mapping Type

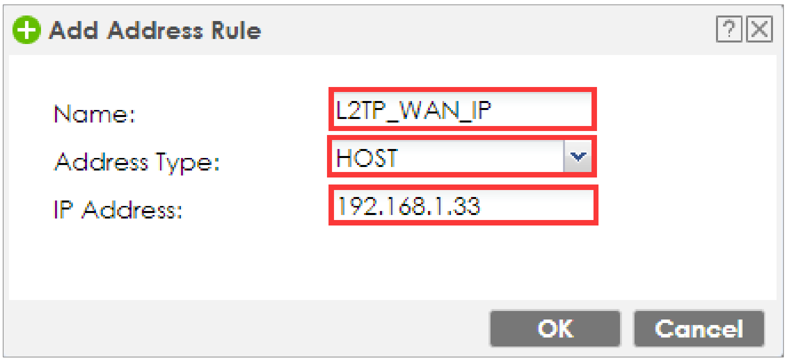
Classification: ○ Virtual Server ● 1:1 NAT ○ Many 1:1 NAT

Mapping Rule

Incoming Interface:	wan1	
Original IP:	User Defined	
User-Defined Original IP:	172.100.20.30	(IP Address)
Mapped IP:	User Defined	
User-Defined Mapped IP:	192.168.1.33	(IP Address)
Port Mapping Type:	any	

Go to **CONFIGURATION > Object > Address > Add**, create an address object as the ZyWALL/USU_HQ's WAN IP address (in the example, 192.168.1.33).

CONFIGURATION > Object > Address



Add Address Rule

Name:	L2TP_WAN_IP
Address Type:	HOST
IP Address:	192.168.1.33

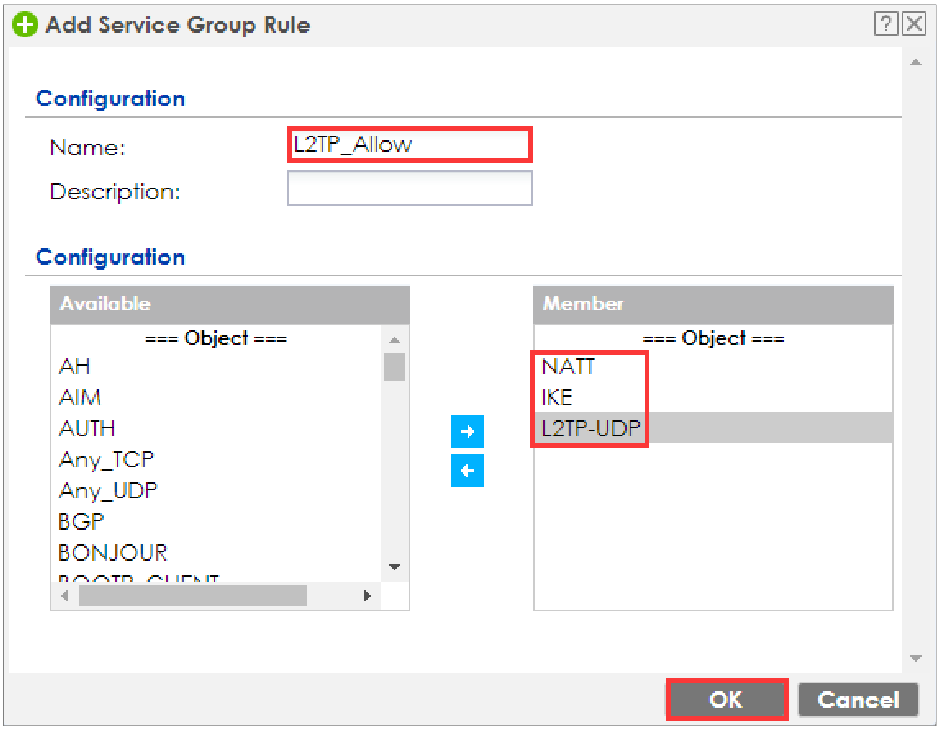
Go to **CONFIGURATION > Object > Service > Service Group**, create a service group for the following UDP ports:

UDP Port Number = 1701 → Used by L2TP

UDP Port Number = 500 → Used by IKE

UDP Port Number = 4500 → Used by NAT-T

CONFIGURATION > Service > Service Group



Add Service Group Rule

Configuration

Name: L2TP_Allow

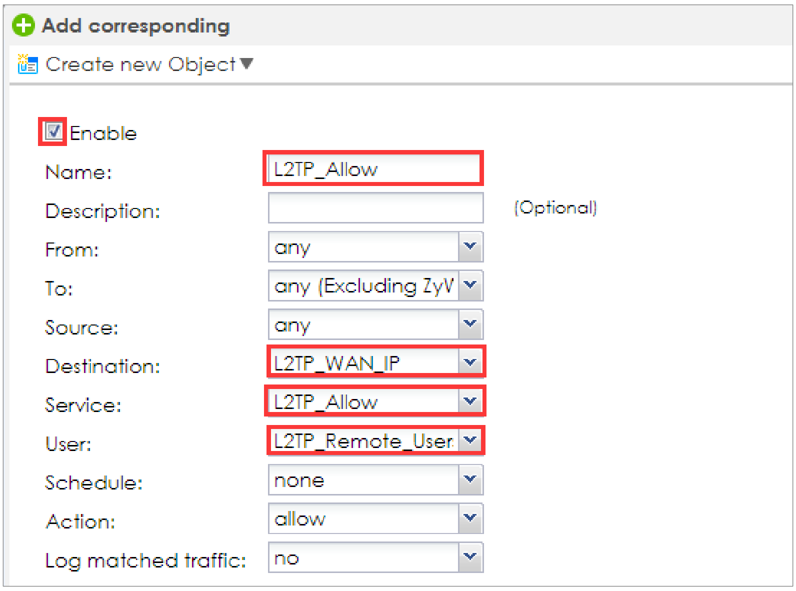
Description:

Configuration

Available	Member
=== Object ===	=== Object ===
AH	NATT
AIM	IKE
AUTH	L2TP-UDP
Any_TCP	
Any_UDP	
BGP	
BONJOUR	

Go to **CONFIGURATION > Security Policy > Policy Control**, add corresponding rule to allow L2TP services.

CONFIGURATION > Security Policy > Policy Control



☑ Enable

Name:	L2TP_Allow
Description:	(Optional)
From:	any
To:	any (Excluding ZyV
Source:	any
Destination:	L2TP_WAN_IP
Service:	L2TP_Allow
User:	L2TP_Remote_User
Schedule:	none
Action:	allow
Log matched traffic:	no

Test the L2TP over IPSec VPN Tunnel

Use a smartphone or a PC to establish a L2TP VPN connection to the ZyWALL/USG. Configure the NAT's public IP address as the L2TP server address on the client. In this example using iOS device to test the result:

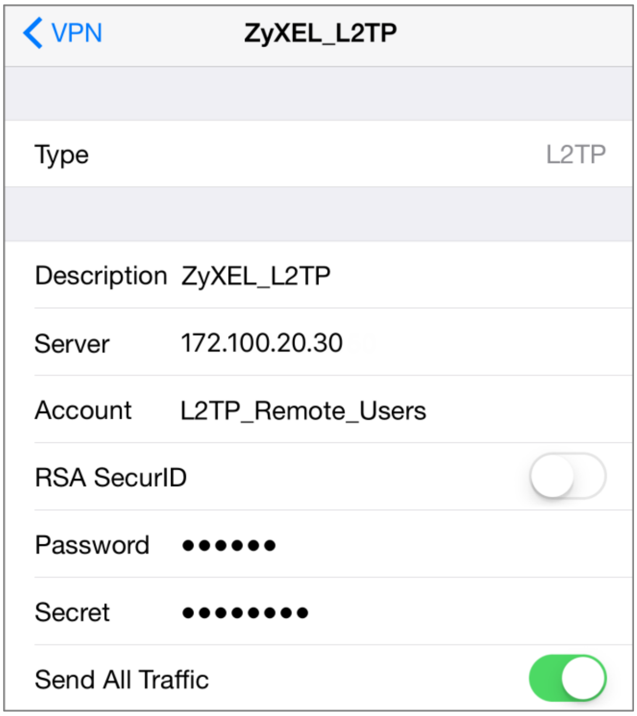
To configure L2TP VPN in an iOS 8.4 device, go to **Menu > Settings > VPN > Add VPN Configuration** and configure as follows.

Description is for you to identify the VPN configuration.

Set **Server** to the ZyWALL/USG's WAN IP address (172.100.20.30 in this example).

Enter **Account** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).

Set **Secret** to the **Pre-Shared Key** of the IPSec VPN gateway the ZyWALL/USG uses for L2TP VPN over IPSec (xyz12345 in this example).



ZyXEL_L2TP

Type L2TP

Description ZyXEL_L2TP

Server 172.100.20.30

Account L2TP_Remote_Users

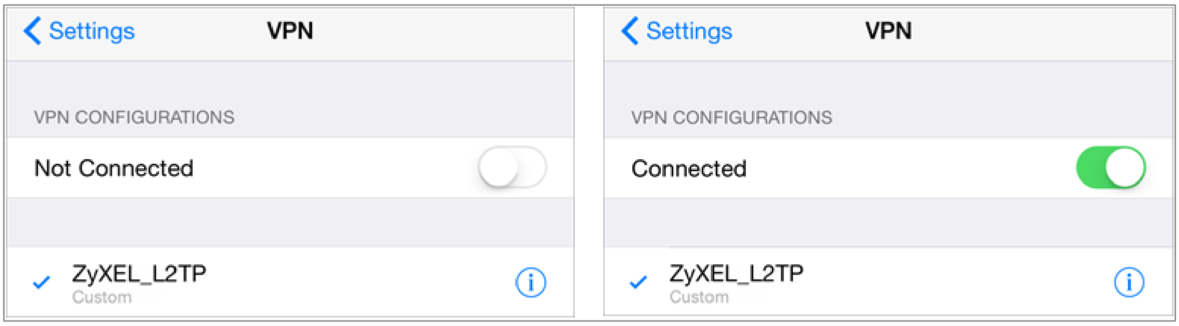
RSA SecurID ○

Password ••••••

Secret ••••••••

Send All Traffic ●

After you create a VPN configuration, slide the button right to the on position to initiate L2TP VPN session.



< Settings VPN

VPN CONFIGURATIONS

Not Connected

✓ ZyXEL_L2TP
Custom

< Settings VPN

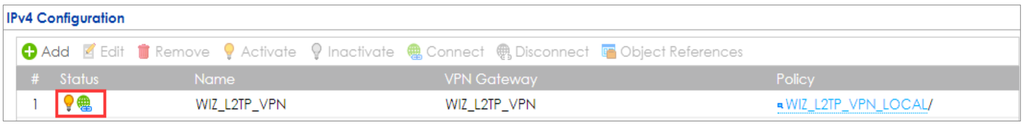
VPN CONFIGURATIONS

Connected

✓ ZyXEL_L2TP
Custom

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

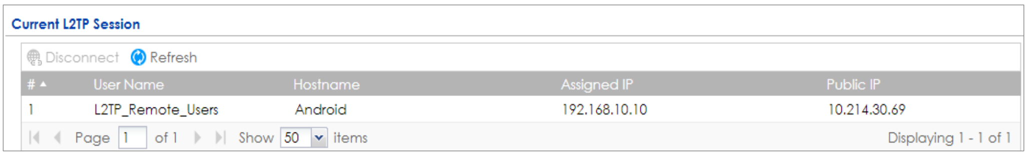


IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1		WIZ_L2TP_VPN	WIZ_L2TP_VPN	WIZ_L2TP_VPN_LOCAL/

Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users



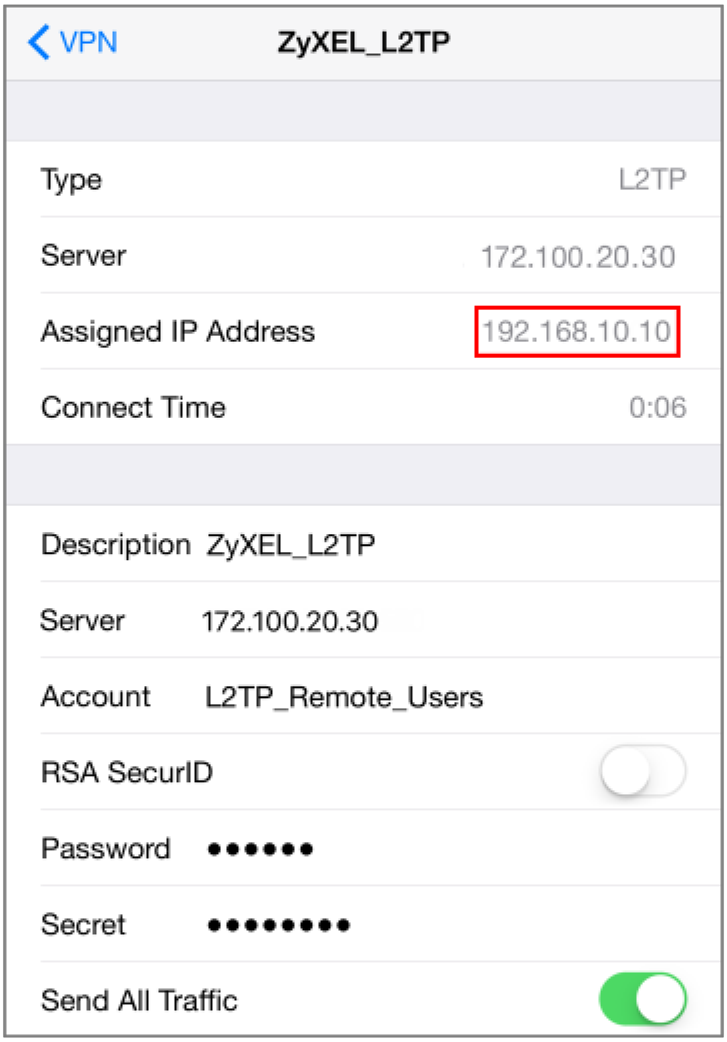
Current L2TP Session

#	User Name	Hostname	Assigned IP	Public IP
1	L2TP_Remote_Users	Android	192.168.10.10	10.214.30.69

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

Go to iOS mobile device **Menu > Settings > VPN > ZyXEL_L2TP** and verify the **Assigned IP Address** and **Connect Time**.

Menu > Settings > VPN > ZyXEL_L2TP



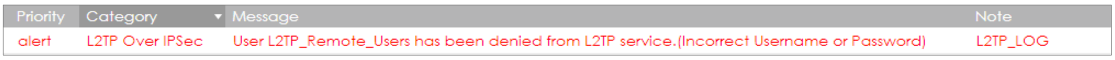
ZyXEL_L2TP

Type	L2TP
Server	172.100.20.30
Assigned IP Address	192.168.10.10
Connect Time	0:06

Description	ZyXEL_L2TP
Server	172.100.20.30
Account	L2TP_Remote_Users
RSA SecurID	○
Password	••••••
Secret	•••••••••
Send All Traffic	●

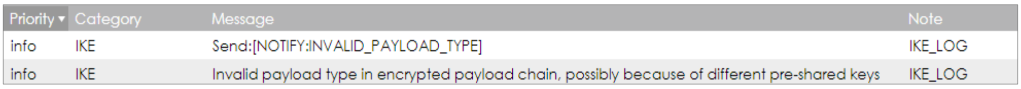
What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP **Allowed User** or **User/Group Settings**. iOS Mobile users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.



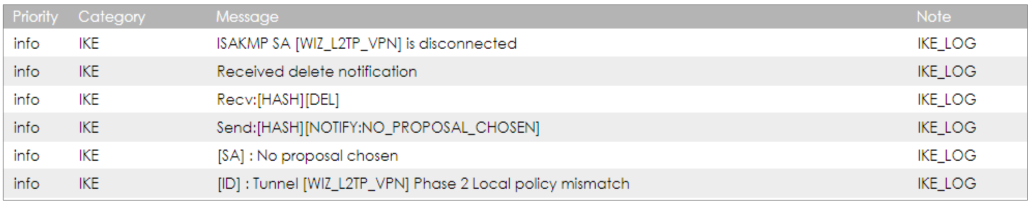
Priority	Category	Message	Note
alert	L2TP Over IPSec	User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password)	L2TP_LOG

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. iOS Mobile users must use the same **Secret** as configured in ZyWALL/USG to establish the IKE SA.



Priority ▾	Category	Message	Note
info	IKE	Send:[NOTIFY:INVALID_PAYLOAD_TYPE]	IKE_LOG
info	IKE	Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys	IKE_LOG

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.



Priority	Category	Message	Note
info	IKE	ISAKMP SA [WIZ_L2TP_VPN] is disconnected	IKE_LOG
info	IKE	Received delete notification	IKE_LOG
info	IKE	Recv:[HASH][DEL]	IKE_LOG
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch	IKE_LOG

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

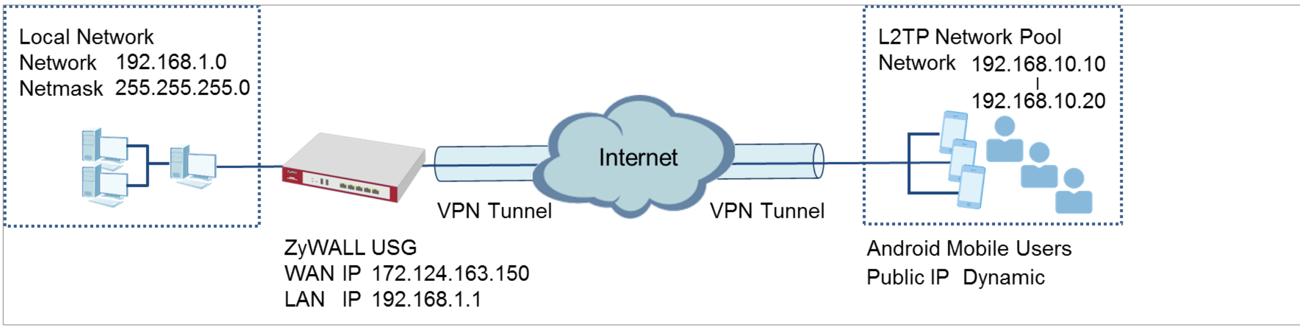
If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Verify that the **Zone** is set correctly in the **Zone** object. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Configure L2TP VPN with Android 5.0 Mobile Devices

This example shows how to use the VPN Setup Wizard to create a L2TP VPN between a ZyWALL/USG and an Android 5.0 Mobile Device. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely and allow traffic from L2TP clients to go to the Internet.



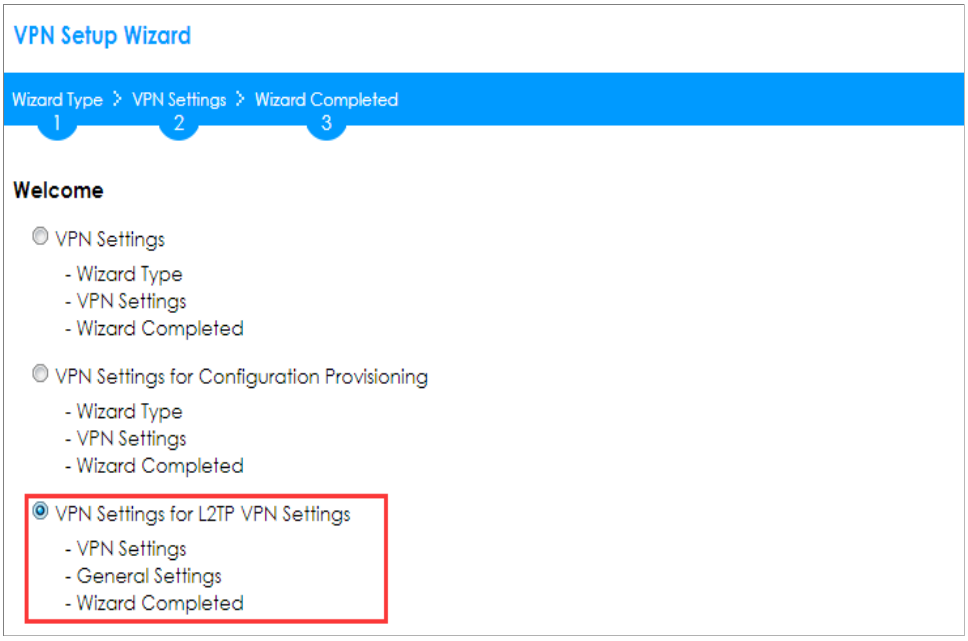
ZyWALL/USG L2TP VPN with Android Mobile Devices Example

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and Android version (Firmware Version: 5.0)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the remote Android Mobile Devices. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

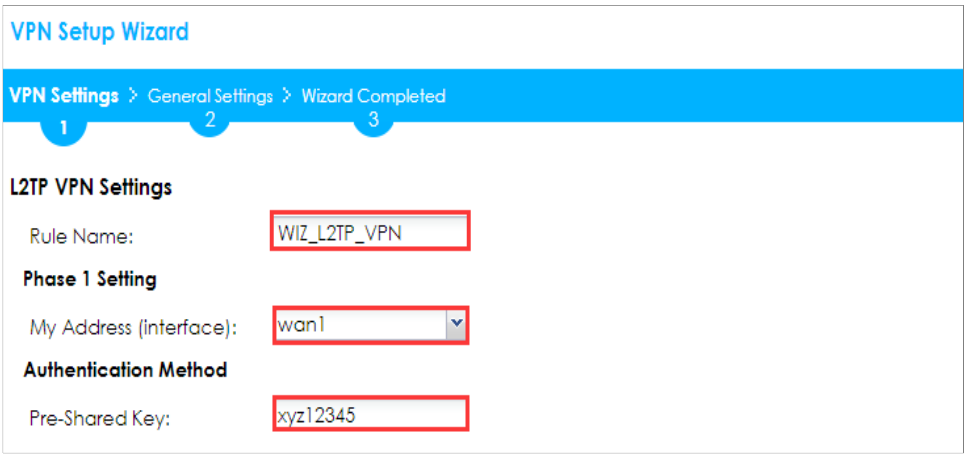
○ VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

● VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



VPN Setup Wizard

L2TP VPN Settings

Rule Name: WIZ_L2TP_VPN

Phase 1 Setting

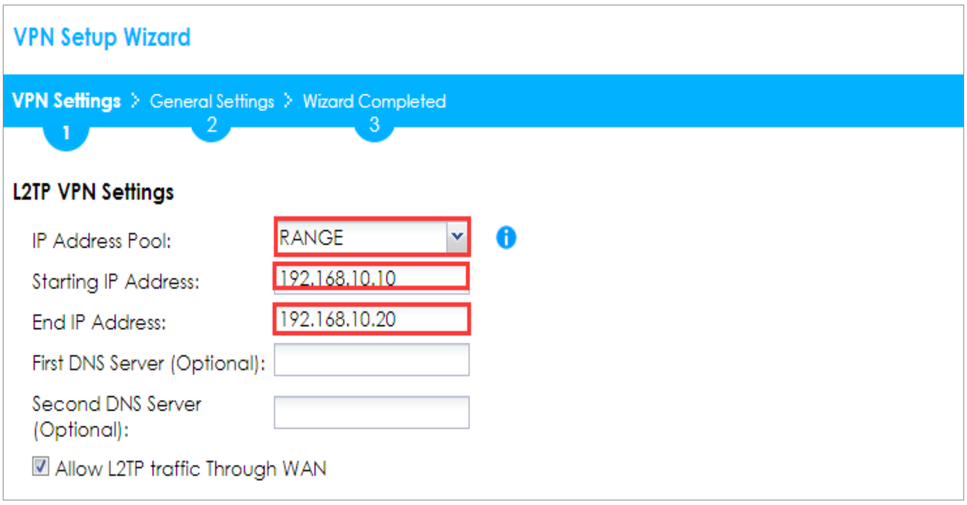
My Address (interface): wan1

Authentication Method

Pre-Shared Key: xyz12345

Assign the remote users IP addresses range from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)



VPN Setup Wizard

L2TP VPN Settings

IP Address Pool: RANGE

Starting IP Address: 192.168.10.10

End IP Address: 192.168.10.20

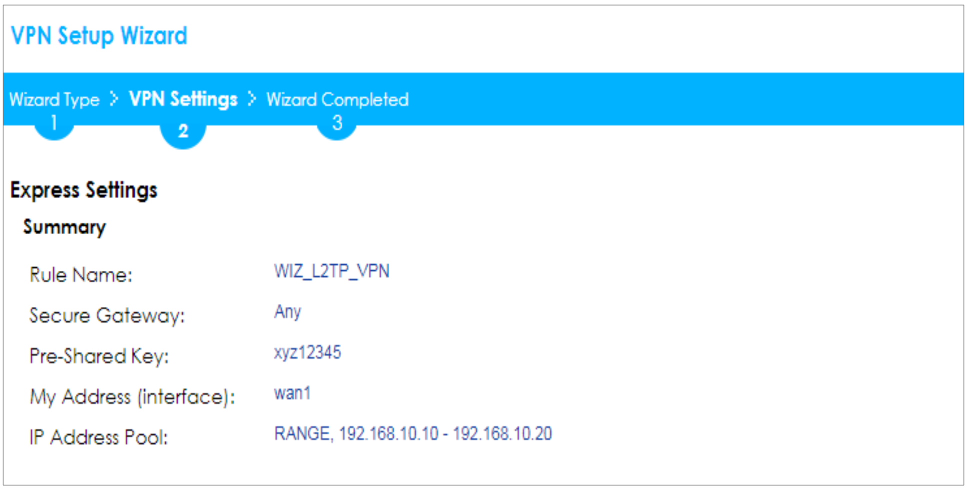
First DNS Server (Optional):

Second DNS Server (Optional):

☑ Allow L2TP traffic Through WAN

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)



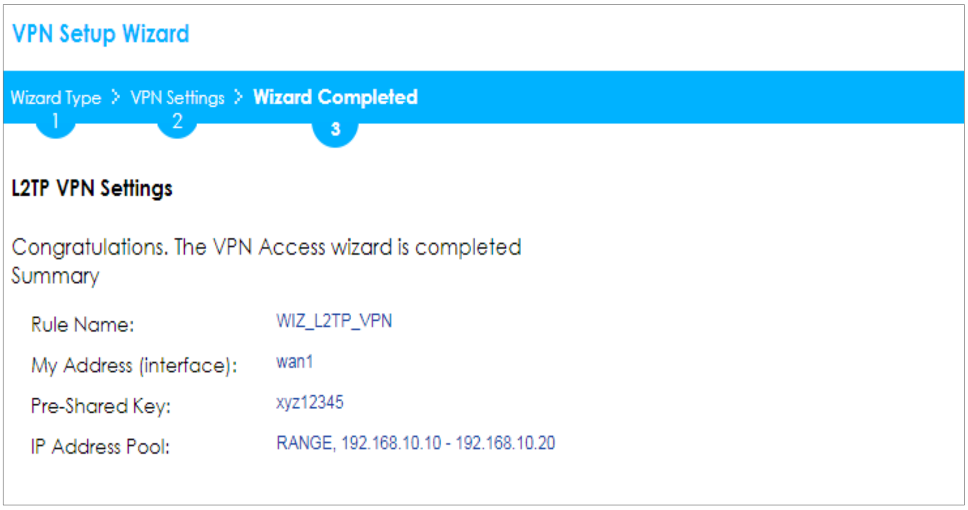
Express Settings

Summary

Rule Name:	WIZ_L2TP_VPN
Secure Gateway:	Any
Pre-Shared Key:	xyz12345
My Address (interface):	wan1
IP Address Pool:	RANGE, 192.168.10.10 - 192.168.10.20

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Wizard Completed



L2TP VPN Settings

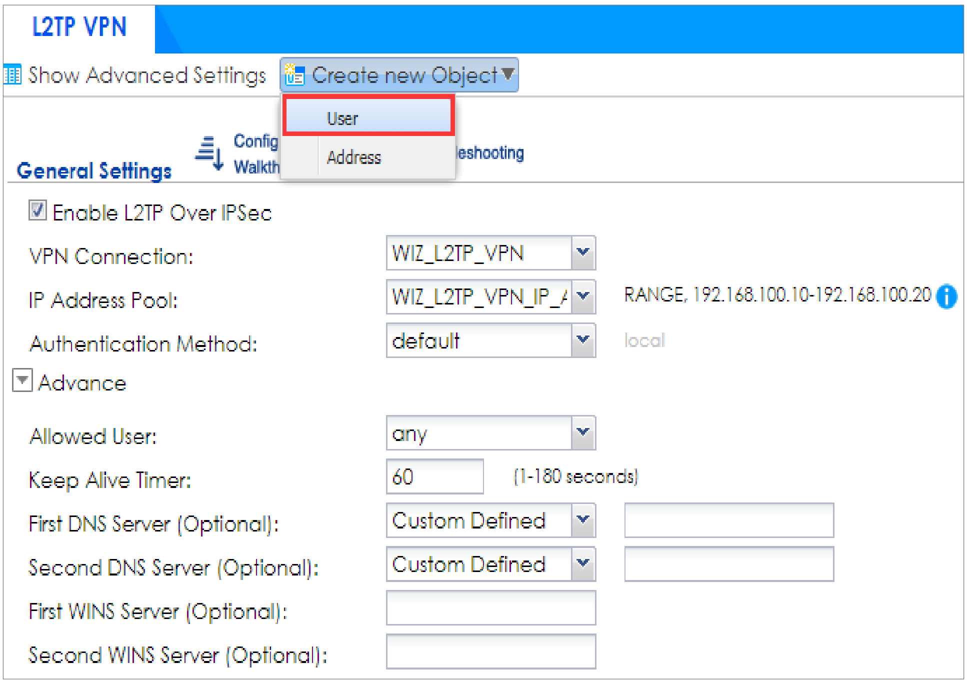
Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_L2TP_VPN
My Address (interface):	wan1
Pre-Shared Key:	xyz12345
IP Address Pool:	RANGE, 192.168.10.10 - 192.168.10.20

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User

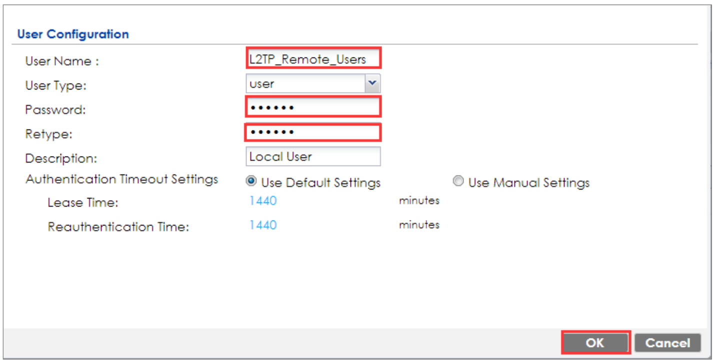


☑ Enable L2TP Over IPSec

VPN Connection:	WIZ_L2TP_VPN	
IP Address Pool:	WIZ_L2TP_VPN_IP_A	RANGE, 192.168.100.10-192.168.100.20
Authentication Method:	default	local

Advance

Allowed User:	any	
Keep Alive Timer:	60	(1-180 seconds)
First DNS Server (Optional):	Custom Defined	
Second DNS Server (Optional):	Custom Defined	
First WINS Server (Optional):		
Second WINS Server (Optional):		

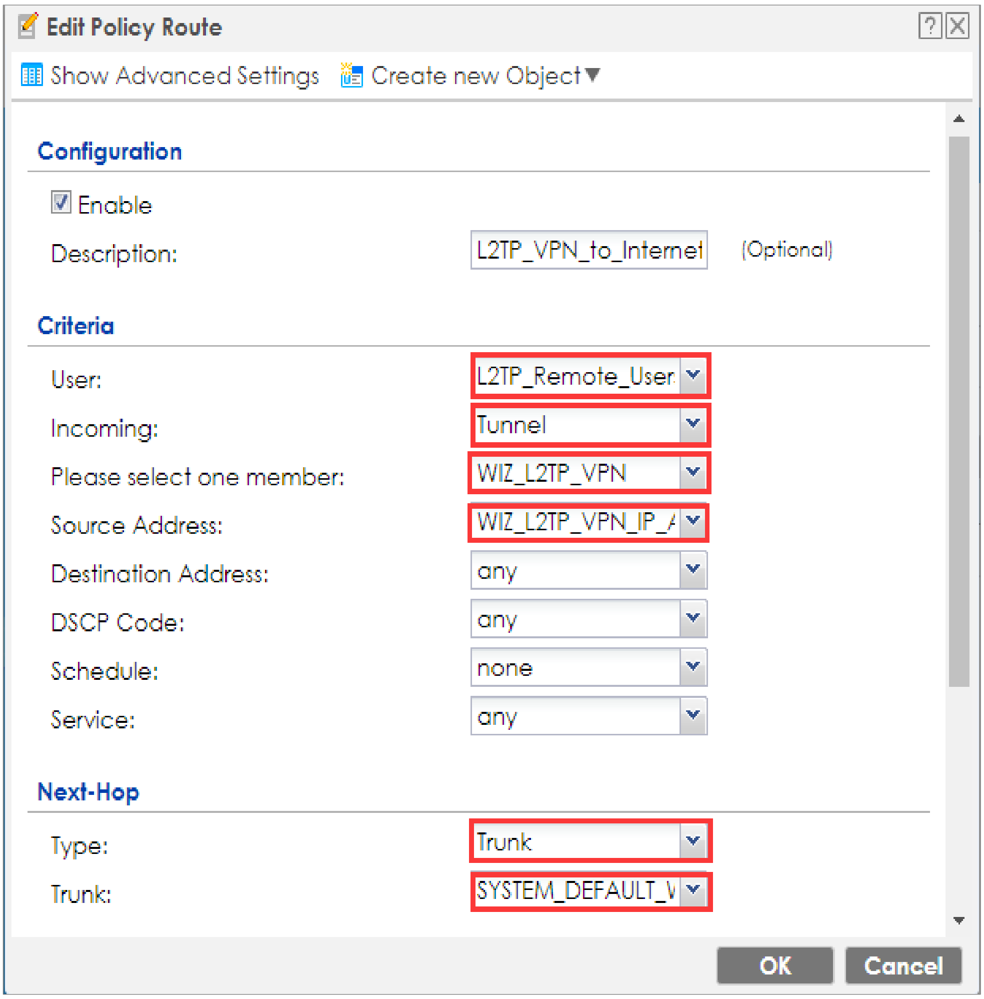


User Configuration

User Name :	L2TP_Remote_Users	
User Type:	user	
Password:	••••••	
Retype:	••••••	
Description:	Local User	
Authentication Timeout Settings	● Use Default Settings	○ Use Manual Settings
Lease Time:	1440	minutes
Reauthentication Time:	1440	minutes

If some of the traffic from the L2TP clients need to go to the Internet, create a policy route to send traffic from the L2TP tunnels out through a WAN trunk. Set **Incoming** to **Tunnel** and select your L2TP VPN connection. Set the **Source Address** to be the L2TP address pool. Set the **Next-Hop Type** to **Trunk** and select the appropriate WAN trunk.

CONFIGURATION > Network > Routing > Policy Route



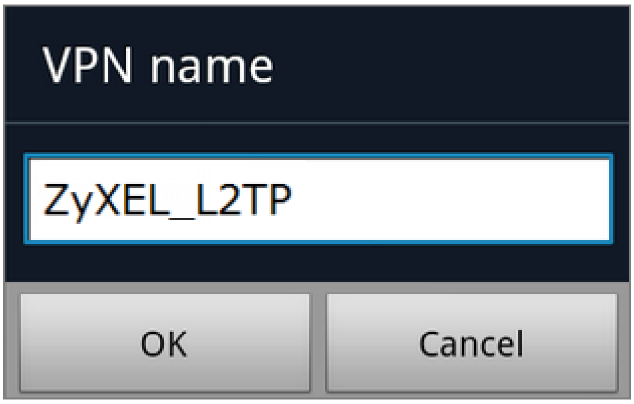
☑ Enable

Description:	L2TP_VPN_to_Internet (Optional)
User:	L2TP_Remote_User
Incoming:	Tunnel
Please select one member:	WIZ_L2TP_VPN
Source Address:	WIZ_L2TP_VPN_IP_/
Destination Address:	any
DSCP Code:	any
Schedule:	none
Service:	any
Type:	Trunk
Trunk:	SYSTEM_DEFAULT_V

Set Up the L2TP VPN Tunnel on the Android Device

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

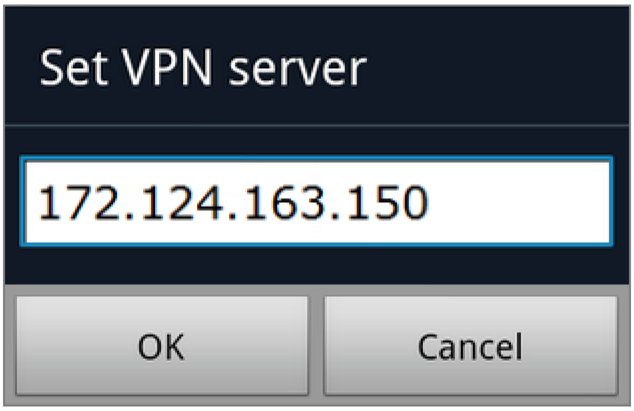
VPN name is for the user to identify the VPN configuration.



VPN name

ZyXEL_L2TP

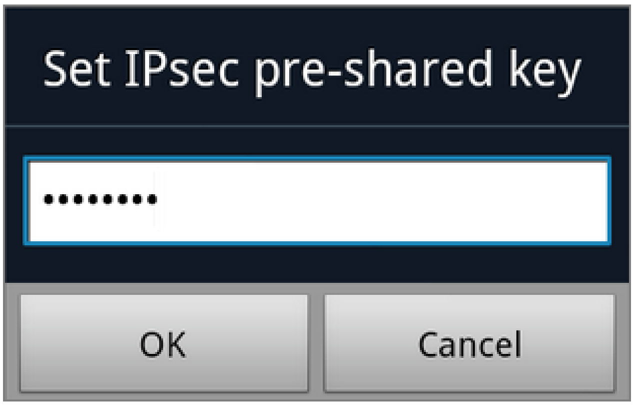
Set **VPN server** to the ZyWALL/USG’s WAN IP address.



Set VPN server

172.124.163.150

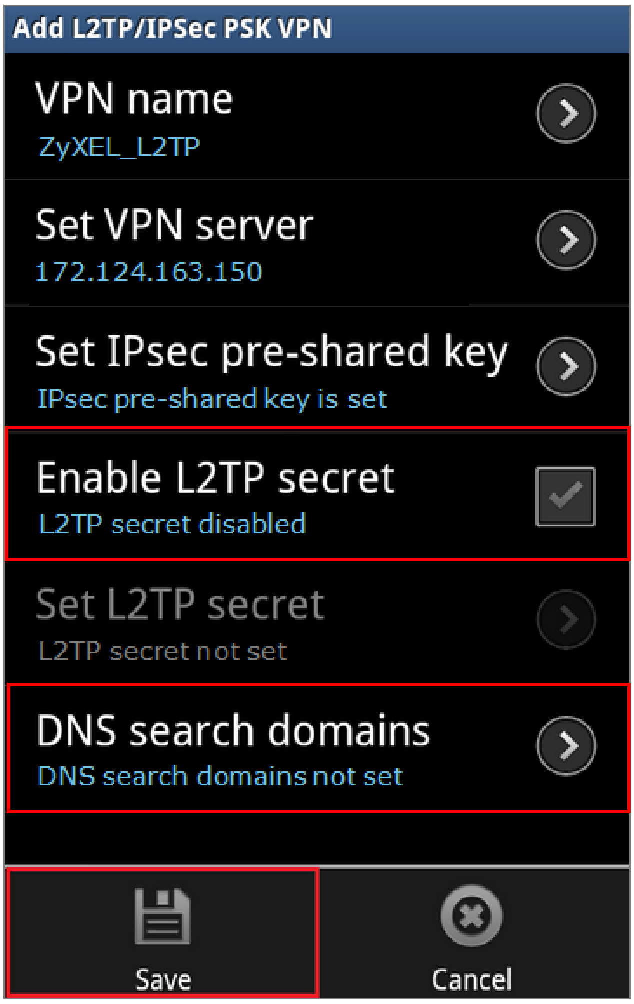
Set **IPSec pre-shared key** to the pre-shared key of the IPSec VPN gateway the ZyWALL/USG uses for L2TP VPN over IPSec (zyx12345 in this example).



Set IPsec pre-shared key

••••••••

Leave **Enable L2TP secret disabled** as default and turn on **DNS search domains** if you need to use the internal DNS servers once your connection is made, enter the DNS server address here. Click **Save**.



Add L2TP/IPSec PSK VPN

VPN name
ZyXEL_L2TP

Set VPN server
172.124.163.150

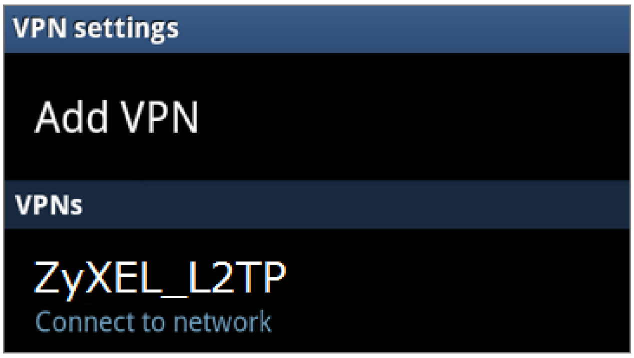
Set IPsec pre-shared key
IPsec pre-shared key is set

Enable L2TP secret ☐
L2TP secret disabled

Set L2TP secret
L2TP secret not set

DNS search domains
DNS search domains not set

Click the VPN rule **ZyXEL_L2TP** to begin the VPN connection.



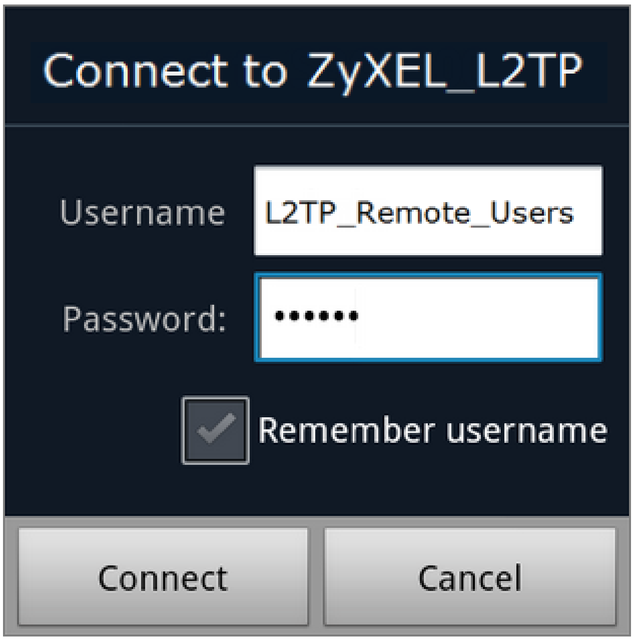
VPN settings

Add VPN

VPNs

ZyXEL_L2TP
Connect to network

When dialing the L2TP VPN, the user will have to enter Username/Password. They are the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).



Connect to ZyXEL_L2TP

Username: L2TP_Remote_Users

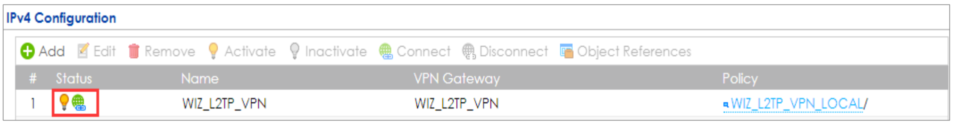
Password: ••••••

☑ Remember username

Test the L2TP over IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

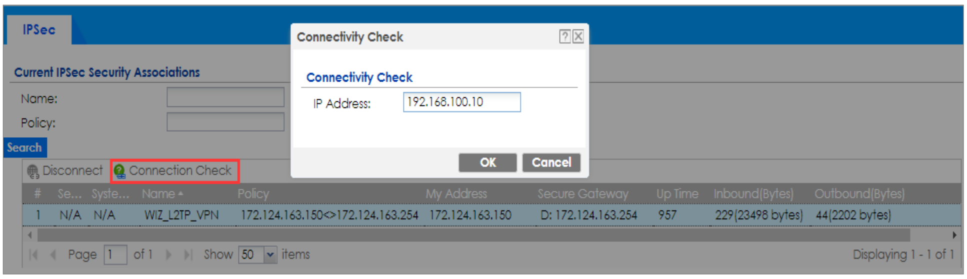


IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1	💡🌐	WIZ_L2TP_VPN	WIZ_L2TP_VPN	WIZ_L2TP_VPN_LOCAL/

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > WIZ_L2TP_VPN



Current IPSec Security Associations

Name:

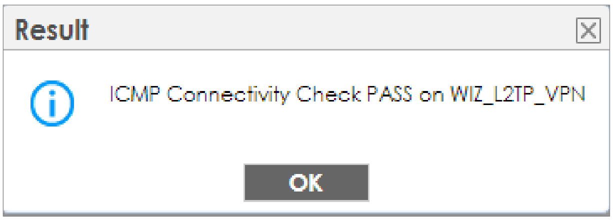
Policy:

Connectivity Check

IP Address: 192.168.100.10

#	Se...	Syste...	Name	Policy	My Address	Secure Gateway	Up Time	Inbound(Bytes)	Outbound(Bytes)
1	N/A	N/A	WIZ_L2TP_VPN	172.124.163.150<>172.124.163.254	172.124.163.150	D: 172.124.163.254	957	229(23498 bytes)	44(2202 bytes)

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

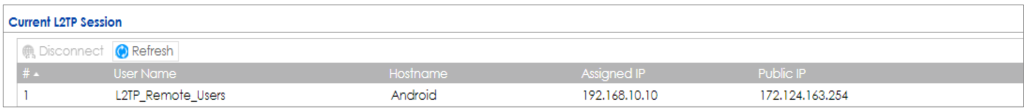


Result

ICMP Connectivity Check PASS on WIZ_L2TP_VPN

Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

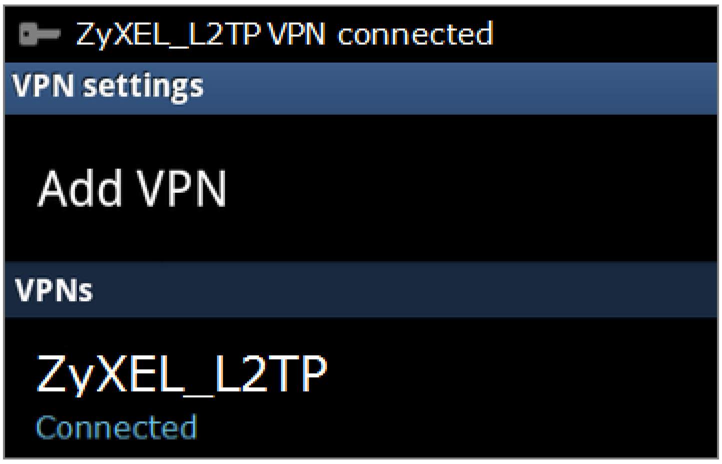


Current L2TP Session

#	User Name	Hostname	Assigned IP	Public IP
1	L2TP_Remote_Users	Android	192.168.10.10	172.124.163.254

Go to Android mobile device **Menu > Settings > Wireless & Networks > VPN** and verify the connection status.

Menu > Settings > Wireless & Networks > VPN



ZyXEL_L2TP VPN connected

VPN settings

Add VPN

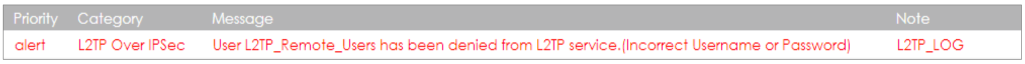
VPNs

ZyXEL_L2TP

Connected

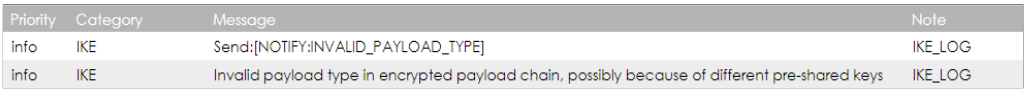
What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP **Allowed User** or **User/Group Settings**. Android Mobile users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.



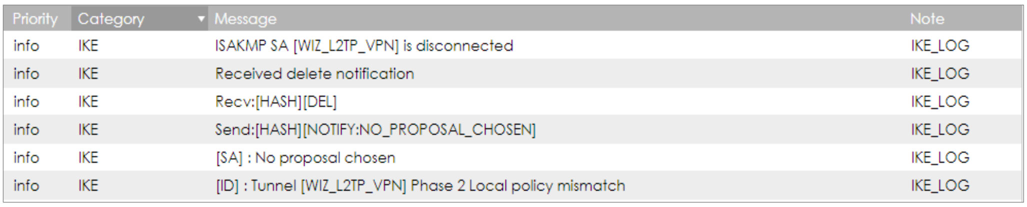
Priority	Category	Message	Note
alert	L2TP Over IPSec	User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password)	L2TP_LOG

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. Android Mobile users must use the same **Secret** as configured in ZyWALL/USG to establish the IKE SA.



Priority	Category	Message	Note
info	IKE	Send:[NOTIFY:INVALID_PAYLOAD_TYPE]	IKE_LOG
info	IKE	Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys	IKE_LOG

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.



Priority	Category	Message	Note
info	IKE	ISAKMP SA [WIZ_L2TP_VPN] is disconnected	IKE_LOG
info	IKE	Received delete notification	IKE_LOG
info	IKE	Recv:[HASH][DEL]	IKE_LOG
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch	IKE_LOG

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

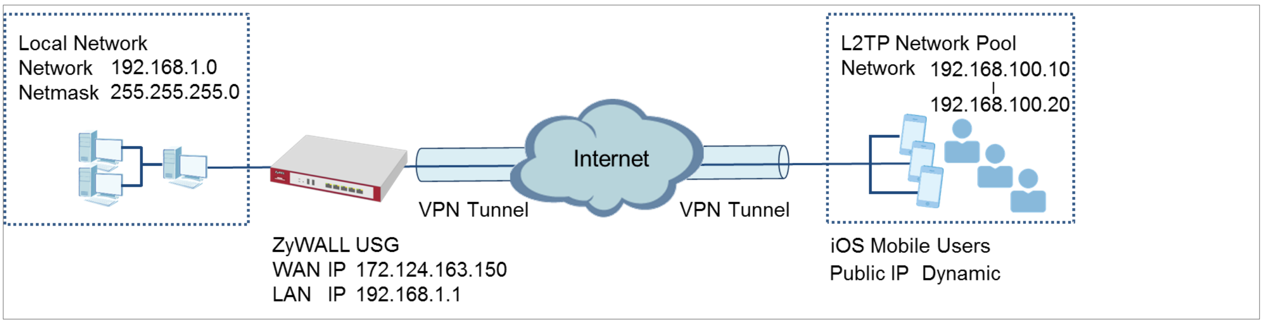
Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Verify that the **Zone** is set correctly in the **Zone** object. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Configure L2TP VPN with iOS 8.4 Mobile Devices

This example shows how to use the VPN Setup Wizard to create a L2TP VPN between a ZyWALL/USG and an iOS 8.4 Mobile Device. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely and allow traffic from L2TP clients to go to the Internet.

ZyWALL/USG L2TP VPN with iOS Mobile Devices Example

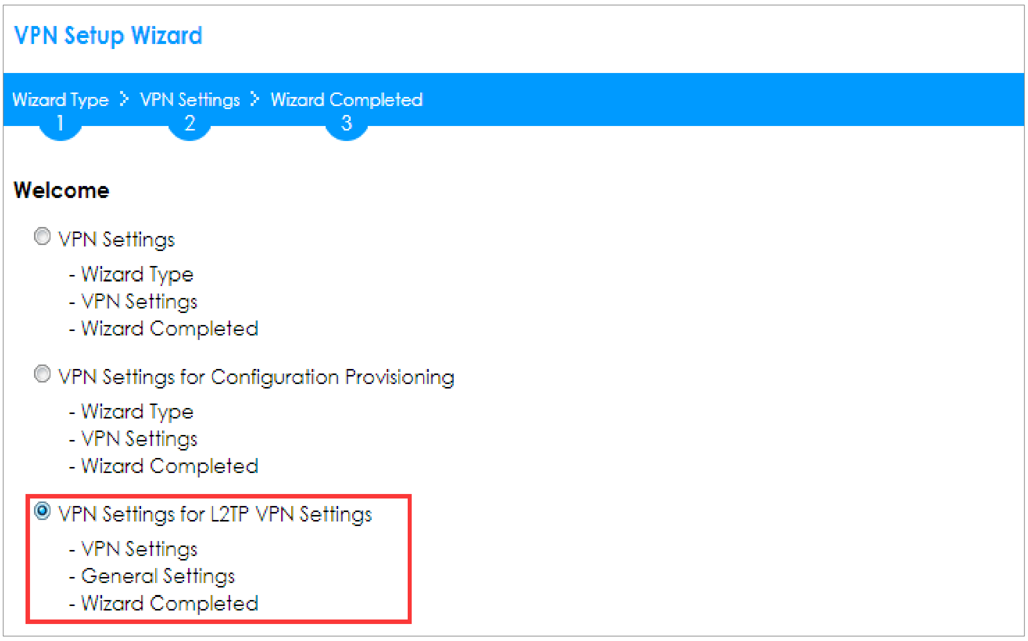


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and iOS (Firmware Version: 8.4).

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the remote iOS Mobile Devices. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

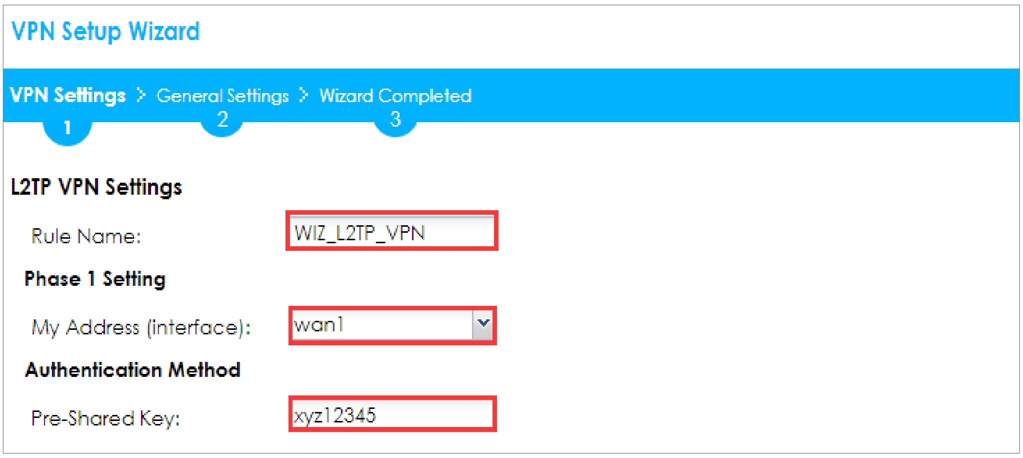
○ VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

● VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



VPN Setup Wizard

L2TP VPN Settings

Rule Name: WIZ_L2TP_VPN

Phase 1 Setting

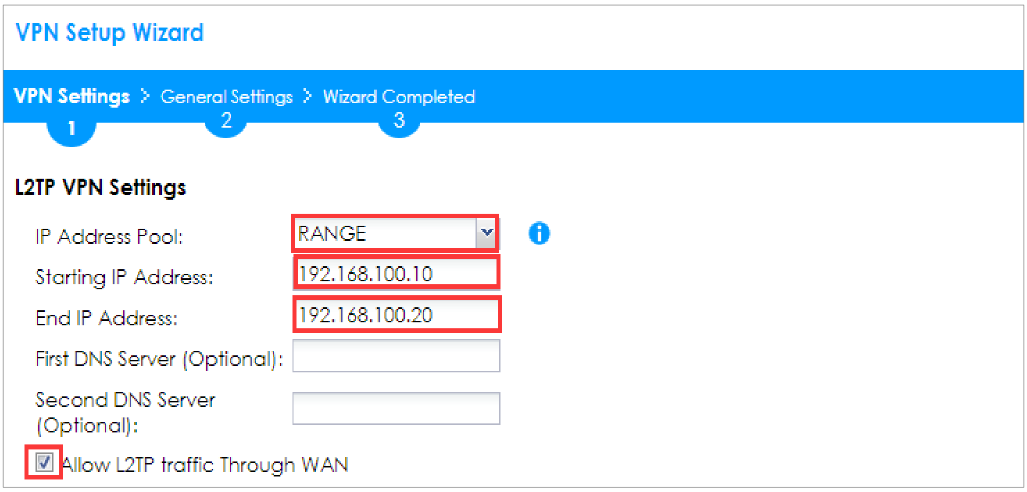
My Address (interface): wan1

Authentication Method

Pre-Shared Key: xyz12345

Assign the remote users IP addresses range from 192.168.100.10 to 192.168.100.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)



L2TP VPN Settings

IP Address Pool: RANGE

Starting IP Address: 192.168.100.10

End IP Address: 192.168.100.20

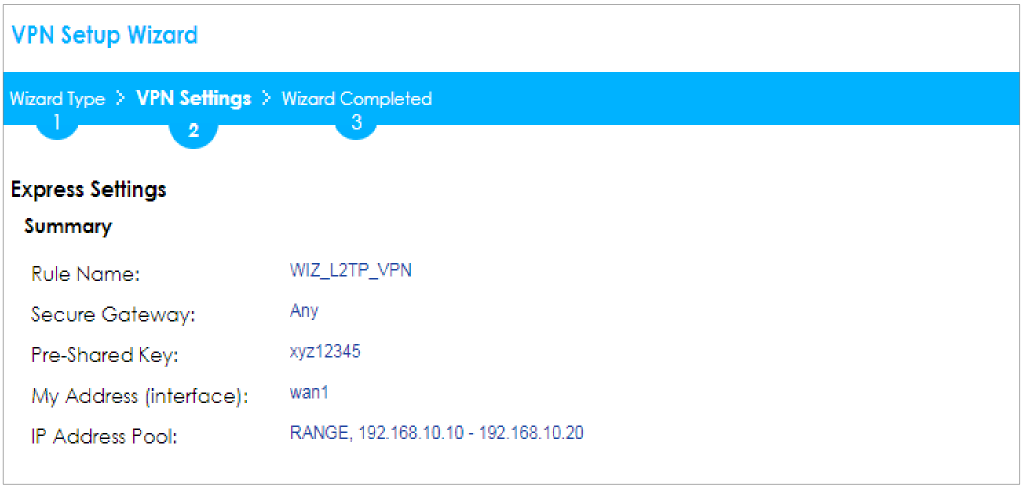
First DNS Server (Optional):

Second DNS Server (Optional):

☑ Allow L2TP traffic Through WAN

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)



Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

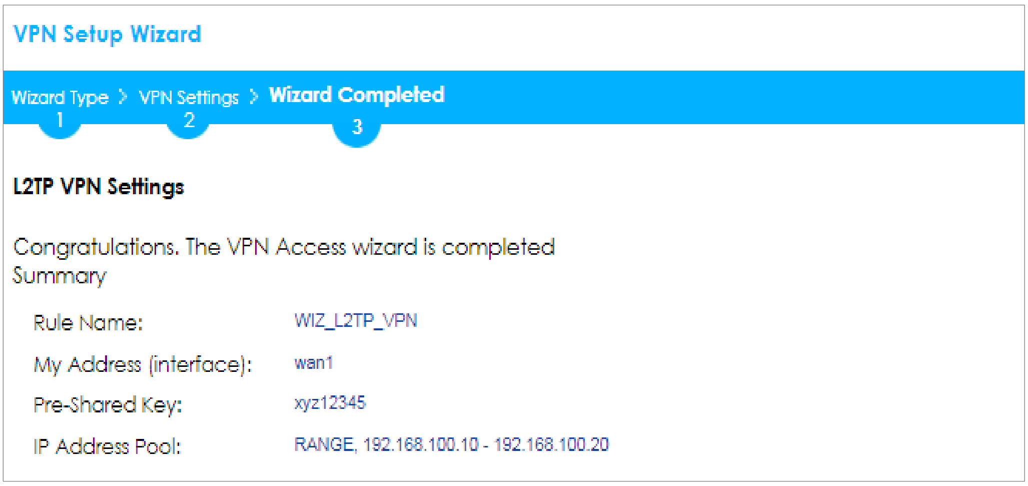
Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Summary > Wizard Completed



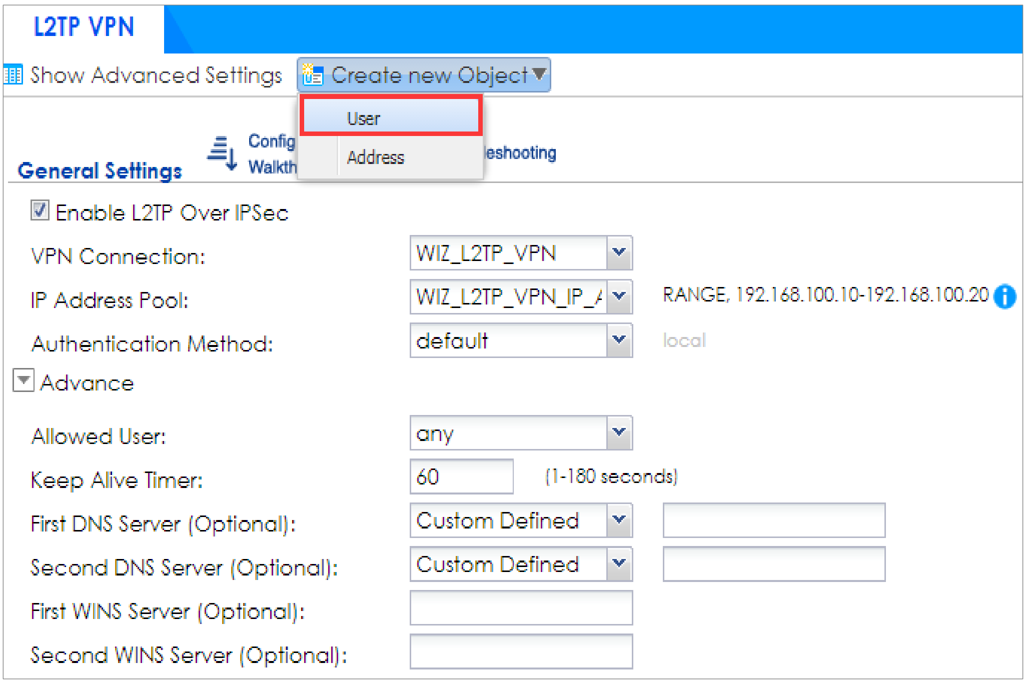
L2TP VPN Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	WIZ_L2TP_VPN
My Address (interface):	wan1
Pre-Shared Key:	xyz12345
IP Address Pool:	RANGE, 192.168.100.10 - 192.168.100.20

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User



General Settings

☑ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_A RANGE, 192.168.100.10-192.168.100.20

Authentication Method: default local

Advance

Allowed User: any

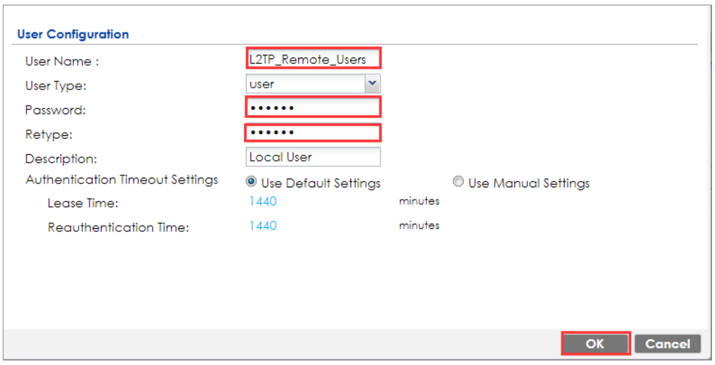
Keep Alive Timer: 60 (1-180 seconds)

First DNS Server (Optional): Custom Defined

Second DNS Server (Optional): Custom Defined

First WINS Server (Optional):

Second WINS Server (Optional):



User Configuration

User Name : L2TP_Remote_Users

User Type: user

Password: ••••••

Retype: ••••••

Description: Local User

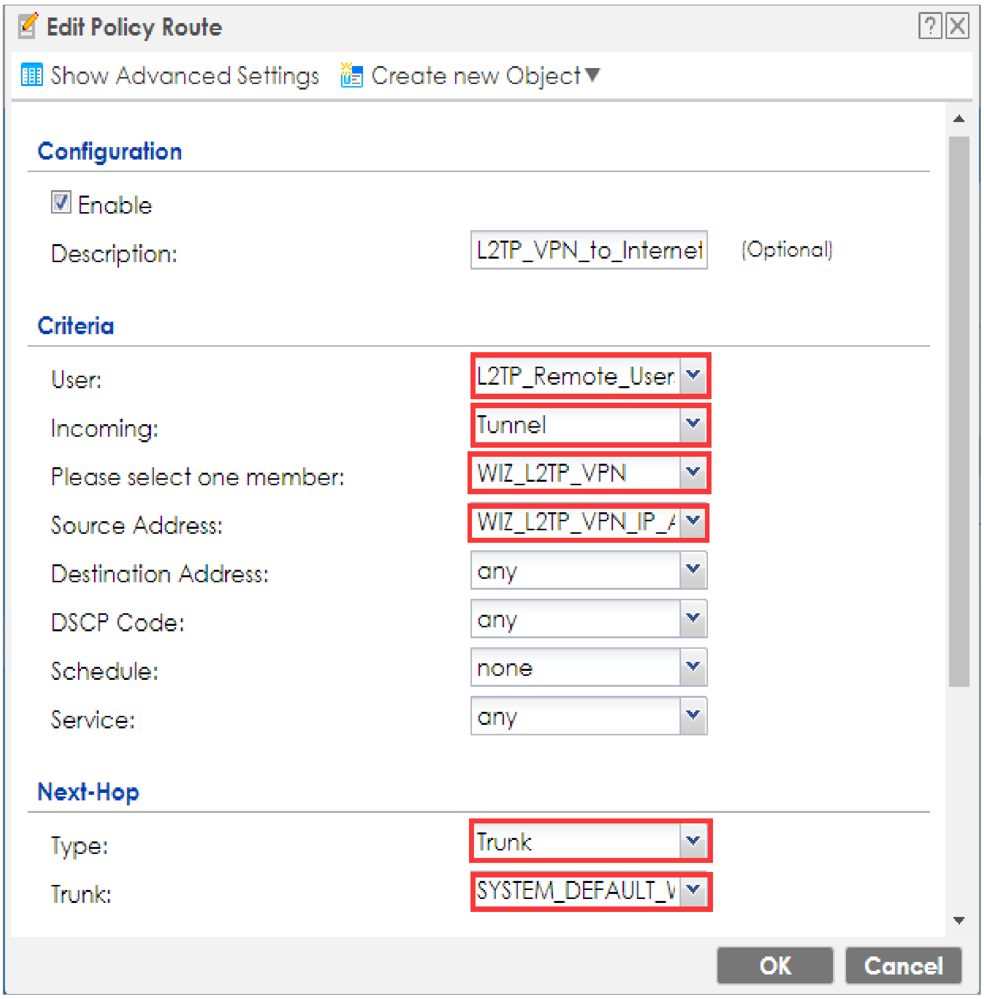
Authentication Timeout Settings ● Use Default Settings ○ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

If some of the traffic from the L2TP clients need to go to the Internet, create a policy route to send traffic from the L2TP tunnels out through a WAN trunk. Set **Incoming** to **Tunnel** and select your L2TP VPN connection. Set the **Source Address** to be the L2TP address pool. Set the **Next-Hop Type** to **Trunk** and select the appropriate WAN trunk.

CONFIGURATION > Network > Routing > Policy Route



Configuration

☑ Enable

Description: L2TP_VPN_to_Internet (Optional)

Criteria

User: L2TP_Remote_User

Incoming: Tunnel

Please select one member: WIZ_L2TP_VPN

Source Address: WIZ_L2TP_VPN_IP_A

Destination Address: any

DSCP Code: any

Schedule: none

Service: any

Next-Hop

Type: Trunk

Trunk: SYSTEM_DEFAULT_W

Set Up the L2TP VPN Tunnel on the iOS Device

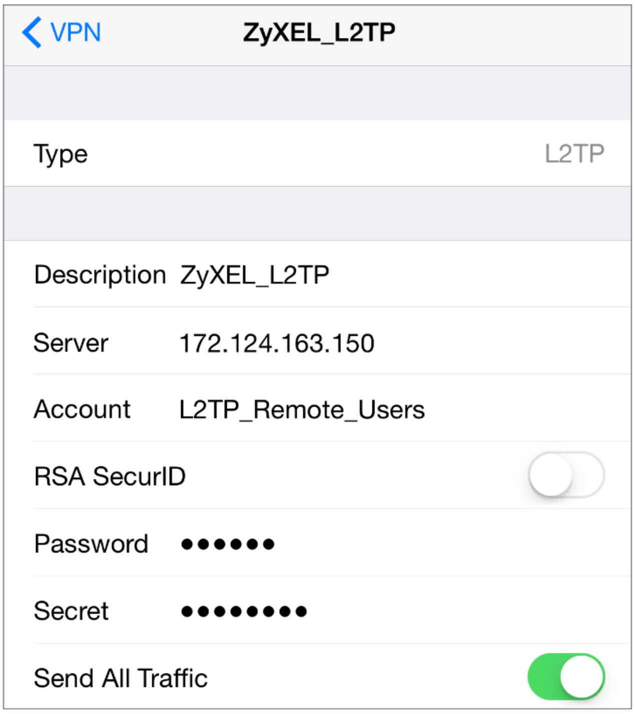
To configure L2TP VPN in an iOS 8.4 device, go to **Menu > Settings > VPN > Add VPN Configuration** and configure as follows.

Description is for you to identify the VPN configuration.

Set **Server** to the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).

Enter **Account** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).

Set **Secret** to the **Pre-Shared Key** of the IPSec VPN gateway the ZyWALL/USG uses for L2TP VPN over IPSec (zyx12345 in this example).



Type L2TP

Description ZyXEL_L2TP

Server 172.124.163.150

Account L2TP_Remote_Users

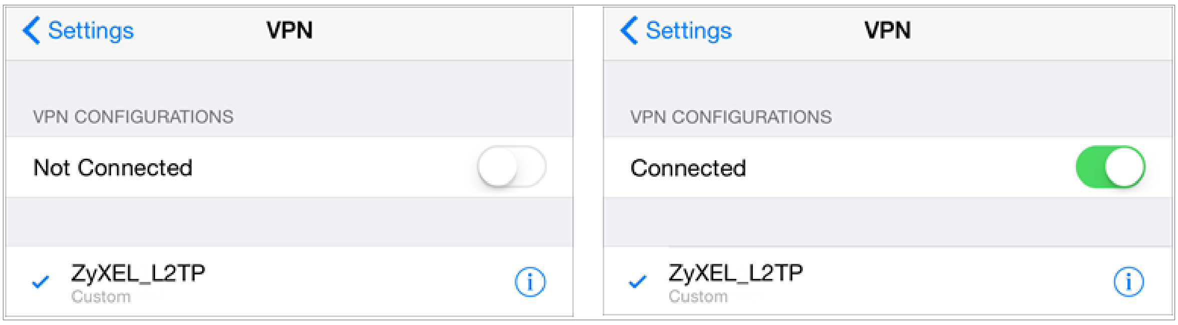
RSA SecurID

Password ••••••

Secret ••••••••

Send All Traffic

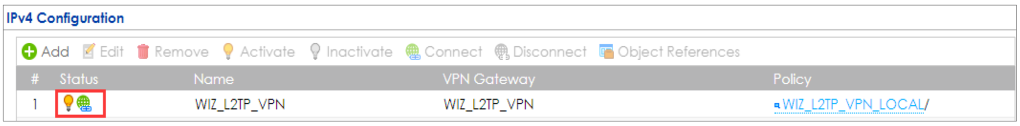
After you create a VPN configuration, slide the button right to the on position to initiate L2TP VPN session.



Test the L2TP over IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

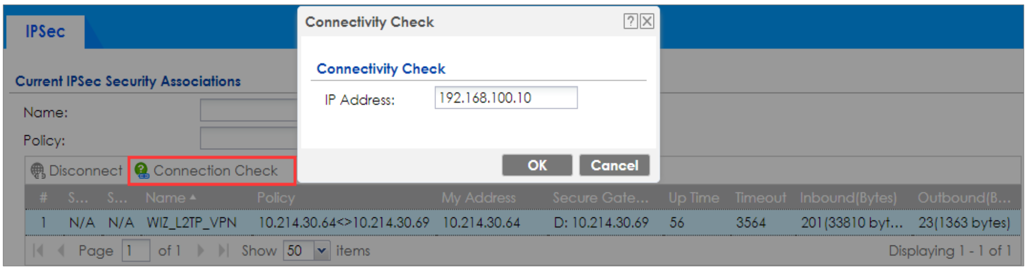


IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1	💡●	WIZ_L2TP_VPN	WIZ_L2TP_VPN	WIZ_L2TP_VPN_LOCAL/

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN

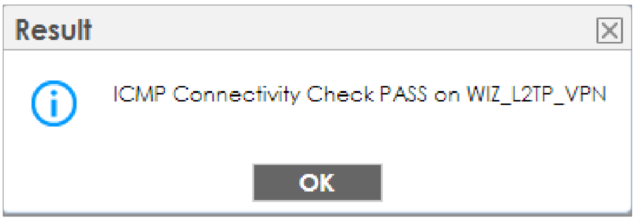


Connectivity Check

IP Address: 192.168.100.10

#	S...	S...	Name ▲	Policy	My Address	Secure Gate...	Up Time	Timeout	Inbound(Bytes)	Outbound(B...
1	N/A	N/A	WIZ_L2TP_VPN	10.214.30.64<>10.214.30.69	10.214.30.64	D: 10.214.30.69	56	3564	201(33810 byt...	23(1363 bytes)

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

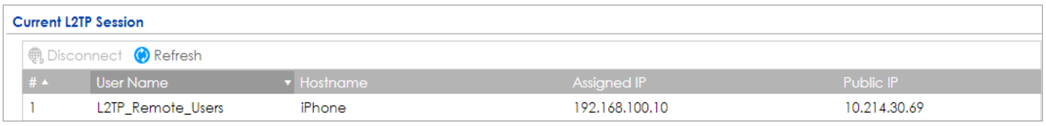


Result

ICMP Connectivity Check PASS on WIZ_L2TP_VPN

Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

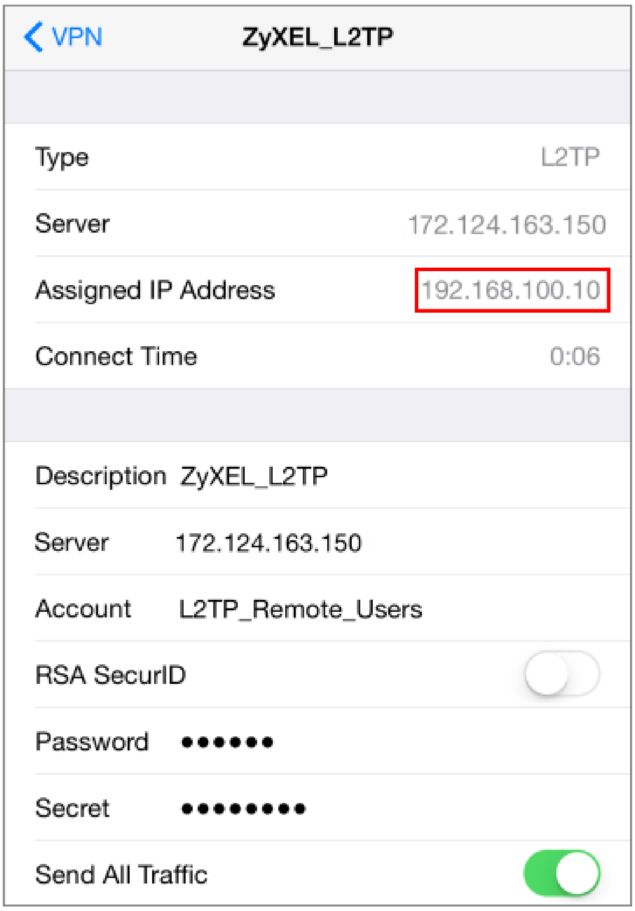


Current L2TP Session

#	User Name	Hostname	Assigned IP	Public IP
1	L2TP_Remote_Users	iPhone	192.168.100.10	10.214.30.69

Go to iOS mobile device **Menu > Settings > VPN > ZyXEL_L2TP** and verify the **Assigned IP Address** and **Connect Time**.

Menu > Settings > VPN > ZyXEL_L2TP

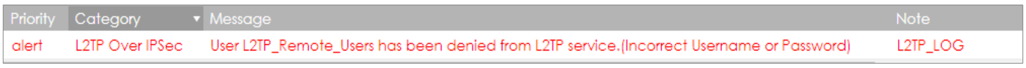


Type	L2TP
Server	172.124.163.150
Assigned IP Address	192.168.100.10
Connect Time	0:06

Description	ZyXEL_L2TP
Server	172.124.163.150
Account	L2TP_Remote_Users
RSA SecurID	○
Password	••••••
Secret	•••••••••
Send All Traffic	●

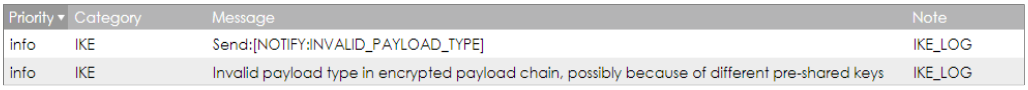
What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP **Allowed User** or **User/Group Settings**. iOS Mobile users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.



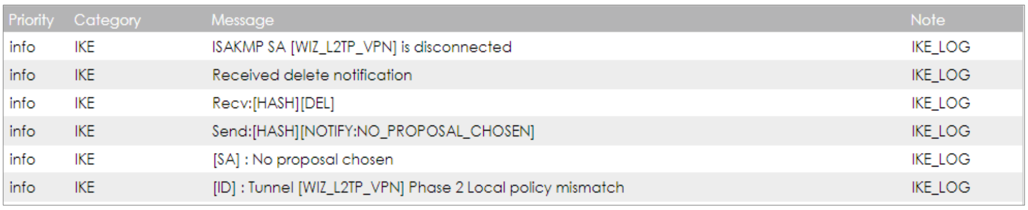
Priority	Category	Message	Note
alert	L2TP Over IPSec	User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password)	L2TP_LOG

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. iOS Mobile users must use the same **Secret** as configured in ZyWALL/USG to establish the IKE SA.



Priority ▾	Category	Message	Note
info	IKE	Send:[NOTIFY:INVALID_PAYLOAD_TYPE]	IKE_LOG
info	IKE	Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys	IKE_LOG

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.



Priority	Category	Message	Note
info	IKE	ISAKMP SA [WIZ_L2TP_VPN] is disconnected	IKE_LOG
info	IKE	Received delete notification	IKE_LOG
info	IKE	Recv:[HASH][DEL]	IKE_LOG
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch	IKE_LOG

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

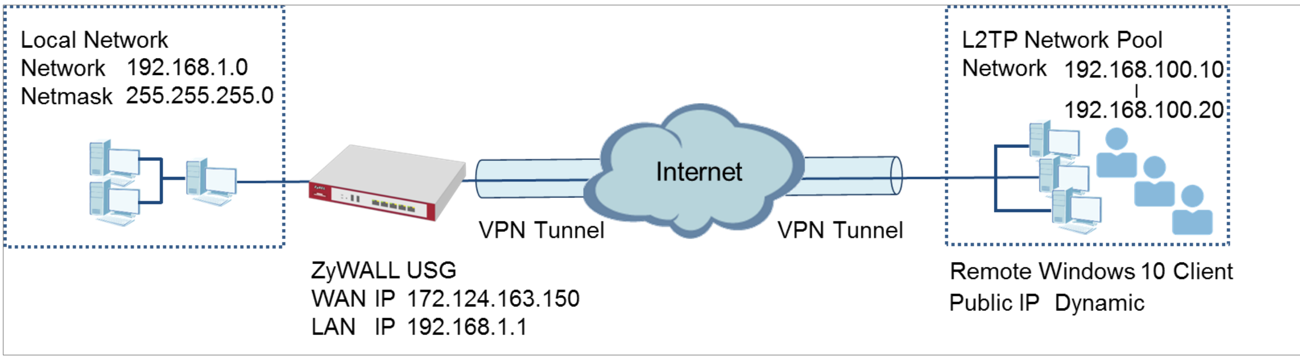
Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Verify that the **Zone** is set correctly in the **Zone** object. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Import ZyWALL/USG Certificate for L2TP over IPsec in Windows 10

This is an example of using the L2TP VPN and VPN client software included in Windows 10 operating systems. When the VPN tunnel is configured, users can securely access the network behind the ZyWALL/USG and allow traffic from L2TP clients to go to the Internet from a Windows 10 computer.

ZyWALL/USG L2TP VPN with Remote Windows 10 Client Example

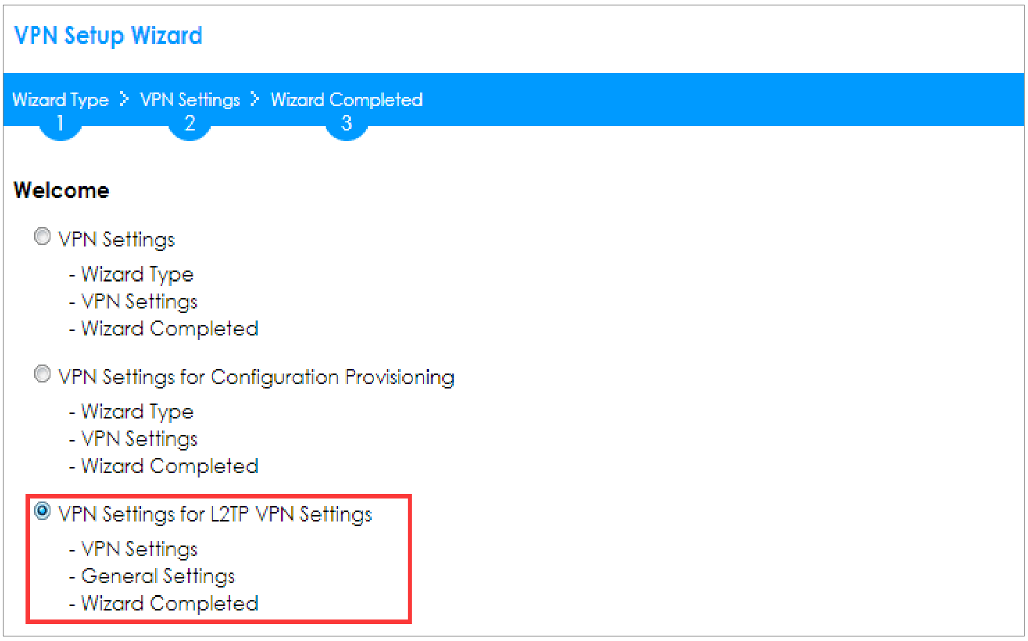


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and Windows 10 Pro (Version: 10.0.10240)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the Window 10 clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

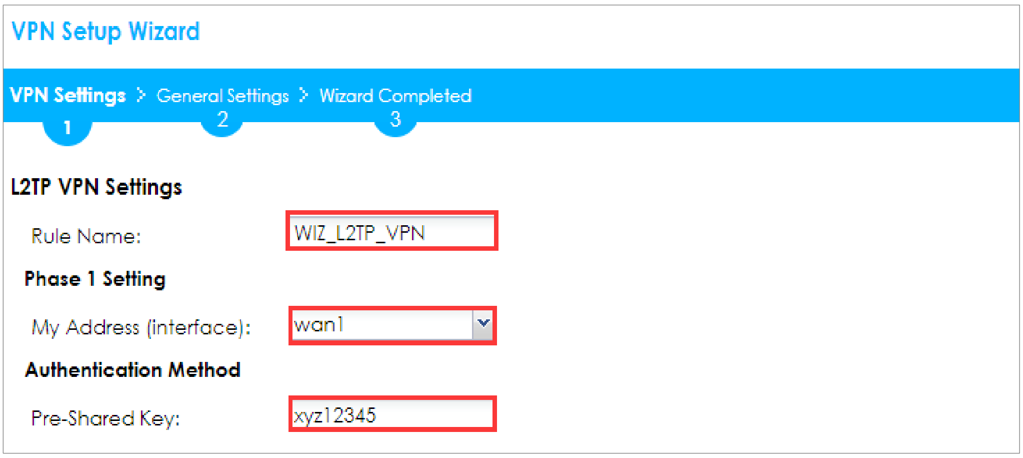
○ VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

● VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



VPN Setup Wizard

L2TP VPN Settings

Rule Name: WIZ_L2TP_VPN

Phase 1 Setting

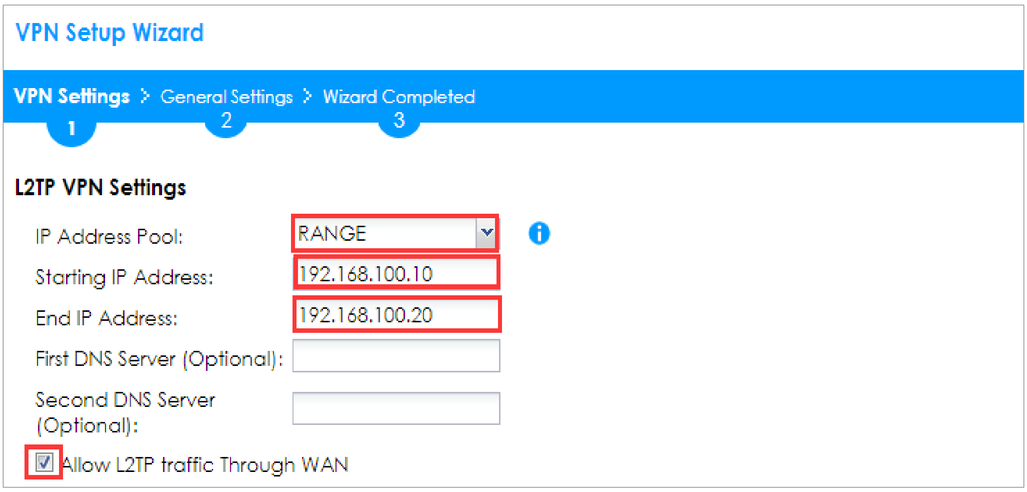
My Address (interface): wan1

Authentication Method

Pre-Shared Key: xyz12345

Assign the L2TP users' IP address range from 192.168.100.10 to 192.168.100.20 for use in the L2TP VPN tunnel and select **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)



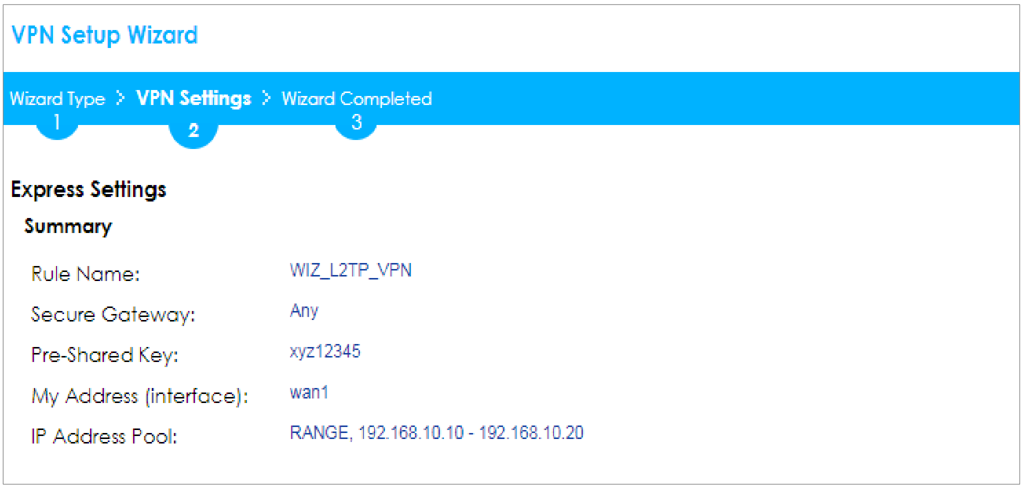
L2TP VPN Settings

IP Address Pool:	RANGE
Starting IP Address:	192.168.100.10
End IP Address:	192.168.100.20
First DNS Server (Optional):	
Second DNS Server (Optional):	

☑ Allow L2TP traffic Through WAN

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)



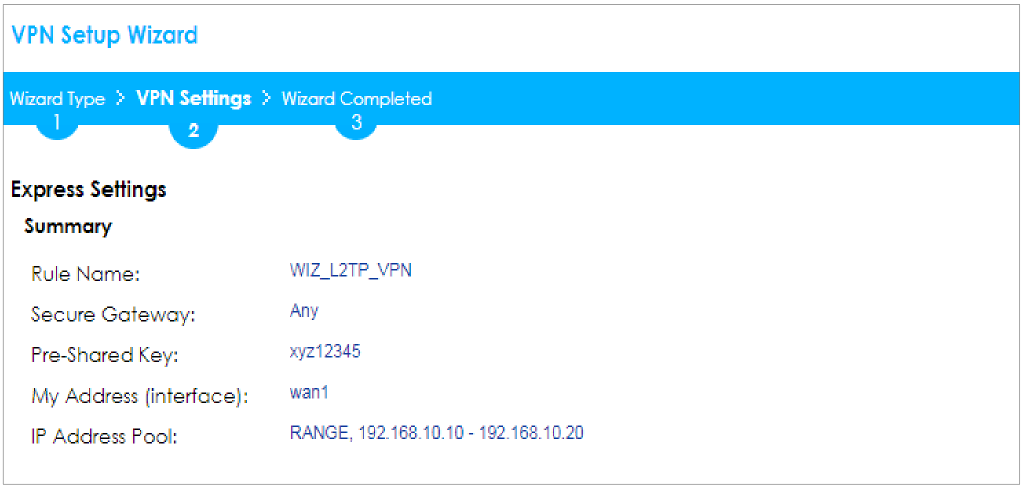
Express Settings

Summary

Rule Name:	WIZ_L2TP_VPN
Secure Gateway:	Any
Pre-Shared Key:	xyz12345
My Address (interface):	wan1
IP Address Pool:	RANGE, 192.168.10.10 - 192.168.10.20

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Wizard Completed



VPN Setup Wizard

Wizard Type 1 > **VPN Settings** 2 > Wizard Completed 3

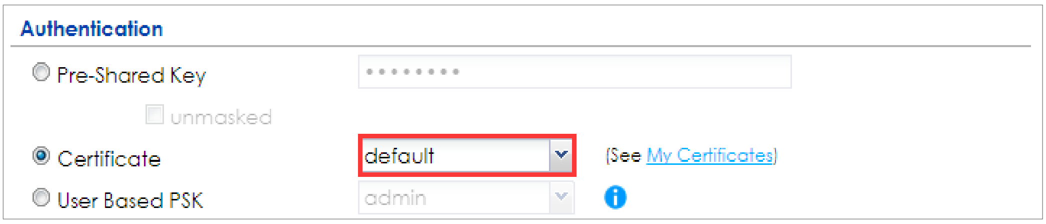
Express Settings

Summary

Rule Name:	WIZ_L2TP_VPN
Secure Gateway:	Any
Pre-Shared Key:	xyz12345
My Address (interface):	wan1
IP Address Pool:	RANGE, 192.168.10.10 - 192.168.10.20

Go to **CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN,** change **Authentication** method to be **Certificate** and select the certificate which ZyWALL/USG uses to identify itself to the Window 10 computer.

CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN > Authentication > Certificate



Authentication

○ Pre-Shared Key ••••••••

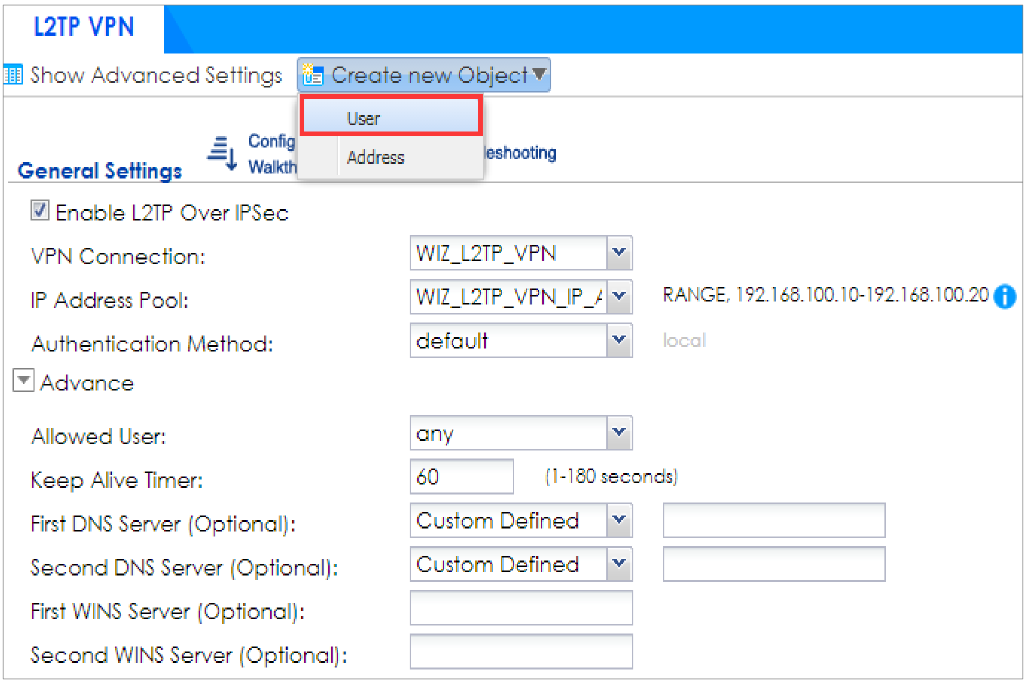
□ unmasked

● Certificate default (See My Certificates)

○ User Based PSK admin

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User



☑ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_A RANGE, 192.168.100.10-192.168.100.20

Authentication Method: default local

Advance

Allowed User: any

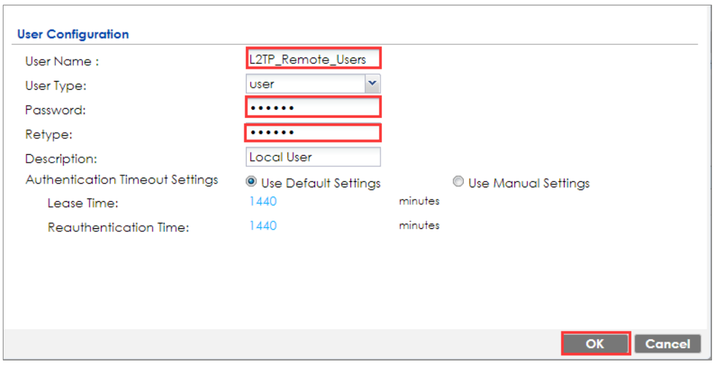
Keep Alive Timer: 60 (1-180 seconds)

First DNS Server (Optional): Custom Defined

Second DNS Server (Optional): Custom Defined

First WINS Server (Optional):

Second WINS Server (Optional):



User Configuration

User Name : L2TP_Remote_Users

User Type: user

Password: ••••••

Retype: ••••••

Description: Local User

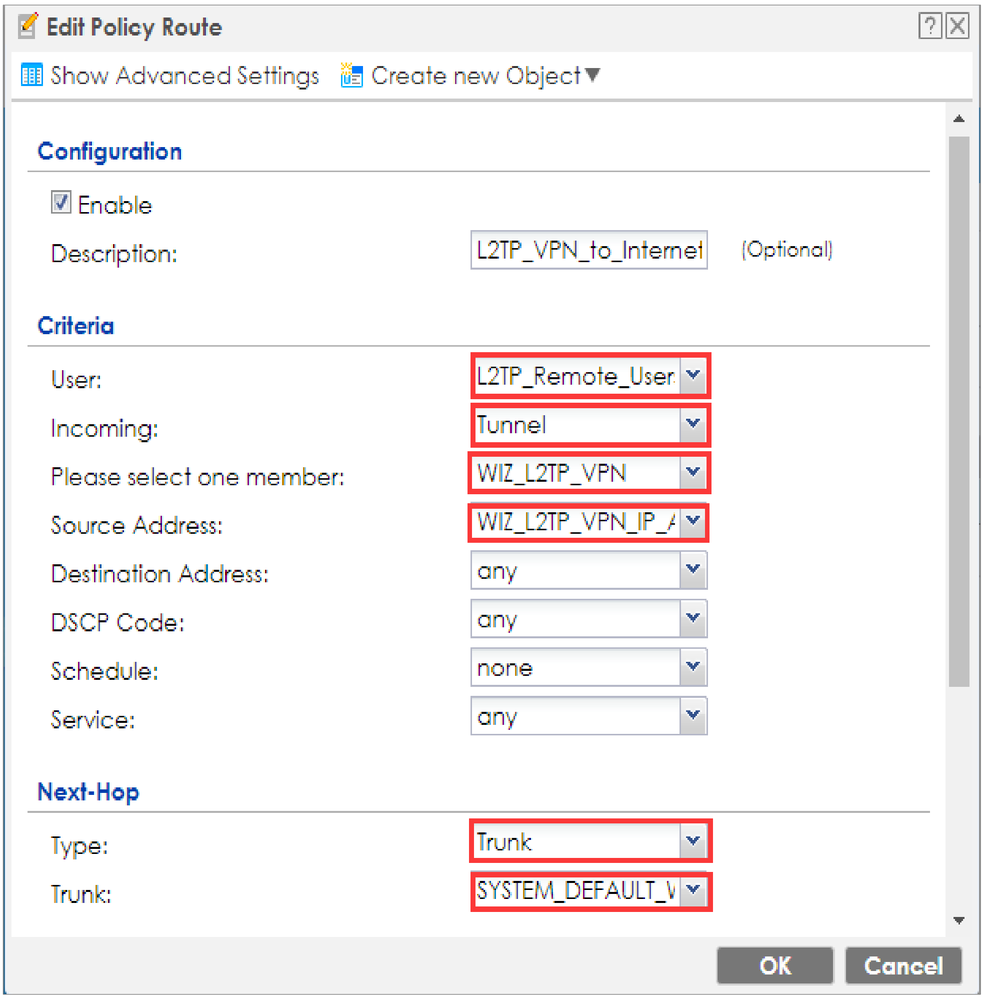
Authentication Timeout Settings ● Use Default Settings ○ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

If some of the traffic from the L2TP clients need to go to the Internet, create a policy route to send traffic from the L2TP tunnels out through a WAN trunk. Set **Incoming** to **Tunnel** and select your L2TP VPN connection. Set the **Source Address** to be the L2TP address pool. Set the **Next-Hop Type** to **Trunk** and select the appropriate WAN trunk.

CONFIGURATION > Network > Routing > Policy Route



Configuration

☑ Enable

Description:	L2TP_VPN_to_Internet	(Optional)

Criteria

User:	L2TP_Remote_User
Incoming:	Tunnel
Please select one member:	WIZ_L2TP_VPN
Source Address:	WIZ_L2TP_VPN_IP_A
Destination Address:	any
DSCP Code:	any
Schedule:	none
Service:	any

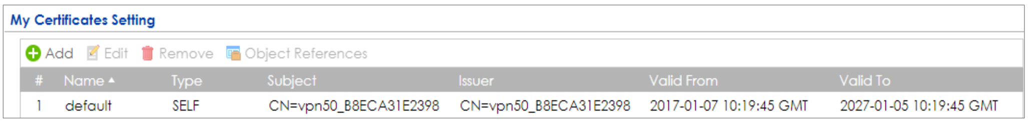
Next-Hop

Type:	Trunk
Trunk:	SYSTEM_DEFAULT_W

Export a Certificate from ZyWALL/USG and Import it to Windows 10 Operating System

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate**, select the certificate (**default** in this example) and click **Edit**.

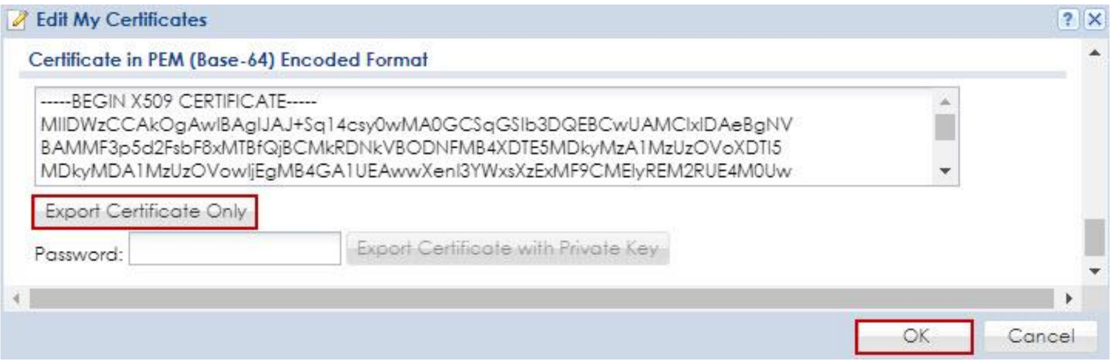
CONFIGURATION > Object > Certificate > default



#	Name ▲	Type	Subject	Issuer	Valid From	Valid To
1	default	SELF	CN=vpn50_B8ECA31E2398	CN=vpn50_B8ECA31E2398	2017-01-07 10:19:45 GMT	2027-01-05 10:19:45 GMT

Export default certificate from ZyWALL/USG.

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only



Edit My Certificates
Certificate in PEM (Base-64) Encoded Format

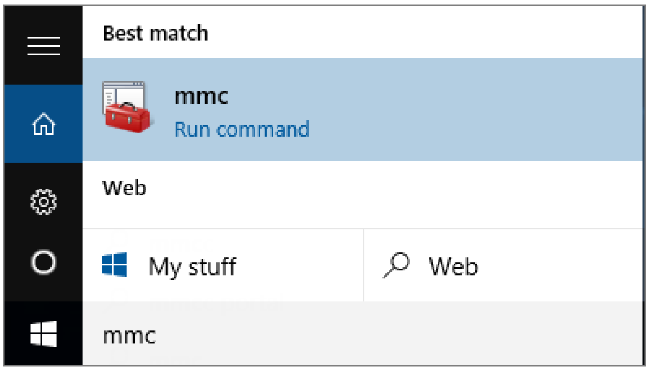
```
-----BEGIN X509 CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIJAJ+Sq14csy0wMA0GCSqGSIb3DQEBCwUAMClxIDAeBgNV
BAMMF3p5d2FsbF8xMTBfQjBCMkRDNkVBODNFMB4XDTE5MDkyMzA1MzUzOVoXDTI5
MDkyMDA1MzUzOVowIjEgMB4GA1UEAwwXenl3YWxsXzExMF9CMElyREM2RUE4M0Uw
```

Export Certificate Only
Password:
Export Certificate with Private Key
OK
Cancel

Save **default** certificate as ***.crt** file to Windows 10 computer.

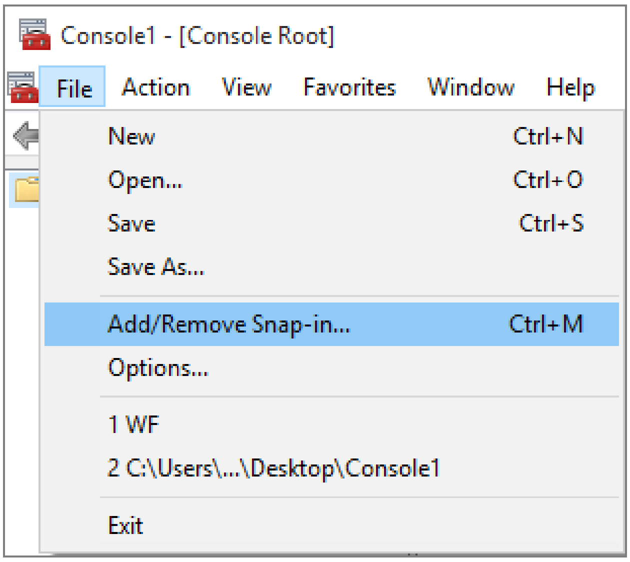
In Windows 10 Operating System, go to **Start Menu > Search Box**. Type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



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

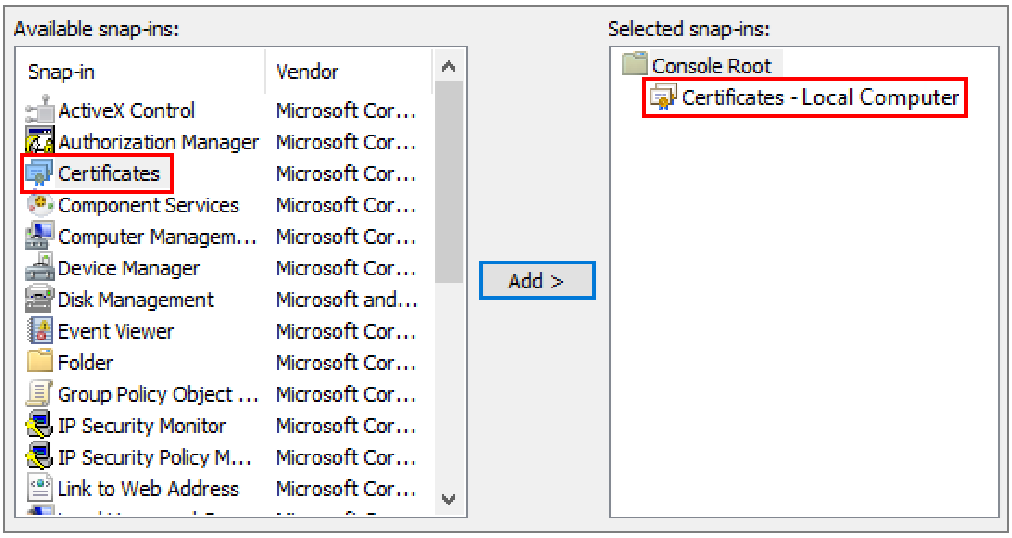
File > Add/Remove Snap-in...



In the **Available snap-ins**, select **Certificates** click **Add**. Then, click **Finished**.

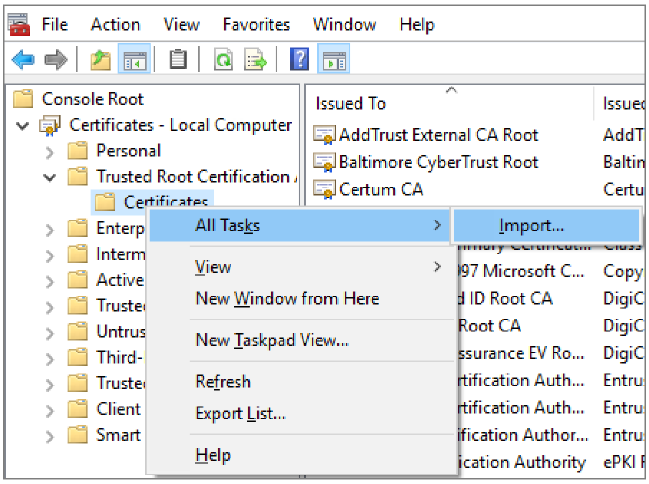
Press **OK** to close the Snap-ins window.

Available snap-ins > Certificates > Add

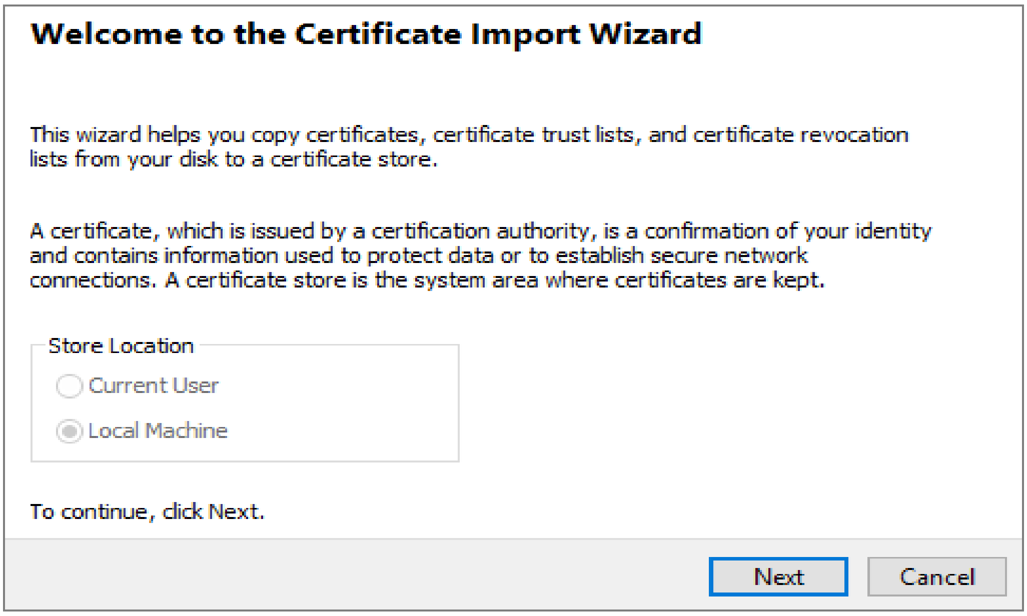


Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft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

In the mmc console window, go to **Certificates (Local Computer) > Trusted Root Certification Authorities,** right click **Certificate > All Tasks > Import…**



Click **Next**.



Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

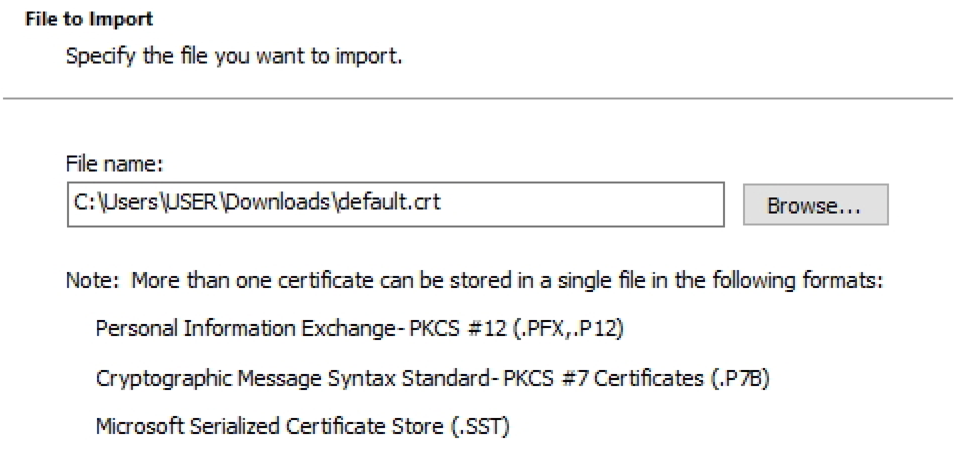
Store Location

○ Current User

● Local Machine

To continue, click Next.

Click **Browse...**, and locate the .crt file you downloaded earlier. Then, click **Next**.



File to Import

Specify the file you want to import.

File name:

C:\Users\USER\Downloads\default.crt

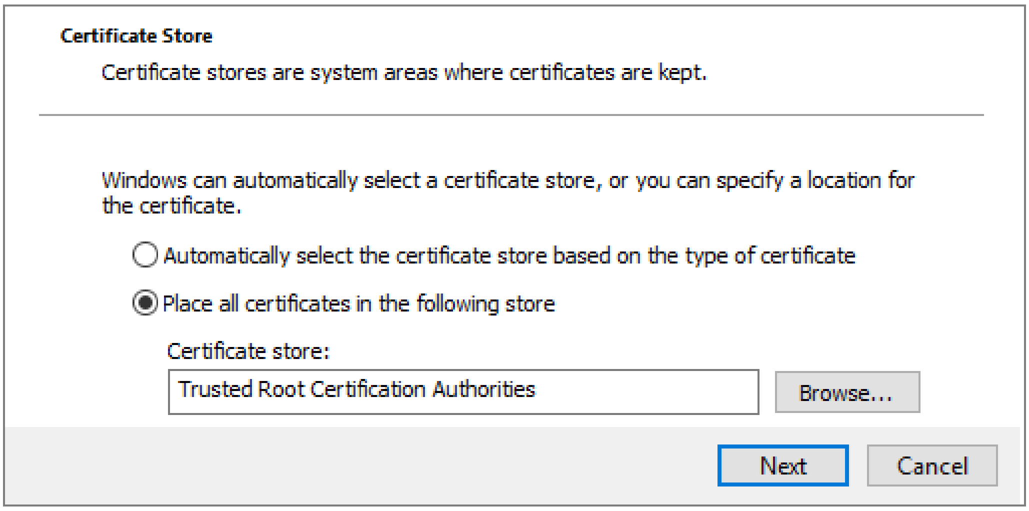
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities.** Click **Next**, then click **Finish**.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Set Up the L2TP VPN Tunnel on the Windows 10

To configure L2TP VPN in Windows 10 operating system, go to **Start > Settings > Network & Internet > VPN > Add a VPN Connection** and configure as follows.

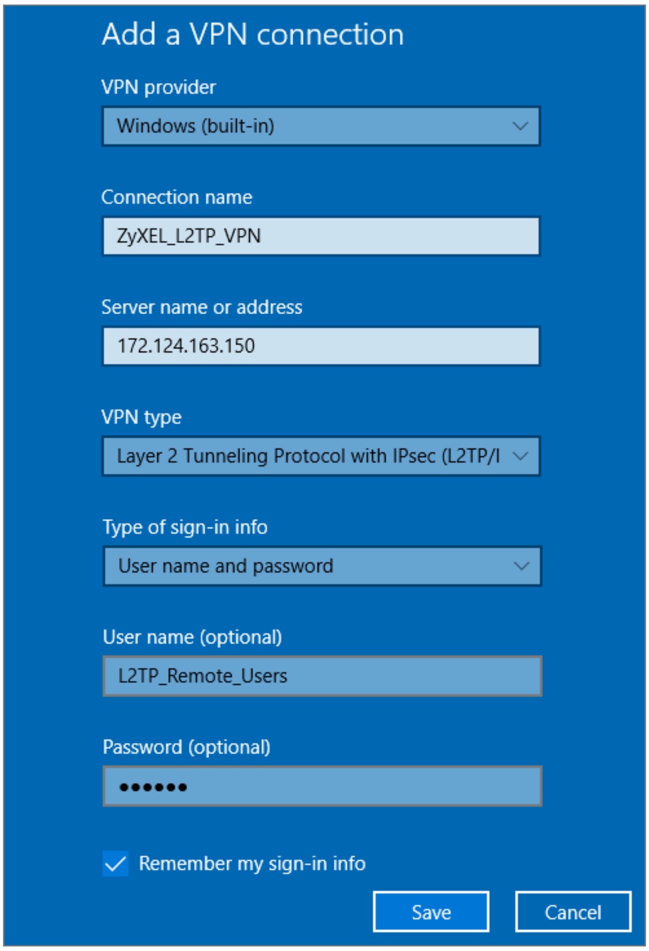
VPN Provider set to **Windows (built-in)**.

Configure **Connection name** for you to identify the VPN configuration.

Set **Server** name or address to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).

Select **VPN type** to **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)**.

Enter **User name** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).



Add a VPN connection

VPN provider: Windows (built-in)

Connection name: ZyXEL_L2TP_VPN

Server name or address: 172.124.163.150

VPN type: Layer 2 Tunneling Protocol with IPsec (L2TP/I

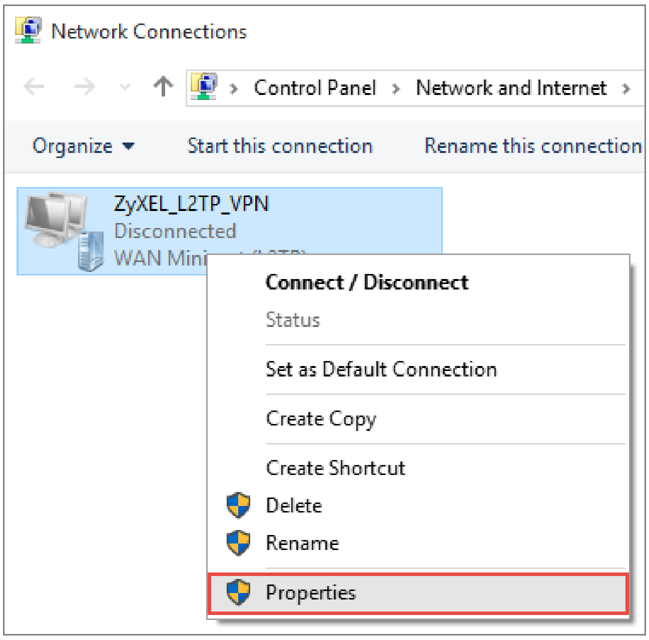
Type of sign-in info: User name and password

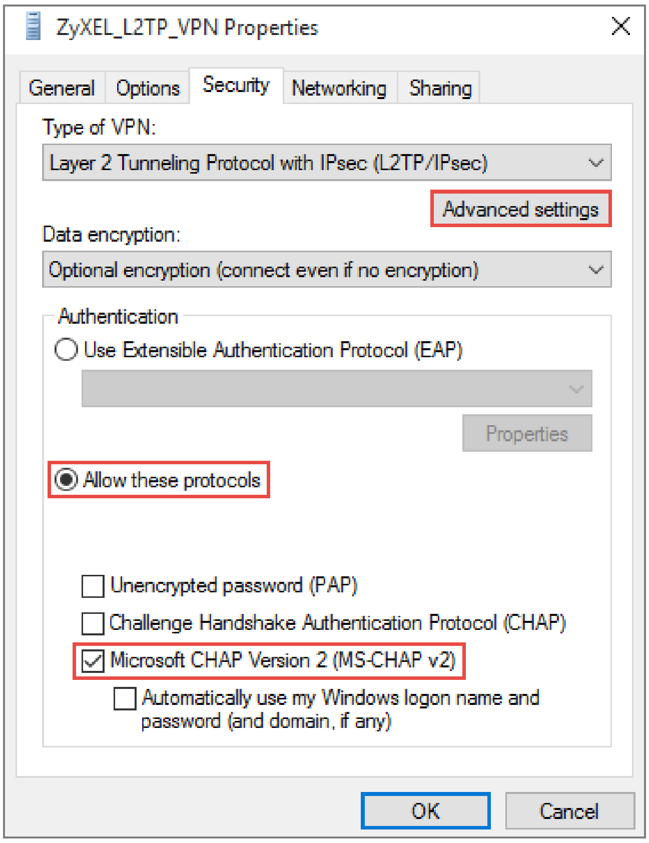
User name (optional): L2TP_Remote_Users

Password (optional): ••••••

☑ Remember my sign-in info

Go to **Control Panel > Network and Internet > Network Connections** and right click **Properties.** Continue to **Security > Advanced settings** and select **Use Certificate for authentication**.





Type of VPN: Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Data encryption: Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

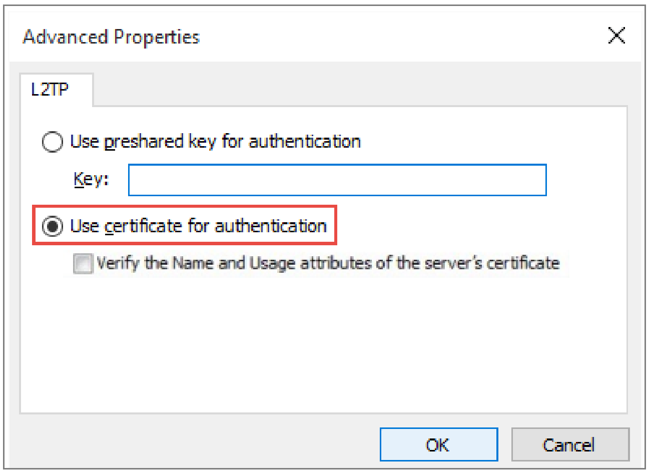
● Allow these protocols

□ Unencrypted password (PAP)

□ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)



Advanced Properties

L2TP

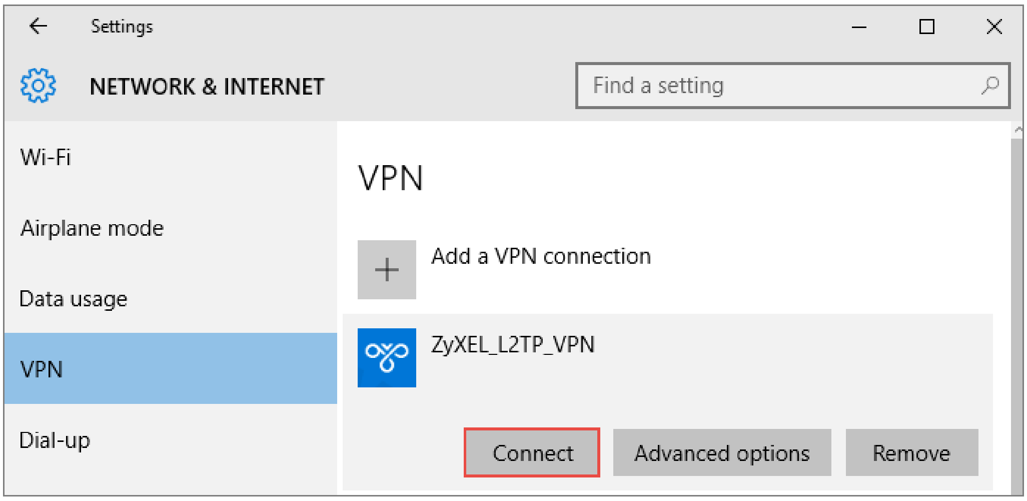
○ Use preshared key for authentication

Key:

● Use certificate for authentication

□ Verify the Name and Usage attributes of the server's certificate

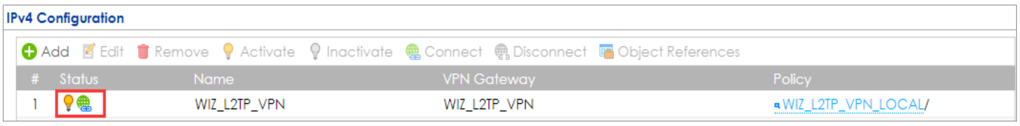
Go to **Network & Internet Settings** window, click **Connect**.



Test the L2TP over IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

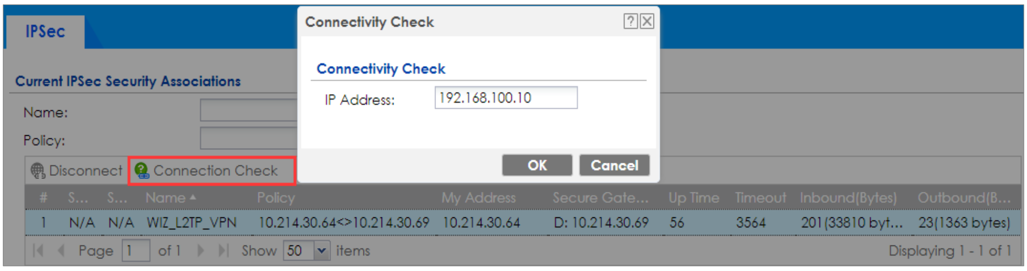


IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1		WIZ_L2TP_VPN	WIZ_L2TP_VPN	WIZ_L2TP_VPN_LOCAL/

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



Current IPSec Security Associations

Name:

Policy:

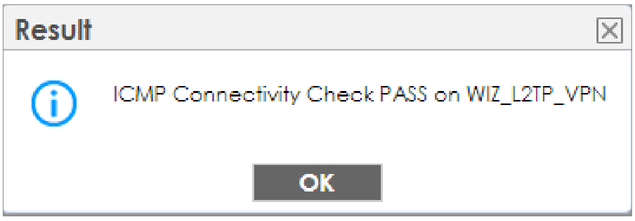
#	S...	S...	Name ▲	Policy	My Address	Secure Gate...	Up Time	Timeout	Inbound(Bytes)	Outbound(B...
1	N/A	N/A	WIZ_L2TP_VPN	10.214.30.64<>10.214.30.69	10.214.30.64	D: 10.214.30.69	56	3564	201(33810 byt...	23(1363 bytes)

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

Connectivity Check

Connectivity Check

IP Address: 192.168.100.10

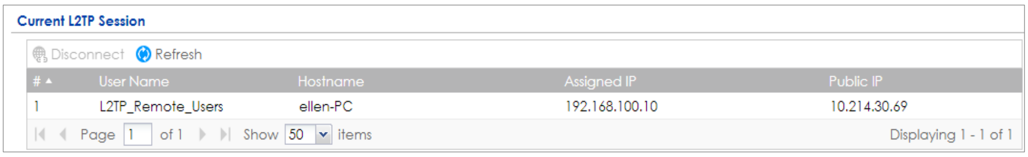


Result

ICMP Connectivity Check PASS on WIZ_L2TP_VPN

Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

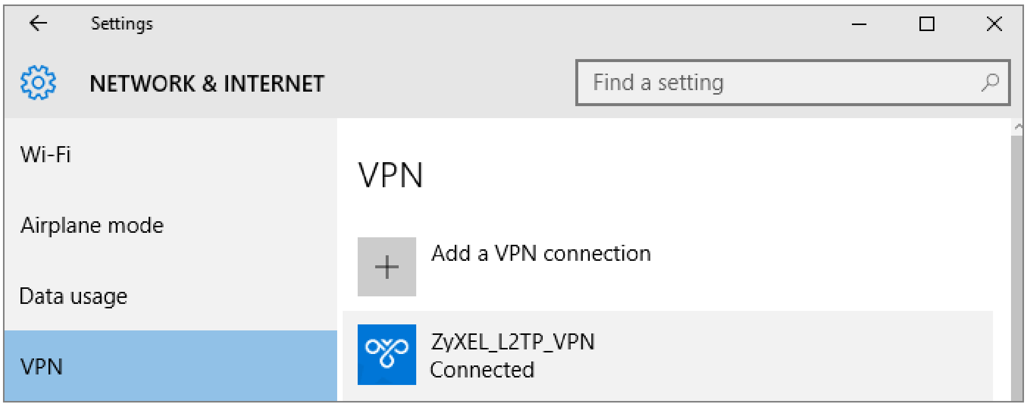


Current L2TP Session

# ▲	User Name	Hostname	Assigned IP	Public IP
1	L2TP_Remote_Users	ellen-PC	192.168.100.10	10.214.30.69

Go to Window 10 operating system **Start > Settings > Network & Internet > VPN** and show **Connected** status.

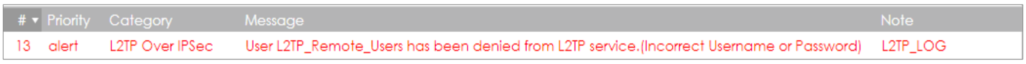
Menu > Settings > VPN > ZyXEL_L2TP



ZyXEL_L2TP_VPN
Connected

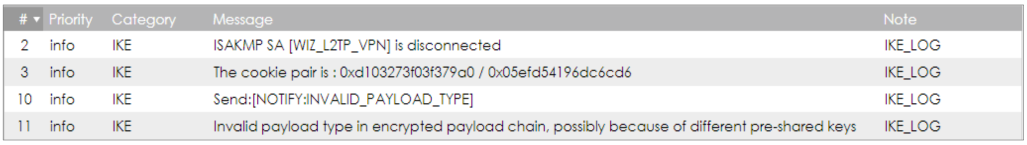
What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP Allowed User or User/Group Settings. Windows 10 users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.



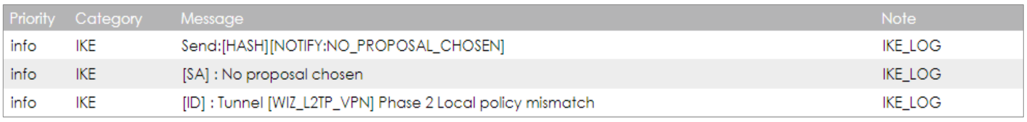
# ▾	Priority	Category	Message	Note
13	alert	L2TP Over IPSec	User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password)	L2TP_LOG

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. Windows 10 operating system users must use the same Pre-Shared Key as configured in ZyWALL/USG to establish the IKE SA.



# ▾	Priority	Category	Message	Note
2	info	IKE	ISAKMP SA [WIZ_L2TP_VPN] is disconnected	IKE_LOG
3	info	IKE	The cookie pair is : 0xd103273f03f379a0 / 0x05efd54196dc6cd6	IKE_LOG
10	info	IKE	Send:[NOTIFY:INVALID_PAYLOAD_TYPE]	IKE_LOG
11	info	IKE	Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys	IKE_LOG

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.



Priority	Category	Message	Note
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch	IKE_LOG

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

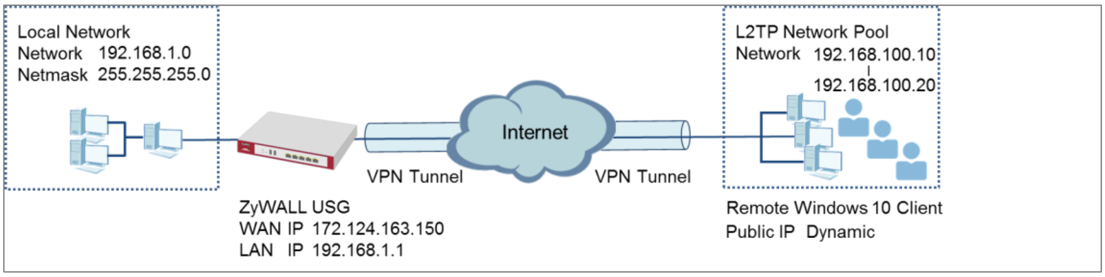
Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Verify that the Zone is set correctly in the VPN Connection rule. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Import ZyWALL/USG Certificate for L2TP over IPsec in iOS mobile phone

This is an example of using the L2TP VPN and VPN client software included in Android mobile phone operating systems. When the VPN tunnel is configured, users can securely access the network behind the ZyWALL/USG and allow traffic from L2TP clients to go to the Internet from an iOS mobile phone.

ZyWALL/USG L2TP VPN with Remote iOS Mobile Phone Client Example

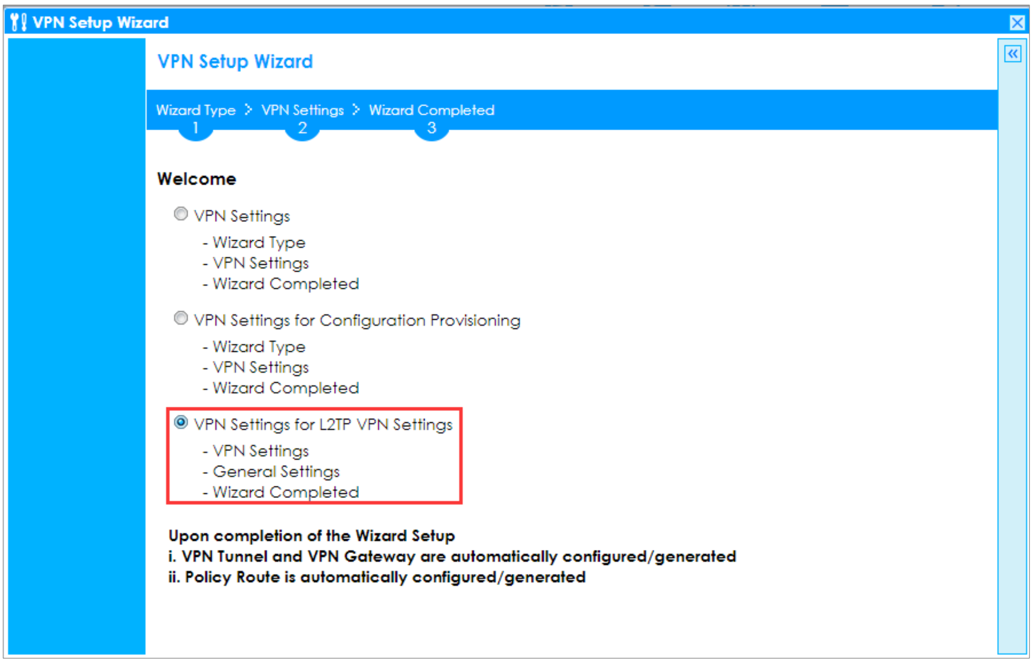


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and iOS (Version: 10.0.10240)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the iOS mobile phone clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



Welcome

○ VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

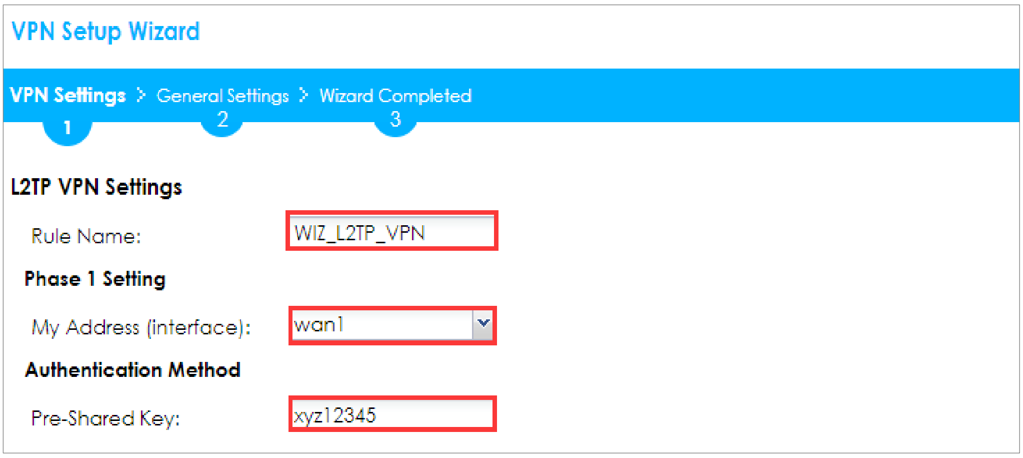
○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

● VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Upon completion of the Wizard Setup
i. VPN Tunnel and VPN Gateway are automatically configured/generated
ii. Policy Route is automatically configured/generated

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



L2TP VPN Settings

Rule Name: WIZ_L2TP_VPN

Phase 1 Setting

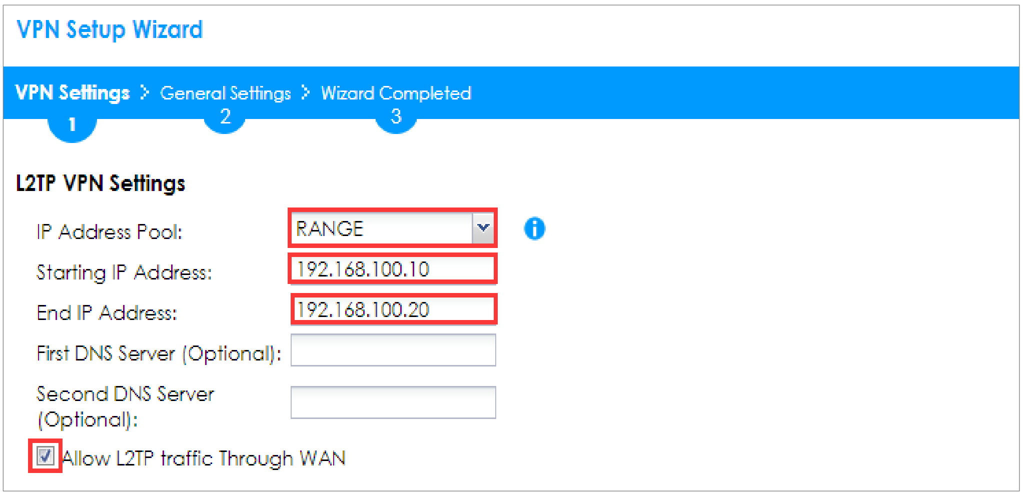
My Address (interface): wan1

Authentication Method

Pre-Shared Key: xyz12345

Assign the L2TP users' IP address range from 192.168.100.10 to 192.168.100.20 for use in the L2TP VPN tunnel and select **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)



VPN Setup Wizard

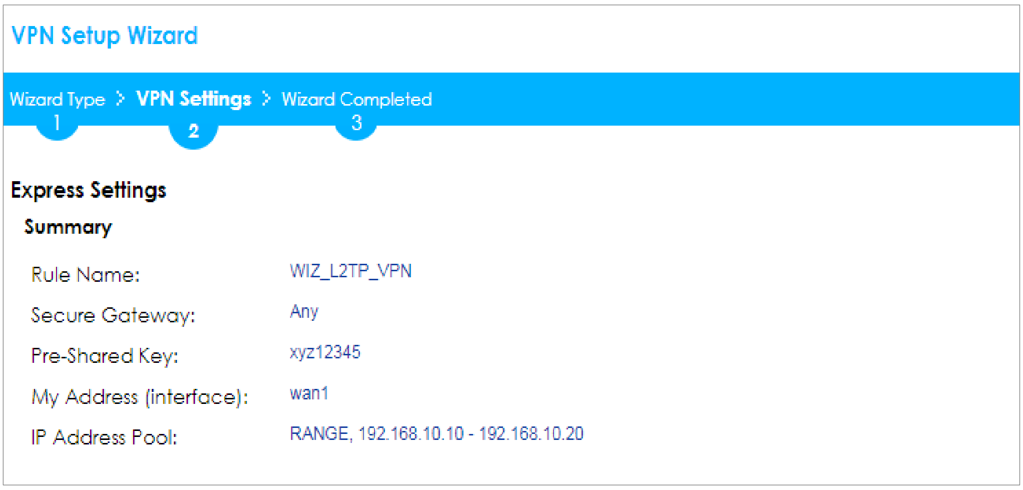
L2TP VPN Settings

IP Address Pool:	RANGE
Starting IP Address:	192.168.100.10
End IP Address:	192.168.100.20
First DNS Server (Optional):	
Second DNS Server (Optional):	

☑ Allow L2TP traffic Through WAN

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)



VPN Setup Wizard

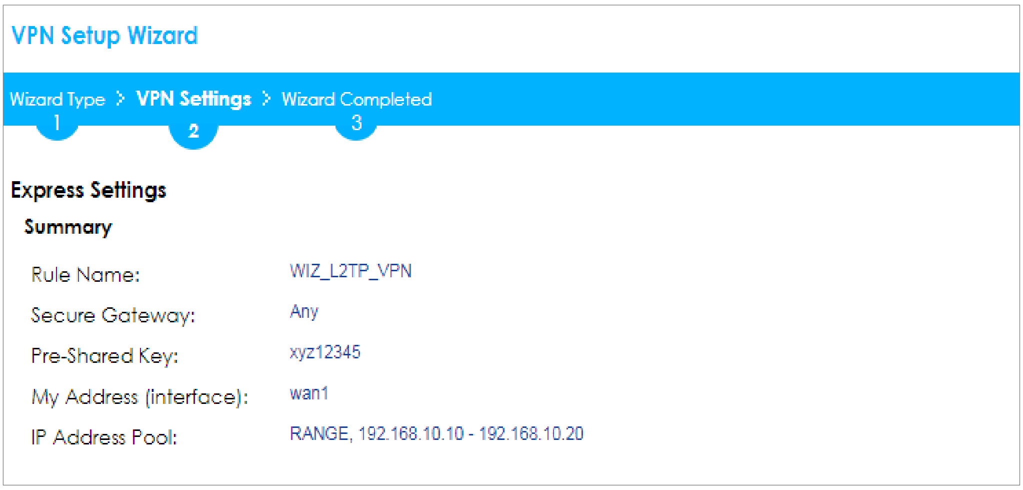
Express Settings

Summary

Rule Name:	WIZ_L2TP_VPN
Secure Gateway:	Any
Pre-Shared Key:	xyz12345
My Address (interface):	wan1
IP Address Pool:	RANGE, 192.168.10.10 - 192.168.10.20

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Wizard Completed



VPN Setup Wizard

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

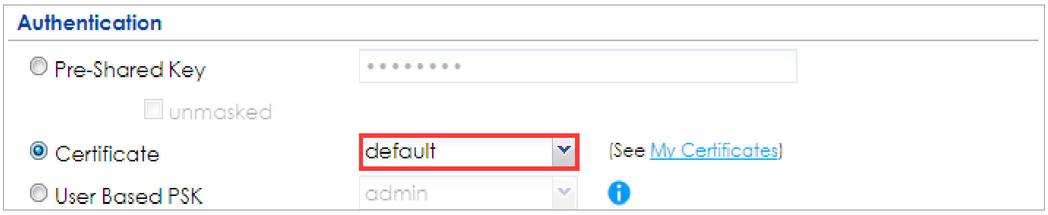
Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

Go to **CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN,** change **Authentication** method to be **Certificate** and select the certificate which ZyWALL/USG uses to identify itself to the Android mobile phone.

CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN > Authentication > Certificate



Authentication

○ Pre-Shared Key ••••••••

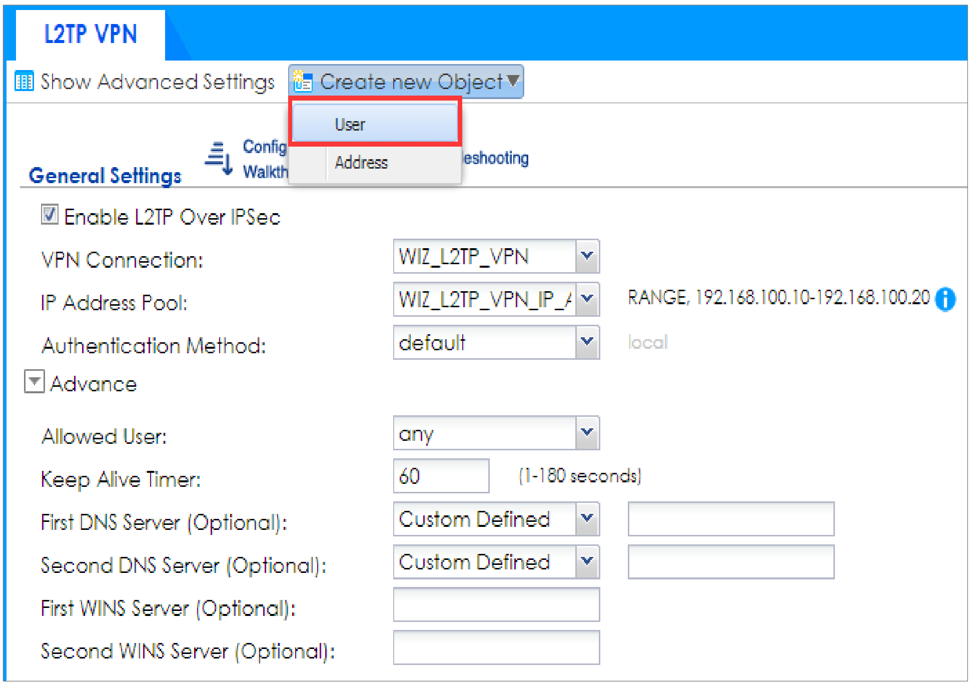
□ unmasked

● Certificate default (See My Certificates)

○ User Based PSK admin

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User



General Settings

☑ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_A RANGE, 192.168.100.10-192.168.100.20

Authentication Method: default local

Advance

Allowed User: any

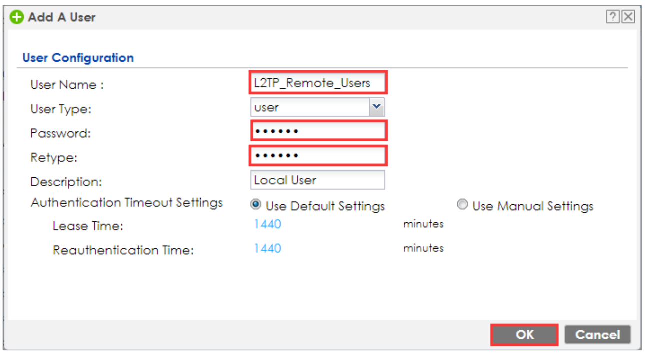
Keep Alive Timer: 60 (1-180 seconds)

First DNS Server (Optional): Custom Defined

Second DNS Server (Optional): Custom Defined

First WINS Server (Optional):

Second WINS Server (Optional):



User Configuration

User Name : L2TP_Remote_Users

User Type: user

Password: ••••••

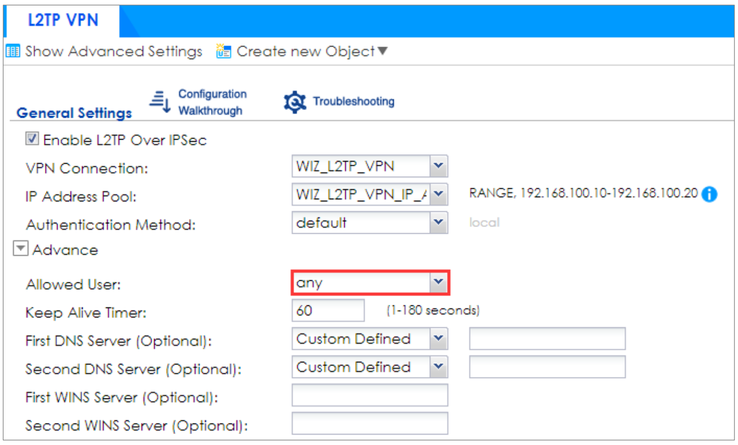
Retype: ••••••

Description: Local User

Authentication Timeout Settings ● Use Default Settings ○ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes



General Settings

☑ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_A RANGE, 192.168.100.10-192.168.100.20

Authentication Method: default local

Advance

Allowed User: any

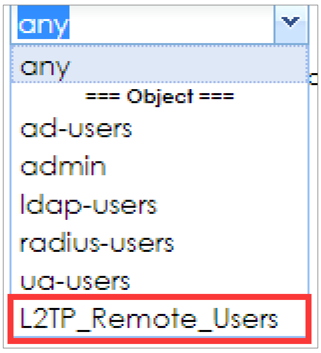
Keep Alive Timer: 60 (1-180 seconds)

First DNS Server (Optional): Custom Defined

Second DNS Server (Optional): Custom Defined

First WINS Server (Optional):

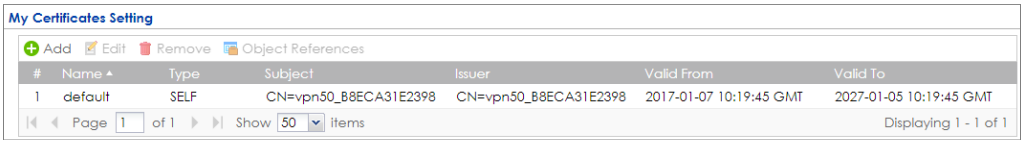
Second WINS Server (Optional):



Export a Certificate from ZyWALL/USG and Import it to iOS Mobile Phone

Go to ZyWALL/USG **CONFIGURATION** > **Object** > **Certificate**, select the certificate (**default** in this example) and click **Edit**.

CONFIGURATION > Object > Certificate > default

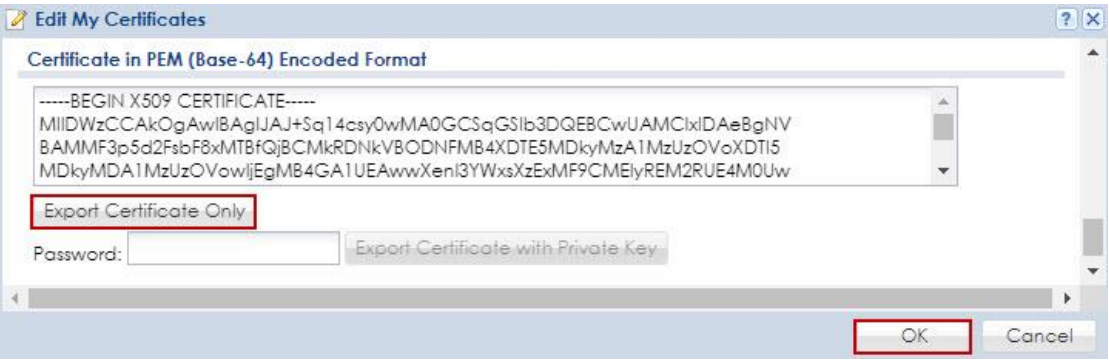


My Certificates Setting

#	Name ▲	Type	Subject	Issuer	Valid From	Valid To
1	default	SELF	CN=vpn50_B8ECA31E2398	CN=vpn50_B8ECA31E2398	2017-01-07 10:19:45 GMT	2027-01-05 10:19:45 GMT

Export default certificate from ZyWALL/USG.

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only



Edit My Certificates

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN X509 CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIJAJ+Sq14csy0wMA0GCSqGSIb3DQEBCwUAMClxIDAeBgNV
BAMMF3p5d2FsbF8xMTBfQjBCMkRDNkVBODNFMB4XDTE5MDkyMzA1MzUzOVoXDTI5
MDkyMDA1MzUzOVowIjEgMB4GA1UEAwwXenI3YWxsXzExMF9CMElyREM2RUE4M0Uw
```

Save **default** certificate as ***.crt** file to Android mobile phone computer.

Set Up the L2TP VPN Tunnel on the iOS Mobile Device

1 To configure L2TP VPN in iOS operating system, go to **Start** > **Settings** > **Network & Internet** > **VPN** > **Add a VPN Connection** and configure as follows.

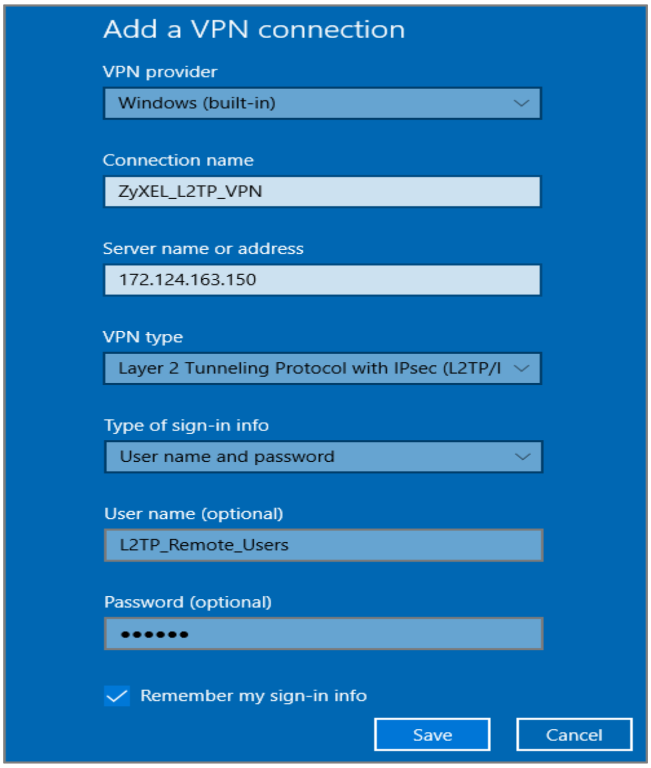
2 VPN Provider set to Windows (built-in).

3 Configure **Connection name** for you to identify the VPN configuration.

4 Set **Server** name or address to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).

5 Select VPN type to Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec).

6 Enter **User name** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).



Add a VPN connection

VPN provider: Windows (built-in)

Connection name: ZyXEL_L2TP_VPN

Server name or address: 172.124.163.150

VPN type: Layer 2 Tunneling Protocol with IPsec (L2TP/I

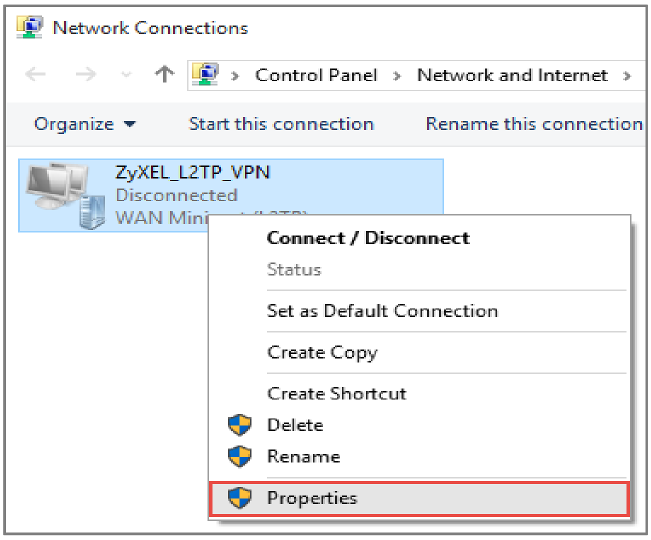
Type of sign-in info: User name and password

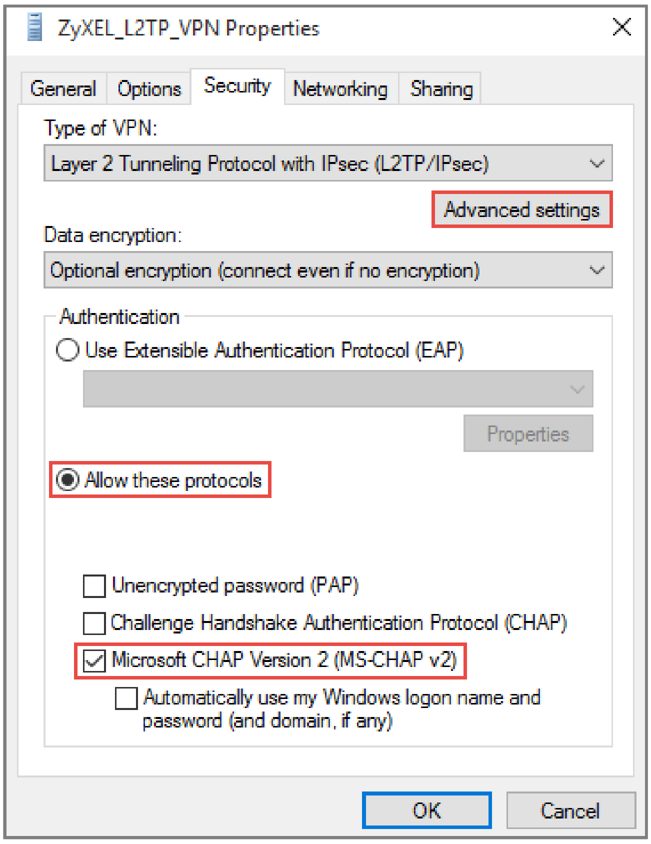
User name (optional): L2TP_Remote_Users

Password (optional): ••••••

☑ Remember my sign-in info

7 Go to Control Panel > Network and Internet > Network Connections and right click Properties. Continue to Security > Advanced settings and select Use Certificate for authentication.




ZyXEL_L2TP_VPN Properties

General | Options | Security | Networking | Sharing

Type of VPN:
Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Advanced settings

Data encryption:
Optional encryption (connect even if no encryption)

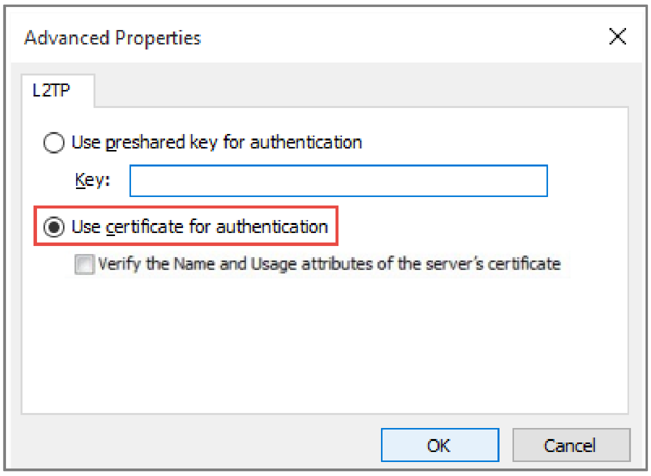
Authentication
○ Use Extensible Authentication Protocol (EAP)

Properties

● Allow these protocols

□ Unencrypted password (PAP)
□ Challenge Handshake Authentication Protocol (CHAP)
☑ Microsoft CHAP Version 2 (MS-CHAP v2)
□ Automatically use my Windows logon name and password (and domain, if any)

OK | Cancel



Advanced Properties

L2TP

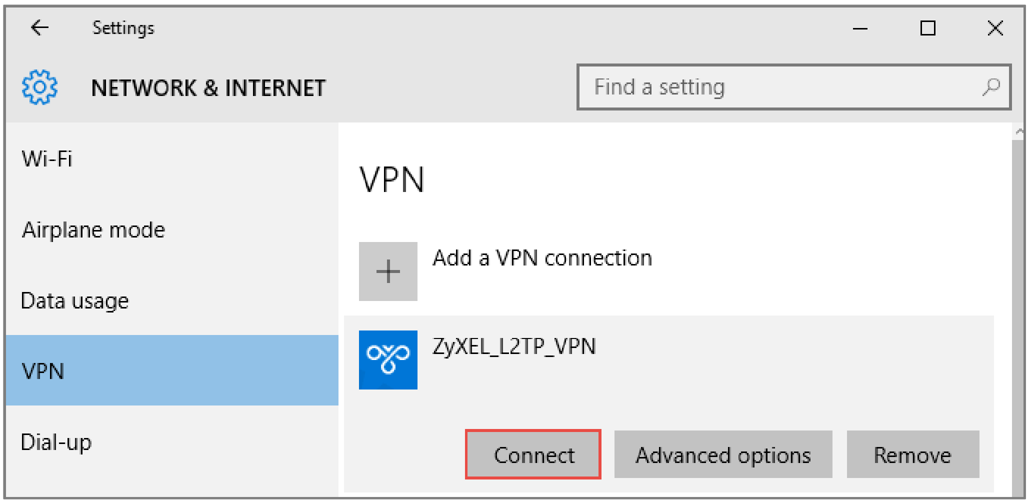
○ Use preshared key for authentication

Key:

● Use certificate for authentication

□ Verify the Name and Usage attributes of the server's certificate

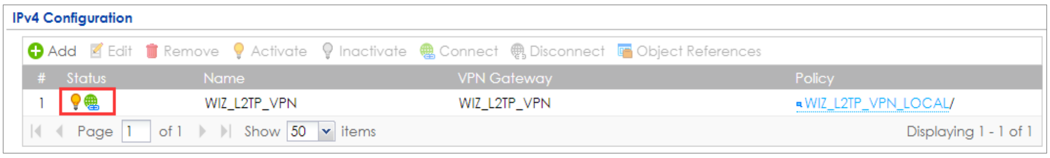
8 Go to Network & Internet Settings window, click Connect.



Test the L2TP over IPSec VPN Tunnel

1. Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



IPv4 Configuration

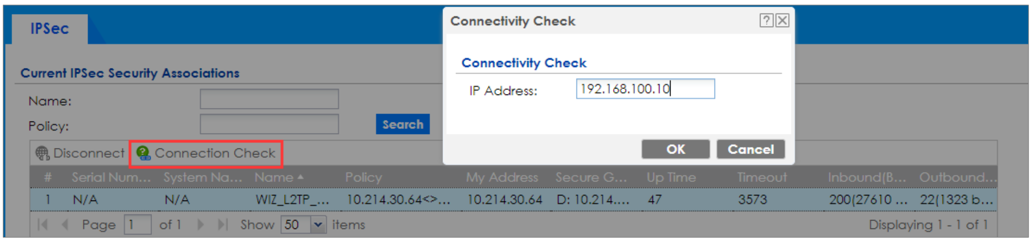
Add Edit Remove Activate Inactivate Connect Disconnect Object References

#	Status	Name	VPN Gateway	Policy
1	💡●	WIZ_L2TP_VPN	WIZ_L2TP_VPN	WIZ_L2TP_VPN_LOCAL/

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

2. Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



Current IPSec Security Associations

Name:

Policy:

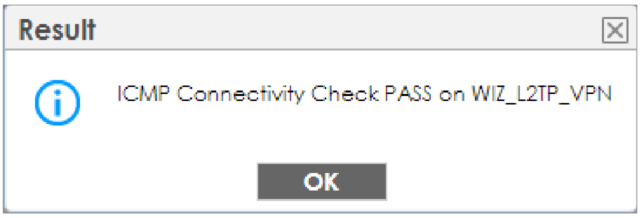
Connectivity Check

Connectivity Check

IP Address: 192.168.100.10

#	Serial Num...	System Na...	Name	Policy	My Address	Secure G...	Up Time	Timeout	Inbound(B...	Outbound...
1	N/A	N/A	WIZ_L2TP_...	10.214.30.64<>...	10.214.30.64	D: 10.214....	47	3573	200(27610 ...	22(1323 b...

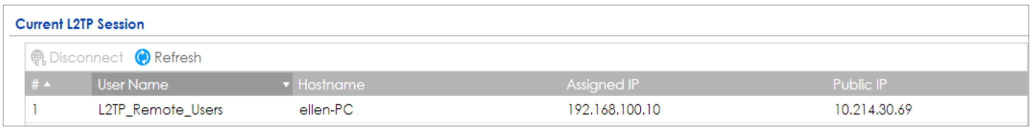
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1



ICMP Connectivity Check PASS on WIZ_L2TP_VPN

3. Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

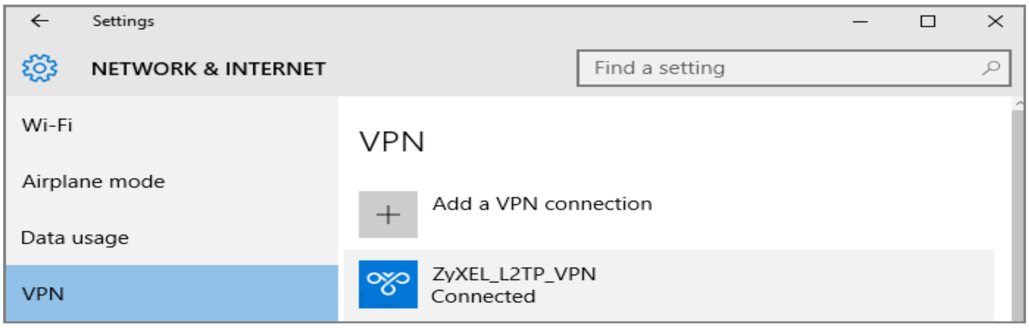


Current L2TP Session

#	User Name	Hostname	Assigned IP	Public IP
1	L2TP_Remote_Users	ellen-PC	192.168.100.10	10.214.30.69

4. Go to iOS operating system **Start > Settings > Network & Internet > VPN** and show **Connected** status.

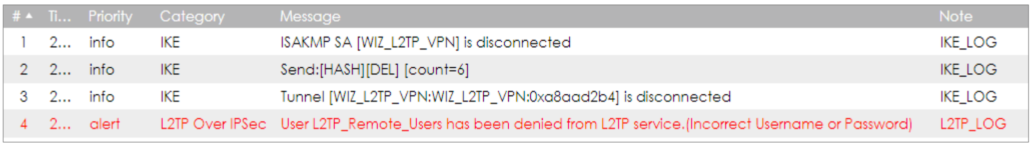
Menu > Settings > VPN > ZyXEL_L2TP



ZyXEL_L2TP_VPN
Connected

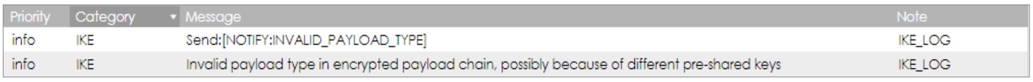
What Could Go Wrong?

1. If you see [alert] log message such as below, please check ZyWALL/USG L2TP Allowed User or User/Group Settings. iOS users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.



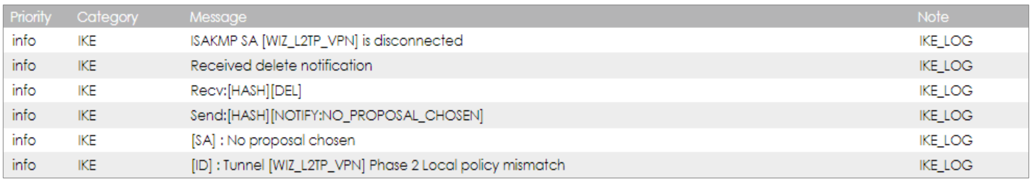
# ▲	Ti...	Priority	Category	Message	Note
1	2...	info	IKE	ISAKMP SA [WIZ_L2TP_VPN] is disconnected	IKE_LOG
2	2...	info	IKE	Send:[HASH][DEL] [count=6]	IKE_LOG
3	2...	info	IKE	Tunnel [WIZ_L2TP_VPN:WIZ_L2TP_VPN:0xa8aad2b4] is disconnected	IKE_LOG
4	2...	alert	L2TP Over IPSec	User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password)	L2TP_LOG

2. If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. iOS users must use the same Pre-Shared Key as configured in ZyWALL/USG to establish the IKE SA.



Priority	Category	Message	Note
info	IKE	Send:[NOTIFY:INVALID_PAYLOAD_TYPE]	IKE_LOG
info	IKE	Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys	IKE_LOG

3. If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.



Priority	Category	Message	Note
info	IKE	ISAKMP SA [WIZ_L2TP_VPN] is disconnected	IKE_LOG
info	IKE	Received delete notification	IKE_LOG
info	IKE	Recv:[HASH][DEL]	IKE_LOG
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch	IKE_LOG

4. Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

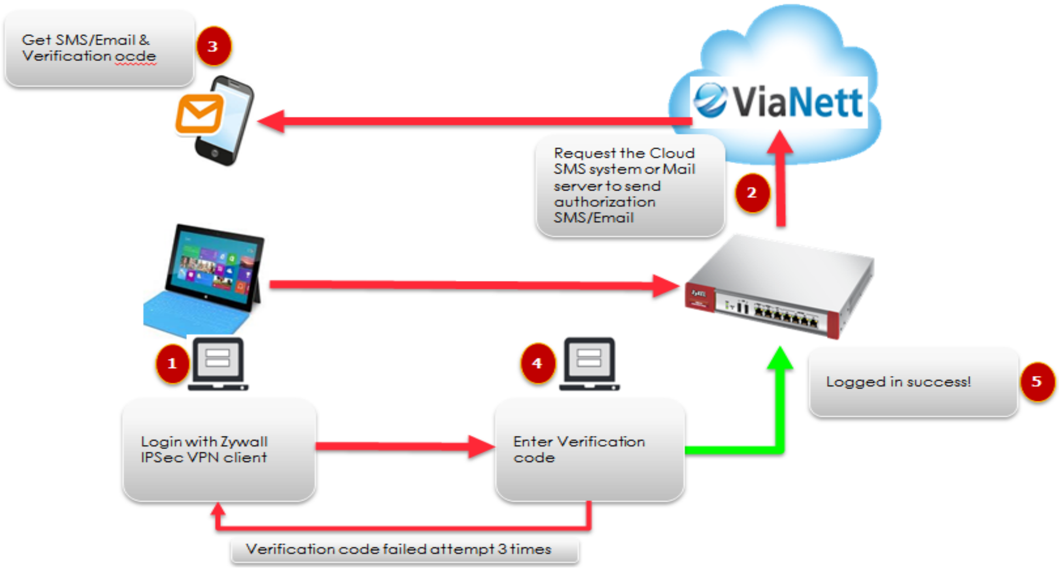
5. If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

6. Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

7. Verify that the Zone is set correctly in the VPN Connection rule. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Configure 2 factor for VPN connection?

This example shows how to use two-factor authentication to have double-layer security to access a secured network behind the Zyxel Device via a VPN tunnel between a ZyWALL/USG and a ZyWALL IPSec VPN Client. The first layer is the VPN client user name / password and the second layer is an authorized SMS (via mobile phone number) or email address.


Get SMS/Email & Verification ocde
3
ViaNett
Request the Cloud SMS system or Mail server to send authorization SMS/Email
2
1
4
Logged in success!
5
Login with Zywall IPSec VPN client
Enter Verification code
Verification code failed attempt 3 times

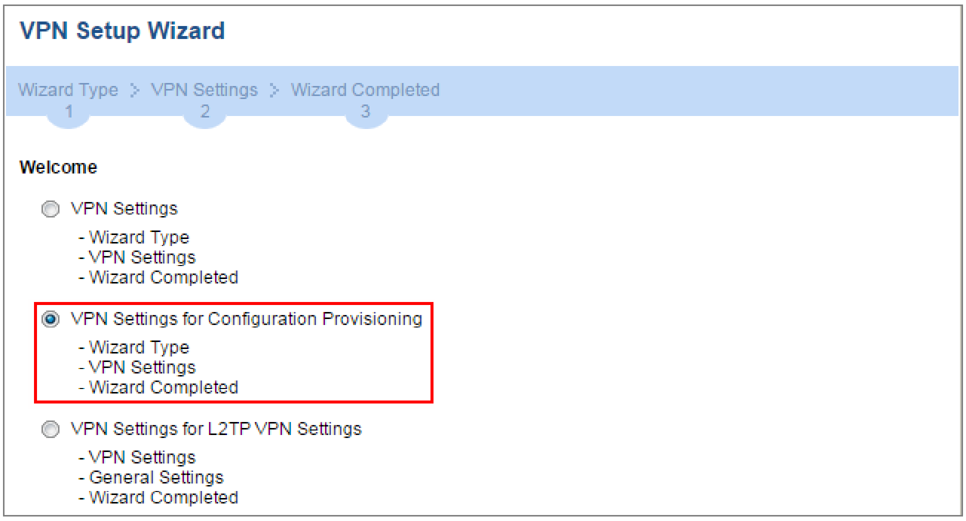
Walkthrough

1. Set up the ZyWALL/USG IPSec VPN Tunnel on USG
2. Set up the ZyWALL IPSec VPN Client on windows client.
3. Set up notification for email and SMS message sending.
4. Enable 2 factor authentications for VPN service.

Set up the ZyWALL/USG IPSec VPN Tunnel

In the ZyWALL/USG, go to **CONFIGURATION >Quick Setup > VPN Setup Wizard**, use the **VPN Settings for Configuration Provisioning** wizard to create a VPN rule that can be used with the ZyWALL IPSec VPN Client. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



Welcome

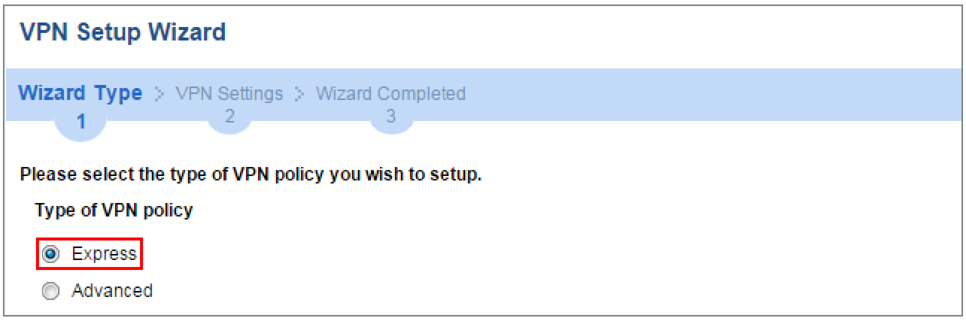
○ VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

● VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



Please select the type of VPN policy you wish to setup.

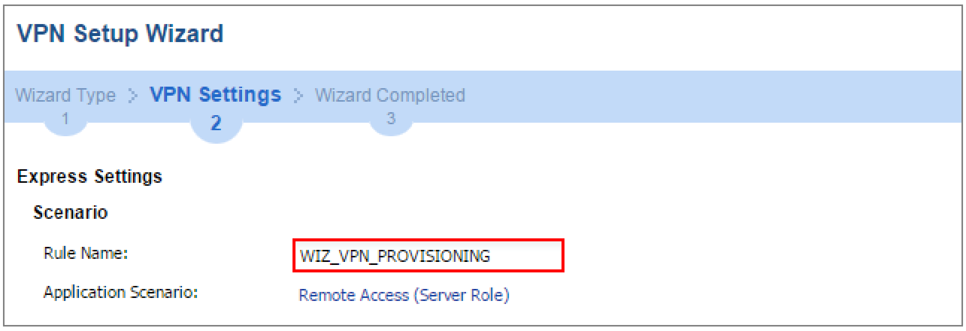
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-1



Express Settings

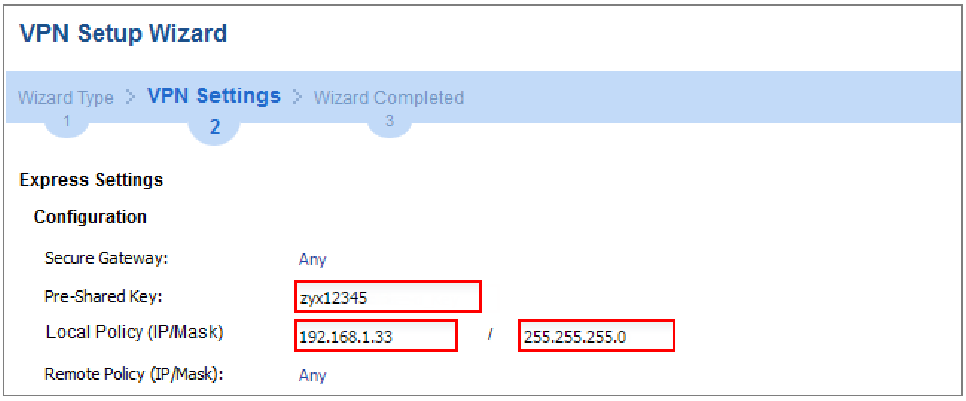
Scenario

Rule Name: WIZ_VPN_PROVISIONING

Application Scenario: Remote Access (Server Role)

Type a secure **Pre-Shared Key** (8-32 characters). Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-2



Express Settings

Configuration

Secure Gateway: Any

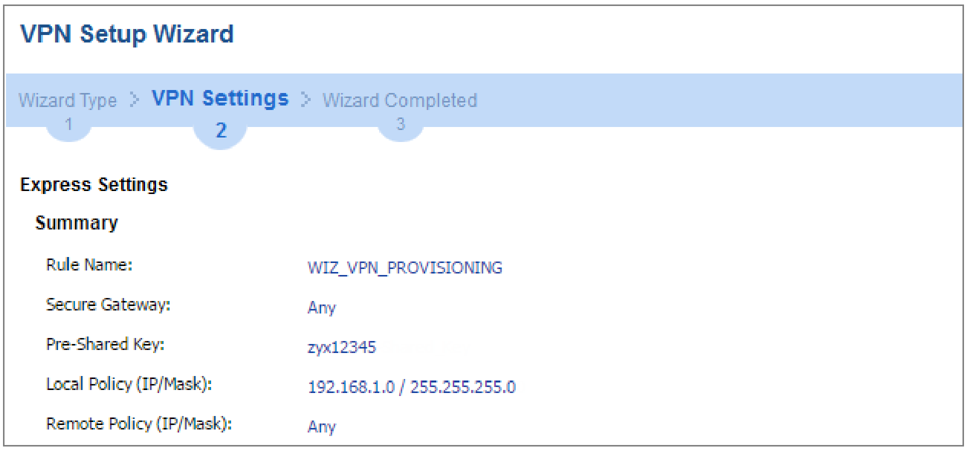
Pre-Shared Key: zyx12345

Local Policy (IP/Mask) 192.168.1.33 / 255.255.255.0

Remote Policy (IP/Mask): Any

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-3



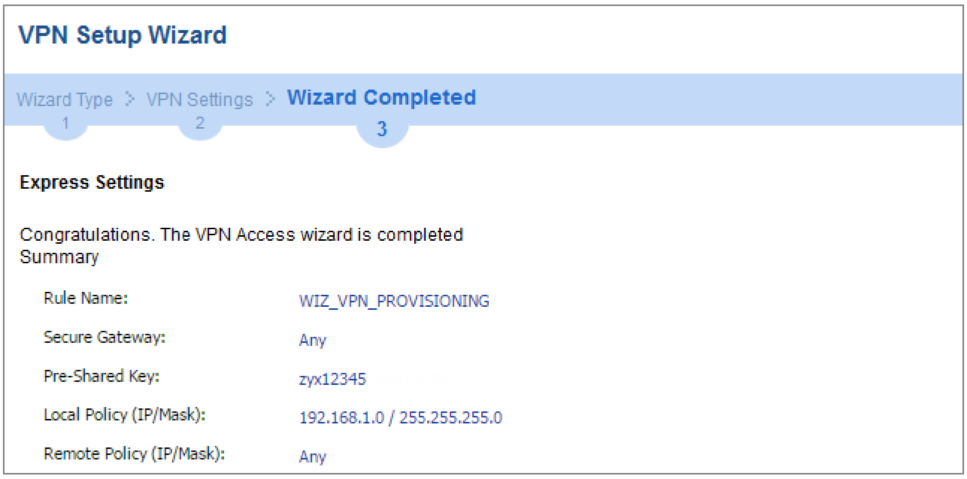
Express Settings

Summary

Rule Name:	WIZ_VPN_PROVISIONING
Secure Gateway:	Any
Pre-Shared Key:	zyx12345
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	Any

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed

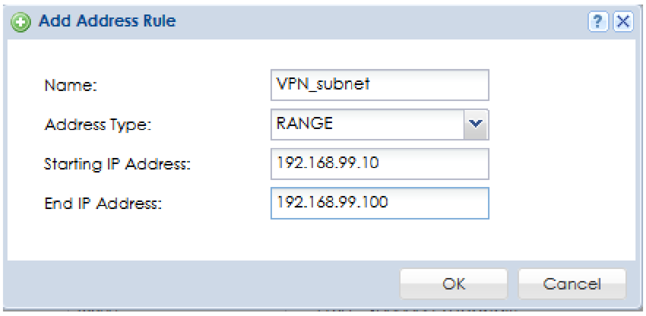


Express Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	WIZ_VPN_PROVISIONING
Secure Gateway:	Any
Pre-Shared Key:	zyx12345
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	Any

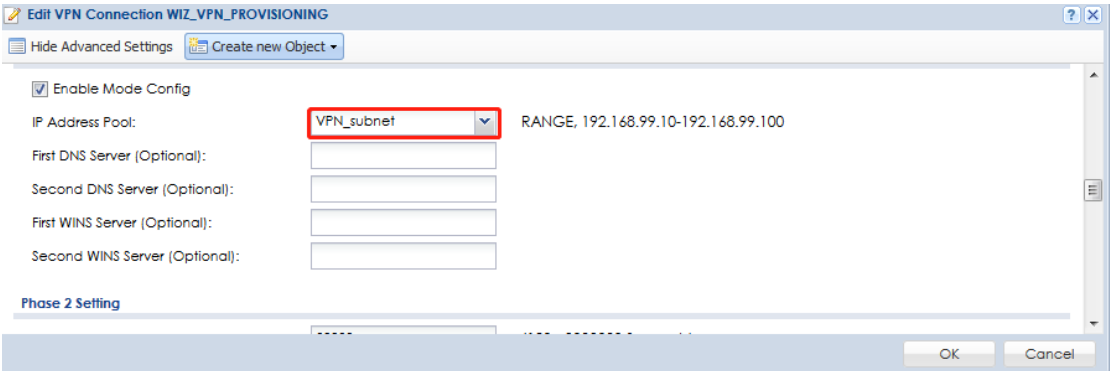
Go to **CONFIGURATION > VPN > IPSec VPN > VPN connection.** Enable **Mode config** for IPSec VPN client connection, create address object



Add Address Rule

Name:	VPN_subnet
Address Type:	RANGE
Starting IP Address:	192.168.99.10
End IP Address:	192.168.99.100

Select the address object for mode config VPN IP address Pool.



Edit VPN Connection WIZ_VPN_PROVISIONING

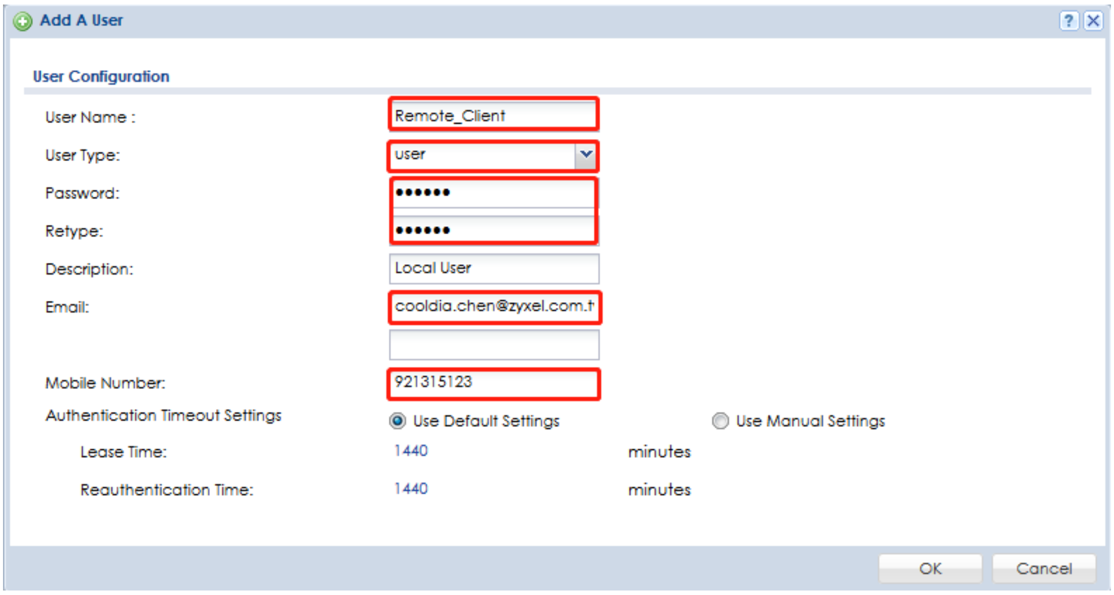
☑ Enable Mode Config

IP Address Pool:	VPN_subnet	RANGE, 192.168.99.10-192.168.99.100
First DNS Server (Optional):		
Second DNS Server (Optional):		
First WINS Server (Optional):		
Second WINS Server (Optional):		

Phase 2 Setting

Go to **CONFIGURATION > Object > User/Group > Add A User** and create a user account for the ZyWALL IPSec VPN Client user. Type one or more valid email addresses and valid mobile telephone number for this user so that messages can be sent to this user for 2 factor authentication.

CONFIGURATION > Object > User/Group > Add A User

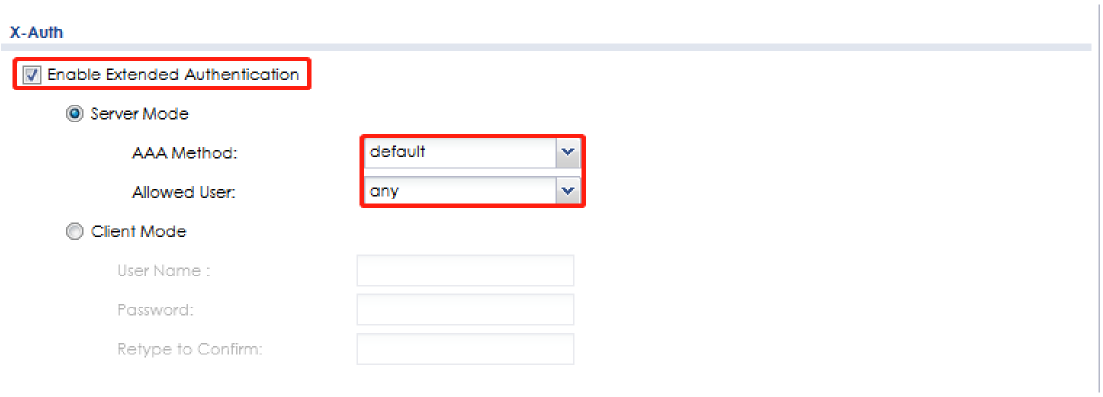


Add A User

User Configuration

User Name :	Remote_Client
User Type:	user
Password:	••••••
Retype:	••••••
Description:	Local User
Email:	cooldia.chen@zyxel.com.t
Mobile Number:	921315123
Authentication Timeout Settings	● Use Default Settings ○ Use Manual Settings
Lease Time:	1440 minutes
Reauthentication Time:	1440 minutes

Go to **CONFIGURATION > VPN > IPSec VPN > Gateway**, enable X-Auth for VPN client authentication.



X-Auth

☑ Enable Extended Authentication

● Server Mode

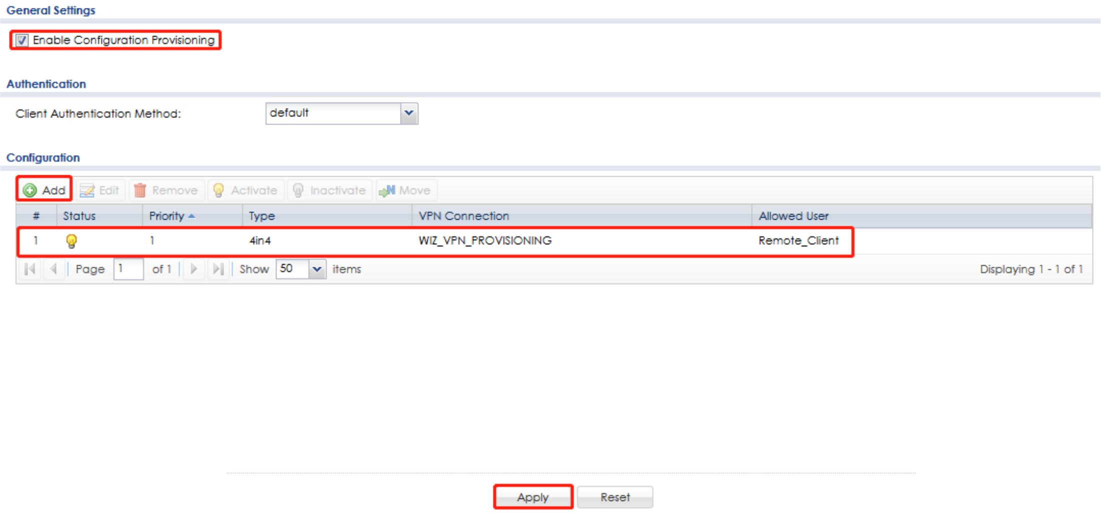
AAA Method:	default
Allowed User:	any

○ Client Mode

User Name :	
Password:	
Retype to Confirm:	

Go to **CONFIGURATION > VPN > IPSec VPN > Configuration Provisioning**. In the **General Settings** section, select the **Enable Configuration Provisioning**. Then, go to the **Configuration** section and click **Add** to bind a configured **VPN Connection** to **Allowed User**. Click **Activate** and **Apply** to save the configuration.

CONFIGURATION > VPN > IPSec VPN > Configuration Provisioning



General Settings

☑ Enable Configuration Provisioning

Authentication

Client Authentication Method: default

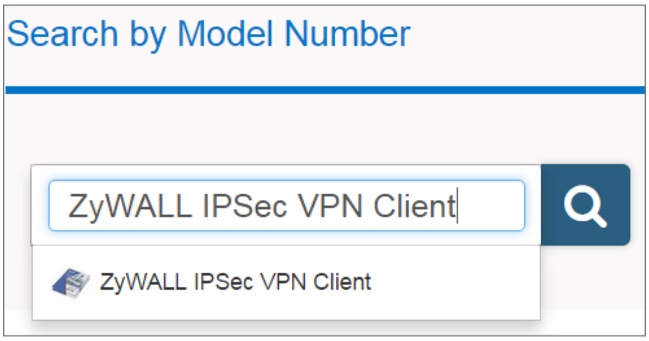
Configuration

#	Status	Priority	Type	VPN Connection	Allowed User
1	💡	1	4in4	WIZ_VPN_PROVISIONING	Remote_Client

Set up the ZyWALL IPSec VPN Client

Download **ZyWALL IPSec VPN Client** software from ZyXEL Download Library:

http://www.zyxel.com/support/download_landing.shtml

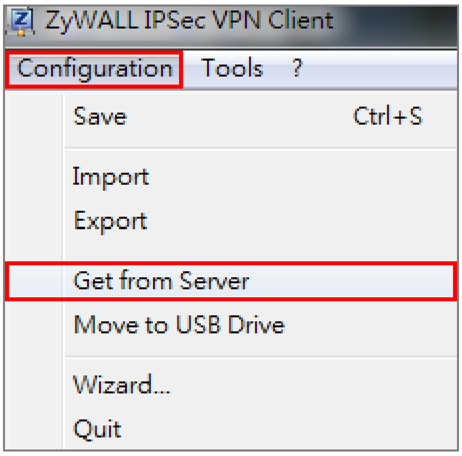


Search by Model Number

ZyWALL IPSec VPN Client

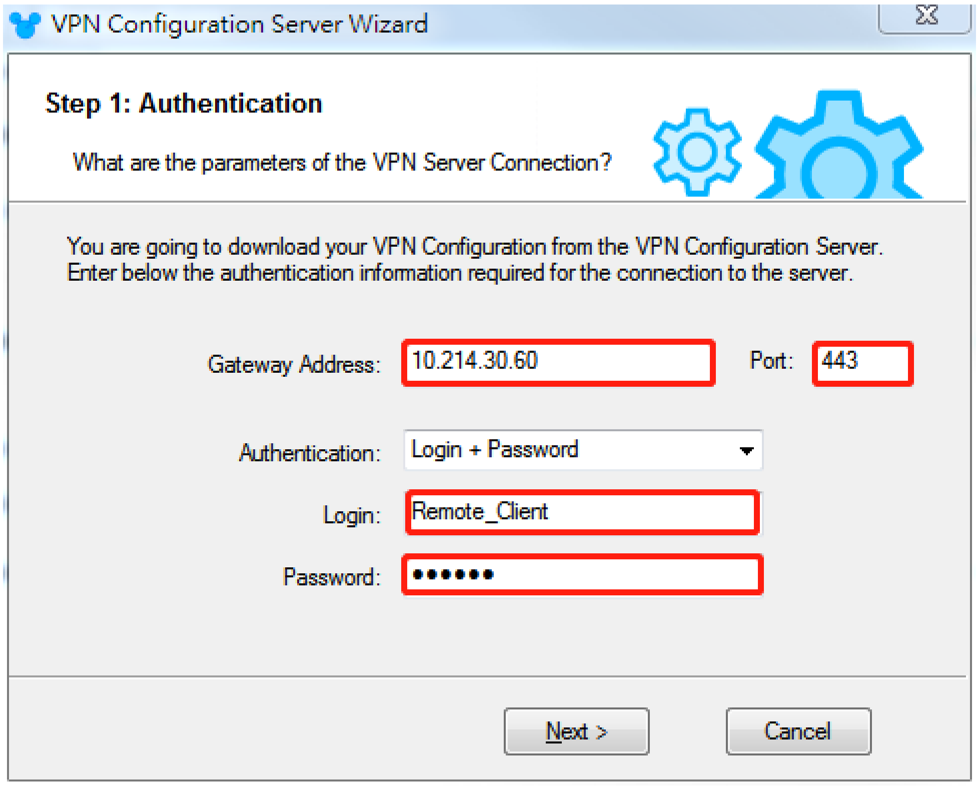
Open ZyWALL IPSec VPN Client, select **CONFIGURATION > Get from Server**.

CONFIGURATION > Get from Server



Enter the WAN IP address or URL for the ZyWALL/USG in the **Gateway Address**. If you changed the default HTTPS **Port** on the ZyWALL/USG, and then enter the new one here. Enter the **Login** user name and **Password** exactly as configured on the ZyWALL or external authentication server. Click **Next**, you will see it's processing VPN configuration from the server.

CONFIGURATION > Get from Server > Step 1: Authentication



VPN Configuration Server Wizard

Step 1: Authentication

What are the parameters of the VPN Server Connection?

You are going to download your VPN Configuration from the VPN Configuration Server. Enter below the authentication information required for the connection to the server.

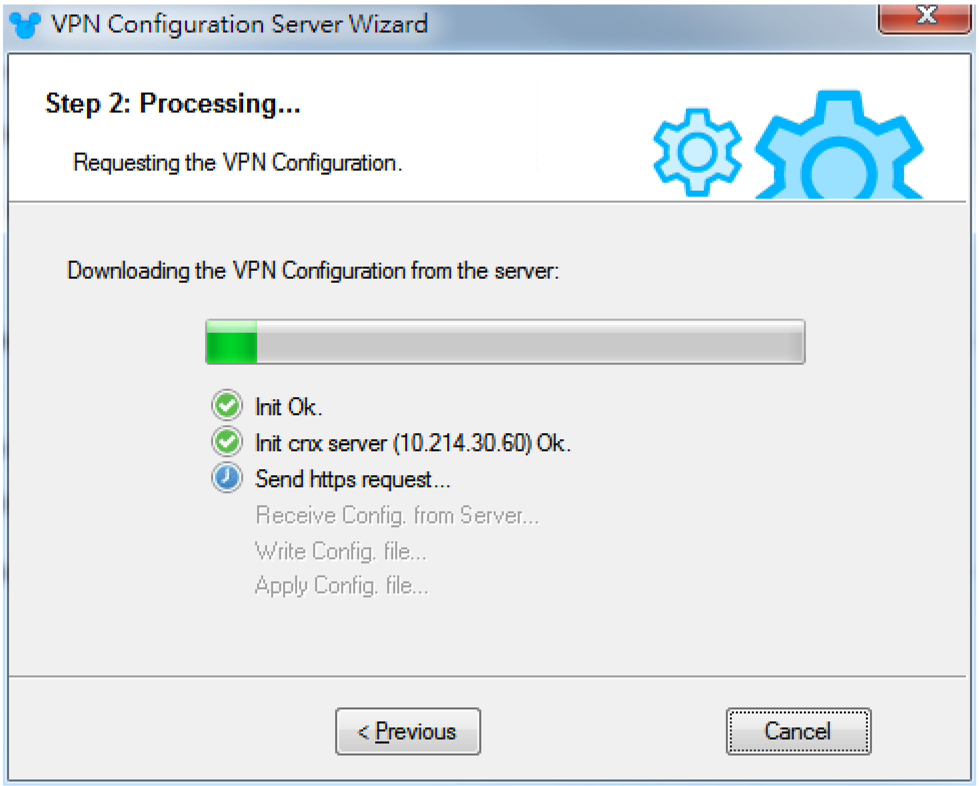
Gateway Address: 10.214.30.60 Port: 443

Authentication: Login + Password

Login: Remote_Client

Password: ••••••

CONFIGURATION > Get from Server > Step 2: Processing



VPN Configuration Server Wizard

Step 2: Processing...

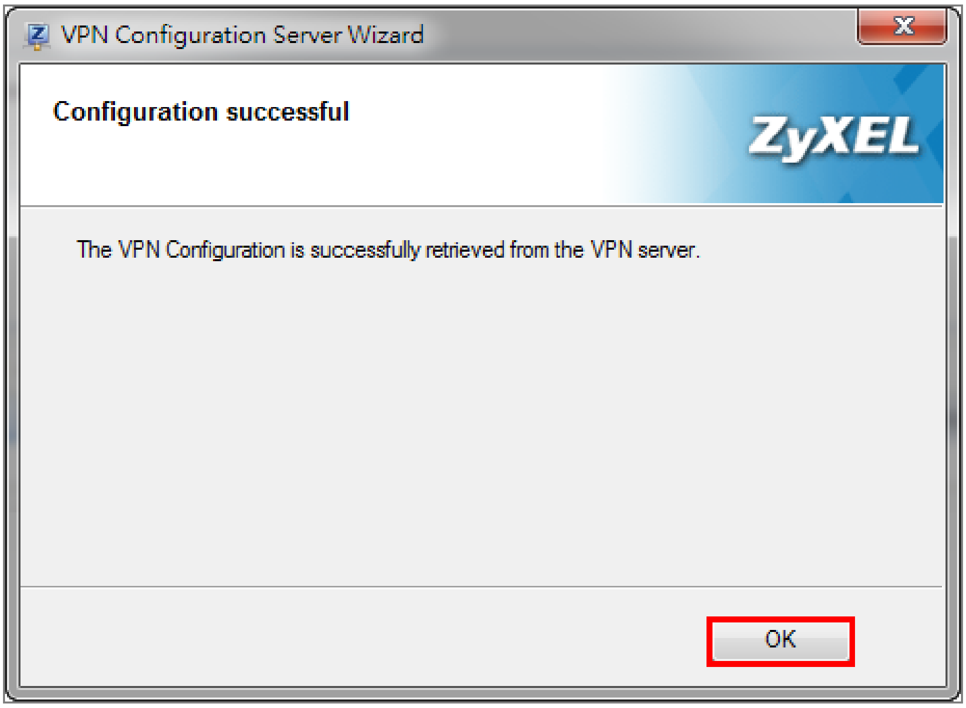
Requesting the VPN Configuration.

Downloading the VPN Configuration from the server:

- ✓ Init Ok.
- ✓ Init cnx server (10.214.30.60) Ok.
- Send https request...
- Receive Config. from Server...
- Write Config. file...
- Apply Config. file...

Then, you will see the **Configuration successful** page, click **OK** to exit the wizard.

CONFIGURATION > Get from Server > Configuration successful

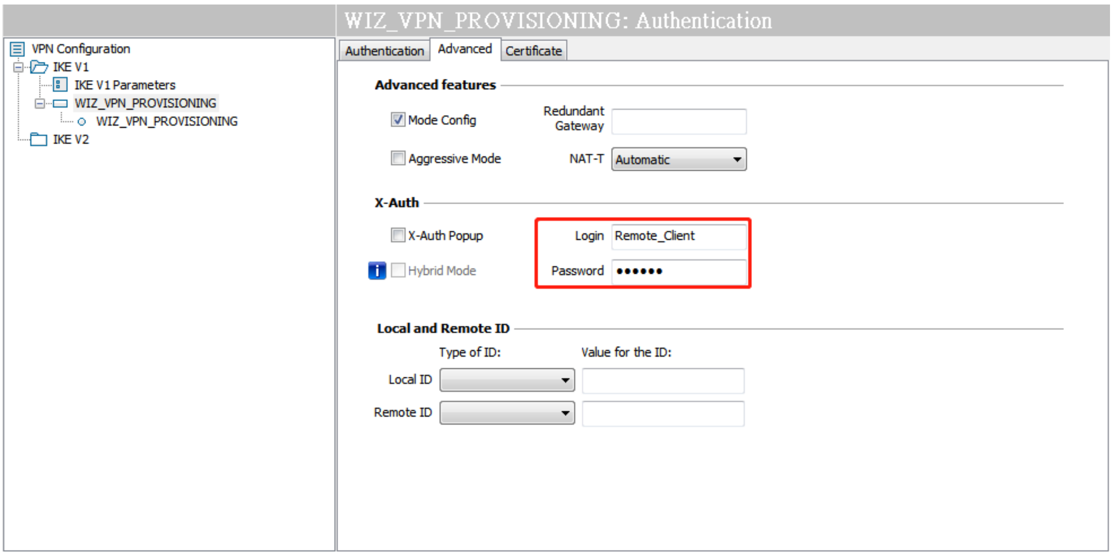


VPN Configuration Server Wizard

Configuration successful

The VPN Configuration is successfully retrieved from the VPN server.

VPN CONFIGURATION > IKE V1 > WIZ_VPN_PROVISIONING > Advanced, type Login account and password for authentication.



WIZ_VPN_PROVISIONING: Authentication

- VPN Configuration
  - IKE V1
    - IKE V1 Parameters
    - WIZ_VPN_PROVISIONING
      - WIZ_VPN_PROVISIONING
  - IKE V2

Authentication | Advanced | Certificate

Advanced features

☑ Mode Config

Redundant Gateway

□ Aggressive Mode

NAT-T Automatic

X-Auth

□ X-Auth Popup

Login Remote_Client

□ Hybrid Mode

Password ••••••

Local and Remote ID

Type of ID: Value for the ID:

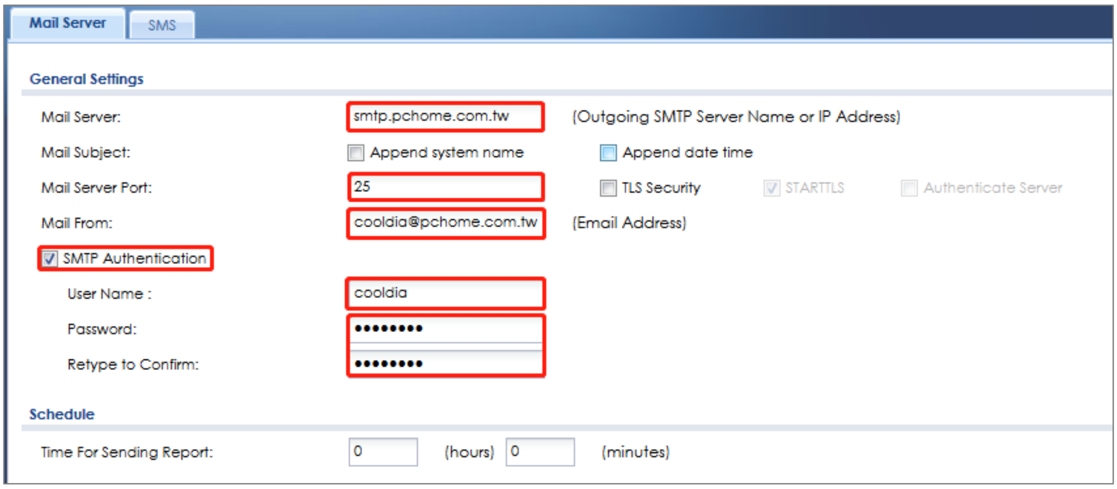
Local ID

Remote ID

Set up notification for 2 factor authentication

In the ZyWALL/USG, go to **CONFIGURATION > System > Notification > Mail Server**

1. Type the name or IP address of the SMTP server.
2. Enter the service port for SMTP.
3. Type the e-mail address from which the outgoing e-mail is delivered.
4. Select this check box if it is necessary to provide a user name and password to the SMTP server.
5. Click **"Apply"** button to save your changes to the Zyxel Device.



General Settings

Mail Server: smtp.pchome.com.tw (Outgoing SMTP Server Name or IP Address)

Mail Subject: □ Append system name □ Append date time

Mail Server Port: 25 □ TLS Security ☑ STARTTLS □ Authenticate Server

Mail From: cooldia@pchome.com.tw (Email Address)

☑ SMTP Authentication

User Name : cooldia

Password: ••••••••

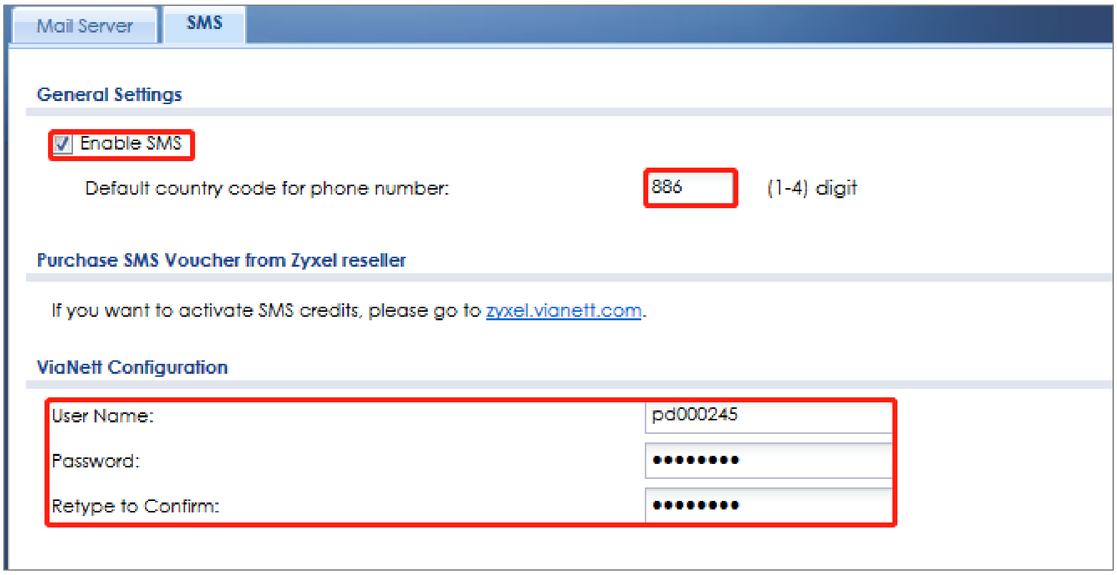
Retype to Confirm: ••••••••

Schedule

Time For Sending Report: 0 (hours) 0 (minutes)

Go to 2nd tab **CONFIGURATION > System > Notification > SMS**, in this scenario, we will use email and SMS for 2 factor authentication.

1. Select the check box "Enable SMS" to turn on the SMS service.
2. Enter the default country code for the mobile phone number to which you want to send SMS messages.
3. Enter the user name and password for your ViaNett account.
4. Click **"Apply"** button to save your changes to the Zyxel Device.



General Settings

☑ Enable SMS

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

Purchase SMS Voucher from Zyxel reseller

If you want to activate SMS credits, please go to zyxel.vianett.com.

ViaNett Configuration

User Name: pd000245

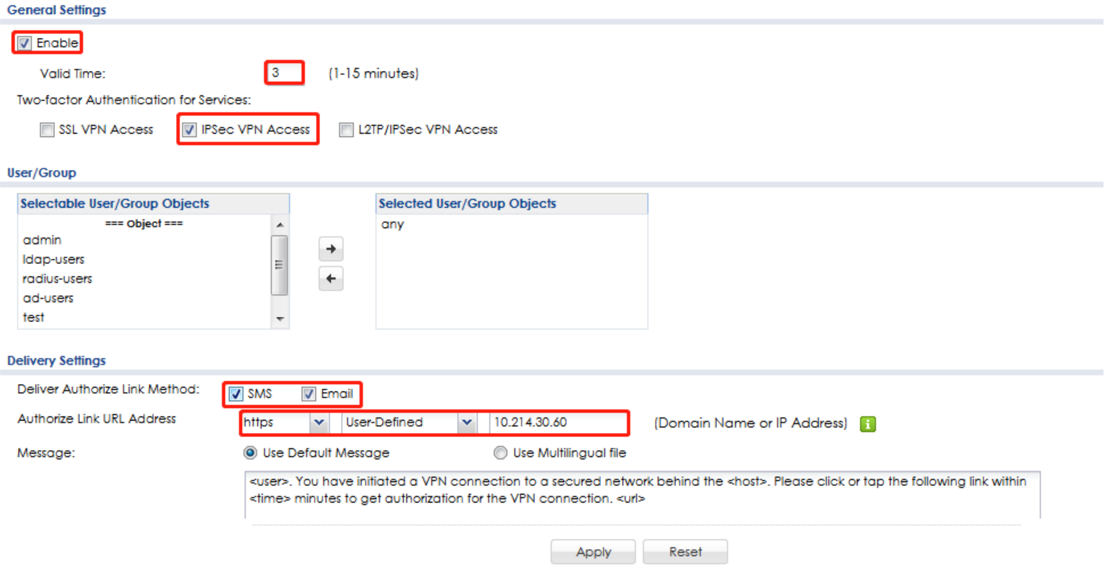
Password: ••••••••

Retype to Confirm: ••••••••

Set up authentication for 2 factor VPN connection

In the ZyWALL/USG, go to **CONFIGURATION > Object > Auth.Method > Two-factor Authentication.**

1. Select the check box **"Enable"** to enable 2 factor authentications.
2. Enter the maximum time (in minutes) that the user must click or tap the authorization link in the SMS or email in order to get authorization for the VPN connection.
3. Select which kinds of VPN tunnels require Two-Factor Authentication. in this scenario, we enable 2 factor authentication on IPSec VPN Access
4. This list displays the names of the users and user groups that can be selected for two-factor authentication.
5. Use this section to configure how to send an SMS or email for authorization. We select both methods in this scenario.
6. Configure the link that the user will receive in the SMS or email. The user must be able to access the link.
7. You can either create a default message in the text box or upload a message file (Use Multilingual file) from your computer.
8. Click **"Apply"** button to save your changes to the Zyxel Device.



General Settings

☑ Enable

Valid Time: 3 (1-15 minutes)

Two-factor Authentication for Services:

☐ SSL VPN Access ☑ IPSec VPN Access ☐ L2TP/IPSec VPN Access

User/Group

Selectable User/Group Objects	Selected User/Group Objects
=== Object ===	any
admin	
ldap-users	
radius-users	
ad-users	
test	

Delivery Settings

Deliver Authorize Link Method: ☑ SMS ☑ Email

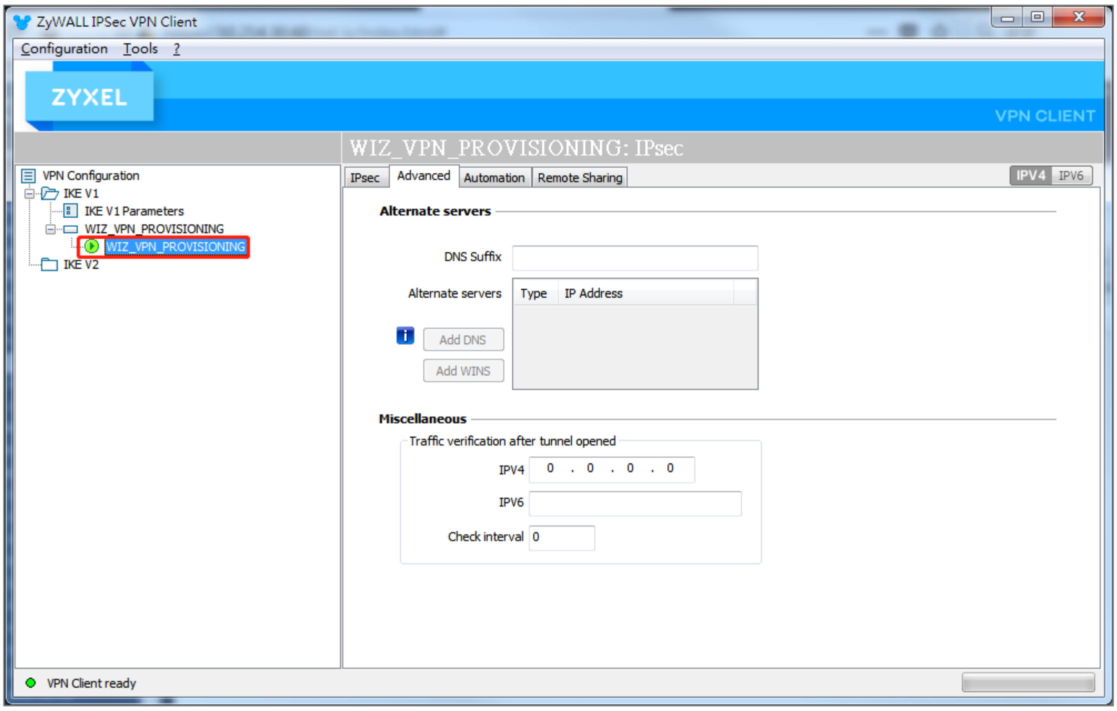
Authorize Link URL Address: https User-Defined 10.214.30.60 (Domain Name or IP Address)

Message: ● Use Default Message ○ Use Multilingual file

<user>. You have initiated a VPN connection to a secured network behind the <host>. Please click or tap the following link within <time> minutes to get authorization for the VPN connection. <url>

Test the Result

Go to **VPN Configuration > IKEv1**, right click the **WIZ_VPN_PROVISIONING** and select **Open tunnel**. You will see the **Tunnel opened** on ZyWALL IPSec VPN client



WIZ_VPN_PROVISIONING: IPsec

Alternate servers

DNS Suffix:

Alternate servers: Type | IP Address

Miscellaneous

Traffic verification after tunnel opened

IPV4 0 . 0 . 0 . 0

IPV6

Check interval 0

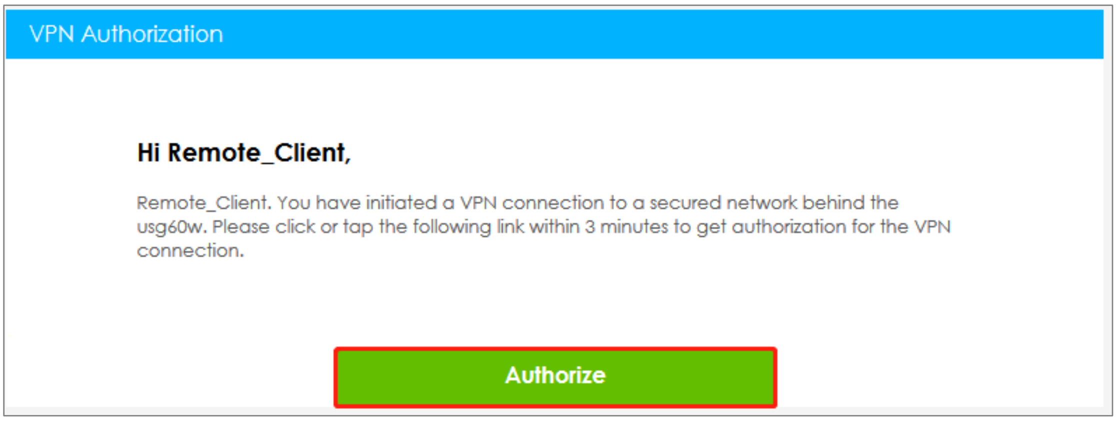
VPN Client ready

The VPN tunnel is created from the ZyWALL IPSec VPN client to the ZyWALL/USG, but we are still unable to access Intranet behind the ZyWALL/USG. The ZyWALL/USG send authorized link via phone number or email address in order to authenticate this user's use of the VPN tunnel (factor 2). If user does not click the link, then the Zyxel Device terminates the VPN connection. The client should access the authorization link sent via SMS or email by the Cloud SMS system within a specified deadline (Valid Time). If the authorization is correct and received on time, then the client can have VPN access to the secured network. If the authorization deadline has expired, then the client will have to run the VPN client again. If authorization credentials are incorrect or if the SMS/email was not received, then the client must check with the network administrator.

The following is authorized example by email and SMS

Authorized by email link

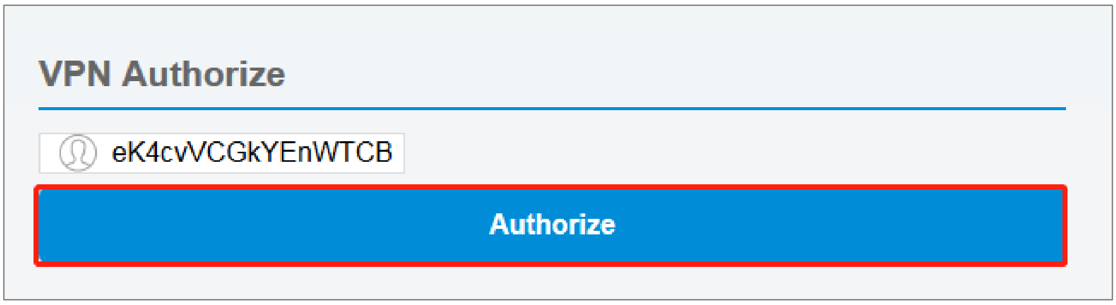
1. Received authorization mail with authorize link.



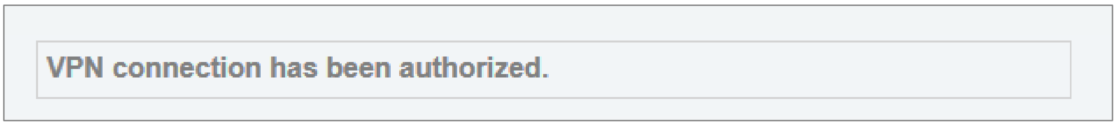
Hi Remote_Client,

Remote_Client. You have initiated a VPN connection to a secured network behind the usg60w. Please click or tap the following link within 3 minutes to get authorization for the VPN connection.

2. Click the **"Authorize" to** authorization.



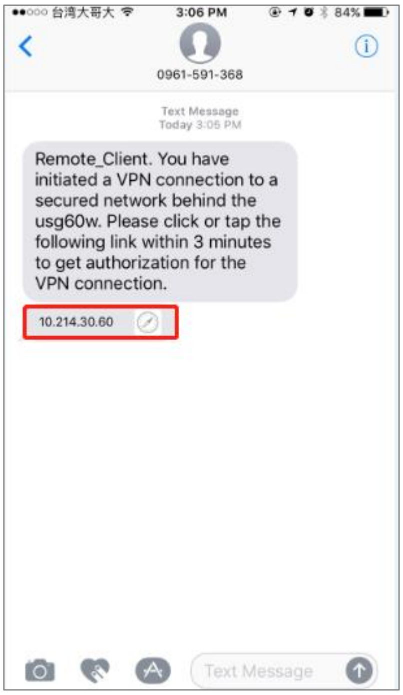
3. After we see "**VPN connection has been authorized**", we can access the secured network behind the ZyWALL/USG.



VPN connection has been authorized.

Authorized by SMS

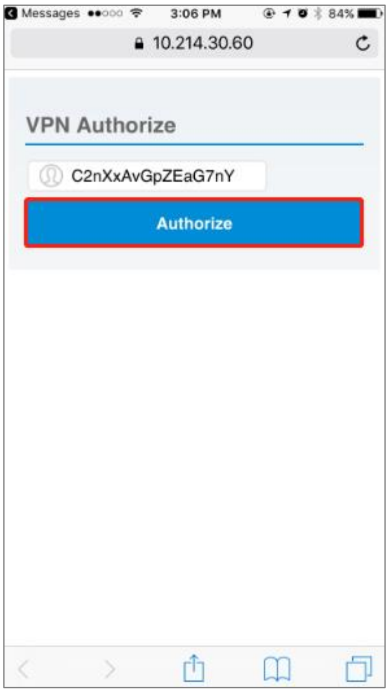
1. Received authorization SMS with authorize link.

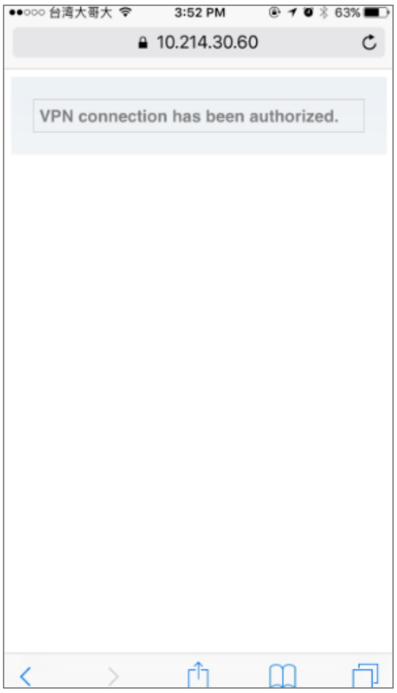


Remote_Client. You have initiated a VPN connection to a secured network behind the usg60w. Please click or tap the following link within 3 minutes to get authorization for the VPN connection.

10.214.30.60

2. Click the SMS link to authorized, after we see "VPN connection has been authorized", we can access the secured network behind the ZyWALL/USG.





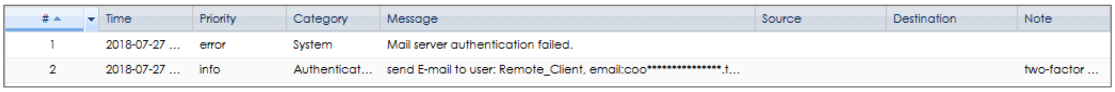
10.214.30.60

VPN connection has been authorized.

What could went wrong

If you see below log message "**Mail server authentication failed.**", please check "**CONFIGURATION > System > Notification > SMTP Server**", Make sure your password is correct for mail authentication

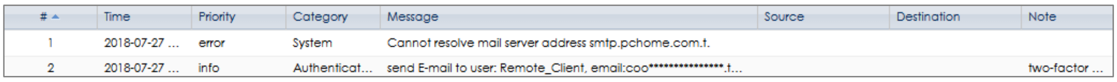
MONITOR > Log



#	Time	Priority	Category	Message	Source	Destination	Note
1	2018-07-27 ...	error	System	Mail server authentication failed.			
2	2018-07-27 ...	info	Authenticat...	send E-mail to user: Remote_Client, email:coo***************.t...			two-factor ...

If you see below log message "**Cannot resolve mail server address smtp.pchome.com.t**" please check "**CONFIGURATION > System > Notification > SMTP Server**", Make sure your service IP/hostname is correct for mail authentication.

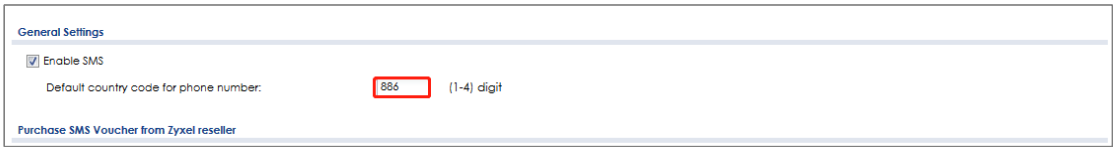
MONITOR > Log



#	Time	Priority	Category	Message	Source	Destination	Note
1	2018-07-27 ...	error	System	Cannot resolve mail server address smtp.pchome.com.t.			
2	2018-07-27 ...	info	Authenticat...	send E-mail to user: Remote_Client, email:coo***************.t...			two-factor ...

If you are unable to received SMS for authorization, please check "**CONFIGURATION > System > Notification > SMS**", confirm the country code is correct for SMS message

CONFIGURATION > System > Notification > SMS



General Settings

☑ Enable SMS

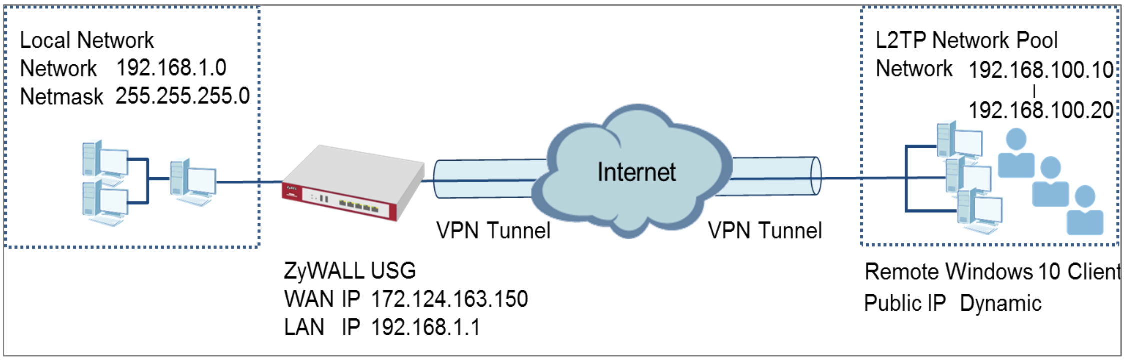
Default country code for phone number: 886 (1-4) digit

Purchase SMS Voucher from Zyxel reseller

How to Import ZyWALL/USG Certificate for L2TP over IPsec in Android mobile phone

This is an example of using the L2TP VPN and VPN client software included in Android mobile phone operating systems. When the VPN tunnel is configured, users can securely access the network behind the ZyWALL/USG and allow traffic from L2TP clients to go to the Internet from an Android mobile phone.

ZyWALL/USG L2TP VPN with Remote Android Mobile Phone Client Example

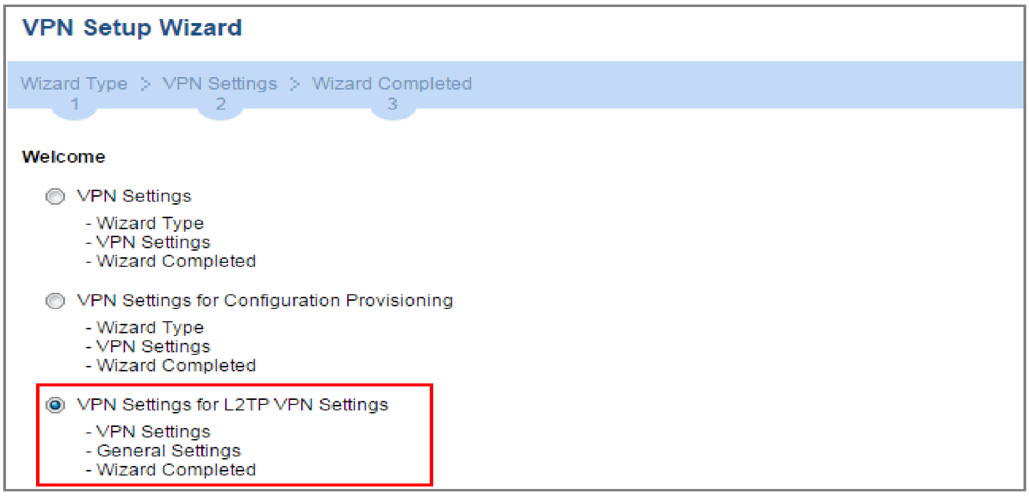


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and Android (Version: 10.0.10240)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the Android mobile phone clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

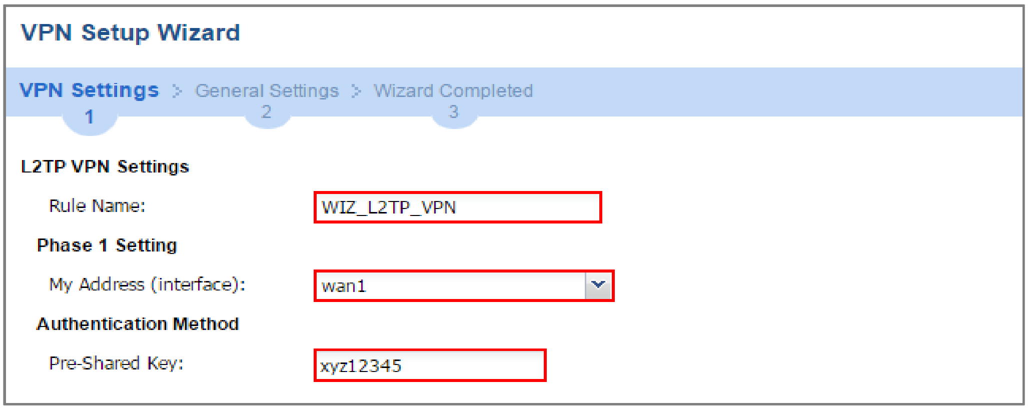
○ VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

● VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



VPN Setup Wizard

L2TP VPN Settings

Rule Name: WIZ_L2TP_VPN

Phase 1 Setting

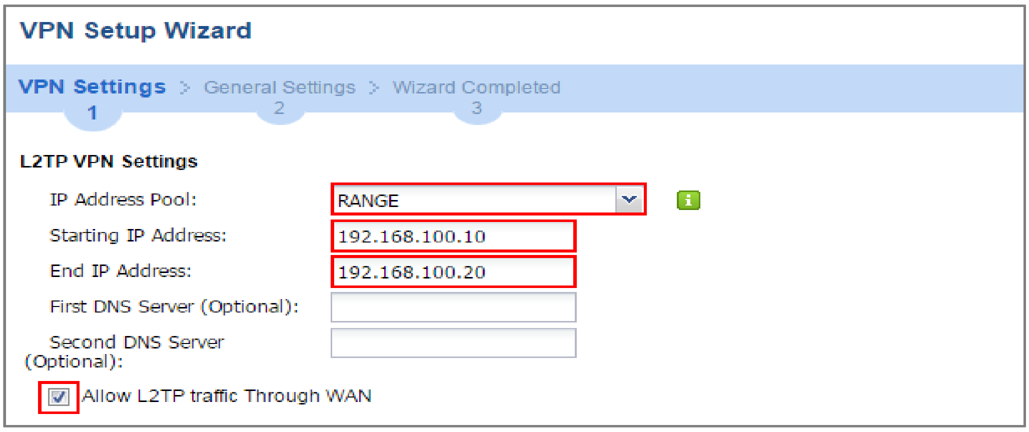
My Address (interface): wan1

Authentication Method

Pre-Shared Key: xyz12345

Assign the L2TP users' IP address range from 192.168.100.10 to 192.168.100.20 for use in the L2TP VPN tunnel and select **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)



VPN Setup Wizard

L2TP VPN Settings

IP Address Pool: RANGE

Starting IP Address: 192.168.100.10

End IP Address: 192.168.100.20

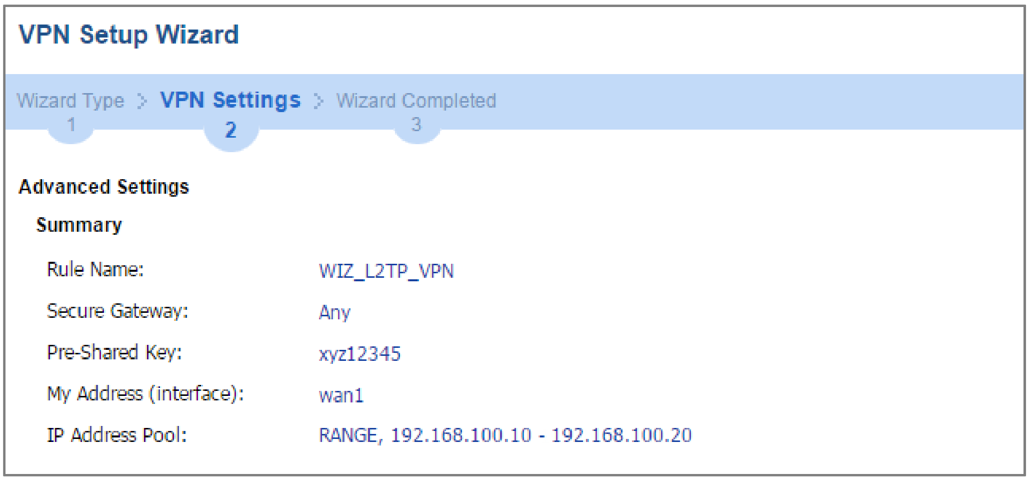
First DNS Server (Optional):

Second DNS Server (Optional):

☑ Allow L2TP traffic Through WAN

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)



VPN Setup Wizard

Advanced Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

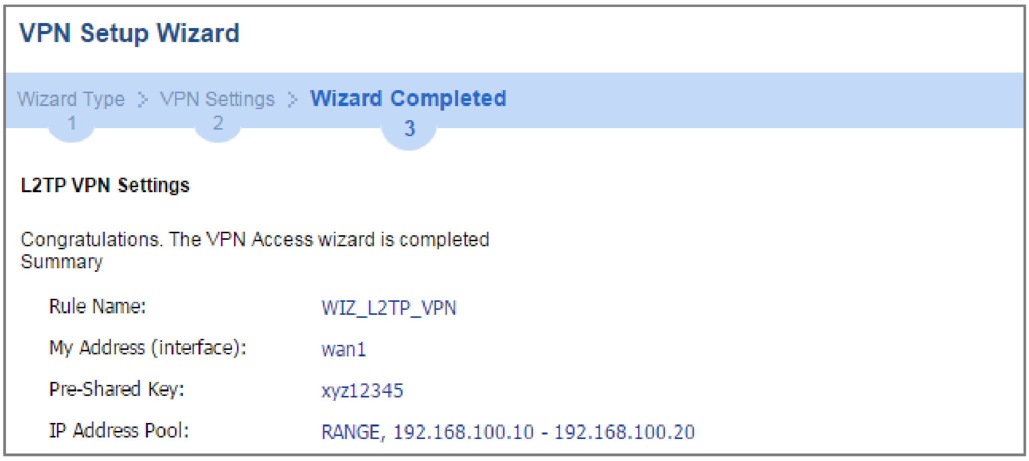
Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.100.10 - 192.168.100.20

Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Wizard Completed



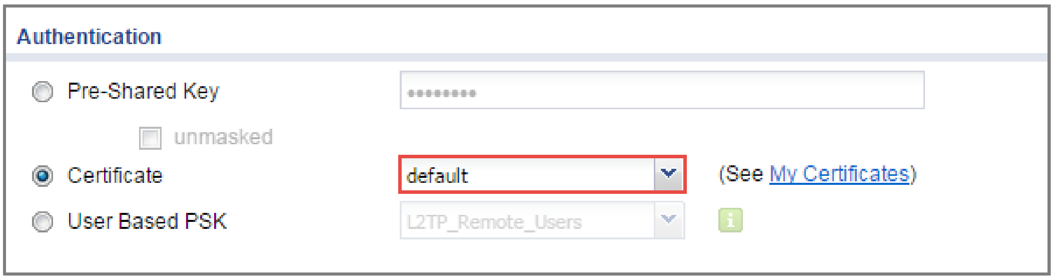
L2TP VPN Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name:	WIZ_L2TP_VPN
My Address (interface):	wan1
Pre-Shared Key:	xyz12345
IP Address Pool:	RANGE, 192.168.100.10 - 192.168.100.20

Go to **CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN,** change **Authentication** method to be **Certificate** and select the certificate which ZyWALL/USG uses to identify itself to the Android mobile phone.

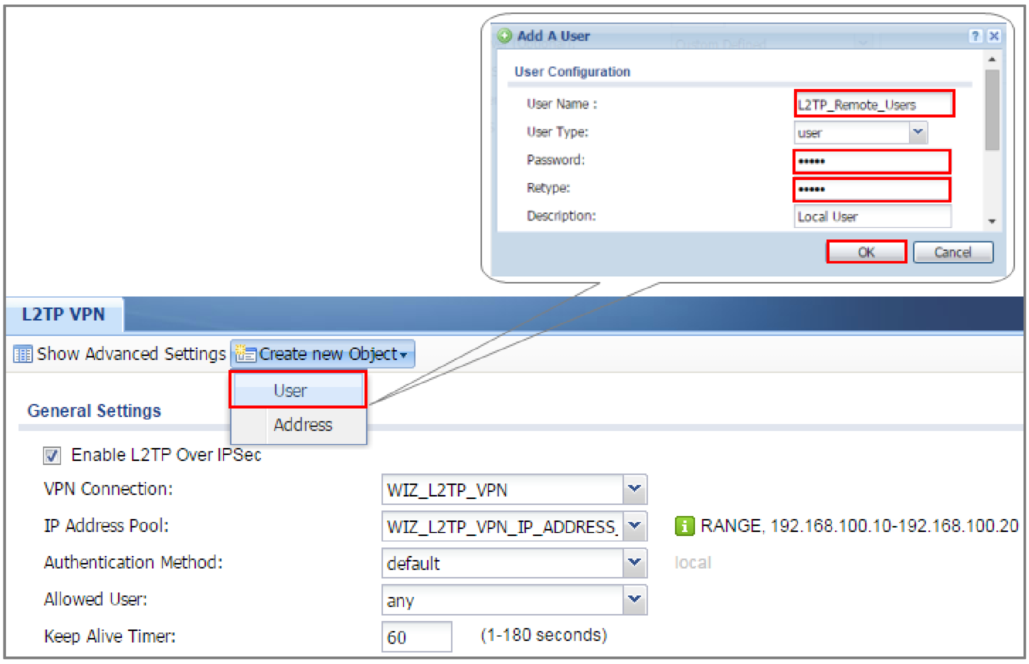
CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN > Authentication > Certificate


Authentication

○ Pre-Shared Key ••••••••
□ unmasked
● Certificate default (See My Certificates)
○ User Based PSK L2TP_Remote_Users

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User



Add A User

User Configuration

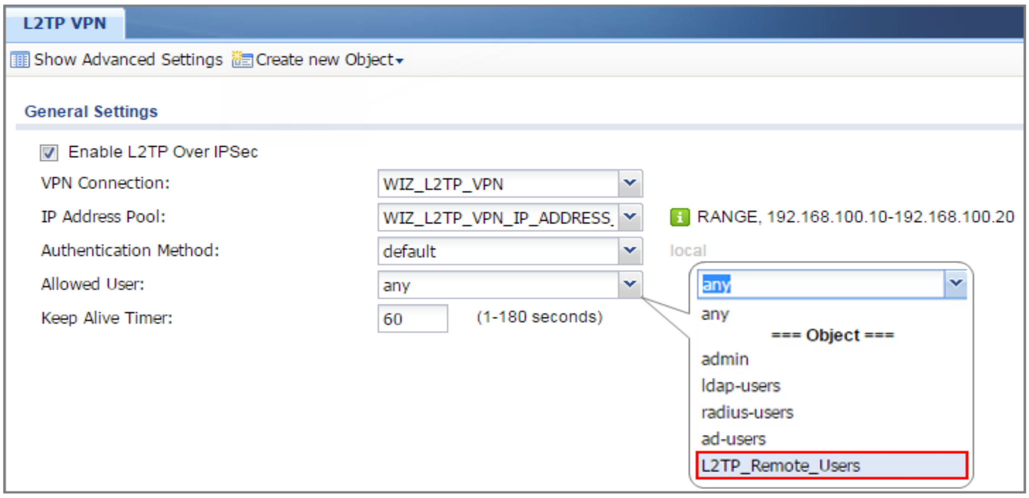
User Name :	L2TP_Remote_Users
User Type:	user
Password:	•••••
Retype:	•••••
Description:	Local User

L2TP VPN

General Settings

☑ Enable L2TP Over IPSec

VPN Connection:	WIZ_L2TP_VPN	
IP Address Pool:	WIZ_L2TP_VPN_IP_ADDRESS_	RANGE, 192.168.100.10-192.168.100.20
Authentication Method:	default	local
Allowed User:	any	
Keep Alive Timer:	60	(1-180 seconds)



L2TP VPN

General Settings

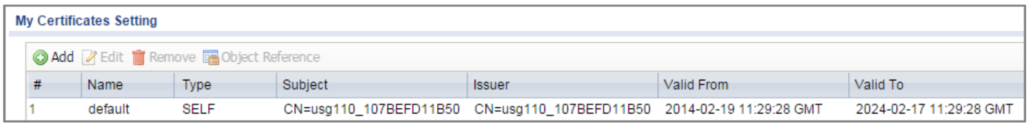
☑ Enable L2TP Over IPSec

VPN Connection:	WIZ_L2TP_VPN	
IP Address Pool:	WIZ_L2TP_VPN_IP_ADDRESS_	RANGE, 192.168.100.10-192.168.100.20
Authentication Method:	default	local
Allowed User:	any	
Keep Alive Timer:	60	(1-180 seconds)

Export a Certificate from ZyWALL/USG and Import it to Android Mobile Phone

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate**, select the certificate (**default** in this example) and click **Edit**.

CONFIGURATION > Object > Certificate > default

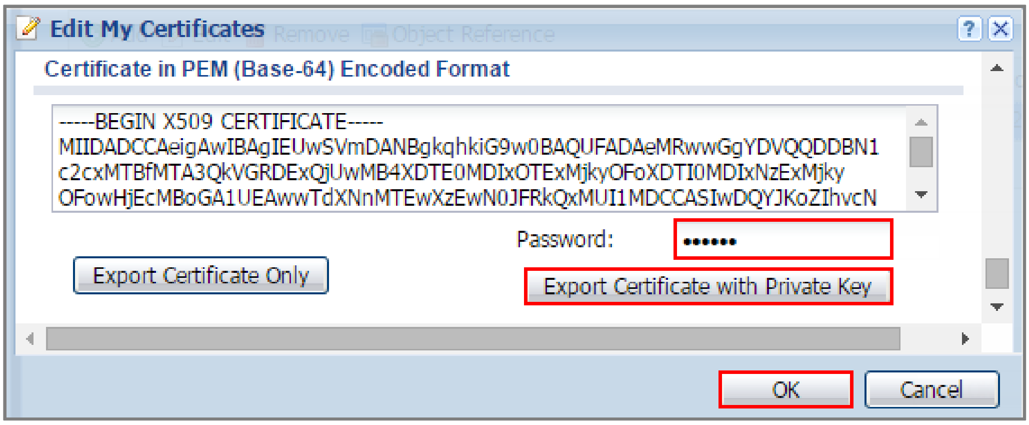


My Certificates Setting

#	Name	Type	Subject	Issuer	Valid From	Valid To
1	default	SELF	CN=usg110_107BEFD11B50	CN=usg110_107BEFD11B50	2014-02-19 11:29:28 GMT	2024-02-17 11:29:28 GMT

Export default certificate from ZyWALL/USG.

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only



Edit My Certificates

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN X509 CERTIFICATE-----
MIIDADCCAeigAwIBAgIEUwSVmDANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDDBN1
c2cxMTBfMTA3QkVGRDExQjUwMB4XDTE0MDIxOTExMjkyOFoXDTI0MDIxNzExMjky
OFowHjEcMBoGA1UEAwwTdXNnMTEwXzEwN0JFRkQxMUI1MDCCASIwDQYJKoZIhvcN
```

Password: ●●●●●●

Save **default** certificate as ***.crt** file to Android mobile phone computer.

Set Up the L2TP VPN Tunnel on the Android Mobile Device

1 To configure L2TP VPN in Android, go to Start > Settings > Network & Internet > VPN > Add a VPN Connection and configure as follows.

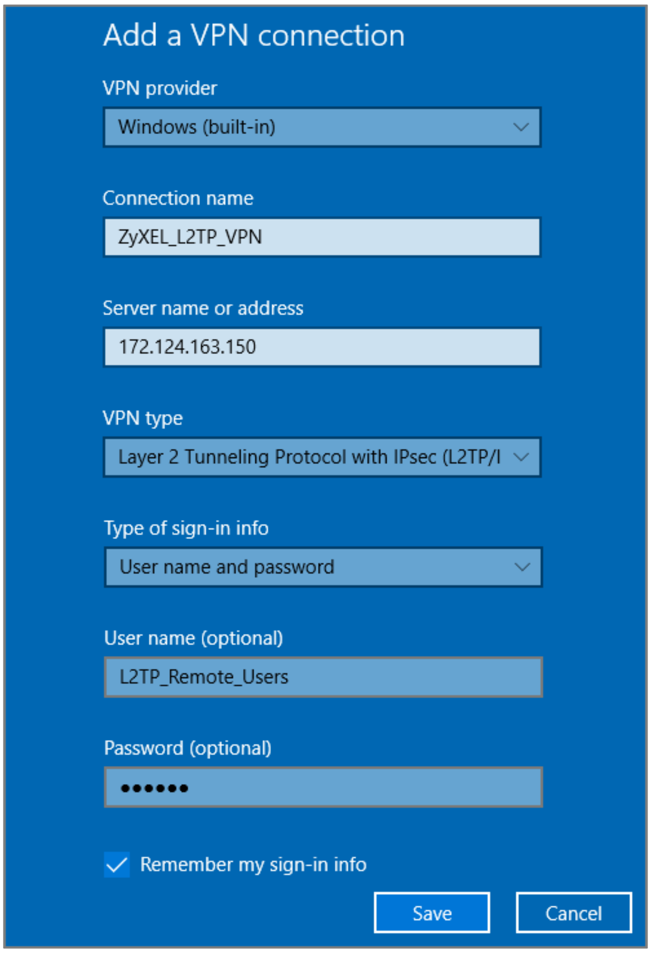
2 VPN Provider set to Windows (built-in).

3 Configure **Connection name** for you to identify the VPN configuration.

4 Set **Server** name or address to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).

5 Select VPN type to Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec).

6 Enter **User name** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).



Add a VPN connection

VPN provider: Windows (built-in)

Connection name: ZyXEL_L2TP_VPN

Server name or address: 172.124.163.150

VPN type: Layer 2 Tunneling Protocol with IPsec (L2TP/I

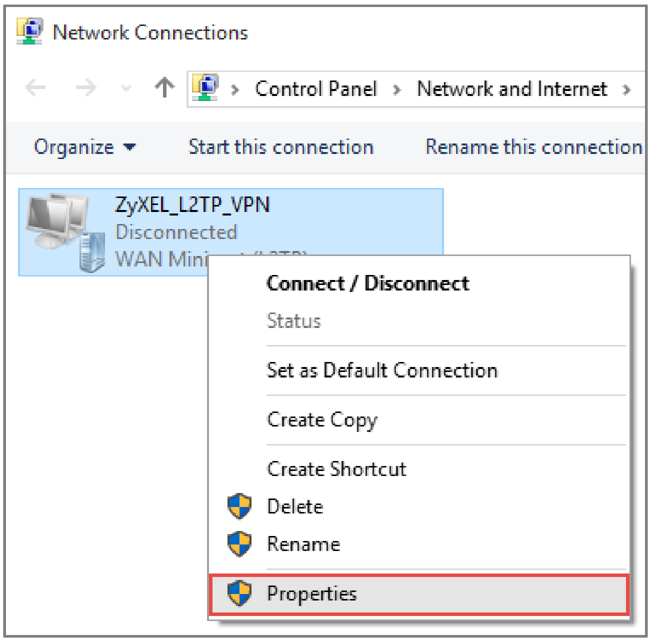
Type of sign-in info: User name and password

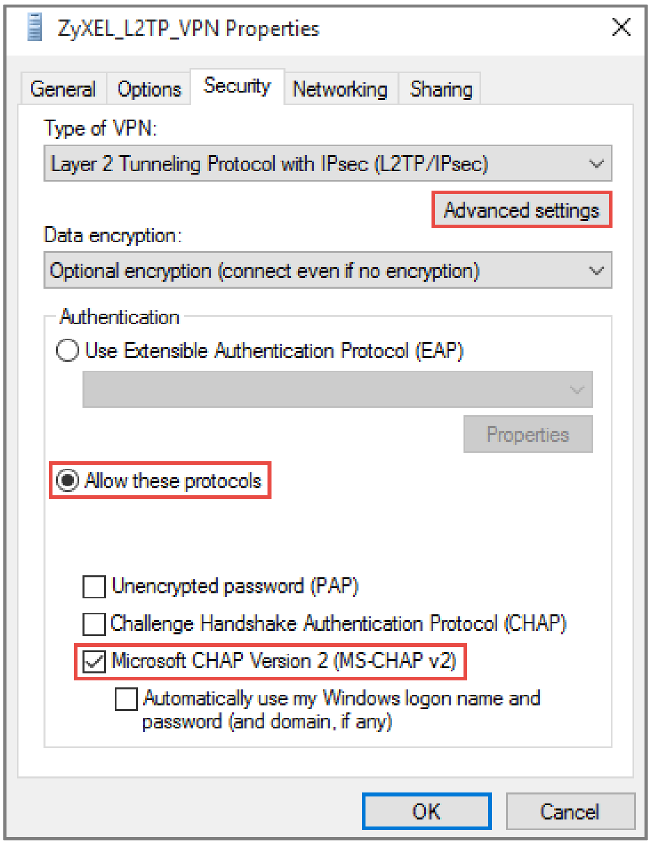
User name (optional): L2TP_Remote_Users

Password (optional): ••••••

☑ Remember my sign-in info

Go to **Control Panel > Network and Internet > Network Connections** and right click **Properties.** Continue to **Security > Advanced settings** and select **Use Certificate for authentication**.




ZyXEL_L2TP_VPN Properties

Type of VPN: Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)

Data encryption: Optional encryption (connect even if no encryption)

Authentication

○ Use Extensible Authentication Protocol (EAP)

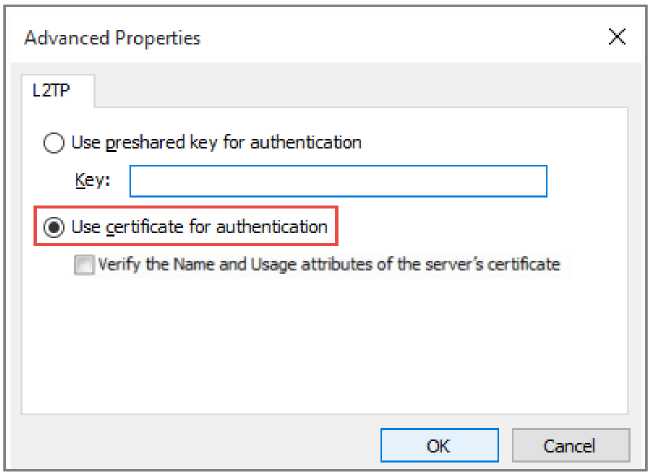
● Allow these protocols

□ Unencrypted password (PAP)

□ Challenge Handshake Authentication Protocol (CHAP)

☑ Microsoft CHAP Version 2 (MS-CHAP v2)

□ Automatically use my Windows logon name and password (and domain, if any)



Advanced Properties

L2TP

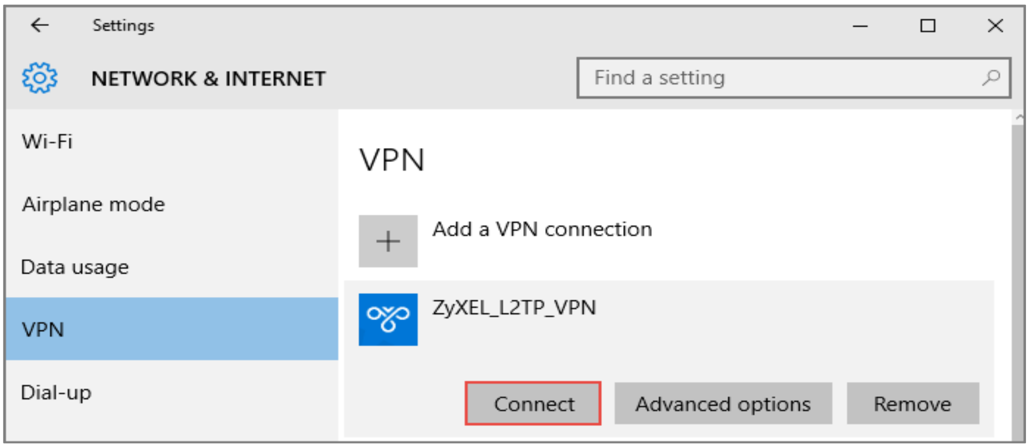
○ Use preshared key for authentication

Key:

● Use certificate for authentication

□ Verify the Name and Usage attributes of the server's certificate

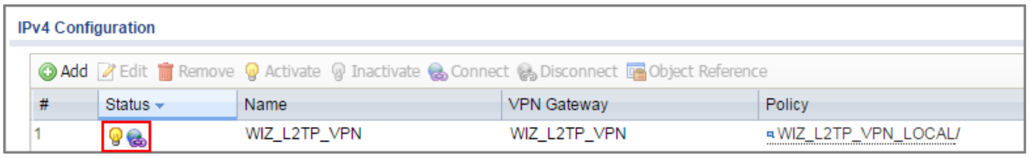
Go to **Network & Internet Settings** window, click **Connect**.



Test the L2TP over IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

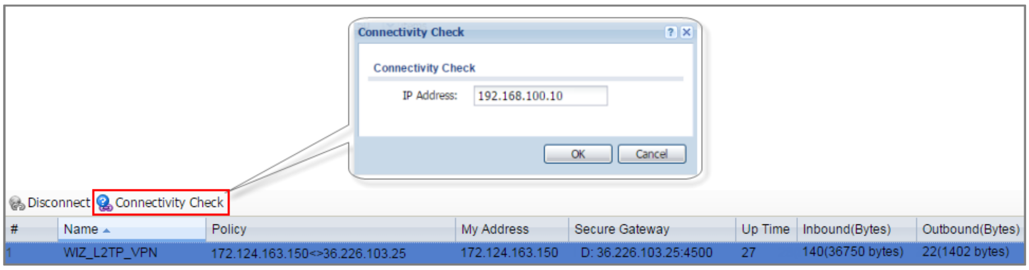


IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1	💡	WIZ_L2TP_VPN	WIZ_L2TP_VPN	WIZ_L2TP_VPN_LOCAL/

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN

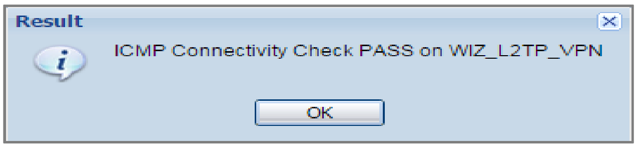


Connectivity Check

Connectivity Check

IP Address: 192.168.100.10

#	Name	Policy	My Address	Secure Gateway	Up Time	Inbound(Bytes)	Outbound(Bytes)
1	WIZ_L2TP_VPN	172.124.163.150<>36.226.103.25	172.124.163.150	D: 36.226.103.25:4500	27	140(36750 bytes)	22(1402 bytes)

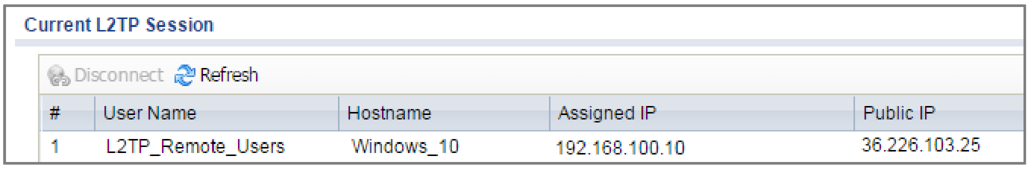


Result

ICMP Connectivity Check PASS on WIZ_L2TP_VPN

Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

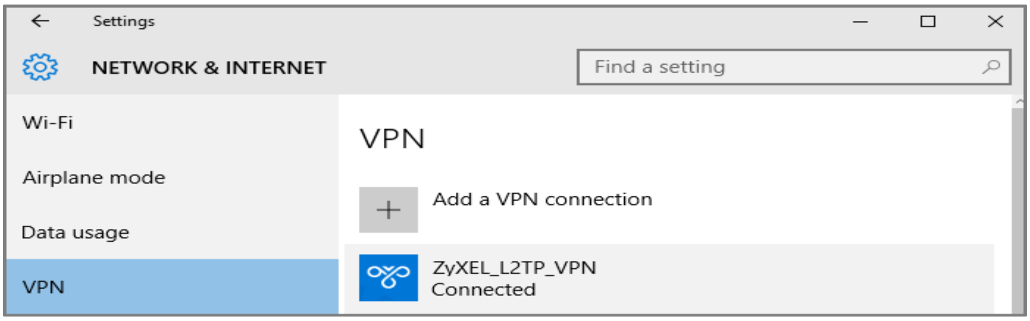


Current L2TP Session

#	User Name	Hostname	Assigned IP	Public IP
1	L2TP_Remote_Users	Windows_10	192.168.100.10	36.226.103.25

Go to Android **Start > Settings > Network & Internet > VPN** and show **Connected** status.

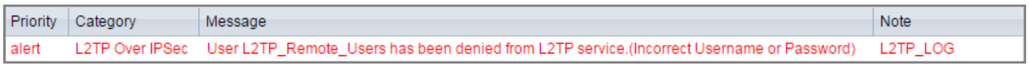
Menu > Settings > VPN > ZyXEL_L2TP



ZyXEL_L2TP_VPN
Connected

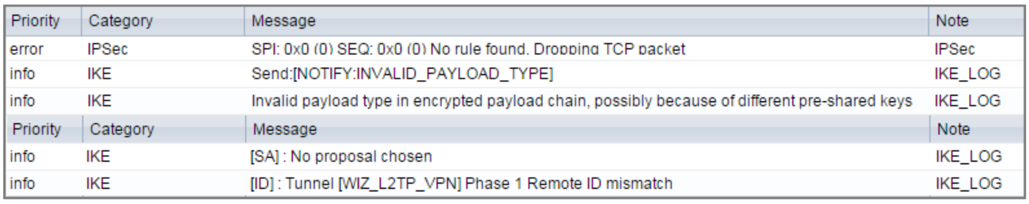
What Could Go Wrong?

7 If you see [alert] log message such as below, please check ZyWALL/USG L2TP Allowed User or User/Group Settings. Android users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.



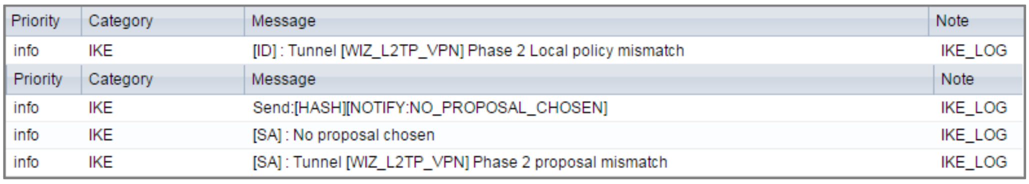
Priority	Category	Message	Note
alert	L2TP Over IPSec	User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password)	L2TP_LOG

8 If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. Android users must use the same Pre-Shared Key as configured in ZyWALL/USG to establish the IKE SA.



Priority	Category	Message	Note
error	IPSec	SPI: 0x0 (0) SEQ: 0x0 (0) No rule found. Dropping TCP packet	IPSec
info	IKE	Send:[NOTIFY:INVALID_PAYLOAD_TYPE]	IKE_LOG
info	IKE	Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys	IKE_LOG
Priority	Category	Message	Note
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 1 Remote ID mismatch	IKE_LOG

9 If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.



Priority	Category	Message	Note
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch	IKE_LOG
Priority	Category	Message	Note
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [WIZ_L2TP_VPN] Phase 2 proposal mismatch	IKE_LOG

10 Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

11 If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

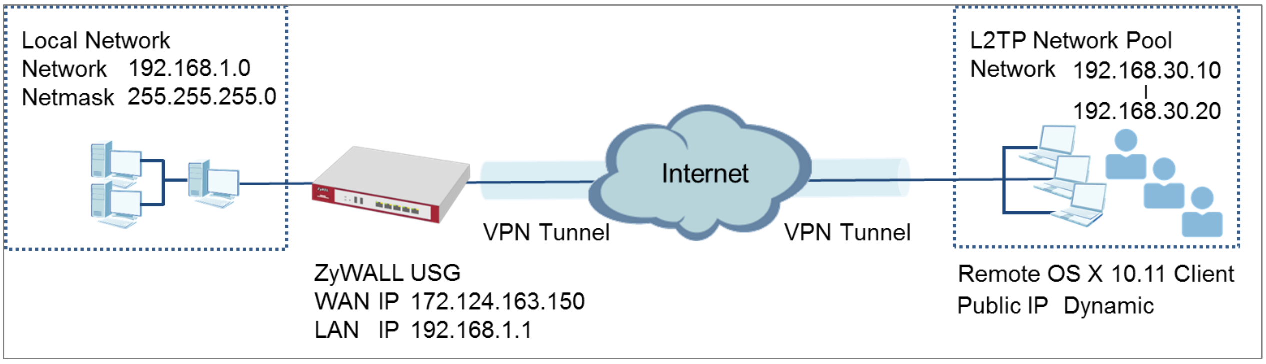
12 Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

13 Verify that the Zone is set correctly in the VPN Connection rule. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Configure the L2TP VPN with Apple MAC OS X 10.11 Operating System

This is an example of using the L2TP VPN and VPN client software included in Apple MAC OS X 10.11 El Capitan operating systems. When the VPN tunnel is configured, users can securely access the network behind the ZyWALL/USG and allow traffic from L2TP clients to go to the Internet from an Apple computer.

ZyWALL/USG L2TP VPN with Apple MAC OS X 10.11 El Capitan

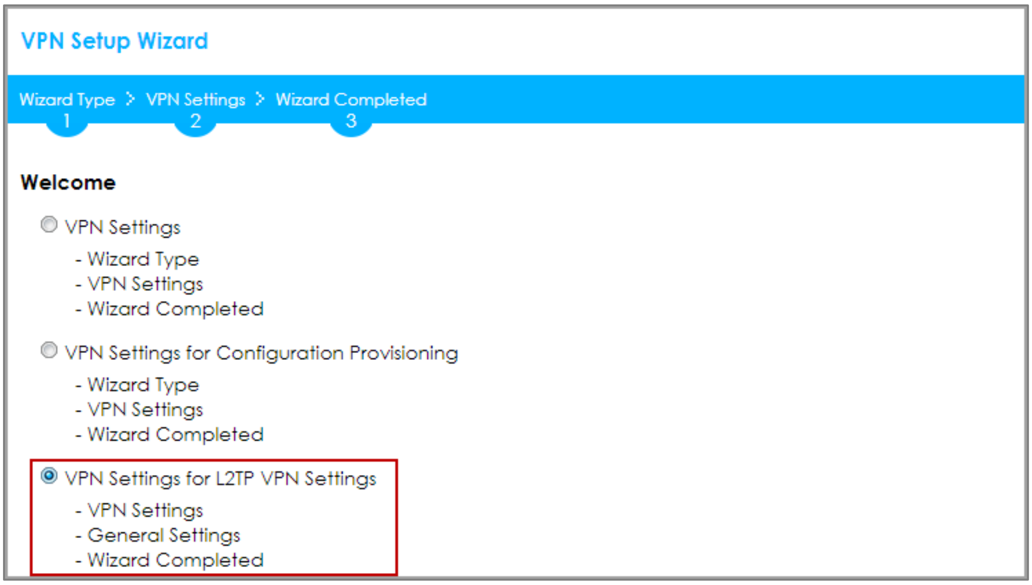


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and Apple MAC (Version: OS X10.11 El Capitan).

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the MAC OS X clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

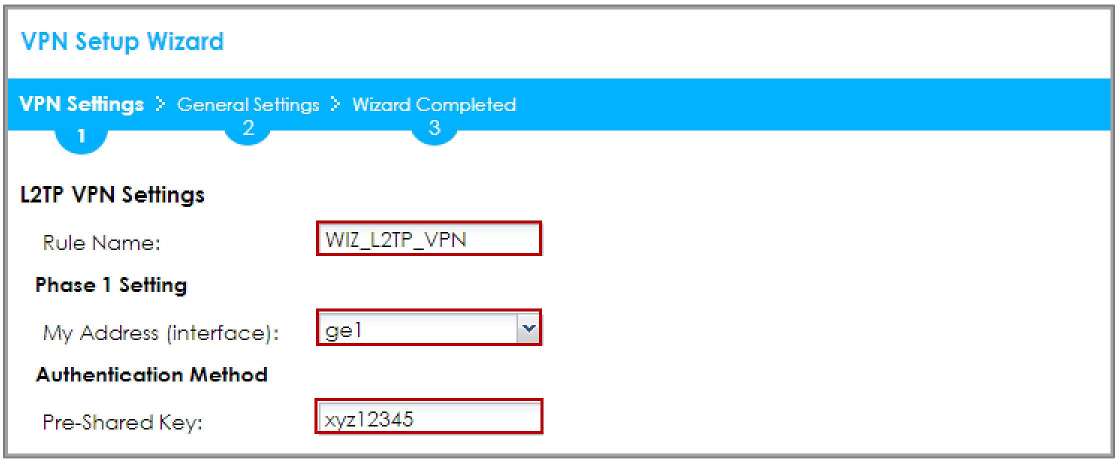
○ VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

● VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



VPN Setup Wizard

L2TP VPN Settings

Rule Name: WIZ_L2TP_VPN

Phase 1 Setting

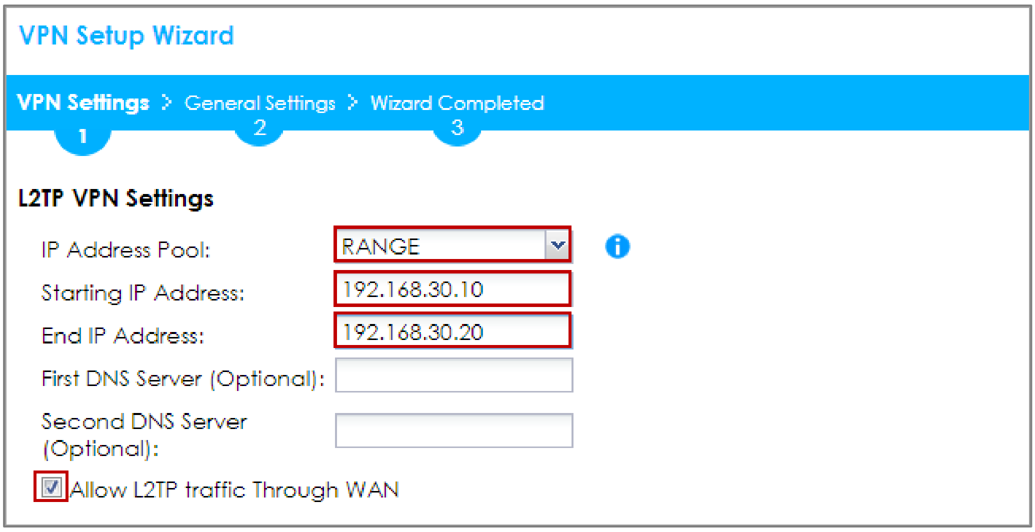
My Address (interface): ge1

Authentication Method

Pre-Shared Key: xyz12345

Configure the L2TP users' IP address range from 192.168.30.10 to 192.168.30.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN**. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



L2TP VPN Settings

IP Address Pool: RANGE

Starting IP Address: 192.168.30.10

End IP Address: 192.168.30.20

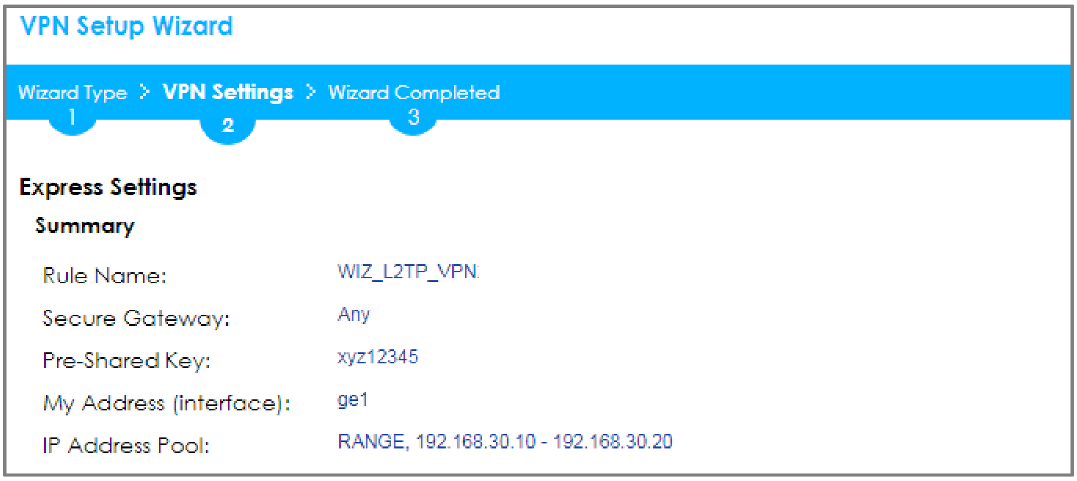
First DNS Server (Optional):

Second DNS Server (Optional):

☑ Allow L2TP traffic Through WAN

Continue to the next page to review your **Summary** and click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Summary



Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

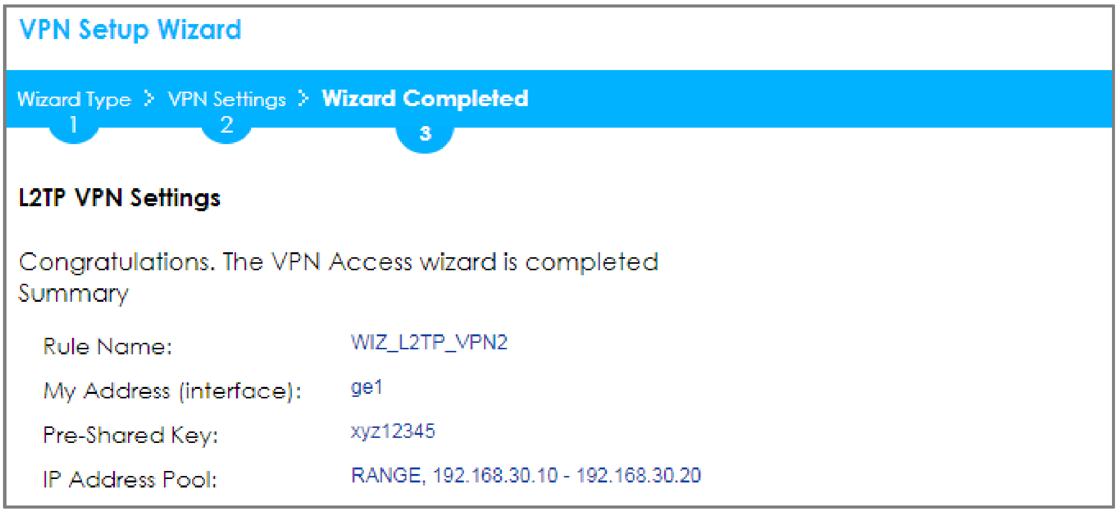
Secure Gateway: Any

Pre-Shared Key: xyz12345

My Address (interface): ge1

IP Address Pool: RANGE, 192.168.30.10 - 192.168.30.20

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Summary > Wizard Completed



L2TP VPN Settings

Congratulations. The VPN Access wizard is completed
Summary

Rule Name: WIZ_L2TP_VPN2

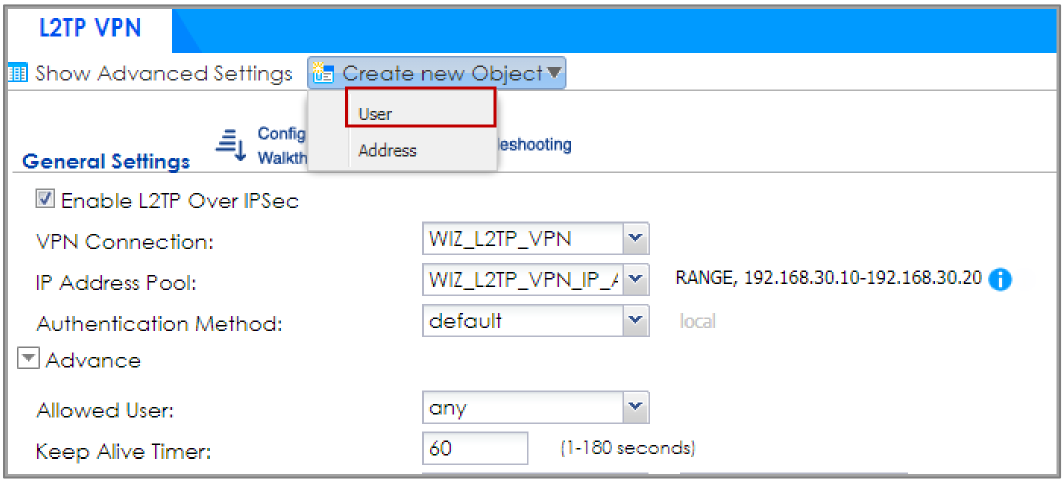
My Address (interface): ge1

Pre-Shared Key: xyz12345

IP Address Pool: RANGE, 192.168.30.10 - 192.168.30.20

Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User



L2TP VPN

Show Advanced Settings | Create new Object ▾

General Settings

☑ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

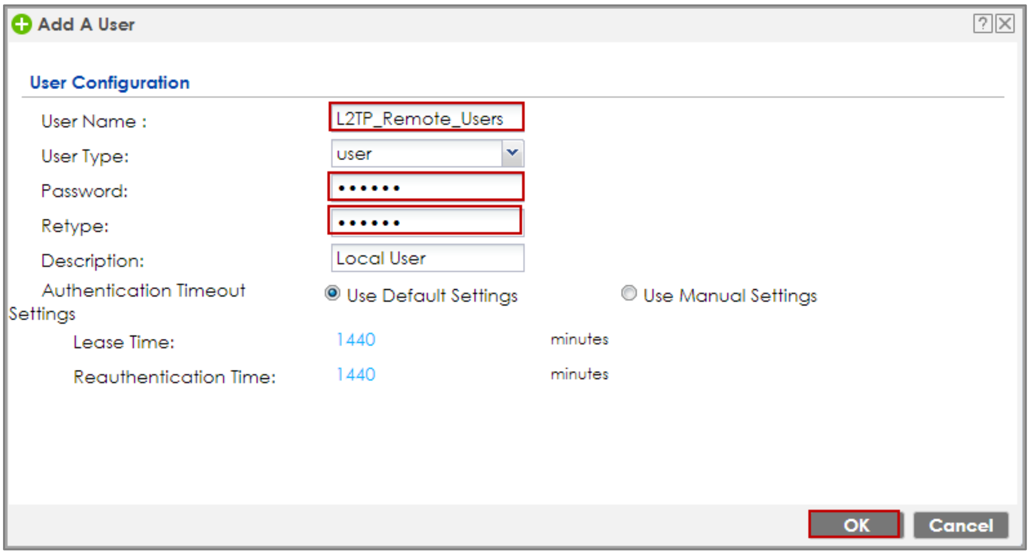
IP Address Pool: WIZ_L2TP_VPN_IP_A RANGE, 192.168.30.10-192.168.30.20

Authentication Method: default local

Advance

Allowed User: any

Keep Alive Timer: 60 (1-180 seconds)



Add A User

User Configuration

User Name : L2TP_Remote_Users

User Type: user

Password: ••••••

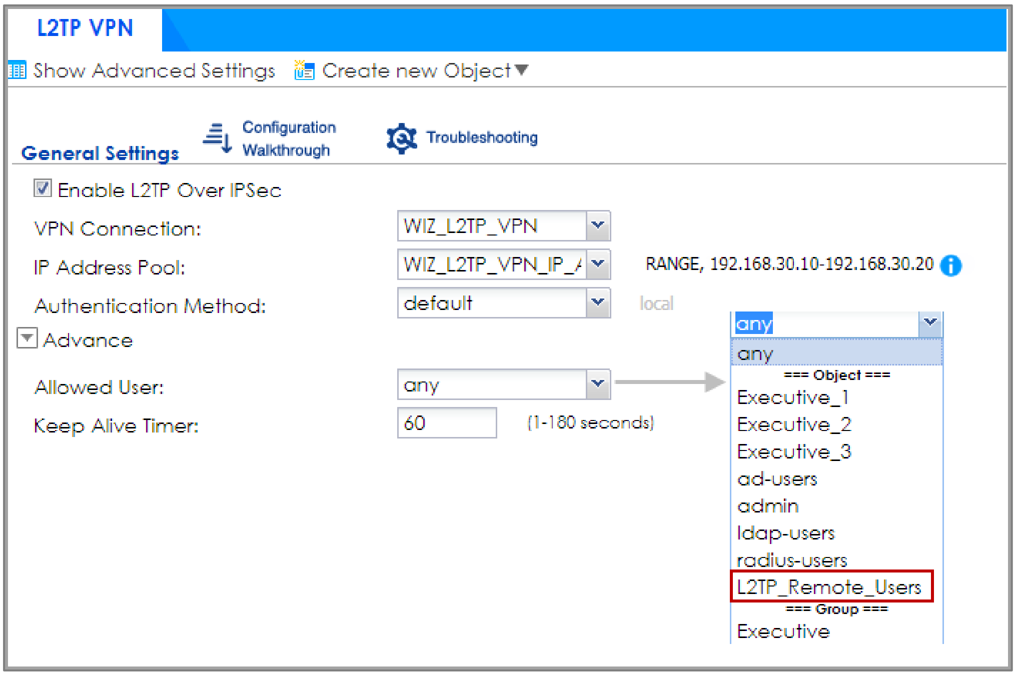
Retype: ••••••

Description: Local User

Authentication Timeout Settings ● Use Default Settings ○ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes



L2TP VPN

Show Advanced Settings | Create new Object▼

General Settings | Configuration Walkthrough | Troubleshooting

☑ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_/ RANGE, 192.168.30.10-192.168.30.20

Authentication Method: default local

Advance

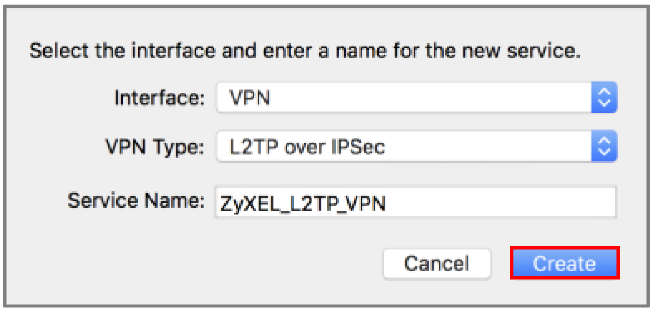
Allowed User: any

Keep Alive Timer: 60 (1-180 seconds)

Set Up the L2TP VPN Tunnel on the Apple MAC OS X 10.11 El Capitan Operating System

To configure L2TP VPN in OS X 10.11 operation system, go to **System Preferences… > Network,** click the "**+**" button at the bottom left of the connections to add a new connection and configure as follows.

Set the **Interface** to be **VPN**, select **VPN Type** to be **L2TP over IPSec**. Configure **Service Name** for you to identify the VPN configuration. Click **Create**.



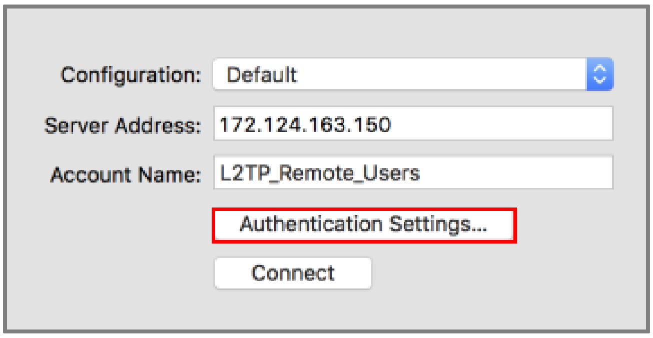
Select the interface and enter a name for the new service.

Interface: VPN

VPN Type: L2TP over IPSec

Service Name: ZyXEL_L2TP_VPN

Configure **Server Address** to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example). Enter **Account Name** which should be the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users in this example). Then, click **Authentication Settings…**.

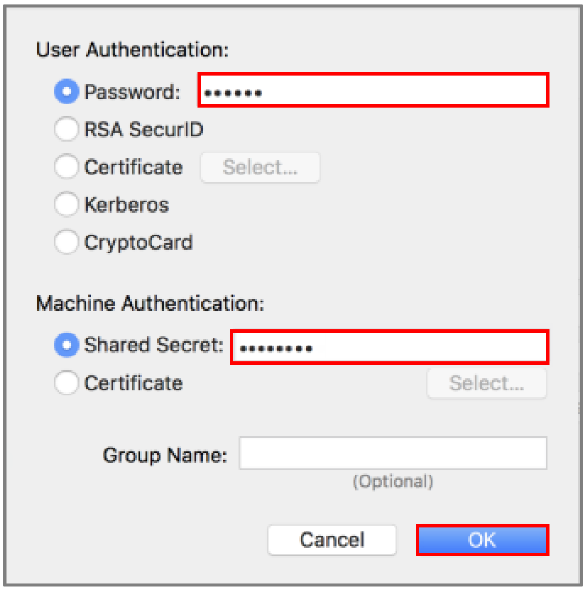

Configuration: Default

Server Address: 172.124.163.150

Account Name: L2TP_Remote_Users

In the **User Authentication** section, enter **Password** which should be the same as **Allowed User** created in ZyWALL/USG (zyx123 in this example).

In the **Machine Authentication** section, enter **Shared Secret** to be the pre-shared key of the IPSec VPN gateway the ZyWALL/USG uses for L2TP VPN over IPSec (zyx12345 in this example). Click **OK**.



User Authentication:

● Password: ••••••

○ RSA SecurID

○ Certificate Select...

○ Kerberos

○ CryptoCard

Machine Authentication:

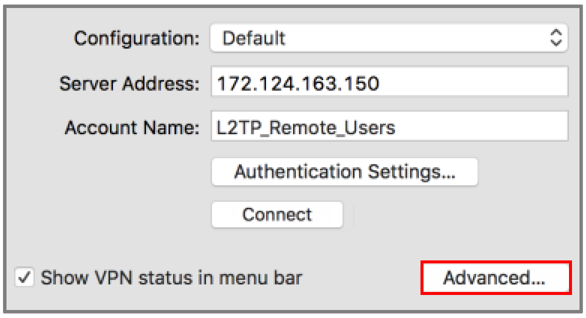
● Shared Secret: ••••••••

○ Certificate Select...

Group Name: (Optional)

Cancel OK

Go back to **Configuration** and click **Advanced…**. Select **Send all traffic over VPN connection** to allow the L2TP/IPSec VPN traffic between ZyWALL/USG and MAC OS X system.



Configuration: Default

Server Address: 172.124.163.150

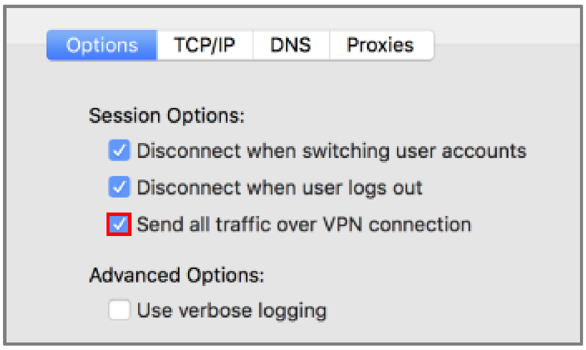
Account Name: L2TP_Remote_Users

Authentication Settings...

Connect

☑ Show VPN status in menu bar

Advanced...



Options TCP/IP DNS Proxies

Session Options:

☑ Disconnect when switching user accounts

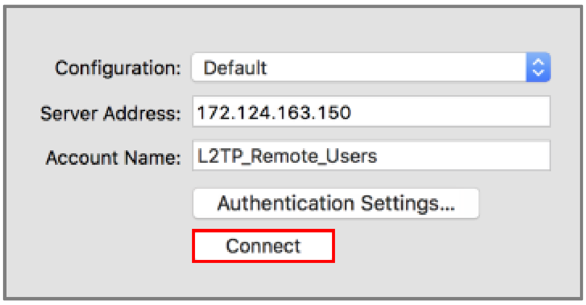
☑ Disconnect when user logs out

☑ Send all traffic over VPN connection

Advanced Options:

□ Use verbose logging

Go back to **Configuration** and click **Connect**.

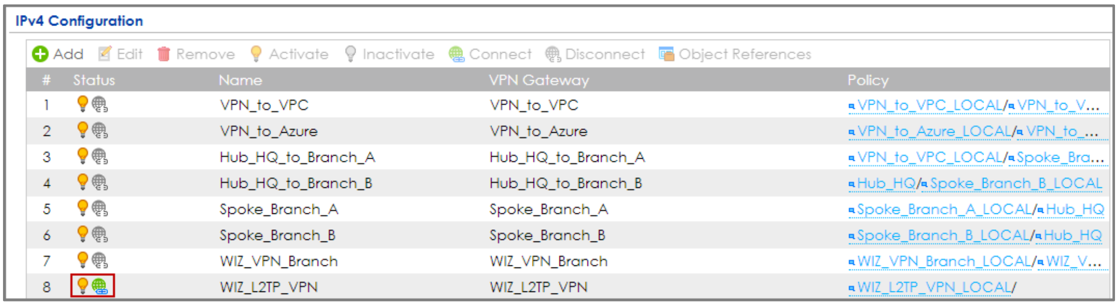


Configuration:	Default
Server Address:	172.124.163.150
Account Name:	L2TP_Remote_Users

Test the L2TP over IPSec VPN Tunnel

Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

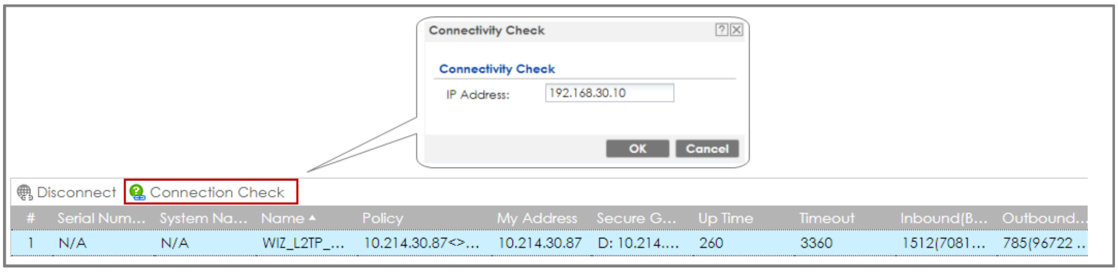


IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1		VPN_to_VPC	VPN_to_VPC	VPN_to_VPC_LOCAL/VPN_to_V...
2		VPN_to_Azure	VPN_to_Azure	VPN_to_Azure_LOCAL/VPN_to_...
3		Hub_HQ_to_Branch_A	Hub_HQ_to_Branch_A	VPN_to_VPC_LOCAL/Spoke_Bra...
4		Hub_HQ_to_Branch_B	Hub_HQ_to_Branch_B	Hub_HQ/Spoke_Branch_B_LOCAL
5		Spoke_Branch_A	Spoke_Branch_A	Spoke_Branch_A_LOCAL/Hub_HQ
6		Spoke_Branch_B	Spoke_Branch_B	Spoke_Branch_B_LOCAL/Hub_HQ
7		WIZ_VPN_Branch	WIZ_VPN_Branch	WIZ_VPN_Branch_LOCAL/WIZ_V...
8		WIZ_L2TP_VPN	WIZ_L2TP_VPN	WIZ_L2TP_VPN_LOCAL/

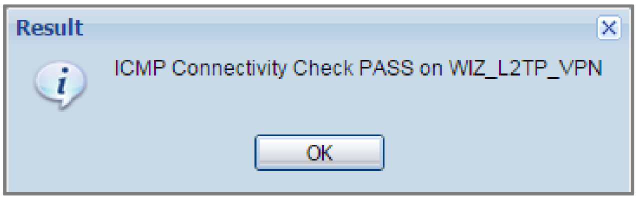
Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



IP Address: 192.168.30.10

#	Serial Num...	System Na...	Name ▲	Policy	My Address	Secure G...	Up Time	Timeout	Inbound(B...	Outbound...
1	N/A	N/A	WIZ_L2TP_...	10.214.30.87<>...	10.214.30.87	D: 10.214....	260	3360	1512(7081...	785(96722 ..

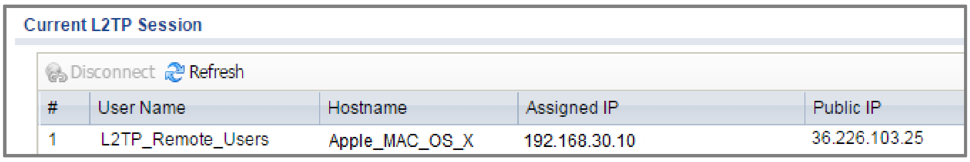


ICMP Connectivity Check PASS on WIZ_L2TP_VPN

功能有問題無法截圖, **connectivity check fail**

Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

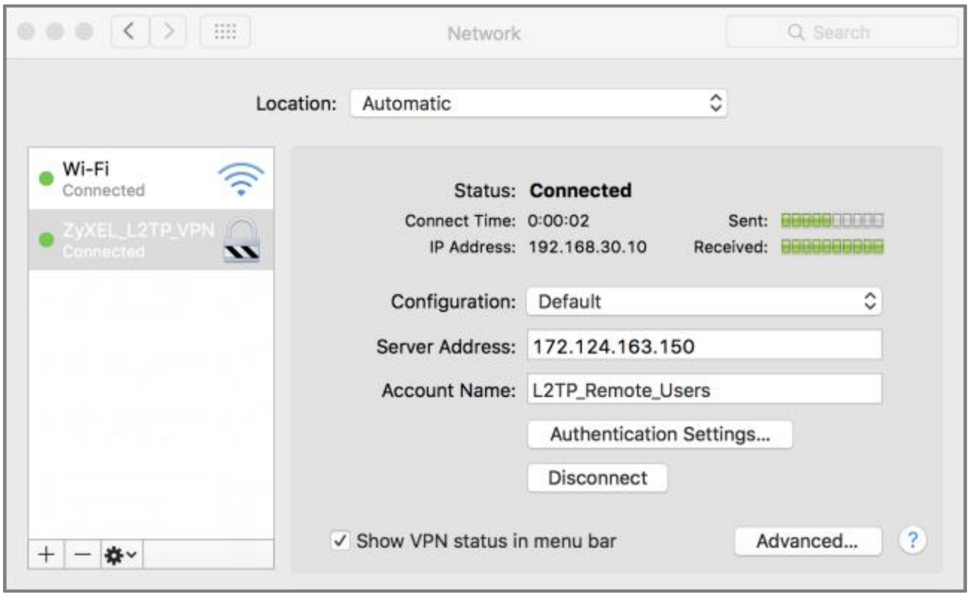
MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users



#	User Name	Hostname	Assigned IP	Public IP
1	L2TP_Remote_Users	Apple_MAC_OS_X	192.168.30.10	36.226.103.25

Go to MAC OS X **System Preferences… > Network** and show **Connected** status, **Connect Time** and assigned **IP Address**.

System Preferences… > Network



Location: Automatic

Wi-Fi Connected

ZyXEL_L2TP_VPN Connected

Status: **Connected**

Connect Time: 0:00:02

IP Address: 192.168.30.10

Configuration: Default

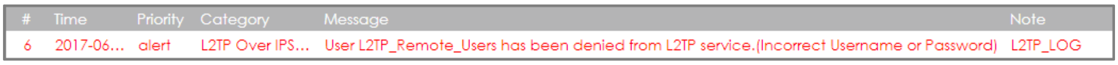
Server Address: 172.124.163.150

Account Name: L2TP_Remote_Users

☑ Show VPN status in menu bar

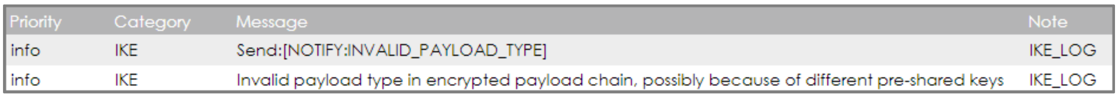
What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP **Allowed User** or **User/Group Settings**. Apple MAC OS X El Capitan operating system users must use the same **Username** and **Password** as configured in ZyWALL/USG to establish the L2TP VPN.

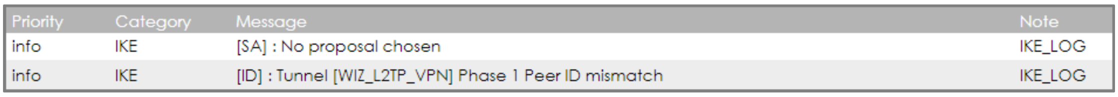


#	Time	Priority	Category	Message	Note
6	2017-06...	alert	L2TP Over IPS...	User L2TP_Remote_Users has been denied from L2TP service.(Incorrect Username or Password)	L2TP_LOG

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. Apple MAC OS X El Capitan operating system users must use the same **Pre-Shared Key** as configured in ZyWALL/USG to establish the IKE SA.

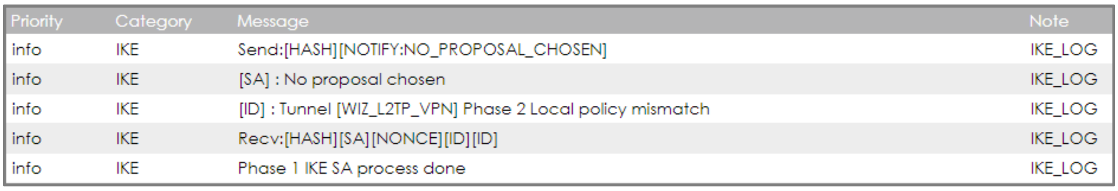


Priority	Category	Message	Note
info	IKE	Send:[NOTIFY:INVALID_PAYLOAD_TYPE]	IKE_LOG
info	IKE	Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys	IKE_LOG

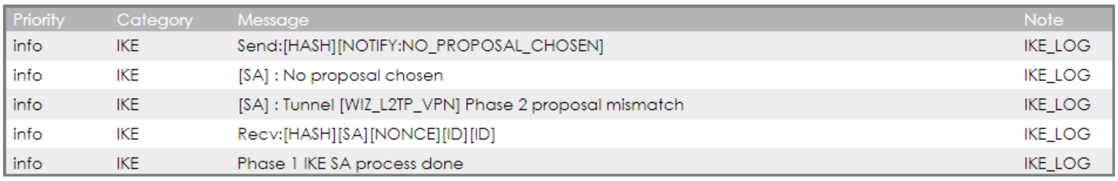


Priority	Category	Message	Note
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 1 Peer ID mismatch	IKE_LOG

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.



Priority	Category	Message	Note
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Phase 1 IKE SA process done	IKE_LOG



Priority	Category	Message	Note
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [WIZ_L2TP_VPN] Phase 2 proposal mismatch	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Phase 1 IKE SA process done	IKE_LOG

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

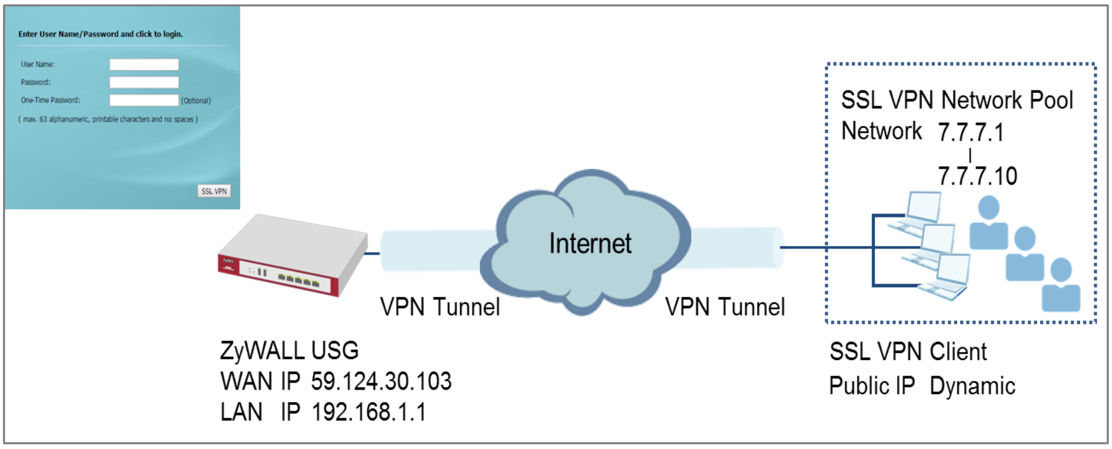
If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Verify that the Zone is set correctly in the Zone object. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to configure if I want user can only see SSL VPN Login button in web portal login page

This example shows how to strict portal access for SSL VPN clients. The example instructs how to allow end users to only see the SSL VPN Login button in the web portal login screen and the administrator can only manage the device from LAN.



ZyWALL/USG only see SSL VPN Login button in web portal login page

Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG60 (Firmware Version: ZLD 4.25).

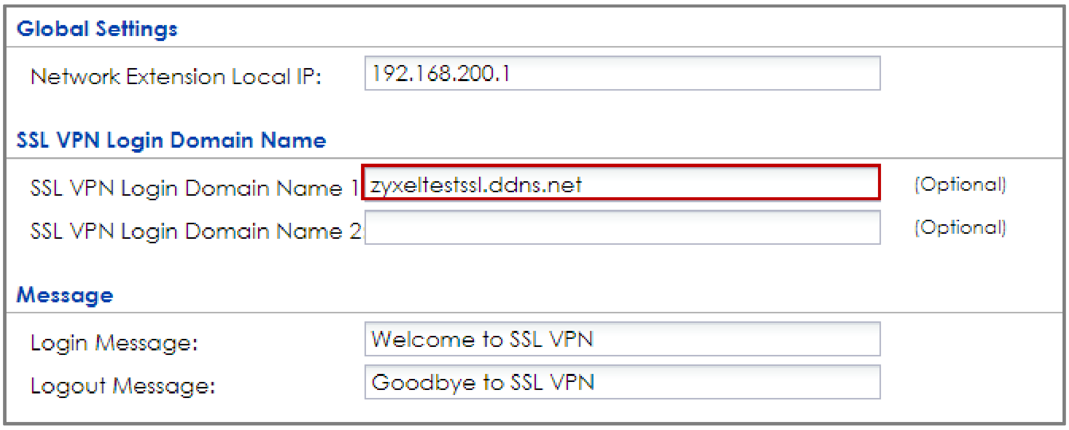
Set Up the DNS Service

In this scenario, you need to have a DNS host to fulfill the requirement. In this example, go to https://www.noip.com/ to register an account and create a DNS host. The following mapping IP address is the public IP of the ZyWALL/USG's WAN IP address.

Set Up the ZyWALL/USG SSL VPN Setting

In the ZyWALL/USG, go to **CONFIGURATION > VPN > SSL VPN > Global Setting > SSL VPN Login Domain Name** and type in the DNS domain name.

CONFIGURATION > VPN > SSL VPN > Global Setting > SSL VPN Login Domain Name



Global Settings

Network Extension Local IP: 192.168.200.1

SSL VPN Login Domain Name

SSL VPN Login Domain Name 1: zyxeltestssl.ddns.net (Optional)

SSL VPN Login Domain Name 2: (Optional)

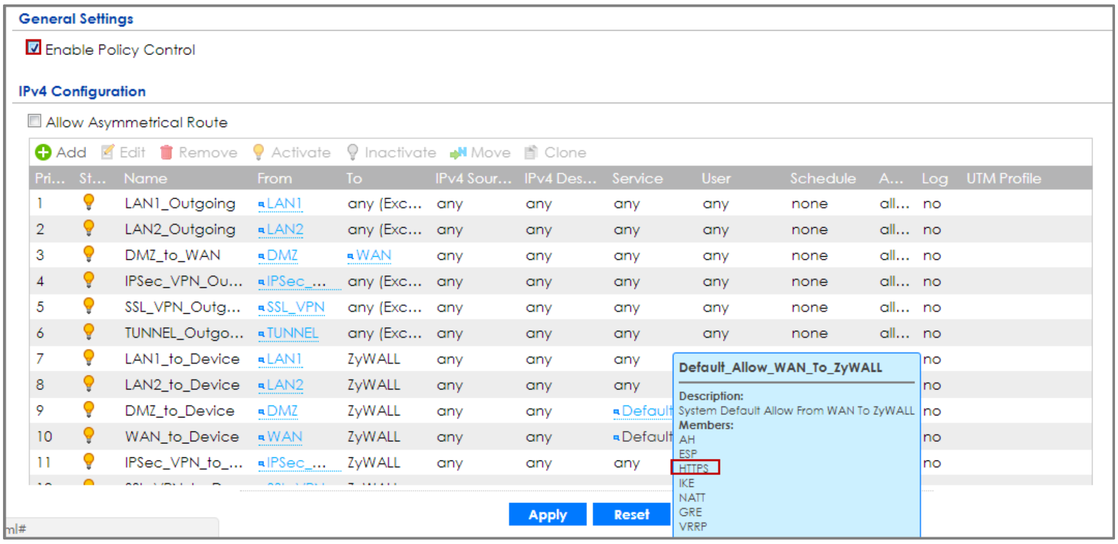
Message

Login Message: Welcome to SSL VPN

Logout Message: Goodbye to SSL VPN

Use SSL VPN, you need to allow users to access the **HTTPS** service. Go to **CONFIGURATION > Security Policy > Policy Control**. Make sure the security policy allows **HTTPS** traffic from the **WAN** interface to the **ZyWALL** (the example shows the default settings).

CONFIGURATION > Security Policy > Policy Control



General Settings

☑ Enable Policy Control

IPv4 Configuration

☐ Allow Asymmetrical Route

Pri...	St...	Name	From	To	IPv4 Sour...	IPv4 Des...	Service	User	Schedule	A...	Log	UTM Profile
1		LAN1_Outgoing	LAN1	any (Exc...	any	any	any	any	none	all...	no	
2		LAN2_Outgoing	LAN2	any (Exc...	any	any	any	any	none	all...	no	
3		DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	all...	no	
4		IPSec_VPN_Ou...	IPSec_...	any (Exc...	any	any	any	any	none	all...	no	
5		SSL_VPN_Outg...	SSL_VPN	any (Exc...	any	any	any	any	none	all...	no	
6		TUNNEL_Outgo...	TUNNEL	any (Exc...	any	any	any	any	none	all...	no	
7		LAN1_to_Device	LAN1	ZyWALL	any	any	any				no	
8		LAN2_to_Device	LAN2	ZyWALL	any	any	any				no	
9		DMZ_to_Device	DMZ	ZyWALL	any	any	Default				no	
10		WAN_to_Device	WAN	ZyWALL	any	any	Default				no	
11		IPSec_VPN_to_...	IPSec_...	ZyWALL	any	any	any				no	

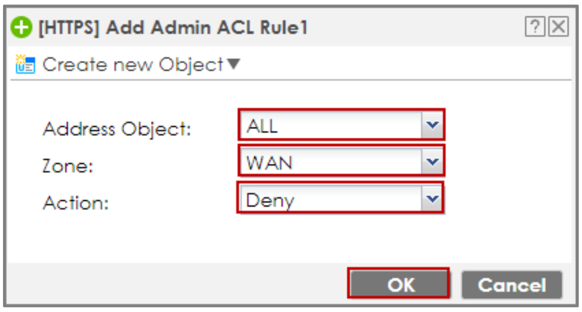
Default_Allow_WAN_To_ZyWALL

Description:
System Default Allow From WAN To ZyWALL
Members:
AH
ESP
HTTPS
IKE
NATT
GRE
VRRP

Set Up the ZyWALL/USG System Setting

Go to **CONFIGURATION > System > WWW > Admin Service Control > Add Admin ACL Rule 1.** Set the address access action as **Deny** for **ALL** address in **WAN**.

CONFIGURATION > System > WWW > Admin Service Control > Add Admin ACL Rule 1

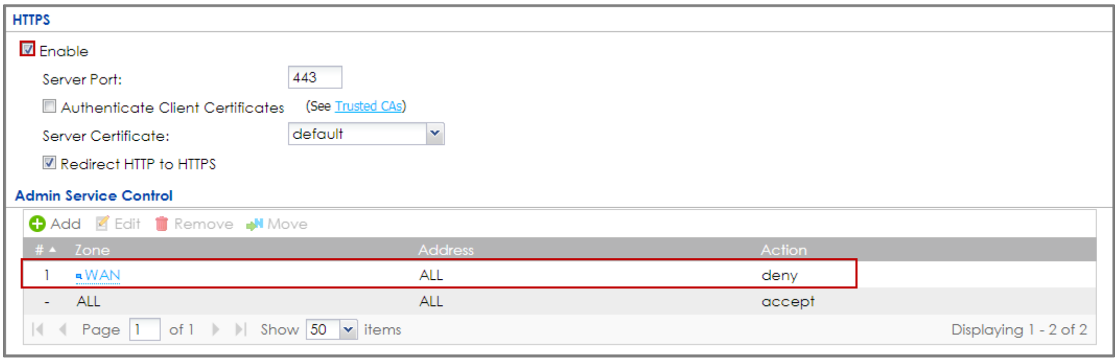


[HTTPS] Add Admin ACL Rule1

Address Object: ALL

Zone: WAN

Action: Deny



HTTPS

☑ Enable

Server Port: 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate: default

☑ Redirect HTTP to HTTPS

Admin Service Control

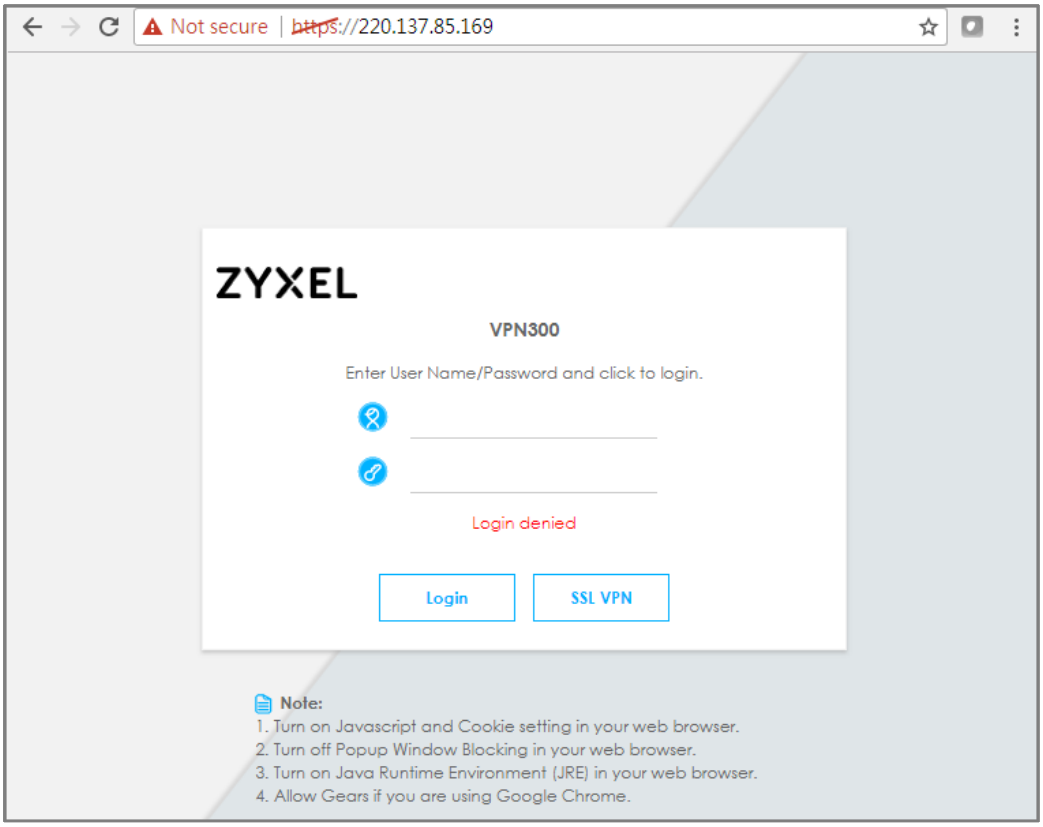
# ▲	Zone	Address	Action
1	WAN	ALL	deny
-	ALL	ALL	accept

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

Test the SSL VPN

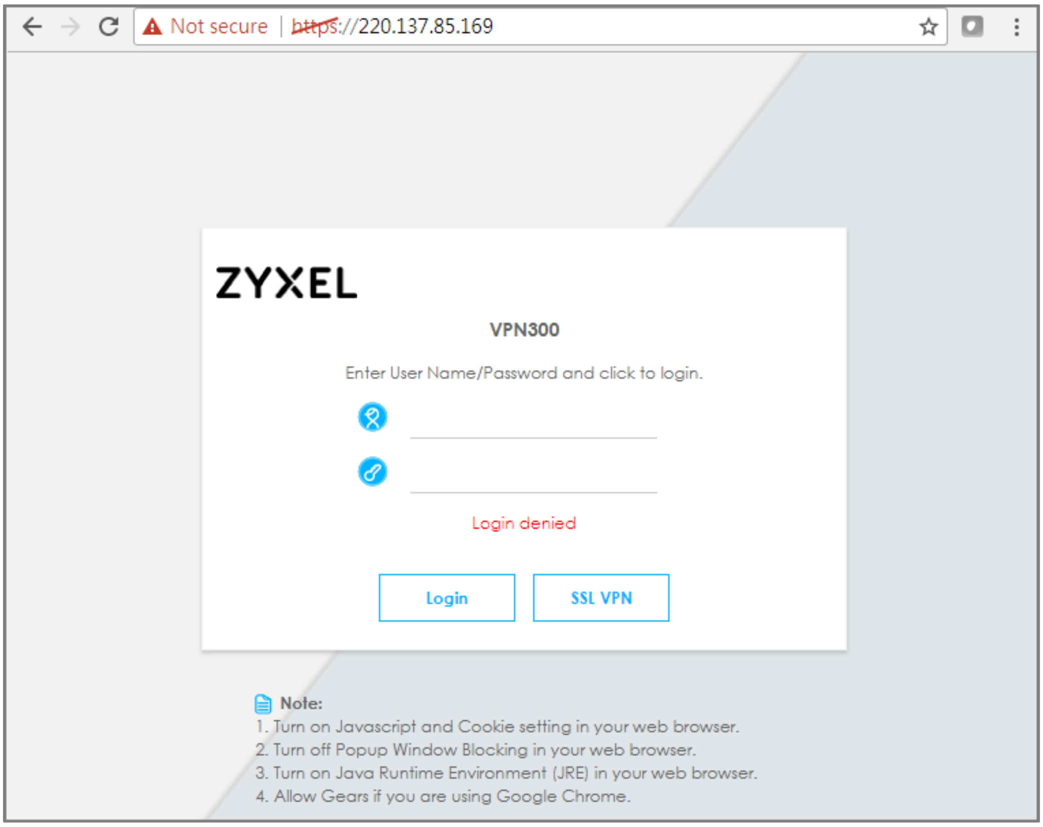
Type in the URL (https://sslvpnzyxeltest.ddns.net) and you will only see the **SSL VPN Login** button in the web portal screen.

Type in the URL (https://sslvpnzyxeltest.ddns.net)


Not secure | ~~https~~://220.137.85.169
ZYXEL
VPN300
Enter User Name/Password and click to login.
Login denied
Login
SSL VPN
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.

Login to the device via the WAN interface with the administrator's user name and password. The screen will show **Login denied**.

Login to the device via the WAN interface

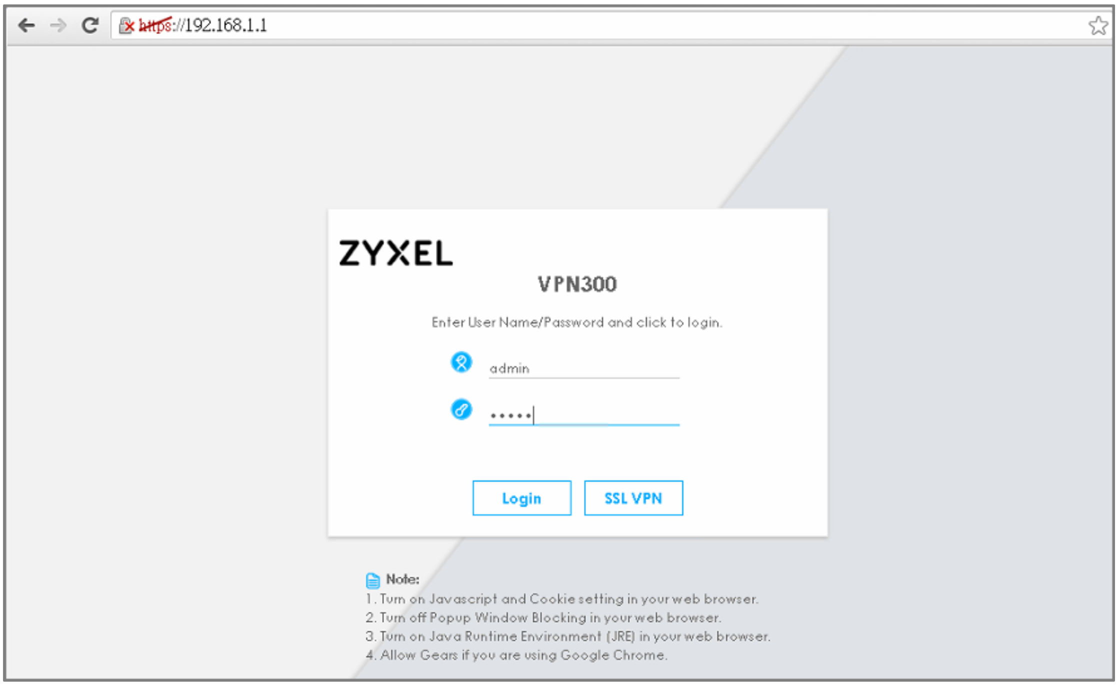


Not secure | ~~https~~://220.137.85.169
ZYXEL
VPN300
Enter User Name/Password and click to login.
Login denied
Login
SSL VPN

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.

Login to the device via the LAN interface with the administrator's user name and password. The management portal will be displayed.

Login to the device via the LAN interface



VPN300

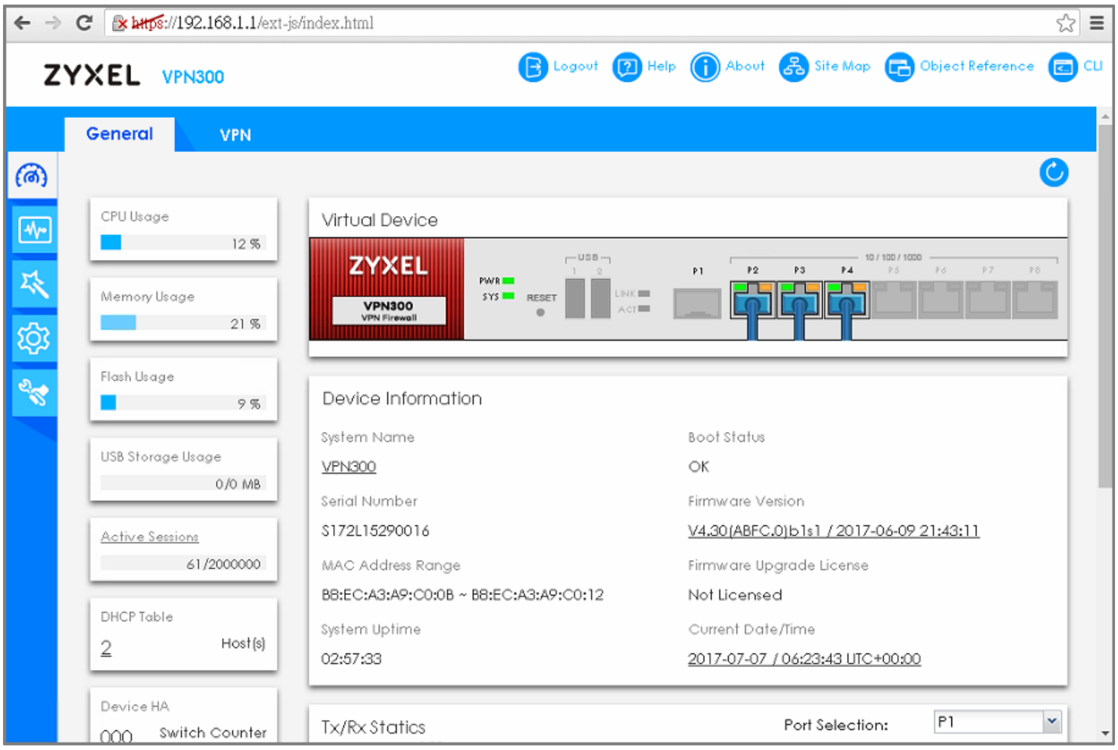
Enter User Name/Password and click to login.

admin

•••••

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.



CPU Usage 12 %

Memory Usage 21 %

Flash Usage 9 %

USB Storage Usage 0/0 MB

Active Sessions 61/2000000

DHCP Table 2 Host(s)

Device HA 000 Switch Counter

Virtual Device

Device Information

System Name: VPN300

Boot Status: OK

Serial Number: S172L15290016

Firmware Version: V4.30(ABFC.0)b1s1 / 2017-06-09 21:43:11

MAC Address Range: B8:EC:A3:A9:C0:0B ~ B8:EC:A3:A9:C0:12

Firmware Upgrade License: Not Licensed

System Uptime: 02:57:33

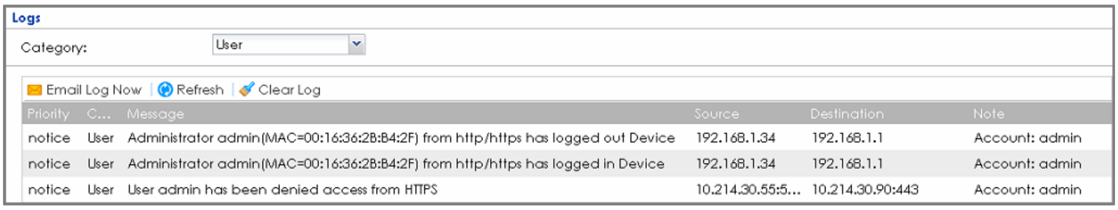
Current Date/Time: 2017-07-07 / 06:23:43 UTC+00:00

Tx/Rx Statics

Port Selection: P1

Go to **MONITOR > Log**. You can see that the admin login has been denied access from the WAN interface but it is allowed from the LAN interface.

MONITOR > Log



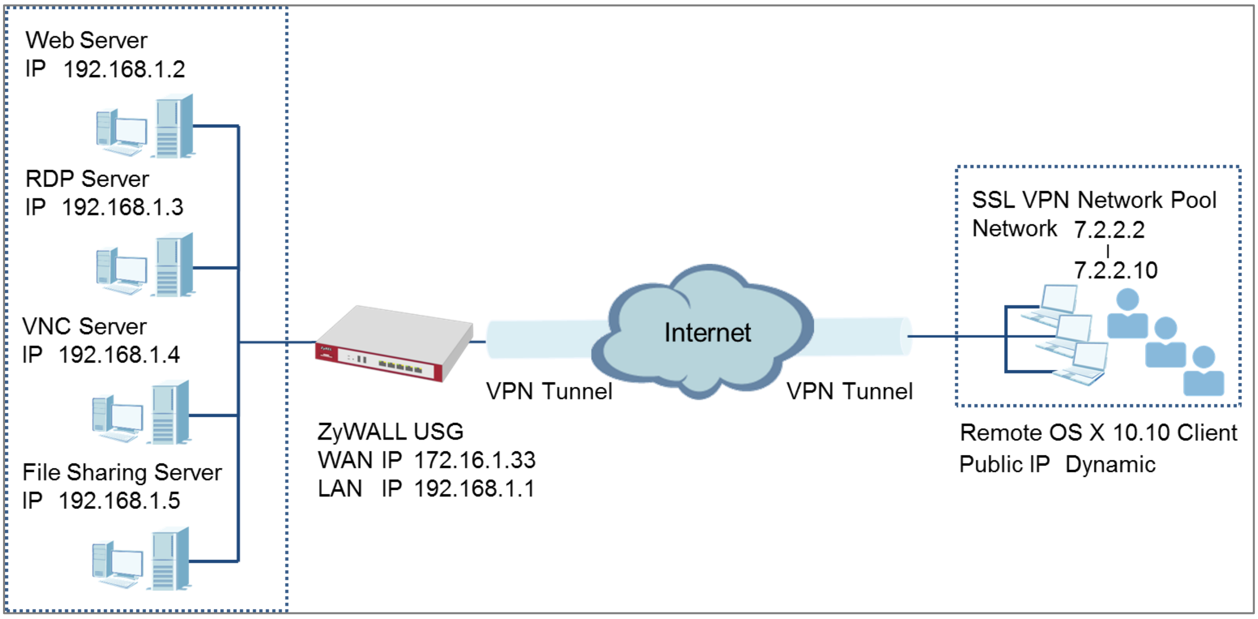
Category: User

Priority	C...	Message	Source	Destination	Note
notice	User	Administrator admin(MAC=00:16:36:2B:B4:2F) from http/https has logged out Device	192.168.1.34	192.168.1.1	Account: admin
notice	User	Administrator admin(MAC=00:16:36:2B:B4:2F) from http/https has logged in Device	192.168.1.34	192.168.1.1	Account: admin
notice	User	User admin has been denied access from HTTPS	10.214.30.55:5...	10.214.30.90:443	Account: admin

How to Deploy SSL VPN with Apple Mac OS X 10.10 Operating System

This is an example of using the ZyWALL/USG SSL VPN client software in Apple MAC OS X 10.10 Yosemite operating systems for secure connections to the network behind the ZyWALL/USG. When the VPN tunnel is configured, users can securely access the network from a Mac OS X 10.11 Yosemite computer.

ZyWALL/USG SSL VPN with Apple MAC OS X 10.10 Yosemite

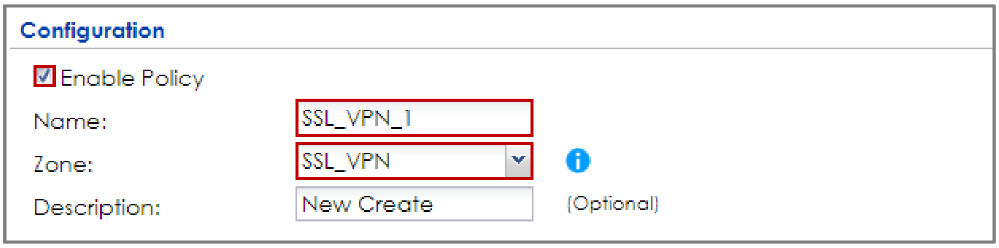


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25) and Apple MAC (Version: OS X10.10 Yosemite).

Set Up the SSL VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > VPN > SSL VPN > Access Privilege** to add an **Access Policy**. Configure a **Name** for you to identify the SSL VPN configuration.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Configuration


Configuration

☑ Enable Policy

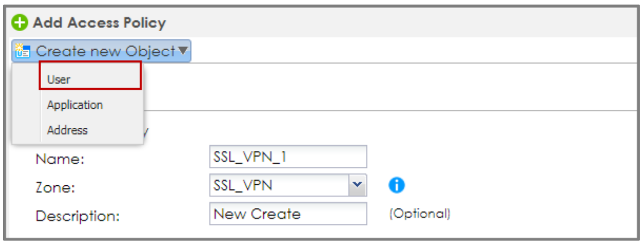
Name: SSL_VPN_1

Zone: SSL_VPN

Description: New Create (Optional)

Go to **Create new Object > User** to add **User Name** (SSL_VPN_1_Users in this example) and **Password** (4-24 characters, zyx168 in this example), click **OK**.

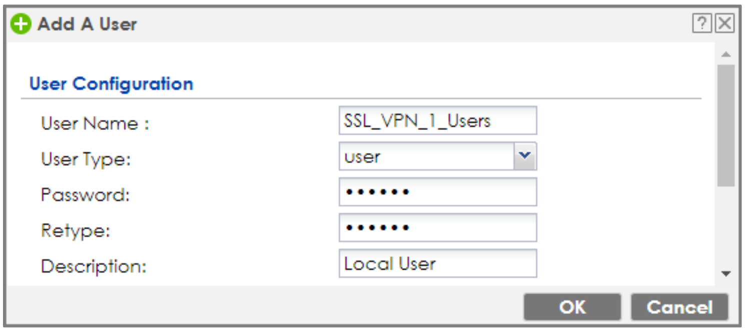
CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > User



Name: SSL_VPN_1

Zone: SSL_VPN

Description: New Create (Optional)


Add A User

User Configuration

User Name : SSL_VPN_1_Users

User Type: user

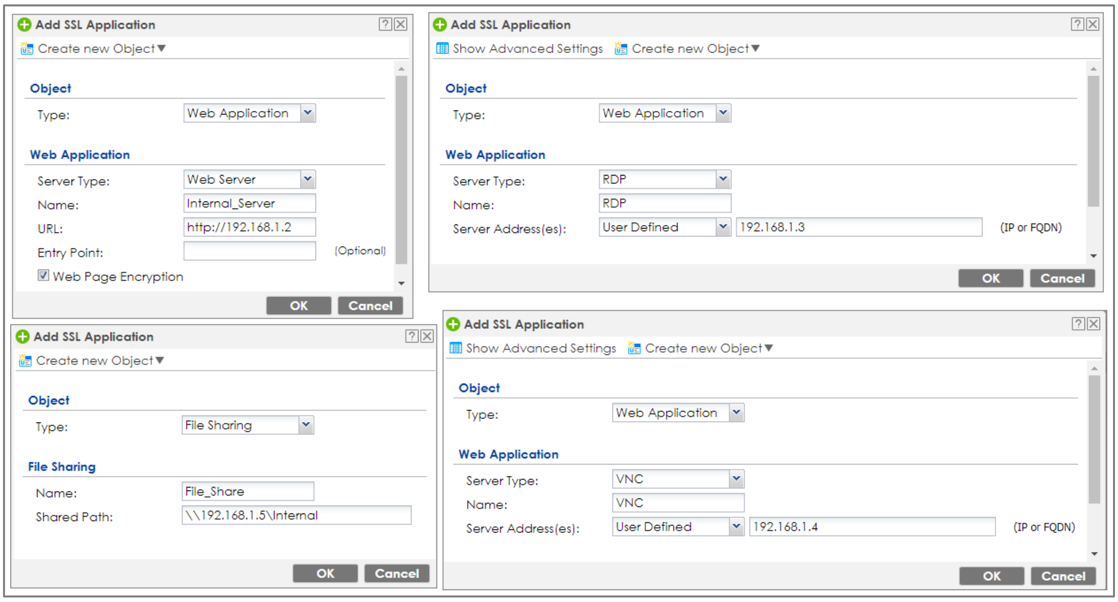
Password: ••••••

Retype: ••••••

Description: Local User

Go to **Create new Object > Application** to add servers you allow **SSL_VPN_1_Users** to access, click **OK**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > Application



Add SSL Application

Create new Object▼

Object

Type: Web Application

Web Application

Server Type: Web Server

Name: Internal_Server

URL: http://192.168.1.2

Entry Point: (Optional)

☑ Web Page Encryption

OK Cancel

Add SSL Application

Show Advanced Settings Create new Object▼

Object

Type: Web Application

Web Application

Server Type: RDP

Name: RDP

Server Address(es): User Defined 192.168.1.3 (IP or FQDN)

OK Cancel

Add SSL Application

Create new Object▼

Object

Type: File Sharing

File Sharing

Name: File_Share

Shared Path: \\192.168.1.5\Internal

OK Cancel

Add SSL Application

Show Advanced Settings Create new Object▼

Object

Type: Web Application

Web Application

Server Type: VNC

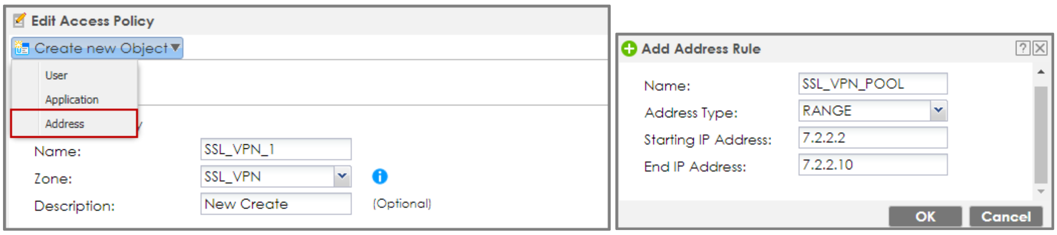
Name: VNC

Server Address(es): User Defined 192.168.1.4 (IP or FQDN)

OK Cancel

Go to **Create new Object > Address** to add the IP address pool for **SSL_VPN_1_Users**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > Address



Edit Access Policy

Create new Object▼

User

Application

Address

Name: SSL_VPN_1

Zone: SSL_VPN

Description: New Create (Optional)

Add Address Rule

Name: SSL_VPN_POOL

Address Type: RANGE

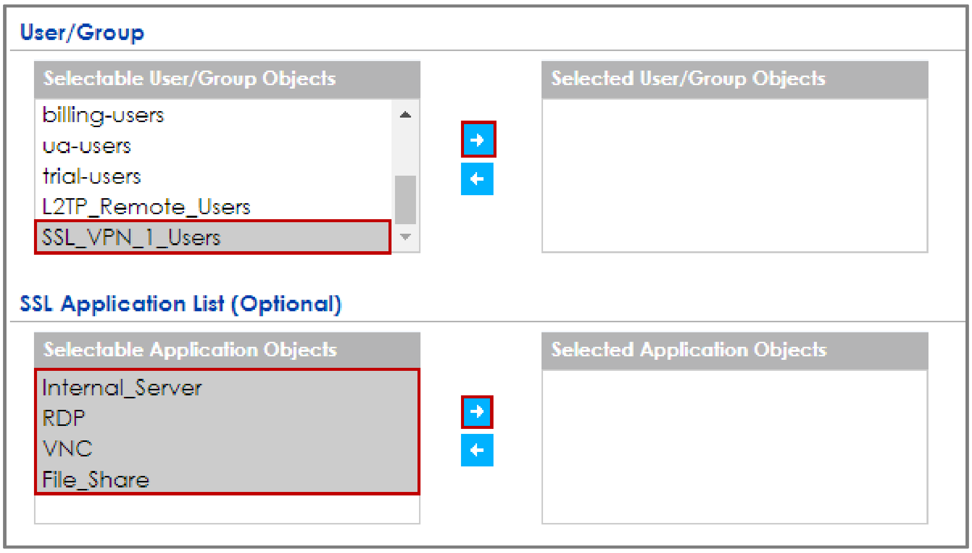
Starting IP Address: 7.2.2.2

End IP Address: 7.2.2.10

OK Cancel

Then, move the just created address object to **Selected User/Group Objects**. Similarly, in **SSL Application List (Optional)** move the servers you want available to SSL users to **Selected Appellation Objects**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > User/Group & SSL Application



User/Group

Selectable User/Group Objects

billing-users
ua-users
trial-users
L2TP_Remote_Users
SSL_VPN_1_Users

Selected User/Group Objects

SSL Application List (Optional)

Selectable Application Objects

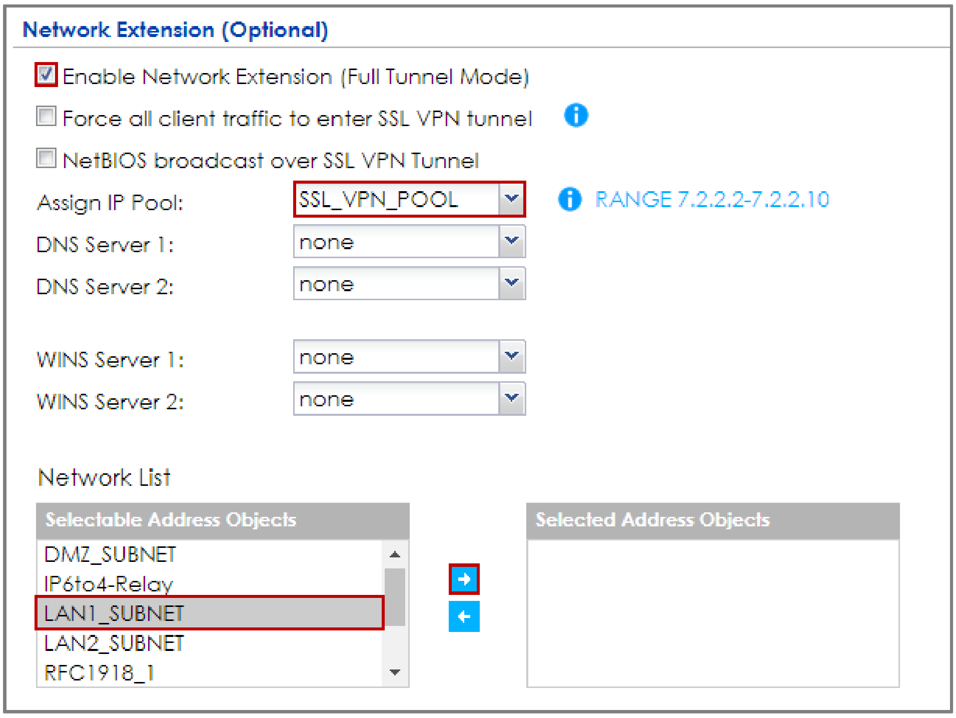
Internal_Server
RDP
VNC
File_Share

Selected Application Objects

Scroll down to **Network Extension (Optional)** to select **Enable Network Extension** to allow SSL VPN users to access the resources behind the ZyWALL/USG local network.

Select network(s) name in the **Selectable Address Objects** list and click the right arrow button to add to the **Selected Address Objects** list. You can select more than one network.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Network Extension (Optional)



Network Extension (Optional)

☑ Enable Network Extension (Full Tunnel Mode)

□ Force all client traffic to enter SSL VPN tunnel

□ NetBIOS broadcast over SSL VPN Tunnel

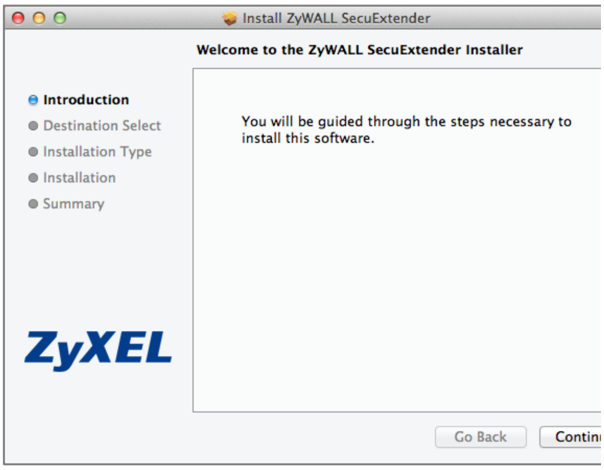
Assign IP Pool:	SSL_VPN_POOL (RANGE 7.2.2.2-7.2.2.10)
DNS Server 1:	none
DNS Server 2:	none
WINS Server 1:	none
WINS Server 2:	none

Network List

Selectable Address Objects	Selected Address Objects
DMZ_SUBNET	
IP6to4-Relay	
LAN1_SUBNET	
LAN2_SUBNET	
RFC1918_1	

Set Up the SSL VPN Tunnel on the Apple MAC OS X 10.10 Operating System

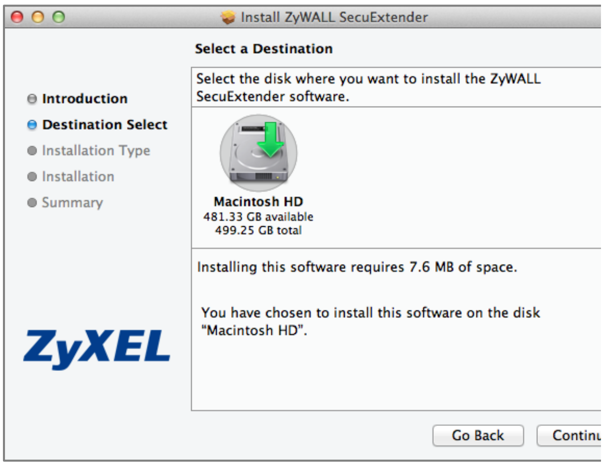
Download SSL VPN Client software: **ZyWALL SecuExtender** for MAC from the ZyXEL Global Website and double-click on the downloaded file to install it.



Install ZyWALL SecuExtender

Welcome to the ZyWALL SecuExtender Installer

You will be guided through the steps necessary to install this software.



Install ZyWALL SecuExtender

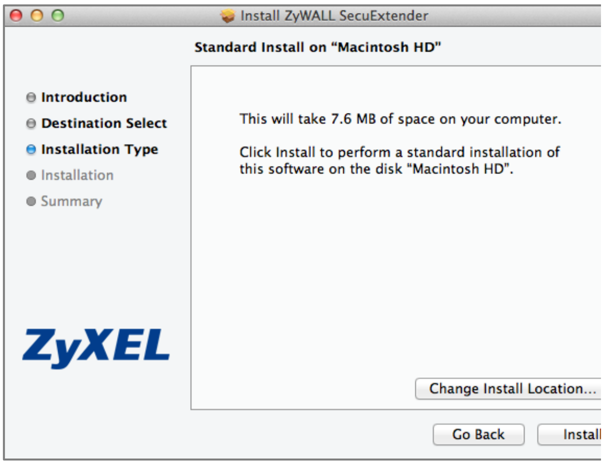
Select a Destination

Select the disk where you want to install the ZyWALL SecuExtender software.

Macintosh HD
481.33 GB available
499.25 GB total

Installing this software requires 7.6 MB of space.

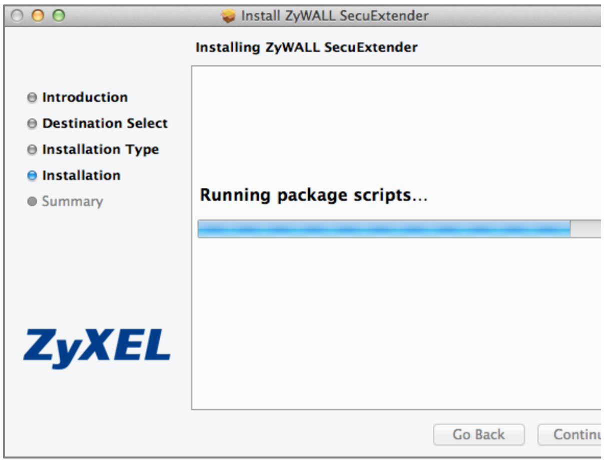
You have chosen to install this software on the disk "Macintosh HD".



Standard Install on "Macintosh HD"

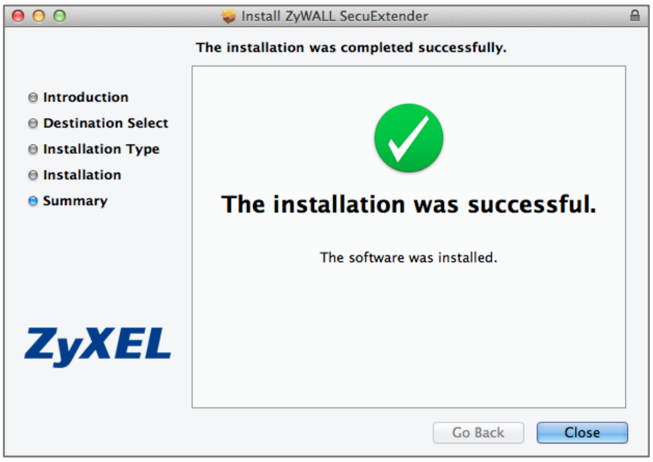
This will take 7.6 MB of space on your computer.

Click Install to perform a standard installation of this software on the disk "Macintosh HD".



Installing ZyWALL SecuExtender

Running package scripts…



The installation was completed successfully.

The installation was successful.

The software was installed.

Go to **ZyWALL SecuExtender > Preferences,** click the "**+**" button at the bottom left to add a new SSL VPN connection.

Configure the **Connection Name** for you to identify the SSL VPN configuration. Then, set the **Remote Server Address** to be the WAN IP of ZyWALL/USG (172.16.1.33 in this example). Click **Save**.

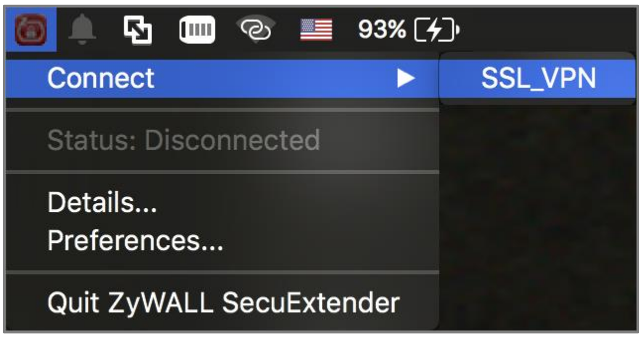
Here are two methods to initiate SSL VPN connections:

From ZyWALL SecuExtender

From a Web Browser

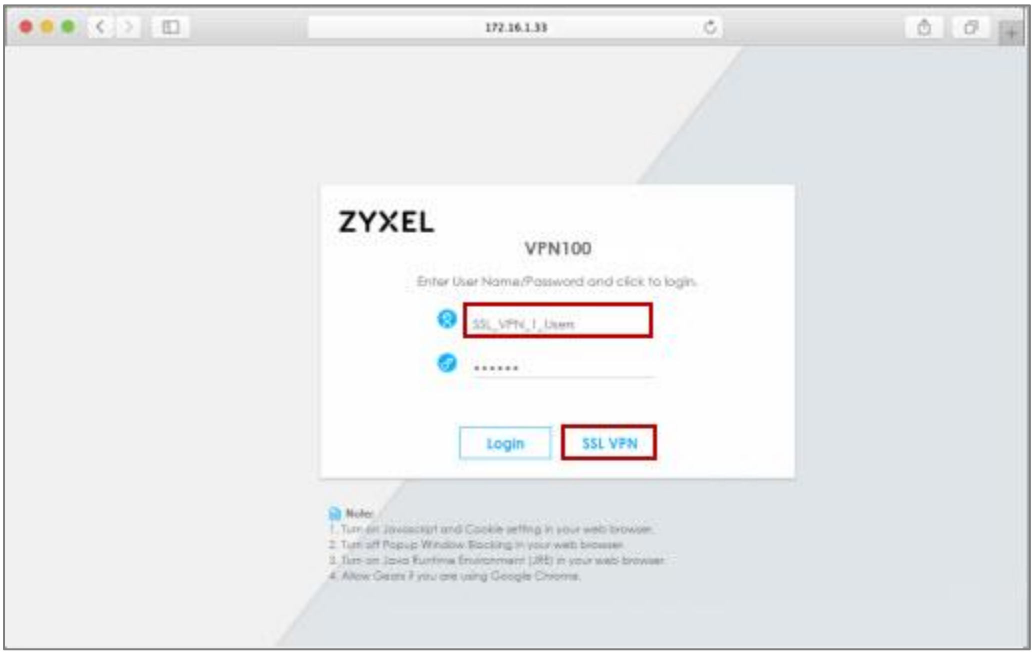
From ZyWALL SecuExtender

Go to **ZyWALL SecuExtender > Connect > SSL_VPN**, to display the username and password dialog box. Set **Username** and **Password** to be the same as your ZyWALL/USG SSL VPN **Selected User/Group** name and password (SSL_VPN_1_Users/zyx168 in this example).



From a Web Browser

Type ZyWALL/USG's WAN IP into the browser, to display the login screen. Enter **User Name** and **Password** to be the same as your ZyWALL/USG SSL VPN **Selected User/Group** name and password (SSL_VPN_1_Users/zyx168 in this example). Click **SSL VPN**.



Enter User Name/Password and click to login.

SSL_VPN_1_Users

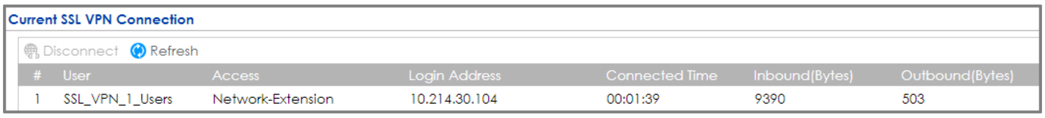
••••••

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.

Test the SSL VPN Tunnel

Go to ZyWALL/USG **MONITOR > VPN Monitor > SSL** and verify the tunnel **Login Address**, **Connected Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic.

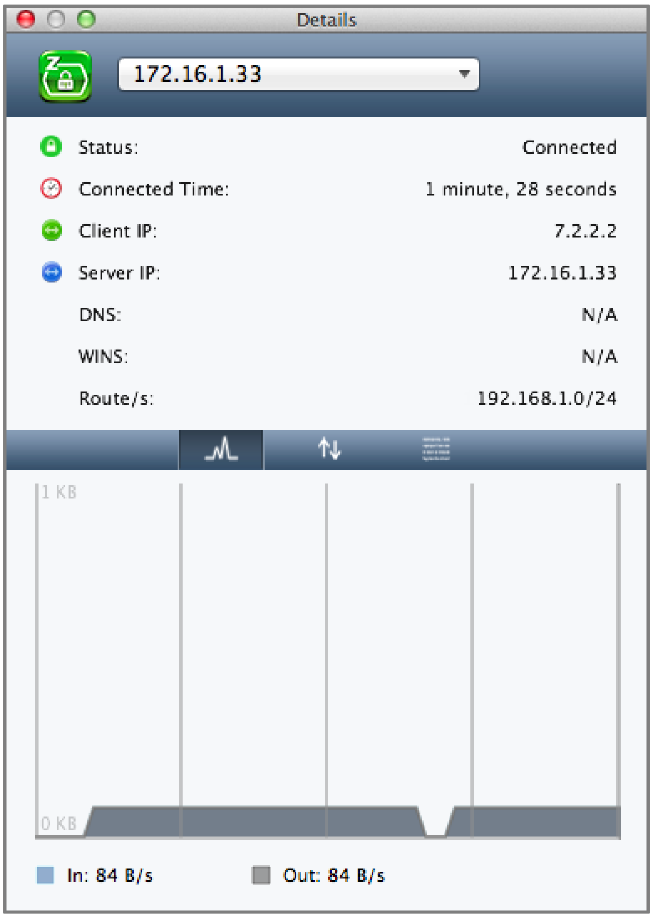
MONITOR > VPN Monitor > SSL > SSL_VPN_1_Users



#	User	Access	Login Address	Connected Time	Inbound(Bytes)	Outbound(Bytes)
1	SSL_VPN_1_Users	Network-Extension	10.214.30.104	00:01:39	9390	503

Go to **ZyWALL SecuExtender > Details** and check **Traffic Graph**, **Network Traffic Statics** and **Log Details**.

ZyWALL SecuExtender > Details > Traffic Graph



Status: Connected

Connected Time: 1 minute, 28 seconds

Client IP: 7.2.2.2

Server IP: 172.16.1.33

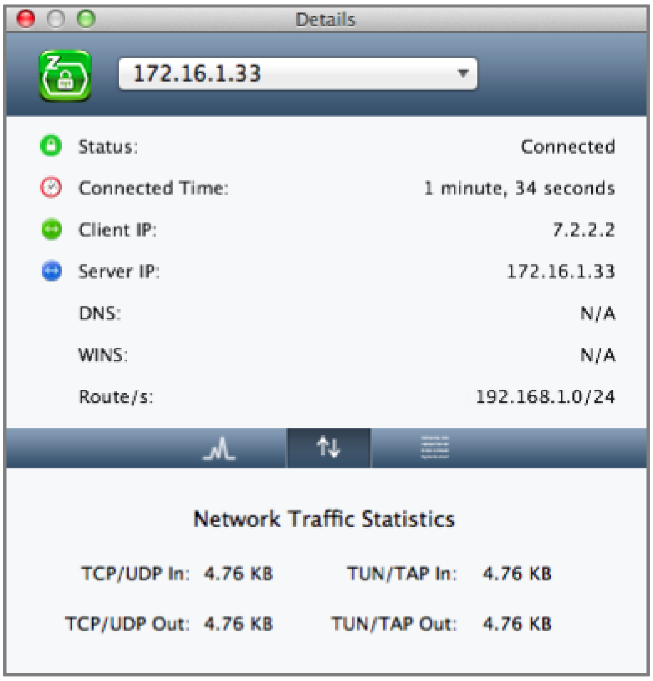
DNS: N/A

WINS: N/A

Route/s: 192.168.1.0/24

▨ In: 84 B/s ▨ Out: 84 B/s

ZyWALL SecuExtender > Details > Network Traffic Statics



172.16.1.33

Status: Connected

Connected Time: 1 minute, 34 seconds

Client IP: 7.2.2.2

Server IP: 172.16.1.33

DNS: N/A

WINS: N/A

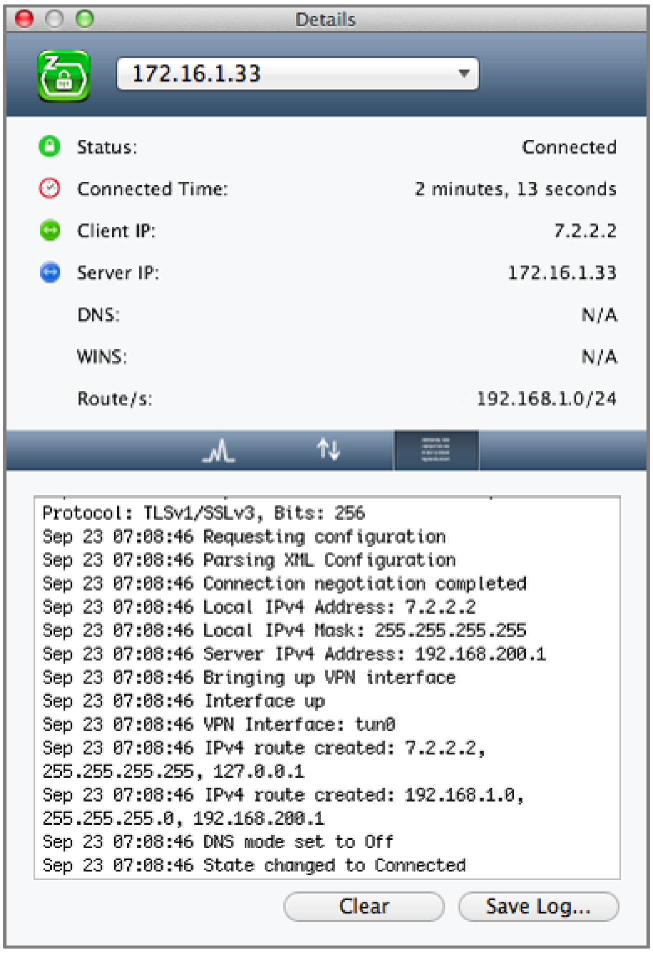
Route/s: 192.168.1.0/24

Network Traffic Statistics

TCP/UDP In: 4.76 KB TUN/TAP In: 4.76 KB

TCP/UDP Out: 4.76 KB TUN/TAP Out: 4.76 KB

ZyWALL SecuExtender > Details > Log Details



Status: Connected

Connected Time: 2 minutes, 13 seconds

Client IP: 7.2.2.2

Server IP: 172.16.1.33

DNS: N/A

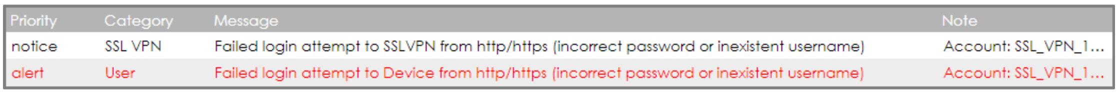
WINS: N/A

Route/s: 192.168.1.0/24

```
Protocol: TLSv1/SSLv3, Bits: 256
Sep 23 07:08:46 Requesting configuration
Sep 23 07:08:46 Parsing XML Configuration
Sep 23 07:08:46 Connection negotiation completed
Sep 23 07:08:46 Local IPv4 Address: 7.2.2.2
Sep 23 07:08:46 Local IPv4 Mask: 255.255.255.255
Sep 23 07:08:46 Server IPv4 Address: 192.168.200.1
Sep 23 07:08:46 Bringing up VPN interface
Sep 23 07:08:46 Interface up
Sep 23 07:08:46 VPN Interface: tun0
Sep 23 07:08:46 IPv4 route created: 7.2.2.2,
255.255.255.255, 127.0.0.1
Sep 23 07:08:46 IPv4 route created: 192.168.1.0,
255.255.255.0, 192.168.200.1
Sep 23 07:08:46 DNS mode set to Off
Sep 23 07:08:46 State changed to Connected
```

What Could Go Wrong?

If you see [notice] or [alert] log message such as below, please check ZyWALL/USG SSL **Selected User/Group Objects** settings. MAC OS X 10.10 Yosemite users must use the same **Username** and **Password** as configured in ZyWALL/USG to establish the SSL VPN tunnel.



Priority	Category	Message	Note
notice	SSL VPN	Failed login attempt to SSLVPN from http/https (incorrect password or inexistent username)	Account: SSL_VPN_1...
alert	User	Failed login attempt to Device from http/https (incorrect password or inexistent username)	Account: SSL_VPN_1...

If you uploaded a logo to show in the SSL VPN user screens but it does not display properly, check that the logo graphic is in GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The

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

If users can log into the SSL VPN but cannot see some of the resource links check the SSL application object's configuration.

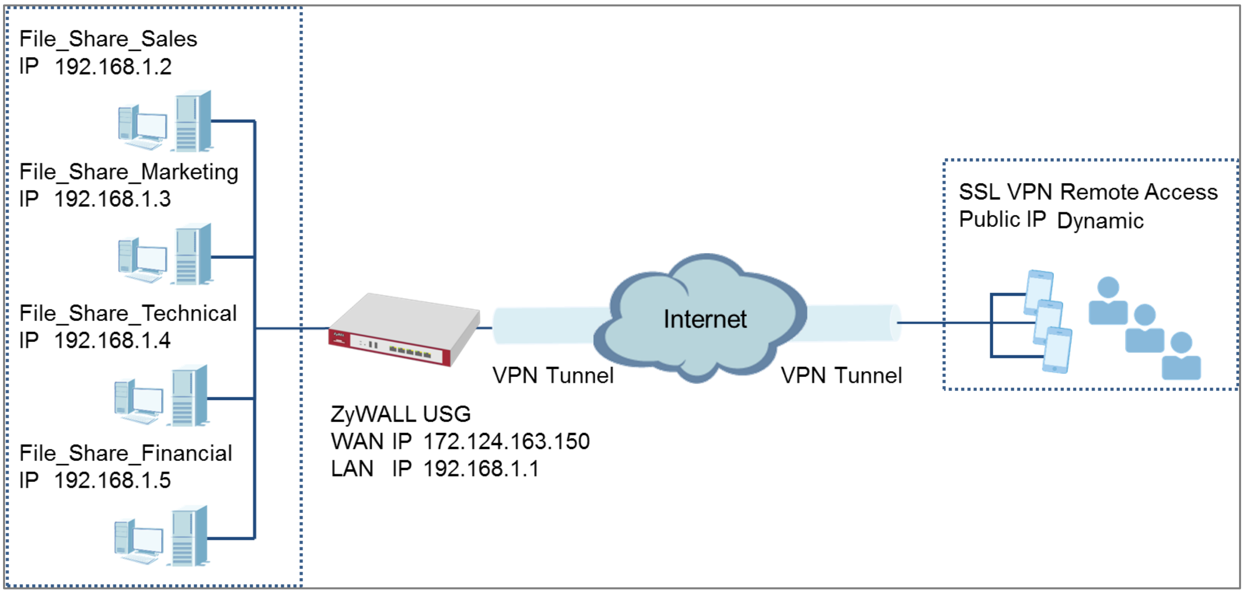
If the ZyWALL/USG redirects the user to the user aware screen, check whether the user account is included in an SSL VPN access policy or not.

Changing the HTTP/HTTPS configuration disconnects SSL VPN network extension sessions. Users need to re-connect if this happens.

How To Configure SSL VPN for Remote Access Mobile Devices

This is an example of using the ZyWALL/USG SSL VPN for remote access mobile devices to securely connect to the File Sharing Server behind the ZyWALL/USG.

ZyWALL/USG SSL VPN for Secure External Access to Network Resources

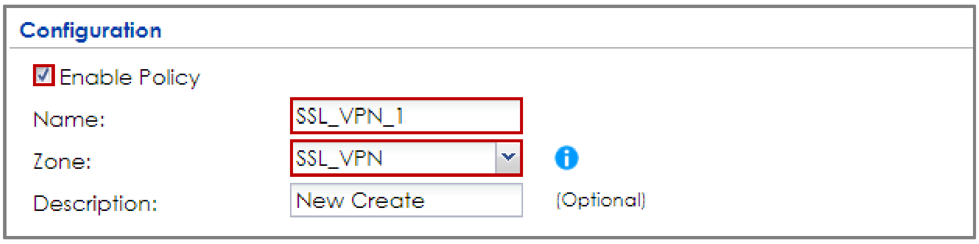


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG1900 (Firmware Version: ZLD 4.25).

Set Up the SSL VPN Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > VPN > SSL VPN > Access Privilege** to add an **Access Policy**. Configure a **Name** for you to identify the SSL VPN configuration.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Configuration



Configuration

☑ Enable Policy

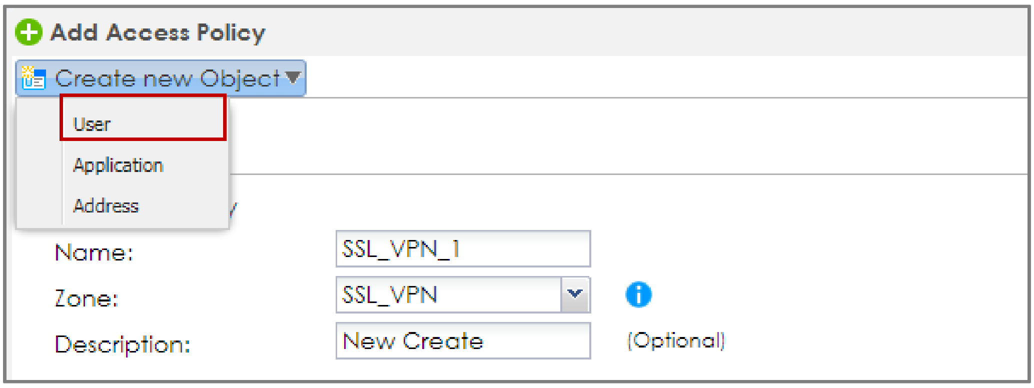
Name: SSL_VPN_1

Zone: SSL_VPN

Description: New Create (Optional)

Go to **Create new Object > User** to add **User Name** (SSL_VPN_1_Users in this example) and **Password** (4-24 characters, zyx168 in this example), click **OK.**

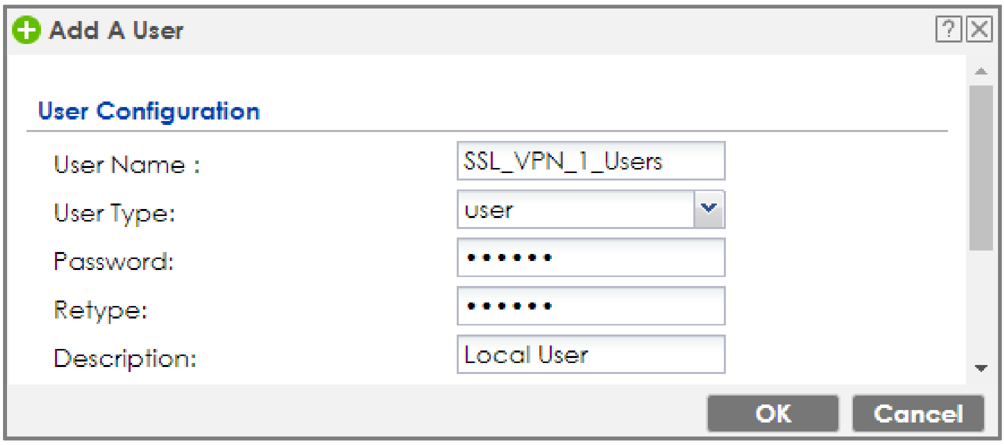
CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > User



Name: SSL_VPN_1

Zone: SSL_VPN

Description: New Create (Optional)



User Configuration

User Name : SSL_VPN_1_Users

User Type: user

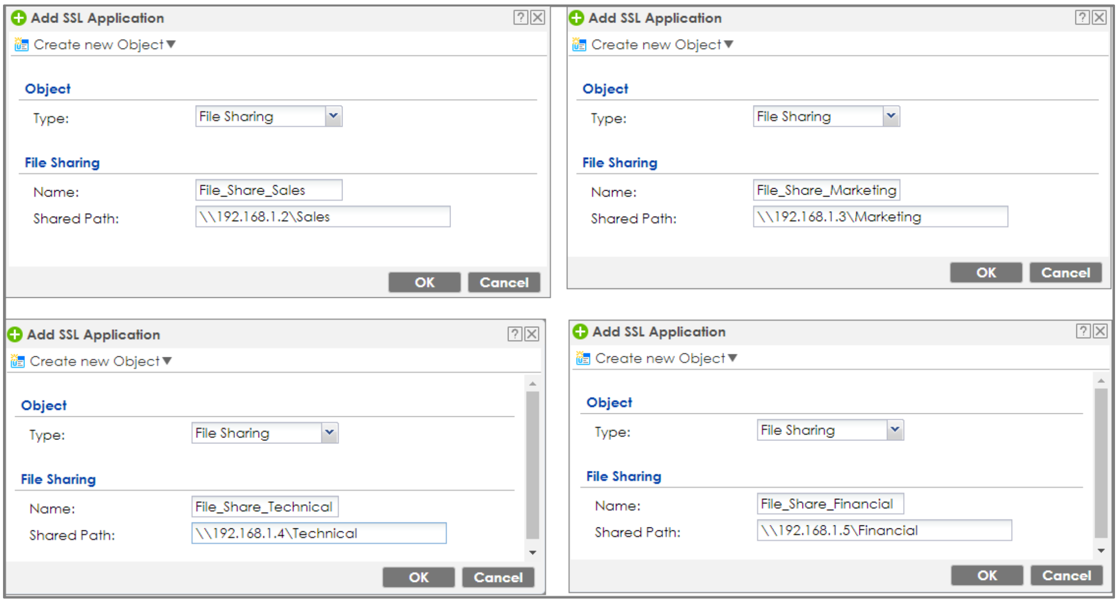
Password: ••••••

Retype: ••••••

Description: Local User

Go to **Create new Object > Application** to add servers that you will allow **SSL_VPN_1_Users** to access. Click **OK**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > Application



Object
Type: File Sharing
File Sharing
Name: File_Share_Sales
Shared Path: \\192.168.1.2\Sales

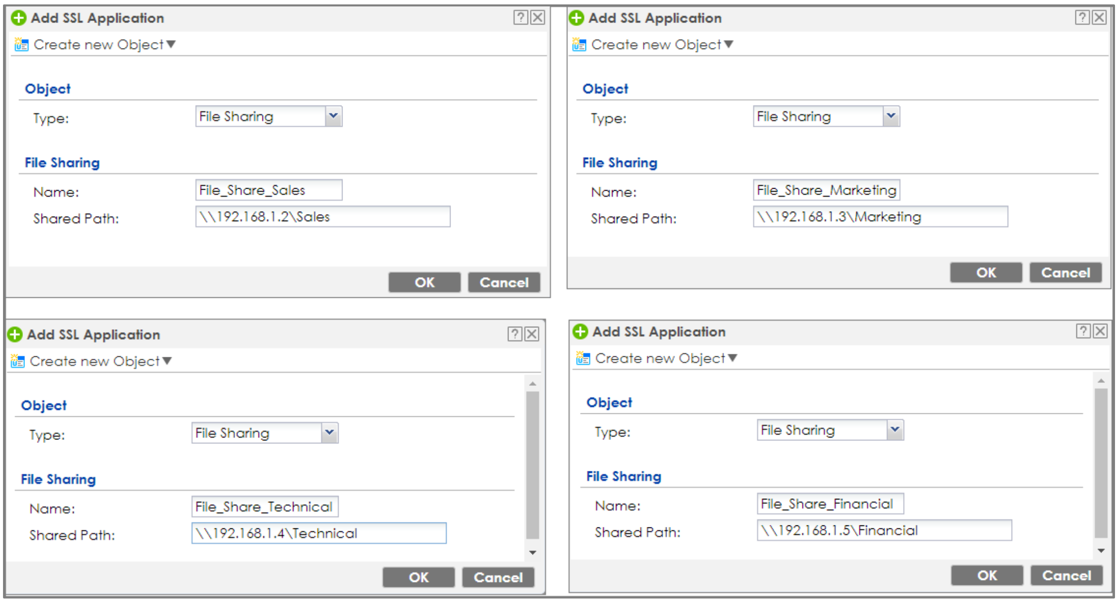
Object
Type: File Sharing
File Sharing
Name: File_Share_Marketing
Shared Path: \\192.168.1.3\Marketing

Object
Type: File Sharing
File Sharing
Name: File_Share_Technical
Shared Path: \\192.168.1.4\Technical

Object
Type: File Sharing
File Sharing
Name: File_Share_Financial
Shared Path: \\192.168.1.5\Financial

Then, move the just created address object to **Selected User/Group Objects**. Similarly, **in SSL Application List (Optional)** move the servers you want available to SSL users **to Selected Application Objects**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > User/Group & SSL Application



Add SSL Application

Object
Type: File Sharing

File Sharing
Name: File_Share_Sales
Shared Path: \\192.168.1.2\Sales

Add SSL Application

Object
Type: File Sharing

File Sharing
Name: File_Share_Marketing
Shared Path: \\192.168.1.3\Marketing

Add SSL Application

Object
Type: File Sharing

File Sharing
Name: File_Share_Technical
Shared Path: \\192.168.1.4\Technical

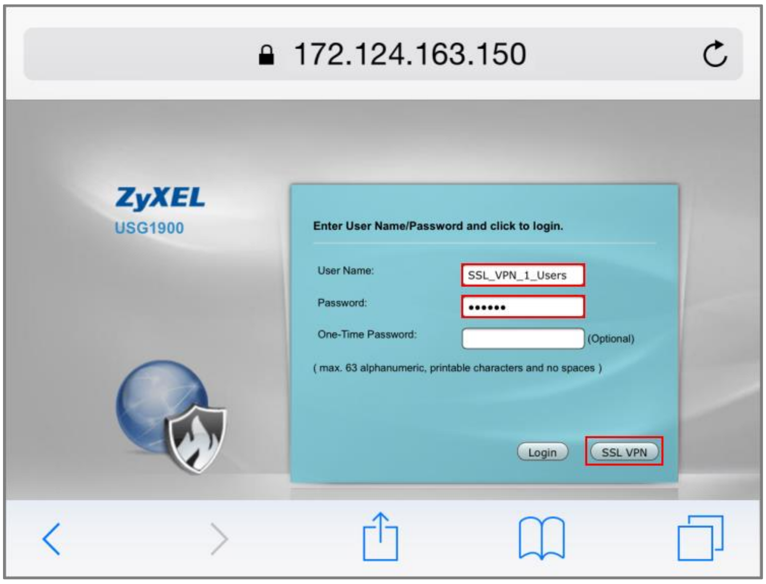
Add SSL Application

Object
Type: File Sharing

File Sharing
Name: File_Share_Financial
Shared Path: \\192.168.1.5\Financial

Test the SSL VPN Tunnel

Type the ZyWALL/USG's WAN IP into the browser, then the login screen appears. Enter **User Name** and **Password** to be the same as your ZyWALL/USG **SSL VPN Selected User/Group** name and password (SSL_VPN_1_Users/zyx168 in this example). Click **SSL VPN**.



Enter User Name/Password and click to login.

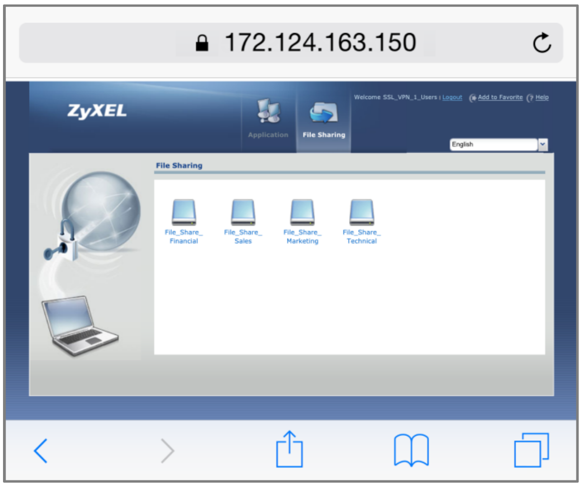
User Name: SSL_VPN_1_Users

Password: ••••••

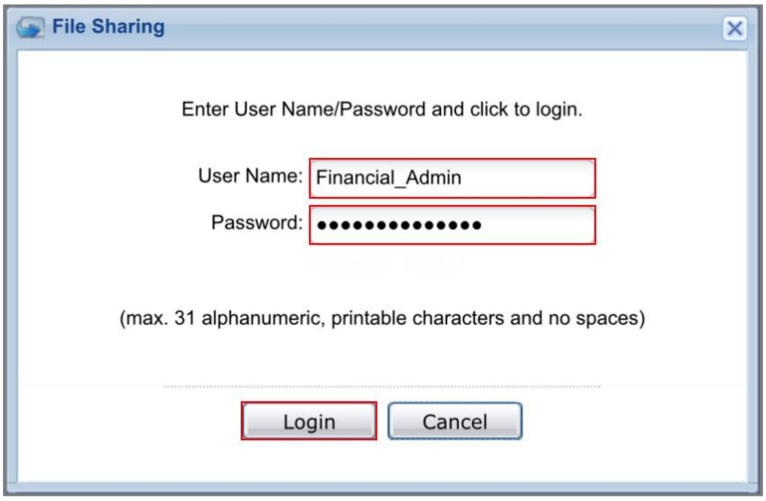
One-Time Password: (Optional)

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

The **File Sharing** server appears.



Click the **File Sharing** folder you want to access, enter **User Name/ Password** of your **File Sharing** server and click **Login**.



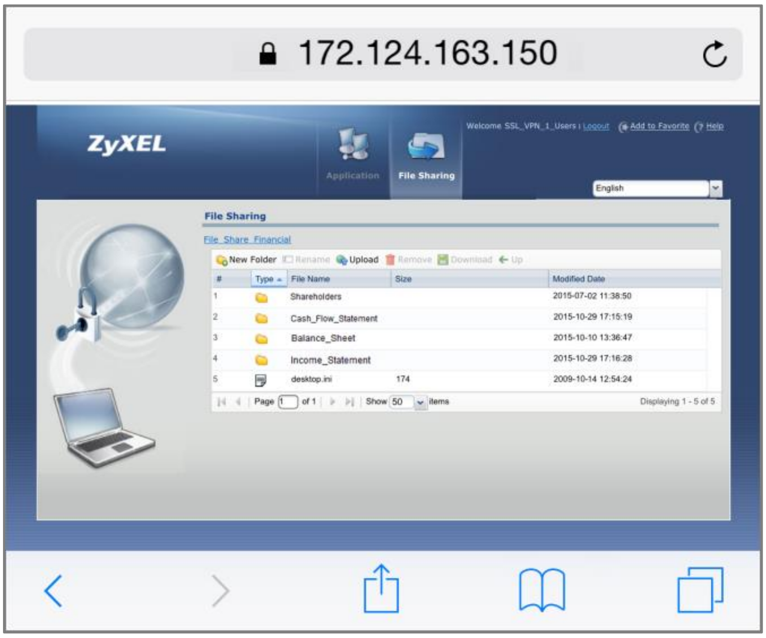
Enter User Name/Password and click to login.

User Name: Financial_Admin

Password: ••••••••••••••

(max. 31 alphanumeric, printable characters and no spaces)

Now you can securely access the files.

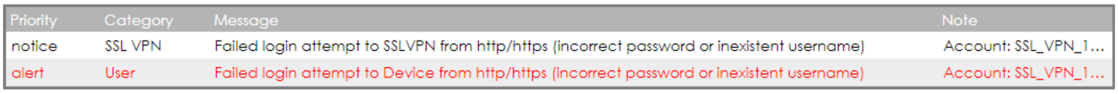


#	Type	File Name	Size	Modified Date
1		Shareholders		2015-07-02 11:38:50
2		Cash_Flow_Statement		2015-10-29 17:15:19
3		Balance_Sheet		2015-10-10 13:36:47
4		Income_Statement		2015-10-29 17:16:28
5		desktop.ini	174	2009-10-14 12:54:24

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

What Could Go Wrong?

If you see [notice] or [alert] log message such as below, please check ZyWALL/USG SSL **Selected User/Group Objects** settings. Windows 10 users must use the same **Username** and **Password** as configured in ZyWALL/USG to establish the SSL VPN tunnel.



Priority	Category	Message	Note
notice	SSL VPN	Failed login attempt to SSLVPN from http/https (incorrect password or inexistent username)	Account: SSL_VPN_1...
alert	User	Failed login attempt to Device from http/https (incorrect password or inexistent username)	Account: SSL_VPN_1...

If you uploaded a logo to show in the SSL VPN user screens but it does not display properly, check that the logo graphic is in GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The ZyWALL/USG automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.

If users can log into the SSL VPN but cannot see some of the resource links check the SSL application object's configuration.

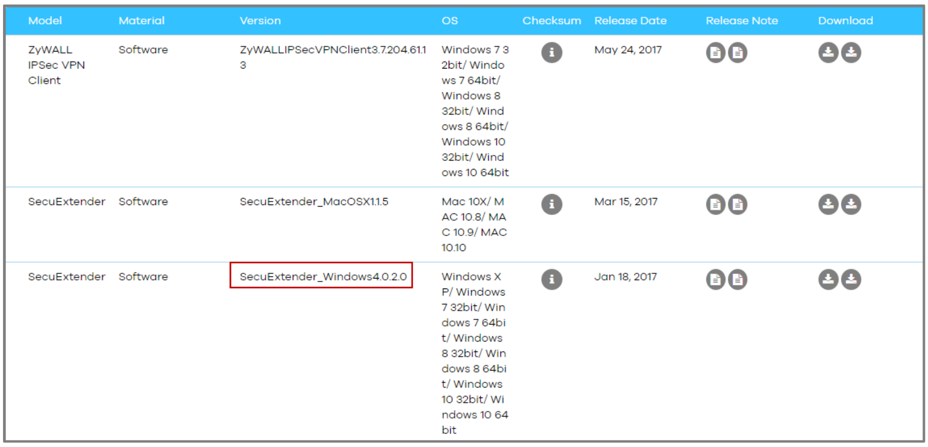
If the ZyWALL/USG redirects the user to the user aware screen, check whether the user account is included in an SSL VPN access policy or not.

Changing the HTTP/HTTPS configuration disconnects SSL VPN network extension sessions. Users need to re-connect if this happens.

How to Configure an SSL VPN Tunnel (with SecuExtender version 4.0.0.1) on the Windows 10 Operating System

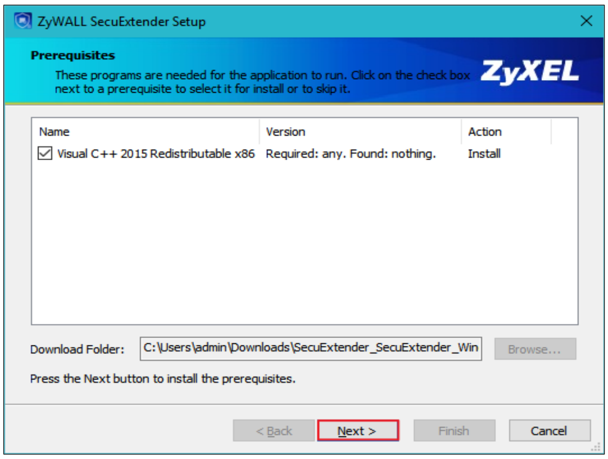
Set up the SSL VPN Tunnel with Windows 10

Please download SecuExtender version 4.0.0.1 from the download library of ZyXEL's official website.



Model	Material	Version	OS	Checksum	Release Date	Release Note	Download
ZyWALL IPSec VPN Client	Software	ZyWALLIPSecVPNClient3.7.204.61.13	Windows 7 32bit/ Windows 7 64bit/ Windows 8 32bit/ Windows 8 64bit/ Windows 10 32bit/ Windows 10 64bit	ℹ	May 24, 2017	🗎 🗎	⬇ ⬇
SecuExtender	Software	SecuExtender_MacOSX1.1.5	Mac 10X/ MAC 10.8/ MAC 10.9/ MAC 10.10	ℹ	Mar 15, 2017	🗎 🗎	⬇ ⬇
SecuExtender	Software	SecuExtender_Windows4.0.2.0	Windows XP/ Windows 7 32bit/ Windows 7 64bit/ Windows 8 32bit/ Windows 8 64bit/ Windows 10 32bit/ Windows 10 64 bit	ℹ	Jan 18, 2017	🗎 🗎	⬇ ⬇

Before you start installing the SecuExtender, it is required to install the "Visual C++ 2015 Redistributable" package first. Click **Next**, select **I agree to the license terms and conditions**, and click **Install** to complete the Visual C++ 2015 Redistributable installation. After that, the setup wizard appears. Please note that the users need to reboot their systems after the SecuExtender installation is completed.



ZyWALL SecuExtender Setup

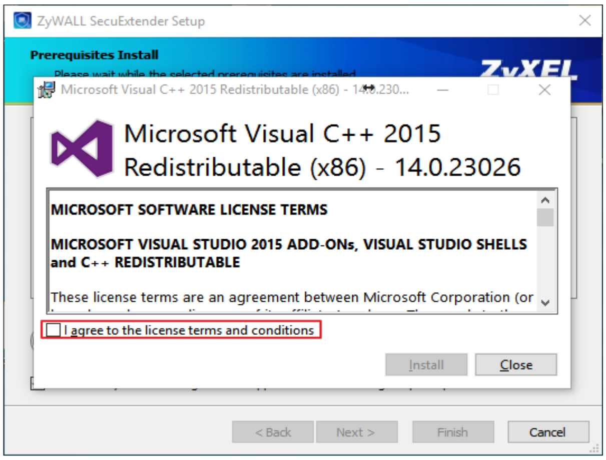
Prerequisites

These programs are needed for the application to run. Click on the check box next to a prerequisite to select it for install or to skip it.

Name	Version	Action
☑ Visual C++ 2015 Redistributable x86	Required: any. Found: nothing.	Install

Download Folder: C:\Users\admin\Downloads\SecuExtender_SecuExtender_Win

Press the Next button to install the prerequisites.



ZyWALL SecuExtender Setup

Prerequisites Install

Please wait while the selected prerequisites are installed

Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.230...

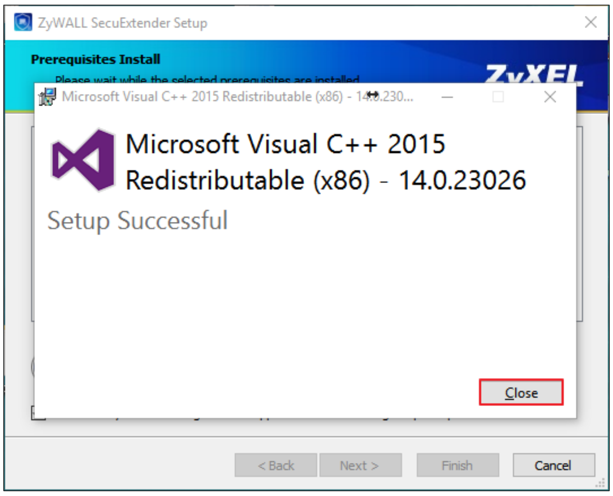
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.23026

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT VISUAL STUDIO 2015 ADD-ONs, VISUAL STUDIO SHELLS and C++ REDISTRIBUTABLE

These license terms are an agreement between Microsoft Corporation (or

□ I agree to the license terms and conditions



ZyWALL SecuExtender Setup

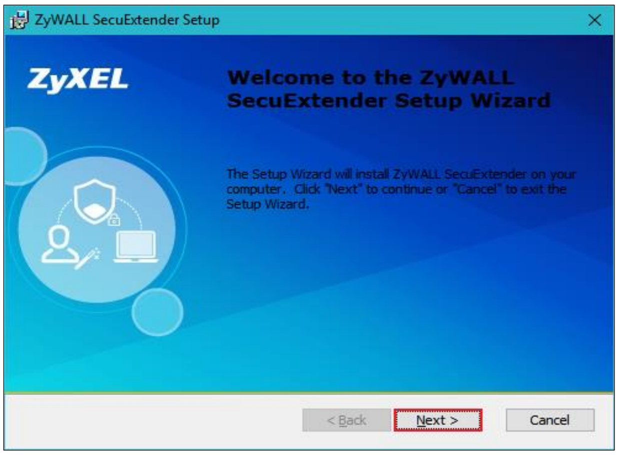
Prerequisites Install

Please wait while the selected prerequisites are installed

Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.230...

Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.23026

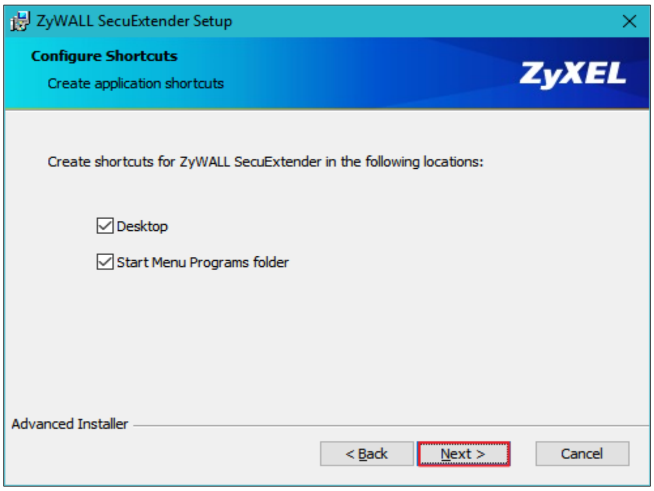
Setup Successful



ZyWALL SecuExtender Setup

Welcome to the ZyWALL SecuExtender Setup Wizard

The Setup Wizard will install ZyWALL SecuExtender on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.



ZyWALL SecuExtender Setup

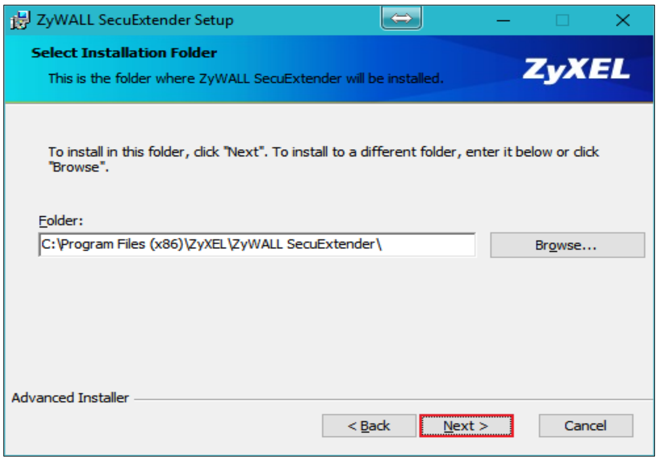
Configure Shortcuts

Create application shortcuts

Create shortcuts for ZyWALL SecuExtender in the following locations:

☑ Desktop

☑ Start Menu Programs folder



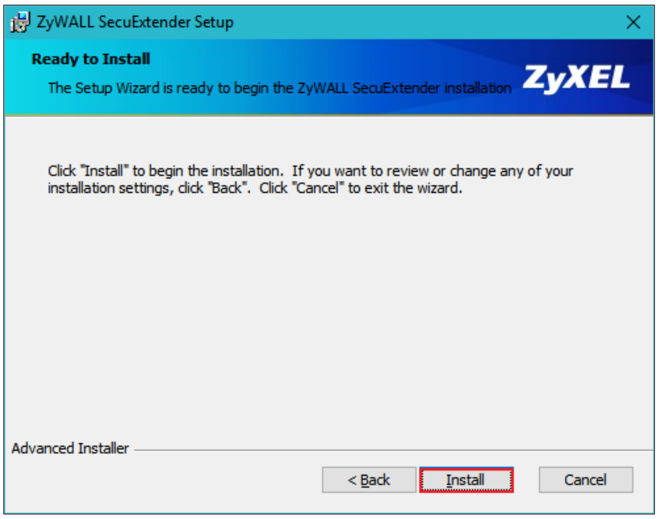
ZyWALL SecuExtender Setup

Select Installation Folder

This is the folder where ZyWALL SecuExtender will be installed.

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\ZyWALL SecuExtender\

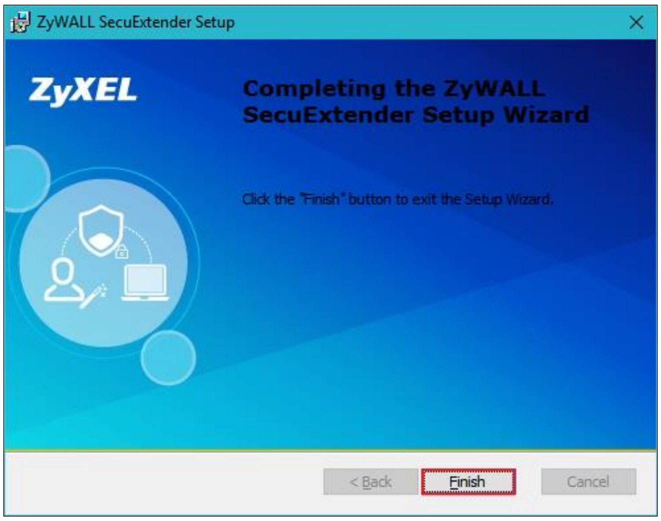


ZyWALL SecuExtender Setup

Ready to Install

The Setup Wizard is ready to begin the ZyWALL SecuExtender installation

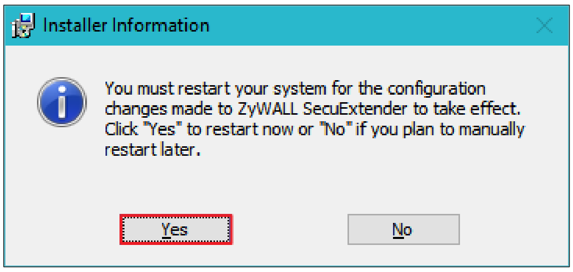
Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.



ZyWALL SecuExtender Setup

Completing the ZyWALL SecuExtender Setup Wizard

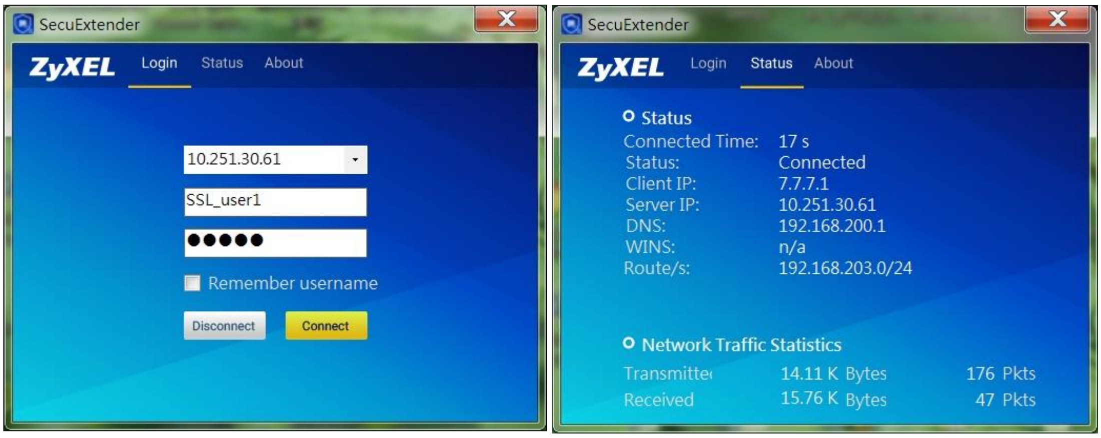
Click the "Finish" button to exit the Setup Wizard.



Installer Information

You must restart your system for the configuration changes made to ZyWALL SecuExtender to take effect. Click "Yes" to restart now or "No" if you plan to manually restart later.

Double-click the shortcut icon on your desktop. It is the same as the SSL VPN standalone software on MAC OS X. Enter the server's IP or domain name, user name, and password to connect to the server. The example below shows that the client IP is **7.7.7.1** and you can also check the traffic statistic in the **Status** screen.



10.251.30.61

SSL_user1

●●●●●

□ Remember username

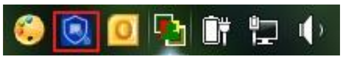
○ Status

Connected Time:	17 s
Status:	Connected
Client IP:	7.7.7.1
Server IP:	10.251.30.61
DNS:	192.168.200.1
WINS:	n/a
Route/s:	192.168.203.0/24

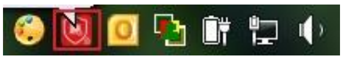
○ Network Traffic Statistics

Transmitte	14.11 K Bytes	176 Pkts
Received	15.76 K Bytes	47 Pkts

You can verify the connection status from the computer's taskbar icon.

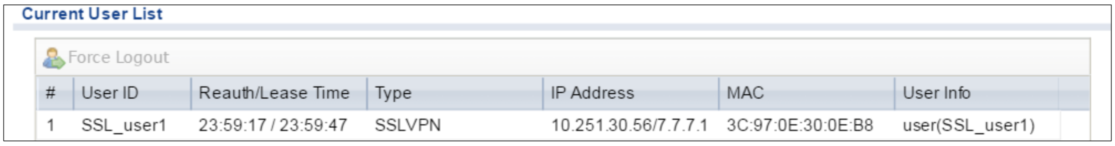


When connected, the icon is blue.



When disconnected, the icon is red.

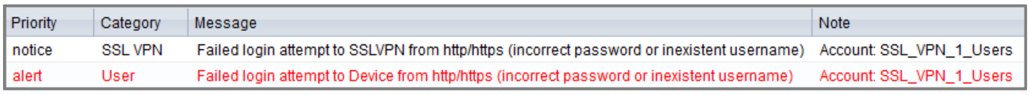
You can also use the USG monitor screen to check the login list of the users.



#	User ID	Reauth/Lease Time	Type	IP Address	MAC	User Info
1	SSL_user1	23:59:17 / 23:59:47	SSLVPN	10.251.30.56/7.7.7.1	3C:97:0E:30:0E:B8	user(SSL_user1)

What Can Go Wrong?

1 If you see a [notice] or [alert] log message such as shown below, please check the ZyWALL/USG SSL's **Selected User/Group Objects** settings. Windows 10 users must use the same **Username** and **Password** as configured in the ZyWALL/USG to establish the SSL VPN tunnel.



Priority	Category	Message	Note
notice	SSL VPN	Failed login attempt to SSLVPN from http/https (incorrect password or inexistent username)	Account: SSL_VPN_1_Users
alert	User	Failed login attempt to Device from http/https (incorrect password or inexistent username)	Account: SSL_VPN_1_Users

2 If you have uploaded a logo to show on the SSL VPN user screens but it does not display properly, check if the logo graphic is in GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The ZyWALL/USG automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.

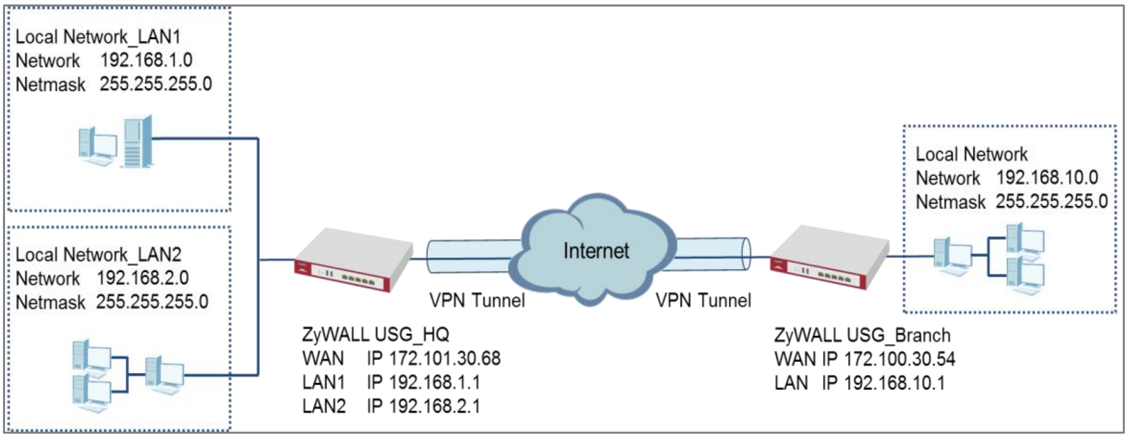
3 If users can log into the SSL VPN but cannot see some of the resource links, check the SSL application object's configurations.

4 If the ZyWALL/USG redirects the user to the user aware screen, check whether the user account is included in an SSL VPN access policy or not.

5 If you have changed the HTTP/HTTPS configuration, the SSL VPN network extension sessions will be disconnected. The sessions need to be reconnected if this happens.

How to redirect multiple LAN interface traffic to the VPN tunnel

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with multiple LAN access to the VPN tunnel. The example instructs how to configure the VPN tunnel between each site and redirect multiple LAN interface traffic to the VPN tunnel. When the VPN tunnel is configured, multiple LAN subnets can be accessed securely.



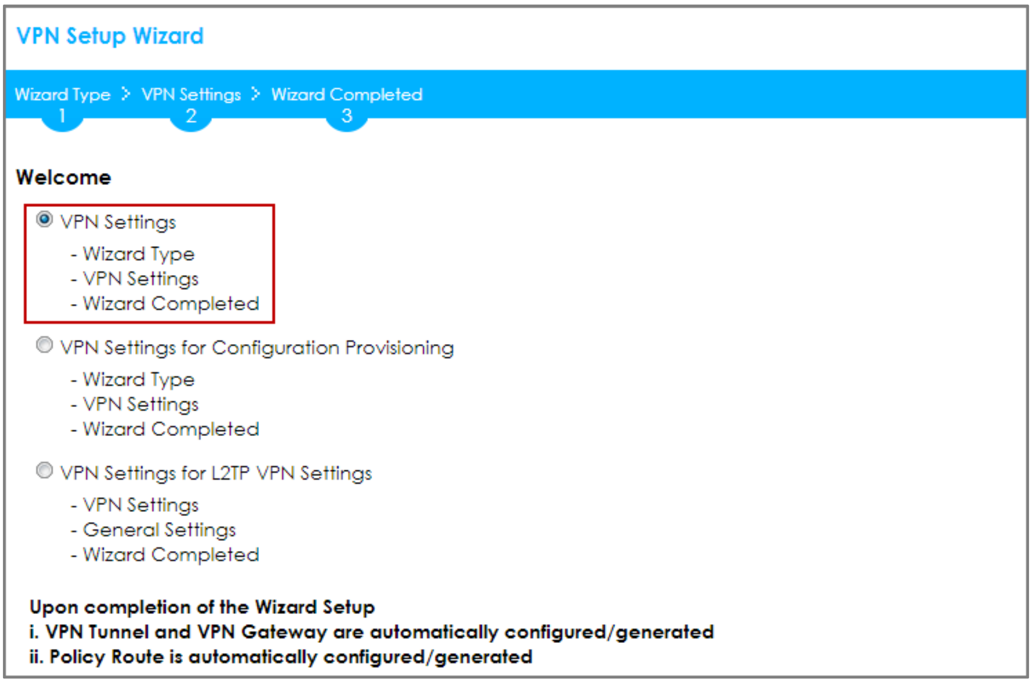
ZyWALL Site-to-site IPSec VPN with multiple LAN access

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (HQ)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Welcome

● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

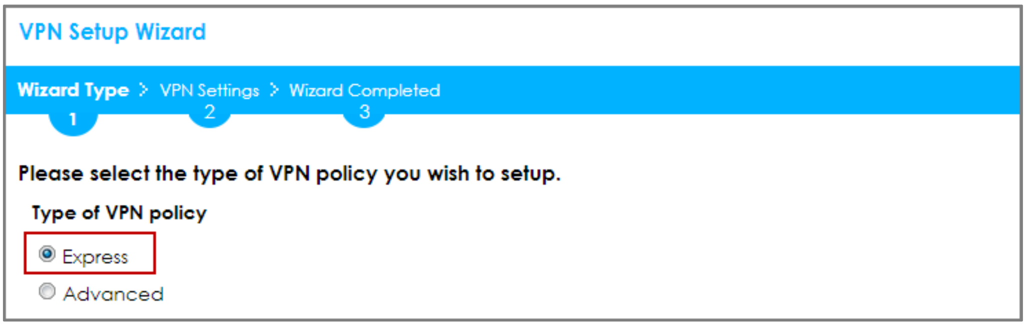
○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Upon completion of the Wizard Setup
i. VPN Tunnel and VPN Gateway are automatically configured/generated
ii. Policy Route is automatically configured/generated

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Wizard Type 1 > VPN Settings 2 > Wizard Completed 3

Please select the type of VPN policy you wish to setup.

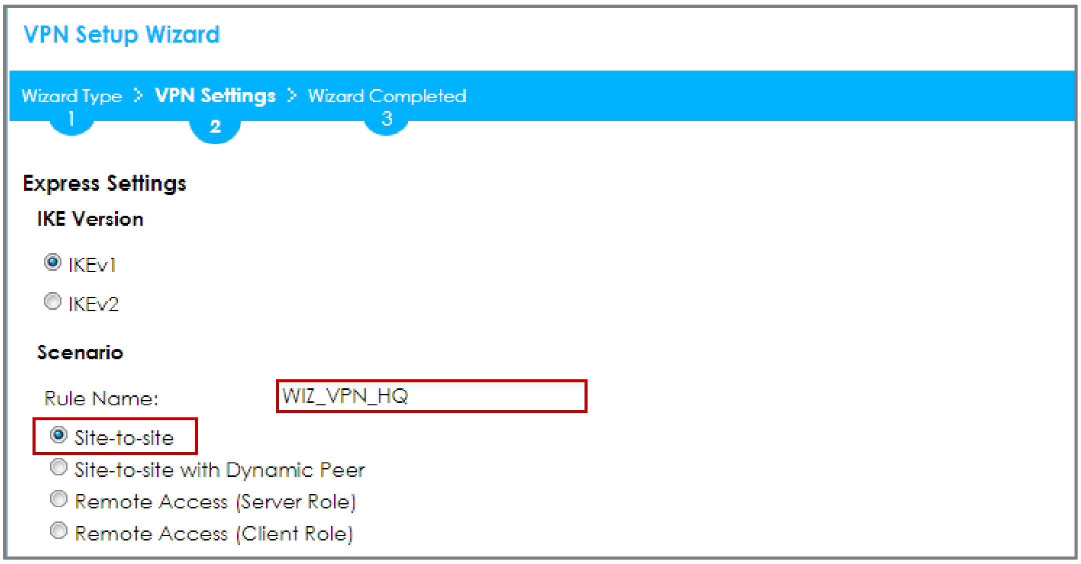
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



Express Settings

IKE Version

● IKEv1
○ IKEv2

Scenario

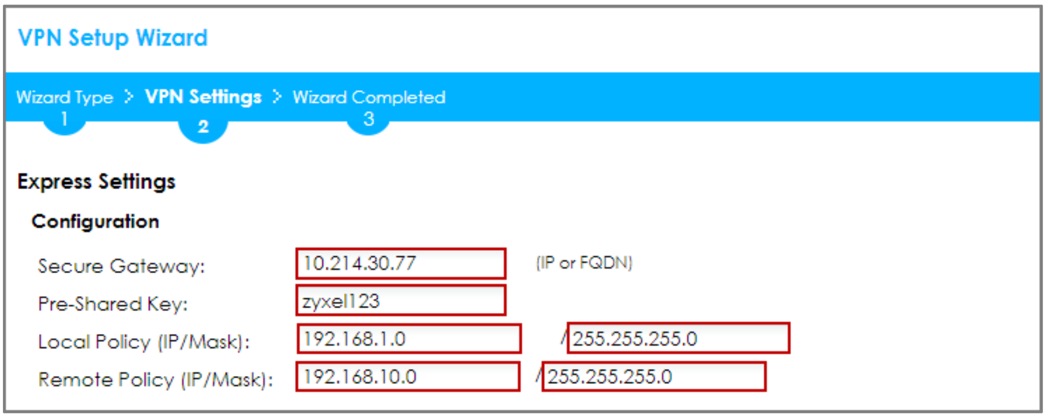
Rule Name: WIZ_VPN_HQ

● Site-to-site
○ Site-to-site with Dynamic Peer
○ Remote Access (Server Role)
○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.100.30.54). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZyWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



Express Settings

Configuration

Secure Gateway: 10.214.30.77 (IP or FQDN)

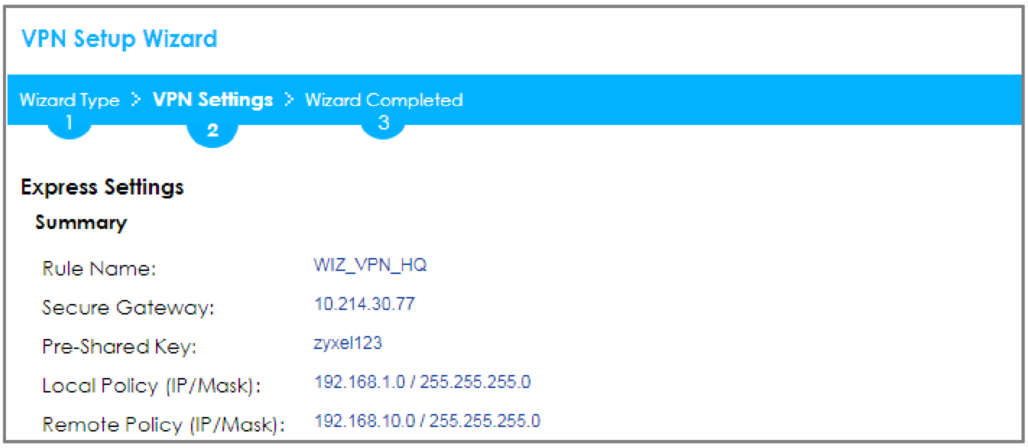
Pre-Shared Key: zyxel123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)


VPN Setup Wizard

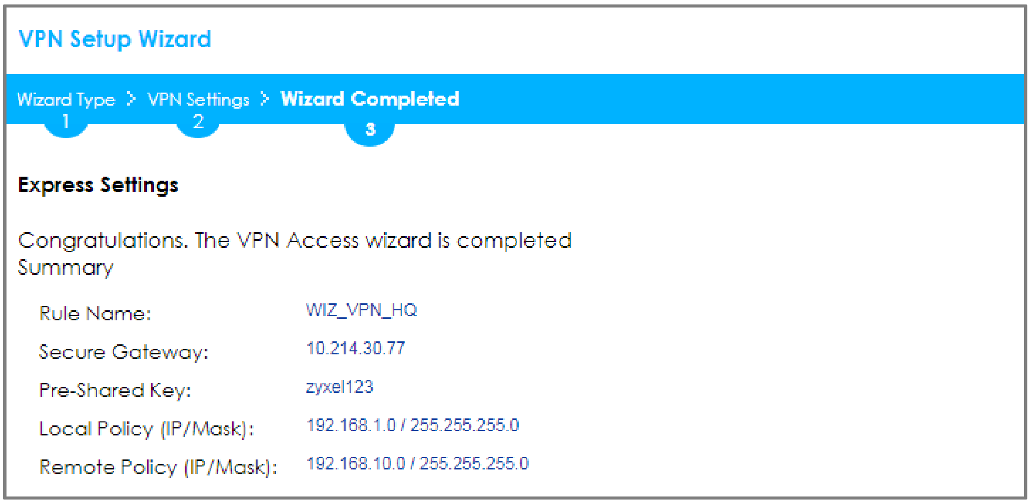
Express Settings

Summary

Rule Name:	WIZ_VPN_HQ
Secure Gateway:	10.214.30.77
Pre-Shared Key:	zyxel123
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed


VPN Setup Wizard

Express Settings

Congratulations. The VPN Access wizard is completed

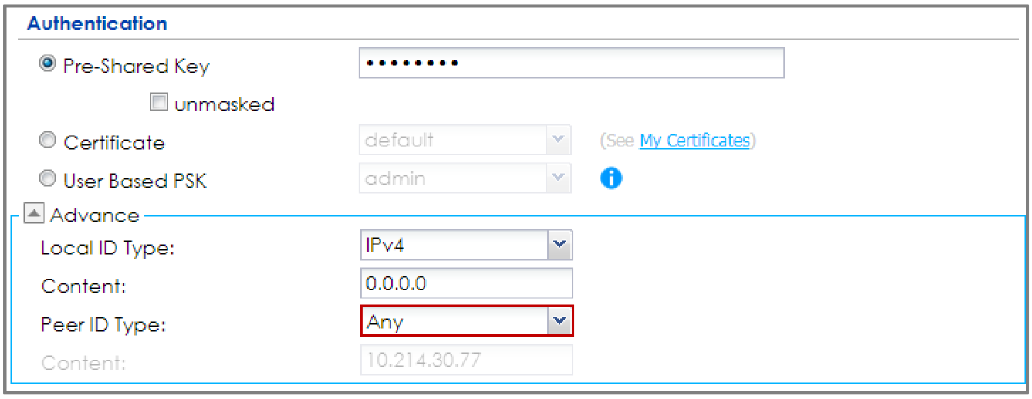
Summary

Rule Name:	WIZ_VPN_HQ
Secure Gateway:	10.214.30.77
Pre-Shared Key:	zyxel123
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the

ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

● Pre-Shared Key ••••••••••

□ unmasked

○ Certificate default (See My Certificates)

○ User Based PSK admin

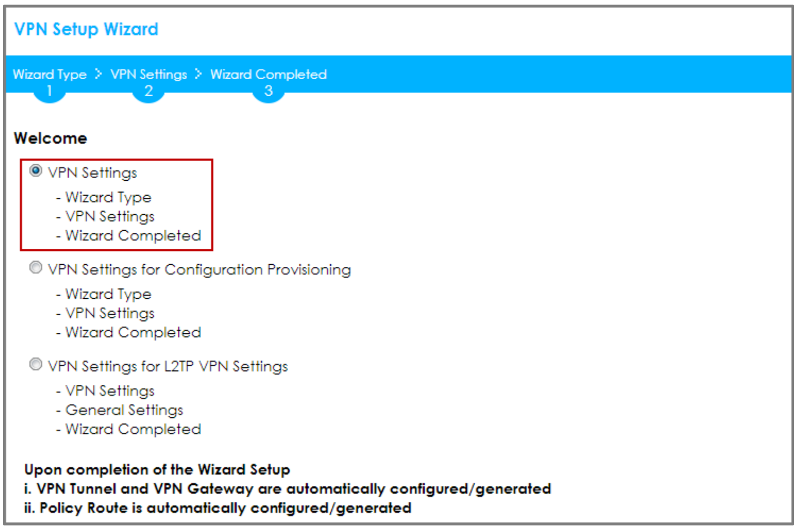
Advance

Local ID Type:	IPv4
Content:	0.0.0.0
Peer ID Type:	Any
Content:	10.214.30.77

Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (Branch)

In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Welcome

● VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

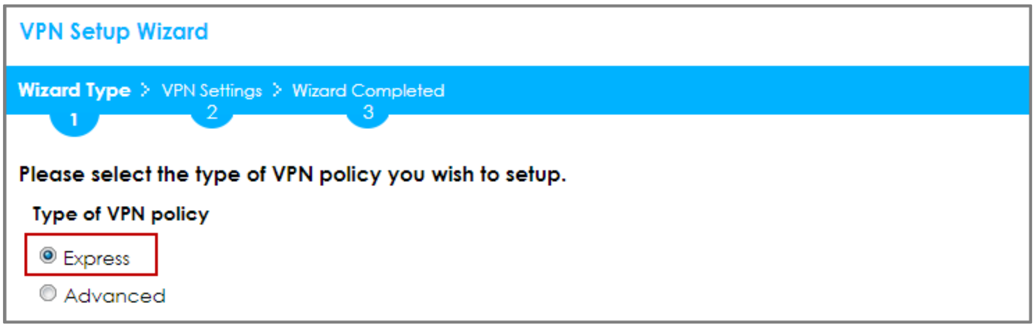
○ VPN Settings for Configuration Provisioning
- Wizard Type
- VPN Settings
- Wizard Completed

○ VPN Settings for L2TP VPN Settings
- VPN Settings
- General Settings
- Wizard Completed

Upon completion of the Wizard Setup
i. VPN Tunnel and VPN Gateway are automatically configured/generated
ii. Policy Route is automatically configured/generated

Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



VPN Setup Wizard

Please select the type of VPN policy you wish to setup.

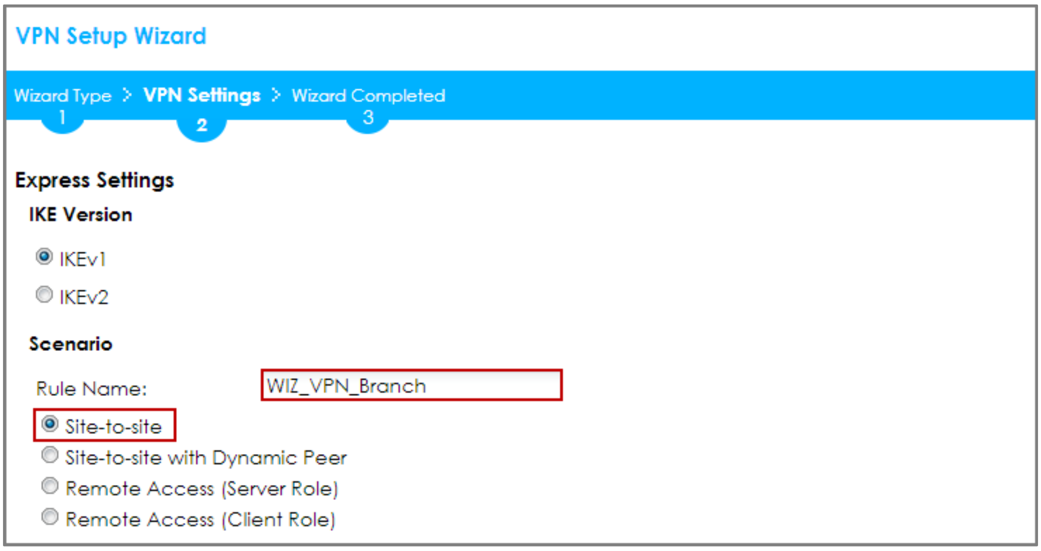
Type of VPN policy

● Express

○ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



VPN Setup Wizard

Express Settings

IKE Version

● IKEv1

○ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch

● Site-to-site

○ Site-to-site with Dynamic Peer

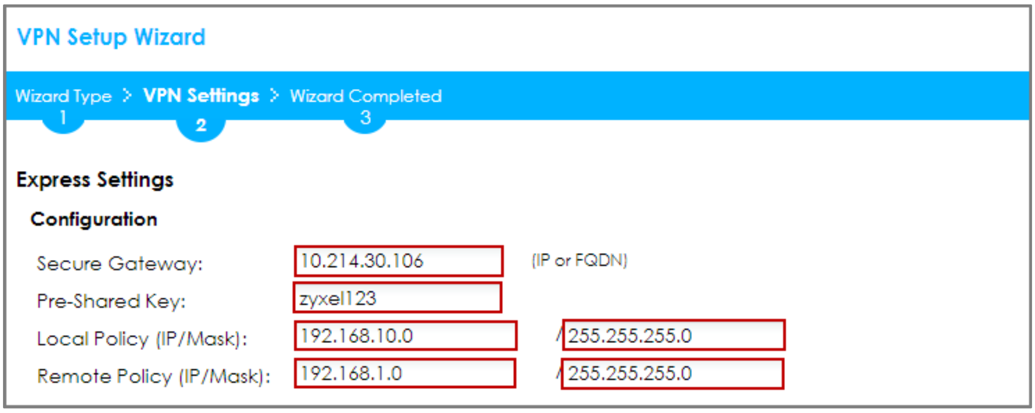
○ Remote Access (Server Role)

○ Remote Access (Client Role)

Configure **Secure Gateway** IP as the peer ZyWALL/USG's WAN IP address (in the example, 172.101.30.68). Type a secure **Pre-Shared Key** (8-32 characters).

Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZYWALL/USG.

Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Configuration)



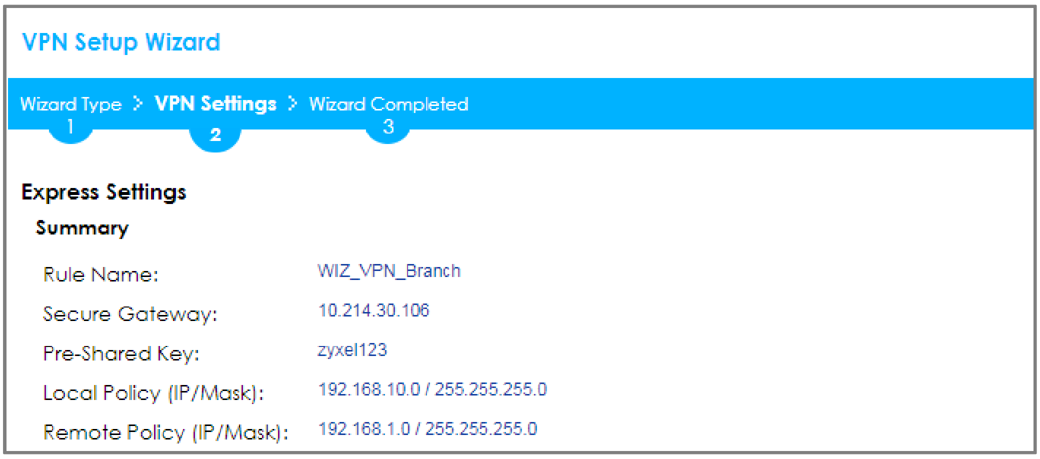
Express Settings

Configuration

Secure Gateway:	10.214.30.106	(IP or FQDN)
Pre-Shared Key:	zyxel123	
Local Policy (IP/Mask):	192.168.10.0	/ 255.255.255.0
Remote Policy (IP/Mask):	192.168.1.0	/ 255.255.255.0

This screen provides a read-only summary of the VPN tunnel. Click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Summary)



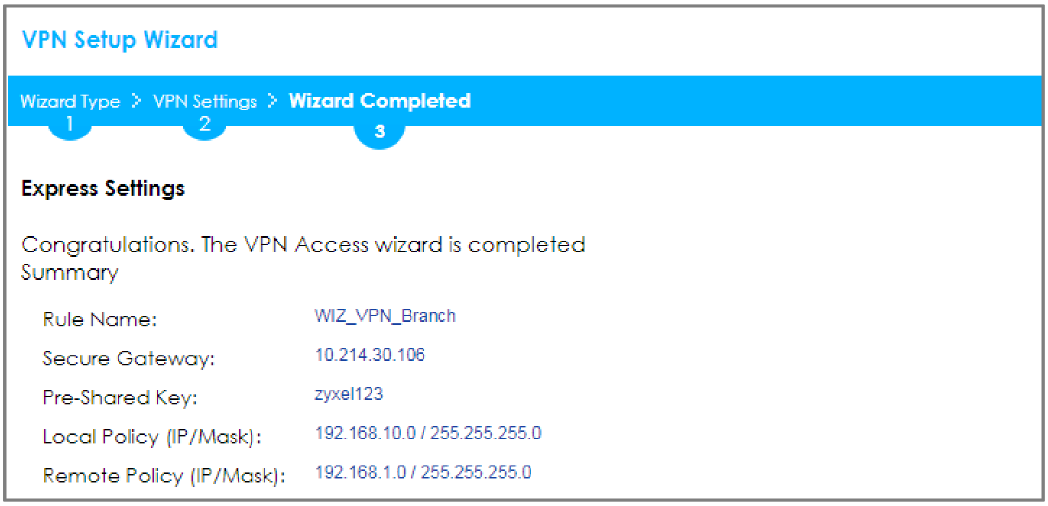
Express Settings

Summary

Rule Name:	WIZ_VPN_Branch
Secure Gateway:	10.214.30.106
Pre-Shared Key:	zyxel123
Local Policy (IP/Mask):	192.168.10.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.1.0 / 255.255.255.0

Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



VPN Setup Wizard

Express Settings

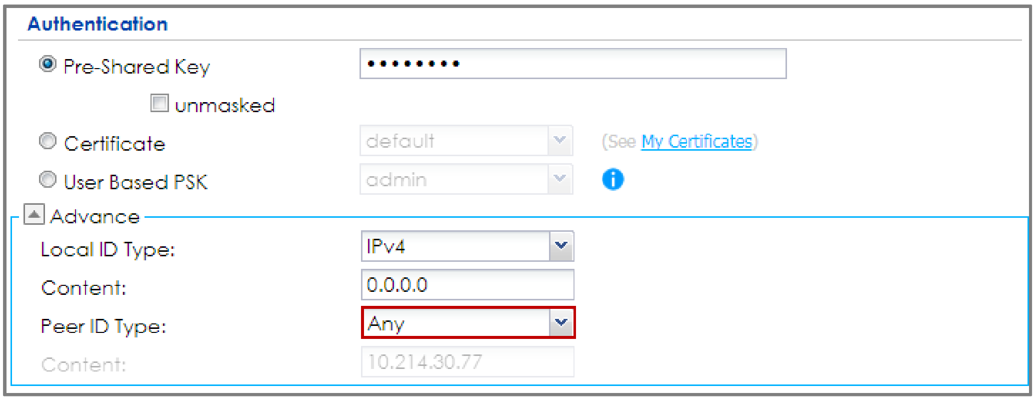
Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_VPN_Branch
Secure Gateway:	10.214.30.106
Pre-Shared Key:	zyxel123
Local Policy (IP/Mask):	192.168.10.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.1.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. **Configure Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Authentication

● Pre-Shared Key: •••••••••

□ unmasked

○ Certificate: default (See My Certificates)

○ User Based PSK: admin

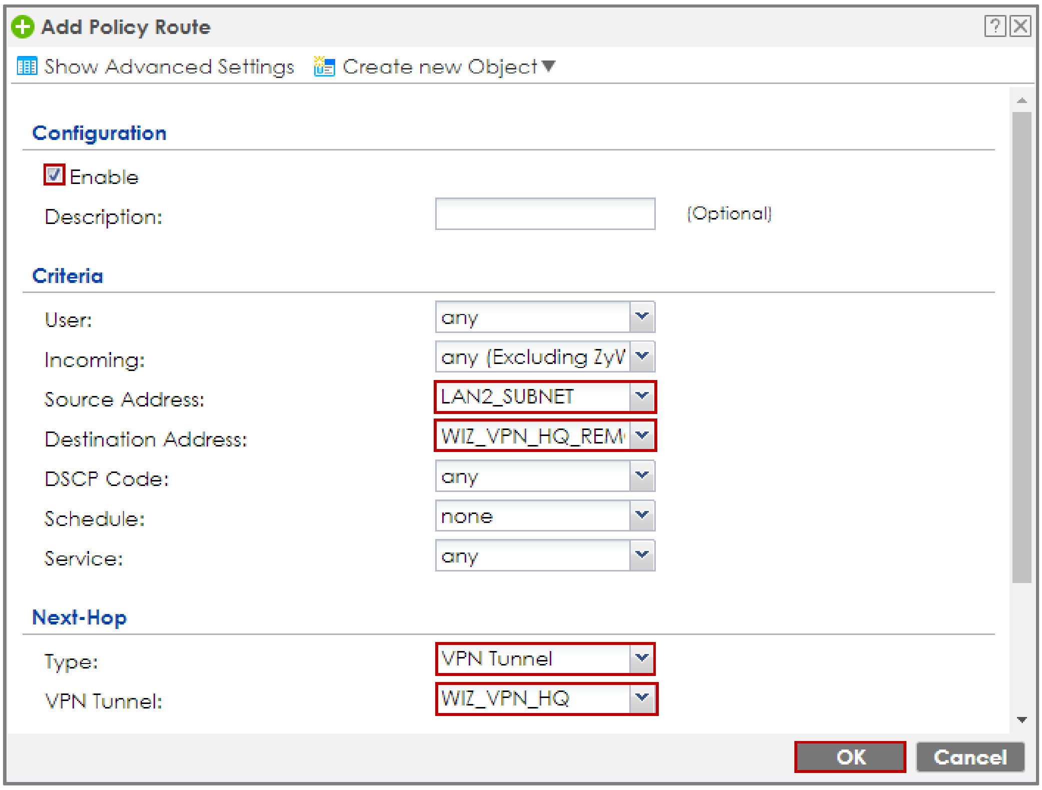
Advance

Local ID Type:	IPv4
Content:	0.0.0.0
Peer ID Type:	Any
Content:	10.214.30.77

Set up the Policy Route (ZyWALL/USG_HQ)

Go to ZyWALL/USG_HQ **CONFIGURATION > Network > Routing > Add**. Set **Source Address** to be the subnet (192.168.2.0/24 in this example) allows joining the VPN tunnel. Set **Destination Address** to be the remote LAN subnet (192.168.10.0/24 in this example).

CONFIGURATION > Network > Routing > Add



Add Policy Route

Show Advanced Settings Create new Object▼

Configuration

☑ Enable

Description: (Optional)

Criteria

User:	any
Incoming:	any (Excluding ZyW
Source Address:	LAN2_SUBNET
Destination Address:	WIZ_VPN_HQ_REM
DSCP Code:	any
Schedule:	none
Service:	any

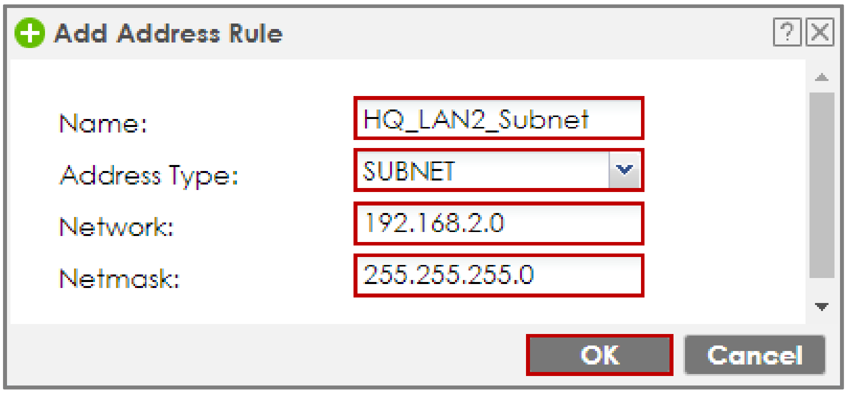
Next-Hop

Type:	VPN Tunnel
VPN Tunnel:	WIZ_VPN_HQ

Set up the Policy Route (ZyWALL/USG_Branch)

Go to ZyWALL/USG_Branch **CONFIGURATION > Network > Routing > Add**, create **Address** to be the remote LAN subnet (192.168.2.0/24 in this example) allows joining the VPN tunnel.

CONFIGURATION > Object > Address > Add



Add Address Rule

Name: HQ_LAN2_Subnet

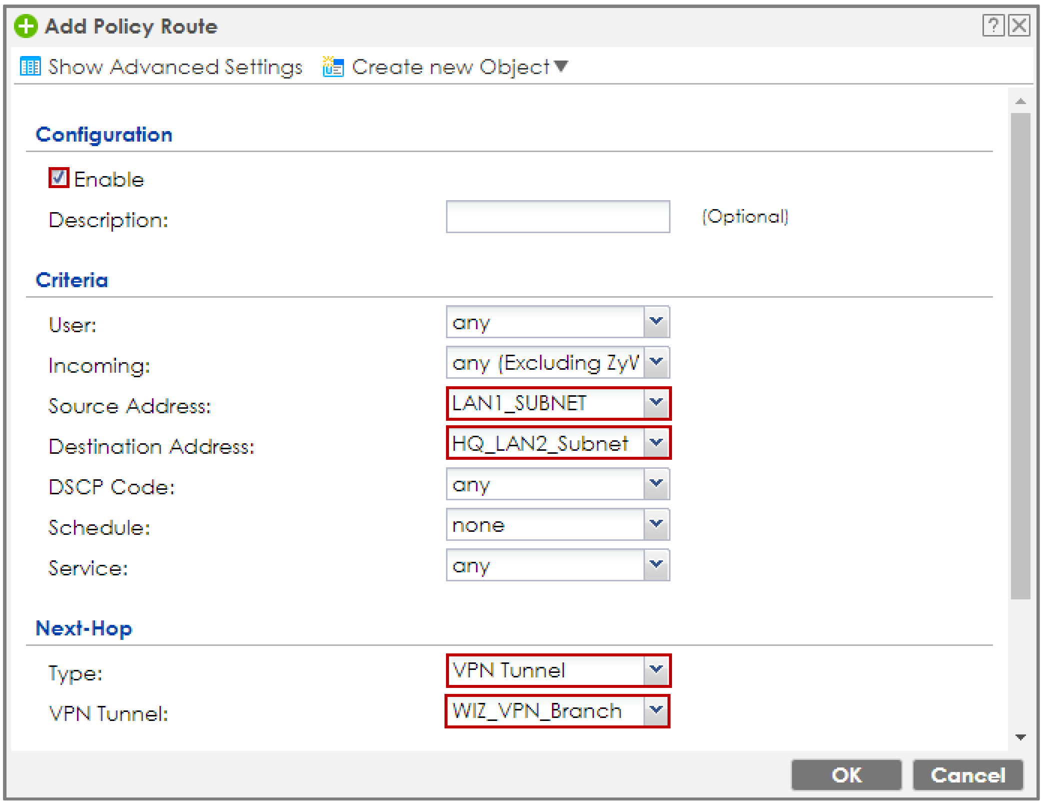
Address Type: SUBNET

Network: 192.168.2.0

Netmask: 255.255.255.0

Go to ZyWALL/USG_Branch **CONFIGURATION > Network > Routing > Add**. Set **Source Address** to be the local subnet (192.168.10.0/24 in this example). Set **Destination Address** to be the remote LAN subnet (192.168.2.0/24 in this example) allows joining the VPN tunnel.

CONFIGURATION > Network > Routing > Add



Add Policy Route

Configuration

☑ Enable

Description: (Optional)

Criteria

User: any

Incoming: any (Excluding ZyW

Source Address: LAN1_SUBNET

Destination Address: HQ_LAN2_Subnet

DSCP Code: any

Schedule: none

Service: any

Next-Hop

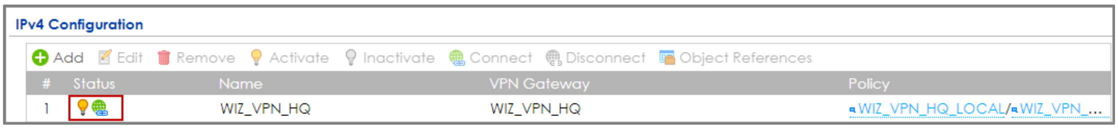
Type: VPN Tunnel

VPN Tunnel: WIZ_VPN_Branch

Test the IPSec VPN Tunnel

Go to ZYWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

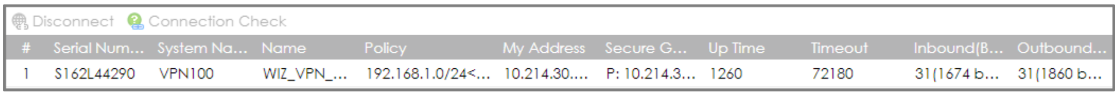


IPv4 Configuration

#	Status	Name	VPN Gateway	Policy
1	💡●	WIZ_VPN_HQ	WIZ_VPN_HQ	WIZ_VPN_HQ_LOCAL/WIZ_VPN_...

Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** Traffic.

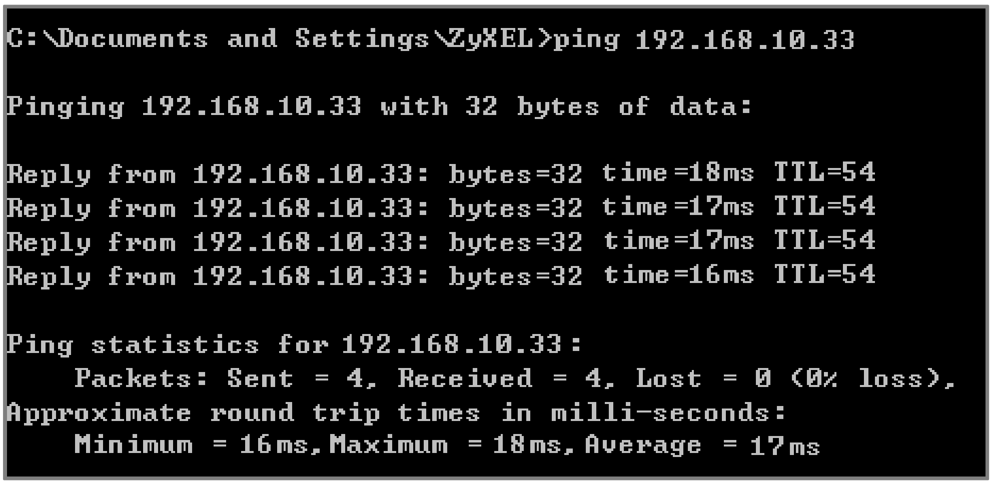
MONITOR > VPN Monitor > IPSec



#	Serial Num...	System Na...	Name	Policy	My Address	Secure G...	Up Time	Timeout	Inbound(B...	Outbound...
1	S162L44290	VPN100	WIZ_VPN_...	192.168.1.0/24<...	10.214.30....	P: 10.214.3...	1260	72180	31(1674 b...	31(1860 b...

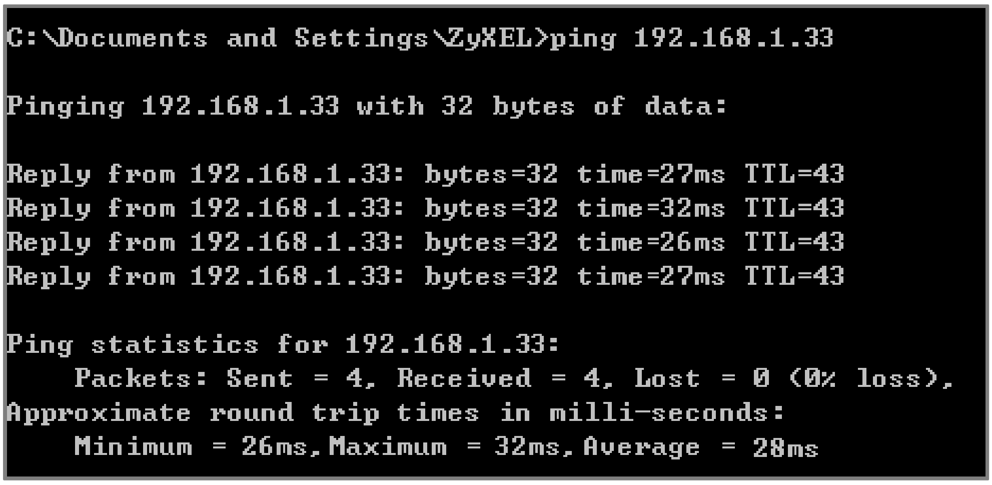
To test whether or not a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC at HQ Office > Window 7 > cmd > ping 192.168.10.33



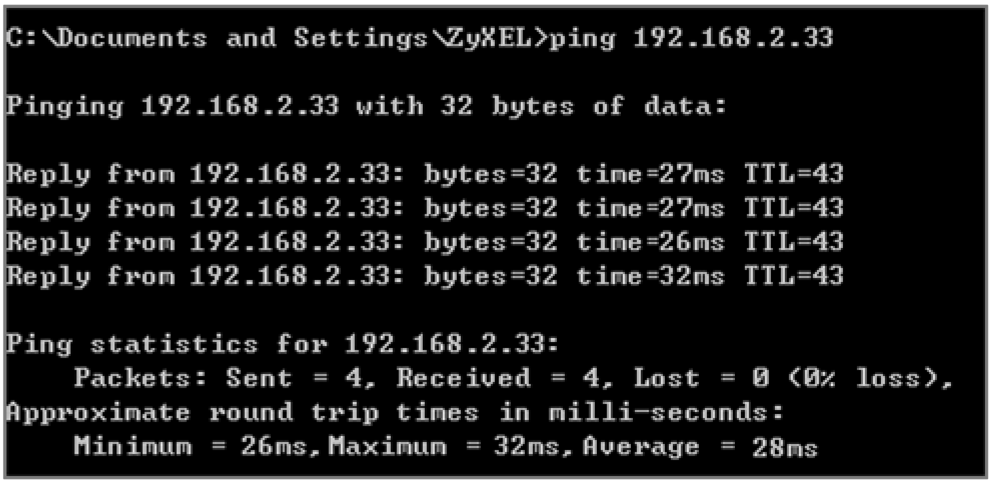
```
C:\Documents and Settings\ZyXEL>ping 192.168.10.33

Pinging 192.168.10.33 with 32 bytes of data:

Reply from 192.168.10.33: bytes=32 time=18ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=17ms TTL=54
Reply from 192.168.10.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.10.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC at Branch Office > Window 7 > cmd > ping 192.168.1.33



```
C:\Documents and Settings\ZyXEL>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

PC at Branch Office > Window 7 > cmd > ping 192.168.2.33

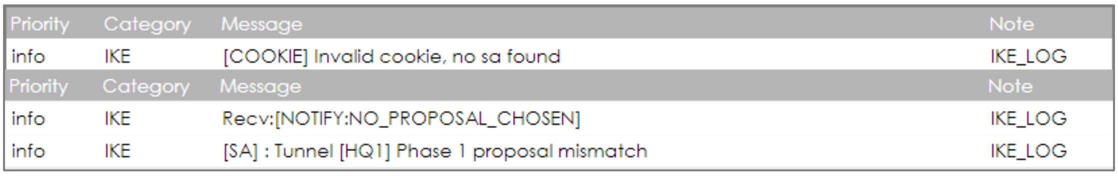


```
C:\Documents and Settings\ZyXEL>ping 192.168.2.33

Pinging 192.168.2.33 with 32 bytes of data:

Reply from 192.168.2.33: bytes=32 time=27ms TTL=43
Reply from 192.168.2.33: bytes=32 time=27ms TTL=43
Reply from 192.168.2.33: bytes=32 time=26ms TTL=43
Reply from 192.168.2.33: bytes=32 time=32ms TTL=43

Ping statistics for 192.168.2.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

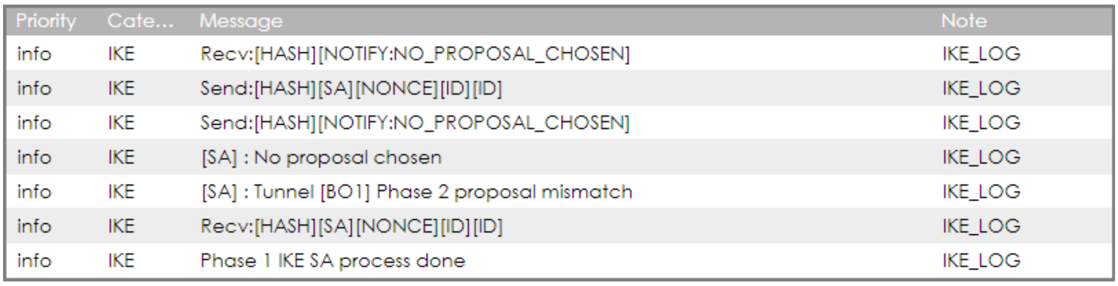
MONITOR > Log



Priority	Category	Message	Note
info	IKE	[COOKIE] Invalid cookie, no sa found	IKE_LOG
Priority	Category	Message	Note
info	IKE	Recv:[NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : Tunnel [HQ1] Phase 1 proposal mismatch	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log



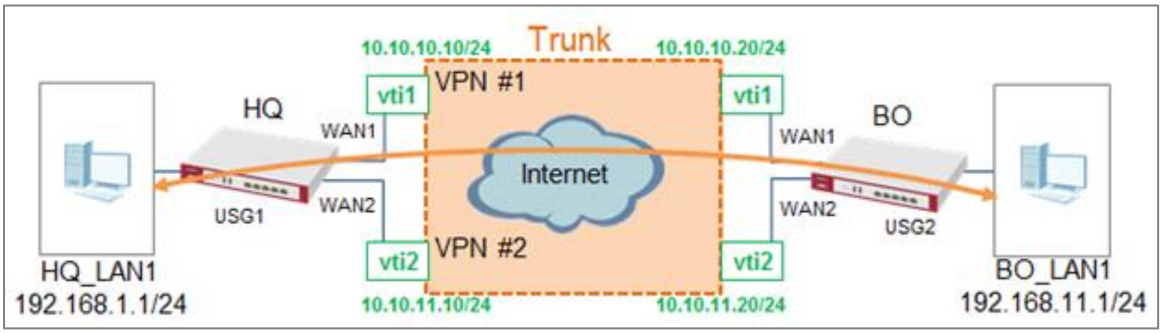
Priority	Cate...	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [BO1] Phase 2 proposal mismatch	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Phase 1 IKE SA process done	IKE_LOG

Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Create VTI and Configure VPN Failover with VTI

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.



VPN Load Balance with VTI

> 💡Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

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.

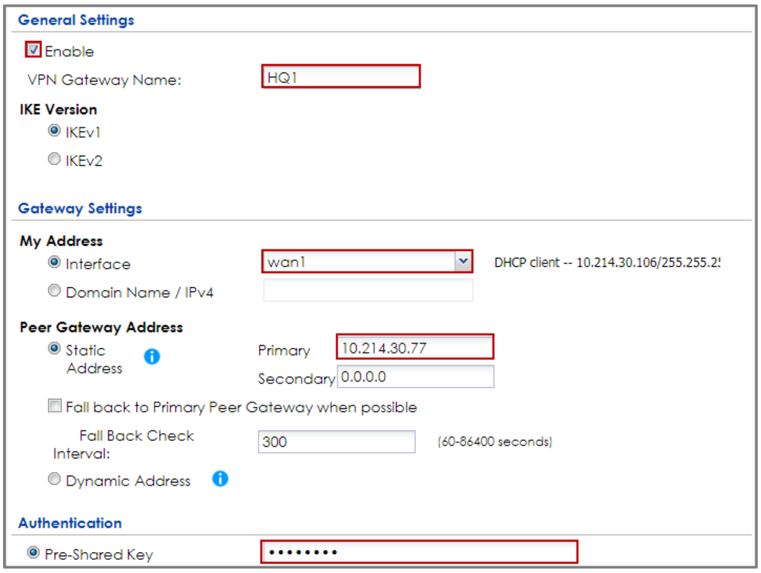
5 Configure a policy route.

6 Connect the VPN tunnels.

Set Up the ZyWALL/USG VTI of Corporate Network (HQ)

1 In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add** to create the VPN gateway **HQ1** with **wan1**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add



General Settings

☑ Enable

VPN Gateway Name: HQ1

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface: wan1 DHCP client -- 10.214.30.106/255.255.2!

○ Domain Name / IPv4

Peer Gateway Address

● Static Address — Primary: 10.214.30.77 — Secondary: 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

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

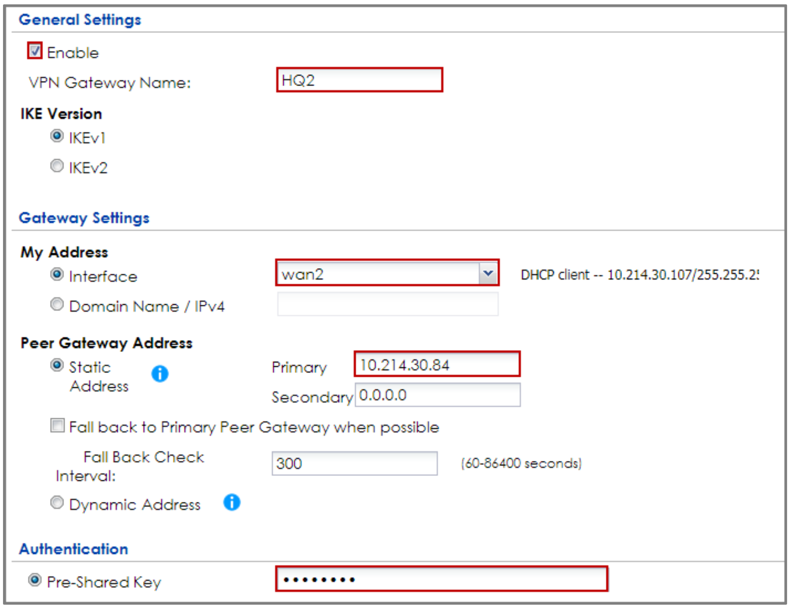
○ Dynamic Address

Authentication

● Pre-Shared Key: ••••••••

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

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add



General Settings

☑ Enable

VPN Gateway Name: HQ2

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface: wan2 DHCP client -- 10.214.30.107/255.255.2!

○ Domain Name / IPv4

Peer Gateway Address

● Static Address — Primary: 10.214.30.84 — Secondary: 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

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

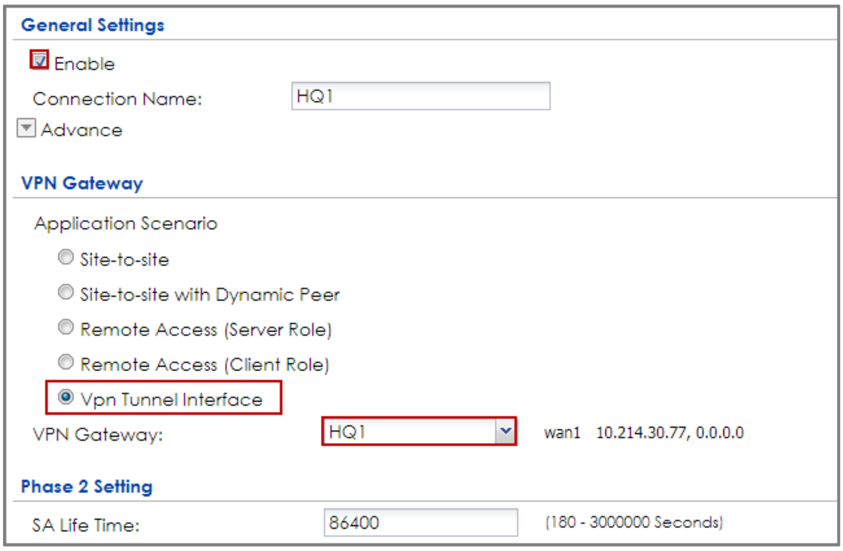
○ Dynamic Address

Authentication

● Pre-Shared Key: ••••••••

3 Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add** and configure a VPN tunnel for the VPN gateway **HQ1**. Select **VPN Tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add



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

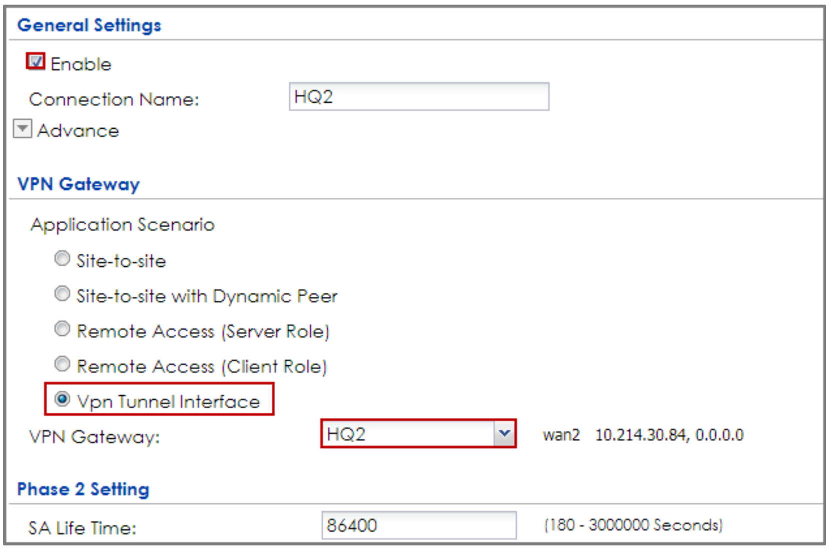
VPN Gateway: HQ1 wan1 10.214.30.77, 0.0.0.0

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

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

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add



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

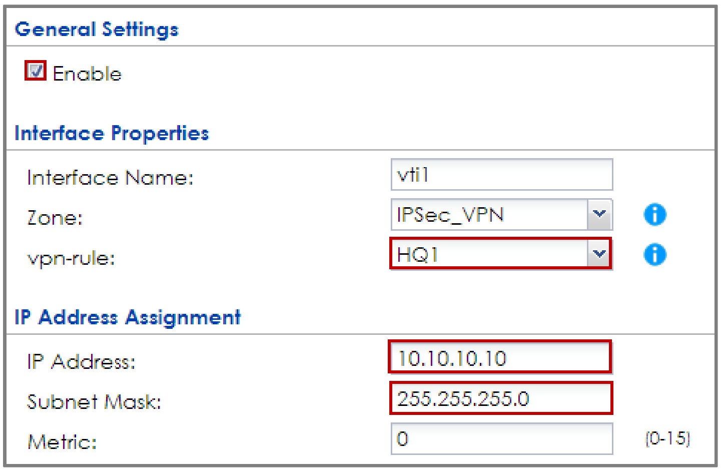
VPN Gateway: HQ2 wan2 10.214.30.84, 0.0.0.0

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

5 Go to **CONFIGURATION > Network > Interface > VTI > Add** to create a VTI for the VPN tunnel **HQ1**. Enable the connectivity check. Enter the IP address of **vti1**, which is configured on **USG2**.

CONFIGURATION > Network > Interface > VTI > Add



General Settings

☑ Enable

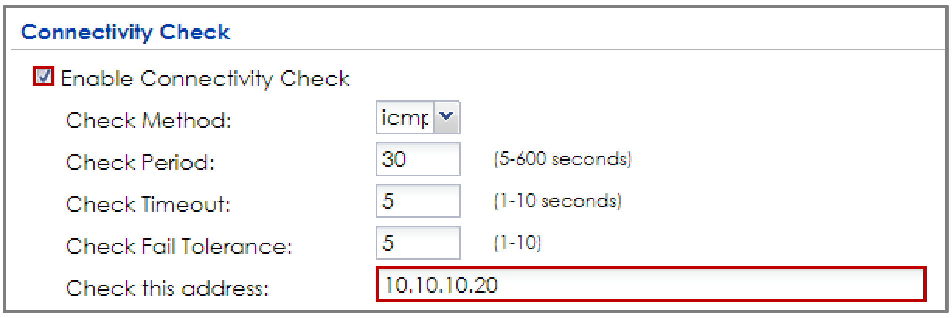
Interface Properties

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)

CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check



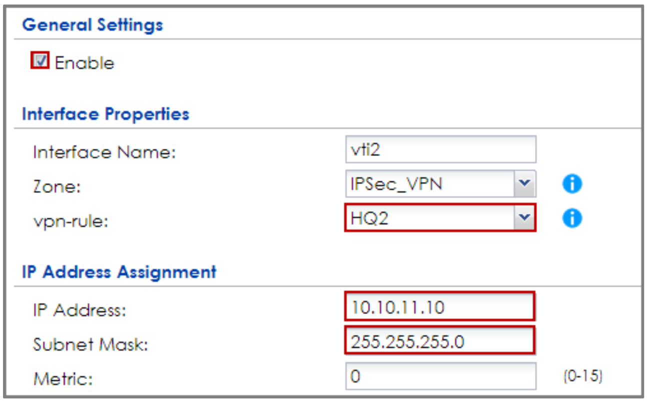
Connectivity Check

☑ 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

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

CONFIGURATION > Network > Interface > VTI > Add



General Settings

☑ Enable

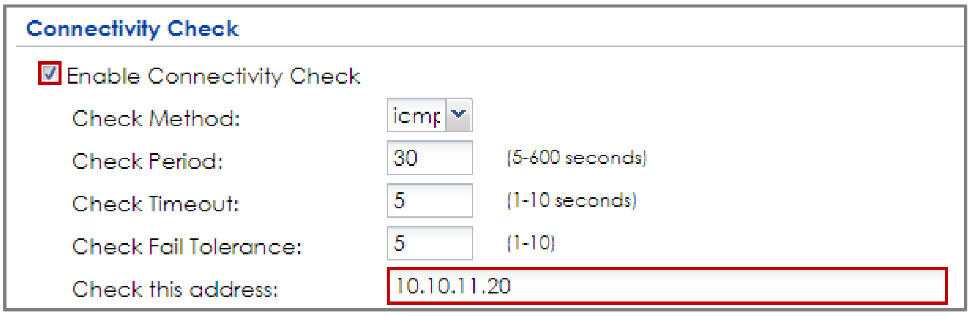
Interface Properties

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)

CONFIGURATION > Network > Interface > VTI > vti2 > Connectivity Check



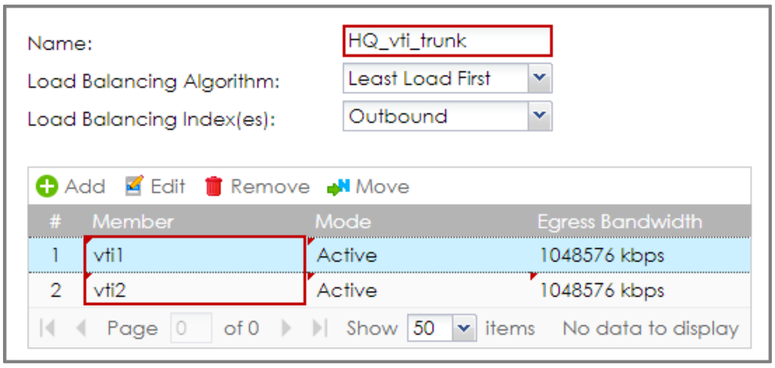
Connectivity Check

☑ 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	

7 Go to **CONFIGURATION > Network > Interface > Trunk > User Configuration > Add** to create a new trunk. Add **vti1** and **vti2** to the new trunk.

CONFIGURATION > Network > Interface > Trunk > User Configuration > Add



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

#	Member	Mode	Egress Bandwidth
1	vti1	Active	1048576 kbps
2	vti2	Active	1048576 kbps

8 Go to **CONFIGURATION > Network > Routing > Policy Route > Add** to configure a policy route.

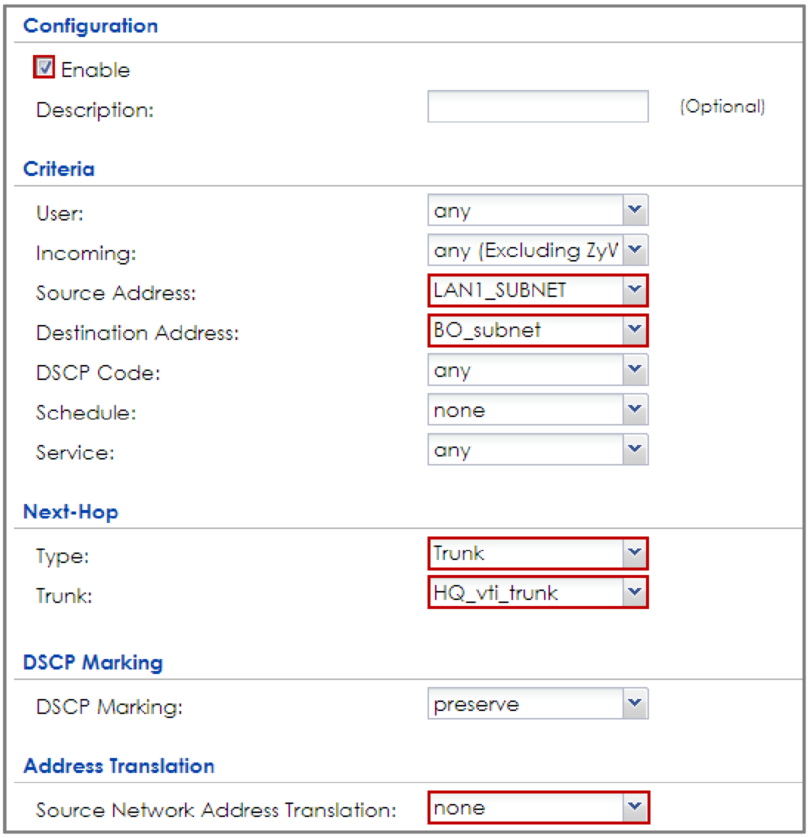
Source Address: LAN1_SUBNET (192.168.1.0/24)

Destination Address: BO_subnet (192.168.11.0/24)

Next-Hop: HQ_vti_trunk

SNAT: none

CONFIGURATION > Network > Routing > Policy Route > Add



Configuration

☑ Enable

Description: (Optional)

Criteria

User:	any
Incoming:	any (Excluding ZyV
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

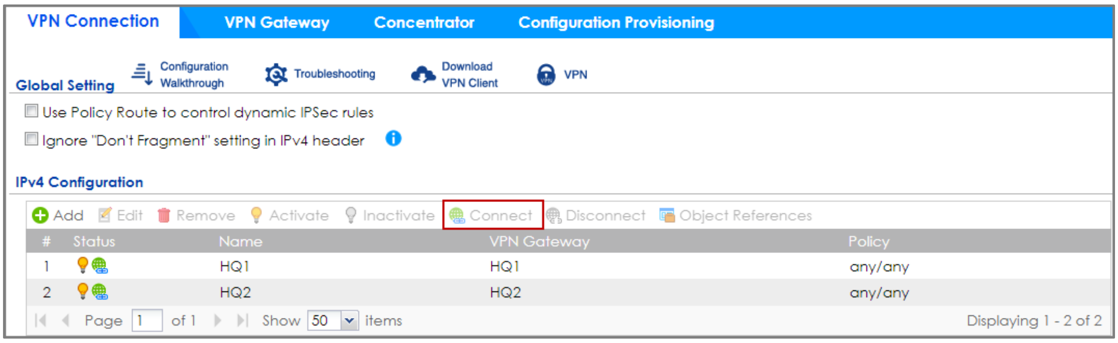
DSCP Marking: preserve

Address Translation

Source Network Address Translation: none

9 Connect the VPN tunnels when the VTIs are ready. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to connect the VPN tunnels.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Connect



Global Setting

□ Use Policy Route to control dynamic IPSec rules

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

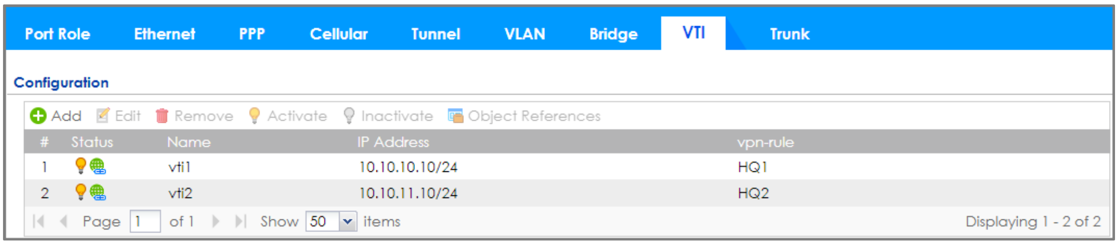
IPv4 Configuration

#	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

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

CONFIGURATION > Network > Interface > VTI



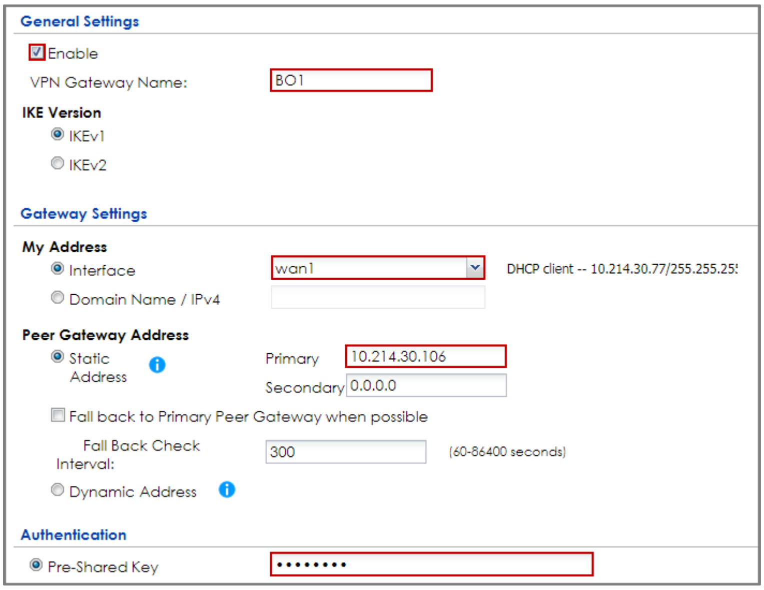
#	Status	Name	IP Address	vpn-rule
1	💡	vti1	10.10.10.10/24	HQ1
2	💡	vti2	10.10.11.10/24	HQ2

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

Set Up the ZyWALL/USG VTI of Corporate Network (Branch)

1 In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add** to create the VPN gateway **BO1** with **wan1**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add



General Settings

☑ Enable

VPN Gateway Name: BO1

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface wan1 DHCP client -- 10.214.30.77/255.255.25

○ Domain Name / IPv4

Peer Gateway Address

● Static Address Primary 10.214.30.106

Secondary 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

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

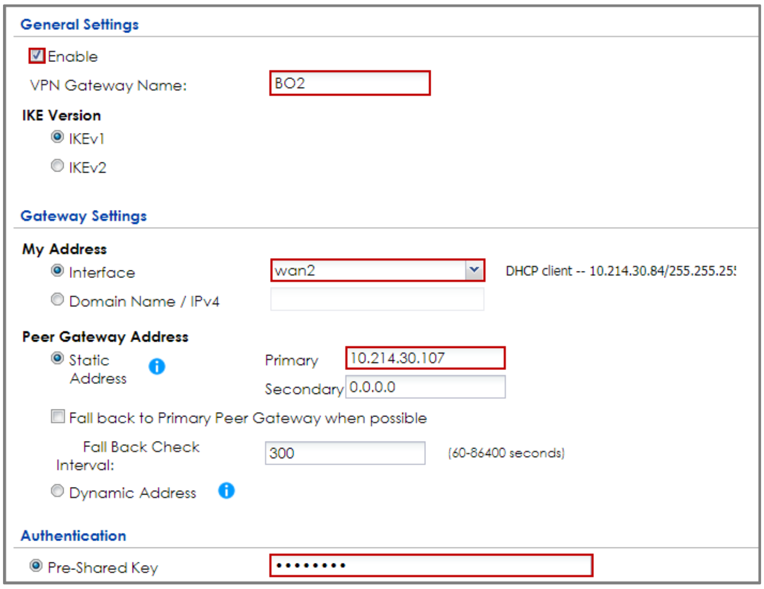
○ Dynamic Address

Authentication

● Pre-Shared Key ••••••••

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

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add



General Settings

☑ Enable

VPN Gateway Name: BO2

IKE Version

● IKEv1

○ IKEv2

Gateway Settings

My Address

● Interface wan2 DHCP client -- 10.214.30.84/255.255.25

○ Domain Name / IPv4

Peer Gateway Address

● Static Address Primary 10.214.30.107

Secondary 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

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

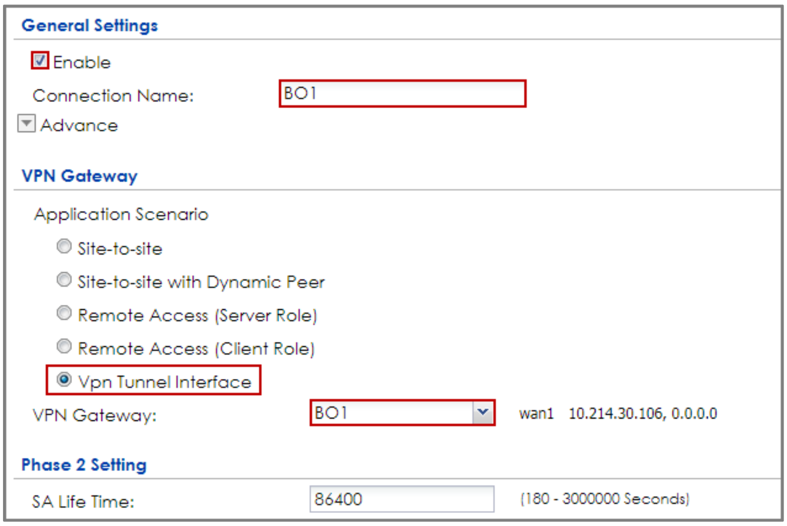
○ Dynamic Address

Authentication

● Pre-Shared Key ••••••••

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

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add



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

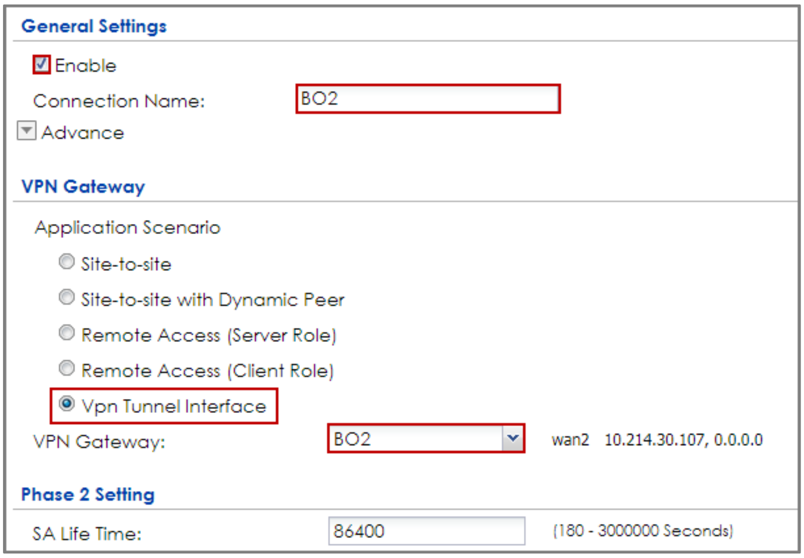
VPN Gateway: BO1 wan1 10.214.30.106, 0.0.0.0

Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

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

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add



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 10.214.30.107, 0.0.0.0

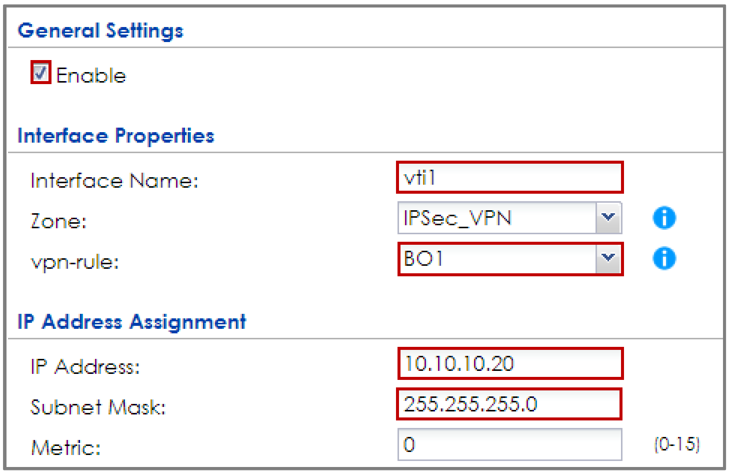
Phase 2 Setting

SA Life Time: 86400 (180 - 3000000 Seconds)

5 Go to **CONFIGURATION > Network > Interface > VTI > Add** to create a VTI for the VPN tunnel **BO1**. 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**. Enable the connectivity check. Enter the IP address of **vti1**, which is configured on **USG1**.

CONFIGURATION > Network > Interface > VTI > Add



General Settings

☑ Enable

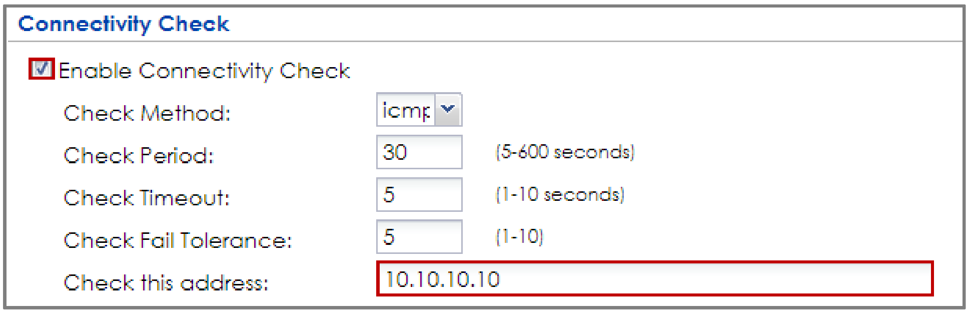
Interface Properties

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)

CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check



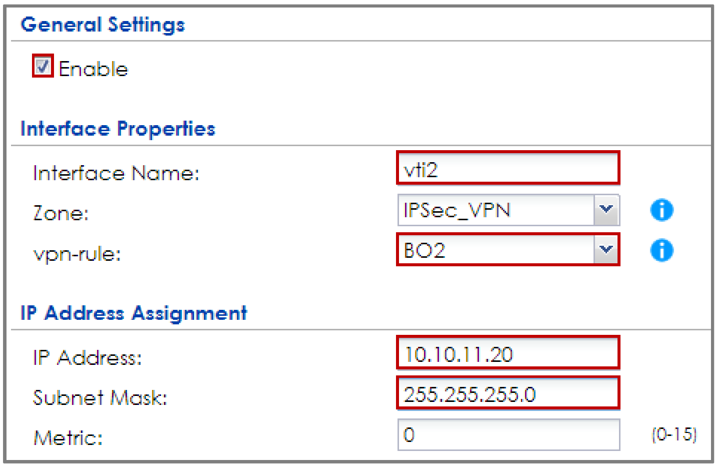
Connectivity Check

☑ 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	

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

CONFIGURATION > Network > Interface > VTI > Add



General Settings

☑ Enable

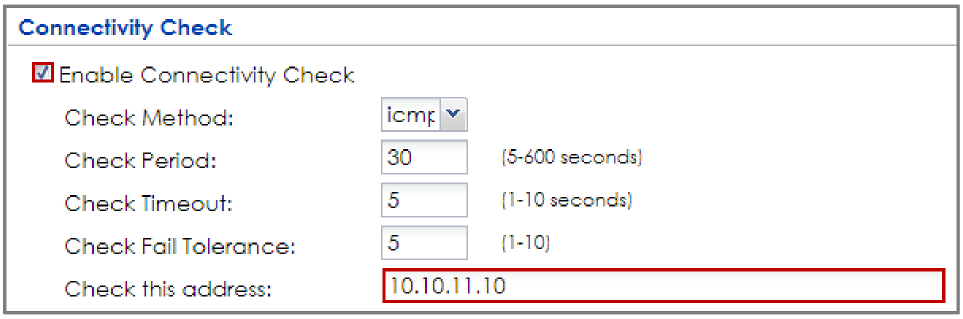
Interface Properties

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)

CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check



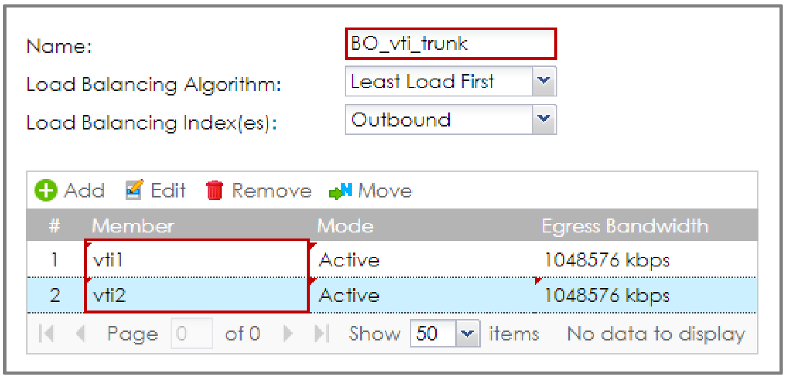
Connectivity Check

☑ 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	

7 Go to **CONFIGURATION > Network > Interface > Trunk > User Configuration > Add** to create a new trunk. Add **vti1** and **vti2** to the new trunk.

CONFIGURATION > Network > Interface > Trunk > User Configuration > Add



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

#	Member	Mode	Egress Bandwidth
1	vti1	Active	1048576 kbps
2	vti2	Active	1048576 kbps

8 Go to **CONFIGURATION > Network > Routing > Policy Route > Add** to configure a policy route.

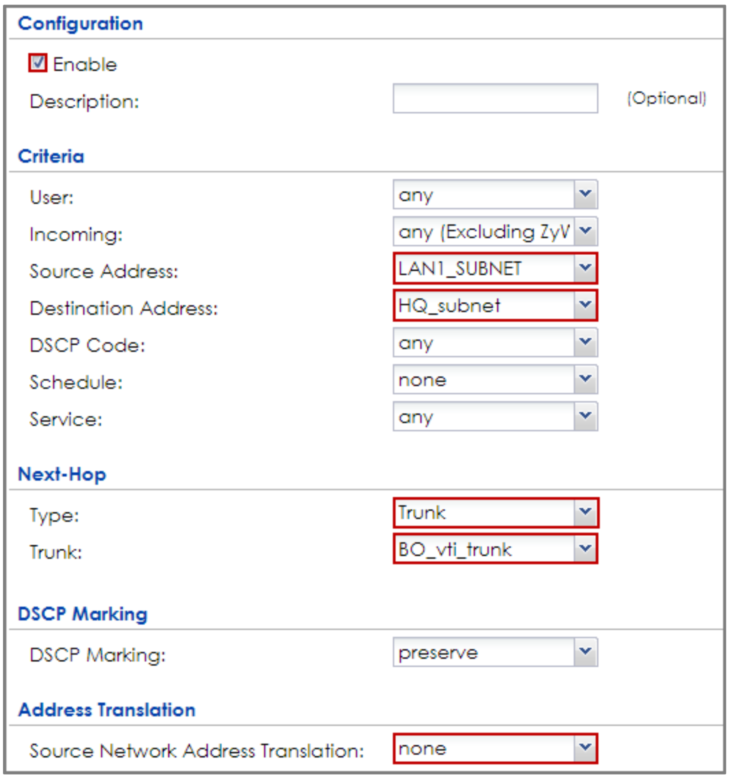
Source Address: LAN1_SUBNET (192.168.11.0/24)

Destination Address: HQ_subnet (192.168.1.0/24)

Next-Hop: BO_vti_trunk

SNAT: none

CONFIGURATION > Network > Routing > Policy Route > Add



Configuration

☑ Enable

Description: (Optional)

Criteria

User: any

Incoming: any (Excluding ZyV

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

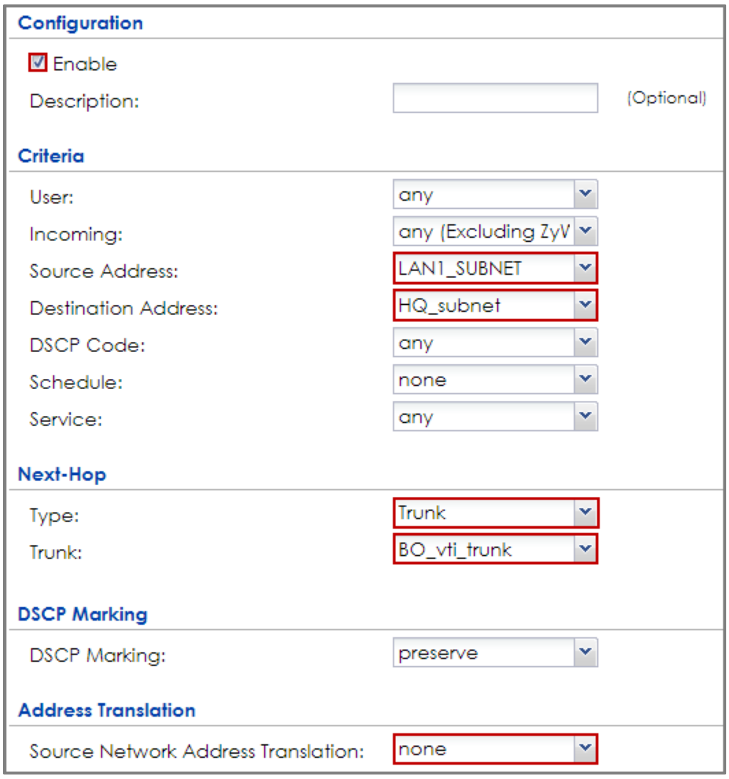
DSCP Marking: preserve

Address Translation

Source Network Address Translation: none

9 Connect the VPN tunnels when the VTIs are ready. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to connect the VPN tunnels.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Connect



Configuration

☑ Enable

Description:		(Optional)

Criteria

User:	any
Incoming:	any (Excluding ZyV
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

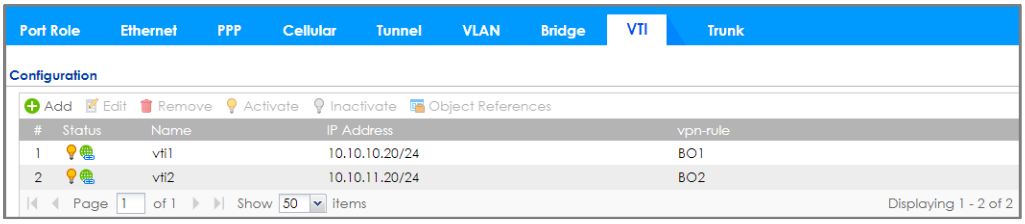
DSCP Marking:	preserve

Address Translation

Source Network Address Translation:	none

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

CONFIGURATION > Network > Interface > VTI



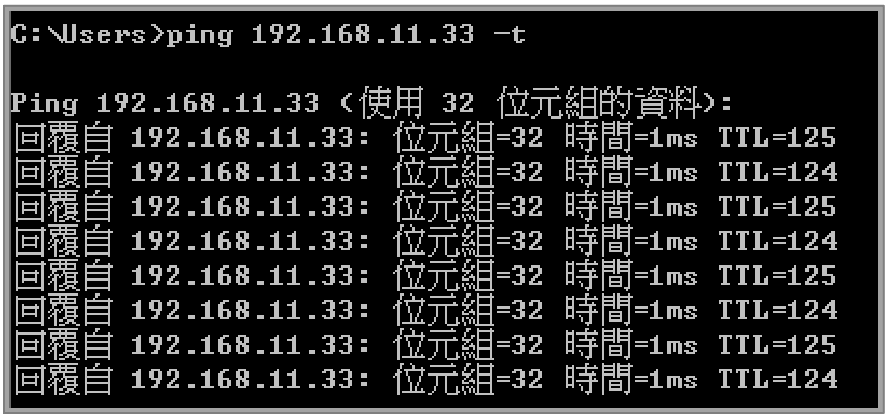
#	Status	Name	IP Address	vpn-rule
1		vti1	10.10.10.20/24	BO1
2		vti2	10.10.11.20/24	BO2

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

Test the IPSec VPN Tunnel

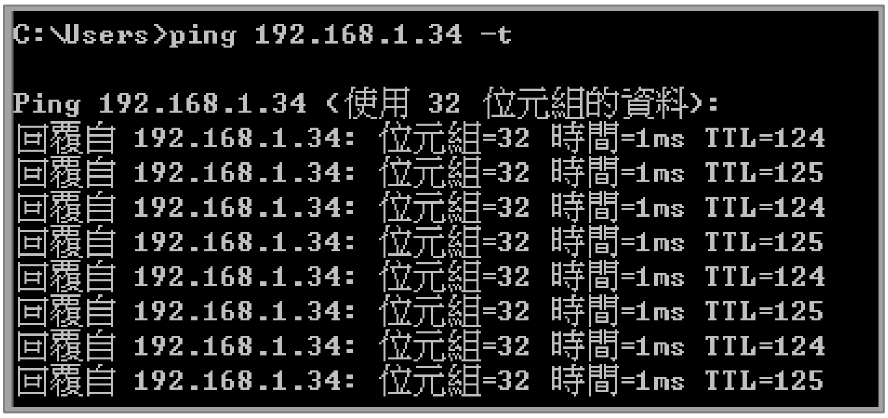
1 To test whether or not a tunnel is working, ping from a PC in LAN1 of USG1 to a PC in LAN1 of USG2 and vice versa.

PC of USG1 (192.168.1.34) > Window 7 > cmd > ping 192.168.11.33



```
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
```

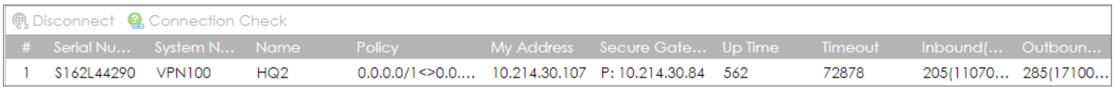
PC of USG2 (192.168.11.33) > Window 7 > cmd > ping 192.168.1.34



```
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
```

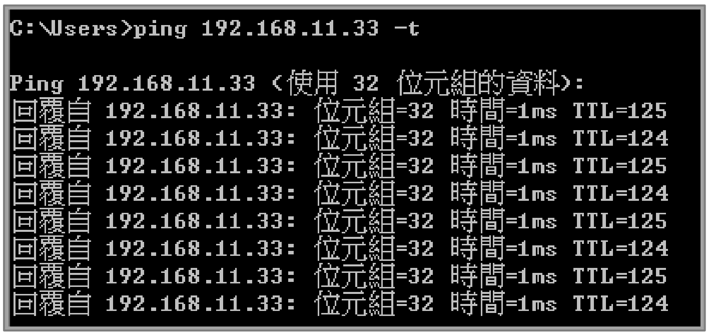
2 To test whether or not VPN failover is working, unplug wan1 of USG1. Then ping from a PC in LAN1 of USG1 to a PC in LAN1 of USG2 and vice versa.

Check the VPN status of the USG1 in the MONITOR > VPN Monitor > IPSec screen.



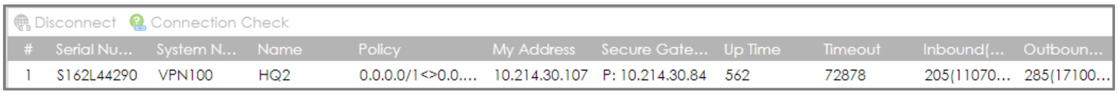
#	Serial Nu...	System N...	Name	Policy	My Address	Secure Gate...	Up Time	Timeout	Inbound(...	Outboun...
1	S162L44290	VPN100	HQ2	0.0.0.0/1<>0.0....	10.214.30.107	P: 10.214.30.84	562	72878	205(11070...	285(17100...

PC of USG1 (192.168.1.34) > Window 7 > cmd > ping 192.168.11.33



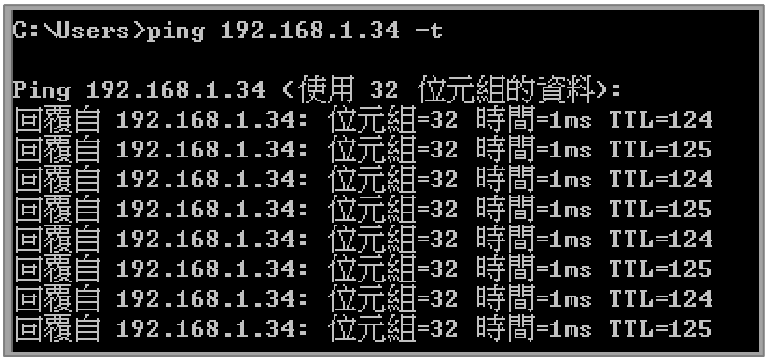
```
C:\Users>ping 192.168.11.33 -t

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 VPN status of the USG2 in the MONITOR > VPN Monitor > IPSec screen.



#	Serial Nu...	System N...	Name	Policy	My Address	Secure Gate...	Up Time	Timeout	Inbound(...	Outboun...
1	S162L44290	VPN100	HQ2	0.0.0.0/1<>0.0....	10.214.30.107	P: 10.214.30.84	562	72878	205(11070...	285(17100...

PC of USG2 (192.168.11.33) > Window 7 > cmd > ping 192.168.1.34

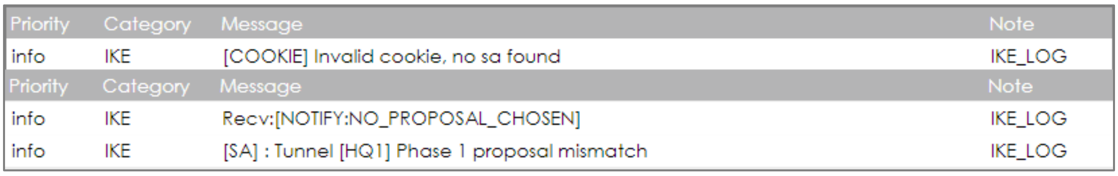


```
C:\Users>ping 192.168.1.34 -t

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
```

What Can Go Wrong?

1 If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

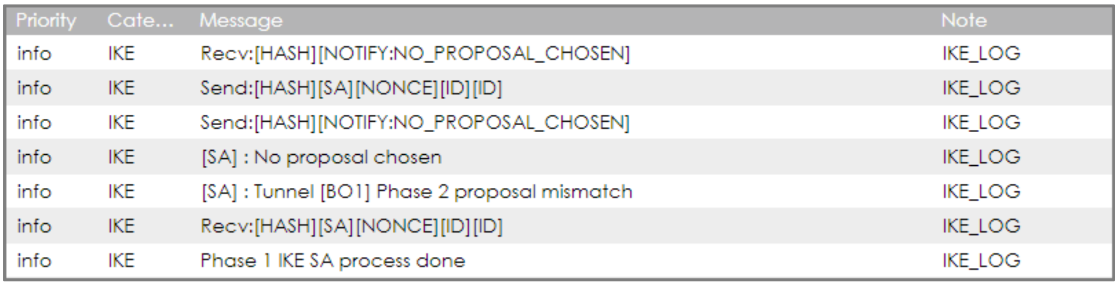
MONITOR > Log



Priority	Category	Message	Note
info	IKE	[COOKIE] Invalid cookie, no sa found	IKE_LOG
Priority	Category	Message	Note
info	IKE	Recv:[NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : Tunnel [HQ1] Phase 1 proposal mismatch	IKE_LOG

2 If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log



Priority	Cate...	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [BO1] Phase 2 proposal mismatch	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Phase 1 IKE SA process done	IKE_LOG

3 Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

4 Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

5 Make sure the both ZyWALL/USG at the HQ and Branch sites use static IP address because VPN Tunnel Interface does not support dynamic peer.

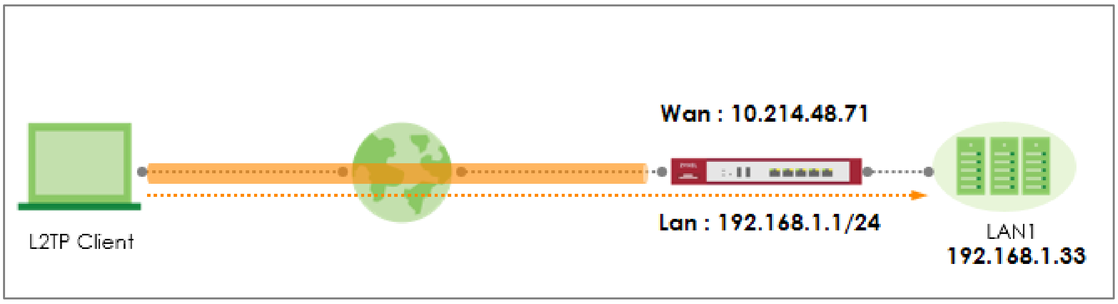
6 Make sure policy routes are configured to control traffic between the subnet of HQ and Branch through VTI.

7 Make sure that the IP address of VTI at the Branch must be in the same subnet as vti1 on HQ. For example, the IP address and subnet mask of vti1 on HQ is 10.10.10.10 and 255.255.255.0 respectively. The IP address of vti1 on the Branch must be in the subnet of 10.10.10.0/24; the IP address and subnet mask of vti2 on HQ is 10.10.11.10 and 255.255.255.0 respectively. The IP address of vti2 on the Branch must be in the subnet of 10.10.10.0/24, and so on.

Remote access VPN Wizard

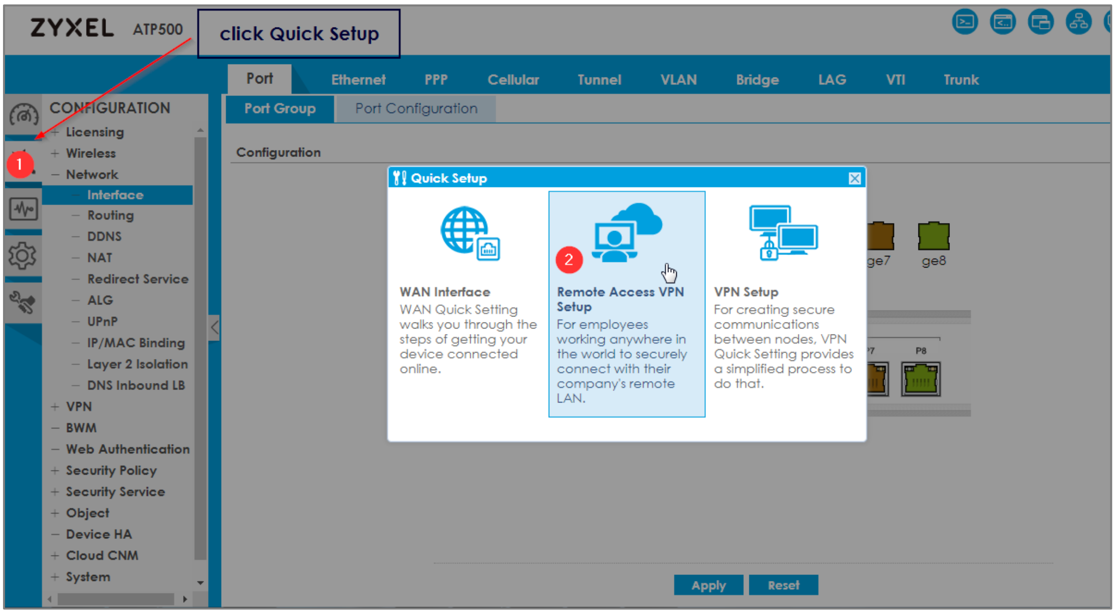
The following is a sample configuration how to build up VPN tunnel with the remote access VPN wizard.

Remote access VPN Wizard is an easy way to quick set up VPN tunnel. Do not need complex configuration to build up VPN tunnel, all you need is to follow the steps on the VPN Wizard. Here are the steps to build L2TP over IPSec VPN tunnel for example.



Set up VPN Tunnel

1. In the ZyWALL/USG, Click Quick Setup, then click Remote Access VPN Setup build up VPN tunnel with the Wizard.

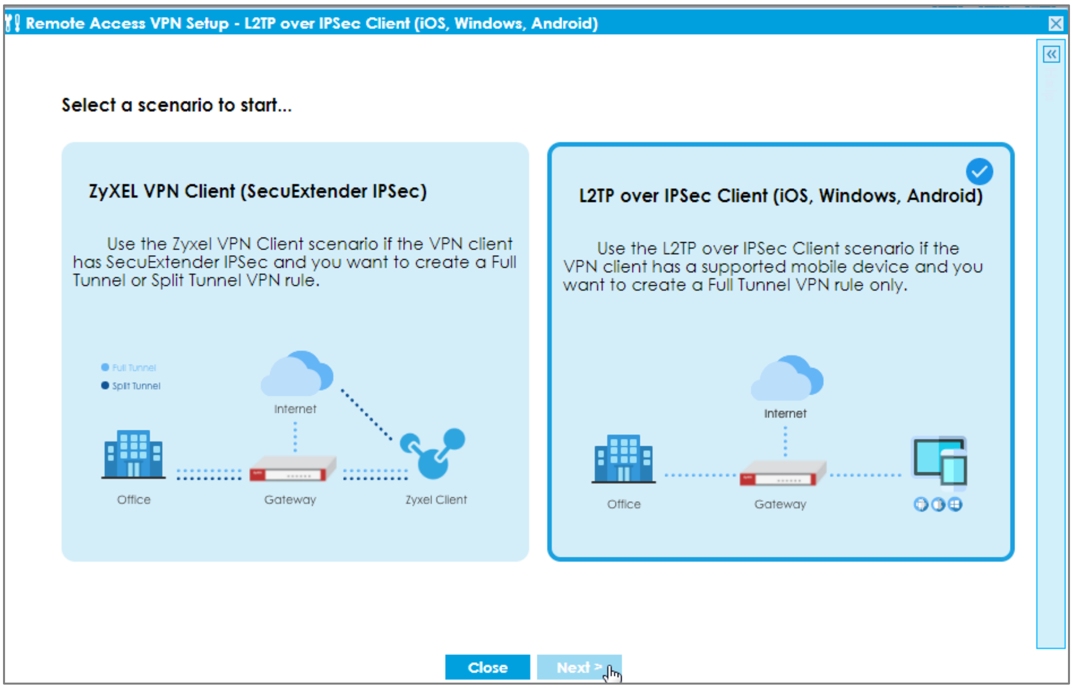


WAN Interface
WAN Quick Setting walks you through the steps of getting your device connected online.

Remote Access VPN Setup
For employees working anywhere in the world to securely connect with their company's remote LAN.

VPN Setup
For creating secure communications between nodes, VPN Quick Setting provides a simplified process to do that.

2. Select remote VPN scenarios, ZyXEL VPN Client(SecuExtender IPSec) or L2TP over IPSec client (IOS, Windows,Android). Here is an example of L2TP over IPSec VPN deployment.



Remote Access VPN Setup - L2TP over IPSec Client (iOS, Windows, Android)

Select a scenario to start...

ZyXEL VPN Client (SecuExtender IPSec)

Use the Zyxel VPN Client scenario if the VPN client has SecuExtender IPSec and you want to create a Full Tunnel or Split Tunnel VPN rule.

L2TP over IPSec Client (iOS, Windows, Android)

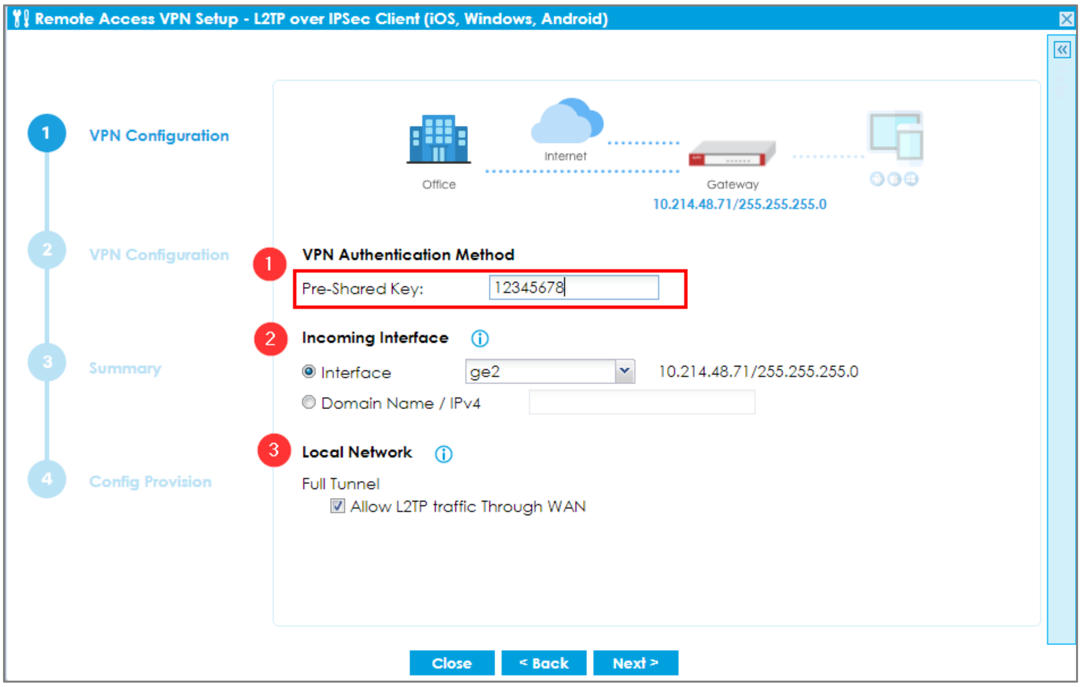
Use the L2TP over IPSec Client scenario if the VPN client has a supported mobile device and you want to create a Full Tunnel VPN rule only.

3. Configure the VPN configuration

(1) Enter the Pre-Shard Key

(2) Choose the Incoming interface

(3) Select the tunnel type, L2TP over IPSec VPN only support full tunnel type. Enable the check box of “Allow L2TP traffic Through WAN”.



Remote Access VPN Setup - L2TP over IPSec Client (iOS, Windows, Android)

1 **VPN Authentication Method**

Pre-Shared Key: 12345678

2 **Incoming Interface**

● Interface ge2 10.214.48.71/255.255.255.0

○ Domain Name / IPv4

3 **Local Network**

Full Tunnel

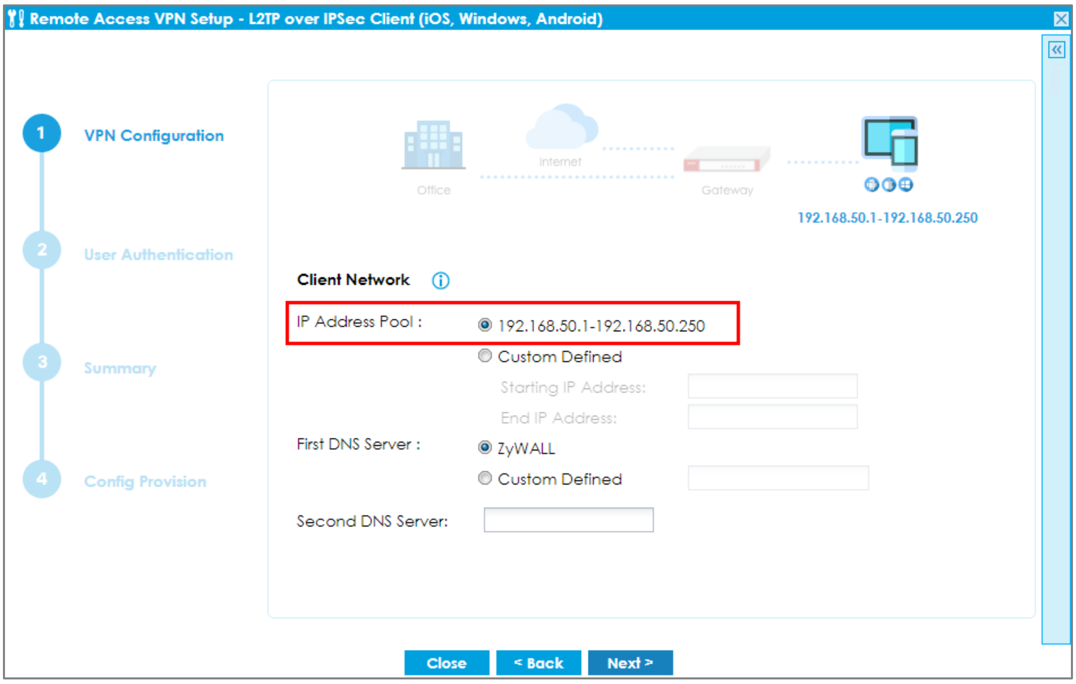
☑ Allow L2TP traffic Through WAN

4. Configure the IP Address Pool for the client

The IP address pool will auto select none use subnet on the device to avoid to set up the same subnet on the device. The auto IP address Pool will begin at 192.168.50.1

If there is 192.168.50.1 subnet exist in the settings, the IP address pool will change to 192.168.51.1 subnet.

Note: The Subnet only detect the subnet mask is under /24, if the subnet is not /24, it will not detect it.



Client Network

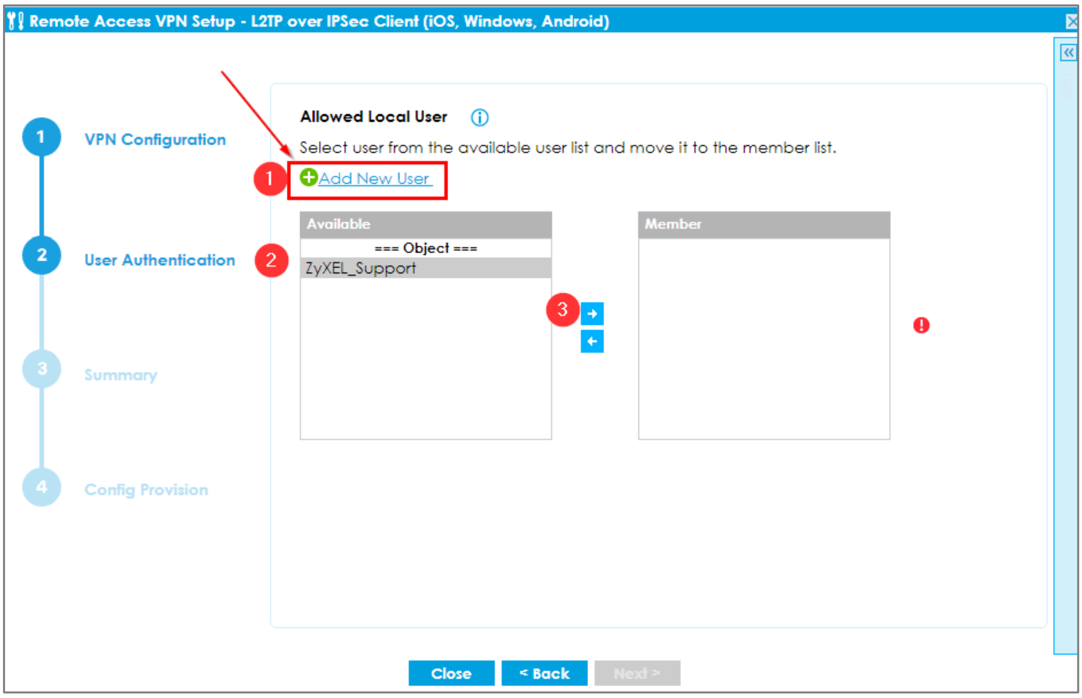
IP Address Pool : ● 192.168.50.1-192.168.50.250
○ Custom Defined
Starting IP Address:
End IP Address:

First DNS Server : ● ZyWALL
○ Custom Defined

Second DNS Server:

5. Allow local user to access the device

If you do not create any users before set up VPN tunnel, you can set up the user here to allow the user to access the device through the VPN tunnel.



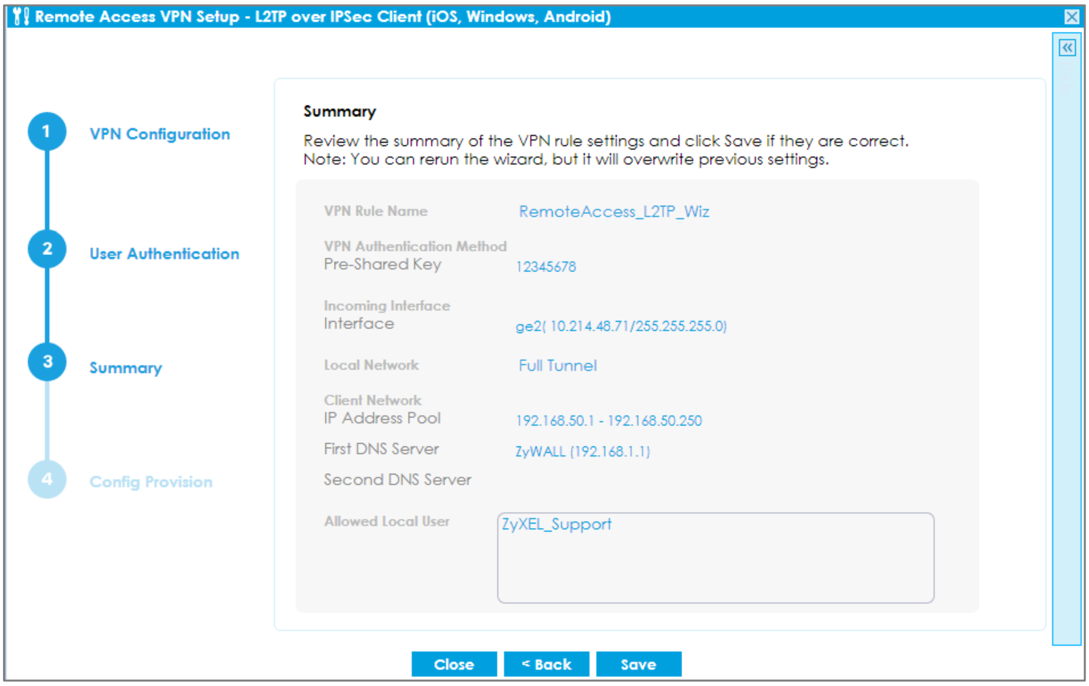
Allowed Local User

Select user from the available user list and move it to the member list.

Add New User

Available	Member
=== Object ===	
ZyXEL_Support	

6. After done all the steps in the wizard, you can check the settings at the final step, if there is any settings wrong, you can click back to reset the configuration.
If the settings are all correct, click save to go next step.



Summary

Review the summary of the VPN rule settings and click Save if they are correct.
Note: You can rerun the wizard, but it will overwrite previous settings.

VPN Rule Name: RemoteAccess_L2TP_Wiz

VPN Authentication Method
Pre-Shared Key: 12345678

Incoming Interface
Interface: ge2(10.214.48.71/255.255.255.0)

Local Network: Full Tunnel

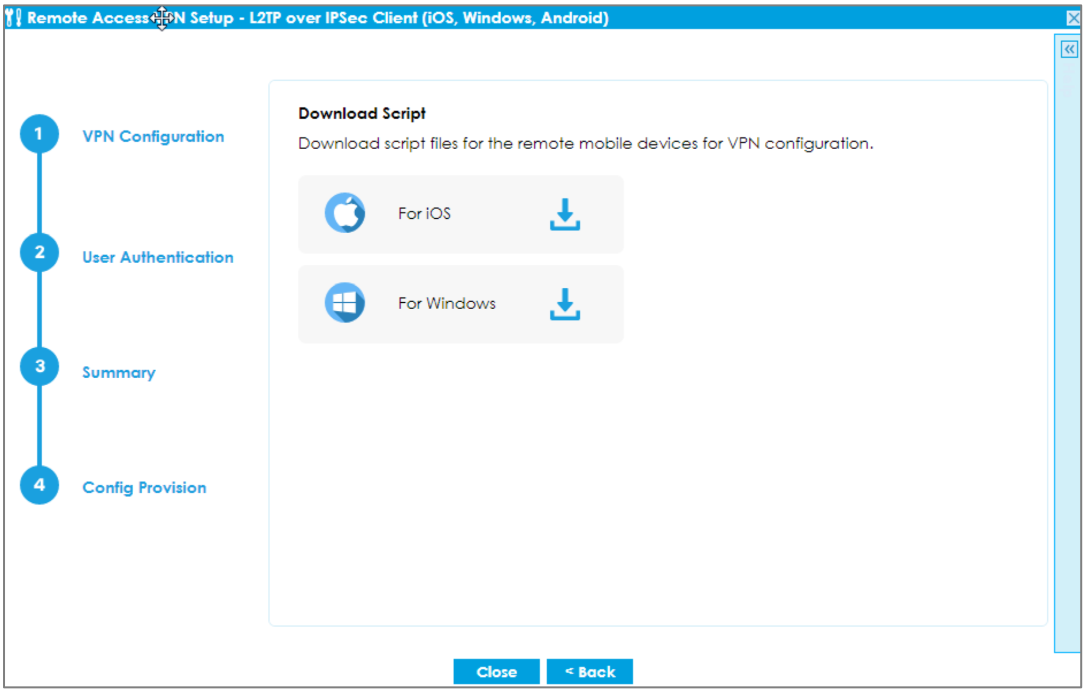
Client Network
IP Address Pool: 192.168.50.1 - 192.168.50.250
First DNS Server: ZyWALL (192.168.1.1)
Second DNS Server

Allowed Local User: ZyXEL_Support

7. Download script for Windows or IOS

To quick connect to the device from client, we support scripts to run on IOS and Windows system.

Note: We do not support the script for Android system.



Remote Access VPN Setup - L2TP over IPSec Client (iOS, Windows, Android)

1 VPN Configuration

2 User Authentication

3 Summary

4 Config Provision

Download Script

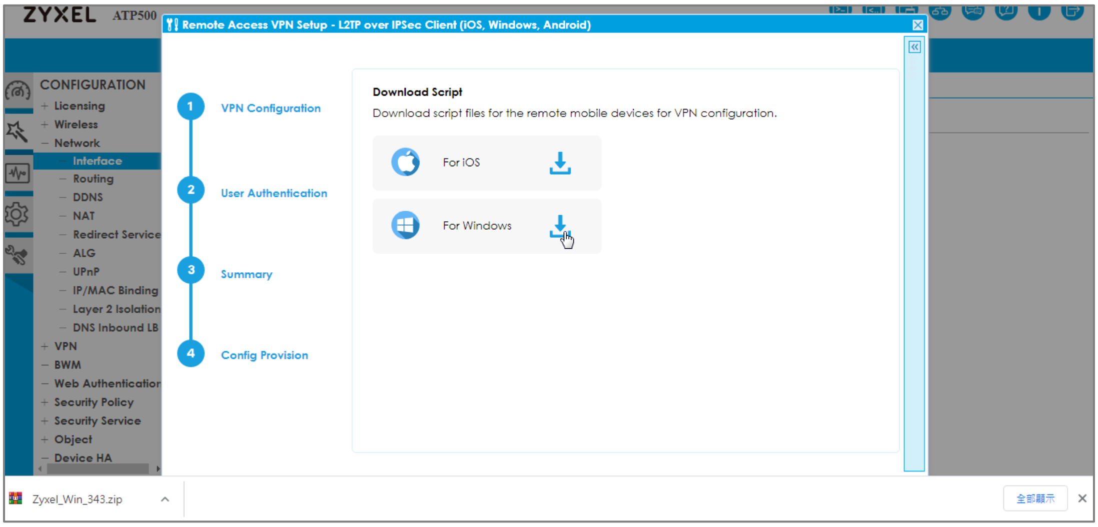
Download script files for the remote mobile devices for VPN configuration.

For iOS

For Windows

8. Download the scripts to quick build up VPN tunnel to the device on the client.

Note: Script file on windows support for Window8/ Window10



Remote Access VPN Setup - L2TP over IPSec Client (iOS, Windows, Android)

1 VPN Configuration

2 User Authentication

3 Summary

4 Config Provision

Download Script

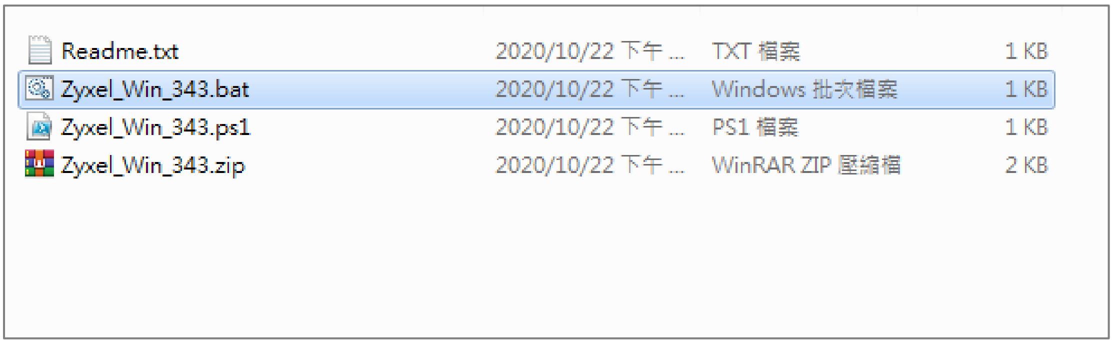
Download script files for the remote mobile devices for VPN configuration.

For iOS

For Windows

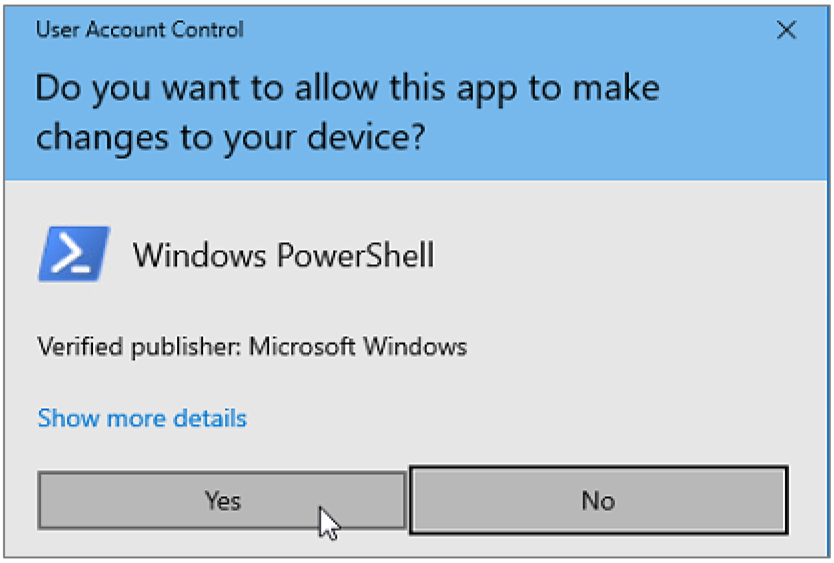
Test the result

1. Extract the download script on windows, and run the scripts



Readme.txt	2020/10/22 下午 ...	TXT 檔案	1 KB
Zyxel_Win_343.bat	2020/10/22 下午 ...	Windows 批次檔案	1 KB
Zyxel_Win_343.ps1	2020/10/22 下午 ...	PS1 檔案	1 KB
Zyxel_Win_343.zip	2020/10/22 下午 ...	WinRAR ZIP 壓縮檔	2 KB

2. Using PowerShell to run the scripts



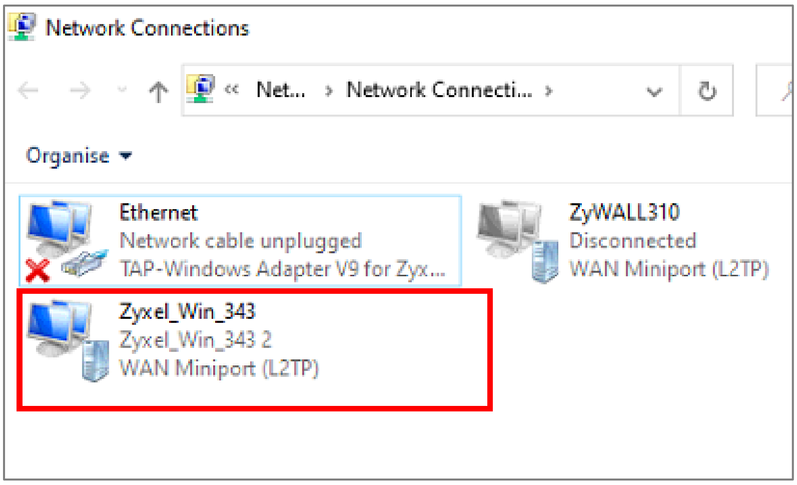
User Account Control

Do you want to allow this app to make changes to your device?

Windows PowerShell

Verified publisher: Microsoft Windows

3. It will generate a site to connect to the device

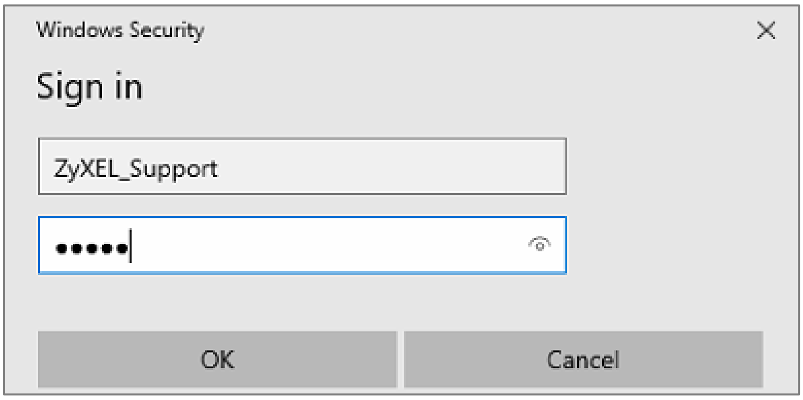


Ethernet
Network cable unplugged
TAP-Windows Adapter V9 for Zyx...

ZyWALL310
Disconnected
WAN Miniport (L2TP)

Zyxel_Win_343
Zyxel_Win_343 2
WAN Miniport (L2TP)

4. Double click the icon and sign in the username and password



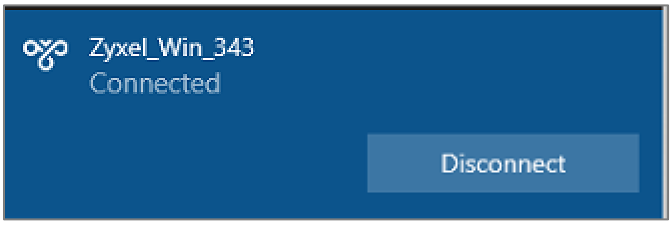
Windows Security

Sign in

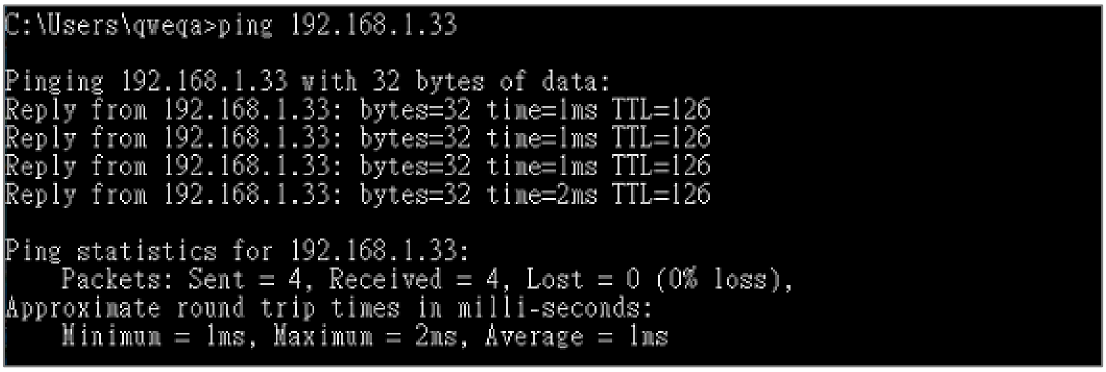
ZyXEL_Support

•••••

Now you can successfully build up the VPN tunnel



Zyxel_Win_343
Connected

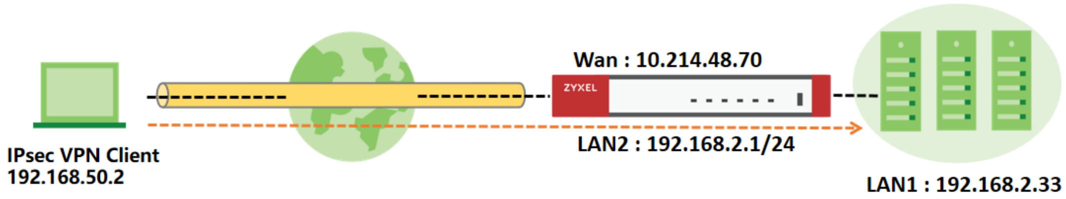


```
C:\Users\qweqa>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:
Reply from 192.168.1.33: bytes=32 time=1ms TTL=126
Reply from 192.168.1.33: bytes=32 time=1ms TTL=126
Reply from 192.168.1.33: bytes=32 time=1ms TTL=126
Reply from 192.168.1.33: bytes=32 time=2ms TTL=126

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

What can go wrong

1. If you're using Window7 to run the scripts, you're unable to run the scripts, the scripts only support Windows8 / Windows10

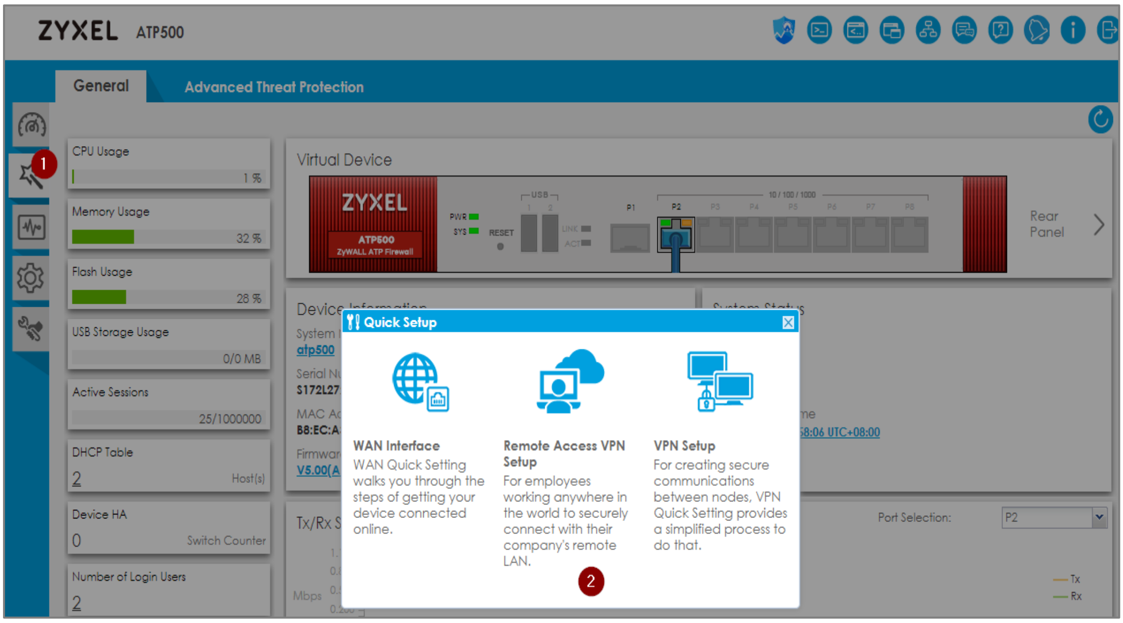
Remote access VPN Wizard-IKEv2 Client



With USG FLEX/ ATP you are able to provision predefined settings on your device to your IPsec VPN Client. This article will show you how to use **Remote Access VPN Setup** Wizard to setup configuration provisioning for IKEv2 VPN connections in combination with the IPSec VPN Client.

Set up VPN Tunnel

1.Log in to the Web GUI of your USG-FLEX/ATP, click **Quick Setup**, then select **Remote Access VPN Setup** to build up VPN tunnel with the Wizard.



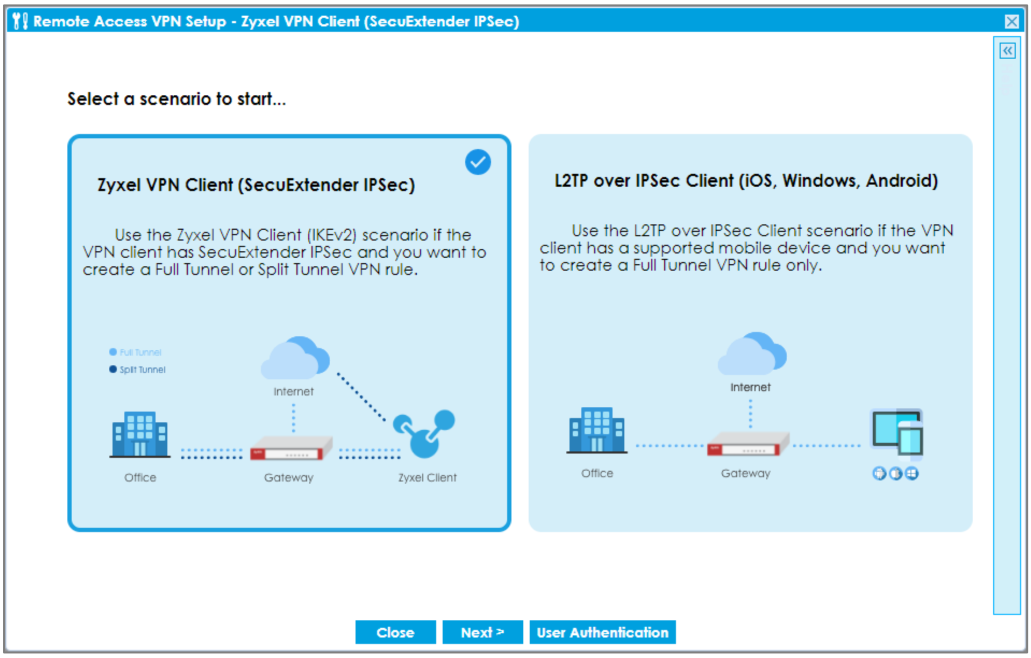
Quick Setup

WAN Interface
WAN Quick Setting walks you through the steps of getting your device connected online.

Remote Access VPN Setup
For employees working anywhere in the world to securely connect with their company's remote LAN.

VPN Setup
For creating secure communications between nodes, VPN Quick Setting provides a simplified process to do that.

2.Select remote VPN scenarios, **ZyXEL VPN Client(SecuExtender IPSec)**.



Remote Access VPN Setup - Zyxel VPN Client (SecuExtender IPSec)

Select a scenario to start...

Zyxel VPN Client (SecuExtender IPSec)

Use the Zyxel VPN Client (IKEv2) scenario if the VPN client has SecuExtender IPSec and you want to create a Full Tunnel or Split Tunnel VPN rule.

L2TP over IPSec Client (iOS, Windows, Android)

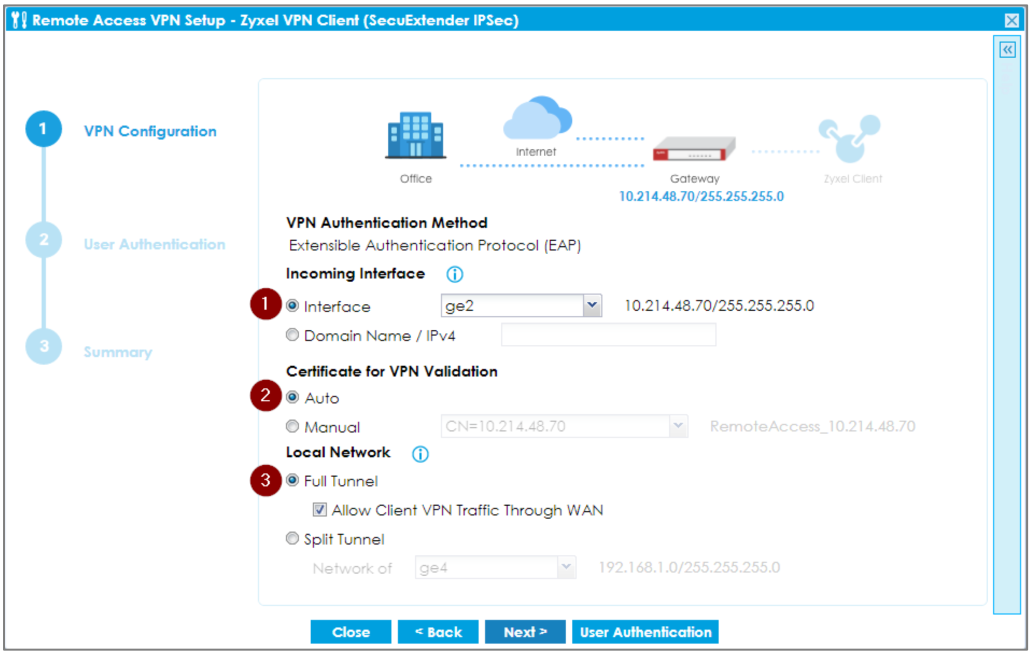
Use the L2TP over IPSec Client scenario if the VPN client has a supported mobile device and you want to create a Full Tunnel VPN rule only.

3.Configure the VPN Authentication Method

(1) Choose Incoming Interface

(2) Choose Certificate for VPN Validation

(3) Select the tunnel type, Full Tunnel and enable the check box of “Allow Client VPN Traffic Through WAN”.



Remote Access VPN Setup - Zyxel VPN Client (SecuExtender IPSec)

1 VPN Configuration

2 User Authentication

3 Summary

VPN Authentication Method

Extensible Authentication Protocol (EAP)

Incoming Interface

1 ● Interface: ge2 — 10.214.48.70/255.255.255.0

○ Domain Name / IPv4

Certificate for VPN Validation

2 ● Auto

○ Manual: CN=10.214.48.70 — RemoteAccess_10.214.48.70

Local Network

3 ● Full Tunnel

☑ Allow Client VPN Traffic Through WAN

○ Split Tunnel

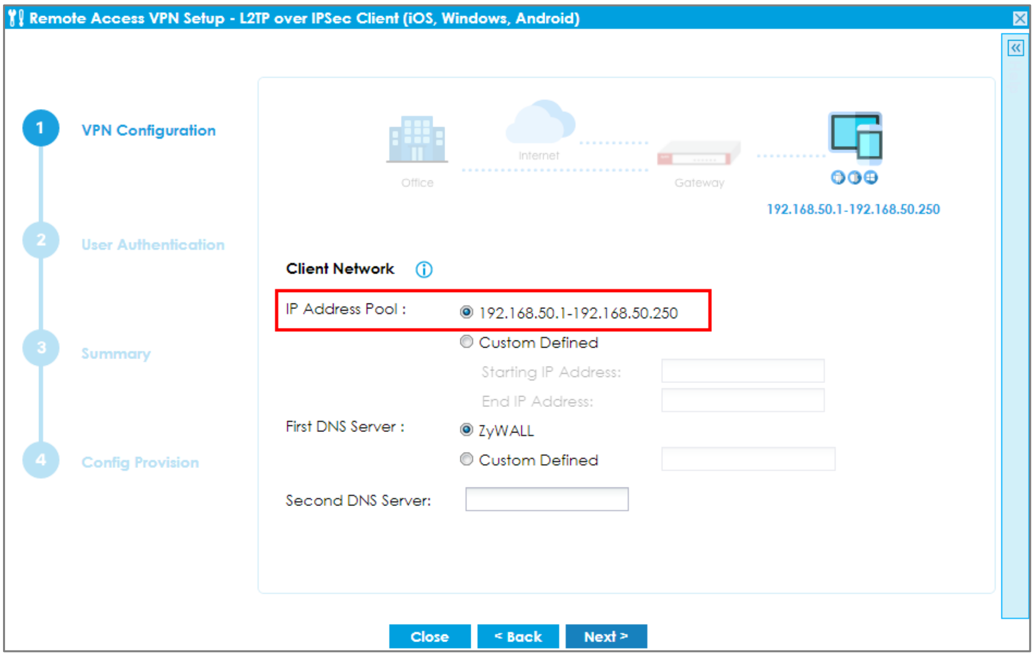
Network of: ge4 — 192.168.1.0/255.255.255.0

4.Configure the IP Address Pool for the client

The IP address pool will auto select none use subnet on the device to avoid to set up the same subnet on the device. The auto IP address Pool will begin at 192.168.50.1

If there is 192.168.50.1 subnet exist in the gateway settings, the IP address pool will auto change to 192.168.51.1 subnet.

Note: the gateway only checks overlapped subnets in /24, not check the other subnet mask.



Remote Access VPN Setup - L2TP over IPSec Client (iOS, Windows, Android)

Client Network

IP Address Pool : ● 192.168.50.1-192.168.50.250

○ Custom Defined

Starting IP Address:

End IP Address:

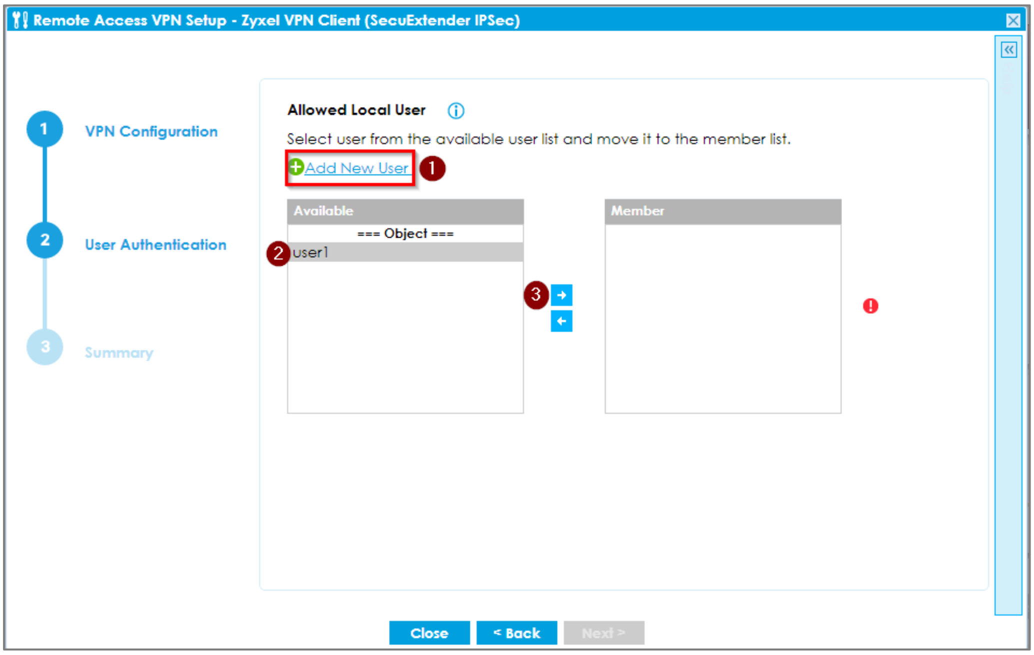
First DNS Server : ● ZyWALL

○ Custom Defined

Second DNS Server:

5.Allow local user to access the device

If you have not created the local users for remote VPN access, you can set up the local user here to allow the user to access the network through the VPN tunnel.



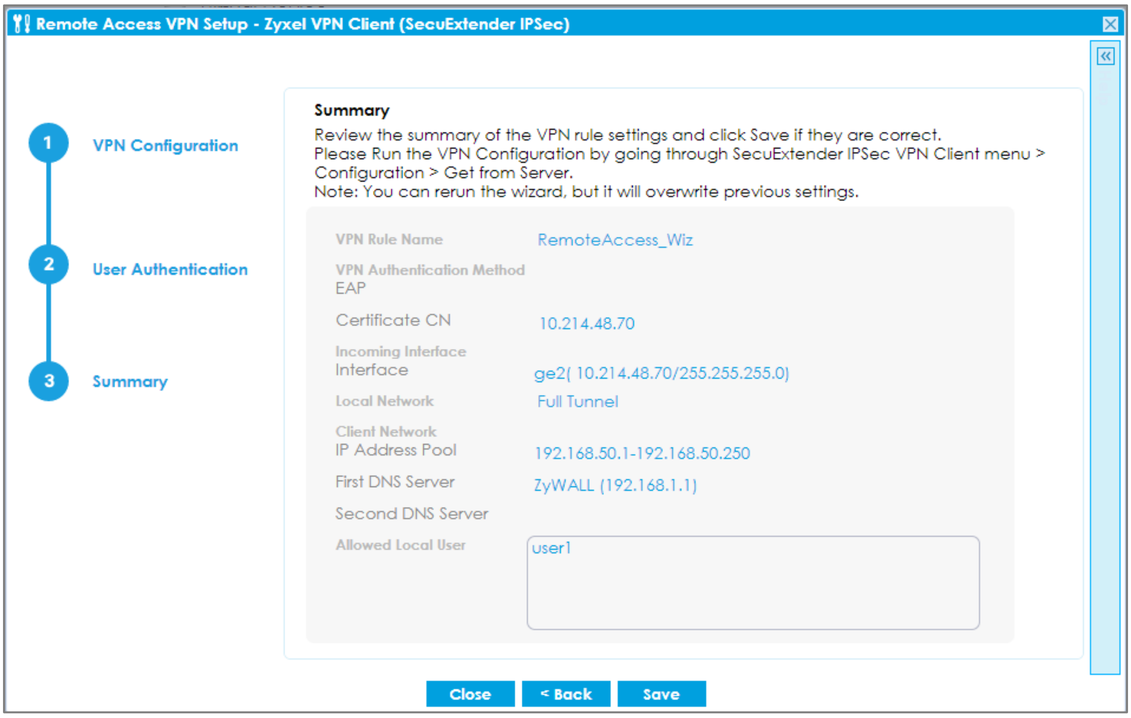
Remote Access VPN Setup - Zyxel VPN Client (SecuExtender IPSec)

Allowed Local User

Select user from the available user list and move it to the member list.

6.After done all the steps in the wizard, you can check the settings at the final step, if there is any settings wrong, you can click back to reset the configuration.

If the settings are all correct, click save to go next step.



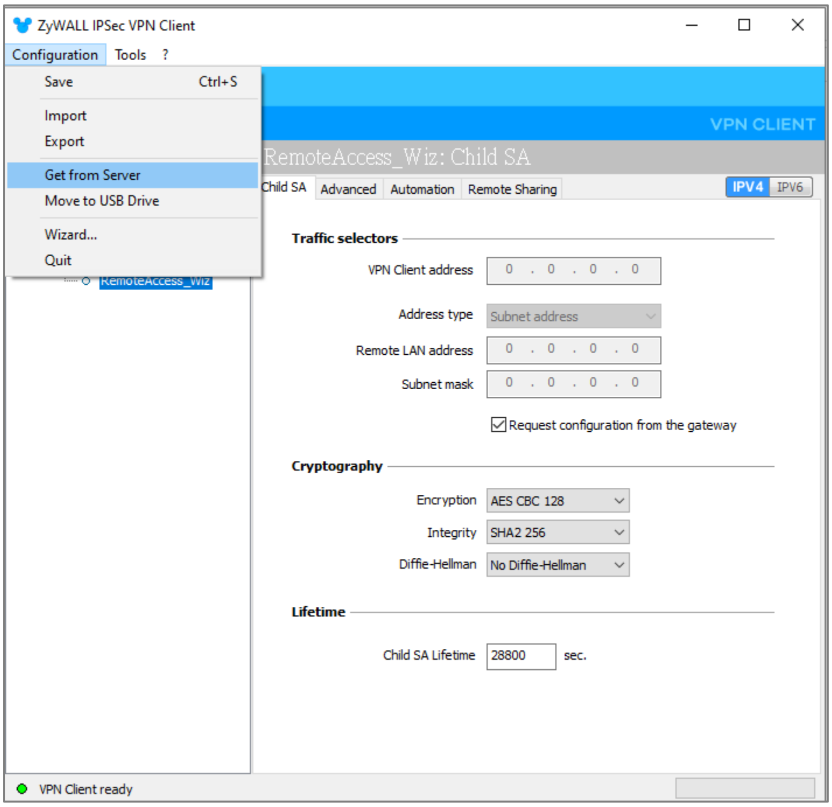
Summary

Review the summary of the VPN rule settings and click Save if they are correct.
Please Run the VPN Configuration by going through SecuExtender IPSec VPN Client menu > Configuration > Get from Server.
Note: You can rerun the wizard, but it will overwrite previous settings.

VPN Rule Name	RemoteAccess_Wiz
VPN Authentication Method EAP	
Certificate CN	10.214.48.70
Incoming Interface Interface	ge2(10.214.48.70/255.255.255.0)
Local Network	Full Tunnel
Client Network IP Address Pool	192.168.50.1-192.168.50.250
First DNS Server	ZyWALL (192.168.1.1)
Second DNS Server	
Allowed Local User	user1

Test the result

1. Open **ZyWALL IPSec VPN Client**, go to **Configuration > Get from Server**



RemoteAccess_Wiz: Child SA

Traffic selectors

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 0 . 0 . 0 . 0

Subnet mask: 0 . 0 . 0 . 0

☑ Request configuration from the gateway

Cryptography

Encryption: AES CBC 128

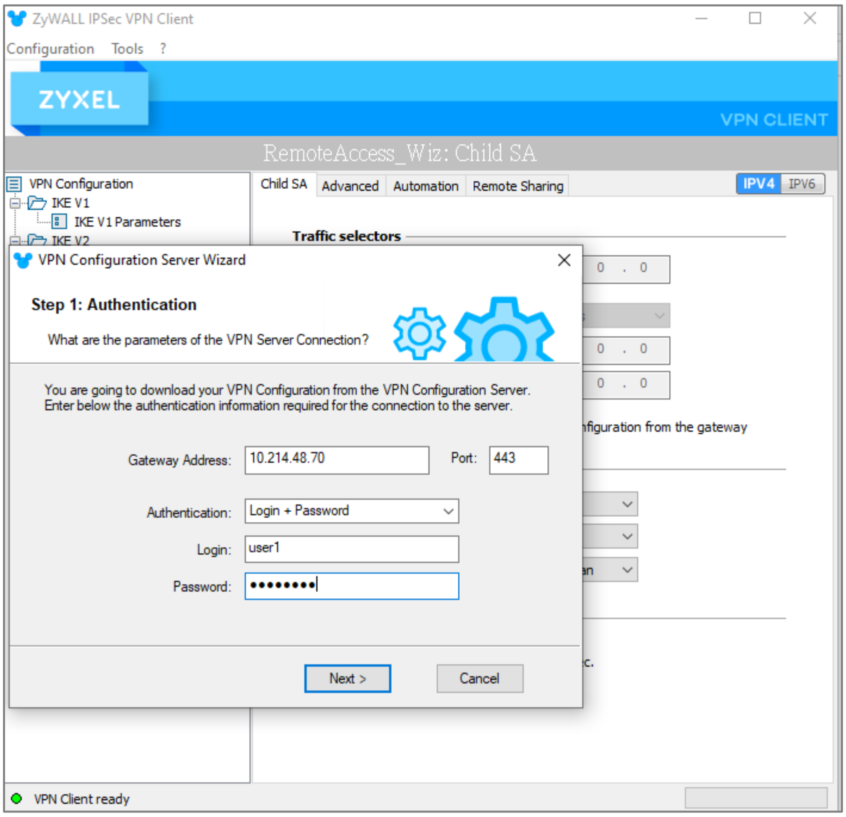
Integrity: SHA2 256

Diffie-Hellman: No Diffie-Hellman

Lifetime

Child SA Lifetime: 28800 sec.

2. Typing the IP address of server, user account, and password. Then click on **Next**



Step 1: Authentication

What are the parameters of the VPN Server Connection?

You are going to download your VPN Configuration from the VPN Configuration Server.
Enter below the authentication information required for the connection to the server.

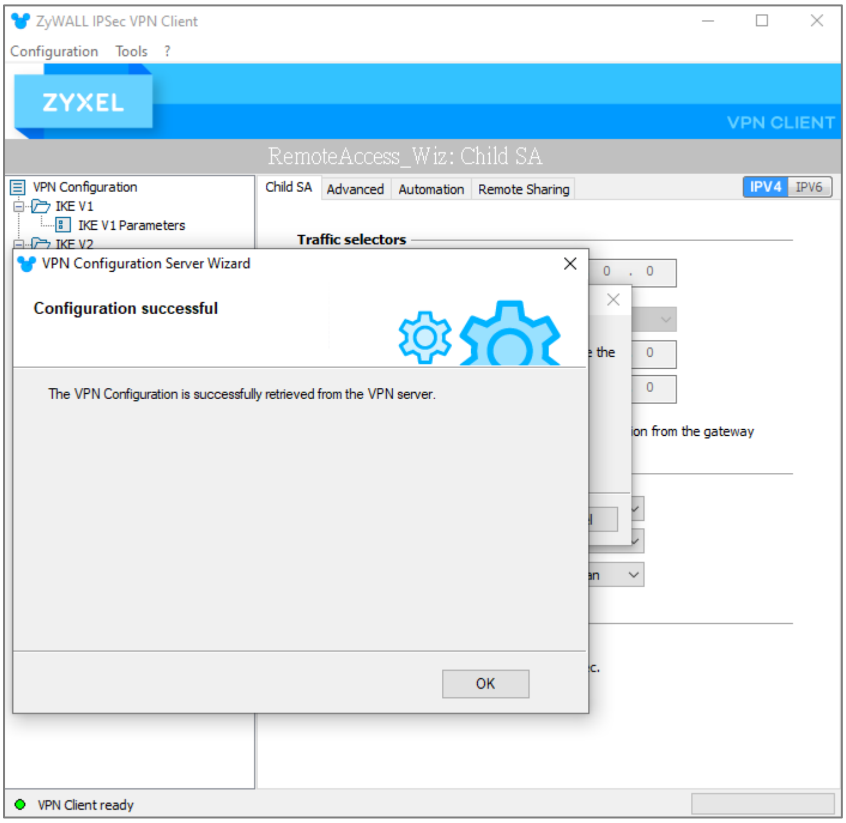
Gateway Address: 10.214.48.70 Port: 443

Authentication: Login + Password

Login: user1

Password: ••••••••

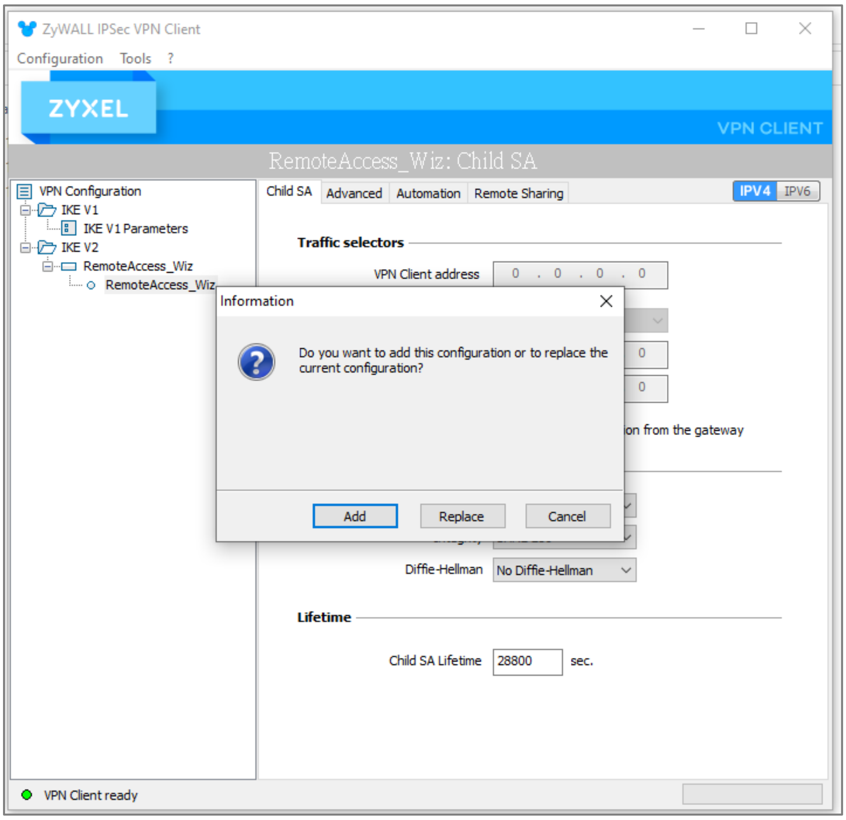
3. Wait until the VPN Client download successfully the configuration from server.



Configuration successful

The VPN Configuration is successfully retrieved from the VPN server.

4. If you have an existing VPN configuration on the VPN client, click **Add** to replace.



RemoteAccess_Wiz: Child SA

Traffic selectors

VPN Client address: 0 . 0 . 0 . 0

on from the gateway

Do you want to add this configuration or to replace the current configuration?

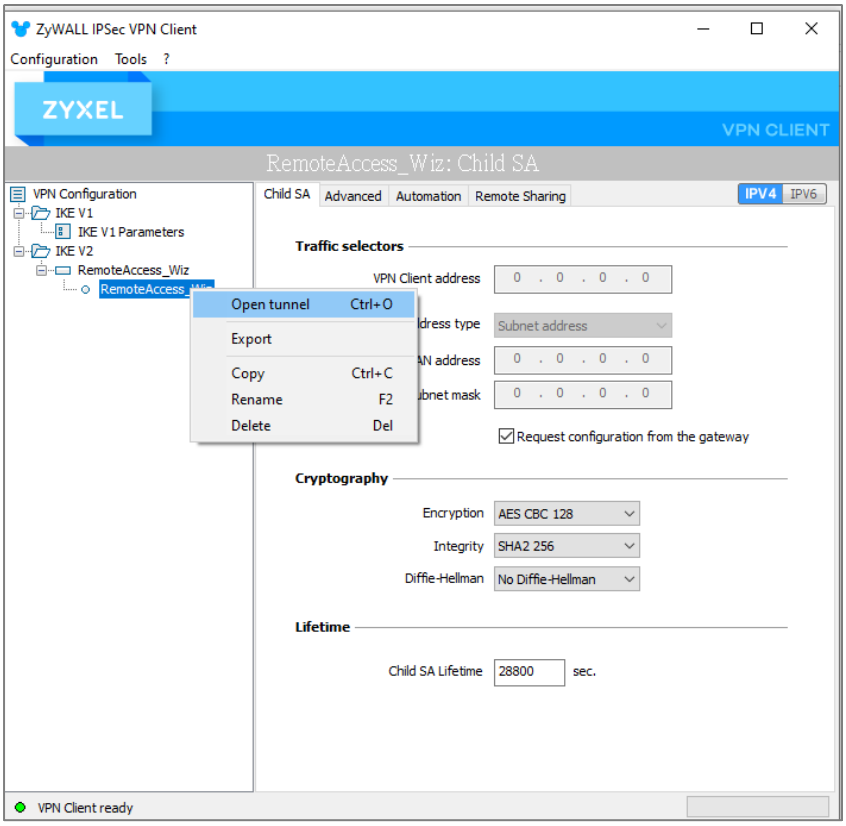
Diffie-Hellman: No Diffie-Hellman

Lifetime

Child SA Lifetime: 28800 sec.

VPN Client ready

5. Right-click this configuration and press Open tunnel.



RemoteAccess_Wiz: Child SA

Traffic selectors

VPN Client address 0 . 0 . 0 . 0

ldress type Subnet address

N address 0 . 0 . 0 . 0

ıbnet mask 0 . 0 . 0 . 0

☑ Request configuration from the gateway

Cryptography

Encryption AES CBC 128

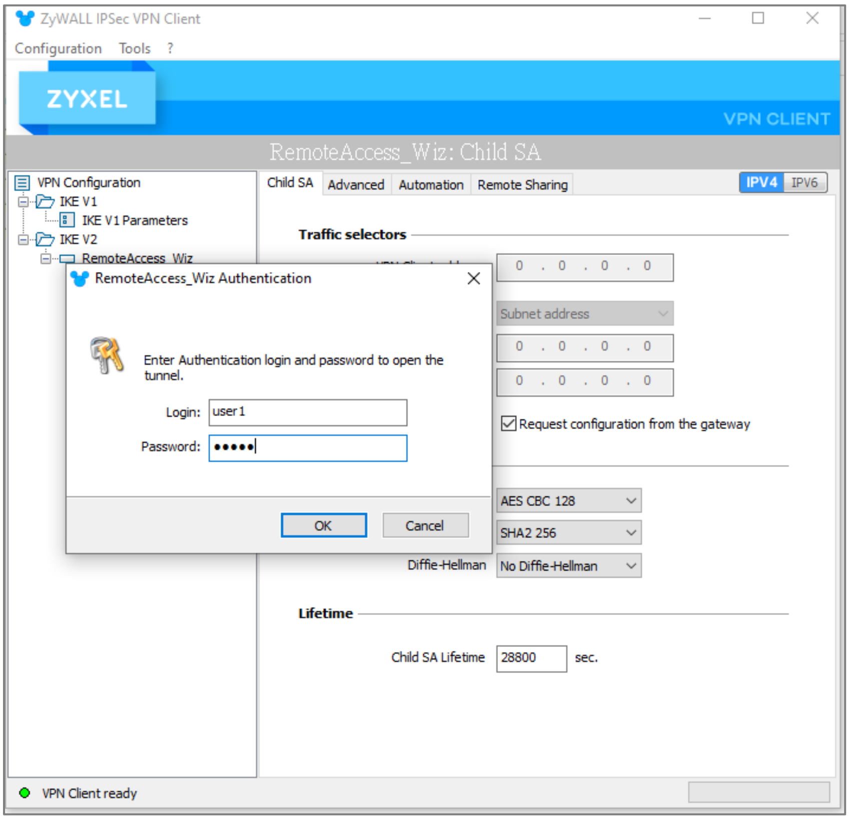
Integrity SHA2 256

Diffie-Hellman No Diffie-Hellman

Lifetime

Child SA Lifetime 28800 sec.

6. Popup window then typing login account and password.



RemoteAccess_Wiz Authentication

Enter Authentication login and password to open the tunnel.

Login: user1

Password: •••••

0 . 0 . 0 . 0

Subnet address

0 . 0 . 0 . 0

0 . 0 . 0 . 0

☑ Request configuration from the gateway

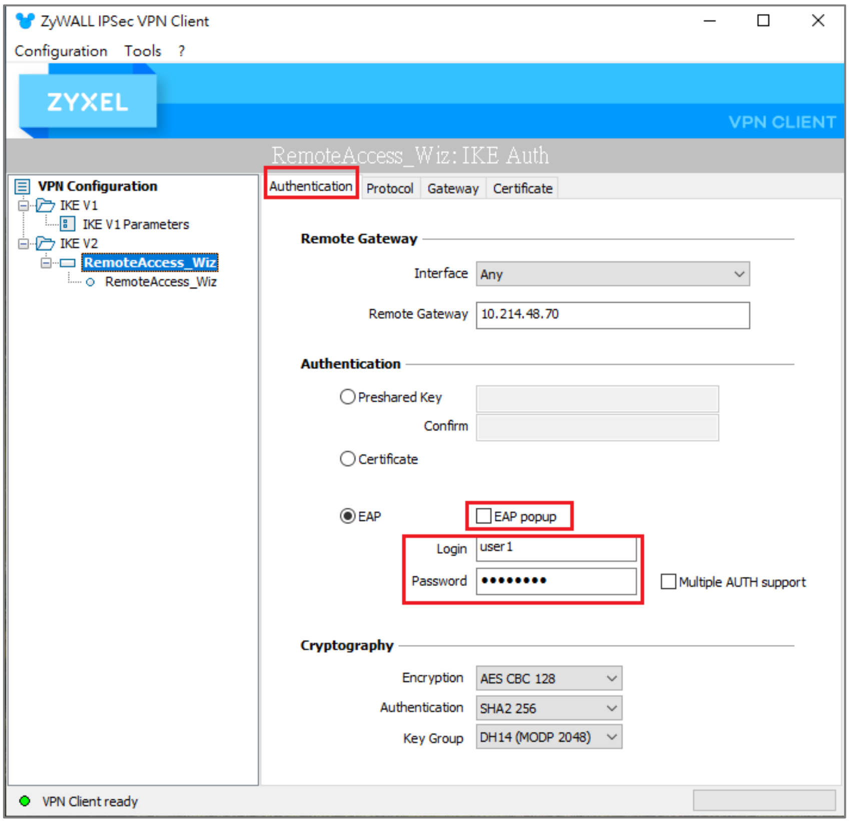
AES CBC 128

SHA2 256

Diffie-Hellman: No Diffie-Hellman

Child SA Lifetime: 28800 sec.

Or you can configure login account and password on Authentication tab in advance.



Remote Gateway

Interface: Any

Remote Gateway: 10.214.48.70

Authentication

○ Preshared Key

Confirm

○ Certificate

● EAP ☐ EAP popup

Login: user1

Password: ••••••••

☐ Multiple AUTH support

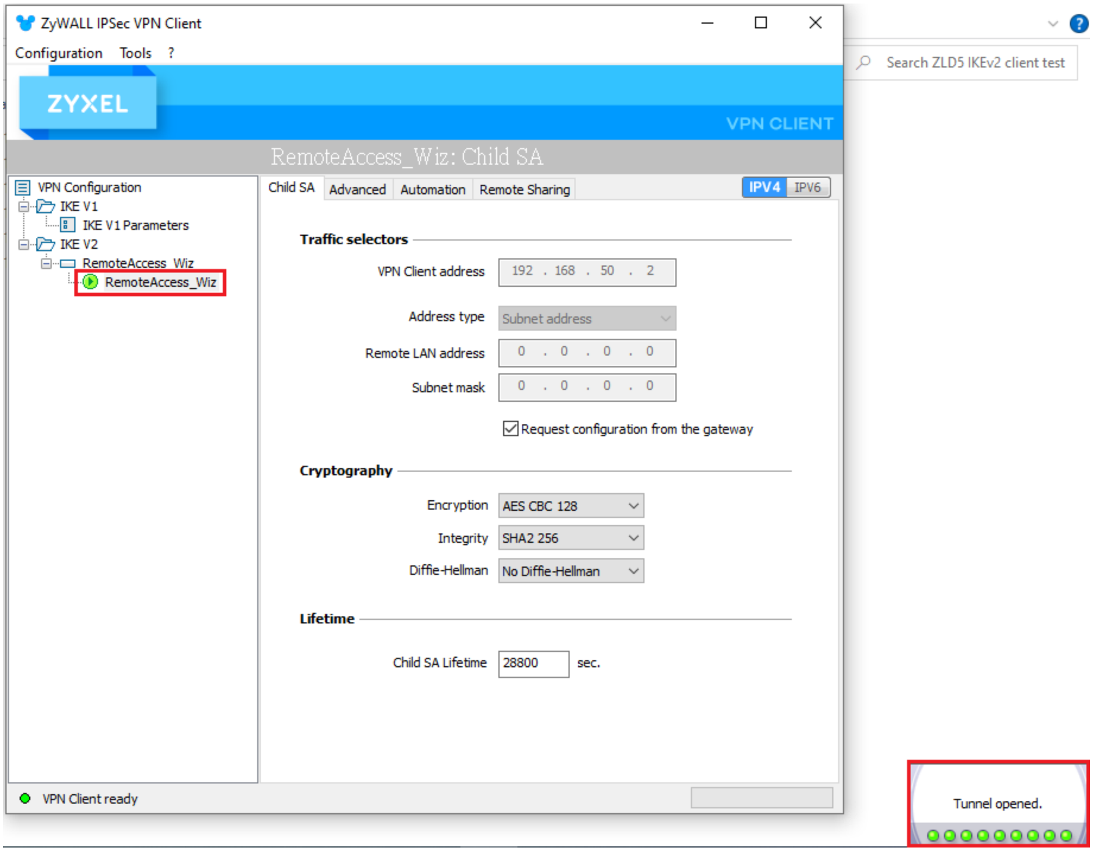
Cryptography

Encryption: AES CBC 128

Authentication: SHA2 256

Key Group: DH14 (MODP 2048)

7. IKEv2 VPN connection established successfully.



ZyWALL IPSec VPN Client

RemoteAccess_Wiz: Child SA

Traffic selectors

VPN Client address: 192 . 168 . 50 . 2

Address type: Subnet address

Remote LAN address: 0 . 0 . 0 . 0

Subnet mask: 0 . 0 . 0 . 0

☑ Request configuration from the gateway

Cryptography

Encryption: AES CBC 128

Integrity: SHA2 256

Diffie-Hellman: No Diffie-Hellman

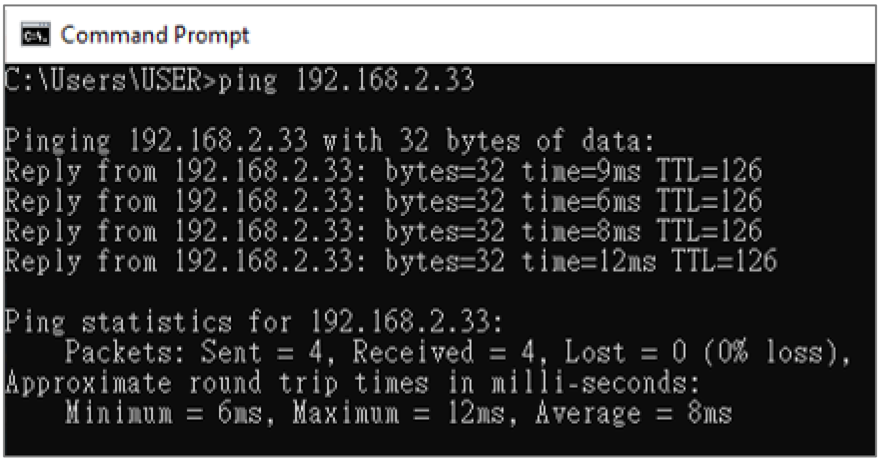
Lifetime

Child SA Lifetime: 28800 sec.

VPN Client ready

Tunnel opened.

8.The remote user can ping the internal network IP address without problem.



Command Prompt

```
C:\Users\USER>ping 192.168.2.33

Pinging 192.168.2.33 with 32 bytes of data:
Reply from 192.168.2.33: bytes=32 time=9ms TTL=126
Reply from 192.168.2.33: bytes=32 time=6ms TTL=126
Reply from 192.168.2.33: bytes=32 time=8ms TTL=126
Reply from 192.168.2.33: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.2.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 12ms, Average = 8ms
```

VPN Configuration Provisioning with Upload Bandwidth Limit

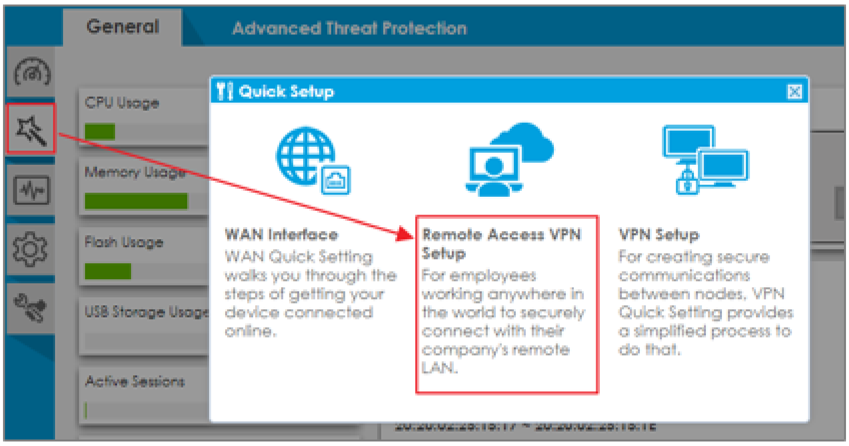
In ZLD5.10, gateway is able to provisioning the VPN configuration with upload bandwidth limit to the time-based Zyxel IPSec VPN client.

Note: Bandwidth limit only support on time-based Zyxel VPN Client

On-premises Mode

Setup Remote Access VPN using Quick Setup Wizard

In the Web GUI, go to Quick Setup > Remote Access VPN Setup. Select Zyxel VPN Client (SecuExtender IPSec) scenario to to run the VPN wizard

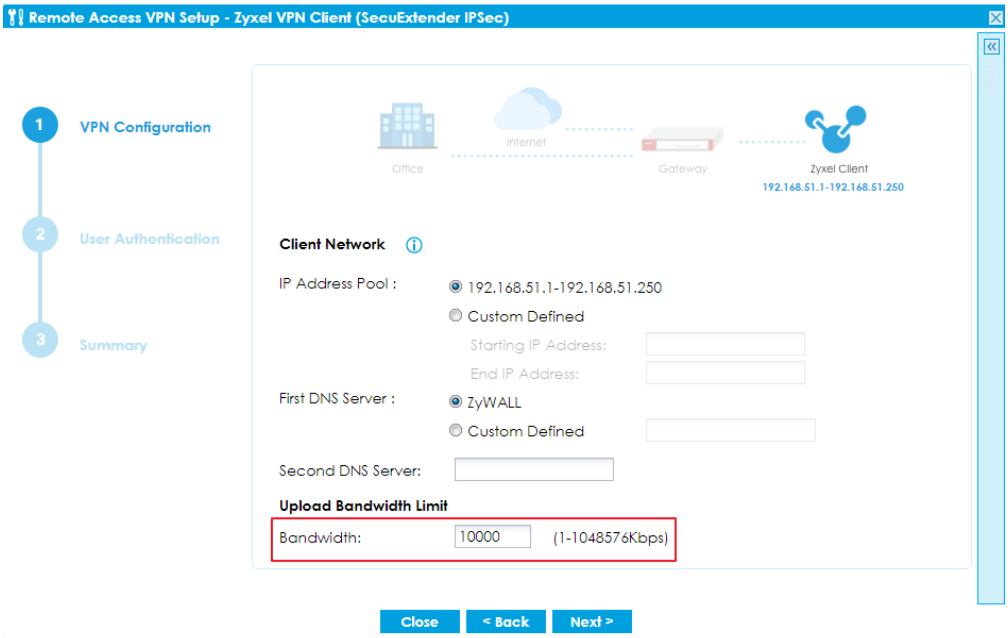


WAN Interface
WAN Quick Setting walks you through the steps of getting your device connected online.

Remote Access VPN Setup
For employees working anywhere in the world to securely connect with their company's remote LAN.

VPN Setup
For creating secure communications between nodes, VPN Quick Setting provides a simplified process to do that.

- In the VPN Configuration step, you are able to input the upload bandwidth limit for Zyxel IPSec VPN client. Upload Bandwidth Limit to set the maximum bandwidth for uploading traffic from Zyxel IPSec VPN clients over IPSec VPN tunnels.



Remote Access VPN Setup - Zyxel VPN Client (SecuExtender IPSec)

1 VPN Configuration

2 User Authentication

3 Summary

Client Network

IP Address Pool : ● 192.168.51.1-192.168.51.250
○ Custom Defined
Starting IP Address:
End IP Address:

First DNS Server : ● ZyWALL
○ Custom Defined

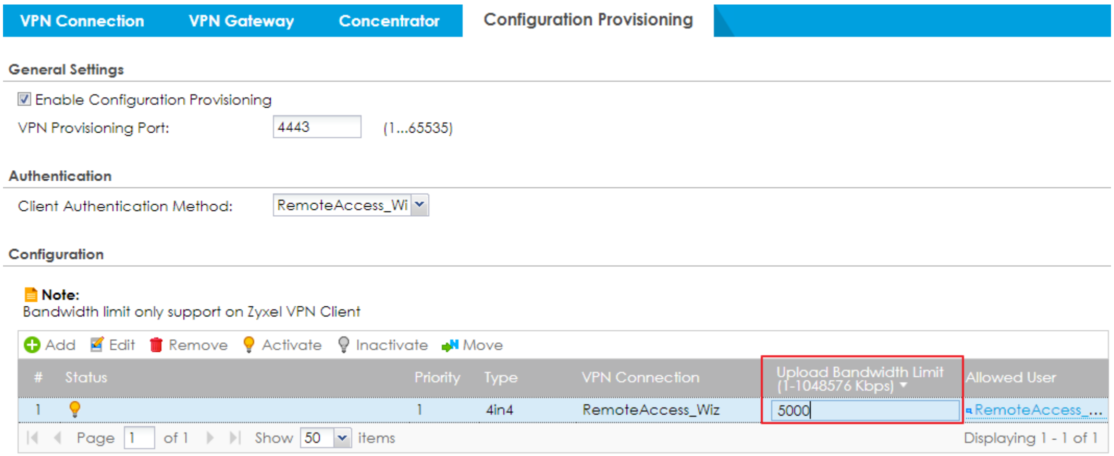
Second DNS Server:

Upload Bandwidth Limit

Bandwidth: 10000 (1-1048576Kbps)

Close | < Back | Next >

After completing VPN Wizard, if you want to modify the upload bandwidth limit, go to Configuration > VPN > IPSec VPN > Configuration Provisioning



VPN Connection | VPN Gateway | Concentrator | Configuration Provisioning

General Settings

☑ Enable Configuration Provisioning

VPN Provisioning Port: 4443 (1...65535)

Authentication

Client Authentication Method: RemoteAccess_Wi

Configuration

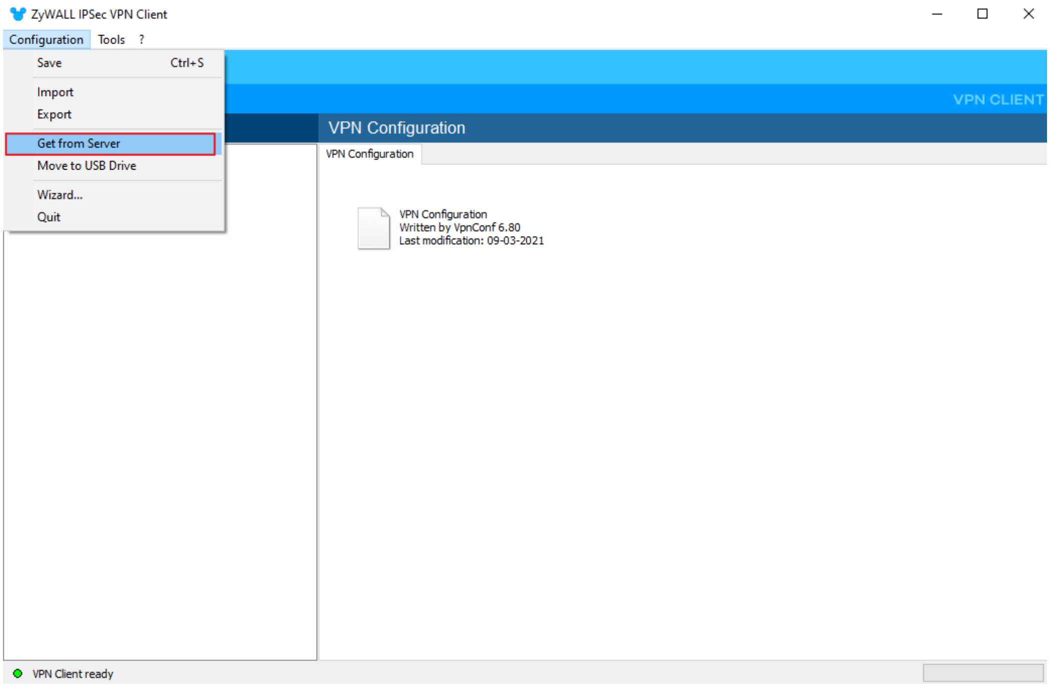
Note:
Bandwidth limit only support on Zyxel VPN Client

Add | Edit | Remove | Activate | Inactivate | Move

#	Status	Priority	Type	VPN Connection	Upload Bandwidth Limit (1-1048576 Kbps)	Allowed User
1	💡	1	4in4	RemoteAccess_Wiz	5000	RemoteAccess_...

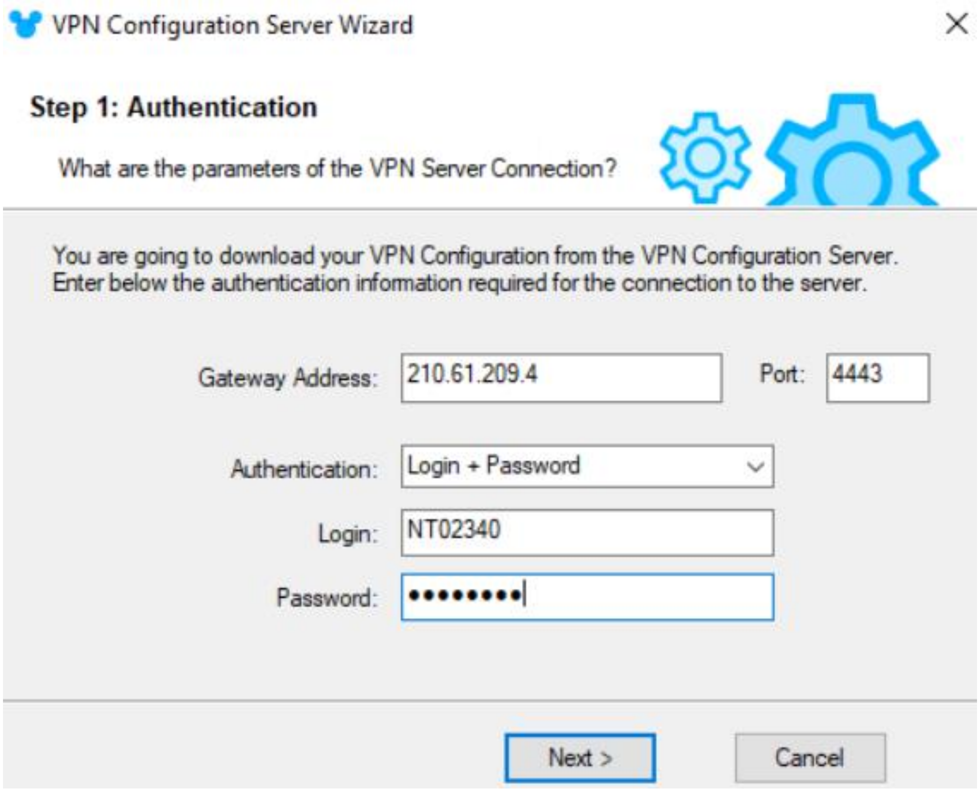
Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

From the Zyxel IPSec VPN client, go to Configuration > Get from Server, input the gateway IP address, username, password then connect to gateway to get the VPN configuration



VPN Configuration
Written by VpnConf 6.80
Last modification: 09-03-2021

VPN Client ready



VPN Configuration Server Wizard

Step 1: Authentication

What are the parameters of the VPN Server Connection?

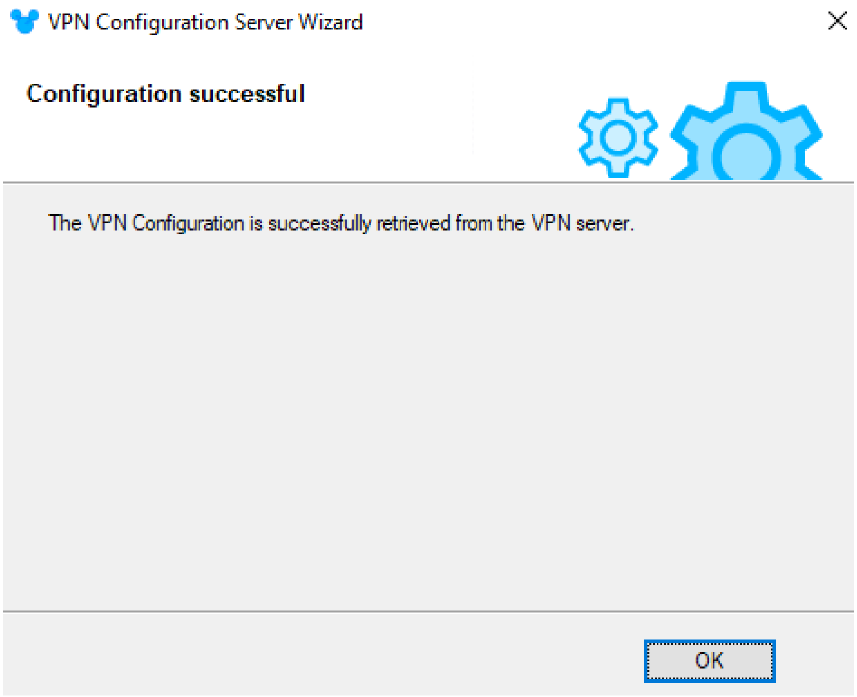
You are going to download your VPN Configuration from the VPN Configuration Server. Enter below the authentication information required for the connection to the server.

Gateway Address: 210.61.209.4 Port: 4443

Authentication: Login + Password

Login: NT02340

Password: ●●●●●●●●●



VPN Configuration Server Wizard

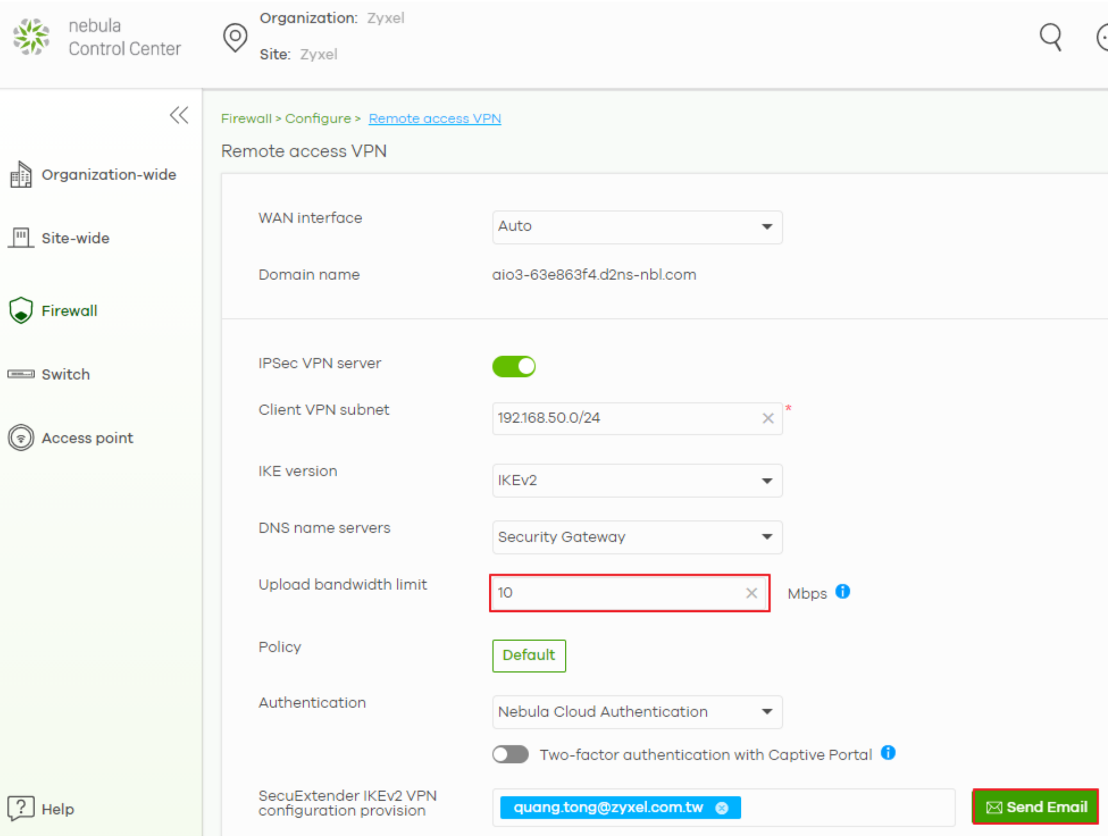
Configuration successful

The VPN Configuration is successfully retrieved from the VPN server.

Nebula Mode

Provisioning VPN configuration on Nebula Control Center

On NCC, go to Firewall > Remote access VPN, enable IPSec VPN Server, input Upload bandwidth limit, recipient's email address, then click to Send Email to provisioning the VPN configuration



Remote access VPN

WAN interface: Auto

Domain name: aio3-63e863f4.d2ns-nbl.com

IPSec VPN server: on

Client VPN subnet: 192.168.50.0/24 *

IKE version: IKEv2

DNS name servers: Security Gateway

Upload bandwidth limit: 10 Mbps

Policy: Default

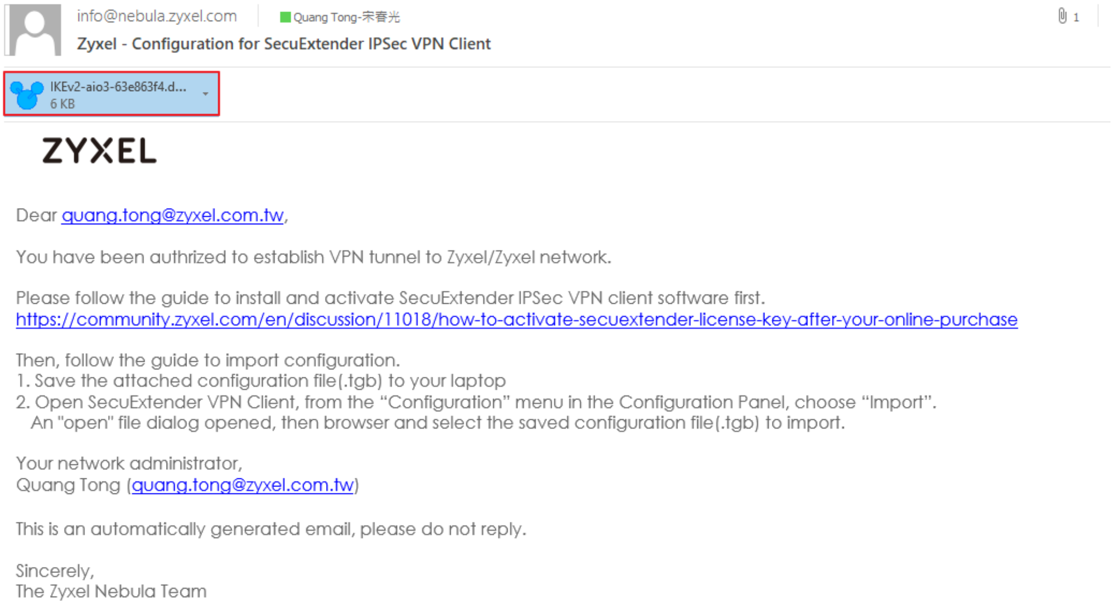
Authentication: Nebula Cloud Authentication

Two-factor authentication with Captive Portal: off

SecuExtender IKEv2 VPN configuration provision: quang.tong@zyxel.com.tw

Send Email

The VPN configuration file will be emailed to you.



info@nebula.zyxel.com | Quang Tong-宋春光

Zyxel - Configuration for SecuExtender IPSec VPN Client

IKEv2-aio3-63e863f4.d...
6 KB

ZYXEL

Dear quang.tong@zyxel.com.tw,

You have been authrized to establish VPN tunnel to Zyxel/Zyxel network.

Please follow the guide to install and activate SecuExtender IPSec VPN client software first.
https://community.zyxel.com/en/discussion/11018/how-to-activate-secuextender-license-key-after-your-online-purchase

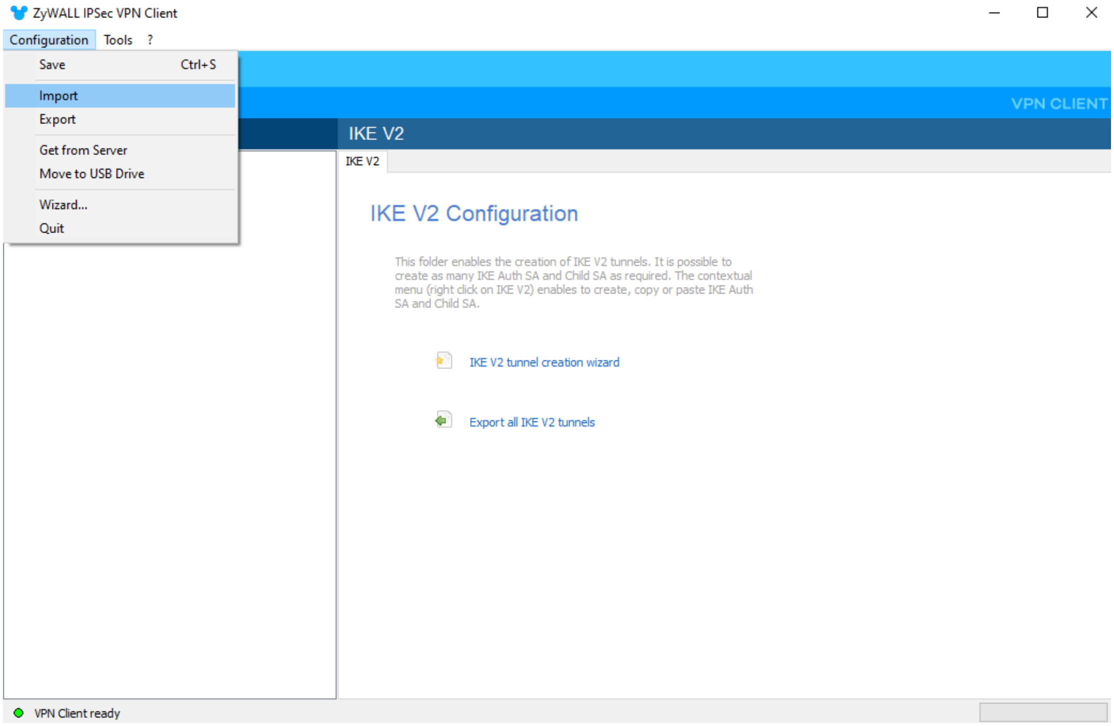
Then, follow the guide to import configuration.
1. Save the attached configuration file(.tgb) to your laptop
2. Open SecuExtender VPN Client, from the "Configuration" menu in the Configuration Panel, choose "Import".
An "open" file dialog opened, then browser and select the saved configuration file(.tgb) to import.

Your network administrator,
Quang Tong (quang.tong@zyxel.com.tw)

This is an automatically generated email, please do not reply.

Sincerely,
The Zyxel Nebula Team

From the Zyxel IPSec VPN client, go to Configuration > Import to upload the VPN configuration file. After that, you can establish VPN connect to the gateway



IKE V2 Configuration

This folder enables the creation of IKE V2 tunnels. It is possible to create as many IKE Auth SA and Child SA as required. The contextual menu (right click on IKE V2) enables to create, copy or paste IKE Auth SA and Child SA.

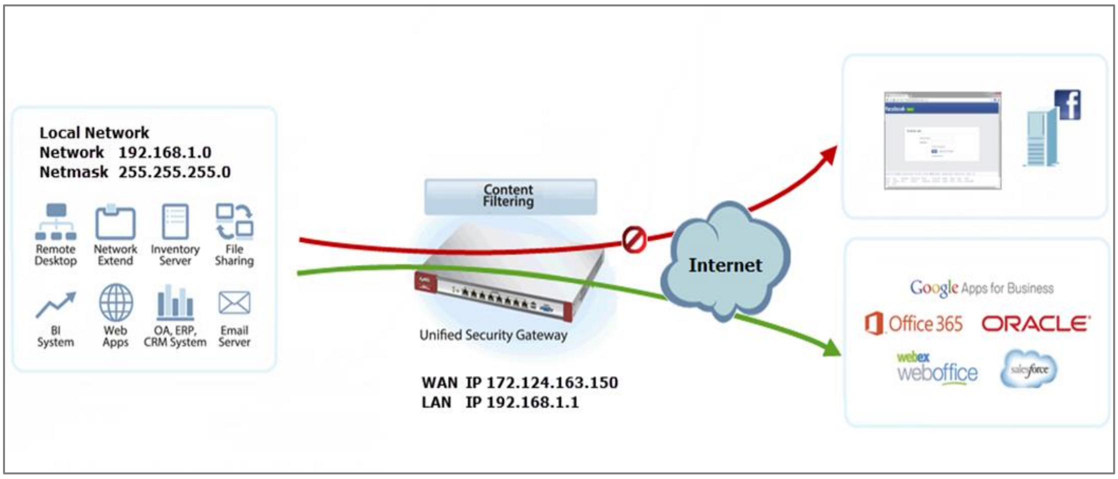
Chapter 2- Security Service

How to block HTTPS websites by Domain Filter without applying SSL Inspection

The Content Filter with HTTPs Domain Filter allows you to block HTTPs websites by category service without SSL-Inspection. The filtering feature is based on more than 50 Managed 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 Commtouch engine, then take action when it matches the block category in Content Filter profile.

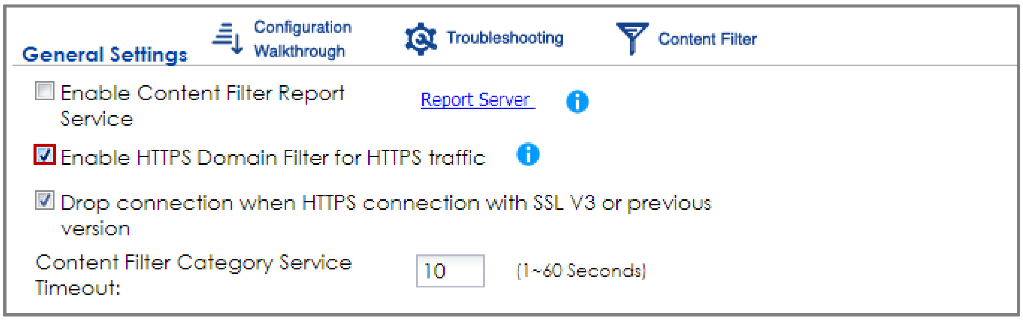
ZyWALL/USG Domain Filter Example



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25)

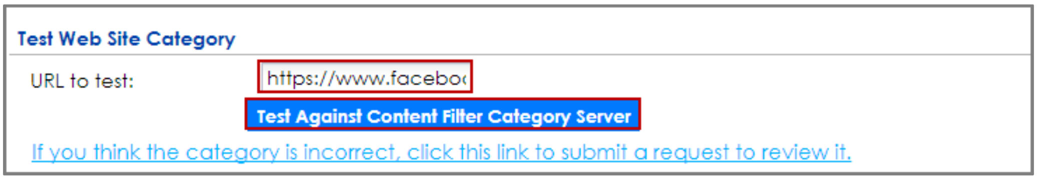
Set Up the Content Filter on the ZyWALL/USG

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



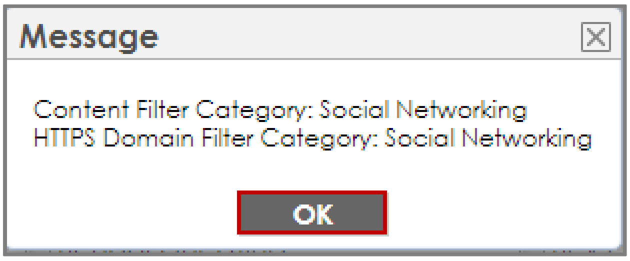
□ Enable Content Filter Report Service
☑ Enable HTTPS Domain Filter for HTTPS traffic
☑ Drop connection when HTTPS connection with SSL V3 or previous version
Content Filter Category Service Timeout: 10 (1~60 Seconds)

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
Test Against Content Filter Category Server
If you think the category is incorrect, click this link to submit a request to review it.

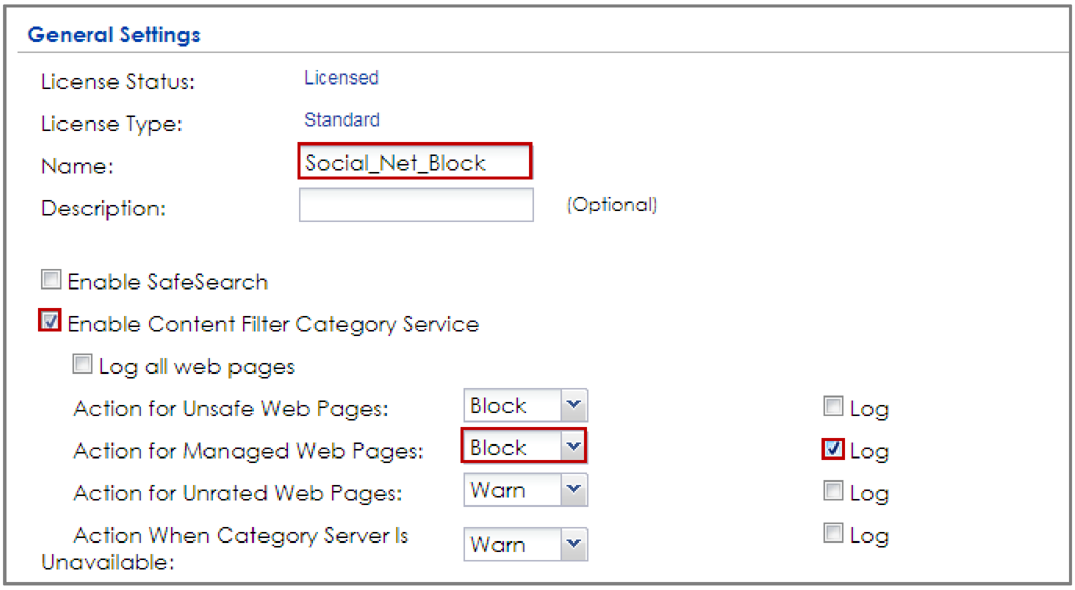
URL to test: https://www.facebo

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



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

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: Standard

Name: Social_Net_Block

Description: (Optional)

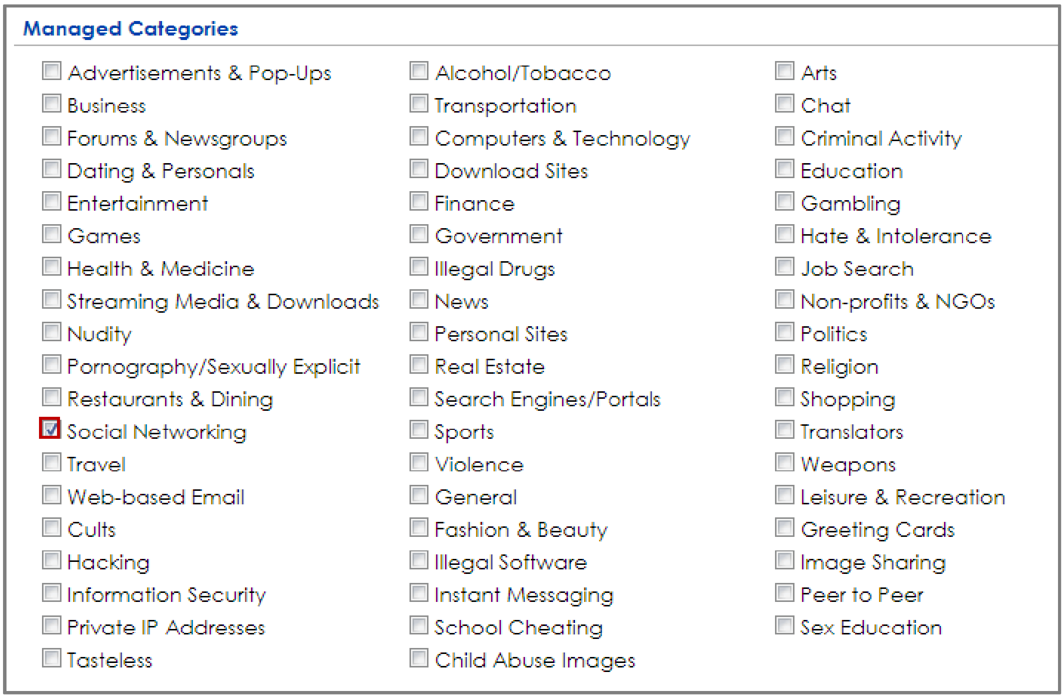
□ Enable SafeSearch

☑ Enable Content Filter Category Service

□ Log all web pages

Action for Unsafe Web Pages:	Block	□ Log
Action for Managed Web Pages:	Block	☑ Log
Action for Unrated Web Pages:	Warn	□ Log
Action When Category Server Is Unavailable:	Warn	□ Log

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.

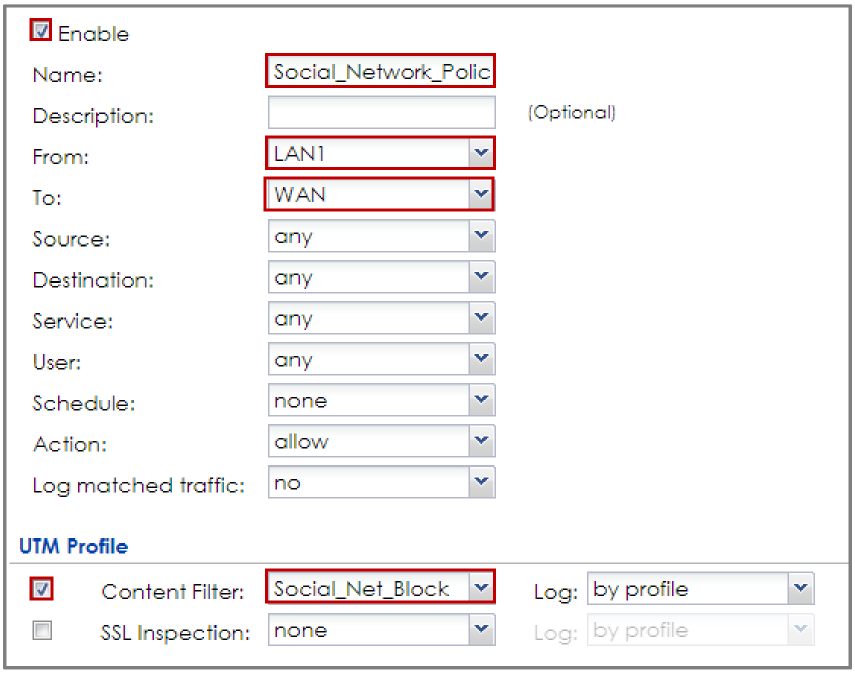


Managed Categories

- □ 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

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

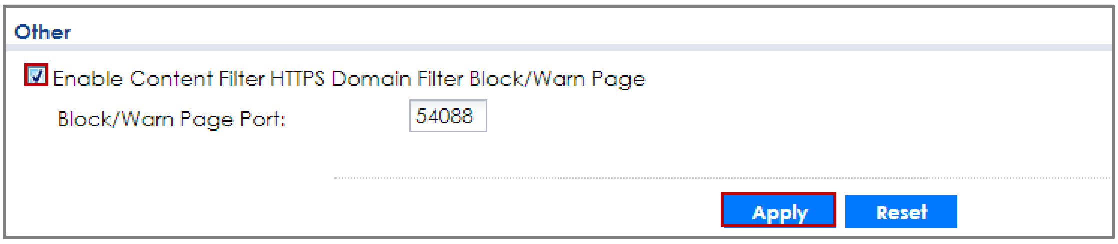
Name:	Social_Network_Polic	
Description:		(Optional)
From:	LAN1	
To:	WAN	
Source:	any	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	no	

UTM Profile

☑	Content Filter:	Social_Net_Block	Log:	by profile
□	SSL Inspection:	none	Log:	by profile

Set Up the System Policy on the ZyWALL/USG

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



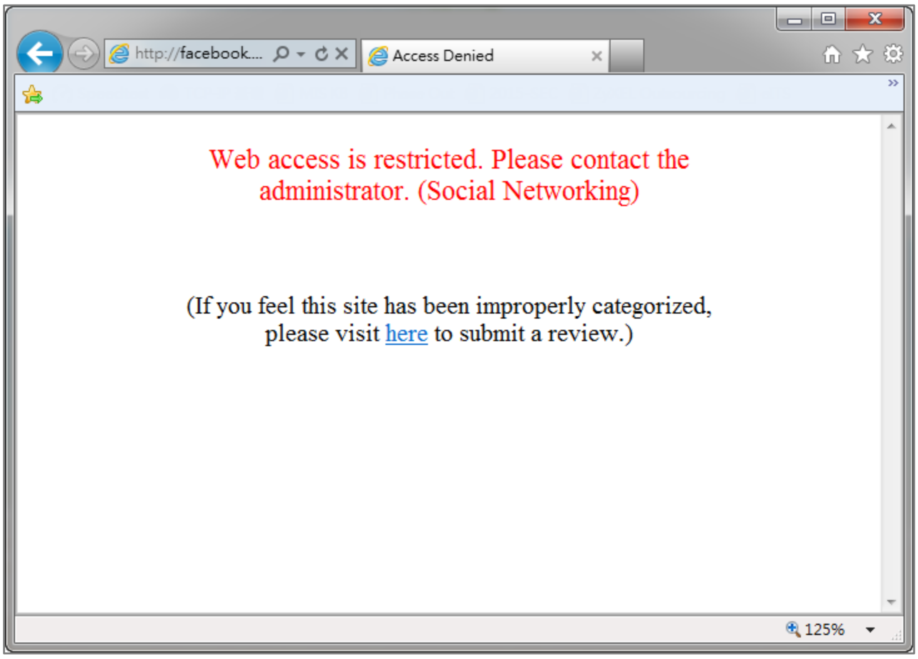
Other

☑ Enable Content Filter HTTPS Domain Filter Block/Warn Page

Block/Warn Page Port: 54088

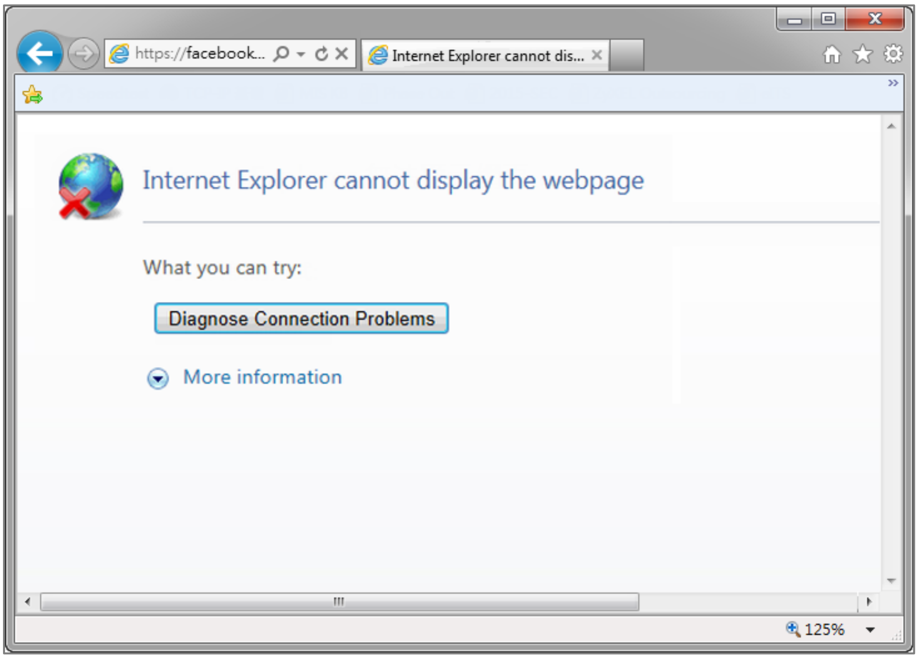
Test the Result

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.)

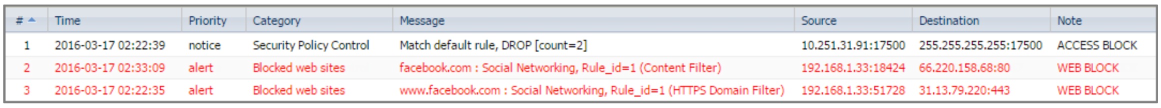


Internet Explorer cannot display the webpage

What you can try:

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.

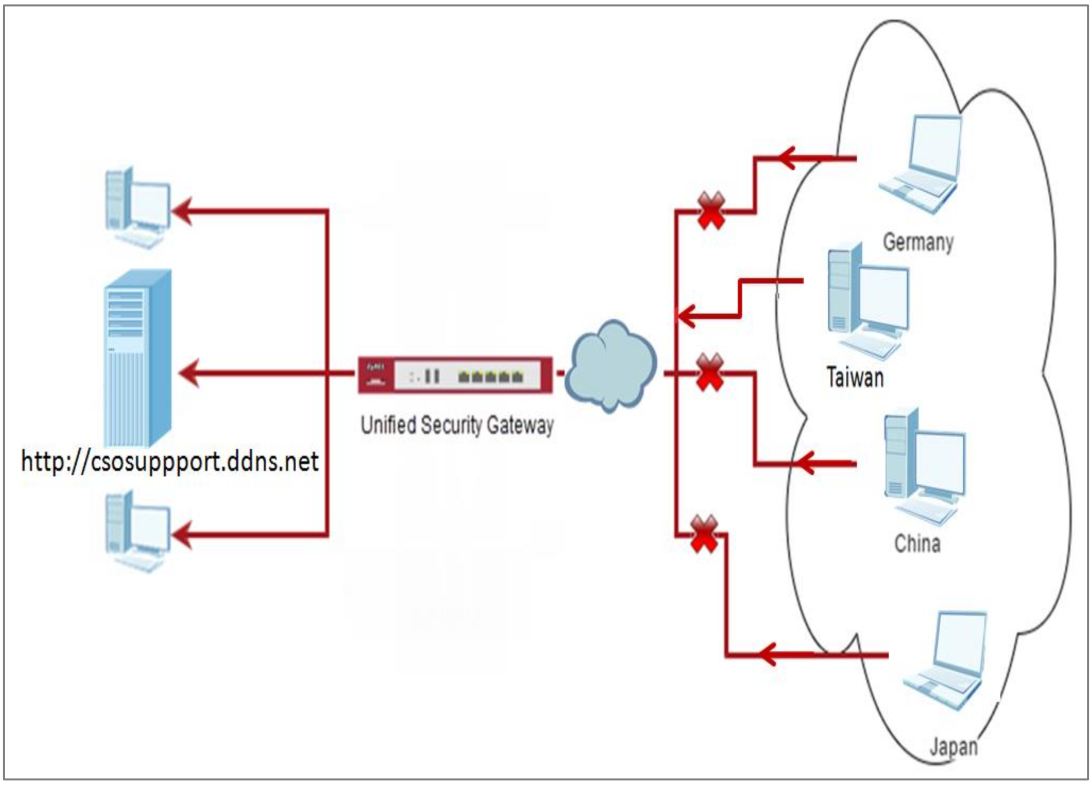
Monitor > Log



# ▲	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

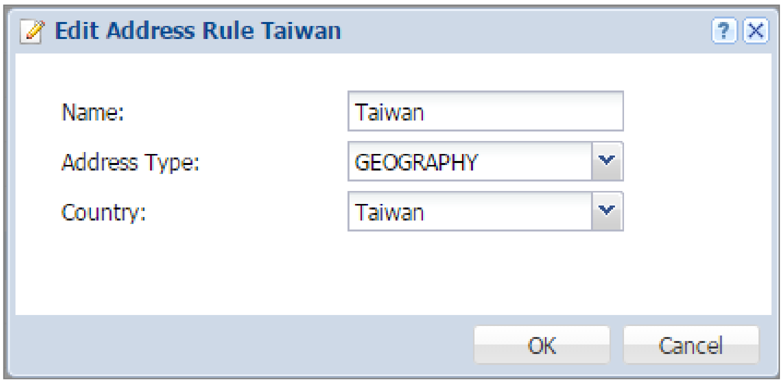
How to Configure Content Filter 2.0 with Geo IP Blocking

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.



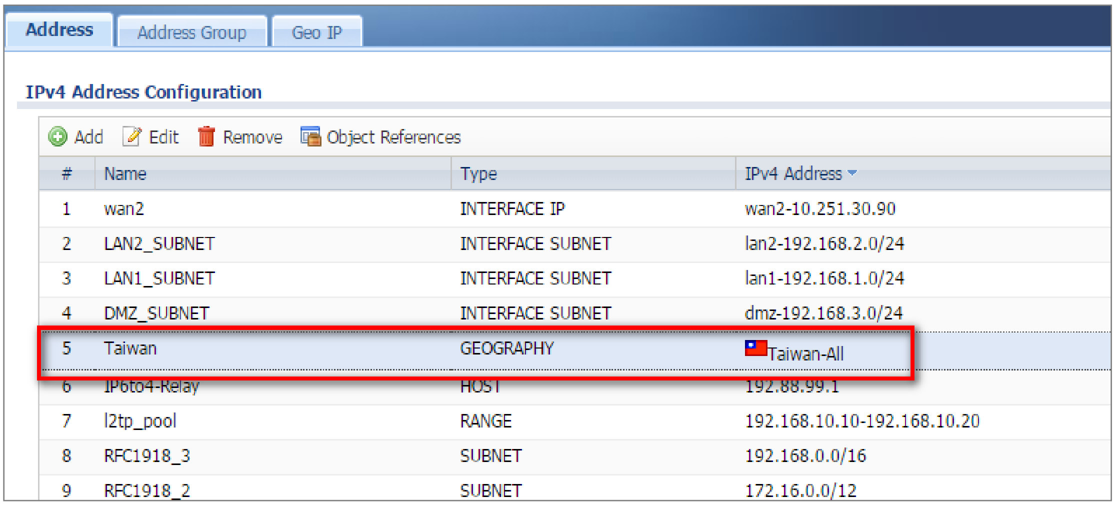
Set Up the Address Objet with Geo IP on the ZyWALL/USG

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



Name: Taiwan
Address Type: GEOGRAPHY
Country: Taiwan

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

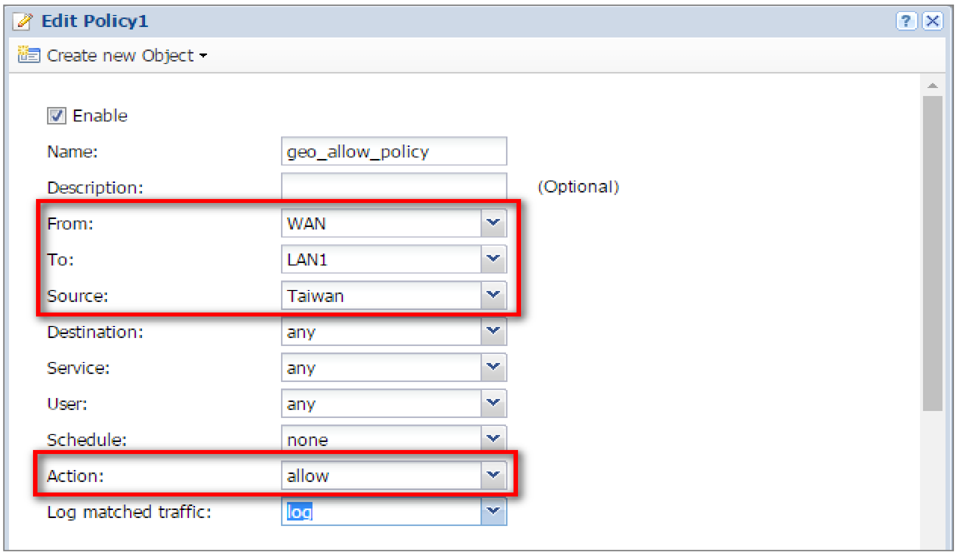


IPv4 Address Configuration

#	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

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).



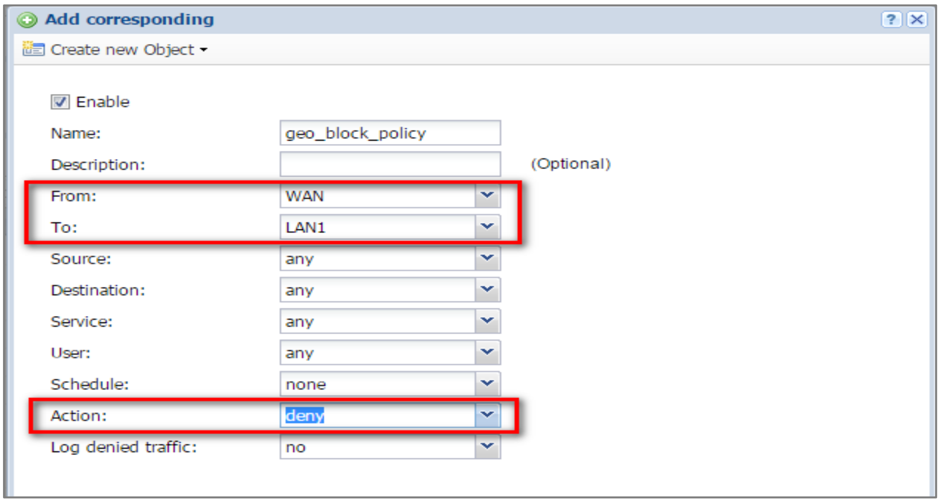
Edit Policy1

Create new Object

☑ 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

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

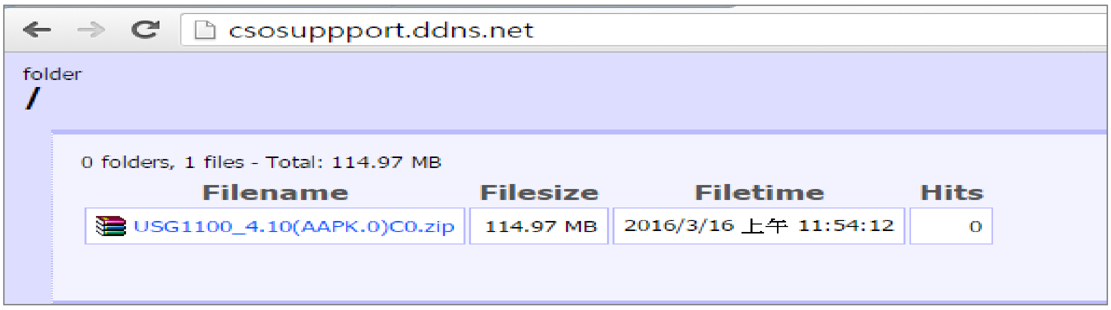
Create new Object

☑ 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

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



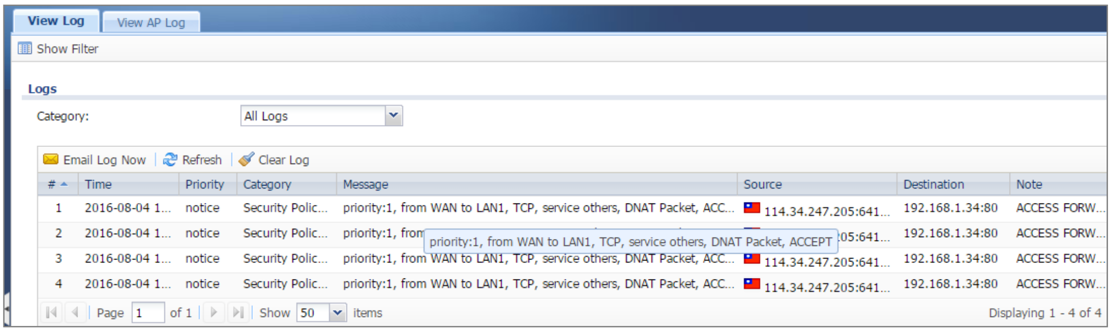
csosuppport.ddns.net

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

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

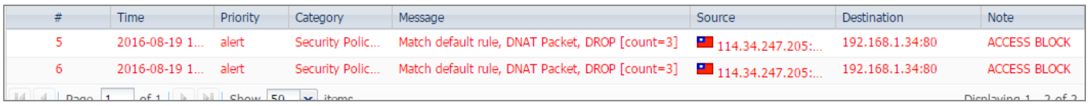
#	Time	Priority	Category	Message	Source	Destination	Note
1	2016-08-04 1...	notice	Security Polic...	priority:1, from WAN to LAN1, TCP, service others, DNAT Packet, ACC...	114.34.247.205:641...	192.168.1.34:80	ACCESS FORW...
2	2016-08-04 1...	notice	Security Polic...	priority:1, from	05:641...	192.168.1.34:80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

What Could Go Wrong?

1. The Security Policy configured wrong. The traffic cannot access the LAN server.



#	Time	Priority	Category	Message	Source	Destination	Note
5	2016-08-19 1...	alert	Security Polic...	Match default rule, DNAT Packet, DROP [count=3]	114.34.247.205:...	192.168.1.34:80	ACCESS BLOCK
6	2016-08-19 1...	alert	Security Polic...	Match default rule, DNAT Packet, DROP [count=3]	114.34.247.205:...	192.168.1.34:80	ACCESS BLOCK

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

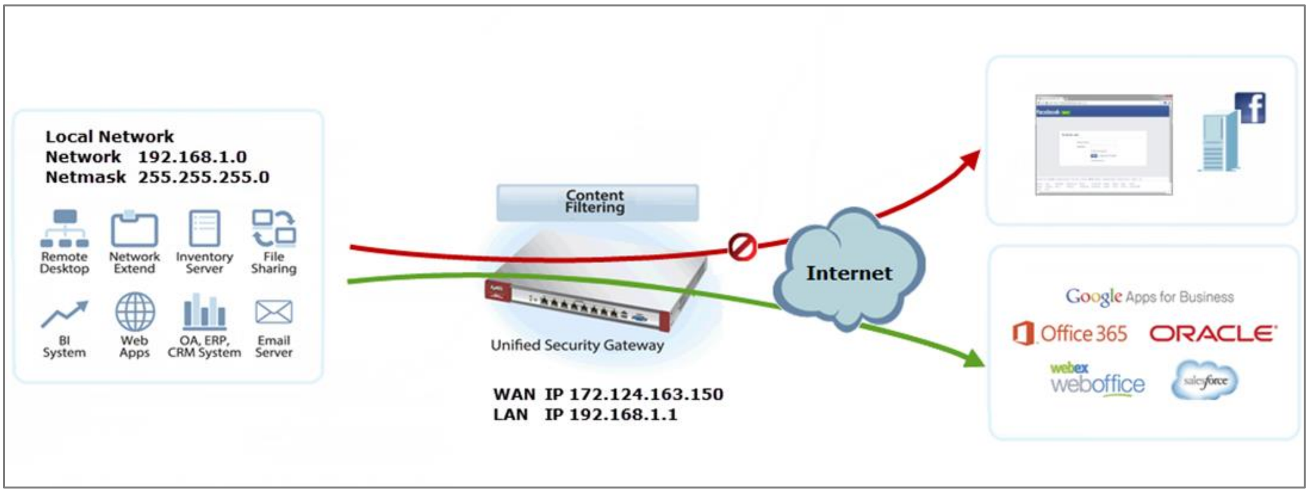
2. The Content-Filter service ix expired. Since Geo-IP server is bind with Content-Filter license, there must be available date for Content-Filter service.

How to Configure Content Filter 2.0 with HTTPs Domain Filter

Application Scenario

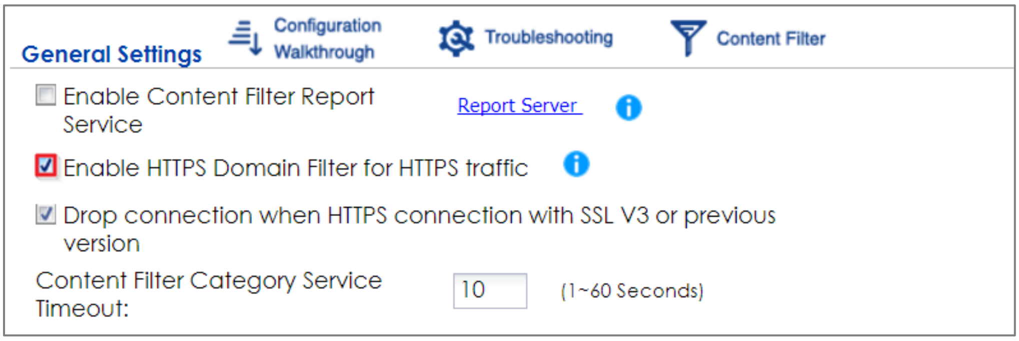
The Content Filter with HTTPs Domain Filter allows you to block HTTPs websites by category service without SSL-Inspection. The filtering feature is based on 64 categories built in ZyWALL/USG such as pornography, gambling, hacking, etc.

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.



Set Up the Content Filter on the ZyWALL/USG

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

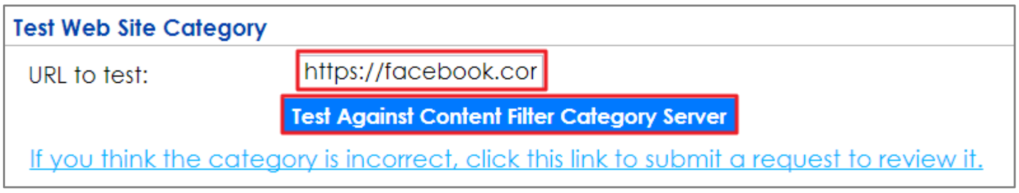
☑ Enable HTTPS Domain Filter for HTTPS traffic

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

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

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.**



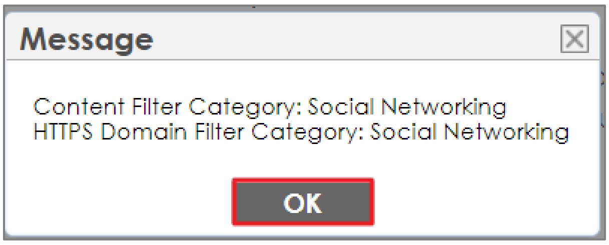
Test Web Site Category

URL to test: https://facebook.cor

Test Against Content Filter Category Server

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

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

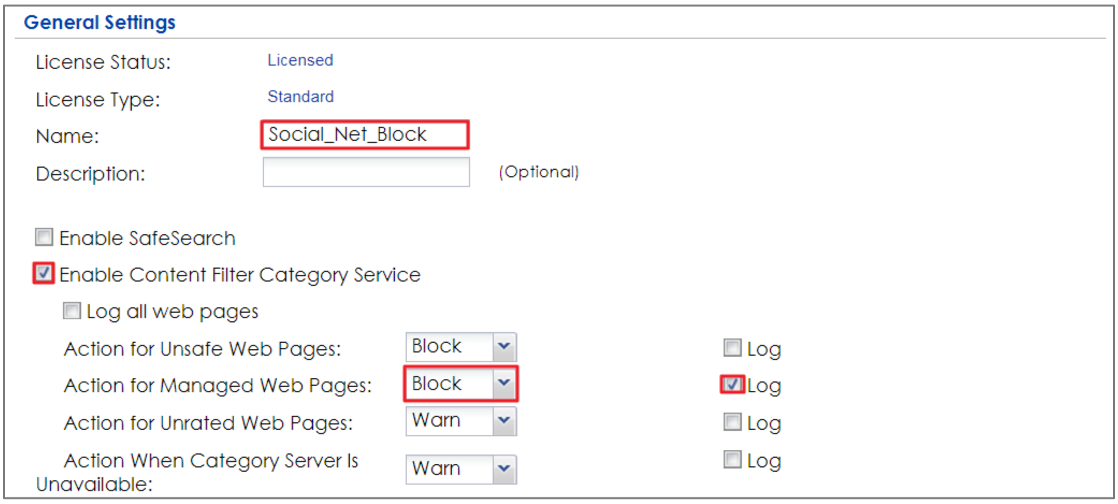


Message

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

OK

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: Standard

Name: Social_Net_Block

Description: (Optional)

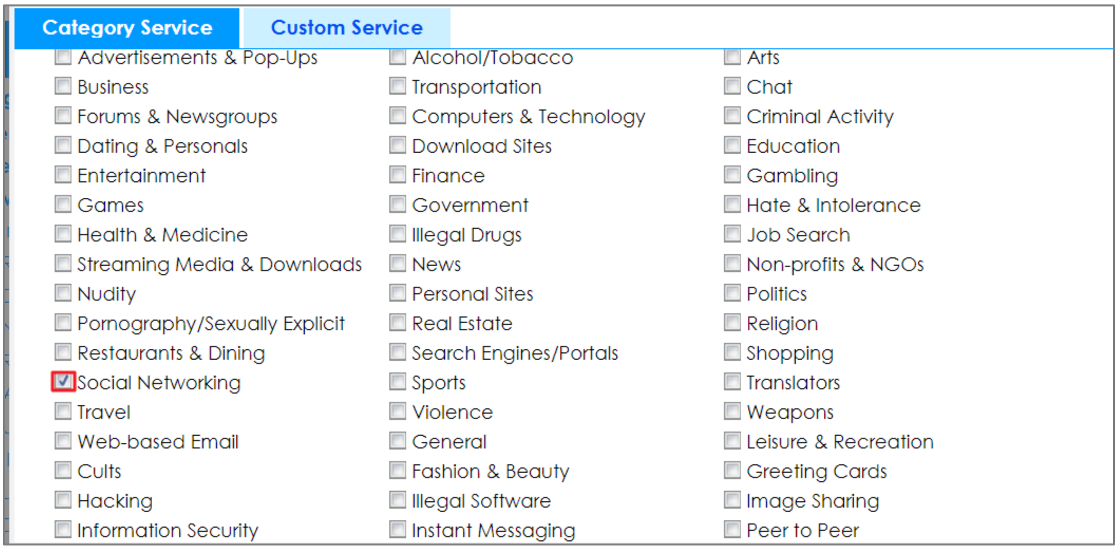
□ Enable SafeSearch

☑ Enable Content Filter Category Service

□ Log all web pages

Action for Unsafe Web Pages:	Block	□ Log
Action for Managed Web Pages:	Block	☑ Log
Action for Unrated Web Pages:	Warn	□ Log
Action When Category Server Is Unavailable:	Warn	□ Log

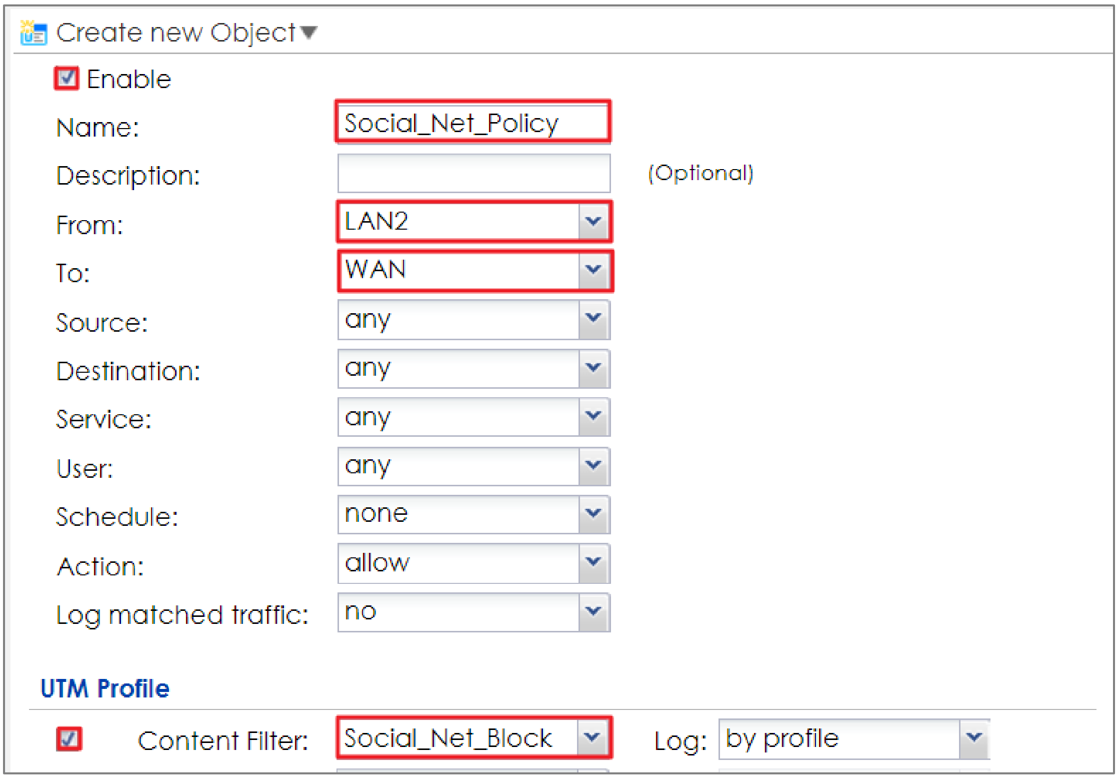
Scroll down to the **Managed Categories** section, select categories in this section to control access to specific types of Internet content. You must have the Content Filtering license to filter these categories.



- □ 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
- □ 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
- □ 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

Set Up the Security Policy on the ZyWALL/USG

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).



Create new Object▼

☑ Enable

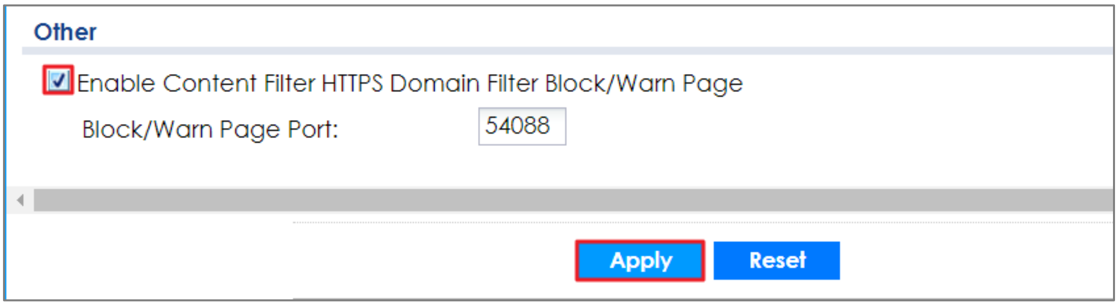
Name:	Social_Net_Policy	
Description:		(Optional)
From:	LAN2	
To:	WAN	
Source:	any	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	no	

UTM Profile

☑ Content Filter: Social_Net_Block Log: by profile

Set Up the System Policy on the ZyWALL/USG

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



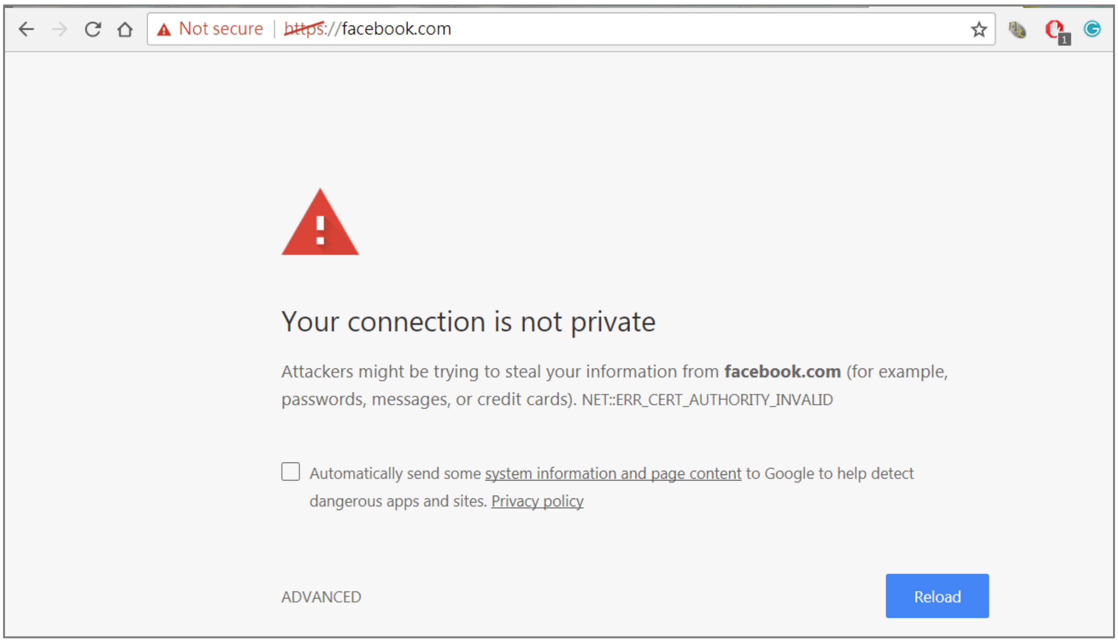
Other

☑ Enable Content Filter HTTPS Domain Filter Block/Warn Page

Block/Warn Page Port: 54088

Test the Result

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



Not secure | ~~https~~://facebook.com

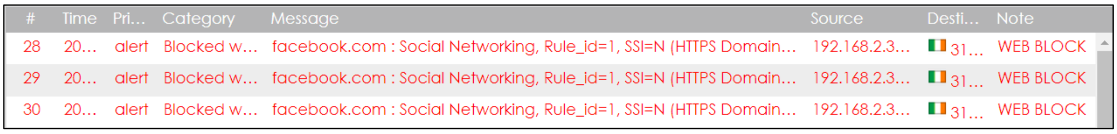
Your connection is not private

Attackers might be trying to steal your information from **facebook.com** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

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.

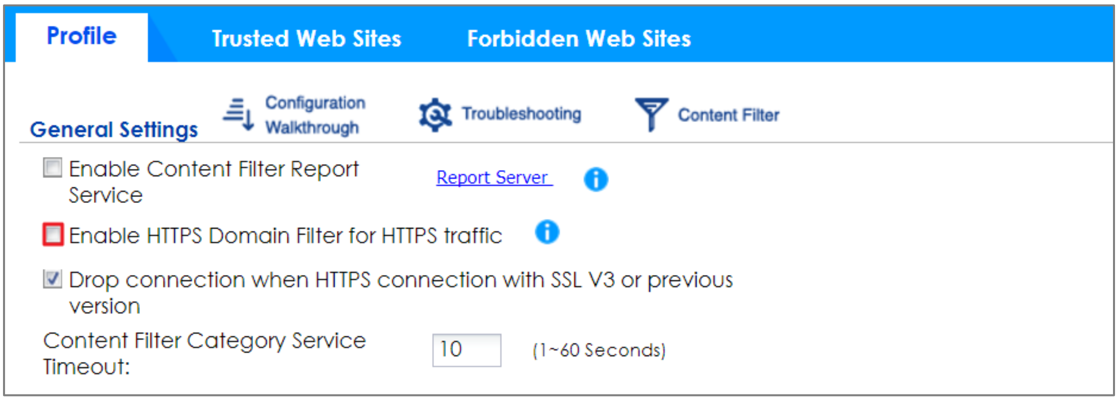
Monitor > Log



#	Time	Pri...	Category	Message	Source	Desti...	Note
28	20...	alert	Blocked w...	facebook.com : Social Networking, Rule_id=1, SSI=N (HTTPS Domain...	192.168.2.3...	31...	WEB BLOCK
29	20...	alert	Blocked w...	facebook.com : Social Networking, Rule_id=1, SSI=N (HTTPS Domain...	192.168.2.3...	31...	WEB BLOCK
30	20...	alert	Blocked w...	facebook.com : Social Networking, Rule_id=1, SSI=N (HTTPS Domain...	192.168.2.3...	31...	WEB BLOCK

What Could Wrong?

1. "Enable HTTPS Domain Filter for HTTPS traffic" is not checked.



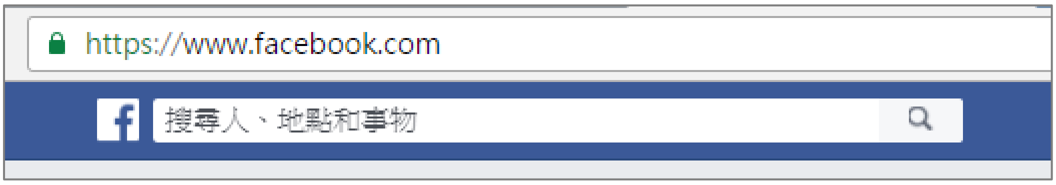
□ Enable Content Filter Report Service Report Server

□ 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)

HTTPs traffic will pass.

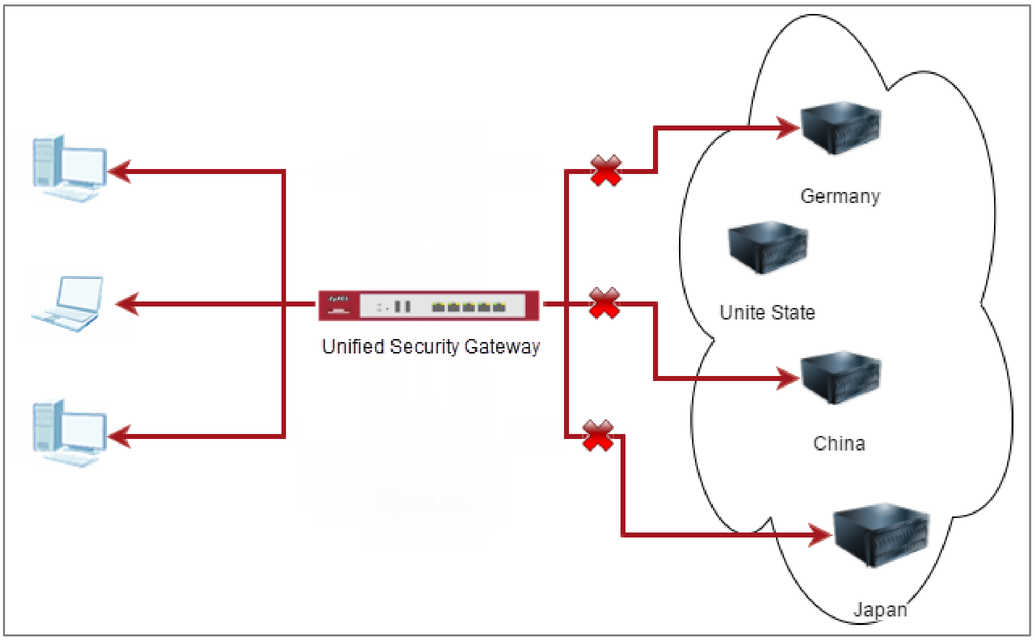


How to block the client accessing to certain country using Geo IP and Content Filter

The Content Filter with Geo IP 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.

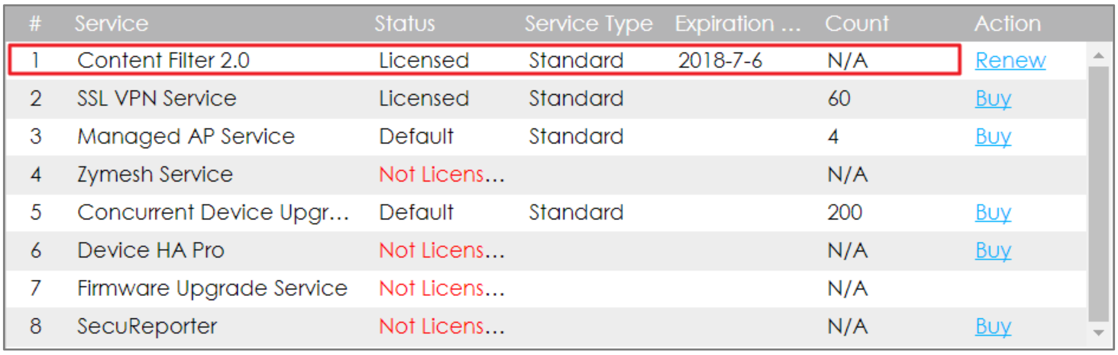
ZyWALL/USG Geo IP Example



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25)

Check Geo IP License Status on the ZyWALL/USG

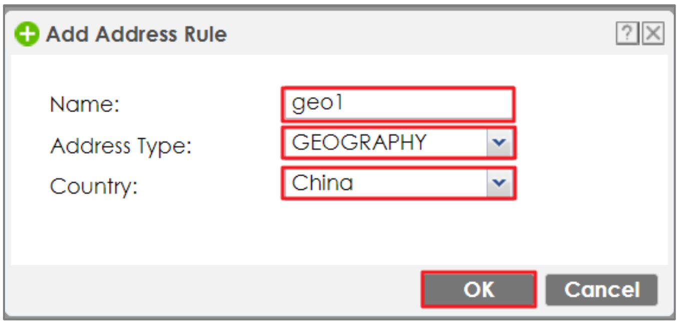
Go to **CONFIGURATION > Licensing > Registration > Service**, the **Geo IP Service** should be **Licensed** to configure this feature.



#	Service	Status	Service Type	Expiration ...	Count	Action
1	Content Filter 2.0	Licensed	Standard	2018-7-6	N/A	Renew
2	SSL VPN Service	Licensed	Standard		60	Buy
3	Managed AP Service	Default	Standard		4	Buy
4	Zymesh Service	Not Licens...			N/A	
5	Concurrent Device Upgr...	Default	Standard		200	Buy
6	Device HA Pro	Not Licens...			N/A	Buy
7	Firmware Upgrade Service	Not Licens...			N/A	
8	SecuReporter	Not Licens...			N/A	Buy

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

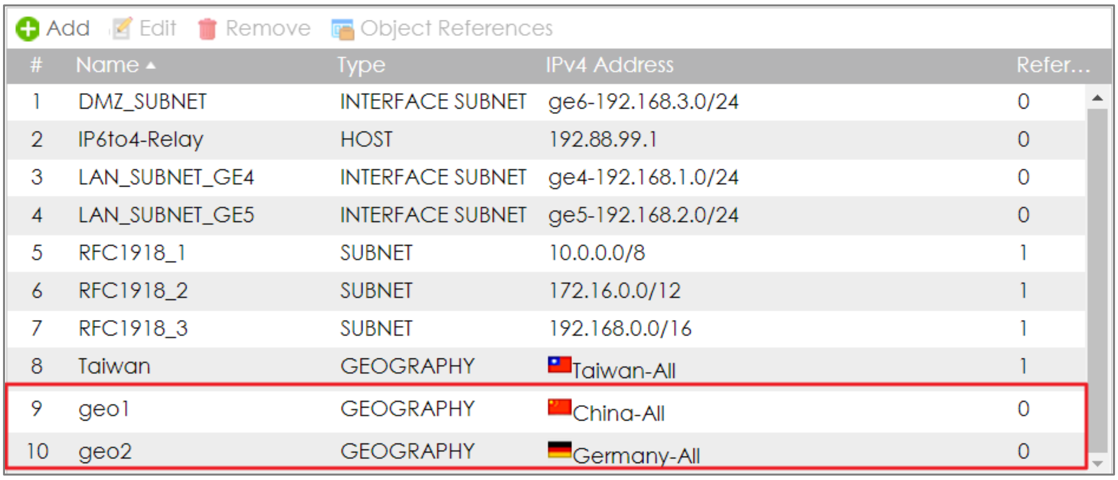
Go to **CONFIGURATION > Object > Address/Geo IP > Address > Add Address Rule**.



Add Address Rule

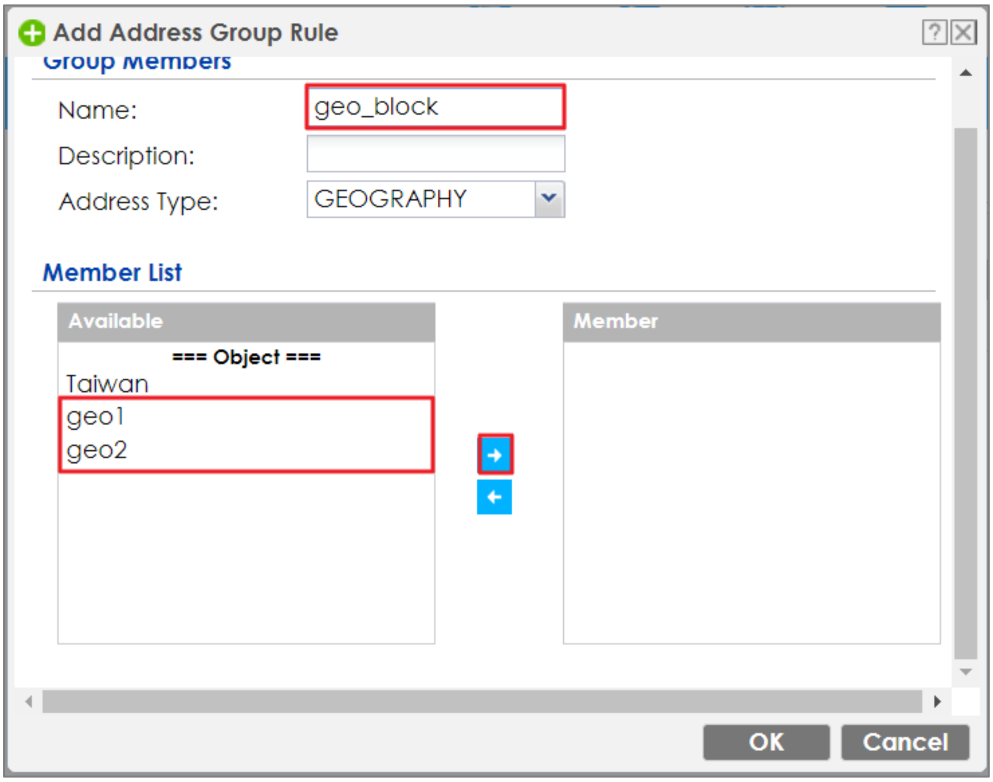
Name:	geo1
Address Type:	GEOGRAPHY
Country:	China

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



#	Name ▴	Type	IPv4 Address	Refer...
1	DMZ_SUBNET	INTERFACE SUBNET	ge6-192.168.3.0/24	0
2	IP6to4-Relay	HOST	192.88.99.1	0
3	LAN_SUBNET_GE4	INTERFACE SUBNET	ge4-192.168.1.0/24	0
4	LAN_SUBNET_GE5	INTERFACE SUBNET	ge5-192.168.2.0/24	0
5	RFC1918_1	SUBNET	10.0.0.0/8	1
6	RFC1918_2	SUBNET	172.16.0.0/12	1
7	RFC1918_3	SUBNET	192.168.0.0/16	1
8	Taiwan	GEOGRAPHY	Taiwan-All	1
9	geo1	GEOGRAPHY	China-All	0
10	geo2	GEOGRAPHY	Germany-All	0

Go to **CONFIGURATION > Object > Address/Geo IP > Address Group> Add Address Group Rule**, add all customized GEOGRAPHY address into the same **Member** object.


Add Address Group Rule

Group Members

Name: geo_block

Description:

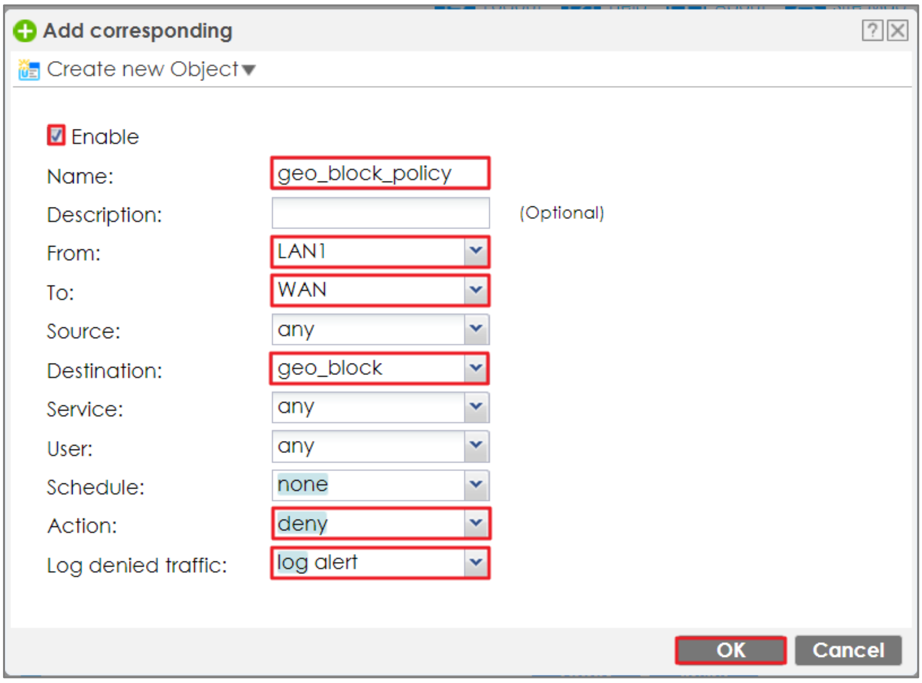
Address Type: GEOGRAPHY

Member List

Available	Member
=== Object === Taiwan geo1 geo2	

Set Up the Security Policy on the ZyWALL/USG

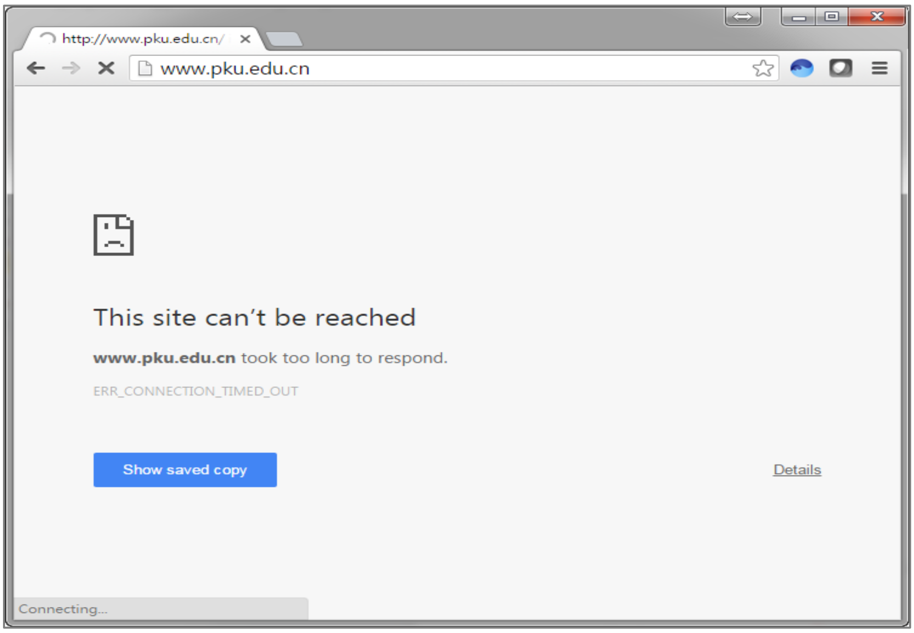
Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set deny Geo IP traffic from LAN to WAN (geo_block_policy in this example).



☑ Enable	
Name:	geo_block_policy
Description:	(Optional)
From:	LAN1
To:	WAN
Source:	any
Destination:	geo_block
Service:	any
User:	any
Schedule:	none
Action:	deny
Log denied traffic:	log alert

Test the Result

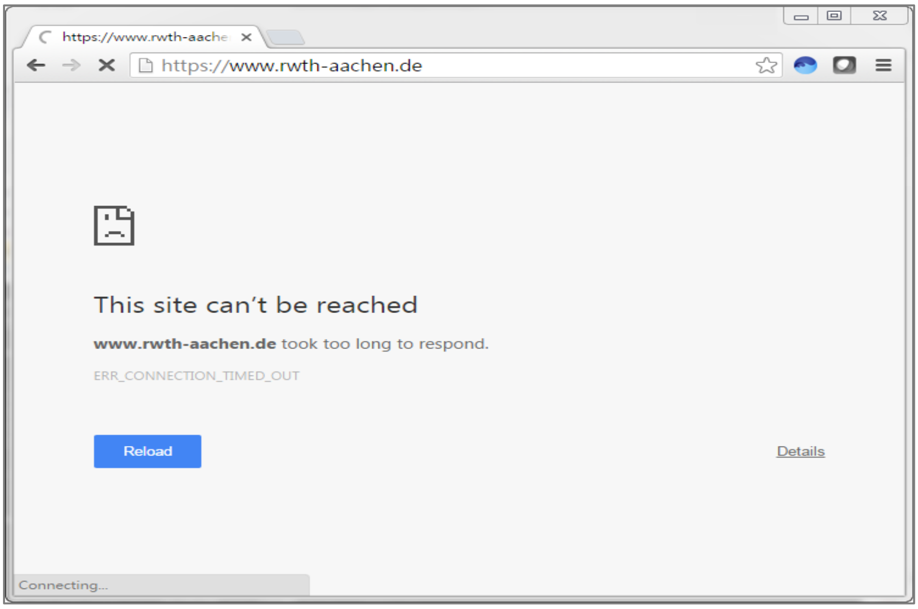
Type http://www.pku.edu.cn/ or https://www.rwth-aachen.de/ into the browser, sites can’t be reached.



This site can’t be reached

www.pku.edu.cn took too long to respond.

ERR_CONNECTION_TIMED_OUT



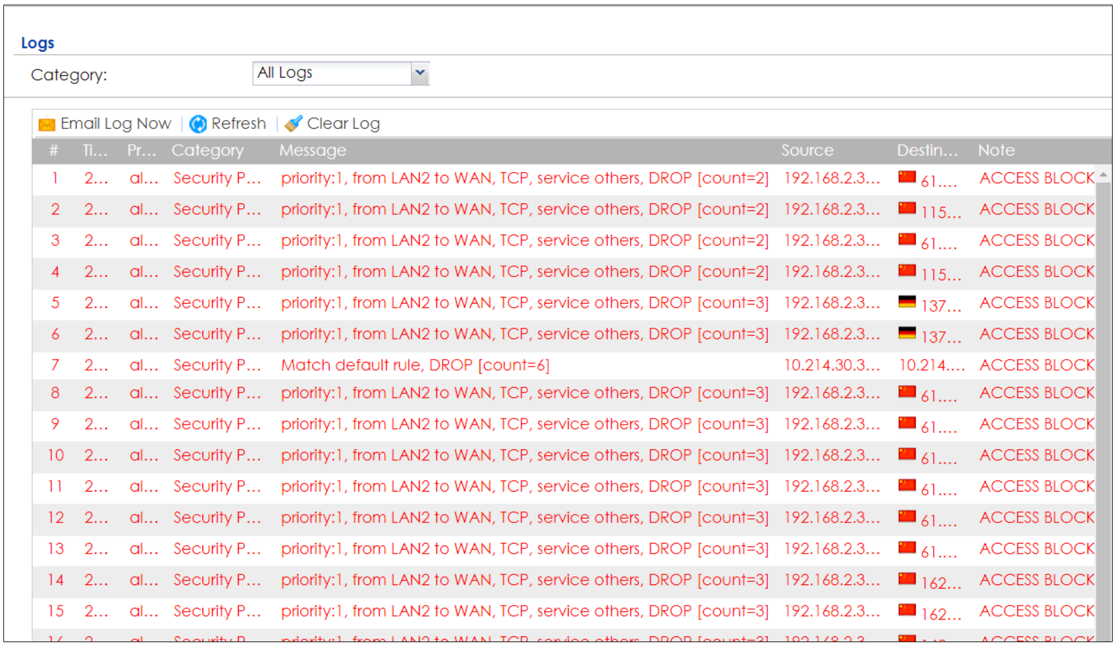
https://www.rwth-aachen.de

This site can’t be reached

www.rwth-aachen.de took too long to respond.

ERR_CONNECTION_TIMED_OUT

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.



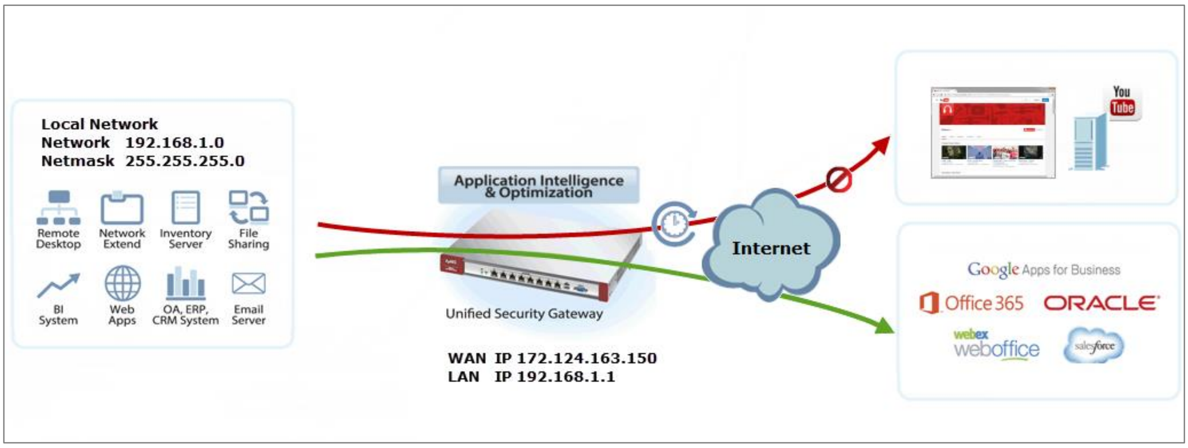
Logs

Category: All Logs

#	Ti...	Pr...	Category	Message	Source	Destin...	Note
1	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2]	192.168.2.3...	🇨🇳 61....	ACCESS BLOCK
2	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2]	192.168.2.3...	🇨🇳 115...	ACCESS BLOCK
3	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2]	192.168.2.3...	🇨🇳 61....	ACCESS BLOCK
4	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2]	192.168.2.3...	🇨🇳 115...	ACCESS BLOCK
5	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	🇩🇪 137...	ACCESS BLOCK
6	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	🇩🇪 137...	ACCESS BLOCK
7	2...	al...	Security P...	Match default rule, DROP [count=6]	10.214.30.3...	10.214....	ACCESS BLOCK
8	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	🇨🇳 61....	ACCESS BLOCK
9	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	🇨🇳 61....	ACCESS BLOCK
10	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	🇨🇳 61....	ACCESS BLOCK
11	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	🇨🇳 61....	ACCESS BLOCK
12	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	🇨🇳 61....	ACCESS BLOCK
13	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	🇨🇳 61....	ACCESS BLOCK
14	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	🇨🇳 162...	ACCESS BLOCK
15	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	🇨🇳 162...	ACCESS BLOCK
16	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	🇨🇳 1...	ACCESS BLOCK

How To Schedule YouTube Access

This is an example of using the ZyWALL/USG UTM Profile and Security Policy to control access to the network. If an application should not have network access during certain hours, you can use Application Patrol, SSL Inspection and Schedule settings to make sure that these applications cannot access the Internet.



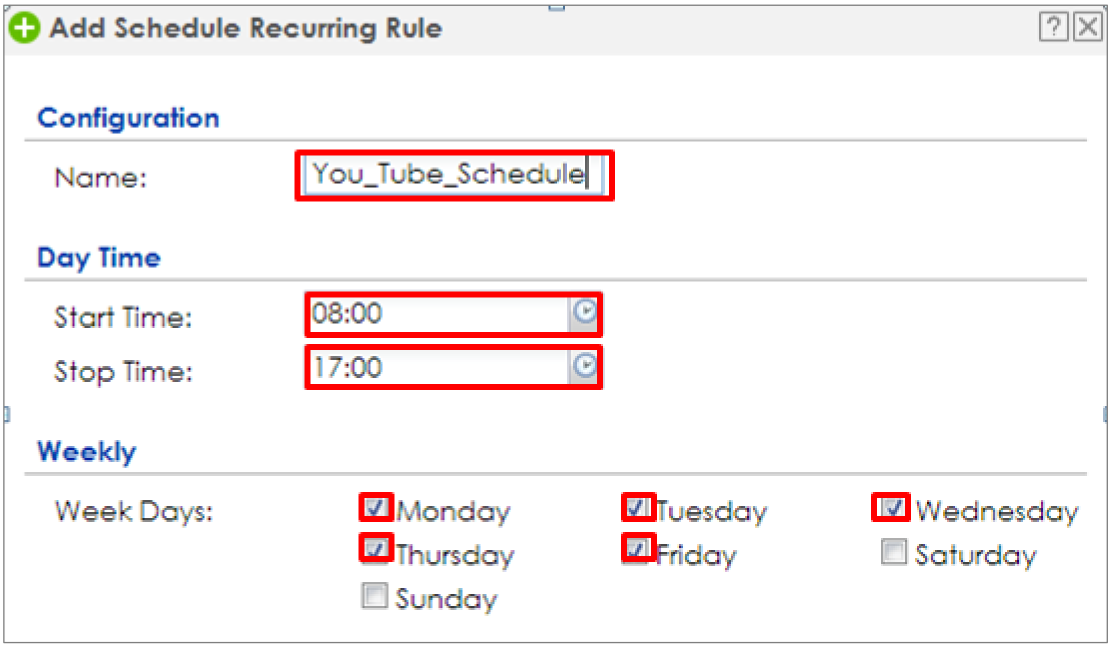
ZyWALL/USG with Scheduled YouTube Access Settings Example

> Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Schedule on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > Schedule > Recurring > Add Schedule Recurring Rule**. Configure a **Name** for you to identify the **Schedule Recurring Rule**. Specify the **Day Time** hour and minute when the schedule begins and ends each day. In the **Weekly** schedule, select each day of the week that the recurring schedule is effective.

CONFIGURATION > Object > Schedule > Recurring



Add Schedule Recurring Rule

Configuration

Name: You_Tube_Schedule

Day Time

Start Time: 08:00

Stop Time: 17:00

Weekly

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

Create the Application Objects on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > Application > Add Application Rule**. Configure a **Name** for you to identify the **Application Profile**. Then, click **Add** to create an **Application Object**.

CONFIGURATION > Object > Application > Add Application Rule

In the **Application Object**, select **By Service**, type a keyword and click **Search** to display all signatures containing that keyword. Check all **Query Result** and Click **OK**.

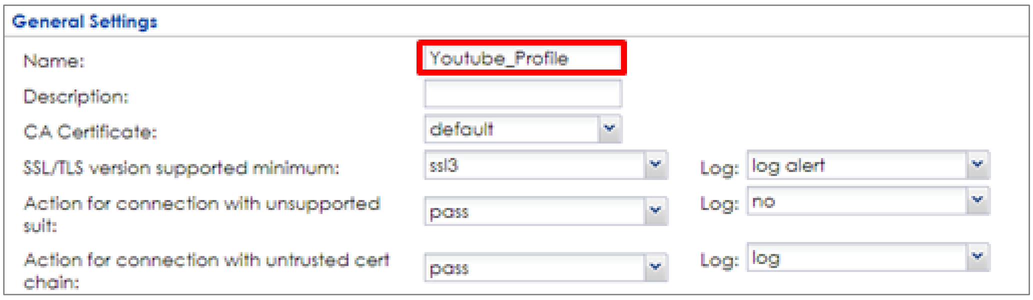
CONFIGURATION > Object > Application > Add Application Rule > Add Application Object

Set Up SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select **Block** to **Action for Connection with SSL v3** and select **Log** type to be **log alert**. Leave other actions as default settings.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule



General Settings

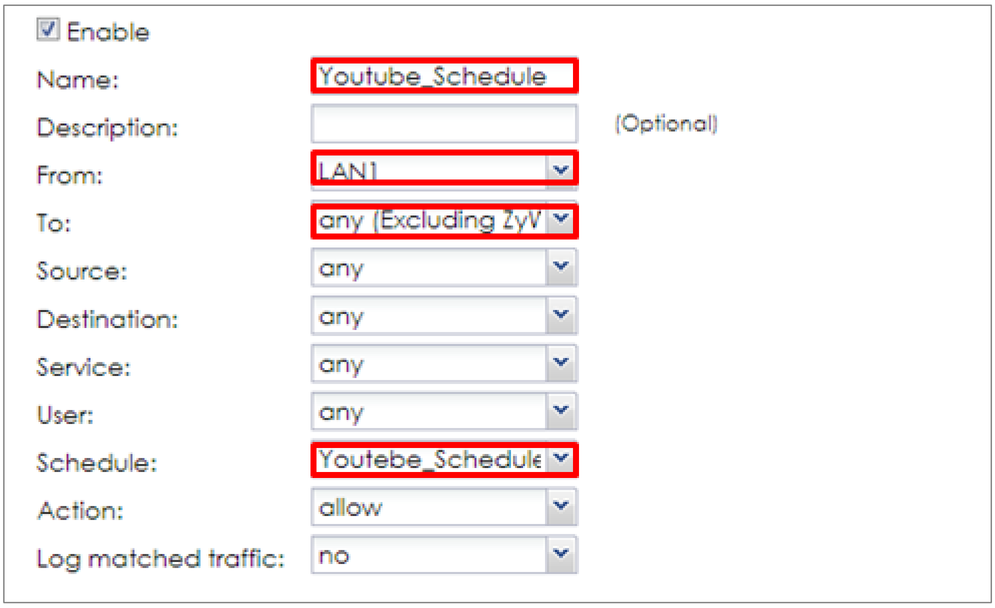
Name:	Youtube_Profile		
Description:			
CA Certificate:	default		
SSL/TLS version supported minimum:	ssl3	Log:	log alert
Action for connection with unsupported suit:	pass	Log:	no
Action for connection with untrusted cert chain:	pass	Log:	log

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select the **Schedule** that defines when the policy applies (Youtube_Schedule in this example).

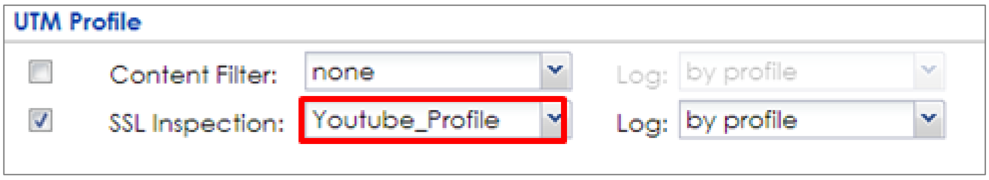
Scroll down to **UTM Profile**, check **Application Patrol** and select a profile from the list box (Youtube_profile in this example). Then, check **SSL Inspection** and select a profile from the list box (Youtube in this example).

CONFIGURATION > Security Policy > Policy Control



☑ Enable

Name:	Youtube_Schedule	
Description:		(Optional)
From:	LAN1	
To:	any (Excluding ZyV	
Source:	any	
Destination:	any	
Service:	any	
User:	any	
Schedule:	Youtebe_Schedule	
Action:	allow	
Log matched traffic:	no	



UTM Profile

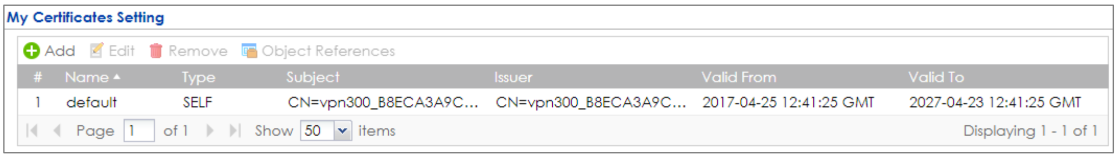
□	Content Filter:	none	Log:	by profile
☑	SSL Inspection:	Youtube_Profile	Log:	by profile

Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG.

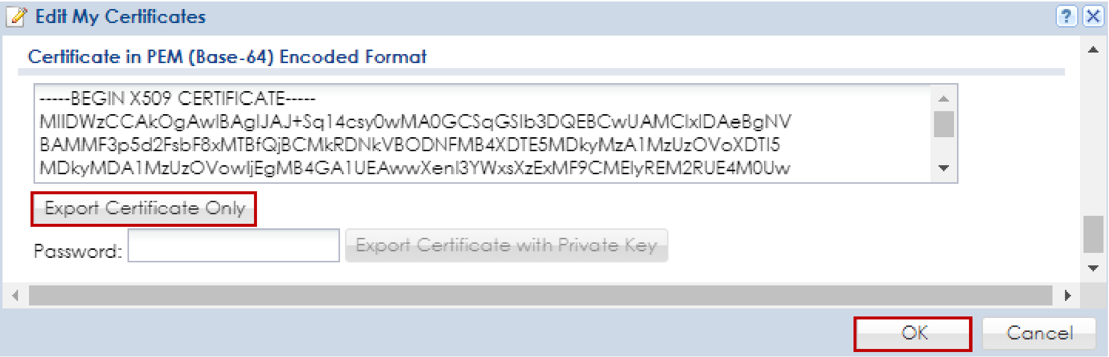
CONFIGURATION > Object > Certificate > default



My Certificates Setting

#	Name	Type	Subject	Issuer	Valid From	Valid To
1	default	SELF	CN=vpn300_B8ECA3A9C...	CN=vpn300_B8ECA3A9C...	2017-04-25 12:41:25 GMT	2027-04-23 12:41:25 GMT

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only



Edit My Certificates

Certificate in PEM (Base-64) Encoded Format

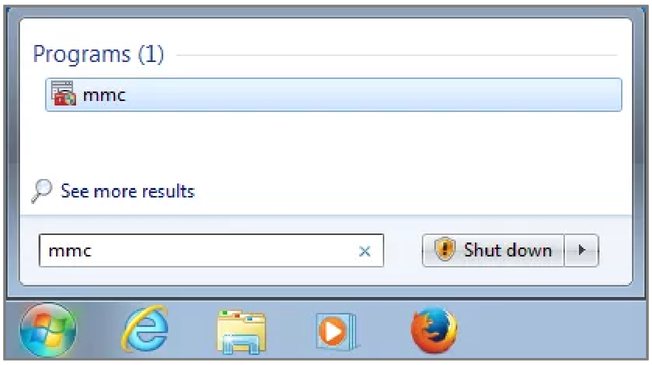
```
-----BEGIN X509 CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIJAJ+Sq14csy0wMA0GCSqGSIb3DQEBCwUAMClxIDAeBgNV
BAMMF3p5d2FsbF8xMTBfQjBCMkRDNkVBODNFMB4XDTE5MDkyMzA1MzUzOVoXDTI5
MDkyMDA1MzUzOVowIjEgMB4GA1UEAwwXenl3YWxsXzExMF9CMElyREM2RUE4M0Uw
```

Save default certificate as *crt file to Windows 7 Operation System.

default.crt

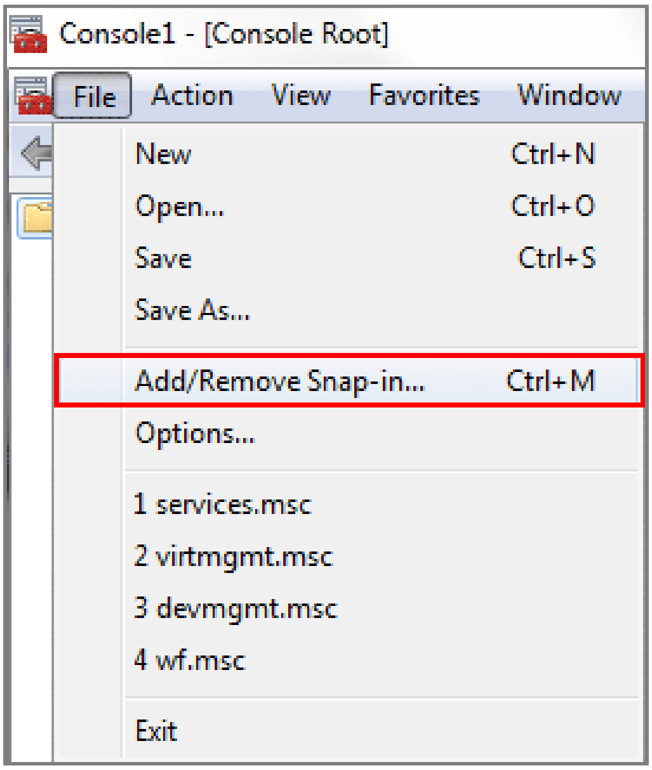
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



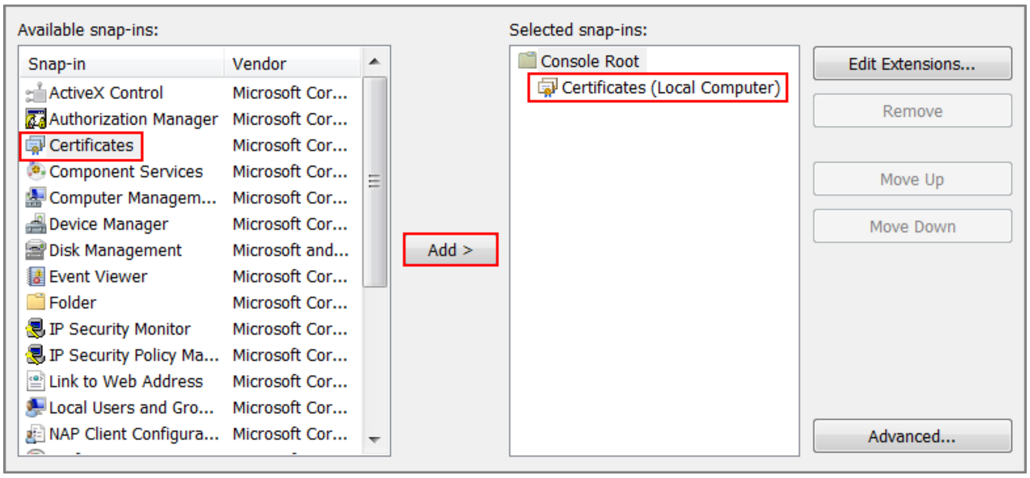
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

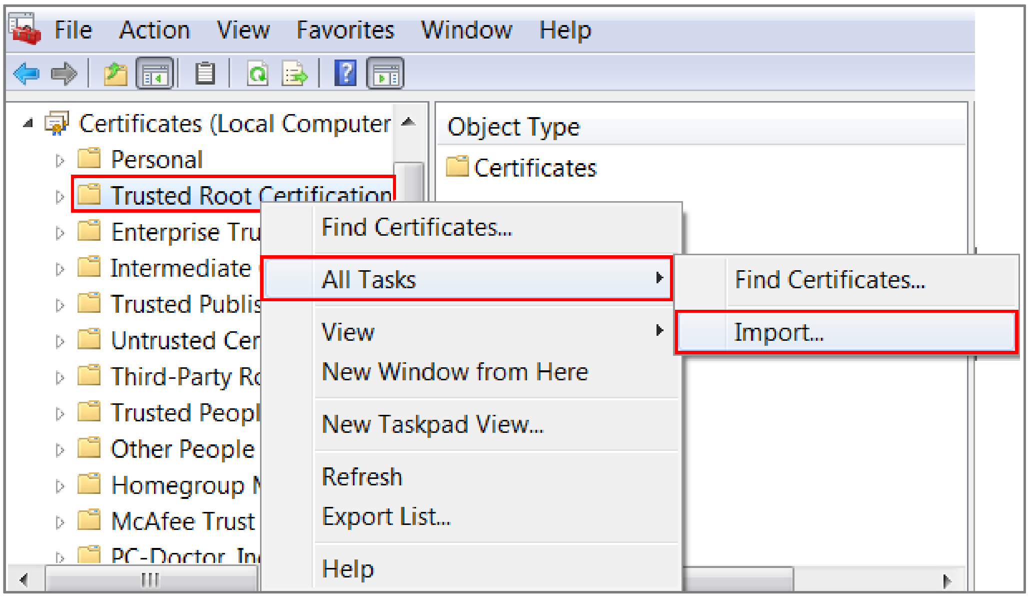


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

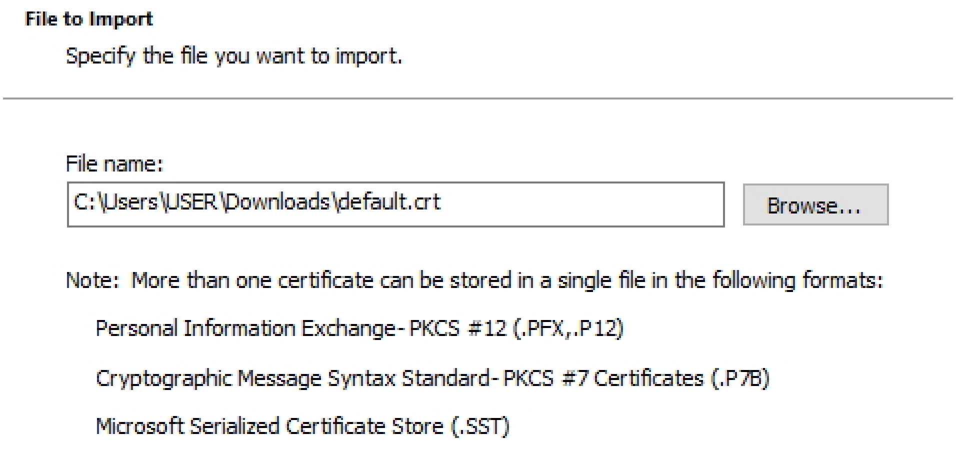
Available snap-ins > Certificates > Add


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...
IP Security Monitor | Microsoft Cor...
IP Security Policy Ma... | Microsoft Cor...
Link to Web Address | Microsoft Cor...
Local Users and Gro... | Microsoft Cor...
NAP Client Configura... | Microsoft Cor...
Add >
Selected snap-ins:
Console Root
Certificates (Local Computer)
Edit Extensions...
Remove
Move Up
Move Down
Advanced...

In the mmc console window, open the **Certificates (Local Computer) > Trusted Root Certification Authorities,** right click **Certificate > All Tasks > Import…**



Click **Next,** Then, **Browse...,** and locate the .crt file you downloaded earlier. Then, click **Next**.



File to Import

Specify the file you want to import.

File name:

C:\Users\USER\Downloads\default.crt

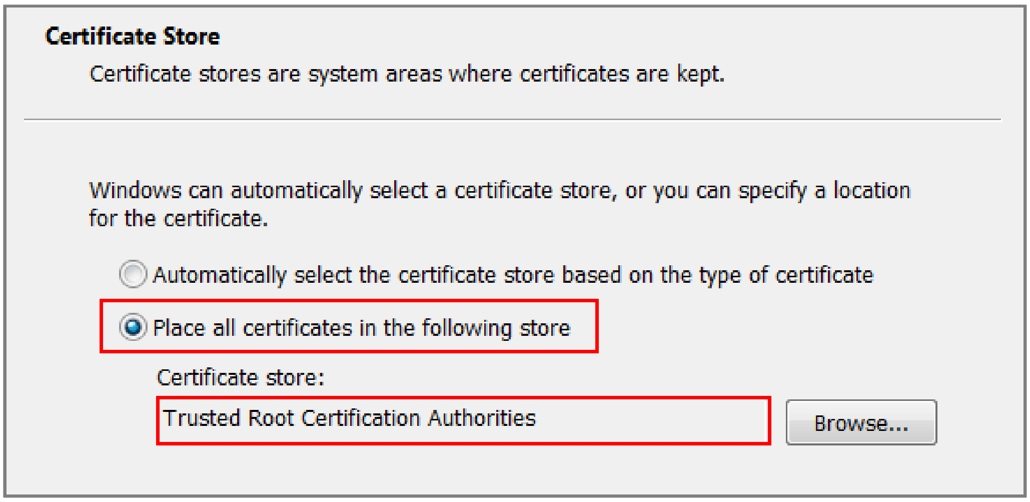
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities.** Click **Next**, then click **Finish**.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

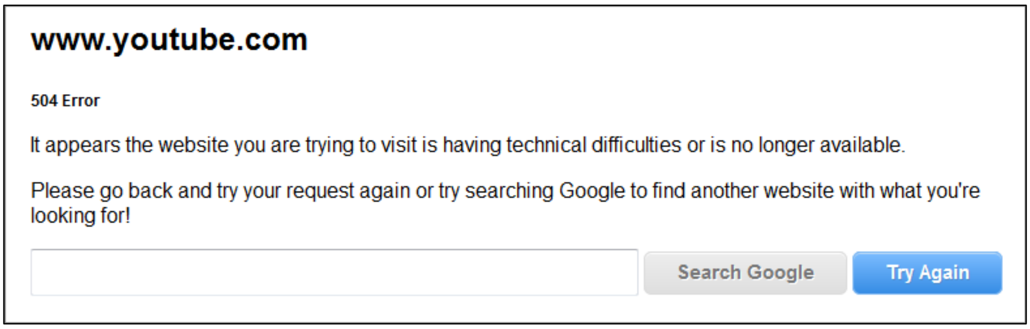
Trusted Root Certification Authorities

Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to the default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Test the Result

Type http://www.youtube.com/ or https://www.youtube.com/ into the browser.

An error message occurs.



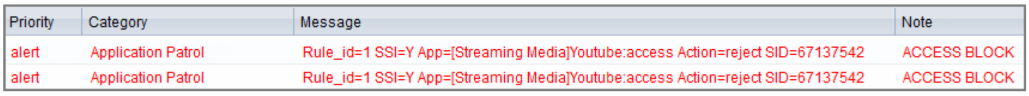
www.youtube.com

504 Error

It appears the website you are trying to visit is having technical difficulties or is no longer available.

Please go back and try your request again or try searching Google to find another website with what you're looking for!

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.



Priority	Category	Message	Note
alert	Application Patrol	Rule_id=1 SSI=Y App=[Streaming Media]Youtube:access Action=reject SID=67137542	ACCESS BLOCK
alert	Application Patrol	Rule_id=1 SSI=Y App=[Streaming Media]Youtube:access Action=reject SID=67137542	ACCESS BLOCK

What Could Go Wrong?

If you are not be able to configure any **Application Patrol** policies or it's not working, there are two possible reasons:

You have not subscribed for the **Application Patrol** service.

You have subscribed for the **Application Patrol** service but the license is expired.

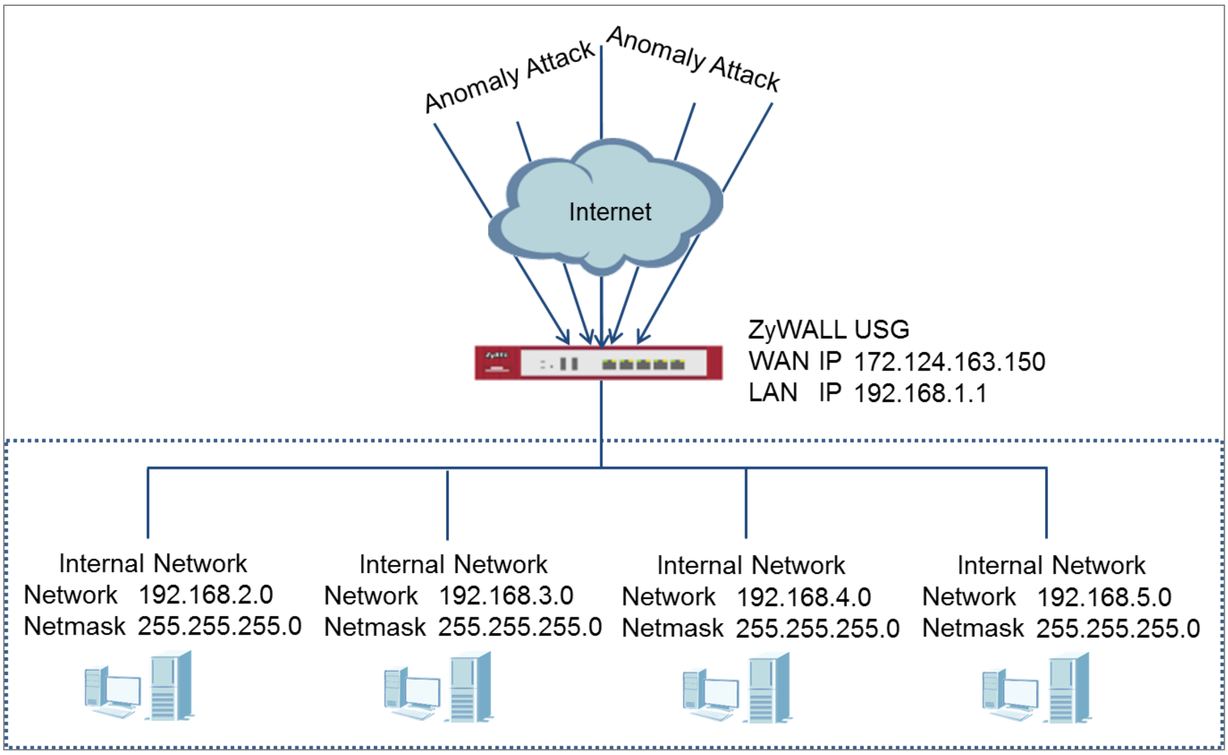
You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **Application Patrol** license.

After you apply the **Application Patrol** service, the running session will continue till it's finished.

How to Detect and Prevent TCP Port Scanning with ADP

This is an example of using a ZyWALL/USG ADP (Anomaly Detection and Prevention) Profile to protect against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal traffic flows such as port scans.

ZyWALL/USG with ADP Profile Setting Example

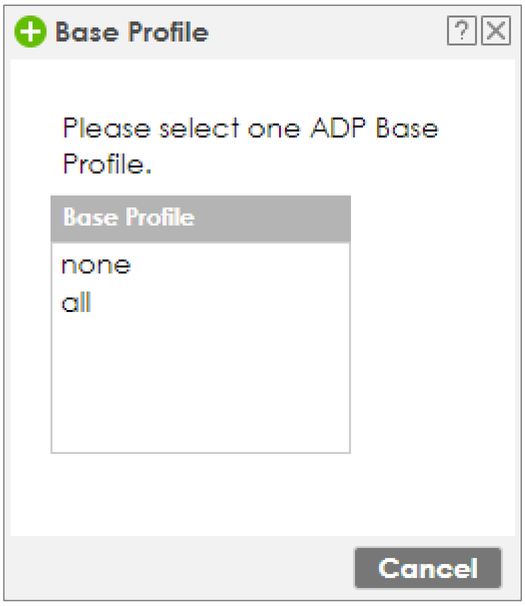


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the ADP Profile on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > ADP > Profile,** click the **Add** icon. A pop-up screen will appear allowing you to choose a base profile. Select a base profile to go to the profile details screen.

CONFIGURATION > Security Policy > ADP > Profile > Base Profile



Base Profile

Please select one ADP Base Profile.

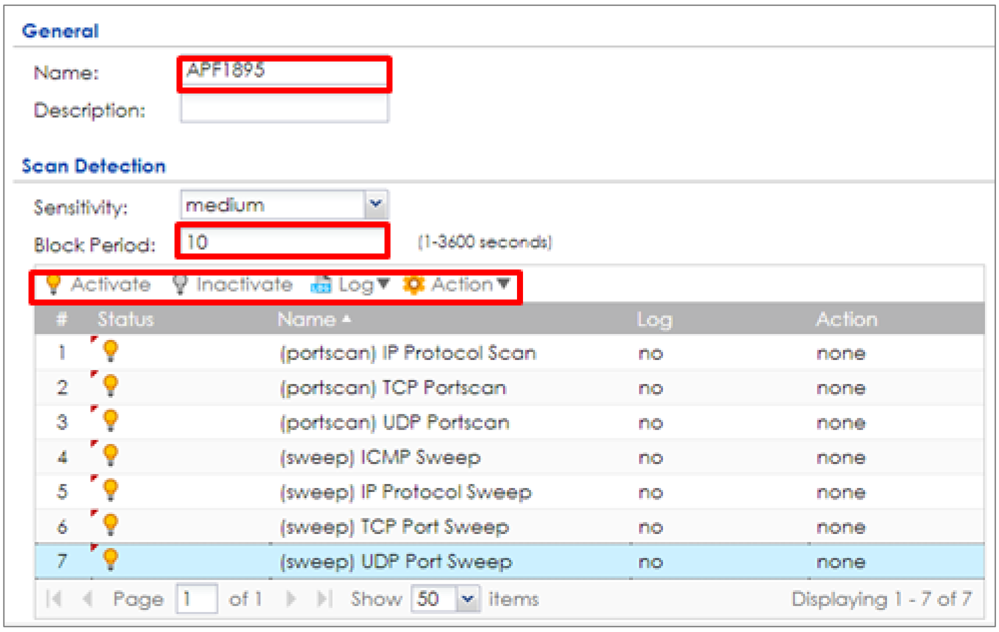
Base Profile
none
all

The **Traffic Anomaly** screen will display. A **Name** is automatically generated that you can edit. Enable or disable individual scan or flood types by selecting a row and clicking **Activate** or **Inactivate**.

In the **Scan Detection** section, selecting levels in the **Sensitivity** drop-down menu and set **Block Period** for the duration applies blocking to the source IP address.

In the **Flood Detection** section, set **Block Period** for the duration applies blocking to the destination IP address. Set a **Threshold** number (the number of packets per second that match the flood detection criteria) for your network. Click **OK**.

CONFIGURATION > Security Policy > ADP > Profile > Base Profile > Traffic Anomaly



General

Name: APF1895

Description:

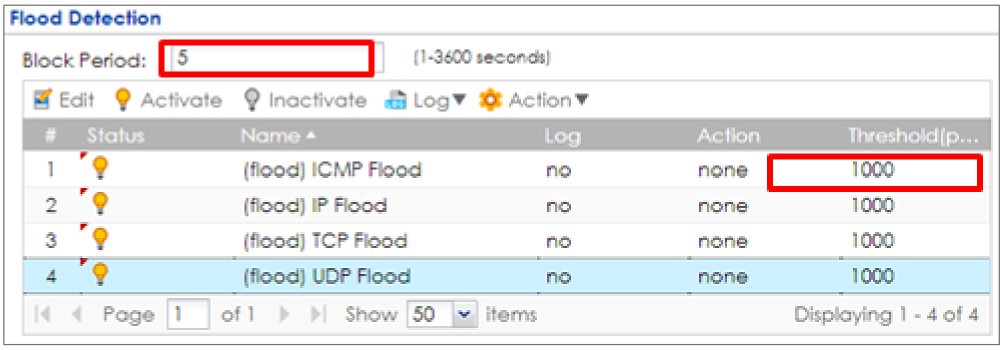
Scan Detection

Sensitivity: medium

Block Period: 10 (1-3600 seconds)

#	Status	Name ▲	Log	Action
1	💡	(portscan) IP Protocol Scan	no	none
2	💡	(portscan) TCP Portscan	no	none
3	💡	(portscan) UDP Portscan	no	none
4	💡	(sweep) ICMP Sweep	no	none
5	💡	(sweep) IP Protocol Sweep	no	none
6	💡	(sweep) TCP Port Sweep	no	none
7	💡	(sweep) UDP Port Sweep	no	none

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



Flood Detection

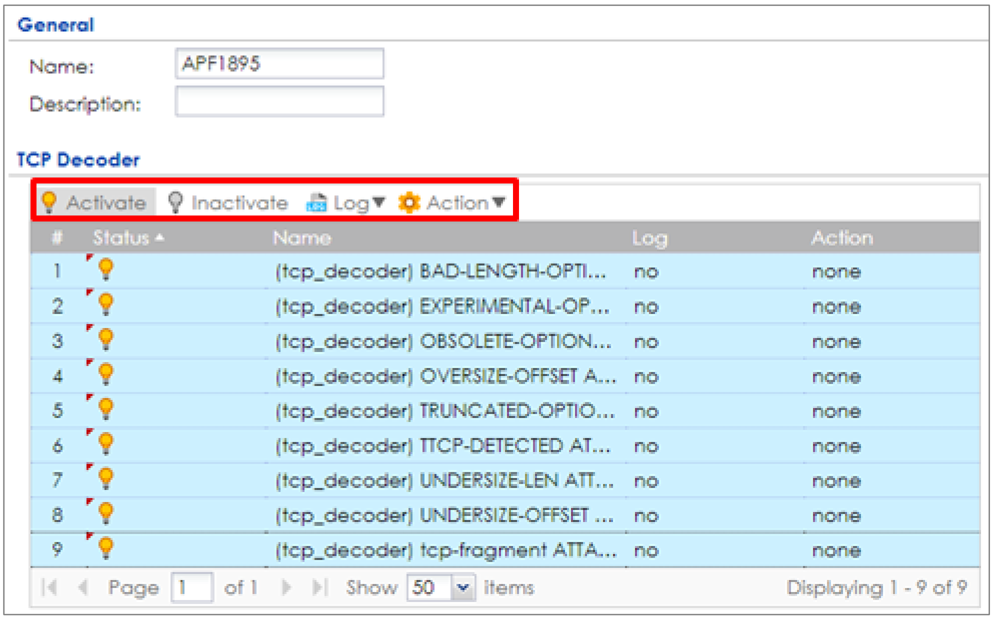
Block Period: 5 (1-3600 seconds)

#	Status	Name ▲	Log	Action	Threshold(p...
1	💡	(flood) ICMP Flood	no	none	1000
2	💡	(flood) IP Flood	no	none	1000
3	💡	(flood) TCP Flood	no	none	1000
4	💡	(flood) UDP Flood	no	none	1000

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

Click the **Protocol Anomaly** tab. A **Name** is automatically generated that you can edit. Enable or disable individual rules by selecting a row and clicking **Activate** or **Inactivate**. Edit the default log options and actions by selecting a row and making a selection in the **Log** or **Action** drop-down menus. Click **OK**.

CONFIGURATION > Security Policy > ADP > Profile > Base Profile > Protocol Anomaly



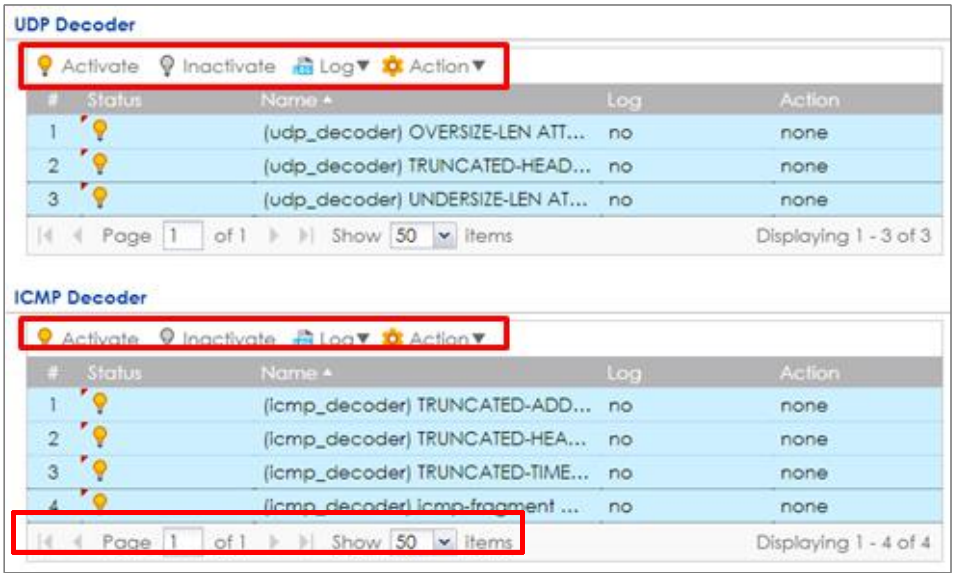
General

Name: APF1895

Description:

TCP Decoder

#	Status ▲	Name	Log	Action
1	💡	(tcp_decoder) BAD-LENGTH-OPTI...	no	none
2	💡	(tcp_decoder) EXPERIMENTAL-OP...	no	none
3	💡	(tcp_decoder) OBSOLETE-OPTION...	no	none
4	💡	(tcp_decoder) OVERSIZE-OFFSET A...	no	none
5	💡	(tcp_decoder) TRUNCATED-OPTIO...	no	none
6	💡	(tcp_decoder) TTCP-DETECTED AT...	no	none
7	💡	(tcp_decoder) UNDERSIZE-LEN ATT...	no	none
8	💡	(tcp_decoder) UNDERSIZE-OFFSET ...	no	none
9	💡	(tcp_decoder) tcp-fragment ATTA...	no	none

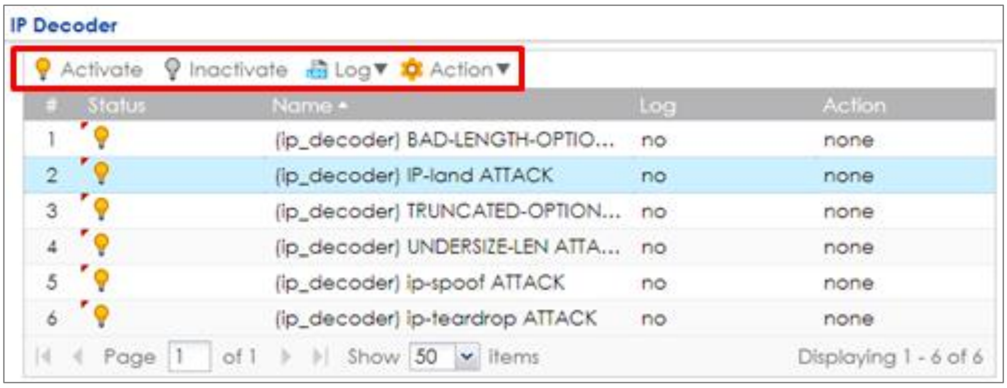


UDP Decoder

#	Status	Name ▲	Log	Action
1	💡	(udp_decoder) OVERSIZE-LEN ATT...	no	none
2	💡	(udp_decoder) TRUNCATED-HEAD...	no	none
3	💡	(udp_decoder) UNDERSIZE-LEN AT...	no	none

ICMP Decoder

#	Status	Name ▲	Log	Action
1	💡	(icmp_decoder) TRUNCATED-ADD...	no	none
2	💡	(icmp_decoder) TRUNCATED-HEA...	no	none
3	💡	(icmp_decoder) TRUNCATED-TIME...	no	none
4	💡	(icmp_decoder) icmp-fragment ...	no	none



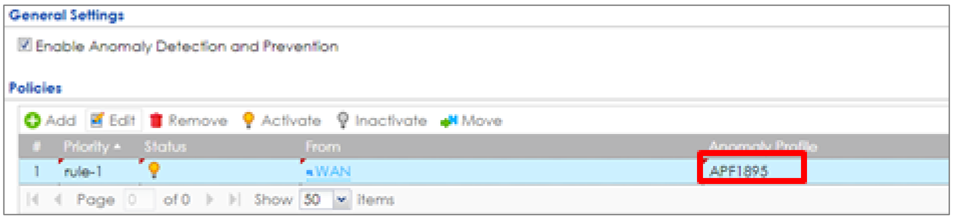
IP Decoder

#	Status	Name ▲	Log	Action
1	💡	(ip_decoder) BAD-LENGTH-OPTIO...	no	none
2	💡	(ip_decoder) IP-land ATTACK	no	none
3	💡	(ip_decoder) TRUNCATED-OPTION...	no	none
4	💡	(ip_decoder) UNDERSIZE-LEN ATTA...	no	none
5	💡	(ip_decoder) ip-spoof ATTACK	no	none
6	💡	(ip_decoder) ip-teardrop ATTACK	no	none

Go to **CONFIGURATION > Security Policy > ADP > General,** select **Enable Anomaly**

Detection and Prevention. Then, select the just created **Anomaly Profile** and click **Apply**.

CONFIGURATION > Security Policy > ADP > General



General Settings

☑ Enable Anomaly Detection and Prevention

Policies

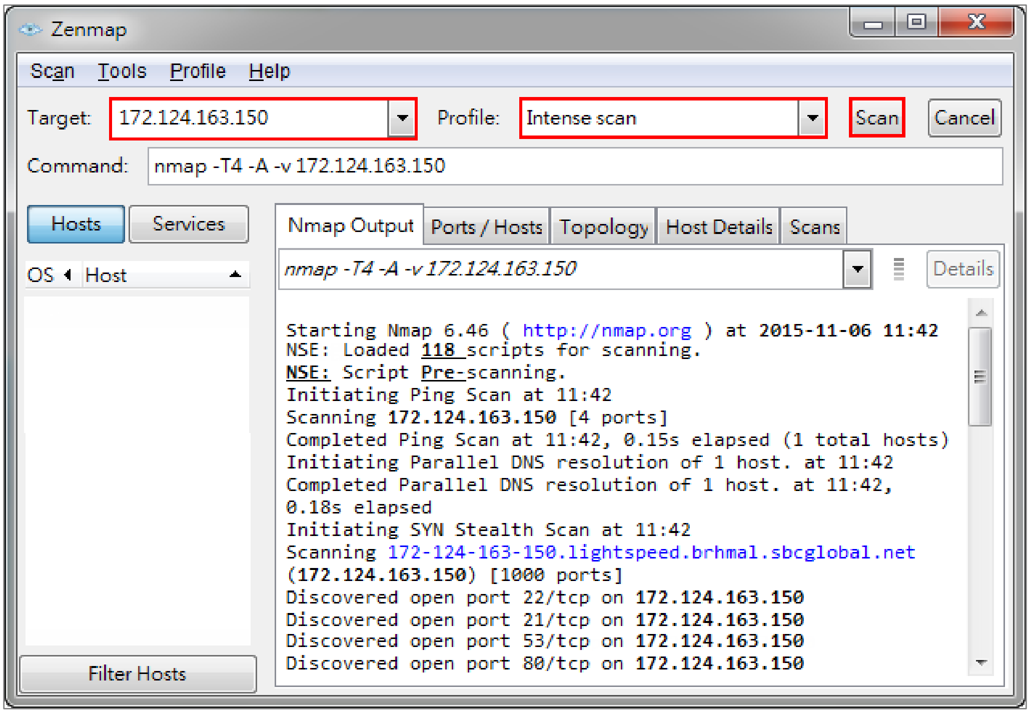
#	Priority	Status	From	Anomaly Profile
1	rule-1	💡	WAN	APF1895

Test the Result

Download Nmap free security scanner for testing the result:

https://nmap.org/download.html

Open the Nmap GUI, set the **Target** to be the WAN IP of ZyWALL/USG (172.124.163.150 in this example) and set **Profile** to be **Intense Scan**. Click **Scan**.



Target: 172.124.163.150

Profile: Intense scan

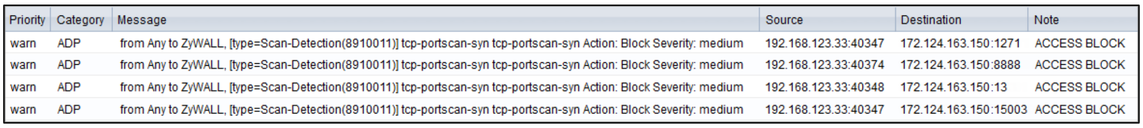
Command: nmap -T4 -A -v 172.124.163.150

nmap -T4 -A -v 172.124.163.150

```
Starting Nmap 6.46 ( http://nmap.org ) at 2015-11-06 11:42
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 11:42
Scanning 172.124.163.150 [4 ports]
Completed Ping Scan at 11:42, 0.15s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:42
Completed Parallel DNS resolution of 1 host. at 11:42,
0.18s elapsed
Initiating SYN Stealth Scan at 11:42
Scanning 172-124-163-150.lightspeed.brhmal.sbcglobal.net
(172.124.163.150) [1000 ports]
Discovered open port 22/tcp on 172.124.163.150
Discovered open port 21/tcp on 172.124.163.150
Discovered open port 53/tcp on 172.124.163.150
Discovered open port 80/tcp on 172.124.163.150
```

Go to the ZyWALL/USG **Monitor > Log**, you will see [warn] log message such as below.

Monitor > Log



Priority	Category	Message	Source	Destination	Note
warn	ADP	from Any to ZyWALL, [type=Scan-Detection(8910011)] tcp-portscan-syn tcp-portscan-syn Action: Block Severity: medium	192.168.123.33:40347	172.124.163.150:1271	ACCESS BLOCK
warn	ADP	from Any to ZyWALL, [type=Scan-Detection(8910011)] tcp-portscan-syn tcp-portscan-syn Action: Block Severity: medium	192.168.123.33:40374	172.124.163.150:8888	ACCESS BLOCK
warn	ADP	from Any to ZyWALL, [type=Scan-Detection(8910011)] tcp-portscan-syn tcp-portscan-syn Action: Block Severity: medium	192.168.123.33:40348	172.124.163.150:13	ACCESS BLOCK
warn	ADP	from Any to ZyWALL, [type=Scan-Detection(8910011)] tcp-portscan-syn tcp-portscan-syn Action: Block Severity: medium	192.168.123.33:40347	172.124.163.150:15003	ACCESS BLOCK

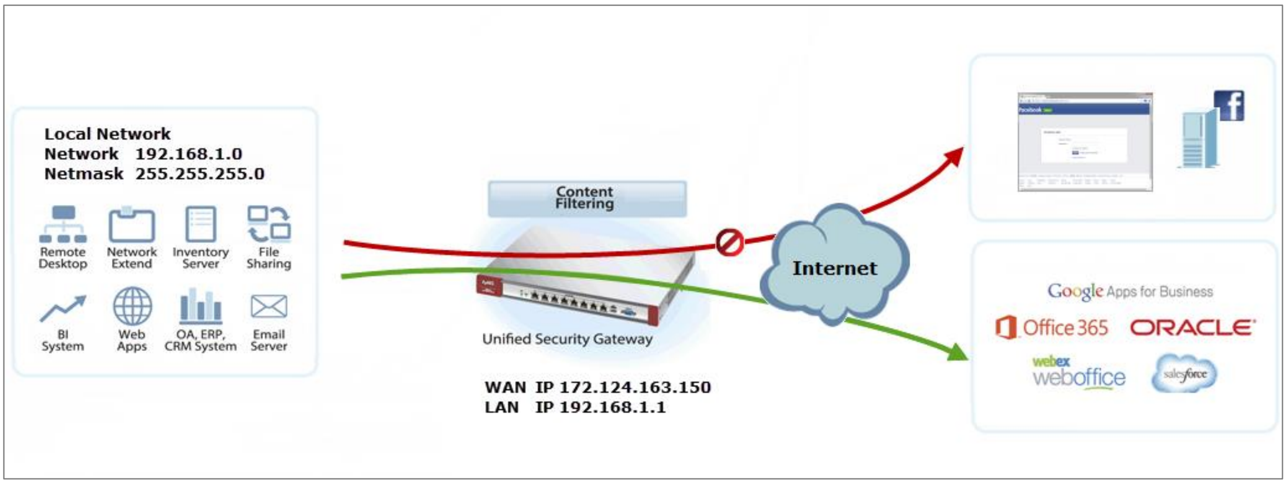
What Could Go Wrong?

You may find that certain rules are triggering too many false positives or false negatives. A false positive is when valid traffic is flagged as an attack. A false negative is when invalid traffic is wrongly allowed to pass through the ZyWALL/USG. As each network is different, false positives and false negatives are common on initial ADP deployment. You could create a new ‘monitor profile’ that creates logs but all actions are disabled. Observe the logs over time and try to eliminate the causes of the false alarms. When you’re satisfied that they have been reduced to an acceptable level, you could then create an ‘inline profile’ whereby you configure appropriate actions to be taken when a packet matches a detection.

How to Block Facebook

This is an example of using a ZyWALL/USG UTM Profile in a Security Policy to block access to a specific social network service. You can use Content Filter, SSL Inspection and Policy Control to make sure that a certain web page cannot be accessed through both HTTP and HTTPS protocols.

ZyWALL/USG with Block Facebook Settings Example

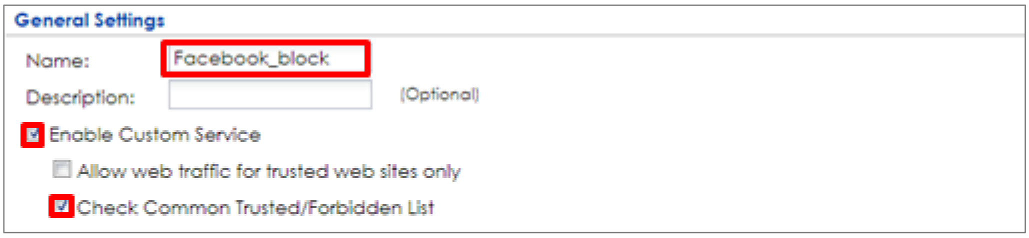


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Content Filter on the ZyWALL/USG

In the ZyWALL/USG, 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 Custom Service.**

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Custom Service > General Settings



General Settings

Name: Facebook_block

Description: (Optional)

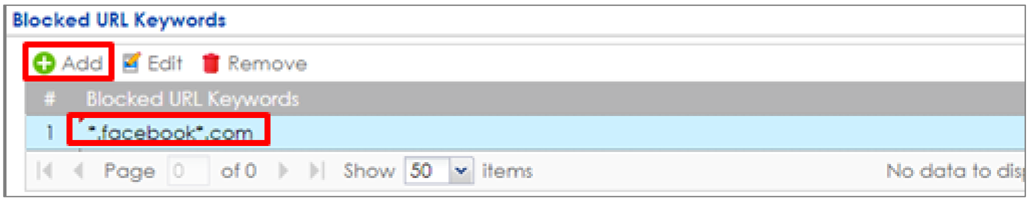
☑ Enable Custom Service

□ Allow web traffic for trusted web sites only

☑ Check Common Trusted/Forbidden List

Scroll down to the **Blocked URL Keywords** section, click **Add** and use "*" as a wildcard to match any string in trusted/forbidden web sites and blocked URL keywords (*.facebook*.com in this example). Click **OK**.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Custom Service > Blocked URL Keywords



Blocked URL Keywords

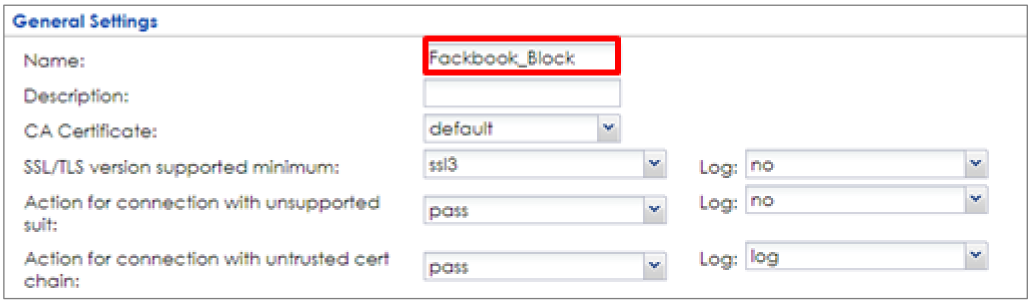
#	Blocked URL Keywords
1	*.facebook*.com

Set Up the SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select **Block** to **Action for Connection with SSL v3** and select **Log** type to be **log alert**. Leave other actions as default settings.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule



General Settings

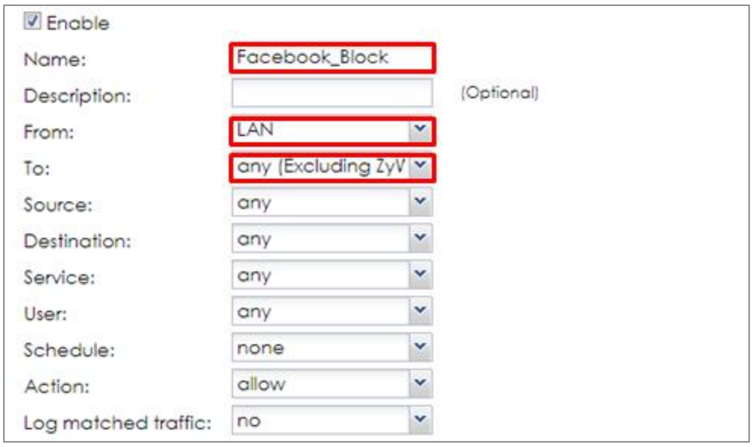
Name:	Fackbook_Block		
Description:			
CA Certificate:	default		
SSL/TLS version supported minimum:	ssl3	Log:	no
Action for connection with unsupported suit:	pass	Log:	no
Action for connection with untrusted cert chain:	pass	Log:	log

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select the **Schedule** that defines when the policy applies (Facebook_Block in this example).

Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Facebook_Block in this example). Then, select **SSL Inspection** and select a profile from the list box (Facebook_Block in this example).

CONFIGURATION > Security Policy > Policy Control



☑ Enable

Name: Facebook_Block

Description: (Optional)

From: LAN

To: any (Excluding ZyV

Source: any

Destination: any

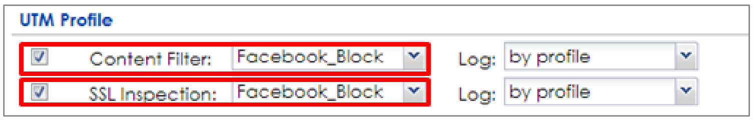
Service: any

User: any

Schedule: none

Action: allow

Log matched traffic: no



UTM Profile

☑ Content Filter: Facebook_Block Log: by profile

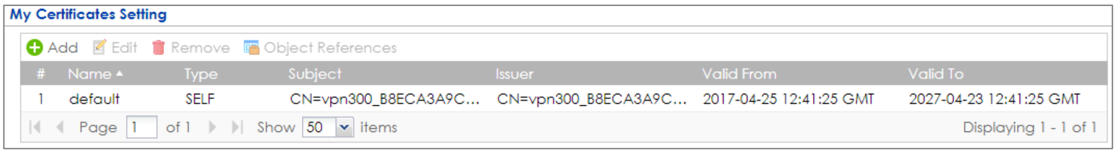
☑ SSL Inspection: Facebook_Block Log: by profile

Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG.

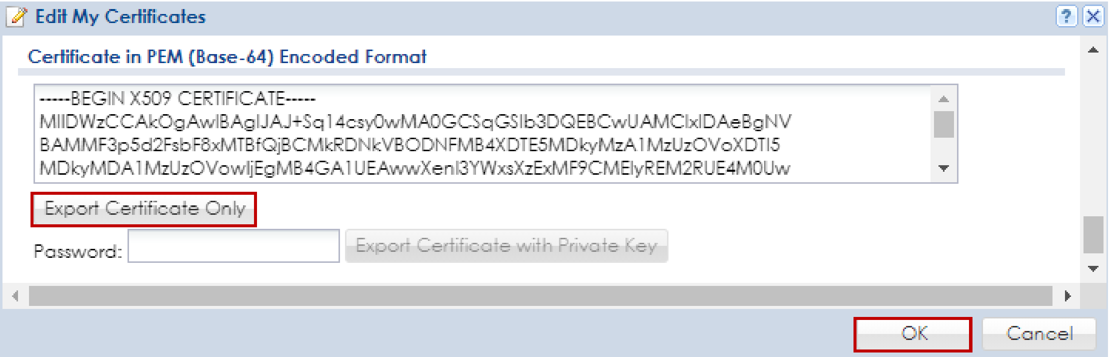
CONFIGURATION > Object > Certificate > default



My Certificates Setting

#	Name ▲	Type	Subject	Issuer	Valid From	Valid To
1	default	SELF	CN=vpn300_B8ECA3A9C...	CN=vpn300_B8ECA3A9C...	2017-04-25 12:41:25 GMT	2027-04-23 12:41:25 GMT

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only



Edit My Certificates

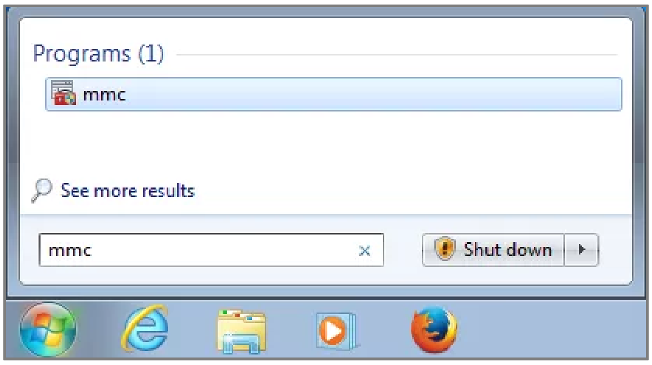
Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN X509 CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIJAJ+Sq14csy0wMA0GCSqGSIb3DQEBCwUAMClxIDAeBgNV
BAMMF3p5d2FsbF8xMTBfQjBCMkRDNkVBODNFMB4XDTE5MDkyMzA1MzUzOVoXDTI5
MDkyMDA1MzUzOVowljEgMB4GA1UEAwwXenl3YWxsXzExMF9CMElyREM2RUE4M0Uw
```

Save default certificate as *.crt file to Windows 7 Operation System.

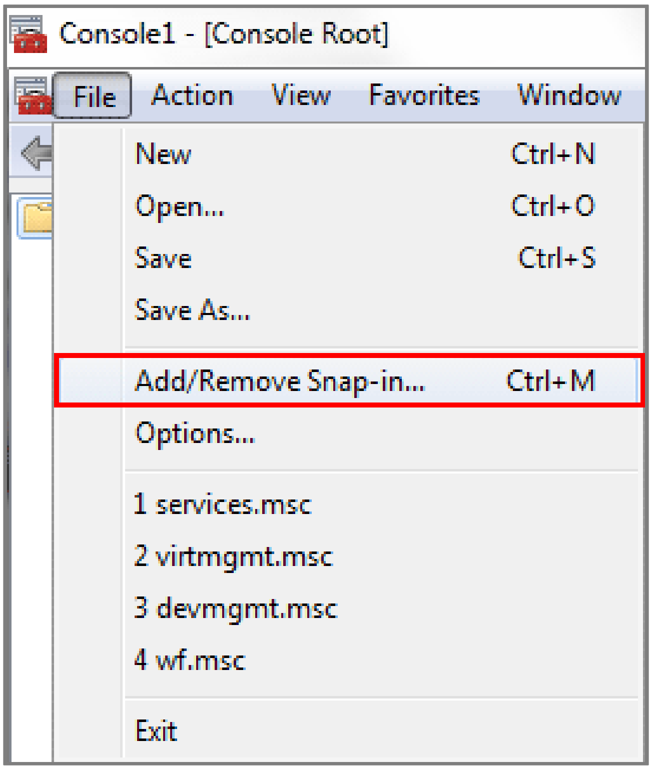
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



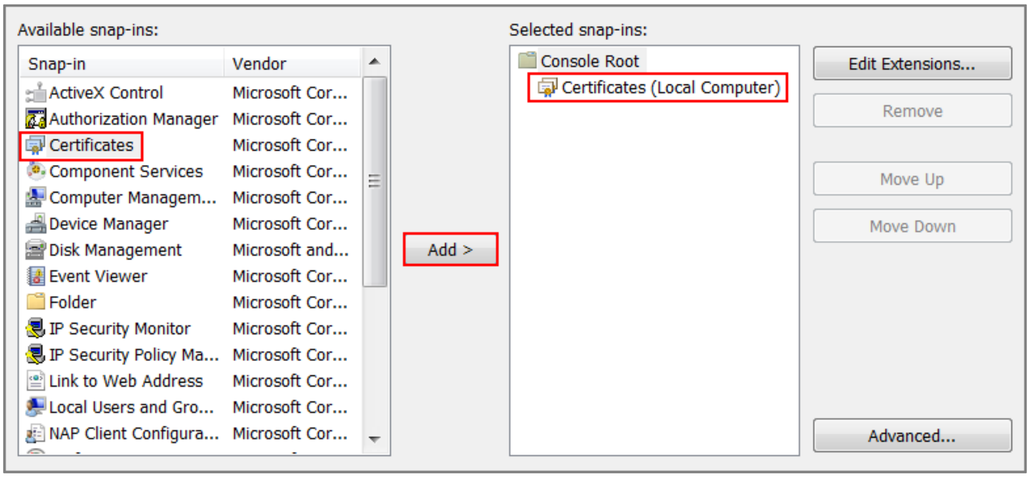
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...



In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

Available snap-ins > Certificates > Add



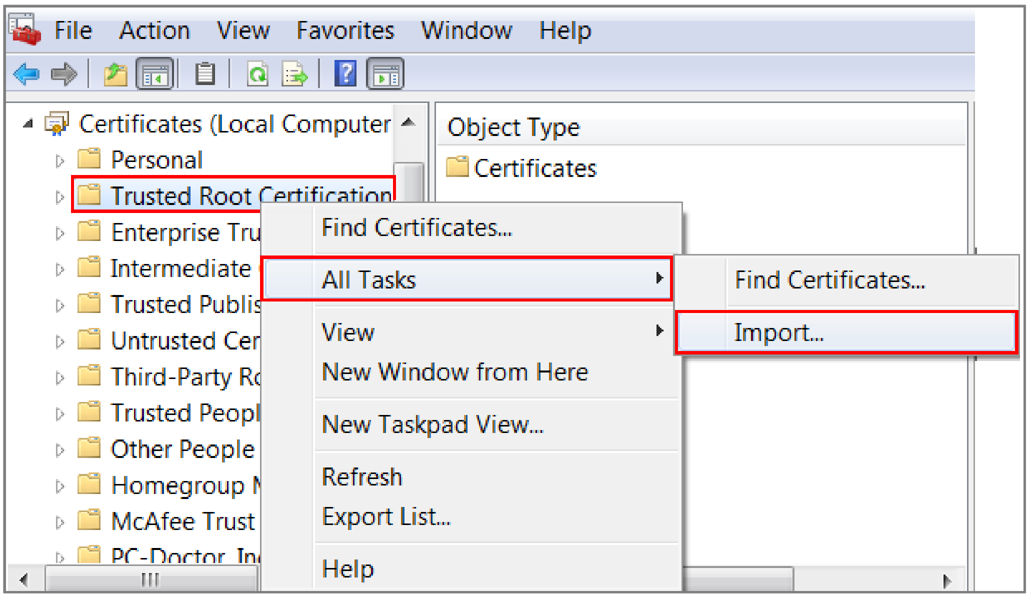
Available snap-ins:

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...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
NAP Client Configura...	Microsoft Cor...

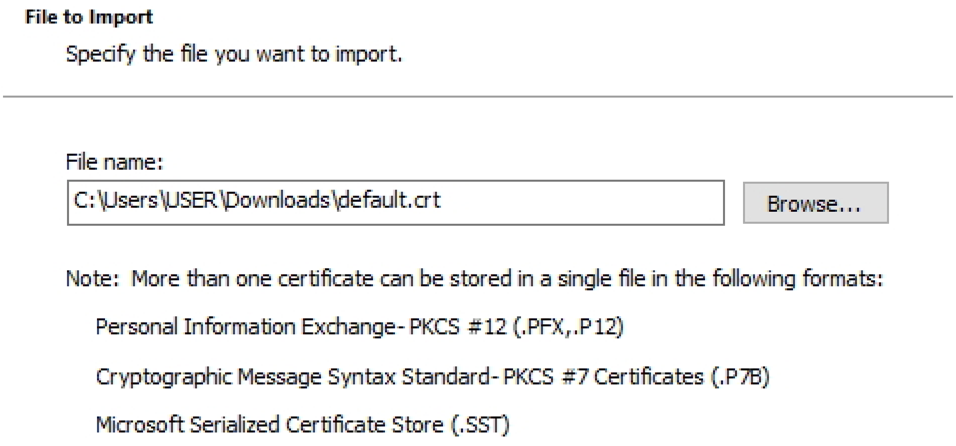
Selected snap-ins:

Console Root
Certificates (Local Computer)

In the mmc console window, open the **Certificates (Local Computer) > Trusted Root Certification Authorities,** right click **Certificate > All Tasks > Import…**



Click **Next**. Then, **Browse...**, and locate the .crt file you downloaded earlier. Then, click **Next**.



File to Import

Specify the file you want to import.

File name:

C:\Users\USER\Downloads\default.crt

Browse...

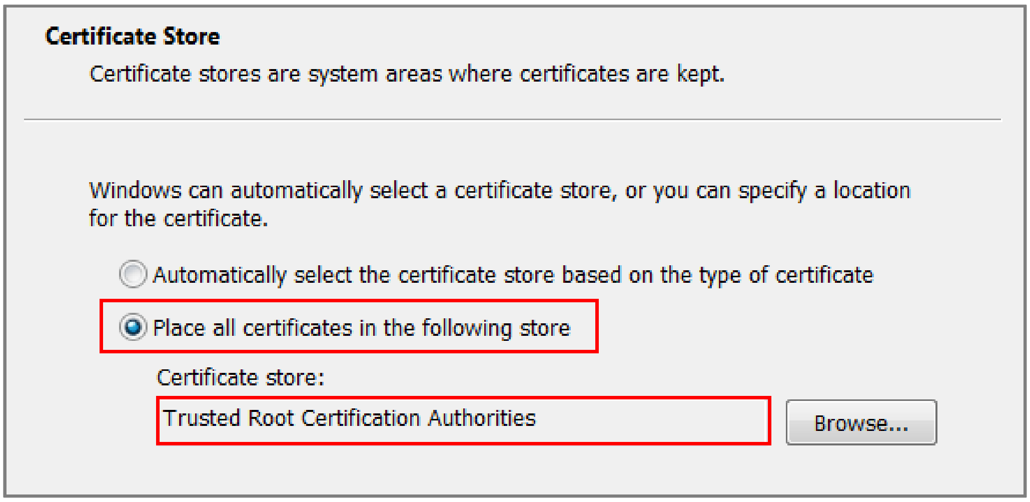
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities.** Click **Next**, then click **Finish**.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

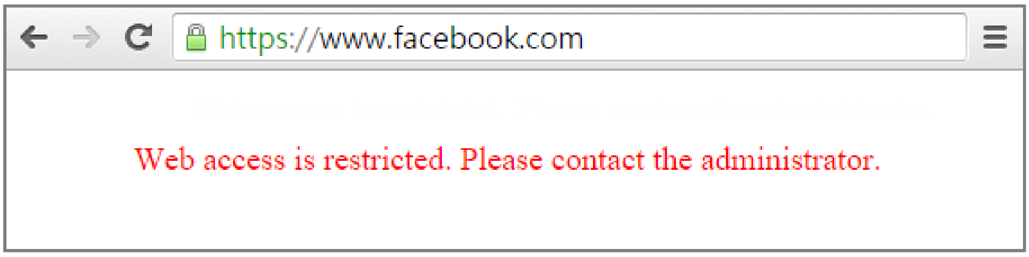
Certificate store:

Trusted Root Certification Authorities

Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Test the Result

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

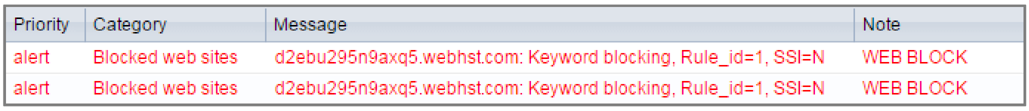


https://www.facebook.com

Web access is restricted. Please contact the administrator.

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

Monitor > Log



Priority	Category	Message	Note
alert	Blocked web sites	d2ebu295n9axq5.webhst.com: Keyword blocking, Rule_id=1, SSI=N	WEB BLOCK
alert	Blocked web sites	d2ebu295n9axq5.webhst.com: Keyword blocking, Rule_id=1, SSI=N	WEB BLOCK

What Could Go Wrong?

If you are not be able to configure any **Content Filter** policies or it's not working, there are two possible reasons:

You have not subscribed for the **Content Filter** service.

You have subscribed for the **Content Filter** service but the license is expired.

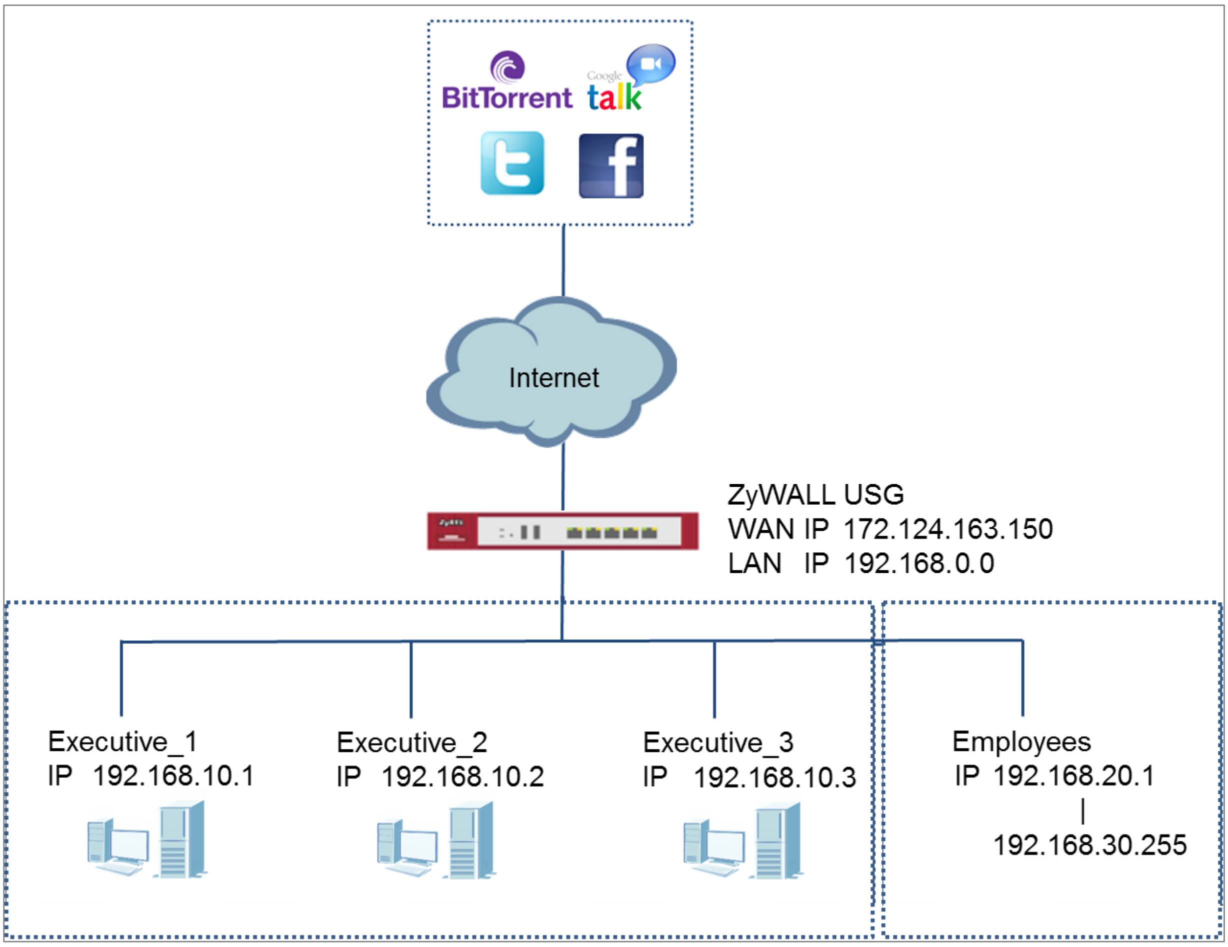
You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **Content Filter** license.

How to Exempt Specific Users from a Blocked Website

This is an example of using a ZyWALL/USG Security Policy to exempt three corporate executives from a blocked Website, while controlling Internet access for other employees' accounts.

With executives connect to a blocked Website using PCs with static IP addresses, you could set up address group to allow their traffic.

ZyWALL/USG with Exempt Specific Users From a Blocked Website Example

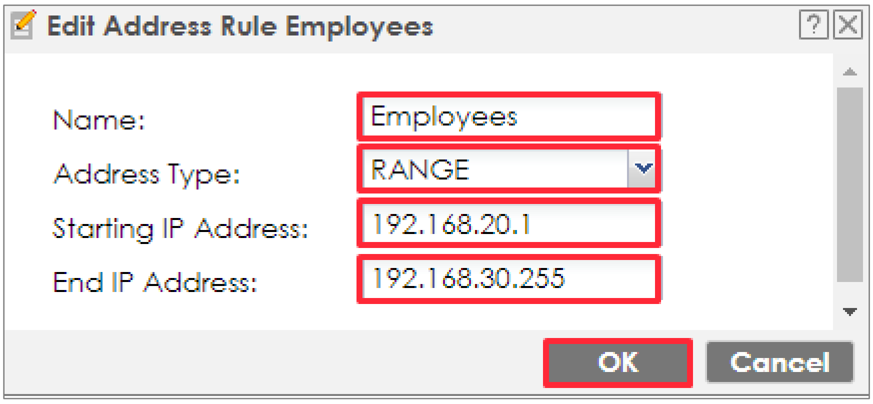


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Security Policy on the ZyWALL/USG for Employees

In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create address range for employees.

CONFIGURATION > Object > Address > Add Address Rule



Edit Address Rule Employees

Name: Employees

Address Type: RANGE

Starting IP Address: 192.168.20.1

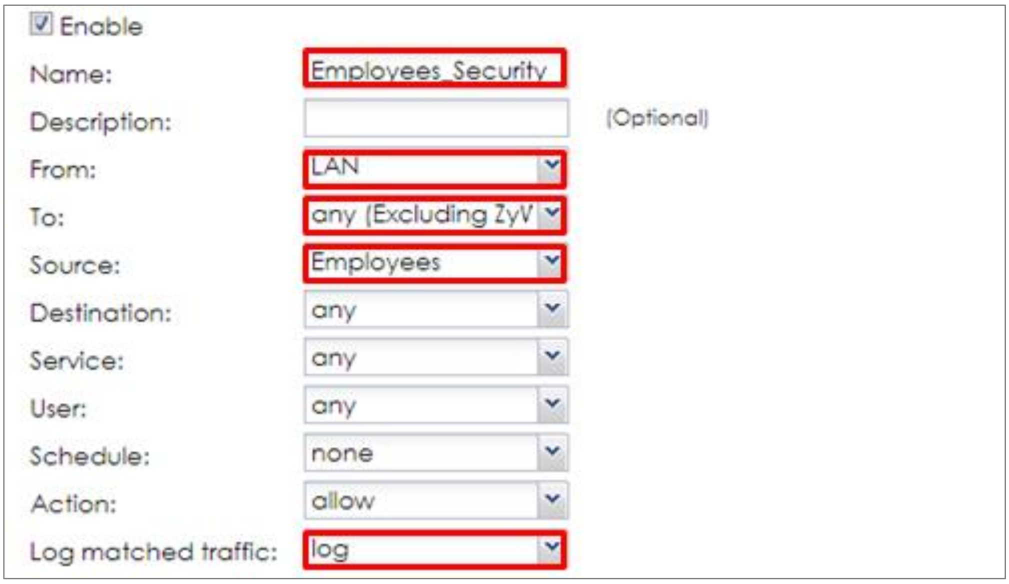
End IP Address: 192.168.30.255

Set up **Security Policy** for employees, go to **CONFIGURATION > Security Policy > Policy Control > Add corresponding**, configure a **Name** for you to identify the employees' **Security Policy** profile.

For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select **Source** to be the **Employees** to apply the policy to all traffic coming from them.

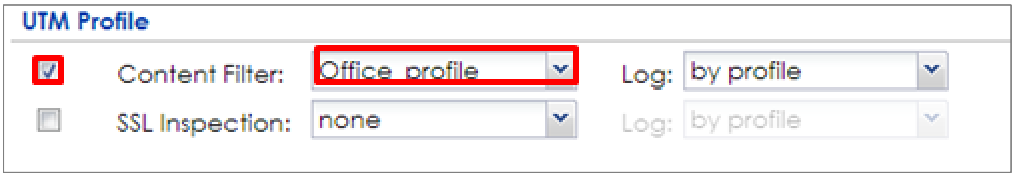
Scroll down to **UTM Profile**, select the general policy that allows employees to access the Internet. (Using built-in Office profile in this example blocks the non-productive services, such as Advertisement & Pop-Ups, Gambling and Peer to Peer services…etc.).

CONFIGURATION > Security Policy > Policy Control > Add corresponding > Employees_Security



☑ Enable

Name:	Employees_Security	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyV	
Source:	Employees	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	log	



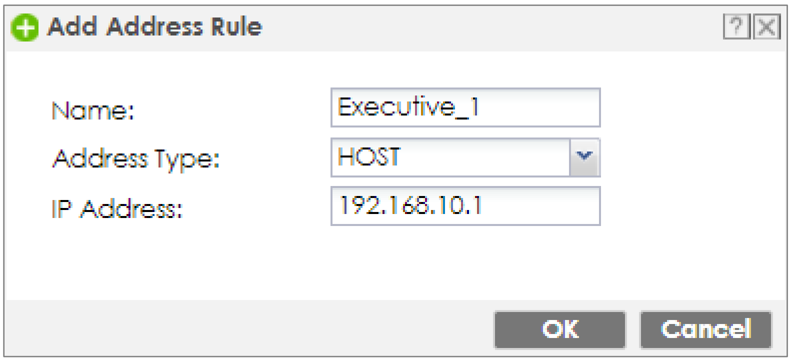
UTM Profile

☑	Content Filter:	Office_profile	Log:	by profile
□	SSL Inspection:	none	Log:	by profile

Set Up the Security Policy on the ZyWALL/USG for Executives

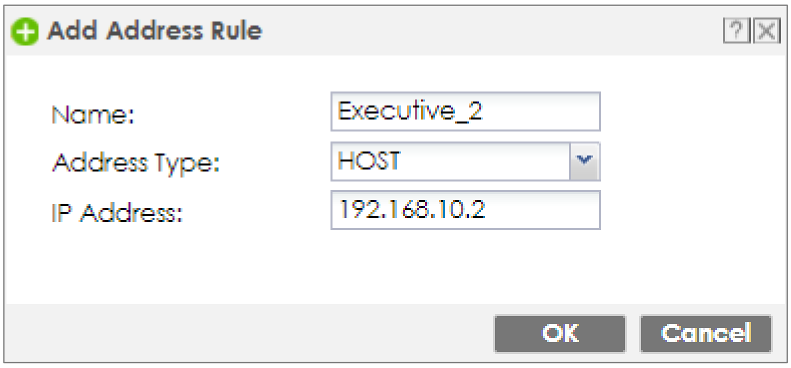
In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create address for each executives.

CONFIGURATION > Object > Address > Add Address Rule



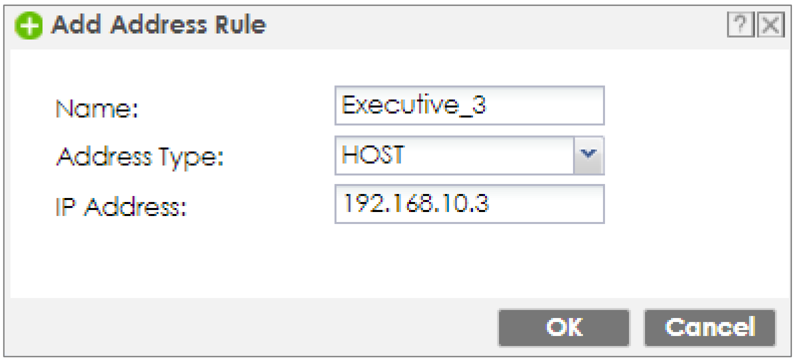
Add Address Rule

Name:	Executive_1
Address Type:	HOST
IP Address:	192.168.10.1



Add Address Rule

Name:	Executive_2
Address Type:	HOST
IP Address:	192.168.10.2

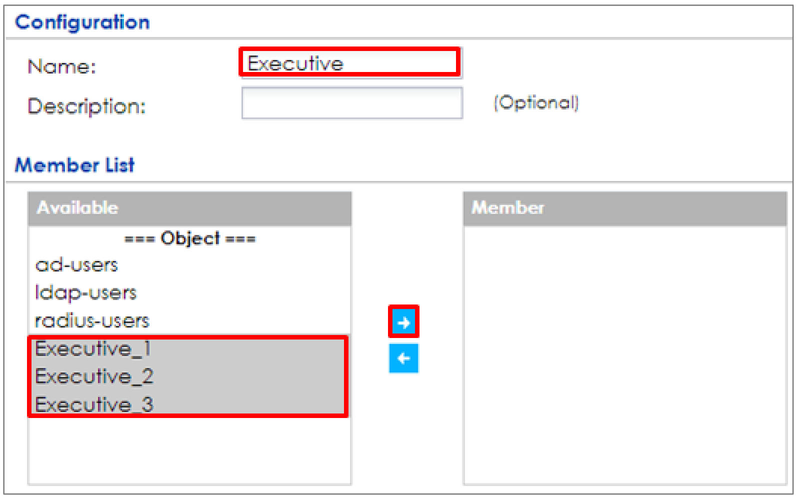


Add Address Rule

Name:	Executive_3
Address Type:	HOST
IP Address:	192.168.10.3

Then, go to **CONFIGURATION > Object > Address Group > Add Address Group Rule** to create a **Group Members' Name** and move the just created executives address object to **Member**.

CONFIGURATION > Object > Address Group > Add Address Group Rule



Configuration

Name: Executive

Description: (Optional)

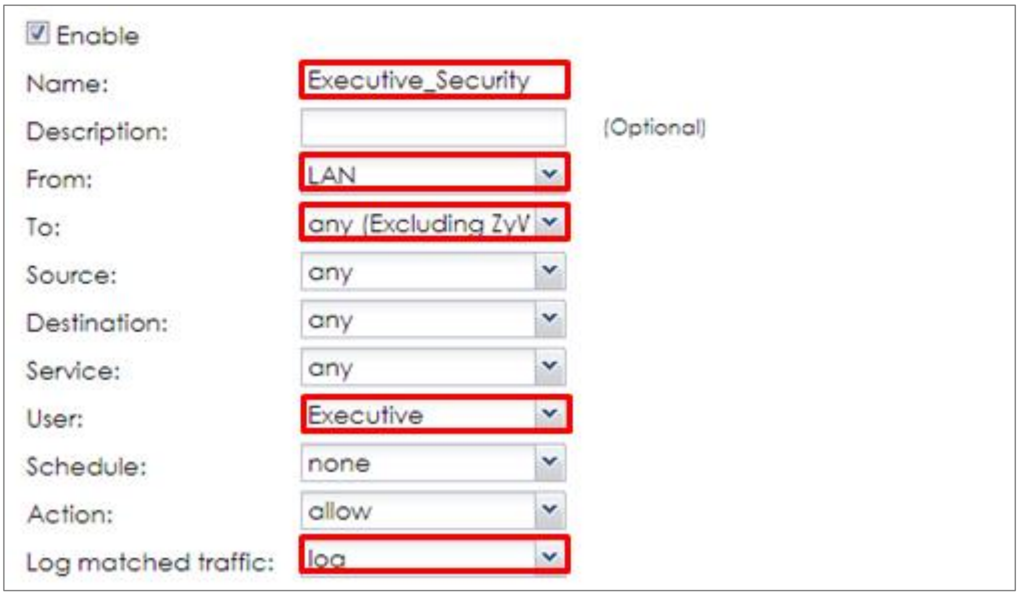
Member List

Set up **Security Policy** for executives, go to **CONFIGURATION > Security Policy > Policy Control > Add corresponding**, configure a **Name** for you to identify the executives' **Security Policy** profile.

For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select **Source** to be the **Executives** to apply the policy to all traffic coming from them. In order to view the results later, to have the ZyWALL/USG generate **Log matched traffic** (**log**).

Leave all UTM Profiles disabled.

CONFIGURATION > Security Policy > Policy Control > Add corresponding > Executives_Security



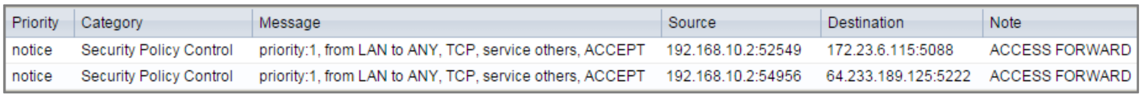
☑ Enable

Name:	Executive_Security	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyV	
Source:	any	
Destination:	any	
Service:	any	
User:	Executive	
Schedule:	none	
Action:	allow	
Log matched traffic:	log	

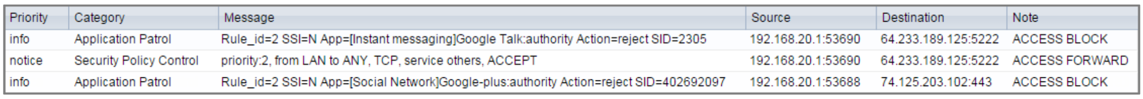
Test the Result

Connect to the Internet from two computers: one from executive_2 address (192.168.10.2) and one from an employee address (192.168.20.1) and both access to https://hangouts.google.com/.

Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] and [info] log message such as below. In this example result, connections from executive_2 address (192.168.10.2) use **Security Policy** priority: 1. Connections from employee address (192.168.20.1) use **Security Policy** priority: 2 and **UTM Profile** Rule_id=2.



Priority	Category	Message	Source	Destination	Note
notice	Security Policy Control	priority:1, from LAN to ANY, TCP, service others, ACCEPT	192.168.10.2:52549	172.23.6.115:5088	ACCESS FORWARD
notice	Security Policy Control	priority:1, from LAN to ANY, TCP, service others, ACCEPT	192.168.10.2:54956	64.233.189.125:5222	ACCESS FORWARD



Priority	Category	Message	Source	Destination	Note
info	Application Patrol	Rule_id=2 SSI=N App=[Instant messaging]Google Talk:authority Action=reject SID=2305	192.168.20.1:53690	64.233.189.125:5222	ACCESS BLOCK
notice	Security Policy Control	priority:2, from LAN to ANY, TCP, service others, ACCEPT	192.168.20.1:53690	64.233.189.125:5222	ACCESS FORWARD
info	Application Patrol	Rule_id=2 SSI=N App=[Social Network]Google-plus:authority Action=reject SID=402692097	192.168.20.1:53688	74.125.203.102:443	ACCESS BLOCK

What Could Go Wrong?

If you are not be able to configure any **UTM** policies or it's not working, there are two possible reasons:

You have not subscribed for the **UTM** service.

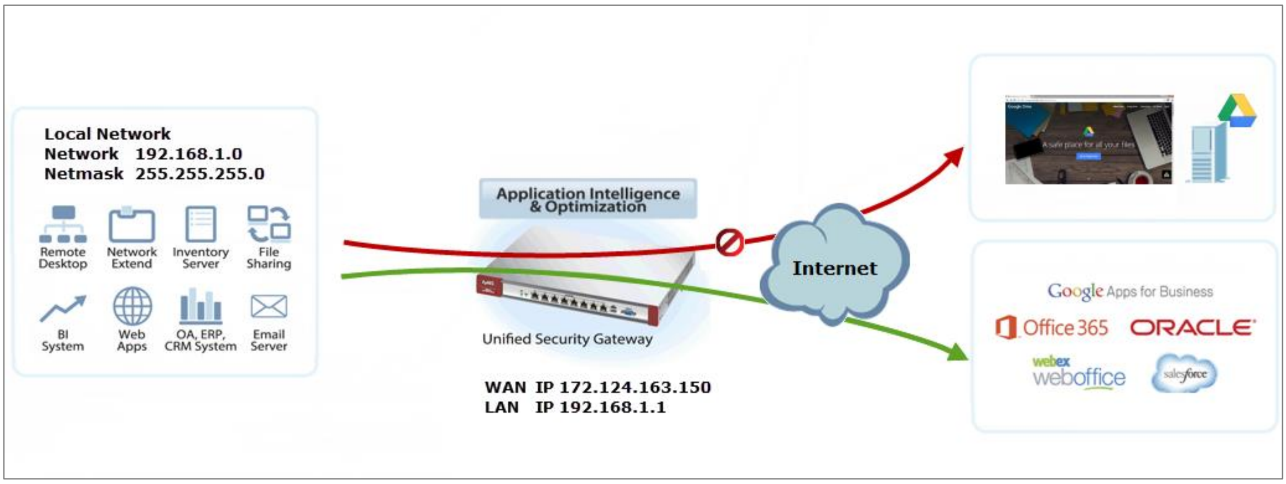
You have subscribed for the **UTM** service but the license is expired.

You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **UTM** license.

How to Control Access To Google Drive

This is an example of using a ZyWALL/USG UTM Profile in a Security Policy to block access to a specific file transfer service. You can use Application Patrol and Policy Control to make sure that a certain file transfer service cannot be accessed through both HTTP and HTTPS protocols.

ZyWALL/USG with Control Access To Google Drive Settings Example



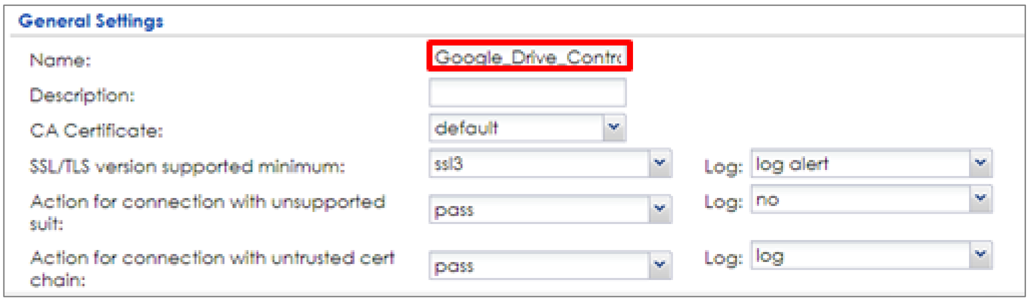
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select **Block** to **Action for Connection with SSL v3** and select **Log** type to be **log alert**. Leave other actions as default settings.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule



General Settings

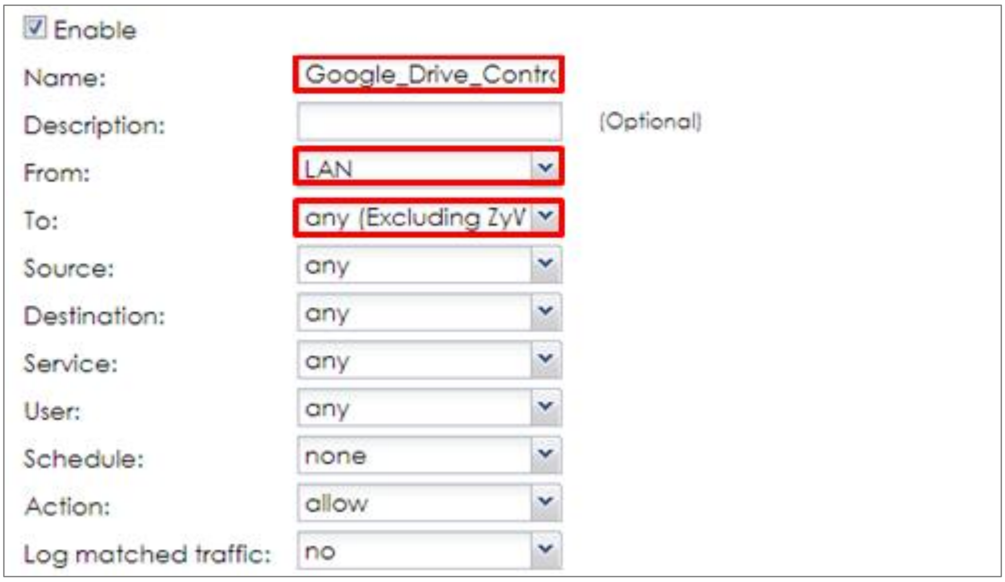
Name:	Google_Drive_Contr(		
Description:			
CA Certificate:	default		
SSL/TLS version supported minimum:	ssl3	Log:	log alert
Action for connection with unsupported suit:	pass	Log:	no
Action for connection with untrusted cert chain:	pass	Log:	log

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies.

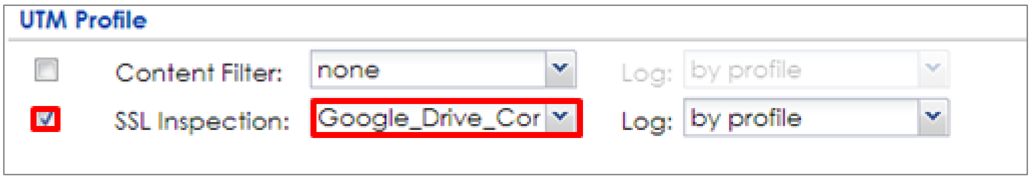
Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Facebook_Block in this example). Then, select **SSL Inspection** and select a profile from the list box (Facebook_Block in this example).

CONFIGURATION > Security Policy > Policy Control



☑ Enable

Name:	Google_Drive_Contr	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyW	
Source:	any	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	no	



UTM Profile

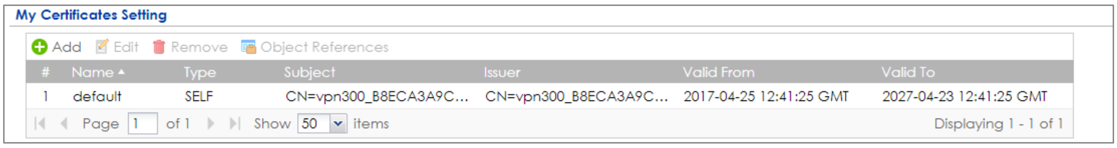
□	Content Filter:	none	Log:	by profile
☑	SSL Inspection:	Google_Drive_Cor	Log:	by profile

Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG.

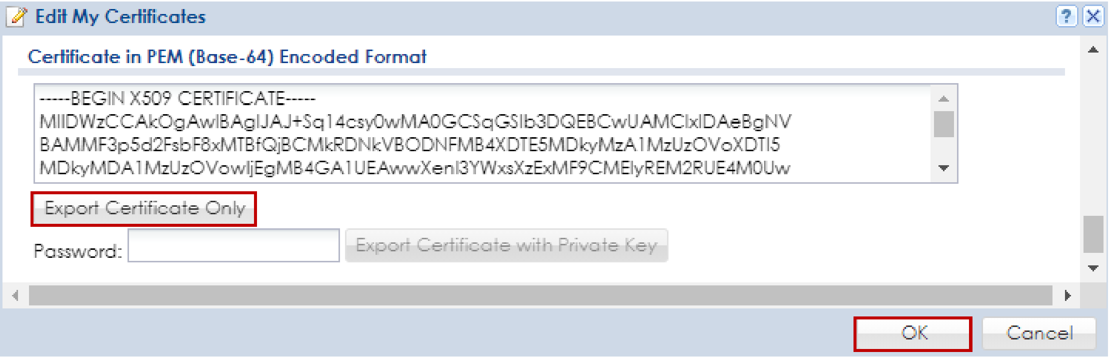
CONFIGURATION > Object > Certificate > default



My Certificates Setting

#	Name ▲	Type	Subject	Issuer	Valid From	Valid To
1	default	SELF	CN=vpn300_B8ECA3A9C...	CN=vpn300_B8ECA3A9C...	2017-04-25 12:41:25 GMT	2027-04-23 12:41:25 GMT

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only



Edit My Certificates

Certificate in PEM (Base-64) Encoded Format

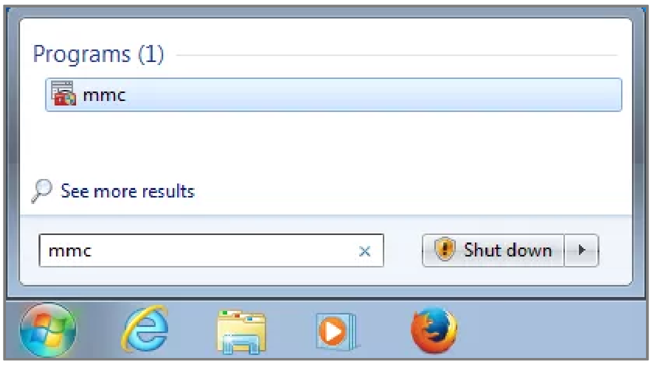
```
-----BEGIN X509 CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIJAJ+Sq14csy0wMA0GCSqGSIb3DQEBCwUAMClxIDAeBgNV
BAMMF3p5d2FsbF8xMTBfQjBCMkRDNkVBODNFMB4XDTE5MDkyMzA1MzUzOVoXDTI5
MDkyMDA1MzUzOVowIjEgMB4GA1UEAwwXenl3YWxsXzExMF9CMElyREM2RUE4M0Uw
```

Save default certificate as *.crt file to Windows 7 Operation System.

default.crt

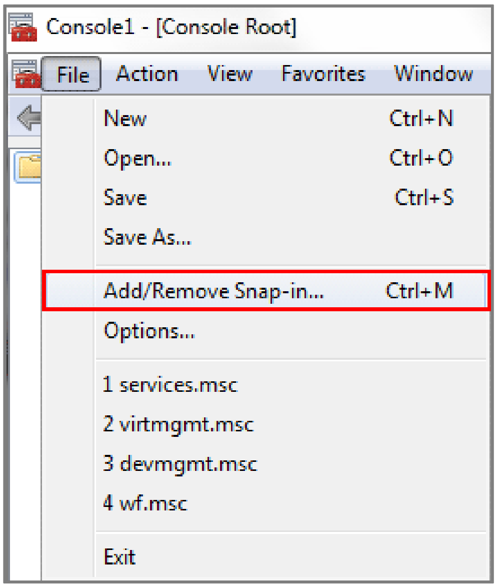
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



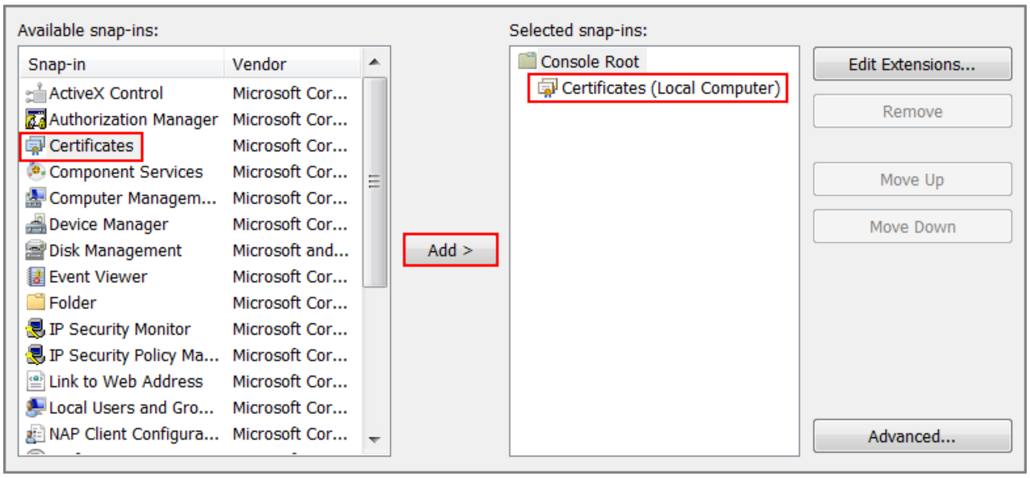
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...



In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

Available snap-ins > Certificates > Add

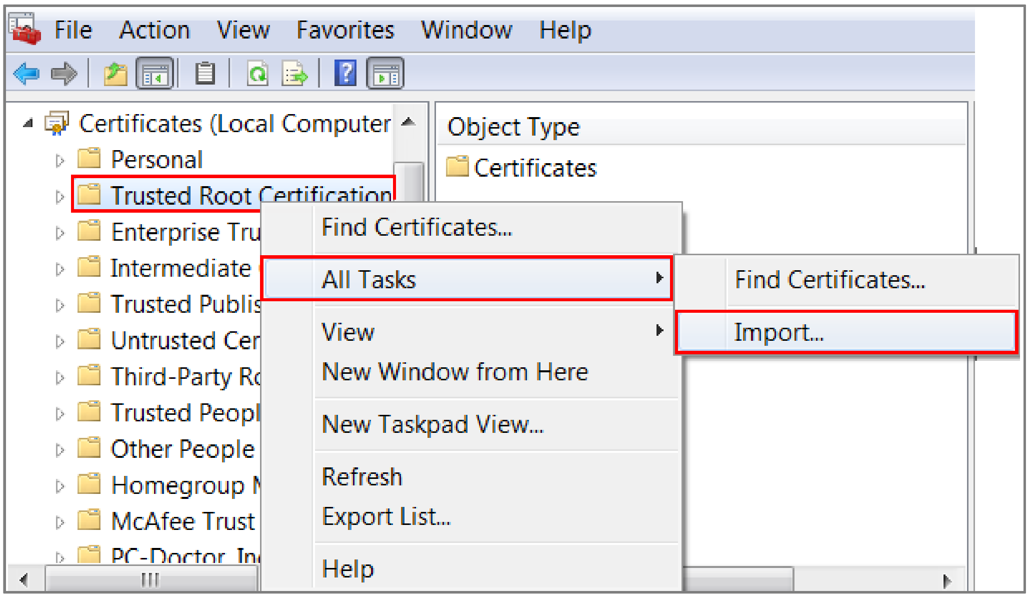

Available snap-ins:

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...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
NAP Client Configura...	Microsoft Cor...

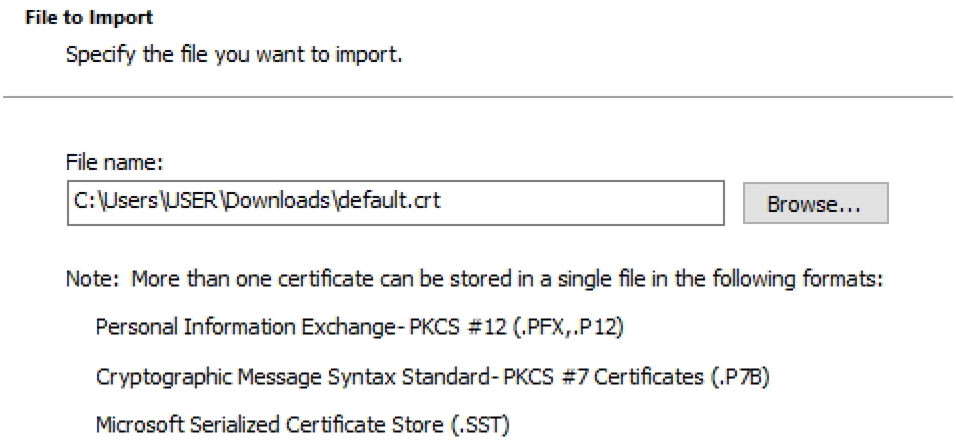
Selected snap-ins:

Console Root
Certificates (Local Computer)

In the mmc console window, open the **Certificates (Local Computer) > Trusted Root Certification Authorities**, right click **Certificate > All Tasks > Import…**



Click **Next**. Then, **Browse…**, and locate the .crt file you downloaded earlier. Then, click **Next**.



File to Import

Specify the file you want to import.

File name:

C:\Users\USER\Downloads\default.crt

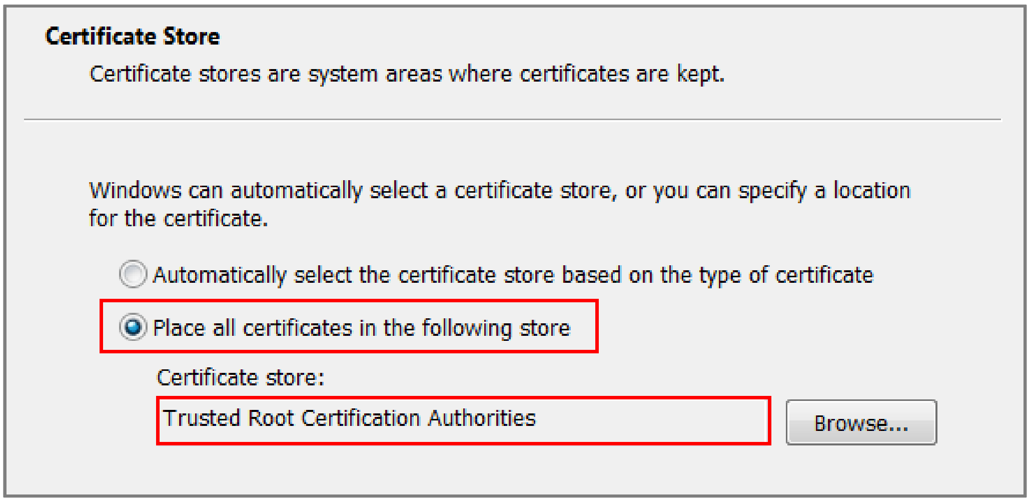
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities.** Click **Next**, then click **Finish**.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

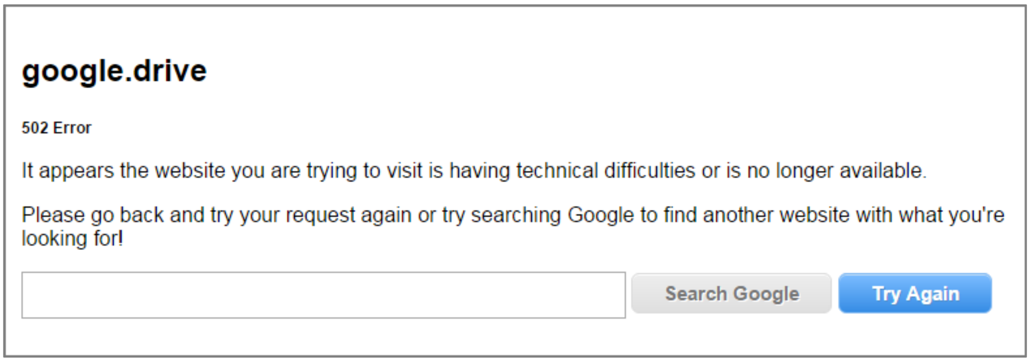
Certificate store:

Trusted Root Certification Authorities

Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Test the Result

Type http://drive.google.com/ or https://drive.google.com/ into the browser, the error message occurs.



google.drive

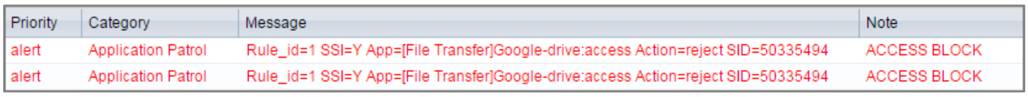
502 Error

It appears the website you are trying to visit is having technical difficulties or is no longer available.

Please go back and try your request again or try searching Google to find another website with what you're looking for!

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

Monitor > Log



Priority	Category	Message	Note
alert	Application Patrol	Rule_id=1 SSI=Y App=[File Transfer]Google-drive:access Action=reject SID=50335494	ACCESS BLOCK
alert	Application Patrol	Rule_id=1 SSI=Y App=[File Transfer]Google-drive:access Action=reject SID=50335494	ACCESS BLOCK

What Could Go Wrong?

If you are not be able to configure any **Application Patrol** policies or it's not working, there are two possible reasons:

You have not subscribed for the **Application Patrol** service.

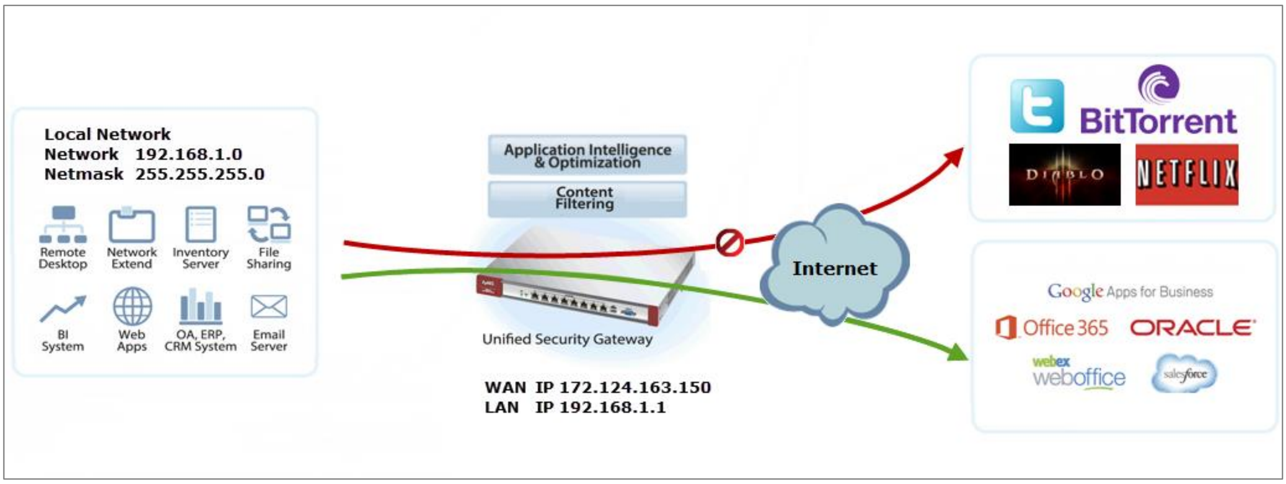
You have subscribed for the **Application Patrol** service but the license is expired.

You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **Application Patrol** license.

How to Block HTTPS Websites Using Content Filtering and SSL Inspection

This is an example of using a ZyWALL/USG Content Filtering, SSL Inspection and Security Policy to block access to malicious or not business-related websites.

ZyWALL/USG with Block HTTPS Websites Using Content Filtering and SSL Inspection Settings Example

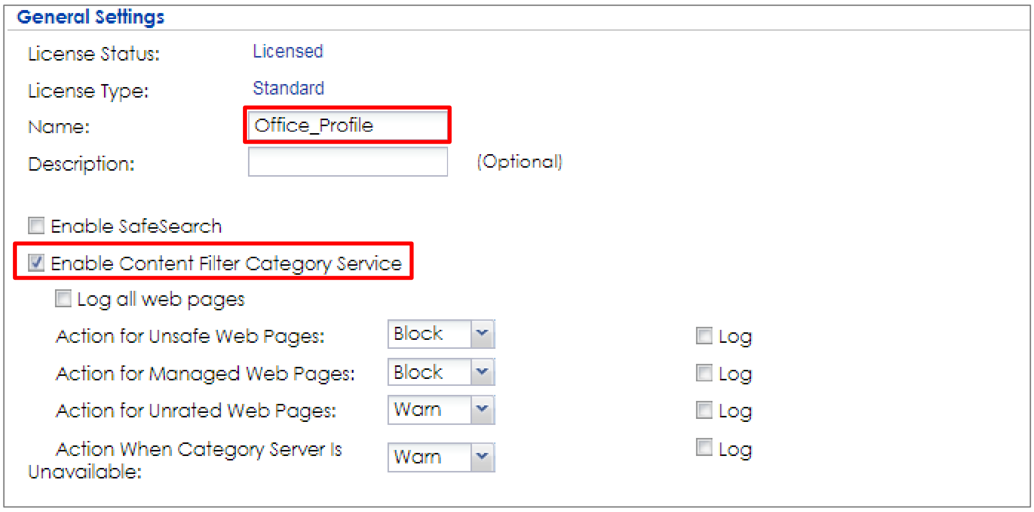


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Content Filter on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile> Content Filter > Profile Management > Add Filter File > Category Service**. Configure a **Name** for you to identify the **Content Filter Profile** and select **Enable Custom Service.**

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add > Category Service > General Settings



General Settings

License Status: Licensed

License Type: Standard

Name: Office_Profile

Description: (Optional)

□ Enable SafeSearch

☑ Enable Content Filter Category Service

□ Log all web pages

Action for Unsafe Web Pages: Block □ Log

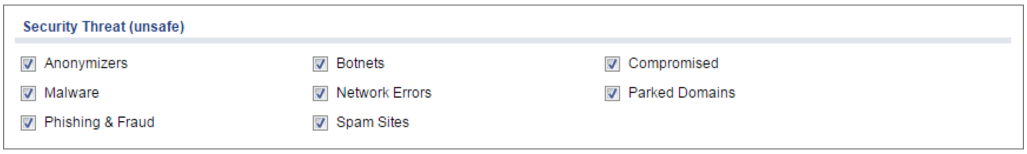
Action for Managed Web Pages: Block □ Log

Action for Unrated Web Pages: Warn □ Log

Action When Category Server Is Unavailable: Warn □ Log

Scroll down to the **Security Threat (unsafe)** section and select all categories of web pages that are known to pose a threat to your computers.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Category **Service > Security Threat (unsafe)**

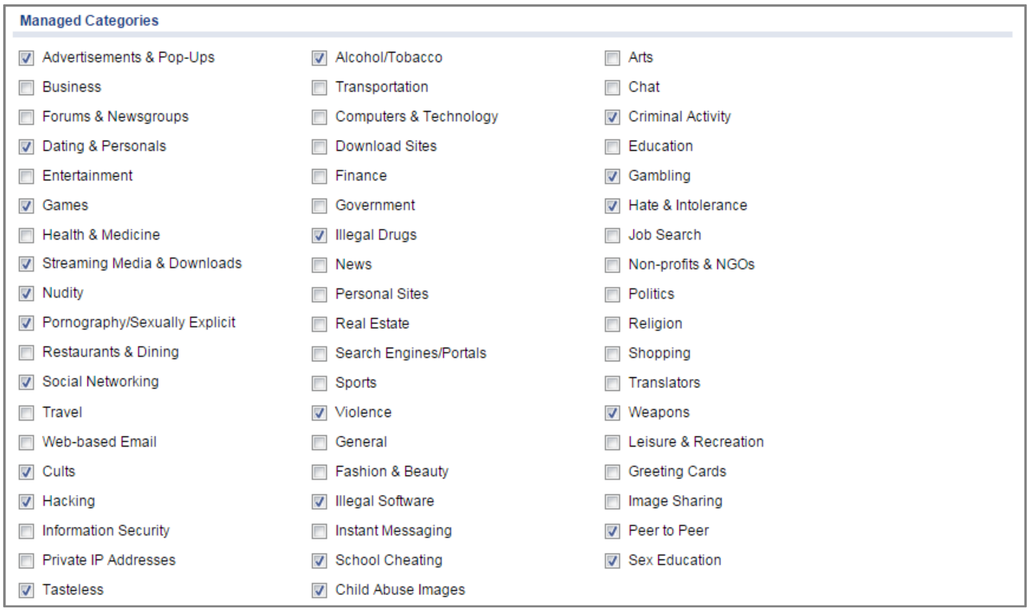


Security Threat (unsafe)

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

Scroll down to the **Managed Categories** section and select the categories that are not business-related. Click **OK**.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Category Service > Managed Categories

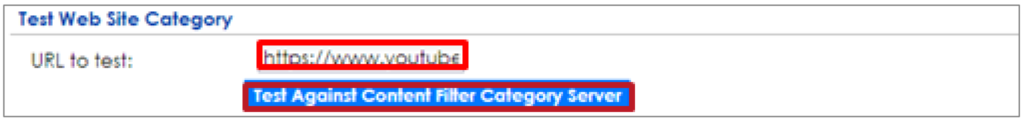


Managed Categories

- ☑ 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

If you are not sure which category a web page belongs to, you can enter a web site URL in the text box of **Test Web Site Category**.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Category Service > Test Web Site Category



Test Web Site Category

URL to test: https://www.youtube

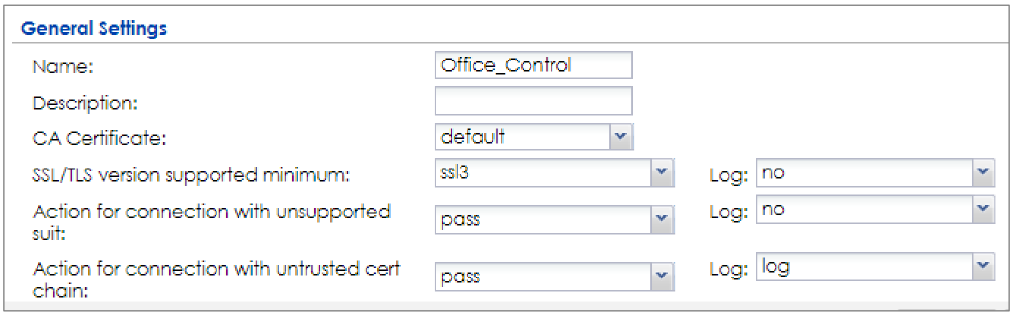
Set Up SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, and configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select to **pass** or **block** SSLv2/unsupported suit/untrusted cert chain traffic that matches traffic bound to this policy here.

Select desired **Log** type whether to have the ZyWALL/USG generate a log (log), log and alert (log alert) or neither (no) by default when traffic matches this policy.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule



General Settings

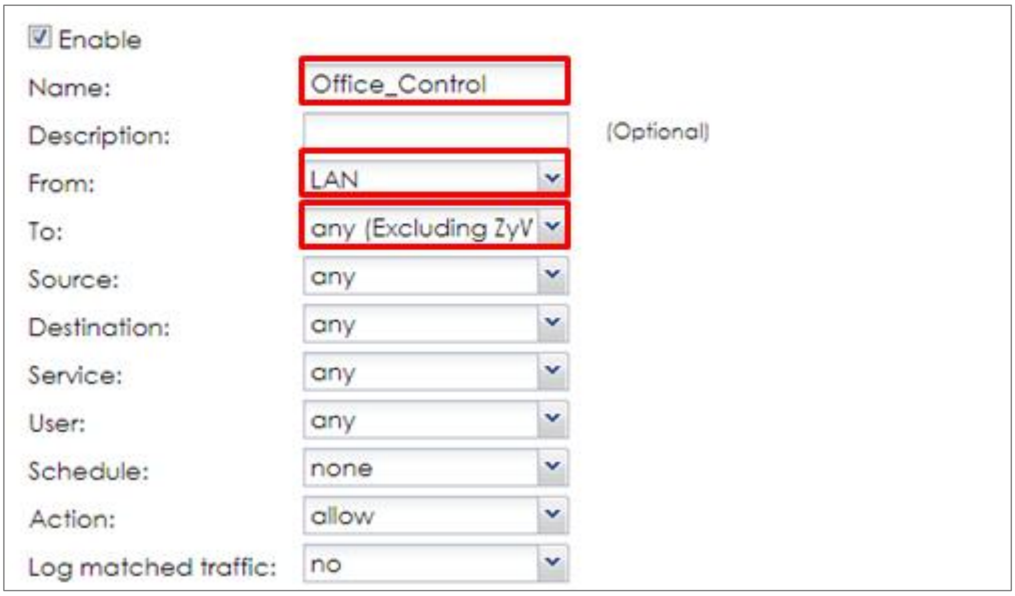
Name:	Office_Control		
Description:			
CA Certificate:	default		
SSL/TLS version supported minimum:	ssl3	Log:	no
Action for connection with unsupported suit:	pass	Log:	no
Action for connection with untrusted cert chain:	pass	Log:	log

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies.

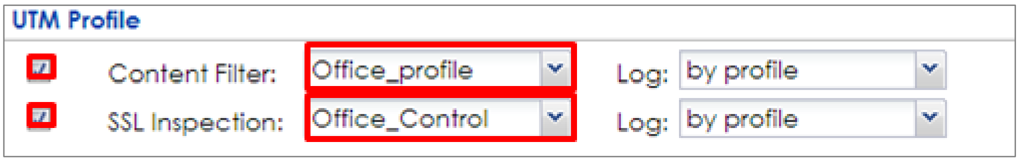
Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Office_profile in this example). Then, select **SSL Inspection** and select a profile from the list box (Office_Control in this example).

CONFIGURATION > Security Policy > Policy Control



☑ Enable

Name:	Office_Control	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyV	
Source:	any	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	no	



UTM Profile

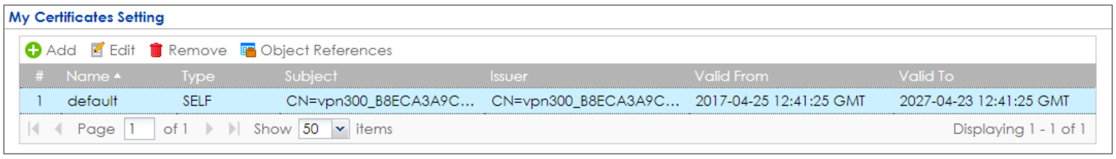
☑	Content Filter:	Office_profile	Log:	by profile
☑	SSL Inspection:	Office_Control	Log:	by profile

Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

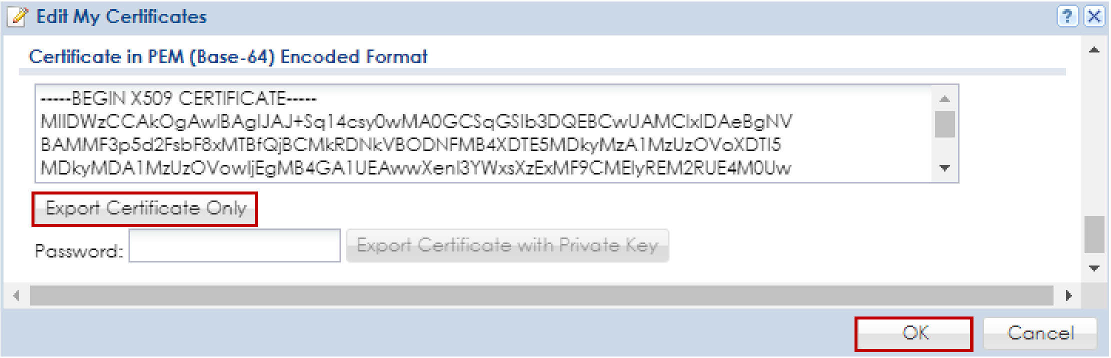
Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG.

CONFIGURATION > Object > Certificate > default


My Certificates Setting

#	Name ▴	Type	Subject	Issuer	Valid From	Valid To
1	default	SELF	CN=vpn300_B8ECA3A9C...	CN=vpn300_B8ECA3A9C...	2017-04-25 12:41:25 GMT	2027-04-23 12:41:25 GMT

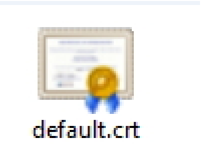
CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only


Edit My Certificates

Certificate in PEM (Base-64) Encoded Format

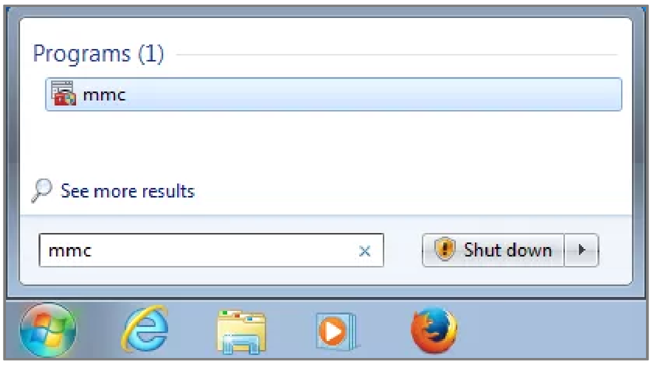
```
-----BEGIN X509 CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIJAJ+Sq14csy0wMA0GCSqGSIb3DQEBCwUAMClxIDAeBgNV
BAMMF3p5d2FsbF8xMTBfQjBCMkRDNkVBODNFMB4XDTE5MDkyMzA1MzUzOVoXDTI5
MDkyMDA1MzUzOVowIjEgMB4GA1UEAwwXenl3YWxsXzExMF9CMElyREM2RUE4M0Uw
```

Save default certificate as *.crt file to Windows 7 Operation System.



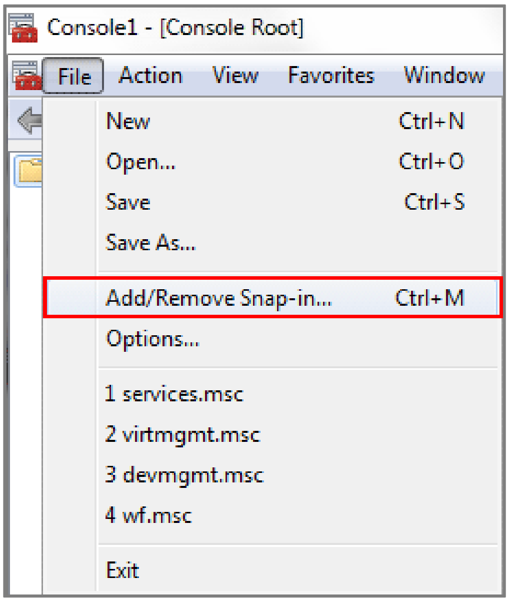
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



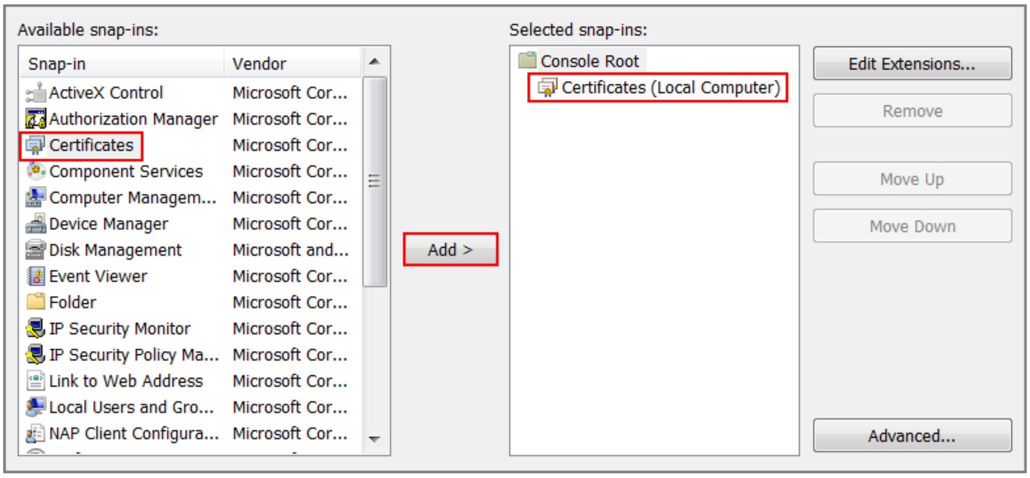
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...



In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

Available snap-ins > Certificates > Add



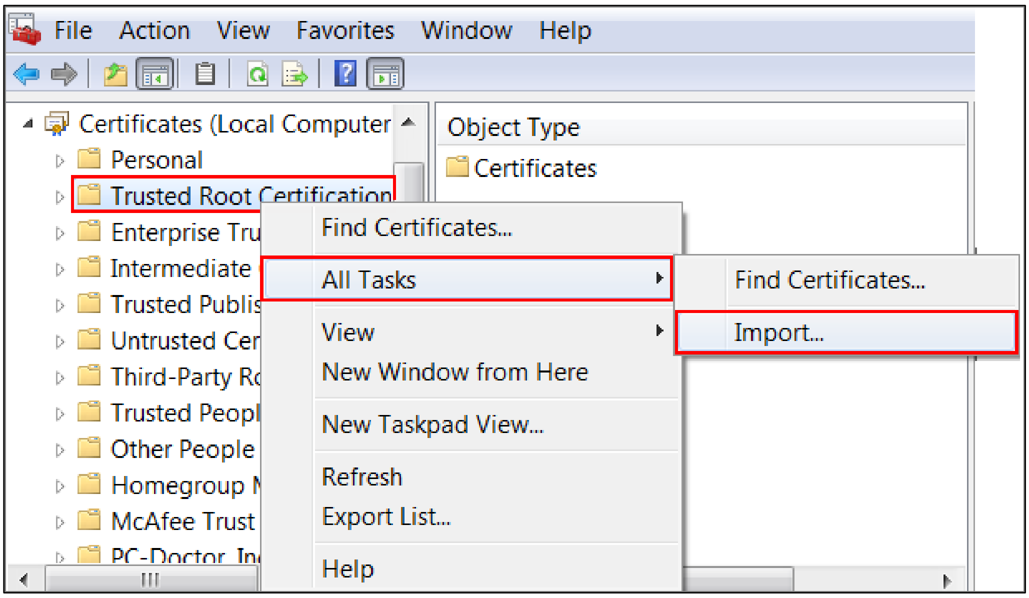
Available snap-ins:

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...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
NAP Client Configura...	Microsoft Cor...

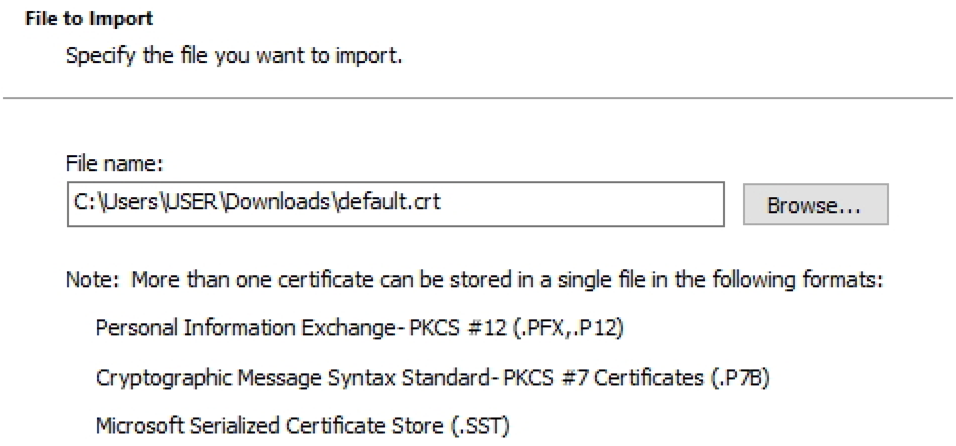
Selected snap-ins:

Console Root
Certificates (Local Computer)

In the mmc console window, open the **Certificates (Local Computer) > Trusted Root Certification Authorities,** right click **Certificate > All Tasks > Import…**



Click **Next**. Then, **Browse...**, and locate the .crt file you downloaded earlier. Then, click **Next**.



File to Import

Specify the file you want to import.

File name:

C:\Users\USER\Downloads\default.crt

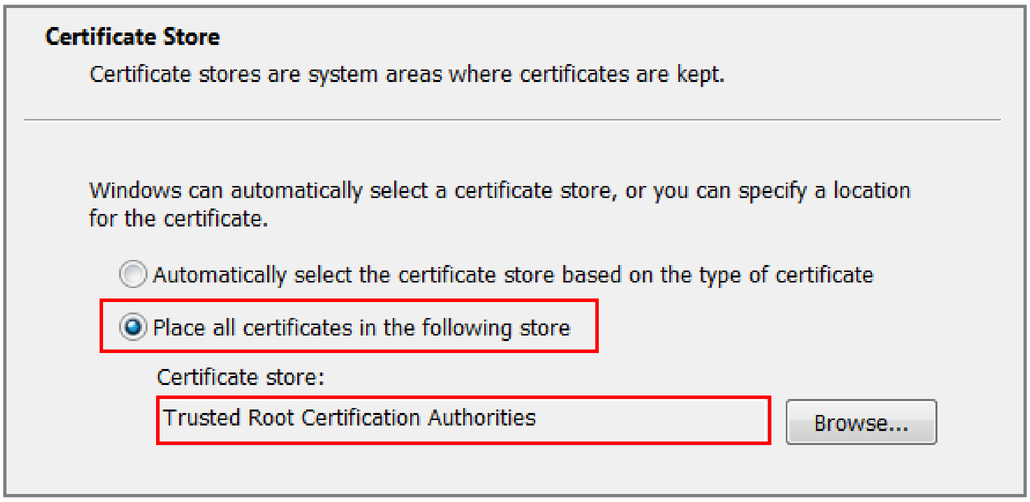
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities.** Click **Next**, then click **Finish**.



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

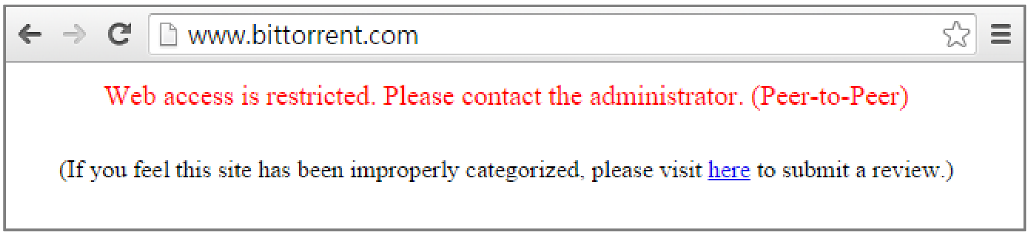
Trusted Root Certification Authorities

Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Test the Result

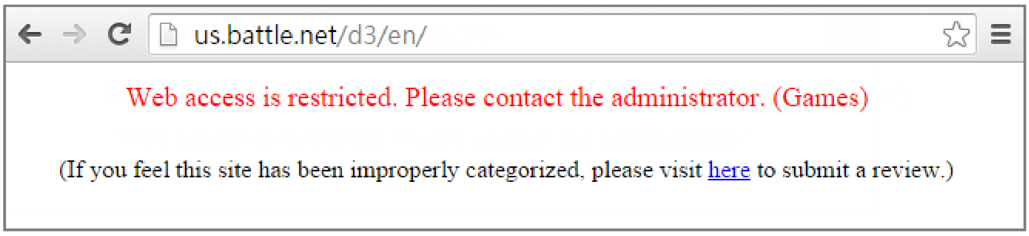
Type http://www.bittorrent.com/ or http://us.battle.net/d3/en/ into the browser.

The error message occurs.



Web access is restricted. Please contact the administrator. (Peer-to-Peer)

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

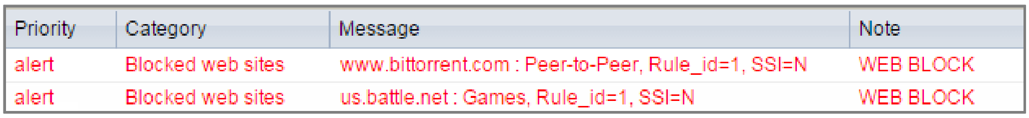


Web access is restricted. Please contact the administrator. (Games)

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

Go to the ZyWALL/USG **Monitor > Log** to see [alert] log message such as below.

Monitor > Log



Priority	Category	Message	Note
alert	Blocked web sites	www.bittorrent.com : Peer-to-Peer, Rule_id=1, SSI=N	WEB BLOCK
alert	Blocked web sites	us.battle.net : Games, Rule_id=1, SSI=N	WEB BLOCK

What Could Go Wrong?

If you are not be able to configure any **Content Filter** policies or it's not working, there are two possible reasons:

You have not subscribed for the **Content Filter** service.

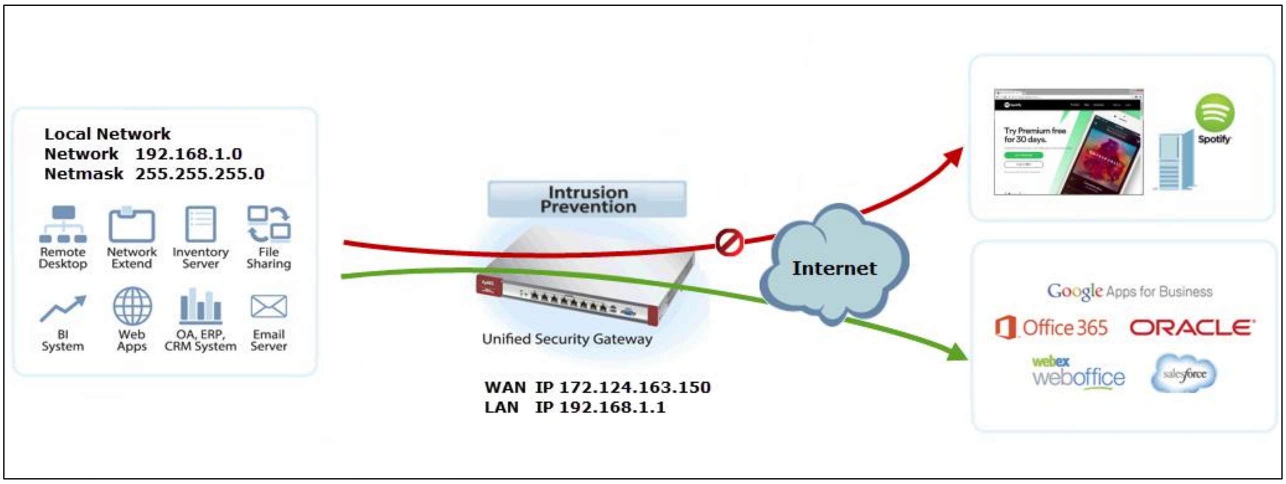
You have subscribed for the **Content Filter** service but the license is expired.

You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **Content Filter** license.

How to Block the Spotify Music Streaming Service

This is an example of using a ZyWALL/USG IDP Profile to block DNS query packet. When the Spotify software launches, it will send a DNS query for Spofity's public server. In this example, you can create a custom IDP to block DNS query packet if this packet includes the Spotify signature.

ZyWALL/USG with Block the Spotify Service Example

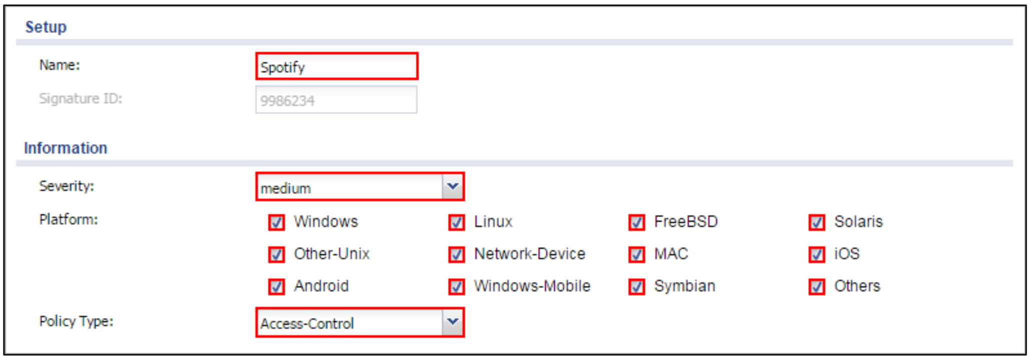


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up IDP Profile on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > IDP > Custom Signatures > Add Custom Signatures,** configure a **Name** for you to identify the **IDP** Profile. Select **medium** as the **Severity** level. Select all **Platform**. Select **Policy Type** to be **Access-Control** here to limit access network resources such as servers.

CONFIGURATION > Security Policy > IDP > Custom Signatures > Add Custom Signatures > Setup & Information



Setup

Name: Spotify

Signature ID: 9986234

Information

Severity: medium

Platform:

☑ Windows ☑ Linux ☑ FreeBSD ☑ Solaris

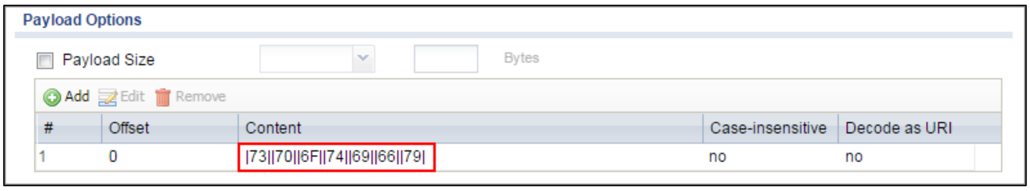
☑ Other-Unix ☑ Network-Device ☑ MAC ☑ iOS

☑ Android ☑ Windows-Mobile ☑ Symbian ☑ Others

Policy Type: Access-Control

Scroll down to the **Payload Options** section, the type Spotify's software signature: |73| |70| |6F| |74| |69| |66| |79|into the **Content** field. Click **OK**.

CONFIGURATION > Security Policy > IDP > Custom Signatures > Add Custom Signatures > Payload Options



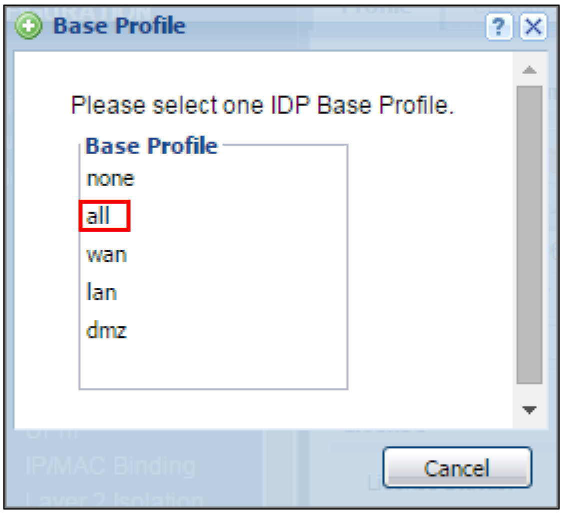
Payload Options

□ Payload Size Bytes

#	Offset	Content	Case-insensitive	Decode as URI
1	0	|73||70||6F||74||69||66||79|	no	no

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > IDP > Profile > Base Profile**. A pop-up screen will appear and select a **Base Profile** to go to the profile details screen.

CONFIGURATION > UTM Profile > IDP > Profile > Base Profile



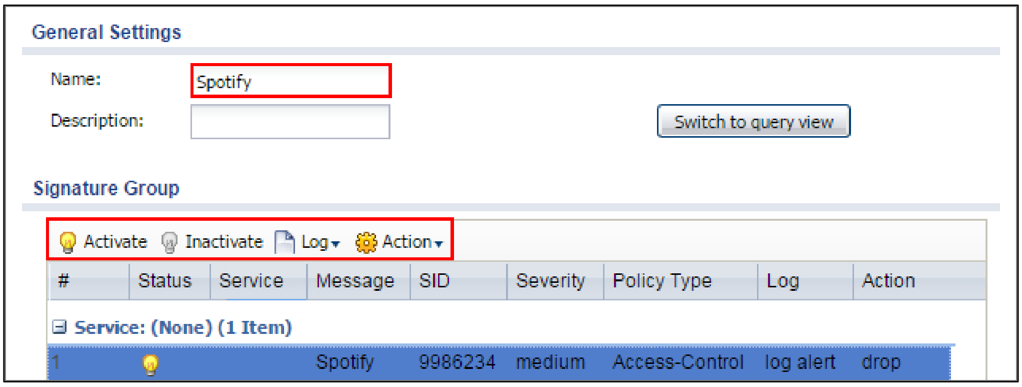
Base Profile

Please select one IDP Base Profile.

Base Profile
- none
- all
- wan
- lan
- dmz

Configure a **Name** for you to identify the **IDP** Profile. **Activate** the newly created IDP Profile and select **Action** to be **drop**. Select **Log** type to be **log alert** in order to view the result later.

CONFIGURATION > UTM Profile > IDP > Profile > Base Profile > Add Profile



General Settings

Name: Spotify

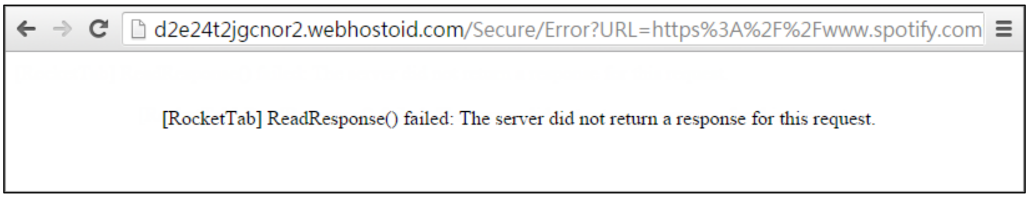
Description:

Signature Group

#	Status	Service	Message	SID	Severity	Policy Type	Log	Action
Service: (None) (1 Item)								
1	💡		Spotify	9986234	medium	Access-Control	log alert	drop

Test the Result

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

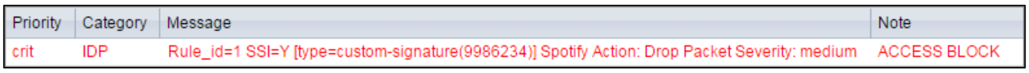


d2e24t2jgcnor2.webhostoid.com/Secure/Error?URL=https%3A%2F%2Fwww.spotify.com

[RocketTab] ReadResponse() failed: The server did not return a response for this request.

Go to the ZyWALL/USG **Monitor > Log**, you will see [crit] log message such as below.

Monitor > Log



Priority	Category	Message	Note
crit	IDP	Rule_id=1 SSI=Y [type=custom-signature(9986234)] Spotify Action: Drop Packet Severity: medium	ACCESS BLOCK

What Could Go Wrong?

If you are not be able to configure any **IDP** policies or it's not working, there are two possible reasons:

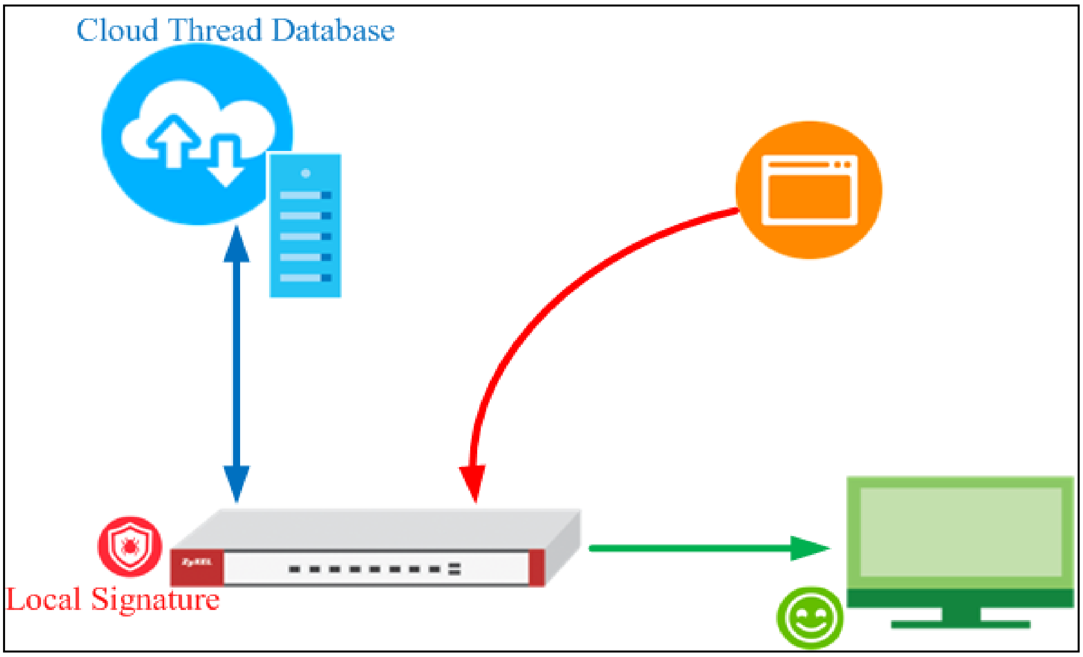
You have not subscribed for the **IDP** service.

You have subscribed for the **IDP** service but the license is expired.

You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **Application Patrol** license.

How does Anti-Malware work

There are many virus exist on the internet. And it may auto-downloaded on unexpected situation when you surfing between websites. The Anti-Malware is a good choose to protecting your computer to downloads unsafe application or files.



After you enabled Anti-Malware function, it will enabled "**Cloud Threat Database**" and "**Anti-Malware Signature**" in the same time.

The **Cloud Threat Database** is means your downloaded files will decompressed by device first, and then check files with cloud data base server if it exist unsafe file or not.

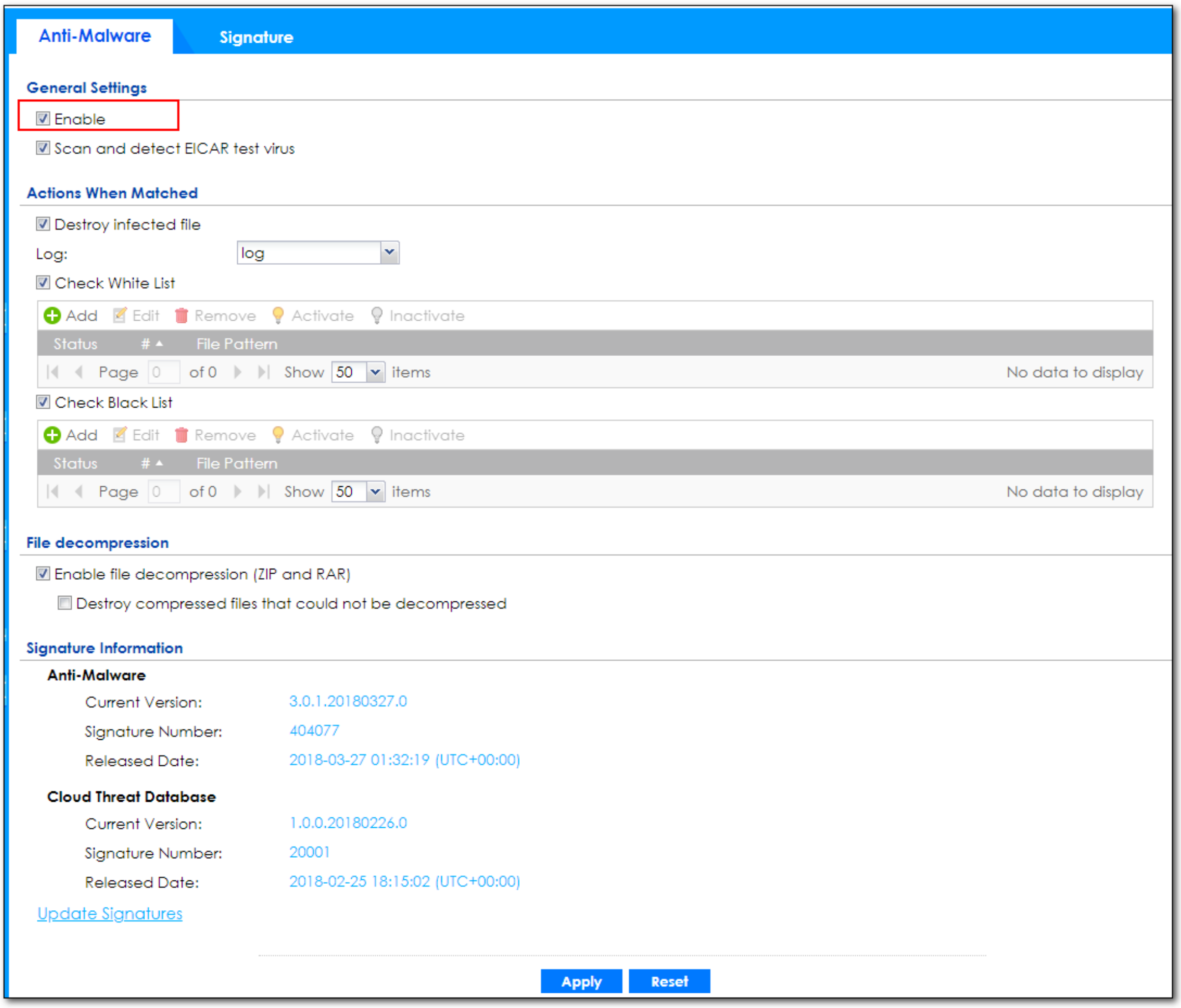
The **Anti-Malware Signature** is means your downloaded files will checked by local signatures that exist on device itself. It is helpful when your device unable access to internet at that moment.

Note: In the default setting, the **Cloud Threat Database** is enabled and with higher priority when scanning the files.

Enable Anti-Malware function to protecting your traffic

Go to **CONFIGURATION > Security Service > Anti-Malware >** Tick in **enable** checkbox to enable Anti-Malware function.

Configuration > Security Service > Anti-Malware > Tick in **enable** checkbox



General Settings

☑ Enable

☑ Scan and detect EICAR test virus

Actions When Matched

☑ Destroy infected file

Log: log

☑ Check White List

Status	# ▲	File Pattern

Page 0 of 0 Show 50 items No data to display

☑ Check Black List

Status	# ▲	File Pattern

Page 0 of 0 Show 50 items No data to display

File decompression

☑ Enable file decompression (ZIP and RAR)

□ Destroy compressed files that could not be decompressed

Signature Information

Anti-Malware

Current Version:	3.0.1.20180327.0
Signature Number:	404077
Released Date:	2018-03-27 01:32:19 (UTC+00:00)

Cloud Threat Database

Current Version:	1.0.0.20180226.0
Signature Number:	20001
Released Date:	2018-02-25 18:15:02 (UTC+00:00)

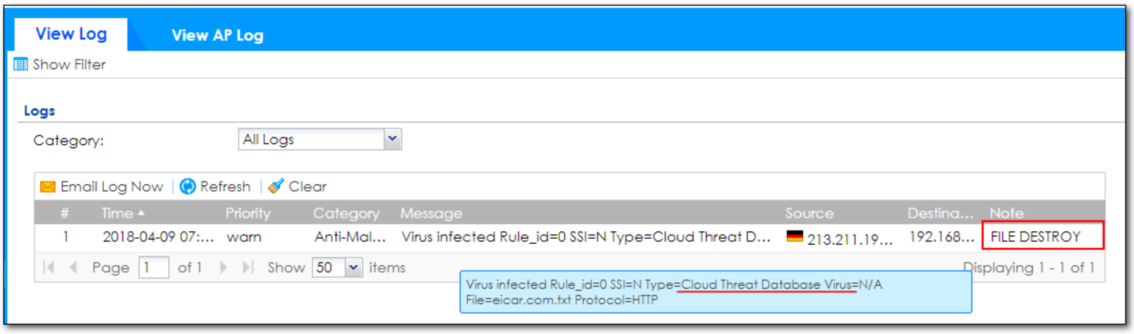
Update Signatures

Note: The Anti-Malware license is required. So you must enabled Anti-Malware function on your myzyxel.com account.

Test the result

After you enabled Anti-Malware function and your PC downloaded the virus file from internet. You device will detected it and drop the file directly.

Then your file is unable opened or replaced by “0”.



View Log | View AP Log

Show Filter

Logs

Category: All Logs

Email Log Now | Refresh | Clear

#	Time ▲	Priority	Category	Message	Source	Destina...	Note
1	2018-04-09 07:...	warn	Anti-Mal...	Virus infected Rule_id=0 SSI=N Type=Cloud Threat D...	213.211.19...	192.168...	FILE DESTROY

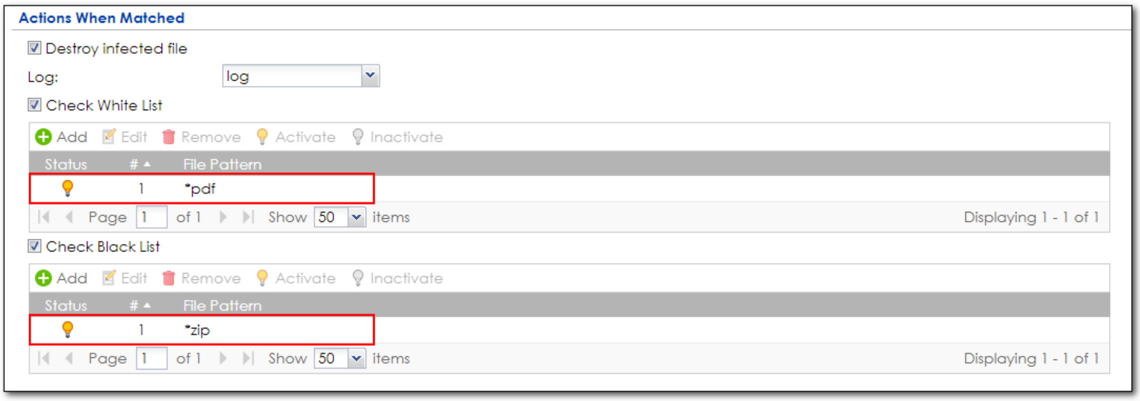
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Virus infected Rule_id=0 SSI=N Type=Cloud Threat Database Virus=N/A File=eicar.com.txt Protocol=HTTP

Additional configuration

White List: You can use wildcard to allowing specific type files.

Black List: You can use wildcard to drop specific type files.



Actions When Matched

☑ Destroy infected file

Log: log

☑ Check White List

Add | Edit | Remove | Activate | Inactivate

Status	# ▲	File Pattern
💡	1	*pdf

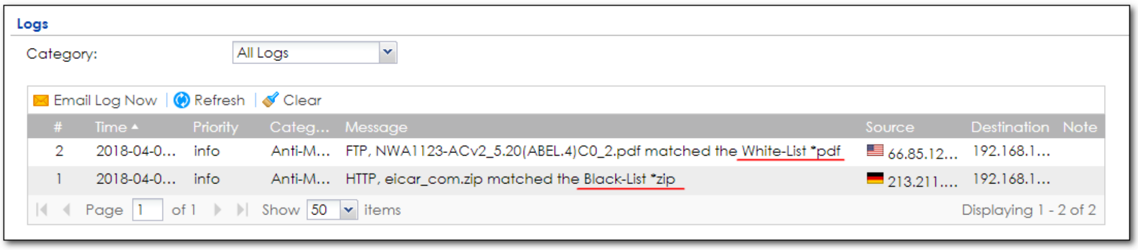
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

☑ Check Black List

Add | Edit | Remove | Activate | Inactivate

Status	# ▲	File Pattern
💡	1	*zip

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



Logs

Category: All Logs

Email Log Now | Refresh | Clear

#	Time ▲	Priority	Categ...	Message	Source	Destination	Note
2	2018-04-0...	info	Anti-M...	FTP, NWA1123-ACv2_5.20(ABEL.4)C0_2.pdf matched the White-List *pdf	66.85.12...	192.168.1...	
1	2018-04-0...	info	Anti-M...	HTTP, eicar_com.zip matched the Black-List *zip	213.211....	192.168.1...	

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

What can go wrong

1 The Anti-Malware service license is required

1 The Anti-Malware is able decompress the file. But it is not support multi-layer zip files.

2 In the default setting, could thread batabase is enabled. You can use the CLI command to activate/deactivate cloud base service. It means the scanning priority will been changed.

  a. ***Router(config)#*** *debug anti-virus ctdb activate*
  b. ***Router(config)#*** *debug anti-virus ctdb deactivate*

How to Configure an Email Security Policy with Mail Scan and DNSBL

This is an example of using ATP Series' UTM Profile to mark or discard spam (unsolicited commercial or junk e-mail). Use the Email Security white list to identify legitimate e-mail. Use the Email Security black list to identify spam e-mail. The ATP Series can also check e-mail against a DNS Black List (DNSBL) of IP addresses of servers that are suspected of being used by spammers.

ATP Series with Email Security Profile to mark or discard spam e-mail Example

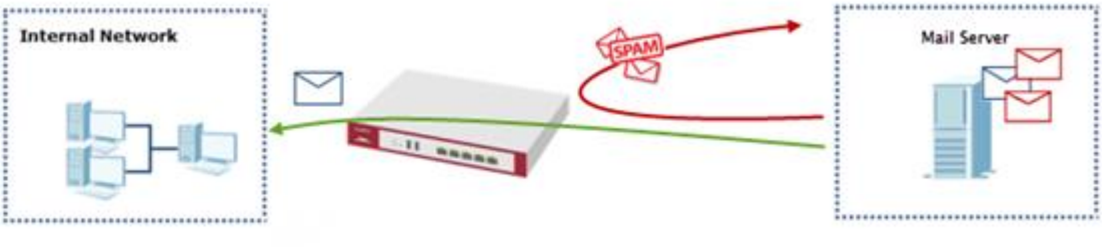


Figure 1 Using Email Security to Detect Spam

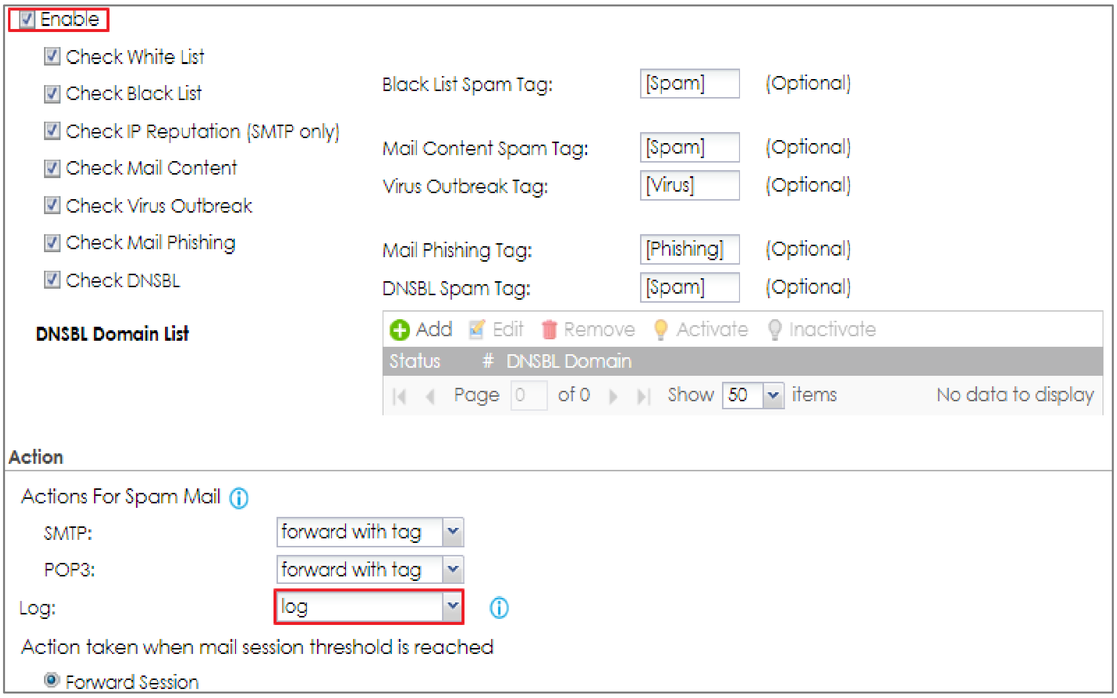
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP200 (Firmware Version: ZLD 4.32).

Set Up the Email Security on ATP Series

In the ATP Series, go to **CONFIGURATION > Security Service> Email Security**; Enable this feature on General Settings page. Select **Check IP Reputation (SMTP only)** to have the ATP Series scan for spam e-mail by IP Reputation. Select **Check Mail Content** to identify Spam Email by content, such as malicious content. Select **Check Virus Outbreak** to scan viruses attached in emails. On advance section, leave Query Timeout Settings to be the default settings.

Select from the list of available **Scan Options** and desired Log type whether to have the ATP Series generate a log (**log**), log and alert (**log alert**) or neither (**no**) by default when traffic matches this policy. Click **Apply** to save the configuration

CONFIGURATION > Security Service > Email Security



☑ Enable

☑ Check White List			
☑ Check Black List	Black List Spam Tag:	[Spam]	(Optional)
☑ Check IP Reputation (SMTP only)			
☑ Check Mail Content	Mail Content Spam Tag:	[Spam]	(Optional)
☑ Check Virus Outbreak	Virus Outbreak Tag:	[Virus]	(Optional)
☑ Check Mail Phishing	Mail Phishing Tag:	[Phishing]	(Optional)
☑ Check DNSBL	DNSBL Spam Tag:	[Spam]	(Optional)

DNSBL Domain List

Status	#	DNSBL Domain

Page 0 of 0 Show 50 items No data to display

Action

Actions For Spam Mail

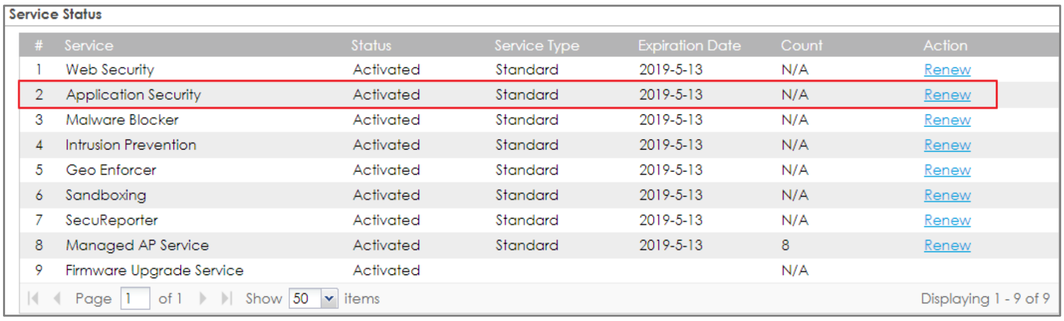
SMTP:	forward with tag
POP3:	forward with tag
Log:	log

Action taken when mail session threshold is reached

● Forward Session

1. Register the device to myZyxel.com.

2. Activate Application Security.

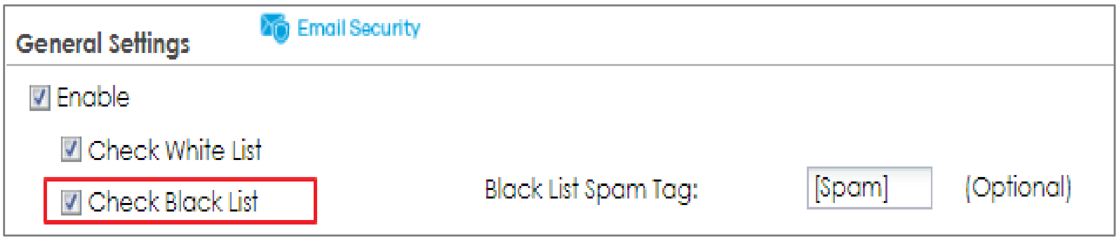


Service Status

#	Service	Status	Service Type	Expiration Date	Count	Action
1	Web Security	Activated	Standard	2019-5-13	N/A	Renew
2	Application Security	Activated	Standard	2019-5-13	N/A	Renew
3	Malware Blocker	Activated	Standard	2019-5-13	N/A	Renew
4	Intrusion Prevention	Activated	Standard	2019-5-13	N/A	Renew
5	Geo Enforcer	Activated	Standard	2019-5-13	N/A	Renew
6	Sandboxing	Activated	Standard	2019-5-13	N/A	Renew
7	SecuReporter	Activated	Standard	2019-5-13	N/A	Renew
8	Managed AP Service	Activated	Standard	2019-5-13	8	Renew
9	Firmware Upgrade Service	Activated			N/A	

Page 1 of 1 Show 50 items Displaying 1 - 9 of 9

3. **Go to CONFIGURATION > Security Service> Email Security>Enable Check Black List** to have the ATP Series treat e-mail that matches (an active) black list entry as spam.



General Settings

☑ Enable

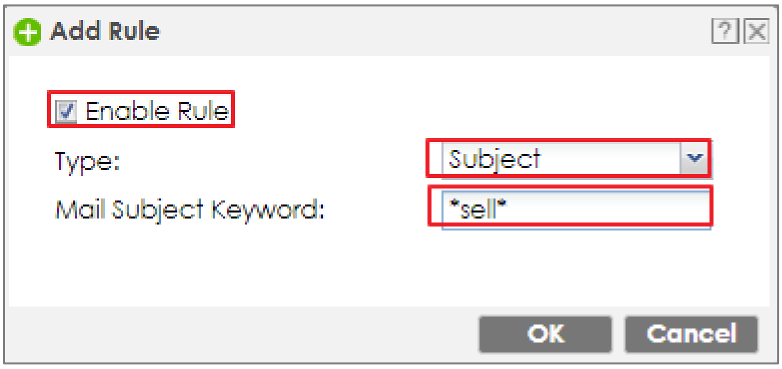
☑ Check White List

☑ Check Black List

Black List Spam Tag: [Spam] (Optional)

4. Continue to **Rule Summary on** Black/White List, click the **Add** icon. A pop-up screen will appear allowing you to configure **Content** (**Subject**, **IP/IPv6 Address**, **E-Mail Address** and **Mail Header**), Use wildcards (*) to configure **Mail Subject Keyword**. (*sell* in this example). Click **OK** to return to the **General** screen.

CONFIGURATION > Security Service> Black/White List



Add Rule

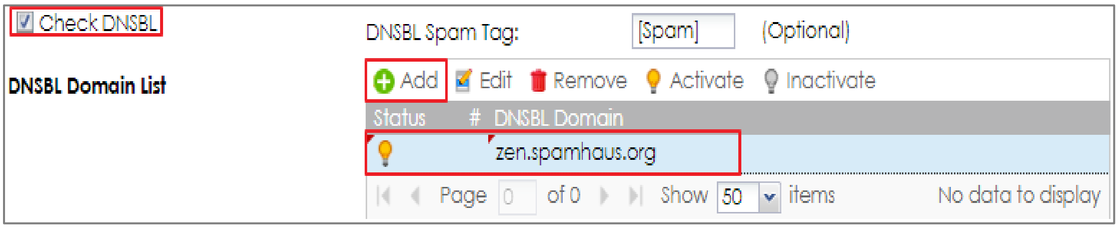
☑ Enable Rule

Type: Subject

Mail Subject Keyword: *sell*

5. In the ATP Series, go to **CONFIGURATION > Security Service> Email Security>Enable Check DNSBL**

Press Add and enter the **DNSBL Domain** for a DNSBL service (zen.spamhaus.org in this example). Click **Apply**.



☑ Check DNSBL

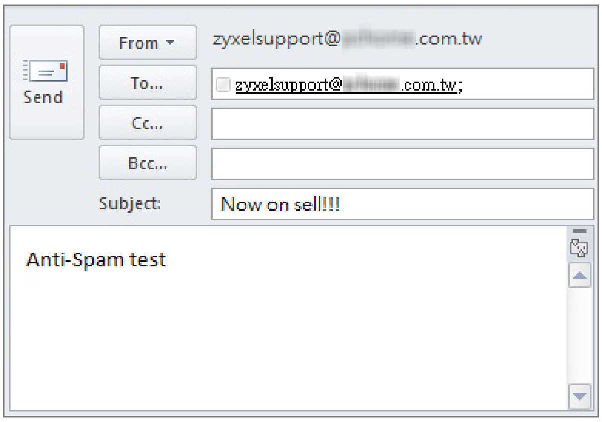
DNSBL Spam Tag: [Spam] (Optional)

DNSBL Domain List

Status	#	DNSBL Domain
💡		zen.spamhaus.org

Test the result

1. Send the mail subject with "sell".



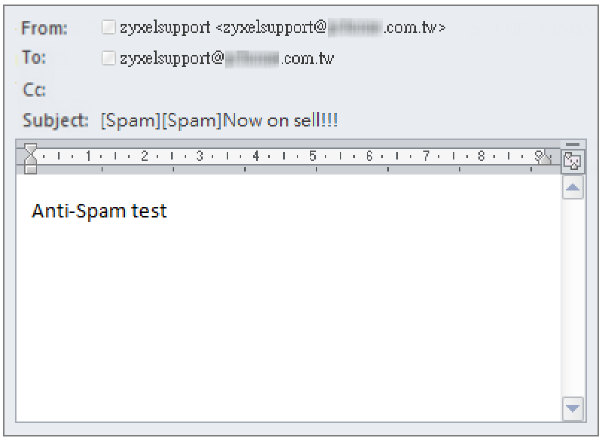
From: zyxelsupport@[redacted].com.tw

To...: zyxelsupport@[redacted].com.tw;

Subject: Now on sell!!!

Anti-Spam test

2. You will receive the mail subject with [Spam] tag.



From: zyxelsupport <zyxelsupport@[redacted].com.tw>

To: zyxelsupport@[redacted].com.tw

Cc:

Subject: [Spam][Spam]Now on sell!!!

Anti-Spam test

What can go wrong

1. If Email Security is not working, there are two possible reasons:

   You have not subscribed for the **Email Security** service.

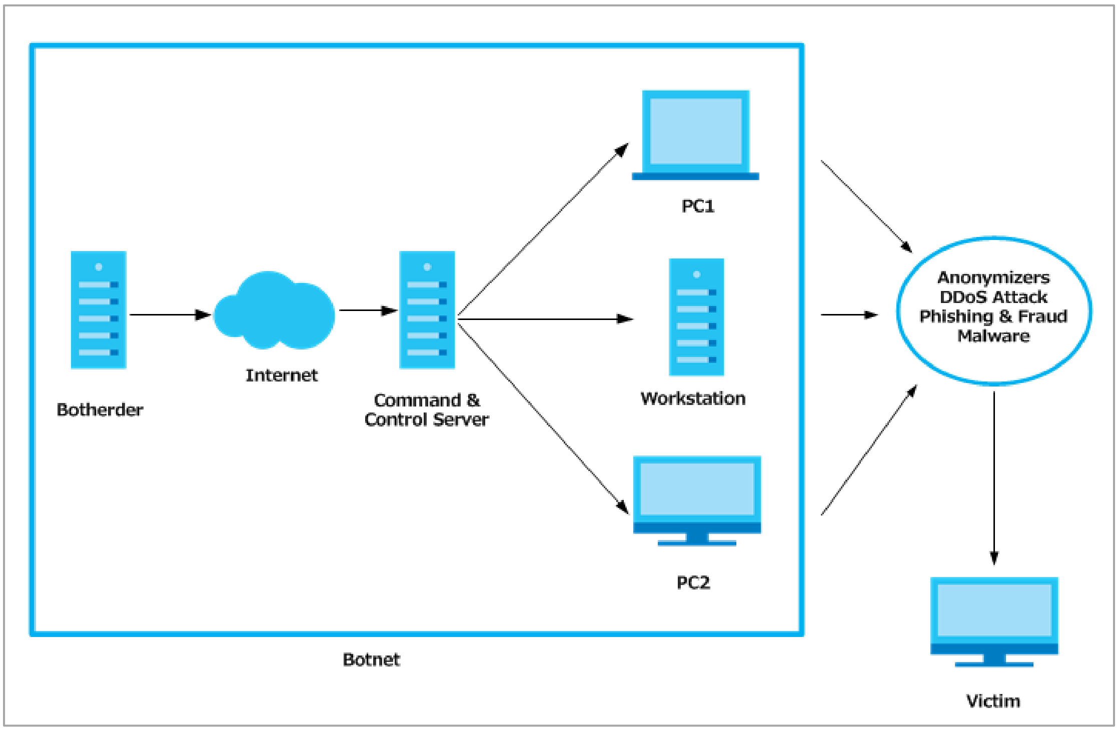
You have subscribed for the **Email Security** service but the license (**Application Security**) is expired.

2. You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **Application Security** license.

How to Configure Botnet Filter on ATP series?

Botnets are organized groups of infected computers. Those infected PCs will try to connect to the command-and-control server and ask for commands. When the attacker sends command to the command-and-control server, it will relay those commands to the clients (infected computers) and perform attacks on particular targets.

The following steps will walk you through an example of how to configure Botnet Filter (IP blocking and URL blocking) on the ATP.



Prerequisites before setting up Botnet Filter function

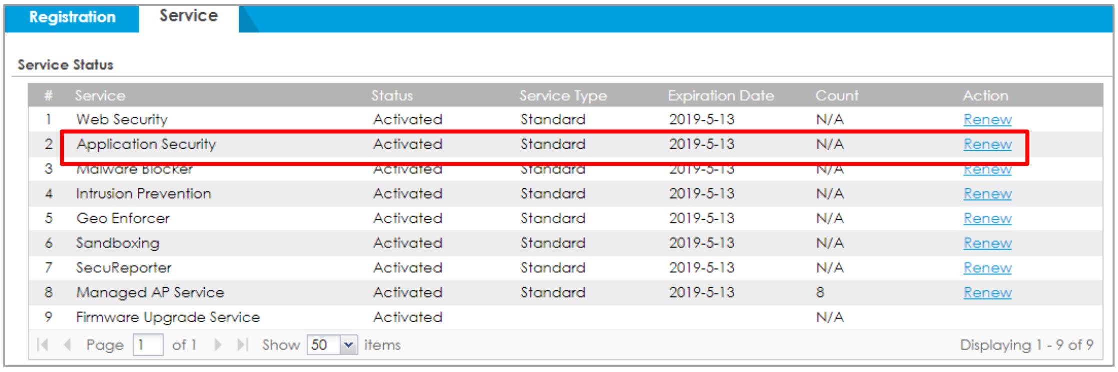
1. License status check
2. Update the Botnet Filter signature

License activation

Before setting up the Botnet Filter function, users need to make sure their licenses are purchased and activated.

To check the license activation status:

Go to configuration > Licensing > Registration > Service and check on the "Application Security" service which includes the Botnet Filtering function.



Service Status

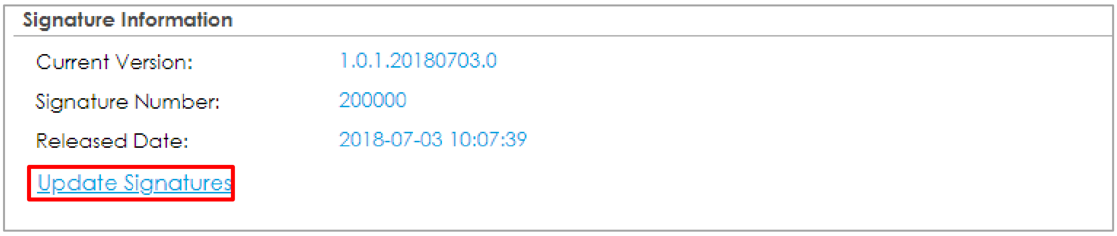
#	Service	Status	Service Type	Expiration Date	Count	Action
1	Web Security	Activated	Standard	2019-5-13	N/A	Renew
2	Application Security	Activated	Standard	2019-5-13	N/A	Renew
3	Malware Blocker	Activated	Standard	2019-5-13	N/A	Renew
4	Intrusion Prevention	Activated	Standard	2019-5-13	N/A	Renew
5	Geo Enforcer	Activated	Standard	2019-5-13	N/A	Renew
6	Sandboxing	Activated	Standard	2019-5-13	N/A	Renew
7	SecuReporter	Activated	Standard	2019-5-13	N/A	Renew
8	Managed AP Service	Activated	Standard	2019-5-13	8	Renew
9	Firmware Upgrade Service	Activated			N/A	

Update Botnet Filter Signatures

To make sure the device has the most updated signature, we suggest users to update their Botnet Filter signature before using this function.

To update the Botnet Filter signature:

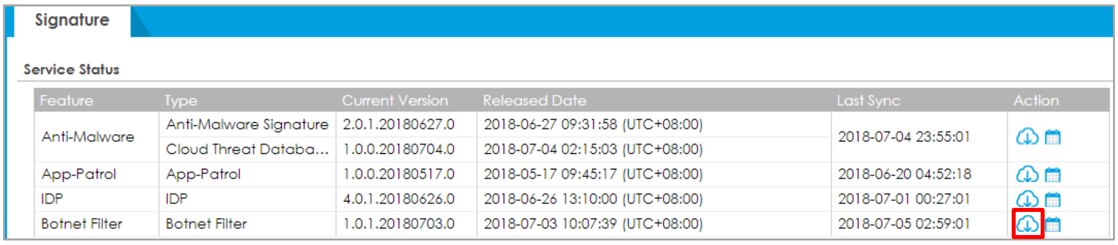
Go to **Configuration** > **Security Service** > **Botnet Filter.** Then click **"Update Signatures"**



Signature Information

Current Version:	1.0.1.20180703.0
Signature Number:	200000
Released Date:	2018-07-03 10:07:39

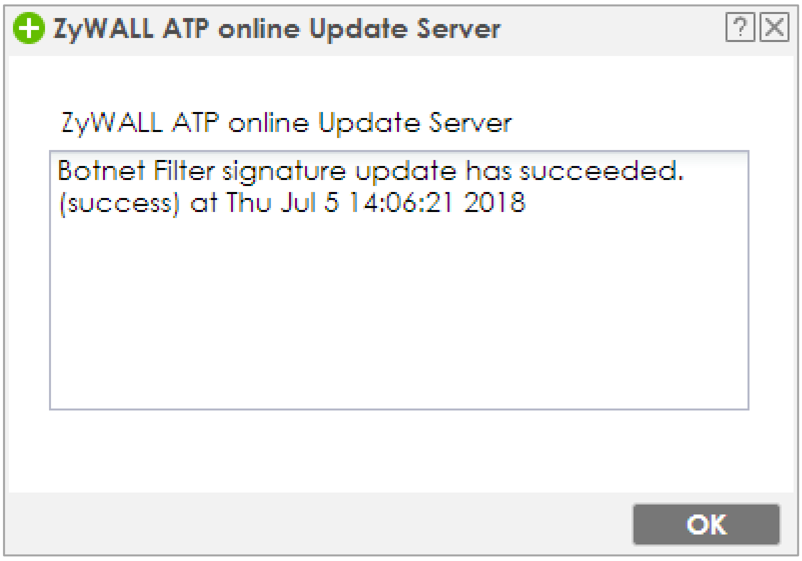
Then the device will redirect users to the "**Service Status**" page. Click on the cloud icon ☁ and the device will start signature downloading process



Service Status

Feature	Type	Current Version	Released Date	Last Sync	Action
Anti-Malware	Anti-Malware Signature	2.0.1.20180627.0	2018-06-27 09:31:58 (UTC+08:00)	2018-07-04 23:55:01	
	Cloud Threat Databa...	1.0.0.20180704.0	2018-07-04 02:15:03 (UTC+08:00)		
App-Patrol	App-Patrol	1.0.0.20180517.0	2018-05-17 09:45:17 (UTC+08:00)	2018-06-20 04:52:18	
IDP	IDP	4.0.1.20180626.0	2018-06-26 13:10:00 (UTC+08:00)	2018-07-01 00:27:01	
Botnet Filter	Botnet Filter	1.0.1.20180703.0	2018-07-03 10:07:39 (UTC+08:00)	2018-07-05 02:59:01	

Once the signature updating process was done. The GUI will pop up the following message to notify users.



ZyWALL ATP online Update Server

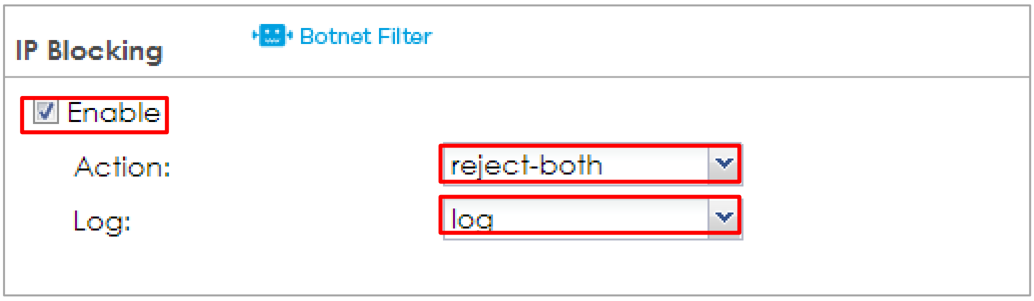
Botnet Filter signature update has succeeded.
(success) at Thu Jul 5 14:06:21 2018

Now the Botnet Filtering function is ready to go.

Set Up the IP Blocking on the ATP series

Go to **Configuration** > **Security Service** > **Botnet Filter.**

Select the **Enable IP Blocking** check box. There're some actions can be selected "reject-both", user can decide if they'd like to "forward", "reject-sender" or "reject-receiver" the blocked IP . In addition, users can select if they want to log the related events or not.



IP Blocking

Botnet Filter

☑ Enable

Action: reject-both

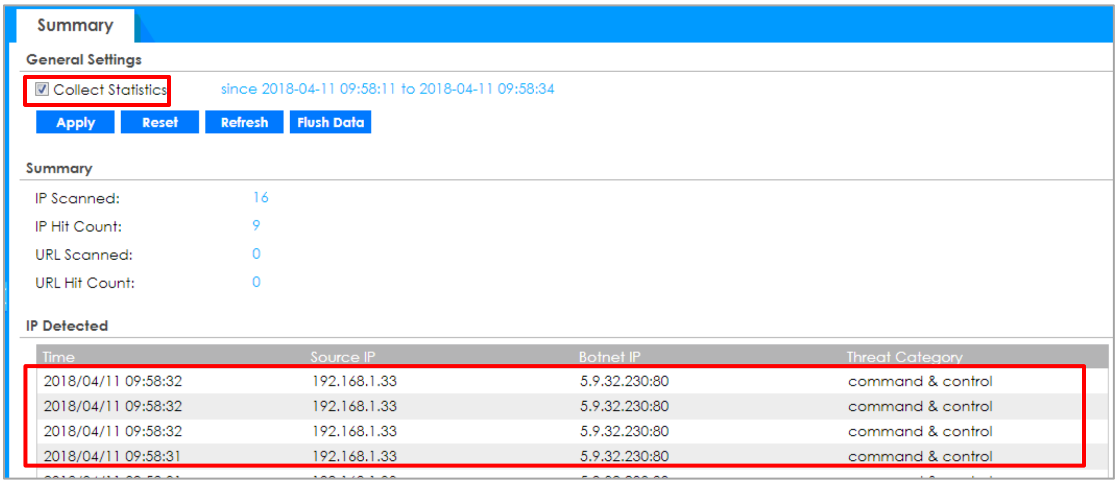
Log: log

Test the Result

User access IP: 5.9.32.230

Go to **Monitor** > **Security Statistics** > **Botnet Filter** to check summary.

IP: 5.9.32.230 is blocked due to command & control.



Summary

General Settings

☑ Collect Statistics since 2018-04-11 09:58:11 to 2018-04-11 09:58:34

Summary

IP Scanned:	16
IP Hit Count:	9
URL Scanned:	0
URL Hit Count:	0

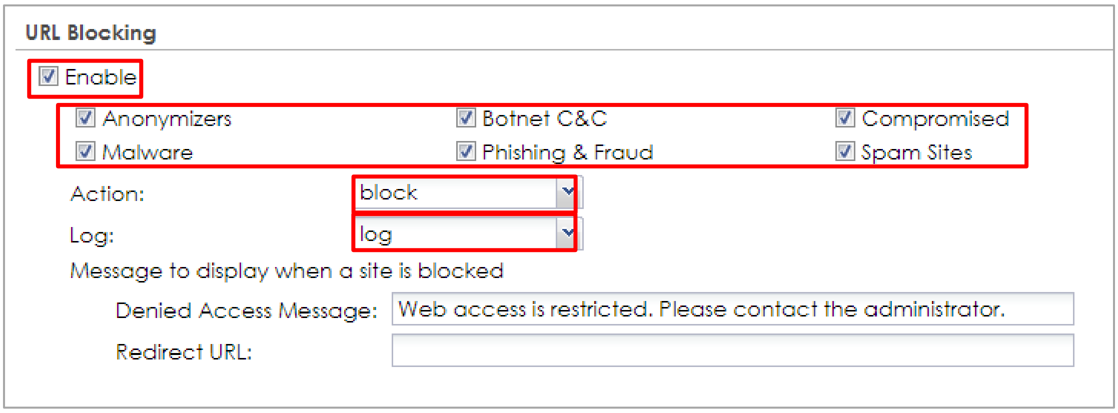
IP Detected

Time	Source IP	Botnet IP	Threat Category
2018/04/11 09:58:32	192.168.1.33	5.9.32.230:80	command & control
2018/04/11 09:58:32	192.168.1.33	5.9.32.230:80	command & control
2018/04/11 09:58:32	192.168.1.33	5.9.32.230:80	command & control
2018/04/11 09:58:31	192.168.1.33	5.9.32.230:80	command & control

Set up the URL Blocking on the ATP series

Go to **Configuration** > **Security Service** > **Botnet Filter.**

Select the **Enable URL Blocking** check box, check the categories that need to be blocked. Users can only check those categories as their requirement. Choose the Action the device will take (In this example we select "block" to block certain URLs) and if they want to Log those events on the device.



URL Blocking

☑ Enable

☑ Anonymizers	☑ Botnet C&C	☑ Compromised
☑ Malware	☑ Phishing & Fraud	☑ Spam Sites

Action: block

Log: log

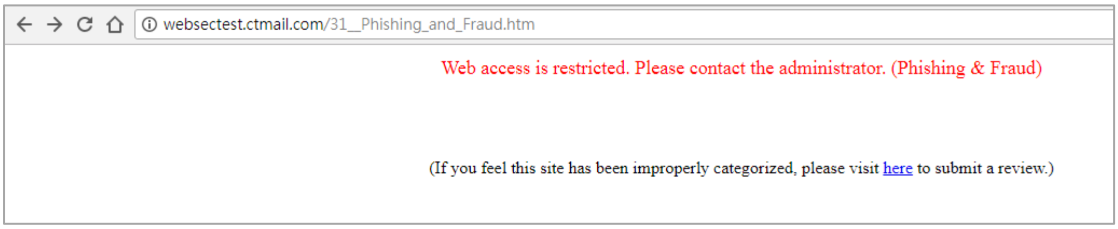
Message to display when a site is blocked

Denied Access Message: Web access is restricted. Please contact the administrator.

Redirect URL:

Test the Result

Browse the Phishing website URL from the host browser. Users will be redirected to an error page in the browser that nofifies users they are visiting to the "Phishing & Fraud" categorized URL

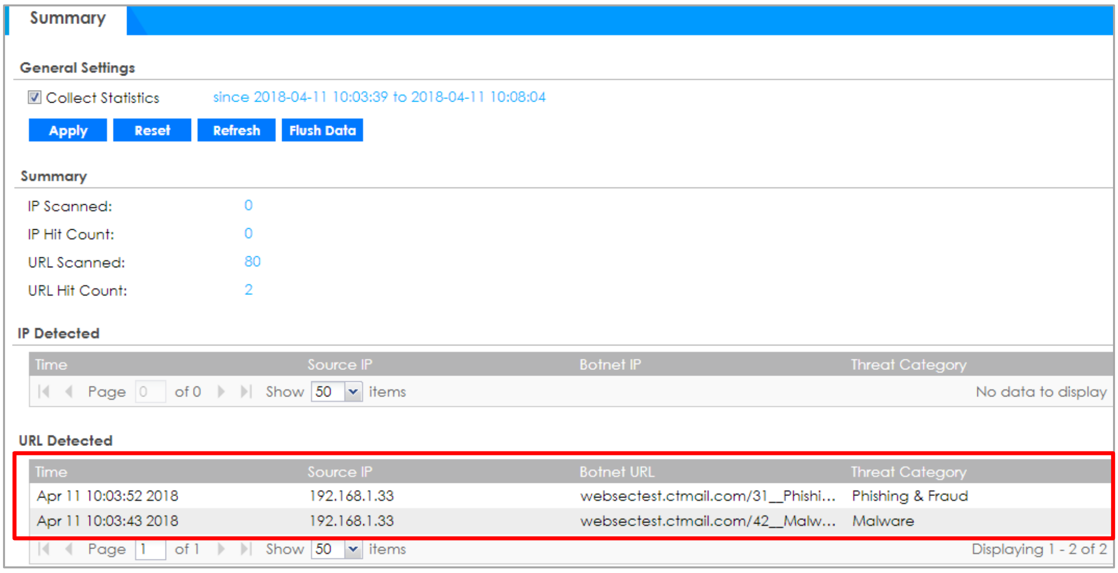


websectest.ctmail.com/31__Phishing_and_Fraud.htm

Web access is restricted. Please contact the administrator. (Phishing & Fraud)

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

Go to **Monitor** > **Security Statistics** > **Botnet Filter** to check summary where users will see the related threat log was recorded



General Settings

☑ Collect Statistics since 2018-04-11 10:03:39 to 2018-04-11 10:08:04

Summary

IP Scanned:	0
IP Hit Count:	0
URL Scanned:	80
URL Hit Count:	2

IP Detected

Time	Source IP	Botnet IP	Threat Category

Page 0 of 0 Show 50 items No data to display

URL Detected

Time	Source IP	Botnet URL	Threat Category
Apr 11 10:03:52 2018	192.168.1.33	websectest.ctmail.com/31__Phishi…	Phishing & Fraud
Apr 11 10:03:43 2018	192.168.1.33	websectest.ctmail.com/42__Malw…	Malware

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

How to Use Sandboxing to Detect Unknown Malware

The traditional security service such as Anti-Virus and IDP are signature-based solution, so they have no chance to detect unknown threats. ZyWALL ATP enhances UTM service and integrates Sandbox solution as a second layer of defense to detect and mitigate advanced threats. Zyxel Sandbox is a cloud-based service that can identify previously unknown malware. Each new threat discovered by Sandbox will be converted to known signatures in the cloud threat database of Anti-Malware. The Anti-Malware examines file for threats before deciding to block or pass to Sandbox. If the file has never been inspected by Sandbox, ZyWALL ATP copies this file to the caches and then forwards the file. A copy of the file is sent to Sandbox for analysis and the analysis result is recorded on device's local cache. Once ZyWALL ATP detects the file again, it can identify the file and take the action based on the previous analysis result on local cache. With the cooperation of Anti-Malware, ATP can immediately block threat which previous detected by Sandbox. This example illustrates how to configure Sandboxing on ATP gateway to detect unknown malware.

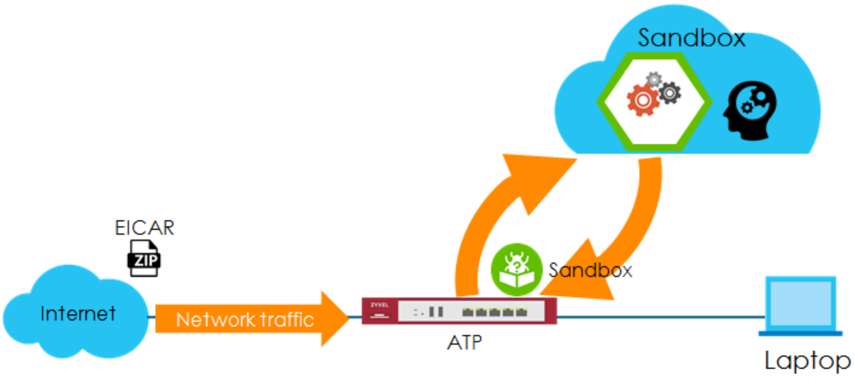
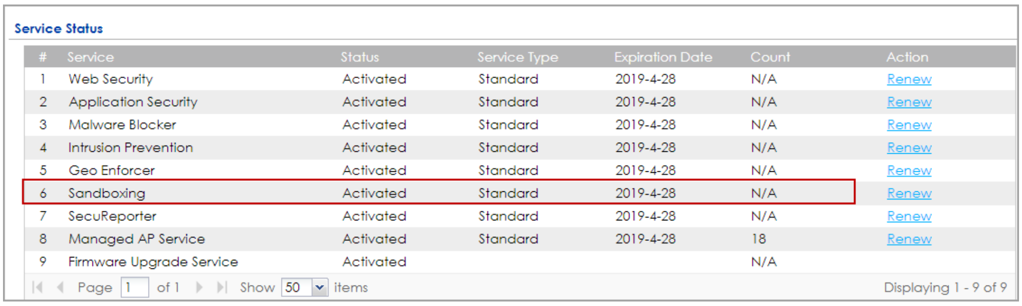


Figure 1 Using Sandboxing to Detect Unknown Malware

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses. This example was tested using the ATP200 (Firmware Version: ZLD 4.32).

Set Up Sandboxing on ATP

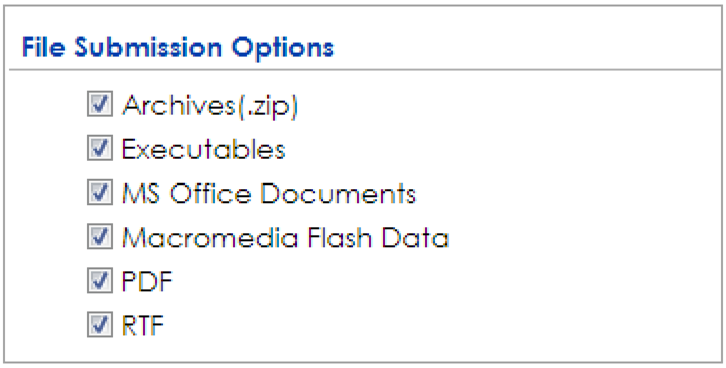
1. Register the device to myZyxel.com.
2. Activate Sandboxing license.



Service Status

#	Service	Status	Service Type	Expiration Date	Count	Action
1	Web Security	Activated	Standard	2019-4-28	N/A	Renew
2	Application Security	Activated	Standard	2019-4-28	N/A	Renew
3	Malware Blocker	Activated	Standard	2019-4-28	N/A	Renew
4	Intrusion Prevention	Activated	Standard	2019-4-28	N/A	Renew
5	Geo Enforcer	Activated	Standard	2019-4-28	N/A	Renew
6	Sandboxing	Activated	Standard	2019-4-28	N/A	Renew
7	SecuReporter	Activated	Standard	2019-4-28	N/A	Renew
8	Managed AP Service	Activated	Standard	2019-4-28	18	Renew
9	Firmware Upgrade Service	Activated			N/A	

3. In the ATP, go to **CONFIGURATION > Security Service > Sandboxing > File Submission Options**, the default supported file types are listed.

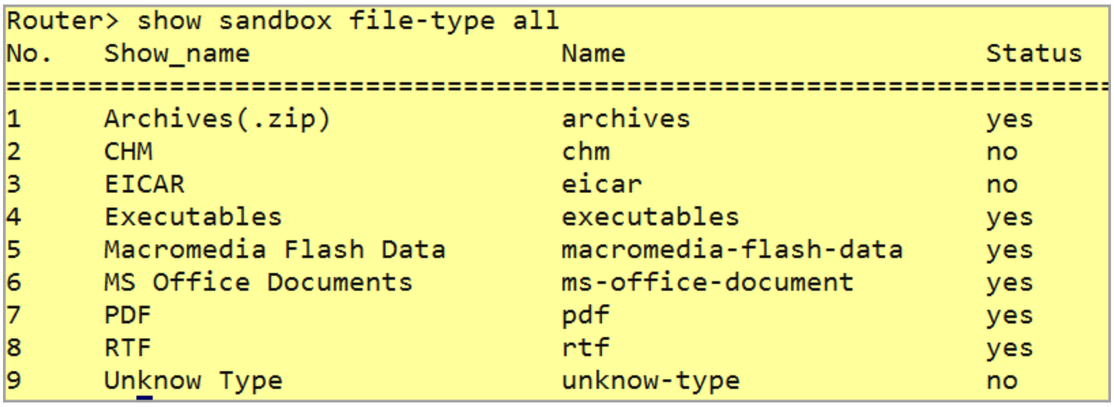


File Submission Options

☑ Archives(.zip)
☑ Executables
☑ MS Office Documents
☑ Macromedia Flash Data
☑ PDF
☑ RTF

Use the command to check the status of each file type. If the status is "no", the file type is not scanned by Sandboxing.

Router> show sandbox file-type all



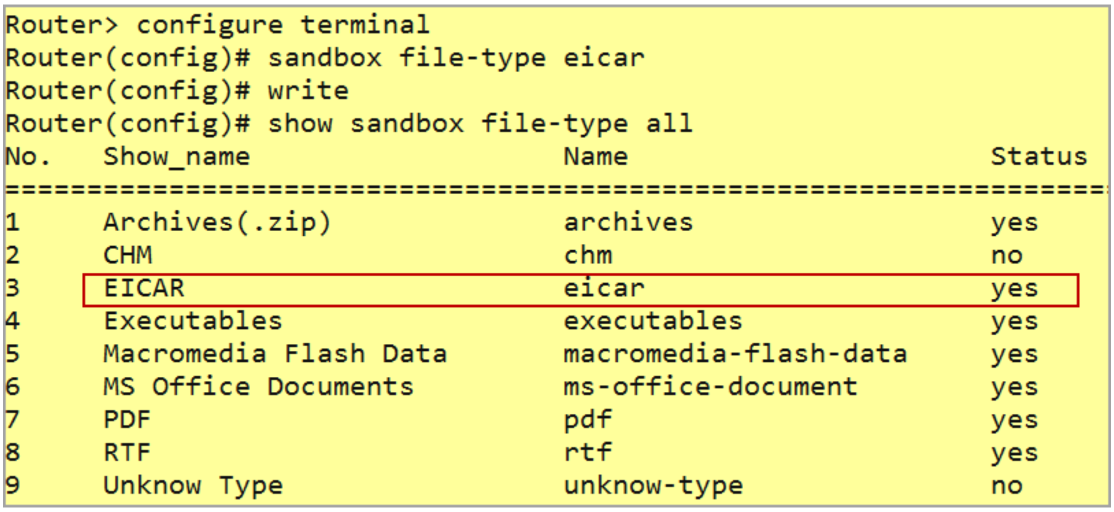
```
Router> show sandbox file-type all
No.   Show_name                    Name                       Status
=====================================================================
1     Archives(.zip)               archives                   yes
2     CHM                          chm                        no
3     EICAR                        eicar                      no
4     Executables                  executables                yes
5     Macromedia Flash Data        macromedia-flash-data      yes
6     MS Office Documents          ms-office-document         yes
7     PDF                          pdf                        yes
8     RTF                          rtf                        yes
9     Unknow Type                  unknow-type                no
```

Use the following commands to make Sandboxing access and check a certain file type.

Router> configure terminal

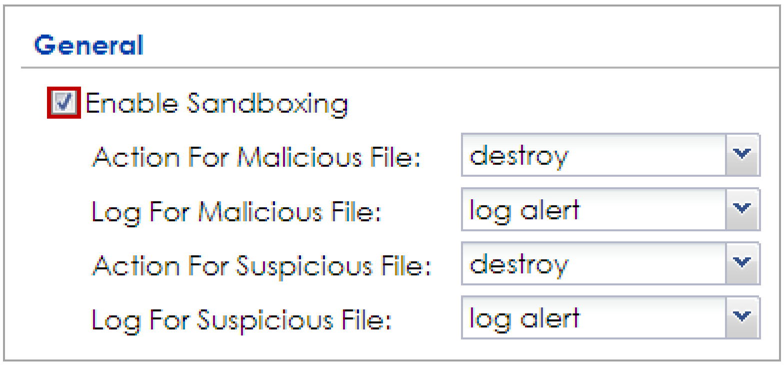
Router(config)# sandbox file-type eicar

Router(config)# write



```
Router> configure terminal
Router(config)# sandbox file-type eicar
Router(config)# write
Router(config)# show sandbox file-type all
No.   Show_name                    Name                       Status
=====================================================================
1     Archives(.zip)               archives                   yes
2     CHM                          chm                        no
3     EICAR                        eicar                      yes
4     Executables                  executables                yes
5     Macromedia Flash Data        macromedia-flash-data      yes
6     MS Office Documents          ms-office-document         yes
7     PDF                          pdf                        yes
8     RTF                          rtf                        yes
9     Unknow Type                  unknow-type                no
```

4. Go to **CONFIGURATION > Security Service > Sandboxing > General**, enable Sandboxing and select action and log for malicious and suspicious files to monitor the result.



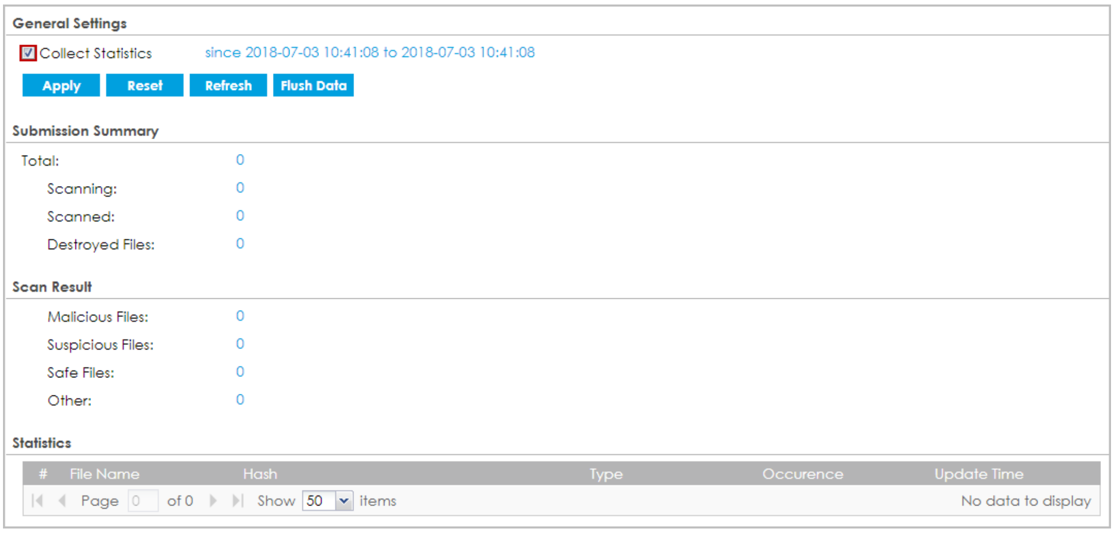
General

☑ Enable Sandboxing

Action For Malicious File:	destroy
Log For Malicious File:	log alert
Action For Suspicious File:	destroy
Log For Suspicious File:	log alert

5. Enable Collect Statistics to monitor the scan results and statistics.

MONITOR > Security Statistics > Sandboxing



General Settings

☑ Collect Statistics since 2018-07-03 10:41:08 to 2018-07-03 10:41:08

Submission Summary

Total:	0
Scanning:	0
Scanned:	0
Destroyed Files:	0

Scan Result

Malicious Files:	0
Suspicious Files:	0
Safe Files:	0
Other:	0

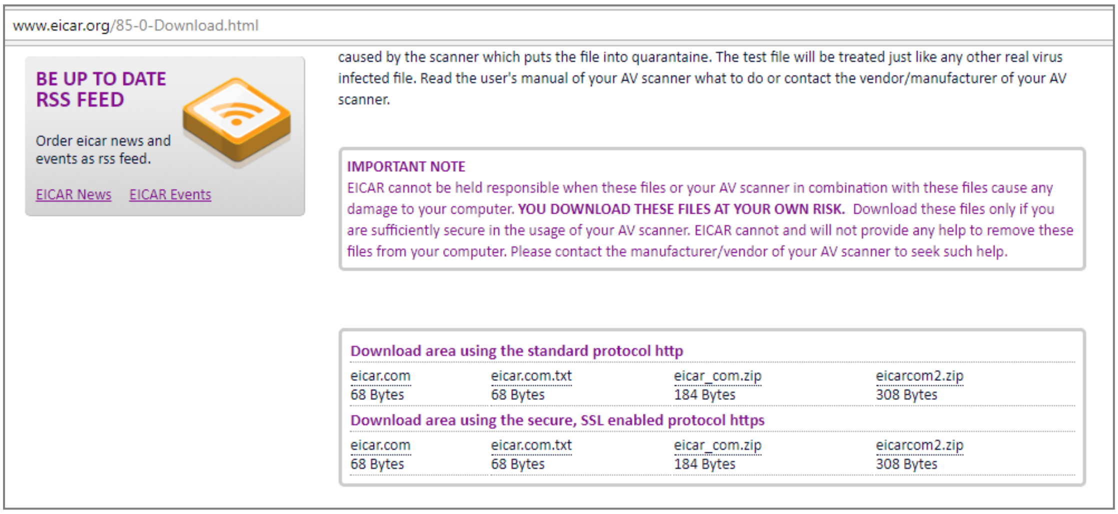
Statistics

#	File Name	Hash	Type	Occurence	Update Time

Page 0 of 0 Show 50 items No data to display

Test the Result

3 Go to http://www.eicar.org/85-0-Download.html to download eicar_com.zip file.



www.eicar.org/85-0-Download.html

BE UP TO DATE RSS FEED

Order eicar news and events as rss feed.

EICAR News   EICAR Events

caused by the scanner which puts the file into quarantaine. The test file will be treated just like any other real virus infected file. Read the user's manual of your AV scanner what to do or contact the vendor/manufacturer of your AV scanner.

IMPORTANT NOTE
EICAR cannot be held responsible when these files or your AV scanner in combination with these files cause any damage to your computer. **YOU DOWNLOAD THESE FILES AT YOUR OWN RISK.** Download these files only if you are sufficiently secure in the usage of your AV scanner. EICAR cannot and will not provide any help to remove these files from your computer. Please contact the manufacturer/vendor of your AV scanner to seek such help.

Download area using the standard protocol http

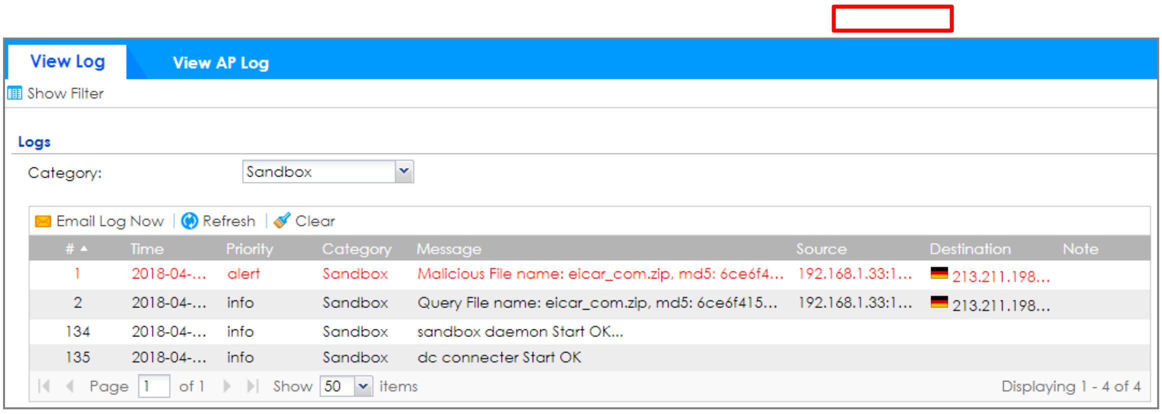
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

Download area using the secure, SSL enabled protocol https

eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

4 When you download eicar_com.zip for the first time, it is considered to be an unknown malware. The file is allowed to pass and a copy of eicar_com.zip will be sent to Sandbox for further scan.

MONITOR > Log > View Log > Sandboxing



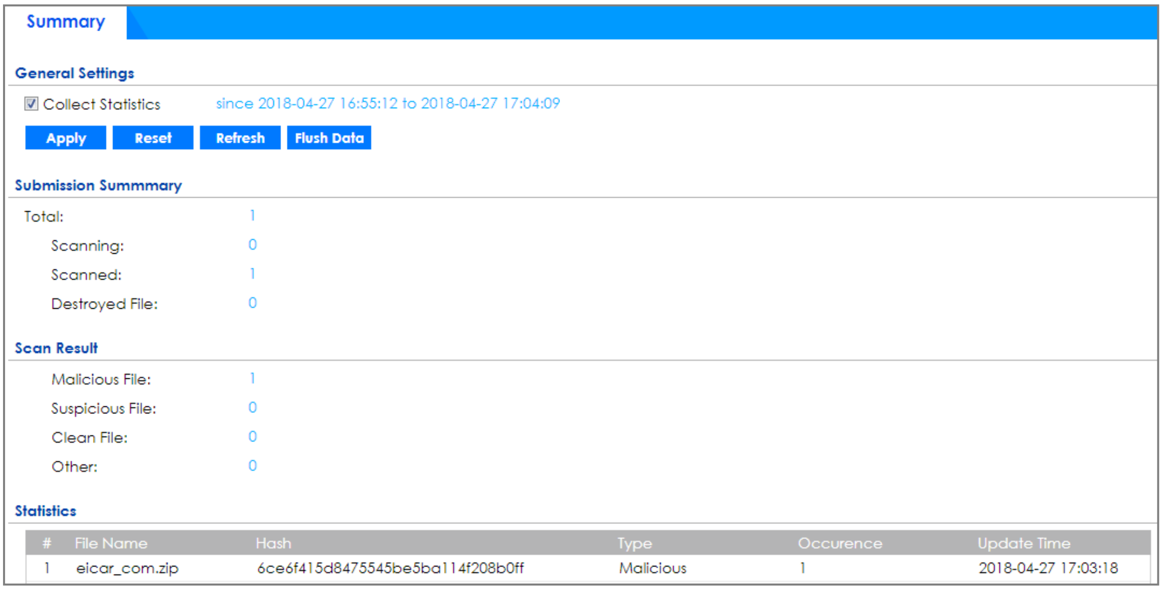
Category: Sandbox

# ▲	Time	Priority	Category	Message	Source	Destination	Note
1	2018-04-...	alert	Sandbox	Malicious File name: eicar_com.zip, md5: 6ce6f4...	192.168.1.33:1...	213.211.198...	
2	2018-04-...	info	Sandbox	Query File name: eicar_com.zip, md5: 6ce6f415...	192.168.1.33:1...	213.211.198...	
134	2018-04-...	info	Sandbox	sandbox daemon Start OK...			
135	2018-04-...	info	Sandbox	dc connecter Start OK			

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

The eicar_com.zip file is detected by Sandbox as a malicious file.

MONITOR > Security Statistics > Sandboxing



General Settings

☑ Collect Statistics since 2018-04-27 16:55:12 to 2018-04-27 17:04:09

Submission Summmary

Total:	1
Scanning:	0
Scanned:	1
Destroyed File:	0

Scan Result

Malicious File:	1
Suspicious File:	0
Clean File:	0
Other:	0

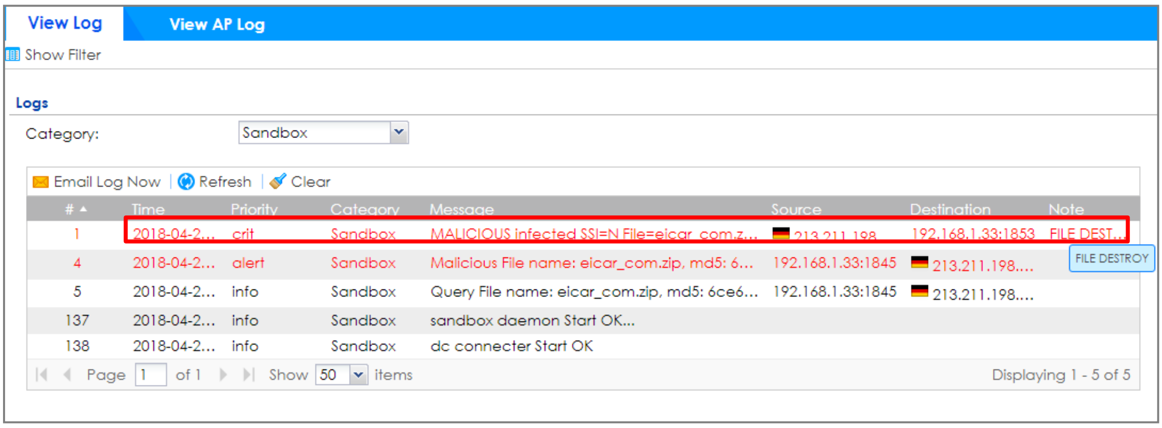
Statistics

#	File Name	Hash	Type	Occurence	Update Time
1	eicar_com.zip	6ce6f415d8475545be5ba114f208b0ff	Malicious	1	2018-04-27 17:03:18

Note: Disable anti-virus software on your laptop in order to test Sandbox.

5 Download eicar_com.zip file again. ZyWALL ATP destroyed the eicar_com.zip file at the second time when you download the file and generate the log.

MONITOR > Log > View Log > Sandboxing



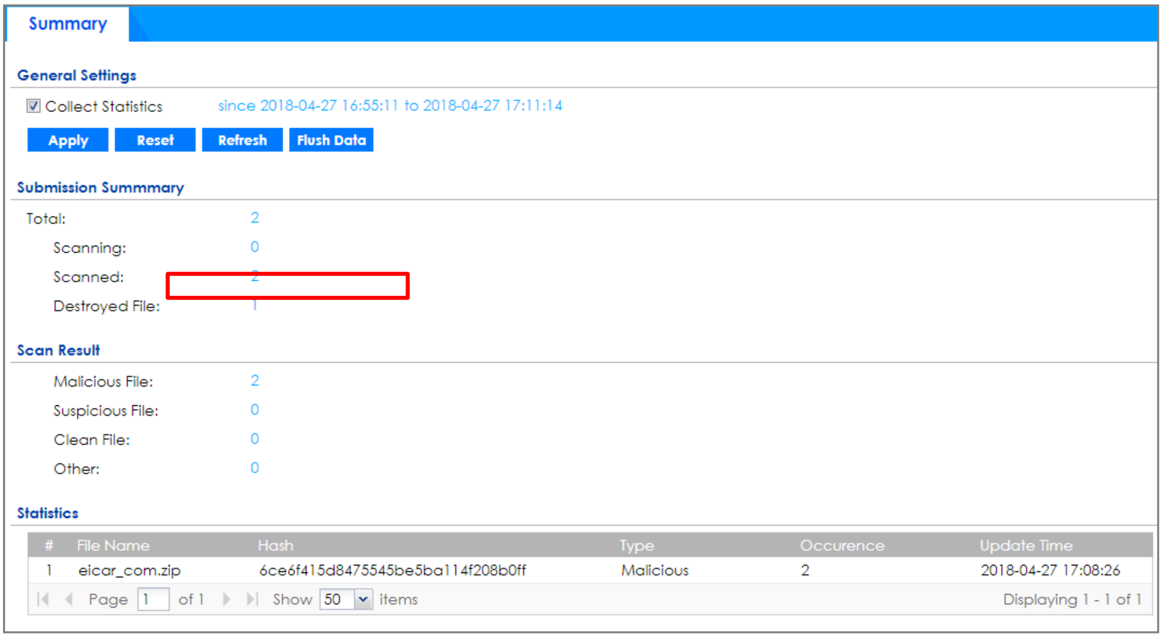
Logs

Category: Sandbox

# ▲	Time	Priority	Category	Message	Source	Destination	Note
1	2018-04-2...	crit	Sandbox	MALICIOUS infected SSI=N File=eicar_com.z...	213.211.198	192.168.1.33:1853	FILE DEST...
4	2018-04-2...	alert	Sandbox	Malicious File name: eicar_com.zip, md5: 6...	192.168.1.33:1845	213.211.198....	
5	2018-04-2...	info	Sandbox	Query File name: eicar_com.zip, md5: 6ce6...	192.168.1.33:1845	213.211.198....	
137	2018-04-2...	info	Sandbox	sandbox daemon Start OK...			
138	2018-04-2...	info	Sandbox	dc connecter Start OK			

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

MONITOR > Security Statistics > Sandboxing



General Settings

☑ Collect Statistics since 2018-04-27 16:55:11 to 2018-04-27 17:11:14

Submission Summmary

Total:	2
Scanning:	0
Scanned:	2
Destroyed File:	1

Scan Result

Malicious File:	2
Suspicious File:	0
Clean File:	0
Other:	0

Statistics

#	File Name	Hash	Type	Occurence	Update Time
1	eicar_com.zip	6ce6f415d8475545be5ba114f208b0ff	Malicious	2	2018-04-27 17:08:26

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

What Can Go Wrong?

6 SSL inspection needs to be enabled and applied to the corresponding security policy rule for HTTPS traffic.

7 Only Windows (Win XP, Win 7, Win 10) and Mac OSX operating system are supported.

8 The local cache of the analysis result will be deleted when the device reboots.

How to configure Email Security for Phishing mail?

(This feature is only supported on ATP series)

The following depicts a sample configuration of Email security for Phishing mail.

Phishing is a type of online scam where criminals send an email with a fake website and asking you to provide sensitive information.

An example of phishing attack:

1. Attacker creates an fake banking websites which copy the content from real banking website
2. Attacker sends user an phishing emails with an embed URLs to ask change the new banking password
3. User opens the mail then click to the embed URLs, it redirects user access to fake banking websites.
4. User enters the current banking account when they attempt change the password
5. Attacker gets the user's banking account and can steal user's money

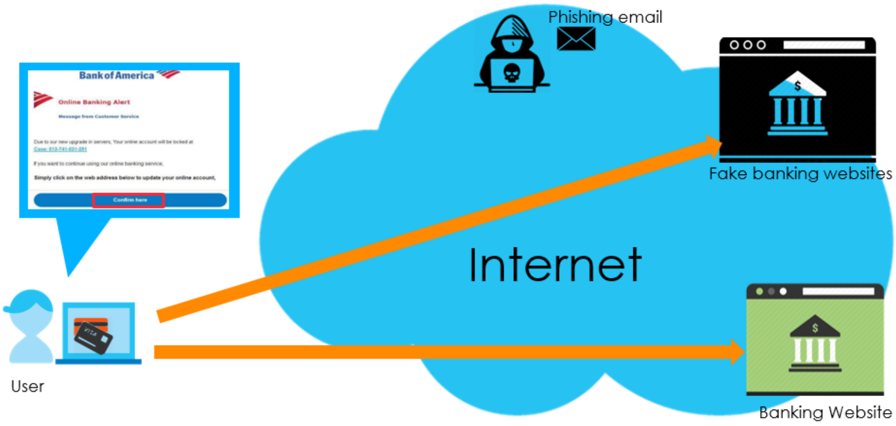
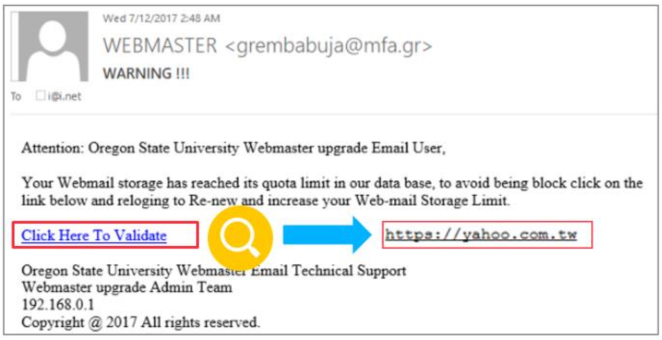

Bank of America
Online Banking Alert
Message from Customer Service
Due to our new upgrade in servers, Your online account will be locked at
Case: 013-741-031-291
If you want to continue using our online banking service,
Simply click on the web address below to update your online account,
Confirm here
Phishing email
Fake banking websites
Internet
User
Banking Website

Figure 1 Using Sandboxing to Detect Unknown Malware

How it works

Gateway inspects the email content to detect the embedded URLs. With Anti-phishing enhancement, ATP gateway inspects the mail content to detect the embedded URLs.



Wed 7/12/2017 2:48 AM

WEBMASTER <grembabuja@mfa.gr>

WARNING !!!

To □i@i.net

Attention: Oregon State University Webmaster upgrade Email User,

Your Webmail storage has reached its quota limit in our data base, to avoid being block click on the link below and reloging to Re-new and increase your Web-mail Storage Limit.

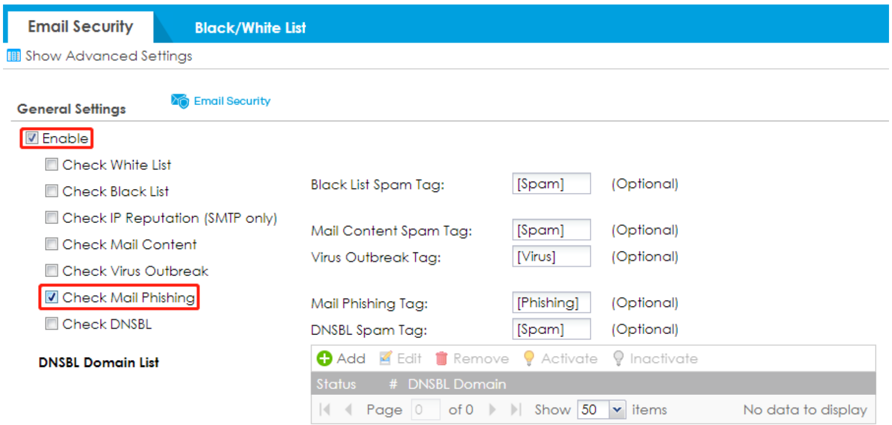
Click Here To Validate → https://yahoo.com.tw

Oregon State University Webmaster Email Technical Support
Webmaster upgrade Admin Team
192.168.0.1
Copyright @ 2017 All rights reserved.

Figure 2 Phishing mail example

Set up Phishing on ATP

In the ATP, Go to **Configuration > Security Service > Email Security** to enable Check Mail Phishing that allows gateway inspects the embed URLs in the email



☑ Enable

□ Check White List

□ Check Black List — Black List Spam Tag: [Spam] (Optional)

□ Check IP Reputation (SMTP only)

□ Check Mail Content — Mail Content Spam Tag: [Spam] (Optional)

□ Check Virus Outbreak — Virus Outbreak Tag: [Virus] (Optional)

☑ Check Mail Phishing — Mail Phishing Tag: [Phishing] (Optional)

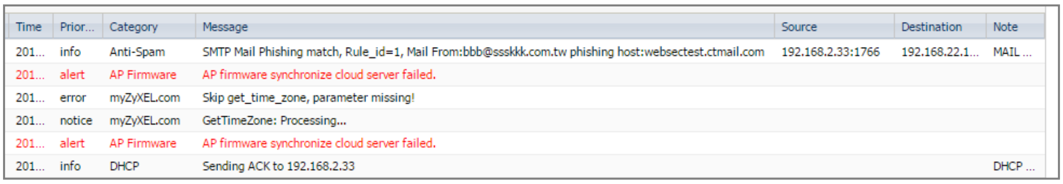
□ Check DNSBL — DNSBL Spam Tag: [Spam] (Optional)

DNSBL Domain List

Test the Result

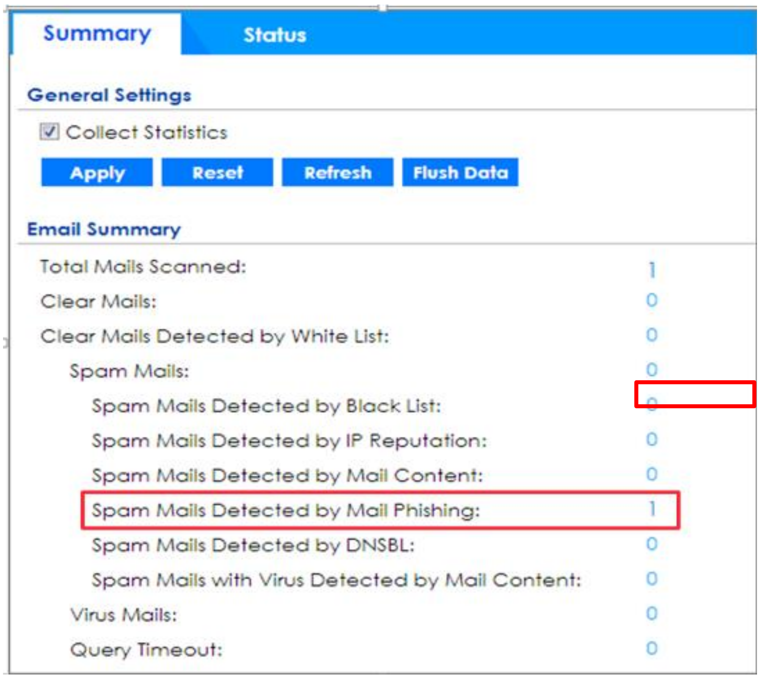
1 Go to **Monitor > Security Statistics > Email Security** to observe mail phishing logs

Monitor > Security Statistics > Email Security



Time	Prior...	Category	Message	Source	Destination	Note
201...	info	Anti-Spam	SMTP Mail Phishing match, Rule_id=1, Mail From:bbb@ssskkk.com.tw phishing host:websectest.ctmail.com	192.168.2.33:1766	192.168.22.1...	MAIL ...
201...	alert	AP Firmware	AP firmware synchronize cloud server failed.			
201...	error	myZyXEL.com	Skip get_time_zone, parameter missing!			
201...	notice	myZyXEL.com	GetTimeZone: Processing...			
201...	alert	AP Firmware	AP firmware synchronize cloud server failed.			
201...	info	DHCP	Sending ACK to 192.168.2.33			DHCP ...

2 Go to **Monitor > Security Statistics > Email Security** to collect Email security statistics



General Settings

☑ Collect Statistics

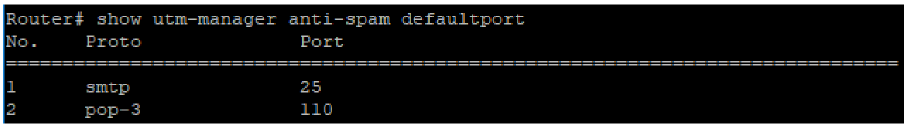
Email Summary

Total Mails Scanned:	1
Clear Mails:	0
Clear Mails Detected by White List:	0
Spam Mails:	0
Spam Mails Detected by Black List:	0
Spam Mails Detected by IP Reputation:	0
Spam Mails Detected by Mail Content:	0
Spam Mails Detected by Mail Phishing:	1
Spam Mails Detected by DNSBL:	0
Spam Mails with Virus Detected by Mail Content:	0
Virus Mails:	0
Query Timeout:	0

What Can Go Wrong?

1 Make sure the Anti-Spam default service port is SMTP or POP3 by CLI

Router# show utm-manager anti-spam defaultport



```
Router# show utm-manager anti-spam defaultport
No.    Proto                 Port
===============================================================================
1      smtp                  25
2      pop-3                 110
```

2 It does not support SSL inspection.

3 The ATP can inspect email up to 50KB. If the mail size greater than 50KB, gateway will inspect the first 50KB from the header

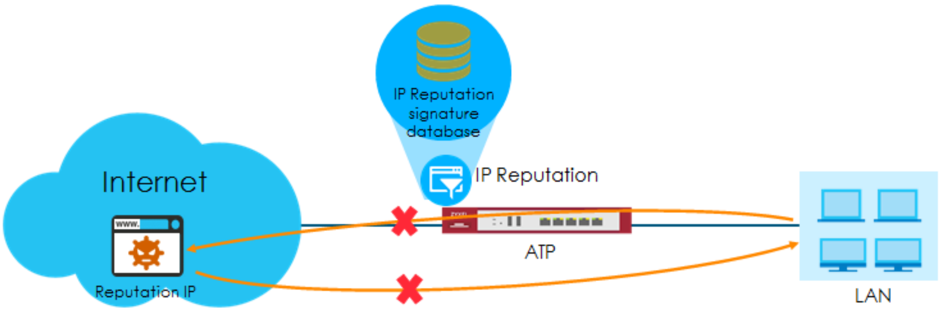
How to Use IP Reputation to Detect Threats

(This feature is only supported on ATP series)

As cyber threats such as scanners, botnets, phishing, etc. grow increasingly, how to identify suspect IP addresses of threats efficiently becomes a crucial task.

With regularly updated IP database, ATP prevents threats by blocking connection to/from known IP addresses based on signature database. It filters source and destination addresses in your network traffic to take the proper risk prevention actions.

This example illustrates how to configure IP Reputation on ATP gateway to detect cyber threats for both incoming and outgoing traffic.

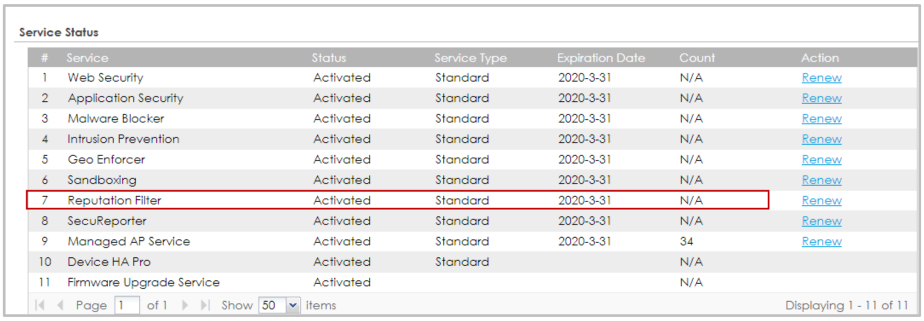


Figure

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses. This example was tested using the ATP500 (Firmware Version: ZLD 4.35).

Activating Reputation Filter Service

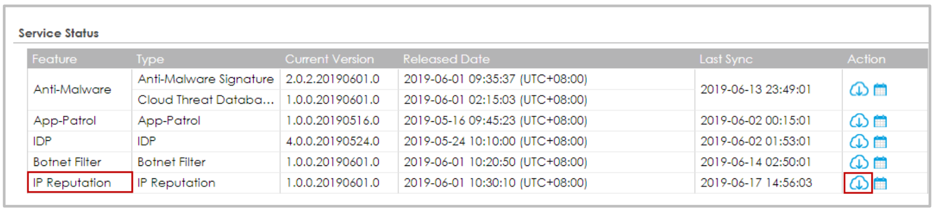
1. Register ATP gateway to myZyxel.com.
2. Activate Reputation Filter license.



Service Status

#	Service	Status	Service Type	Expiration Date	Count	Action
1	Web Security	Activated	Standard	2020-3-31	N/A	Renew
2	Application Security	Activated	Standard	2020-3-31	N/A	Renew
3	Malware Blocker	Activated	Standard	2020-3-31	N/A	Renew
4	Intrusion Prevention	Activated	Standard	2020-3-31	N/A	Renew
5	Geo Enforcer	Activated	Standard	2020-3-31	N/A	Renew
6	Sandboxing	Activated	Standard	2020-3-31	N/A	Renew
7	Reputation Filter	Activated	Standard	2020-3-31	N/A	Renew
8	SecuReporter	Activated	Standard	2020-3-31	N/A	Renew
9	Managed AP Service	Activated	Standard	2020-3-31	34	Renew
10	Device HA Pro	Activated	Standard		N/A	
11	Firmware Upgrade Service	Activated			N/A	

3. On ATP, go to **CONFIGURATION > Licensing > Signature Update.** Click the **Update** icon to check for new signatures.

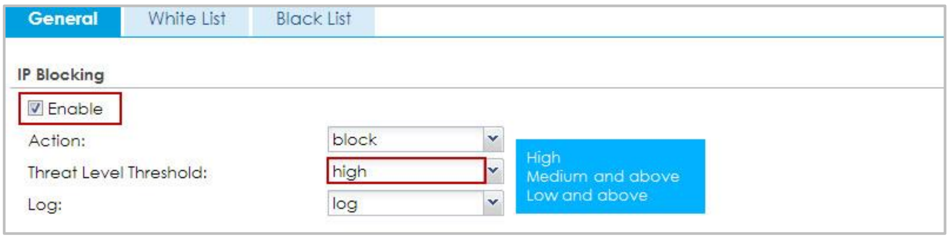


Service Status

Feature	Type	Current Version	Released Date	Last Sync	Action
Anti-Malware	Anti-Malware Signature	2.0.2.20190601.0	2019-06-01 09:35:37 (UTC+08:00)	2019-06-13 23:49:01	
	Cloud Threat Databa...	1.0.0.20190601.0	2019-06-01 02:15:03 (UTC+08:00)		
App-Patrol	App-Patrol	1.0.0.20190516.0	2019-05-16 09:45:23 (UTC+08:00)	2019-06-02 00:15:01	
IDP	IDP	4.0.0.20190524.0	2019-05-24 10:10:00 (UTC+08:00)	2019-06-02 01:53:01	
Botnet Filter	Botnet Filter	1.0.0.20190601.0	2019-06-01 10:20:50 (UTC+08:00)	2019-06-14 02:50:01	
IP Reputation	IP Reputation	1.0.0.20190601.0	2019-06-01 10:30:10 (UTC+08:00)	2019-06-17 14:56:03	

Enabling IP Blocking on ATP

Go to **CONFIGURATION > Security Service > Reputation Filter > IP Reputation > General**. Click **Enable** to detect reputation IPs. The threat level threshold is measured by the query score of IP signature database.



IP Blocking

☑ Enable

Action: block

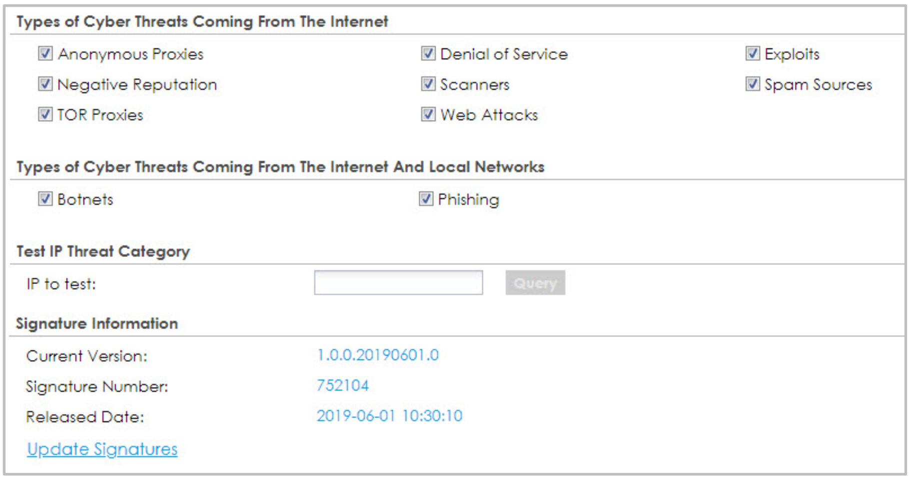
Threat Level Threshold: high

Log: log

Selecting specific type of IP addresses to block

In Types of Cyber Threats Coming From The Internet, select the type of threats that are known to pose a security threat for incoming traffic.

In Types of Cyber Threats Coming From The Internet And Local Networks, select the type of threats that are known to pose a security threat for both incoming and outgoing traffic.



Types of Cyber Threats Coming From The Internet

☑ Anonymous Proxies ☑ Denial of Service ☑ Exploits

☑ Negative Reputation ☑ Scanners ☑ Spam Sources

☑ TOR Proxies ☑ Web Attacks

Types of Cyber Threats Coming From The Internet And Local Networks

☑ Botnets ☑ Phishing

Test IP Threat Category

IP to test: [ ] Query

Signature Information

Current Version: 1.0.0.20190601.0

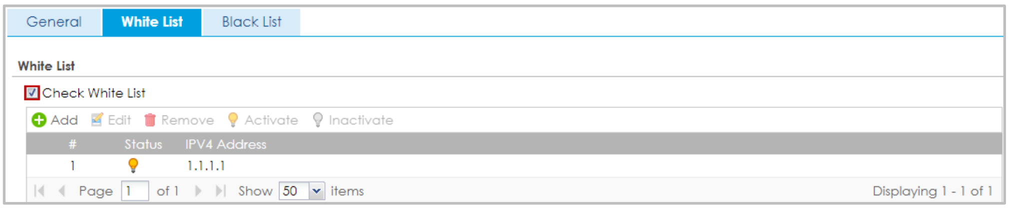
Signature Number: 752104

Released Date: 2019-06-01 10:30:10

Update Signatures

Adding IP addresses to white list and black list

Go to **CONFIGURATION > Security Service > Reputation Filter > IP Reputation > White List** and **Black List** to manually adding IP addresses to the White List and Black List.



General | White List | Black List

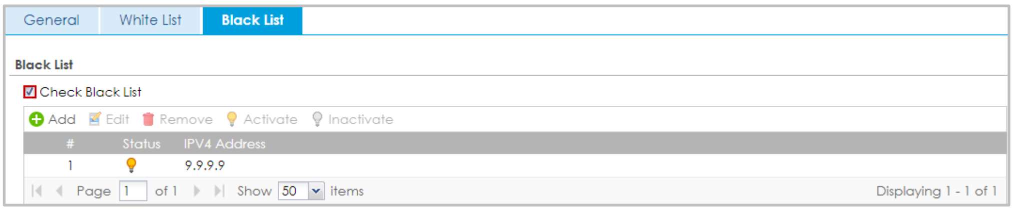
White List

☑ Check White List

Add Edit Remove Activate Inactivate

#	Status	IPV4 Address
1	●	1.1.1.1

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



General | White List | Black List

Black List

☑ Check Black List

Add Edit Remove Activate Inactivate

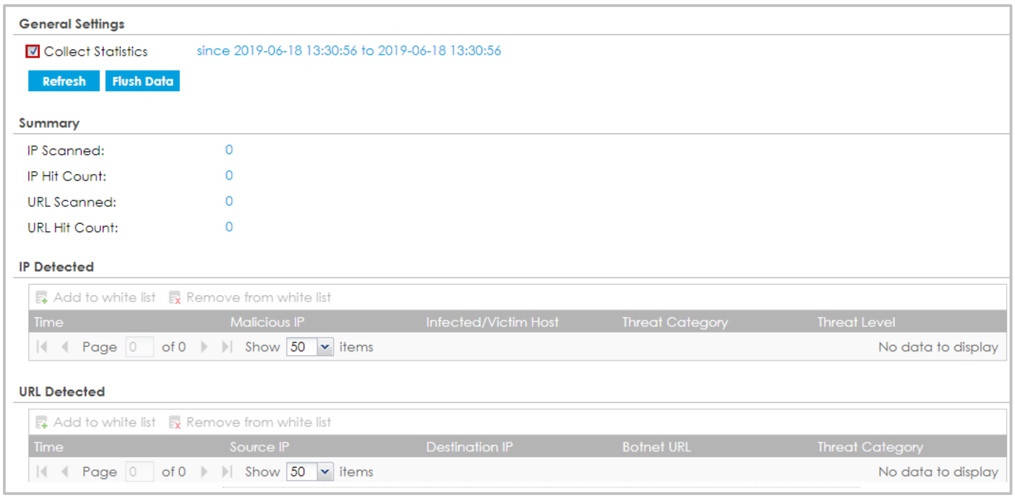
#	Status	IPV4 Address
1	●	9.9.9.9

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

Monitoring statistics for IP detection

Enable Collect Statistics to monitor the scanned result and detected IP.

MONITOR > Security Statistics > Reputation Filter



General Settings

☑ Collect Statistics since 2019-06-18 13:30:56 to 2019-06-18 13:30:56

Summary

IP Scanned:	0
IP Hit Count:	0
URL Scanned:	0
URL Hit Count:	0

IP Detected

Time	Malicious IP	Infected/Victim Host	Threat Category	Threat Level

Page 0 of 0 Show 50 items No data to display

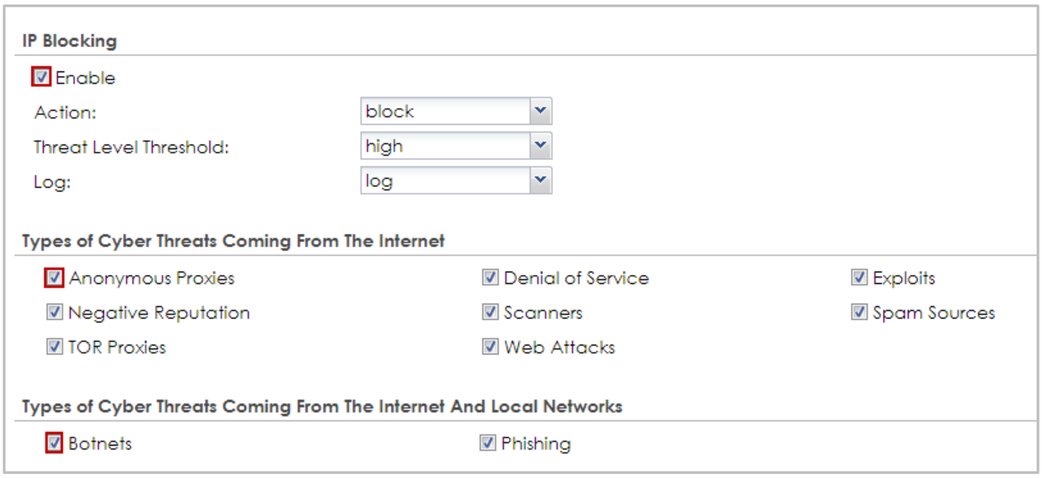
URL Detected

Time	Source IP	Destination IP	Botnet URL	Threat Category

Page 0 of 0 Show 50 items No data to display

Test the Result

1 Select Anonymous Proxies for detecting incoming traffic and Botnet for outgoing traffic.



IP Blocking

☑ Enable

Action: block

Threat Level Threshold: high

Log: log

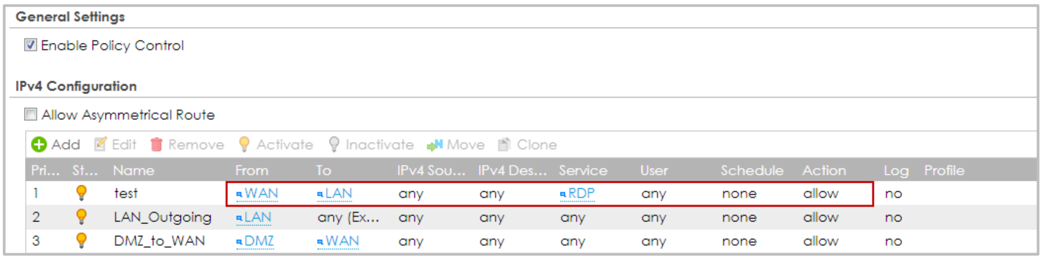
Types of Cyber Threats Coming From The Internet

☑ Anonymous Proxies ☑ Denial of Service ☑ Exploits
☑ Negative Reputation ☑ Scanners ☑ Spam Sources
☑ TOR Proxies ☑ Web Attacks

Types of Cyber Threats Coming From The Internet And Local Networks

☑ Botnets ☑ Phishing

2 For incoming traffic, set a NAT rule and add a security policy rule for allowing traffic from WAN to LAN.



General Settings

☑ Enable Policy Control

IPv4 Configuration

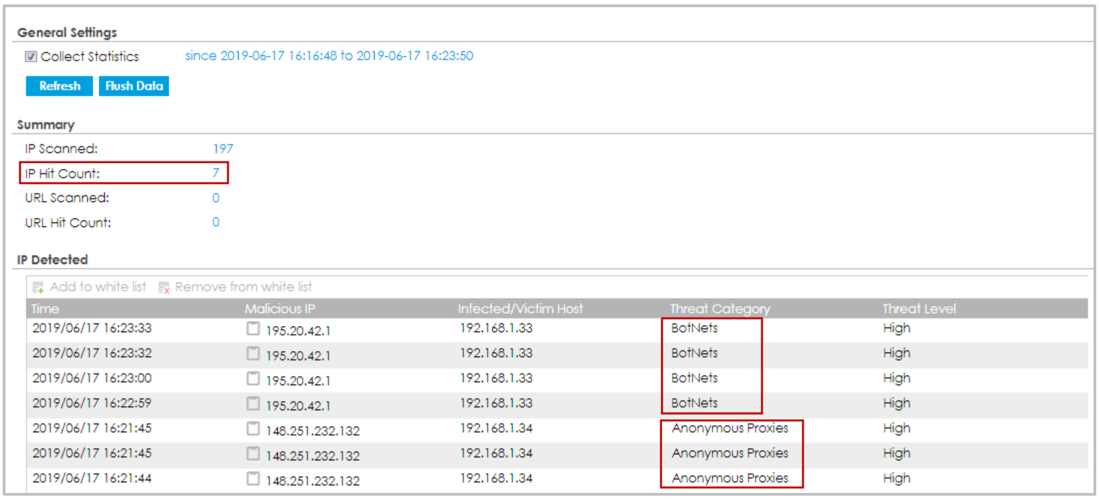
☐ Allow Asymmetrical Route

Pri...	St...	Name	From	To	IPv4 Sou...	IPv4 Des...	Service	User	Schedule	Action	Log	Profile
1		test	WAN	LAN	any	any	RDP	any	none	allow	no	
2		LAN_Outgoing	LAN	any (Ex...	any	any	any	any	none	allow	no	
3		DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	allow	no	

For outgoing traffic, ping an IP address in the threat category "Botnets" from LAN.

3 Check statistics for detected IPs.

MONITOR > Security Statistics > Reputation Filter



General Settings

☑ Collect Statistics since 2019-06-17 16:16:48 to 2019-06-17 16:23:50

Summary

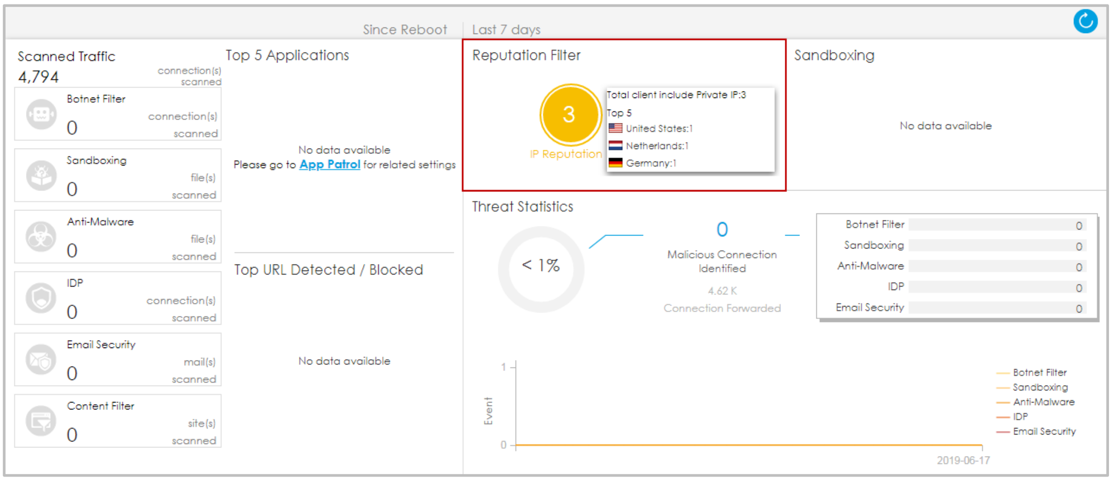
IP Scanned:	197
IP Hit Count:	7
URL Scanned:	0
URL Hit Count:	0

IP Detected

Time	Malicious IP	Infected/Victim Host	Threat Category	Threat Level
2019/06/17 16:23:33	☐ 195.20.42.1	192.168.1.33	BotNets	High
2019/06/17 16:23:32	☐ 195.20.42.1	192.168.1.33	BotNets	High
2019/06/17 16:23:00	☐ 195.20.42.1	192.168.1.33	BotNets	High
2019/06/17 16:22:59	☐ 195.20.42.1	192.168.1.33	BotNets	High
2019/06/17 16:21:45	☐ 148.251.232.132	192.168.1.34	Anonymous Proxies	High
2019/06/17 16:21:45	☐ 148.251.232.132	192.168.1.34	Anonymous Proxies	High
2019/06/17 16:21:44	☐ 148.251.232.132	192.168.1.34	Anonymous Proxies	High

On dashboard, you can find top 5 countries that are detected the most by IP Reputation.

Dashboard > Advanced Threat Protection



What Can Go Wrong?

1. For device HA or HA Pro, signature synchronization is required.
2. Cloud query is not supported.
3. It doesn't support for IPv6.

How to Configure Reputation Filter- DNS Filter

DNS Filter is a mechanism aimed at protecting users by intercepting DNS request attempting to connect to known malicious or unwanted domains and returning a false, or rather controlled IP address. The controlled IP address points to a sinkhole server defined by the administrator.

Suppose of there a client who wants to access malicious domain. This will send query to the DNS server for getting the domain name details. All of the traffic now here gateway intercepts this query which is outgoing. Gateway contains DNS signatures and identifies that this is bad site. What gateway can do here is send the redirect IP address where we deploy a blocked page to the client. The client will connect to redirect IP address instead of the real IP address of malicious domain, and get the blocked page with the web access. This example will show you how to configure DNS Filter to redirect web access after client hit the filter profile.

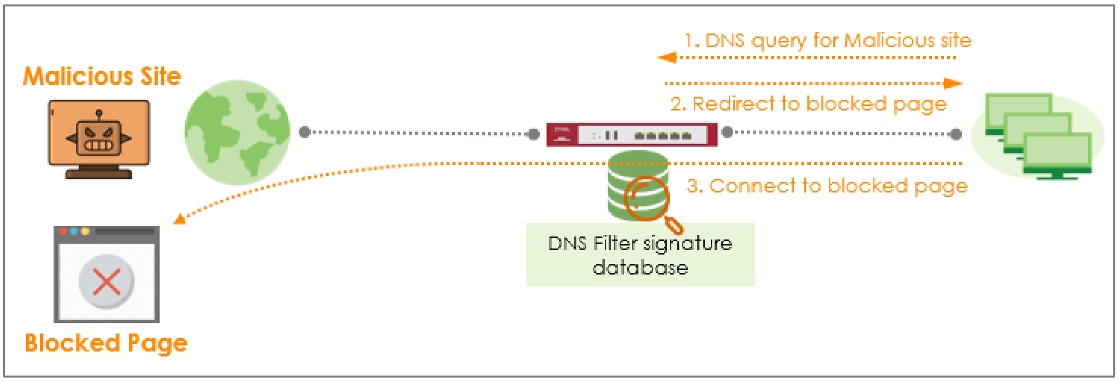
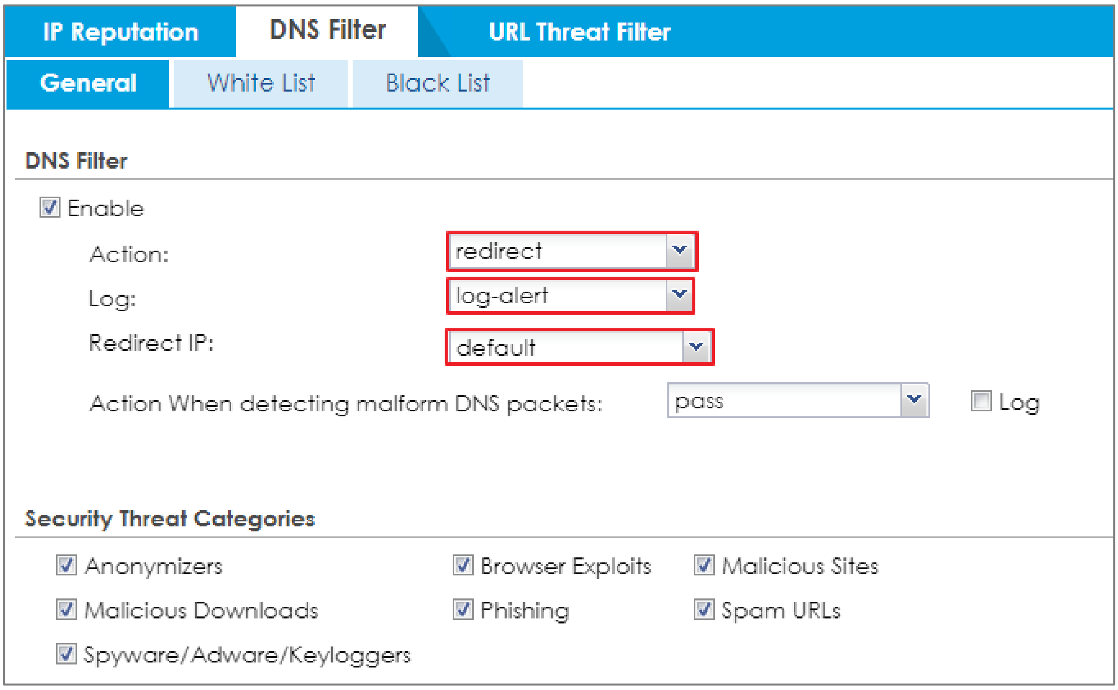

Malicious Site
1. DNS query for Malicious site
2. Redirect to blocked page
3. Connect to blocked page
DNS Filter signature database
Blocked Page

Figure. DNS Filter protects user from malicious websites

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP500 (Firmware Version: ZLD 4.60).

Set Up the DNS Filter on ATP Series

In the ATP Series, go to **CONFIGURATION** > **Security Service**> **Reputation Filter**>**DNS Filter**; Enable this feature on General Settings page. Select **Redirect** on Action field**.** If user select the redirect, when client hit DNS Filter, the page will be redirect to our blocked page or a custom IP address. Choose **Log-alert** on Log field. Configure **Default** on Redirect IP field to allow gateway redirect to our blocked page. Then Press **Apply** button.



DNS Filter

☑ Enable

Action: redirect

Log: log-alert

Redirect IP: default

Action When detecting malform DNS packets: pass □ Log

Security Threat Categories

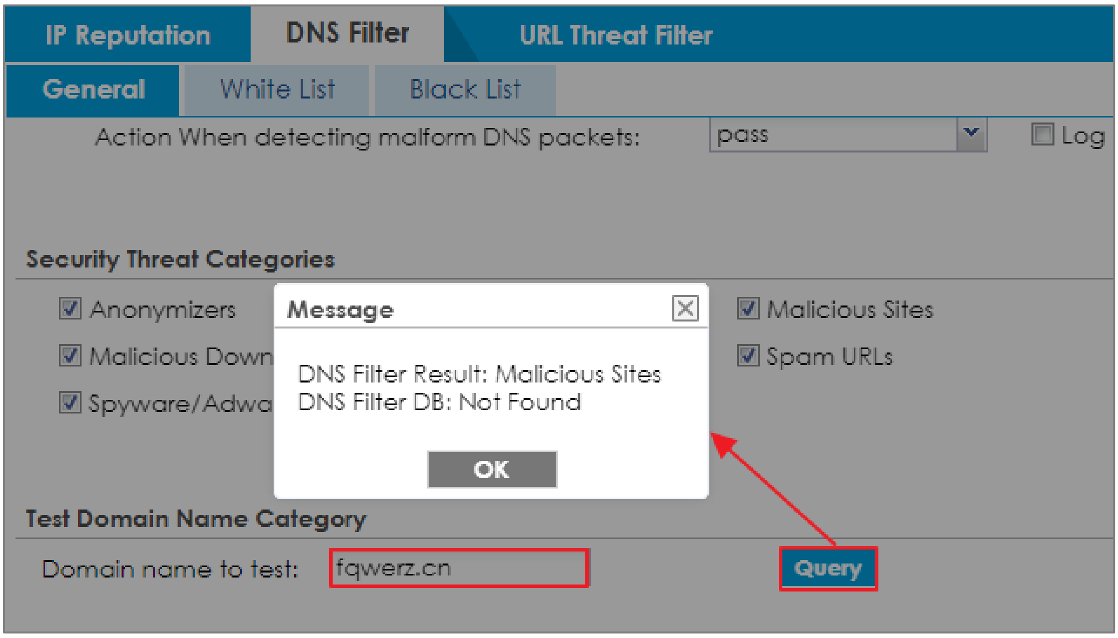
☑ Anonymizers ☑ Browser Exploits ☑ Malicious Sites

☑ Malicious Downloads ☑ Phishing ☑ Spam URLs

☑ Spyware/Adware/Keyloggers

Test the Result

Verify a domain name in the Security Threat Categories. Go to **CONFIGURATION** > **Security Service**> **Reputation Filter**>**DNS Filter**; enter a malicious domain to test:



Action When detecting malform DNS packets: pass □ Log

Security Threat Categories

☑ Anonymizers
☑ Malicious Down
☑ Spyware/Adwa
☑ Malicious Sites
☑ Spam URLs

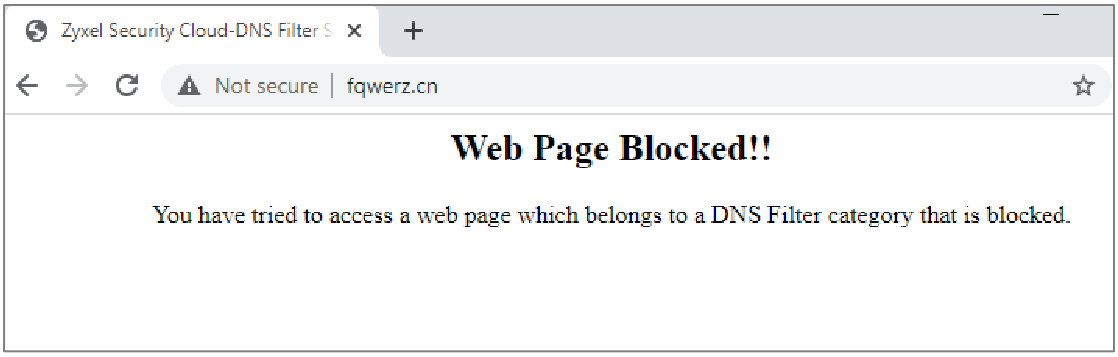
Message

DNS Filter Result: Malicious Sites
DNS Filter DB: Not Found

Test Domain Name Category

Domain name to test: fqwerz.cn

Using Web Browser to access the malicious site. The gateway will redirect you to blocked page.

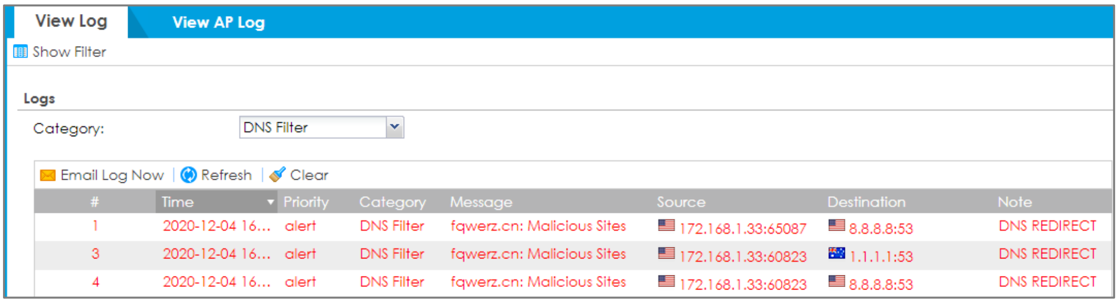


Web Page Blocked!!

You have tried to access a web page which belongs to a DNS Filter category that is blocked.

Go to **Monitor**>**Log**, select DNS Filter category.

Log message will be appeared after the profile of DNS Filter be hit.



Logs

Category: DNS Filter

#	Time	Priority	Category	Message	Source	Destination	Note
1	2020-12-04 16...	alert	DNS Filter	fqwerz.cn: Malicious Sites	172.168.1.33:65087	8.8.8.8:53	DNS REDIRECT
3	2020-12-04 16...	alert	DNS Filter	fqwerz.cn: Malicious Sites	172.168.1.33:60823	1.1.1.1:53	DNS REDIRECT
4	2020-12-04 16...	alert	DNS Filter	fqwerz.cn: Malicious Sites	172.168.1.33:60823	8.8.8.8:53	DNS REDIRECT

What Could Go Wrong?

1. If DNS Filter is not working, there are two possible reasons:

   You have not subscribed for the **DNS Filter** service.

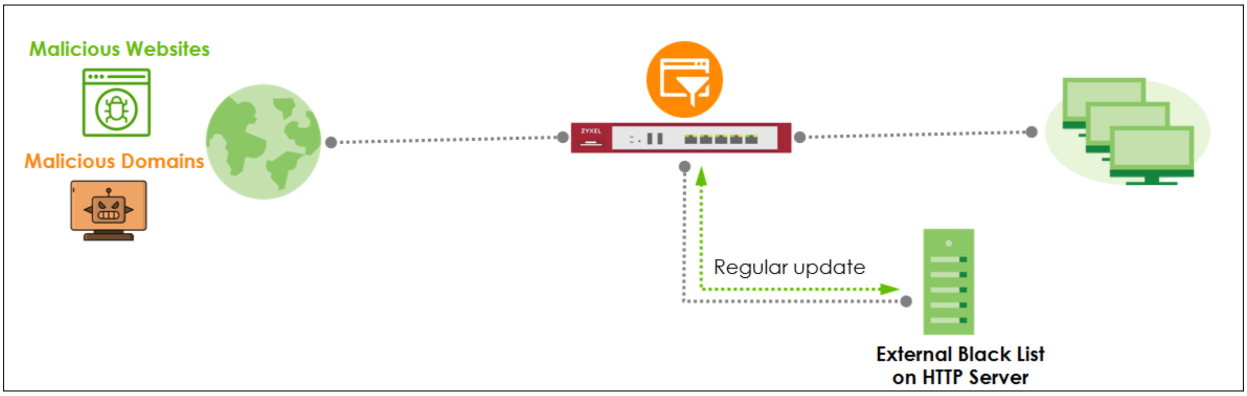
   You have subscribed for the **DNS Filter** service but the license (**Gold Security Pack Standard**) is expired.

2. You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com from the portal page (https://portal.myzyxel.com/) to register or extend your **Gold Security Pack Standard** license.

How to customize external block list in Reputation Filter

Reputation Filter function support importing customize block list from external server. You can configure system update block list by schedule automatically.
You can list unsafe WebSite or IP address as multiple ".txt" files on your HTTP server. It can easily and quickly to deploy the lists to multiple devices in the same time.

In this scenario will guide you how to configure ".txt" file manually and check behavior after connection is dropped successfully.



Configure Block list in .txt file

IP Reputation format

1.1.1.1 (IPv4 Single Host)

1.1.1.0/24 (IPv4 CIDR)

1.1.1.10-1.1.1.20 (IPv4 Range)

2001:0DB8:02de:0000:0000:0000:0000:0e13 (IPv6 Single Host)

2001:DB8:2de::e14/32 (IPv6 CIDR)

URL Threat Filter format

https://example.com (URL)

www.example.com (Hostname)

example.com (Domain name)

*.example.com (Wildcard domain name)

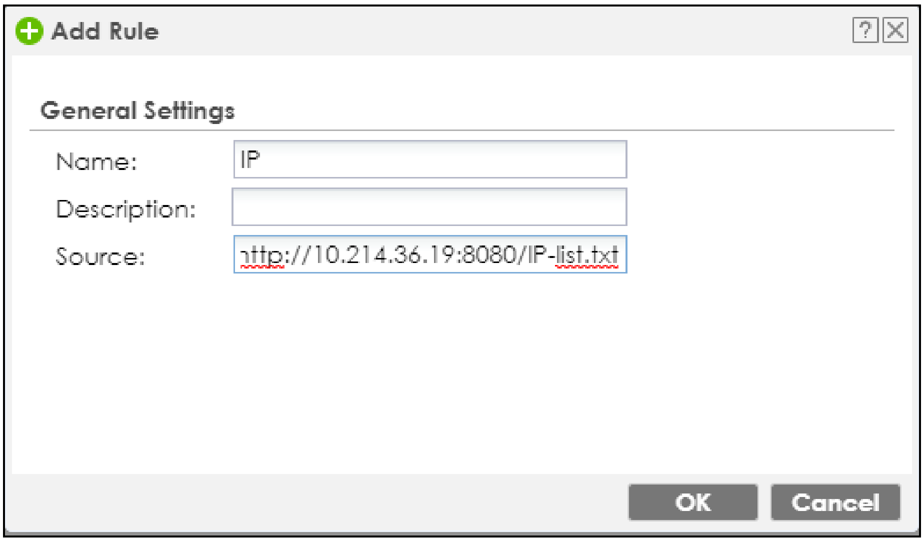
After configured list completely, you can save your .txt file on your HTTP server. (e.g. Software: HTTP File Server)

Configure External Block list setting

IP Reputation

Go to Configuration > Security Service > Reputation Filter > IP Reputation > External Black List.

Click Add button to download source on your HTTP Server.



Add Rule

General Settings

Name: IP

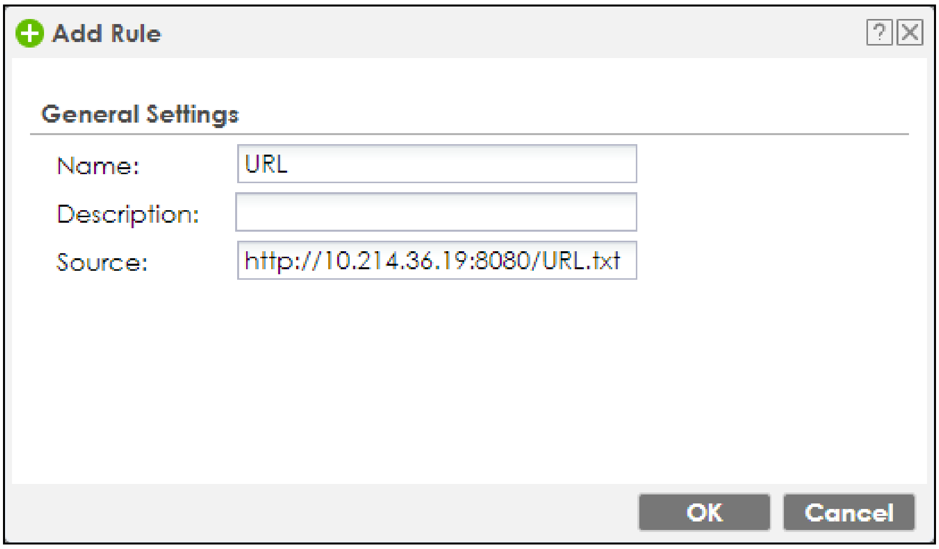
Description:

Source: http://10.214.36.19:8080/IP-list.txt

URL Threat Filter

Go to Configuration > Security Service > Reputation Filter > URL Threat Filter > External Black List.

Click Add button to download source on your HTTP Server.



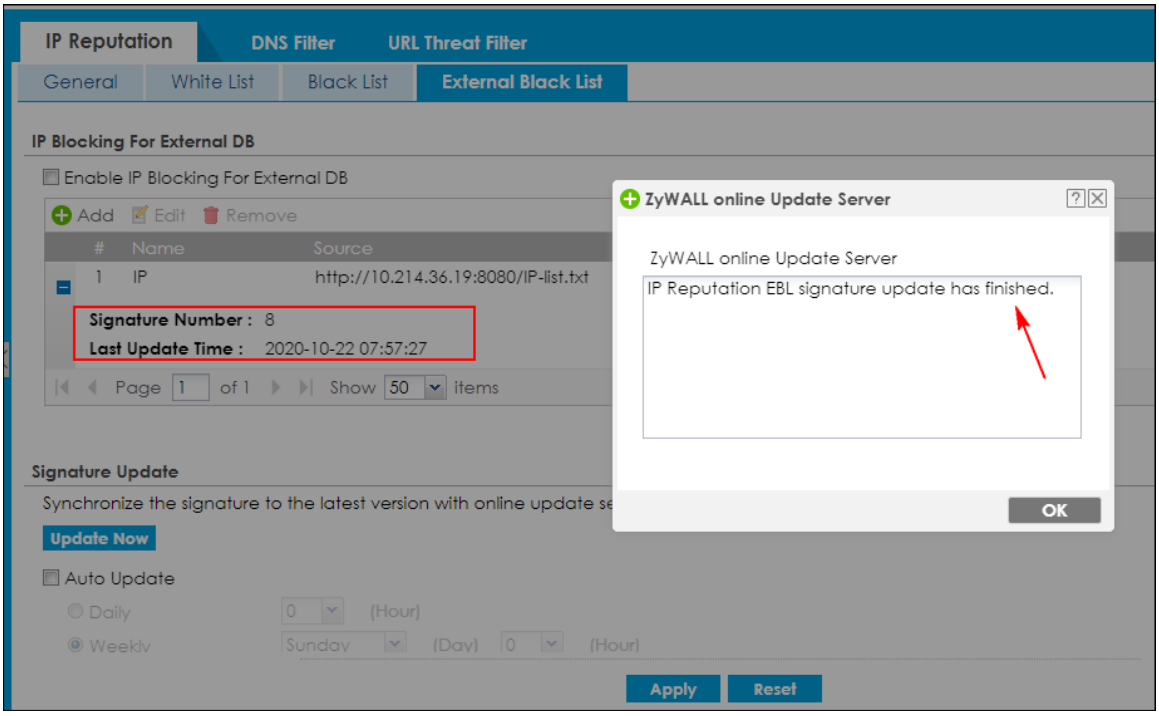
Name: URL

Description:

Source: http://10.214.36.19:8080/URL.txt

Check External Block List update status

IP Reputation



IP Blocking For External DB

□ Enable IP Blocking For External DB

#	Name	Source
1	IP	http://10.214.36.19:8080/IP-list.txt

Signature Number : 8

Last Update Time : 2020-10-22 07:57:27

Page 1 of 1 Show 50 items

Signature Update

Synchronize the signature to the latest version with online update se

□ Auto Update

○ Daily 0 (Hour)

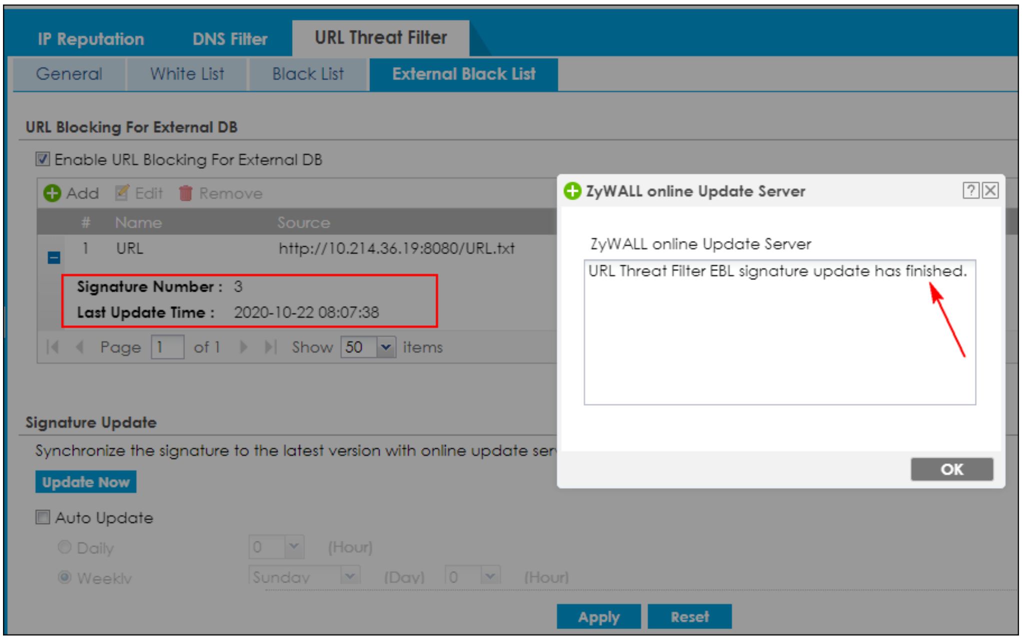
● Weekly Sunday (Day) 0 (Hour)

ZyWALL online Update Server

ZyWALL online Update Server

IP Reputation EBL signature update has finished.

URL Threat Filter



URL Blocking For External DB

☑ Enable URL Blocking For External DB

#	Name	Source
1	URL	http://10.214.36.19:8080/URL.txt

Signature Number : 3

Last Update Time : 2020-10-22 08:07:38

Page 1 of 1 Show 50 items

Signature Update

Synchronize the signature to the latest version with online update ser

□ Auto Update

○ Daily 0 (Hour)

● Weekly Sunday (Day) 0 (Hour)

ZyWALL online Update Server

ZyWALL online Update Server

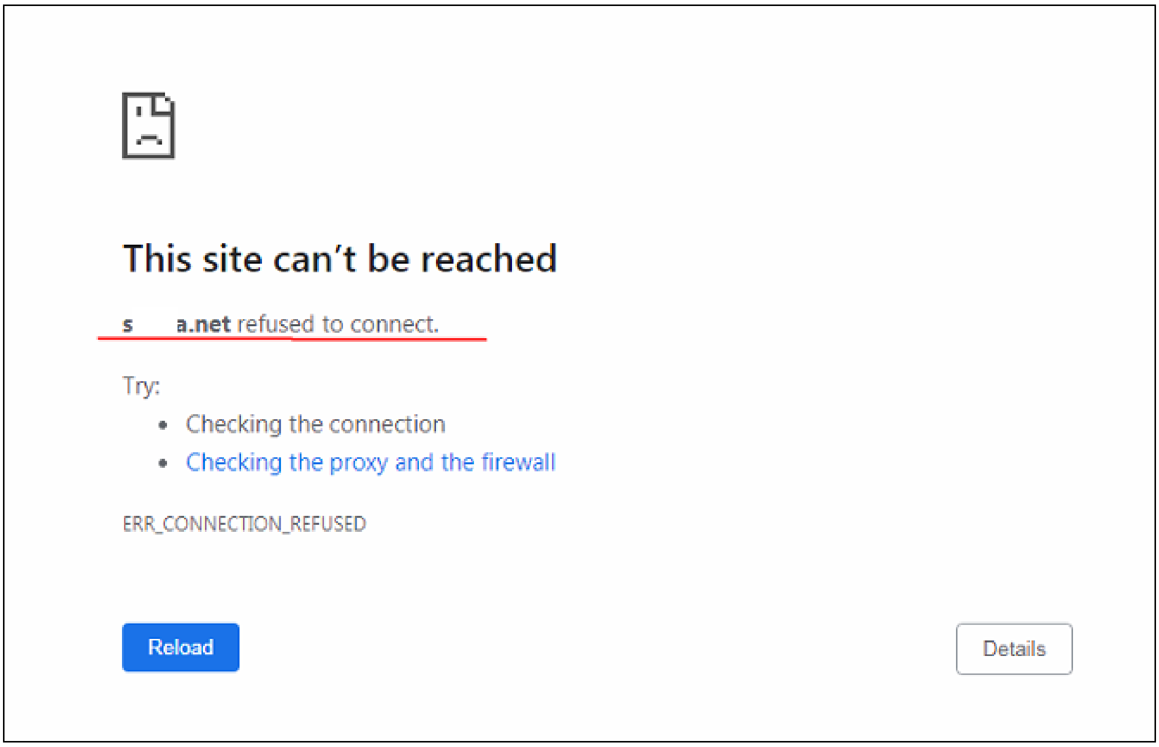
URL Threat Filter EBL signature update has finished.

Note: Please must make sure **block list format** in your ".txt" file correct. Otherwise the data will unable import to system completely. You can check "**Signature Number**" if amount is the same as your list.

Verification

IP Reputation block page

If client traffic is blocked by IP Reputation, website will unable to access to will display it.



This site can’t be reached

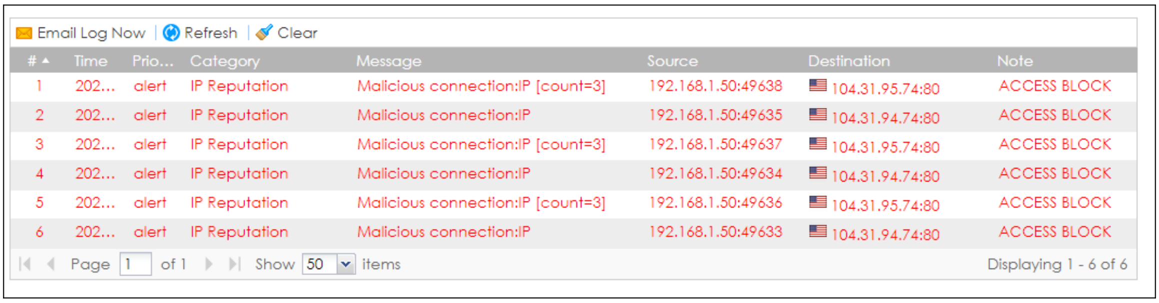
s a.net refused to connect.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_REFUSED

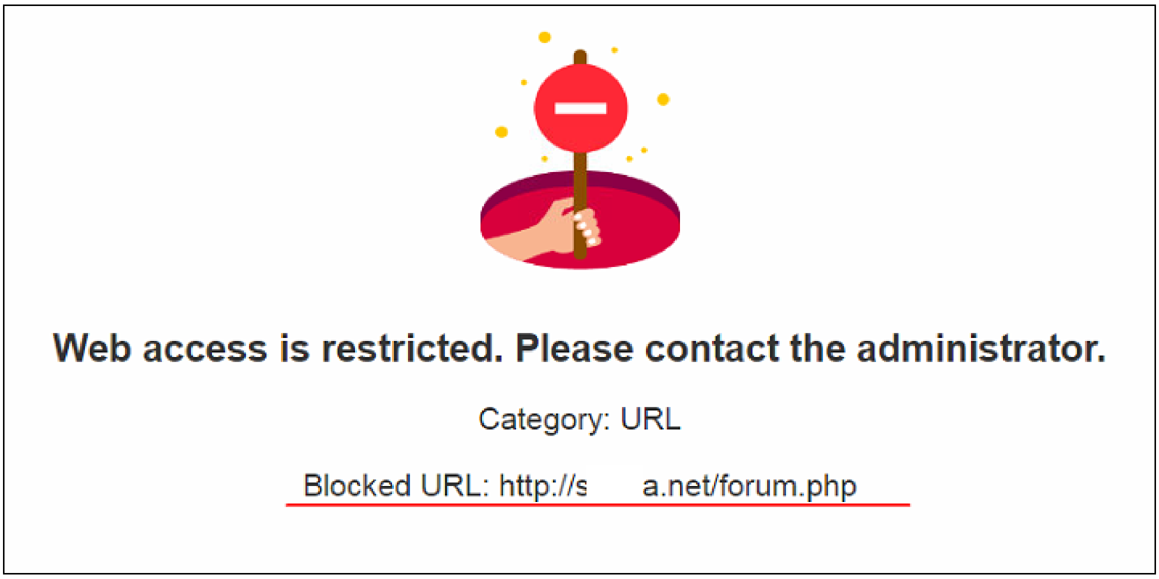
IP Reputation Log



# ▲	Time	Prio...	Category	Message	Source	Destination	Note
1	202...	alert	IP Reputation	Malicious connection:IP [count=3]	192.168.1.50:49638	104.31.95.74:80	ACCESS BLOCK
2	202...	alert	IP Reputation	Malicious connection:IP	192.168.1.50:49635	104.31.94.74:80	ACCESS BLOCK
3	202...	alert	IP Reputation	Malicious connection:IP [count=3]	192.168.1.50:49637	104.31.95.74:80	ACCESS BLOCK
4	202...	alert	IP Reputation	Malicious connection:IP	192.168.1.50:49634	104.31.94.74:80	ACCESS BLOCK
5	202...	alert	IP Reputation	Malicious connection:IP [count=3]	192.168.1.50:49636	104.31.95.74:80	ACCESS BLOCK
6	202...	alert	IP Reputation	Malicious connection:IP	192.168.1.50:49633	104.31.94.74:80	ACCESS BLOCK

URL Threat Filter

If client traffic is blocked by URL Threat Filter, website will unable to access to will display it.

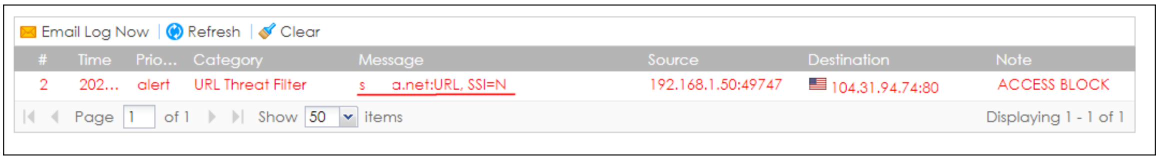


Web access is restricted. Please contact the administrator.

Category: URL

Blocked URL: http://s a.net/forum.php

URL Threat Filter Log



#	Time	Prio...	Category	Message	Source	Destination	Note
2	202...	alert	URL Threat Filter	s a.net:URL, SSI=N	192.168.1.50:49747	104.31.94.74:80	ACCESS BLOCK

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

What Can Go Wrong

1. Must make sure IP/FDQN format in Block List file. Otherwise system will stop to import data into system.
2. Must make sure your HTTP server is reachable from device.
3. If destination server working in HTTPS, Block page may only display certificate error.

How to Configure DNS Content Filter (On-Premises)

There are more browser support and users are encouraged to switch to TLS 1.3 because of its increased security, but websites using TLS 1.3 may not be categorized by URL content filtering without SSL inspection. For that, we need a solution to have early check on categorizations by DNS query instead. Compared to traditional content filter, DNS content filter is a stronger tool for SMB(s), because it can restrict the number of attacks faced by network access, thereby helping to reduce the remediation workload of IT professionals. Effective DNS content filter can even prevent up to 88% of Internet-spread malware.

DNS content filter intercept DNS request from client, check the domain name category and takes a corresponding action, reducing the risk of phishing attacks, and obfuscate source IPs using hijacked domain names. Fully customizable blacklist to ban access to any unwanted domains and prevent reaching those known domains hosting malicious content.
In this scenario, gateway works in on-premises mode, we configure DNS Content Filter via device Web GUI to block users in the local network to access the social networking site such as Facebook.

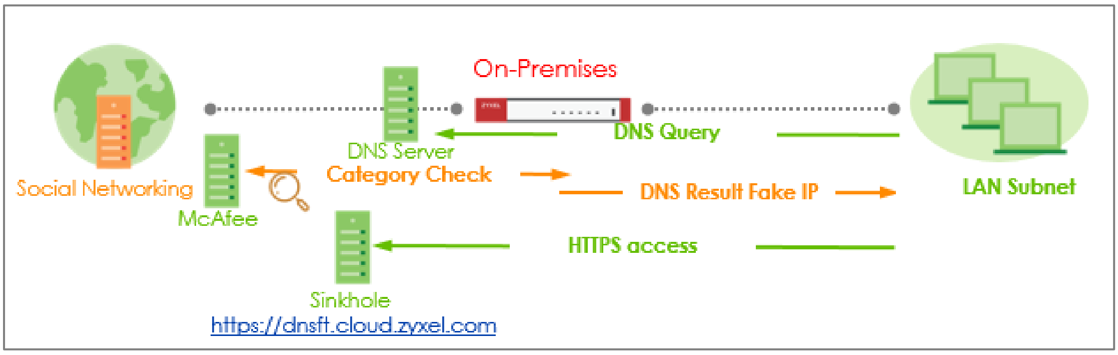


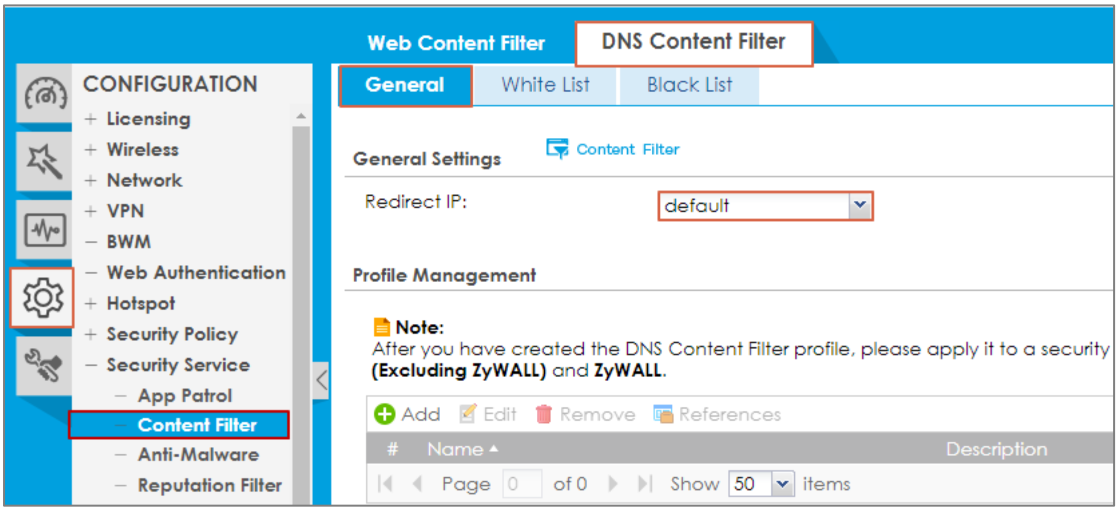
Figure: DNS Content Filter protects user to inappropriate website

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG Flex 500 (Firmware Version: ZLD 5.00).

Set Up the DNS Content Filter on USG Flex Series

In the USG Flex Web GUI, go to **Configuration** > **Security Service**> **Content Filter**>**DNS Content Filter**; Select Redirect IP to indicated IP address or default one. If user selects the default, when client hit DNS Content Filter profile, the page will be redirect to block page http://dnsft.cloud.zyxel.com/.

If user selects the custom defined, the page will be redirect indicated IP address.



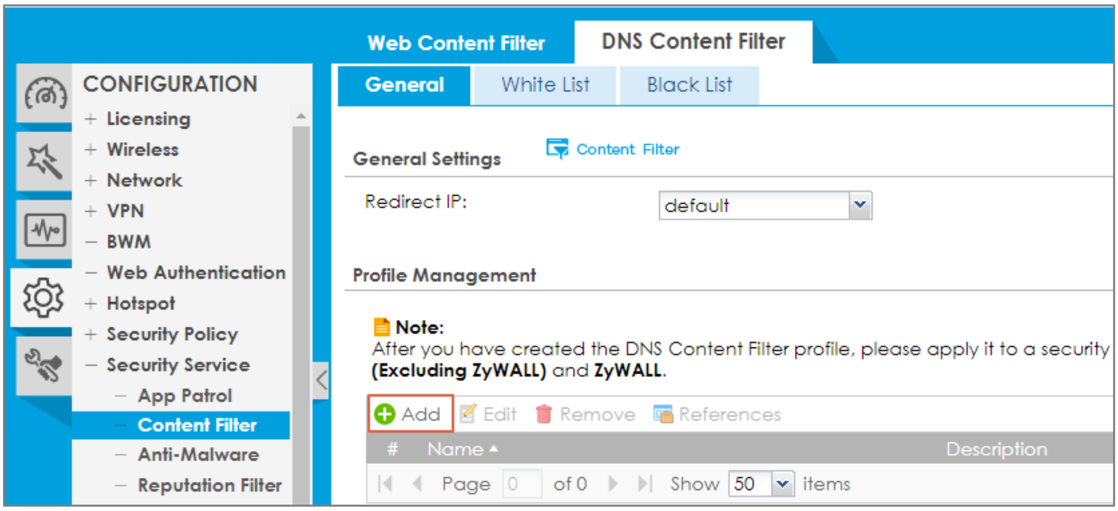
General Settings

Redirect IP: default

Profile Management

Note:
After you have created the DNS Content Filter profile, please apply it to a security
(Excluding ZyWALL) and **ZyWALL**.

Add profile on the general page. Select **Redirect** on action field, and choose **Log** on log field. Click **Social Networking**(as Example) on managed categories.

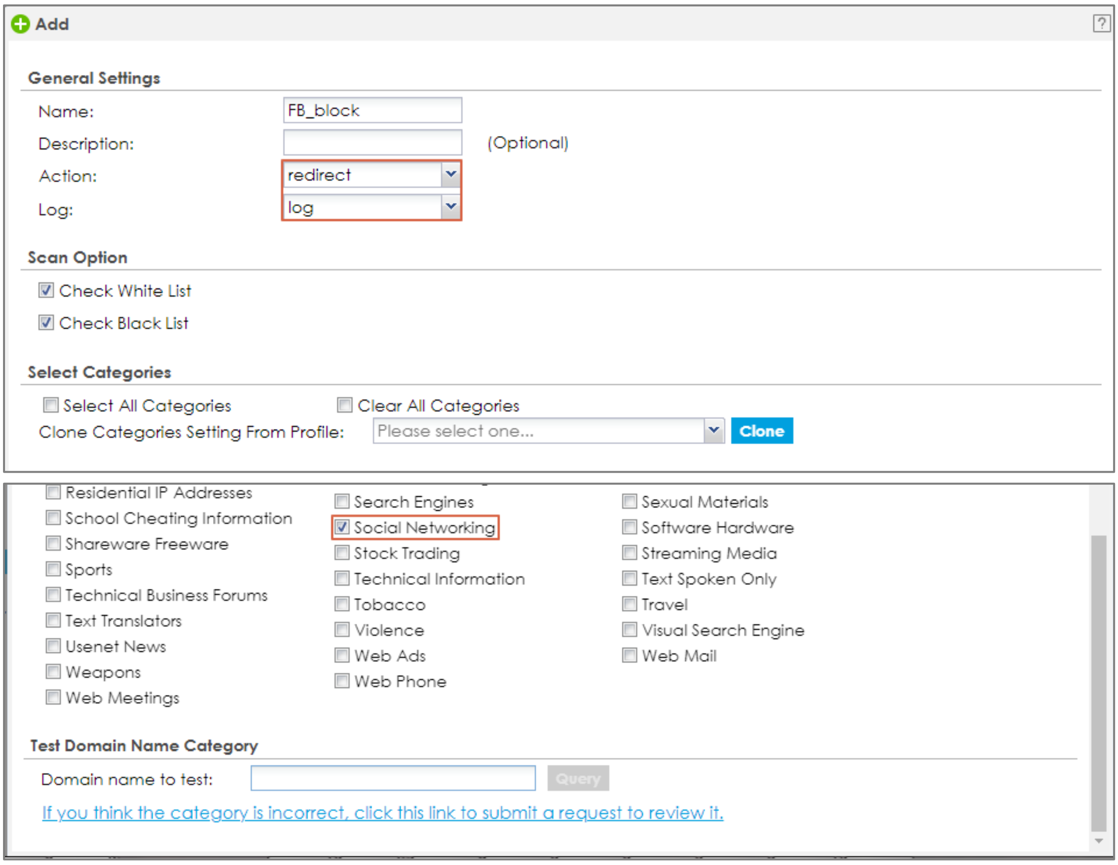


General Settings

Redirect IP: default

Profile Management

Note:
After you have created the DNS Content Filter profile, please apply it to a security
(Excluding ZyWALL) and **ZyWALL**.



Add

General Settings

Name: FB_block

Description: (Optional)

Action: redirect

Log: log

Scan Option

☑ Check White List

☑ Check Black List

Select Categories

□ Select All Categories □ Clear All Categories

Clone Categories Setting From Profile: Please select one... Clone

□ Residential IP Addresses
□ School Cheating Information
□ Shareware Freeware
□ Sports
□ Technical Business Forums
□ Text Translators
□ Usenet News
□ Weapons
□ Web Meetings

□ Search Engines
☑ Social Networking
□ Stock Trading
□ Technical Information
□ Tobacco
□ Violence
□ Web Ads
□ Web Phone

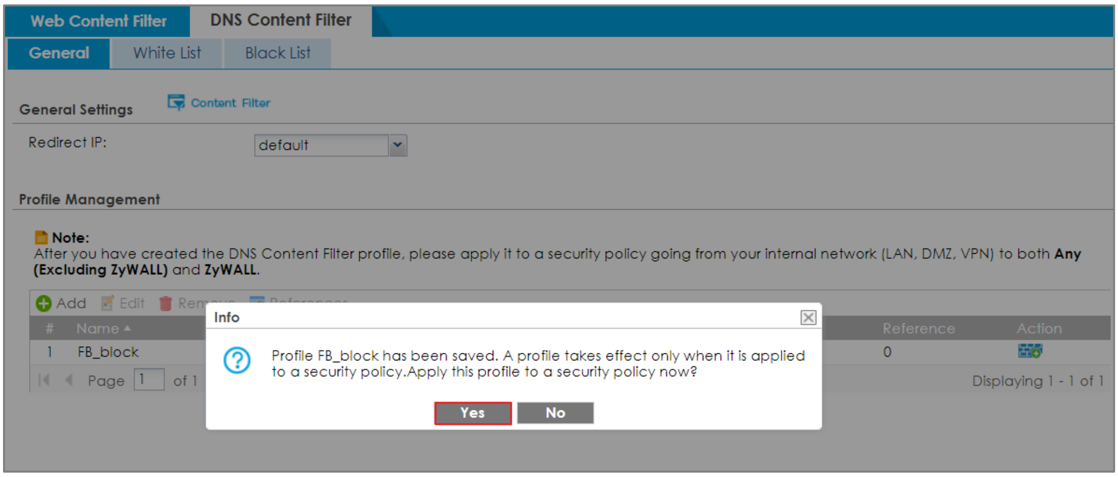
□ Sexual Materials
□ Software Hardware
□ Streaming Media
□ Text Spoken Only
□ Travel
□ Visual Search Engine
□ Web Mail

Test Domain Name Category

Domain name to test: Query

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

Once the DNS Content Filter profile is created, a windows shows up to instruct you to apply this profile to security policy. Click **Yes** to continue



Web Content Filter | DNS Content Filter

General | White List | Black List

General Settings Content Filter

Redirect IP: default

Profile Management

Note:
After you have created the DNS Content Filter profile, please apply it to a security policy going from your internal network (LAN, DMZ, VPN) to both **Any (Excluding ZyWALL)** and **ZyWALL**.

Add Edit Remove References

#	Name ▲	Reference	Action
1	FB_block	0	

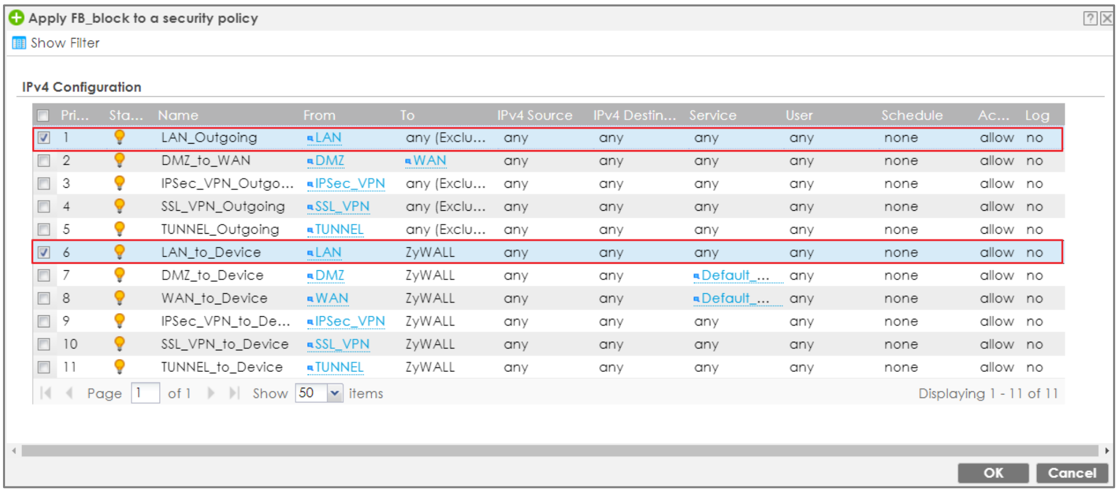
Page 1 of 1 Displaying 1 - 1 of 1

Info

Profile FB_block has been saved. A profile takes effect only when it is applied to a security policy.Apply this profile to a security policy now?

Yes No

Please apply this profile to a security policy going from your internal network to both **Any (Excluding ZyWALL)** and **ZyWALL**.



Apply FB_block to a security policy

Show Filter

IPv4 Configuration

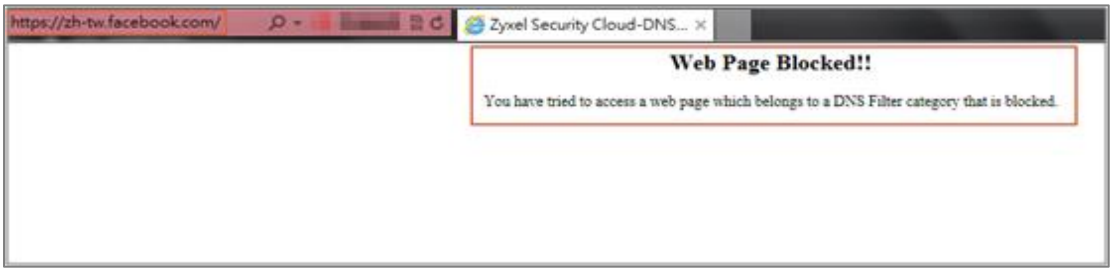
□	Pri...	Sta...	Name	From	To	IPv4 Source	IPv4 Destin...	Service	User	Schedule	Ac...	Log
☑	1	💡	LAN_Outgoing	LAN	any (Exclu...	any	any	any	any	none	allow	no
□	2	💡	DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	allow	no
□	3	💡	IPSec_VPN_Outgo...	IPSec_VPN	any (Exclu...	any	any	any	any	none	allow	no
□	4	💡	SSL_VPN_Outgoing	SSL_VPN	any (Exclu...	any	any	any	any	none	allow	no
□	5	💡	TUNNEL_Outgoing	TUNNEL	any (Exclu...	any	any	any	any	none	allow	no
☑	6	💡	LAN_to_Device	LAN	ZyWALL	any	any	any	any	none	allow	no
□	7	💡	DMZ_to_Device	DMZ	ZyWALL	any	any	Default_...	any	none	allow	no
□	8	💡	WAN_to_Device	WAN	ZyWALL	any	any	Default_...	any	none	allow	no
□	9	💡	IPSec_VPN_to_De...	IPSec_VPN	ZyWALL	any	any	any	any	none	allow	no
□	10	💡	SSL_VPN_to_Device	SSL_VPN	ZyWALL	any	any	any	any	none	allow	no
□	11	💡	TUNNEL_to_Device	TUNNEL	ZyWALL	any	any	any	any	none	allow	no

Page 1 of 1 Show 50 items Displaying 1 - 11 of 11

OK Cancel

Test the Result

When you access Facebook.com which is in Social Networking Category, the Web Access will be redirected to block page.



https://zh-tw.facebook.com/

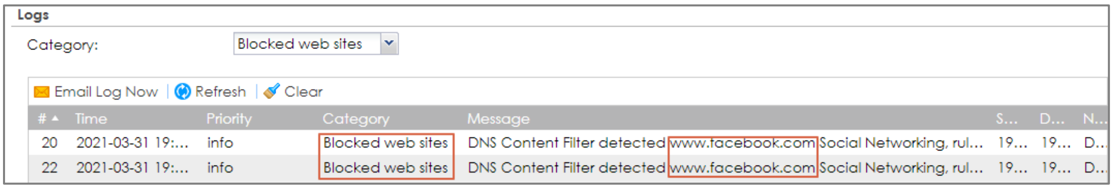
Zyxel Security Cloud-DNS...

Web Page Blocked!!

You have tried to access a web page which belongs to a DNS Filter category that is blocked.

Go to **Monitor**>**Log**,

Log message will show DNS Content Filter detect www.facebook.com (Blocked) after the profile of DNS Content Filter be hit.



Logs

Category: Blocked web sites

Email Log Now | Refresh | Clear

# ▲	Time	Priority	Category	Message			S...	D...	N...
20	2021-03-31 19:...	info	Blocked web sites	DNS Content Filter detected	www.facebook.com	Social Networking, rul...	19...	19...	D...
22	2021-03-31 19:...	info	Blocked web sites	DNS Content Filter detected	www.facebook.com	Social Networking, rul...	19...	19...	D...

What Could Go Wrong?

1. If DNS Content Filter is not working, there are two possible reasons:

You have not subscribed for the **Web Filtering** service.

You have subscribed for the **Web Filtering** service but the license is expired.

2. You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com from the portal page (https://portal.myzyxel.com/) to register or extend your **Web Filtering** license.

How to Configure DNS Content Filter (On-Cloud)

In this scenario, the gateway is managed by Nebula. The example shows you how to configure DNS content filtering on Nebula portal to block the social networking site such as Facebook.

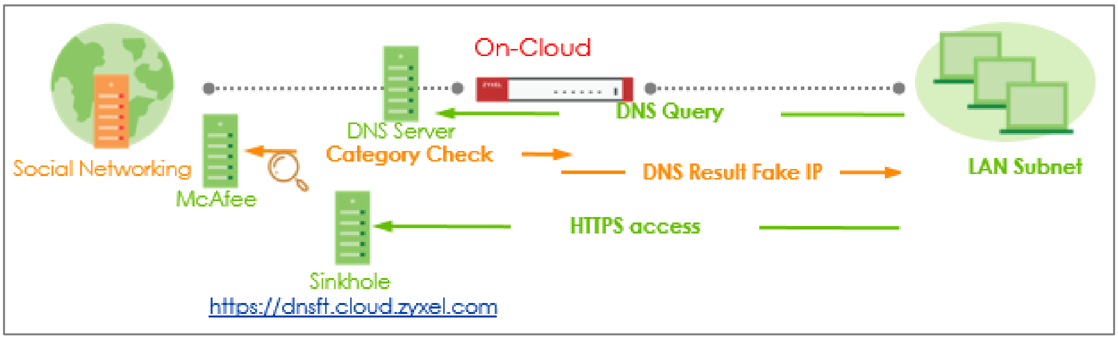


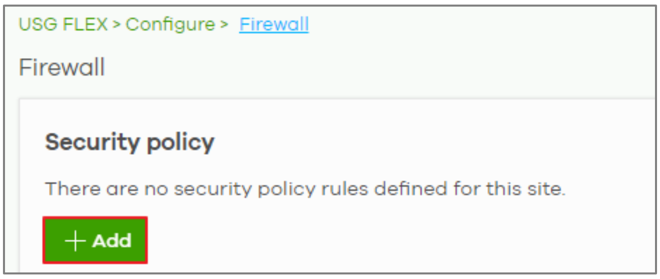
Figure: DNS Content Filter protects user to inappropriate website

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG Flex 500 (Firmware Version: ZLD 5.00).

Set Up the DNS Content Filter on Nebula

Make sure your gateway has been managed by Nebula. Log in Nebula Control Center with your myZyxel account, select the organization and site you want to manage. Go to **USG Flex**> **Configure** > **Firewall**

In **Security policy**, click **Add** to create a new rule



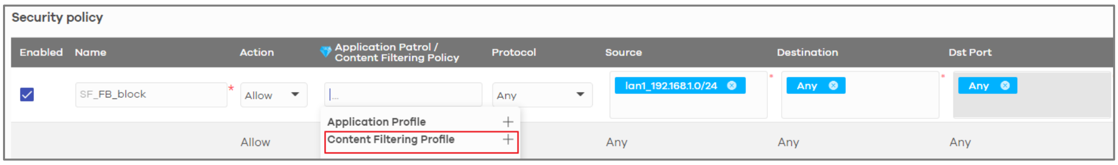
USG FLEX > Configure > Firewall

Firewall

Security policy

There are no security policy rules defined for this site.

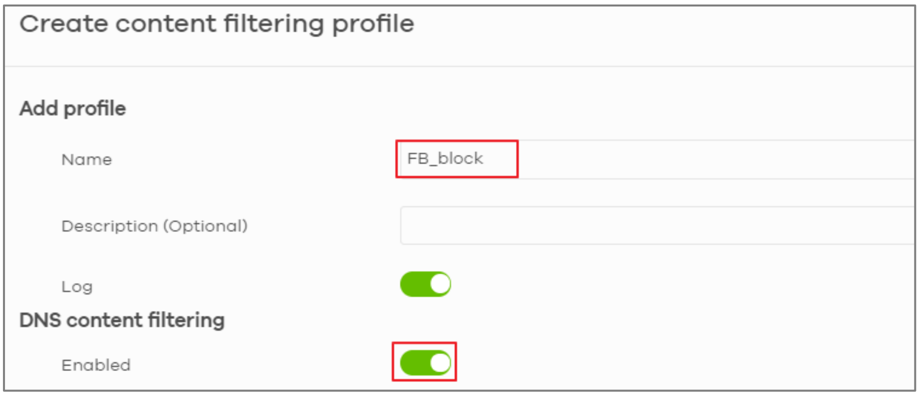
Name the rule, select Allow in **Action**, Lan1 in **Source**, Any in **Destination** field. In **Application Patrol / Content Filtering Policy** field, click [+] to add a new Content Filter profile



Security policy

Enabled	Name	Action	Application Patrol / Content Filtering Policy	Protocol	Source	Destination	Dst Port
☑	SF_FB_block	Allow		Any	lan1_192.168.1.0/24	Any	Any
		Allow			Any	Any	Any

The DNS content filtering is a part of Content filtering feature, name the profile, scroll down, then enable DNS content filtering



Create content filtering profile

Add profile

Name: FB_block

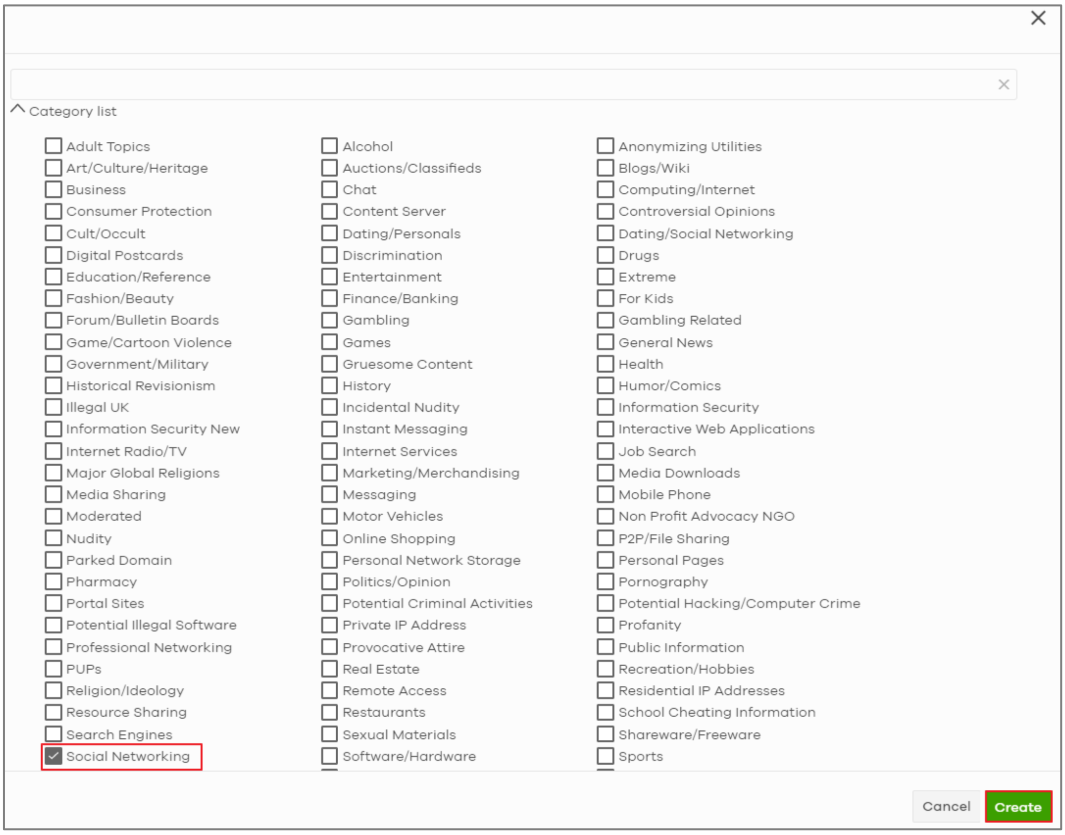
Description (Optional):

Log: on

DNS content filtering

Enabled: on

Click the **category list,** select **Social Networking**, then press **Create** button



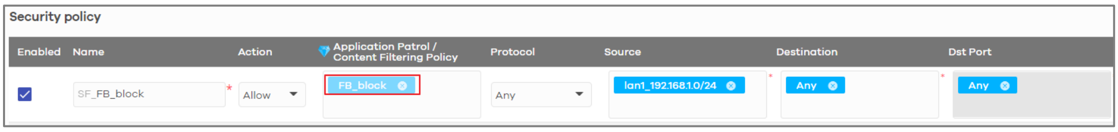
Category list

□ Adult Topics
□ Art/Culture/Heritage
□ Business
□ Consumer Protection
□ Cult/Occult
□ Digital Postcards
□ Education/Reference
□ Fashion/Beauty
□ Forum/Bulletin Boards
□ Game/Cartoon Violence
□ Government/Military
□ Historical Revisionism
□ Illegal UK
□ Information Security New
□ Internet Radio/TV
□ Major Global Religions
□ Media Sharing
□ Moderated
□ Nudity
□ Parked Domain
□ Pharmacy
□ Portal Sites
□ Potential Illegal Software
□ Professional Networking
□ PUPs
□ Religion/Ideology
□ Resource Sharing
□ Search Engines
☑ Social Networking

□ Alcohol
□ Auctions/Classifieds
□ Chat
□ Content Server
□ Dating/Personals
□ Discrimination
□ Entertainment
□ Finance/Banking
□ Gambling
□ Games
□ Gruesome Content
□ History
□ Incidental Nudity
□ Instant Messaging
□ Internet Services
□ Marketing/Merchandising
□ Messaging
□ Motor Vehicles
□ Online Shopping
□ Personal Network Storage
□ Politics/Opinion
□ Potential Criminal Activities
□ Private IP Address
□ Provocative Attire
□ Real Estate
□ Remote Access
□ Restaurants
□ Sexual Materials
□ Software/Hardware

□ Anonymizing Utilities
□ Blogs/Wiki
□ Computing/Internet
□ Controversial Opinions
□ Dating/Social Networking
□ Drugs
□ Extreme
□ For Kids
□ Gambling Related
□ General News
□ Health
□ Humor/Comics
□ Information Security
□ Interactive Web Applications
□ Job Search
□ Media Downloads
□ Mobile Phone
□ Non Profit Advocacy NGO
□ P2P/File Sharing
□ Personal Pages
□ Pornography
□ Potential Hacking/Computer Crime
□ Profanity
□ Public Information
□ Recreation/Hobbies
□ Residential IP Addresses
□ School Cheating Information
□ Shareware/Freeware
□ Sports

Make sure this profile is applied to the security policy

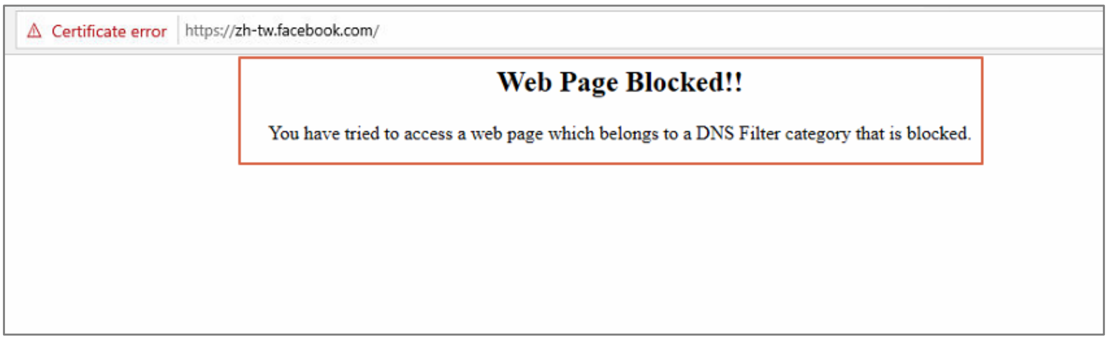


Security policy

Enabled	Name	Action	Application Patrol / Content Filtering Policy	Protocol	Source	Destination	Dst Port
☑	SF_FB_block *	Allow	FB_block	Any	lan1_192.168.1.0/24	Any	Any

Test the Result

The Facebook has been restricted from access from users under LAN1, the user will see the block page instead.

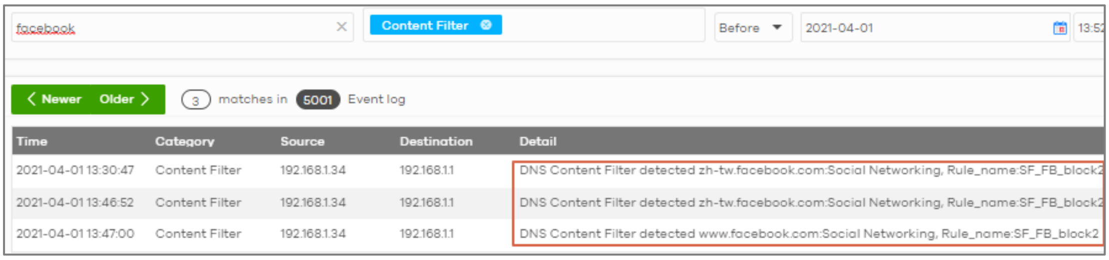


Certificate error https://zh-tw.facebook.com/

Web Page Blocked!!

You have tried to access a web page which belongs to a DNS Filter category that is blocked.

Go to the **Monitor**>**Even Log,** select the Content Filter category, Nebula will show the access to www.facebook.com has been blocked.



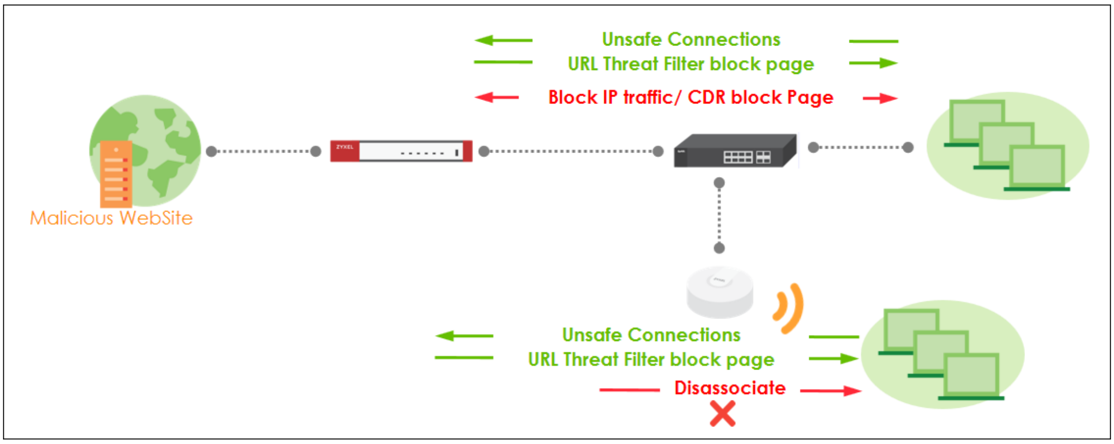
3 matches in 5001 Event log

Time	Category	Source	Destination	Detail
2021-04-01 13:30:47	Content Filter	192.168.1.34	192.168.1.1	DNS Content Filter detected zh-tw.facebook.com:Social Networking, Rule_name:SF_FB_block2
2021-04-01 13:46:52	Content Filter	192.168.1.34	192.168.1.1	DNS Content Filter detected zh-tw.facebook.com:Social Networking, Rule_name:SF_FB_block2
2021-04-01 13:47:00	Content Filter	192.168.1.34	192.168.1.1	DNS Content Filter detected www.facebook.com:Social Networking, Rule_name:SF_FB_block2

How to configure Collaborative Detection & Response to identify and quarantine compromised devices from your network

The IDP/ Anti-Malware/ URL Threat Filter services could block unsafe connections one by one. But it is unable to stop client initialing connection continually. It means the infected computer may connect to unsafe website continually or attacks Intranet devices.

Collaborative Detection & Response(CDR) now makes it easier for you to block compromised devices from your network. After you identify a device as compromised (for example, if a device has been infected with malware and is performing command and control actions), you can send alert to administrator, block or quarantine compromised devices from your network for a period time. CDR can collaborate managed AP to identify the compromised devices from the wireless network.


Unsafe Connections
URL Threat Filter block page
Block IP traffic/ CDR block Page
Malicious WebSite
Unsafe Connections
URL Threat Filter block page
Disassociate

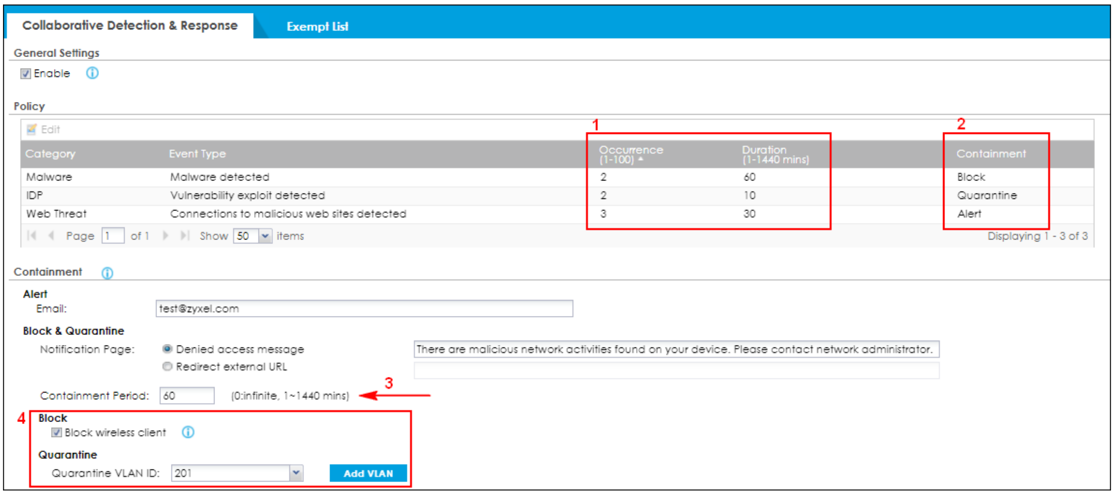
Note: In quarantine scenario, it can quarantine client to managed VLAN which has a third-party scanning server. The infected client can scan disk by third-party server or download required patch after quarantined.

Setup CDR configuration

Configuration > Security Service > CDR

You can threshold event violation rule for each security service category, and select the corresponding action: alert, block or quarantine.

1. Containment action.
2. Containment period time.
3. Collaborative managed AP setting.



General Settings

☑ Enable

Policy

Category	Event Type	Occurrence (1-100)	Duration (1-1440 mins)	Containment
Malware	Malware detected	2	60	Block
IDP	Vulnerability exploit detected	2	10	Quarantine
Web Threat	Connections to malicious web sites detected	3	30	Alert

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

Containment

Alert

Email: test@zyxel.com

Block & Quarantine

Notification Page: ● Denied access message ○ Redirect external URL

There are malicious network activities found on your device. Please contact network administrator.

Containment Period: 60 (0:infinite, 1~1440 mins)

Block

☑ Block wireless client

Quarantine

Quarantine VLAN ID: 201

CDR database include IDP, Anti-Malware and Web Threat Filter services. The current signature including those most critical variabilities:

IDP Signatures:

CVE-2019-0708(117760, 130797, 130801), CVE-2020-0796(130822,130823,130824,130825), 117723, 117724, 117726

Anti-Malware Signature:

All Signatures

URL Threat Filter Categories:

Browser Exploits, Malicious Downloads, Malicious Sites, Phishing

Note: CDR service is counting the event from supported UTM feature. So IDP, Anti-Malware, URL Threat Filter services have to enable.

You can threshold event violation rule by pre-configure the occurrence of event within a specific period. Once the client violates the threshold, gateway triggers the actions. There are 3 types of actions:

Alert:

CDR will Send alert mail when client violates threshold.

Block:

Wired Client: Block client IP traffic for a period time and show block page for client.

Wi-Fi Client: Client associate to AP. Gateway will Block client IP traffic for a period time and show block page.

If enabled **Block Wireless Client**: Managed AP will disassociate and block client by MAC address for a period time. Wireless client will unable connect to AP until containment period is countdown to 0.

Quarantine:

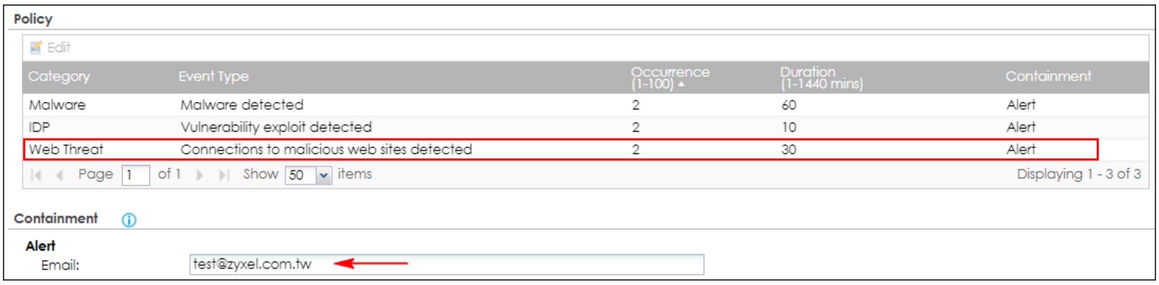
Wired Client: Block client IP traffic for a period time and show block page for client.

Wi-Fi Client: Managed AP will disassociate client. Client will quarantine to managed VLAN after re-associate with AP. And client IP traffic will block by gateway for a period time.

Verification

You can access to malicious website to verify behavior between different actions.

Alert:



Policy

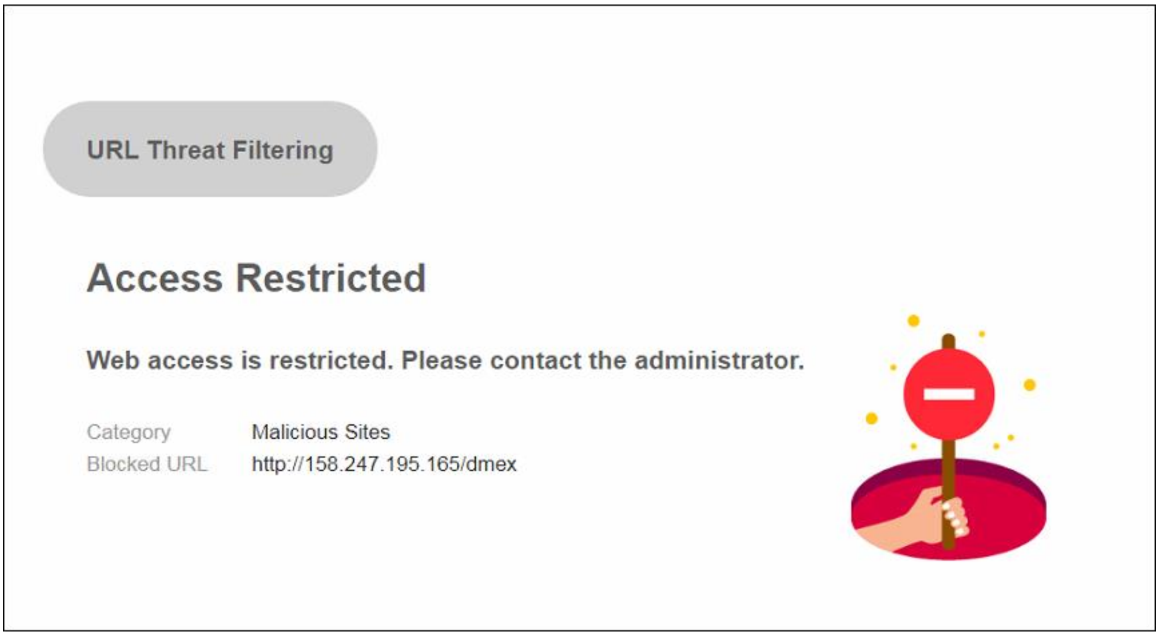
Category	Event Type	Occurrence (1-100) ▲	Duration (1-1440 mins)	Containment
Malware	Malware detected	2	60	Alert
IDP	Vulnerability exploit detected	2	10	Alert
Web Threat	Connections to malicious web sites detected	2	30	Alert

Containment

Alert

Email: test@zyxel.com.tw

If client access to malicious website. The connection will be detected by Web Threat Filter service. So browser will display Web Threat Filter page first.



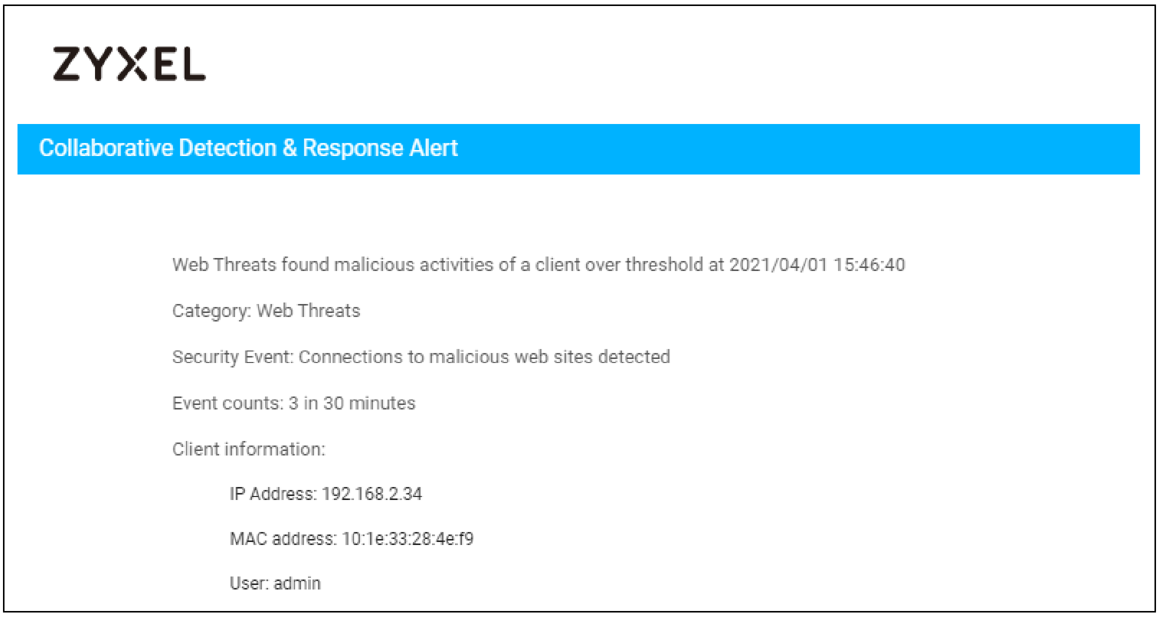
URL Threat Filtering

Access Restricted

Web access is restricted. Please contact the administrator.

Category	Malicious Sites
Blocked URL	http://158.247.195.165/dmex

After connection reaching to the threshold, it will trigger gateway send alert mail you configured.



ZYXEL

Collaborative Detection & Response Alert

Web Threats found malicious activities of a client over threshold at 2021/04/01 15:46:40

Category: Web Threats

Security Event: Connections to malicious web sites detected

Event counts: 3 in 30 minutes

Client information:

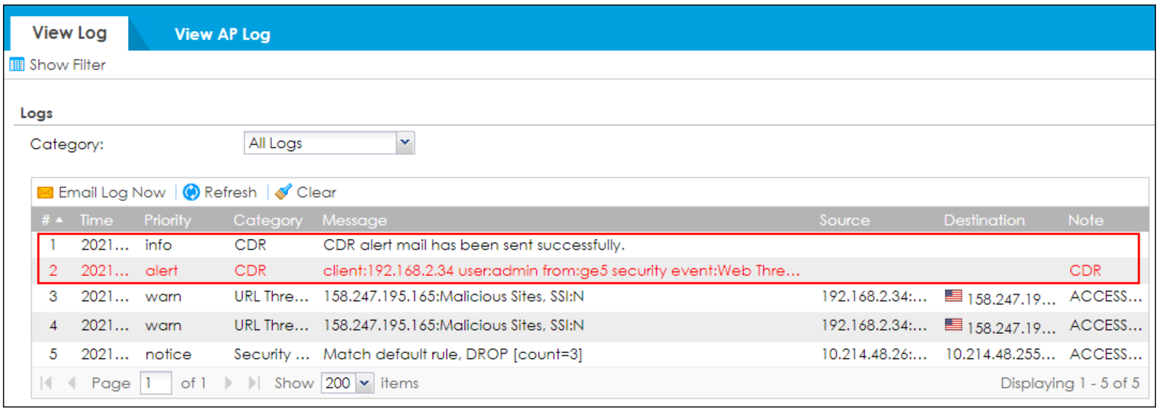
IP Address: 192.168.2.34

MAC address: 10:1e:33:28:4e:f9

User: admin

In mail, it will display CDR alert reason and client IP/MAC information.

And also, you can check system log



View Log | View AP Log

Show Filter

Logs

Category: All Logs

Email Log Now | Refresh | Clear

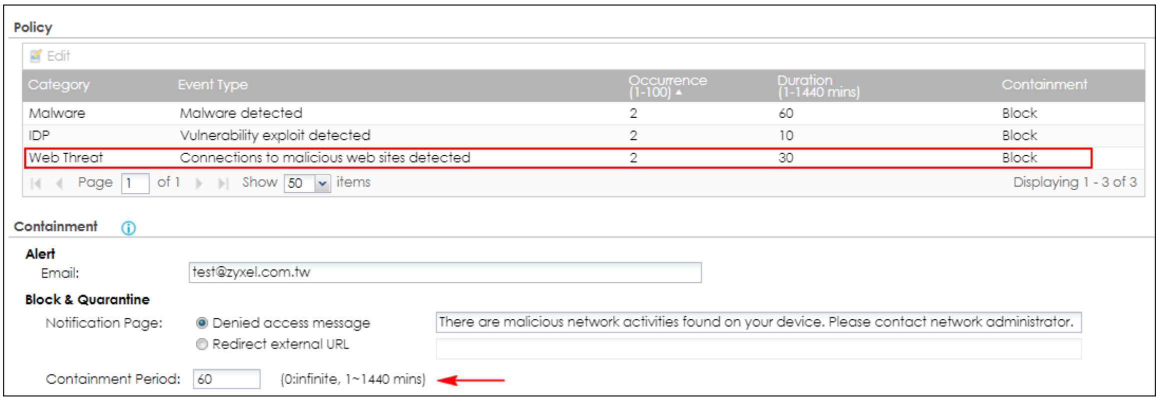
#	Time	Priority	Category	Message	Source	Destination	Note
1	2021...	info	CDR	CDR alert mail has been sent successfully.			
2	2021...	alert	CDR	client:192.168.2.34 user:admin from:ge5 security event:Web Thre...			CDR
3	2021...	warn	URL Thre...	158.247.195.165:Malicious Sites, SSI:N	192.168.2.34:...	158.247.19...	ACCESS...
4	2021...	warn	URL Thre...	158.247.195.165:Malicious Sites, SSI:N	192.168.2.34:...	158.247.19...	ACCESS...
5	2021...	notice	Security ...	Match default rule, DROP [count=3]	10.214.48.26:...	10.214.48.255...	ACCESS...

Page 1 of 1 Show 200 items Displaying 1 - 5 of 5

In system log, client traffic will block by Web Threat Filter first. If connection over threshold, it will trigger CDR to send email.

Note: If CDR is configured as “Alert”, CDR will only send alert mail without additional action, but client traffic still protected by others UTM services.

Block:



Policy

Edit

Category	Event Type	Occurrence (1-100)	Duration (1-1440 mins)	Containment
Malware	Malware detected	2	60	Block
IDP	Vulnerability exploit detected	2	10	Block
Web Threat	Connections to malicious web sites detected	2	30	Block

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

Containment

Alert

Email: test@zyxel.com.tw

Block & Quarantine

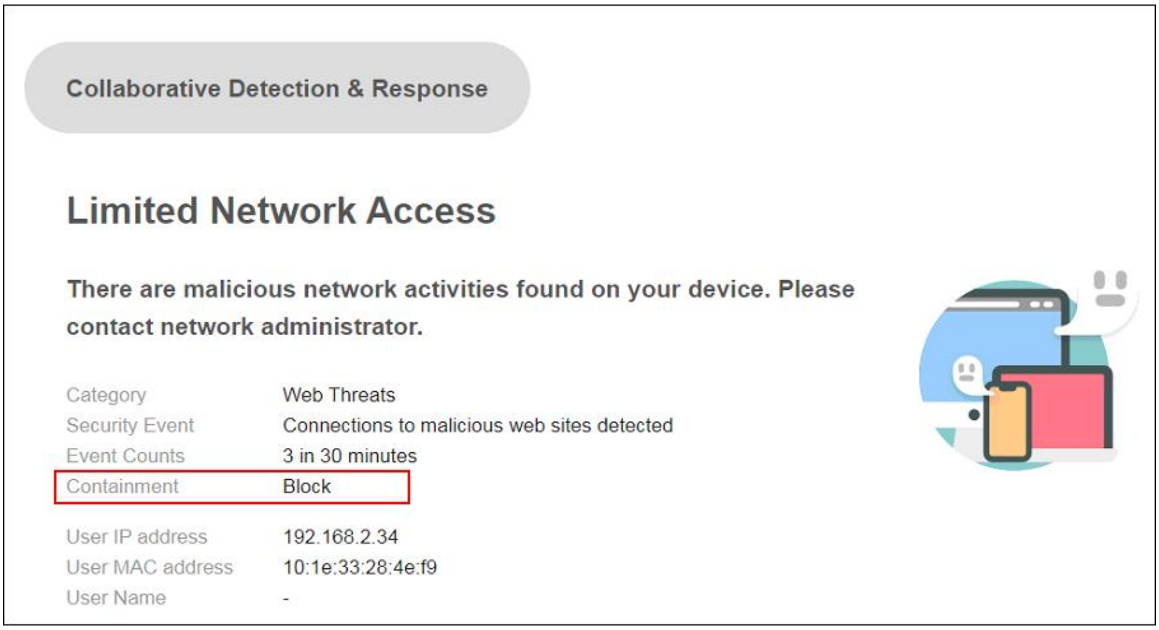
Notification Page: ● Denied access message ○ Redirect external URL

There are malicious network activities found on your device. Please contact network administrator.

Containment Period: 60 (0:infinite, 1~1440 mins)

If client accesses to malicious website. The connection will be detected by Web Threat Filter service. So browser will display block page of Web Threat Filter page first. When connection reaches threshold, then all of client IP traffic will be blocked by CDR function in a period time.

On client browser, it will display CDR block page.



Collaborative Detection & Response

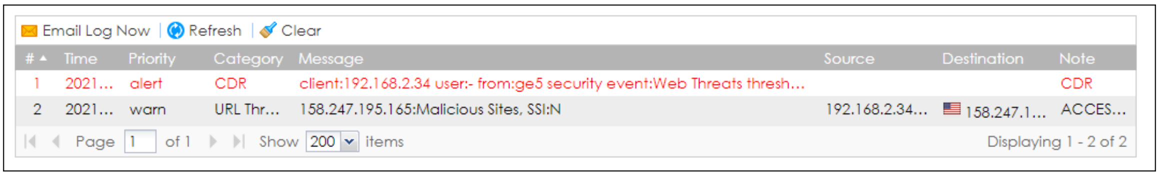
Limited Network Access

There are malicious network activities found on your device. Please contact network administrator.

Category	Web Threats
Security Event	Connections to malicious web sites detected
Event Counts	3 in 30 minutes
Containment	Block
User IP address	192.168.2.34
User MAC address	10:1e:33:28:4e:f9
User Name	-

In block page, it will show block reason and client IP/MAC information.

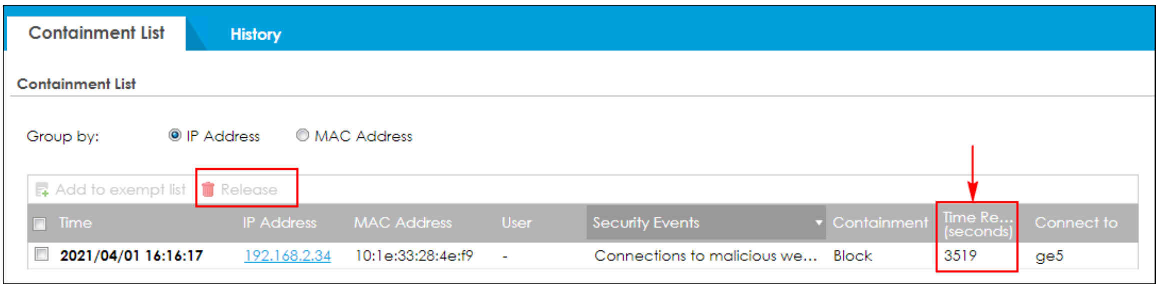
System log:



# ▲	Time	Priority	Category	Message	Source	Destination	Note
1	2021…	alert	CDR	client:192.168.2.34 user:- from:ge5 security event:Web Threats thresh…			CDR
2	2021…	warn	URL Thr…	158.247.195.165:Malicious Sites, SSI:N	192.168.2.34…	158.247.1…	ACCES…

You can also check containment list:

Monitor > Security Statistics > CDR

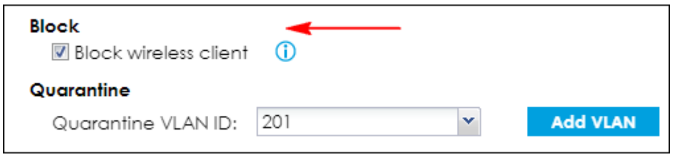


Group by: ● IP Address ○ MAC Address

□	Time	IP Address	MAC Address	User	Security Events	Containment	Time Re… (seconds)	Connect to
□	2021/04/01 16:16:17	192.168.2.34	10:1e:33:28:4e:f9	-	Connections to malicious we…	Block	3519	ge5

If client is blocked by CDR, client will be added into containment list. In this list, you can check the remaining time of block period. Client will be automatically released once the remaining time is countdown to 0. Or you can click release button to release client manually.

For wireless client. You can enable "Block Wireless client" checkbox to prevent the wireless client re-associates to the AP.

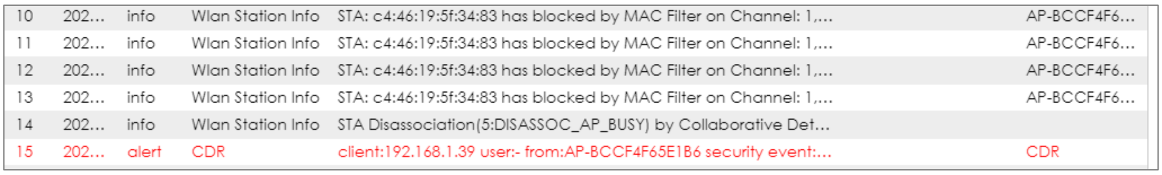


Block
☑ Block wireless client

Quarantine
Quarantine VLAN ID: 201

If wireless client connection reached threshold, managed AP will disassociate client and block client by MAC address. Then client will unable to connect to AP in block period.

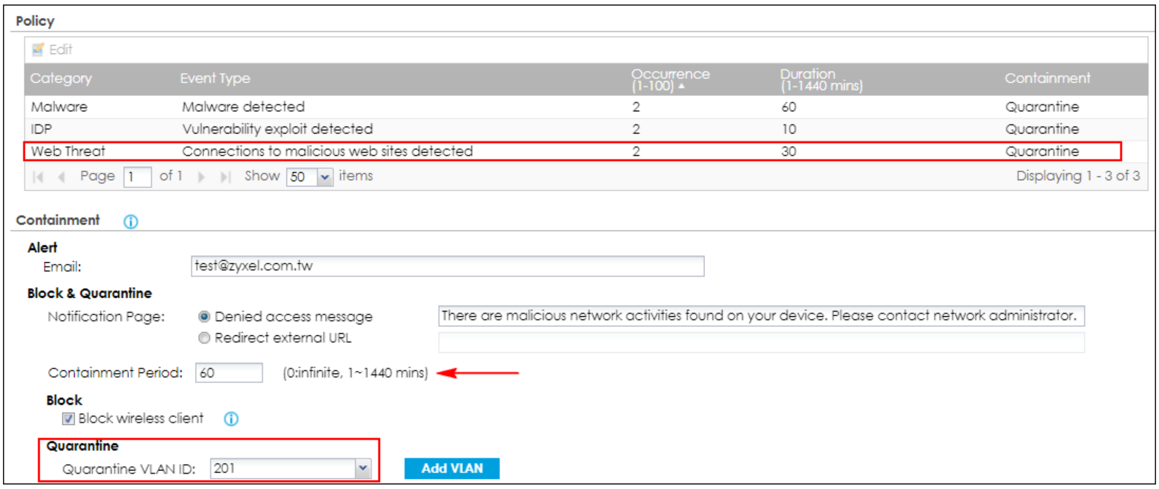
System log:



```
10   202...  info   Wlan Station Info   STA: c4:46:19:5f:34:83 has blocked by MAC Filter on Channel: 1,...        AP-BCCF4F6...
11   202...  info   Wlan Station Info   STA: c4:46:19:5f:34:83 has blocked by MAC Filter on Channel: 1,...        AP-BCCF4F6...
12   202...  info   Wlan Station Info   STA: c4:46:19:5f:34:83 has blocked by MAC Filter on Channel: 1,...        AP-BCCF4F6...
13   202...  info   Wlan Station Info   STA: c4:46:19:5f:34:83 has blocked by MAC Filter on Channel: 1,...        AP-BCCF4F6...
14   202...  info   Wlan Station Info   STA Disassociation(5:DISASSOC_AP_BUSY) by Collaborative Det...
15   202...  alert  CDR                 client:192.168.1.39 user:- from:AP-BCCF4F65E1B6 security event:...        CDR
```

Note: If "Block Wireless Client" checkbox is disabled, the wireless client still keep connection with AP but traffic is blocked by CDR.

Quarantine:



Policy

Category	Event Type	Occurrence (1-100)	Duration (1-1440 mins)	Containment
Malware	Malware detected	2	60	Quarantine
IDP	Vulnerability exploit detected	2	10	Quarantine
Web Threat	Connections to malicious web sites detected	2	30	Quarantine

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

Containment

Alert
Email: test@zyxel.com.tw

Block & Quarantine
Notification Page: ● Denied access message — There are malicious network activities found on your device. Please contact network administrator.
○ Redirect external URL

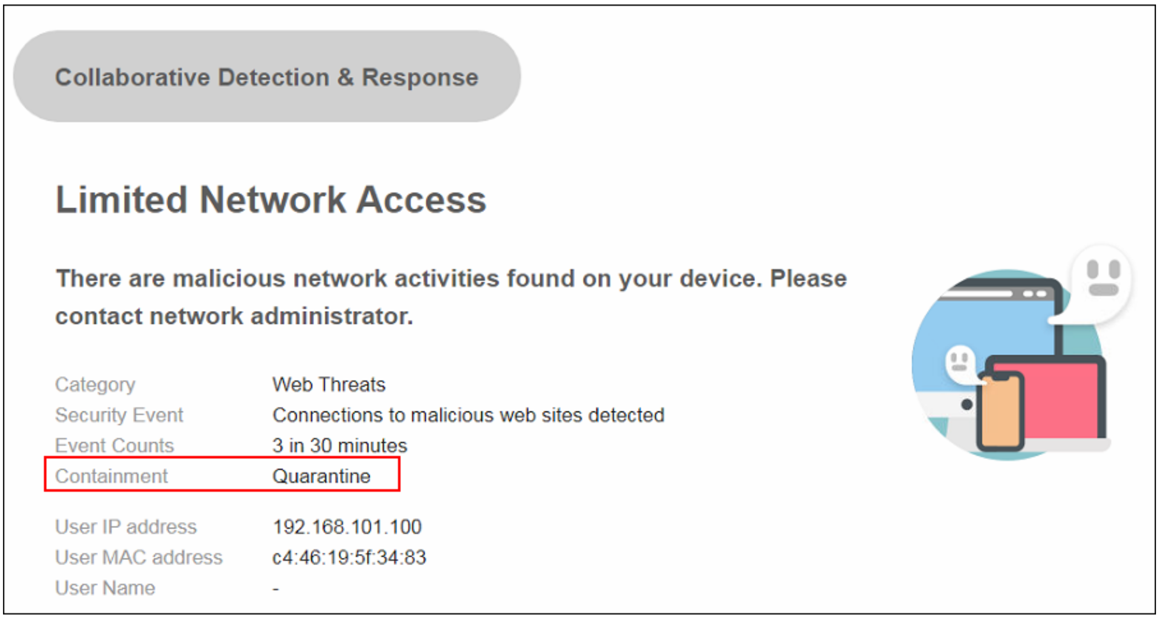
Containment Period: 60 (0:infinite, 1~1440 mins)

Block
☑ Block wireless client

Quarantine
Quarantine VLAN ID: 201

If client accesses to malicious website. The connection will be detected by Web Threat Filter service. So browser will display block page of Web Threat Filter page first. When connection reaches threshold, then all of client IP traffic will be blocked by CDR function in a period time.

On client browser, it will display CDR block page.



Collaborative Detection & Response

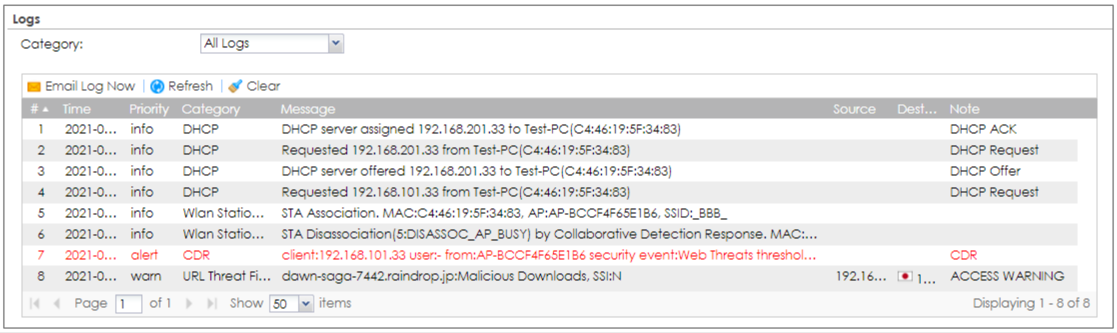
Limited Network Access

There are malicious network activities found on your device. Please contact network administrator.

Category	Web Threats
Security Event	Connections to malicious web sites detected
Event Counts	3 in 30 minutes
Containment	Quarantine
User IP address	192.168.101.100
User MAC address	c4:46:19:5f:34:83
User Name	-

For wireless client, managed AP will disassociate to client. Client will be quarantined to configured VLAN after associating again.

In system log, client will get quarantined VLAN after associating with AP.



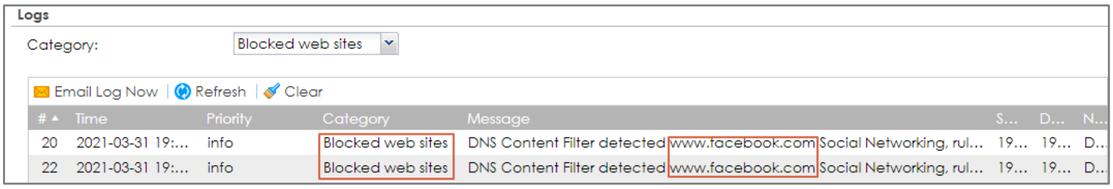
Logs

Category: All Logs

# ▲	Time	Priority	Category	Message	Source	Dest...	Note
1	2021-0...	info	DHCP	DHCP server assigned 192.168.201.33 to Test-PC(C4:46:19:5F:34:83)			DHCP ACK
2	2021-0...	info	DHCP	Requested 192.168.201.33 from Test-PC(C4:46:19:5F:34:83)			DHCP Request
3	2021-0...	info	DHCP	DHCP server offered 192.168.201.33 to Test-PC(C4:46:19:5F:34:83)			DHCP Offer
4	2021-0...	info	DHCP	Requested 192.168.101.33 from Test-PC(C4:46:19:5F:34:83)			DHCP Request
5	2021-0...	info	Wlan Statio...	STA Association. MAC:C4:46:19:5F:34:83, AP:AP-BCCF4F65E1B6, SSID:_BBB_			
6	2021-0...	info	Wlan Statio...	STA Disassociation(5:DISASSOC_AP_BUSY) by Collaborative Detection Response. MAC:...			
7	2021-0...	alert	CDR	client:192.168.101.33 user:- from:AP-BCCF4F65E1B6 security event:Web Threats threshol...			CDR
8	2021-0...	warn	URL Threat Fi...	dawn-saga-7442.raindrop.jp:Malicious Downloads, SSI:N	192.16...	1...	ACCESS WARNING

Note: The quarantine VLAN should be a unique VLAN which doesn't use in your network environment. Whole of VLAN traffic will be blocked by CDR after configured in quarantine VLAN.

The profile of DNS Content Filter be hit.



Logs

Category: Blocked web sites

# ▲	Time	Priority	Category	Message			S...	D...	N...
20	2021-03-31 19:...	info	Blocked web sites	DNS Content Filter detected	www.facebook.com	Social Networking, rul...	19...	19...	D...
22	2021-03-31 19:...	info	Blocked web sites	DNS Content Filter detected	www.facebook.com	Social Networking, rul...	19...	19...	D...

What Can Go Wrong

1. CDR function support to block client traffic by IP address or MAC address. The default setting is blocking by IP address. You can enter CLI comment to change the setting.

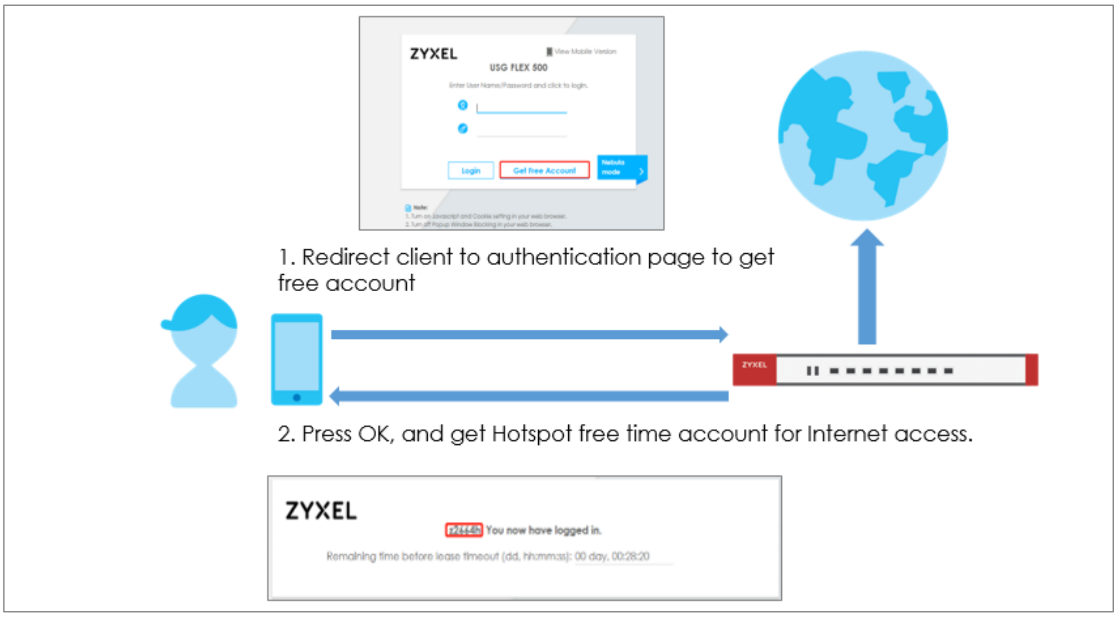
   Router(config)# cdr blocked-by ip | mac
2. CDR service support these AP models: WAX650S / WAX610D / WAX510D / WAC500 / WAC500H
3. Containment list will keep on gateway/managed AP even reboot.
4. CDR service license is required.

Chapter 3- Authentication

How to Activate Hotspot Free Time Service

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 Hotspot free time service, hotel guests are redirected to a web-based authentication portal to get a free account 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. Guests can get free access to the Internet in a matter of seconds simply by entering credential.

Hotspot Free Time


ZYXEL
View Mobile Version
USG FLEX 500
Enter User Name/Password and click to login.
Login
Get Free Account
Nebula mode
Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
ZYXEL
ZYXEL
z2664h You now have logged in.
Remaining time before lease timeout (dd, hh:mm:ss): 00 day, 00:28:20

1. Redirect client to authentication page to get free account

2. Press OK, and get Hotspot free time account for Internet access.

💡Note: Only FLEX and VPN support hotspot feature. ATP doesn't support hotspot.

Configuration Guide
Network Conditions

- WAN: 10.214.48.68
- LAN 1: 192.168.1.1/255.255.255.0
- User's laptop: 192.168.1.33

Enable Web authentication

Configurations on the FLEX500

The Free time service of this feature allows clients to access the Internet without a pre-configured guest account. An authentication portal is used as the first page when a user attempts to access the Internet.

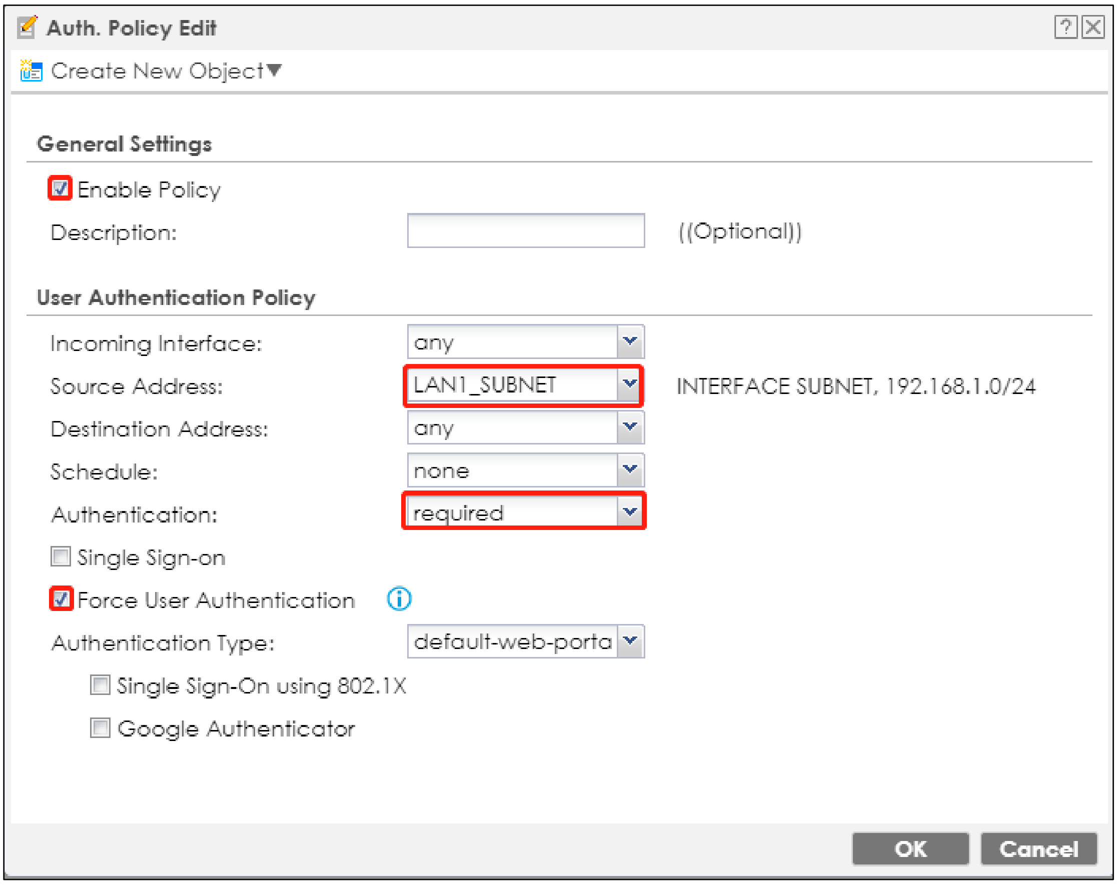
1. On the FLEX500, go to **Configuration** > **Web Authentication** > **General**. Select **Enable Web Authentication** and click **Add** in the **Web Authentication Policy Summary** section.

(1) Select **Enable Policy**.

(2) Select **LAN1_SUBNET**

(3) Select **default-web-portal** as the **Authentication Type**.

(4) Click **OK** to add the policy.



General Settings

☑ Enable Policy

Description: ((Optional))

User Authentication Policy

Incoming Interface: any

Source Address: LAN1_SUBNET INTERFACE SUBNET, 192.168.1.0/24

Destination Address: any

Schedule: none

Authentication: required

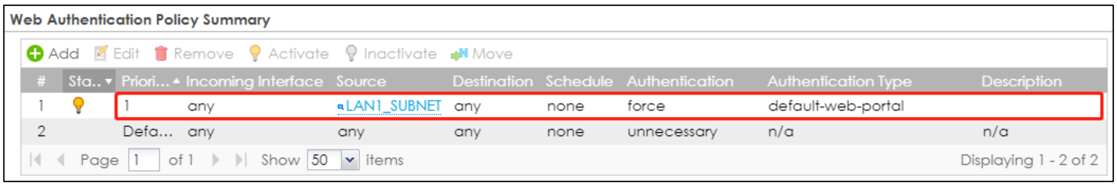
□ Single Sign-on

☑ Force User Authentication

Authentication Type: default-web-porta

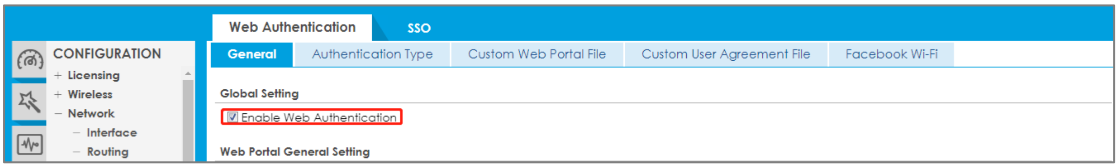
□ Single Sign-On using 802.1X

□ Google Authenticator



#	Sta..	Priori...	Incoming Interface	Source	Destination	Schedule	Authentication	Authentication Type	Description
1		1	any	LAN1_SUBNET	any	none	force	default-web-portal	
2		Defa...	any	any	any	none	unnecessary	n/a	n/a

2. Go to **Configuration** > **Web Authentication**. Select **Enable Web Authentication** and click **Apply**.



Global Setting

☑ Enable Web Authentication

Web Portal General Setting

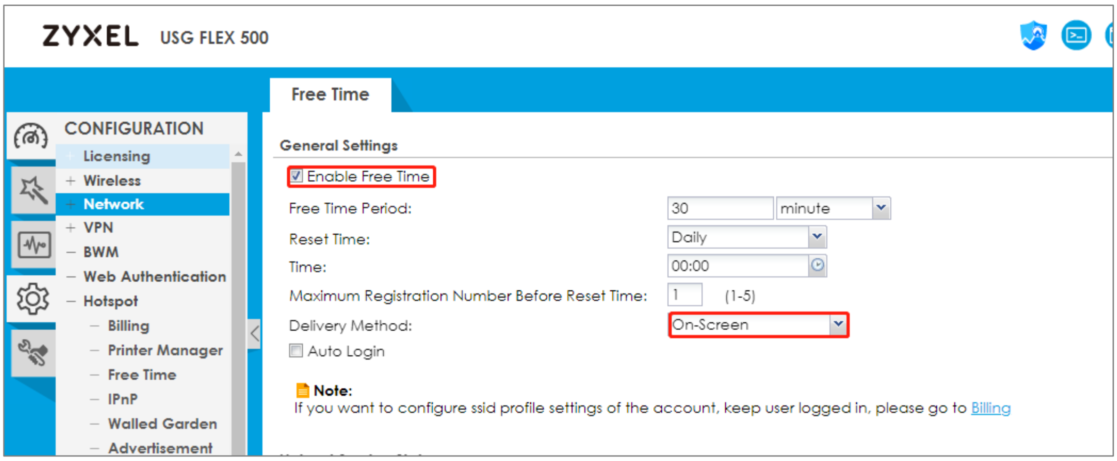
Enable the Free Time Feature

Configurations on the FLEX500

On the FLEX500, you need to enable **Free Time** feature.

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

(1) Select **Enable Free Time** and set up the free time period. By default, the **Reset Time** is Daily. You also can set up maximum registration number can access the Internet.



General Settings

☑ Enable Free Time

Free Time Period: 30 minute

Reset Time: Daily

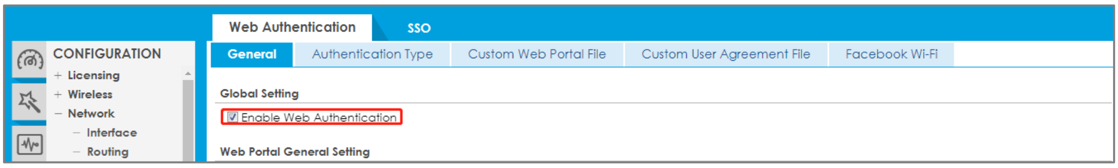
Time: 00:00

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

Delivery Method: On-Screen

□ Auto Login

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



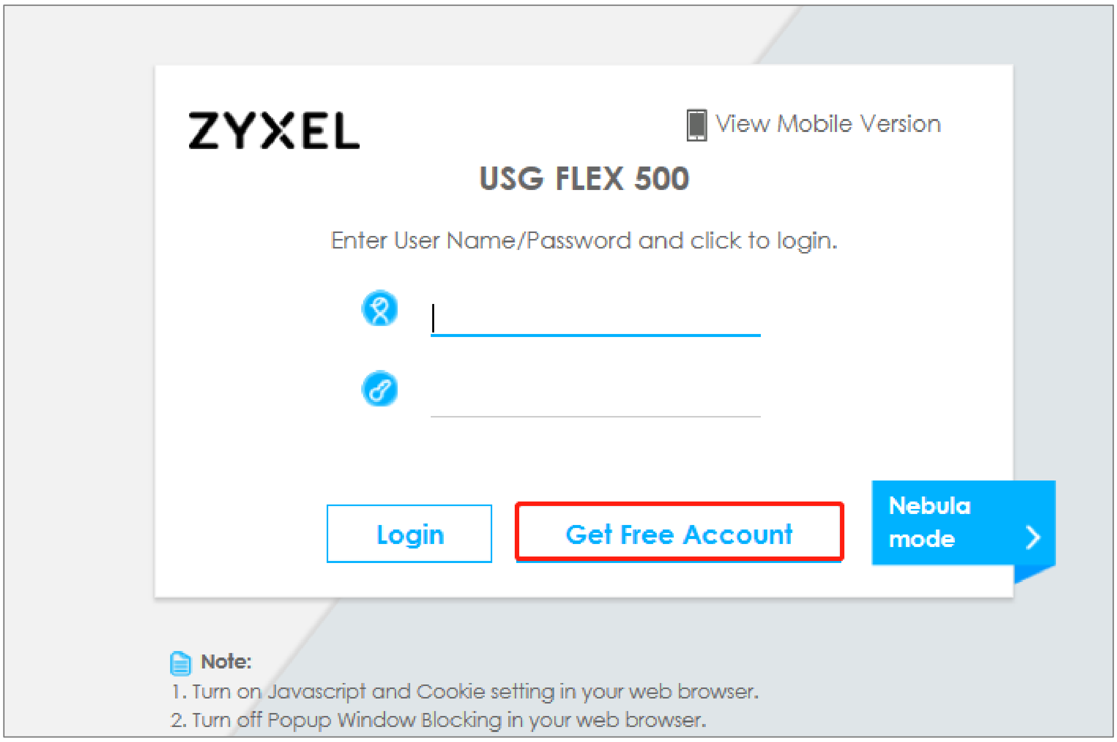
Global Setting

☑ Enable Web Authentication

Web Portal General Setting

Test Free Time Feature

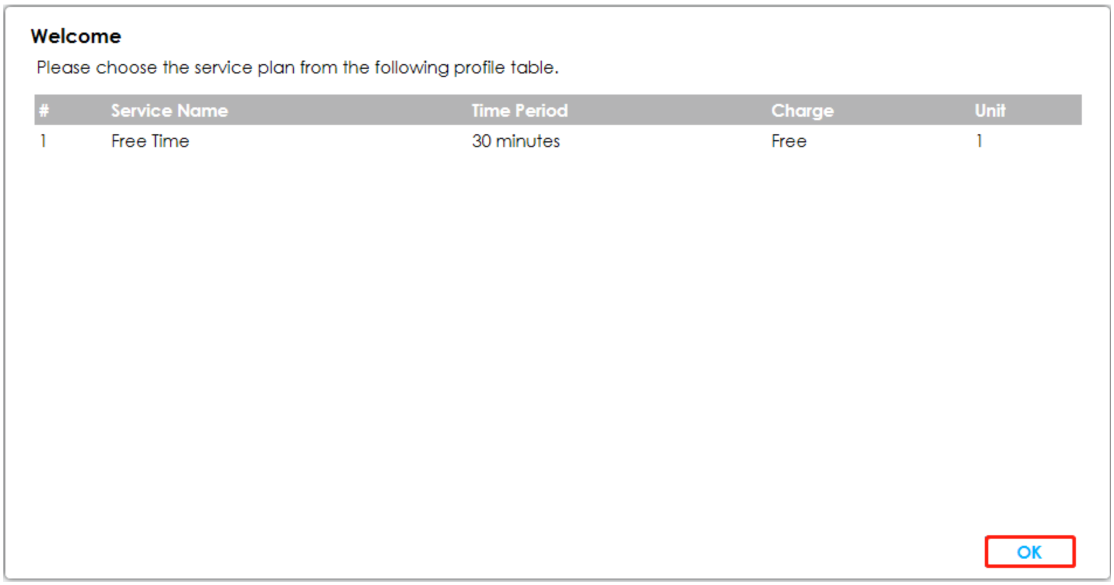
1. The user will be redirected to the **Login** screen before he/she is permitted to access the Internet. Click on the button **Get Free Account** to get a free account.



Note:

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.

2. Select **Free Time** as the service plan. Then click ok to get credential.

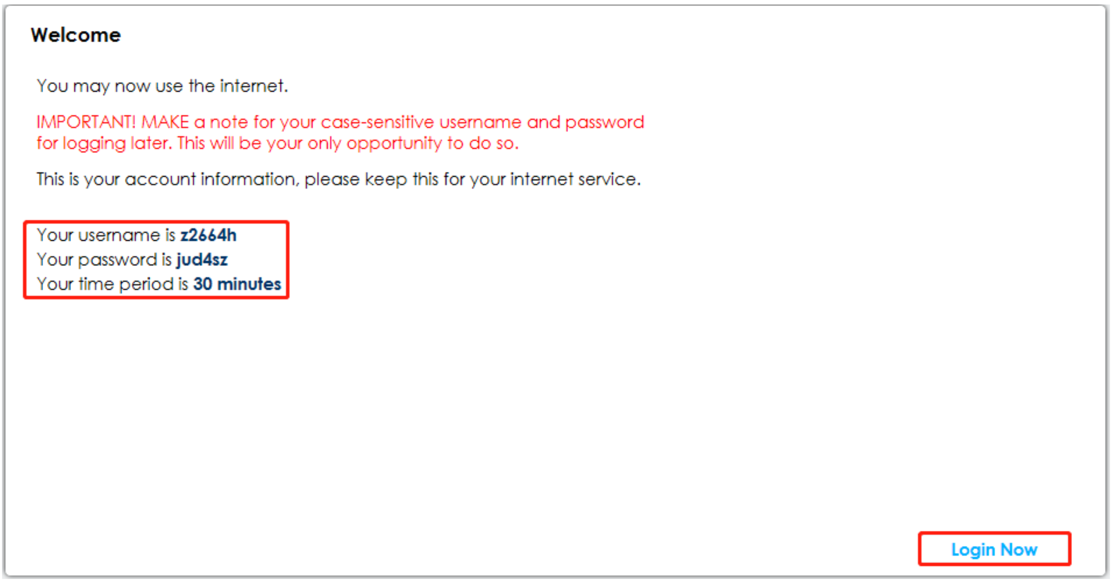


Welcome

Please choose the service plan from the following profile table.

#	Service Name	Time Period	Charge	Unit
1	Free Time	30 minutes	Free	1

3. The account and password will be show in this page. Click “Login Now”



Welcome

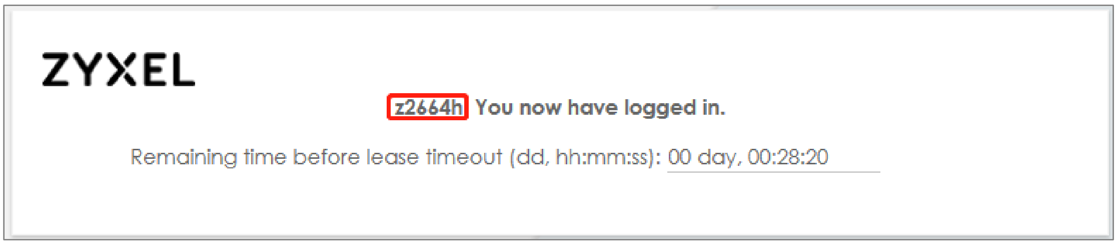
You may now use the internet.

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 **z2664h**
Your password is **jud4sz**
Your time period is **30 minutes**

4. Check your account information. the Internet can be access as now for 30 minutes.

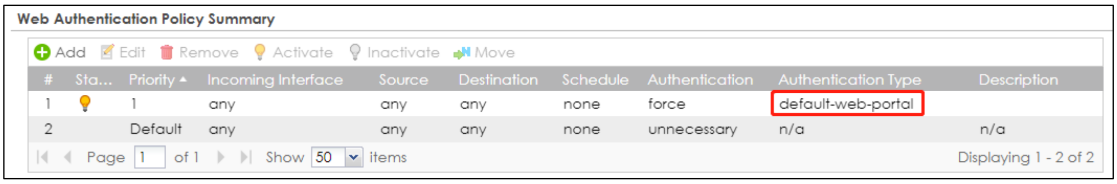


z2664h You now have logged in.

Remaining time before lease timeout (dd, hh:mm:ss): 00 day, 00:28:20

What Can Go Wrong?

If client cannot get the Login page correctly, please make sure Web Authentication Policy type is default-web-portal.



Web Authentication Policy Summary

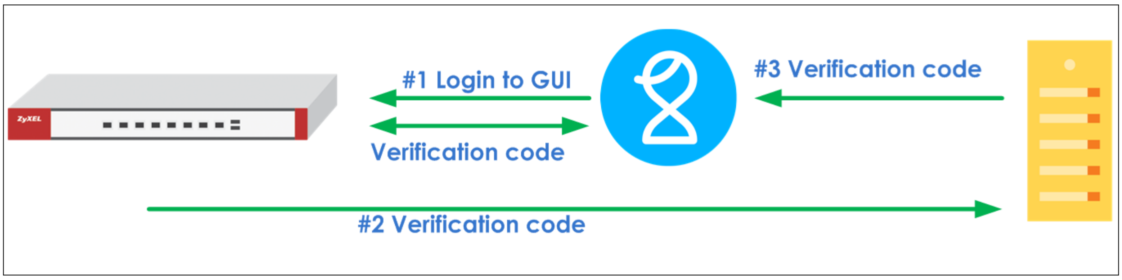
Add Edit Remove Activate Inactivate Move

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

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

How to setup Two-Factor Authentication for admin login

2 Factor Authentication is a function can prevent your device login by hacker. It needs additional verification code after logged into WebGUI/SSH/Telnet



You can follow these steps to setup 2 factor authentication when logging to system.

Setup SMTP function on your device

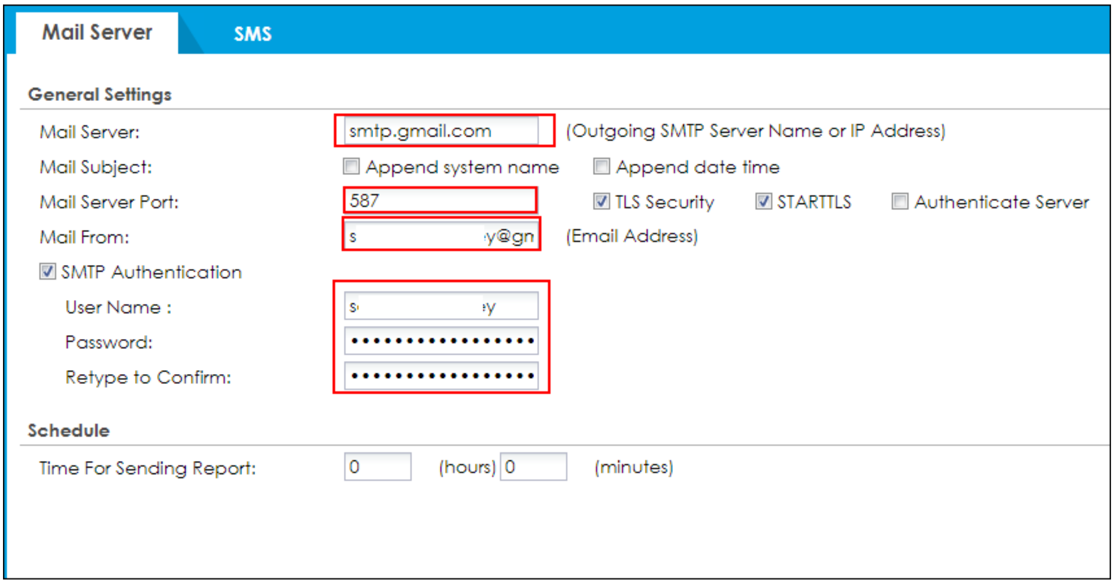
Go to **CONFIGURATION > System > Notification > Mail Server** Field your SMTP serve configuration.

a. Mail server

b. Mail server ports

c. Mail From

d. SMTP Authentication



General Settings

Mail Server: smtp.gmail.com (Outgoing SMTP Server Name or IP Address)

Mail Subject: □ Append system name □ Append date time

Mail Server Port: 587 ☑ TLS Security ☑ STARTTLS □ Authenticate Server

Mail From: s y@gn (Email Address)

☑ SMTP Authentication

User Name : s y

Password: ••••••••••••••••

Retype to Confirm: ••••••••••••••••

Schedule

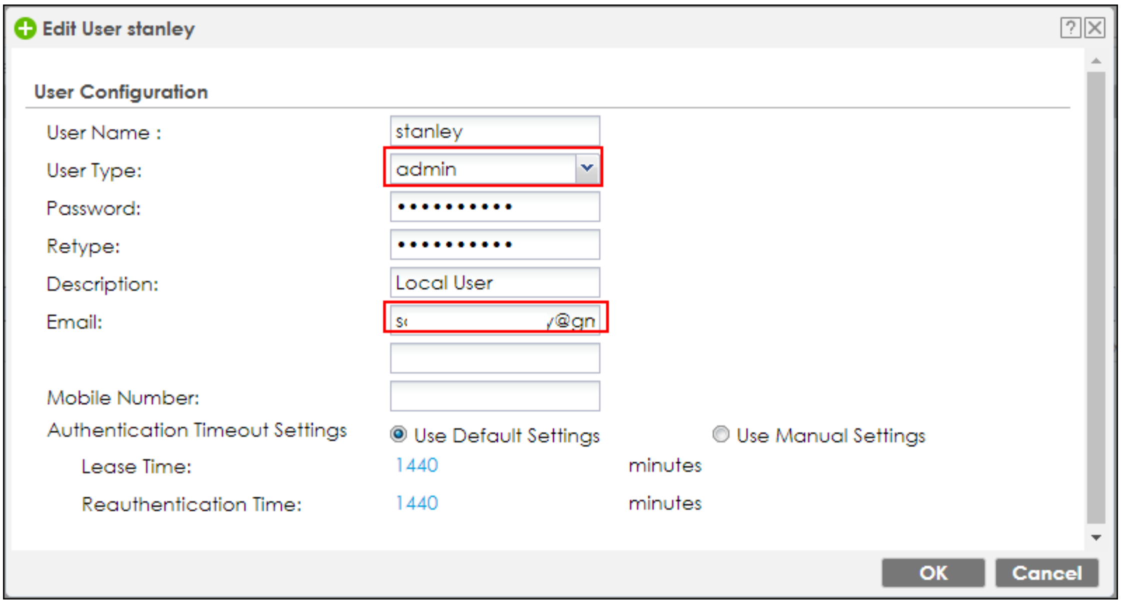
Time For Sending Report: 0 (hours) 0 (minutes)

Note: Must make sure SMTP Server configuration is correct otherwise user will unable receive mail successfully.

Create admin type user on device

Go to **Configuration > Object > User/Group > User Click** Add button to create an user and user type is admin.

And also entered email address of this user.



Edit User stanley

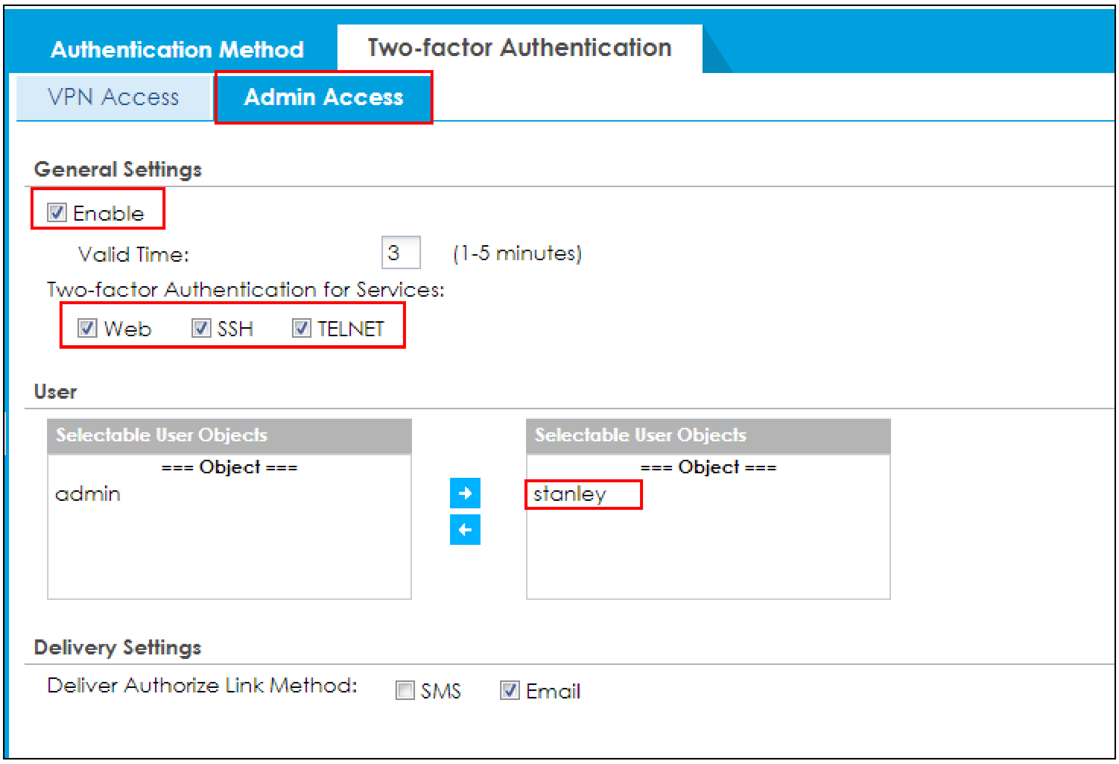
User Configuration

User Name :	stanley
User Type:	admin
Password:	•••••••••••
Retype:	•••••••••••
Description:	Local User
Email:	s[redacted]y@gn
Mobile Number:	
Authentication Timeout Settings	● Use Default Settings ○ Use Manual Settings
Lease Time:	1440 minutes
Reauthentication Time:	1440 minutes

Setup Two-Factor Authentication for admin on your device

Go to **Configuration > Object > Auth Method > Two-Factor Authentication > Admin Access**

Enable the function and add admin user which you added in step2 in the rule, and you can select what services are 2 Factor authentication needed.



Authentication Method | Two-factor Authentication

VPN Access | Admin Access

General Settings

☑ Enable

Valid Time: 3 (1-5 minutes)

Two-factor Authentication for Services:

☑ Web ☑ SSH ☑ TELNET

User

Selectable User Objects		Selectable User Objects
=== Object ===		=== Object ===
admin	→ ←	stanley

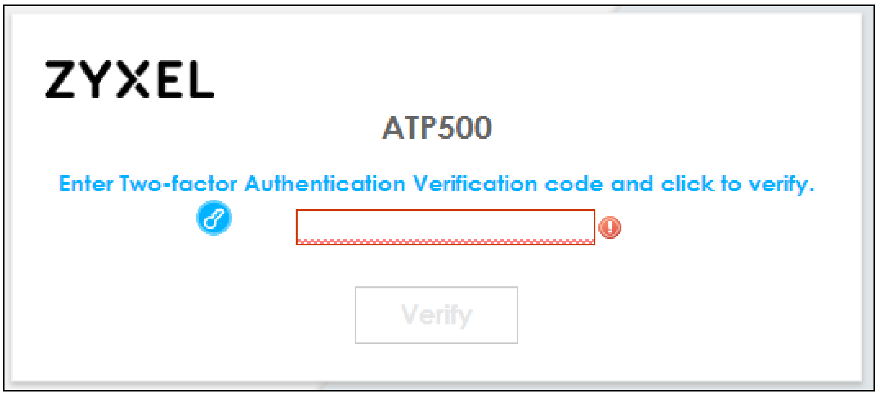
Delivery Settings

Deliver Authorize Link Method: □ SMS ☑ Email

Test the Result

After setup these steps and login to device by admin user, the verification code is required.

Web Service:

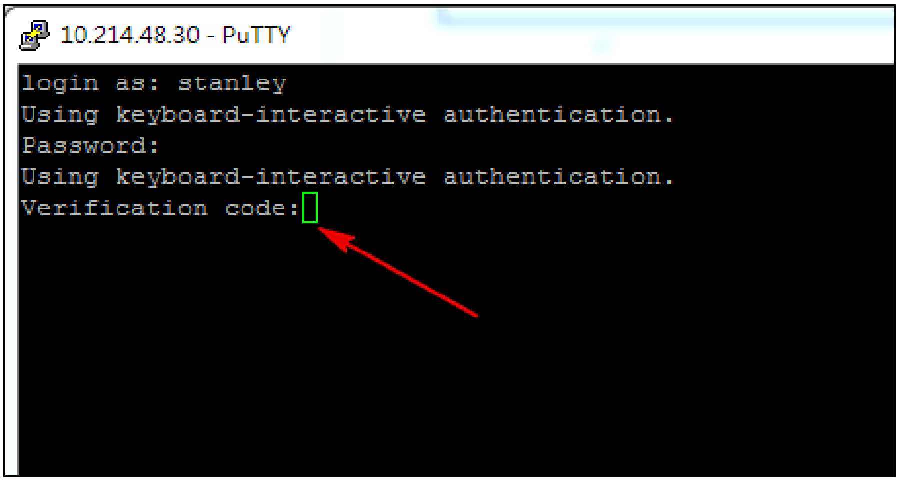


ZYXEL

ATP500

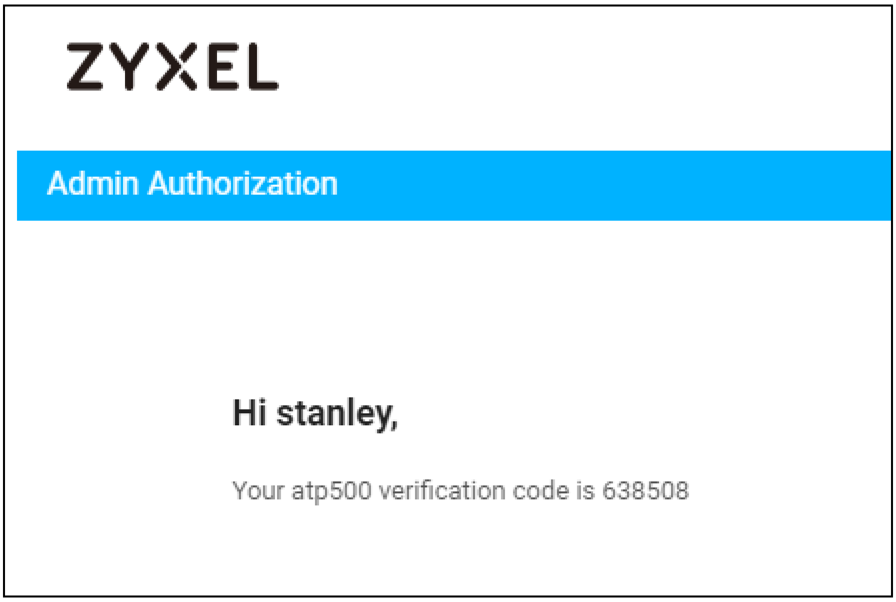
Enter Two-factor Authentication Verification code and click to verify.

SSH Service:


10.214.48.30 - PuTTY

```
login as: stanley
Using keyboard-interactive authentication.
Password:
Using keyboard-interactive authentication.
Verification code:
```

You will receive verification code by Email.


ZYXEL

Admin Authorization

Hi stanley,

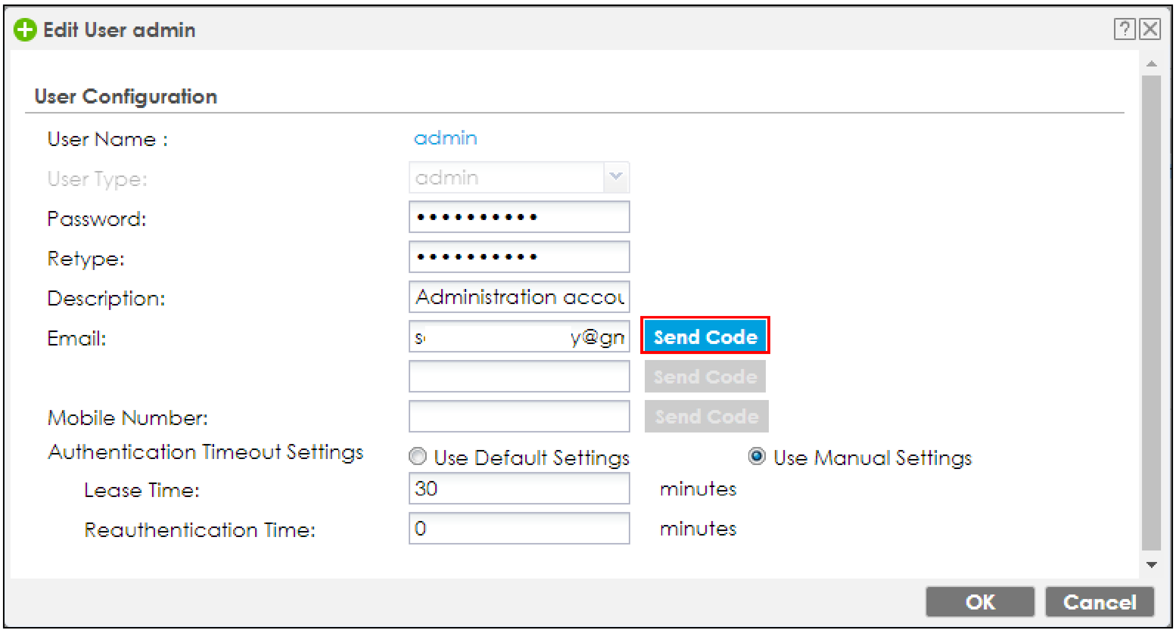
Your atp500 verification code is 638508

What Can Go Wrong?

1. **Must make sure SMTP server configuration is correct.**

2. **If you would like to add "admin" into the 2FA rule, you must do verify admin email first**

2-1 Enter Email address and click "send code" button



Edit User admin

User Configuration

User Name : admin

User Type: admin

Password: ••••••••••

Retype: ••••••••••

Description: Administration accou

Email: s y@gn

Mobile Number:

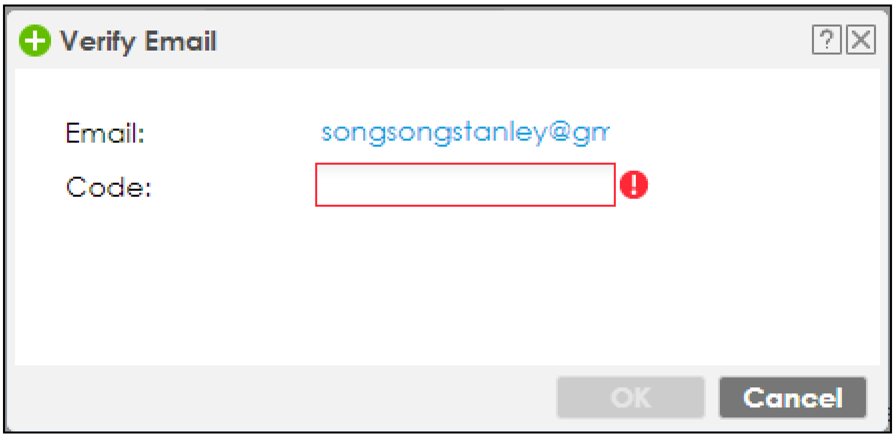
Authentication Timeout Settings ○ Use Default Settings ● Use Manual Settings

Lease Time: 30 minutes

Reauthentication Time: 0 minutes

2.2 After clicked "Send Code", you will receive code by Email.

2.3 Enter code that you received.

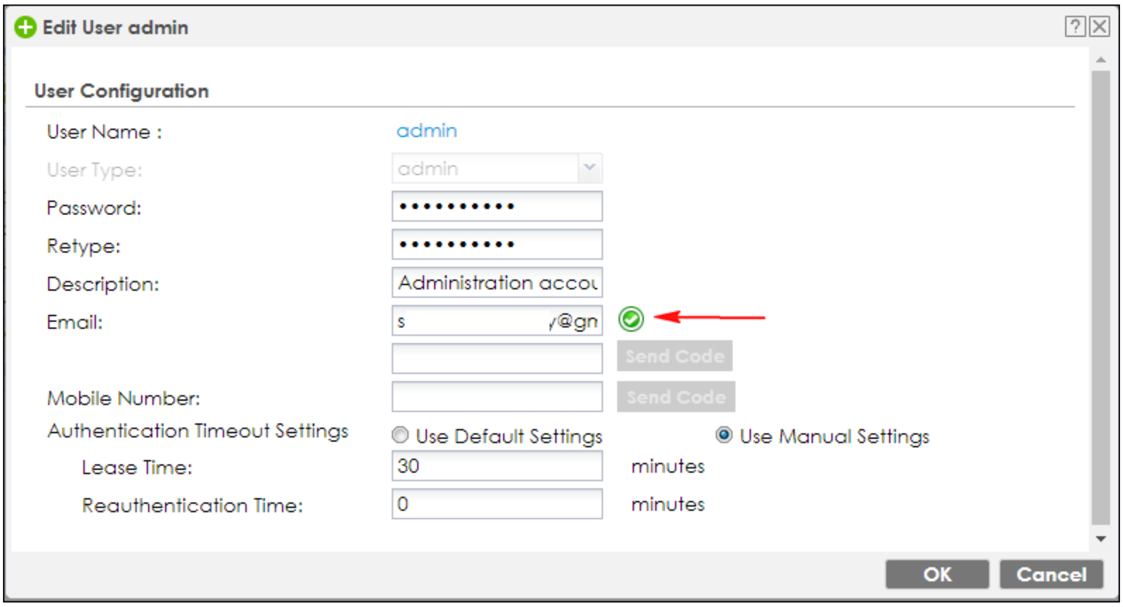


Verify Email

Email: songsongstanley@gm

Code:

2.4 After admin Email is verified, it will display success.



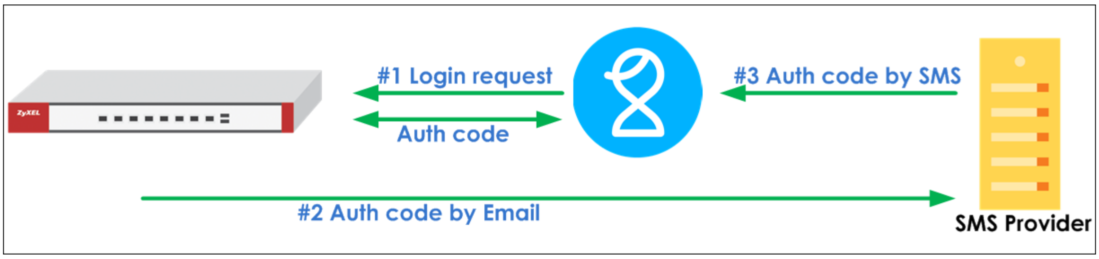
Edit User admin

User Configuration

User Name :	admin	
User Type:	admin	
Password:	•••••••••••	
Retype:	•••••••••••	
Description:	Administration accou	
Email:	s y@gn	✓
		Send Code
Mobile Number:		Send Code
Authentication Timeout Settings	○ Use Default Settings	● Use Manual Settings
Lease Time:	30	minutes
Reauthentication Time:	0	minutes

How to setup Email to SMS

The Email to SMS function can help to send the SMS to client. The SMS message is initialed from device to SMS provider, and then SMS provider send the SMS to client. This function can help to make sure user receives SMS if client without Internet connection.



You can follow these steps to Email to SMS.

Setup SMTP function on your device

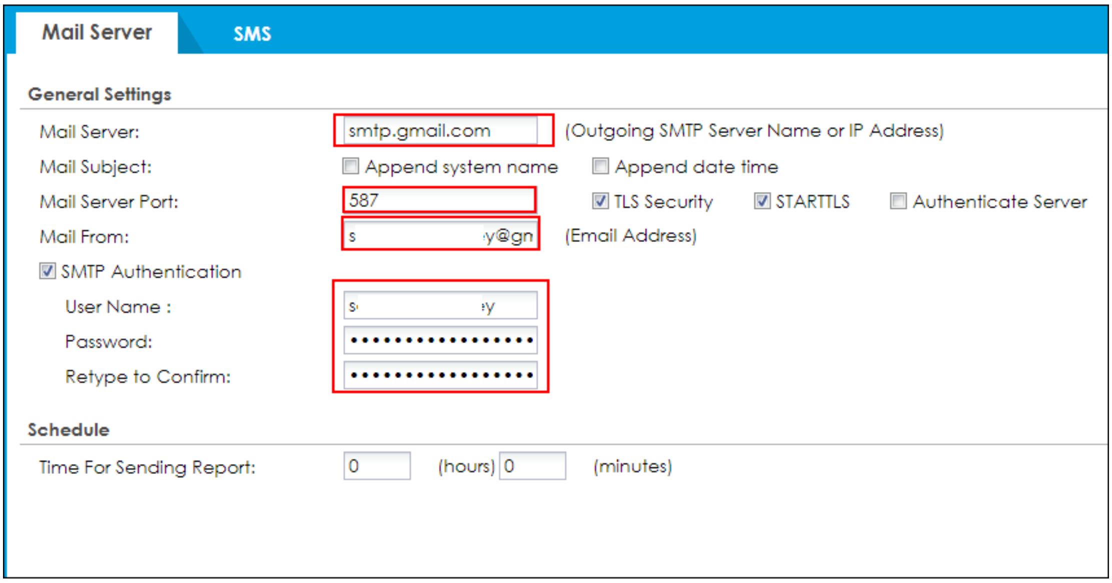
Go to **CONFIGURATION > System > Notification > Mail Server** Field your SMTP serve configuration.

A. Mail server

B. Mail server ports

C. Mail From

D. SMTP Authentication



General Settings

Mail Server: smtp.gmail.com (Outgoing SMTP Server Name or IP Address)

Mail Subject: □ Append system name □ Append date time

Mail Server Port: 587 ☑ TLS Security ☑ STARTTLS □ Authenticate Server

Mail From: s y@gn (Email Address)

☑ SMTP Authentication

User Name : s y

Password: ••••••••••••••••

Retype to Confirm: ••••••••••••••••

Schedule

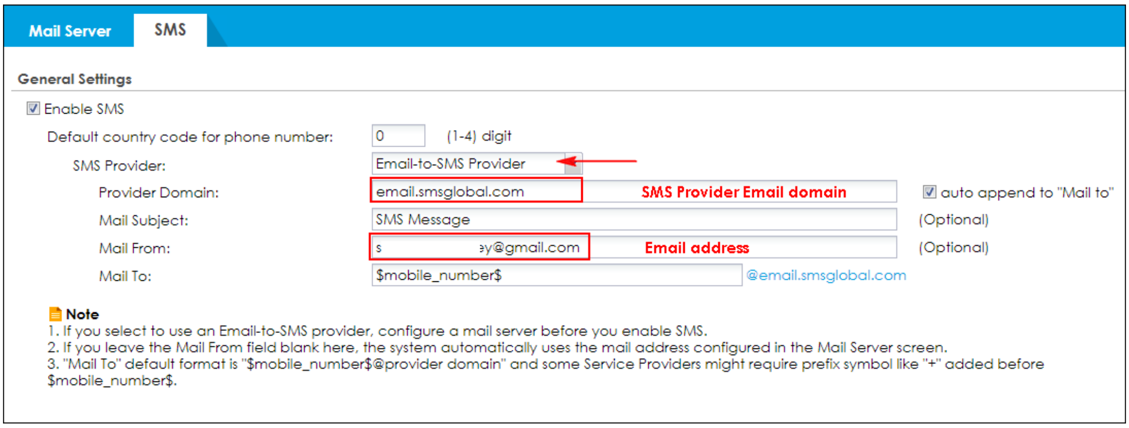
Time For Sending Report: 0 (hours) 0 (minutes)

Note: Must make sure SMTP Server configuration is correct otherwise message will unable send to SMS provider successfully.

Setup Email to SMS Provider configuration

Go to “**Configuration > system > Notification > SMS Select “SMS Provider”** as Email to SMS Provider. Enter SMS Provider Email server domain name.

And configuring sender mail address in “Mail From”



General Settings

☑ Enable SMS

Default country code for phone number: 0 (1-4) digit

SMS Provider: Email-to-SMS Provider

Provider Domain: email.smsglobal.com ☑ auto append to "Mail to"

Mail Subject: SMS Message (Optional)

Mail From: s ɜy@gmail.com (Optional)

Mail To: $mobile_number$ @email.smsglobal.com

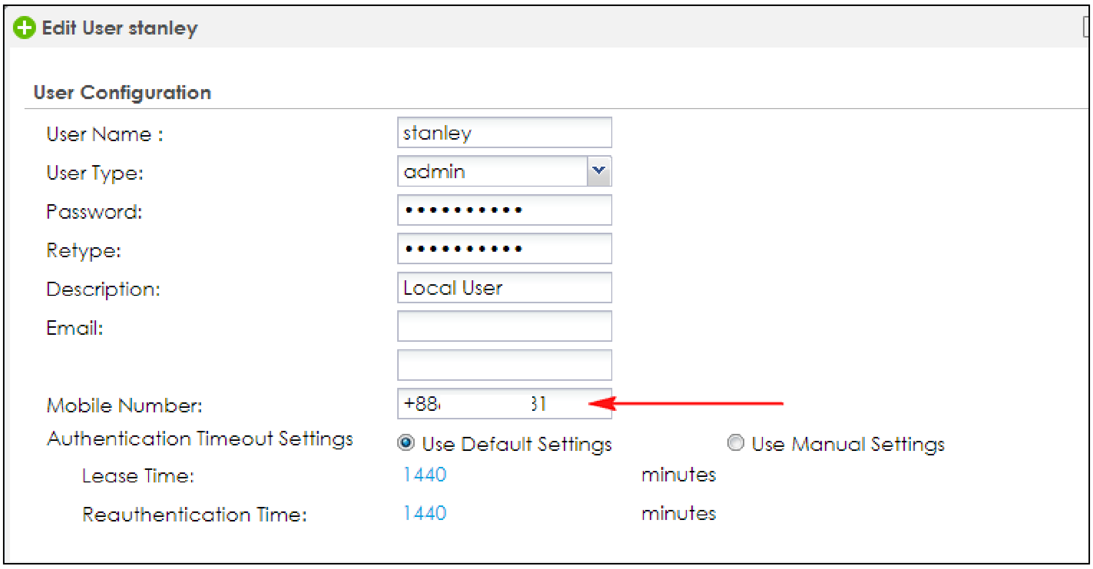
Note

1. If you select to use an Email-to-SMS provider, configure a mail server before you enable SMS.
2. If you leave the Mail From field blank here, the system automatically uses the mail address configured in the Mail Server screen.
3. "Mail To" default format is "$mobile_number$@provider domain" and some Service Providers might require prefix symbol like "+" added before $mobile_number$.

Note: Your SMS provider has to allow the email address which configured in “Mail From” to prevent the email is denied by SMS provider’s mailbox.

Create admin type user on device

Go to **Configuration > Object > User/Group > User** Click Add button to create an user and user type is admin. And also entered phone number of this user.



Edit User stanley

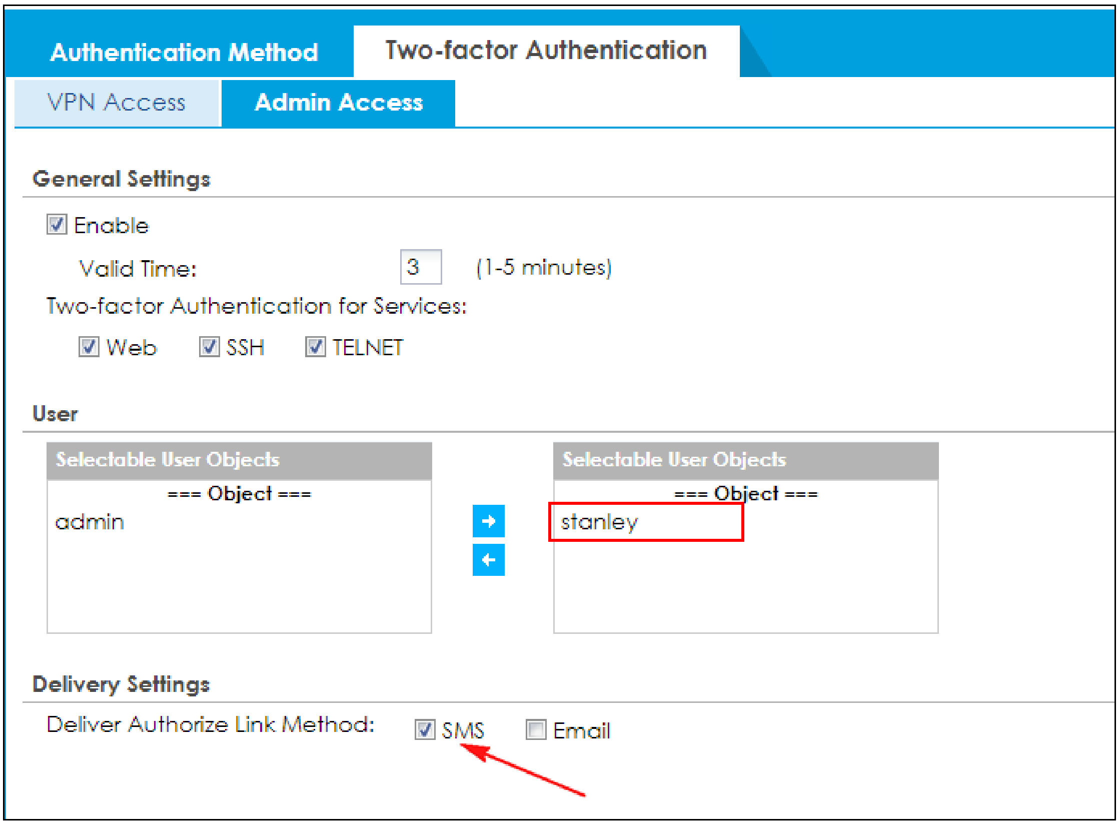
User Configuration

User Name :	stanley	
User Type:	admin	
Password:	••••••••••	
Retype:	••••••••••	
Description:	Local User	
Email:		
Mobile Number:	+88[redacted]31	
Authentication Timeout Settings	● Use Default Settings	○ Use Manual Settings
Lease Time:	1440	minutes
Reauthentication Time:	1440	minutes

Setup Two-Factor Authentication for admin on your device

Go to **Configuration > Object > Auth Method > Two-Factor Authentication > Admin Access**

Enable the function and add admin user which you added in step3 in the rule, and you can select what services are 2 Factor authentication needed. Enable SMS function to send verification code by SMS.



Authentication Method | Two-factor Authentication

VPN Access | Admin Access

General Settings

☑ Enable

Valid Time: 3 (1-5 minutes)

Two-factor Authentication for Services:

☑ Web ☑ SSH ☑ TELNET

User

Selectable User Objects		Selectable User Objects
=== Object ===	→	=== Object ===
admin	←	stanley

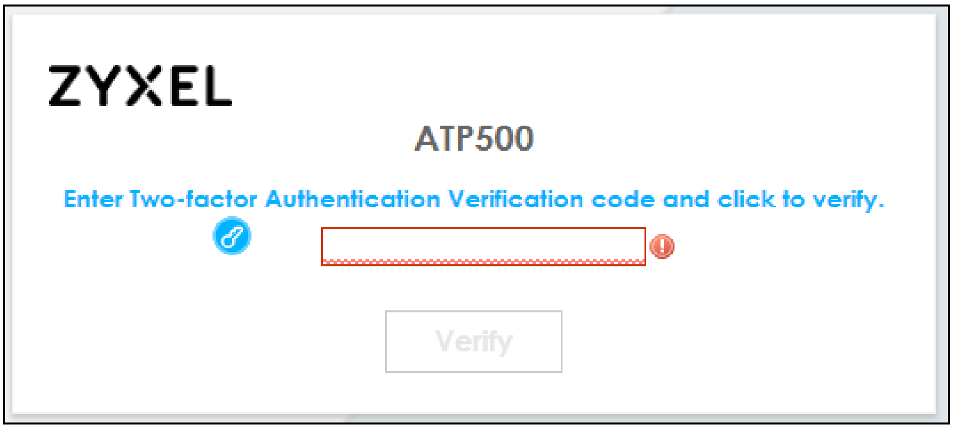
Delivery Settings

Deliver Authorize Link Method: ☑ SMS □ Email

Test the Result

After setup these steps and login to device by admin user, the verification code is required.

Web Service:

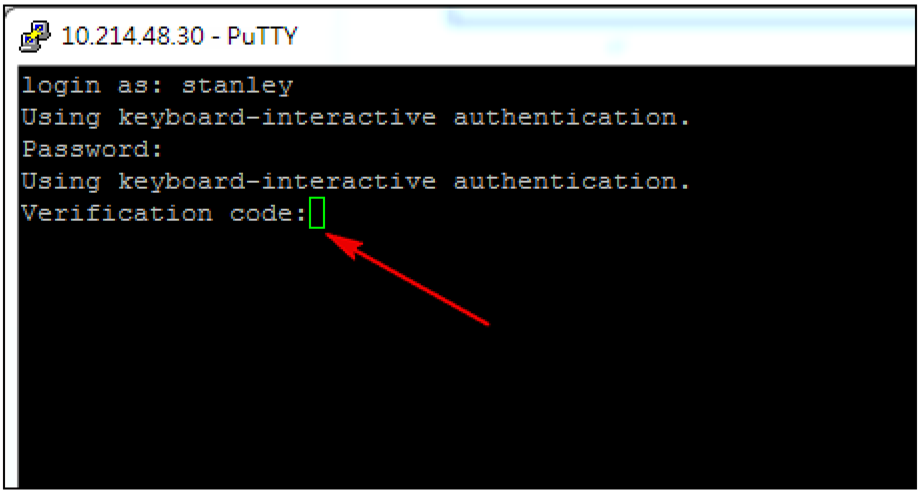


ZYXEL

ATP500

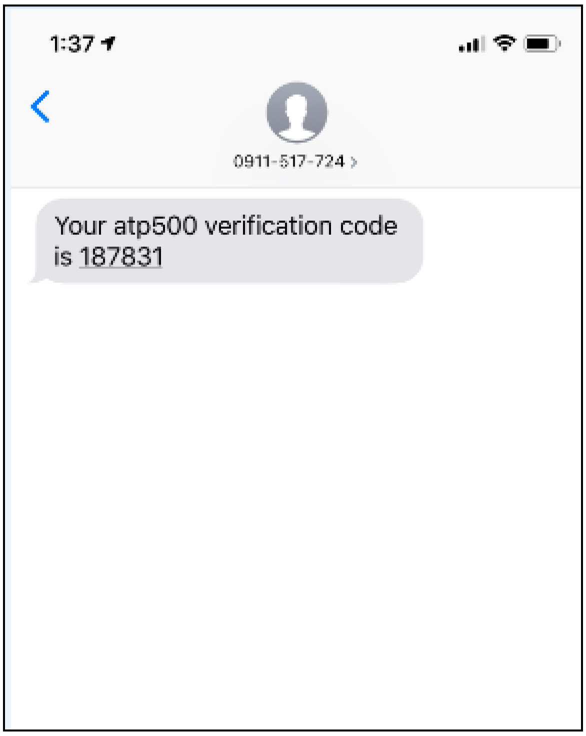
Enter Two-factor Authentication Verification code and click to verify.

SSH Service:



```
login as: stanley
Using keyboard-interactive authentication.
Password:
Using keyboard-interactive authentication.
Verification code:
```

You will receive verification code by SMS.



Your atp500 verification code is 187831

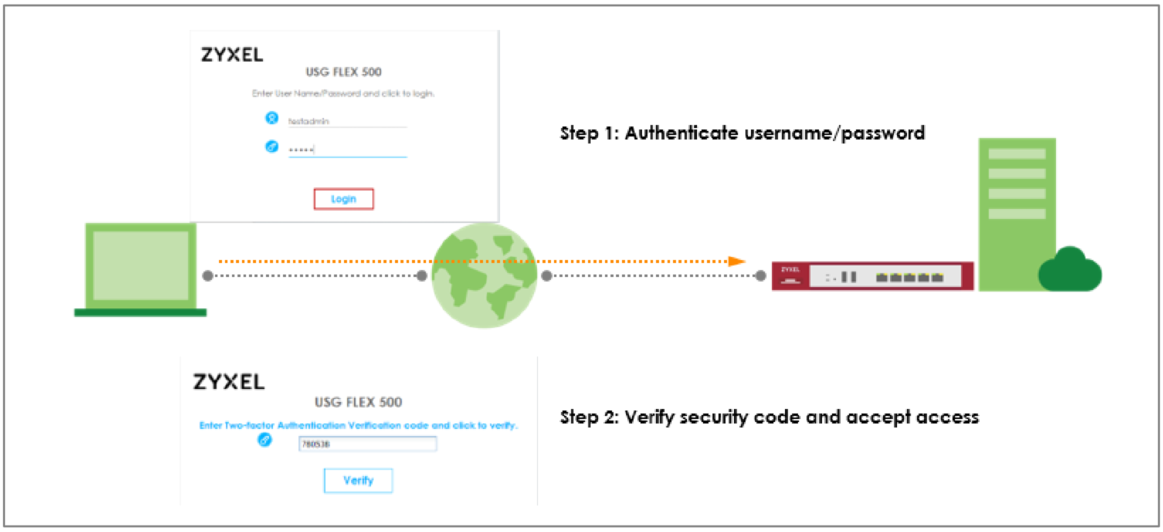
What Can Go Wrong?

1. Must make sure SMTP server configuration is correct.
2. Must make sure your SMS provider is supported Mail to SMS function.

3 Make sure your email address is allowed by your SMS provider.

How to Use Two Factor with Google Authenticator for Admin Access

In previous firmware versions, USG supports pin code by SMS/Email as two-factor authentication method. However, SMS-based two-factor authentication is not safe. Compared to SMS-based method, Google authenticator is the most secure method to receive verification code for 2-factor authentication. Google authenticator gives a new code every 30 seconds, so each code expires in just 30 seconds which make it a secure option to generate codes for 2-step verification. Furthermore, Google authenticator is free to download, easy to use, and is able to work without Internet. This example illustrates how to set up two factor with Google Authenticator for admin access.


ZYXEL
USG FLEX 500
Enter User Name/Password and click to login.
testadmin
•••••
Login
ZYXEL
USG FLEX 500
Enter Two-factor Authentication Verification code and click to verify.
780538
Verify

Step 1: Authenticate username/password

Step 2: Verify security code and accept access

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses. This example was tested using the USG FLEX 500 (Firmware Version: ZLD 4.60).

Two Factor with Google Authenticator Flow

1. Enable Google Authentication on specific admin user

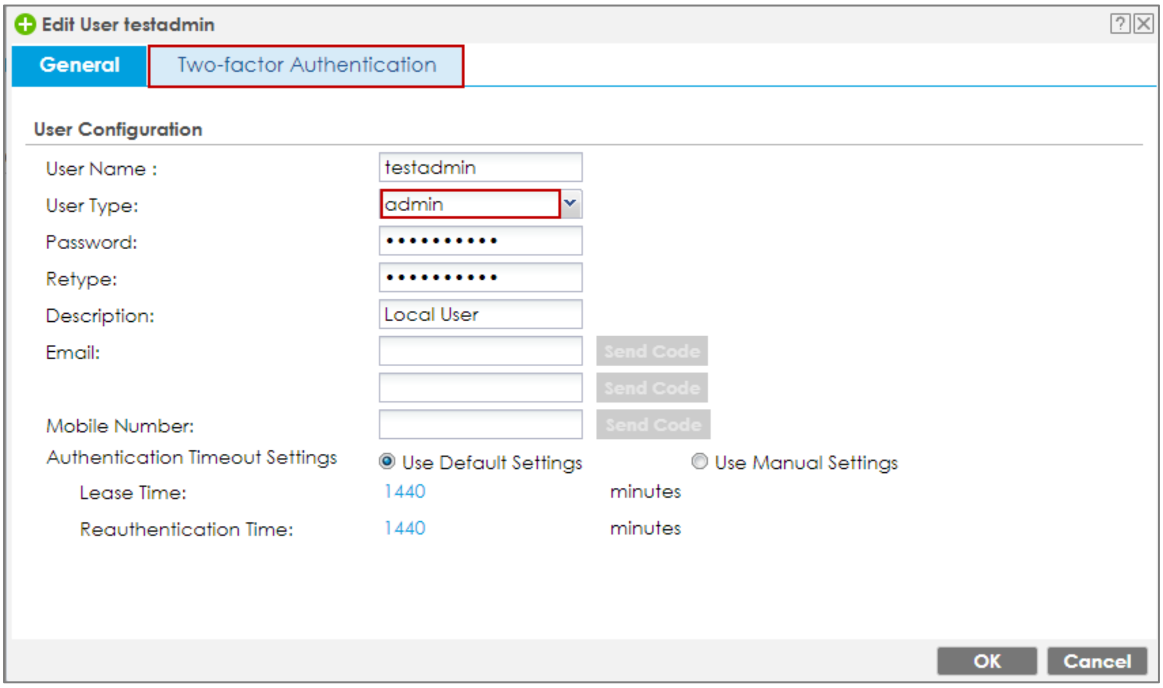
2. Set up Google Authenticator

3. Configure valid time and login service types.

Enable Google Authentication on specific admin user

Select a specific admin user and switch to Two-factor Authentication tab.

CONFIGURATION > Object > User/Group > admin user



Edit User testadmin

General | Two-factor Authentication

User Configuration

User Name : testadmin

User Type: admin

Password: ••••••••••

Retype: ••••••••••

Description: Local User

Email:

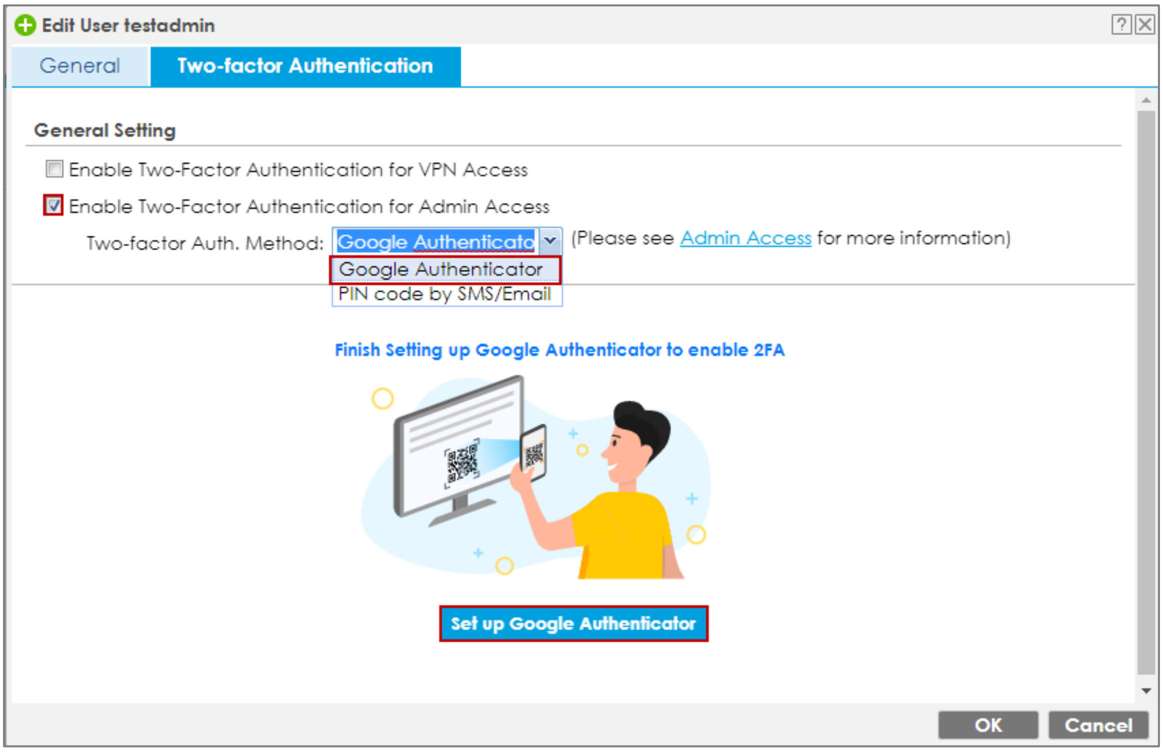
Mobile Number:

Authentication Timeout Settings ● Use Default Settings ○ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Enable Two-Factor Authentication for Admin Access checkbox. In Two-factor Auth. Method, select "Google Authenticator". Click "Set up Google Authenticator" to start setting up Google Authenticator on your mobile phone and USG.



Edit User testadmin

General | Two-factor Authentication

General Setting

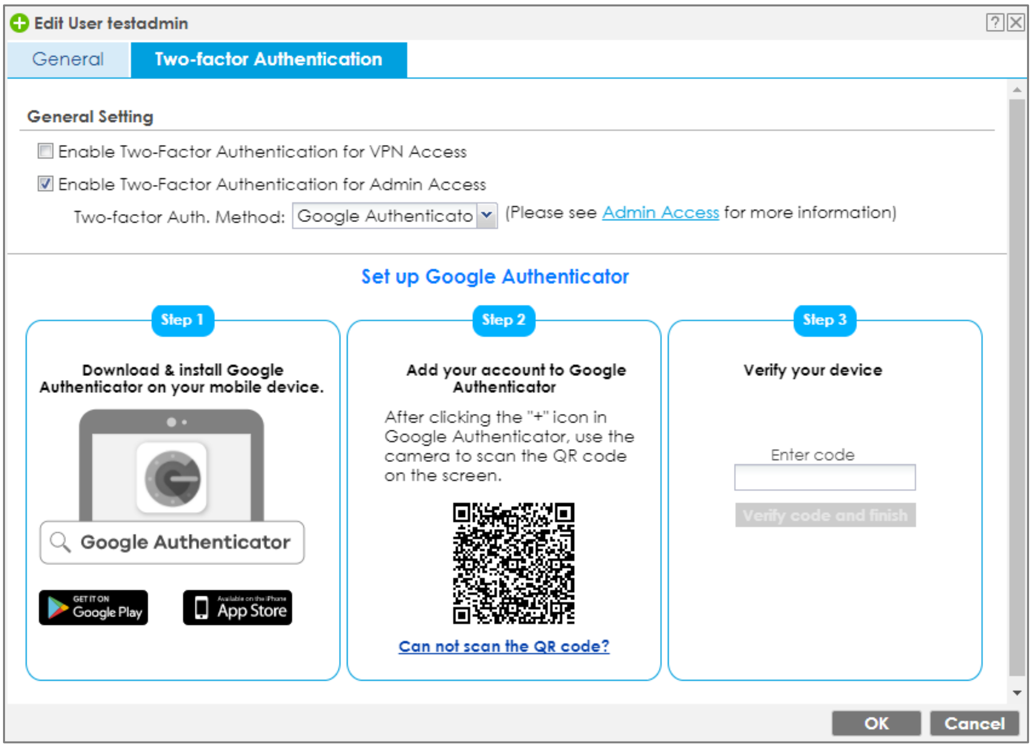
□ Enable Two-Factor Authentication for VPN Access

☑ Enable Two-Factor Authentication for Admin Access

Two-factor Auth. Method: Google Authenticato (Please see Admin Access for more information)

Google Authenticator
PIN code by SMS/Email
Finish Setting up Google Authenticator to enable 2FA
Set up Google Authenticator
OK
Cancel

Set up Google Authenticator



Edit User testadmin

General | Two-factor Authentication

General Setting

□ Enable Two-Factor Authentication for VPN Access

☑ Enable Two-Factor Authentication for Admin Access

Two-factor Auth. Method: Google Authenticato (Please see Admin Access for more information)

Set up Google Authenticator

Step 1 Download & install Google Authenticator on your mobile device.

Step 2 Add your account to Google Authenticator

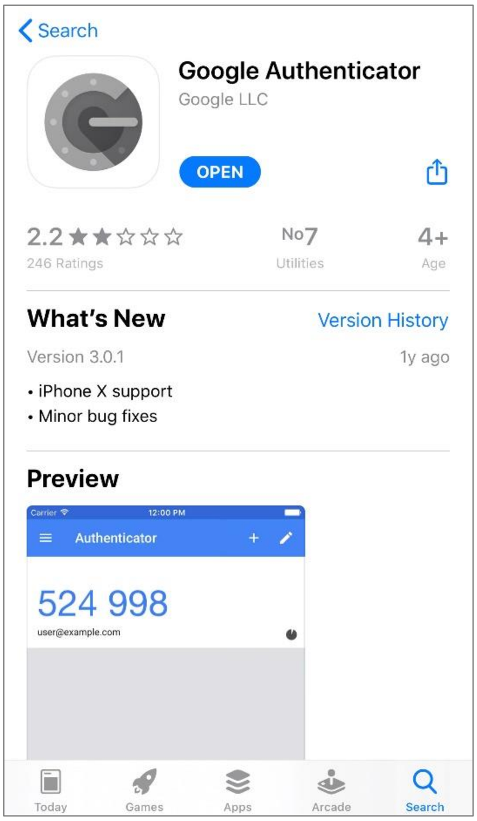
After clicking the "+" icon in Google Authenticator, use the camera to scan the QR code on the screen.

Step 3 Verify your device

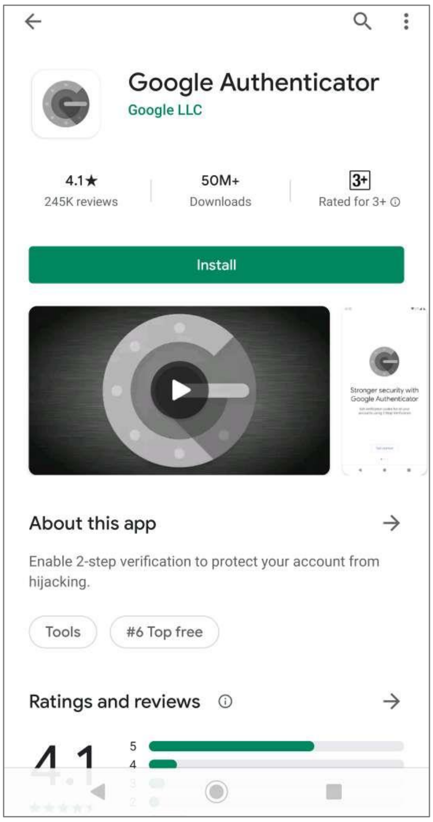
Enter code

1. Download and install Google Authenticator on your mobile device.

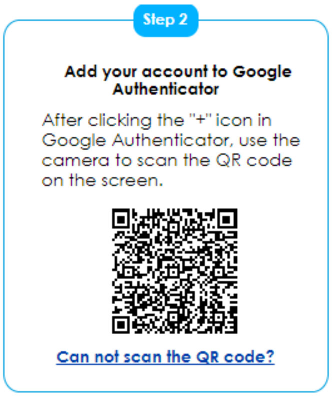
Apple Store



Google Play



2. Register the admin account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.

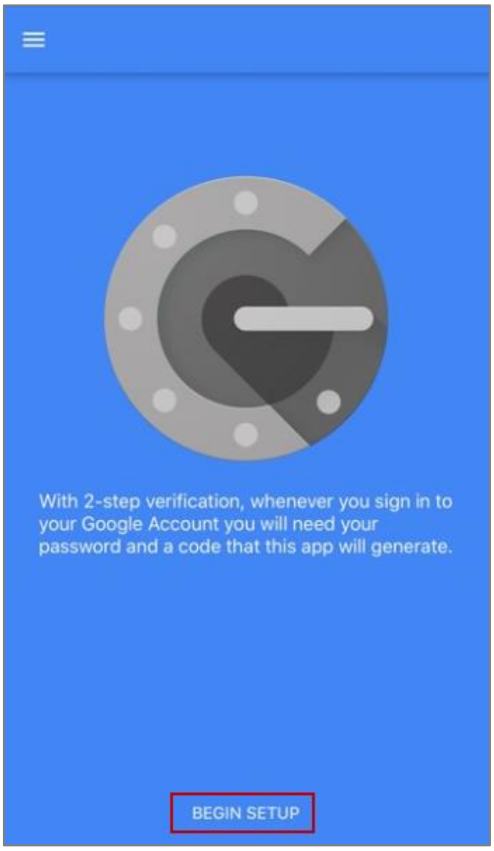


Step 2

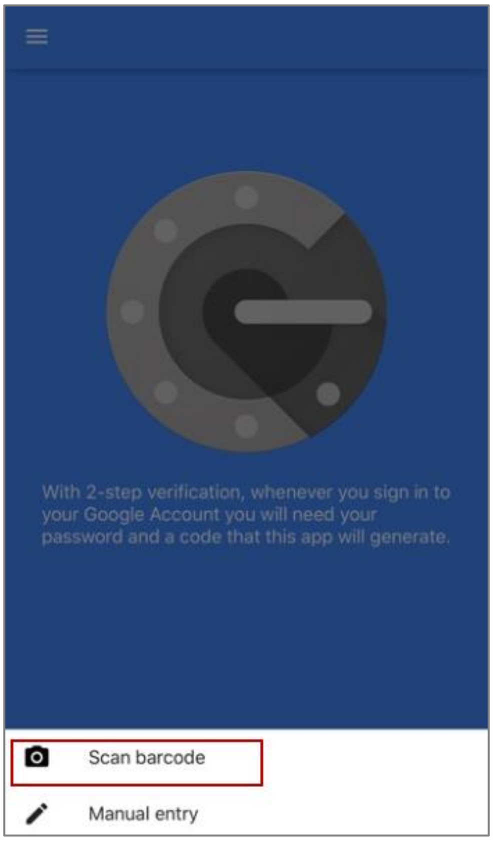
Add your account to Google Authenticator

After clicking the "+" icon in Google Authenticator, use the camera to scan the QR code on the screen.

Can not scan the QR code?

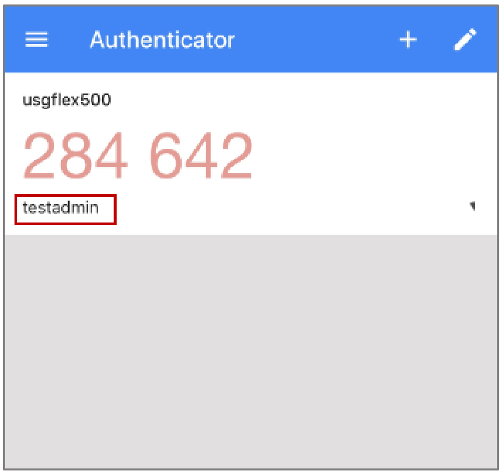


With 2-step verification, whenever you sign in to your Google Account you will need your password and a code that this app will generate.



With 2-step verification, whenever you sign in to your Google Account you will need your password and a code that this app will generate.

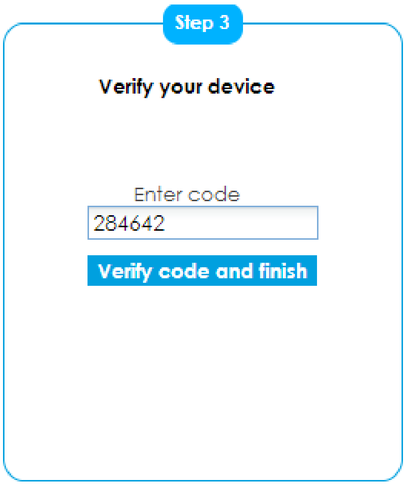
3. Enter the token code which displays on Google Authenticator to "Step 3" and click "Verify code and finish" to submit and verify the code.



usgflex500

284 642

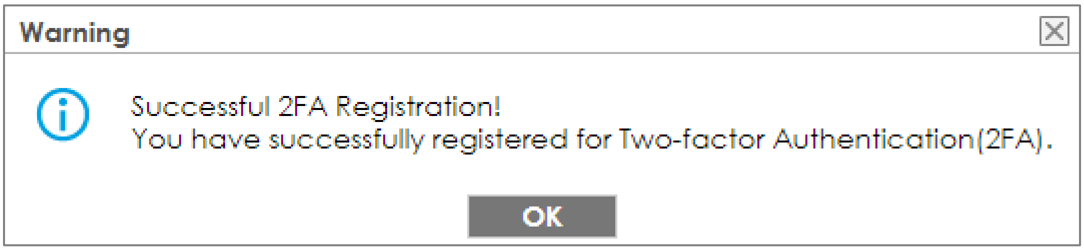
testadmin



Verify your device

Enter code: 284642

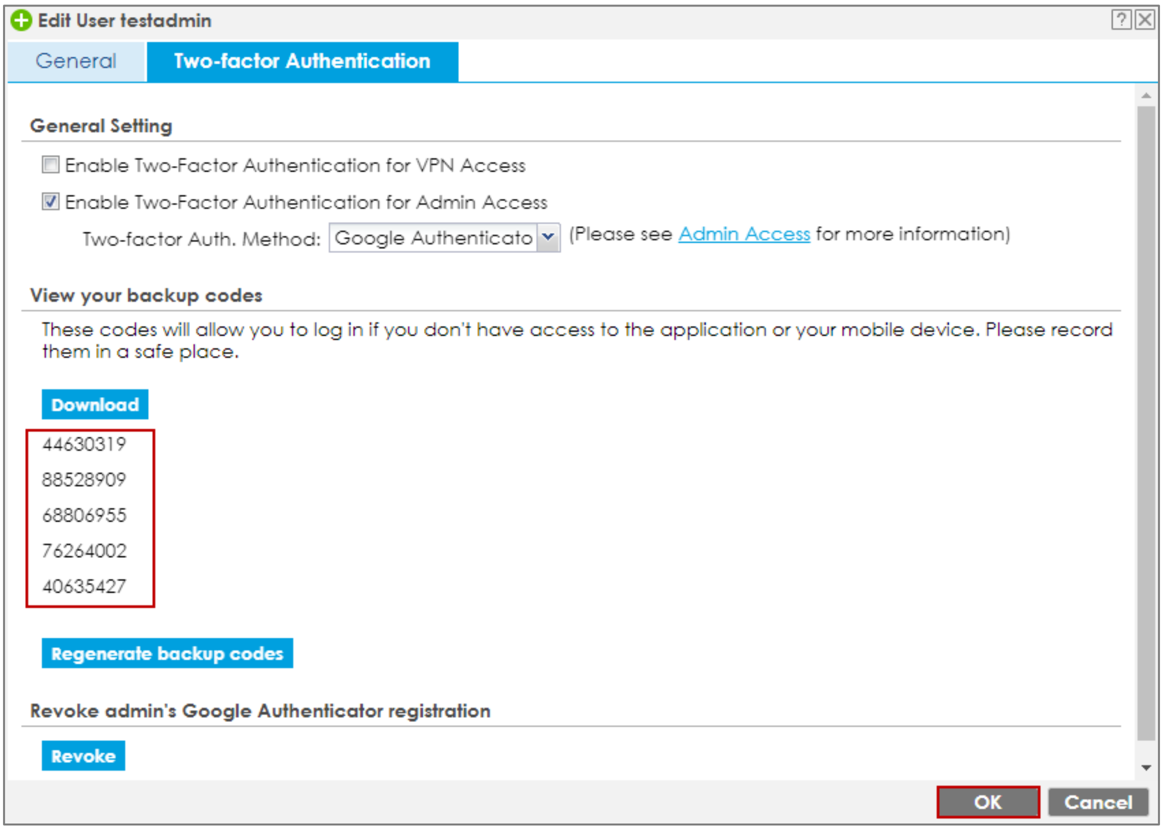
The pop-up window message informs the verification result.



Warning

Successful 2FA Registration!
You have successfully registered for Two-factor Authentication(2FA).

4. After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.



Edit User testadmin

General Setting

□ Enable Two-Factor Authentication for VPN Access

☑ Enable Two-Factor Authentication for Admin Access

Two-factor Auth. Method: Google Authenticato (Please see Admin Access for more information)

View your backup codes

These codes will allow you to log in if you don't have access to the application or your mobile device. Please record them in a safe place.

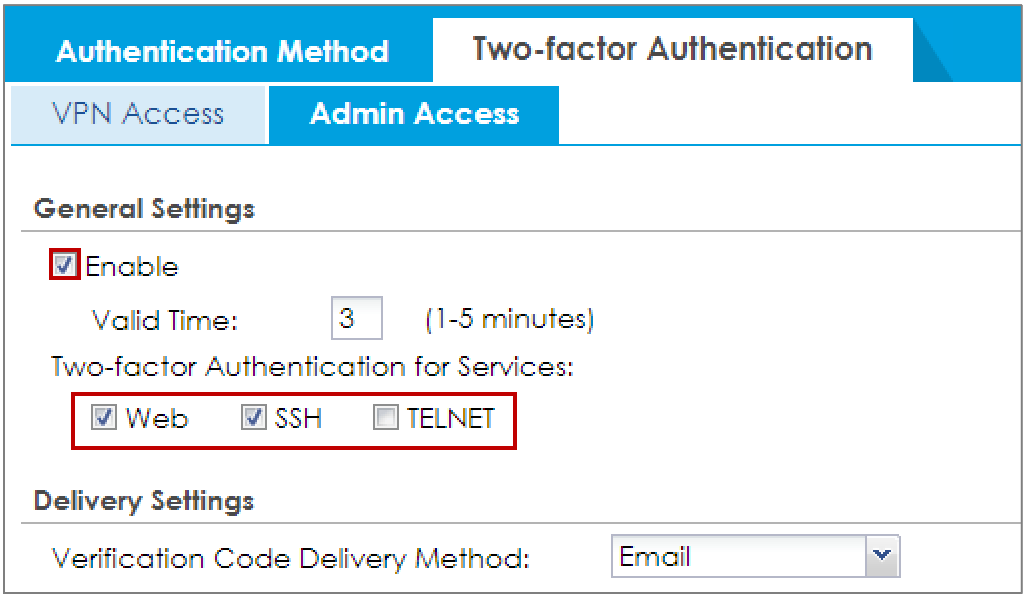
44630319
88528909
68806955
76264002
40635427

Revoke admin's Google Authenticator registration

Configure valid time and login service types

Enable two factor authentication for admin access. Configure valid time and select which services require two-factor authentication for admin user. The valid time is the deadline that admin needs to submit the two-factor authentication code to get the access. The access request is rejected if submitting the code later than valid time. By default, the valid time is 3 minutes.

CONFIGURATION > Object > Auth. Method > Two-factor Authentication > Admin Access



General Settings

☑ Enable

Valid Time: 3 (1-5 minutes)

Two-factor Authentication for Services:

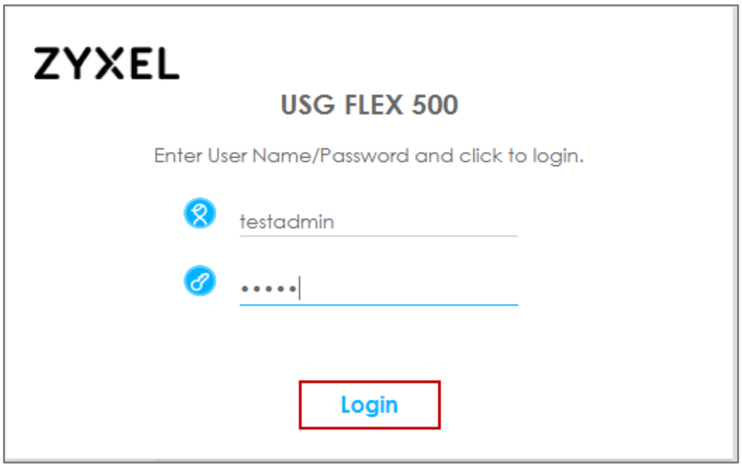
☑ Web ☑ SSH □ TELNET

Delivery Settings

Verification Code Delivery Method: Email

Test the Result

1. Login with the admin account "testadmin".



ZYXEL

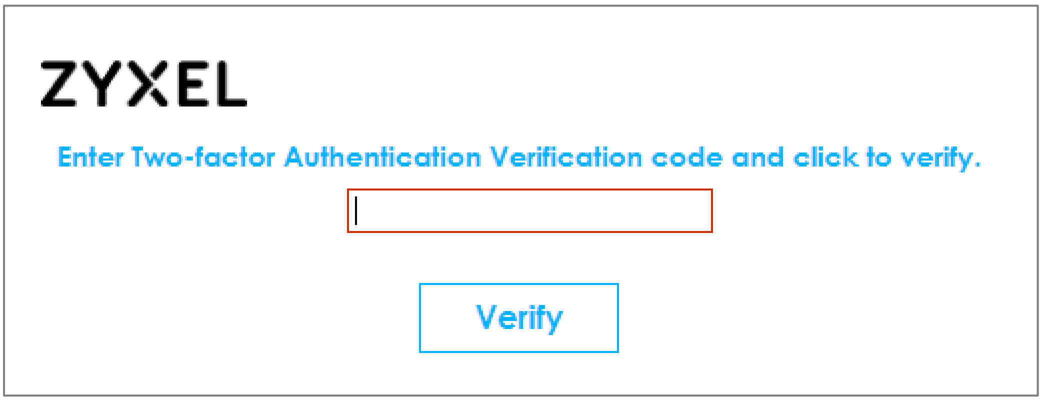
USG FLEX 500

Enter User Name/Password and click to login.

testadmin

•••••

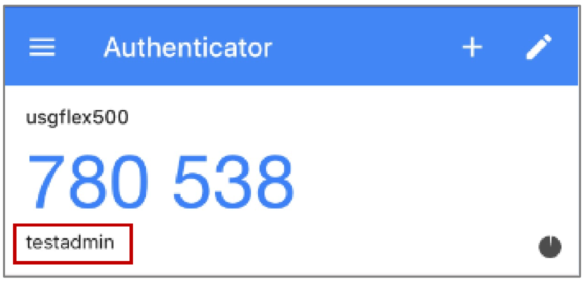
2. A pop-up window appears for administrator to enter the verification code.



ZYXEL

Enter Two-factor Authentication Verification code and click to verify.

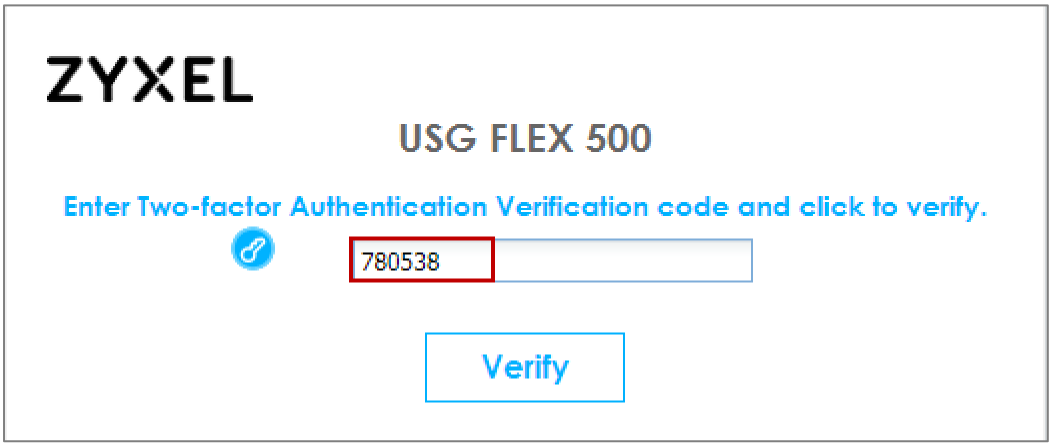
3. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.



usgflex500

780 538

testadmin



ZYXEL

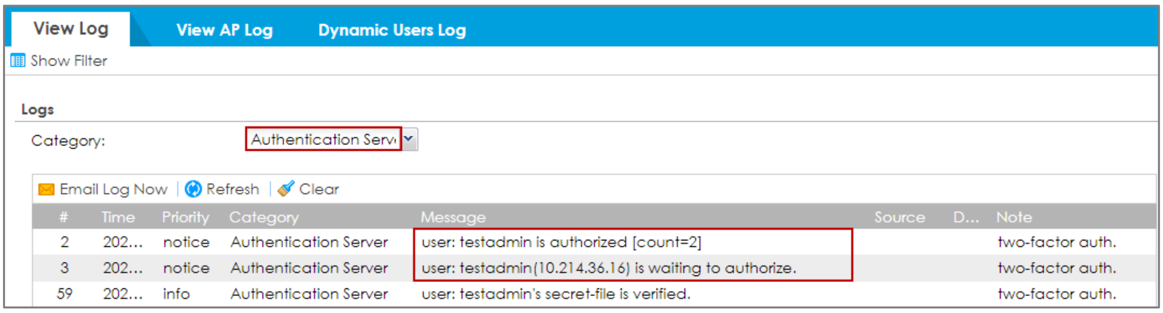
USG FLEX 500

Enter Two-factor Authentication Verification code and click to verify.

780538

4. Authorize with username, password and the token code successfully.

MONITOR > Log > View Log > Category and select "Authentication Server"



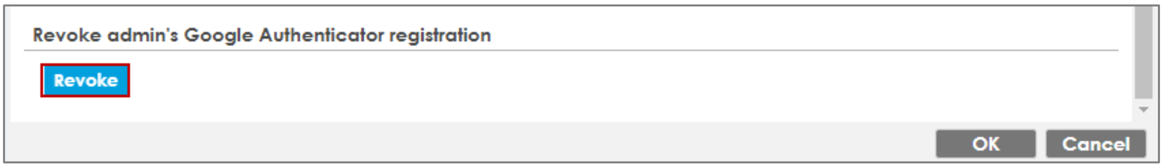
Logs

Category: Authentication Serv

#	Time	Priority	Category	Message	Source	D...	Note
2	202...	notice	Authentication Server	user: testadmin is authorized [count=2]			two-factor auth.
3	202...	notice	Authentication Server	user: testadmin(10.214.36.16) is waiting to authorize.			two-factor auth.
59	202...	info	Authentication Server	user: testadmin's secret-file is verified.			two-factor auth.

What Can Go Wrong?

1. An admin user only can be registered on one Google Authenticator. If you would like to use another mobile device to authenticate the same admin user, click “Revoke” to revoke registered user and user another mobile device to set up Google Authenticator again.

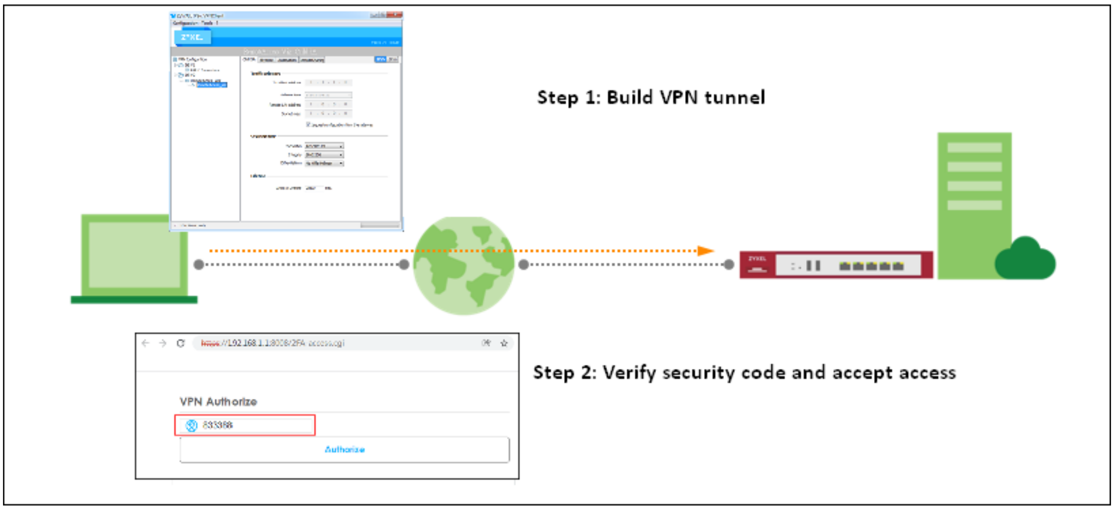


Revoke admin's Google Authenticator registration

2. Each admin user has 5 backup codes and each backup code could be used only once for login.

How to Use Two Factor with Google Authenticator for VPN Access

In previous firmware versions, USG supports pin code by SMS/Email as two-factor authentication method. However, SMS-based two-factor authentication is not safe. Compared to SMS-based method, Google authenticator is the most secure method to receive verification code for 2-factor authentication. Google authenticator gives a new code every 30 seconds, so each code expires in just 30 seconds which make it a secure option to generate codes for 2-step verification. Furthermore, Google authenticator is free to download, easy to use, and is able to work without Internet. This example illustrates how to set up two factor with Google Authenticator for VPN access.


Step 1: Build VPN tunnel
https://192.168.1.1:8008/2FA-access.cgi
VPN Authorize
833388
Authorize
Step 2: Verify security code and accept access

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses. This example was tested using the USG FLEX 500 (Firmware Version: ZLD 5.20).

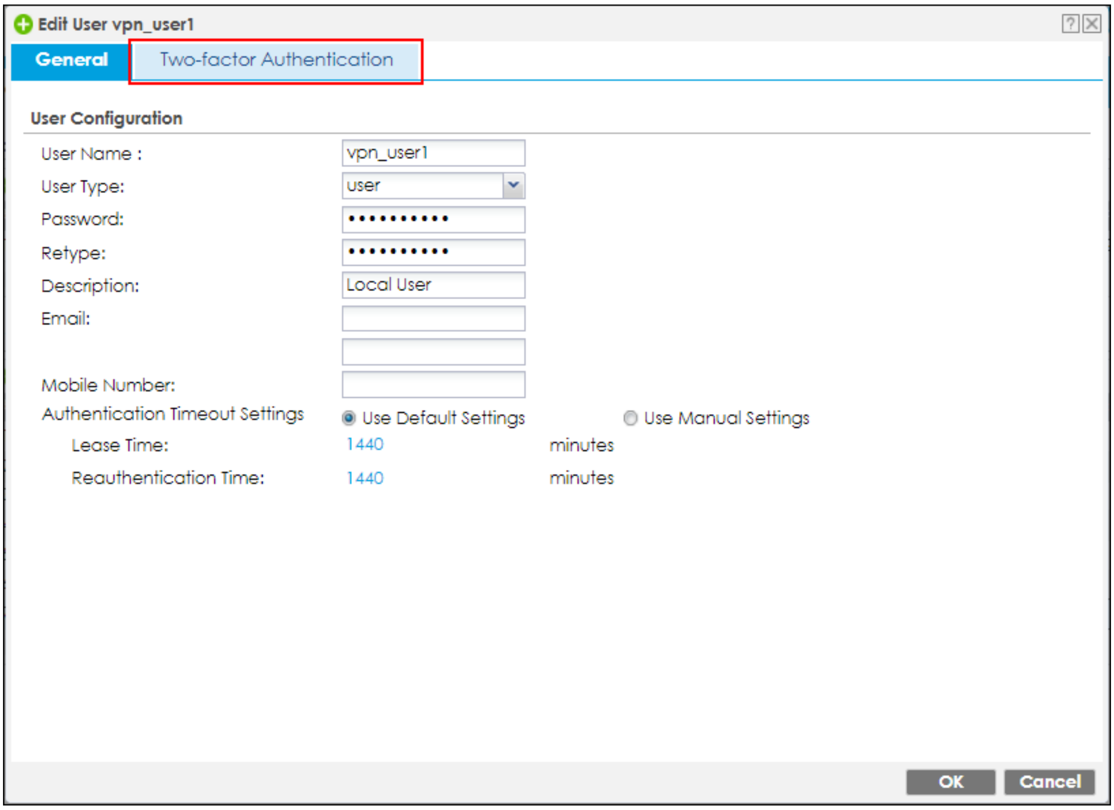
Two Factor with Google Authenticator Flow

1. Enable Google Authentication on user
2. Set up Google Authenticator
3. Configure valid time and login service types

Enable Google Authentication on user

Select a VPN user and switch to Two-factor Authentication tab.

CONFIGURATION > Object > User/Group > User, create a new user



User Configuration

User Name : vpn_user1

User Type: user

Password: ••••••••••

Retype: ••••••••••

Description: Local User

Email:

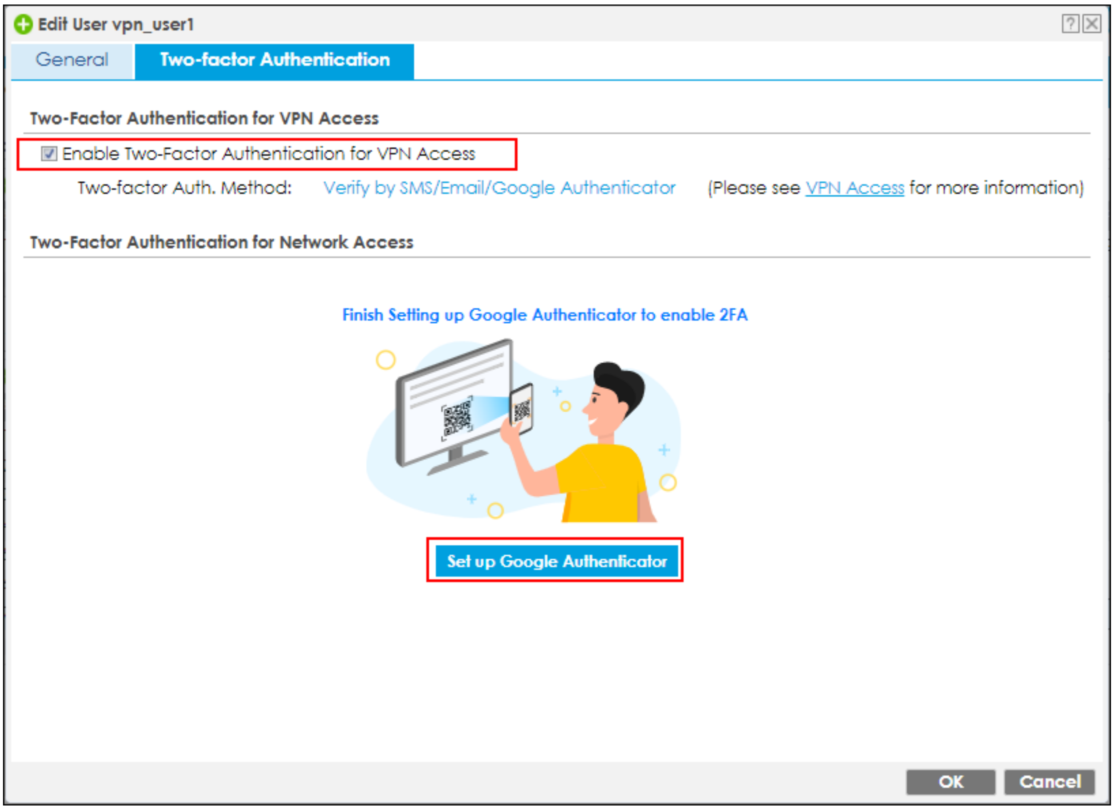
Mobile Number:

Authentication Timeout Settings ● Use Default Settings ○ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Enable Two-Factor Authentication for VPN Access checkbox.



Edit User vpn_user1

Two-Factor Authentication for VPN Access

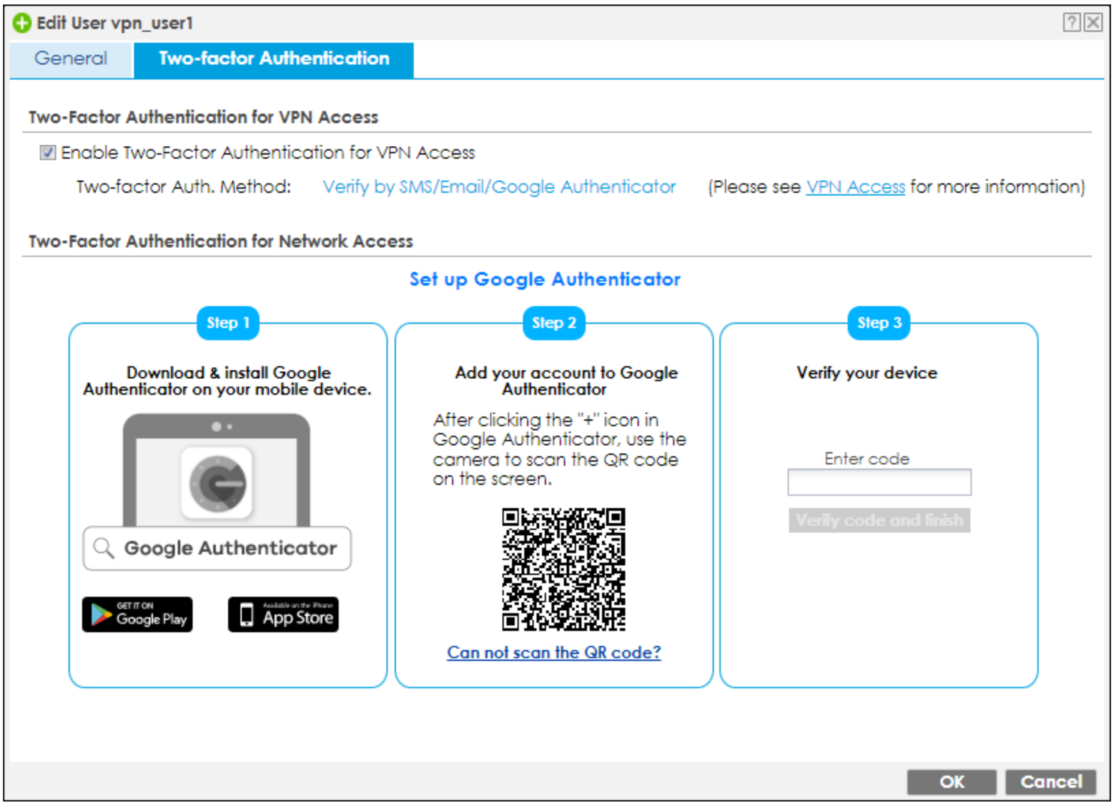
☑ Enable Two-Factor Authentication for VPN Access

Two-factor Auth. Method: Verify by SMS/Email/Google Authenticator (Please see VPN Access for more information)

Two-Factor Authentication for Network Access

Finish Setting up Google Authenticator to enable 2FA

Set up Google Authenticator



Edit User vpn_user1

Two-Factor Authentication for VPN Access

☑ Enable Two-Factor Authentication for VPN Access

Two-factor Auth. Method: Verify by SMS/Email/Google Authenticator (Please see VPN Access for more information)

Two-Factor Authentication for Network Access

Set up Google Authenticator

Step 1

Download & install Google Authenticator on your mobile device.

Step 2

Add your account to Google Authenticator

After clicking the "+" icon in Google Authenticator, use the camera to scan the QR code on the screen.

Can not scan the QR code?

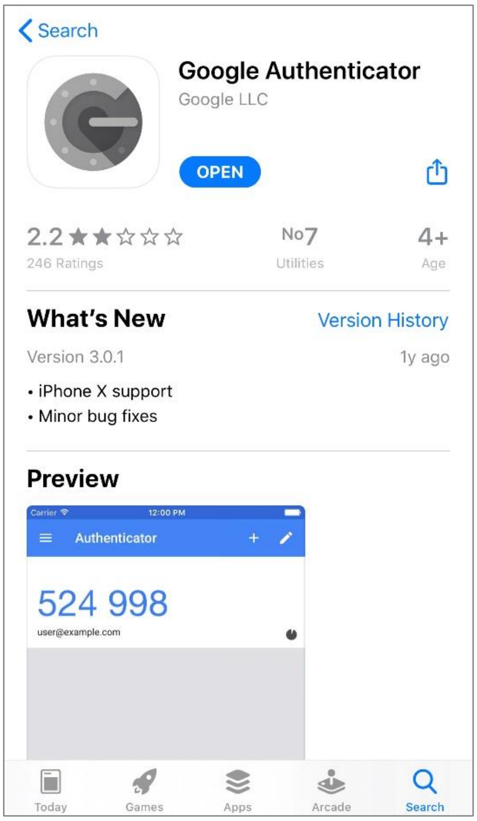
Step 3

Verify your device

Enter code

1. Download and install Google Authenticator on your mobile device.

Apple Store



Search

Google Authenticator

Google LLC

OPEN

2.2 ★★☆☆☆ 246 Ratings

No7 Utilities

4+ Age

What's New

Version History

Version 3.0.1

1y ago

- iPhone X support
- Minor bug fixes

Preview

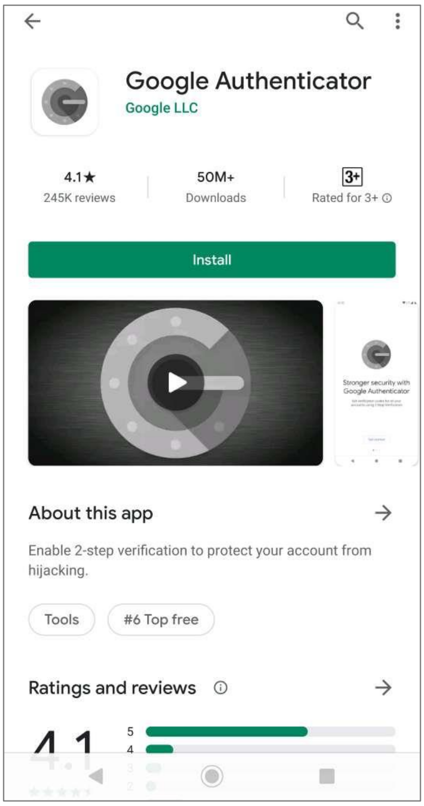
Carrier 12:00 PM

Authenticator

524 998

user@example.com

Google Play



Google Authenticator

Google LLC

4.1★ 245K reviews

50M+ Downloads

3+ Rated for 3+

Install

About this app

Enable 2-step verification to protect your account from hijacking.

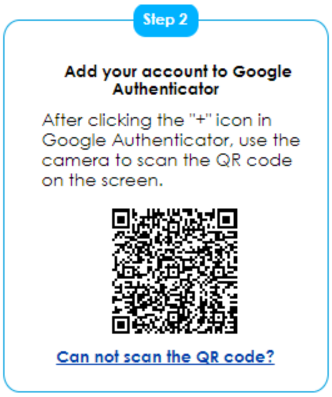
Tools

#6 Top free

Ratings and reviews

4.1

2. Register the VPN user account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.

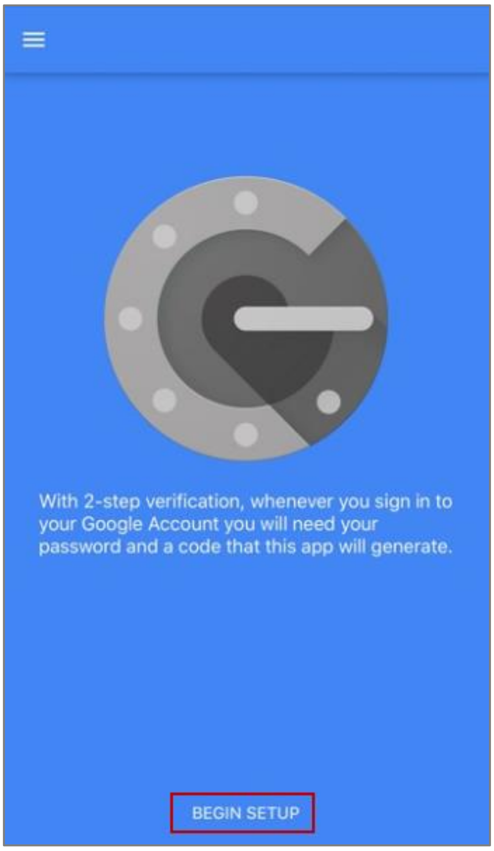


Step 2

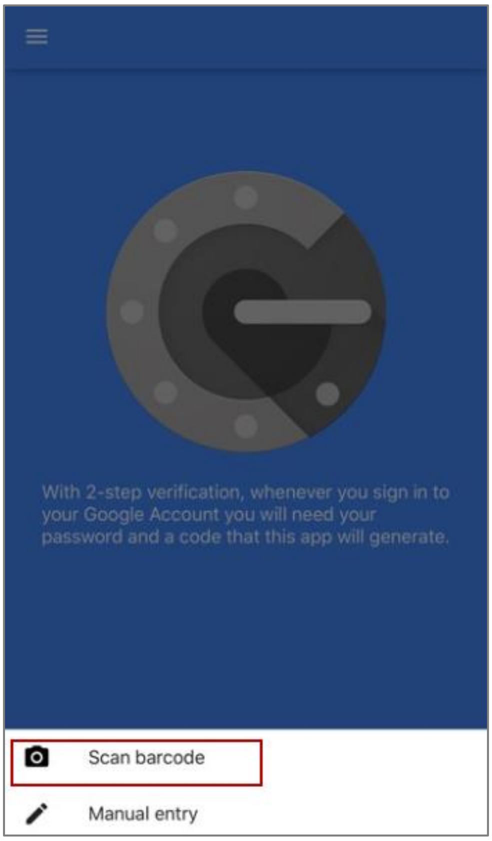
Add your account to Google Authenticator

After clicking the "+" icon in Google Authenticator, use the camera to scan the QR code on the screen.

Can not scan the QR code?

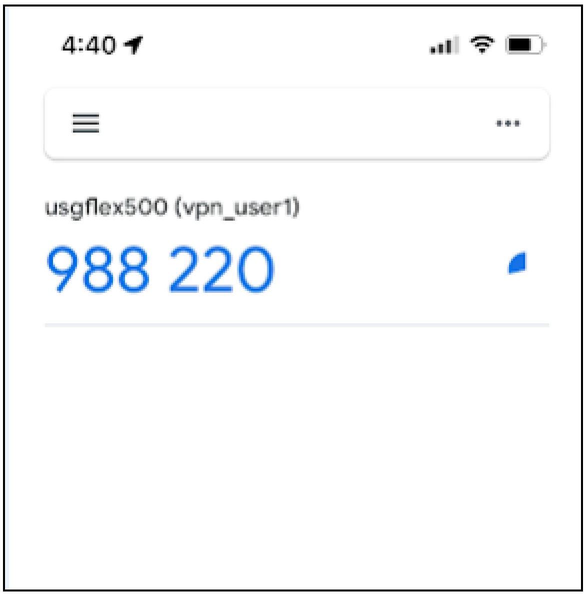


With 2-step verification, whenever you sign in to your Google Account you will need your password and a code that this app will generate.



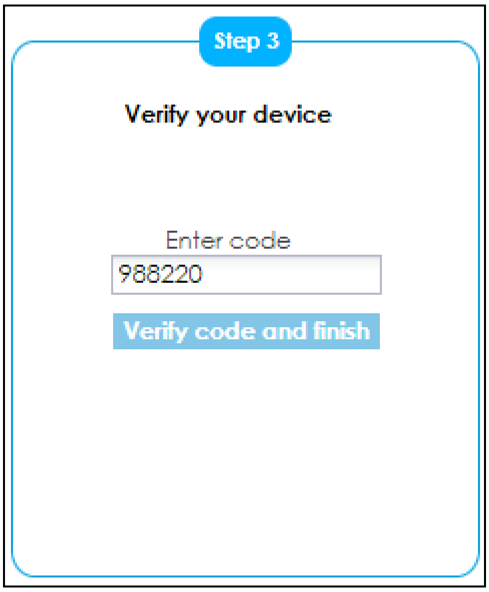
With 2-step verification, whenever you sign in to your Google Account you will need your password and a code that this app will generate.

3. Enter the token code which displays on Google Authenticator to "Step 3" and click "Verify code and finish" to submit and verify the code.



usgflex500 (vpn_user1)

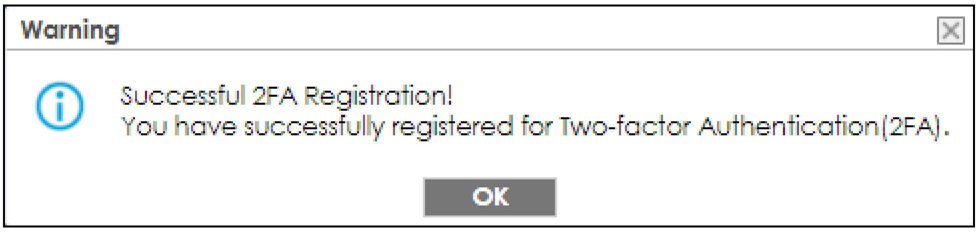
988 220



Verify your device

Enter code: 988220

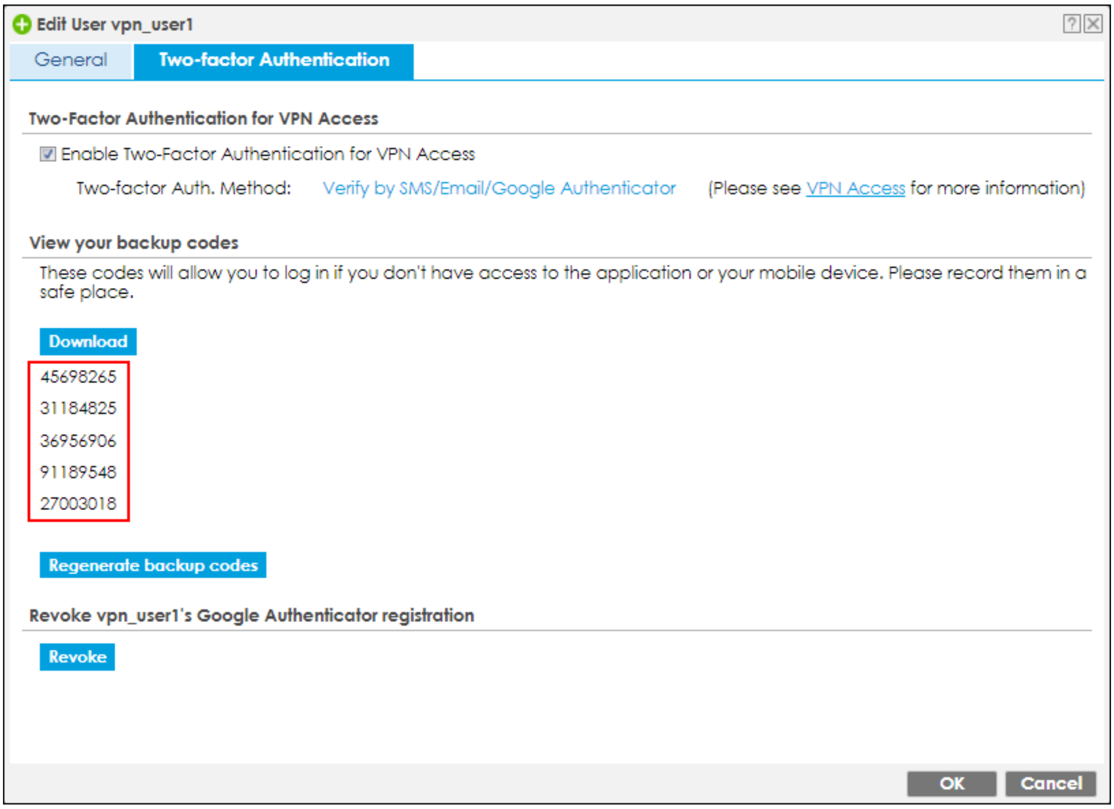
The pop-up window message informs the verification result.



Warning

Successful 2FA Registration!
You have successfully registered for Two-factor Authentication(2FA).

4. After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.



Edit User vpn_user1

Two-Factor Authentication for VPN Access

☑ Enable Two-Factor Authentication for VPN Access

Two-factor Auth. Method: Verify by SMS/Email/Google Authenticator (Please see VPN Access for more information)

View your backup codes

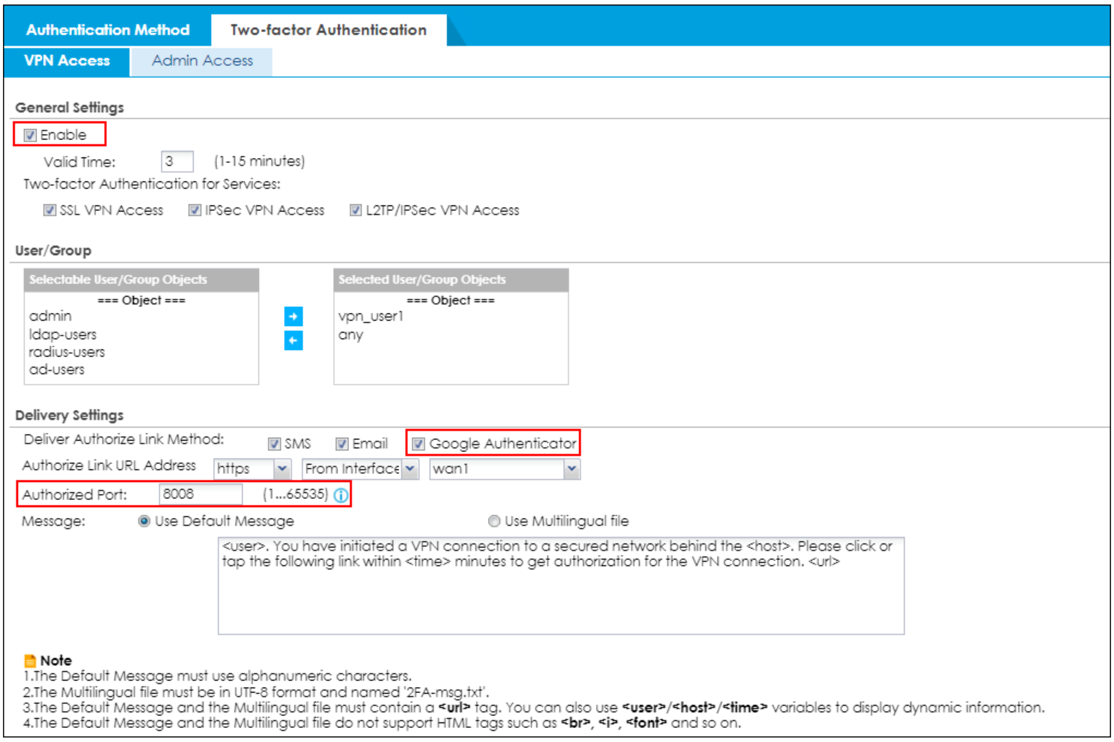
These codes will allow you to log in if you don't have access to the application or your mobile device. Please record them in a safe place.

45698265
31184825
36956906
91189548
27003018

Revoke vpn_user1's Google Authenticator registration

Configure valid time and login service types

Enable two factor authentication for VPN access. Configure valid time and select which VPN types require two-factor authentication for VPN user. The valid time is the deadline that user needs to submit the two-factor authentication code to get the VPN access. The request is rejected if submitting the code later than valid time. By default, the valid time is 3 minutes. The authentication page is working on specific service port. After building up VPN tunnel, user have to enter the code in the Web GUI.



General Settings

☑ Enable

Valid Time: 3 (1-15 minutes)

Two-factor Authentication for Services:

☑ SSL VPN Access ☑ IPSec VPN Access ☑ L2TP/IPSec VPN Access

User/Group

Selectable User/Group Objects	Selected User/Group Objects
=== Object ===	=== Object ===
admin	vpn_user1
ldap-users	any
radius-users	
ad-users	

Delivery Settings

Deliver Authorize Link Method: ☑ SMS ☑ Email ☑ Google Authenticator

Authorize Link URL Address https From Interface wan1

Authorized Port: 8008 (1...65535)

Message: ● Use Default Message ○ Use Multilingual file

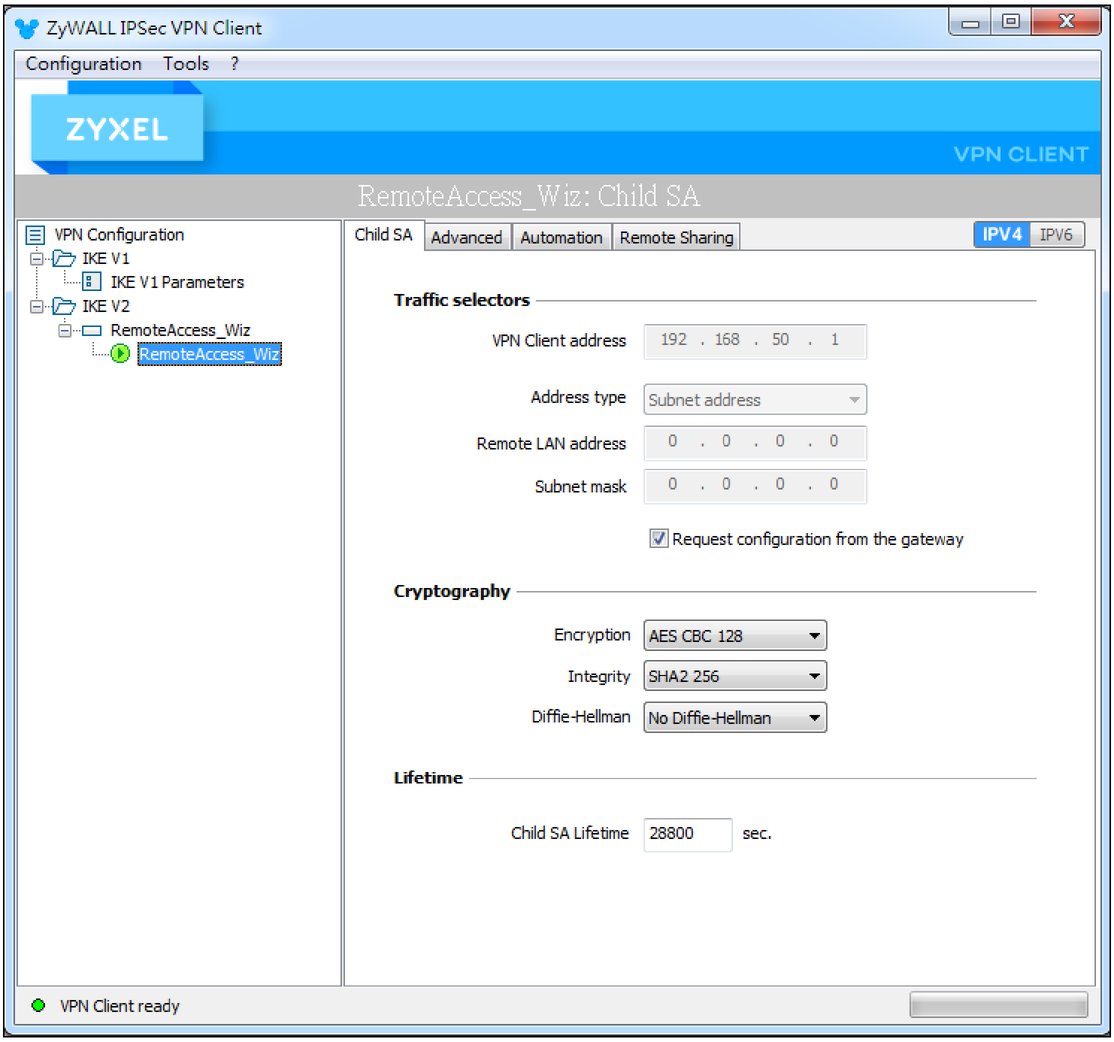
<user>. You have initiated a VPN connection to a secured network behind the <host>. Please click or tap the following link within <time> minutes to get authorization for the VPN connection. <url>

Note
1.The Default Message must use alphanumeric characters.
2.The Multilingual file must be in UTF-8 format and named '2FA-msg.txt'.
3.The Default Message and the Multilingual file must contain a **<url>** tag. You can also use **<user>**/**<host>**/**<time>** variables to display dynamic information.
4.The Default Message and the Multilingual file do not support HTML tags such as **
, **<i>, **<font>** and so on.

Note: If users use Zyxel VPN Client to build VPN tunnel, it will pop up authentication page on browser automatically. For SSL VPN or L2TP VPN, users have to enter correct URL on browser manually. (e.g. https://YourDeviceIP:8080)

Test the Result

1. Build VPN tunnel on Zyxel VPN Client.



RemoteAccess_Wiz: Child SA

Traffic selectors

VPN Client address: 192 . 168 . 50 . 1

Address type: Subnet address

Remote LAN address: 0 . 0 . 0 . 0

Subnet mask: 0 . 0 . 0 . 0

☑ Request configuration from the gateway

Cryptography

Encryption: AES CBC 128

Integrity: SHA2 256

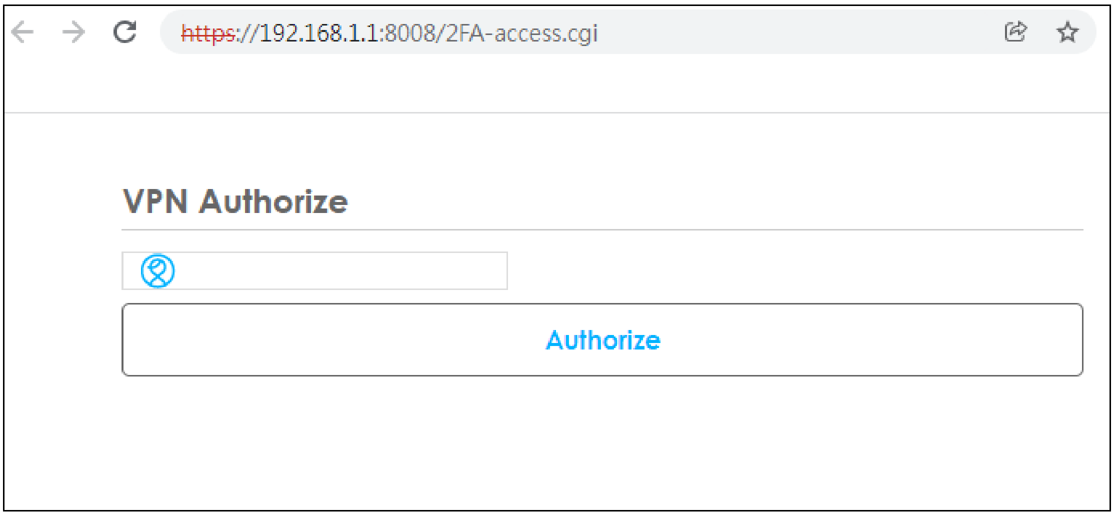
Diffie-Hellman: No Diffie-Hellman

Lifetime

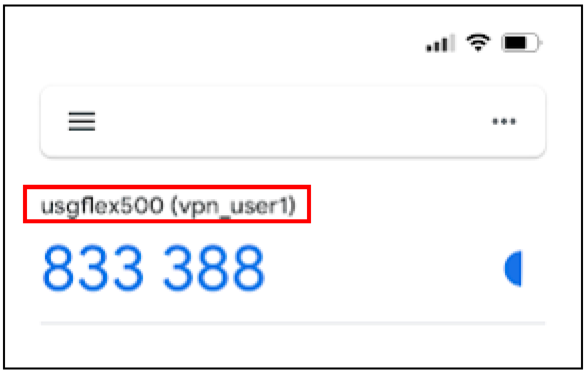
Child SA Lifetime: 28800 sec.

● VPN Client ready

2. Browser will pop up authentication page to enter the verification code.

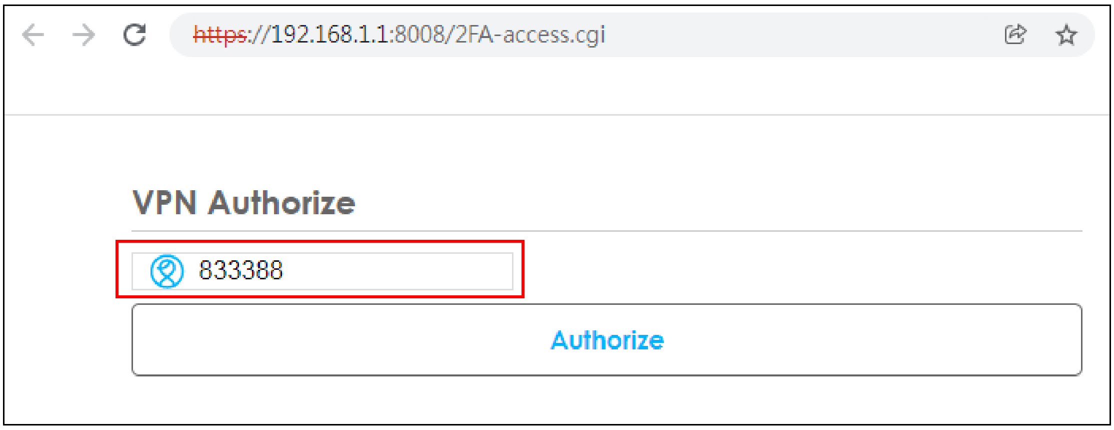


3. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.



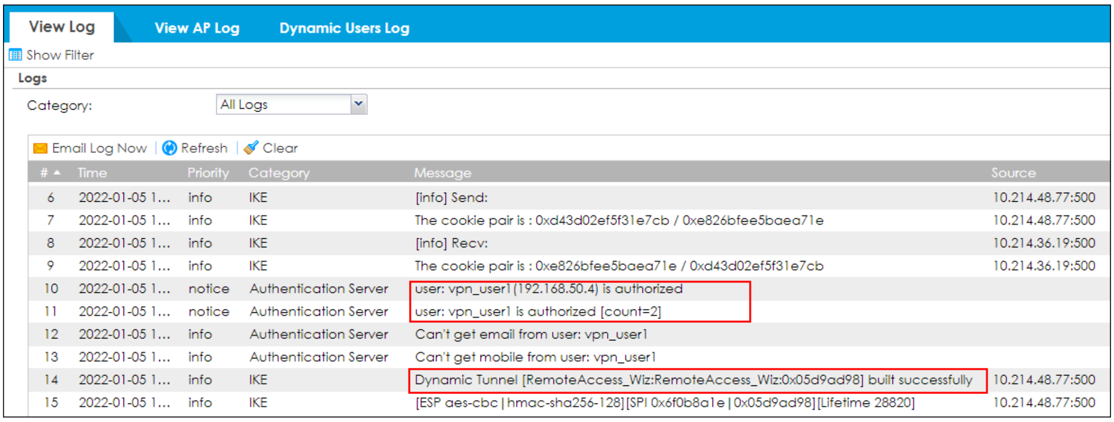
usgflex500 (vpn_user1)

833 388



833388

4. Authorize with username, password and the token code successfully.



Category: All Logs

#	Time	Priority	Category	Message	Source
6	2022-01-05 1...	info	IKE	[info] Send:	10.214.48.77:500
7	2022-01-05 1...	info	IKE	The cookie pair is : 0xd43d02ef5f31e7cb / 0xe826bfee5baea71e	10.214.48.77:500
8	2022-01-05 1...	info	IKE	[info] Recv:	10.214.36.19:500
9	2022-01-05 1...	info	IKE	The cookie pair is : 0xe826bfee5baea71e / 0xd43d02ef5f31e7cb	10.214.36.19:500
10	2022-01-05 1...	notice	Authentication Server	user: vpn_user1 (192.168.50.4) is authorized	
11	2022-01-05 1...	notice	Authentication Server	user: vpn_user1 is authorized [count=2]	
12	2022-01-05 1...	info	Authentication Server	Can't get email from user: vpn_user1	
13	2022-01-05 1...	info	Authentication Server	Can't get mobile from user: vpn_user1	
14	2022-01-05 1...	info	IKE	Dynamic Tunnel [RemoteAccess_Wiz:RemoteAccess_Wiz:0x05d9ad98] built successfully	10.214.48.77:500
15	2022-01-05 1...	info	IKE	[ESP aes-cbc | hmac-sha256-128][SPI 0x6f0b8a1e | 0x05d9ad98][Lifetime 28820]	10.214.48.77:500

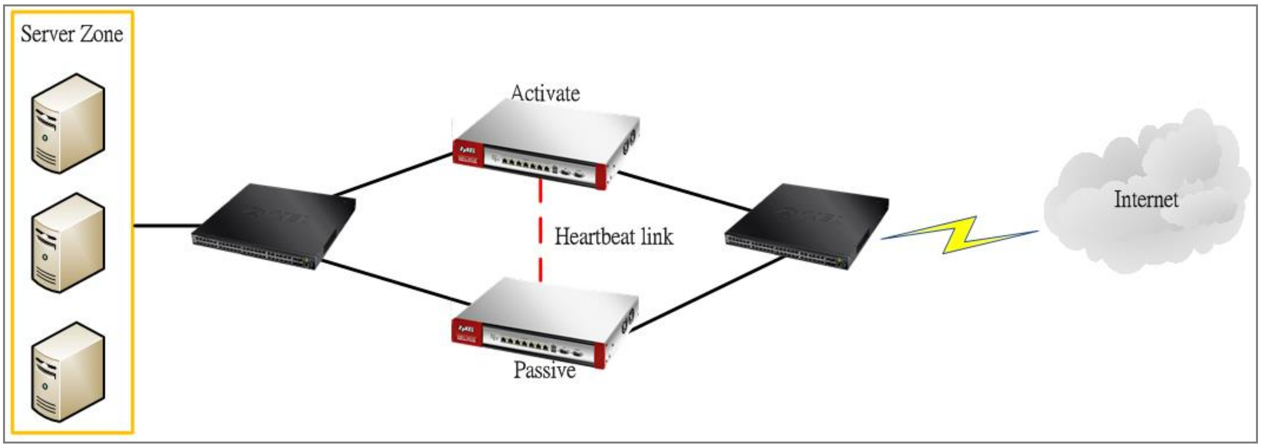
What Can Go Wrong

1. Default Authentication service port is working on 8008 port. You can customize it to others. Of course you have to allow service port (to Zywall) in your Policy Control rule.
2. Zyxel VPN Client will pop up authentication page automatically on browser. If user build VPN tunnel by SSL VPN or L2TP VPN, then user have to enter correct URL for enter verification code.
3. No matter SMS, Email or Google Authenticator are enabled, one of three types is verified then VPN user is authorized.

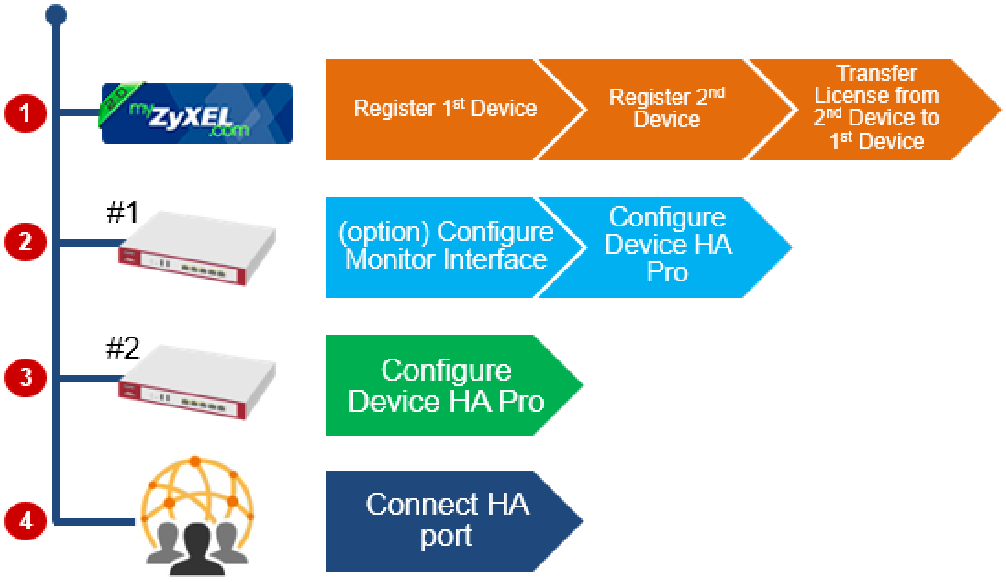
Chapter 4- Device HA

How to Configure 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 V4.25, 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.



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 become "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 Setting Screen

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

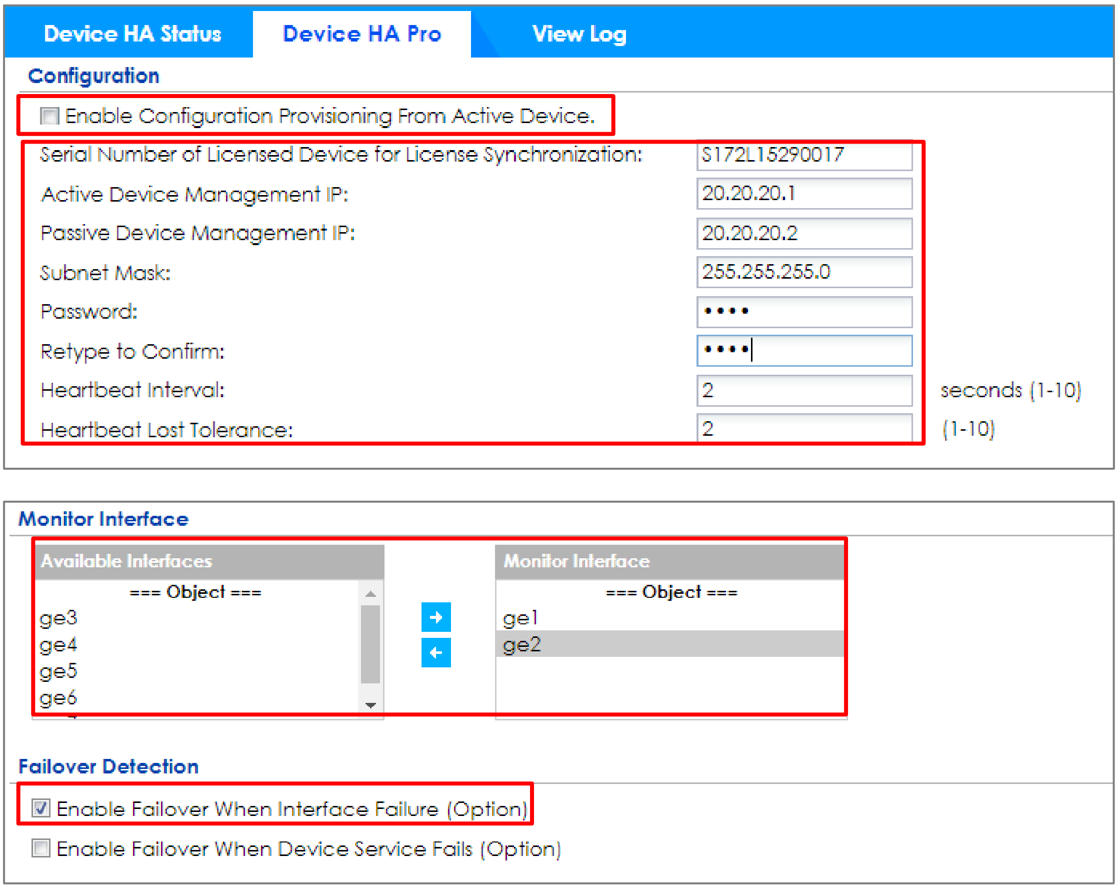
Enter the management IP address of the active and passive devices. Also, enter the password for synchronizing configuration with each other.

D. Monitoring Interfaces

Select the interfaces which you would like to monitor.

E. Synchronization

Enable failover when one of the interfaces fails.



Configuration

□ Enable Configuration Provisioning From Active Device.

Serial Number of Licensed Device for License Synchronization:	S172L15290017	
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)
Heartbeat Lost Tolerance:	2	(1-10)

Monitor Interface

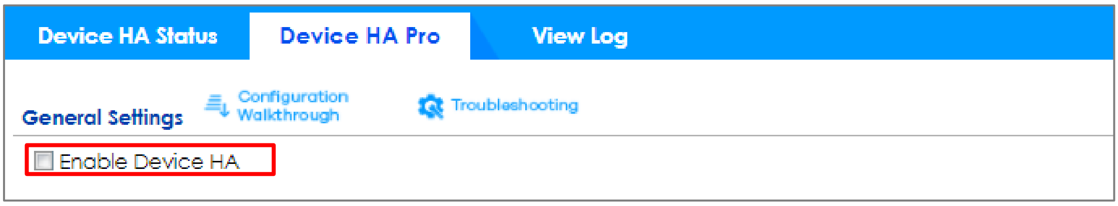
Available Interfaces	Monitor Interface
=== Object ===	=== Object ===
ge3	ge1
ge4	ge2
ge5	
ge6	

Failover Detection

☑ Enable Failover When Interface Failure (Option)

□ Enable Failover When Device Service Fails (Option)

The Main Function of the Device HA Pro



General Settings

□ Enable Device HA

Heartbeat Link

The heartbeat port is a new physical port on the device.

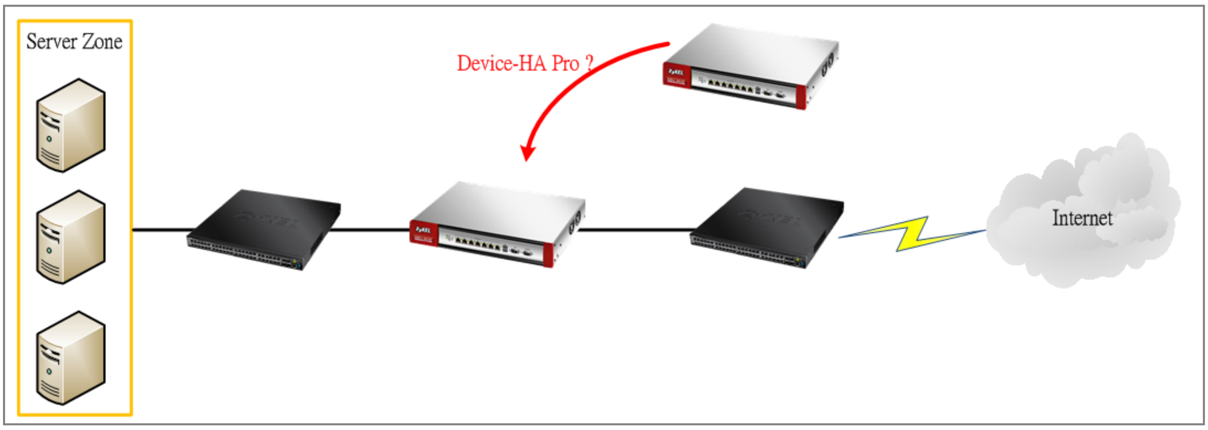
After you have enabled Device HA Pro, the devices will transmit multicast packets (UDP 694) to check each device's status.

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

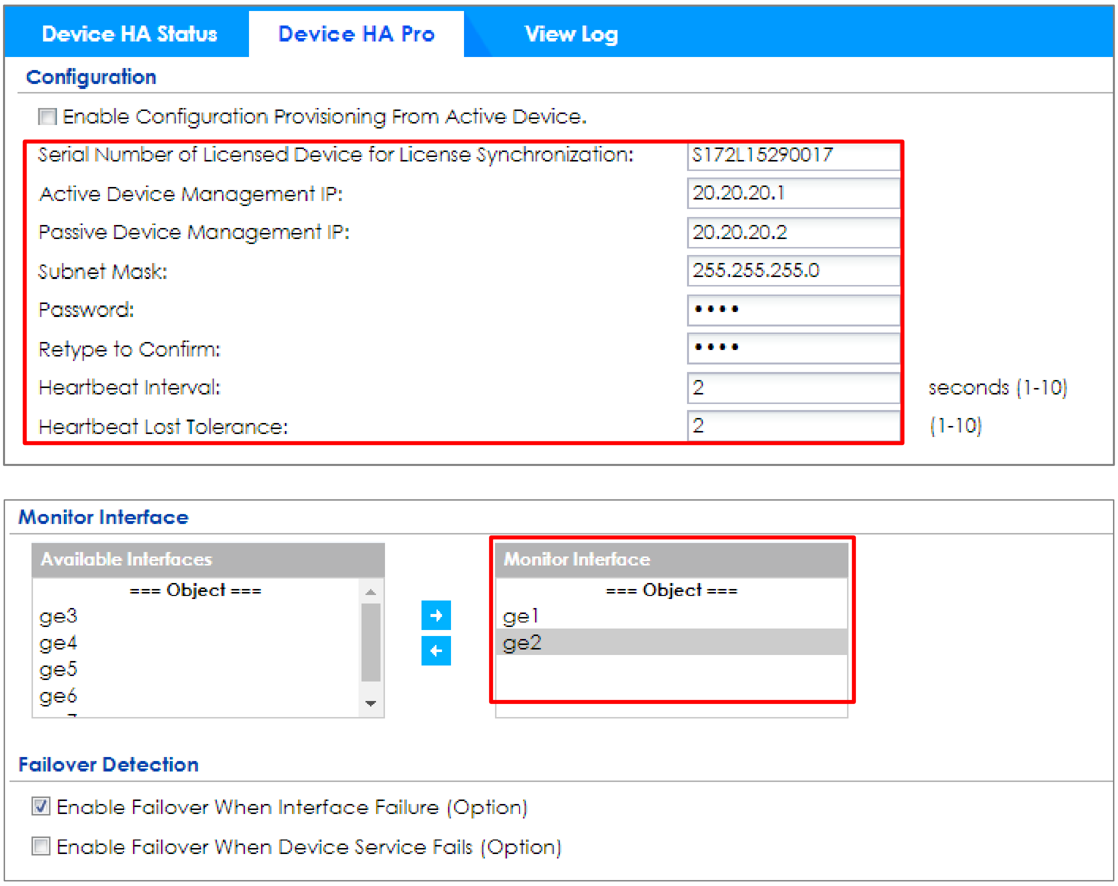
1. Transfer all the licenses to the primary device. This helps to avoid the system from recounting licenses every time.
2. Enable the connectivity check function on the monitored interfaces. When an interface doesn't receive any response from the remote server for a certain period of time, the device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

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



Configurations on the Primary Device

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



Configuration

□ Enable Configuration Provisioning From Active Device.

Serial Number of Licensed Device for License Synchronization:	S172L15290017	
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)
Heartbeat Lost Tolerance:	2	(1-10)

Monitor Interface

Available Interfaces	Monitor Interface
=== Object ===	=== Object ===
ge3	ge1
ge4	ge2
ge5	
ge6	

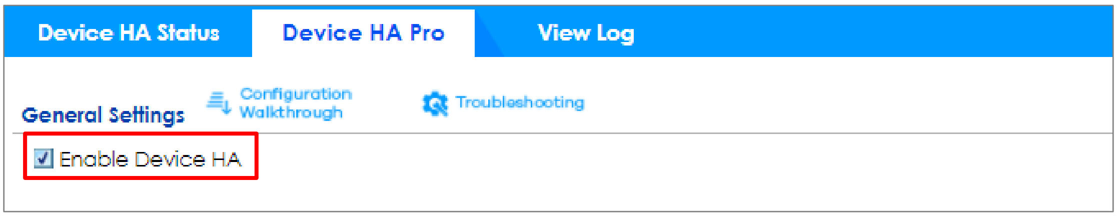
Failover Detection

☑ Enable Failover When Interface Failure (Option)

□ Enable Failover When Device Service Fails (Option)

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

Select **Enable Device HA** and click **Apply** to enable Device HA Pro.



General Settings

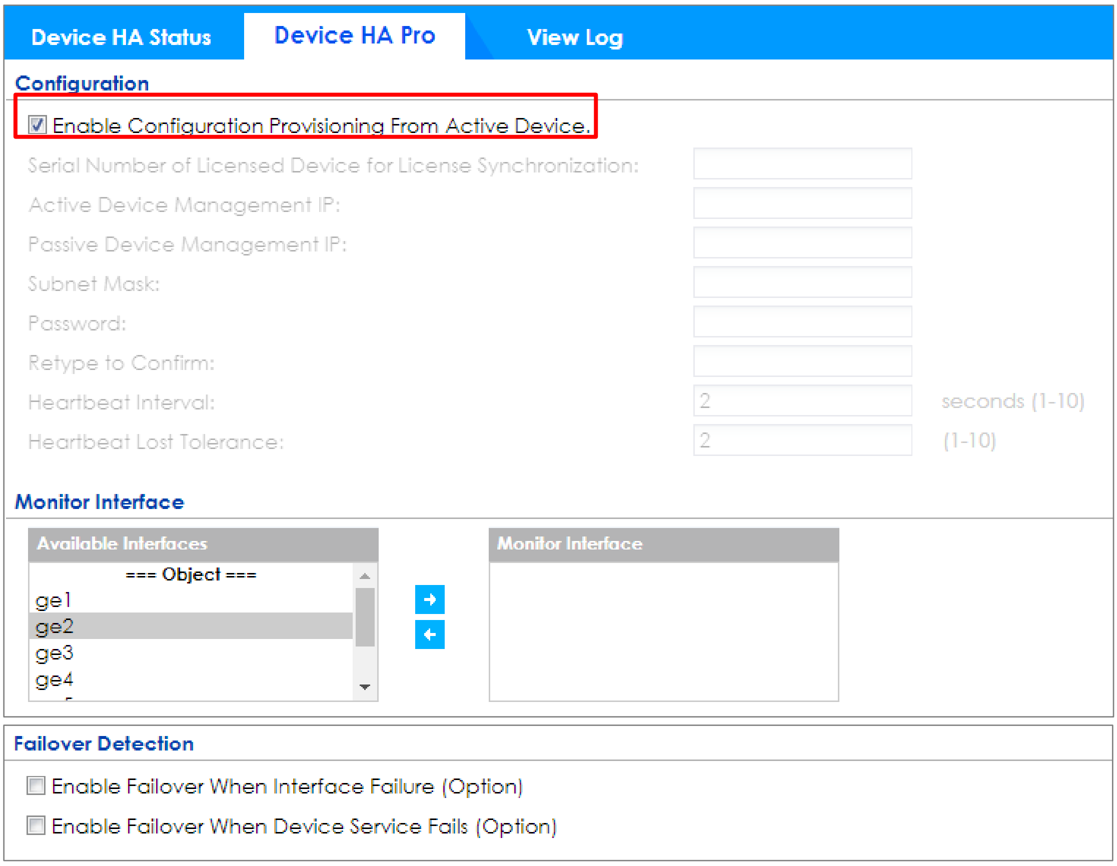
☑ Enable Device HA

Configurations on the Secondary Device

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

Select **Enable Configuration Provisioning from Active Device**.

Click **Apply**.



Configuration

☑ 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)
Heartbeat Lost Tolerance:	2	(1-10)

Monitor Interface

Available Interfaces: === Object === ge1, ge2, ge3, ge4

Monitor Interface

Failover Detection

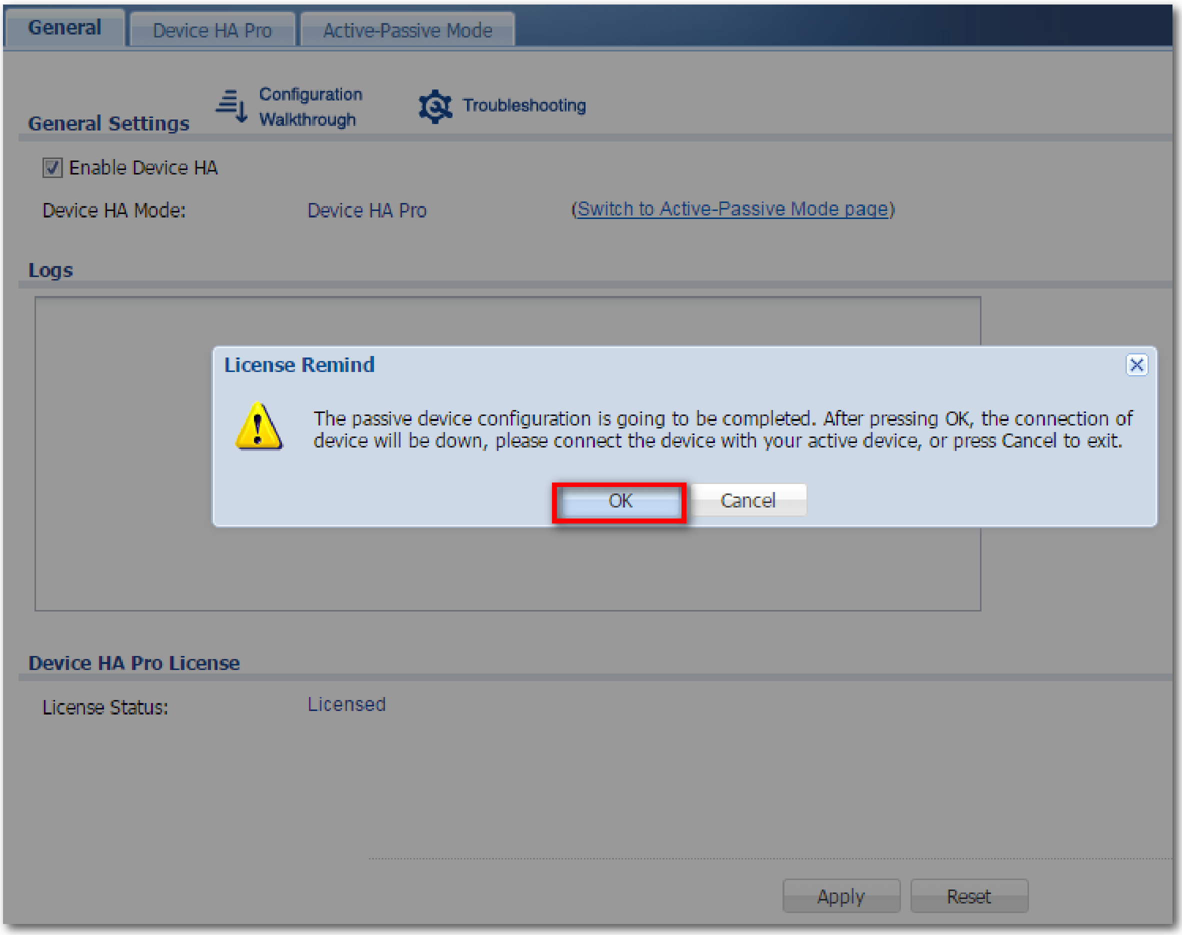
□ Enable Failover When Interface Failure (Option)

□ Enable Failover When Device Service Fails (Option)

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.



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

1. 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.

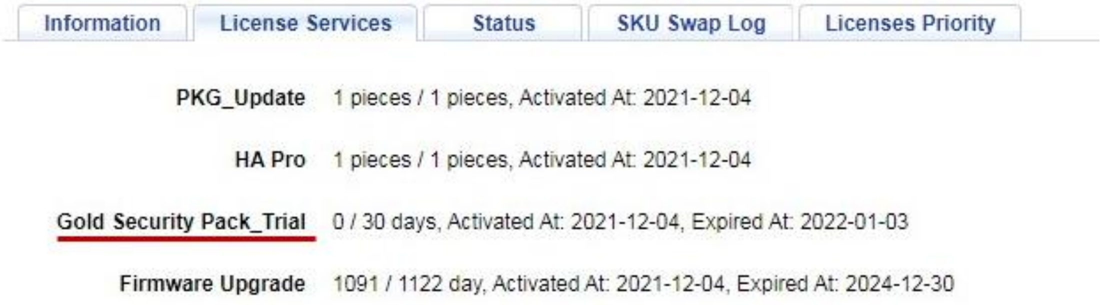
What can go wrong?

1. **Why I can't see correct license status from myzyxel.com server?**

   On the Device-HA Pro setting, there is a function "Serial number of the licensed device for license synchronization". You should enter device's S/N which with licenses. So you can transfer all of the licenses to "Activate" device, and entering this device's S/N in frame.

Note: The default bundled one-year Gold Security Pack license of ATP gateways is non-transferable. For Device HA deployment, please contact Zyxel support in your country/region to help you transfer licenses. https://www.zyxel.com/where_to_buy/where-to-buy.shtml. Without license transfer, the default bundled UTM license or Gold Security Pack license on the secondary

After licenses are transferred to the primary device, the secondary device has Trial license only. You can login to myZyxel.com to check the license status of each device.



PKG_Update 1 pieces / 1 pieces, Activated At: 2021-12-04

HA Pro 1 pieces / 1 pieces, Activated At: 2021-12-04

Gold Security Pack_Trial 0 / 30 days, Activated At: 2021-12-04, Expired At: 2022-01-03

Firmware Upgrade 1091 / 1122 day, Activated At: 2021-12-04, Expired At: 2024-12-30

2. **Why nothing happened after enabled Device-HA Pro?**

   After you enabled Device-HA Pro, the secondary device will not forward any traffic any more except the latest physical port. So you must confirm the physical port already connected with each other.

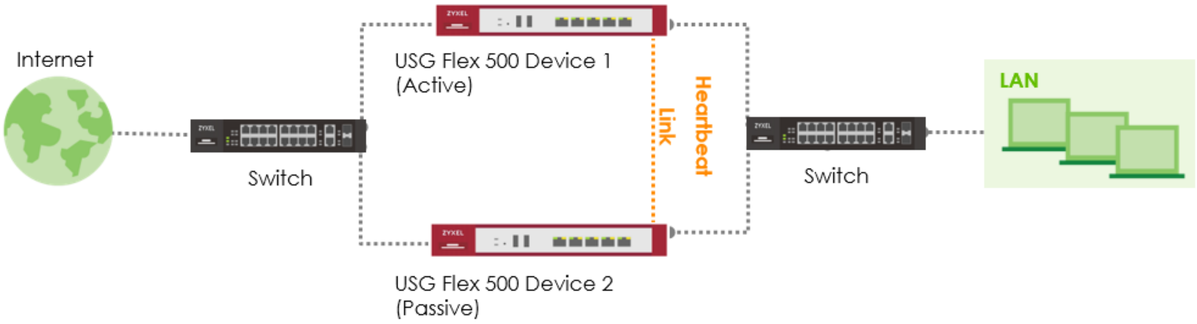
3. **Why after Device-HA failover to secondary device, it will not fallback to primary device?**

   Because Device-HA Pro purpose is for networking environment stability, so after mechanism failover to secondary device it will keeping the latest status even primary device is back. It can avoid the network service unstable.

How to Configure Schedule Reboot in Device HA

In ZLD 4.60, user can schedule device reboot one time, daily, weekly or monthly. We can apply schedule reboot to enhance device’s stability.

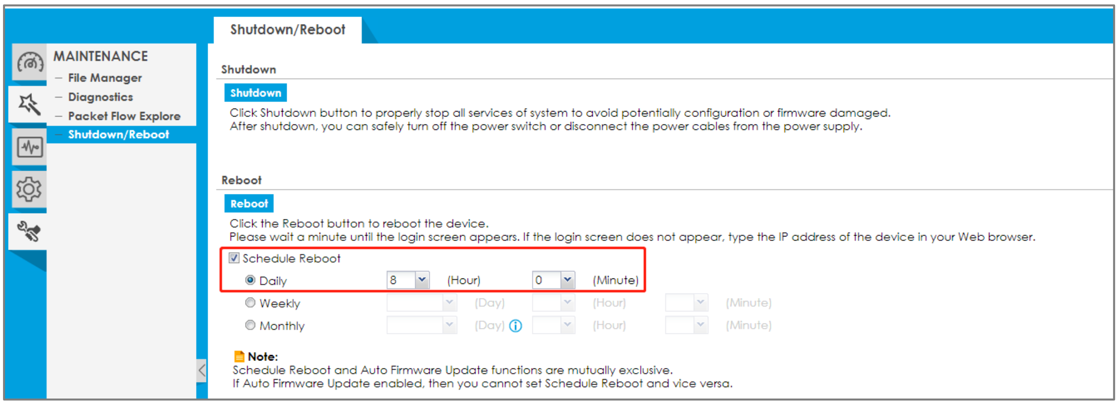
The following figure depicts Device HA scenario.



Note: Assuming Device HA had been setting ready and works perfectly for a period of time.

Configurations

Go to **MAINTENANCE** > **Shutdown/Reboot,** and enable schedule reboot. You can specify the time to reboot the device based on your requirement. In this case, we apply schedule reboot on a daily basis.



Shutdown/Reboot

Shutdown

Shutdown

Click Shutdown button to properly stop all services of system to avoid potentially configuration or firmware damaged.
After shutdown, you can safely turn off the power switch or disconnect the power cables from the power supply.

Reboot

Reboot

Click the Reboot button to reboot the device.
Please wait a minute until the login screen appears. If the login screen does not appear, type the IP address of the device in your Web browser.

☑ Schedule Reboot

● Daily 8 (Hour) 0 (Minute)

○ Weekly (Day) (Hour) (Minute)

○ Monthly (Day) (Hour) (Minute)

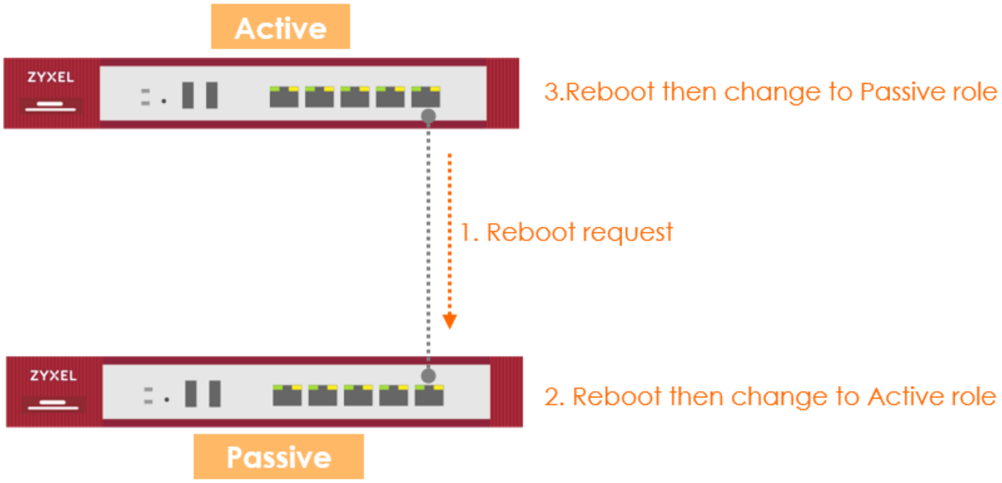
Note:
Schedule Reboot and Auto Firmware Update functions are mutually exclusive.
If Auto Firmware Update enabled, then you cannot set Schedule Reboot and vice versa.

Verification

When you enable schedule reboot in Device HA mode, the active device will send reboot request to passive device first.

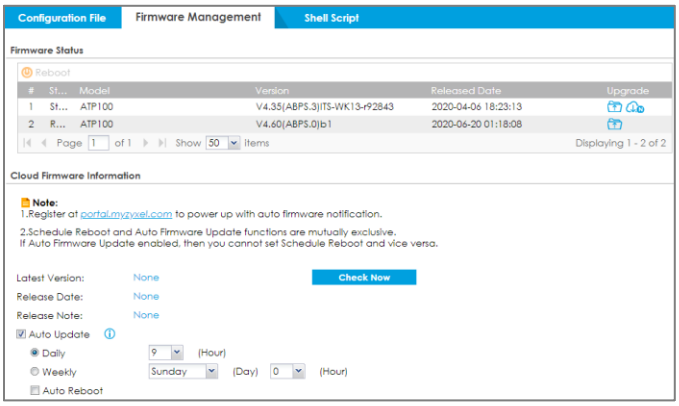
After passive device reboot successfully, the passive device changes to active role.

The original active device then reboots and changes to passive role afterward.
If the passive device fails to reboot, the active device will reject the reboot process and show a log: “schedule reboot, device-HA reboot sync fail”


Active
ZYXEL
3.Reboot then change to Passive role
1. Reboot request
ZYXEL
2. Reboot then change to Active role
Passive

What could go wrong

Schedule Reboot and Auto Firmware Upgrade are mutually exclusive, so if Auto Firmware Update enabled, then you cannot set Schedule Reboot and vice versa.



Firmware Status

Reboot

#	St...	Model	Version	Released Date	Upgrade
1	St...	ATP100	V4.35(ABPS.3)ITS-WK13-r92843	2020-04-06 18:23:13	
2	R...	ATP100	V4.60(ABPS.0)b1	2020-06-20 01:18:08	

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

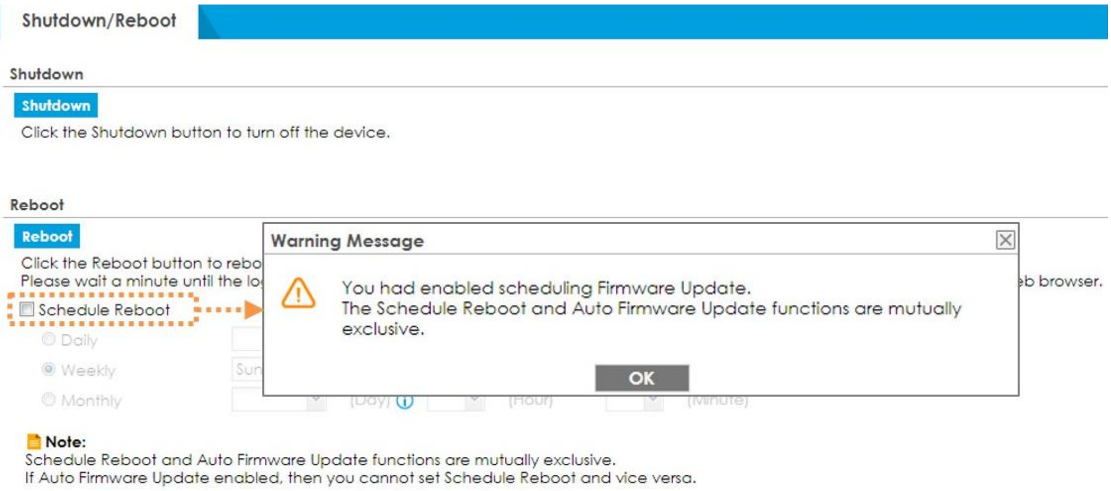
Cloud Firmware Information

Note:
1.Register at portal.myzyxel.com to power up with auto firmware notification.
2.Schedule Reboot and Auto Firmware Update functions are mutually exclusive.
If Auto Firmware Update enabled, then you cannot set Schedule Reboot and vice versa.

Latest Version: None
Release Date: None
Release Note: None

Check Now

☑ Auto Update
● Daily 9 (Hour)
○ Weekly Sunday (Day) 0 (Hour)
□ Auto Reboot



Shutdown/Reboot

Shutdown

Click the Shutdown button to turn off the device.

Reboot

Click the Reboot button to rebo

Please wait a minute until the lo ...b browser.

□ Schedule Reboot

Warning Message

You had enabled scheduling Firmware Update.
The Schedule Reboot and Auto Firmware Update functions are mutually exclusive.

Note:
Schedule Reboot and Auto Firmware Update functions are mutually exclusive.
If Auto Firmware Update enabled, then you cannot set Schedule Reboot and vice versa.

Chapter 5- IPv6

How to set up 6to4 on the WAN and autoconf on the LAN

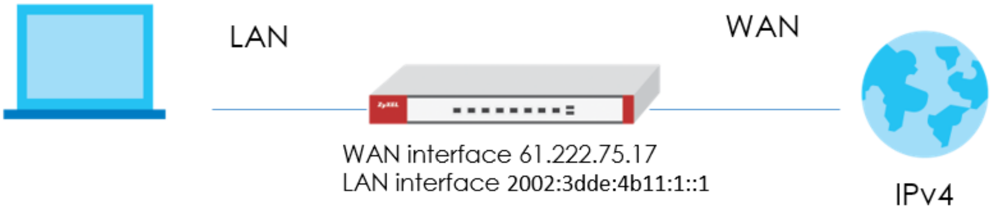
This example shows how to configure your ATP/USG Flex's WAN as IPv4 address and LAN interface as auto-configuration.

In this scenario:

WAN IPv4 Address is 61.222.75.17

DNS Server Set as 2001:4860:4860::8888

LAN Subnet Set as 2002:3dde:4b11:1::/64

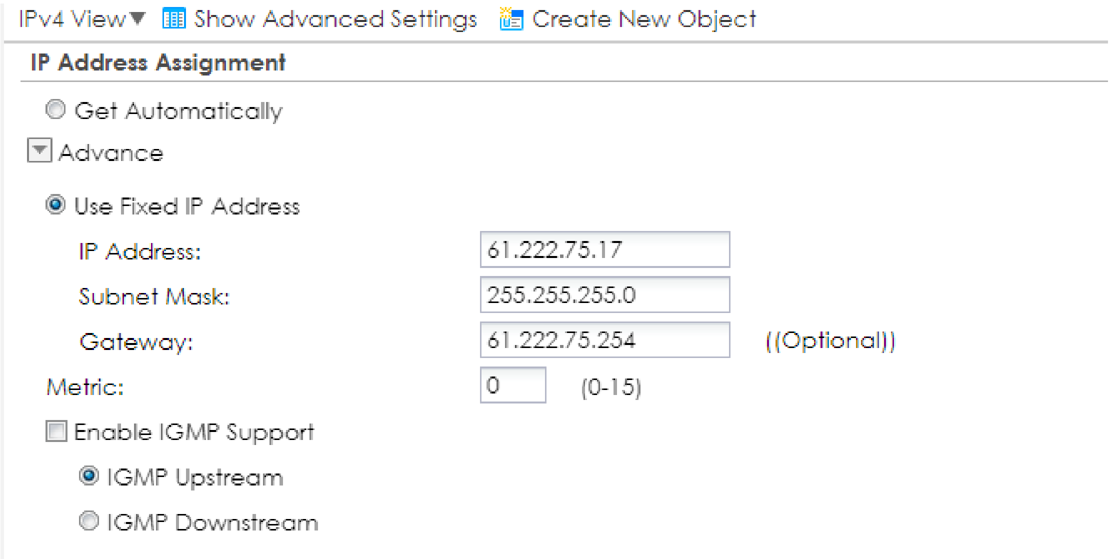


Setting Up the IPv4 Interfaces

Wan

1. In the Configuration > Ethernet > IPv4 Configuration section, double-click the WAN interface you want to modify.

2. Set a IPv4 IP address for example the below IP address is 61.222.75.17.



IPv4 View▼ Show Advanced Settings Create New Object

IP Address Assignment

○ Get Automatically

▾ Advance

● Use Fixed IP Address

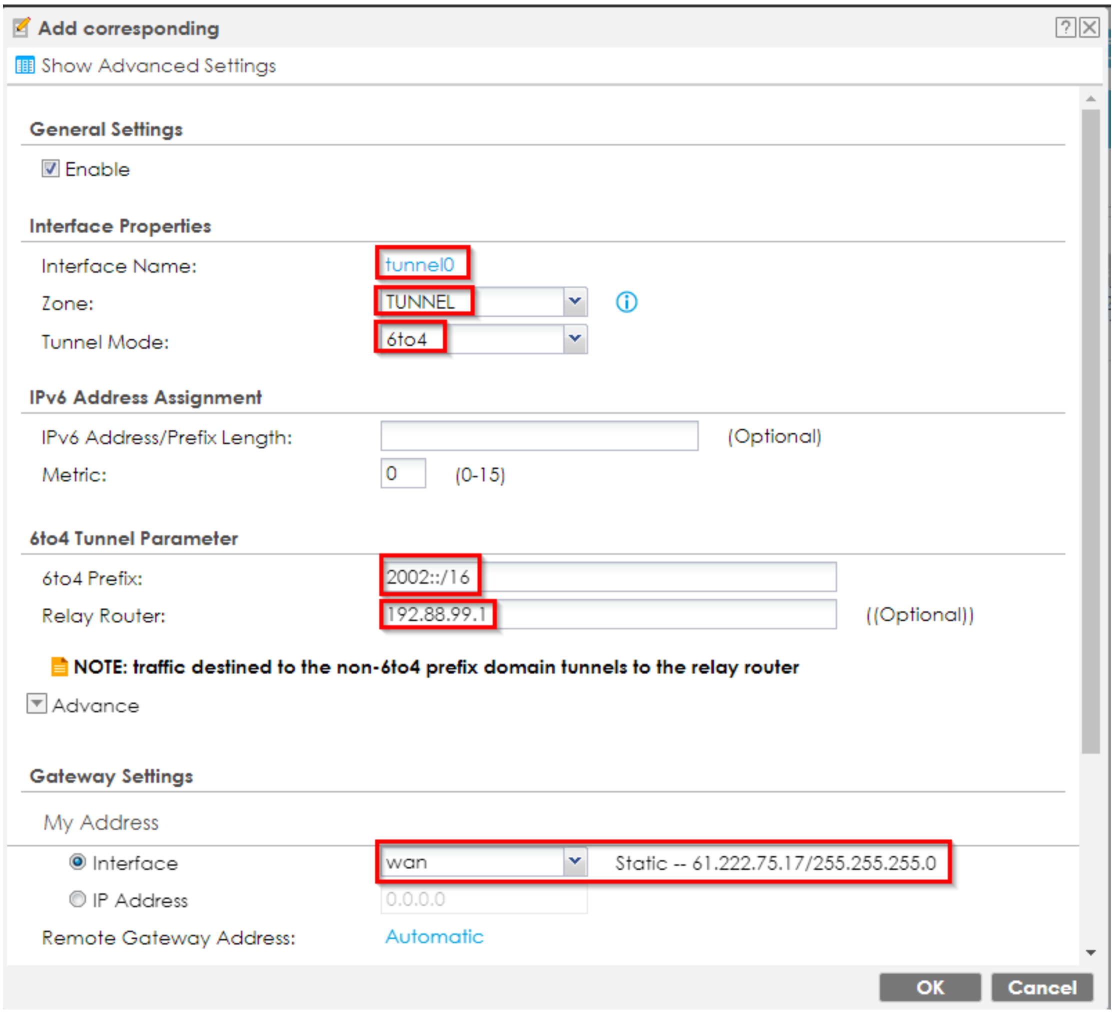
IP Address:	61.222.75.17	
Subnet Mask:	255.255.255.0	
Gateway:	61.222.75.254	((Optional))
Metric:	0	(0-15)

□ Enable IGMP Support

● IGMP Upstream

○ IGMP Downstream

3. Navigate to CONFIGURATION > Network > Interface > Tunnel > Add, Select Enable. Enter tunnel0 as the Interface Name and select 6to4 as the Tunnel Mode. In the 6to4 Tunnel Parameter section, this example just simply uses the default 6to4 Prefix, 2002:://16. Enter your Relay Router's IP address (192.88.99.1 in this example). Select wan1 as the Gateway. Click OK



Add corresponding

Show Advanced Settings

General Settings

☑ Enable

Interface Properties

Interface Name: tunnel0

Zone: TUNNEL

Tunnel Mode: 6to4

IPv6 Address Assignment

IPv6 Address/Prefix Length: (Optional)

Metric: 0 (0-15)

6to4 Tunnel Parameter

6to4 Prefix: 2002::/16

Relay Router: 192.88.99.1 ((Optional))

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

Advance

Gateway Settings

My Address

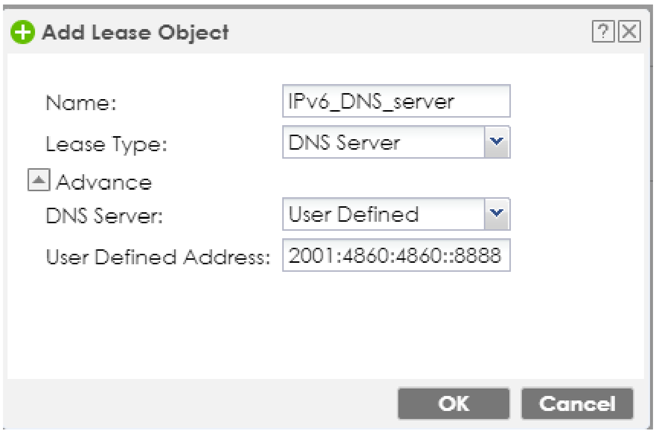
● Interface wan Static -- 61.222.75.17/255.255.255.0

○ IP Address 0.0.0.0

Remote Gateway Address: Automatic

Lan

1. Create IPv6 DHCP DNS Server object. (Configuration > Object > DHCPv6 > Lease > Add)



Add Lease Object

Name: IPv6_DNS_server

Lease Type: DNS Server

Advance

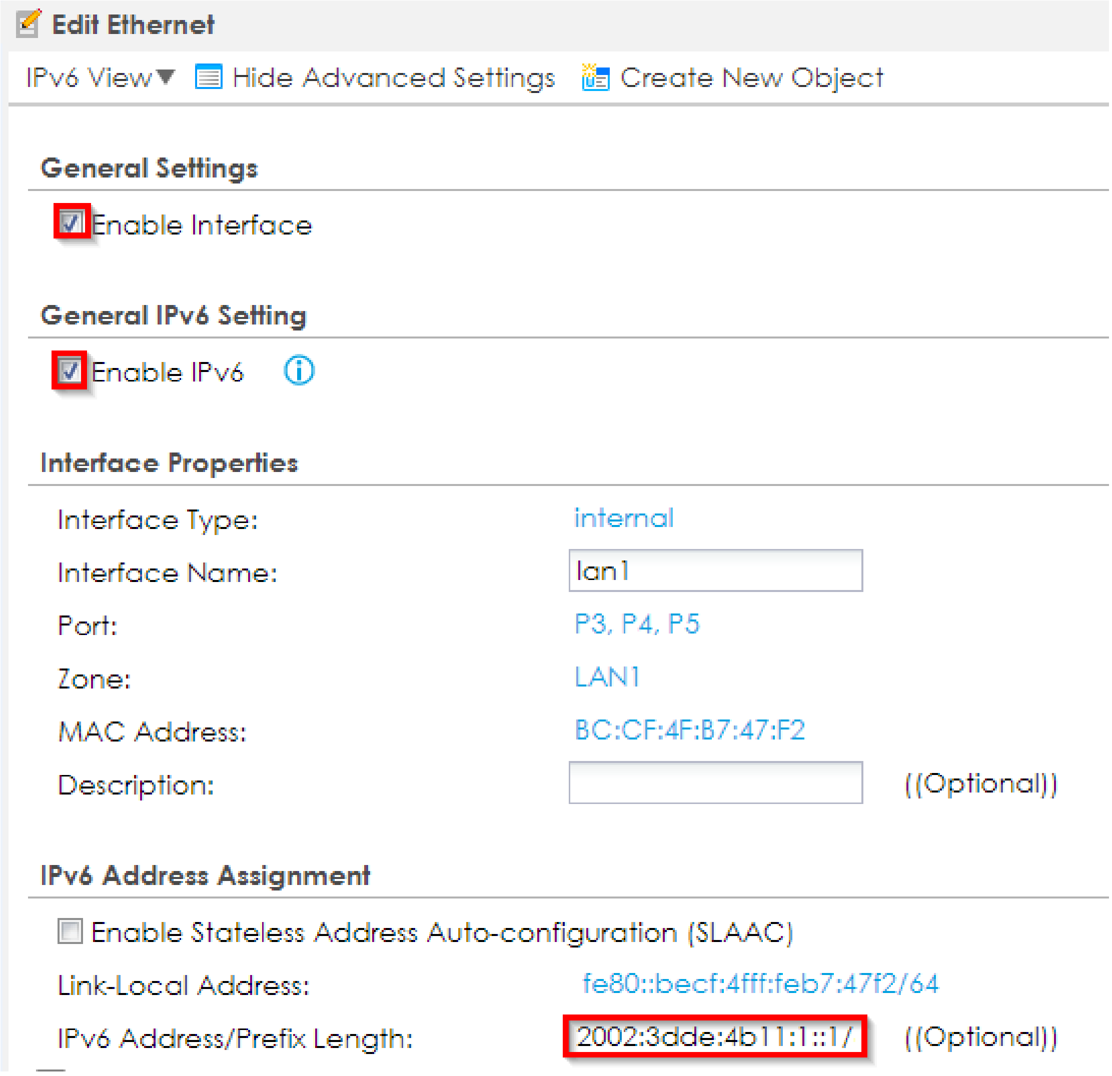
DNS Server: User Defined

User Defined Address: 2001:4860:4860::8888

In the Configuration > Ethernet > IPv6 Configuration section, double-click the LAN interface you want to modify.

2. Enable Interface and Enable IPv6.

Key in IPv6 Address/Prefix Length:2002:3dde:4b11:1::1/64



Edit Ethernet

General Settings

☑ Enable Interface

General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Type:	internal	
Interface Name:	lan1	
Port:	P3, P4, P5	
Zone:	LAN1	
MAC Address:	BC:CF:4F:B7:47:F2	
Description:		((Optional))

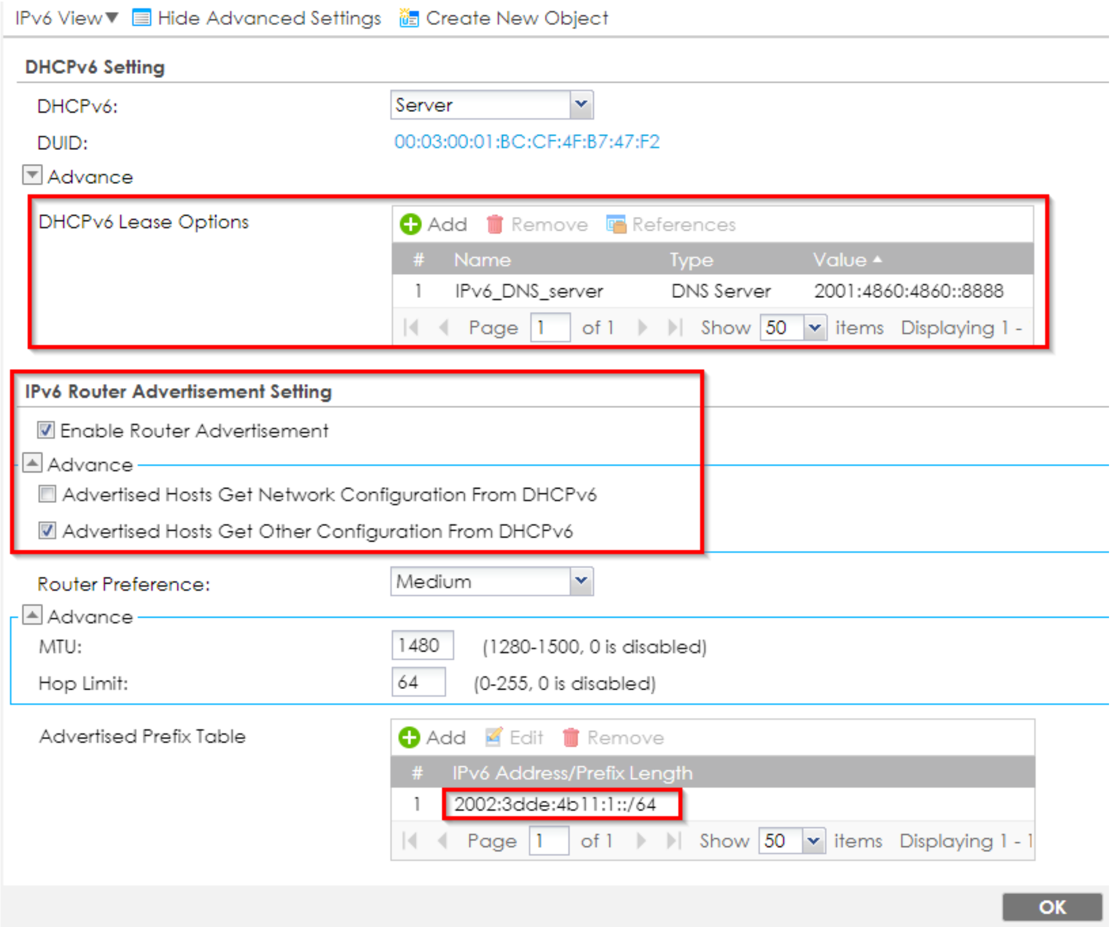
IPv6 Address Assignment

☐ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address:	fe80::becf:4fff:feb7:47f2/64	
IPv6 Address/Prefix Length:	2002:3dde:4b11:1::1/	((Optional))

3. Assign IPv6 DNS Server into DHCPv6 Lease Options.

Enable Router Advertisement and enable Advertised Host Get Other Configuration from DHCPv6 checkboxes. Key in Advertised Prefix Table: 2002:3dde:4b11:1::/64



DHCPv6 Setting

DHCPv6: Server

DUID: 00:03:00:01:BC:CF:4F:B7:47:F2

Advance

DHCPv6 Lease Options

#	Name	Type	Value ▲
1	IPv6_DNS_server	DNS Server	2001:4860:4860::8888

IPv6 Router Advertisement Setting

☑ Enable Router Advertisement

Advance

□ Advertised Hosts Get Network Configuration From DHCPv6

☑ Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

Advance

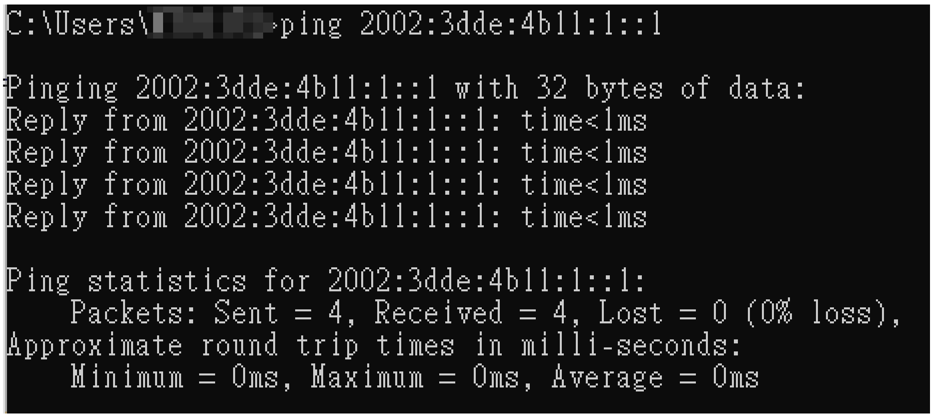
MTU: 1480 (1280-1500, 0 is disabled)

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

Advertised Prefix Table

#	IPv6 Address/Prefix Length
1	2002:3dde:4b11:1::/64

Test the result



```
C:\Users\[redacted]>ping 2002:3dde:4b11:1::1

Pinging 2002:3dde:4b11:1::1 with 32 bytes of data:
Reply from 2002:3dde:4b11:1::1: time<1ms
Reply from 2002:3dde:4b11:1::1: time<1ms
Reply from 2002:3dde:4b11:1::1: time<1ms
Reply from 2002:3dde:4b11:1::1: time<1ms

Ping statistics for 2002:3dde:4b11:1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

How to set up 6to4 on the WAN and DHCPv6 on the LAN

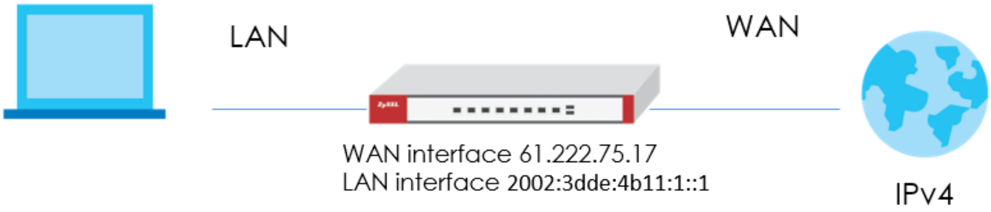
This example shows how to configure your ATP/USG Flex's WAN as IPv4 address and LAN interface as auto-configuration.

In this scenario:

WAN IPv4 Address is 61.222.75.17

DNS Server Set as 2001:4860:4860::8888

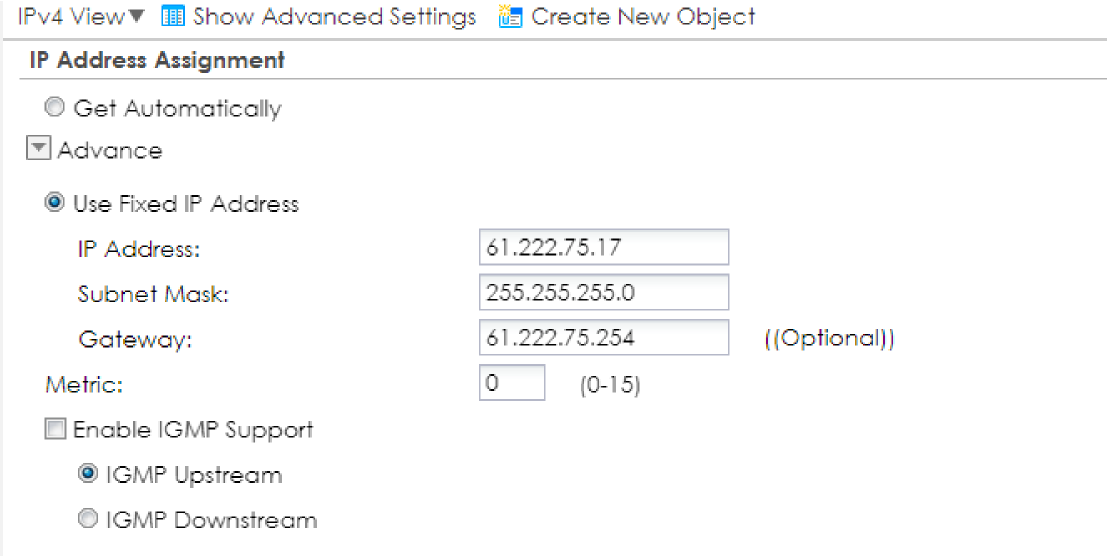
LAN Subnet Set as 2002:3dde:4b11:1::/64



Setting Up the IPv4 Interfaces

Wan

1. In the Configuration > Ethernet > IPv4 Configuration section, double-click the WAN interface you want to modify.
2. Set a IPv4 IP address for example the below IP address is 61.222.75.17.



IP Address Assignment

○ Get Automatically

Advance

● Use Fixed IP Address

IP Address: 61.222.75.17

Subnet Mask: 255.255.255.0

Gateway: 61.222.75.254 ((Optional))

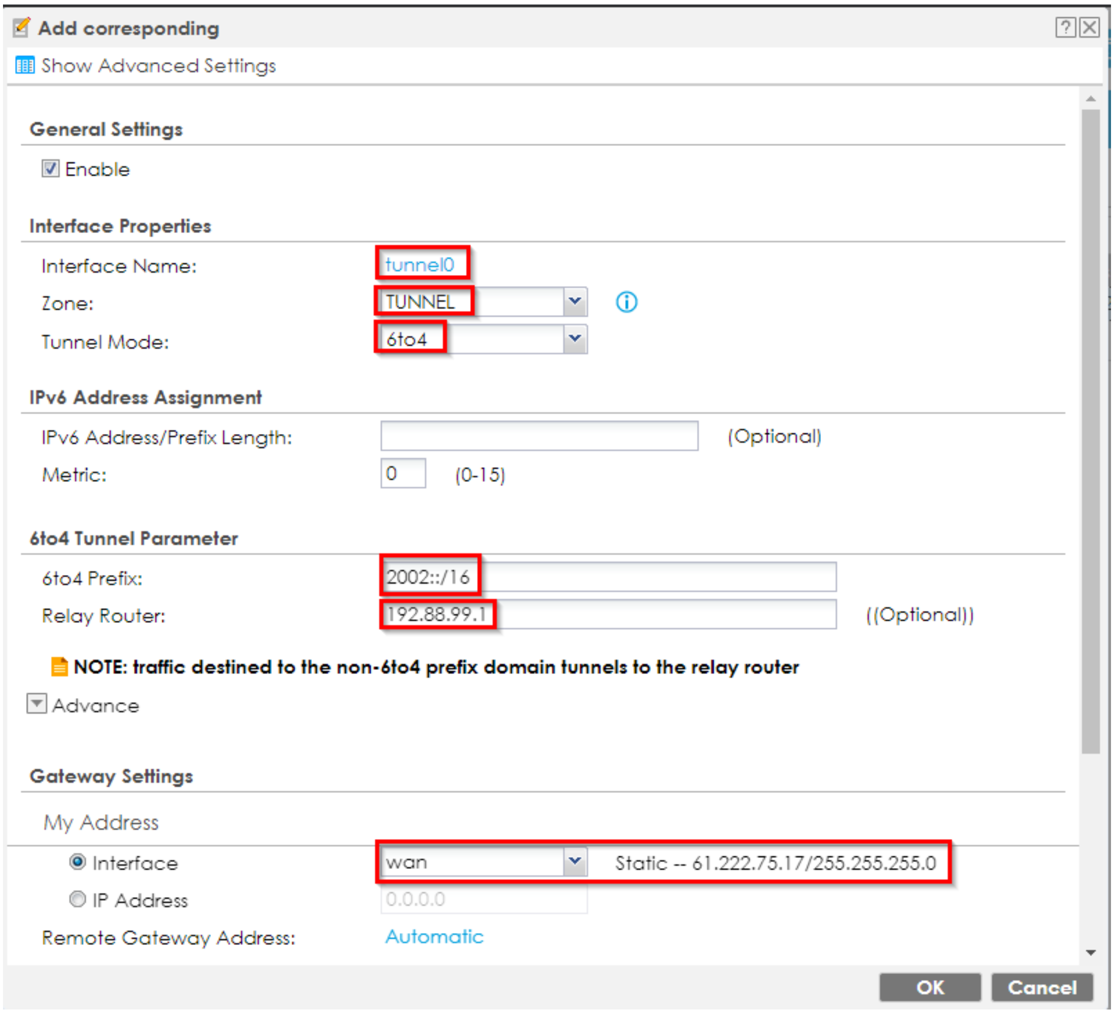
Metric: 0 (0-15)

☐ Enable IGMP Support

● IGMP Upstream

○ IGMP Downstream

3. Navigate to CONFIGURATION > Network > Interface > Tunnel > Add, Select Enable. Enter tunnel0 as the Interface Name and select 6to4 as the Tunnel Mode. In the 6to4 Tunnel Parameter section, this example just simply uses the default 6to4 Prefix, 2002:://16. Enter your Relay Router's IP address (192.88.99.1 in this example). Select wan1 as the Gateway. Click OK



Add corresponding

Show Advanced Settings

General Settings

☑ Enable

Interface Properties

Interface Name: tunnel0

Zone: TUNNEL

Tunnel Mode: 6to4

IPv6 Address Assignment

IPv6 Address/Prefix Length: (Optional)

Metric: 0 (0-15)

6to4 Tunnel Parameter

6to4 Prefix: 2002::/16

Relay Router: 192.88.99.1 ((Optional))

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

Advance

Gateway Settings

My Address

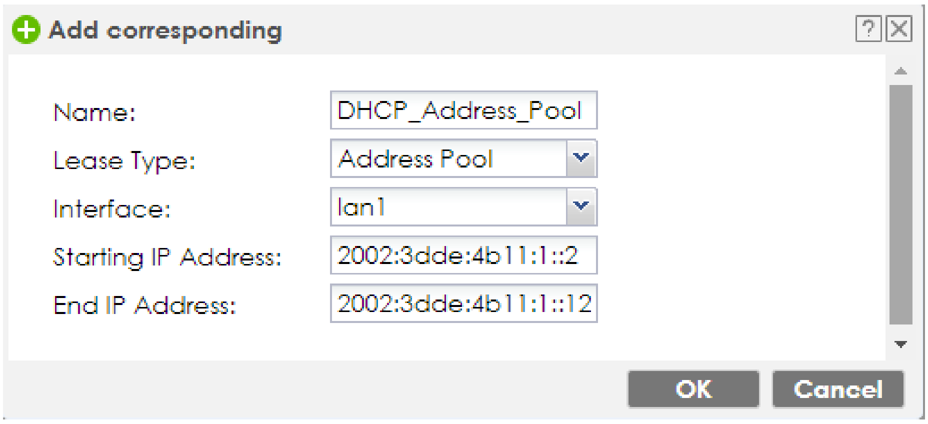
● Interface wan Static -- 61.222.75.17/255.255.255.0

○ IP Address 0.0.0.0

Remote Gateway Address: Automatic

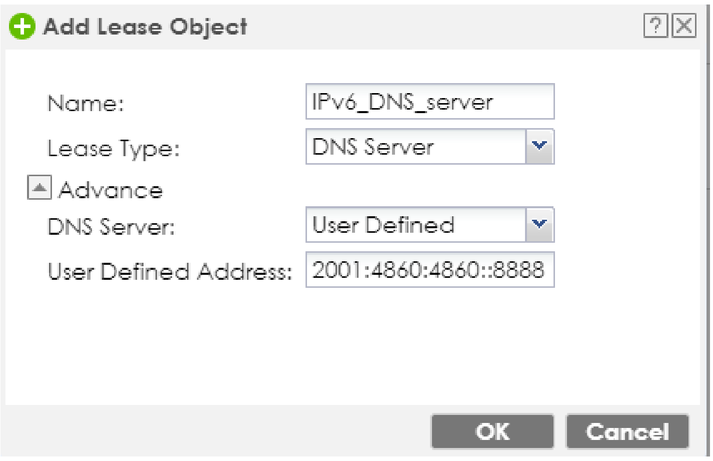
Lan

1. Create IPv6 DHCP Pool (Configuration > Object > DHCPv6 > Lease > Add)



Name:	DHCP_Address_Pool
Lease Type:	Address Pool
Interface:	lan1
Starting IP Address:	2002:3dde:4b11:1::2
End IP Address:	2002:3dde:4b11:1::12

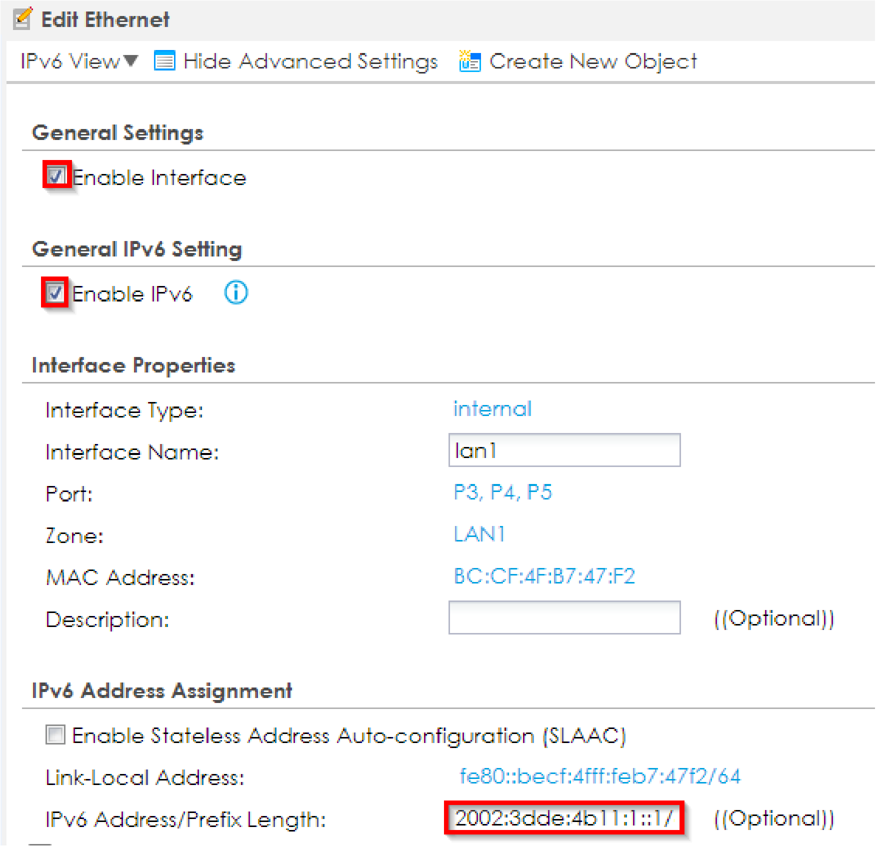
2. Create IPv6 DHCP DNS Server object. (Configuration > Object > DHCPv6 > Lease > Add)



Name:	IPv6_DNS_server
Lease Type:	DNS Server
DNS Server:	User Defined
User Defined Address:	2001:4860:4860::8888

In the Configuration > Ethernet > IPv6 Configuration section, double-click the LAN interface you want to modify.

3. Enable Interface and Enable IPv6. Key in IPv6 Address/Prefix Length: 2002:3dde:4b11:1::1/64



Edit Ethernet

IPv6 View▼ Hide Advanced Settings Create New Object

General Settings

☑ Enable Interface

General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Type:	internal
Interface Name:	lan1
Port:	P3, P4, P5
Zone:	LAN1
MAC Address:	BC:CF:4F:B7:47:F2
Description:	((Optional))

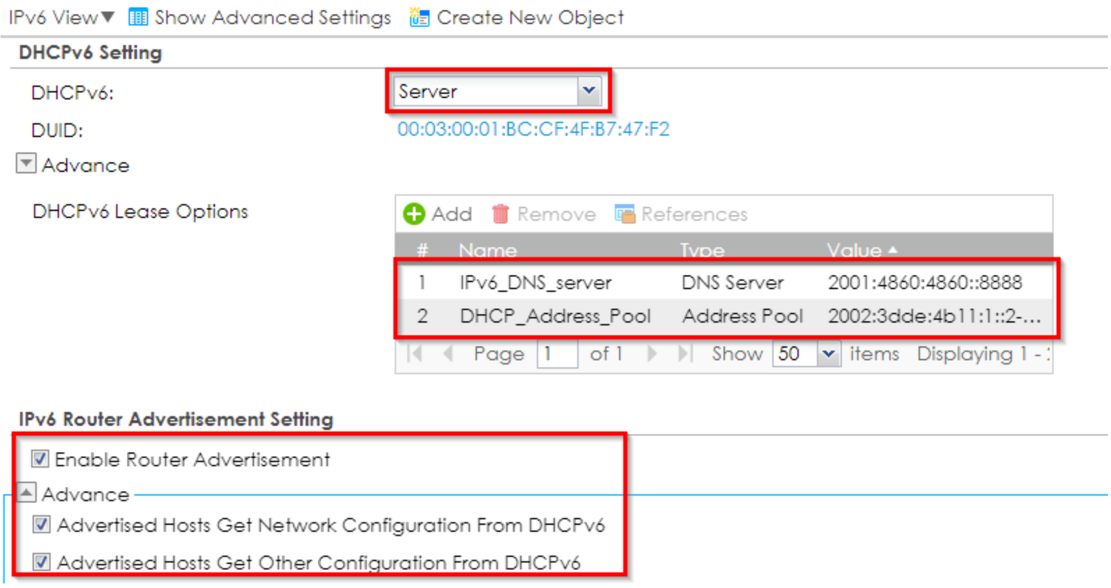
IPv6 Address Assignment

□ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address:	fe80::becf:4fff:feb7:47f2/64
IPv6 Address/Prefix Length:	2002:3dde:4b11:1::1/ ((Optional))

4. Scroll down and choose Server for DHCPv6 dropdown menu. Navigate to IPv6 Router Advertisement Setting.

5. Enable Router Advertisement, Host Get Network Configuration From DHCPv6 and Hosts Get Other Configuration From DHCPv6 checkboxes.



IPv6 View▼ Show Advanced Settings Create New Object

DHCPv6 Setting

DHCPv6: Server

DUID: 00:03:00:01:BC:CF:4F:B7:47:F2

Advance

DHCPv6 Lease Options

Add Remove References

#	Name	Type	Value ▲
1	IPv6_DNS_server	DNS Server	2001:4860:4860::8888
2	DHCP_Address_Pool	Address Pool	2002:3dde:4b11:1::2-...

Page 1 of 1 Show 50 items Displaying 1 - :

IPv6 Router Advertisement Setting

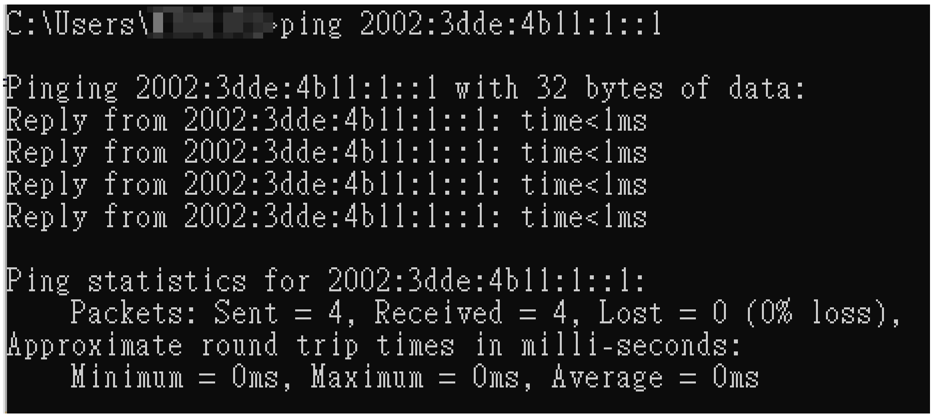
☑ Enable Router Advertisement

Advance

☑ Advertised Hosts Get Network Configuration From DHCPv6

☑ Advertised Hosts Get Other Configuration From DHCPv6

Test the result

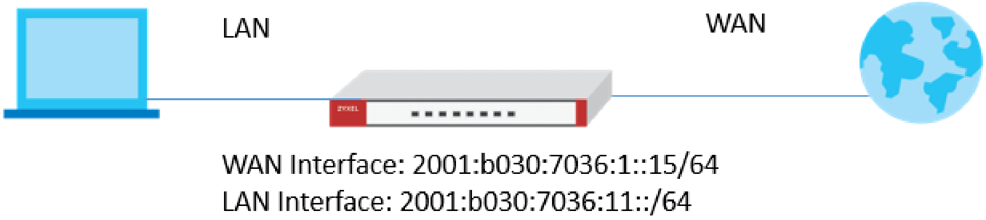


```
C:\Users\[redacted]>ping 2002:3dde:4b11:1::1

Pinging 2002:3dde:4b11:1::1 with 32 bytes of data:
Reply from 2002:3dde:4b11:1::1: time<1ms
Reply from 2002:3dde:4b11:1::1: time<1ms
Reply from 2002:3dde:4b11:1::1: time<1ms
Reply from 2002:3dde:4b11:1::1: time<1ms

Ping statistics for 2002:3dde:4b11:1::1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

How to set up Static IPv6 on WAN and auto-configuration on the LAN

This example shows how to configure your USG's WAN as Static IPv6 and LAN interface as auto-configuration.

In this scenario :
ISP's IPv6 Address is 2001:b030:7036:1::1
ISP Provided 2001:b030:7036:1::15/64 IPv6 IP Address.
DNS Server Set as 2001:4860:4860::8888
LAN Subnet Set as 2001:b030:7036:11::/64

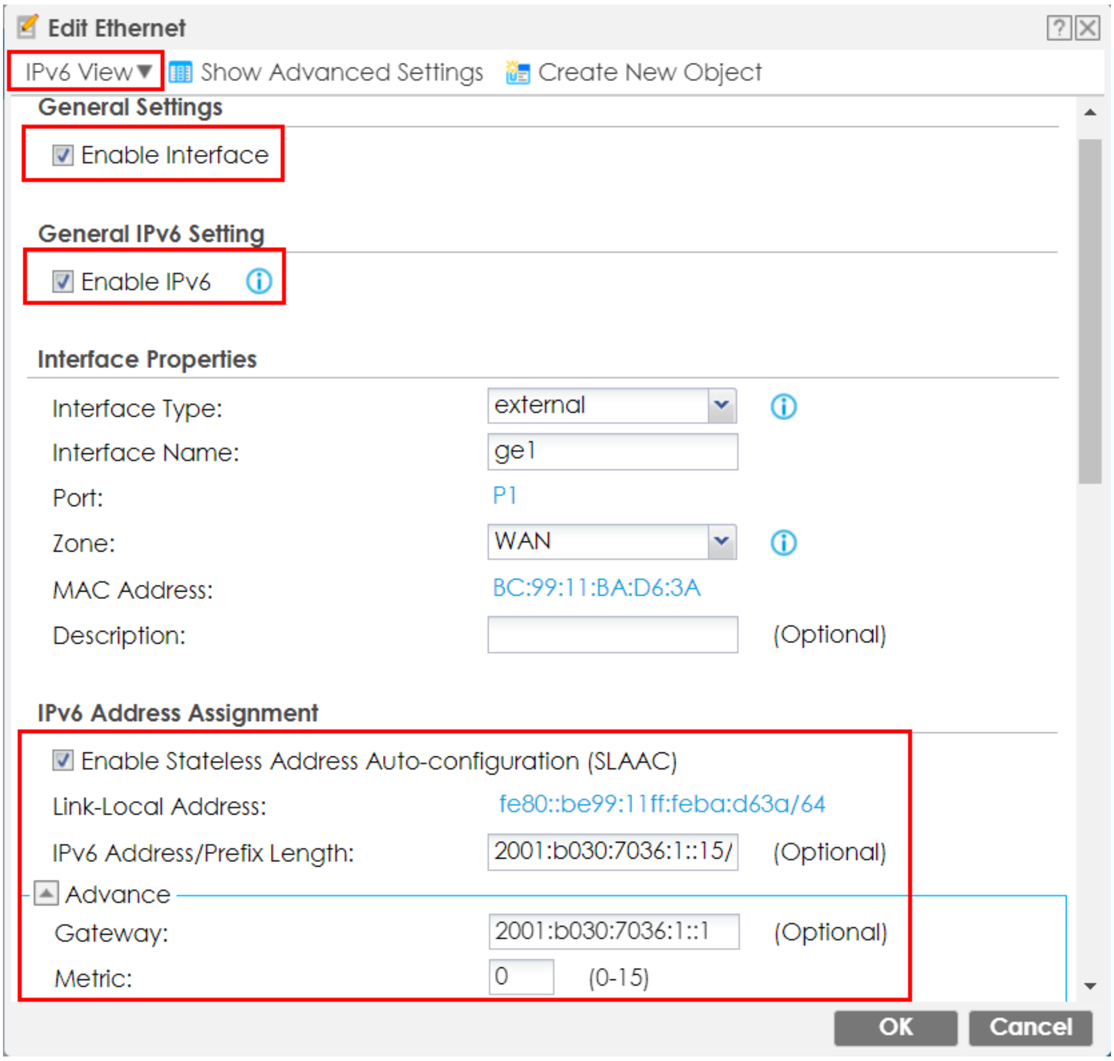

LAN
WAN
WAN Interface: 2001:b030:7036:1::15/64
LAN Interface: 2001:b030:7036:11::/64

Setting Up the IPv6 Interfaces

Wan

1. In the Configuration > Ethernet > IPv6 Configuration section, double-click the WAN interface you want to modify.

2. Choose IPv6 View, Enable Interface and Enable IPv6. In IPv6Address/Prefix Length text box, key in the Static IPv6 address.



General Settings

☑ Enable Interface

General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Type:	external	
Interface Name:	ge1	
Port:	P1	
Zone:	WAN	
MAC Address:	BC:99:11:BA:D6:3A	
Description:		(Optional)

IPv6 Address Assignment

☑ Enable Stateless Address Auto-configuration (SLAAC)

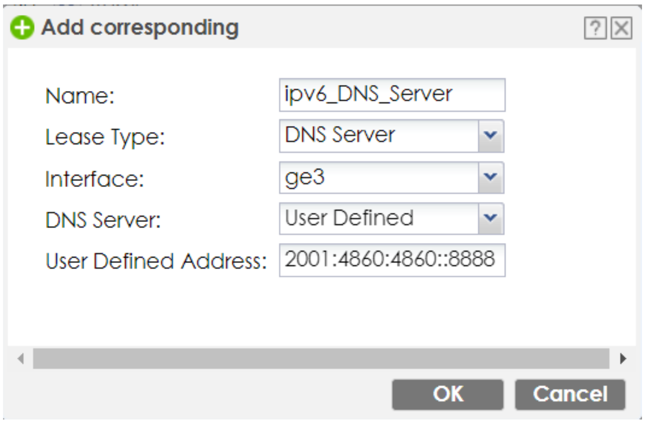
Link-Local Address:	fe80::be99:11ff:feba:d63a/64	
IPv6 Address/Prefix Length:	2001:b030:7036:1::15/	(Optional)

Advance

Gateway:	2001:b030:7036:1::1	(Optional)
Metric:	0	(0-15)

Lan

1. Create IPv6 DHCP DNS Server object. (Configuration > Object > DHCPv6 > Lease > Add)

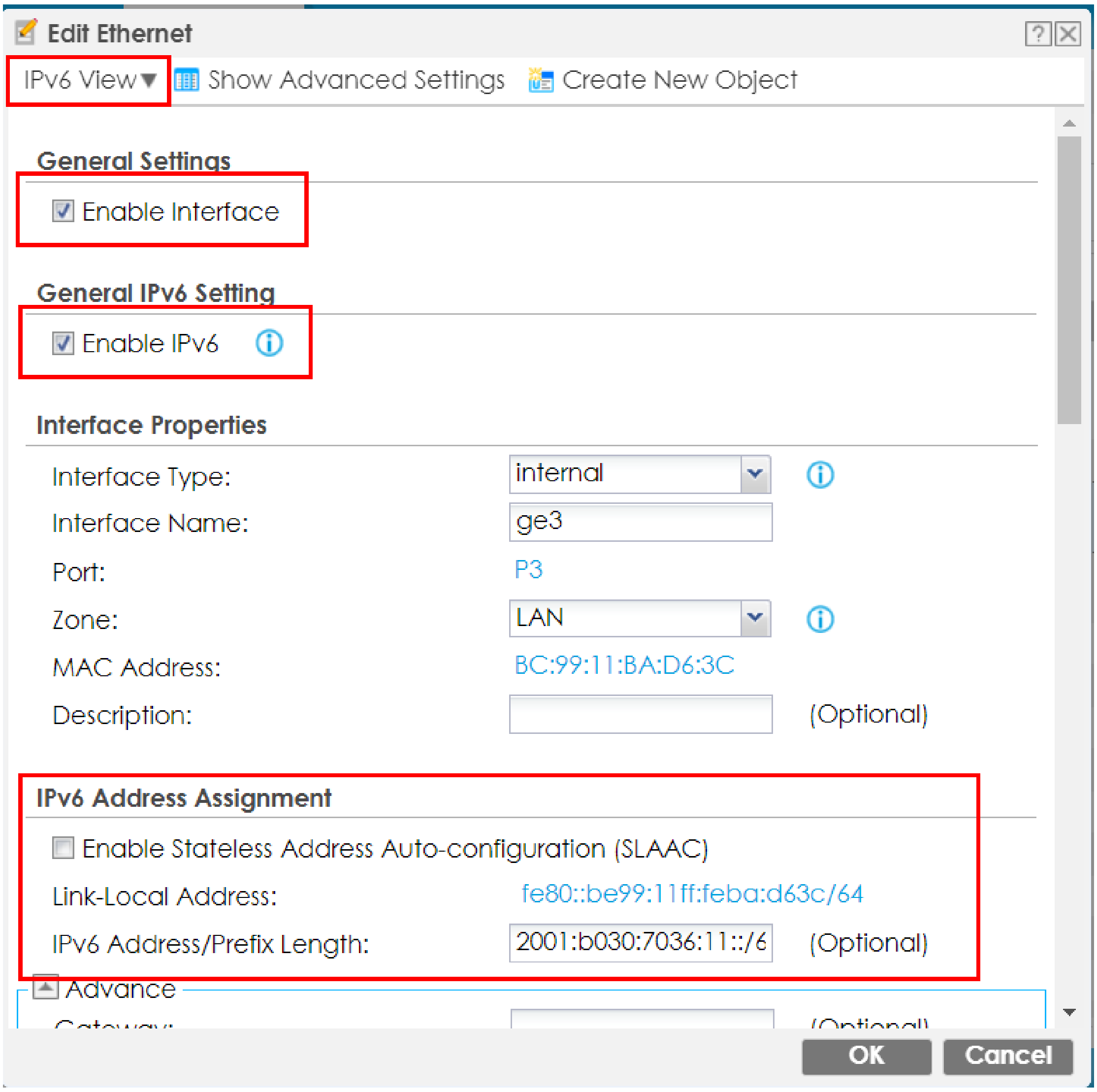

Add corresponding

Name:	ipv6_DNS_Server
Lease Type:	DNS Server
Interface:	ge3
DNS Server:	User Defined
User Defined Address:	2001:4860:4860::8888

In the Configuration > Ethernet > IPv6 Configuration section, double-click the LAN interface you want to modify.

2. Enable Interface and Enable IPv6.

Key in IPv6 Address/Prefix Length.



Edit Ethernet

General Settings

☑ Enable Interface

General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Type:	internal
Interface Name:	ge3
Port:	P3
Zone:	LAN
MAC Address:	BC:99:11:BA:D6:3C
Description:	(Optional)

IPv6 Address Assignment

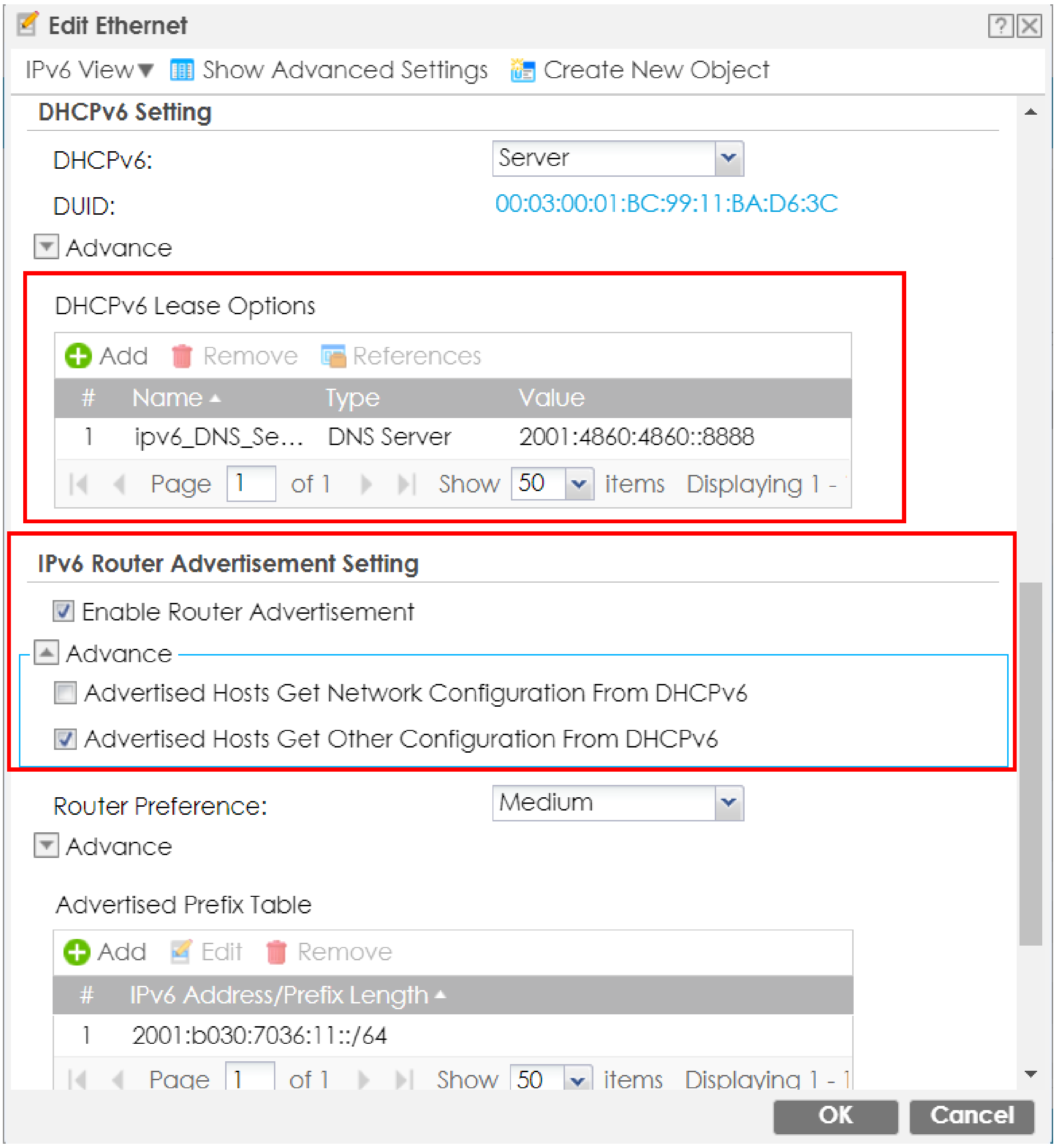
☐ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address:	fe80::be99:11ff:feba:d63c/64
IPv6 Address/Prefix Length:	2001:b030:7036:11::/6 (Optional)

3. Assign IPv6 DNS Server into DHCPv6 Lease Options.

Enable Router Advertisement and enable Advertised Host Get Other Configuration From DHCPv6 checkboxes.

Key in Advertised Prefix Table.



DHCPv6 Setting

DHCPv6: Server

DUID: 00:03:00:01:BC:99:11:BA:D6:3C

Advance

DHCPv6 Lease Options

#	Name	Type	Value
1	ipv6_DNS_Se…	DNS Server	2001:4860:4860::8888

Page 1 of 1 Show 50 items Displaying 1 -

IPv6 Router Advertisement Setting

☑ Enable Router Advertisement

Advance

☐ Advertised Hosts Get Network Configuration From DHCPv6

☑ Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

Advance

Advertised Prefix Table

#	IPv6 Address/Prefix Length
1	2001:b030:7036:11::/64

Page 1 of 1 Show 50 items Displaying 1 - 1

How to set up Static IPv6 on WAN and DHCPv6 on the LAN

This example shows how to configure your USG's WAN as Static IPv6 and LAN interface as DHCPv6.

In this scenario:

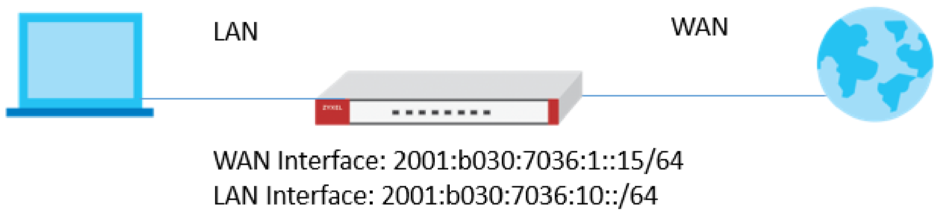
ISP's IPv6 Address is 2001:b030:7036:1::1

ISP Provided 2001:b030:7036:1::15/64 IPv6 IP Address.

DNS Server Set as 2001:4860:4860::8888

LAN Subnet Set as 2001:b030:7036:10::/64

LAN DHCP Pool Set as 2001:b030:7036:10::-2001:b030:7036:10::12

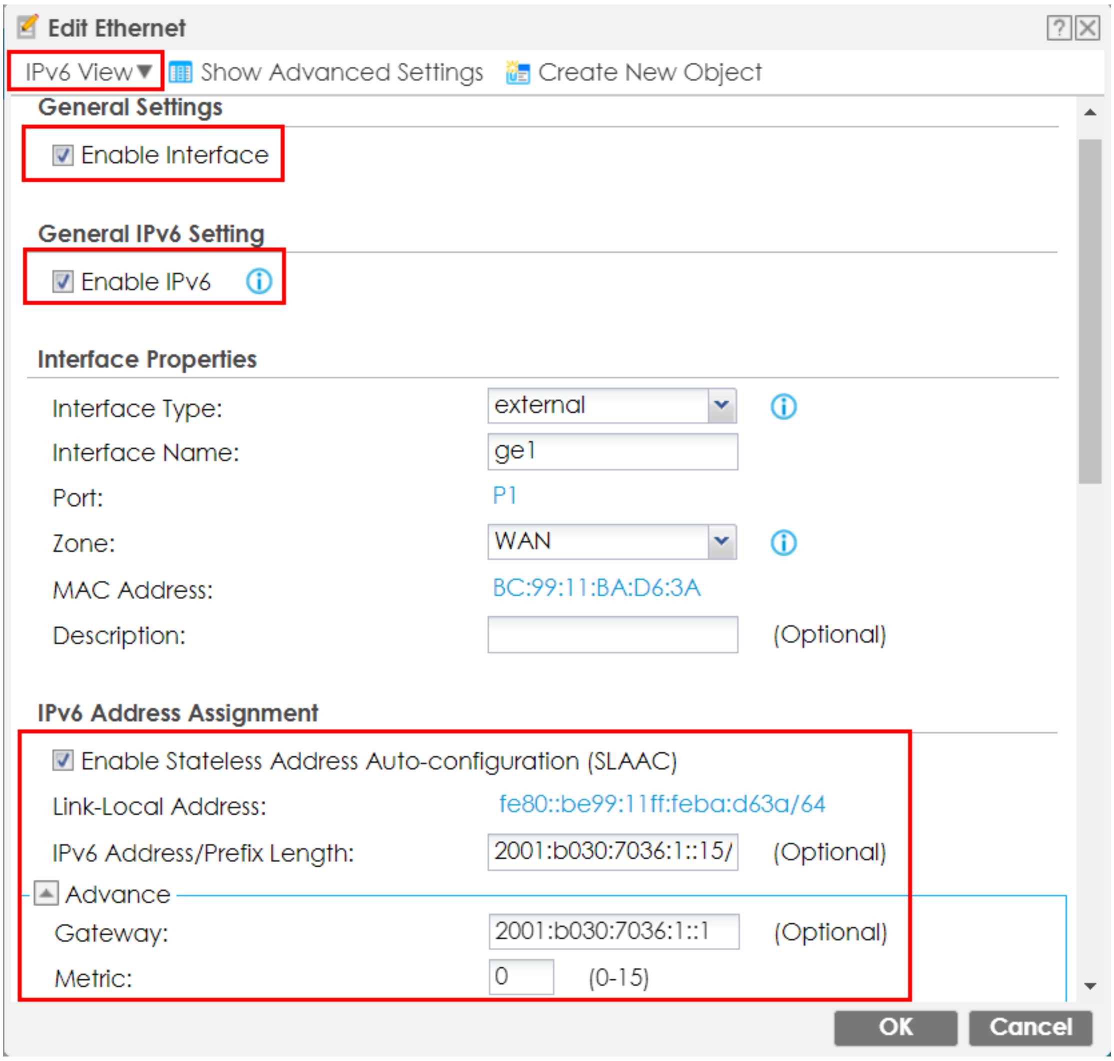

LAN
WAN
WAN Interface: 2001:b030:7036:1::15/64
LAN Interface: 2001:b030:7036:10::/64

Setting Up the IPv6 Interfaces

Wan

In the Configuration > Ethernet > IPv6 Configuration section, double-click the WAN interface you want to modify.

1. Choose IPv6 View and Enable Interface and Enable IPv6.
2. In IPv6Address/Prefix Length text box, key in the Static IPv6 address.



General Settings

☑ Enable Interface

General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Type:	external	
Interface Name:	ge1	
Port:	P1	
Zone:	WAN	
MAC Address:	BC:99:11:BA:D6:3A	
Description:		(Optional)

IPv6 Address Assignment

☑ Enable Stateless Address Auto-configuration (SLAAC)

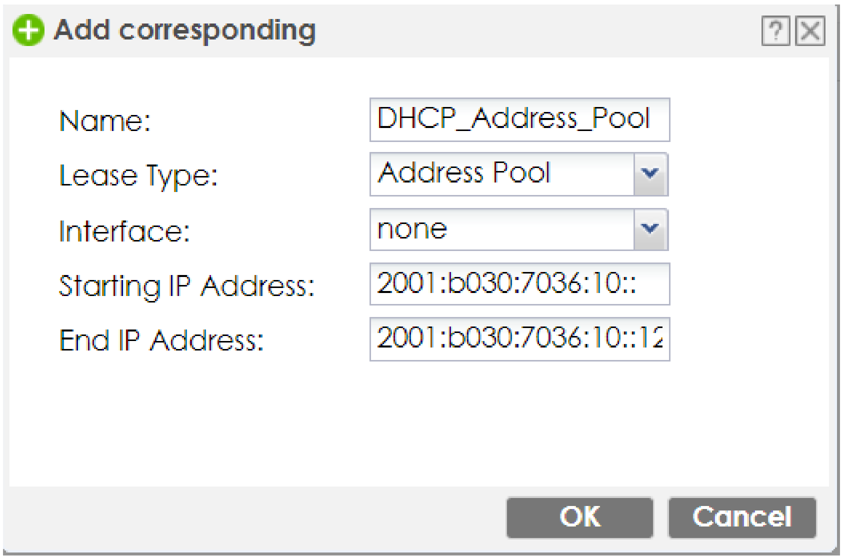
Link-Local Address:	fe80::be99:11ff:feba:d63a/64	
IPv6 Address/Prefix Length:	2001:b030:7036:1::15/	(Optional)

Advance

Gateway:	2001:b030:7036:1::1	(Optional)
Metric:	0	(0-15)

Lan

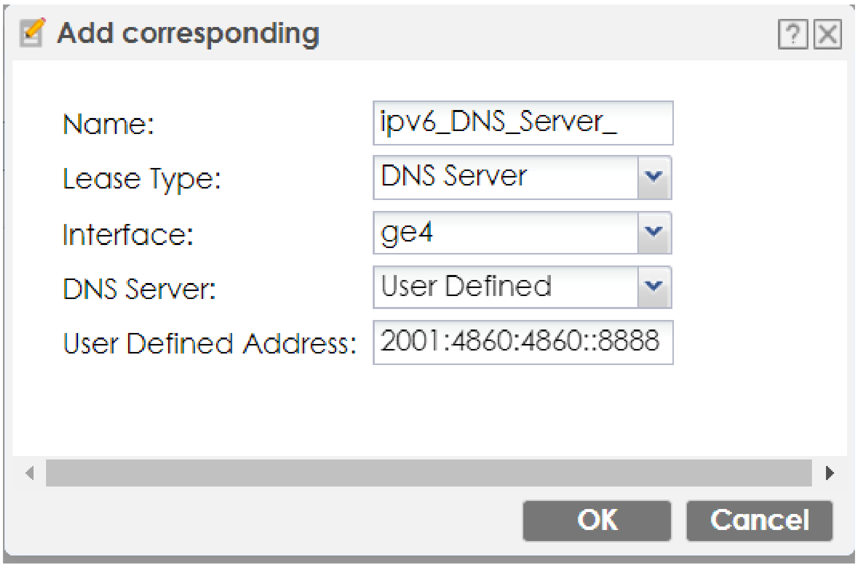
1. Create IPv6 DHCP Pool(Configuration > Object > DHCPv6 > Lease > Add)



Add corresponding

Name:	DHCP_Address_Pool
Lease Type:	Address Pool
Interface:	none
Starting IP Address:	2001:b030:7036:10::
End IP Address:	2001:b030:7036:10::12

2. Create IPv6 DHCP DNS Server object. (Configuration > Object > DHCPv6 > Lease > Add)



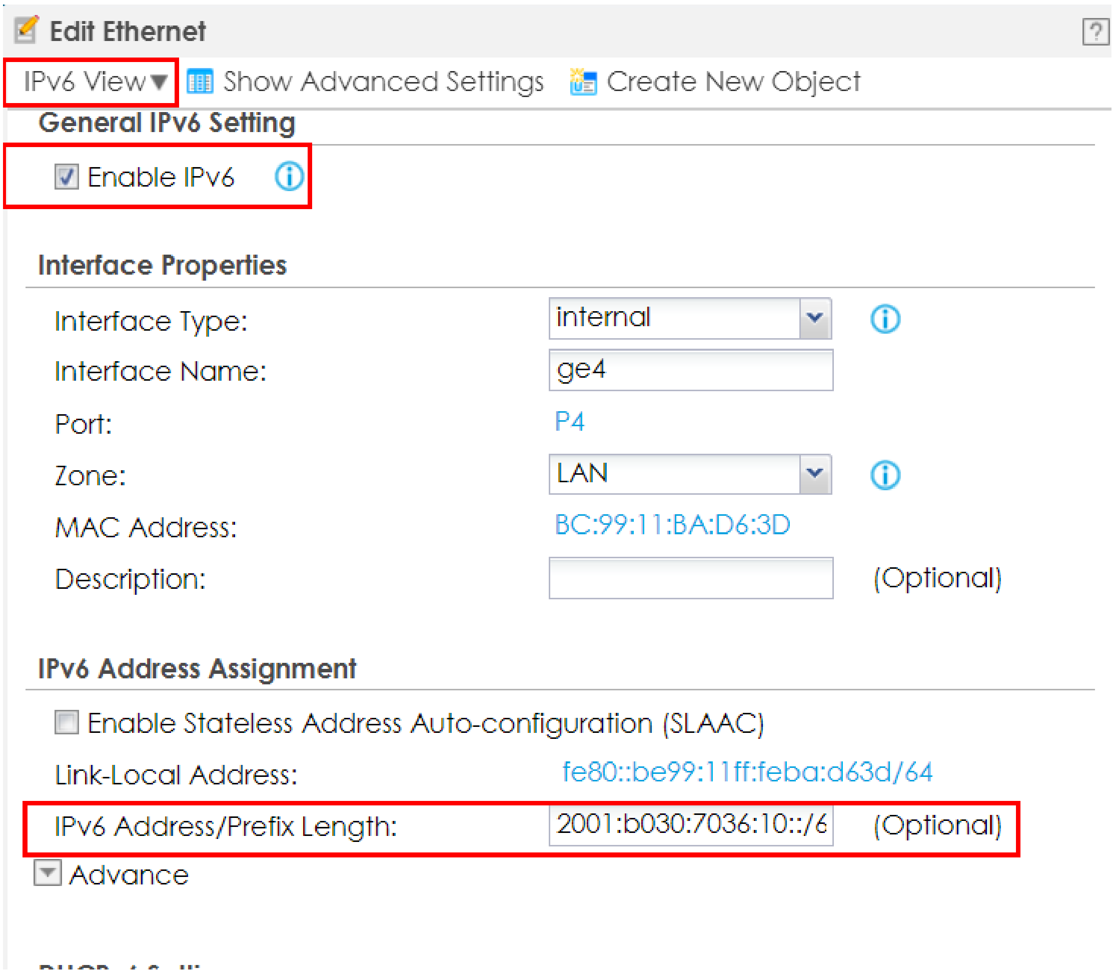
Add corresponding

Name:	ipv6_DNS_Server_
Lease Type:	DNS Server
Interface:	ge4
DNS Server:	User Defined
User Defined Address:	2001:4860:4860::8888

In the Configuration > Ethernet > IPv6 Configuration section, double-click the LAN interface you want to modify.

3. Enable Interface and Enable IPv6.

Key in IPv6 Address/Prefix Length



General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Type:	internal	
Interface Name:	ge4	
Port:	P4	
Zone:	LAN	
MAC Address:	BC:99:11:BA:D6:3D	
Description:		(Optional)

IPv6 Address Assignment

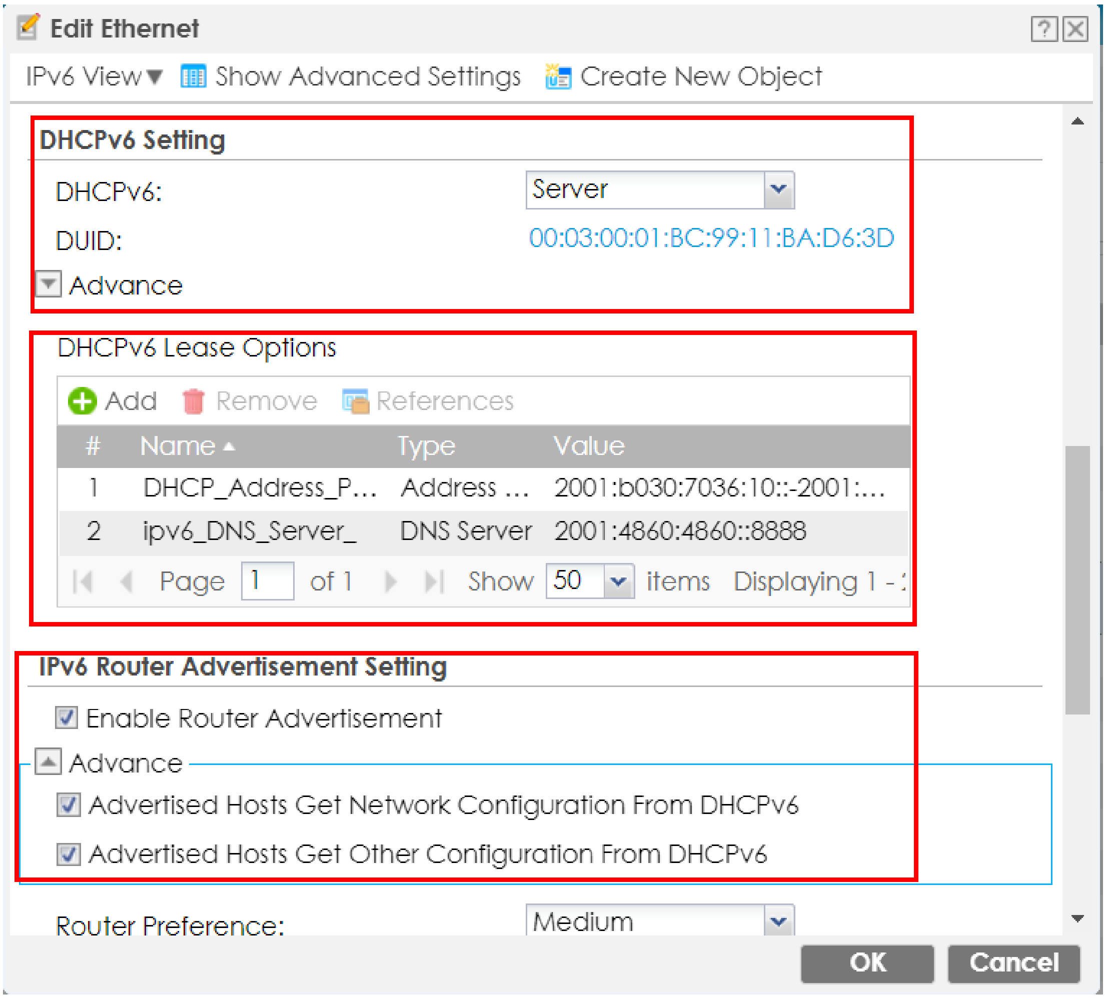
☐ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address:	fe80::be99:11ff:feba:d63d/64	
IPv6 Address/Prefix Length:	2001:b030:7036:10::/6	(Optional)

4. Scroll down and choose Server for DHCPv6 dropdown menu.

Navigate to IPv6 Router Advertisement Setting.

5. Enable Router Advertisement, Host Get Network Configuration From DHCPv6 and Hosts Get Other Configuration From DHCPv6 checkboxes.



Edit Ethernet
IPv6 View▼ Show Advanced Settings Create New Object

DHCPv6 Setting

DHCPv6: Server

DUID: 00:03:00:01:BC:99:11:BA:D6:3D

▼ Advance

DHCPv6 Lease Options

#	Name ▲	Type	Value
1	DHCP_Address_P…	Address …	2001:b030:7036:10::-2001:…
2	ipv6_DNS_Server_	DNS Server	2001:4860:4860::8888

Page 1 of 1 Show 50 items Displaying 1 - :

IPv6 Router Advertisement Setting

☑ Enable Router Advertisement

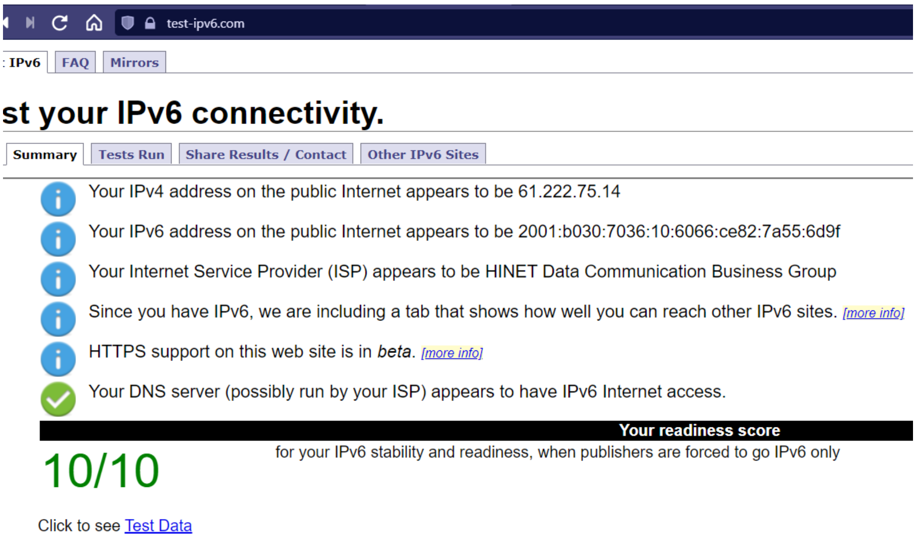
▲ Advance

☑ Advertised Hosts Get Network Configuration From DHCPv6

☑ Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

Test The Result



st your IPv6 connectivity.

Your IPv4 address on the public Internet appears to be 61.222.75.14

Your IPv6 address on the public Internet appears to be 2001:b030:7036:10:6066:ce82:7a55:6d9f

Your Internet Service Provider (ISP) appears to be HINET Data Communication Business Group

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [more info]

HTTPS support on this web site is in *beta*. [more info]

Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

Your readiness score

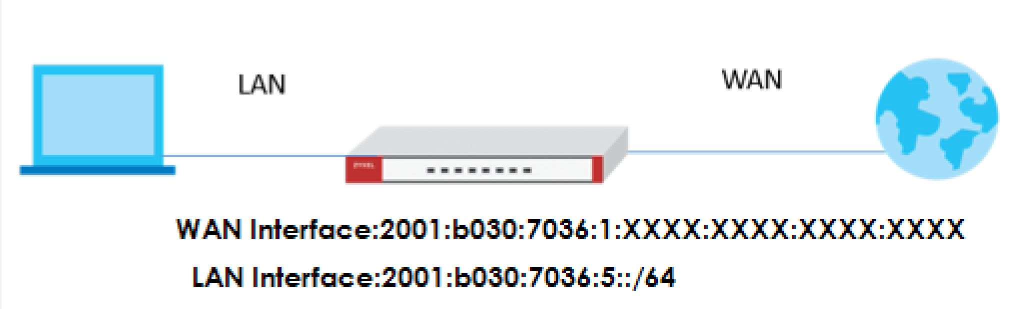
10/10 for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

Click to see Test Data

How to Set Up DHCPv6 without prefix delegation on the WAN and autoconf on the LAN

This example shows how to configure your ATP/USG Flex's WAN as DHCPv6 without prefix delegation and LAN interface as auto-configuration.

In this scenario:
ISP's IPv6 Address is 2001:b030:7036:1::/64
ISP Provided 2001:b030:7036:1:becf:4fff:fec9:9f04 IPv6 IP Address.
DNS Server Set as 2001:4860:4860::8888
LAN Subnet Set as 2001:b030:7036:5::/64


LAN
WAN
WAN Interface:2001:b030:7036:1:XXXX:XXXX:XXXX:XXXX
LAN Interface:2001:b030:7036:5::/64

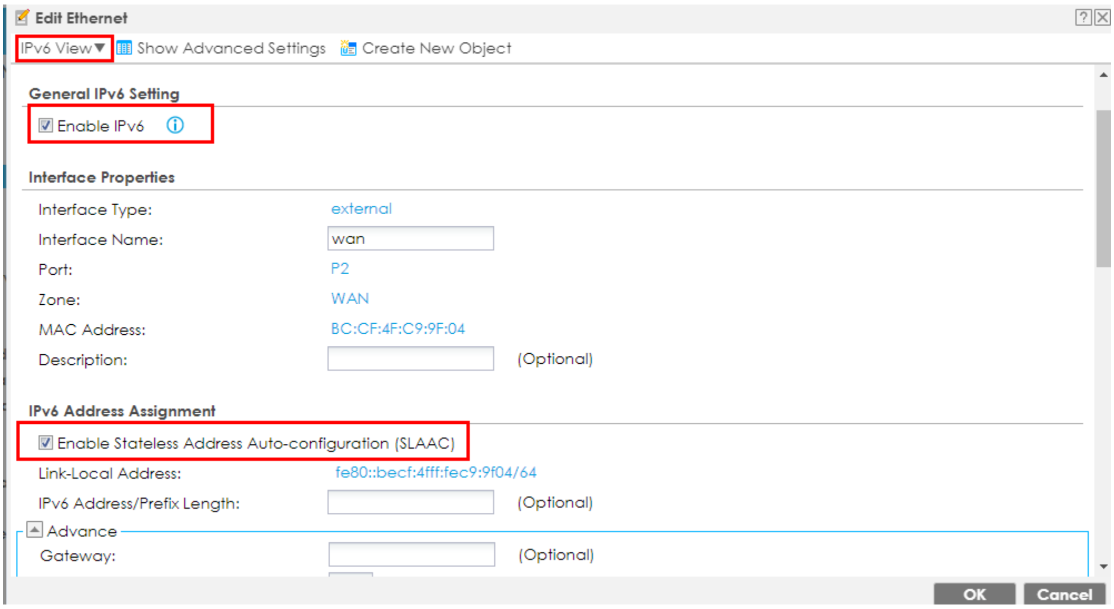
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP/USG Flex (Firmware Version: 5.00)

Setting Up the IPv6 Interfaces

Wan

1. In the Configuration > Ethernet > IPv6 Configuration section, double-click the WAN interface you want to modify.

2. Choose IPv6 View, Enable Interface and Enable IPv6. In IPv6Address Assignment text box, enable Stateless Address Auto-configuration (SLAAC)



General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Type:	external	
Interface Name:	wan	
Port:	P2	
Zone:	WAN	
MAC Address:	BC:CF:4F:C9:9F:04	
Description:		(Optional)

IPv6 Address Assignment

☑ Enable Stateless Address Auto-configuration (SLAAC)

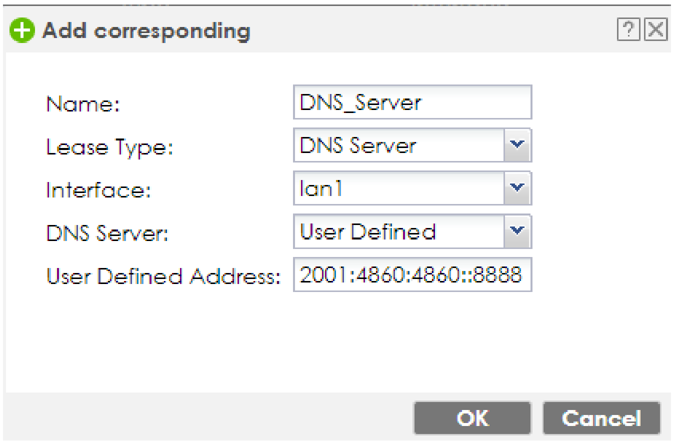
Link-Local Address:	fe80::becf:4fff:fec9:9f04/64	
IPv6 Address/Prefix Length:		(Optional)

Advance

Gateway:		(Optional)

Lan

1. Create IPv6 DHCP DNS Server object. (Configuration > Object > DHCPv6 > Lease > Add)

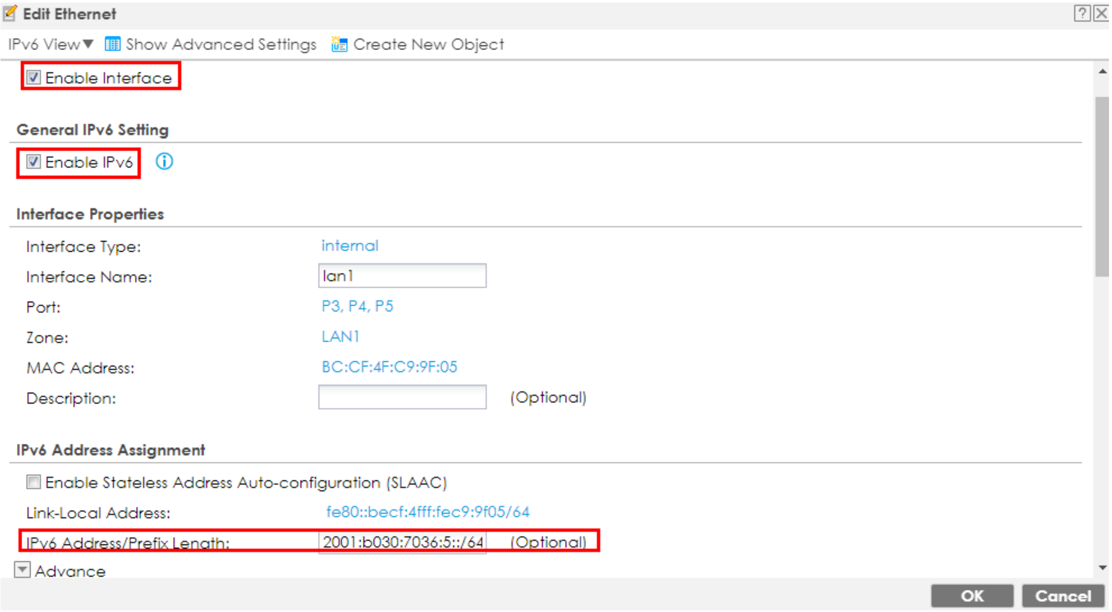


Name:	DNS_Server
Lease Type:	DNS Server
Interface:	lan1
DNS Server:	User Defined
User Defined Address:	2001:4860:4860::8888

In the Configuration > Ethernet > IPv6 Configuration section, double-click the LAN interface you want to modify.

2. Enable Interface and Enable IPv6.

Key in IPv6 Address/Prefix Length.



Edit Ethernet

☑ Enable Interface

General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Type:	internal
Interface Name:	lan1
Port:	P3, P4, P5
Zone:	LAN1
MAC Address:	BC:CF:4F:C9:9F:05
Description:	(Optional)

IPv6 Address Assignment

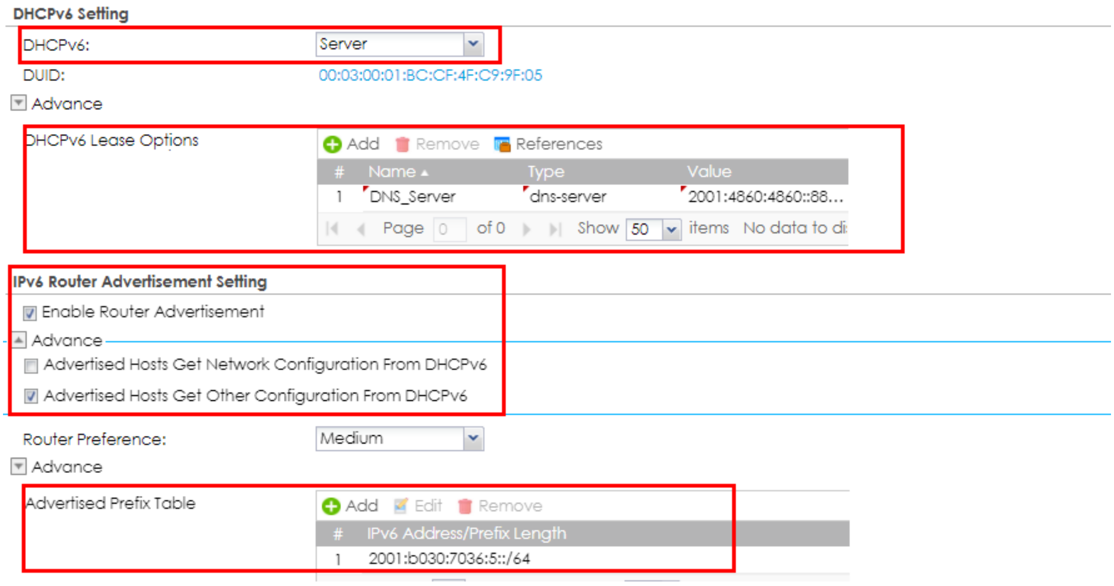
□ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address:	fe80::becf:4fff:fec9:9f05/64
IPv6 Address/Prefix Length:	2001:b030:7036:5::/64 (Optional)

3. Assign IPv6 DNS Server into DHCPv6 Lease Options.

Enable Router Advertisement and enable Advertised Host Get Other Configuration From DHCPv6 checkboxes.

Key in Advertised Prefix Table.



DHCPv6 Setting

DHCPv6: Server

DUID: 00:03:00:01:BC:CF:4F:C9:9F:05

Advance

DHCPv6 Lease Options

Add Remove References

#	Name ▲	Type	Value
1	DNS_Server	dns-server	2001:4860:4860::88...

Page 0 of 0 Show 50 items No data to di

IPv6 Router Advertisement Setting

☑ Enable Router Advertisement

Advance

□ Advertised Hosts Get Network Configuration From DHCPv6

☑ Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

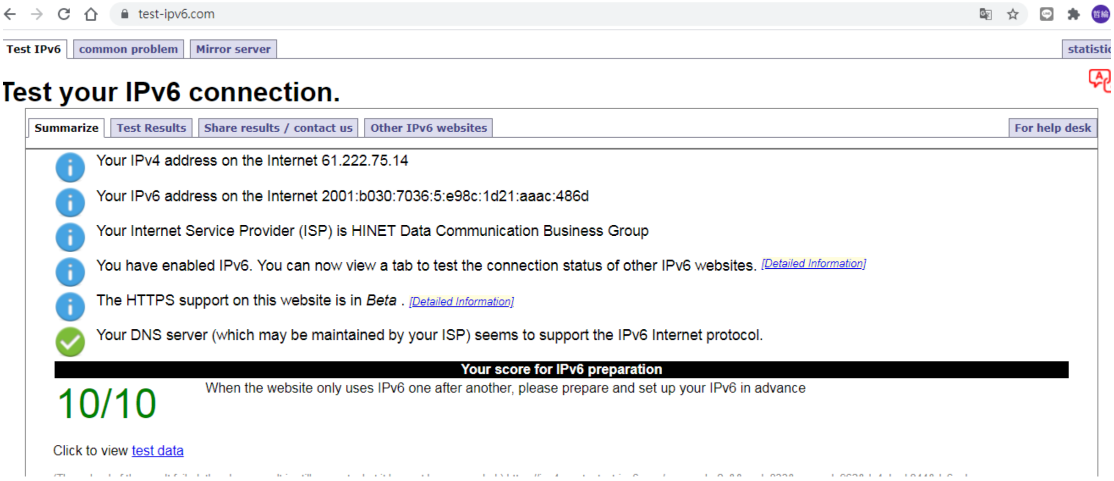
Advance

Advertised Prefix Table

Add Edit Remove

#	IPv6 Address/Prefix Length
1	2001:b030:7036:5::/64

Test the Result



Test your IPv6 connection.

Your IPv4 address on the Internet 61.222.75.14

Your IPv6 address on the Internet 2001:b030:7036:5:e98c:1d21:aaac:486d

Your Internet Service Provider (ISP) is HINET Data Communication Business Group

You have enabled IPv6. You can now view a tab to test the connection status of other IPv6 websites. [Detailed Information]

The HTTPS support on this website is in *Beta* . [Detailed Information]

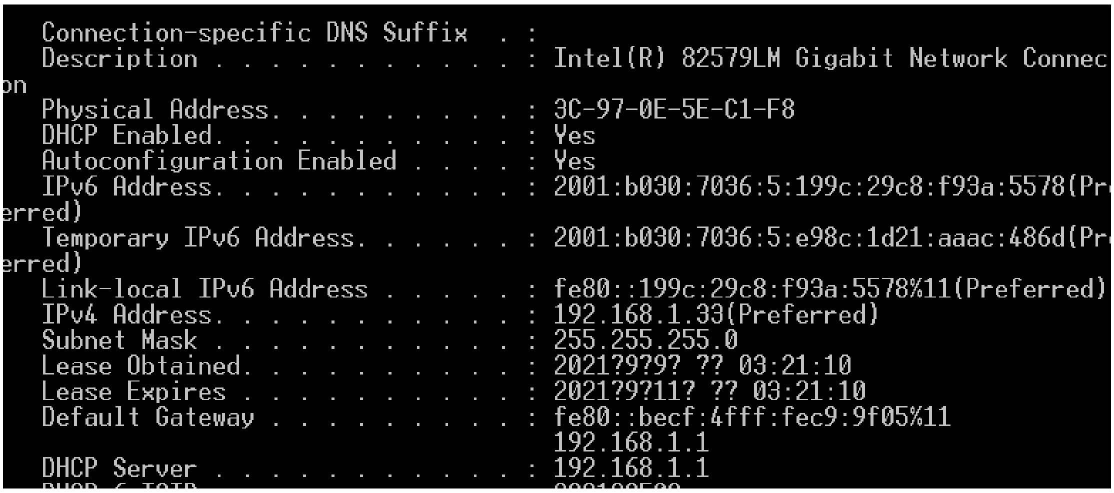
Your DNS server (which may be maintained by your ISP) seems to support the IPv6 Internet protocol.

Your score for IPv6 preparation

10/10

When the website only uses IPv6 one after another, please prepare and set up your IPv6 in advance

Click to view test data

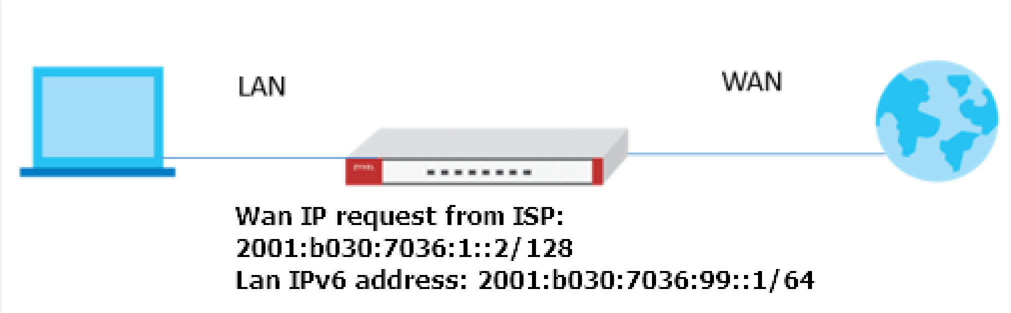


```
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) 82579LM Gigabit Network Connec
on
   Physical Address. . . . . . . . . : 3C-97-0E-5E-C1-F8
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:b030:7036:5:199c:29c8:f93a:5578(Pr
erred)
   Temporary IPv6 Address. . . . . . : 2001:b030:7036:5:e98c:1d21:aaac:486d(Pr
erred)
   Link-local IPv6 Address . . . . . : fe80::199c:29c8:f93a:5578%11(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.33(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : 2021?9?9? ?? 03:21:10
   Lease Expires . . . . . . . . . . : 2021?9?11? ?? 03:21:10
   Default Gateway . . . . . . . . . : fe80::becf:4fff:fec9:9f05%11
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
```

How to Set Up DHCPv6 with prefix delegation on the WAN and DHCPv6 on the LAN

This example shows how to configure your ATP/USG Flex's WAN as DHCPv6 with prefix delegation and LAN interface as DHCPv6.

In this scenario:
Device's wan request IPv6 Address from ISP.
Request result:
DHCP -- 2001:b030:7036:1::2/128
LAN Subnet Set as **2001:b030:7036:99::1/64**

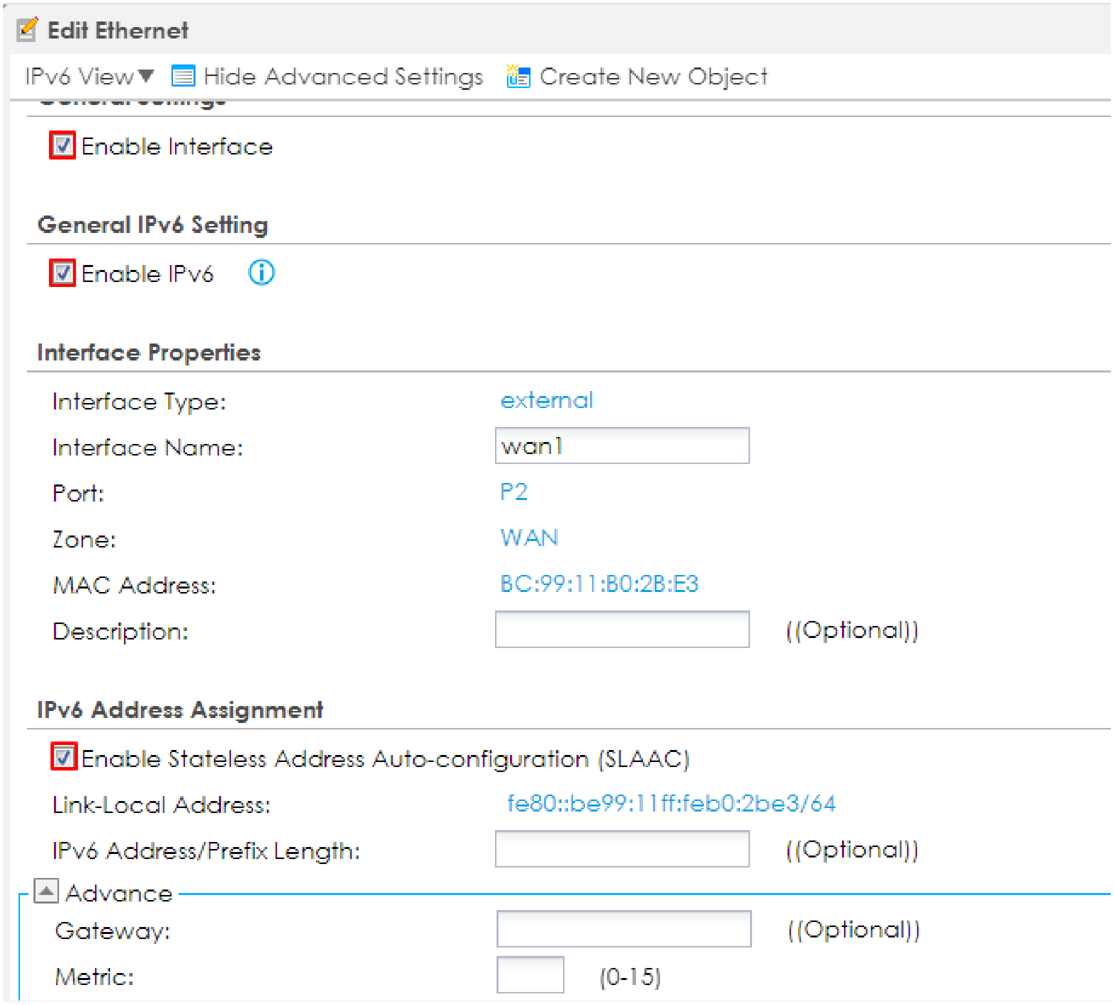


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP/USG Flex (Firmware Version: 5.00)

Configure on the Wan IPv6 interface

In the Configuration > Ethernet > IPv6 Configuration section, double-click the WAN interface you want to modify.

Choose IPv6 View, Enable Interface and Enable IPv6. In IPv6Address Assignment text box, enable Stateless Address Auto-configuration (SLAAC)



☑ Enable Interface

General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Type:	external
Interface Name:	wan1
Port:	P2
Zone:	WAN
MAC Address:	BC:99:11:B0:2B:E3
Description:	((Optional))

IPv6 Address Assignment

☑ Enable Stateless Address Auto-configuration (SLAAC)

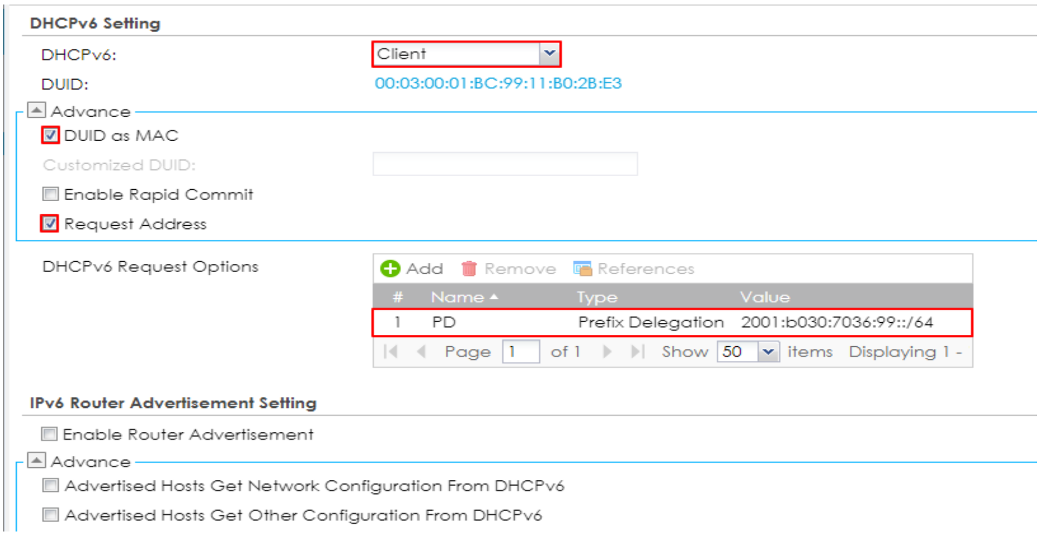
Link-Local Address:	fe80::be99:11ff:feb0:2be3/64
IPv6 Address/Prefix Length:	((Optional))

Advance

Gateway:	((Optional))
Metric:	(0-15)

On DHCPv6, select **Client**, then Enable **DUID as MAC**, and tick **Request Address**

Next, create PD on DHCPv6 Request Options, and PD's Value: **2001:b030:7036:99::/64**



DHCPv6 Setting

DHCPv6: Client

DUID: 00:03:00:01:BC:99:11:B0:2B:E3

Advance

☑ DUID as MAC

Customized DUID:

□ Enable Rapid Commit

☑ Request Address

DHCPv6 Request Options

#	Name ▲	Type	Value
1	PD	Prefix Delegation	2001:b030:7036:99::/64

IPv6 Router Advertisement Setting

□ Enable Router Advertisement

Advance

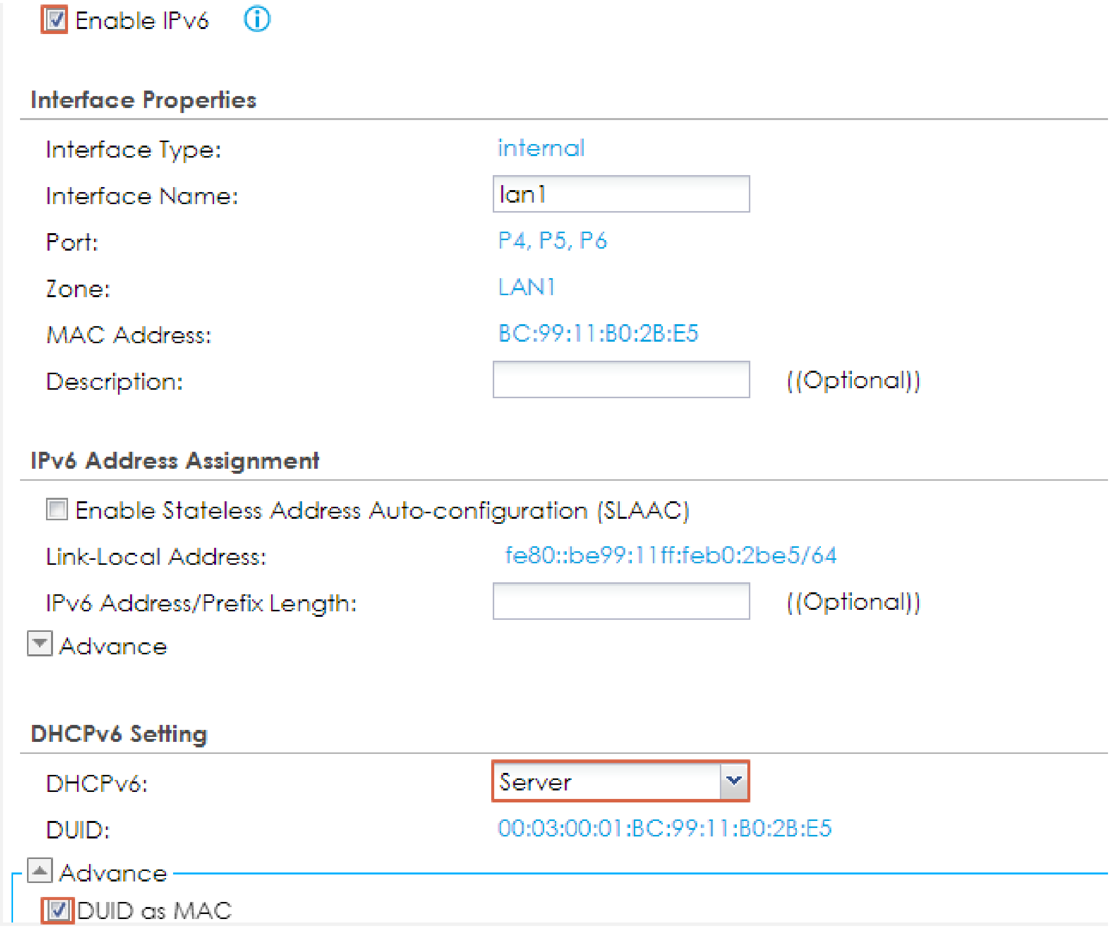
□ Advertised Hosts Get Network Configuration From DHCPv6

□ Advertised Hosts Get Other Configuration From DHCPv6

Configure on the Lan IPv6 interface

Tick **Enable IPv6**, then fill IPv6 address which provide from ISP:

Select **Server** as DHCPv6. Enable **DUID as MAC**.



☑ Enable IPv6

Interface Properties

Interface Type:	internal	
Interface Name:	lan1	
Port:	P4, P5, P6	
Zone:	LAN1	
MAC Address:	BC:99:11:B0:2B:E5	
Description:		((Optional))

IPv6 Address Assignment

□ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address:	fe80::be99:11ff:feb0:2be5/64	
IPv6 Address/Prefix Length:		((Optional))

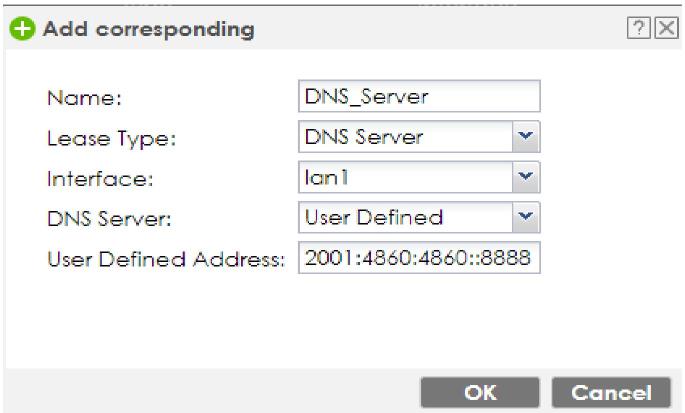
DHCPv6 Setting

DHCPv6:	Server
DUID:	00:03:00:01:BC:99:11:B0:2B:E5

☑ DUID as MAC

Next, On the DHCPv6 Lease Options, add **2001:4860:4860::8888** as DNS server

Add the **2001:b030:7036:99::10-2001:b030:7036:99::100** as Address Pool



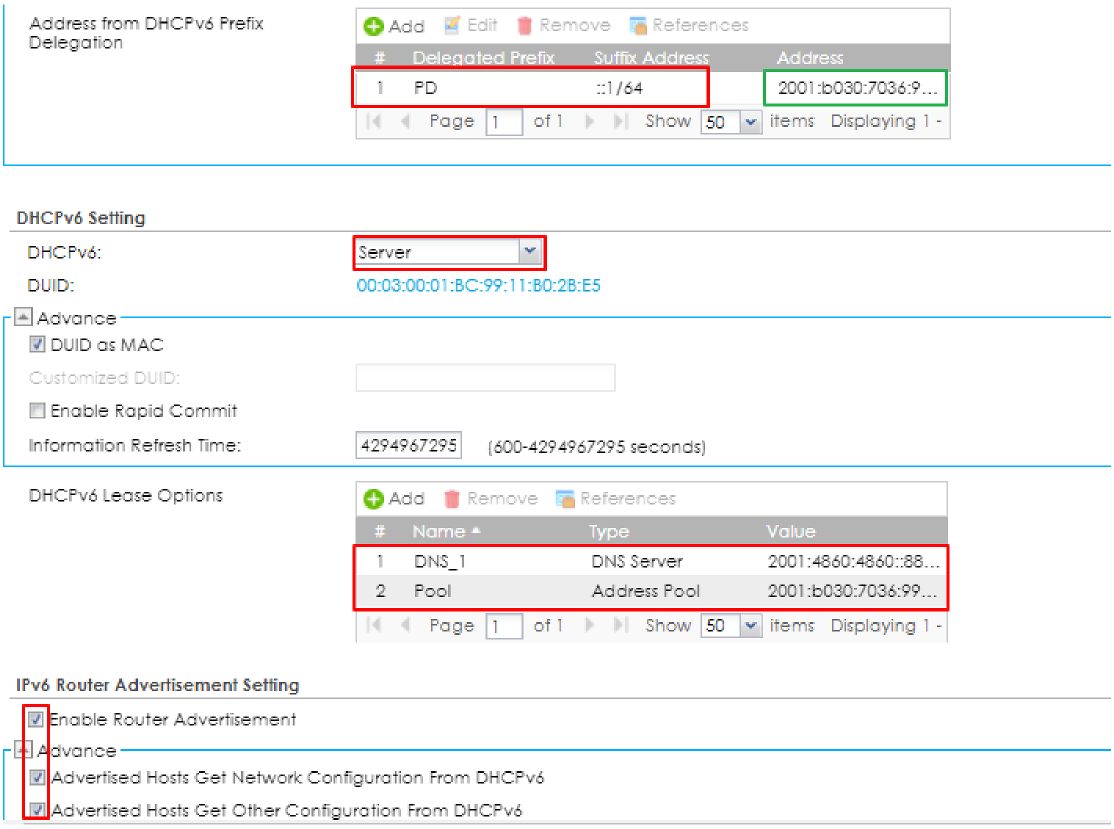
Name:	DNS_Server
Lease Type:	DNS Server
Interface:	lan1
DNS Server:	User Defined
User Defined Address:	2001:4860:4860::8888

On Address from DHCPv6 Prefix Delegation, fill **::1/64 as PD.**

Enable **Router Advertisement** then enable **Advertised Hosts Get Network**

Configuration From DHCPv6 and enable **Advertised Hosts Get Other Configuration From DHCPv6**

Note: After Save the below configuration on Lan, the **Address** on On Address from DHCPv6 Prefix Delegation will be generated automatically.



Address from DHCPv6 Prefix Delegation

#	Delegated Prefix	Suffix Address	Address
1	PD	::1/64	2001:b030:7036:9...

DHCPv6 Setting

DHCPv6: Server

DUID: 00:03:00:01:BC:99:11:B0:2B:E5

Advance

☑ DUID as MAC

Customized DUID:

□ Enable Rapid Commit

Information Refresh Time: 4294967295 (600-4294967295 seconds)

DHCPv6 Lease Options

#	Name	Type	Value
1	DNS_1	DNS Server	2001:4860:4860::88...
2	Pool	Address Pool	2001:b030:7036:99...

IPv6 Router Advertisement Setting

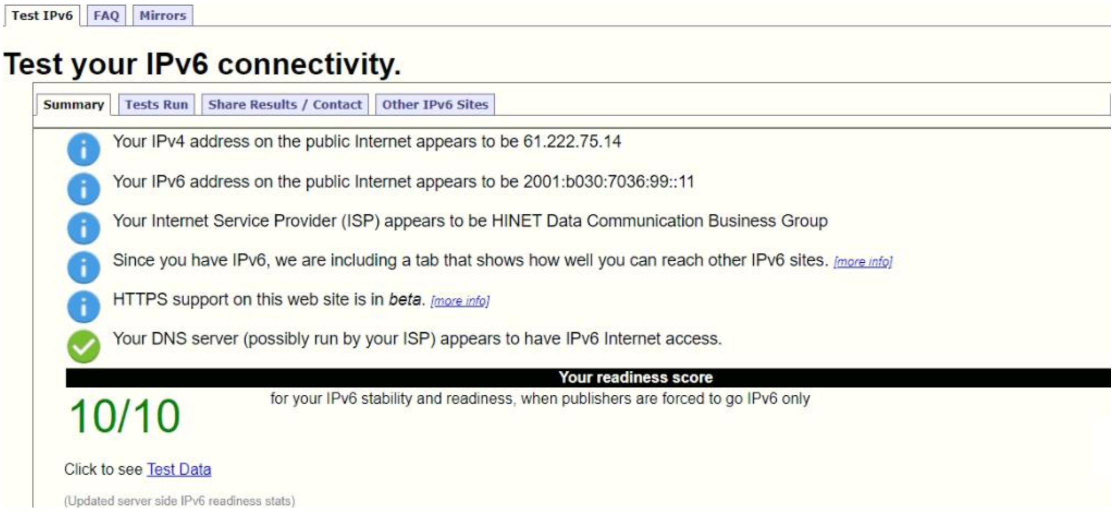
☑ Enable Router Advertisement

Advance

☑ Advertised Hosts Get Network Configuration From DHCPv6

☑ Advertised Hosts Get Other Configuration From DHCPv6

Test the Result



Test your IPv6 connectivity.

ⓘ Your IPv4 address on the public Internet appears to be 61.222.75.14

ⓘ Your IPv6 address on the public Internet appears to be 2001:b030:7036:99::11

ⓘ Your Internet Service Provider (ISP) appears to be HINET Data Communication Business Group

ⓘ Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [more info]

ⓘ HTTPS support on this web site is in *beta*. [more info]

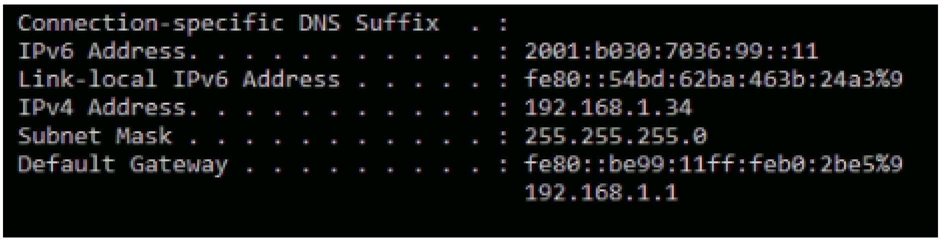
✓ Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

Your readiness score

10/10 for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

Click to see Test Data

(Updated server side IPv6 readiness stats)



```
Connection-specific DNS Suffix  . :
IPv6 Address. . . . . . . . . . . : 2001:b030:7036:99::11
Link-local IPv6 Address . . . . . : fe80::54bd:62ba:463b:24a3%9
IPv4 Address. . . . . . . . . . . : 192.168.1.34
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : fe80::be99:11ff:feb0:2be5%9
                                    192.168.1.1
```

How to Set Up Autoconf on the WAN and DHCPv6 on the LAN

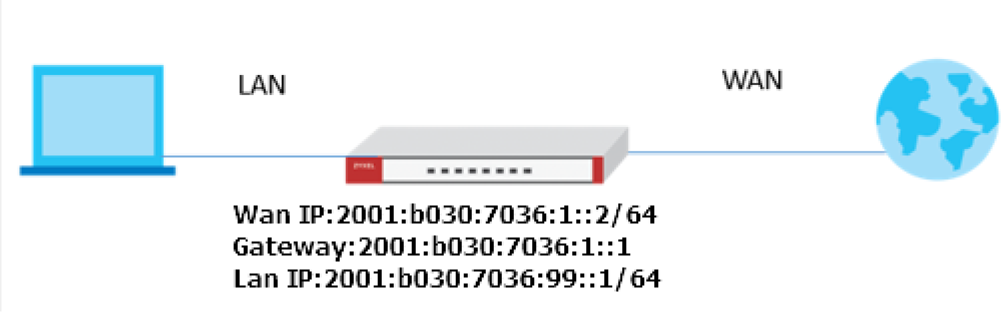
This example shows how to configure your ATP/USG Flex's WAN as Autoconf on the WAN and DHCPv6 on the LAN

In this scenario:

ISP assign the IPv6 address for wan subnet: 2001:b030:7036:1::2/64

Gateway: 2001:b030:7036:1::1

ISP assign IPv6 address for LAN Subnet: 2001:b030:7036:99::1/64

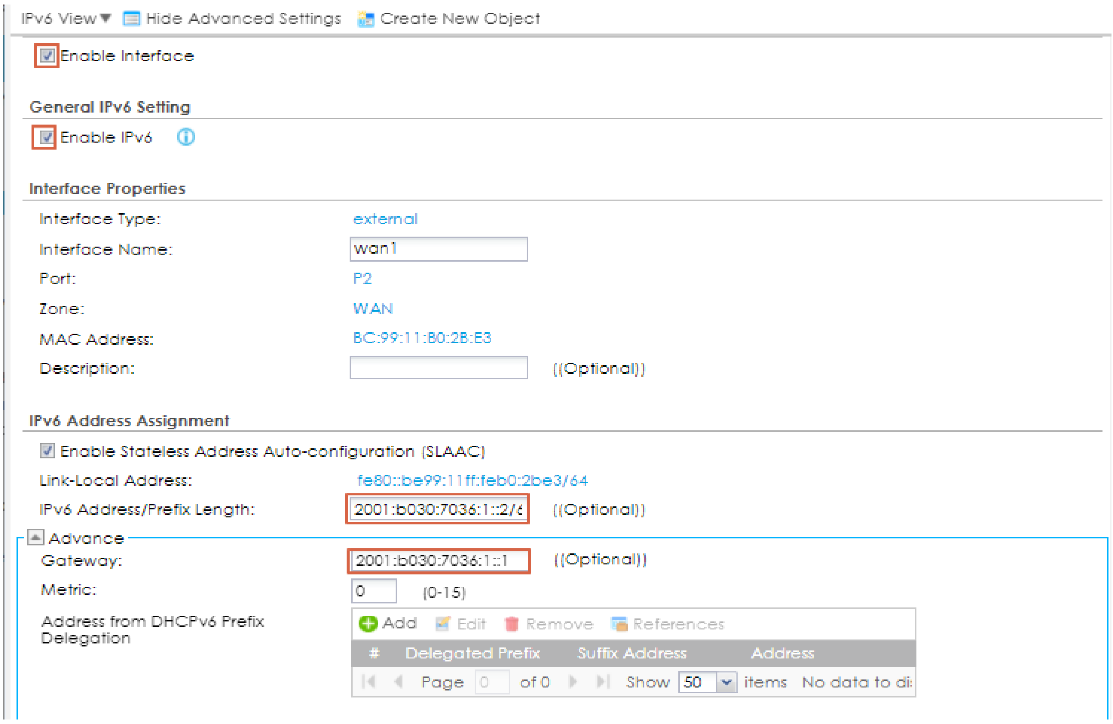

LAN
WAN
Wan IP:2001:b030:7036:1::2/64
Gateway:2001:b030:7036:1::1
Lan IP:2001:b030:7036:99::1/64

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP/USG Flex (Firmware Version: 5.00)

Configure on the Wan IPv6 interface

In the Configuration > Ethernet > IPv6 Configuration section, double-click the WAN interface you want to modify.

Choose IPv6 View, Enable Interface and Enable IPv6. In IPv6Address Assignment text box, enable Stateless Address Auto-configuration (SLAAC)
Fill IPv6 address: 2001:b030:7036:1::2/64 on IPv6 Address/Prefix Length
Fill IPv6 Gateway IP: 2001:b030:7036:1::1



☑ Enable Interface

General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Type:	external
Interface Name:	wan1
Port:	P2
Zone:	WAN
MAC Address:	BC:99:11:B0:2B:E3
Description:	((Optional))

IPv6 Address Assignment

☑ Enable Stateless Address Auto-configuration (SLAAC)

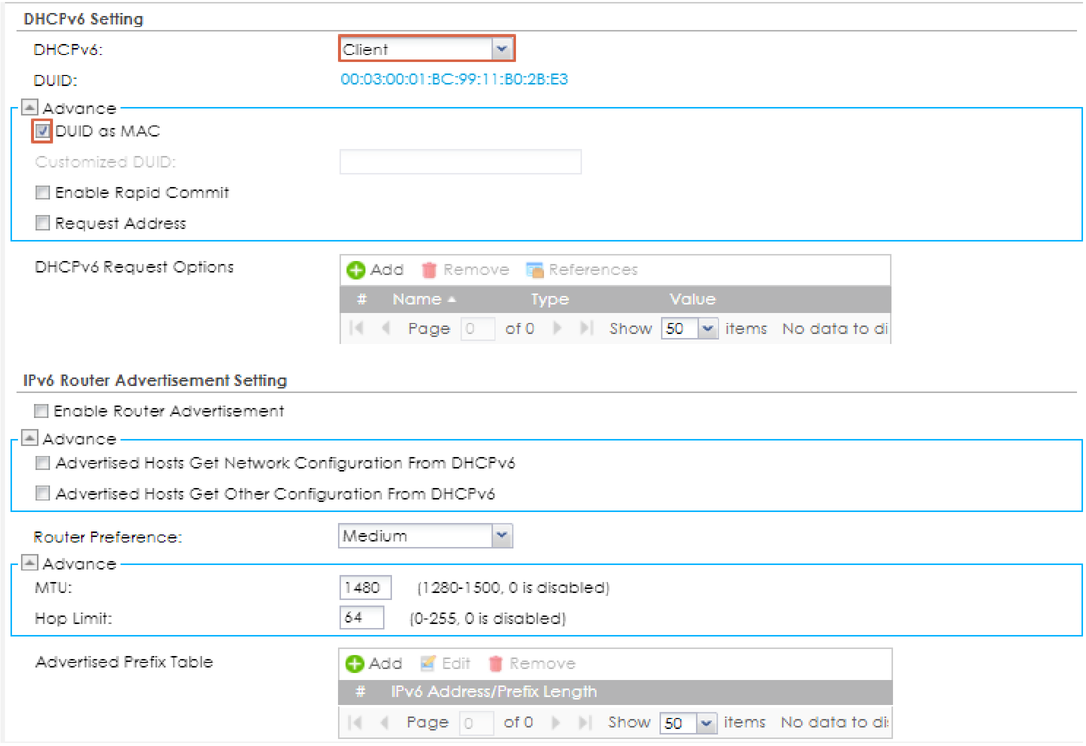
Link-Local Address:	fe80::be99:11ff:feb0:2be3/64
IPv6 Address/Prefix Length:	2001:b030:7036:1::2/6 ((Optional))

Advance

Gateway:	2001:b030:7036:1::1 ((Optional))
Metric:	0 (0-15)
Address from DHCPv6 Prefix Delegation	

#	Delegated Prefix	Suffix Address	Address

On DHCPv6, select **Client**, then Enable **DUID as MAC**



DHCPv6 Setting

DHCPv6: Client

DUID: 00:03:00:01:BC:99:11:B0:2B:E3

Advance

☑ DUID as MAC

Customized DUID:

□ Enable Rapid Commit

□ Request Address

DHCPv6 Request Options

#	Name ▲	Type	Value

Page 0 of 0 Show 50 items No data to di

IPv6 Router Advertisement Setting

□ Enable Router Advertisement

Advance

□ Advertised Hosts Get Network Configuration From DHCPv6

□ Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

Advance

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

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

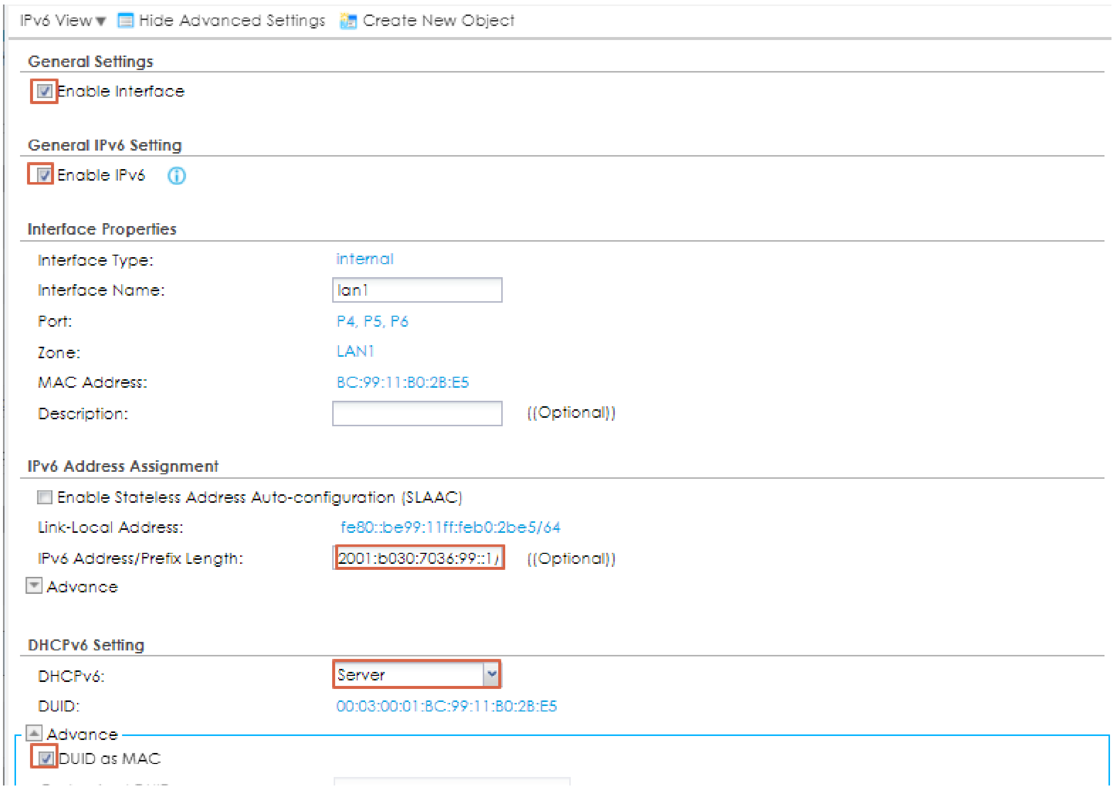
Advertised Prefix Table

#	IPv6 Address/Prefix Length

Page 0 of 0 Show 50 items No data to di

Configure on the Lan IPv6 interface

Tick **Enable IPv6**, then fill IPv6 address: **2001:b030:7036:99::1/64** which provide from ISP. Select **Server** as DHCPv6. Enable **DUID as MAC**.



General Settings

☑ Enable Interface

General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Type: internal
Interface Name: lan1
Port: P4, P5, P6
Zone: LAN1
MAC Address: BC:99:11:B0:2B:E5
Description: ((Optional))

IPv6 Address Assignment

☐ Enable Stateless Address Auto-configuration (SLAAC)
Link-Local Address: fe80::be99:11ff:feb0:2be5/64
IPv6 Address/Prefix Length: 2001:b030:7036:99::1/ ((Optional))

Advance

DHCPv6 Setting

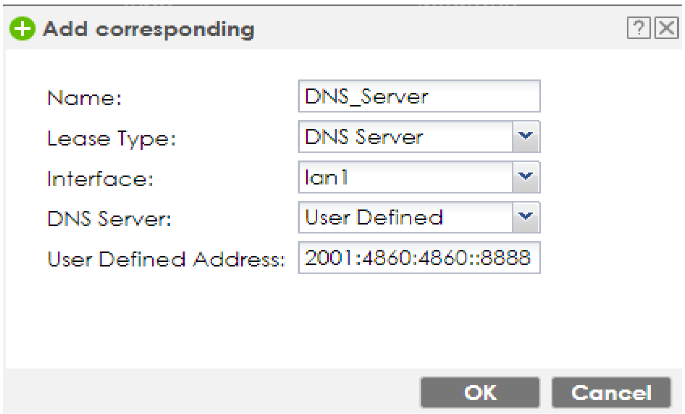
DHCPv6: Server
DUID: 00:03:00:01:BC:99:11:B0:2B:E5

Advance

☑ DUID as MAC

Next, On the DHCPv6 Lease Options, add **2001:4860:4860::8888** as DNS server

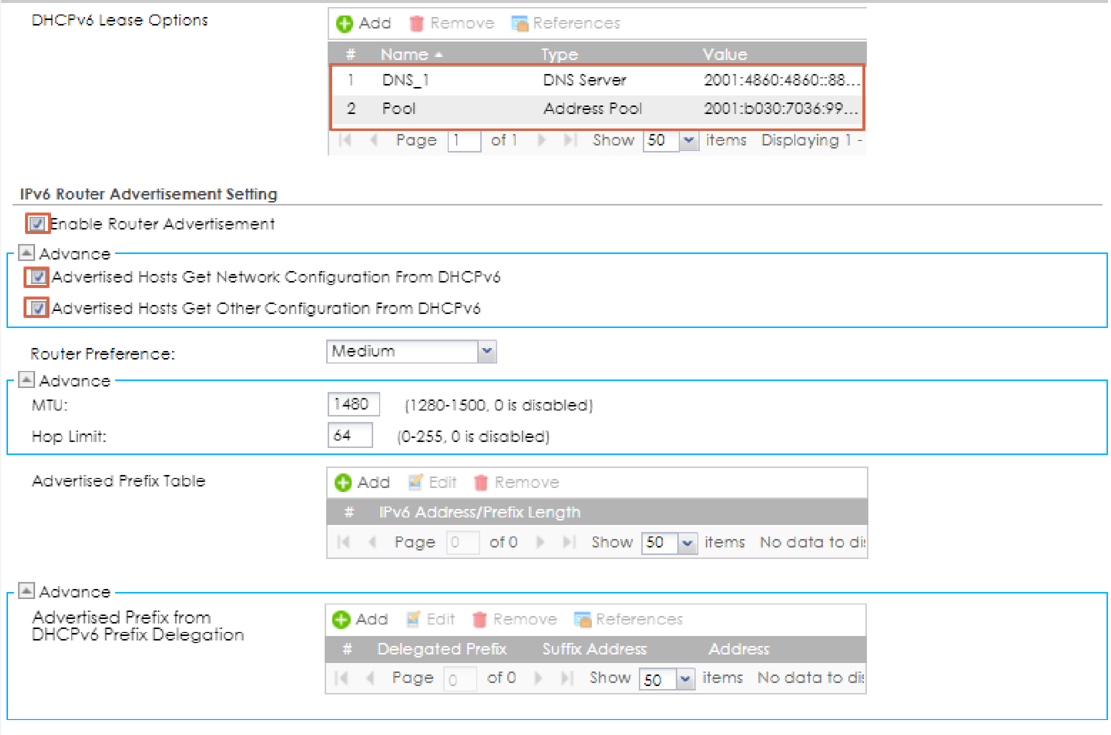
Add the **2001:b030:7036:99::10-2001:b030:7036:99::100** as Address Pool



Add corresponding

Name: DNS_Server
Lease Type: DNS Server
Interface: lan1
DNS Server: User Defined
User Defined Address: 2001:4860:4860::8888

Next, Enable **Router Advertisement**, **Advertised Hosts Get Network Configuration From DHCPv6** and **Advertised Hosts Get Other Configuration From DHCPv6**



DHCPv6 Lease Options

#	Name ▲	Type	Value
1	DNS_1	DNS Server	2001:4860:4860::88…
2	Pool	Address Pool	2001:b030:7036:99…

IPv6 Router Advertisement Setting

☑ Enable Router Advertisement

Advance

☑ Advertised Hosts Get Network Configuration From DHCPv6

☑ Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

Advance

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

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

Advertised Prefix Table

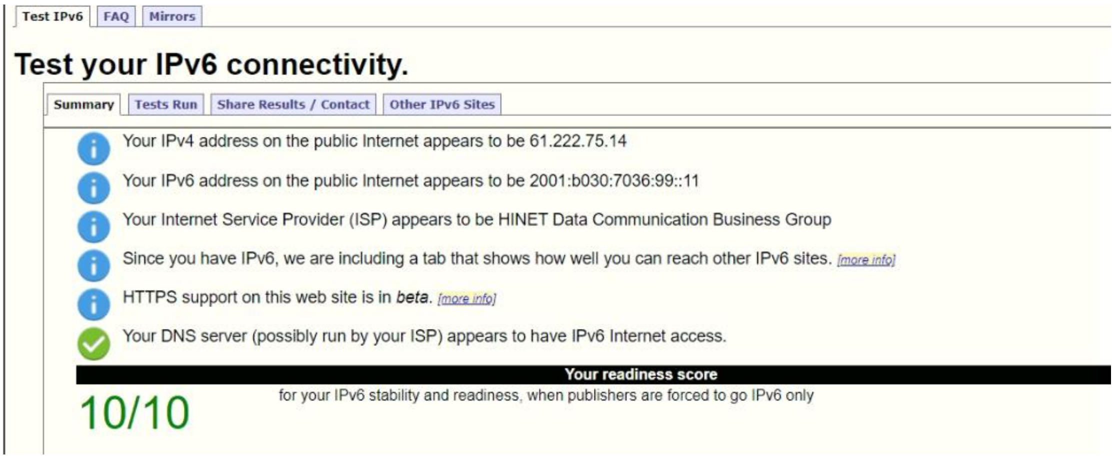
Add
Edit
Remove
# IPv6 Address/Prefix Length
Page 0 of 0 Show 50 items No data to di

Advance

Advertised Prefix from DHCPv6 Prefix Delegation

Add
Edit
Remove
References
# Delegated Prefix Suffix Address Address
Page 0 of 0 Show 50 items No data to di

Test the Result



Test your IPv6 connectivity.

Your IPv4 address on the public Internet appears to be 61.222.75.14

Your IPv6 address on the public Internet appears to be 2001:b030:7036:99::11

Your Internet Service Provider (ISP) appears to be HINET Data Communication Business Group

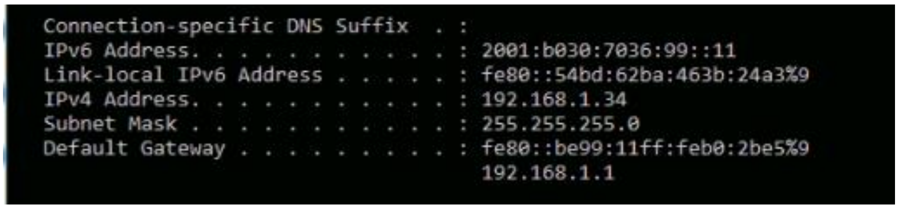
Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [more info]

HTTPS support on this web site is in *beta*. [more info]

✓ Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

Your readiness score

10/10 for your IPv6 stability and readiness, when publishers are forced to go IPv6 only



```
Connection-specific DNS Suffix  . :
IPv6 Address. . . . . . . . . . . : 2001:b030:7036:99::11
Link-local IPv6 Address . . . . . : fe80::54bd:62ba:463b:24a3%9
IPv4 Address. . . . . . . . . . . : 192.168.1.34
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : fe80::be99:11ff:feb0:2be5%9
                                    192.168.1.1
```

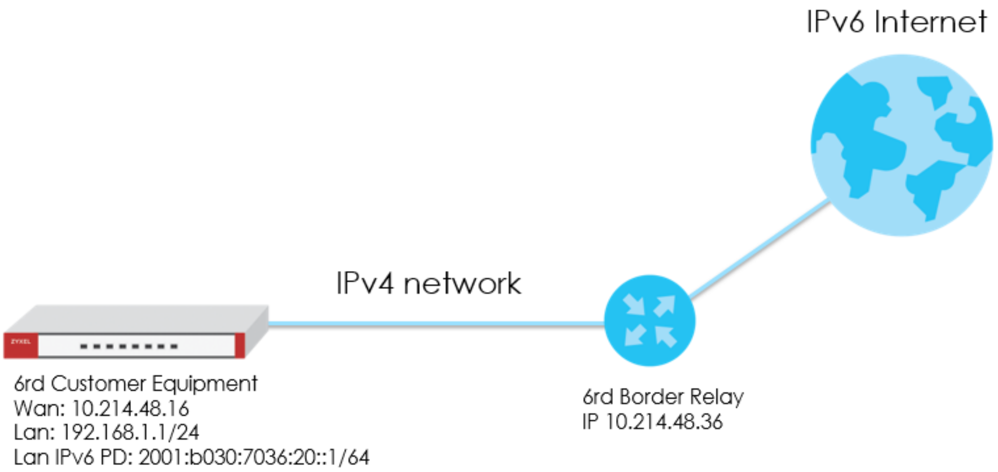
How to Set Up 6rd on the WAN and autoconf on the LAN

This example shows how to configure your ATP/USG Flex's with 6rd (IPv6 rapid deployment) to access Internet IPv6. It is IPv6 in IPv4 encapsulation in order to transit IPv4-only network infrastructure.

In this scenario:

6rd CE (Customer Equipment) is 10.214.48.16

6rd BR（Border Relay） is 10.214.48.36, which is provided by ISP. The given prefix for LAN is 2001:b030:7036:20::1/64



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP/USG Flex (Firmware Version: 5.00)

Setting Up the IPv6 tunnel for 6rd scenario

Tunnel

1. In the Configuration > Network > Interface > tunnel Configuration section, click Add to create a tunnel.

2. Fill in following information for tunnel setting in this scenario.

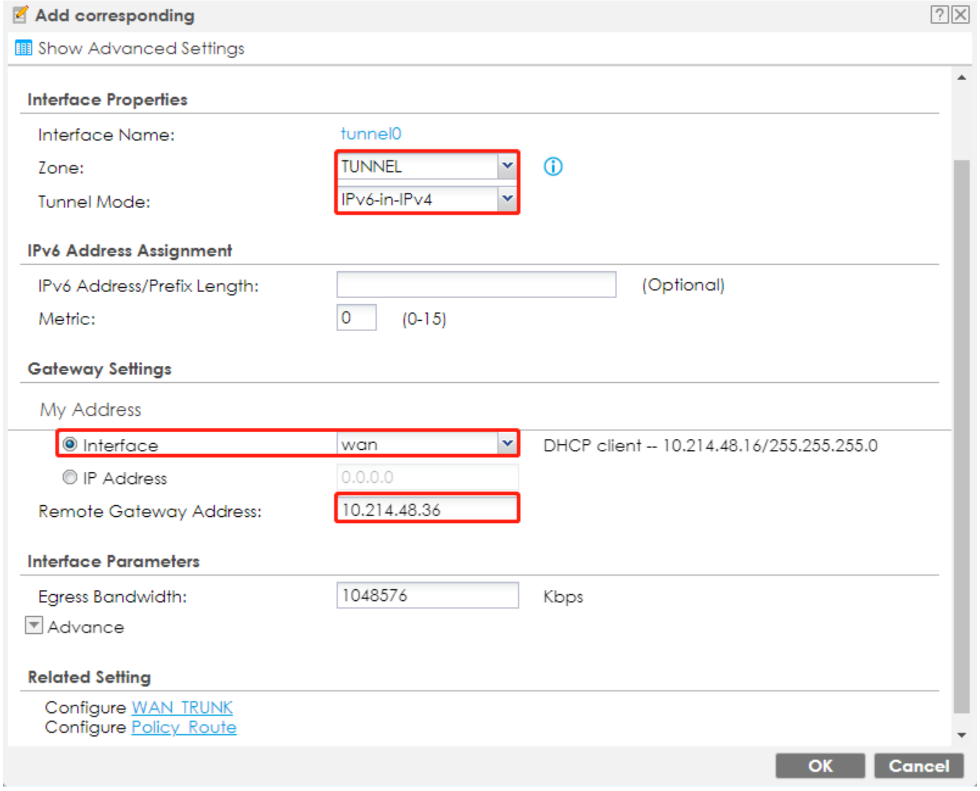
Interface name: Tunnel0

Zone: Tunnel

Tunnel mode: IPv6-in-IPv4

My address: Wan interface

Remote Gateway address : 10.214.48.36 （Border Relay）



Add corresponding

Show Advanced Settings

Interface Properties

Interface Name: tunnel0

Zone: TUNNEL

Tunnel Mode: IPv6-in-IPv4

IPv6 Address Assignment

IPv6 Address/Prefix Length: (Optional)

Metric: 0 (0-15)

Gateway Settings

My Address

● Interface wan DHCP client -- 10.214.48.16/255.255.255.0

○ IP Address 0.0.0.0

Remote Gateway Address: 10.214.48.36

Interface Parameters

Egress Bandwidth: 1048576 Kbps

Advance

Related Setting

Configure WAN TRUNK

Configure Policy Route

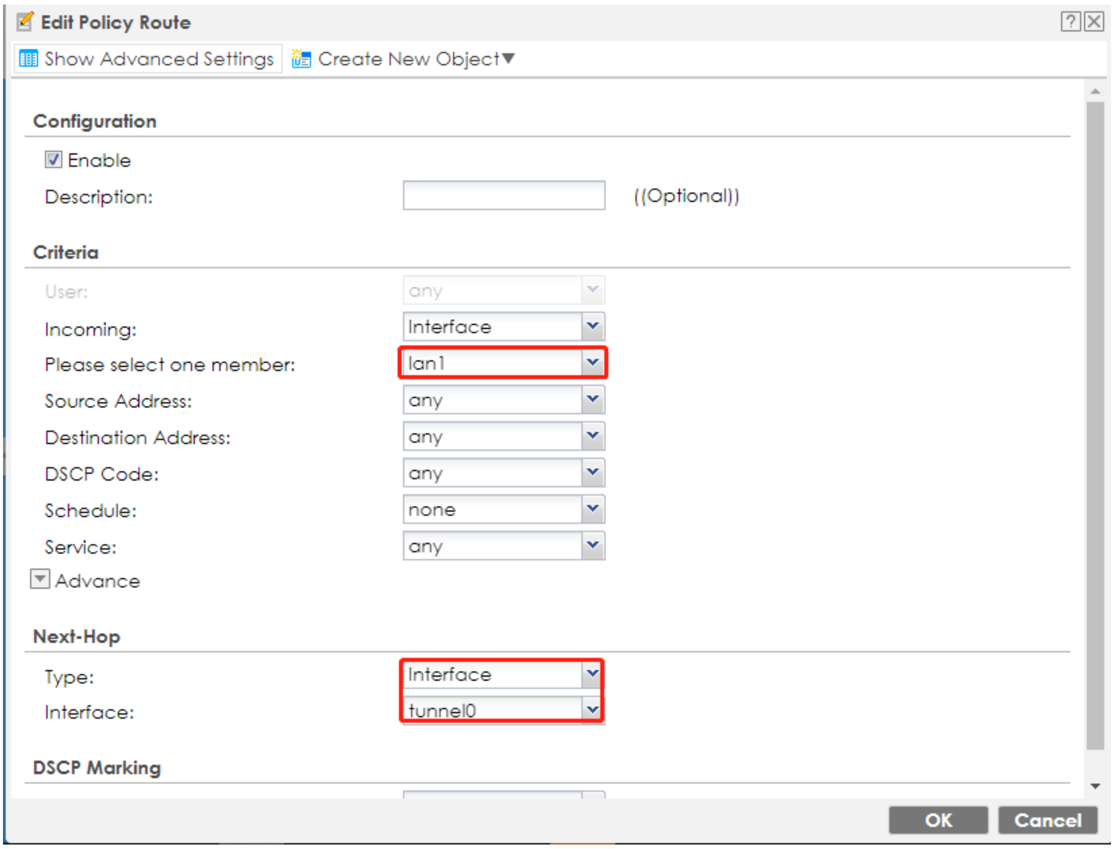
Policy route

Go to Configuration > Network > Routing > Policy route. click Add to create a policy route for V6 routing.

Incoming interface: lan1

Destination Address: any

Next hop: Tunnel0



Configuration

☑ Enable

Description: ((Optional))

Criteria

User: any

Incoming: Interface

Please select one member: lan1

Source Address: any

Destination Address: any

DSCP Code: any

Schedule: none

Service: any

Next-Hop

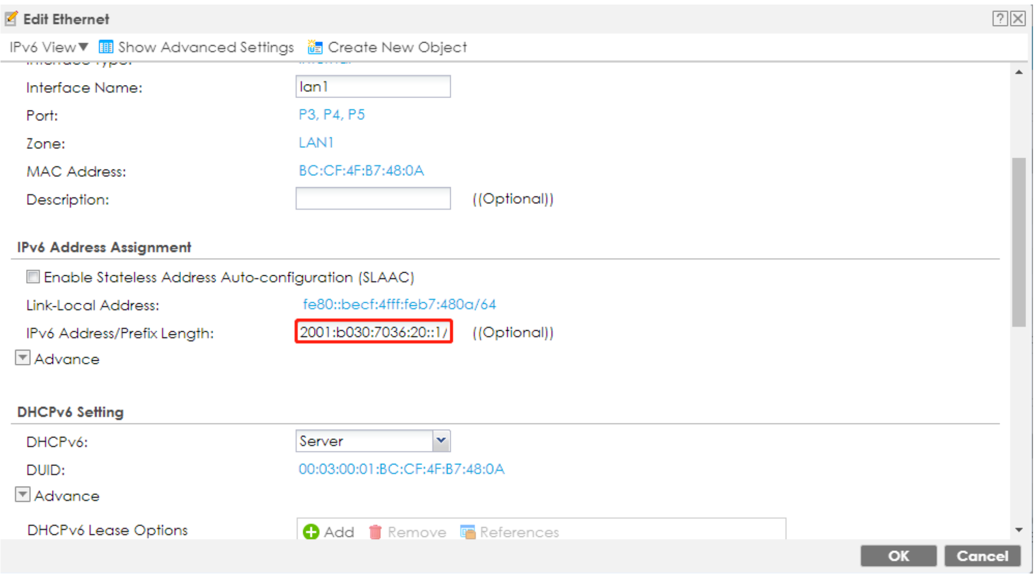
Type: Interface

Interface: tunnel0

DSCP Marking

Lan

1. In the Configuration > Network > Interface > Ethernet Configuration section, double-click the LAN interface you want to modify.
2. LAN interface IPv6 address is 2001:b030:7036:20::1/64



Interface Name: lan1

Port: P3, P4, P5

Zone: LAN1

MAC Address: BC:CF:4F:B7:48:0A

Description: ((Optional))

IPv6 Address Assignment

□ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: fe80::becf:4fff:feb7:480a/64

IPv6 Address/Prefix Length: 2001:b030:7036:20::1/ ((Optional))

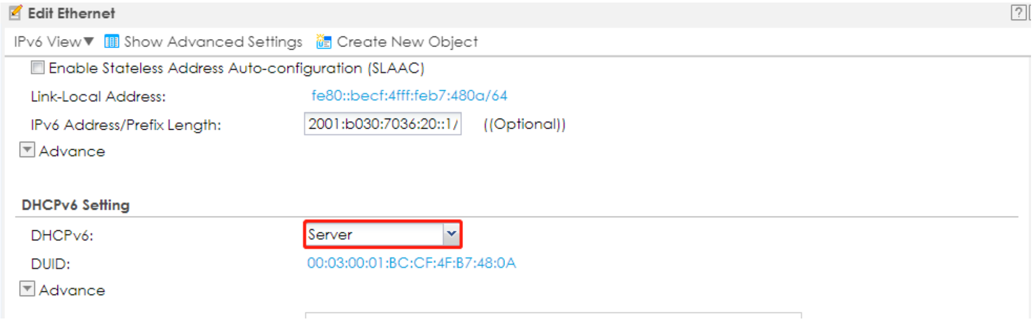
DHCPv6 Setting

DHCPv6: Server

DUID: 00:03:00:01:BC:CF:4F:B7:48:0A

DHCPv6 Lease Options

3. Enable IPv6 DHCP server.



□ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: fe80::becf:4fff:feb7:480a/64

IPv6 Address/Prefix Length: 2001:b030:7036:20::1/ ((Optional))

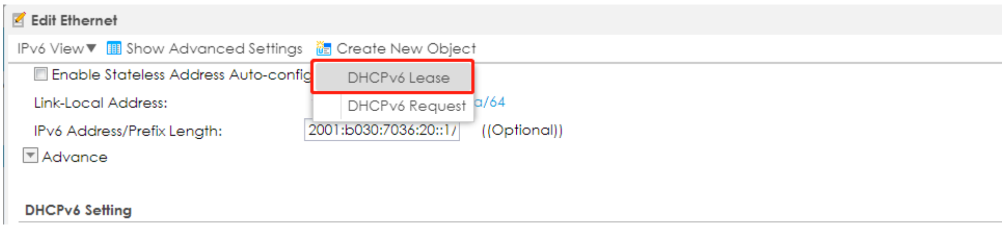
DHCPv6 Setting

DHCPv6: Server

DUID: 00:03:00:01:BC:CF:4F:B7:48:0A

4. Add DHCP release object for LAN DNS setting.

Create New Object > DHCPv6 Lease



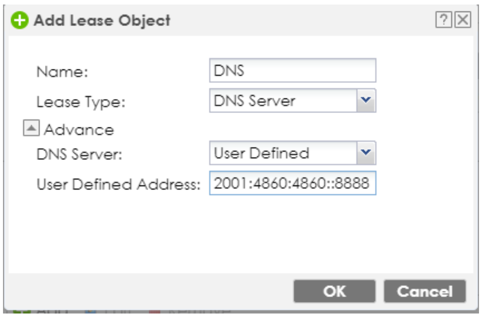
□ Enable Stateless Address Auto-config

Link-Local Address: a/64

IPv6 Address/Prefix Length: 2001:b030:7036:20::1/ ((Optional))

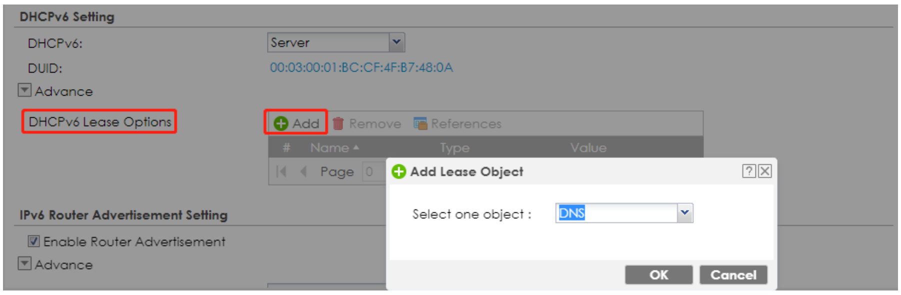
DHCPv6 Setting

In this scenario, we use Google V6 DNS server for LAN client. Click OK to save.



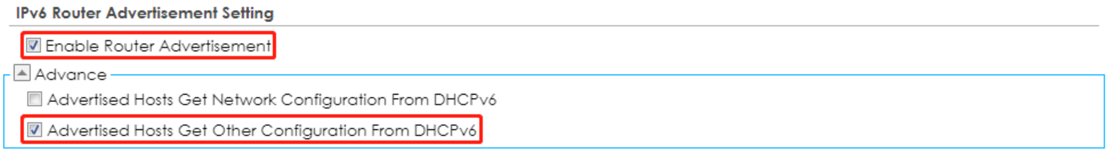
Name: DNS
Lease Type: DNS Server
Advance
DNS Server: User Defined
User Defined Address: 2001:4860:4860::8888

Add this Lease object in DHCPv6 Lease options.



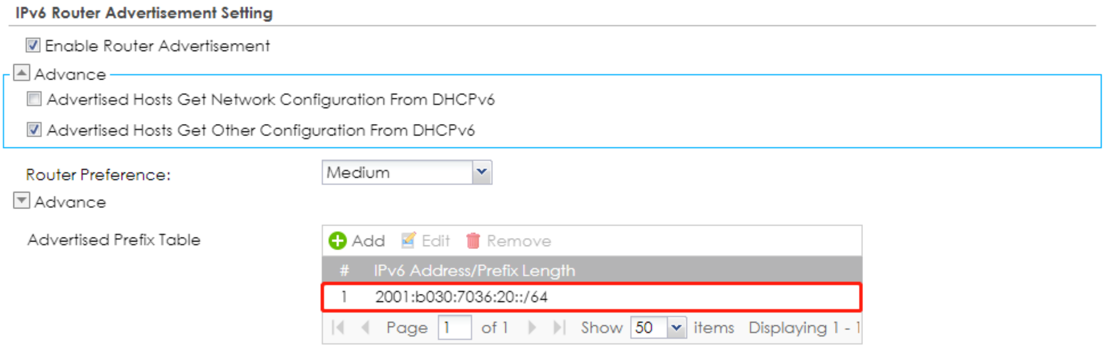
DHCPv6: Server
DUID: 00:03:00:01:BC:CF:4F:B7:48:0A
Advance
DHCPv6 Lease Options
Select one object : DNS
☑ Enable Router Advertisement
Advance

5. Tick “Enable Router Advertisement”, and "Advertised Hosts Get Other Configuration From DHCPv6".



☑ Enable Router Advertisement
Advance
□ Advertised Hosts Get Network Configuration From DHCPv6
☑ Advertised Hosts Get Other Configuration From DHCPv6

6. Set up Advertised Prefix from DHCPv6 Prefix Delegation. In this scenario, we set 2001:b030:7036:20::/64 for LAN prefix.



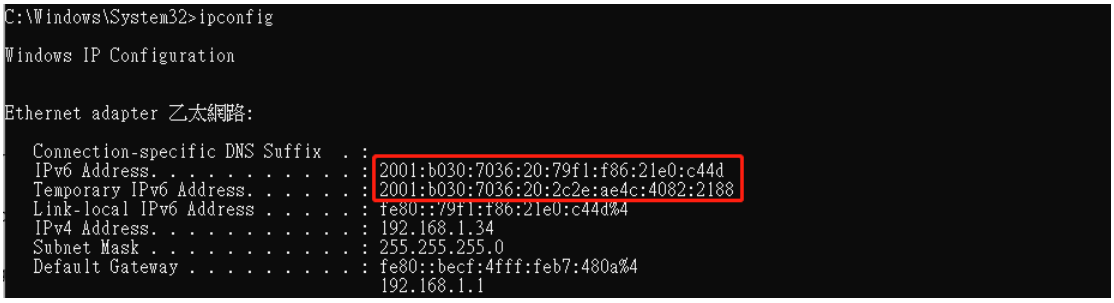
☑ Enable Router Advertisement
Advance
□ Advertised Hosts Get Network Configuration From DHCPv6
☑ Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium
Advance
Advertised Prefix Table

#	IPv6 Address/Prefix Length
1	2001:b030:7036:20::/64

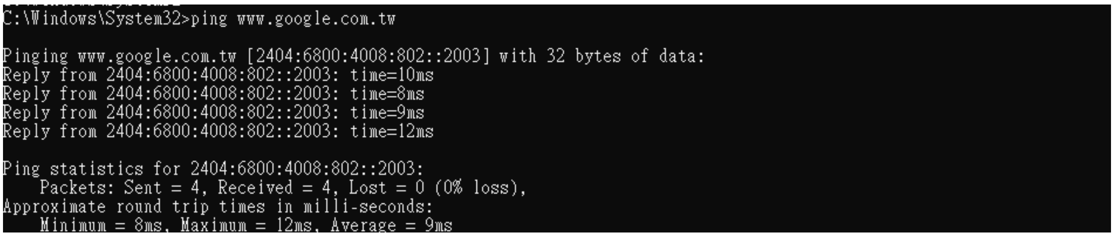
Test the Result

Client IPv6 address.



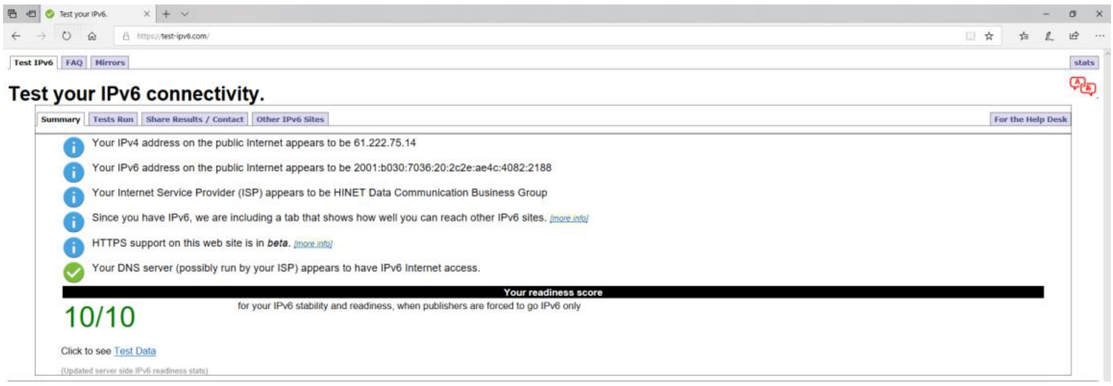
```
C:\Windows\System32>ipconfig

Windows IP Configuration

Ethernet adapter 乙太網路:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:b030:7036:20:79f1:f86:21e0:c44d
   Temporary IPv6 Address. . . . . . : 2001:b030:7036:20:2c2e:ae4c:4082:2188
   Link-local IPv6 Address . . . . . : fe80::79f1:f86:21e0:c44d%4
   IPv4 Address. . . . . . . . . . . : 192.168.1.34
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::becf:4fff:feb7:480a%4
                                       192.168.1.1
```

Ping to Google web site.



```
C:\Windows\System32>ping www.google.com.tw

Pinging www.google.com.tw [2404:6800:4008:802::2003] with 32 bytes of data:
Reply from 2404:6800:4008:802::2003: time=10ms
Reply from 2404:6800:4008:802::2003: time=8ms
Reply from 2404:6800:4008:802::2003: time=9ms
Reply from 2404:6800:4008:802::2003: time=12ms

Ping statistics for 2404:6800:4008:802::2003:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 12ms, Average = 9ms
```

Test Your IPv6 connection.



Test your IPv6 connectivity.

Your IPv4 address on the public Internet appears to be 61.222.75.14

Your IPv6 address on the public Internet appears to be 2001:b030:7036:20:2c2e:ae4c:4082:2188

Your Internet Service Provider (ISP) appears to be HINET Data Communication Business Group

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [more info]

HTTPS support on this web site is in *beta*. [more info]

Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

Your readiness score

10/10 for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

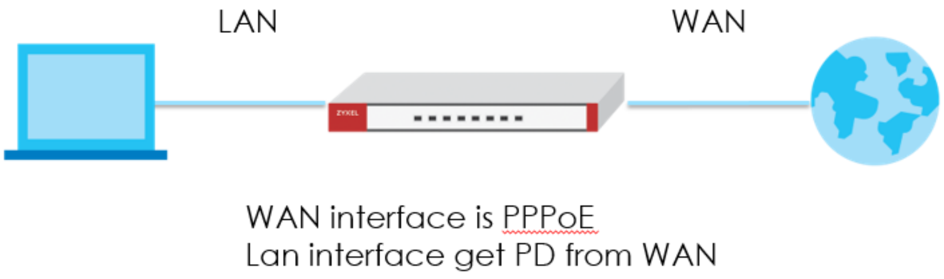
Click to see Test Data

(Updated server side IPv6 readiness stats)

How to Set Up IPv6 over PPPoE on the WAN

This example shows how to configure your ATP/USG Flex's WAN interface as PPPoE with prefix delegation. Device PPPoE interface run as DHCP client to get prefix and DNS from ISP.

In this scenario:
PPPoE interface run as DHCP client to request prefix delegation and DNS server from ISP.



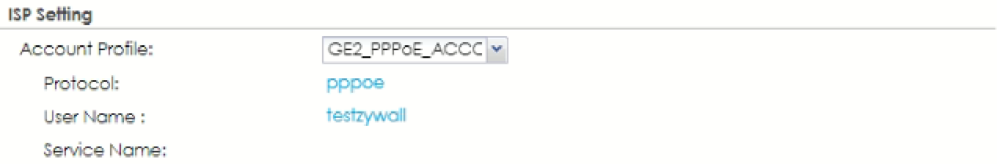
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP/USG Flex (Firmware Version: 5.00)

Setting Up the IPv6 Interfaces

Wan

1. In the Configuration > Network > Interface > PPP Configuration section, double-click the PPP interface you want to modify.

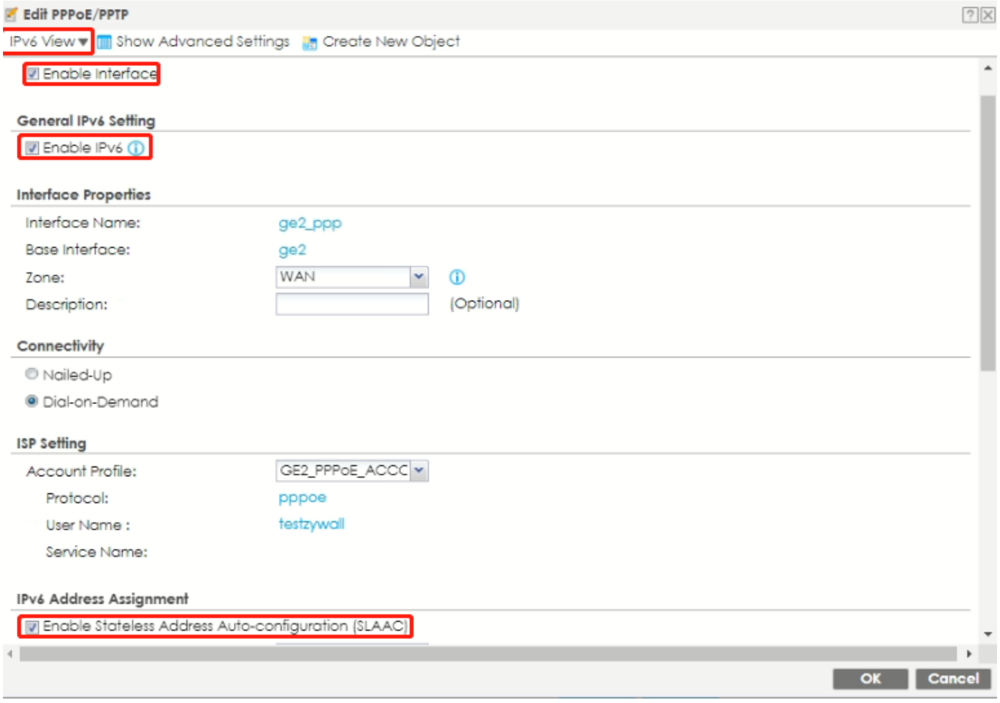
2. Select account profile in ISP Setting.



ISP Setting

Account Profile:	GE2_PPPoE_ACCC
Protocol:	pppoe
User Name :	testzywall
Service Name:	

3. Choose IPv6 View, Enable Interface and Enable IPv6. In IPv6Address Assignment text box, enable Stateless Address Auto-configuration (SLAAC)



☑ Enable Interface

General IPv6 Setting

☑ Enable IPv6

Interface Properties

Interface Name:	ge2_ppp	
Base Interface:	ge2	
Zone:	WAN	
Description:		(Optional)

Connectivity

○ Nailed-Up
● Dial-on-Demand

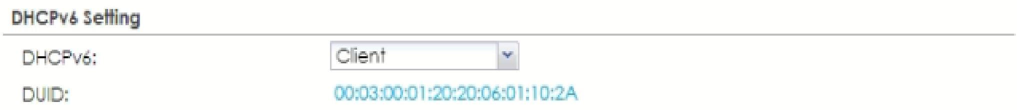
ISP Setting

Account Profile:	GE2_PPPoE_ACCC
Protocol:	pppoe
User Name :	testzywall
Service Name:	

IPv6 Address Assignment

☑ Enable Stateless Address Auto-configuration (SLAAC)

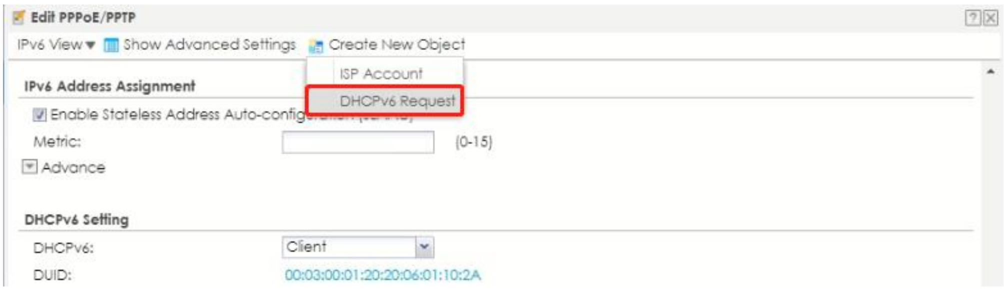
4. Set up interface as V6 client.



DHCPv6 Setting

DHCPv6:	Client
DUID:	00:03:00:01:20:20:06:01:10:2A

5. Create DHCPv6 Request object to get Prefix Delegation and DNS from ISP.



IPv6 Address Assignment

☑ Enable Stateless Address Auto-config

Metric: (0-15)

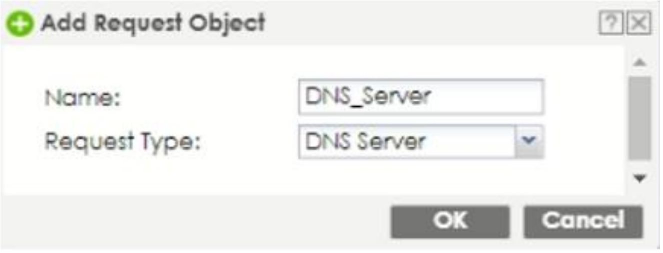
Advance

DHCPv6 Setting

DHCPv6: Client

DUID: 00:03:00:01:20:20:06:01:10:2A

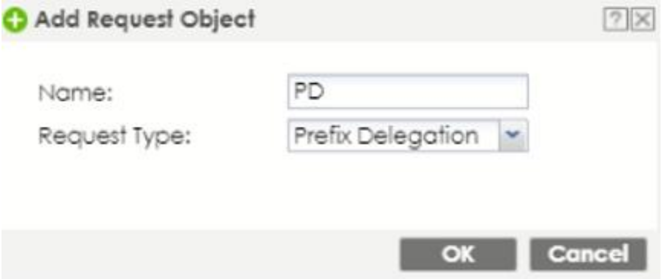
DNS object



Name: DNS_Server

Request Type: DNS Server

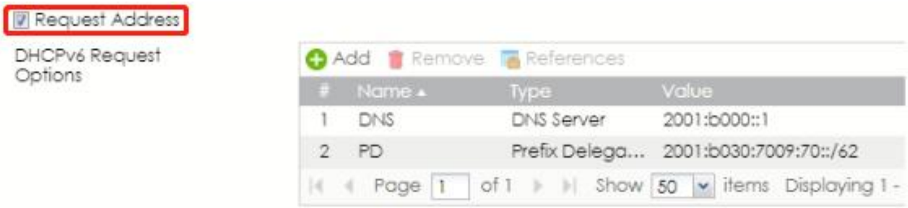
Prefix delegation



Name: PD

Request Type: Prefix Delegation

6. Tick Request Address.



☑ Request Address

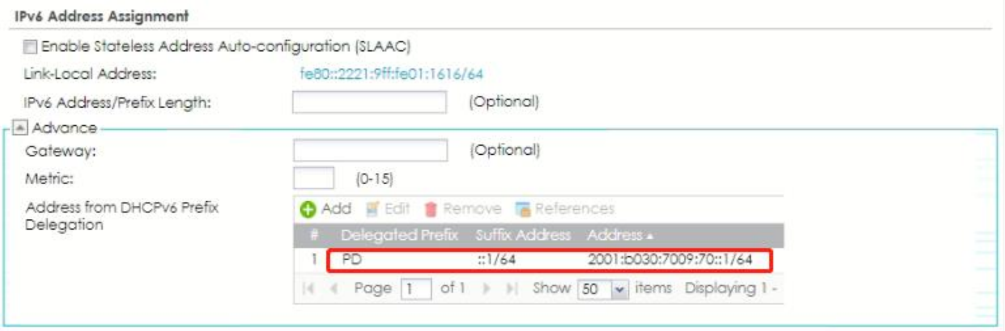
DHCPv6 Request Options

#	Name ▴	Type	Value
1	DNS	DNS Server	2001:b000::1
2	PD	Prefix Delega...	2001:b030:7009:70::/62

Lan

1. In the Configuration > Network > Interface > Ethernet Configuration section, double-click the LAN interface you want to modify.

2. LAN interface IP assignment gets from Prefix Delegation and Suffix setting. In this case, we set suffix to ::1/64



IPv6 Address Assignment

□ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: fe80::2221:9ff:fe01:1616/64

IPv6 Address/Prefix Length: (Optional)

Advance

Gateway: (Optional)

Metric: (0-15)

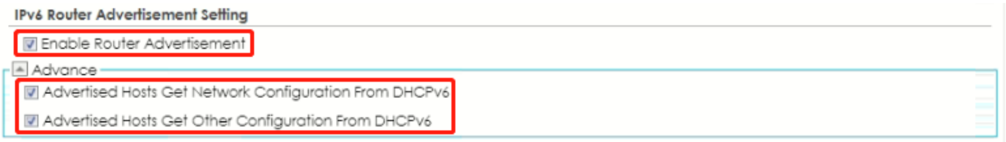
Address from DHCPv6 Prefix Delegation

Add Edit Remove References

#	Delegated Prefix	Suffix Address	Address
1	PD	::1/64	2001:b030:7009:70::1/64

Page 1 of 1 Show 50 items Displaying 1 -

3. Tick "Enable Router Advertisement", "Advertised Hosts Get Network Configuration From DHCPv6", and "Advertised Hosts Get Other Configuration From DHCPv6".



IPv6 Router Advertisement Setting

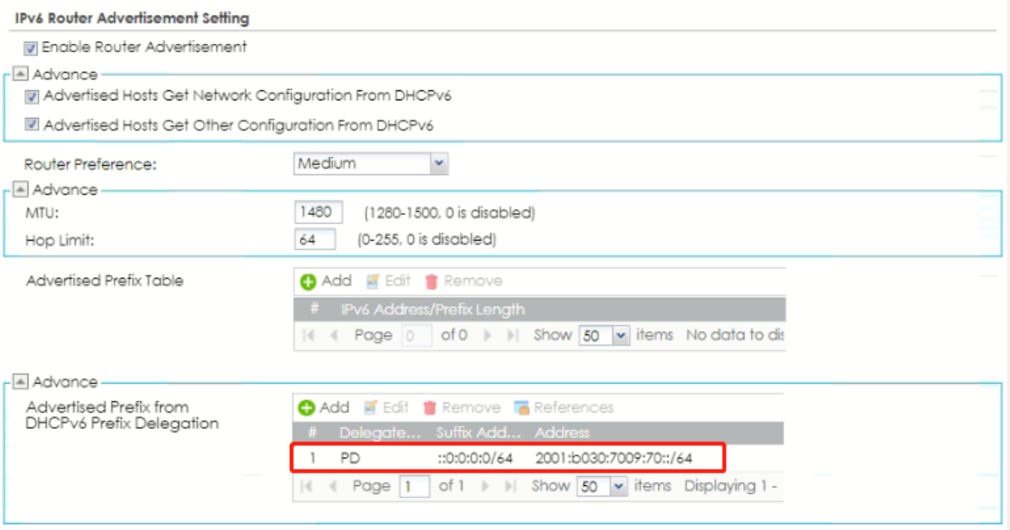
☑ Enable Router Advertisement

Advance

☑ Advertised Hosts Get Network Configuration From DHCPv6

☑ Advertised Hosts Get Other Configuration From DHCPv6

4. Set up Advertised Prefix from DHCPv6 Prefix Delegation.



IPv6 Router Advertisement Setting

☑ Enable Router Advertisement

Advance

☑ Advertised Hosts Get Network Configuration From DHCPv6

☑ Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

Advance

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

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

Advertised Prefix Table

#	IPv6 Address/Prefix Length

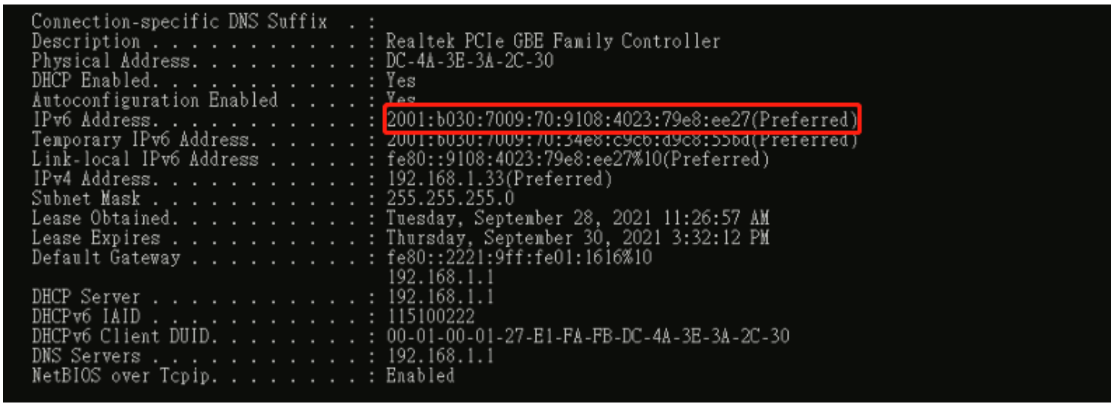
Advance

Advertised Prefix from DHCPv6 Prefix Delegation

#	Delegate...	Suffix Add...	Address
1	PD	::0:0:0:0/64	2001:b030:7009:70::/64

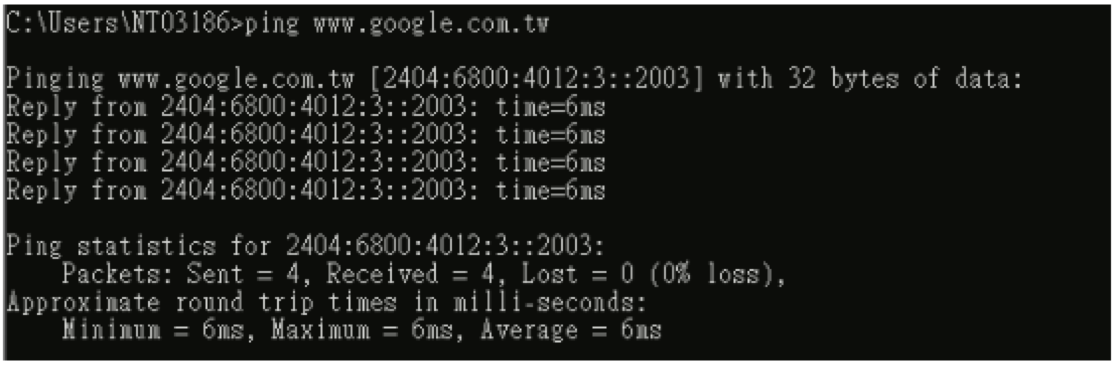
Test Result

Client IPv6 address.



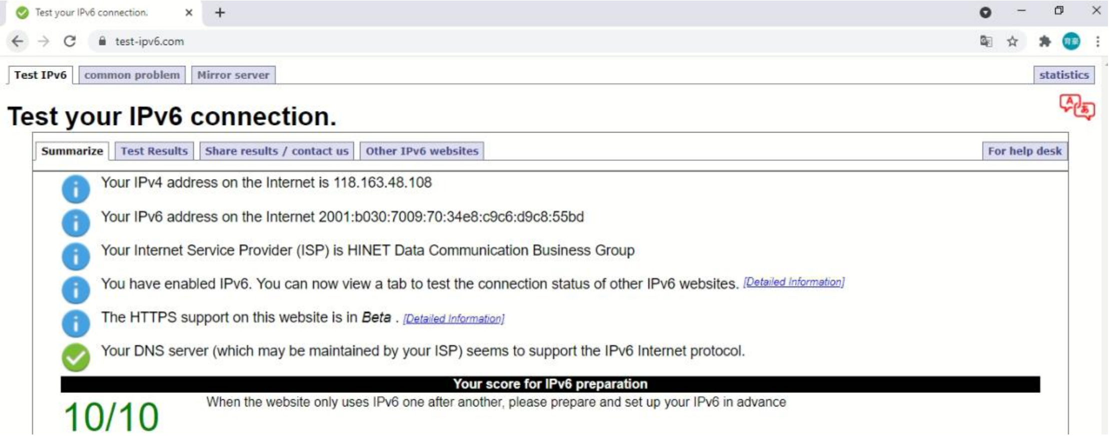
```
   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : DC-4A-3E-3A-2C-30
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:b030:7009:70:9108:4023:79e8:ee27(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:b030:7009:70:34e8:c9c6:d9c8:55bd(Preferred)
   Link-local IPv6 Address . . . . . : fe80::9108:4023:79e8:ee27%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.1.33(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Tuesday, September 28, 2021 11:26:57 AM
   Lease Expires . . . . . . . . . . : Thursday, September 30, 2021 3:32:12 PM
   Default Gateway . . . . . . . . . : fe80::2221:9ff:fe01:1616%10
                                       192.168.1.1
   DHCP Server . . . . . . . . . . . : 192.168.1.1
   DHCPv6 IAID . . . . . . . . . . . : 115100222
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-27-E1-FA-FB-DC-4A-3E-3A-2C-30
   DNS Servers . . . . . . . . . . . : 192.168.1.1
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

Ping to Google web site.



```
C:\Users\NT03186>ping www.google.com.tw

Pinging www.google.com.tw [2404:6800:4012:3::2003] with 32 bytes of data:
Reply from 2404:6800:4012:3::2003: time=6ms
Reply from 2404:6800:4012:3::2003: time=6ms
Reply from 2404:6800:4012:3::2003: time=6ms
Reply from 2404:6800:4012:3::2003: time=6ms

Ping statistics for 2404:6800:4012:3::2003:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 6ms, Maximum = 6ms, Average = 6ms
```

Test Your IPv6 connection.



Test your IPv6 connection.

Your IPv4 address on the Internet is 118.163.48.108

Your IPv6 address on the Internet 2001:b030:7009:70:34e8:c9c6:d9c8:55bd

Your Internet Service Provider (ISP) is HINET Data Communication Business Group

You have enabled IPv6. You can now view a tab to test the connection status of other IPv6 websites. [Detailed Information]

The HTTPS support on this website is in *Beta* . [Detailed Information]

Your DNS server (which may be maintained by your ISP) seems to support the IPv6 Internet protocol.

Your score for IPv6 preparation

10/10

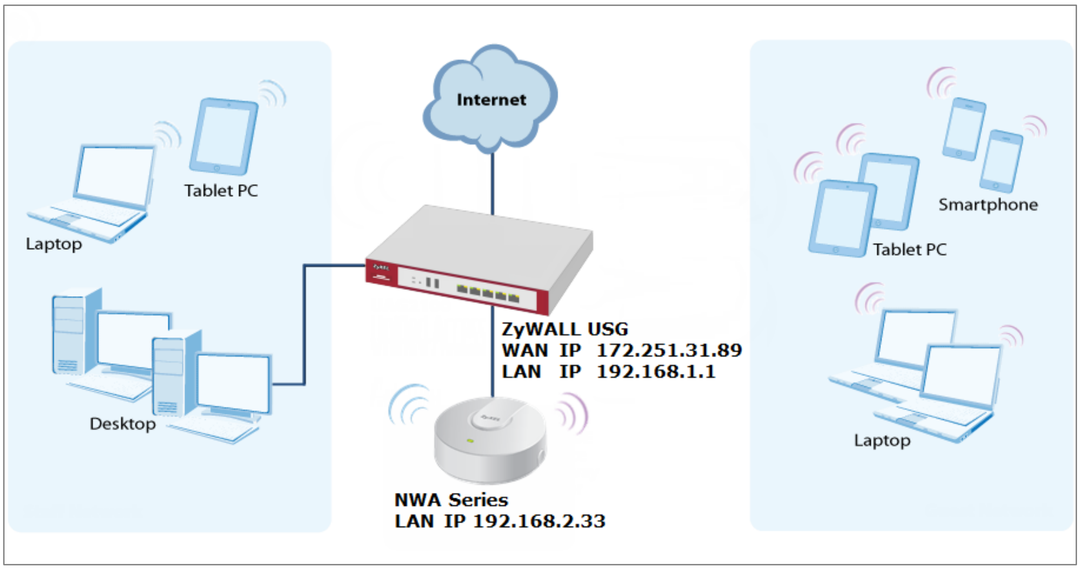
When the website only uses IPv6 one after another, please prepare and set up your IPv6 in advance

Chapter 6- Wireless

How to Set Up a WiFi Network with ZyXEL APs

This is an example of using ZyWALL/USG to manage the Access Points (APs) and allow wireless access to the network.

ZyWALL/USG as AP Controller Example

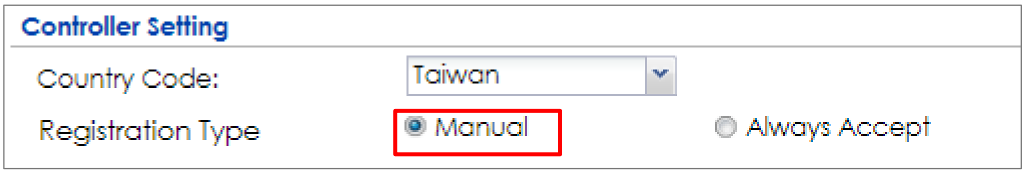


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the AP Management on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Wireless > Controller > Configuration**, set **Registration Type** to **Manual**. This is recommended as the registration mechanism cannot automatically differentiate between friendly and rogue APs.

CONFIGURATION > Wireless > Controller > Configuration



Controller Setting

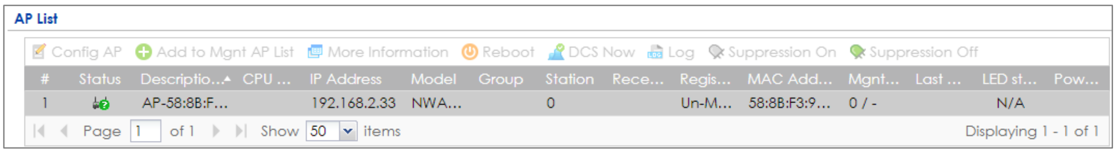
Country Code: Taiwan

Registration Type ● Manual ○ Always Accept

Connect the ZyXEL AP unit to the lan interface.

Go to **MONITOR > Wireless > AP Information > AP List** and the ZyXEL AP is listed. A green question mark displays in the Status column since the AP is not yet managed by the ZyWALL/USG. Select the listed AP and click **Add to Mgnt AP List** on the upper bar.

Monitor > Wireless > AP Information > AP List



AP List

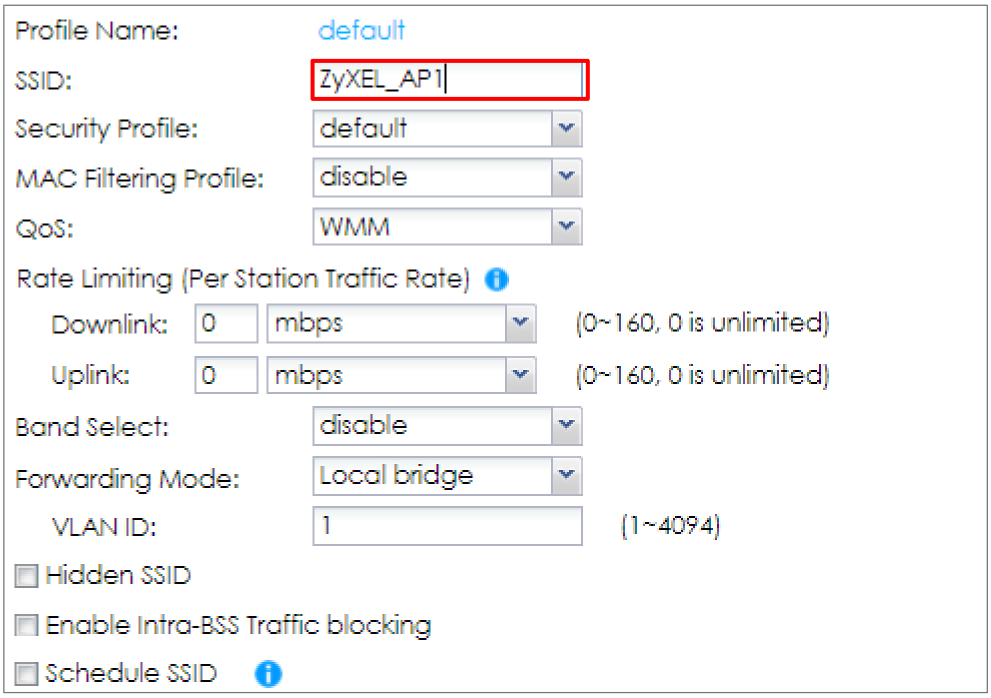
#	Status	Descriptio...	CPU ...	IP Address	Model	Group	Station	Rece...	Regis...	MAC Add...	Mgnt...	Last ...	LED st...	Pow...
1	?	AP-58:8B:F...		192.168.2.33	NWA...		0		Un-M...	58:8B:F3:9...	0 / -		N/A	

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

Note: The APs may take few minutes to appear in the AP List.

Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List** to configure a name to identify the **SSID**.

CONFIGURATION > Object > AP Profile > SSID > SSID List



Profile Name:	default		
SSID:	ZyXEL_AP1		
Security Profile:	default		
MAC Filtering Profile:	disable		
QoS:	WMM		
Rate Limiting (Per Station Traffic Rate)			
Downlink:	0	mbps	(0~160, 0 is unlimited)
Uplink:	0	mbps	(0~160, 0 is unlimited)
Band Select:	disable		
Forwarding Mode:	Local bridge		
VLAN ID:	1	(1~4094)	

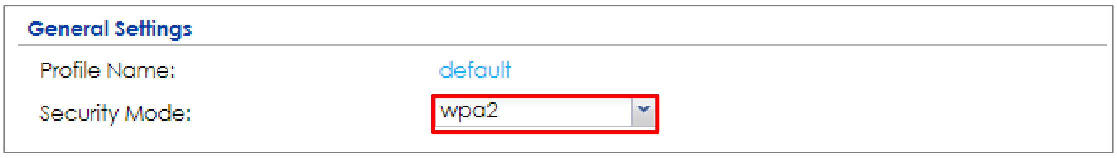
□ Hidden SSID

□ Enable Intra-BSS Traffic blocking

□ Schedule SSID

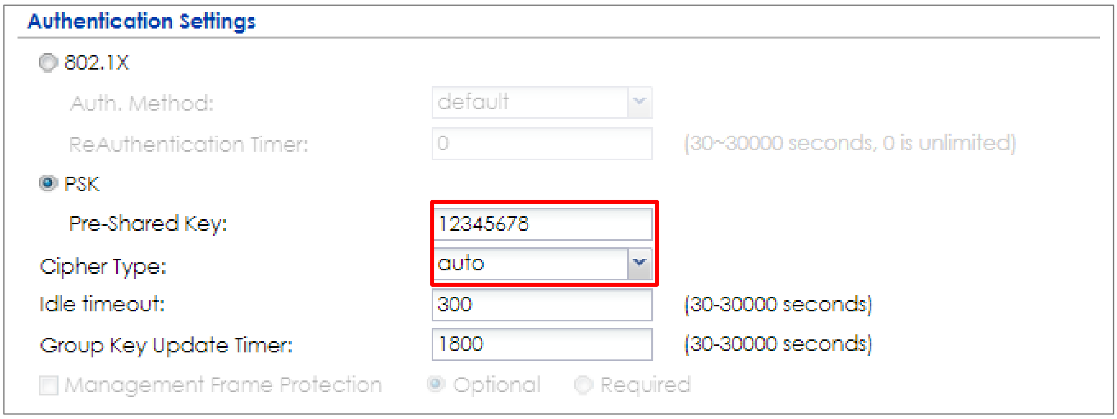
Go to **CONFIGURATION > Object > AP Profile > SSID > Security List** to select the **Security Mode** to be the **wpa2**. Then, set a **Pre-Shared Key** (8-63 characters) and select the **Cipher Type** to be the **auto** to have ZyWALL/USG automatically chooses the best available cipher based on the cipher currently in use by the wireless network. Click **OK**.

CONFIGURATION > Object > AP Profile > SSID > Security List



General Settings

Profile Name:	default
Security Mode:	wpa2



Authentication Settings

○ 802.1X

Auth. Method: default

ReAuthentication Timer: 0 (30~30000 seconds, 0 is unlimited)

● PSK

Pre-Shared Key: 12345678

Cipher Type: auto

Idle timeout: 300 (30-30000 seconds)

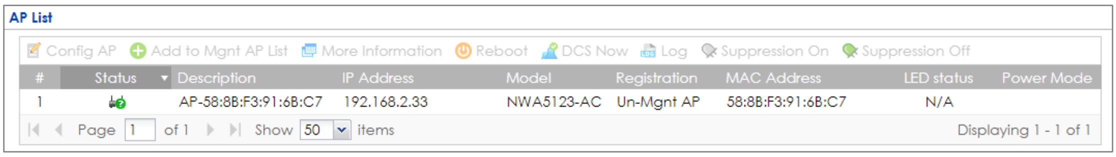
Group Key Update Timer: 1800 (30-30000 seconds)

□ Management Frame Protection ● Optional ○ Required

Test the Result

Go to the ZyWALL/USG **Monitor > Wireless > AP Information > AP List**, you can check the list of APs which are currently connected to it and the details information such as **Registration** type, **Model** and **Recent On-line Time /Last Off-line Time**.

MONITOR > Wireless > AP Information > AP List



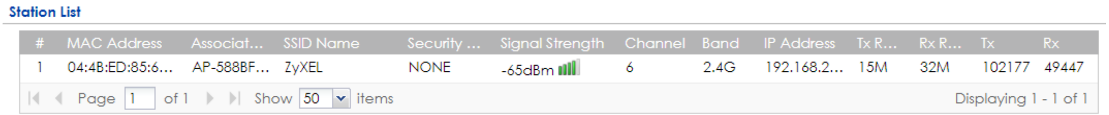
AP List

#	Status	Description	IP Address	Model	Registration	MAC Address	LED status	Power Mode
1		AP-58:8B:F3:91:6B:C7	192.168.2.33	NWA5123-AC	Un-Mgnt AP	58:8B:F3:91:6B:C7	N/A	

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

Go to the ZyWALL/USG **Monitor > Wireless > Station Info > Station List**, you can check the list of wireless stations associated with a managed AP and the details information such as **SSID Name**, **Signal Strength** and the transmit (**Tx**)/receive (**Rx**) data rate.

MONITOR > Wireless > Station Info > Station List



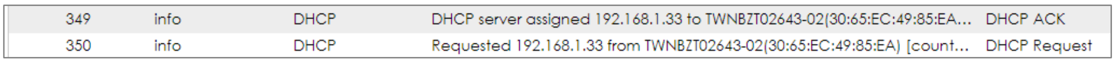
Station List

#	MAC Address	Associat...	SSID Name	Security ...	Signal Strength	Channel	Band	IP Address	Tx R...	Rx R...	Tx	Rx
1	04:4B:ED:85:6...	AP-588BF...	ZyXEL	NONE	-65dBm	6	2.4G	192.168.2...	15M	32M	102177	49447

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

Using a mobile device to connect to SSID: **ZyXEL_AP1** and type the password (zyxel123) for authentication. Go to the ZyWALL/USG **Monitor > Log**, you will see [info] log message as shown below. The ZyWALL/USG will assign an IP address to the mobile device and the mobile device can access the Internet.

MONITOR > Log



349	info	DHCP	DHCP server assigned 192.168.1.33 to TWNBZT02643-02(30:65:EC:49:85:EA...	DHCP ACK
350	info	DHCP	Requested 192.168.1.33 from TWNBZT02643-02(30:65:EC:49:85:EA) [count...	DHCP Request

What Could Go Wrong?

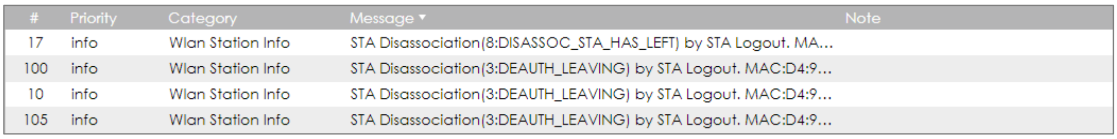
If you can't see AP information in the AP List, please check the number of APs connected to the ZyWALL/USG has exceeded the maximum Managed AP number it can support. You can check the maximum support number of each ZyWALL/USG in the Datasheet from ZyXEL Download Library - http://www.zyxel.com/support/download_landing.shtml

If your mobile device can't find the AP SSID you configured, please go **to CONFIGURATION > Object > AP Profile > SSID > SSID List** and check if the **Hidden SSID** option is enabled.

If your mobile device can't access to the Internet via AP connects to the ZyWALL/USG, please check if the LAN outgoing security policy allow access to the Internet.

If your mobile device is not connected to the AP automatically even you've joined the Wifi network before and you see [Wlan Station Info] log message as shown below, please check if this AP is removed from your mobile device's saved Wifi network list.

MONITOR > Log

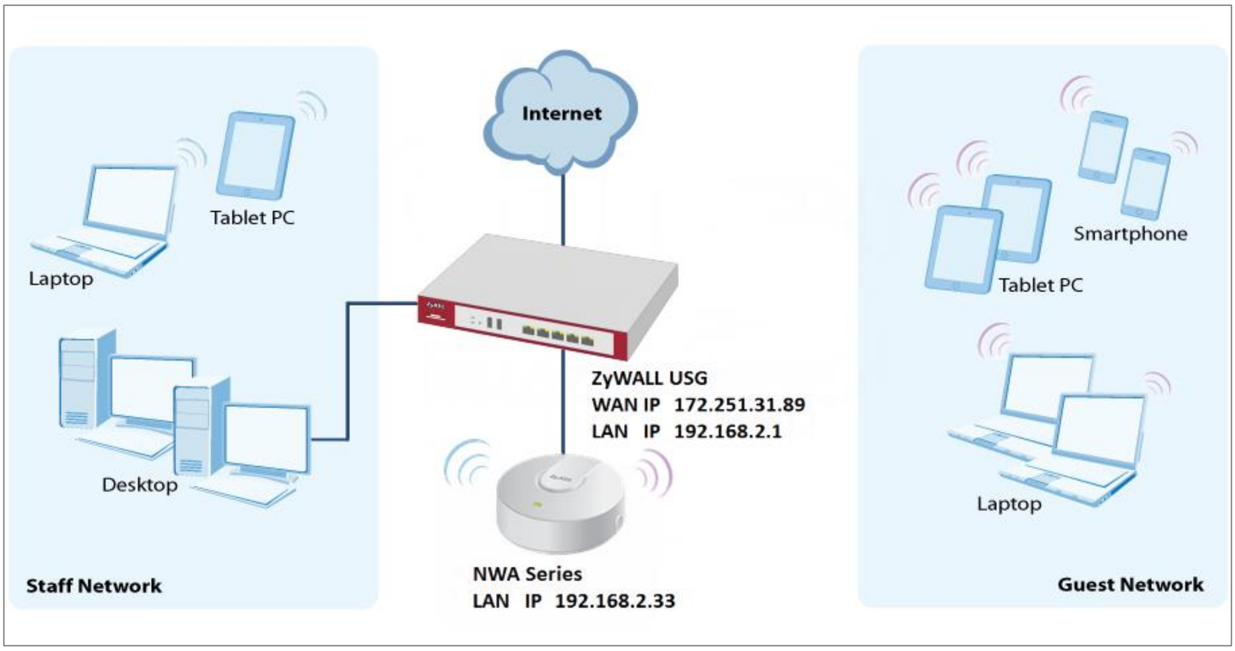


#	Priority	Category	Message ▾	Note
17	info	Wlan Station Info	STA Disassociation(8:DISASSOC_STA_HAS_LEFT) by STA Logout. MA...	
100	info	Wlan Station Info	STA Disassociation(3:DEAUTH_LEAVING) by STA Logout. MAC:D4:9...	
10	info	Wlan Station Info	STA Disassociation(3:DEAUTH_LEAVING) by STA Logout. MAC:D4:9...	
105	info	Wlan Station Info	STA Disassociation(3:DEAUTH_LEAVING) by STA Logout. MAC:D4:9...	

How to Set Up Guest WiFi Network Accounts

This is an example of using ZyWALL/USG to configure guest WiFi accounts to allow limited wireless access to the Internet using only HTTP, HTTPS, and DNS protocols. For the wireless network setup, please see the tutorial about How to Set Up WiFi with ZyXEL AP.

ZyWALL/USG with Guest WiFi Accounts Example



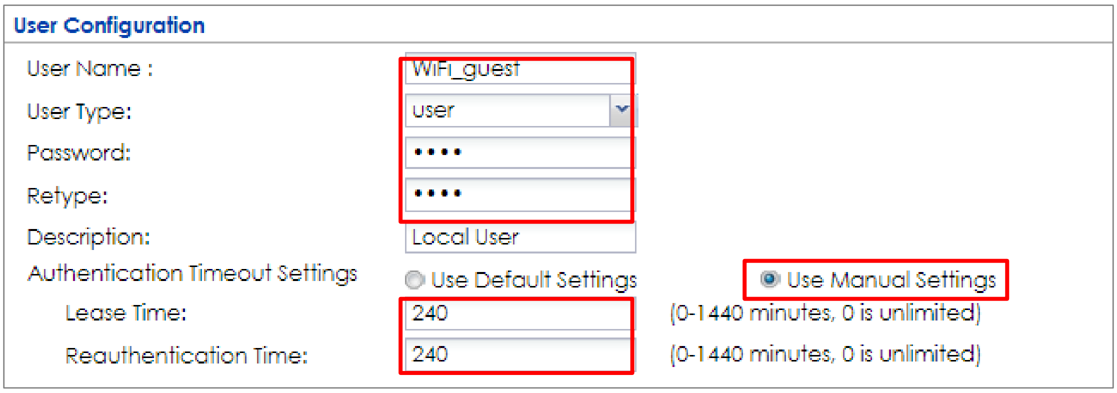
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the WiFi Guest Account, Address Range and Service Rule on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > User/Group > User > Add A User** to configure the **User Name** the guest Wi-Fi user and set **User Type** to **guest**. Set a secured **Password** (4-31 characters) and enter it again for confirmation.

Set the **Authentication Timeout Settings** to be **Use Manual Settings** to enter the number of minutes this user has to renew the current session before the user is logged out.

CONFIGURATION > Object > User/Group > User > Add A User

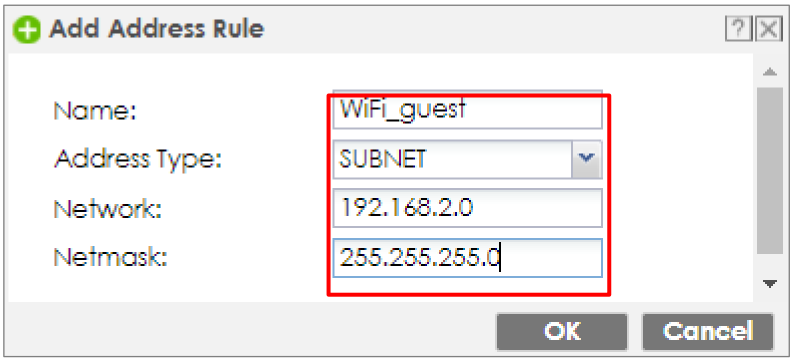


User Configuration

User Name :	WiFi_guest	
User Type:	user	
Password:	••••	
Retype:	••••	
Description:	Local User	
Authentication Timeout Settings	○ Use Default Settings	● Use Manual Settings
Lease Time:	240	(0-1440 minutes, 0 is unlimited)
Reauthentication Time:	240	(0-1440 minutes, 0 is unlimited)

In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create the guest Wi-Fi user access subnet. In this example, AP is connected to ZyWALL/USG LAN interface 192.168.2.0/24. Configure the **Name** for you to identify the Wi-Fi guest subnet. Set the **Network** to be 192.168.2.0 and set the **Netmask** to be 255.255.255.0. Click **OK**.

CONFIGURATION > Object > Address > Add Address Rule

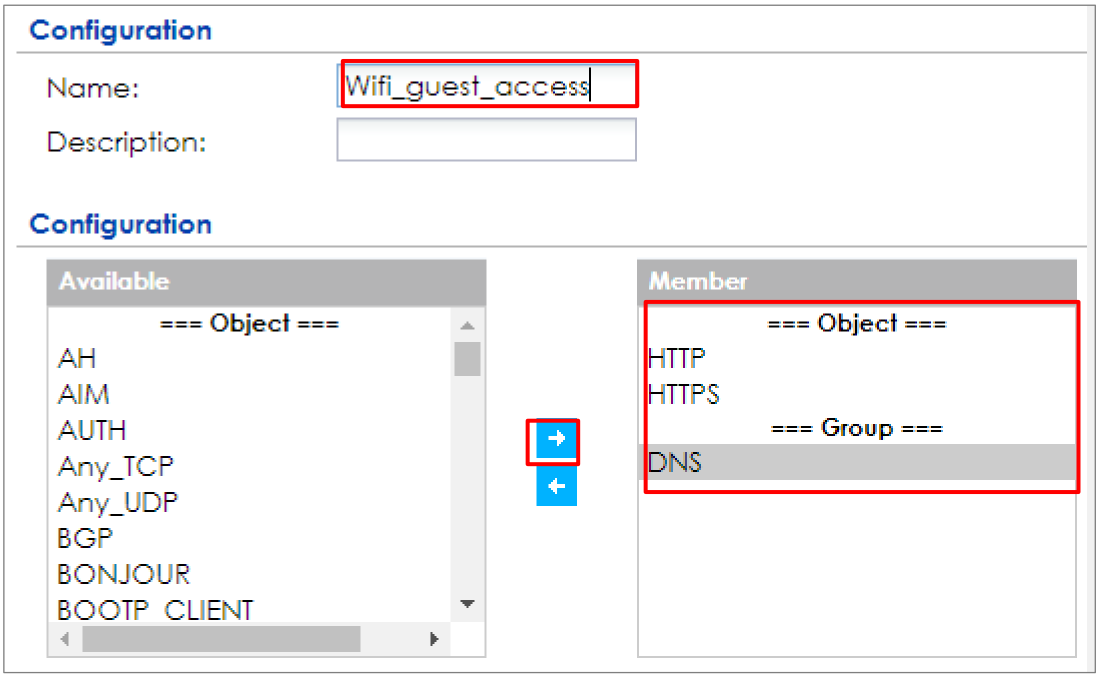


Add Address Rule

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

In the ZyWALL/USG, go to **CONFIGURATION > Object > Service > Service Group > Add Service Group Rule** to create the allowed protocols for guest Wi-Fi user. Configure the **Name** for you to identify the **Service Group**. Set **HTTP**, **HTTPS** and **DNS** to be in the same member group and click **OK**.

CONFIGURATION > Object > Service > Service Group > Add Service Group Rule



Configuration

Name: Wifi_guest_access

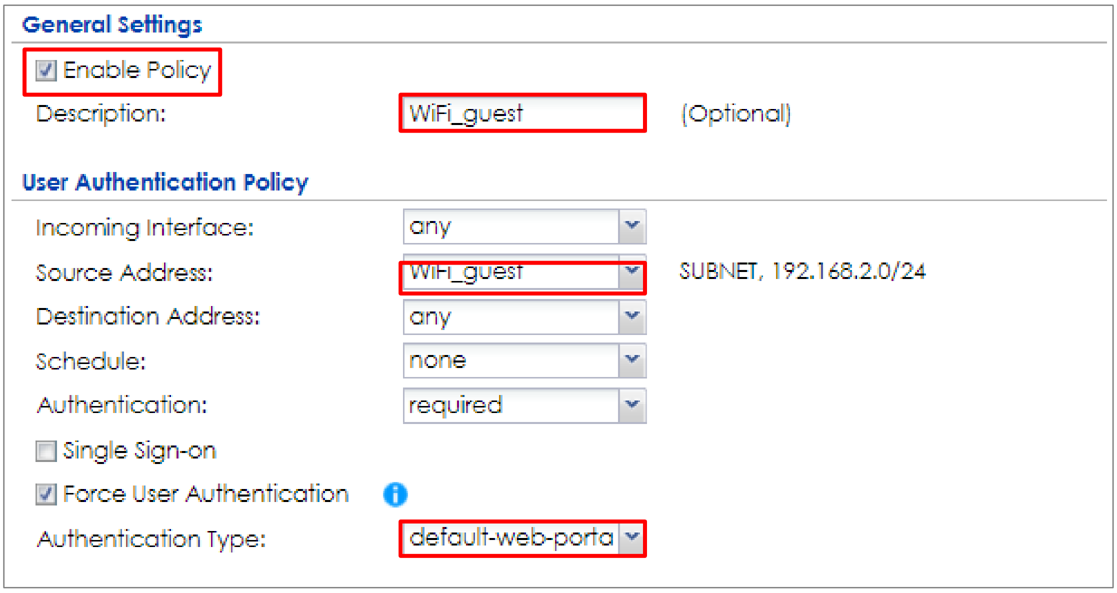
Description:

Configuration

Set Up the Web Authentication on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Web Authentication > Web Authentication Policy Summary > Auth. Policy Add** to configure policy to redirect HTTP traffic to the user login screen. Configure the **Description** (**Optional**) for you to identify the auth. Policy. Then, scroll down the **Source Address** list to choose the newly created **wifi-guest**. Set the **Authentication** to be **required**. Select **Force User Authentication**.

CONFIGURATION > Web Authentication > Web Authentication Policy Summary > Auth. Policy Add



General Settings

☑ Enable Policy

Description:	WiFi_guest	(Optional)

User Authentication Policy

Incoming Interface:	any	
Source Address:	WiFi_guest	SUBNET, 192.168.2.0/24
Destination Address:	any	
Schedule:	none	
Authentication:	required	

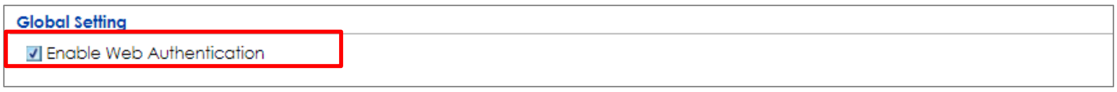
□ Single Sign-on

☑ Force User Authentication

Authentication Type:	default-web-porta

In the ZyWALL/USG, go to **CONFIGURATION > Web Authentication > General Settings** and select **Enable Web Authentication.**

CONFIGURATION > Web Authentication > General Settings



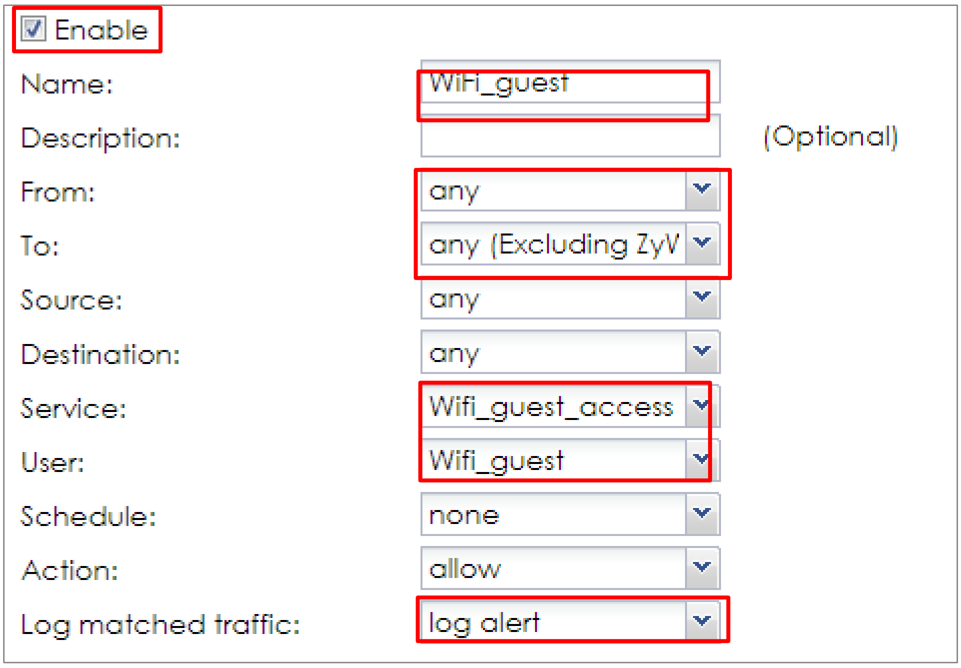
Global Setting

☑ Enable Web Authentication

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy > Add corresponding**. Configure a **Name** for you to identify the **Security Policy** profile. Set **From: LAN** and **To: any (Excluding ZyWALL)**. Set **Service** to be the Service Group Rule (wifi_guest_access in this example). Set **User** to be the Wi-Fi guest user (wifi_guest_access in this example).   Select Log type to **log alert** in order to view the result later.

CONFIGURATION > Security Policy > Policy > Add corresponding

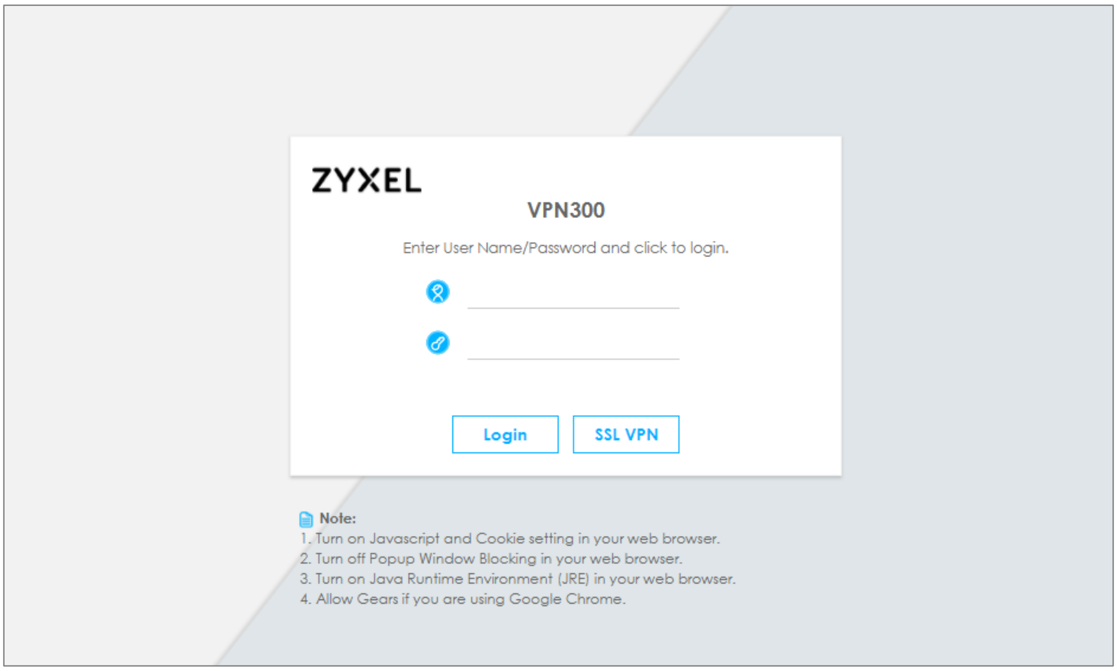


☑ Enable

Name:	WiFi_guest	
Description:		(Optional)
From:	any	
To:	any (Excluding ZyW	
Source:	any	
Destination:	any	
Service:	Wifi_guest_access	
User:	Wifi_guest	
Schedule:	none	
Action:	allow	
Log matched traffic:	log alert	

Test the Result

Using a mobile device to connect to the AP which is connected to the ZyWALL/USG. When you try to access the Internet, it will redirect to the user login screen.



ZYXEL

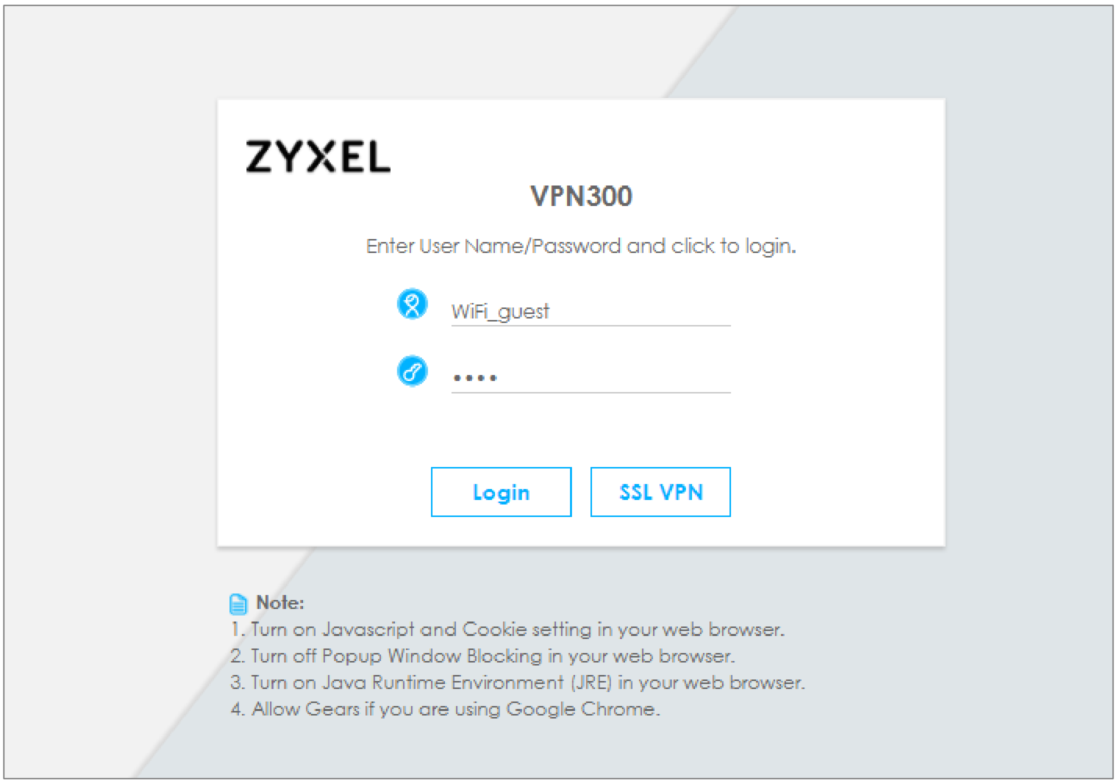
VPN300

Enter User Name/Password and click to login.

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.

Type the Wi-Fi guest **User Name** and **Password**, click **Login**.



ZYXEL

VPN300

Enter User Name/Password and click to login.

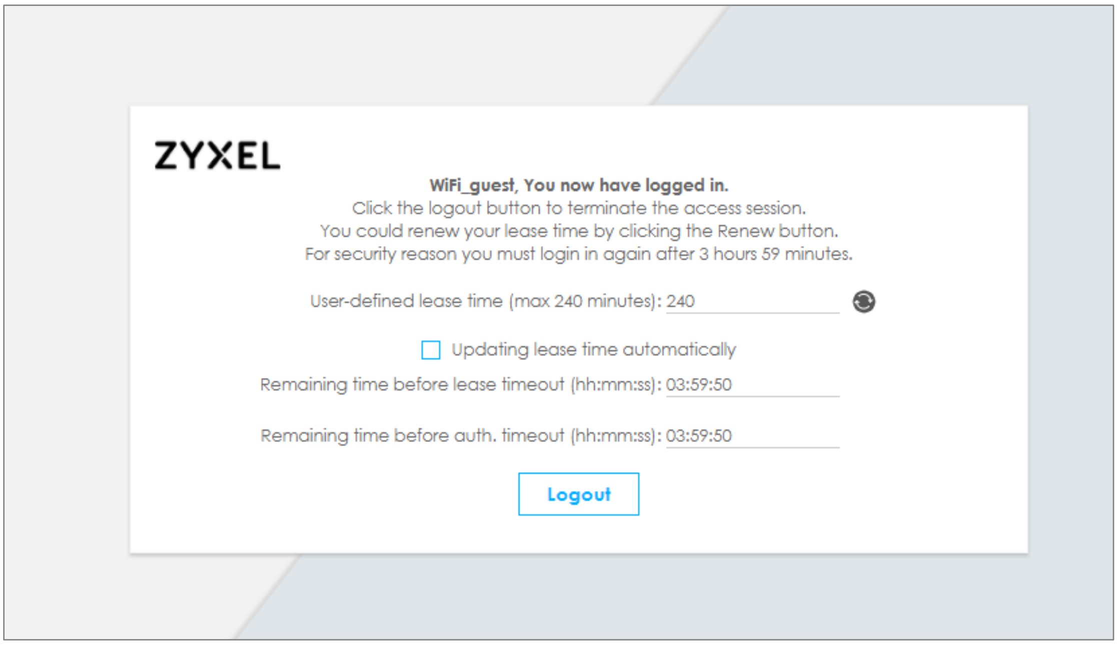
WiFi_guest

••••

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.

The access session page will appear.



WiFi_guest, You now have logged in.
Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after 3 hours 59 minutes.

User-defined lease time (max 240 minutes): 240

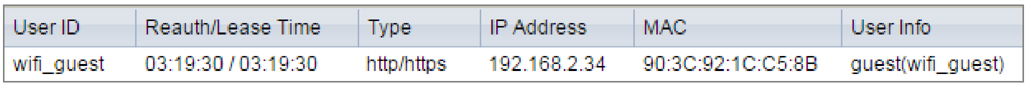
☐ Updating lease time automatically

Remaining time before lease timeout (hh:mm:ss): 03:59:50

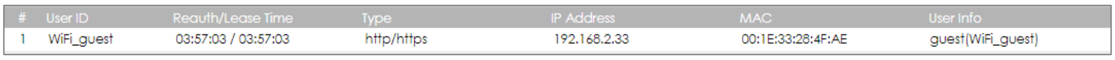
Remaining time before auth. timeout (hh:mm:ss): 03:59:50

Go to the ZyWALL/USG **Monitor > System Status > Login Users**, you will see current login user list shown as below.

Monitor > System Status > Login Users

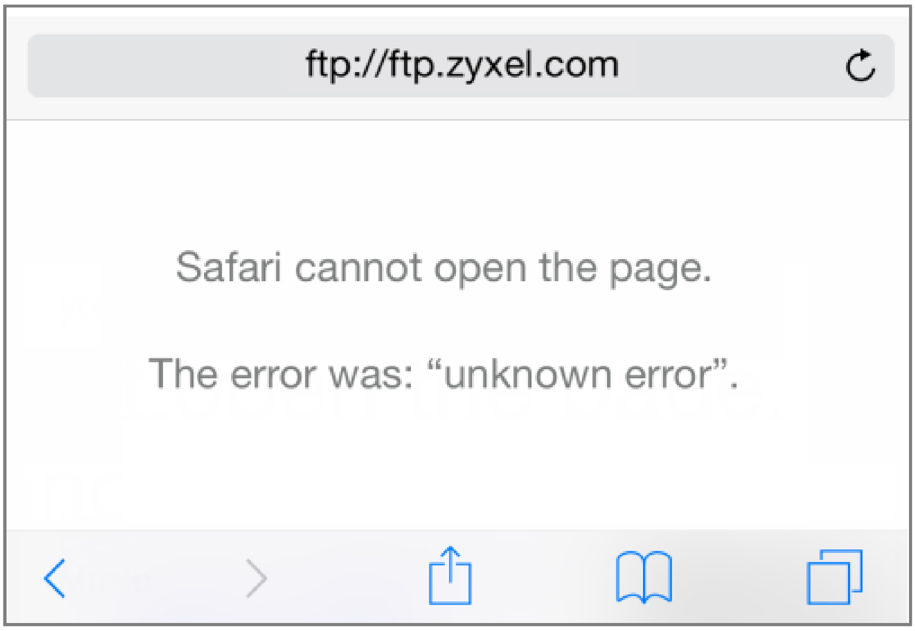


User ID	Reauth/Lease Time	Type	IP Address	MAC	User Info
wifi_guest	03:19:30 / 03:19:30	http/https	192.168.2.34	90:3C:92:1C:C5:8B	guest(wifi_guest)



#	User ID	Reauth/Lease Time	Type	IP Address	MAC	User Info
1	WiFi_guest	03:57:03 / 03:57:03	http/https	192.168.2.33	00:1E:33:28:4F:AE	guest(WiFi_guest)

Attempt to access FTP server (prohibited service in this example) and it gets an error message.



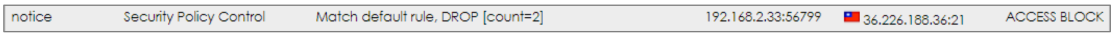
ftp://ftp.zyxel.com

Safari cannot open the page.

The error was: “unknown error”.

Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] log message shown as below. The access to FTP service port 21 is blocked in this example.

Monitor > Log

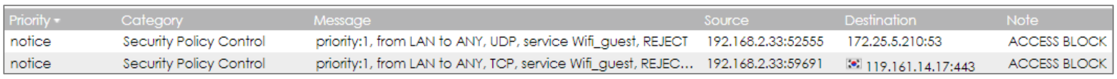


notice	Security Policy Control	Match default rule, DROP [count=2]	192.168.2.33:56799	36.226.188.36:21	ACCESS BLOCK

What Could Go Wrong?

If you see [notice] log shown as below, the Wi-Fi guest traffic is blocked by the **priority 1 Security Policy**. The ZyWALL/USG checks the security policy in order and applies the first security policy to the matched traffic. If the Wi-Fi guest traffic matches a policy that comes earlier in the list, it may be unexpectedly blocked. Please change your policy setting or move the Wi-Fi guest policy to the higher priority.

Monitor > Log

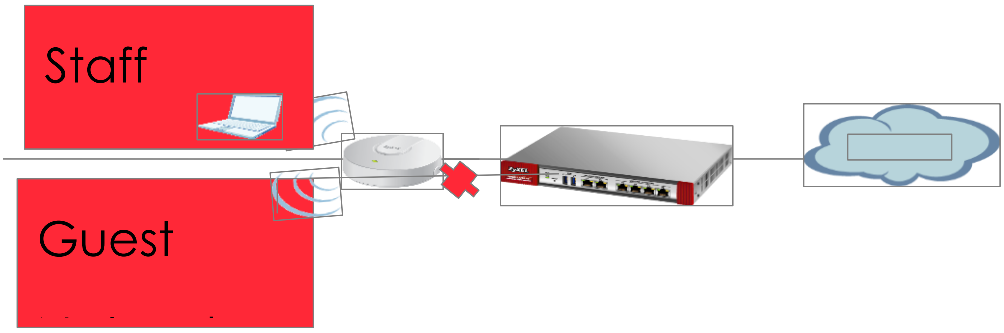


Priority ▾	Category	Message	Source	Destination	Note
notice	Security Policy Control	priority:1, from LAN to ANY, UDP, service Wifi_guest, REJECT	192.168.2.33:52555	172.25.5.210:53	ACCESS BLOCK
notice	Security Policy Control	priority:1, from LAN to ANY, TCP, service Wifi_guest, REJEC...	192.168.2.33:59691	119.161.14.17:443	ACCESS BLOCK

Note: The default setting of **Security Policy** is without log notification (except **PolicyDefault**), if you want to check which policy may potentially block the traffic, please select this policy and set the **Log matched traffic** to be **log** or **log alert**.

How to create a Wi-Fi VLAN interfaces to separate staff network and Guest network

This example shows how to create Wi-Fi VLAN interfaces to separate staff network and Guest network. Suppose there should be no limitation for the staff network, but restrict the guests not access the USG.



Separate the Staff and Guest network

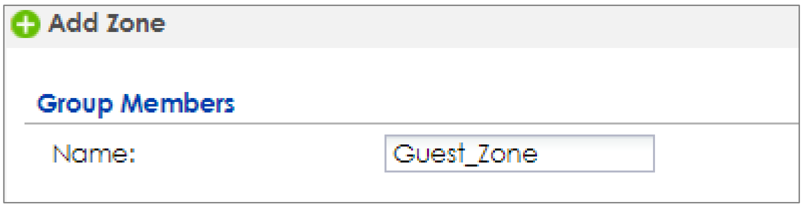
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG210 (Firmware Version: ZLD 4.25)

Set up Wi-Fi VLAN interfaces

Create VLAN interfaces

Go to **CONFIGURATION > Object > Zone**. Create a zone for the guest.

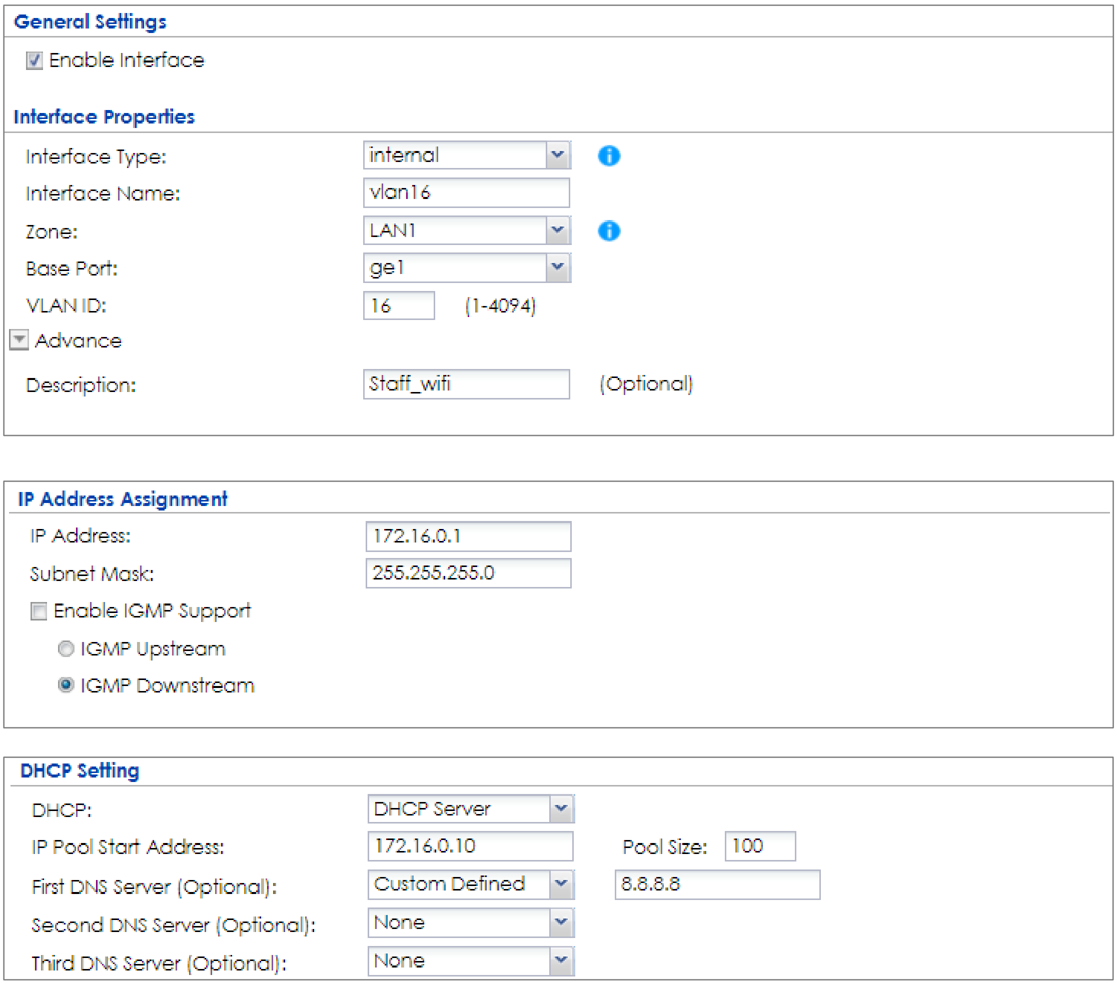
CONFIGURATION > Object > Zone



Name: Guest_Zone

Go to **CONFIGURATION > Network > Interface > VLAN.** Create VLAN16 for Staff_WiFi and VLAN17 for Guest_WiF

CONFIGURATION > Network > Interface > VLAN > VLAN16



General Settings

☑ Enable Interface

Interface Properties

Interface Type:	internal
Interface Name:	vlan16
Zone:	LAN1
Base Port:	ge1
VLAN ID:	16 (1-4094)

Advance

Description:	Staff_wifi (Optional)

IP Address Assignment

IP Address:	172.16.0.1
Subnet Mask:	255.255.255.0

□ Enable IGMP Support

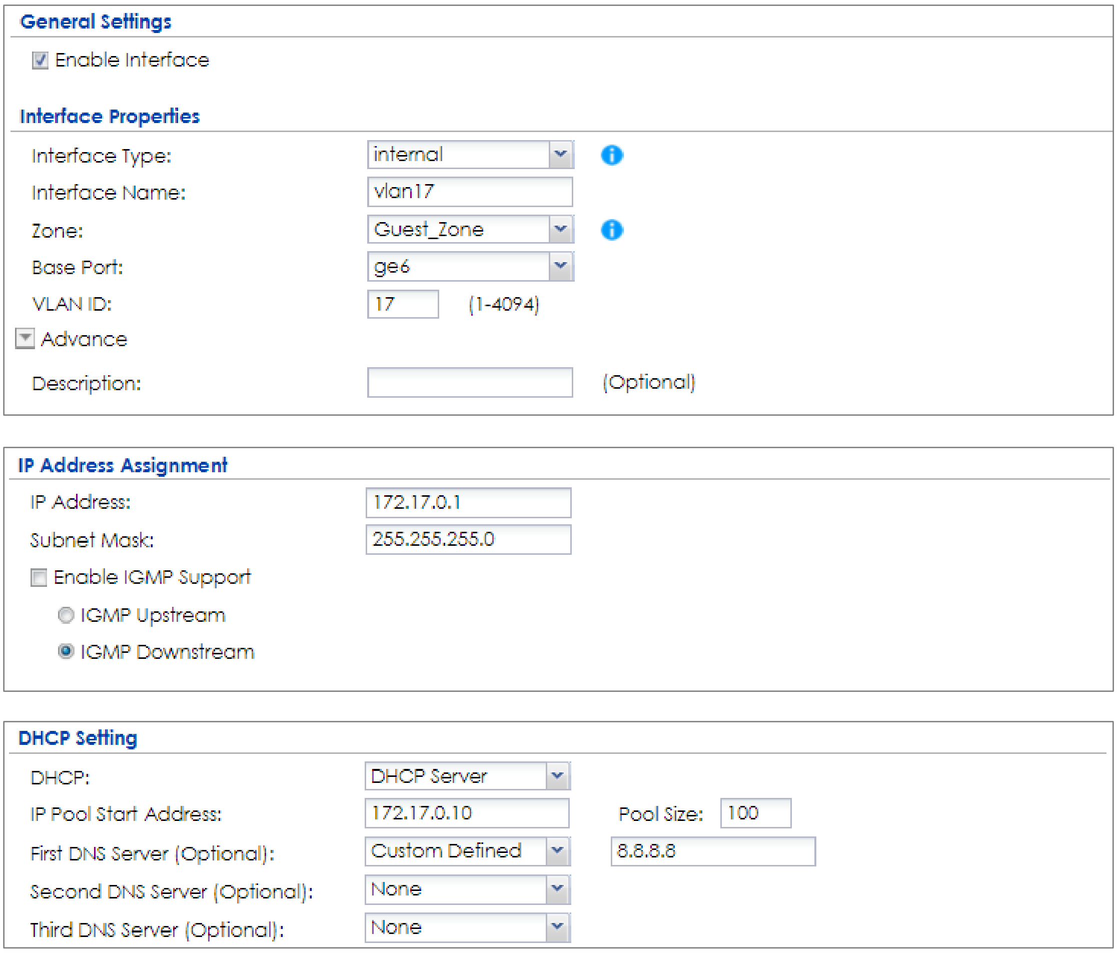
○ IGMP Upstream

● IGMP Downstream

DHCP Setting

DHCP:	DHCP Server		
IP Pool Start Address:	172.16.0.10	Pool Size:	100
First DNS Server (Optional):	Custom Defined	8.8.8.8	
Second DNS Server (Optional):	None		
Third DNS Server (Optional):	None		

CONFIGURATION > Network > Interface > VLAN > VLAN17



General Settings

☑ Enable Interface

Interface Properties

Interface Type:	internal
Interface Name:	vlan17
Zone:	Guest_Zone
Base Port:	ge6
VLAN ID:	17 (1-4094)

Advance

Description:	(Optional)

IP Address Assignment

IP Address:	172.17.0.1
Subnet Mask:	255.255.255.0

□ Enable IGMP Support

○ IGMP Upstream

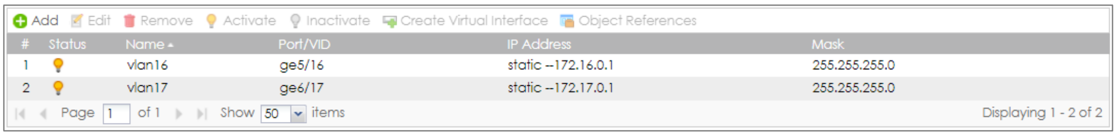
● IGMP Downstream

DHCP Setting

DHCP:	DHCP Server		
IP Pool Start Address:	172.17.0.10	Pool Size:	100
First DNS Server (Optional):	Custom Defined	8.8.8.8	
Second DNS Server (Optional):	None		
Third DNS Server (Optional):	None		

There will be two VLAN interfaces.

CONFIGURATION > Network > Interface > VLAN



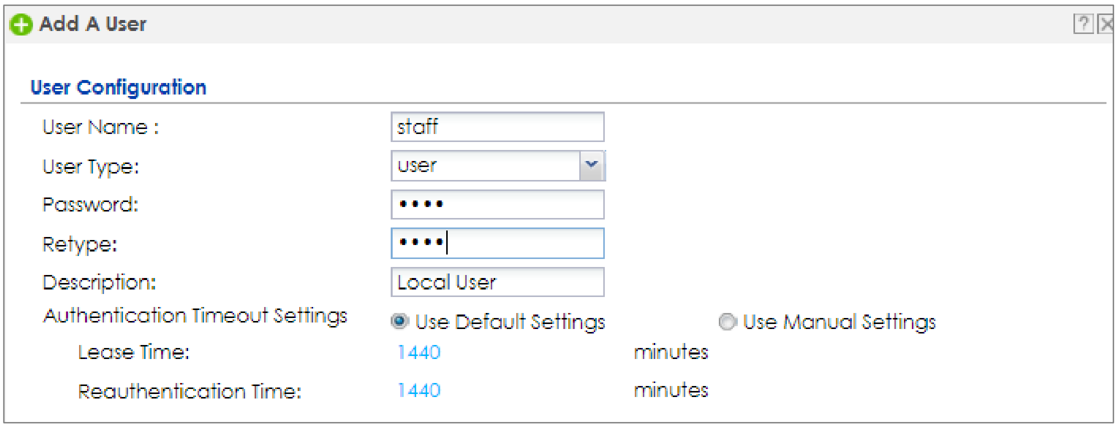
#	Status	Name	Port/VID	IP Address	Mask
1	💡	vlan16	ge5/16	static --172.16.0.1	255.255.255.0
2	💡	vlan17	ge6/17	static --172.17.0.1	255.255.255.0

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

Set Up the User

Go to **Configuration > Object > User/Group > User**, and create users for the staff and the guest

Configuration > Object > User/Group > User > staff

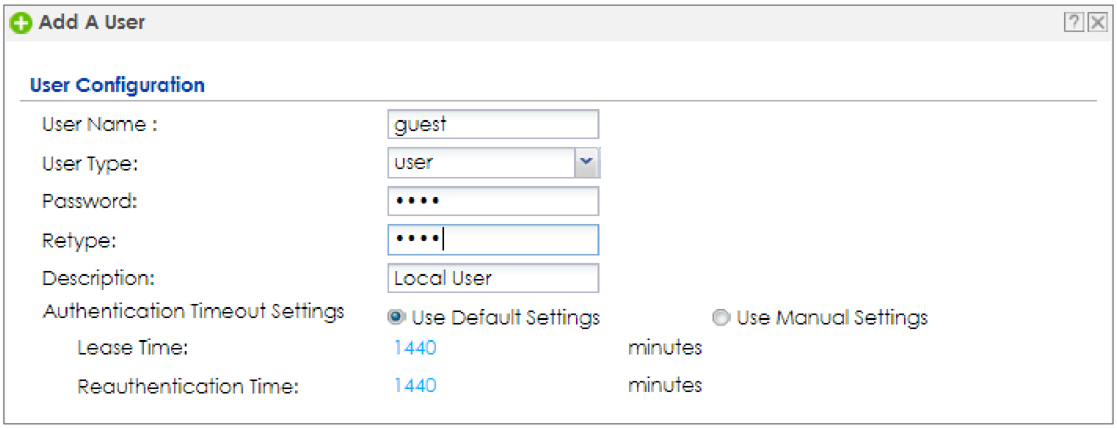


Add A User

User Configuration

User Name :	staff
User Type:	user
Password:	••••
Retype:	••••
Description:	Local User
Authentication Timeout Settings	● Use Default Settings ○ Use Manual Settings
Lease Time:	1440 minutes
Reauthentication Time:	1440 minutes

Configuration > Object > User/Group > User > guest

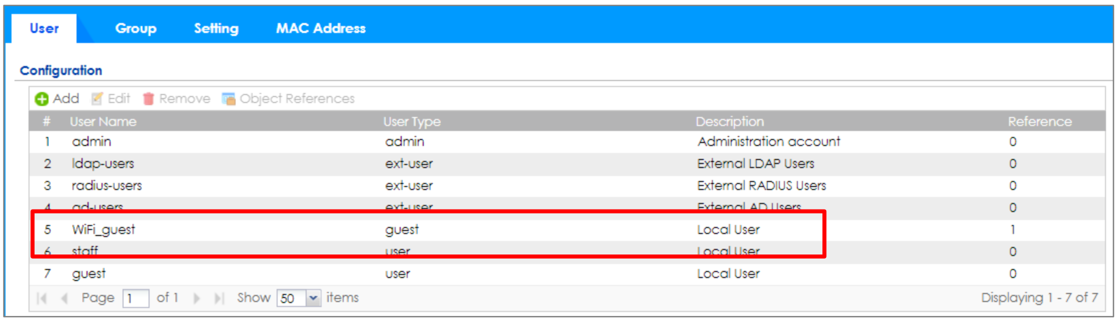


Add A User

User Configuration

User Name :	guest
User Type:	user
Password:	••••
Retype:	••••
Description:	Local User
Authentication Timeout Settings	● Use Default Settings ○ Use Manual Settings
Lease Time:	1440 minutes
Reauthentication Time:	1440 minutes

There will be two users.



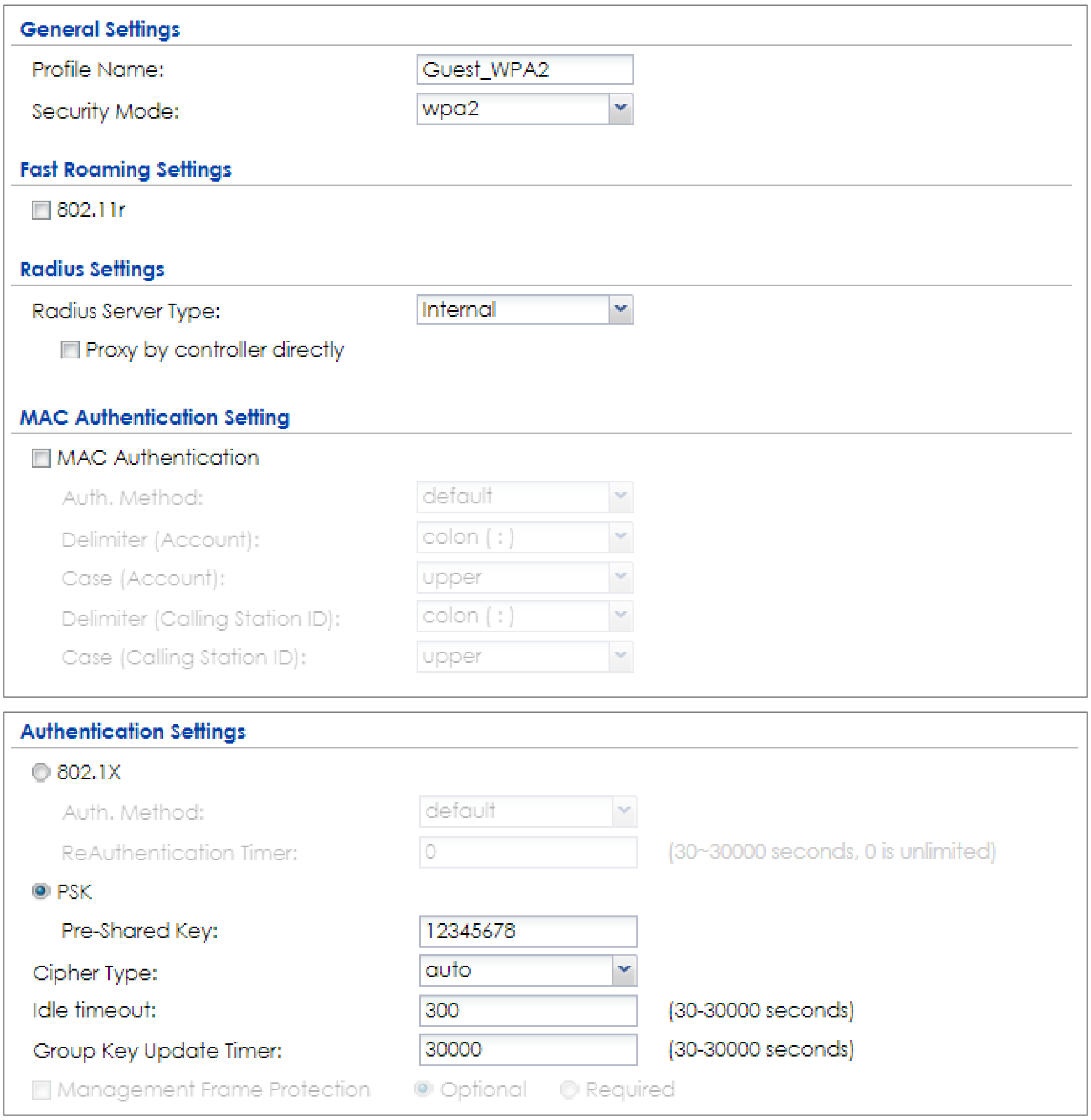
#	User Name	User Type	Description	Reference
1	admin	admin	Administration account	0
2	ldap-users	ext-user	External LDAP Users	0
3	radius-users	ext-user	External RADIUS Users	0
4	ad-users	ext-user	External AD Users	0
5	WiFi_guest	guest	Local User	1
6	staff	user	Local User	0
7	guest	user	Local User	0

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

Set Up the AP Profile

Go to **CONFIGURATION > Object > AP Profile > SSID > Security List,** and create two security profiles.

CONFIGURATION > Object > AP Profile > SSID > Security List > Guest_WPA2



General Settings

Profile Name:	Guest_WPA2
Security Mode:	wpa2

Fast Roaming Settings

□ 802.11r

Radius Settings

Radius Server Type: Internal

□ Proxy by controller directly

MAC Authentication Setting

□ MAC Authentication

Auth. Method:	default
Delimiter (Account):	colon (:)
Case (Account):	upper
Delimiter (Calling Station ID):	colon (:)
Case (Calling Station ID):	upper

Authentication Settings

○ 802.1X

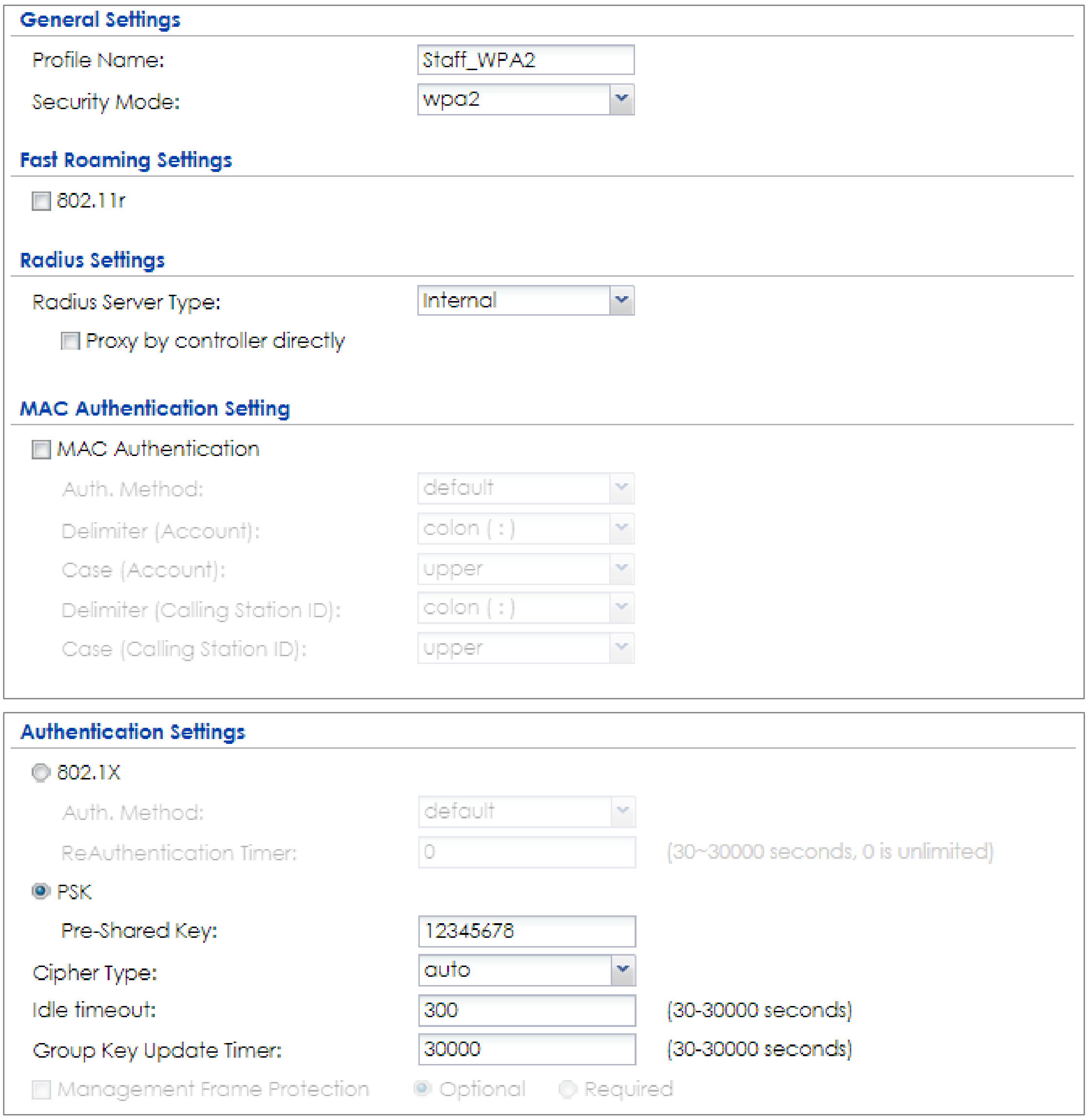
Auth. Method:	default	
ReAuthentication Timer:	0	(30~30000 seconds, 0 is unlimited)

● PSK

Pre-Shared Key:	12345678	
Cipher Type:	auto	
Idle timeout:	300	(30-30000 seconds)
Group Key Update Timer:	30000	(30-30000 seconds)

□ Management Frame Protection ● Optional ○ Required

CONFIGURATION > Object > AP Profile > SSID > Security List > Staff_WPA2



General Settings

Profile Name: Staff_WPA2

Security Mode: wpa2

Fast Roaming Settings

□ 802.11r

Radius Settings

Radius Server Type: Internal

□ Proxy by controller directly

MAC Authentication Setting

□ MAC Authentication

Auth. Method: default

Delimiter (Account): colon (:)

Case (Account): upper

Delimiter (Calling Station ID): colon (:)

Case (Calling Station ID): upper

Authentication Settings

○ 802.1X

Auth. Method: default

ReAuthentication Timer: 0 (30~30000 seconds, 0 is unlimited)

● PSK

Pre-Shared Key: 12345678

Cipher Type: auto

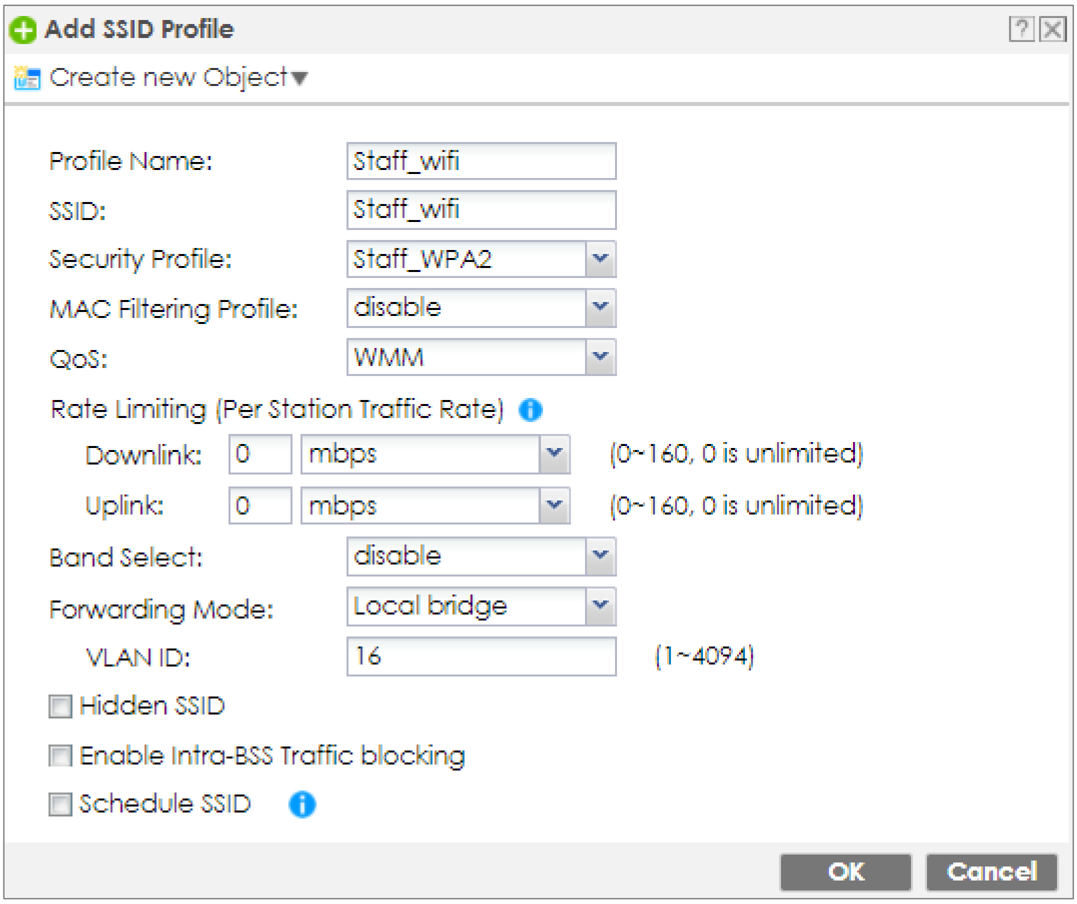
Idle timeout: 300 (30-30000 seconds)

Group Key Update Timer: 30000 (30-30000 seconds)

□ Management Frame Protection ● Optional ○ Required

Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List,** and create two SSID profiles.

CONFIGURATION > Object > AP Profile > SSID > SSID List > Staff_Wifi



Profile Name: Staff_wifi

SSID: Staff_wifi

Security Profile: Staff_WPA2

MAC Filtering Profile: disable

QoS: WMM

Rate Limiting (Per Station Traffic Rate)

Downlink: 0 mbps (0~160, 0 is unlimited)

Uplink: 0 mbps (0~160, 0 is unlimited)

Band Select: disable

Forwarding Mode: Local bridge

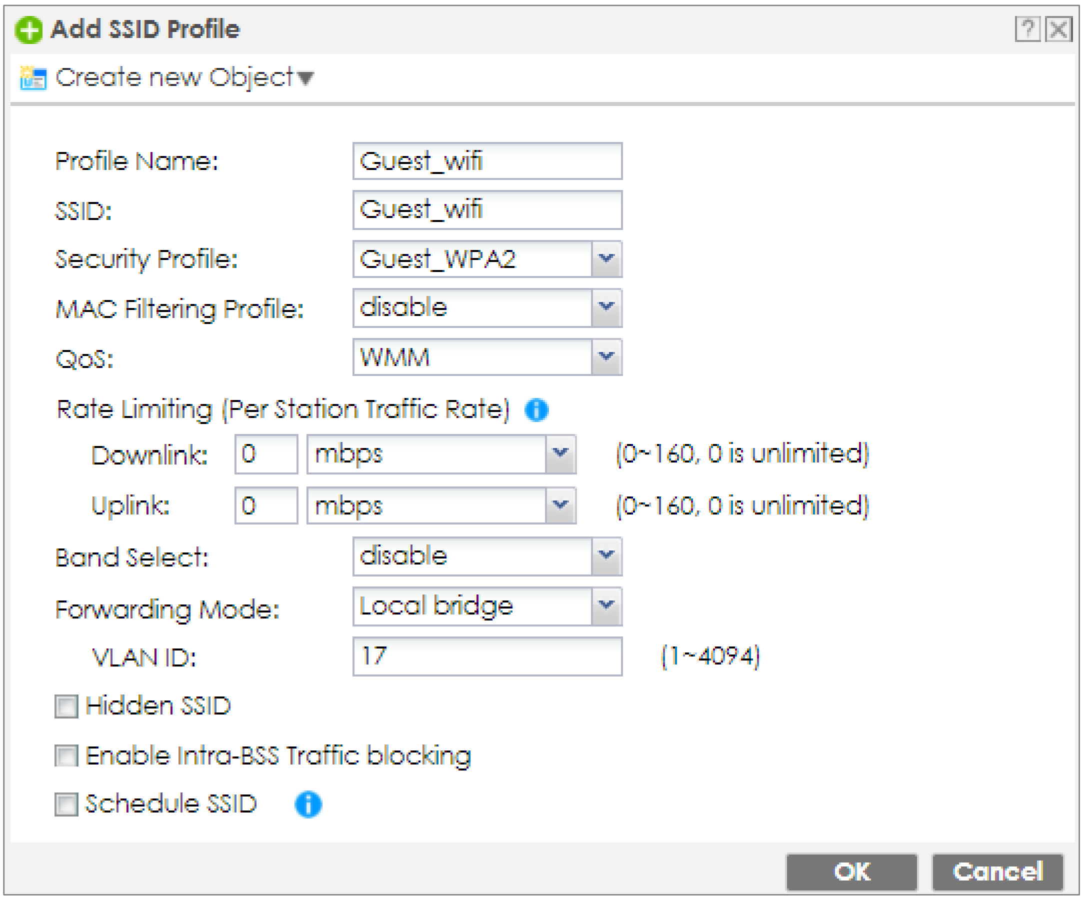
VLAN ID: 16 (1~4094)

□ Hidden SSID

□ Enable Intra-BSS Traffic blocking

□ Schedule SSID

CONFIGURATION > Object > AP Profile > SSID > SSID List > Guest_Wifi



Profile Name:	Guest_wifi	
SSID:	Guest_wifi	
Security Profile:	Guest_WPA2	
MAC Filtering Profile:	disable	
QoS:	WMM	
Rate Limiting (Per Station Traffic Rate)		
Downlink:	0 mbps	(0~160, 0 is unlimited)
Uplink:	0 mbps	(0~160, 0 is unlimited)
Band Select:	disable	
Forwarding Mode:	Local bridge	
VLAN ID:	17	(1~4094)

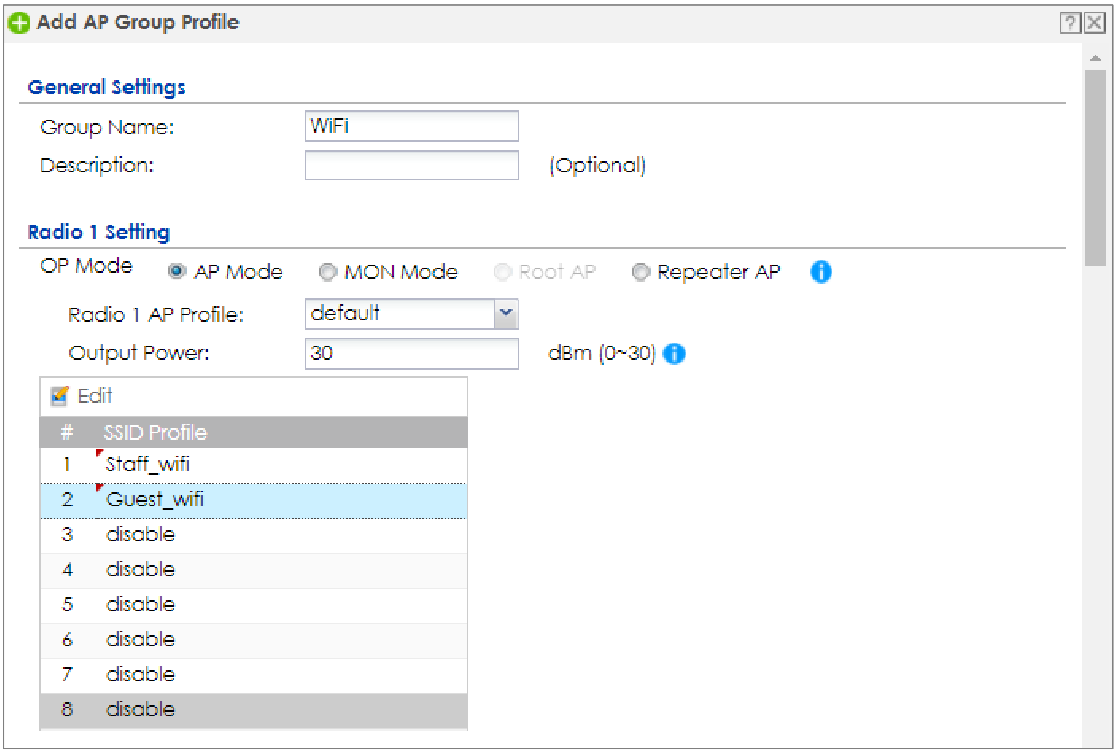
□ Hidden SSID

□ Enable Intra-BSS Traffic blocking

□ Schedule SSID

Go to **CONFIGURATION > Wireless > AP Management > AP Group**, and add an AP Group as **WiFi**.

CONFIGURATION > Wireless > AP Management > AP Group



Add AP Group Profile

General Settings

Group Name: WiFi

Description: (Optional)

Radio 1 Setting

OP Mode ● AP Mode ○ MON Mode ○ Root AP ○ Repeater AP

Radio 1 AP Profile: default

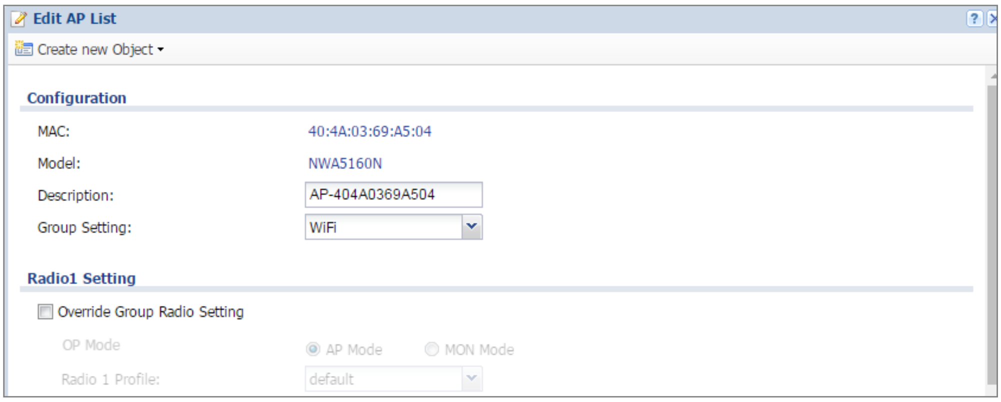
Output Power: 30 dBm (0~30)

Edit

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

Go to **CONFIGURATION > Wireless > AP Management > Mgnt. AP List**, and Edit the AP List. Change the Group setting as **WiFi**

CONFIGURATION > Wireless > AP Management > Mgnt. AP List,



Edit AP List

Create new Object ▾

Configuration

MAC: 40:4A:03:69:A5:04

Model: NWA5160N

Description: AP-404A0369A504

Group Setting: WiFi

Radio1 Setting

□ Override Group Radio Setting

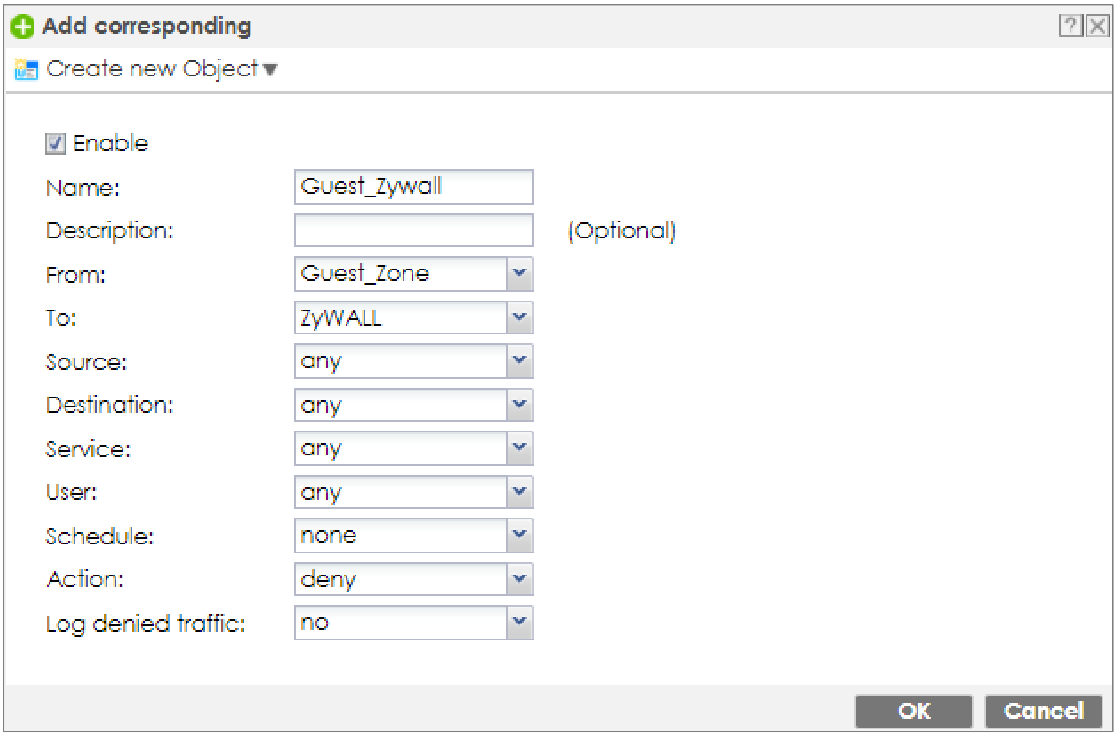
OP Mode ● AP Mode ○ MON Mode

Radio 1 Profile: default

Set Up the Security policy rule

Go to **CONFIGURATION > Security Policy > Policy Control > Policy**. Add one rule to restrict Guest access USG, and another one to allow to access internet.

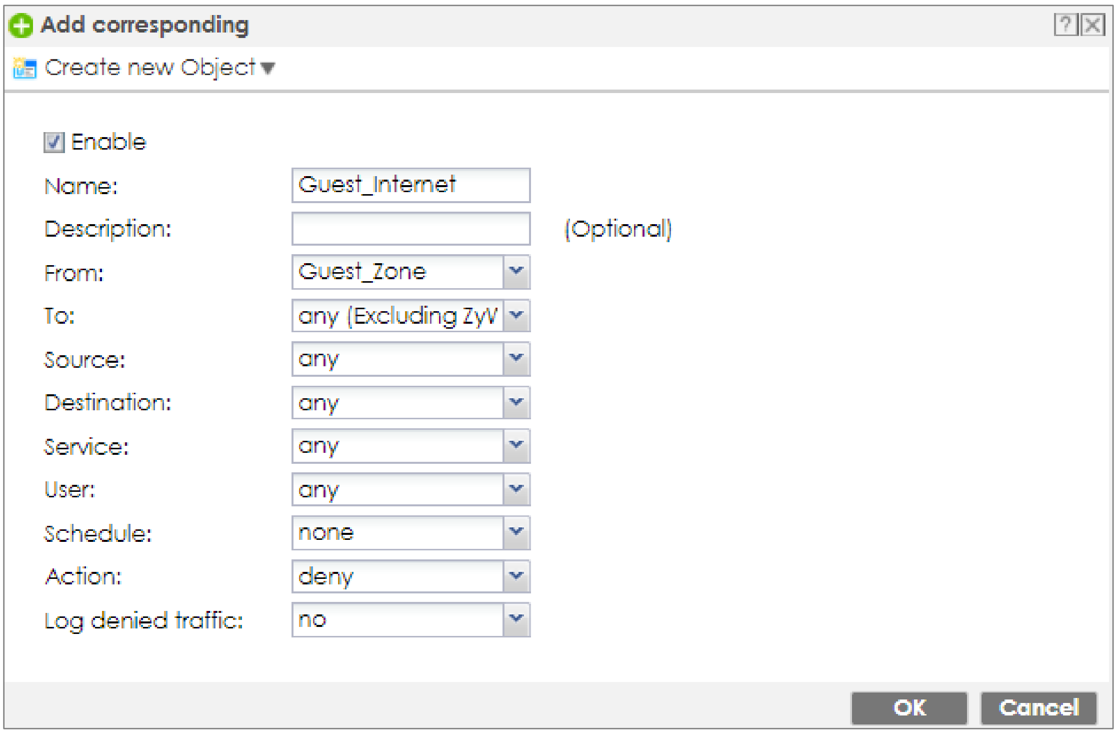
CONFIGURATION > Security Policy > Policy Control > Policy > Guest_ZyWALL



☑ Enable

Name:	Guest_Zywall	
Description:		(Optional)
From:	Guest_Zone	
To:	ZyWALL	
Source:	any	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	deny	
Log denied traffic:	no	

CONFIGURATION > Security Policy > Policy Control > Policy > Guest_Internet

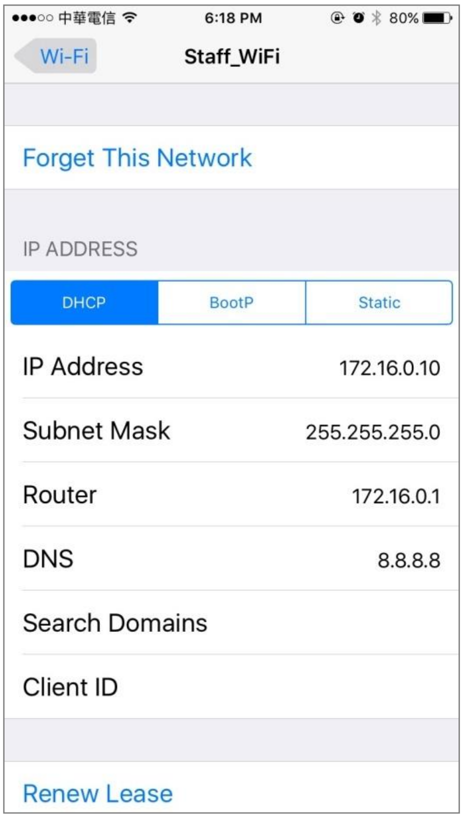


☑ Enable

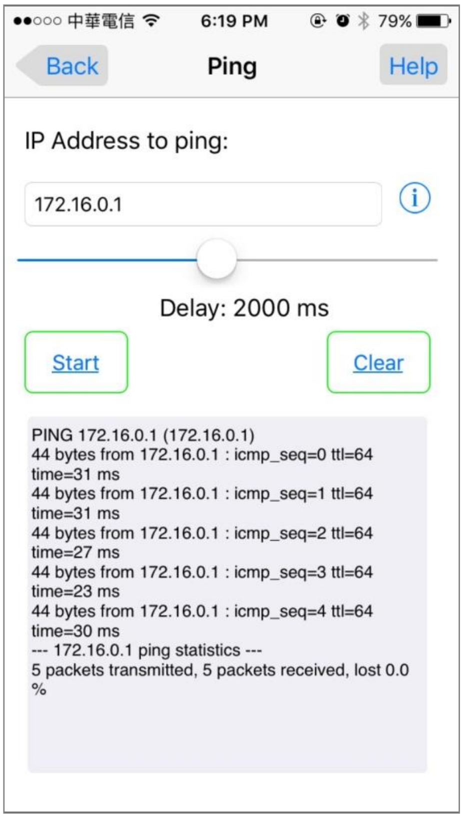
Name:	Guest_Internet
Description:	(Optional)
From:	Guest_Zone
To:	any (Excluding ZyW
Source:	any
Destination:	any
Service:	any
User:	any
Schedule:	none
Action:	deny
Log denied traffic:	no

Test result

Connect to the SSID Staff_WiFi, and ping the USG interface.



IP Address	172.16.0.10
Subnet Mask	255.255.255.0
Router	172.16.0.1
DNS	8.8.8.8
Search Domains	
Client ID	

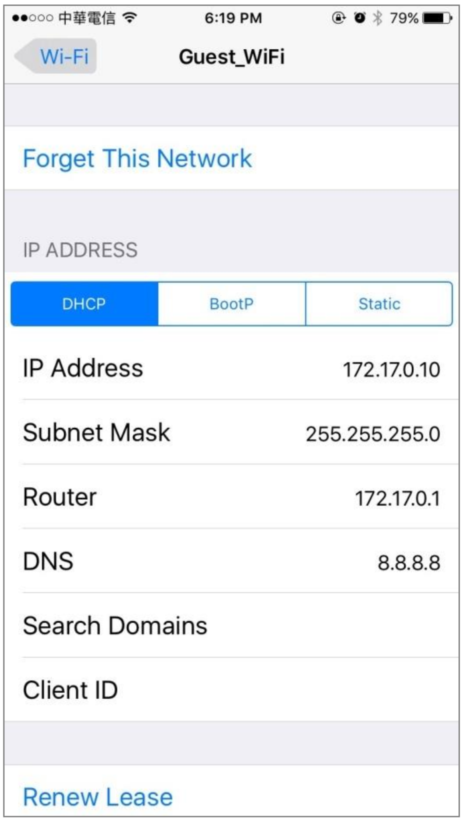


IP Address to ping: 172.16.0.1

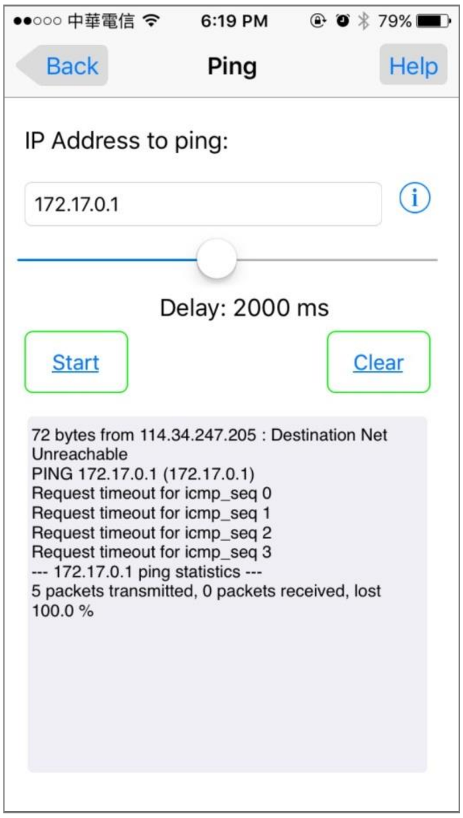
Delay: 2000 ms

```
PING 172.16.0.1 (172.16.0.1)
44 bytes from 172.16.0.1 : icmp_seq=0 ttl=64
time=31 ms
44 bytes from 172.16.0.1 : icmp_seq=1 ttl=64
time=31 ms
44 bytes from 172.16.0.1 : icmp_seq=2 ttl=64
time=27 ms
44 bytes from 172.16.0.1 : icmp_seq=3 ttl=64
time=23 ms
44 bytes from 172.16.0.1 : icmp_seq=4 ttl=64
time=30 ms
--- 172.16.0.1 ping statistics ---
5 packets transmitted, 5 packets received, lost 0.0
%
```

Connect to the SSID Guest_WiFi, and ping the USG interface



IP Address	172.17.0.10
Subnet Mask	255.255.255.0
Router	172.17.0.1
DNS	8.8.8.8
Search Domains	
Client ID	



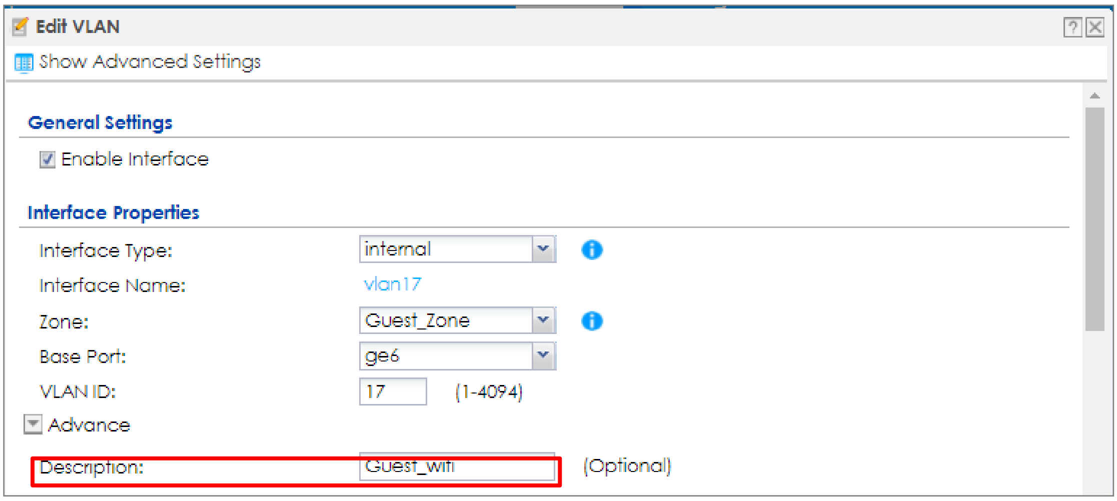
IP Address to ping: 172.17.0.1

Delay: 2000 ms

```
72 bytes from 114.34.247.205 : Destination Net
Unreachable
PING 172.17.0.1 (172.17.0.1)
Request timeout for icmp_seq 0
Request timeout for icmp_seq 1
Request timeout for icmp_seq 2
Request timeout for icmp_seq 3
--- 172.17.0.1 ping statistics ---
5 packets transmitted, 0 packets received, lost
100.0 %
```

What could go wrong

Choose the wrong zone for the Guest VLAN interface.



General Settings

☑ Enable Interface

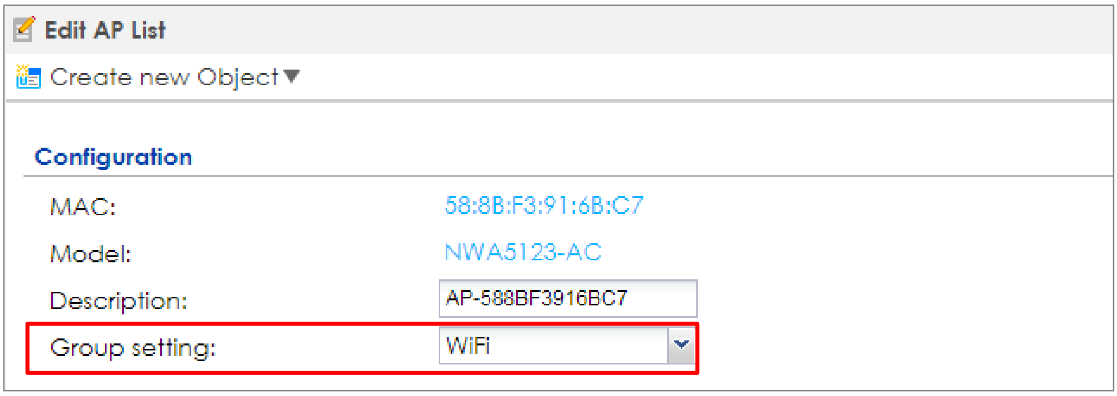
Interface Properties

Interface Type:	internal
Interface Name:	vlan17
Zone:	Guest_Zone
Base Port:	ge6
VLAN ID:	17 (1-4094)

Advance

Description: Guest_wifi (Optional)

Not change the AP to the correct group

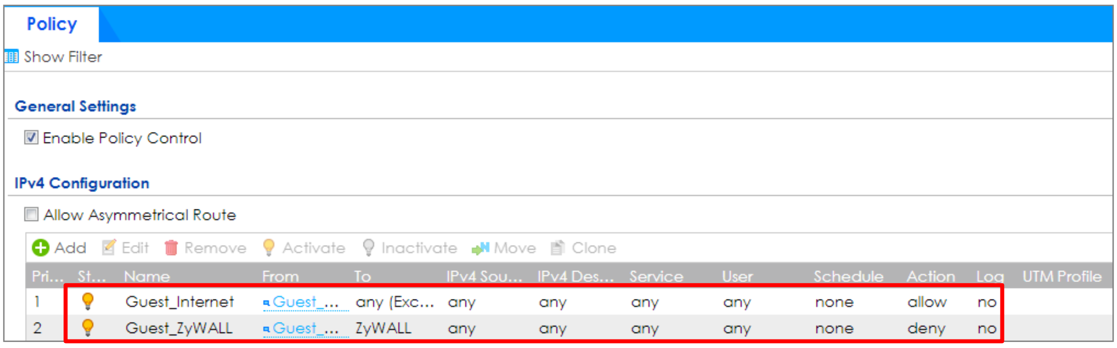


Edit AP List

Create new Object▼

Configuration

MAC:	58:8B:F3:91:6B:C7
Model:	NWA5123-AC
Description:	AP-588BF3916BC7
Group setting:	WiFi



General Settings

☑ Enable Policy Control

IPv4 Configuration

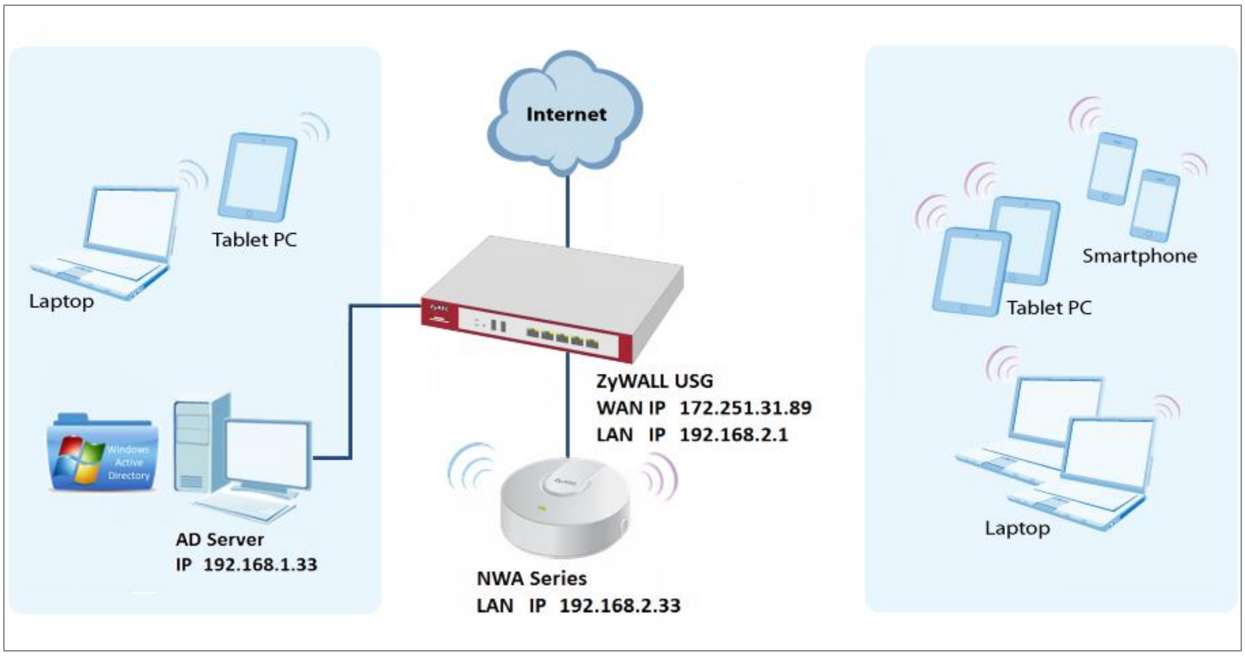
□ Allow Asymmetrical Route

Pri…	St…	Name	From	To	IPv4 Sou…	IPv4 Des…	Service	User	Schedule	Action	Log	UTM Profile
1		Guest_Internet	Guest_…	any (Exc…	any	any	any	any	none	allow	no	
2		Guest_ZyWALL	Guest_…	ZyWALL	any	any	any	any	none	deny	no	

How to Set Up WiFi Networks with Microsoft Active Directory Authentication

This is an example of using ZyWALL/USG to configure guest WiFi accounts with Microsoft Active Directory (AD) to authenticate your WiFi guests. For the wireless network setup, please go to How to Set Up WiFi with ZyXEL AP.

ZyWALL/USG with AD Guest WiFi Accounts Example

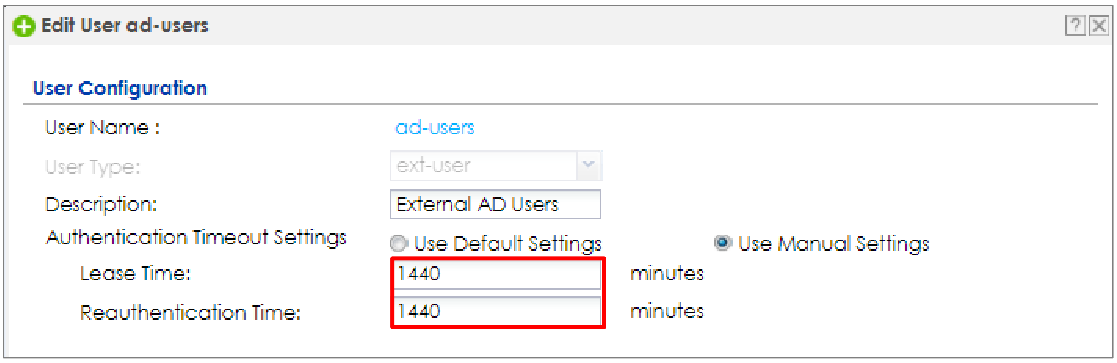


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Wi-Fi Guest Account and Authentication Method on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > User/Group > User > ad-users**, set the **Authentication Timeout Settings** to **Use Manual Settings** and enter the number of minutes this user has to renew the current session before the user is logged out.

CONFIGURATION > Object > User/Group > User > ad-users



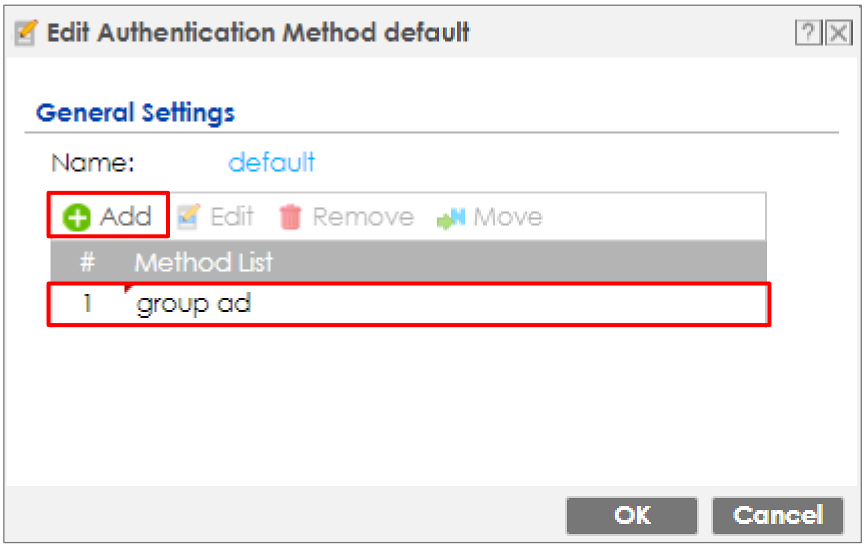
Edit User ad-users

User Configuration

User Name :	ad-users
User Type:	ext-user
Description:	External AD Users
Authentication Timeout Settings	○ Use Default Settings ● Use Manual Settings
Lease Time:	1440 minutes
Reauthentication Time:	1440 minutes

In the ZyWALL/USG, go to **CONFIGURATION > Object > Authentication Method > default > Edit Authentication Method default**, click **Add** to insert group ad in the table. Click **OK**.

CONFIGURATION > Object > User/Group > User > ad-users



Edit Authentication Method default

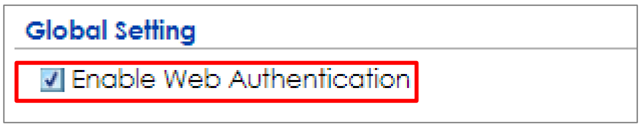
General Settings

Name: default

#	Method List
1	group ad

In the ZyWALL/USG, go to **CONFIGURATION > Web Authentication > General Settings** and select **Enable Web Authentication**.

CONFIGURATION > Web Authentication > General Settings



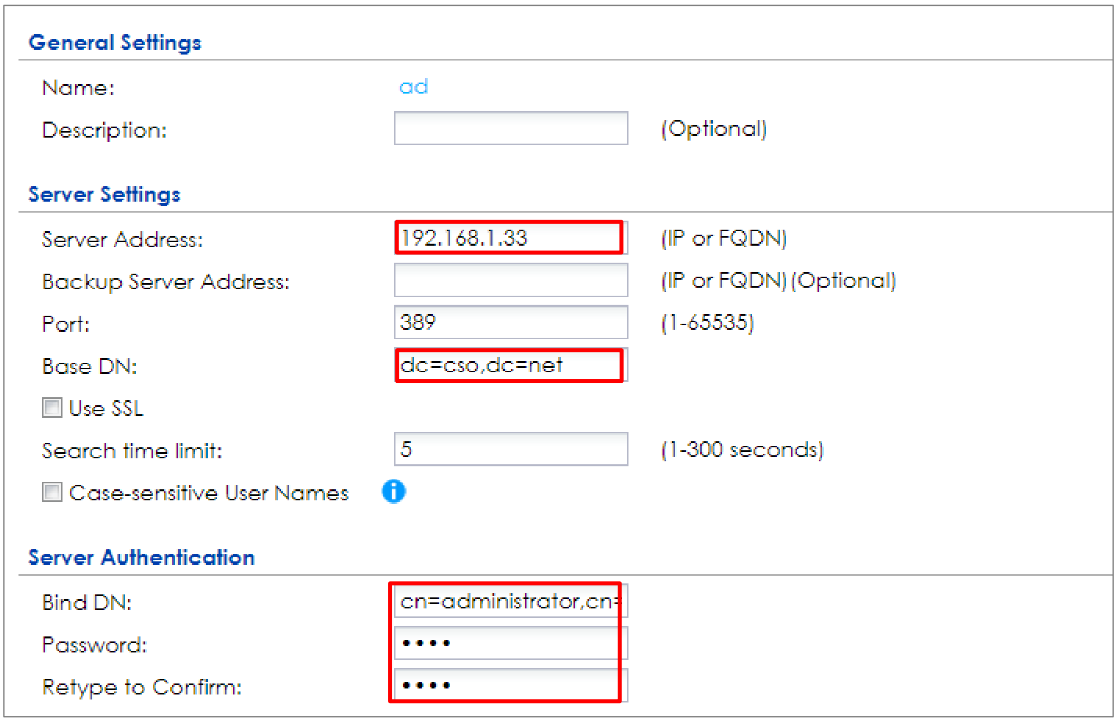
Global Setting

☑ Enable Web Authentication

Set Up the Active Directory Server Account on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > AAA Server > Active Directory > Add Active Directory** to configure the AD sever. Enter the **Server Address** (192.168.1.33 in this example) and **Based DN** (dc=cso,dc=net in this example). Specify the **Bind DN** for logging into the AD server (cn=Administrator,cn=users,dc=cso,dc=net in this example). If required, enter the **Password** for the ZyWALL/USG to bind (or log in) to the AD server.

CONFIGURATION > Object > AAA Server > Active Directory > Add Active Directory



General Settings

Name:	ad	
Description:		(Optional)

Server Settings

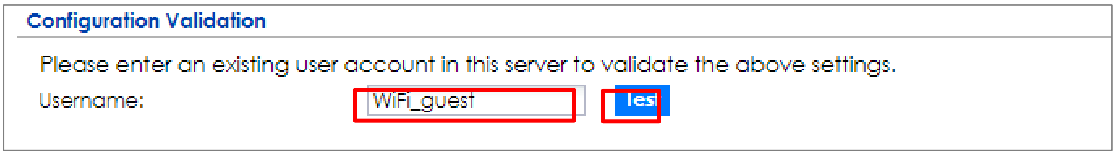
Server Address:	192.168.1.33	(IP or FQDN)
Backup Server Address:		(IP or FQDN) (Optional)
Port:	389	(1-65535)
Base DN:	dc=cso,dc=net	
□ Use SSL		
Search time limit:	5	(1-300 seconds)
□ Case-sensitive User Names		

Server Authentication

Bind DN:	cn=administrator,cn=
Password:	••••
Retype to Confirm:	••••

Scroll down to the **Configuration Validation** section, use a user account from the server specified above to test if the configuration is correct. Enter the account's user name (wifi_guest in this example) in the **Username** field and click **Test**. A popup screen will appear allowing you to view the test result. Click **OK** to save the configuration.

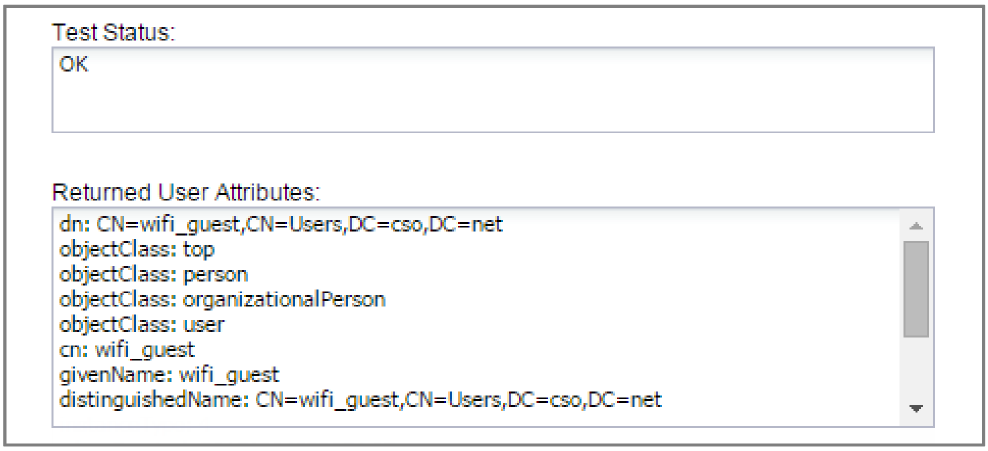
CONFIGURATION > Object > AAA Server > Active Directory > Add Active Directory



Configuration Validation

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

Username: WiFi_guest



Test Status:

OK

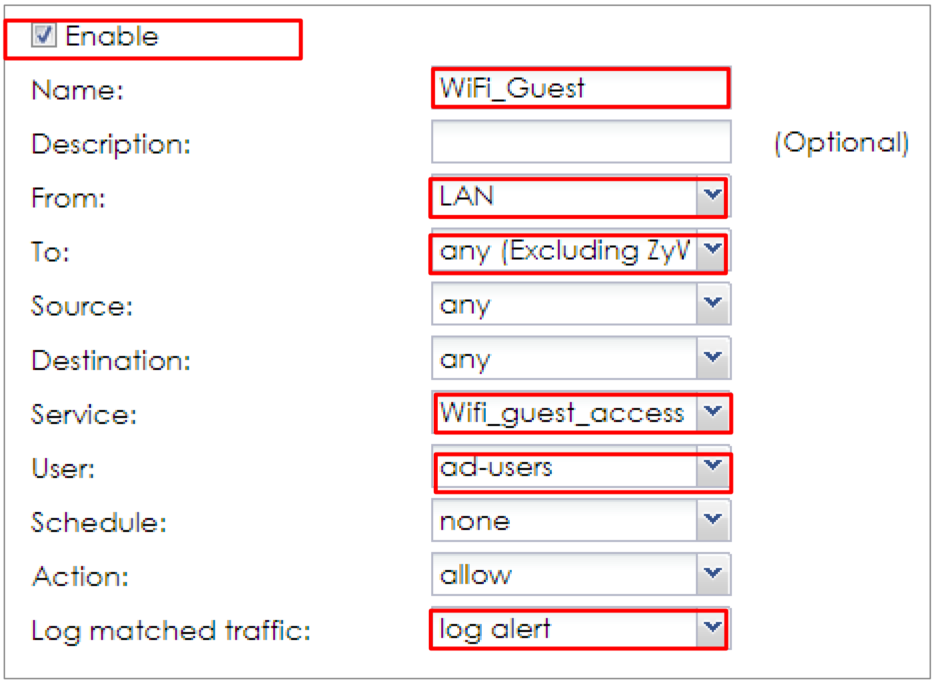
Returned User Attributes:

```
dn: CN=wifi_guest,CN=Users,DC=cso,DC=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: wifi_guest
givenName: wifi_guest
distinguishedName: CN=wifi_guest,CN=Users,DC=cso,DC=net
```

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy > Add corresponding**. Configure a **Name** for you to identify the **Security Policy** profile. Set **From: LAN** and **To: any (Excluding ZyWALL)**. Set **Service** to be the service rule for Wi-Fi guest (wifi_guest_access in this example). Set **User** to be the Wi-Fi guest user (ad-users in this example).   Select Log type to be **log alert** in order to view the result later.

CONFIGURATION > Security Policy > Policy > Add corresponding

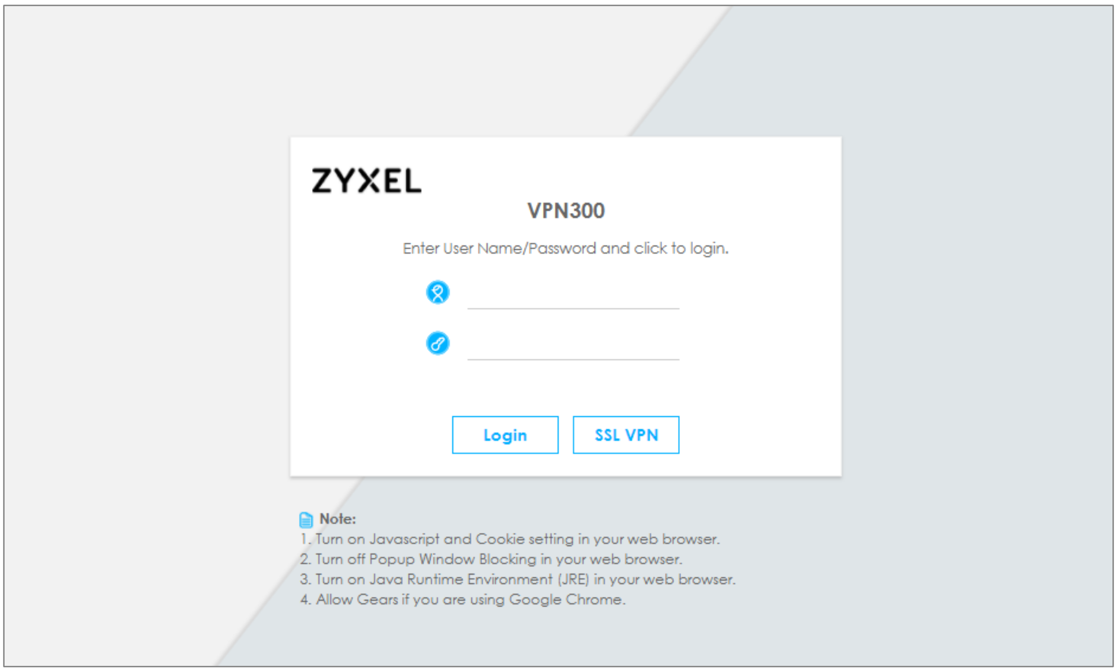


☑ Enable

Name:	WiFi_Guest	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyV	
Source:	any	
Destination:	any	
Service:	Wifi_guest_access	
User:	ad-users	
Schedule:	none	
Action:	allow	
Log matched traffic:	log alert	

Test the Result

Using a mobile device to connect to the AP which is connected to the ZyWALL/USG. When you try to access the Internet, it will redirect to the user login screen.



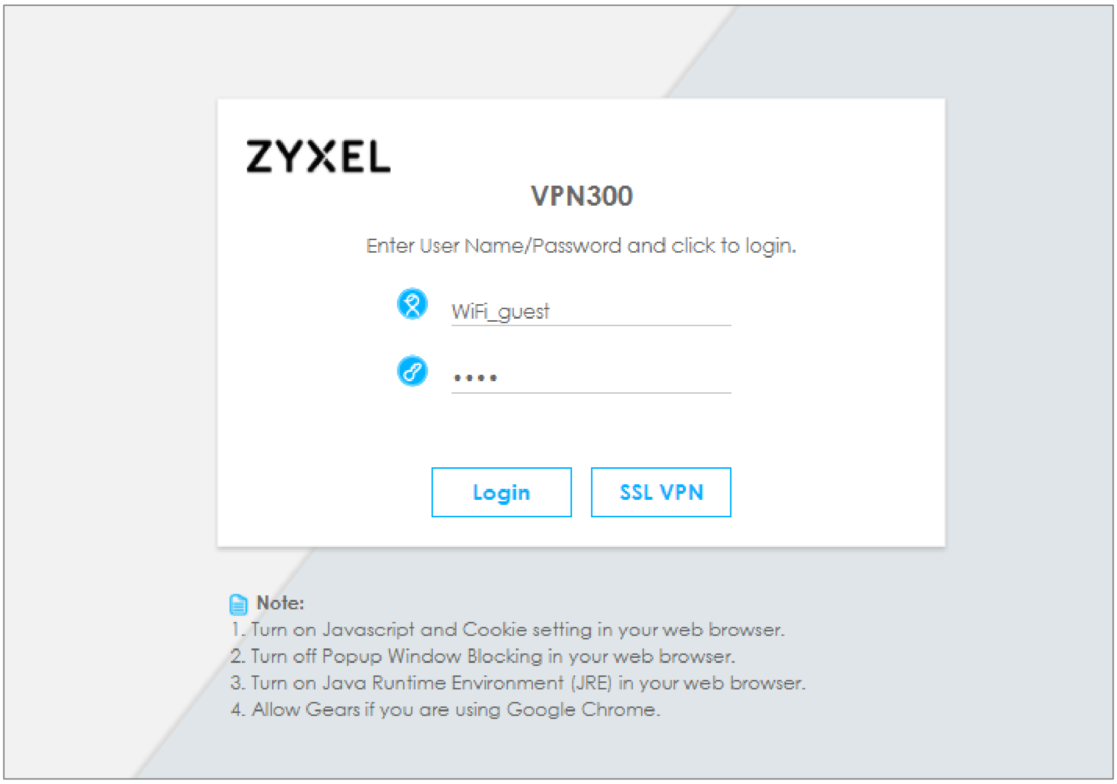
ZYXEL

VPN300

Enter User Name/Password and click to login.

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.

Type the Wi-Fi guest **User Name** and **Password**, click **Login**.



ZYXEL

VPN300

Enter User Name/Password and click to login.

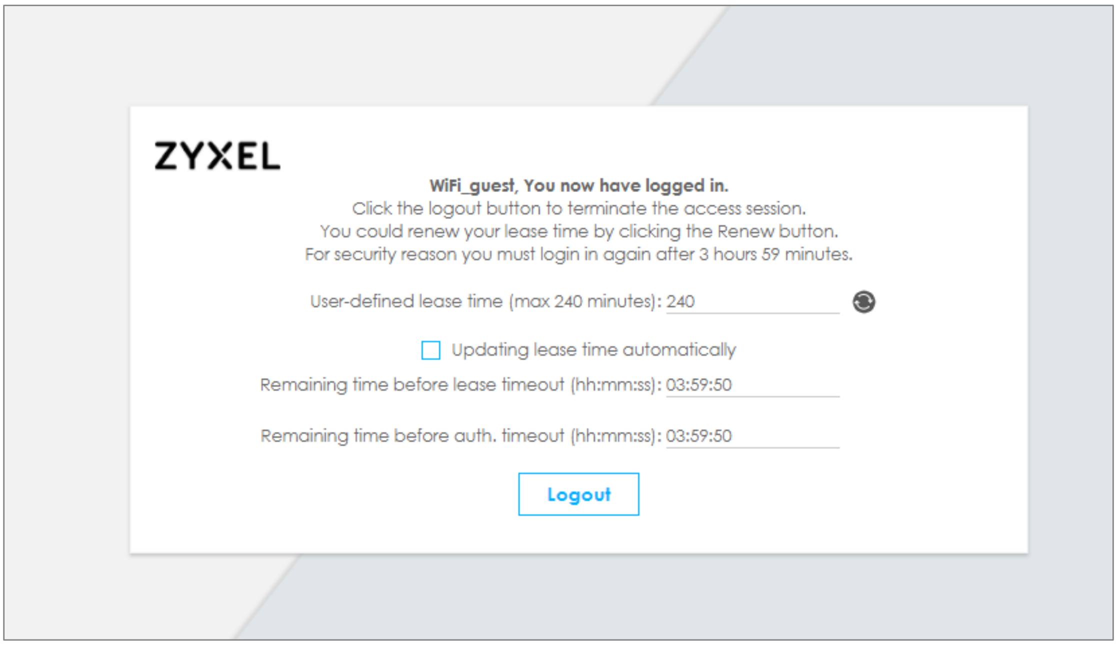
WiFi_guest

••••

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.

The access session page will appear.



ZYXEL

WiFi_guest, You now have logged in.
Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after 3 hours 59 minutes.

User-defined lease time (max 240 minutes): 240

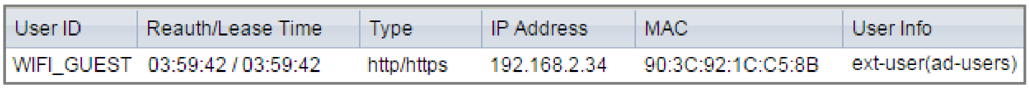
□ Updating lease time automatically

Remaining time before lease timeout (hh:mm:ss): 03:59:50

Remaining time before auth. timeout (hh:mm:ss): 03:59:50

Go to the ZyWALL/USG **Monitor > System Status > Login Users**, you will see current login user list as below.

Monitor > System Status > Login Users

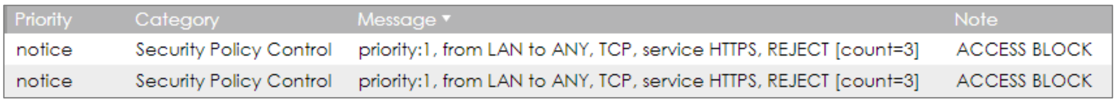


User ID	Reauth/Lease Time	Type	IP Address	MAC	User Info
WIFI_GUEST	03:59:42 / 03:59:42	http/https	192.168.2.34	90:3C:92:1C:C5:8B	ext-user(ad-users)

What Could Go Wrong?

If you see [notice] log shown as below, the Wi-Fi guest traffic is blocked by the **priority 1 Security Policy**. The ZyWALL/USG checks the security policy in order and applies the first security policy the traffic matches. If the Wi-Fi guest traffic matches a policy that comes earlier in the list, it may be unexpectedly blocked. Please change your policy setting or move the Wi-Fi guest policy to the higher priority.

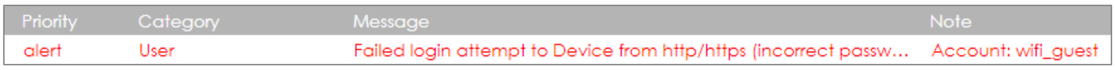
Monitor > Log



Priority	Category	Message ▾	Note
notice	Security Policy Control	priority:1, from LAN to ANY, TCP, service HTTPS, REJECT [count=3]	ACCESS BLOCK
notice	Security Policy Control	priority:1, from LAN to ANY, TCP, service HTTPS, REJECT [count=3]	ACCESS BLOCK

If you see [alert] log message shown as below, the Wi-Fi guest traffic failed. Please make sure you enable **Web Authentication** and check your AD server is working properly.

Monitor > Log

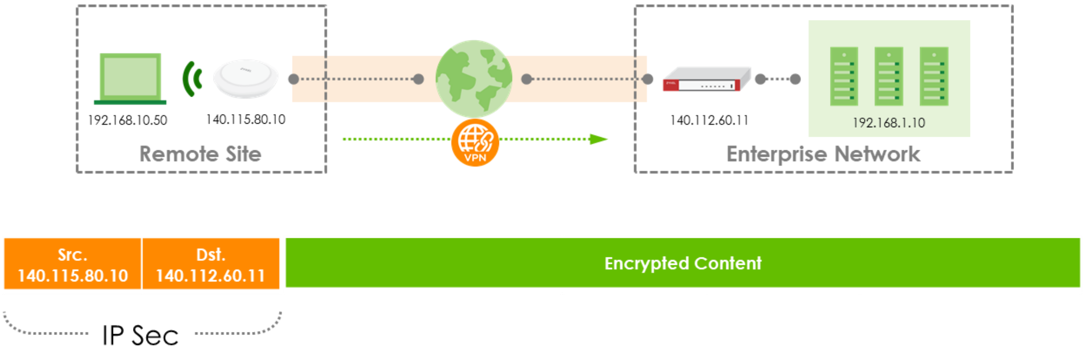


Priority	Category	Message	Note
alert	User	Failed login attempt to Device from http/https (incorrect passw...	Account: wifi_guest

Note: The default setting of **Security Policy** is without log notification (except **PolicyDefault**), if you want to check which policy may potentially block the traffic, please select this policy and set the **Log matched traffic** to be **log** or **log alert**.

How to Configure Secure Wi-Fi to Secure the Wireless Environment?

In a Secure Wi-Fi, AP acts as a VPN Client and establish the IPsec tunnel to Gateway then the traffic of tunnel mode SSID can be protected by IPsec VPN. This approach provides data encryption for teleworker's traffic (GRE over IPsec VPN) without any settings on user end device. The example instructs how to set up Secure Wi-Fi on AP controller to encrypt the traffic from station in remote site to enterprise network.

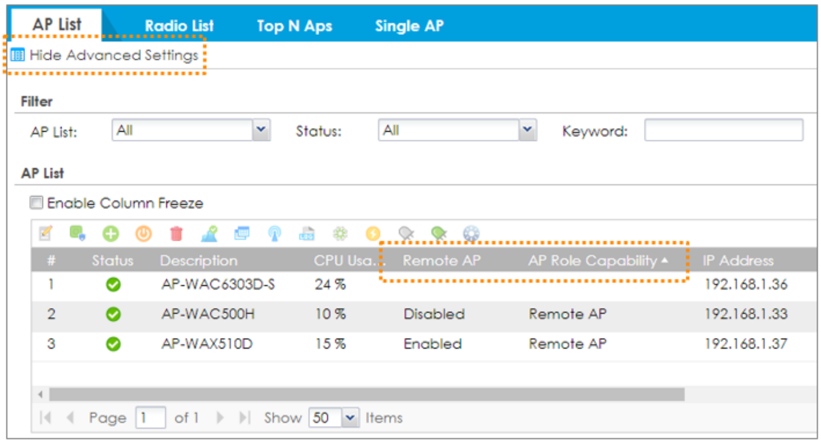


Secure Wi-Fi supported models:

AP Controller (with ZLD5.00): ATP Series, USG Series

Access Point (with WLAN 6.20): WAX650S / WAX610D / WAX510D / WAC500 / WAC500H

The capability of Remote AP can be checked at: **Monitor > Wireless > AP Information > AP List > Show Advanced Settings.**



Filter

AP List: All Status: All Keyword:

AP List

□ Enable Column Freeze

#	Status	Description	CPU Usa...	Remote AP	AP Role Capability ▲	IP Address
1	✓	AP-WAC6303D-S	24 %			192.168.1.36
2	✓	AP-WAC500H	10 %	Disabled	Remote AP	192.168.1.33
3	✓	AP-WAX510D	15 %	Enabled	Remote AP	192.168.1.37

Page 1 of 1 Show 50 Items

Note: To protect the Security Gateway from overloading due to handle to much tunnel traffic, only 25% of managed APs can be configured as Remote AP.

Set up Secure Wi-Fi on AP controller

There're two stages when deploy the Secure Wi-Fi on AP managed by AP Controller and status is online.

Stage one, finish the configuration inside enterprise network.

- Configure AP role as Remote AP and SSID setting
- Update the Controller IP as the USG's WAN IP

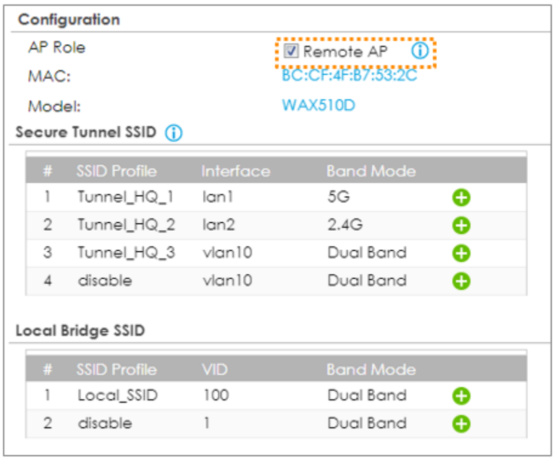
Stage two, remote users power up the AP, and then the IP Sec tunnel will be established automatically.

- Power up remote APs at remote side

Configure AP role as Remote AP and SSID setting

Secure Wi-Fi is per AP setting at **Configuration > Wireless > AP Management > Mgmt. AP List > Specific AP.**

Enable the AP Role to Remote AP. The maximum of Secure Tunnel SSIDs is up to four. Then define which interface the traffic will be tunneled to, and where to transmit the traffic at.



Configuration

AP Role ☑ Remote AP ⓘ

MAC: BC:CF:4F:B7:53:2C

Model: WAX510D

Secure Tunnel SSID ⓘ

#	SSID Profile	Interface	Band Mode	
1	Tunnel_HQ_1	lan1	5G	⊕
2	Tunnel_HQ_2	lan2	2.4G	⊕
3	Tunnel_HQ_3	vlan10	Dual Band	⊕
4	disable	vlan10	Dual Band	⊕

Local Bridge SSID

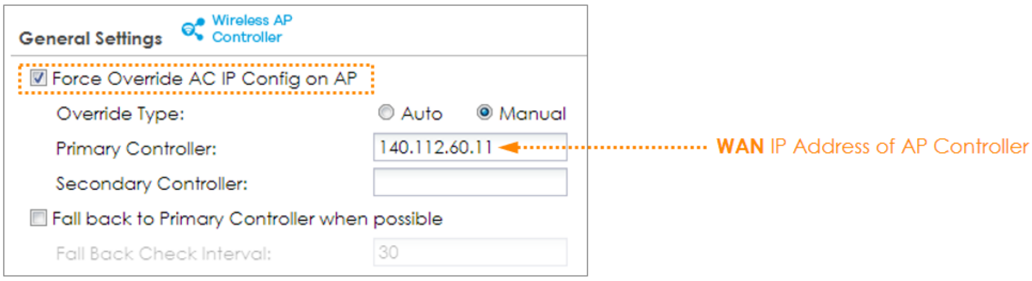
#	SSID Profile	VID	Band Mode	
1	Local_SSID	100	Dual Band	⊕
2	disable	1	Dual Band	⊕

NOTE: Secure Tunnel can be only applied to SSID, Ethernet traffic from clients connecting to AP's LAN port won't be tunneled back to Controller.

Update the Controller IP as the USG's WAN IP

Besides setting the SSID also need to override the Controller's IP address on AP to let it connect back to HQ's Gateway after booting up in remote site. If Gateway supports dual WAN, add another WAN IP in the "secondary controller" column. FQDN is also an available input option for dynamic WAN IP, but requires corresponding DNS settings.

Assign Gateway's WAN IP as AP's Controller IP at: **Configuration > Wireless > AP Management > AP Policy**



General Settings

☑ Force Override AC IP Config on AP

Override Type: ○ Auto ● Manual

Primary Controller: 140.112.60.11

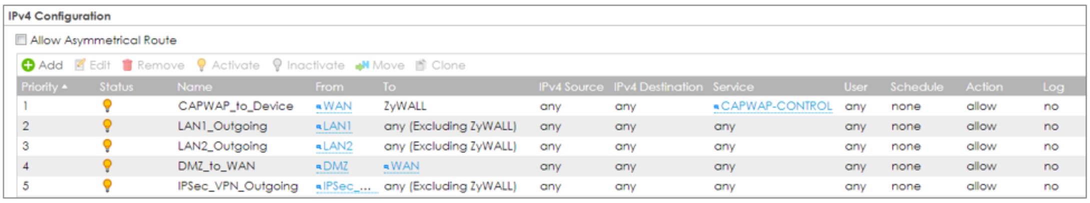
Secondary Controller:

☐ Fall back to Primary Controller when possible

Fall Back Check Interval: 30

WAN IP Address of AP Controller

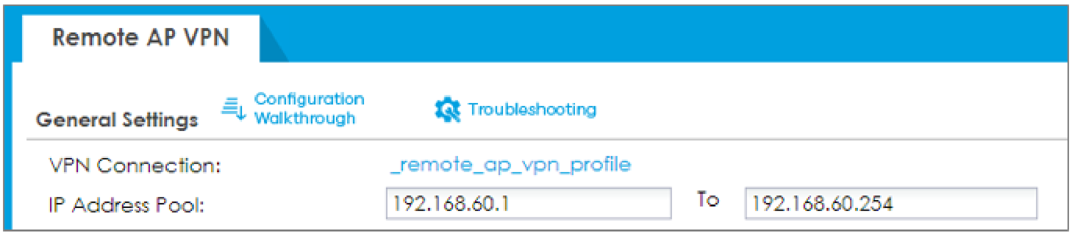
Firewall Policy Rule that is for CAPWAP connection and Remote AP VPN IP Address Pool that is a new subnet (192.168.60.1/24) for Remote AP VPN Client use will be auto-added when Remote AP is enabled.



IPv4 Configuration

☐ Allow Asymmetrical Route

Priority ▲	Status	Name	From	To	IPv4 Source	IPv4 Destination	Service	User	Schedule	Action	Log
1	💡	CAPWAP_to_Device	WAN	ZyWALL	any	any	CAPWAP-CONTROL	any	none	allow	no
2	💡	LAN1_Outgoing	LAN1	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
3	💡	LAN2_Outgoing	LAN2	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
4	💡	DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	allow	no
5	💡	IPSec_VPN_Outgoing	IPSec_...	any (Excluding ZyWALL)	any	any	any	any	none	allow	no



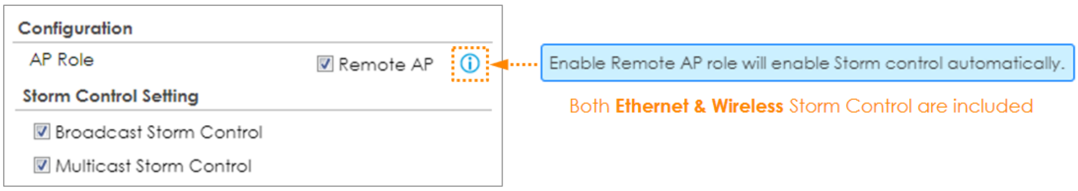
Remote AP VPN

General Settings — Configuration Walkthrough — Troubleshooting

VPN Connection: _remote_ap_vpn_profile

IP Address Pool: 192.168.60.1 To 192.168.60.254

On remote AP, Storm Control is automatically activated in order to avoid huge broadcast traffic flooding from wireless part to Gateway and to other Remote APs. Both Wireless and Ethernet Storm Control will be auto-enabled on Remote AP.



Configuration

AP Role ☑ Remote AP ⓘ

Storm Control Setting

☑ Broadcast Storm Control

☑ Multicast Storm Control

Enable Remote AP role will enable Storm control automatically.

Both **Ethernet & Wireless** Storm Control are included

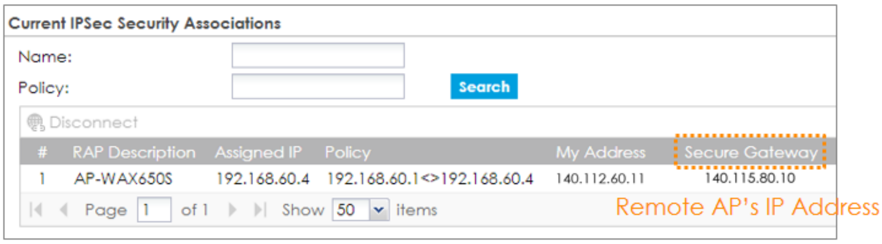
Power up remote APs at remote side

Remote users power up the AP, and then the IP Sec tunnel will be established automatically.

Test the Result

After Remote AP boots up in the remote site, AP will automatically establish the IPSec VPN connection with HQ. AP and tunnel information displays on the Web GUI at:

Monitor > VPN Monitor > Remote AP VPN > Remote AP VPN



Current IPSec Security Associations

Name:

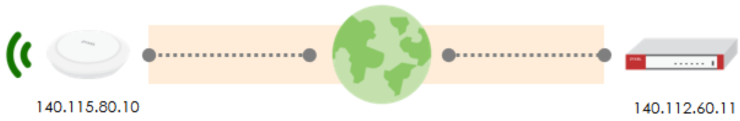
Policy: Search

Disconnect

#	RAP Description	Assigned IP	Policy	My Address	Secure Gateway
1	AP-WAX650S	192.168.60.4	192.168.60.1<>192.168.60.4	140.112.60.11	140.115.80.10

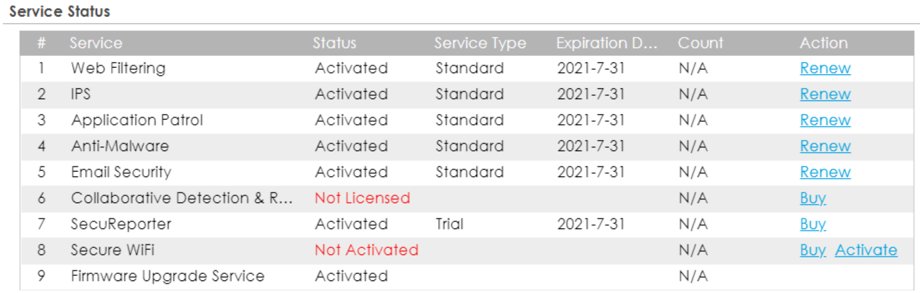
Page 1 of 1 Show 50 items

Remote AP's IP Address



What can go wrong

1. Configure all the corresponding setting on interface before you connect the link.
2. Maximum Remote AP number is limited by Device's capability of "Max. Concurrent IPsec Tunnel" and 25% of Maximum managed AP number.
3. Secure Wi-Fi requires specific license on AP.

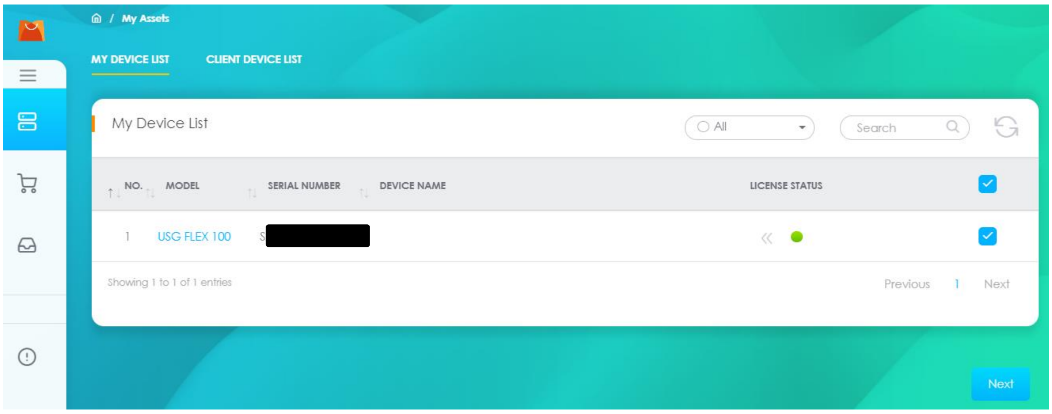


Service Status

#	Service	Status	Service Type	Expiration D...	Count	Action
1	Web Filtering	Activated	Standard	2021-7-31	N/A	Renew
2	IPS	Activated	Standard	2021-7-31	N/A	Renew
3	Application Patrol	Activated	Standard	2021-7-31	N/A	Renew
4	Anti-Malware	Activated	Standard	2021-7-31	N/A	Renew
5	Email Security	Activated	Standard	2021-7-31	N/A	Renew
6	Collaborative Detection & R...	Not Licensed			N/A	Buy
7	SecuReporter	Activated	Trial	2021-7-31	N/A	Buy
8	Secure WiFi	Not Activated			N/A	Buy Activate
9	Firmware Upgrade Service	Activated			N/A	

You check license status at: **Configuration > Licensing > Registration > Service**

Click Activate to use the Secure Wi-Fi feature. Click Buy, a new webpage will redirect to the Zyxel Marketplace for purchasing the license.



My Device List

NO.	MODEL	SERIAL NUMBER	DEVICE NAME	LICENSE STATUS	☑
1	USG FLEX 100	S[redacted]		●	☑

Showing 1 to 1 of 1 entries

Previous 1 Next

When license expired, VPN connection from Remote AP will be closed, Secure Tunnel SSID on remote AP will be disabled and will Auto-recovery after a new license activated.

Chapter 7- Maintenance

How to Manage ZyWALL/USG Configuration Files

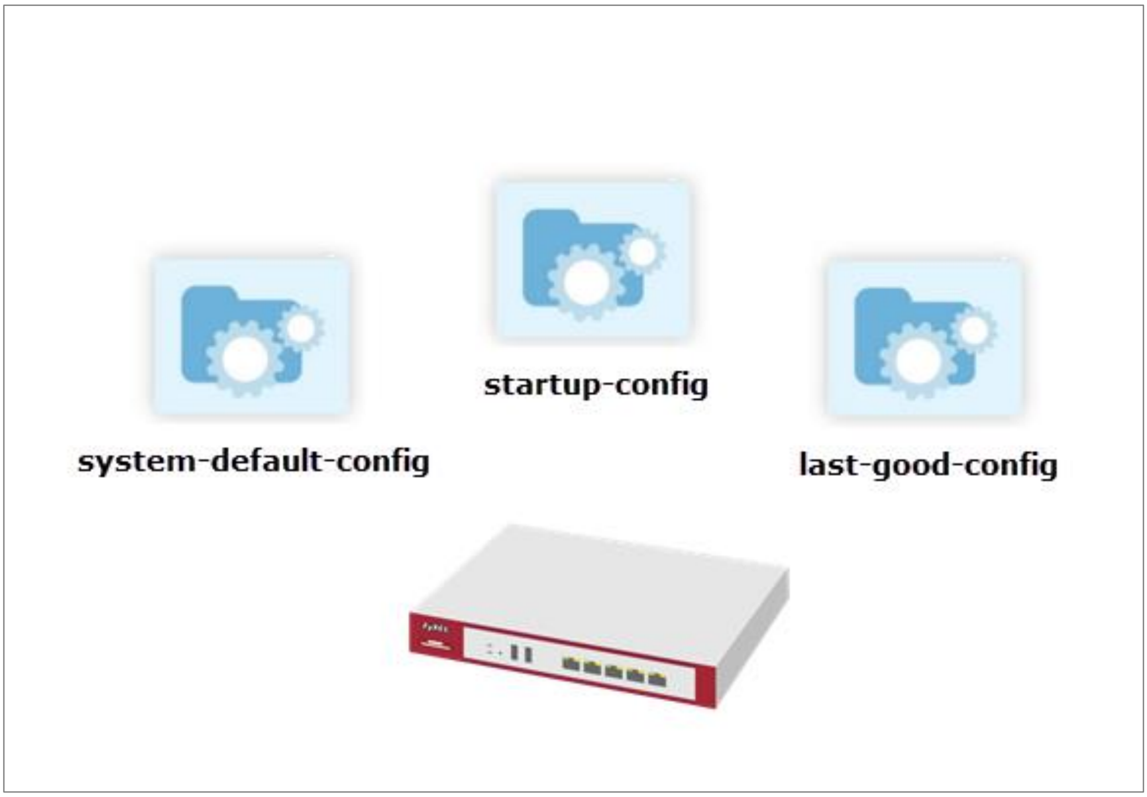
This is an example of how to rename, download, copy, apply and upload configuration files. Once your ZyWALL/USG is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

The **system-default.conf** file contains the ZyWALL/USG's default settings. This configuration file is included when you upload a firmware package.

The startup-config.conf file is the configuration file that the ZyWALL/USG is currently using. If you make and save changes during your management session, the changes are applied to this configuration file.

The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted.

ZyWALL/USG with Configuration Files Example

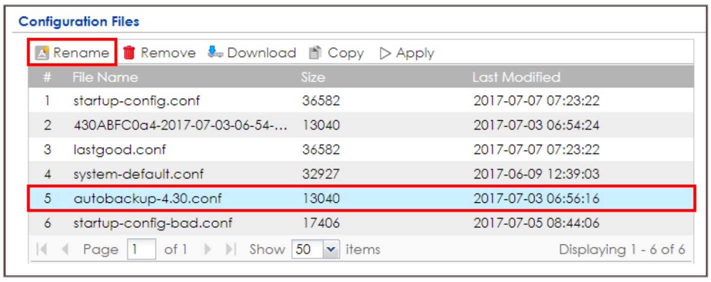


Note: This example was using USG310 (Firmware Version: ZLD 4.25).

Rename the Configuration Files from the ZyWALL/USG

In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File**, select the configuration file and click **Rename**. A pop-up screen will appear allowing you to edit the **Target file** name. Click **OK** to save the **Rename** configuration.

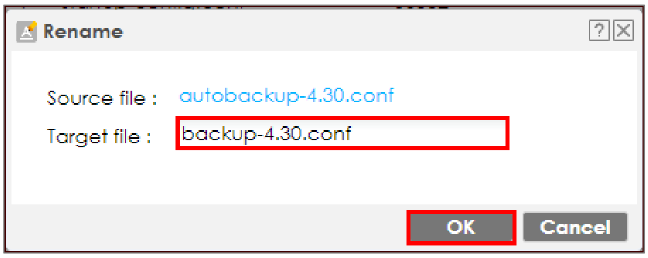
MAINTENANCE > File Manager > Configuration File


Configuration Files

#	File Name	Size	Last Modified
1	startup-config.conf	36582	2017-07-07 07:23:22
2	430ABFC0a4-2017-07-03-06-54-...	13040	2017-07-03 06:54:24
3	lastgood.conf	36582	2017-07-07 07:23:22
4	system-default.conf	32927	2017-06-09 12:39:03
5	autobackup-4.30.conf	13040	2017-07-03 06:56:16
6	startup-config-bad.conf	17406	2017-07-05 08:44:06

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

MAINTENANCE > File Manager > Configuration File > Rename



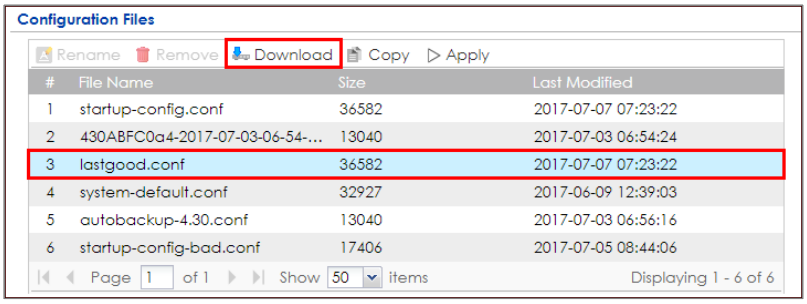
Source file : autobackup-4.30.conf

Target file : backup-4.30.conf

Download the Configuration Files on the ZyWALL/USG

In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File**, select the configuration file and click **Download** to back up your configuration file from ZyWALL/USG to your computer.

MAINTENANCE > File Manager > Configuration File

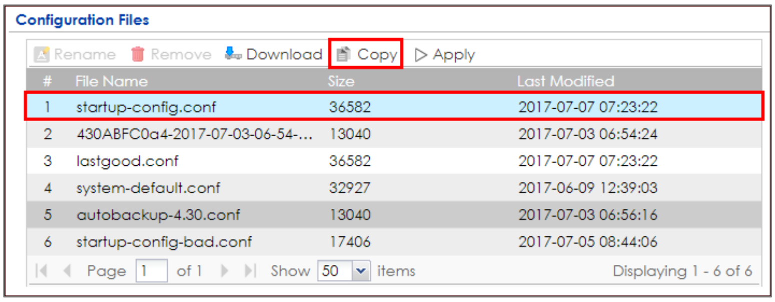


#	File Name	Size	Last Modified
1	startup-config.conf	36582	2017-07-07 07:23:22
2	430ABFC0a4-2017-07-03-06-54-...	13040	2017-07-03 06:54:24
3	lastgood.conf	36582	2017-07-07 07:23:22
4	system-default.conf	32927	2017-06-09 12:39:03
5	autobackup-4.30.conf	13040	2017-07-03 06:56:16
6	startup-config-bad.conf	17406	2017-07-05 08:44:06

Copy the Configuration Files on the ZyWALL/USG

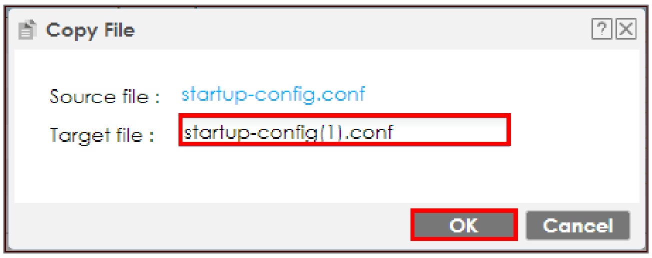
In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File**, select the configuration file and click **Copy**. A pop-up screen will appear allowing you to edit the **Target file** name. Click **OK** to save the **Copy** configuration.

MAINTENANCE > File Manager > Configuration File



#	File Name	Size	Last Modified
1	startup-config.conf	36582	2017-07-07 07:23:22
2	430ABFC0a4-2017-07-03-06-54-...	13040	2017-07-03 06:54:24
3	lastgood.conf	36582	2017-07-07 07:23:22
4	system-default.conf	32927	2017-06-09 12:39:03
5	autobackup-4.30.conf	13040	2017-07-03 06:56:16
6	startup-config-bad.conf	17406	2017-07-05 08:44:06

MAINTENANCE > File Manager > Configuration File > Copy



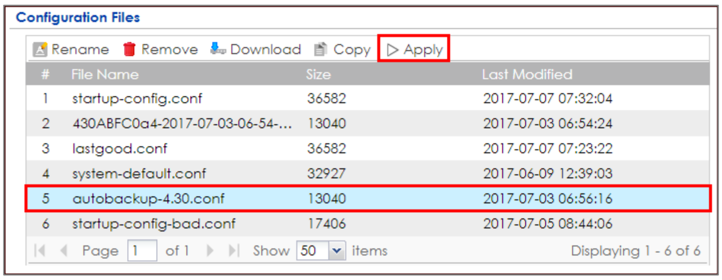
Source file : startup-config.conf

Target file : startup-config(1).conf

Apply the Configuration Files on the ZyWALL/USG

In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File**, select a specific configuration file to have ZyWALL/USG use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL/USG settings to the factory defaults. Or select the **lastgood.conf** which is the most recently used (valid) configuration file that was saved when the device last restarted. If you uploaded and applied a configuration file with an error, select this file then click **Apply** to return to a valid configuration.

MAINTENANCE > File Manager > Configuration File

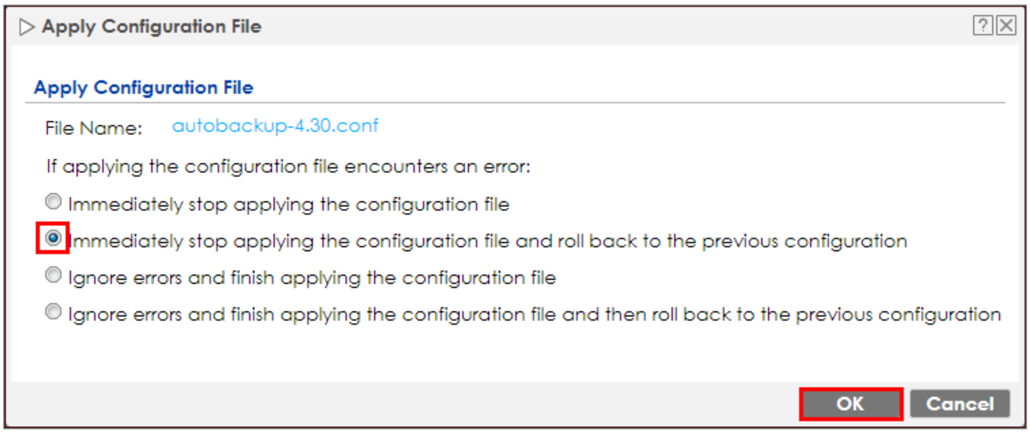


Configuration Files

#	File Name	Size	Last Modified
1	startup-config.conf	36582	2017-07-07 07:32:04
2	430ABFC0a4-2017-07-03-06-54-...	13040	2017-07-03 06:54:24
3	lastgood.conf	36582	2017-07-07 07:23:22
4	system-default.conf	32927	2017-06-09 12:39:03
5	autobackup-4.30.conf	13040	2017-07-03 06:56:16
6	startup-config-bad.conf	17406	2017-07-05 08:44:06

A pop-up screen will appear allowing you to edit the **Target file** name. Select **Immediately stop applying the configuration file and roll back to the previous configuration** to get the ZyWALL/USG started with a fully valid configuration file as quickly as possible. Click **OK** to have the ZyWALL/USG start applying the configuration file.

MAINTENANCE > File Manager > Configuration File > Apply Configuration File



▷ Apply Configuration File

Apply Configuration File

File Name: autobackup-4.30.conf

If applying the configuration file encounters an error:

○ Immediately stop applying the configuration file

● Immediately stop applying the configuration file and roll back to the previous configuration

○ Ignore errors and finish applying the configuration file

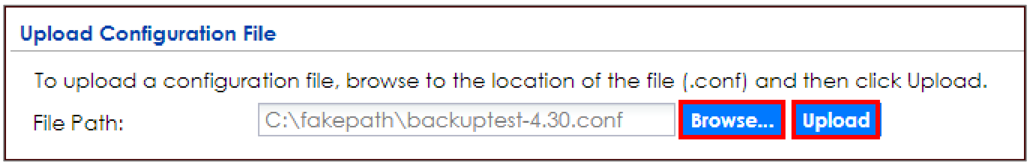
○ Ignore errors and finish applying the configuration file and then roll back to the previous configuration

Note: Do not shut down the ZyWALL/USG while the configuration file is being applied.

Upload the Configuration Files from the ZyWALL/USG

In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File > Upload Configuration File**, select **Browse** to upload a new or previously saved configuration file from your computer to your ZyWALL/USG. You cannot upload a configuration file named **system-default.conf** or **lastgood.conf**. If you upload **startup-config.conf**, it will replace the current configuration and immediately apply the new settings.

MAINTENANCE > File Manager > Configuration File



Upload Configuration File

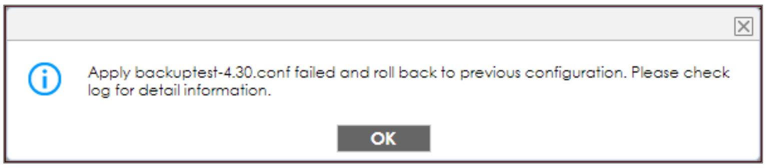
To upload a configuration file, browse to the location of the file (.conf) and then click Upload.

File Path: C:\fakepath\backuptest-4.30.conf

What Could Go Wrong?

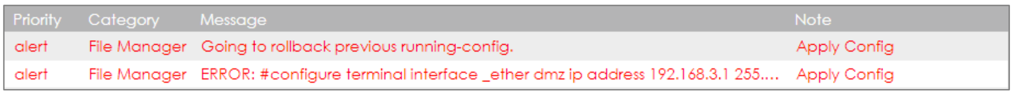
If you cannot apply a configuration file and the device shows error message, go to **Monitor > Log** to check the [alert] log message and make the correction of the configuration file. In this example, the [alert] log message shows the configuration file has an incomplete static DHCP address so that the device can't apply it.

MAINTENANCE > File Manager > Configuration File > Apply Configuration File



Apply backuptest-4.30.conf failed and roll back to previous configuration. Please check log for detail information.

Monitor > Log

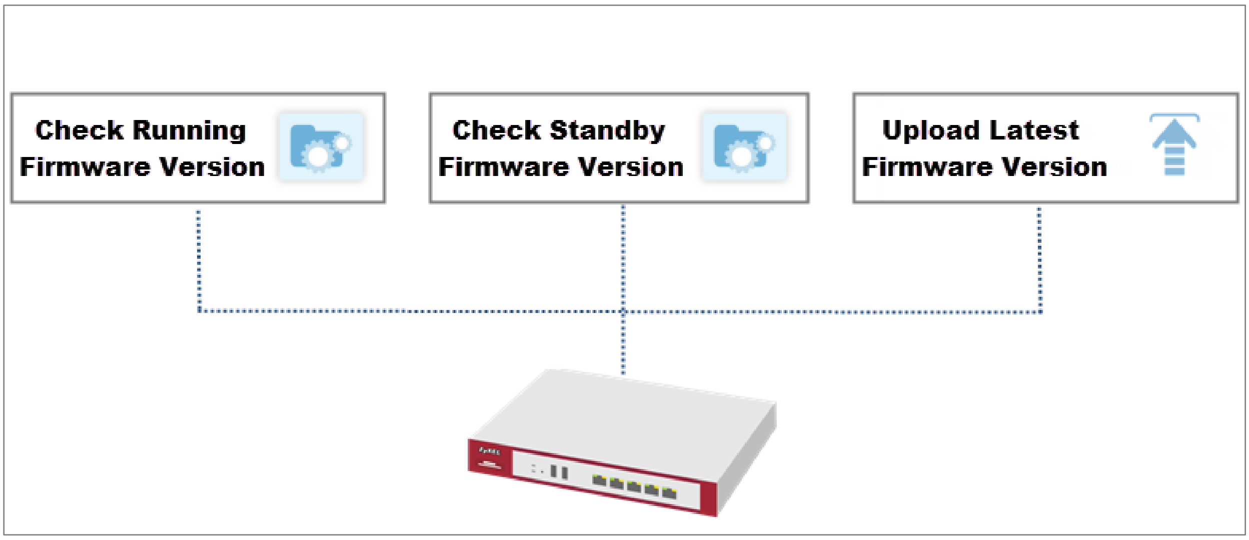


Priority	Category	Message	Note
alert	File Manager	Going to rollback previous running-config.	Apply Config
alert	File Manager	ERROR: #configure terminal interface _ether dmz ip address 192.168.3.1 255....	Apply Config

How to Manage ZyWALL/USG Firmware

This is an example of using ZyWALL/USG to check your current firmware version and upload firmware to the ZyWALL/USG. You can upload firmware to be the **Running** firmware or **Standby** firmware.

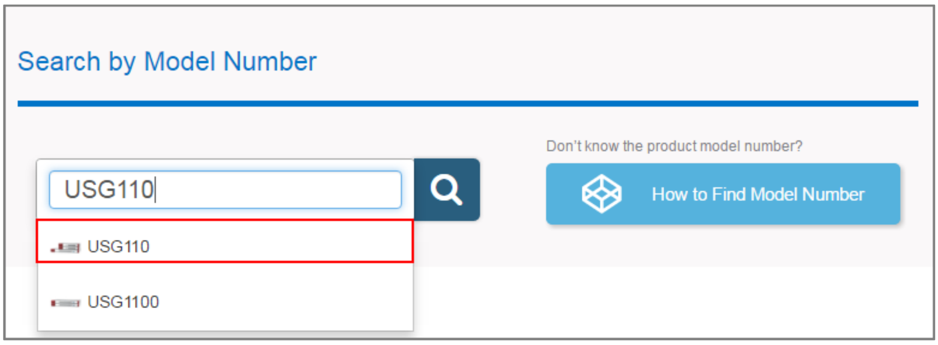
ZyWALL/USG with Firmware Management Example


Check Running Firmware Version
Check Standby Firmware Version
Upload Latest Firmware Version

Note: The firmware update can take up to five minutes. Do not turn off or reset the ZyWALL/USG while the firmware update is in progress. This example was using USG110 (Firmware Version: ZLD 4.25).

Download the Current Firmware Version from ZyXEL.com

Go to www.zyxel.com/support/download_landing.shtml and download the current firmware package.



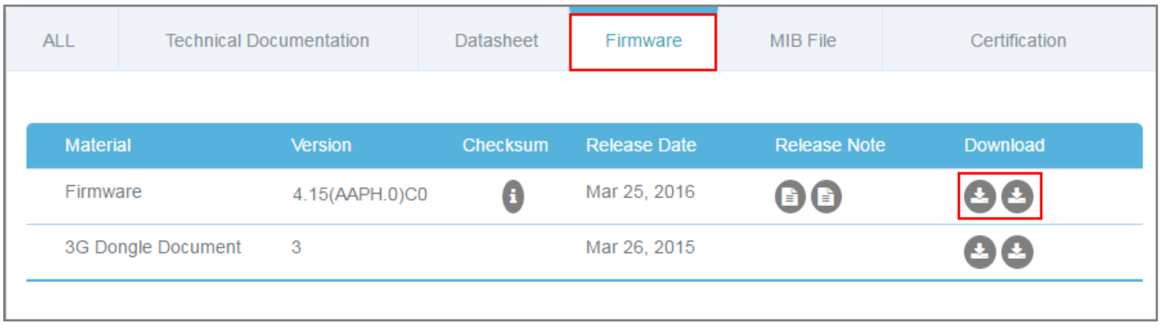
Search by Model Number

USG110

- USG110
- USG1100

Don't know the product model number?

How to Find Model Number

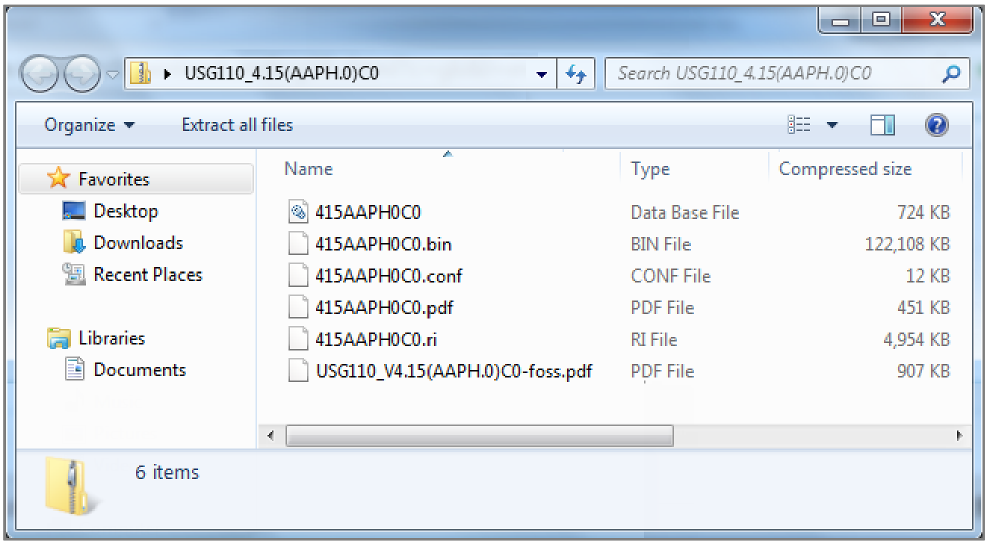


ALL | Technical Documentation | Datasheet | Firmware | MIB File | Certification

Material	Version	Checksum	Release Date	Release Note	Download
Firmware	4.15(AAPH.0)C0	ℹ	Mar 25, 2016	🗎 🗎	⬇ ⬇
3G Dongle Document	3		Mar 26, 2015		⬇ ⬇

Extract firmware zip file.

USG110_4.15(AAPH.0)C0.zip



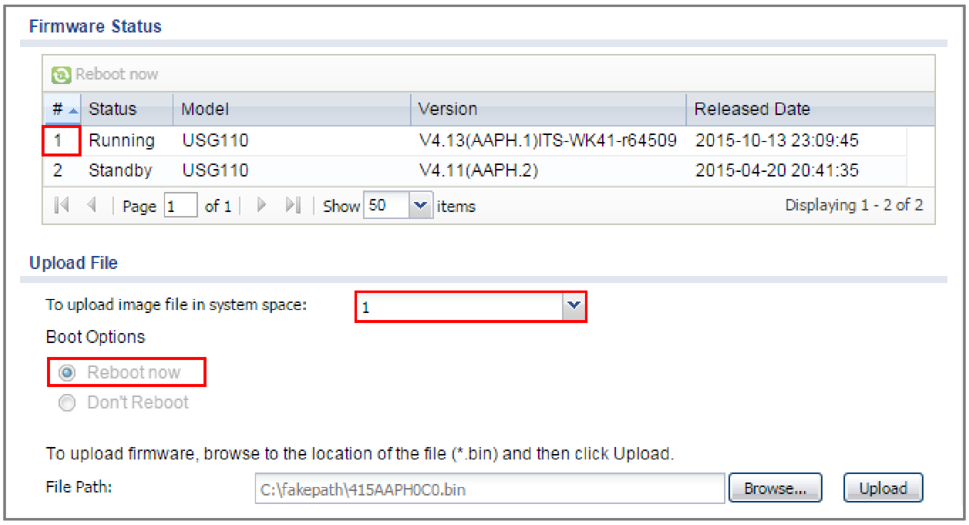
Name	Type	Compressed size
415AAPH0C0	Data Base File	724 KB
415AAPH0C0.bin	BIN File	122,108 KB
415AAPH0C0.conf	CONF File	12 KB
415AAPH0C0.pdf	PDF File	451 KB
415AAPH0C0.ri	RI File	4,954 KB
USG110_V4.15(AAPH.0)C0-foss.pdf	PDF File	907 KB

Upload the Firmware on the ZyWALL/USG

In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Firmware Package > Upload File**. Click the **To upload image file in system space** pull-down menu and select (**1**) or (**2**). The default **Standby** system space is (**2**), so if you want to upload new firmware to be the **Running** firmware, then select the **Running** system space (**1**). The ZyWALL/USG will reboot automatically.

If you upload firmware to the **Standby** system space (2), you have the option to select **Reboot now** or **Don't Reboot**.

MAINTENANCE > File Manager > Firmware Package > Upload File > (1)



#	Status	Model	Version	Released Date
1	Running	USG110	V4.13(AAPH.1)ITS-WK41-r64509	2015-10-13 23:09:45
2	Standby	USG110	V4.11(AAPH.2)	2015-04-20 20:41:35

To upload image file in system space: 1

Boot Options

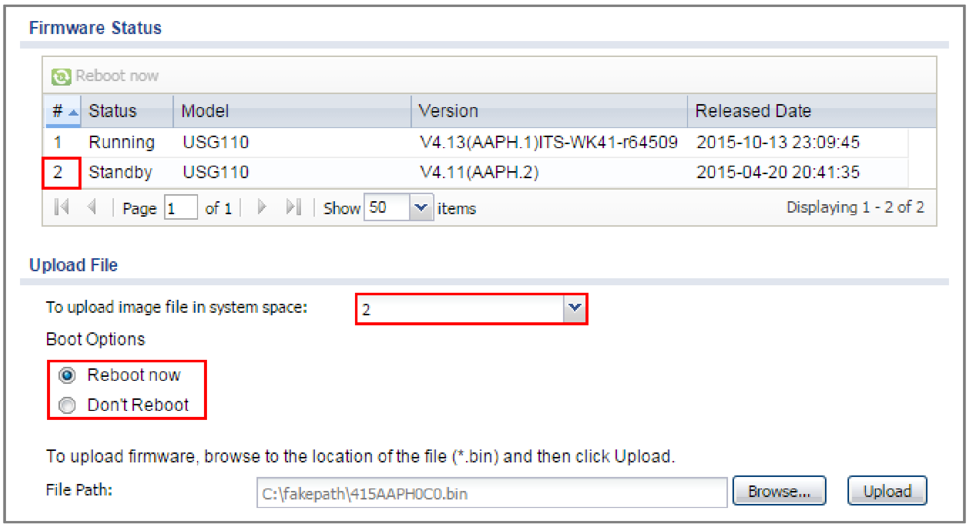
● Reboot now

○ Don't Reboot

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path: C:\fakepath\415AAPH0C0.bin

MAINTENANCE > File Manager > Firmware Package > Upload File > (2)



Firmware Status

#	Status	Model	Version	Released Date
1	Running	USG110	V4.13(AAPH.1)ITS-WK41-r64509	2015-10-13 23:09:45
2	Standby	USG110	V4.11(AAPH.2)	2015-04-20 20:41:35

Upload File

To upload image file in system space: 2

Boot Options

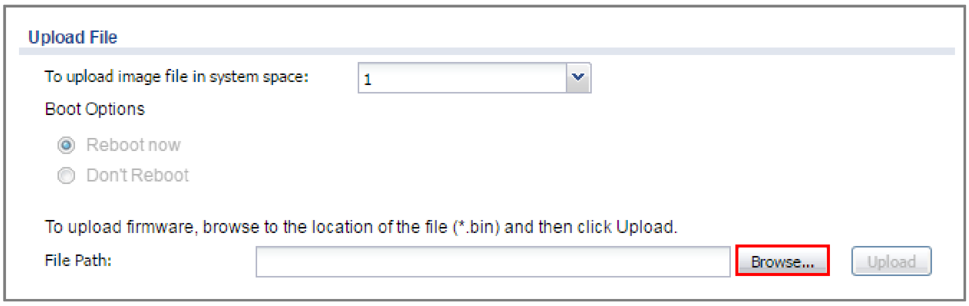
● Reboot now

○ Don't Reboot

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path: C:\fakepath\415AAPH0C0.bin

To upload firmware, click **Browse** to the location of the file (*.bin) and then click **Upload**.



Upload File

To upload image file in system space: 1

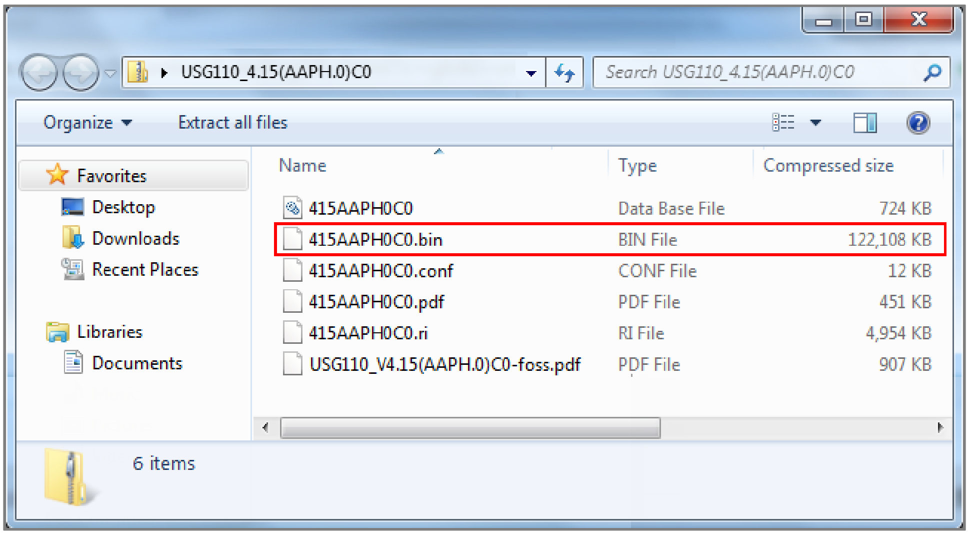
Boot Options

● Reboot now

○ Don't Reboot

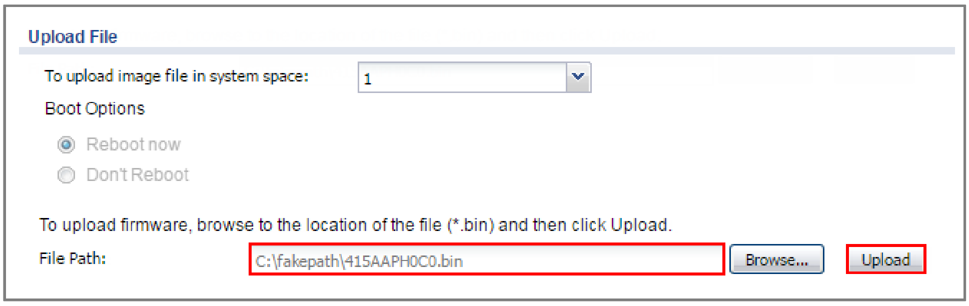
To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path:



USG110_4.15(AAPH.0)C0

Name	Type	Compressed size
415AAPH0C0	Data Base File	724 KB
415AAPH0C0.bin	BIN File	122,108 KB
415AAPH0C0.conf	CONF File	12 KB
415AAPH0C0.pdf	PDF File	451 KB
415AAPH0C0.ri	RI File	4,954 KB
USG110_V4.15(AAPH.0)C0-foss.pdf	PDF File	907 KB



Upload File

To upload image file in system space: 1

Boot Options

● Reboot now

○ Don't Reboot

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path: C:\fakepath\415AAPH0C0.bin

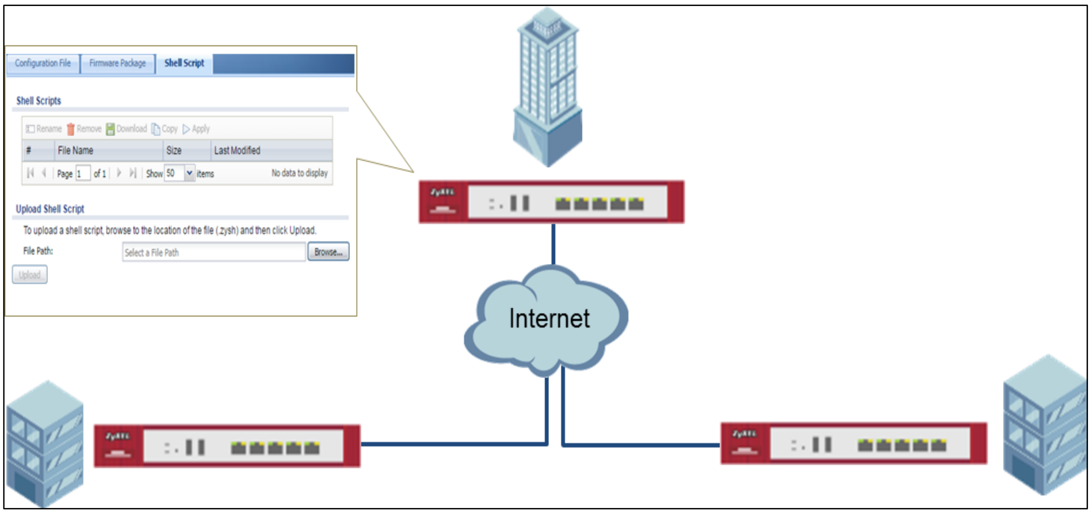
Note: The default **Running** system space is (1), the **Standby** system space is (2). If you select the **Standby** firmware and click **Reboot now** or you upload file to **Standby** system space (2) and select **Boot Options** to be **Reboot now**. After reboot process complete, the **Running** system space will be (2). **Standby** system space will be (1).

What Could Go Wrong?

If you cannot download the firmware, please check if you enable the **Destroy compressed files that could not be decompressed** function in **Anti-Virus**. ZyWALL/USG firmware package is ZIP file, the ZyWALL/USG classifies the firmware package as not being able to decompress will delete it. Please disable this option while downloading the firmware package.

How to Automatically Reboot the ZyWALL/USG by Schedule

This example shows how to use shell script and schedule run to reboot device automatically for maintenance purpose.



No data to display

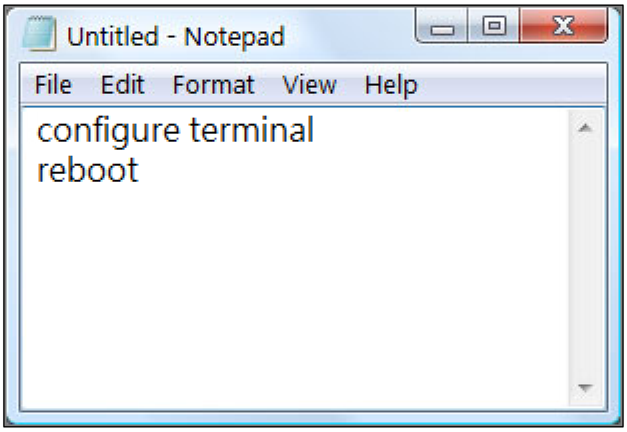
To upload a shell script, browse to the location of the file (.zysh) and then click Upload.

ZyWALL/USG Auto Schedule Reboot Settings

Note: This example was tested using USG110 (Firmware Version: ZLD 4.25).

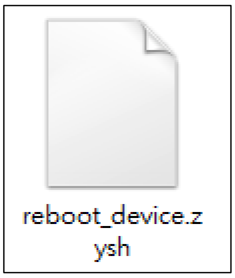
Set Up the Shell Script

1 Run Windows Notepad application and input below command:

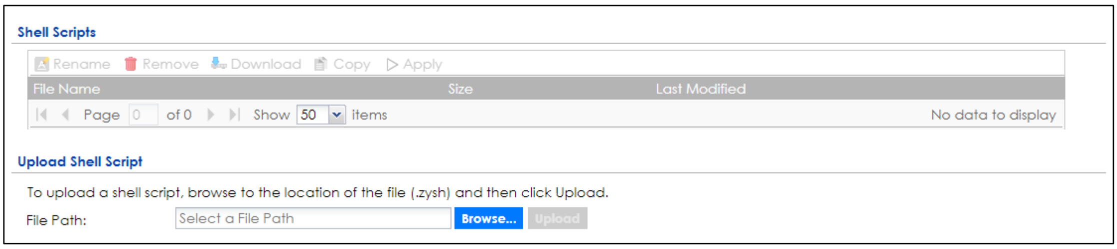


```
configure terminal
reboot
```

2 Save this file as "reboot_device.zysh"



3 In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Shell Script**. Click **Browse**... to find the reboot_device.zysh file. Click **Upload** to begin the upload process.

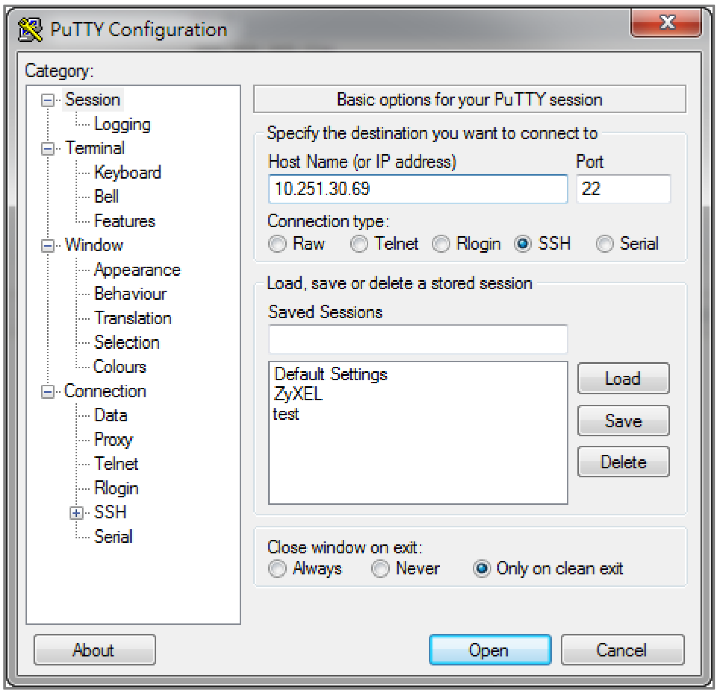

Shell Scripts
Rename Remove Download Copy Apply
File Name Size Last Modified
Page 0 of 0 Show 50 items No data to display
Upload Shell Script

To upload a shell script, browse to the location of the file (.zysh) and then click Upload.

File Path: Select a File Path

Set Up the Schedule Run

1 Login the device via console/telnet/SSH (using PuTTY in this example)



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.251.30.69

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

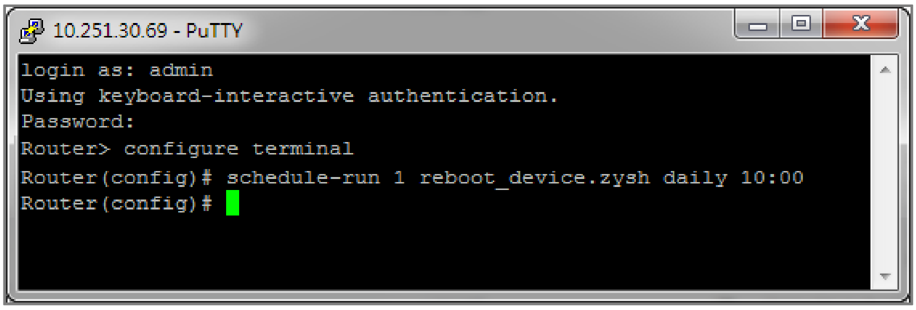
Default Settings
ZyXEL
test

Close window on exit: ○ Always ○ Never ● Only on clean exit

2 Issuing below commands based on three different (daily, weekly and monthly) user scenarios:

a. Router(config)# schedule-run 1 reboot_device.zysh daily 10:00

(The device will reboot at 10:00 everyday)

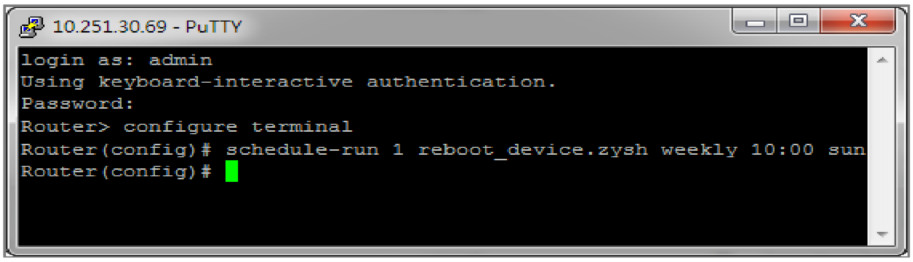


10.251.30.69 - PuTTY

```
login as: admin
Using keyboard-interactive authentication.
Password:
Router> configure terminal
Router(config)# schedule-run 1 reboot_device.zysh daily 10:00
Router(config)#
```

b. Router(config)# schedule-run 1 reboot_device.zysh weekly 10:00 sun

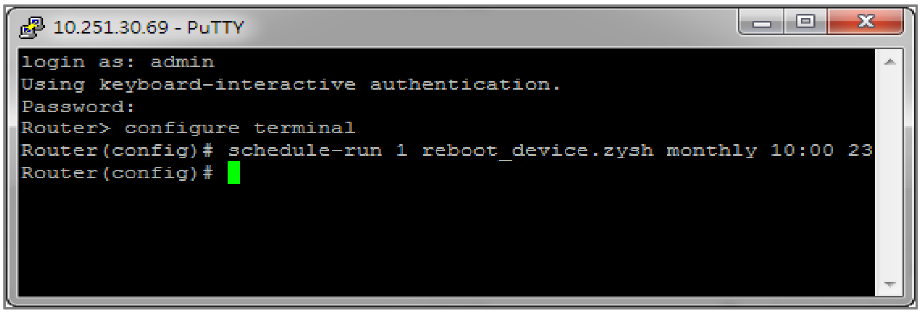
(The device will reboot at 10:00 every Sunday)



```
login as: admin
Using keyboard-interactive authentication.
Password:
Router> configure terminal
Router(config)# schedule-run 1 reboot_device.zysh weekly 10:00 sun
Router(config)#
```

c. Router(config)# schedule-run 1 reboot_device.zysh monthly 10:00 23

(The device will reboot at 10:00 every month on 23th)



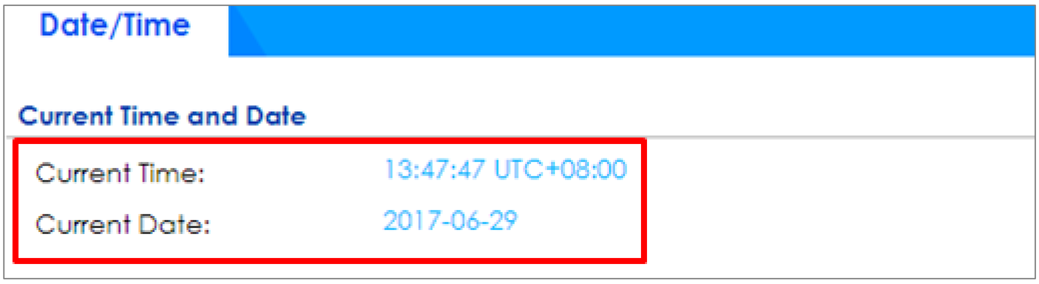
```
login as: admin
Using keyboard-interactive authentication.
Password:
Router> configure terminal
Router(config)# schedule-run 1 reboot_device.zysh monthly 10:00 23
Router(config)#
```

Check the Reboot Status

3 Login the device via console/telnet/SSH, the reboot runs as scheduled

4 Go to **Configuration > System> Date/Time**, check **Current Date/Time**.

Figure Configuration > System >Date/Time

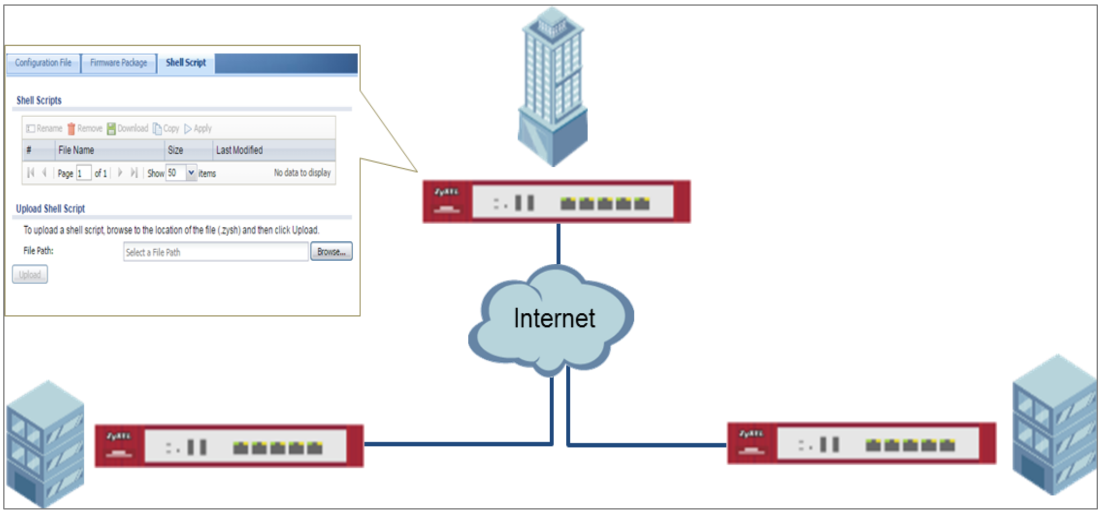


Current Time: 13:47:47 UTC+08:00

Current Date: 2017-06-29

How to continuously run a ZySH script

This example shows how to use shell script and continuously run a ZySH script automatically for maintenance purpose.



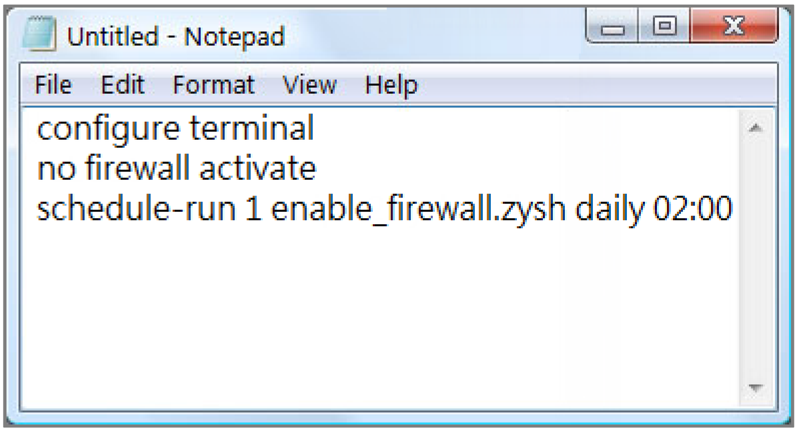
To upload a shell script, browse to the location of the file (.zysh) and then click Upload.

ZyWALL/USG continuously run a ZySH script Settings

> Note: This example was tested using USG110 (Firmware Version: ZLD 4.25).

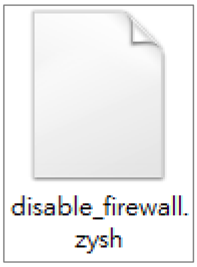
Set Up the Shell Script

1 Run Windows Notepad application and input below command:

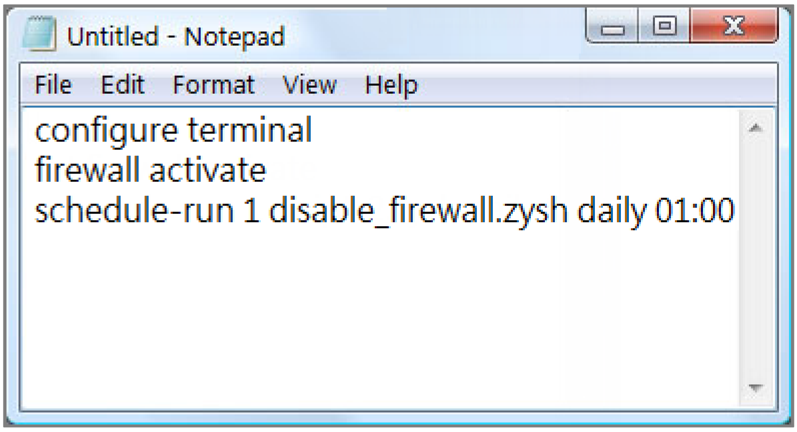


```
configure terminal
no firewall activate
schedule-run 1 enable_firewall.zysh daily 02:00
```

2 Save this file as "disable_firewall.zysh"

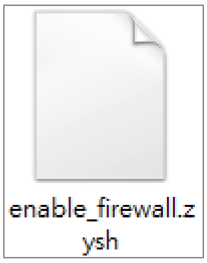


3 Run Windows Notepad application and input below command:

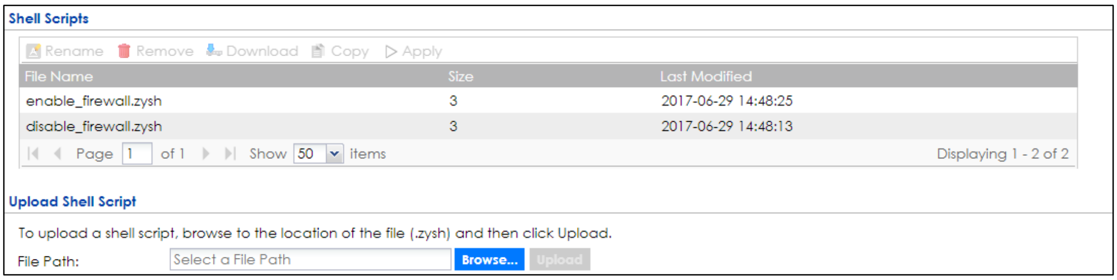


```
configure terminal
firewall activate
schedule-run 1 disable_firewall.zysh daily 01:00
```

4 Save this file as "enable_firewall.zysh"



5 In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Shell Script**. Click **Browse**... to find the disable_firewall.zysh and enable_firewall.zysh file. Click **Upload** to begin the upload process.



Shell Scripts

File Name	Size	Last Modified
enable_firewall.zysh	3	2017-06-29 14:48:25
disable_firewall.zysh	3	2017-06-29 14:48:13

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

Upload Shell Script

To upload a shell script, browse to the location of the file (.zysh) and then click Upload.

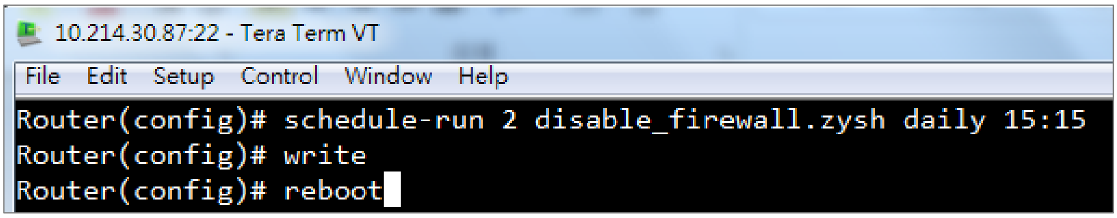
File Path: Select a File Path

Set Up the Schedule Run

6 Issuing below commands:

Router> configure terminal

Router(config)# schedule-run 1 disable_firewall.zysh daily 15:15

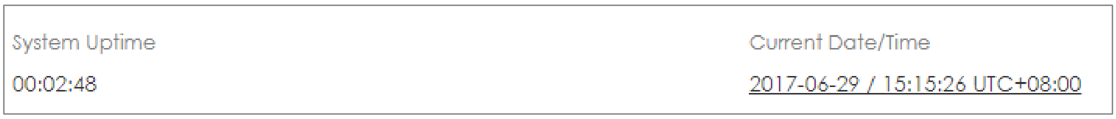


```
Router(config)# schedule-run 2 disable_firewall.zysh daily 15:15
Router(config)# write
Router(config)# reboot
```

Check the Result

1 In the ZyWALL/USG, go to **DASHBOARD**.

DASHBOARD



System Uptime

00:02:48

Current Date/Time

2017-06-29 / 15:15:26 UTC+08:00

How to Update Firmware Automatically from a USB Storage

This example illustrates how to update the ZyWALL/USG’s firmware automatically from a USB storage. With this feature, it is more efficient for users to upgrade the firmware for numerous devices without Internet or GUI access. The user can also downgrade the firmware by using this feature.

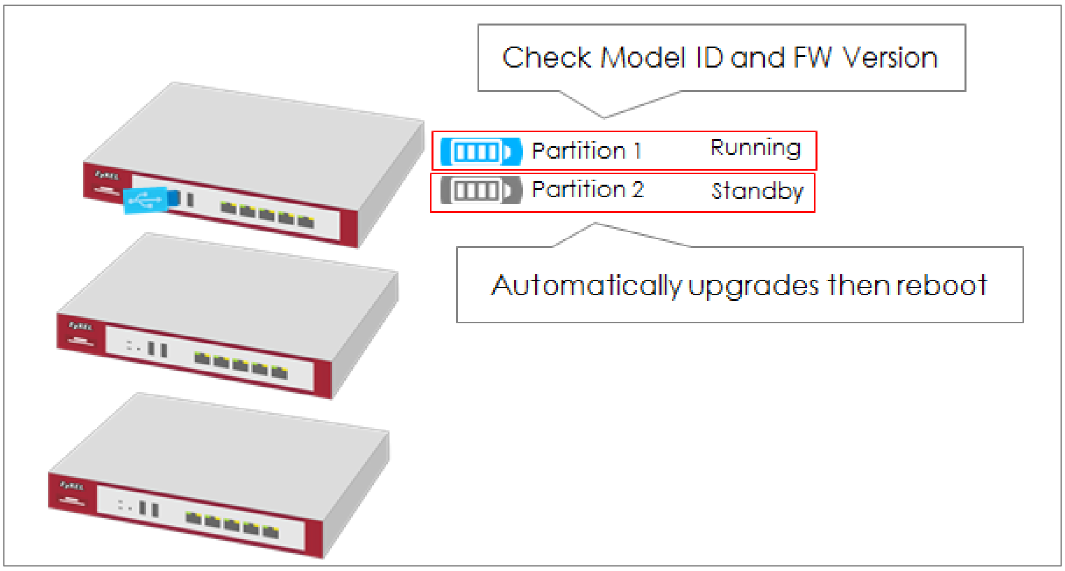

Check Model ID and FW Version
Partition 1
Running
Partition 2
Standby
Automatically upgrades then reboot

Figure 1 Automatic USB Firmware Upgrade

Note: This feature does not support Device HA Pro firmware auto upgrade to passive devices. Do not use USB firmware upgrade on the devices with Device HA Pro function activated. This example was tested using the USG210 (Firmware Version: ZLD 4.25).

2 Save the firmware on the USB.

3 Plug the USB into the device.

4 The device checks running partition for the model ID and the firmware version.

5 Upgrade the firmware to the standby partition and then the device reboots.

Enable the USB Firmware Upgrade Function by CLI Command

For security concerns, the function is disabled by default. The administrator needs to enable the function by the following CLI command:

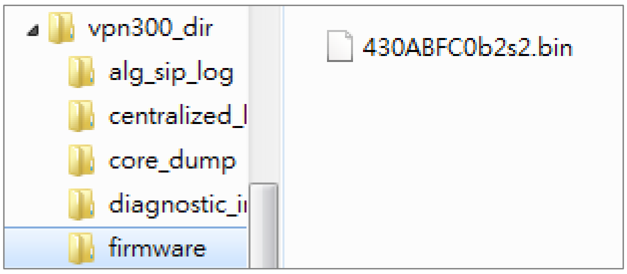
```
Router(config)# usb-storage update-firmware enable
```

Save the Firmware on the USB

There are two ways to create the firmware folder on the USB storage.

1 Follow the folder structure to create the firmware folder manually. It does not matter if the letters of the folder name are capitalized or not. For example: D:\vpn300_dir\firmware

Create the Firmware Folder Manually: Root Directory\vpn300_dir\firmware



2 Plug the USB storage to the device and the device will automatically create the folder **Vpn300_dir**, which includes the following sub-folders. Save the .bin file to the **firmware** folder.

centralized_log

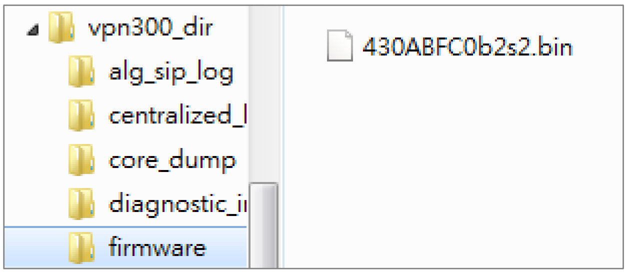
core_dump

diagnostic_info

firmware

packet_trace

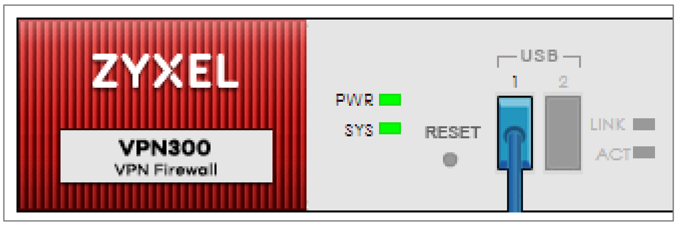
Firmware Folder is Created Automatically



Plug the USB into the Device

Once the .bin file in the firmware folder is detected, the device will copy it to the RAM.

Plug the USB storage into the USB port



The following message shows on the console if the device fails to copy the .bin file.

Router> USB update-firmware failed: firmware copy fail

The Device Checks Running Partition for the Model ID and the Firmware Version

The device checks the USB firmware with the running partition only. It does not check the standby partition.

1 Check model ID:

If incompatible, the device deletes the firmware in the RAM.

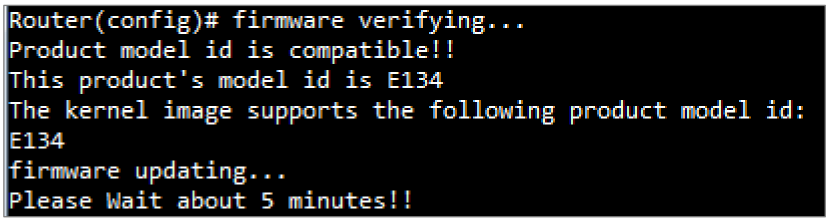
If compatible, the device checks the firmware version.

2 Check firmware version:

If it is the same as the running firmware, the device deletes the firmware in the RAM.

If it is not the same as the running version, the device starts to upgrade to the standby partition.

Check Model ID and Firmware Version

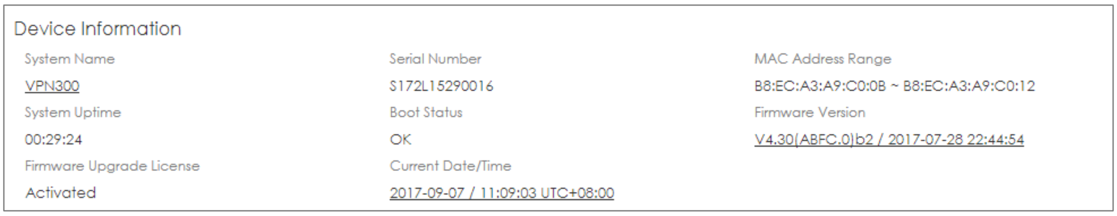


```
Router(config)# firmware verifying...
Product model id is compatible!!
This product's model id is E134
The kernel image supports the following product model id:
E134
firmware updating...
Please Wait about 5 minutes!!
```

Check Firmware Status

The device upgrades the standby partition and then reboots. After been upgraded to the standby partition, the device automatically reboots to switch from running to standby partition. The SYS LED starts to blink when the device begins to upgrade its firmware until the rebooting process is completed.

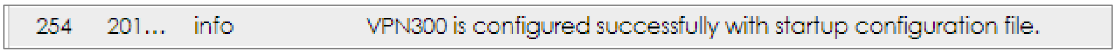
Check the Firmware Version on the Dashboard



Device Information

System Name	Serial Number	MAC Address Range
VPN300	S172L15290016	B8:EC:A3:A9:C0:0B ~ B8:EC:A3:A9:C0:12
System Uptime	Boot Status	Firmware Version
00:29:24	OK	V4.30(ABFC.0)b2 / 2017-07-28 22:44:54
Firmware Upgrade License	Current Date/Time	
Activated	2017-09-07 / 11:09:03 UTC+08:00	

MONITOR > Log > View log



```
254   201...   info          VPN300 is configured successfully with startup configuration file.
```

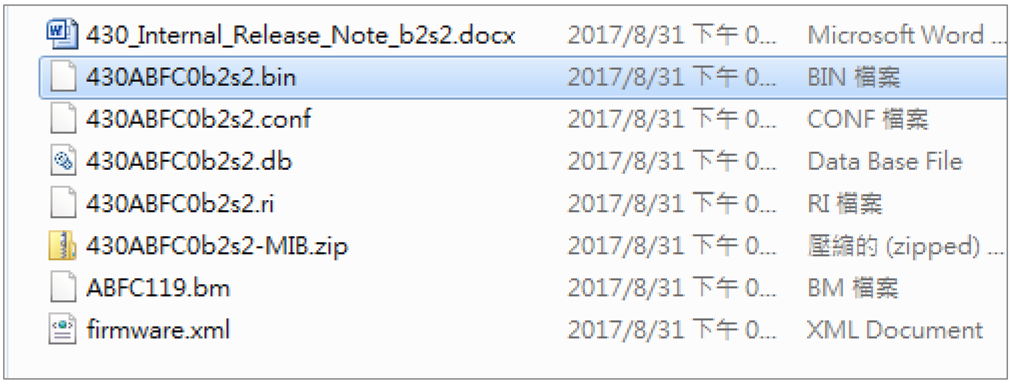
What Can Go Wrong?

1 The USB storage must use the FAT16, FAT32, EXT2, or EXT3 file system. Otherwise, it may not be detected by the ZyWALL/USG.

2 The device only checks the firmware under the specific folder. Therefore, make sure the firmware is saved in the correct folder under the root directory: **\ProductName_dir\firmware**. For example: \vpn300_dir\firmware

3 If there are multiple firmware files in the firmware folder of one model, the device only checks the first one in order.

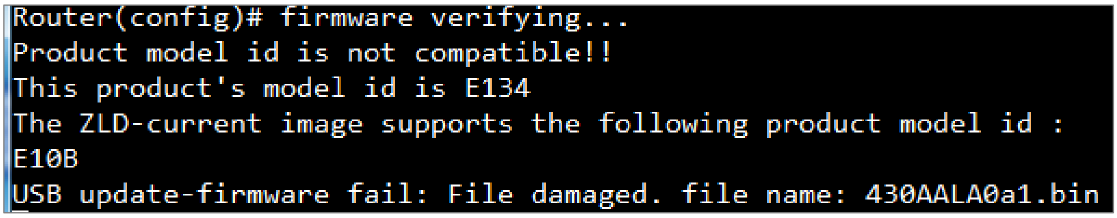
Multiple firmware files of one model in the same folder is not supported.



430_Internal_Release_Note_b2s2.docx	2017/8/31 下午 0...	Microsoft Word ...
430ABFC0b2s2.bin	2017/8/31 下午 0...	BIN 檔案
430ABFC0b2s2.conf	2017/8/31 下午 0...	CONF 檔案
430ABFC0b2s2.db	2017/8/31 下午 0...	Data Base File
430ABFC0b2s2.ri	2017/8/31 下午 0...	RI 檔案
430ABFC0b2s2-MIB.zip	2017/8/31 下午 0...	壓縮的 (zipped) ...
ABFC119.bm	2017/8/31 下午 0...	BM 檔案
firmware.xml	2017/8/31 下午 0...	XML Document

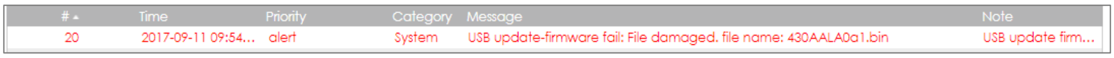
4 Make sure the product model ID of the USB firmware is compatible with the device. The device writes logs on the console and device log if the firmware model ID is incompatible.

Console Message



```
Router(config)# firmware verifying...
Product model id is not compatible!!
This product's model id is E134
The ZLD-current image supports the following product model id :
E10B
USB update-firmware fail: File damaged. file name: 430AALA0a1.bin
```

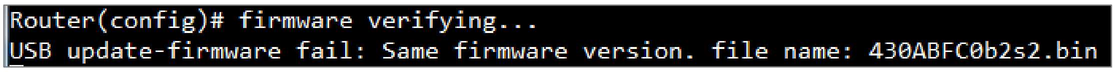
MONITOR > Log > View log



# ▲	Time	Priority	Category	Message	Note
20	2017-09-11 09:54...	alert	System	USB update-firmware fail: File damaged. file name: 430AALA0a1.bin	USB update firm...

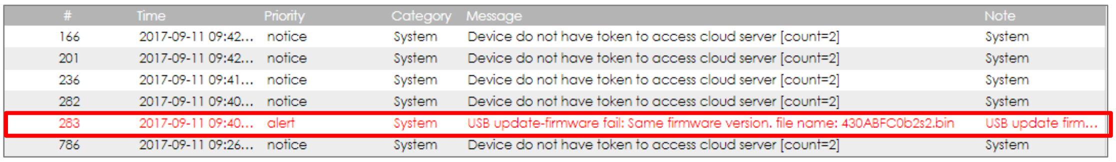
5 Make sure the version of the USB firmware is different from that of the running partition. The device writes logs on the console and device log if the firmware version is the same as the running firmware.

Console Message



```
Router(config)# firmware verifying...
USB update-firmware fail: Same firmware version. file name: 430ABFC0b2s2.bin
```

MONITOR > Log > View log



#	Time	Priority	Category	Message	Note
166	2017-09-11 09:42...	notice	System	Device do not have token to access cloud server [count=2]	System
201	2017-09-11 09:42...	notice	System	Device do not have token to access cloud server [count=2]	System
236	2017-09-11 09:41...	notice	System	Device do not have token to access cloud server [count=2]	System
282	2017-09-11 09:40...	notice	System	Device do not have token to access cloud server [count=2]	System
283	2017-09-11 09:40...	alert	System	USB update-firmware fail: Same firmware version. file name: 430ABFC0b2s2.bin	USB update firm...
786	2017-09-11 09:26...	notice	System	Device do not have token to access cloud server [count=2]	System

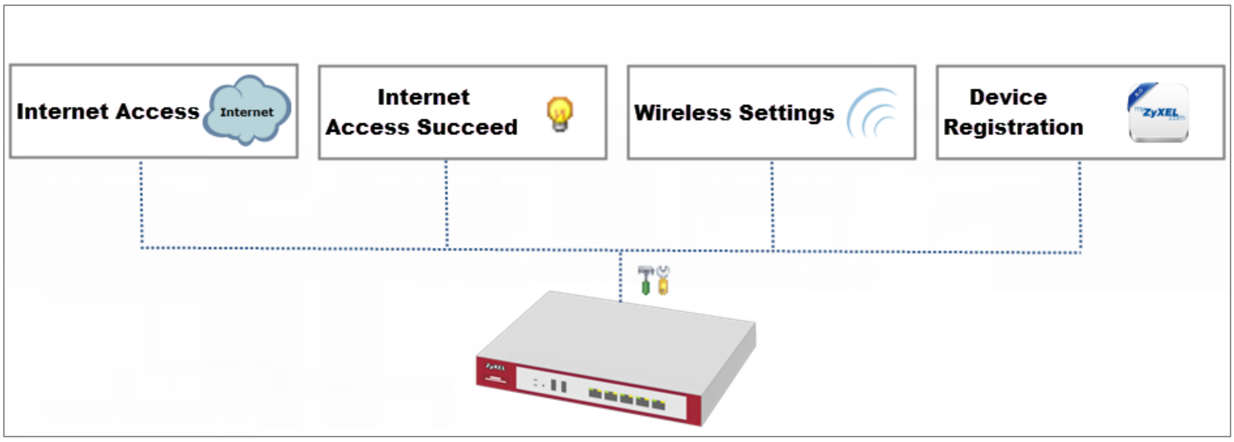
6 This feature does not support the Device HA Pro firmware auto upgrade to passive devices. Do not use USB firmware upgrade on devices with Device HA Pro function activated. When using USB firmware upgrade on a device HA or in a device HA Pro scenario, make sure you plug the USB storage to the passive device for firmware upgrade first. After the passive device has finished firmware upgrading through the USB, plug the USB storage to the active device for firmware upgrade.

Chapter 8- Others

How to Get Started Using the Wizards

When you log into the Web Configurator for the first time or when you reset the ZyWALL/USG to its default configuration, the **Installation Setup Wizard** screen displays. This is an example of using ZyWALL/USG Wizards to configure Internet connection settings, wireless settings and device registration services.

ZyWALL/USG with Installation Setup Wizard Example

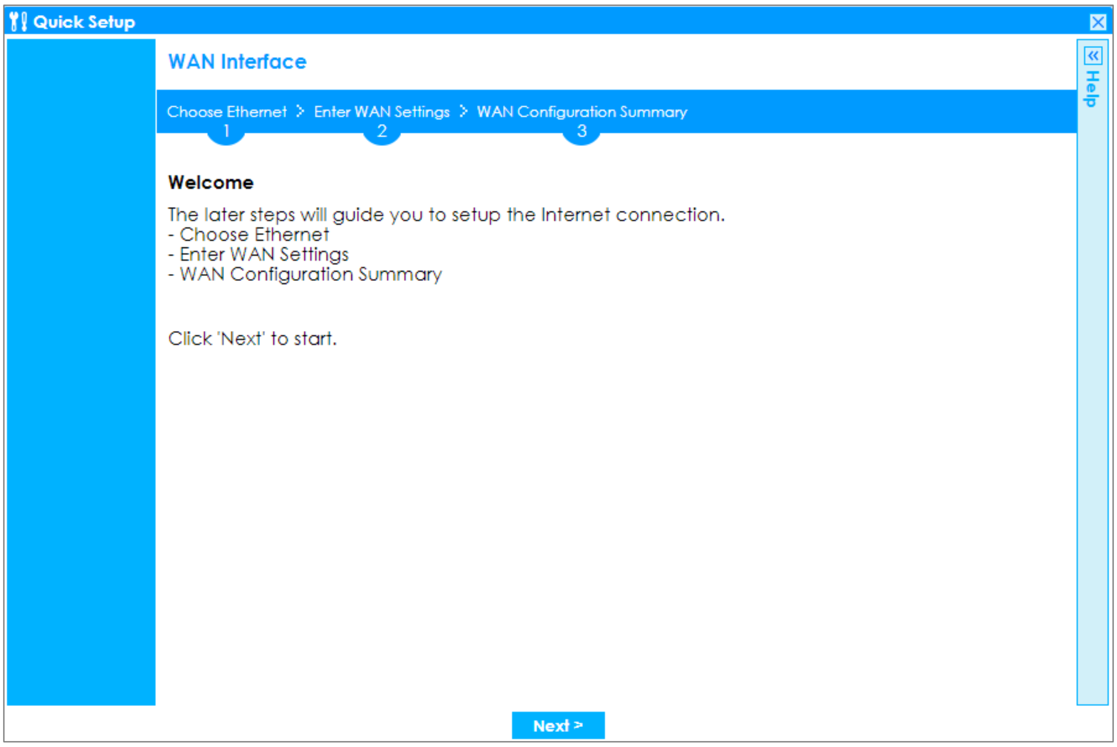


Note: You need internet access to activate your ZyWALL/USG subscription services. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Internet Access (Ethernet) Wizard on the ZyWALL/USG

In the ZyWALL/USG **Installation Setup Wizard** Welcome page, click **Next** to start configuring. Click the double arrow in the upper right corner to display («) or hide (») the help.

Installation Setup Wizard > Welcome


Quick Setup
WAN Interface
Choose Ethernet 1 > Enter WAN Settings 2 > WAN Configuration Summary 3
Help
Next >

Welcome

The later steps will guide you to setup the Internet connection.
- Choose Ethernet
- Enter WAN Settings
- WAN Configuration Summary

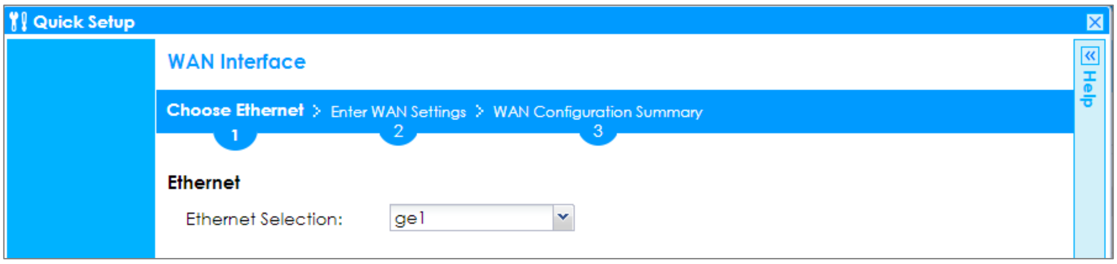
Click 'Next' to start.

In the **Internet Access** page, you can configure Internet connections from two Internet service providers (ISPs). Connect your ISP devices to your ZyWALL/USG WAN port, select **I have two ISPs** if you want to configure two Internet connections or leave it cleared to configure just one.

Choose the **Encapsulation** option to be **Ethernet**, leave **Zone** as default setting Internet connection belongs to the WAN zone.

In the **IP Address Assignment** section, select **Auto** if your ISP did not assign you a fixed IP address or select **Static** if your ISP did assign you a fixed IP address. Click **Next**.

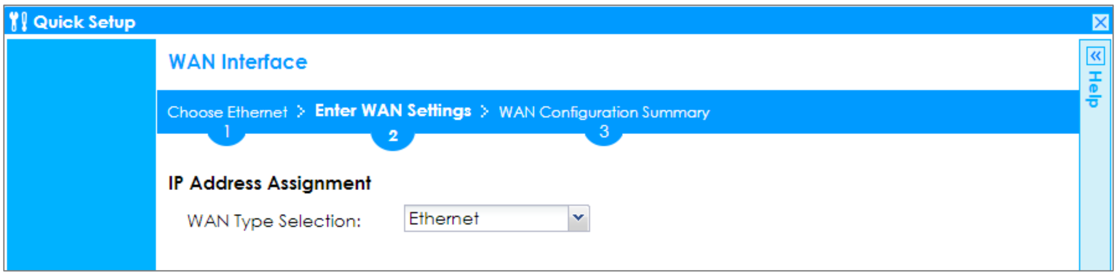
Installation Setup Wizard > Welcome > Internet Access


Quick Setup
Help
Choose Ethernet 1 > Enter WAN Settings 2 > WAN Configuration Summary 3

WAN Interface

Ethernet

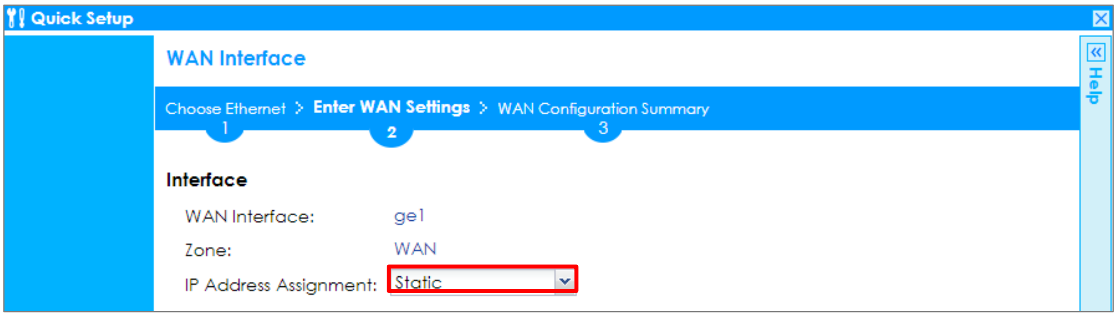
Ethernet Selection: ge1


Quick Setup
Help
Choose Ethernet 1 > Enter WAN Settings 2 > WAN Configuration Summary 3

WAN Interface

IP Address Assignment

WAN Type Selection: Ethernet


Quick Setup
Help
Choose Ethernet 1 > Enter WAN Settings 2 > WAN Configuration Summary 3

WAN Interface

Interface

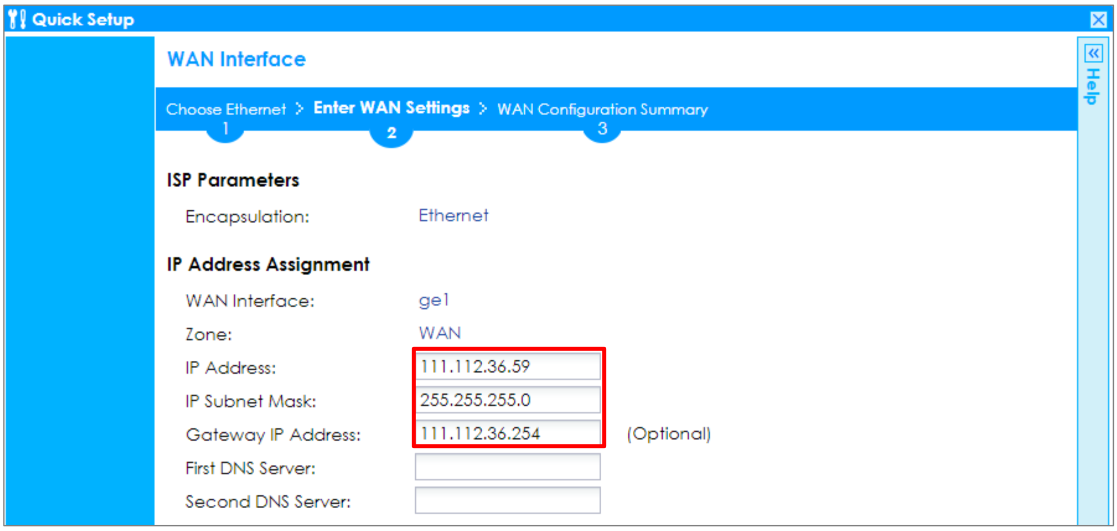
WAN Interface: ge1

Zone: WAN

IP Address Assignment: Static

Enter the **IP Address**, **IP Subnet Mask** and **Gateway IP Address** exactly as given by your ISP or network administrator. First/Second DNS Servers are optional. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access


Quick Setup
Help
Choose Ethernet 1 > Enter WAN Settings 2 > WAN Configuration Summary 3

WAN Interface

ISP Parameters

Encapsulation: Ethernet

IP Address Assignment

WAN Interface: ge1

Zone: WAN

IP Address: 111.112.36.59

IP Subnet Mask: 255.255.255.0

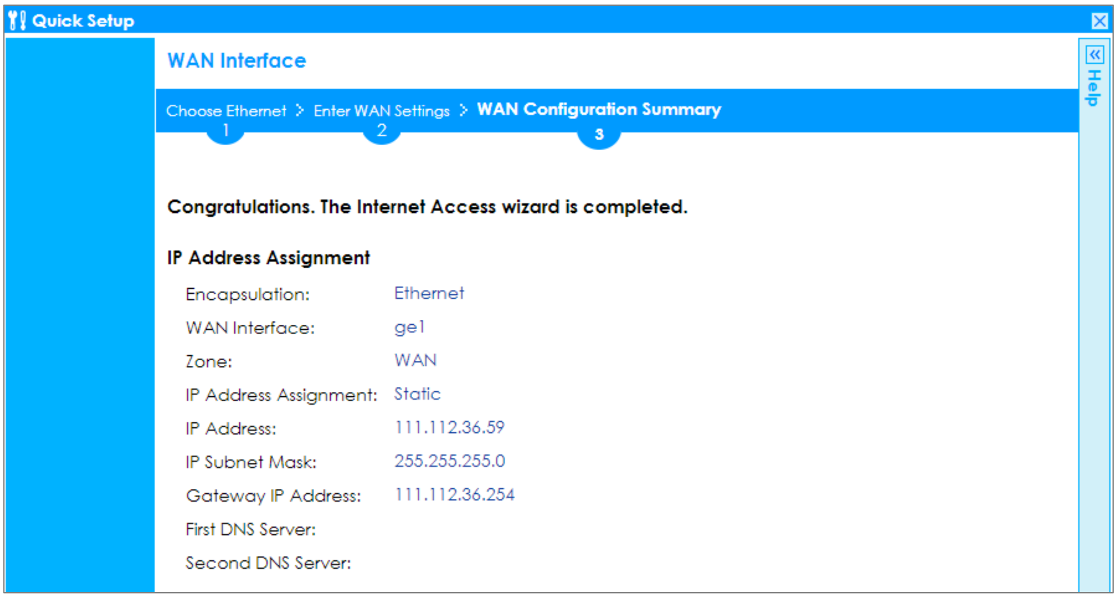
Gateway IP Address: 111.112.36.254 (Optional)

First DNS Server:

Second DNS Server:

The **Internet Access Succeed** page will display the summary of Internet access of the **First Setting**. If you select **I have two ISPs** in **Internet Access > ISP Setting**, click **Next** to configure the second WAN interface or continue to the **Wireless Settings** page.

Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed


Quick Setup
Help
Choose Ethernet 1 > Enter WAN Settings 2 > WAN Configuration Summary 3

WAN Interface

Congratulations. The Internet Access wizard is completed.

IP Address Assignment

Encapsulation: Ethernet

WAN Interface: ge1

Zone: WAN

IP Address Assignment: Static

IP Address: 111.112.36.59

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 111.112.36.254

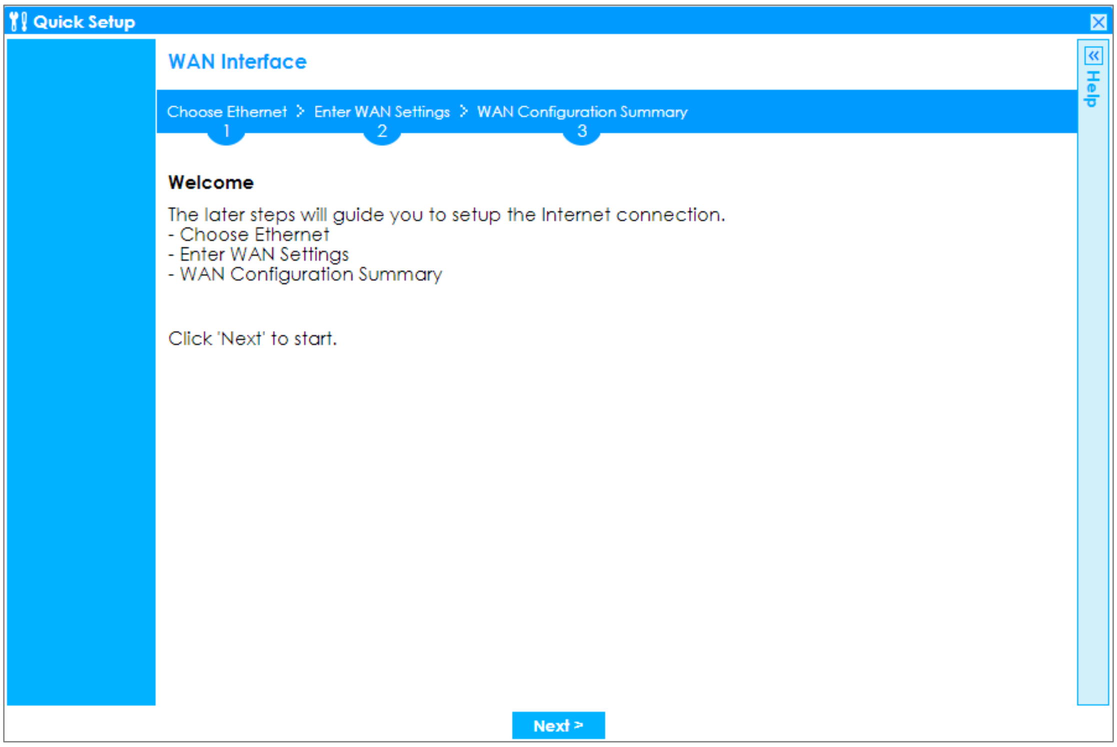
First DNS Server:

Second DNS Server:

Set Up the Internet Access (PPPoE) Wizard on the ZyWALL/USG

In the ZyWALL/USG **Installation Setup Wizard** Welcome page, click **Next** to start configuring for Internet. Click the double arrow in the upper right corner to display (≪) or hide (≫) the help.

Installation Setup Wizard > Welcome



WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary
1 2 3

Welcome

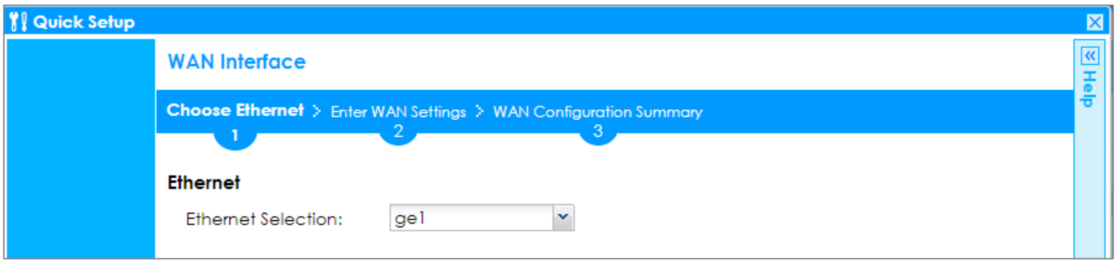
The later steps will guide you to setup the Internet connection.
- Choose Ethernet
- Enter WAN Settings
- WAN Configuration Summary

Click 'Next' to start.

In the **Internet Access** page, you can configure Internet connections from two Internet service providers (ISPs). Connect your ISP devices to your ZyWALL/USG WAN port, select **I have two ISPs** if you want to configure two Internet connections or leave it cleared to configure just one.

Choose the **Encapsulation** option to be **PPP over Ethernet**, leave **Zone** as default setting Internet connection belongs to the WAN zone. Leave the **IP Address Assignment** section to be the **Auto** and click **Next**.

Installation Setup Wizard > Welcome > Internet Access



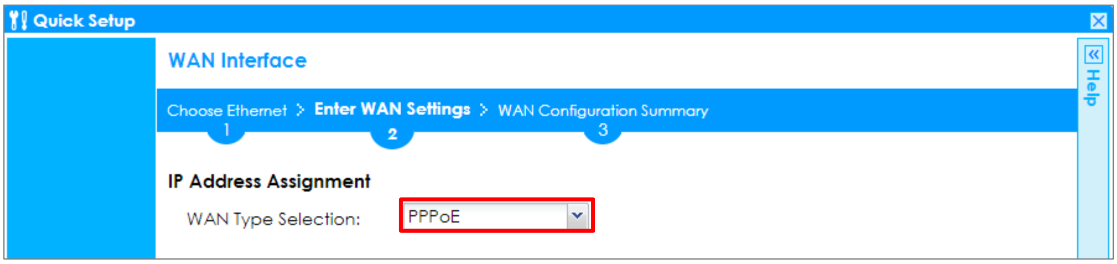
Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary
1 2 3

Ethernet

Ethernet Selection: ge1



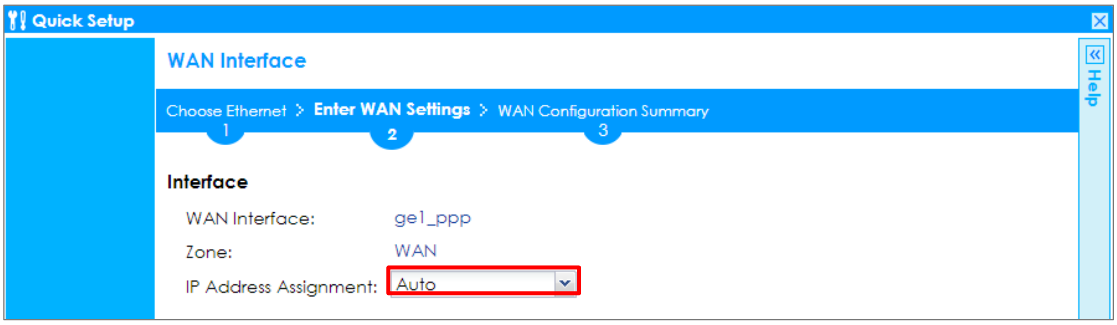
Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary
1 2 3

IP Address Assignment

WAN Type Selection: PPPoE



Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary
1 2 3

Interface

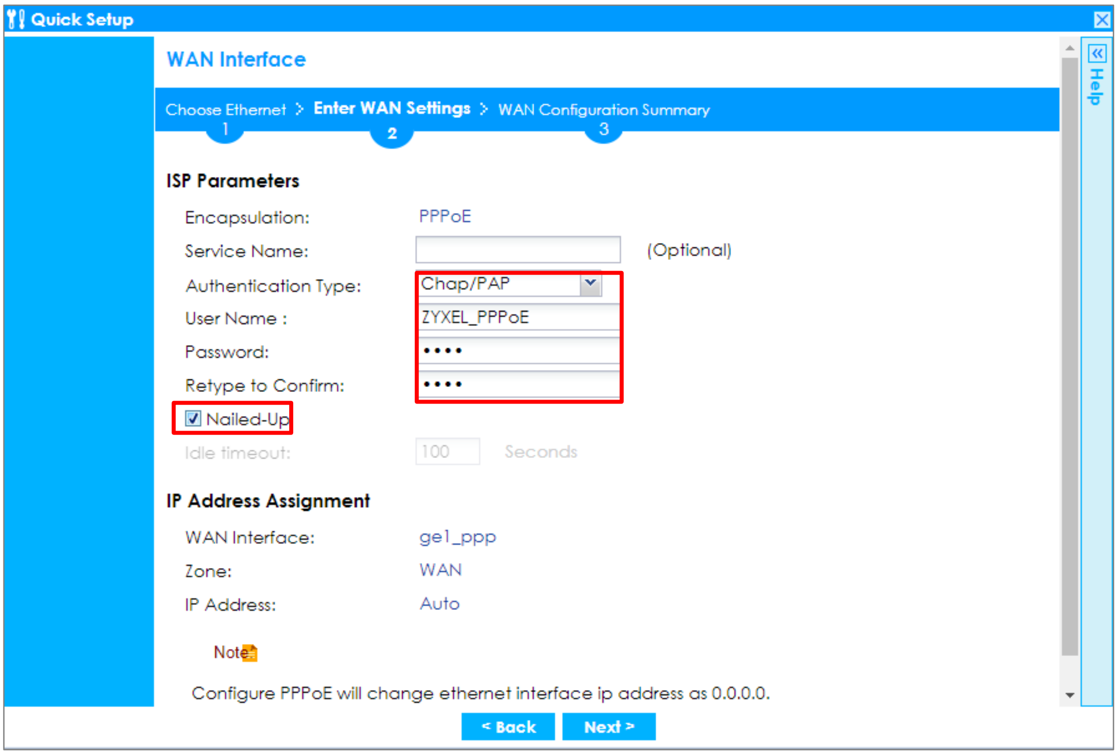
WAN Interface: ge1_ppp

Zone: WAN

IP Address Assignment: Auto

Select the **Authentication Type** to be the authentication method by the remote node. Enter the **User Name** and **Password** exactly as given by your ISP or network administrator. Select **Nailed-UP** if you want to keep the connection always up or type the desired **Idle Timeout** value in seconds. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access



WAN Interface

Choose Ethernet 1 > Enter WAN Settings 2 > WAN Configuration Summary 3

ISP Parameters

Encapsulation: PPPoE

Service Name: (Optional)

Authentication Type: Chap/PAP

User Name : ZYXEL_PPPoE

Password: ••••

Retype to Confirm: ••••

☑ Nailed-Up

Idle timeout: 100 Seconds

IP Address Assignment

WAN Interface: ge1_ppp

Zone: WAN

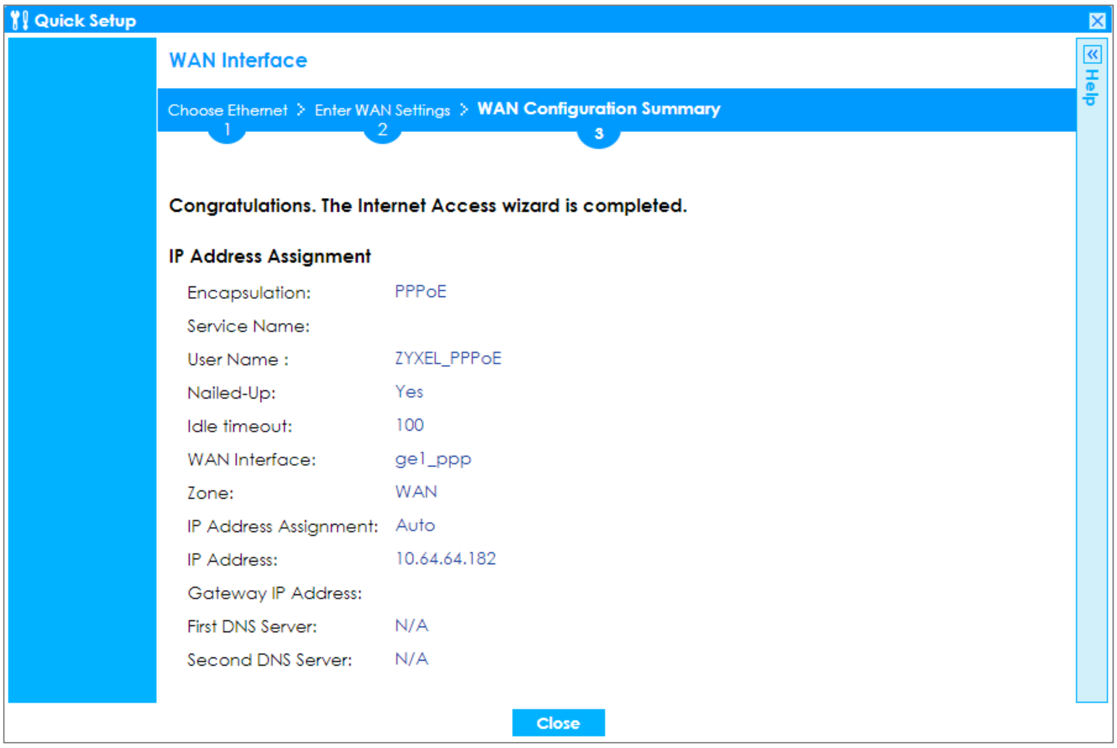
IP Address: Auto

Note

Configure PPPoE will change ethernet interface ip address as 0.0.0.0.

The **Internet Access Succeed** page will display the summary of Internet access of the **First Setting**. If you select **I have two ISPs** in **Internet Access > ISP Setting**, click **Next** to configure the second WAN interface.

Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed


Quick Setup
WAN Interface
Choose Ethernet 1 > Enter WAN Settings 2 > WAN Configuration Summary 3
Help
Close

Congratulations. The Internet Access wizard is completed.

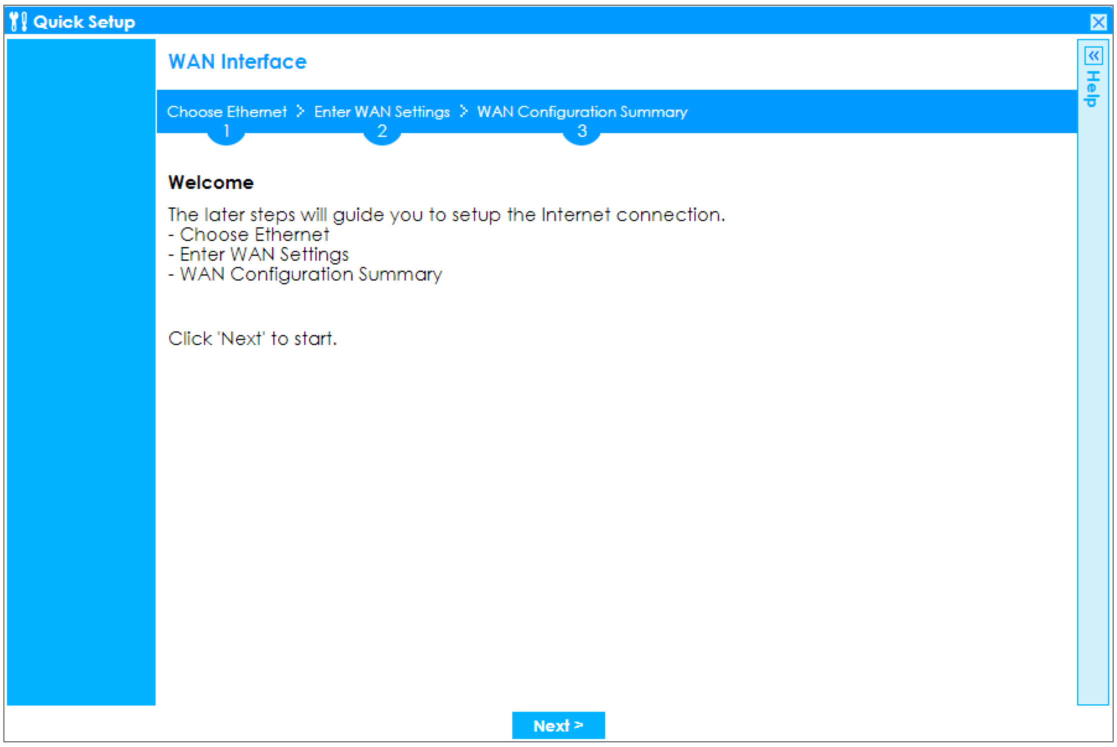
IP Address Assignment

Encapsulation:	PPPoE
Service Name:	
User Name :	ZYXEL_PPPoE
Nailed-Up:	Yes
Idle timeout:	100
WAN Interface:	ge1_ppp
Zone:	WAN
IP Address Assignment:	Auto
IP Address:	10.64.64.182
Gateway IP Address:	
First DNS Server:	N/A
Second DNS Server:	N/A

Set Up the Internet Access (PPTP) Wizard on the ZyWALL/USG

In the ZyWALL/USG **Installation Setup Wizard** Welcome page, click **Next** to start configuring for Internet. Click the double arrow in the upper right corner to display (≪) or hide (≫) the help.

Installation Setup Wizard > Welcome



WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary
1 2 3

Welcome

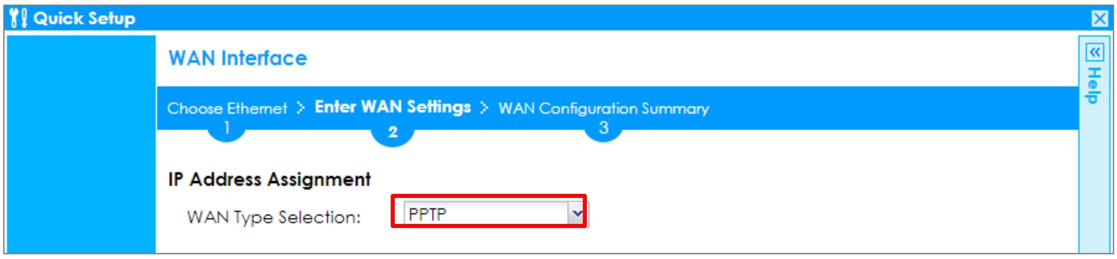
The later steps will guide you to setup the Internet connection.
- Choose Ethernet
- Enter WAN Settings
- WAN Configuration Summary

Click 'Next' to start.

In the **Internet Access** page, you can configure Internet connections from two Internet service providers (ISPs). Connect your ISP devices to your ZyWALL/USG WAN port, select **I have two ISPs** if you want to configure two Internet connections or leave it cleared to configure just one.

Choose the **Encapsulation** option to be the **PPTP**, leave **Zone** as default setting Internet connection belongs to the WAN zone. Leave the **IP Address Assignment** section to be the **Auto** and click **Next**.

Installation Setup Wizard > Welcome > Internet Access



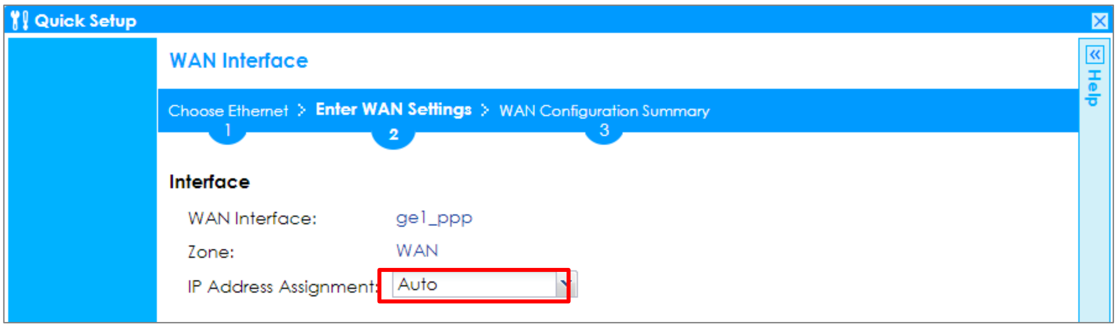
Quick Setup

WAN Interface

Choose Ethernet 1 > Enter WAN Settings 2 > WAN Configuration Summary 3

IP Address Assignment

WAN Type Selection: PPTP



Quick Setup

WAN Interface

Choose Ethernet 1 > Enter WAN Settings 2 > WAN Configuration Summary 3

Interface

WAN Interface: ge1_ppp

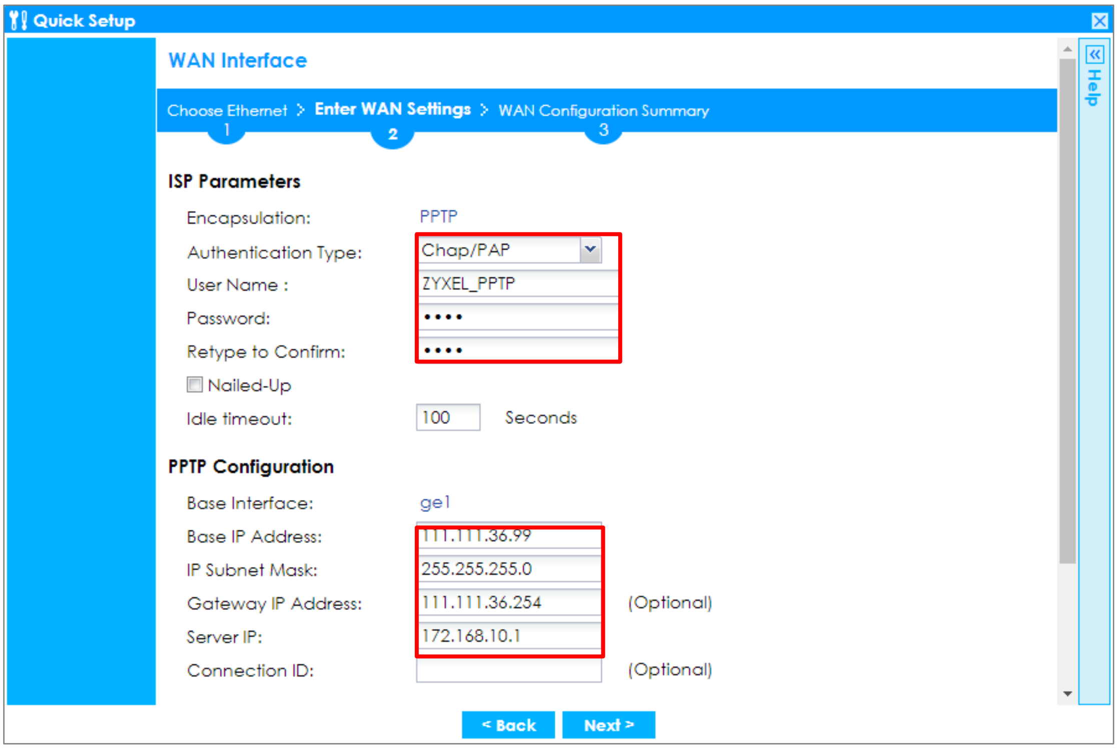
Zone: WAN

IP Address Assignment: Auto

Select the **Authentication Type** to be the authentication method by the remote node. Enter the **User Name** and **Password** exactly as given by your ISP or network administrator. Select **Nailed-UP** if you want to keep the connection always up or type the desired **Idle Timeout** value in seconds. Click **Next**.

Enter the **Base IP Address**, **IP Subnet Mask**, **Gateway IP Address** assigned to you by your ISP. Type the **Server IP** address of the **PPTP Server**. Click **Next.**

Installation Setup Wizard > Welcome > Internet Access


Quick Setup
WAN Interface
Choose Ethernet 1 > Enter WAN Settings 2 > WAN Configuration Summary 3
Help
< Back
Next >

ISP Parameters

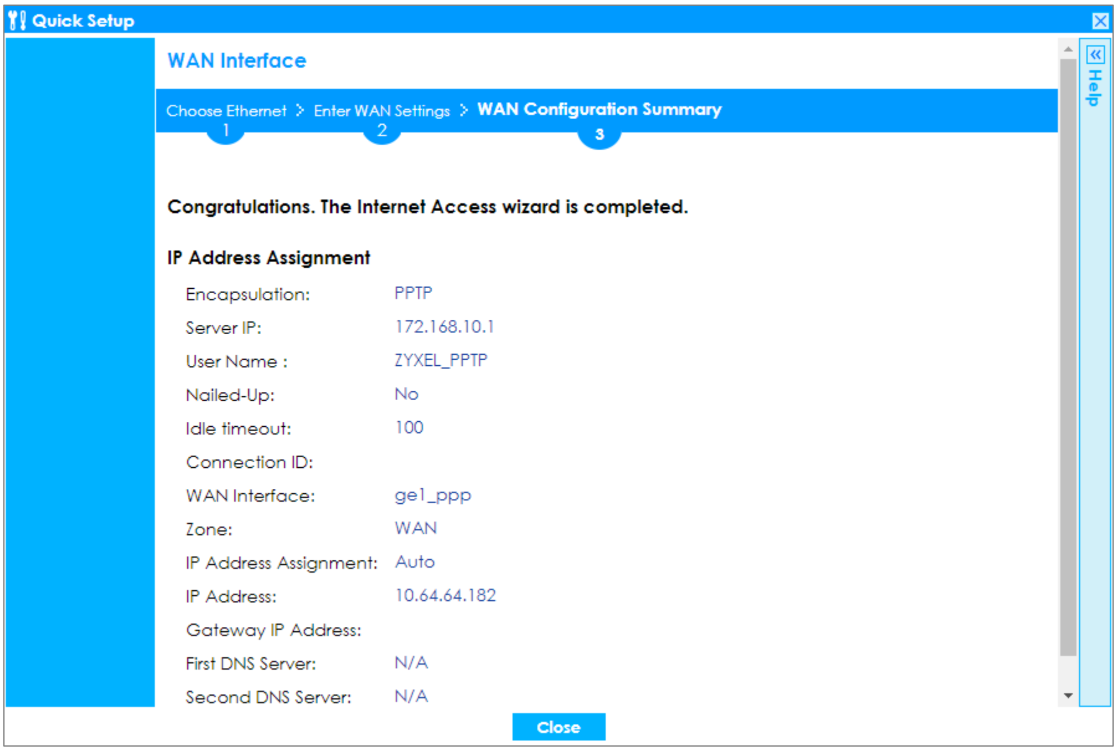
Encapsulation:	PPTP
Authentication Type:	Chap/PAP
User Name :	ZYXEL_PPTP
Password:	••••
Retype to Confirm:	••••
□ Nailed-Up	
Idle timeout:	100 Seconds

PPTP Configuration

Base Interface:	ge1
Base IP Address:	111.111.36.99
IP Subnet Mask:	255.255.255.0
Gateway IP Address:	111.111.36.254 (Optional)
Server IP:	172.168.10.1
Connection ID:	(Optional)

The **Internet Access Succeed** page will display the summary of Internet access of the **First Setting**. If you select **I have two ISPs** in **Internet Access > ISP Setting**, click **Next** to configure the second WAN interface.

Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed



WAN Interface

Congratulations. The Internet Access wizard is completed.

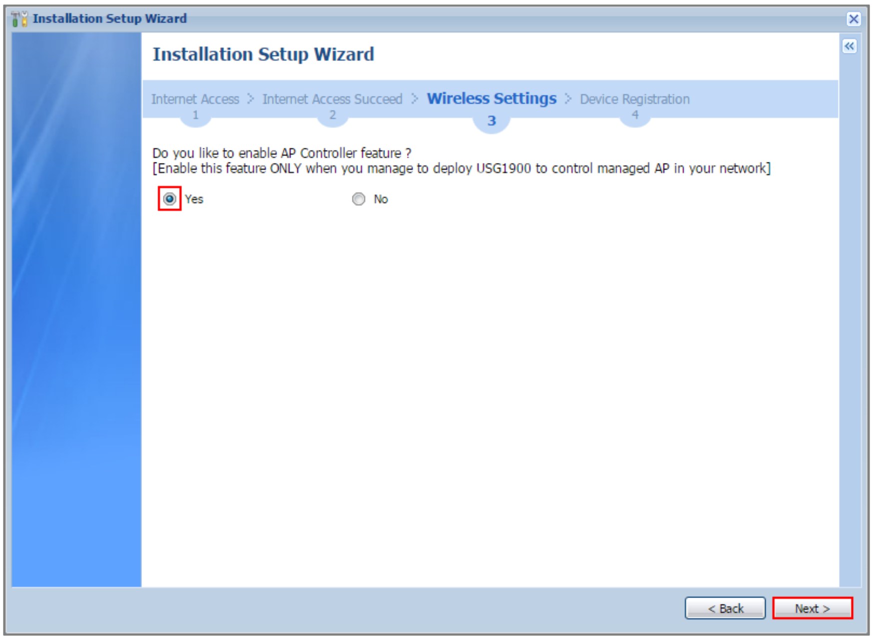
IP Address Assignment

Encapsulation:	PPTP
Server IP:	172.168.10.1
User Name :	ZYXEL_PPTP
Nailed-Up:	No
Idle timeout:	100
Connection ID:	
WAN Interface:	ge1_ppp
Zone:	WAN
IP Address Assignment:	Auto
IP Address:	10.64.64.182
Gateway IP Address:	
First DNS Server:	N/A
Second DNS Server:	N/A

Set Up the Wireless Settings Wizard on the ZyWALL/USG

In the **Wireless Settings** page, select **Yes** if you want the ZyWALL/USG to enable AP Controller feature in your network; select **No** if you want to skip this setting. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed > Wireless Settings



Installation Setup Wizard

Internet Access > Internet Access Succeed > Wireless Settings > Device Registration

Do you like to enable AP Controller feature ?
[Enable this feature ONLY when you manage to deploy USG1900 to control managed AP in your network]

● Yes ○ No

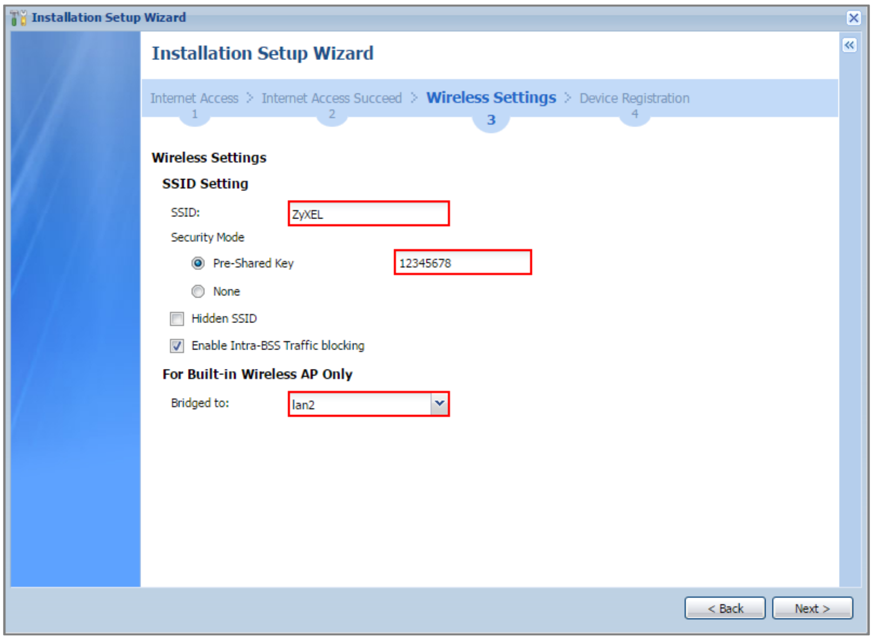
Configure descriptive **SSID** name (1-32 characters) for the wireless LAN. Select **Pre-Shared Key** (8-63 characters) to add security on this wireless network. Otherwise, select **None** to allow any wireless client to associate this network without authentication.

Select **Hidden SSID** to hide the SSID from site tool scanning.

Select **Enable Intra-BSS Traffic blocking** if you want to prevent crossover traffic from within the same wireless network. Wireless clients in that network can still access the wired network but cannot communicate with each other.

For Built-in Wireless AP only, ZyWALL/USGs with **W** in the model name have a built-in AP. Select an interface to bridge with the built-in AP wireless network. Devices connected to this interface will then be in the same broadcast domain as devices in the AP wireless network.

Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed > Wireless Settings



Installation Setup Wizard

Wireless Settings

SSID Setting

SSID: ZyXEL

Security Mode

● Pre-Shared Key 12345678

○ None

□ Hidden SSID

☑ Enable Intra-BSS Traffic blocking

For Built-in Wireless AP Only

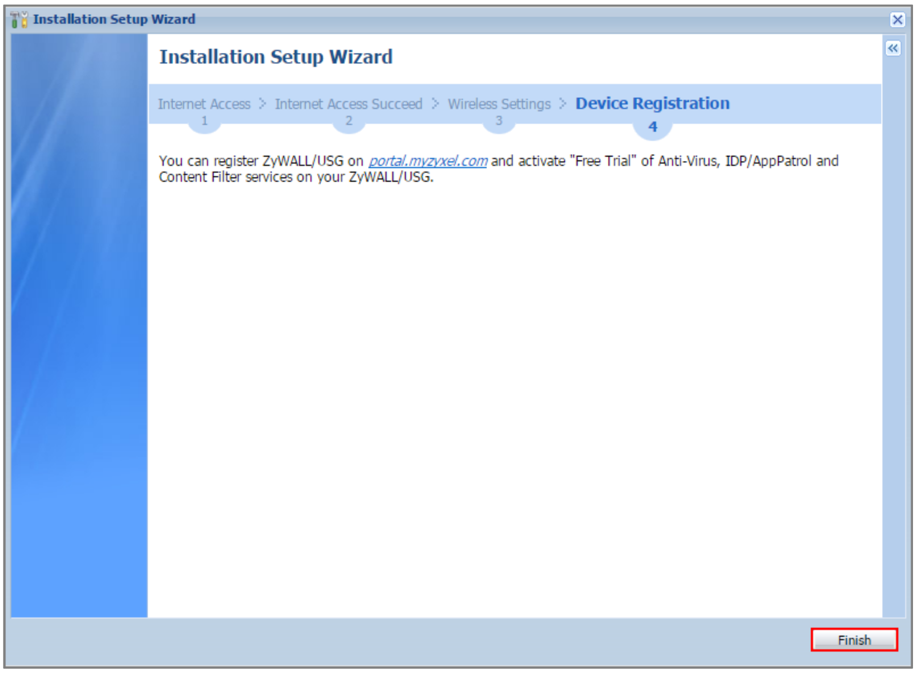
Bridged to: lan2

Set Up the Device Registration on the ZyWALL/USG

The ZyWALL/USG must be connected to the Internet in order to register.

Click **portal.myzyxel.com** to register the device, you need the ZyWALL/USG's serial number and LAN MAC address to register it. See **How To Register Your Device and Services at myZyXEL.com** for more details. Use the **Configuration > Licensing > Registration > Service** screen to update your service subscription status. Click **Finish**.

Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed > Wireless Settings > Device Registration



Installation Setup Wizard
Installation Setup Wizard
Internet Access 1
Internet Access Succeed 2
Wireless Settings 3
Device Registration 4
Finish

You can register ZyWALL/USG on portal.myzyxel.com and activate "Free Trial" of Anti-Virus, IDP/AppPatrol and Content Filter services on your ZyWALL/USG.

How to Restrict Web Portal access from the Internet

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with multiple LAN access to the VPN tunnel. The example instructs how to configure the VPN tunnel between each site and redirect multiple LAN interface traffic to the VPN tunnel. When the VPN tunnel is configured, multiple LAN subnets can be accessed securely.

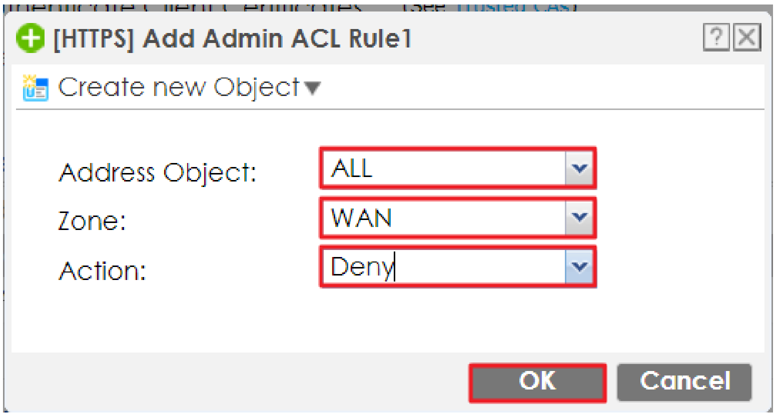
ZyWALL/USG Restrict Web Portal Access from the Internet

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG60 (Firmware Version: ZLD 4.25).

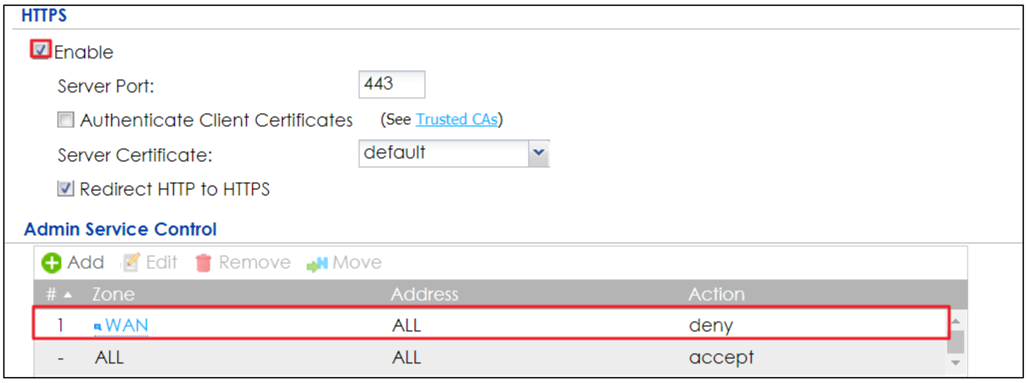
Set Up the ZyWALL/USG System Setting

Go to **CONFIGURATION > System > WWW > Admin Service Control > Add Admin ACL Rule 1.** Set the address access action as **Deny** for **ALL** address in **WAN**.

CONFIGURATION > System > WWW > Admin Service Control > Add Admin ACL Rule 1



Address Object: ALL
Zone: WAN
Action: Deny



HTTPS

☑ Enable

Server Port: 443

☐ Authenticate Client Certificates (See Trusted CAs)

Server Certificate: default

☑ Redirect HTTP to HTTPS

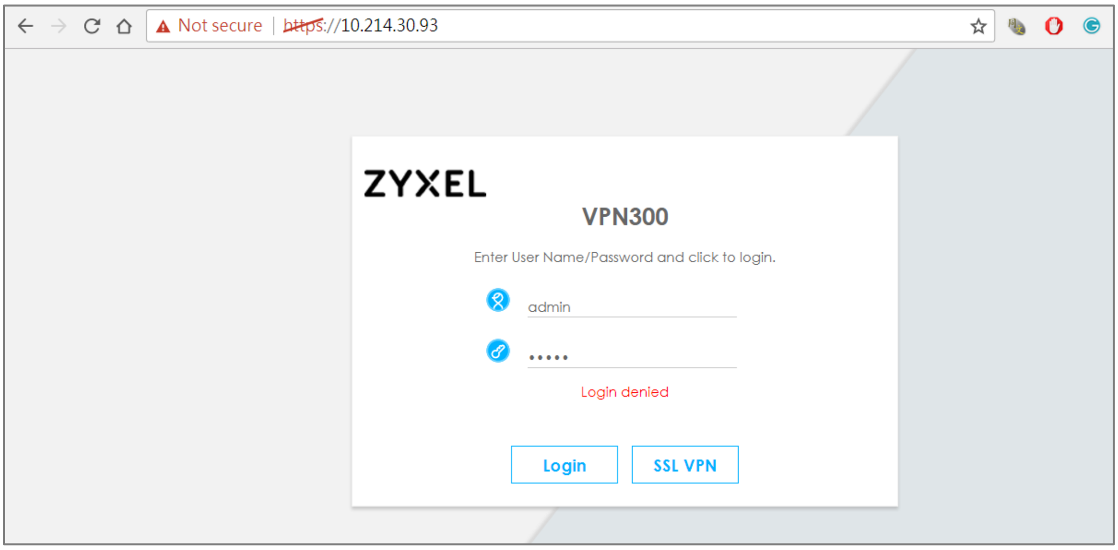
Admin Service Control

#	Zone	Address	Action
1	WAN	ALL	deny
-	ALL	ALL	accept

Test the Web Access

Login to the device via the WAN interface with the administrator's user name and password. The screen will show **Login denied**.

Login to the device via the WAN interface



Not secure | ~~https~~://10.214.30.93

ZYXEL

VPN300

Enter User Name/Password and click to login.

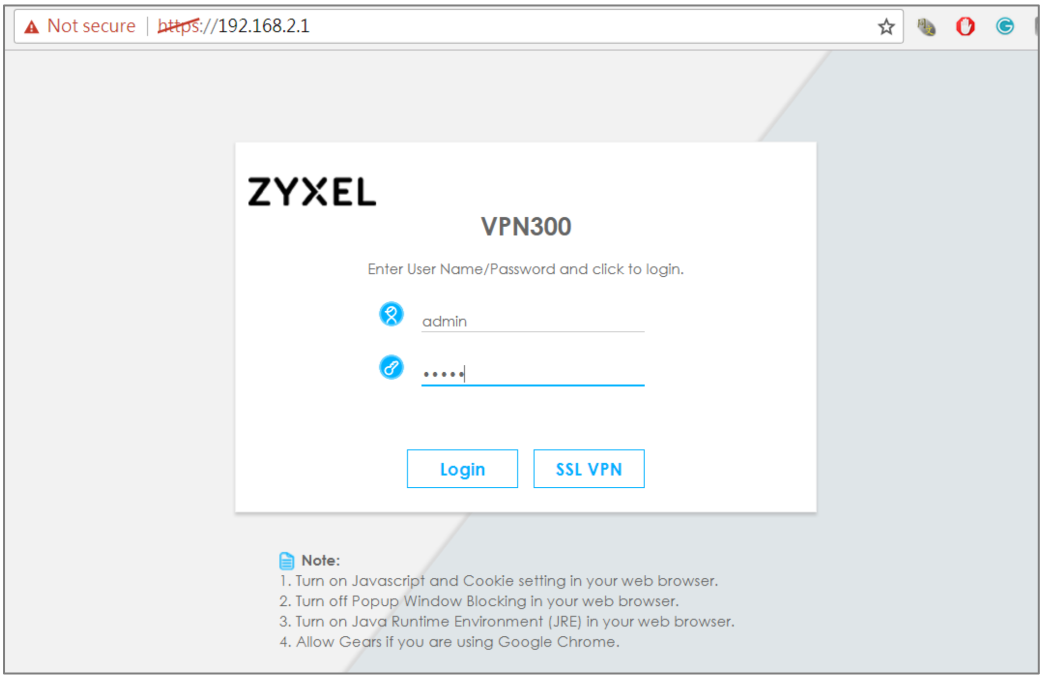
admin

•••••

Login denied

Login to the device via the LAN interface with the administrator's user name and password. The management portal will be displayed.

Login to the device via the LAN interface



Not secure | ~~https~~://192.168.2.1

ZYXEL

VPN300

Enter User Name/Password and click to login.

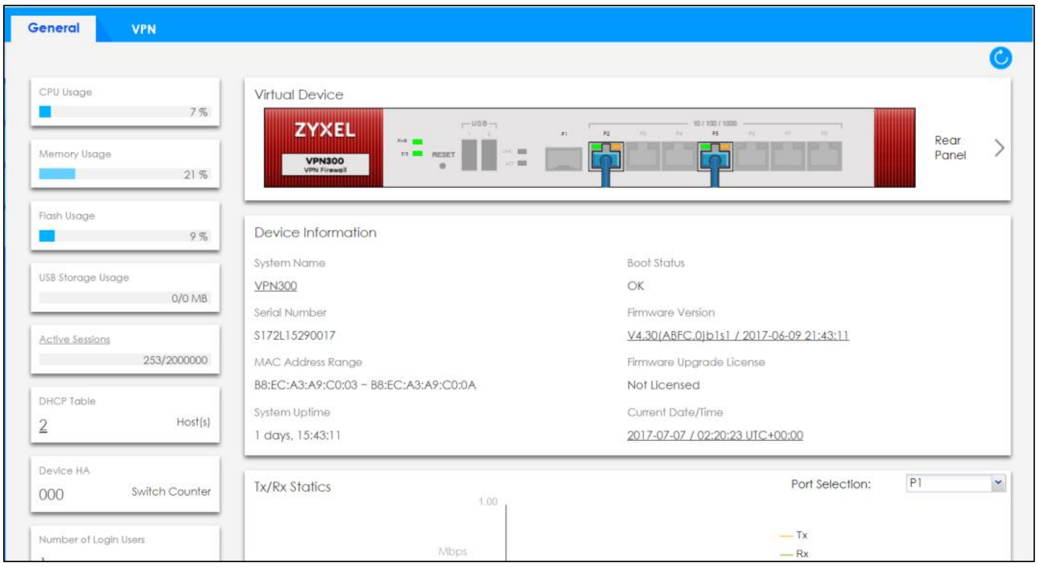
admin

•••••

Login SSL VPN

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.



CPU Usage 7 %

Memory Usage 21 %

Flash Usage 9 %

USB Storage Usage 0/0 MB

Active Sessions 253/2000000

DHCP Table 2 Host(s)

Device HA 000 Switch Counter

Number of Login Users

Virtual Device

Device Information

System Name: VPN300

Boot Status: OK

Serial Number: S172L15290017

Firmware Version: V4.30(ABFC.0)b1s1 / 2017-06-09 21:43:11

MAC Address Range: B8:EC:A3:A9:C0:03 ~ B8:EC:A3:A9:C0:0A

Firmware Upgrade License: Not Licensed

System Uptime: 1 days, 15:43:11

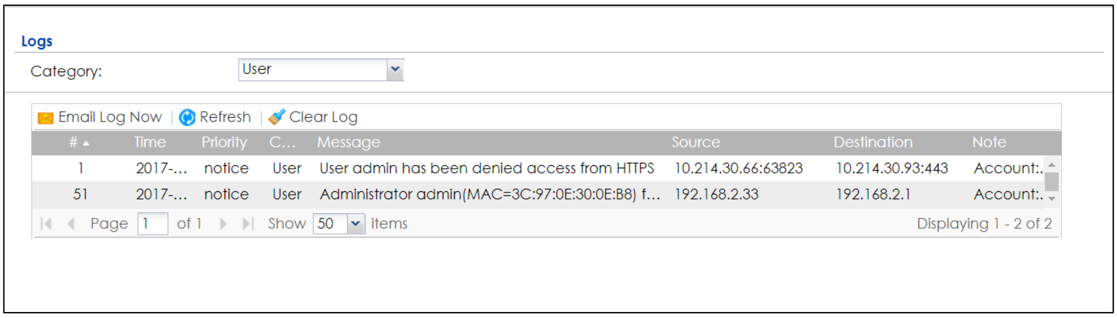
Current Date/Time: 2017-07-07 / 02:20:23 UTC+00:00

Tx/Rx Statics

Port Selection: P1

Go to **MONITOR > Log**. You can see that the admin login has been denied access from the WAN interface but it is allowed from the LAN interface.

MONITOR > Log



Logs

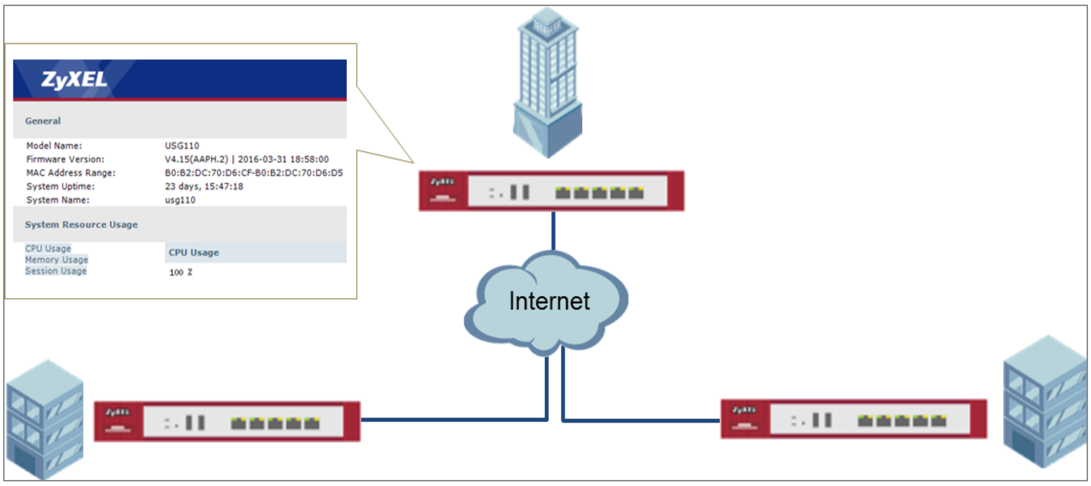
Category: User

# ▲	Time	Priority	C...	Message	Source	Destination	Note
1	2017-...	notice	User	User admin has been denied access from HTTPS	10.214.30.66:63823	10.214.30.93:443	Account:..
51	2017-...	notice	User	Administrator admin(MAC=3C:97:0E:30:0E:B8) f...	192.168.2.33	192.168.2.1	Account:..

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

How to Setup and Configure Daily Report

This example shows how to set up the data collection and view various statistics about traffic passing through your ZyWALL/USG. When the Daily Report is configured, you will receive statistics report every day.



General

Model Name: USG110
Firmware Version: V4.15(AAPH.2) | 2016-03-31 18:58:00
MAC Address Range: B0:B2:DC:70:D6:CF-B0:B2:DC:70:D6:D5
System Uptime: 23 days, 15:47:18
System Name: usg110

System Resource Usage

CPU Usage
Memory Usage
Session Usage

CPU Usage
100 %

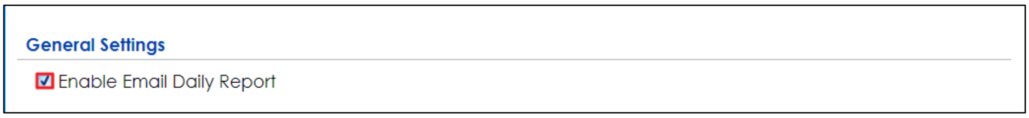
ZyWALL/USG Setup and Configure Daily Report

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the ZyWALL/USG Email Daily Report Setting

Go to **CONFIGURATION > Log & Report > Email Daily Report > General Settings.** Select **Enable Email Daily Report** to send reports by e-mail every day.

CONFIGURATION > Log & Report > Email Daily Report > General Settings

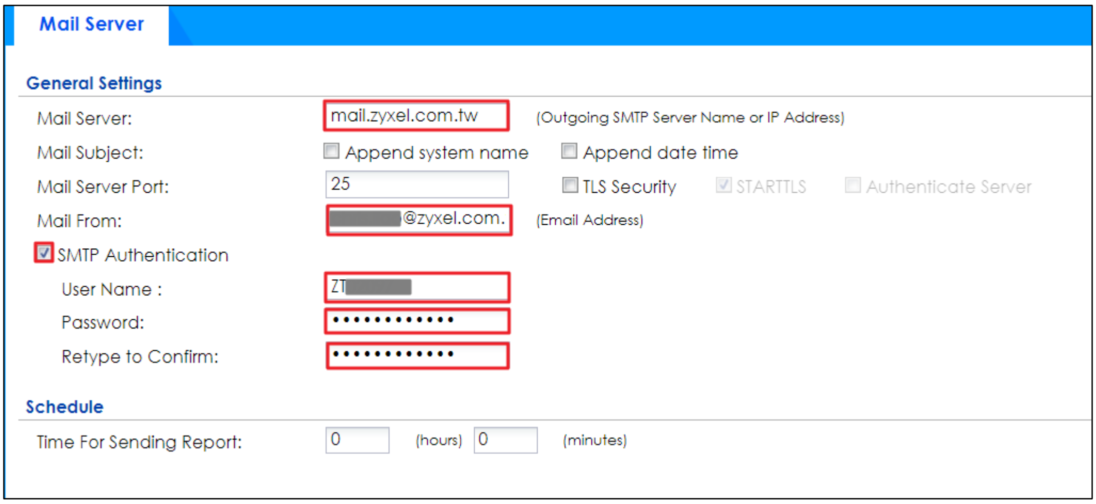


General Settings

☑ Enable Email Daily Report

Type the SMTP server name or IP address. In **Mail From**, type the e-mail address from which the outgoing e-mail is delivered. In **Mail To**, type the e-mail address to which the outgoing e-mail is delivered. Select **SMTP Authentication** if it is necessary to provide a user name and password to the SMTP server.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings



Mail Server

General Settings

Mail Server: mail.zyxel.com.tw (Outgoing SMTP Server Name or IP Address)

Mail Subject: □ Append system name □ Append date time

Mail Server Port: 25 □ TLS Security ☑ STARTTLS □ Authenticate Server

Mail From: [redacted]@zyxel.com. (Email Address)

☑ SMTP Authentication

User Name : ZT[redacted]

Password: ••••••••••••

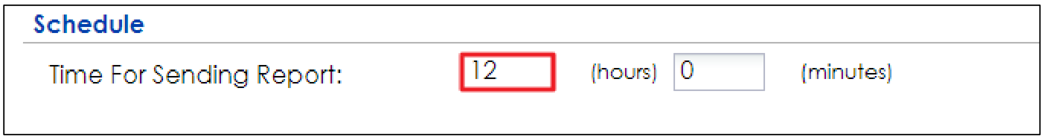
Retype to Confirm: ••••••••••••

Schedule

Time For Sending Report: 0 (hours) 0 (minutes)

In the **CONFIGURATION > Log & Report > Email Daily Report > Schedule**. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.

CONFIGURATION > Log & Report > Email Daily Report > Schedule

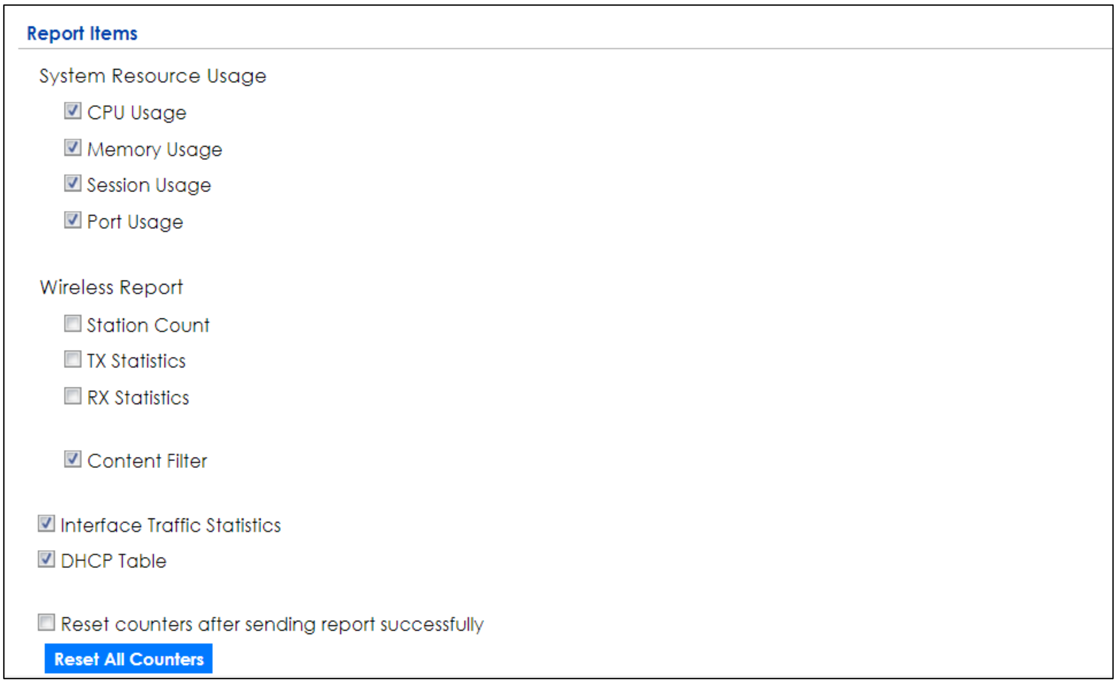


Time For Sending Report: 12 (hours) 0 (minutes)

Select the information to include in the report. Types of information include **System Resource Usage**, **Wireless Report**, **Threat Report**, and **Interface Traffic Statistics**.

Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period.

CONFIGURATION > Log & Report > Email Daily Report > Report Items



System Resource Usage

☑ CPU Usage

☑ Memory Usage

☑ Session Usage

☑ Port Usage

Wireless Report

☐ Station Count

☐ TX Statistics

☐ RX Statistics

☑ Content Filter

☑ Interface Traffic Statistics

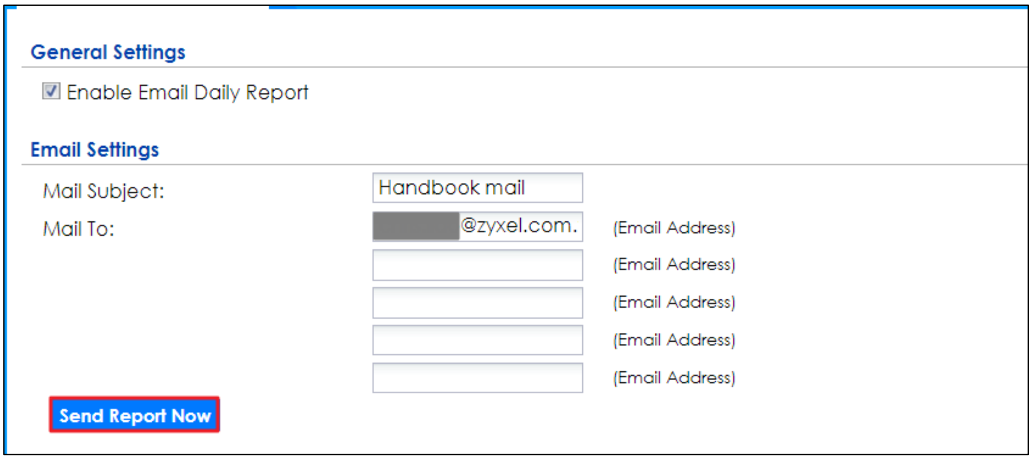
☑ DHCP Table

☐ Reset counters after sending report successfully

Test the Daily Log Report

Click **Send Report Now** to have the ZyWALL/USG send the daily e-mail report immediately.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings



General Settings

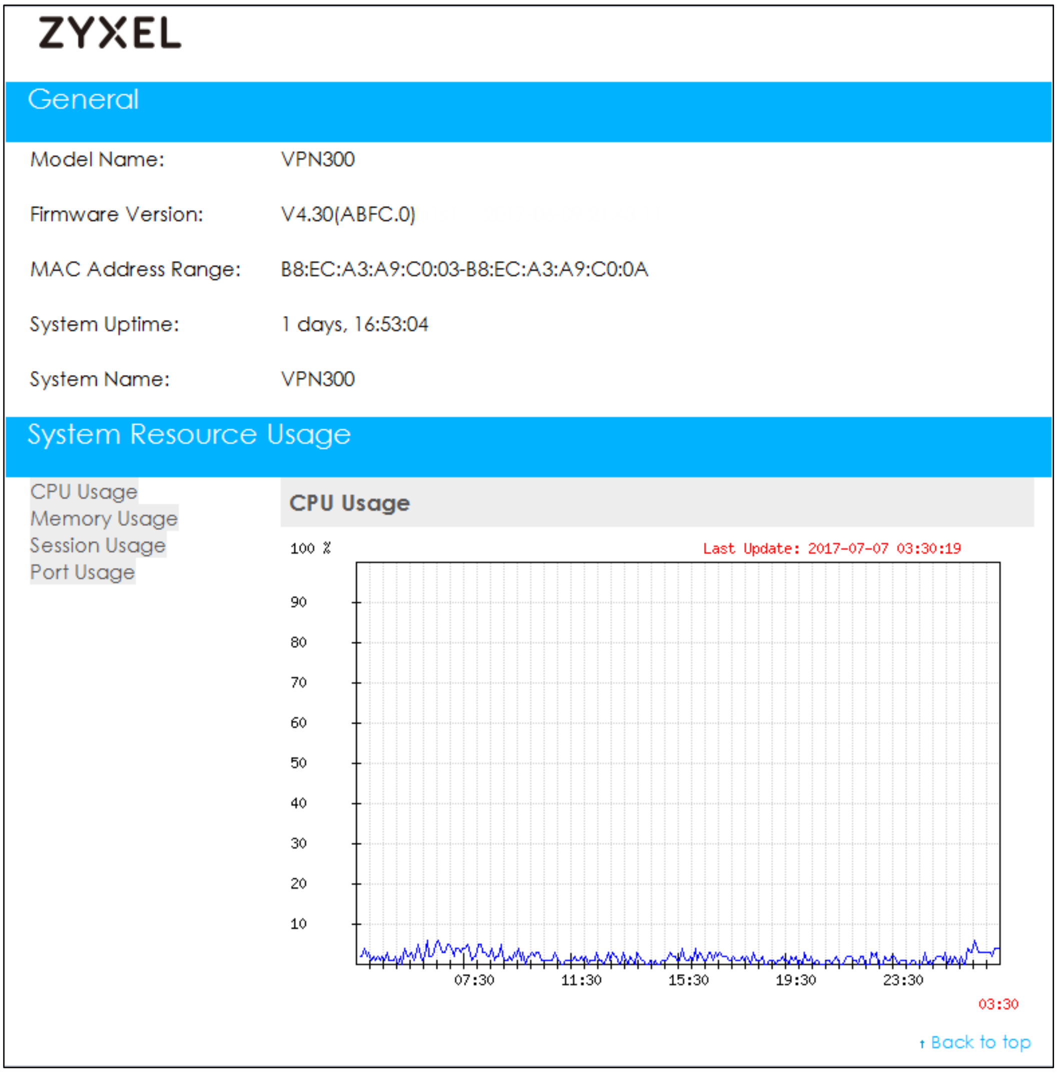
☑ Enable Email Daily Report

Email Settings

Mail Subject:	Handbook mail	
Mail To:	[redacted]@zyxel.com.	(Email Address)
		(Email Address)
		(Email Address)
		(Email Address)
		(Email Address)

You will receive a daily report mail.

ZyXEL Daily Report Mail



ZYXEL

General

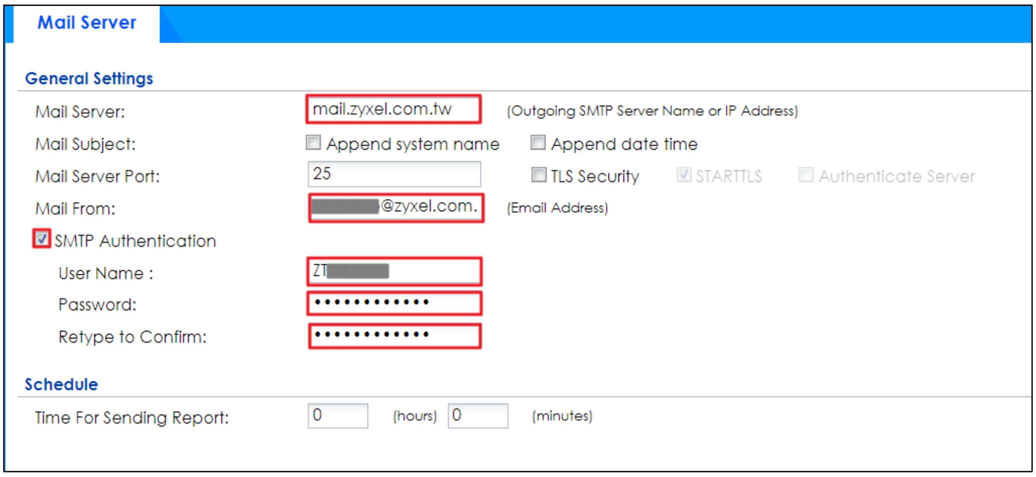
Model Name:	VPN300
Firmware Version:	V4.30(ABFC.0)
MAC Address Range:	B8:EC:A3:A9:C0:03-B8:EC:A3:A9:C0:0A
System Uptime:	1 days, 16:53:04
System Name:	VPN300

System Resource Usage

What Could Go Wrong?

Make sure your Email settings are all correct.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings



Mail Server

General Settings

Mail Server: mail.zyxel.com.tw (Outgoing SMTP Server Name or IP Address)

Mail Subject: □ Append system name □ Append date time

Mail Server Port: 25 □ TLS Security ☑ STARTTLS □ Authenticate Server

Mail From: [redacted]@zyxel.com. (Email Address)

☑ SMTP Authentication

User Name : ZT[redacted]

Password: •••••••••••••

Retype to Confirm: •••••••••••••

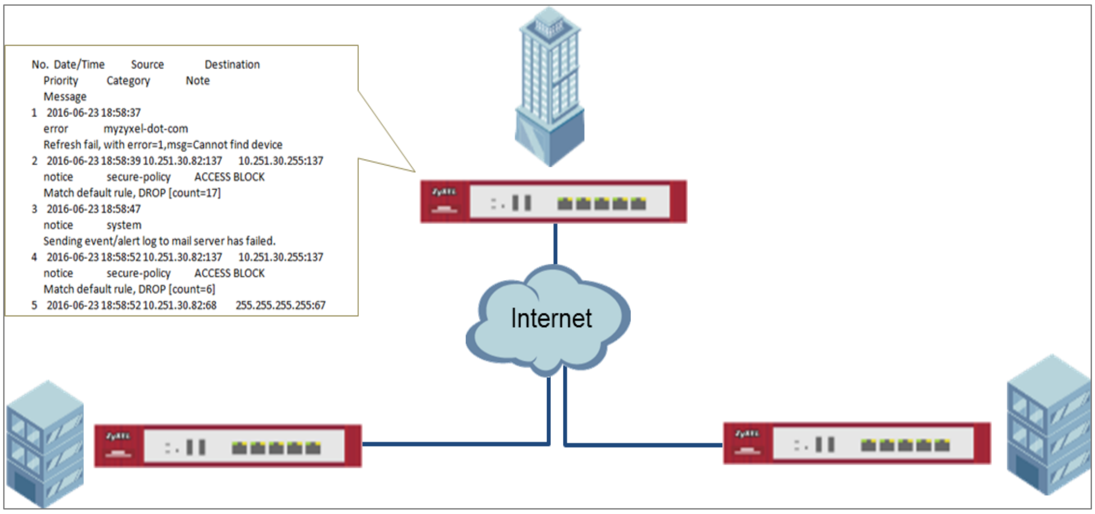
Schedule

Time For Sending Report: 0 (hours) 0 (minutes)

Make sure your ZyWALL to WAN security policy allow.

How to Setup and Configure Email Logs

This example shows how to set up the e-mail profiles to mail ZyWALL/USG log messages to the specific destinations. You can also specify which log messages to e-mail, and where and how often to e-mail them. When the Email Logs is configured, you will receive logs email report base on customized schedule.



```
No. Date/Time         Source              Destination
    Priority          Category            Note
    Message
1   2016-06-23 18:58:37
    error             myzyxel-dot-com
    Refresh fail, with error=1,msg=Cannot find device
2   2016-06-23 18:58:39 10.251.30.82:137    10.251.30.255:137
    notice            secure-policy       ACCESS BLOCK
    Match default rule, DROP [count=17]
3   2016-06-23 18:58:47
    notice            system
    Sending event/alert log to mail server has failed.
4   2016-06-23 18:58:52 10.251.30.82:137    10.251.30.255:137
    notice            secure-policy       ACCESS BLOCK
    Match default rule, DROP [count=6]
5   2016-06-23 18:58:52 10.251.30.82:68     255.255.255.255:67
```

ZyWALL/USG Setup and Configure E-mail Logs

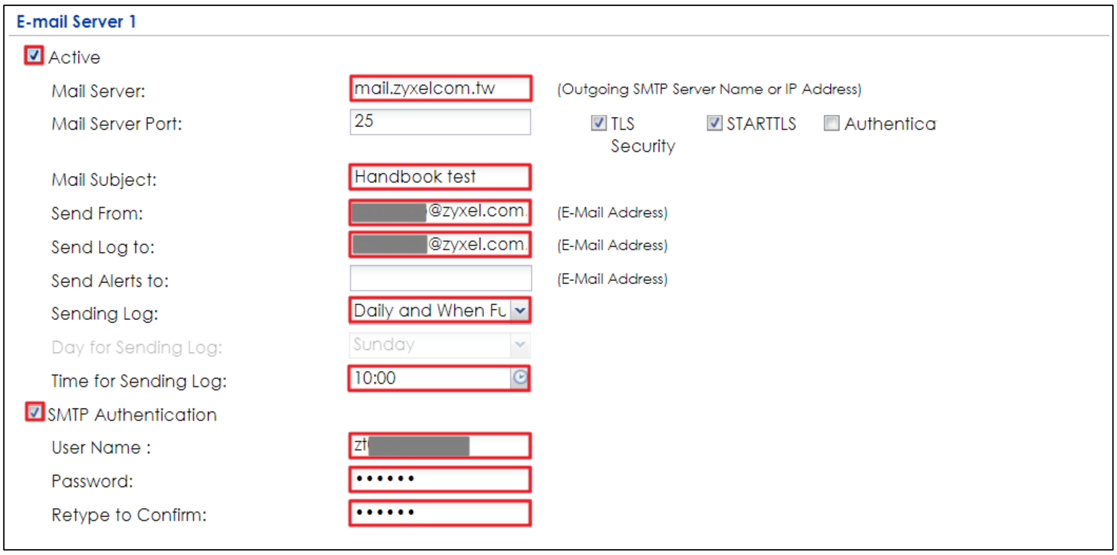
> Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Server 1. Select **Active.** Type the SMTP server name or IP address. In **Mail From**, type the e-mail address from which the outgoing e-mail is delivered. In **Mail To**, type the e-mail address to which the outgoing e-mail is delivered.

2. **Day for Sending Log** is available if the log is e-mailed weekly. Select the day of the week the log is e-mailed.
3. **Time for Sending Log** is available if the log is e-mailed weekly or daily. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.

4. Select **SMTP Authentication** if it is necessary to provide a user name and password to the SMTP server.

CONFIGURATION > Log & Report > Log Settings > System Log > Edit > E-mail Server 1



E-mail Server 1

☑ Active

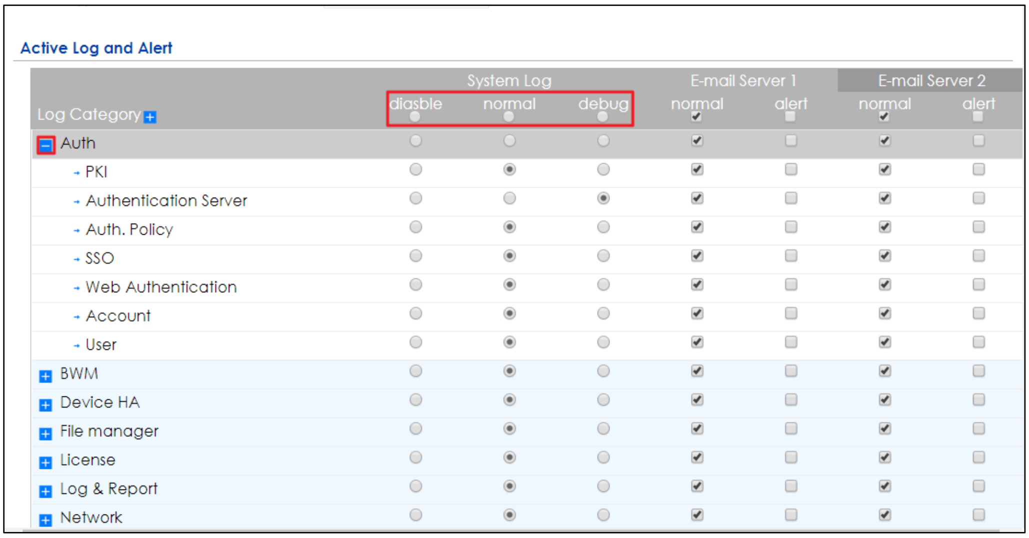
Mail Server:	mail.zyxelcom.tw	(Outgoing SMTP Server Name or IP Address)
Mail Server Port:	25	☑ TLS Security ☑ STARTTLS □ Authentica
Mail Subject:	Handbook test	
Send From:	[redacted]@zyxel.com	(E-Mail Address)
Send Log to:	[redacted]@zyxel.com	(E-Mail Address)
Send Alerts to:		(E-Mail Address)
Sending Log:	Daily and When Fu	
Day for Sending Log:	Sunday	
Time for Sending Log:	10:00	

☑ SMTP Authentication

User Name :	zt[redacted]
Password:	••••••
Retype to Confirm:	••••••

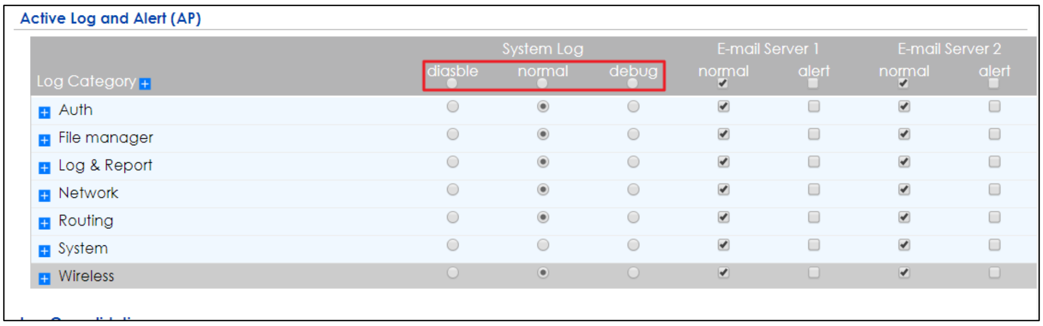
5. Go to **CONFIGURATION > Log & Report > Log Settings > System Log > Edit > Active Log and Alert.** Use the **System Log** drop-down list to change the log settings for all of the log categories.

CONFIGURATION > Log & Report > Log Settings > System Log > Edit > Active Log and Alert.



Active Log and Alert

Log Category ⊞	System Log			E-mail Server 1		E-mail Server 2	
	diasble ○	normal ○	debug ○	normal ☑	alert □	normal ☑	alert □
⊟ Auth	○	○	○	☑	□	☑	□
→ PKI	○	●	○	☑	□	☑	□
→ Authentication Server	○	○	●	☑	□	☑	□
→ Auth. Policy	○	●	○	☑	□	☑	□
→ SSO	○	●	○	☑	□	☑	□
→ Web Authentication	○	●	○	☑	□	☑	□
→ Account	○	●	○	☑	□	☑	□
→ User	○	●	○	☑	□	☑	□
⊞ BWM	○	●	○	☑	□	☑	□
⊞ Device HA	○	●	○	☑	□	☑	□
⊞ File manager	○	●	○	☑	□	☑	□
⊞ License	○	●	○	☑	□	☑	□
⊞ Log & Report	○	●	○	☑	□	☑	□
⊞ Network	○	●	○	☑	□	☑	□



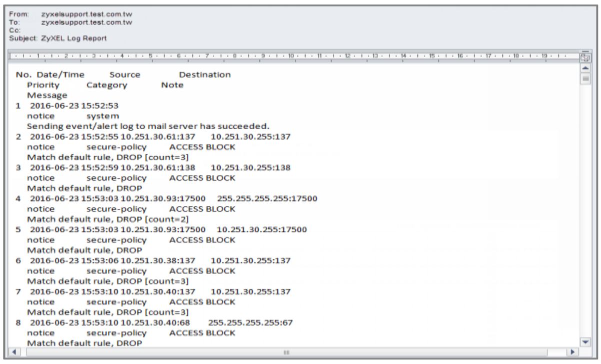
Active Log and Alert (AP)

Log Category ⊞	System Log			E-mail Server 1		E-mail Server 2	
	diasble ○	normal ○	debug ○	normal ☑	alert □	normal ☑	alert □
⊞ Auth	○	●	○	☑	□	☑	□
⊞ File manager	○	●	○	☑	□	☑	□
⊞ Log & Report	○	●	○	☑	□	☑	□
⊞ Network	○	●	○	☑	□	☑	□
⊞ Routing	○	●	○	☑	□	☑	□
⊞ System	○	○	○	☑	□	☑	□
⊞ Wireless	○	●	○	☑	□	☑	□

Test the Email Log

You will receive a log mail depends on the time you set in the E-mail Server.

ZyXEL Log Mail



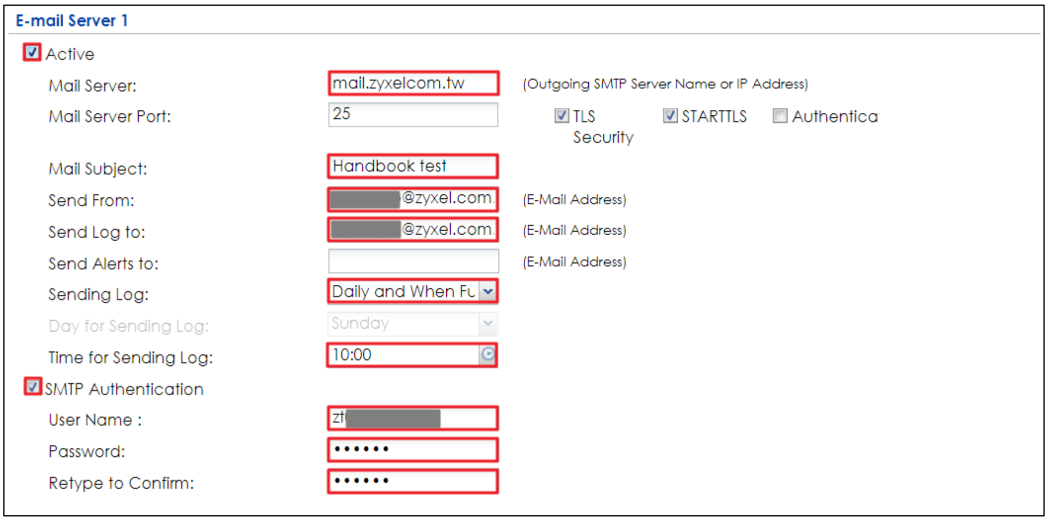
From: zyxelsupport.test.com.tw
To: zyxelsupport.test.com.tw
Cc:
Subject: ZyXEL Log Report

```
No.  Date/Time        Source            Destination
   Priority        Category          Note
   Message
1   2016-06-23 15:52:53
   notice          system
   Sending event/alert log to mail server has succeeded.
2   2016-06-23 15:52:55 10.251.30.61:137      10.251.30.255:137
   notice          secure-policy       ACCESS BLOCK
   Match default rule, DROP [count=3]
3   2016-06-23 15:52:59 10.251.30.61:138      10.251.30.255:138
   notice          secure-policy       ACCESS BLOCK
   Match default rule, DROP
4   2016-06-23 15:53:03 10.251.30.93:17500    255.255.255.255:17500
   notice          secure-policy       ACCESS BLOCK
   Match default rule, DROP [count=2]
5   2016-06-23 15:53:03 10.251.30.93:17500    10.251.30.255:17500
   notice          secure-policy       ACCESS BLOCK
   Match default rule, DROP
6   2016-06-23 15:53:06 10.251.30.38:137      10.251.30.255:137
   notice          secure-policy       ACCESS BLOCK
   Match default rule, DROP [count=3]
7   2016-06-23 15:53:10 10.251.30.40:137      10.251.30.255:137
   notice          secure-policy       ACCESS BLOCK
   Match default rule, DROP [count=3]
8   2016-06-23 15:53:10 10.251.30.40:68      255.255.255.255:67
   notice          secure-policy       ACCESS BLOCK
   Match default rule, DROP
```

What Could Go Wrong?

Make sure your Email settings are all correct.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings



E-mail Server 1

☑ Active

Mail Server:	mail.zyxelcom.tw	(Outgoing SMTP Server Name or IP Address)
Mail Server Port:	25	☑ TLS Security ☑ STARTTLS □ Authentica
Mail Subject:	Handbook test	
Send From:	[redacted]@zyxel.com	(E-Mail Address)
Send Log to:	[redacted]@zyxel.com	(E-Mail Address)
Send Alerts to:		(E-Mail Address)
Sending Log:	Daily and When Fu	
Day for Sending Log:	Sunday	
Time for Sending Log:	10:00	

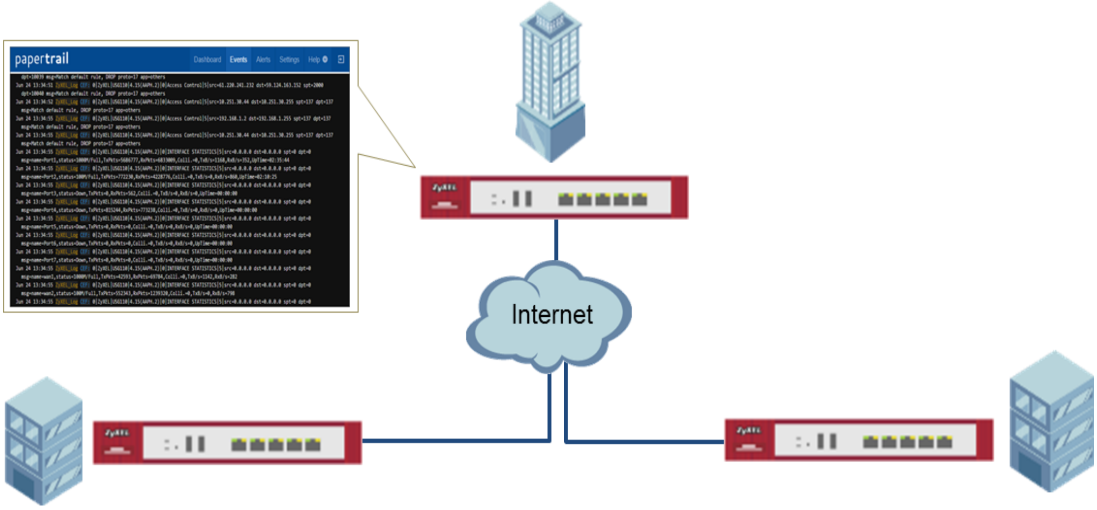
☑ SMTP Authentication

User Name :	zt[redacted]
Password:	••••••
Retype to Confirm:	••••••

Make sure your ZyWALL to WAN security policy allow.

How to Setup and send logs to a Syslog Server

This example shows how to set up the syslog server profiles to mail ZyWALL/USG log messages to the specific destinations. You can also specify which log messages to syslog server. When the syslog server is configured, you will receive the real time system logs.



```
  dpt=10039 msg=Match default rule, DROP proto=17 app=others
Jun 24 13:34:51 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=61.220.241.232 dst=59.124.163.152 spt=2000
  dpt=10040 msg=Match default rule, DROP proto=17 app=others
Jun 24 13:34:52 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=10.251.30.44 dst=10.251.30.255 spt=137 dpt=137
  msg=Match default rule, DROP proto=17 app=others
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=192.168.1.2 dst=192.168.1.255 spt=137 dpt=137
  msg=Match default rule, DROP proto=17 app=others
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=10.251.30.44 dst=10.251.30.255 spt=137 dpt=137
  msg=Match default rule, DROP proto=17 app=others
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
  msg=name=Port1,status=1000M/Full,TxPkts=5686777,RxPkts=6833009,Colli.=0,TxB/s=1168,RxB/s=352,UpTime=02:35:44
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
  msg=name=Port2,status=100M/Full,TxPkts=772230,RxPkts=4228776,Colli.=0,TxB/s=0,RxB/s=860,UpTime=02:10:25
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
  msg=name=Port3,status=Down,TxPkts=0,RxPkts=562,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
  msg=name=Port4,status=Down,TxPkts=815244,RxPkts=773238,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
  msg=name=Port5,status=Down,TxPkts=0,RxPkts=0,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
  msg=name=Port6,status=Down,TxPkts=0,RxPkts=0,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
  msg=name=Port7,status=Down,TxPkts=0,RxPkts=0,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
  msg=name=wan1,status=1000M/Full,TxPkts=42593,RxPkts=69784,Colli.=0,TxB/s=1142,RxB/s=282
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
  msg=name=wan2,status=100M/Full,TxPkts=552343,RxPkts=1239320,Colli.=0,TxB/s=0,RxB/s=798
Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
```

ZyWALL/USG Setup and Configure sending logs to a syslog and Vantage Reports Server

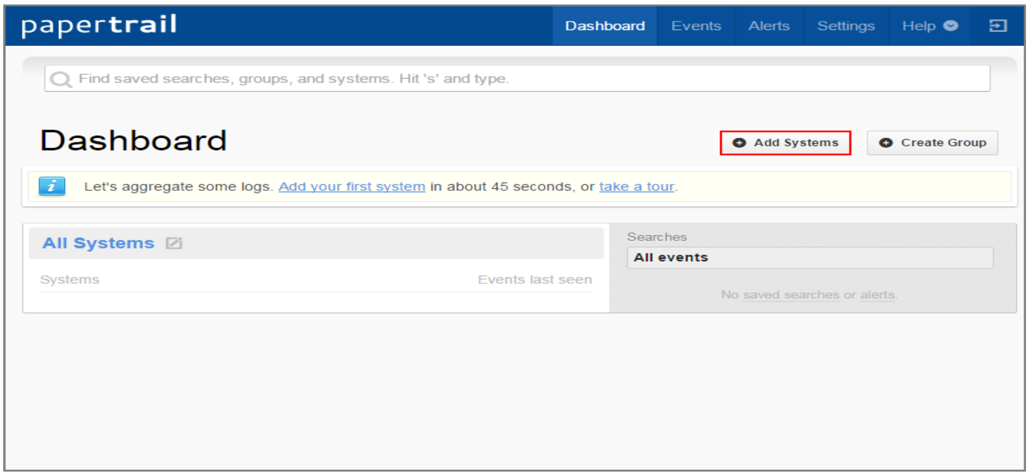
> Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the Syslog Server (Use Papertrail syslog in this example)

Register an account on Papertrail: https://papertrailapp.com

Go to **Dashboard > Add Systems**.

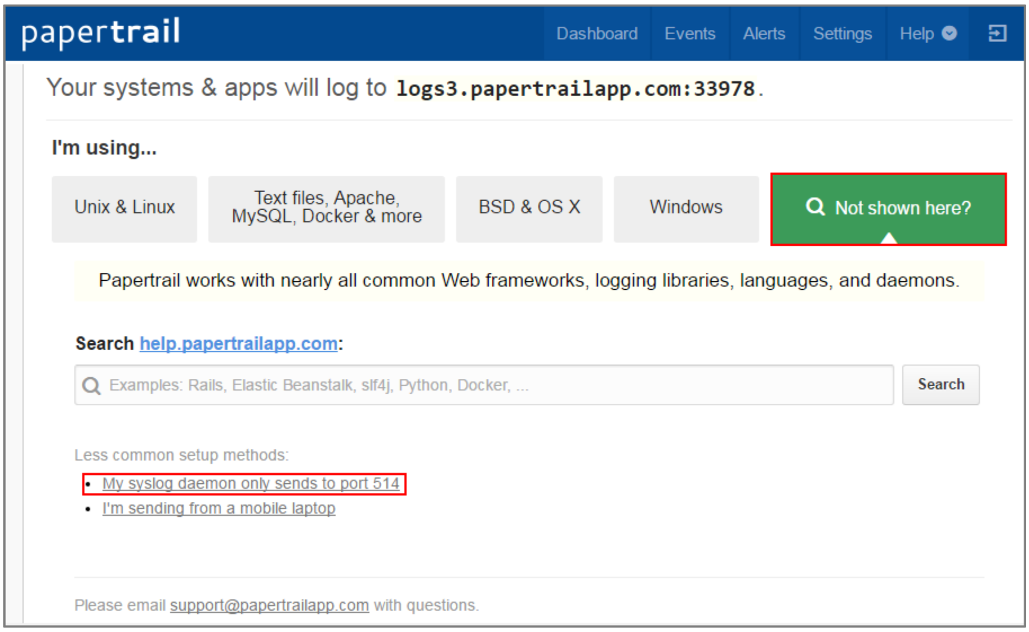
Dashboard > Add Systems



papertrail
Dashboard
Events
Alerts
Settings
Help
Find saved searches, groups, and systems. Hit 's' and type.
Dashboard
Add Systems
Create Group
Let's aggregate some logs. Add your first system in about 45 seconds, or take a tour.
All Systems
Systems
Events last seen
Searches
All events
No saved searches or alerts.

Select **Not shown here?** and **My syslog daemon only sends to port 514**.

Dashboard > Add Systems > I'm using



papertrail
Dashboard
Events
Alerts
Settings
Help
I'm using...
Unix & Linux
Text files, Apache, MySQL, Docker & more
BSD & OS X
Windows
Not shown here?
Search
Less common setup methods:
My syslog daemon only sends to port 514
I'm sending from a mobile laptop

Your systems & apps will log to `logs3.papertrailapp.com:33978`.

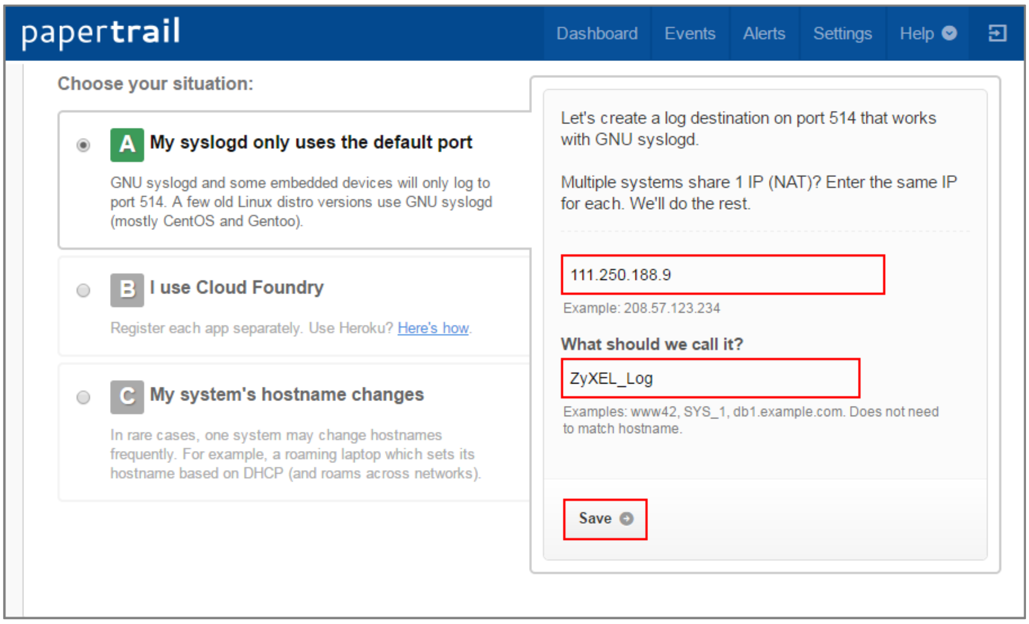
Papertrail works with nearly all common Web frameworks, logging libraries, languages, and daemons.

Search help.papertrailapp.com: Examples: Rails, Elastic Beanstalk, slf4j, Python, Docker, ...

Please email support@papertrailapp.com with questions.

Select **My syslogd only uses the default port**, set ZyWALL/USG public IP address (111.250.188.9 in this example) and name the log system. Click **Save**.

Dashboard > Add Systems > > I'm using > Choose your situation



Choose your situation:

● **A My syslogd only uses the default port**

GNU syslogd and some embedded devices will only log to port 514. A few old Linux distro versions use GNU syslogd (mostly CentOS and Gentoo).

○ **B I use Cloud Foundry**

Register each app separately. Use Heroku? Here's how.

○ **C My system's hostname changes**

In rare cases, one system may change hostnames frequently. For example, a roaming laptop which sets its hostname based on DHCP (and roams across networks).

Let's create a log destination on port 514 that works with GNU syslogd.

Multiple systems share 1 IP (NAT)? Enter the same IP for each. We'll do the rest.

111.250.188.9

Example: 208.57.123.234

What should we call it?

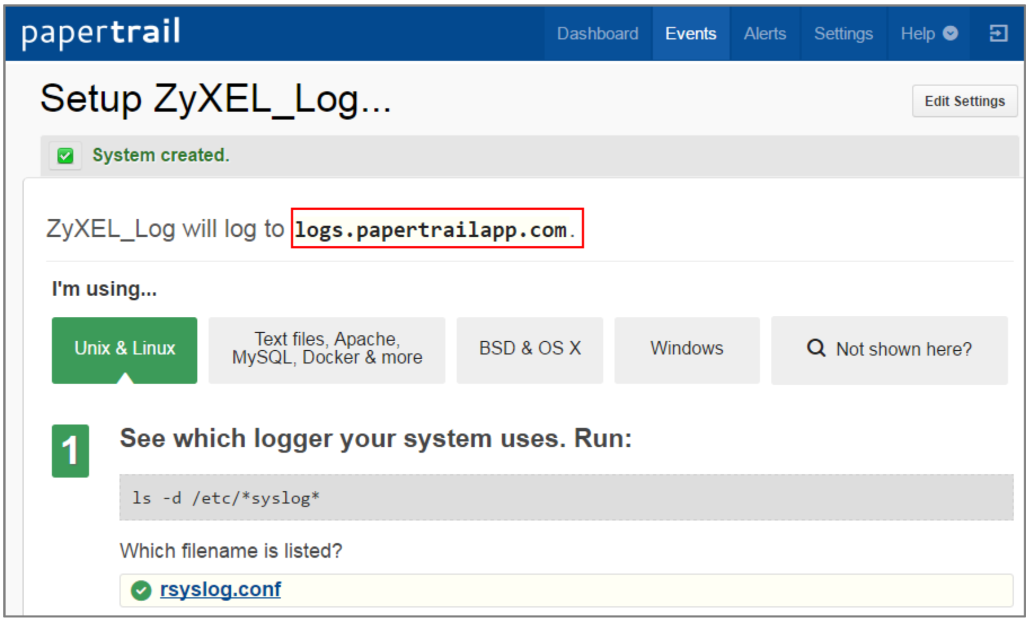
ZyXEL_Log

Examples: www42, SYS_1, db1.example.com. Does not need to match hostname.

Save

Write down the Papertrail-provided domain name (logs.papertrialpp.com in this example).

Dashboard > Add Systems > > I'm using > Choose your situation > System Created



Setup ZyXEL_Log...

✓ System created.

ZyXEL_Log will log to `logs.papertrailapp.com`.

I'm using...

Unix & Linux | Text files, Apache, MySQL, Docker & more | BSD & OS X | Windows | Not shown here?

1 **See which logger your system uses. Run:**

```
ls -d /etc/*syslog*
```

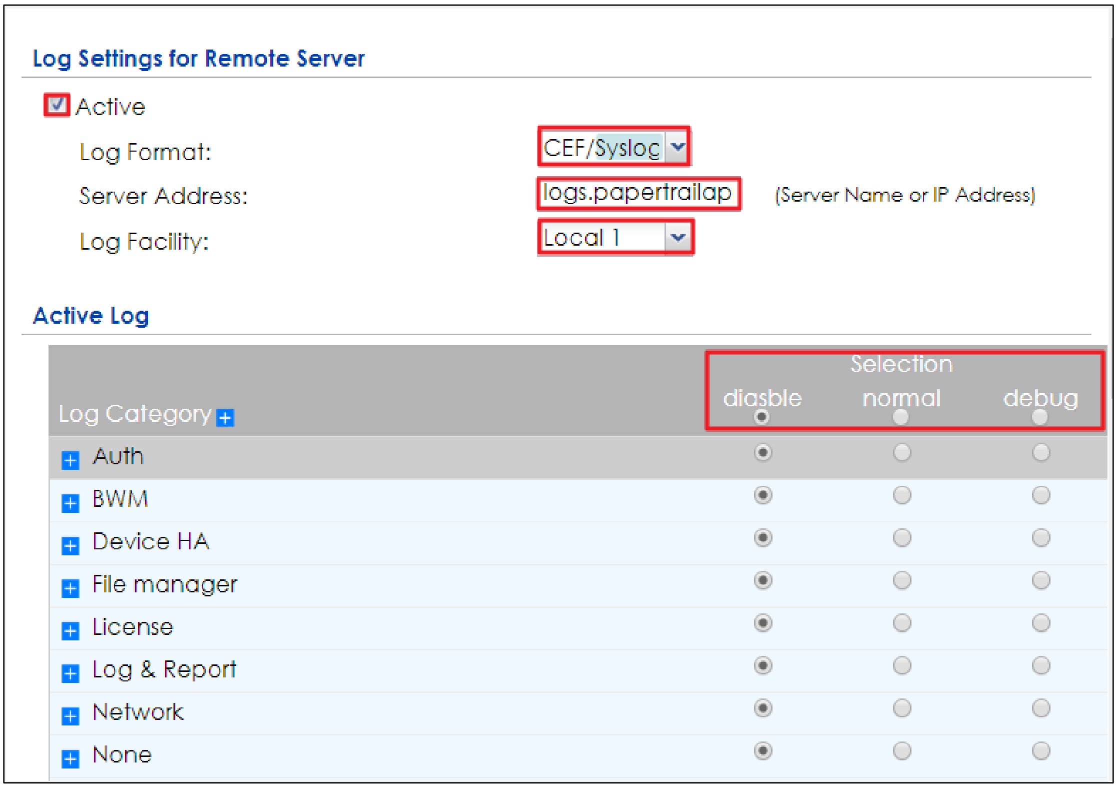
Which filename is listed?

✓ rsyslog.conf

Set Up the ZyWALL/USG Remote Server Setting

1. Go to **CONFIGURATION > Log & Report > Log Settings > Remote Server > Edit**. Set **Log Format** to be **CEF/Syslog**. Type the **Server Address** to be the Papertrail-provided domain name (logs.papertrialpp.com in this example).
2. Use the **System Log** drop-down list to change the log settings for all of the log categories.

CONFIGURATION > Log & Report > Log Settings > Remote Server > Edit



Log Settings for Remote Server

☑ Active

Log Format: CEF/Syslog

Server Address: logs.papertrailap (Server Name or IP Address)

Log Facility: Local 1

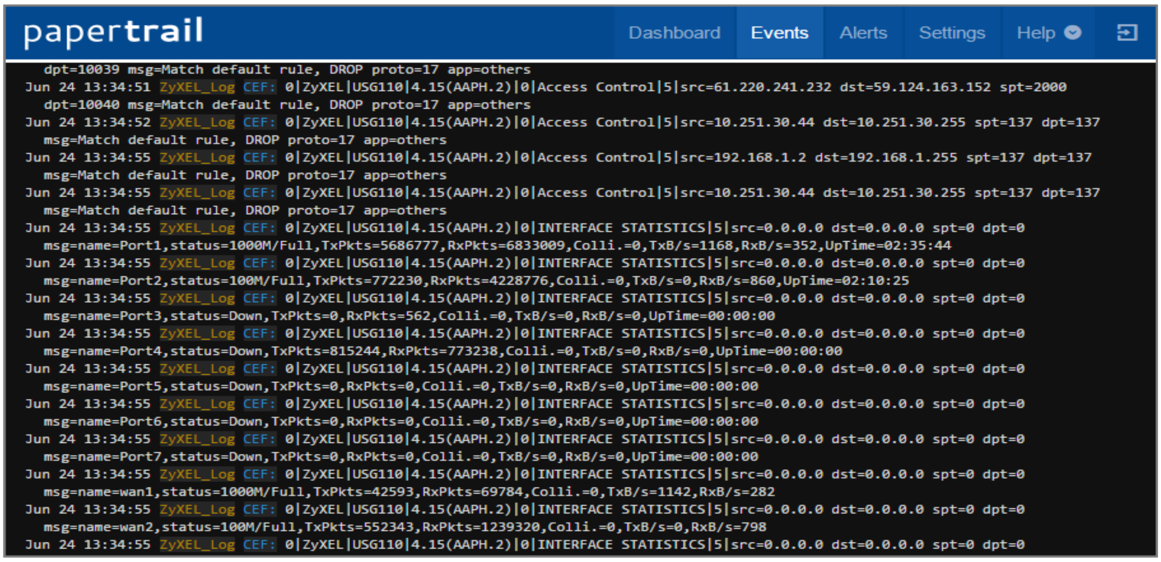
Active Log

Log Category	Selection		
	diasble	normal	debug
	●	○	○
Auth	●	○	○
BWM	●	○	○
Device HA	●	○	○
File manager	●	○	○
License	●	○	○
Log & Report	●	○	○
Network	●	○	○
None	●	○	○

Test the Remote Server

You will receive a log mail depends on the time you set in the E-mail Server.

ZyXEL Log Mail

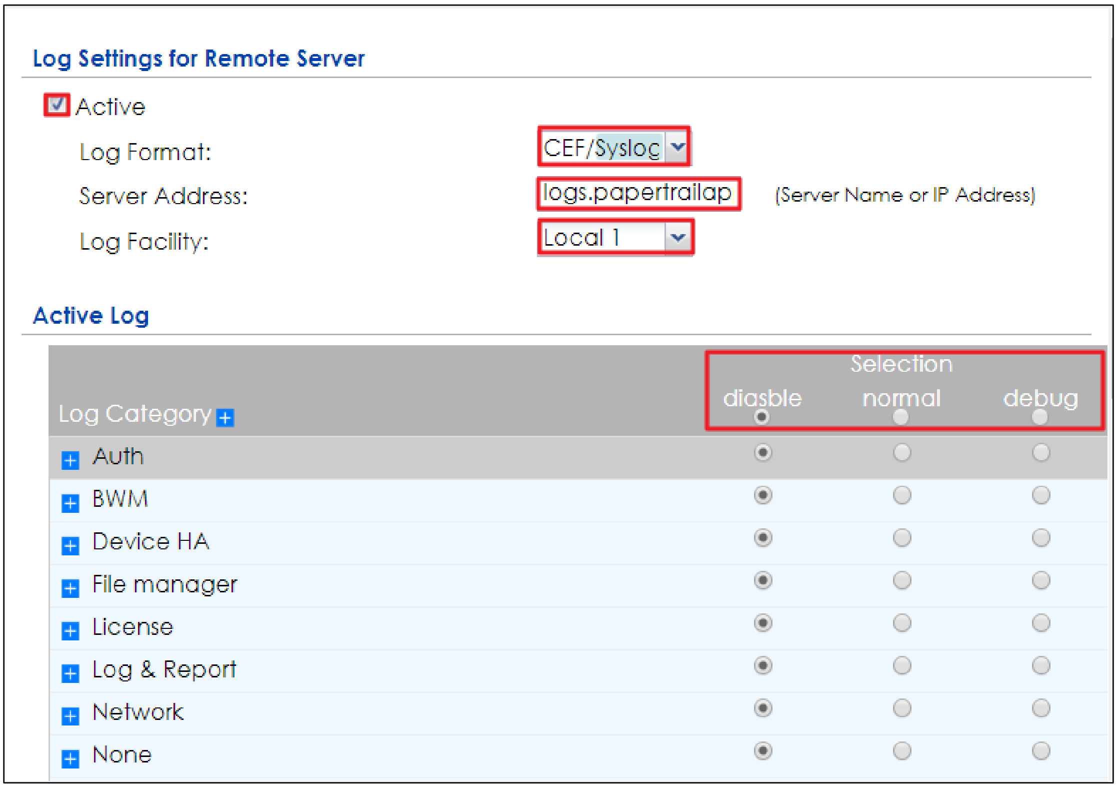


```
   dpt=10039 msg=Match default rule, DROP proto=17 app=others
 Jun 24 13:34:51 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=61.220.241.232 dst=59.124.163.152 spt=2000
   dpt=10040 msg=Match default rule, DROP proto=17 app=others
 Jun 24 13:34:52 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=10.251.30.44 dst=10.251.30.255 spt=137 dpt=137
   msg=Match default rule, DROP proto=17 app=others
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=192.168.1.2 dst=192.168.1.255 spt=137 dpt=137
   msg=Match default rule, DROP proto=17 app=others
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=10.251.30.44 dst=10.251.30.255 spt=137 dpt=137
   msg=Match default rule, DROP proto=17 app=others
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
   msg=name=Port1,status=1000M/Full,TxPkts=5686777,RxPkts=6833009,Colli.=0,TxB/s=1168,RxB/s=352,UpTime=02:35:44
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
   msg=name=Port2,status=100M/Full,TxPkts=772230,RxPkts=4228776,Colli.=0,TxB/s=0,RxB/s=860,UpTime=02:10:25
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
   msg=name=Port3,status=Down,TxPkts=0,RxPkts=562,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
   msg=name=Port4,status=Down,TxPkts=815244,RxPkts=773238,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
   msg=name=Port5,status=Down,TxPkts=0,RxPkts=0,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
   msg=name=Port6,status=Down,TxPkts=0,RxPkts=0,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
   msg=name=Port7,status=Down,TxPkts=0,RxPkts=0,Colli.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
   msg=name=wan1,status=1000M/Full,TxPkts=42593,RxPkts=69784,Colli.=0,TxB/s=1142,RxB/s=282
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
   msg=name=wan2,status=100M/Full,TxPkts=552343,RxPkts=1239320,Colli.=0,TxB/s=0,RxB/s=798
 Jun 24 13:34:55 ZyXEL_Log CEF: 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
```

What Could Go Wrong?

Make sure your **Log settings for Remote Server** are all correct.

CONFIGURATION > Log & Report > Log Settings > Remote Server



Log Settings for Remote Server

☑ Active

Log Format: CEF/Syslog

Server Address: logs.papertrailap (Server Name or IP Address)

Log Facility: Local 1

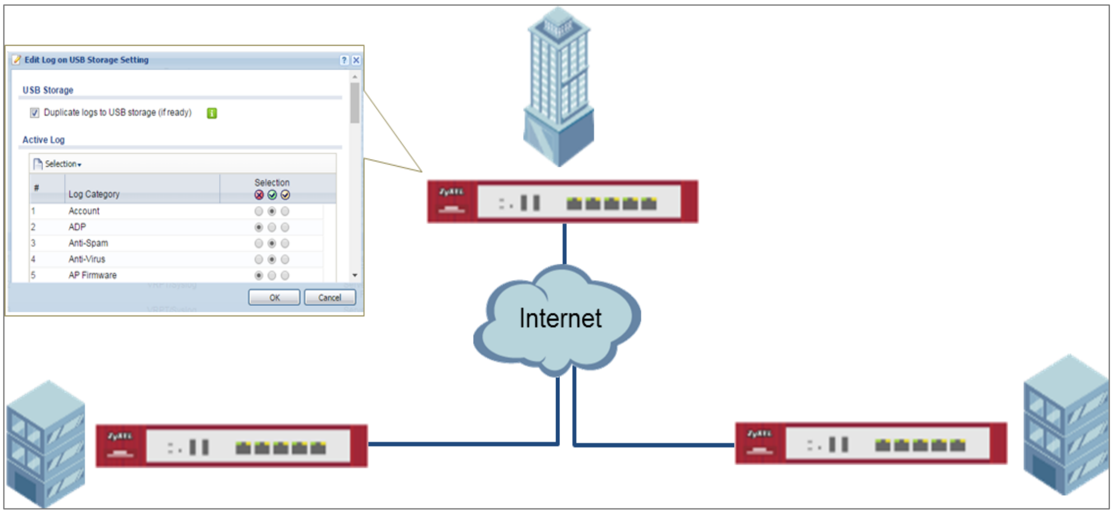
Active Log

Log Category	Selection diasble	 normal	 debug
Auth	●	○	○
BWM	●	○	○
Device HA	●	○	○
File manager	●	○	○
License	●	○	○
Log & Report	●	○	○
Network	●	○	○
None	●	○	○

Make sure your ZyWALL to WAN security policy allow traffic to log server.

How to Setup and send logs to the USB storage

This example shows how to use the USB device to store the system log information.



Edit Log on USB Storage Setting

USB Storage

☑ Duplicate logs to USB storage (if ready)

Active Log

Selection▾

#	Log Category	Selection ✗	Selection ✓	Selection ✓
1	Account	○	●	○
2	ADP	●	○	○
3	Anti-Spam	○	●	○
4	Anti-Virus	○	●	○
5	AP Firmware	●	○	○

ZyWALL/USG enable and send logs to the USB storage

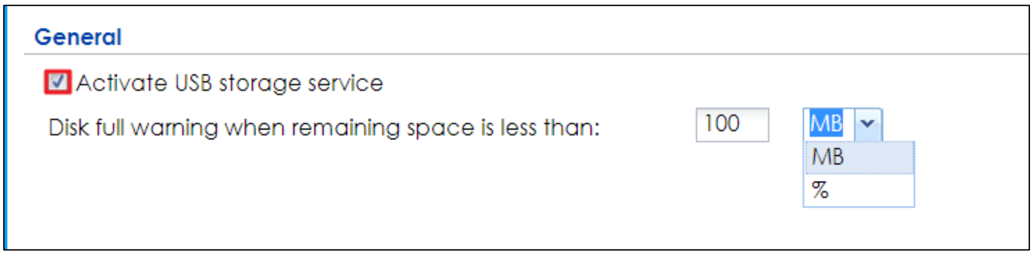
Note: Only connect one USB device. It must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the USB System Settings

Go to **CONFIGURATION > System > USB Storage > Settings > General**. Select **Activate USB storage service** if you want to use the connected USB device(s).

Set a number and select a unit (MB or %) to have the ZyWALL/USG send a warning message when the remaining USB storage space is less than the value you set here.

CONFIGURATION > System > USB Storage > Settings > General



General

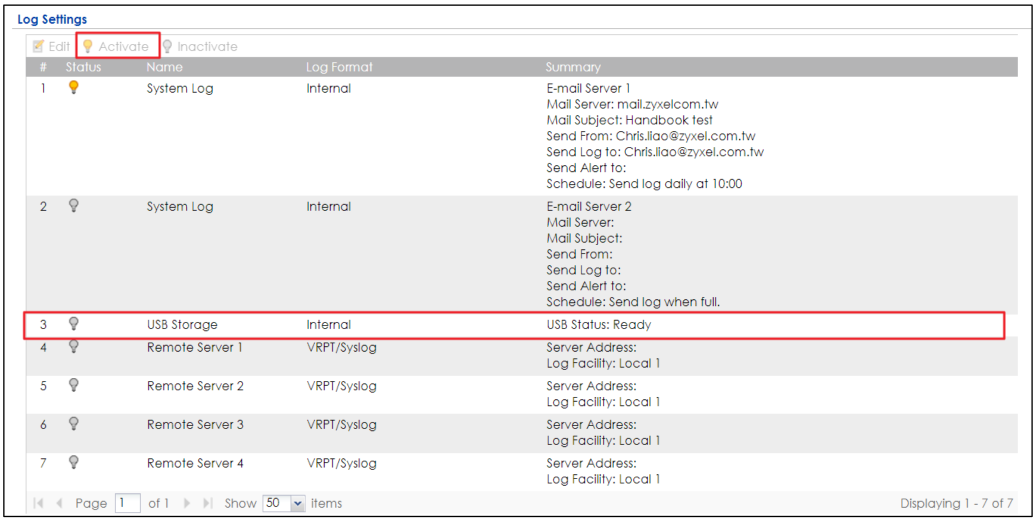
☑ Activate USB storage service

Disk full warning when remaining space is less than: 100 MB

Set Up the USB Log Storage

Go to **CONFIGURATION > Log & Report > Log Settings**, select **USB Storage** and click **Activate**. Click **Apply** to save your changes.

CONFIGURATION > Log & Report > Log Settings



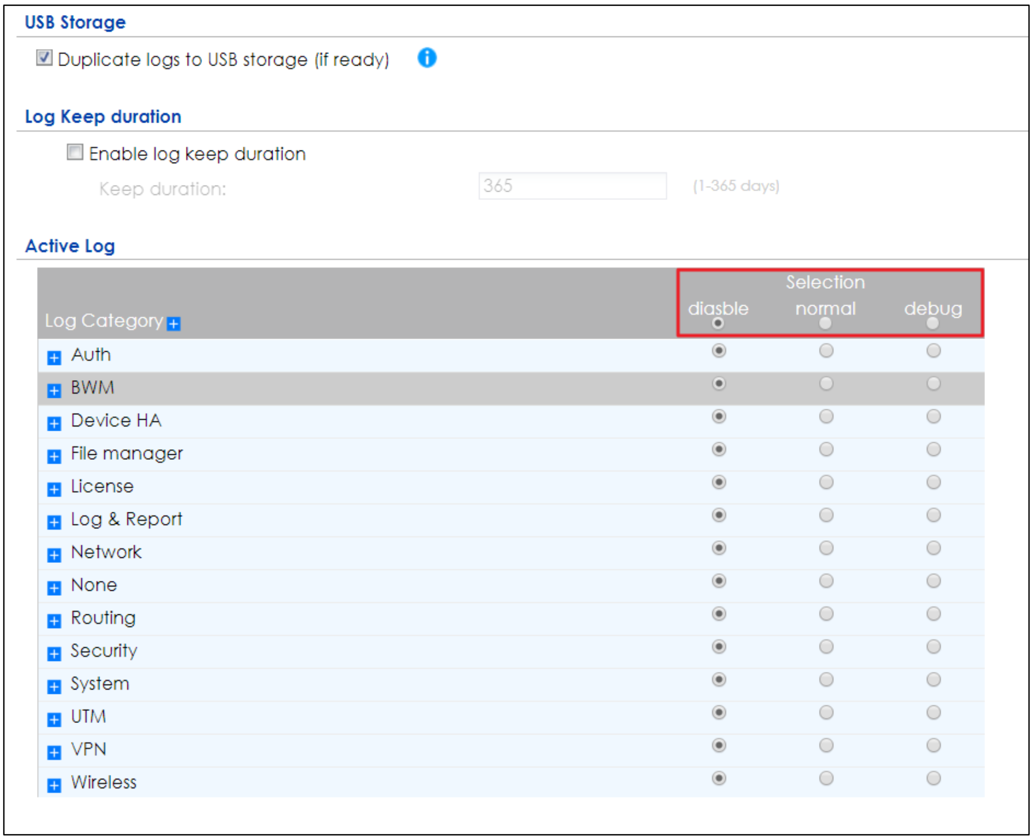
Log Settings

#	Status	Name	Log Format	Summary
1	●	System Log	Internal	E-mail Server 1 Mail Server: mail.zyxelcom.tw Mail Subject: Handbook test Send From: Chris.liao@zyxel.com.tw Send Log to: Chris.liao@zyxel.com.tw Send Alert to: Schedule: Send log daily at 10:00
2	○	System Log	Internal	E-mail Server 2 Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full.
3	○	USB Storage	Internal	USB Status: Ready
4	○	Remote Server 1	VRPT/Syslog	Server Address: Log Facility: Local 1
5	○	Remote Server 2	VRPT/Syslog	Server Address: Log Facility: Local 1
6	○	Remote Server 3	VRPT/Syslog	Server Address: Log Facility: Local 1
7	○	Remote Server 4	VRPT/Syslog	Server Address: Log Facility: Local 1

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

Go to **CONFIGURATION > Log & Report > Log Settings > USB Storage > Edit**. Select **Duplicate logs to USB storage (if ready)** to have the ZyWALL/USG save a copy of its system logs to a connected USB storage device. Use the **Selection** drop-down list to change the log settings for all of the log categories.

CONFIGURATION > Log & Report > Log Settings



USB Storage

☑ Duplicate logs to USB storage (if ready)

Log Keep duration

□ Enable log keep duration

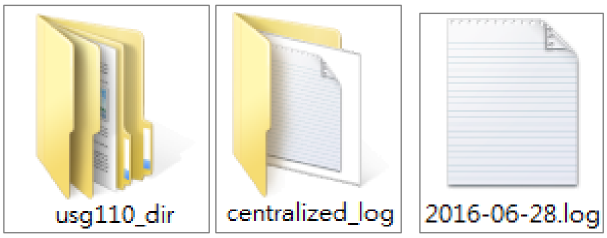
Keep duration: 365 (1-365 days)

Active Log

Log Category	Selection diasble	 normal	 debug
Auth	●	○	○
BWM	●	○	○
Device HA	●	○	○
File manager	●	○	○
License	●	○	○
Log & Report	●	○	○
Network	●	○	○
None	●	○	○
Routing	●	○	○
Security	●	○	○
System	●	○	○
UTM	●	○	○
VPN	●	○	○
Wireless	●	○	○

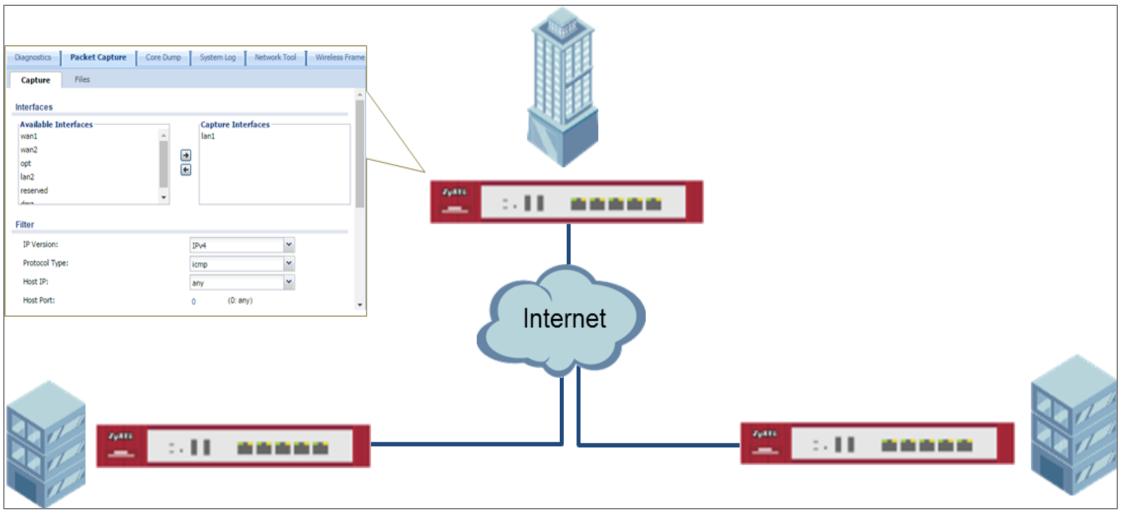
Check the USG Log Files

Connect the USB to PC and you can find the files in the following path:\Model Name_dir\centralized_log\YYYY-MM-DD.log



How to Perform and Use the Packet Capture Feature on the ZyWALL/USG

This example shows how to use the Packet Capture feature to capture network traffic going through the ZyWALL/USG's interfaces. Studying these packet captures may help you identify network problems.



Capture Interfaces: lan1

IP Version: IPv4

Protocol Type: icmp

Host IP: any

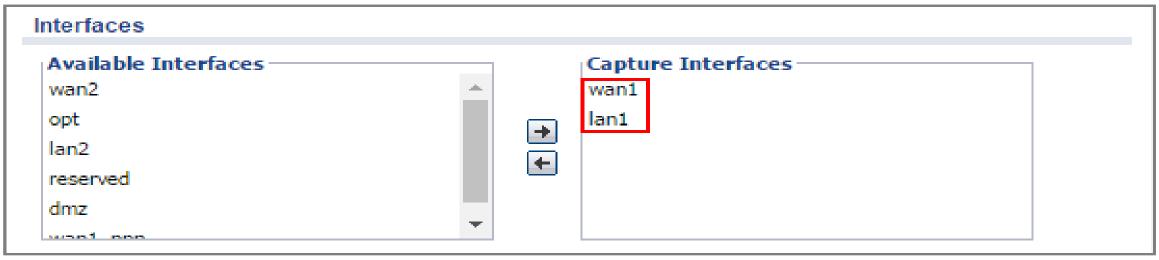
Host Port: 0 (0: any)

ZyWALL/USG Packet Capture Feature Settings

Note: New capture files overwrite existing files of the same name. Change the File Suffix field's setting to avoid this. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the Packet Capture Feature

7 Go to **MAINTENANCE** > **Diagnostics** > **Packet Capture** > **Capture** > **Interfaces**. Select interfaces for which to capture packets and click the right arrow button to move them to the **Capture Interfaces** list.



Interfaces

Available Interfaces

wan2
opt
lan2
reserved
dmz
wan1_ppp

Capture Interfaces

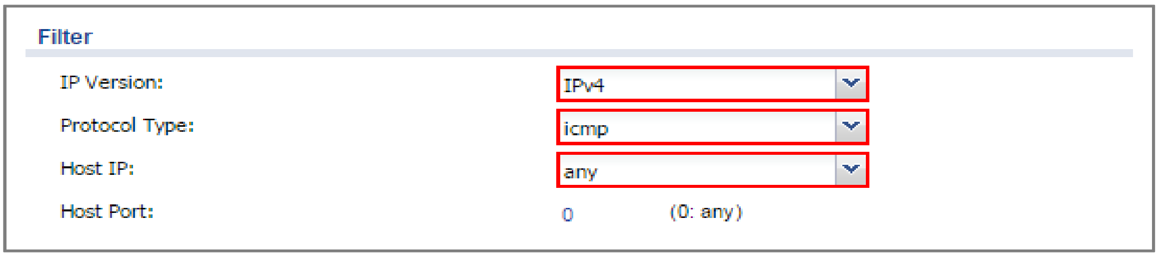
wan1
lan1

8 Go to **MAINTENANCE** > **Diagnostics** > **Packet Capture** > **Capture** > **Filter**.

Select **IP Version** (IPv4 or IPv6) for which to capture packets or select **any** to capture packets for all IP versions.

Select the **Protocol Type** of traffic for which to capture packets. Select **any** to capture packets for all types of traffic.

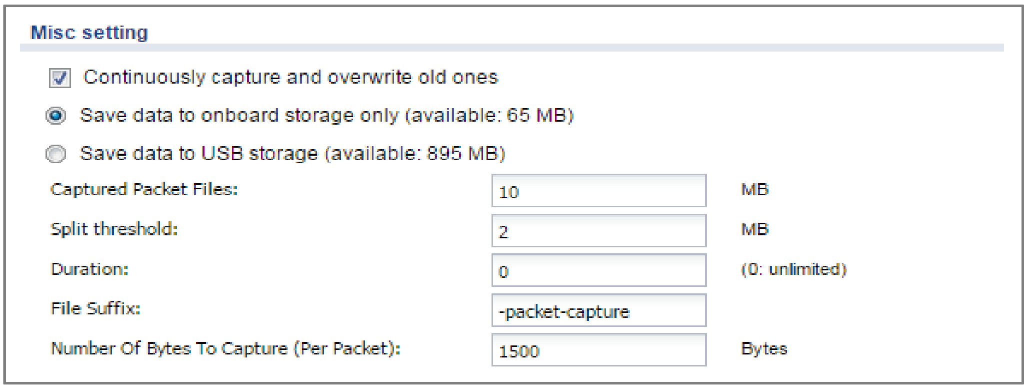
Select a **Host IP** address object for which to capture packets. Select **any** to capture packets for all hosts. Select **User Defined** to be able to enter an IP address.



Filter

IP Version:	IPv4	
Protocol Type:	icmp	
Host IP:	any	
Host Port:	0	(0: any)

9 Go to **MAINTENANCE > Diagnostics > Packet Capture > Capture > Misc setitng**. Select **Continuously capture and overwrite old ones** to have the ZyWALL/USG keep capturing traffic and overwriting old packet capture entries when the available storage space runs out. Select **Save data to onboard storage only** or **Save data to USB storage** (If status shows service deactivated, go to **CONFIGURATION > Object > USB Storage**, select Activate USB storage service)



Misc setting

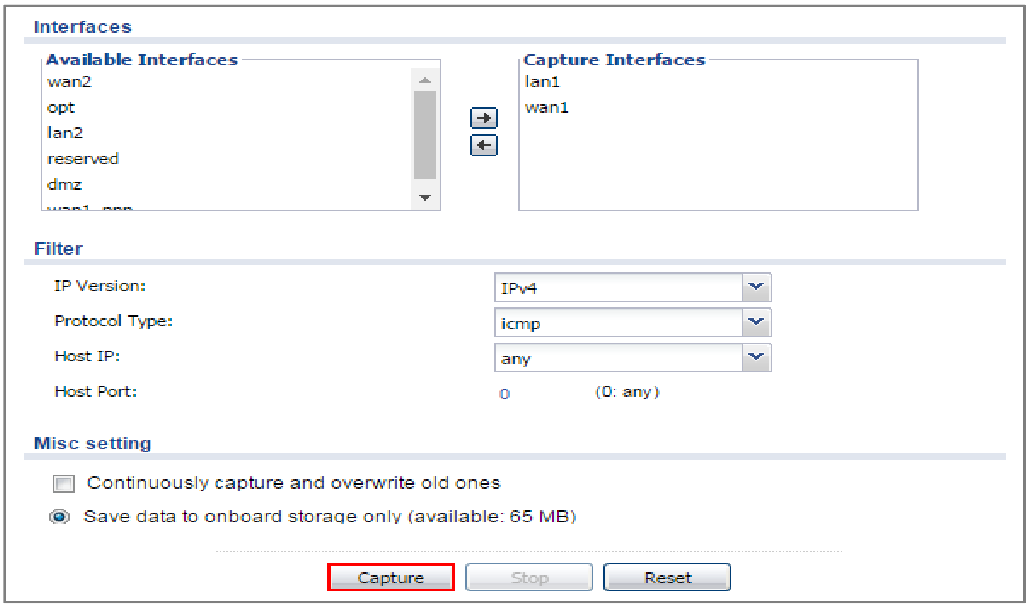
☑ Continuously capture and overwrite old ones

● Save data to onboard storage only (available: 65 MB)

○ Save data to USB storage (available: 895 MB)

Captured Packet Files:	10	MB
Split threshold:	2	MB
Duration:	0	(0: unlimited)
File Suffix:	-packet-capture	
Number Of Bytes To Capture (Per Packet):	1500	Bytes

10 Click **Capture**.



Interfaces

Available Interfaces: wan2, opt, lan2, reserved, dmz

Capture Interfaces: lan1, wan1

Filter

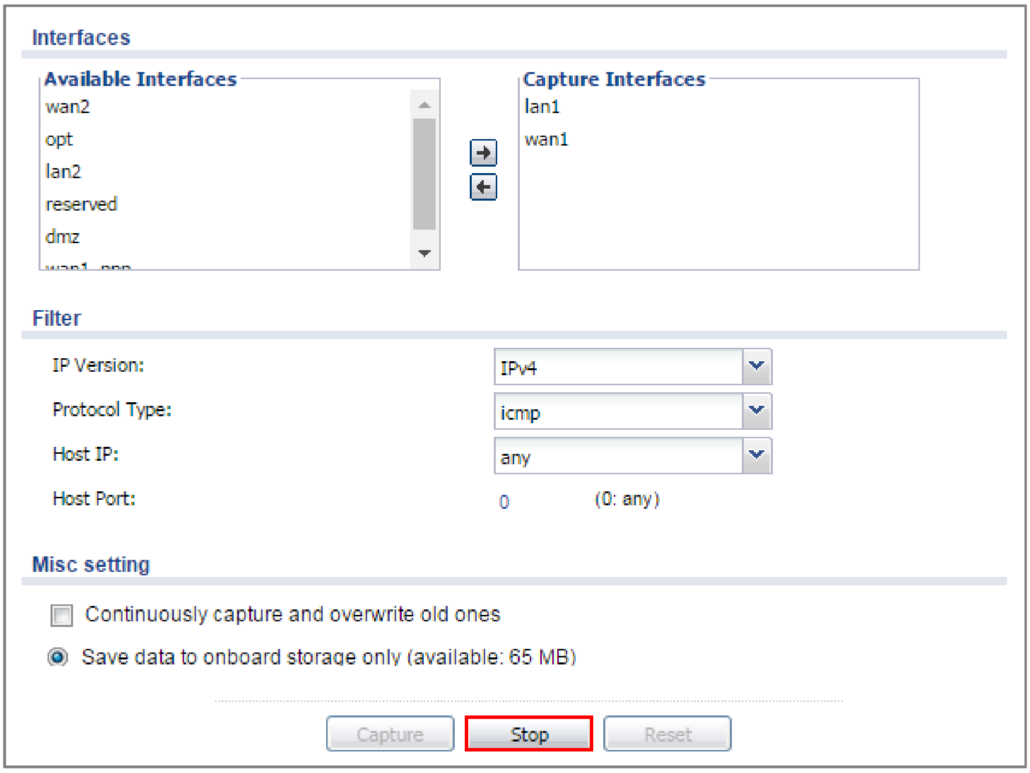
IP Version:	IPv4	
Protocol Type:	icmp	
Host IP:	any	
Host Port:	0	(0: any)

Misc setting

□ Continuously capture and overwrite old ones

● Save data to onboard storage only (available: 65 MB)

11 Click **Stop** when collection is done.



Interfaces

Available Interfaces: wan2, opt, lan2, reserved, dmz, wan1_ppp

Capture Interfaces: lan1, wan1

Filter

IP Version:	IPv4
Protocol Type:	icmp
Host IP:	any
Host Port:	0 (0: any)

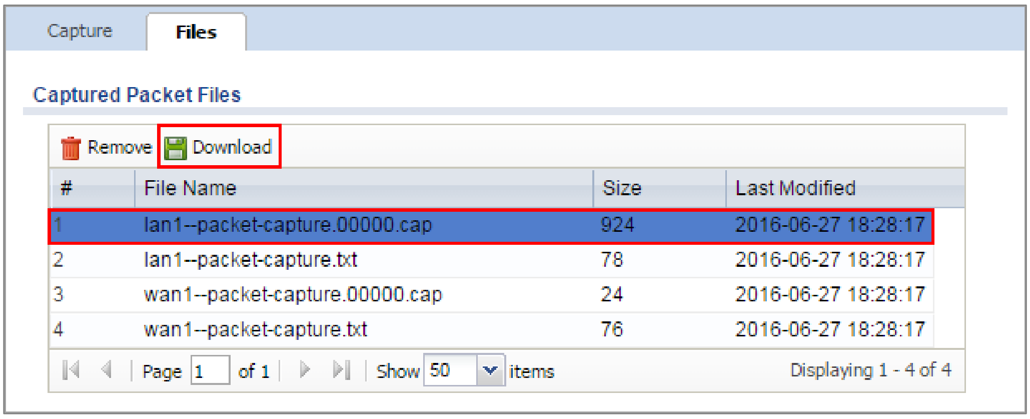
Misc setting

□ Continuously capture and overwrite old ones

● Save data to onboard storage only (available: 65 MB)

Check the Capture Files

12 Go to **MAINTENANCE > Diagnostics > Packet Capture > Files**, select the .cap file and click **Download**.

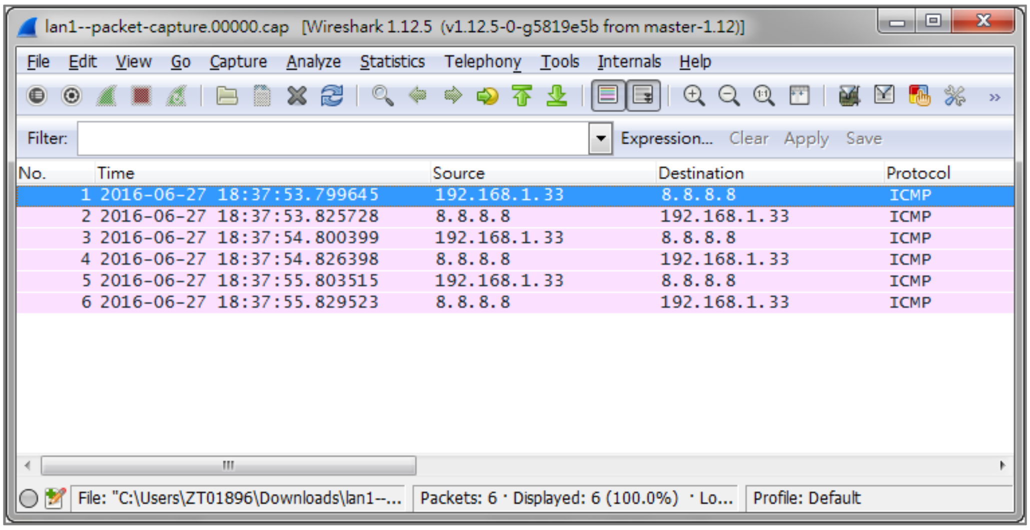


Captured Packet Files

#	File Name	Size	Last Modified
1	lan1--packet-capture.00000.cap	924	2016-06-27 18:28:17
2	lan1--packet-capture.txt	78	2016-06-27 18:28:17
3	wan1--packet-capture.00000.cap	24	2016-06-27 18:28:17
4	wan1--packet-capture.txt	76	2016-06-27 18:28:17

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

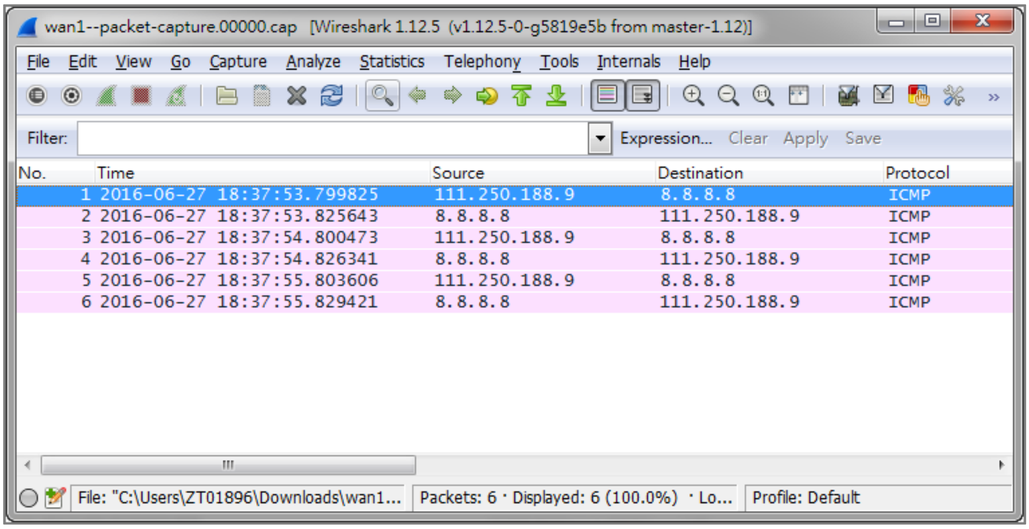
13 Open .cap files with Wireshark



lan1--packet-capture.00000.cap [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

No.	Time	Source	Destination	Protocol
1	2016-06-27 18:37:53.799645	192.168.1.33	8.8.8.8	ICMP
2	2016-06-27 18:37:53.825728	8.8.8.8	192.168.1.33	ICMP
3	2016-06-27 18:37:54.800399	192.168.1.33	8.8.8.8	ICMP
4	2016-06-27 18:37:54.826398	8.8.8.8	192.168.1.33	ICMP
5	2016-06-27 18:37:55.803515	192.168.1.33	8.8.8.8	ICMP
6	2016-06-27 18:37:55.829523	8.8.8.8	192.168.1.33	ICMP

File: "C:\Users\ZT01896\Downloads\lan1--... Packets: 6 · Displayed: 6 (100.0%) · Lo... Profile: Default



wan1--packet-capture.00000.cap [Wireshark 1.12.5 (v1.12.5-0-g5819e5b from master-1.12)]

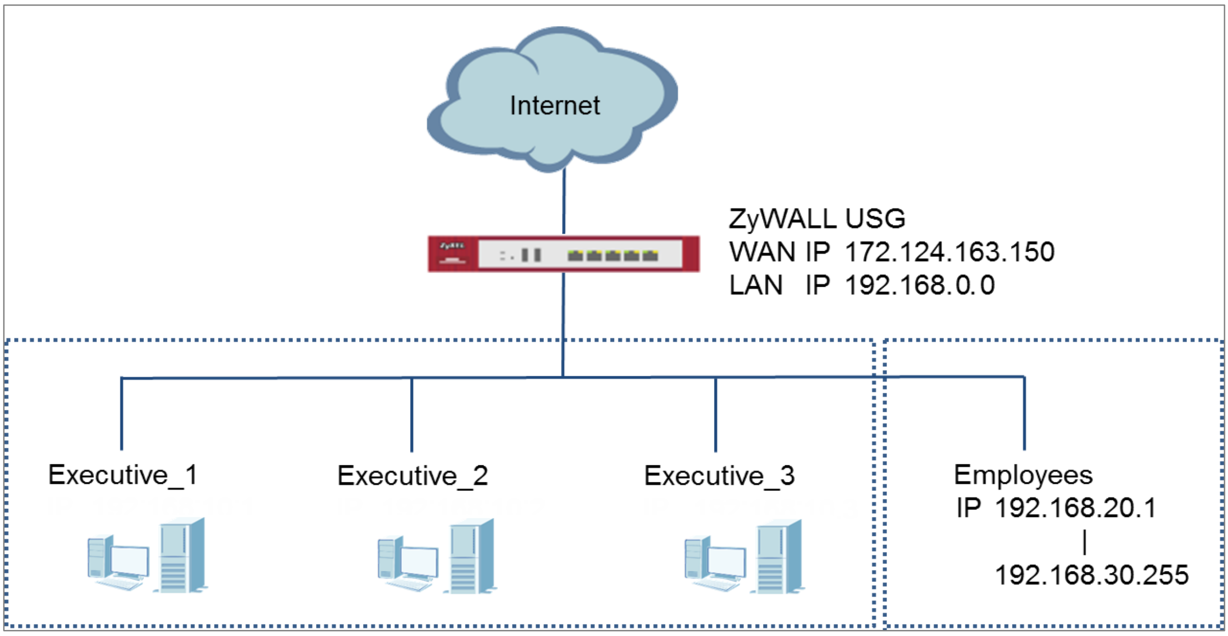
No.	Time	Source	Destination	Protocol
1	2016-06-27 18:37:53.799825	111.250.188.9	8.8.8.8	ICMP
2	2016-06-27 18:37:53.825643	8.8.8.8	111.250.188.9	ICMP
3	2016-06-27 18:37:54.800473	111.250.188.9	8.8.8.8	ICMP
4	2016-06-27 18:37:54.826341	8.8.8.8	111.250.188.9	ICMP
5	2016-06-27 18:37:55.803606	111.250.188.9	8.8.8.8	ICMP
6	2016-06-27 18:37:55.829421	8.8.8.8	111.250.188.9	ICMP

File: "C:\Users\ZT01896\Downloads\wan1... Packets: 6 · Displayed: 6 (100.0%) · Lo... Profile: Default

How to Exempt Specific Users from Security Control

This is an example of using a ZyWALL/USG Security Policy to exempt three corporate executives from security control, while controlling Internet access for other employees' accounts.

Exempt Specific Users from Security Control Example

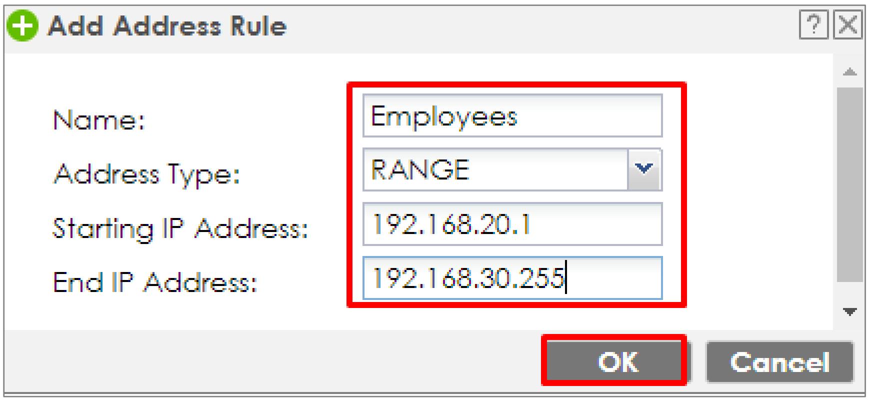


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Security Policy on the ZyWALL/USG for Employees

In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create address range for employees.

CONFIGURATION > Object > Address > Add Address Rule



Name: Employees

Address Type: RANGE

Starting IP Address: 192.168.20.1

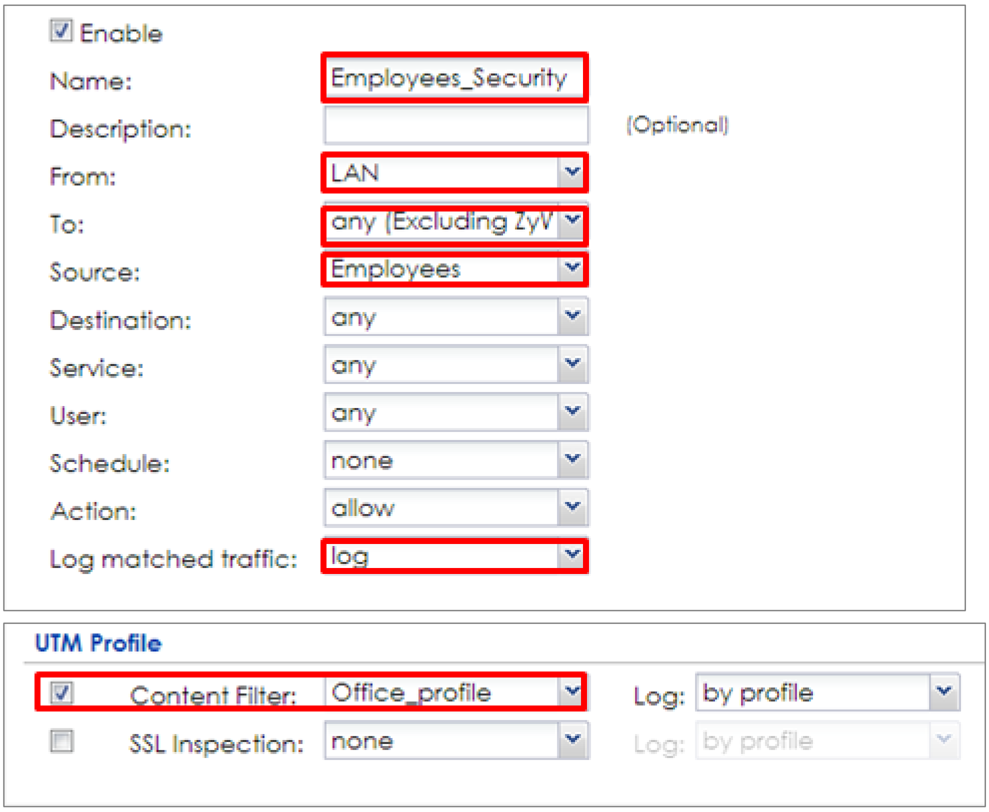
End IP Address: 192.168.30.255

Set up **Security Policy** for employees, go to **CONFIGURATION > Security Policy > Policy Control > Add corresponding**, configure a **Name** for you to identify the employees' **Security Policy** profile.

For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select **Source** to be the **Employees** to apply the policy to all traffic coming from them. In order to view the test result later on, set **Log matched traffic** to be **log**.

Scroll down to **UTM Profile**, select the general policy that allows employees to access the Internet. (Using built-in Office profile in this example blocks the non-productive services, such as Advertisement & Pop-Ups, Gambling and Peer to Peer services…etc.).

CONFIGURATION > Security Policy > Policy Control > Add corresponding > Employees_Security



☑ Enable

Name:	Employees_Security	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyW	
Source:	Employees	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	log	

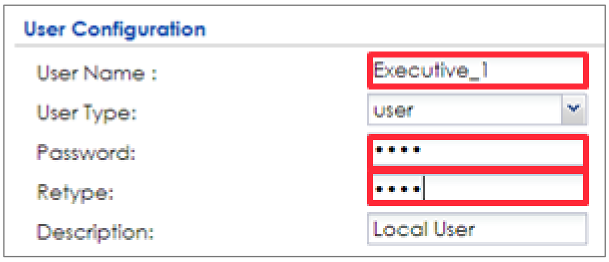
UTM Profile

☑	Content Filter:	Office_profile	Log:	by profile
□	SSL Inspection:	none	Log:	by profile

Set Up the Security Policy on the ZyWALL/USG for Executives

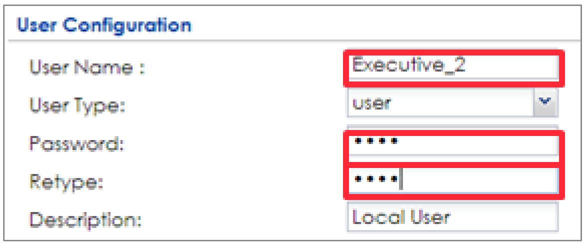
In the ZyWALL/USG, go to **CONFIGURATION > Object > User/Group > Add A User** to create **User Name/Password** for each executive.

CONFIGURATION > Object > User/Group > Add A User



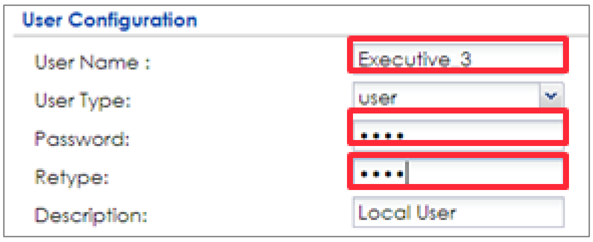
User Configuration

User Name :	Executive_1
User Type:	user
Password:	••••
Retype:	••••
Description:	Local User



User Configuration

User Name :	Executive_2
User Type:	user
Password:	••••
Retype:	••••
Description:	Local User

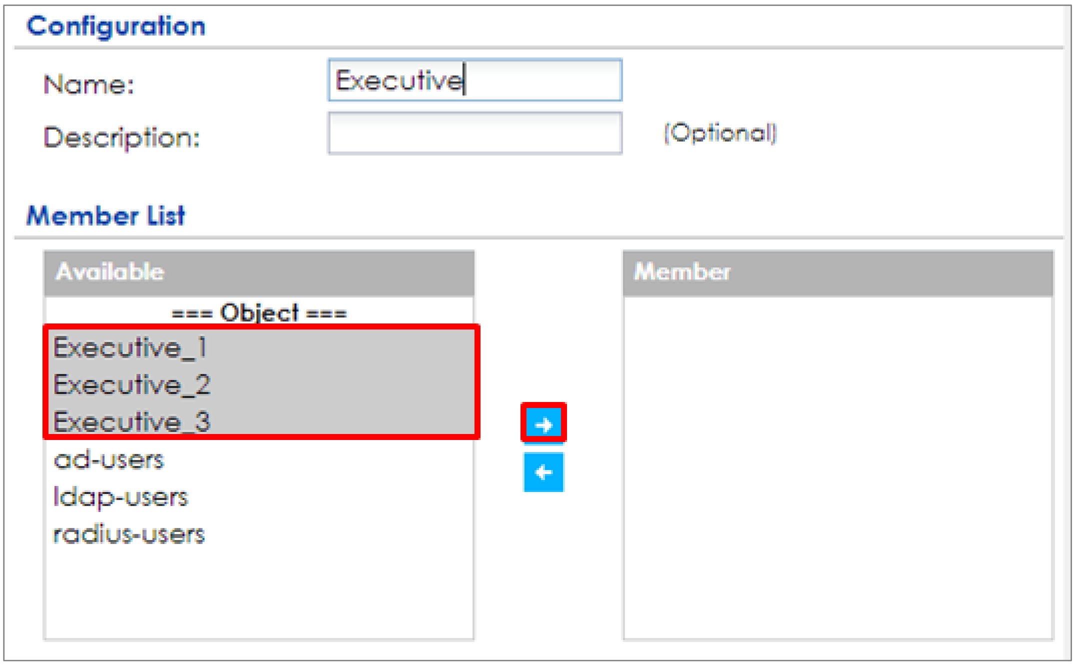


User Configuration

User Name :	Executive_3
User Type:	user
Password:	••••
Retype:	••••
Description:	Local User

Then, go to **CONFIGURATION > Object > User/Group > Group > Add Group** to create a **Group Members' Name** and move the just created executives user object to **Member**.

CONFIGURATION > Object > Address Group > Add Address Group Rule



Configuration

Name: Executive

Description: (Optional)

Member List

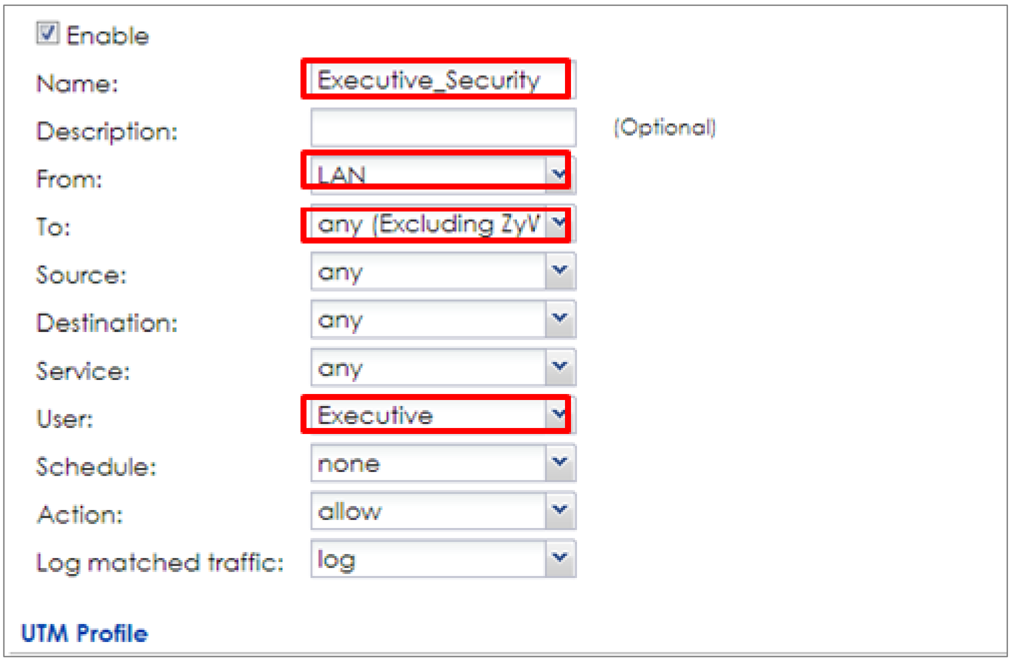
Set up **Security Policy** for executives, go to **CONFIGURATION > Security Policy > Policy Control > Add corresponding**, configure a **Name** for you to identify the executives' **Security Policy** profile.

For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select **User** to be the **Executives** to apply the policy to all traffic coming from them.

In order to view the test result later on, set **Log matched traffic** to be **log**.

Leave all **UTM Profiles** disabled.

CONFIGURATION > Security Policy > Policy Control > Add corresponding > Employees_Security



☑ Enable

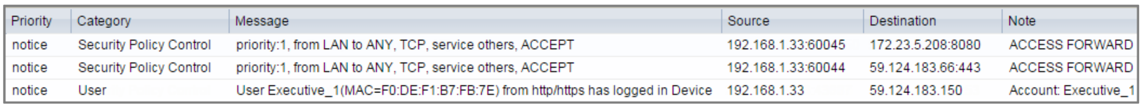
Name:	Executive_Security	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyW	
Source:	any	
Destination:	any	
Service:	any	
User:	Executive	
Schedule:	none	
Action:	allow	
Log matched traffic:	log	

Test the Result

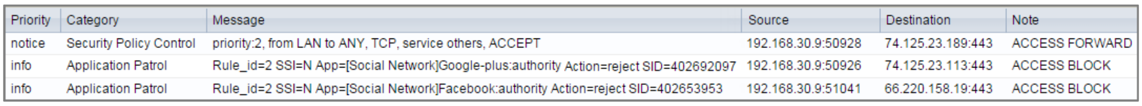
Connect to the Internet from two computers: one from executive_1 and one from an employee address (192.168.30.9).

Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] log message such as below. In this example result, a connection from executive_1 has user login message and always with **ACCESS FORWARD** information. A connection from employee address (192.168.30.9) and some of the services are with **ACCESS BLOCK** information

Monitor > Log



Priority	Category	Message	Source	Destination	Note
notice	Security Policy Control	priority:1, from LAN to ANY, TCP, service others, ACCEPT	192.168.1.33:60045	172.23.5.208:8080	ACCESS FORWARD
notice	Security Policy Control	priority:1, from LAN to ANY, TCP, service others, ACCEPT	192.168.1.33:60044	59.124.183.66:443	ACCESS FORWARD
notice	User	User Executive_1(MAC=F0:DE:F1:B7:FB:7E) from http/https has logged in Device	192.168.1.33	59.124.183.150	Account: Executive_1



Priority	Category	Message	Source	Destination	Note
notice	Security Policy Control	priority:2, from LAN to ANY, TCP, service others, ACCEPT	192.168.30.9:50928	74.125.23.189:443	ACCESS FORWARD
info	Application Patrol	Rule_id=2 SSI=N App=[Social Network]Google-plus:authority Action=reject SID=402692097	192.168.30.9:50926	74.125.23.113:443	ACCESS BLOCK
info	Application Patrol	Rule_id=2 SSI=N App=[Social Network]Facebook:authority Action=reject SID=402653953	192.168.30.9:51041	66.220.158.19:443	ACCESS BLOCK

What Could Go Wrong?

If you are not be able to configure any **UTM** policies or it's not working, there are two possible reasons:

You have not subscribed for the **UTM** service.

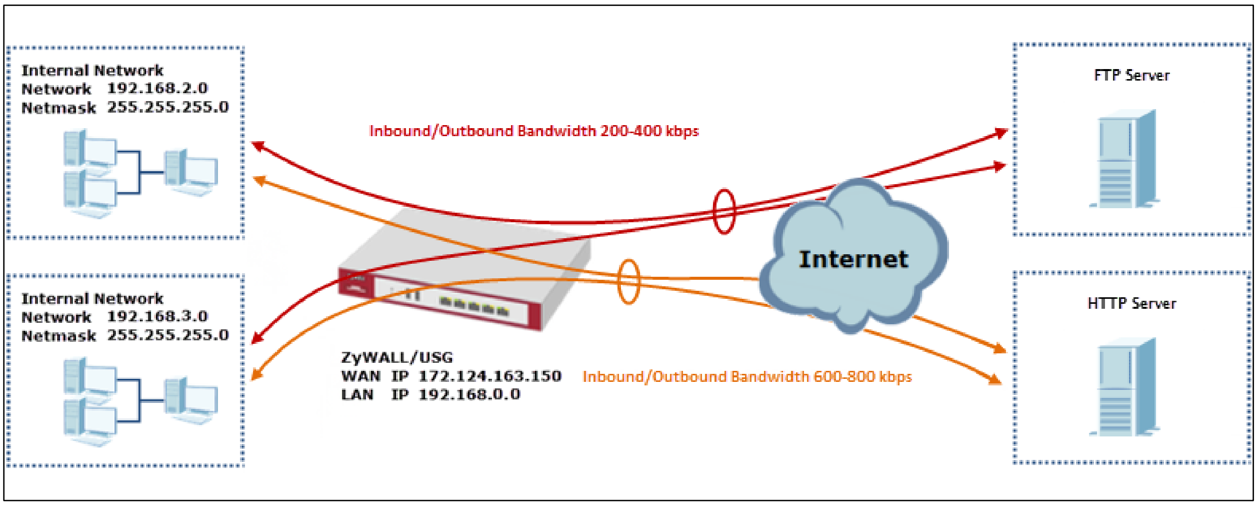
You have subscribed for the **UTM** service but the license is expired.

You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **UTM** license.

How to Configure Bandwidth Management for FTP and HTTP Traffic

This is an example of using ZyWALL/USG Bandwidth Management (BWM) to control the bandwidth allocation for FTP and HTTP traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions to allocate bandwidth for the matching packets. When the BWM is configured, you can limit bandwidth consuming services, such as FTP, while providing consistent HTTP service with bandwidth guarantees.

ZyWALL/USG with Bandwidth Management for HTTP and FTP Traffic Example



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. The total available bandwidth assumption is 1,600 kbps. This example was tested using USG310

Set Up the Bandwidth Management for FTP on the ZyWALL/USG

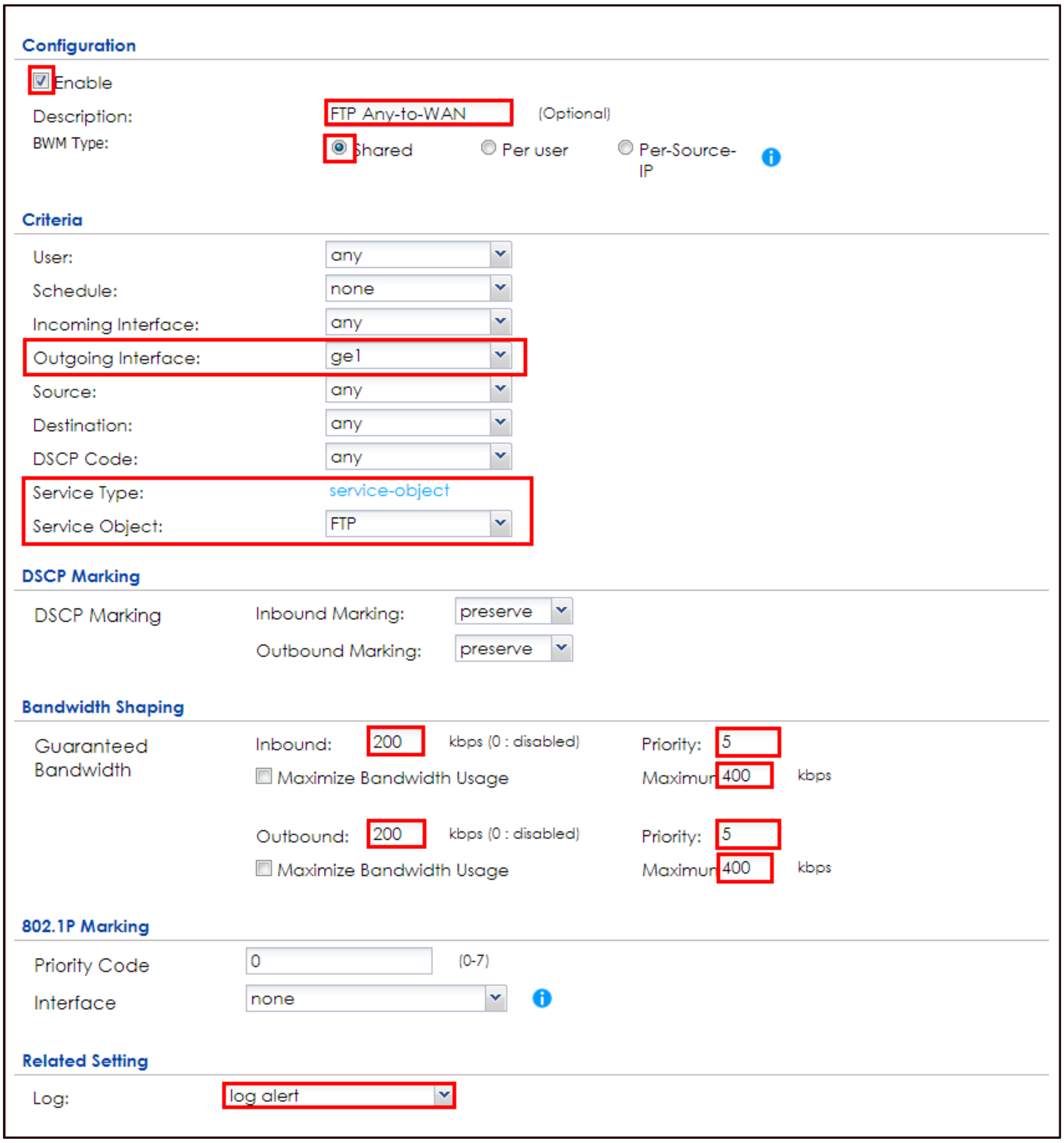
In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **FTP Any-to-WAN** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **wan1**. Select **Service Type** to be the **Service Object** and select **FTP** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 200 (kbps) and set **Priority 5** (low-to-medium). Set the **Maximum** to 400 (kbps). Set the **Guaranteed Bandwidth Outbound** to 200 (kbps) and set **Priority** 5. Set the **Maximum** to 400 (kbps).

In order to view the result later, set the **Log** setting to be **log alert**. Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy



Configuration

☑ Enable

Description: FTP Any-to-WAN (Optional)

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

Criteria

User:	any
Schedule:	none
Incoming Interface:	any
Outgoing Interface:	ge1
Source:	any
Destination:	any
DSCP Code:	any
Service Type:	service-object
Service Object:	FTP

DSCP Marking

DSCP Marking
Inbound Marking: preserve
Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth

Inbound: 200 kbps (0 : disabled) Priority: 5
□ Maximize Bandwidth Usage Maximum 400 kbps

Outbound: 200 kbps (0 : disabled) Priority: 5
□ Maximize Bandwidth Usage Maximum 400 kbps

802.1P Marking

Priority Code 0 (0-7)
Interface none

Related Setting

Log: log alert

Note: In Bandwidth Management, the highest priority is (1) the lowest priority is (7).

Set Up the Bandwidth Management for HTTP on the ZyWALL/USG

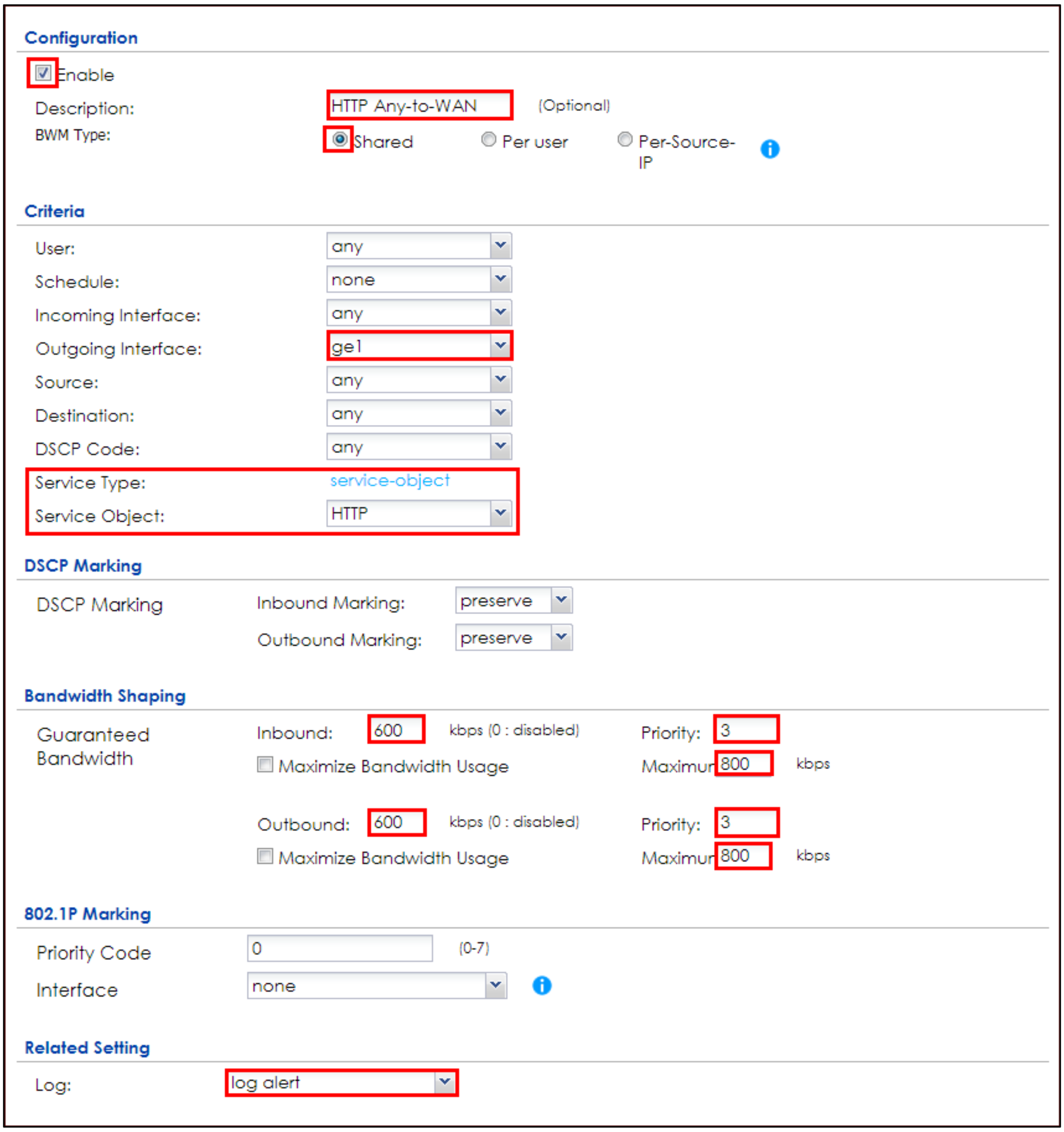
In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **HTTP Any-to-WAN** as the policy's Description (Optional).

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **wan1**. Select **Service Type** to be the **Service Object** and select **HTTP** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 600 (kbps) and set higher **Priority 3**. Set the **Maximum** to 800 (kbps). Set the **Guaranteed Bandwidth Outbound Priority 3**.

In order to view the result later, set the **Log** setting to be **log alert**. Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy



Configuration

☑ Enable

Description:	HTTP Any-to-WAN (Optional)
BWM Type:	● Shared ○ Per user ○ Per-Source-IP

Criteria

User:	any
Schedule:	none
Incoming Interface:	any
Outgoing Interface:	ge1
Source:	any
Destination:	any
DSCP Code:	any
Service Type:	service-object
Service Object:	HTTP

DSCP Marking

DSCP Marking	Inbound Marking:	preserve
	Outbound Marking:	preserve

Bandwidth Shaping

Guaranteed Bandwidth

Inbound:	600	kbps (0 : disabled)	Priority:	3	
□ Maximize Bandwidth Usage			Maximur	800	kbps
Outbound:	600	kbps (0 : disabled)	Priority:	3	
□ Maximize Bandwidth Usage			Maximur	800	kbps

802.1P Marking

Priority Code	0	(0-7)
Interface	none	

Related Setting

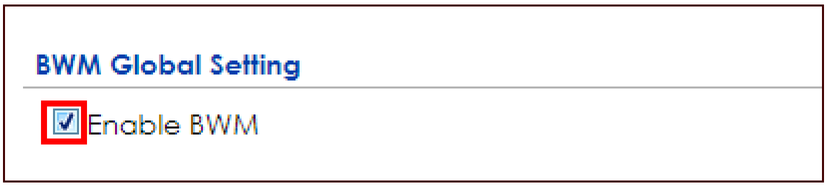
Log:	log alert

Note: In Bandwidth Management, the highest priority is (1) the lowest priority is (7).

Set Up the Bandwidth Management Global Setting on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > BWM Global Setting**, select **Enable**.

CONFIGURATION > BWM > BWM Global Setting

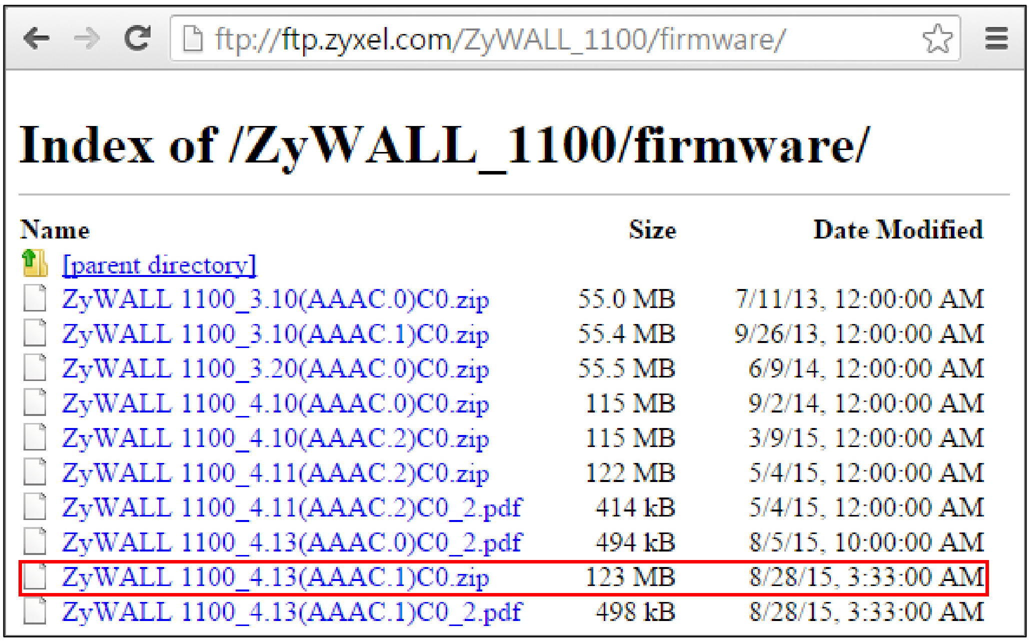


BWM Global Setting

☑ Enable BWM

Test the Result

Access the Internet to generate FTP traffic and HTTP traffic. In this example, a 123 MB file is downloading from an FTP server. The FTP file should download slowly.



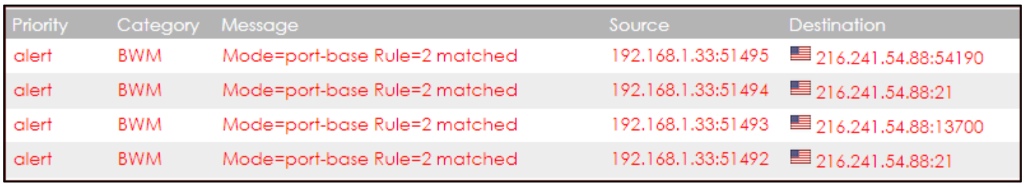
ftp://ftp.zyxel.com/ZyWALL_1100/firmware/

Index of /ZyWALL_1100/firmware/

Name	Size	Date Modified
[parent directory]		
ZyWALL 1100_3.10(AAAC.0)C0.zip	55.0 MB	7/11/13, 12:00:00 AM
ZyWALL 1100_3.10(AAAC.1)C0.zip	55.4 MB	9/26/13, 12:00:00 AM
ZyWALL 1100_3.20(AAAC.0)C0.zip	55.5 MB	6/9/14, 12:00:00 AM
ZyWALL 1100_4.10(AAAC.0)C0.zip	115 MB	9/2/14, 12:00:00 AM
ZyWALL 1100_4.10(AAAC.2)C0.zip	115 MB	3/9/15, 12:00:00 AM
ZyWALL 1100_4.11(AAAC.2)C0.zip	122 MB	5/4/15, 12:00:00 AM
ZyWALL 1100_4.11(AAAC.2)C0_2.pdf	414 kB	5/4/15, 12:00:00 AM
ZyWALL 1100_4.13(AAAC.0)C0_2.pdf	494 kB	8/5/15, 10:00:00 AM
ZyWALL 1100_4.13(AAAC.1)C0.zip	123 MB	8/28/15, 3:33:00 AM
ZyWALL 1100_4.13(AAAC.1)C0_2.pdf	498 kB	8/28/15, 3:33:00 AM

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

Monitor > Log



Priority	Category	Message	Source	Destination
alert	BWM	Mode=port-base Rule=2 matched	192.168.1.33:51495	216.241.54.88:54190
alert	BWM	Mode=port-base Rule=2 matched	192.168.1.33:51494	216.241.54.88:21
alert	BWM	Mode=port-base Rule=2 matched	192.168.1.33:51493	216.241.54.88:13700
alert	BWM	Mode=port-base Rule=2 matched	192.168.1.33:51492	216.241.54.88:21

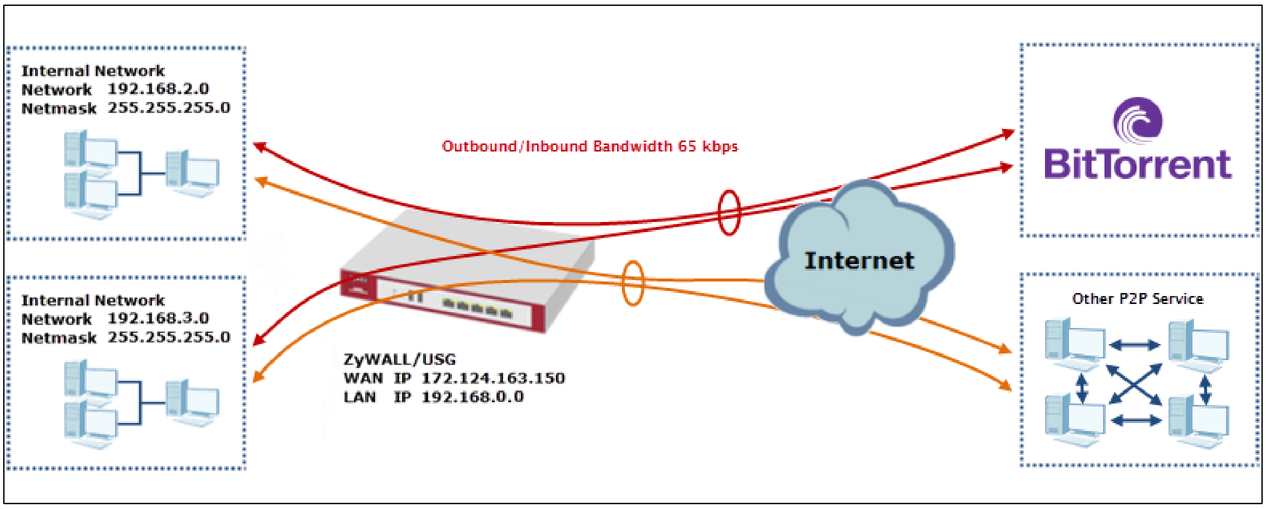
What Could Go Wrong?

If the “outbound” in the guaranteed bandwidth settings apply to traffic going from the connection initiator to the outgoing interface. “Inbound” refers to the reverse direction.

How to Limit BitTorrent or Other Peer-to-Peer Traffic

This is an example of using ZyWALL/USG Bandwidth Management (BWM) to control the bandwidth allocation for peer-to-peer traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions to allocate bandwidth for the matching packets. When the BWM is configured, you can limit bandwidth consuming Application traffic, such as Peer-to-Peer (P2P) service.

ZyWALL/USG with Bandwidth Management for Peer-to-Peer Traffic Example

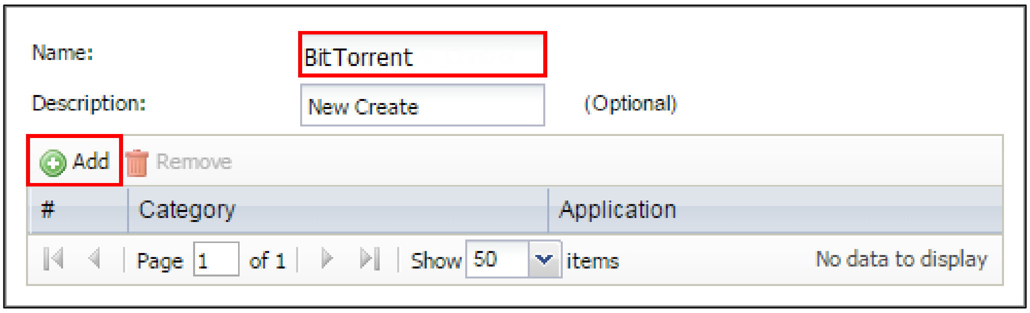


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. The total available bandwidth assumption is 1,600 kbps. This example was tested using USG310

Set Up the Application Patrol Profile on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > Application > Add Application Rule**. Configure a **Name** for you to identify the **Application Profile**. Then, click **Add** to create an **Application Object**.

CONFIGURATION > Object > Application > Add Application Rule



Name: BitTorrent

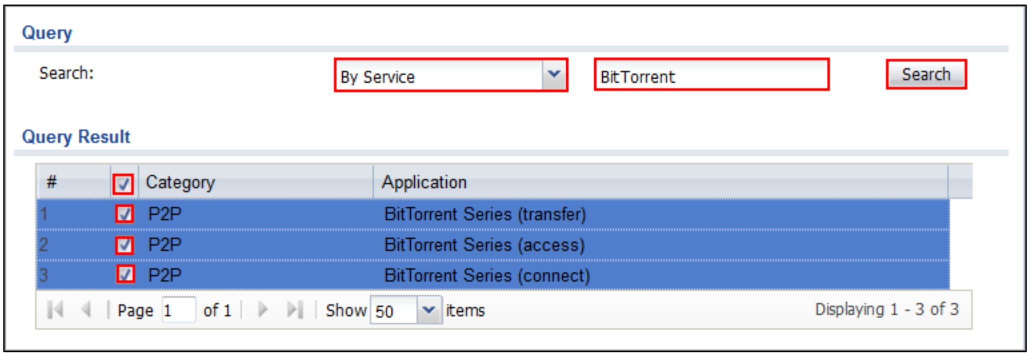
Description: New Create (Optional)

#	Category	Application

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

In the **Application Object**, select **By Service**, type a keyword and click **Search** to display all signatures containing that keyword. Select all **Query Result** and Click **OK**.

CONFIGURATION > Object > Application > Add Application Rule > Add Application Object



Query

Search: By Service | BitTorrent

Query Result

#	☑	Category	Application
1	☑	P2P	BitTorrent Series (transfer)
2	☑	P2P	BitTorrent Series (access)
3	☑	P2P	BitTorrent Series (connect)

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

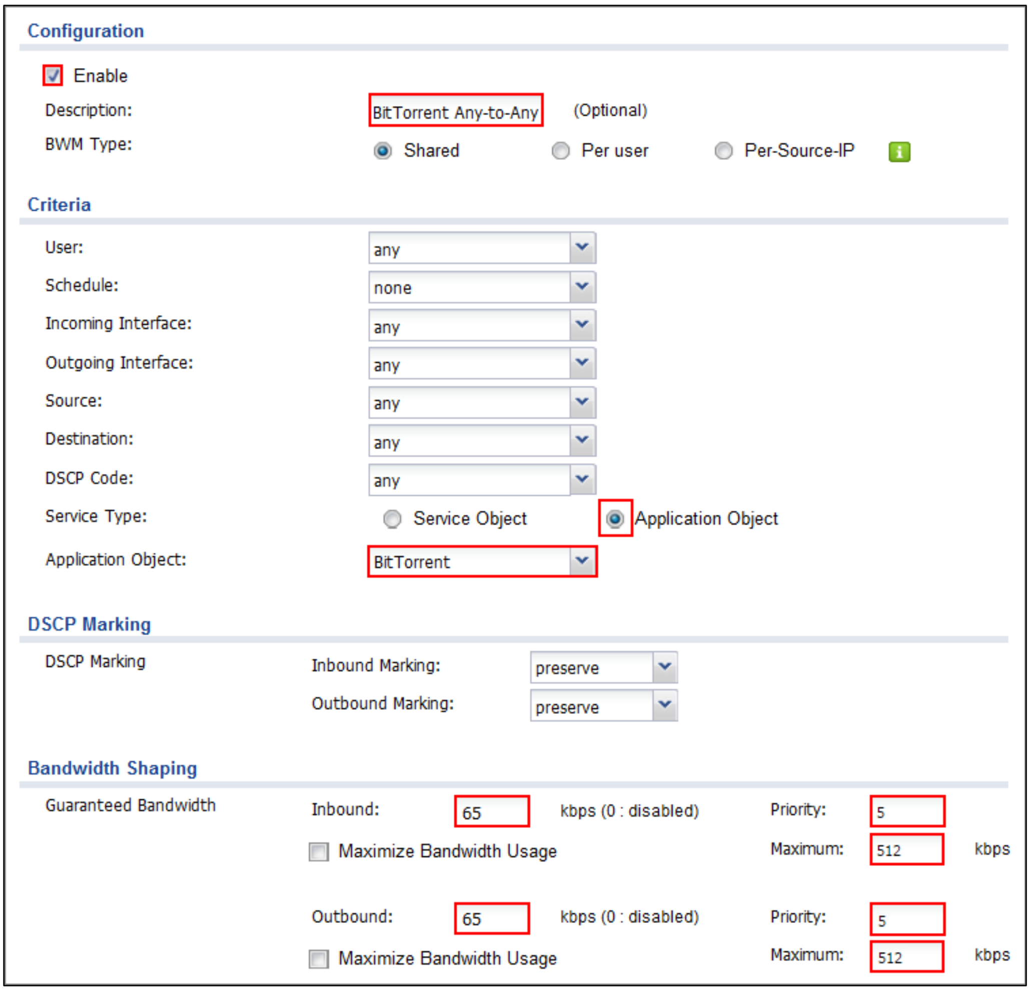
Set Up the Bandwidth Management for BitTorrent on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **BitTorrent Any-to-Any** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **wan1**. Select **Service Type** to be the **Service Object** and select **BitTorrent** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 65 (kbps) and set **Priority 5** (low-to-medium). Set the **Maximum** to 512(kbps). Set the **Guaranteed Bandwidth Outbound** to 65 (kbps) and set **Priority 5**. Set the **Maximum** to 512 (kbps). Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy



Configuration

☑ Enable

Description: BitTorrent Any-to-Any (Optional)

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

Criteria

User: any

Schedule: none

Incoming Interface: any

Outgoing Interface: any

Source: any

Destination: any

DSCP Code: any

Service Type: ○ Service Object ● Application Object

Application Object: BitTorrent

DSCP Marking

DSCP Marking Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth Inbound: 65 kbps (0 : disabled) Priority: 5

□ Maximize Bandwidth Usage Maximum: 512 kbps

Outbound: 65 kbps (0 : disabled) Priority: 5

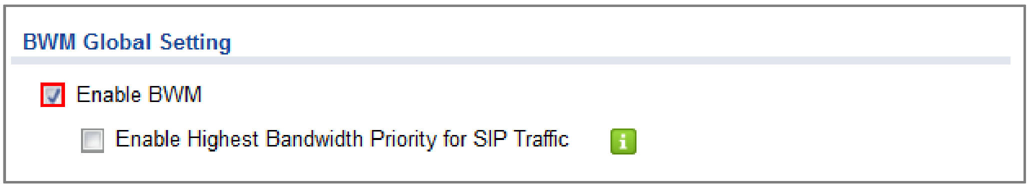
□ Maximize Bandwidth Usage Maximum: 512 kbps

Note: In Bandwidth Management, the highest priority is (1) the lowest priority is (7).

Set Up the Bandwidth Management Global Setting on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > BWM Global Setting**, select **Enable**.

CONFIGURATION > BWM > BWM Global Setting



BWM Global Setting

☑ Enable BWM

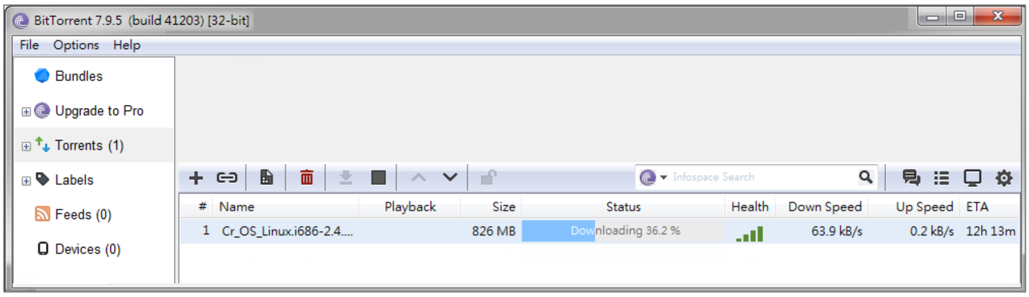
□ Enable Highest Bandwidth Priority for SIP Traffic

Test the Result

Download BitTorrent application for testing the result:

http://www.bittorrent.com/downloads

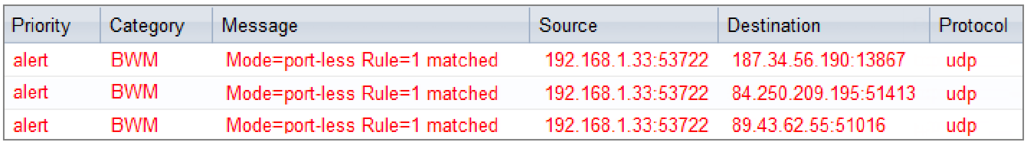
In this example, an 826 MB file is downloading, the **Down Speed** limited to maximum 65 kB/s.



#	Name	Playback	Size	Status	Health	Down Speed	Up Speed	ETA
1	Cr_OS_Linux.i686-2.4....		826 MB	Downloading 36.2 %		63.9 kB/s	0.2 kB/s	12h 13m

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

Monitor > Log

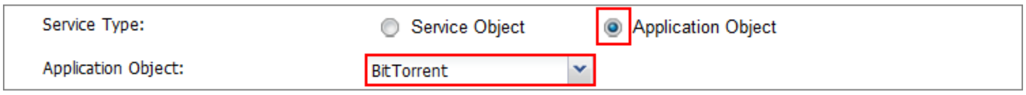


Priority	Category	Message	Source	Destination	Protocol
alert	BWM	Mode=port-less Rule=1 matched	192.168.1.33:53722	187.34.56.190:13867	udp
alert	BWM	Mode=port-less Rule=1 matched	192.168.1.33:53722	84.250.209.195:51413	udp
alert	BWM	Mode=port-less Rule=1 matched	192.168.1.33:53722	89.43.62.55:51016	udp

What Could Go Wrong?

If the "outbound" in the guaranteed bandwidth settings apply to traffic going from the connection initiator to the outgoing interface. “Inbound” refers to the reverse direction.

Make sure you have registered the **Application Patrol** service on the ZyWALL/USG to use **Application Object** as the **Service Type** in the bandwidth management rules.



Service Type: ○ Service Object ● Application Object

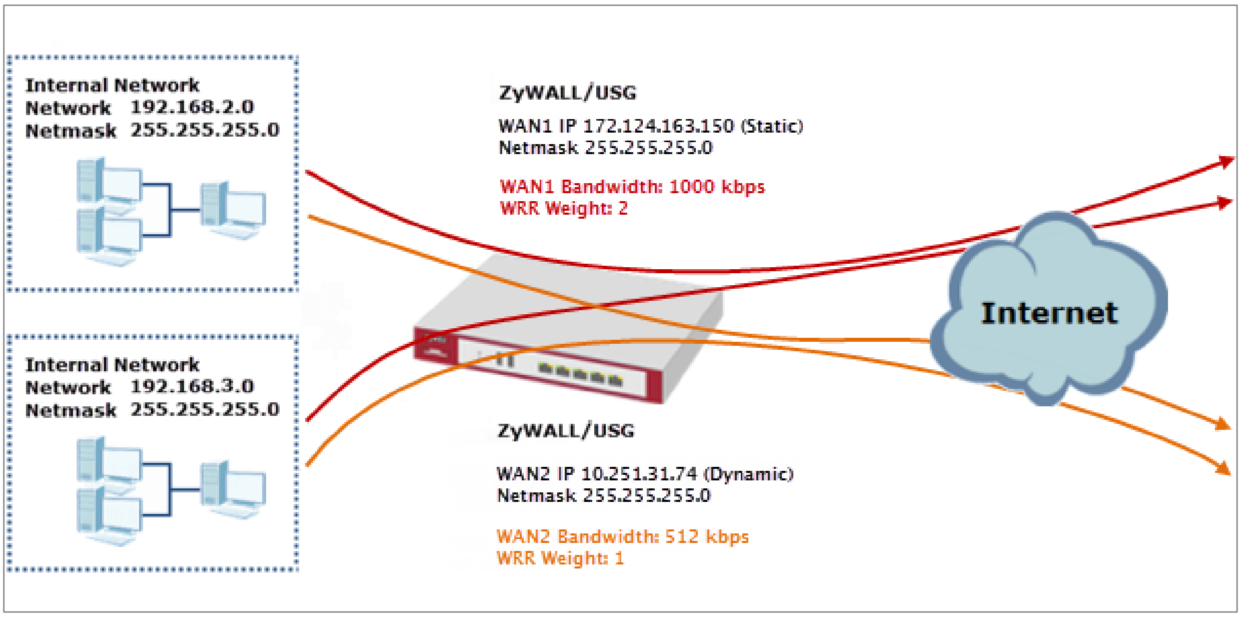
Application Object: BitTorrent

You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device’s Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **Application Patrol** license.

How to Configure a Trunk for WAN Load Balancing with a Static or Dynamic IP Address

This is an example of using ZyWALL/USG Trunk for two WAN connections to the Internet. The available bandwidth for the connections is 1000 kbps (wan1 with static IP address) and 512 Kbps (wan2 with dynamic IP address) respectively. As these connections have different bandwidths, we will use the Weighted Round Robin (WRR) algorithm to send traffic to wan1 and wan2 in a 2:1 ratio.

ZyWALL/USG with WAN Load Balancing Example

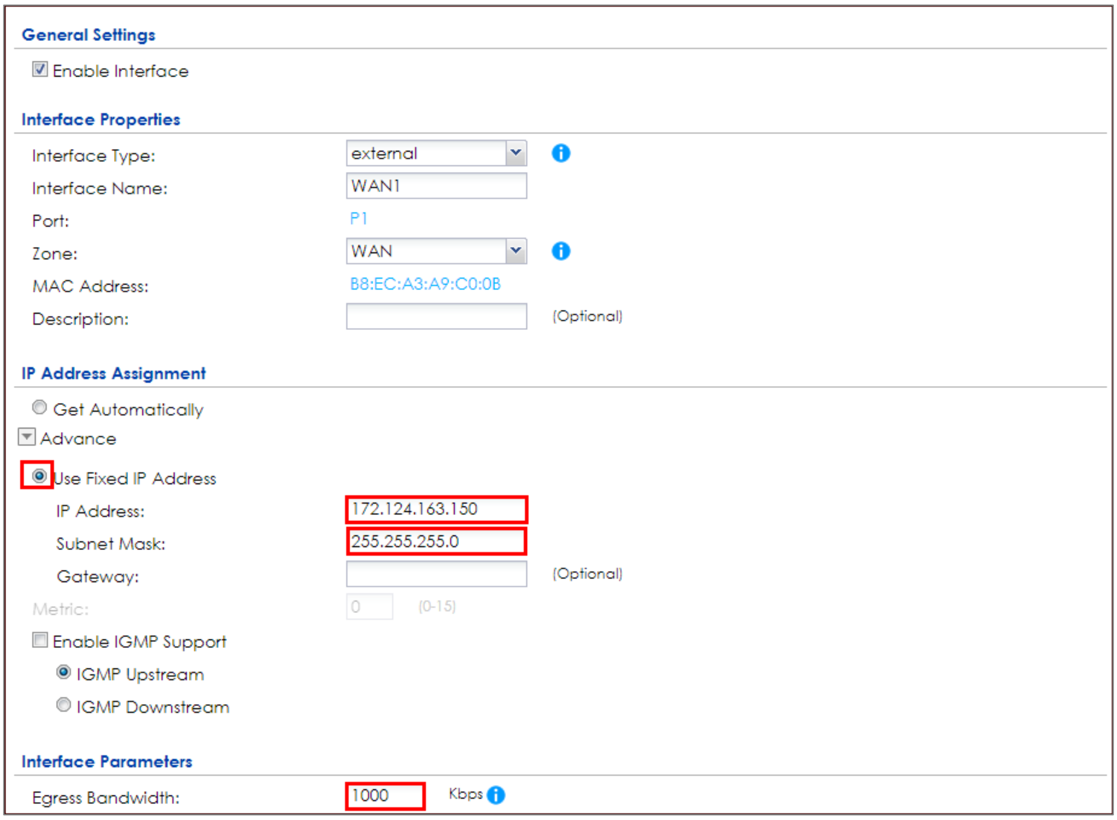


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Available Bandwidth on WAN1 Interfaces on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION** > **Interface** > **Ethernet** > **WAN1** > **Egress Bandwidth** and enter the available bandwidth (1000 kbps) in the **Egress Bandwidth** field. Click **OK**.

CONFIGURATION > **Interface** > **Ethernet** > **WAN1**



General Settings

☑ Enable Interface

Interface Properties

Interface Type:	external
Interface Name:	WAN1
Port:	P1
Zone:	WAN
MAC Address:	B8:EC:A3:A9:C0:0B
Description:	(Optional)

IP Address Assignment

○ Get Automatically

Advance

● Use Fixed IP Address

IP Address:	172.124.163.150
Subnet Mask:	255.255.255.0
Gateway:	(Optional)
Metric:	0 (0-15)

□ Enable IGMP Support

● IGMP Upstream

○ IGMP Downstream

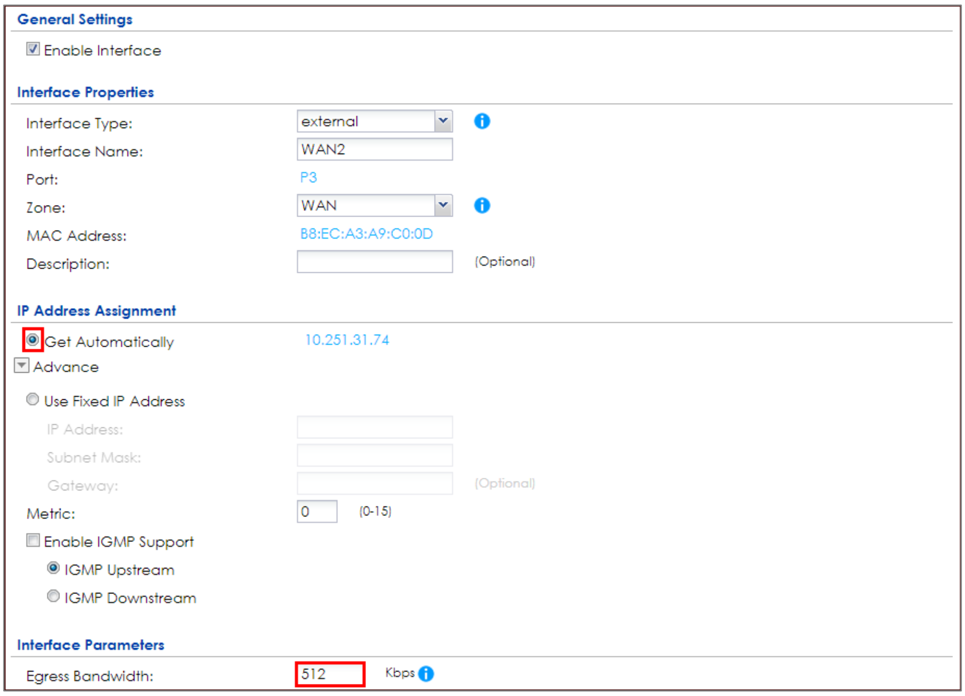
Interface Parameters

Egress Bandwidth: 1000 Kbps

Set Up the Available Bandwidth on WAN2 Interfaces on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION** > **Interface** > **Ethernet** > **WAN2** > **Egress Bandwidth** and enter the available bandwidth (512 kbps) in the **Egress Bandwidth** field. Click **OK**.

CONFIGURATION > Interface > Ethernet > WAN2



General Settings

☑ Enable Interface

Interface Properties

Interface Type:	external
Interface Name:	WAN2
Port:	P3
Zone:	WAN
MAC Address:	B8:EC:A3:A9:C0:0D
Description:	(Optional)

IP Address Assignment

● Get Automatically 10.251.31.74

Advance

○ Use Fixed IP Address

IP Address:	
Subnet Mask:	
Gateway:	(Optional)
Metric:	0 (0-15)

□ Enable IGMP Support

● IGMP Upstream

○ IGMP Downstream

Interface Parameters

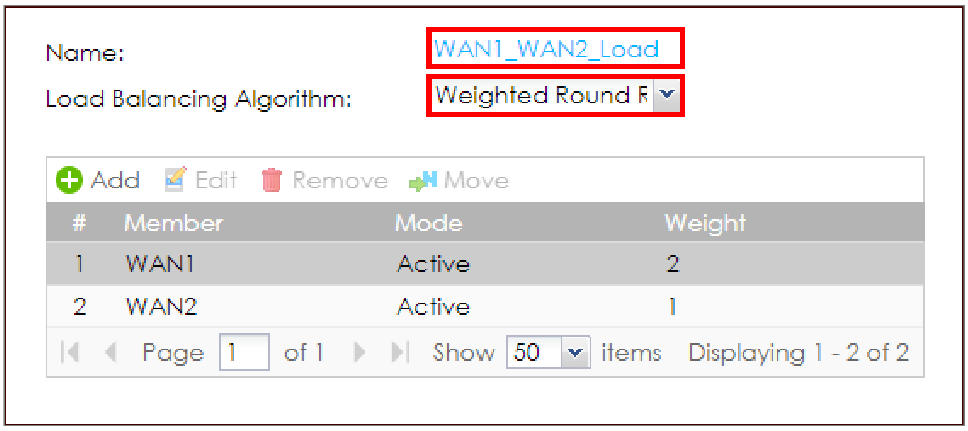
Egress Bandwidth: 512 Kbps

Set Up the WAN Trunk on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Interface > Trunk > User Configuration > Add Trunk.** Configure a **Name** for you to identify the Trunk profile and set the **Load Balancing Algorithm** field to be the **Weighted Round Robin**.

Add **WAN1** and enter **2** in the **Weight** column. Add **WAN2** and enter **1** in the **Weight** column. Click **OK** to return to the **Configuration** screen.

CONFIGURATION > Interface > Trunk > User Configuration > Add Trunk



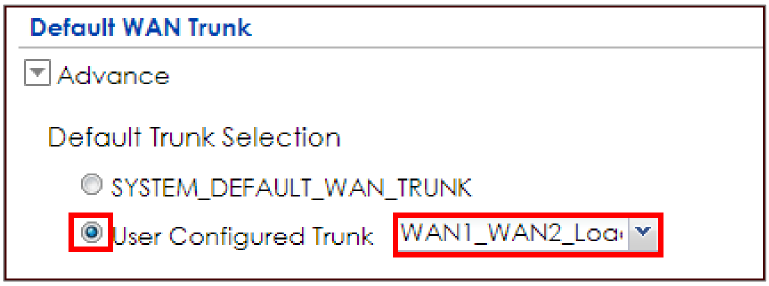
Name: WAN1_WAN2_Load

Load Balancing Algorithm: Weighted Round R

#	Member	Mode	Weight
1	WAN1	Active	2
2	WAN2	Active	1

In the **Configuration** screen, go to **Default WAN Trunk** section, select **User Configured Trunk** and select the newly created Trunk from the list box. Click **Apply**.

CONFIGURATION > Interface > Trunk > Default WAN Trunk



Default WAN Trunk

Advance

Default Trunk Selection

○ SYSTEM_DEFAULT_WAN_TRUNK

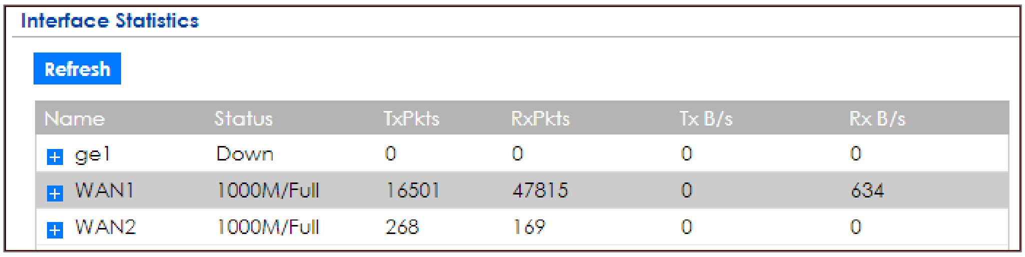
● User Configured Trunk: WAN1_WAN2_Loa

Test the Result

Browse any website to test the result.

The Weighted Round Robin (WRR) algorithm is best suited for situations where the bandwidths set for the two WAN interfaces are different. An interface with a larger weight (**WAN1**) gets more chances to transmit traffic than an interface with a smaller weight (**WAN2**).

MONITOR > Interface Summary > Interface Statistics



Interface Statistics

Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s
ge1	Down	0	0	0	0
WAN1	1000M/Full	16501	47815	0	634
WAN2	1000M/Full	268	169	0	0

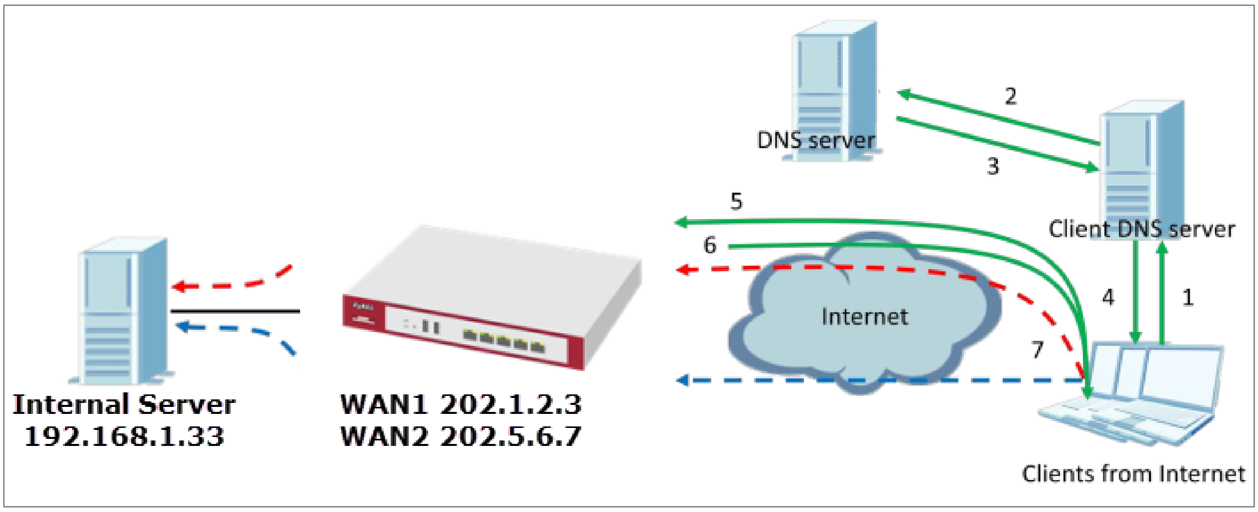
What Could Go Wrong?

If there is no traffic passing through either WAN1 or WAN2 interfaces, check that the **Mode** of both WAN1 & WAN2 should be **Active**. If a trunk is in **Passive** mode, the ZyWALL/USG will use this connection only when all of the connections set to **Active** mode are down.

How to Configure DNS Inbound Load Balancing to balance DNS Queries Among Interfaces

This is an example of using the ZyWALL/USG dynamically responding to DNS query messages with its least loaded interface's IP address. The DNS query senders will then transmit packets to that interface instead of an interface that has a heavy load. This example assumes that your company's domain name is www.example.com. You want your ZyWALL/USG's WAN1 (202.1.2.3) and WAN2 (202.5.6.7) to use DNS inbound load balancing to balance traffic loading coming from the Internet.

ZyWALL/USG with DNS Inbound Load Balancing Example

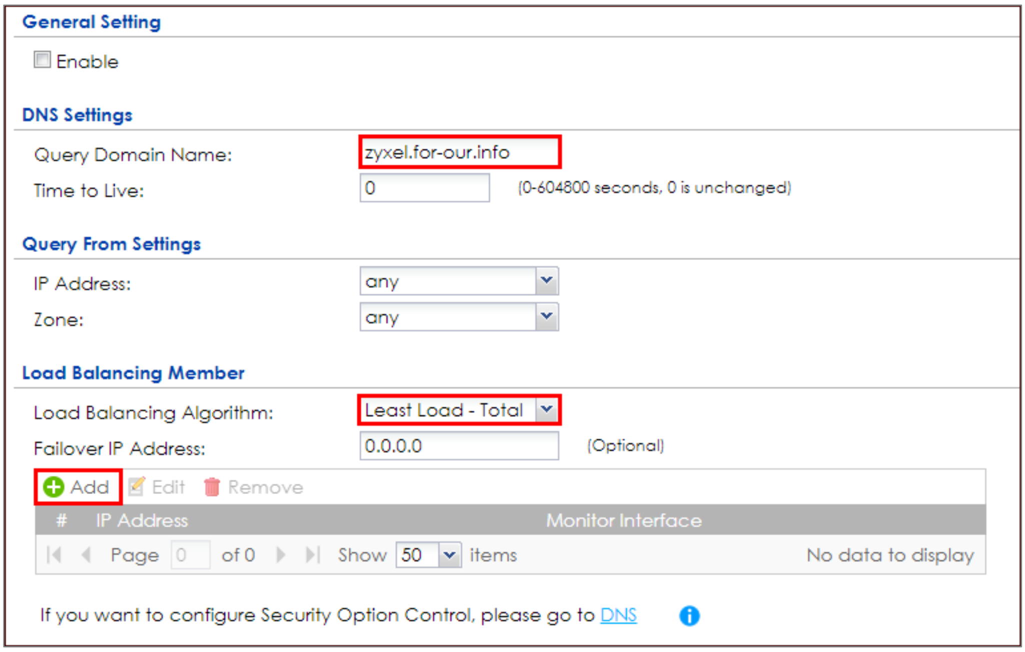


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the DNS Inbound Load Balancing on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > DNS Inbound LB**. Edit the **Query Domain Name**, set the **Load Balancing Algorithm** field to be the **Least Load - Total**. Click **Add** to create a new **Load Balancing Member**.

CONFIGURATION > Network > DNS Inbound LB



General Setting

□ Enable

DNS Settings

Query Domain Name: zyxel.for-our.info

Time to Live: 0 (0-604800 seconds, 0 is unchanged)

Query From Settings

IP Address: any

Zone: any

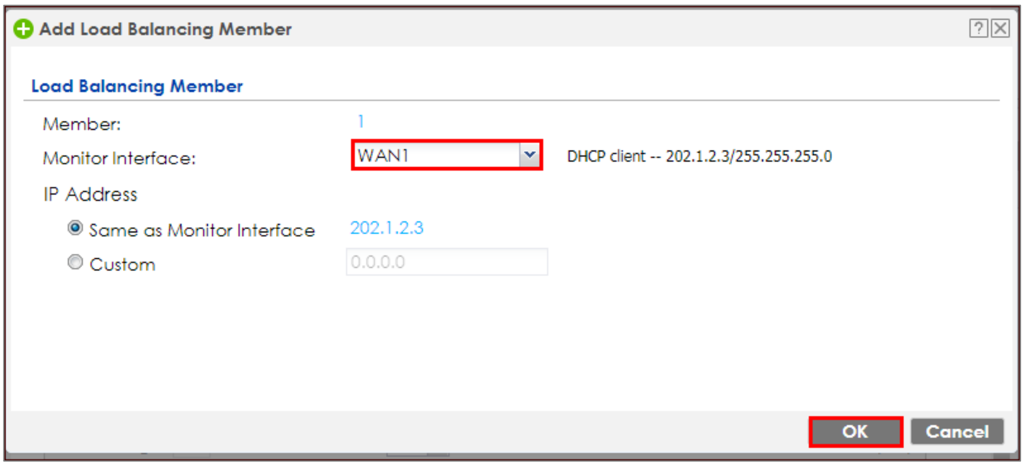
Load Balancing Member

Load Balancing Algorithm: Least Load - Total

Failover IP Address: 0.0.0.0 (Optional)

If you want to configure Security Option Control, please go to DNS

CONFIGURATION > Network > DNS Inbound LB



Add Load Balancing Member

Load Balancing Member

Member: 1

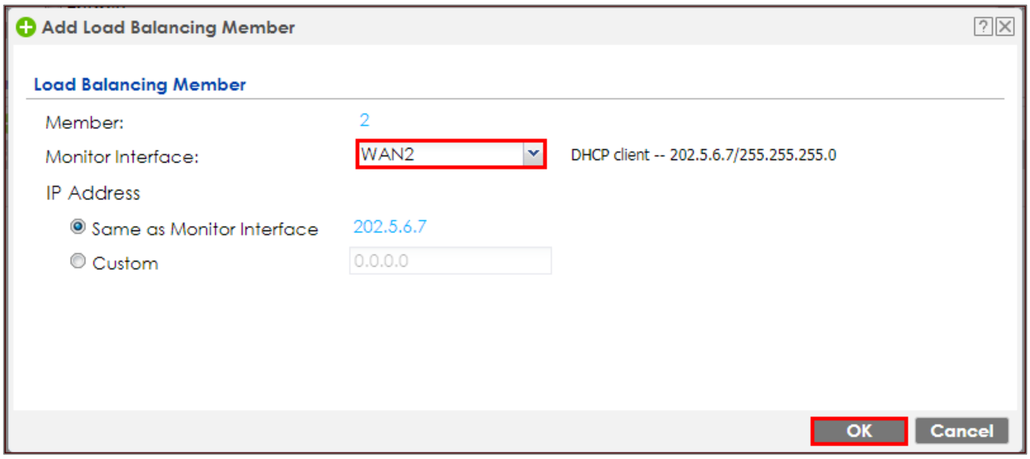
Monitor Interface: WAN1 DHCP client -- 202.1.2.3/255.255.255.0

IP Address

● Same as Monitor Interface 202.1.2.3

○ Custom 0.0.0.0

CONFIGURATION > Network > DNS Inbound LB


Add Load Balancing Member

Load Balancing Member

Member: 2

Monitor Interface: WAN2 DHCP client -- 202.5.6.7/255.255.255.0

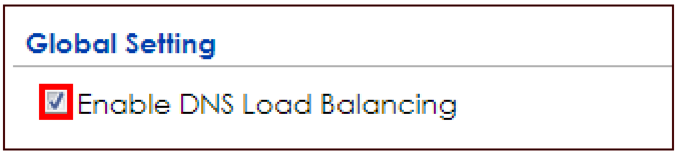
IP Address

● Same as Monitor Interface 202.5.6.7

○ Custom 0.0.0.0

Go to **the Global Setting page to select Enable DNS Load Balancing.**

CONFIGURATION > Network > DNS Inbound LB

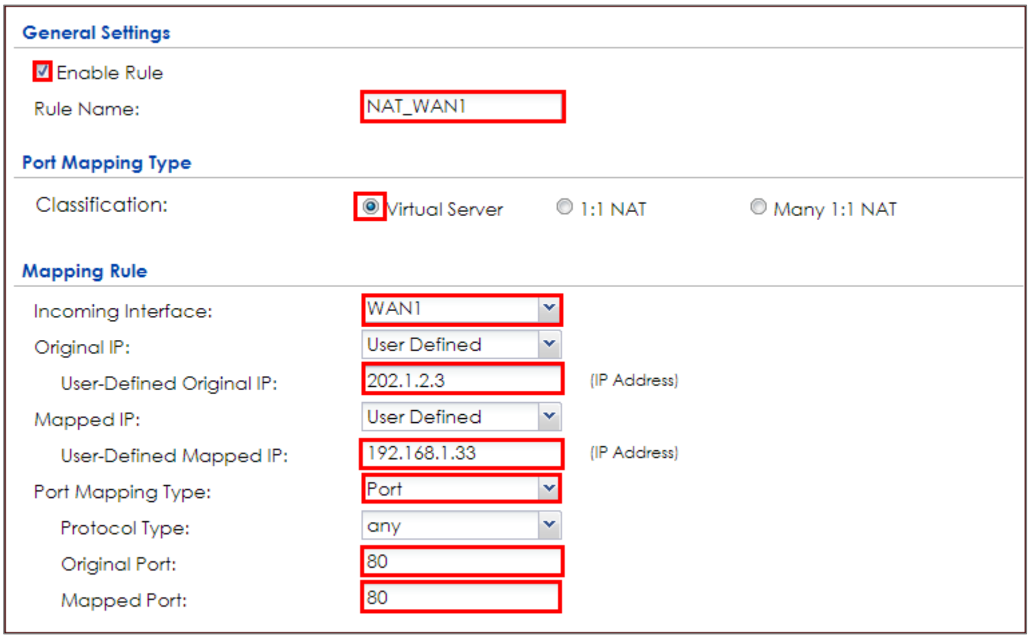

Global Setting

☑ Enable DNS Load Balancing

Set Up the NAT Rule on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > NAT**. Configure the **Virtual Server** to forward the traffic from WAN to Internal Server (192.168.1.33). Click **OK**.

CONFIGURATION > Network > NAT



General Settings

☑ Enable Rule

Rule Name: NAT_WAN1

Port Mapping Type

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

Mapping Rule

Incoming Interface: WAN1

Original IP: User Defined

User-Defined Original IP: 202.1.2.3 (IP Address)

Mapped IP: User Defined

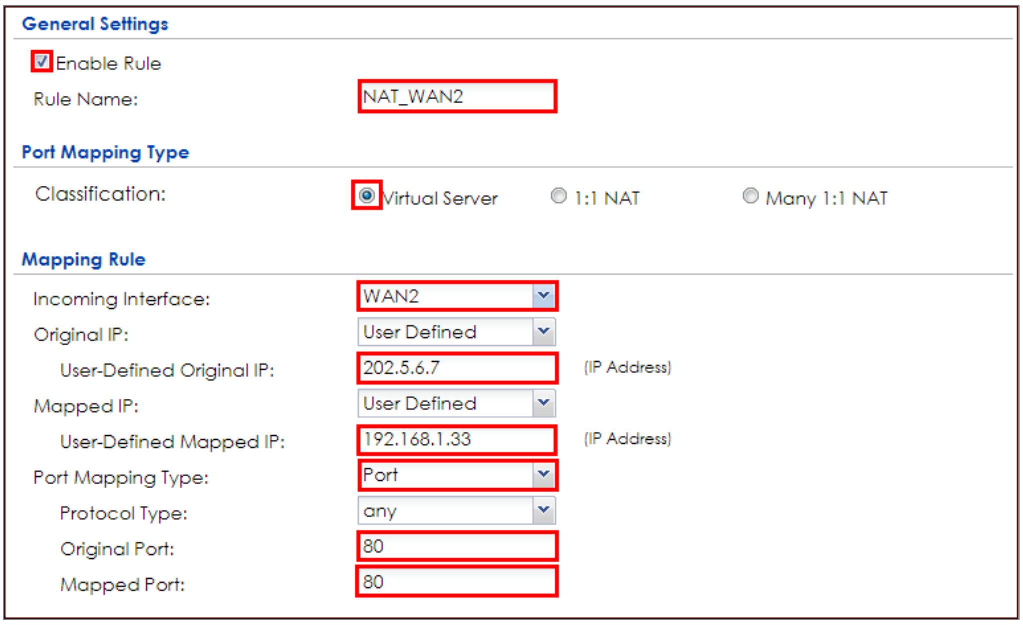
User-Defined Mapped IP: 192.168.1.33 (IP Address)

Port Mapping Type: Port

Protocol Type: any

Original Port: 80

Mapped Port: 80



General Settings

☑ Enable Rule

Rule Name: NAT_WAN2

Port Mapping Type

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

Mapping Rule

Incoming Interface: WAN2

Original IP: User Defined

User-Defined Original IP: 202.5.6.7 (IP Address)

Mapped IP: User Defined

User-Defined Mapped IP: 192.168.1.33 (IP Address)

Port Mapping Type: Port

Protocol Type: any

Original Port: 80

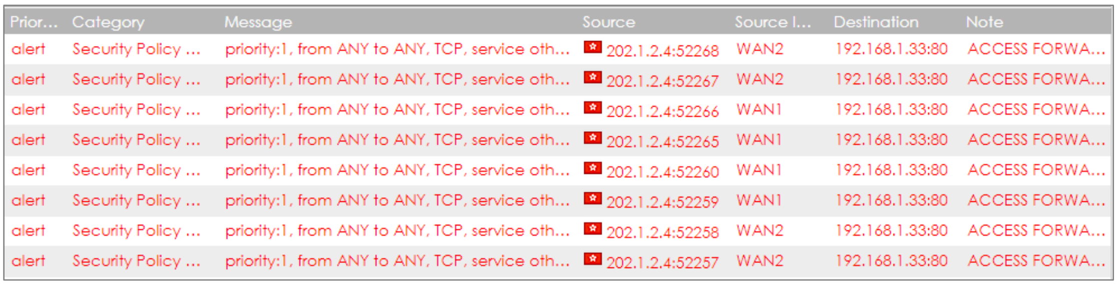
Mapped Port: 80

Test the Result

Open the browser and query **http://zyxel.for-our.info/.**

Create a **Security Policy** in order to view the testing result. Set **Destination** to be the Internal Server IP address (192.168.1.33 in this example) and set **Log** type to be the **Log Alert**.

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below. The **Source Interface** is the WAN1 or WAN2 interface which is handling the least amount of outgoing and incoming traffic.



Prior...	Category	Message	Source	Source I...	Destination	Note
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52268	WAN2	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52267	WAN2	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52266	WAN1	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52265	WAN1	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52260	WAN1	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52259	WAN1	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52258	WAN2	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52257	WAN2	192.168.1.33:80	ACCESS FORWA...

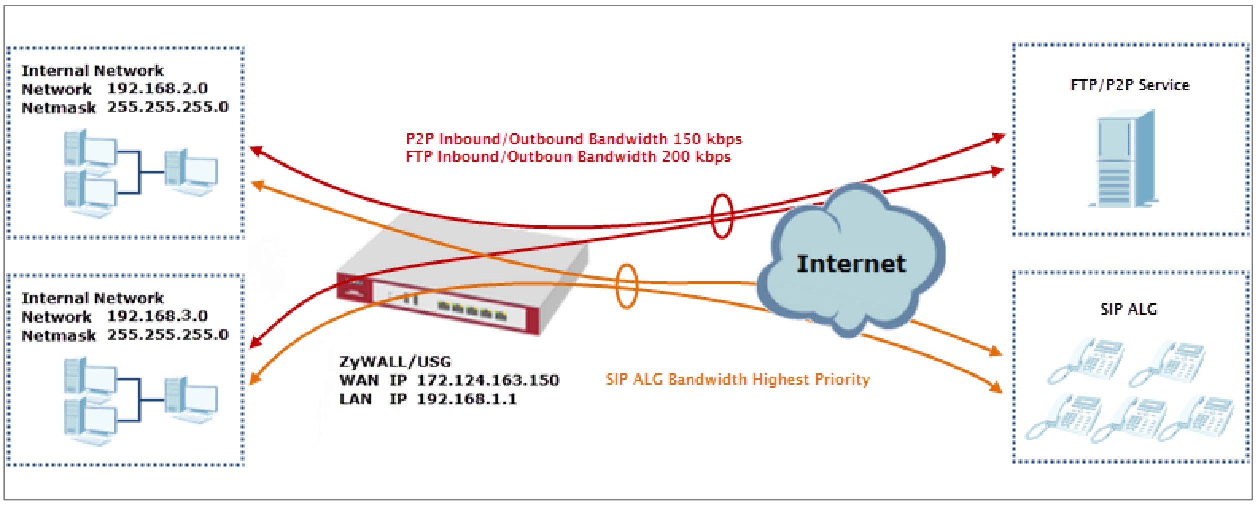
What Could Go Wrong?

If you cannot access the Internal Server, please check that the NAT configuration matches the Internal Server IP address and Port number. If the NAT configuration is correct, please check the system status of your Internal Server is up.

How to Manage Voice Traffic

This is an example of using Application Layer Gateway (ALG) to allow the SIP (Session Initiation Protocol) voice traffic through the ZyWALL/USG. To achieve high-quality voice transmissions, use ZyWALL/USG provides Bandwidth Management (BWM) function to effectively manage bandwidth according to flexible criteria. You can limit bandwidth consuming services, such as Peer-to-Peer (P2P) and FTP service while providing a higher priority and consistent bandwidth for voice traffic.

ZyWALL/USG with Voice Traffic Management Example

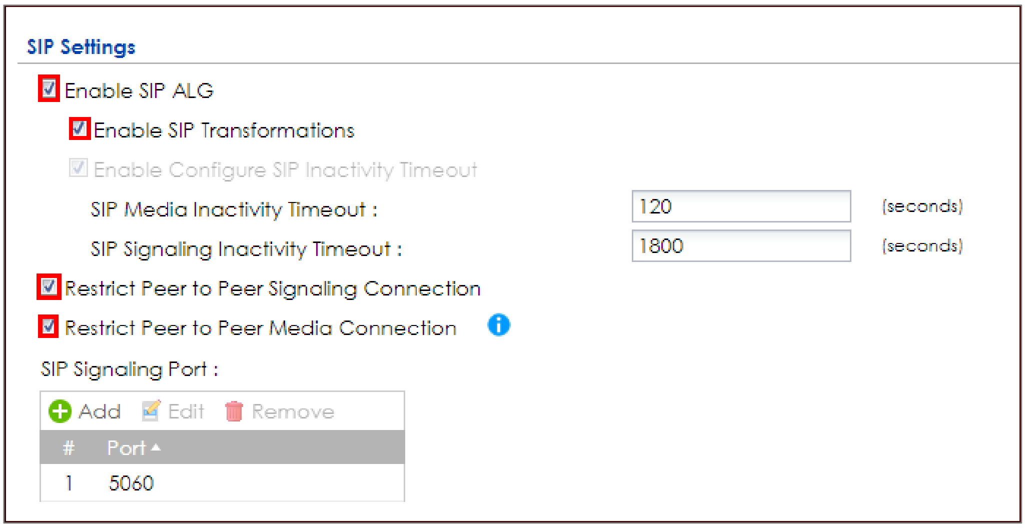


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the SIP ALG on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > SIP > SIP Settings**, select **Enable SIP ALG**, **Enable SIP Transformations** (optional), **Restrict Peer to Peer Signaling Connection** and **Restrict Peer to Peer Media Connection**. Make sure the **SIP Signaling Port** is configured the same as your VoIP phone SIP signaling port. Click **Apply.**

CONFIGURATION > BWM > Configuration > Add Policy



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 :

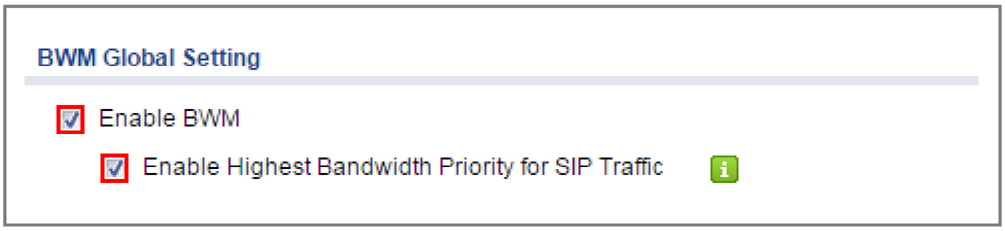
#	Port ▲
1	5060

Note: If you are using a custom or additional UDP port number (not 5060) for SIP traffic, use the **Add** icon to add **SIP Signaling Port** numbers.

Set Up the Bandwidth Management for SIP on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > BWM Global Settings,** select **Enable BWM** and **Enable Highest Bandwidth Priority for SIP Traffic**.

CONFIGURATION > BWM > BWM Global Settings > Enable BWM



BWM Global Setting

☑ Enable BWM

☑ Enable Highest Bandwidth Priority for SIP Traffic

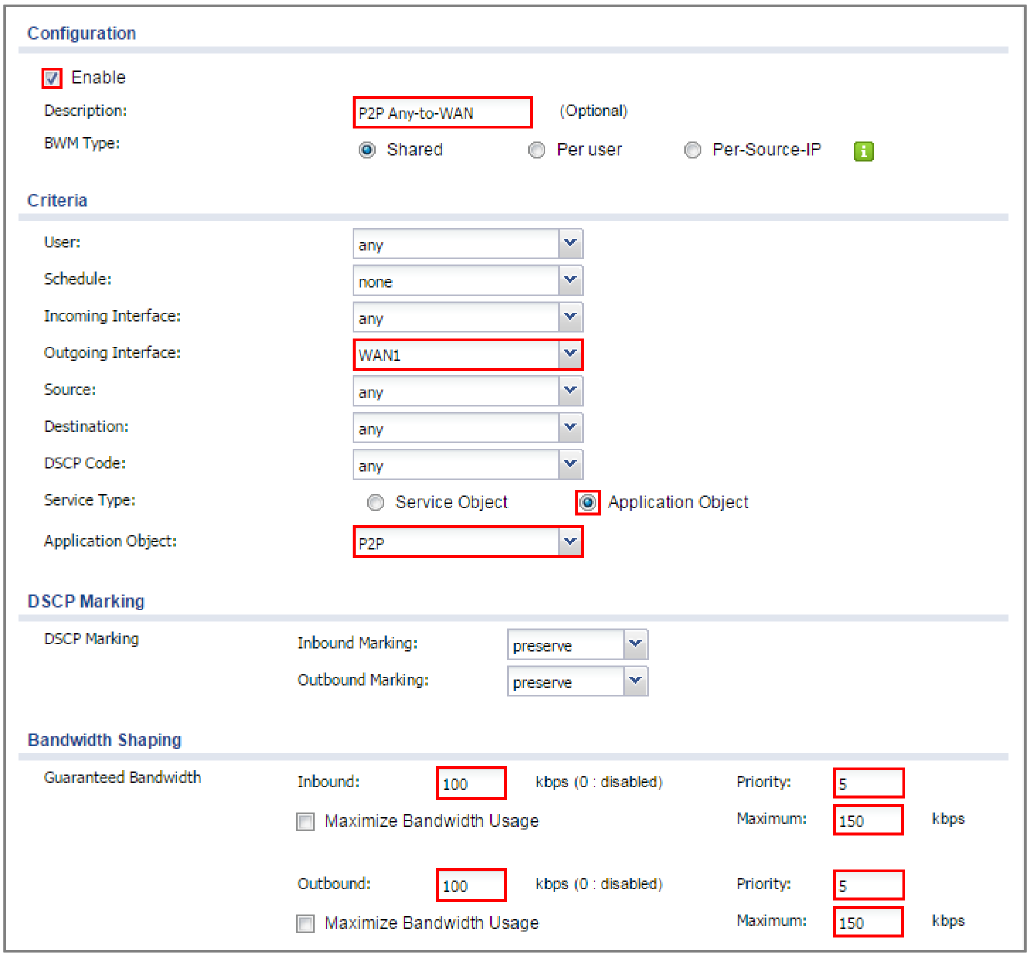
Set Up the Bandwidth Management for P2P on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **P2P Any-to-WAN** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **WAN1**. Select **Service Type** to be the **Application Object** and select **P2P** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 100 (kbps) and set **Priority** 5. Set the **Maximum** to 150 (kbps). Set the **Guaranteed Bandwidth Outbound** to 100 (kbps) and set **Priority** 5. Set the **Maximum** to 150 (kbps). Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy



Configuration

☑ Enable

Description: P2P Any-to-WAN (Optional)

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

Criteria

User: any

Schedule: none

Incoming Interface: any

Outgoing Interface: WAN1

Source: any

Destination: any

DSCP Code: any

Service Type: ○ Service Object ● Application Object

Application Object: P2P

DSCP Marking

DSCP Marking Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth Inbound: 100 kbps (0 : disabled) Priority: 5

□ Maximize Bandwidth Usage Maximum: 150 kbps

Outbound: 100 kbps (0 : disabled) Priority: 5

□ Maximize Bandwidth Usage Maximum: 150 kbps

Note: In Bandwidth Shaping, the highest priority is (1) the lowest priority is (7).

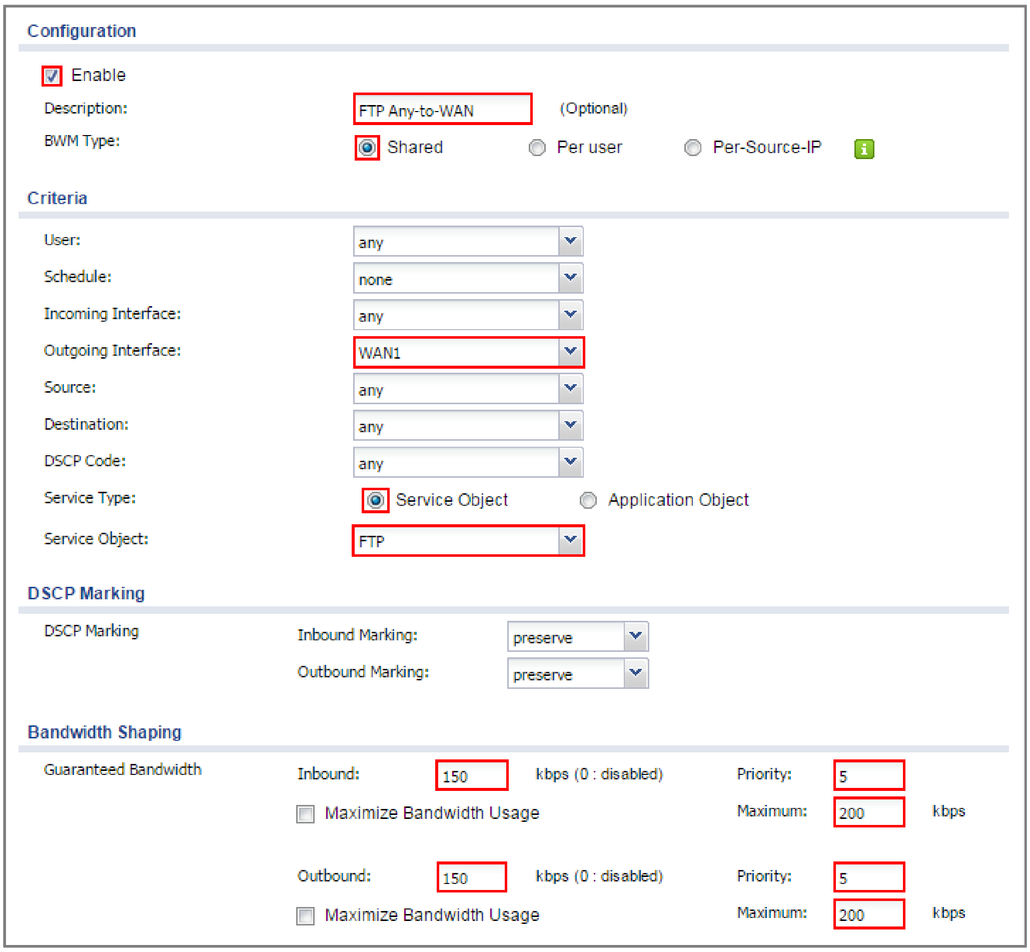
Set Up the Bandwidth Management for FTP on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **FTP Any-to-Any** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **WAN1**. Select **Service Type** to be the **Service Object** and select **FTP** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 150 (kbps) and set **Priority** 5. Set the **Maximum** to 200 (kbps). Set the **Guaranteed Bandwidth Outbound** to 150 (kbps) and set **Priority** 5. Set the **Maximum** to 200 (kbps). Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy



Configuration

☑ Enable

Description: FTP Any-to-WAN (Optional)

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

Criteria

User: any

Schedule: none

Incoming Interface: any

Outgoing Interface: WAN1

Source: any

Destination: any

DSCP Code: any

Service Type: ● Service Object ○ Application Object

Service Object: FTP

DSCP Marking

DSCP Marking Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth Inbound: 150 kbps (0 : disabled) Priority: 5

□ Maximize Bandwidth Usage Maximum: 200 kbps

Outbound: 150 kbps (0 : disabled) Priority: 5

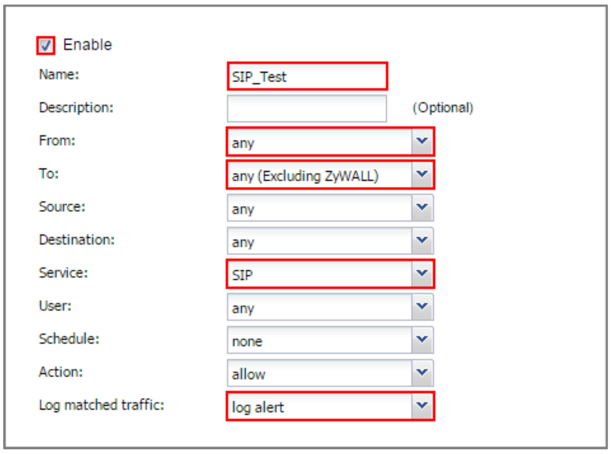
□ Maximize Bandwidth Usage Maximum: 200 kbps

Note: In Bandwidth Shaping, the highest priority is (1) the lowest priority is (7).

Test the Result

Add a **Security Policy** rule to view the SIP log:

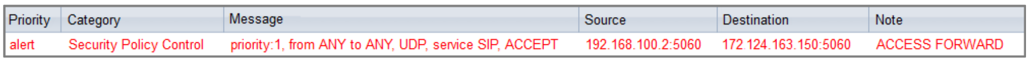
CONFIGURATION > BWM > Configuration > Add Policy



☑ Enable	
Name:	SIP_Test
Description:	(Optional)
From:	any
To:	any (Excluding ZyWALL)
Source:	any
Destination:	any
Service:	SIP
User:	any
Schedule:	none
Action:	allow
Log matched traffic:	log alert

Dial Phone Number 1001 (192.168.10.2 in this example) from Phone Number 1002 (192.168.100.2 in this example), go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below. The **Destination** IP address is the SIP Server IP address.

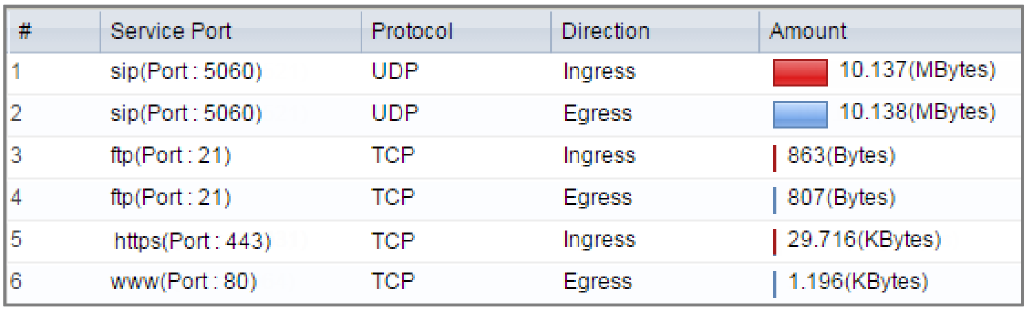
Monitor > Log



Priority	Category	Message	Source	Destination	Note
alert	Security Policy Control	priority:1, from ANY to ANY, UDP, service SIP, ACCEPT	192.168.100.2:5060	172.124.163.150:5060	ACCESS FORWARD

Go to the ZyWALL/USG **Monitor > Traffic Statics** and review the SIP traffic and other services to optimize the **Guaranteed** and **Maximum BMW** of bandwidth consuming services.

Monitor > Traffic Statics

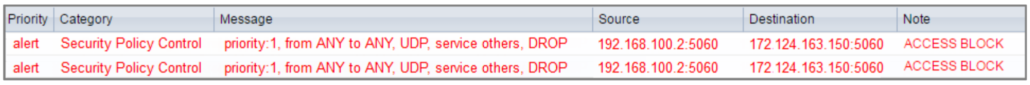


#	Service Port	Protocol	Direction	Amount
1	sip(Port : 5060)	UDP	Ingress	🟥 10.137(MBytes)
2	sip(Port : 5060)	UDP	Egress	🟦 10.138(MBytes)
3	ftp(Port : 21)	TCP	Ingress	863(Bytes)
4	ftp(Port : 21)	TCP	Egress	807(Bytes)
5	https(Port : 443)	TCP	Ingress	29.716(KBytes)
6	www(Port : 80)	TCP	Egress	1.196(KBytes)

What Could Go Wrong?

If you see [alert] log message such as below, the voice traffic is blocked by the priority 1 **Security Policy.** The ZyWALL/USG checks the security policy in order and applies the first security policy the traffic matches. If the voice traffic matches a policy that comes earlier in the list, it may be unexpectedly blocked. Please change your policy setting or move the voice traffic policy to the higher priority.

Monitor > Log

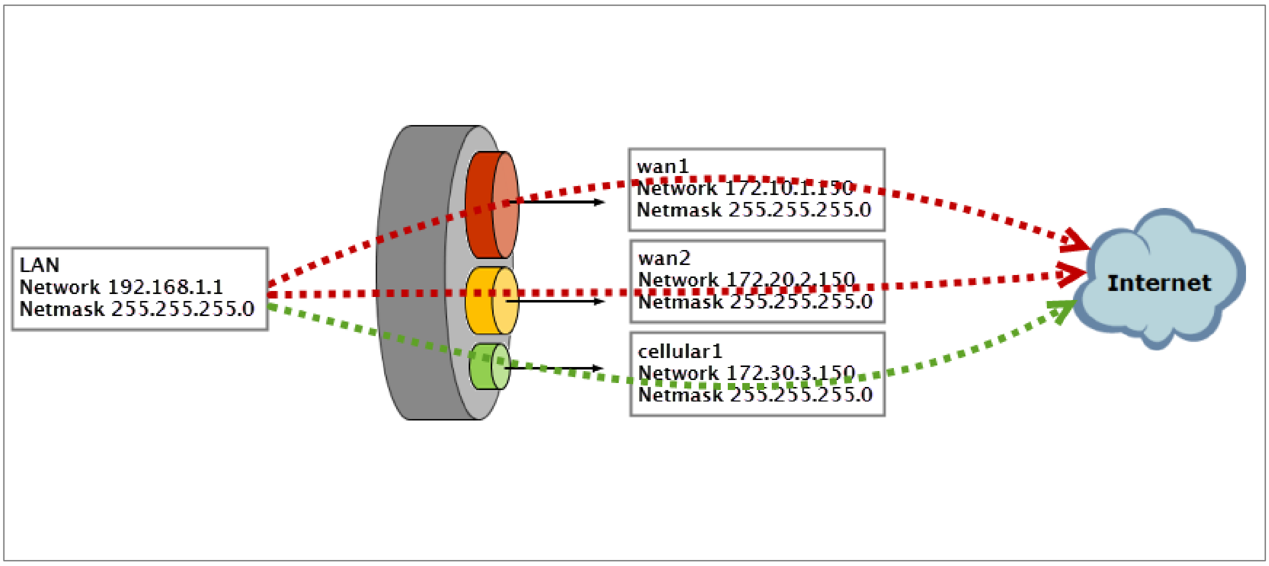


Priority	Category	Message	Source	Destination	Note
alert	Security Policy Control	priority:1, from ANY to ANY, UDP, service others, DROP	192.168.100.2:5060	172.124.163.150:5060	ACCESS BLOCK
alert	Security Policy Control	priority:1, from ANY to ANY, UDP, service others, DROP	192.168.100.2:5060	172.124.163.150:5060	ACCESS BLOCK

How to Configure the 3G/LTE Interface on the ZyWALL/USG as a WAN Backup

This is an example of using ZyWALL/USG to configure 3G/LTE interface as a WAN backup that ensures the ZyWALL/USG provides the continuously Internet connections when the primary WAN interface is down. After configuration, it can provide additional mobile broadband WAN connectivity or a redundant link for maximum reliability.

ZyWALL/USG with 3G/LTE Interface as a WAN Backup Example



Note: This example includes weighted load balancing (Weighted Round Robin) so that most of your Internet traffic is handled by ISP connected to wan1 before it fails over to 3G/LTE.

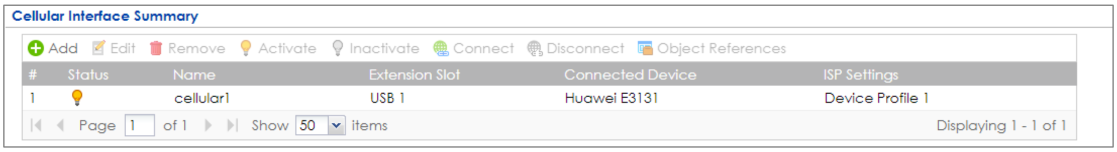
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the 3G/LTE Interface on the ZyWALL/USG

Connect a compatible mobile broadband USB device to use a cellular connection.

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Cellular**, the connected device will automatically display in the **Cellular Interface Summary**. Click **Activate** and then the **Apply** button at the bottom of this page.

CONFIGURATION > Network > Interface > Cellular > Activate



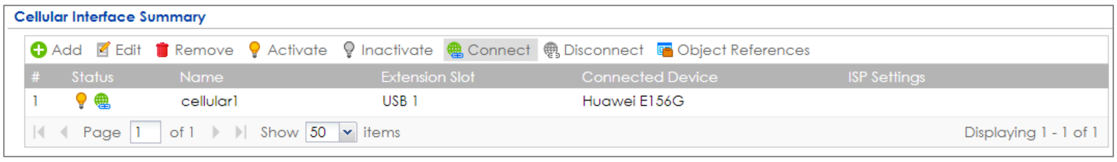
Cellular Interface Summary

#	Status	Name	Extension Slot	Connected Device	ISP Settings
1	●	cellular1	USB 1	Huawei E3131	Device Profile 1

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

The default **Connectivity** method is **Nailed-Up**. The connection should always be up after you activate the cellular interface. You can click **Edit** and go to the **Connectivity** section to clear the **Nailed-Up** check box to have the ZyWALL/USG to establish the connection only when there is traffic.

CONFIGURATION > Network > Interface > Cellular > Connect

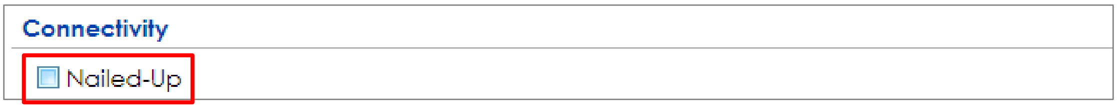


Cellular Interface Summary

#	Status	Name	Extension Slot	Connected Device	ISP Settings
1	● ●	cellular1	USB 1	Huawei E156G	

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

CONFIGURATION > Network > Interface > Cellular > Edit



Connectivity

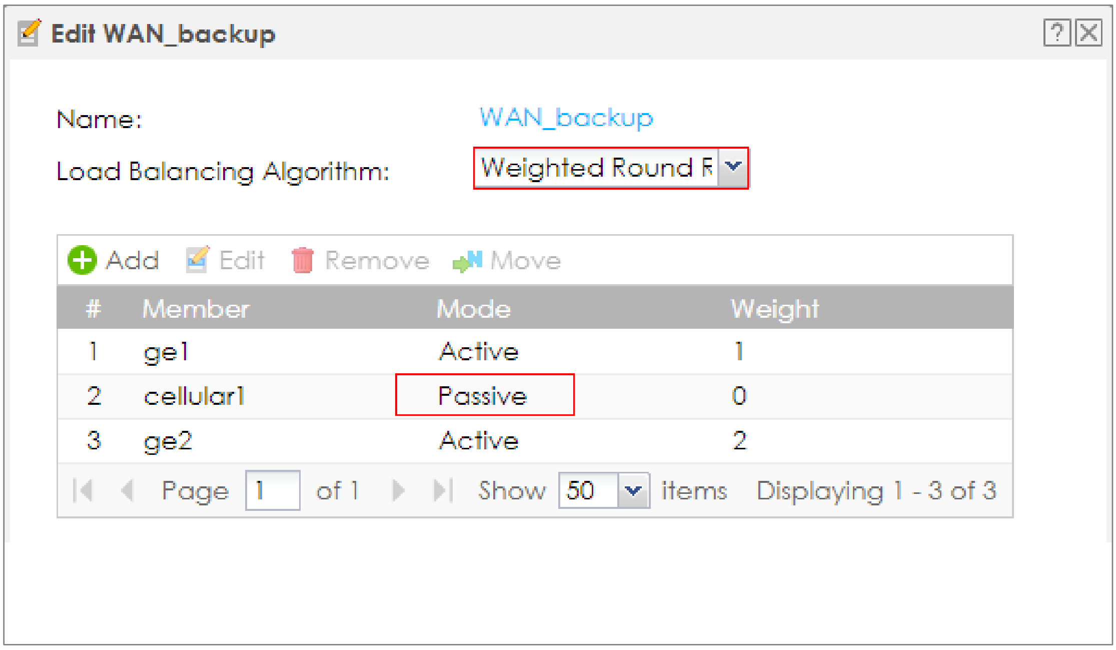
☐ Nailed-Up

Set Up the Trunk on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Trunk > User Configuration > Add Trunk**, configure a **Name** for you to identify the Trunk profile and set the **Load Balancing Algorithm** field to be the **Weighted Round Robin**.

Add **wan1** and enter **3** in the **Weight** column. Add **wan2** and enter **2** in the **Weight** column. Add **cellular1**, change **Mode** to be the **Passive** mode, enter **1** in the **Weight** column. Click **OK** to return to the **Configuration** screen.

CONFIGURATION > Network > Interface > Trunk > User Configuration > Add Trunk



Edit WAN_backup

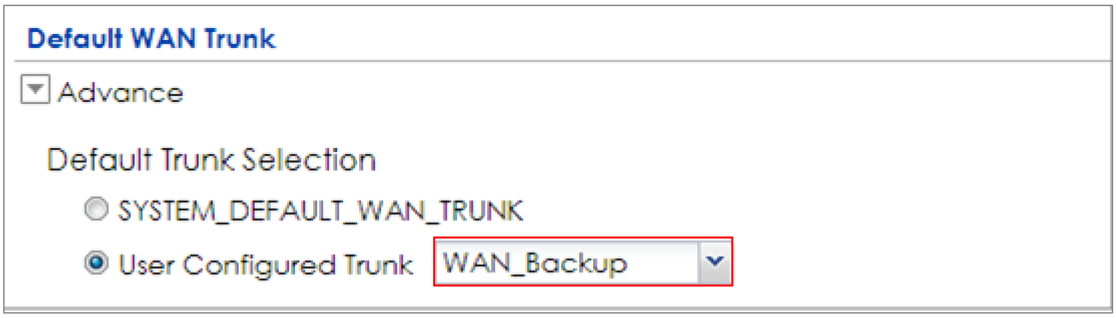
Name: WAN_backup

Load Balancing Algorithm: Weighted Round R

#	Member	Mode	Weight
1	ge1	Active	1
2	cellular1	Passive	0
3	ge2	Active	2

In the **Configuration** screen, go to **Default WAN Trunk** section, select **User Configured Trunk** and select the newly created Trunk from the list box. Click **Apply**.

CONFIGURATION > Network > Interface > Trunk > Default WAN Trunk > User Configured Trunk



Default WAN Trunk

Advance

Default Trunk Selection

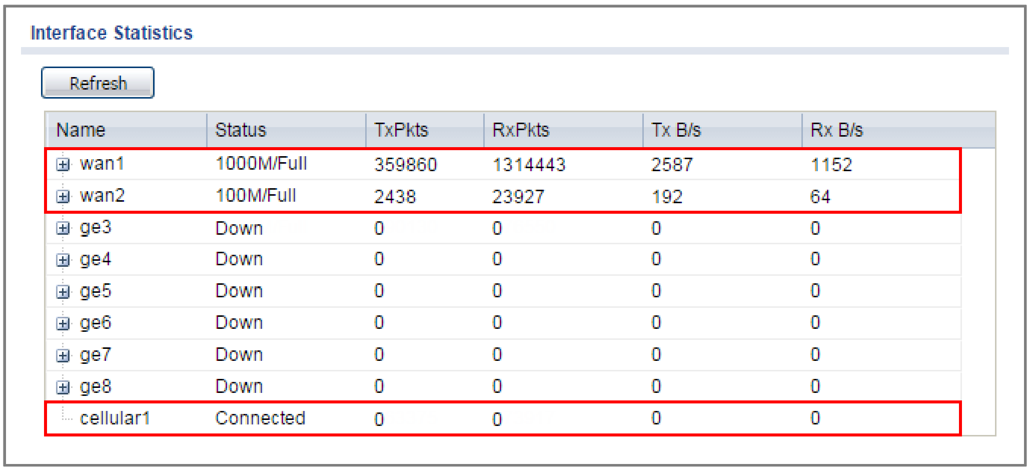
○ SYSTEM_DEFAULT_WAN_TRUNK

● User Configured Trunk WAN_Backup

Test the Result

Check the **Interface Statistics** when wan1 and wan2 connections are up. You can see both wan1 and wan2 **Status** are up, **Tx B/s** displays the transmission speed and **Rx B/s** displays the reception speed; cellular1 **Status** is connected but there is no traffic going through this interface.

MONITOR > Interface Status > Interface Statistics



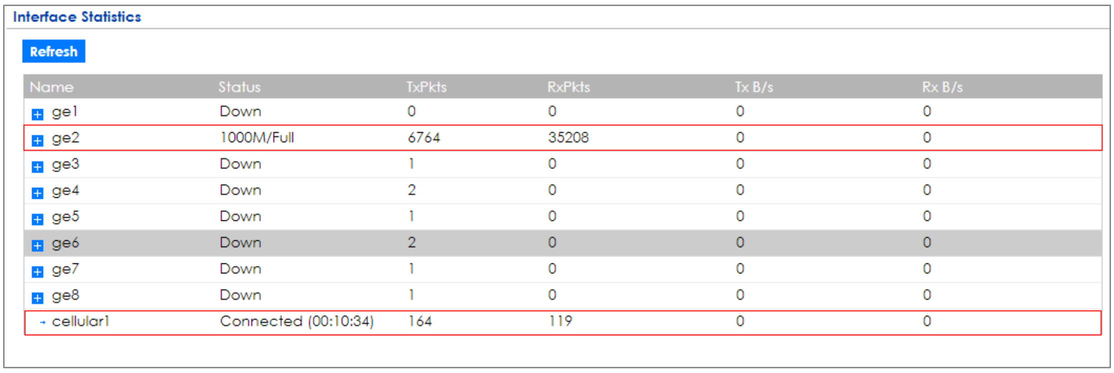
Interface Statistics

Refresh

Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s
⊞ wan1	1000M/Full	359860	1314443	2587	1152
⊞ wan2	100M/Full	2438	23927	192	64
⊞ ge3	Down	0	0	0	0
⊞ ge4	Down	0	0	0	0
⊞ ge5	Down	0	0	0	0
⊞ ge6	Down	0	0	0	0
⊞ ge7	Down	0	0	0	0
⊞ ge8	Down	0	0	0	0
cellular1	Connected	0	0	0	0

After disconnecting both wan1 and wan2, you can see both wan1 and wan2 **Status** are **Down** and no traffic goes through these two interfaces. The backup cellular1 **Status** is connected and all the traffic is going through this interface.

MONITOR > Interface Status > Interface Statistics



Interface Statistics

Refresh

Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s
⊞ ge1	Down	0	0	0	0
⊞ ge2	1000M/Full	6764	35208	0	0
⊞ ge3	Down	1	0	0	0
⊞ ge4	Down	2	0	0	0
⊞ ge5	Down	1	0	0	0
⊞ ge6	Down	2	0	0	0
⊞ ge7	Down	1	0	0	0
⊞ ge8	Down	1	0	0	0
→ cellular1	Connected (00:10:34)	164	119	0	0

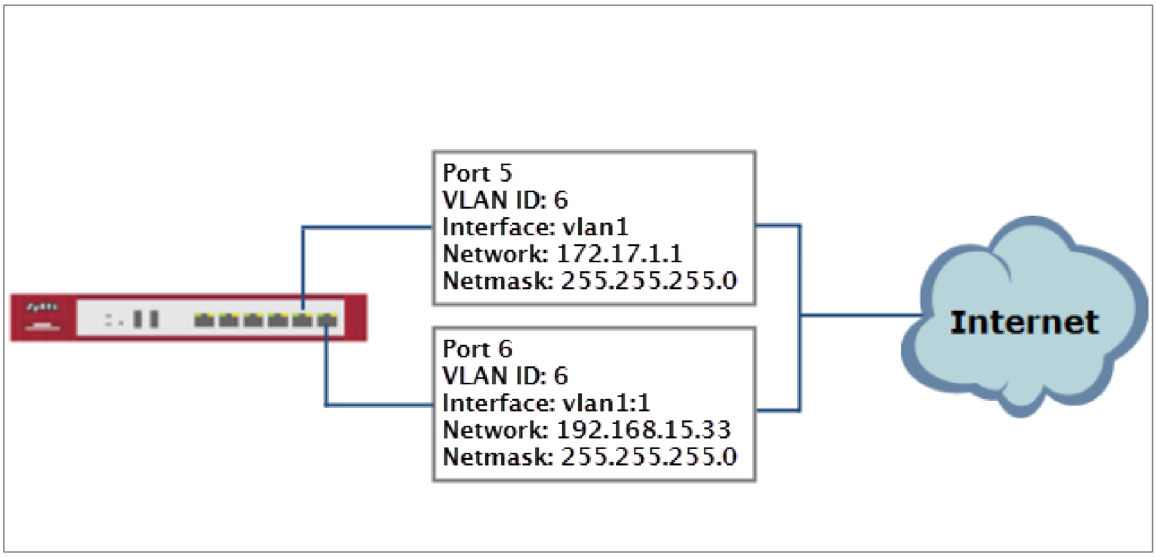
What Could Go Wrong?

If there is no traffic going through cellular interface when other interfaces are down, please make sure you have a compatible mobile broadband device installed or connected. Go to http://www.zyxel.com/support/download_landing.shtml and see the **3G Dongle Document** to check the compatible mobile broadband devices. Also, make sure the cellular interface is enabled and the cellular interface has the correct user name, password, and PIN code configured with the correct casing.

How to Configure Two Different WAN Interfaces with Different IP Addresses in the Same VLAN

This is an example of using ZyWALL/USG to configure two different WAN interfaces with different IP addresses in the same VLAN. After configuration, you can have the same VLAN ID for two different WAN interfaces.

ZyWALL/USG with Two Different WAN Interfaces with Different IP Addresses in the Same VLAN Example

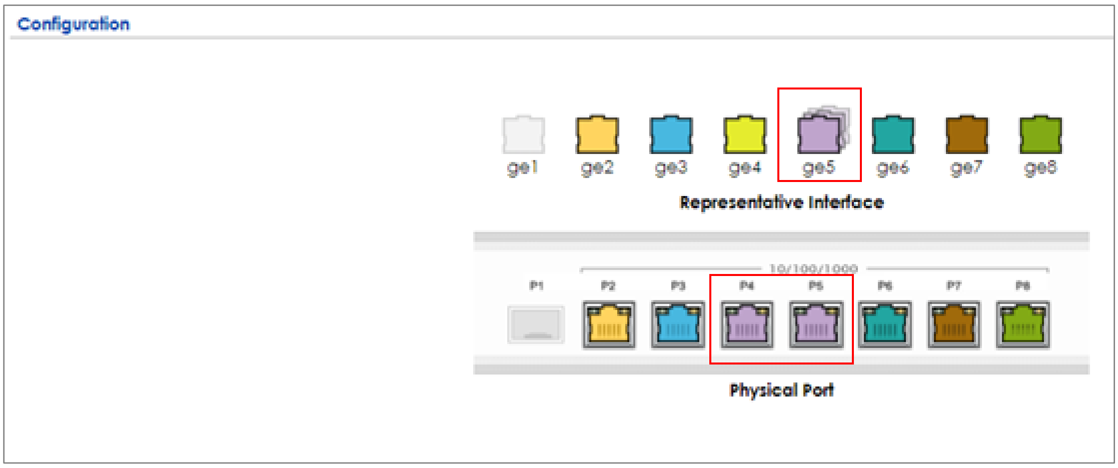


Note: This example requires the ZyWALL/USG models which can apply port grouping. All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ZyWALL USG300 (Firmware Version: ZLD 4.25).

Set Up the Port Grouping on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Port Grouping**, select the ports that you want to assign to a representative Interface (in this example, **Port 4** and **Port 5** are configured as **ge5**).

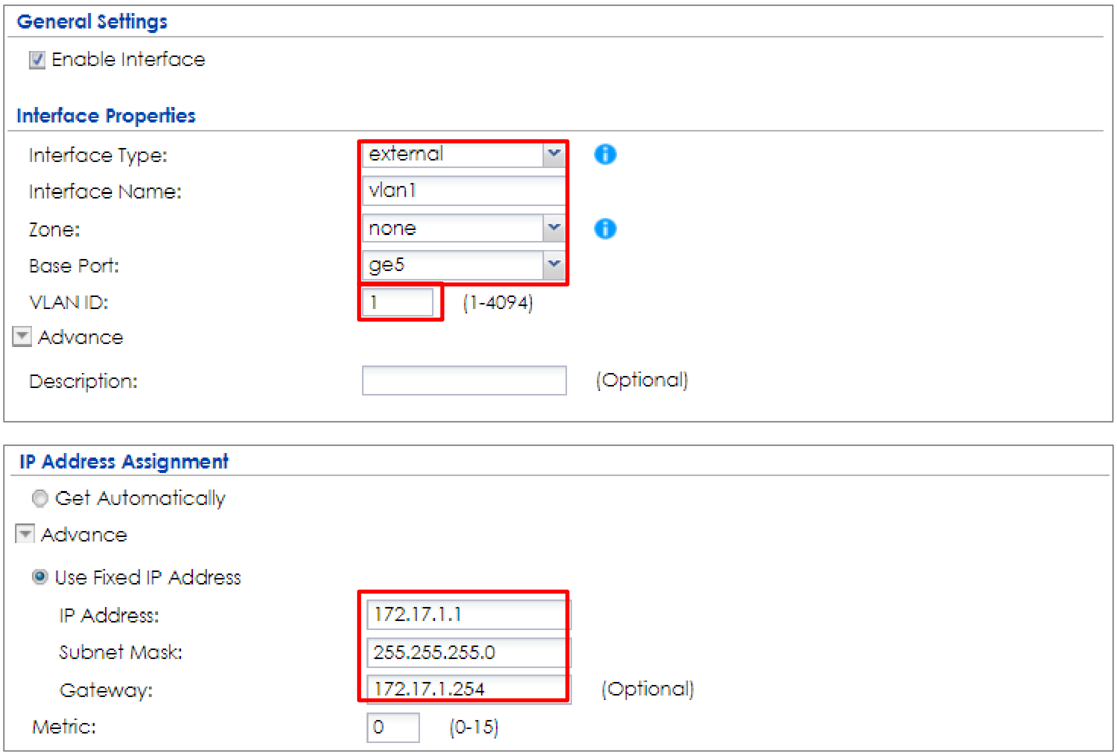
CONFIGURATION > Network > Interface > Port Grouping



Set Up the VLAN on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > VLAN**. Set **Interface Type** to be **External**. Set **Zone** to be **WAN**, configure **Base Port** to be **ge5**. Enter the **VLAN ID** and configure the fixed IP address (172.17.1.1/24 in this example). Click **OK** to go back to the **Configuration** page.

CONFIGURATION > Network > Interface > VLAN



General Settings

☑ Enable Interface

Interface Properties

Interface Type:	external
Interface Name:	vlan1
Zone:	none
Base Port:	ge5
VLAN ID:	1 (1-4094)

Advance

Description:	(Optional)

IP Address Assignment

○ Get Automatically

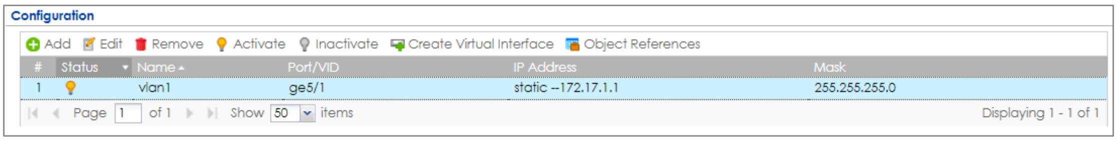
Advance

● Use Fixed IP Address

IP Address:	172.17.1.1
Subnet Mask:	255.255.255.0
Gateway:	172.17.1.254 (Optional)
Metric:	0 (0-15)

In the **Configuration** page, select the **vlan1** entry and click **Create Virtual Interface** on the upper bar. Configure the Fixed IP address (192.168.15.33/24 in this example). Click **OK**.

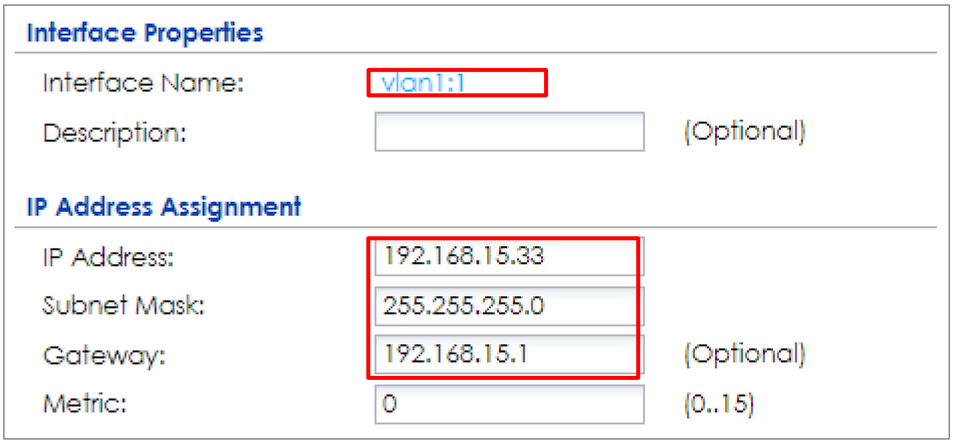
CONFIGURATION > Network > Interface > VLAN > vlan1



Configuration

#	Status	Name	Port/VID	IP Address	Mask
1	●	vlan1	ge5/1	static --172.17.1.1	255.255.255.0

CONFIGURATION > Network > Interface > VLAN > vlan1:1



Interface Properties

Interface Name:	vlan1:1
Description:	(Optional)

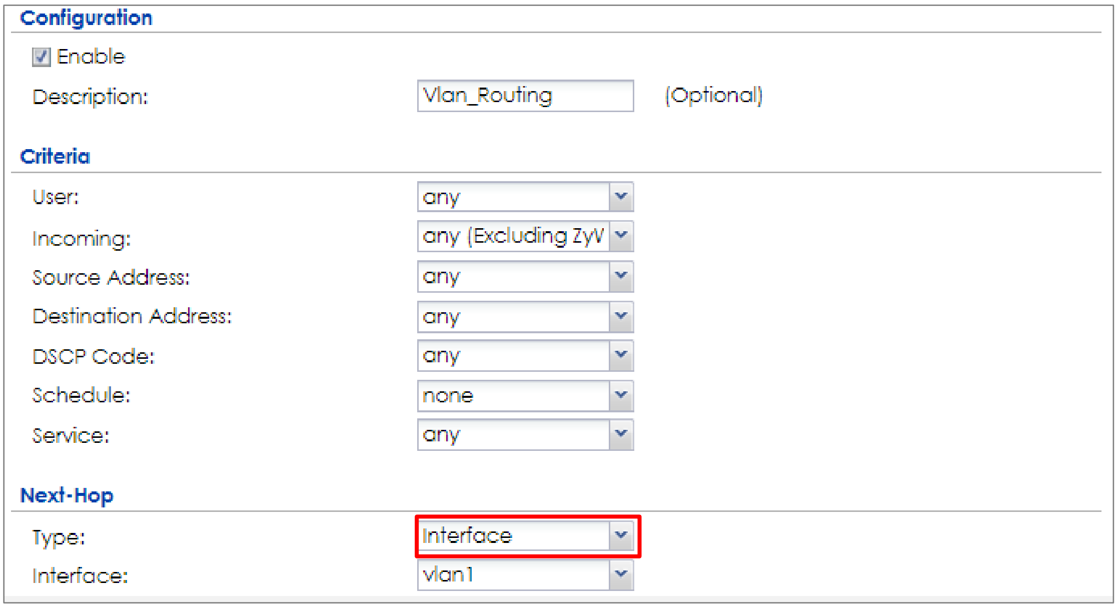
IP Address Assignment

IP Address:	192.168.15.33
Subnet Mask:	255.255.255.0
Gateway:	192.168.15.1 (Optional)
Metric:	0 (0..15)

Set Up the Routing on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Routing**, set **Next-Hop Type** to be **Interface** and set **Interface** to be the **vlan1**.

CONFIGURATION > Network > Routing



Configuration

☑ Enable

Description:	Vlan_Routing	(Optional)

Criteria

User:	any
Incoming:	any (Excluding ZyW
Source Address:	any
Destination Address:	any
DSCP Code:	any
Schedule:	none
Service:	any

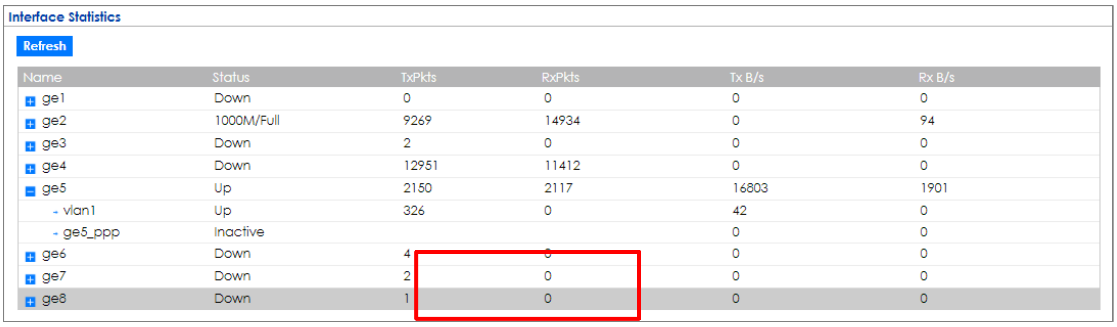
Next-Hop

Type:	Interface
Interface:	vlan1

Test the Result

Check the **Interface Statistics**, you can see vlan1 **Status** is up, **Tx B/s** displays the transmission speed and **Rx B/s** displays the reception speed. Port 5 and Port 6 are configured in the same vlan1 but use different IP addresses.

MONITOR > Interface Status > Interface Statistics



Interface Statistics

Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s
ge1	Down	0	0	0	0
ge2	1000M/Full	9269	14934	0	94
ge3	Down	2	0	0	0
ge4	Down	12951	11412	0	0
ge5	Up	2150	2117	16803	1901
- vlan1	Up	326	0	42	0
- ge5_ppp	Inactive			0	0
ge6	Down	4	0	0	0
ge7	Down	2	0	0	0
ge8	Down	1	0	0	0

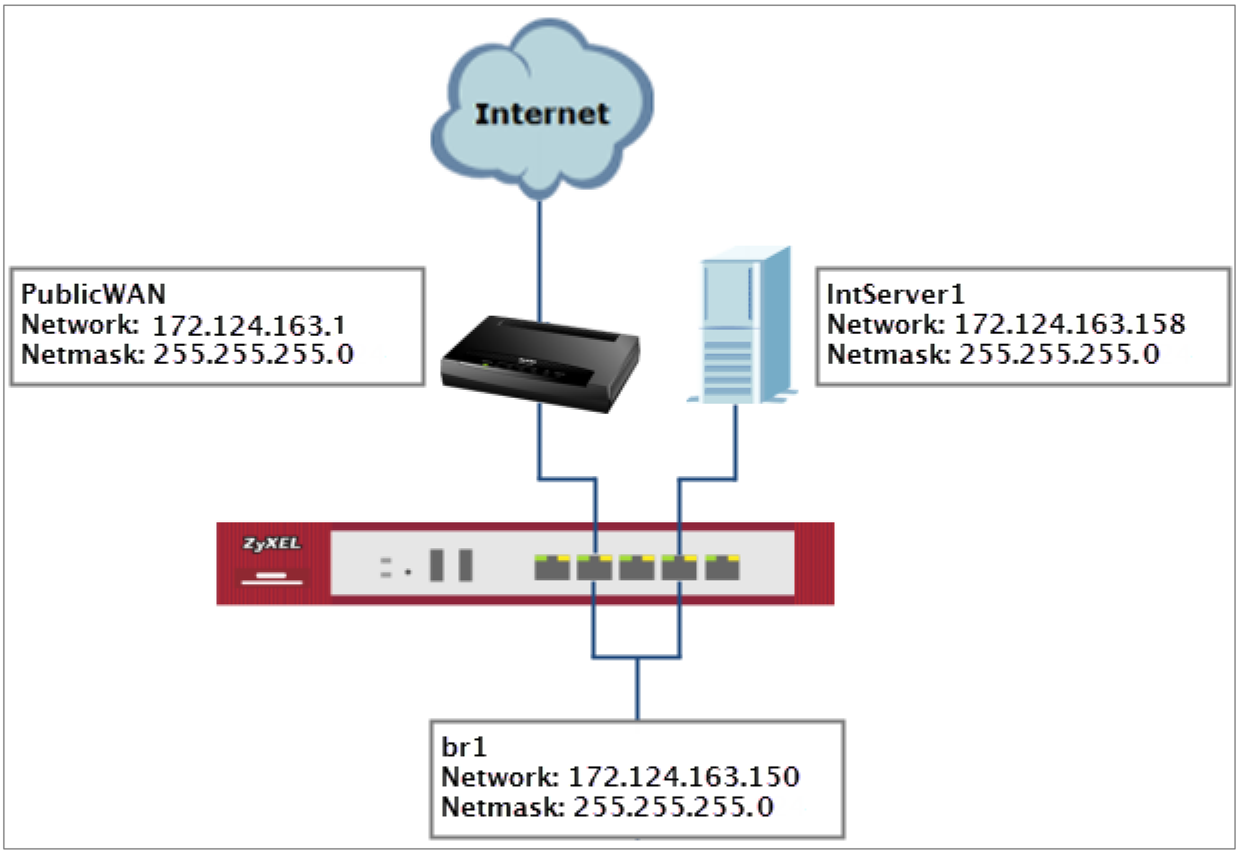
What Could Go Wrong?

If you cannot configure a particular VLAN interface on top of an Ethernet interface, please whether this VLAN has just been created on top of other Ethernet interface.

How to Let a Server Use the Same Public IP Address as the WAN Interface Using the Bridge Interface

This is an example of using ZyWALL/USG to configure an internal server in bridge mode without applying network address translation (NAT). The Internet users can reach this server directly by its public IP address.

ZyWALL/USG with Bridge Interface Example



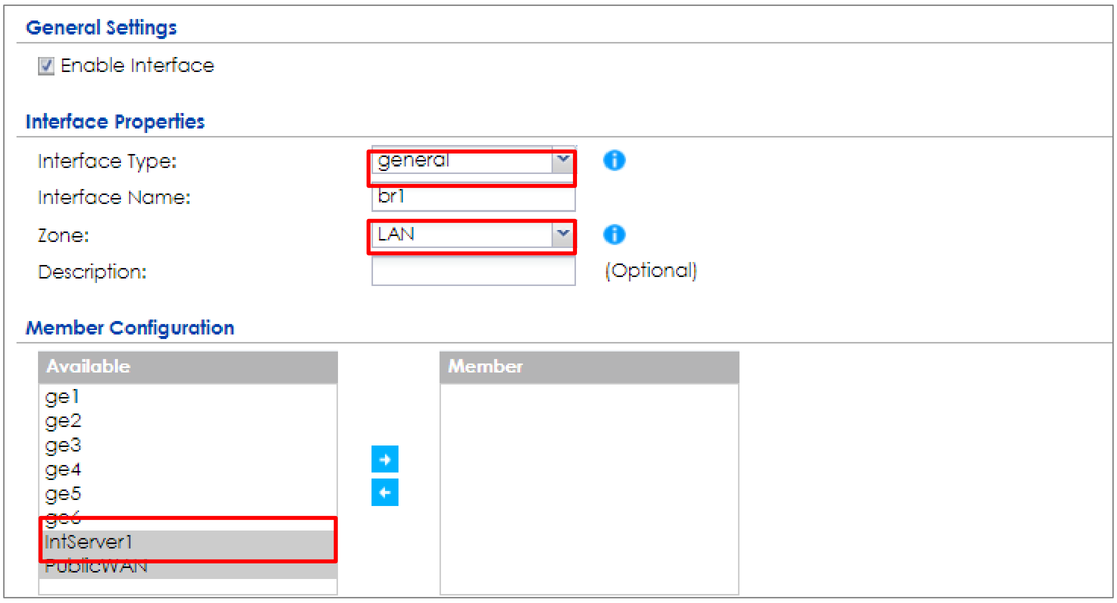
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Bridge Interface on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Bridge > add Bridge**, select **Interface Type** to be the **general** type, select **Zone** to be the **LAN** zone. In the **Member Configuration**, select internal server (**IntServer1** interface in this example) and public IP address (**Public WAN** interface in this example) to be in the same member group.

In the **IP Address Assignment** section, select **Used Fixed IP Address** and configure br1 IP address (172.124.163.150/24 in this example).

CONFIGURATION > Network > Interface > Bridge > add Bridge



General Settings

☑ Enable Interface

Interface Properties

Interface Type: general

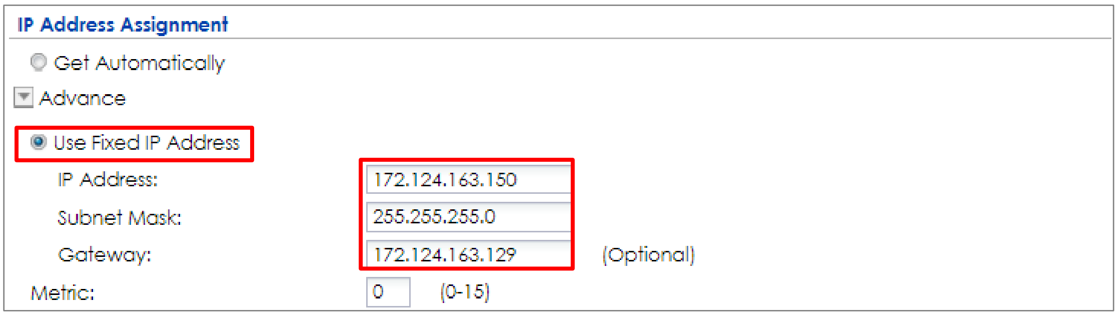
Interface Name: br1

Zone: LAN

Description: (Optional)

Member Configuration

Available	Member
ge1 ge2 ge3 ge4 ge5 ge6 IntServer1 PublicWAN	



IP Address Assignment

○ Get Automatically

Advance

● Use Fixed IP Address

IP Address: 172.124.163.150

Subnet Mask: 255.255.255.0

Gateway: 172.124.163.129 (Optional)

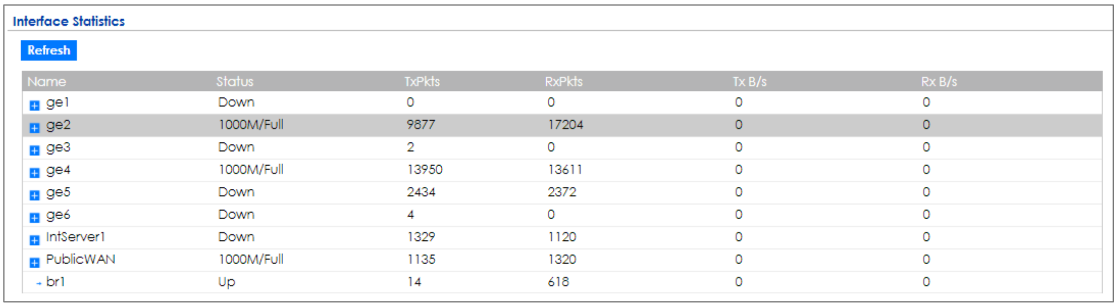
Metric: 0 (0-15)

After creating the bridge interface, connect the server's network cable to **IntServer1** port and set the server's IP to be in the same subnet (172.124.163.158 in this example).

Test the Result

Check the **Interface Statistics**, you can see br1 **Status** is up, **Tx B/s** displays the transmission speed and **Rx B/s** displays the reception speed. **IntServer1** and **PublicWAN** are configured in the same vlan1 but using different IP address.

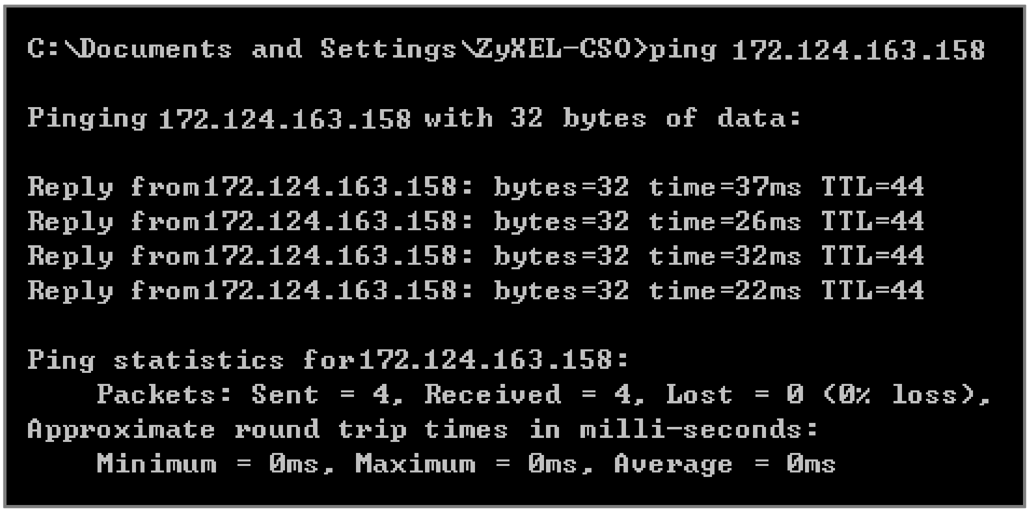
MONITOR > Interface Status > Interface Statistics



Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s
ge1	Down	0	0	0	0
ge2	1000M/Full	9877	17204	0	0
ge3	Down	2	0	0	0
ge4	1000M/Full	13950	13611	0	0
ge5	Down	2434	2372	0	0
ge6	Down	4	0	0	0
IntServer1	Down	1329	1120	0	0
PublicWAN	1000M/Full	1135	1320	0	0
br1	Up	14	618	0	0

Server can access Internet successfully by using its IP address (172.124.163.158 in this example) and Internet users can also reach this server by this public address as well.

Windows 7 > cmd > ping 172.124.163.158



```
C:\Documents and Settings\ZyXEL-CSO>ping 172.124.163.158

Pinging 172.124.163.158 with 32 bytes of data:

Reply from172.124.163.158: bytes=32 time=37ms TTL=44
Reply from172.124.163.158: bytes=32 time=26ms TTL=44
Reply from172.124.163.158: bytes=32 time=32ms TTL=44
Reply from172.124.163.158: bytes=32 time=22ms TTL=44

Ping statistics for172.124.163.158:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

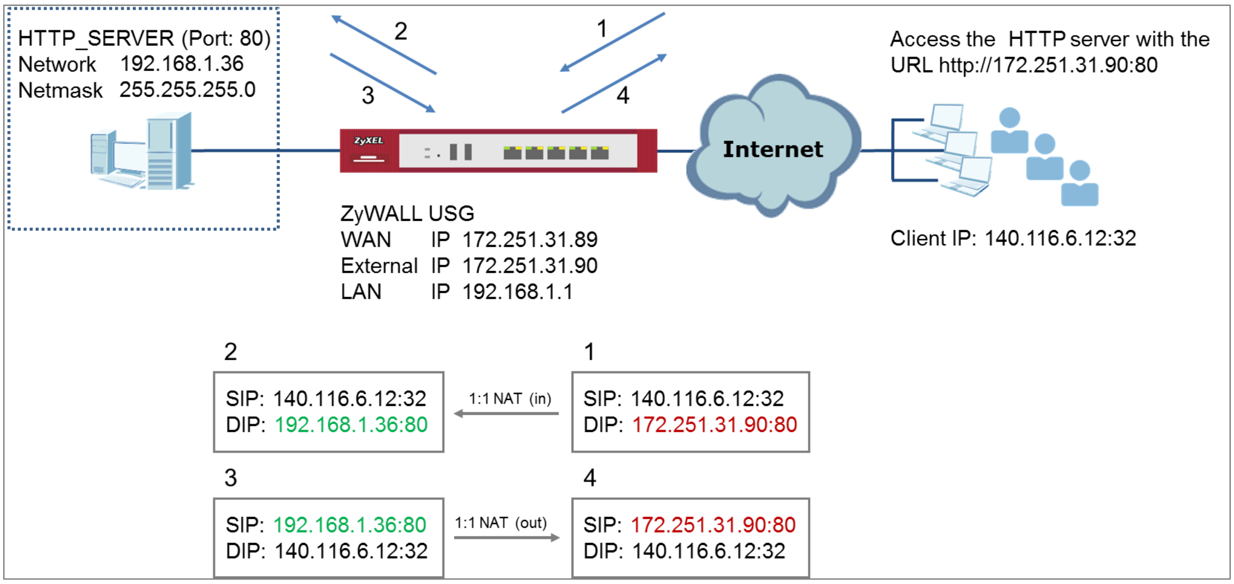
What Could Go Wrong?

If you cannot configure a particular bridge IP address, please check is this IP address already created on other Ethernet interface.

How to Allow Public Access to a Server Behind ZyWALL/USG

This is an example of using ZyWALL/USG to configure a securely access to internal server behind ZyWALL/USG with network address translation (NAT). The Internet users can reach this server directly by its public IP address and a NAT mapping rule will forward the traffic from the Internet to the Intranet. It provides security and decrease the number of IP addresses an organization needs.

ZyWALL/USG enables Public Access to a Server with NAT



HTTP_SERVER (Port: 80)
Network 192.168.1.36
Netmask 255.255.255.0

ZyWALL USG
WAN IP 172.251.31.89
External IP 172.251.31.90
LAN IP 192.168.1.1

Access the HTTP server with the URL http://172.251.31.90:80

Client IP: 140.116.6.12:32

2
SIP: 140.116.6.12:32
DIP: 192.168.1.36:80

1
SIP: 140.116.6.12:32
DIP: 172.251.31.90:80

3
SIP: 192.168.1.36:80
DIP: 140.116.6.12:32

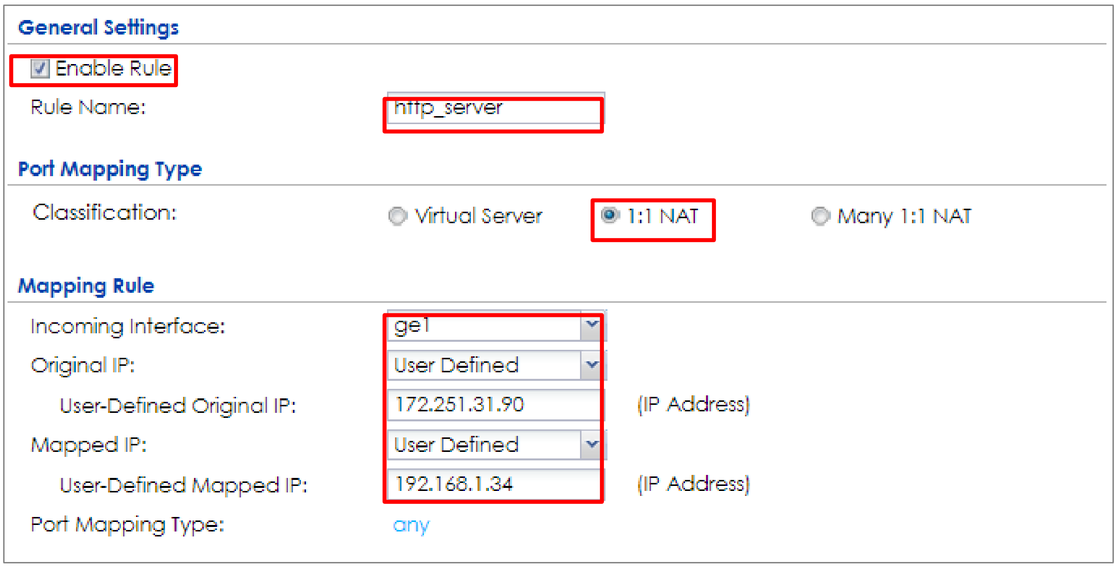
4
SIP: 172.251.31.90:80
DIP: 140.116.6.12:32

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the NAT on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > NAT > add NAT**, select **Enable Rule**. Select **1:1 NAT**. Set **Incoming Interface** to be the **wan1** interface. Type **User-Defined Original IP** (**172.251.31.90** in this example) and type **User-Defined Mapped IP** (**192.168.1.34** in this example). Set **Port Mapping Type** to **Service**, set **Original Service** and **Mapped Service** to **HTTP** in this example. Click **OK**.

CONFIGURATION > Network > NAT > add NAT



General Settings

☑ Enable Rule

Rule Name:	http_server

Port Mapping Type

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

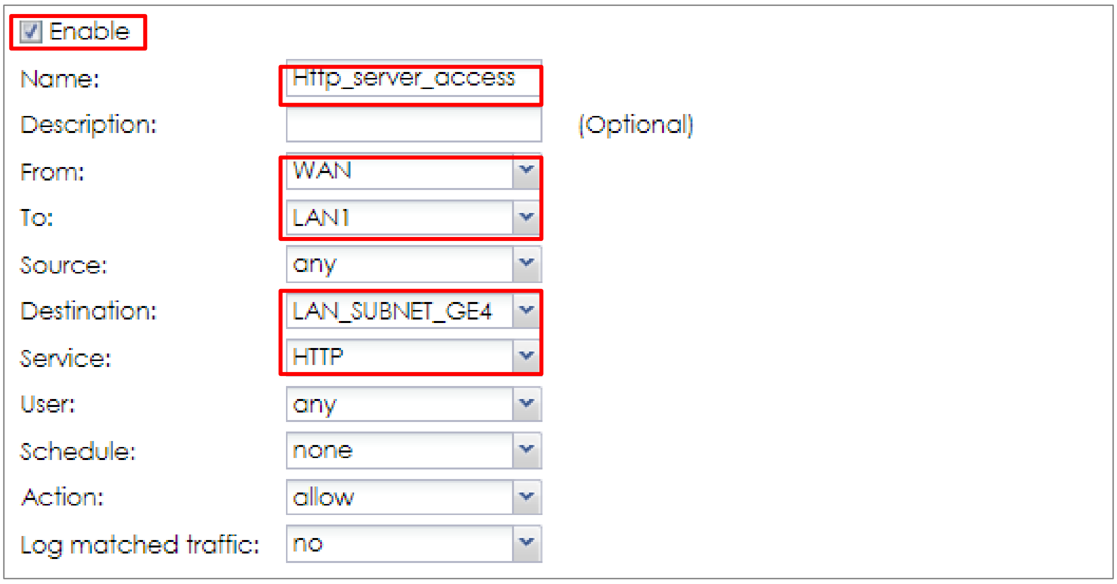
Mapping Rule

Incoming Interface:	ge1	
Original IP:	User Defined	
User-Defined Original IP:	172.251.31.90	(IP Address)
Mapped IP:	User Defined	
User-Defined Mapped IP:	192.168.1.34	(IP Address)
Port Mapping Type:	any	

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control > add corresponding**, select **Enable**. Configure a Name for your to identify the security policy (http_server_access in this example). Set **From: WAN** and **To: LAN1**. Set **Destination** to the lan subnet where your server is (LAN_SUBNET_GE3 in this example). Set **Service** to **HTTP**, set **Action** to **allow**. Click **OK**.

CONFIGURATION > Security Policy > Policy Control > add corresponding

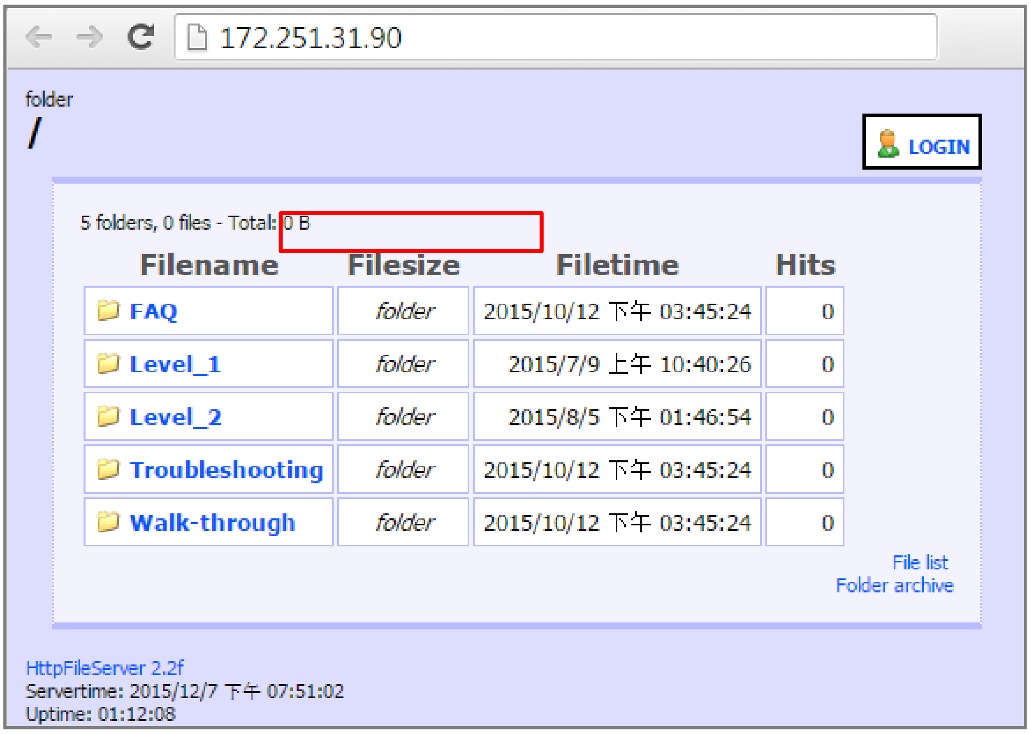


☑ Enable

Name:	Http_server_access	
Description:		(Optional)
From:	WAN	
To:	LAN1	
Source:	any	
Destination:	LAN_SUBNET_GE4	
Service:	HTTP	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	no	

Test the Result

Type http://172.251.31.90/ into the browser, it displays the HTTP service page.



172.251.31.90

folder
/

LOGIN

5 folders, 0 files - Total: 0 B

Filename	Filesize	Filetime	Hits
FAQ	folder	2015/10/12 下午 03:45:24	0
Level_1	folder	2015/7/9 上午 10:40:26	0
Level_2	folder	2015/8/5 下午 01:46:54	0
Troubleshooting	folder	2015/10/12 下午 03:45:24	0
Walk-through	folder	2015/10/12 下午 03:45:24	0

File list
Folder archive

HttpFileServer 2.2f
Servertime: 2015/12/7 下午 07:51:02
Uptime: 01:12:08

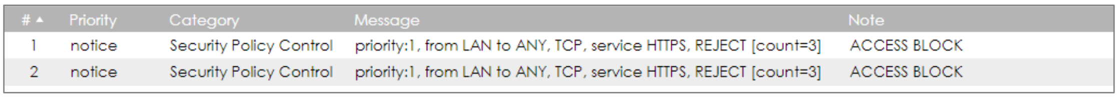
What Could Go Wrong?

If you cannot access your server via public IP address, please make sure all your public IP addresses are routing properly. To do one by one assign them to the ZyWALL's WAN port. Test to make sure you have internet access with the public IP address.

If you cannot access the ZyWALL from the internet with any IP address on your public IP, this is a routing issue on the service end. Please contact the ISP to fix the routing for the public IPs.

If you see [notice] log message as below, the HTTPS traffic is blocked by the priority 1 Security Policy. The ZyWALL/USG checks the security policy in order and applies the first security policy the traffic matches. If the HTTPS traffic matches a policy that comes earlier in the list, it may be unexpectedly blocked. Please change your policy setting or move the policy to the higher priority.

Monitor > Log



# ▲	Priority	Category	Message	Note
1	notice	Security Policy Control	priority:1, from LAN to ANY, TCP, service HTTPS, REJECT [count=3]	ACCESS BLOCK
2	notice	Security Policy Control	priority:1, from LAN to ANY, TCP, service HTTPS, REJECT [count=3]	ACCESS BLOCK

Note: The default setting of **Security Policy** is without log notification (except **PolicyDefault**), if you want to check which policy may potentially block the traffic, please select this policy and set the **Log matched traffic** to be **log** or **log alert**.

How to Configure DHCP Option 60 – Vendor Class Identifier

The following figure depicts how the ZyWALL/USG uses DHCP option 60. By matching the VCI strings, a DHCP client can choose one specific DHCP server on the WAN network. This function is useful when there are several DHCP servers providing different services in an environment. Clients that need Internet service can be directed to the DHCP server which provides Internet connection information with the same option 60 string. IPTV clients may relay to another DHCP server which obtains IPTV service information.

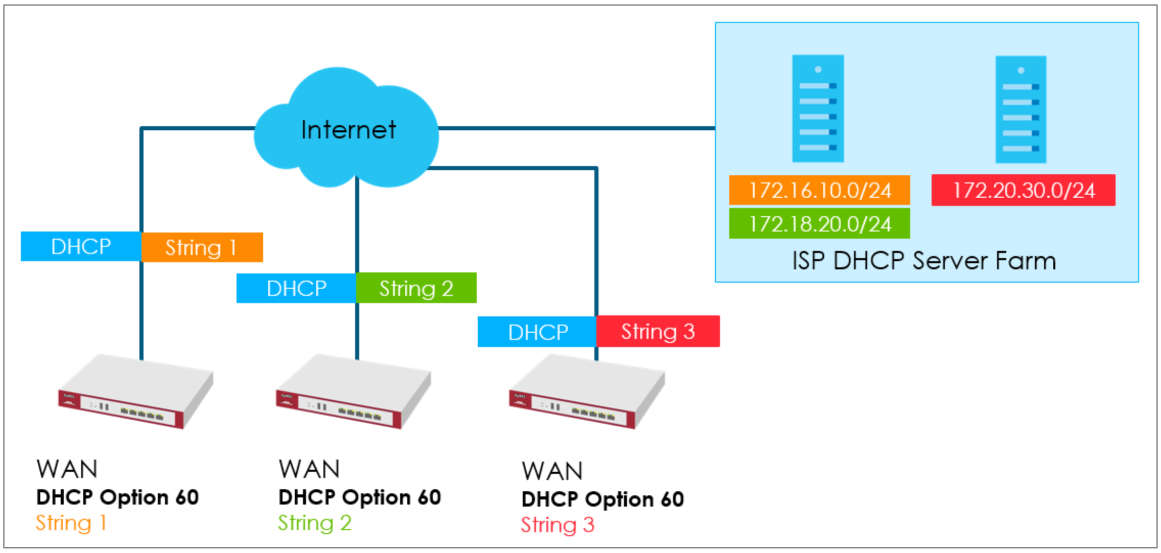


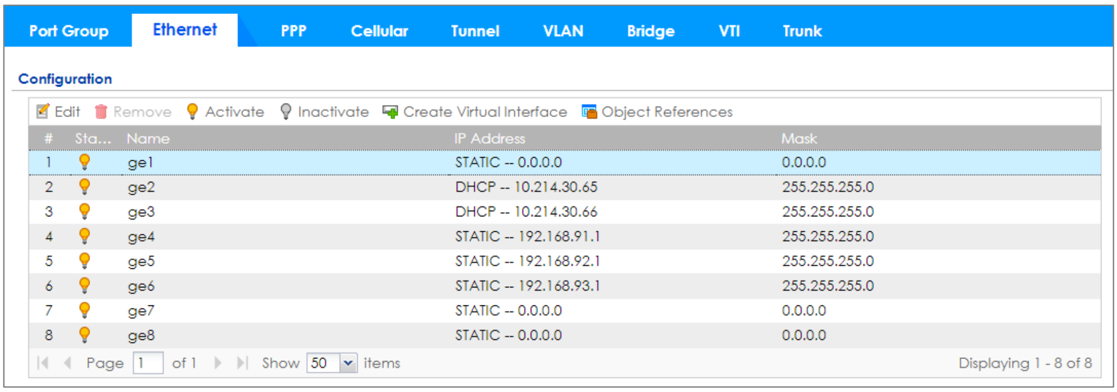
Figure 1 DHCP Option 60 Vendor Class Identifier

DHCP Option 60 Deployment Flow

1. Enable the WAN ports as DHCP clients (enabled by default).
2. Navigate to the WAN interface configuration screen.
3. Type in user defined option 60 string in the **Advance** setting section.

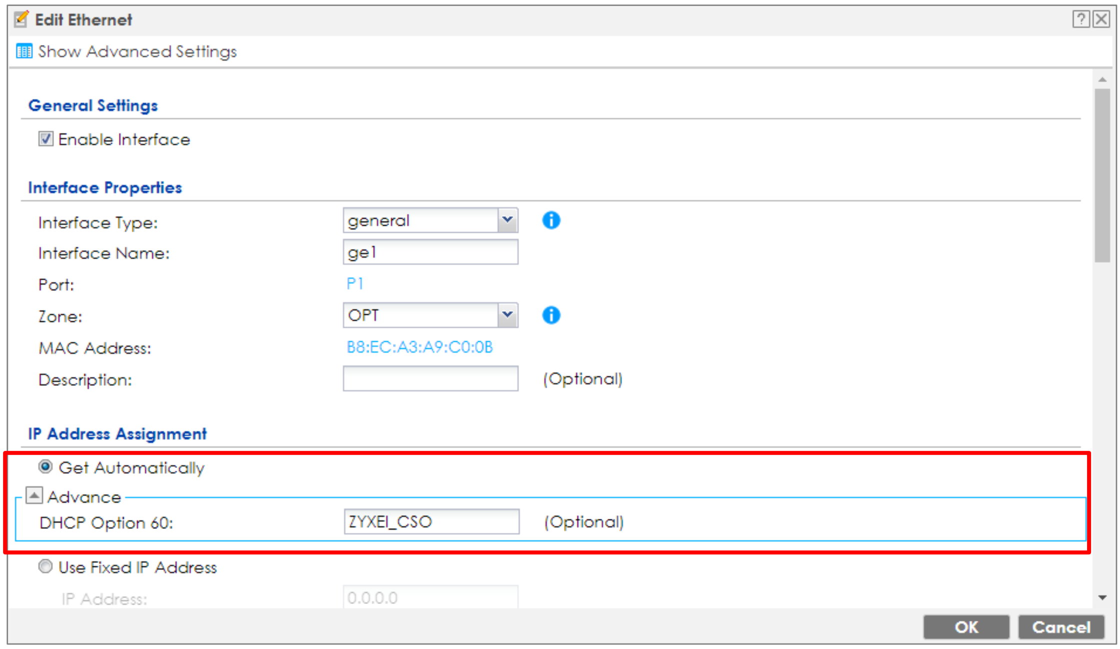
Setting Up DHCP Option 60 on the Web GUI

1 In the ZyWALL/USG's navigation panel, go to **Configuration > Network > Interface**.



#	Sta...	Name	IP Address	Mask
1	💡	ge1	STATIC -- 0.0.0.0	0.0.0.0
2	💡	ge2	DHCP -- 10.214.30.65	255.255.255.0
3	💡	ge3	DHCP -- 10.214.30.66	255.255.255.0
4	💡	ge4	STATIC -- 192.168.91.1	255.255.255.0
5	💡	ge5	STATIC -- 192.168.92.1	255.255.255.0
6	💡	ge6	STATIC -- 192.168.93.1	255.255.255.0
7	💡	ge7	STATIC -- 0.0.0.0	0.0.0.0
8	💡	ge8	STATIC -- 0.0.0.0	0.0.0.0

2 Click the **Ethernet** tab, go to **WAN > Edit**. Enter the VCI string in the **Advance** section of **DHCP Option 60**.



☑ Enable Interface

Interface Type: general

Interface Name: ge1

Port: P1

Zone: OPT

MAC Address: B8:EC:A3:A9:C0:0B

Description: (Optional)

● Get Automatically

Advance

DHCP Option 60: ZYXEL_CSO (Optional)

○ Use Fixed IP Address

IP Address: 0.0.0.0

Setting Up DHCP Option 60 on the CLI

Under the specific interface path, use these commands to:

Enable option 60

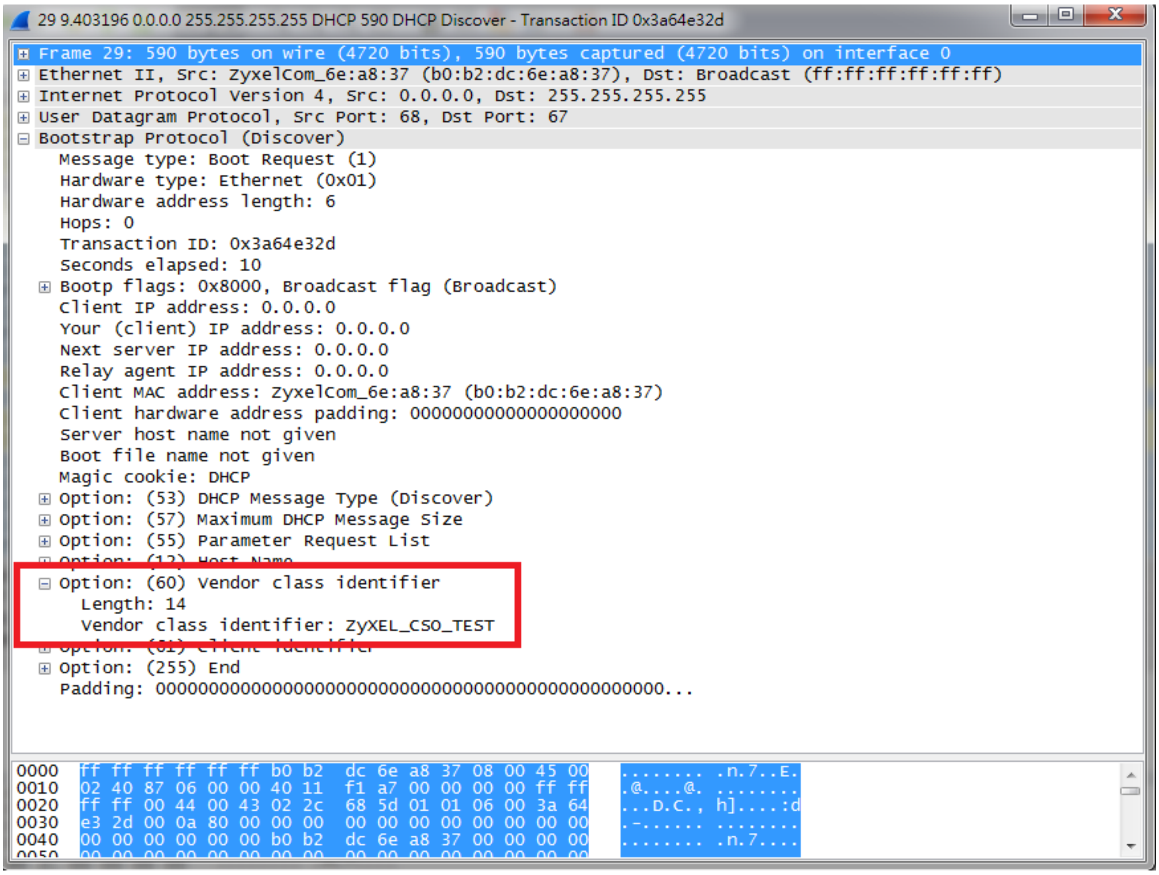
Router(config-if-wan1)# ip address dhcp option-60 {VCI_STRING}

Disable option 60

Router(config-if-wan1)# no ip address dhcp option-60

Test DHCP Option 60

To test the DHCP option 60 function, use a packet capture software to check if option 60 string exists in the DHCP discover message sent from the ZyWALL/USG WAN port.



29 9.403196 0.0.0.0 255.255.255.255 DHCP 590 DHCP Discover - Transaction ID 0x3a64e32d

```
⊞ Frame 29: 590 bytes on wire (4720 bits), 590 bytes captured (4720 bits) on interface 0
⊞ Ethernet II, Src: ZyxelCom_6e:a8:37 (b0:b2:dc:6e:a8:37), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
⊞ User Datagram Protocol, Src Port: 68, Dst Port: 67
⊟ Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x3a64e32d
    Seconds elapsed: 10
  ⊞ Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: ZyxelCom_6e:a8:37 (b0:b2:dc:6e:a8:37)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ⊞ Option: (53) DHCP Message Type (Discover)
  ⊞ Option: (57) Maximum DHCP Message Size
  ⊞ Option: (55) Parameter Request List
  ⊞ Option: (12) Host Name
  ⊟ Option: (60) Vendor class identifier
      Length: 14
      Vendor class identifier: ZyXEL_CSO_TEST
  ⊞ Option: (61) Client identifier
  ⊞ Option: (255) End
    Padding: 000000000000000000000000000000000000000000000000...

0000  ff ff ff ff ff ff b0 b2  dc 6e a8 37 08 00 45 00   ........ .n.7..E.
0010  02 40 87 06 00 00 40 11  f1 a7 00 00 00 00 ff ff   .@....@. ........
0020  ff ff 00 44 00 43 02 2c  68 5d 01 01 06 00 3a 64   ...D.C., h]....:d
0030  e3 2d 00 0a 80 00 00 00  00 00 00 00 00 00 00 00   .-...... ........
0040  00 00 00 00 00 00 b0 b2  dc 6e a8 37 00 00 00 00   ........ .n.7....
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

What Can Go Wrong?

1 Avoid using the same option 60 string on two or more DHCP servers. It may cause duplicate DHCP serving confliction.

2 Since packets with option 60 are clear, do not consider it as a secure way for DHCP server authentication.

How to set up Link Aggregation Group (LAG)

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.

LAG interface supported models: ZyWALL 310/1100/1900, USG 310/1100/1900/2200, ATP500/700/800, USG FLEX500/700, VPN300/1000.

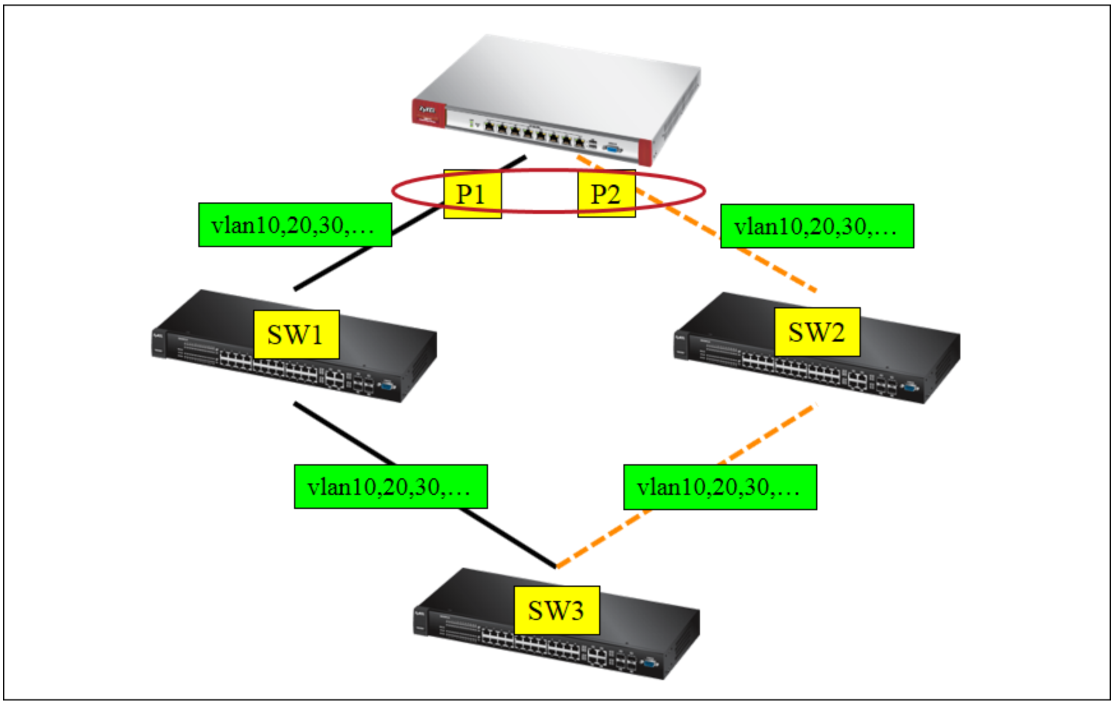
The link aggregation supported models have Active-backup, 802.3ad (LACP), and Balance-alb modes. Link aggregation supports IPSec tunnel, VLAN, and bridge interface.

Device HA Pro is supported on the LAG interface.

Set up the Active-backup, 802.3ad, Balance-alb

Active-backup Mode:

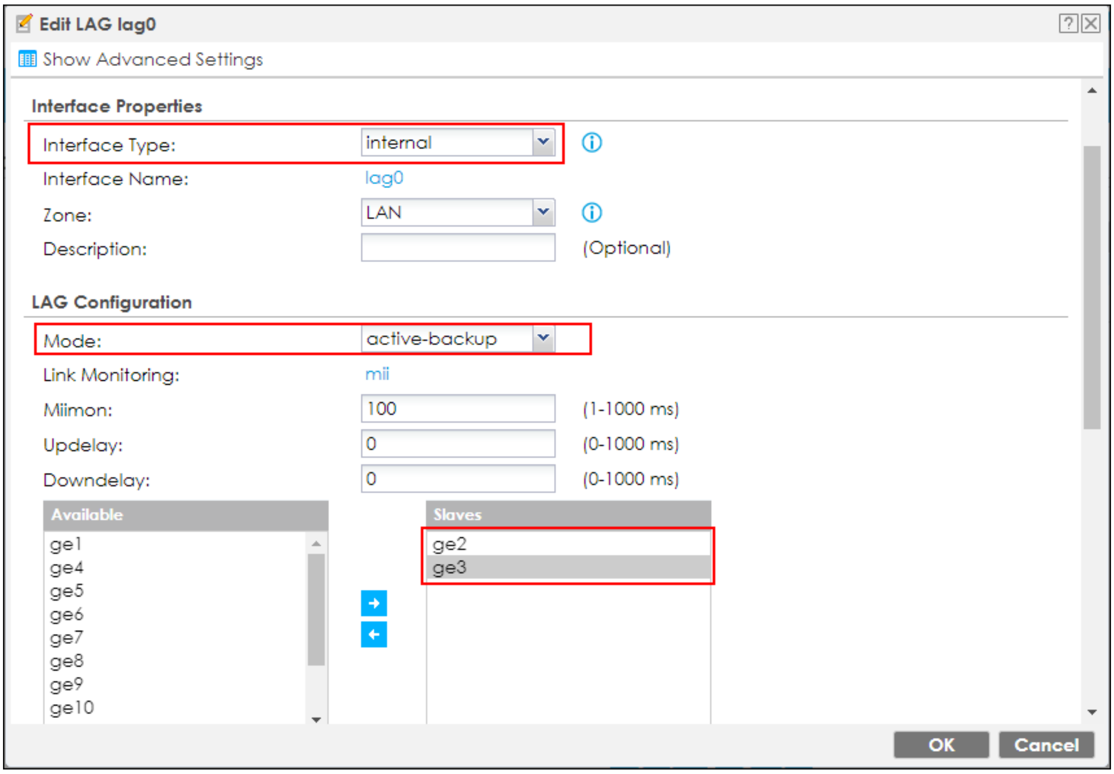
(Does not require switch configuration and one or multiple switches can be used.)



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.



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: mii

Miimon: 100 (1-1000 ms)

Updelay: 0 (0-1000 ms)

Downdelay: 0 (0-1000 ms)

Available	Slaves
ge1 ge4 ge5 ge6 ge7 ge8 ge9 ge10	ge2 ge3

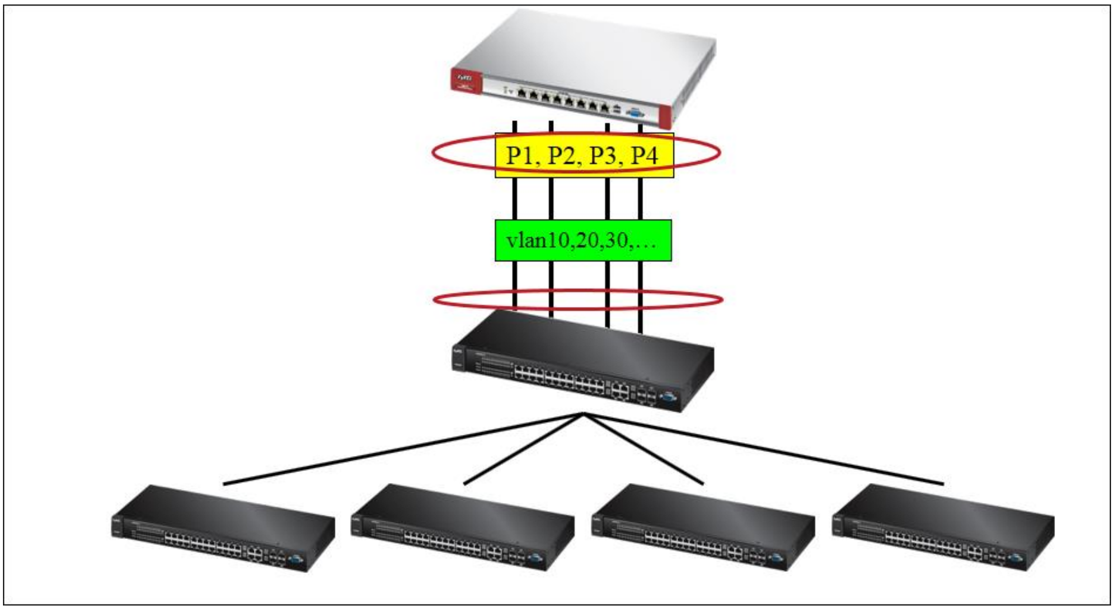
Link Monitoring: Mii monitoring monitors the state of the local interface.

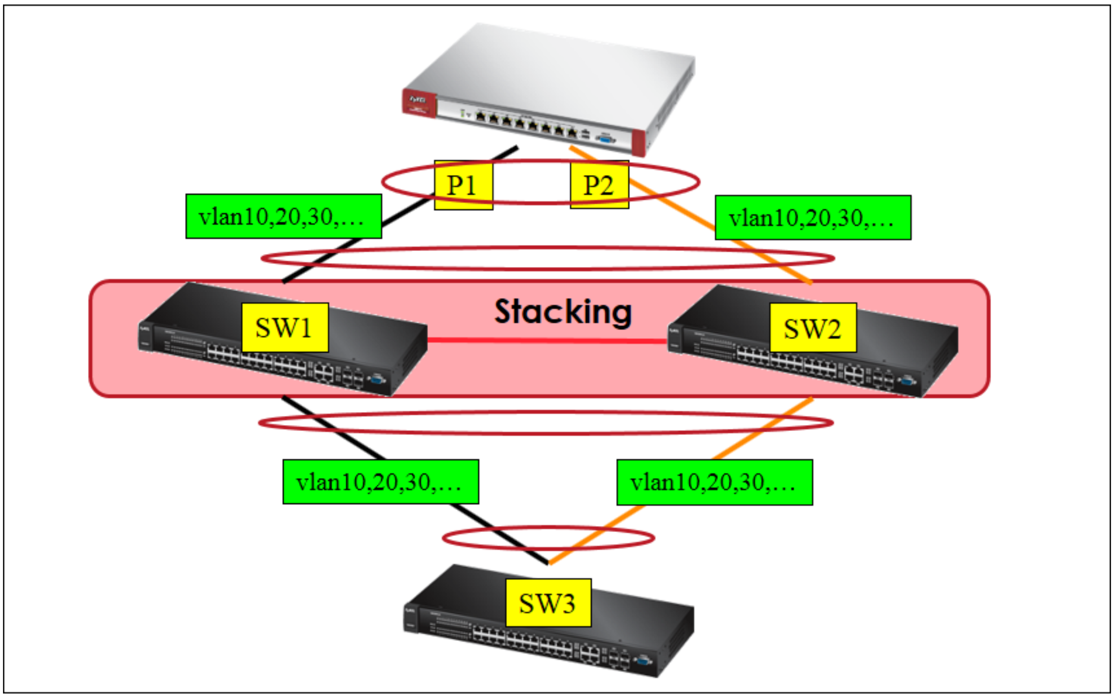
Updelay is the time to wait to enable the slave port after the device detects the link recovery.

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

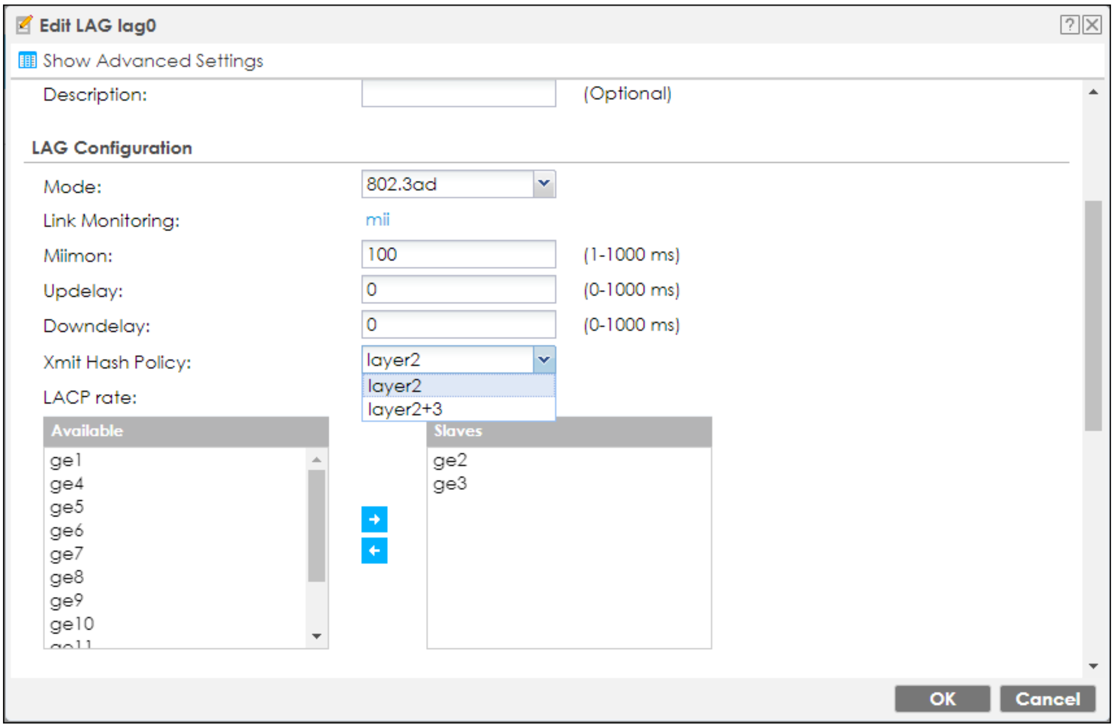
802.3ad (LACP) Mode:

(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

Description: (Optional)

LAG Configuration

Mode: 802.3ad

Link Monitoring: mii

Miimon: 100 (1-1000 ms)

Updelay: 0 (0-1000 ms)

Downdelay: 0 (0-1000 ms)

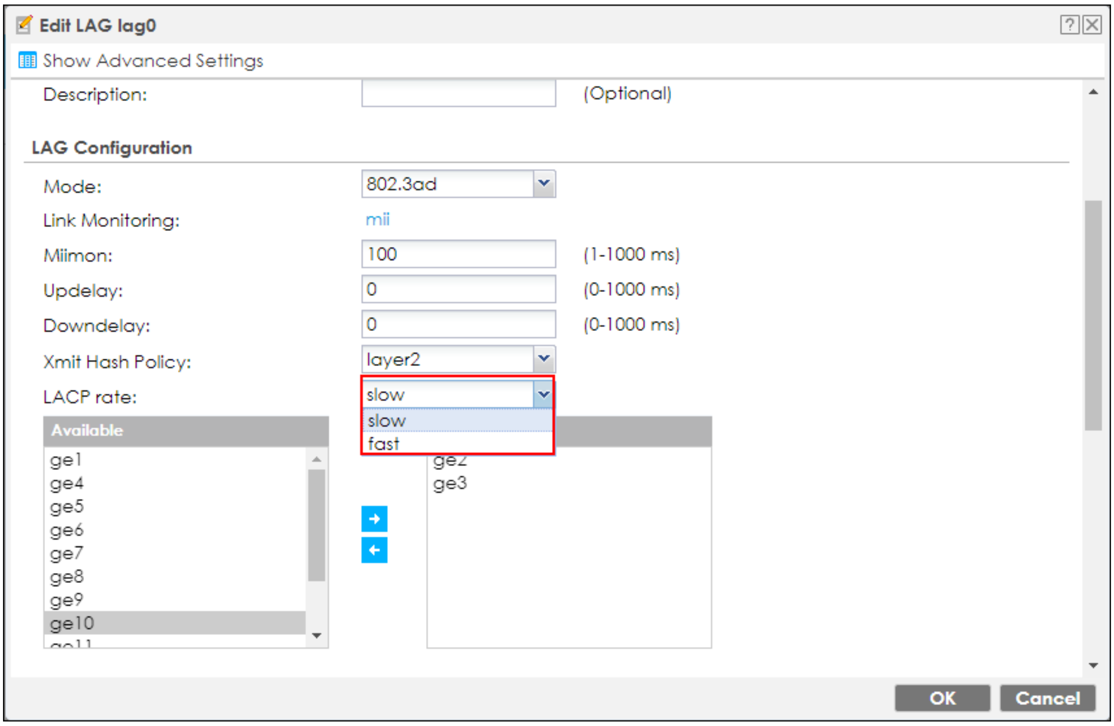
Xmit Hash Policy: layer2

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

Description: (Optional)

LAG Configuration

Mode: 802.3ad

Link Monitoring: mii

Miimon: 100 (1-1000 ms)

Updelay: 0 (0-1000 ms)

Downdelay: 0 (0-1000 ms)

Xmit Hash Policy: layer2

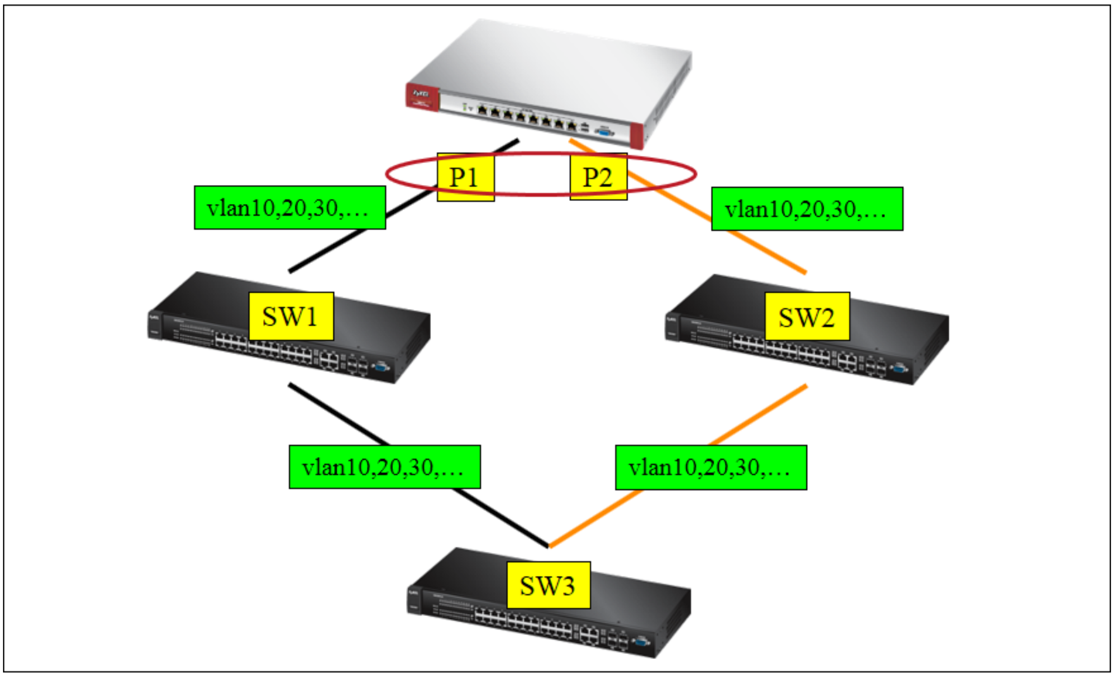
LACP rate: slow

LACP rate:

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

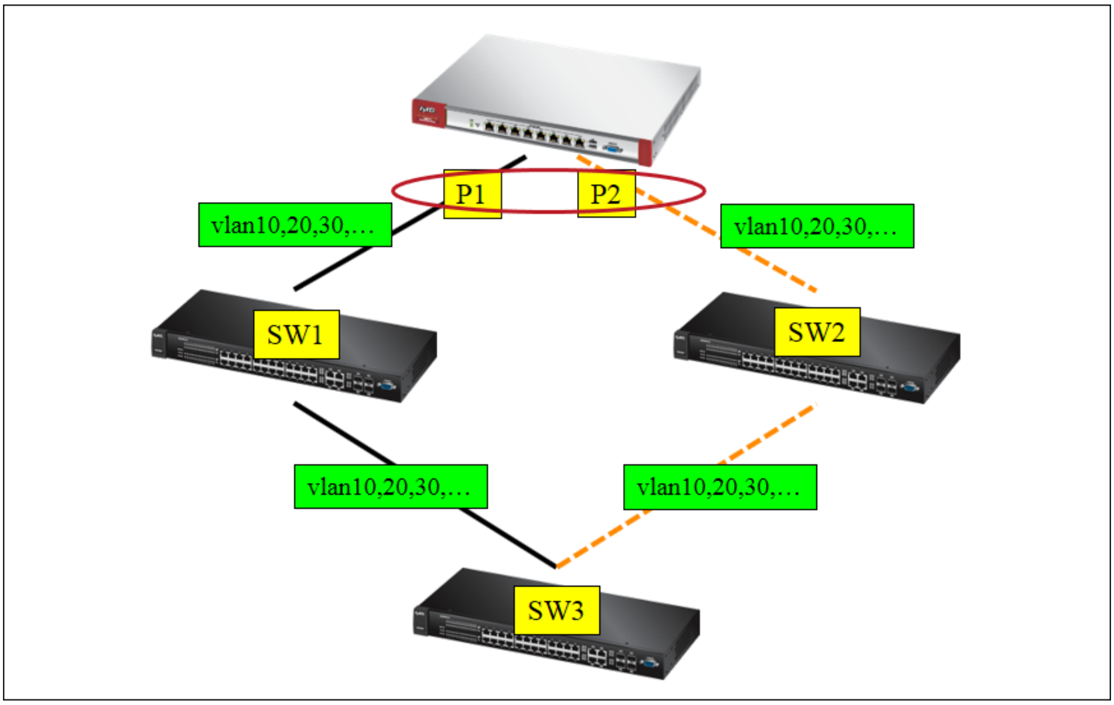
Balance-alb Mode:

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

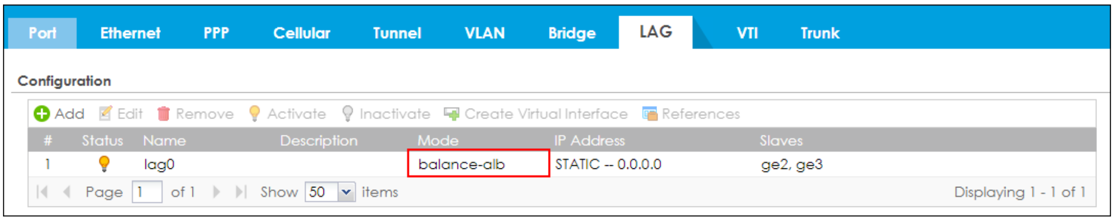


Set up the balance-alb mode.

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**.

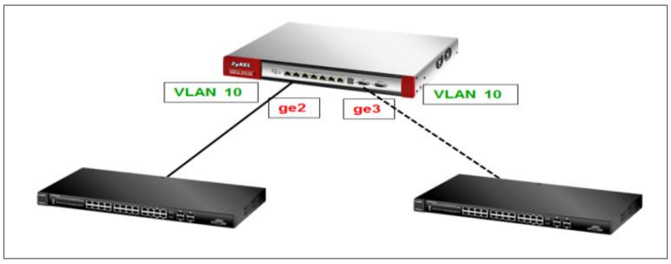


Configuration

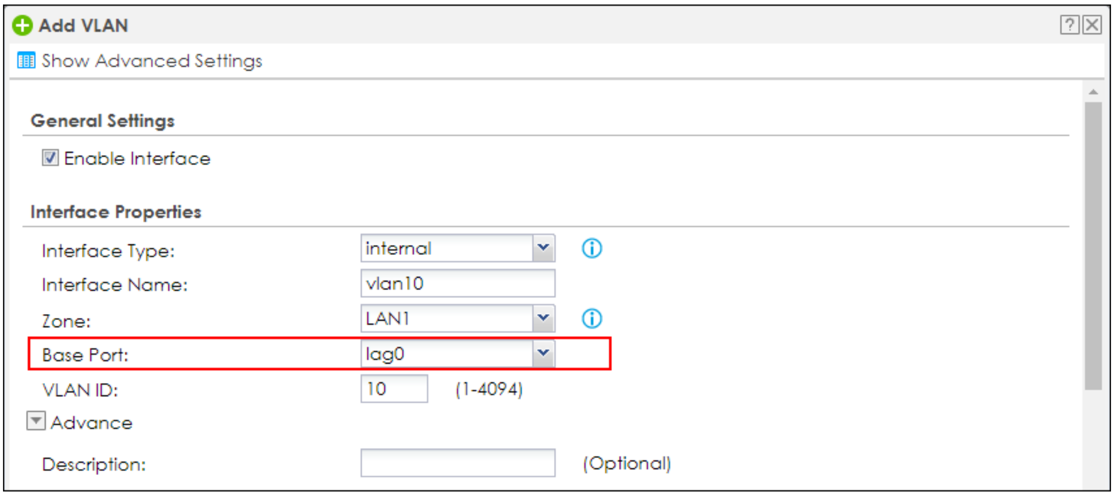
#	Status	Name	Description	Mode	IP Address	Slaves
1	💡	lag0		balance-alb	STATIC -- 0.0.0.0	ge2, ge3

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

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.



Add VLAN

Show Advanced Settings

General Settings

☑ Enable Interface

Interface Properties

Interface Type: internal

Interface Name: vlan10

Zone: LAN1

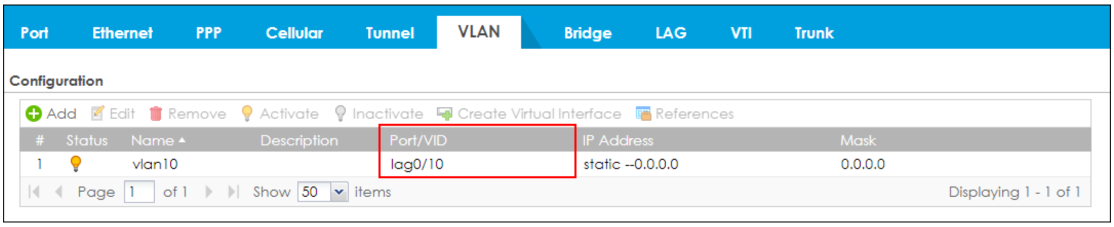
Base Port: lag0

VLAN ID: 10 (1-4094)

Advance

Description: (Optional)

You can find the LAG interface in the VLAN interface.

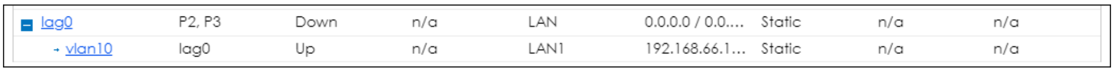


#	Status	Name	Description	Port/VID	IP Address	Mask
1		vlan10		lag0/10	static --0.0.0.0	0.0.0.0

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

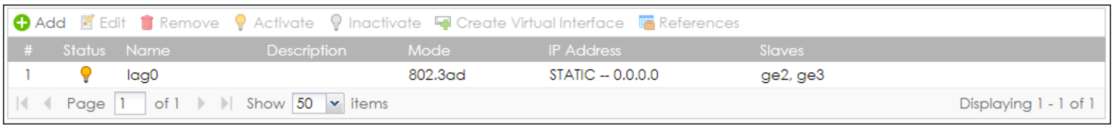
Test the Result

After the deployment you can see the interface status through **Monitor>interface Status**



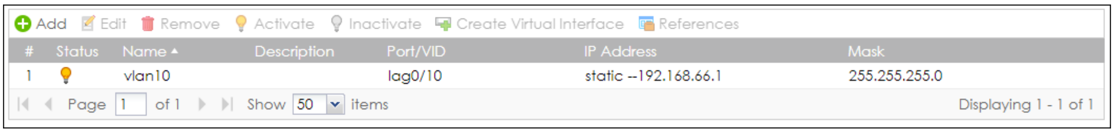
lag0	P2, P3	Down	n/a	LAN	0.0.0.0 / 0.0....	Static	n/a	n/a
vlan10	lag0	Up	n/a	LAN1	192.168.66.1...	Static	n/a	n/a

Below we are using 802.3ad LAG interface with Vlan66 for the example, unplug one of the network cable during the ping, the connection should still alive after one ping lost.



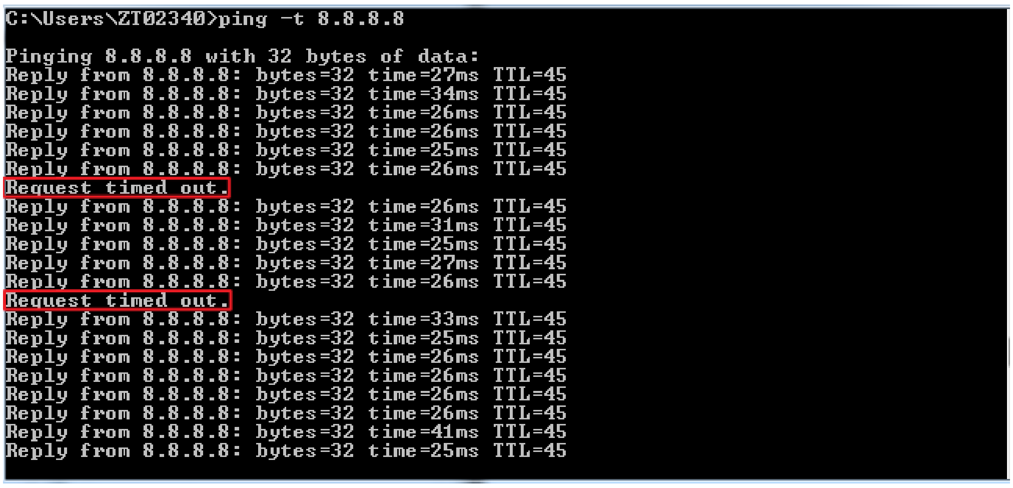
#	Status	Name	Description	Mode	IP Address	Slaves
1		lag0		802.3ad	STATIC -- 0.0.0.0	ge2, ge3

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



#	Status	Name	Description	Port/VID	IP Address	Mask
1		vlan10		lag0/10	static --192.168.66.1	255.255.255.0

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



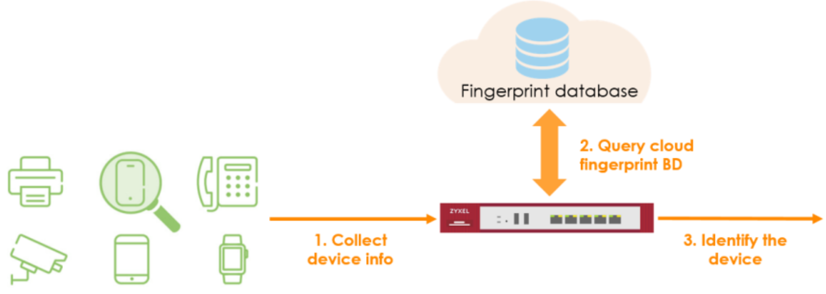
```
C:\Users\ZT02340>ping -t 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=27ms TTL=45
Reply from 8.8.8.8: bytes=32 time=34ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=25ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Request timed out.
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=31ms TTL=45
Reply from 8.8.8.8: bytes=32 time=25ms TTL=45
Reply from 8.8.8.8: bytes=32 time=27ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Request timed out.
Reply from 8.8.8.8: bytes=32 time=33ms TTL=45
Reply from 8.8.8.8: bytes=32 time=25ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=41ms TTL=45
Reply from 8.8.8.8: bytes=32 time=25ms TTL=45
```

What can go wrong

1. Configure all the related setting on LAG interface before you connect the link.
2. Make sure you have the corresponding setting on your switch if using 802.3ad (LACP).
3. Check the Xmit Hash policy or the link monitoring method.
4. To adjust the sensitivity of the updelay and downdelay when using active-backup or balance-alb mode.

How to configure Device Insight

Device Insight continuously monitors the network to detect wired and wireless devices, collect their information, and classify them into specific categories or operating system. It helps users simply discover and manage devices.

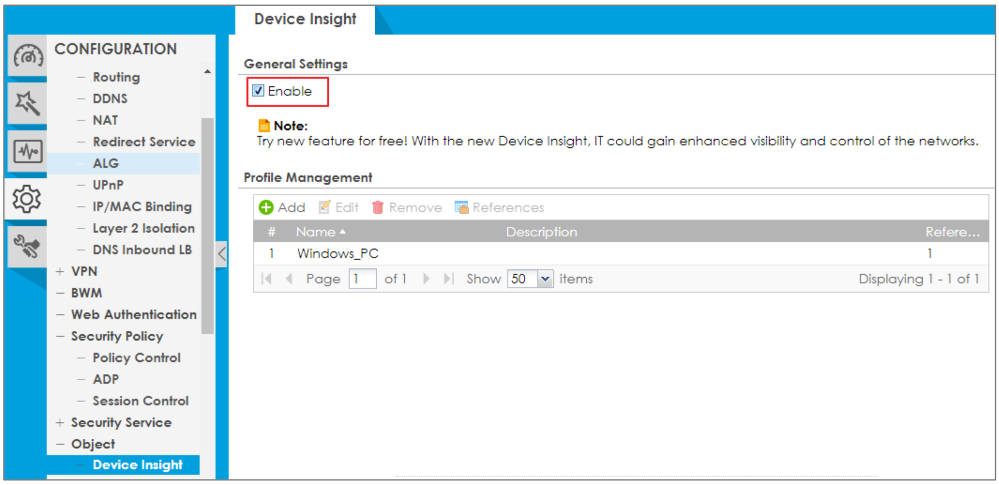


Device Information

Status: Online
MAC address :
88:ac:c0:91:20:d9
IP address: 192.168.1.33
Hostname: Alice
Manufacturer: Apple Inc.
Category: Mobile Phone/Table
OS: iOS
Type: Apple iPhone
Last Seen: 2021-08-19 09:23:20
User: NT12345
Connected to: vlan12

Enable Device Insight and create profile

In the Web GUI, go to **Configuration > Object > Device Insight**, enable the checkbox



Device Insight

General Settings

☑ Enable

Note:
Try new feature for free! With the new Device Insight, IT could gain enhanced visibility and control of the networks.

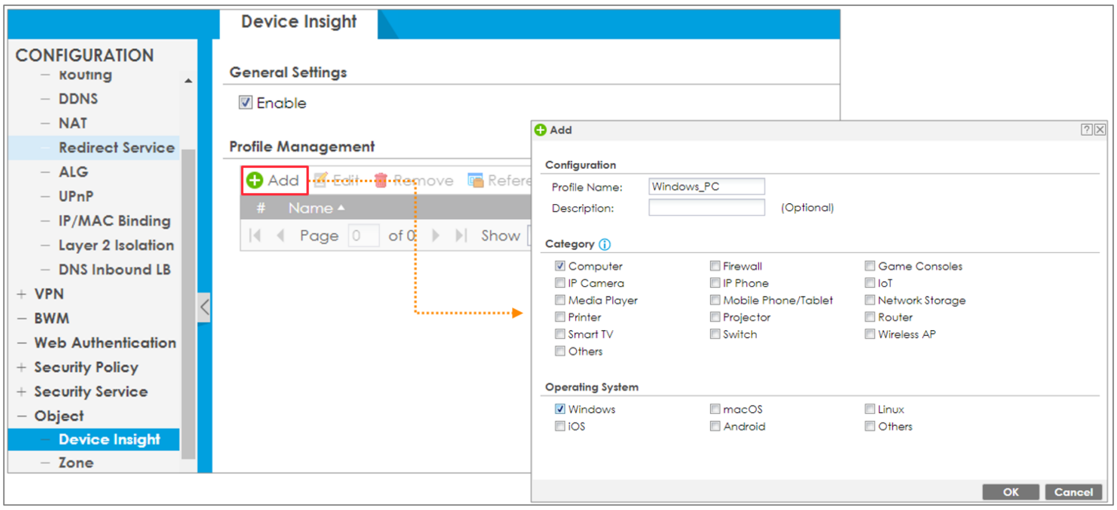
Profile Management

Add Edit Remove References

#	Name ▴	Description	Refere...
1	Windows_PC		1

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

Then, click to Add button to create a new profile, select the device based on category and operating system you want to manage.



General Settings

☑ Enable

Profile Management

Configuration

Profile Name: Windows_PC

Description: (Optional)

Category

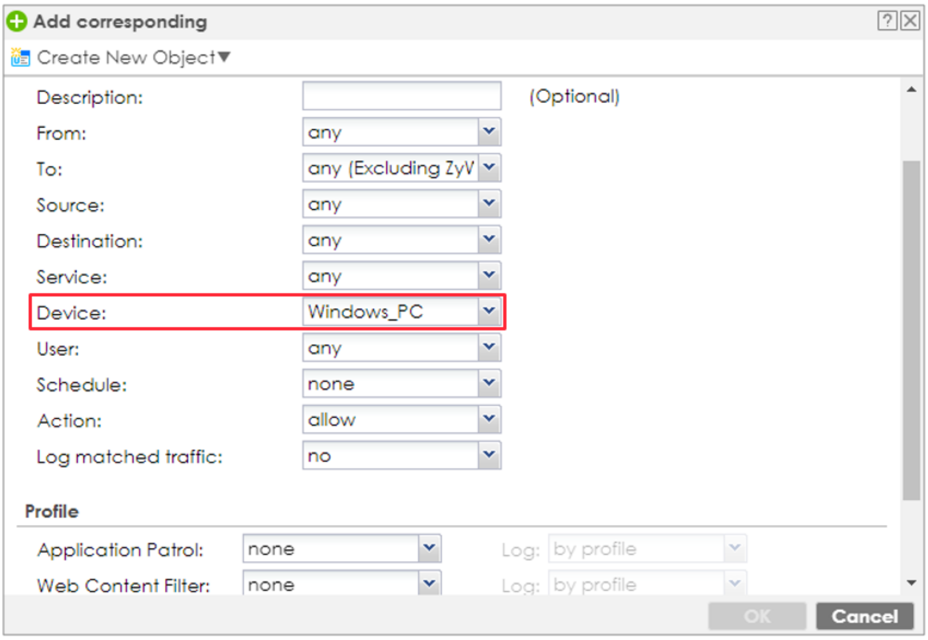
☑ Computer	☐ Firewall	☐ Game Consoles
☐ IP Camera	☐ IP Phone	☐ IoT
☐ Media Player	☐ Mobile Phone/Tablet	☐ Network Storage
☐ Printer	☐ Projector	☐ Router
☐ Smart TV	☐ Switch	☐ Wireless AP
☐ Others		

Operating System

☑ Windows	☐ macOS	☐ Linux
☐ iOS	☐ Android	☐ Others

Apply the Device Insight profile to policy control

Go to **Configuration > Security Policy > Policy Control**, create a new policy rule or select an existing one to apply the Device Insight profile. In the Device field, choose the Device Insight profile.



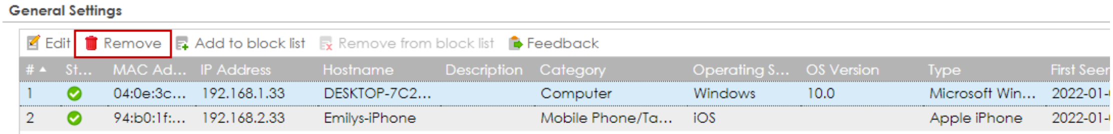
Description:		(Optional)
From:	any	
To:	any (Excluding ZyV	
Source:	any	
Destination:	any	
Service:	any	
Device:	Windows_PC	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	no	

Profile

Application Patrol:	none	Log: by profile
Web Content Filter:	none	Log: by profile

Remove selected device from the table

Go to **Monitor > Network Status > Device Insight**. Select one or more rules and click **Remove** to remove devices from the table. If the device is on the block list, it cannot be removed.



General Settings

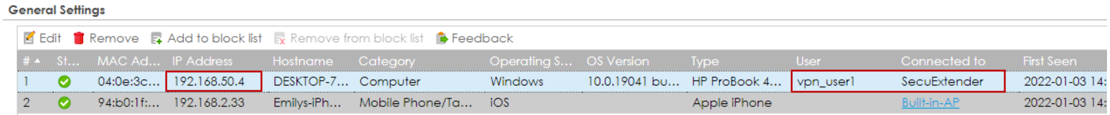
Edit | Remove | Add to block list | Remove from block list | Feedback

# ▲	St...	MAC Ad...	IP Address	Hostname	Description	Category	Operating S...	OS Version	Type	First Seer
1	✓	04:0e:3c...	192.168.1.33	DESKTOP-7C2...		Computer	Windows	10.0	Microsoft Win...	2022-01-
2	✓	94:b0:1f:...	192.168.2.33	Emilys-iPhone		Mobile Phone/Ta...	iOS		Apple iPhone	2022-01-

Online status of IPSec VPN client

Once the IPSec VPN client is connected and shows on **MONITOR > VPN Monitor > IPSec**, the online status and user name of IPSec VP client display in **MONIOR > Device Insight**.

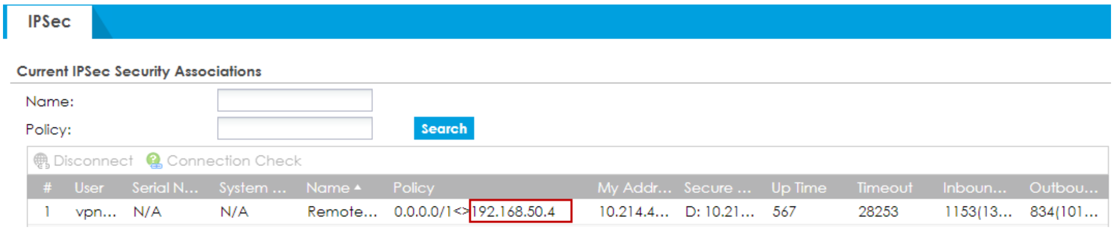
> Note: The version of IPSec VPN client must be IPSec_6.6.86.016(subscription_based) and later version.



General Settings

Edit | Remove | Add to block list | Remove from block list | Feedback

# ▲	St...	MAC Ad...	IP Address	Hostname	Category	Operating S...	OS Version	Type	User	Connected to	First Seen
1	✓	04:0e:3c...	192.168.50.4	DESKTOP-7...	Computer	Windows	10.0.19041 bu...	HP ProBook 4...	vpn_user1	SecuExtender	2022-01-03 14:
2	✓	94:b0:1f:...	192.168.2.33	Emilys-iPh...	Mobile Phone/Ta...	iOS		Apple iPhone		Built-in-AP	2022-01-03 14:



IPSec

Current IPSec Security Associations

Name:

Policy:

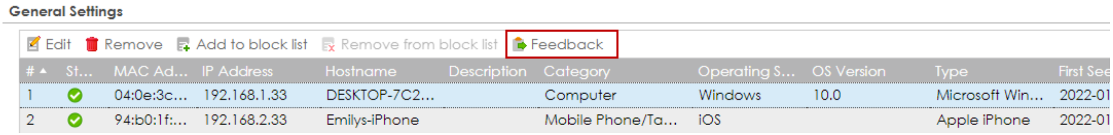
Search

Disconnect | Connection Check

#	User	Serial N...	System ...	Name ▲	Policy	My Addr...	Secure ...	Up Time	Timeout	Inboun...	Outbou...
1	vpn...	N/A	N/A	Remote...	0.0.0.0/1<>192.168.50.4	10.214.4...	D: 10.21...	567	28253	1153(13...	834(101...

Feedback button for Category/OS/Type

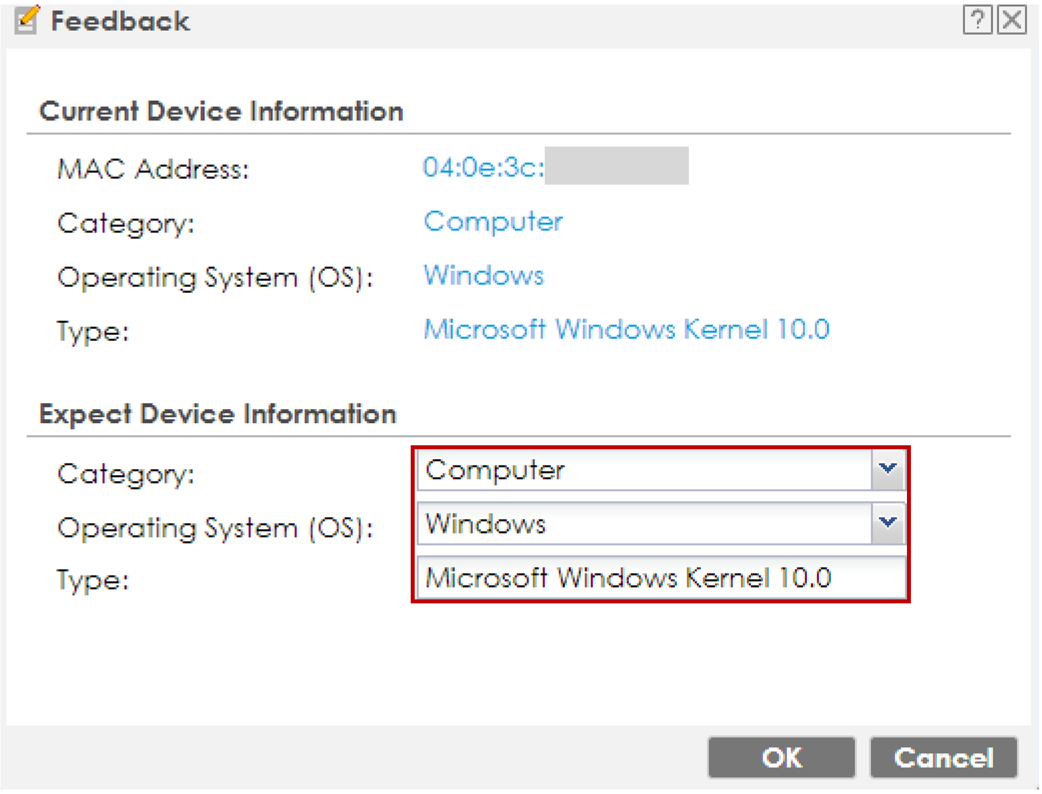
Select one rule and click Feedback to submit the request if Category/OS/Type of the device is incorrect.



General Settings

Edit | Remove | Add to block list | Remove from block list | Feedback

# ▲	St...	MAC Ad...	IP Address	Hostname	Description	Category	Operating S...	OS Version	Type	First See
1	✓	04:0e:3c...	192.168.1.33	DESKTOP-7C2...		Computer	Windows	10.0	Microsoft Win...	2022-01
2	✓	94:b0:1f:...	192.168.2.33	Emilys-iPhone		Mobile Phone/Ta...	iOS		Apple iPhone	2022-01



Current Device Information

MAC Address: 04:0e:3c:[redacted]

Category: Computer

Operating System (OS): Windows

Type: Microsoft Windows Kernel 10.0

Expect Device Information

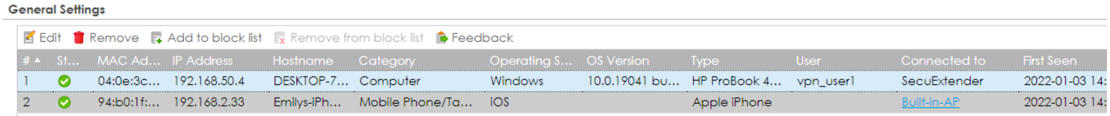
Category: Computer

Operating System (OS): Windows

Type: Microsoft Windows Kernel 10.0

Test result

Once you enable Device Insight, gateway starts to collect client device's information, and query the fingerprint database to deeply identify. Go to **Monitor > Network Status > Device Insight**, you can monitor the client device list with their detail information. Based on device info, you also can restrict access by adding to block list.

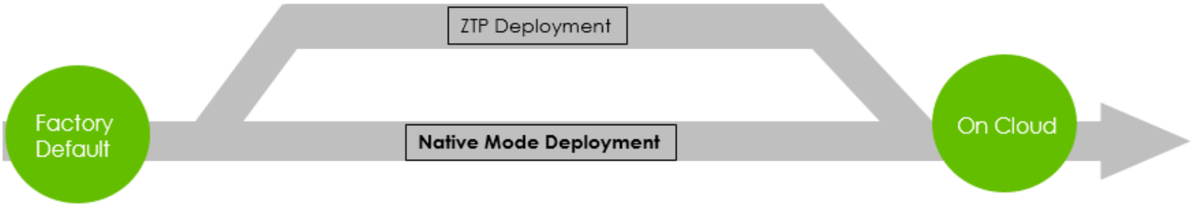


# ▲	St...	MAC Ad...	IP Address	Hostname	Category	Operating S...	OS Version	Type	User	Connected to	First Seen
1	✓	04:0e:3c...	192.168.50.4	DESKTOP-7...	Computer	Windows	10.0.19041 bu...	HP ProBook 4...	vpn_user1	SecuExtender	2022-01-03 14:
2	✓	94:b0:1f:...	192.168.2.33	Emilys-iPh...	Mobile Phone/Ta...	iOS		Apple iPhone		Built-in-AP	2022-01-03 14:

Chapter 9- Nebula Mode

How to Deploy with Nebula Native Mode for Gateway obtained ZTP Certificate?

In previous firmware versions, we use Zero-Touch Provision (ZTP) to deploy USG FLEX on the cloud. ZTP requires activation via hyperlink or USB Flash drive every time device is assigned to site, and WAN setting must be complete on Nebula Control Center. Since firmware 5.10, Native Mode provides an easier installation to deploy USG FLEX on cloud. You only require local device WAN setting to access Internet, and WAN setting can be complete on Wizard or WEB GUI. This example illustrates how to deploy the device on cloud using Nebula Native Mode.



Note: This example was tested using USG FLEX 500 (Firmware Version: ZLD 5.10). Only **USG FLEX series**, **ATP series**, **USG20-VPN** and **USG20W-VPN** support Nebula Native Mode.

Native Mode Deployment Flow

1. Verify if the device has ZTP Certificate files

2. Reset the device to factory default settings

3. Select a management mode: Nebula Mode

4. Follow the Initial Setup Wizard to configure wan IP

5. Create Organization and Site on Nebula portal and add the device to Nebula

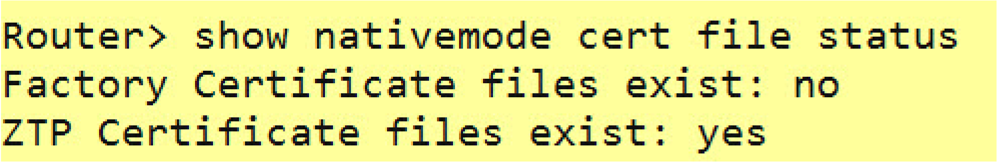
Verify if the device has ZTP Certificate files

Use the command to check the status of certificate files.

Router> show nativemode cert file status

Factory certificate files: New manufactured devices with factory certificate embedded

ZTP certificate files: Device has done the ZTP flow and gotten the ZTP certificates



```
Router> show nativemode cert file status
Factory Certificate files exist: no
ZTP Certificate files exist: yes
```

Note: Only hardware running firmware ZLD5.10 and later version with ZTP certificate or Factory Certificate can initiate Nebula Native Mode. Only **USG FLEX series**, **ATP series**, **USG20-VPN** and **USG20W-VPN** support Nebula Native Mode.

Reset the device to factory default settings

Administrator must locally apply factory default settings by pressing reset button of firewall panel before switching to cloud mode. Only the following settings may be changed and still allow firewall to switch to cloud mode:

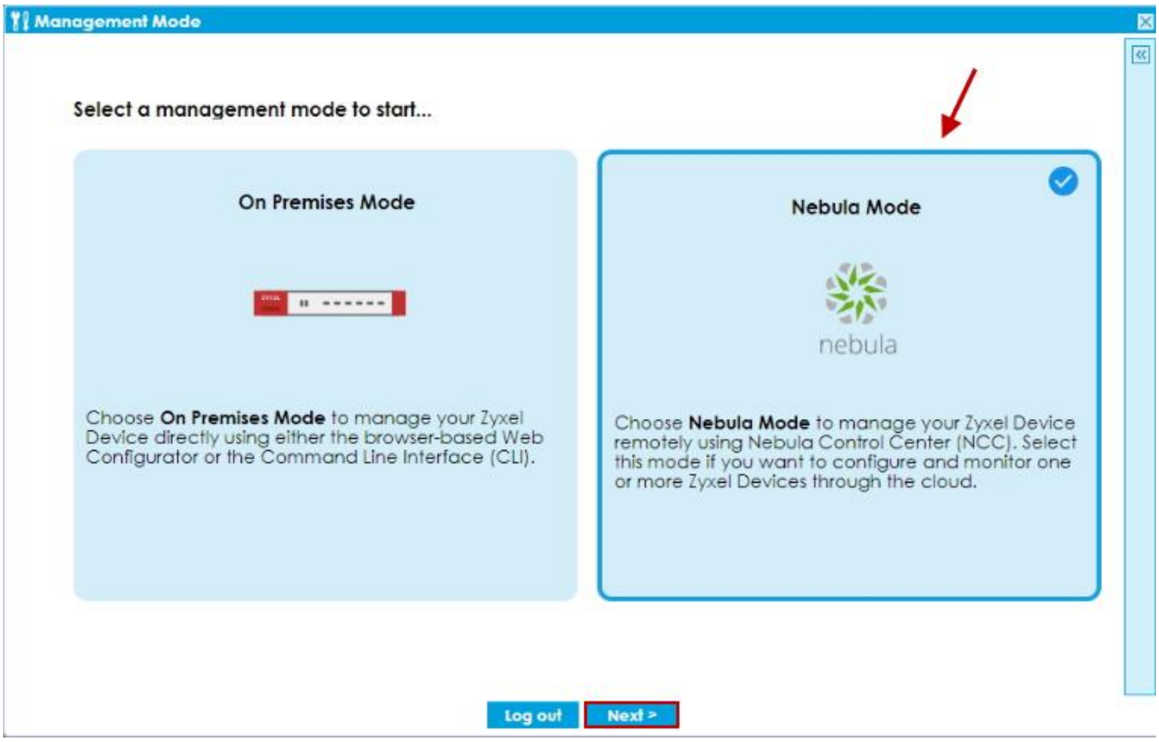
1. Default admin account's password

2. WAN settings

Select a management mode: Nebula Mode

After the device is reset to factory default, access the Setup Wizard via https://192.168.1.1.

Select **Nebula Mode** and click **Next**.

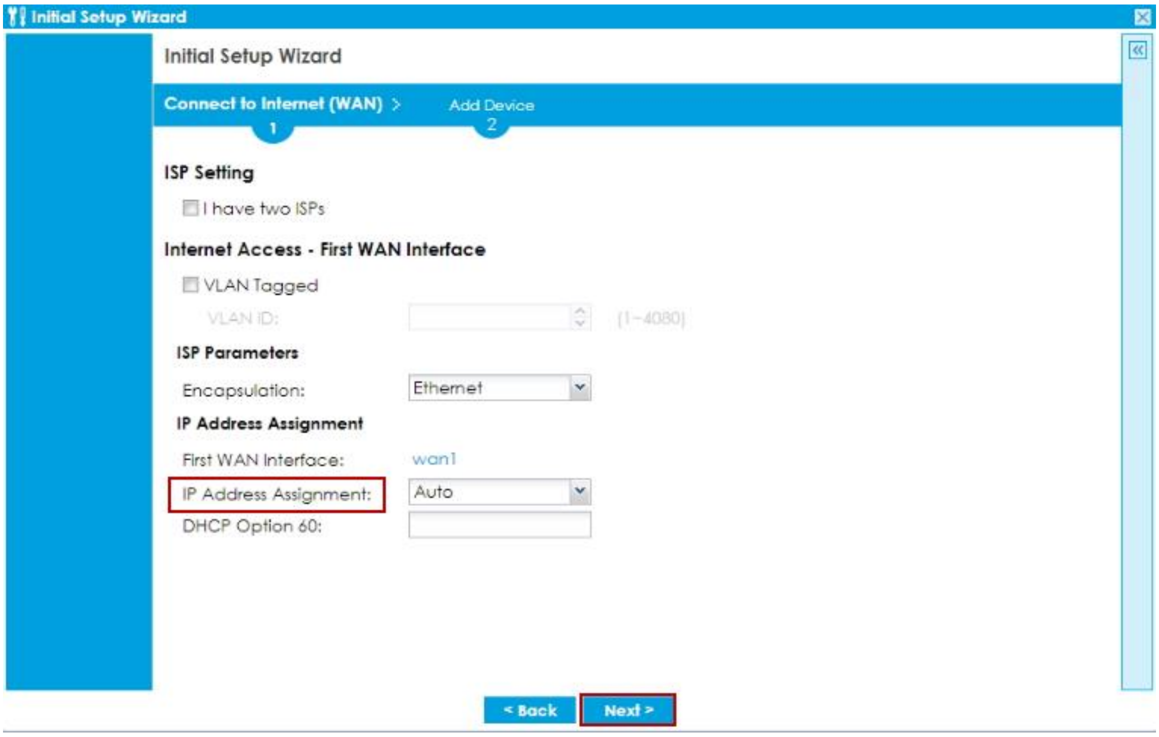


Choose **On Premises Mode** to manage your Zyxel Device directly using either the browser-based Web Configurator or the Command Line Interface (CLI).

Choose **Nebula Mode** to manage your Zyxel Device remotely using Nebula Control Center (NCC). Select this mode if you want to configure and monitor one or more Zyxel Devices through the cloud.

Note: Only device with factory default setting supports management mode selection for the first time login.

Configure WAN settings and click **Next**.



Initial Setup Wizard

Initial Setup Wizard

Connect to Internet (WAN) > 1 Add Device 2

ISP Setting

□ I have two ISPs

Internet Access - First WAN Interface

□ VLAN Tagged

VLAN ID: (1~4080)

ISP Parameters

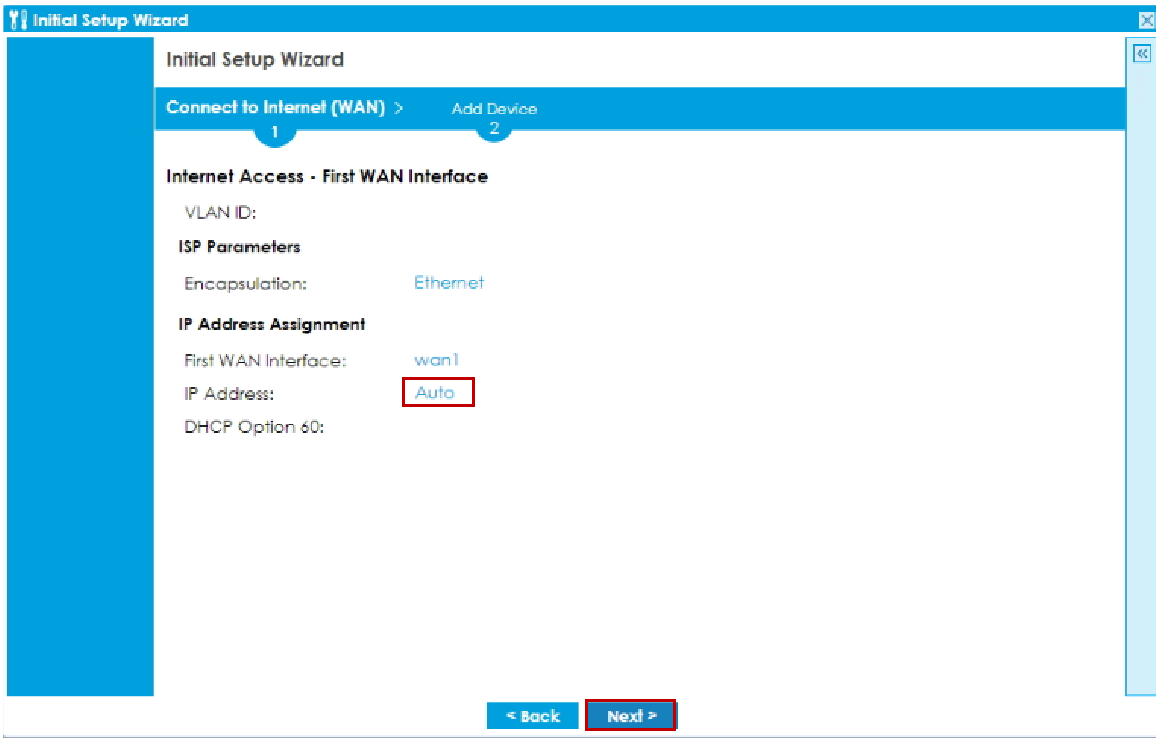
Encapsulation: Ethernet

IP Address Assignment

First WAN Interface: wan1

IP Address Assignment: Auto

DHCP Option 60:



Initial Setup Wizard

Initial Setup Wizard

Connect to Internet (WAN) > 1 Add Device 2

Internet Access - First WAN Interface

VLAN ID:

ISP Parameters

Encapsulation: Ethernet

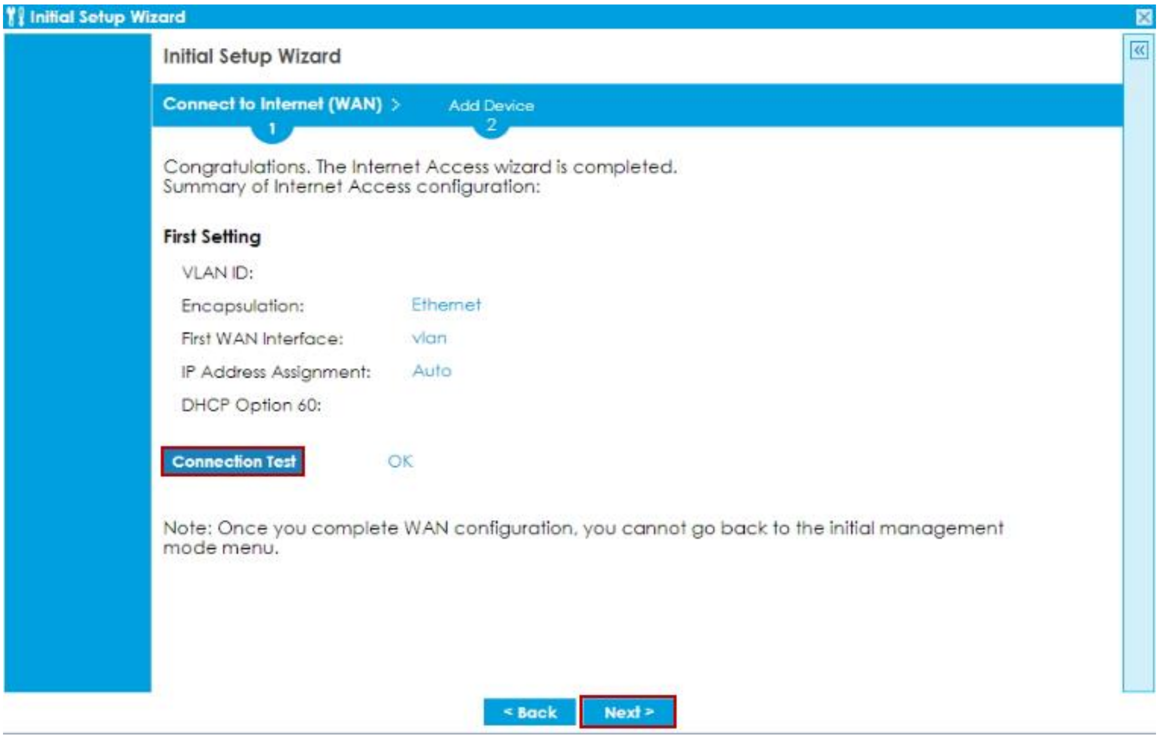
IP Address Assignment

First WAN Interface: wan1

IP Address: Auto

DHCP Option 60:

Test wan connection and click **Next**.



Initial Setup Wizard

Congratulations. The Internet Access wizard is completed.
Summary of Internet Access configuration:

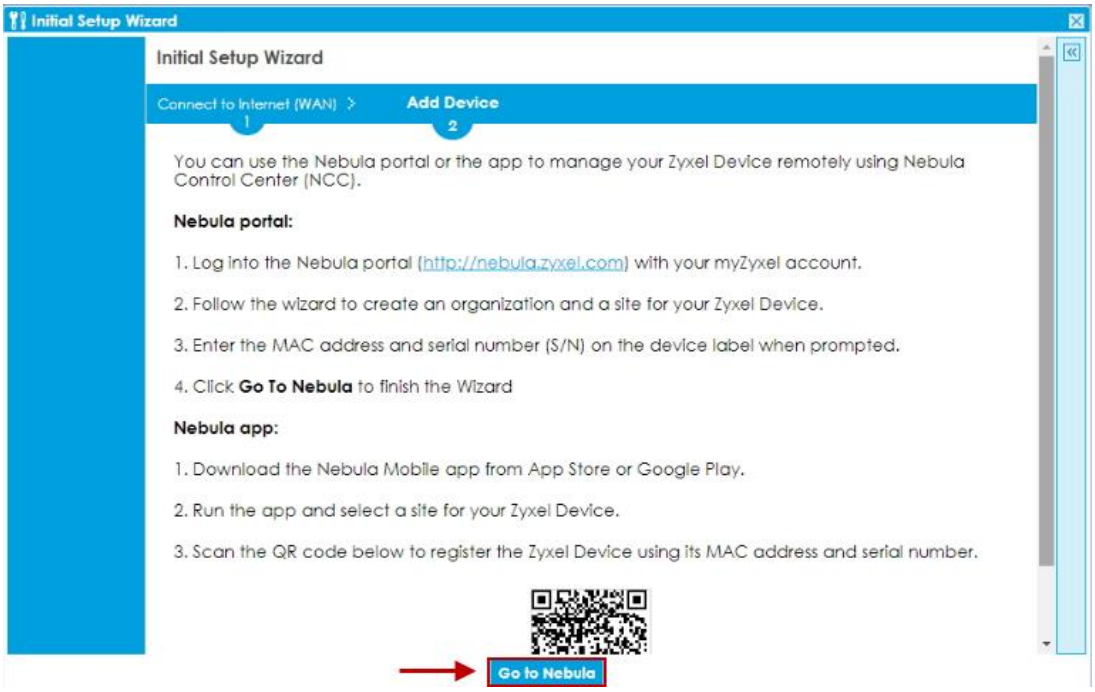
First Setting

VLAN ID:	
Encapsulation:	Ethernet
First WAN Interface:	vlan
IP Address Assignment:	Auto
DHCP Option 60:	

Connection Test OK

Note: Once you complete WAN configuration, you cannot go back to the initial management mode menu.

Click **Go to Nebula** to create Organization and Site.



Initial Setup Wizard

You can use the Nebula portal or the app to manage your Zyxel Device remotely using Nebula Control Center (NCC).

Nebula portal:

1. Log into the Nebula portal (http://nebula.zyxel.com) with your myZyxel account.

2. Follow the wizard to create an organization and a site for your Zyxel Device.

3. Enter the MAC address and serial number (S/N) on the device label when prompted.

4. Click **Go To Nebula** to finish the Wizard

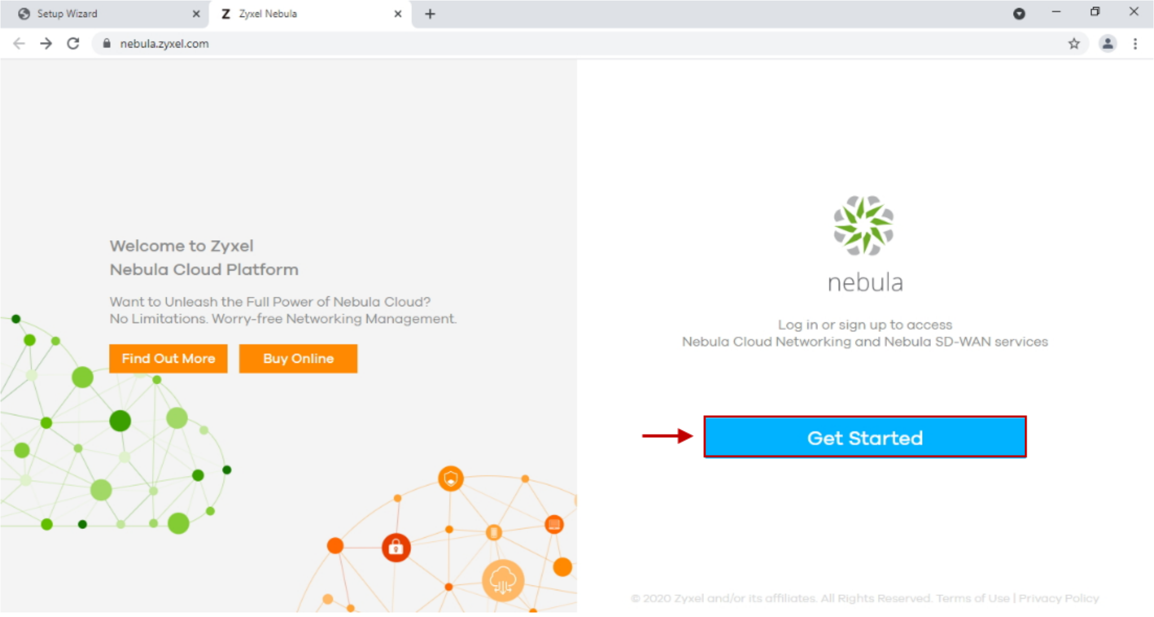
Nebula app:

1. Download the Nebula Mobile app from App Store or Google Play.

2. Run the app and select a site for your Zyxel Device.

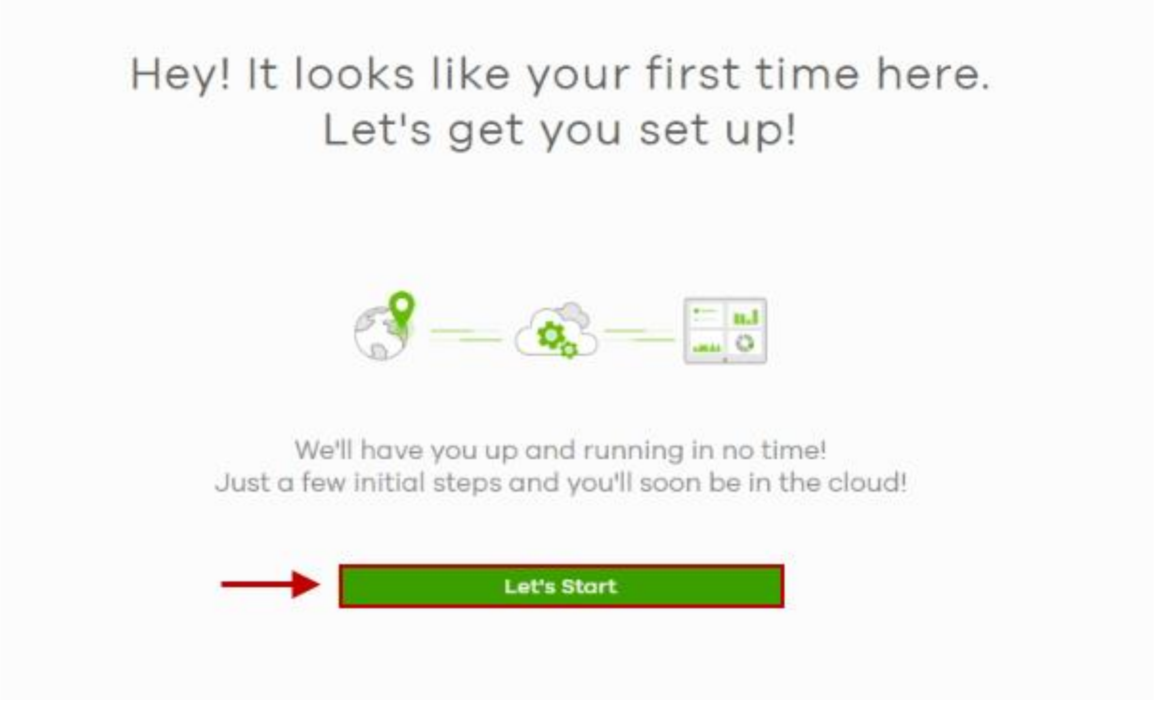
3. Scan the QR code below to register the Zyxel Device using its MAC address and serial number.

You will be redirected to nebula.zyxel.com. Click **Get Started**.



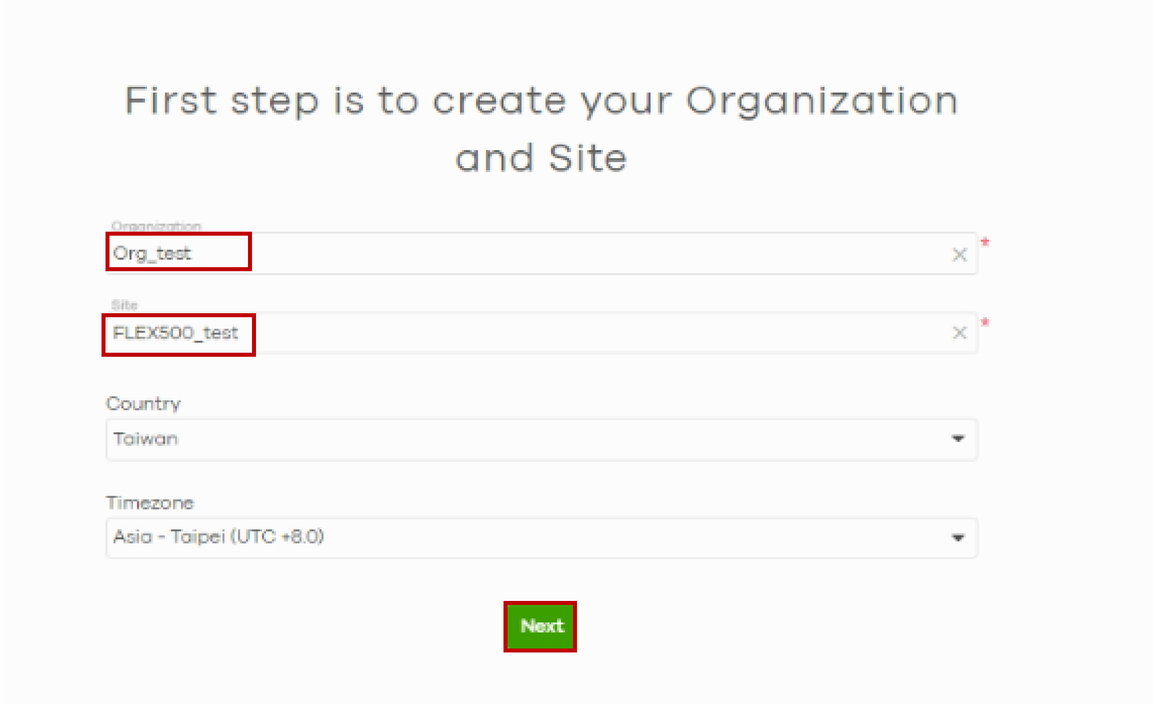
Setup Wizard
Zyxel Nebula
nebula.zyxel.com
Welcome to Zyxel
Nebula Cloud Platform
Want to Unleash the Full Power of Nebula Cloud?
No Limitations. Worry-free Networking Management.
Find Out More
Buy Online
nebula
Log in or sign up to access
Nebula Cloud Networking and Nebula SD-WAN services
Get Started
© 2020 Zyxel and/or its affiliates. All Rights Reserved. Terms of Use | Privacy Policy

Start the Nebula wizard and click **Let's Start**.



Hey! It looks like your first time here.
Let's get you set up!
We'll have you up and running in no time!
Just a few initial steps and you'll soon be in the cloud!
Let's Start

Create the organization and site.



First step is to create your Organization and Site

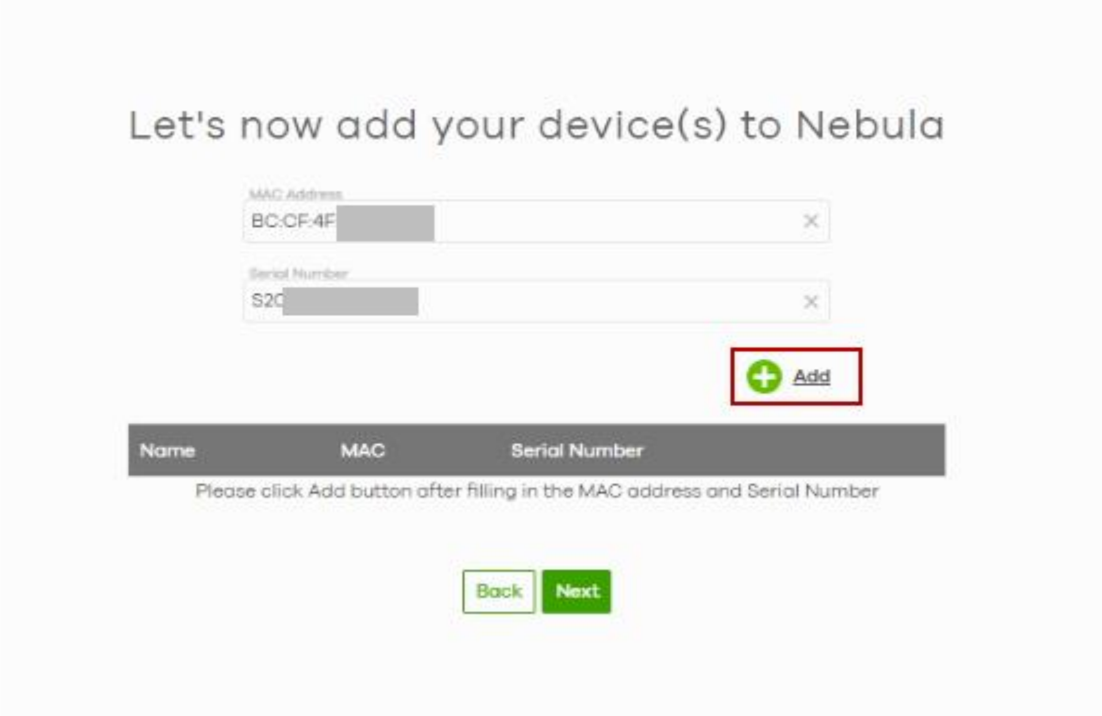
Organization: Org_test *

Site: FLEX500_test *

Country: Taiwan

Timezone: Asia - Taipei (UTC +8.0)

Enter MAC address and Serial number to add device.



Let's now add your device(s) to Nebula

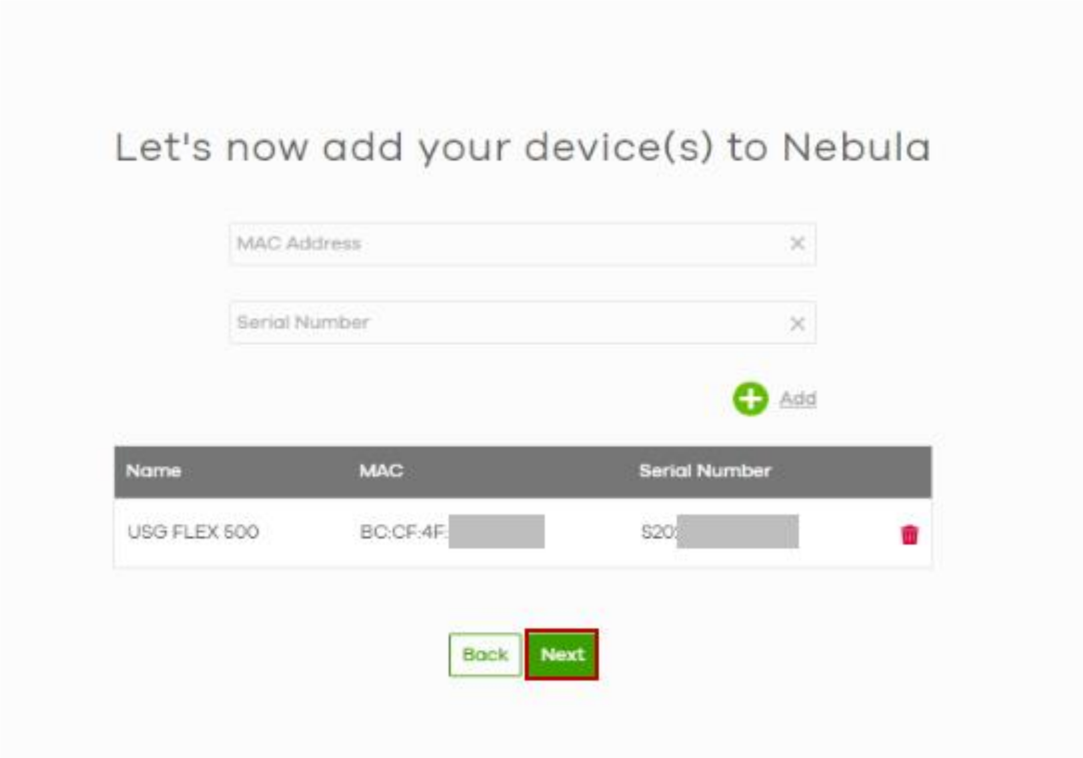
MAC Address: BC:CF:4F[redacted]

Serial Number: S2[redacted]

Name	MAC	Serial Number

Please click Add button after filling in the MAC address and Serial Number

Click **Next**.



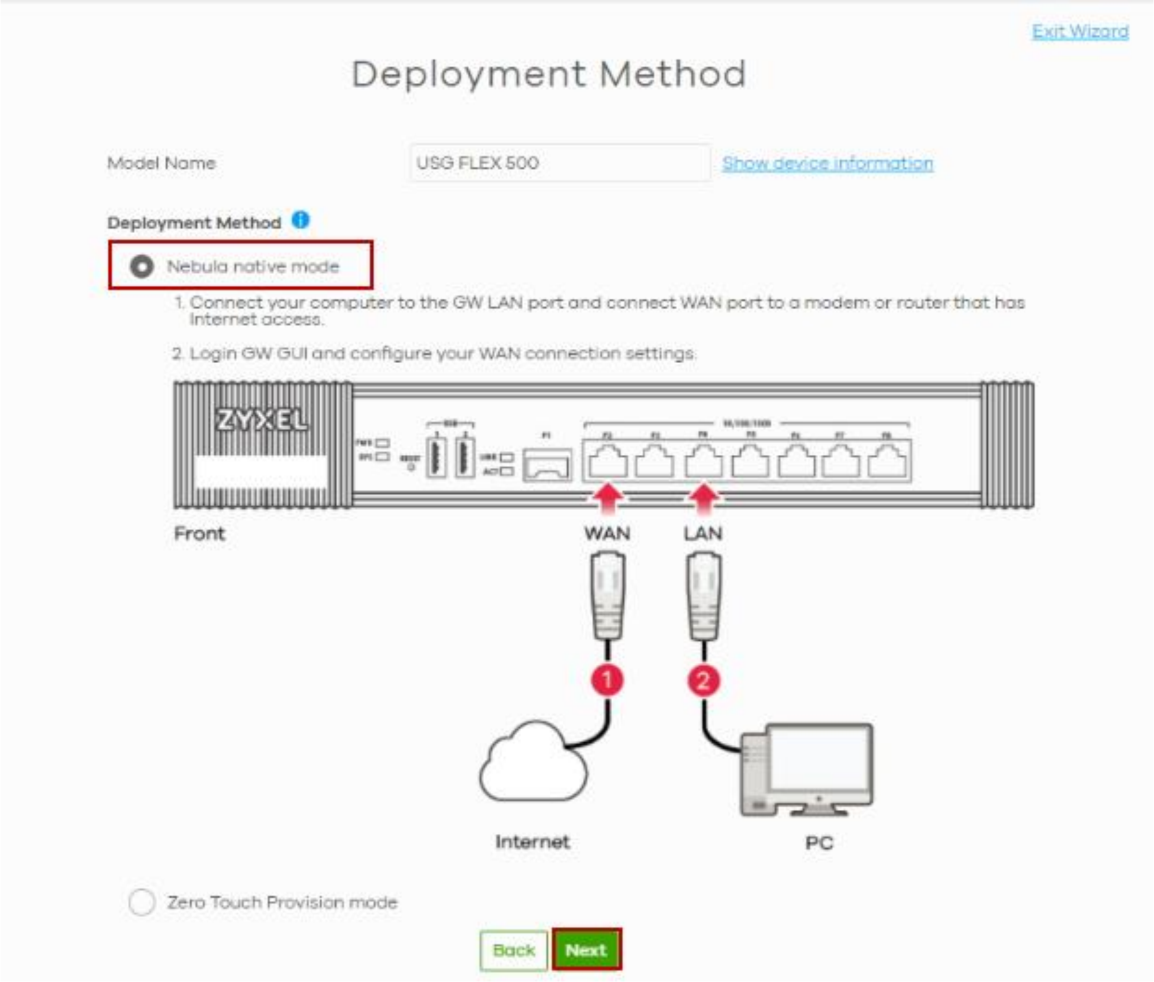
Let's now add your device(s) to Nebula

MAC Address ×

Serial Number ×

Name	MAC	Serial Number
USG FLEX 500	BC:CF:4F:[redacted]	S20[redacted]

Select **Nebula native mode** and click **Next**.



Exit Wizard

Deployment Method

Model Name: USG FLEX 500 — Show device information

Deployment Method

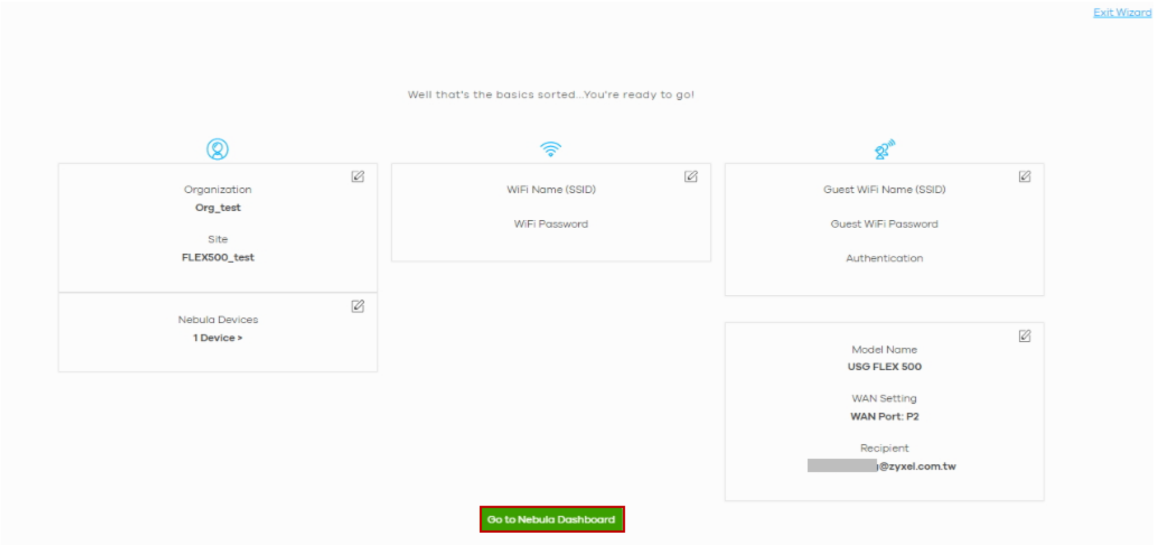
● Nebula native mode

1. Connect your computer to the GW LAN port and connect WAN port to a modem or router that has Internet access.

2. Login GW GUI and configure your WAN connection settings.

○ Zero Touch Provision mode

Check the information of the device and click **Go to Nebula Dashboard**.



Well that's the basics sorted...You're ready to go!

Organization
Org_test

Site
FLEX500_test

Nebula Devices
1 Device >

WiFi Name (SSID)

WiFi Password

Guest WiFi Name (SSID)

Guest WiFi Password

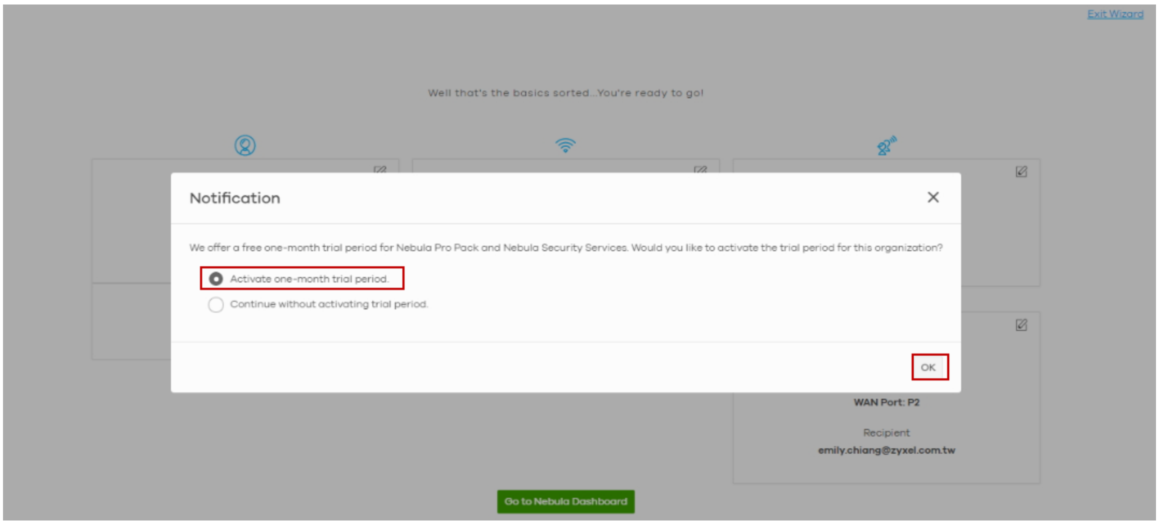
Authentication

Model Name
USG FLEX 500

WAN Setting
WAN Port: P2

Recipient
[redacted]@zyxel.com.tw

Select if you’d like to activate trial period of the license.



Well that's the basics sorted...You're ready to go!

Notification

We offer a free one-month trial period for Nebula Pro Pack and Nebula Security Services. Would you like to activate the trial period for this organization?

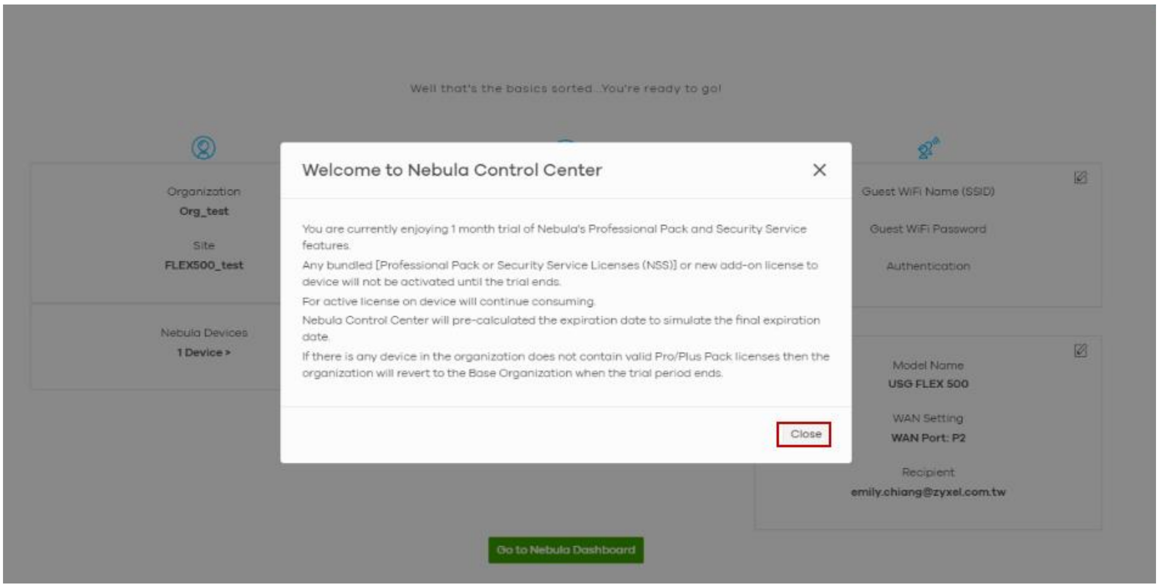
● Activate one-month trial period.

○ Continue without activating trial period.

WAN Port: P2

Recipient
emily.chiang@zyxel.com.tw

Click **Close**.



Well that's the basics sorted...You're ready to go!

Organization
Org_test

Site
FLEX500_test

Nebula Devices
1 Device >

Guest WiFi Name (SSID)

Guest WiFi Password

Authentication

Model Name
USG FLEX 500

WAN Setting
WAN Port: P2

Recipient
emily.chiang@zyxel.com.tw

Welcome to Nebula Control Center

You are currently enjoying 1 month trial of Nebula's Professional Pack and Security Service features.

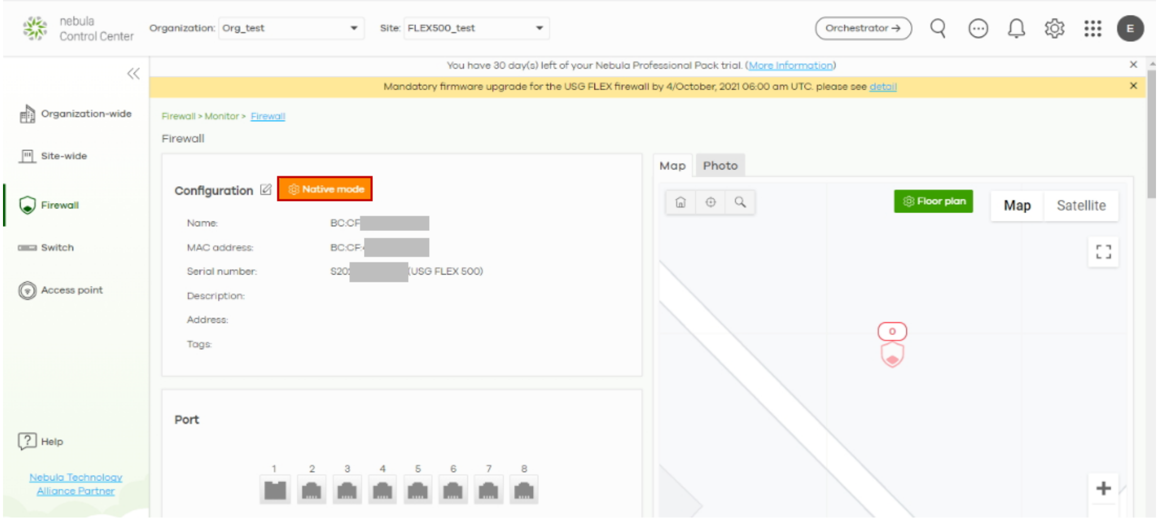
Any bundled [Professional Pack or Security Service Licenses (NSS)] or new add-on license to device will not be activated until the trial ends.

For active license on device will continue consuming.

Nebula Control Center will pre-calculated the expiration date to simulate the final expiration date.

If there is any device in the organization does not contain valid Pro/Plus Pack licenses then the organization will revert to the Base Organization when the trial period ends.

You will be redirected to Nebula Dashboard. The device is going online.



Organization: Org_test

Site: FLEX500_test

You have 30 day(s) left of your Nebula Professional Pack trial. (More Information)

Mandatory firmware upgrade for the USG FLEX firewall by 4/October, 2021 06:00 am UTC. please see detail

Firewall > Monitor > Firewall

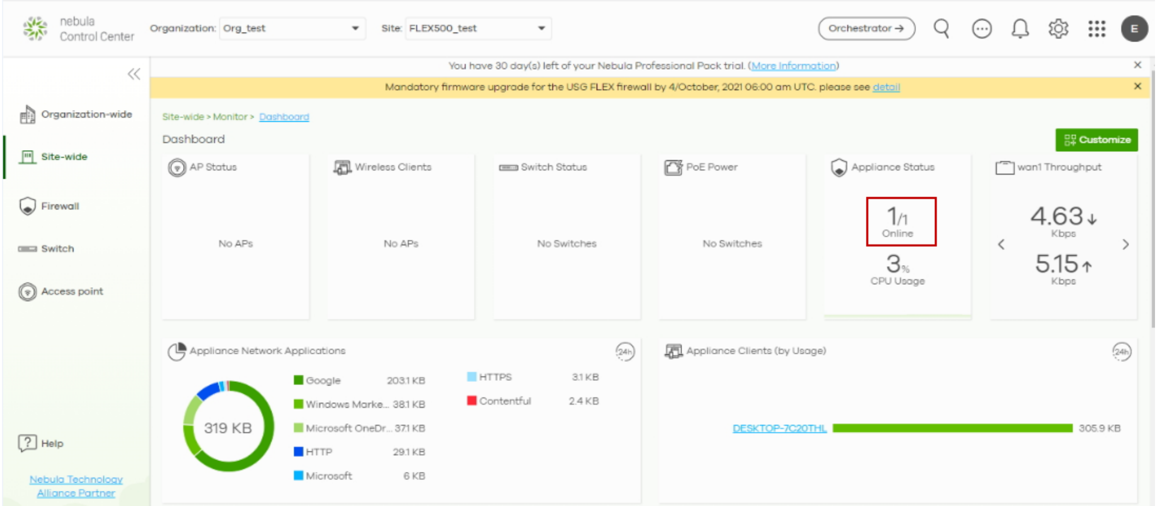
Firewall

Configuration Native mode

Name:	BC:CF[redacted]
MAC address:	BC:CF[redacted]
Serial number:	S20[redacted](USG FLEX 500)
Description:	
Address:	
Tags:	

Test the Result

Go to **Site-wide > Monitor > Dashboard** and check if the device is online.



You have 30 day(s) left of your Nebula Professional Pack trial. (More Information)

Mandatory firmware upgrade for the USG FLEX firewall by 4/October, 2021 06:00 am UTC. please see detail

Organization: Org_test

Site: FLEX500_test

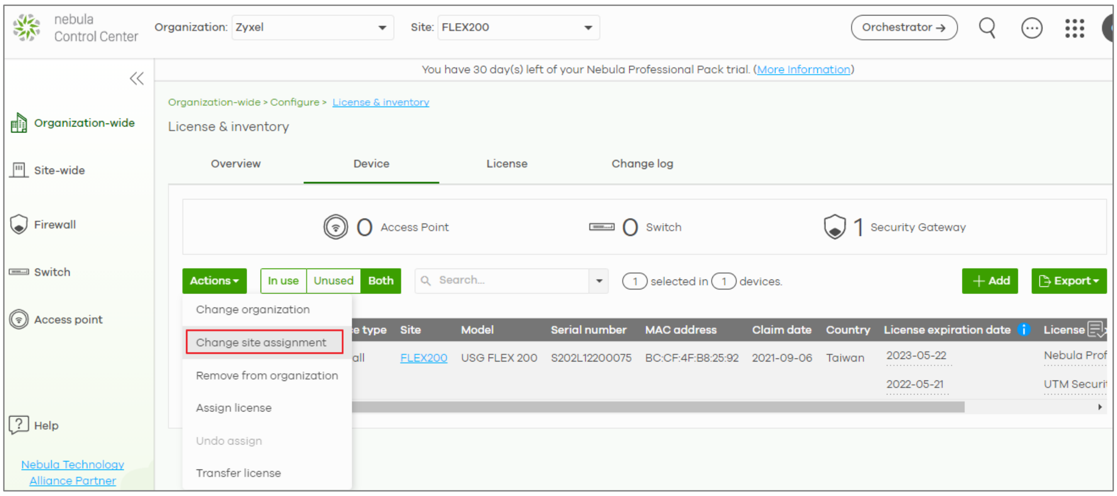
Change Site and Organization without Doing ZTP

If your gateway is running ZLD5.10 and be managed by Nebula, you are able to change device to the other site/organization on Nebula Control Center without doing Zero Touch Provisioning (ZTP).

Change to the other site within the Organization

When you change the device to other site within the Organization, the gateway's WAN setting has been remained. This enhancement helps gateway keep connection with Nebula, user don't need to go on-site to do ZTP one more time.

On Nebula, go to **Organization-wide > Configure > License & inventory > Device**, select device, then click to **Action** button and select **Change site assignment**



Organization: Zyxel

Site: FLEX200

You have 30 day(s) left of your Nebula Professional Pack trial. (More information)

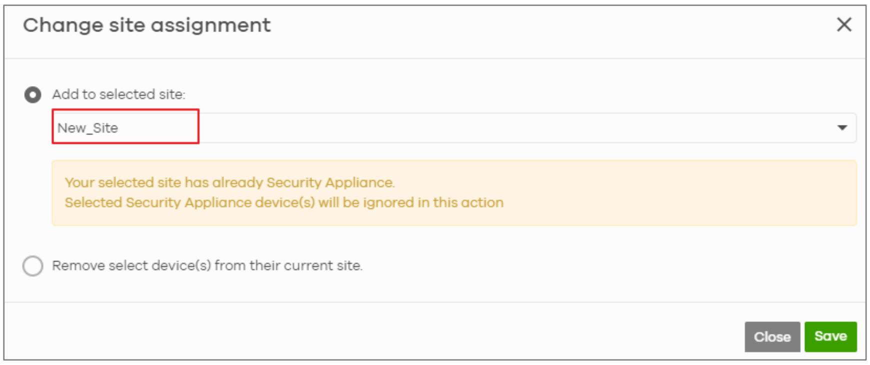
Organization-wide > Configure > License & inventory

License & inventory

1 selected in 1 devices.

e type	Site	Model	Serial number	MAC address	Claim date	Country	License expiration date	License
all	FLEX200	USG FLEX 200	S202L12200075	BC:CF:4F:B8:25:92	2021-09-06	Taiwan	2023-05-22	Nebula Prof
							2022-05-21	UTM Securi

Select **Add to selected site**, and choose target site



Change site assignment

● Add to selected site:

New_Site

Your selected site has already Security Appliance.
Selected Security Appliance device(s) will be ignored in this action

○ Remove select device(s) from their current site.

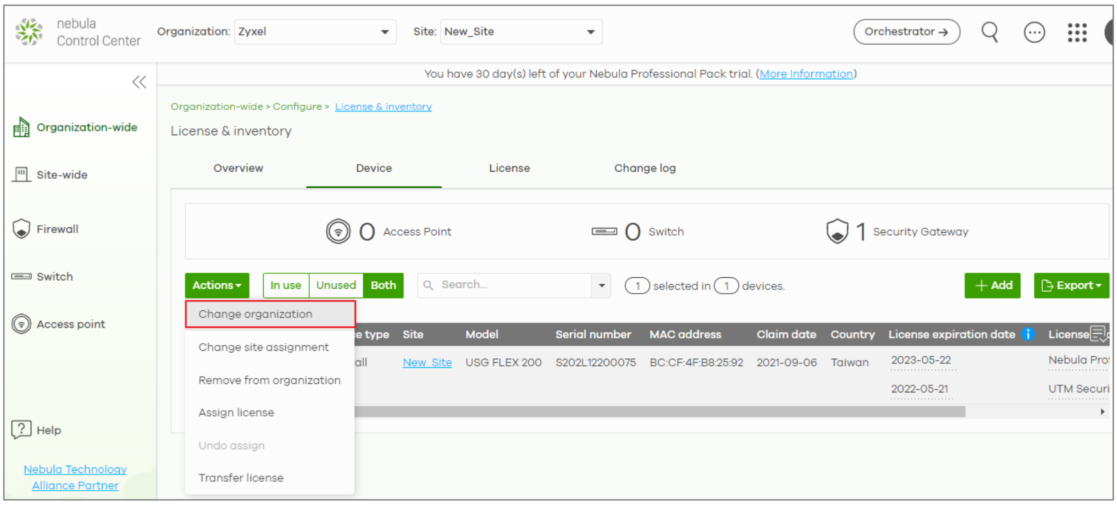
After change the site, gateway receive the request to reset to default setting but keep WAN settings from Nebula. It takes several minutes for device to reboot and get up. Then gateway will be managed by new Site on Nebula without do ZTP again.

Change to the other Organization

If you are MSP (require MSP license), you have multiple Organization. You wish to change the gateway to other Organization without repeating ZTP when your network environment doesn't change.

Now, when you change the gateway to other Organization on Nebula, you have option to remain the WAN settings. This enhancement helps gateway keep connection with Nebula even it has been changed to other Organization.

On Nebula, go to **Organization-wide > Configure > License & inventory > Device, select device**, then click to **Action** button and select **Change organization.**



Organization: Zyxel

Site: New_Site

You have 30 day(s) left of your Nebula Professional Pack trial. (More Information)

Organization-wide > Configure > License & inventory

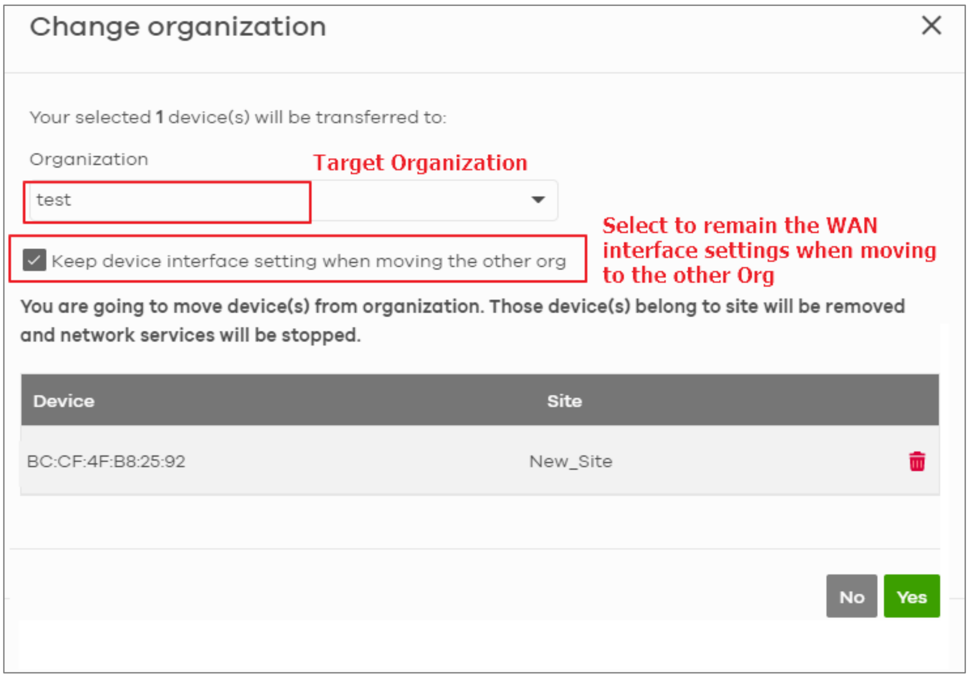
License & inventory

0 Access Point 0 Switch 1 Security Gateway

1 selected in 1 devices.

e type	Site	Model	Serial number	MAC address	Claim date	Country	License expiration date	License
all	New_Site	USG FLEX 200	S202L12200075	BC:CF:4F:B8:25:92	2021-09-06	Taiwan	2023-05-22 2022-05-21	Nebula Pro UTM Securi

Select the target organization, and select **Keep device interface setting when moving the other org.**



Change organization

Your selected **1** device(s) will be transferred to:

Organization: test

Target Organization

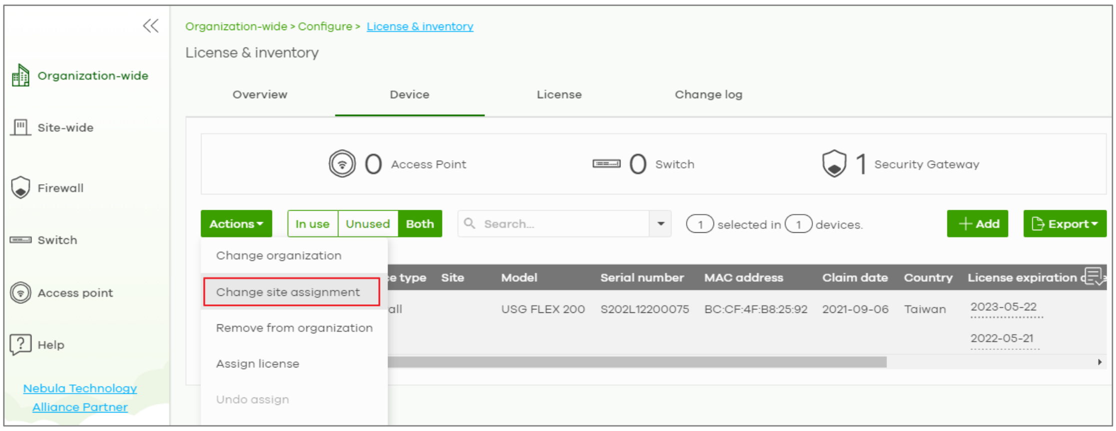
☑ Keep device interface setting when moving the other org

Select to remain the WAN interface settings when moving to the other Org

You are going to move device(s) from organization. Those device(s) belong to site will be removed and network services will be stopped.

Device	Site
BC:CF:4F:B8:25:92	New_Site

After moving the device to the new organization, you can assign the device to specific site



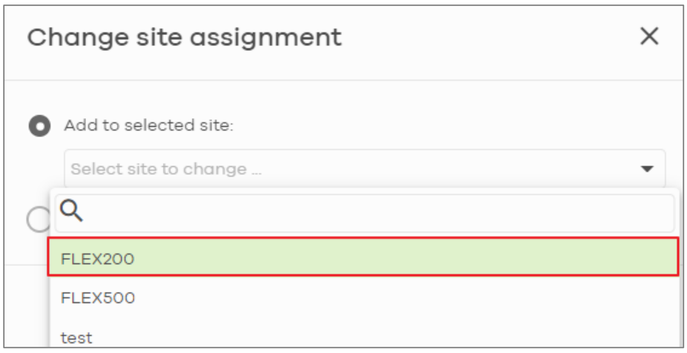
Organization-wide > Configure > License & inventory

License & inventory

0 Access Point　0 Switch　1 Security Gateway

1 selected in 1 devices.

e type	Site	Model	Serial number	MAC address	Claim date	Country	License expiration
all		USG FLEX 200	S202L12200075	BC:CF:4F:B8:25:92	2021-09-06	Taiwan	2023-05-22 2022-05-21



Change site assignment

● Add to selected site:

Select site to change ...