ZYXEL

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

copyright © 2022 ZyXEL Communications Corporation

Table of Content

Chapter 1- VPN 7

How to Configure Site-to-site IPSec VPN with Amazon VPC 7

How to Configure Site-to-site IPSec VPN with Microsoft (MS) Azure 20

How to Configure GRE over IPSec VPN Tunnel 37

How to Configure Site-to-site IPSec VPN Where the Peer has a Static IP Address 50

How to Configure Site-to-site IPSec VPN Where the Peer has a Dynamic IP Address 62

How to Configure IPSec Site to Site VPN while one Site is behind a NAT router 74

How to Configure Hub-and-Spoke IPSec VPN 87

How to Use Dual-WAN to Perform Fail-Over on VPN Using the VPN Concentrator 128

Remote Access VPN Wizard for SecuExtender IPSec and Non-SecuExtender IPSec VPN Clients 147

How to Configure Site-to-site IPSec VPN with FortiGate 165

How to Configure Site-to-site IPSec VPN with WatchGuard 177

How to Configure Site-to-site IPSec VPN with Cisco 190

How to Configure Site-to-site IPSec VPN with a SonicWALL router 204

How to Configure IPSec VPN Failover 220

How to Configure L2TP over IPSec VPN while the ZyWALL/USG is behind a NAT router 235

How to Configure L2TP VPN with Android 5.0 Mobile Devices 248

How to Configure L2TP VPN with iOS 8.4 Mobile Devices 260

How to Import ZyWALL/USG Certificate for L2TP over IPsec in Windows 10 271

How to Import ZyWALL/USG Certificate for L2TP over IPsec in iOS mobile phone 289

How to Configure 2 factor for VPN connection? 300
How to Import ZyWALL/USG Certificate for L2TP over IPsec in Android mobile phone 316
How to Configure the L2TP VPN with Apple MAC OS X 10.11 Operating System 329
How to configure if I want user can only see SSL VPN Login button in web portal login page 341
How to Deploy SSL VPN with Apple Mac OS X 10.10 Operating System 348
How To Configure SSL VPN for Remote Access Mobile Devices 361
How to Configure an SSL VPN Tunnel (with SecuExtender version 4.0.0.1) on the Windows 10 Operating System 368
How to redirect multiple LAN interface traffic to the VPN tunnel..... 374
How to Create VTI and Configure VPN Failover with VTI..... 387
Remote access VPN Wizard 403
Remote access VPN Wizard-IKEv2 Client 411
VPN Configuration Provisioning with Upload Bandwidth Limit..... 424
Chapter 2- Security Service..... 430
How to block HTTPS websites by Domain Filter without applying SSL Inspection 430
How to Configure Content Filter 2.0 with Geo IP Blocking 437
How to Configure Content Filter 2.0 with HTTPs Domain Filter..... 441
How to block the client accessing to certain country using Geo IP and Content Filter..... 447
How To Schedule YouTube Access 454
How to Detect and Prevent TCP Port Scanning with ADP 464
How to Block Facebook..... 470
How to Exempt Specific Users from a Blocked Website 480
How to Control Access To Google Drive..... 488

How to Block HTTPS Websites Using Content Filtering and SSL Inspection 496
How to Block the Spotify Music Streaming Service 507
How does Anti-Malware work 511
How to Configure an Email Security Policy with Mail Scan and DNSBL515
How to Configure Botnet Filter on ATP series? 520
How to Use Sandboxing to Detect Unknown Malware 526
How to configure Email Security for Phishing mail?.....533
How to Use IP Reputation to Detect Threats.....537
How to Configure Reputation Filter- DNS Filter 543
How to customize external block list in Reputation Filter.....547
How to Configure DNS Content Filter (On-Premises) 553
How to Configure DNS Content Filter (On-Cloud) 558
How to configure Collaborative Detection & Response to identify and quarantine compromised devices from your network.....562
Chapter 3- Authentication.....571
How to Activate Hotspot Free Time Service 571
How to setup Two-Factor Authentication for admin login 577
How to setup Email to SMS 584
How to Use Two Factor with Google Authenticator for Admin Access 590
How to Use Two Factor with Google Authenticator for VPN Access ..599
Chapter 4- Device HA.....609
How to Configure Device HA Pro 609
How to Configure Schedule Reboot in Device HA 617
Chapter 5- IPv6 620
How to set up 6to4 on the WAN and autoconf on the LAN 620
How to set up 6to4 on the WAN and DHCPv6 on the LAN 625

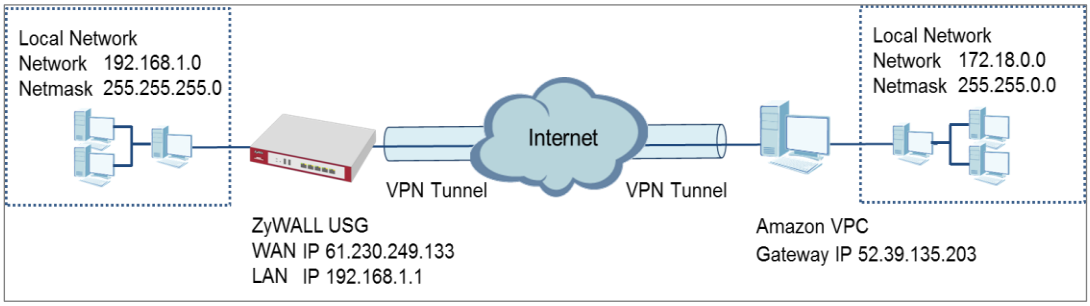
How to set up Static IPv6 on WAN and auto-configuration on the LAN 630
How to set up Static IPv6 on WAN and DHCPv6 on the LAN 635
How to Set Up DHCPv6 without prefix delegation on the WAN and autoconf on the LAN 640
How to Set Up DHCPv6 with prefix delegation on the WAN and DHCPv6 on the LAN 645
How to Set Up Autoconf on the WAN and DHCPv6 on the LAN 651
How to Set Up 6rd on the WAN and autoconf on the LAN 656
How to Set Up IPv6 over PPPoE on the WAN 662
Chapter 6- Wireless 667
How to Set Up a WiFi Network with ZyXEL APs 667
How to Set Up Guest WiFi Network Accounts 672
How to create a Wi-Fi VLAN interfaces to separate staff network and Guest network 681
How to Set Up WiFi Networks with Microsoft Active Directory Authentication 696
How to Configure Secure Wi-Fi to Secure the Wireless Environment? 704
Chapter 7- Maintenance 709
How to Manage ZyWALL/USG Configuration Files 709
How to Manage ZyWALL/USG Firmware 715
How to Automatically Reboot the ZyWALL/USG by Schedule 721
How to continuously run a ZySH script 726
How to Update Firmware Automatically from a USB Storage 730
Chapter 8- Others 737
How to Get Started Using the Wizards 737
How to Restrict Web Portal access from the Internet 752
How to Setup and Configure Daily Report 756

How to Setup and Configure Email Logs 762
How to Setup and send logs to a Syslog Server 766
How to Setup and send logs to the USB storage 772
How to Perform and Use the Packet Capture Feature on the ZyWALL/USG 776
How to Exempt Specific Users from Security Control 781
How to Configure Bandwidth Management for FTP and HTTP Traffic .788
How to Limit BitTorrent or Other Peer-to-Peer Traffic 795
How to Configure a Trunk for WAN Load Balancing with a Static or Dynamic IP Address.....801
How to Configure DNS Inbound Load Balancing to balance DNS Queries Among Interfaces.....806
How to Manage Voice Traffic 811
How to Configure the 3G/LTE Interface on the ZyWALL/USG as a WAN Backup.....818
How to Configure Two Different WAN Interfaces with Different IP Addresses in the Same VLAN 823
How to Let a Server Use the Same Public IP Address as the WAN Interface Using the Bridge Interface 828
How to Allow Public Access to a Server Behind ZyWALL/USG 831
How to Configure DHCP Option 60 – Vendor Class Identifier.....835
How to set up Link Aggregation Group (LAG) 839
How to configure Device Insight.....847
Chapter 9- Nebula Mode 851
How to Deploy with Nebula Native Mode for Gateway obtained ZTP Certificate? 851
Change Site and Organization without Doing ZTP.....863

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.



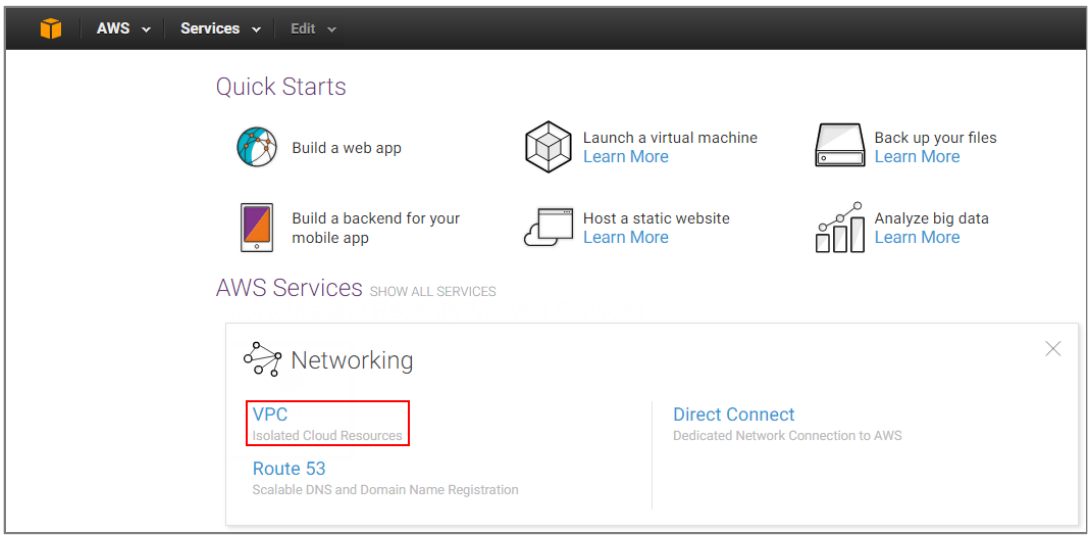
ZyWALL/USG Site-to-site IPSec VPN with Amazon VPC

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

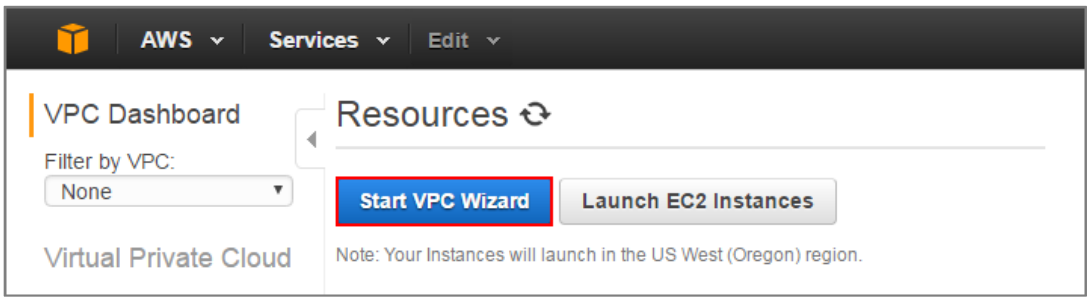
1 Sign into the Amazon AWS Management Console. Go to Networking > VPC.

Amazon AWS Management Console > Networking > VPC



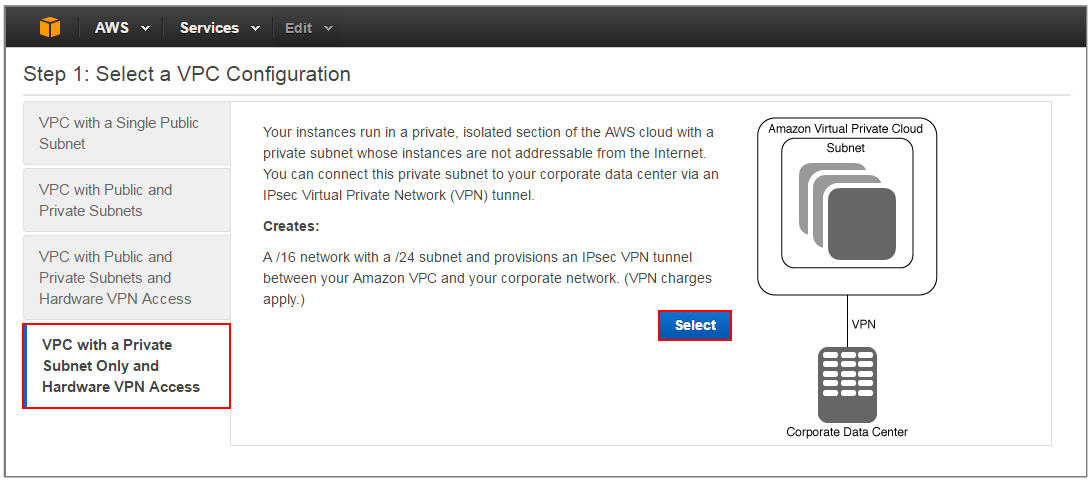
2 In the upper left-hand of the screen, click **Start VPC Wizard**.

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



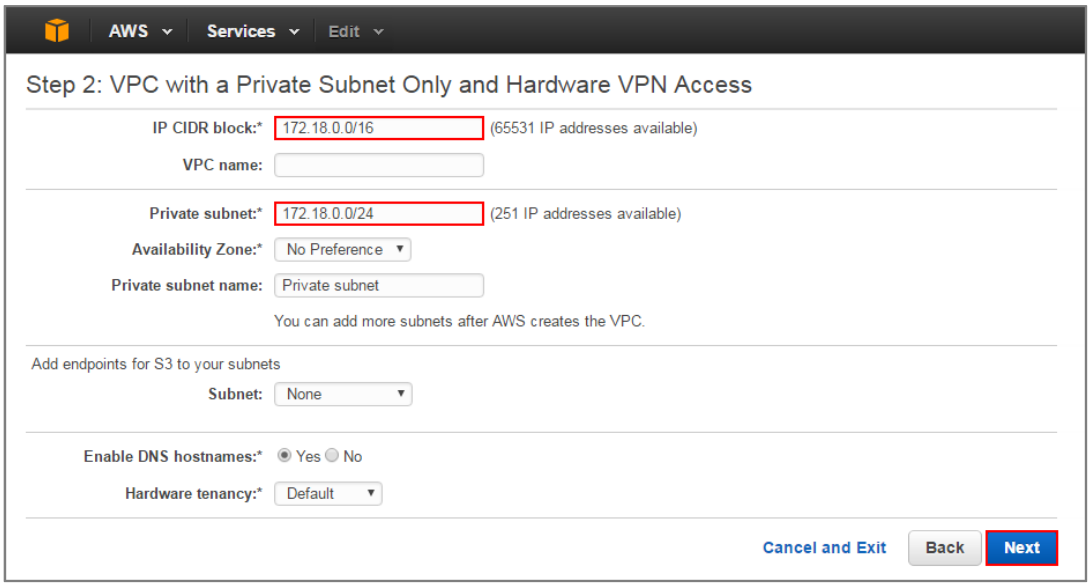
3 Select a VPC Configuration, select VPC with a Private Subnet Only and Hardware VPN Access, and then click Select.

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



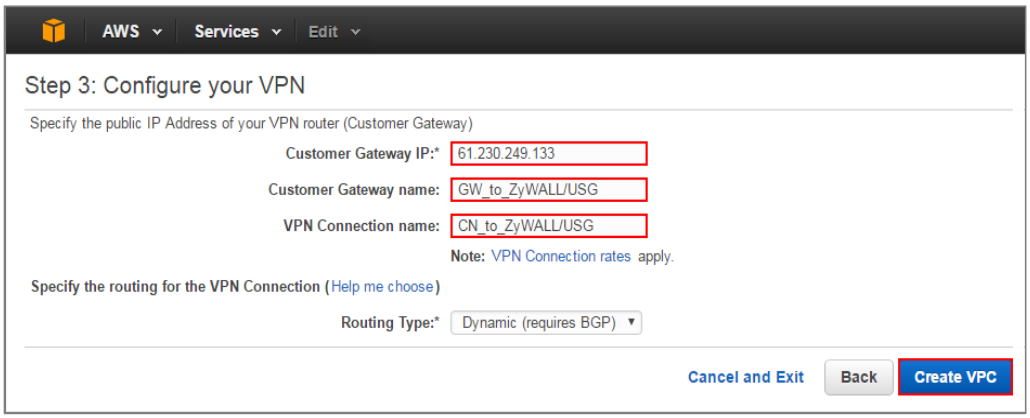
4 VPC with a Private Subnet Only and Hardware VPN, add your **IP CIDR block** and **Private subnet**. Click **Next**.

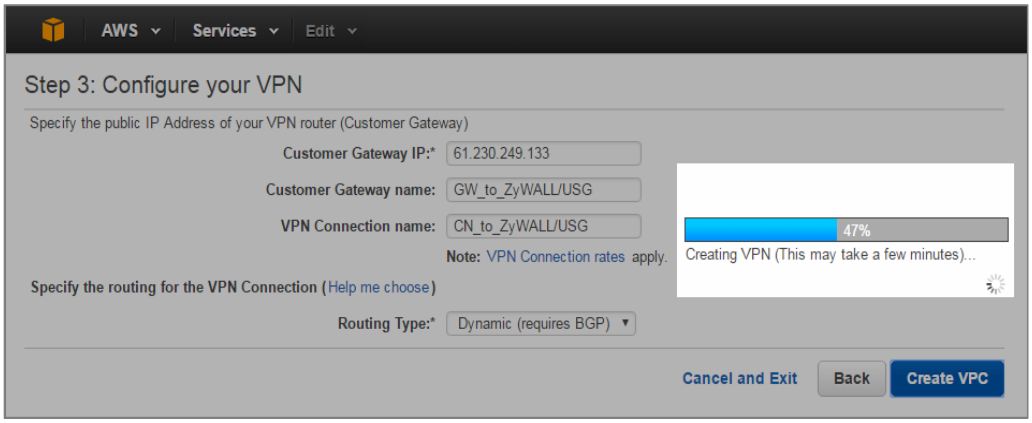
VPC with a Private Subnet Only and Hardware VPN



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.

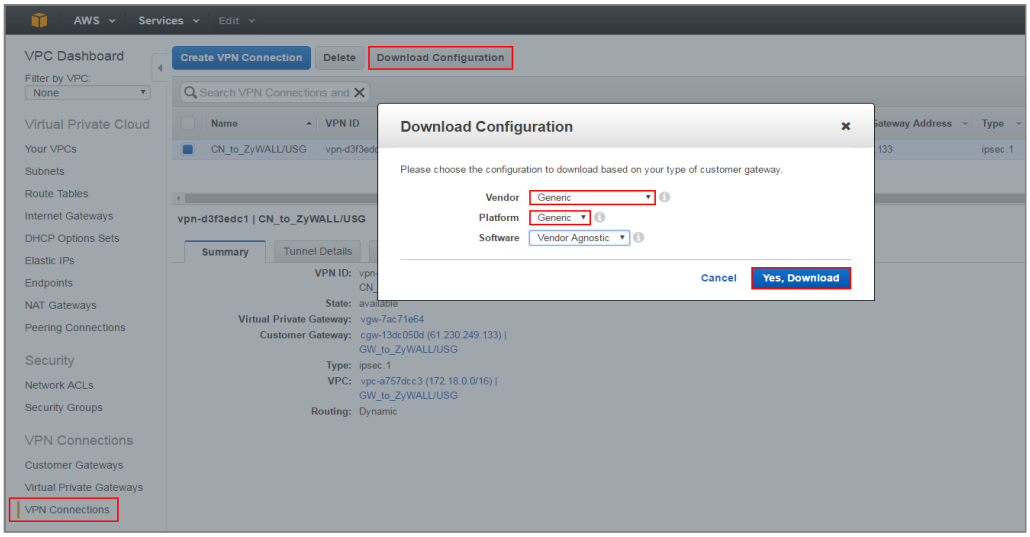
Configure your VPN





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



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.

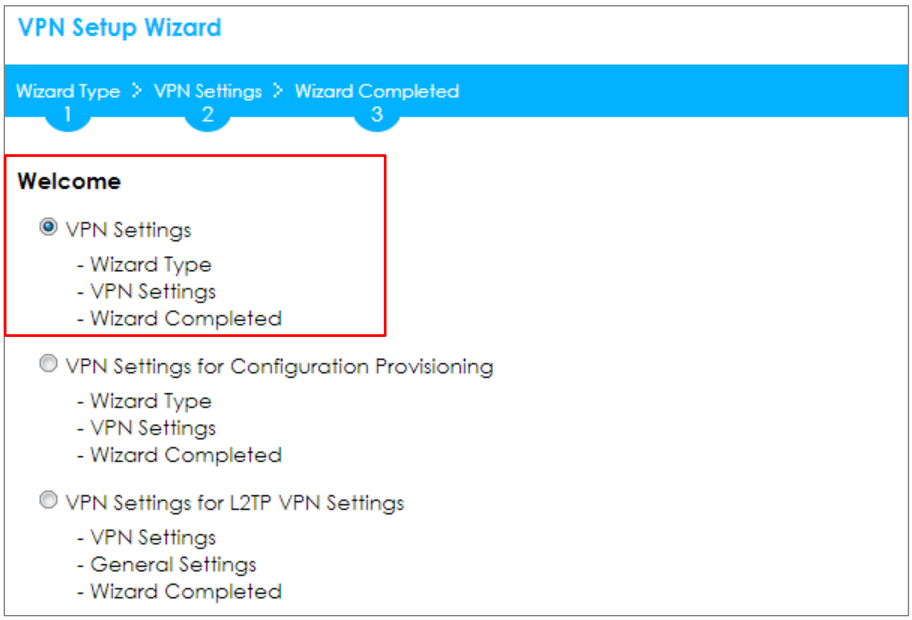
Configuration txt. File

```
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

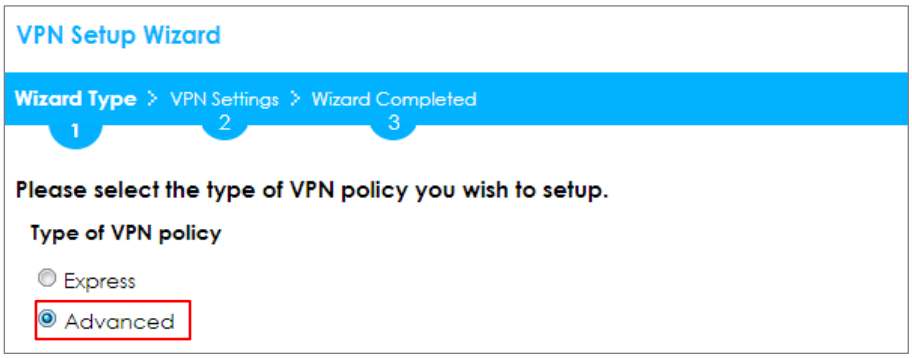
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the Amazon VPC. Click **Next**.

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



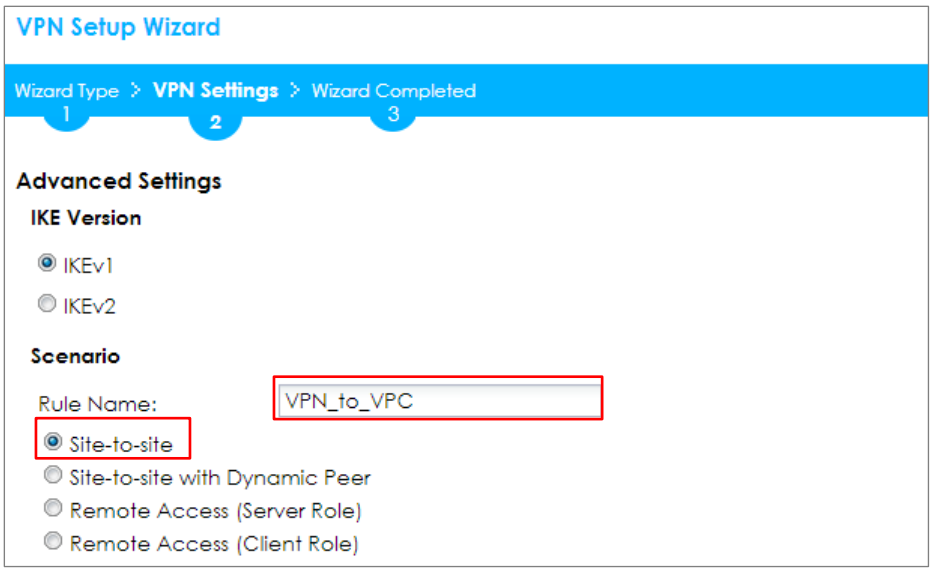
Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



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**.

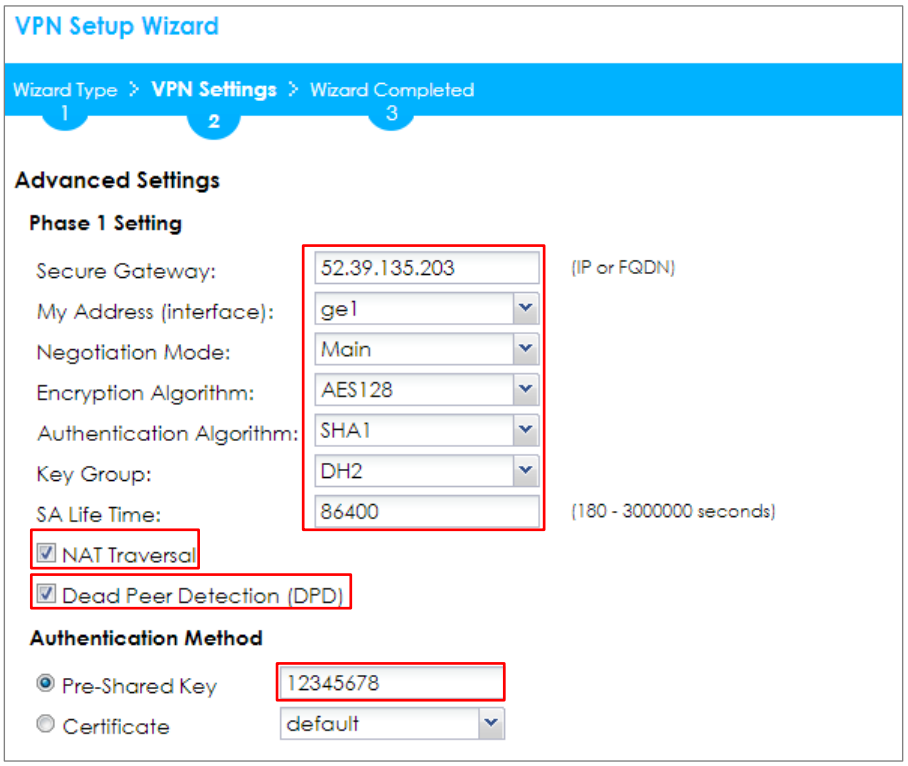
Quick Setup **> VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)**



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**.

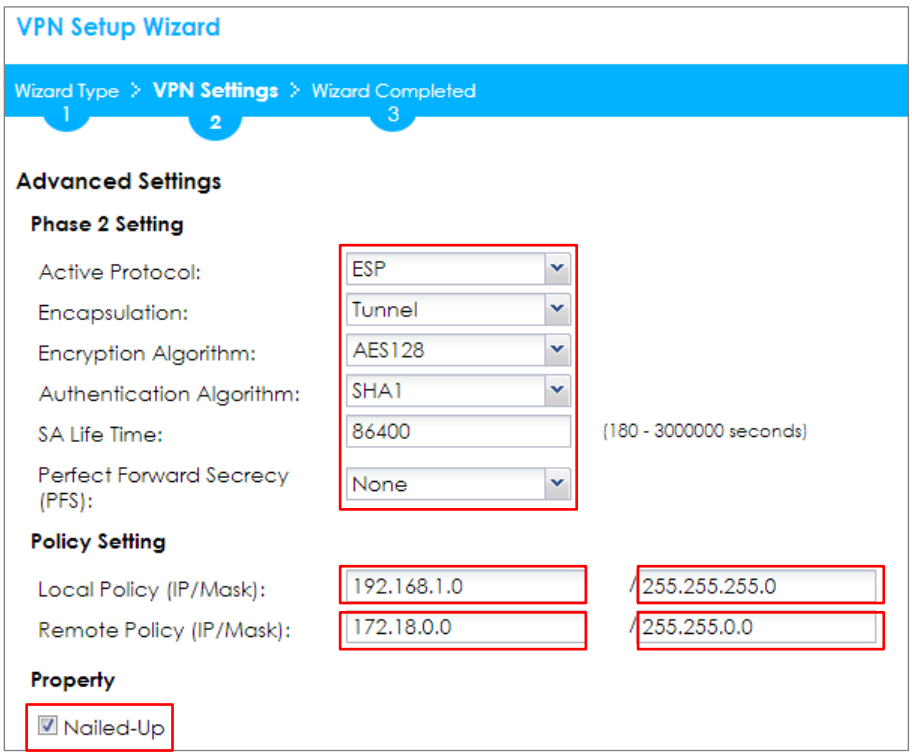
Quick Setup **> VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 1 Setting)**



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)**



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

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**

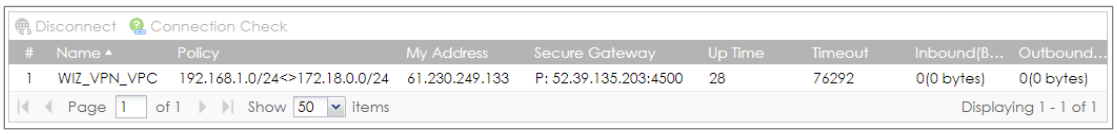
Test the IPSec VPN Tunnel

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

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



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

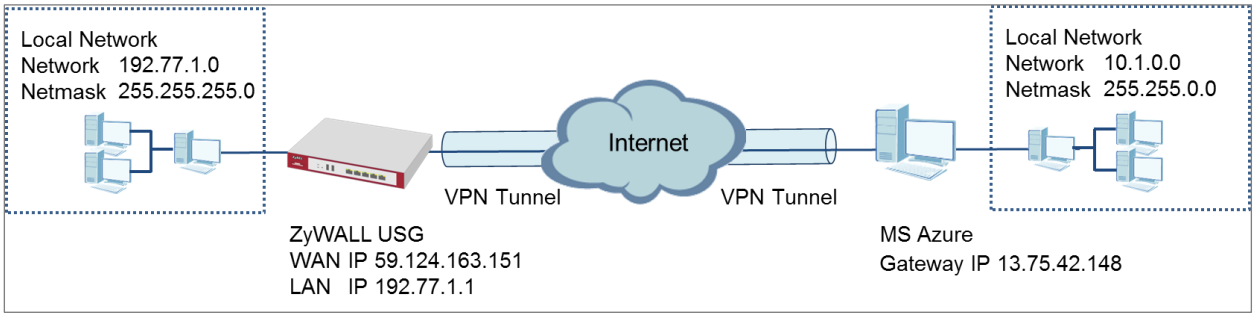
If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Make sure your ZyWALL/USG Phase 2 Settings are supported in the Amazon VPC IKE Phase 2 setup list.

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.



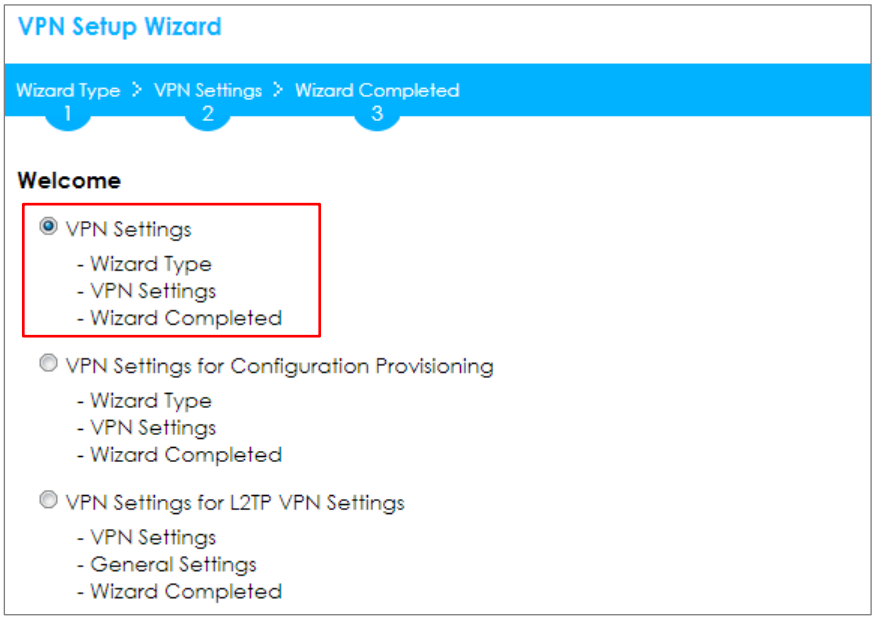
ZyWALL Site-to-site IPSec VPN with Microsoft (MS) Azure

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

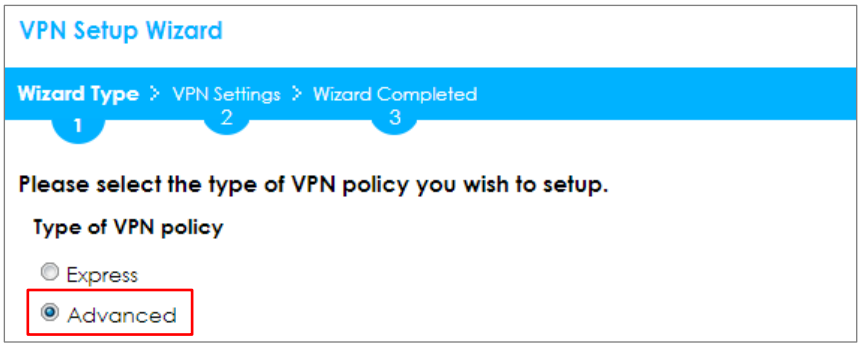
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the MS Azure. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



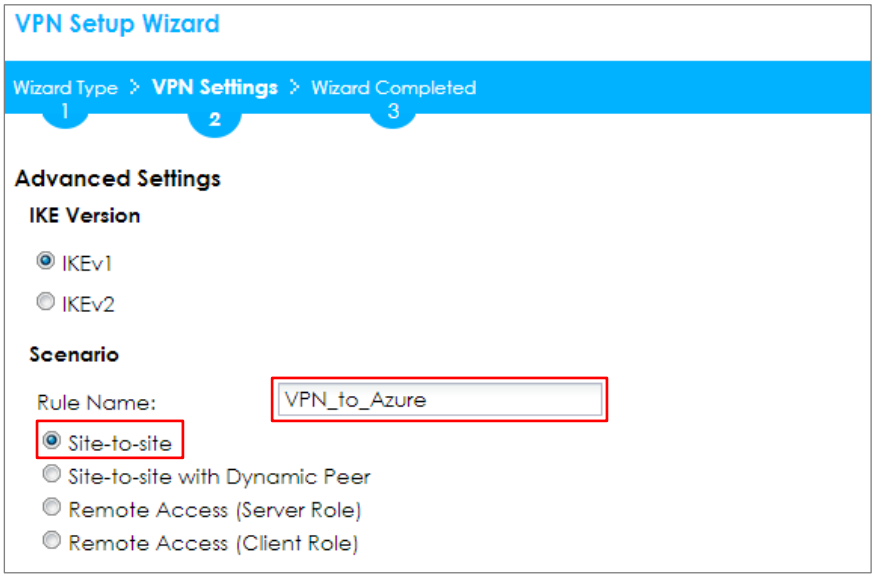
Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



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**.

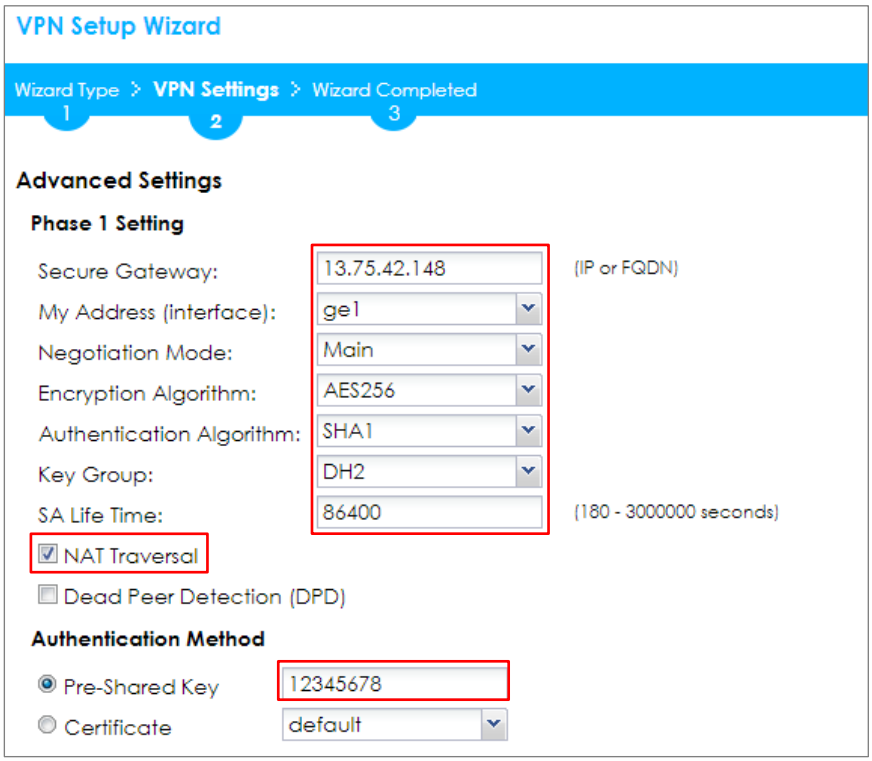
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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)

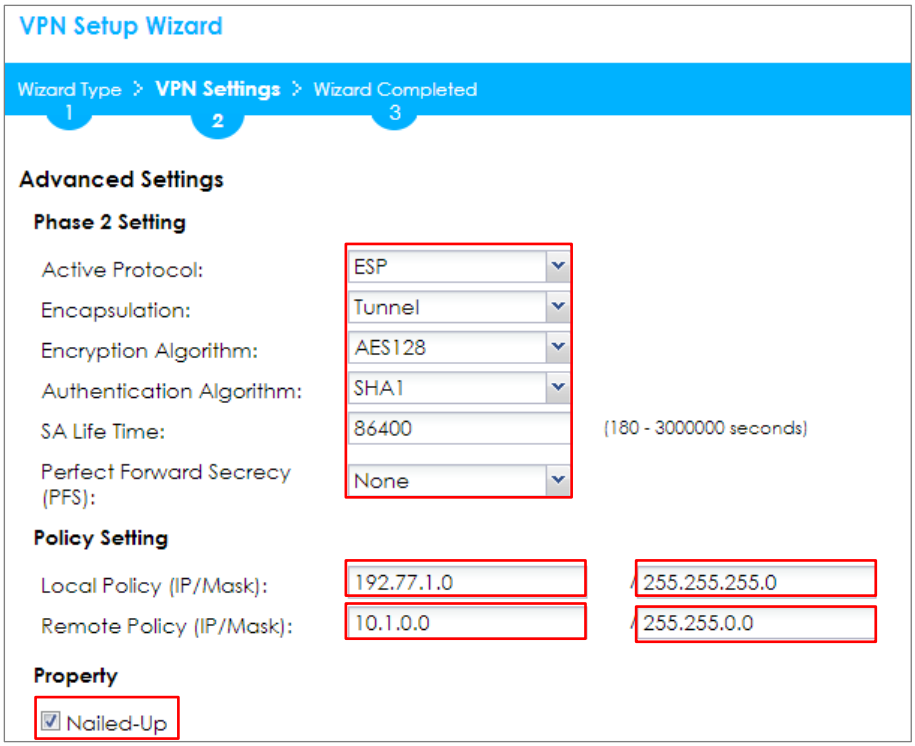


Note: For more information about the IPsec Parameters supported in MS Azure, see the Microsoft Azure Documentation **About VPN devices** for Site-to-Site VPN Gateway connections.

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**.

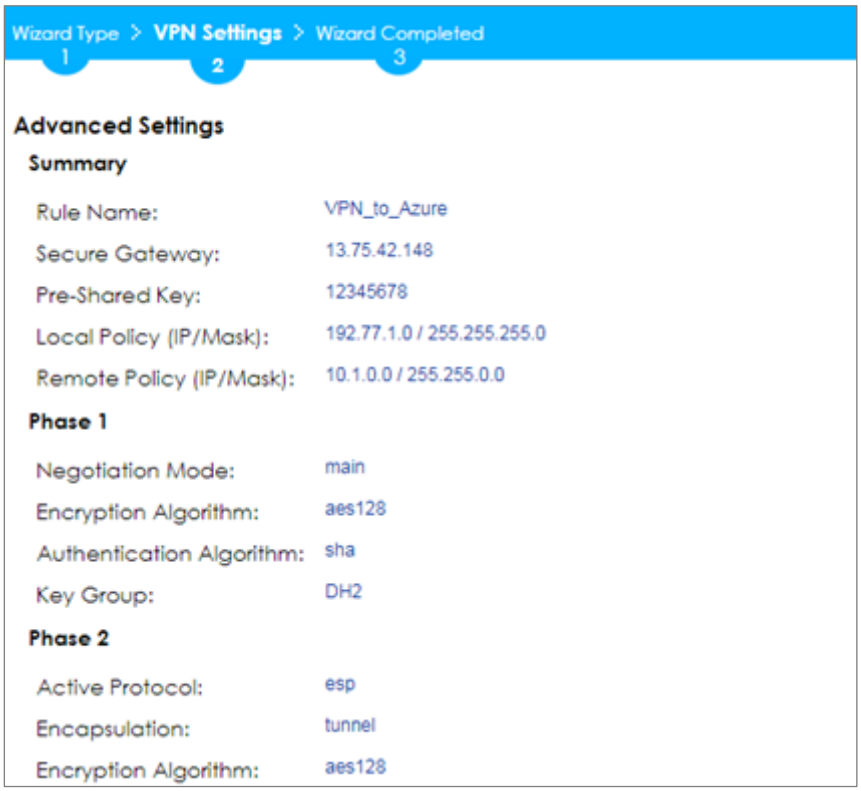
Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 2 Setting)



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.

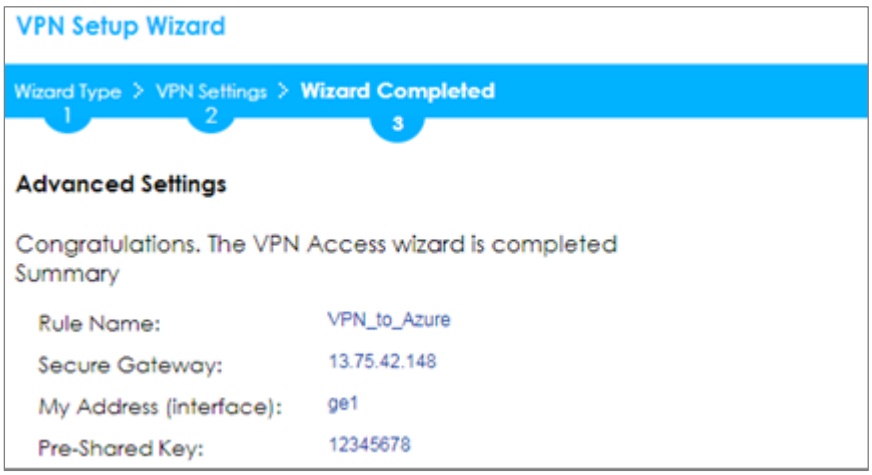
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



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.

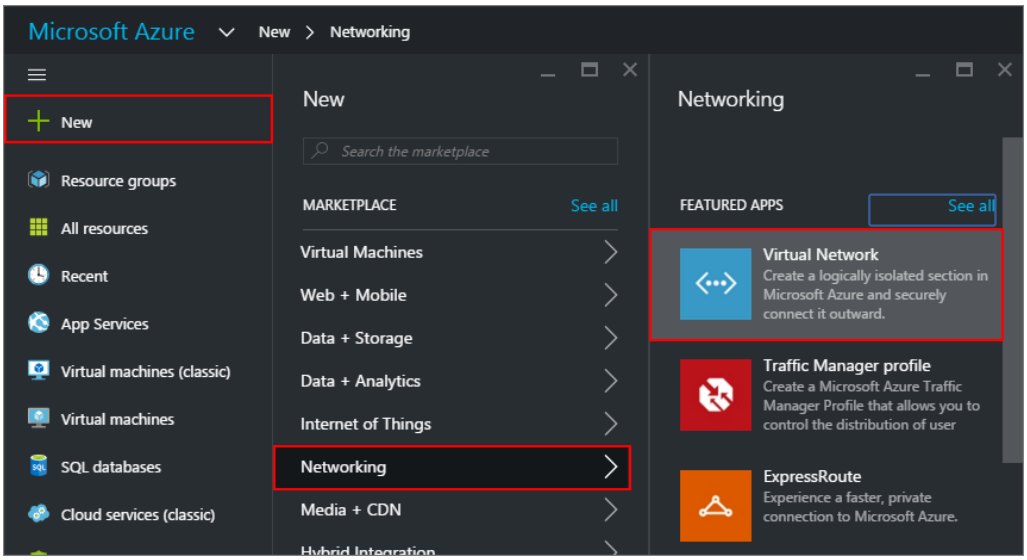
Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



Set Up the IPSec VPN Tunnel on the MS Azure

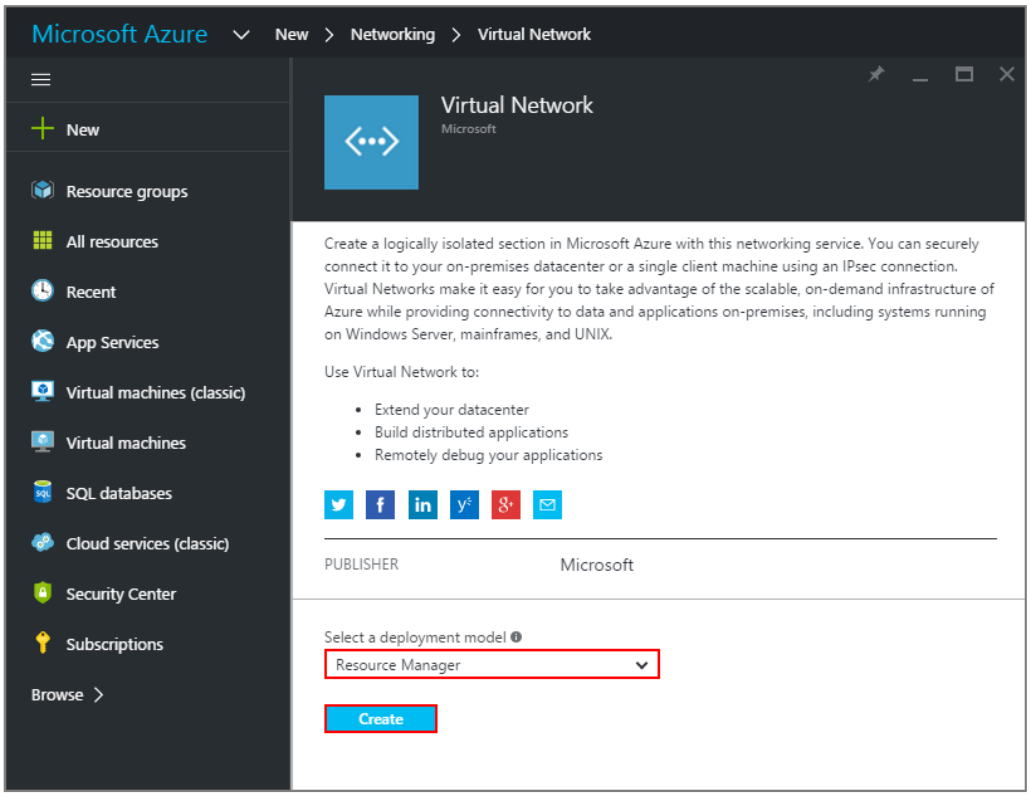
Sign into the **Windows Azure Management Portal.** In the upper left-hand corner of the screen, click **+New > Networking > Virtual Network**.

Azure portal > New > Networking > Virtual Network



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



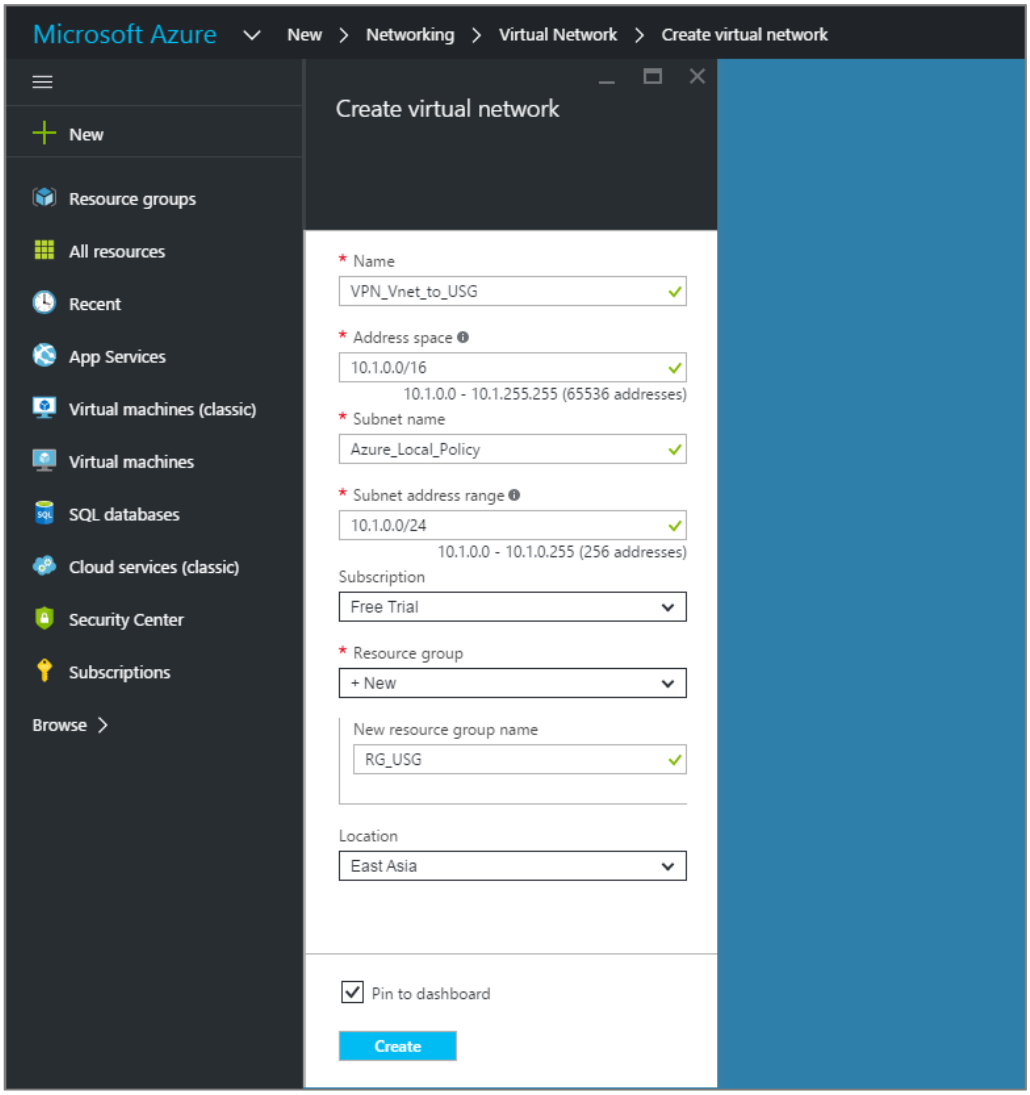
On the **Create virtual network** page, enter the **NAME** for the VPN network. For example, **VPN_Vnet_to_USG**. Add your **Address Space**, **Subnet name** and a single **Subnet address range**.

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.

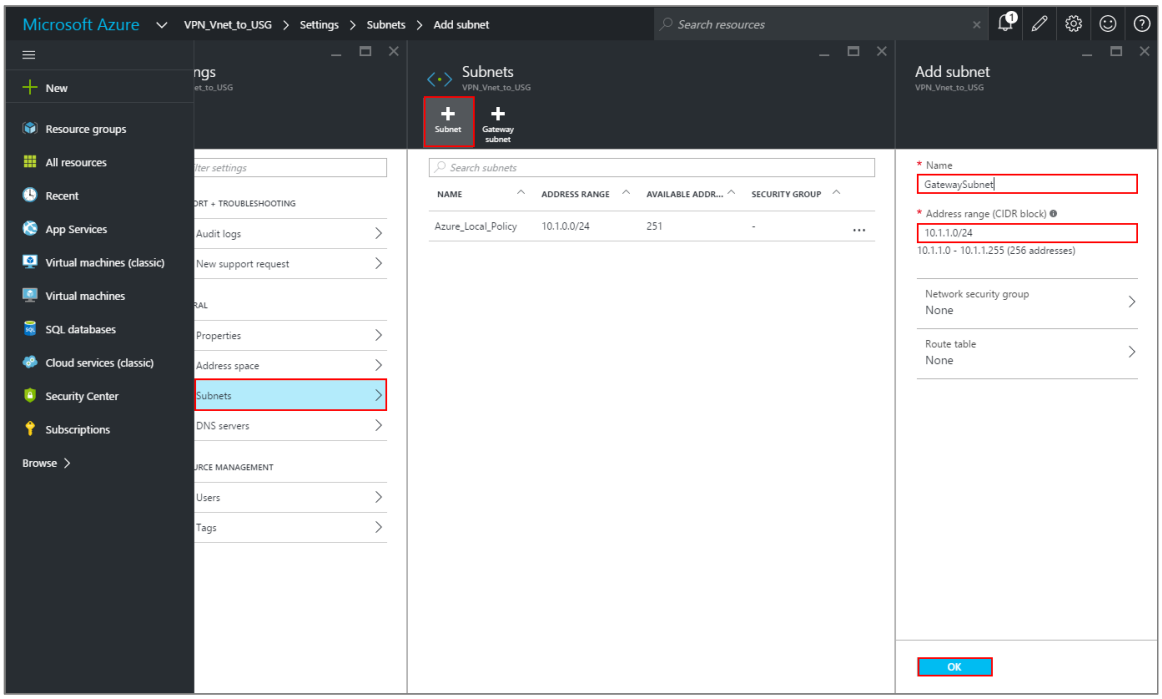
Then, click the **Create** button. After clicking Create, you will see a tile on your dashboard that will reflect the progress of your VNet. The tile will change as the VNet is being created.

New > Networking > Virtual Network > Create virtual network



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

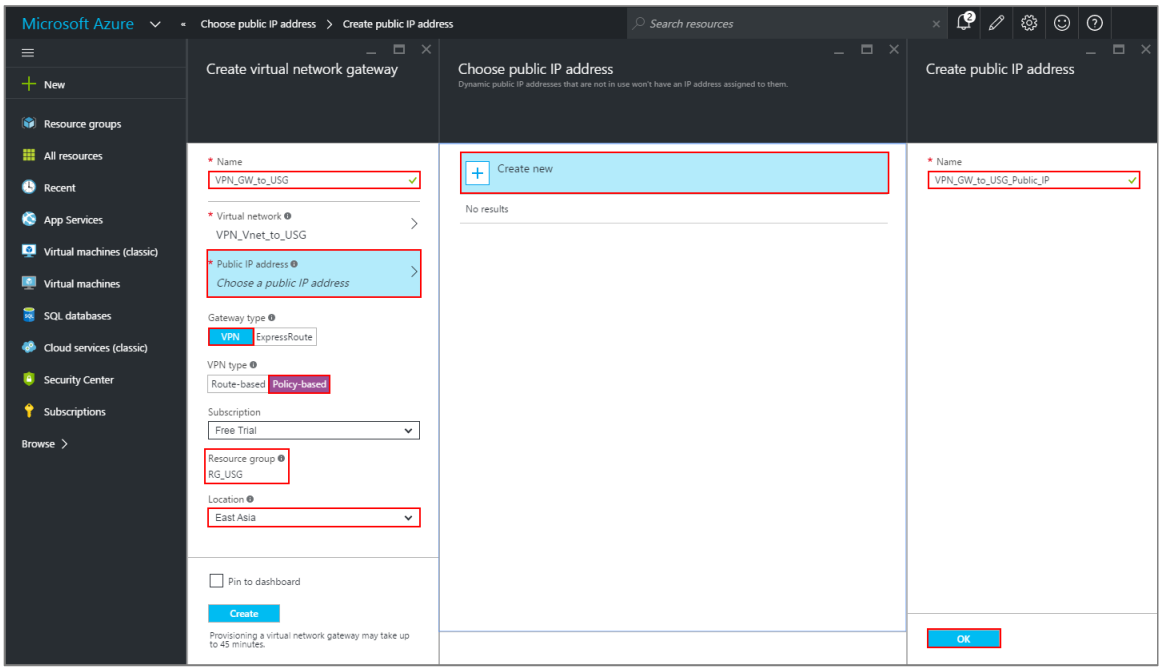


In the portal, go to **New**, then Networking. Select **Virtual network gateway** from the list. On the **Create virtual network gateway** blade **Name** field, name your gateway. Next, choose the **Virtual network** that you want to deploy this gateway to.

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



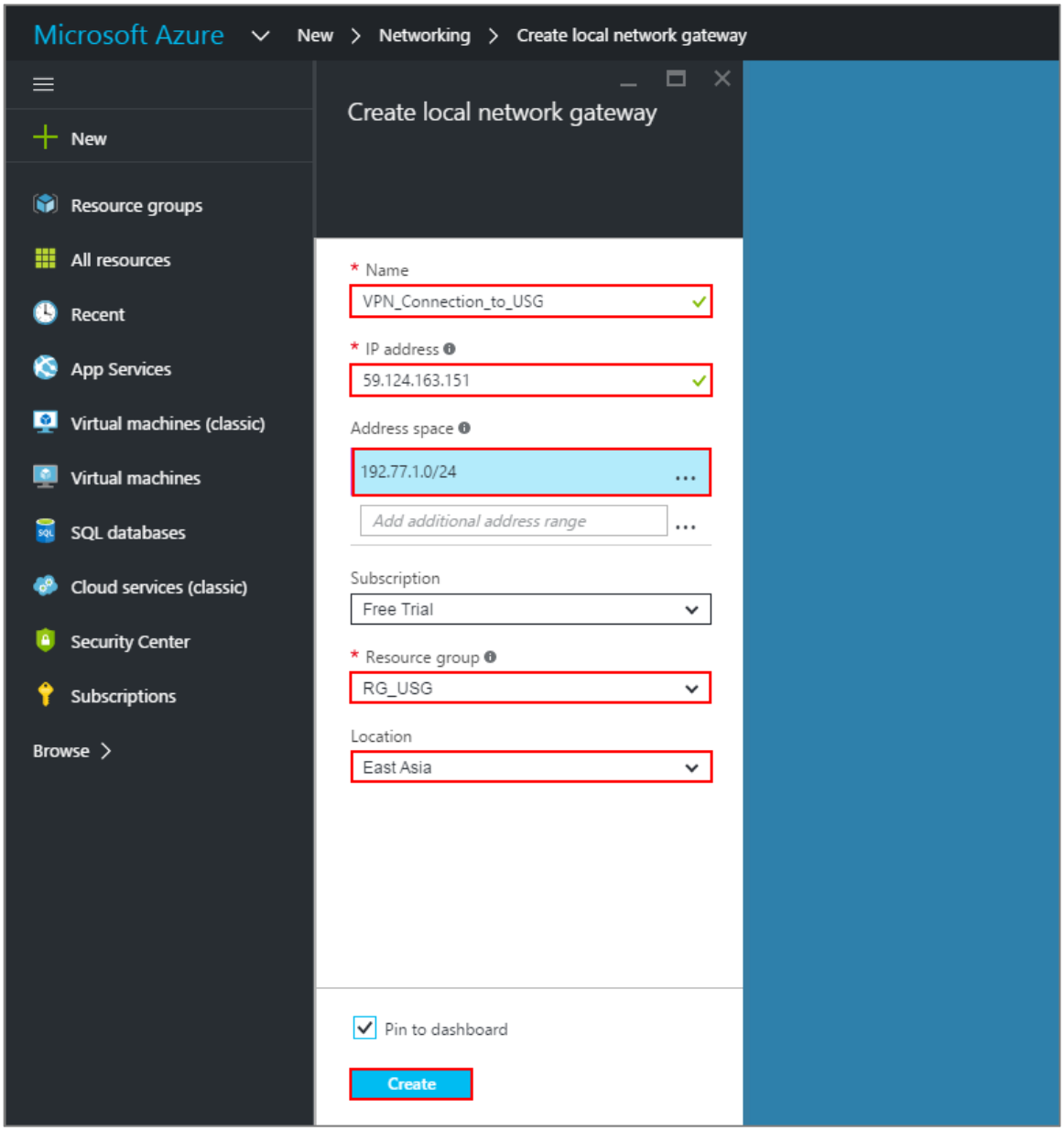
In the Azure Portal, navigate to **New > Networking > Local network gateway**. The local network gateway refers to your ZyWALL/USG public IP and local subnet settings.

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

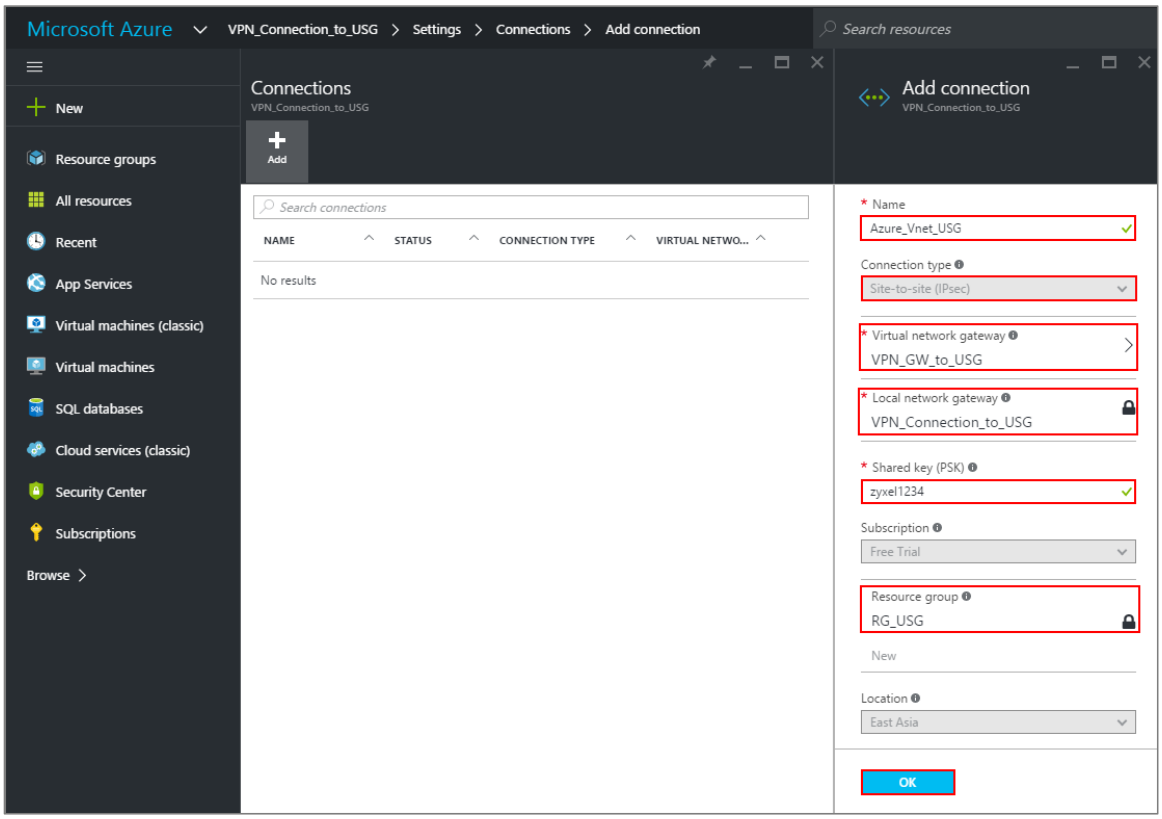


Locate your virtual network gateway (VPN_Connection_to_USG in this example) and click **Settings > Connection > Add connection**, **Name** your connection. For **Connection type**, select **Site-to-site (IPSec)**. For **Virtual network gateway**, the value is fixed because you are connecting from this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

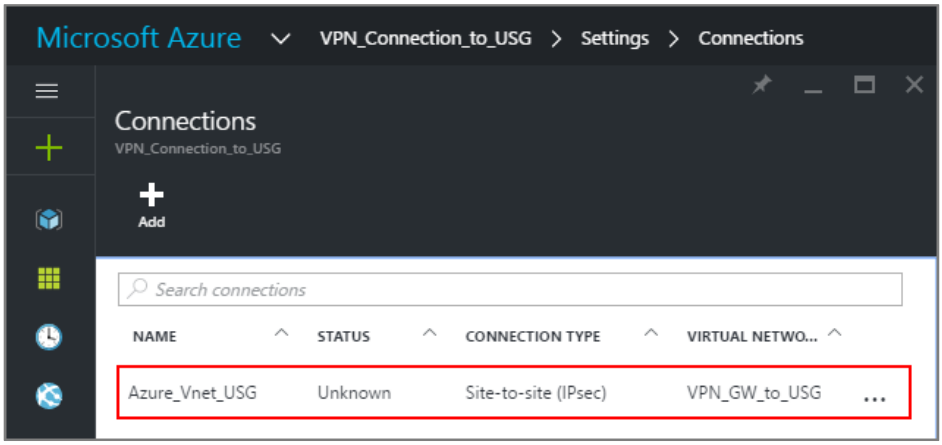
For **Shared Key (PSK)**, the value here must match the value that you are using for your ZyWALL/USG device. For **Resource Group**, select the resource group that you **created before**. Click **OK** to create your connection.

VPN_Connection_to_USG > Settings > Connections > Add connection



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

VPN_Connection_to_USG > Settings > Connections



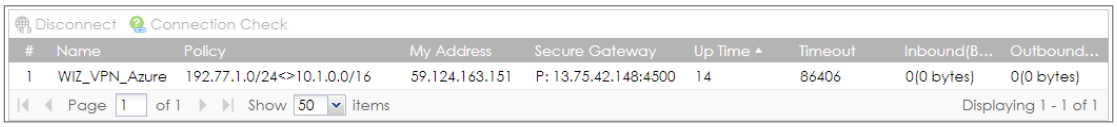
Test the IPSec VPN Tunnel

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

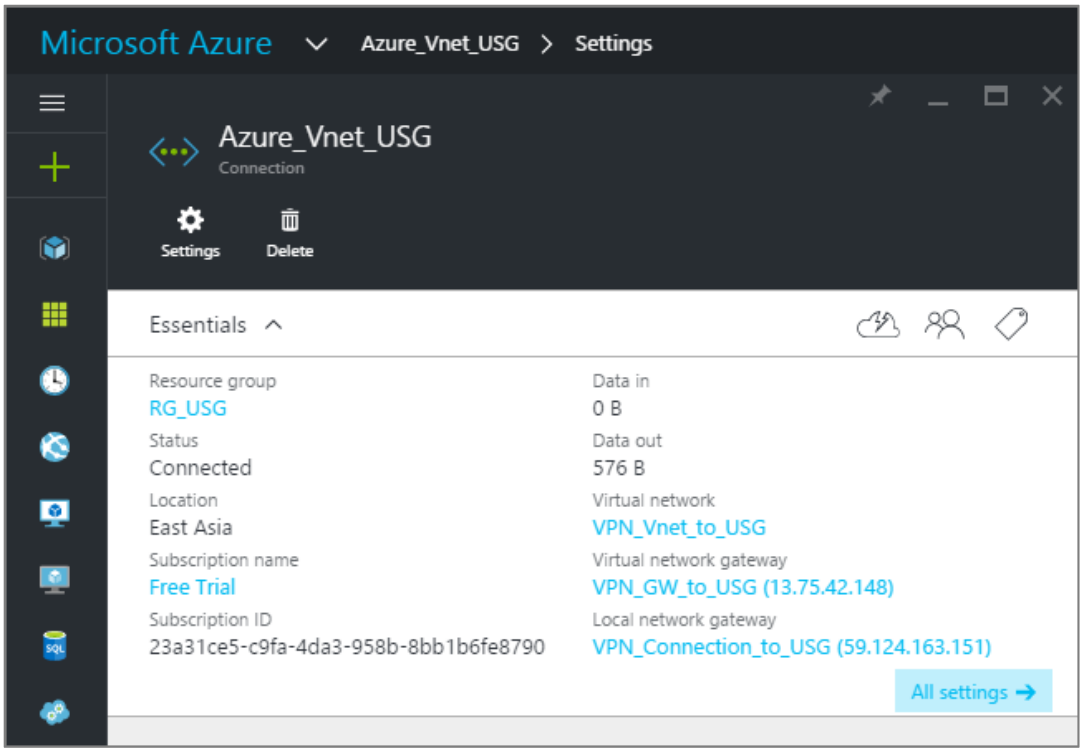
Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec



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

VPN > VPN Settings > Currently Active VPN Tunnels



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.

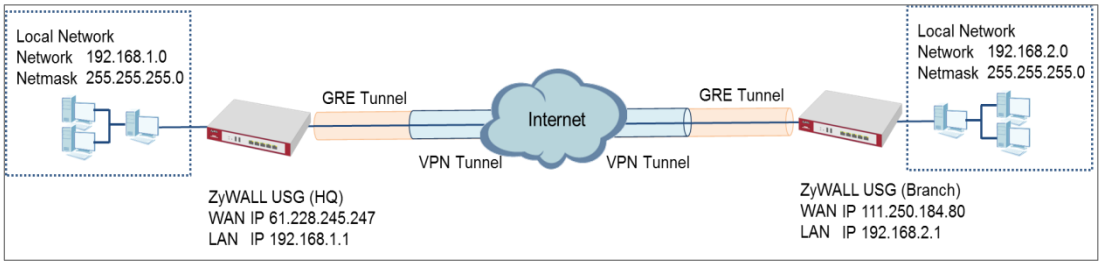
MONITOR > Log

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.



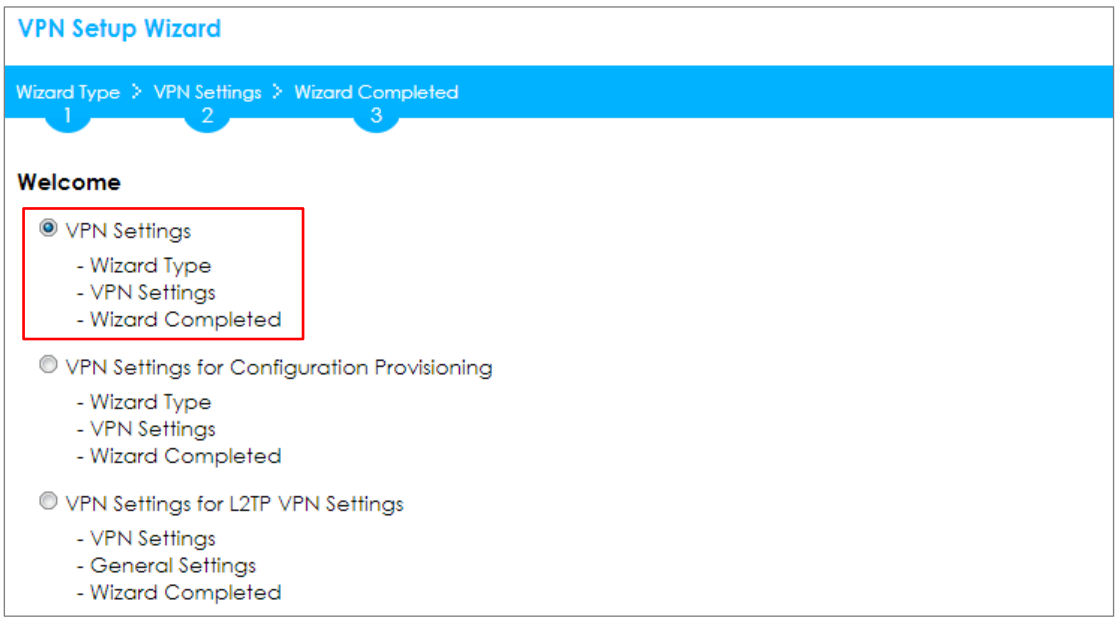
ZyWALL/USG GRE over IPSec VPN

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)

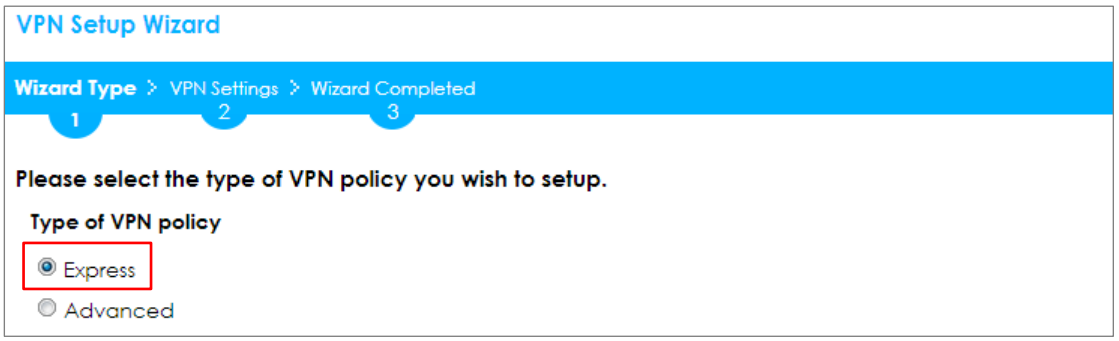
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

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



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**



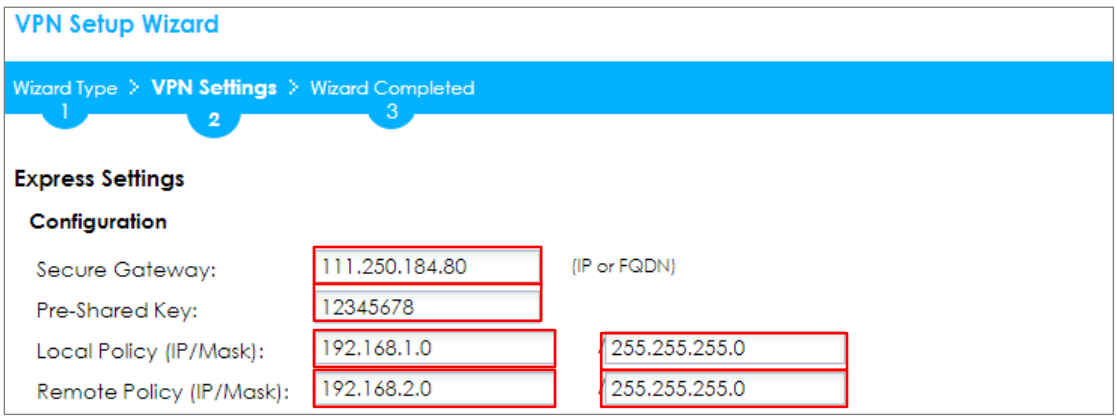
Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

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

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).

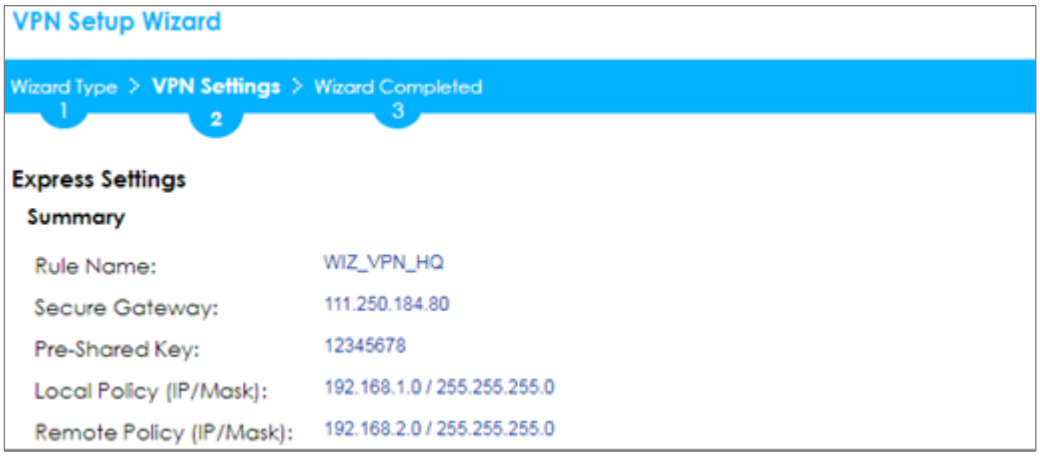
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG (HQ) and **Remote Policy** to be the IP address range of the network connected to the ZyWALL/USG (Branch).

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



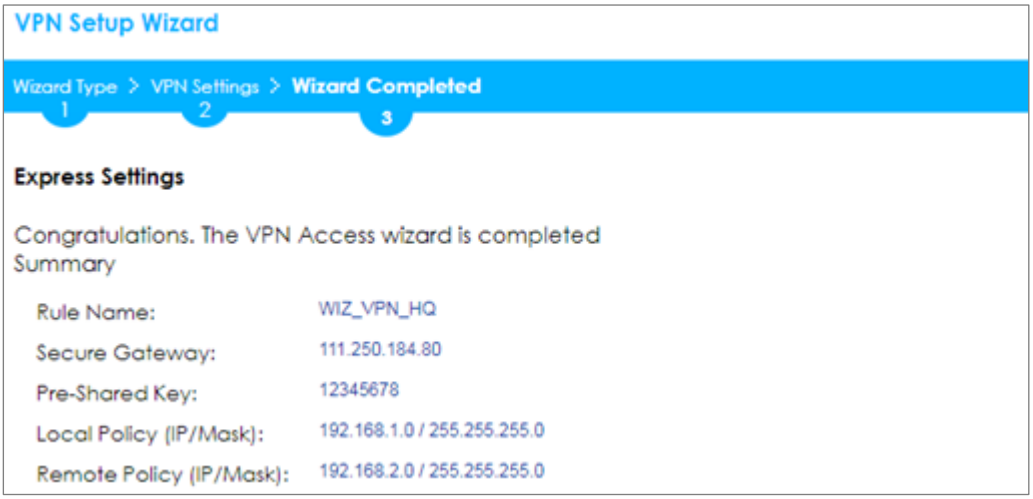
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



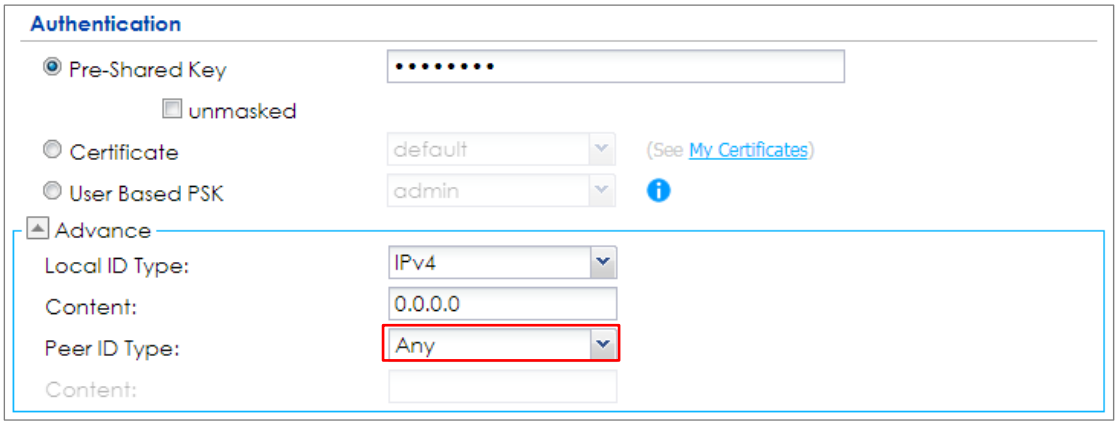
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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



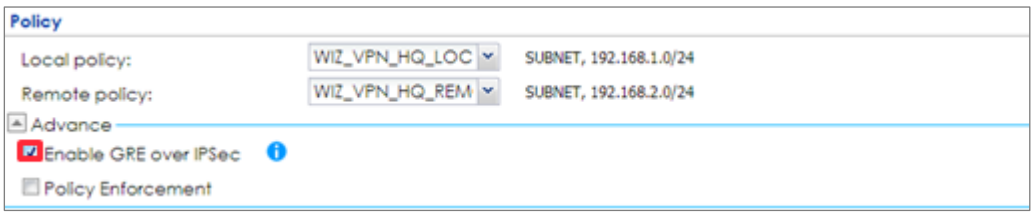
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

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



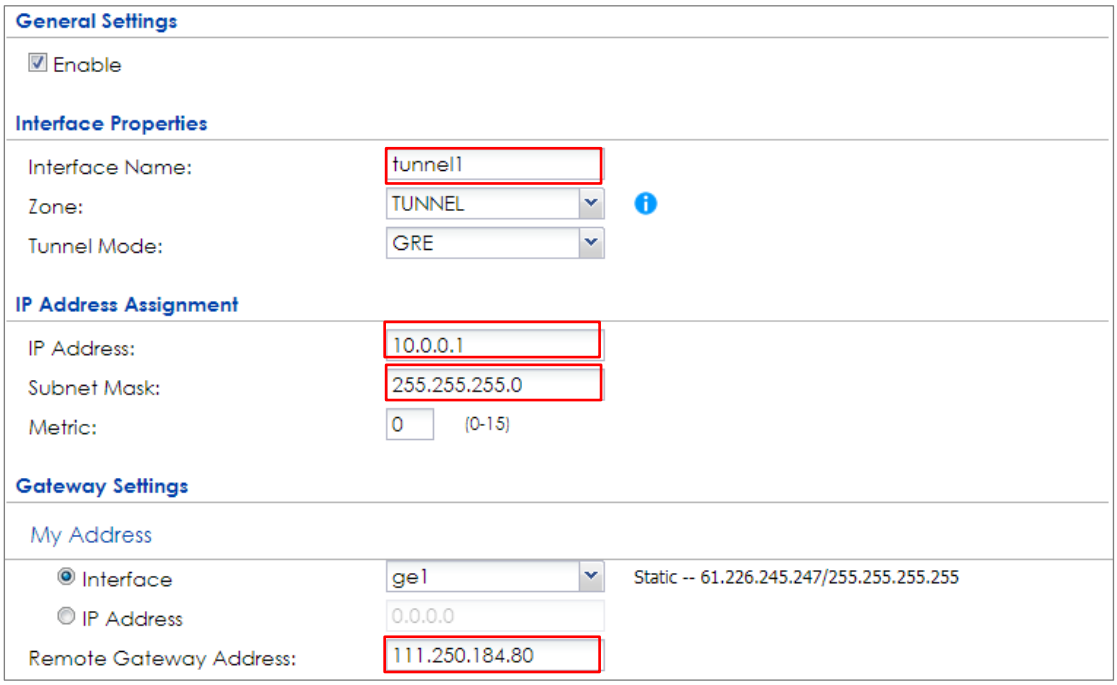
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** > **Show Advanced Settings > Policy**. Select **Enable GRE over IPSec**.

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



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.

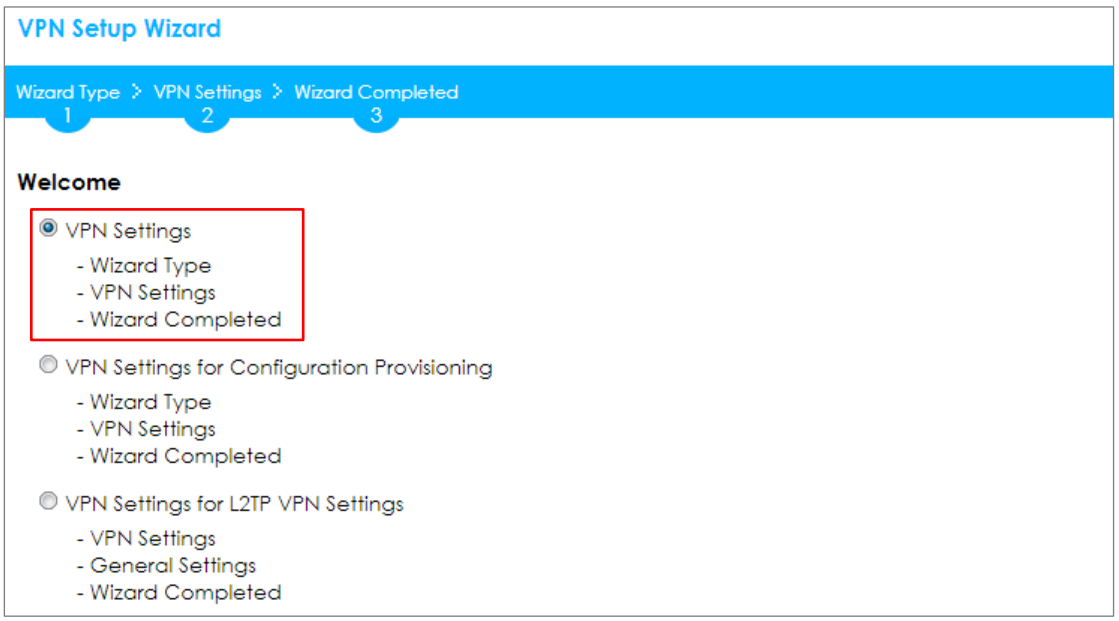
CONFIGURATION > Network > Interface > Tunnel > Add



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

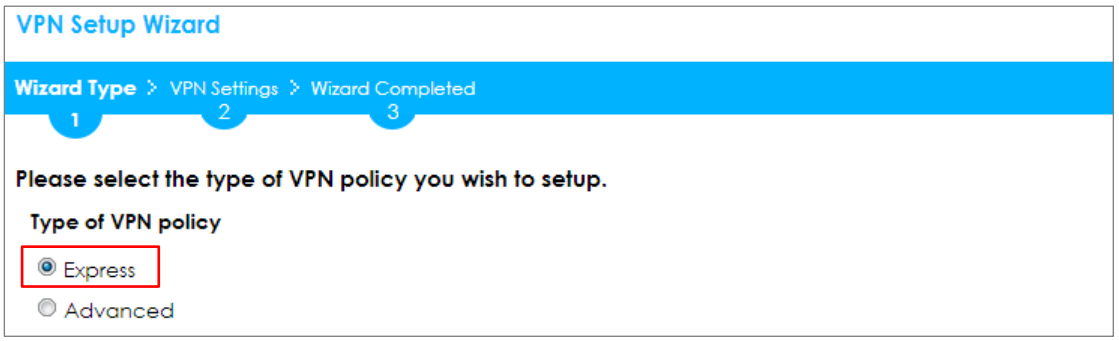
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



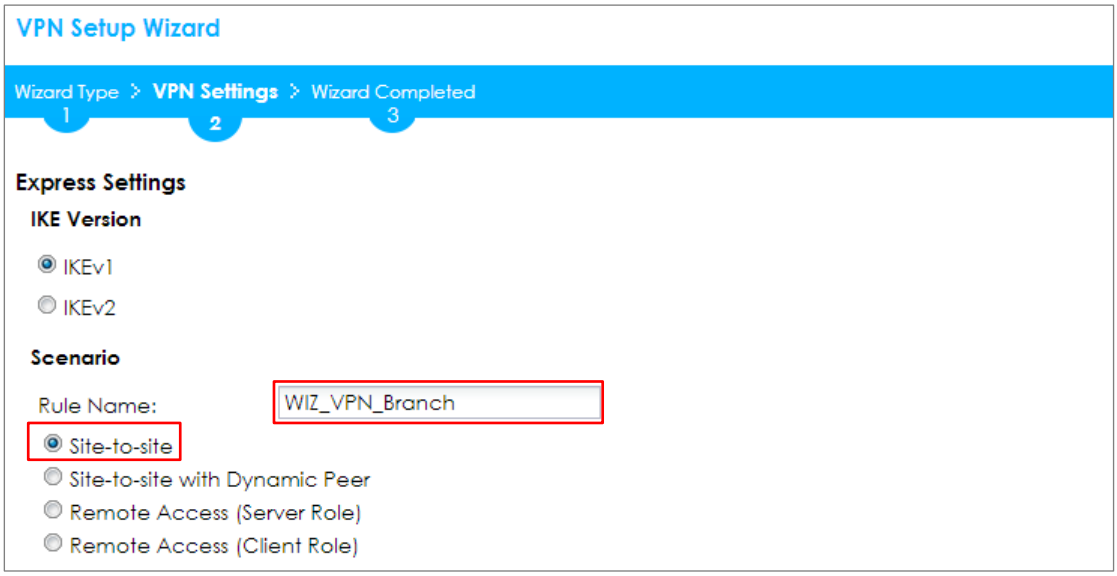
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

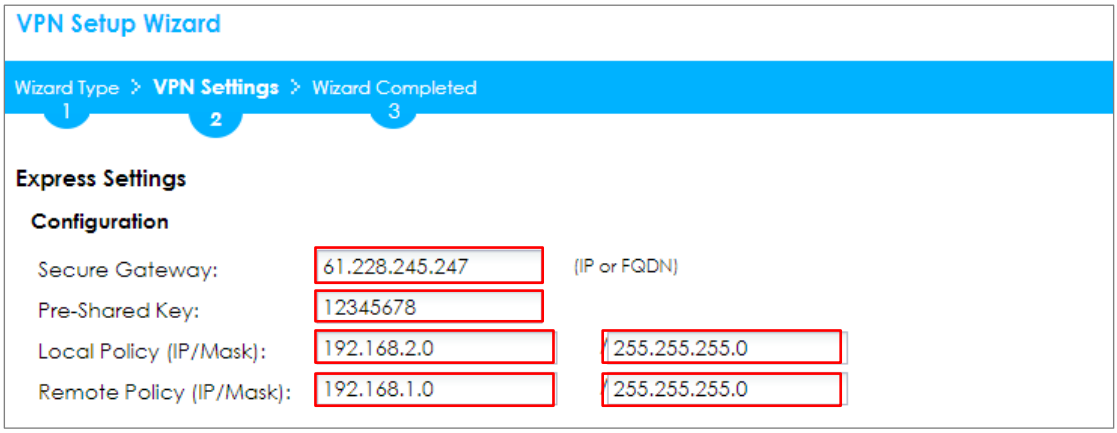
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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)

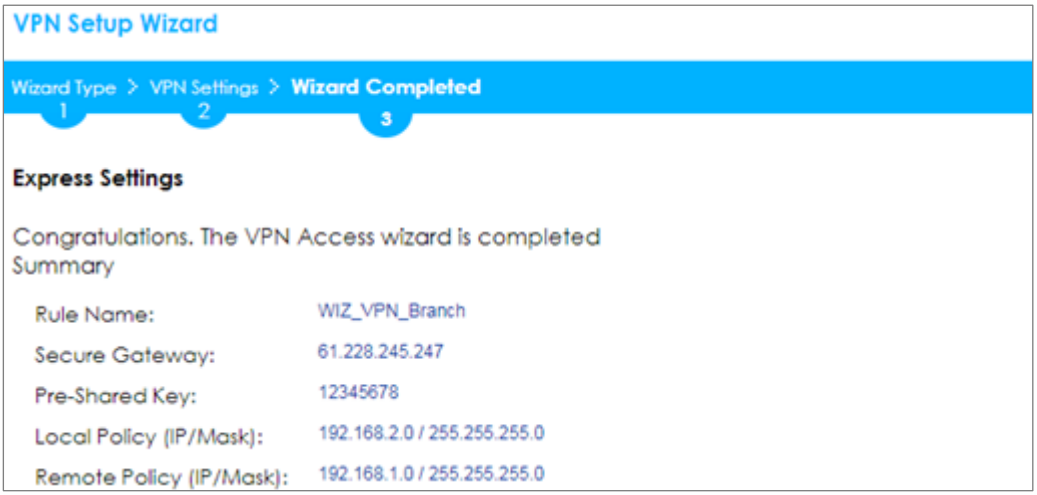


This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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

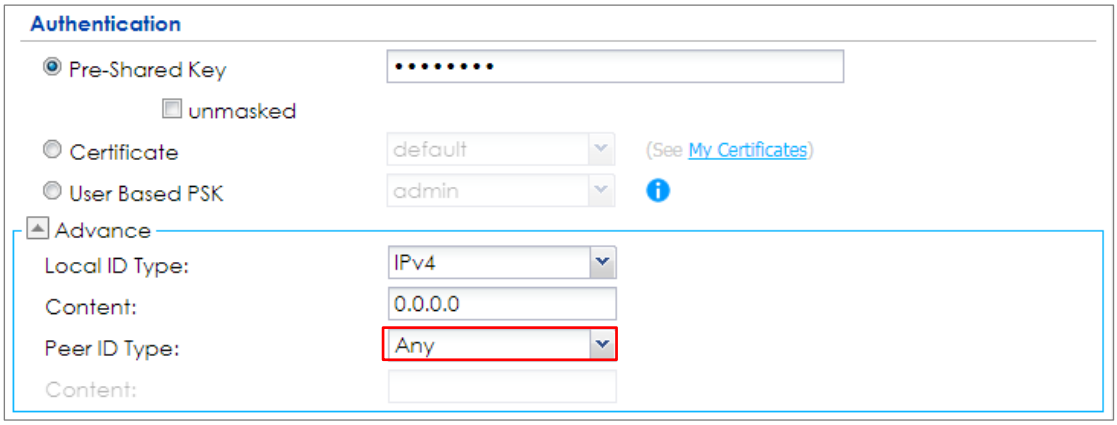
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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



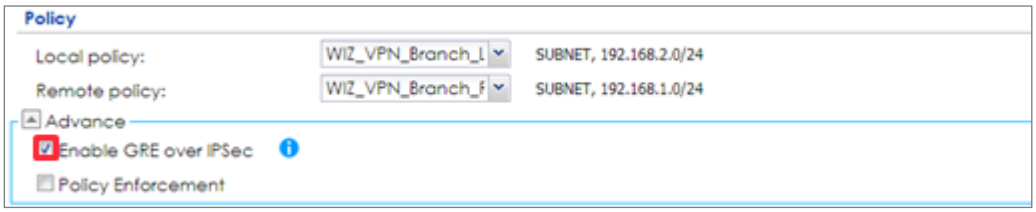
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

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



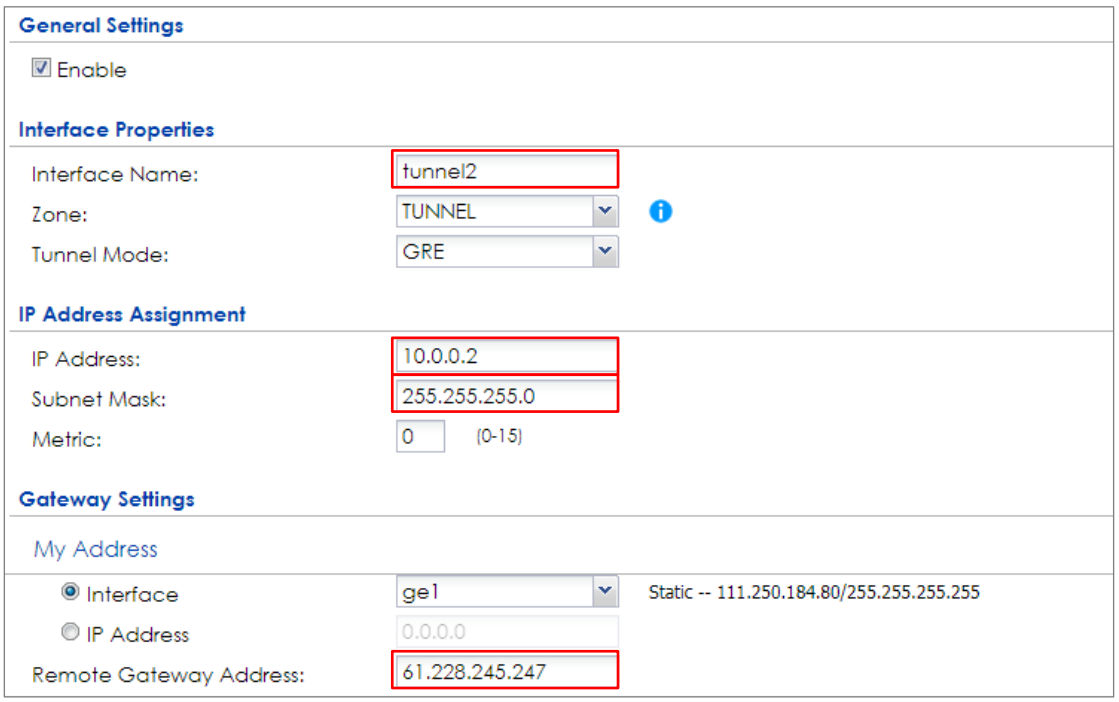
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** > **Show Advanced Settings > Policy**. Select **Enable GRE over IPSec**.

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



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



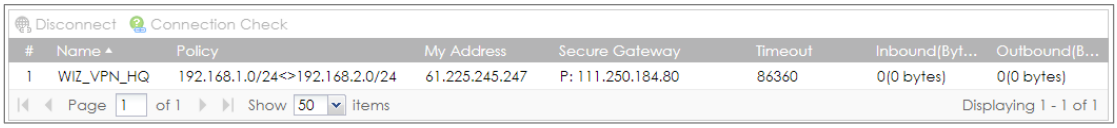
Test the GRE over IPSec VPN Tunnel

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

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

#	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)

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

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.

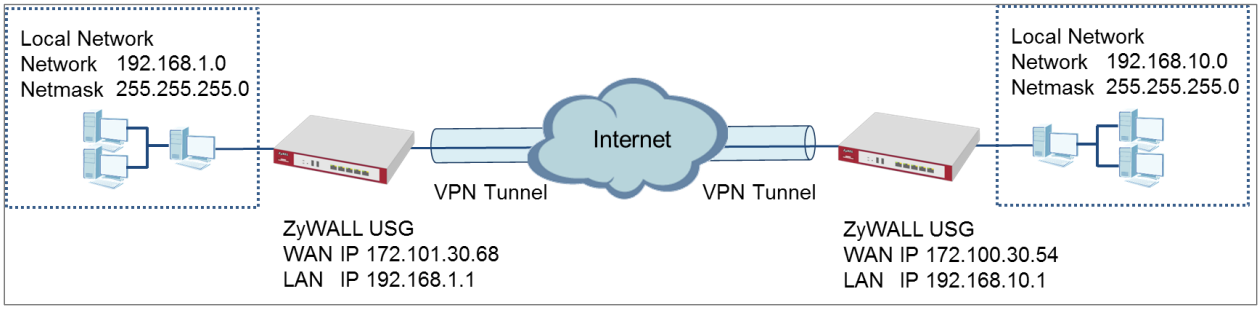
MONITOR > Log

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.

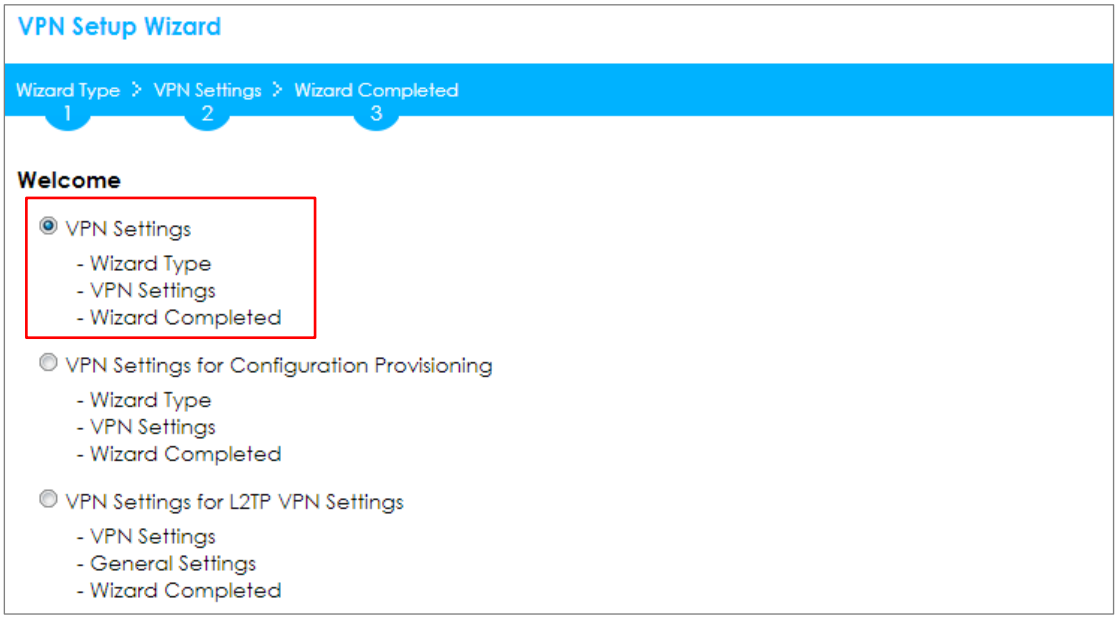


ZyWALL Site-to-site IPSec VPN with a Static IP Address Peer

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).

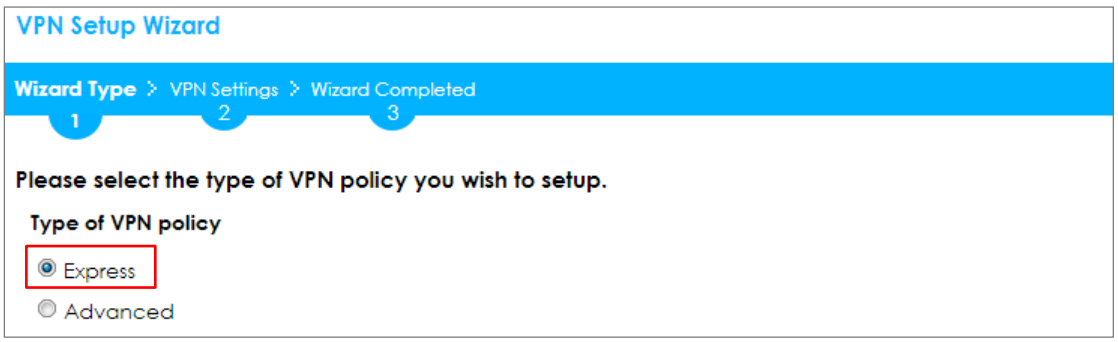
Set Up the ZyWALL/USG IPSec VPN Tunnel of Corporate Network (HQ)In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



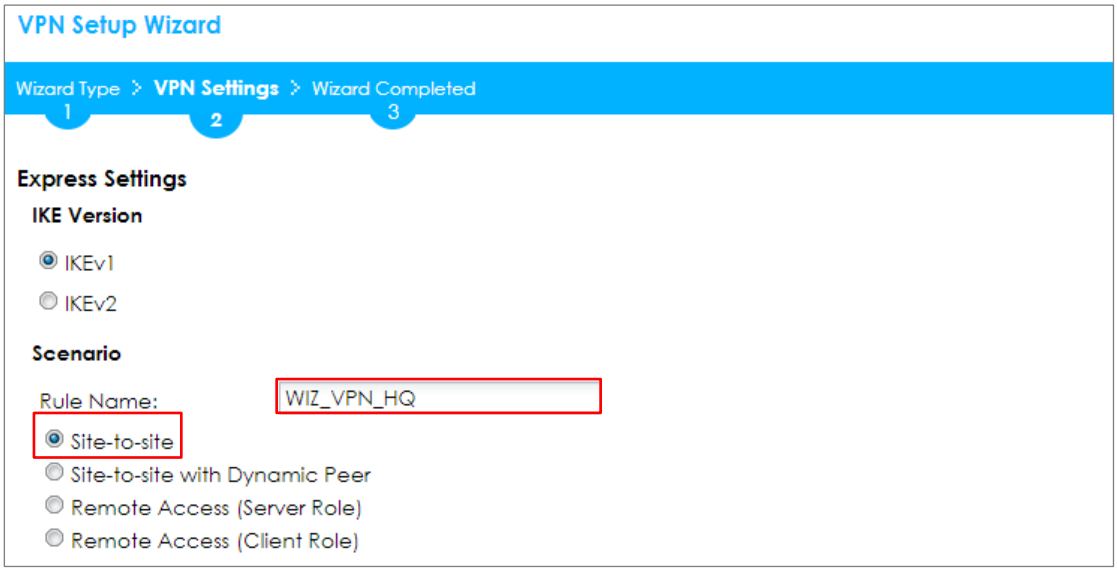
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

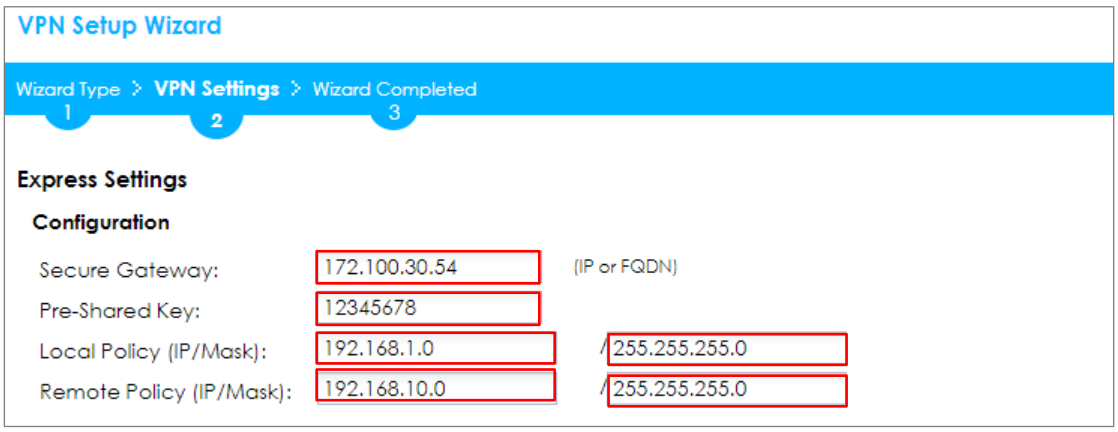
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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).

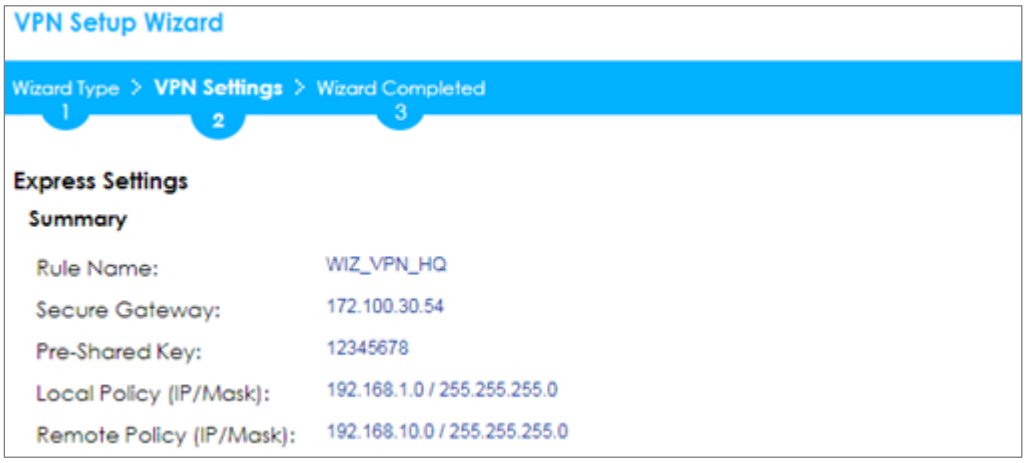
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZyWALL/USG.

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



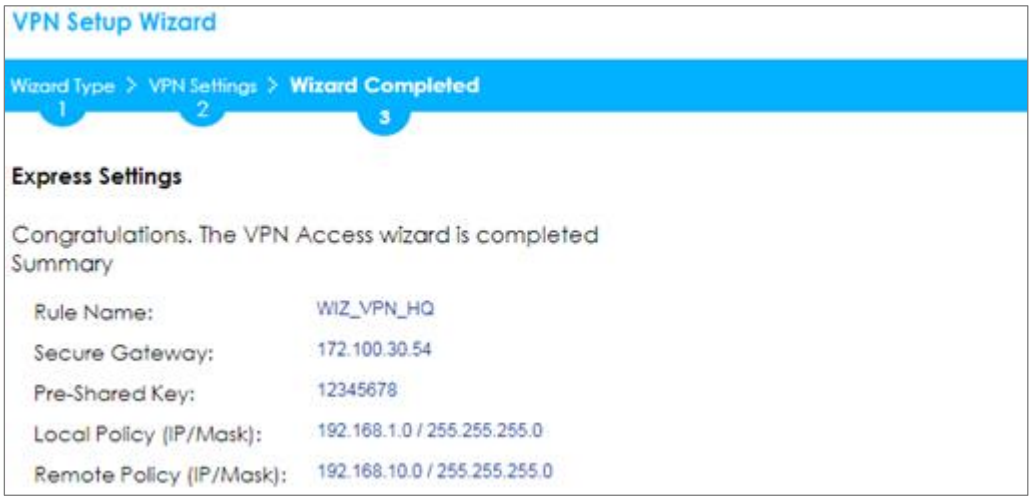
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



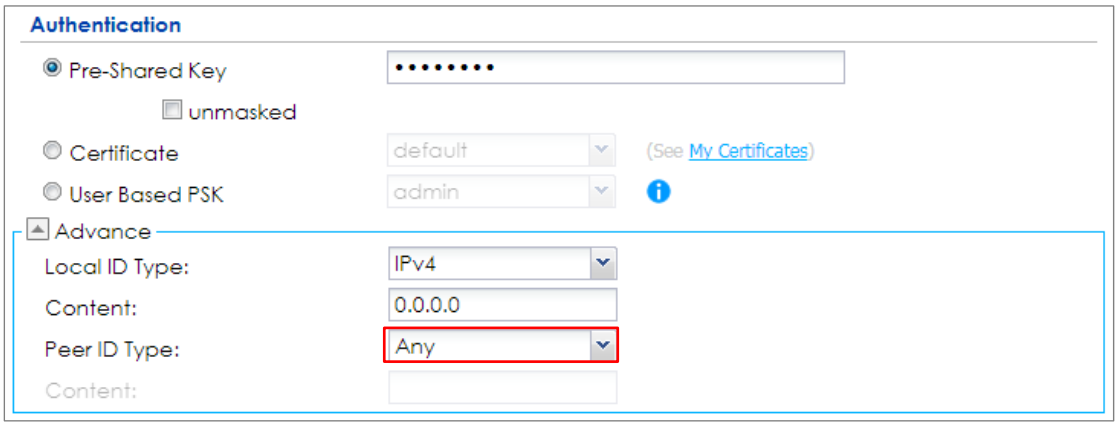
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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



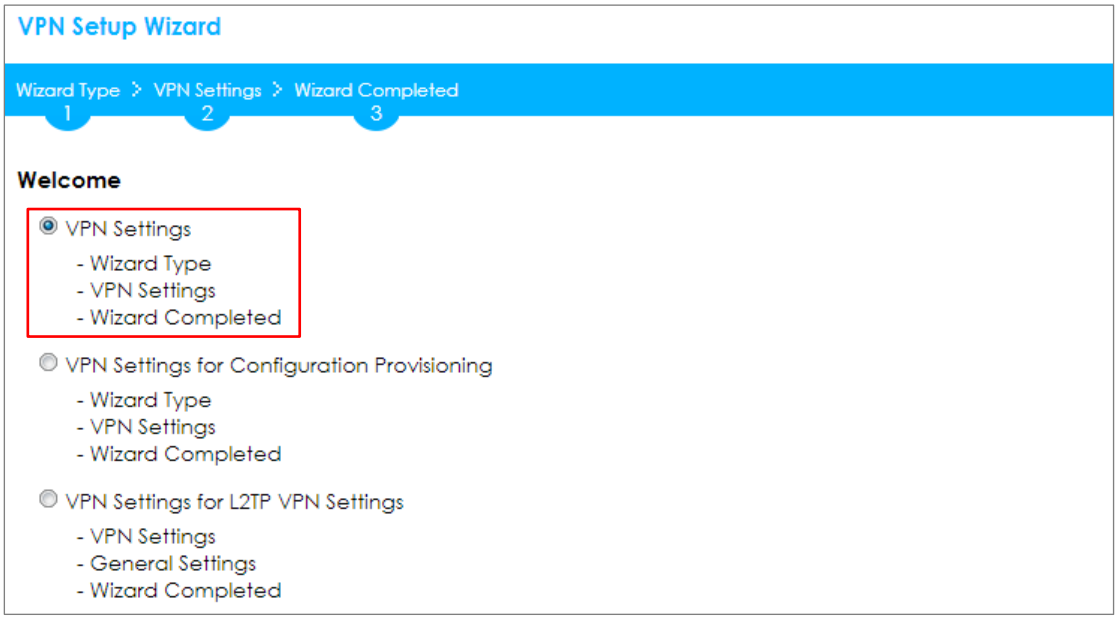
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

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



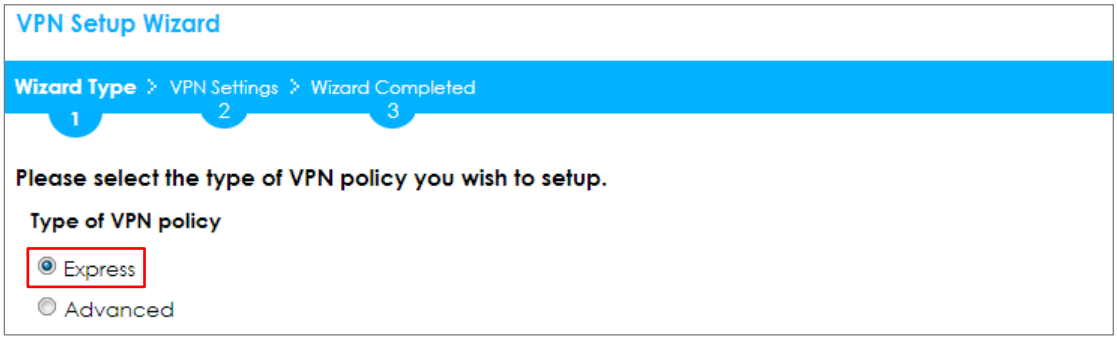
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



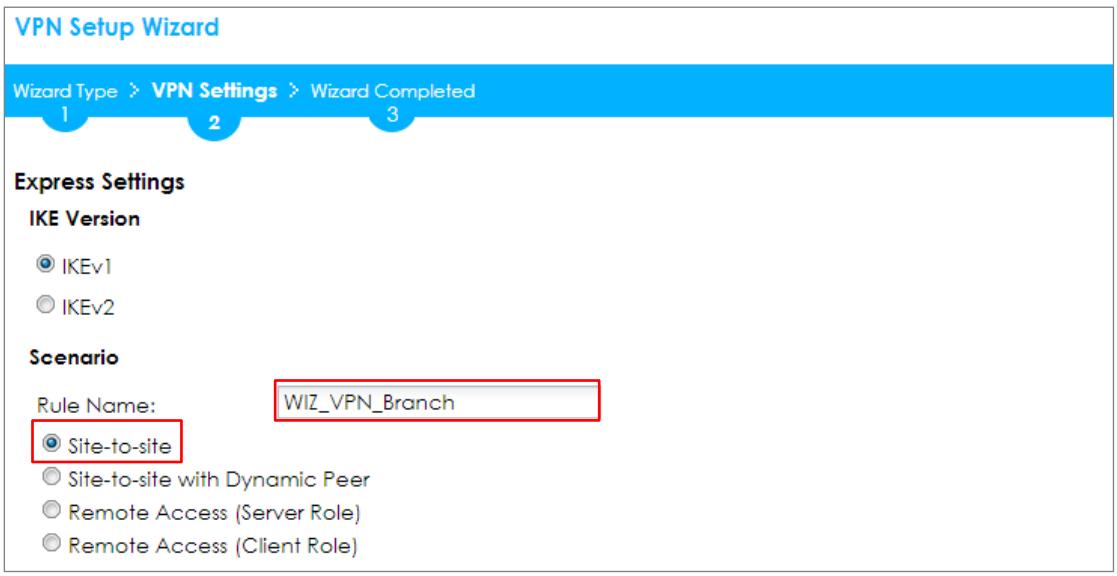
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

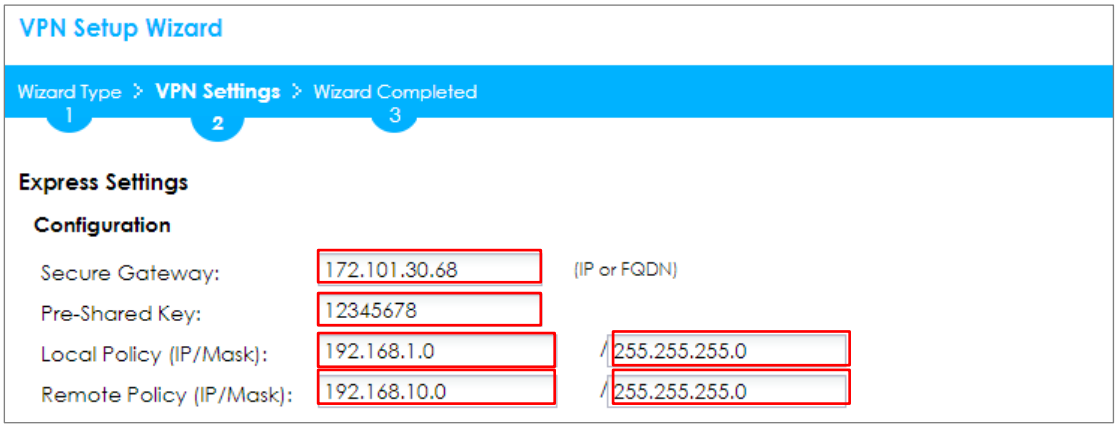
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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).

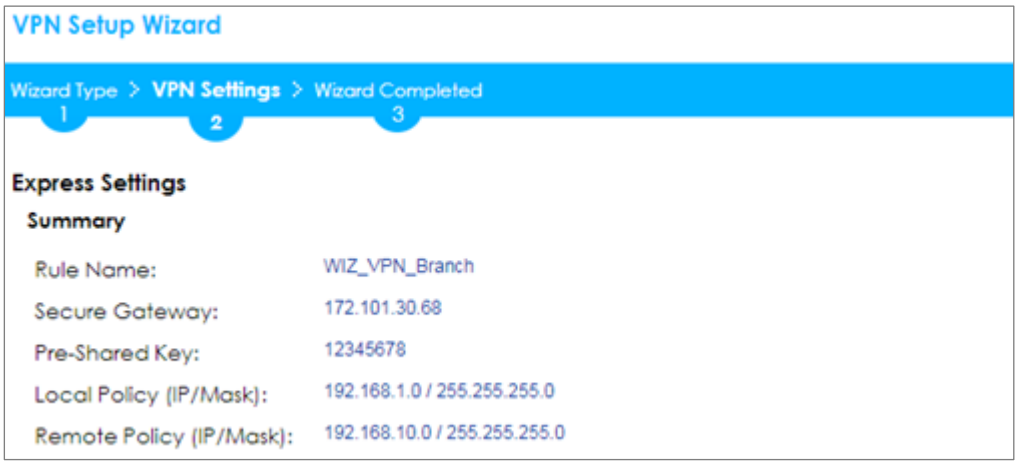
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZYWALL/USG.

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



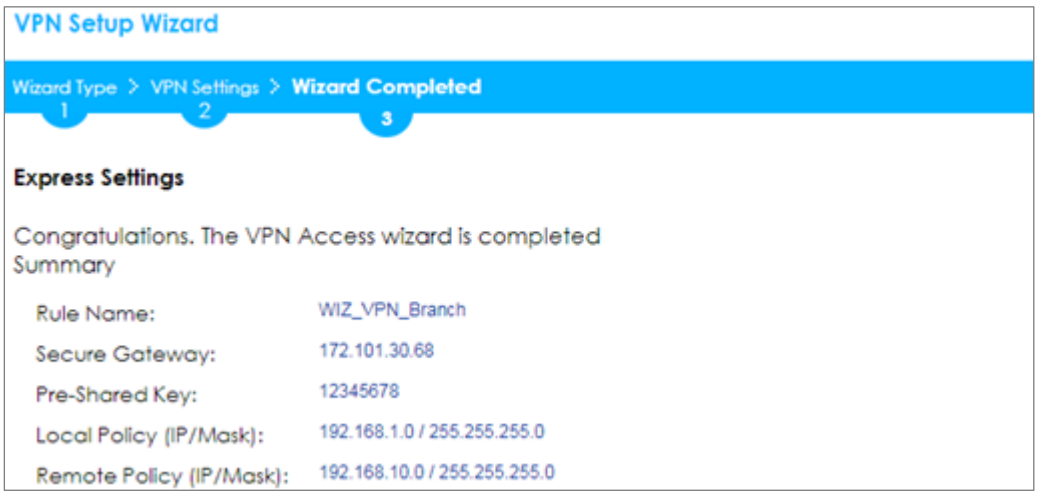
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



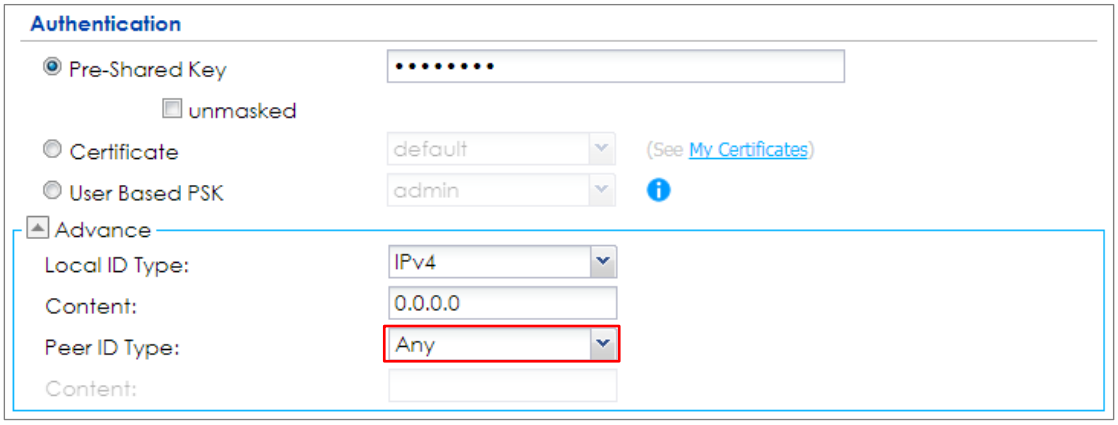
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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



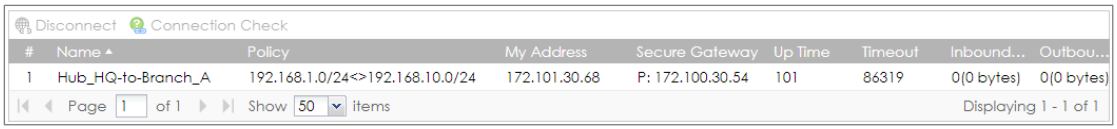
Test the IPSec VPN Tunnel

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

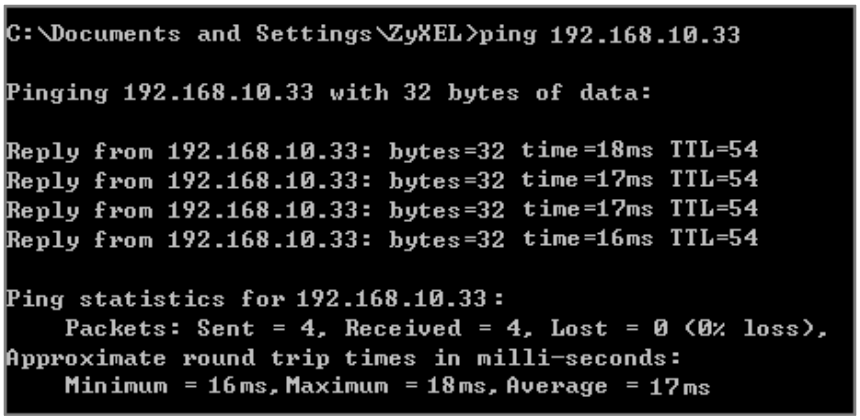
Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** Traffic.

MONITOR > VPN Monitor > IPSec



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



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

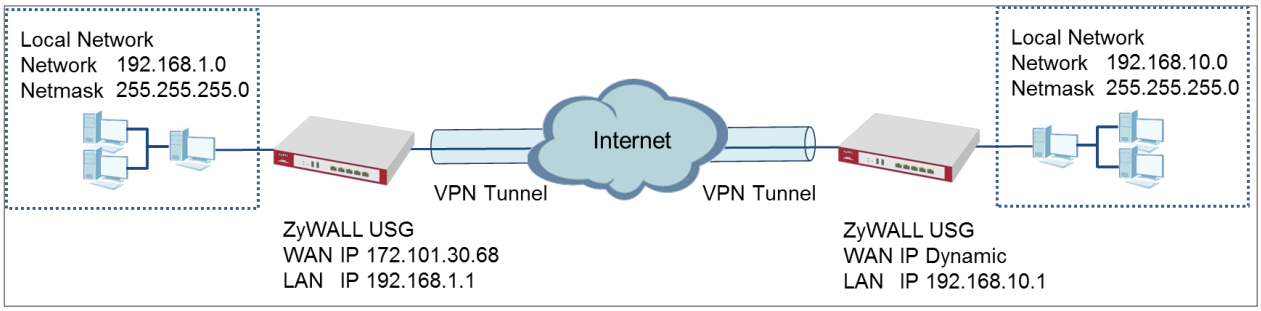
31	2017-09-11 ...	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

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.



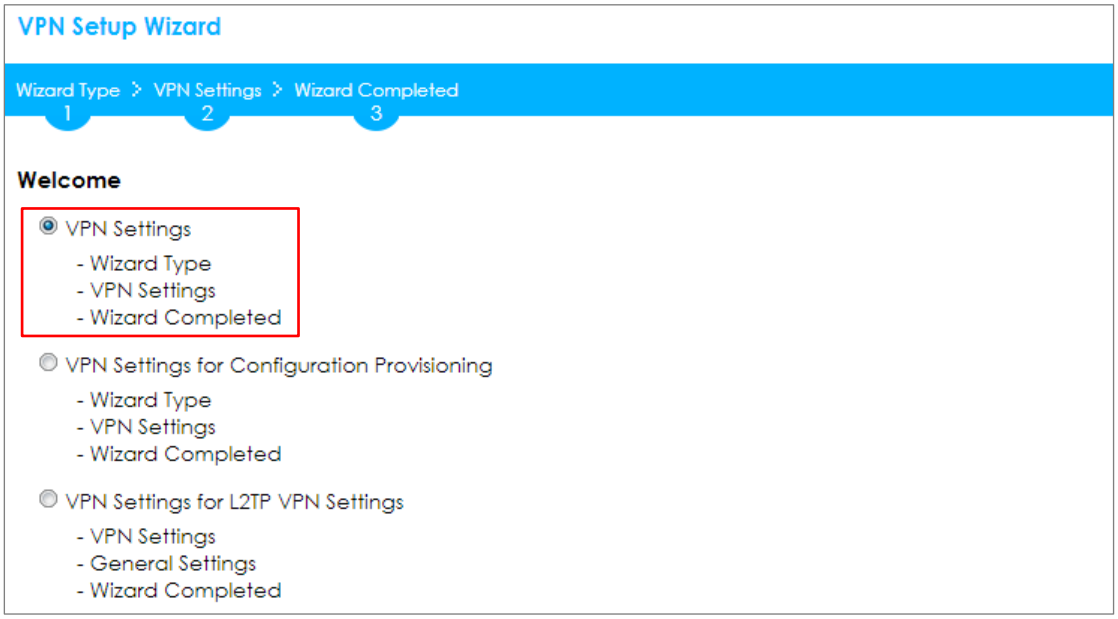
ZyWALL Site-to-site IPSec VPN with a Dynamic IP Address Peer

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)

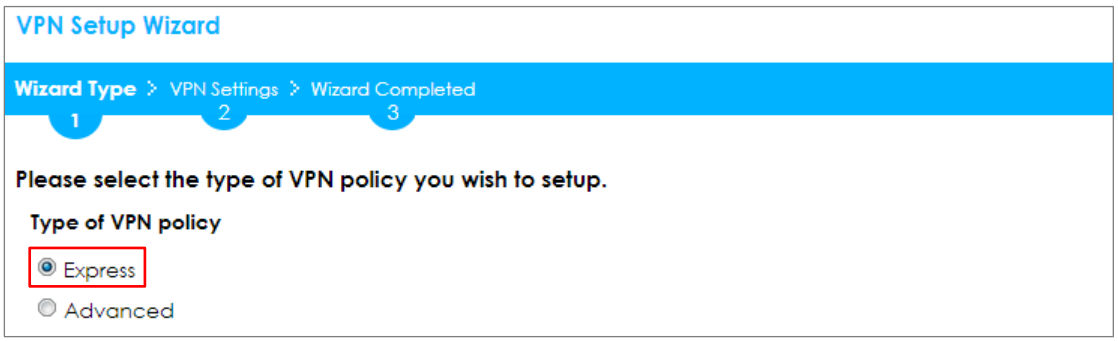
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



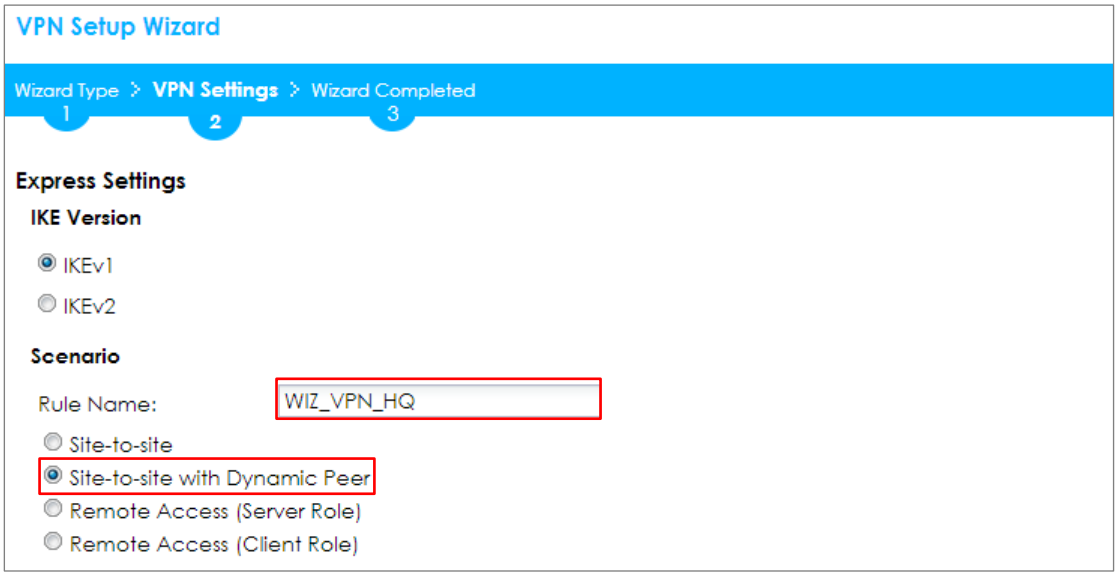
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



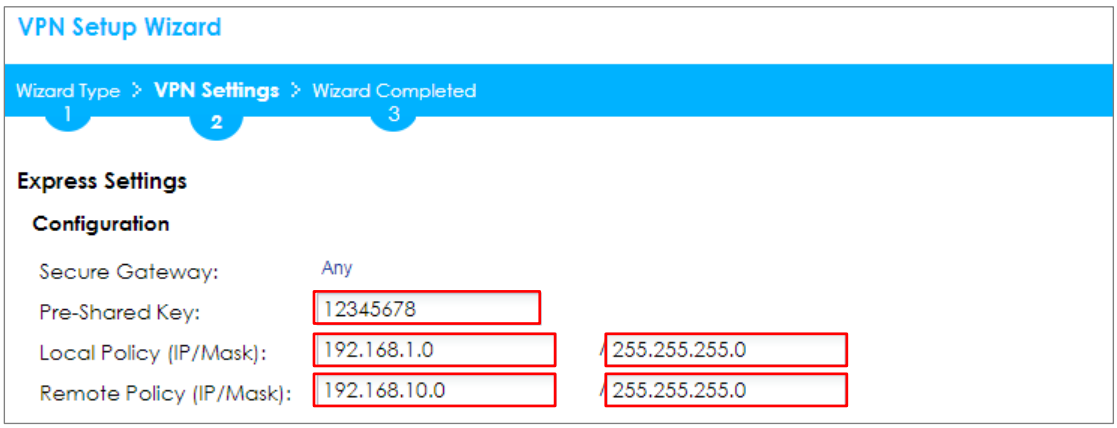
Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site with Dynamic Peer**. Click **Next**.

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



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)

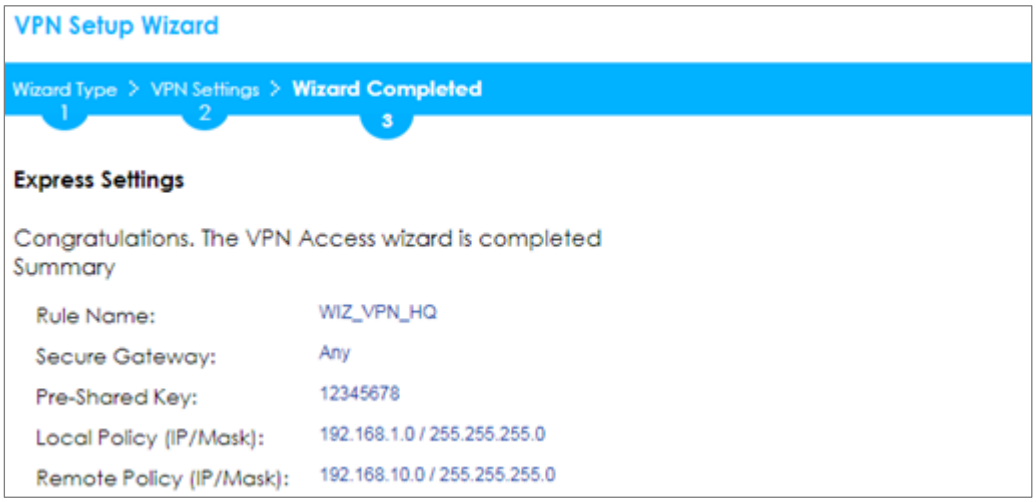


This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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

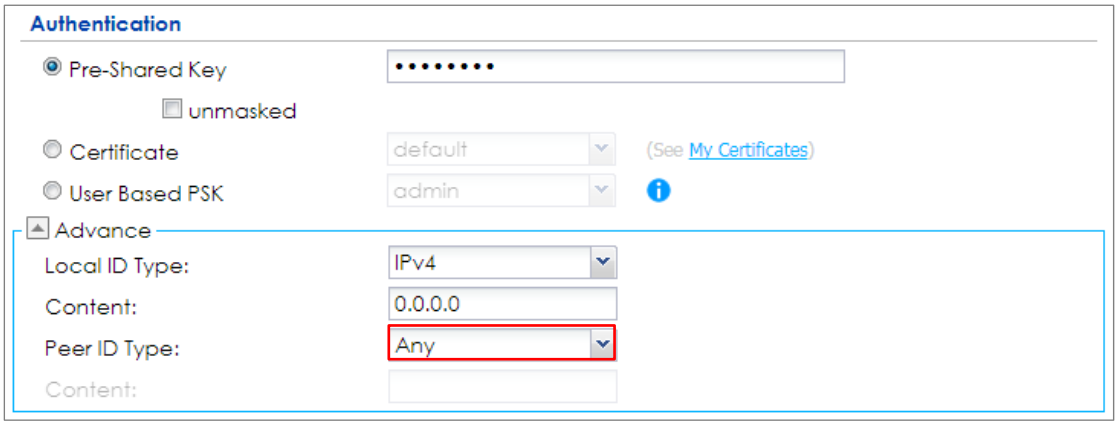
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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



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.

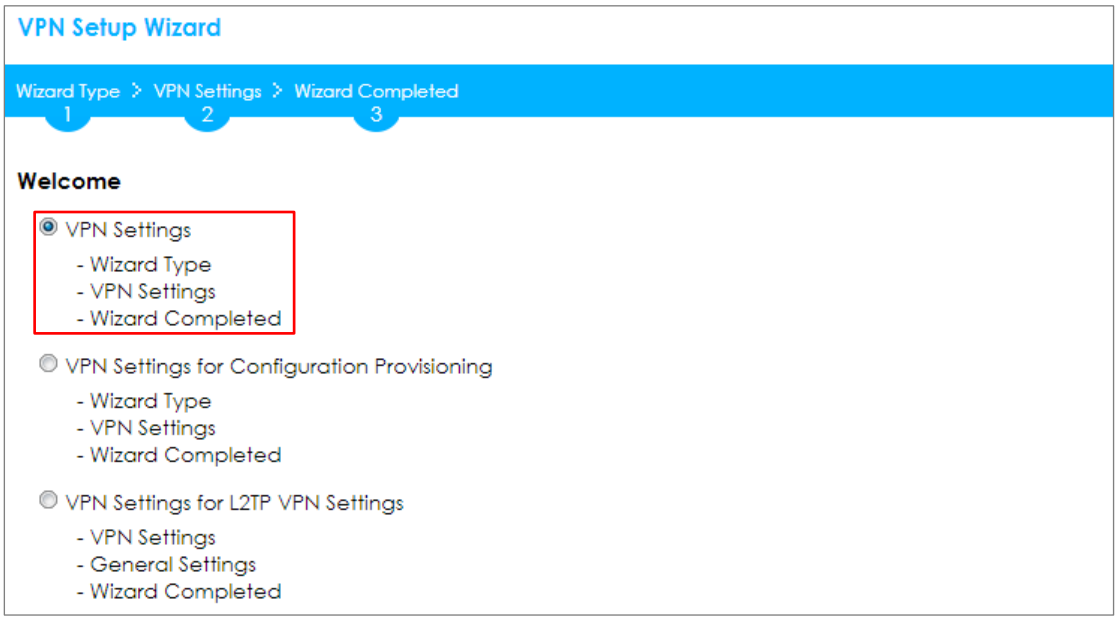
CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



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

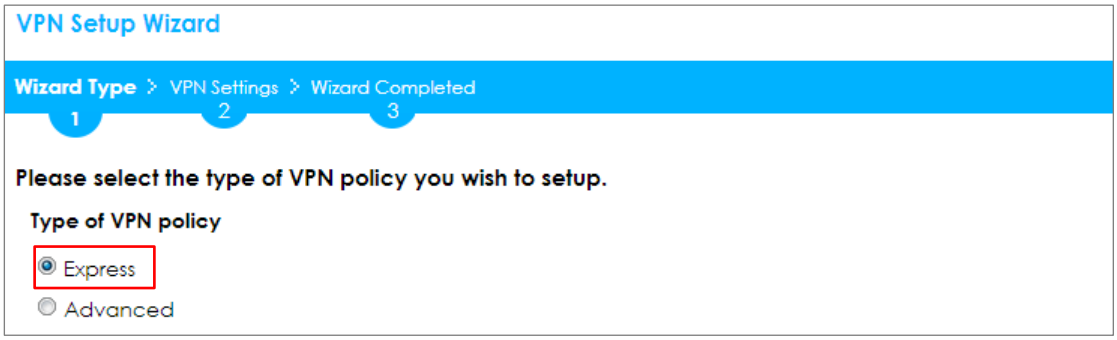
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** to create a **Site-to-site VPN** Rule Name.

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



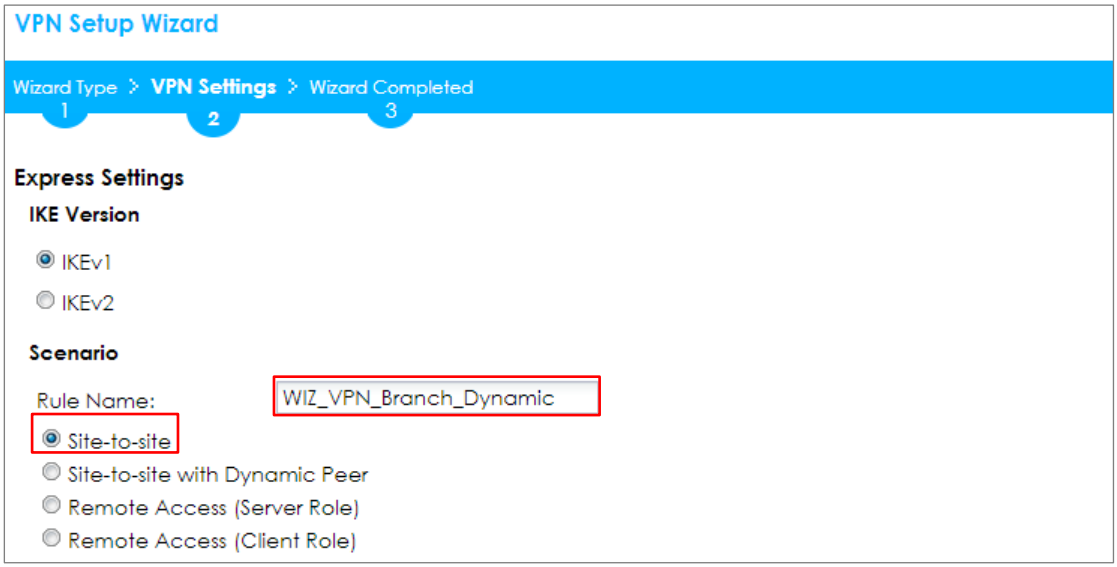
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

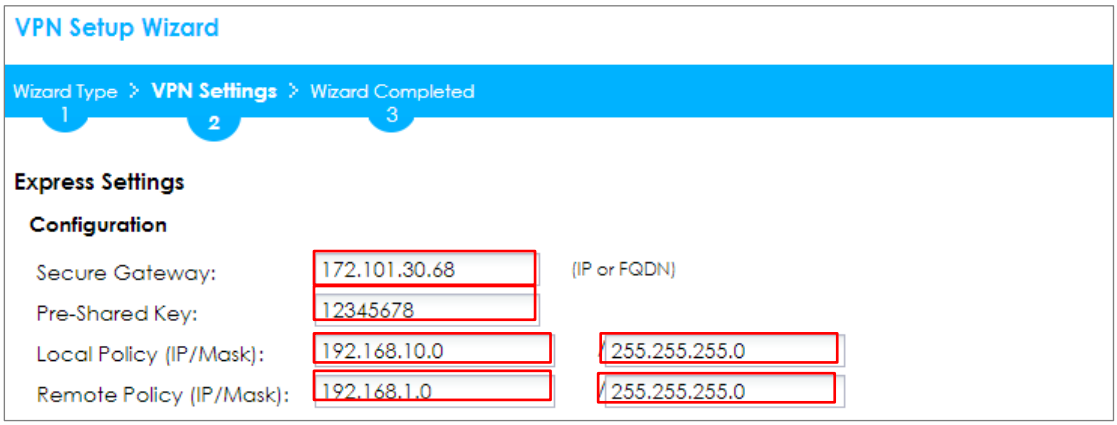
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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).

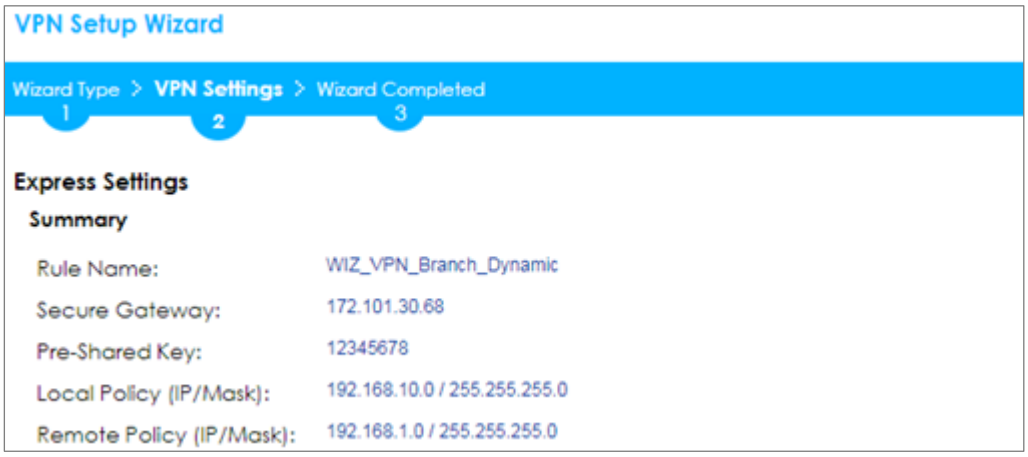
Set **Local Policy** to be the ZyWALL/USG local IP address that can use the VPN tunnel and set **Remote Policy** to the peer ZyWALL/USG local IP address that can use the VPN tunnel. Click **OK**.

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



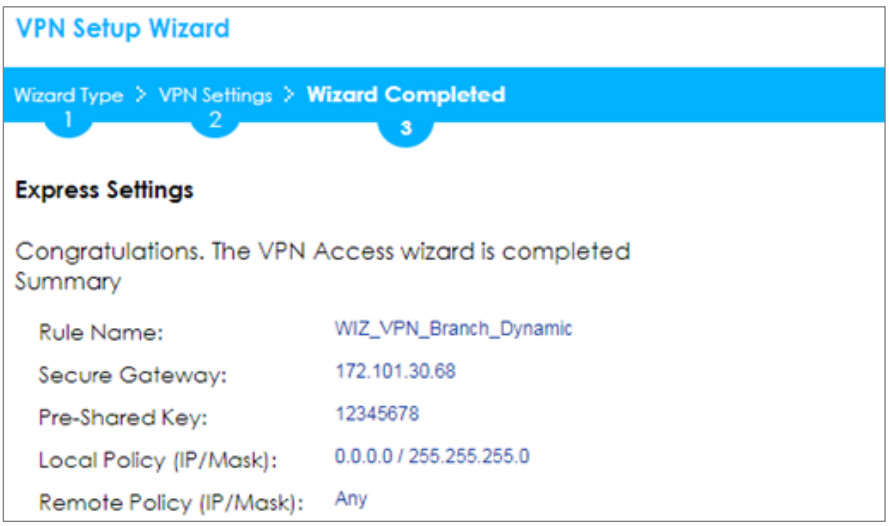
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



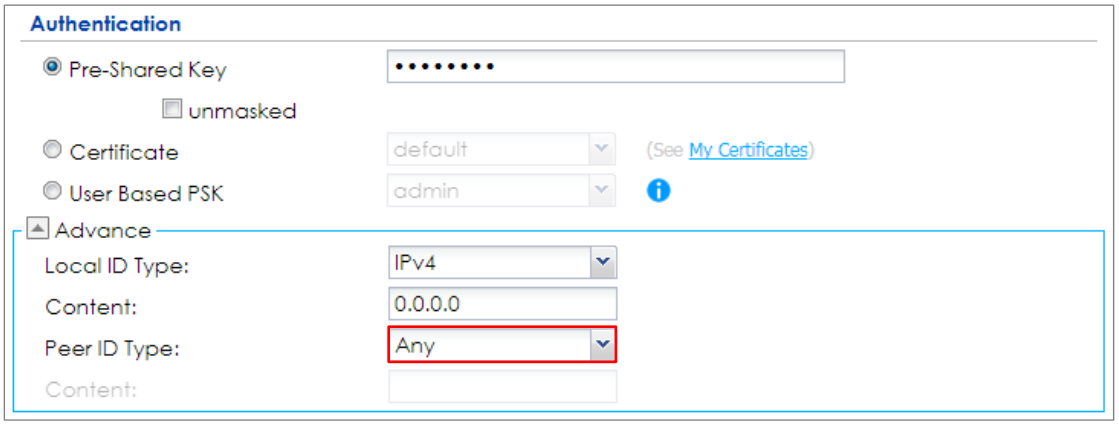
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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



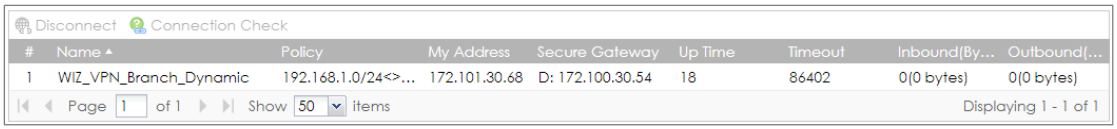
Test the IPSec VPN Tunnel

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

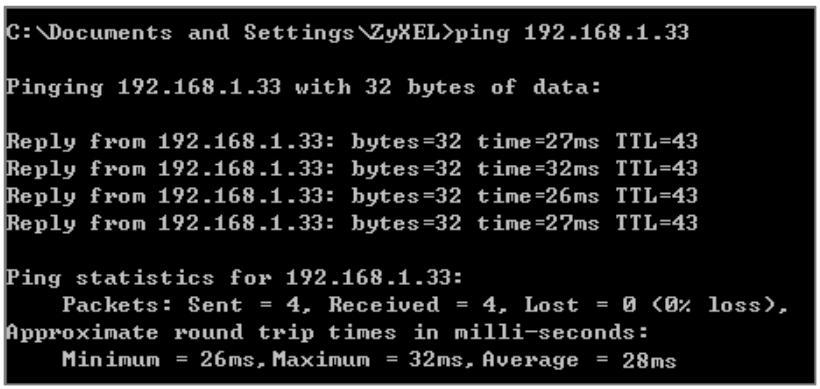
Go to **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** Traffic.

MONITOR > VPN Monitor > IPSec



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



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

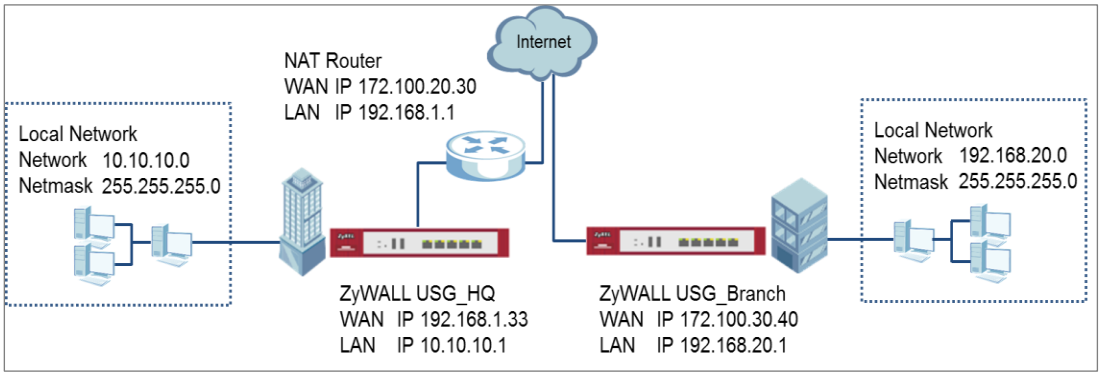
31	2017-09-11 ...	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

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.



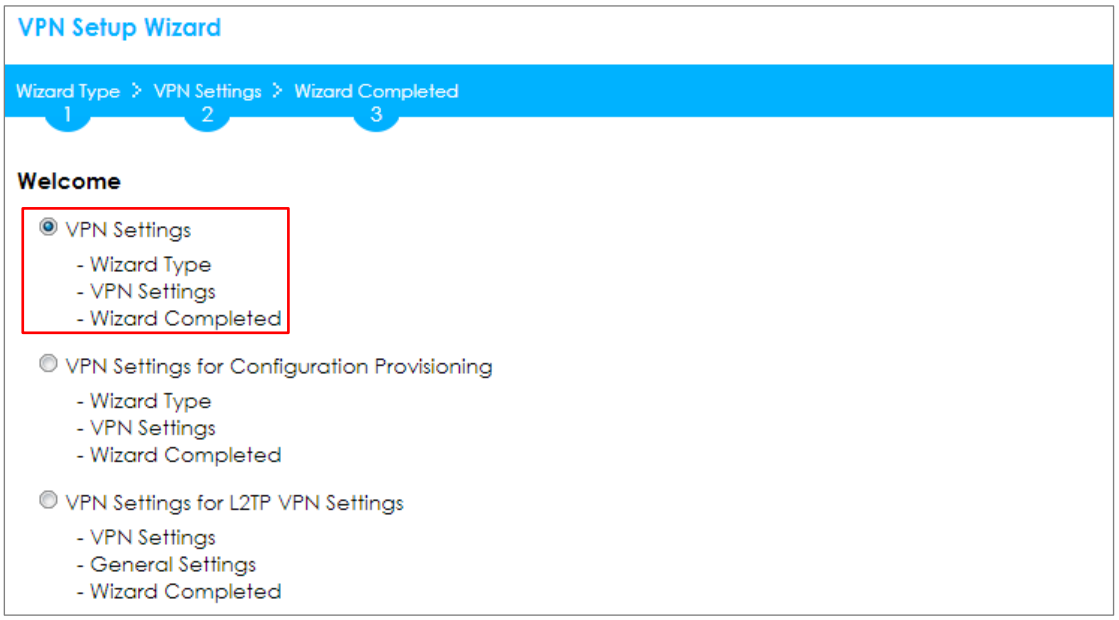
ZyWALL/USG Site to Site VPN while one Site is behind a NAT router

> 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)

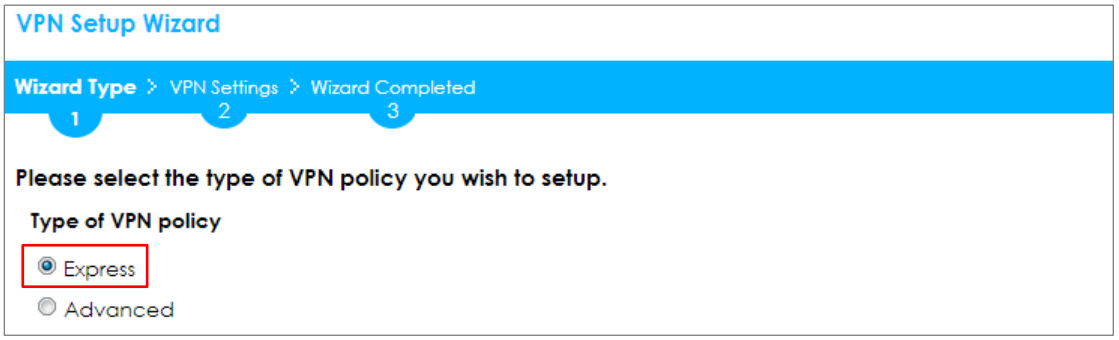
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



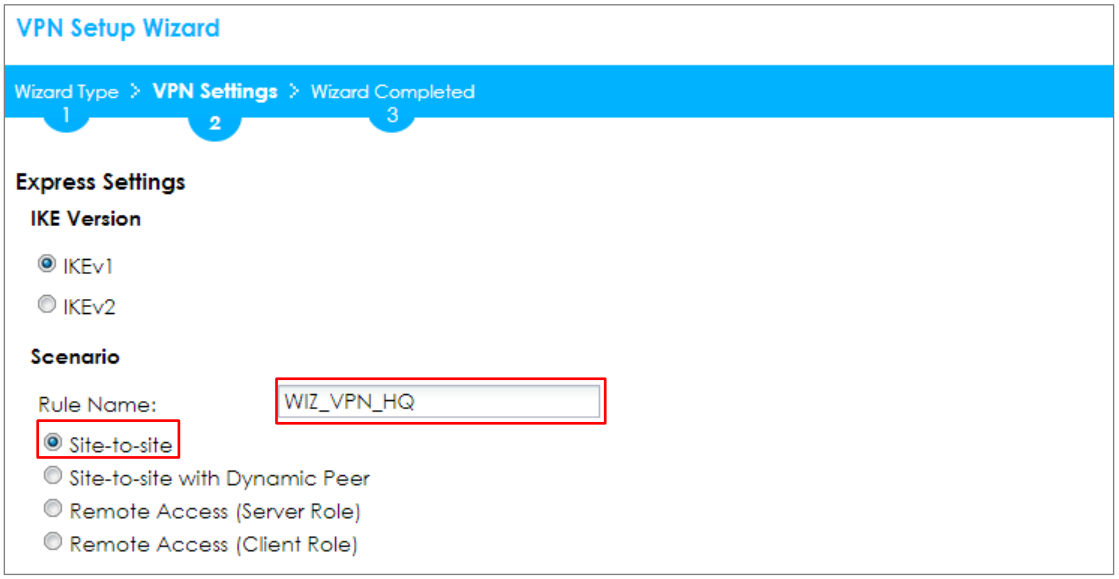
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

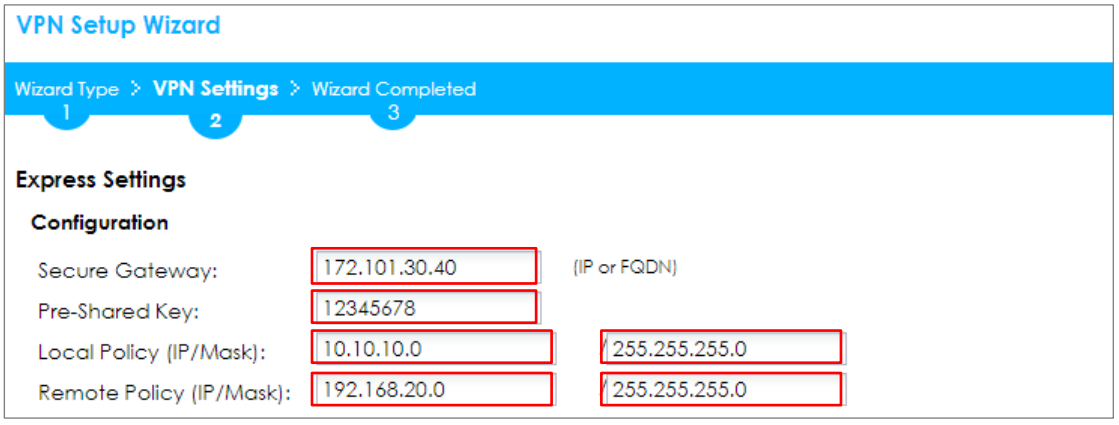
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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).

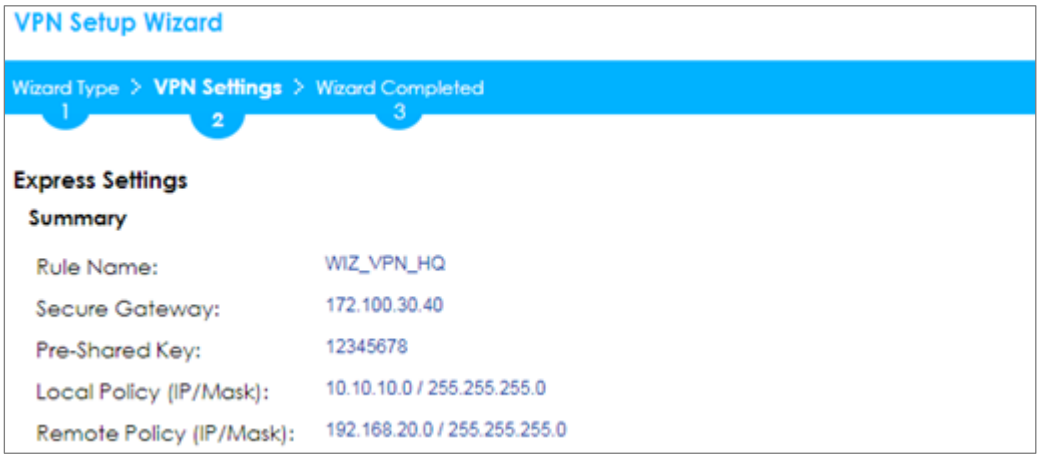
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG (HQ) and **Remote Policy** to be the IP address range of the network connected to the ZyWALL/USG (Branch).

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



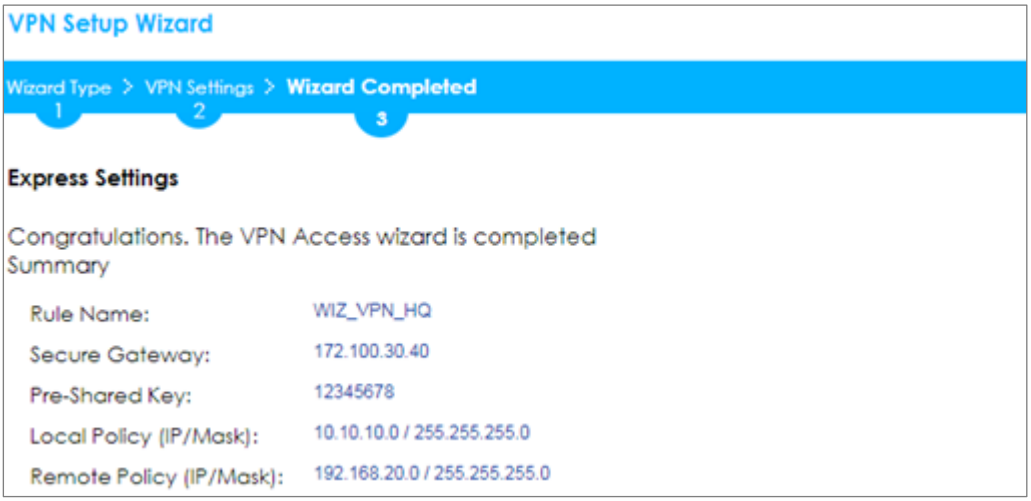
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



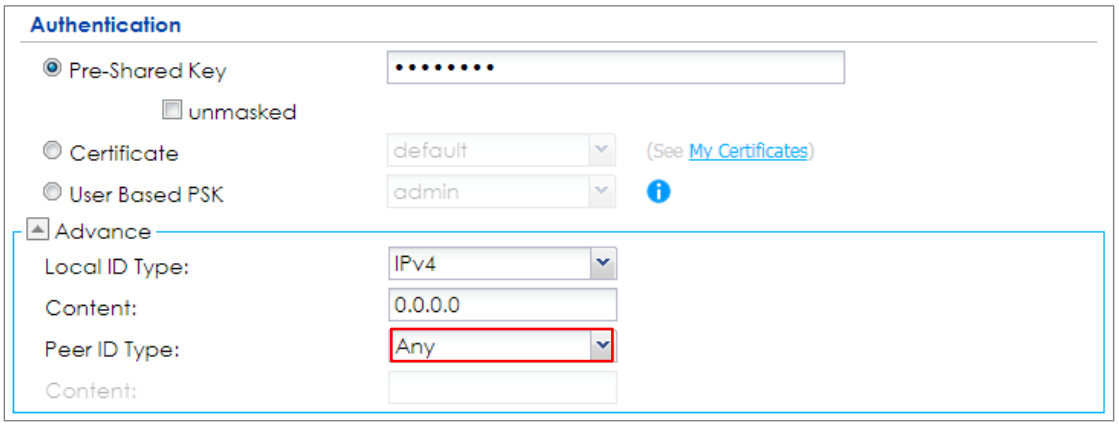
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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



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

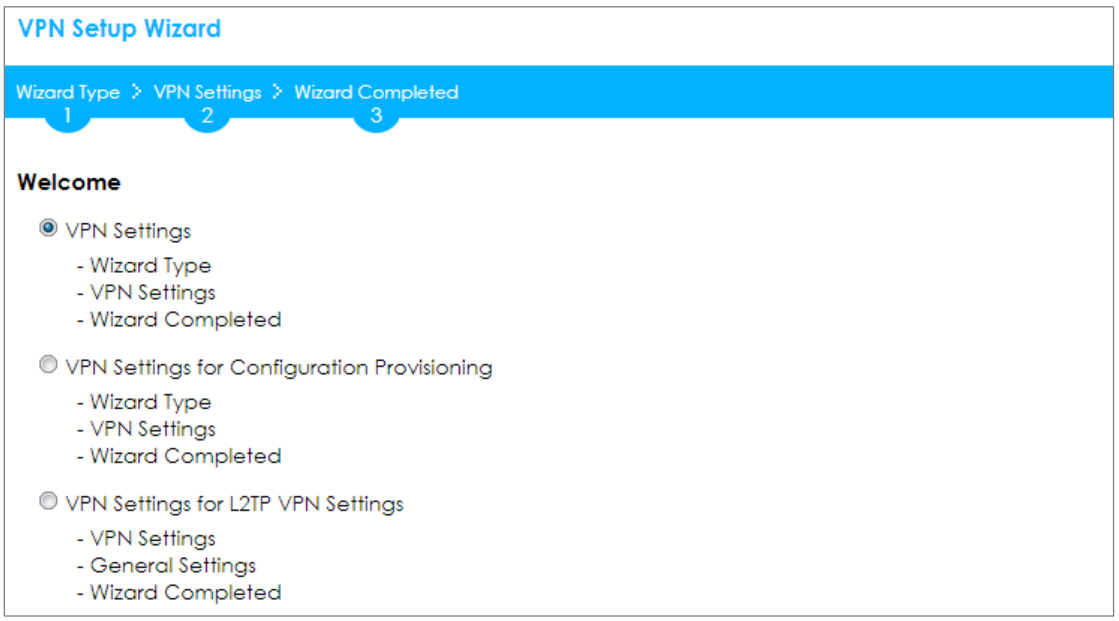
CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



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

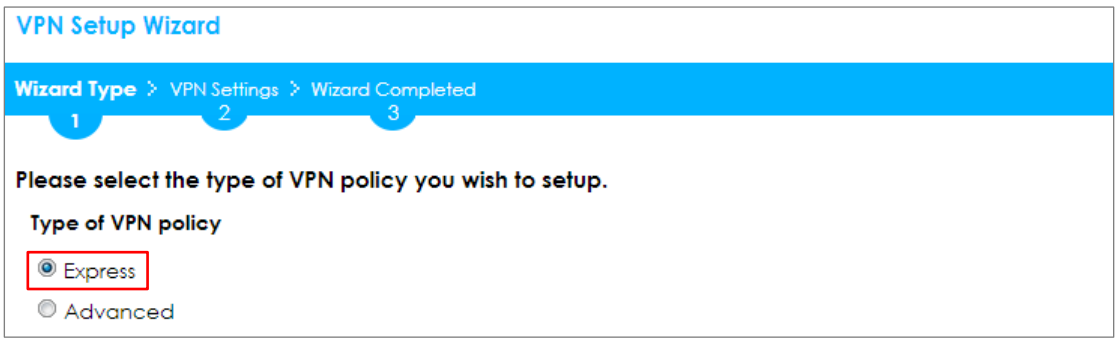
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



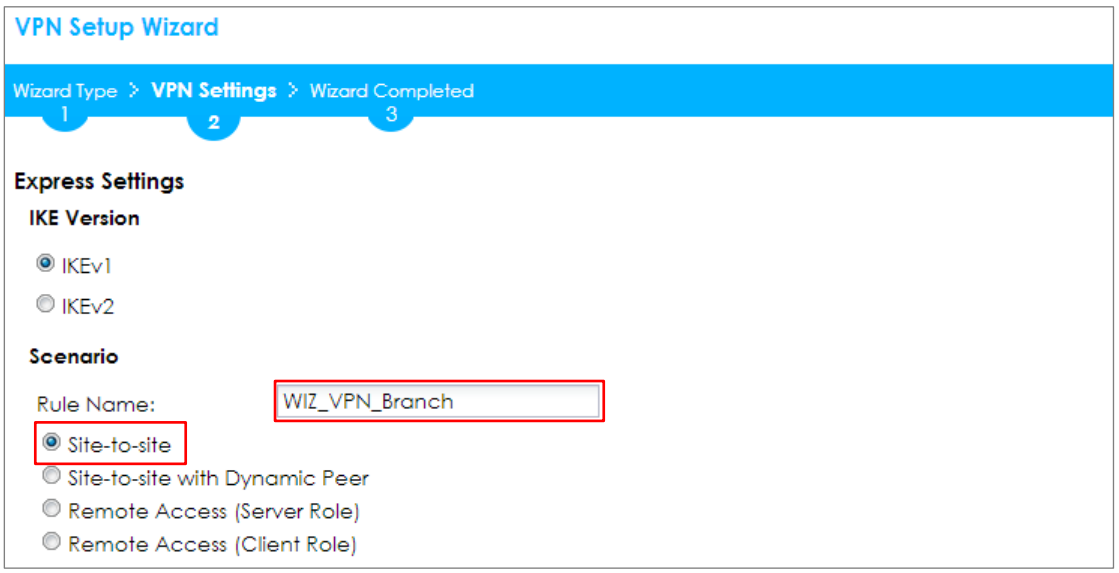
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

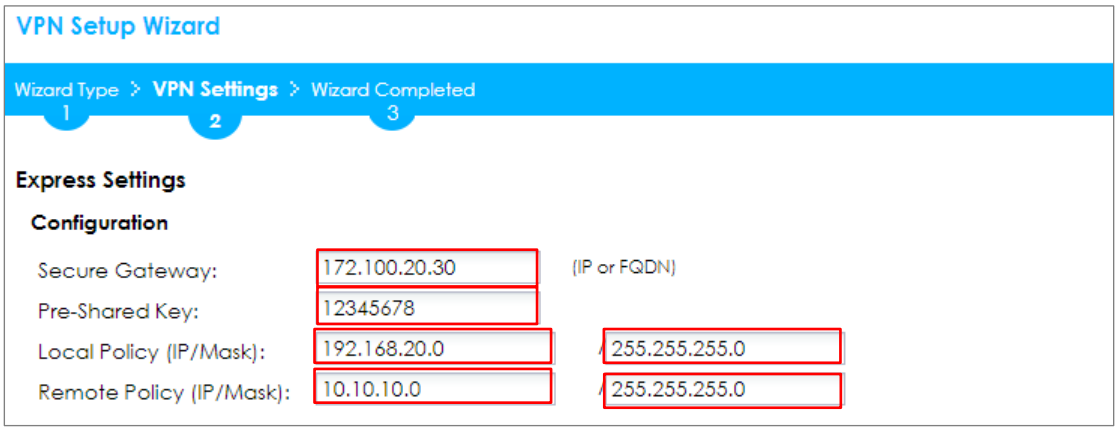
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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).

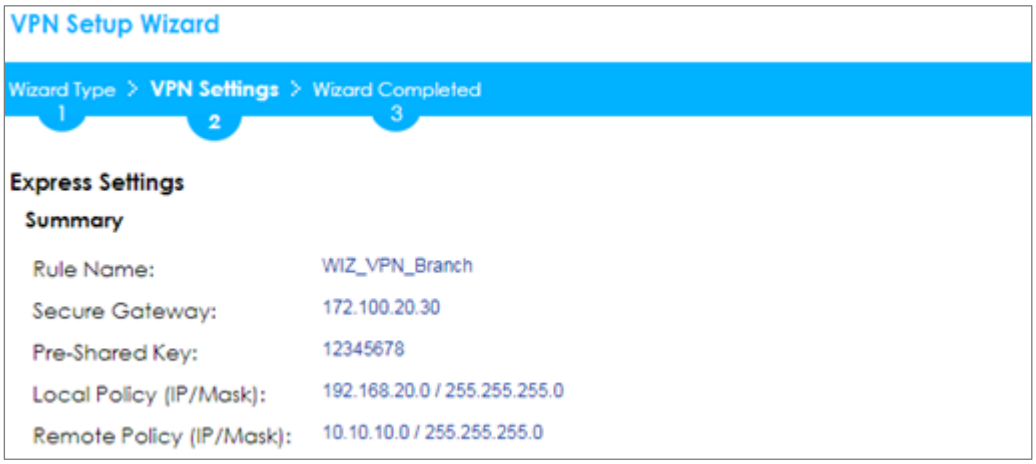
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG (HQ) and **Remote Policy** to be the IP address range of the network connected to the ZyWALL/USG (Branch).

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



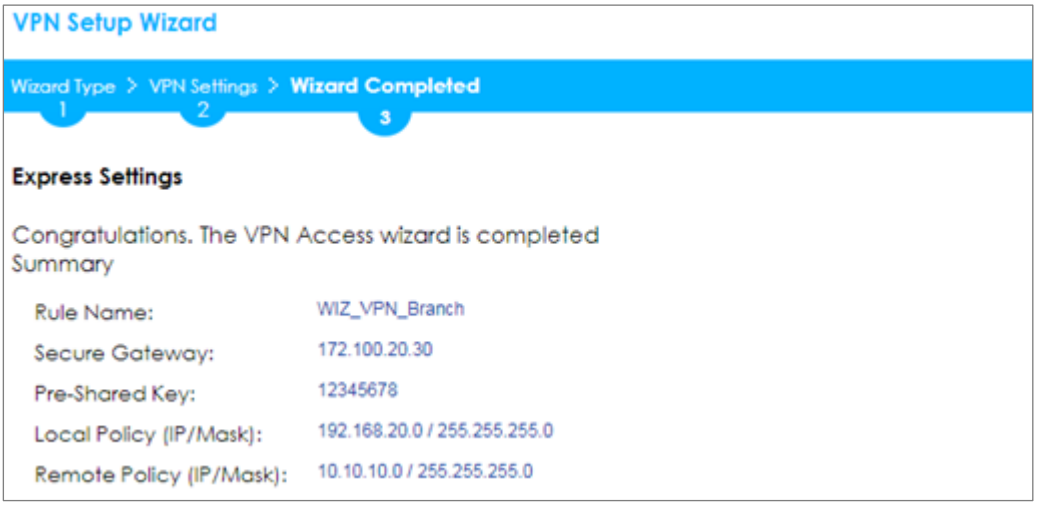
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



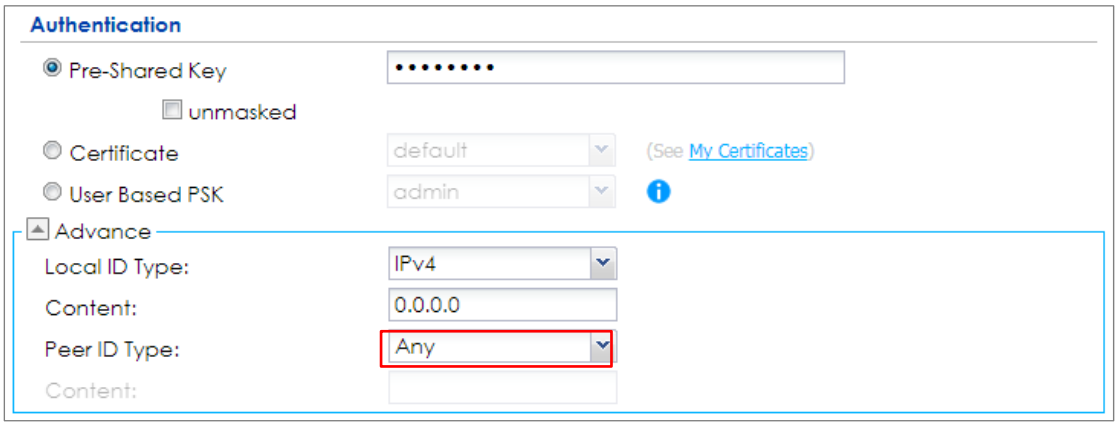
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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



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

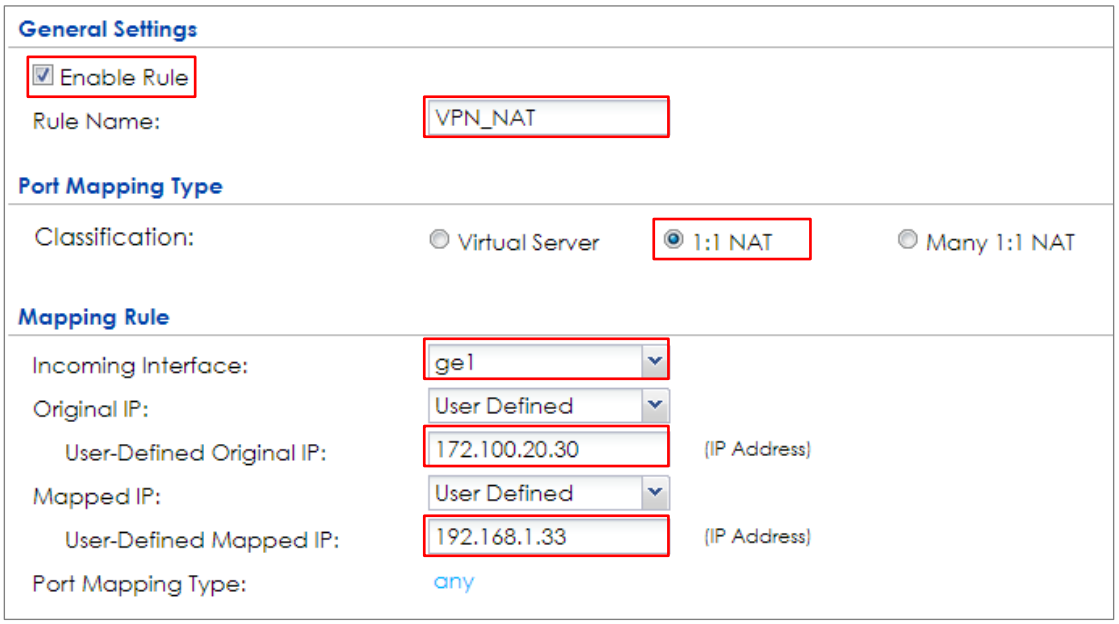


Set Up the NAT Router (Using ZyWALL USG device in this example)

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



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

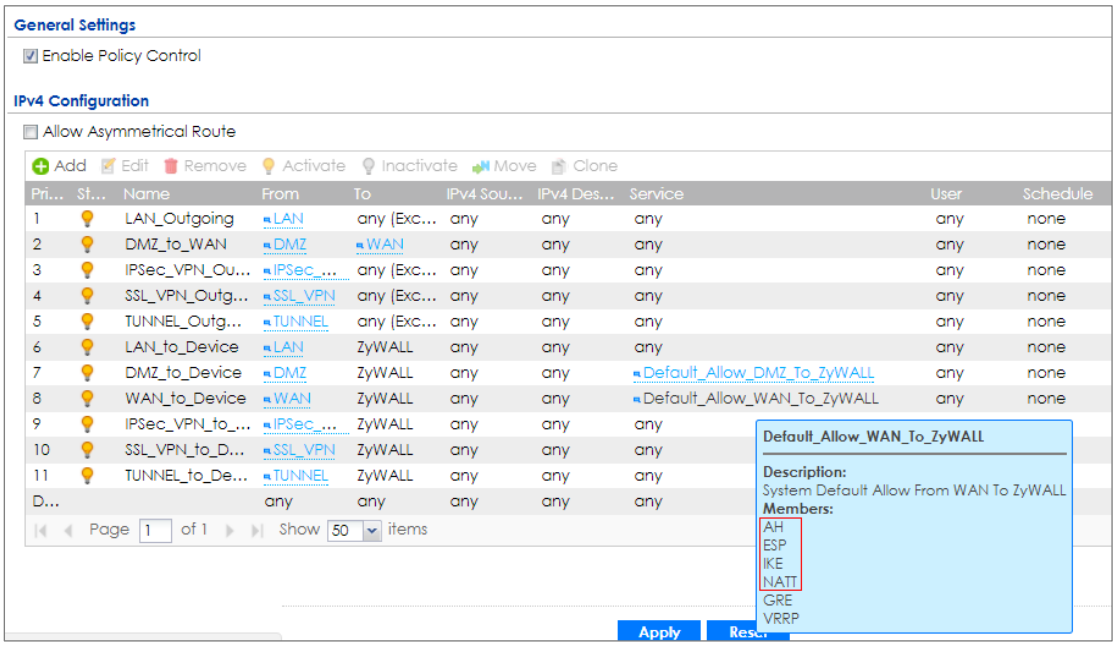
IP protocol = 50 → Used by data path (ESP)

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



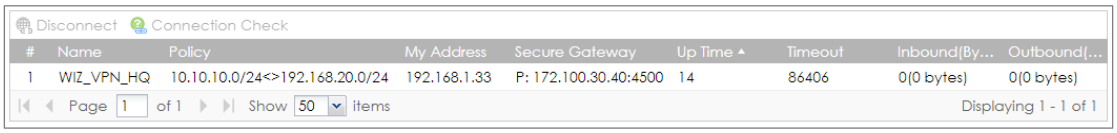
Test the IPSec VPN Tunnel

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

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

MONITOR > VPN Monitor > IPSec



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

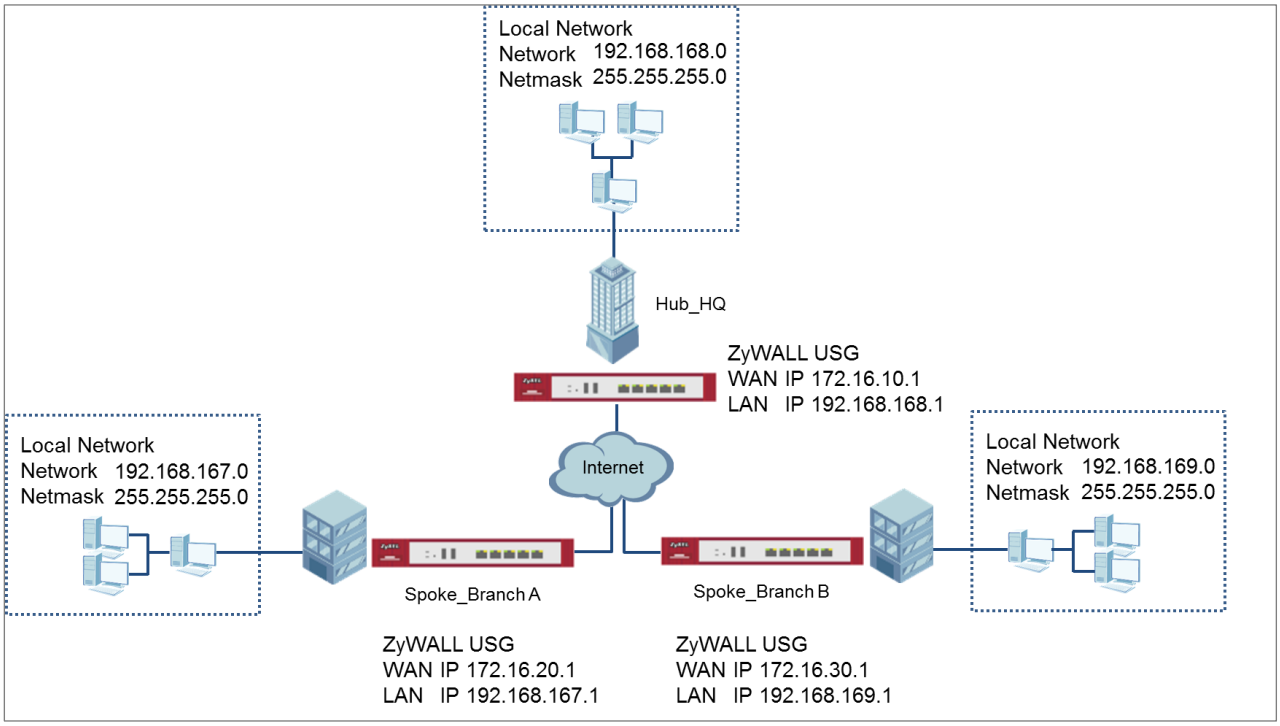
Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

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

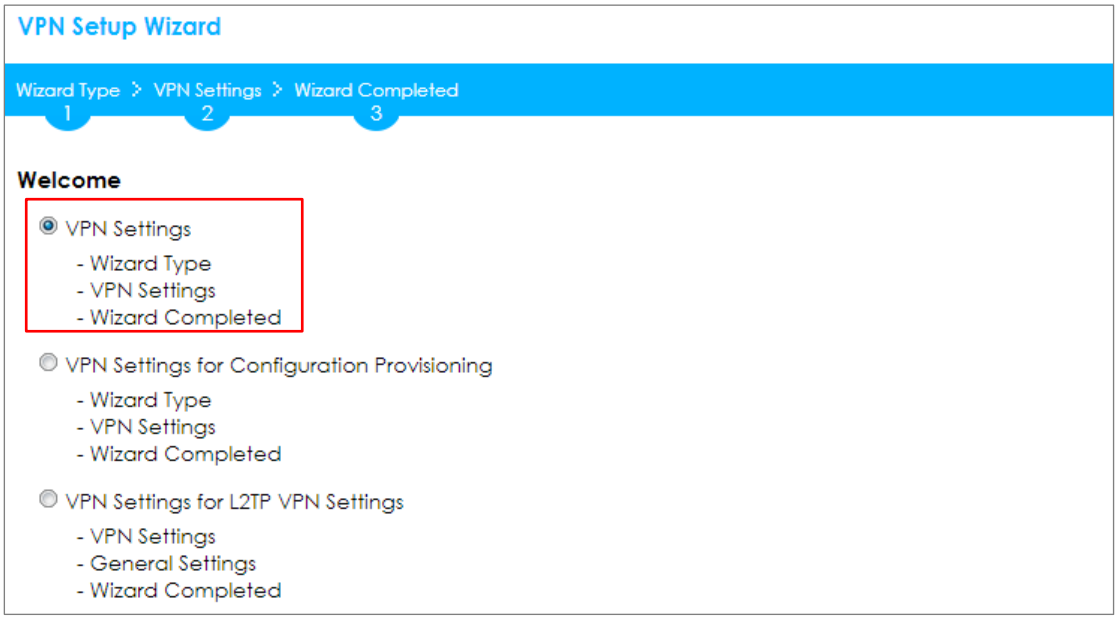


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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

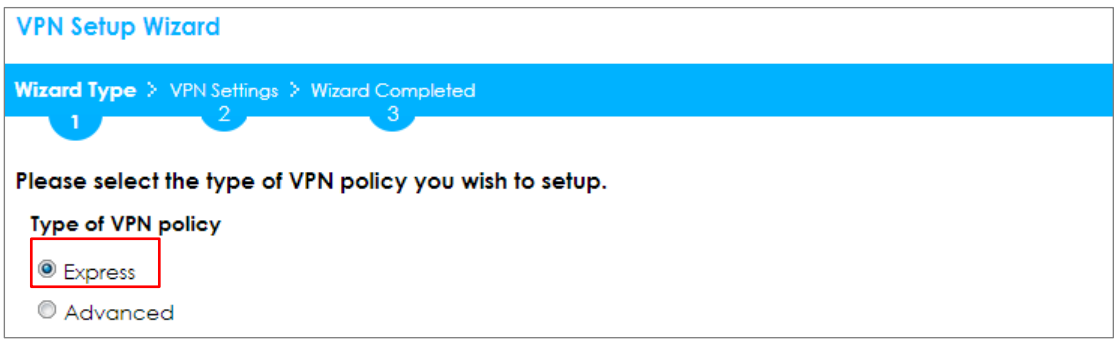
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



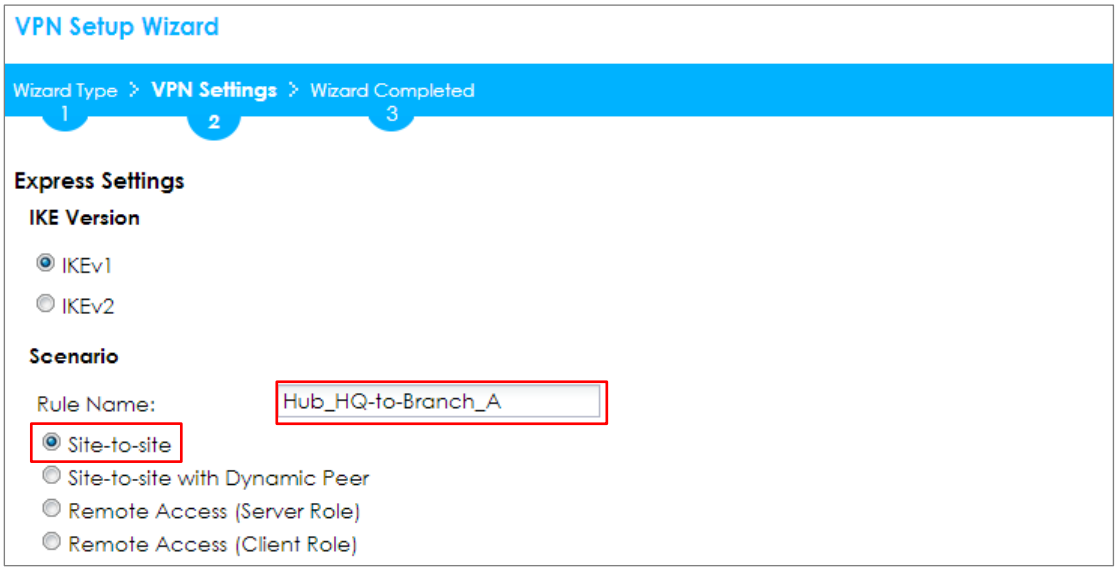
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



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**.

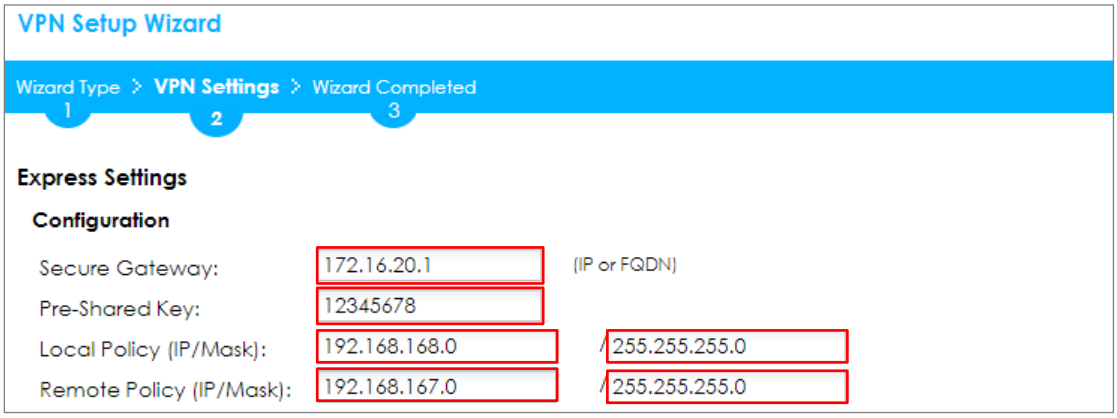
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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)

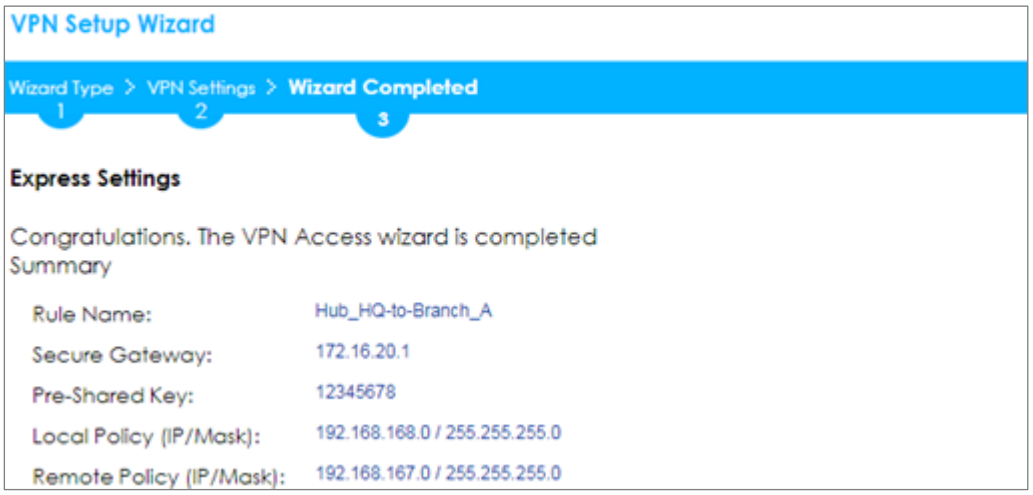


This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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

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.

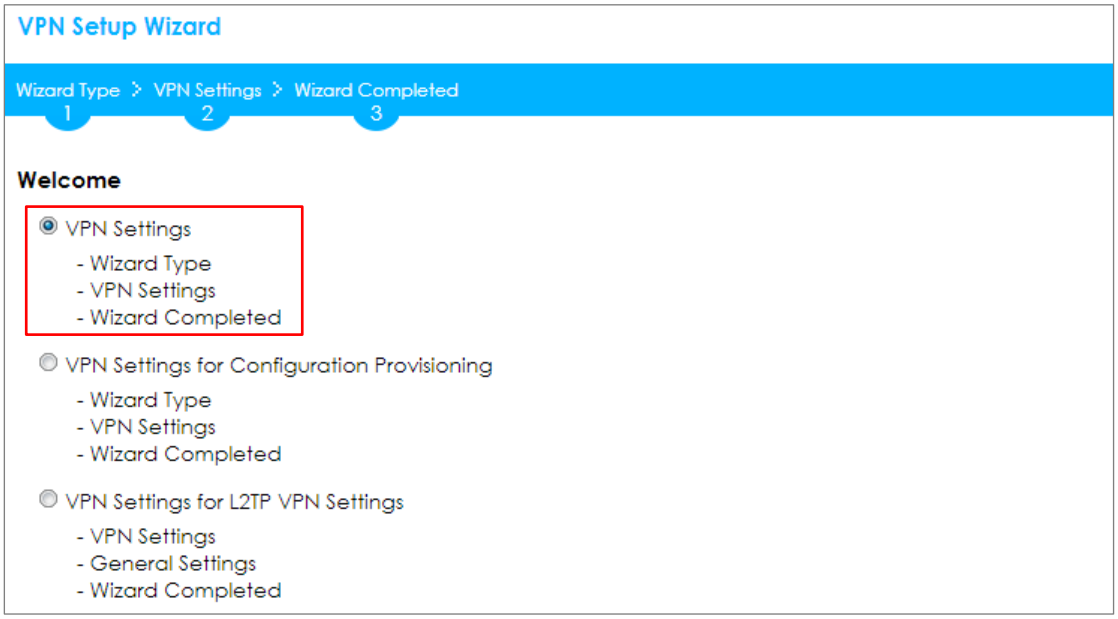
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard Completed



Hub_HQ-to-Branch_B

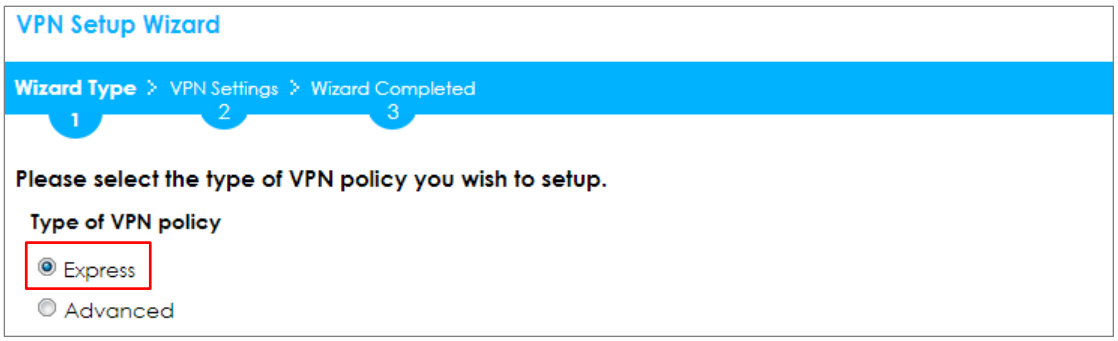
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



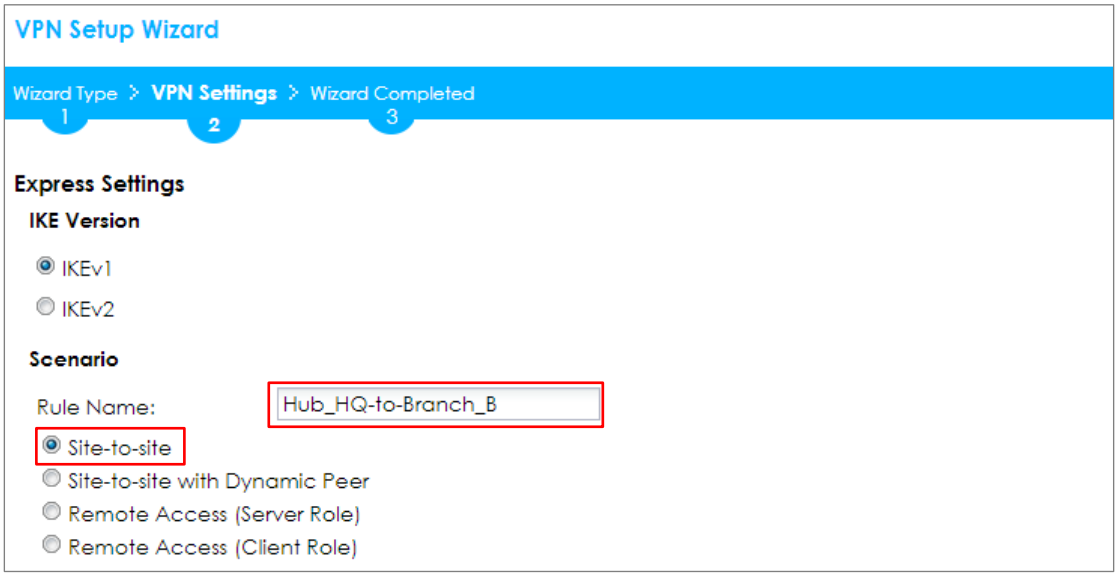
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



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**.

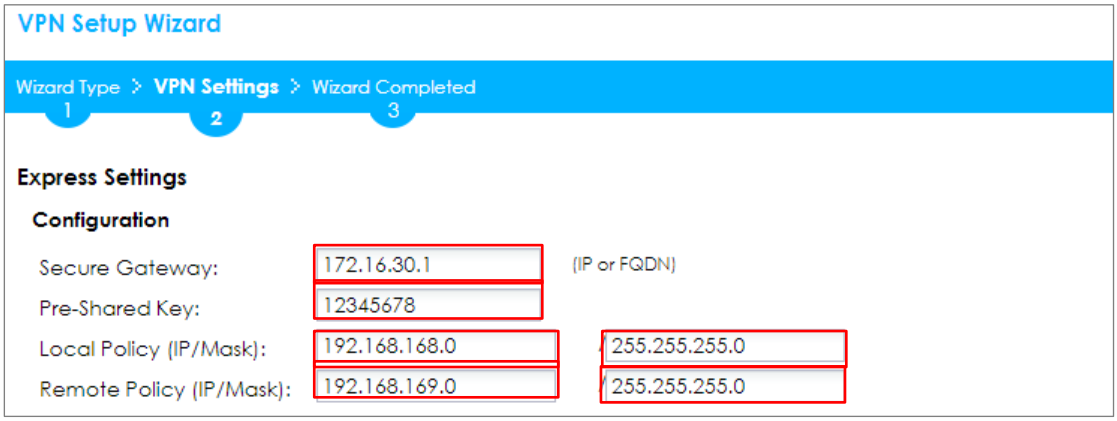
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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.

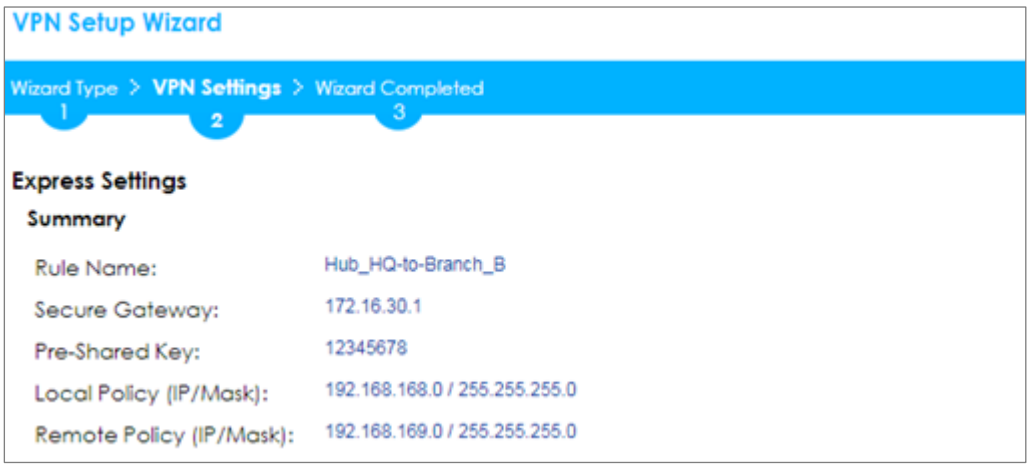
Set **Local Policy** to be the IP address range of the network connected to the **Hub_HQ** and **Remote Policy** to be the IP address range of the network connected to the **Branch B**. Click **OK**.

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



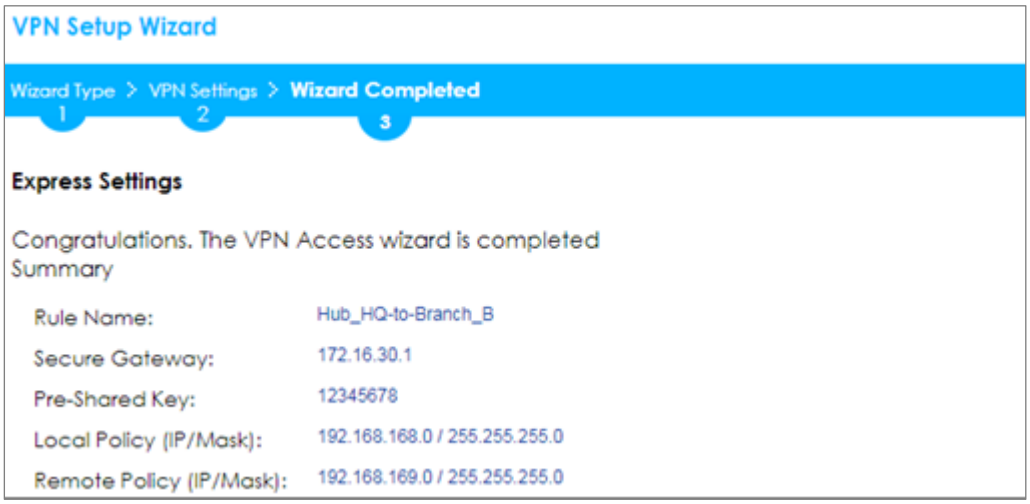
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



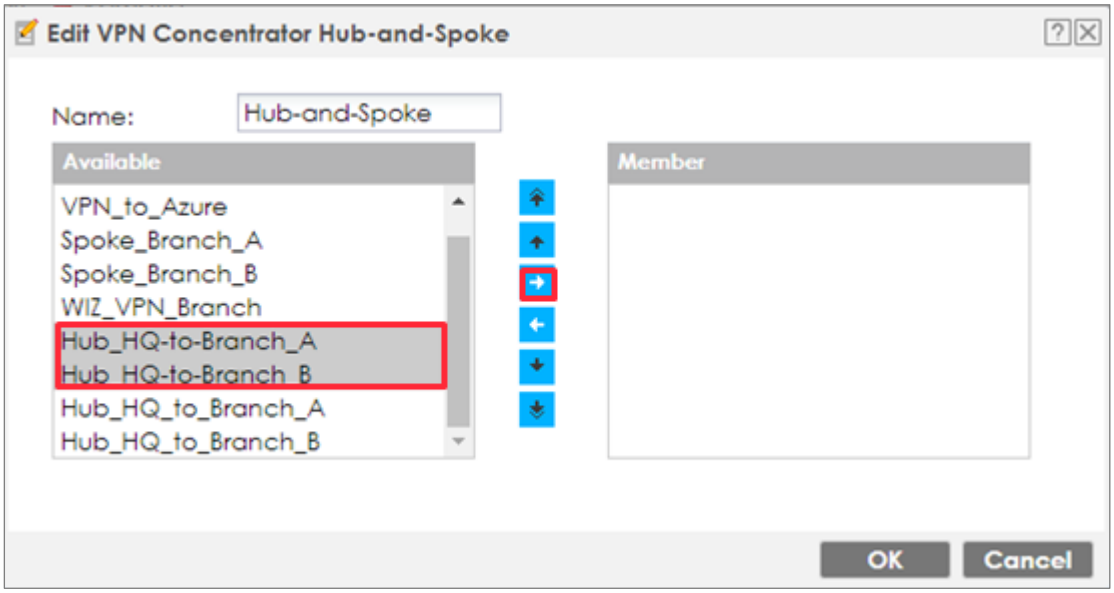
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

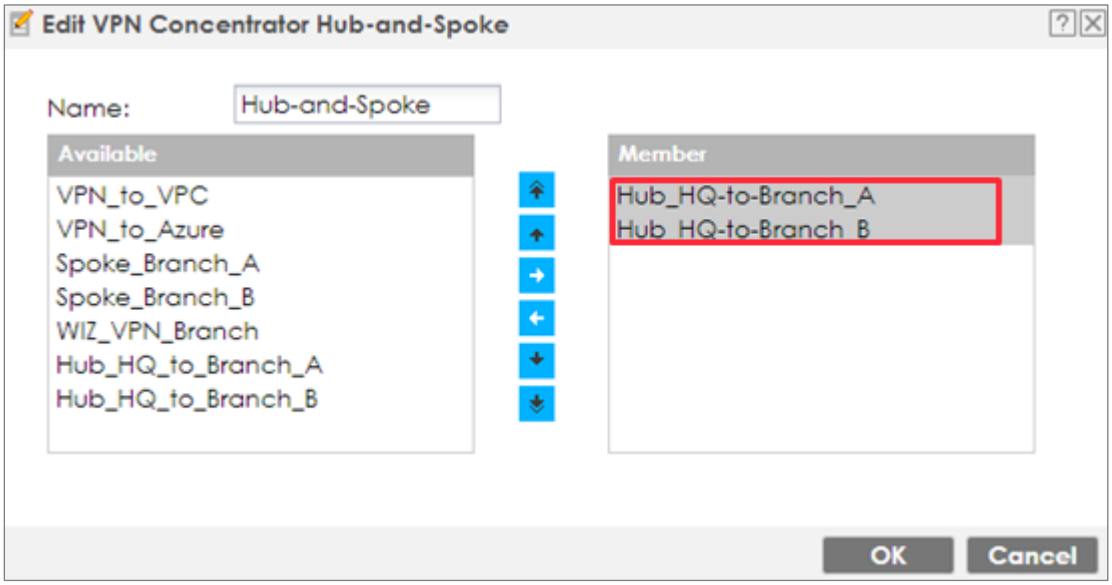
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings > Wizard Completed



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**.

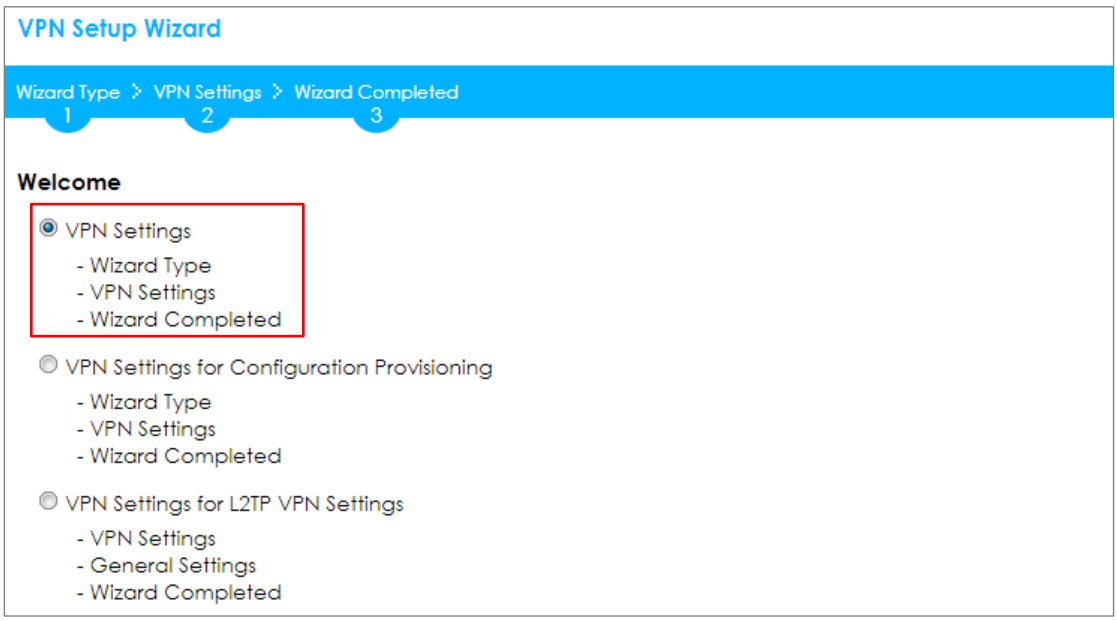




Spoke_Branch_A

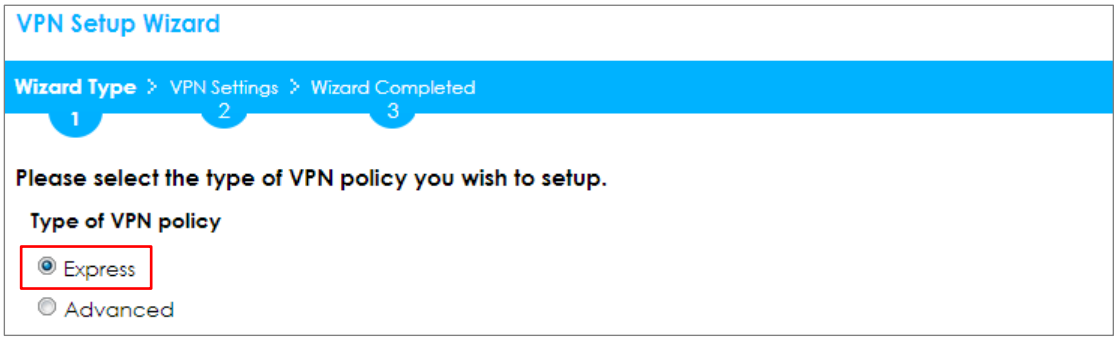
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



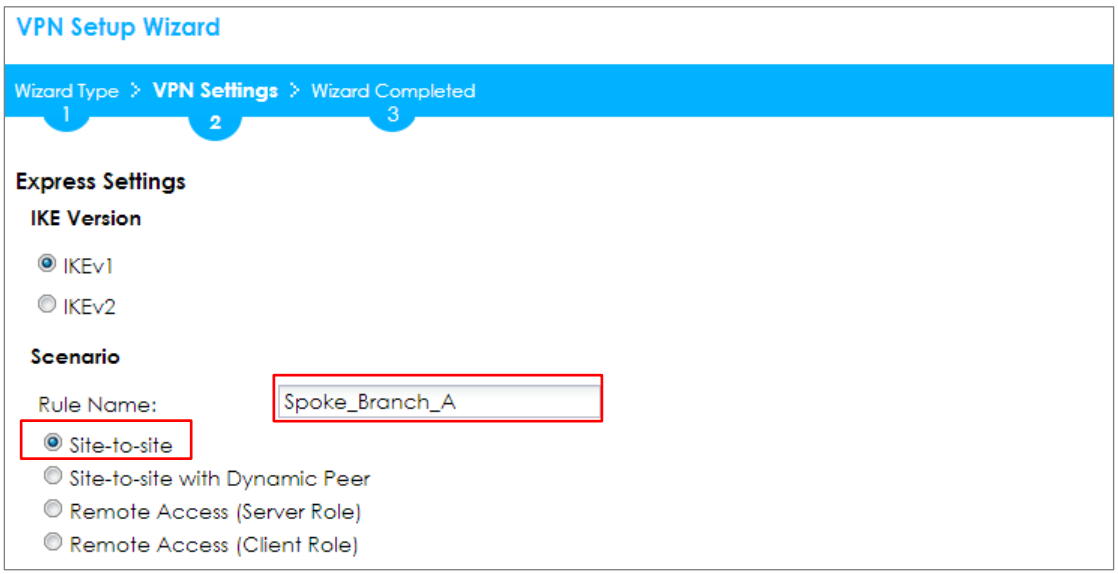
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



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**.

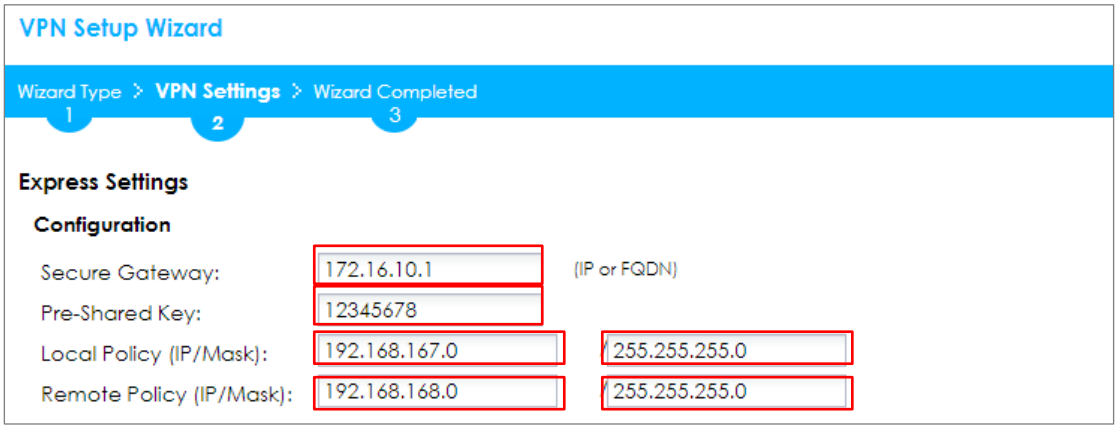
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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)

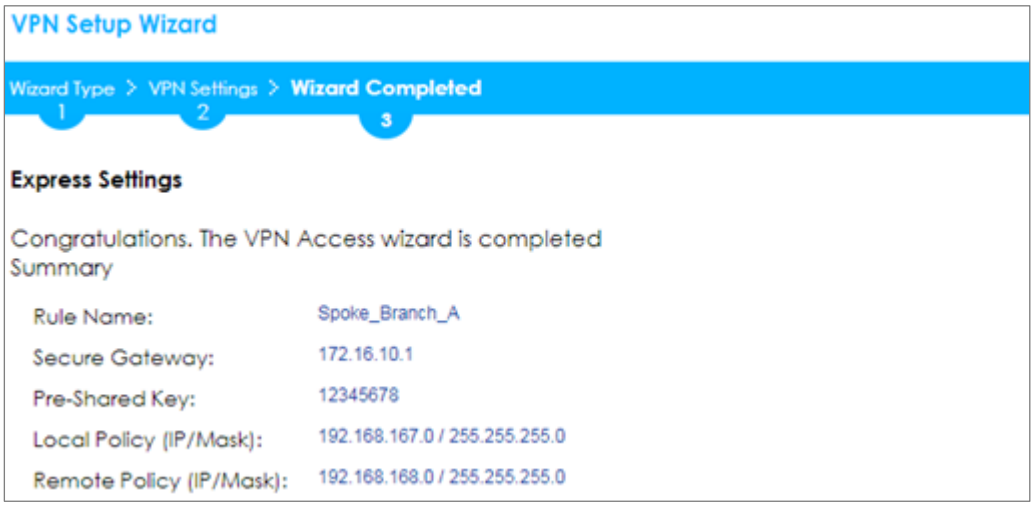


This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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

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

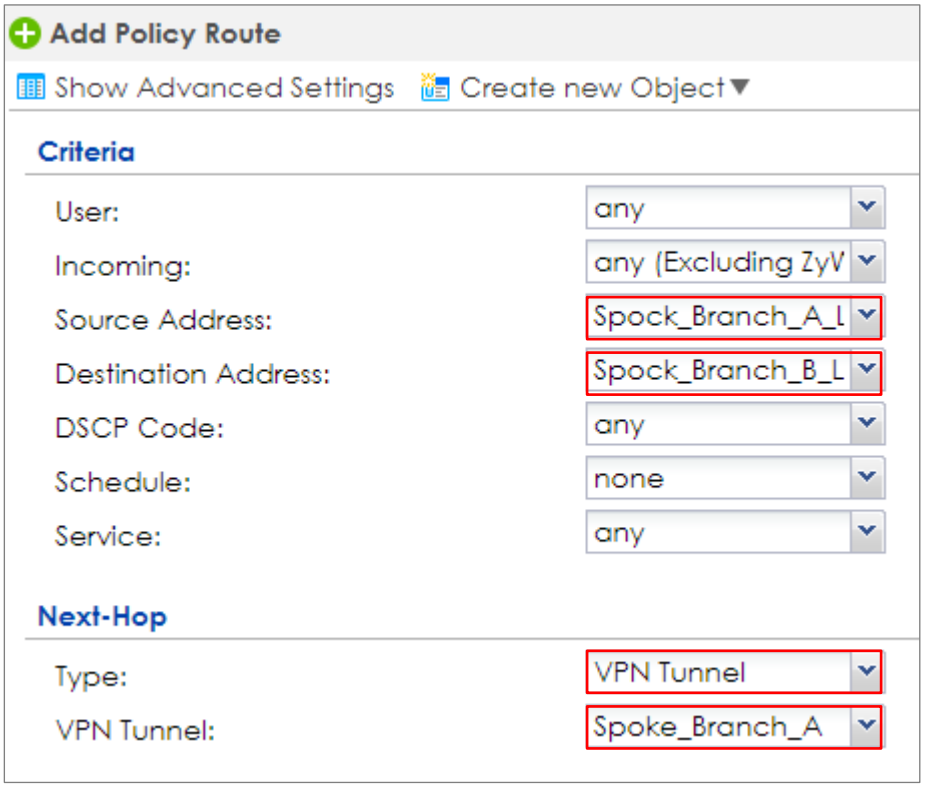


Go to **Network > Routing > Policy Route** to add a **Policy Route** to allow traffic from **Spoke_Branch_A** to **Spoke_Branch_B**.

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**.

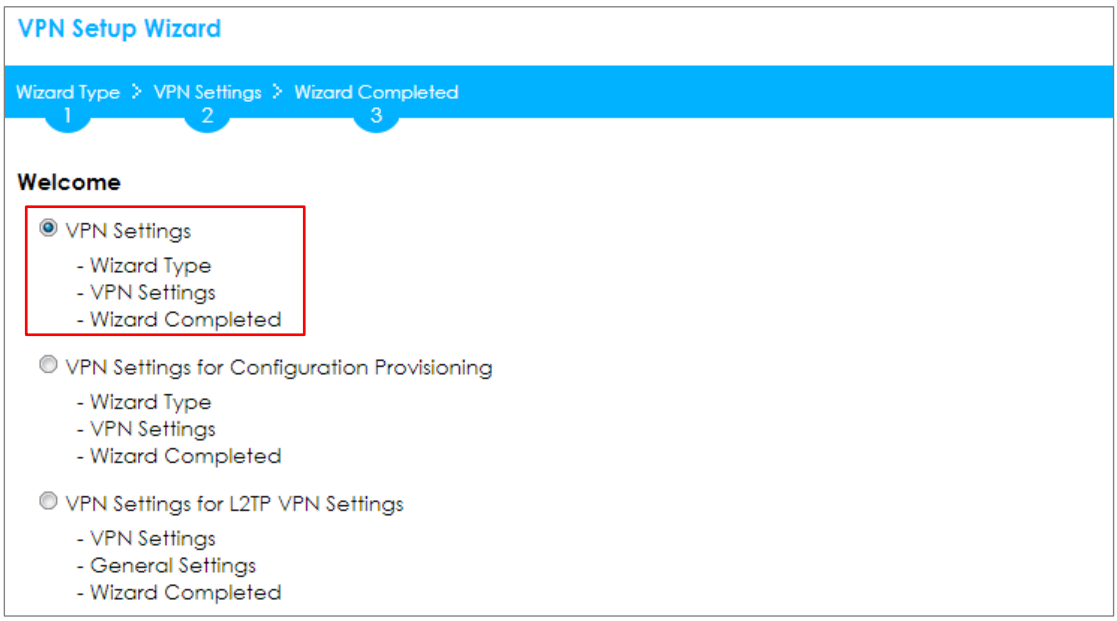
Network > Routing > Policy Route



Spoke_Branch_B

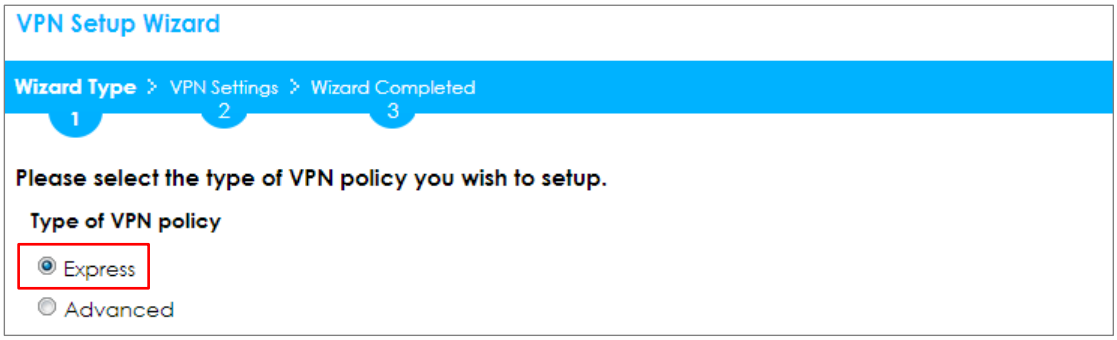
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



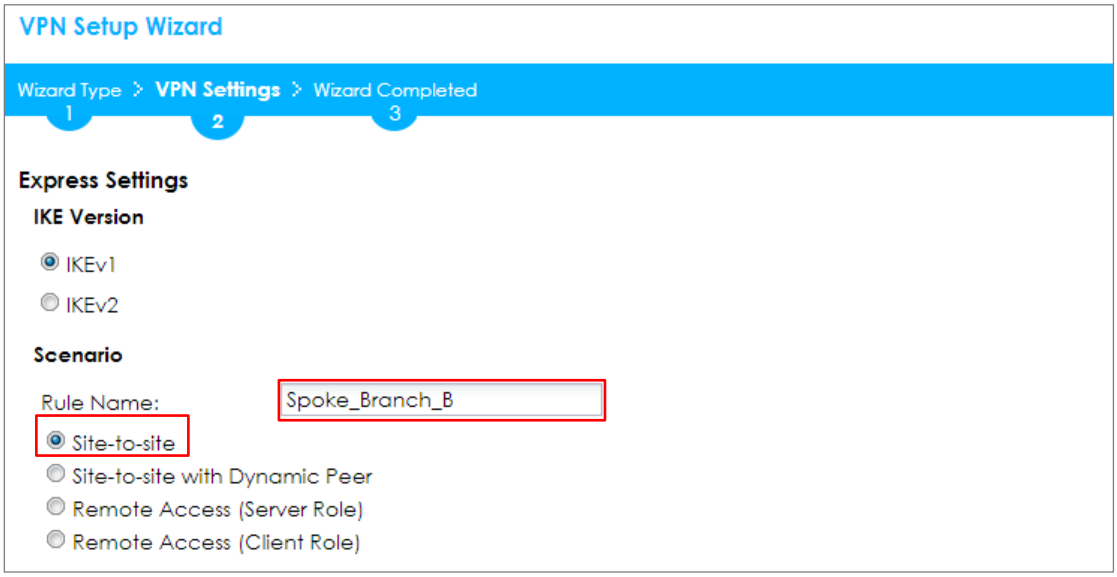
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



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**.

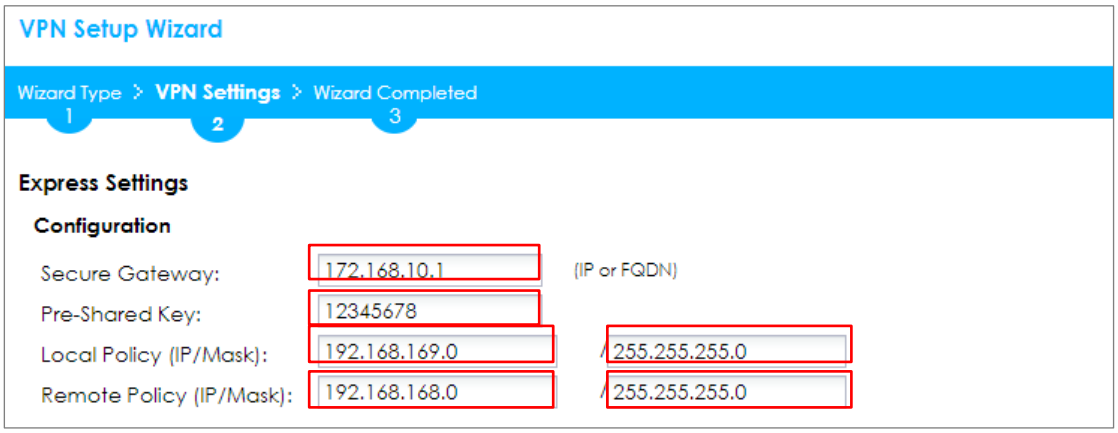
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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.

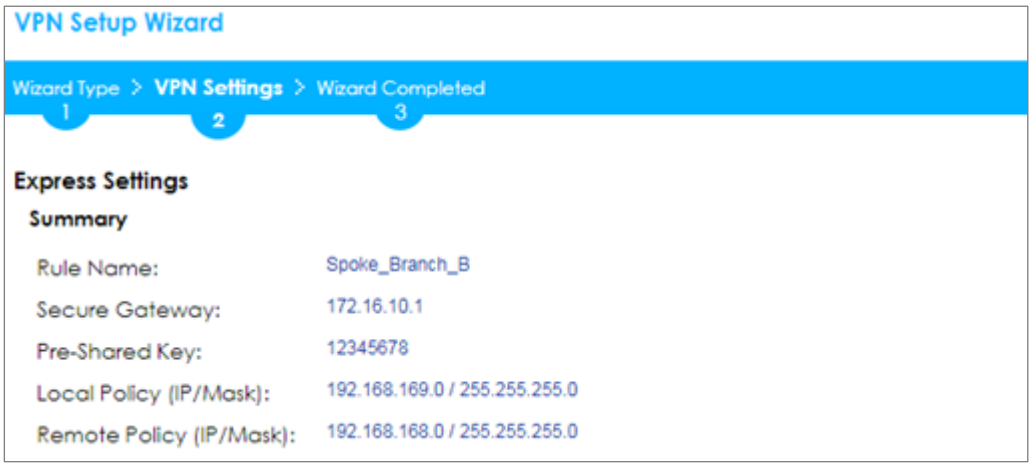
Set **Local Policy** to be the IP address range of the network connected to the **Spoke_Branch_B** and **Remote Policy** to be the IP address range of the network connected to the **Hub_HQ**. Click **OK**.

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



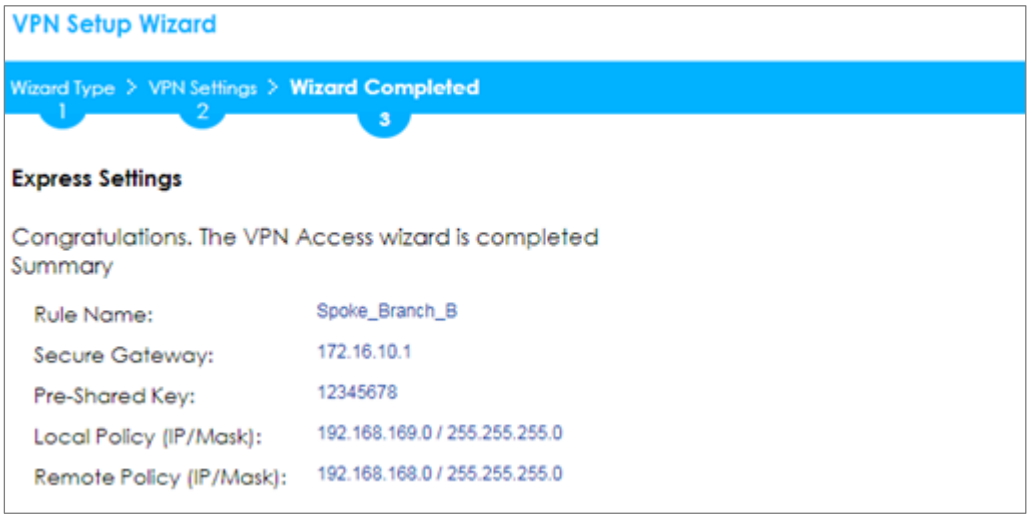
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



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

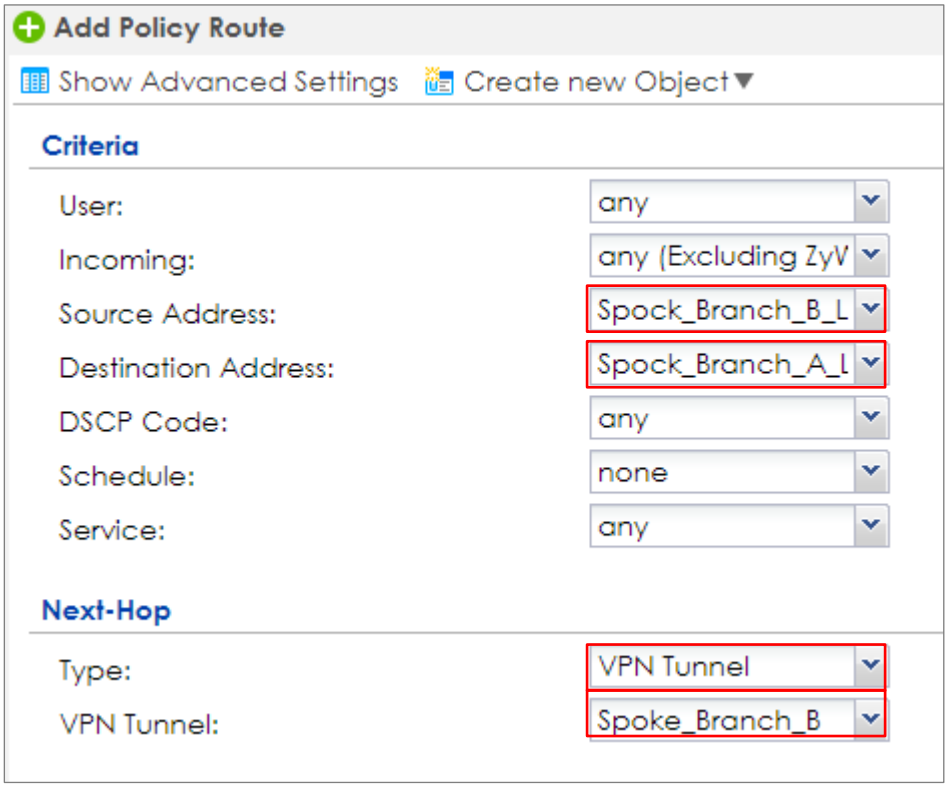


Go to **Network > Routing > Policy Route** to add a Policy Route to allow traffic from **Spoke_Branch_B** to **Spoke_Branch_A**.

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**.

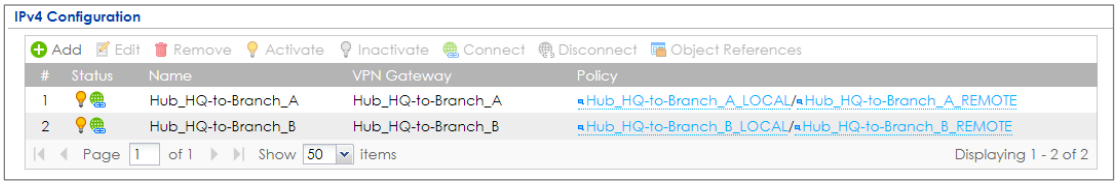
Network > Routing > Policy Route



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

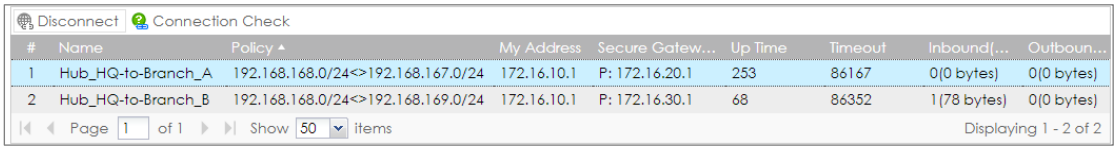


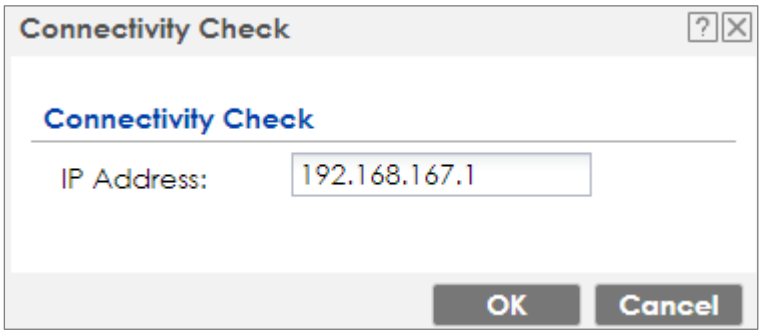
Spoke_Branch_A > CONFIGURATION > VPN > IPSec VPN > VPN Connection

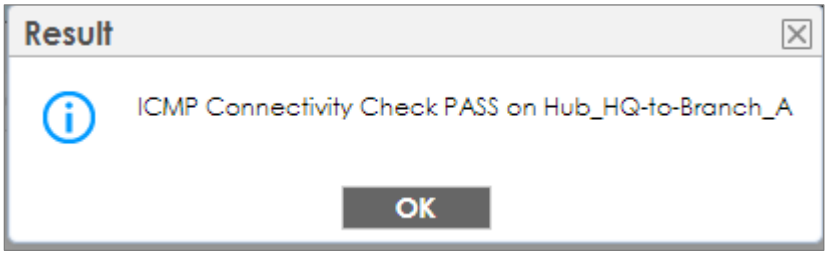
Spoke_Branch_B > CONFIGURATION > VPN > IPSec VPN > VPN Connection

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.

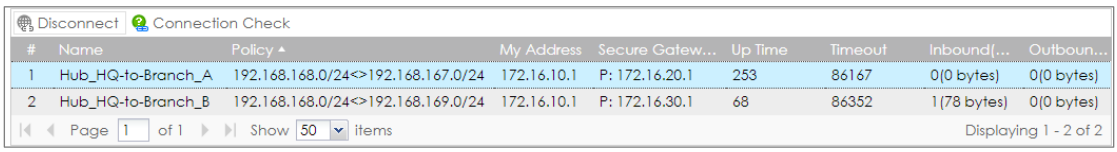
Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_A

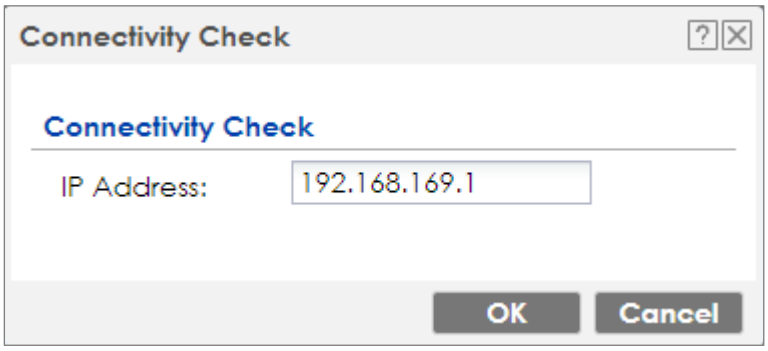


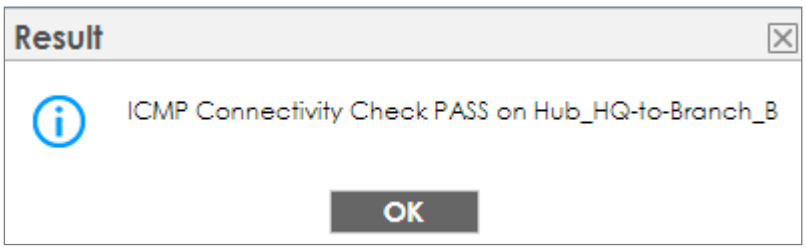




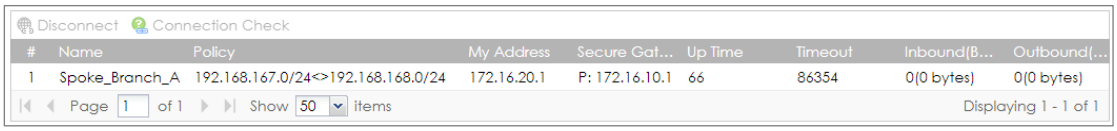
Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_B

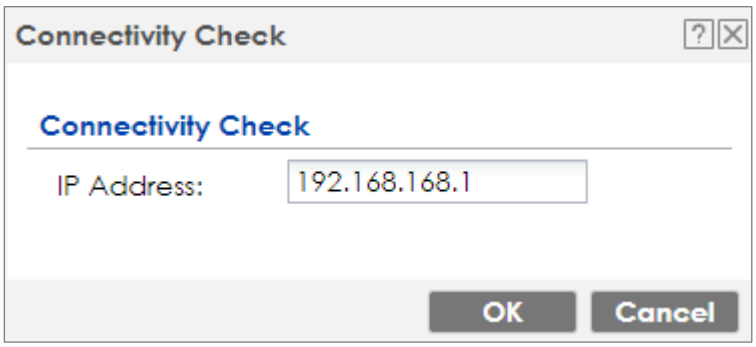


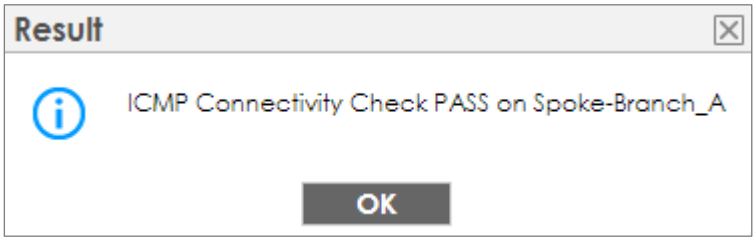




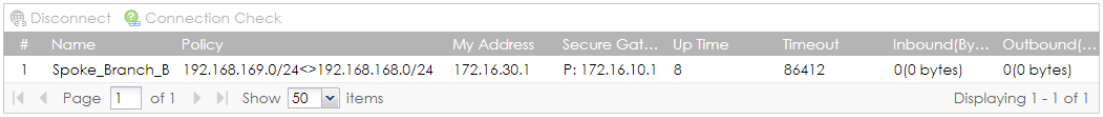
Spoke_Branch_A > MONITOR > VPN Monitor > IPSec

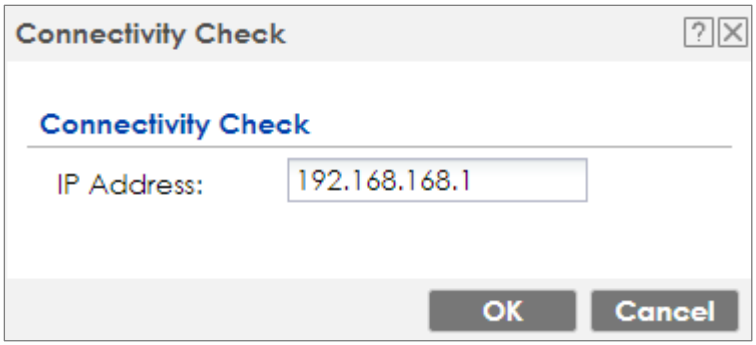


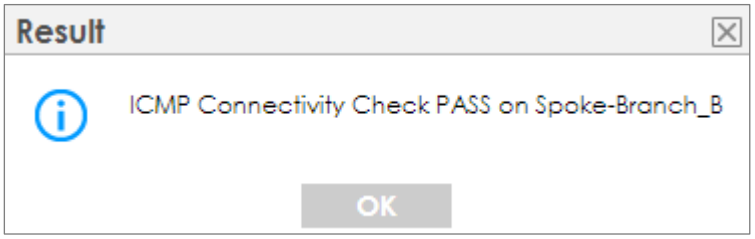




Spoke_Branch_B > MONITOR > VPN Monitor > IPSec







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.

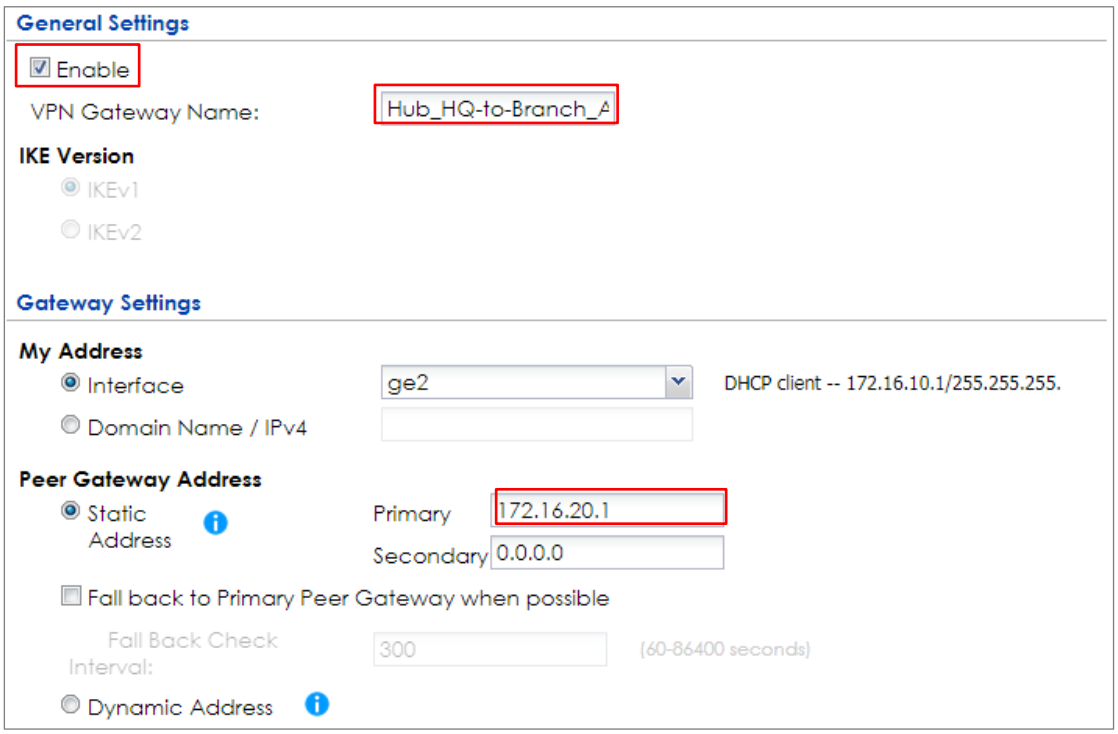
By default, NAT traversal is enabled on ZyWALL/USG, so please make sure the remote IPSec device also has NAT traversal enabled.

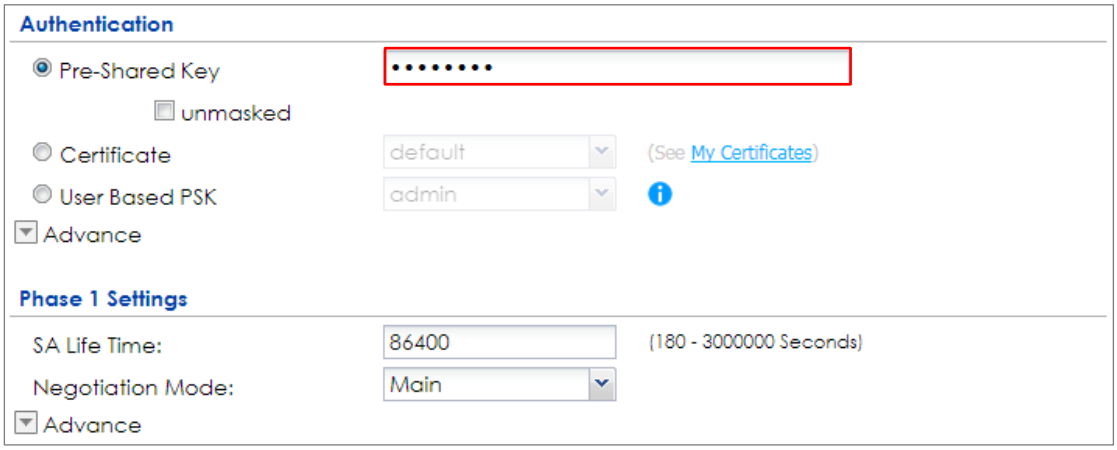
Set Up the IPSec VPN Tunnel of ZyWALL/USG without Using VPN Concentrator Hub_HQ-to-Branch_A

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**.

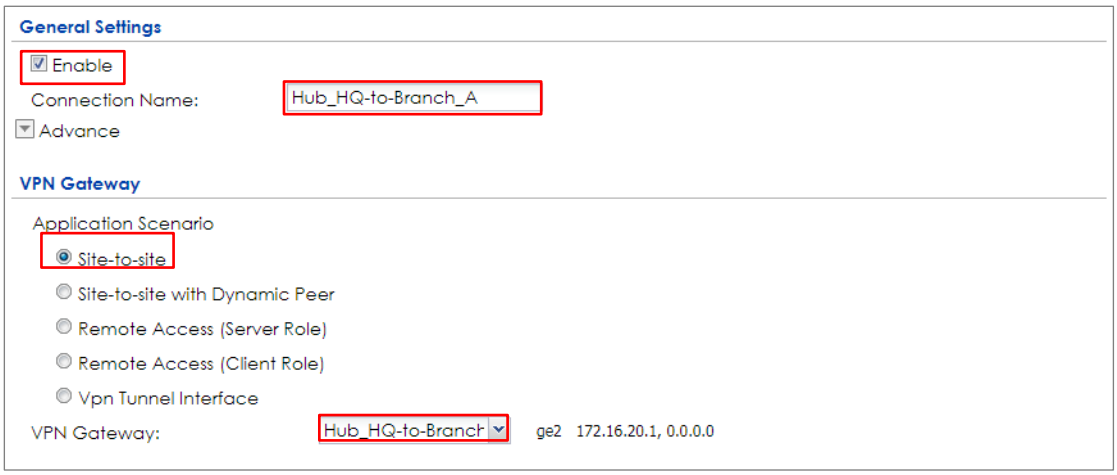
CONFIGURATION > VPN > IPSec VPN > VPN Gateway





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.

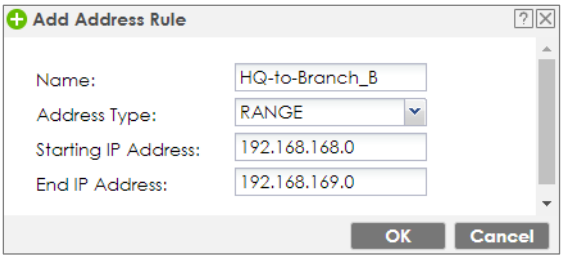
CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



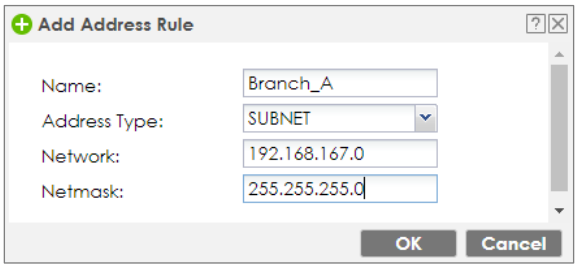
Click **Create new Object** on the upper bar to add the address range of the local network behind **Hub_HQ** to **Branch_B** and an address of local network behind **Branch A**.

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

Local Policy

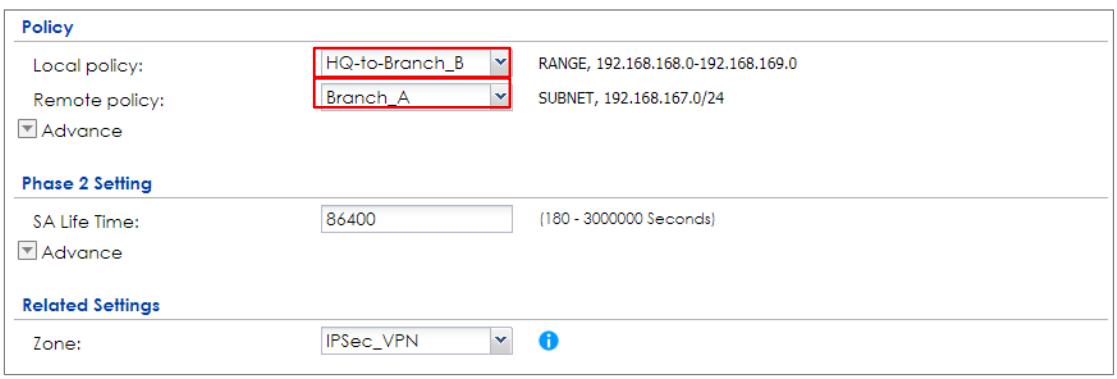


Remote Policy



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

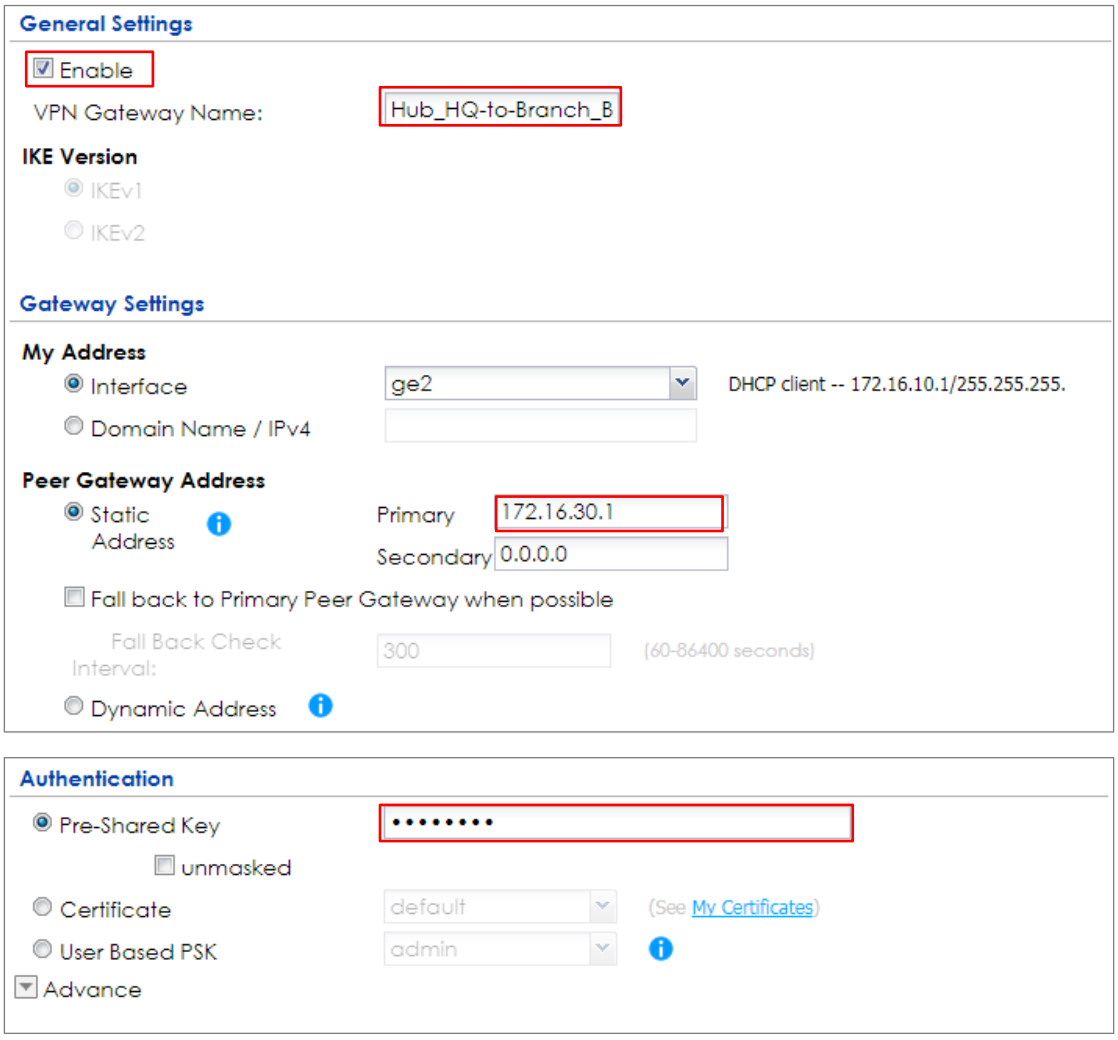


Hub_HQ-to-Branch_B

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



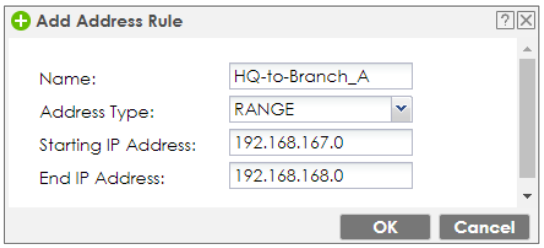
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

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

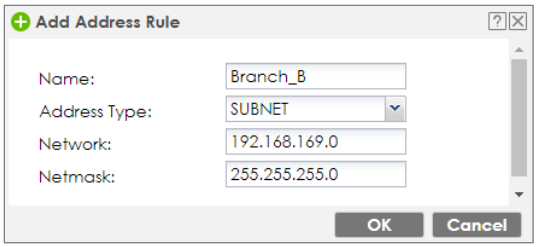
Click **Create new Object** on the upper bar to add the address range of the local network behind **Hub_HQ** to **Branch_A** and an address of local network behind **Branch B**.

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

Local Policy

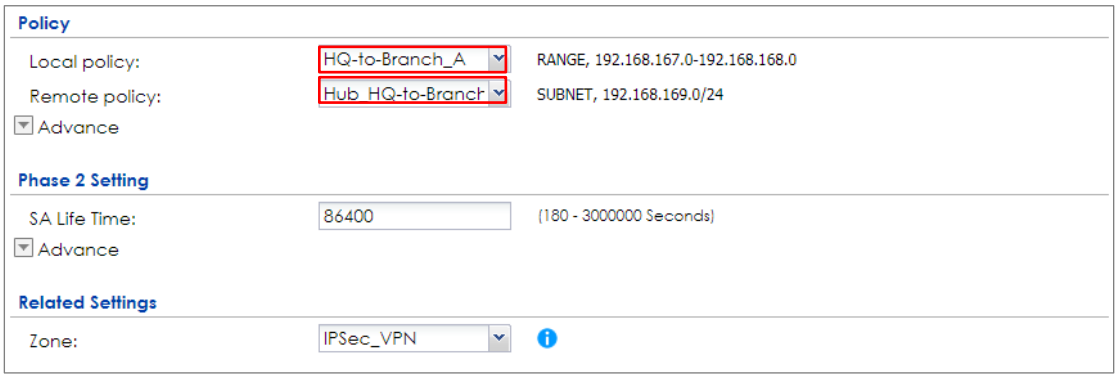


Remote Policy



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

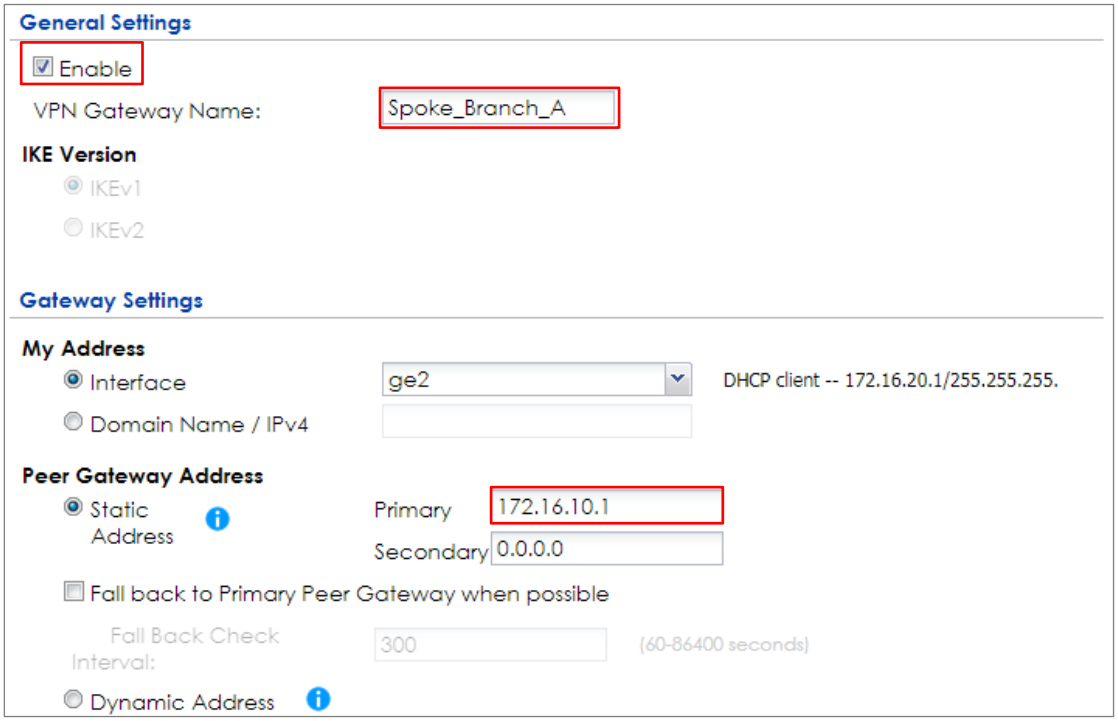


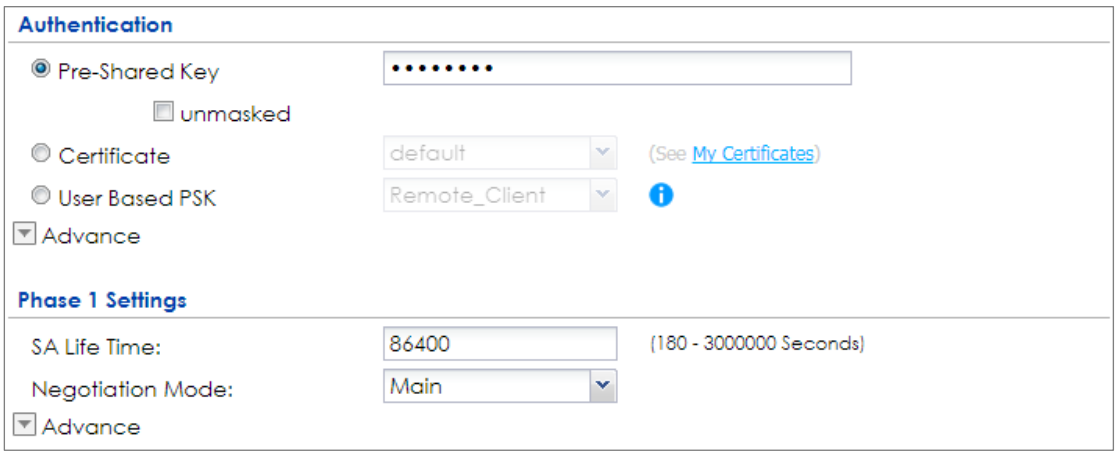
Spoke_Branch_A

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**.

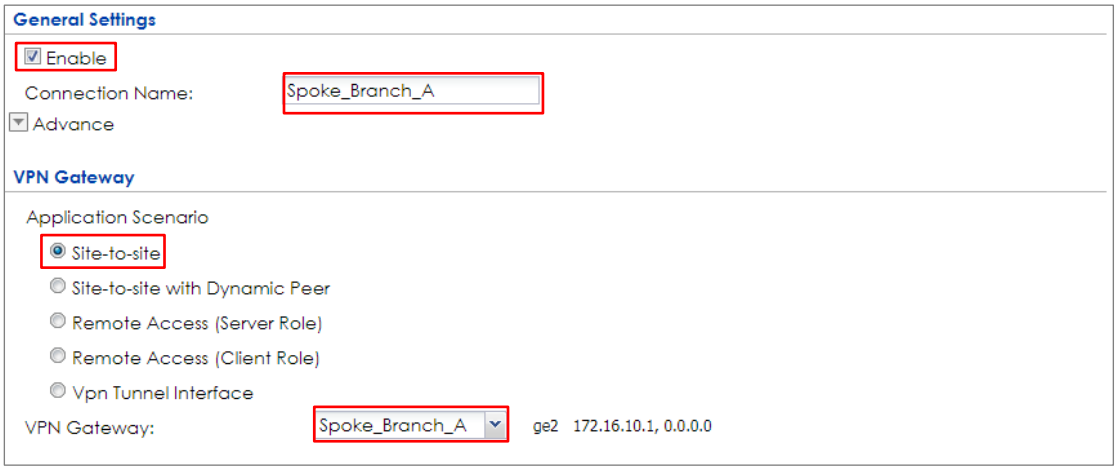
CONFIGURATION > VPN > IPSec VPN > VPN Gateway





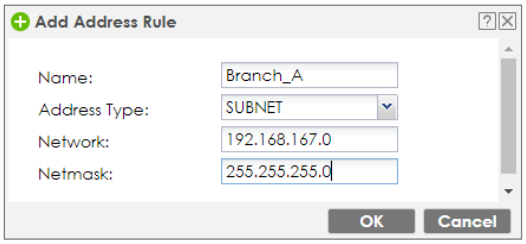
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

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

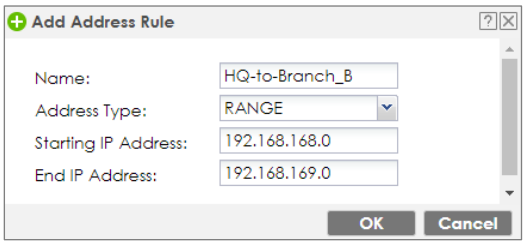


Click **Create new Object** on the upper bar to add the address of the local network behind **Branch A** and **the** address range of the local network behind **Hub_HQ** to **Branch_B**.

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

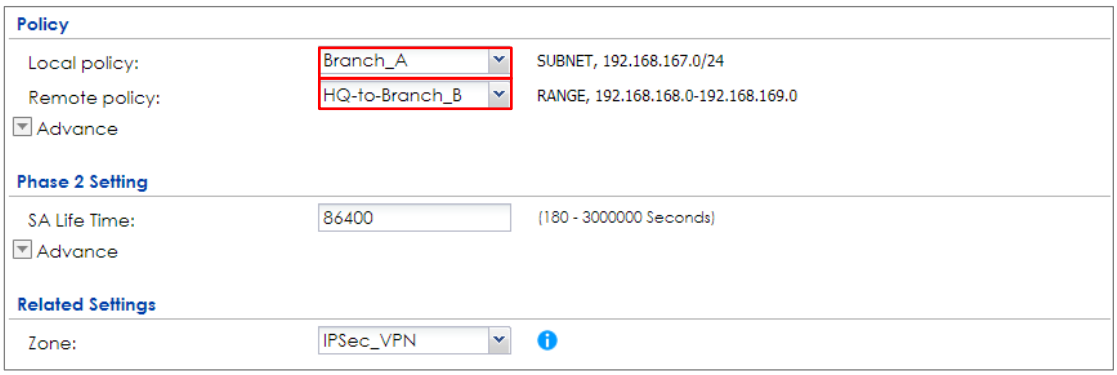


Remote Policy



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

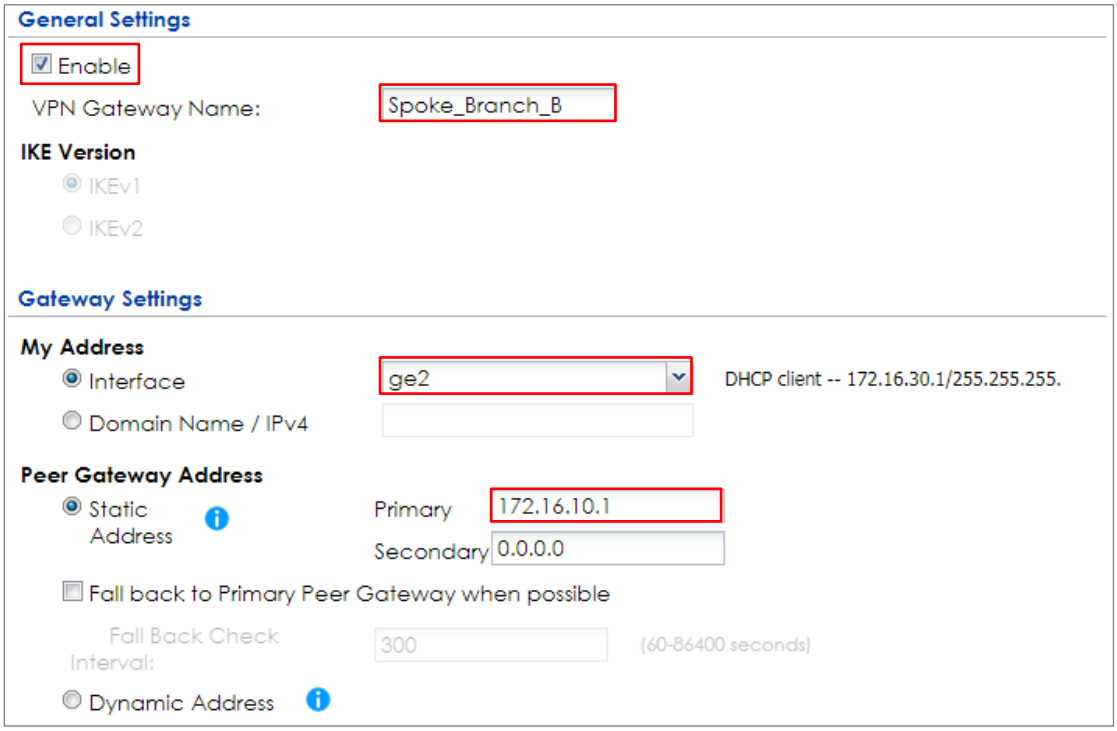


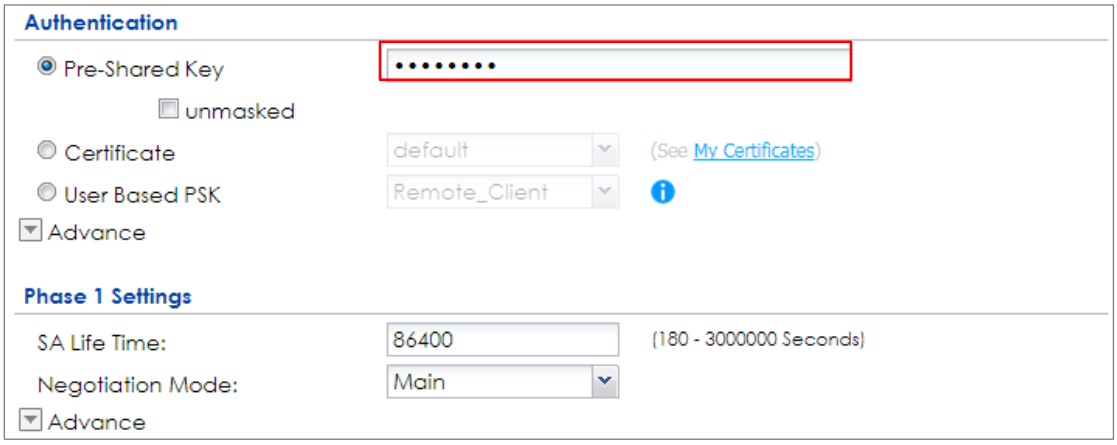
Spoke_Branch_B

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**.

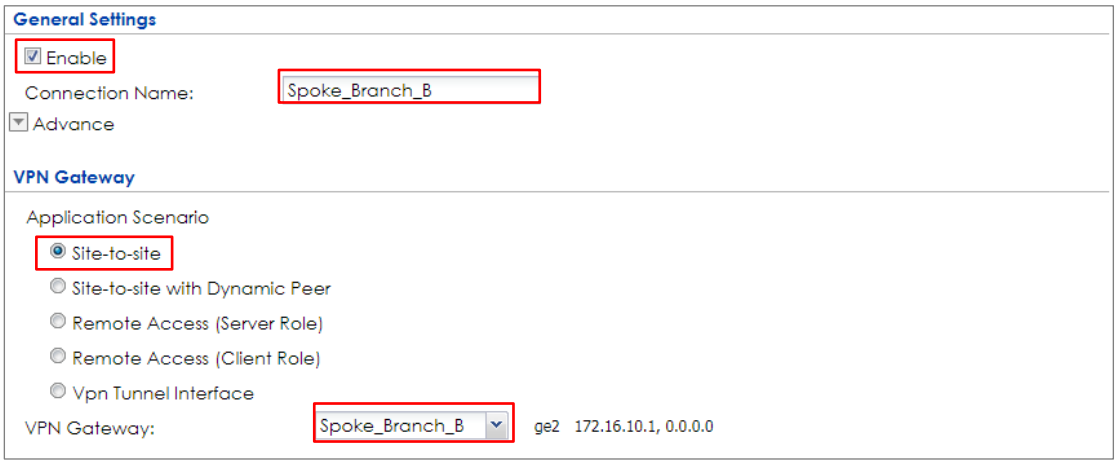
CONFIGURATION > VPN > IPSec VPN > VPN Gateway





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.

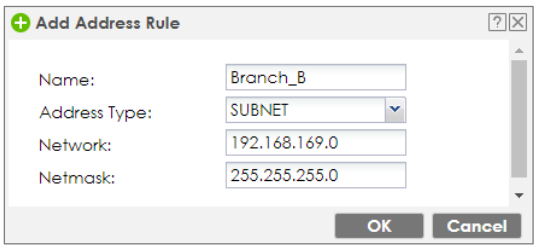
CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



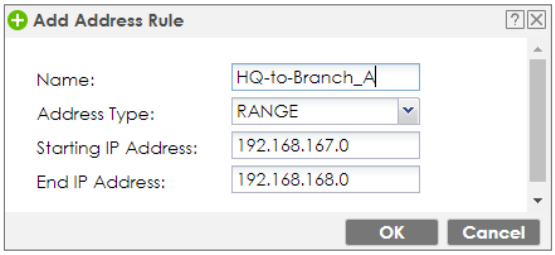
Click **Create new Object** on the upper bar to add the address of local network behind **Branch B** and address range of local network behind **Hub_HQ** to **Branch_A**.

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

Local Policy

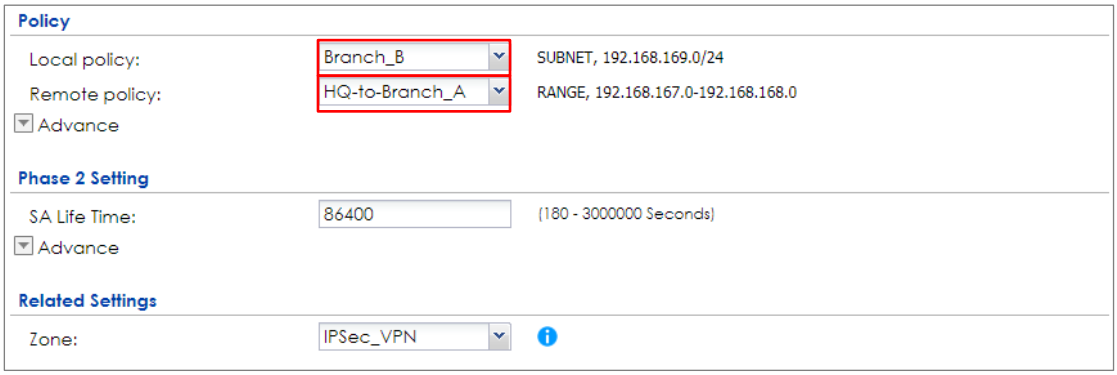


Remote Policy



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

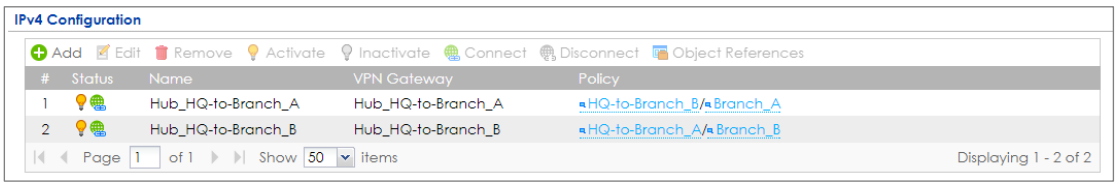
CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



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

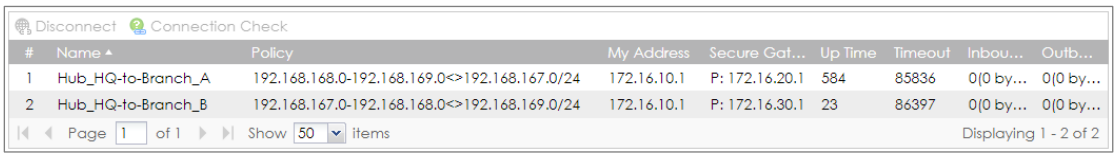


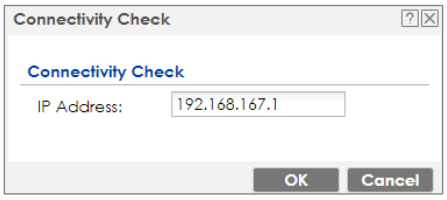
Spoke_Branch_A > CONFIGURATION > VPN > IPSec VPN > VPN Connection

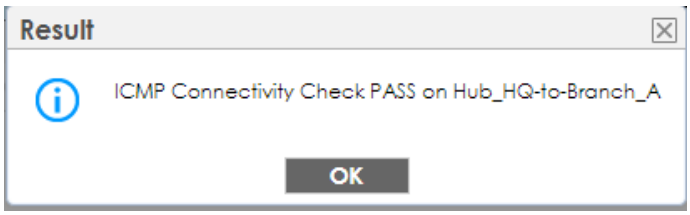
Spoke_Branch_B > CONFIGURATION > VPN > IPSec VPN > VPN Connection

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.

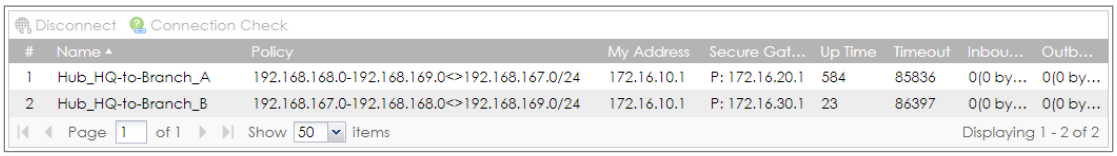
Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_A

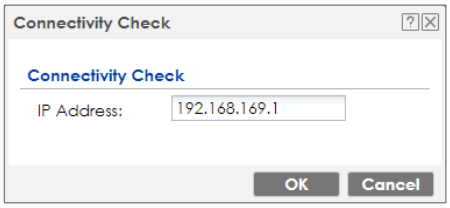


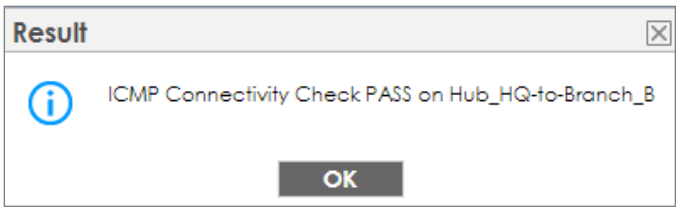




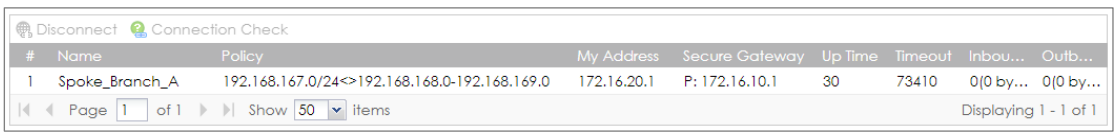
Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_B

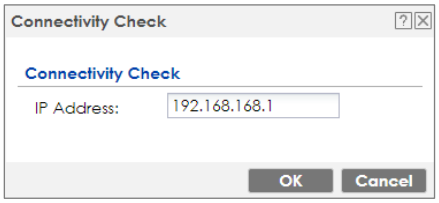


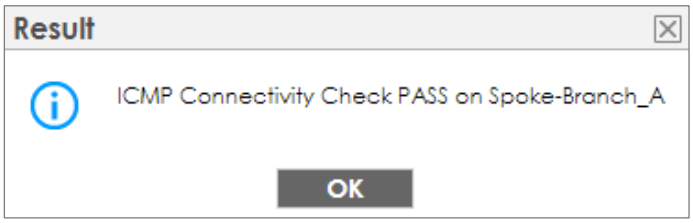




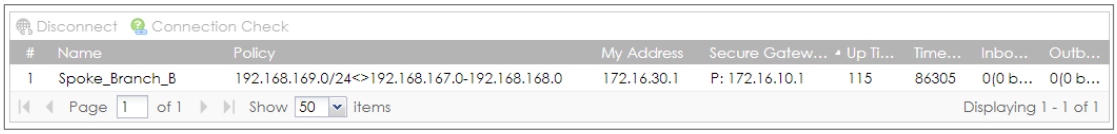
Spoke_Branch_A > MONITOR > VPN Monitor > IPSec

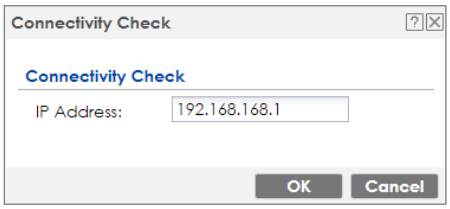


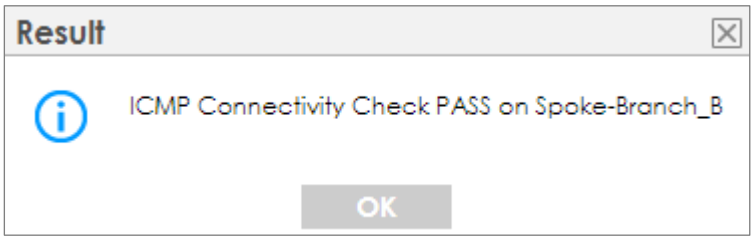




Spoke_Branch_B > MONITOR > VPN Monitor > IPSec







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

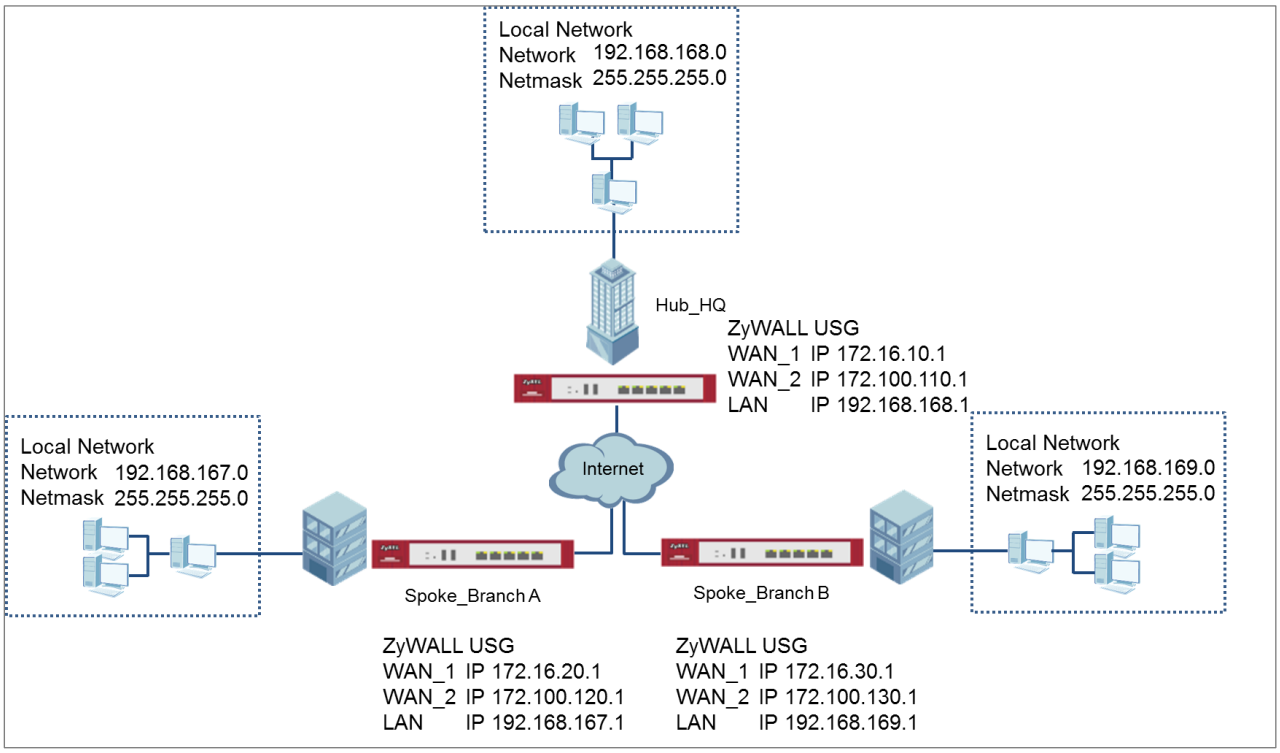
31	2017-09-11 ...	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

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).

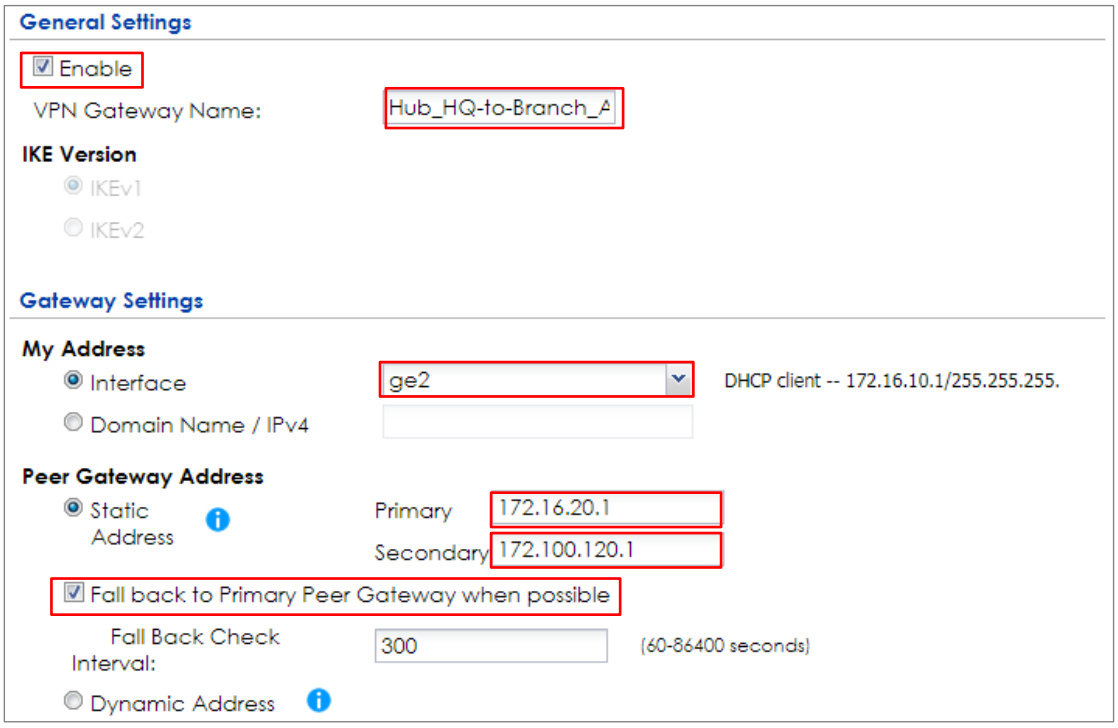
Set Up the IPSec VPN Tunnel on the ZyWALL/USG Hub_HQ-to-Branch_A

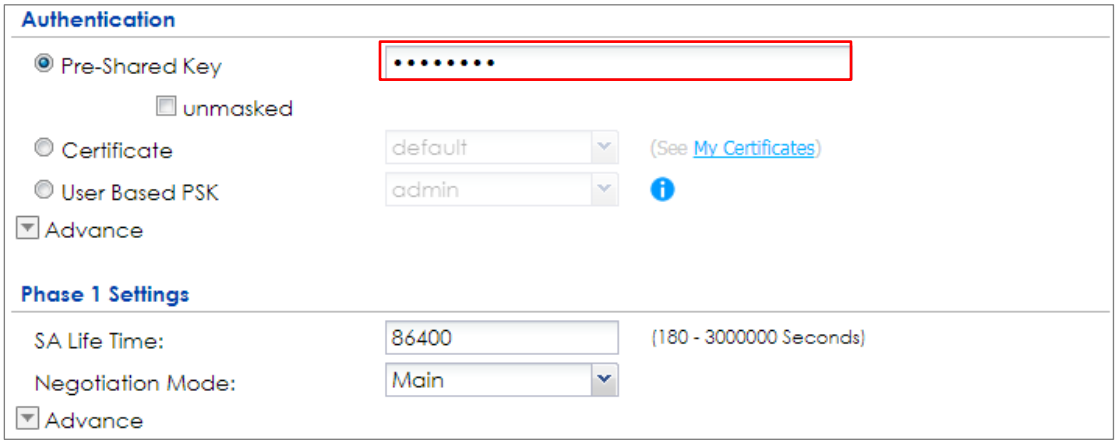
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

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





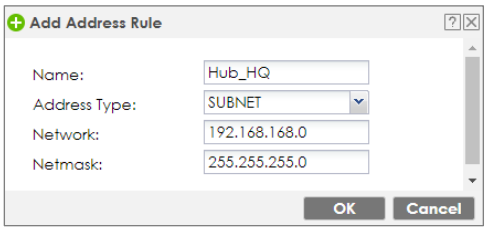
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

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

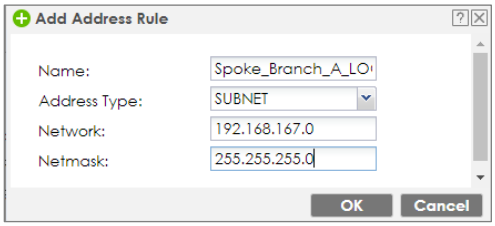
Click **Create new Object** to add the address of local network behind **Hub_HQ** and an address of local network behind **Branch A**.

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

Local Policy

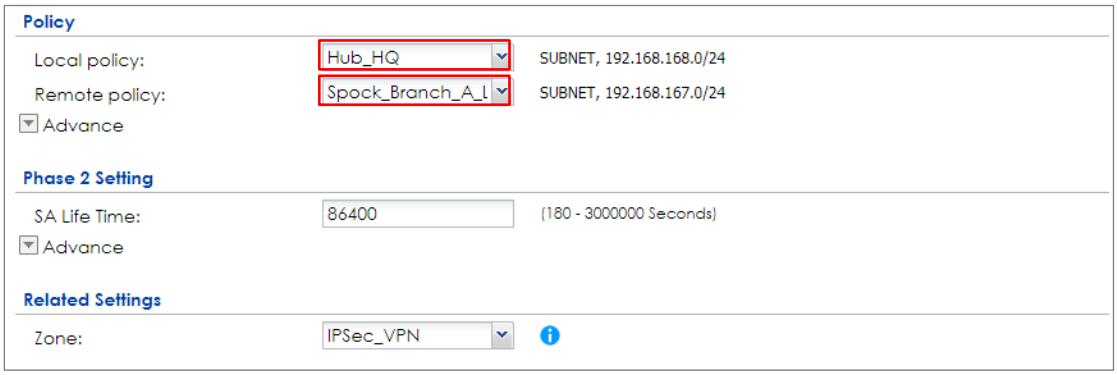


Remote Policy



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



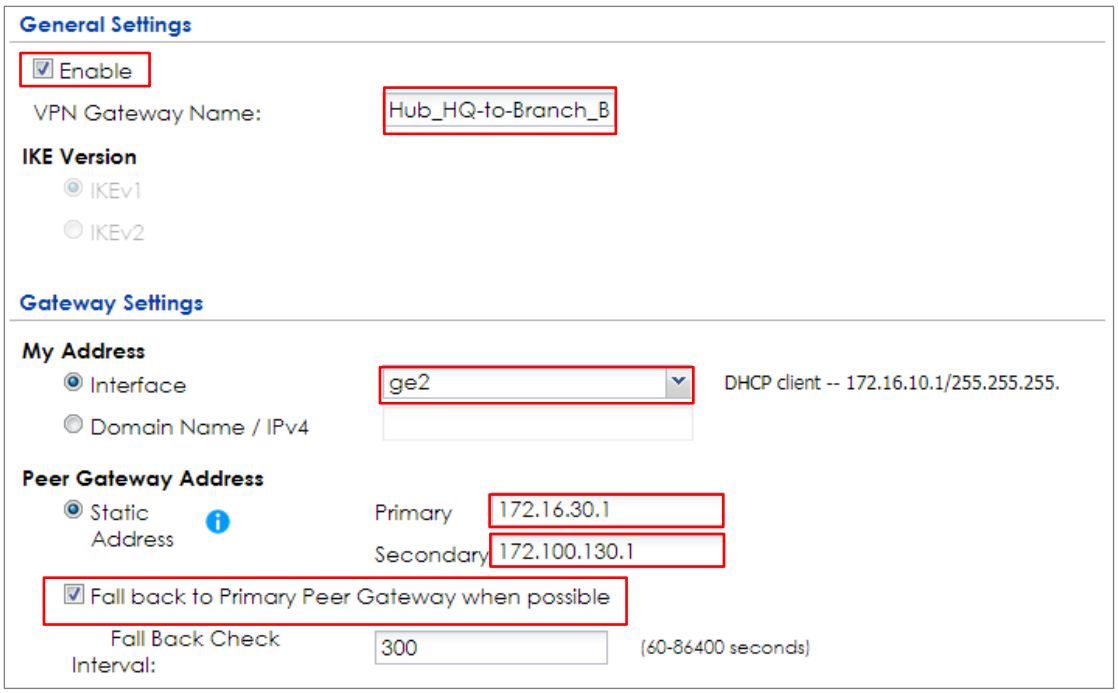
Hub_HQ-to-Branch_B

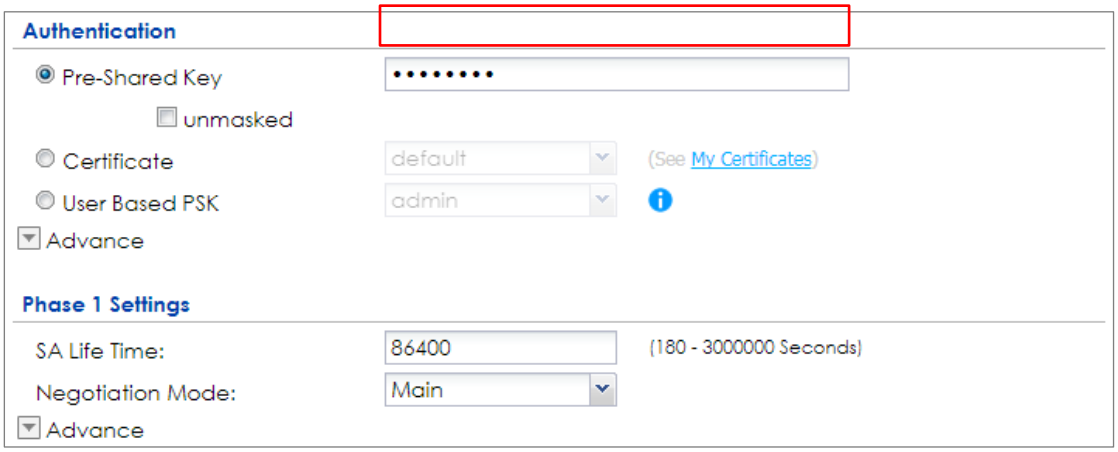
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

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**.

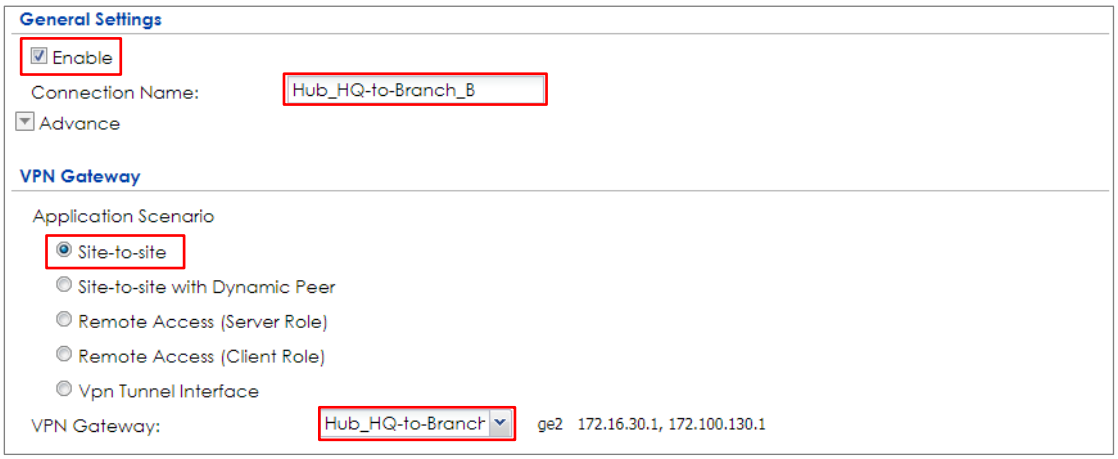
CONFIGURATION > VPN > IPSec VPN > VPN Gateway





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.

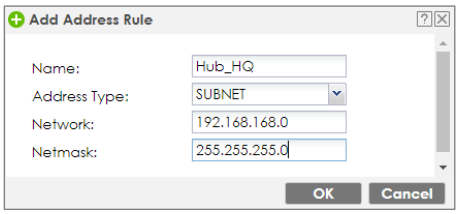
CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



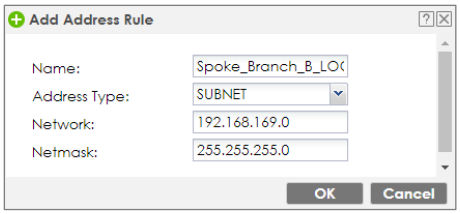
Click **Create new Object** to add an address of local network behind **Hub_HQ** and an address of local network behind **Branch B**.

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

Local Policy

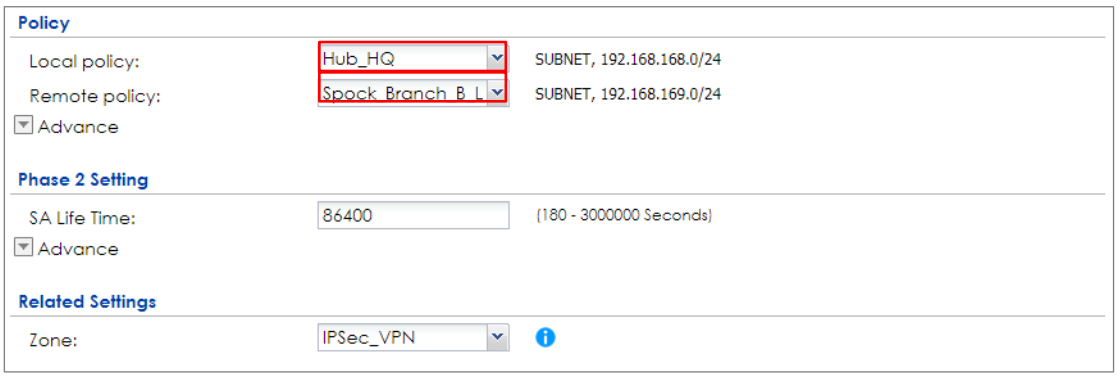


Remote Policy



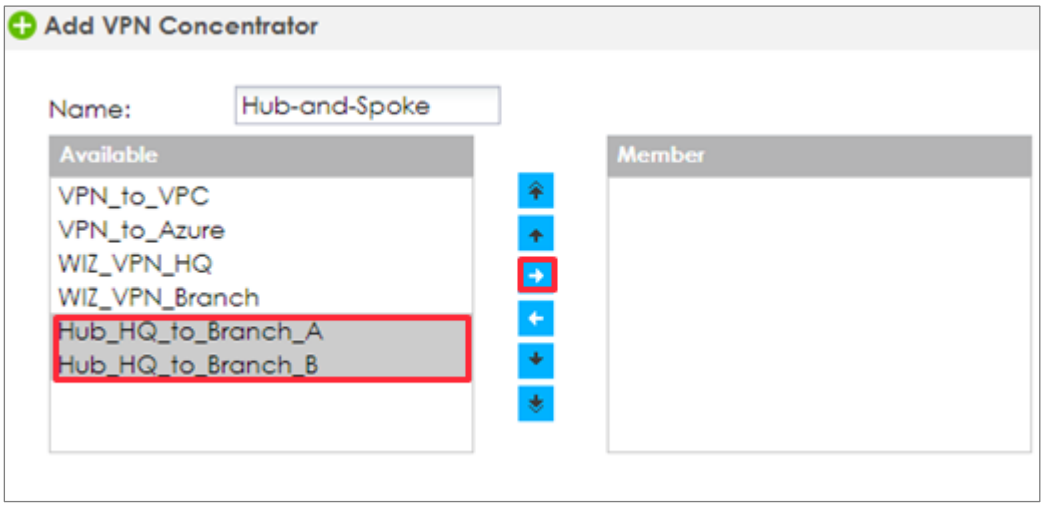
Set **Local Policy** to be **Hub_HQ** and **Remote Policy** to **Branch_B** which are newly created. Click **OK**.

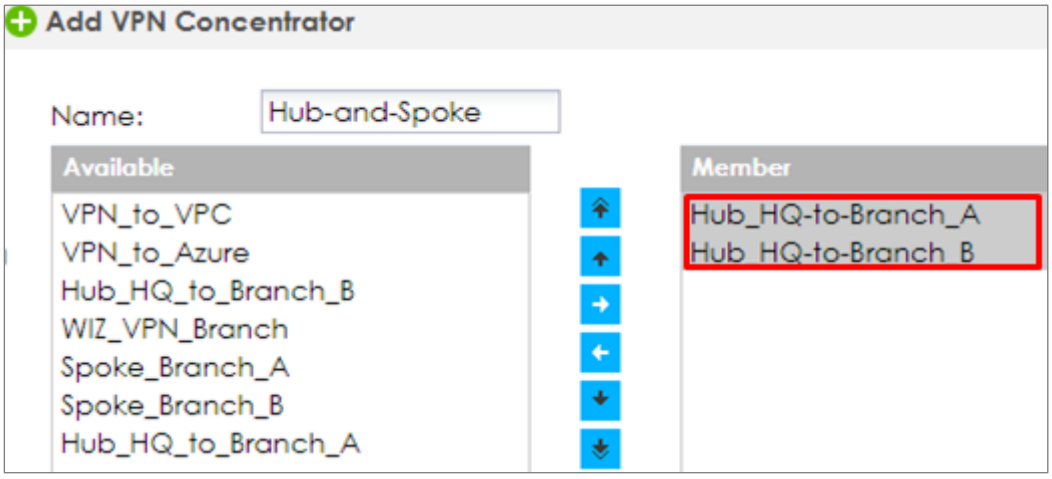
CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



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**.





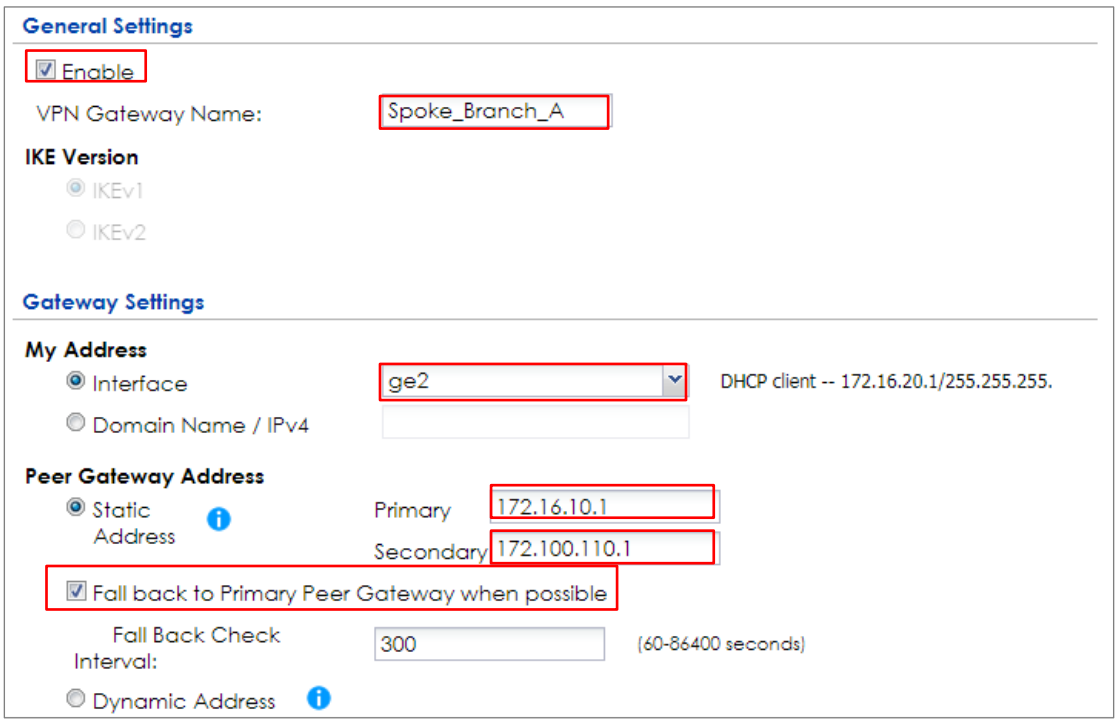
Spoke_Branch_A

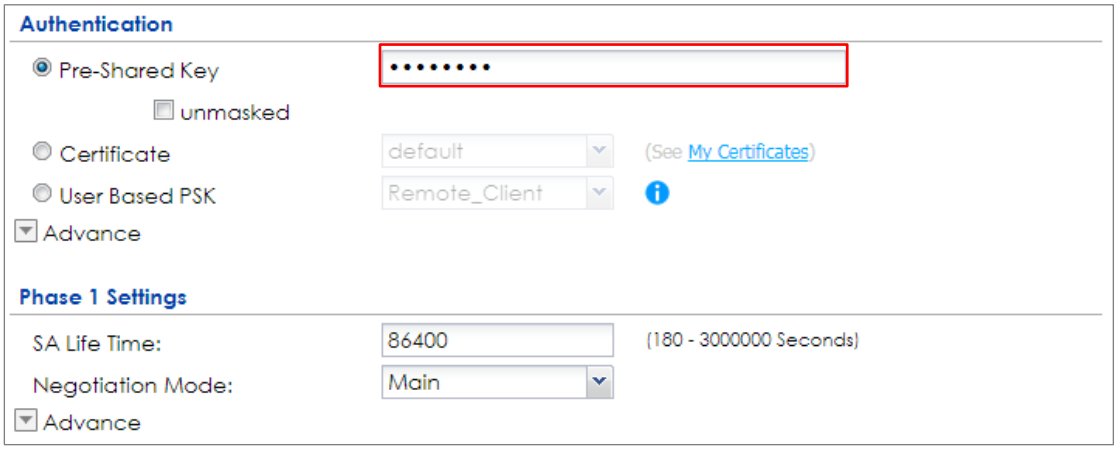
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, select **Enable**. Type the **VPN Gateway Name** used to identify this VPN gateway.

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





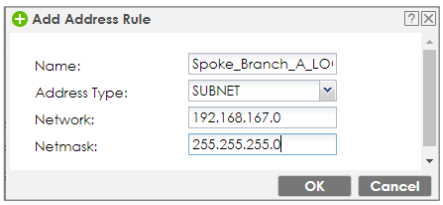
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**. Type the **Connection Name** used to identify this VPN connection. Select scenario as **Site-to-site** and VPN Gateway which is configured in Step 1.

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

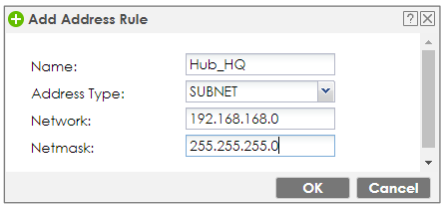
Click **Create new Object** to add the address of local network behind **Branch A** and an address of local network behind **Hub_HQ**

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

Local Policy

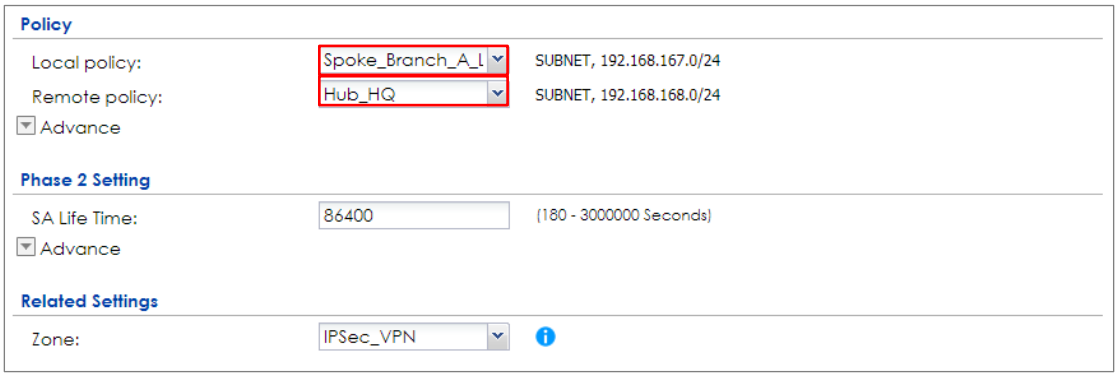


Remote Policy



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

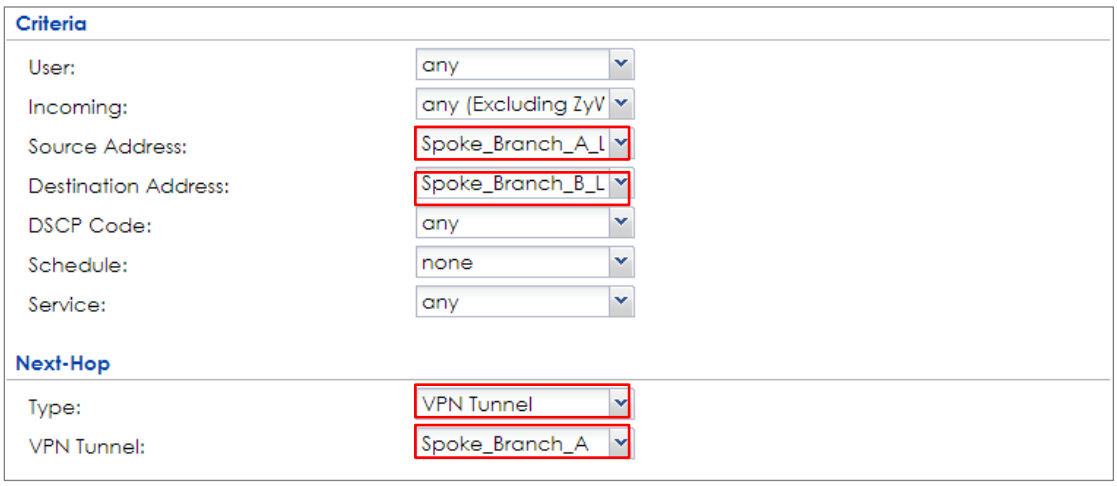
CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



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



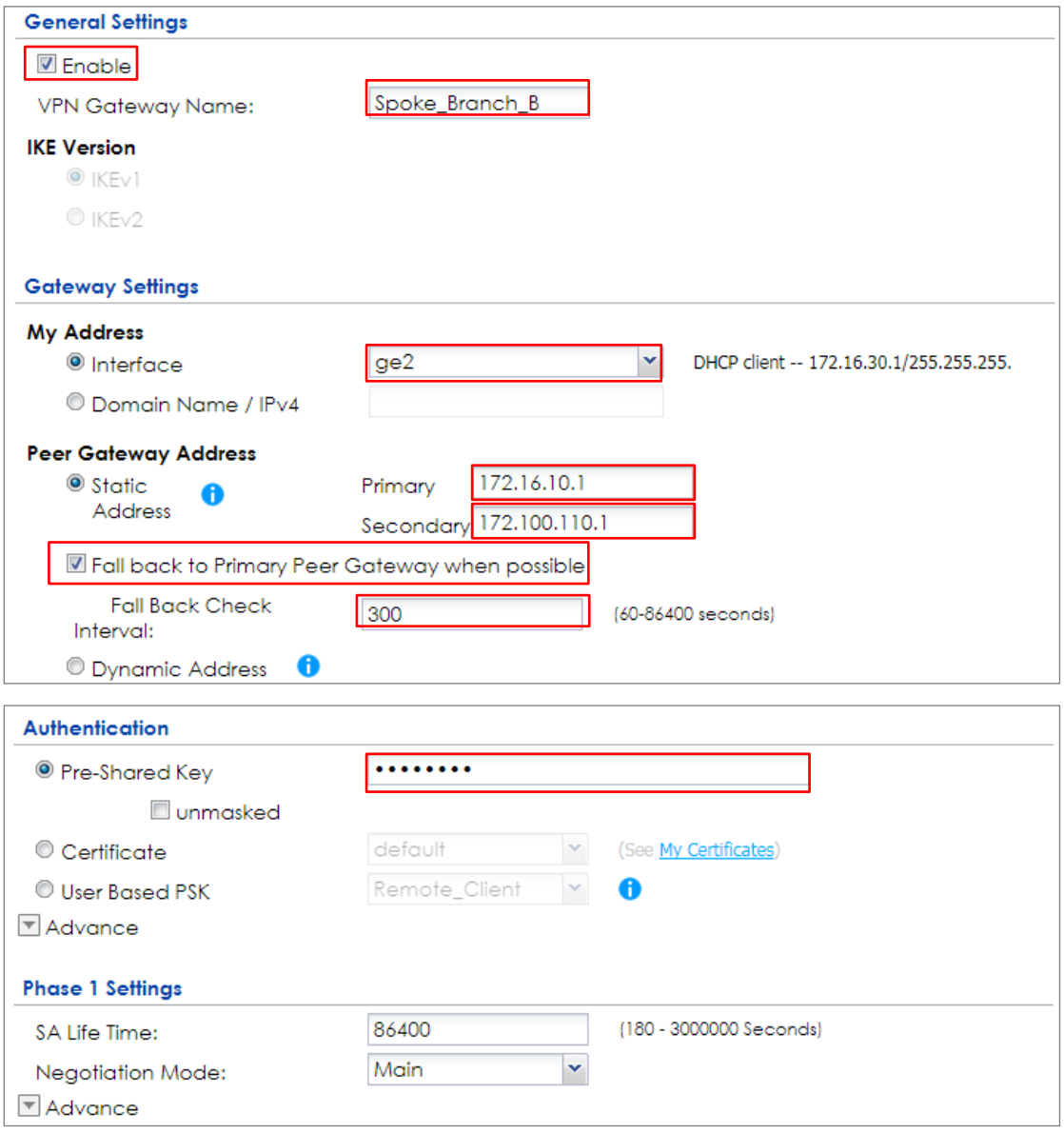
Spoke_Branch_B

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.

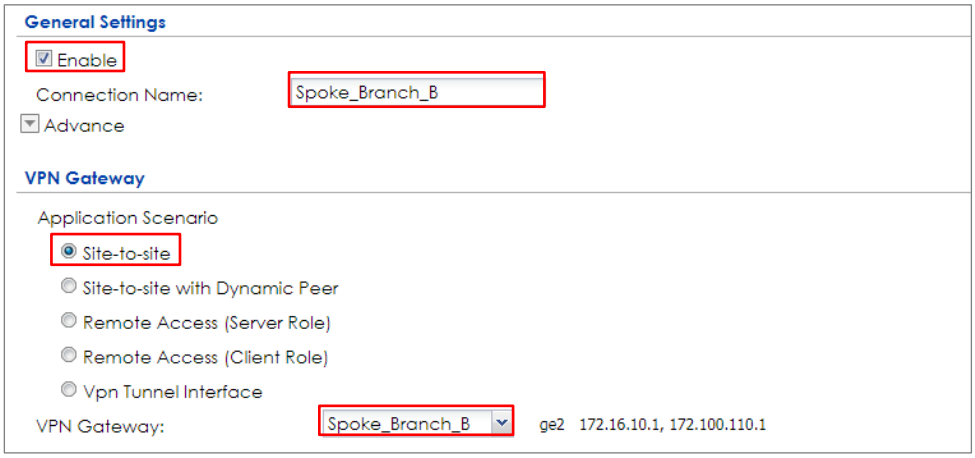
Type a secure **Pre-Shared Key** (8-32 characters) which must match your **Hub_HQ**'s Pre-Shared Key and click **OK**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway



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.

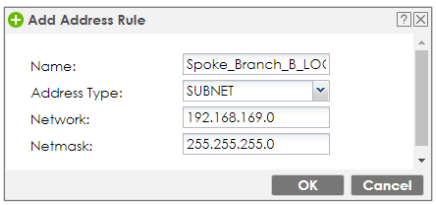
CONFIGURATION > VPN > IPSec VPN > VPN Connection > General Settings and VPN Gateway



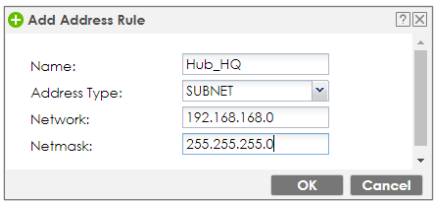
Click **Create new Object** to add the address of local network behind **Branch B** and an address of local network behind **Hub_HQ**.

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

Local Policy

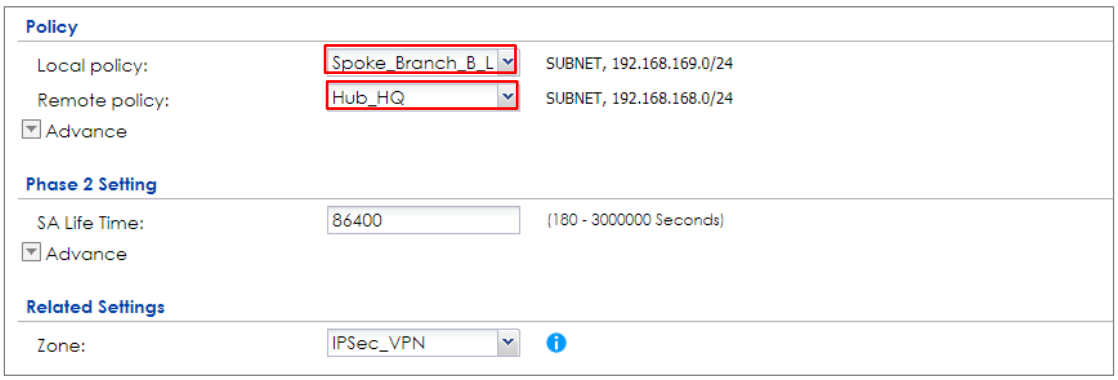


Remote Policy



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

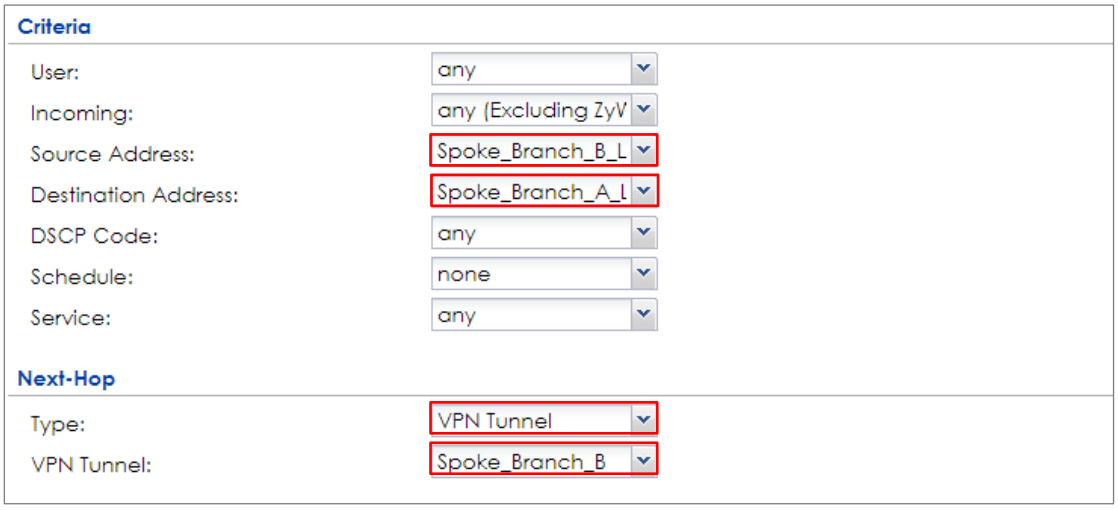
CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy



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**.

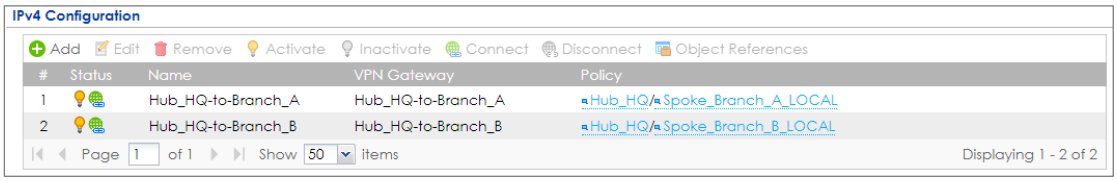
Network > Routing > Policy Route



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

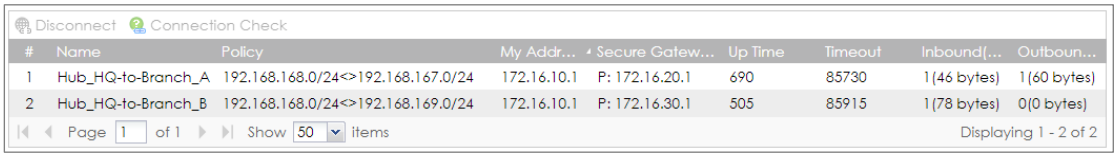


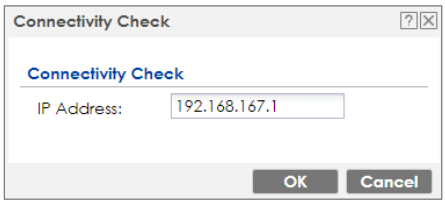
Spoke_Branch_A > CONFIGURATION > VPN > IPSec VPN > VPN Connection

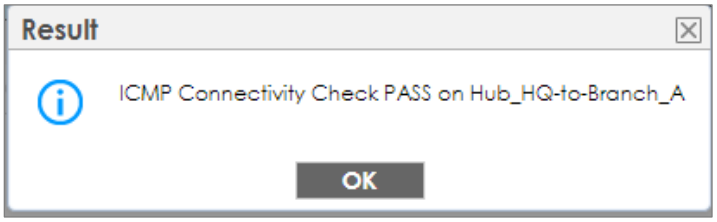
Spoke_Branch_B > CONFIGURATION > VPN > IPSec VPN > VPN Connection

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.

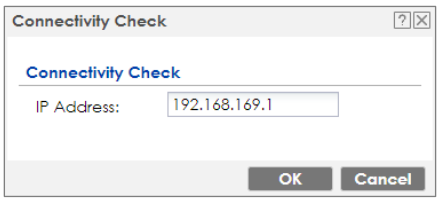
Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_A

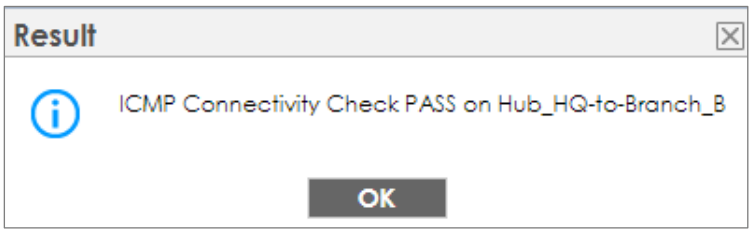




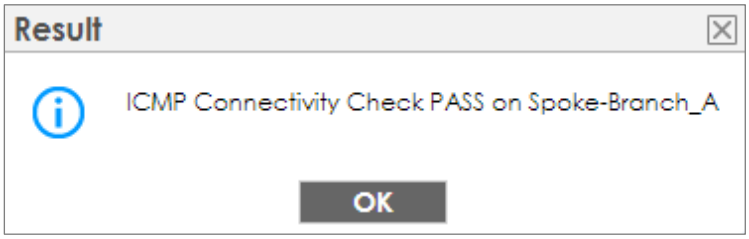


Hub_HQ > MONITOR > VPN Monitor > IPSec > Hub_HQ-to-Branch_B

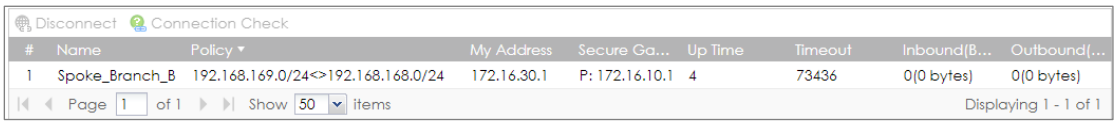


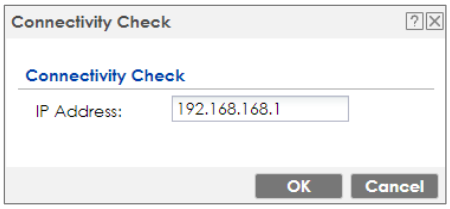


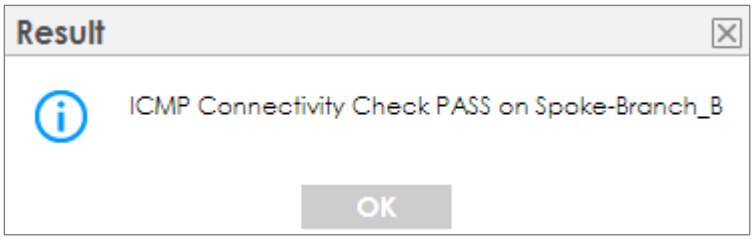
Spoke_Branch_A > MONITOR > VPN Monitor > IPSec



Spoke_Branch_B > MONITOR > VPN Monitor > IPSec







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

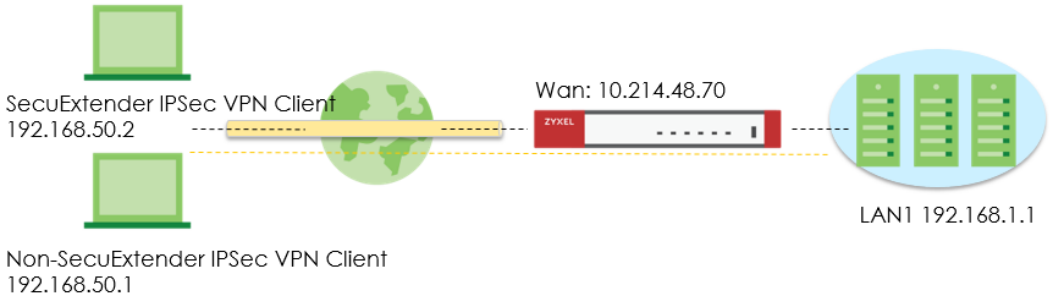
31	2017-09-11 ...	info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

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.

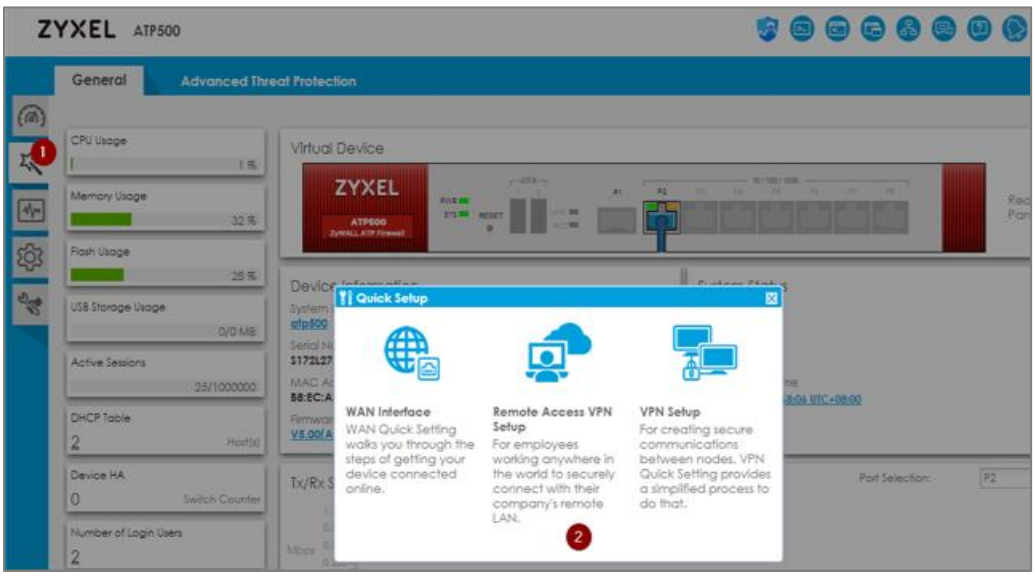
Remote Access VPN Wizard for SecuExtender IPSec and Non-SecuExtender IPSec VPN Clients

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.

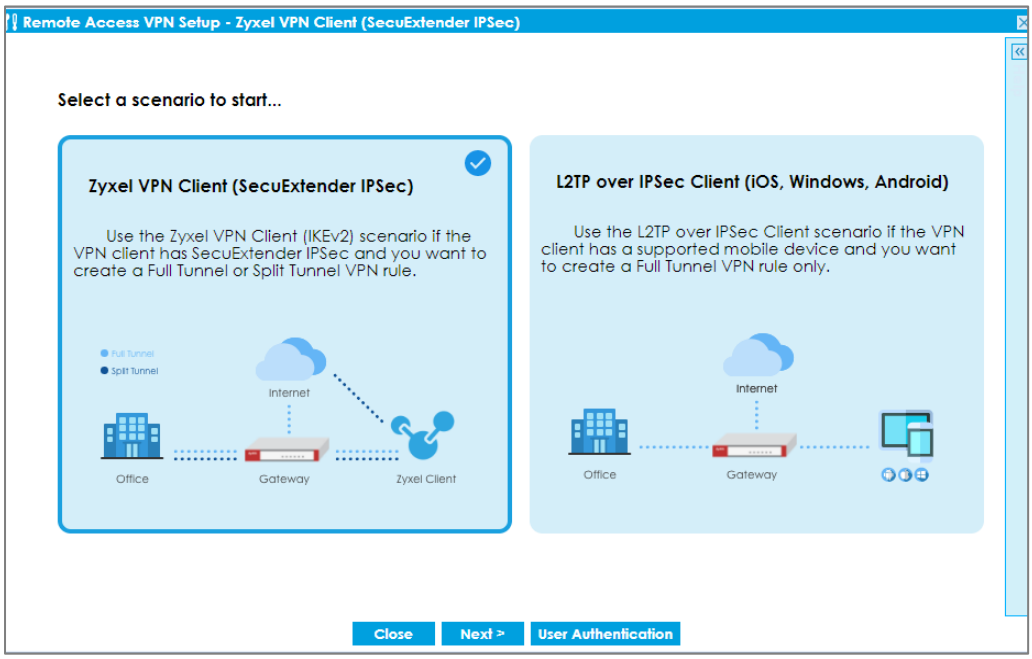


Set up VPN Tunnel on ATP/USG FLEX

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.



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

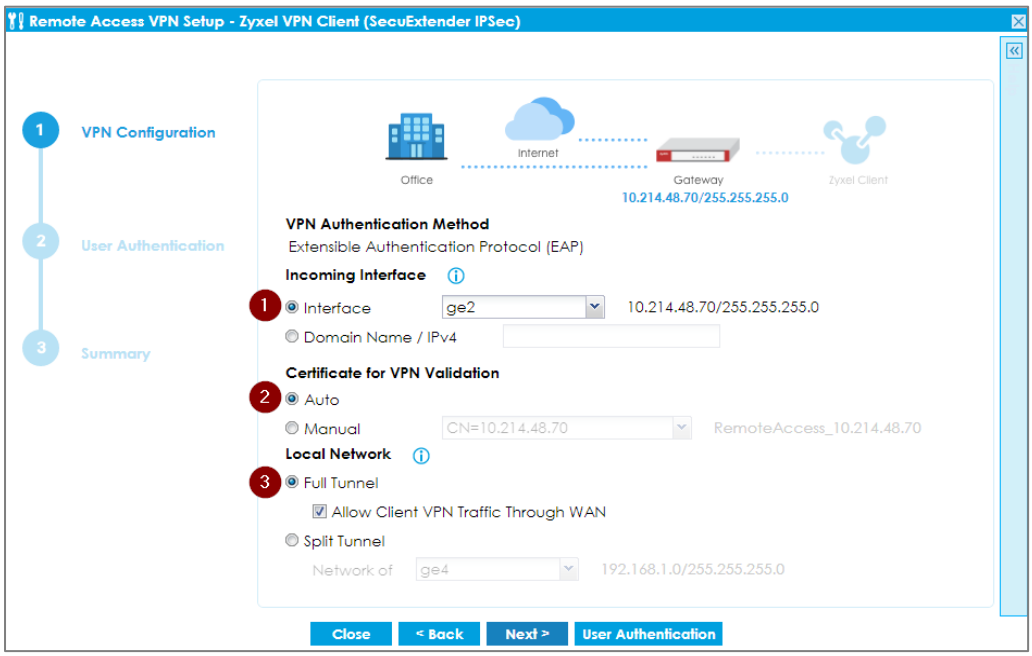


3.Configure the VPN Authentication Method

(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**.

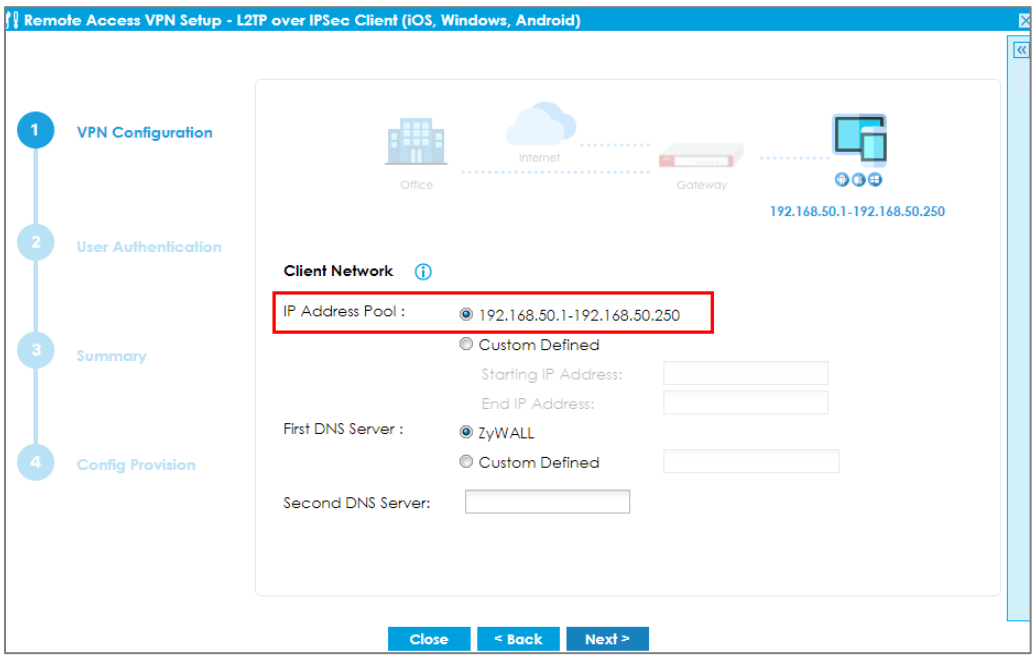


4.Configure the IP Address Pool for the client

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

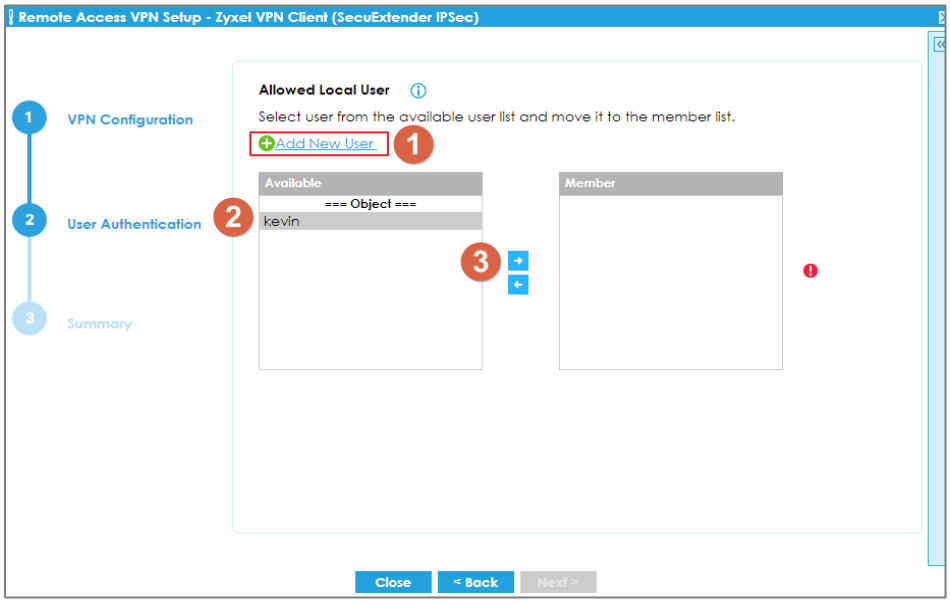
If the subnet 192.168.50.1 exists in the gateway settings, the IP address pool will automatically change to 192.168.51.1 subnet.

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



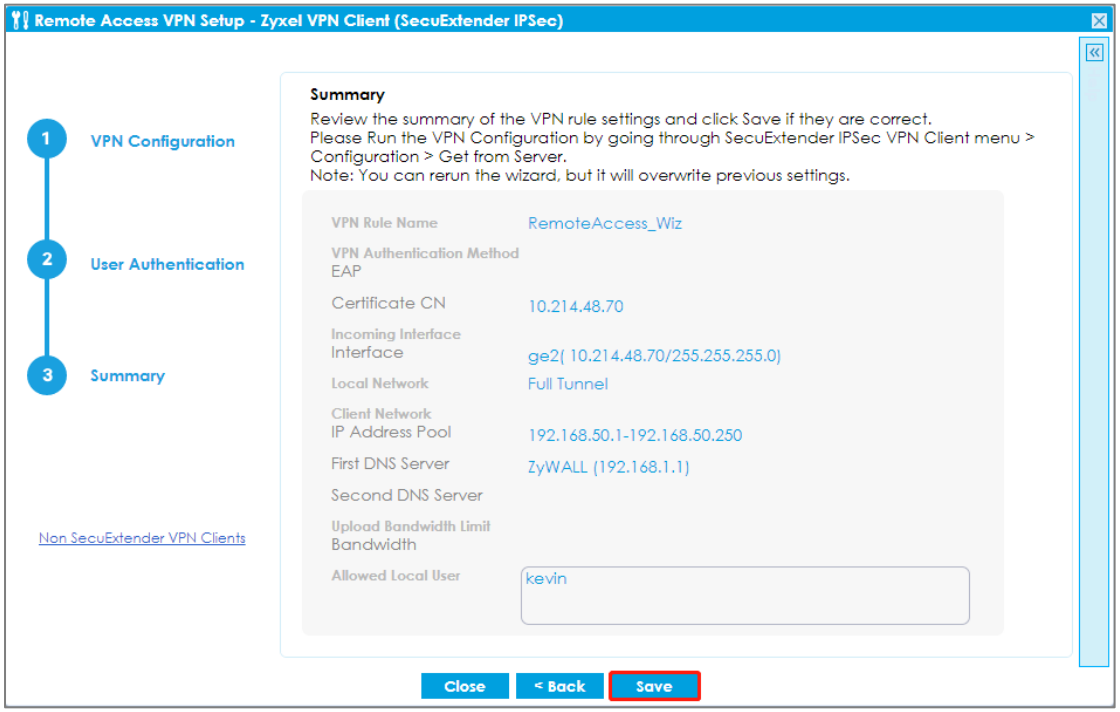
5. Allow local user to access the device via VPN tunnel

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.

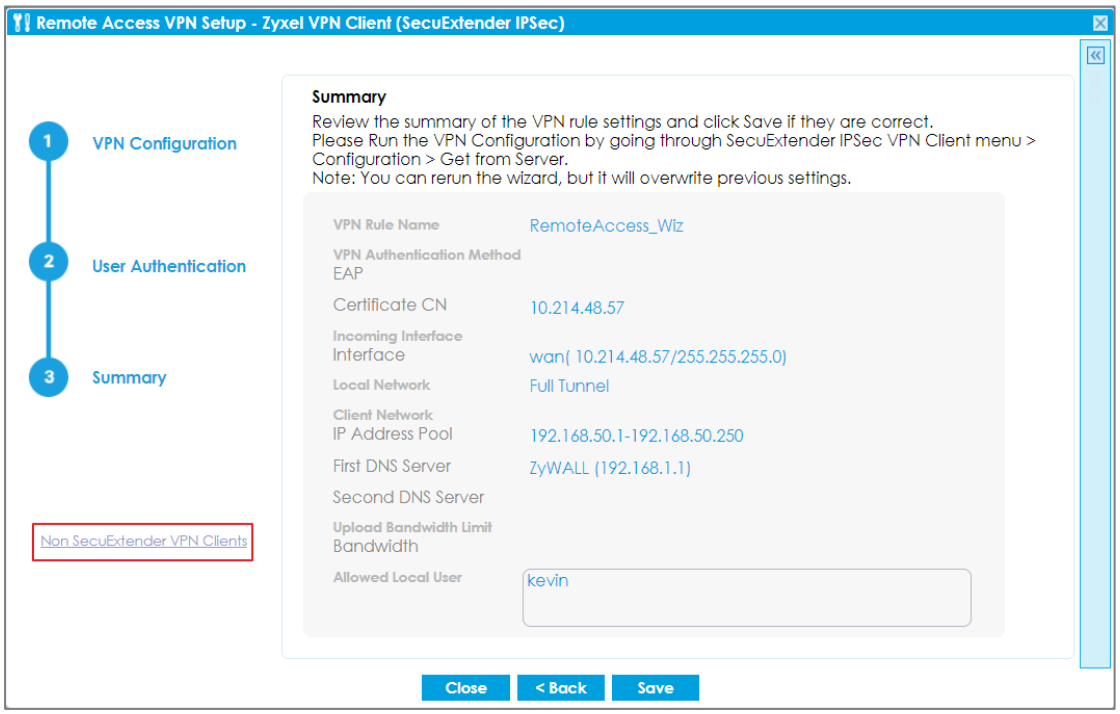


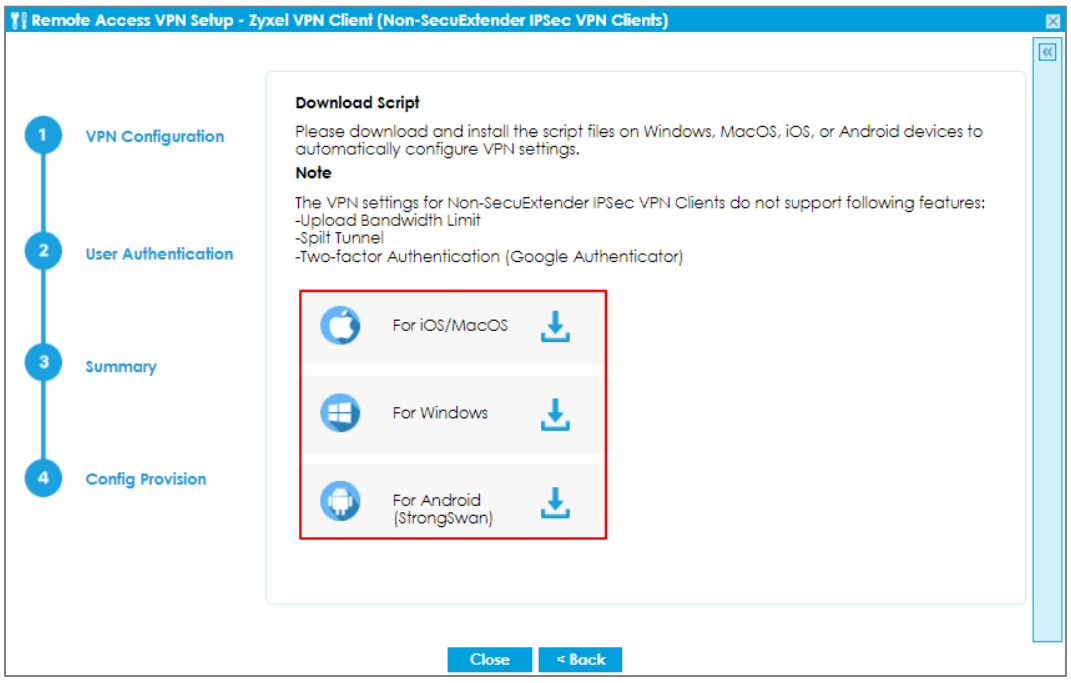
6. After done all the steps in the wizard, you can choose using either SecuExtender IPSec or non- SecuExtender IPSec VPN clients (iOS/MacOS, Windows, Strongswan-Android) to provision the VPN settings

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



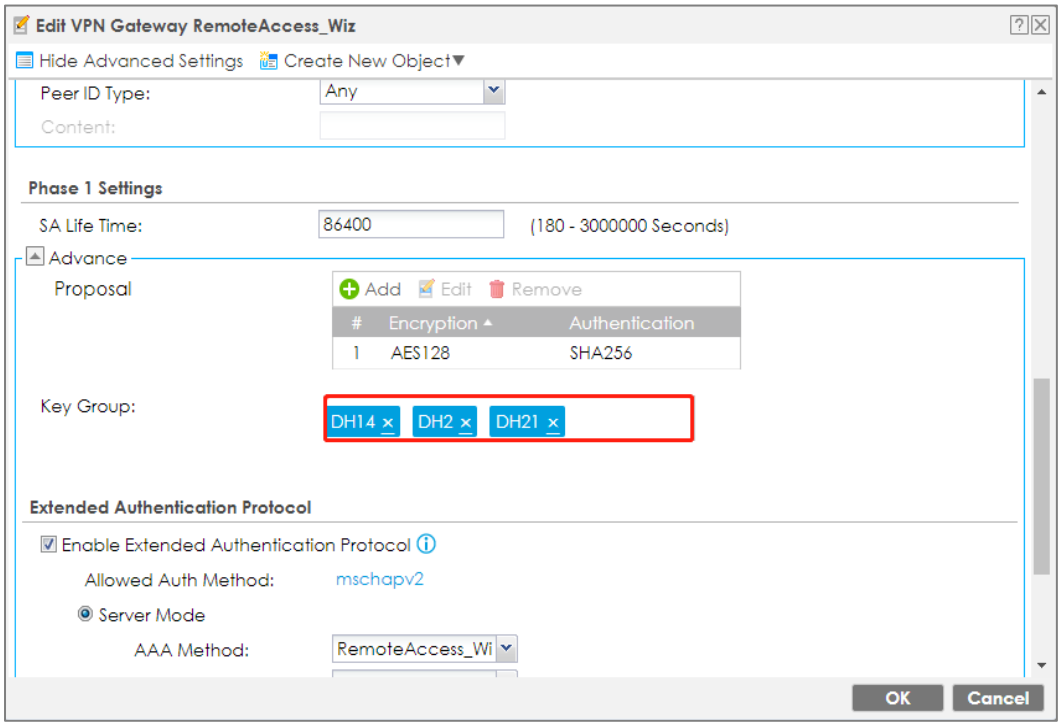
- Non-SecuExtender IPSec VPN client: Click to Non-SecuExtender VPN Client at the left hand side, then choose which device's operating system you want to download the script to install on.





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)

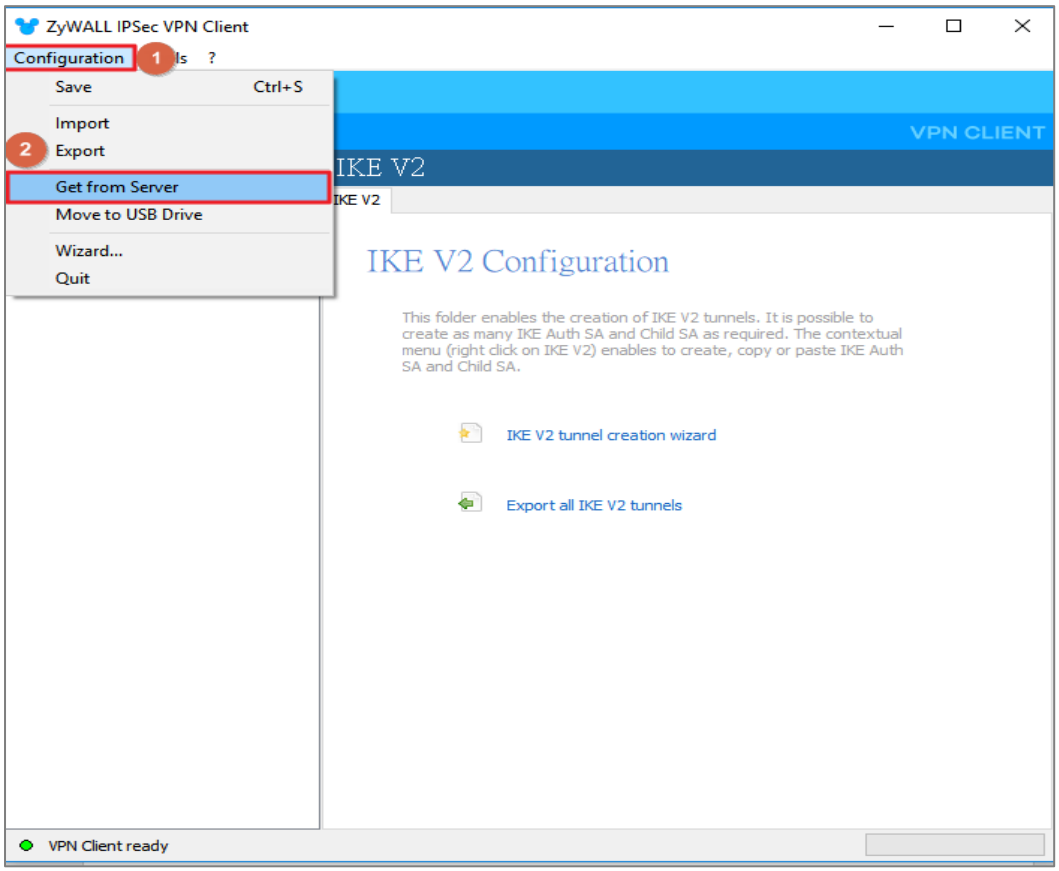


Note:
- IKEv2 Remote Access VPN using IKEv2 only supports single proposal (Authentication + Encryption)
- Remote Access VPN client using IKEv2 + EAP/MSCHAPv2 does not support using local-id to differentiate multiple rules. For multiple remote VPN rule, user must to choose different proposal (phase 2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

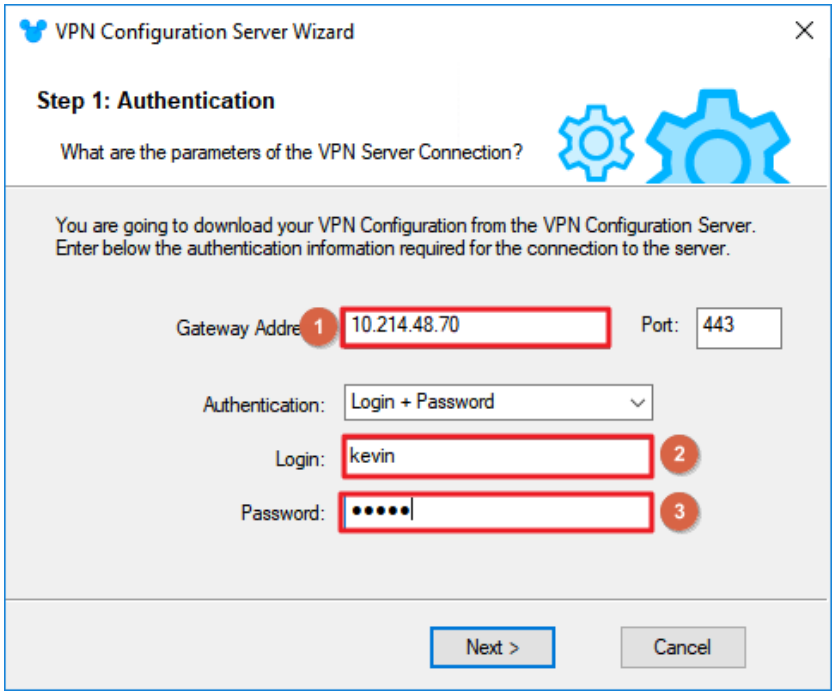
Test the result

For Windows SecuExtender IPSec VPN client:

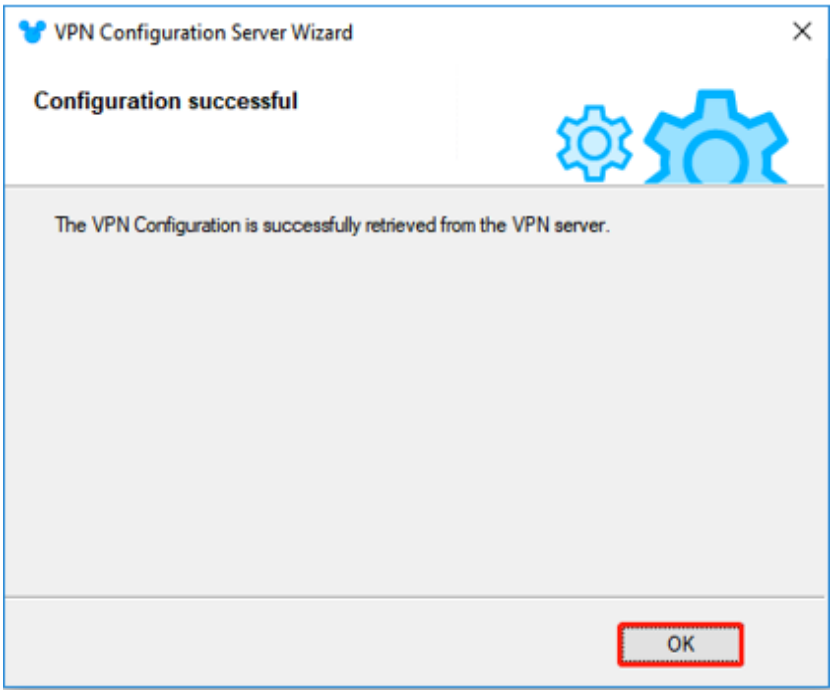
1. Go to Configuration tab, and click "Get from Server"



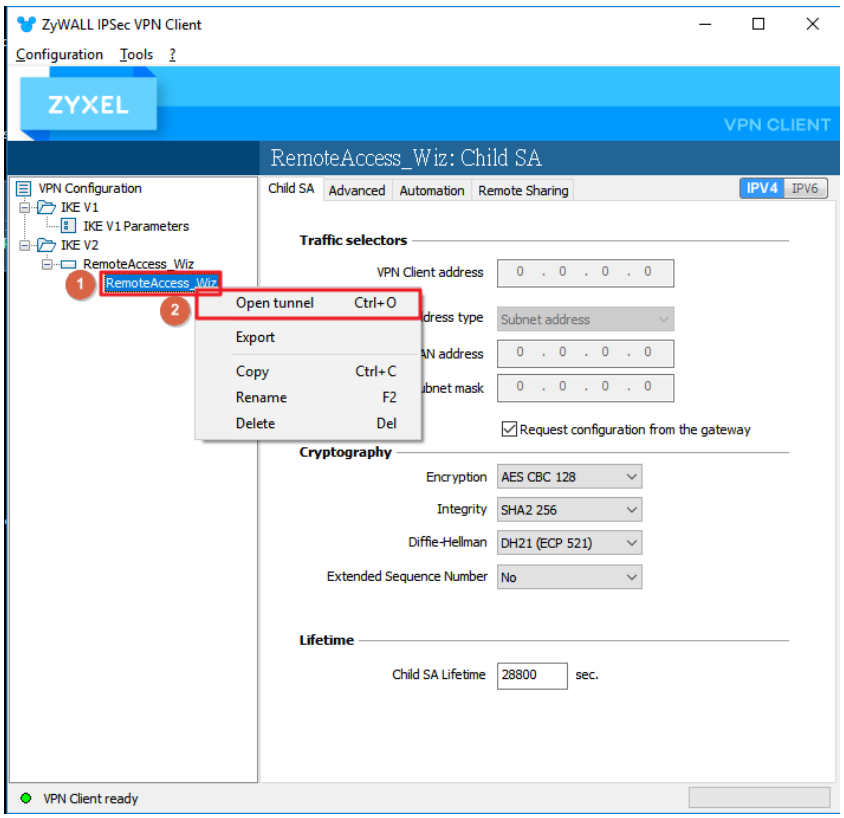
2. Enter gateway IP and credential to get provision file from gateway.



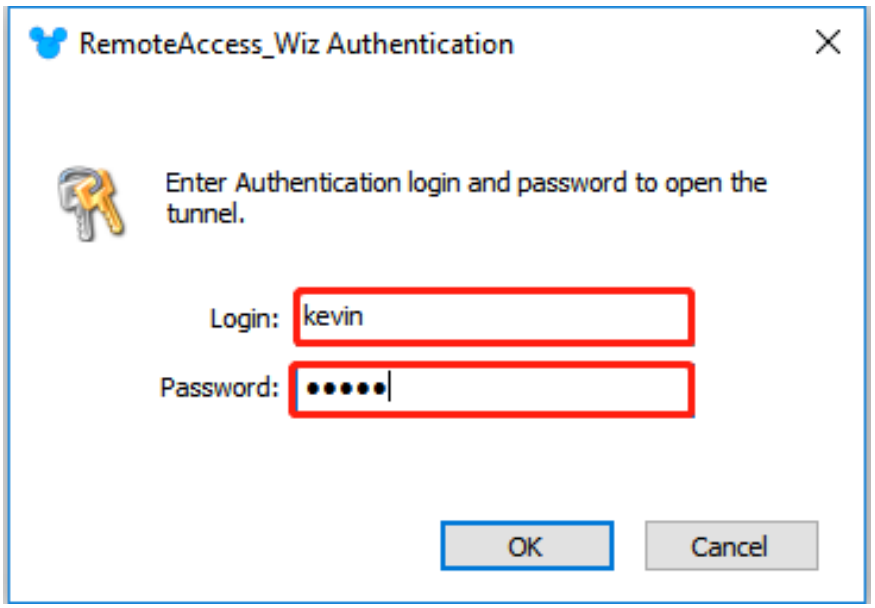
Click "OK" to finish.



3. Click "Open tunnel" to build up VPN connection.



Enter credential and click "OK".



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

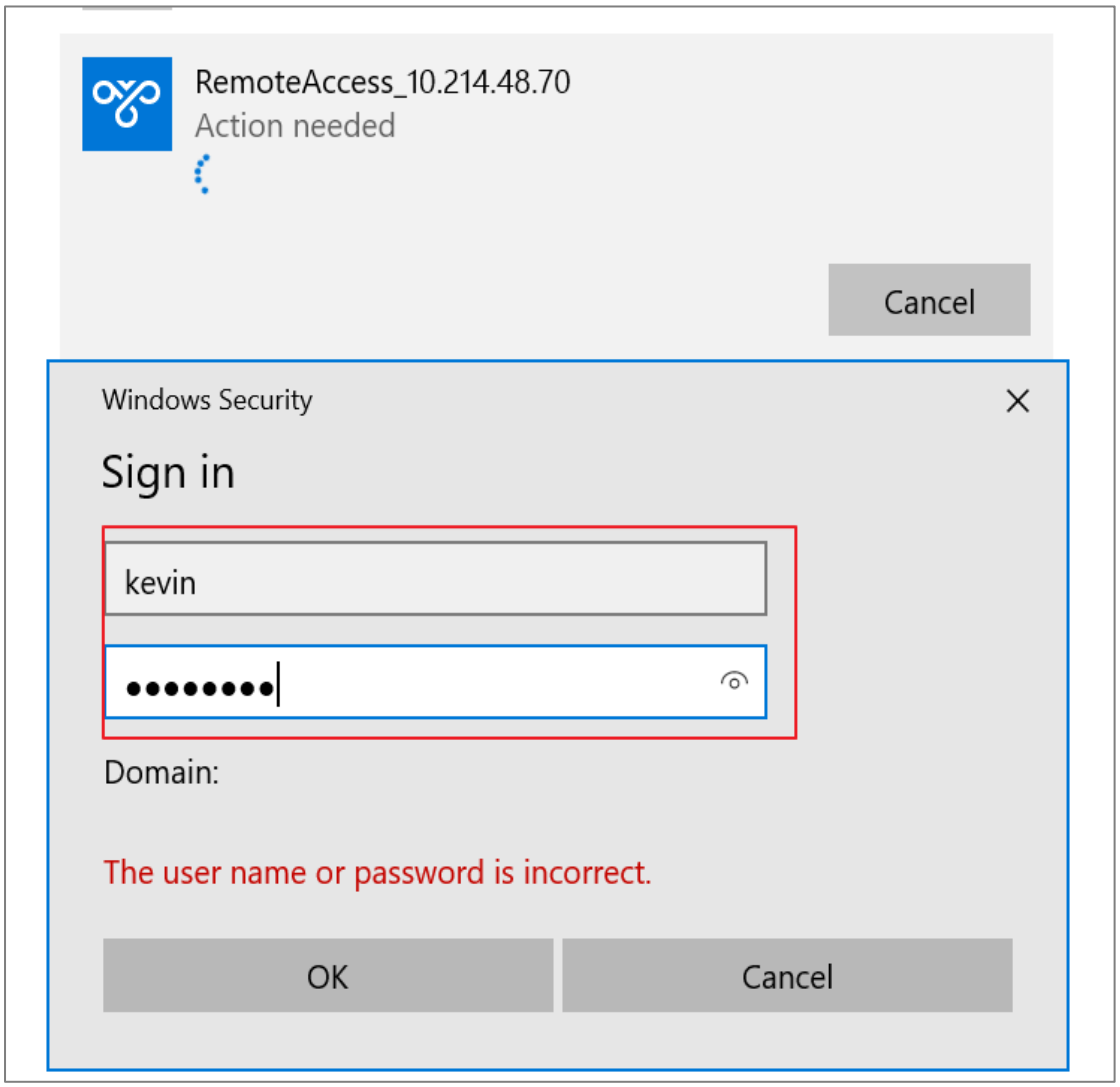
```
C:\Windows\system32>ping 192.168.1.1

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.

2. VPN for Native IKEV2 is created successfully.

3. Enter the VPN credential to complete the connection.

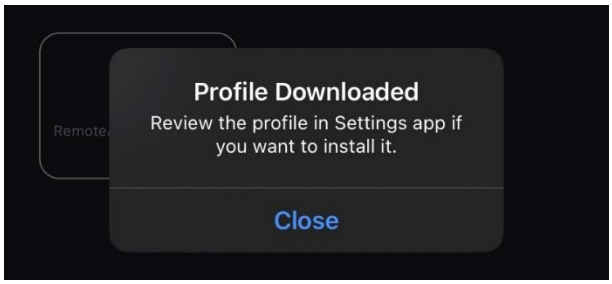


4. The remote user can ping the internal network now.

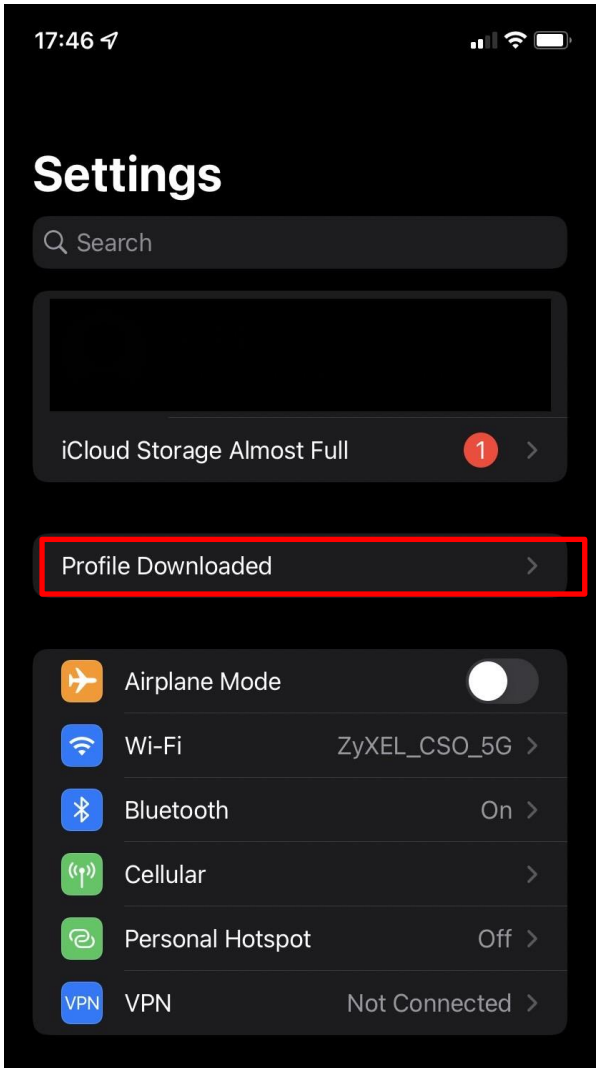
```
C:\Windows\system32>ping 192.168.1.1

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:

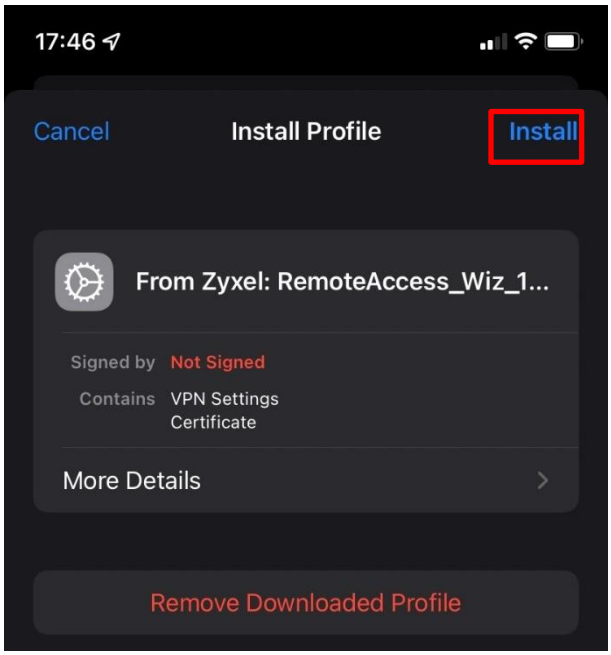
1.Send the Script to Device via email in example, then download the file



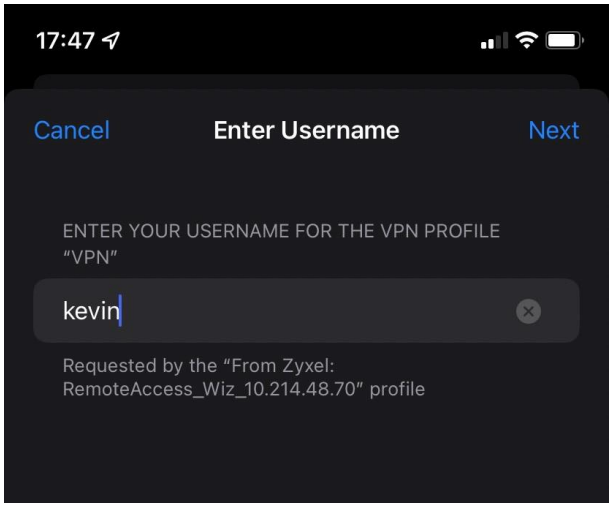
2.Settings->Profile Downloaded

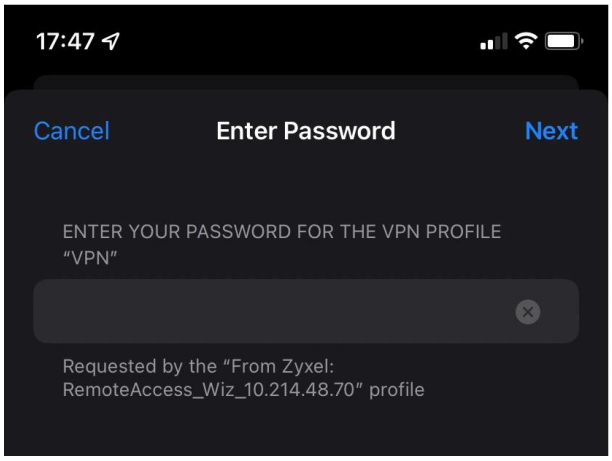


3.Press Install

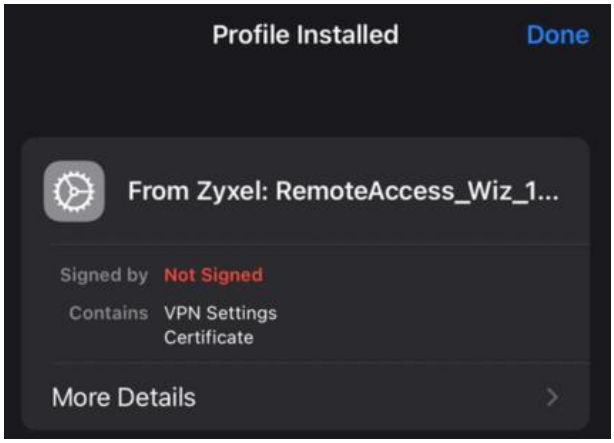


4.Enter Username and Password

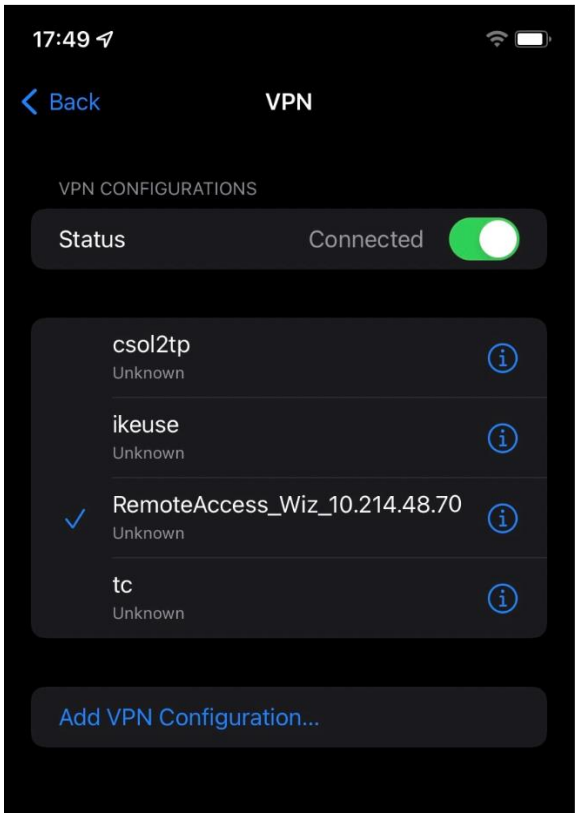


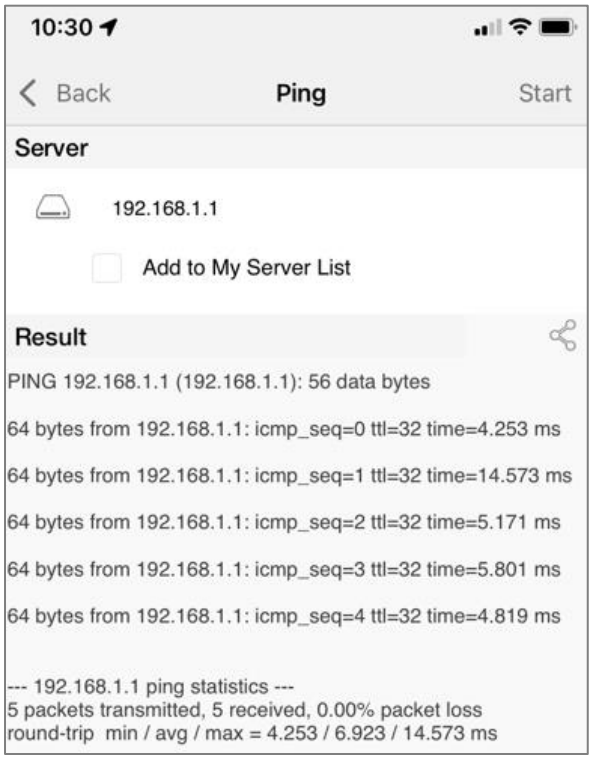


5.Profile Installed Done



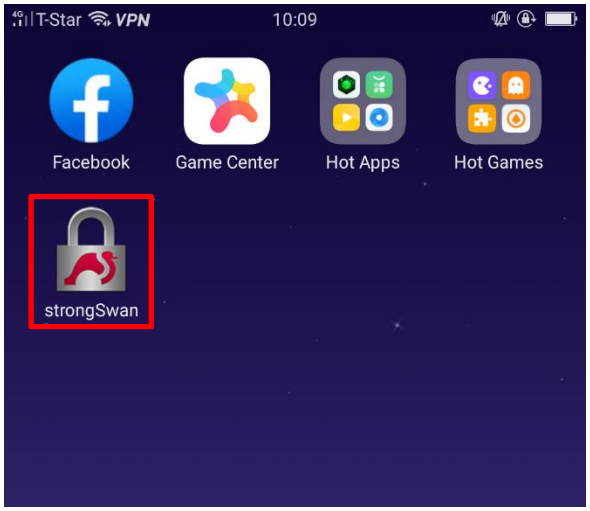
6.Now, it can connect



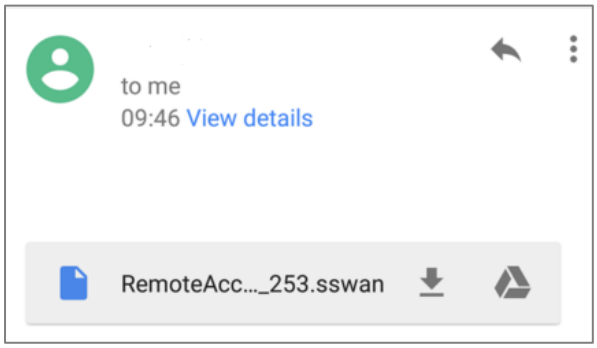


For Android:

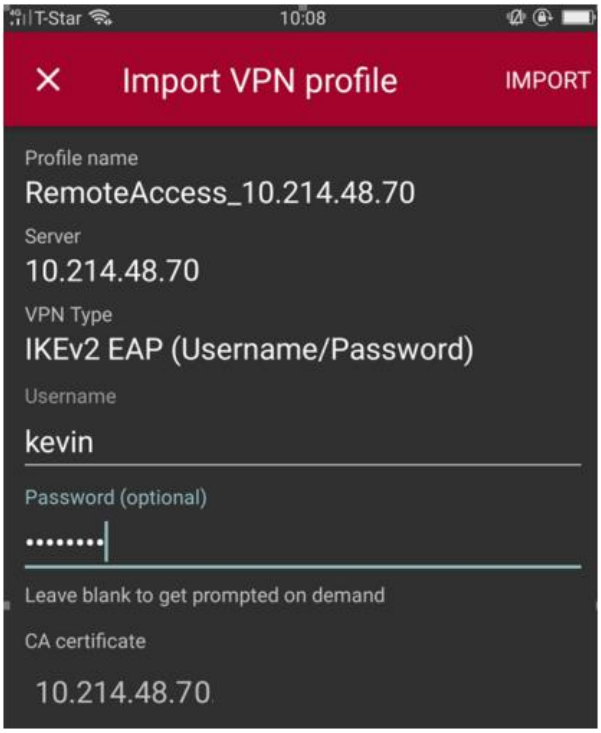
1.Download strongSwan from Google Play Store



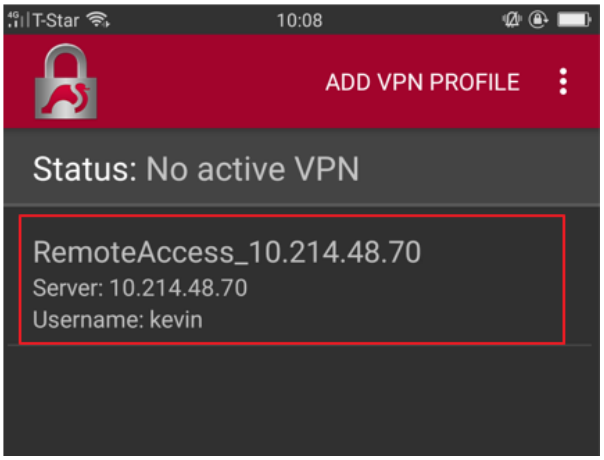
2.Send the Script to Device via email

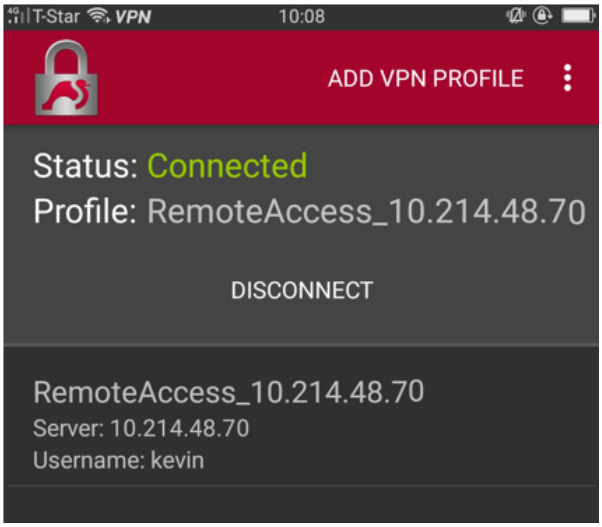


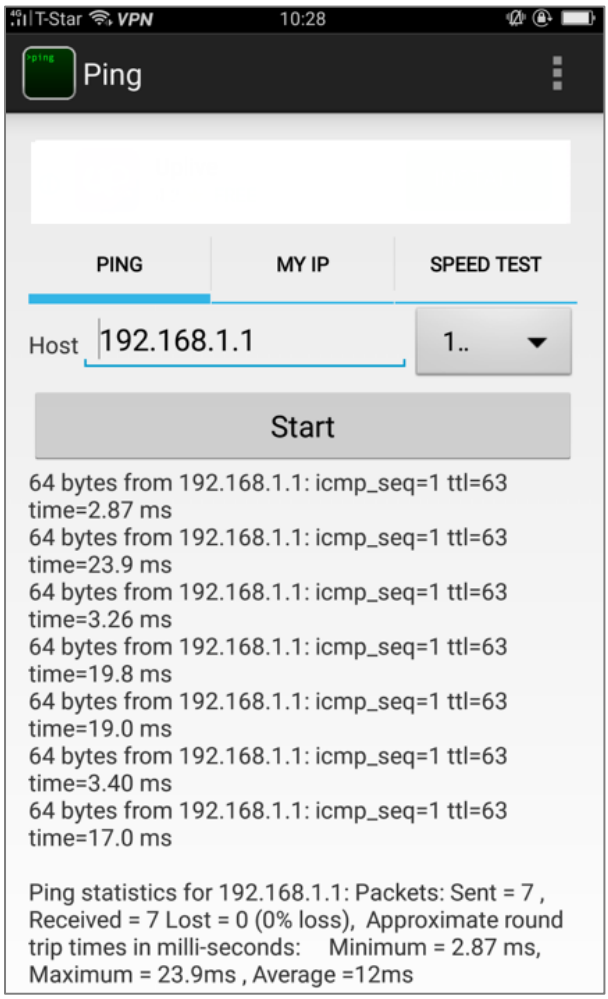
3.Import the Script into strongSwan and enter Username, Password



4.Now, it can connect.

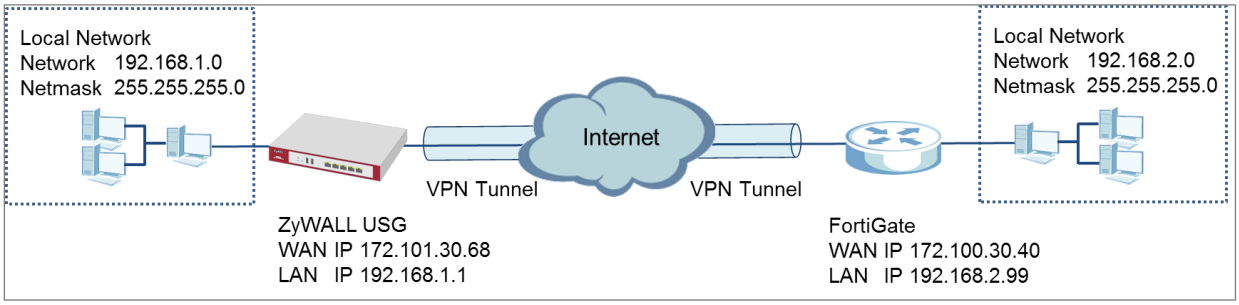



T-Star VPN 10:08
ADD VPN PROFILE
Status: Connected
Profile: RemoteAccess_10.214.48.70
DISCONNECT
RemoteAccess_10.214.48.70
Server: 10.214.48.70
Username: kevin


T-Star VPN 10:28
Ping
PING
MY IP
SPEED TEST
Host 192.168.1.1
1..
Start
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.



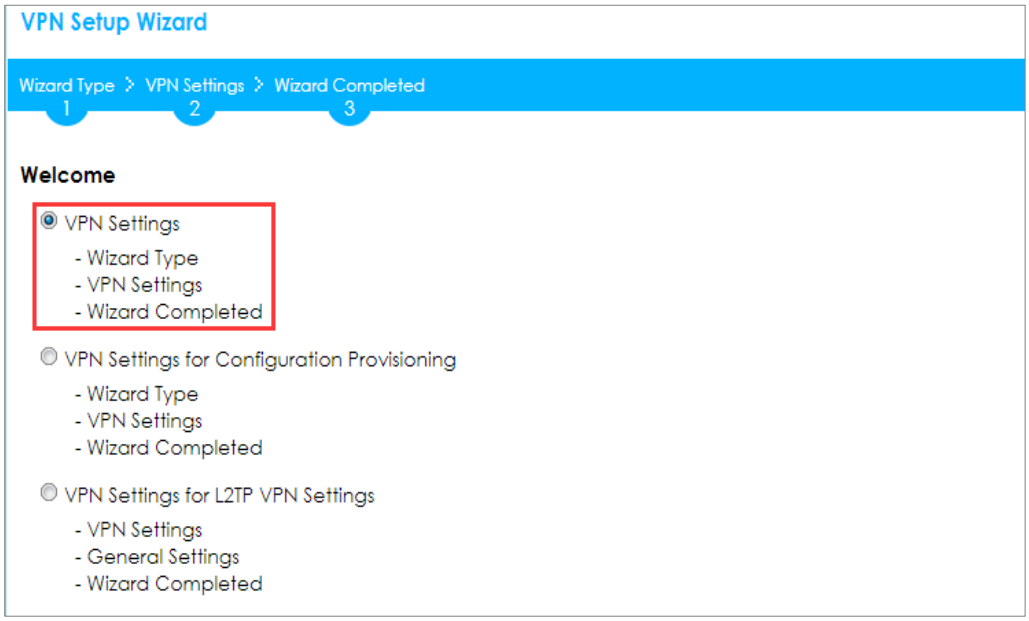
ZyWALL Site-to-site IPSec VPN with FortiGate Connected

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

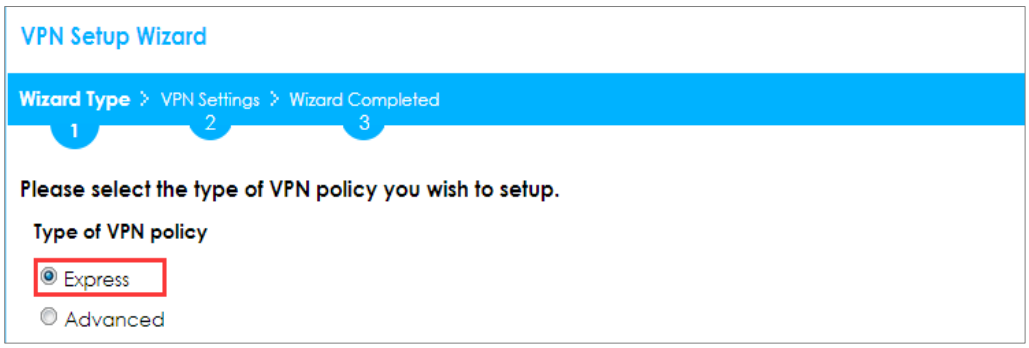
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the FortiGate. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



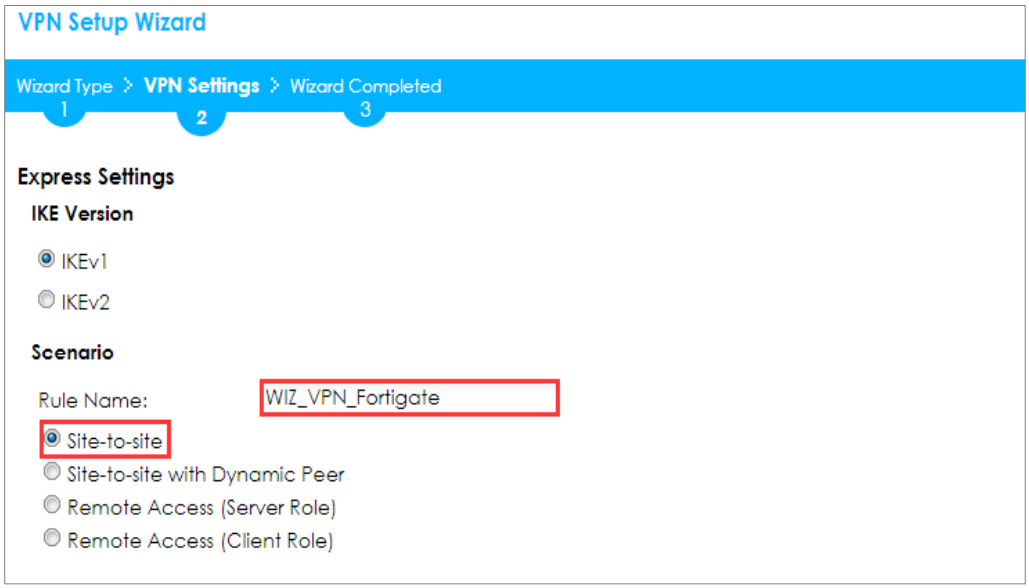
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

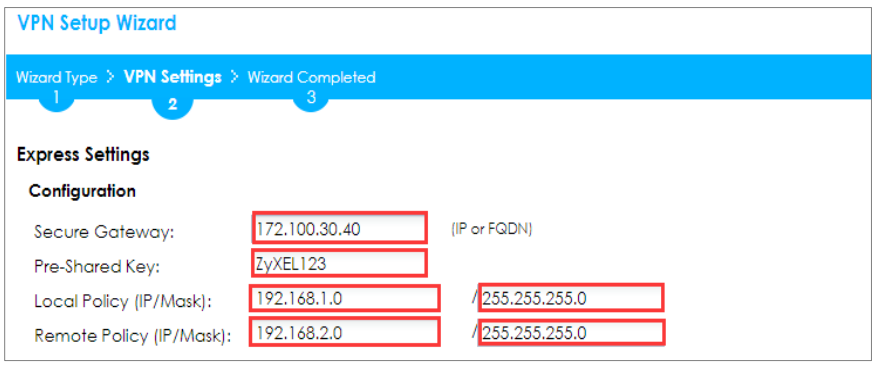
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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).

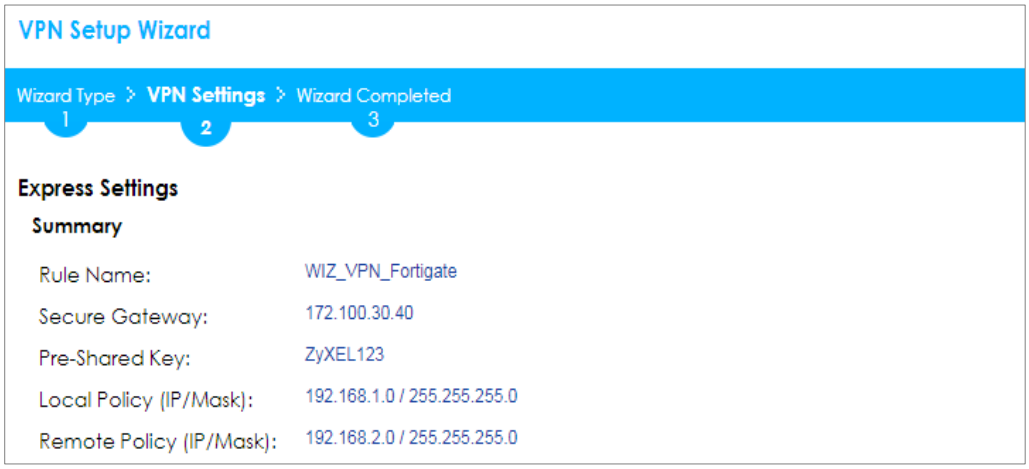
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the FortiGate.

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



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

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

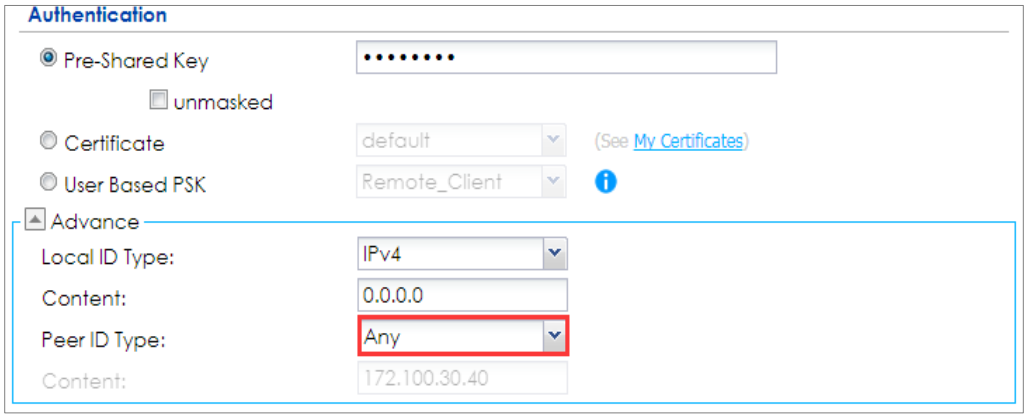


Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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.

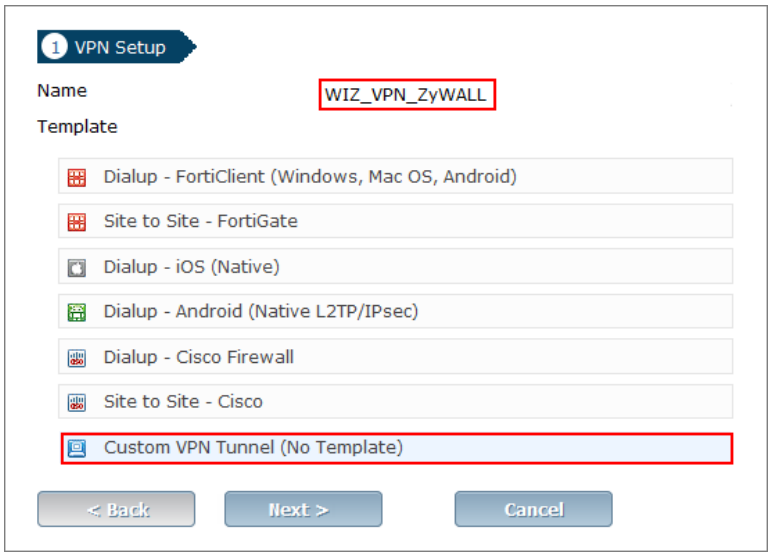
CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Set Up the IPSec VPN Tunnel on the FortiGate

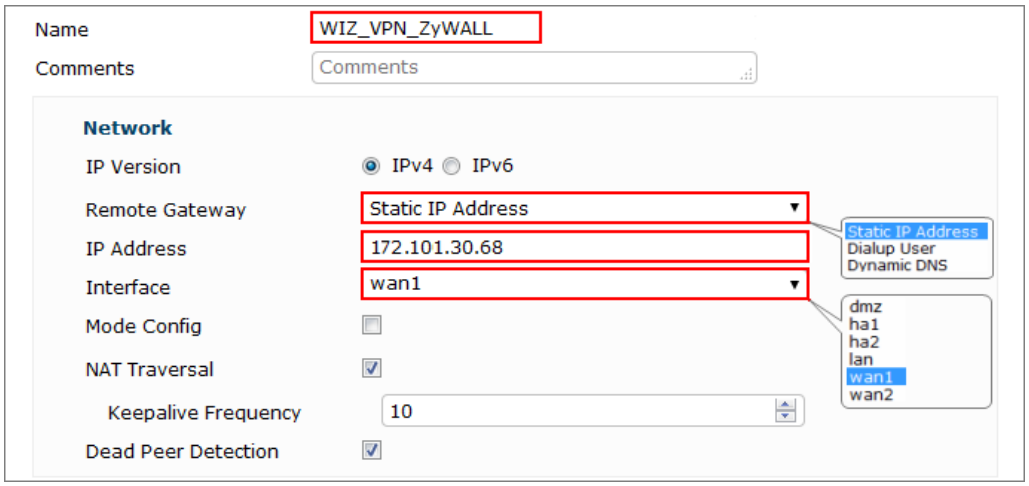
In the FortiGate **VPN > IPsec > Wizard > Custom VPN Tunnel (No Template)**, use the **VPN Setup** to create a **Site-to-site VPN** rule **Name**.

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



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

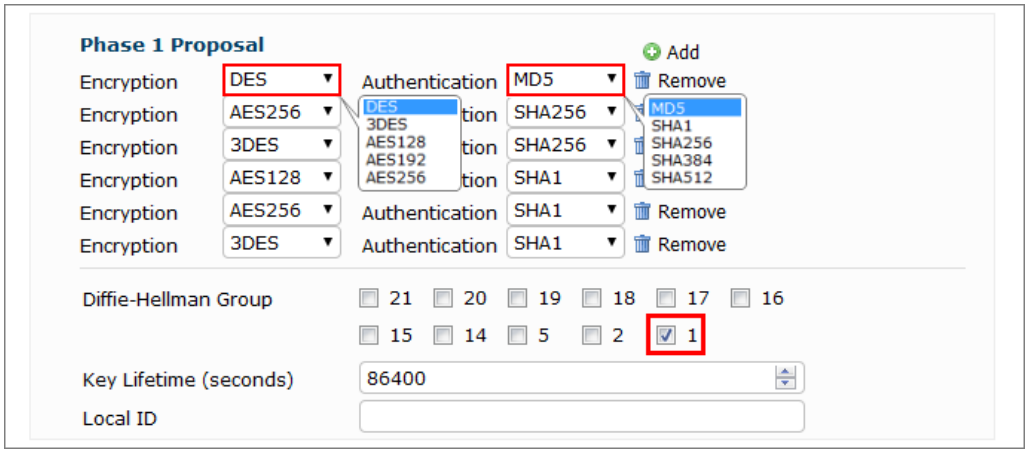


Go to **Authentication** section, enter **Pre-shared Key** and choose negotiation **Mode** the same as the peer ZyWALL/USG's.

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

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

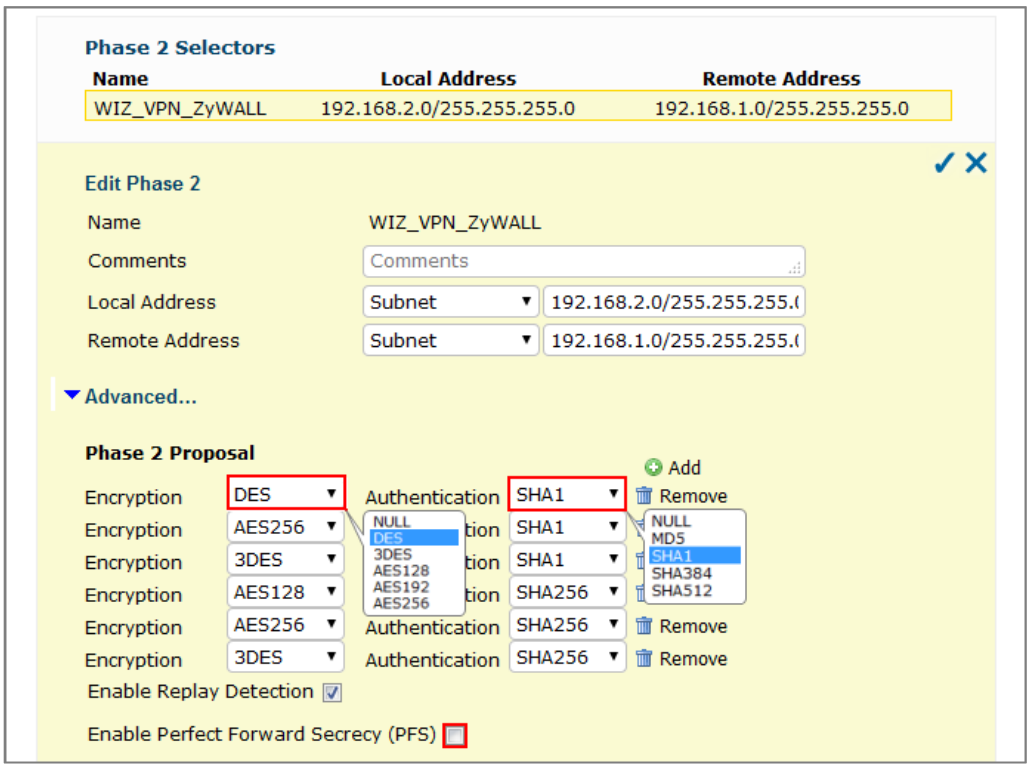


Go to **Phase 2 Selectors > Advanced** and configure **Phase 2 Proposal** as the peer ZyWALL/USG Advanced Settings' **Phase 2 Settings > Proposal**.

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.

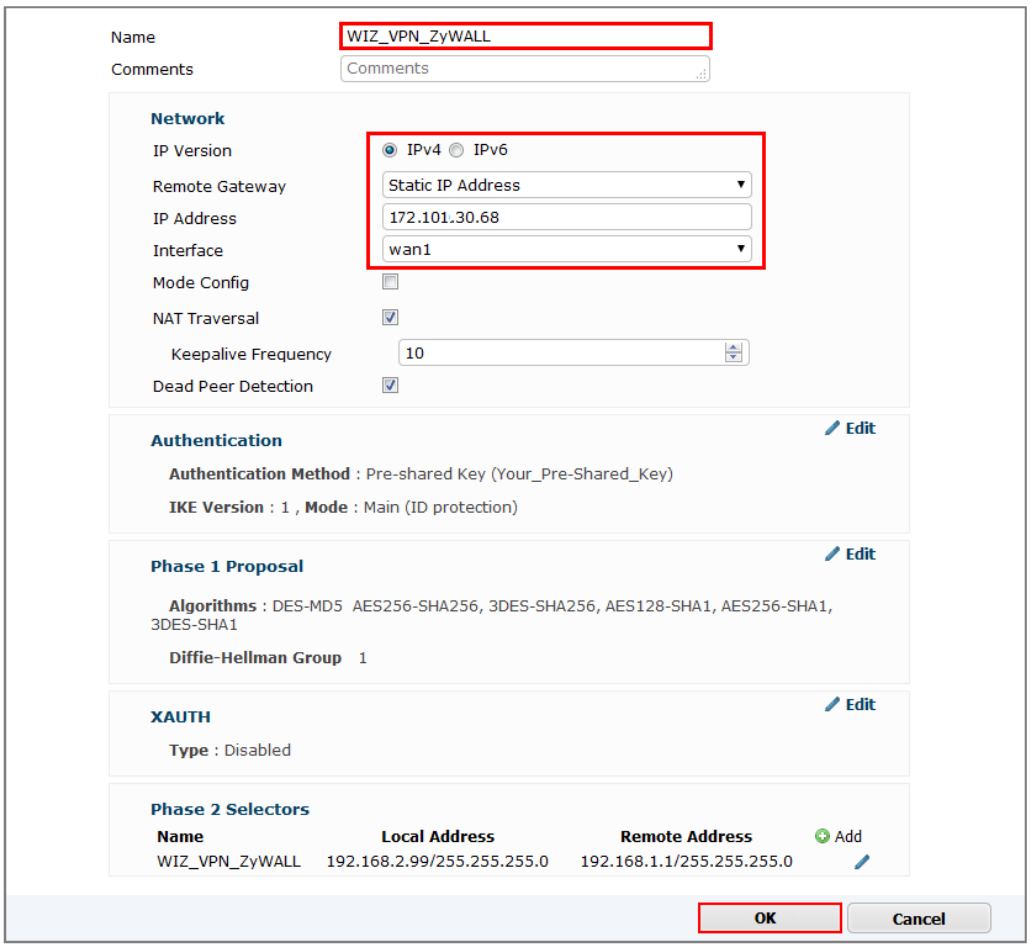
Make sure you uncheck **Enable Perfect Forward Secrecy (PFS)** if this function is disabled in the peer ZyWALL/USG.

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
Encryption
3DES
Encryption
AES128
Encryption
AES256
Encryption
3DES
NULL
DES
3DES
AES128
AES192
AES256
NULL
MD5
SHA1
SHA384
SHA512
Enable Replay Detection
Enable Perfect Forward Secrecy (PFS)

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

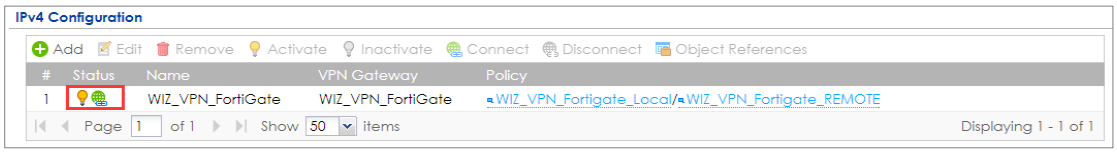
VPN > IPsec > Wizard > Custom VPN Tunnel (No Template)



Test the IPSec VPN Tunnel

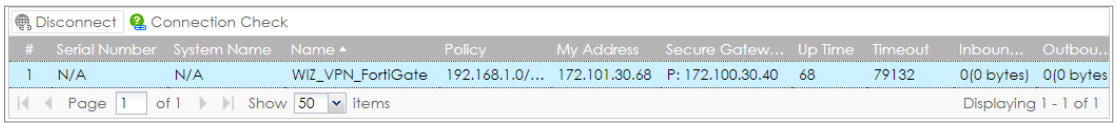
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



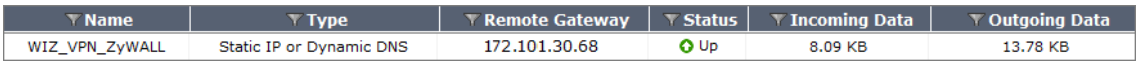
Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec



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

VPN > Monitor > IPsec Monitor



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

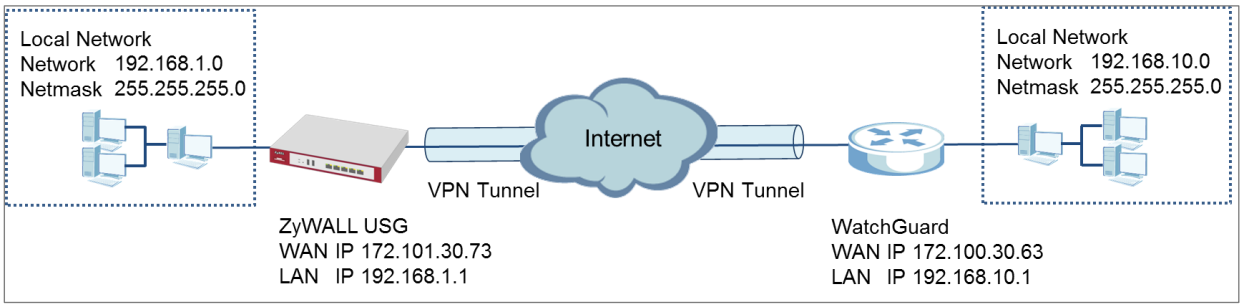
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [WIZ_VPN_FortiGate] Phase 2 proposal mismatch	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Phase 1 IKE SA process done	IKE_LOG

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.



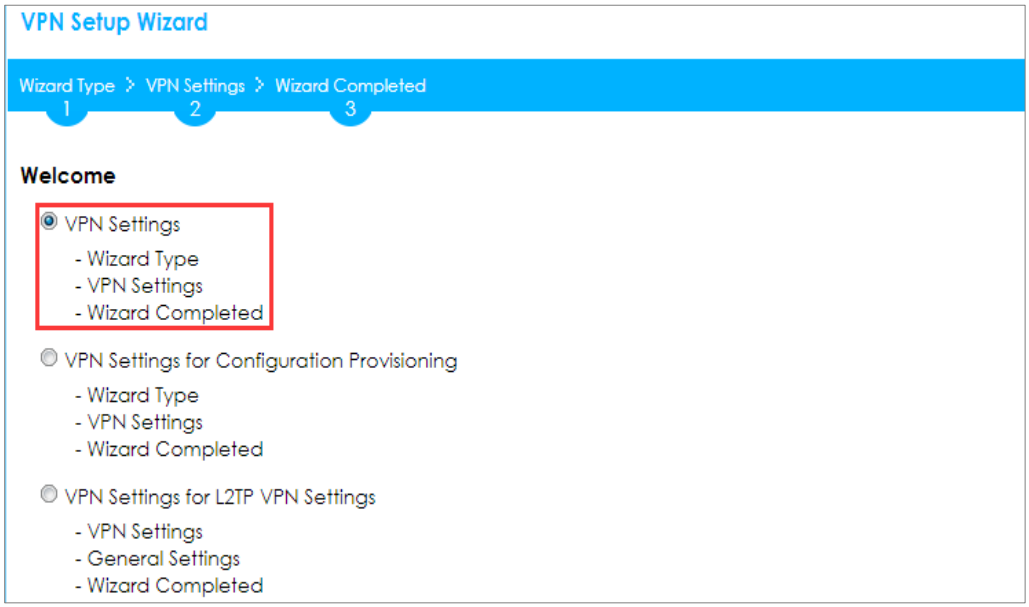
ZyWALL Site-to-site IPSec VPN with WatchGuard Connected

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

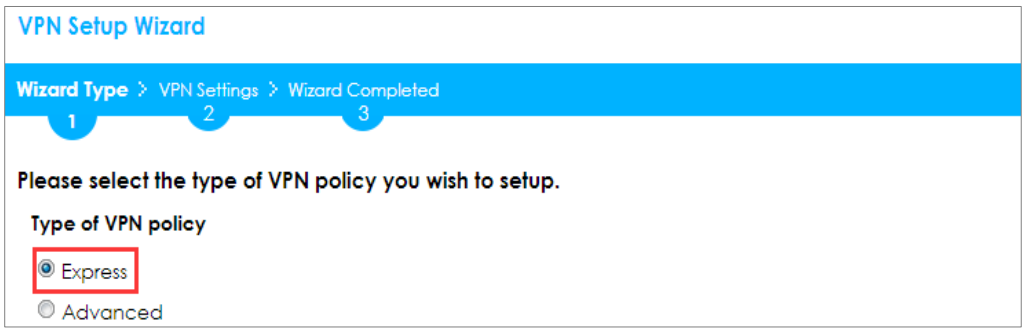
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the WatchGuard. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



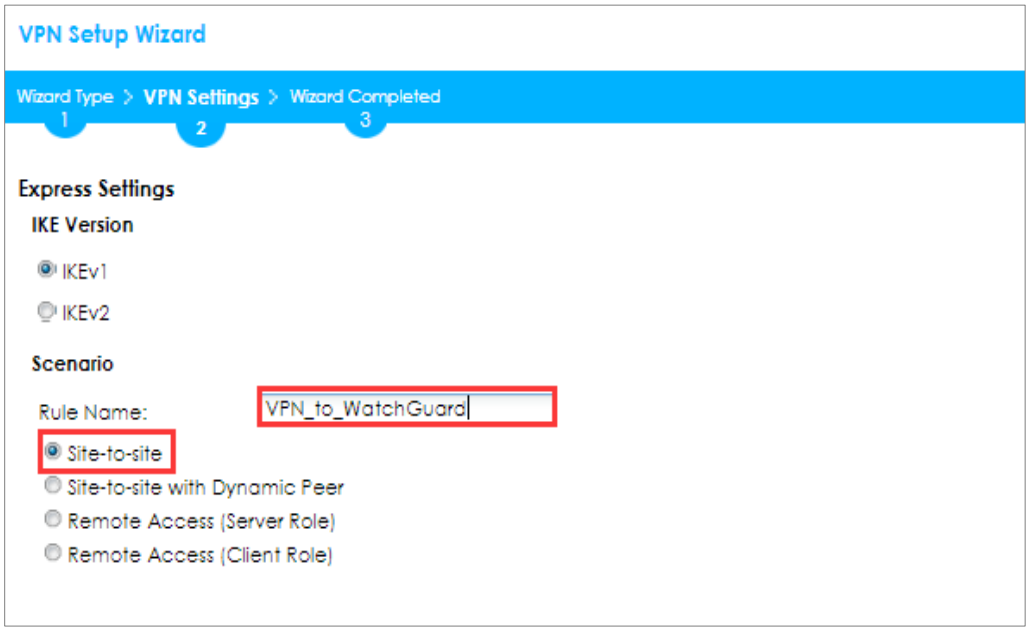
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

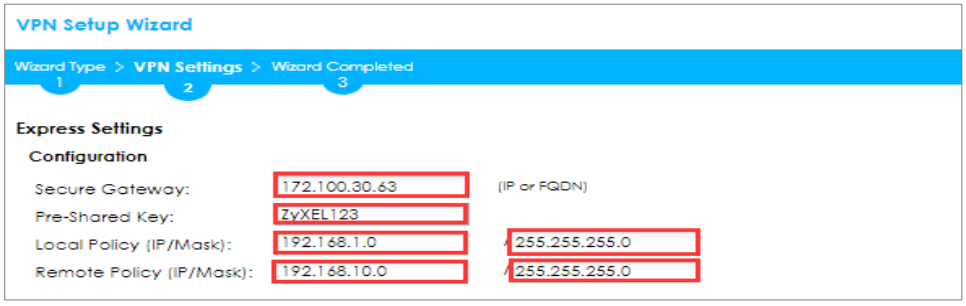
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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).

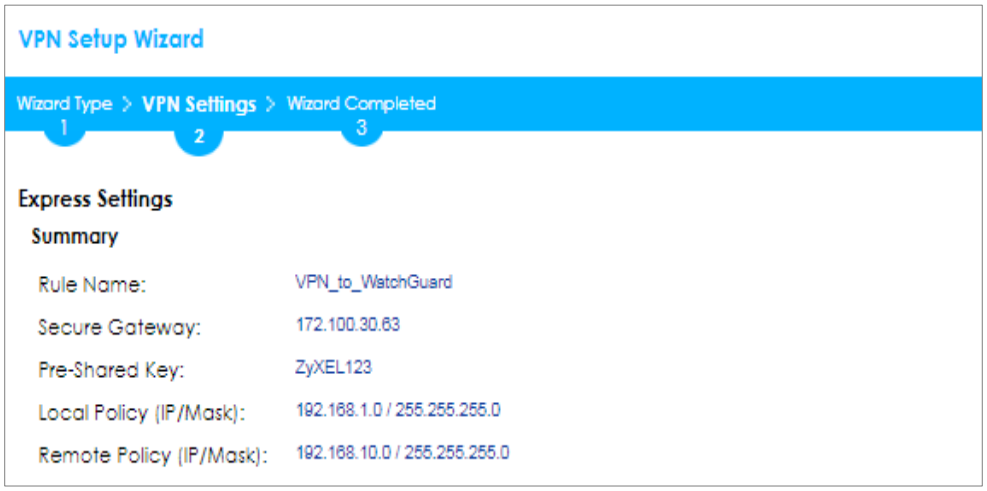
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the WatchGuard. Click **OK**.

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



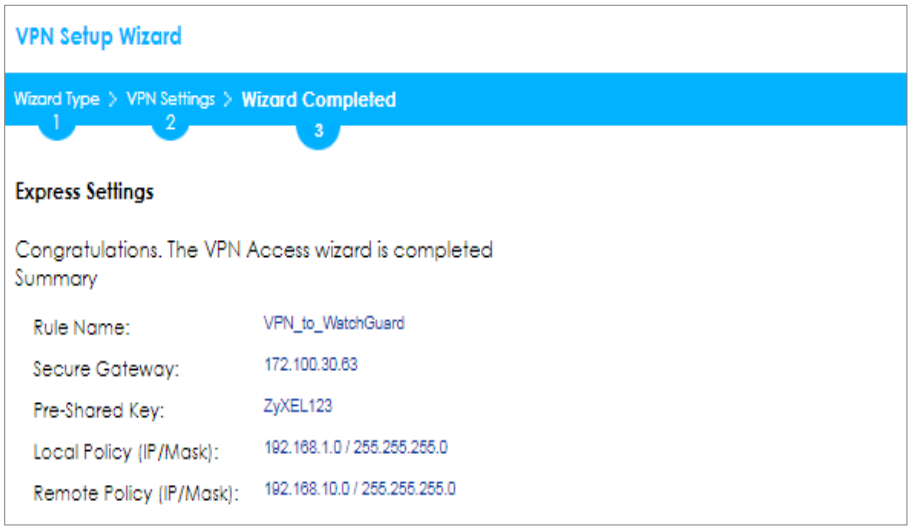
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



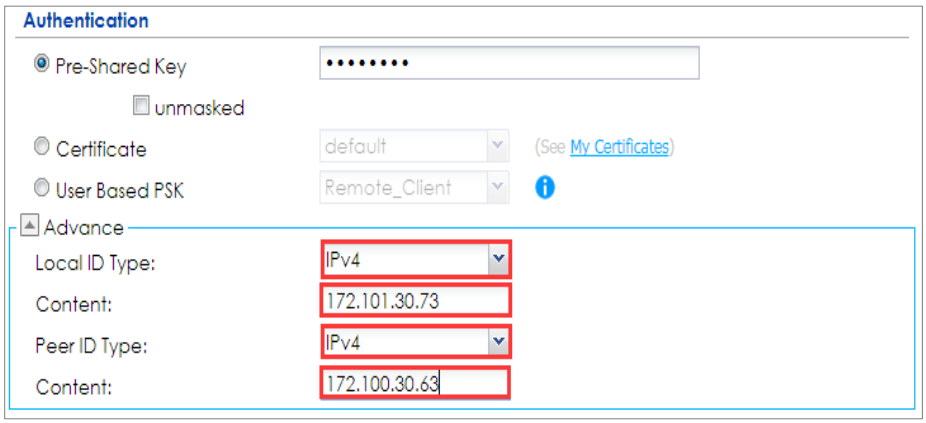
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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



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**.

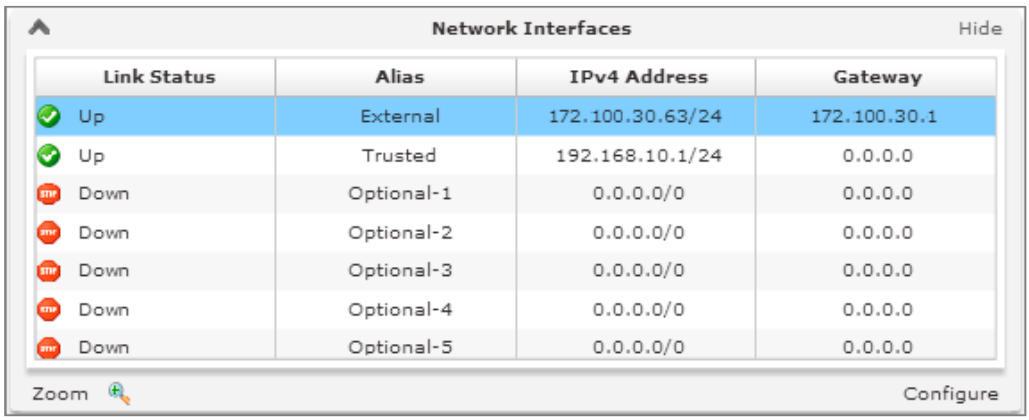
CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



Set Up the IPSec VPN Tunnel on the WatchGuard

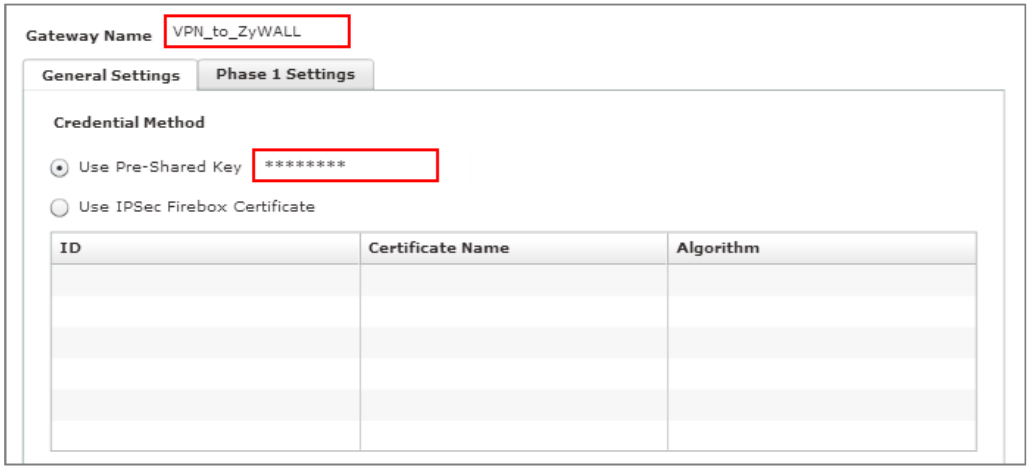
Go to **Dashboard > Network Interfaces** to check your **External IP Address** (the Internet-facing interface) and **Trusted IP Address** (the Local IP address).

Dashboard > Network Interfaces



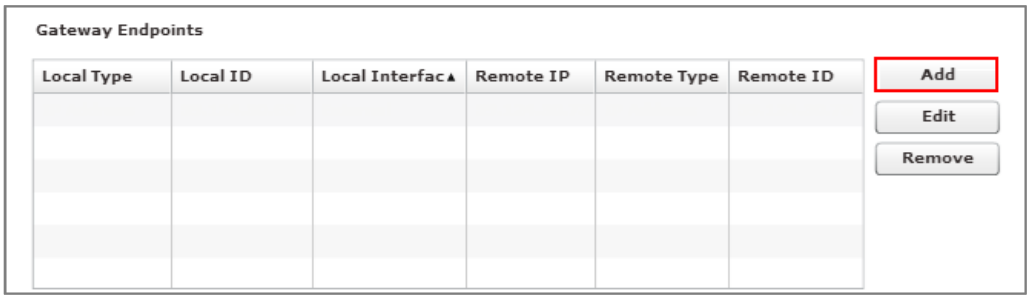
In the WatchGuard **VPN > Branch Office VPN > Gateway > General Settings** create a Site-to-site VPN **Gateway Name** and set a secure **Pre-Shared Key**.

VPN > Branch Office VPN > Gateway > General Settings > Credential Method



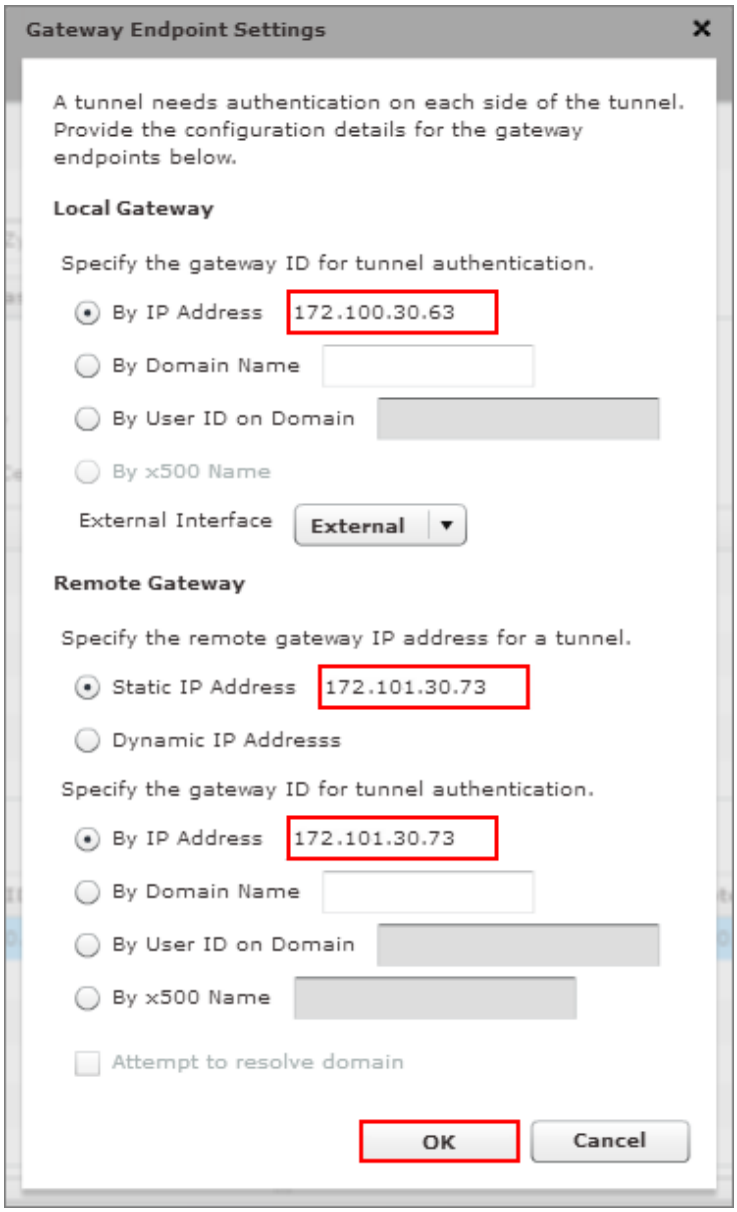
To add a **Gateway Endpoint**, click **Add.**

VPN > Branch Office VPN > Gateway > General Settings > Gateway Endpoints



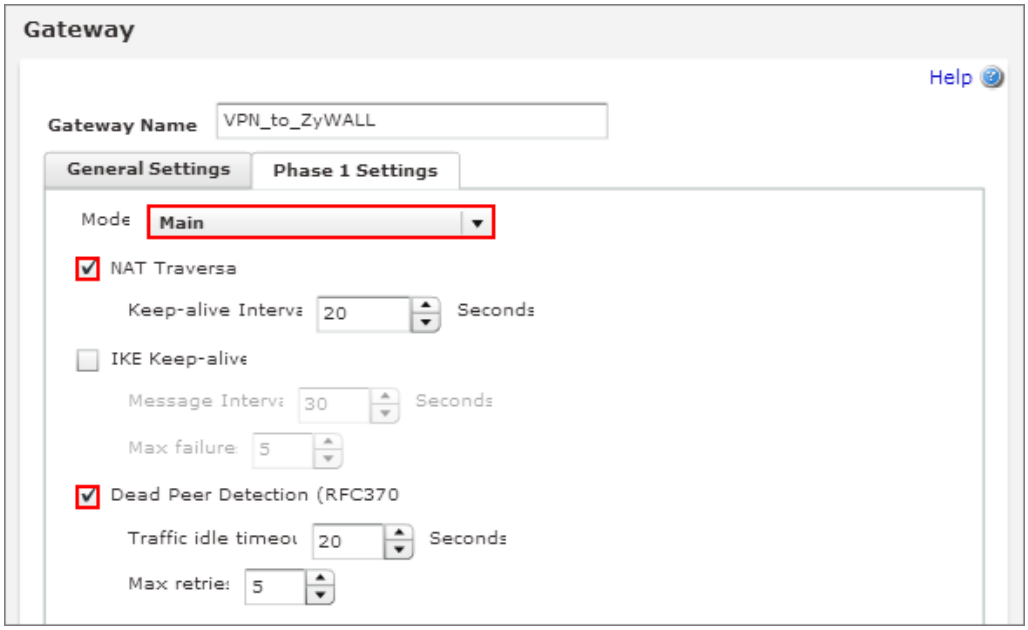
The new **Gateway Endpoint** dialog box appears. Configure your **Local Gateway** identity as WatchGuard's **External IP Address** (in the example, 172.100.30.63) and **Remote Gateway** identity as your ZyWALL/USG's **WAN IP Address** (in the example, 172.101.30.73). Click **OK**.

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
OK
Cancel

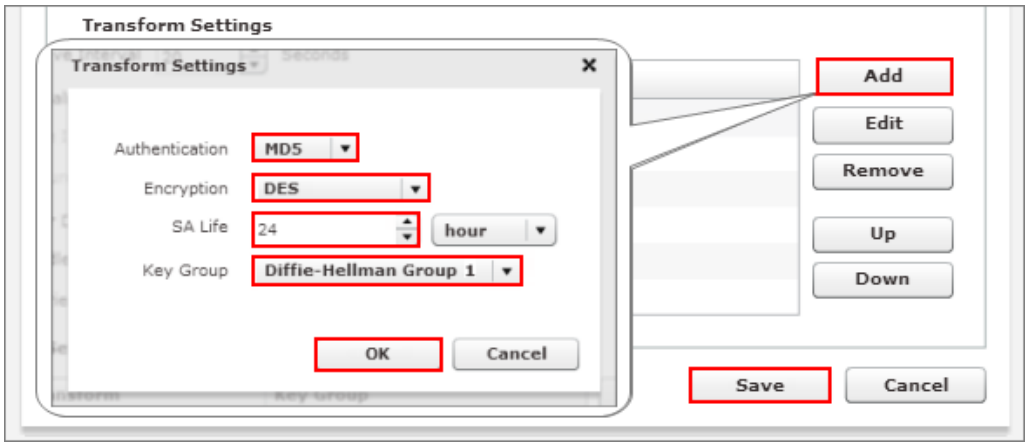
Then, go to **VPN > Branch Office VPN > Gateway > Phase 1 Settings** to select negotiation **Mode** the same as your ZyWALL/USG's Phase 1 Settings. Make sure you enable both **NAT Traversa** and **Dead Peer Detection** options if both options are enabled in the ZyWALL/USG.

VPN > Branch Office VPN > Gateway > Phase 1 Settings



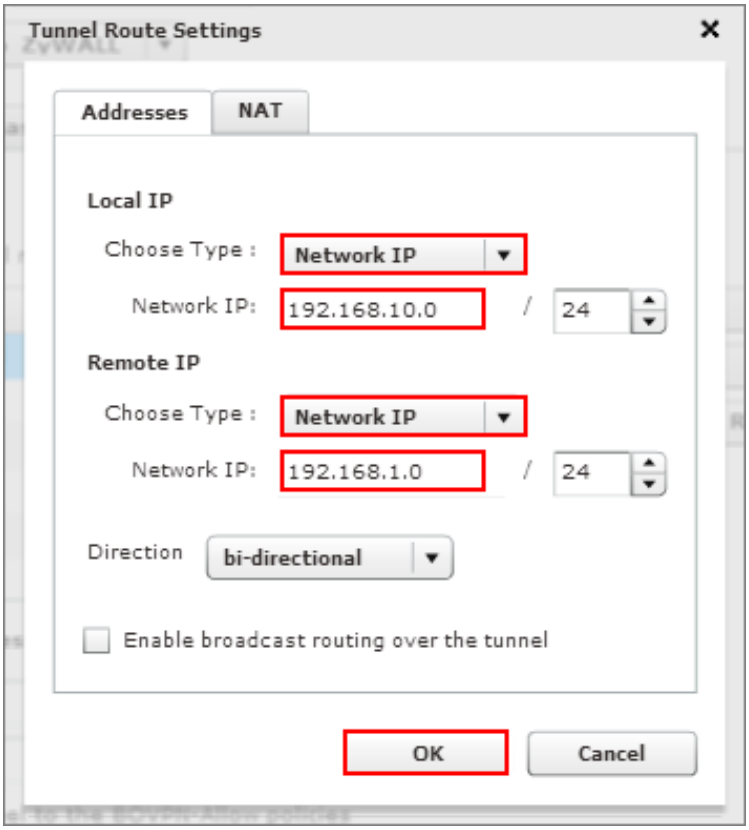
Use **Transform Settings** to create the same security settings as in the ZyWALL/USG Phase 1 settings. Click **OK** and **Save** to exit the **Transform Settings** page.

VPN > Branch Office VPN > Gateway > Phase 1 Settings > Transform Settings



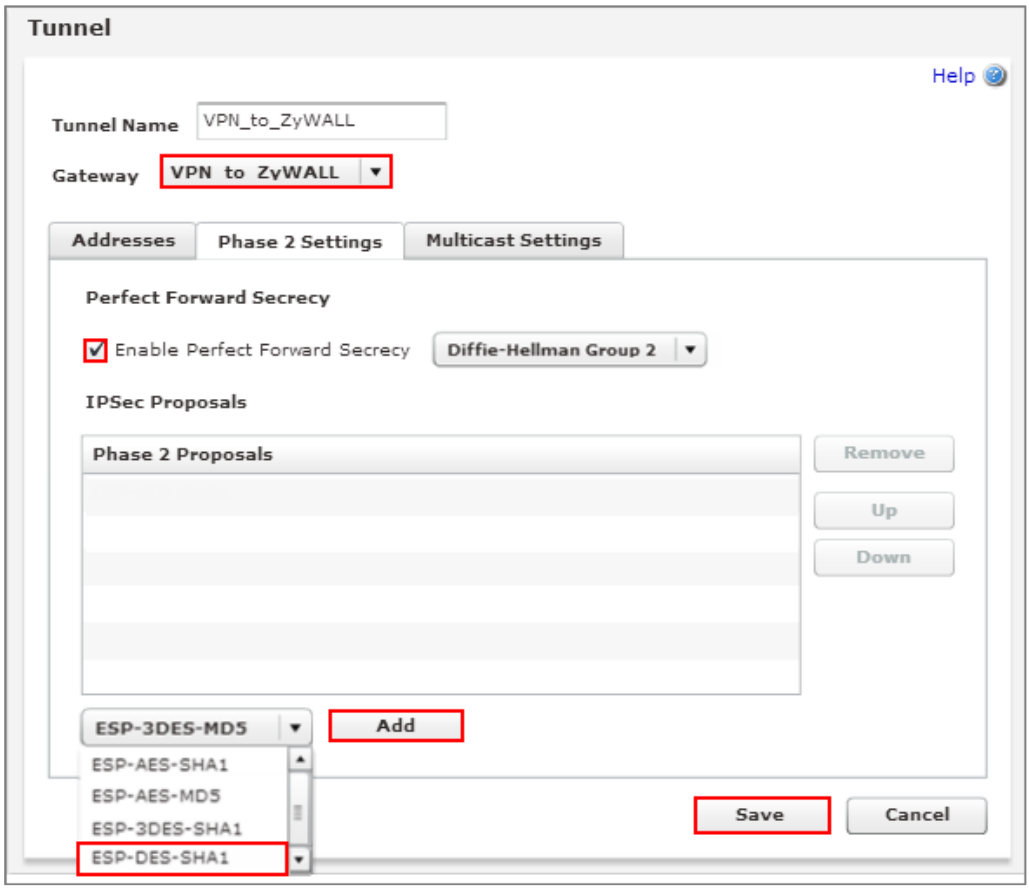
Then, go to **VPN > Branch Office VPN > Tunnel** to add a Tunnel Route Settings. In the **Local IP** section, set **the Network IP** to be the IP address range of the network connected to the WatchGuard. In the **Remote IP** section, set **the Network IP** to be the IP address range of the network connected to the ZyWALL/USG. Click **OK**.

VPN > Branch Office VPN > Tunnel > Address



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**.

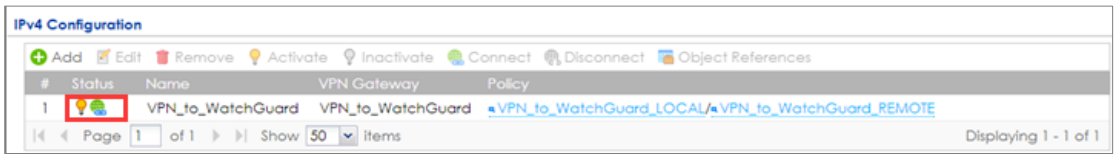
VPN > Branch Office VPN > Tunnel > Phase 2 Settings



Test the IPSec VPN Tunnel

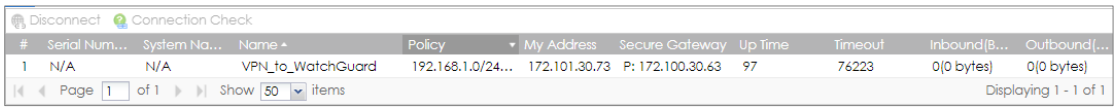
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



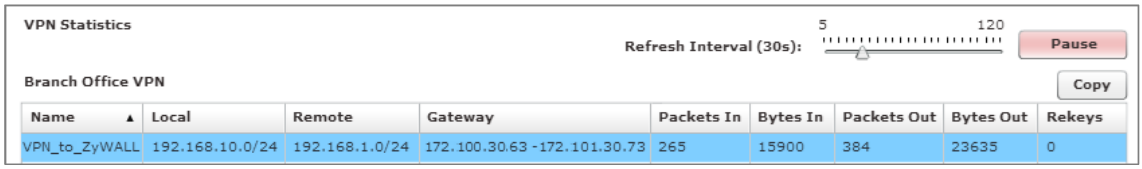
Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec



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



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

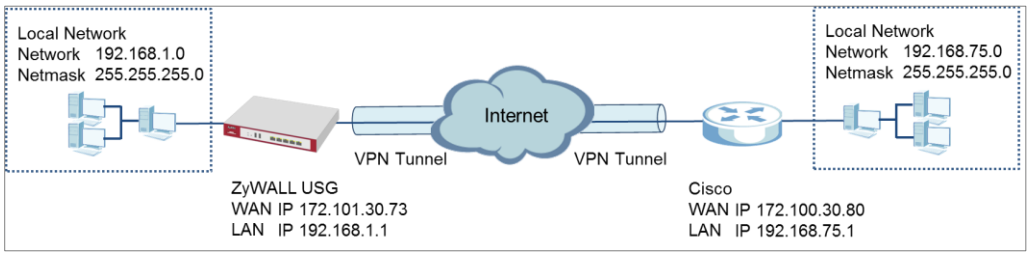
info	IKE	[SA] : No proposal chosen	172.101.30.73:500	172.100.30.63:500	IKE_LOG
info	IKE	[SA] : Tunnel [VPN_to_WatchGuard] Phase 2 proposal mismatch	172.101.30.73:500	172.100.30.63:500	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	172.100.30.63:500	172.101.30.73:500	IKE_LOG
info	IKE	Phase 1 IKE SA process 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.



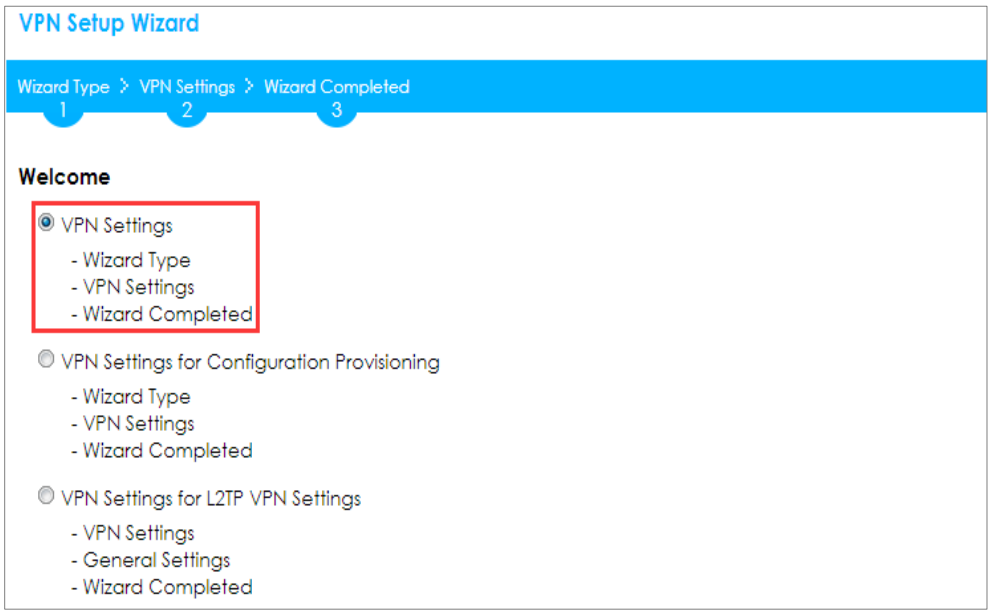
ZyWALL Site-to-site IPSec VPN with Cisco Connected

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

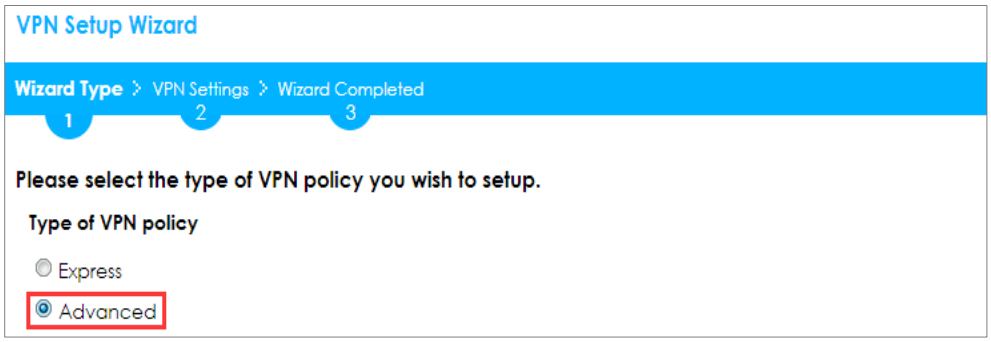
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the Cisco. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



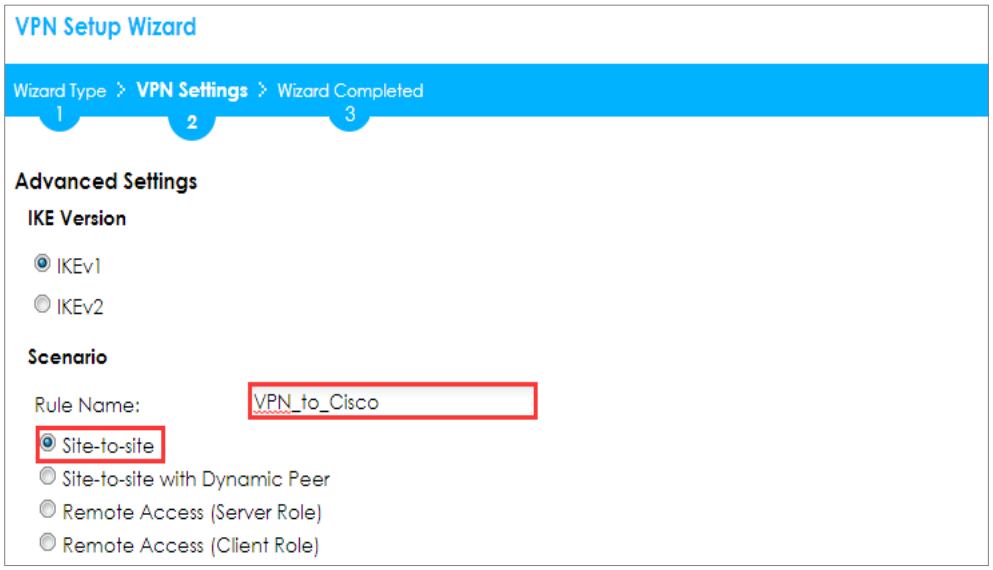
Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

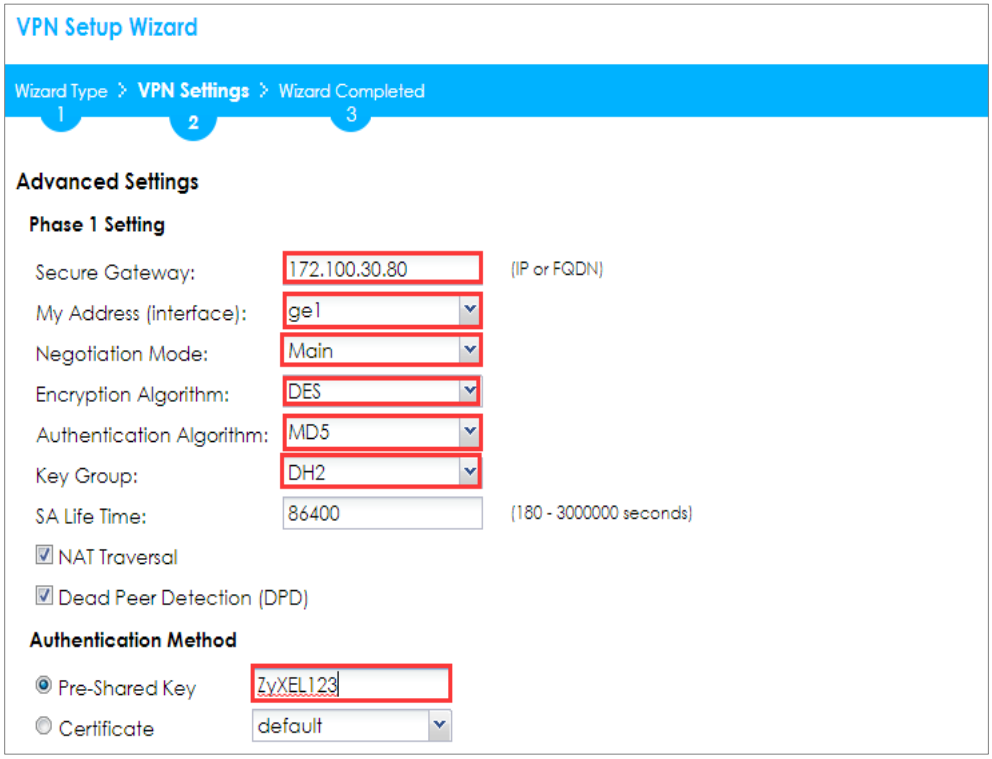
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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**.

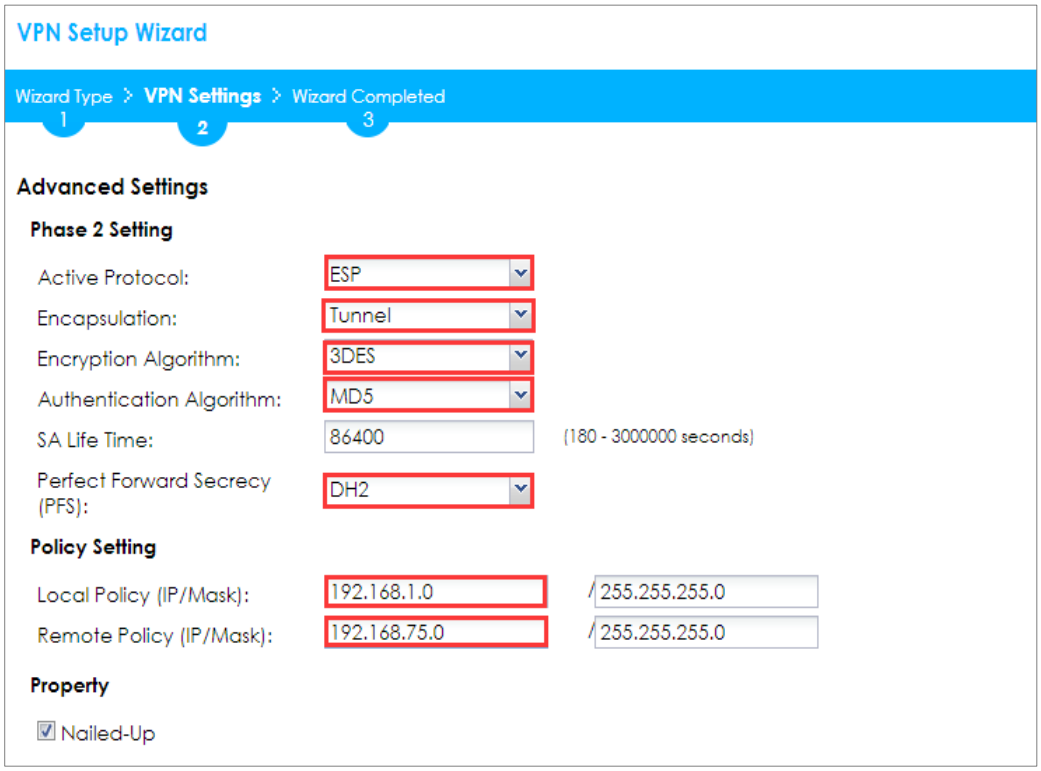
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Phase 1 Setting)



Continue to **Phase 2 Settings** to select the desired **Encapsulation**, **Encryption**, **Authentication**, and **Perfect Forward Secrecy (PFS)** settings.

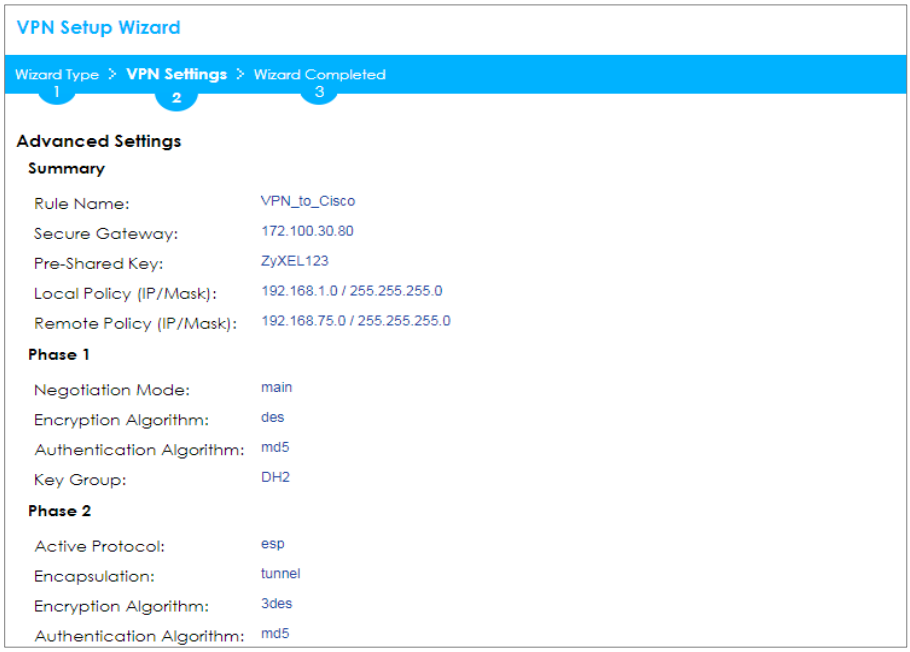
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the Cisco. Click **OK**.

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



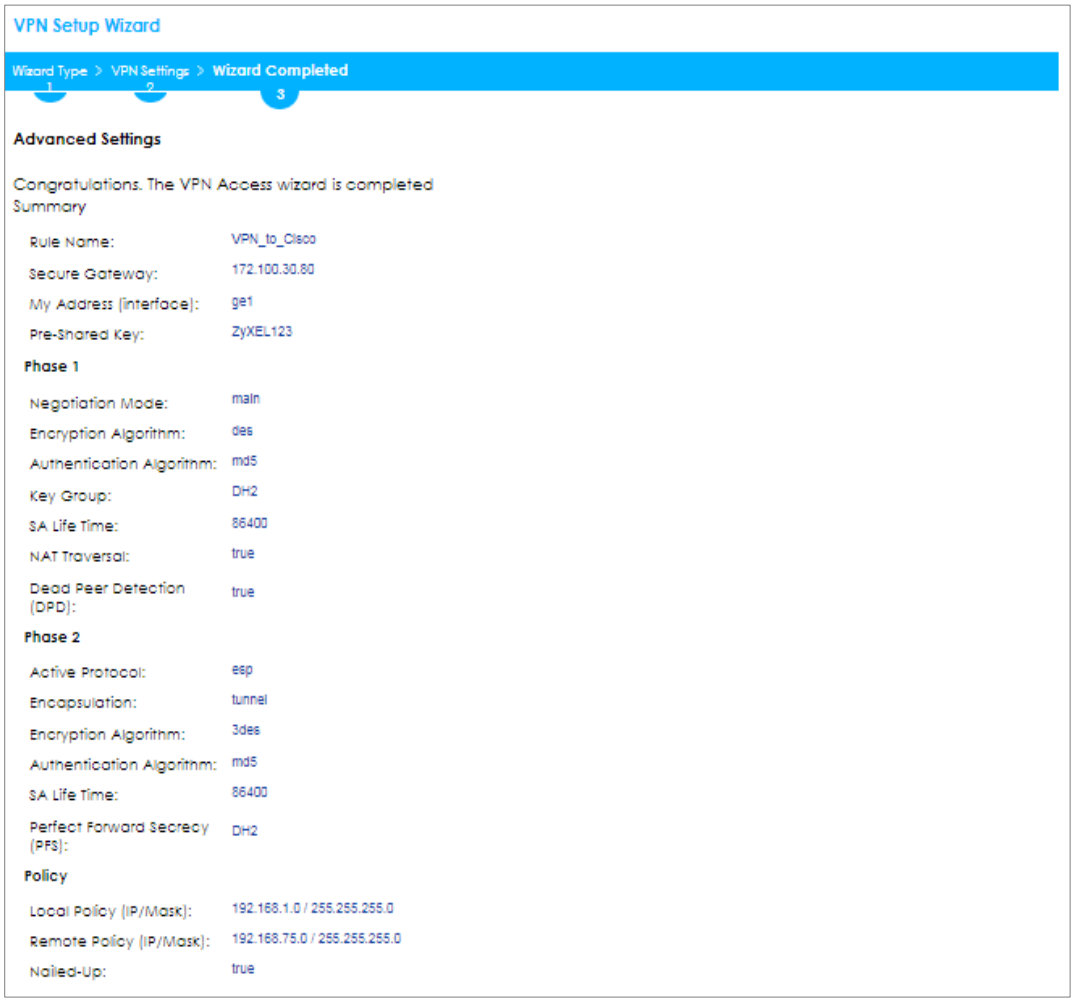
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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

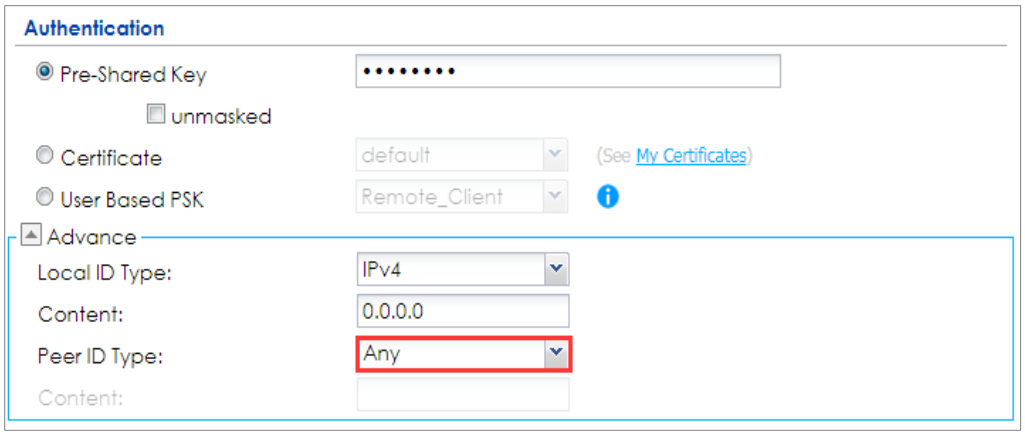


Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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.

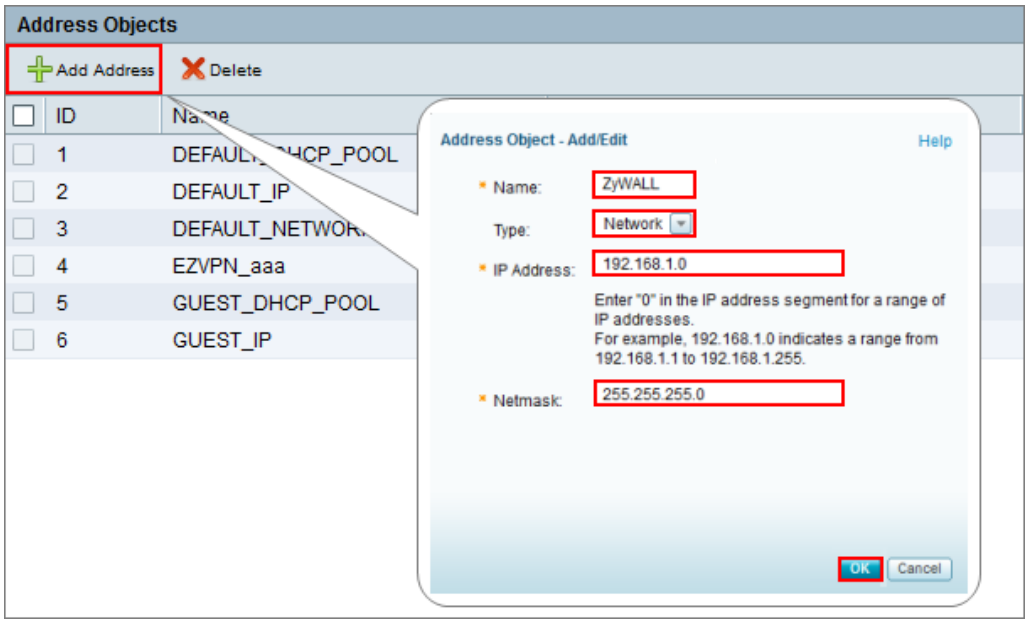


CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type

Set Up the IPSec VPN Tunnel on the Cisco

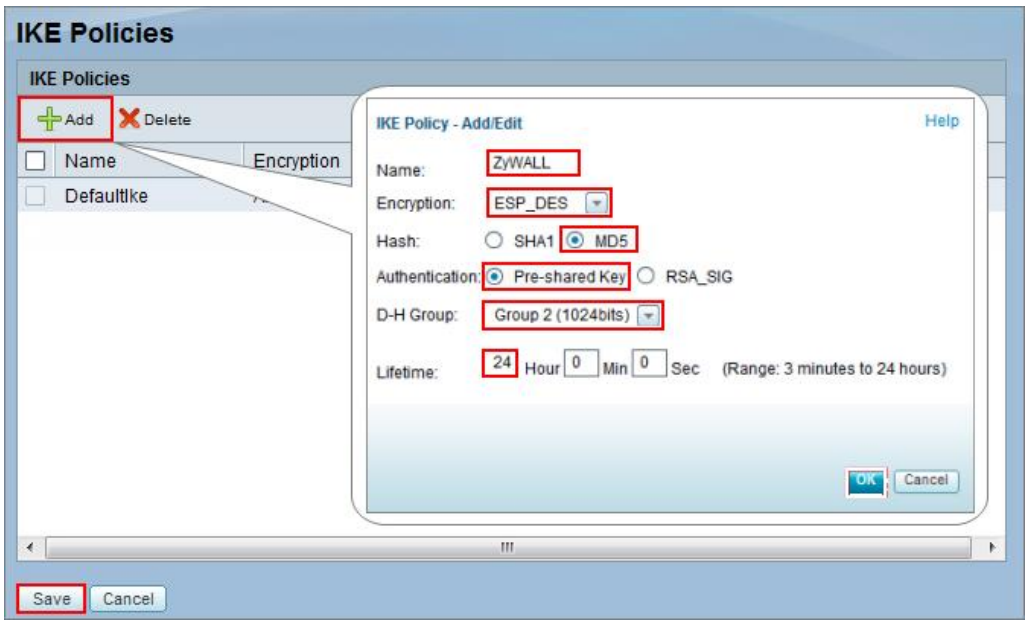
To create an **Address Object Name** of your peer ZyWALL/USG Local IP address, go to **Networking > Address Management > Address Objects** and click **Add Address**. Select **Network** as the **Type**. Configure **IP Address** and **Netmask** to be the IP address range of the network connected to the ZyWALL/USG. Click **OK**.

Networking > Address Management > Address Objects



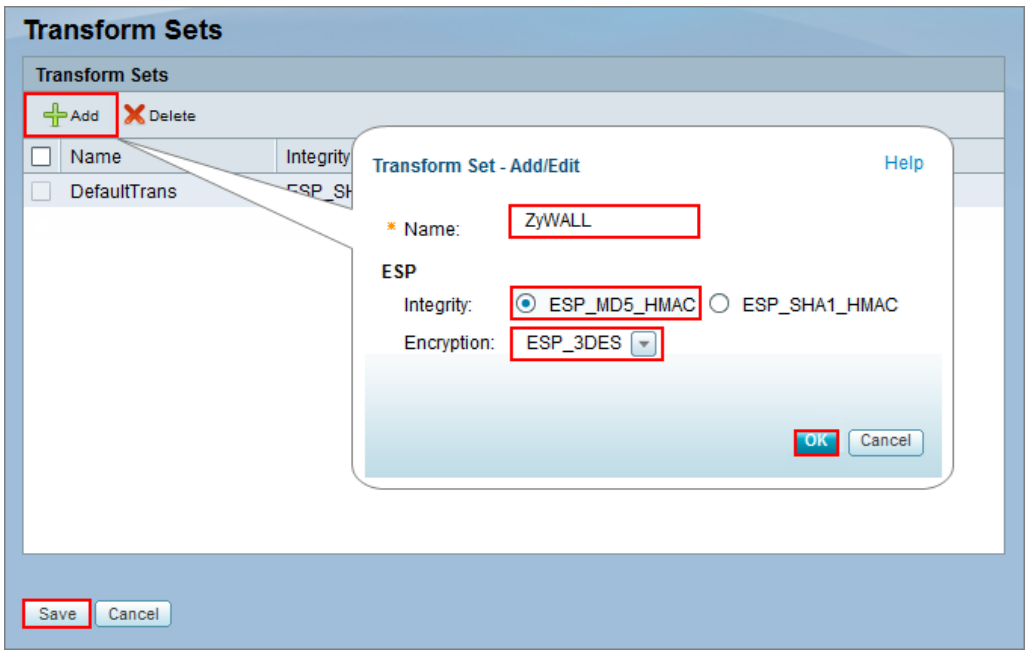
Go to **VPN > Site-to-site > IKE Policies**, click **Add** to create a new IKE Policy **Name**. Then, select **Encryption, Hash**, **Pre-shared Key** and **D-H Group** to match your ZyWALL/USG's **VPN Gateway > Phase 1 Settings**. Set **Lifetime** to **24** hours and click **OK** then click **Save** to exit the **IKE Policies** page.

VPN > Site-to-site > IKE Policies



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



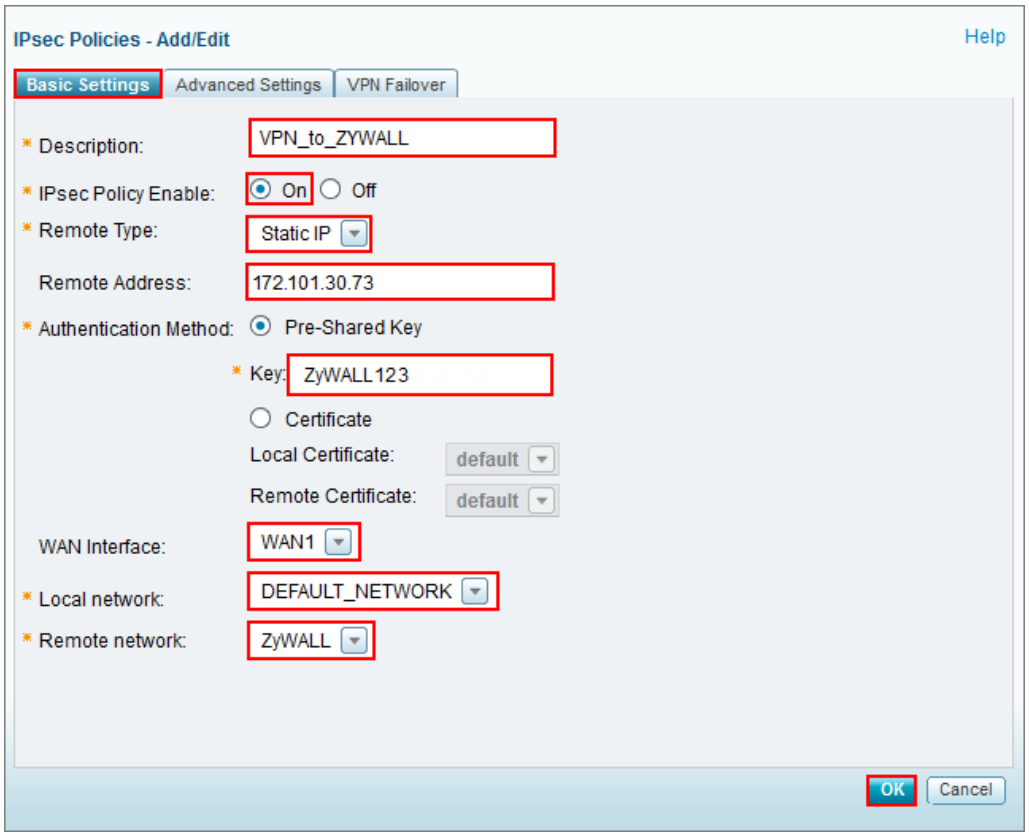
Go to **VPN > Site-to-site > IPsec Policies** and click **Add**. The new **IPsec Policies** dialog box appears. Go to **Basic Settings,** create IPsec policy **Description** name and click **On** the **IPsec Policy Enable** option.

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)

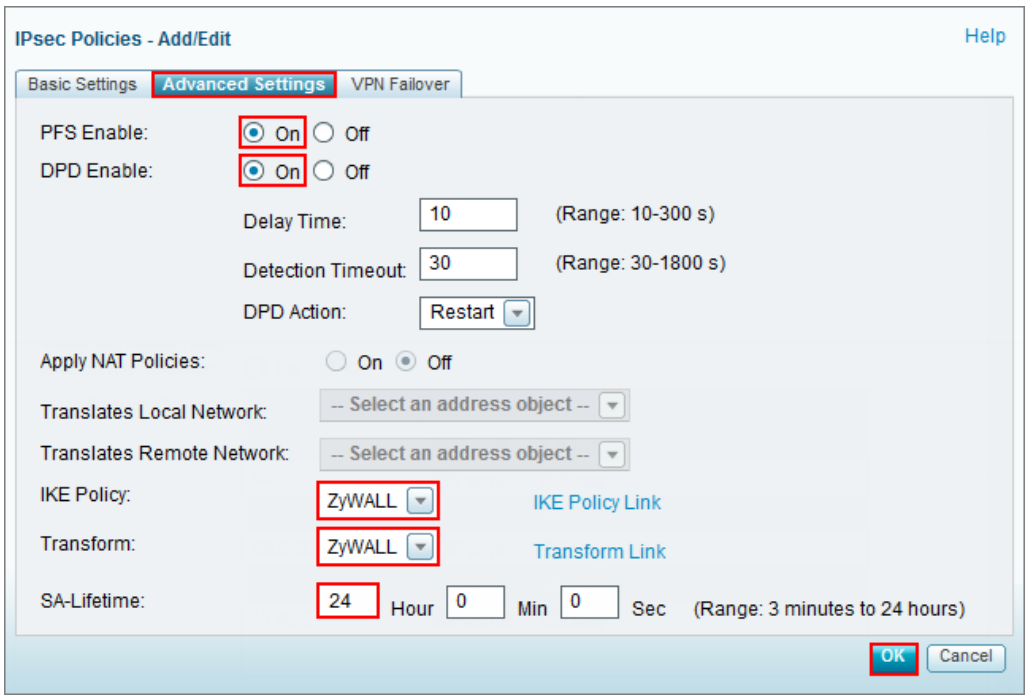
VPN > Site-to-site > IPsec Policies > Basic Settings

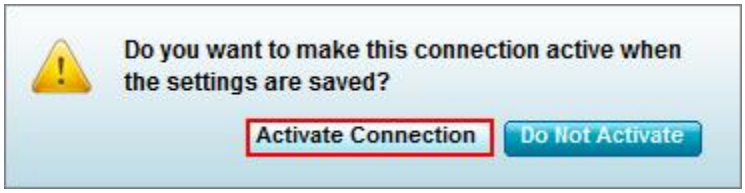


Then, go to **Advanced Settings** enable **PFS** and **DPD** if you enable both options in the ZyWALL/USG. Set **IKE Policy** to be the **IKE Policy** created in Step 2 (found under **IKE Policy Link**); set **Transform** to be the **Transform Set** created in Step 3 (found under **Transform Link**) 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

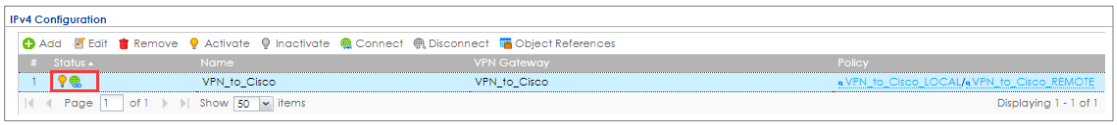




Test the IPSec VPN Tunnel

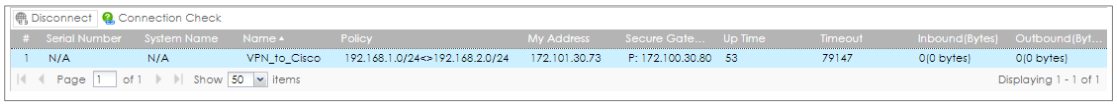
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



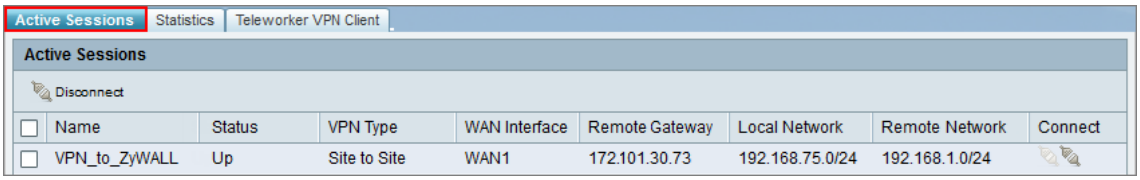
Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec



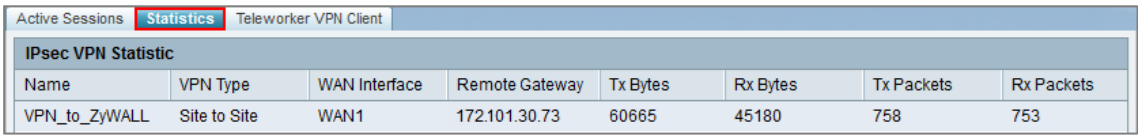
Go to Cisco **VPN > VPN Status > IPsec VPN Status > Active Sessions** and check the tunnel **Status** is up.

VPN > VPN Status > IPsec VPN Status > Active Sessions



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



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

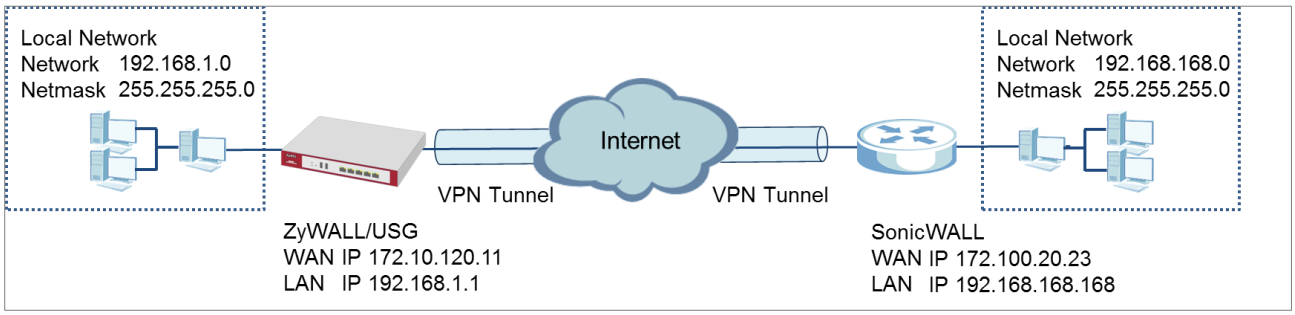
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	172.101.30.73:500	172.100.30.80:500	IKE_LOG
info	IKE	[SA] : No proposal chosen	172.101.30.73:500	172.100.30.80:500	IKE_LOG
info	IKE	[SA] : Tunnel [VPN_to_Cisco] Phase 2 proposal mismatch	172.101.30.73:500	172.100.30.80:500	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	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.



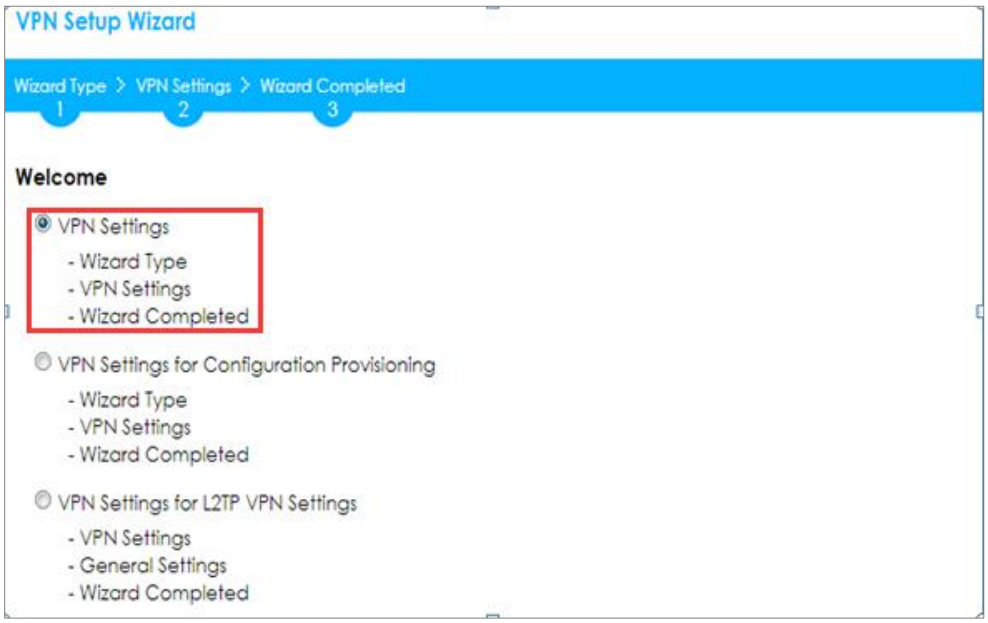
ZyWALL/USG Site-to-site IPSec VPN with SonicWALL

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

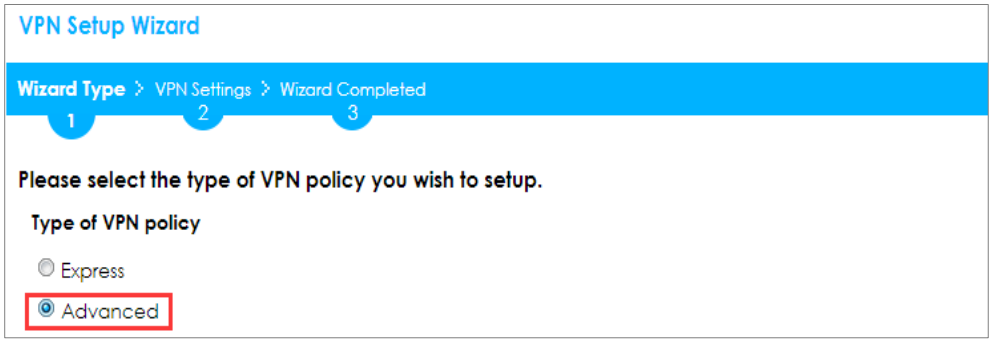
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the SonicWALL. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



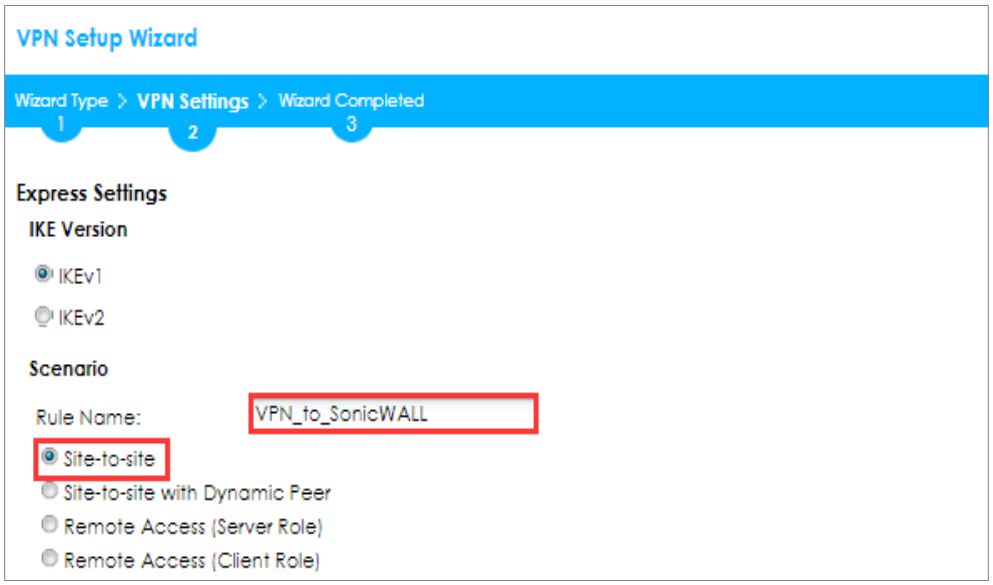
Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



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**.

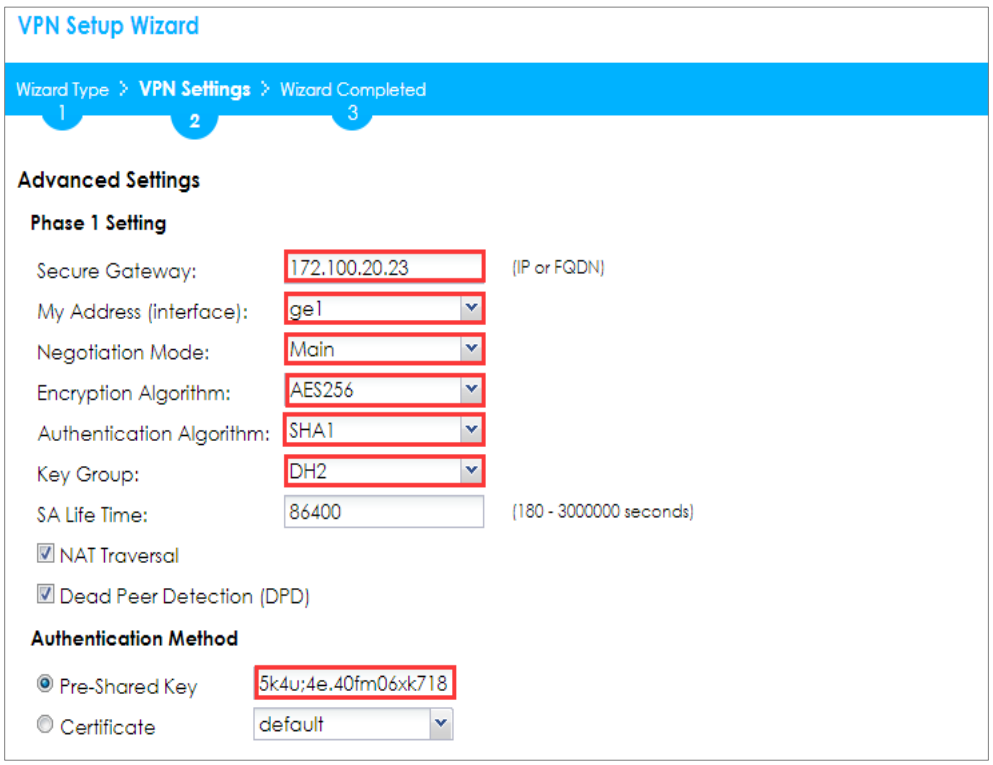
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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**.

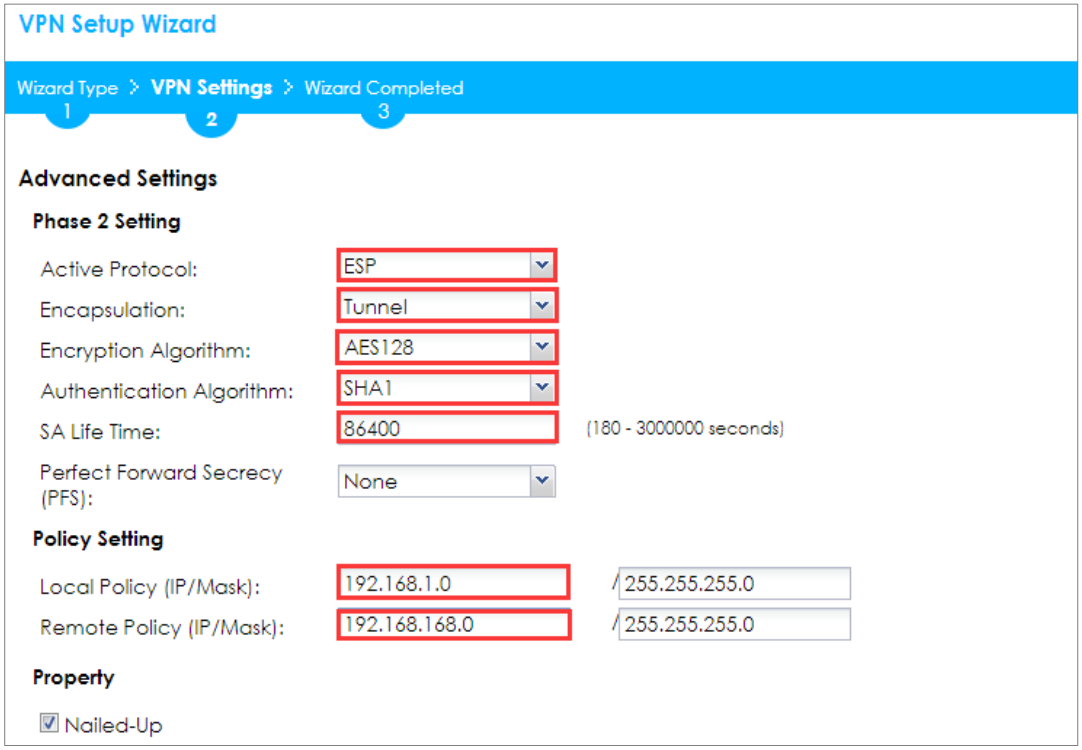
Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings (Phase 1 Setting)



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)



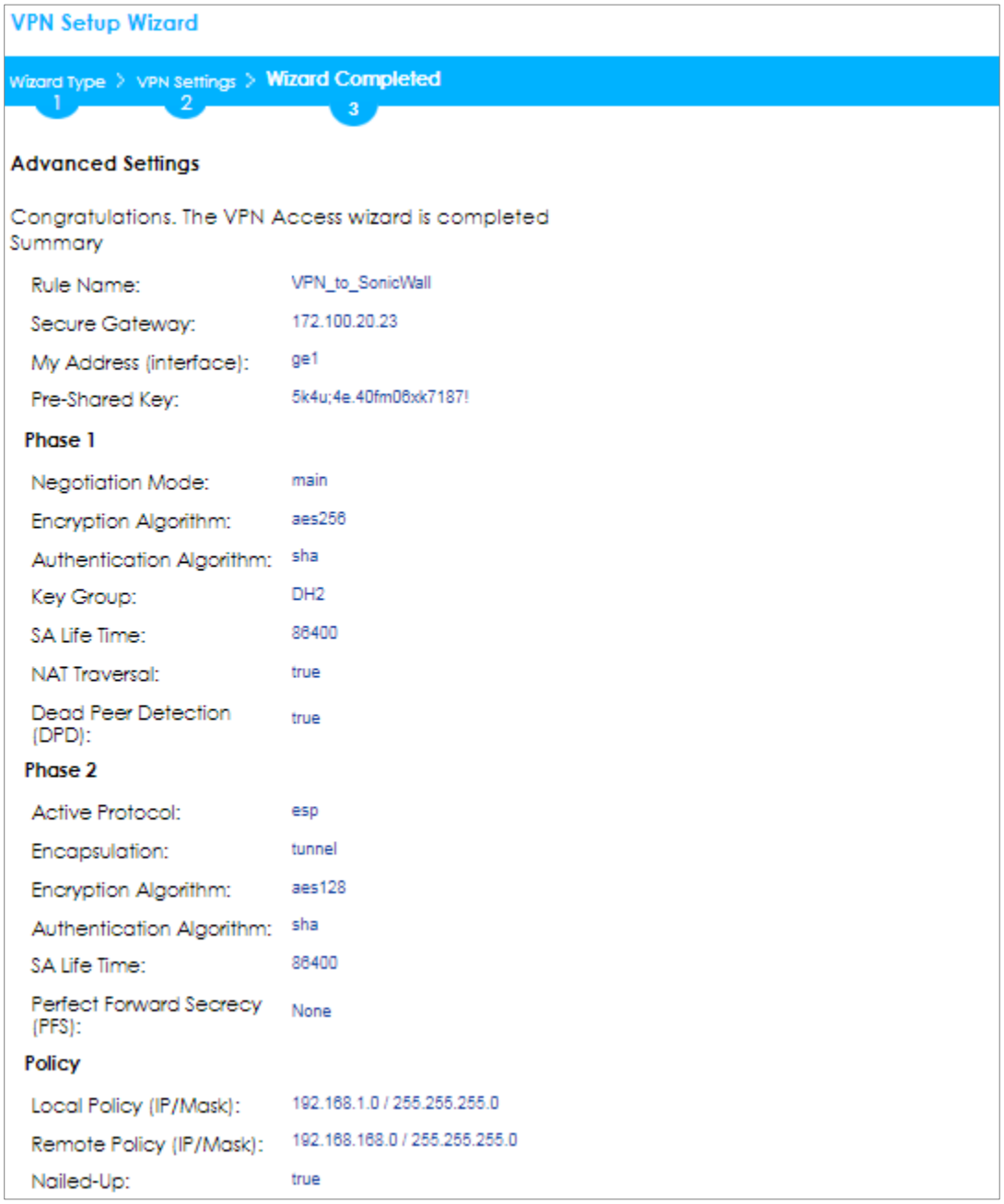
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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

Note: The Phase 1 and Phase 2 settings established here must match the Phase 1 and Phase 2 settings configured later in the SonicWALL.

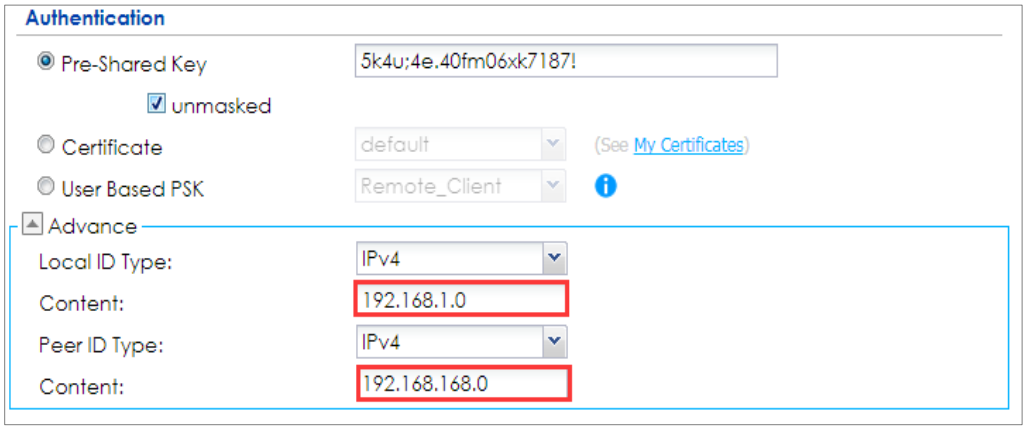
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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



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

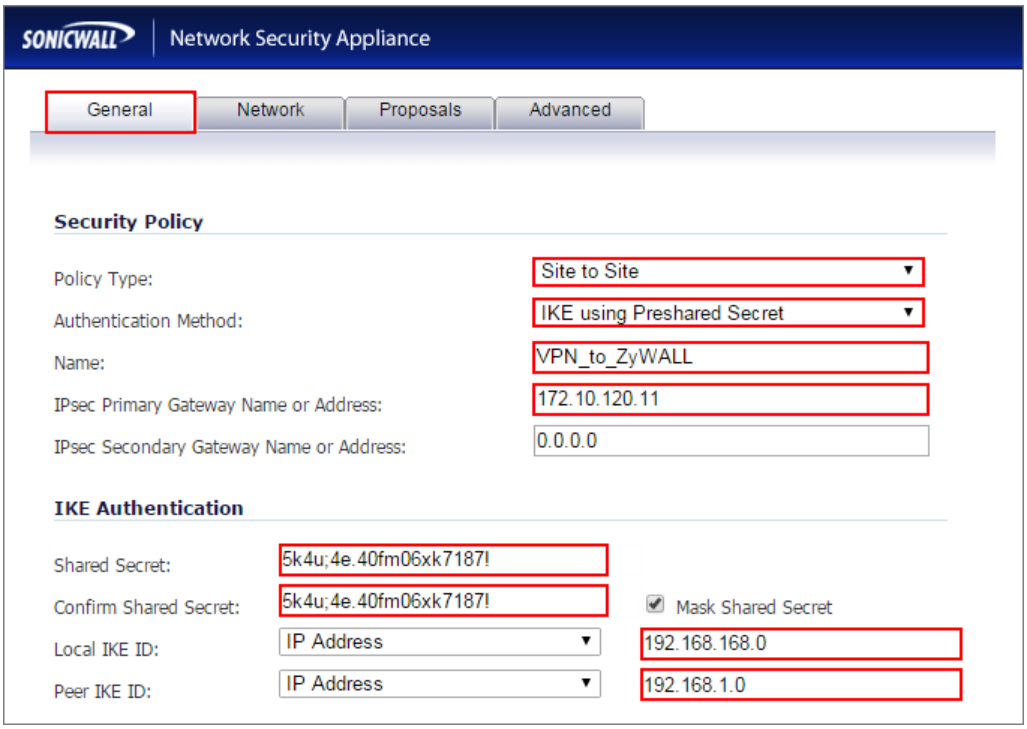


Set Up the IPSec VPN Tunnel on the SonicWALL

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**.

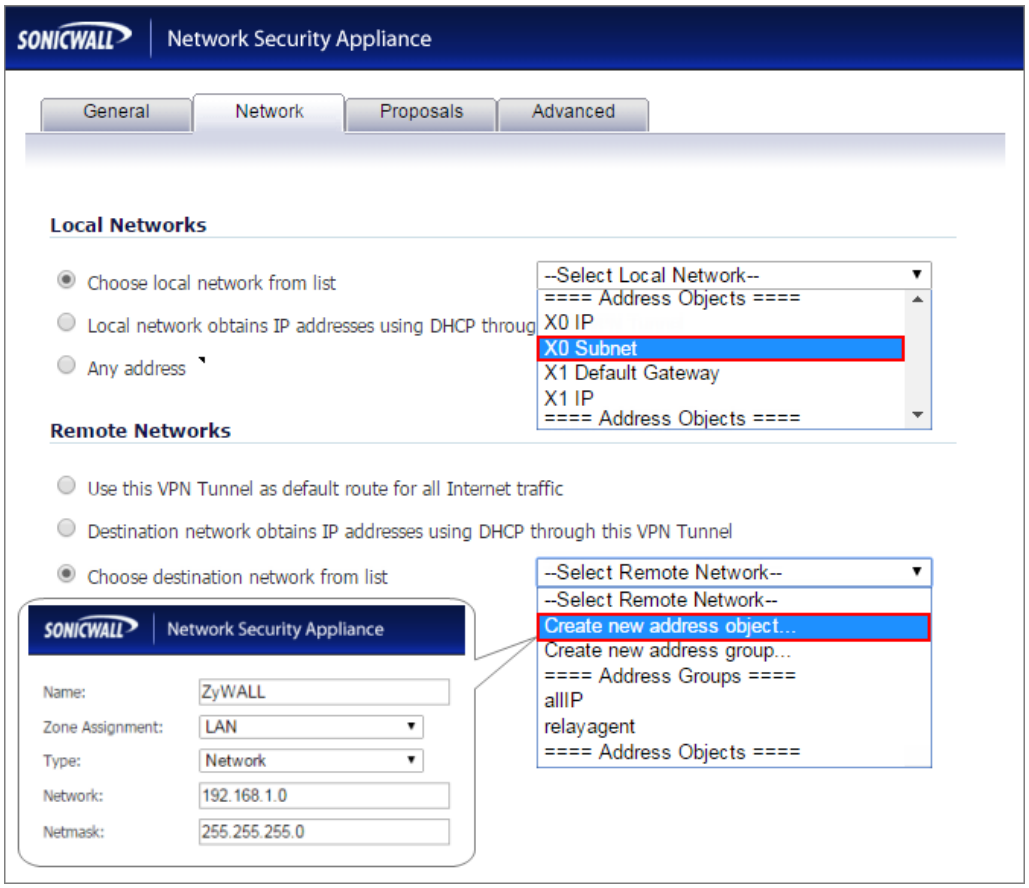
VPN > Settings > VPN Policies > General

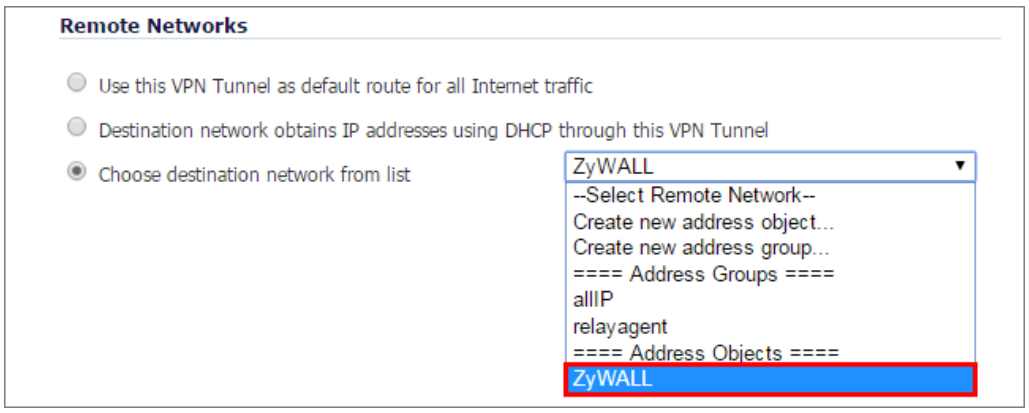


In the SonicWALL **VPN > Settings > VPN Policies > Network**, choose **Local Network** to be the IP address range of the network connected to the **SonicWALL** (found under **SonicWALL > Network > Interfaces > LAN**).

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

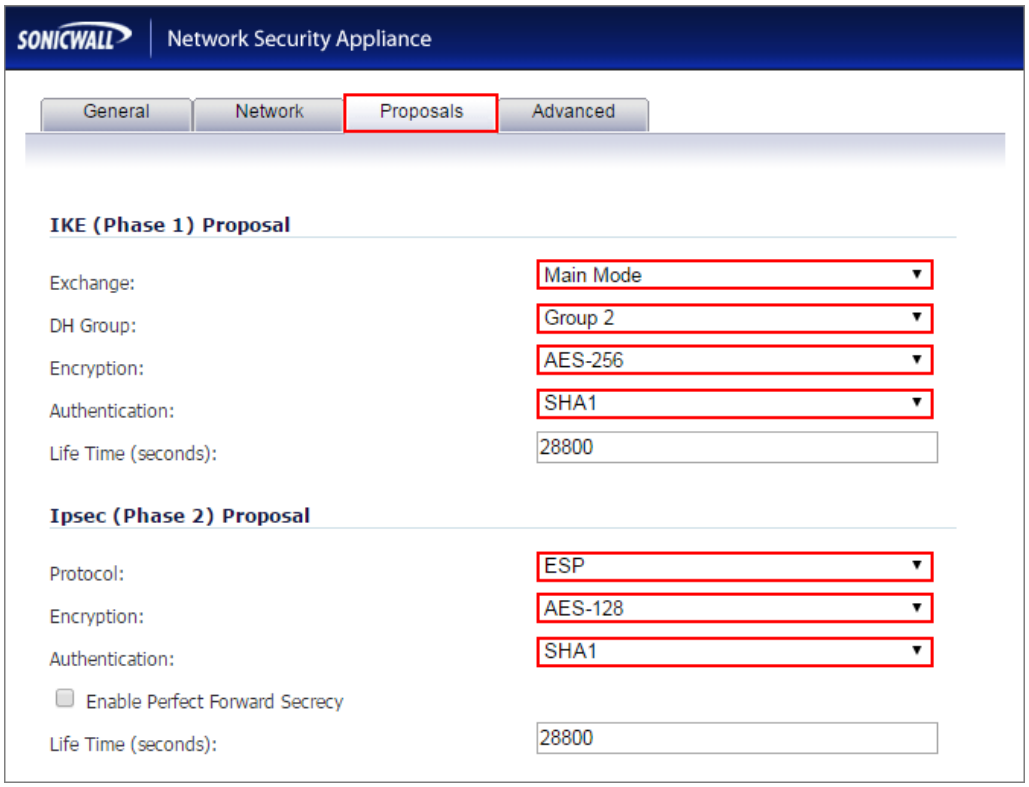




In the SonicWALL **VPN > Settings > VPN Policies > Proposals** > **IKE (Phase 1) Proposal** and set **Exchange**, **DH Group**, **Encryption** and **Authentication** to match your ZyWALL/USG's **VPN Gateway > Show Advanced Settings > Phase 1 Settings**.

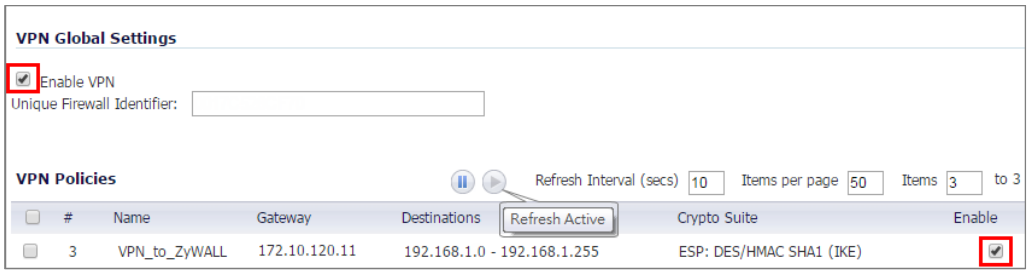
Go to **IKE (Phase 2) Proposal** and set the **Protocol**, **Encryption** and **Authentication** to match your ZyWALL/USG's **VPN Connection > Show Advanced Settings > Phase 2 Settings**.

VPN > Settings > VPN Policies > Proposals



Select **Enable VPN** and click **Refresh Active**.

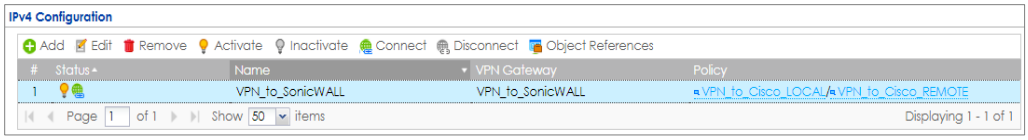
VPN > Settings > VPN Global Settings



Test the IPSec VPN Tunnel

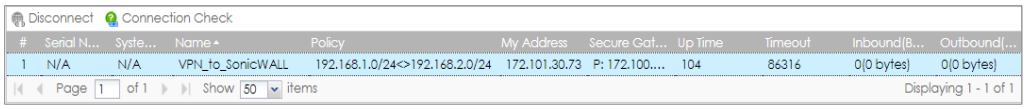
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



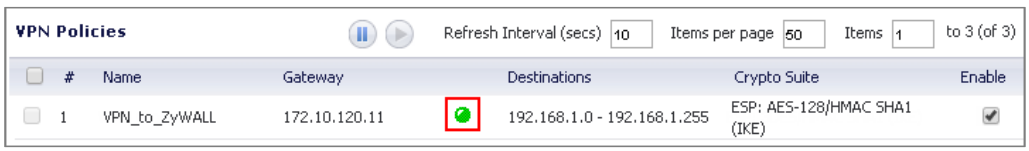
Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > IPSec



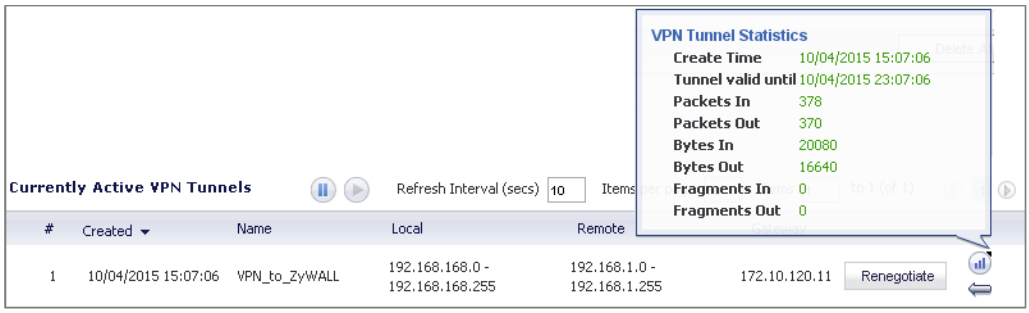
Go to SonicWALL **VPN > VPN Settings > VPN Policies**, the status green light is on.

VPN > VPN Settings > VPN Policies



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



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

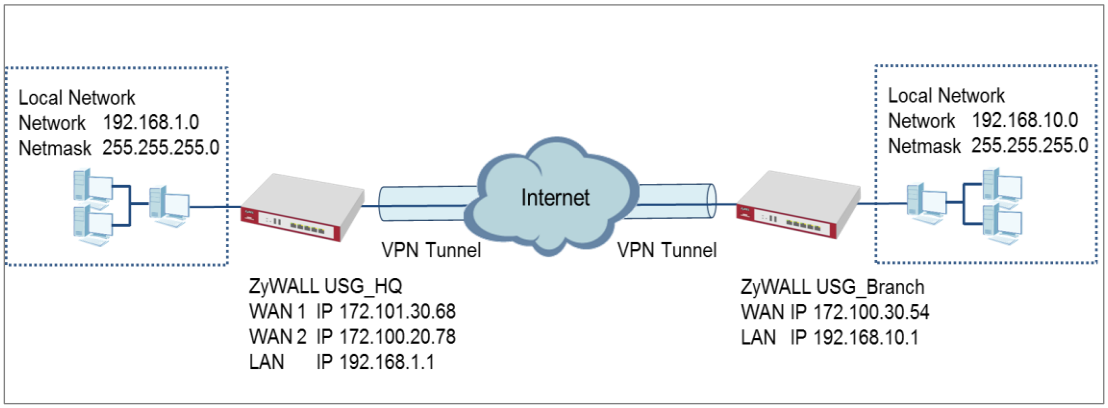
Priority	Category	Message	Source	Destination	Note
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	172.101.30.73:...	172.100.30.80:...	IKE_LOG
info	IKE	[SA] : No proposal chosen	172.101.30.73:...	172.100.30.80:...	IKE_LOG
info	IKE	[SA] : Tunnel [VPN_to_SonicWALL] Phase 2 proposal mismatch	172.101.30.73:...	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.



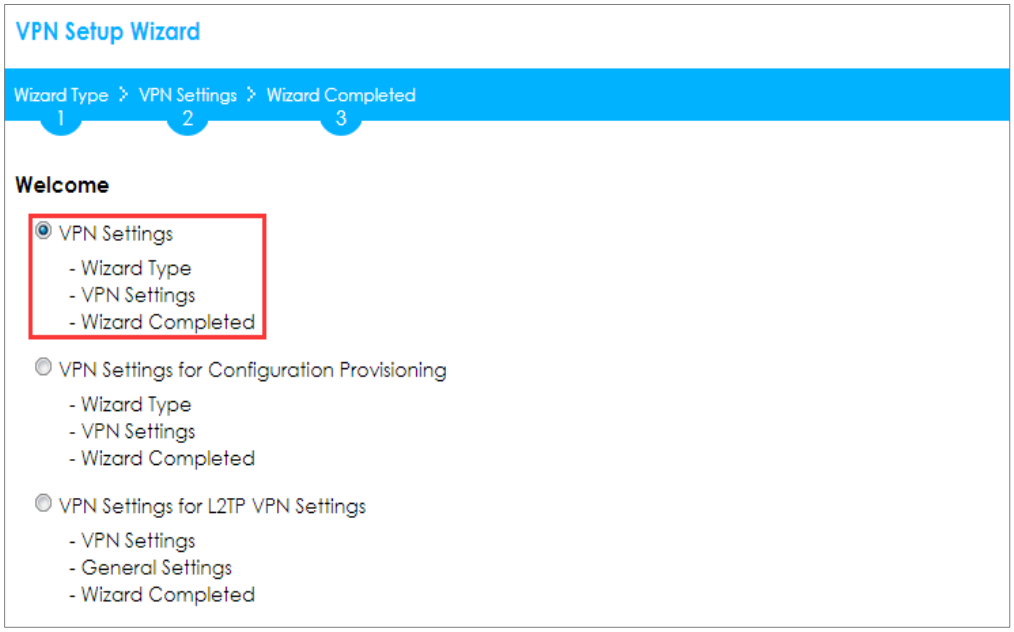
ZyWALL Site-to-site IPSec VPN with multiple WAN failover

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)

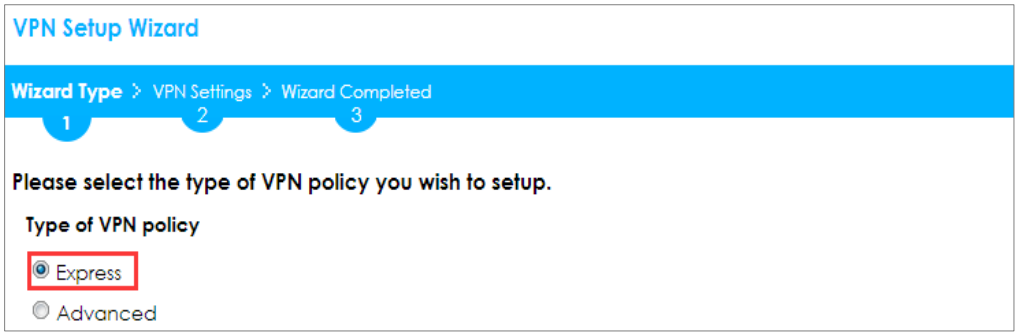
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



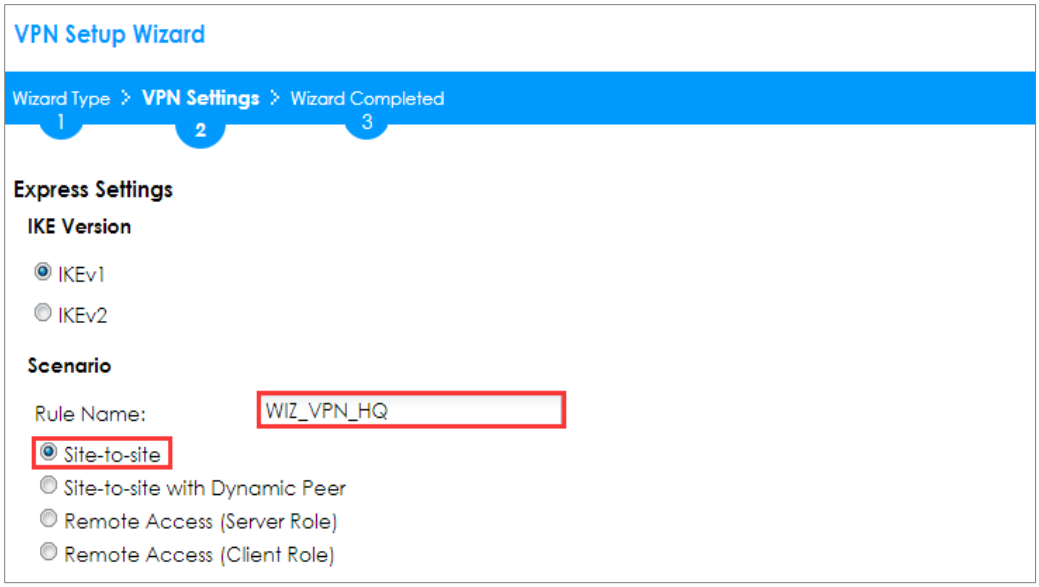
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

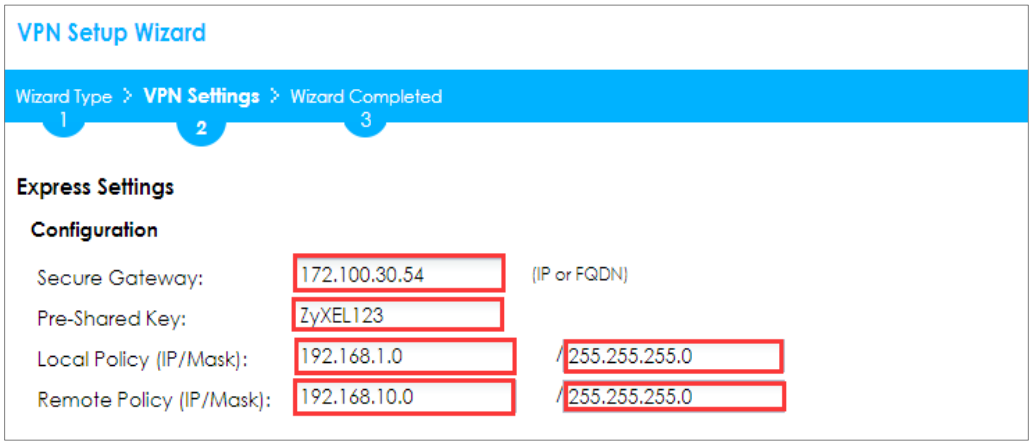
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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).

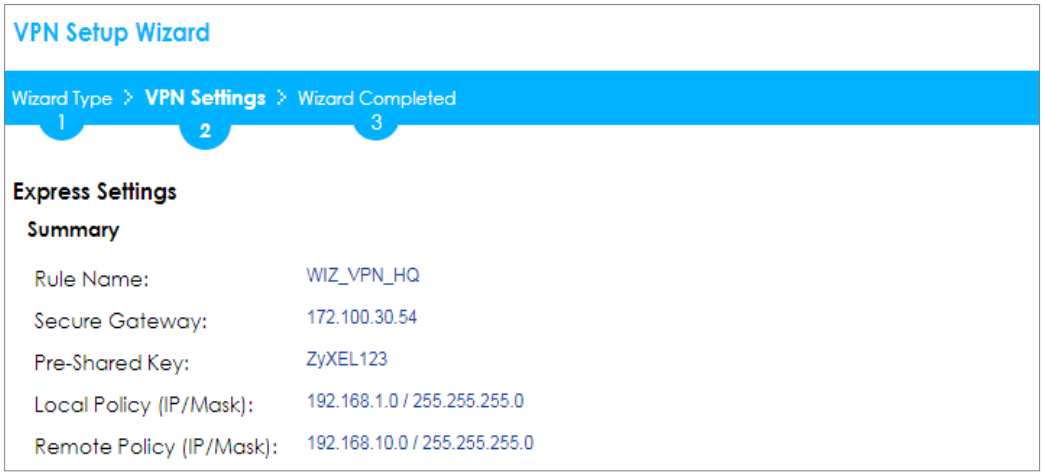
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZyWALL/USG.

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



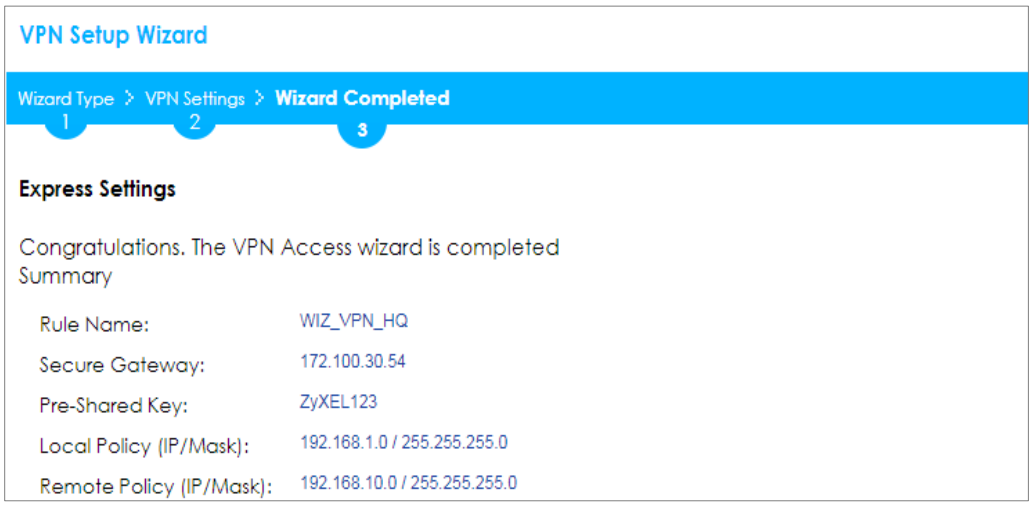
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



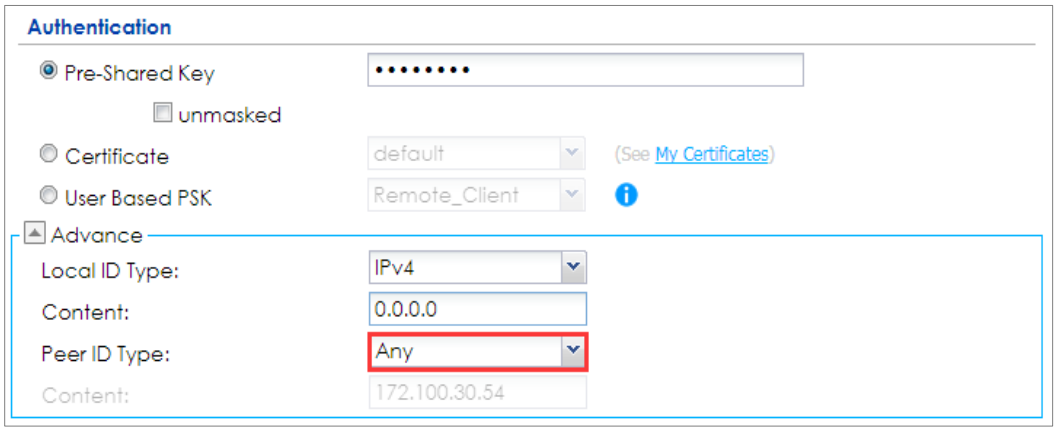
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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.

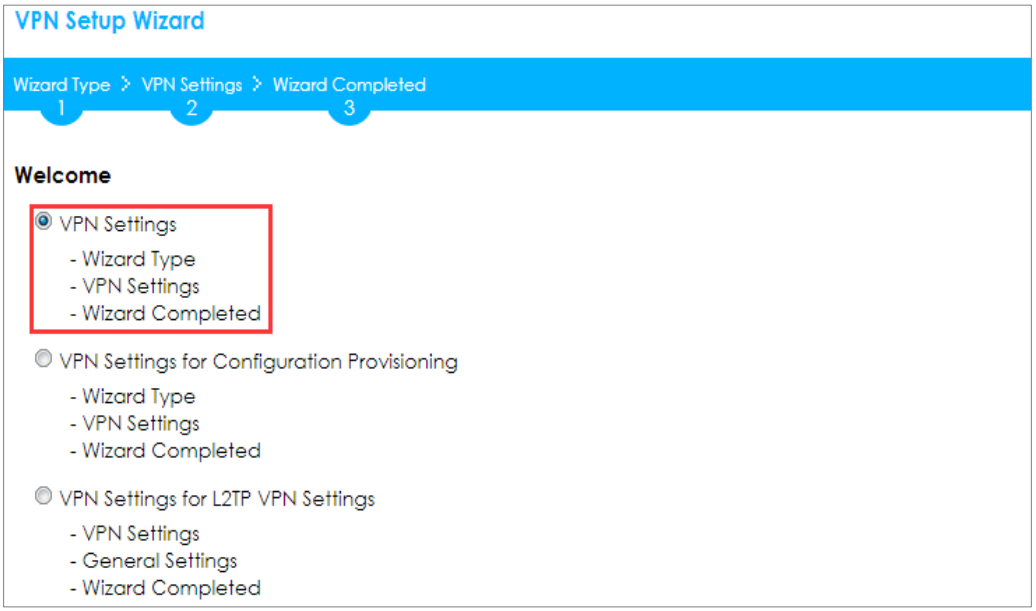
CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



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

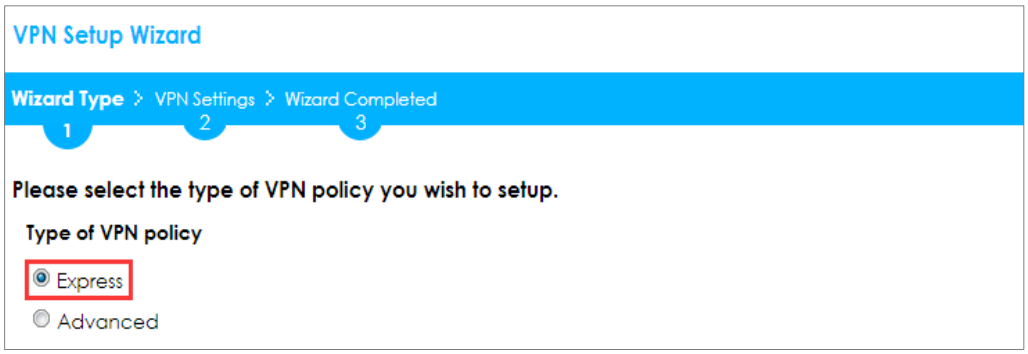
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



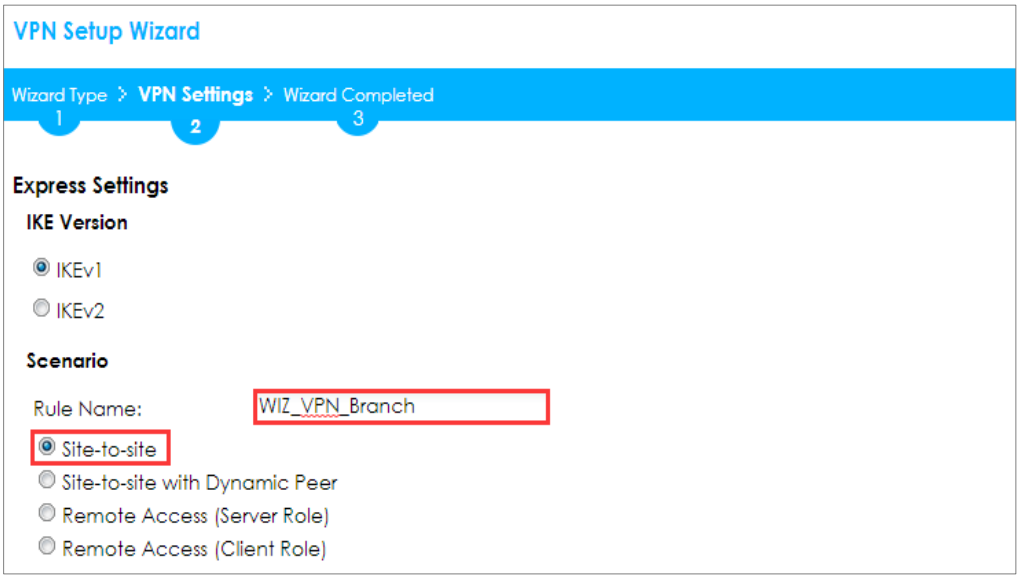
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

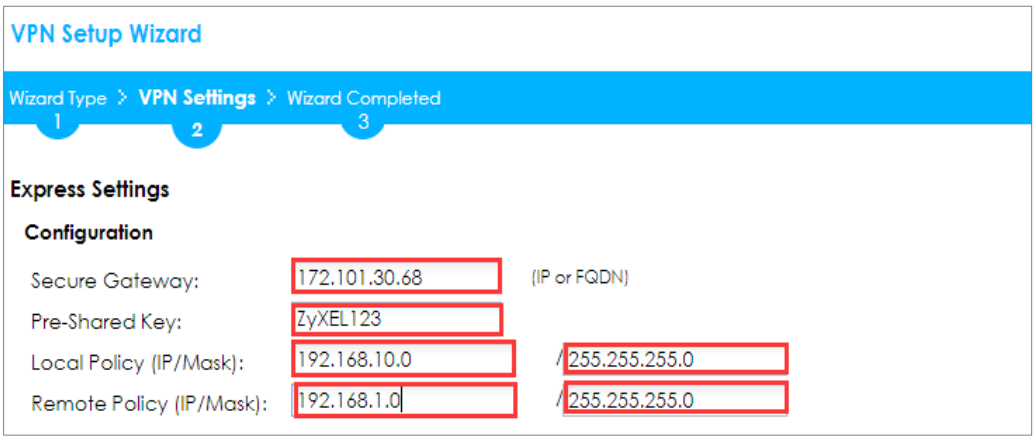
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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).

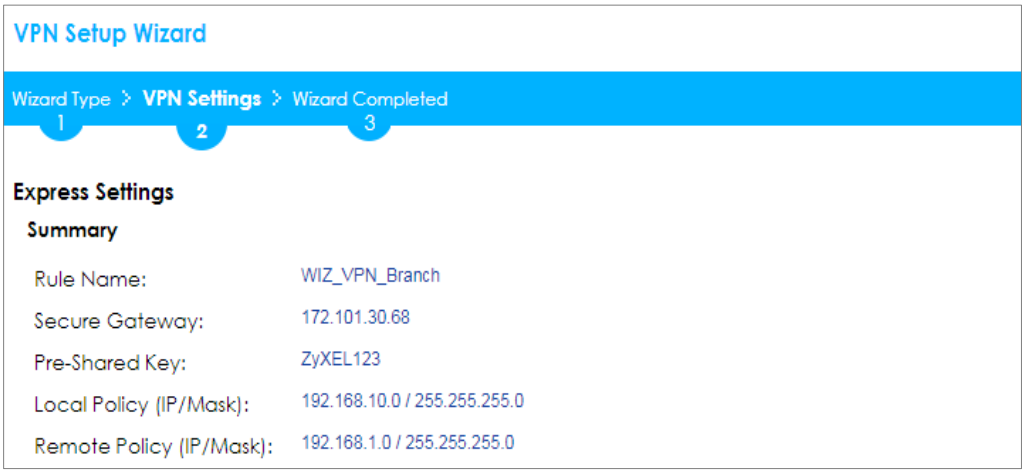
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZYWALL/USG.

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



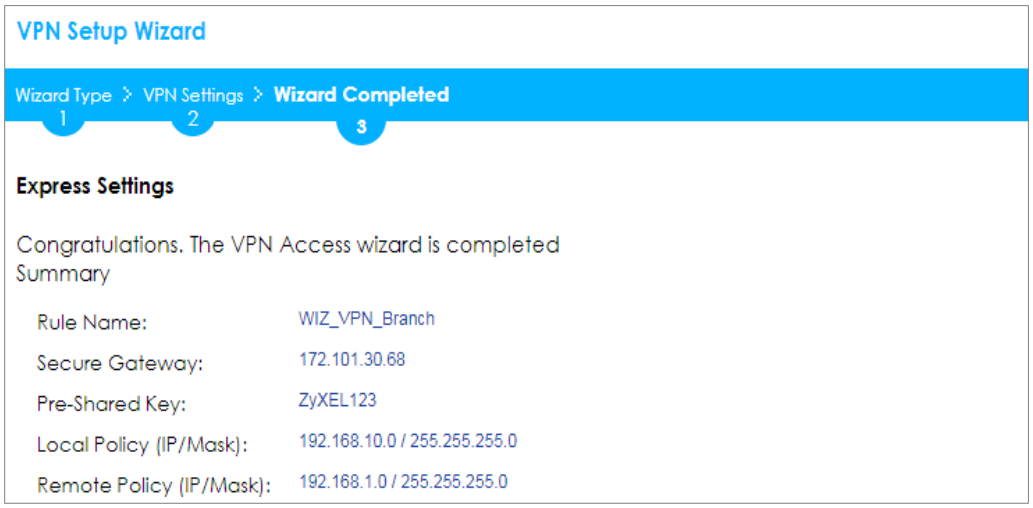
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



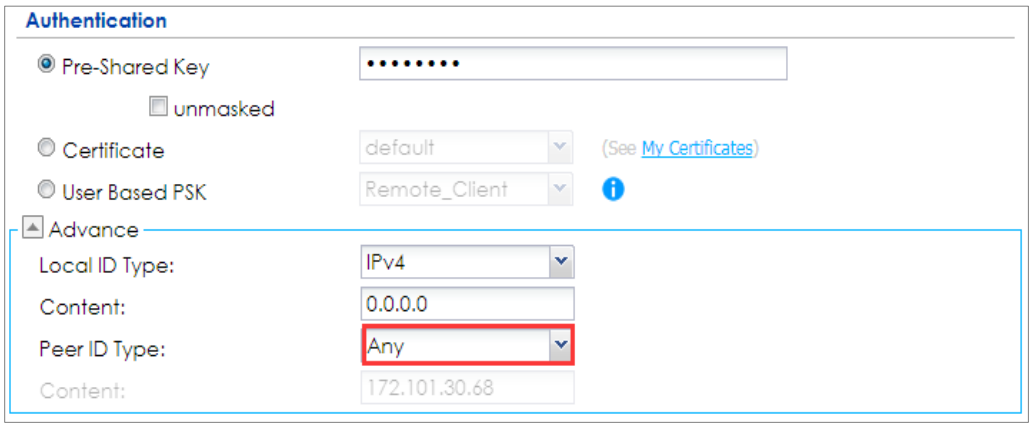
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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



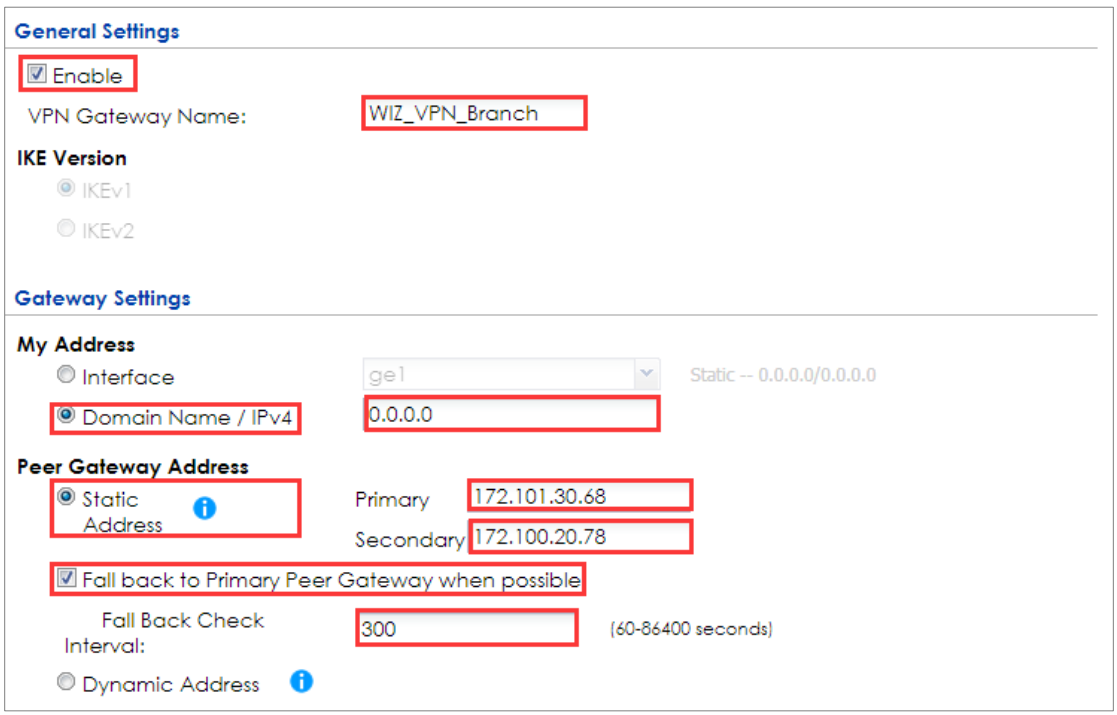
Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. **Configure Authentication > Peer ID Type** as **Any** to let the ZyWALL/USG does not require to check the identity content of the remote IPSec router.

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



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.

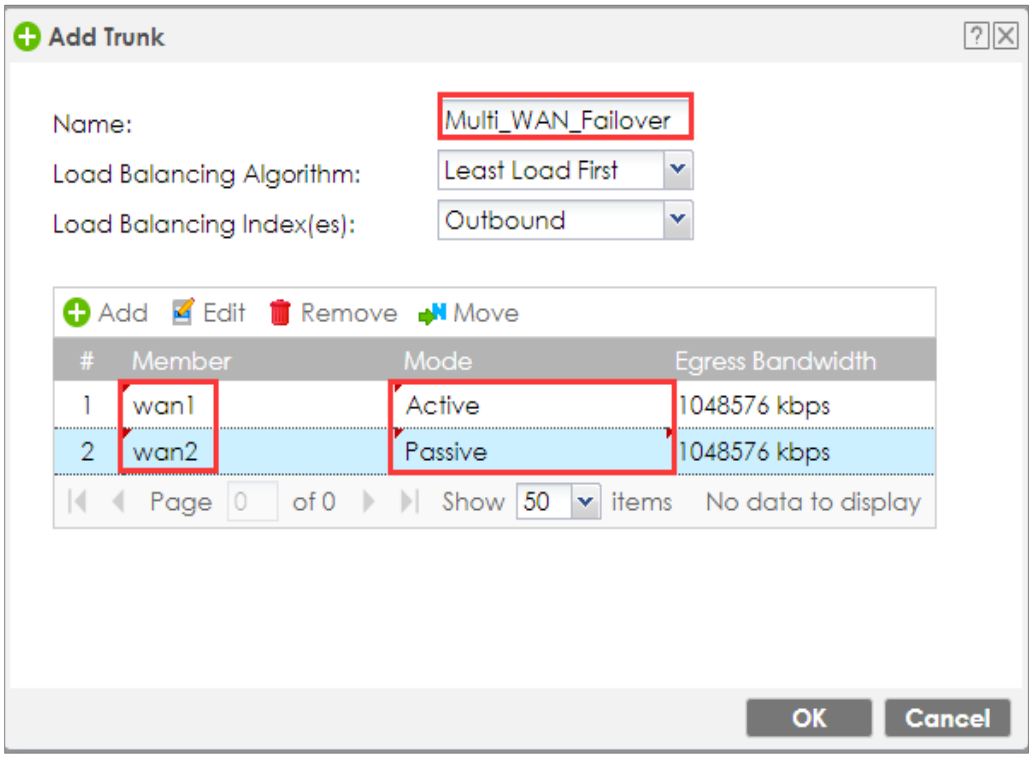
Configuration > VPN > IPSec VPN > VPN Gateway > Gateway Settings



Set up the WAN Trunk (ZyWALL/USG_HQ)

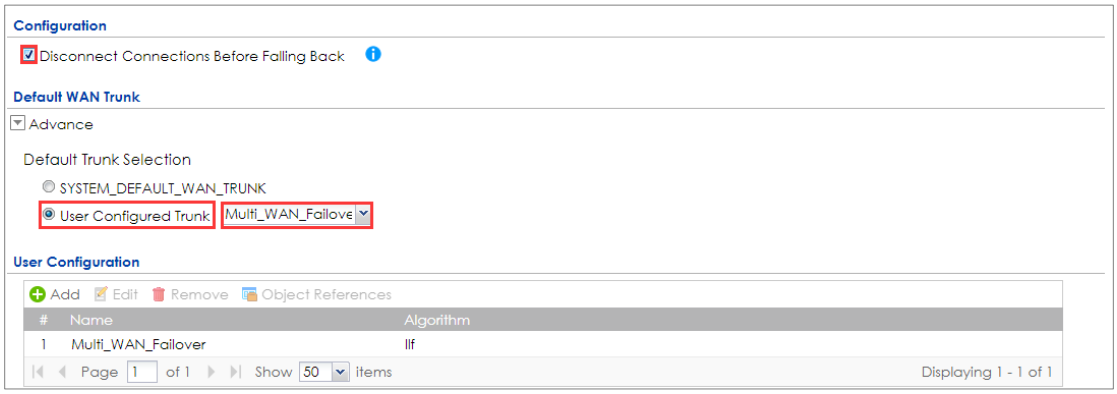
Go to **CONFIGURATION > Interface > Trunk > User Configuration > Add**. Select wan1 and wan2 into the trunk **Member** and set wan2 **Mode** to be **Passive**.

CONFIGURATION > Interface > Trunk > User Configuration > Add



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).

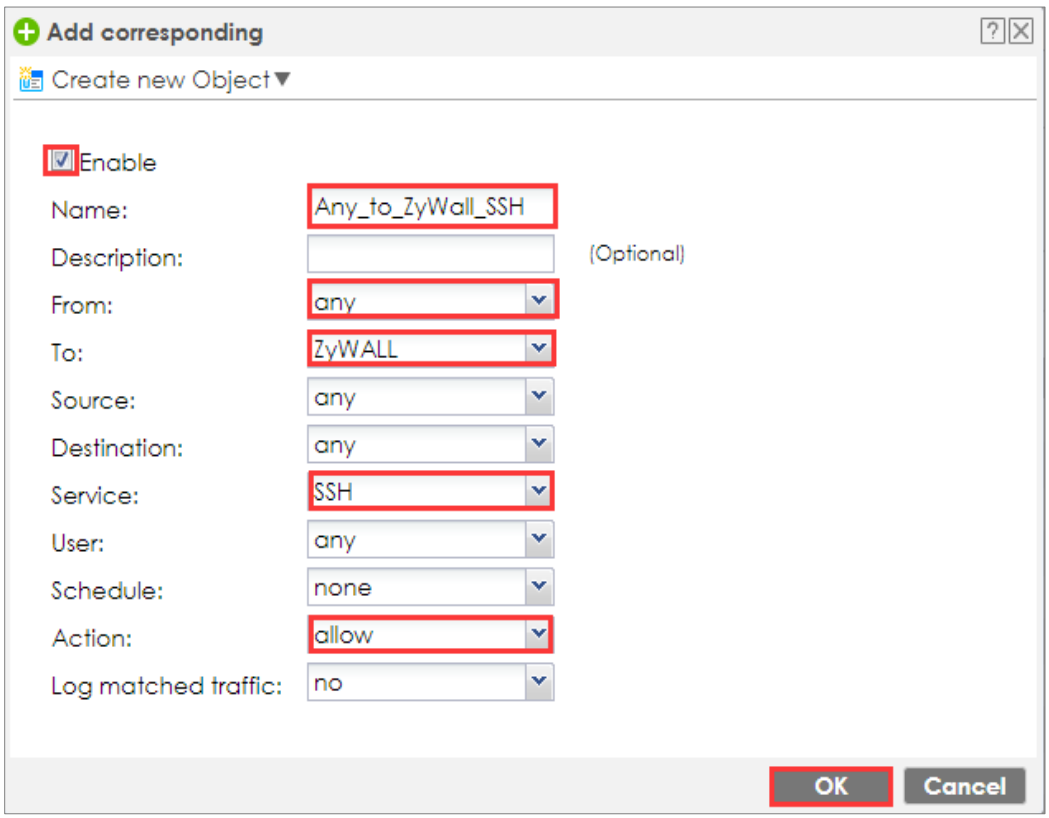
CONFIGURATION > Interface > Trunk > User Configuration > Add



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



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

Enter the command line in terminal mode (Using Tera Term in this example).

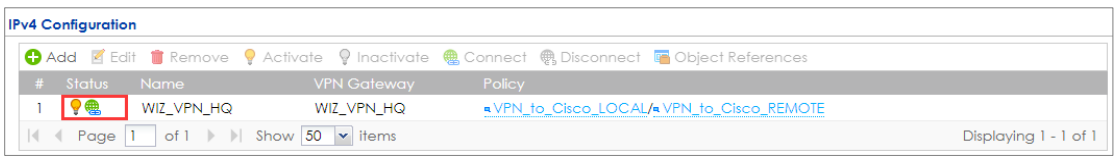
Tera Term command

```
Welcome to USG110

Username: admin
Password:
Router> configure terminal
Router(config)# client-side-vpn-failover-fallback activate
```

Test the IPSec VPN Tunnel

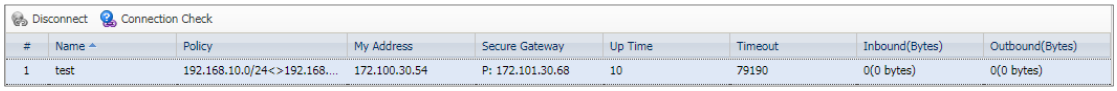
8 Go to ZYWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



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

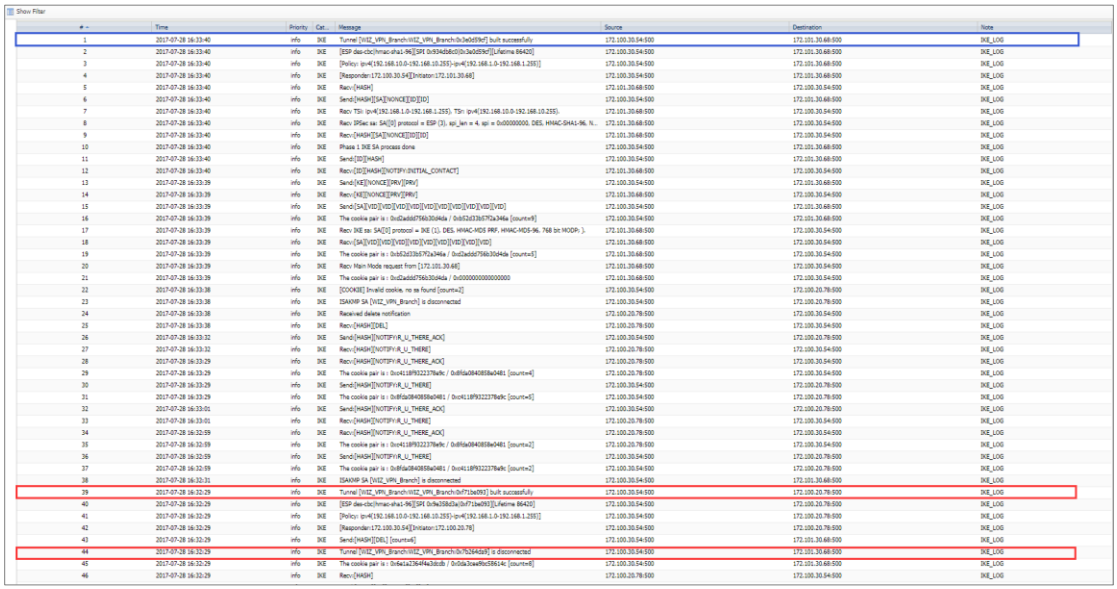


Disconnect | Connection Check

#	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



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

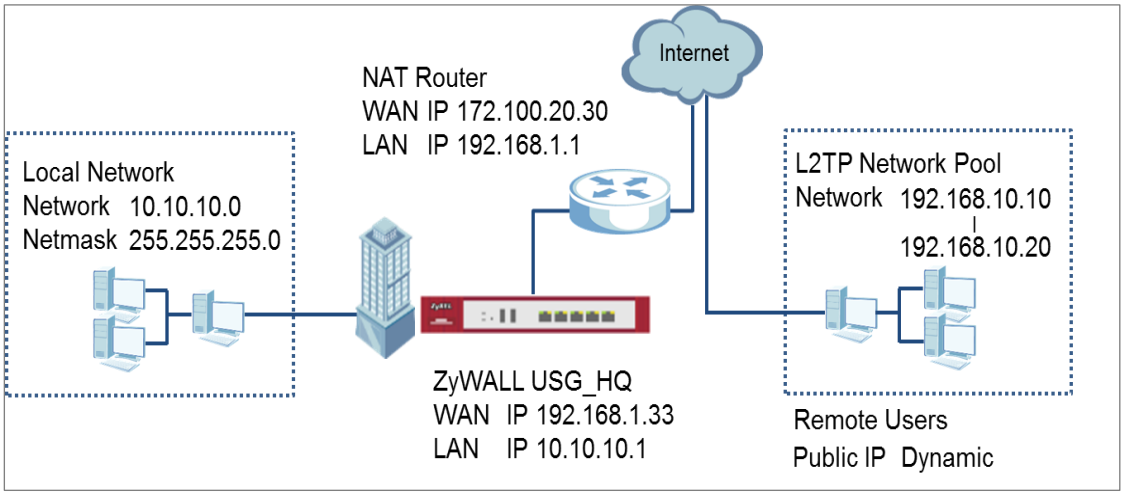
Priority	Category	Message	Note
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [WIZ_VPN_HQ] Phase 2 proposal mismatch	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Phase 1 IKE SA process done	IKE_LOG

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.



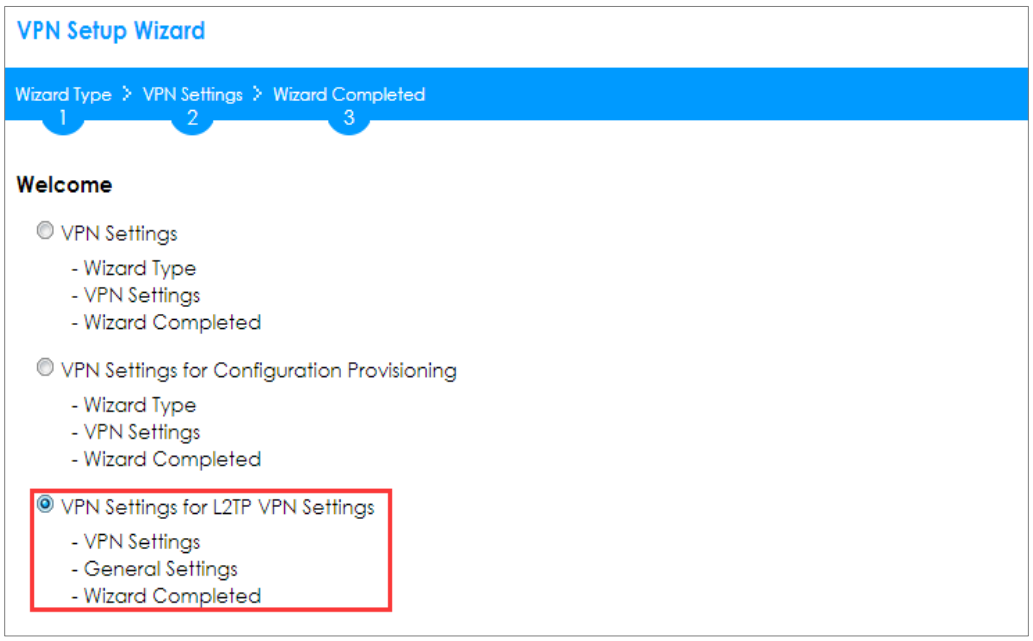
ZyWALL/USG L2TP over IPSec VPN while the ZyWALL/USG is behind a NAT router

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

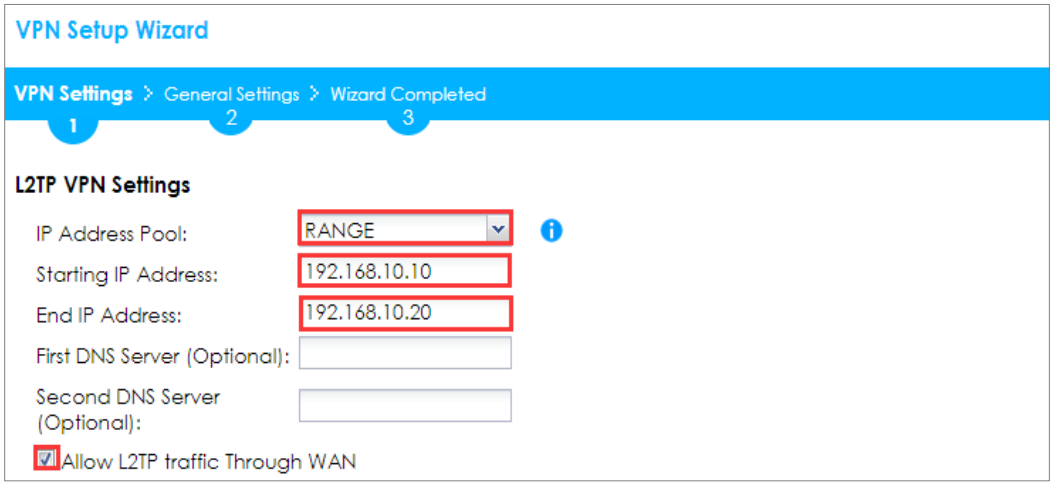


Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

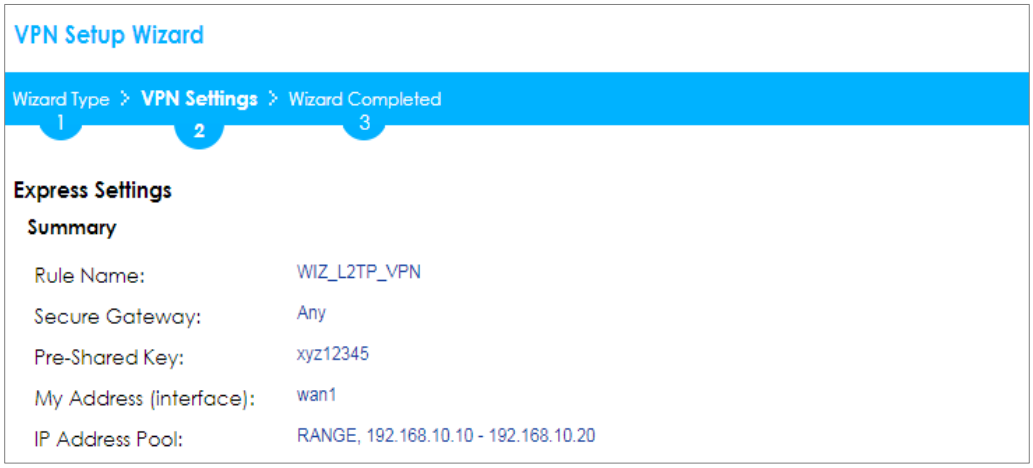
Assign the remote users IP addresses range from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)



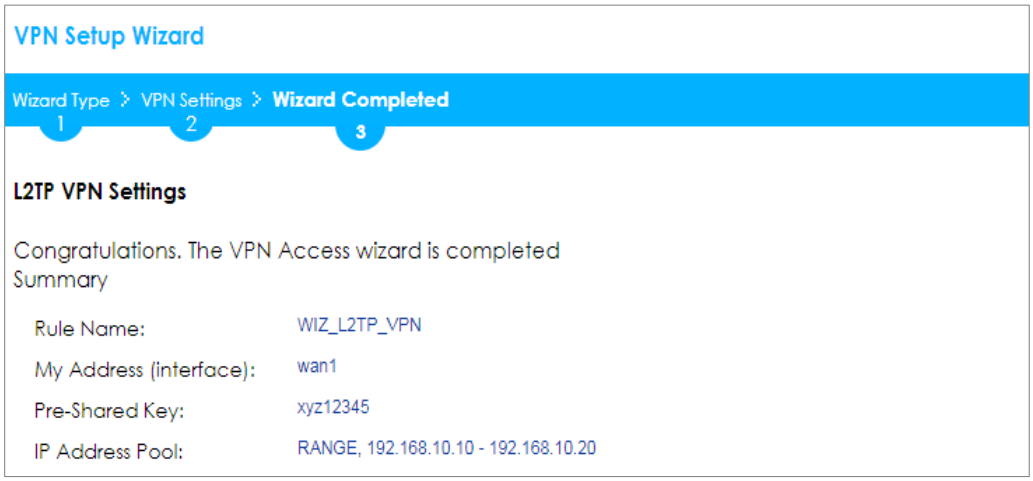
15 This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



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

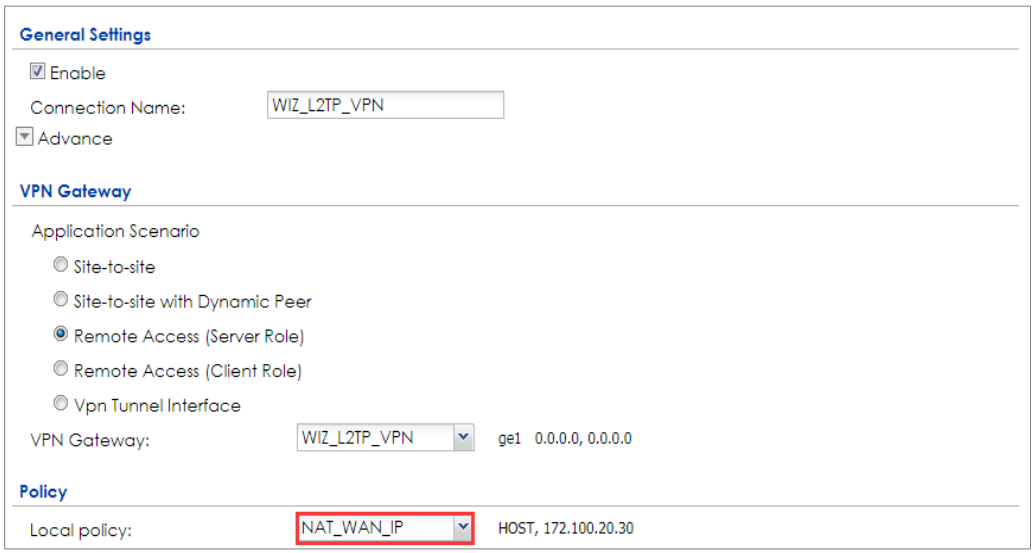


Go to **CONFIGURATION > VPN Connection > Create new Object > Create Address**, create an address object as the NAT router's WAN IP address (in the example, 172.100.20.30).

CONFIGURATION > VPN Connection > Create new Object > Create Address

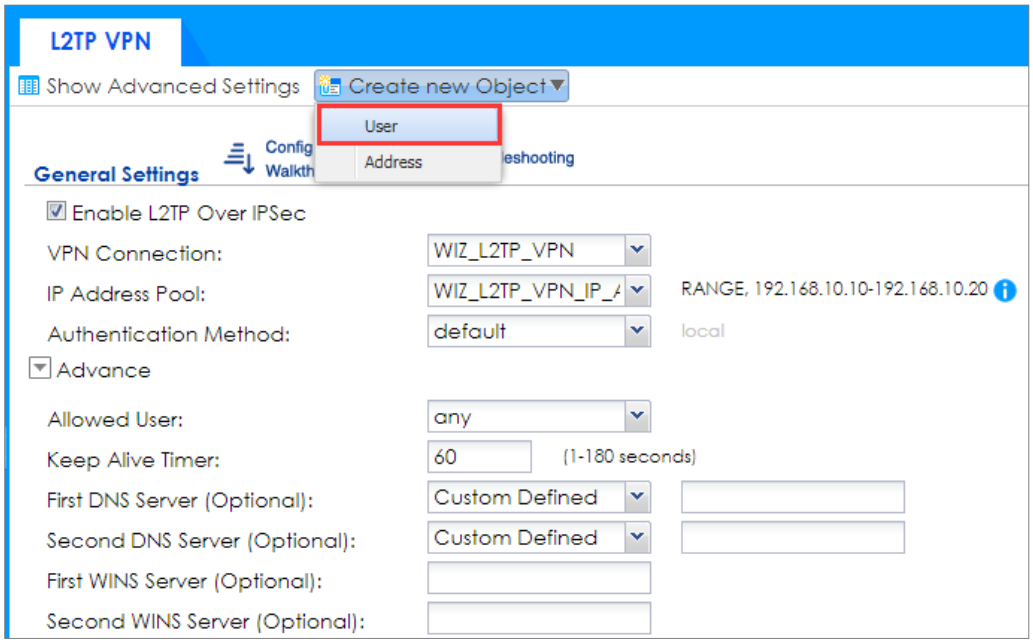
Go to **CONFIGURATION > VPN Connection > Policy > Local Policy**, select it be to the NAT router's WAN IP address (in the example, 172.100.20.30).

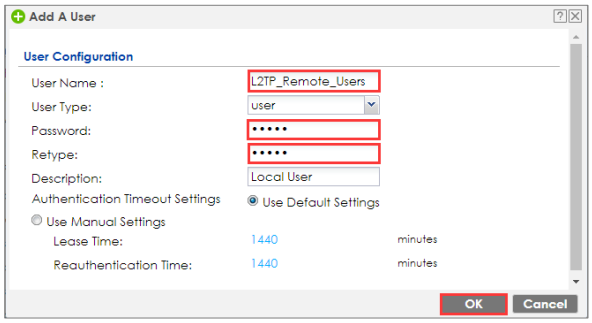
CONFIGURATION > VPN Connection > Policy > Local Policy



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

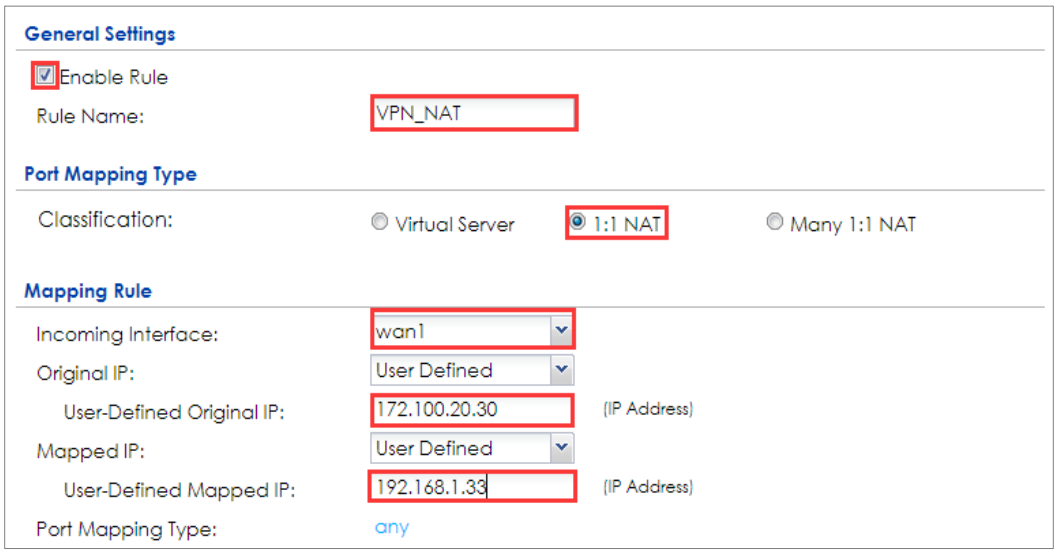




Set Up the NAT Router (Using ZyWALL USG device in this example)

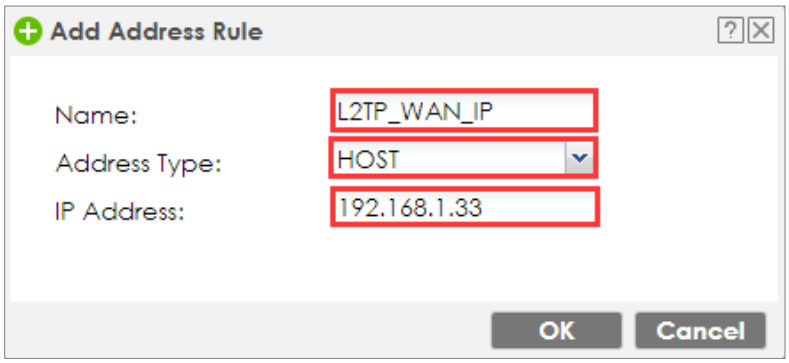
Go to **CONFIGURATION > Network > NAT > Add**. Select the **Incoming Interface** on which packets for the NAT rule must be received. Specified the **User-Defined Original IP** field and Type the translated destination IP address that this NAT rule supports.

CONFIGURATION > Network > NAT > Add



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



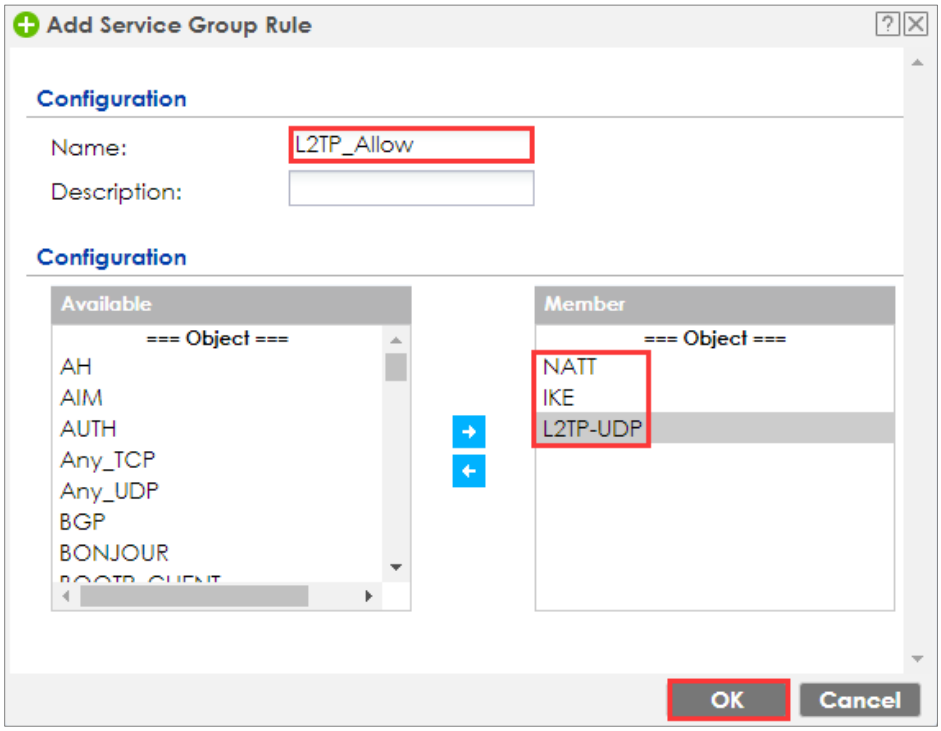
Go to **CONFIGURATION > Object > Service > Service Group**, create a service group for the following UDP ports:

UDP Port Number = 1701 → Used by L2TP

UDP Port Number = 500 → Used by IKE

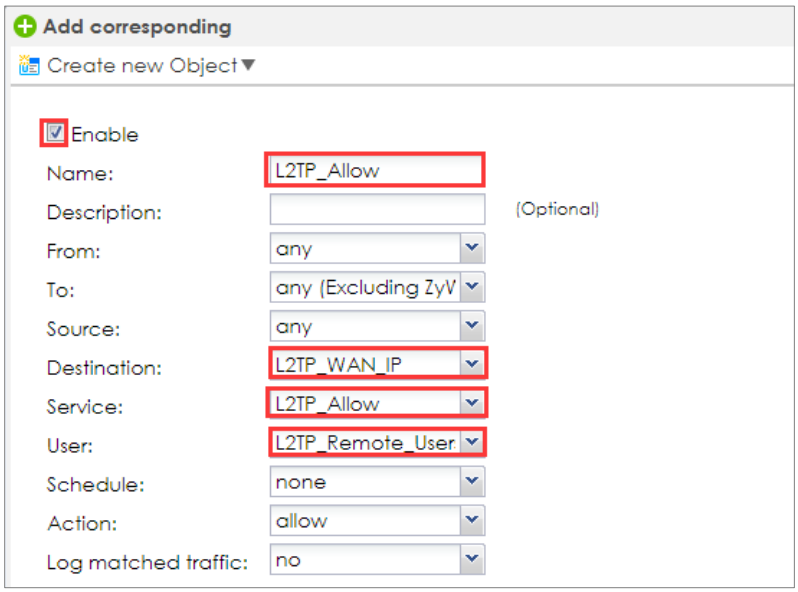
UDP Port Number = 4500 → Used by NAT-T

CONFIGURATION > Service > Service Group



Go to **CONFIGURATION > Security Policy > Policy Control**, add corresponding rule to allow L2TP services.

CONFIGURATION > Security Policy > Policy Control



Test the L2TP over IPSec VPN Tunnel

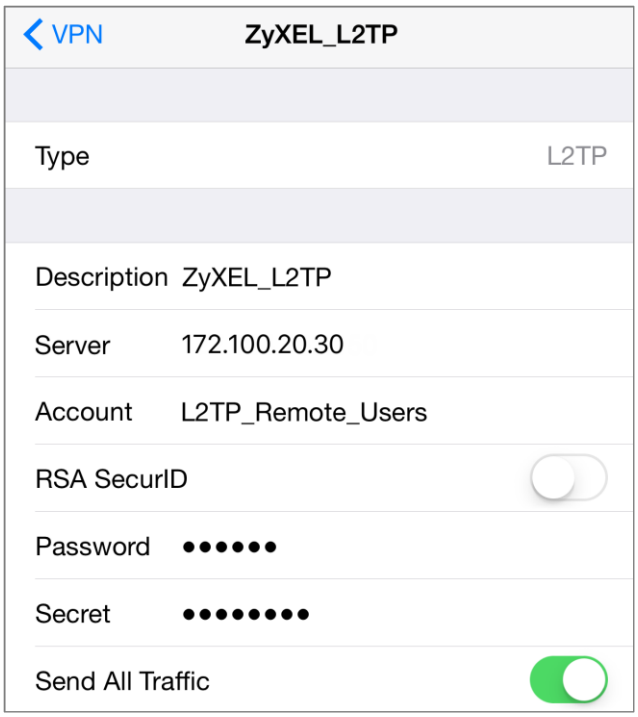
Use a smartphone or a PC to establish a L2TP VPN connection to the ZyWALL/USG. Configure the NAT's public IP address as the L2TP server address on the client. In this example using iOS device to test the result:

To configure L2TP VPN in an iOS 8.4 device, go to **Menu > Settings > VPN > Add VPN Configuration** and configure as follows.

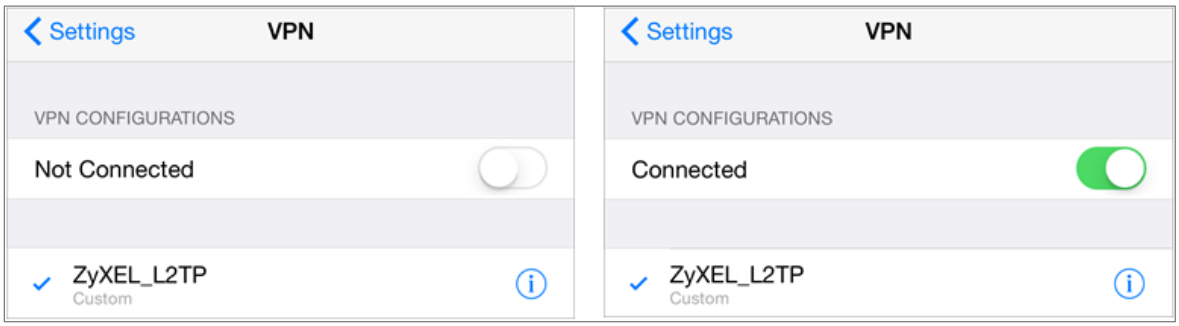
Description is for you to identify the VPN configuration.

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).



After you create a VPN configuration, slide the button right to the on position to initiate L2TP VPN session.

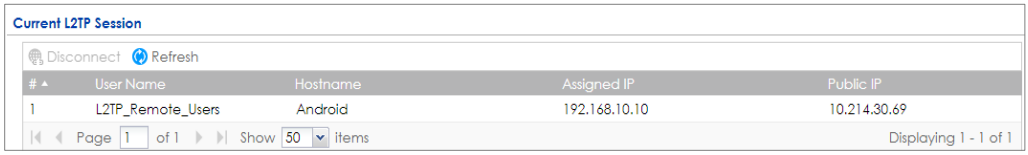


Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, click **Connect** on the upper bar. The **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

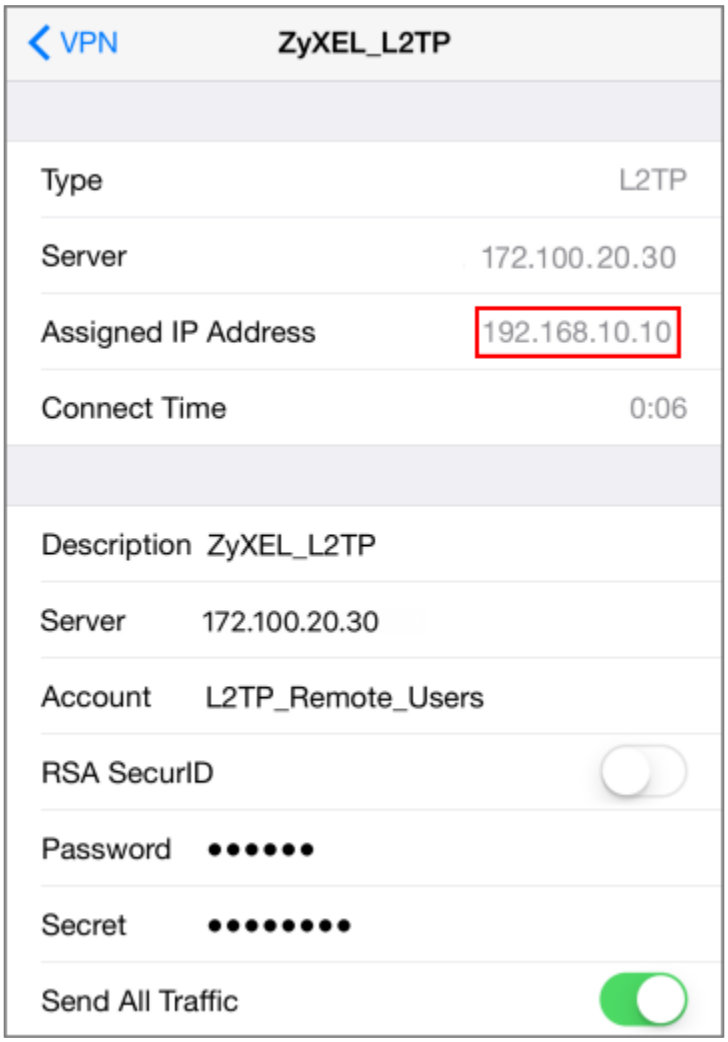
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users



Go to iOS mobile device **Menu > Settings > VPN > ZyXEL_L2TP** and verify the **Assigned IP Address** and **Connect Time**.

Menu > Settings > VPN > ZyXEL_L2TP



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.

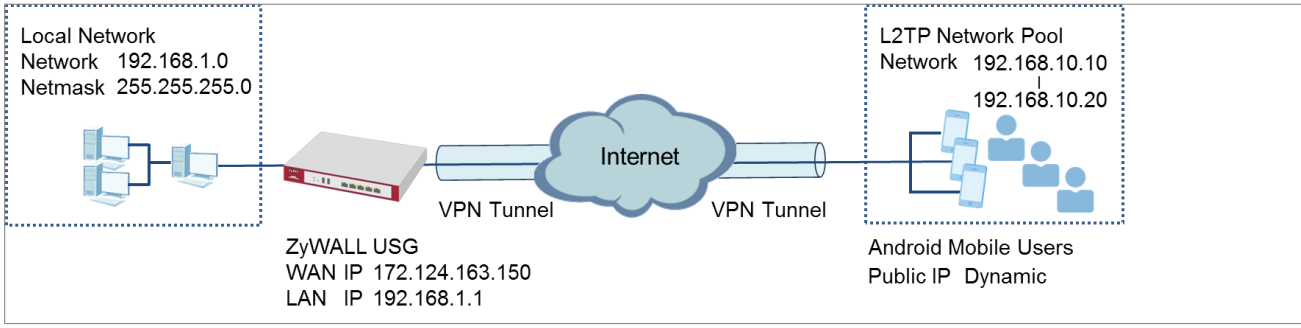
If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

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.



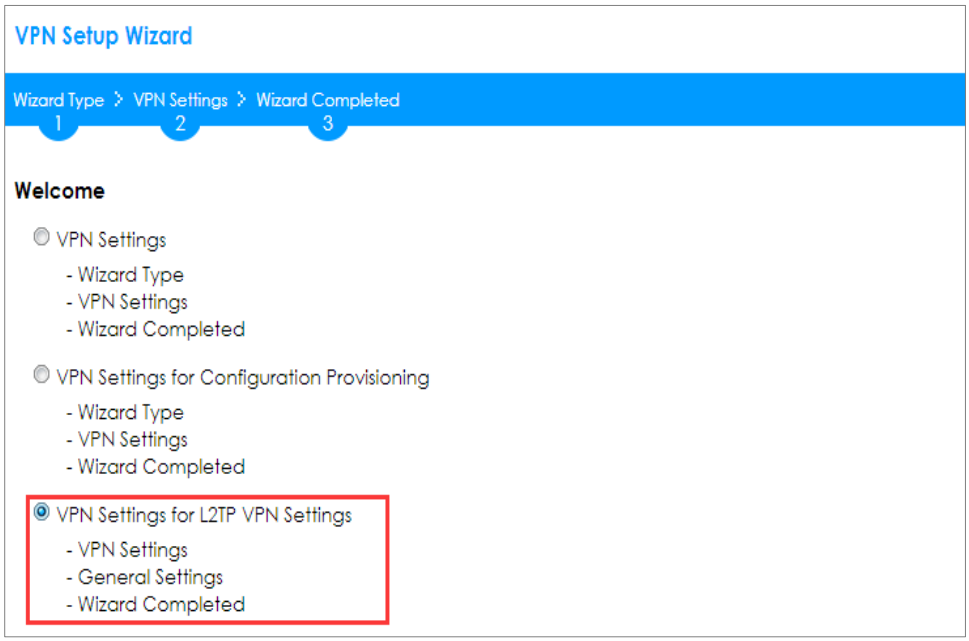
ZyWALL/USG L2TP VPN with Android Mobile Devices Example

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

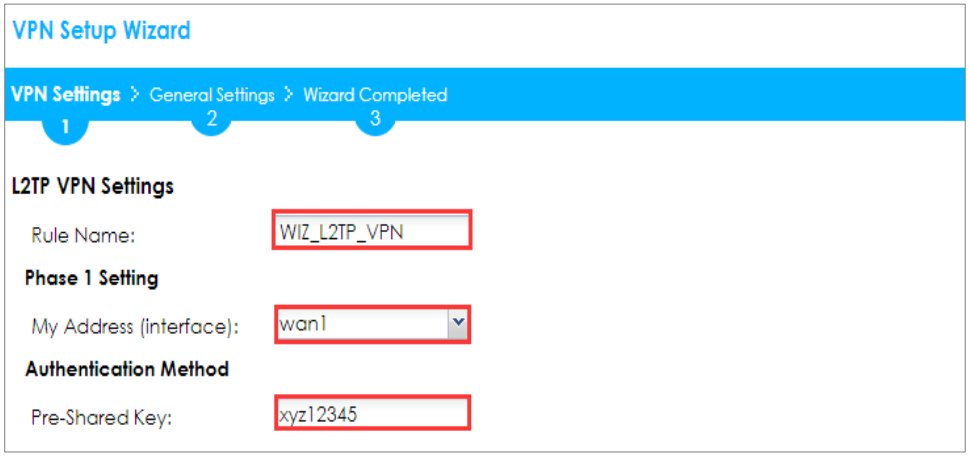
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the remote Android Mobile Devices. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



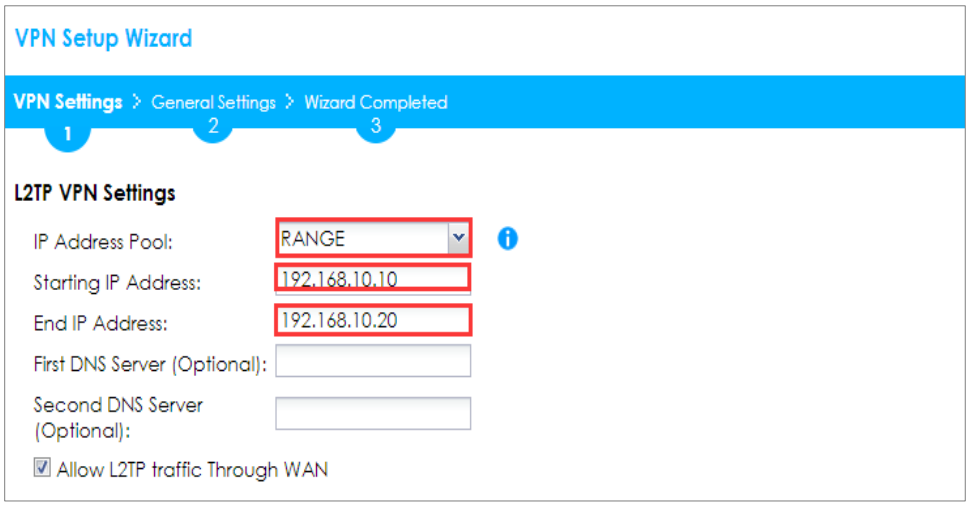
Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



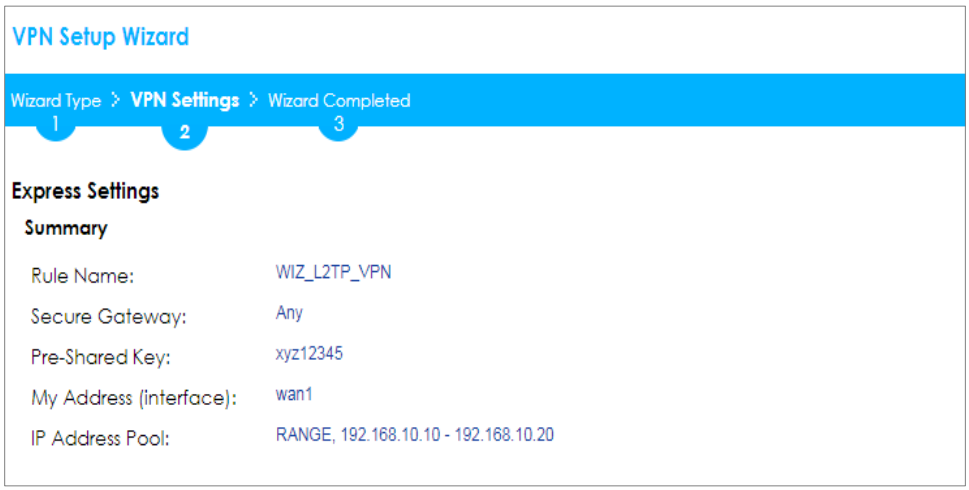
Assign the remote users IP addresses range from 192.168.10.10 to 192.168.10.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)



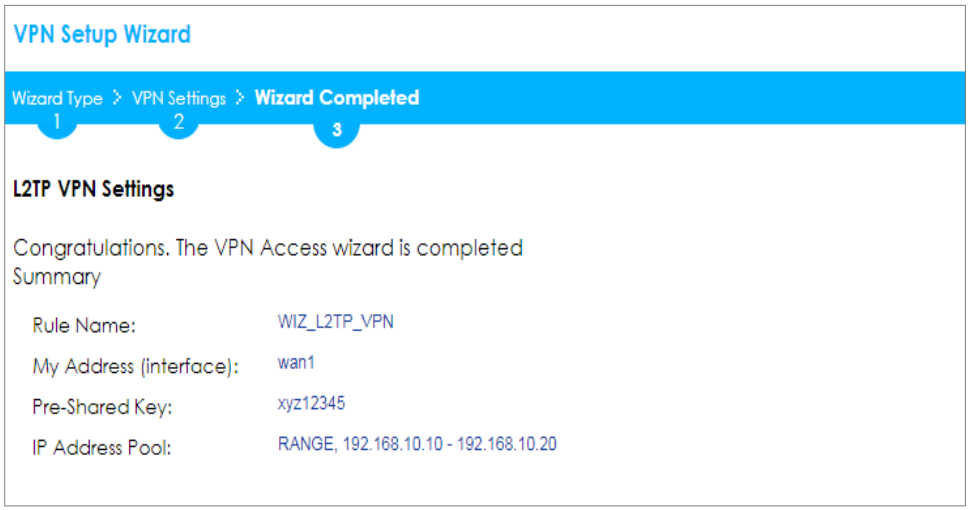
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



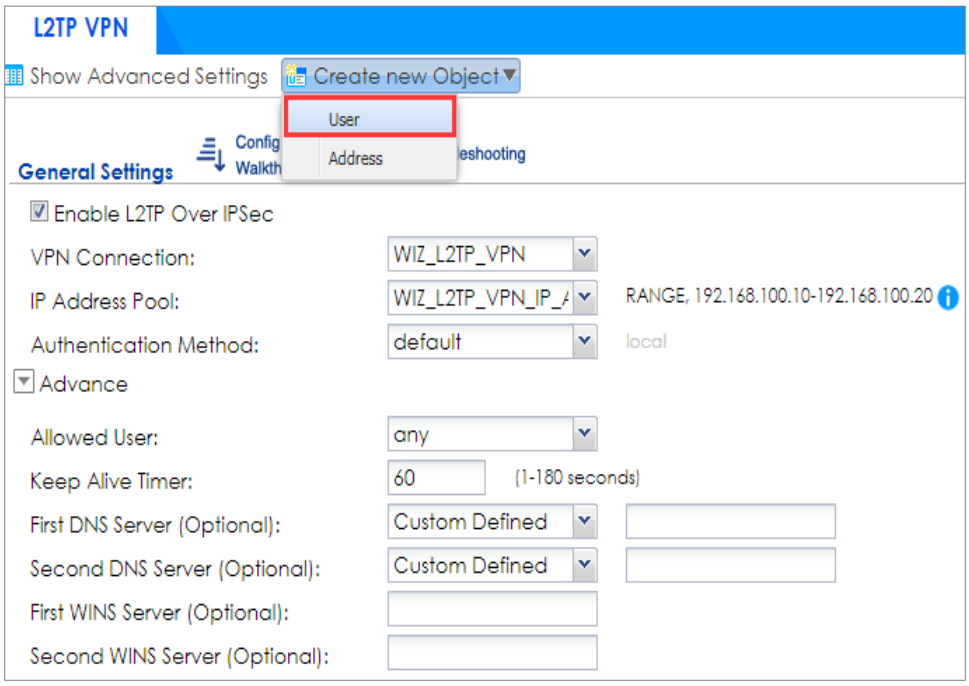
Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

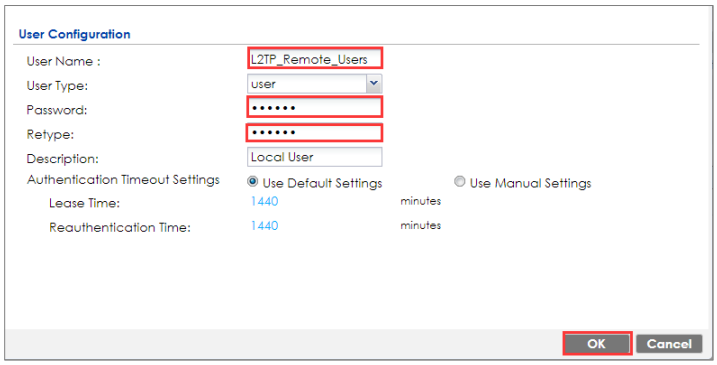
Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Wizard Completed



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).

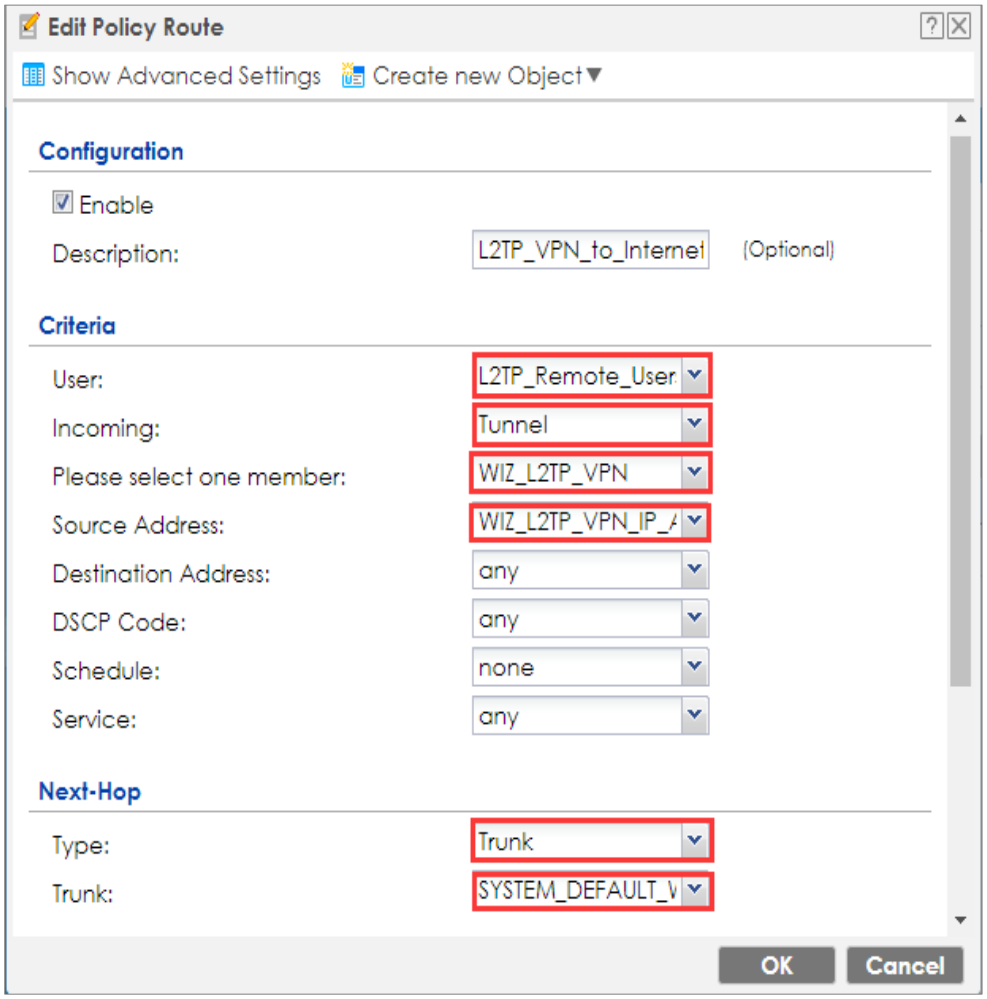
CONFIGURATION > VPN > L2TP VPN > Create new Object > User





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.

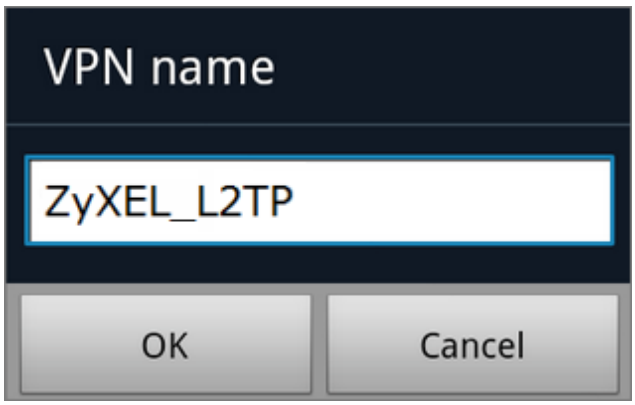
CONFIGURATION > Network > Routing > Policy Route



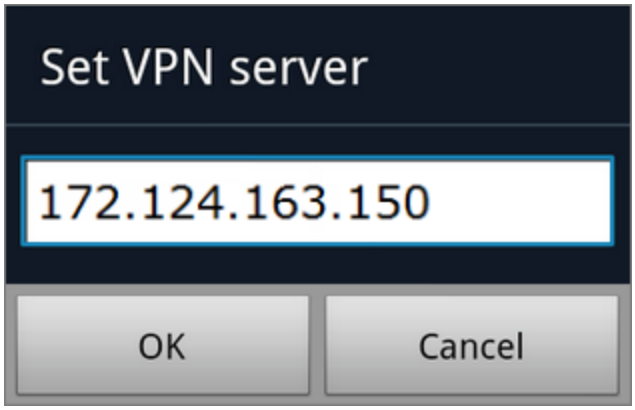
Set Up the L2TP VPN Tunnel on the Android Device

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.

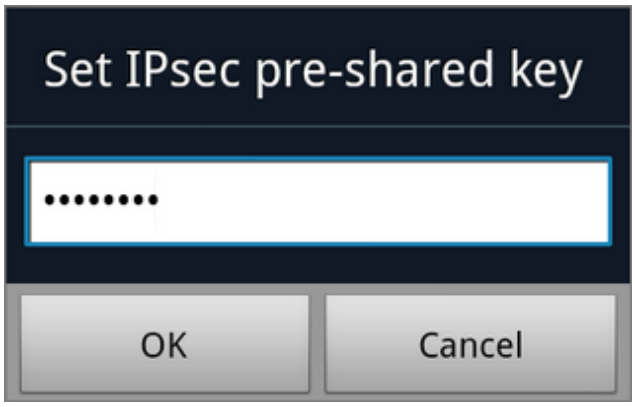
VPN name is for the user to identify the VPN configuration.



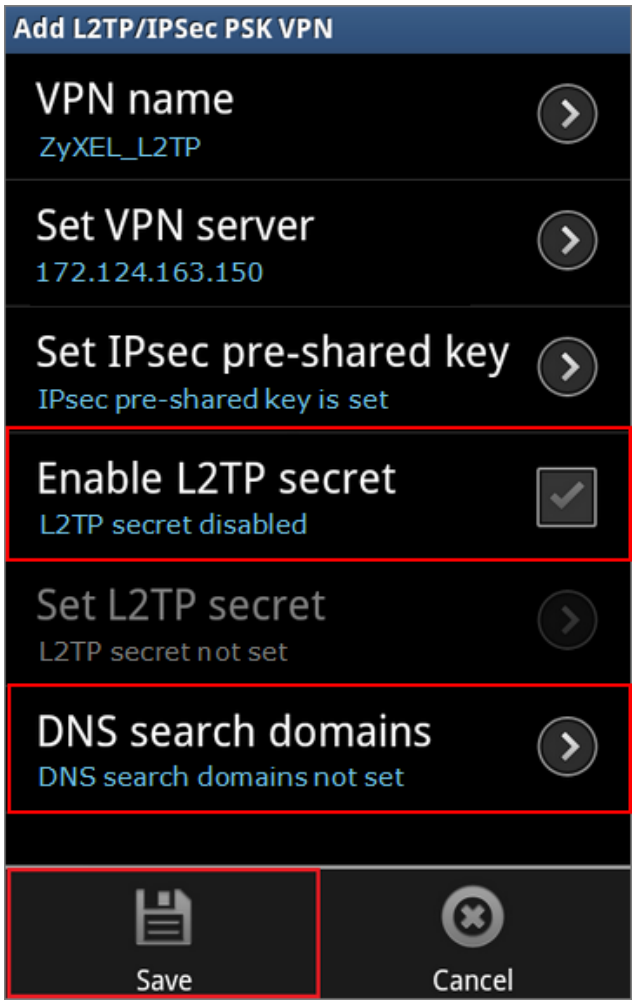
Set **VPN server** to the ZyWALL/USG's WAN IP address.



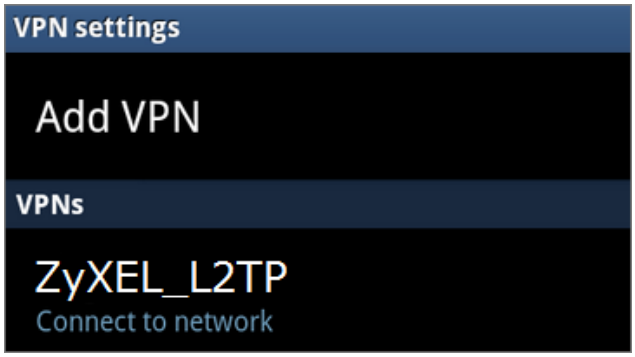
Set **IPSec pre-shared key** to the pre-shared key of the IPSec VPN gateway the ZyWALL/USG uses for L2TP VPN over IPSec (zyx12345 in this example).



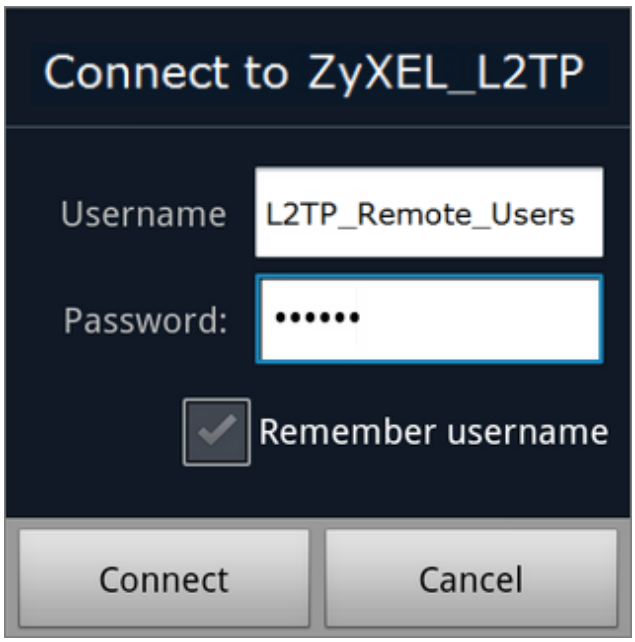
Leave **Enable L2TP secret disabled** as default and turn on **DNS search domains** if you need to use the internal DNS servers once your connection is made, enter the DNS server address here. Click **Save**.



Click the VPN rule **ZyXEL_L2TP** to begin the VPN connection.



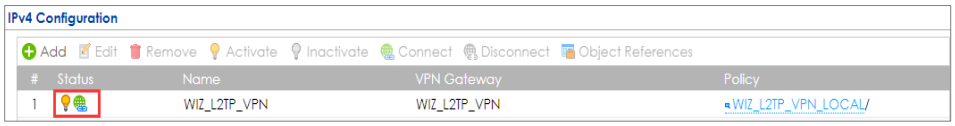
When dialing the L2TP VPN, the user will have to enter Username/Password. They are the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).



Test the L2TP over IPSec VPN Tunnel

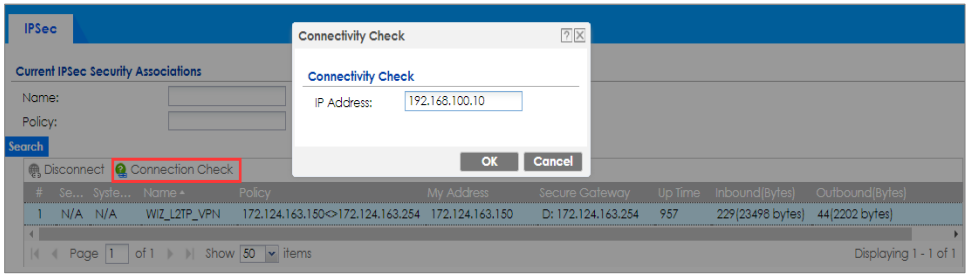
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

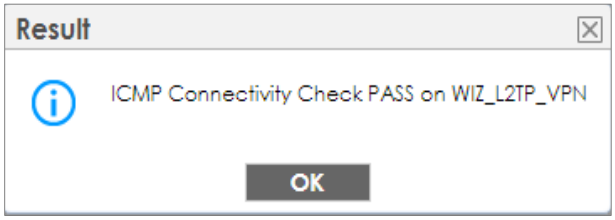
CONFIGURATION > VPN > IPSec VPN > VPN Connection



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.

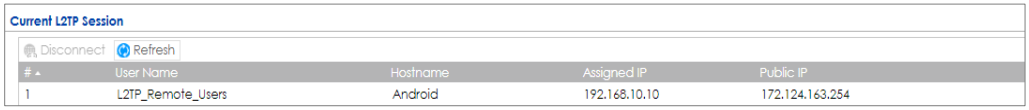
Hub_HQ > MONITOR > VPN Monitor > WIZ_L2TP_VPN





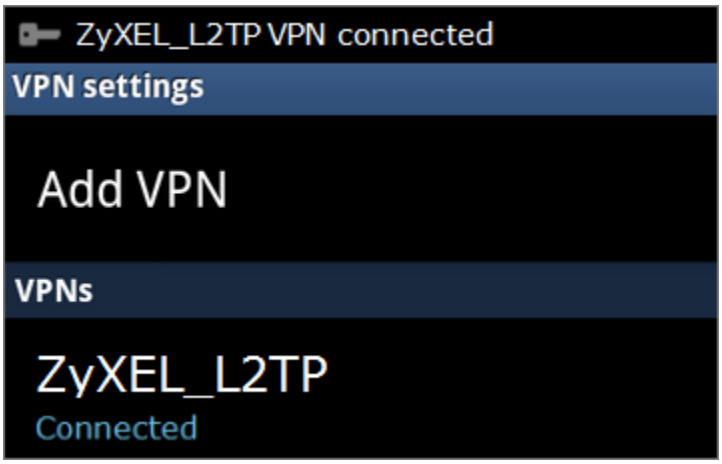
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users



Go to Android mobile device **Menu > Settings > Wireless & Networks > VPN** and verify the connection status.

Menu > Settings > Wireless & Networks > VPN



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.

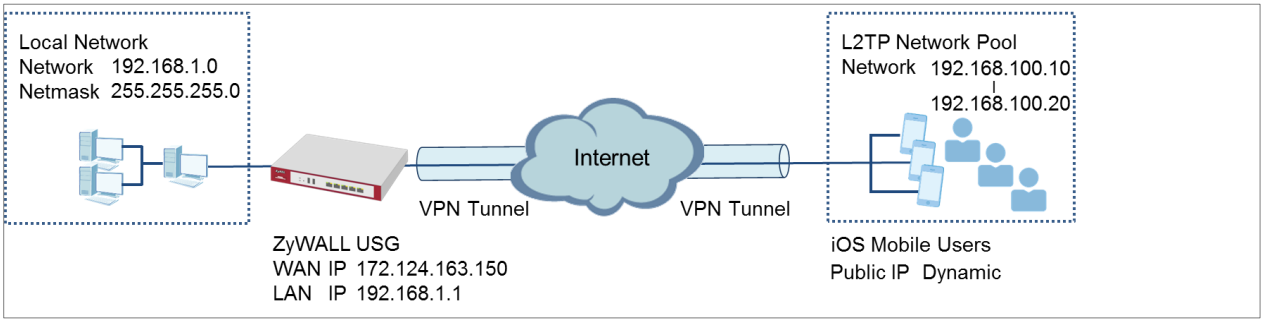
Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

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

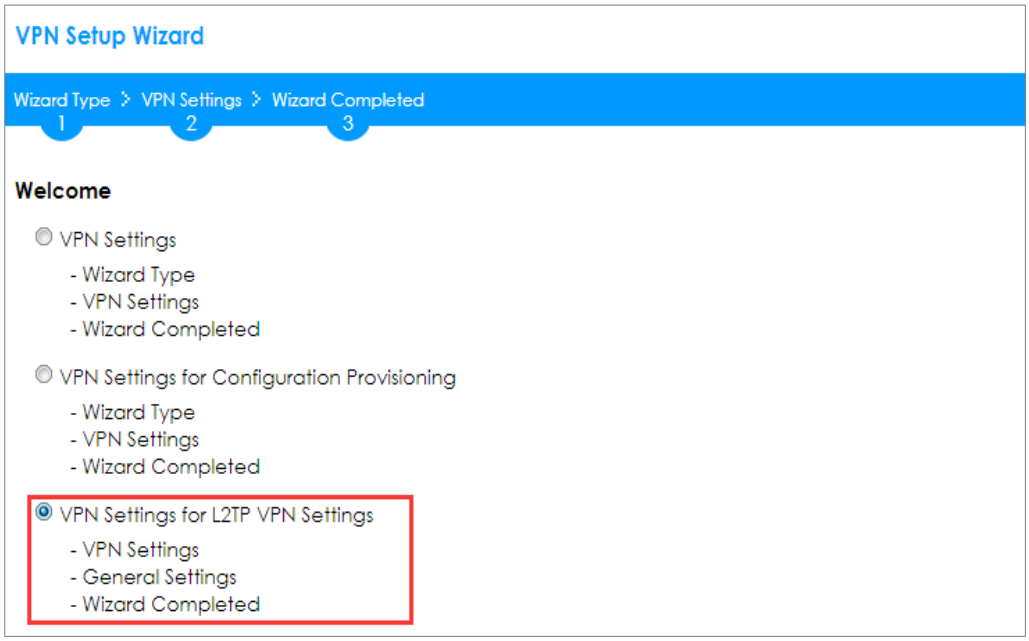


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and iOS (Firmware Version: 8.4).

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

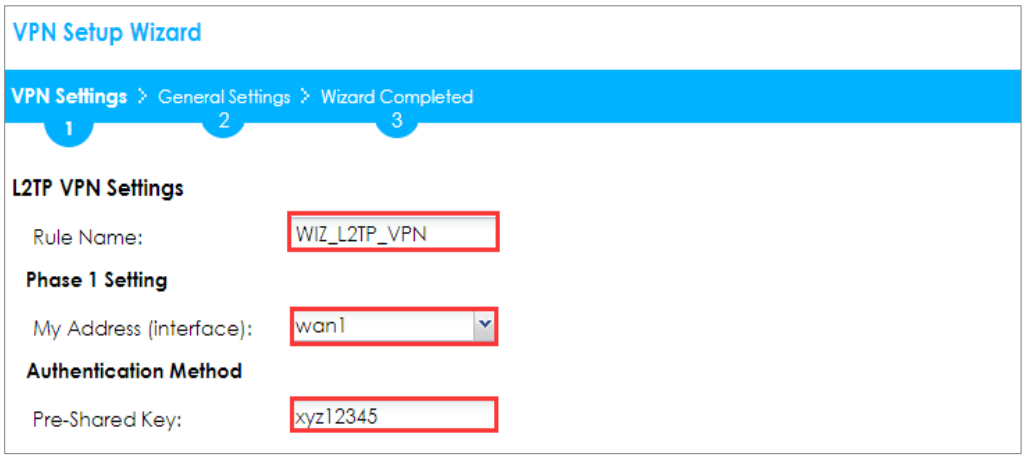
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the remote iOS Mobile Devices. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



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

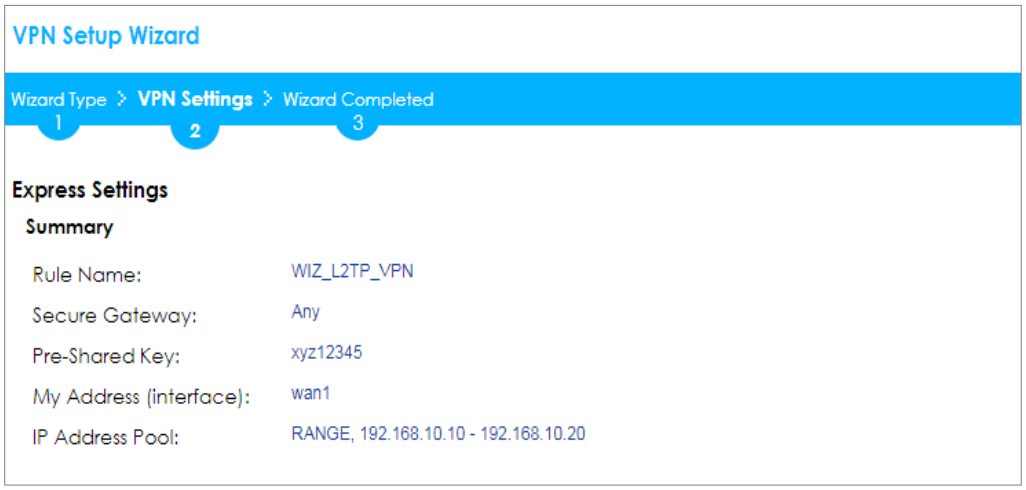


Assign the remote users IP addresses range from 192.168.100.10 to 192.168.100.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)

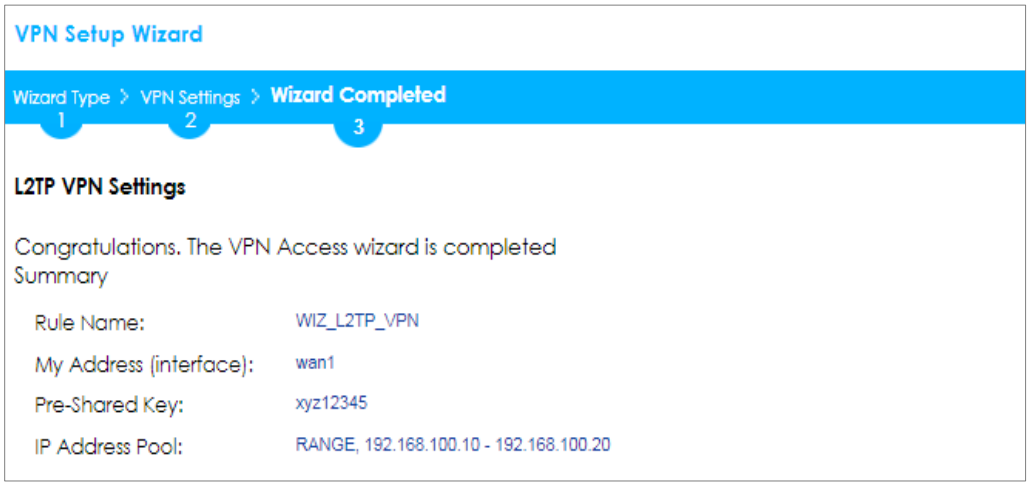
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



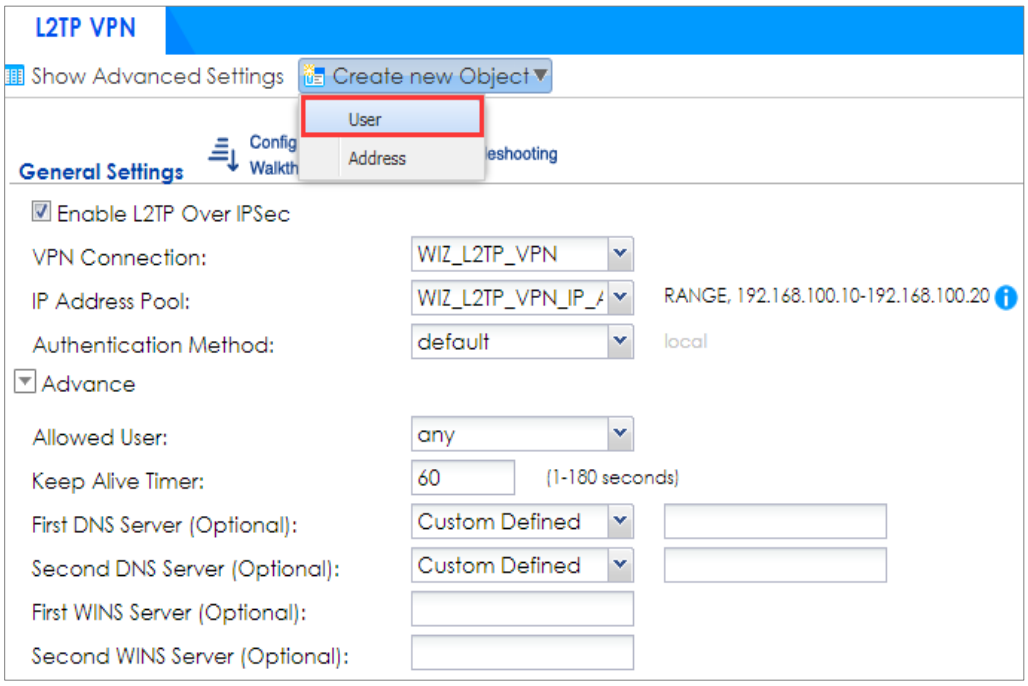
Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

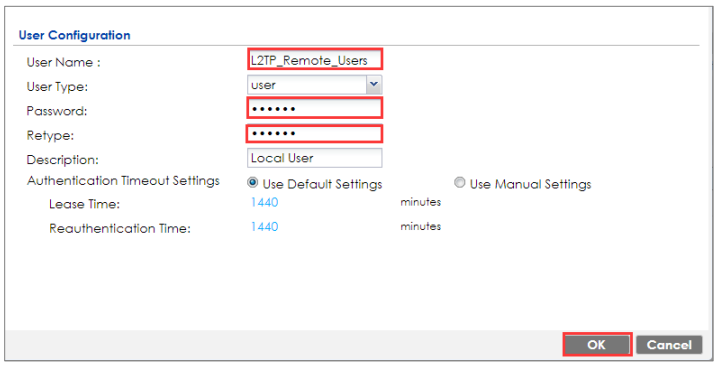
Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Summary > Wizard Completed



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).

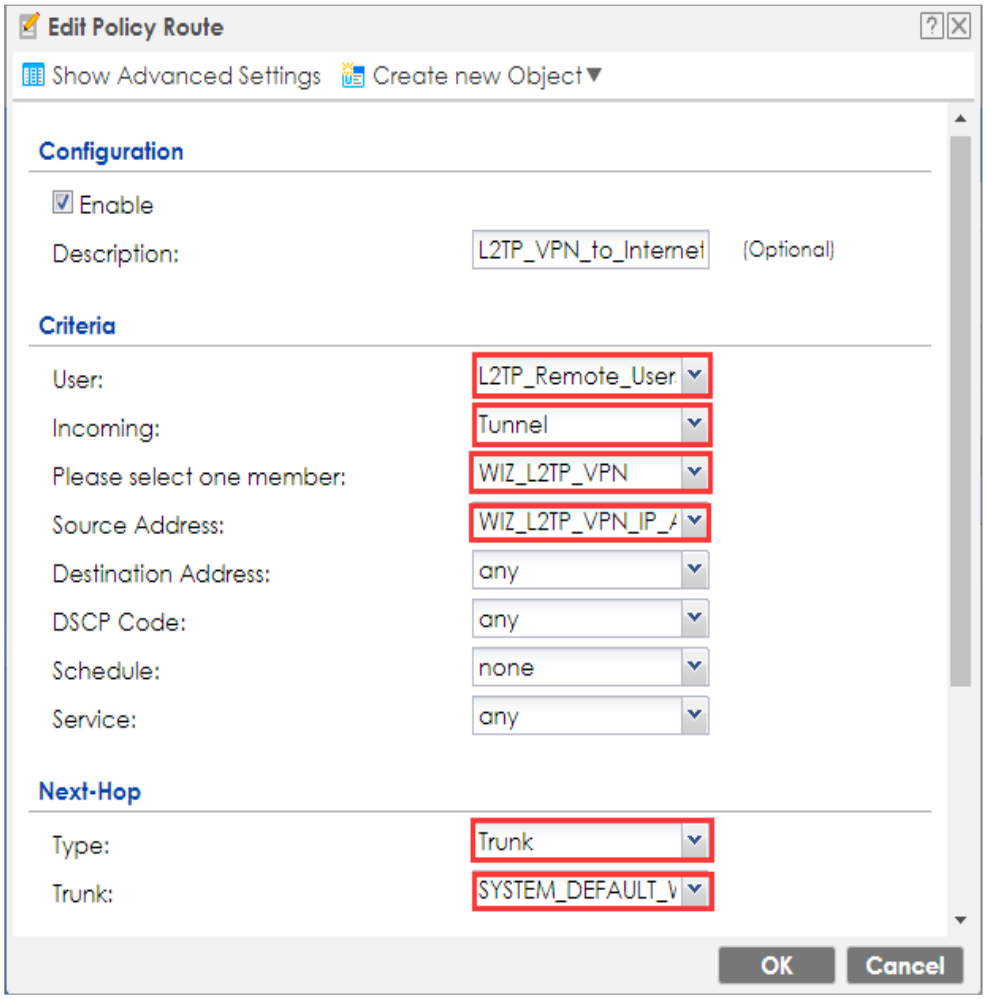
CONFIGURATION > VPN > L2TP VPN > Create new Object > User





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



Set Up the L2TP VPN Tunnel on the iOS Device

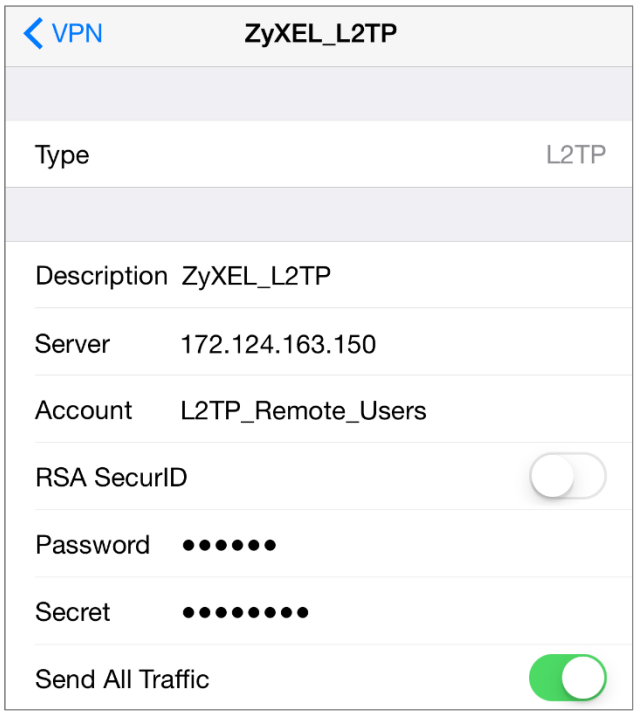
To configure L2TP VPN in an iOS 8.4 device, go to **Menu > Settings > VPN > Add VPN Configuration** and configure as follows.

Description is for you to identify the VPN configuration.

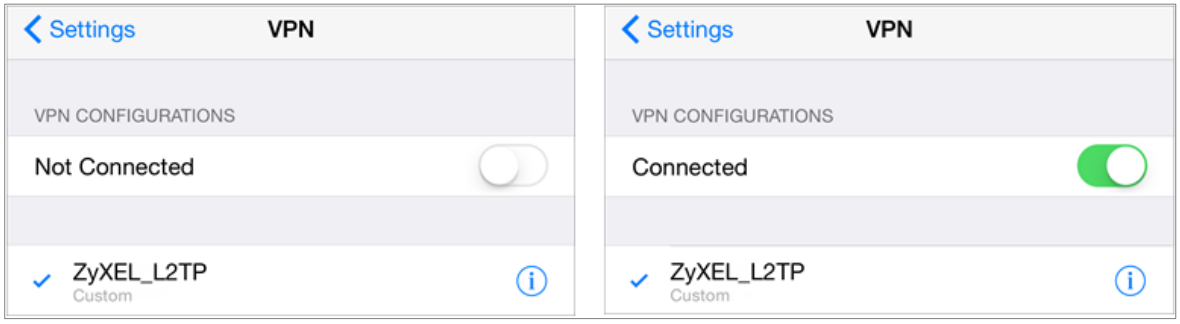
Set **Server** to the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).

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).



After you create a VPN configuration, slide the button right to the on position to initiate L2TP VPN session.



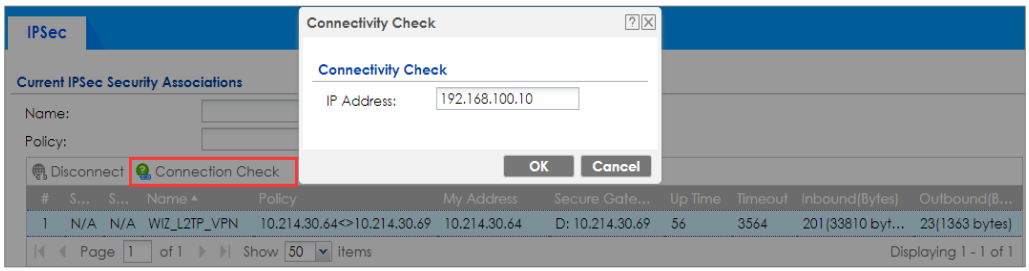
Test the L2TP over IPSec VPN Tunnel

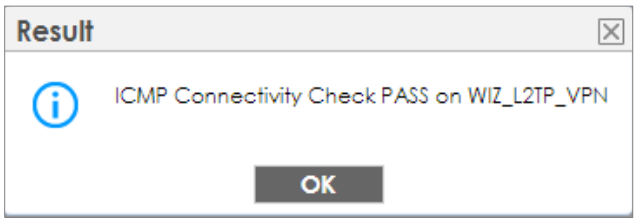
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

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.

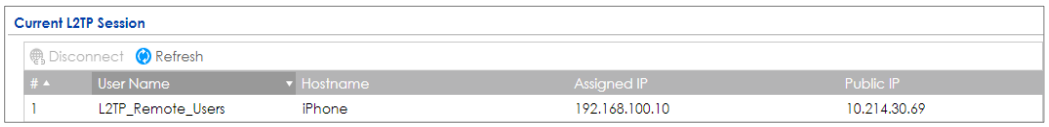
Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN





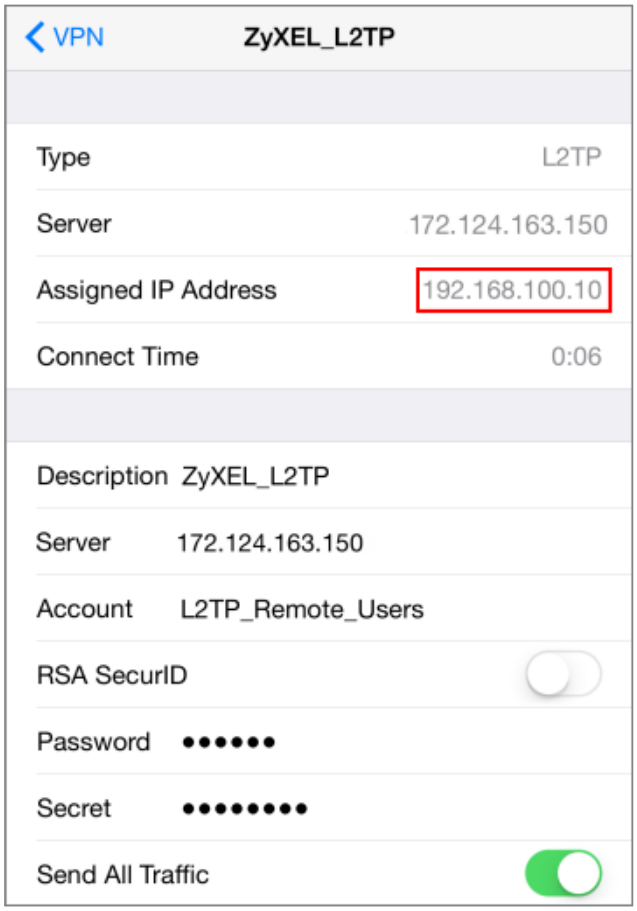
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users



Go to iOS mobile device **Menu > Settings > VPN > ZyXEL_L2TP** and verify the **Assigned IP Address** and **Connect Time**.

Menu > Settings > VPN > ZyXEL_L2TP



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.

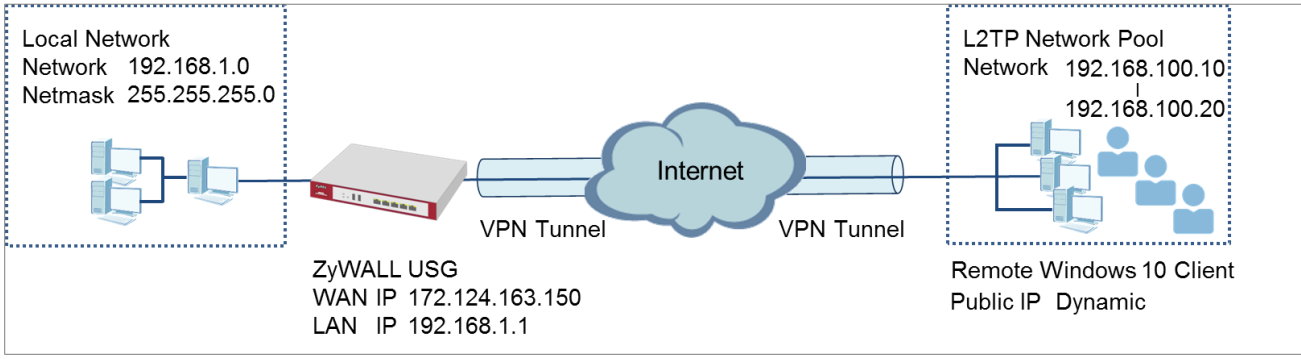
Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

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

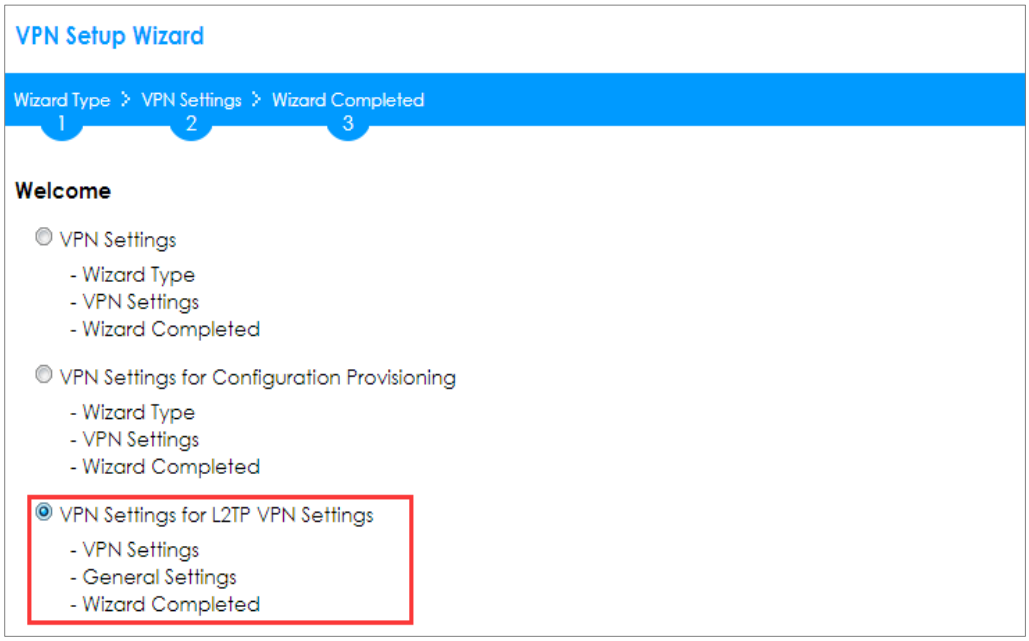


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and Windows 10 Pro (Version: 10.0.10240)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

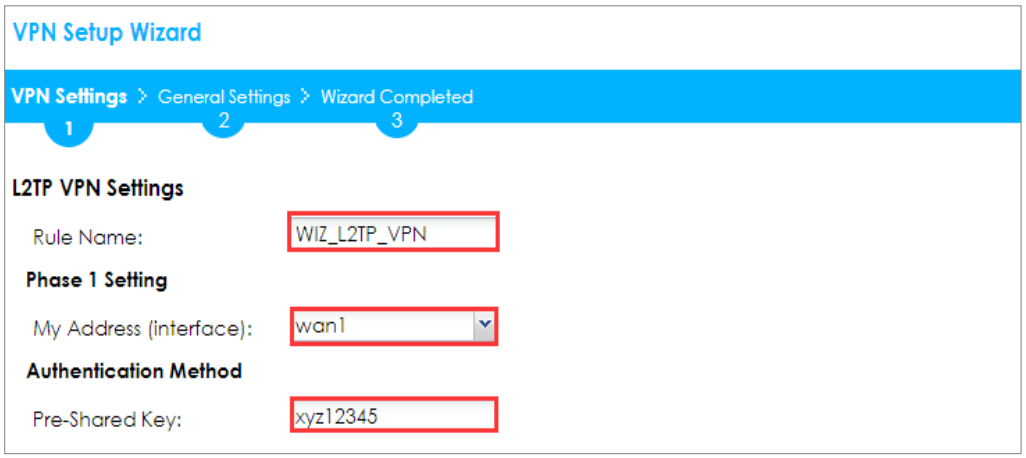
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the Window 10 clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



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

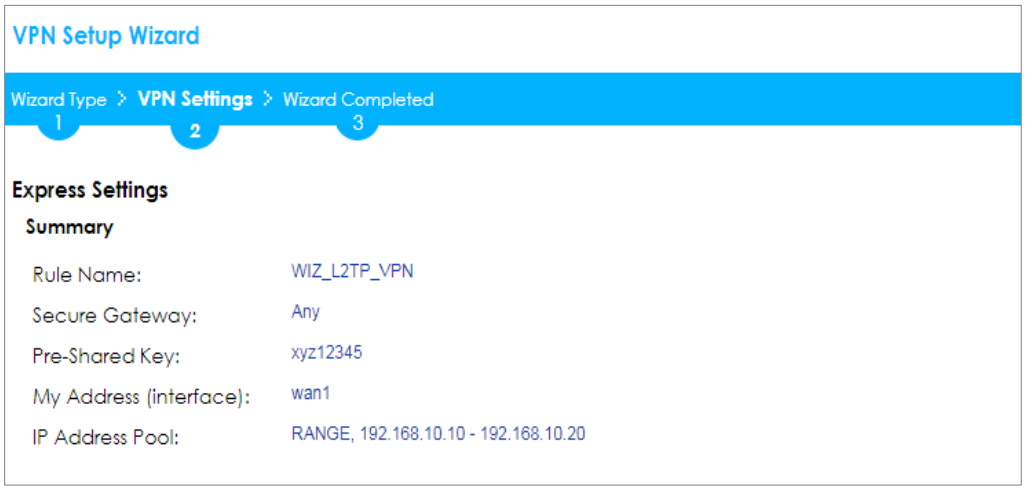


Assign the L2TP users' IP address range from 192.168.100.10 to 192.168.100.20 for use in the L2TP VPN tunnel and select **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)

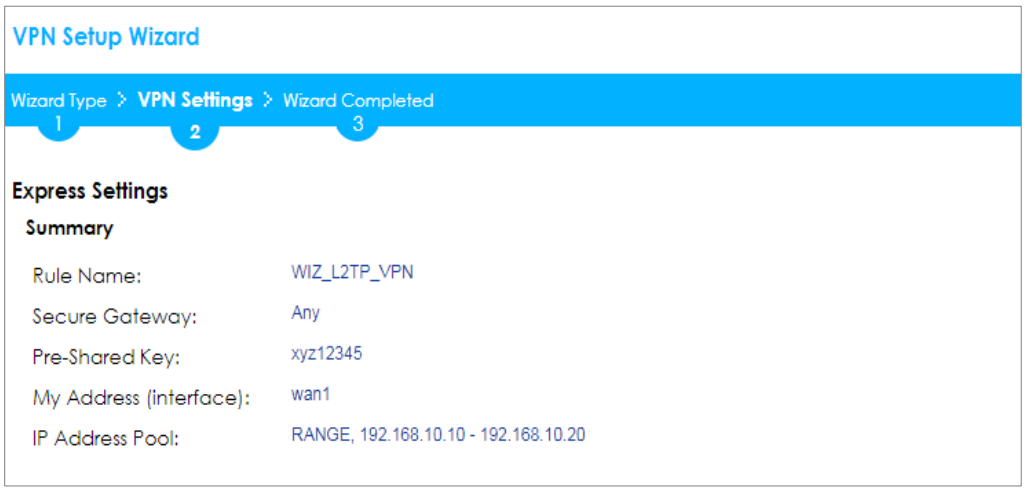
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



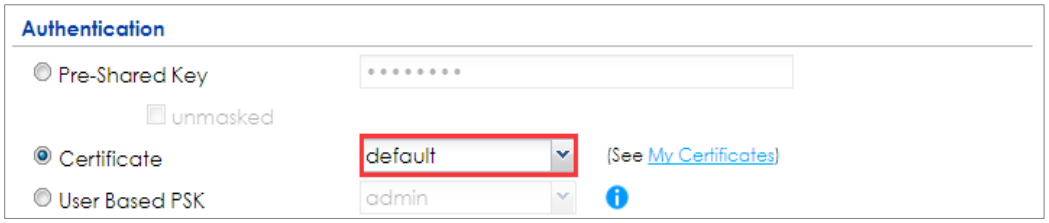
Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

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



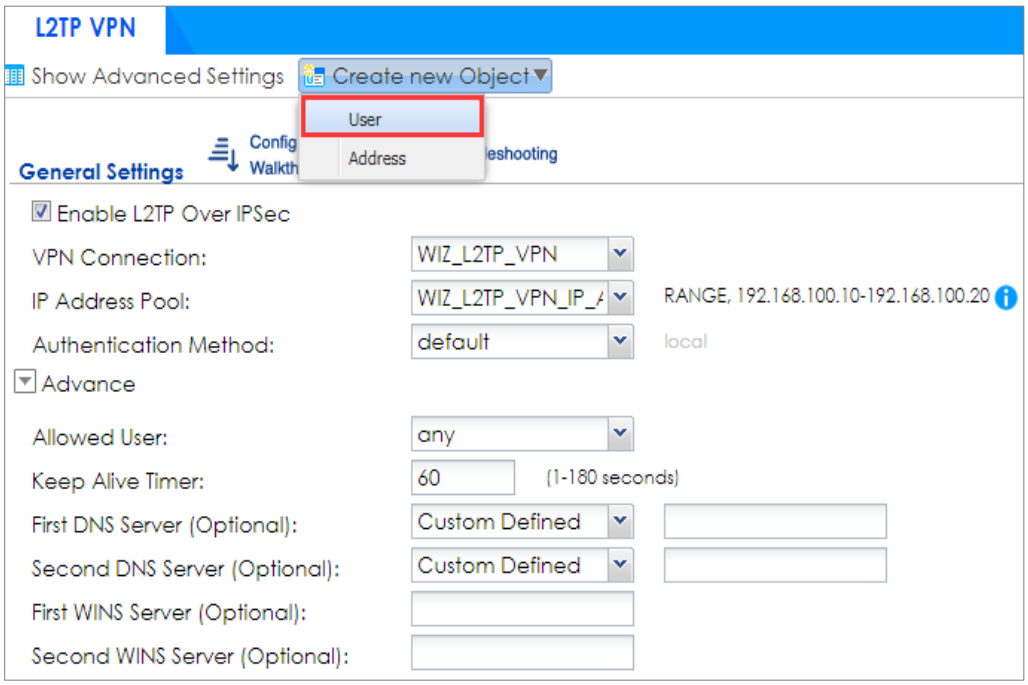
Go to **CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN**, change **Authentication** method to be **Certificate** and select the certificate which ZyWALL/USG uses to identify itself to the Window 10 computer.

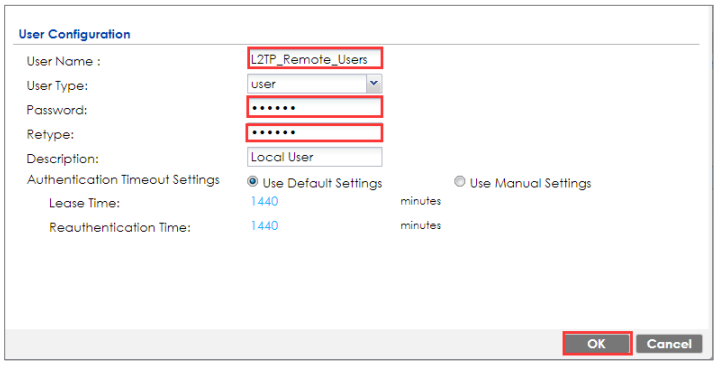
CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN > Authentication > Certificate



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).

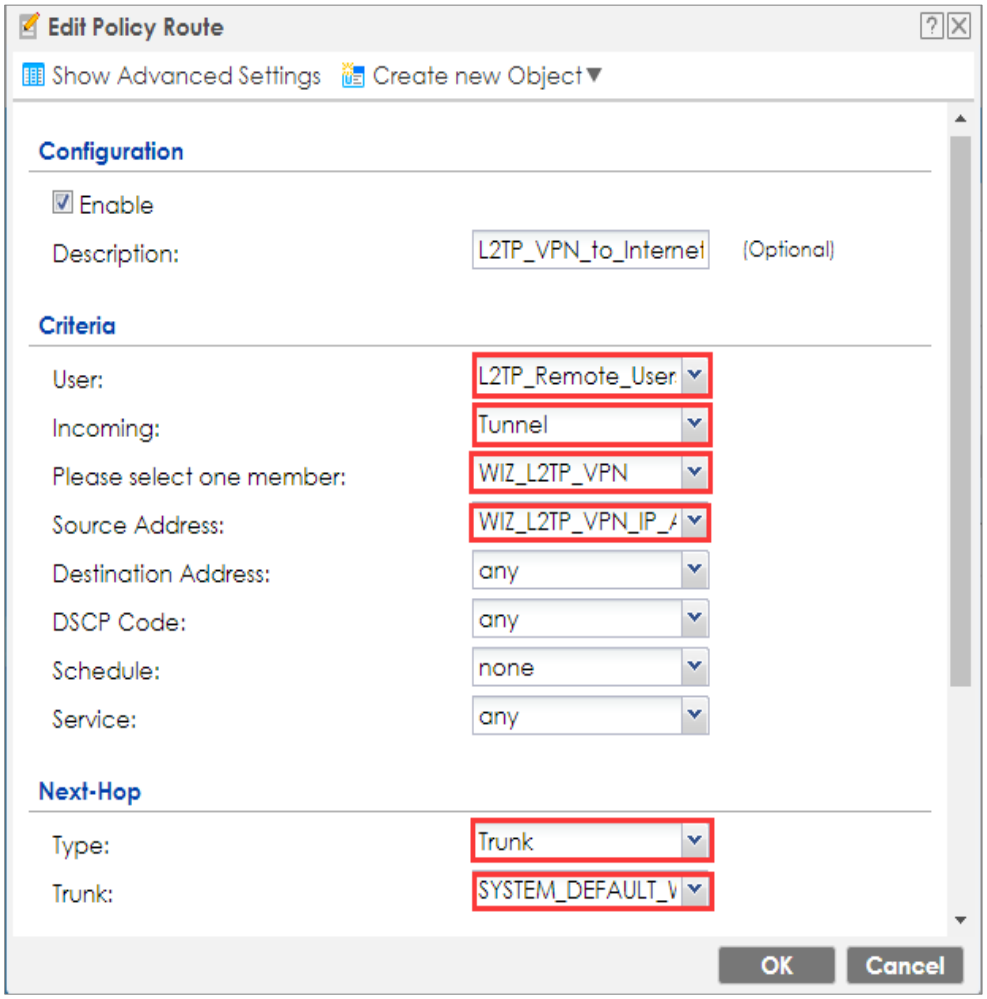
CONFIGURATION > VPN > L2TP VPN > Create new Object > User





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.

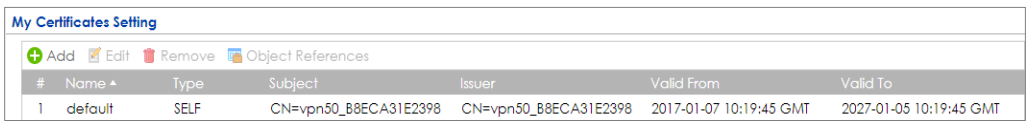
CONFIGURATION > Network > Routing > Policy Route



Export a Certificate from ZyWALL/USG and Import it to Windows 10 Operating System

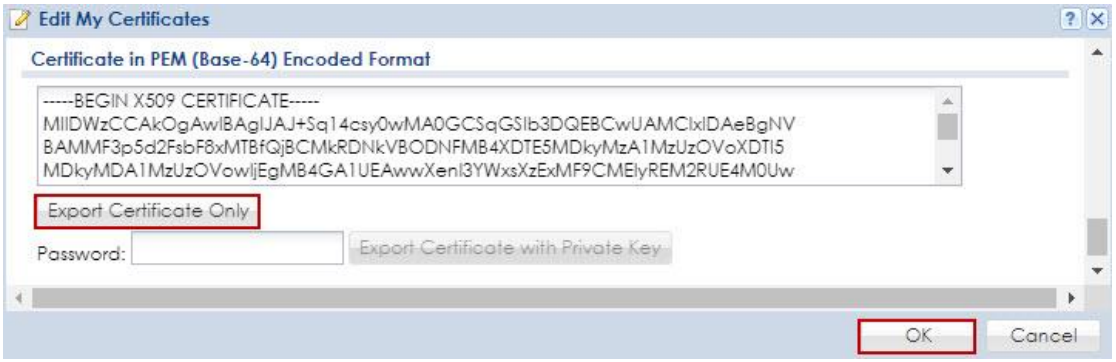
Go to ZyWALL/USG **CONFIGURATION > Object > Certificate**, select the certificate (**default** in this example) and click **Edit**.

CONFIGURATION > Object > Certificate > default

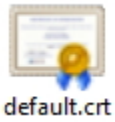


Export default certificate from ZyWALL/USG.

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only

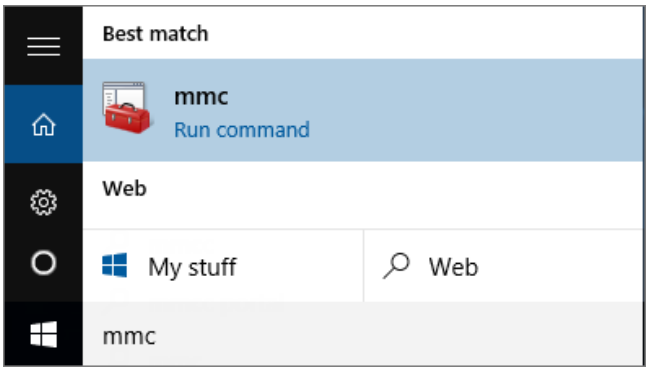


Save **default** certificate as ***.crt** file to Windows 10 computer.



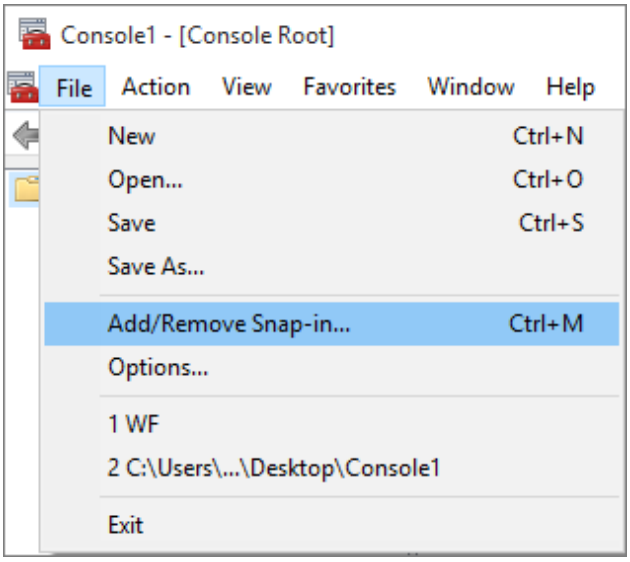
In Windows 10 Operating System, go to **Start Menu > Search Box**. Type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



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

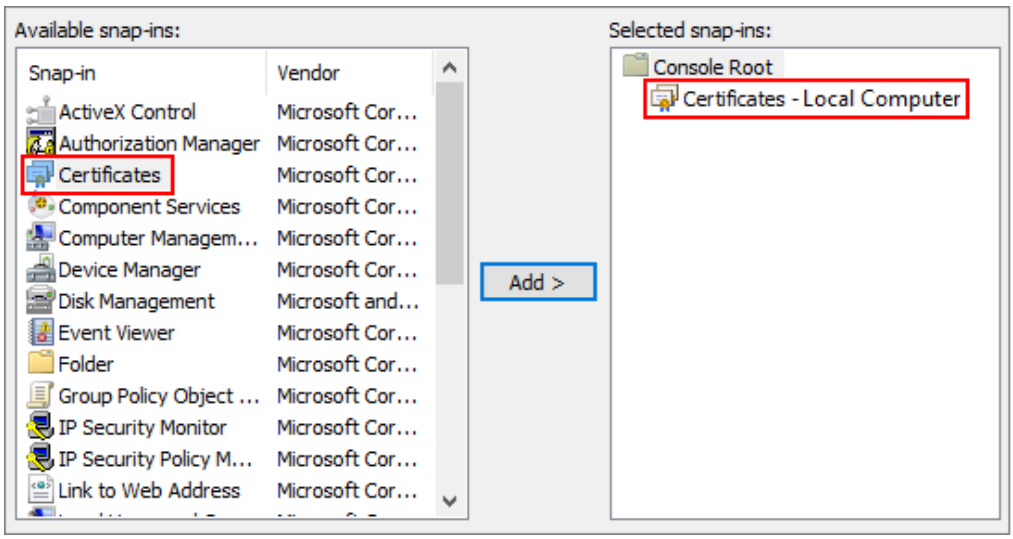
File > Add/Remove Snap-in...



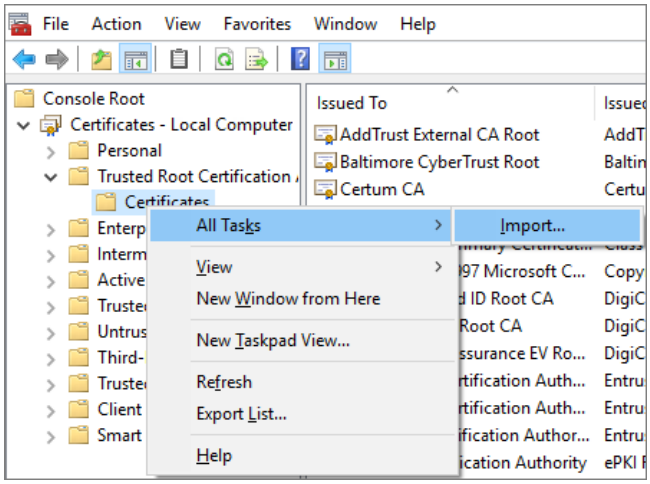
In the **Available snap-ins**, select **Certificates** click **Add**. Then, click **Finished**.

Press **OK** to close the Snap-ins window.

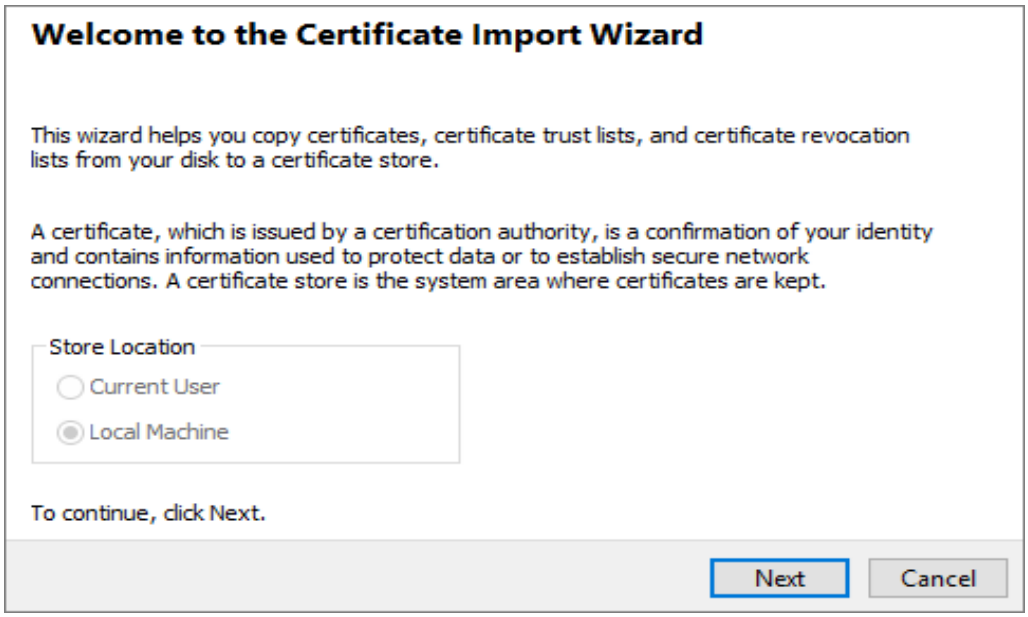
Available snap-ins > Certificates > Add



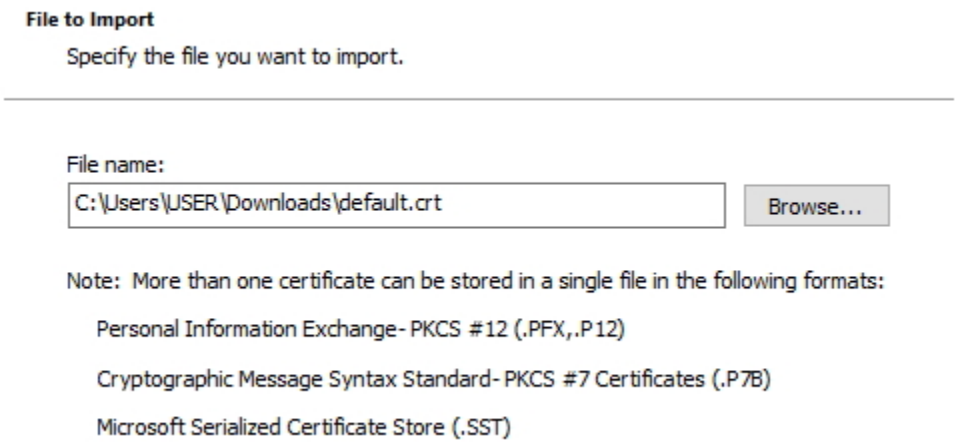
In the mmc console window, go to **Certificates (Local Computer) > Trusted Root Certification Authorities**, right click **Certificate > All Tasks > Import…**



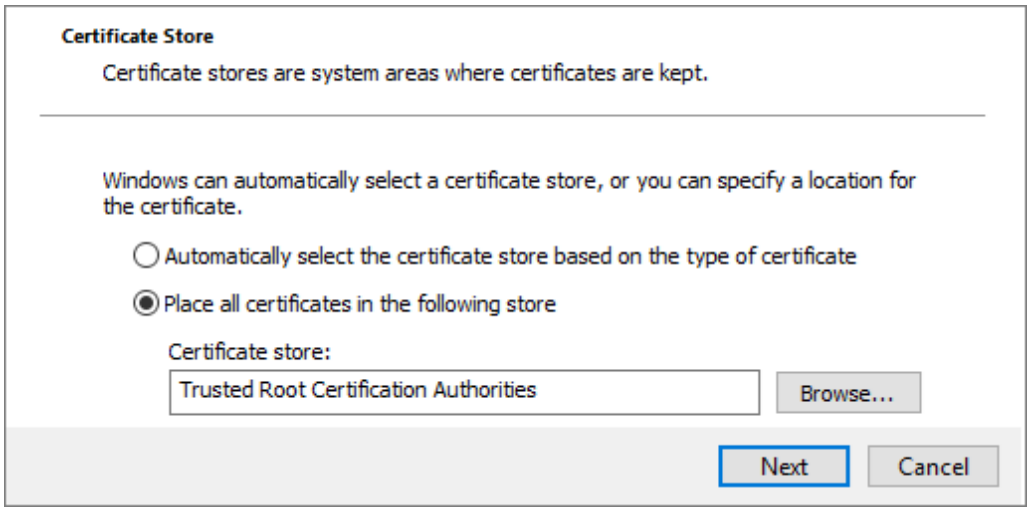
Click **Next**.



Click **Browse...**, and locate the .crt file you downloaded earlier. Then, click **Next**.



Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities.** Click **Next**, then click **Finish**.



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.

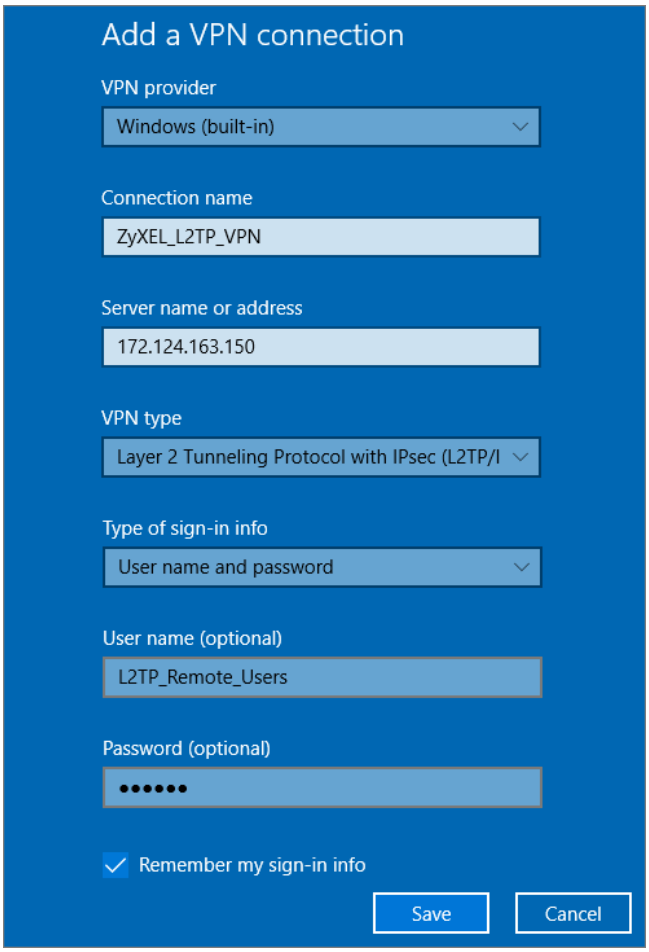
VPN Provider set to **Windows (built-in)**.

Configure **Connection name** for you to identify the VPN configuration.

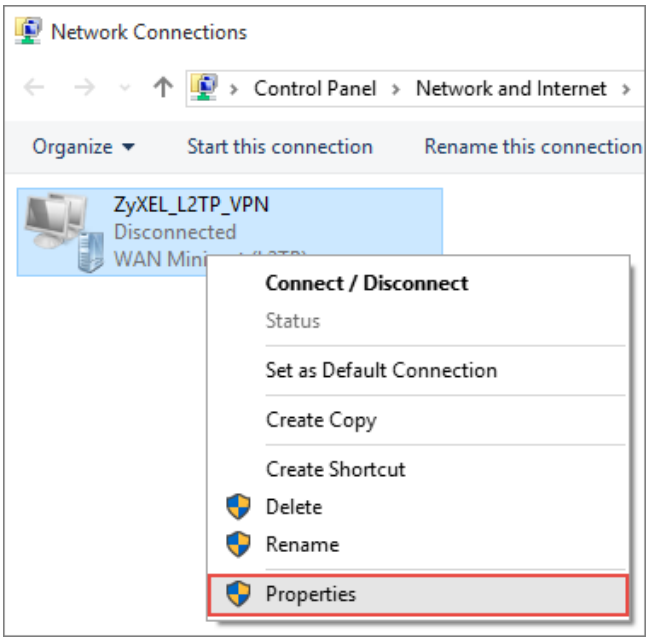
Set **Server** name or address to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).

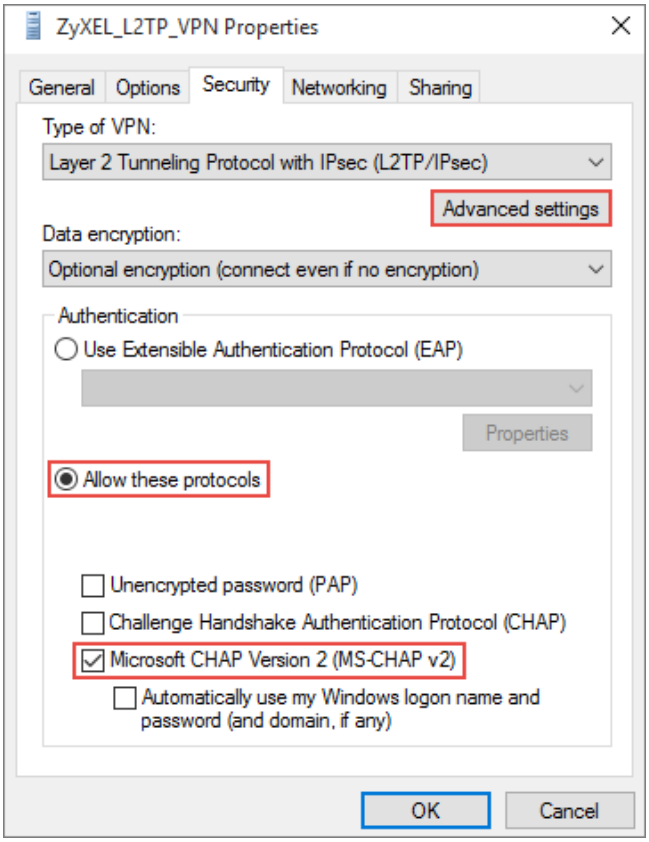
Select **VPN type** to **Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec)**.

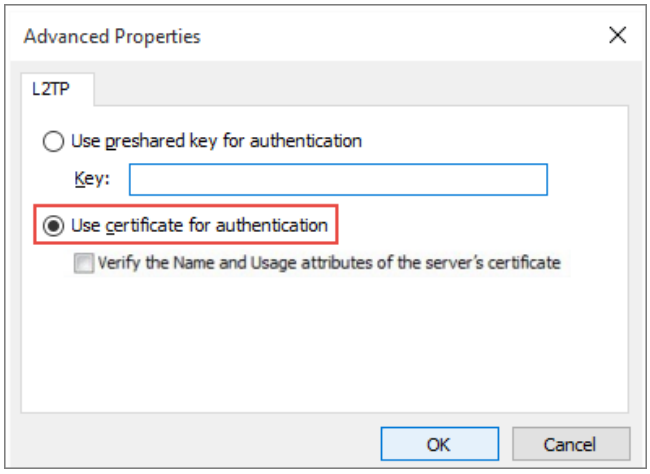
Enter **User name** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).



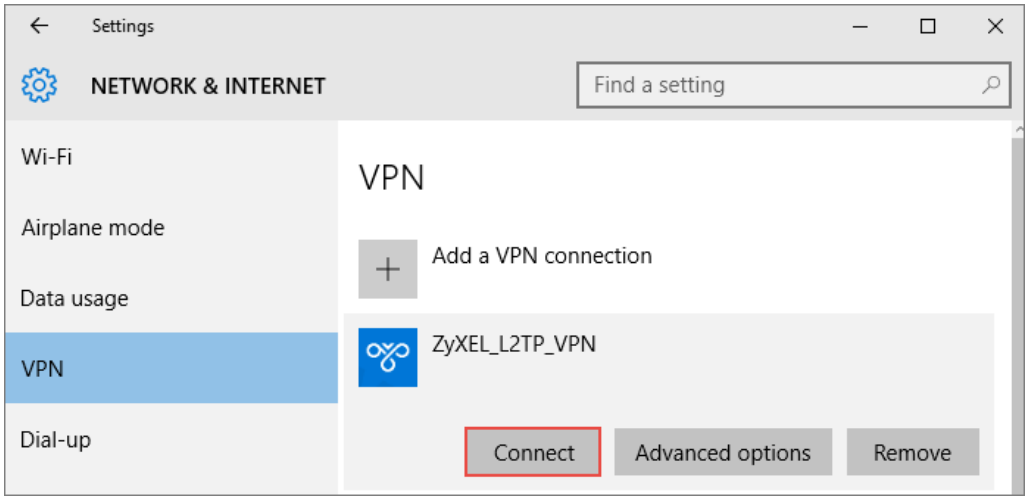
Go to **Control Panel > Network and Internet > Network Connections** and right click **Properties.** Continue to **Security > Advanced settings** and select **Use Certificate for authentication**.


Network Connections
Control Panel › Network and Internet ›
Organize
Start this connection
Rename this connection
ZyXEL_L2TP_VPN
Disconnected
Connect / Disconnect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
Properties


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



Go to **Network & Internet Settings** window, click **Connect**.



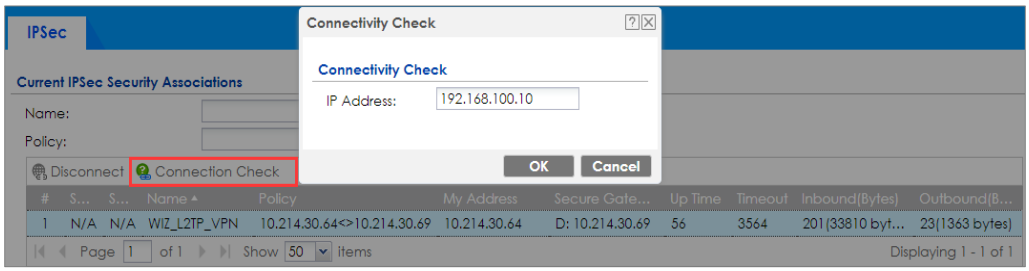
Test the L2TP over IPSec VPN Tunnel

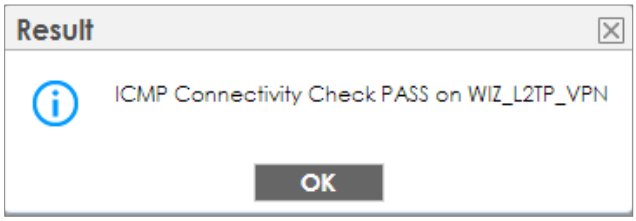
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

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.

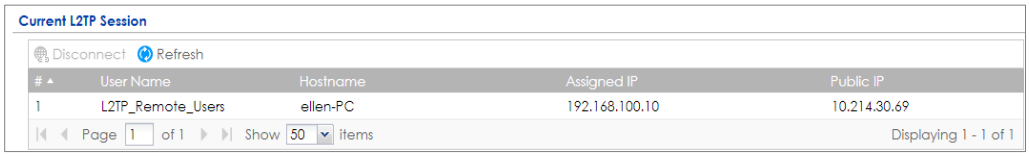
Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN





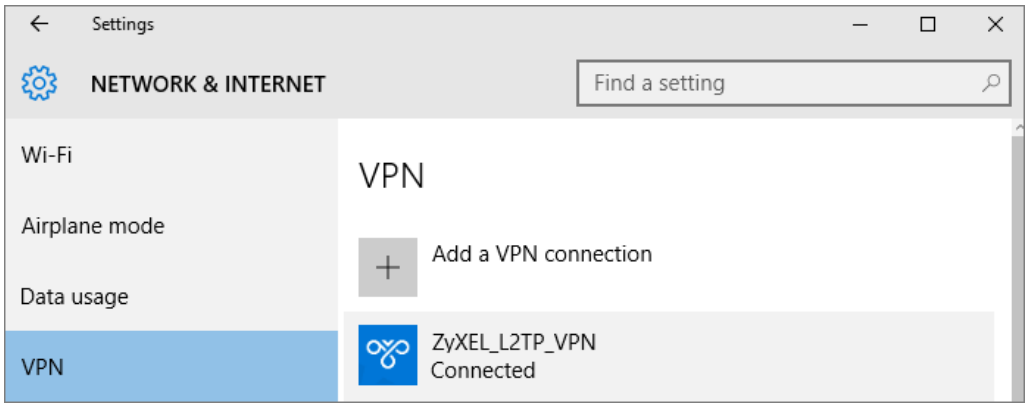
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users



Go to Window 10 operating system **Start > Settings > Network & Internet > VPN** and show **Connected** status.

Menu > Settings > VPN > ZyXEL_L2TP



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.

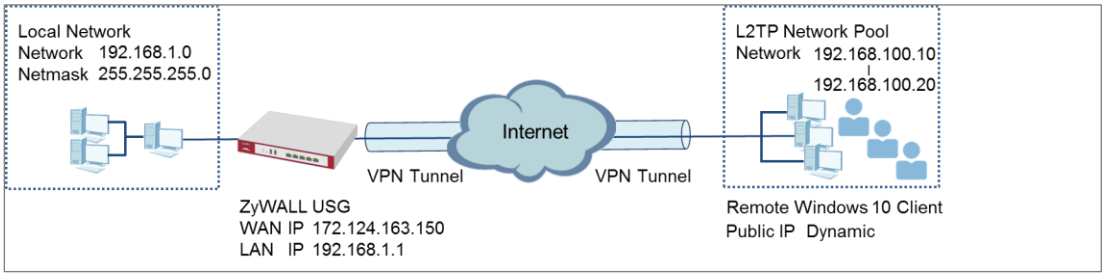
Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

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

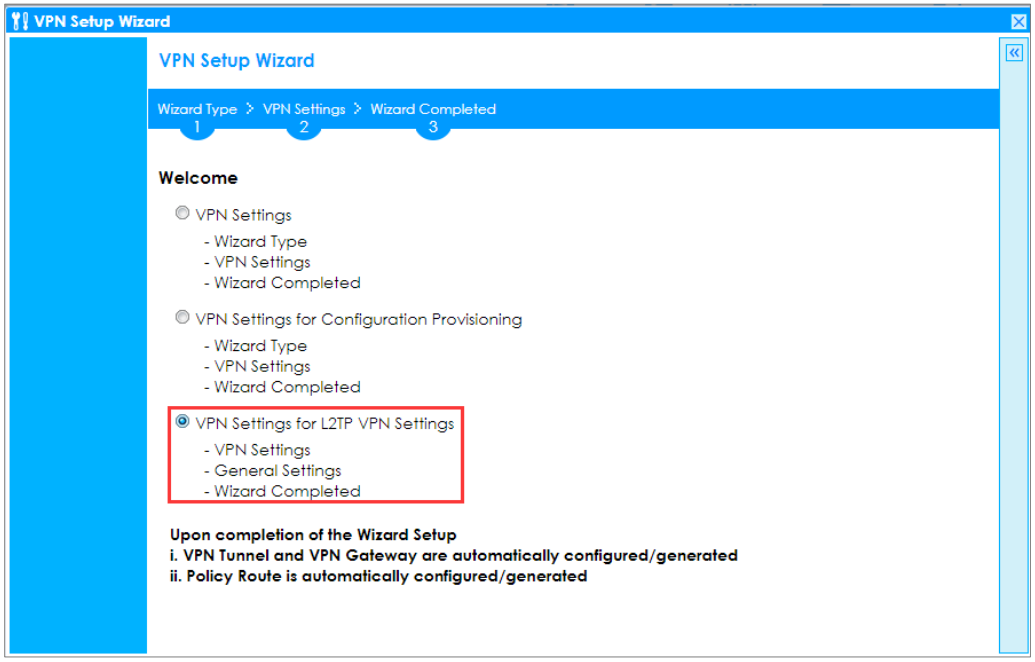


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and iOS (Version: 10.0.10240)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

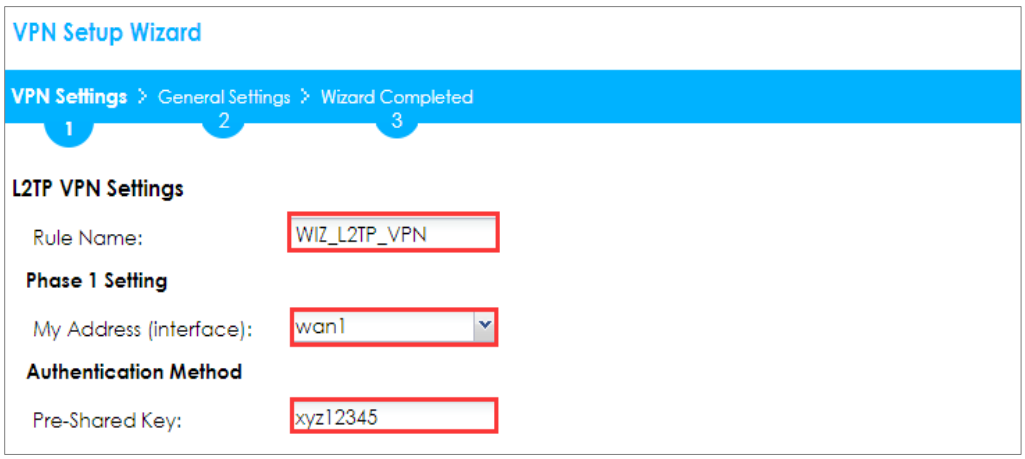
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the iOS mobile phone clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



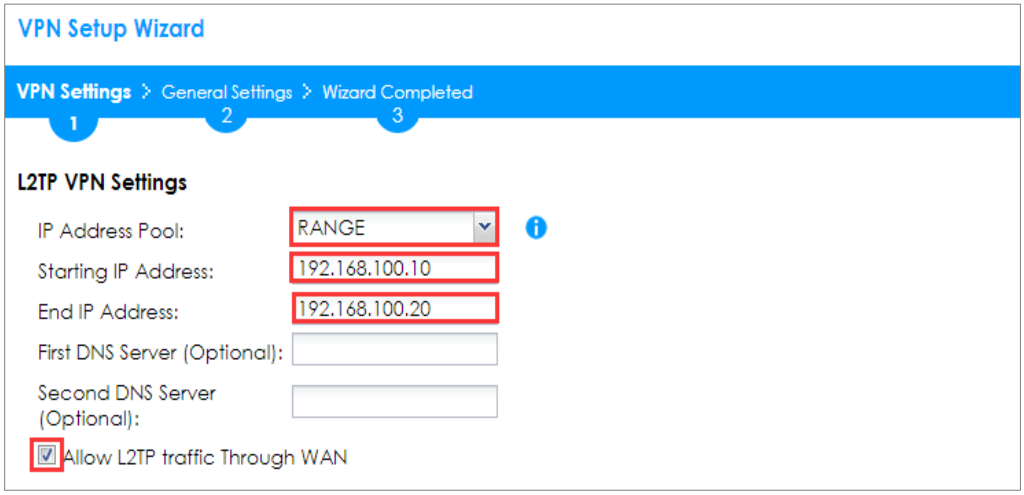
Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



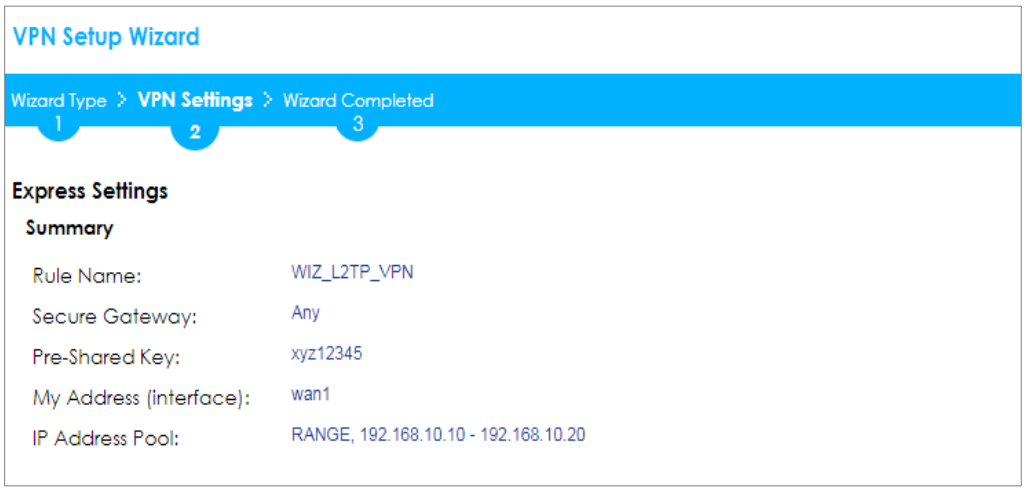
Assign the L2TP users' IP address range from 192.168.100.10 to 192.168.100.20 for use in the L2TP VPN tunnel and select **Allow L2TP traffic Through WAN** to allow traffic from L2TP clients to go to the Internet. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (L2TP VPN Settings)



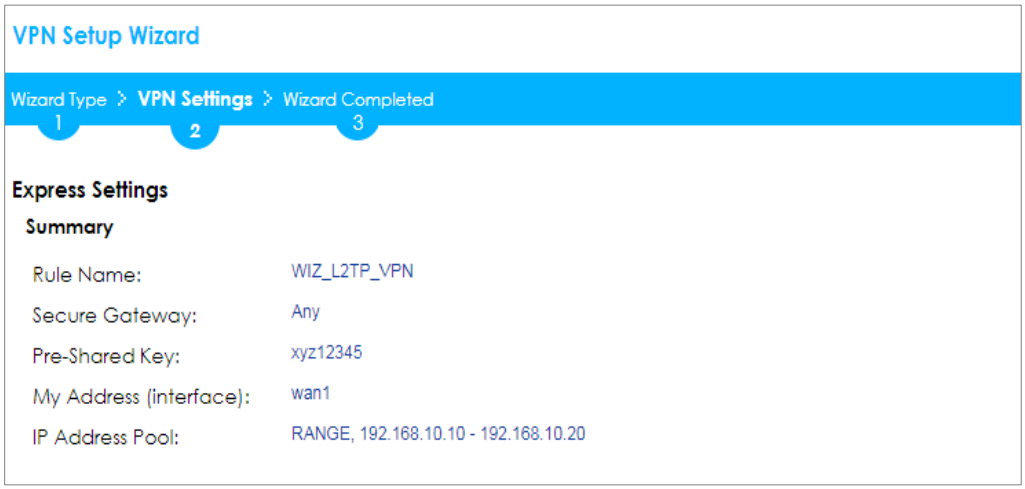
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



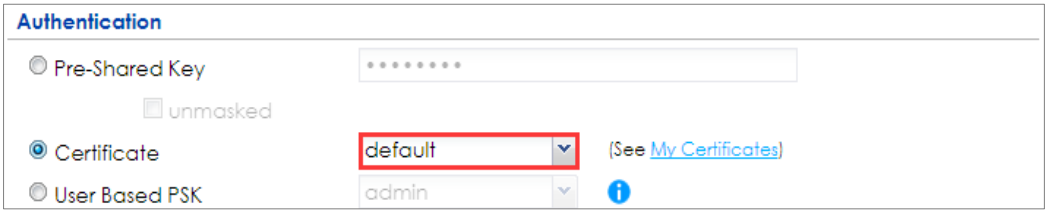
Now the rule is configured on the ZyWALL/USG. The rule settings appear in the **VPN > L2TP VPN** screen. Click **Close** to exit the wizard.

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



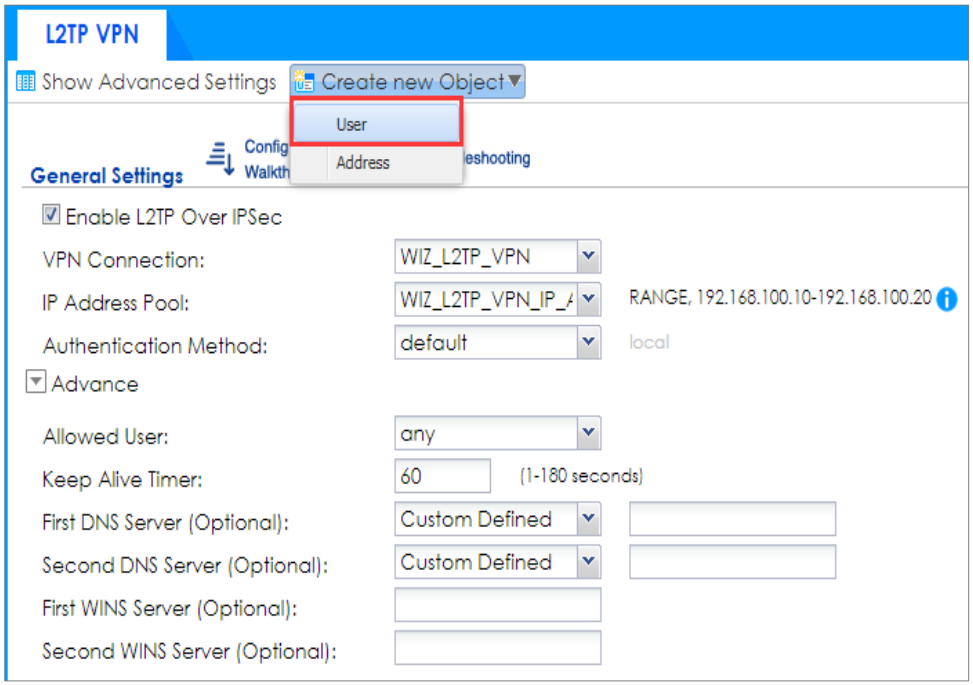
Go to **CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN**, change **Authentication** method to be **Certificate** and select the certificate which ZyWALL/USG uses to identify itself to the Android mobile phone.

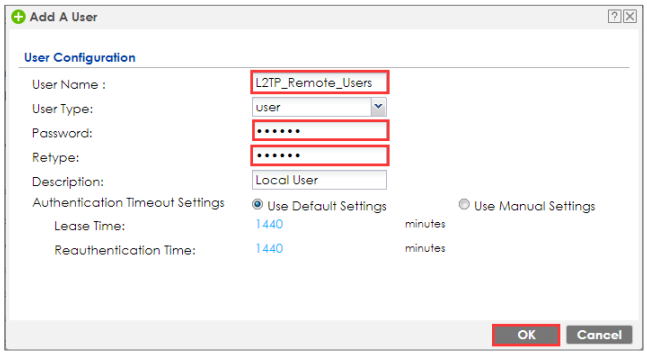
CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN > Authentication > Certificate

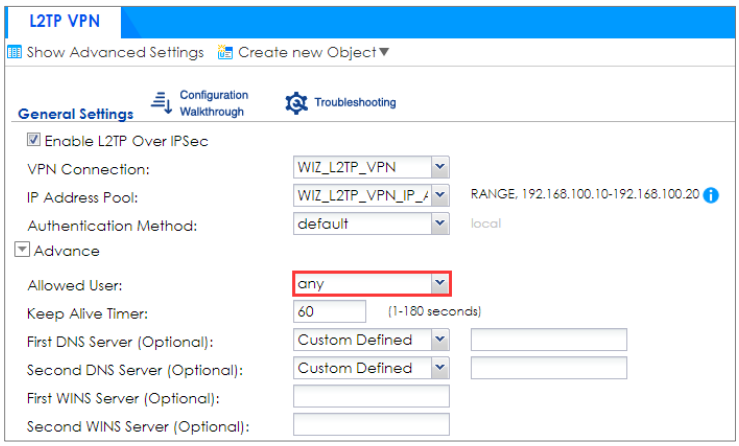


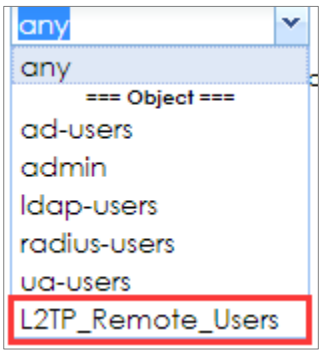
Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User


L2TP VPN
Show Advanced Settings
Create new Object
User
Address
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):


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
OK
Cancel


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_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):


any
any
=== Object ===
ad-users
admin
ldap-users
radius-users
ua-users
L2TP_Remote_Users

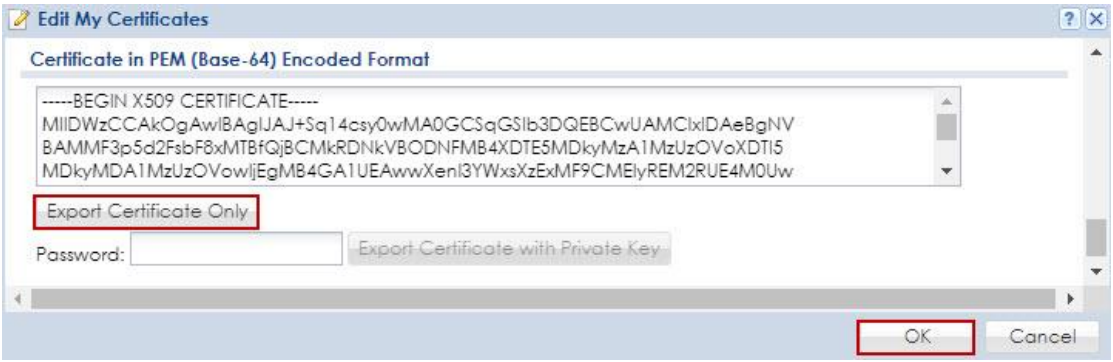
Export a Certificate from ZyWALL/USG and Import it to iOS Mobile Phone

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate**, select the certificate (**default** in this example) and click **Edit**.

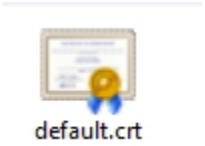
CONFIGURATION > Object > Certificate > default

Export default certificate from ZyWALL/USG.

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only



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.

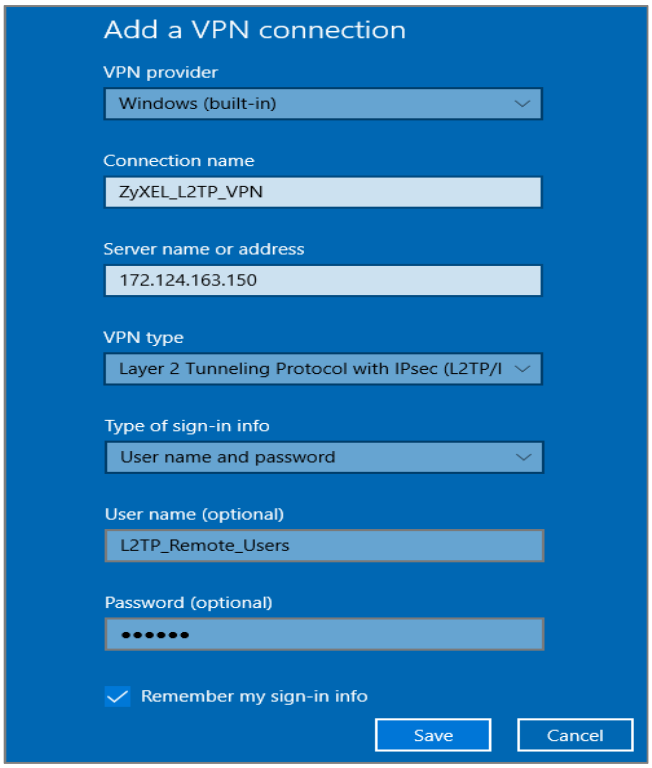
2. VPN Provider set to Windows (built-in).

3. Configure **Connection name** for you to identify the VPN configuration.

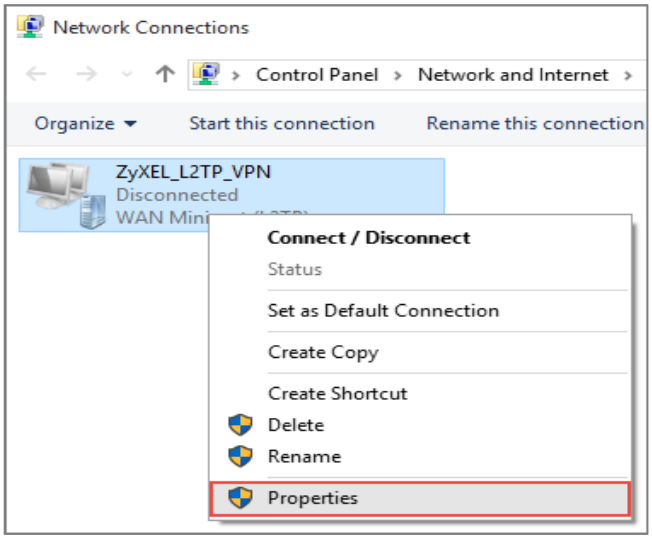
4 Set **Server** name or address to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).

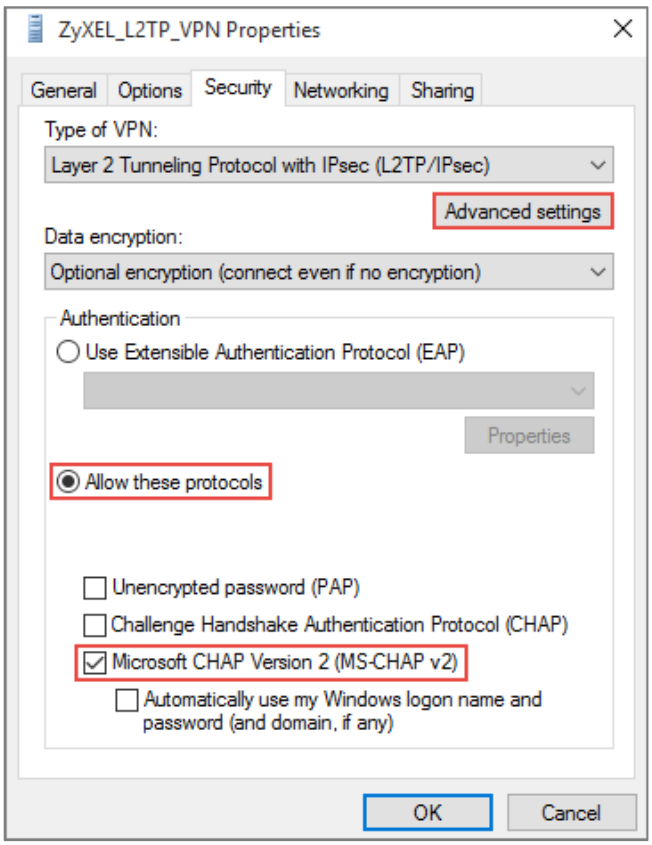
5 Select VPN type to Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec).

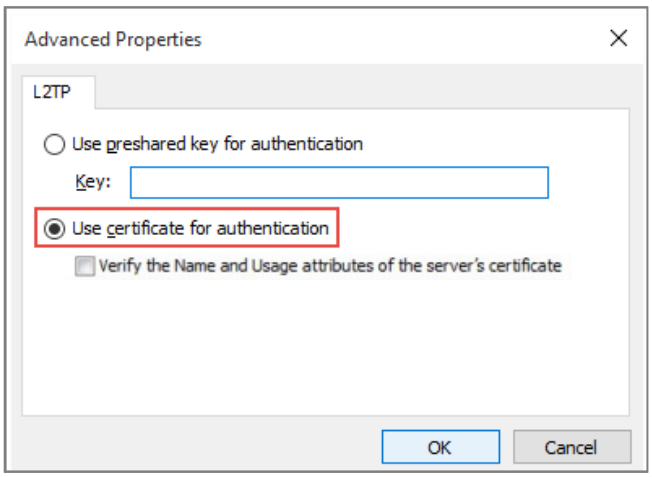
6 Enter **User name** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).



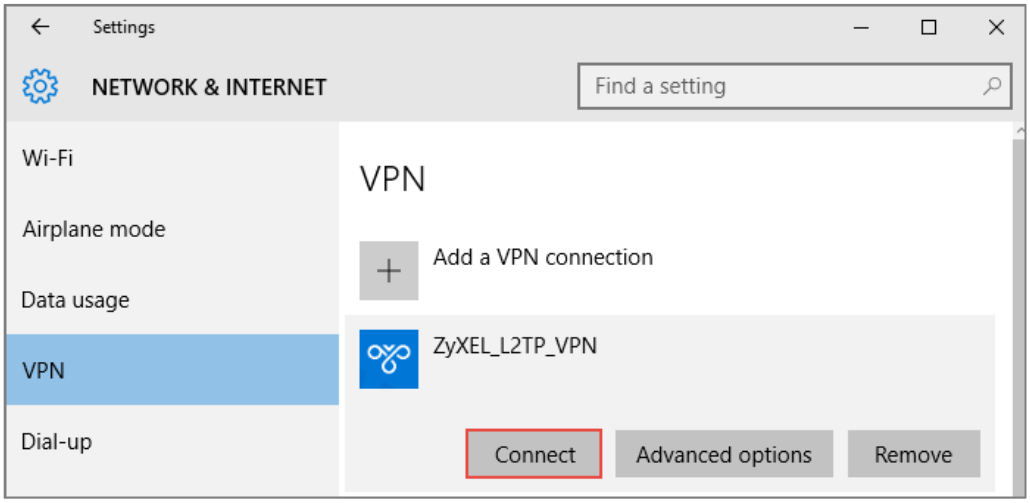
7 Go to Control Panel > Network and Internet > Network Connections and right click Properties. Continue to Security > Advanced settings and select Use Certificate for authentication.


Network Connections
Control Panel › Network and Internet ›
Organize
Start this connection
Rename this connection
ZyXEL_L2TP_VPN
Disconnected
Connect / Disconnect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
Properties


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



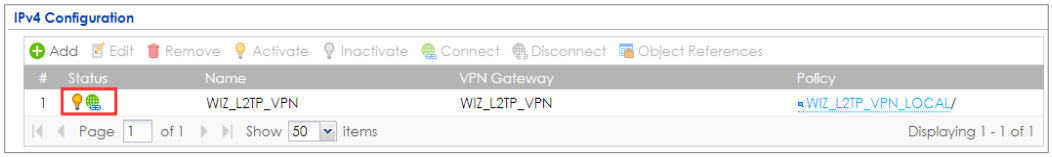
8 Go to Network & Internet Settings window, click Connect.



Test the L2TP over IPSec VPN Tunnel

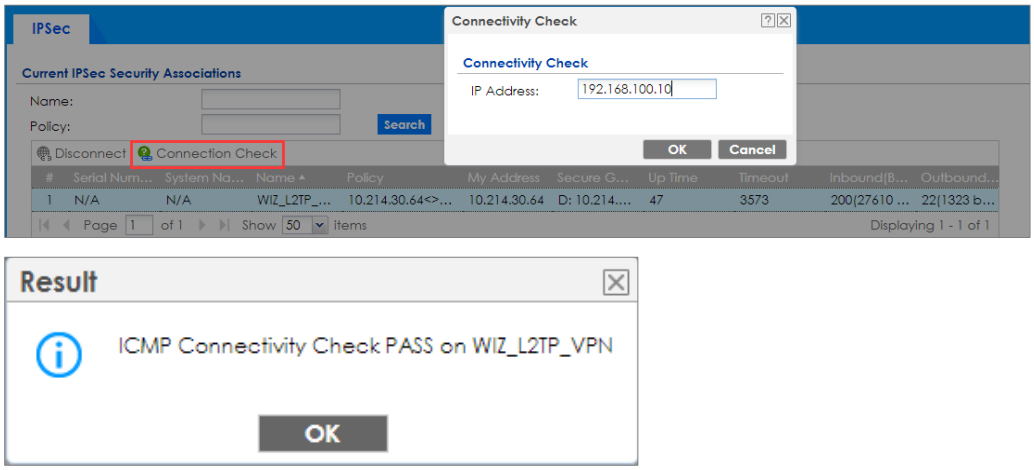
1. Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



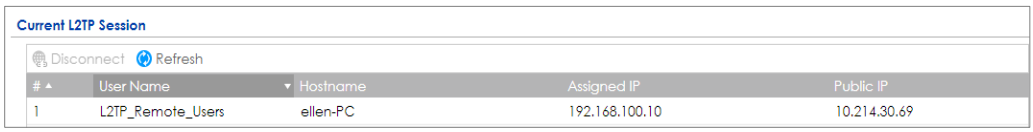
2. Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



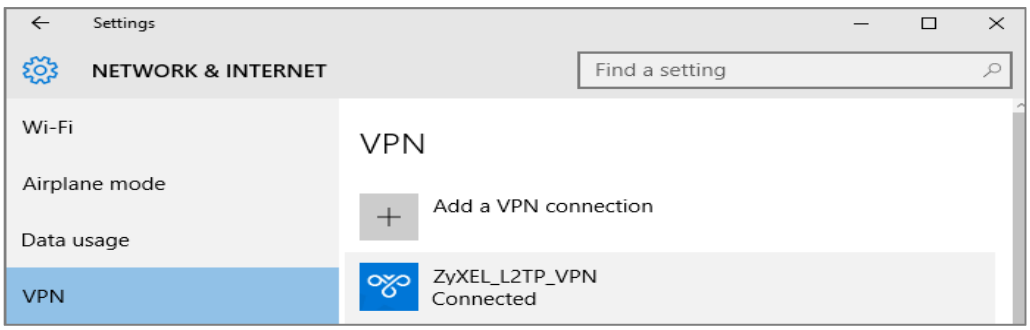
3. Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users



4. Go to iOS operating system **Start > Settings > Network & Internet > VPN** and show **Connected** status.

Menu > Settings > VPN > ZyXEL_L2TP



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.

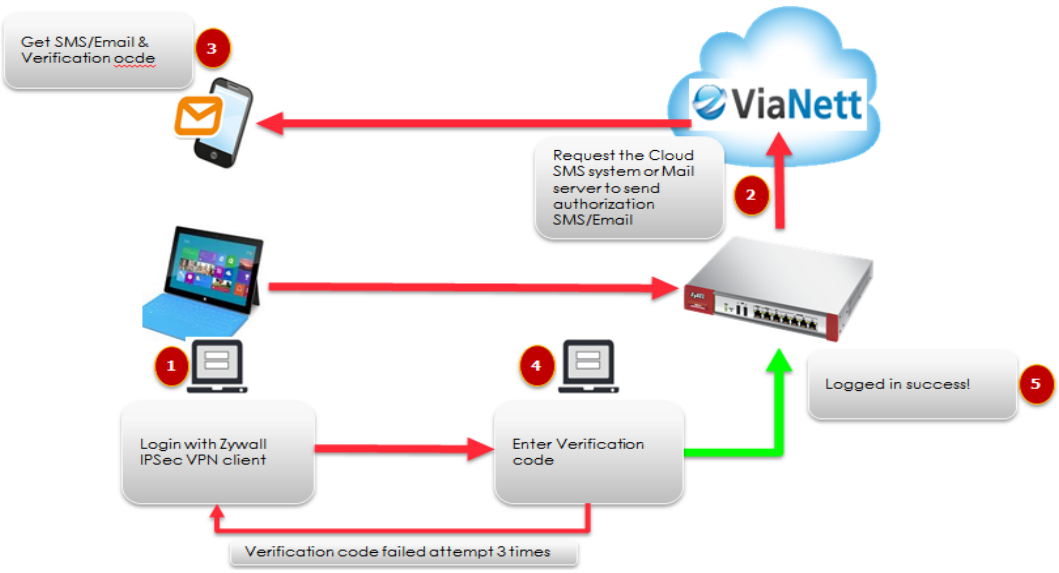
5. If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

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.



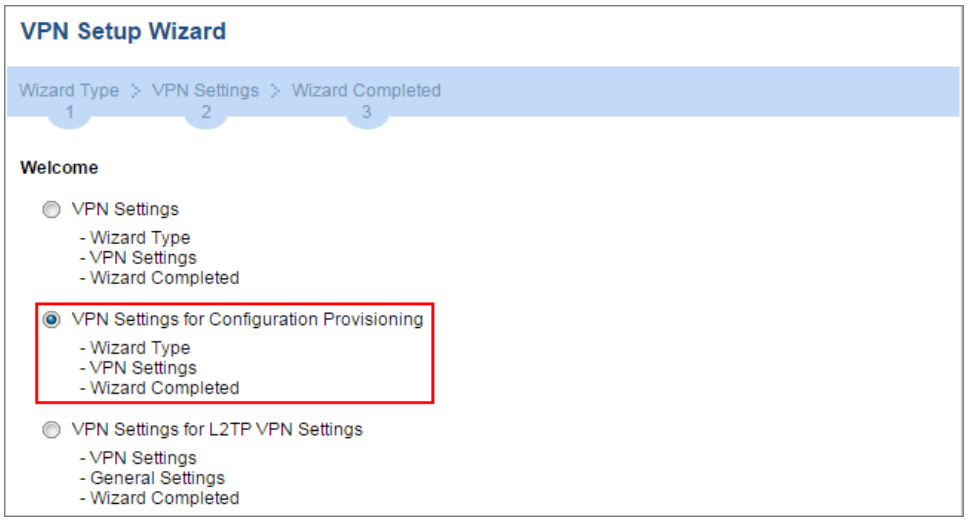
Walkthrough

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

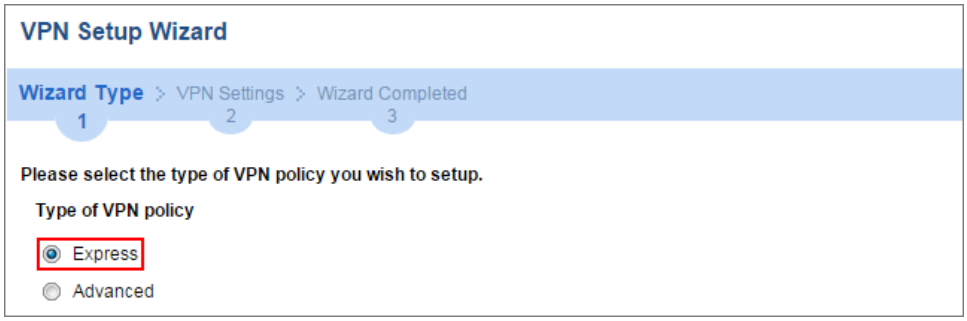
In the ZyWALL/USG, go to **CONFIGURATION >Quick Setup > VPN Setup Wizard**, use the **VPN Settings for Configuration Provisioning** wizard to create a VPN rule that can be used with the ZyWALL IPSec VPN Client. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



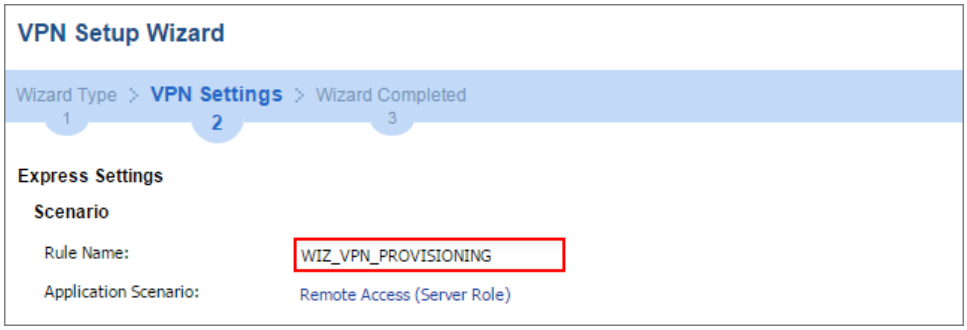
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



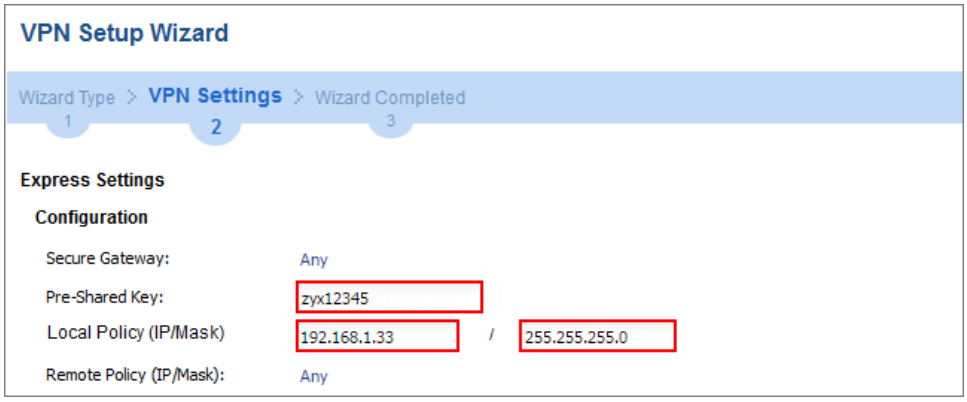
Type the **Rule Name** used to identify this VPN connection (and VPN gateway). You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-1



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

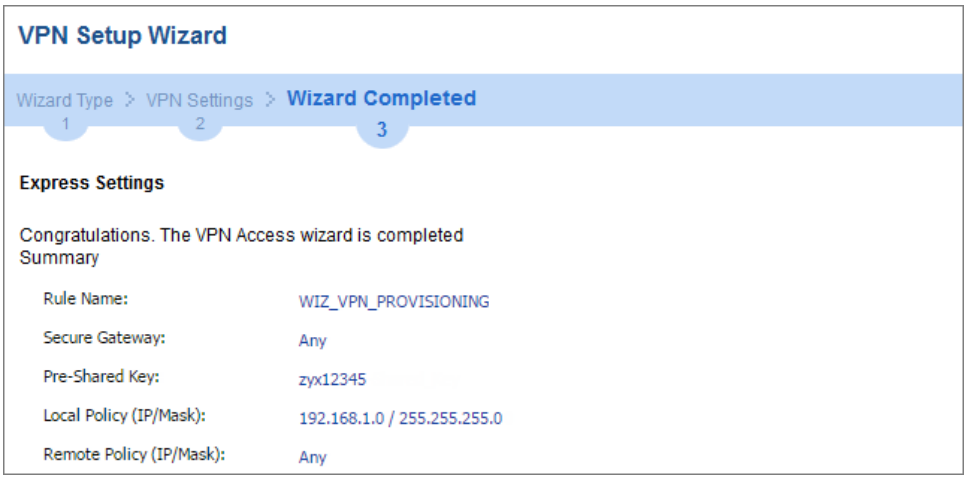


This screen provides a read-only summary of the VPN tunnel. Click **Save**.

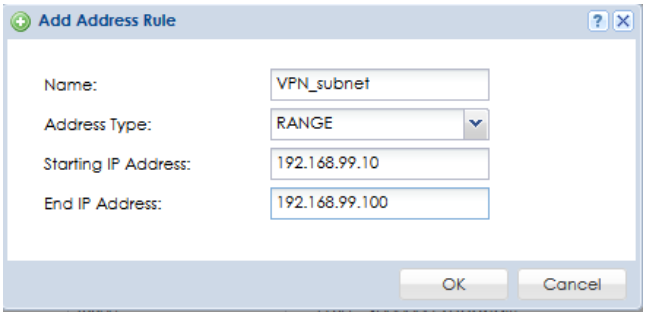
Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-3

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.

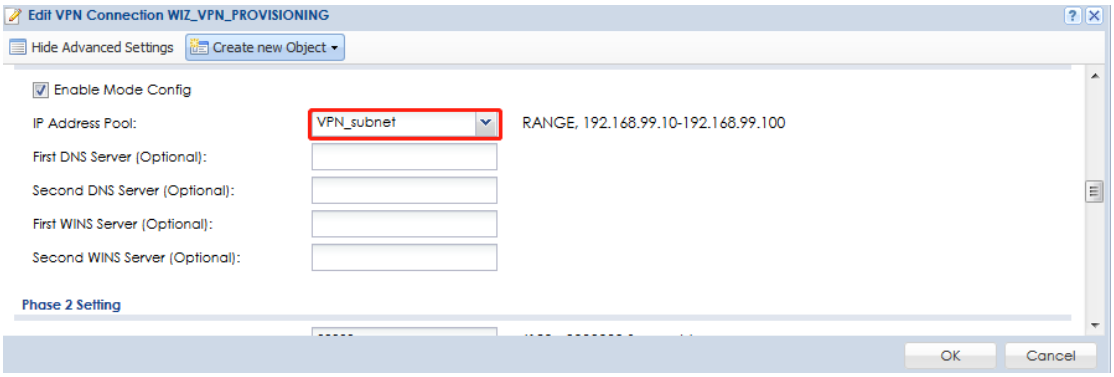
Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



Go to **CONFIGURATION > VPN > IPSec VPN > VPN connection.** Enable **Mode config** for IPSec VPN client connection, create address object

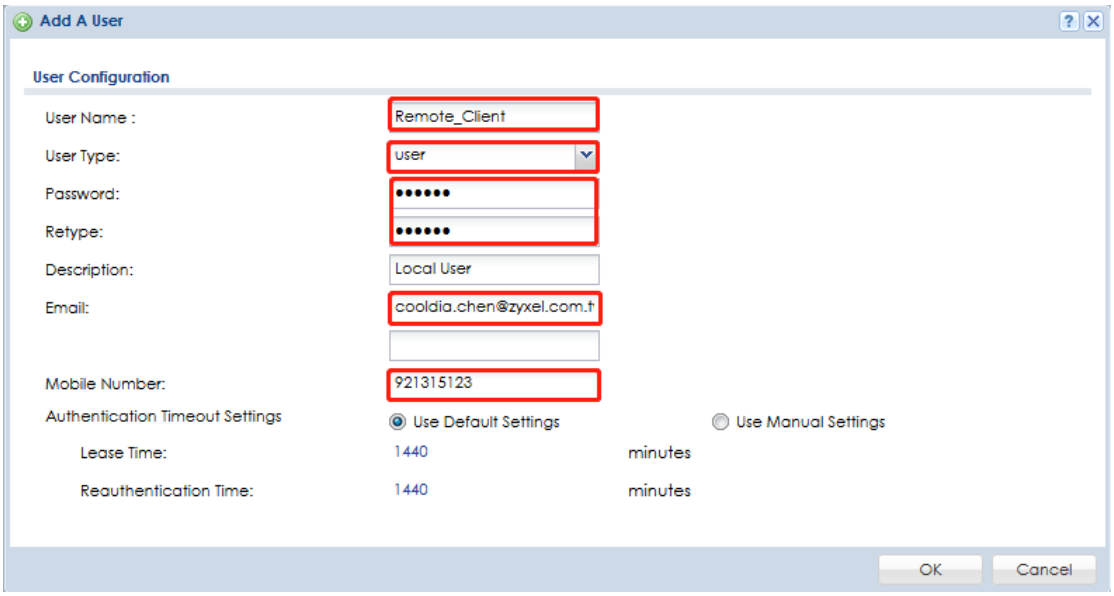


Select the address object for mode config VPN IP address Pool.

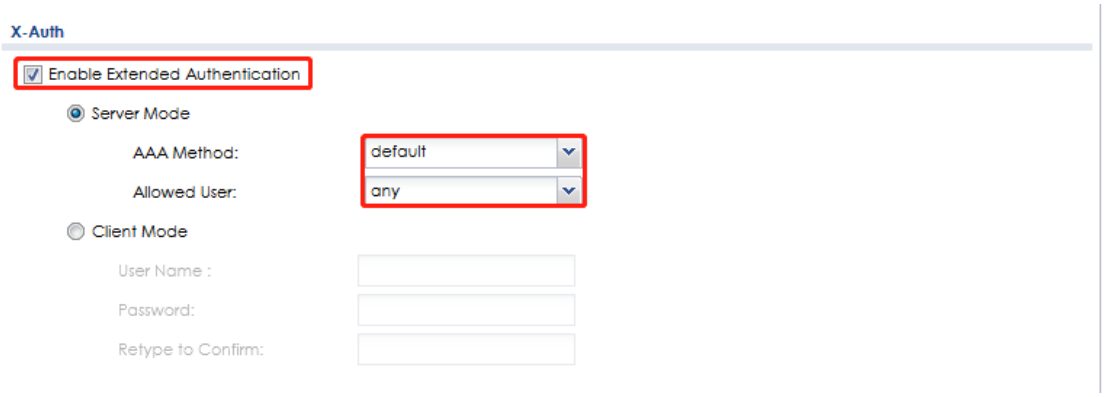


Go to **CONFIGURATION > Object > User/Group > Add A User** and create a user account for the ZyWALL IPSec VPN Client user. Type one or more valid email addresses and valid mobile telephone number for this user so that messages can be sent to this user for 2 factor authentication.

CONFIGURATION > Object > User/Group > Add A User



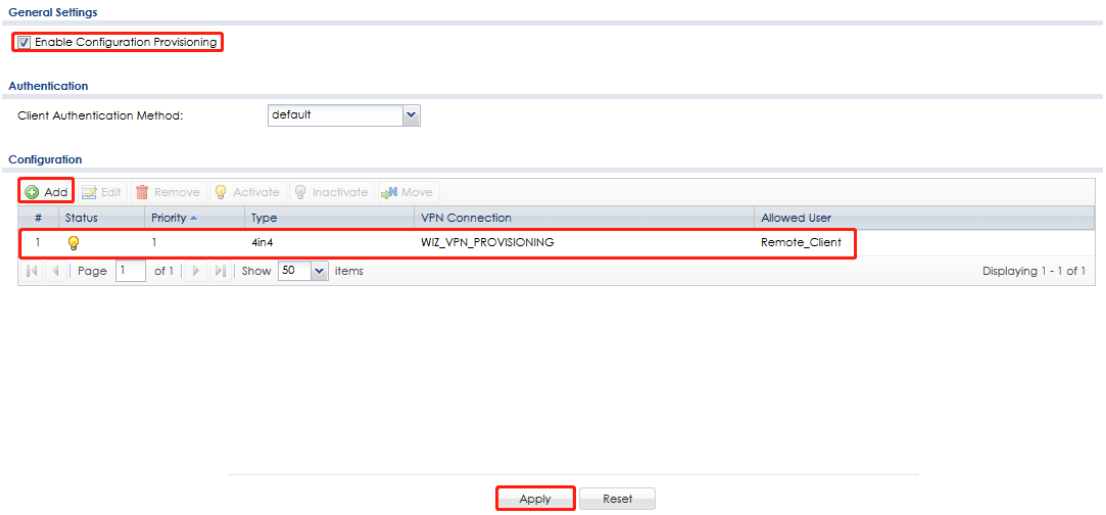
Go to **CONFIGURATION > VPN > IPSec VPN > Gateway**, enable X-Auth for VPN client authentication.



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.

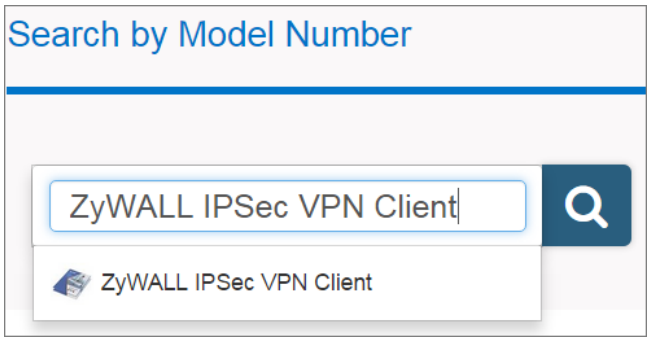
CONFIGURATION > VPN > IPSec VPN > Configuration Provisioning



Set up the ZyWALL IPSec VPN Client

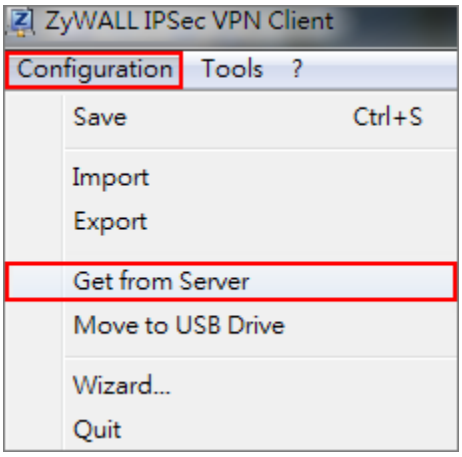
Download **ZyWALL IPSec VPN Client** software from ZyXEL Download Library:

http://www.zyxel.com/support/download_landing.shtml



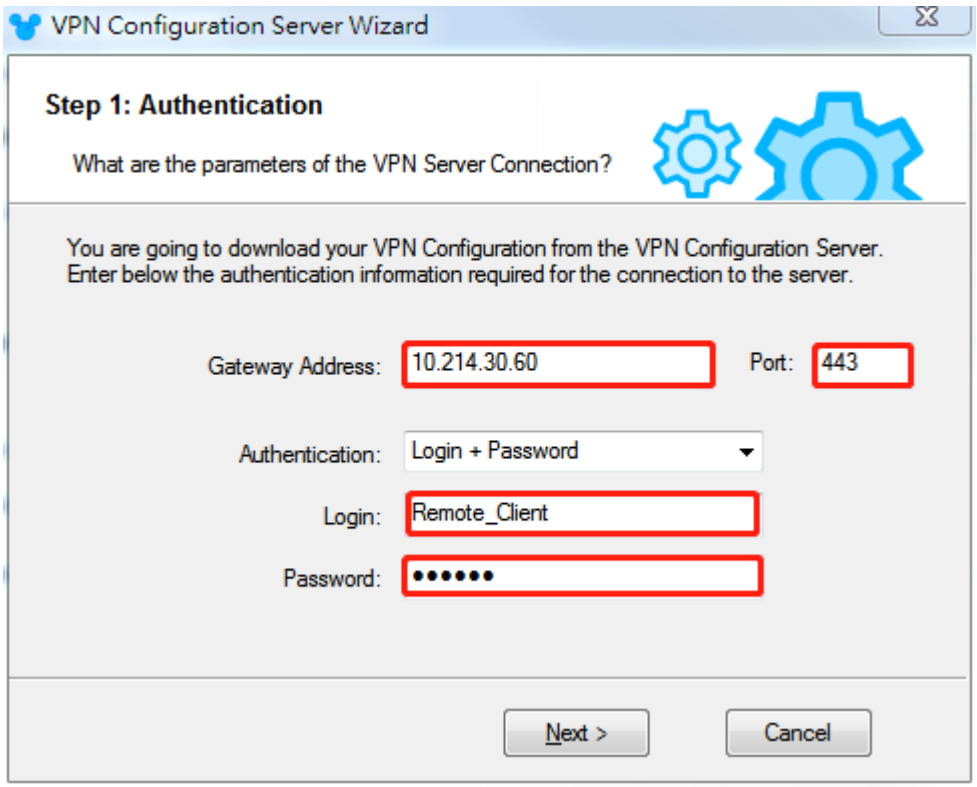
Open ZyWALL IPSec VPN Client, select **CONFIGURATION > Get from Server**.

CONFIGURATION > Get from Server

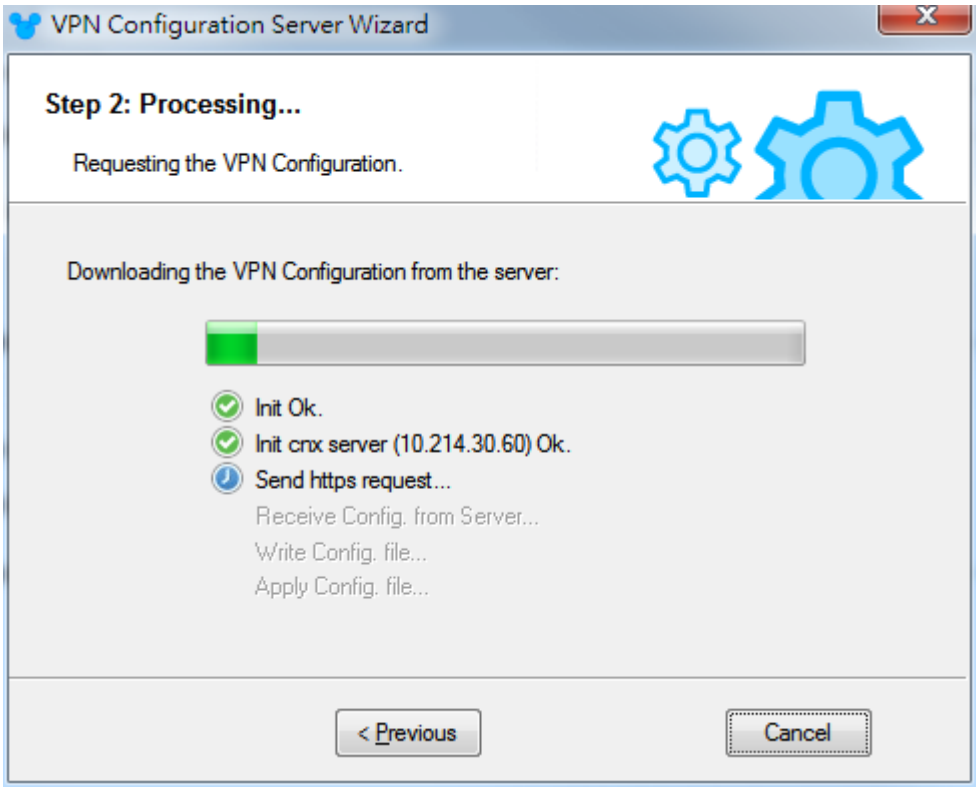


Enter the WAN IP address or URL for the ZyWALL/USG in the **Gateway Address**. If you changed the default HTTPS **Port** on the ZyWALL/USG, and then enter the new one here. Enter the **Login** user name and **Password** exactly as configured on the ZyWALL or external authentication server. Click **Next**, you will see it's processing VPN configuration from the server.

CONFIGURATION > Get from Server > Step 1: Authentication

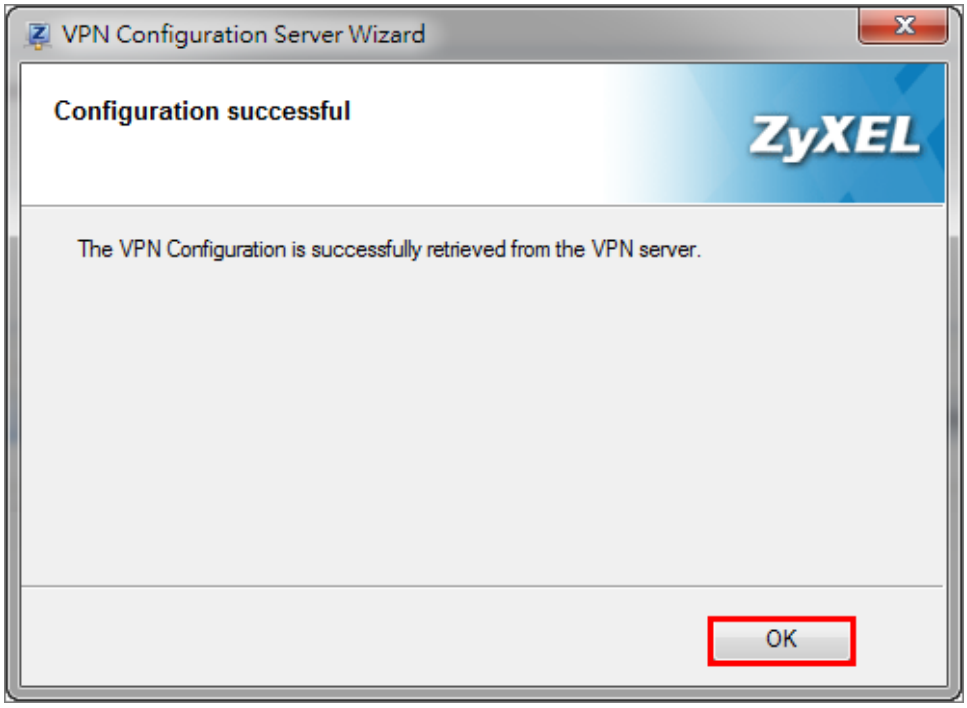


CONFIGURATION > Get from Server > Step 2: Processing

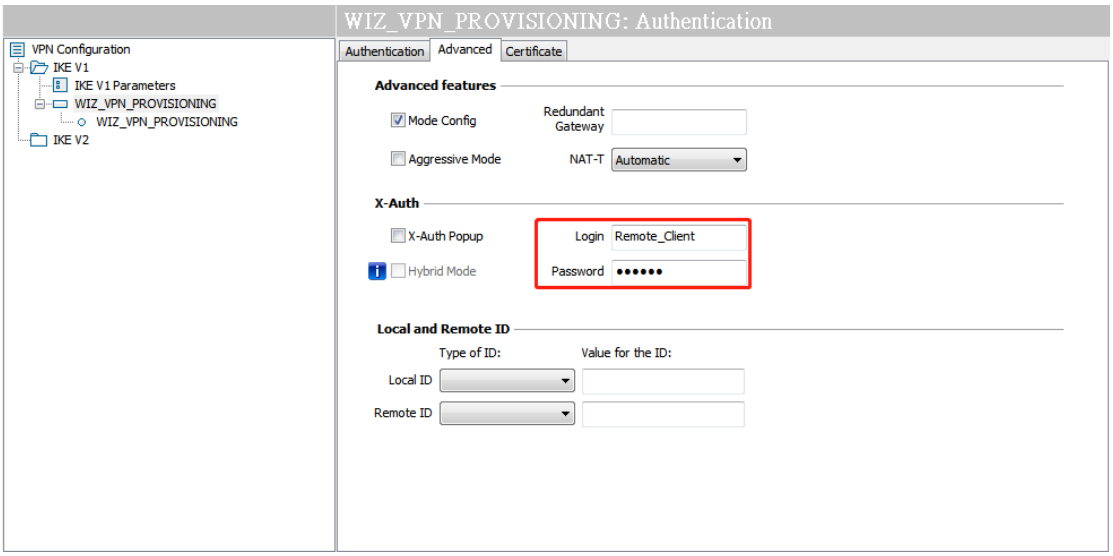


Then, you will see the **Configuration successful** page, click **OK** to exit the wizard.

CONFIGURATION > Get from Server > Configuration successful



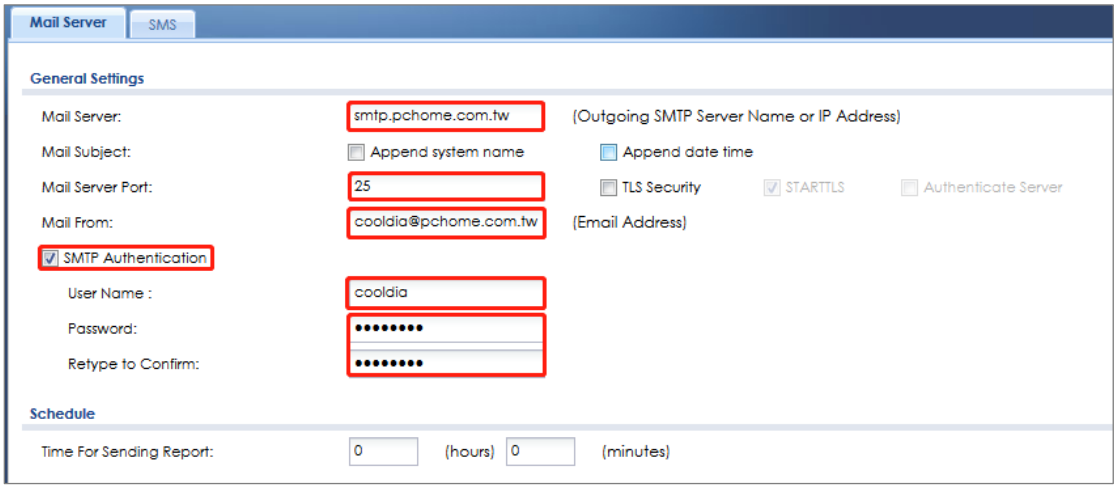
VPN CONFIGURATION > IKE V1 > WIZ_VPN_PROVISIONING > Advanced, type Login account and password for authentication.



Set up notification for 2 factor authentication

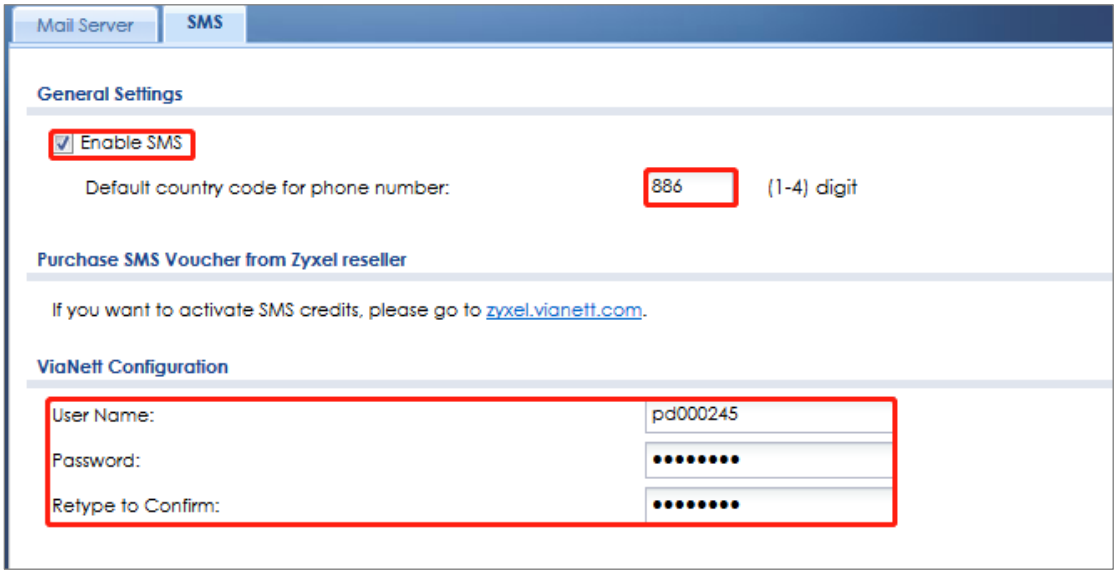
In the ZyWALL/USG, go to **CONFIGURATION > System > Notification > Mail Server**

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.



Go to 2nd tab **CONFIGURATION > System > Notification > SMS,** in this scenario, we will use email and SMS for 2 factor authentication.

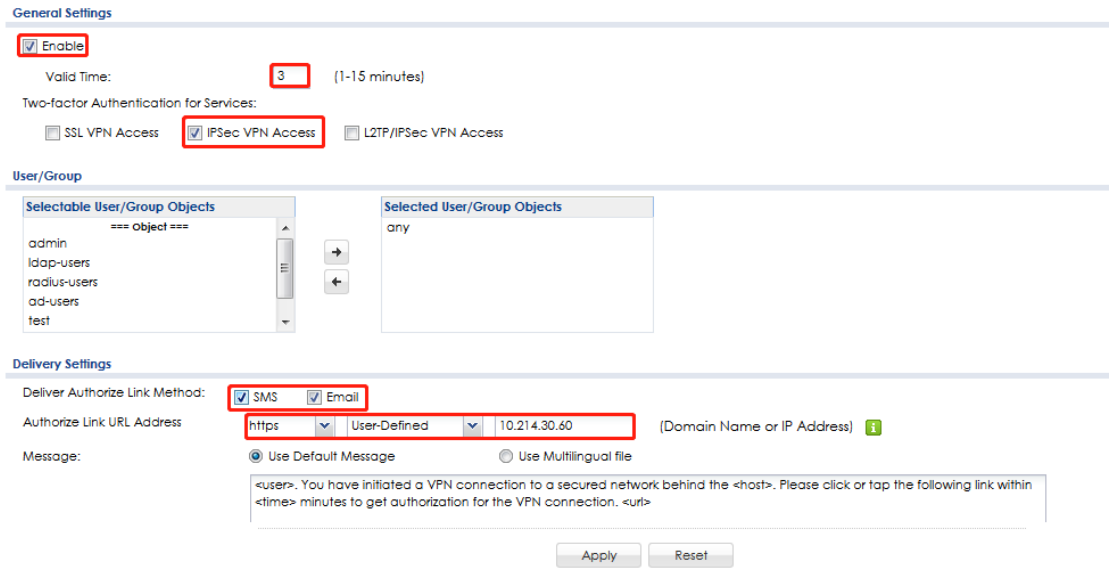
1. Select the check box "Enable SMS" to turn on the SMS service.
2. Enter the default country code for the mobile phone number to which you want to send SMS messages.
3. Enter the user name and password for your ViaNett account.
4. Click **"Apply"** button to save your changes to the Zyxel Device.



Set up authentication for 2 factor VPN connection

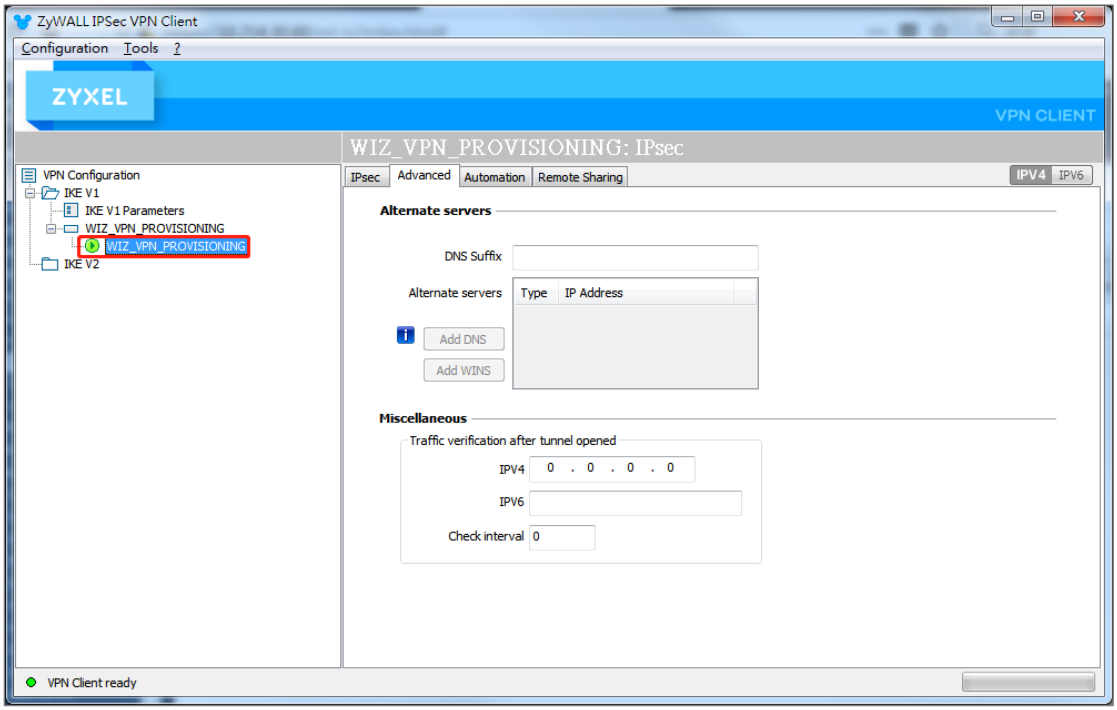
In the ZyWALL/USG, go to **CONFIGURATION > Object > Auth.Method > Two-factor Authentication.**

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.



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



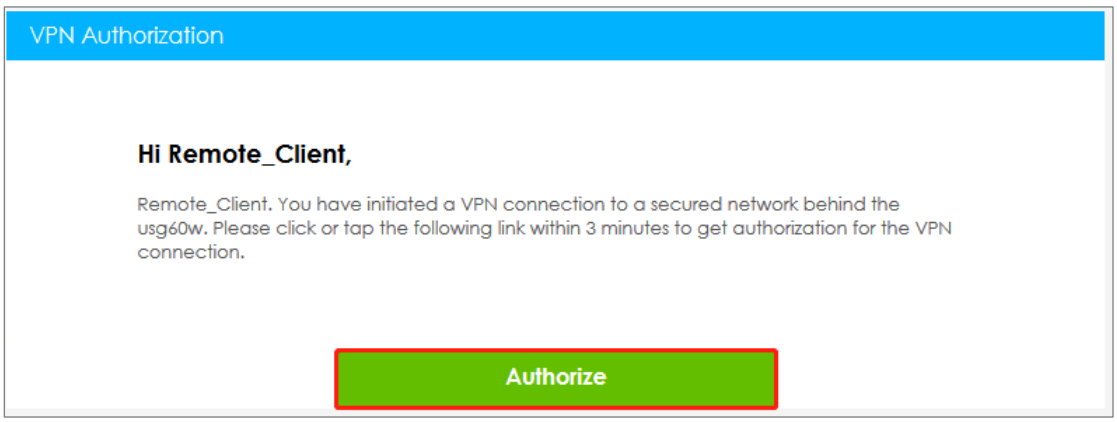
The VPN tunnel is created from the ZyWALL IPSec VPN client to the ZyWALL/USG, but we are still unable to access Intranet behind the ZyWALL/USG. The ZyWALL/USG send authorized link via phone number or email address in order to authenticate this user's

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.

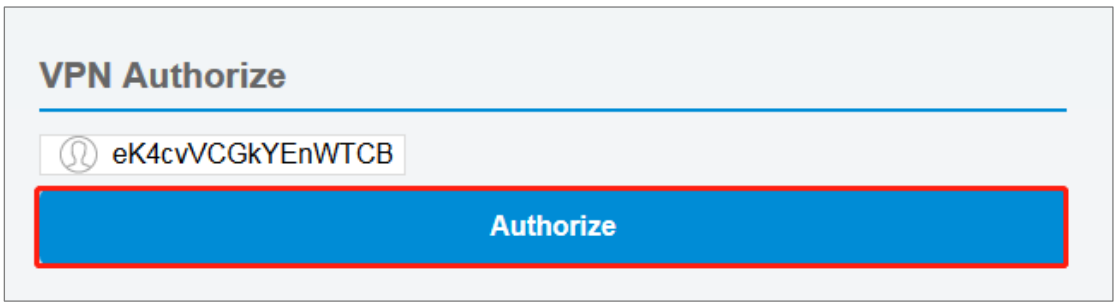
The following is authorized example by email and SMS

Authorized by email link

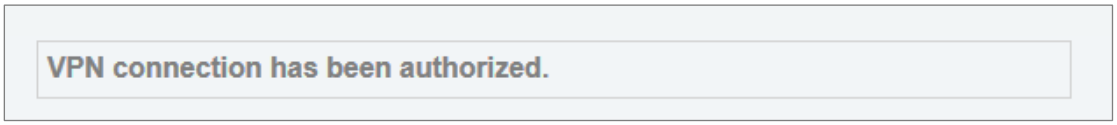
1. Received authorization mail with authorize link.



2. Click the **"Authorize" to** authorization.

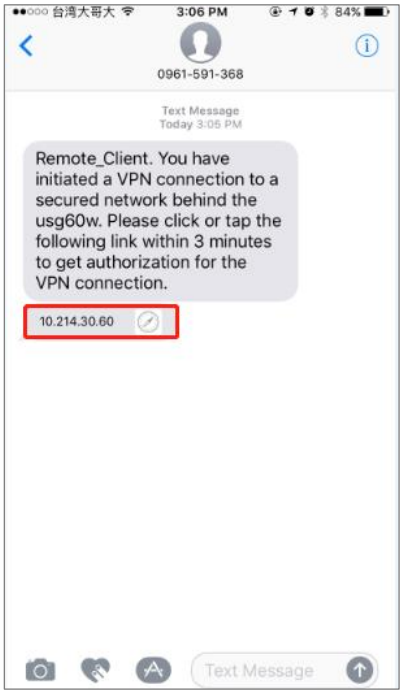


3. After we see "**VPN connection has been authorized**", we can access the secured network behind the ZyWALL/USG.

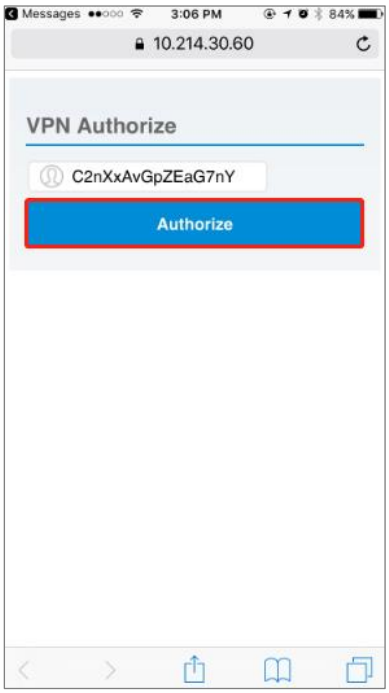


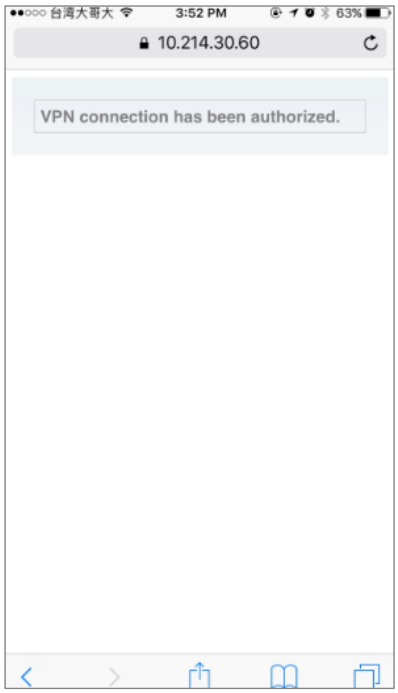
Authorized by SMS

1. Received authorization SMS with authorize link.



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.





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 ...

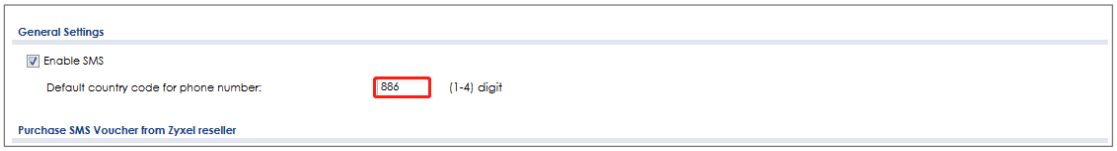
If you see below log message "**Cannot resolve mail server address smtp.pchome.com.t**" please check "**CONFIGURATION > System > Notification > SMTP Server**", Make sure your service IP/hostname is correct for mail authentication.

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

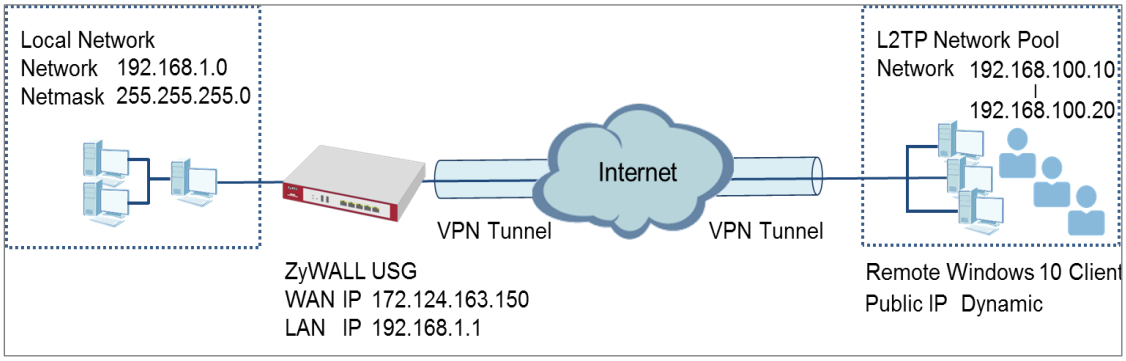
CONFIGURATION > System > Notification > SMS



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

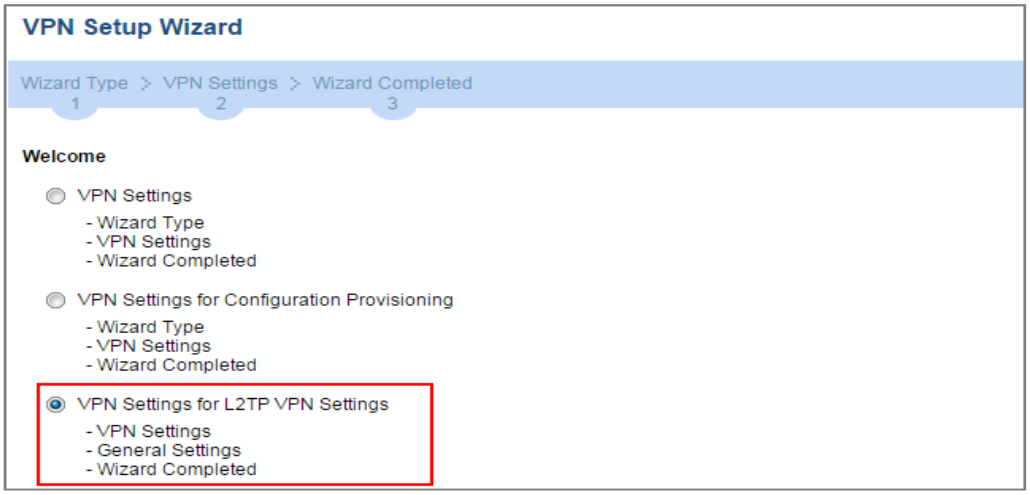


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and Android (Version: 10.0.10240)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

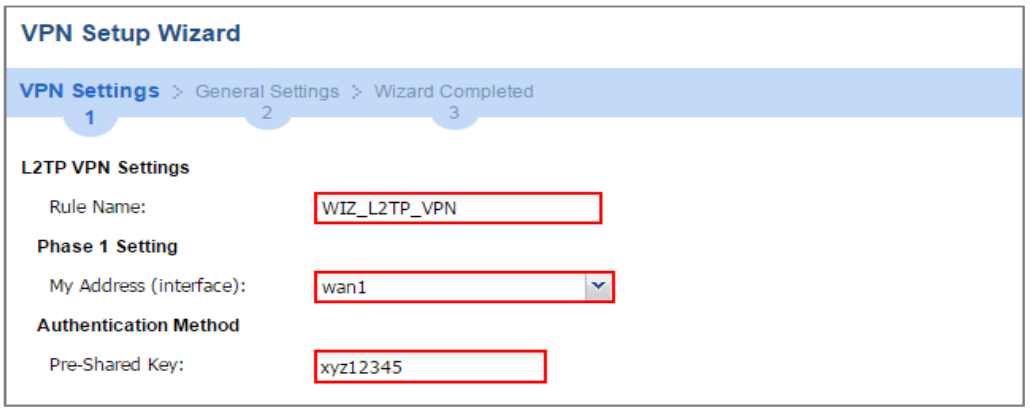
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the Android mobile phone clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



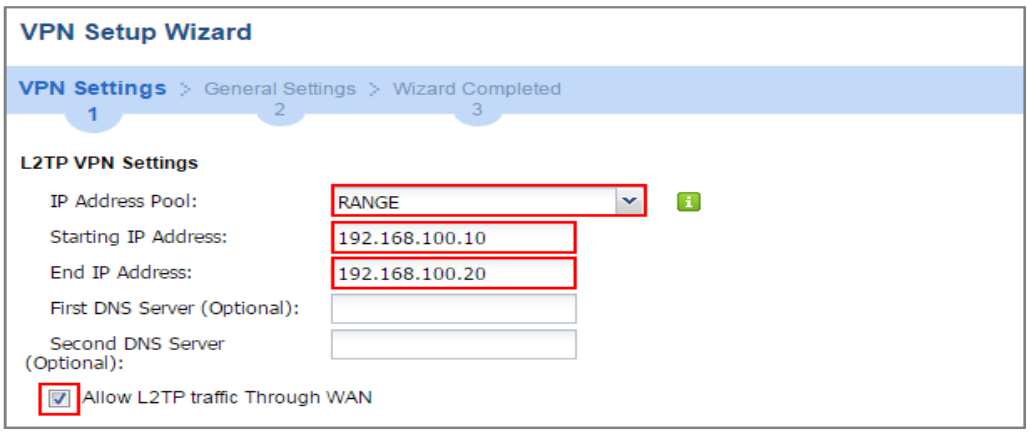
Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



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)



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

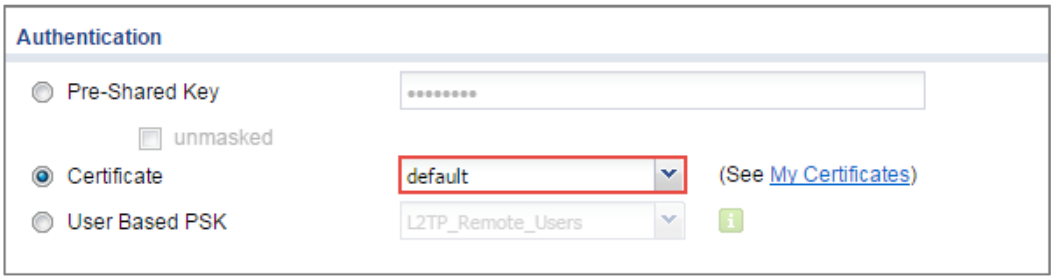
Quick Setup > VPN Setup Wizard > Welcome > VPN Settings (Summary)

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

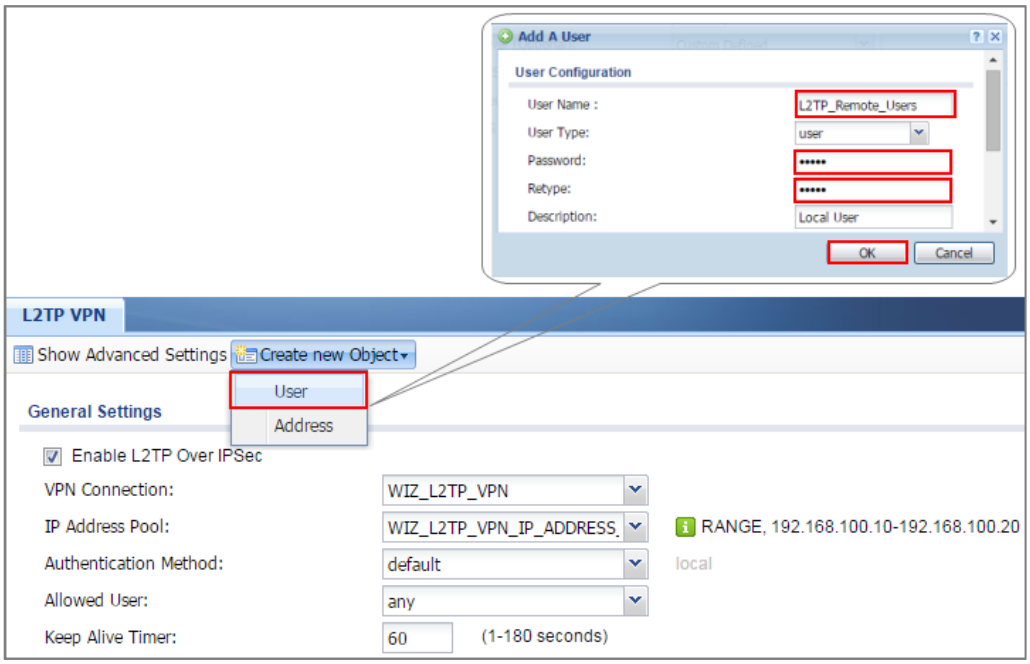
Go to **CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN**, change **Authentication** method to be **Certificate** and select the certificate which ZyWALL/USG uses to identify itself to the Android mobile phone.

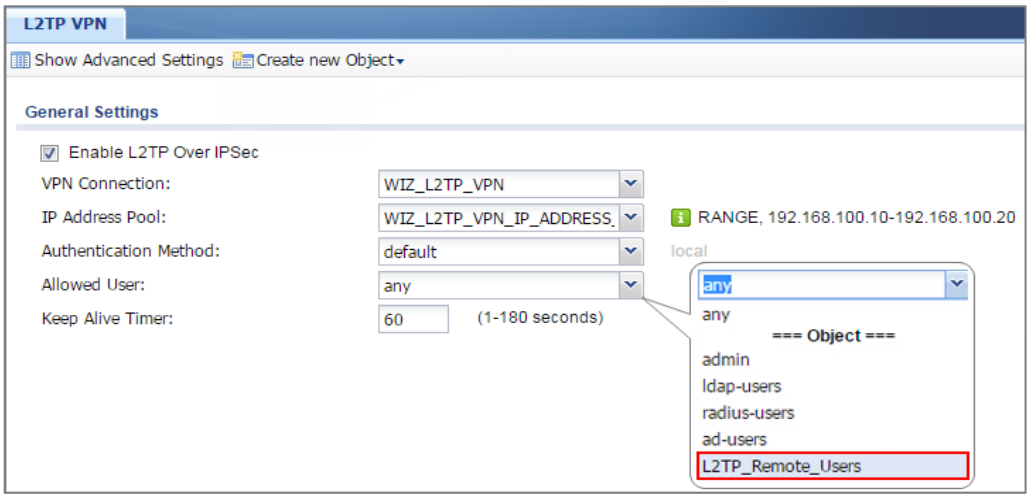
CONFIGURATION > VPN > VPN Gateway > WIZ_L2TP_VPN > Authentication > Certificate



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

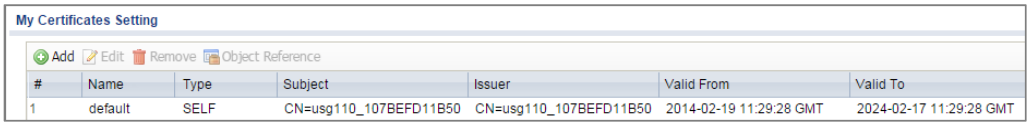

Add A User
User Configuration
User Name :
L2TP_Remote_Users
User Type:
user
Password:
Retype:
Description:
Local User
OK
Cancel
L2TP VPN
Show Advanced Settings
Create new Object
User
Address
General Settings
Enable L2TP Over IPSec
VPN Connection:
WIZ_L2TP_VPN
IP Address Pool:
WIZ_L2TP_VPN_IP_ADDRESS
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
Show Advanced Settings
Create new Object
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)
any
any
=== Object ===
admin
ldap-users
radius-users
ad-users
L2TP_Remote_Users

Export a Certificate from ZyWALL/USG and Import it to Android Mobile Phone

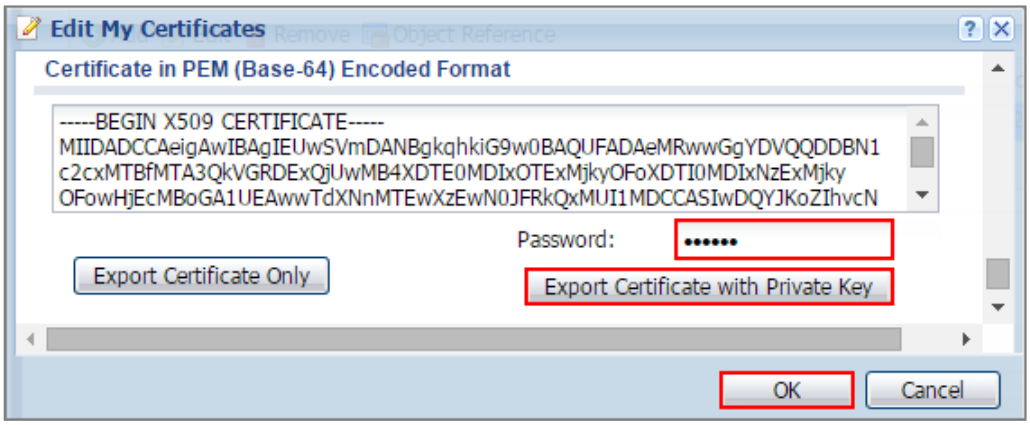
Go to ZyWALL/USG **CONFIGURATION > Object > Certificate**, select the certificate (**default** in this example) and click **Edit**.

CONFIGURATION > Object > Certificate > default

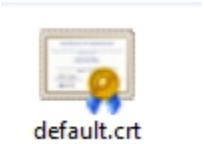


Export default certificate from ZyWALL/USG.

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only



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.

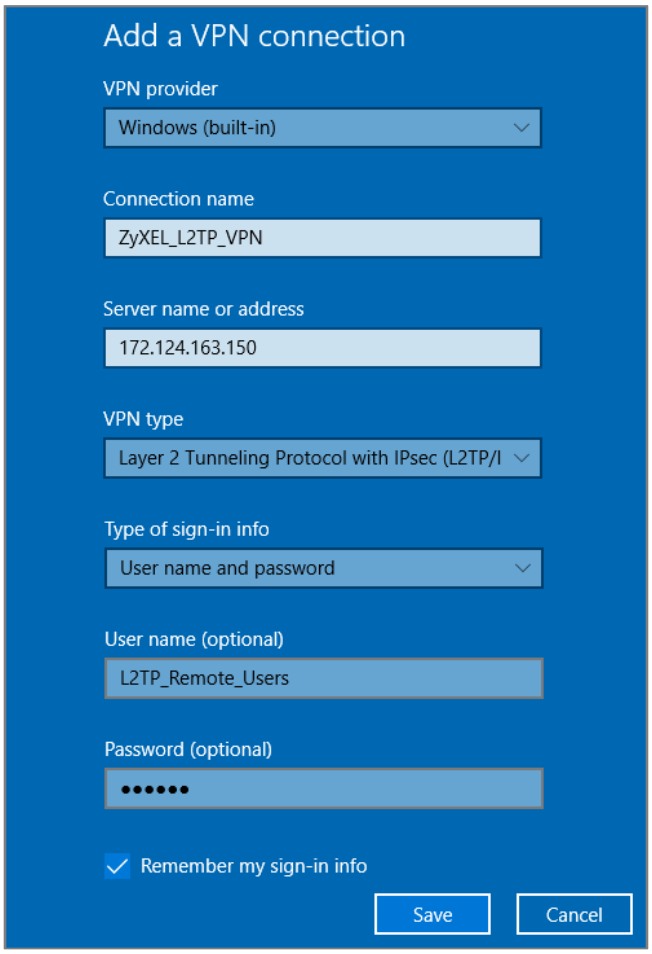
2 VPN Provider set to Windows (built-in).

3 Configure **Connection name** for you to identify the VPN configuration.

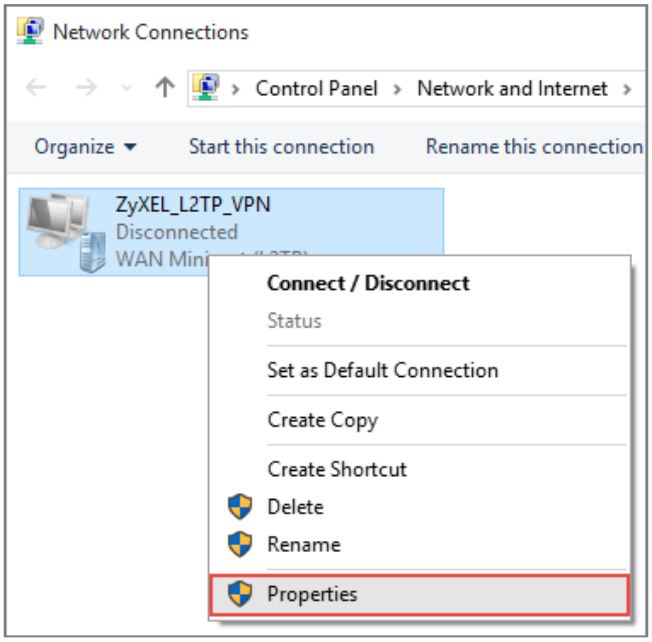
4 Set **Server** name or address to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).

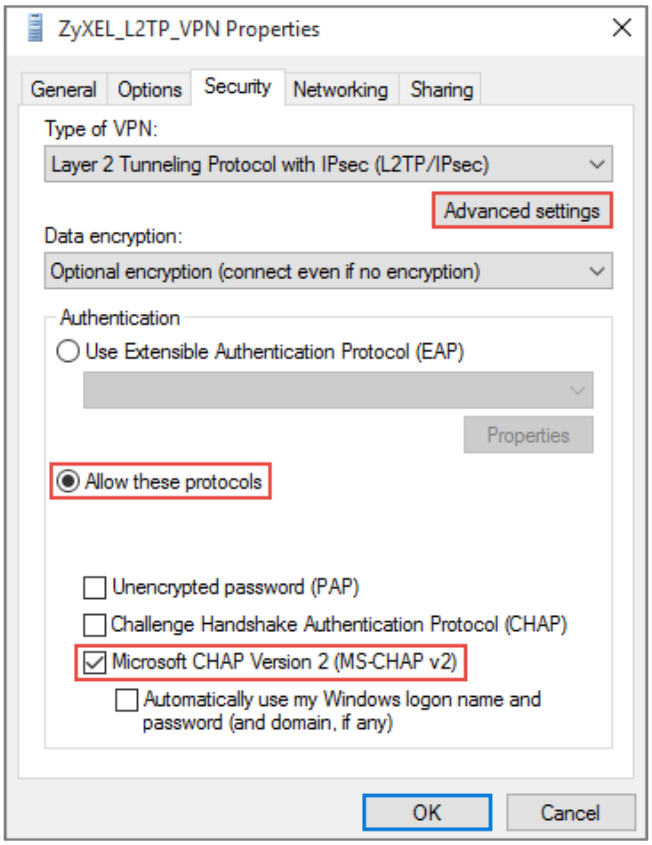
5 Select VPN type to Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec).

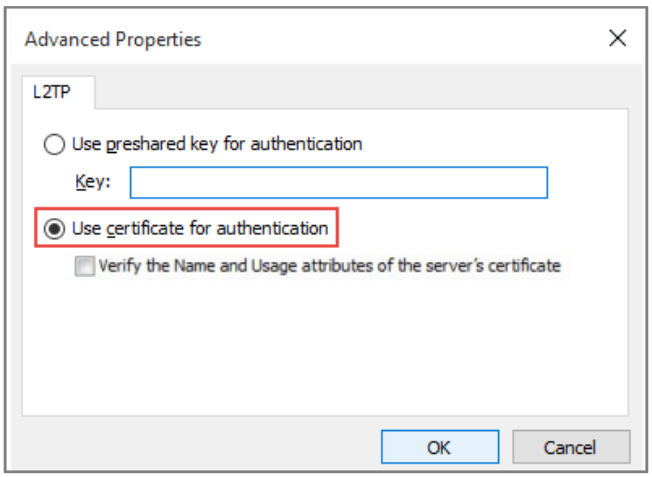
6 Enter **User name** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).



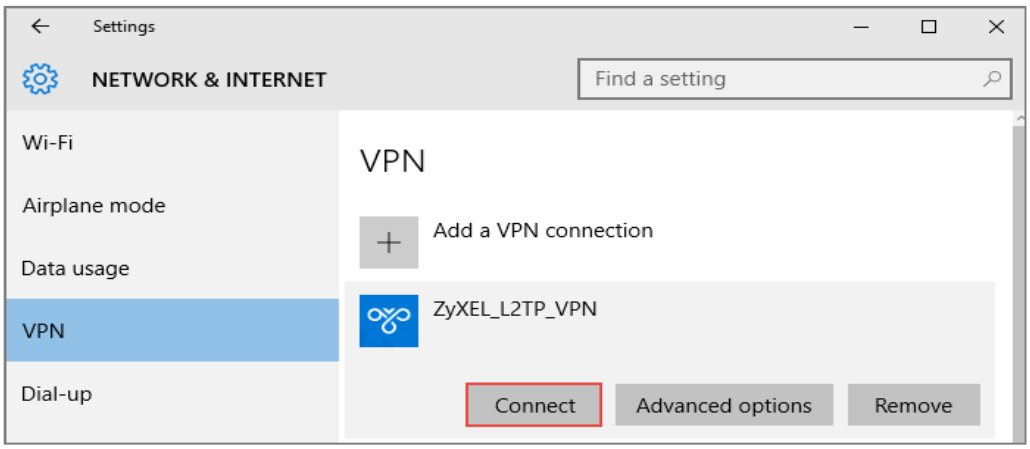
Go to **Control Panel > Network and Internet > Network Connections** and right click **Properties.** Continue to **Security > Advanced settings** and select **Use Certificate for authentication**.


Network Connections
Control Panel › Network and Internet ›
Organize
Start this connection
Rename this connection
ZyXEL_L2TP_VPN
Disconnected
Connect / Disconnect
Status
Set as Default Connection
Create Copy
Create Shortcut
Delete
Rename
Properties


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



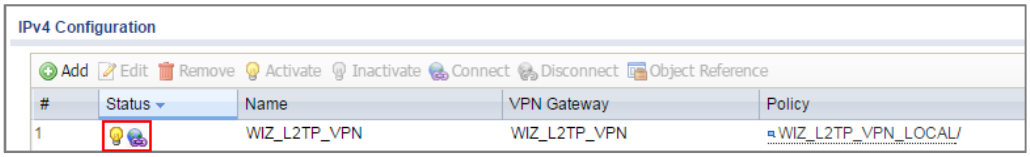
Go to **Network & Internet Settings** window, click **Connect**.



Test the L2TP over IPSec VPN Tunnel

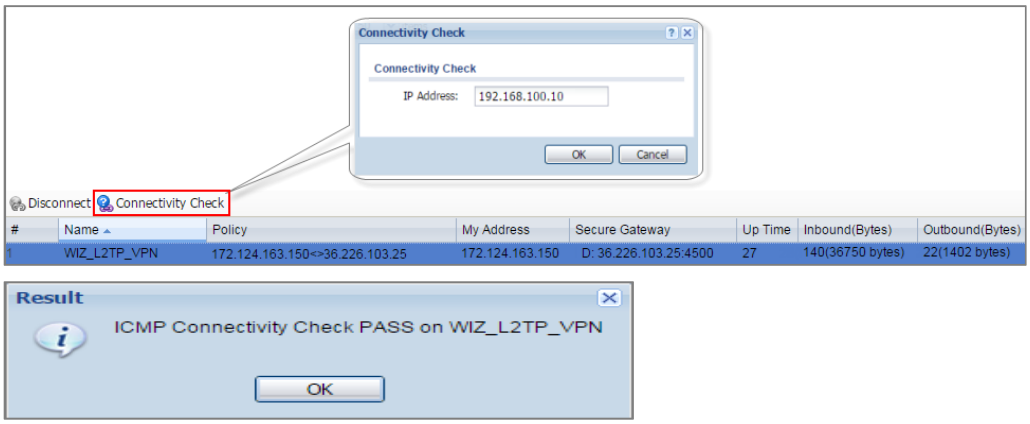
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



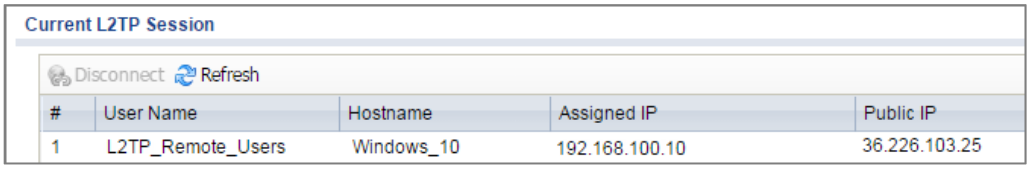
Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic. Click **Connectivity Check** to verify the result of ICMP Connectivity.

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



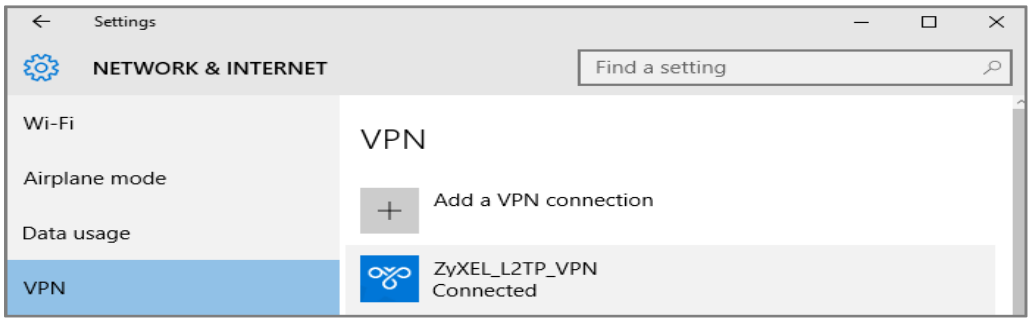
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users



Go to Android **Start > Settings > Network & Internet > VPN** and show **Connected** status.

Menu > Settings > VPN > ZyXEL_L2TP



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.

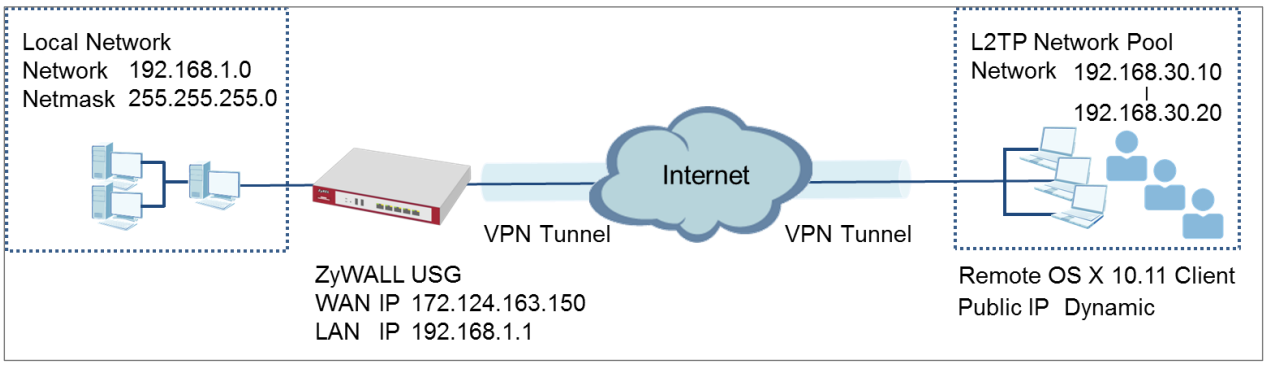
12 Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

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

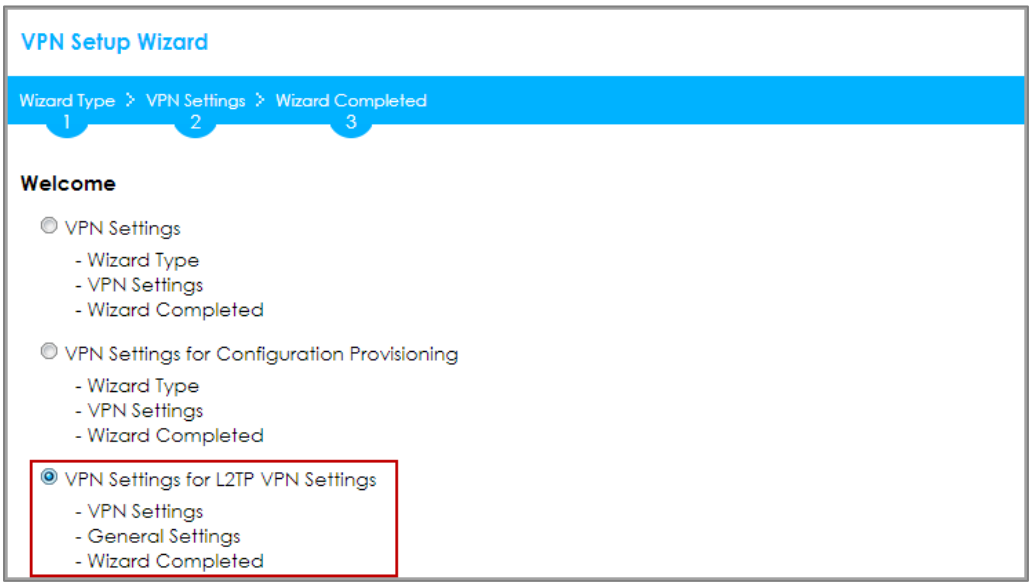


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and Apple MAC (Version: OS X10.11 El Capitan).

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

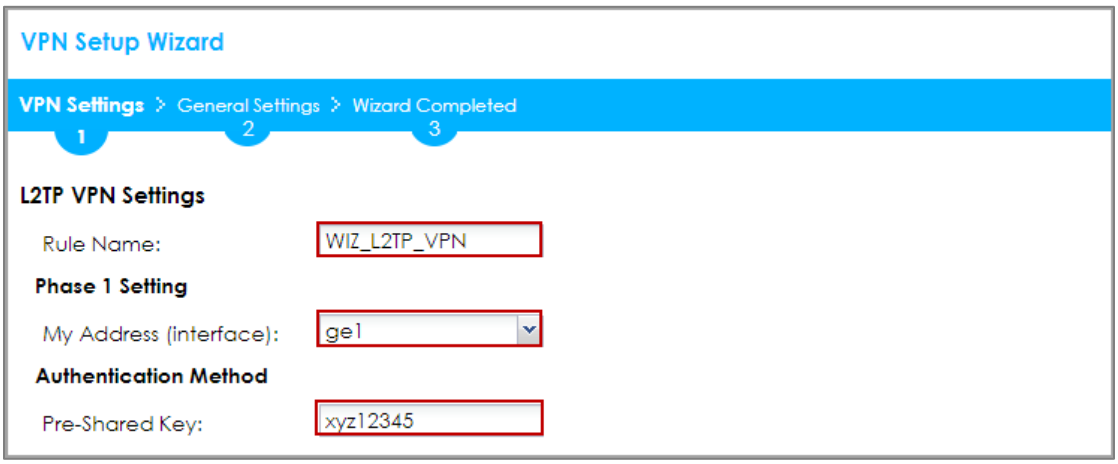
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings for L2TP VPN Settings** wizard to create a **L2TP VPN** rule that can be used with the MAC OS X clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



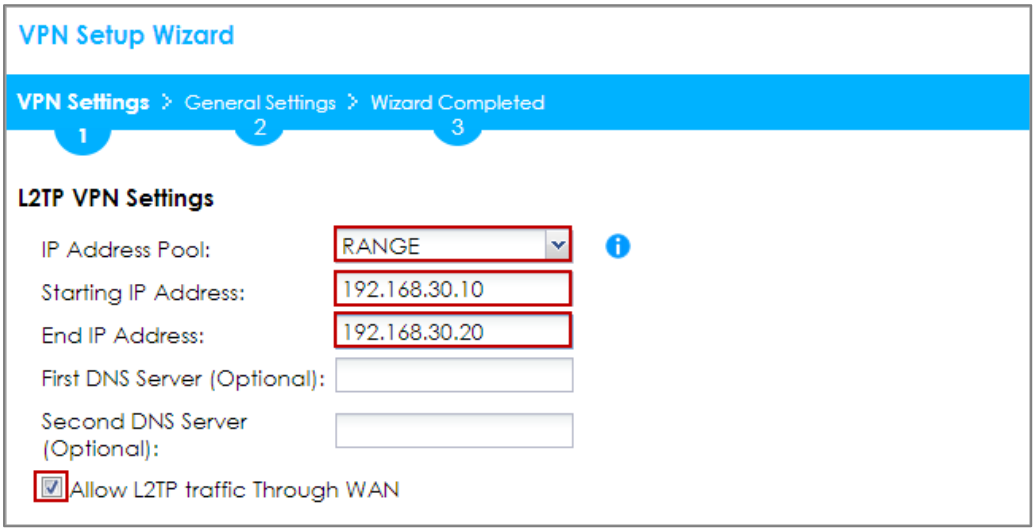
Then, configure the **Rule Name** and set **My Address** to be the **wan1** interface which is connected to the Internet. Type a secure **Pre-Shared Key** (8-32 characters).

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



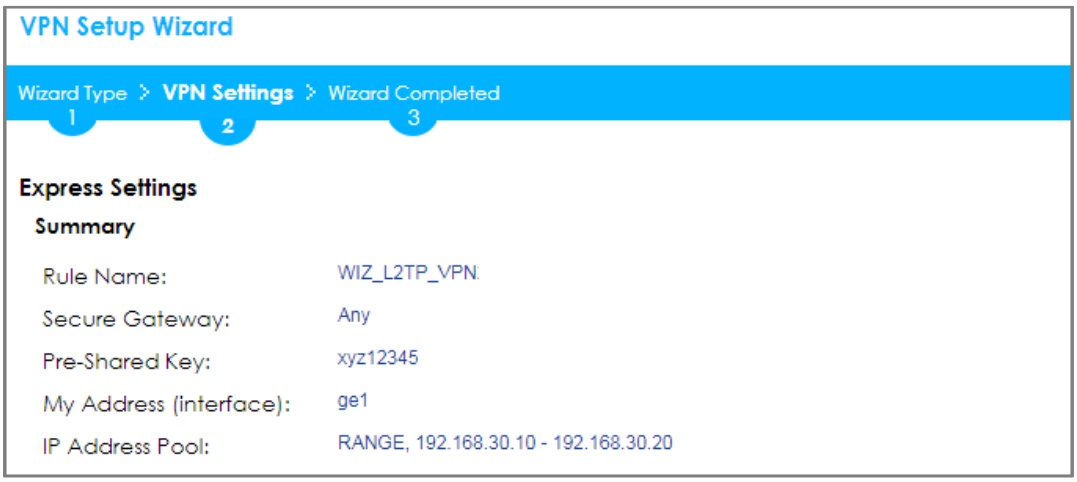
Configure the L2TP users' IP address range from 192.168.30.10 to 192.168.30.20 for use in the L2TP VPN tunnel and check **Allow L2TP traffic Through WAN**. Click **OK**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

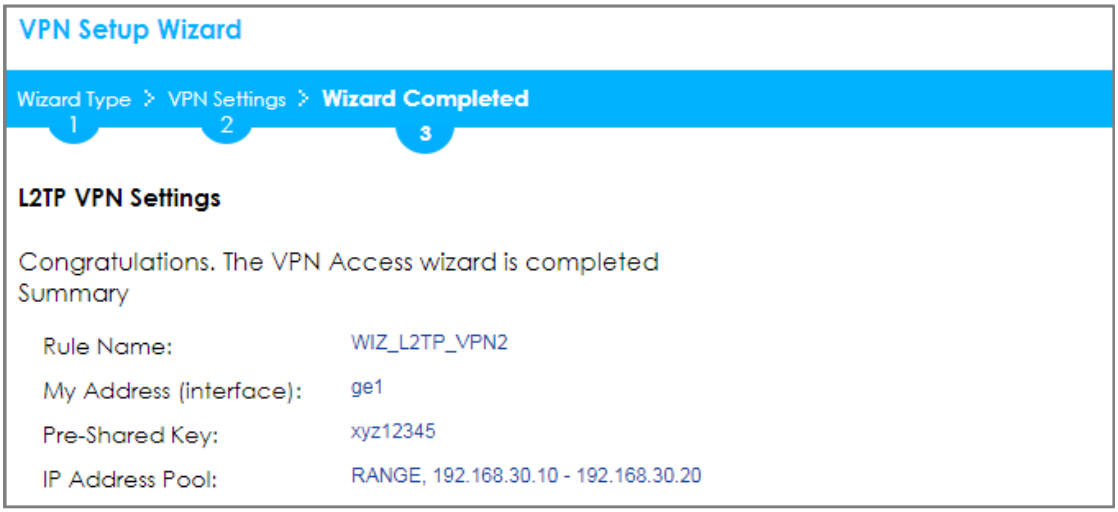


Continue to the next page to review your **Summary** and click **Save**.

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Summary

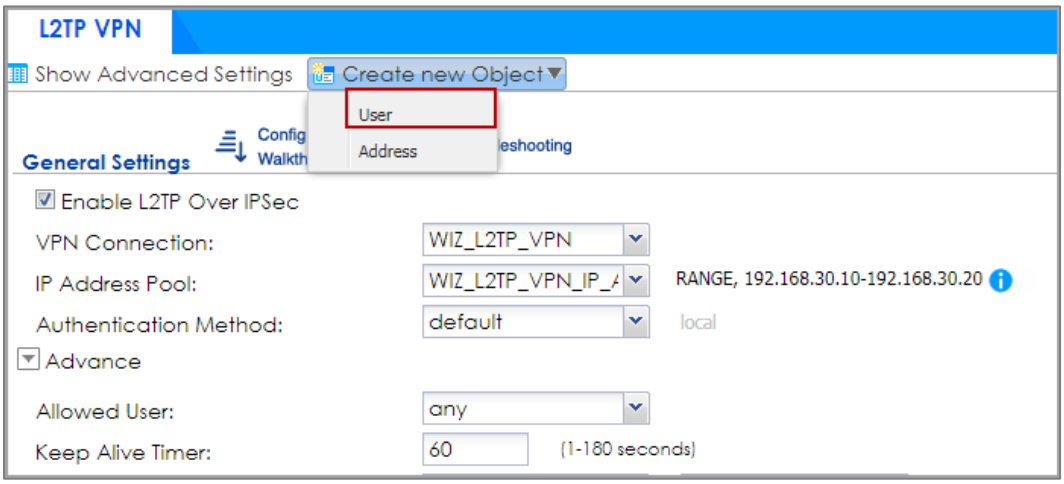


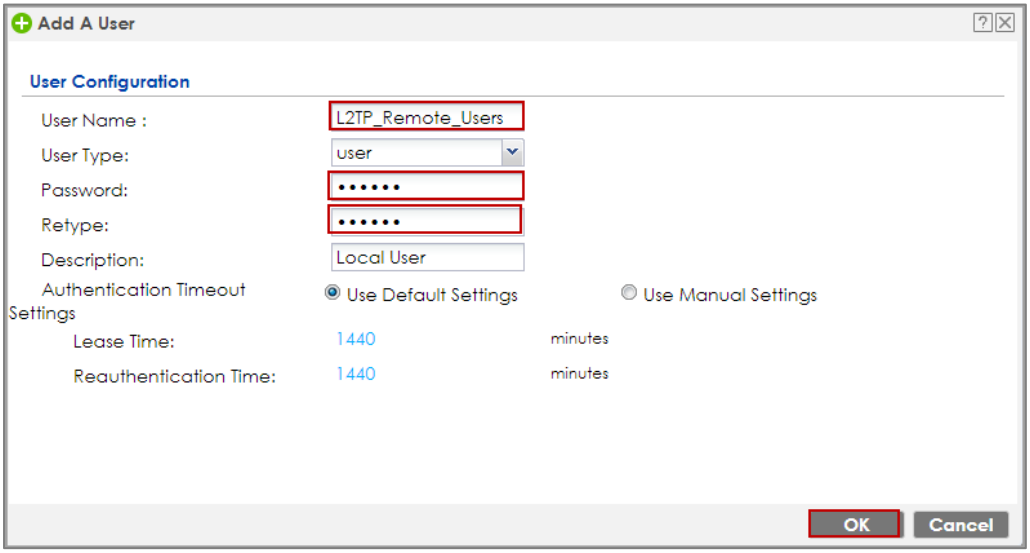
Quick Setup > VPN Setup Wizard > Welcome > VPN Settings > Summary > Wizard Completed

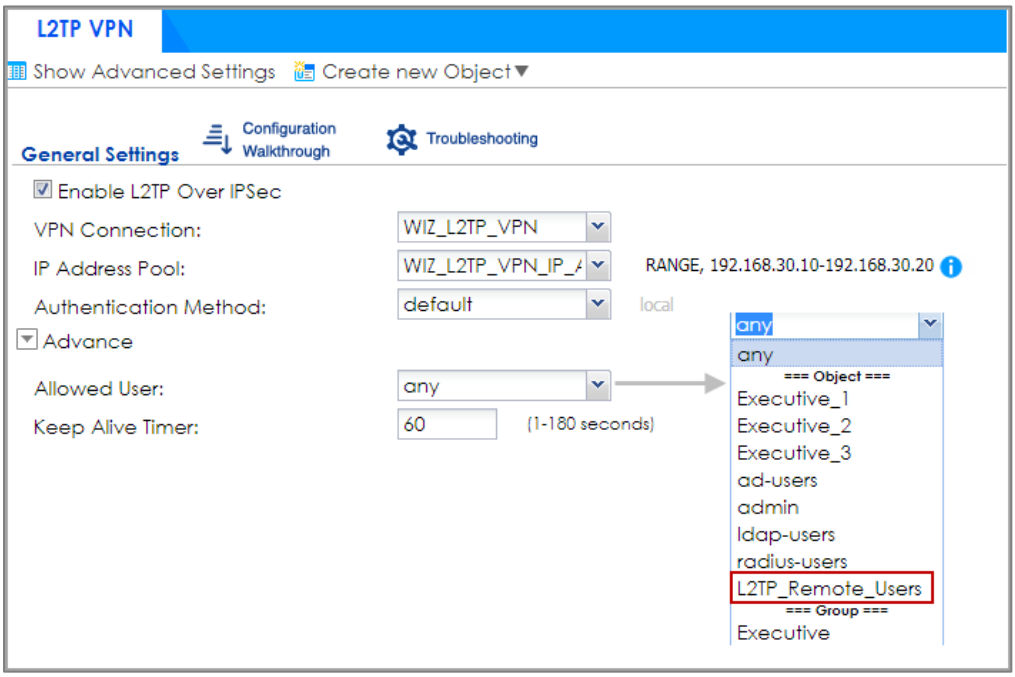


Go to **CONFIGURATION > VPN > L2TP VPN > Create new Object > User** to add **User Name** and **Password** (4-24 characters). Then, set **Allowed User** to the newly created object (L2TP_Remote_Users/zyx168 in this example).

CONFIGURATION > VPN > L2TP VPN > Create new Object > User


L2TP VPN
Show Advanced Settings
Create new Object
User
Address
General Settings
Config Walkth
eshooting
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
OK
Cancel

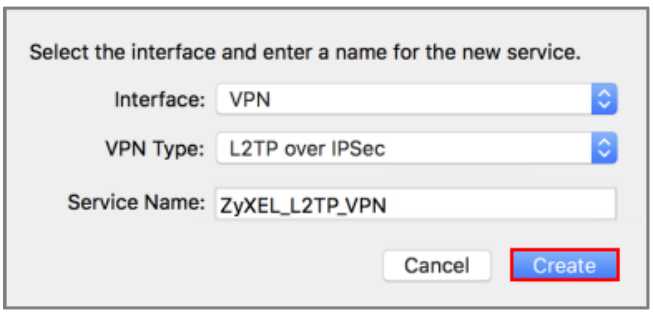


Set Up the L2TP VPN Tunnel on the Apple MAC OS X 10.11 El Capitan Operating System

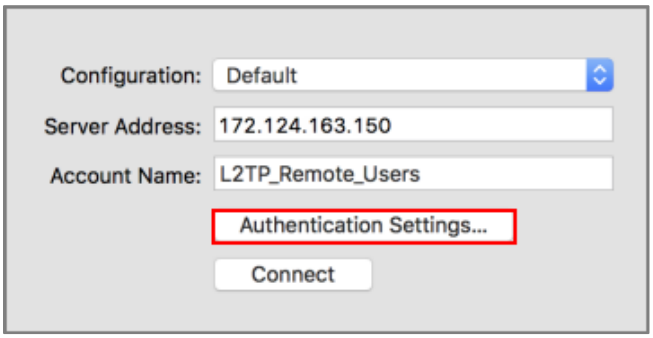
To configure L2TP VPN in OS X 10.11 operation system, go to **System Preferences… > Network,** click the "**+**" button at the bottom left of the connections to add a new connection and configure as follows.

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**.

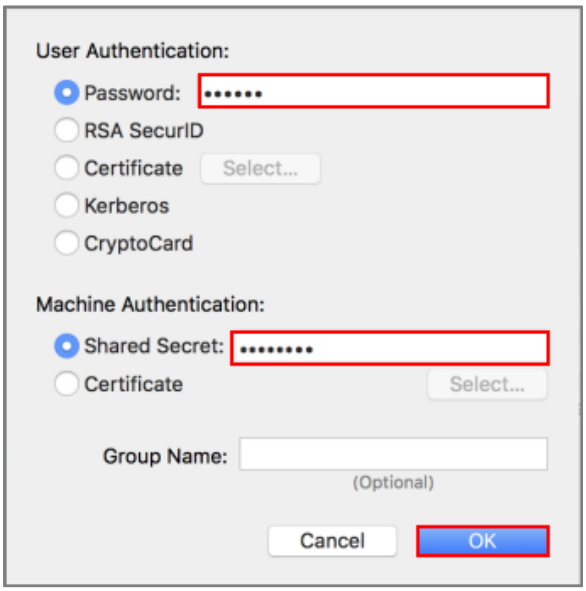


Configure **Server Address** to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example). Enter **Account Name** which should be the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users in this example). Then, click **Authentication Settings...**.

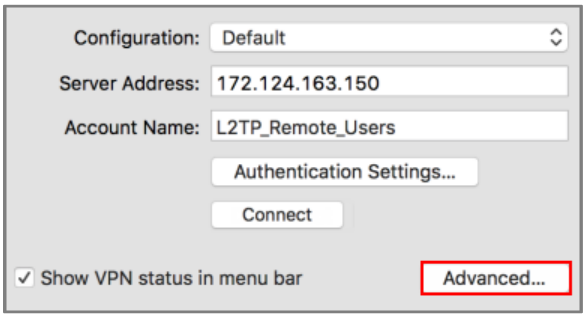


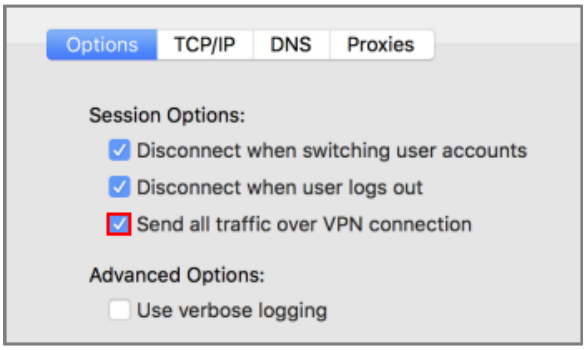
In the **User Authentication** section, enter **Password** which should be the same as **Allowed User** created in ZyWALL/USG (zyx123 in this example).

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**.

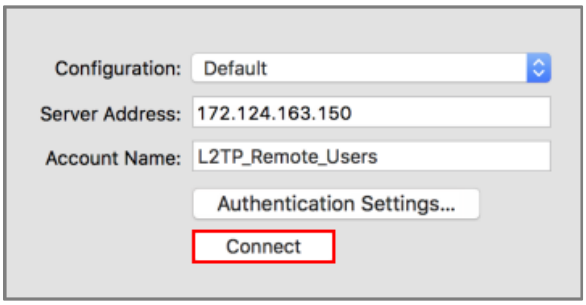


Go back to **Configuration** and click **Advanced…**. Select **Send all traffic over VPN connection** to allow the L2TP/IPSec VPN traffic between ZyWALL/USG and MAC OS X system.





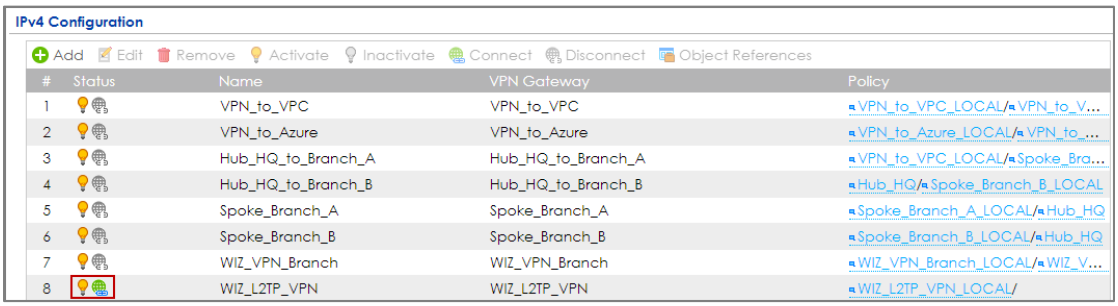
Go back to **Configuration** and click **Connect**.



Test the L2TP over IPSec VPN Tunnel

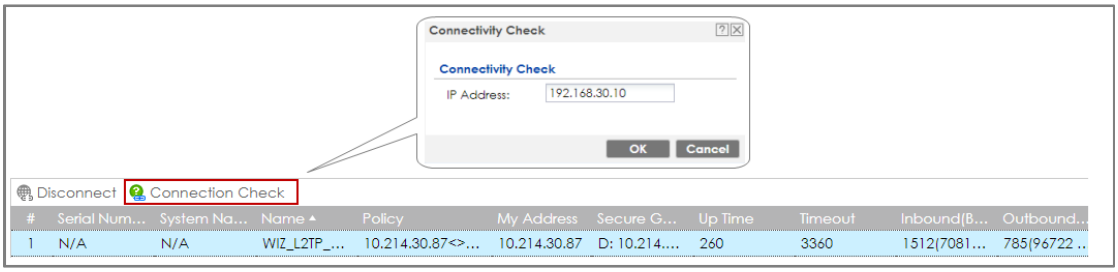
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

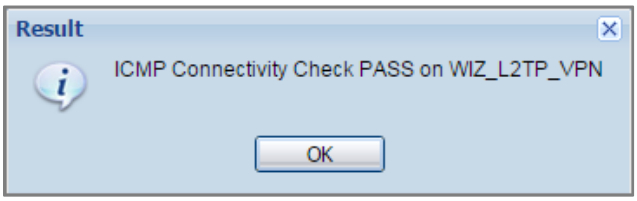
CONFIGURATION > VPN > IPSec VPN > VPN Connection



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

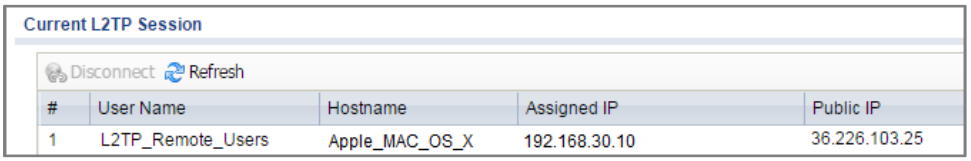




功能有問題無法截圖, **connectivity check fail**

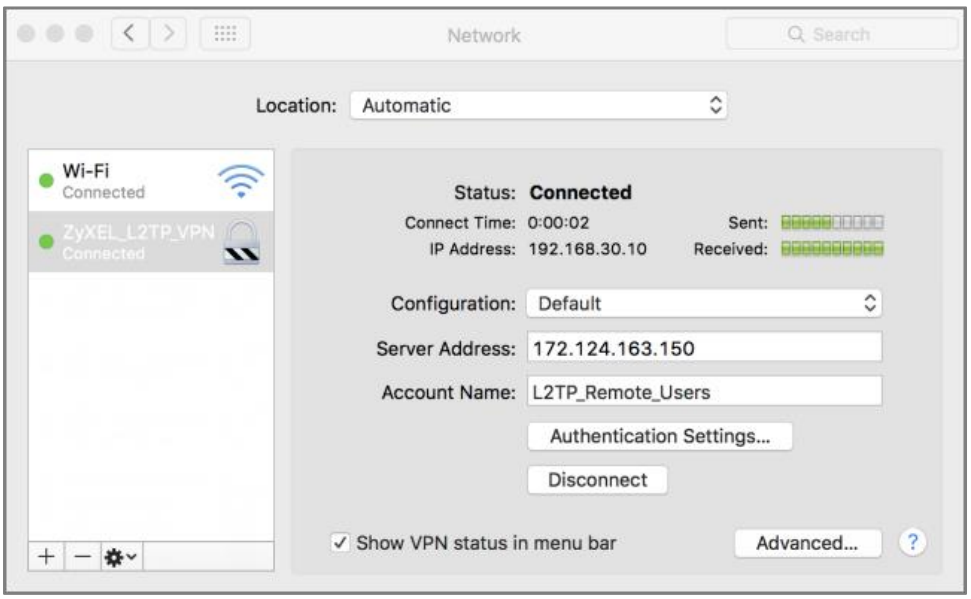
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users



Go to MAC OS X **System Preferences… > Network** and show **Connected** status, **Connect Time** and assigned **IP Address**.

System Preferences… > Network



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.

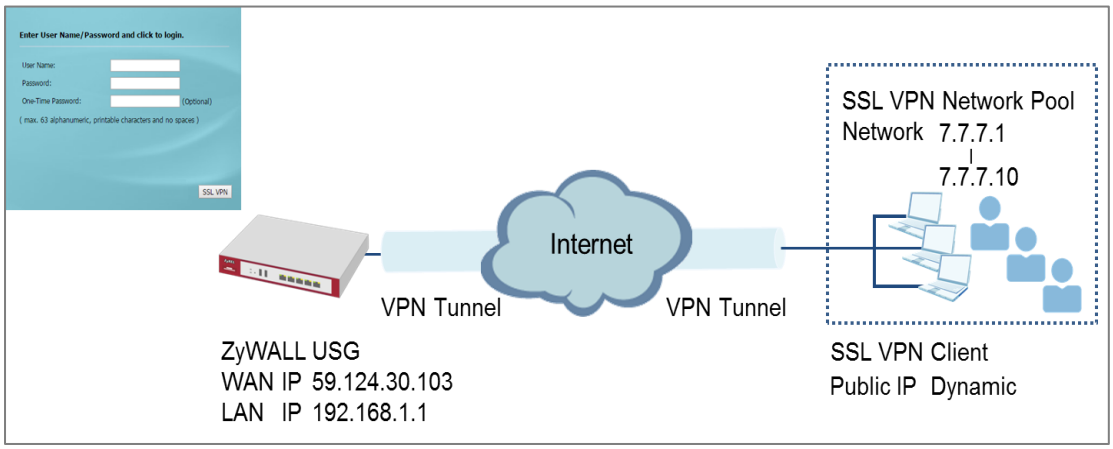
If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

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).

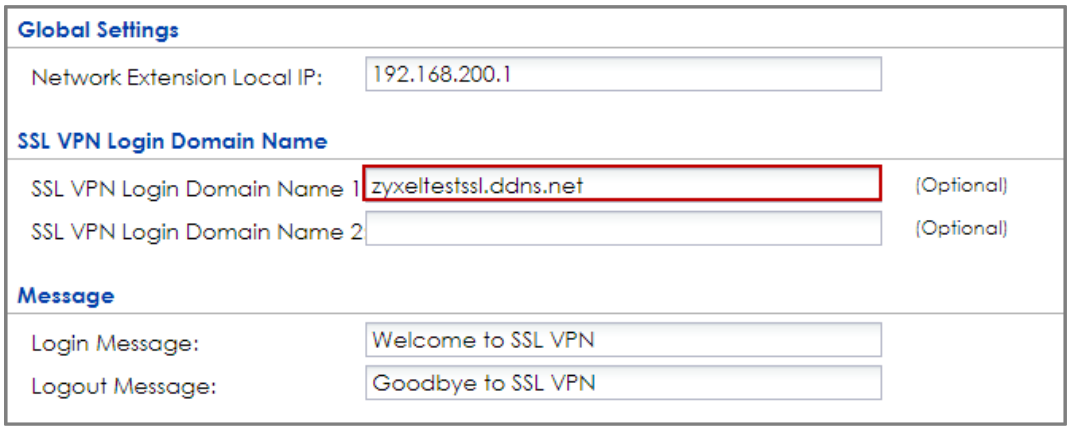
Set Up the DNS Service

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

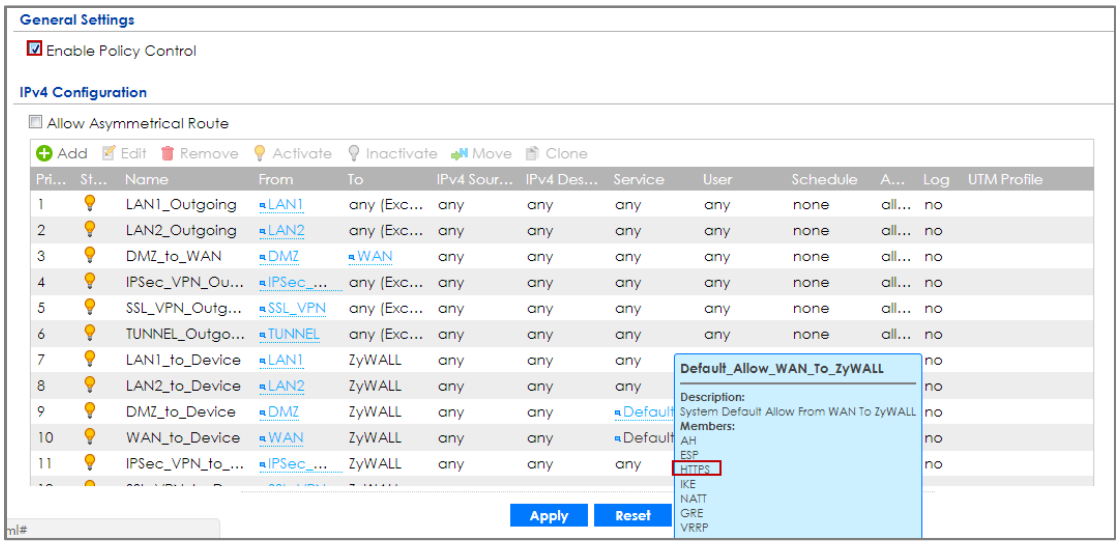
In the ZyWALL/USG, go to **CONFIGURATION > VPN > SSL VPN > Global Setting > SSL VPN Login Domain Name** and type in the DNS domain name.

CONFIGURATION > VPN > SSL VPN > Global Setting > SSL VPN Login Domain Name



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).

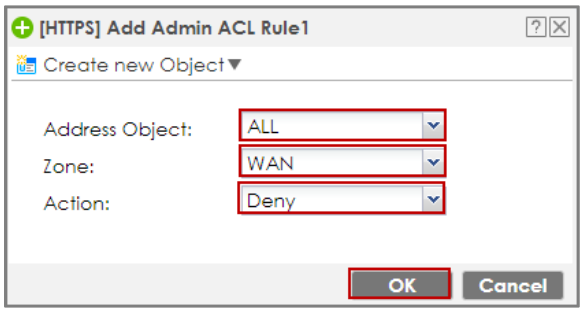
CONFIGURATION > Security Policy > Policy Control

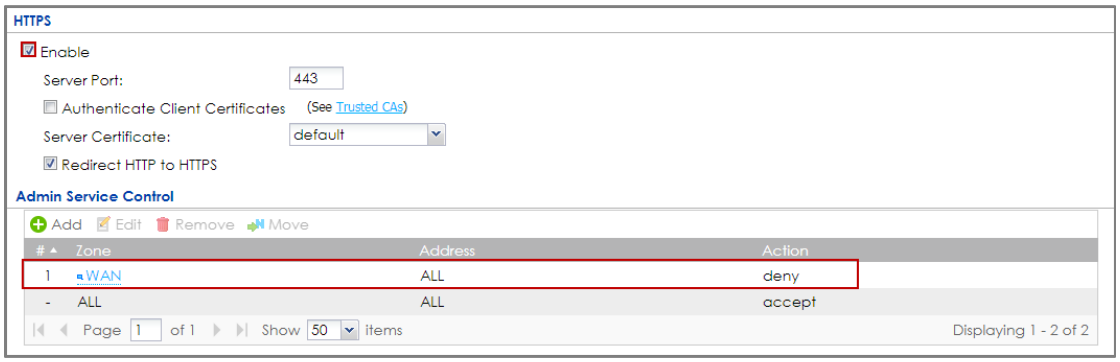


Set Up the ZyWALL/USG System Setting

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

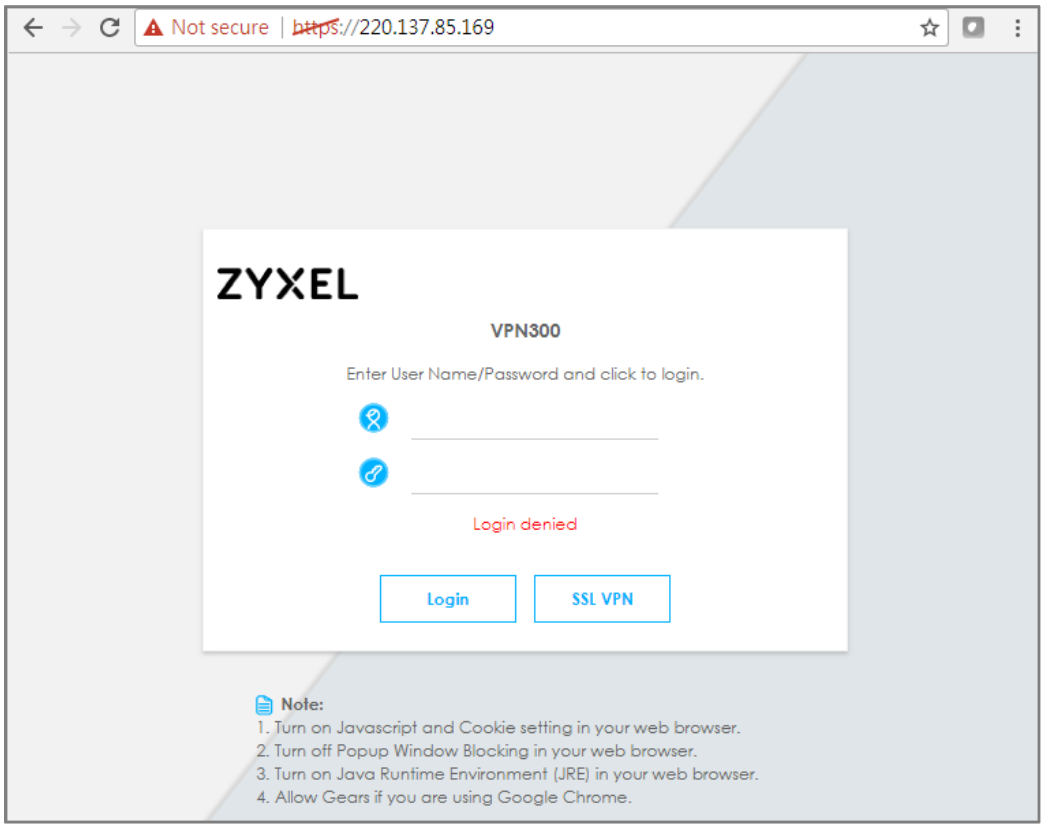




Test the SSL VPN

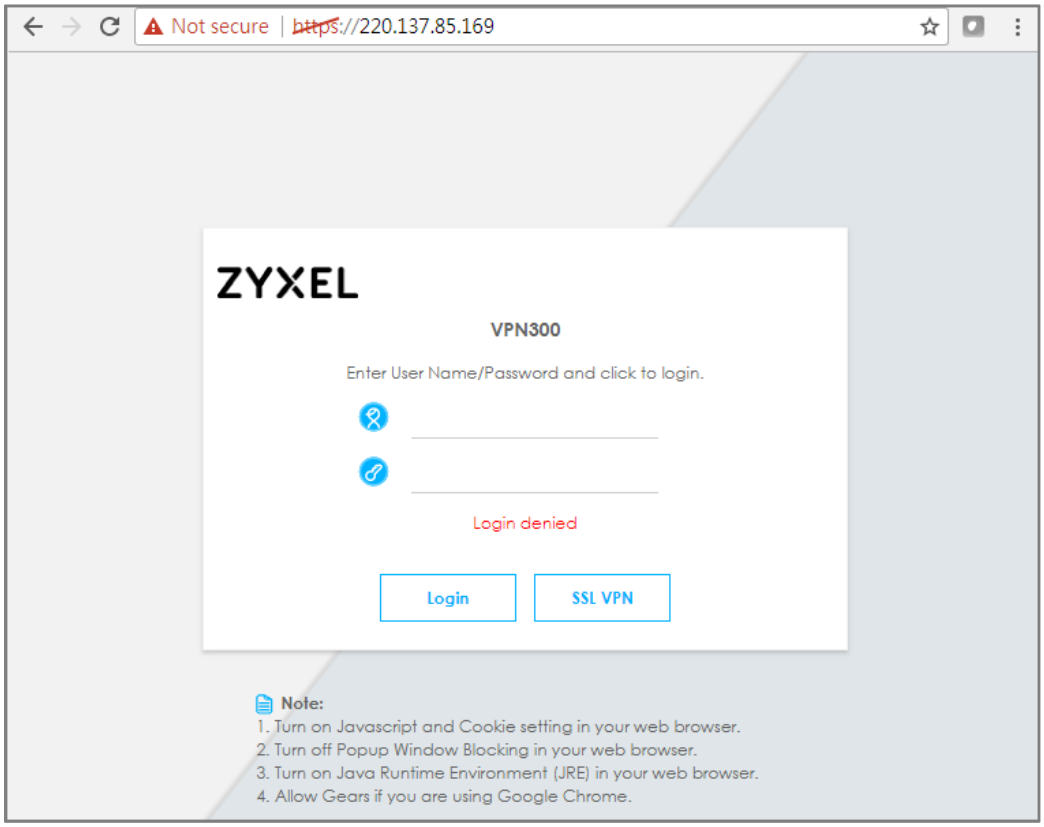
Type in the URL (https://sslvpnzyxeltest.ddns.net) and you will only see the **SSL VPN Login** button in the web portal screen.

Type in the URL (https://sslvpnzyxeltest.ddns.net)



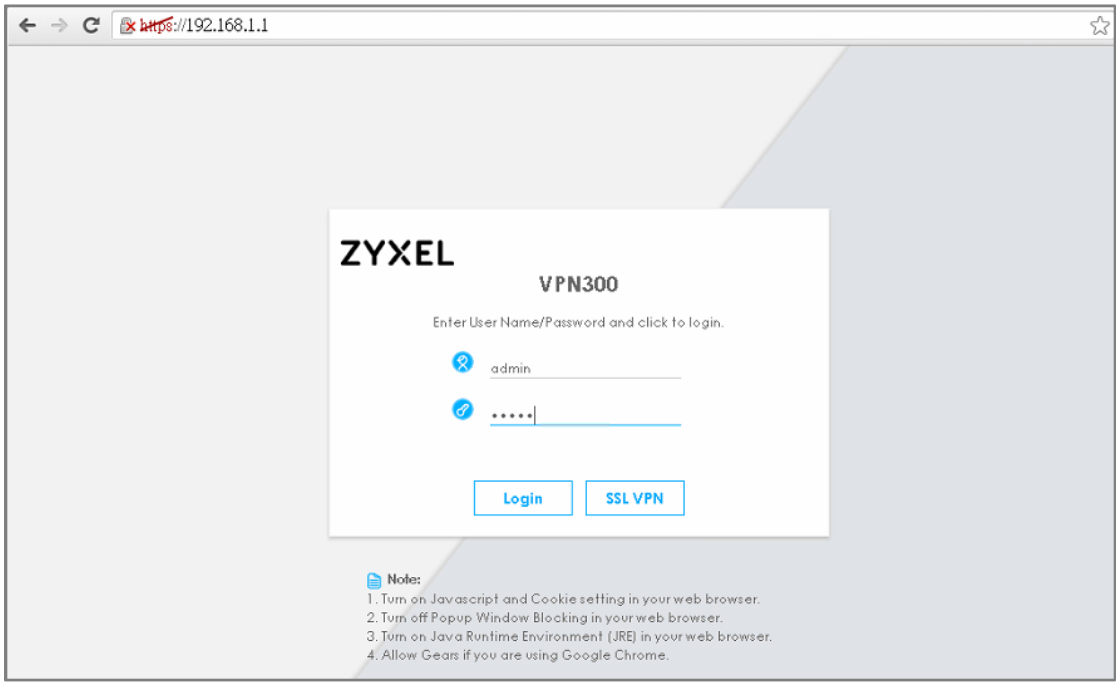
Login to the device via the WAN interface with the administrator's user name and password. The screen will show **Login denied**.

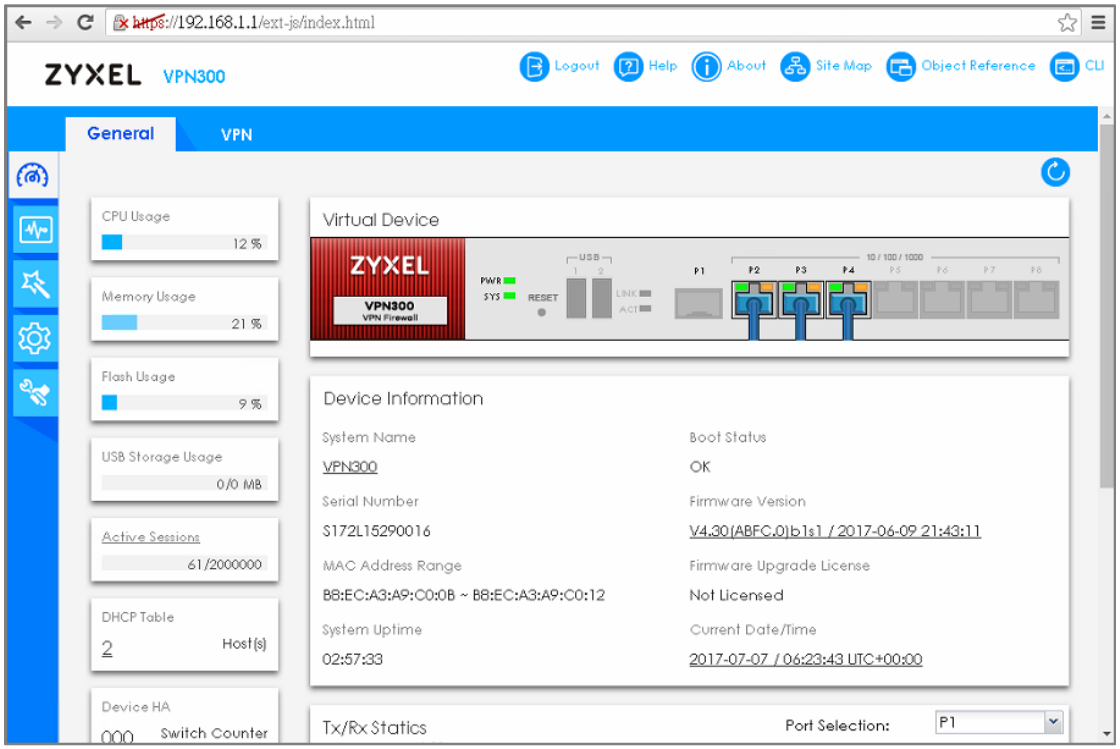
Login to the device via the WAN interface



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





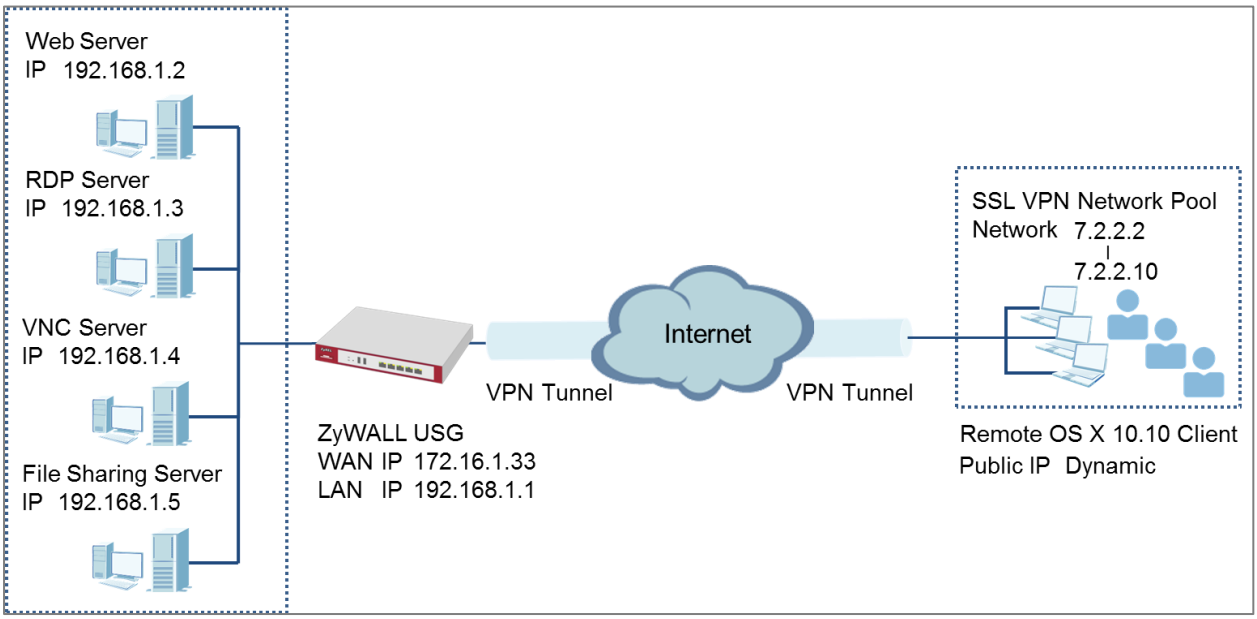
Go to **MONITOR > Log**. You can see that the admin login has been denied access from the WAN interface but it is allowed from the LAN interface.

MONITOR > Log

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

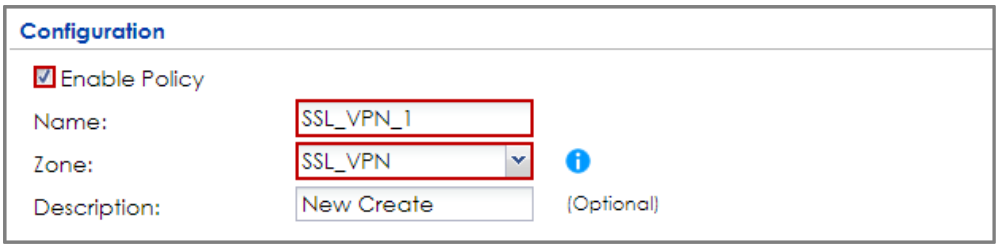


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25) and Apple MAC (Version: OS X10.10 Yosemite).

Set Up the SSL VPN Tunnel on the ZyWALL/USG

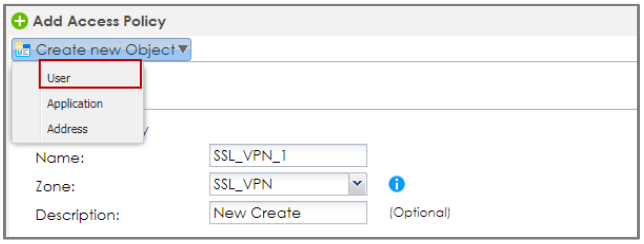
In the ZyWALL/USG, go to **CONFIGURATION > VPN > SSL VPN > Access Privilege** to add an **Access Policy**. Configure a **Name** for you to identify the SSL VPN configuration.

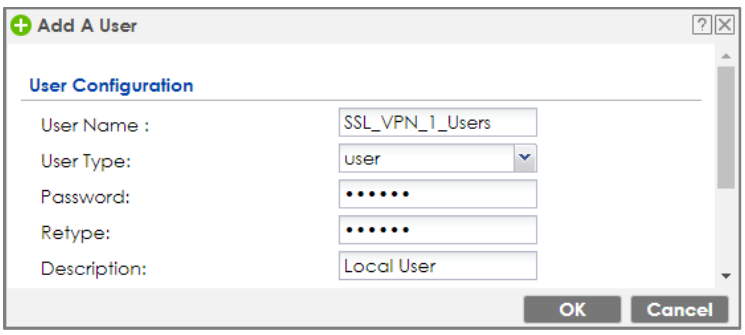
CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Configuration



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**.

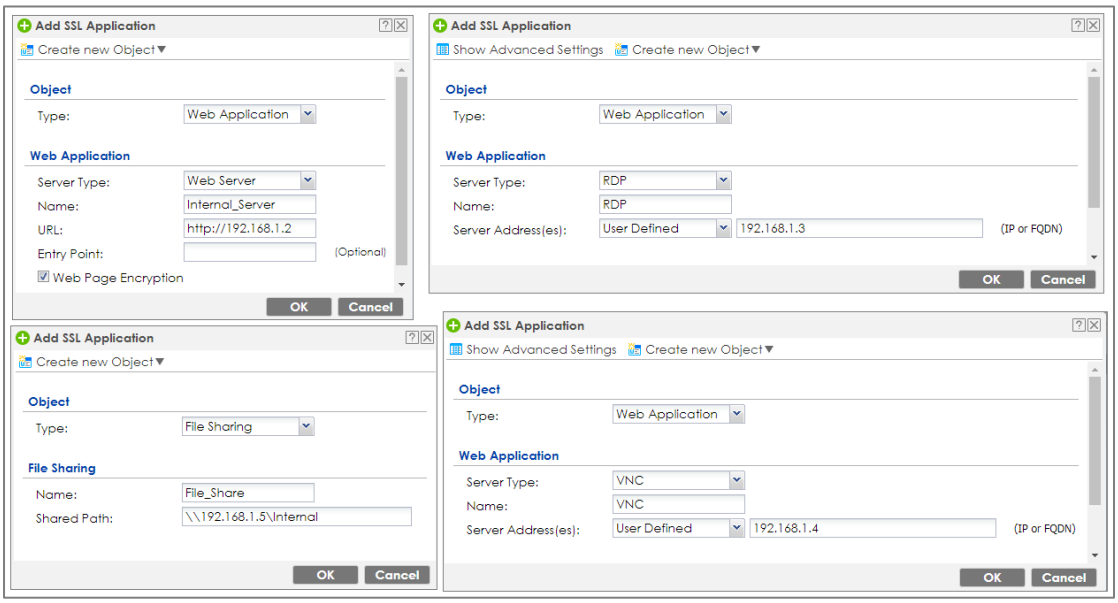
CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > User





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

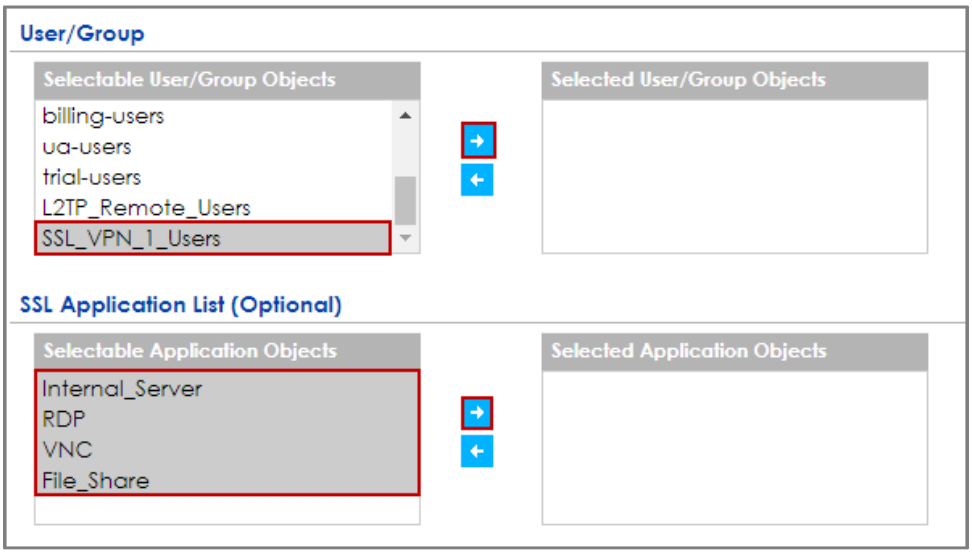


Go to **Create new Object > Address** to add the IP address pool for **SSL_VPN_1_Users**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > Address

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**.

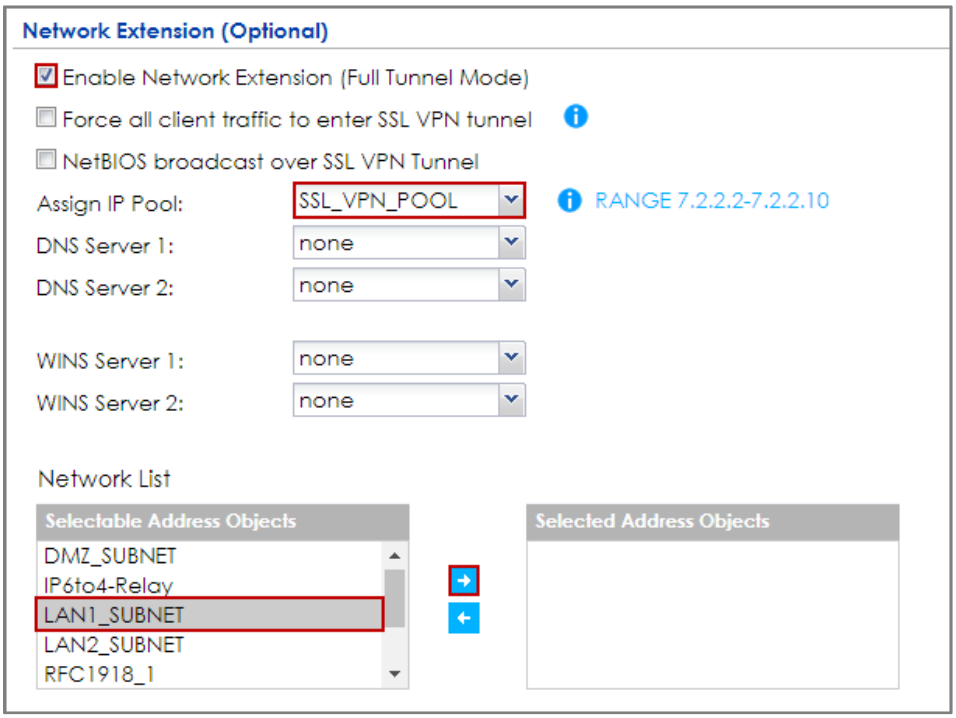
CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > User/Group & SSL Application



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.

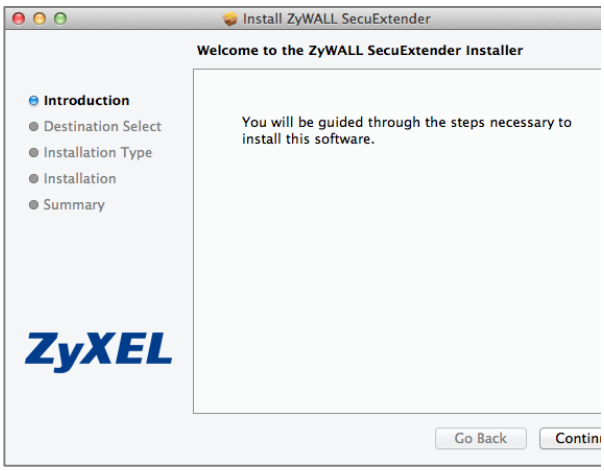
Select network(s) name in the **Selectable Address Objects** list and click the right arrow button to add to the **Selected Address Objects** list. You can select more than one network.

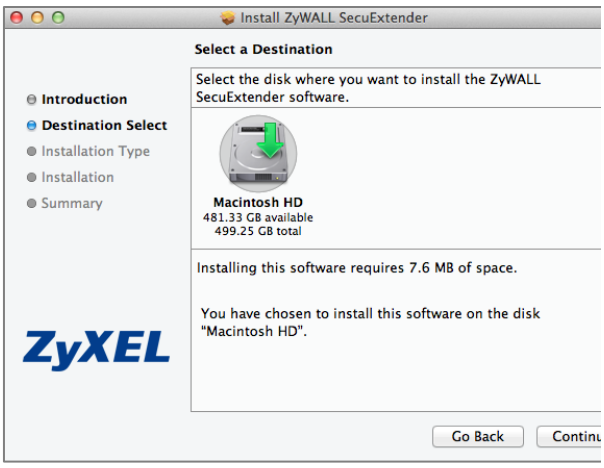
CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Network Extension (Optional)

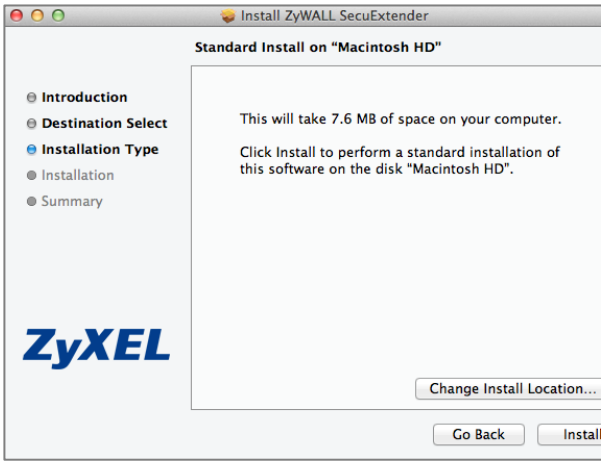


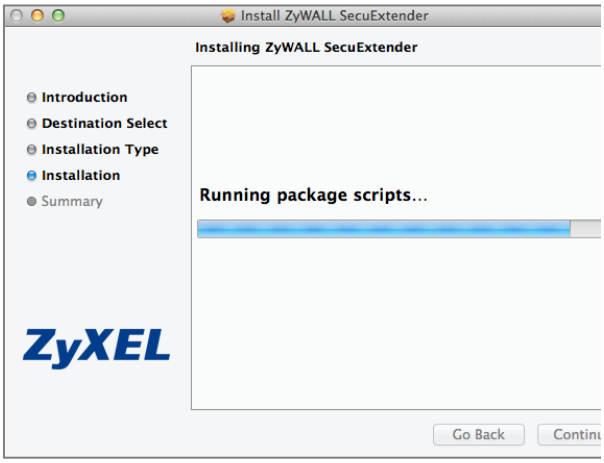
Set Up the SSL VPN Tunnel on the Apple MAC OS X 10.10 Operating System

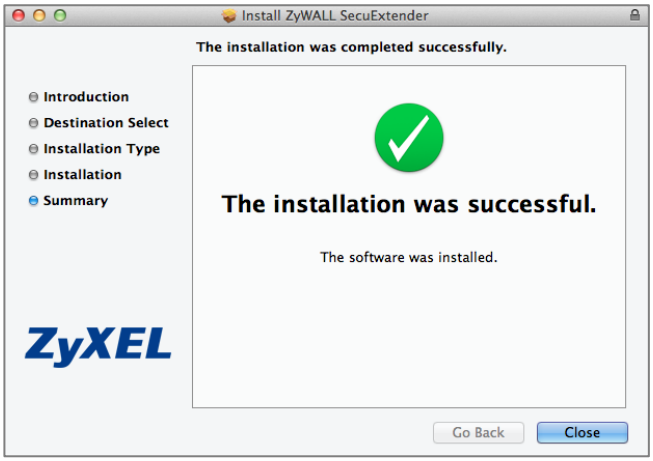
Download SSL VPN Client software: **ZyWALL SecuExtender** for MAC from the ZyXEL Global Website and double-click on the downloaded file to install it.











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**.

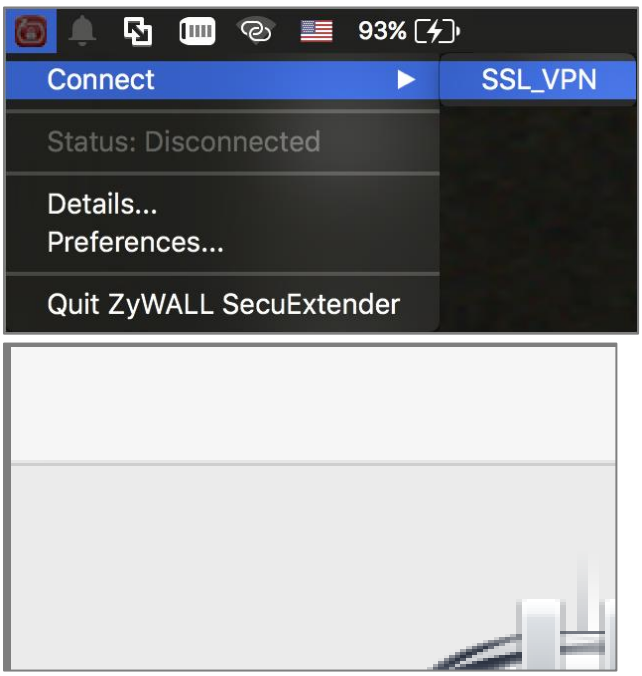
Here are two methods to initiate SSL VPN connections:

From ZyWALL SecuExtender

From a Web Browser

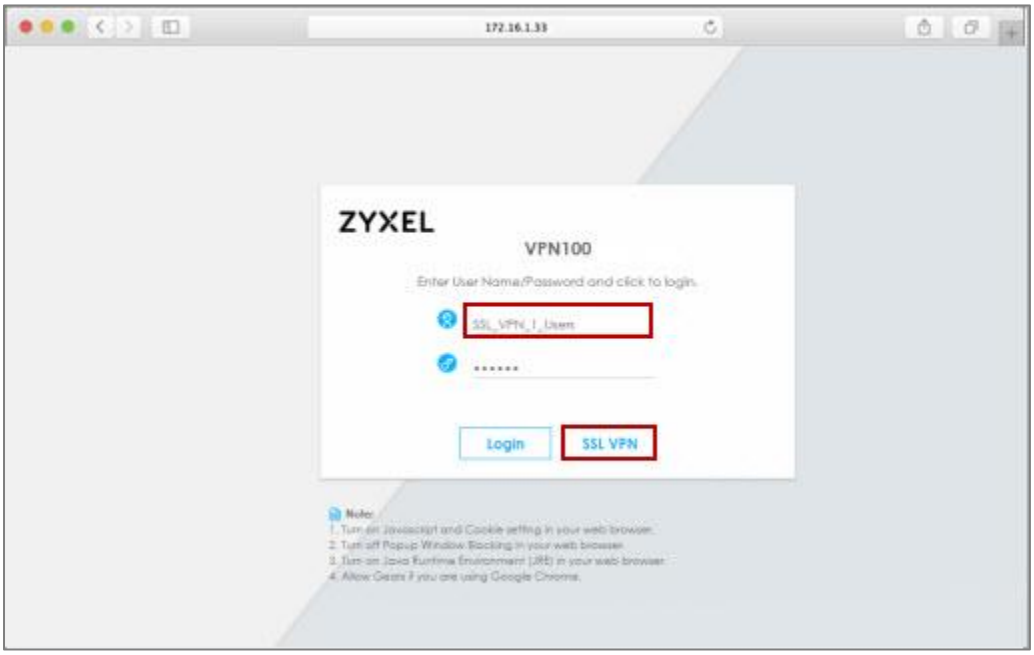
From ZyWALL SecuExtender

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

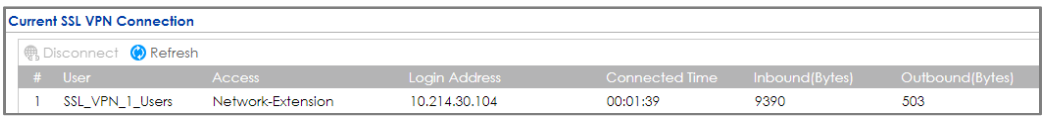
Type ZyWALL/USG's WAN IP into the browser, to display the login screen. Enter **User Name** and **Password** to be the same as your ZyWALL/USG SSL VPN **Selected User/Group** name and password (SSL_VPN_1_Users/zyx168 in this example). Click **SSL VPN**.



Test the SSL VPN Tunnel

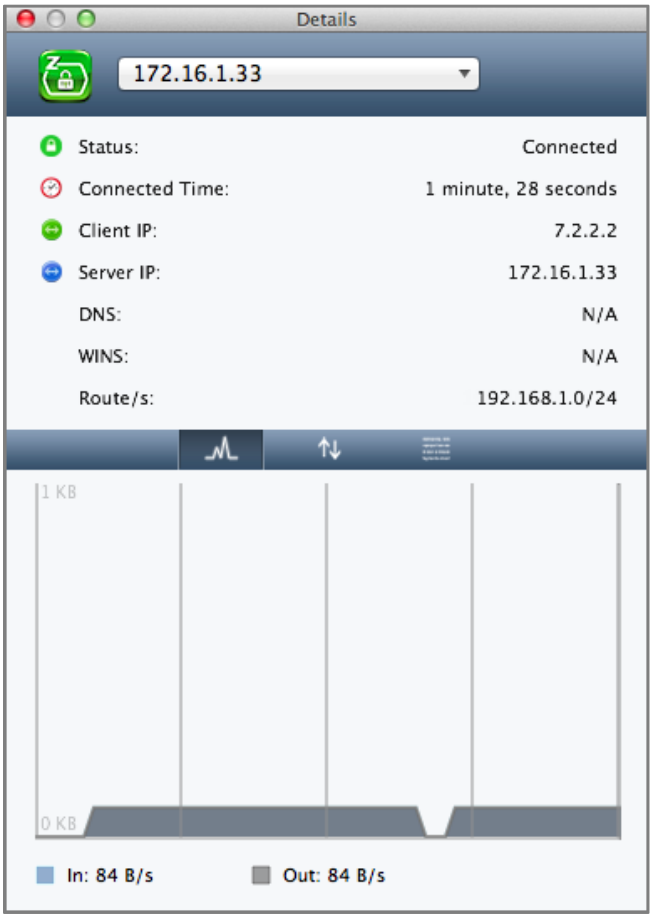
Go to ZyWALL/USG **MONITOR > VPN Monitor > SSL** and verify the tunnel **Login Address**, **Connected Time** and the **Inbound(Bytes)/Outbound(Bytes)** traffic.

MONITOR > VPN Monitor > SSL > SSL_VPN_1_Users

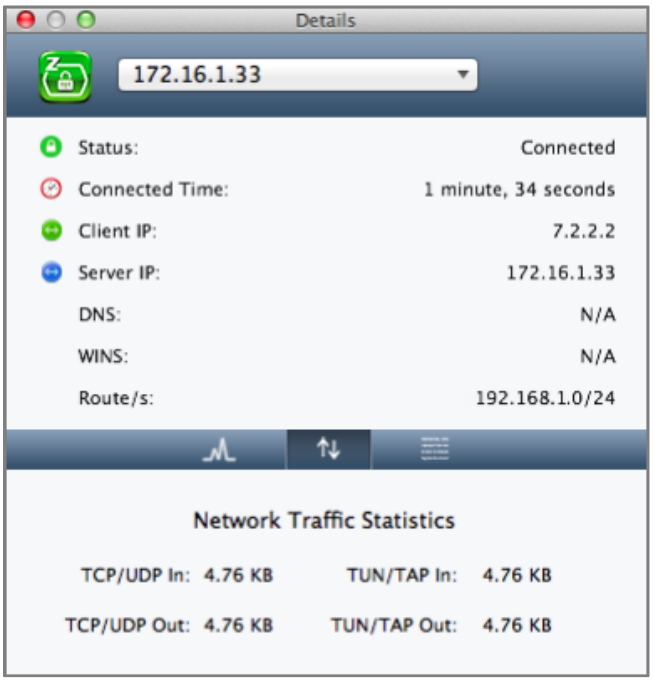


Go to **ZyWALL SecuExtender > Details** and check **Traffic Graph**, **Network Traffic Statics** and **Log Details**.

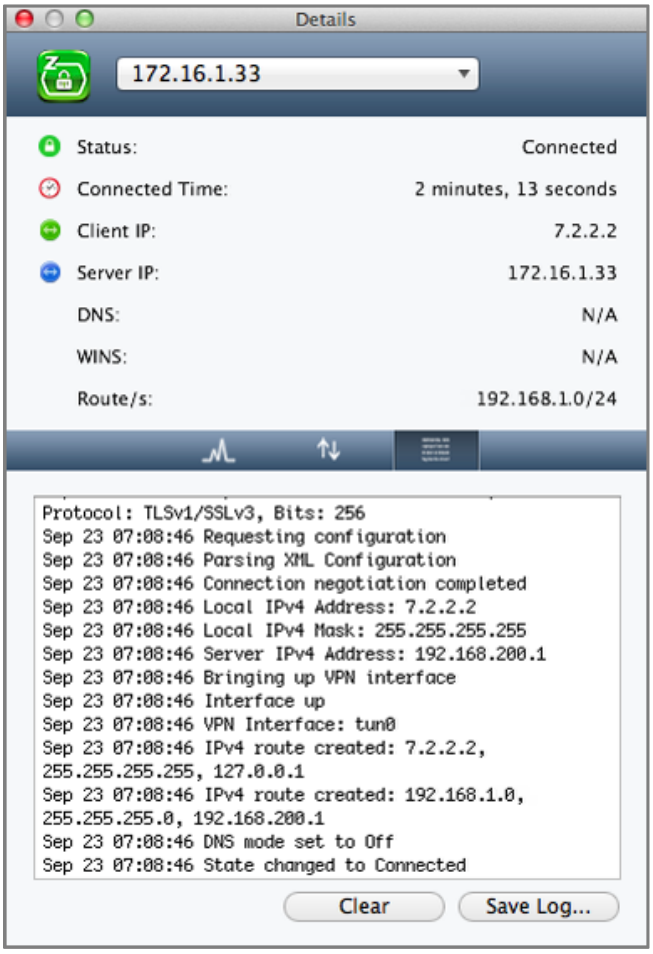
ZyWALL SecuExtender > Details > Traffic Graph



ZyWALL SecuExtender > Details > Network Traffic Statics



ZyWALL SecuExtender > Details > Log Details



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.

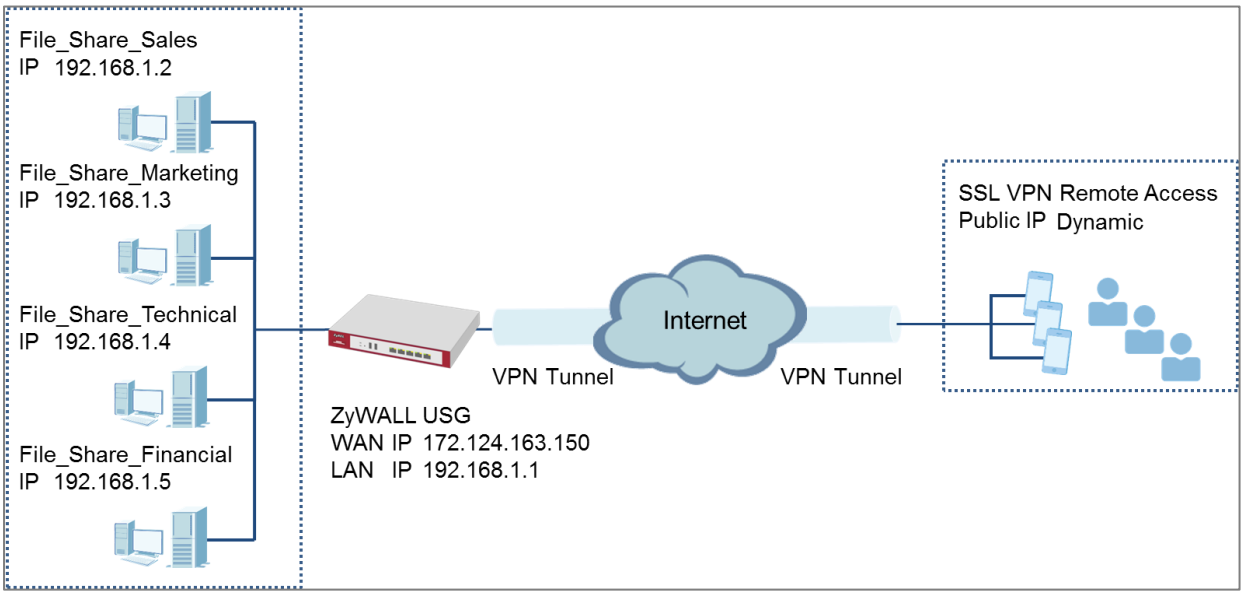
If the ZyWALL/USG redirects the user to the user aware screen, check whether the user account is included in an SSL VPN access policy or not.

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

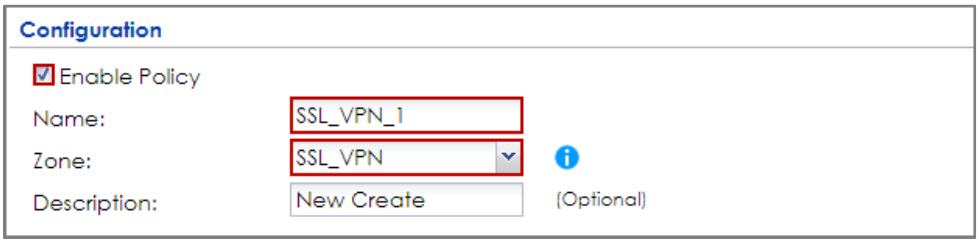


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG1900 (Firmware Version: ZLD 4.25).

Set Up the SSL VPN Tunnel on the ZyWALL/USG

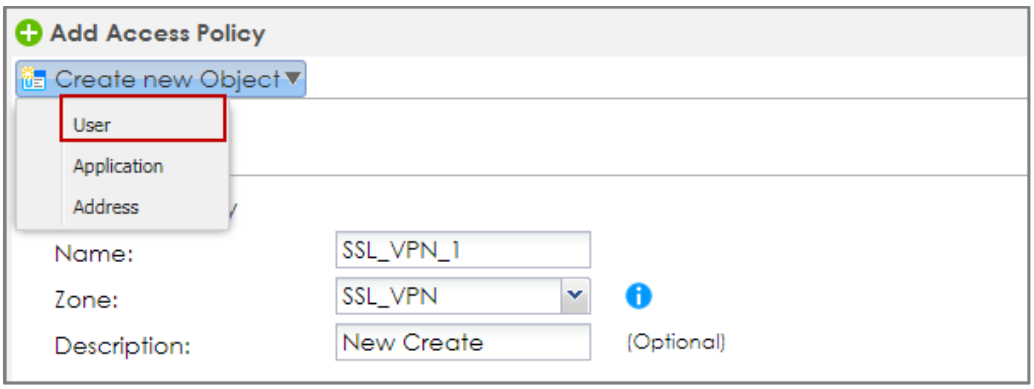
In the ZyWALL/USG, go to **CONFIGURATION > VPN > SSL VPN > Access Privilege** to add an **Access Policy**. Configure a **Name** for you to identify the SSL VPN configuration.

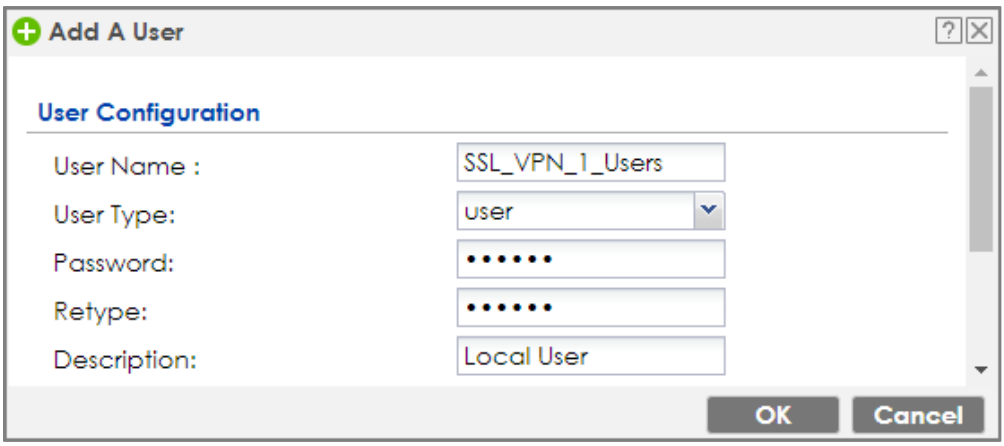
CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Configuration



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**.

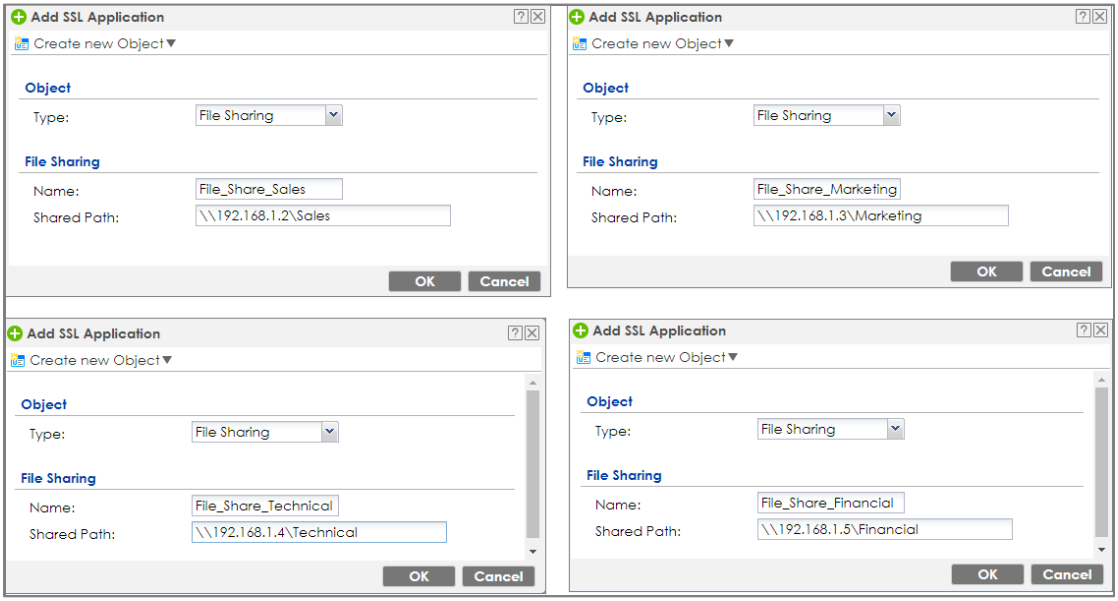
CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > User





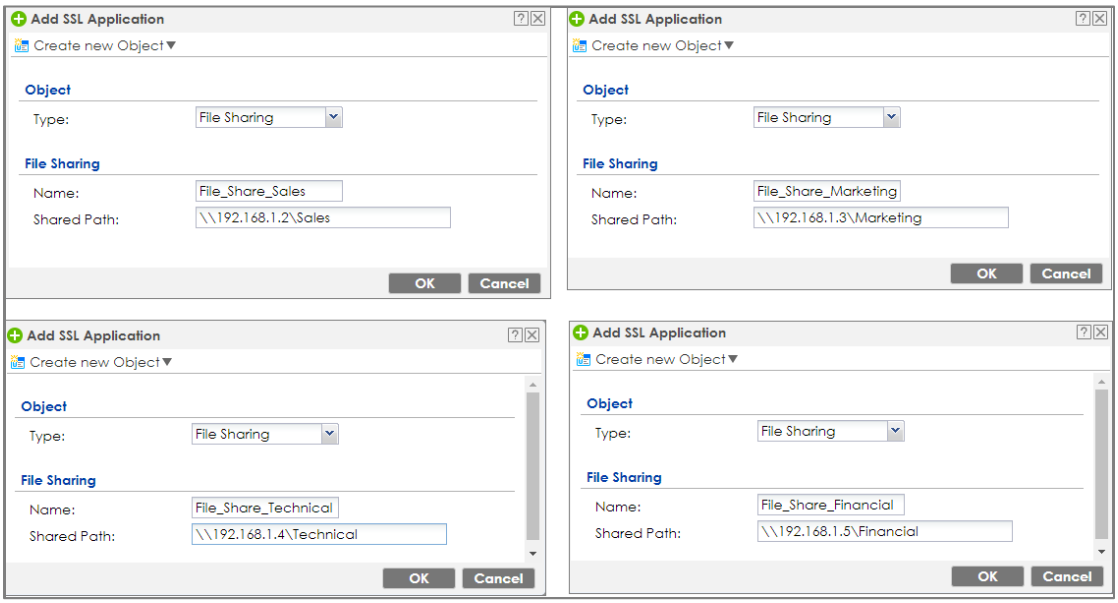
Go to **Create new Object > Application** to add servers that you will allow **SSL_VPN_1_Users** to access. Click **OK**.

CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > Application



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**.

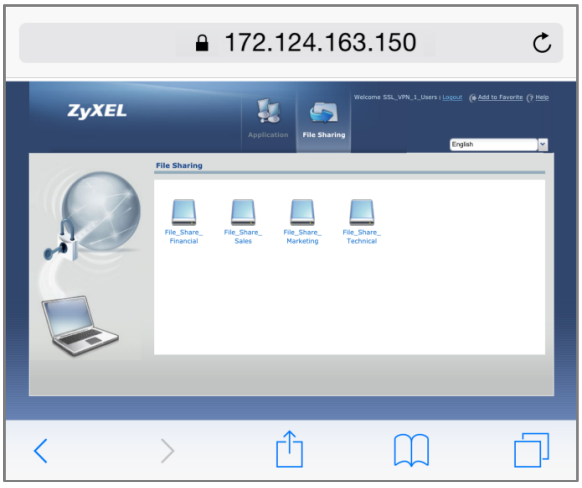
CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > User/Group & SSL Application



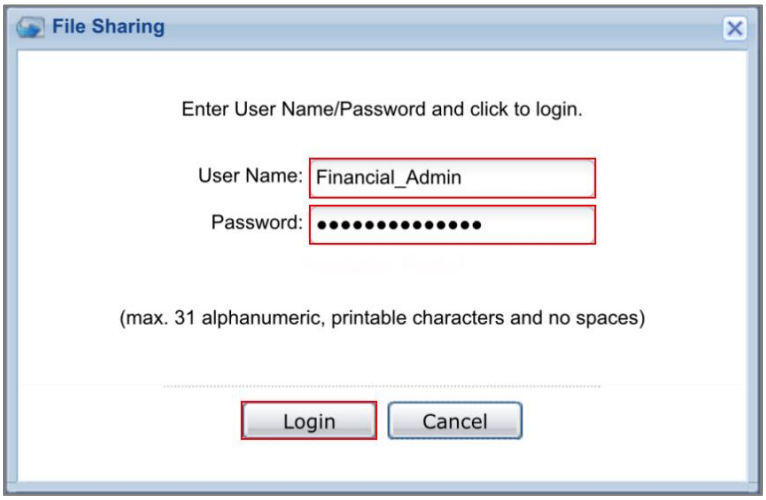
Test the SSL VPN Tunnel

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**.

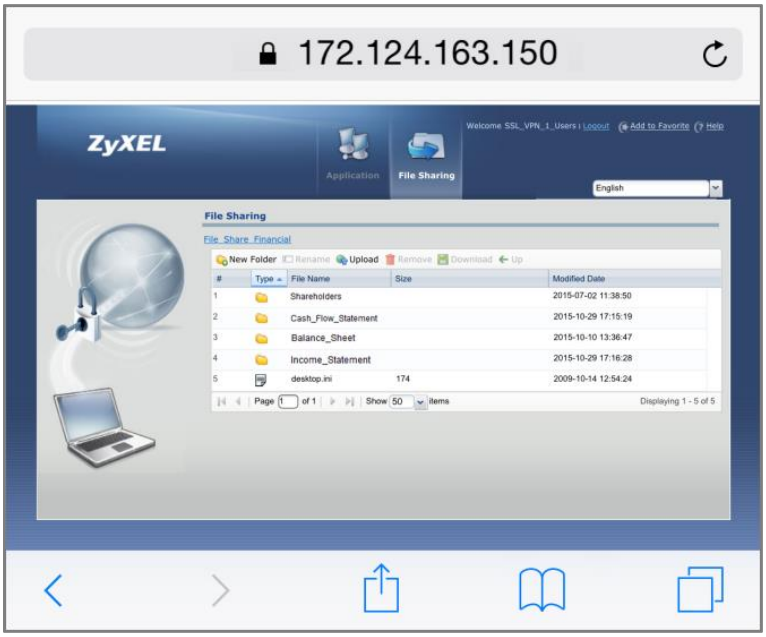
The **File Sharing** server appears.



Click the **File Sharing** folder you want to access, enter **User Name/ Password** of your **File Sharing** server and click **Login**.



Now you can securely access the files.



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.

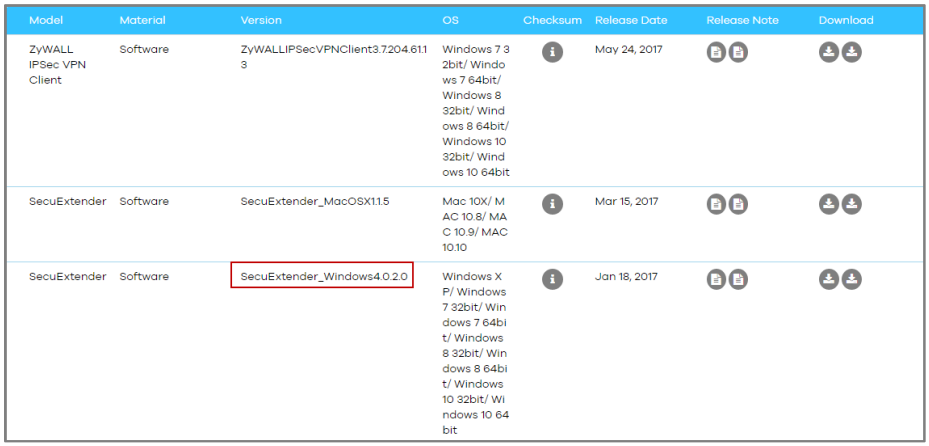
If the ZyWALL/USG redirects the user to the user aware screen, check whether the user account is included in an SSL VPN access policy or not.

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

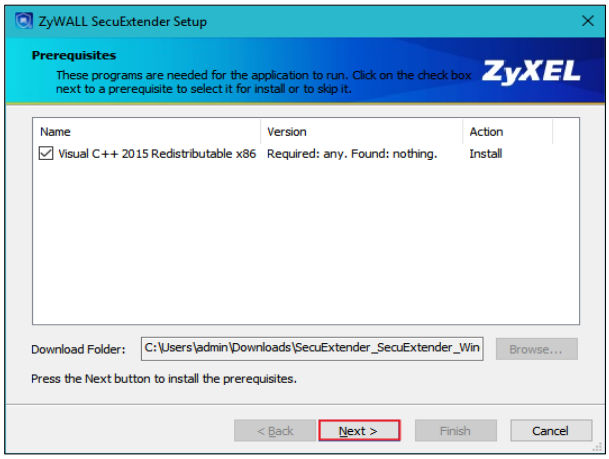
Set up the SSL VPN Tunnel with Windows 10

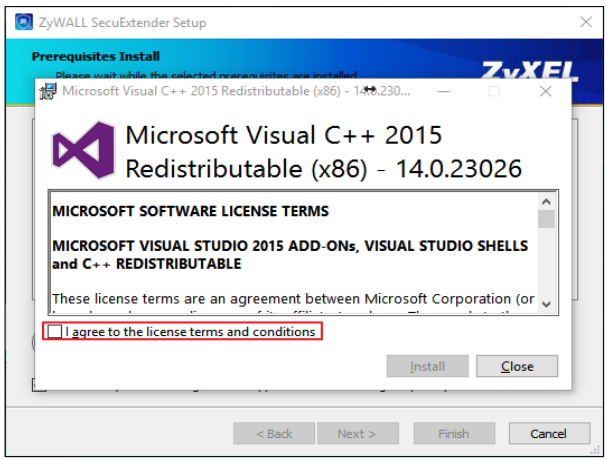
Please download SecuExtender version 4.0.0.1 from the download library of ZyXEL's official website.

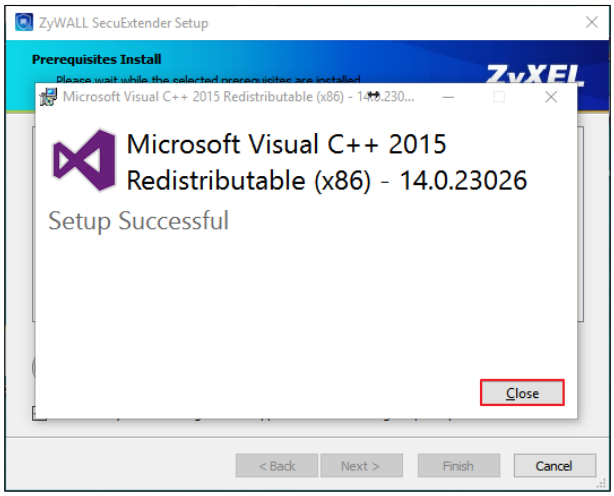


Model	Material	Version	OS	Checksum	Release Date	Release Note	Download
ZyWALL IPSec VPN Client	Software	ZyWALLIPSecVPNClient3.7.204.61.13	Windows 7 32bit/ Windows 7 64bit/ Windows 8 32bit/ Windows 8 64bit/ Windows 10 32bit/ Windows 10 64bit		May 24, 2017		
SecuExtender	Software	SecuExtender_MacOSX1.1.5	Mac 10X/ MAC 10.8/ MAC 10.9/ MAC 10.10		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		Jan 18, 2017		

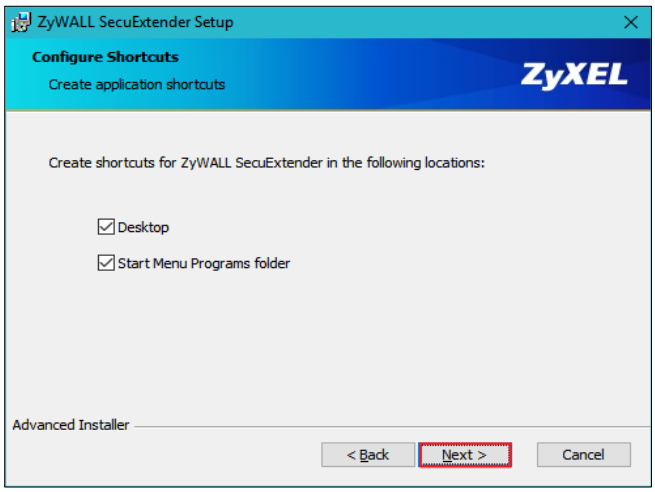
Before you start installing the SecuExtender, it is required to install the "Visual C++ 2015 Redistributable" package first. Click **Next**, select **I agree to the license terms and conditions**, and click **Install** to complete the Visual C++ 2015 Redistributable installation. After that, the setup wizard appears. Please note that the users need to reboot their systems after the SecuExtender installation is completed.

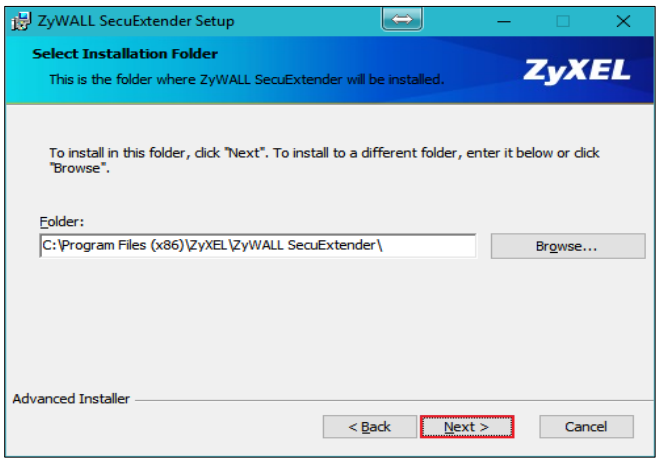

ZyWALL SecuExtender Setup
Prerequisites
These programs are needed for the application to run. Click on the check box next to a prerequisite to select it for install or to skip it.
ZyXEL
Name
Version
Action
Visual C++ 2015 Redistributable x86
Required: any. Found: nothing.
Install
Download Folder:
C:\Users\admin\Downloads\SecuExtender_SecuExtender_Win
Browse...
Press the Next button to install the prerequisites.
< Back
Next >
Finish
Cancel

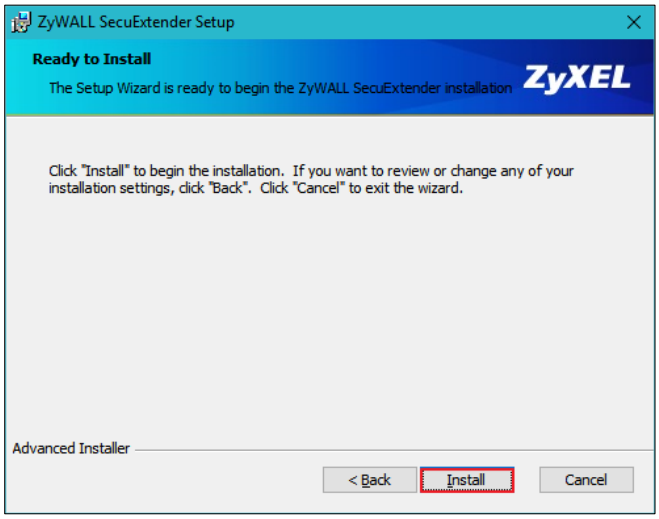

ZyWALL SecuExtender Setup
Prerequisites Install
ZyXEL
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.23026
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.23026
MICROSOFT SOFTWARE LICENSE TERMS
MICROSOFT VISUAL STUDIO 2015 ADD-ONs, VISUAL STUDIO SHELLS and C++ REDISTRIBUTABLE
These license terms are an agreement between Microsoft Corporation (or
I agree to the license terms and conditions
Install
Close
< Back
Next >
Finish
Cancel


ZyWALL SecuExtender Setup
Prerequisites Install
ZyXEL
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.23026
Microsoft Visual C++ 2015 Redistributable (x86) - 14.0.23026
Setup Successful
Close
< Back
Next >
Finish
Cancel

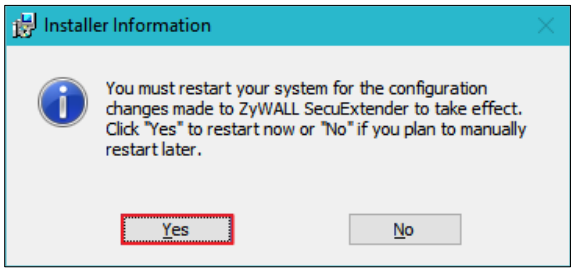
ZyWALL SecuExtender Setup
ZyXEL
Welcome to the ZyWALL SecuExtender Setup Wizard
The Setup Wizard will install ZyWALL SecuExtender on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.
< Back
Next >
Cancel


ZyWALL SecuExtender Setup
Configure Shortcuts
Create application shortcuts
ZyXEL
Create shortcuts for ZyWALL SecuExtender in the following locations:
Desktop
Start Menu Programs folder
Advanced Installer
< Back
Next >
Cancel

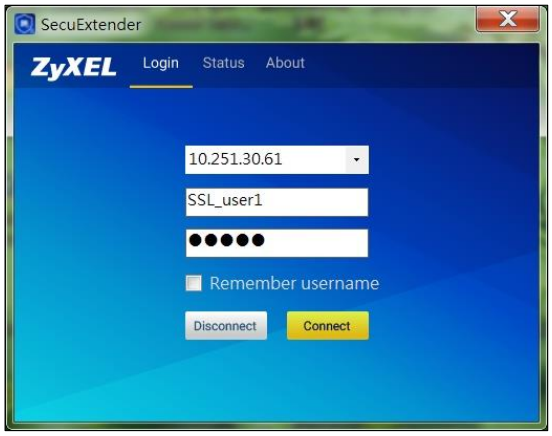

ZyWALL SecuExtender Setup
Select Installation Folder
This is the folder where ZyWALL SecuExtender will be installed.
ZyXEL
To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".
Folder:
C:\Program Files (x86)\ZyXEL\ZyWALL SecuExtender\
Browse...
Advanced Installer
< Back
Next >
Cancel


ZyWALL SecuExtender Setup
Ready to Install
The Setup Wizard is ready to begin the ZyWALL SecuExtender installation
ZyXEL
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.
Advanced Installer
< Back
Install
Cancel

ZyWALL SecuExtender Setup
ZyXEL
Completing the ZyWALL SecuExtender Setup Wizard
Click the "Finish" button to exit the Setup Wizard.
< Back
Finish
Cancel


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.
Yes
No

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.

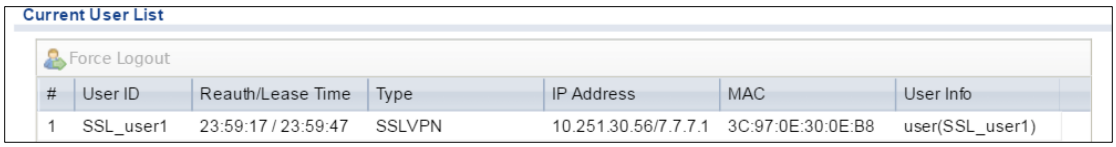


You can verify the connection status from the computer's taskbar icon.

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.



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.

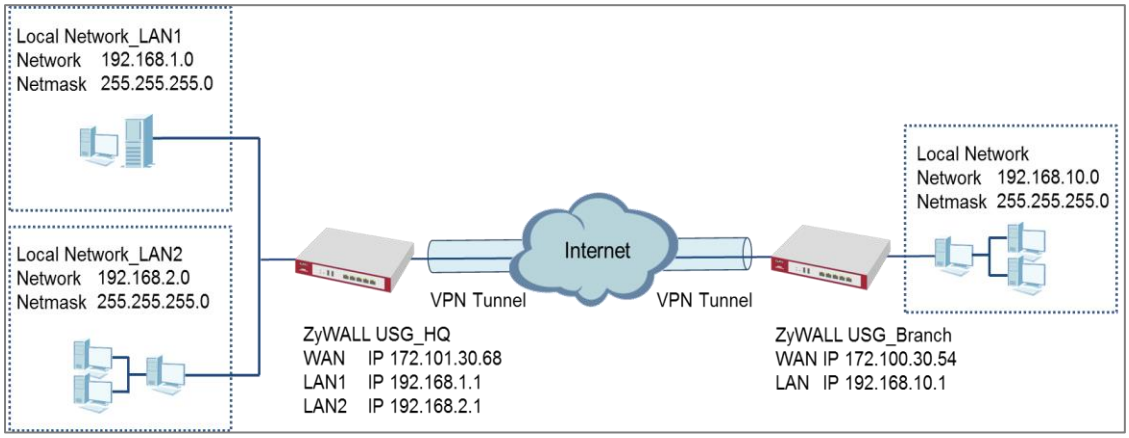
3 If users can log into the SSL VPN but cannot see some of the resource links, check the SSL application object's configurations.

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.



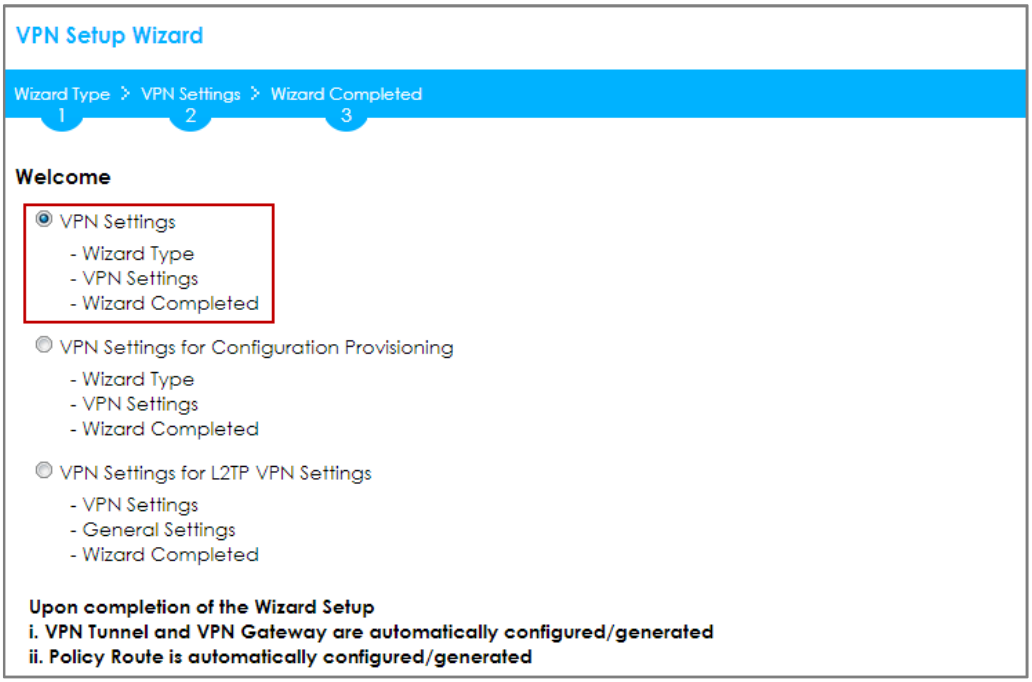
ZyWALL Site-to-site IPSec VPN with multiple LAN access

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)

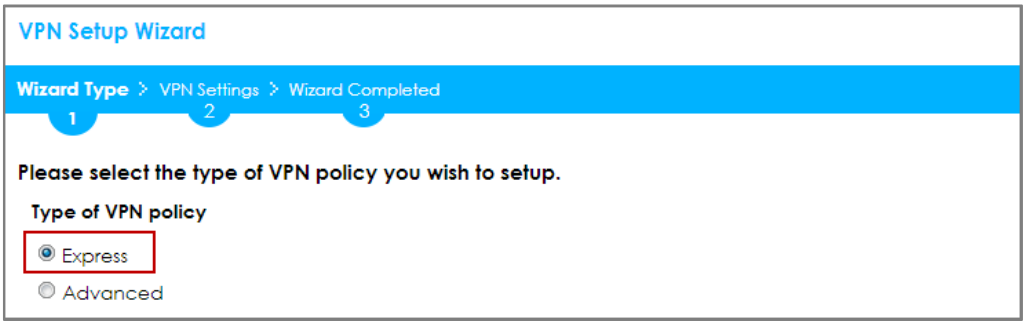
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



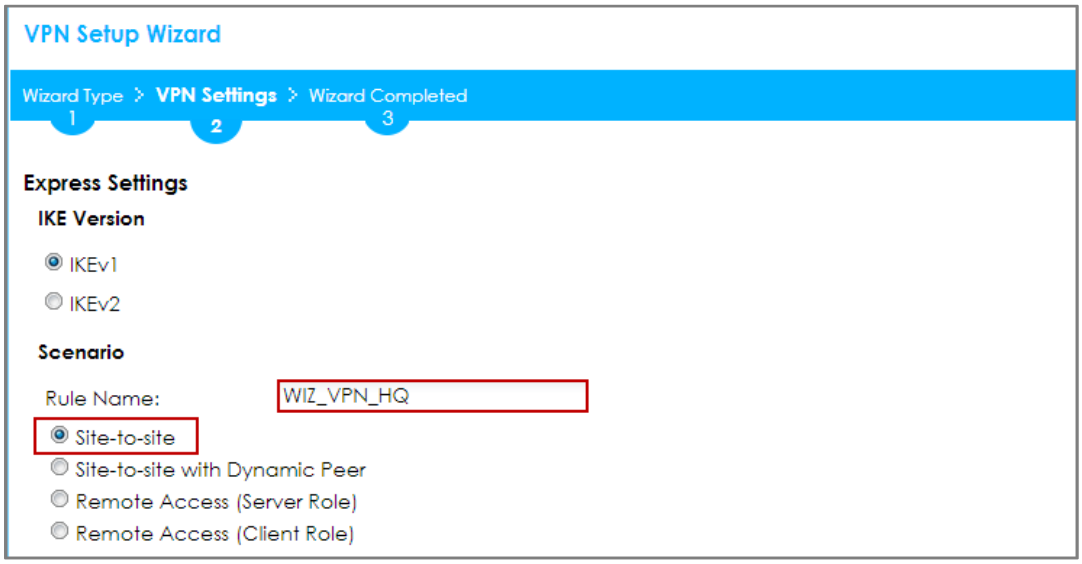
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and use a pre-shared key to be the authentication method. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

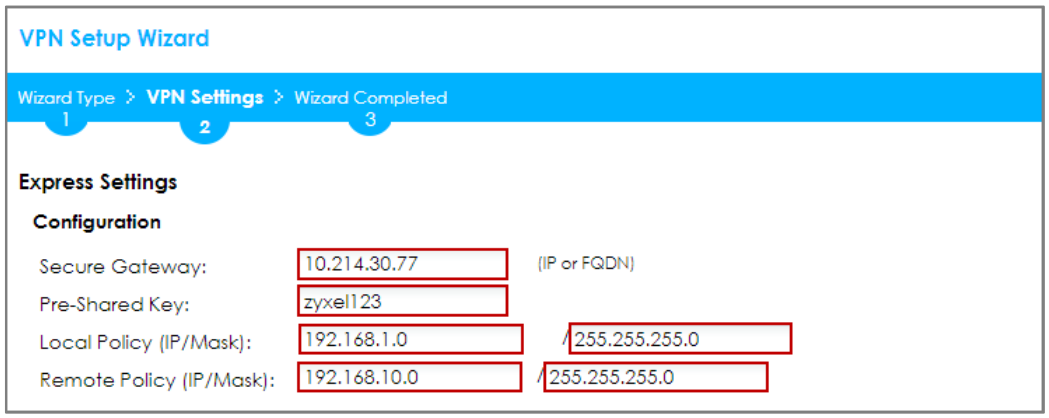
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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).

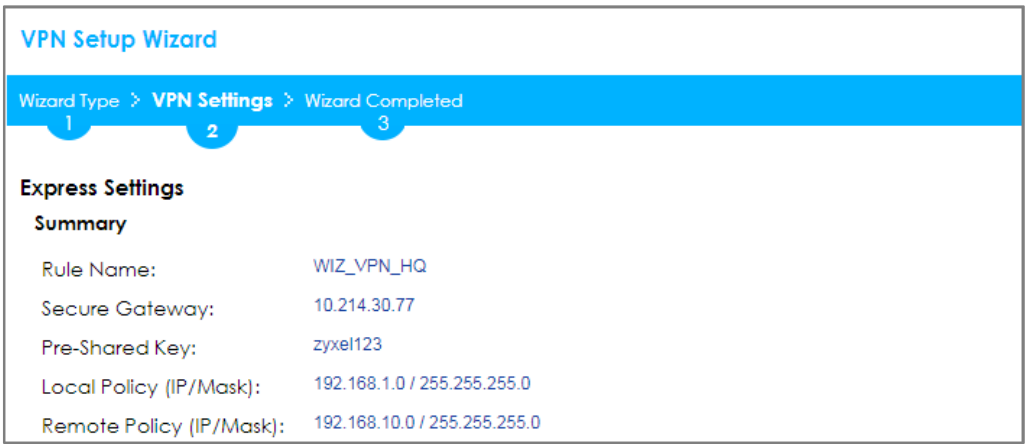
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZyWALL/USG.

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



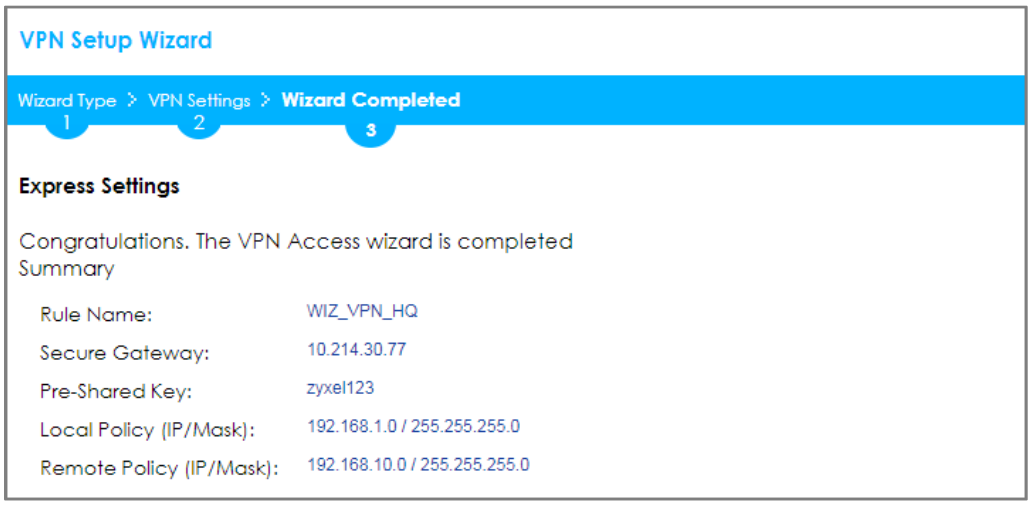
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



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.

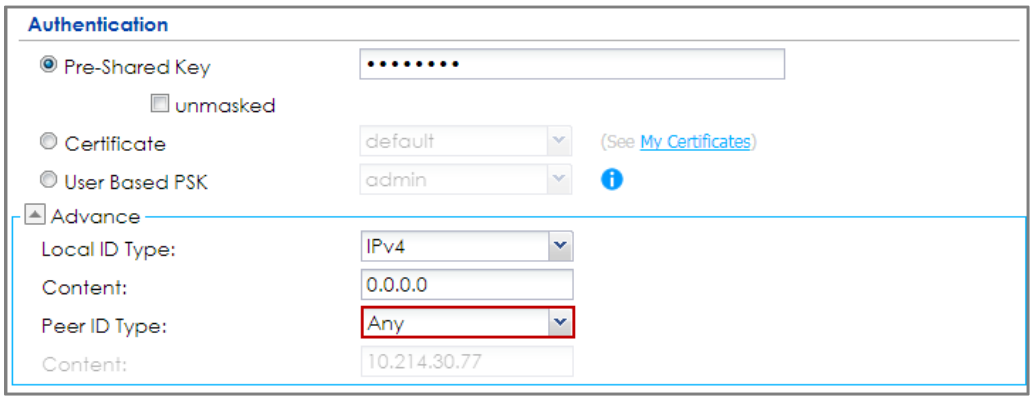
Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



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.

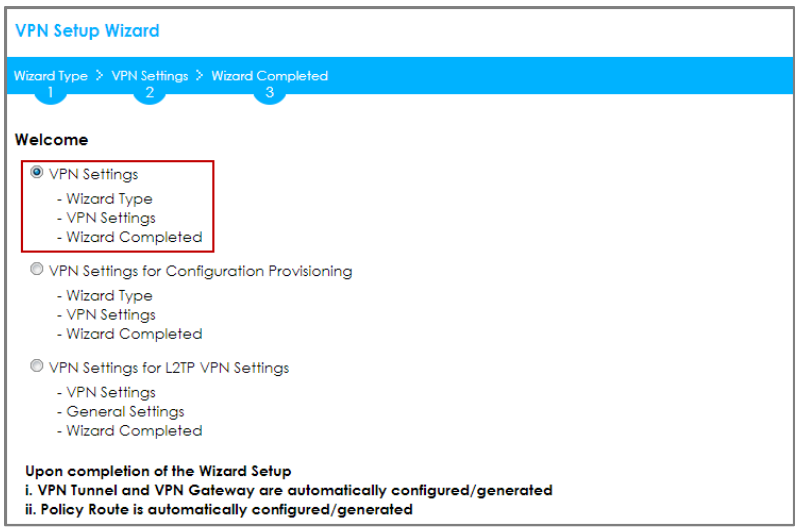
CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Show Advanced Settings > Authentication > Peer ID Type



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

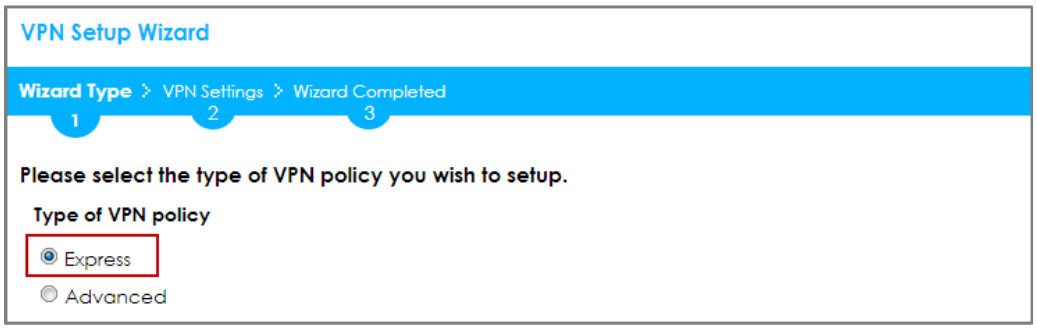
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the remote ZyWALL/USG. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



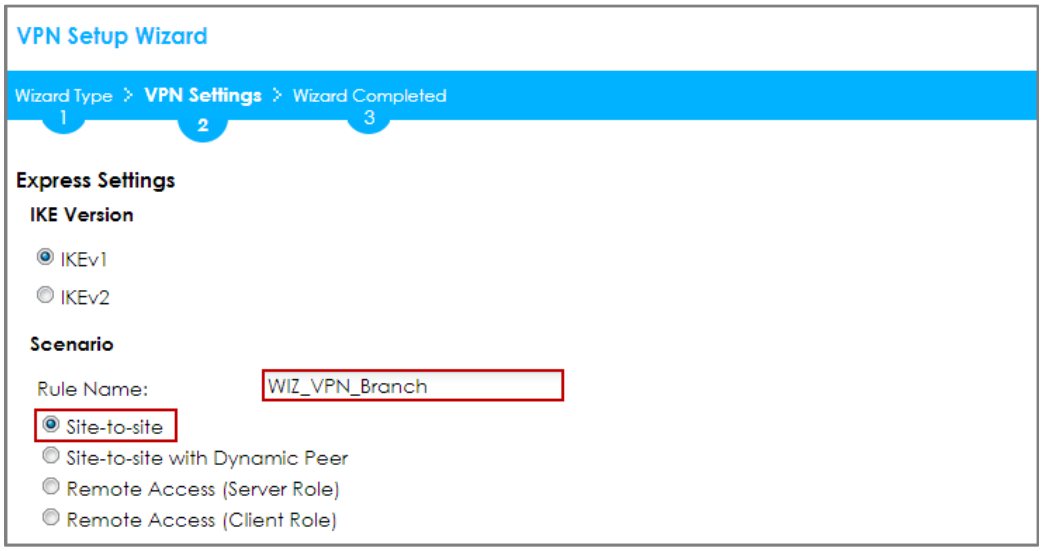
Choose **Express** to create a VPN rule with the default phase 1 and phase 2 settings and to use a pre-shared key. Click **Next**.

Quick Setup > VPN Setup Wizard > Wizard Type



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**.

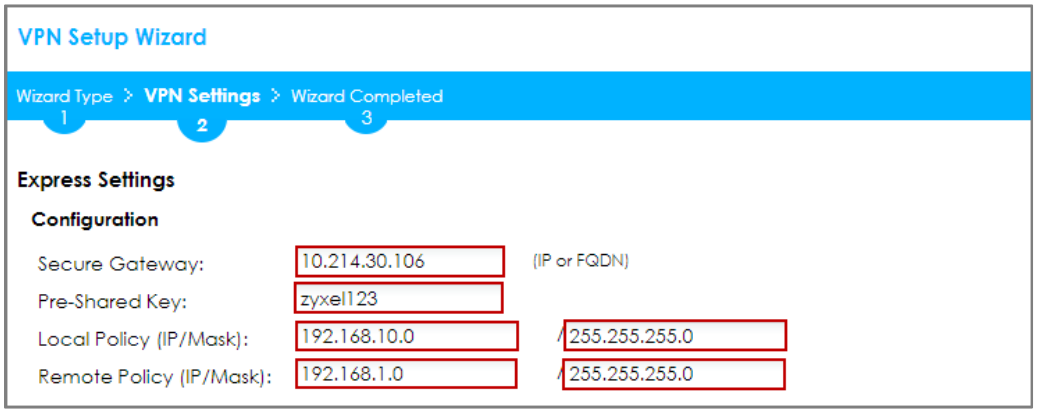
Quick Setup > VPN Setup Wizard > Wizard Type > VPN Settings (Scenario)



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).

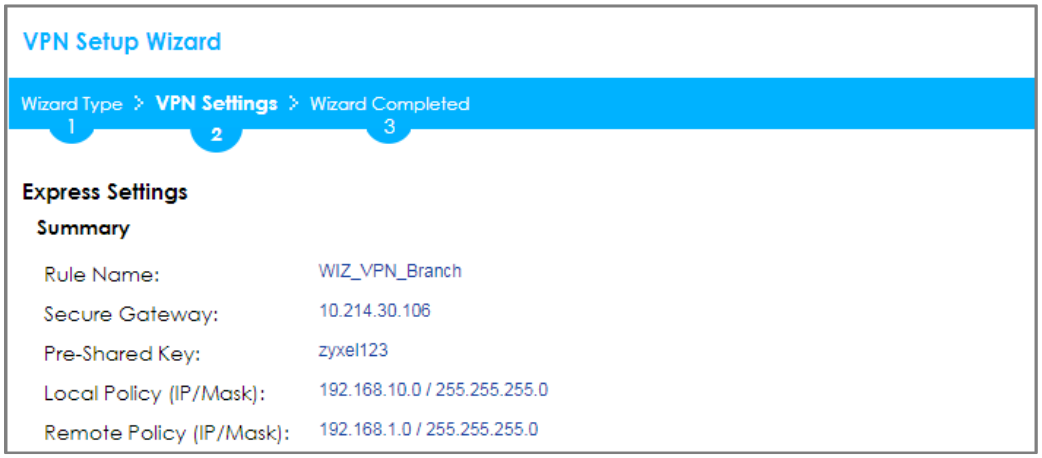
Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG and **Remote Policy** to be the IP address range of the network connected to the peer ZYWALL/USG.

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



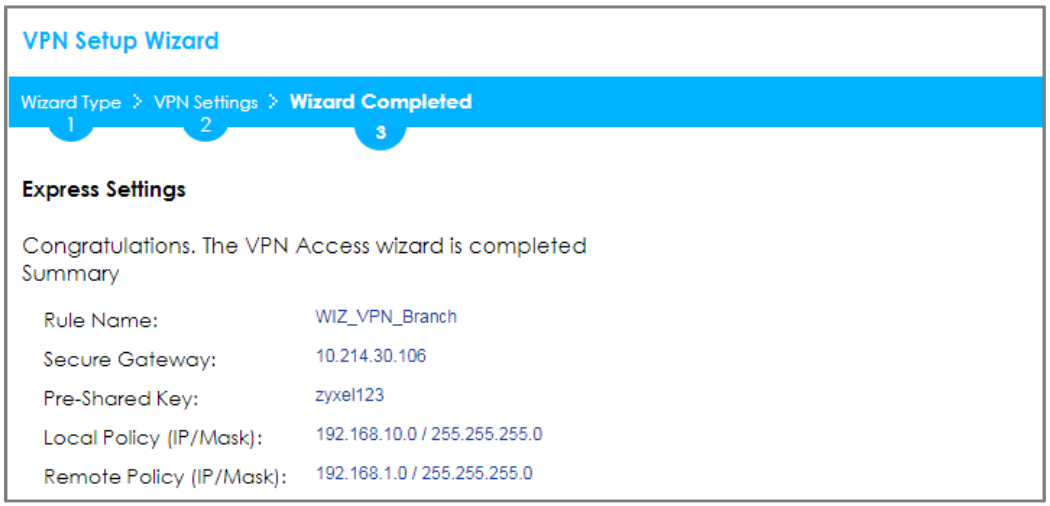
This screen provides a read-only summary of the VPN tunnel. Click **Save**.

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



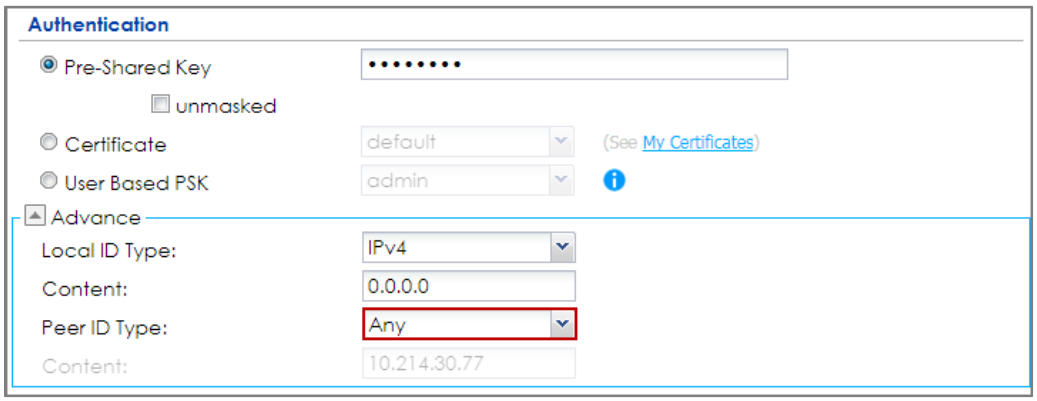
Now the rule is configured on the ZyWALL/USG. The Phase 1 rule settings appear in the **VPN > IPSec VPN > VPN Gateway** screen and the Phase 2 rule settings appear in the **VPN > IPSec VPN > VPN Connection** screen. Click **Close** to exit the wizard.

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

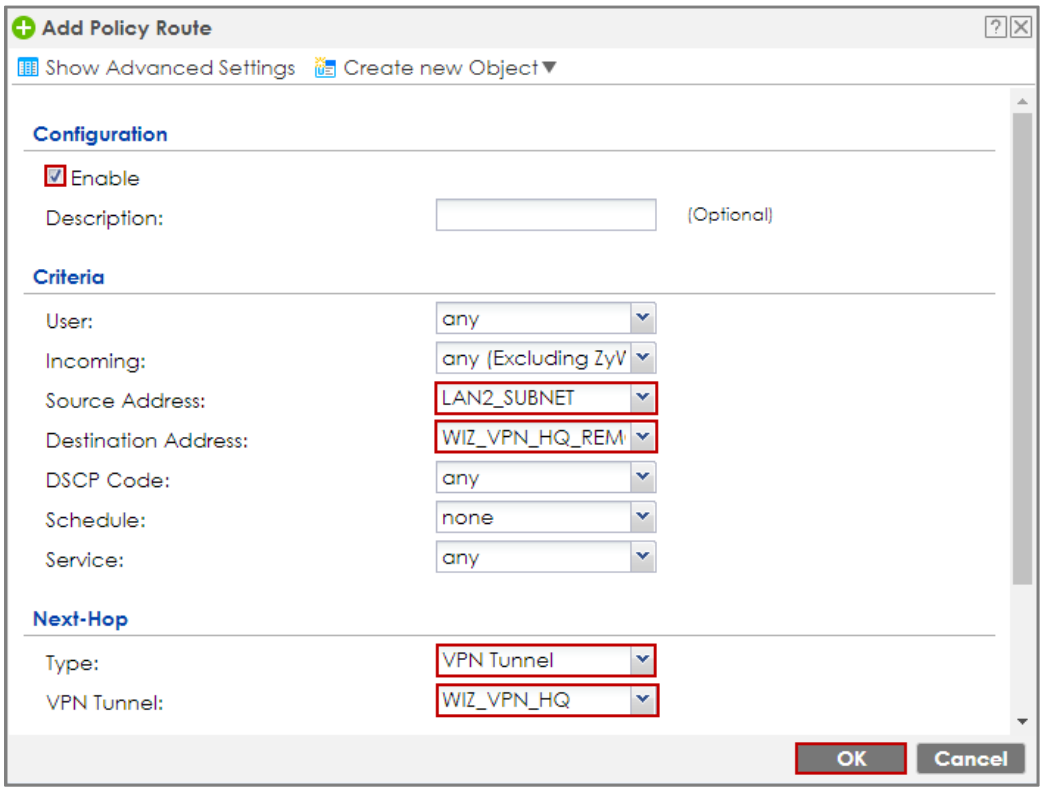


Set up the Policy Route (ZyWALL/USG_HQ)

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).

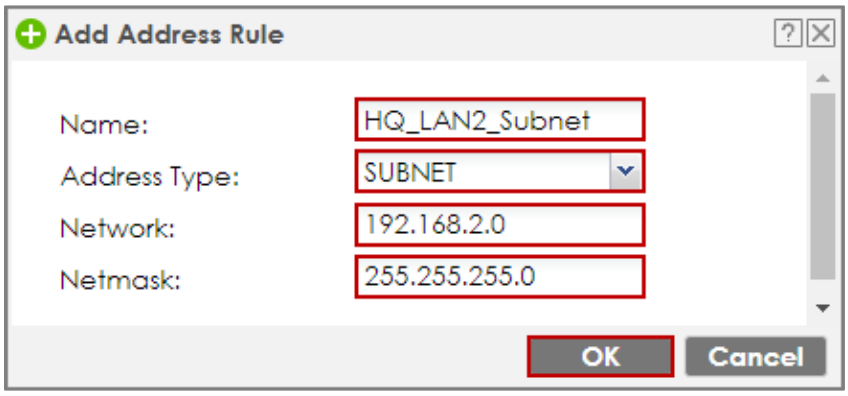
CONFIGURATION > Network > Routing > Add



Set up the Policy Route (ZyWALL/USG_Branch)

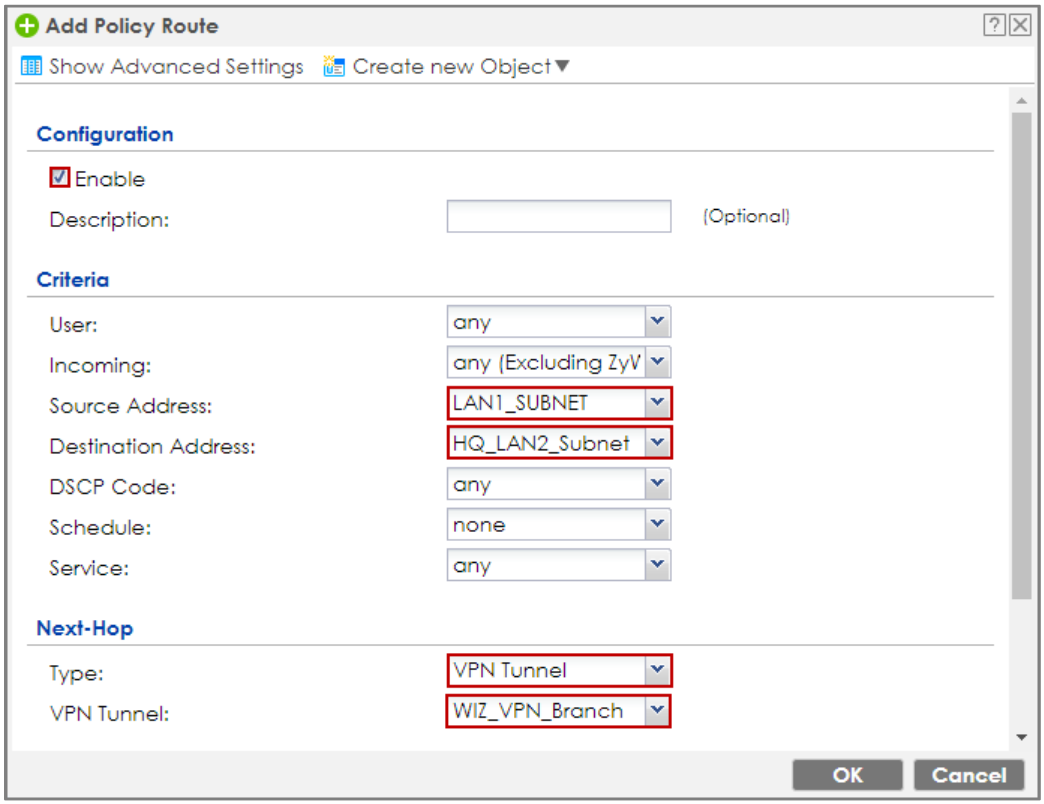
Go to ZyWALL/USG_Branch **CONFIGURATION > Network > Routing > Add**, create **Address** to be the remote LAN subnet (192.168.2.0/24 in this example) allows joining the VPN tunnel.

CONFIGURATION > Object > Address > Add



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



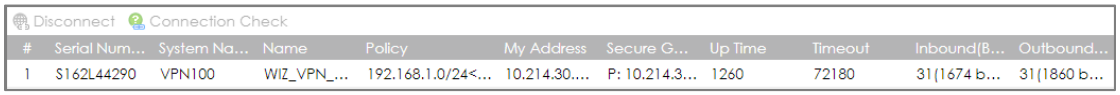
Test the IPSec VPN Tunnel

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

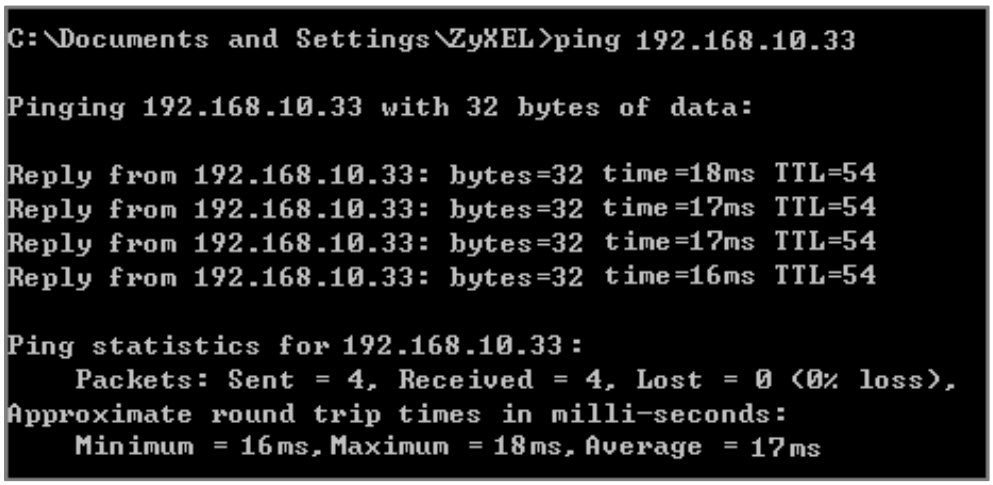
Go to ZyWALL/USG **MONITOR > VPN Monitor > IPSec** and verify the tunnel **Up Time** and **Inbound(Bytes)/Outbound(Bytes)** Traffic.

MONITOR > VPN Monitor > IPSec



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



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

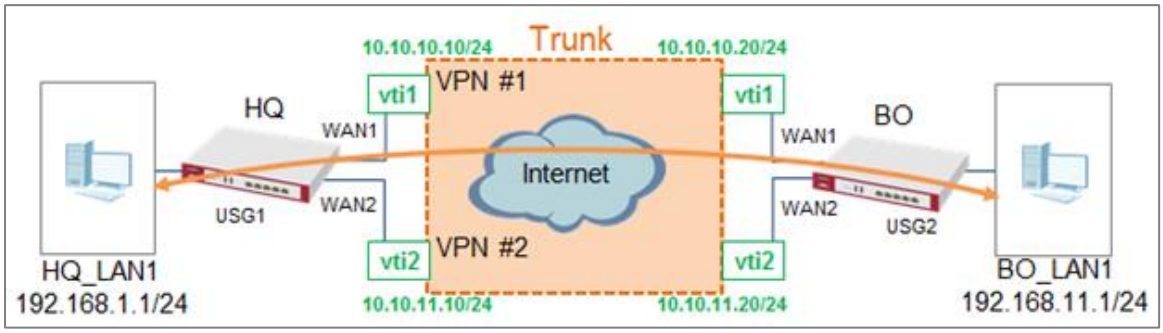
Priority	Cate...	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [BO1] Phase 2 proposal mismatch	IKE_LOG
info	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.

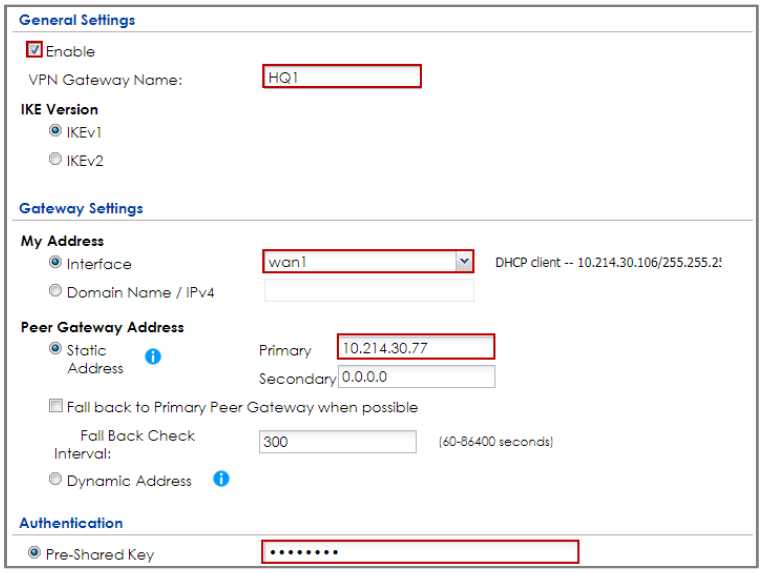
5 Configure a policy route.

6 Connect the VPN tunnels.

Set Up the ZyWALL/USG VTI of Corporate Network (HQ)

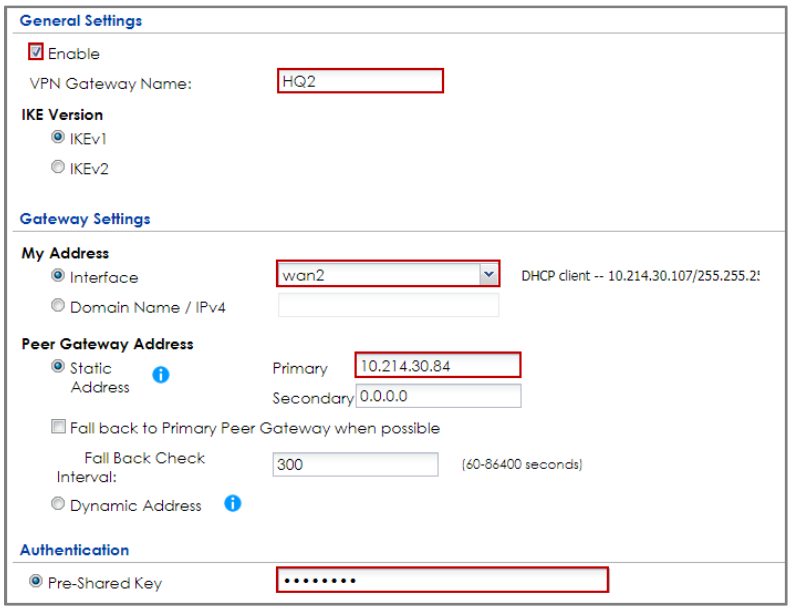
1 In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add** to create the VPN gateway **HQ1** with **wan1**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add



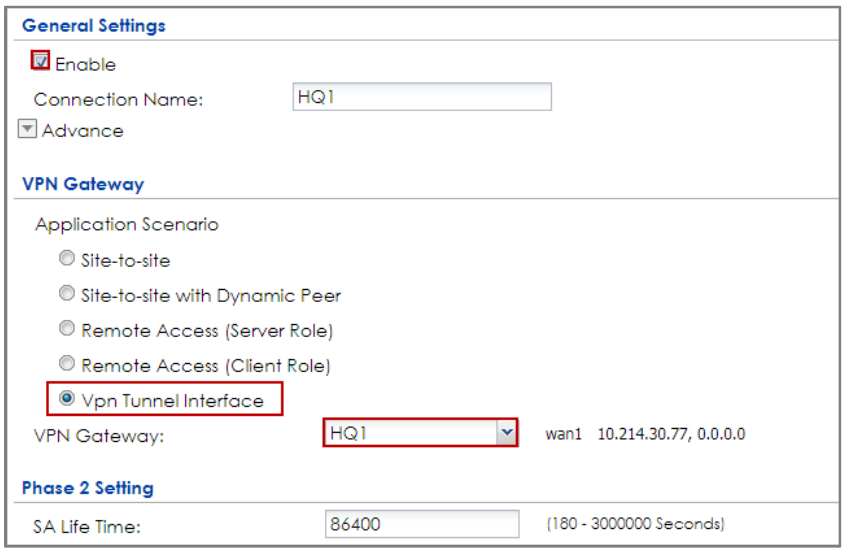
2 In the same screen, create the VPN gateway **HQ2** with **wan2**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add



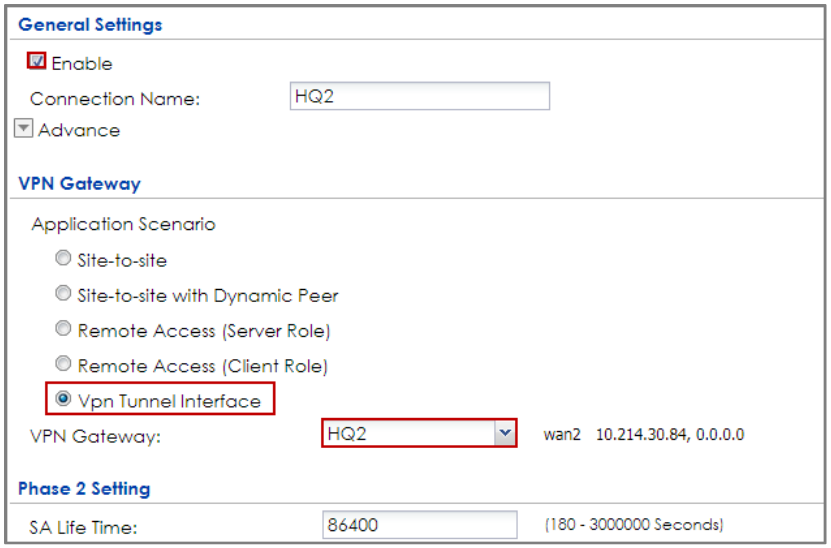
3 Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add** and configure a VPN tunnel for the VPN gateway **HQ1**. Select **VPN Tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add



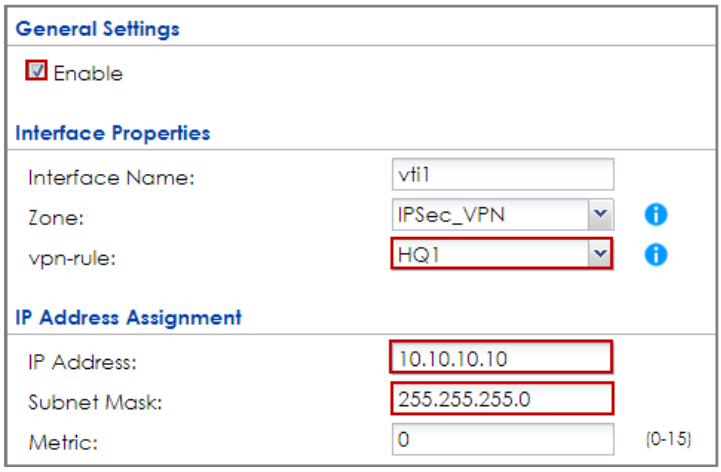
4 In the same screen, create a VPN tunnel for the VPN gateway **HQ2**. Select **VPN tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add

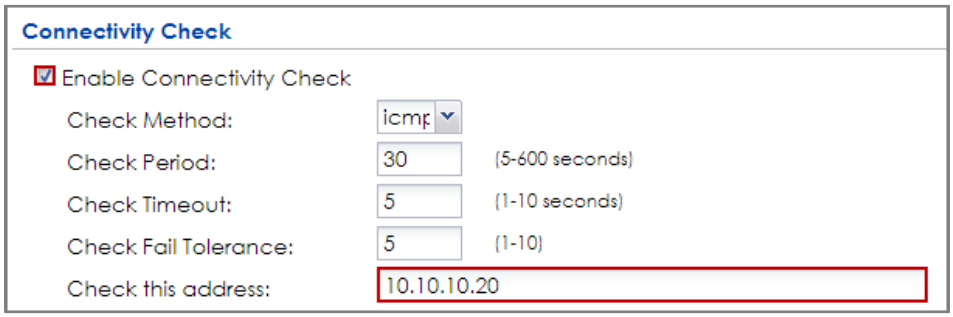


5 Go to **CONFIGURATION > Network > Interface > VTI > Add** to create a VTI for the VPN tunnel **HQ1**. Enable the connectivity check. Enter the IP address of **vti1**, which is configured on **USG2**.

CONFIGURATION > Network > Interface > VTI > Add

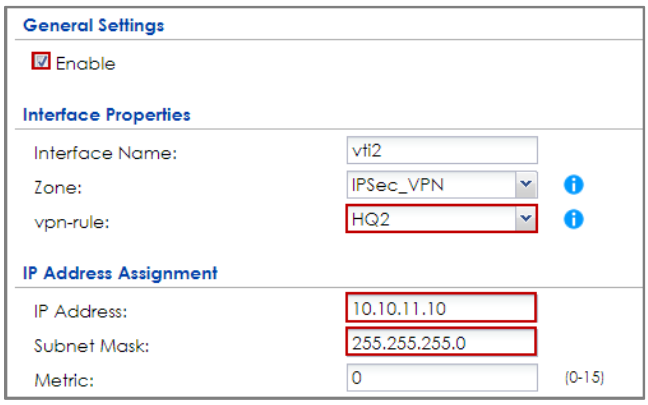


CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check

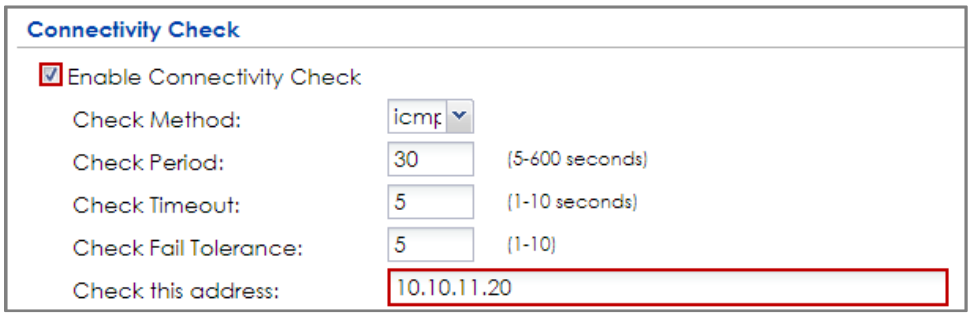


6 In the same screen, create a VTI for the VPN tunnel **HQ2**.

CONFIGURATION > Network > Interface > VTI > Add

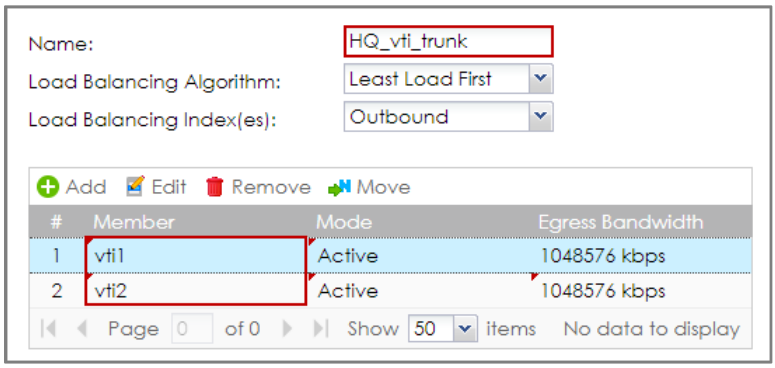


CONFIGURATION > Network > Interface > VTI > vti2 > Connectivity Check



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



8 Go to **CONFIGURATION > Network > Routing > Policy Route > Add** to configure a policy route.

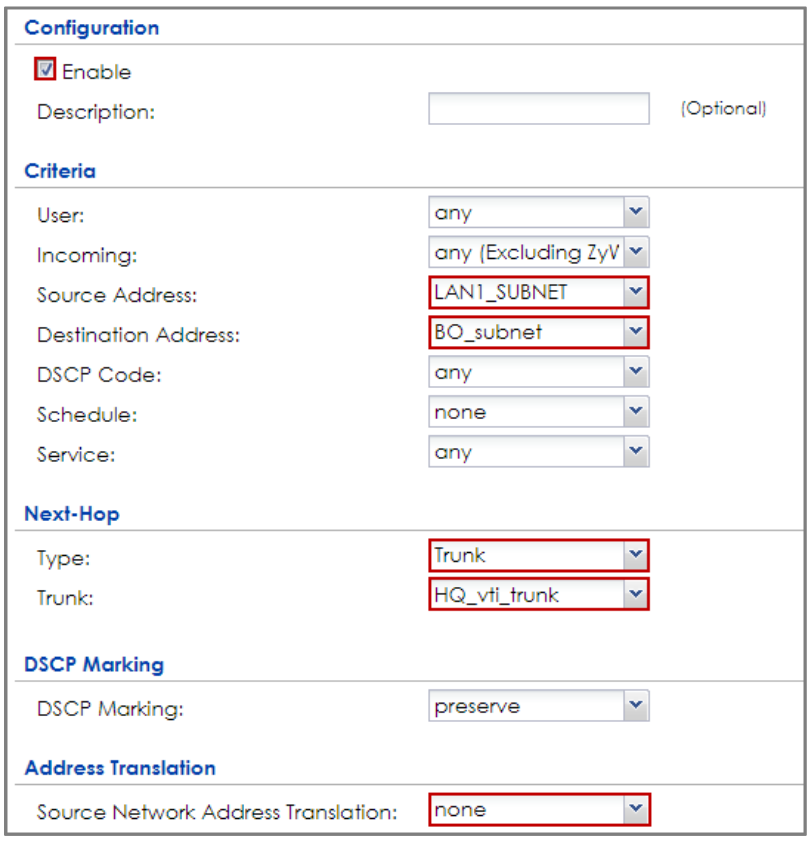
Source Address: LAN1_SUBNET (192.168.1.0/24)

Destination Address: BO_subnet (192.168.11.0/24)

Next-Hop: HQ_vti_trunk

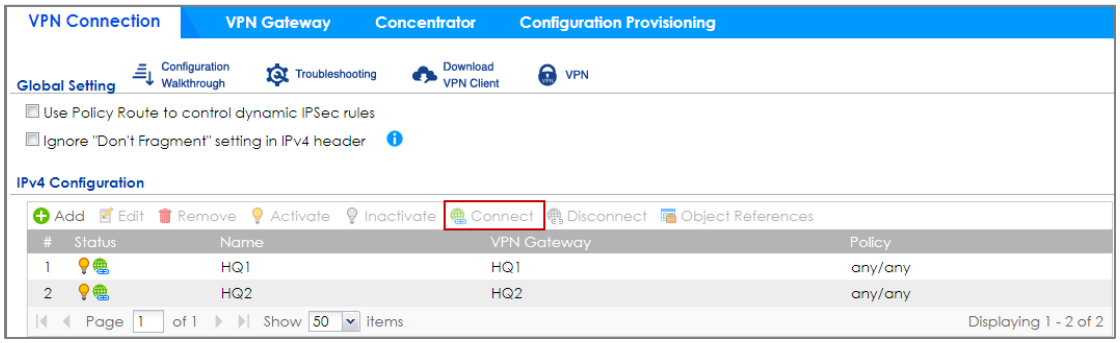
SNAT: none

CONFIGURATION > Network > Routing > Policy Route > Add



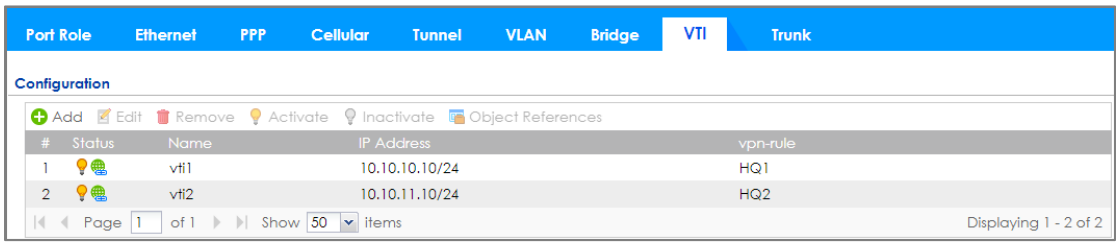
9 Connect the VPN tunnels when the VTIs are ready. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to connect the VPN tunnels.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Connect



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.

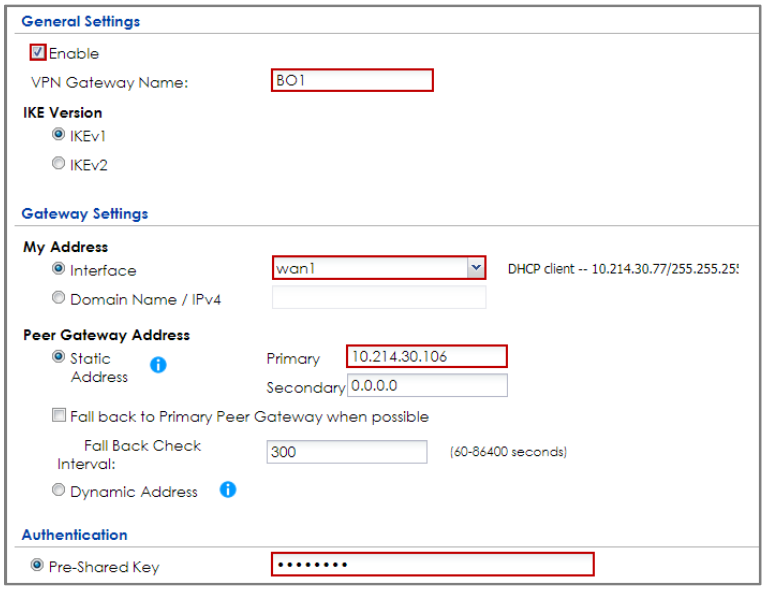
CONFIGURATION > Network > Interface > VTI



Set Up the ZyWALL/USG VTI of Corporate Network (Branch)

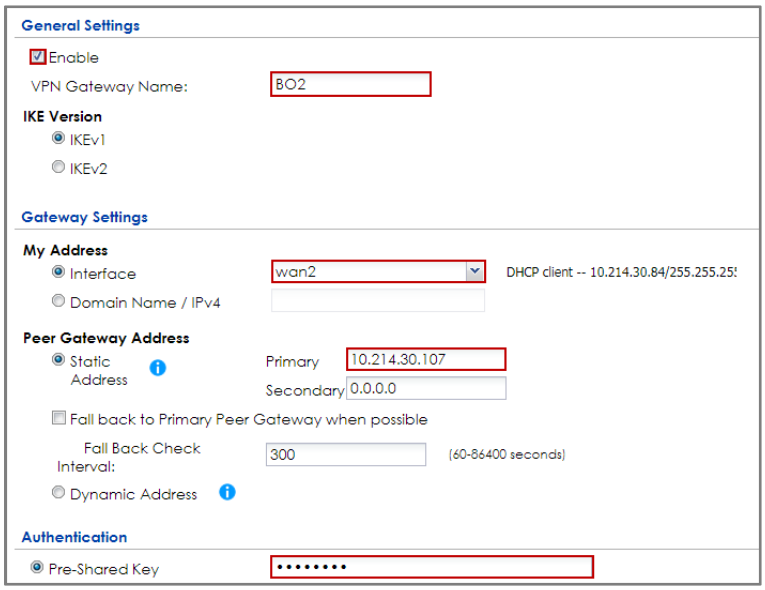
1 In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add** to create the VPN gateway **BO1** with **wan1**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add



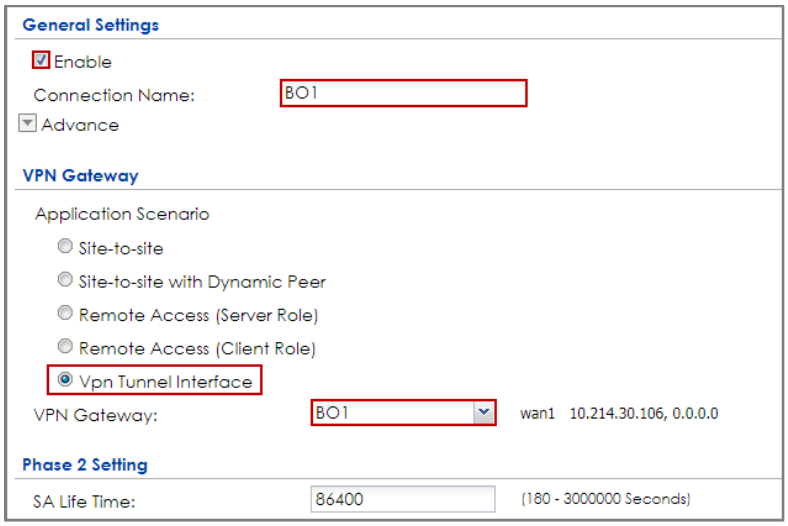
2 In the same screen, create the VPN gateway **BO2** with **wan2**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add



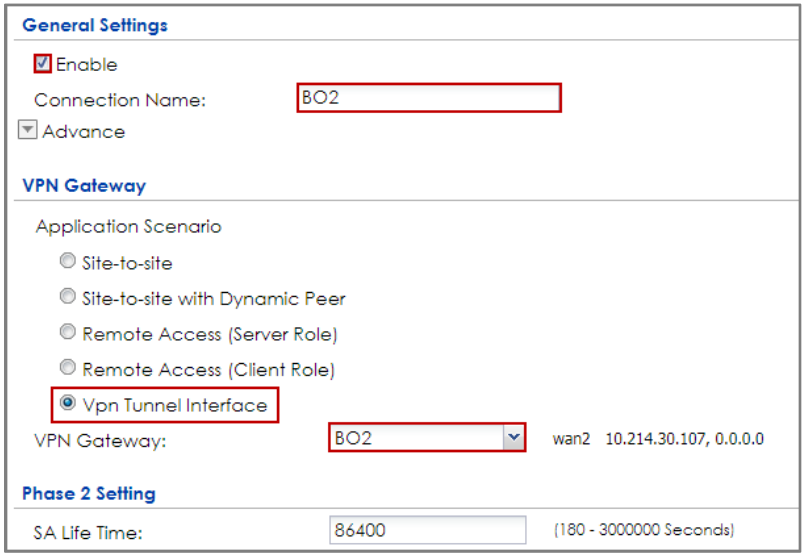
3 Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add** and configure a VPN tunnel for the VPN gateway **BO1**. Select **VPN Tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add



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

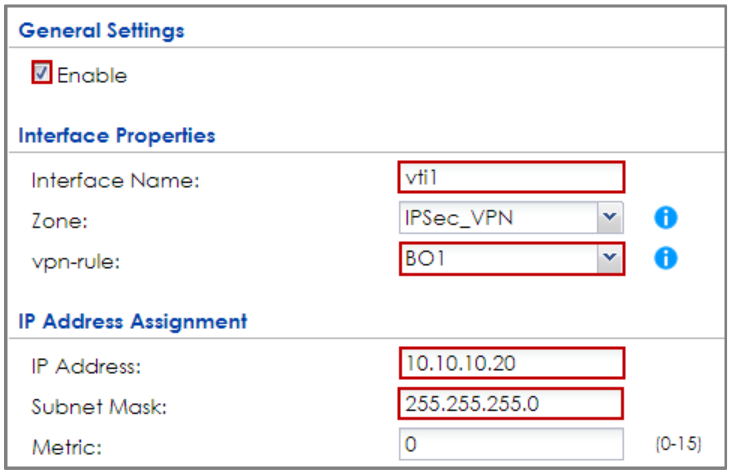
CONFIGURATION > VPN > IPSec VPN > VPN Connection > Add



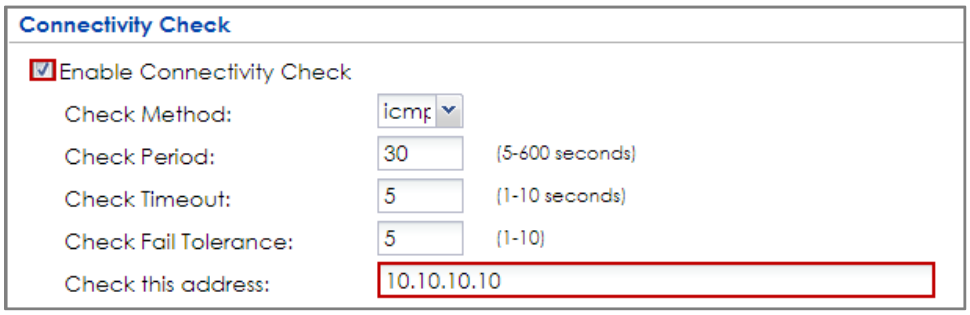
5 Go to **CONFIGURATION > Network > Interface > VTI > Add** to create a VTI for the VPN tunnel **BO1**. Be aware that the IP address of this VTI must be in the same subnet as **vti1** on **USG1**.

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

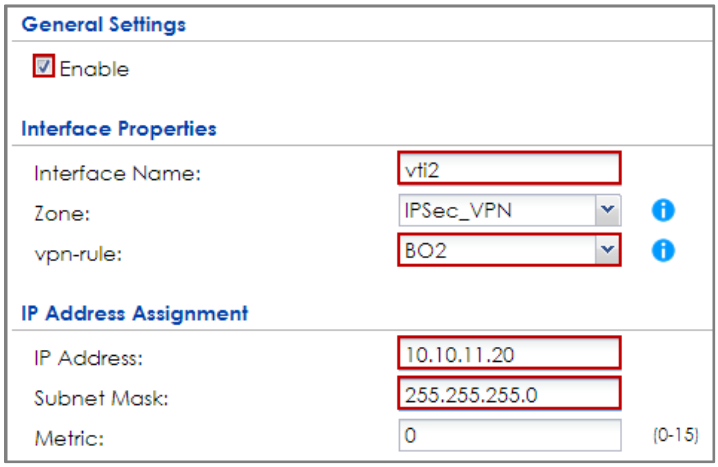


CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check

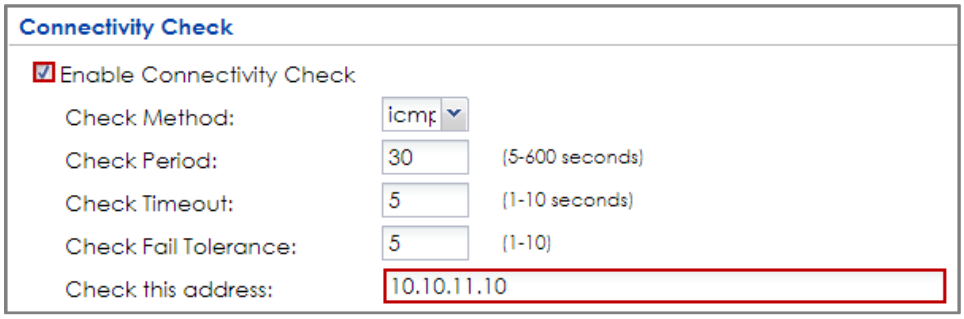


6 In the same screen, create a VTI for the VPN tunnel **BO2**. Be aware that the IP address of this VTI must be in the same subnet as **vti2** on **USG1**. In this example, the IP address and subnet mask of **vti2** on **USG1** is **10.10.11.10** and **255.255.255.0** respectively. The IP address of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

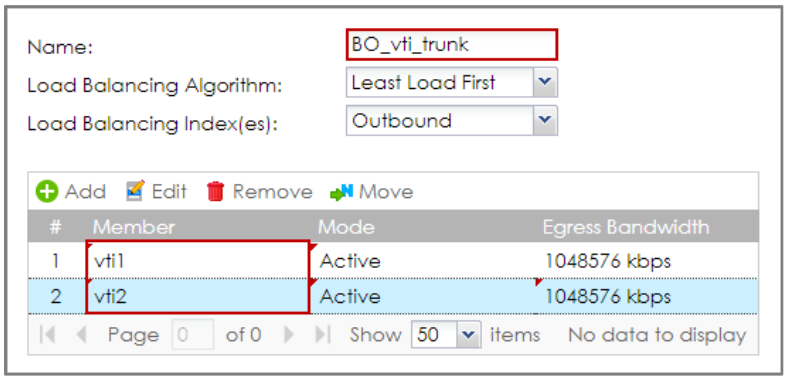


CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check



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



8 Go to **CONFIGURATION > Network > Routing > Policy Route > Add** to configure a policy route.

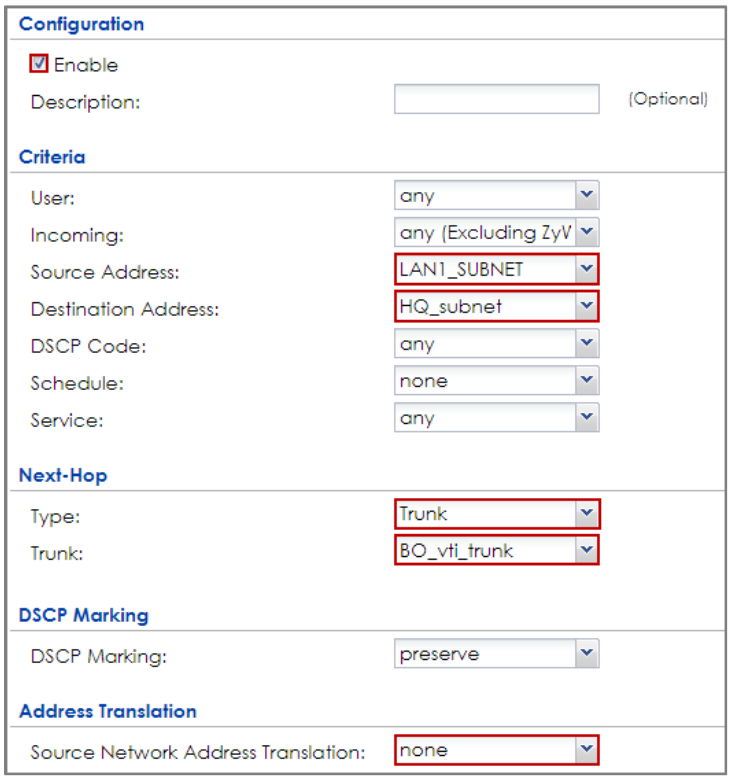
Source Address: LAN1_SUBNET (192.168.11.0/24)

Destination Address: HQ_subnet (192.168.1.0/24)

Next-Hop: BO_vti_trunk

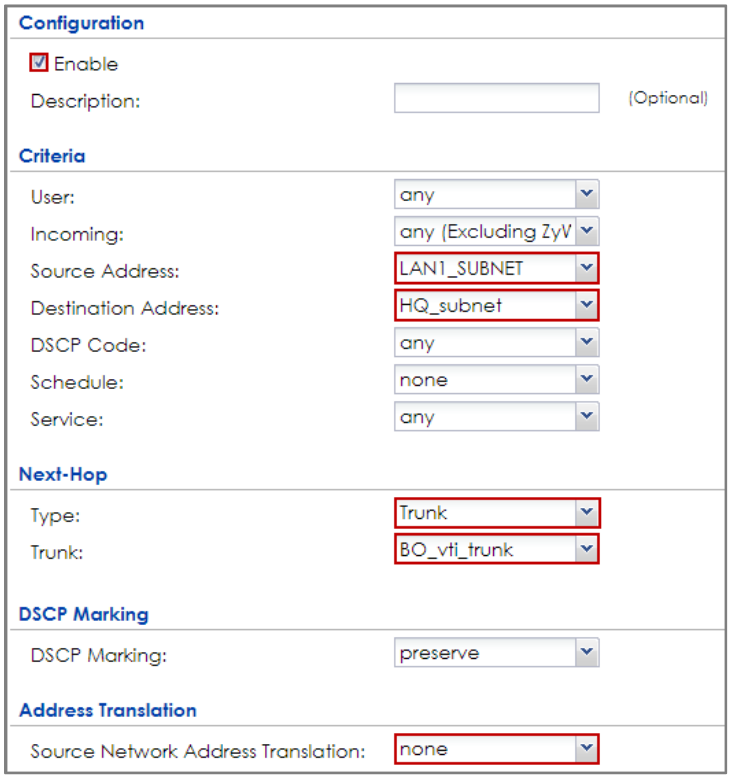
SNAT: none

CONFIGURATION > Network > Routing > Policy Route > Add



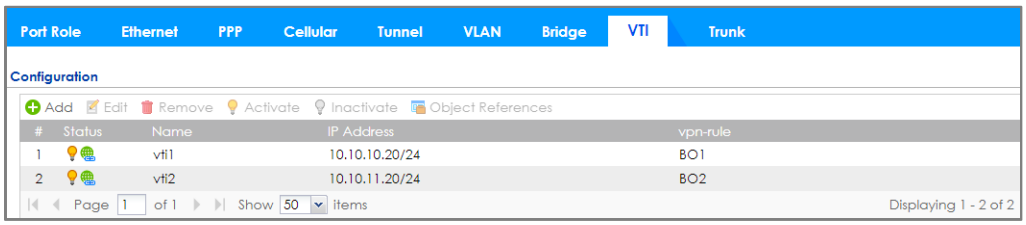
9 Connect the VPN tunnels when the VTIs are ready. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to connect the VPN tunnels.

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Connect



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

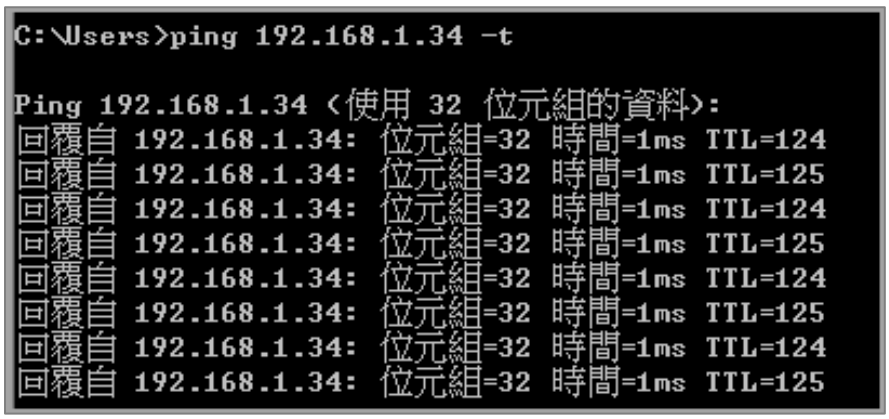


Test the IPSec VPN Tunnel

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.

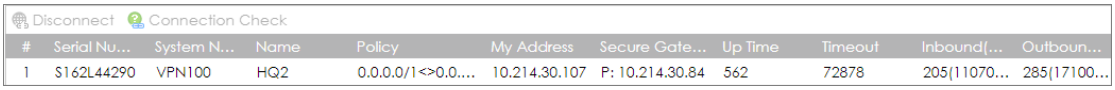
PC of USG1 (192.168.1.34) > Window 7 > cmd > ping 192.168.11.33

PC of USG2 (192.168.11.33) > Window 7 > cmd > ping 192.168.1.34



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.


Disconnect Connection Check

#	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...

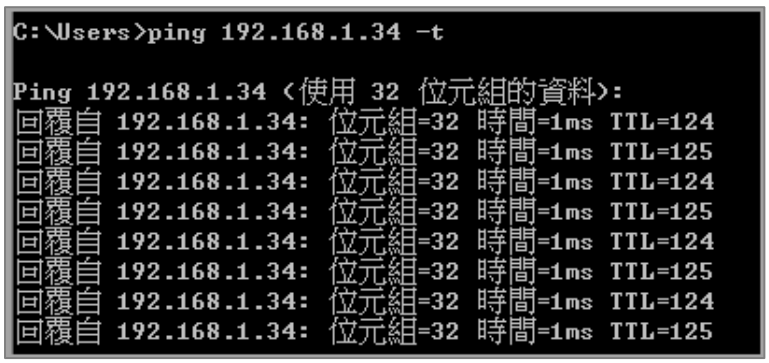
PC of USG1 (192.168.1.34) > Window 7 > cmd > ping 192.168.11.33

Check the VPN status of the USG2 in the MONITOR > VPN Monitor > IPSec screen.

Disconnect Connection Check

#	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



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.

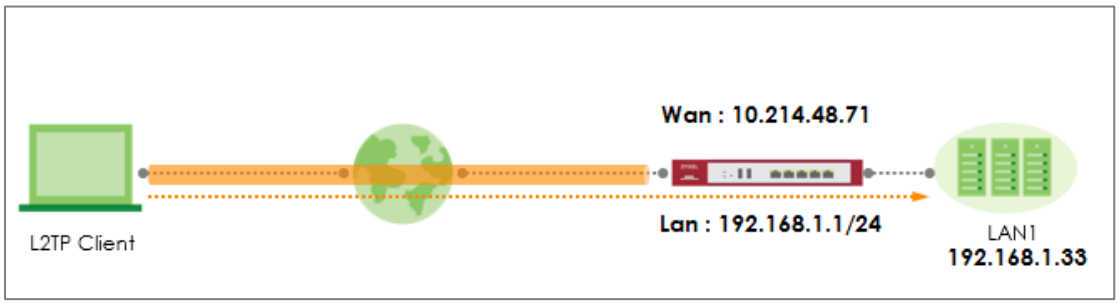
6 Make sure policy routes are configured to control traffic between the subnet of HQ and Branch through VTI.

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

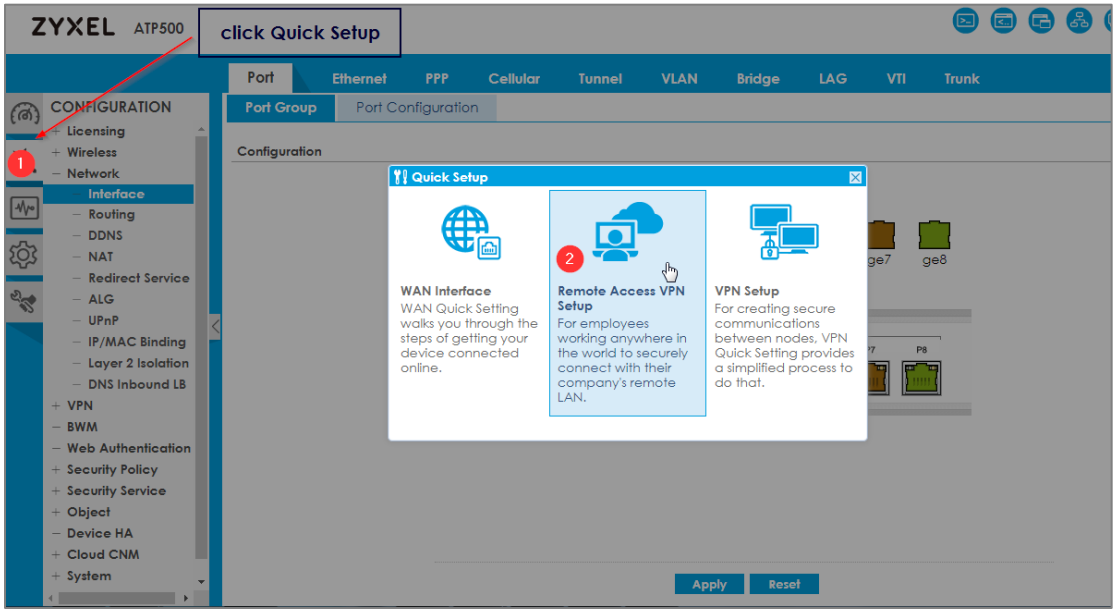
The following is a sample configuration how to build up VPN tunnel with the remote access VPN wizard.

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.

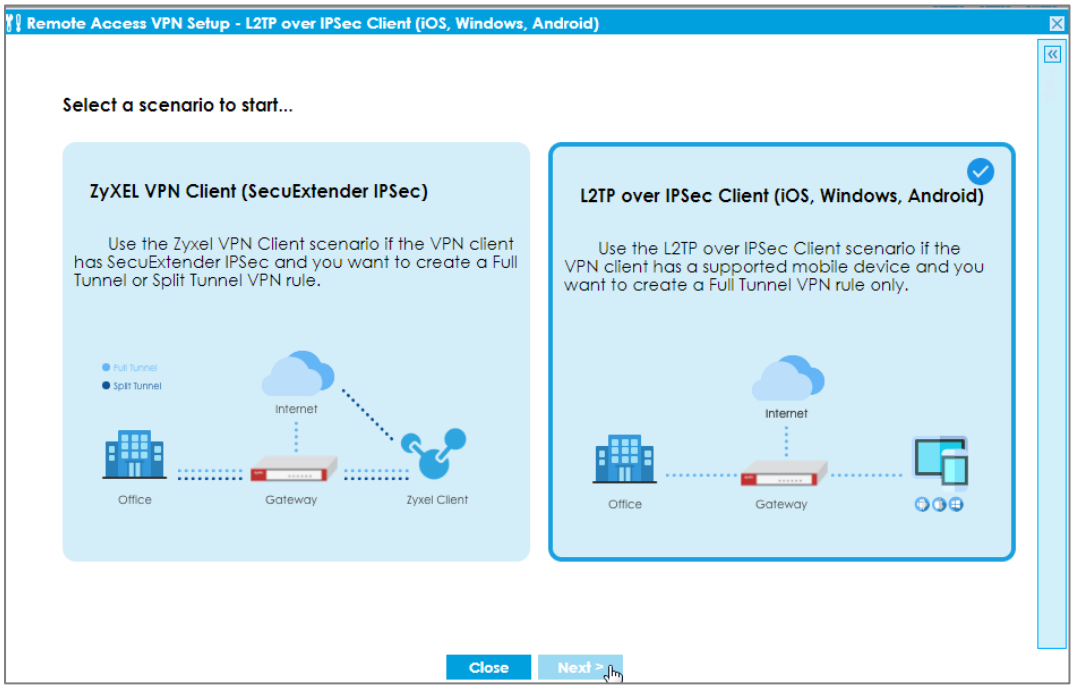


Set up VPN Tunnel

1. In the ZyWALL/USG, Click Quick Setup, then click Remote Access VPN Setup build up VPN tunnel with the Wizard.



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.

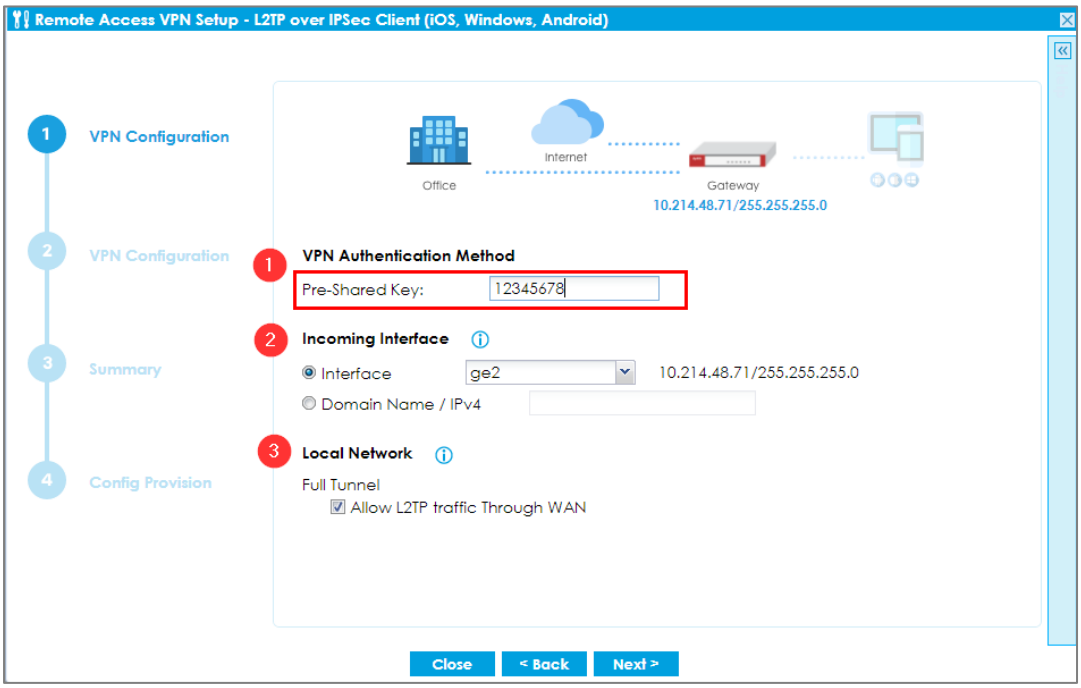


3. Configure the VPN configuration

(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".

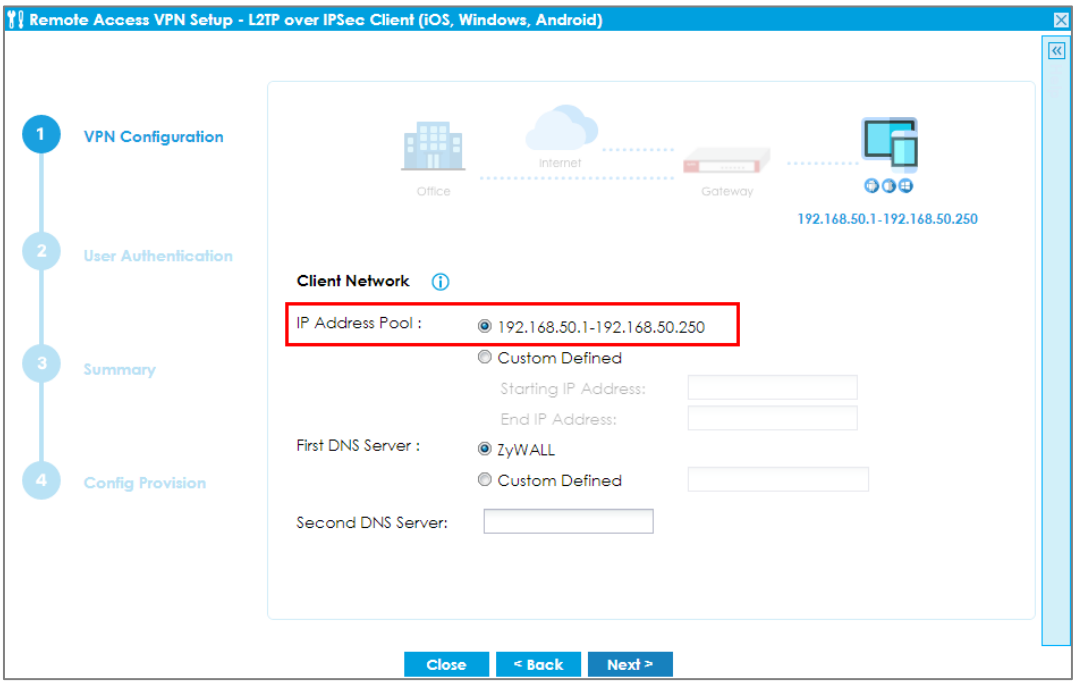


4. Configure the IP Address Pool for the client

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

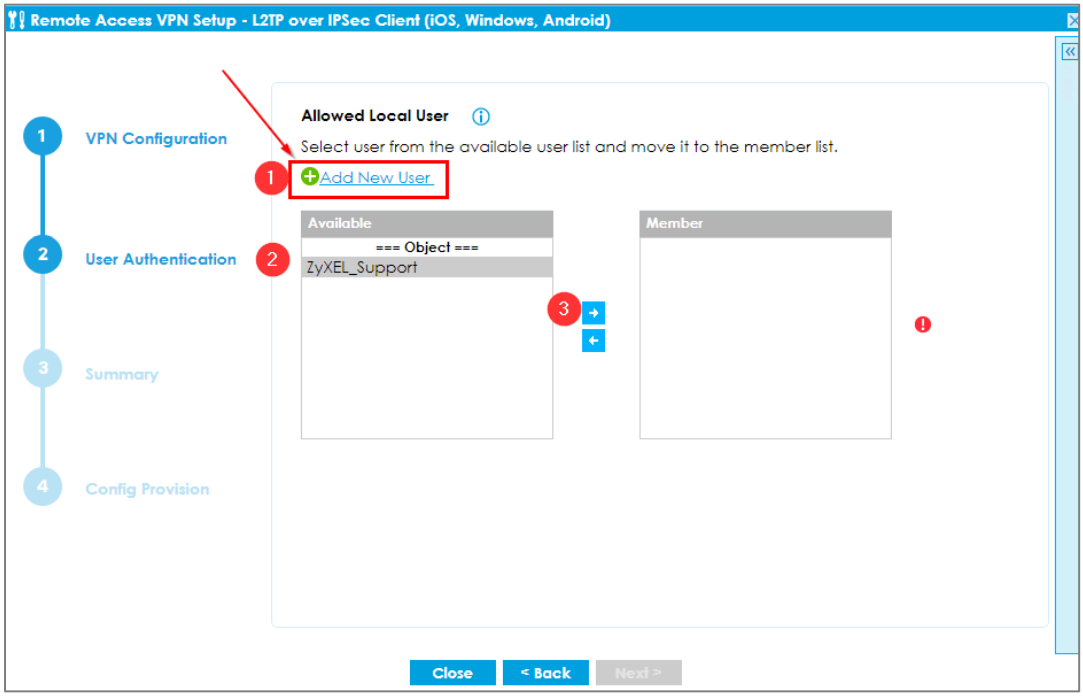
If there is 192.168.50.1 subnet exist in the settings, the IP address pool will change to 192.168.51.1 subnet.

Note: The Subnet only detect the subnet mask is under /24, if the subnet is not /24, it will not detect it.

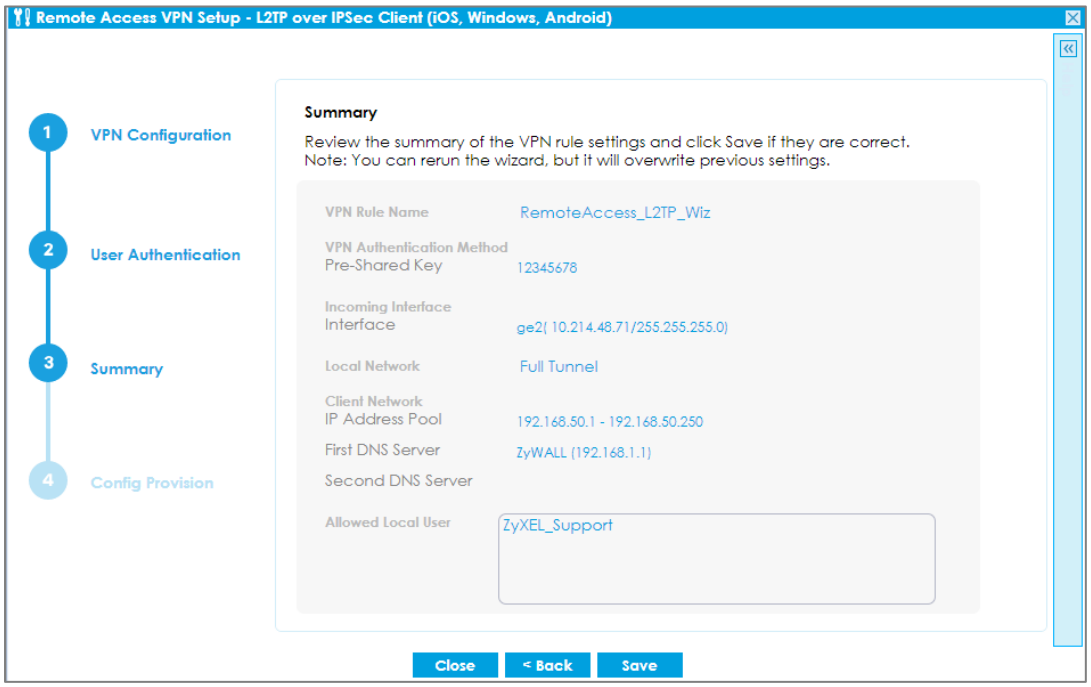


5. Allow local user to access the device

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.



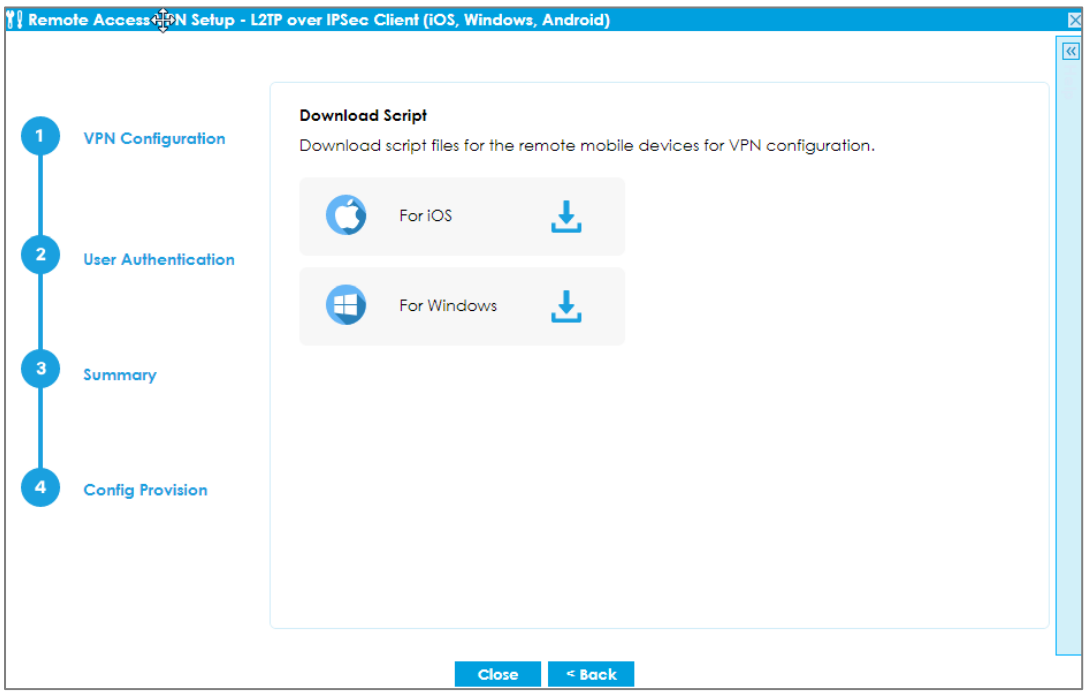
6. After done all the steps in the wizard, you can check the settings at the final step, if there is any settings wrong, you can click back to reset the configuration.
If the settings are all correct, click save to go next step.



7. Download script for Windows or IOS

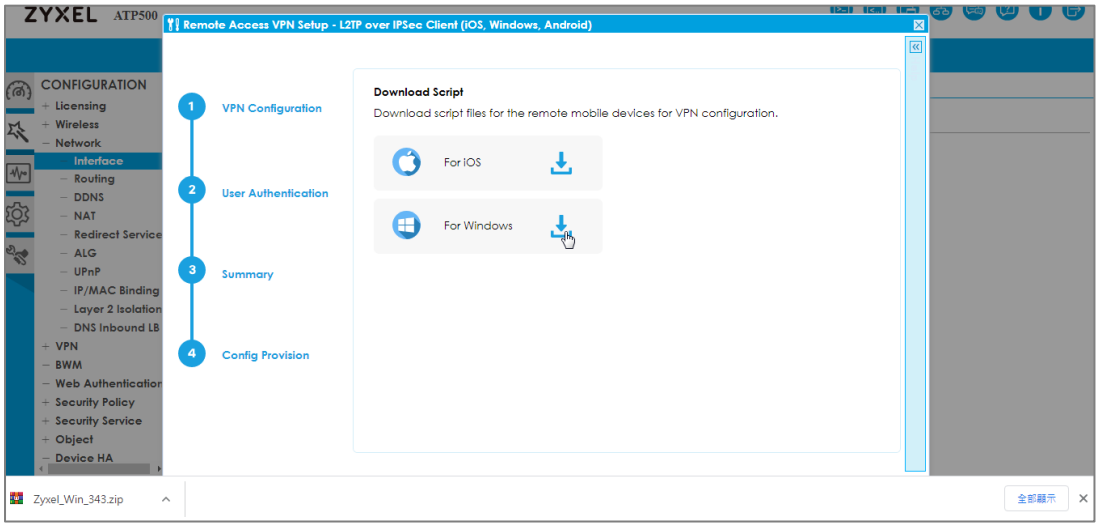
To quick connect to the device from client, we support scripts to run on IOS and Windows system.

Note: We do not support the script for Android system.



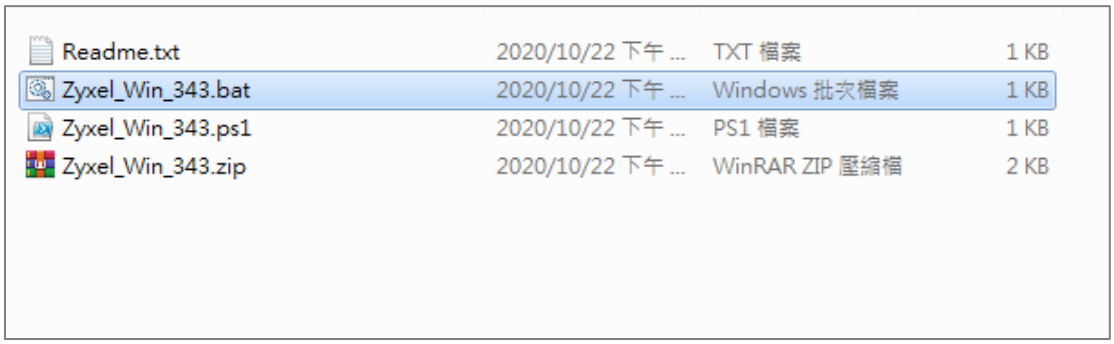
8. Download the scripts to quick build up VPN tunnel to the device on the client.

Note: Script file on windows support for Window8/ Window10



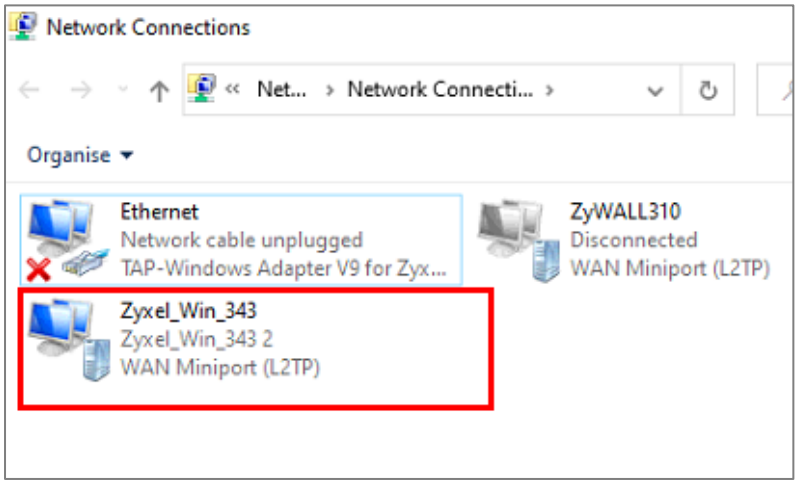
Test the result

1. Extract the download script on windows, and run the scripts

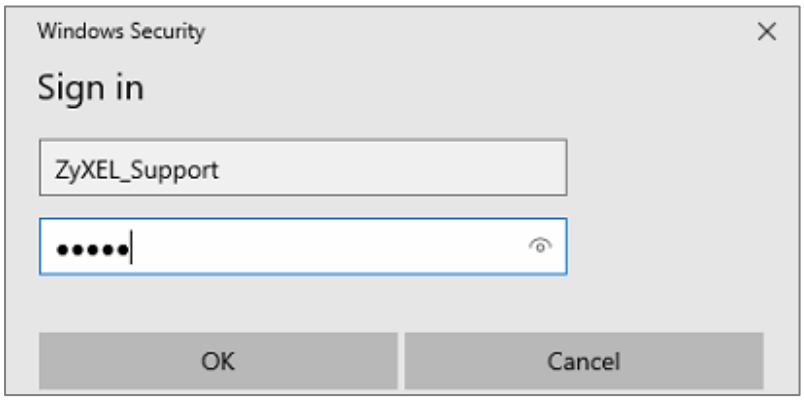


2. Using PowerShell to run the scripts

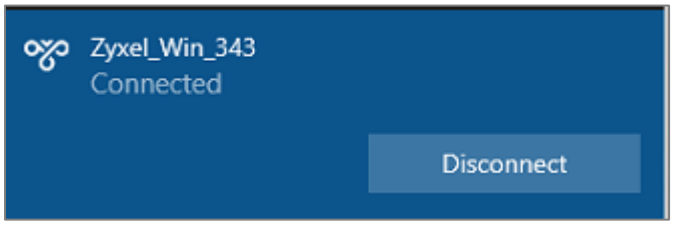
3. It will generate a site to connect to the device



4. Double click the icon and sign in the username and password



Now you can successfully build up the VPN tunnel

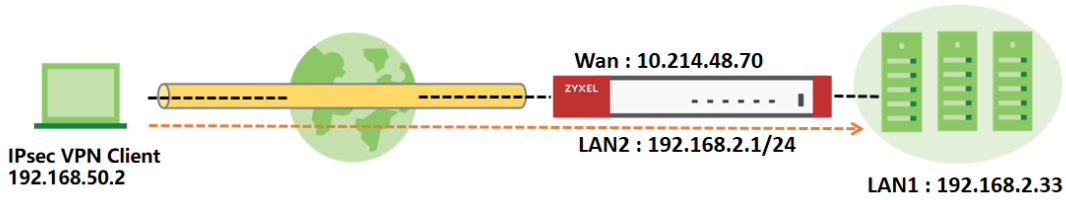



```
C:\Users\qweqa>ping 192.168.1.33

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

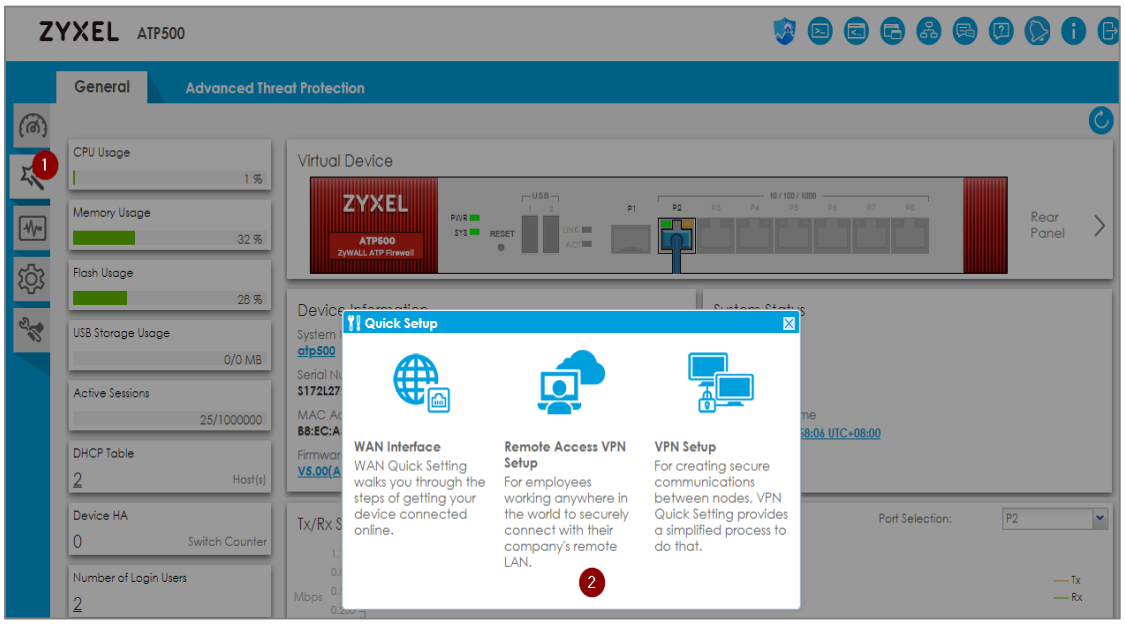
Remote access VPN Wizard-IKEv2 Client



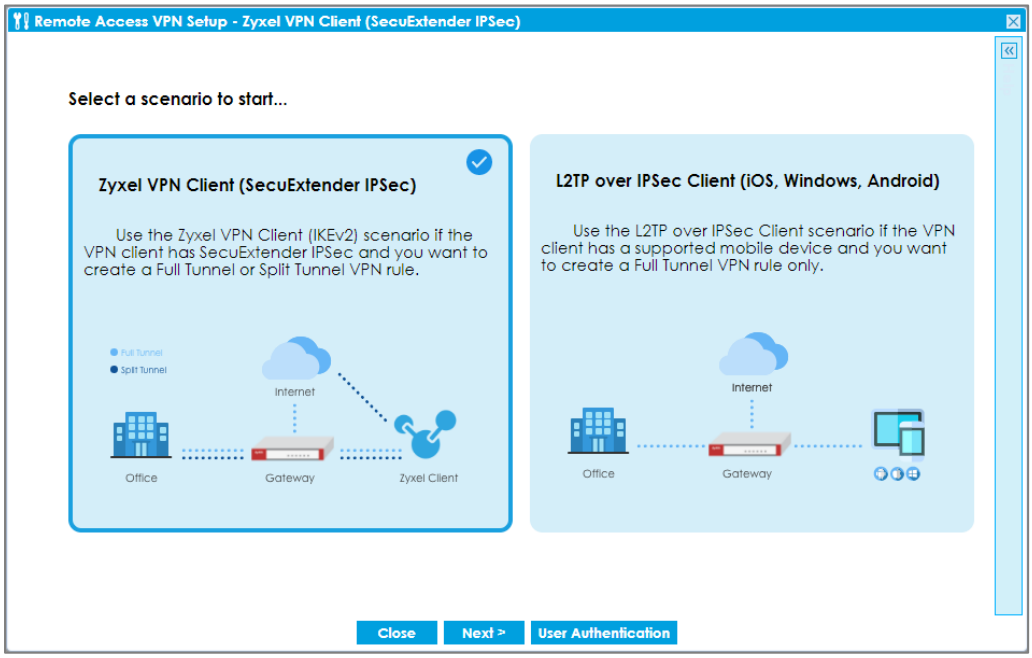
With USG FLEX/ ATP you are able to provision predefined settings on your device to your IPsec VPN Client. This article will show you how to use **Remote Access VPN Setup** Wizard to setup configuration provisioning for IKEv2 VPN connections in combination with the IPSec VPN Client.

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.



2.Select remote VPN scenarios, **ZyXEL VPN Client(SecuExtender IPSec)**.

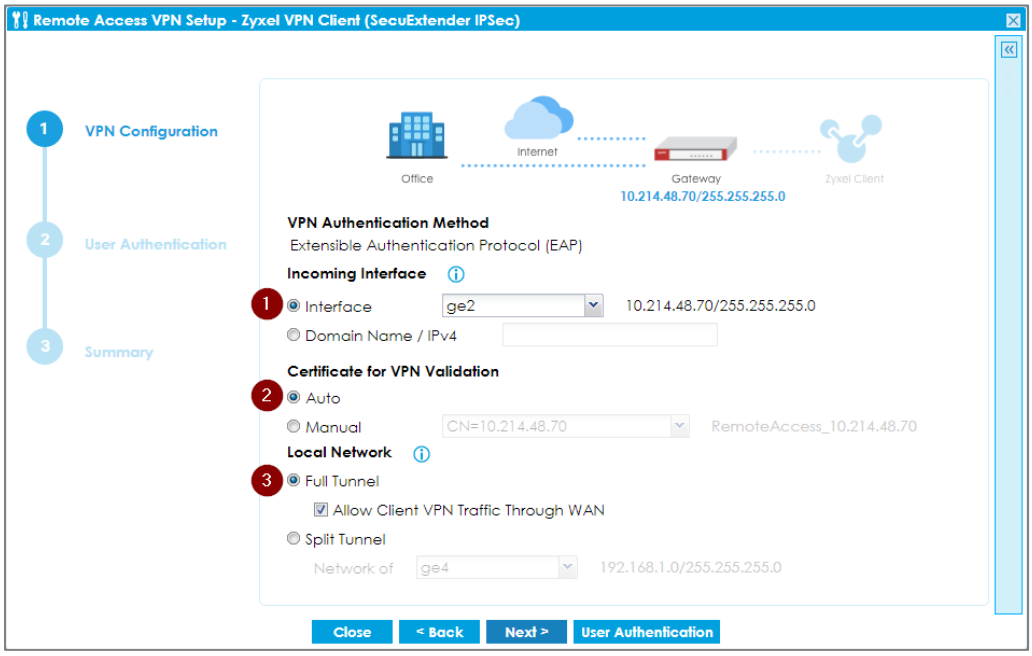


3.Configure the VPN Authentication Method

(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".

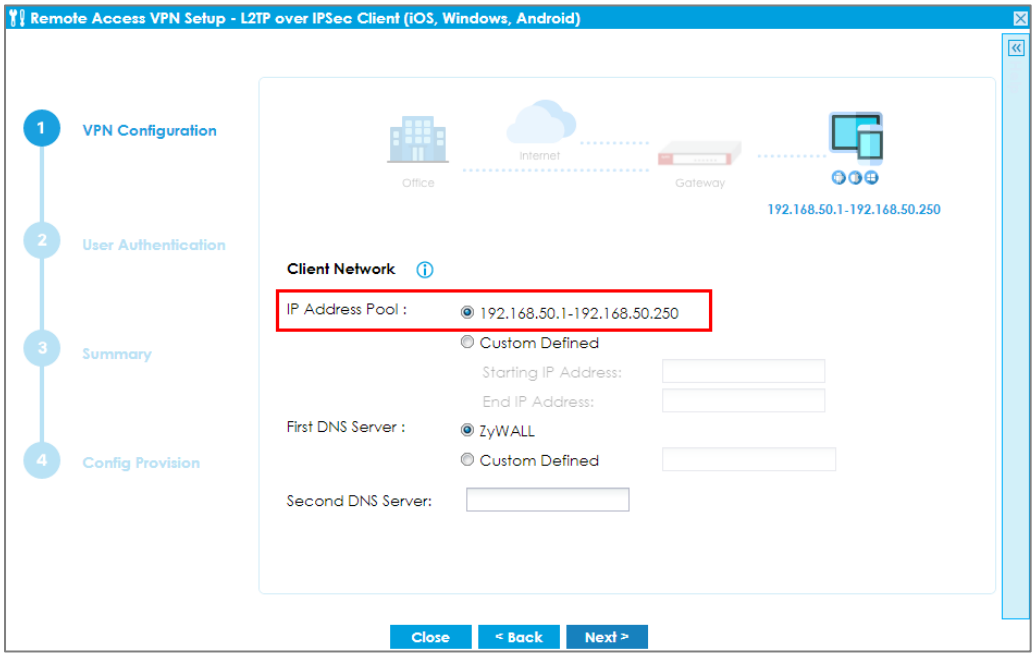


4.Configure the IP Address Pool for the client

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

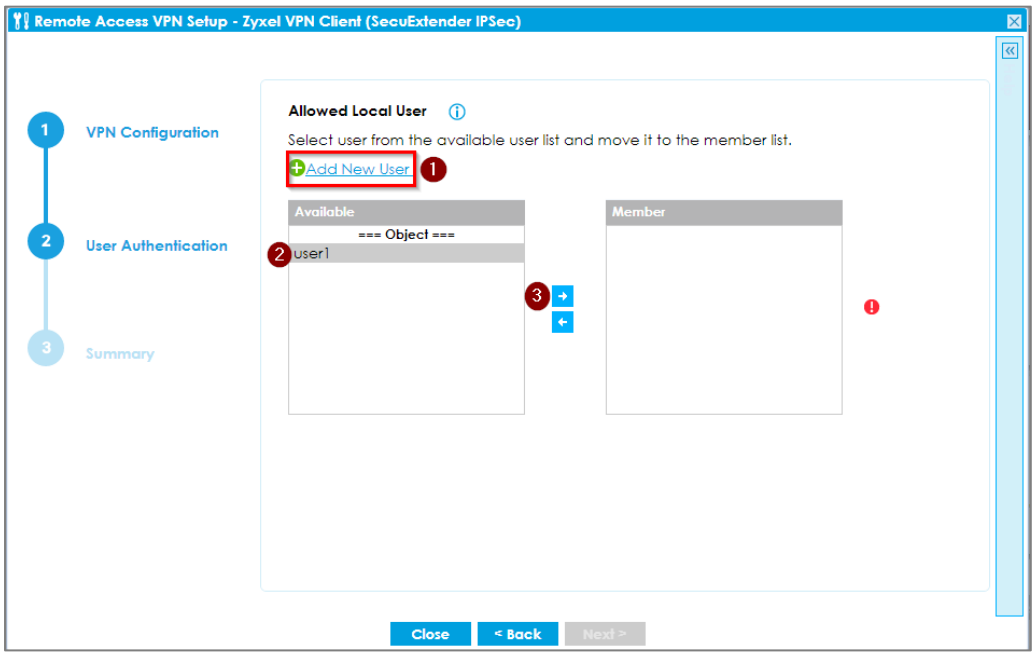
If there is 192.168.50.1 subnet exist in the gateway settings, the IP address pool will auto change to 192.168.51.1 subnet.

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



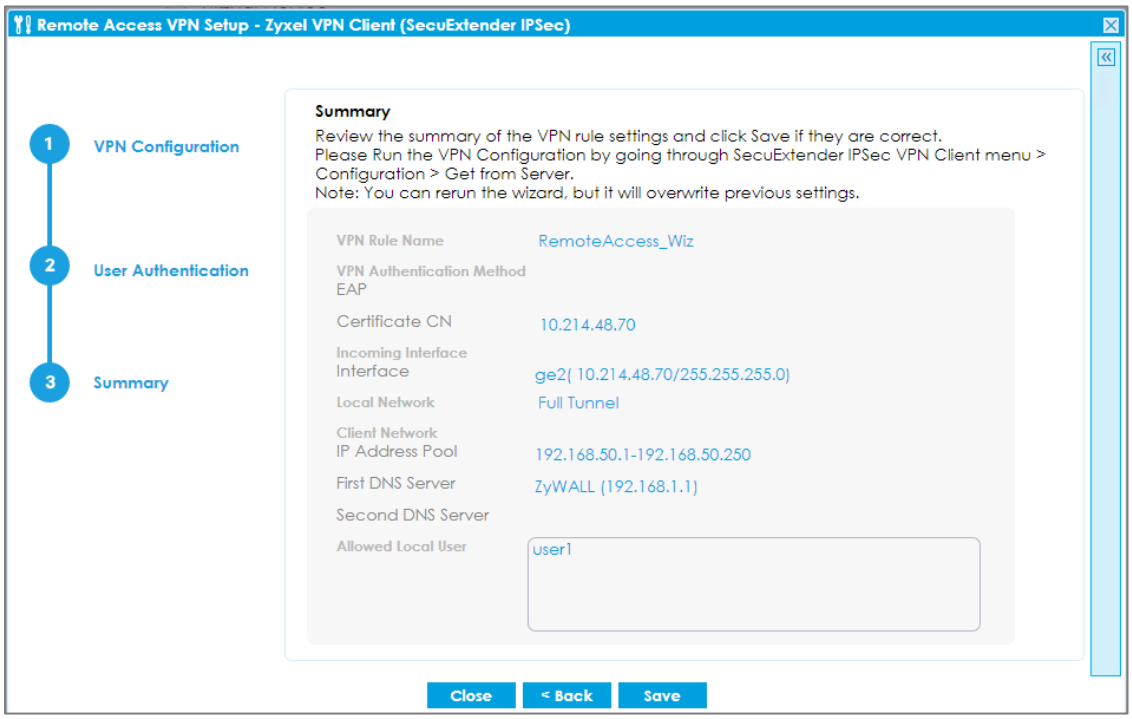
5.Allow local user to access the device

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.



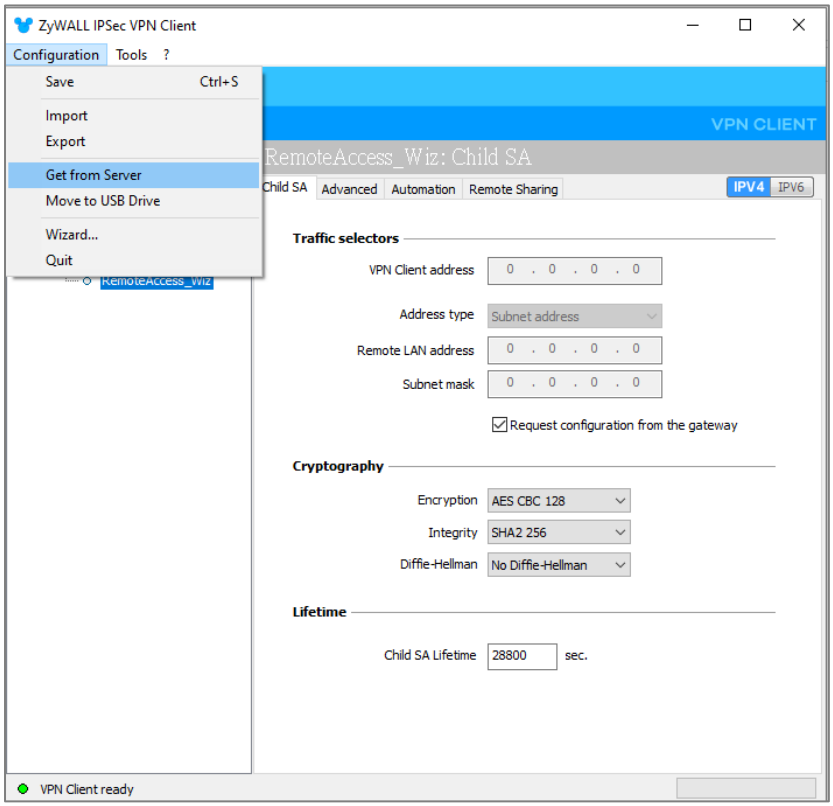
6.After done all the steps in the wizard, you can check the settings at the final step, if there is any settings wrong, you can click back to reset the configuration.

If the settings are all correct, click save to go next step.

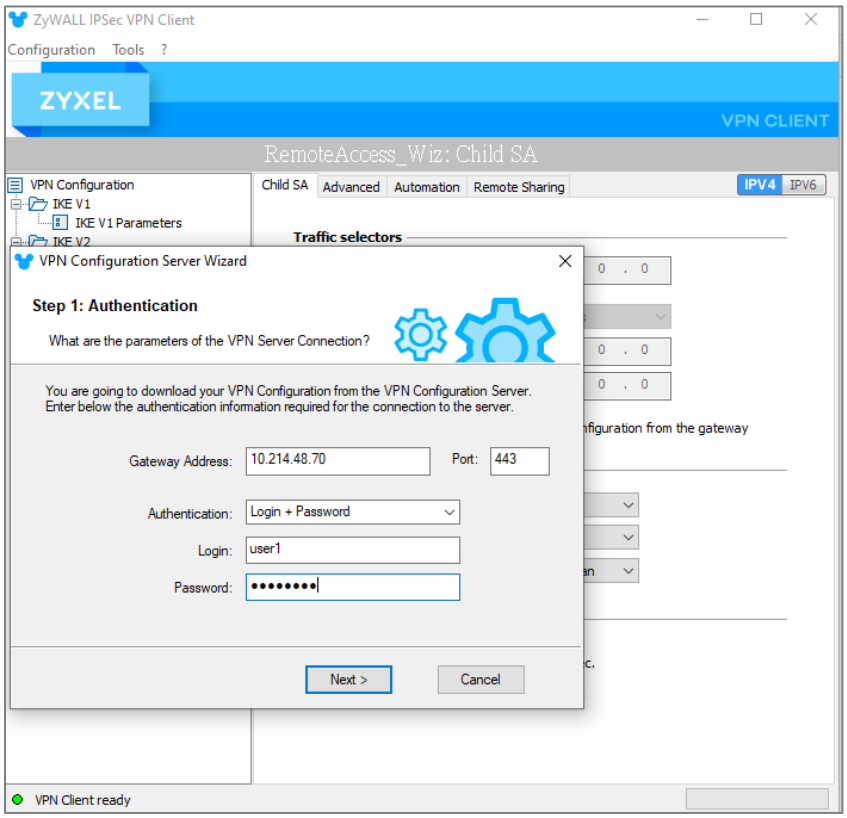


Test the result

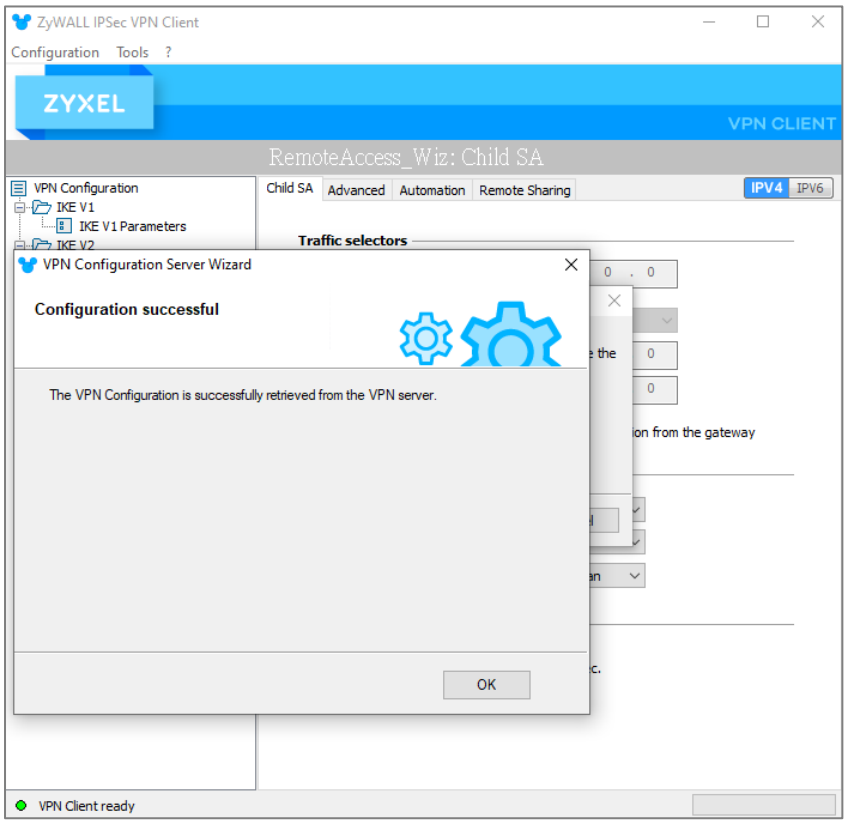
1. Open **ZyWALL IPSec VPN Client**, go to **Configuration > Get from Server**



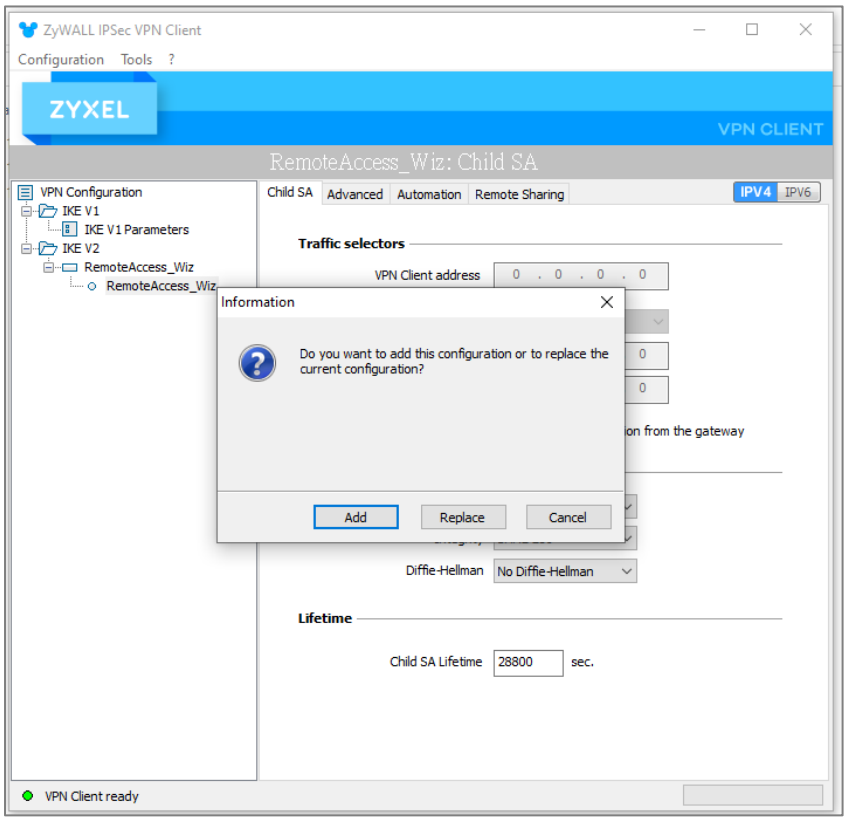
2. Typing the IP address of server, user account, and password. Then click on **Next**



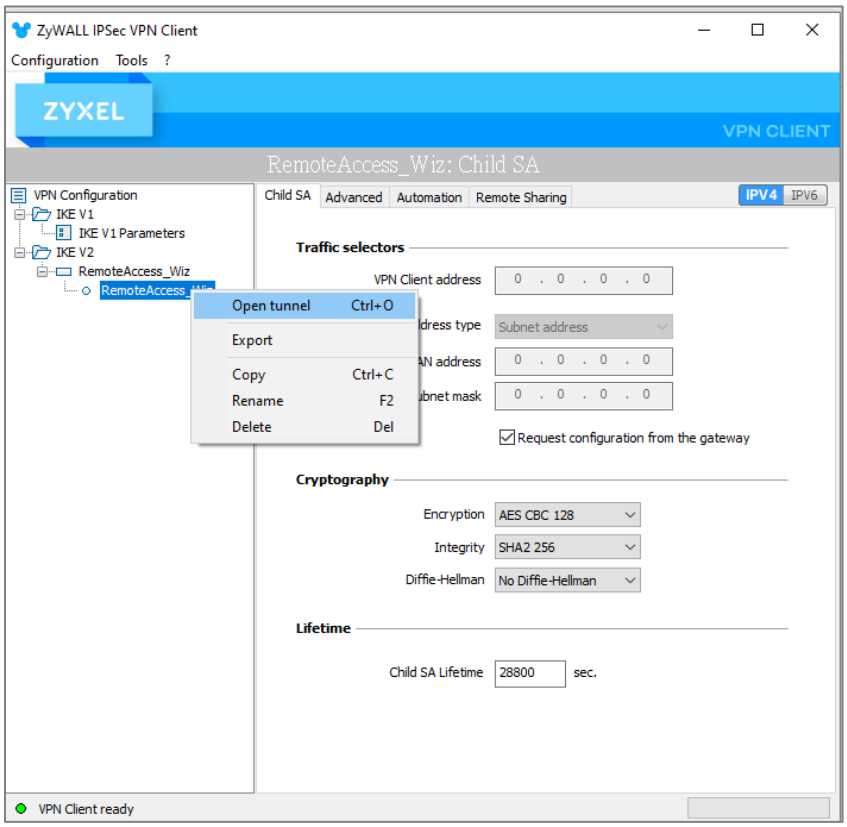
3. Wait until the VPN Client download successfully the configuration from server.



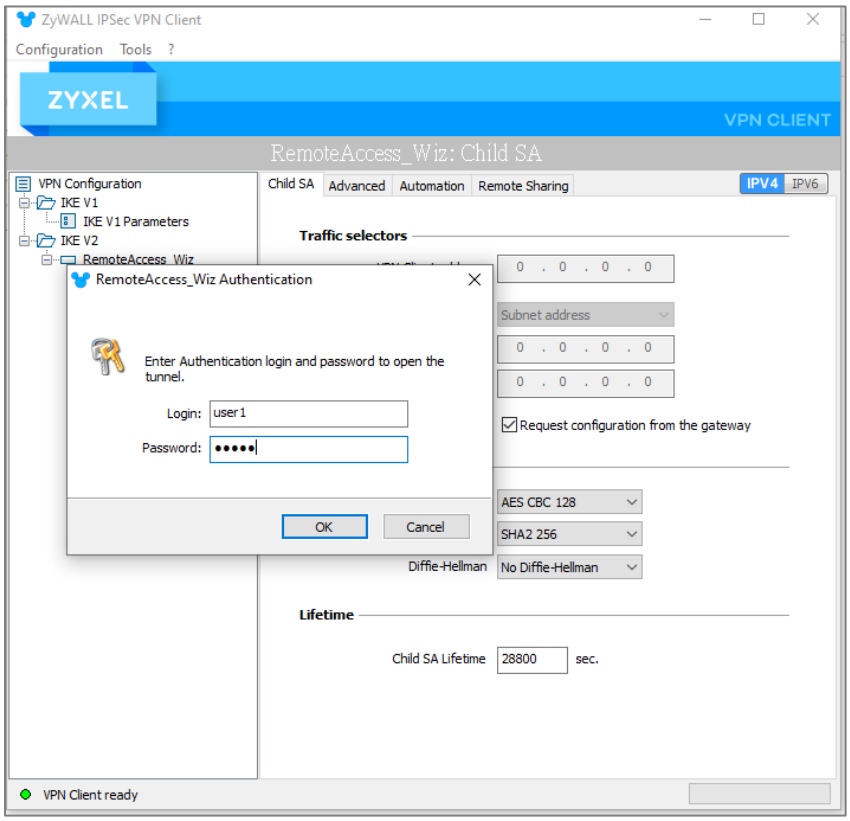
4. If you have an existing VPN configuration on the VPN client, click **Add** to replace.



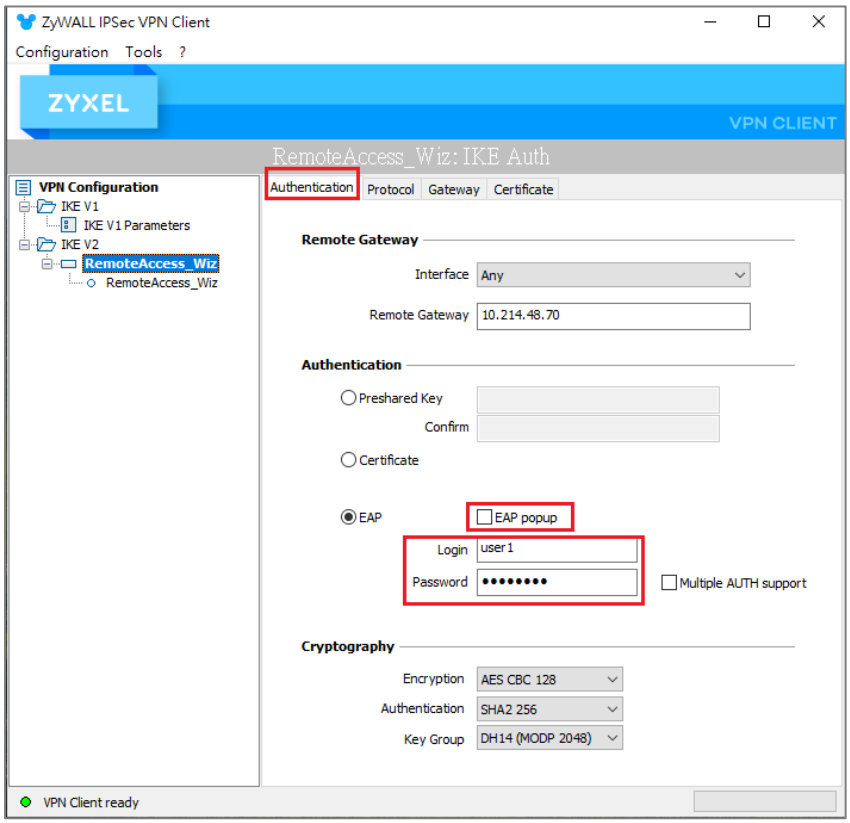
5. Right-click this configuration and press Open tunnel.



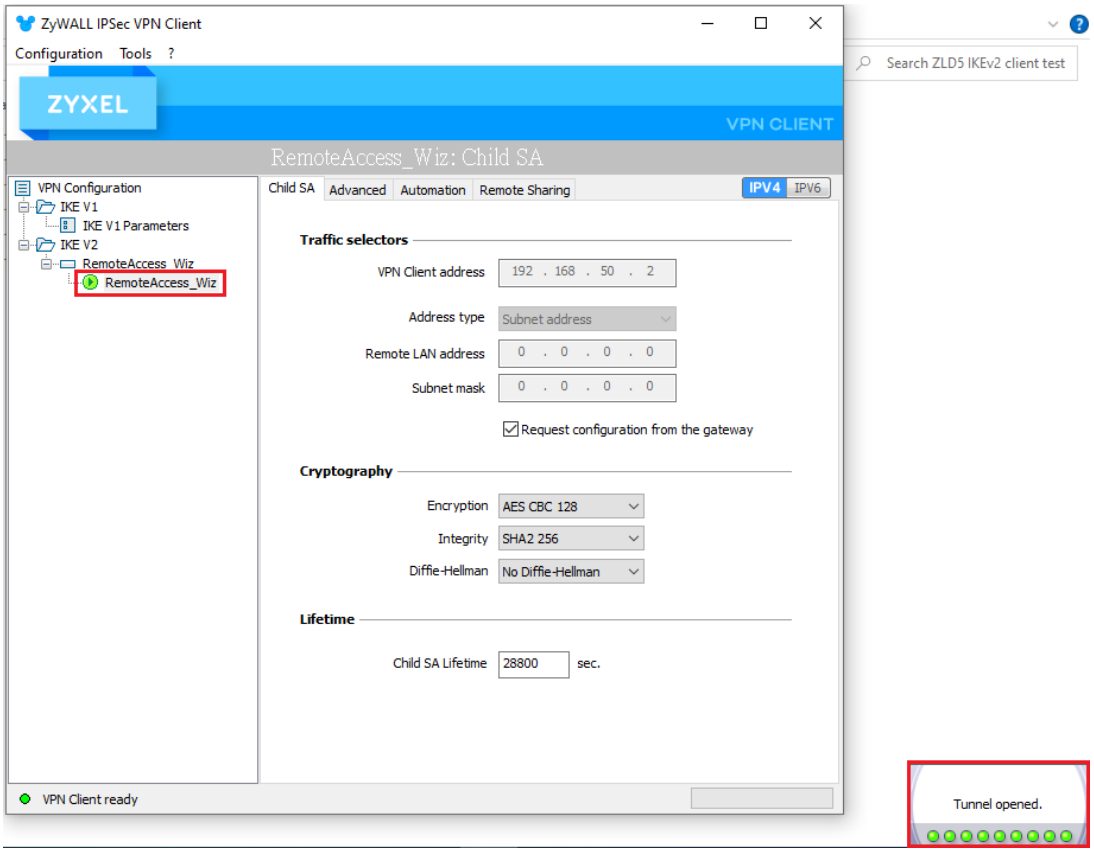
6. Popup window then typing login account and password.



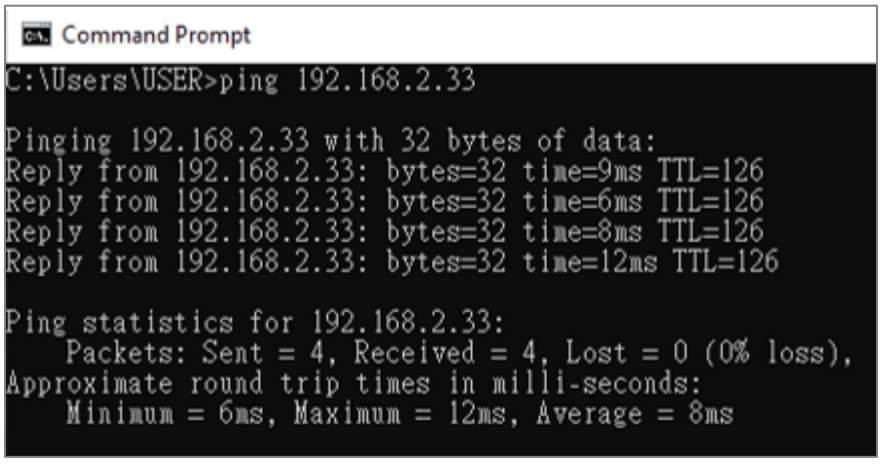
Or you can configure login account and password on Authentication tab in advance.



7. IKEv2 VPN connection established successfully.



8.The remote user can ping the internal network IP address without problem.



VPN Configuration Provisioning with Upload Bandwidth Limit

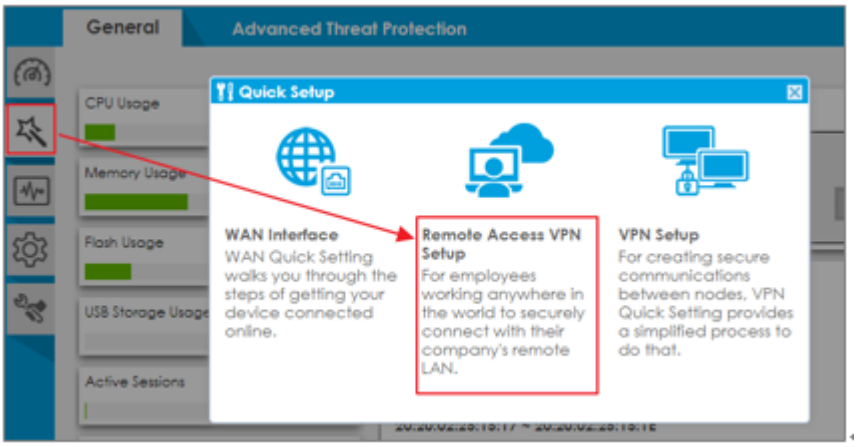
In ZLD5.10, gateway is able to provisioning the VPN configuration with upload bandwidth limit to the time-based Zyxel IPSec VPN client.

> Note: Bandwidth limit only support on time-based Zyxel VPN Client

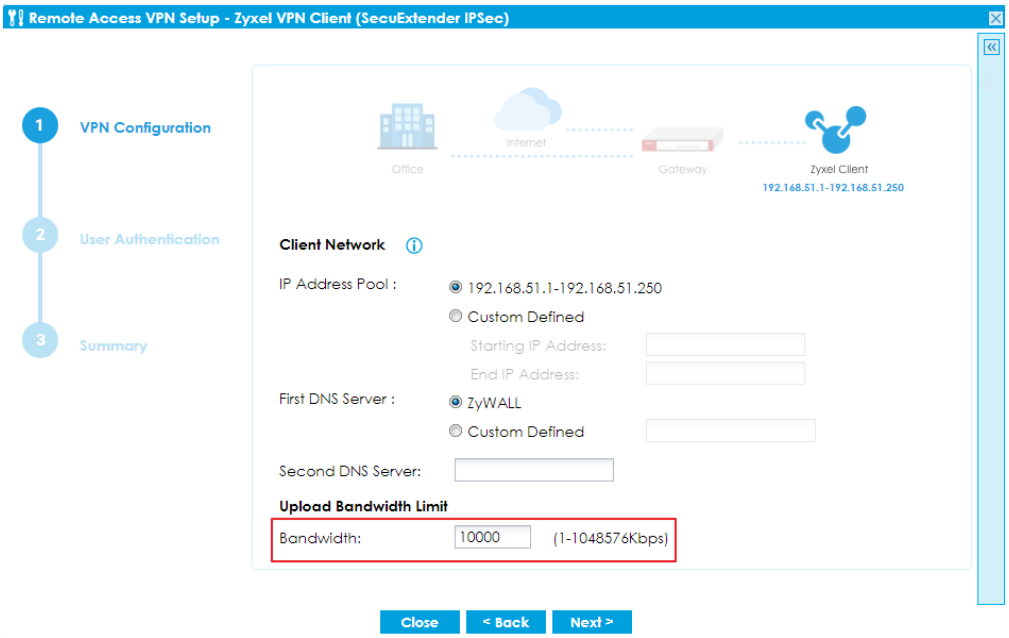
On-premises Mode

Setup Remote Access VPN using Quick Setup Wizard

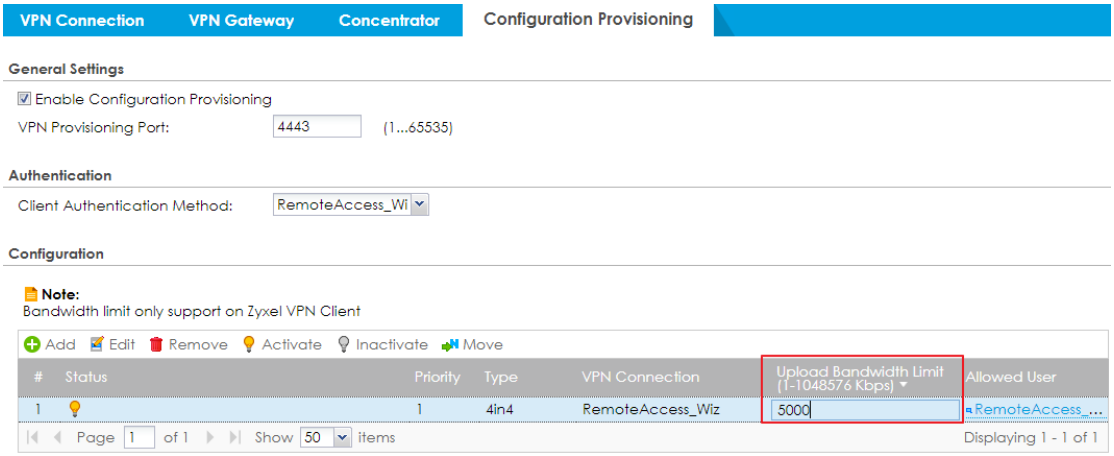
In the Web GUI, go to Quick Setup > Remote Access VPN Setup. Select Zyxel VPN Client (SecuExtender IPSec) scenario to to run the VPN wizard



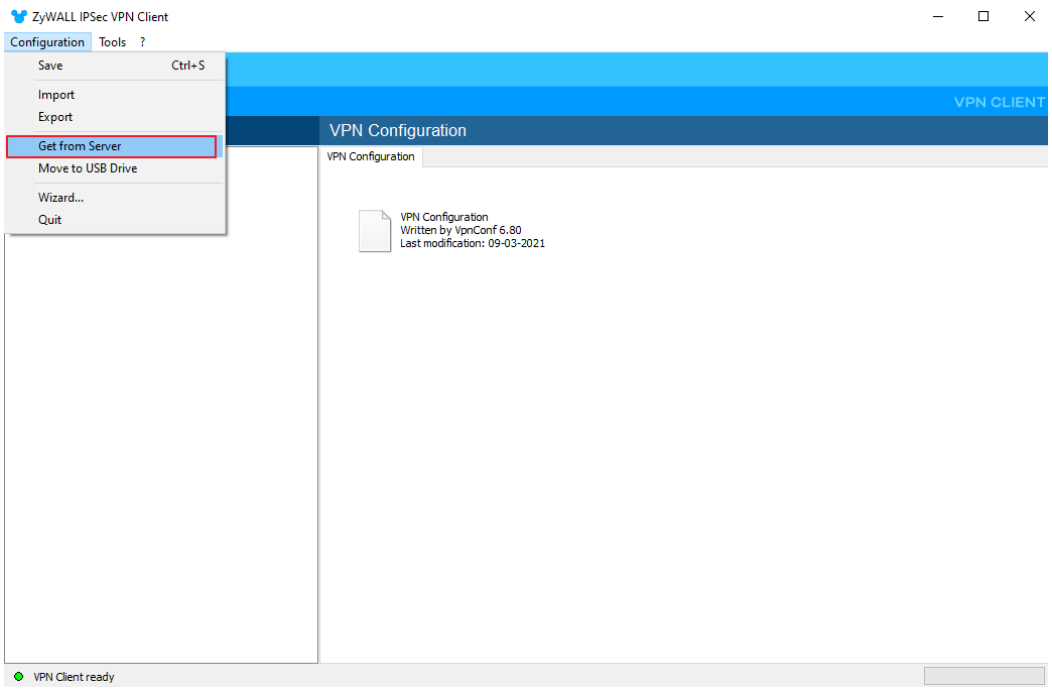
- In the VPN Configuration step, you are able to input the upload bandwidth limit for Zyxel IPSec VPN client. Upload Bandwidth Limit to set the maximum bandwidth for uploading traffic from Zyxel IPSec VPN clients over IPSec VPN tunnels.

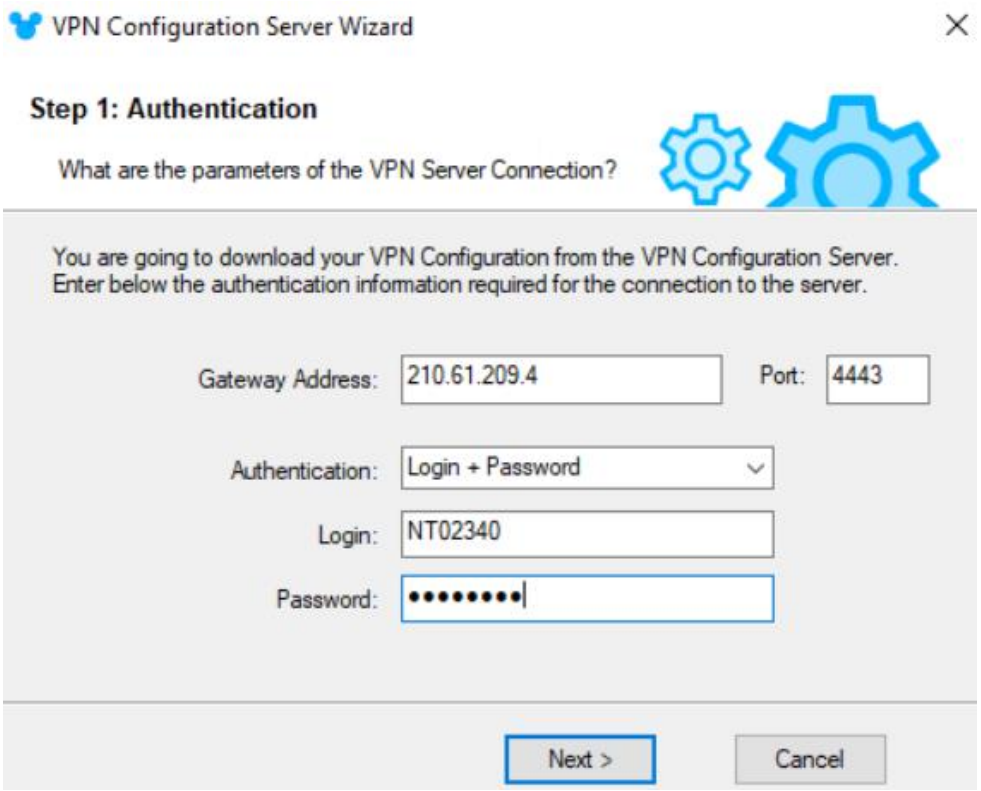


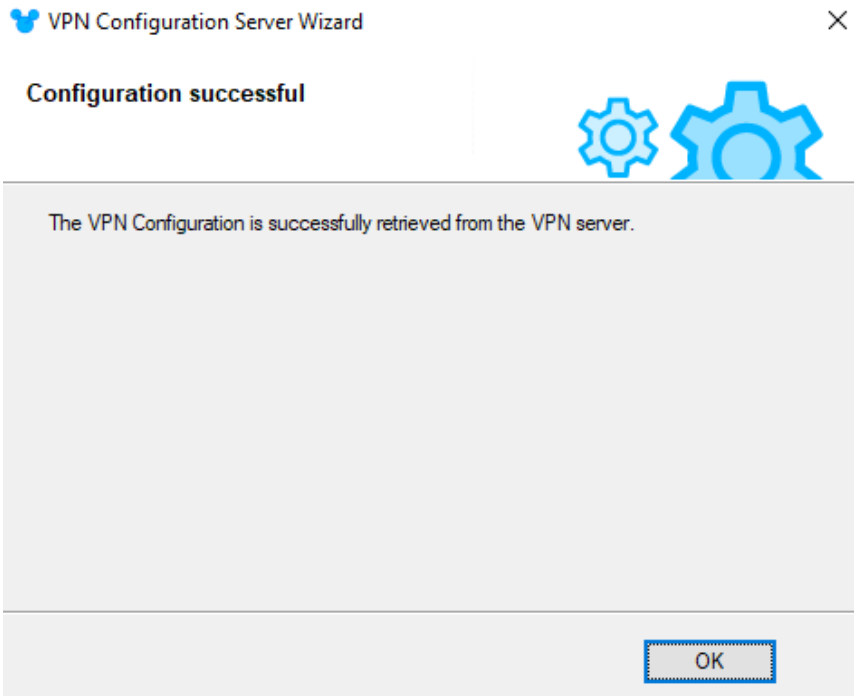
After completing VPN Wizard, if you want to modify the upload bandwidth limit, go to Configuration > VPN > IPSec VPN > Configuration Provisioning



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


ZyWALL IPSec VPN Client
Configuration
Tools
?
Save
Ctrl+S
Import
Export
Get from Server
Move to USB Drive
Wizard...
Quit
VPN CLIENT
VPN Configuration
VPN Configuration
VPN Configuration
Written by VpnConf 6.80
Last modification: 09-03-2021
VPN Client ready

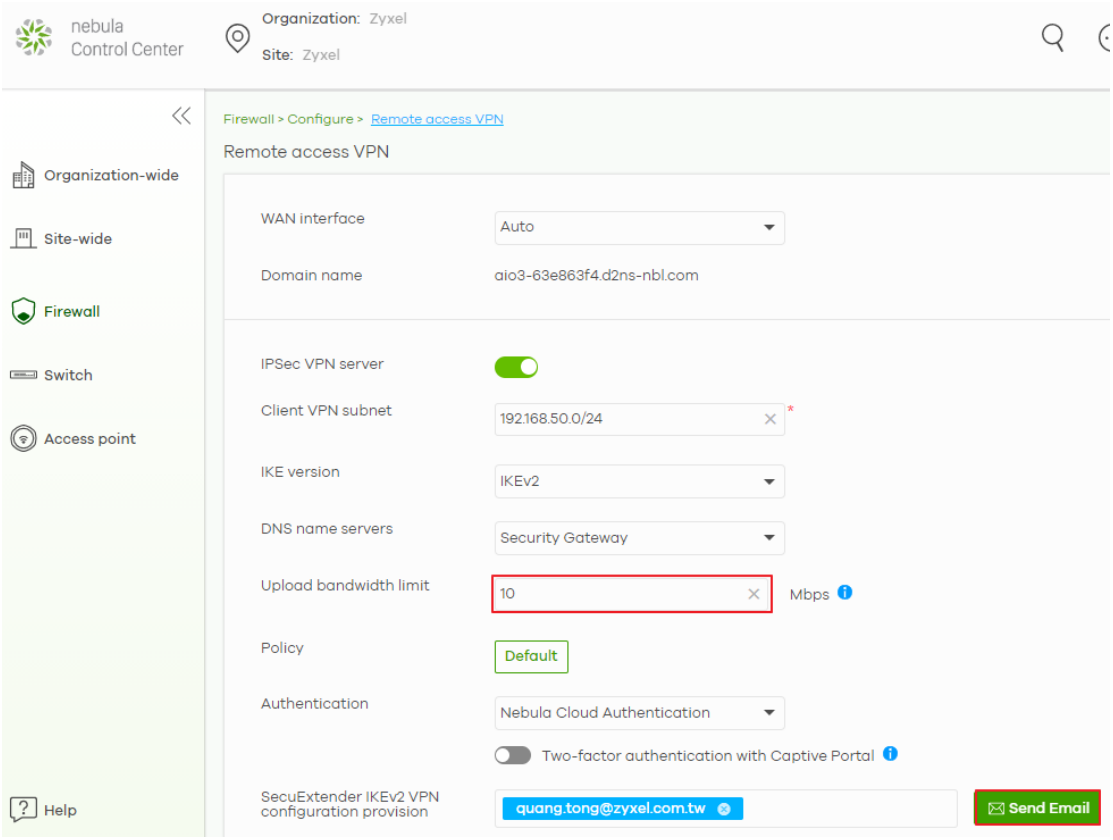

VPN Configuration Server Wizard
Step 1: Authentication
What are the parameters of the VPN Server Connection?
You are going to download your VPN Configuration from the VPN Configuration Server.
Enter below the authentication information required for the connection to the server.
Gateway Address:
210.61.209.4
Port:
4443
Authentication:
Login + Password
Login:
NT02340
Password:
Next >
Cancel


VPN Configuration Server Wizard
Configuration successful
The VPN Configuration is successfully retrieved from the VPN server.
OK

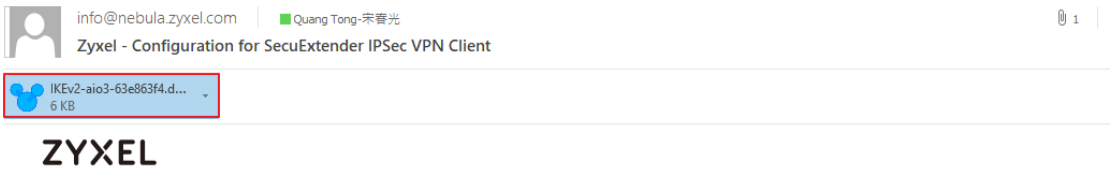
Nebula Mode

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



The VPN configuration file will be emailed to you.



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

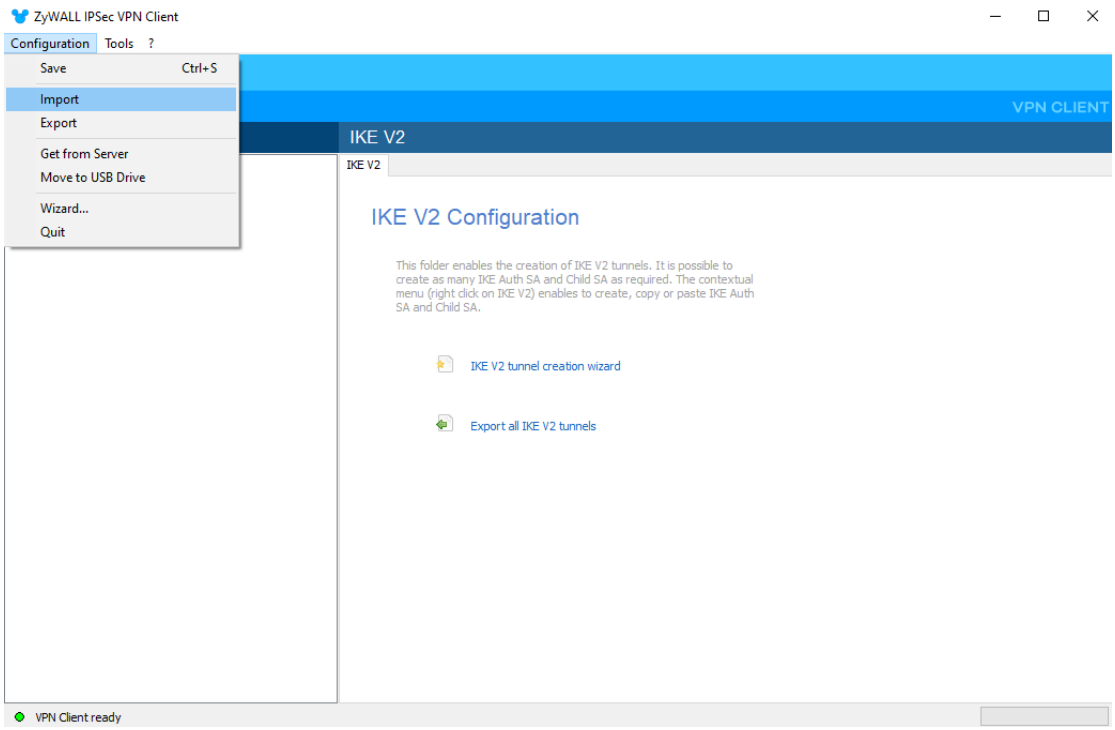
Then, follow the guide to import configuration.
1. Save the attached configuration file(.tgb) to your laptop
2. Open SecuExtender VPN Client, from the "Configuration" menu in the Configuration Panel, choose "Import".
   An "open" file dialog opened, then browser and select the saved configuration file(.tgb) 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



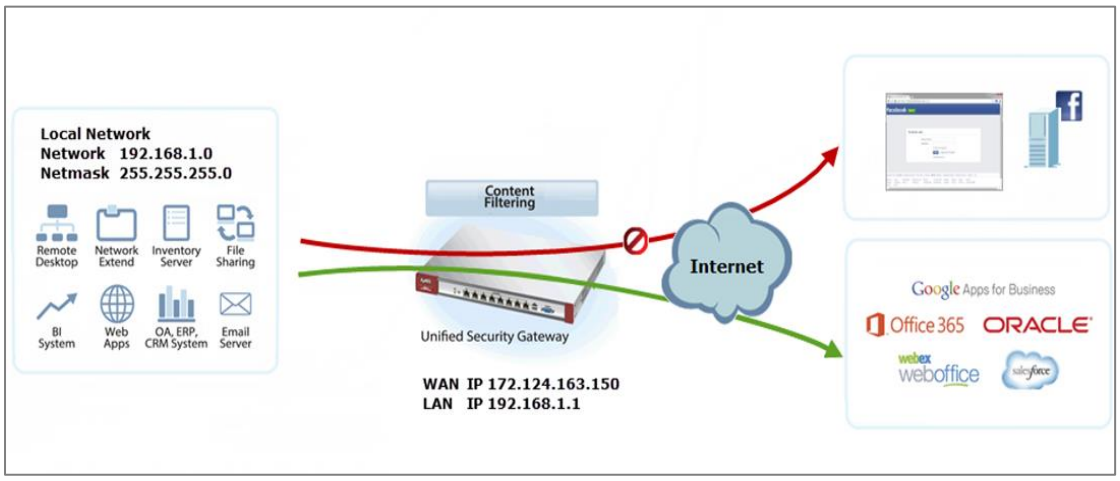
Chapter 2- Security Service

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.

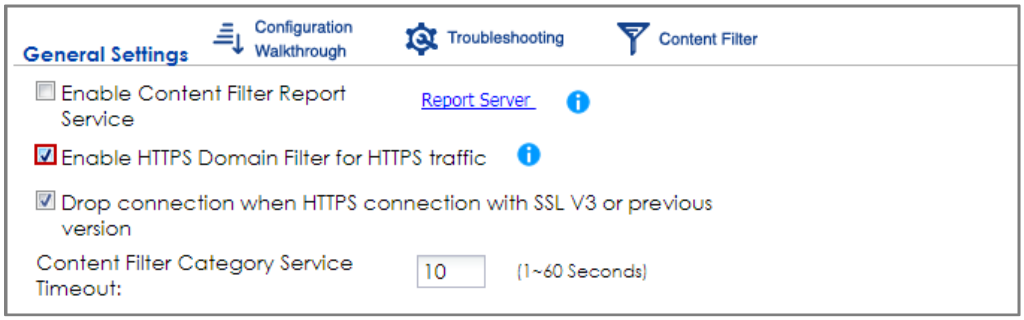
ZyWALL/USG Domain Filter Example



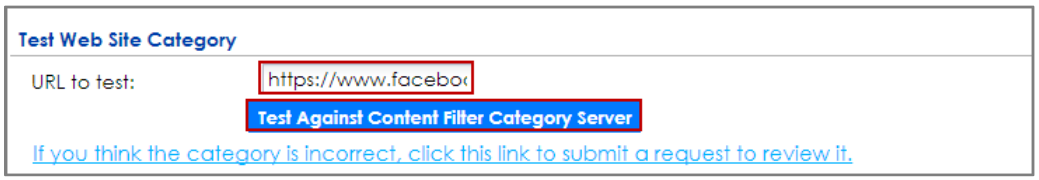
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25)

Set Up the Content Filter on the ZyWALL/USG

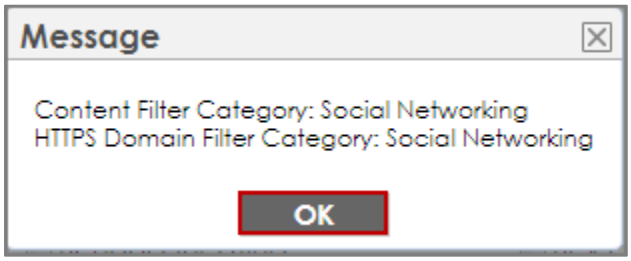
Go to **CONFIGURATION > UTM Profile> Content Filter > Profile > General Settings**. Select **Enable HTTPS Domain Filter for HTTPS traffic.**



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.**

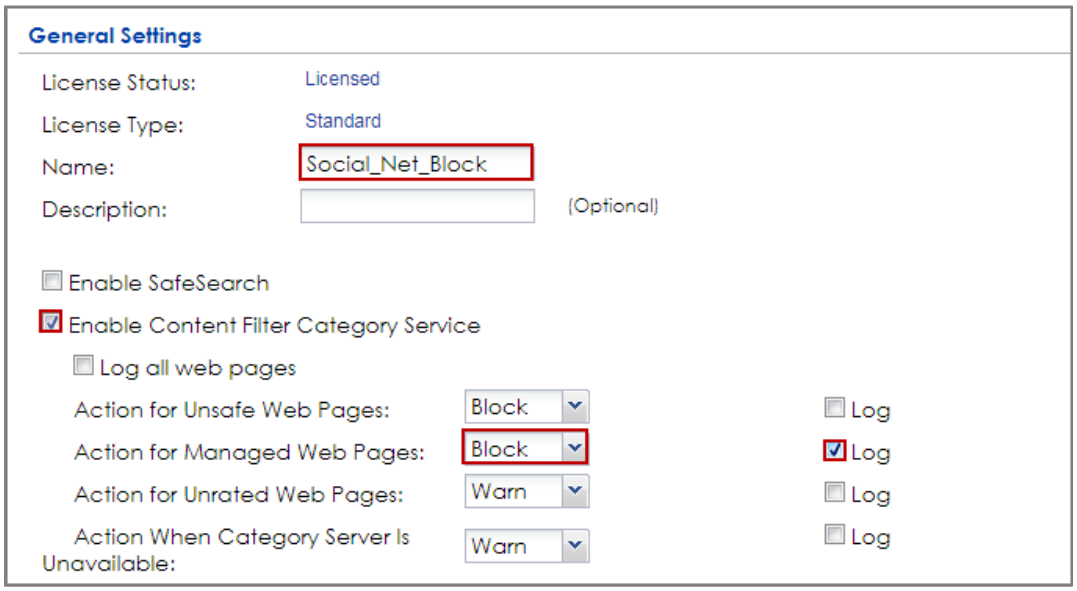


You will see the category recorded in the external content filter server's database for both HTTP and HTTPS Domain you specified.



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

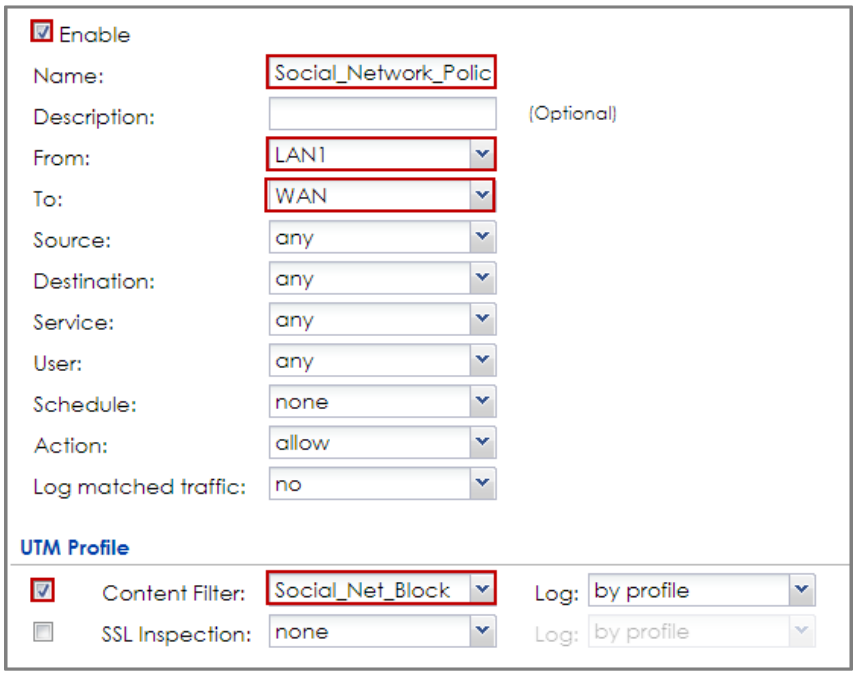
accessing web pages that match the managed categories that you select below. Select **Log** to record attempts to access web pages that match the unsafe categories that you select below.



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.

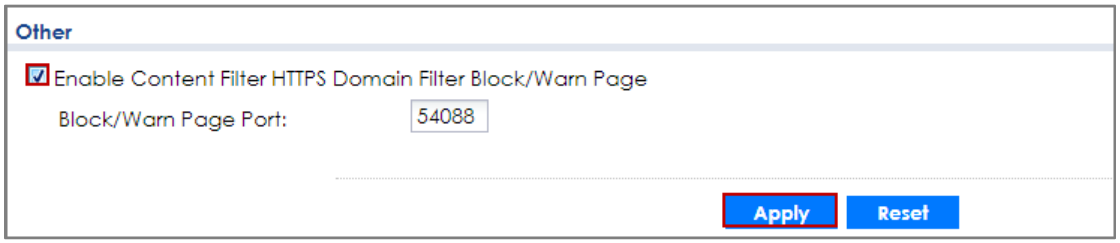
Set Up the Security Policy on the ZyWALL/USG

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).



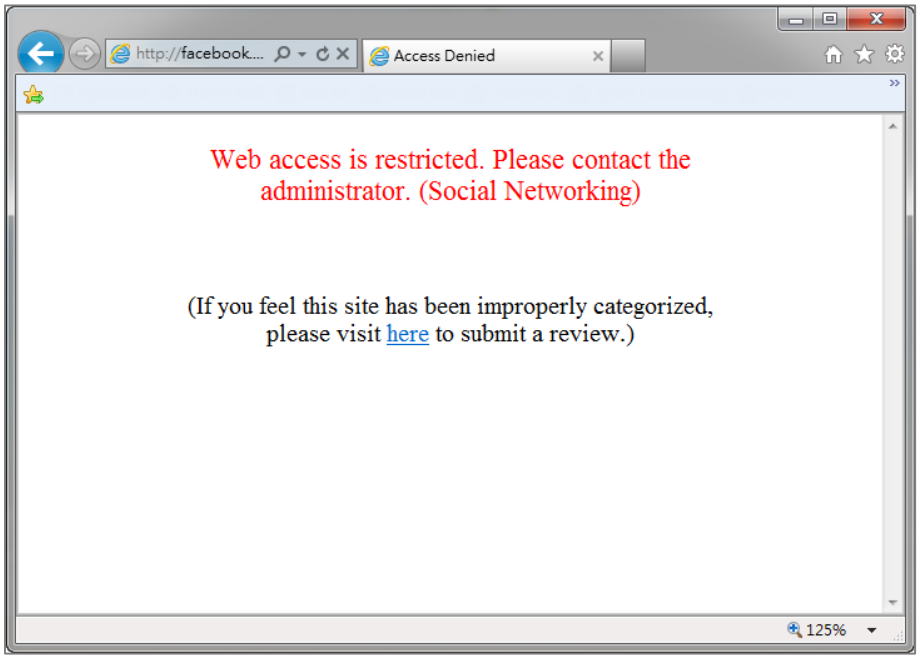
Set Up the System Policy on the ZyWALL/USG

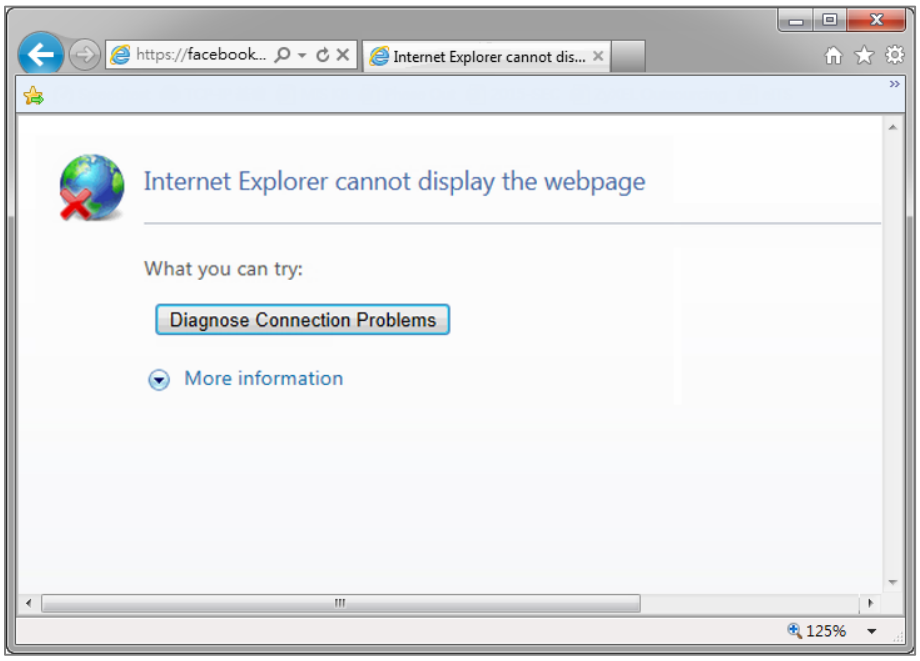
Go to **CONFIGURATION > System > WWW > Show Advanced Settings > Other**, click **Enable Content Filter HTTPS Domain Filter Block/Warn Page**.



Test the Result

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





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

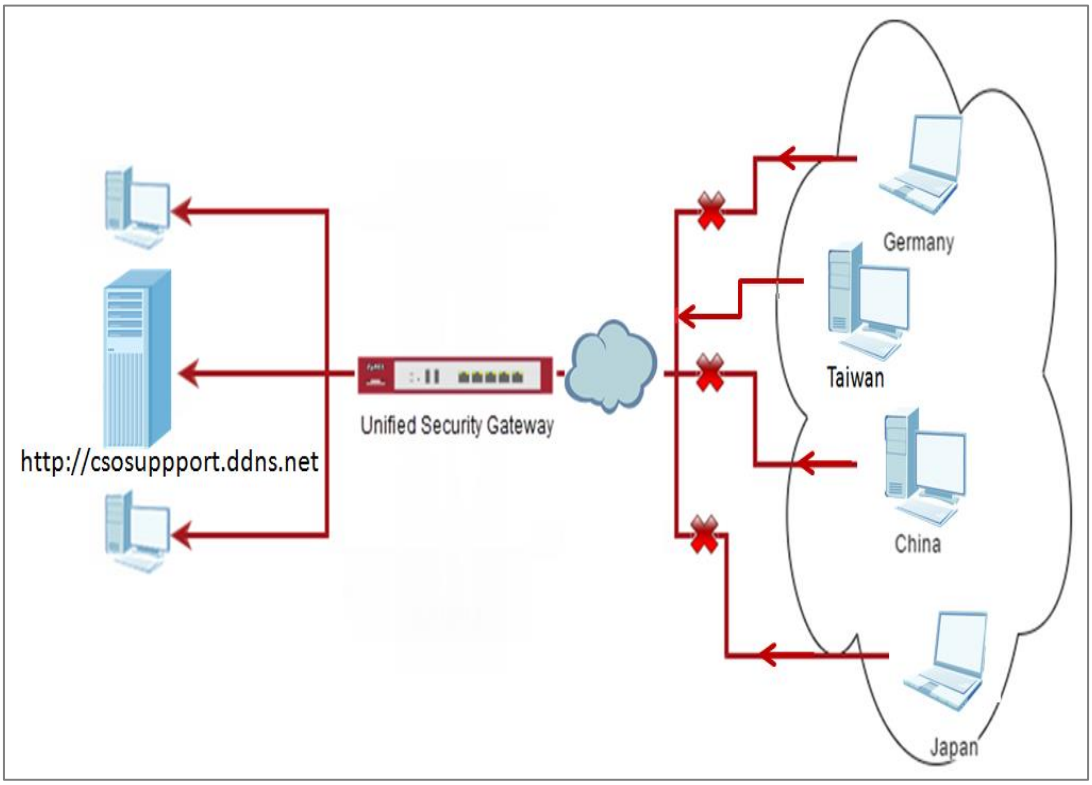
How to Configure Content Filter 2.0 with Geo IP Blocking

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.

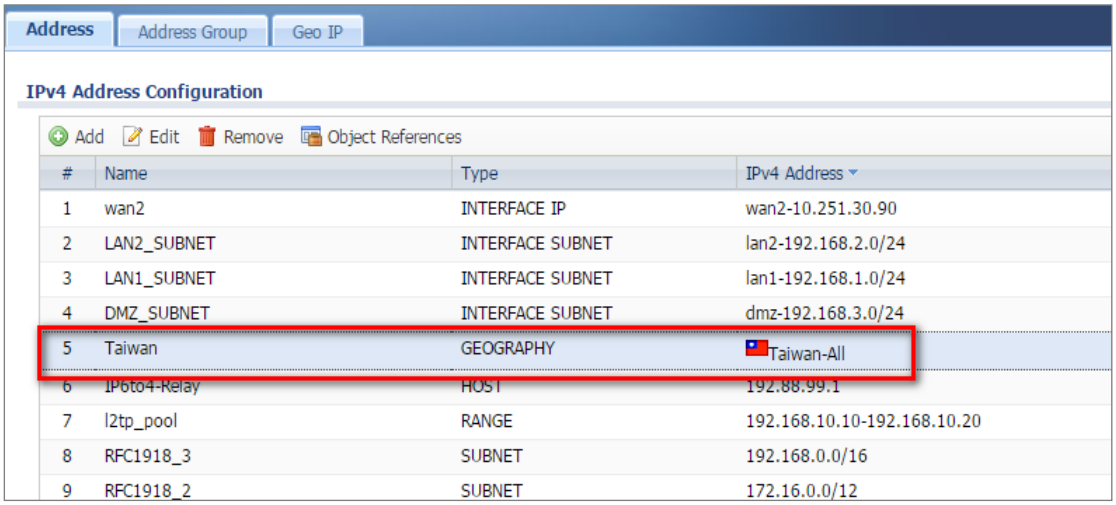
Also this feature offer an easy and effective way to prevent bogus, bots, brute force hacks, vulnerability scanners, and web crawlers from other countries.



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

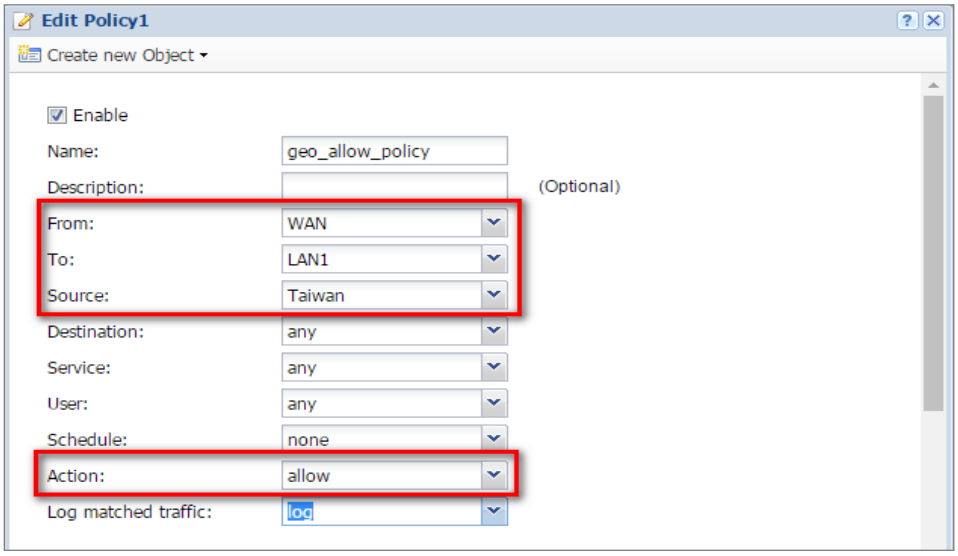
Go to **CONFIGURATION > Object > Address/Geo IP > Address > Add Address Rule**.

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

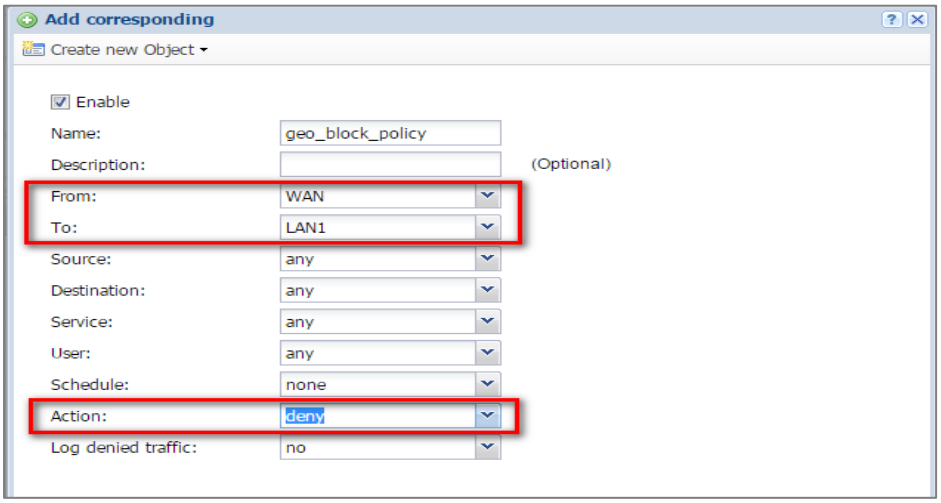


Set Up the Security Policy on the ZyWALL/USG

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).

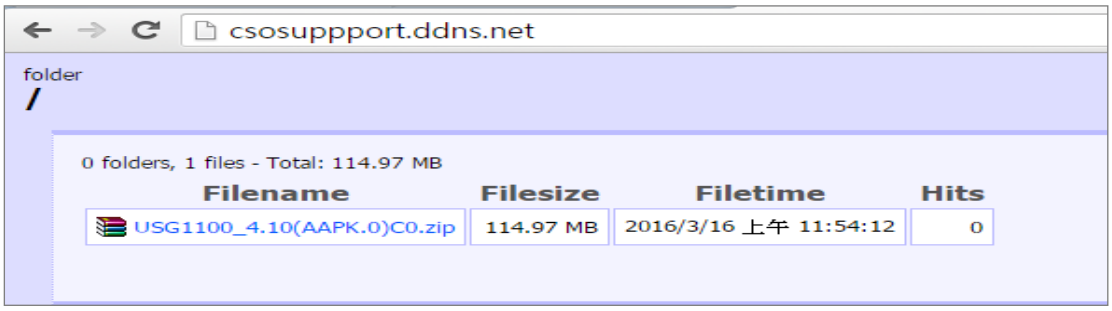


Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set traffic from WAN to LAN deny (geo_block_policy in this example).

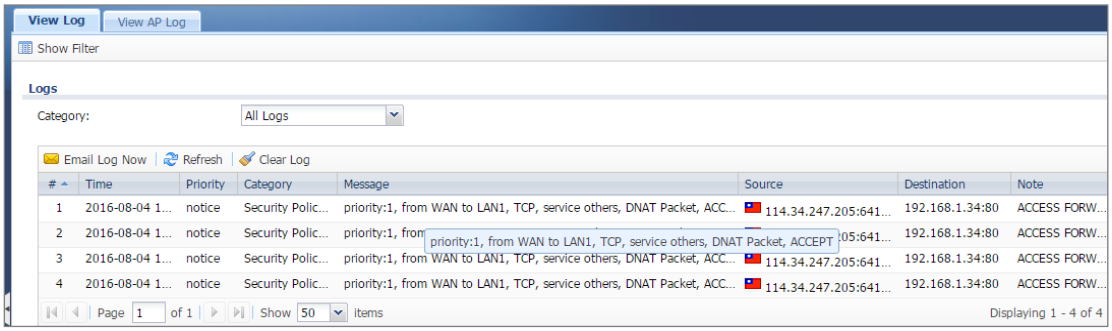


Test the Result

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

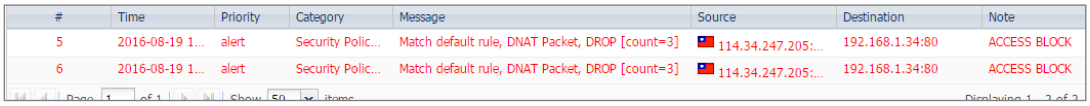


Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] log message such as below. Traffic matches Geo IP policy will be blocked and shows in message field.



What Could Go Wrong?

1. The Security Policy configured wrong. The traffic cannot access the LAN server.



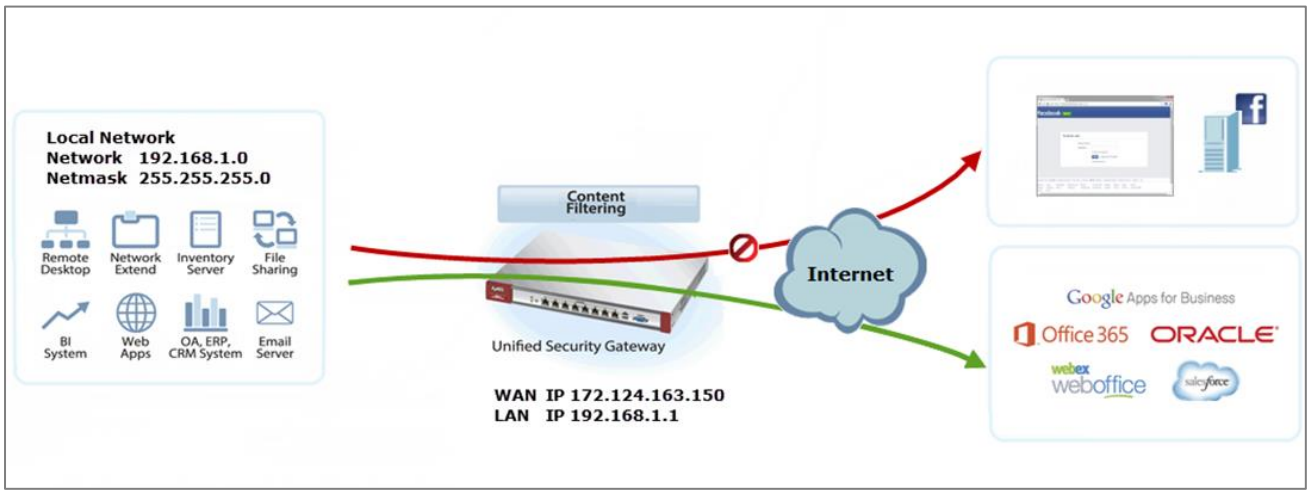
2. The Content-Filter service ix expired. Since Geo-IP server is bind with Content-Filter license, there must be available date for Content-Filter service.

How to Configure Content Filter 2.0 with HTTPs Domain Filter

Application Scenario

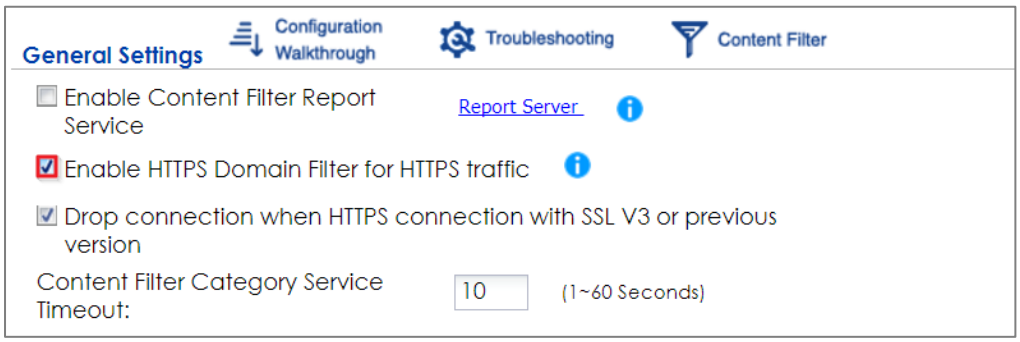
The Content Filter with HTTPs Domain Filter allows you to block HTTPs websites by category service without SSL-Inspection. The filtering feature is based on 64 categories built in ZyWALL/USG such as pornography, gambling, hacking, etc.

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

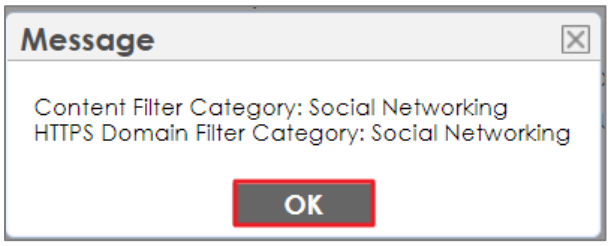
Go to **CONFIGURATION > UTM Profile> Content Filter > Profile > General Settings**. Select **Enable HTTPS Domain Filter for HTTPS traffic.**



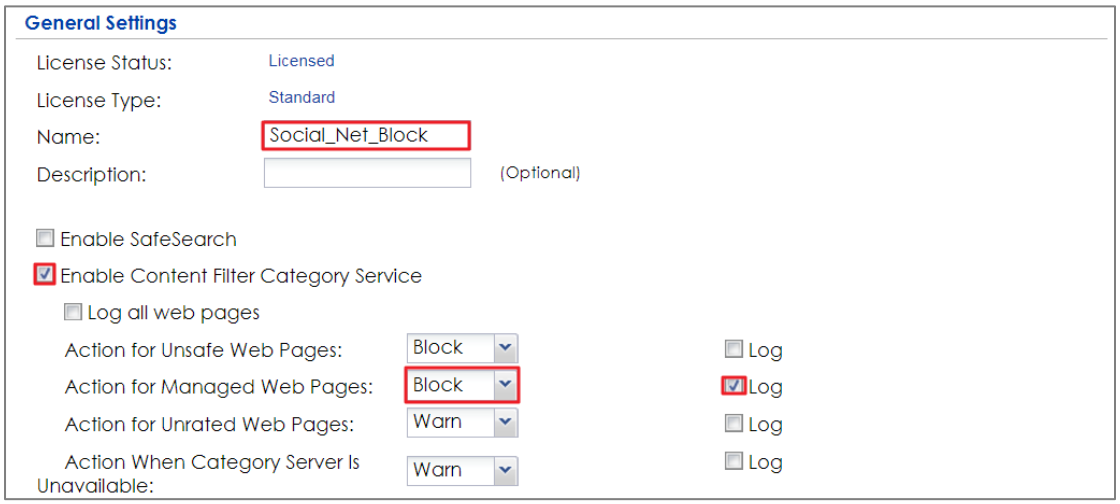
Go to **CONFIGURATION > UTM Profile> Content Filter > Profile Management > Add Filter**

Profile > Test Web Site Category. Type URL to test the category and click **Test Against Content Filter Category Server.**

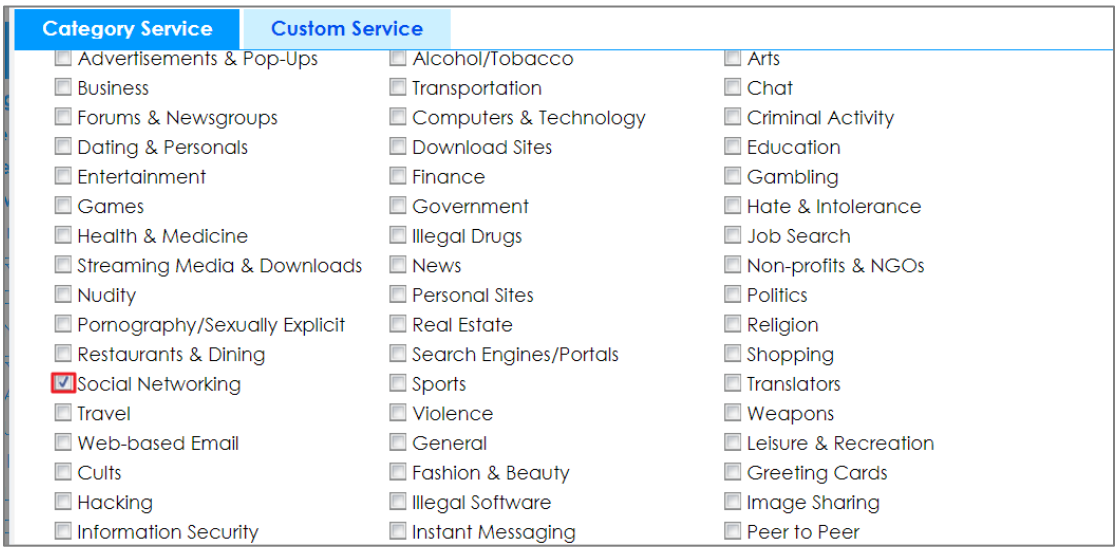
You will see the category recorded in the external content filter server's database for both HTTP and HTTPS Domain you specified.



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.

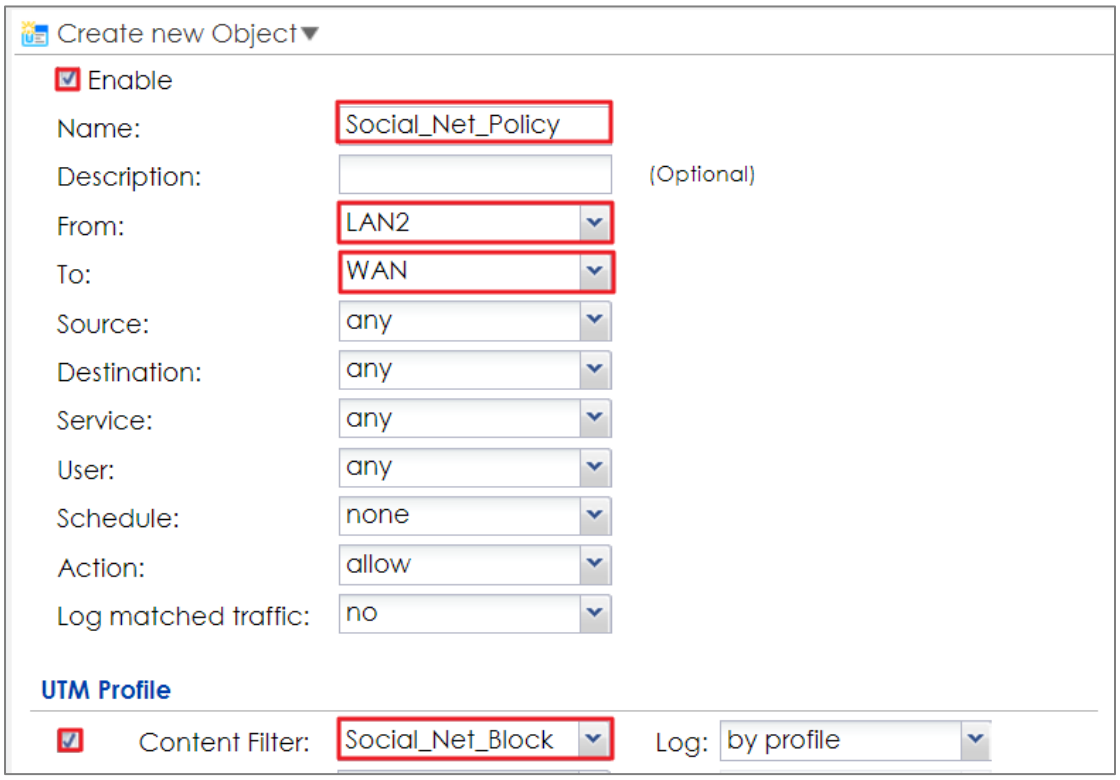


Scroll down to the **Managed Categories** section, select categories in this section to control access to specific types of Internet content. You must have the Content Filtering license to filter these categories.



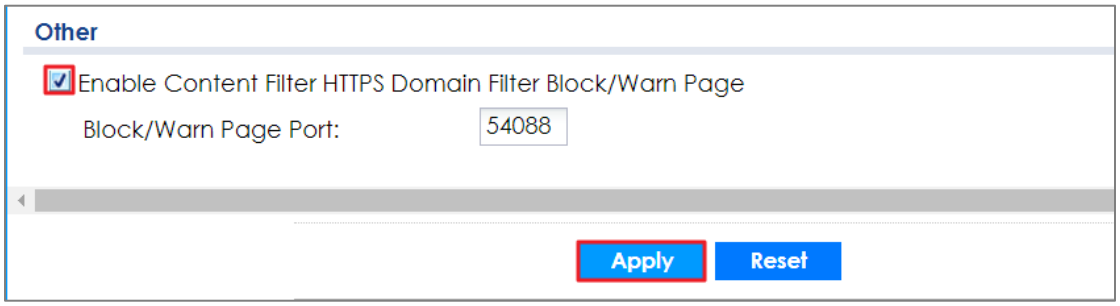
Set Up the Security Policy on the ZyWALL/USG

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).



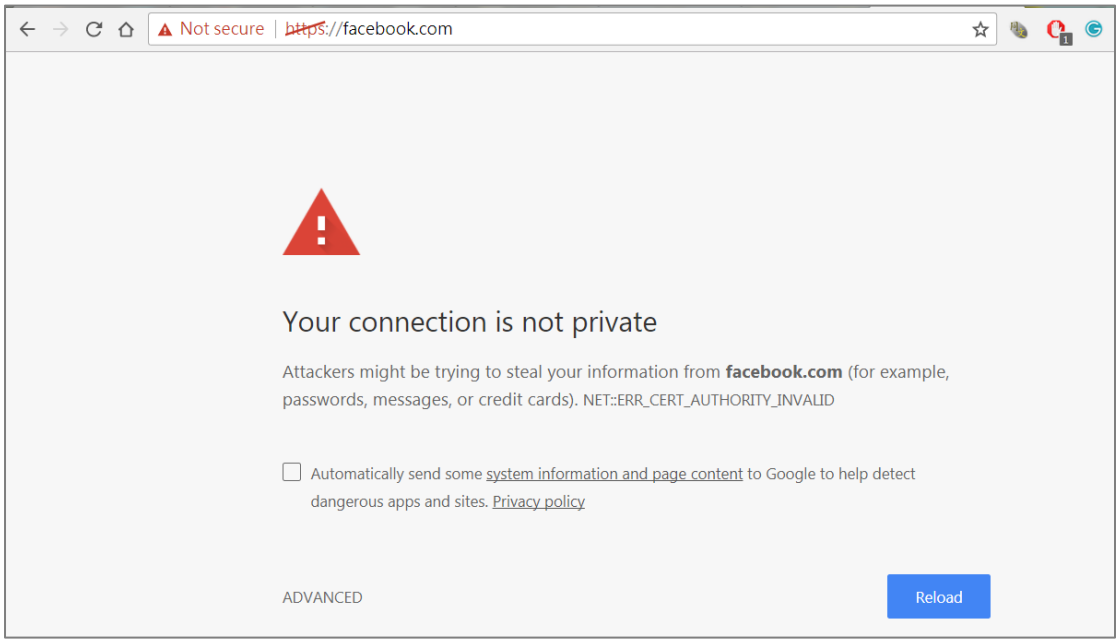
Set Up the System Policy on the ZyWALL/USG

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



Test the Result

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



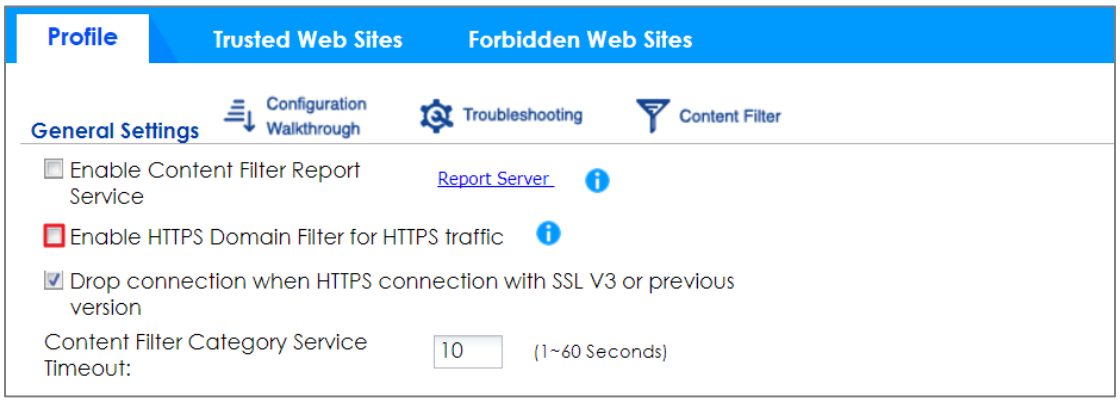
Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below. HTTP traffic log matches (Content Filter) and HTTPS traffic log matches (HTTPS Domain Filter) in message field.

Monitor > Log

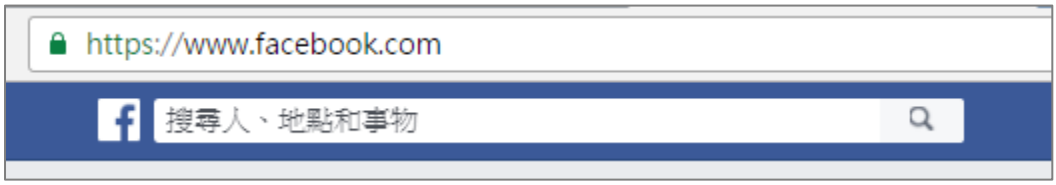
#	Time	Pri...	Category	Message	Source	Desti...	Note
28	20...	alert	Blocked w...	facebook.com : Social Networking, Rule_id=1, SSI=N (HTTPS Domain...	192.168.2.3...	31...	WEB BLOCK
29	20...	alert	Blocked w...	facebook.com : Social Networking, Rule_id=1, SSI=N (HTTPS Domain...	192.168.2.3...	31...	WEB BLOCK
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.



HTTPs traffic will pass.

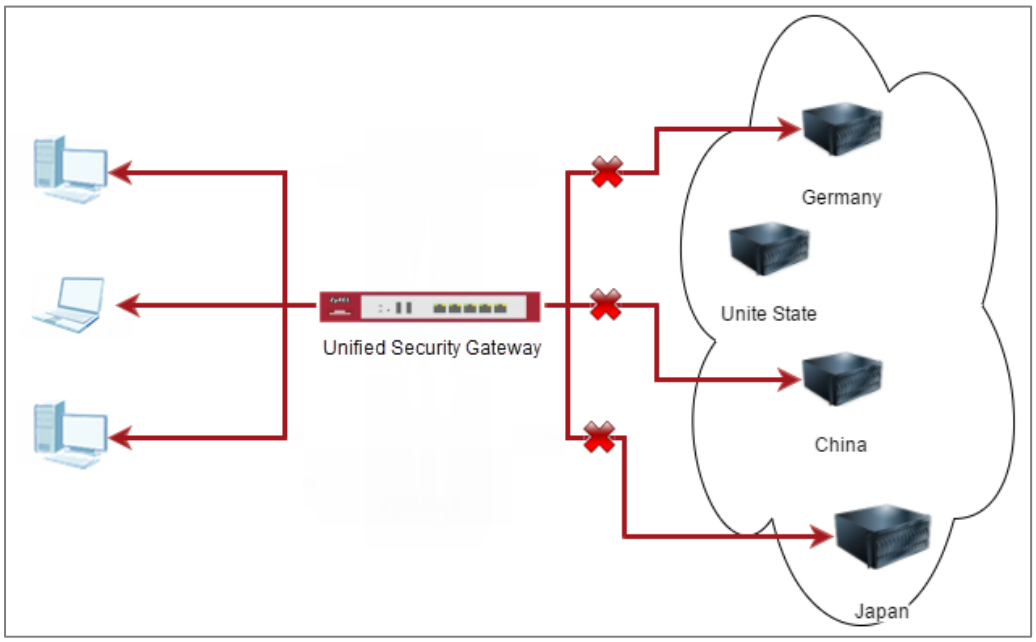


How to block the client accessing to certain country using Geo IP and Content Filter

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

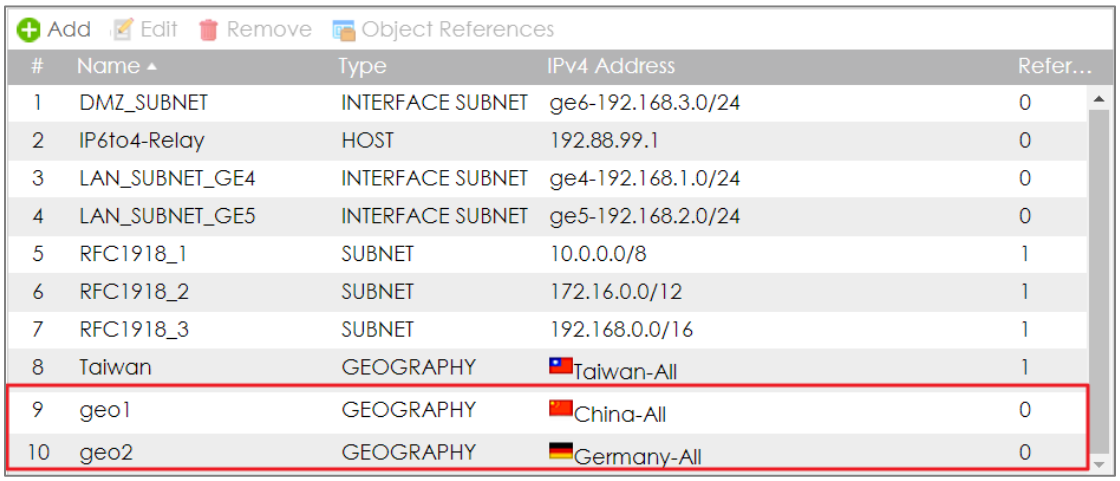
Go to **CONFIGURATION > Licensing > Registration > Service**, the **Geo IP Service** should be **Licensed** to configure this feature.

#	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

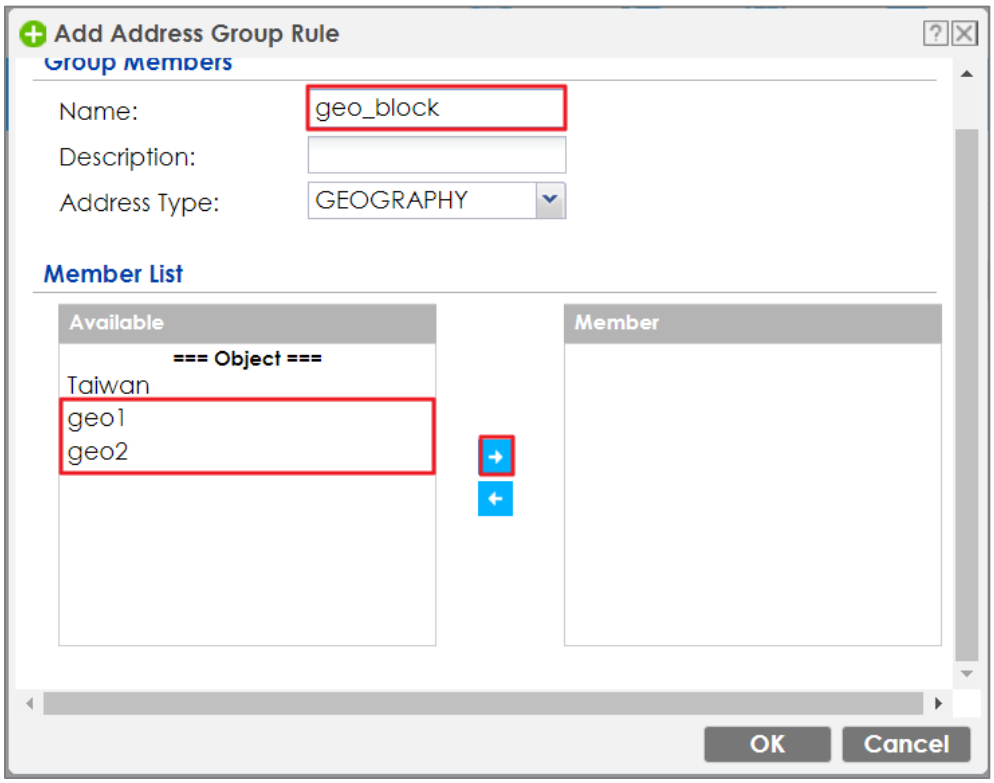
Set Up the Address Objet with Geo IP on the ZyWALL/USG

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

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



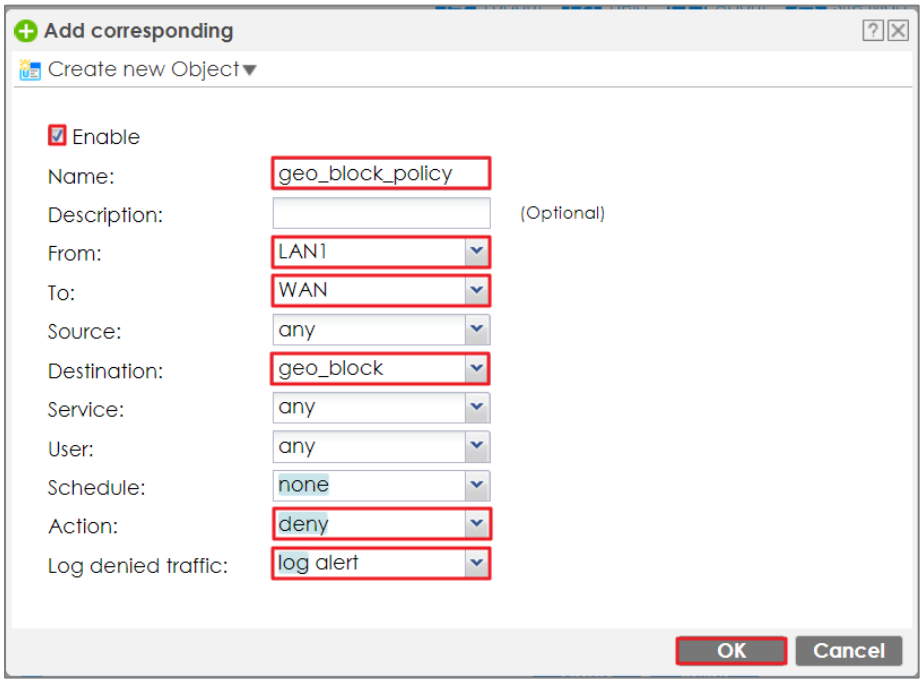
Go to **CONFIGURATION > Object > Address/Geo IP > Address Group> Add Address Group Rule**, add all customized GEOGRAPHY address into the same **Member** object.



Set Up the Security Policy on the ZyWALL/USG

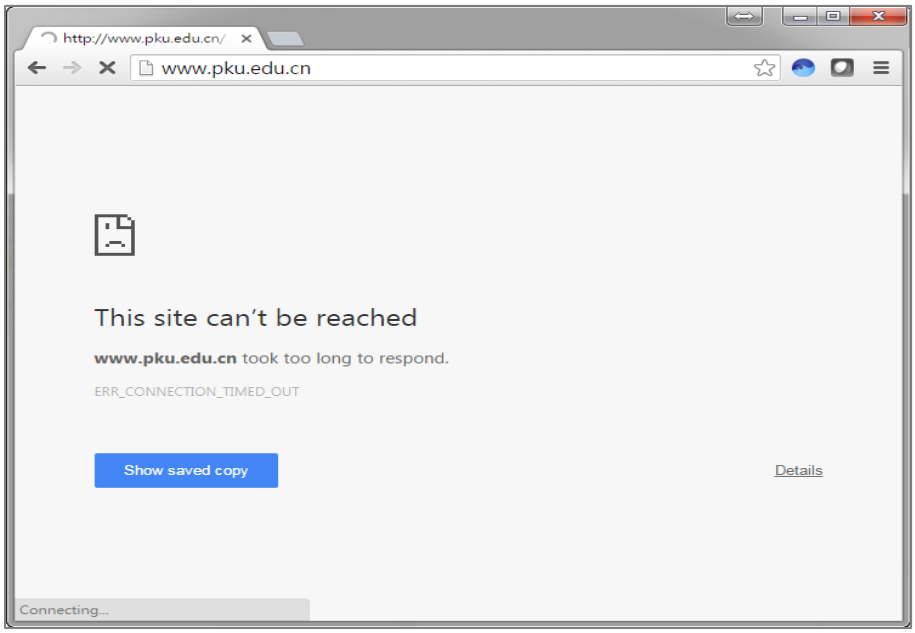
Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set deny Geo IP traffic from LAN to WAN

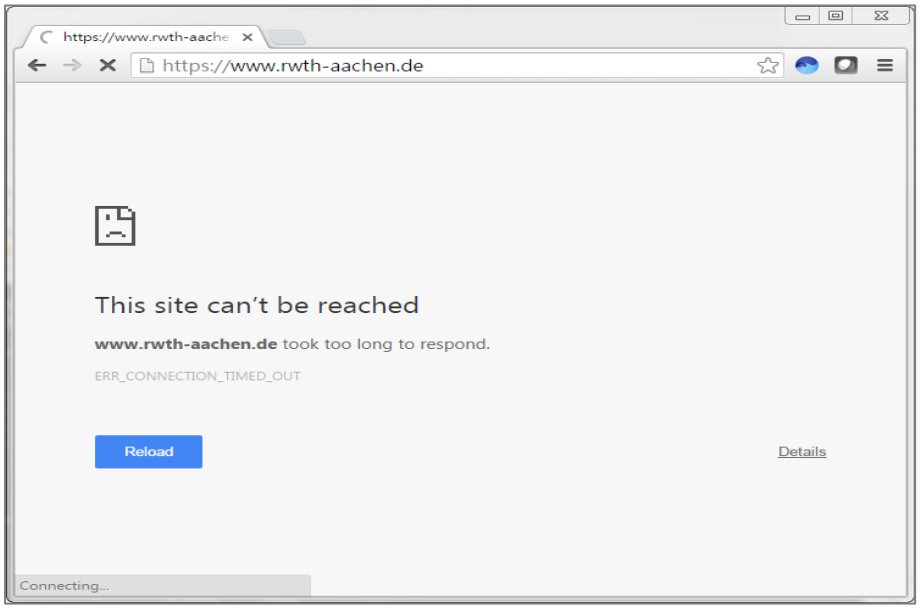
(geo_block_policy in this example).



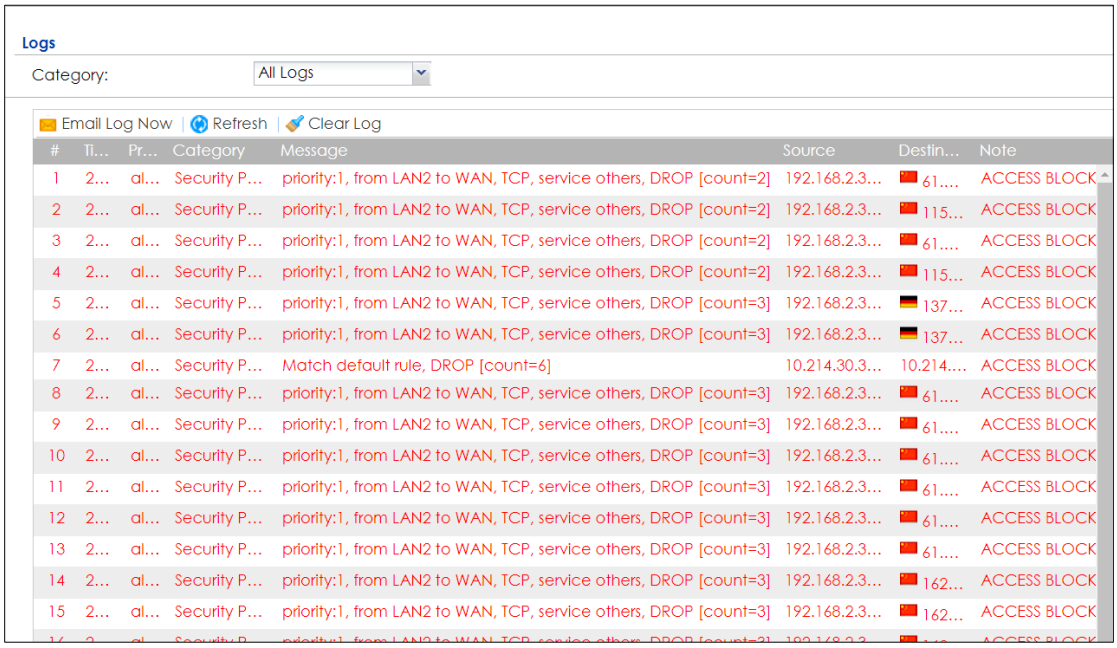
Test the Result

Type http://www.pku.edu.cn/ or https://www.rwth-aachen.de/ into the browser, sites can't be reached.



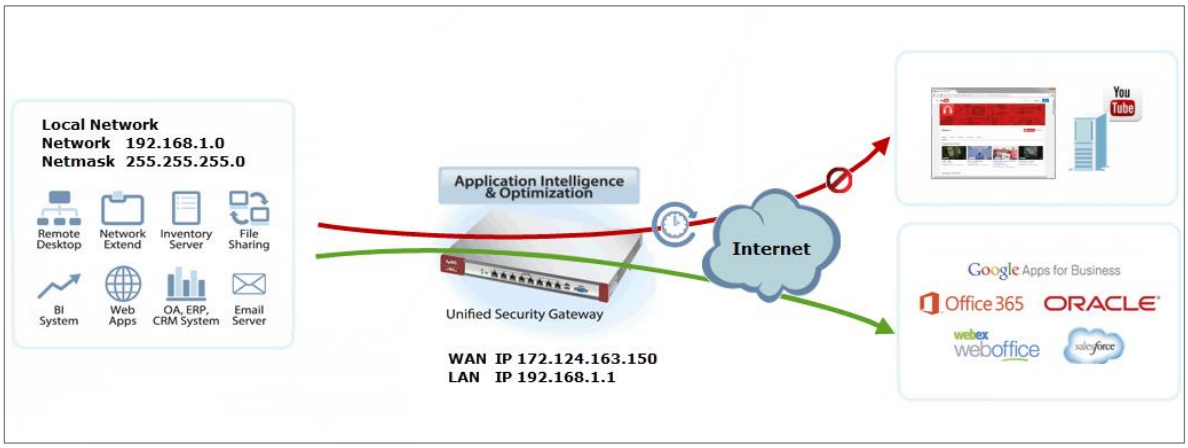


Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] log message such as below. Traffic matches Geo IP policy will be blocked and shows in message field.



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.



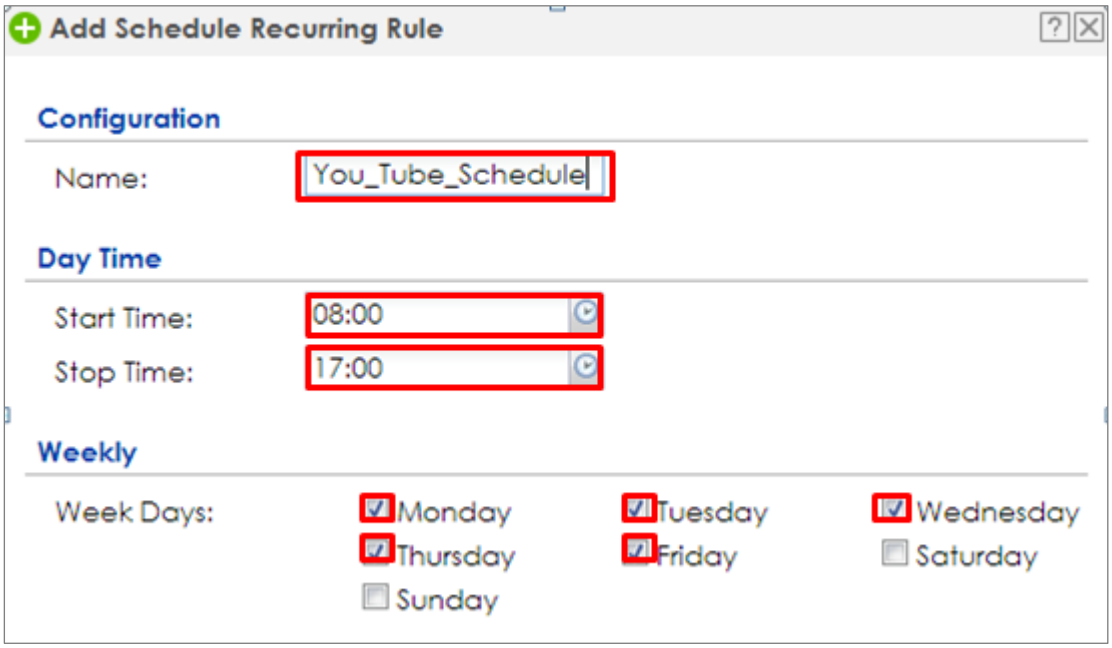
ZyWALL/USG with Scheduled YouTube Access Settings Example

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



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

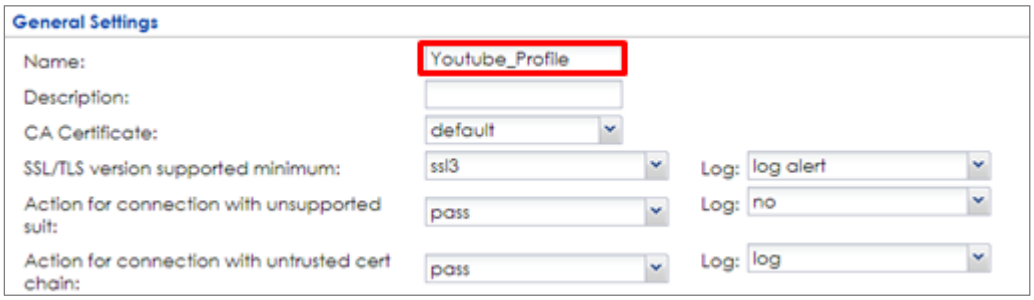
Set Up SSL Inspection on the ZyWALL/USG

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

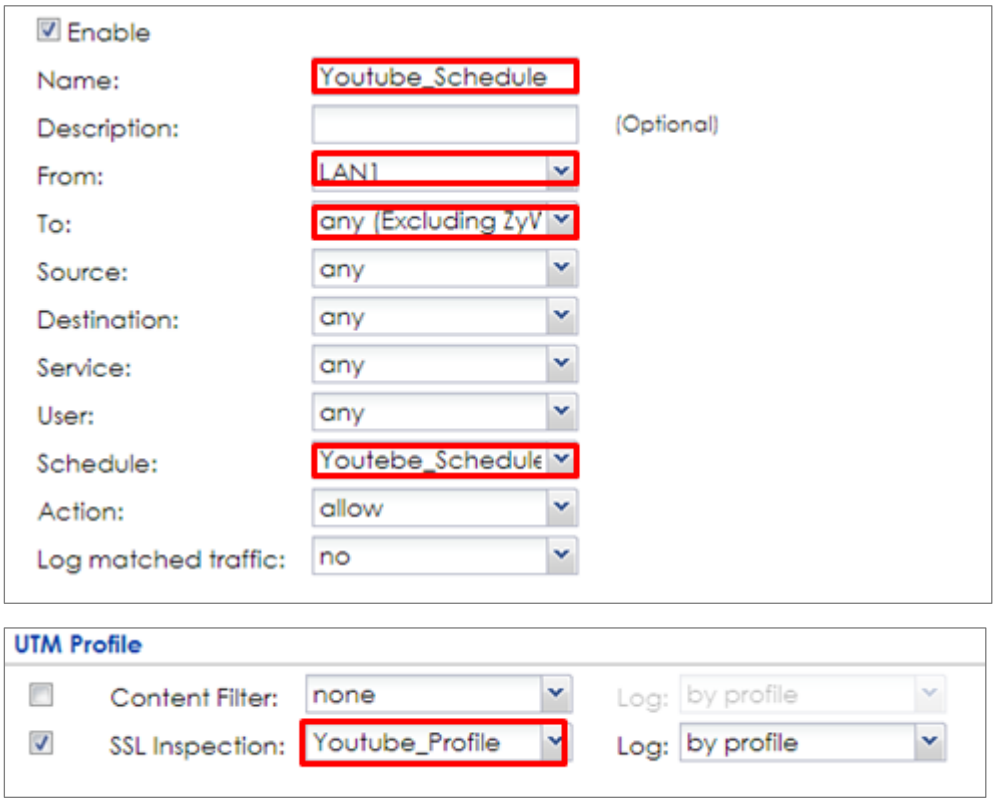


Set Up the Security Policy on the ZyWALL/USG

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

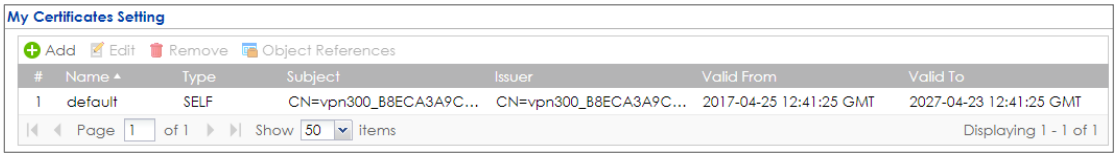


Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

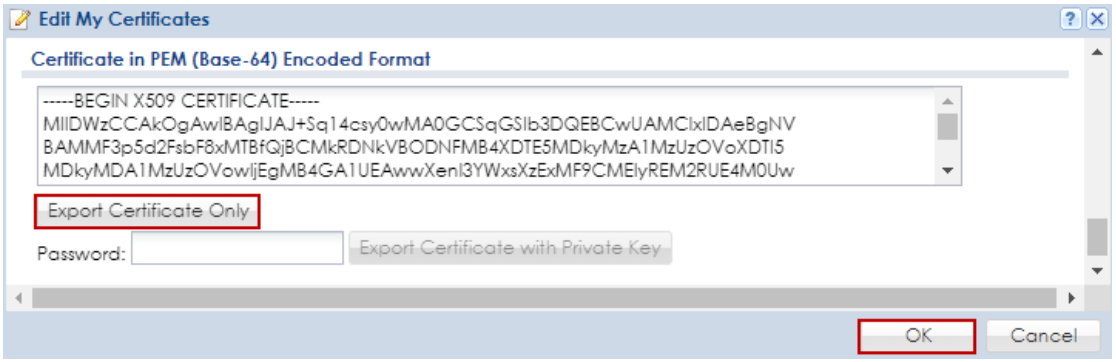
When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG.

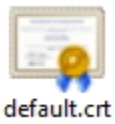
CONFIGURATION > Object > Certificate > default



CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only

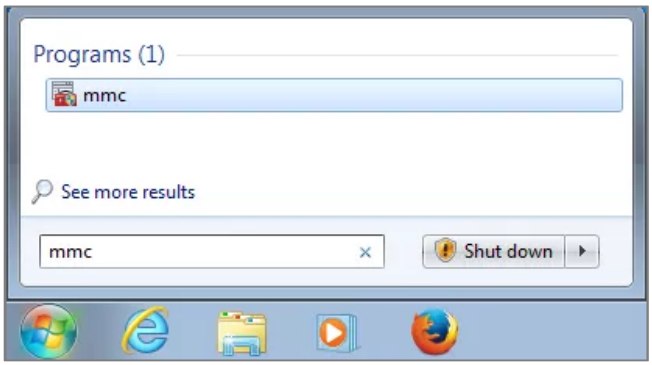


Save default certificate as *crt file to Windows 7 Operation System.



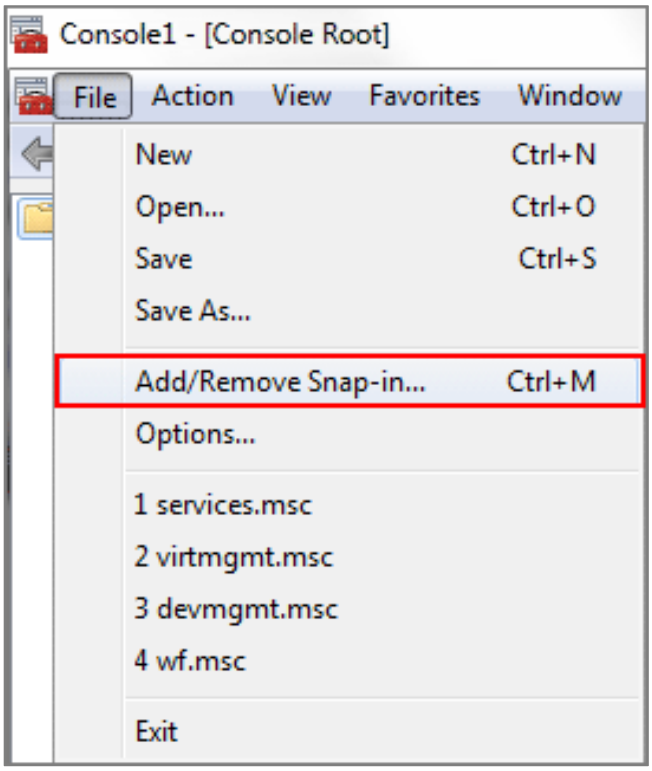
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



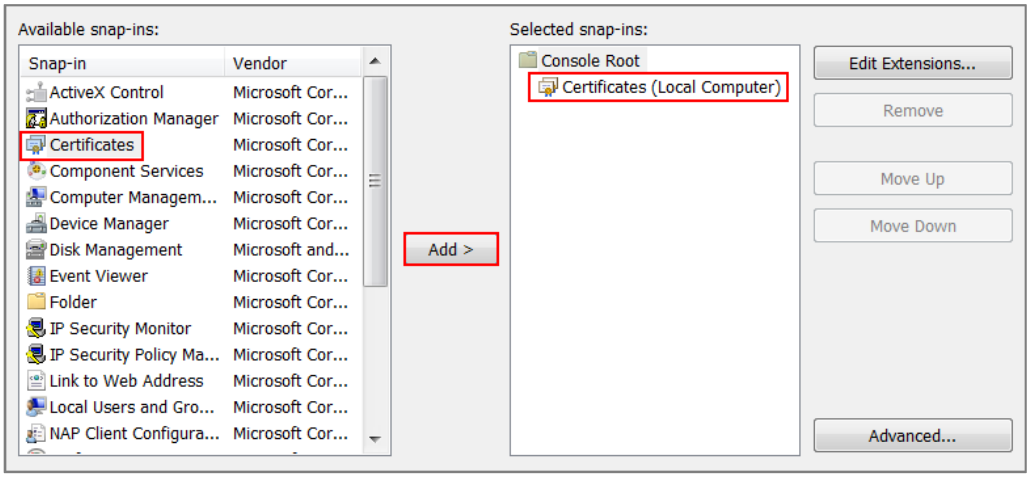
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

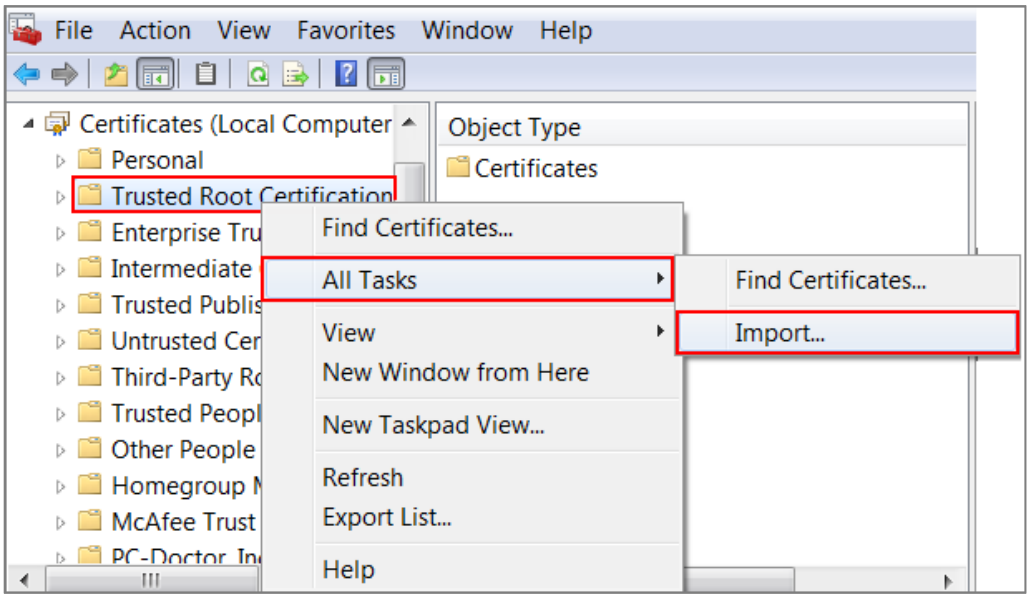


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

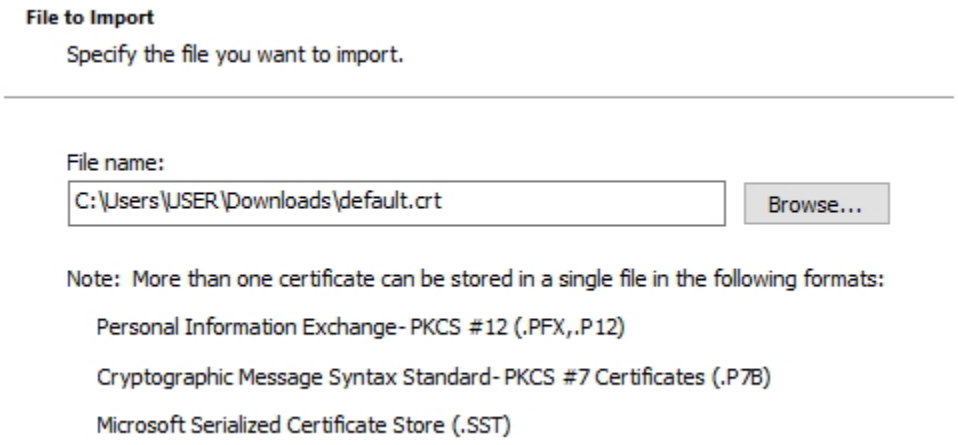
Available snap-ins > Certificates > Add



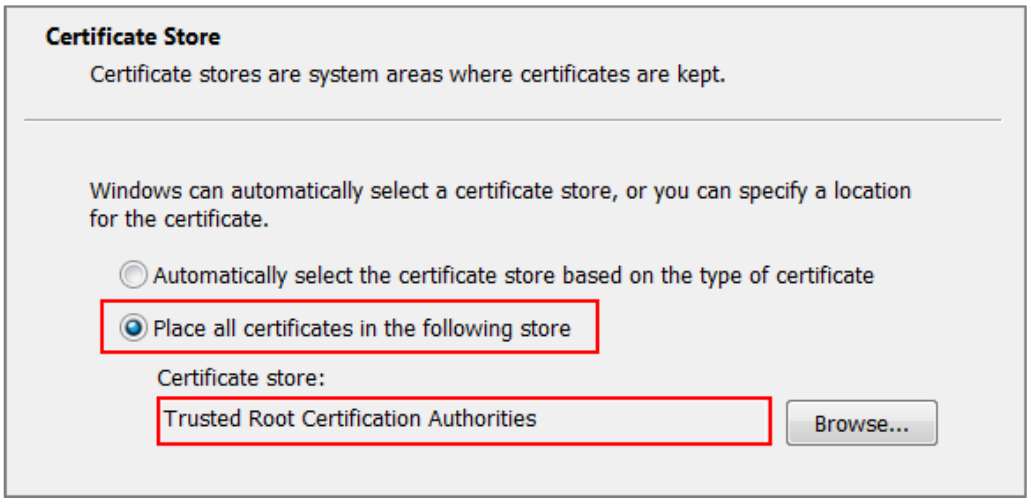
In the mmc console window, open the **Certificates (Local Computer) > Trusted Root Certification Authorities,** right click **Certificate > All Tasks > Import…**



Click **Next,** Then, **Browse...,** and locate the .crt file you downloaded earlier. Then, click **Next**.



Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities.** Click **Next**, then click **Finish**.

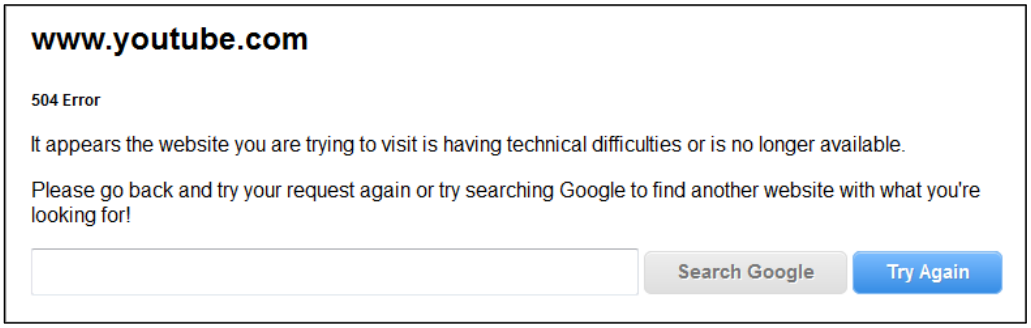


Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to the default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Test the Result

Type http://www.youtube.com/ or https://www.youtube.com/ into the browser.

An error message occurs.



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.

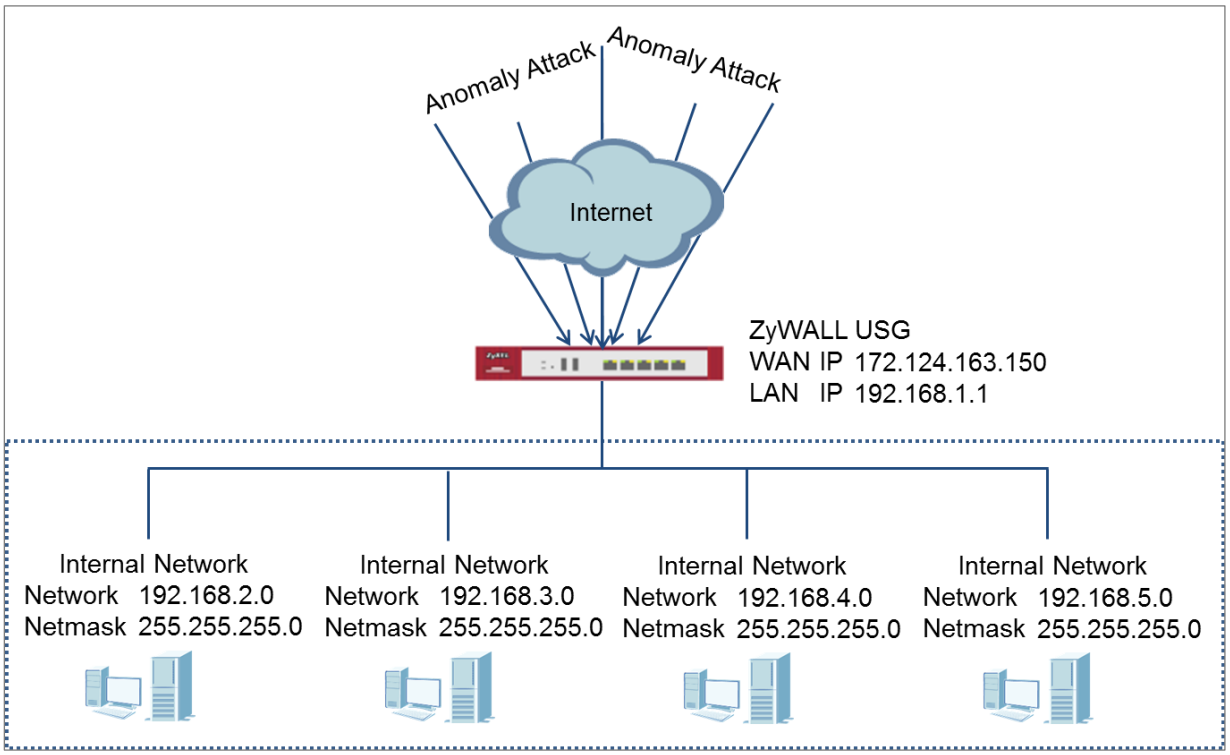
You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **Application Patrol** license.

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

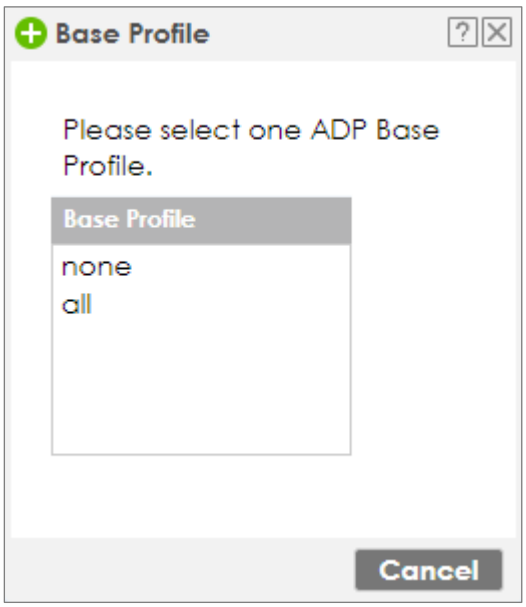


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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



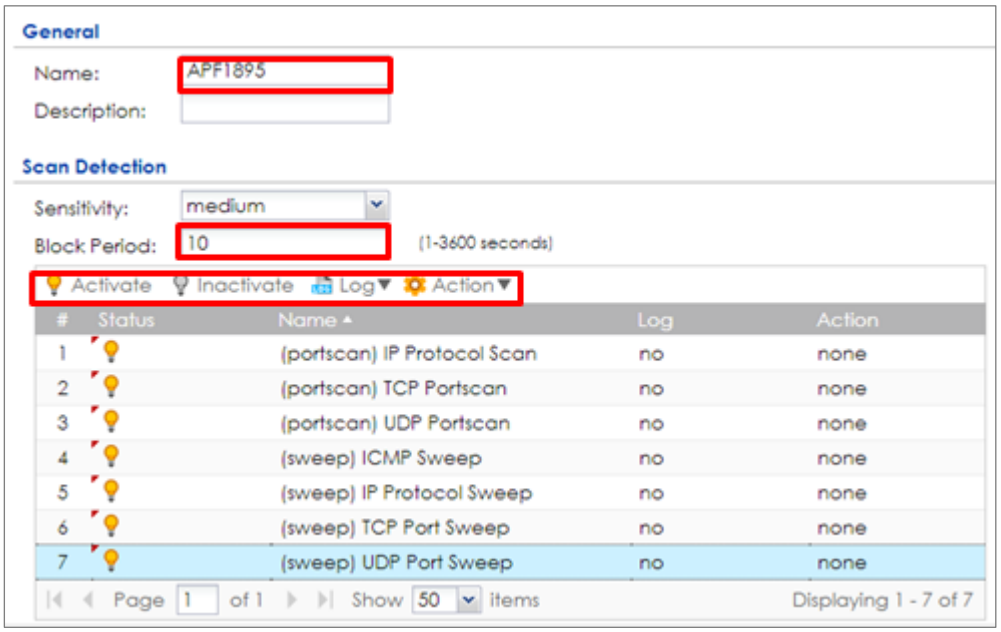
The **Traffic Anomaly** screen will display. A **Name** is automatically generated that you can edit. Enable or disable individual scan or flood types by selecting a row and clicking **Activate** or **Inactivate**.

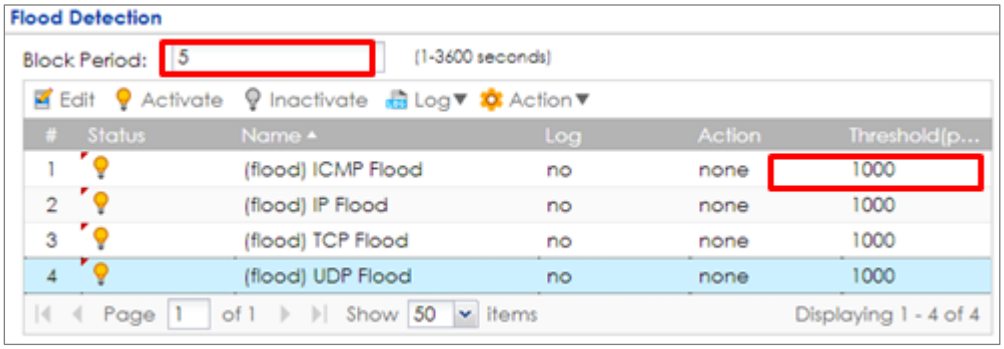
In the **Scan Detection** section, selecting levels in the **Sensitivity** drop-down menu and set **Block Period** for the duration applies blocking to the source IP address.

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**.

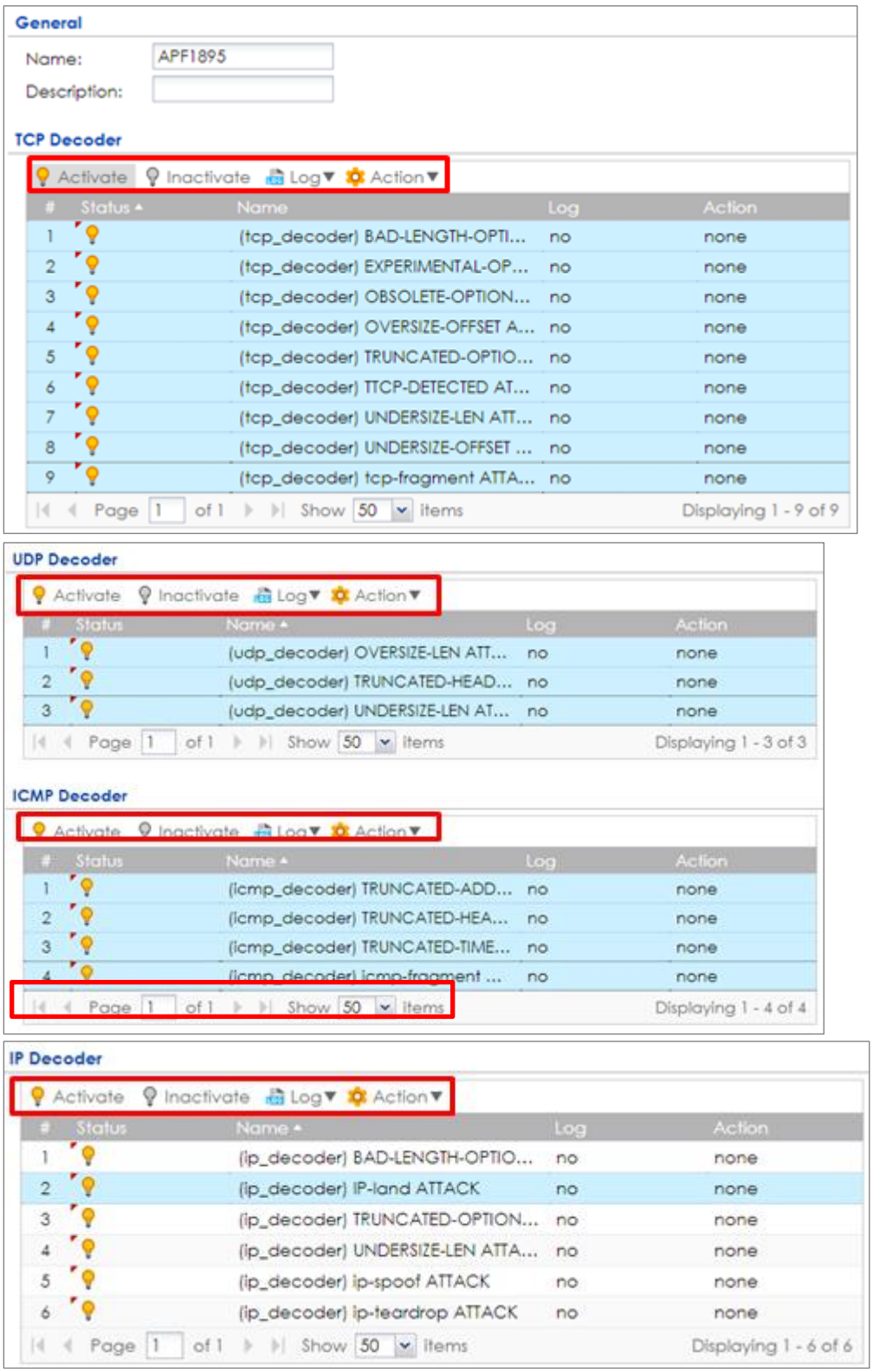
CONFIGURATION > Security Policy > ADP > Profile > Base Profile > Traffic Anomaly





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**.

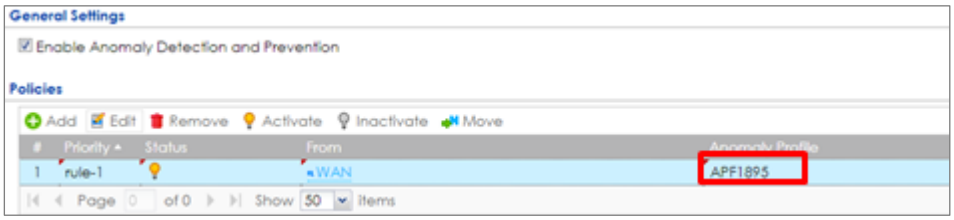
CONFIGURATION > Security Policy > ADP > Profile > Base Profile > Protocol Anomaly



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

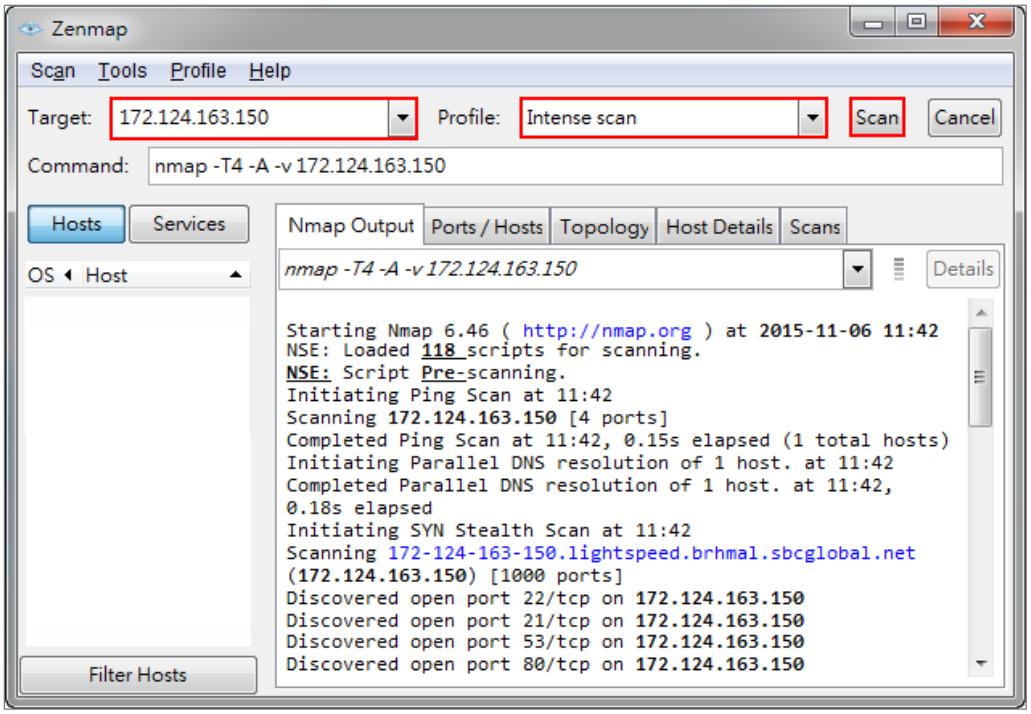


Test the Result

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**.



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

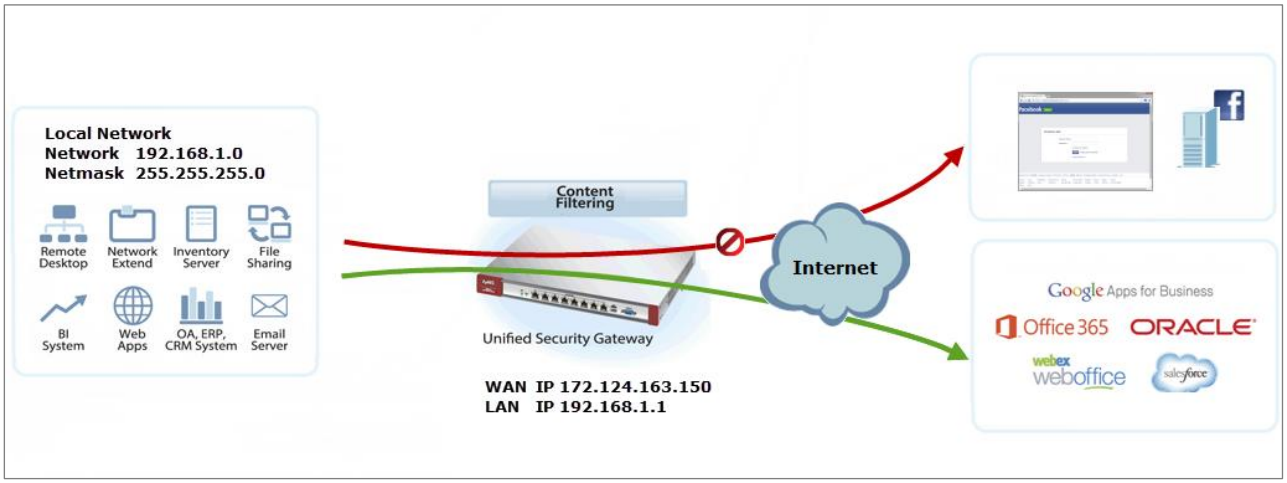
What Could Go Wrong?

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).

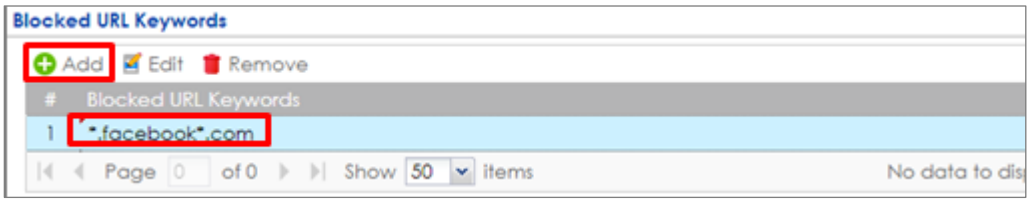
Set Up the Content Filter on the ZyWALL/USG

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

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



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

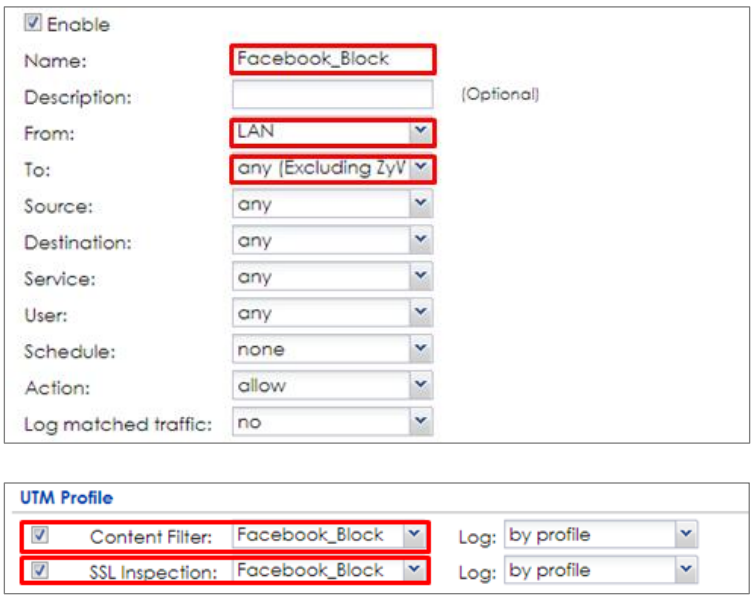
Set Up the Security Policy on the ZyWALL/USG

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

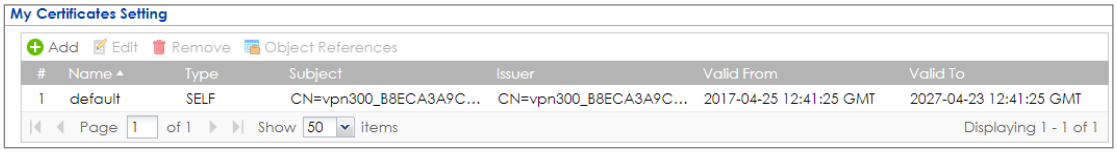


Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

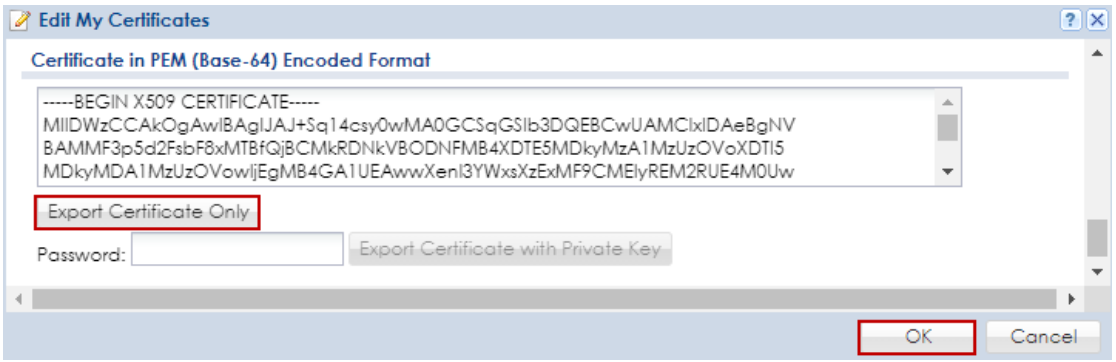
When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG.

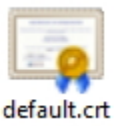
CONFIGURATION > Object > Certificate > default



CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only

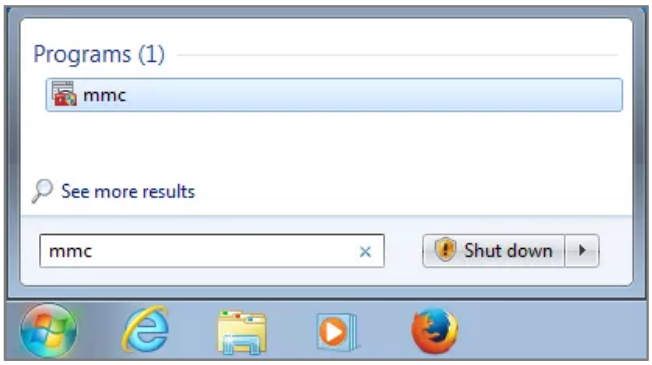


Save default certificate as *.crt file to Windows 7 Operation System.



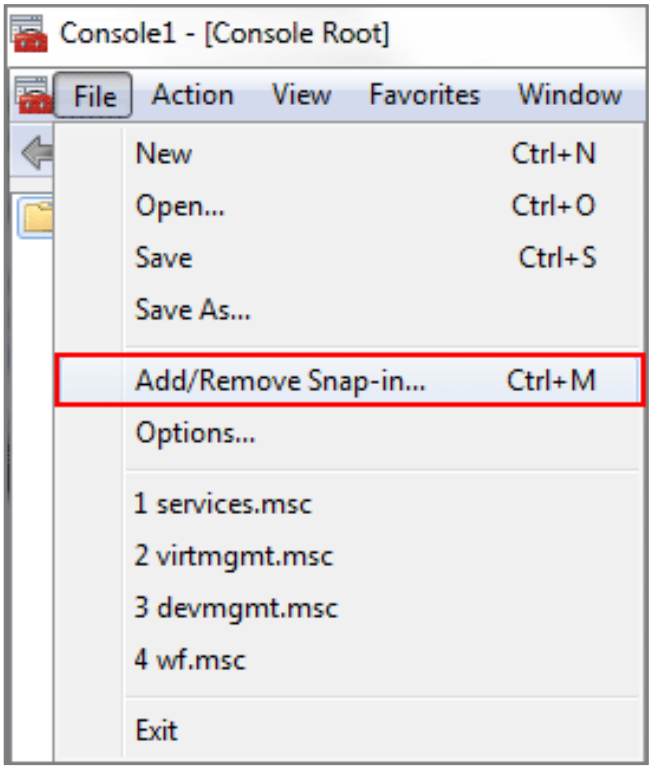
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



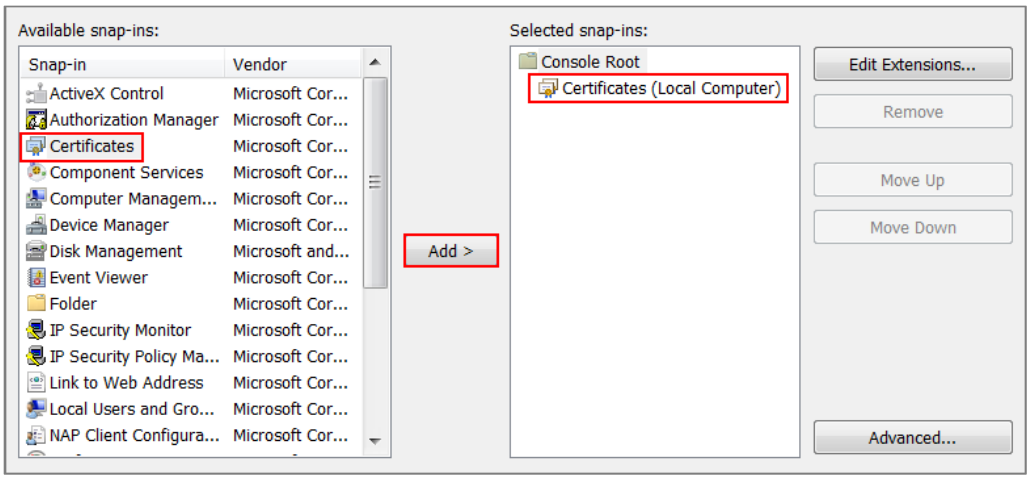
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

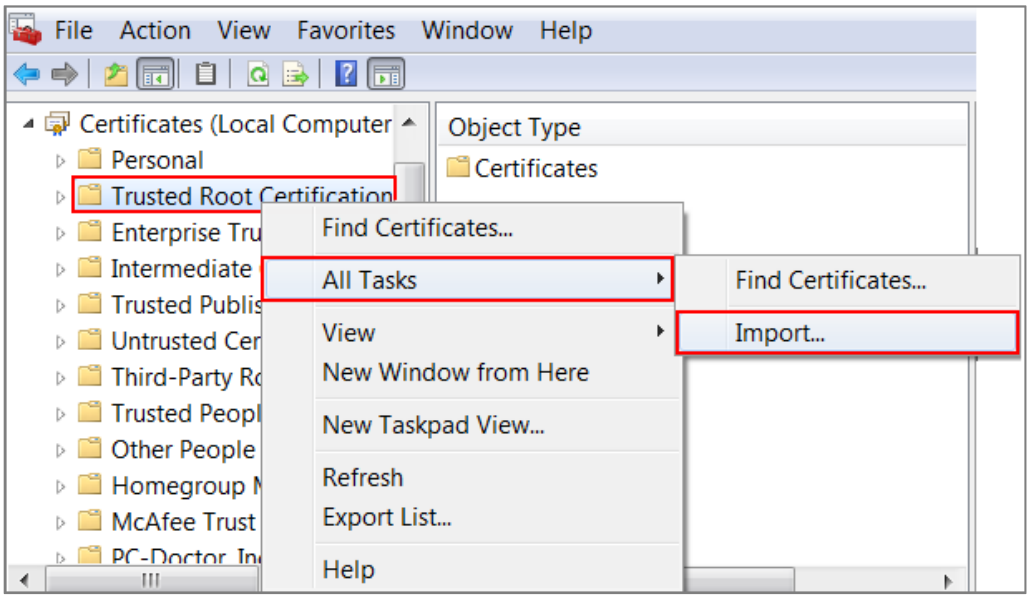


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

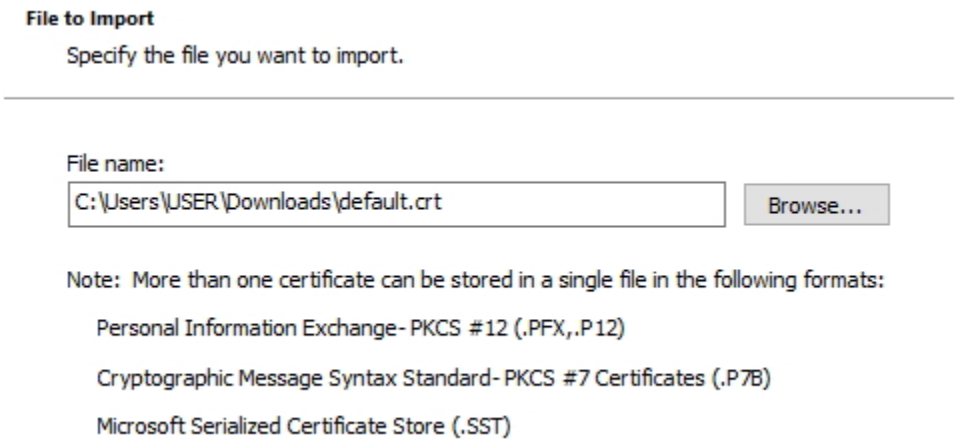
Available snap-ins > Certificates > Add



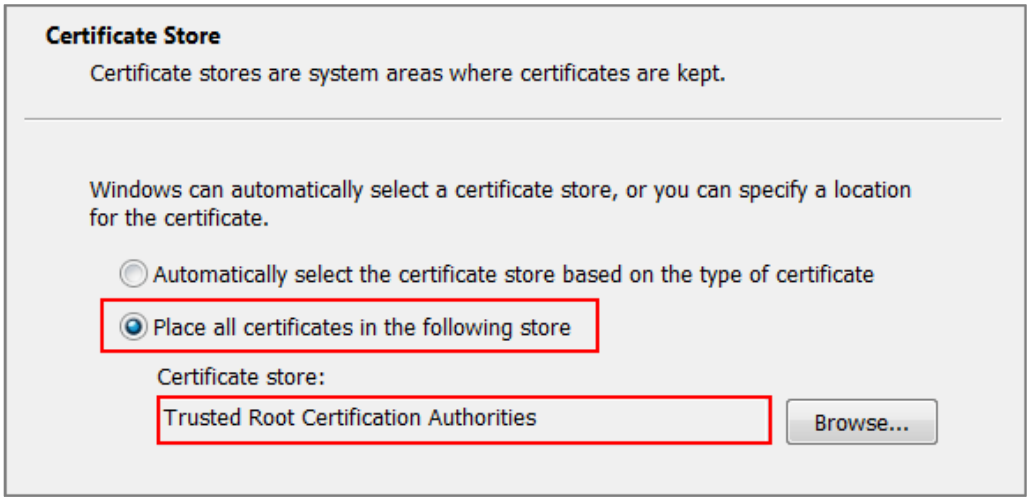
In the mmc console window, open the **Certificates (Local Computer) > Trusted Root Certification Authorities**, right click **Certificate > All Tasks > Import…**



Click **Next**. Then, **Browse...**, and locate the .crt file you downloaded earlier. Then, click **Next**.



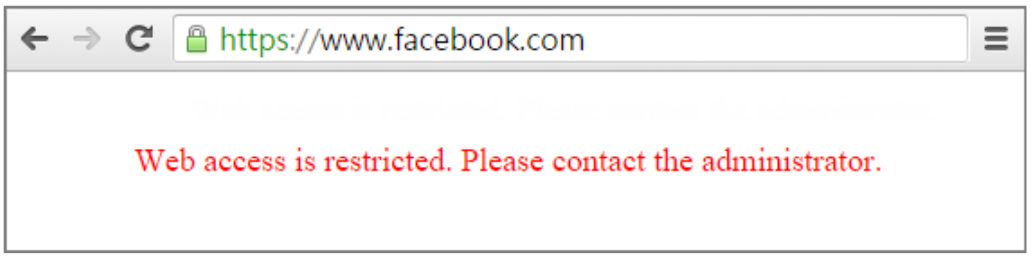
Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities.** Click **Next**, then click **Finish**.



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.



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.

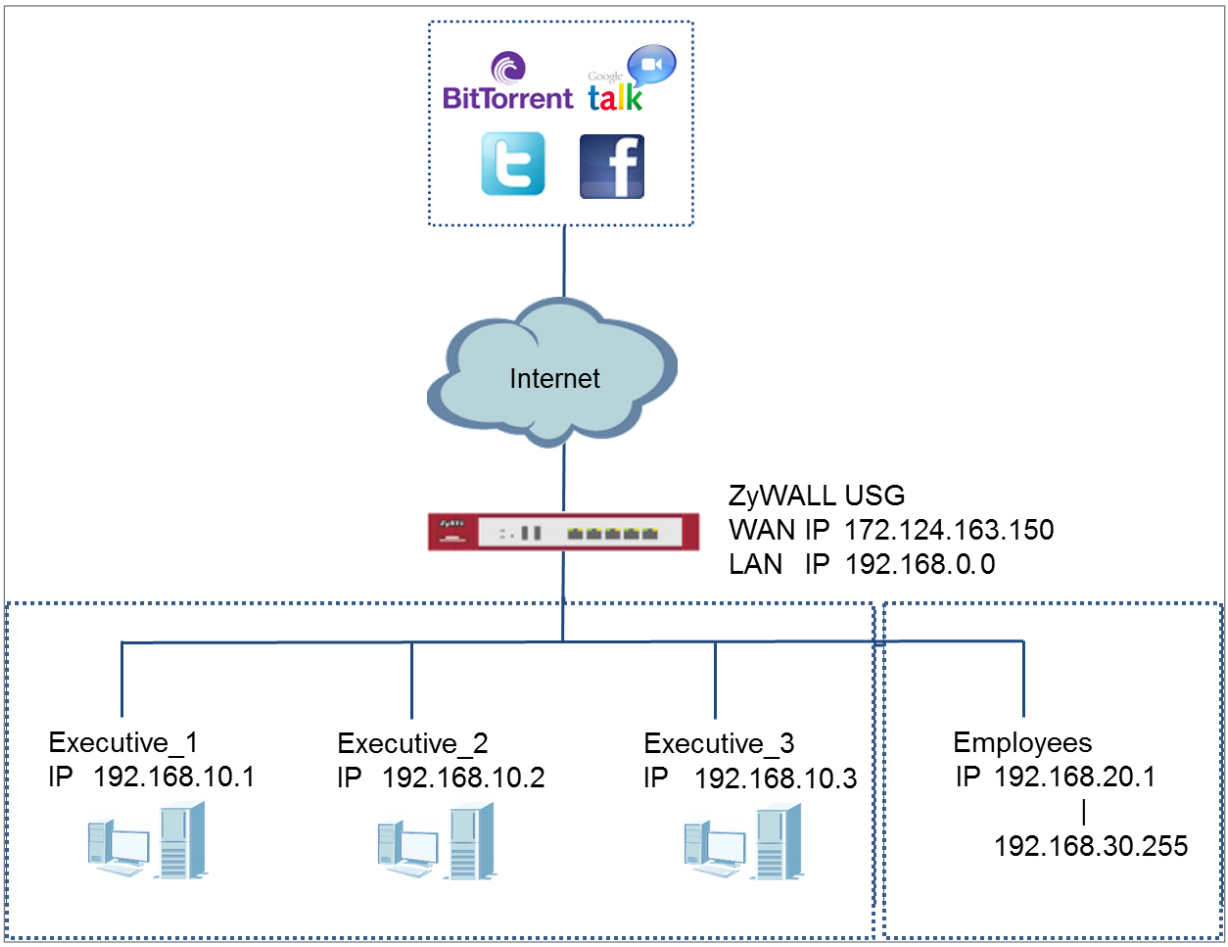
You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **Content Filter** license.

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

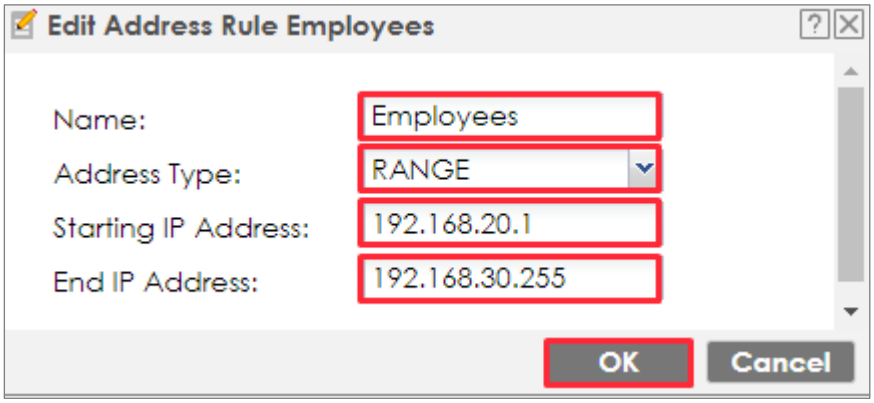


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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



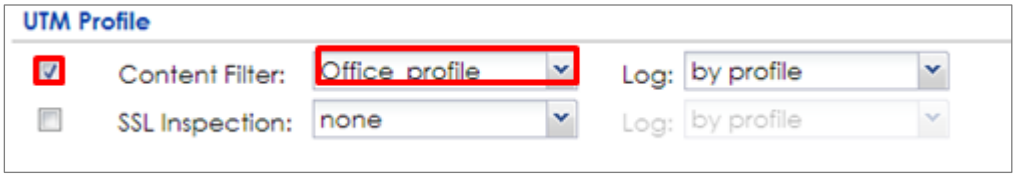
Set up **Security Policy** for employees, go to **CONFIGURATION > Security Policy > Policy Control > Add corresponding**, configure a **Name** for you to identify the employees' **Security Policy** profile.

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.).

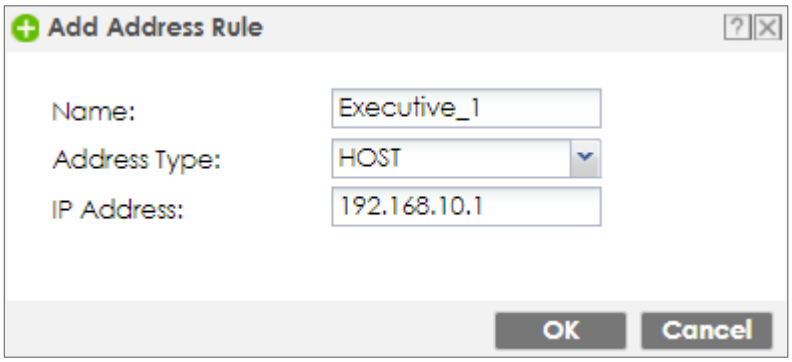
CONFIGURATION > Security Policy > Policy Control > Add corresponding > Employees_Security

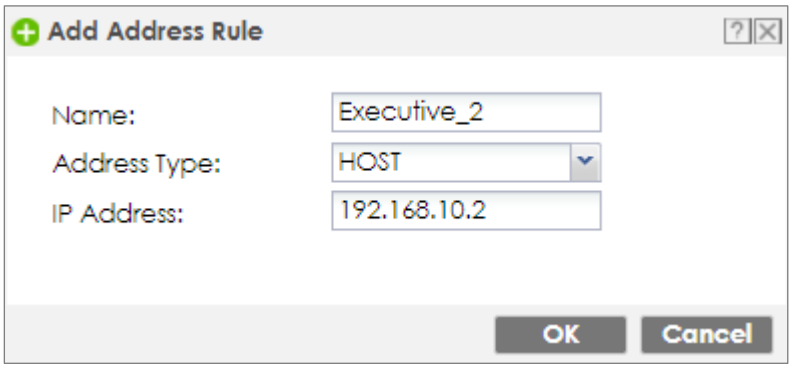


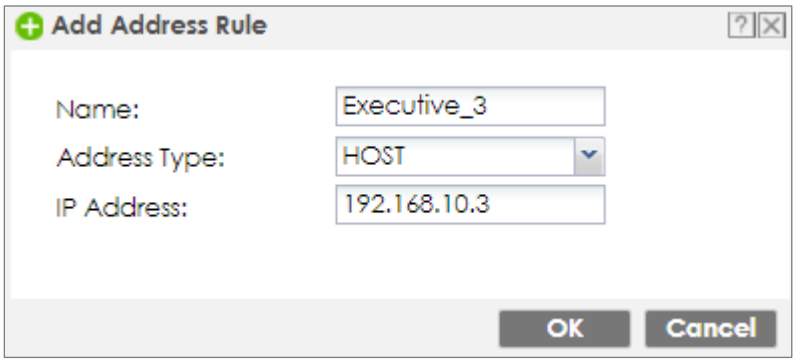
Set Up the Security Policy on the ZyWALL/USG for Executives

In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create address for each executives.

CONFIGURATION > Object > Address > Add Address Rule

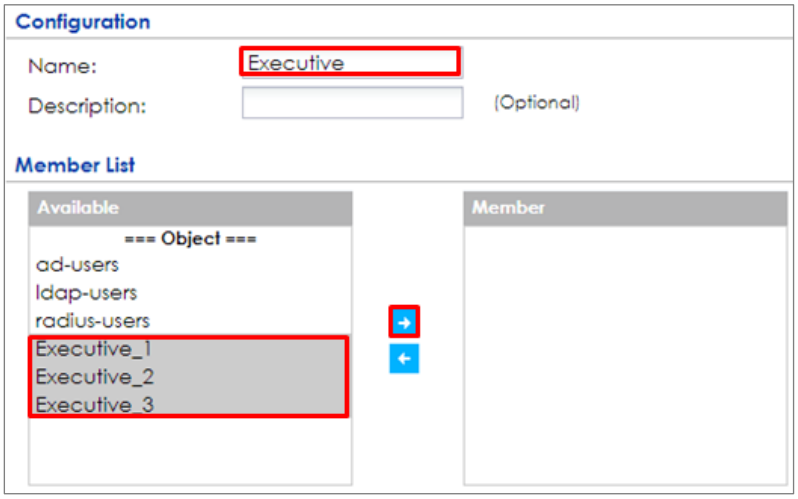






Then, go to **CONFIGURATION > Object > Address Group > Add Address Group Rule** to create a **Group Members' Name** and move the just created executives address object to **Member**.

CONFIGURATION > Object > Address Group > Add Address Group Rule



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

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.

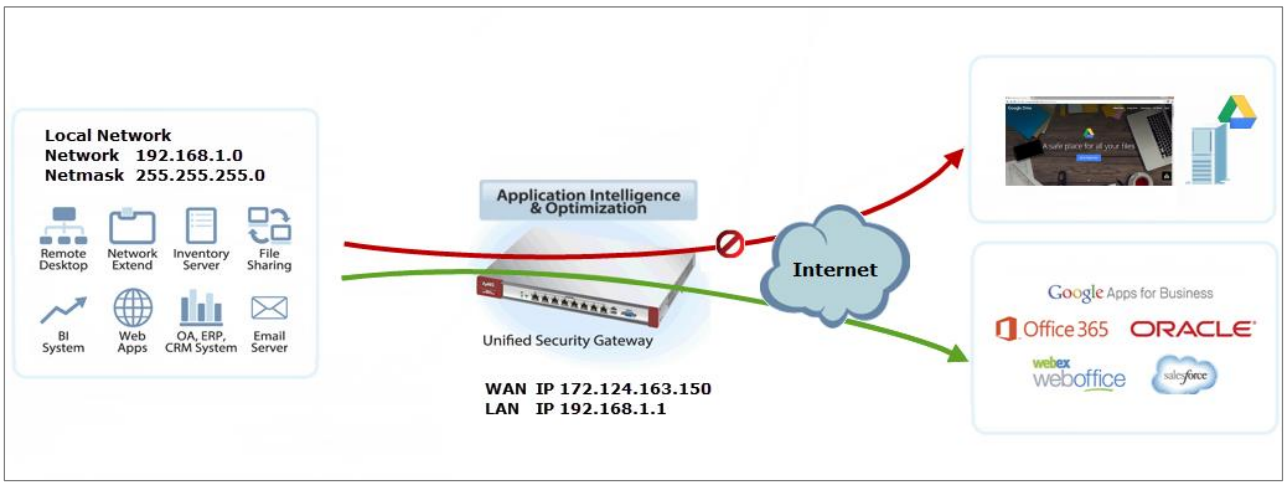
You have subscribed for the **UTM** service but the license is expired.

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



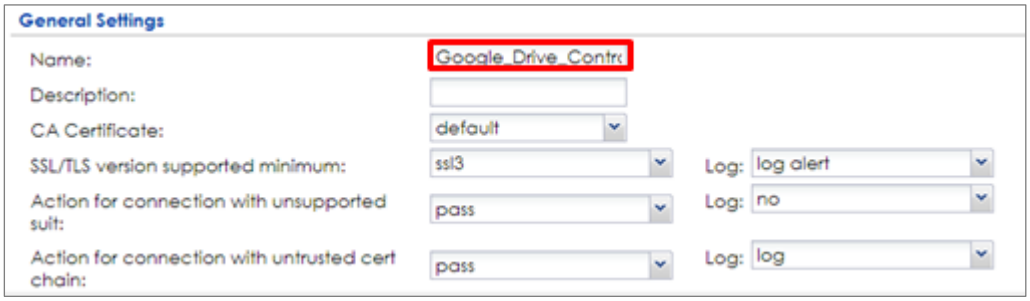
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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

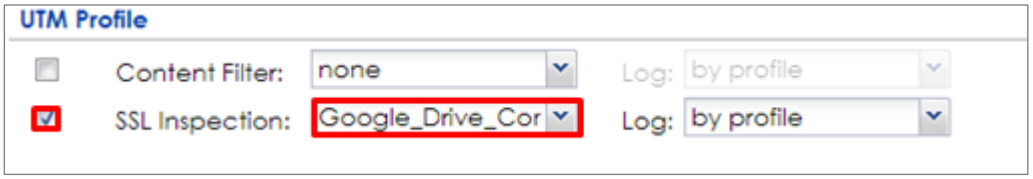


Set Up the Security Policy on the ZyWALL/USG

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



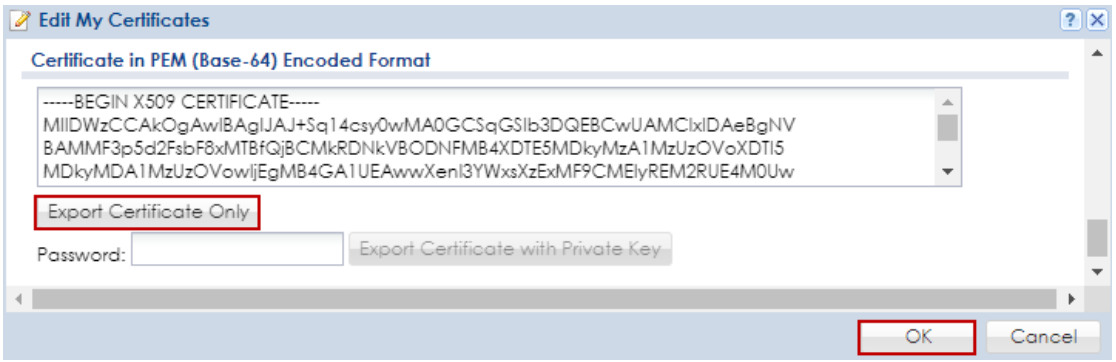
Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

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.

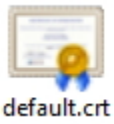
Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG.

CONFIGURATION > Object > Certificate > default

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only

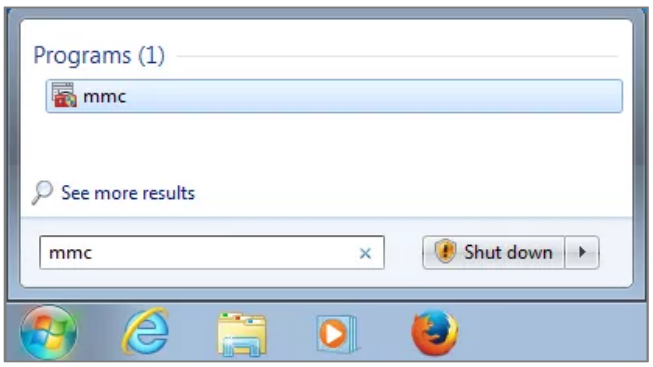


Save default certificate as *.crt file to Windows 7 Operation System.



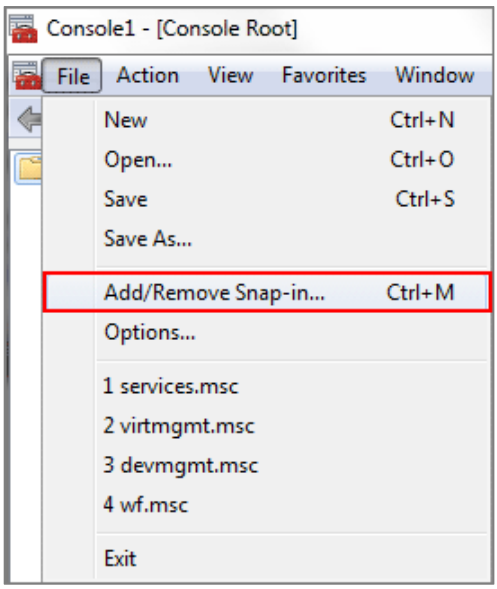
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



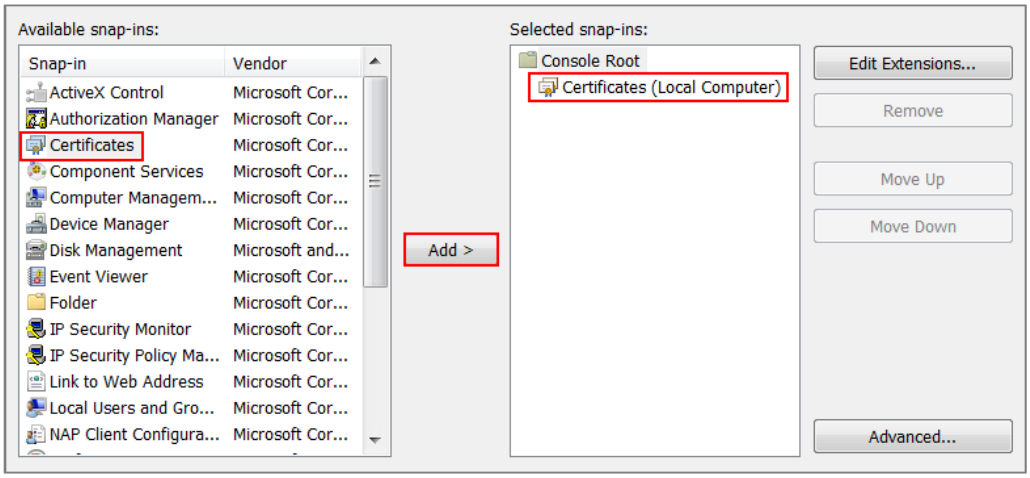
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

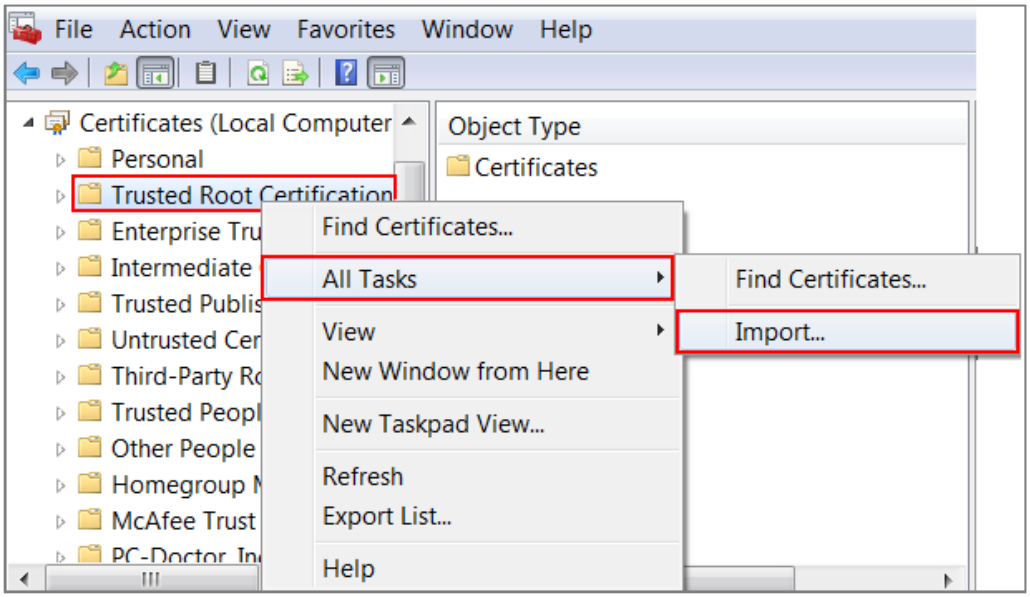


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

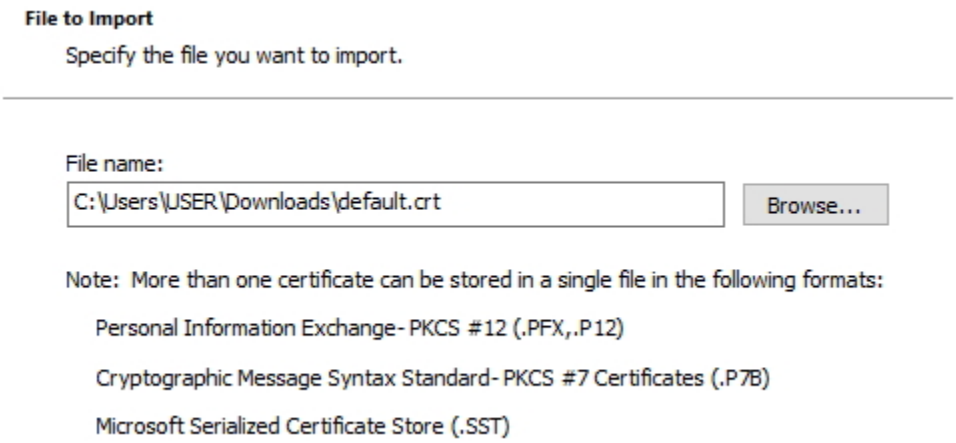
Available snap-ins > Certificates > Add



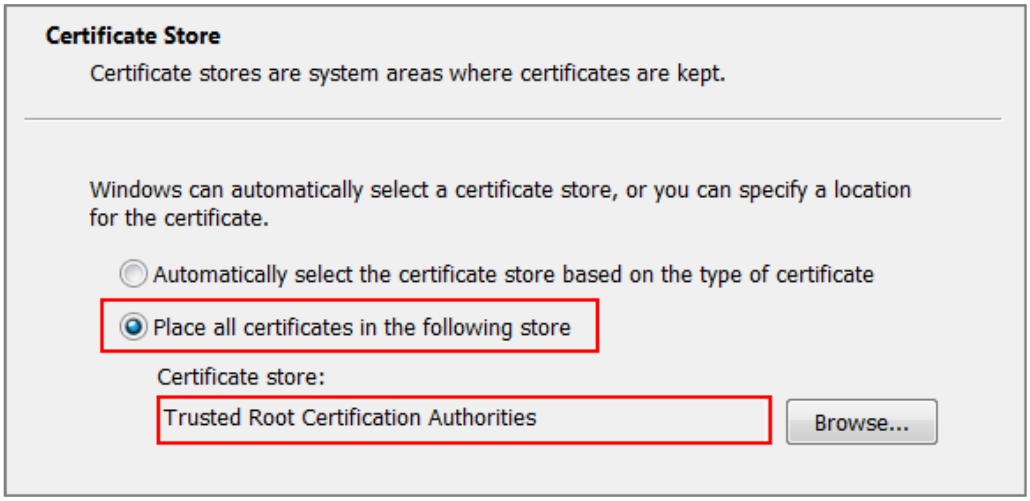
In the mmc console window, open the **Certificates (Local Computer) > Trusted Root Certification Authorities,** right click **Certificate > All Tasks > Import…**



Click **Next**. Then, **Browse...,** and locate the .crt file you downloaded earlier. Then, click **Next**.



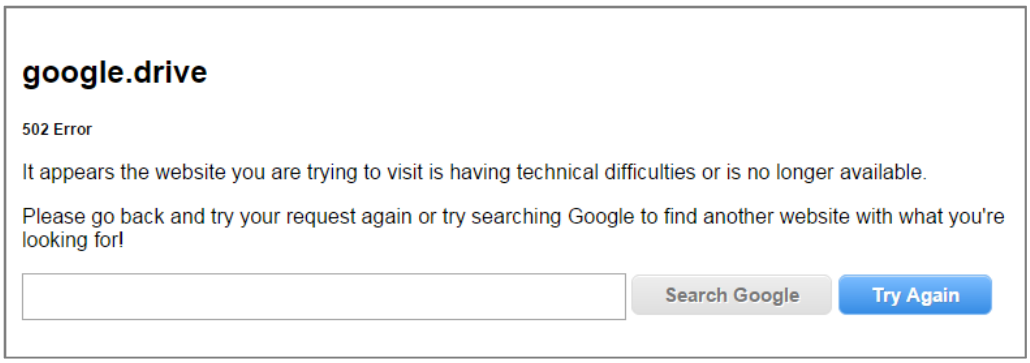
Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities.** Click **Next**, then click **Finish**.



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.



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:

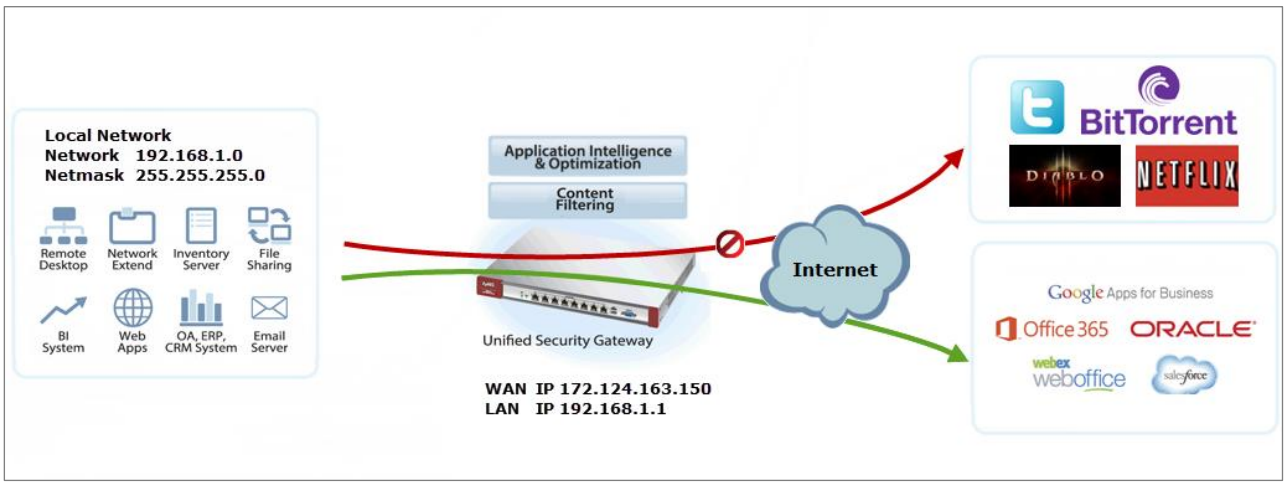
You have not subscribed for the **Application Patrol** service.
You have subscribed for the **Application Patrol** service but the license is expired.

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

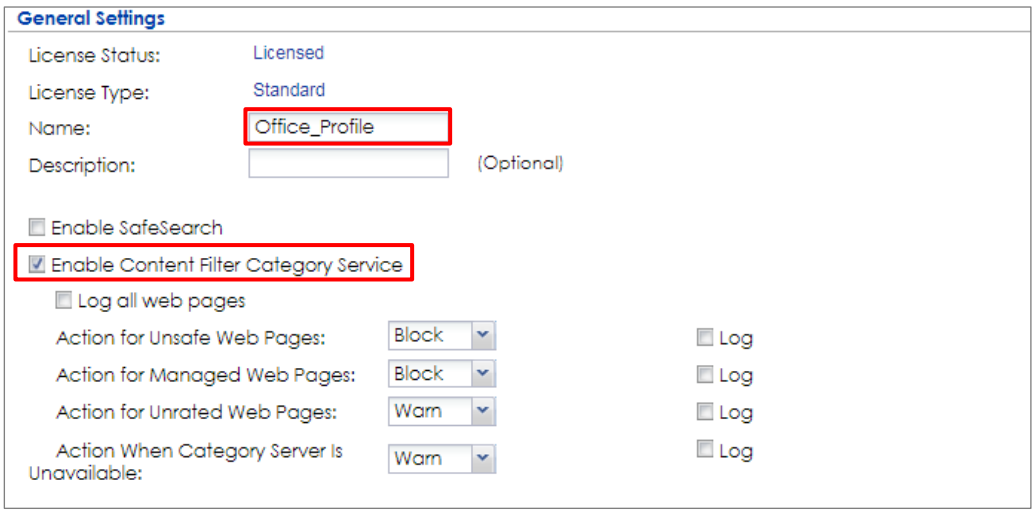


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Content Filter on the ZyWALL/USG

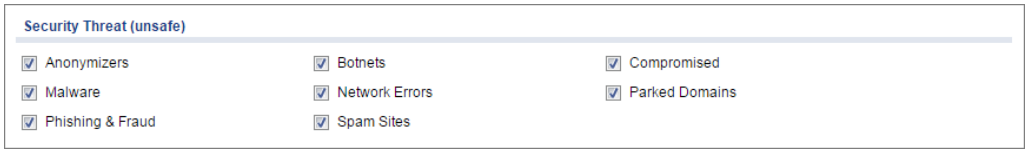
In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile> Content Filter > Profile Management > Add Filter File > Category Service**. Configure a **Name** for you to identify the **Content Filter Profile** and select **Enable Custom Service.**

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add > Category Service > General Settings



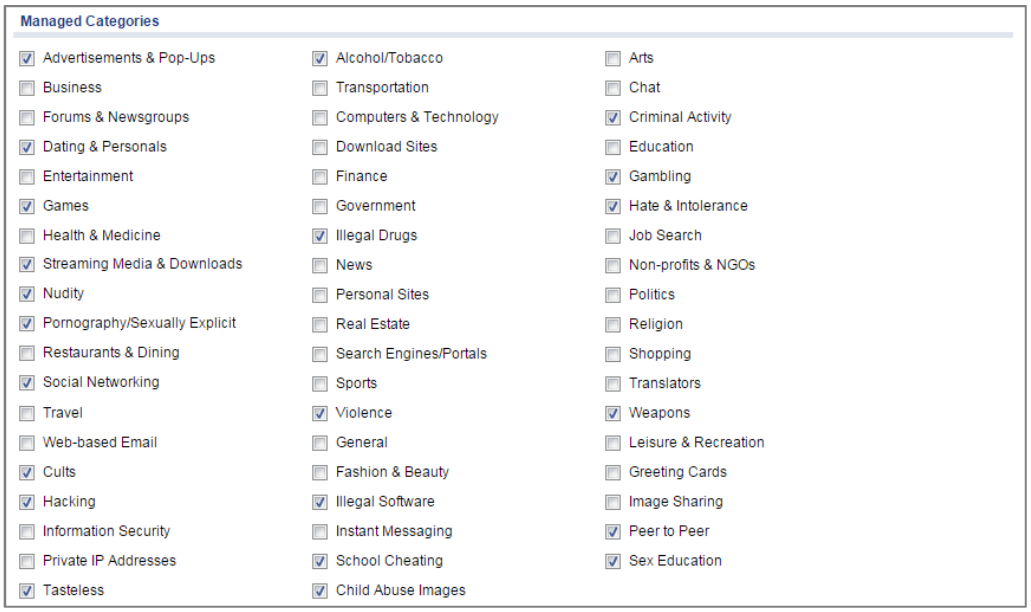
Scroll down to the **Security Threat (unsafe)** section and select all categories of web pages that are known to pose a threat to your computers.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Category **Service > Security Threat (unsafe)**



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



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

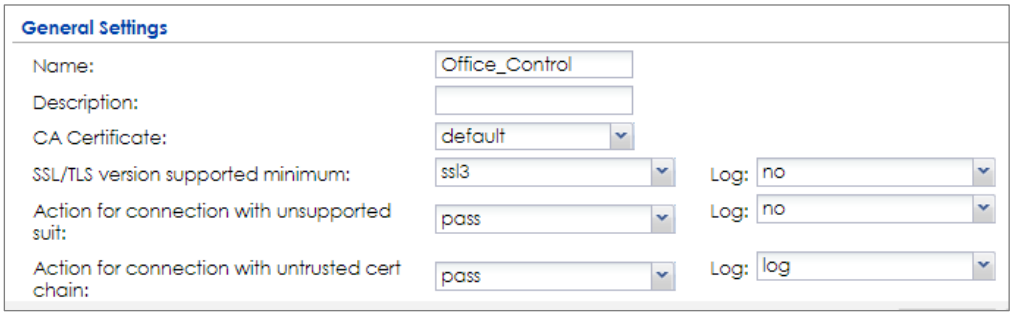
Set Up SSL Inspection on the ZyWALL/USG

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

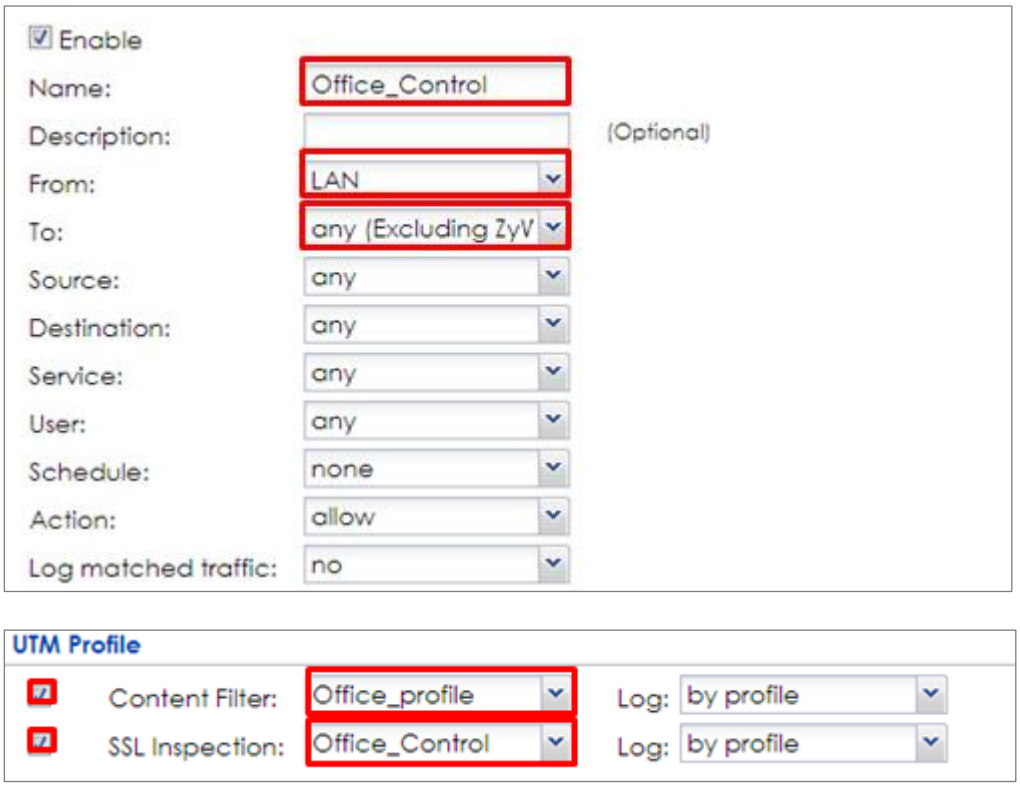


Set Up the Security Policy on the ZyWALL/USG

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

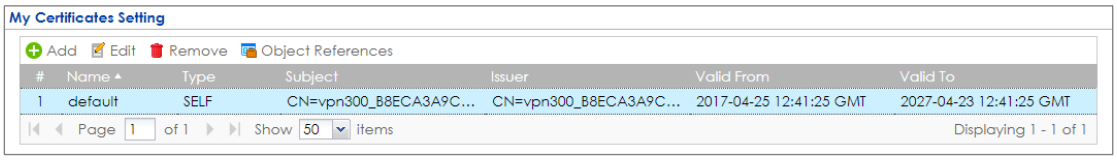


Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

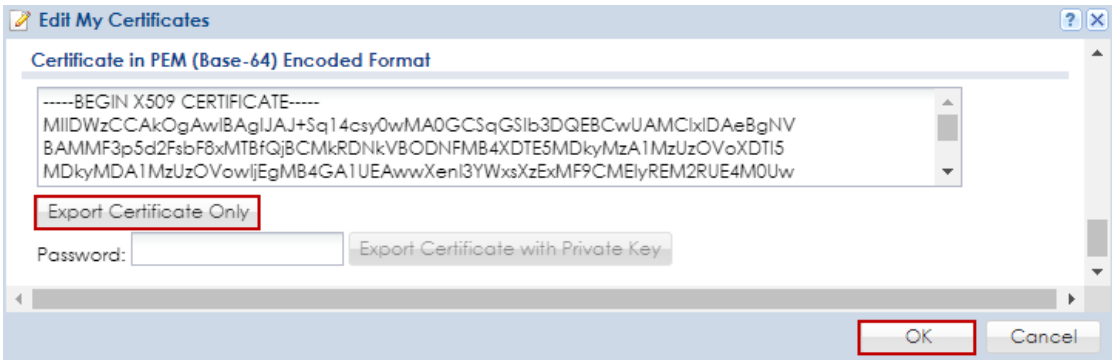
When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG.

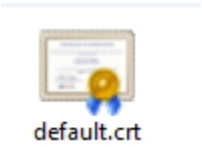
CONFIGURATION > Object > Certificate > default



CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only

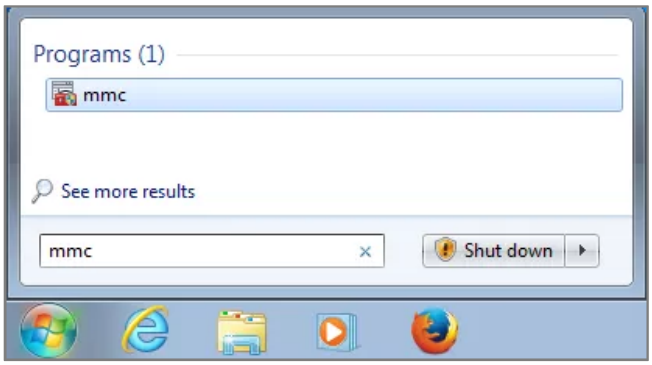


Save default certificate as *.crt file to Windows 7 Operation System.



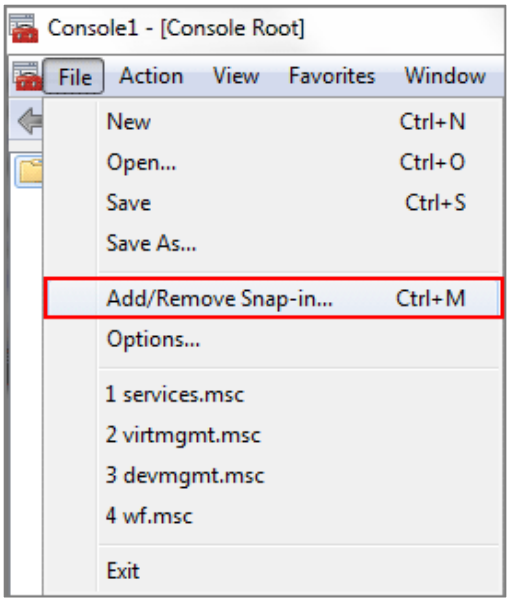
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



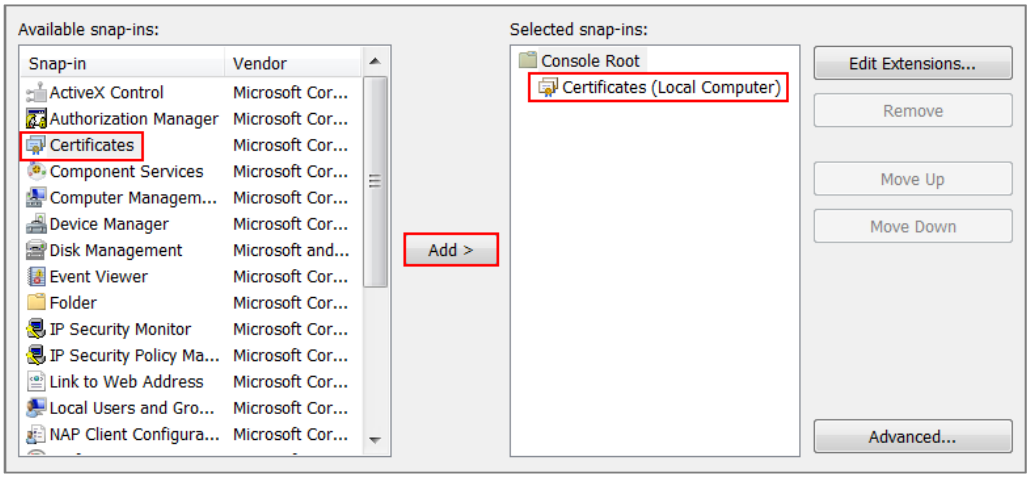
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

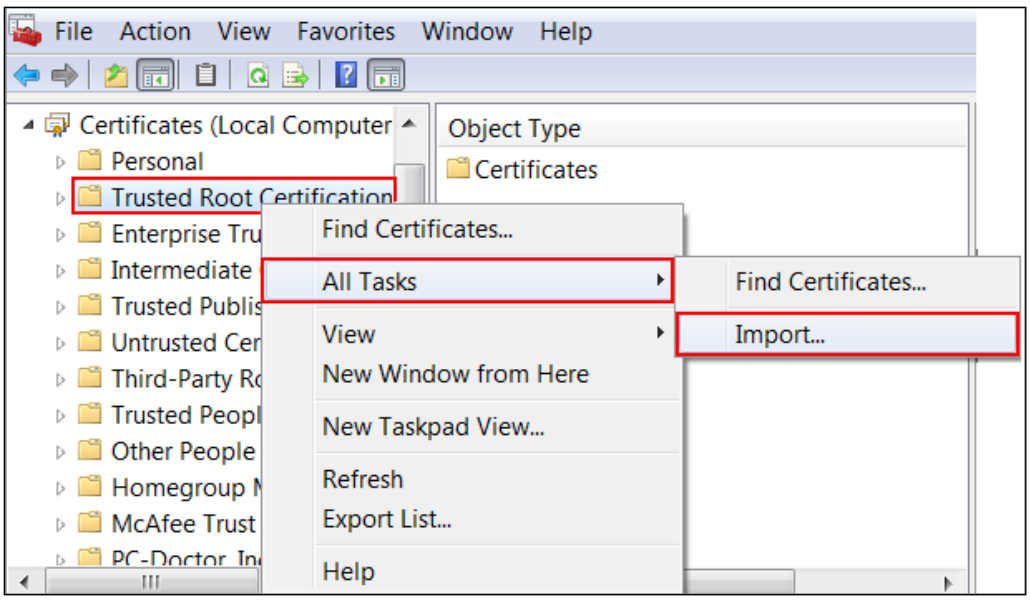


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

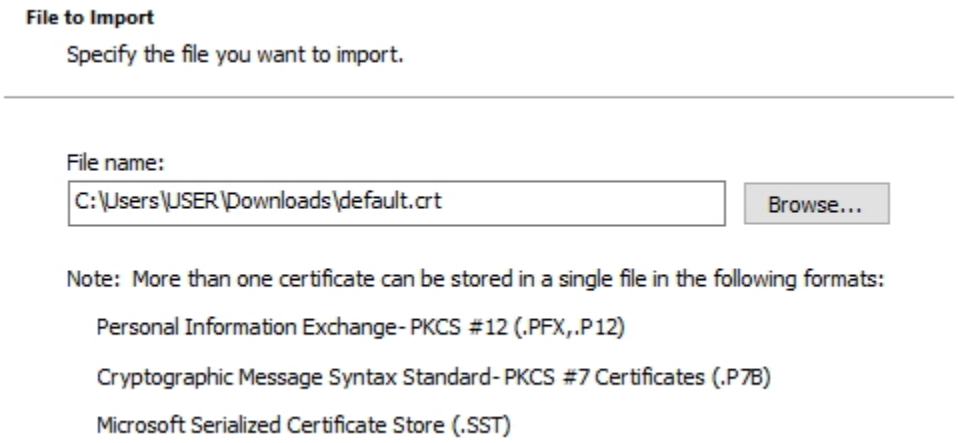
Available snap-ins > Certificates > Add



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**.



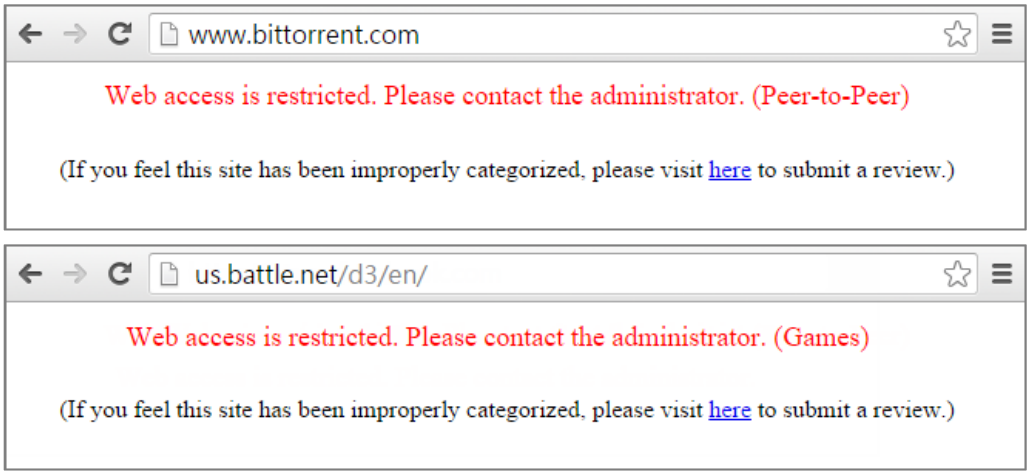
Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities.** Click **Next**, then click **Finish**.

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.



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:

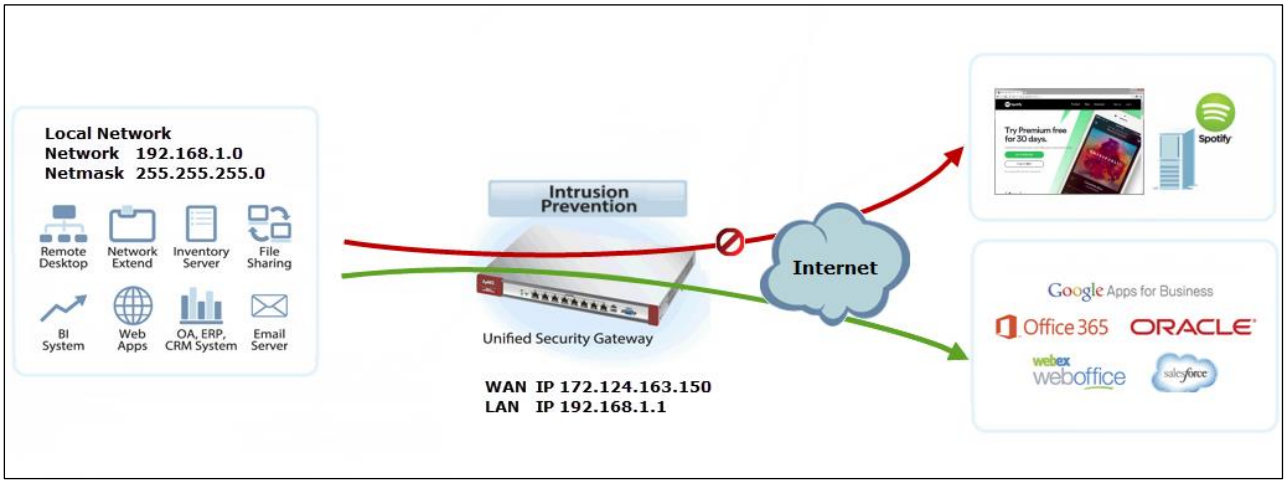
You have not subscribed for the **Content Filter** service.
You have subscribed for the **Content Filter** service but the license is expired.

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

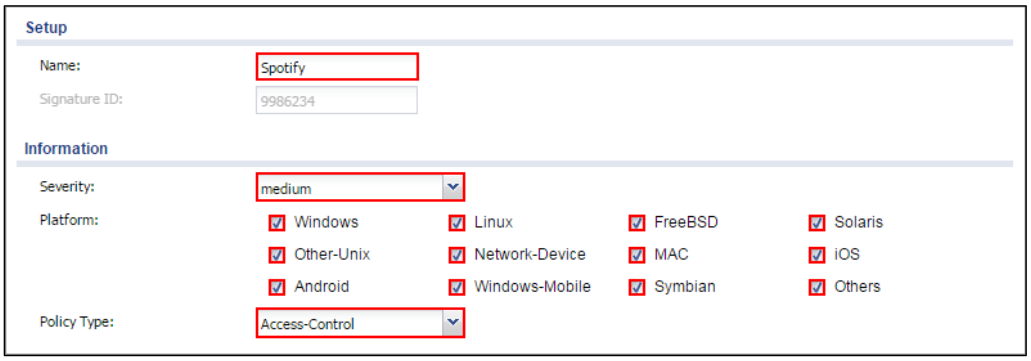


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up IDP Profile on the ZyWALL/USG

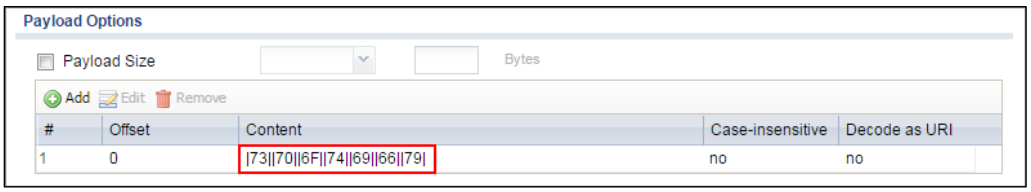
In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > IDP > Custom Signatures > Add Custom Signatures,** configure a **Name** for you to identify the **IDP** Profile. Select **medium** as the **Severity** level. Select all **Platform**. Select **Policy Type** to be **Access-Control** here to limit access network resources such as servers.

CONFIGURATION > Security Policy > IDP > Custom Signatures > Add Custom Signatures > Setup & Information



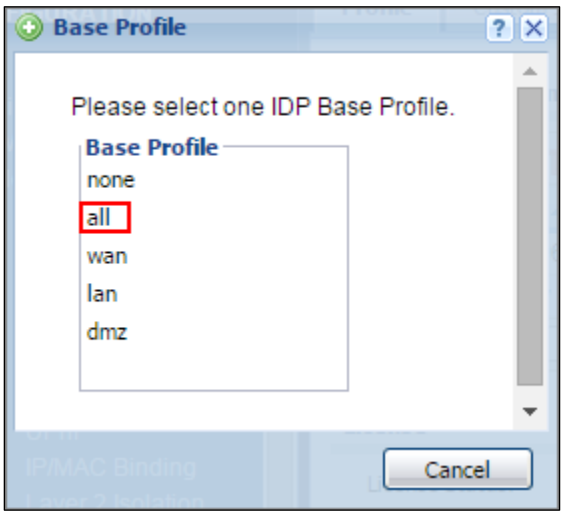
Scroll down to the **Payload Options** section, the type Spotify's software signature: |73| |70| |6F| |74| |69| |66| |79| into the **Content** field. Click **OK**.

CONFIGURATION > Security Policy > IDP > Custom Signatures > Add Custom Signatures > Payload Options



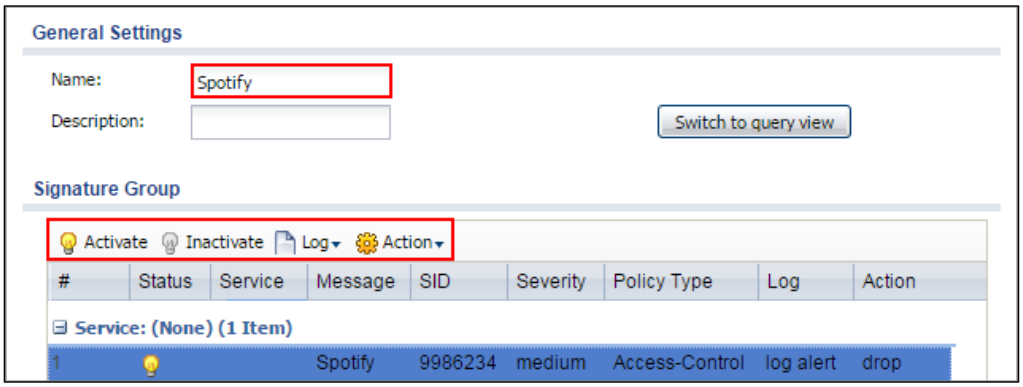
In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > IDP > Profile > Base Profile**. A pop-up screen will appear and select a **Base Profile** to go to the profile details screen.

CONFIGURATION > UTM Profile > IDP > Profile > Base Profile



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



Test the Result

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

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?

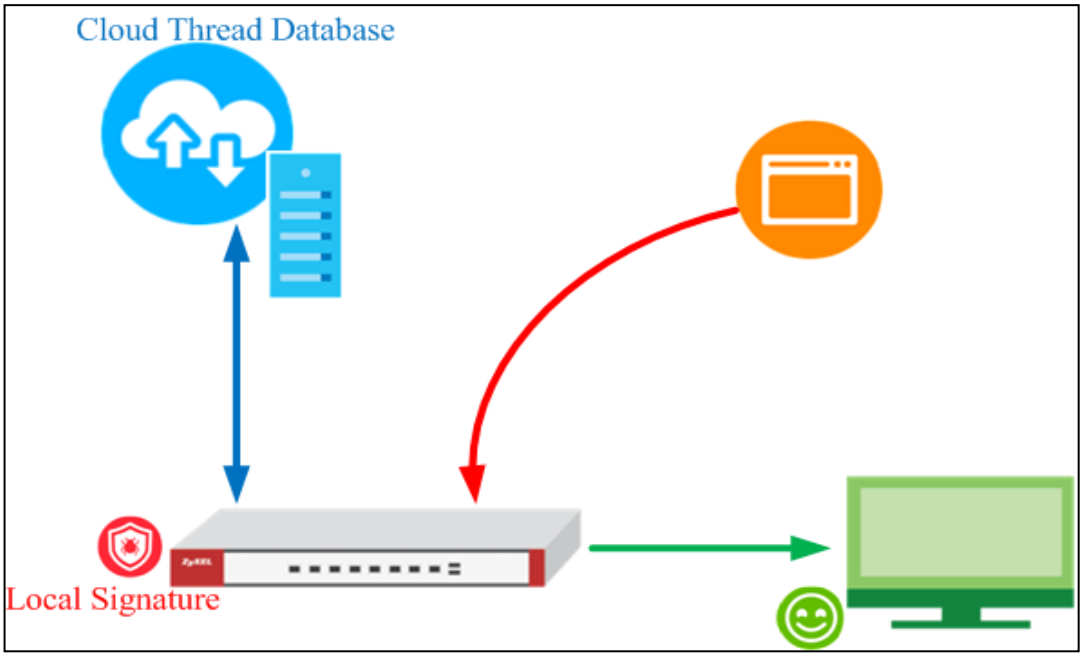
If you are not be able to configure any **IDP** policies or it's not working, there are two possible reasons:

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.

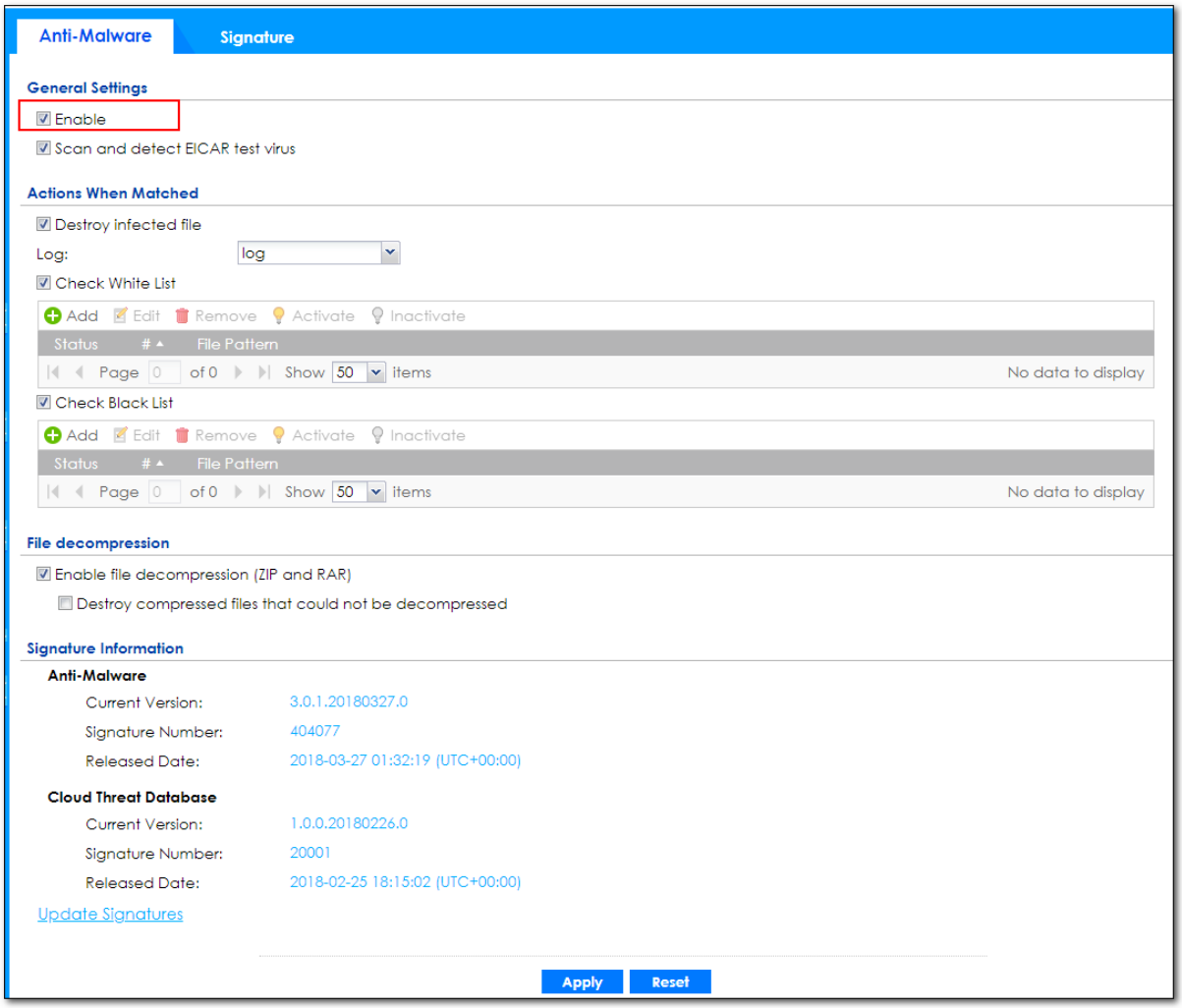
The **Anti-Malware Signature** is means your downloaded files will checked by local signatures that exist on device itself. It is helpful when your device unable access to internet at that moment.

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

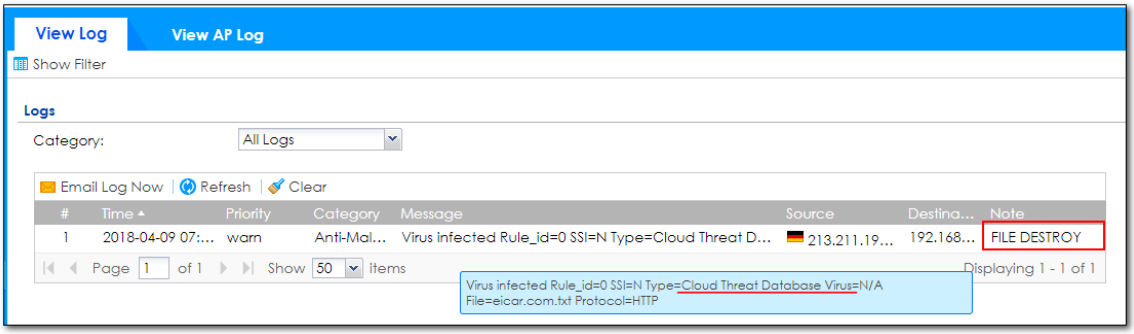


Note: The Anti-Malware license is required. So you must enabled Anti-Malware function on your myzyxel.com account.

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.

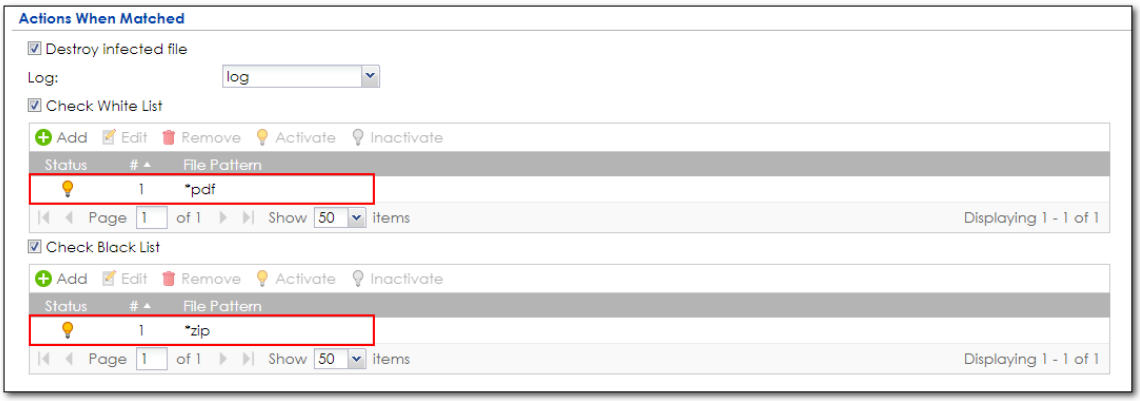
Then your file is unable opened or replaced by “0”.

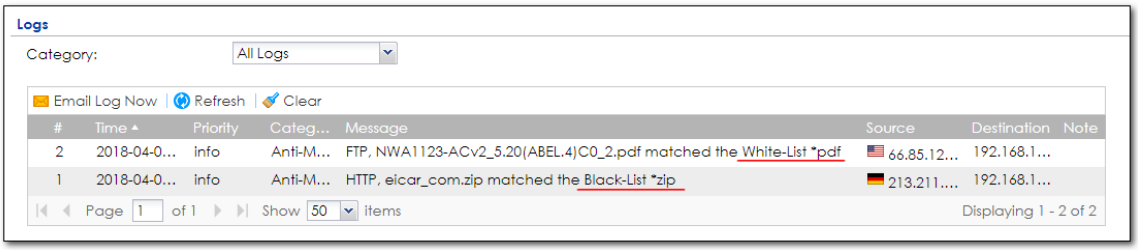


Additional configuration

White List: You can use wildcard to allowing specific type files.

Black List: You can use wildcard to drop specific type files.





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

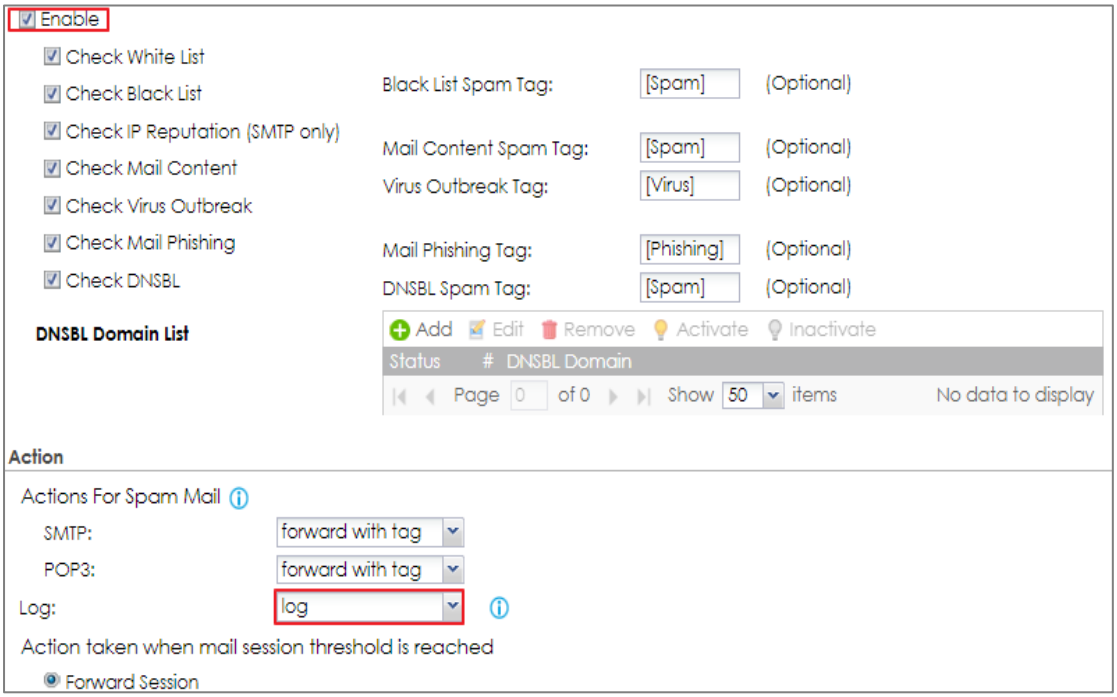
Figure 1 Using Email Security to Detect Spam

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).

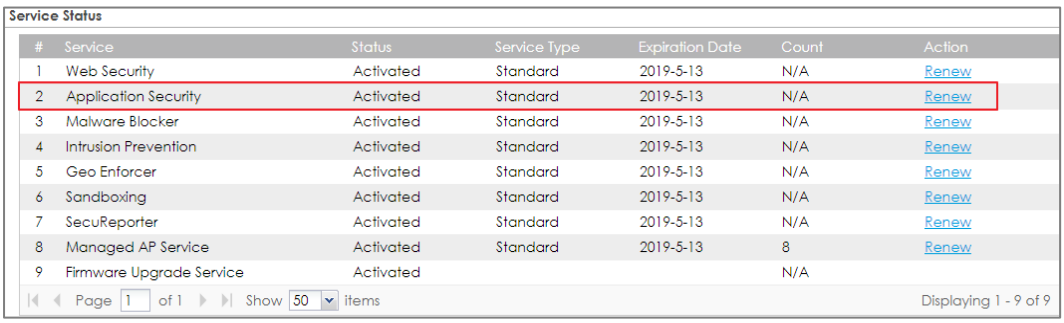
Set Up the Email Security on ATP Series

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.

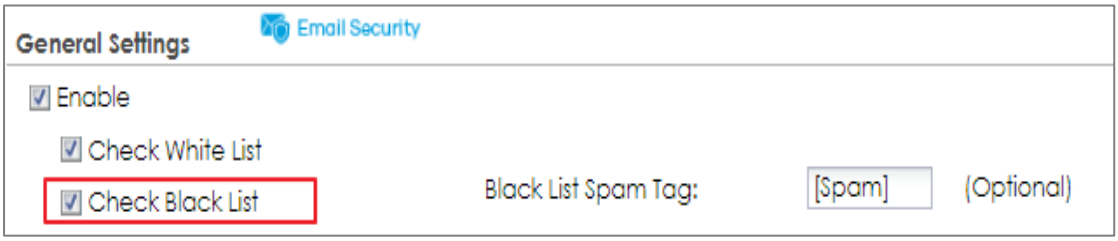
Select from the list of available **Scan Options** and desired Log type whether to have the ATP Series generate a log (**log**), log and alert (**log alert**) or neither (**no**) by default when traffic matches this policy. Click **Apply** to save the configuration **CONFIGURATION > Security Service > Email Security**



1. Register the device to myZyxel.com.
2. Activate Application Security.

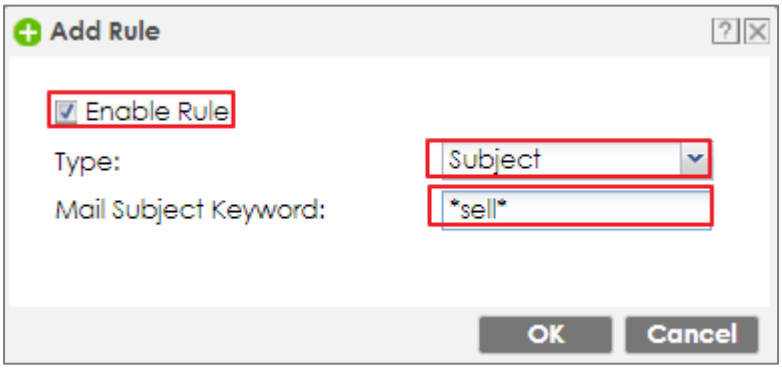


3. **Go to CONFIGURATION > Security Service> Email Security>Enable Check Black List** to have the ATP Series treat e-mail that matches (an active) black list entry as spam.



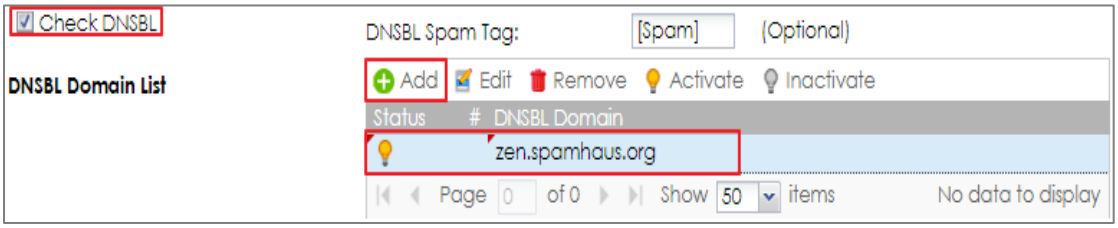
4. Continue to **Rule Summary on** Black/White List, click the **Add** icon. A pop-up screen will appear allowing you to configure **Content** (**Subject**, **IP/IPv6 Address**, **E-Mail Address** and **Mail Header**), Use wildcards (*) to configure **Mail Subject Keyword**. (*sell* in this example). Click **OK** to return to the **General** screen.

CONFIGURATION > Security Service> Black/White List



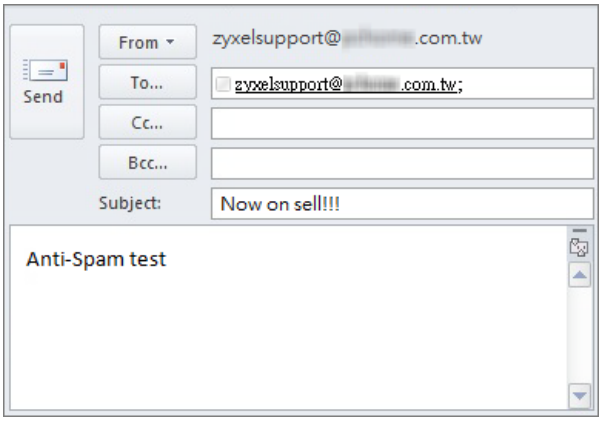
5. In the ATP Series, go to **CONFIGURATION > Security Service> Email Security>Enable Check DNSBL**

Press Add and enter the **DNSBL Domain** for a DNSBL service (zen.spamhaus.org in this example). Click **Apply**.

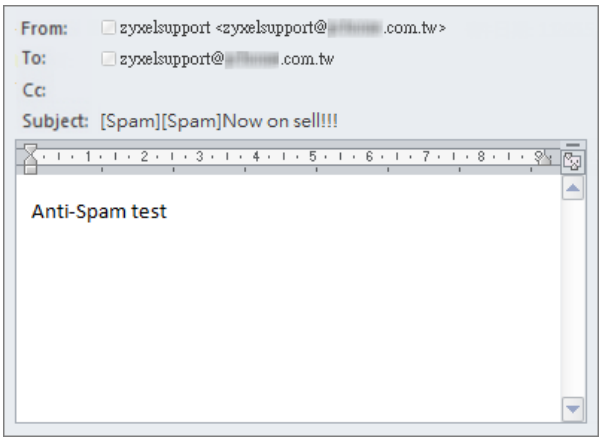


Test the result

1. Send the mail subject with "sell".



2. You will receive the mail subject with [Spam] tag.



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.

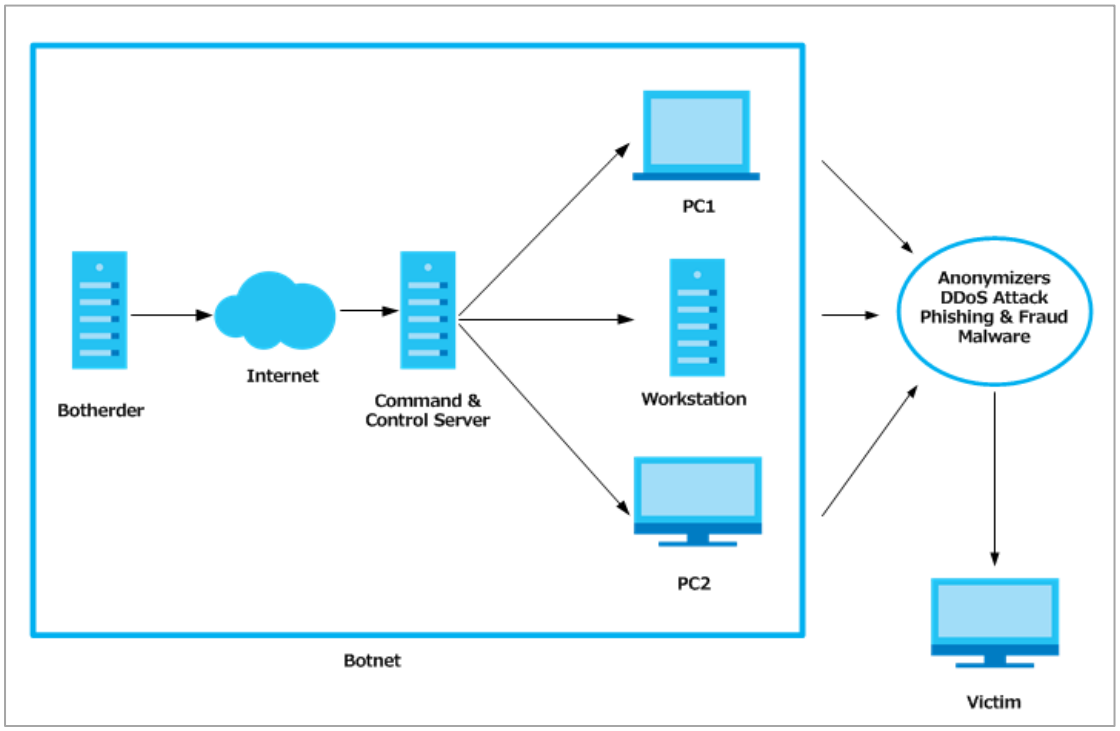
You have subscribed for the **Email Security** service but the license (**Application Security**) is expired.

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

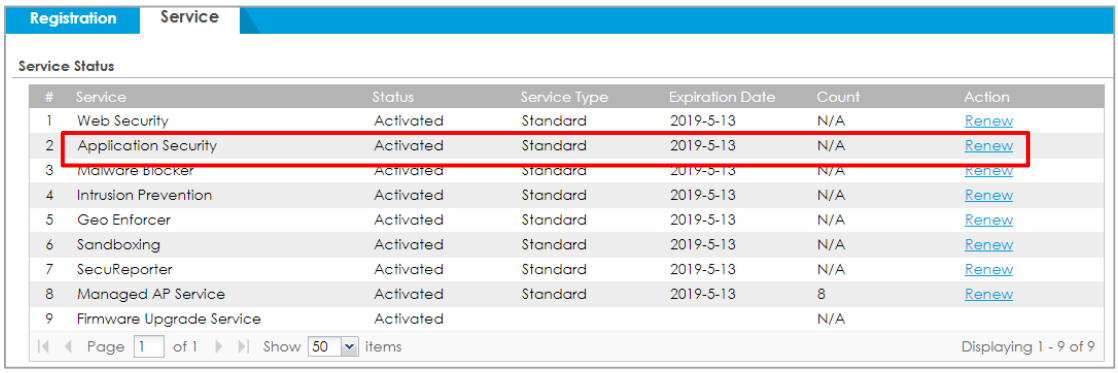
1. License status check
2. Update the Botnet Filter signature

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.

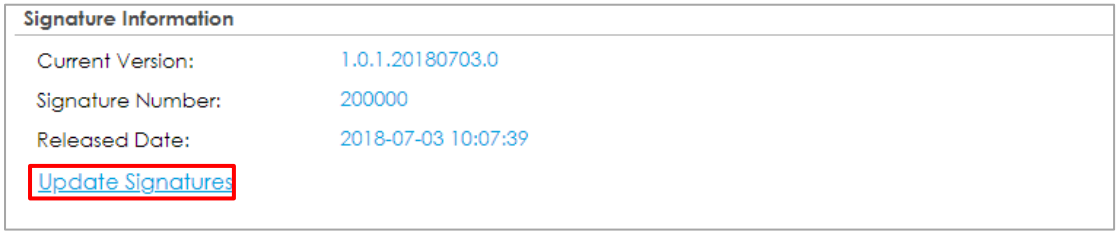


Update Botnet Filter Signatures

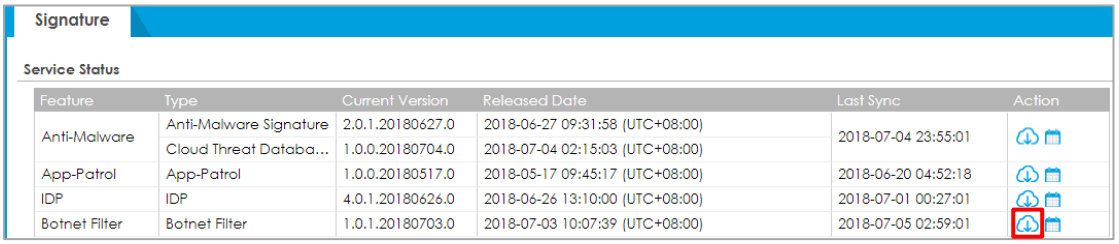
To make sure the device has the most updated signature, we suggest users to update their Botnet Filter signature before using this function.

To update the Botnet Filter signature:

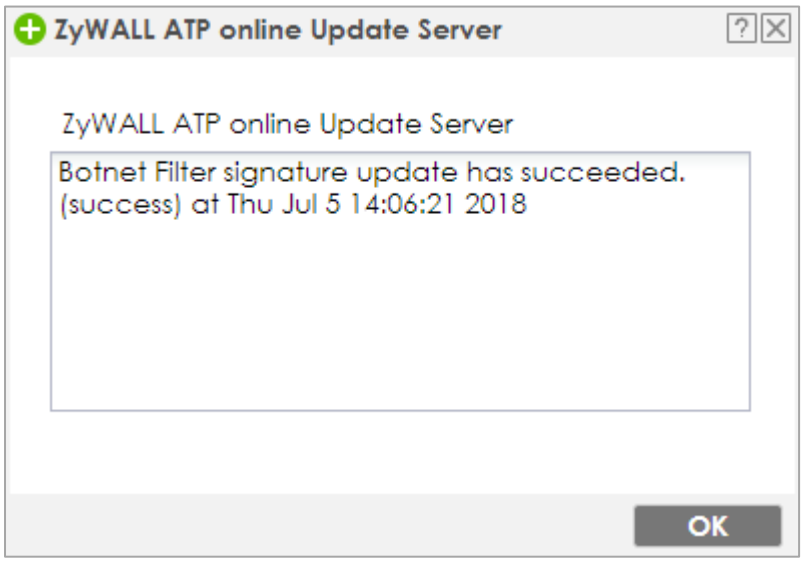
Go to **Configuration** > **Security Service** > **Botnet Filter.** Then click **"Update Signatures"**



Then the device will redirect users to the "**Service Status**" page. Click on the cloud icon and the device will start signature downloading process



Once the signature updating process was done. The GUI will pop up the following message to notify users.

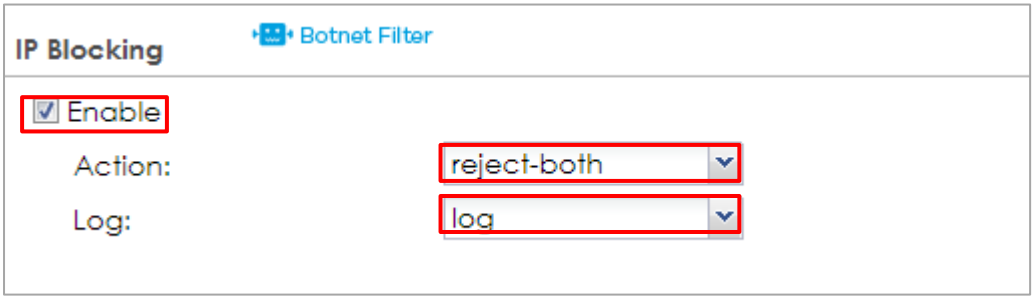


Now the Botnet Filtering function is ready to go.

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.

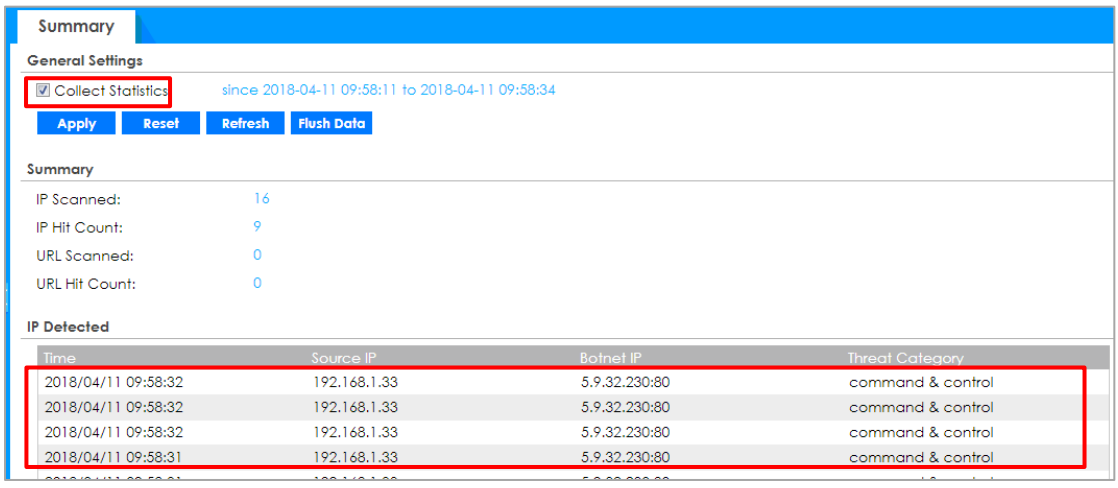


Test the Result

User access IP: 5.9.32.230

Go to **Monitor** > **Security Statistics** > **Botnet Filter** to check summary.

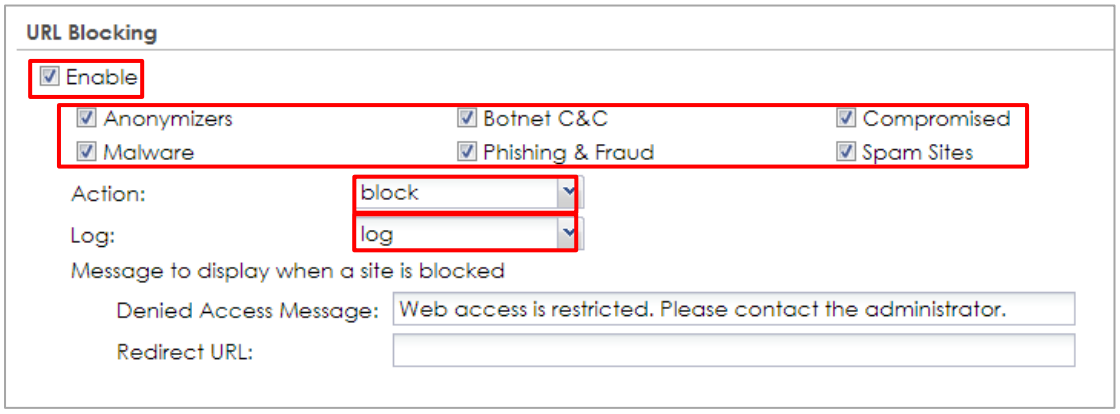
IP: 5.9.32.230 is blocked due to command & control.



Set up the URL Blocking on the ATP series

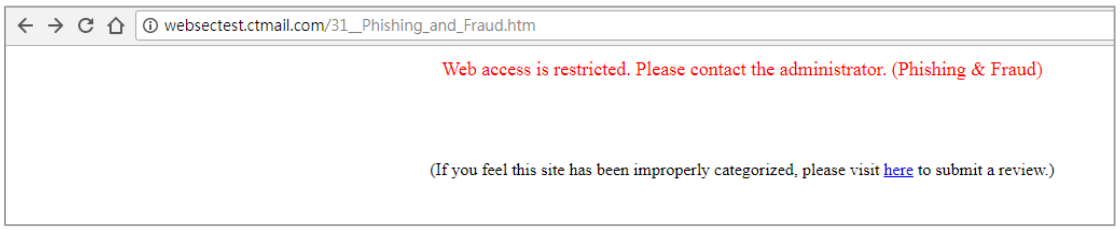
Go to **Configuration** > **Security Service** > **Botnet Filter.**

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.

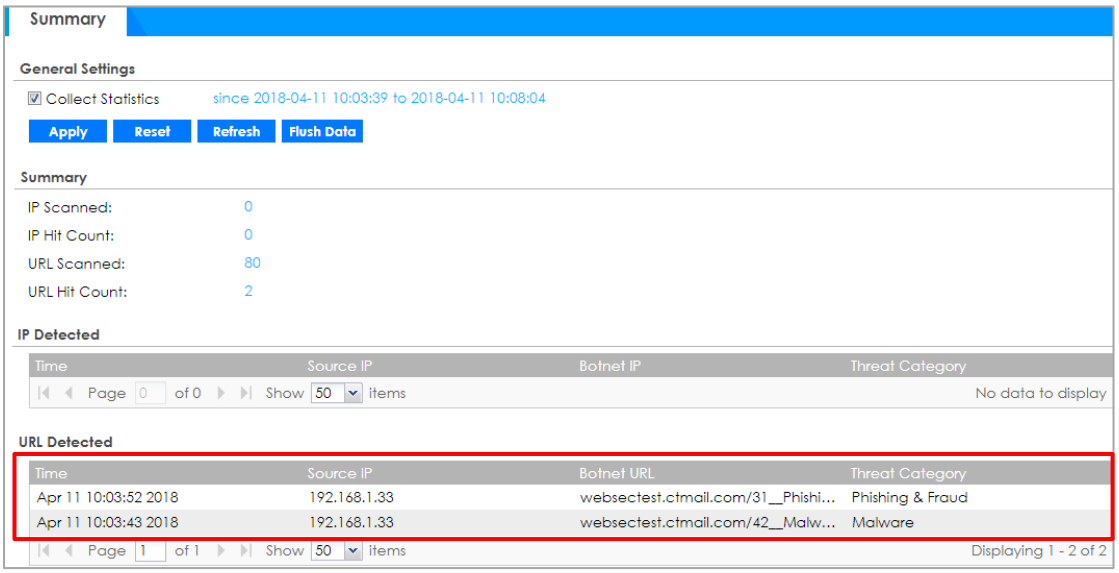


Test the Result

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



Go to **Monitor** > **Security Statistics** > **Botnet Filter** to check summary where users will see the related threat log was recorded


Summary
General Settings
Collect Statistics
since 2018-04-11 10:03:39 to 2018-04-11 10:08:04
Apply
Reset
Refresh
Flush Data
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.

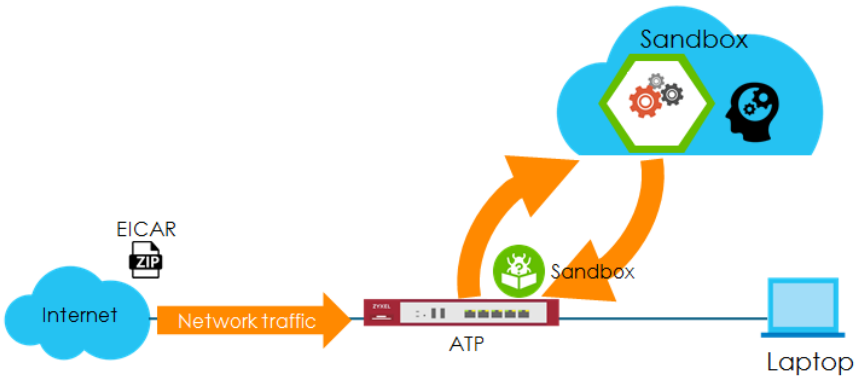
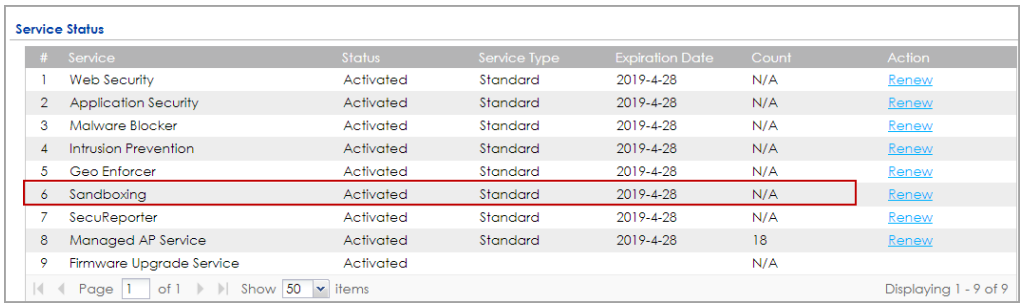


Figure 1 Using Sandboxing to Detect Unknown Malware

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

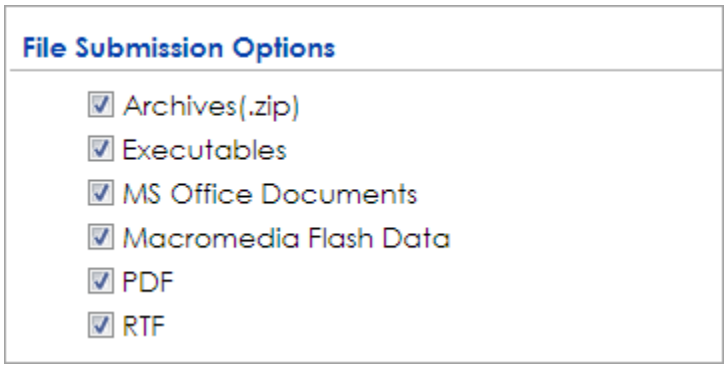
1. Register the device to myZyxel.com.
2. Activate Sandboxing license.


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	

Page 1 of 1 Show 50 items Displaying 1 - 9 of 9

3. In the ATP, go to **CONFIGURATION > Security Service > Sandboxing > File Submission Options**, the default supported file types are listed.



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.

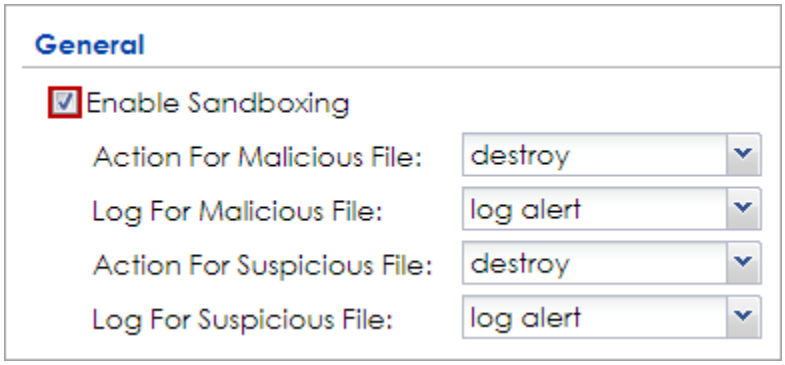
Router> configure terminal

Router(config)# sandbox file-type eicar

Router(config)# write

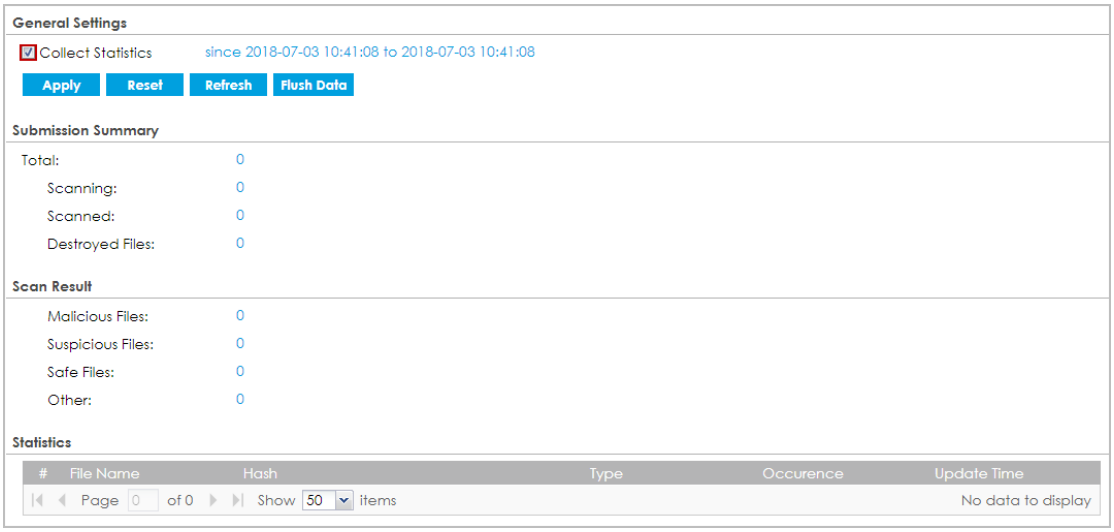
```
Router> configure terminal
Router(config)# sandbox file-type eicar
Router(config)# write
Router(config)# show sandbox file-type all
No.    Show_name                    Name                         Status
=============================================================================
1      Archives(.zip)               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.



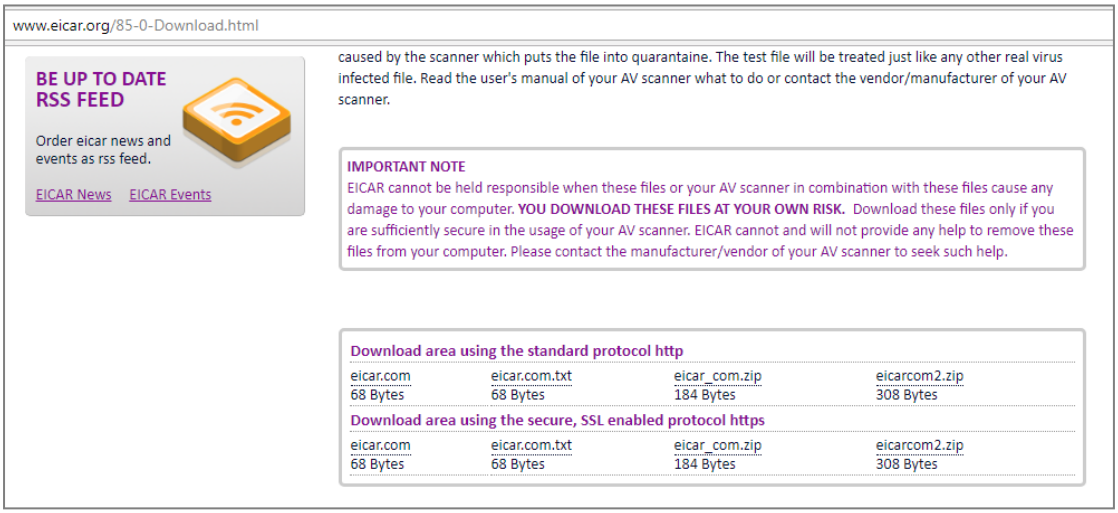
5. Enable Collect Statistics to monitor the scan results and statistics.

MONITOR > Security Statistics > Sandboxing



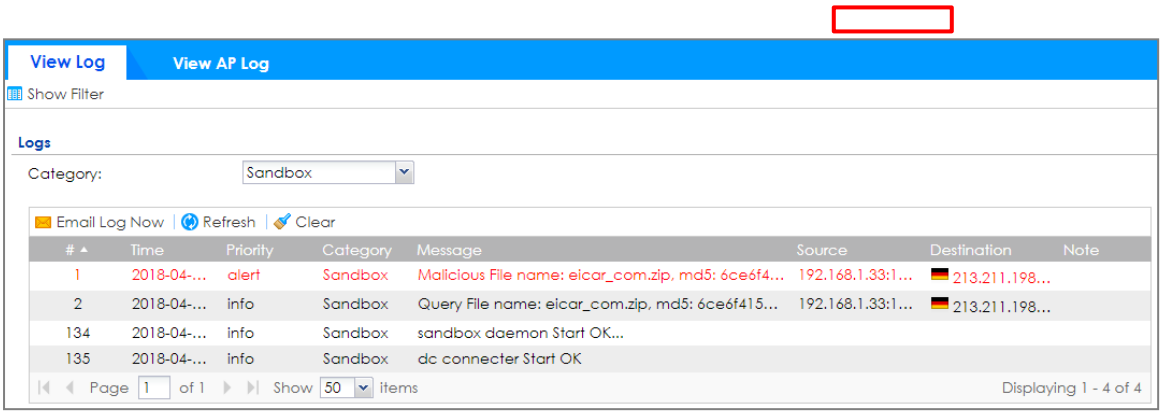
Test the Result

3 Go to http://www.eicar.org/85-0-Download.html to download eicar_com.zip file.



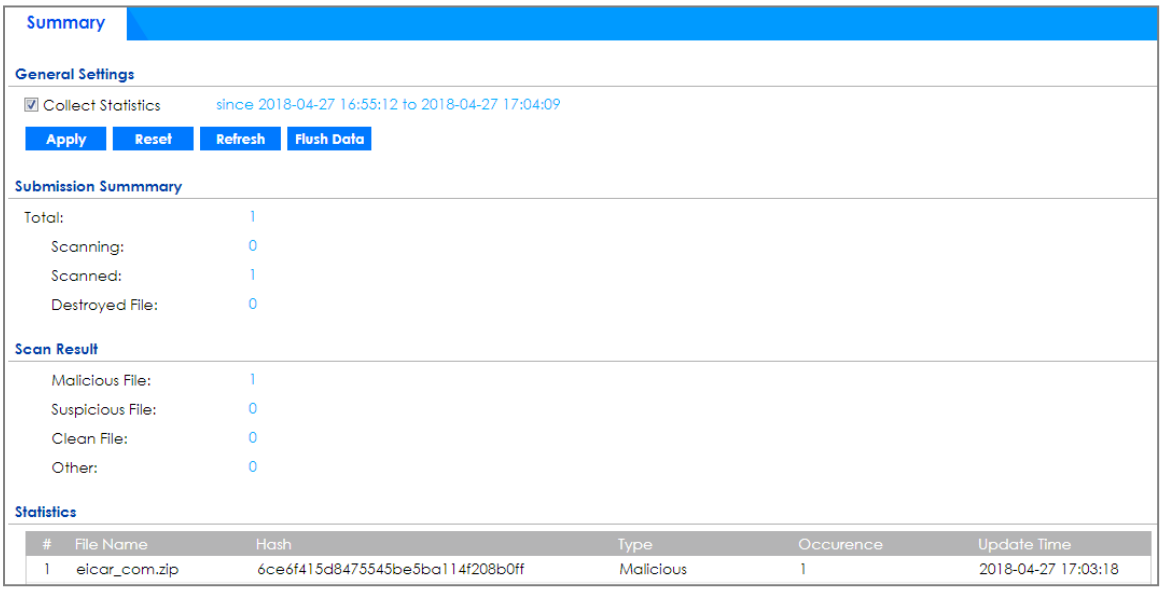
4 When you download eicar_com.zip for the first time, it is considered to be an unknown malware. The file is allowed to pass and a copy of eicar_com.zip will be sent to Sandbox for further scan.

MONITOR > Log > View Log > Sandboxing



The eicar_com.zip file is detected by Sandbox as a malicious file.

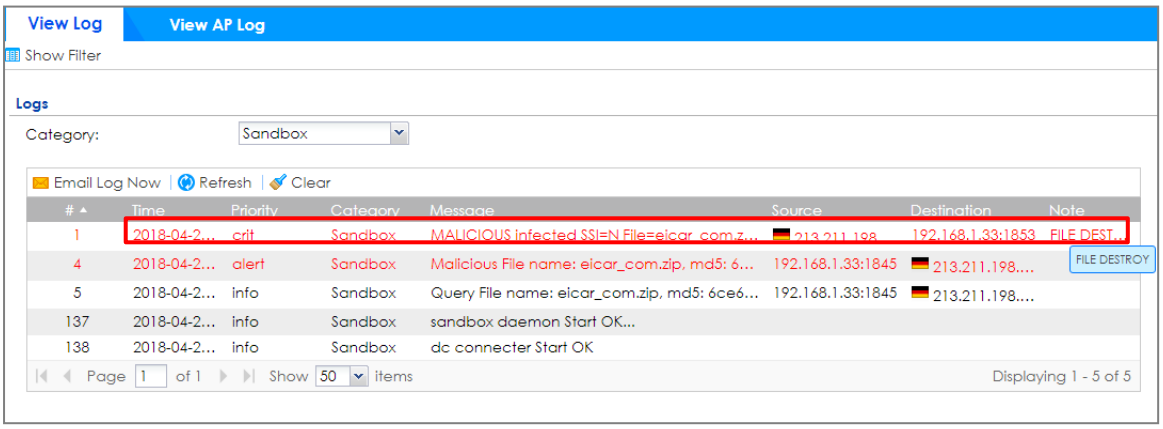
MONITOR > Security Statistics > Sandboxing



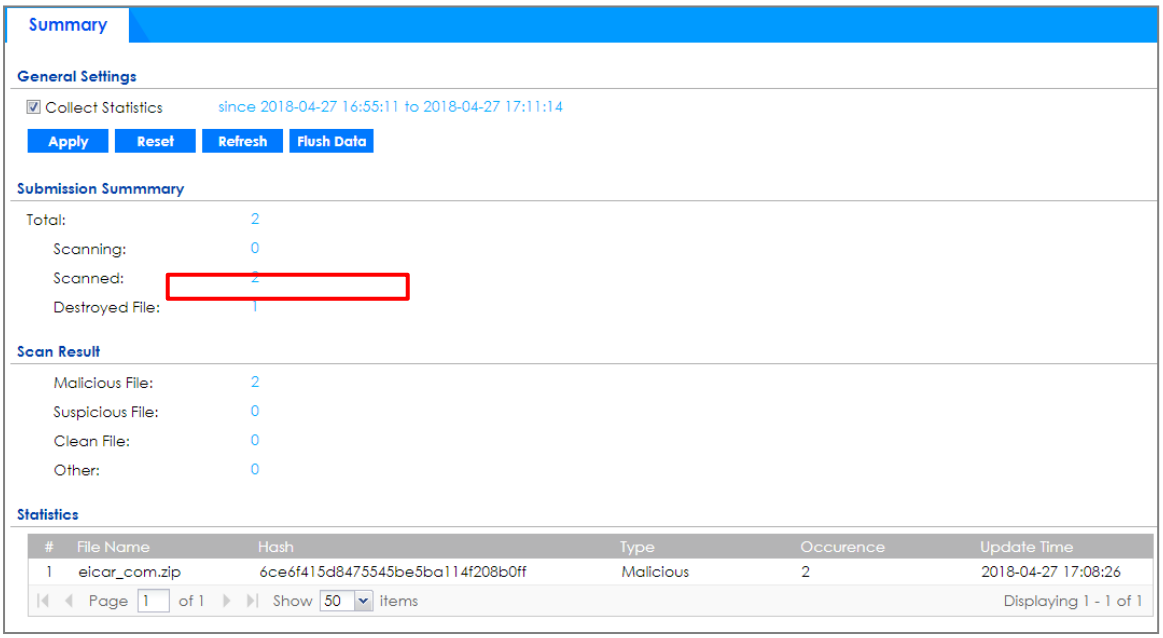
Note: Disable anti-virus software on your laptop in order to test Sandbox.

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



MONITOR > Security Statistics > Sandboxing



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

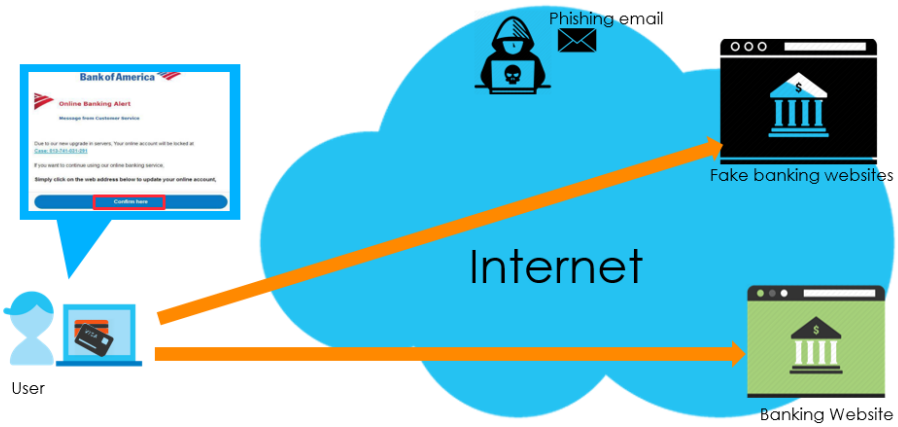


Figure 1 Using Sandboxing to Detect Unknown Malware

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.

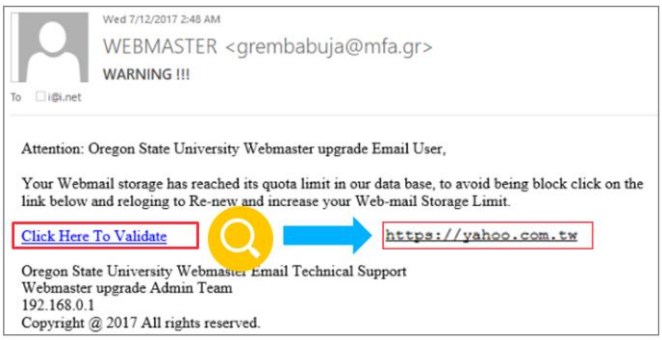
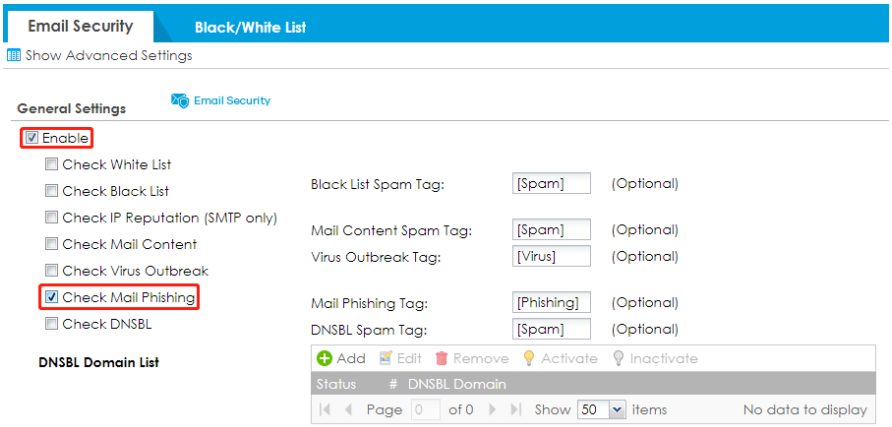


Figure 2 Phishing mail example

Set up Phishing on ATP

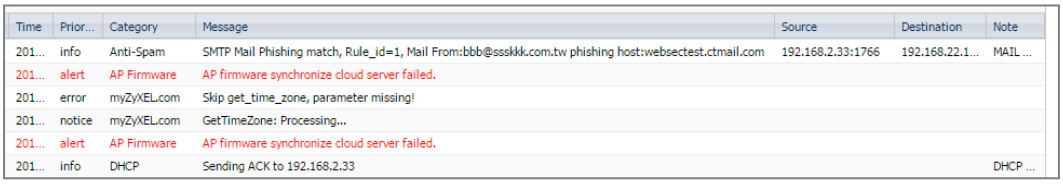
In the ATP, Go to **Configuration > Security Service > Email Security** to enable Check Mail Phishing that allows gateway inspects the embed URLs in the email



Test the Result

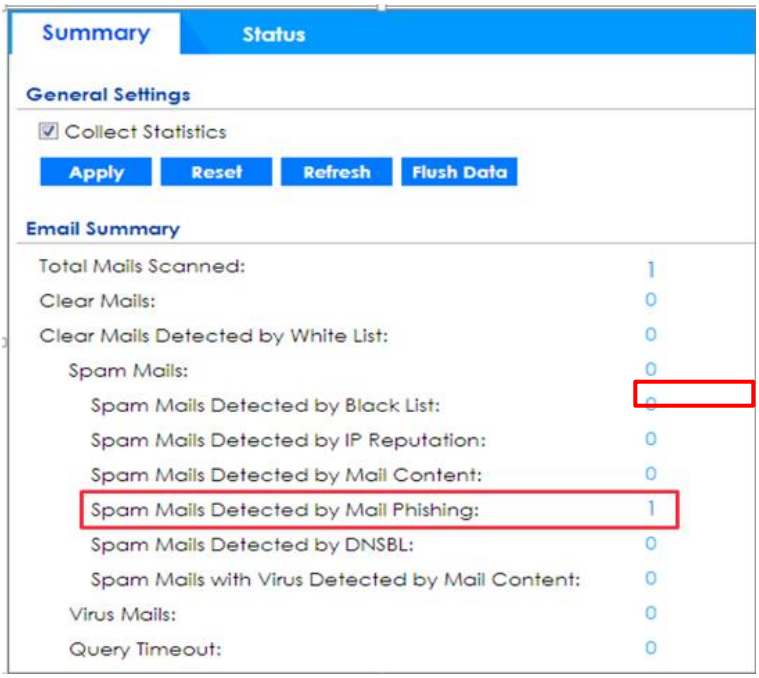
1 Go to **Monitor > Security Statistics > Email Security** to observe mail phishing logs

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



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

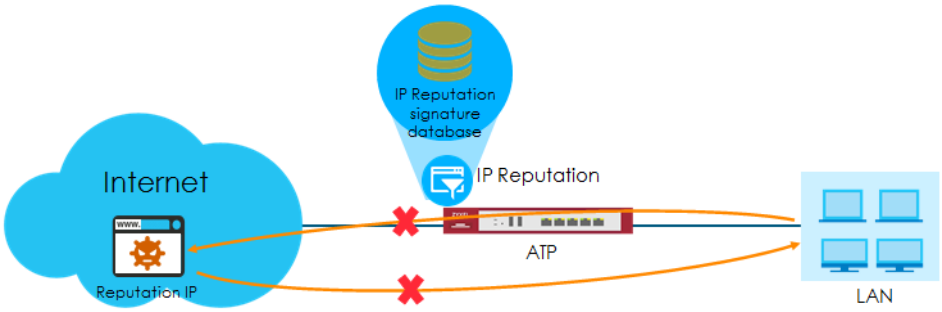
How to Use IP Reputation to Detect Threats

(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.



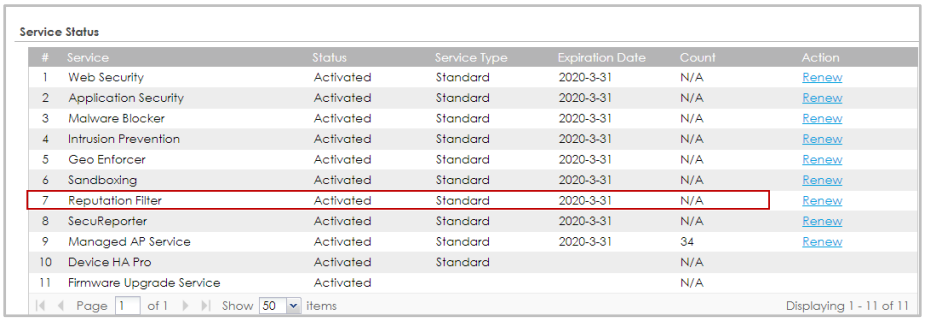
Figure

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).

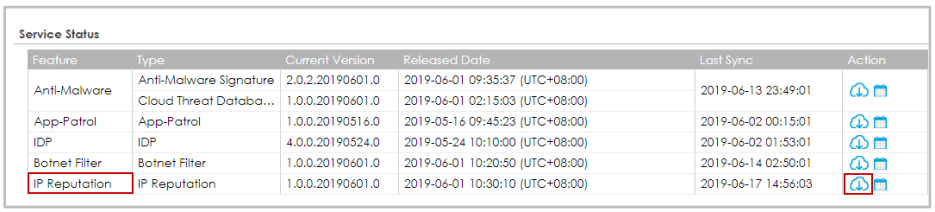
Activating Reputation Filter Service

1 Register ATP gateway to myZyxel.com.

2 Activate Reputation Filter license.

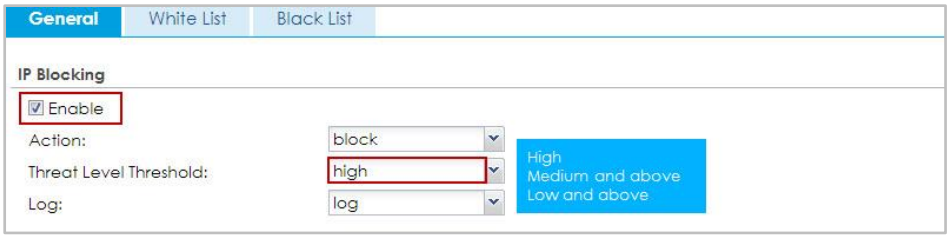


3 On ATP, go to **CONFIGURATION > Licensing > Signature Update.** Click the **Update** icon to check for new signatures.



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.

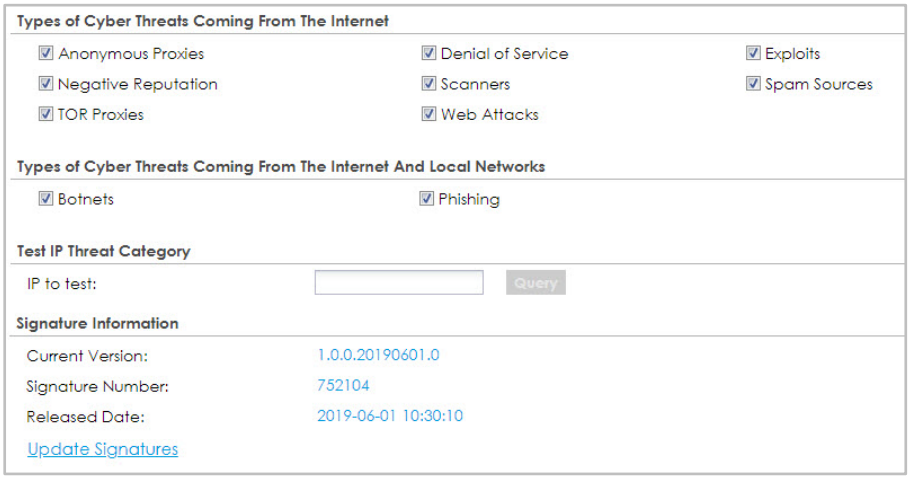


Selecting specific type of IP addresses to block

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.

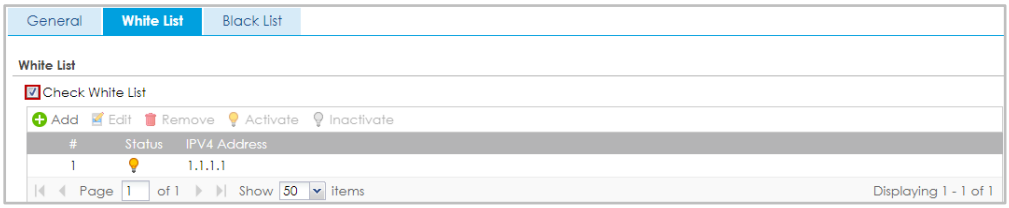
In Types of Cyber Threats Coming From The Internet And Local Networks, select the type of threats that are known to pose a security threat for both incoming

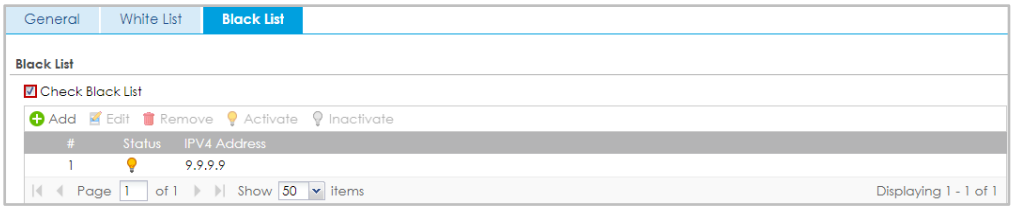
and outgoing traffic.



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.

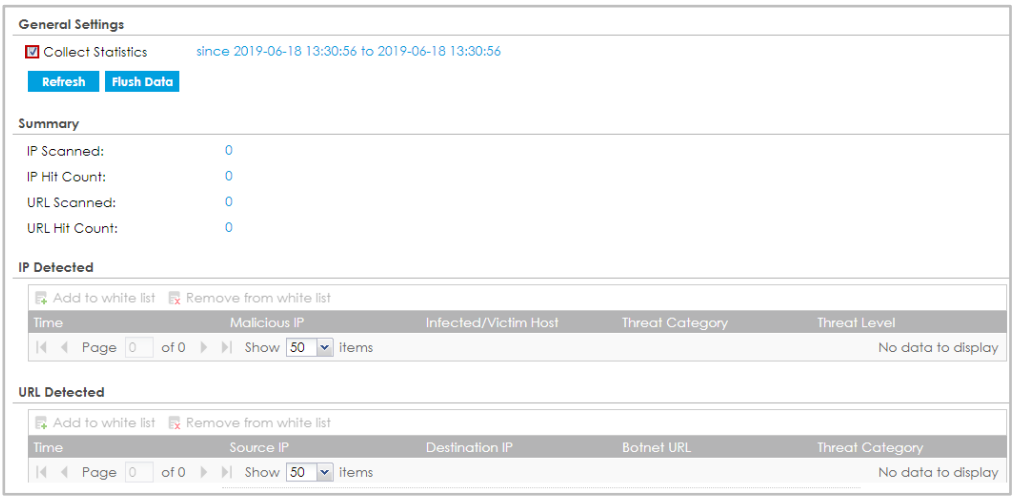




Monitoring statistics for IP detection

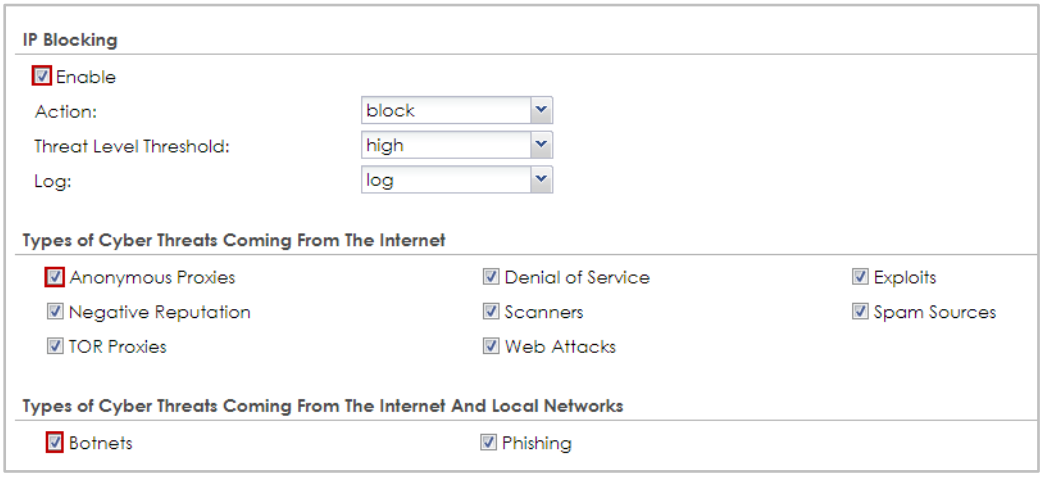
Enable Collect Statistics to monitor the scanned result and detected IP.

MONITOR > Security Statistics > Reputation Filter

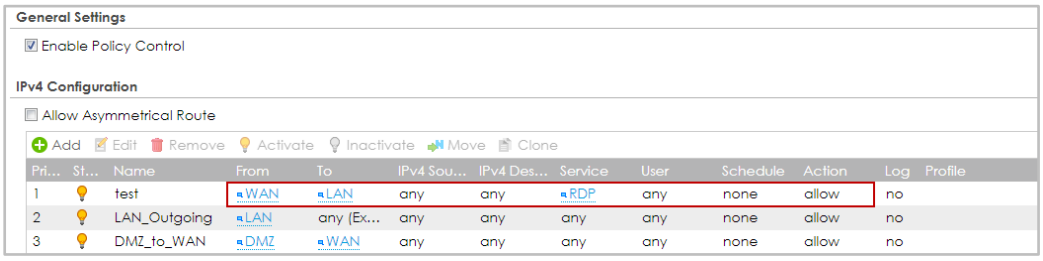


Test the Result

1 Select Anonymous Proxies for detecting incoming traffic and Botnet for outgoing traffic.



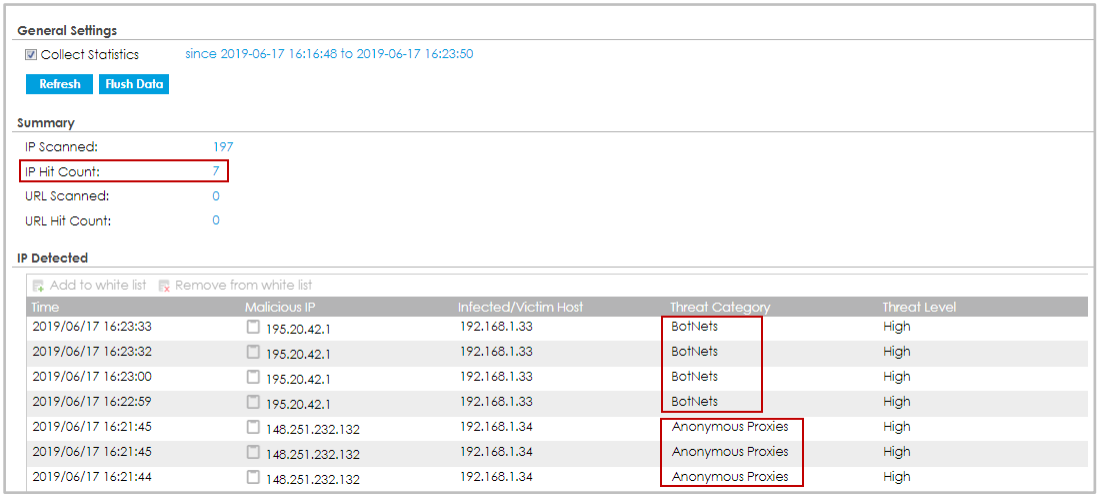
2 For incoming traffic, set a NAT rule and add a security policy rule for allowing traffic from WAN to LAN.



For outgoing traffic, ping an IP address in the threat category "Botnets" from LAN.

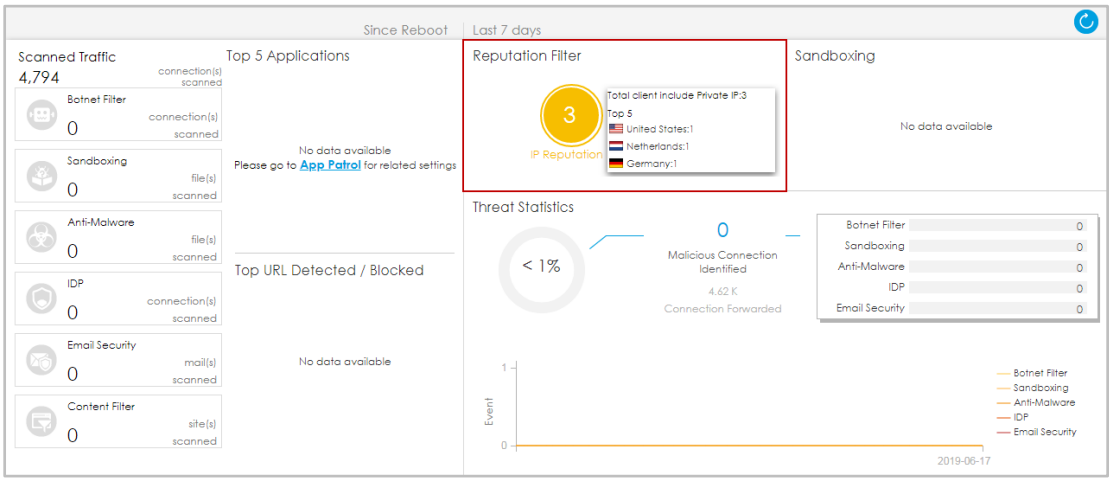
3 Check statistics for detected IPs.

MONITOR > Security Statistics > Reputation Filter



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.

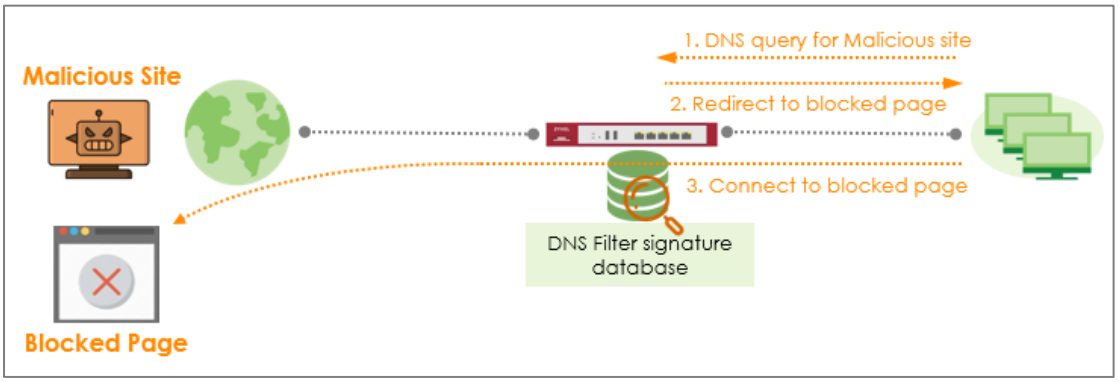
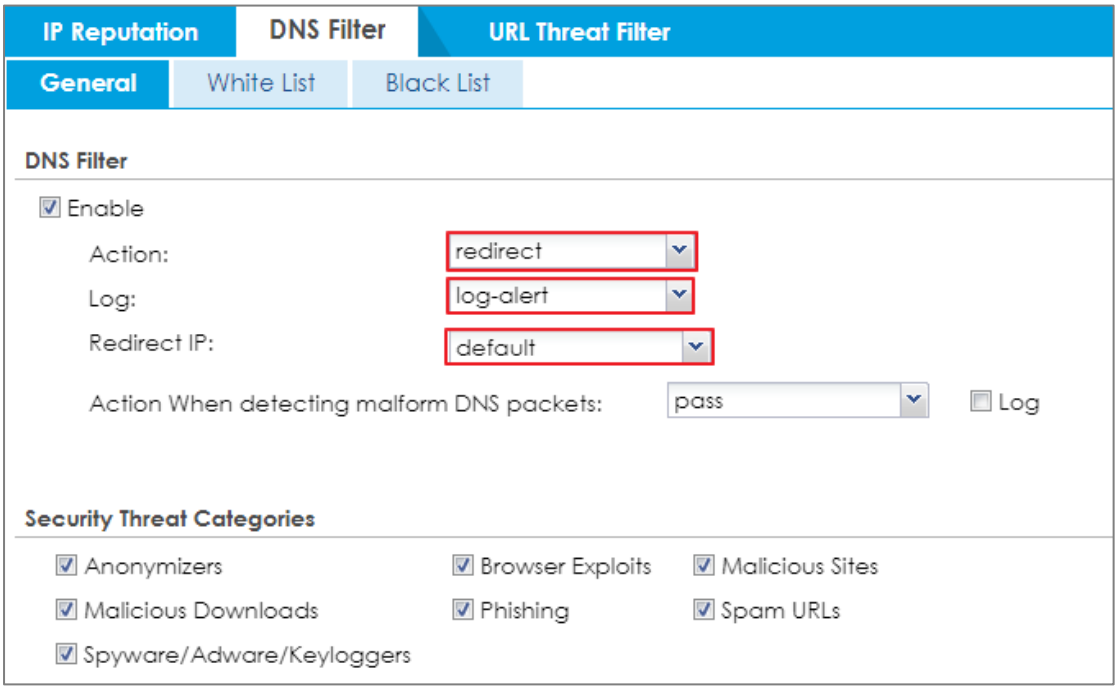


Figure. DNS Filter protects user from malicious websites

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).

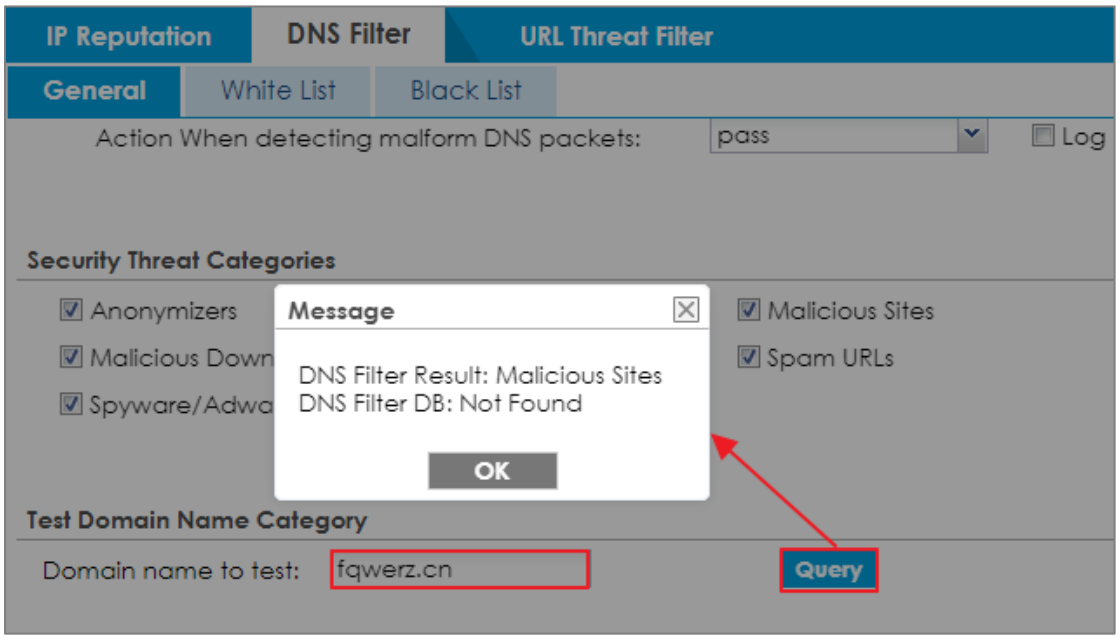
Set Up the DNS Filter on ATP Series

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.



Test the Result

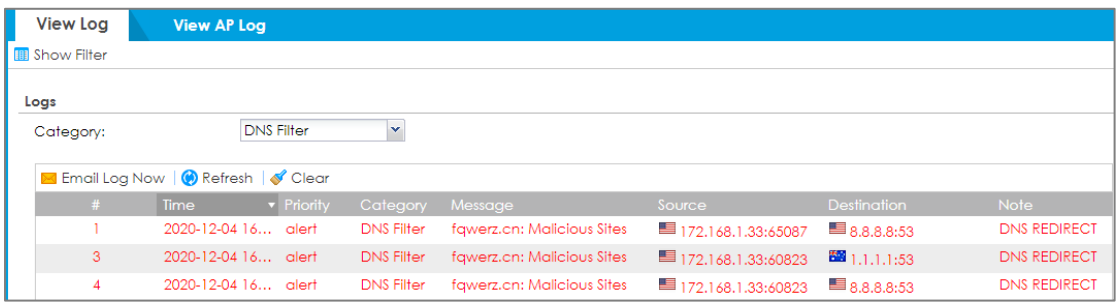
Verify a domain name in the Security Threat Categories. Go to **CONFIGURATION** > **Security Service**> **Reputation Filter**>**DNS Filter**; enter a malicious domain to test:



Using Web Browser to access the malicious site. The gateway will redirect you to blocked page.

Go to **Monitor**>**Log**, select DNS Filter category.

Log message will be appeared after the profile of DNS Filter be hit.



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.

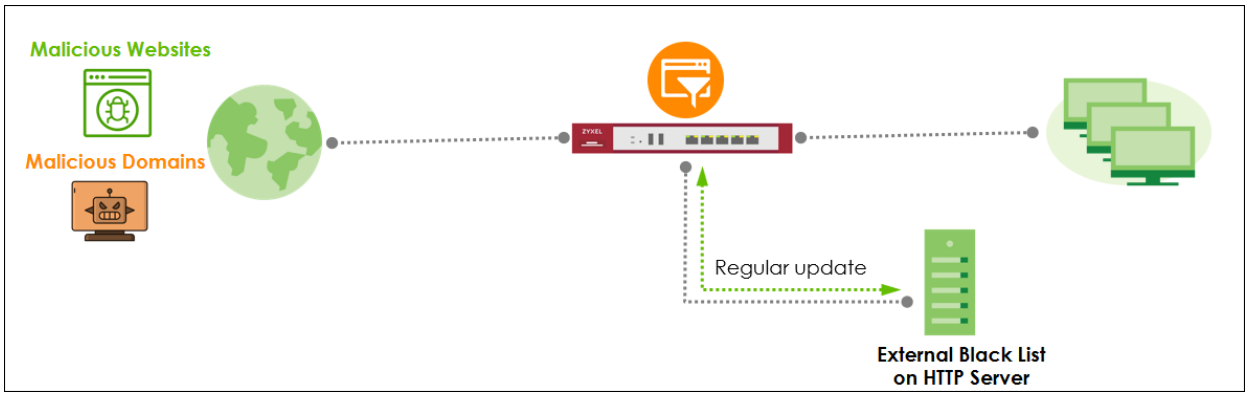
   You have subscribed for the **DNS Filter** service but the license (**Gold Security Pack Standard**) is expired.

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)

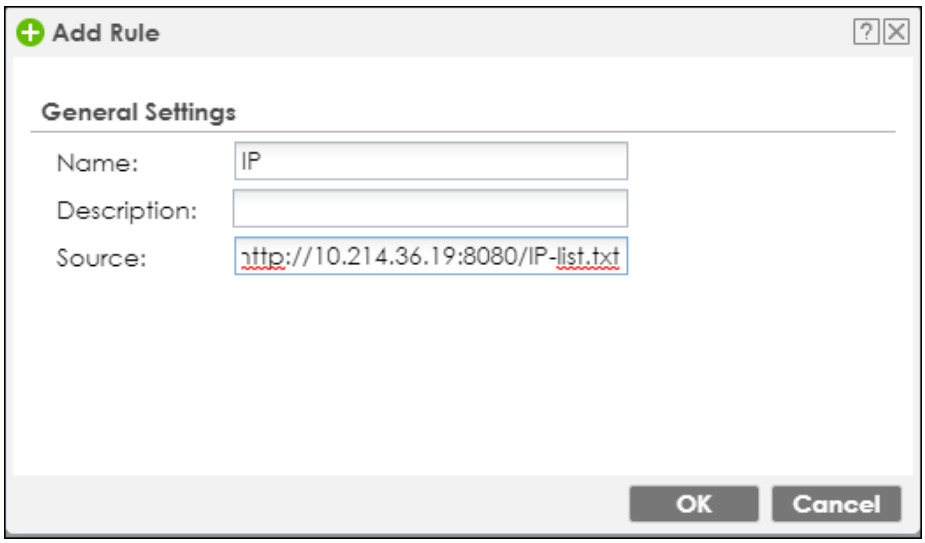
After configured list completely, you can save your .txt file on your HTTP server. (e.g. Software: HTTP File Server)

Configure External Block list setting

IP Reputation

Go to Configuration > Security Service > Reputation Filter > IP Reputation > External Black List.

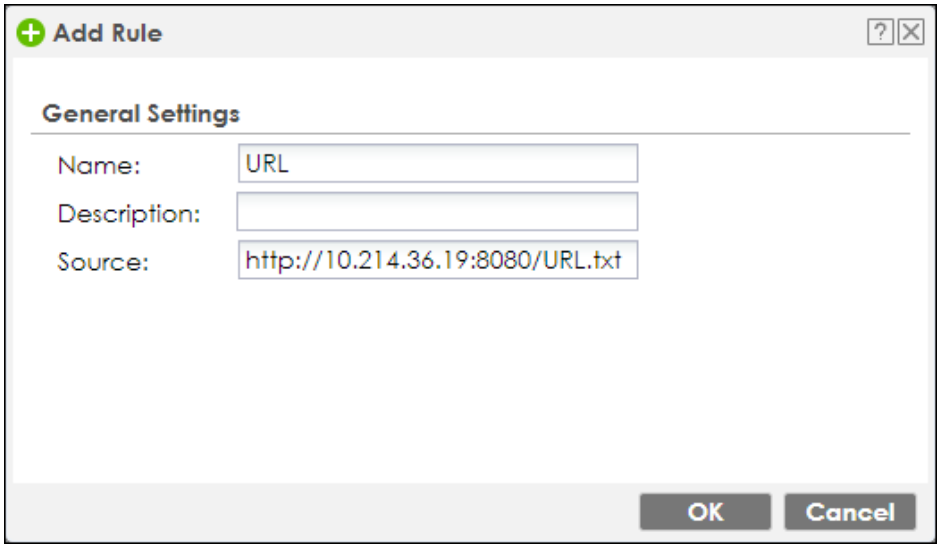
Click Add button to download source on your HTTP Server.



URL Threat Filter

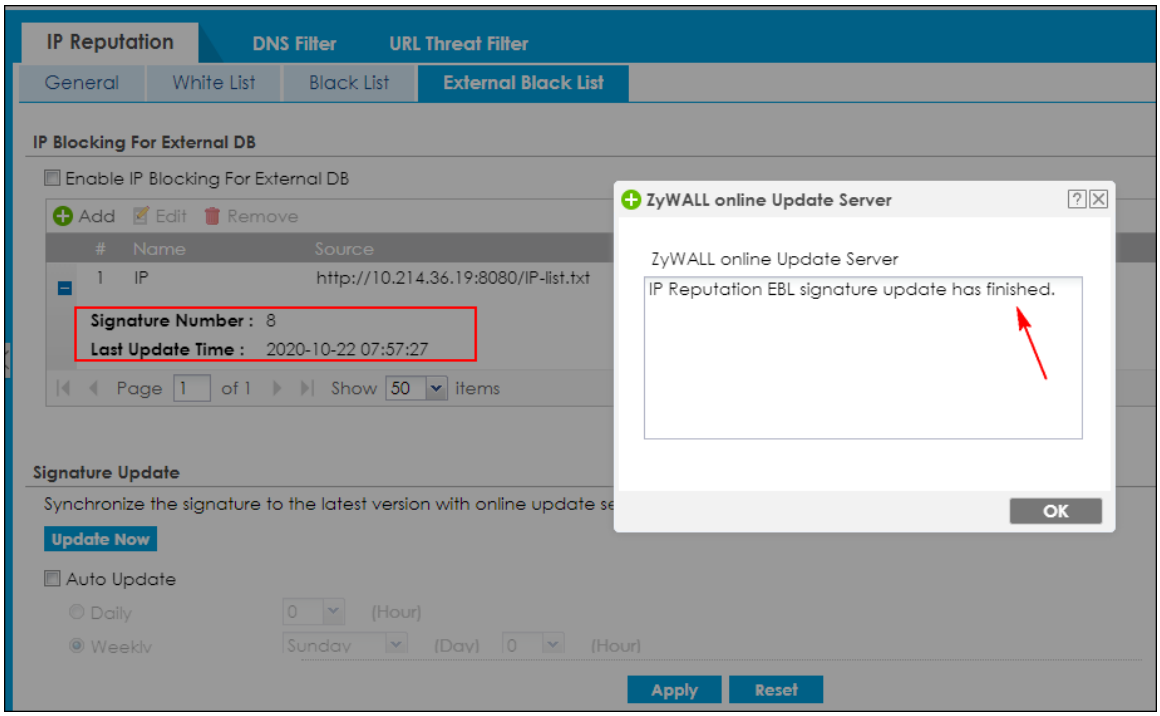
Go to Configuration > Security Service > Reputation Filter > URL Threat Filter > External Black List.

Click Add button to download source on your HTTP Server.

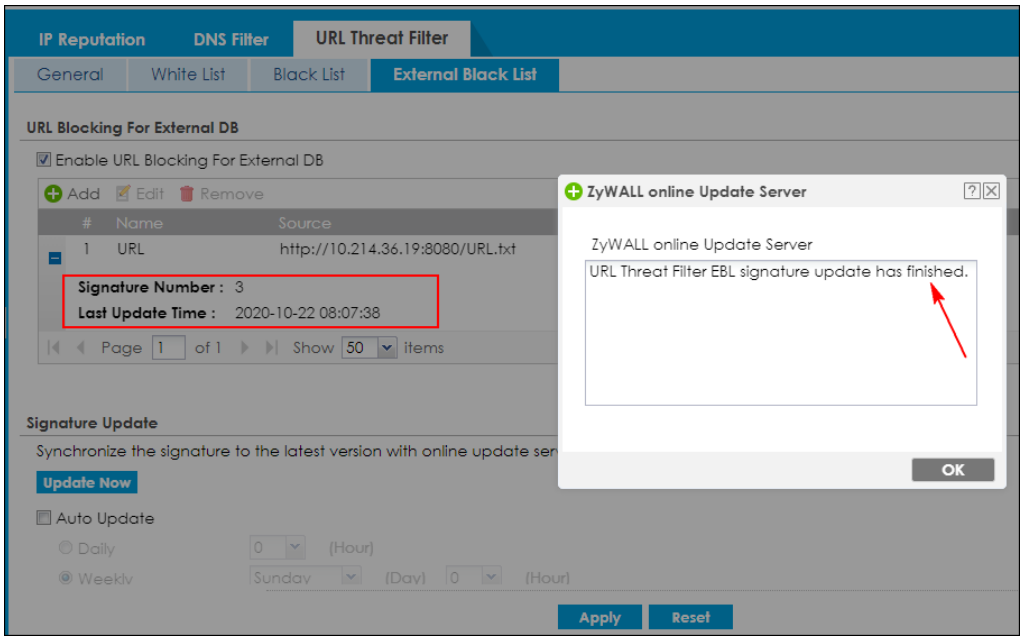


Check External Block List update status

IP Reputation



URL Threat Filter

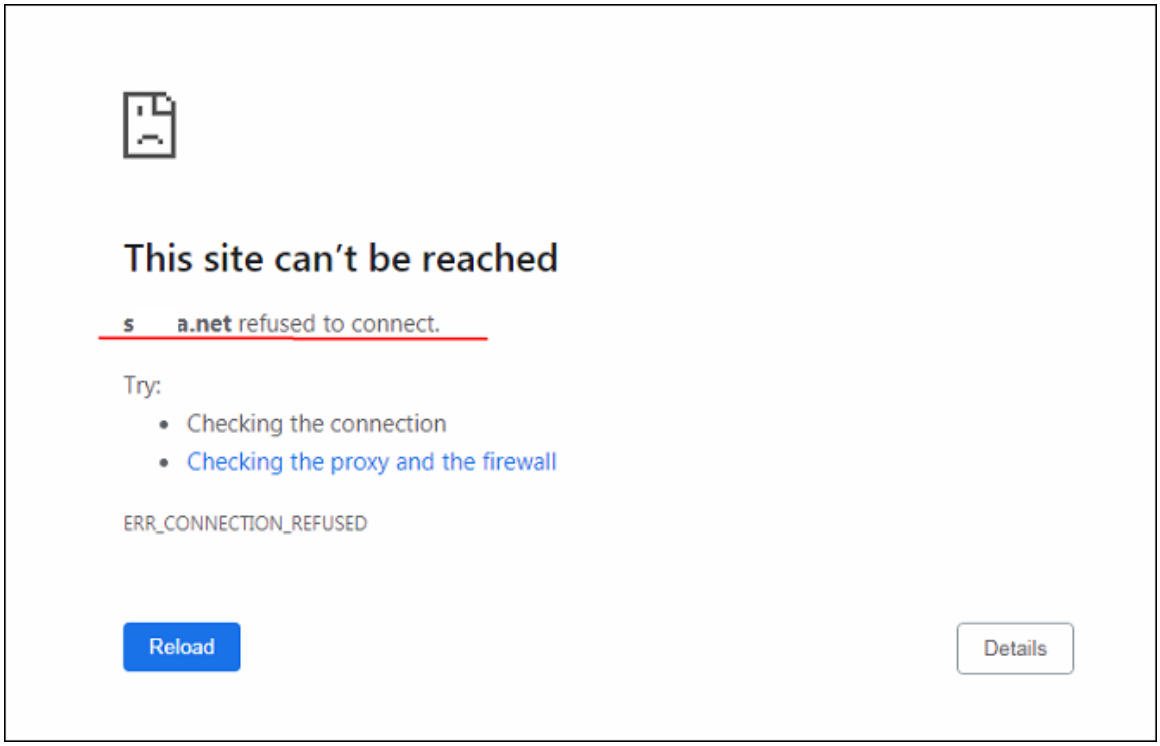


Note: Please must make sure **block list format** in your ".txt" file correct. Otherwise the data will unable import to system completely. You can check "**Signature Number**" if amount is the same as your list.

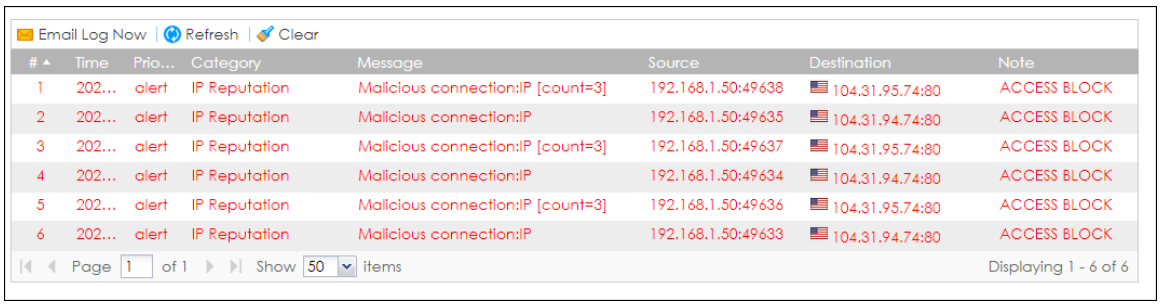
Verification

IP Reputation block page

If client traffic is blocked by IP Reputation, website will unable to access to will display it.

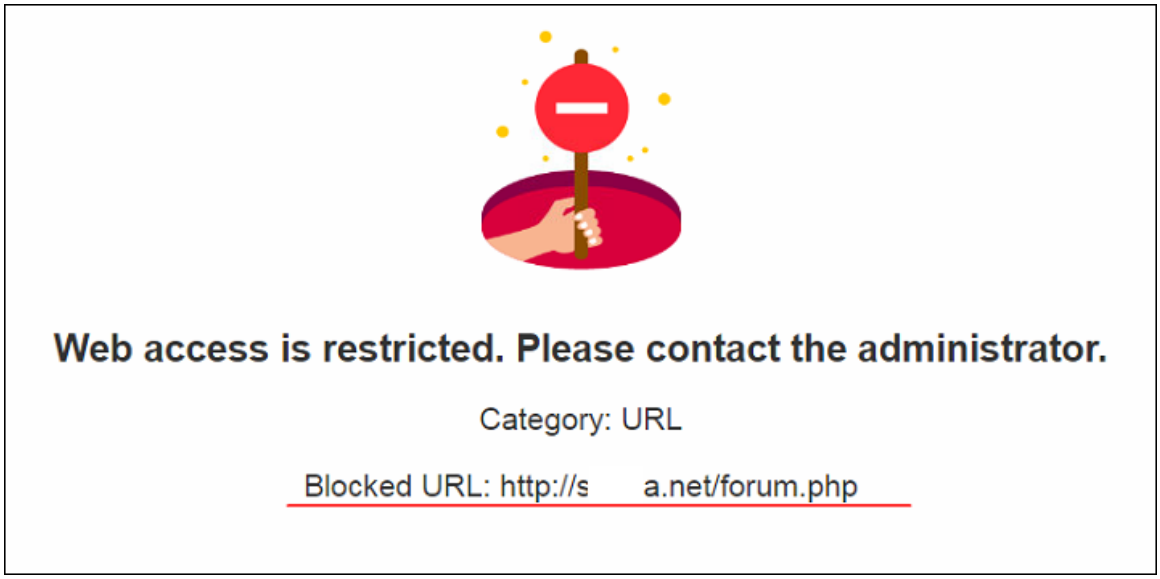


IP Reputation Log

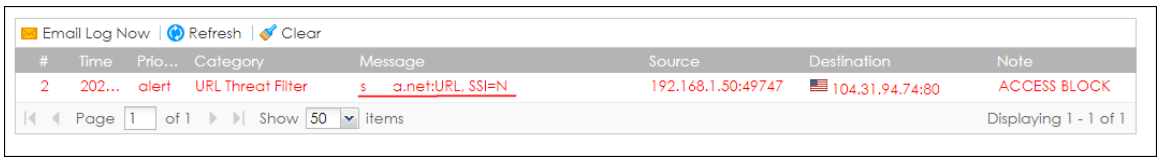


URL Threat Filter

If client traffic is blocked by URL Threat Filter, website will unable to access to will display it.



URL Threat Filter Log



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.

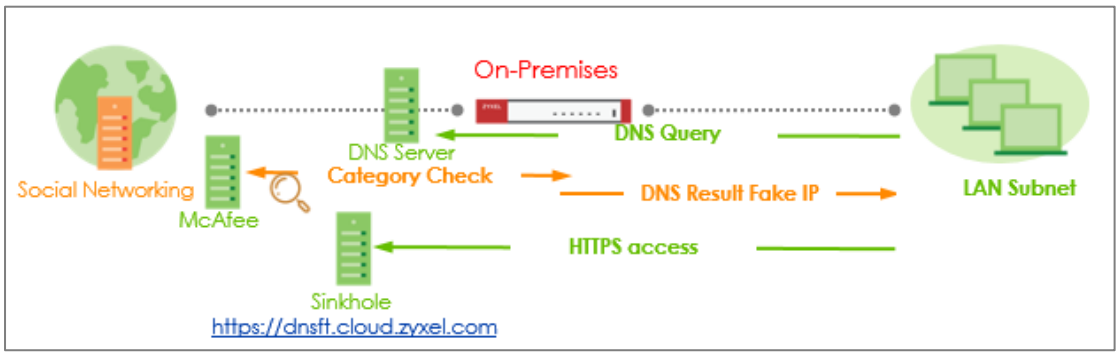


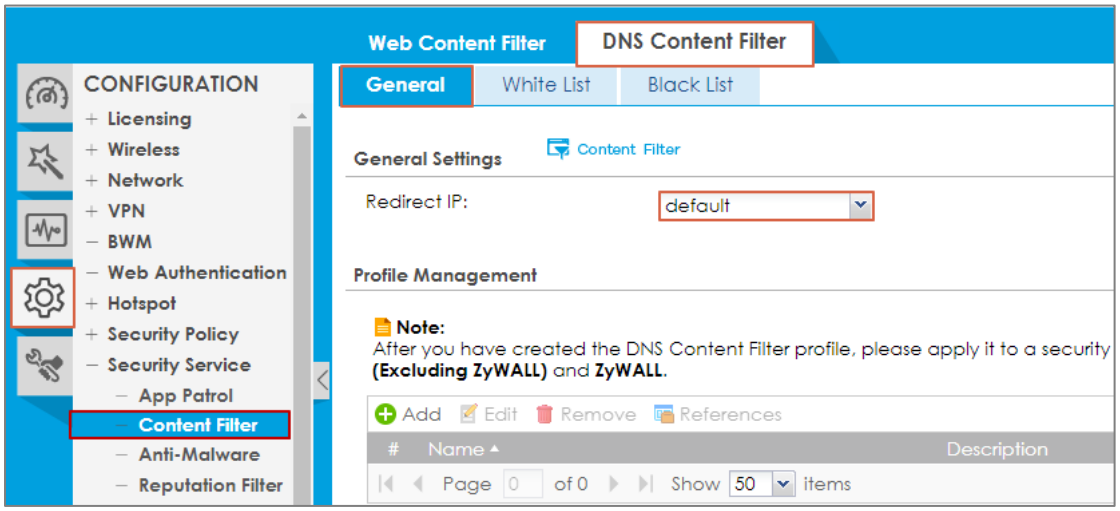
Figure: DNS Content Filter protects user to inappropriate website

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).

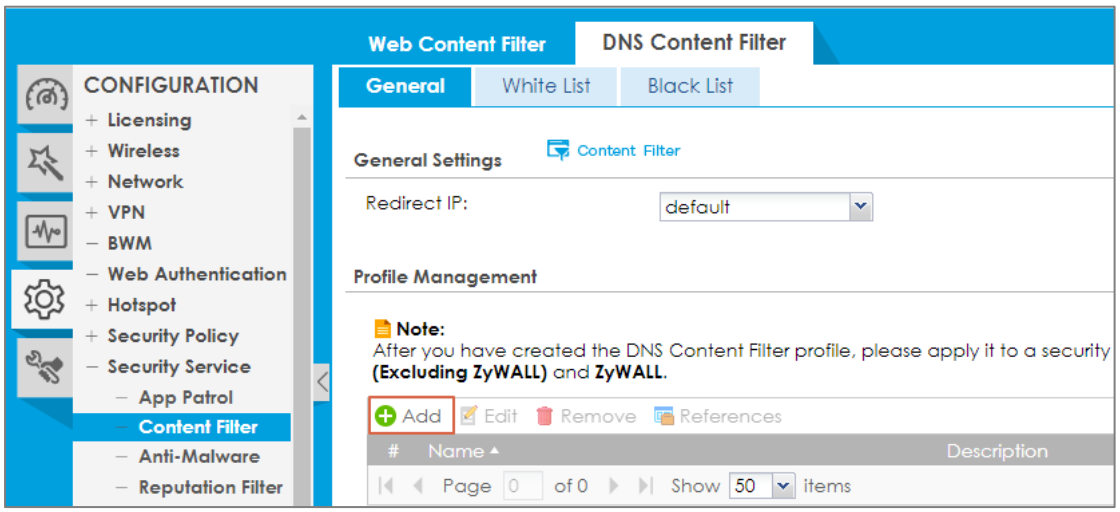
Set Up the DNS Content Filter on USG Flex Series

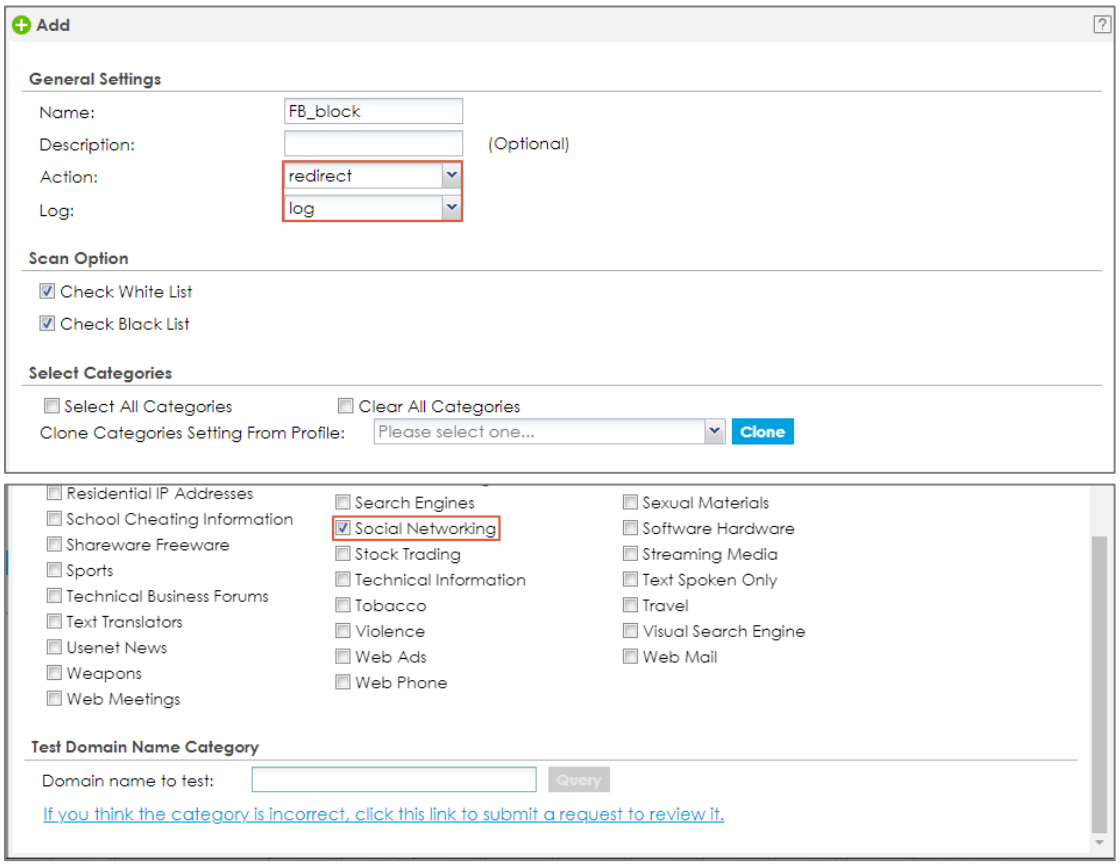
In the USG Flex Web GUI, go to **Configuration** > **Security Service**> **Content Filter**>**DNS Content Filter**; Select Redirect IP to indicated IP address or default one. If user selects the default, when client hit DNS Content Filter profile, the page will be redirect to block page http://dnsft.cloud.zyxel.com/.

If user selects the custom defined, the page will be redirect indicated IP address.

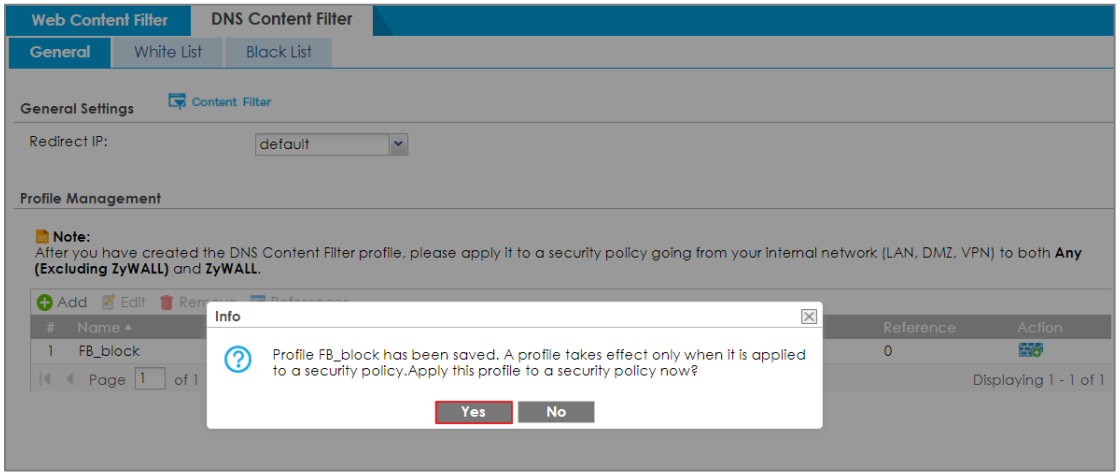


Add profile on the general page. Select **Redirect** on action field, and choose **Log** on log field. Click **Social Networking**(as Example) on managed categories.

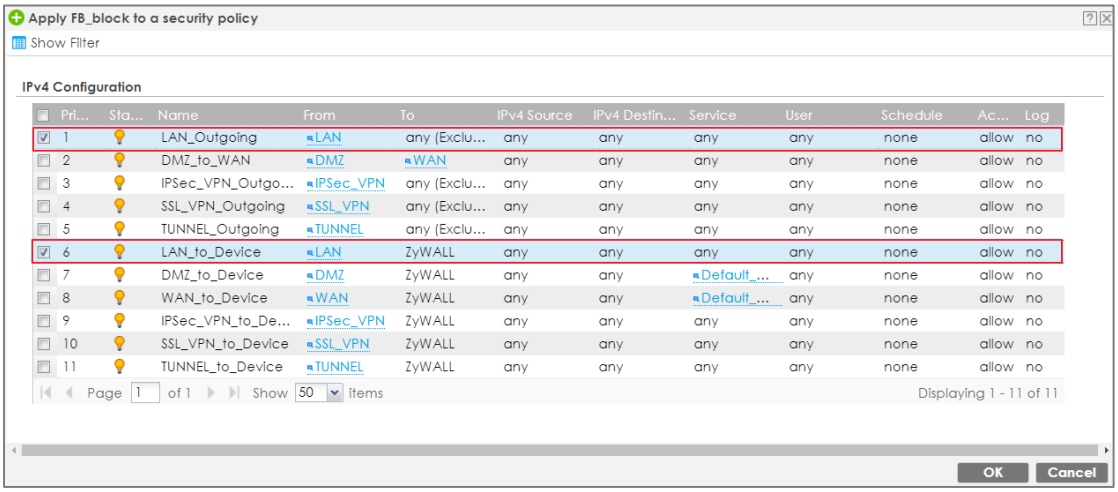




Once the DNS Content Filter profile is created, a windows shows up to instruct you to apply this profile to security policy. Click **Yes** to continue



Please apply this profile to a security policy going from your internal network to both **Any (Excluding ZyWALL)** and **ZyWALL**.

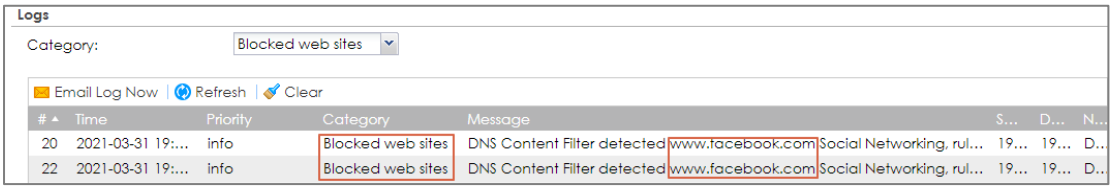


Test the Result

When you access Facebook.com which is in Social Networking Category, the Web Access will be redirected to block page.

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.



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.

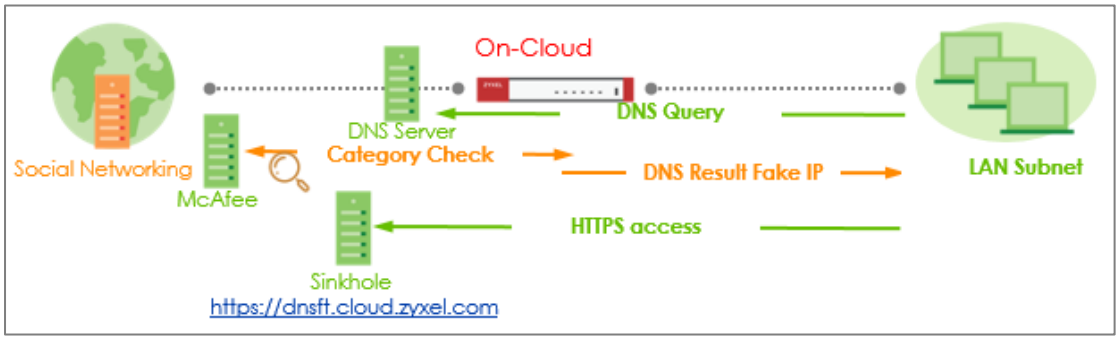


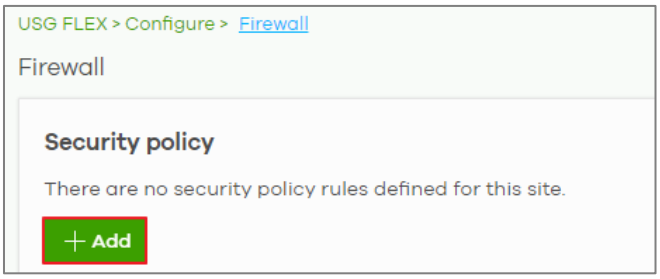
Figure: DNS Content Filter protects user to inappropriate website

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).

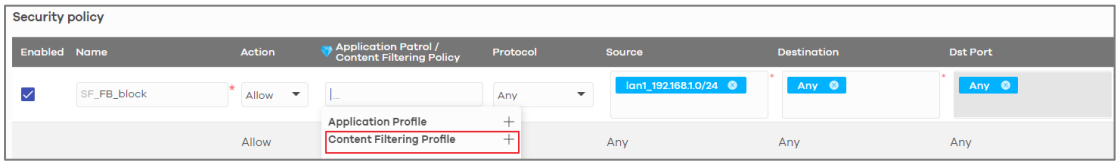
Set Up the DNS Content Filter on Nebula

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**

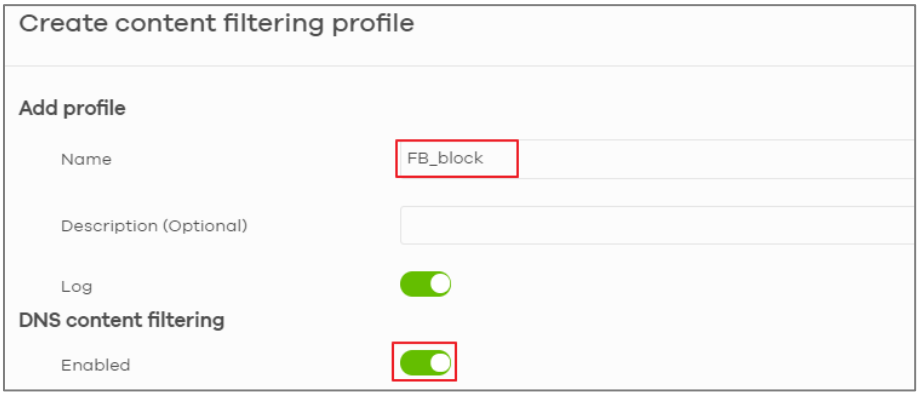
In **Security policy**, click **Add** to create a new rule



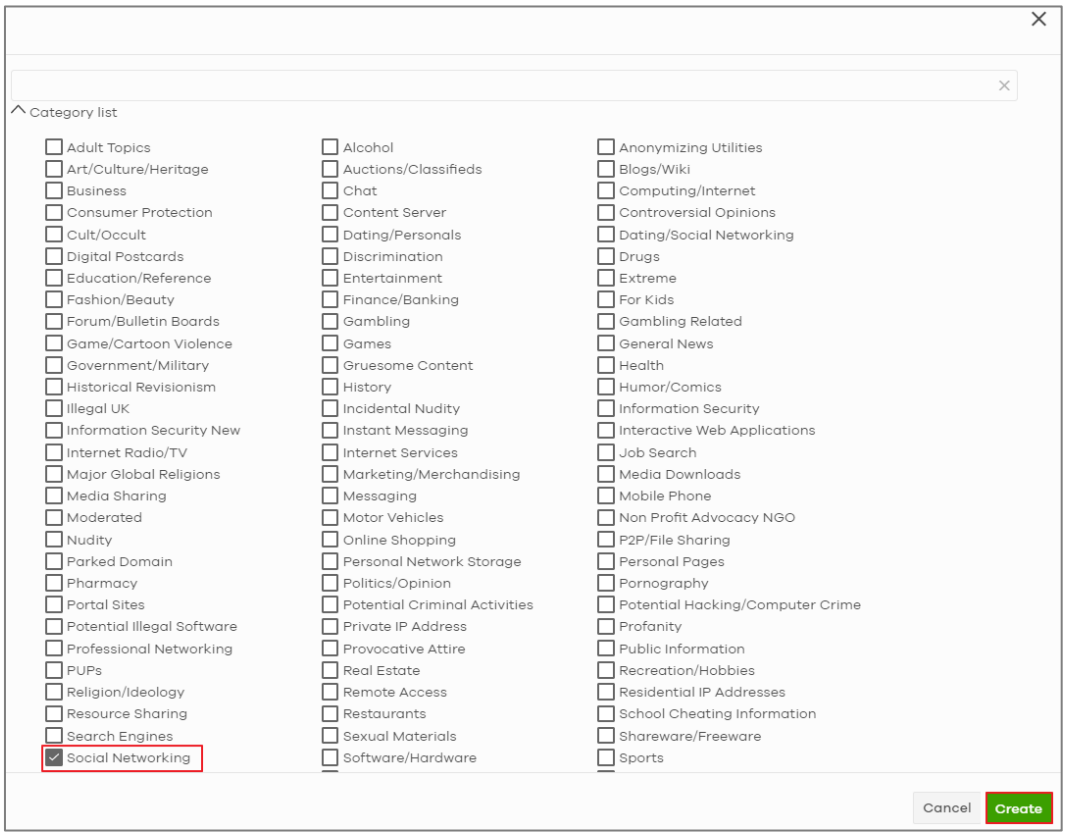
Name the rule, select Allow in **Action**, Lan1 in **Source**, Any in **Destination** field. In **Application Patrol / Content Filtering Policy** field, click [+] to add a new Content Filter profile



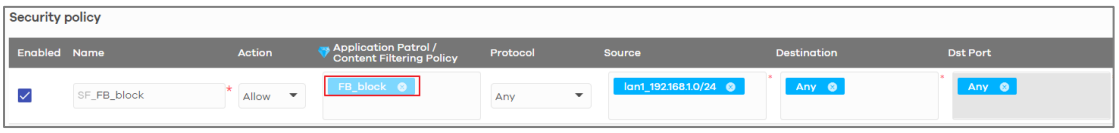
The DNS content filtering is a part of Content filtering feature, name the profile, scroll down, then enable DNS content filtering



Click the **category list,** select **Social Networking**, then press **Create** button



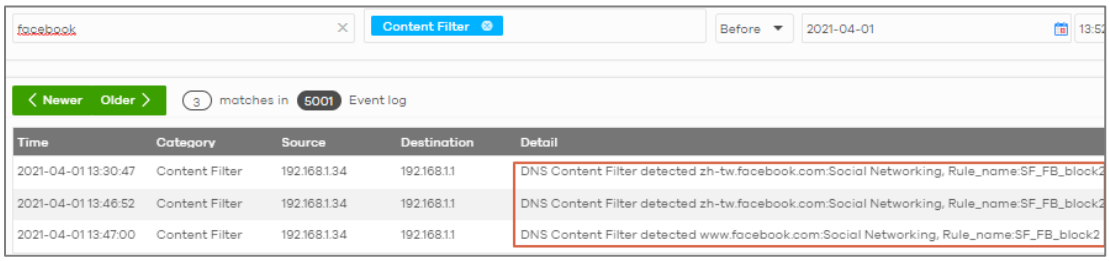
Make sure this profile is applied to the security policy



Test the Result

The Facebook has been restricted from access from users under LAN1, the user will see the block page instead.

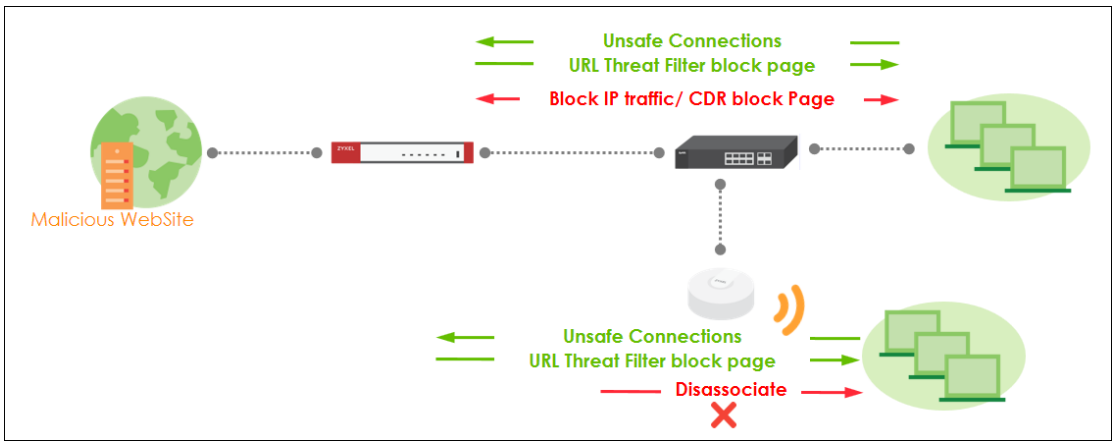
Go to the **Monitor**>**Even Log,** select the Content Filter category, Nebula will show the access to www.facebook.com has been blocked.



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.



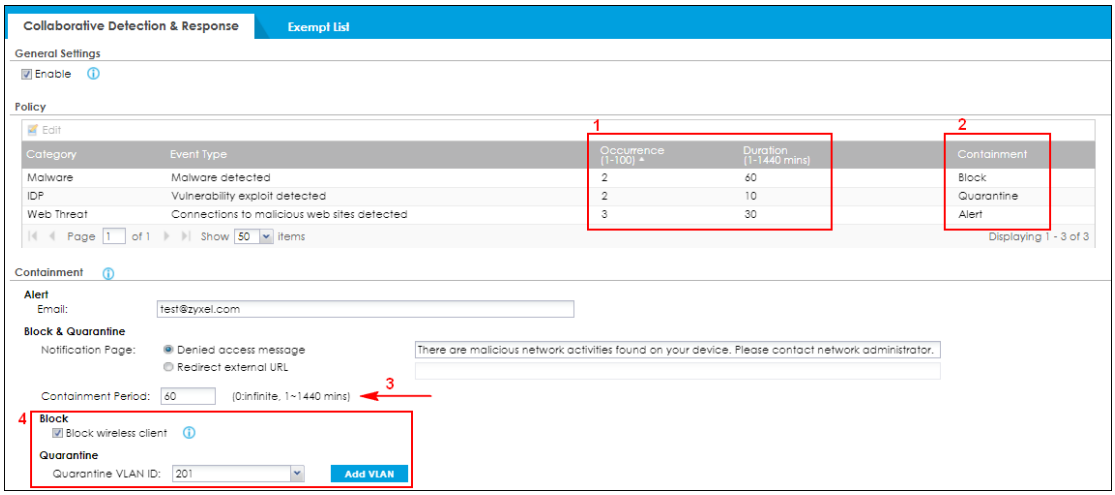
Note: In quarantine scenario, it can quarantine client to managed VLAN which has a third-party scanning server. The infected client can scan disk by third-party server or download required patch after quarantined.

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.



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:

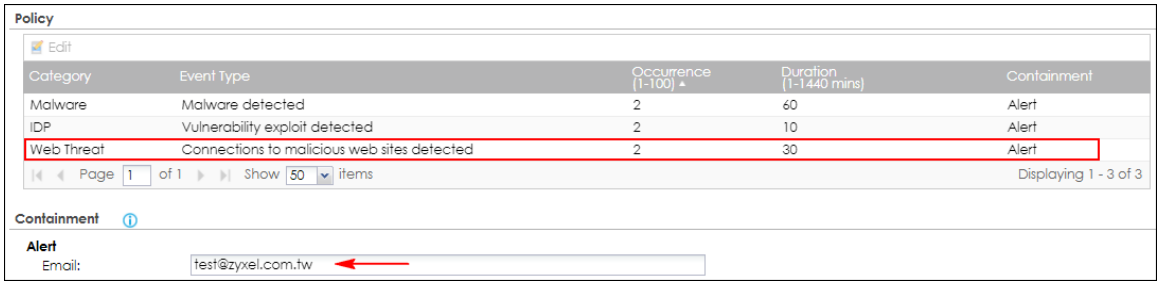
Wired Client: Block client IP traffic for a period time and show block page for client.

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.

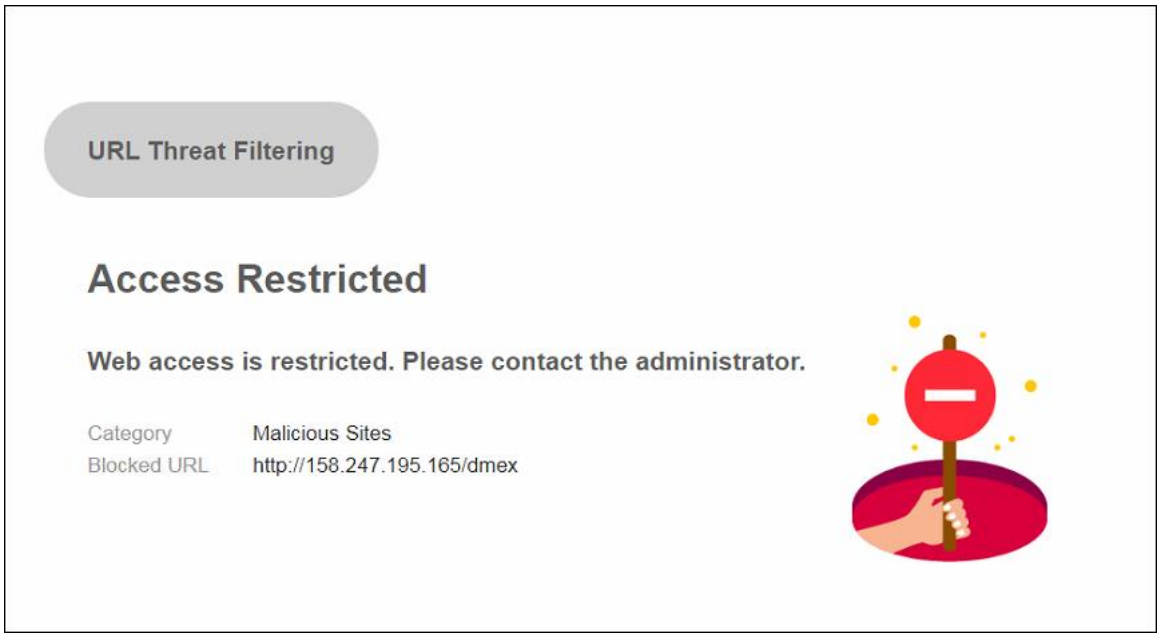
Verification

You can access to malicious website to verify behavior between different actions.

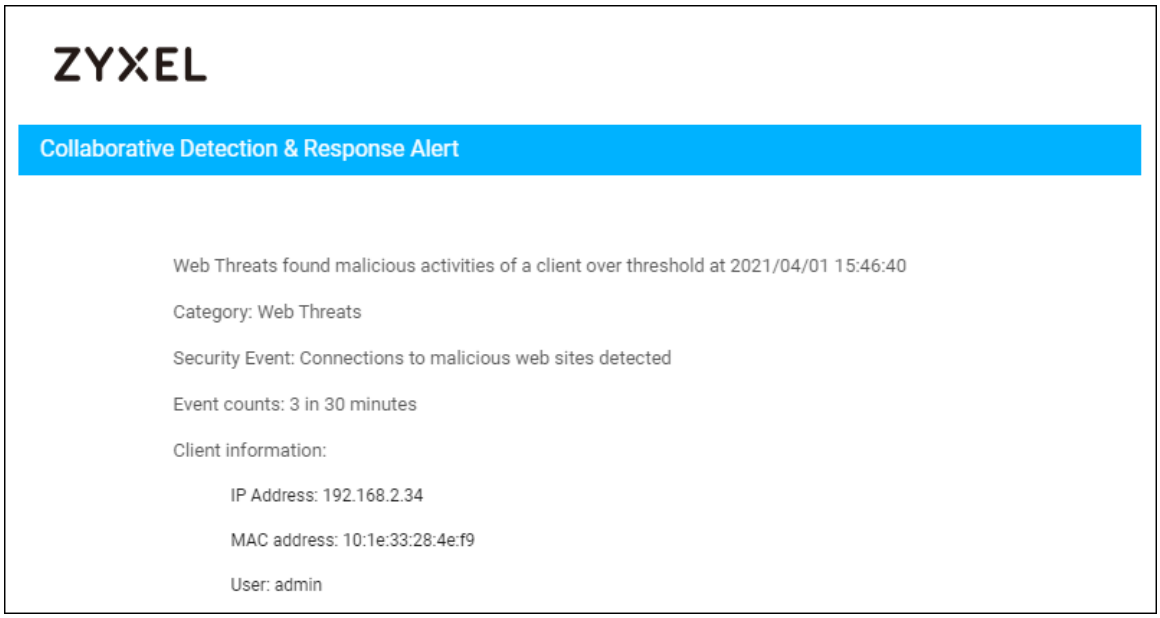
Alert:



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.

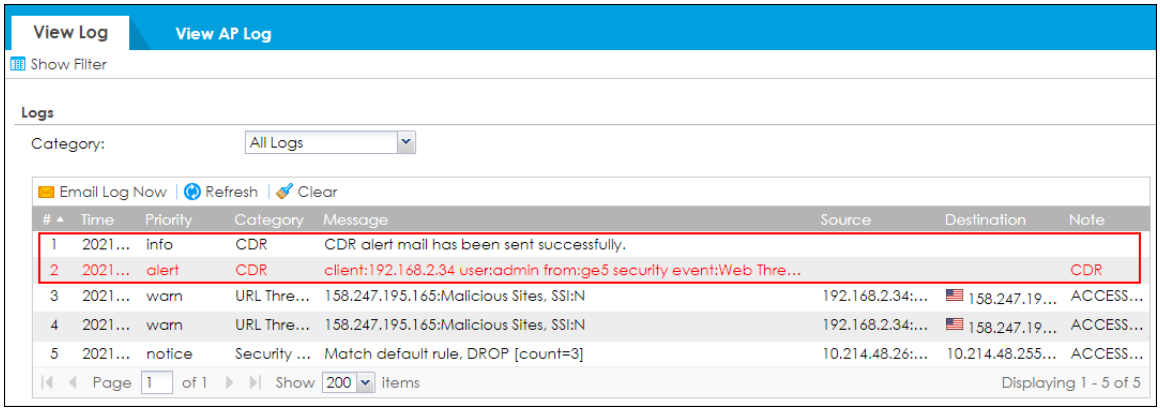


After connection reaching to the threshold, it will trigger gateway send alert mail you configured.



In mail, it will display CDR alert reason and client IP/MAC information.

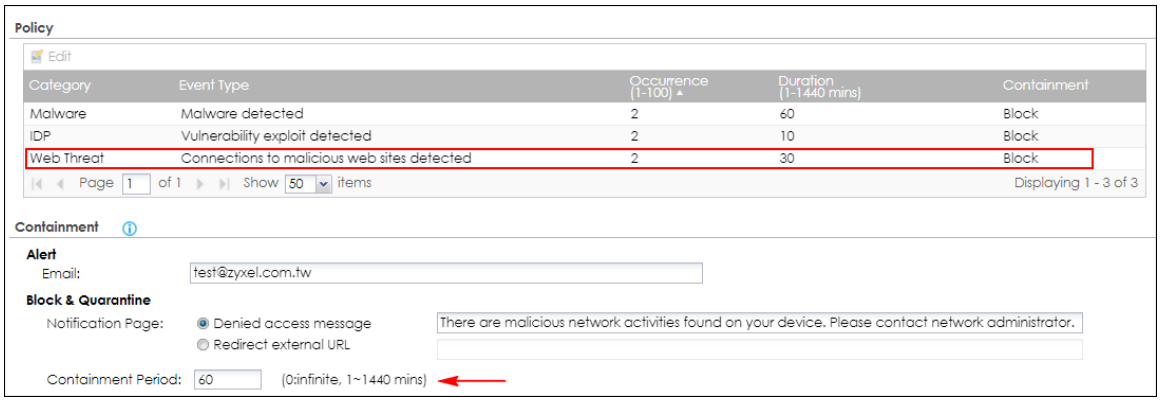
And also, you can check system log



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:

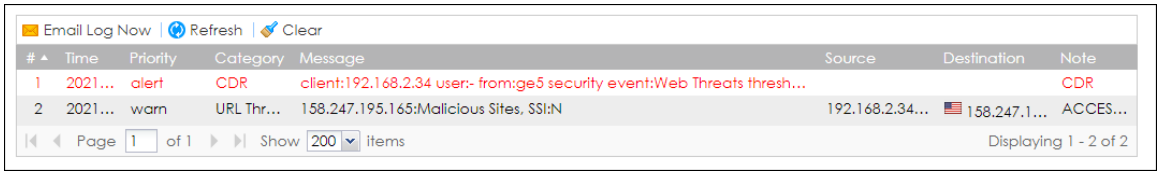


If client accesses to malicious website. The connection will be detected by Web Threat Filter service. So browser will display block page of Web Threat Filter page first. When connection reaches threshold, then all of client IP traffic will be blocked by CDR function in a period time.

On client browser, it will display CDR block page.

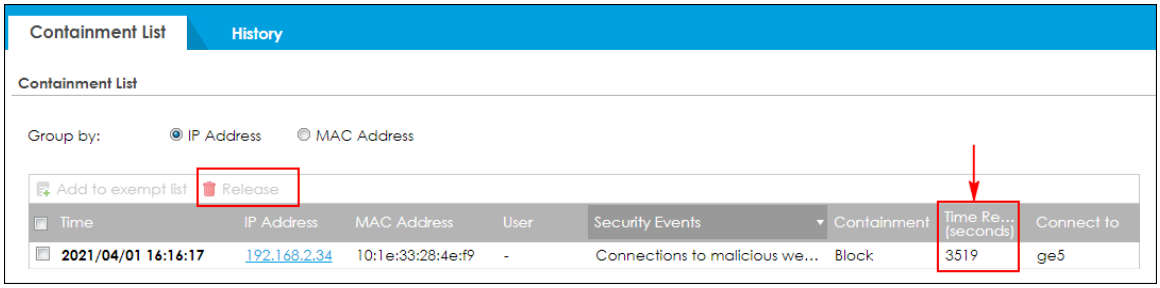
In block page, it will show block reason and client IP/MAC information.

System log:



You can also check containment list:

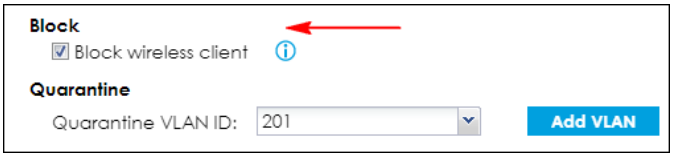
Monitor > Security Statistics > CDR



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.

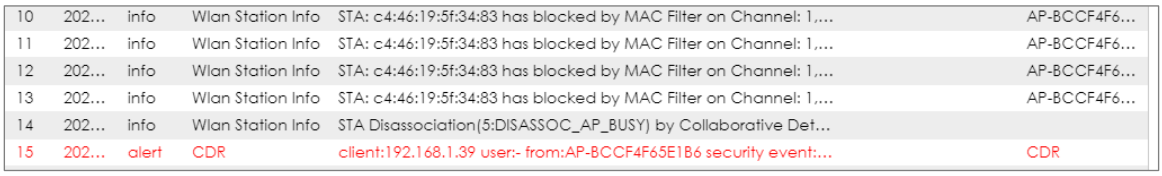
For wireless client. You can enable "Block Wireless client" checkbox to prevent the

wireless client re-associates to the AP.



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.

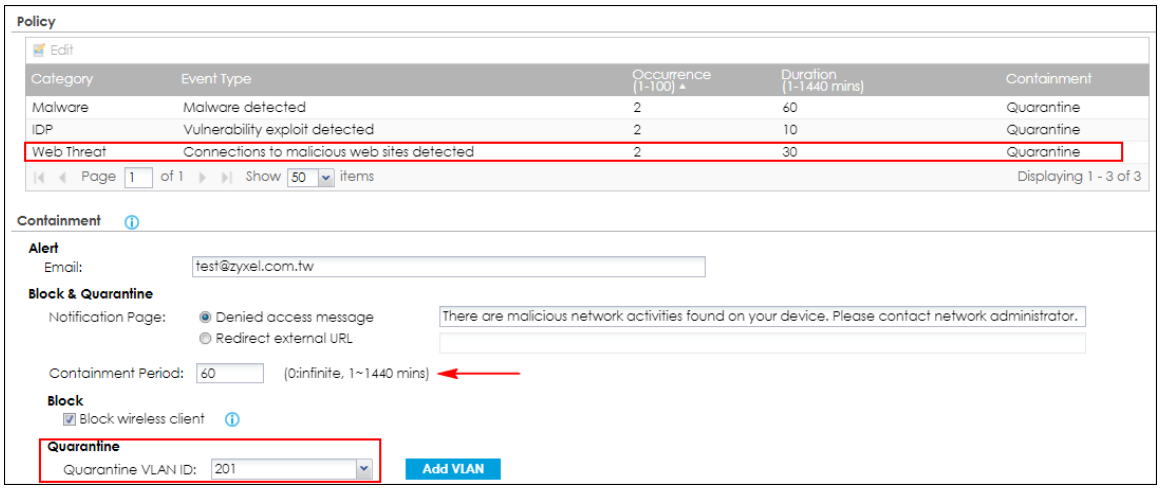
System log:



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

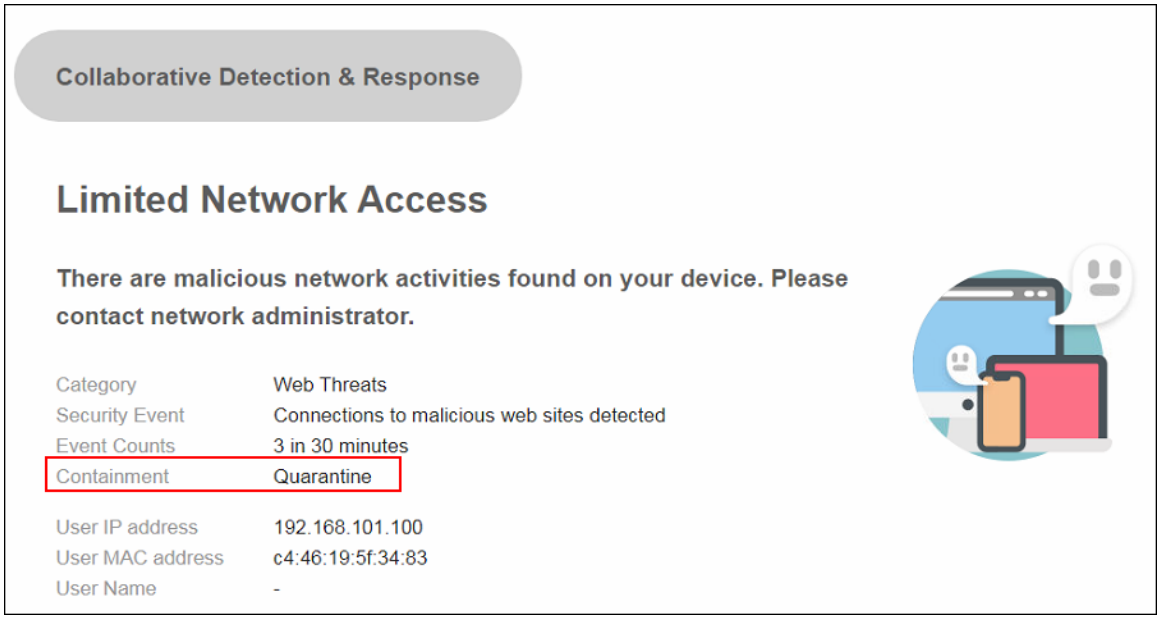
Note: If "Block Wireless Client" checkbox is disabled, the wireless client still keep connection with AP but traffic is blocked by CDR.

Quarantine:



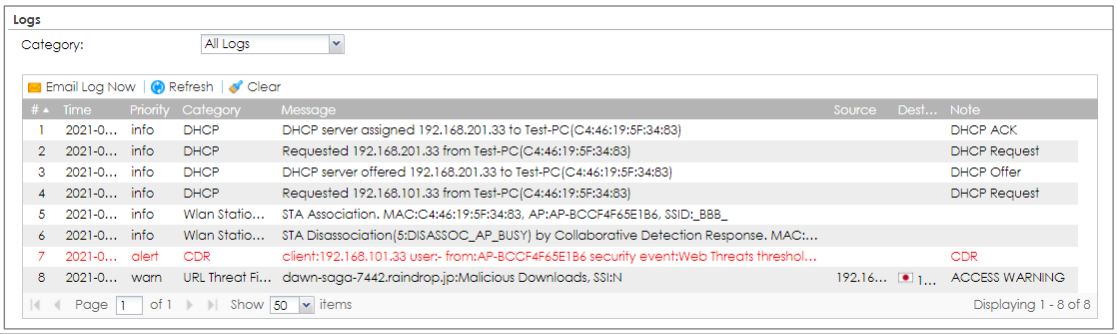
If client accesses to malicious website. The connection will be detected by Web Threat Filter service. So browser will display block page of Web Threat Filter page first. When connection reaches threshold, then all of client IP traffic will be blocked by CDR function in a period time.

On client browser, it will display CDR block page.

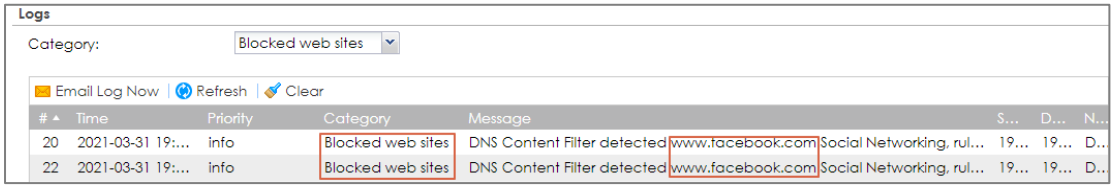


For wireless client, managed AP will disassociate to client. Client will be quarantined to configured VLAN after associating again.

In system log, client will get quarantined VLAN after associating with AP.



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.



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

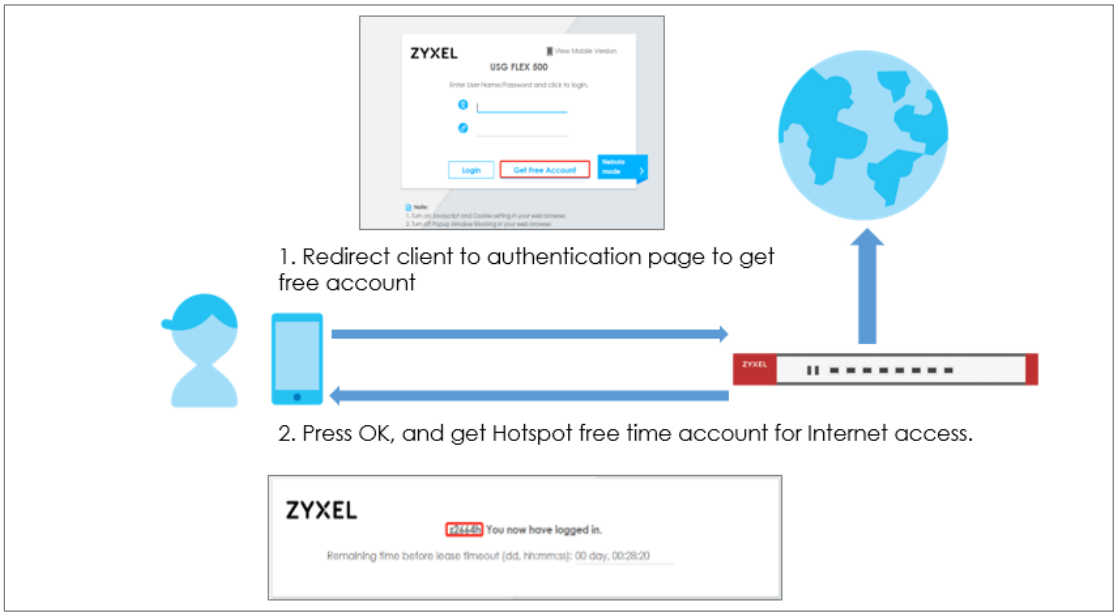
2. CDR service support these AP models: WAX650S / WAX610D / WAX510D / WAC500 / WAC500H
3. Containment list will keep on gateway/managed AP even reboot.
4. CDR service license is required.

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



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.

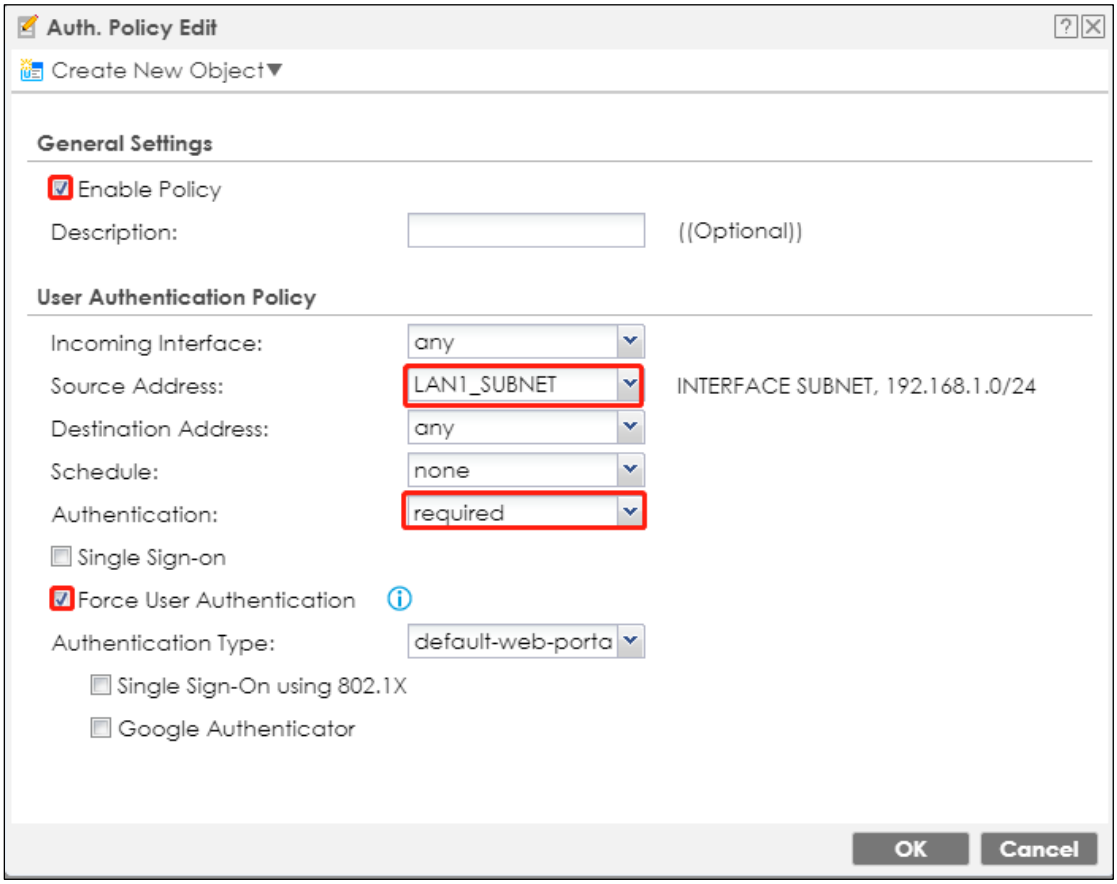
1. On the FLEX500, go to **Configuration** > **Web Authentication** > **General**. Select **Enable Web Authentication** and click **Add** in the **Web Authentication Policy Summary** section.

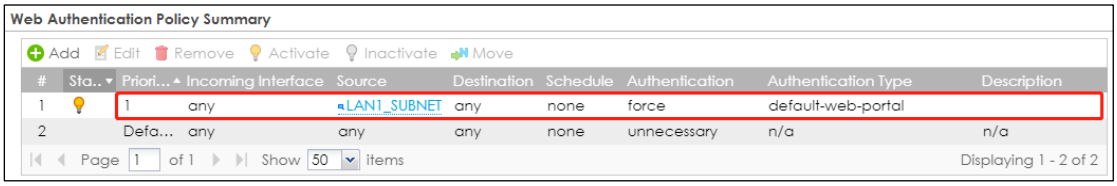
(1) Select **Enable Policy**.

(2) Select **LAN1_SUBNET**

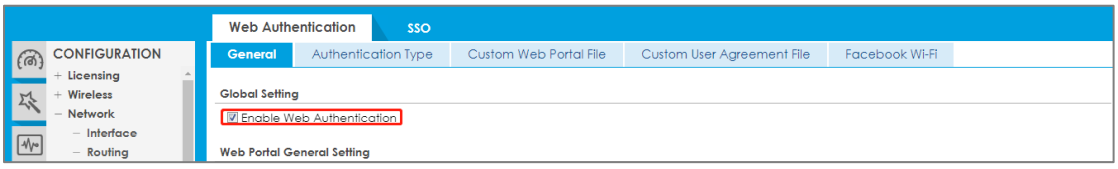
(3) Select **default-web-portal** as the **Authentication Type**.

(4) Click **OK** to add the policy.





2. Go to **Configuration** > **Web Authentication**. Select **Enable Web Authentication** and click **Apply**.



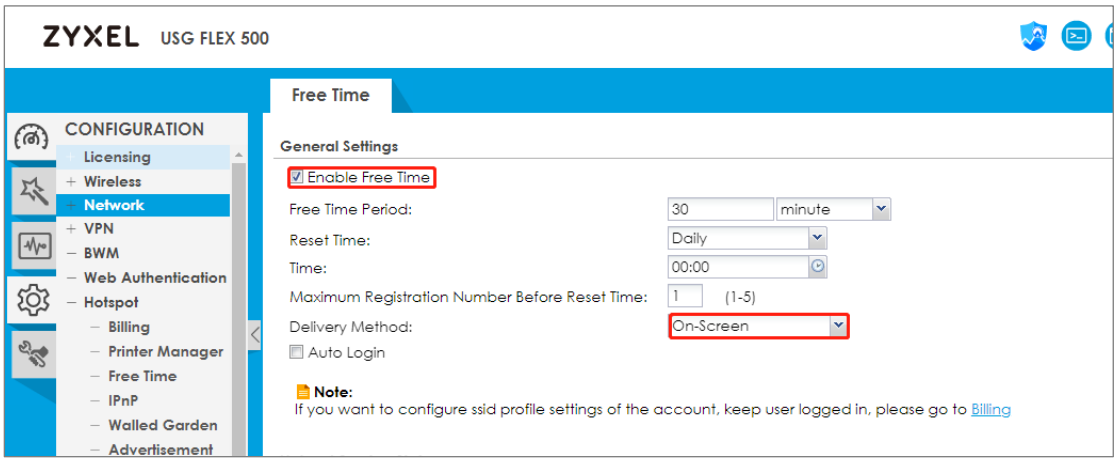
Enable the Free Time Feature

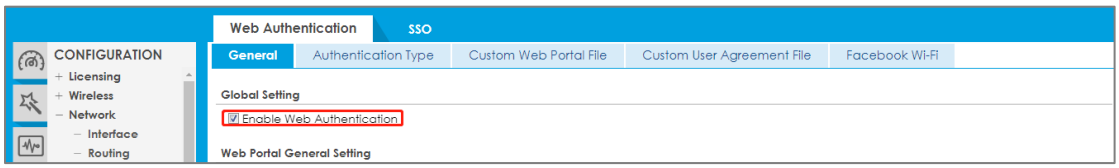
Configurations on the FLEX500

On the FLEX500, you need to enable **Free Time** feature.

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

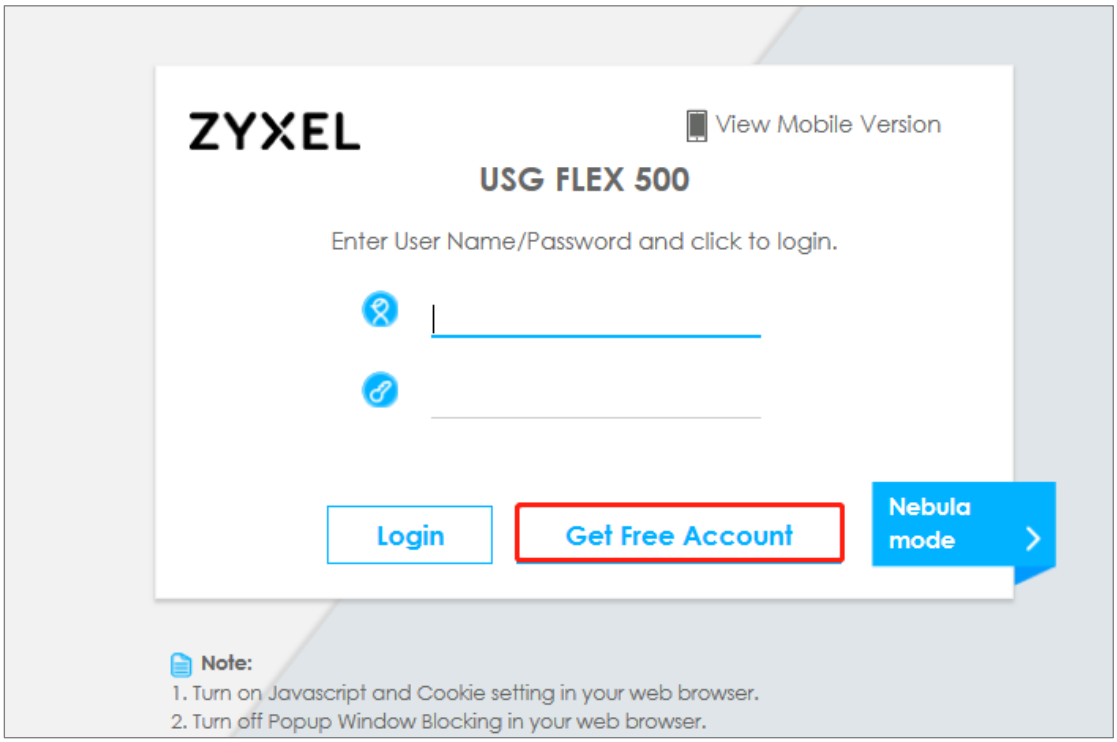
(1) Select **Enable Free Time** and set up the free time period. By default, the **Reset Time** is Daily. You also can set up maximum registration number can access the Internet.



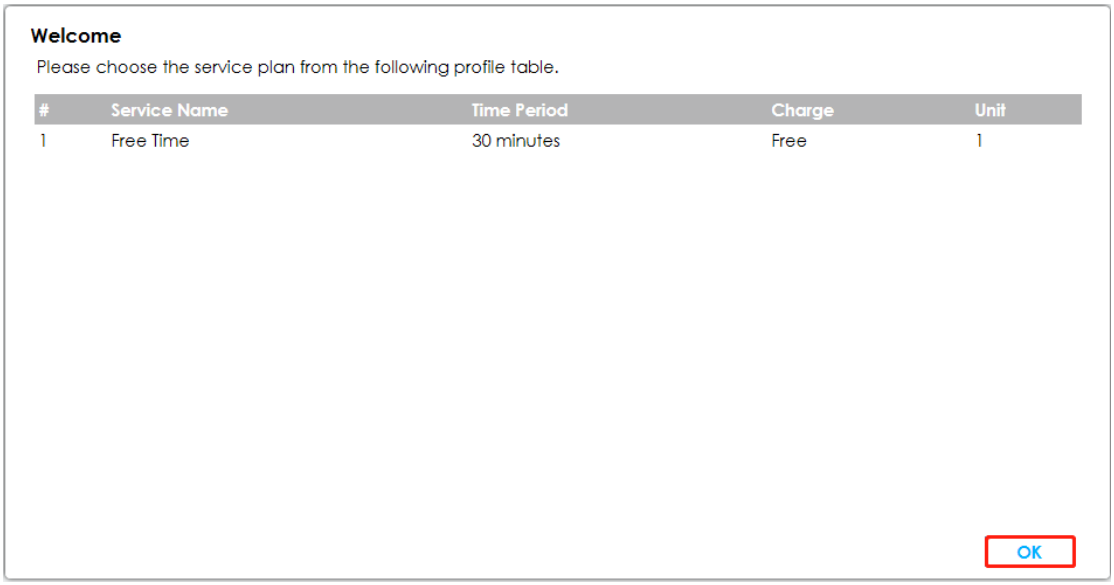


Test Free Time Feature

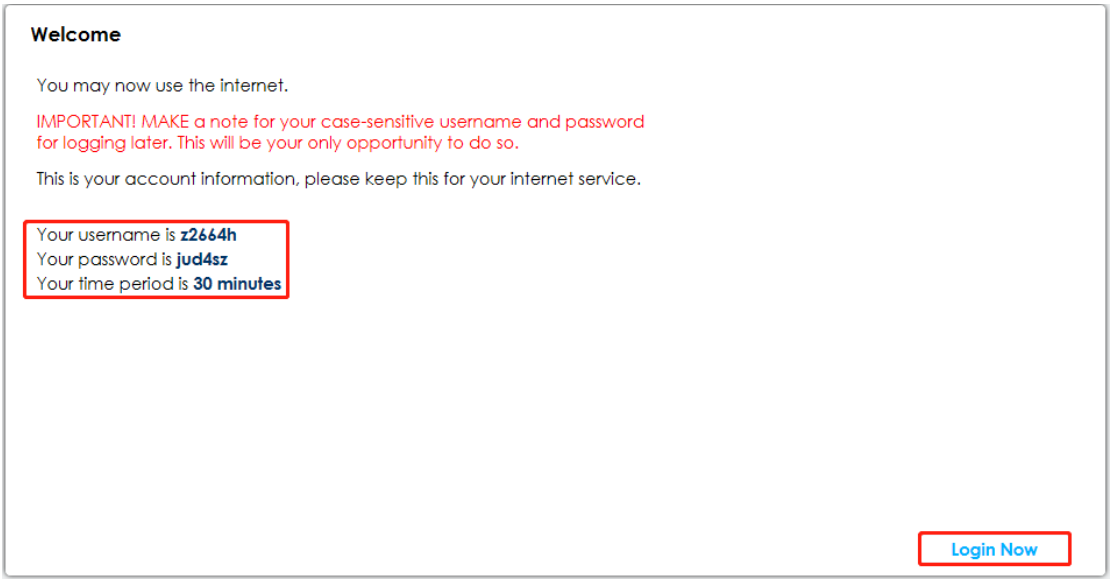
1. The user will be redirected to the **Login** screen before he/she is permitted to access the Internet. Click on the button **Get Free Account** to get a free account.



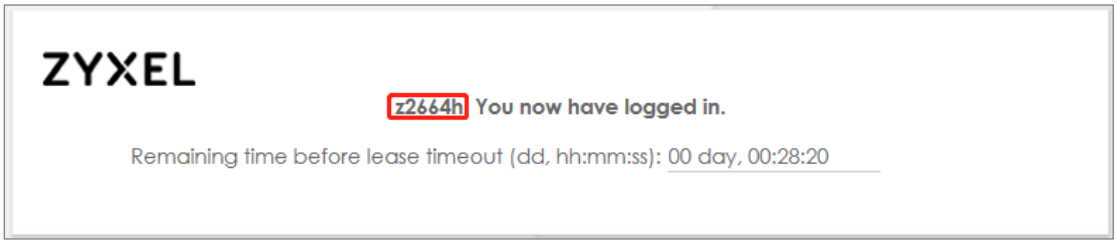
2. Select **Free Time** as the service plan. Then click ok to get credential.



3. The account and password will be show in this page. Click "Login Now"

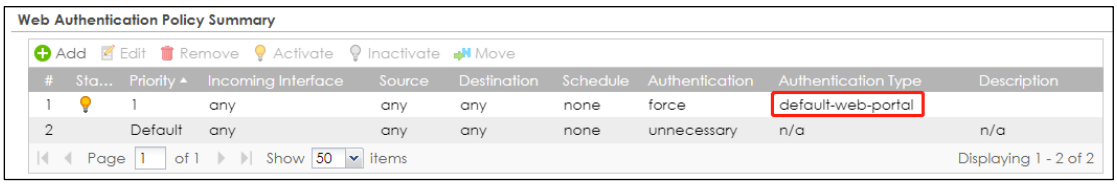


4. Check your account information. the Internet can be access as now for 30 minutes.



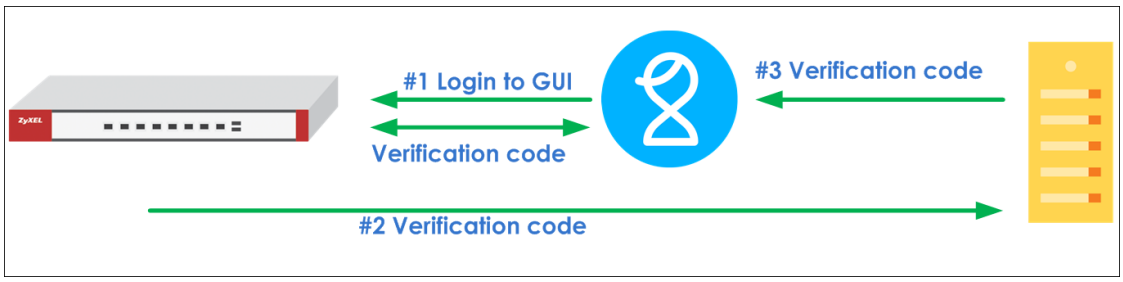
What Can Go Wrong?

If client cannot get the Login page correctly, please make sure Web Authentication Policy type is default-web-portal.



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

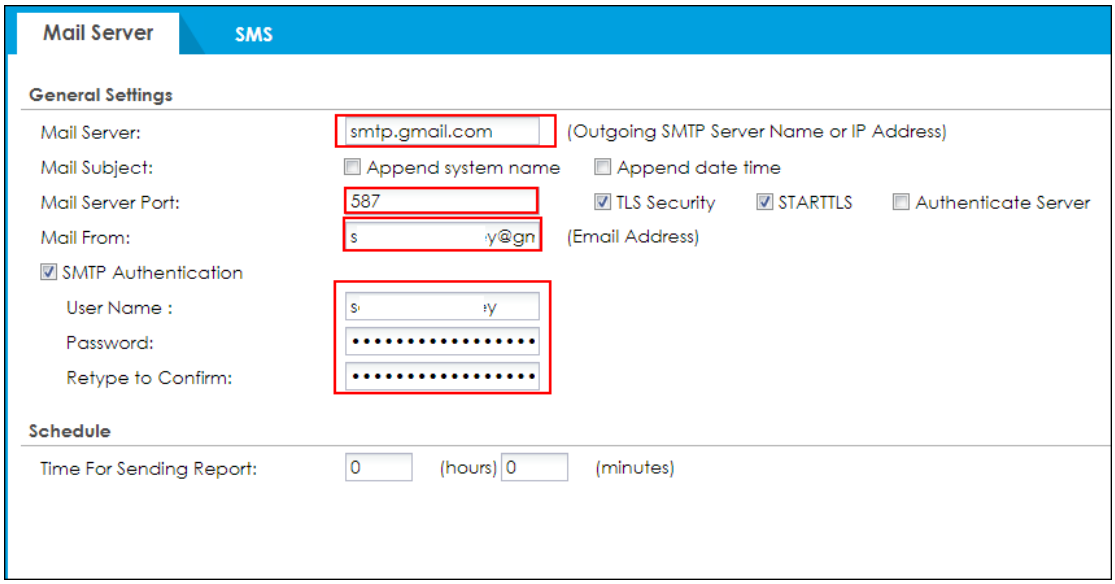


You can follow these steps to setup 2 factor authentication when logging to system.

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

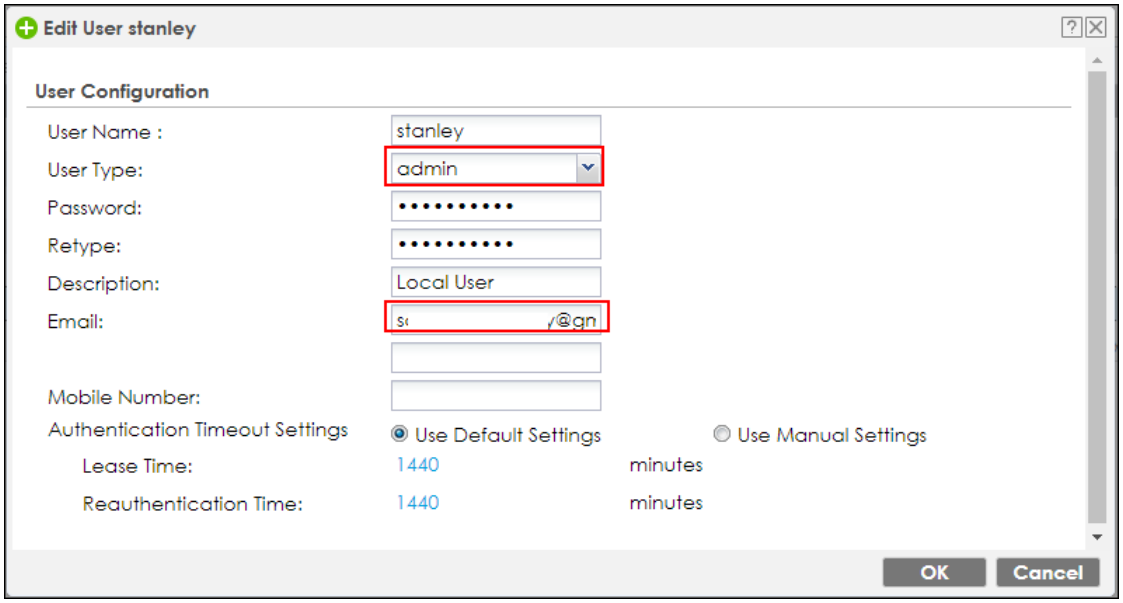


Note: Must make sure SMTP Server configuration is correct otherwise user will unable receive mail successfully.

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.

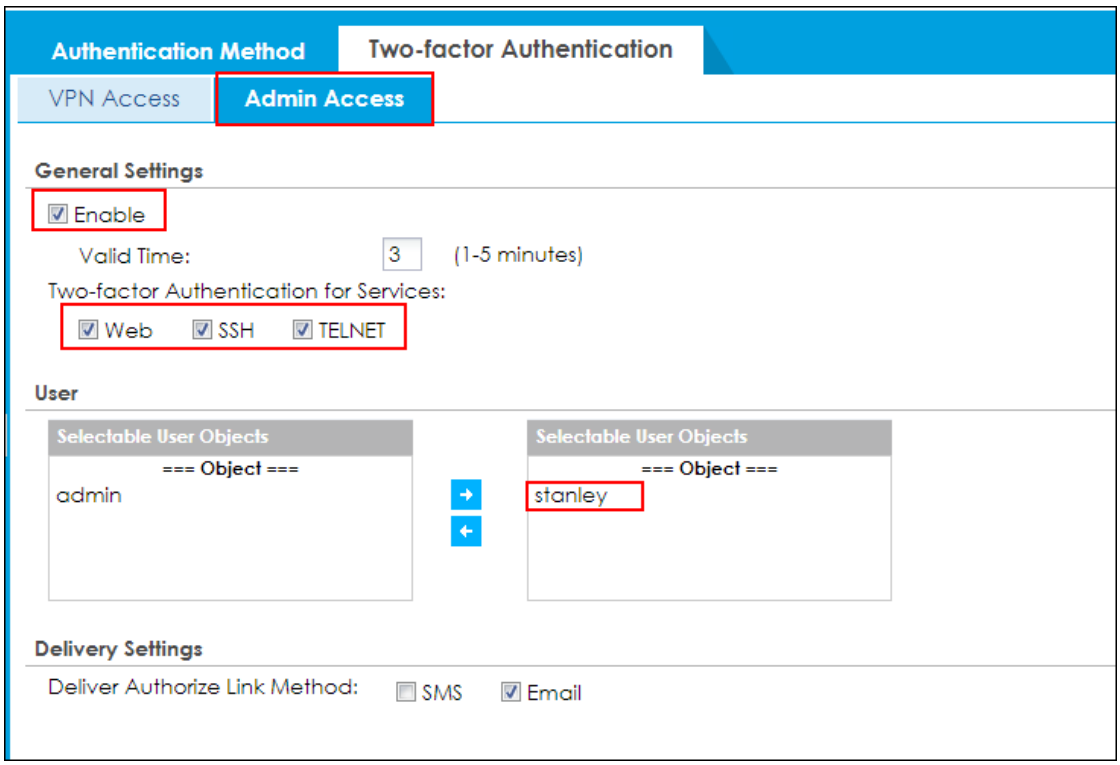
And also entered email address of this user.



Setup Two-Factor Authentication for admin on your device

Go to **Configuration > Object > Auth Method > Two-Factor Authentication > Admin Access**

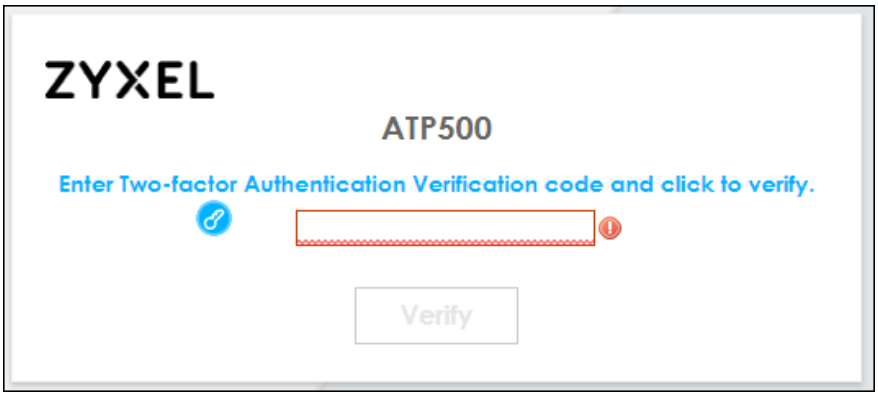
Enable the function and add admin user which you added in step2 in the rule, and you can select what services are 2 Factor authentication needed.



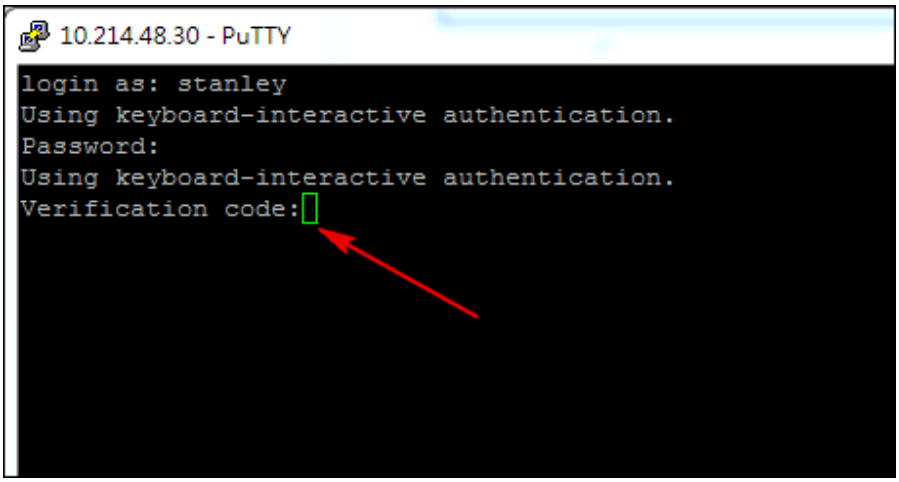
Test the Result

After setup these steps and login to device by admin user, the verification code is required.

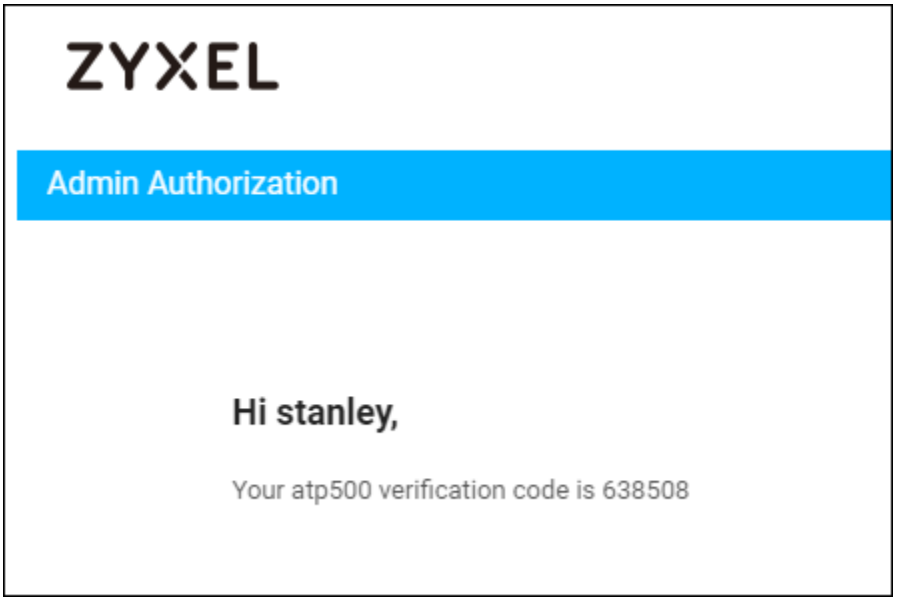
Web Service:



SSH Service:



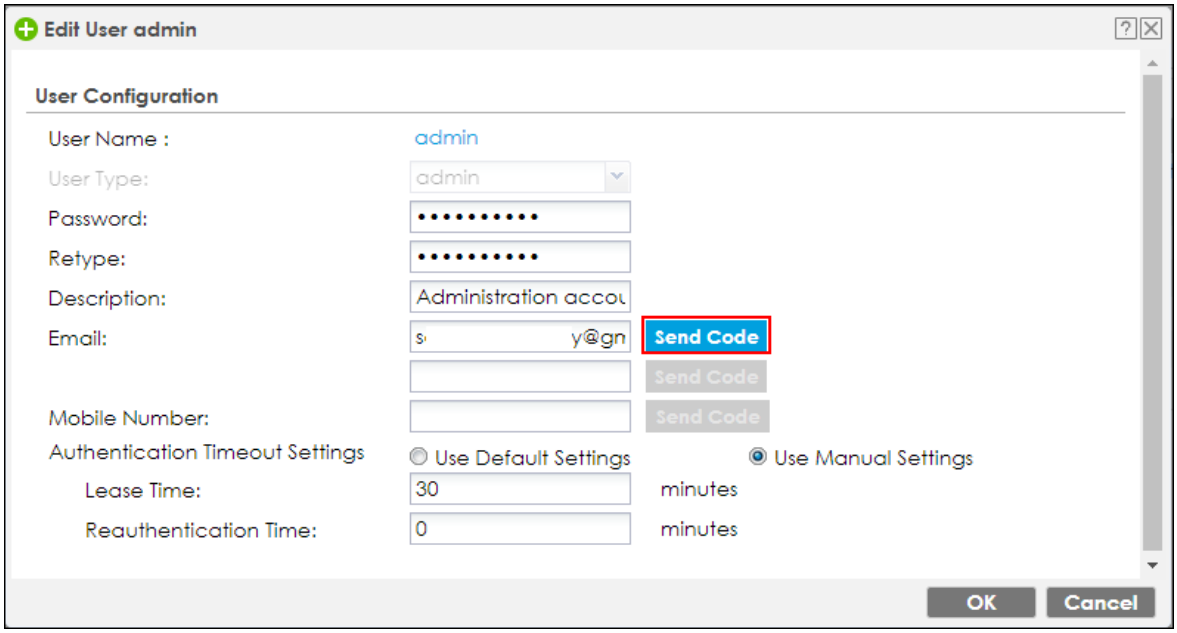
You will receive verification code by Email.



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**

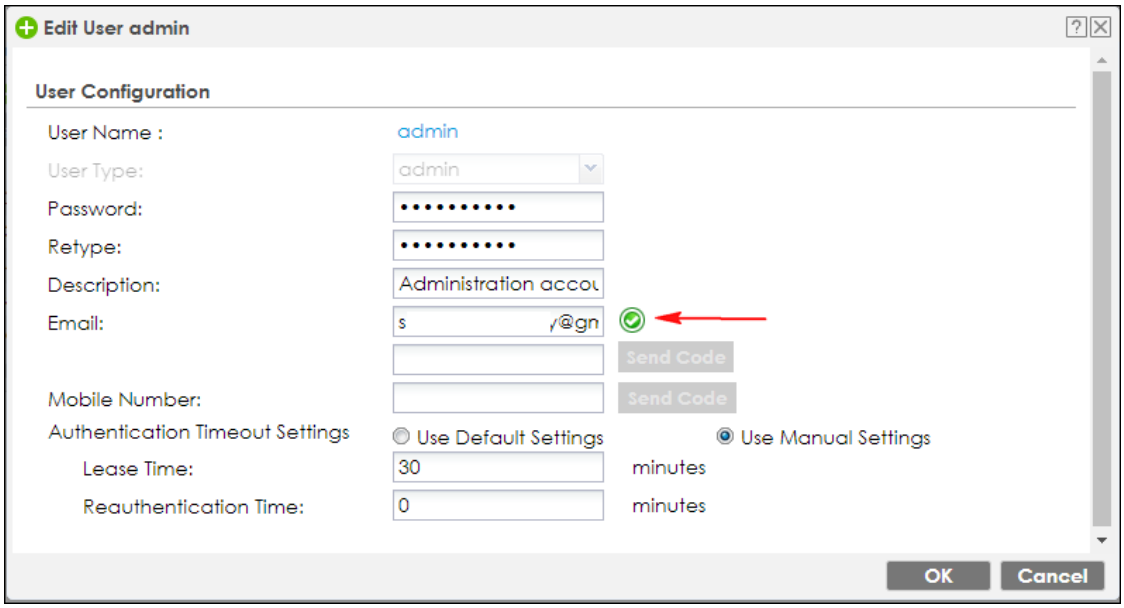
2-1 Enter Email address and click "send code" button



2.2 After clicked "Send Code", you will receive code by Email.

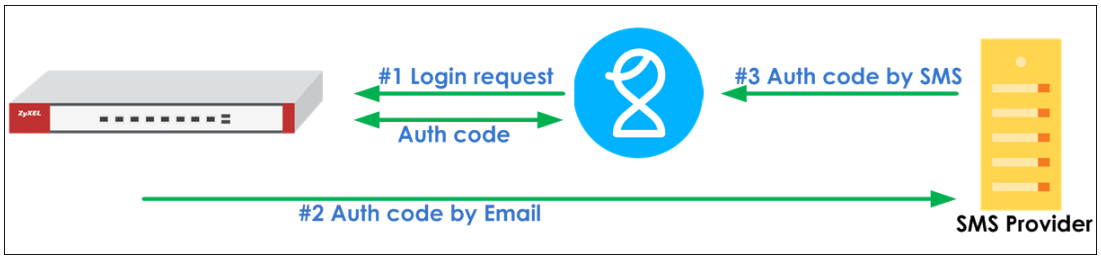
2.3 Enter code that you received.

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
/@gn
Send Code
Mobile Number:
Send Code
Authentication Timeout Settings
Use Default Settings
Use Manual Settings
Lease Time:
30
minutes
Reauthentication Time:
0
minutes
OK
Cancel

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.

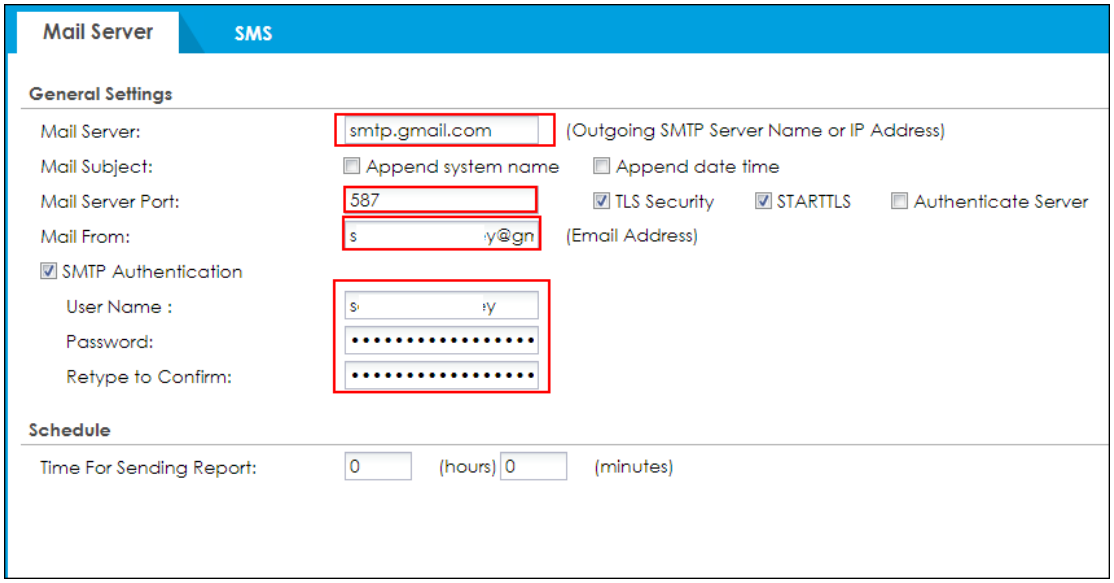


You can follow these steps to Email to SMS.

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

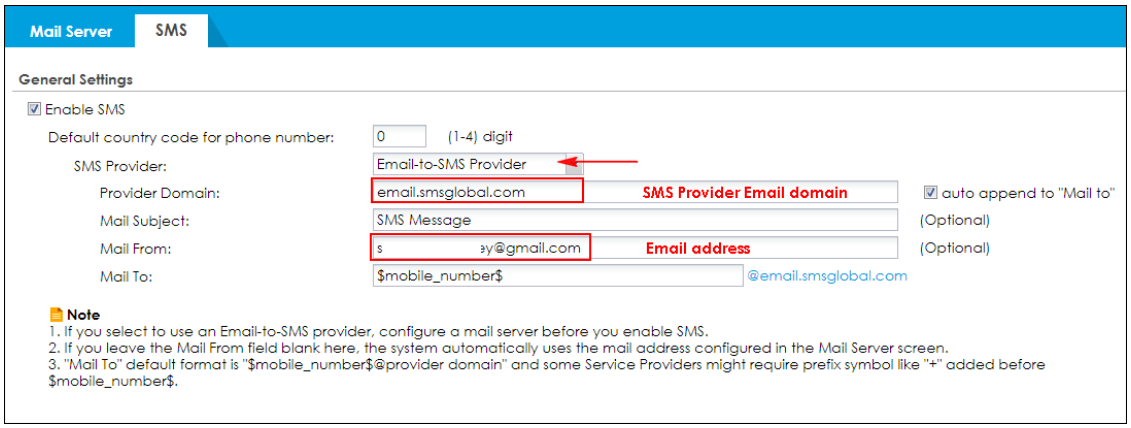


Note: Must make sure SMTP Server configuration is correct otherwise message will unable send to SMS provider successfully.

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.

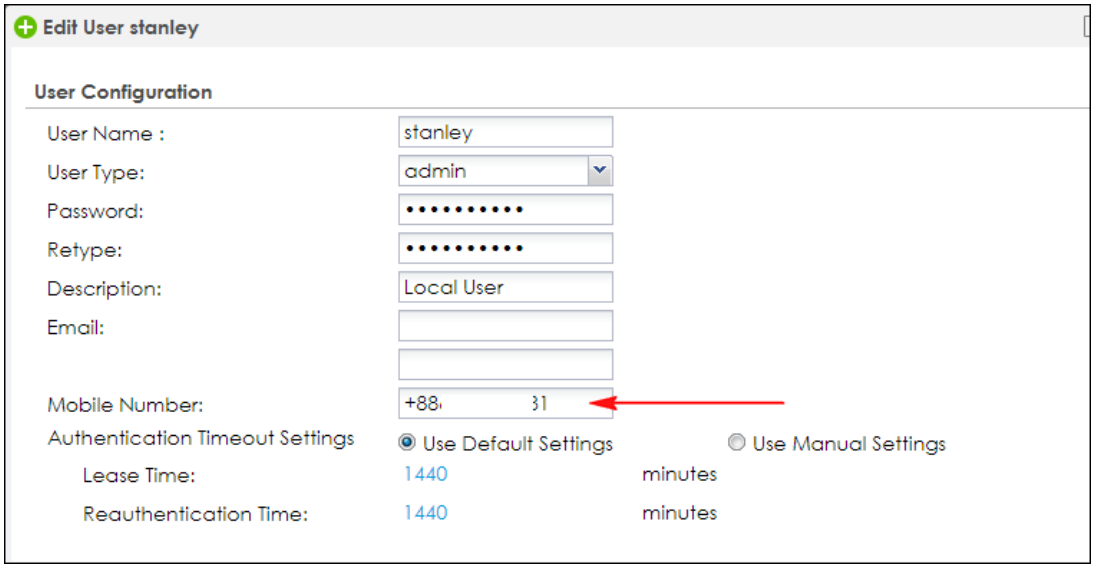
And configuring sender mail address in "Mail From"



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

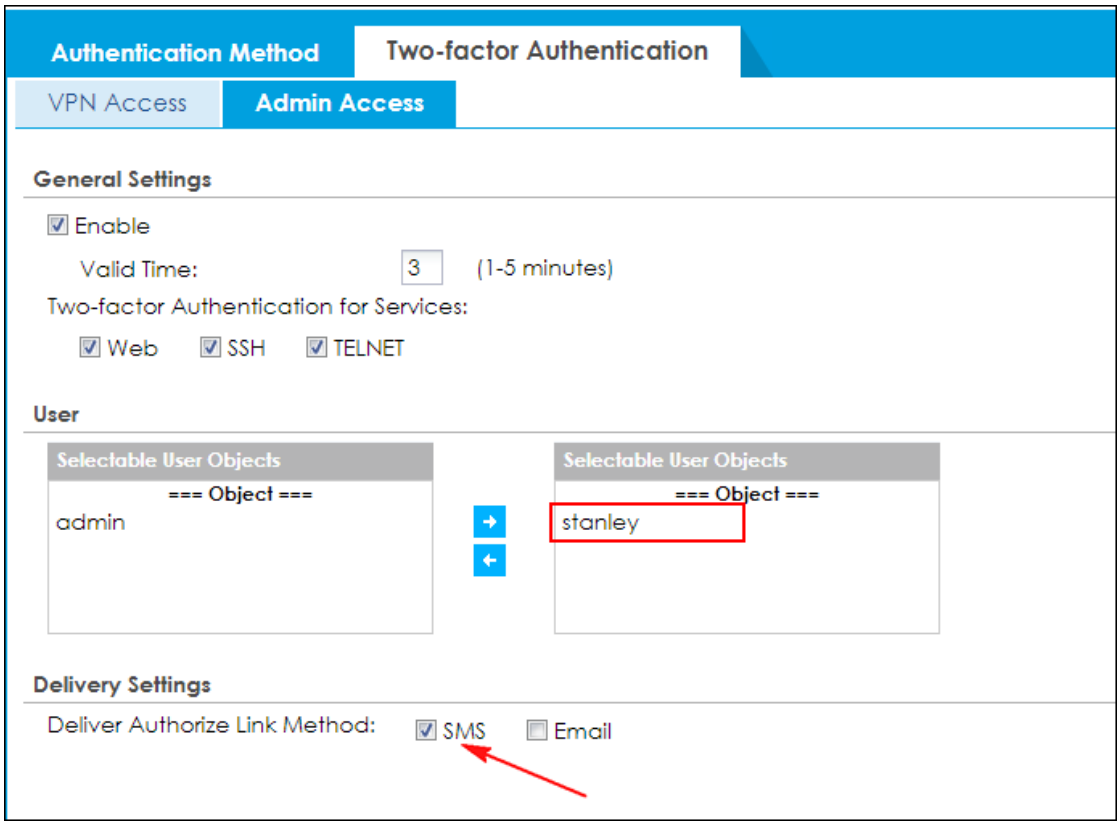
Go to **Configuration > Object > User/Group > User** Click Add button to create an user and user type is admin. And also entered phone number of this user.



Setup Two-Factor Authentication for admin on your device

Go to **Configuration > Object > Auth Method > Two-Factor Authentication > Admin Access**

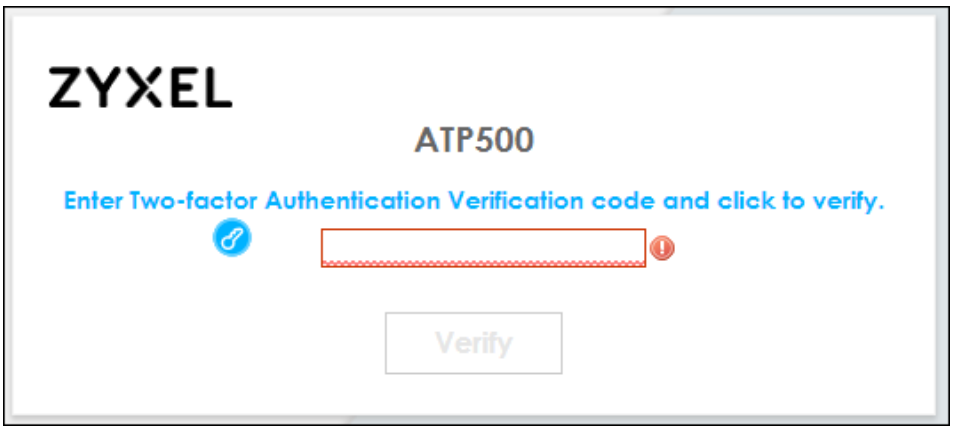
Enable the function and add admin user which you added in step3 in the rule, and you can select what services are 2 Factor authentication needed. Enable SMS function to send verification code by SMS.



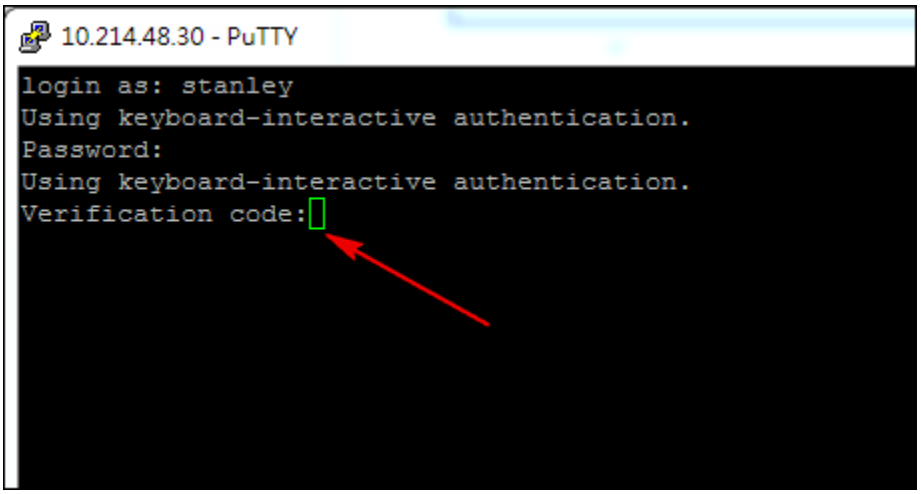
Test the Result

After setup these steps and login to device by admin user, the verification code is required.

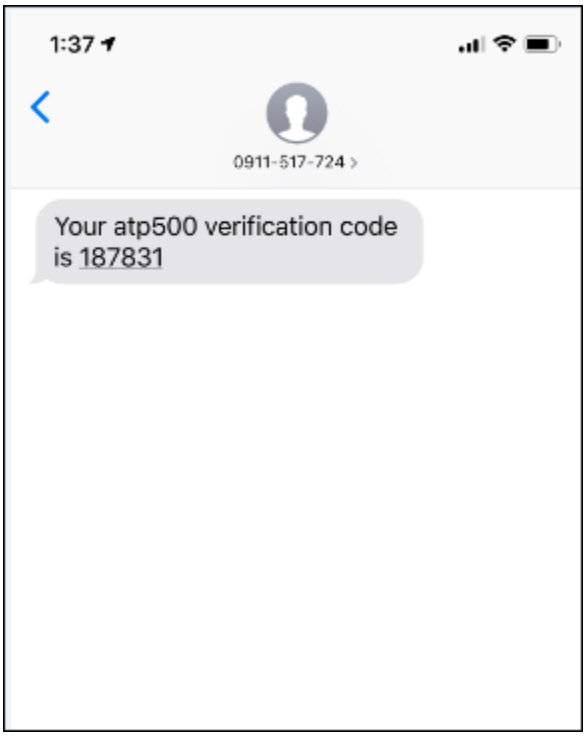
Web Service:



SSH Service:



You will receive verification code by SMS.



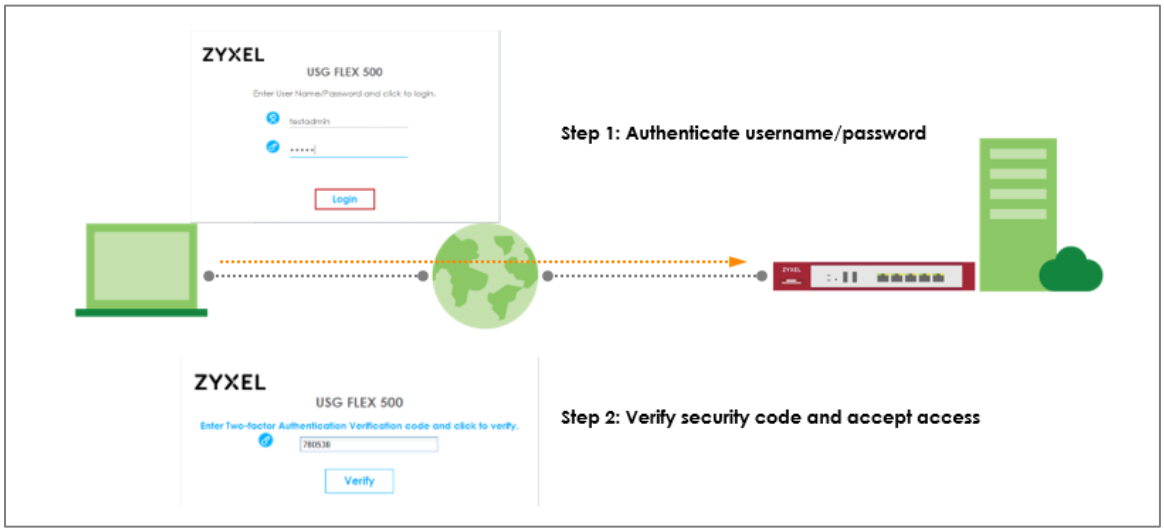
What Can Go Wrong?

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.



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).

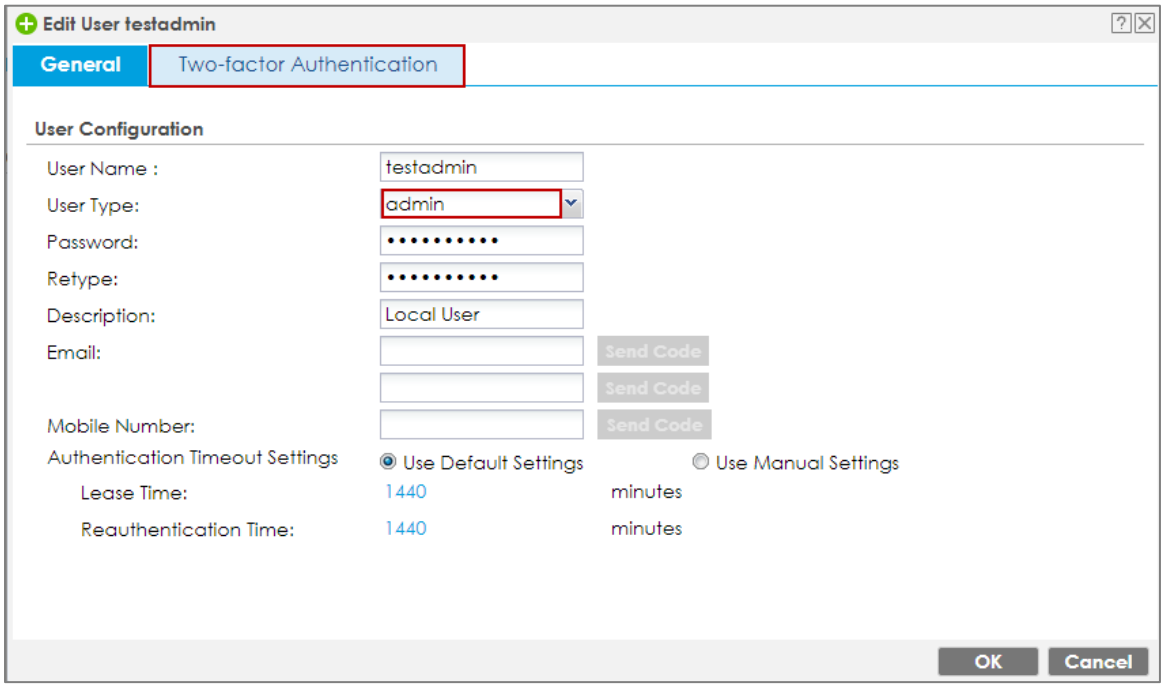
Two Factor with Google Authenticator Flow

1. Enable Google Authentication on specific admin user
2. Set up Google Authenticator
3. Configure valid time and login service types.

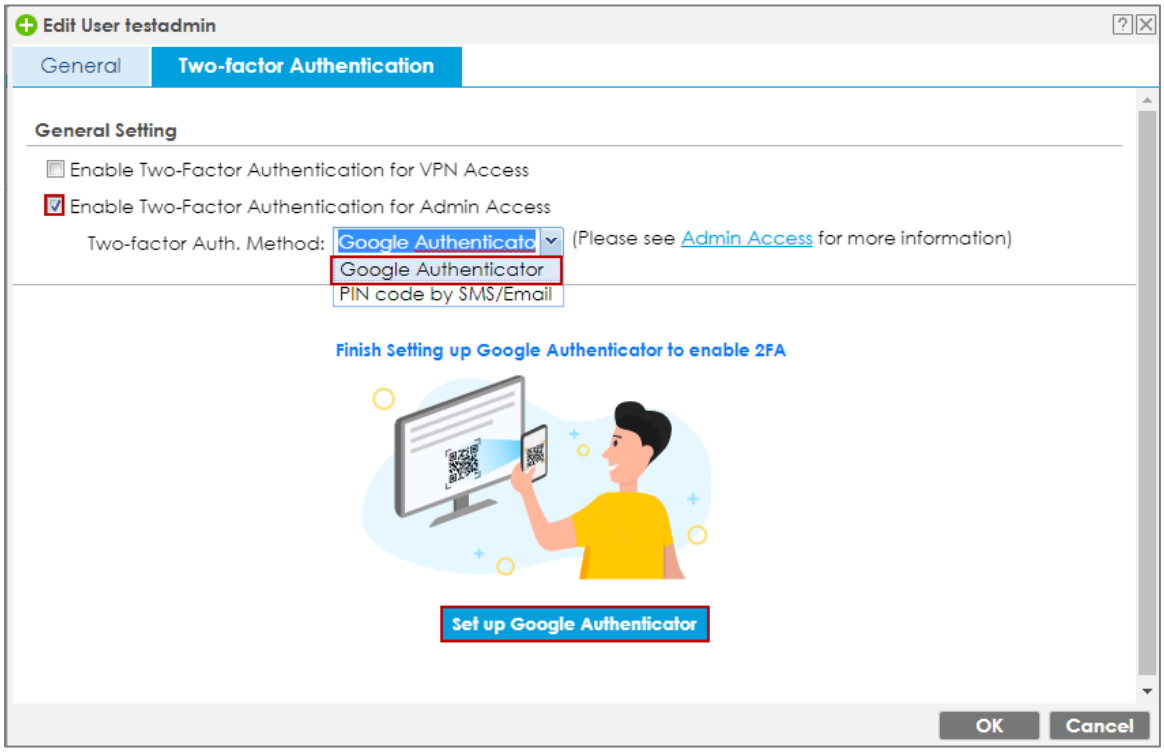
Enable Google Authentication on specific admin user

Select a specific admin user and switch to Two-factor Authentication tab.

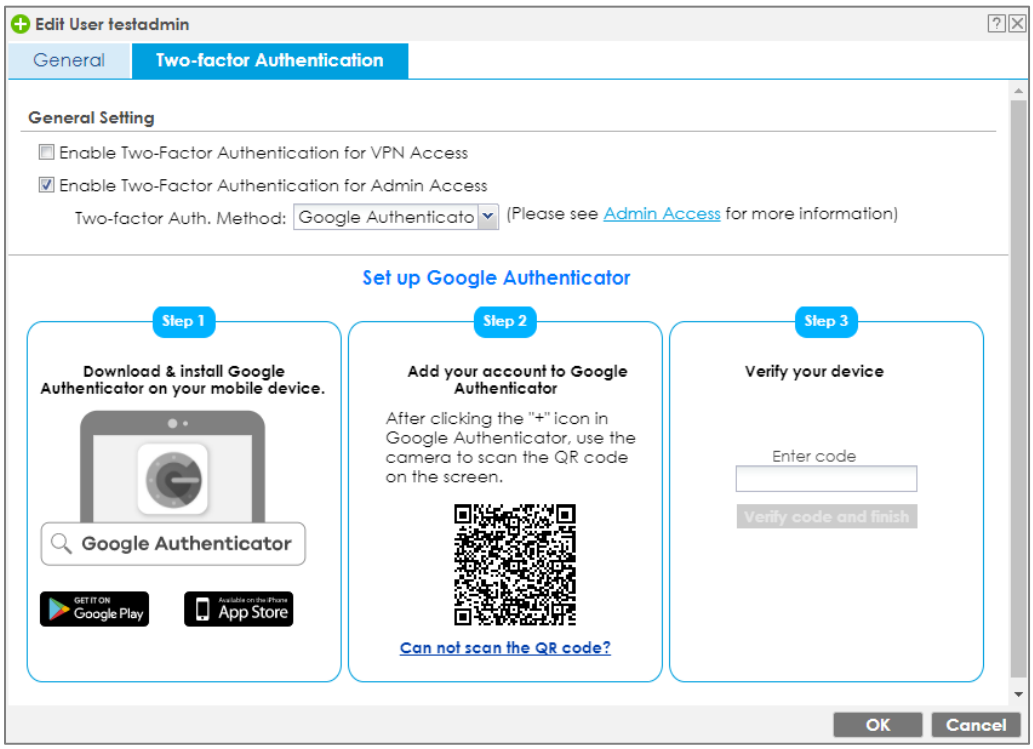
CONFIGURATION > Object > User/Group > admin user



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.

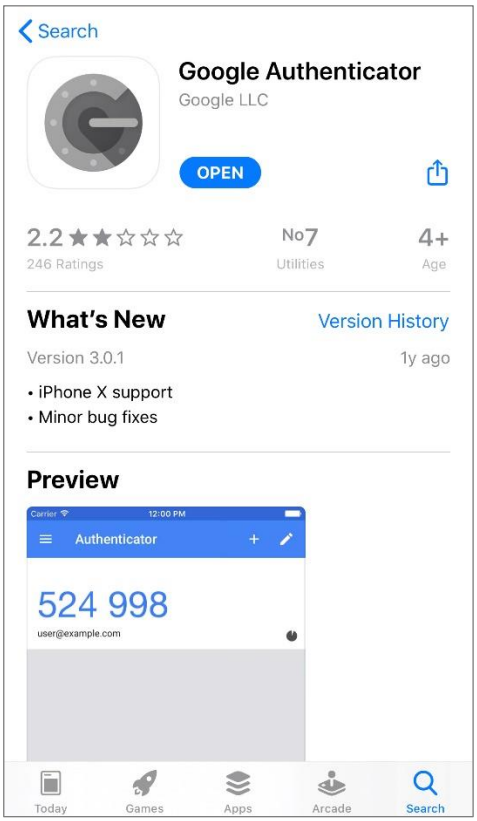


Set up Google Authenticator

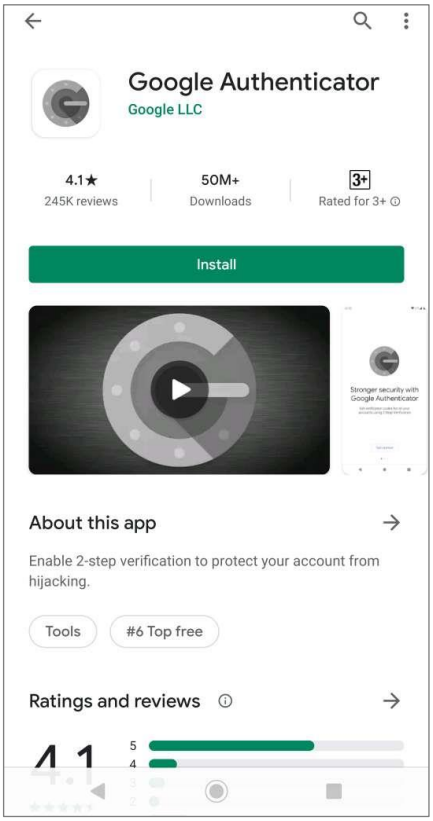


1. Download and install Google Authenticator on your mobile device.

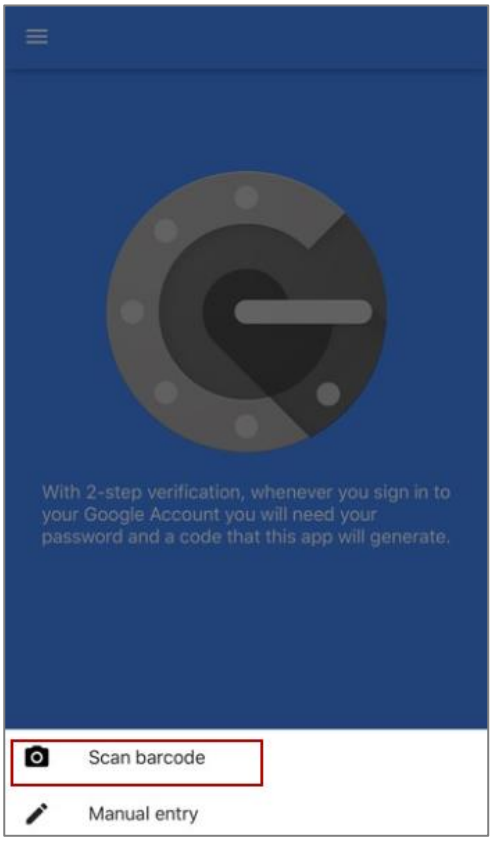
Apple Store



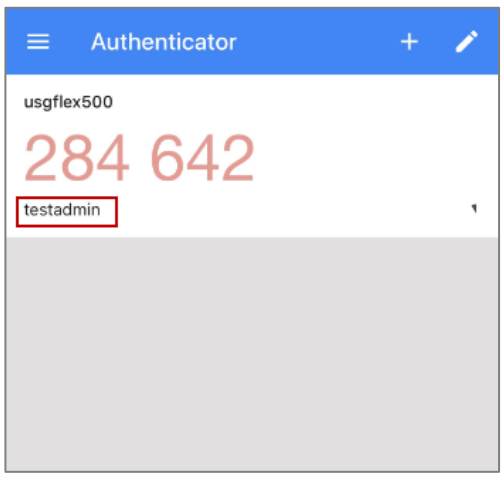
Google Play

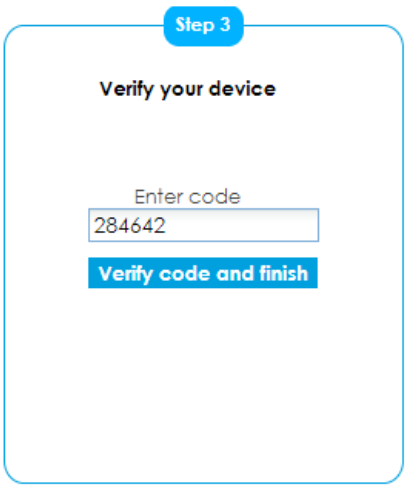


2. Register the admin account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.

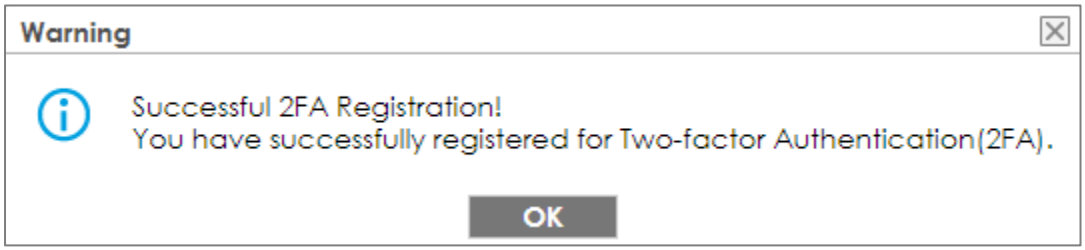


3. Enter the token code which displays on Google Authenticator to "Step 3" and click "Verify code and finish" to submit and verify the code.

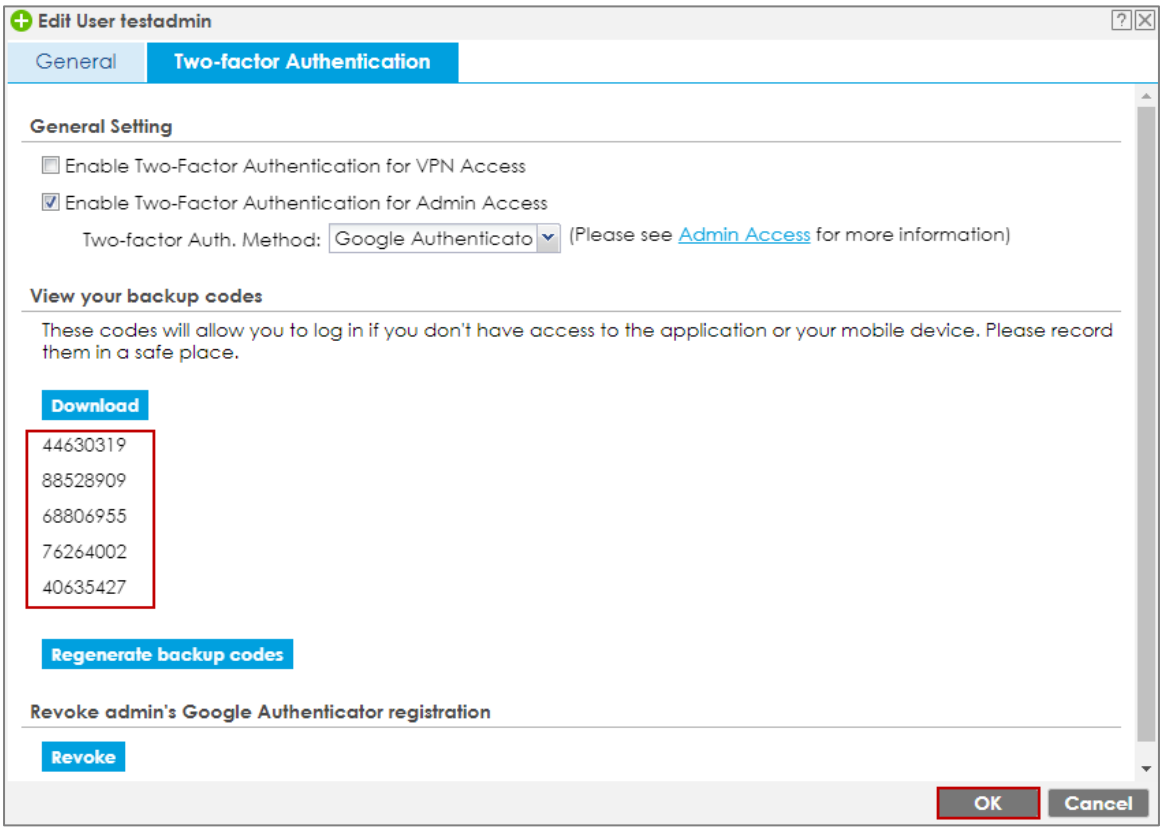




The pop-up window message informs the verification result.



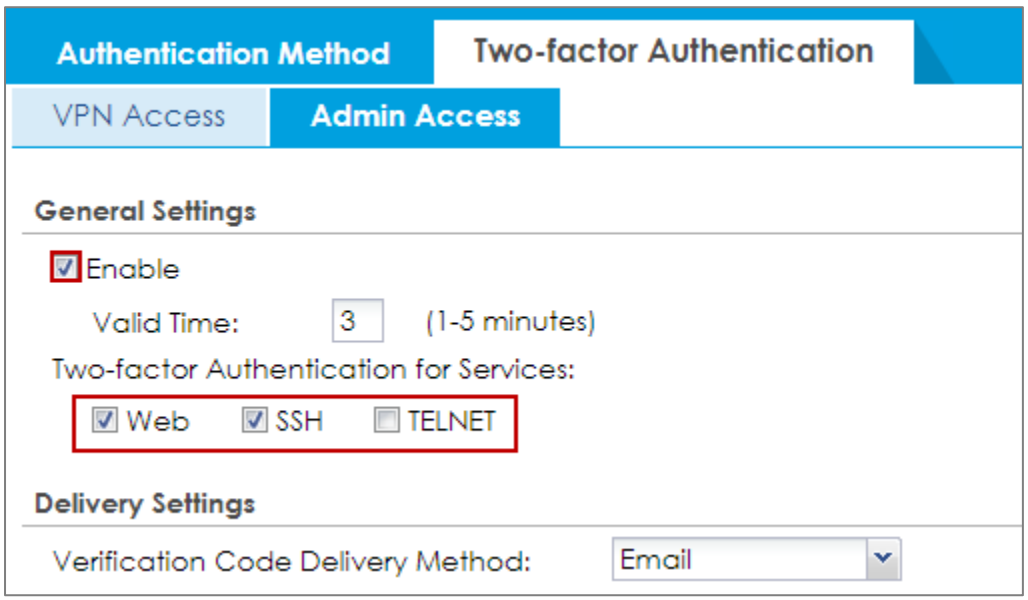
4. After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.



Configure valid time and login service types

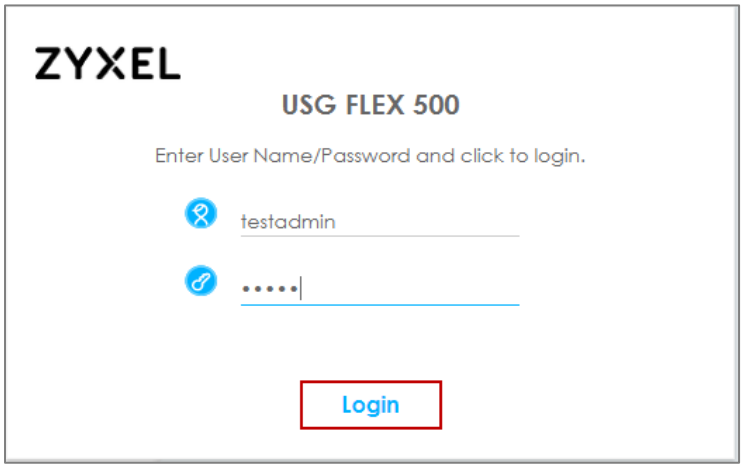
Enable two factor authentication for admin access. Configure valid time and select which services require two-factor authentication for admin user. The valid time is the deadline that admin needs to submit the two-factor authentication code to get the access. The access request is rejected if submitting the code later than valid time. By default, the valid time is 3 minutes.

CONFIGURATION > Object > Auth. Method > Two-factor Authentication > Admin Access

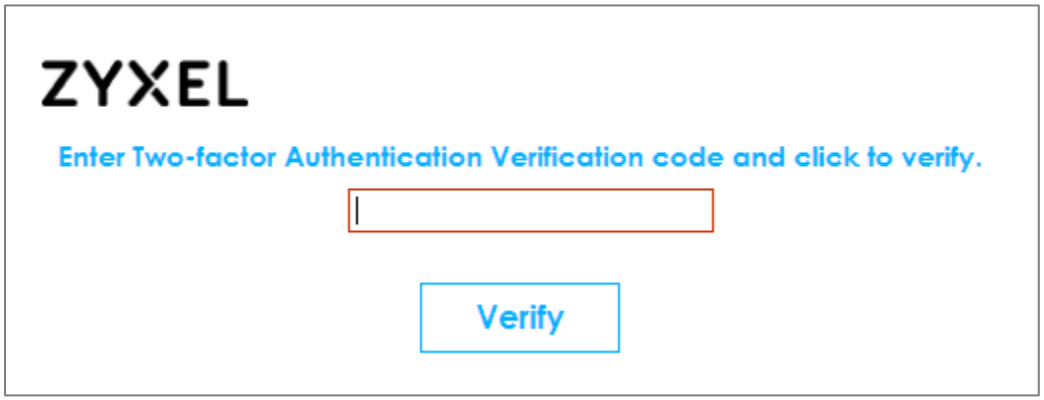


Test the Result

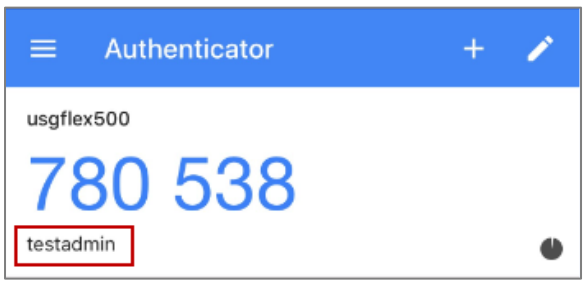
1. Login with the admin account "testadmin".



2. A pop-up window appears for administrator to enter the verification code.

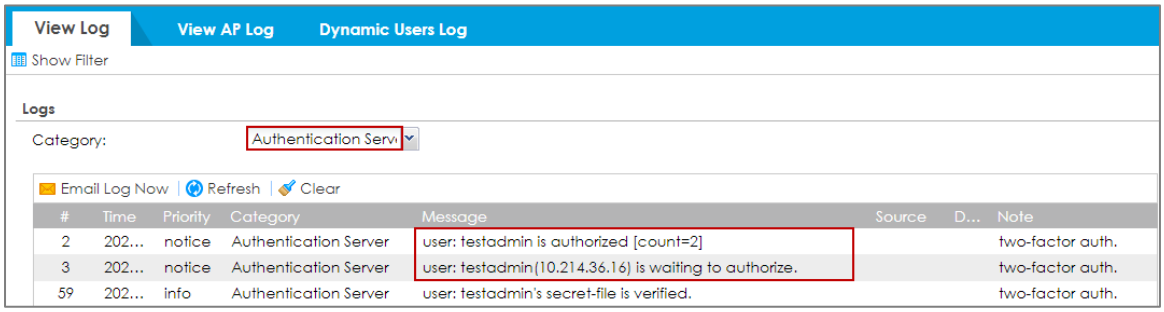


3. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.



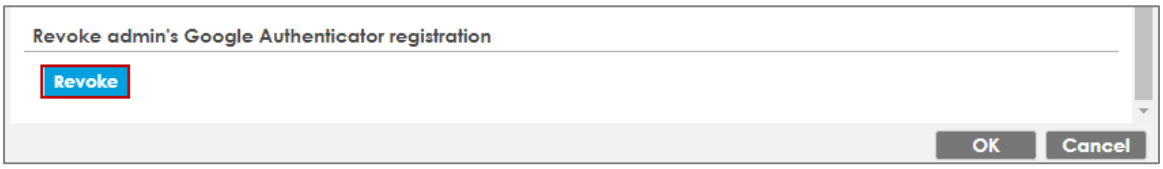
4. Authorize with username, password and the token code successfully.

MONITOR > Log > View Log > Category and select "Authentication Server"



What Can Go Wrong?

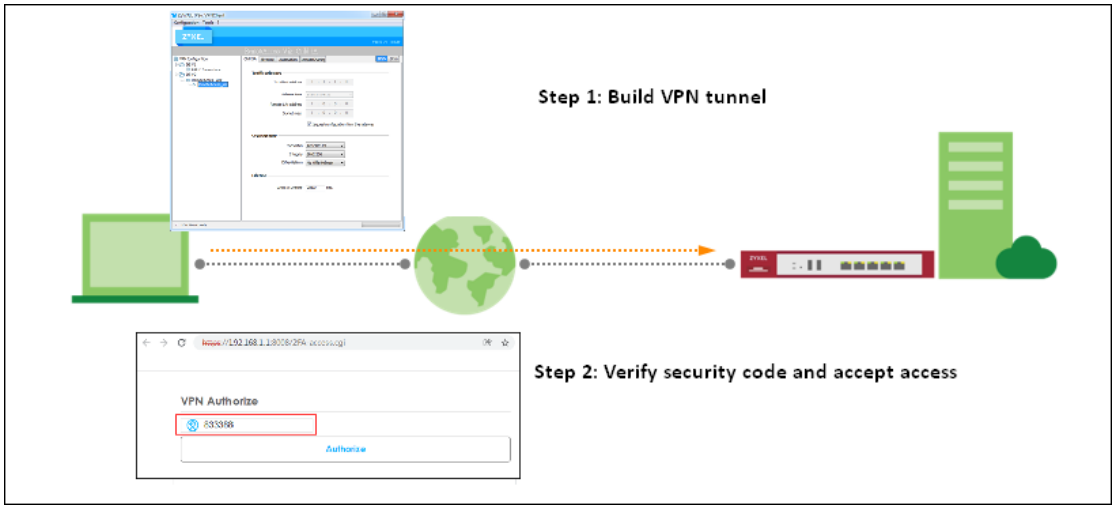
1. An admin user only can be registered on one Google Authenticator. If you would like to use another mobile device to authenticate the same admin user, click "Revoke" to revoke registered user and user another mobile device to set up Google Authenticator again.



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.



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).

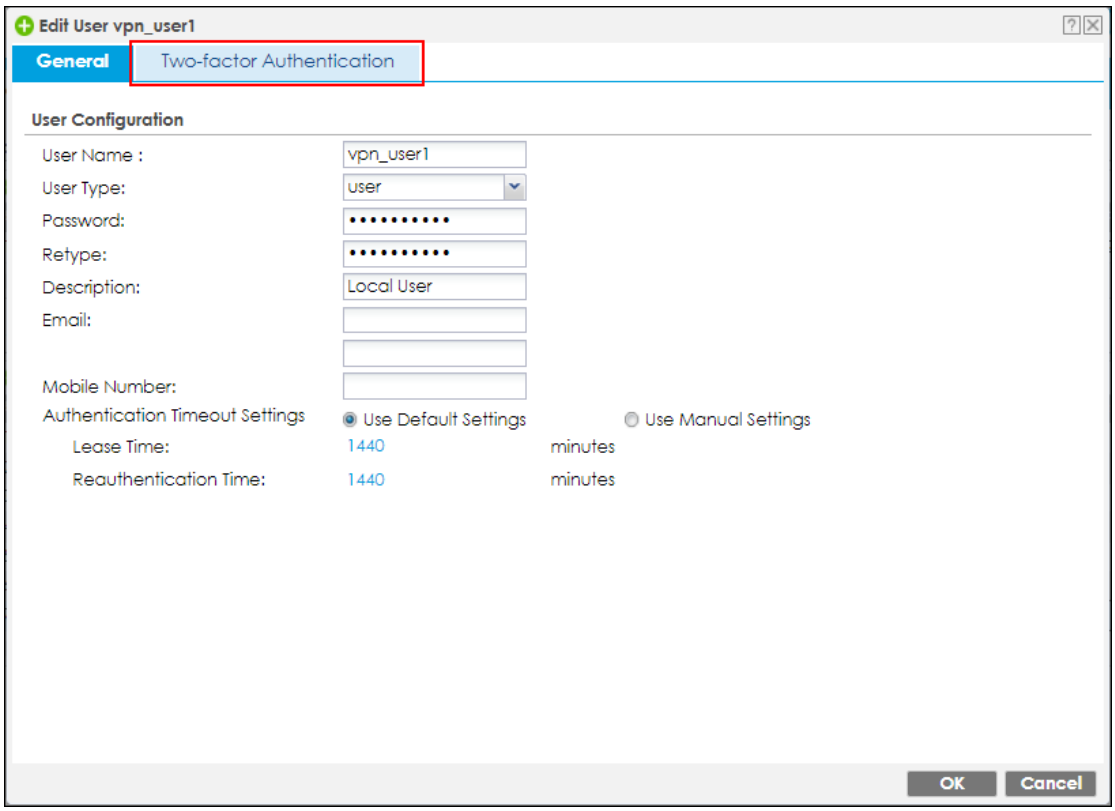
Two Factor with Google Authenticator Flow

1. Enable Google Authentication on user
2. Set up Google Authenticator
3. Configure valid time and login service types

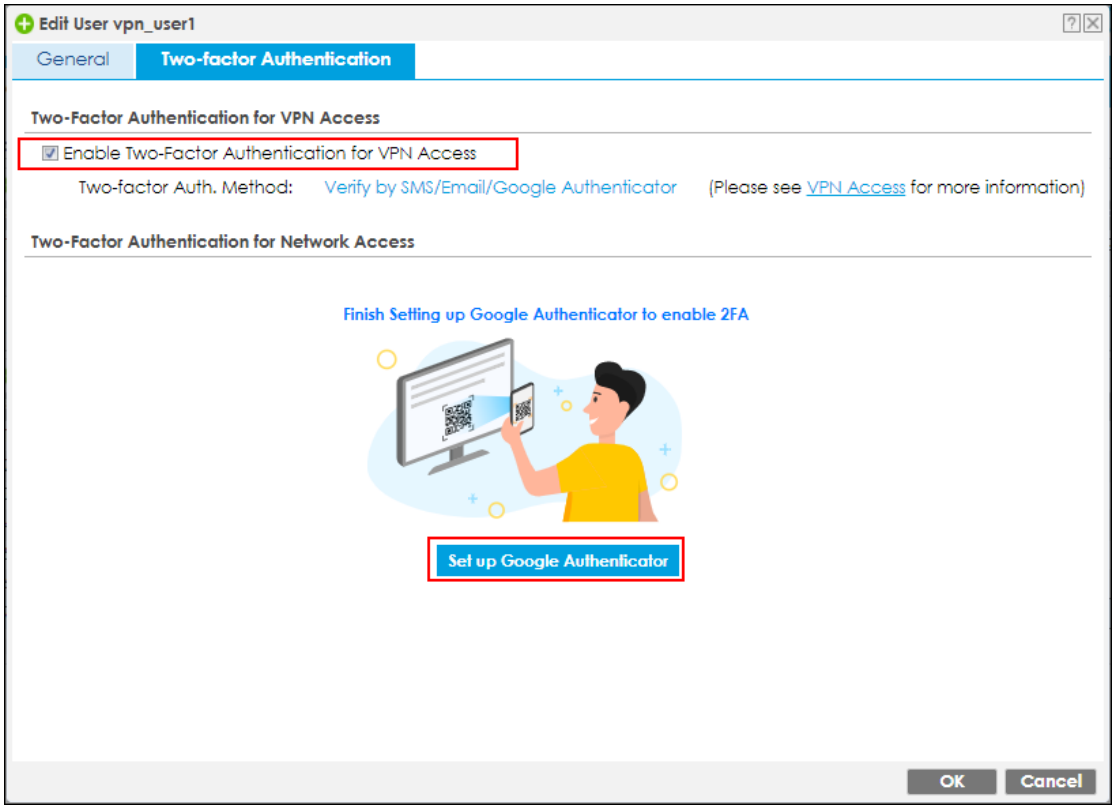
Enable Google Authentication on user

Select a VPN user and switch to Two-factor Authentication tab.

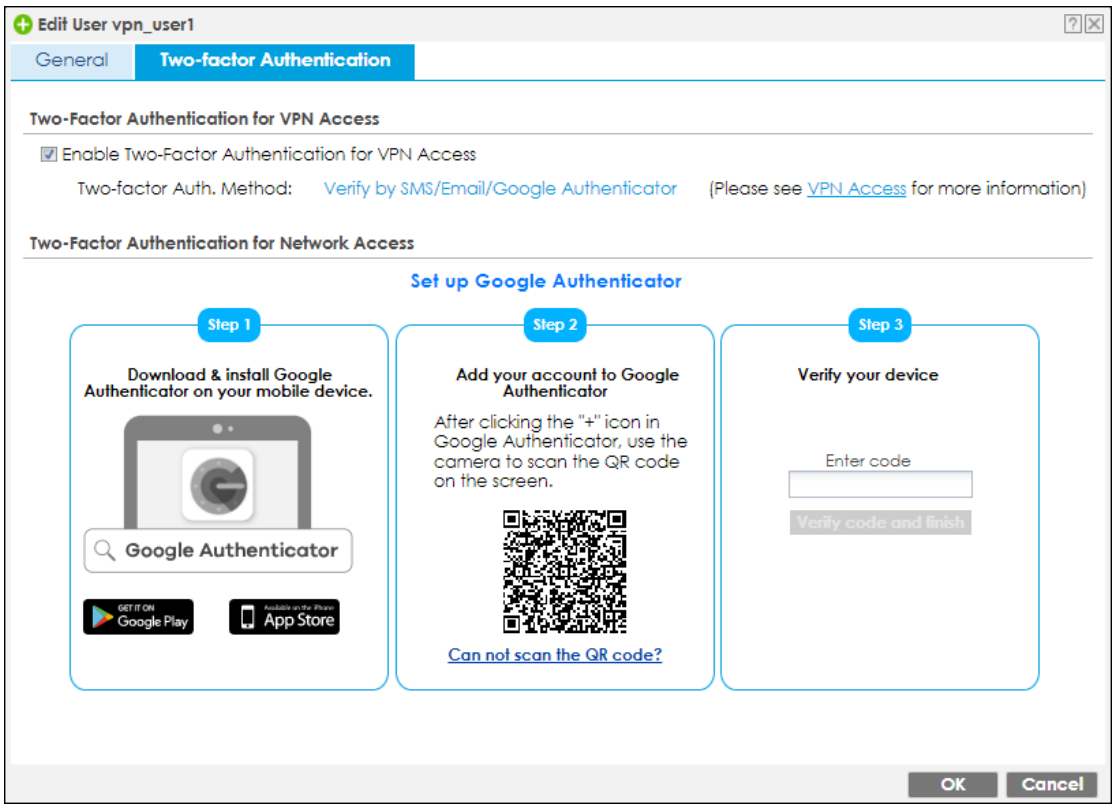
CONFIGURATION > Object > User/Group > User, create a new user



Enable Two-Factor Authentication for VPN Access checkbox.

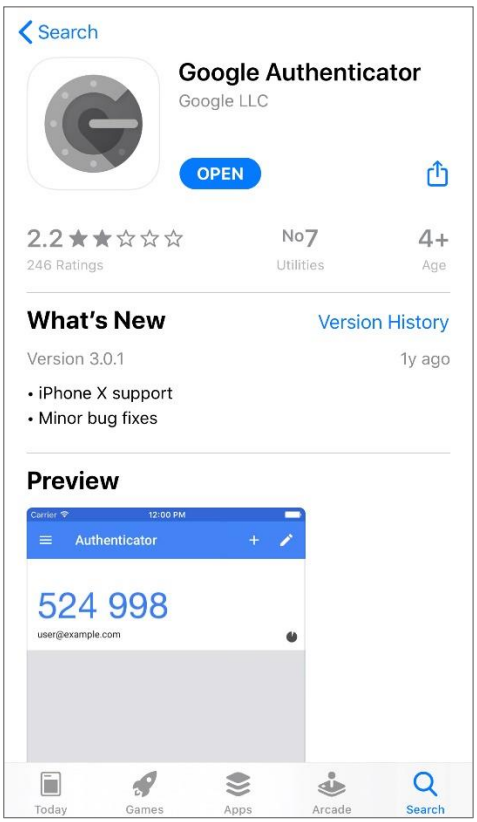


Set up Google Authenticator

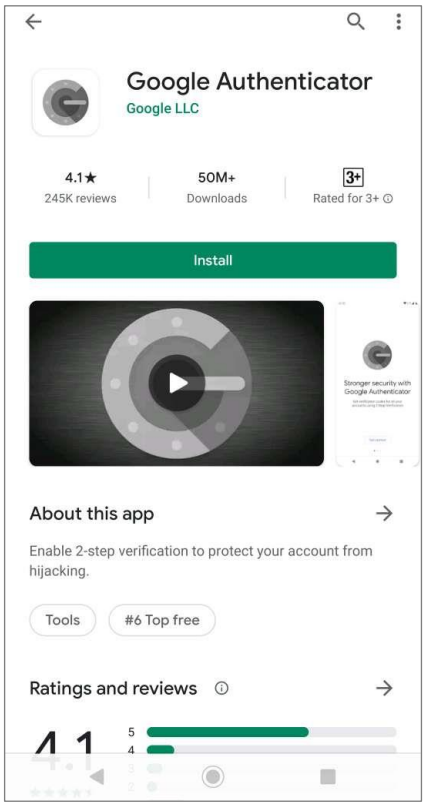


1. Download and install Google Authenticator on your mobile device.

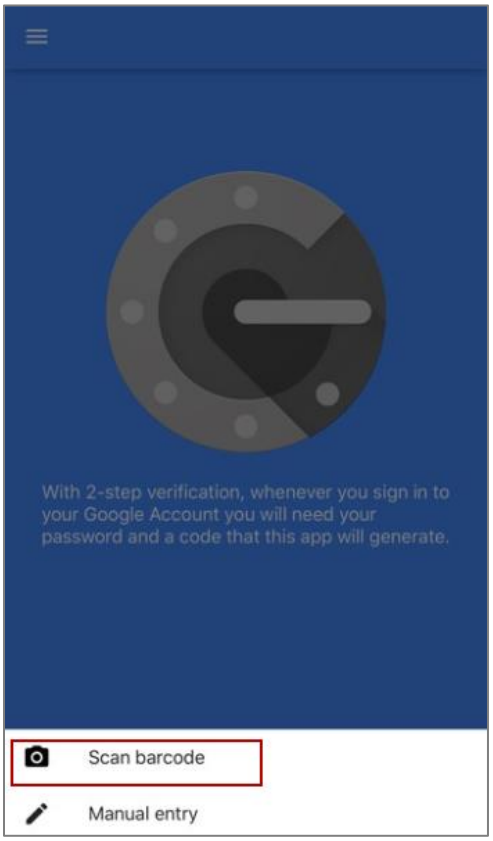
Apple Store



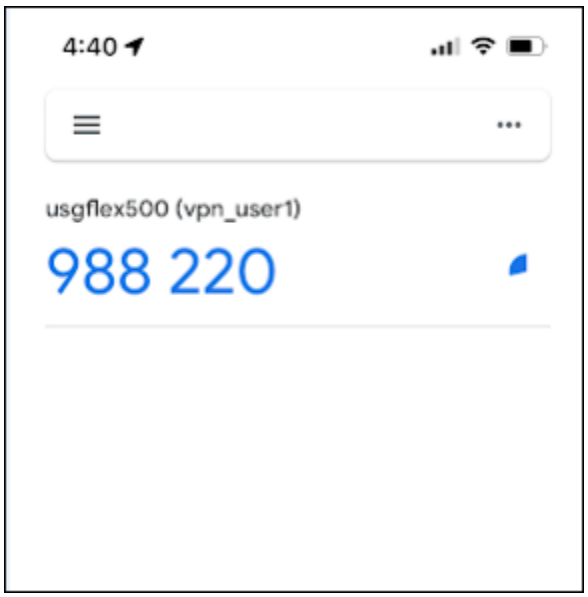
Google Play

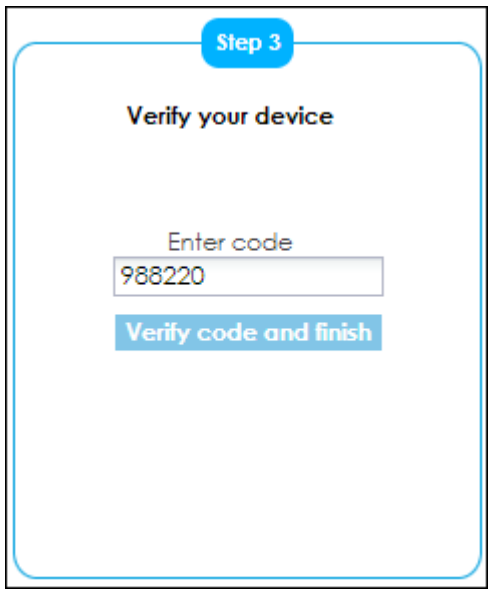


2. Register the VPN user account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.

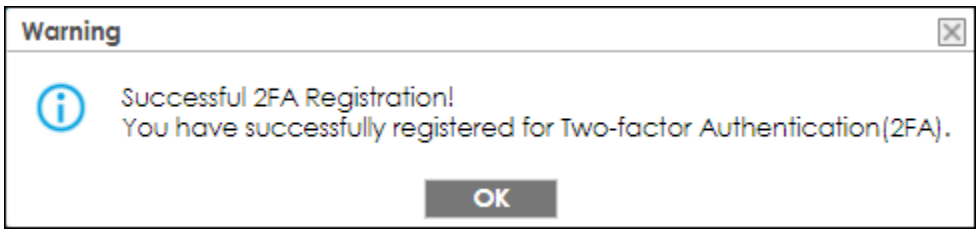


3. Enter the token code which displays on Google Authenticator to "Step 3" and click "Verify code and finish" to submit and verify the code.

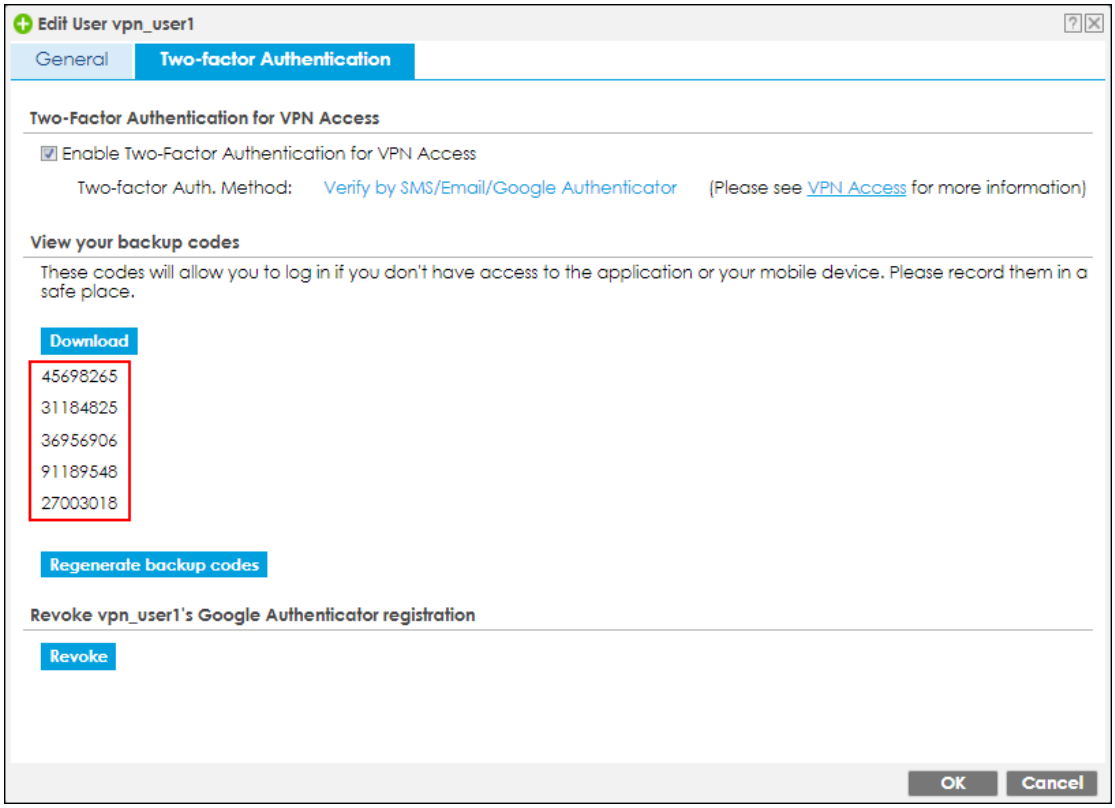




The pop-up window message informs the verification result.



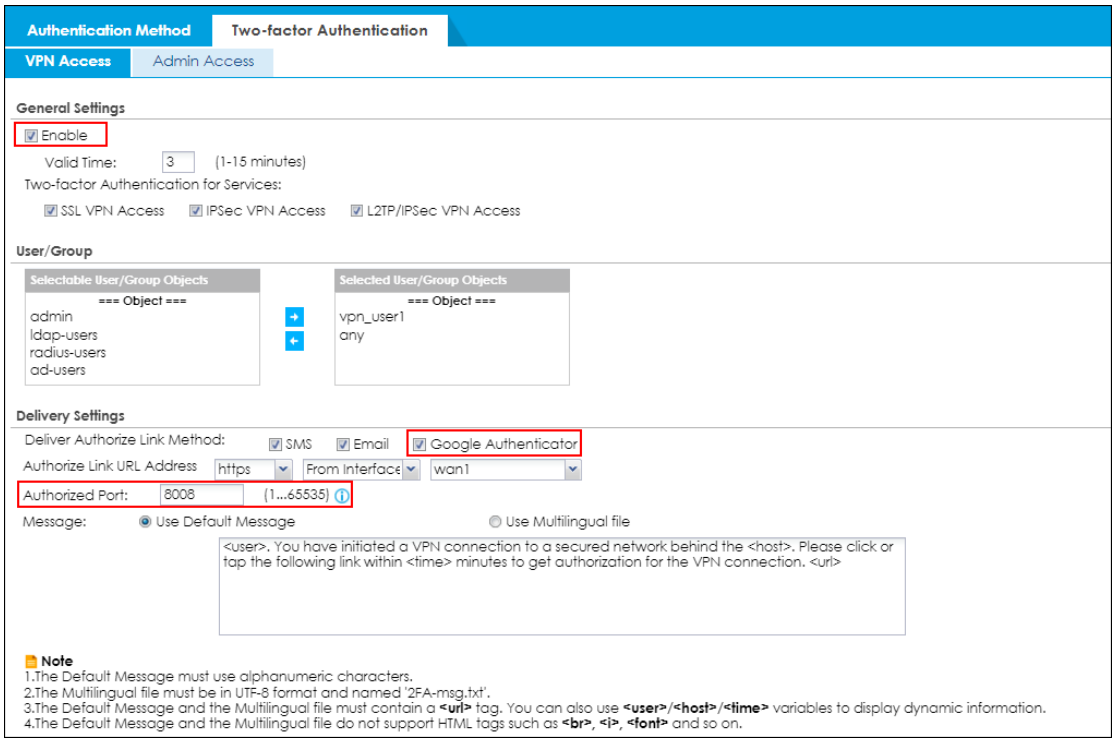
4. After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.



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

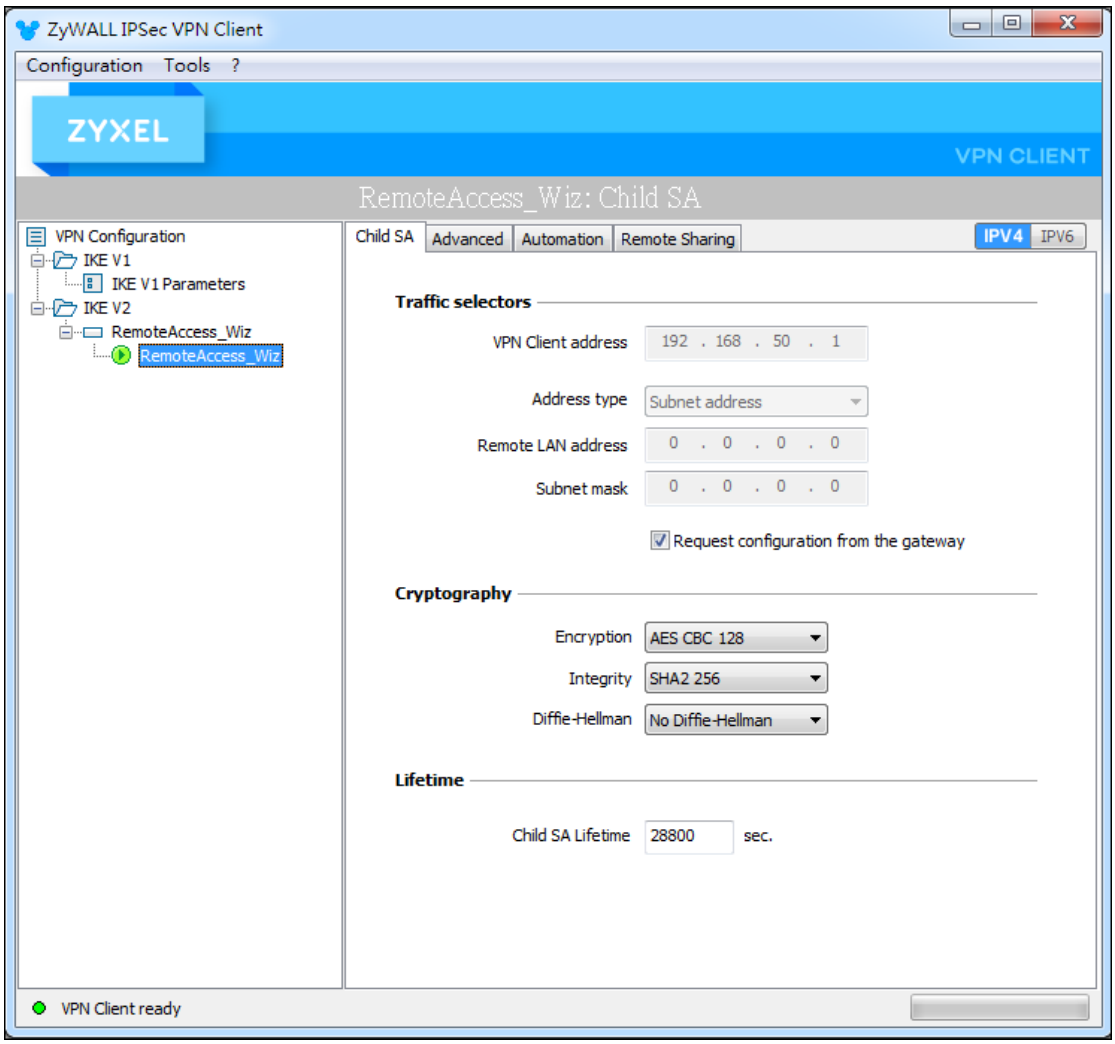
service port. After building up VPN tunnel, user have to enter the code in the Web GUI.



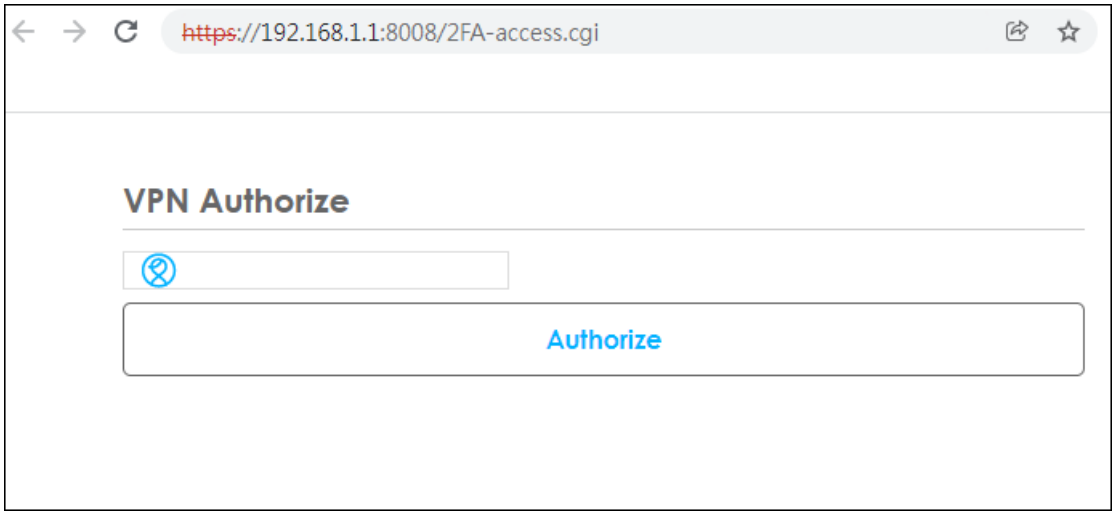
Note: If users use Zyxel VPN Client to build VPN tunnel, it will pop up authentication page on browser automatically. For SSL VPN or L2TP VPN, users have to enter correct URL on browser manually. (e.g. https://YourDeviceIP:8080)

Test the Result

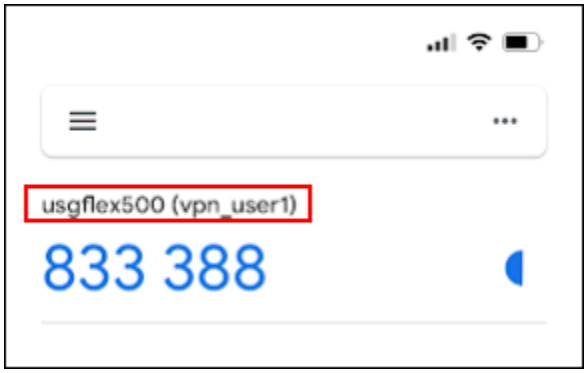
1. Build VPN tunnel on Zyxel VPN Client.



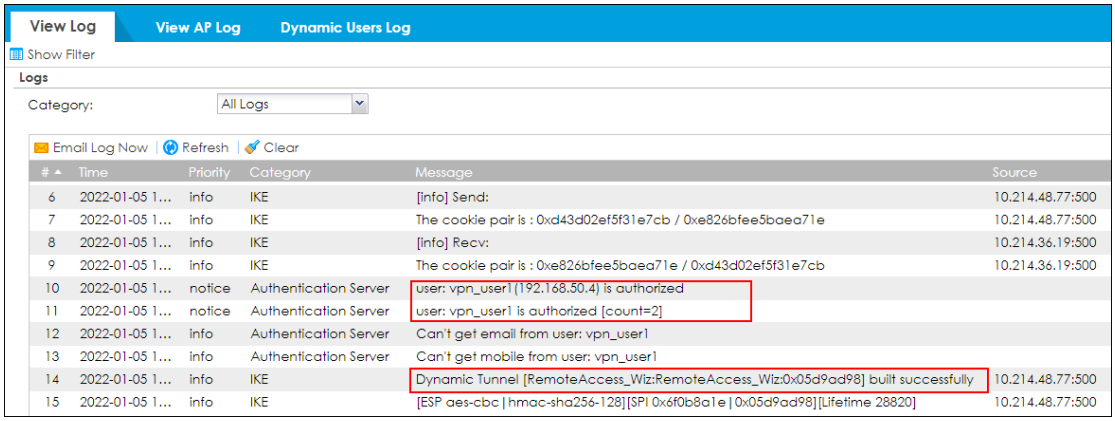
2. Browser will pop up authentication page to enter the verification code.



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.



4. Authorize with username, password and the token code successfully.



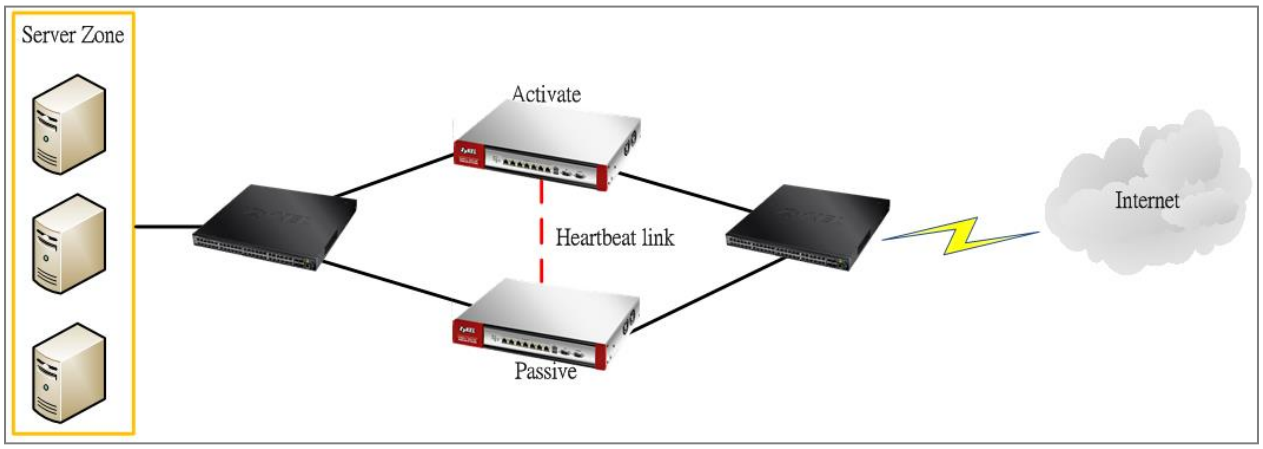
What Can Go Wrong

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.

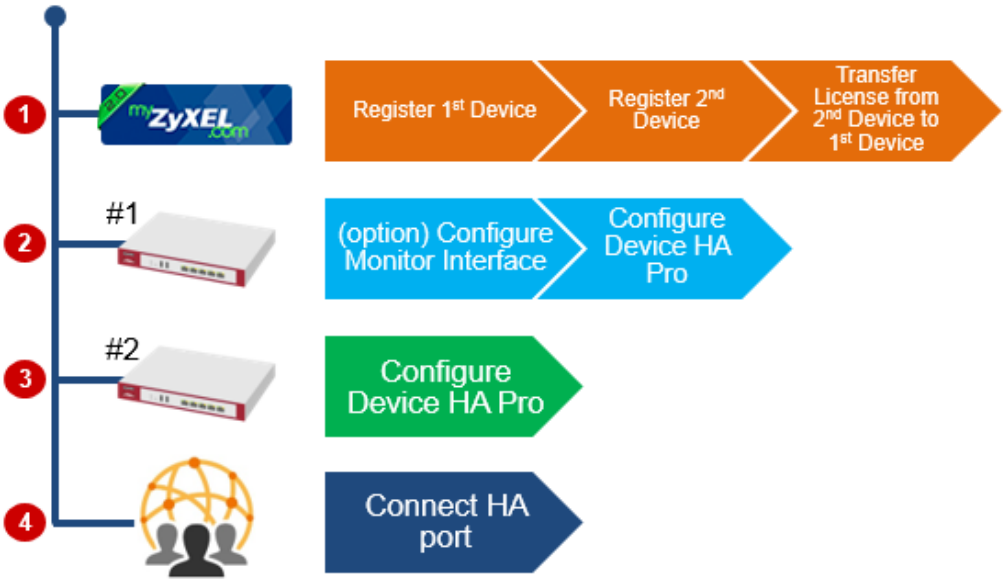
Chapter 4- Device HA

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

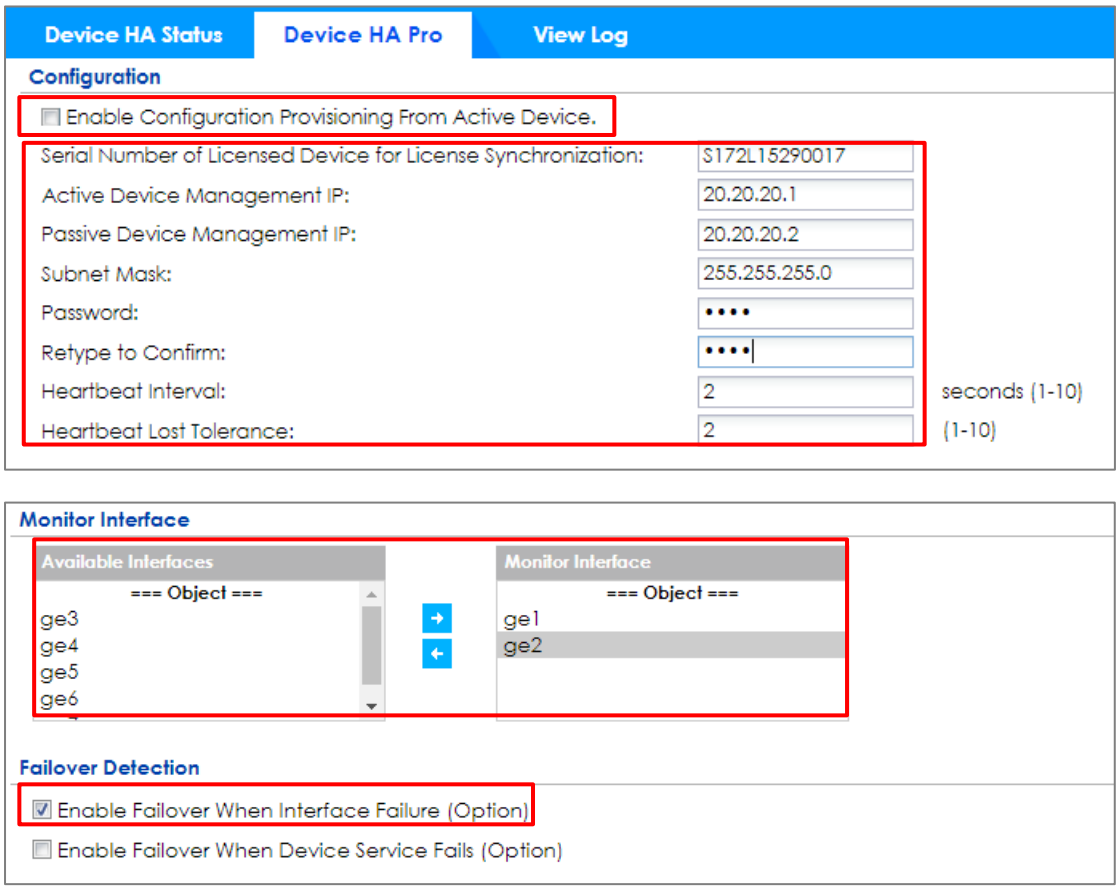
Enter the management IP address of the active and passive devices. Also, enter the password for synchronizing configuration with each other.

D. Monitoring Interfaces

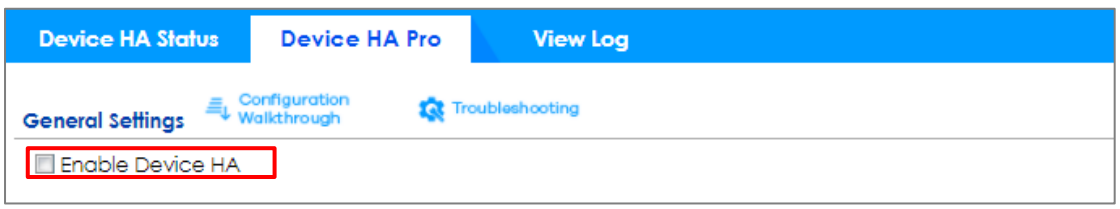
Select the interfaces which you would like to monitor.

E. Synchronization

Enable failover when one of the interfaces fails.



The Main Function of the Device HA Pro



Heartbeat Link

The heartbeat port is a new physical port on the device.

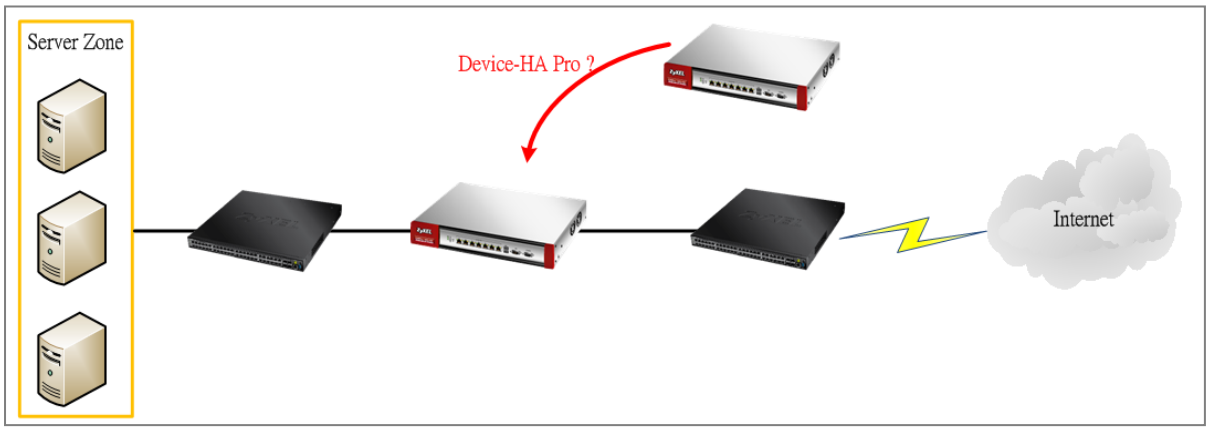
After you have enabled Device HA Pro, the devices will transmit multicast packets (UDP 694) to check each device's status.

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

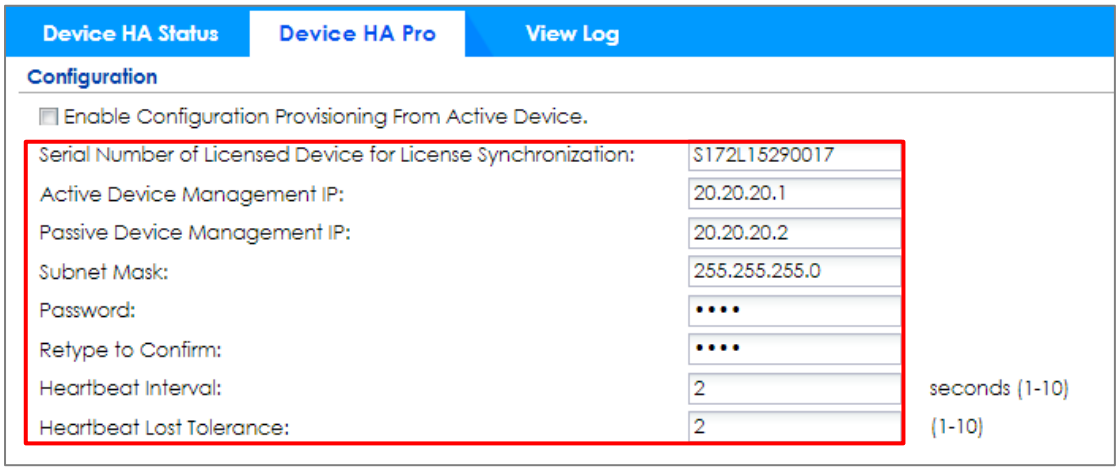
1. Transfer all the licenses to the primary device. This helps to avoid the system from recounting licenses every time.
2. Enable the connectivity check function on the monitored interfaces. When an interface doesn't receive any response from the remote server for a certain period of time, the device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

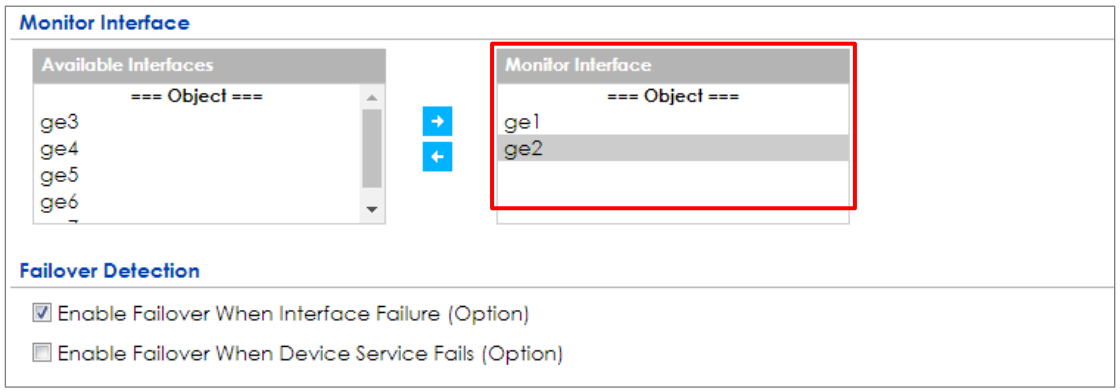
How do I Configure Device HA Pro in My Current Environment?



Configurations on the Primary Device

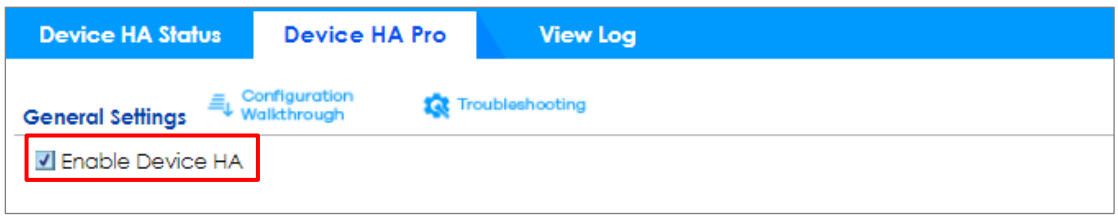
1. Go to the **Configuration** > **Device HA** > **Device HA Pro** screen.
2. Enter the device's license serial number from the **myZyXEL.com** server.
3. Enter the management IP address after enabling the Device HA Pro feature.
4. Select the interfaces which you would like to monitor.
5. Enable failover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





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

Select **Enable Device HA** and click **Apply** to enable Device HA Pro.

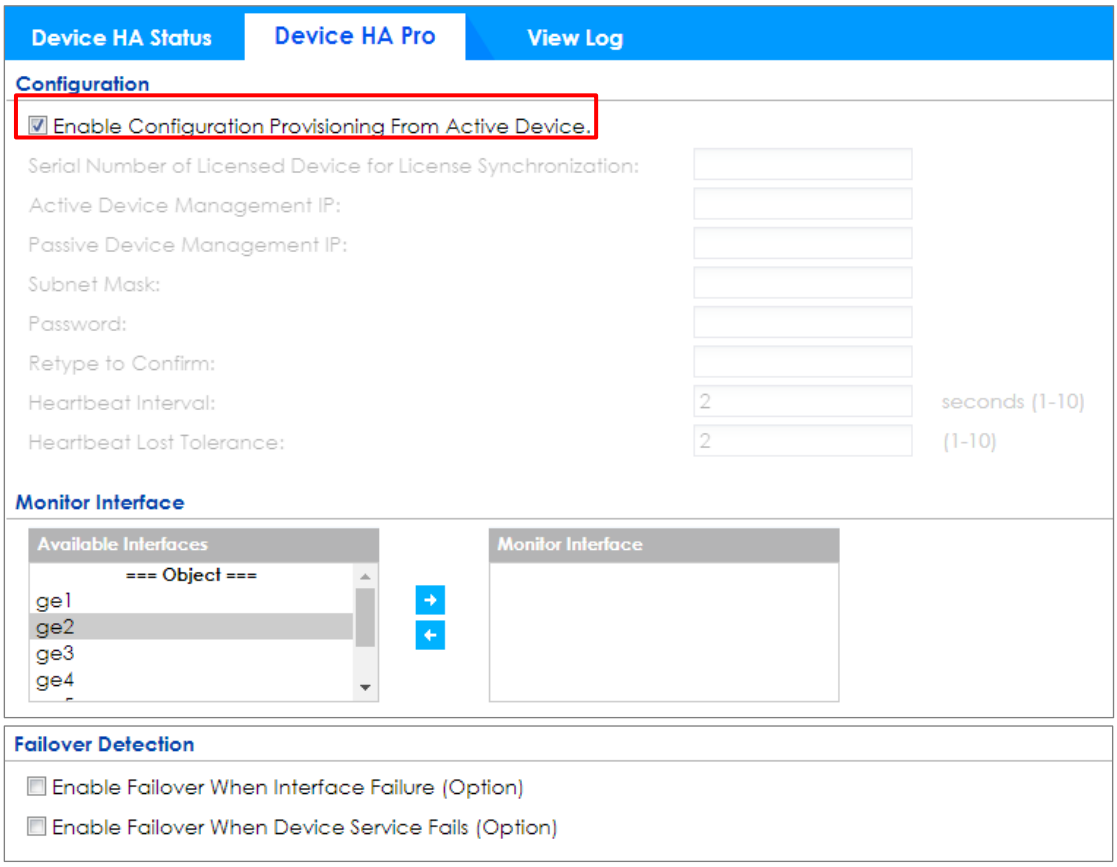


Configurations on the Secondary Device

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

Select **Enable Configuration Provisioning from Active Device**.

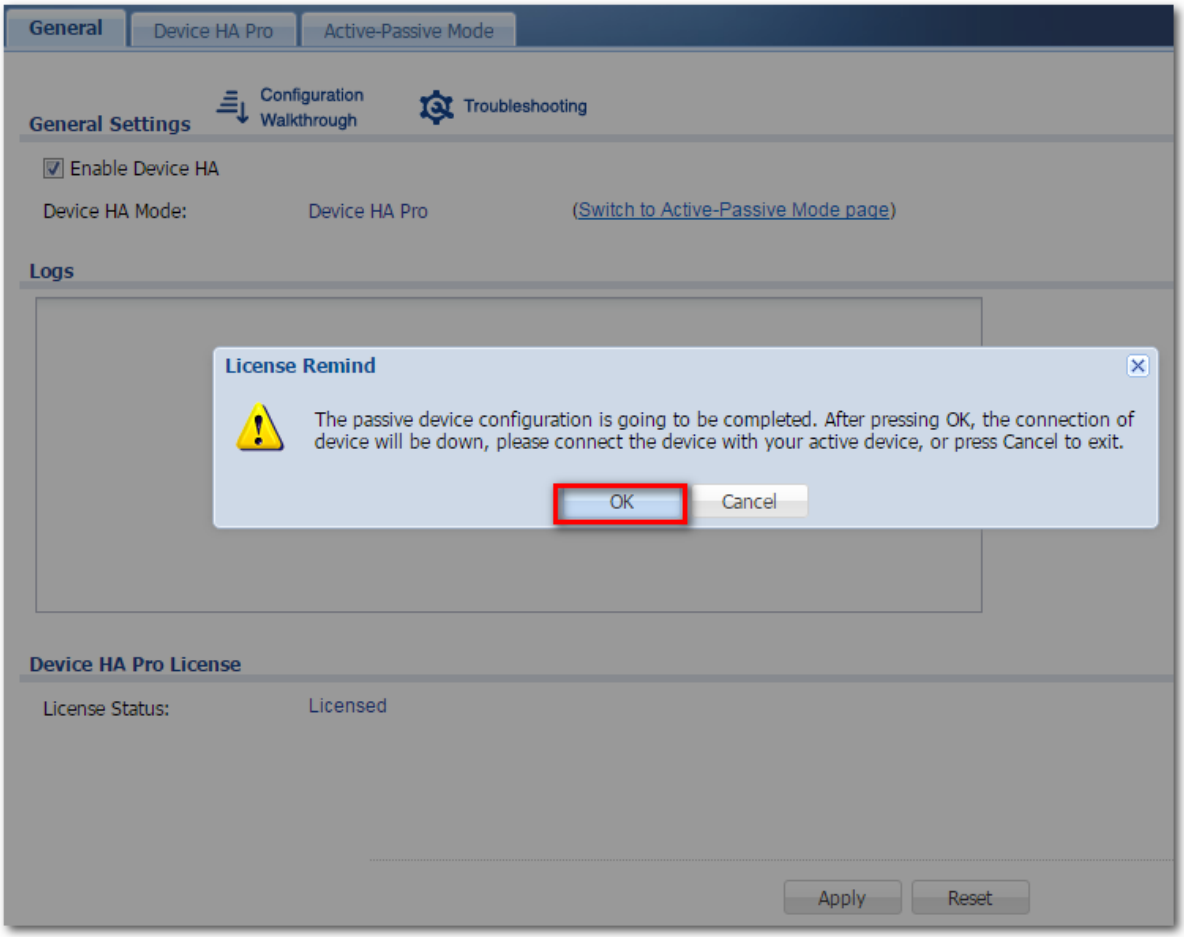
Click **Apply**.



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.



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.

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.

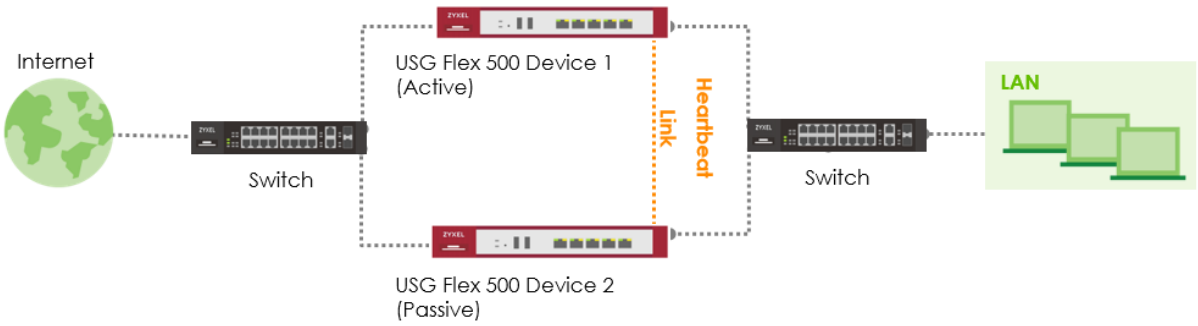
3. **Why after Device-HA failover to secondary device, it will not fallback to primary device?**

   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.

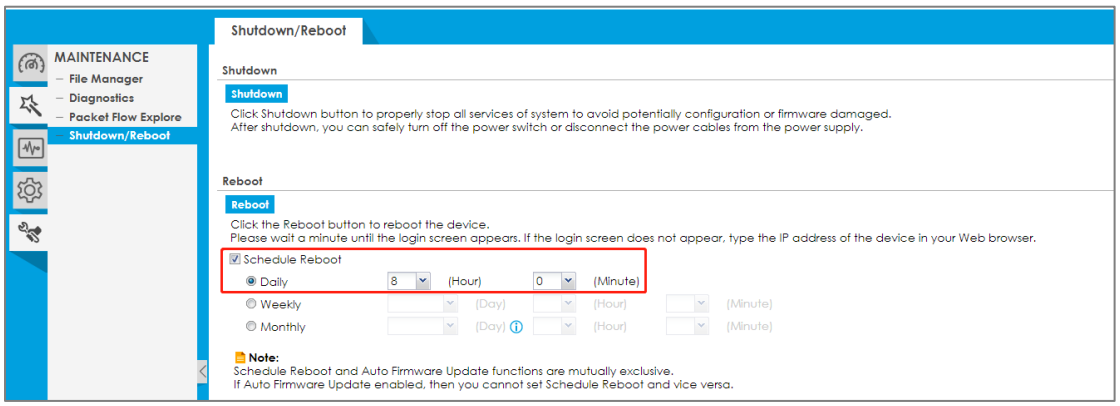
The following figure depicts Device HA scenario.



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.

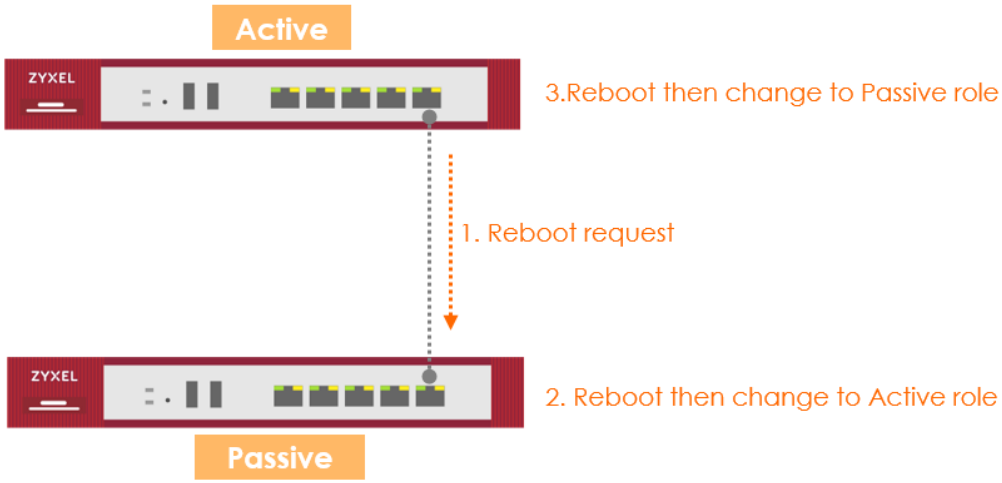


Verification

When you enable schedule reboot in Device HA mode, the active device will send reboot request to passive device first.

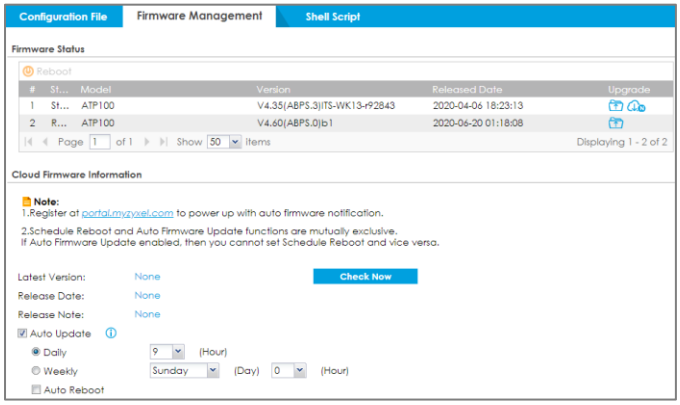
After passive device reboot successfully, the passive device changes to active role.

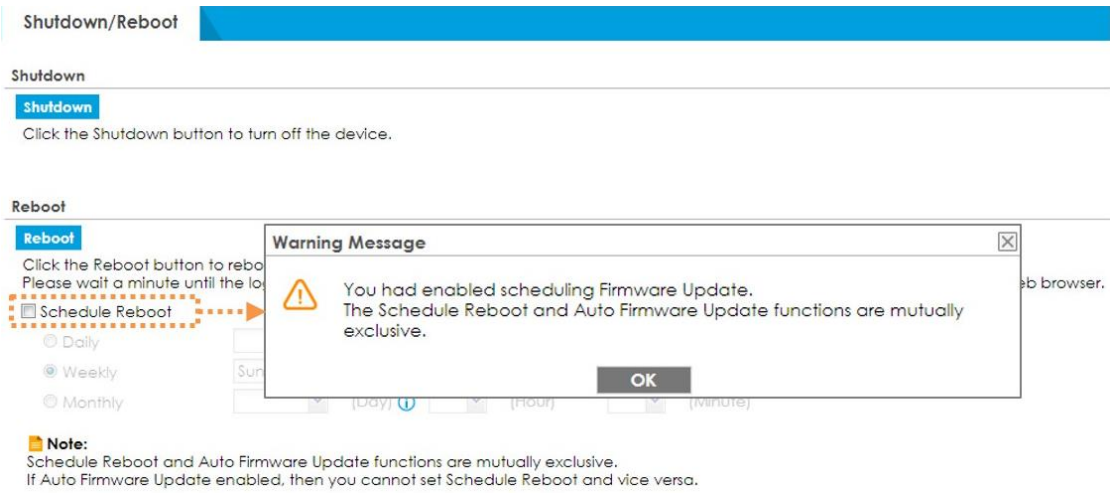
The original active device then reboots and changes to passive role afterward.
If the passive device fails to reboot, the active device will reject the reboot process and show a log: "schedule reboot, device-HA reboot sync fail"



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.




Shutdown/Reboot
Shutdown
Shutdown
Click the Shutdown button to turn off the device.
Reboot
Reboot
Click the Reboot button to rebo
Please wait a minute until the lo
b browser.
Schedule Reboot
Daily
Weekly
Monthly
Warning Message
You had enabled scheduling Firmware Update.
The Schedule Reboot and Auto Firmware Update functions are mutually exclusive.
OK
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

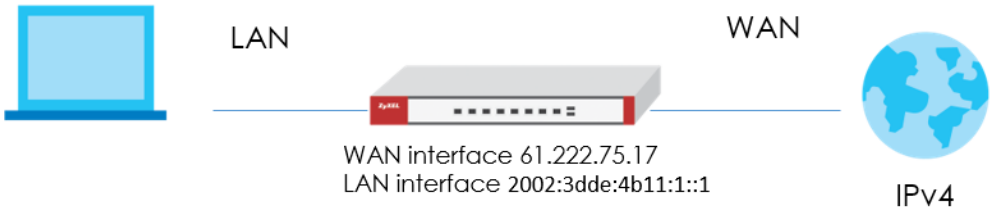
This example shows how to configure your ATP/USG Flex's WAN as IPv4 address and LAN interface as auto-configuration.

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

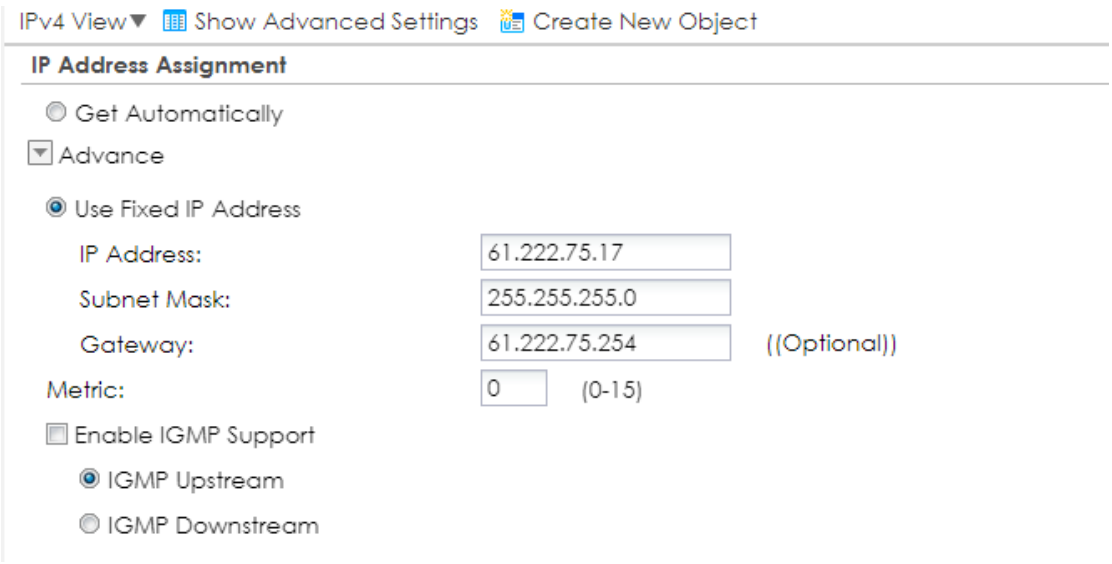


Setting Up the IPv4 Interfaces

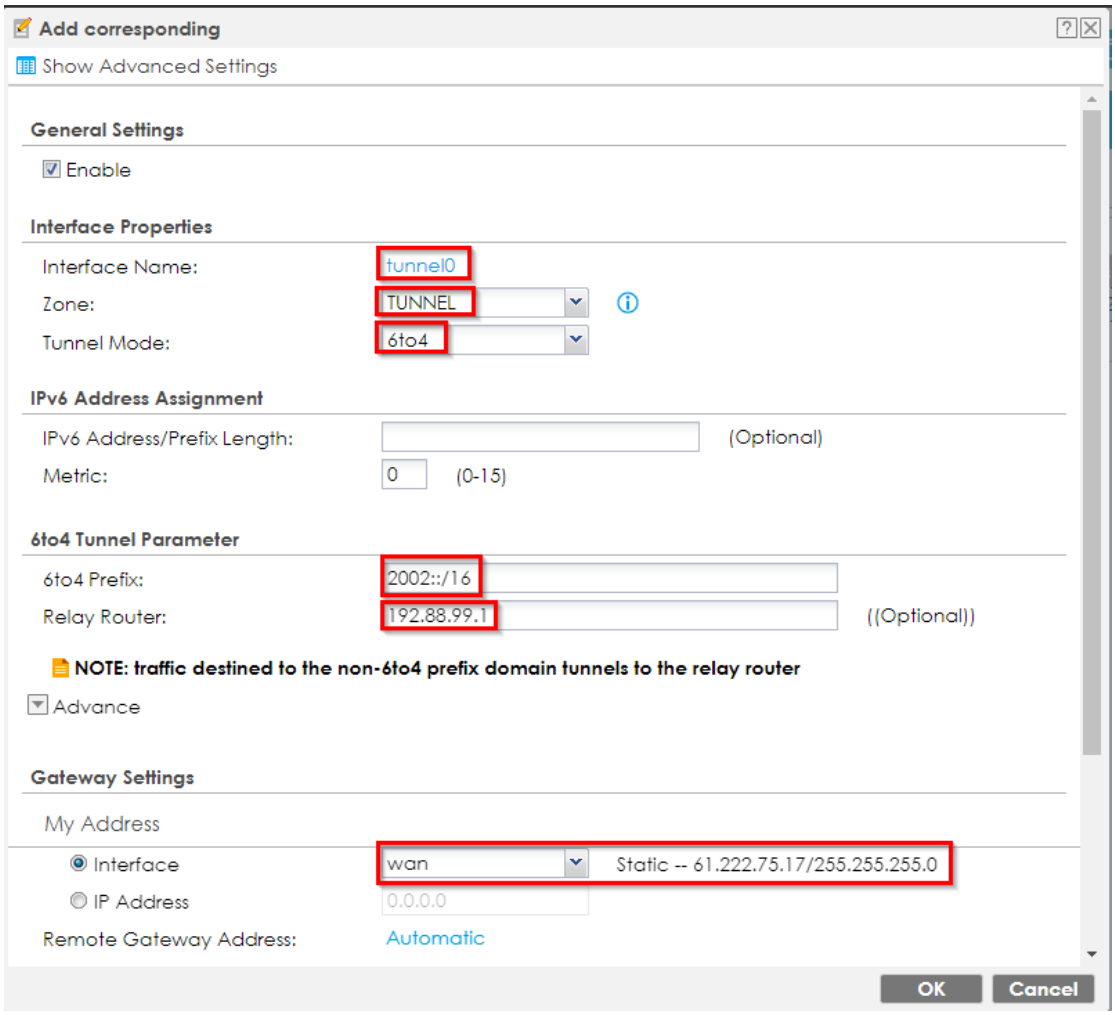
Wan

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.

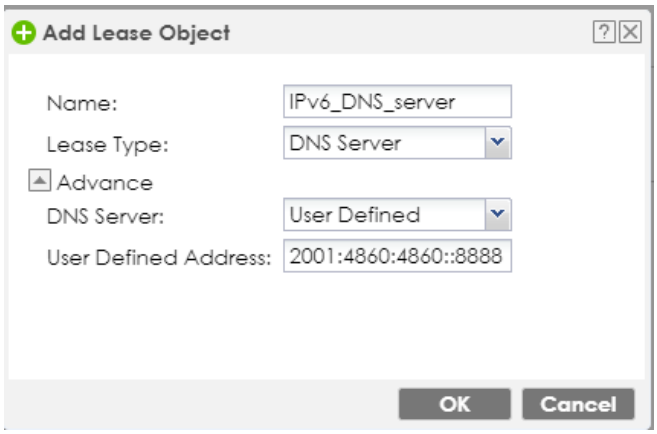


3. Navigate to CONFIGURATION > Network > Interface > Tunnel > Add, Select Enable. Enter tunnel0 as the Interface Name and select 6to4 as the Tunnel Mode. In the 6to4 Tunnel Parameter section, this example just simply uses the default 6to4 Prefix, 2002::/16. Enter your Relay Router's IP address (192.88.99.1 in this example). Select wan1 as the Gateway. Click OK



Lan

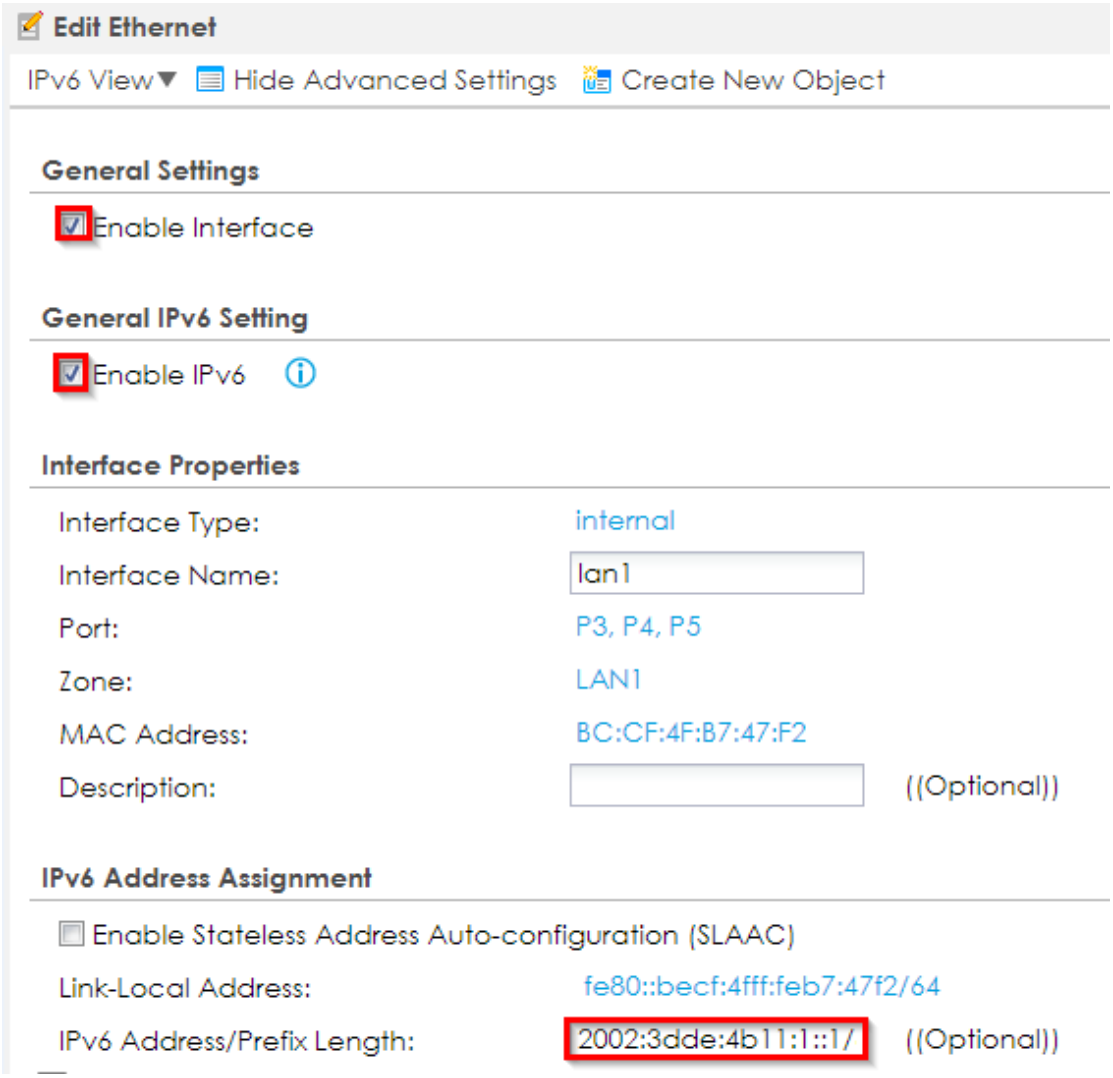
1. Create IPv6 DHCP DNS Server object. (Configuration > Object > DHCPv6 > Lease > Add)



In the Configuration > Ethernet > IPv6 Configuration section, double-click the LAN interface you want to modify.

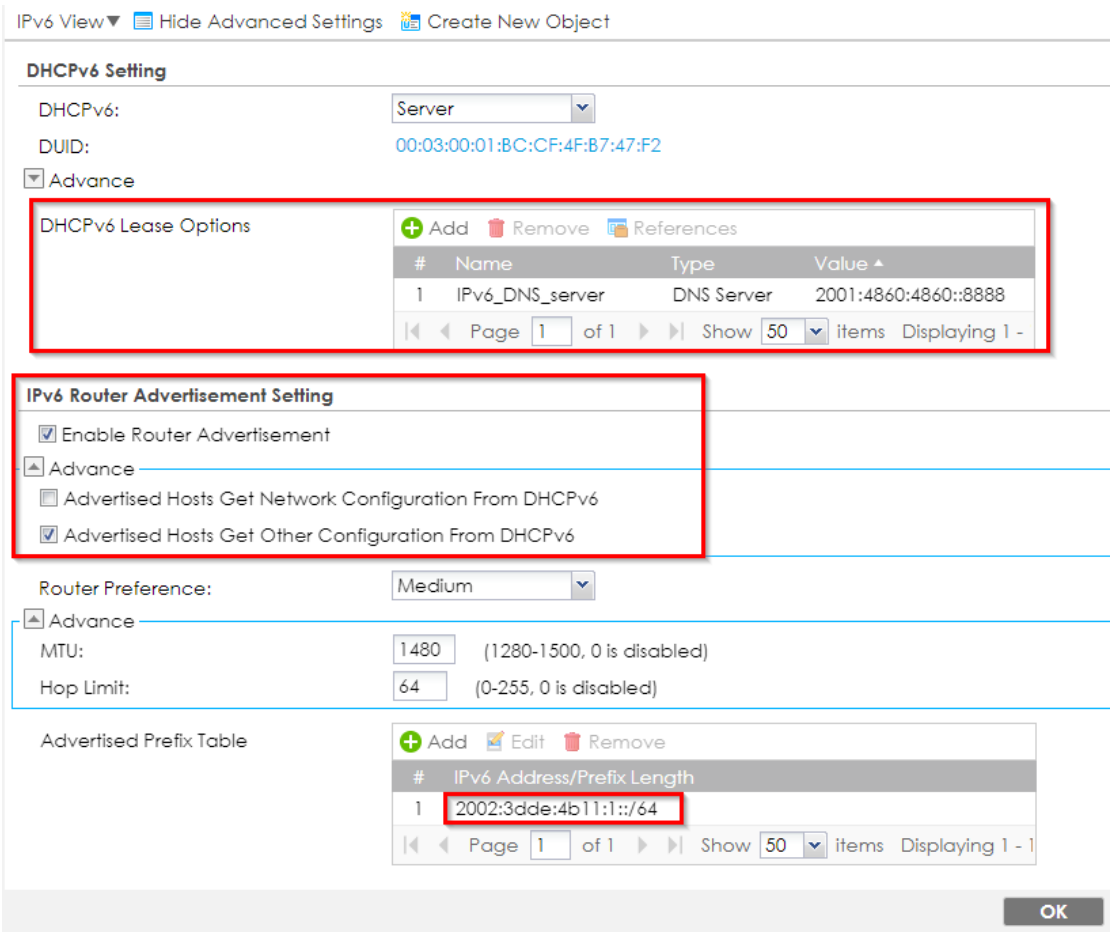
2. Enable Interface and Enable IPv6.

Key in IPv6 Address/Prefix Length:2002:3dde:4b11:1::1/64



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



Test the result

How to set up 6to4 on the WAN and DHCPv6 on the LAN

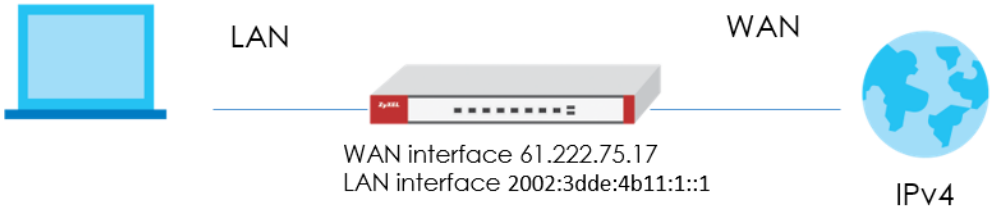
This example shows how to configure your ATP/USG Flex's WAN as IPv4 address and LAN interface as auto-configuration.

In this scenario:

WAN IPv4 Address is 61.222.75.17

DNS Server Set as 2001:4860:4860::8888

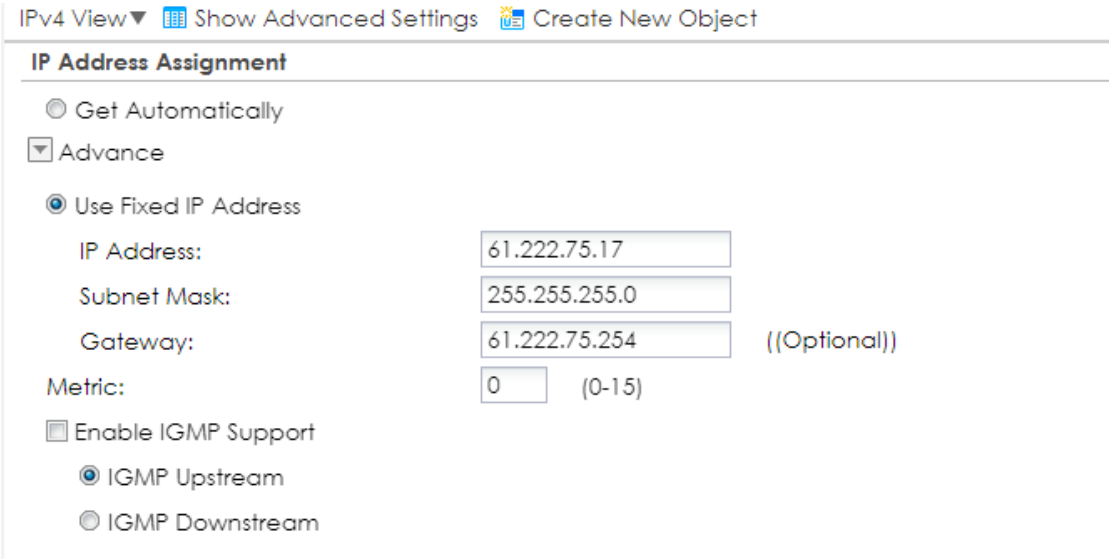
LAN Subnet Set as 2002:3dde:4b11:1::/64



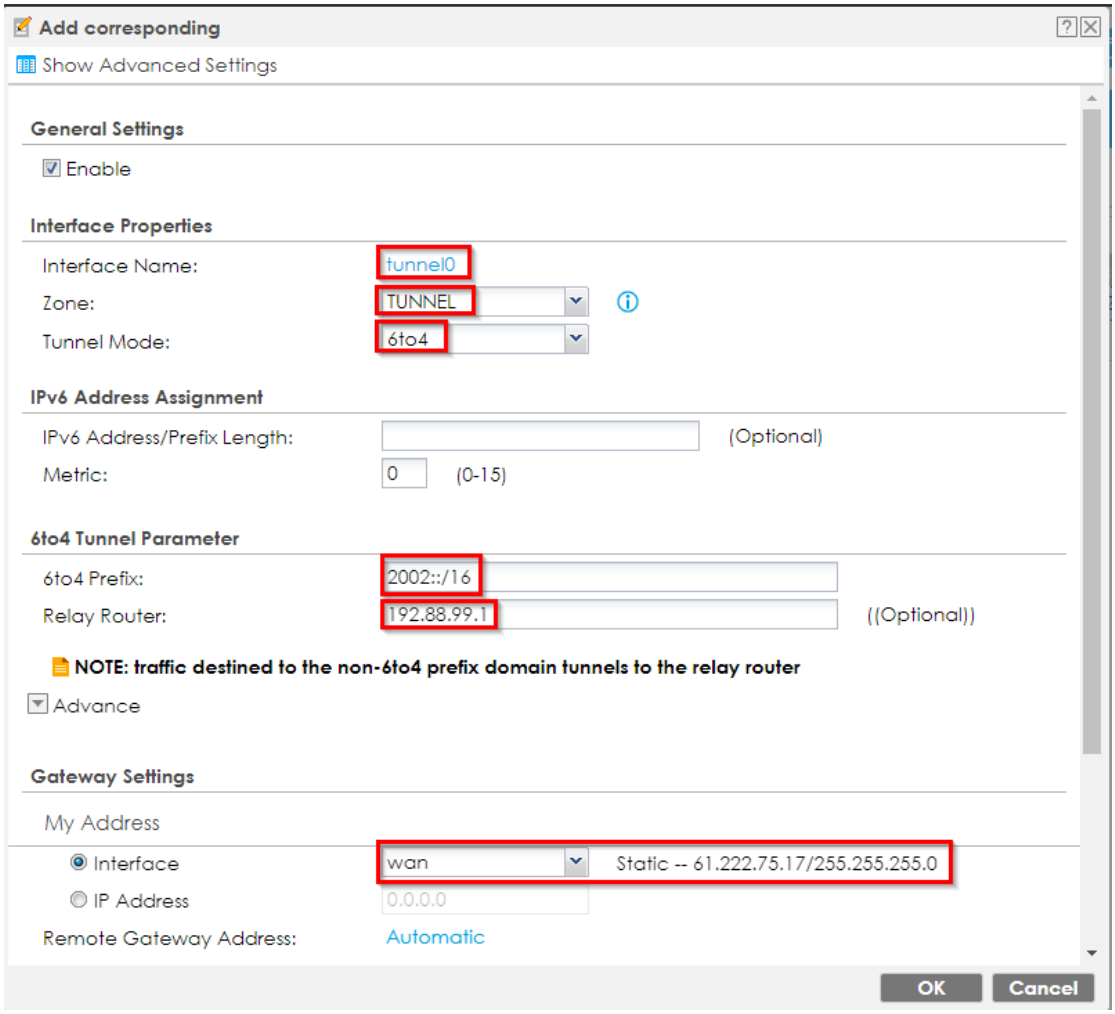
Setting Up the IPv4 Interfaces

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.

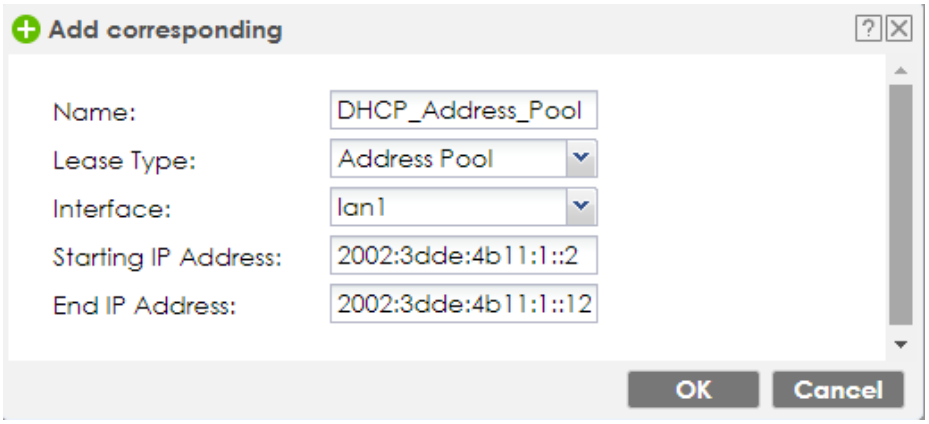


3. Navigate to CONFIGURATION > Network > Interface > Tunnel > Add, Select Enable. Enter tunnel0 as the Interface Name and select 6to4 as the Tunnel Mode. In the 6to4 Tunnel Parameter section, this example just simply uses the default 6to4 Prefix, 2002::/16. Enter your Relay Router's IP address (192.88.99.1 in this example). Select wan1 as the Gateway. Click OK

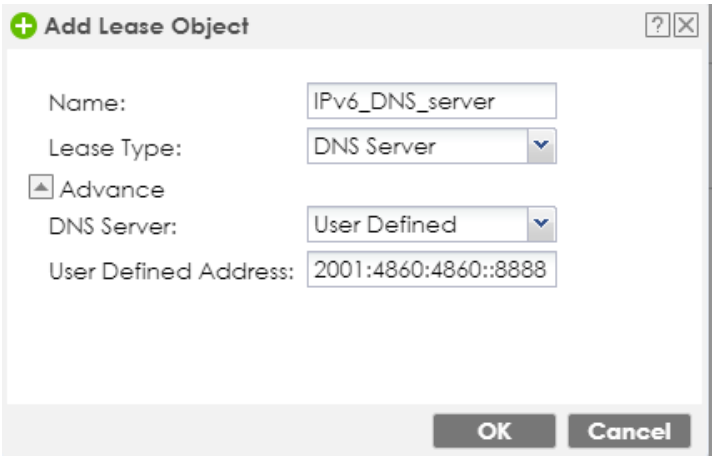


Lan

1. Create IPv6 DHCP Pool (Configuration > Object > DHCPv6 > Lease > Add)

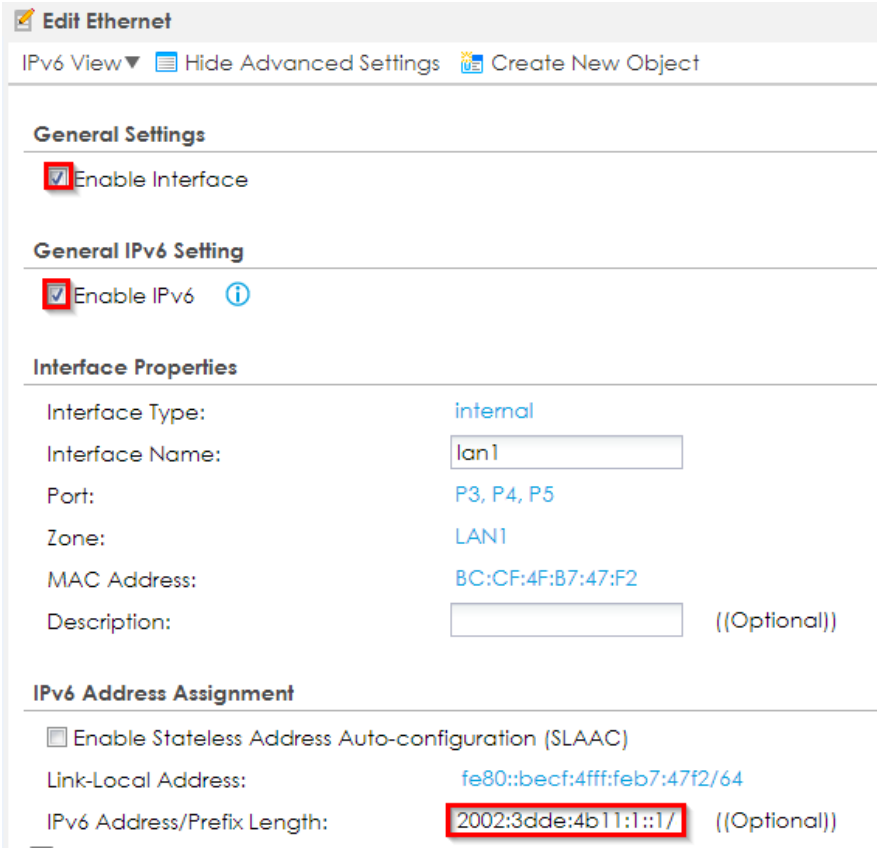


2. Create IPv6 DHCP DNS Server object. (Configuration > Object > DHCPv6 > Lease > Add)



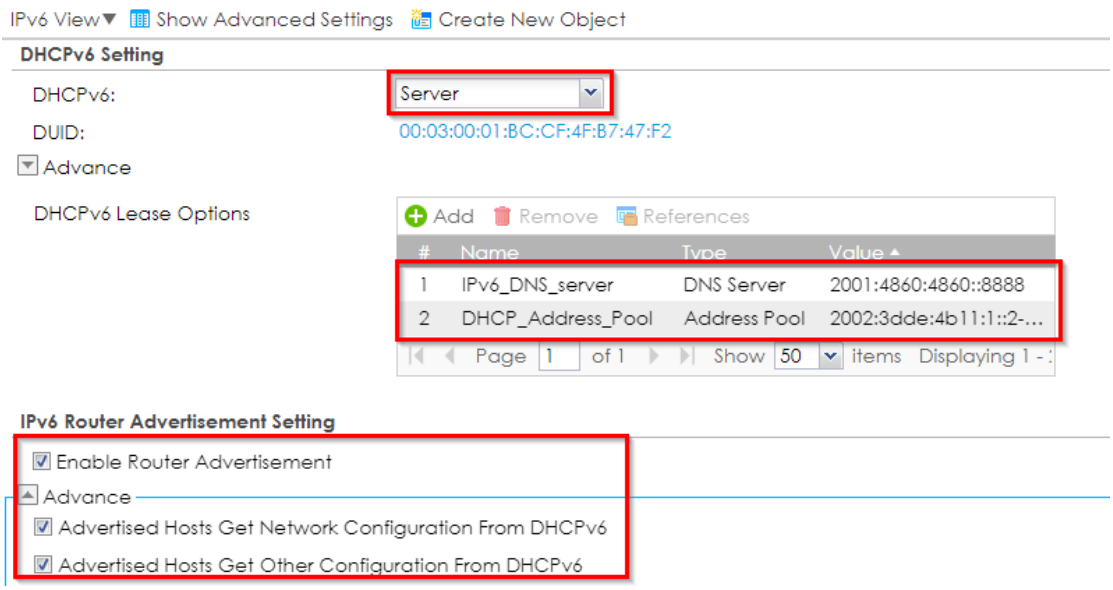
In the Configuration > Ethernet > IPv6 Configuration section, double-click the LAN interface you want to modify.

3. Enable Interface and Enable IPv6. Key in IPv6 Address/Prefix Length: 2002:3dde:4b11:1::1/64



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.

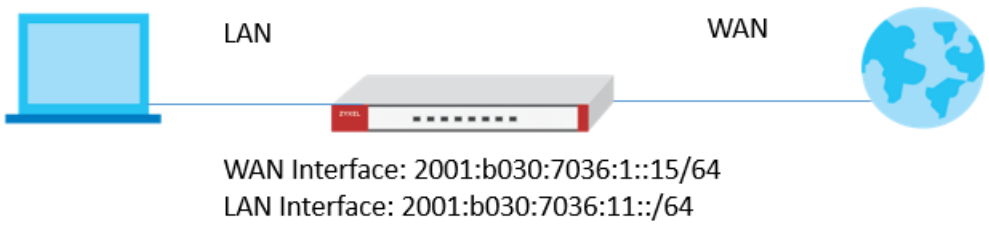


Test the result

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

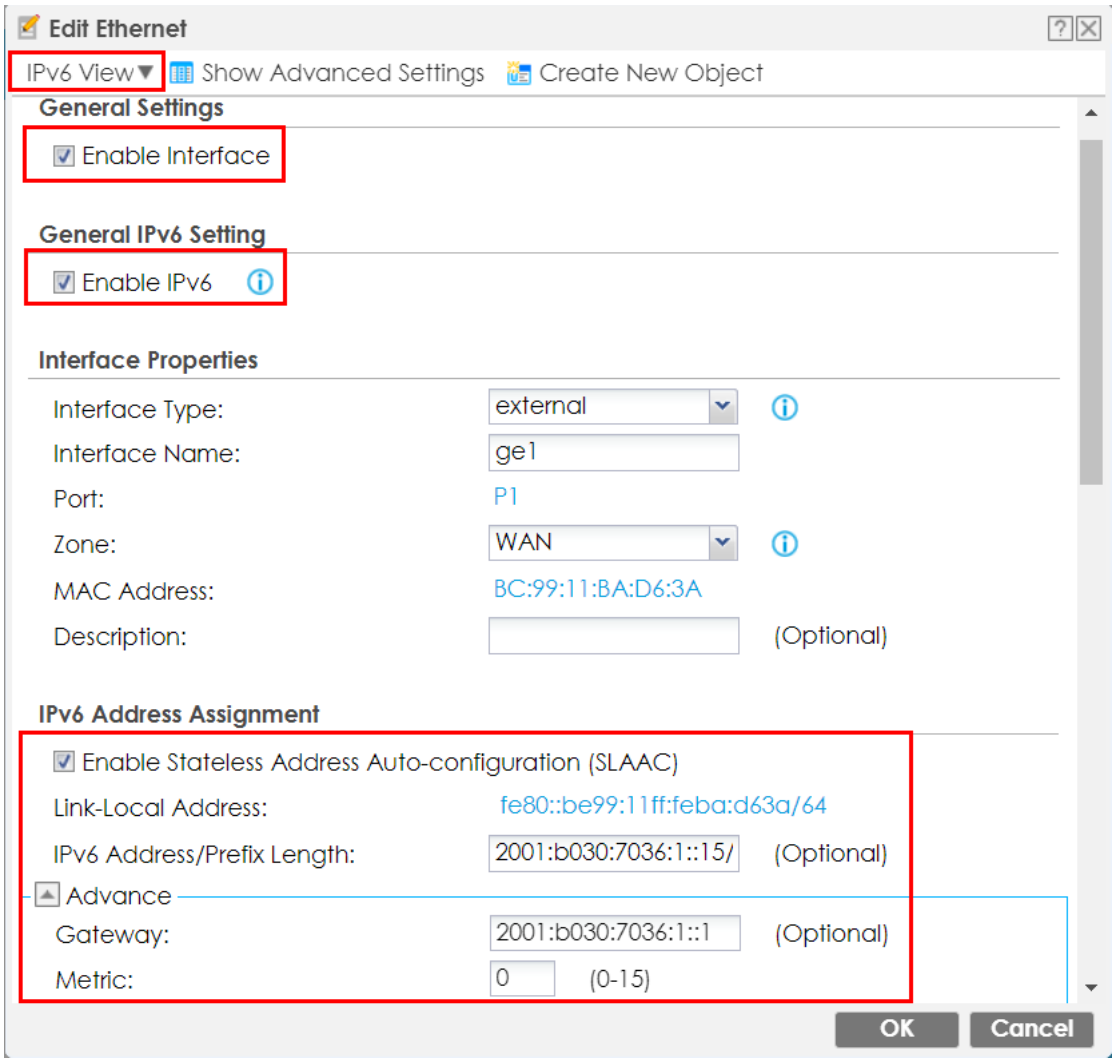


Setting Up the IPv6 Interfaces

Wan

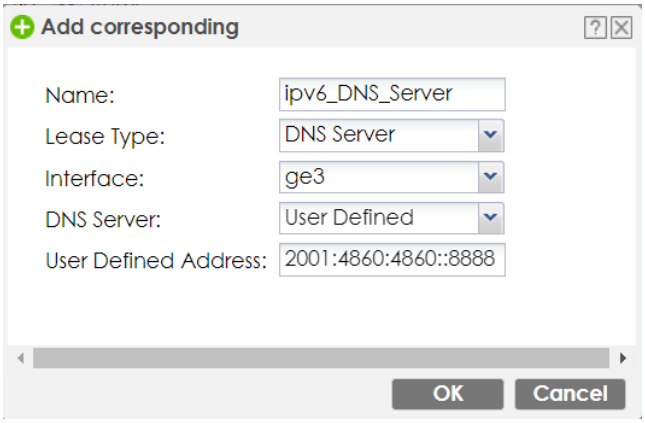
1. In the Configuration > Ethernet > IPv6 Configuration section, double-click the WAN interface you want to modify.

2. Choose IPv6 View, Enable Interface and Enable IPv6. In IPv6Address/Prefix Length text box, key in the Static IPv6 address.



Lan

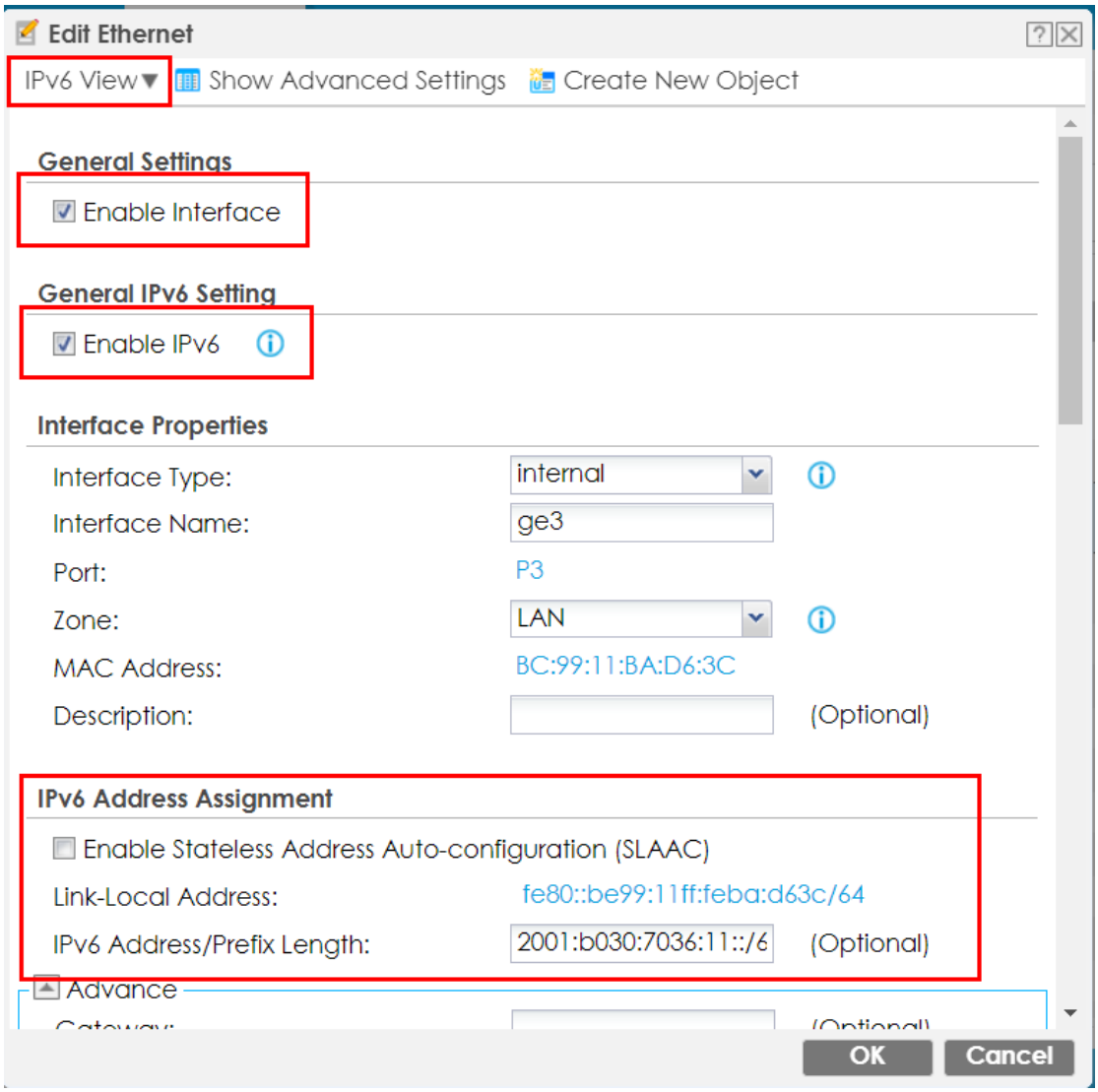
1. Create IPv6 DHCP DNS Server object. (Configuration > Object > DHCPv6 > Lease > Add)



In the Configuration > Ethernet > IPv6 Configuration section, double-click the LAN interface you want to modify.

2. Enable Interface and Enable IPv6.

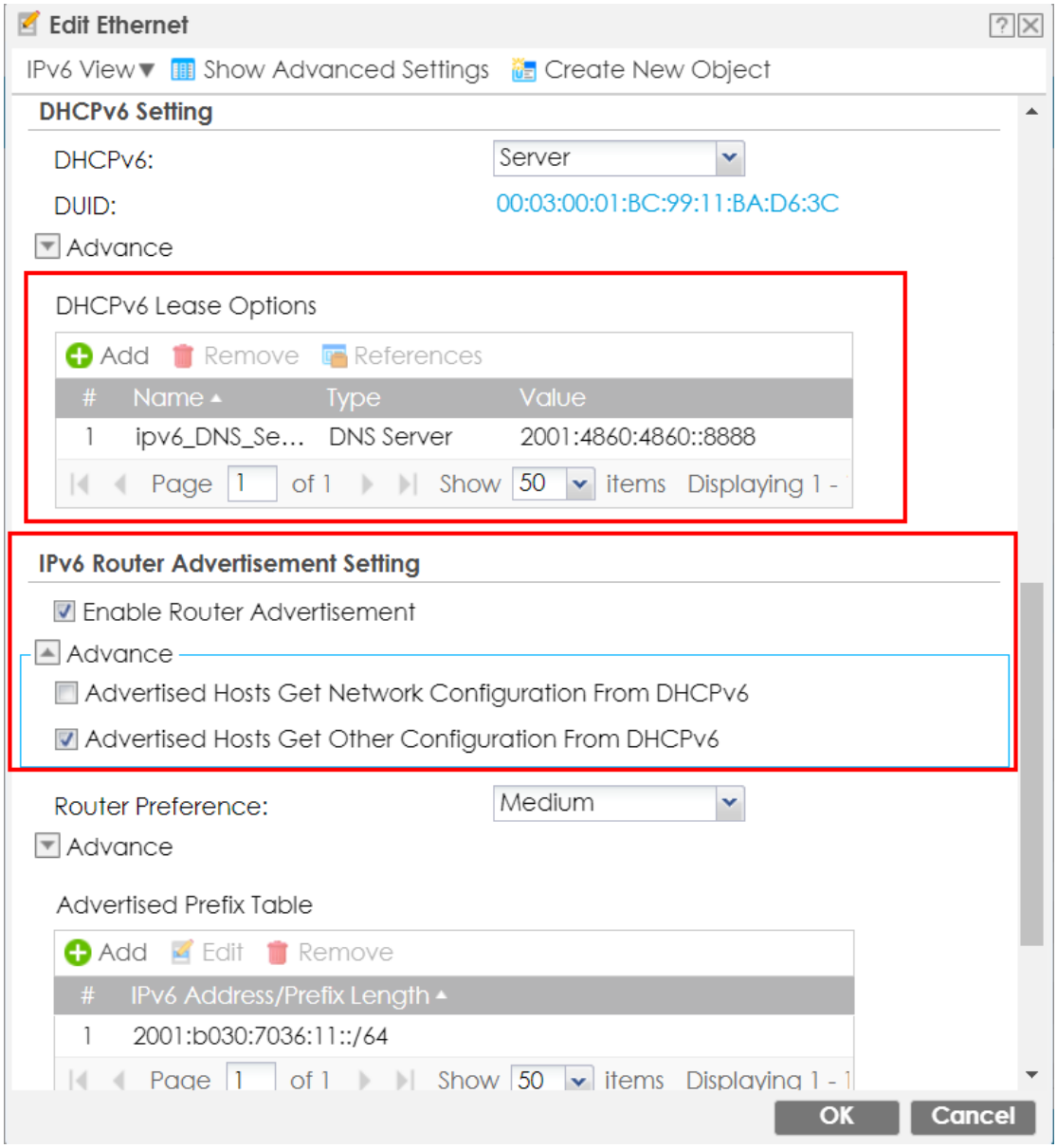
Key in IPv6 Address/Prefix Length.



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.



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

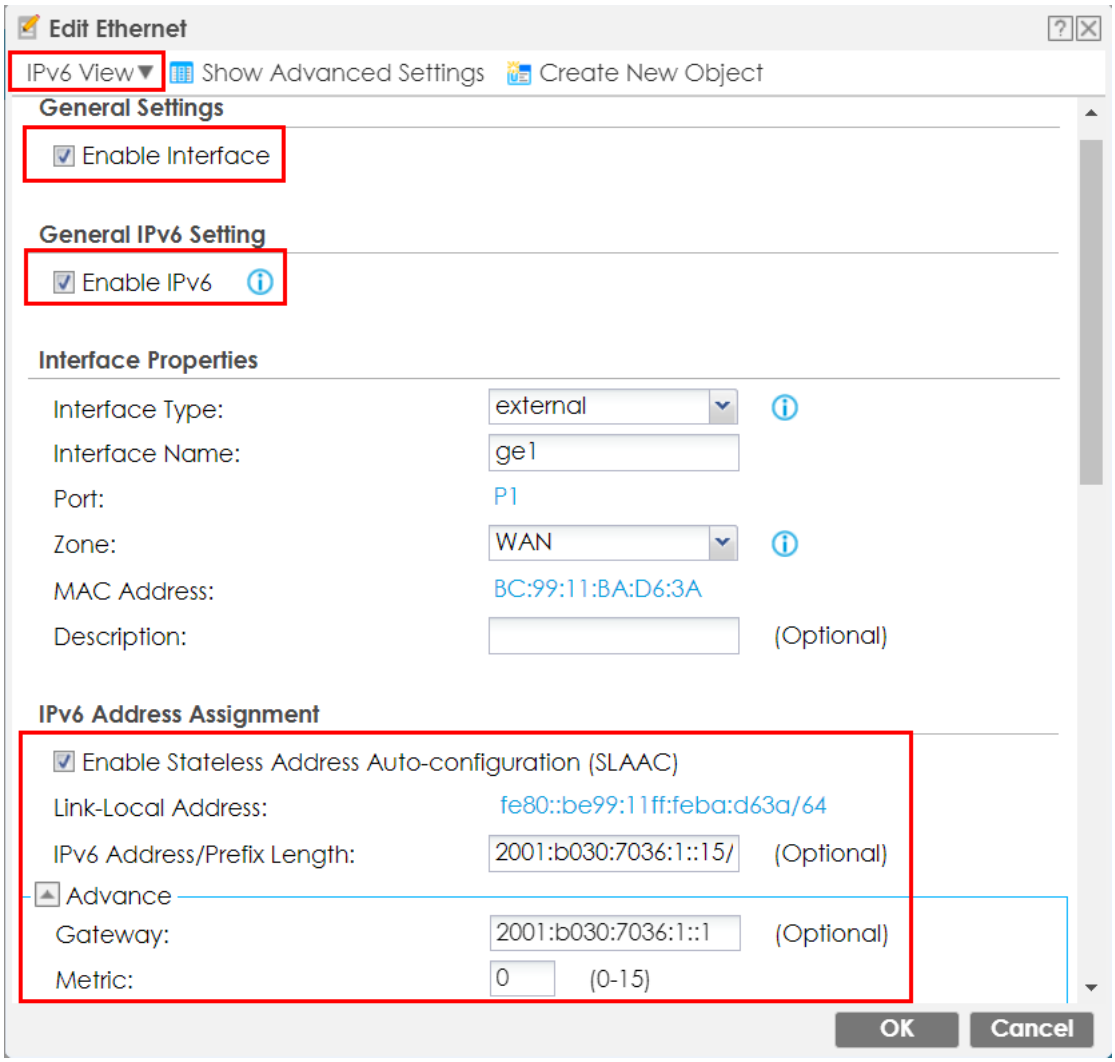
WAN Interface: 2001:b030:7036:1::15/64
LAN Interface: 2001:b030:7036:10::/64

Setting Up the IPv6 Interfaces

Wan

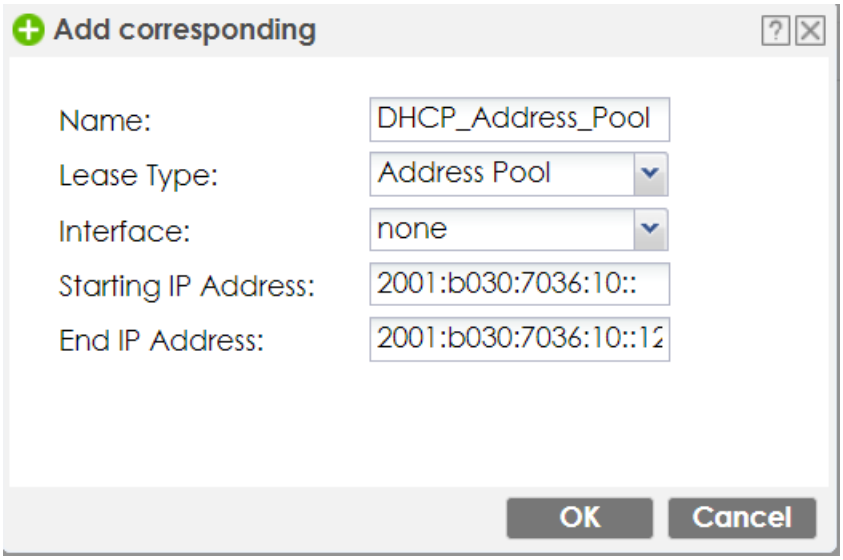
In the Configuration > Ethernet > IPv6 Configuration section, double-click the WAN interface you want to modify.

1. Choose IPv6 View and Enable Interface and Enable IPv6.
2. In IPv6Address/Prefix Length text box, key in the Static IPv6 address.

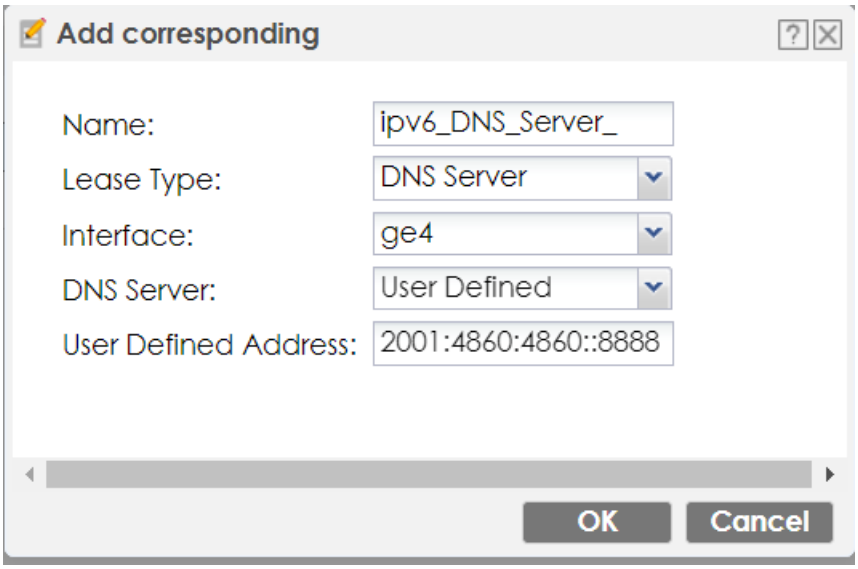


Lan

1. Create IPv6 DHCP Pool(Configuration > Object > DHCPv6 > Lease > Add)



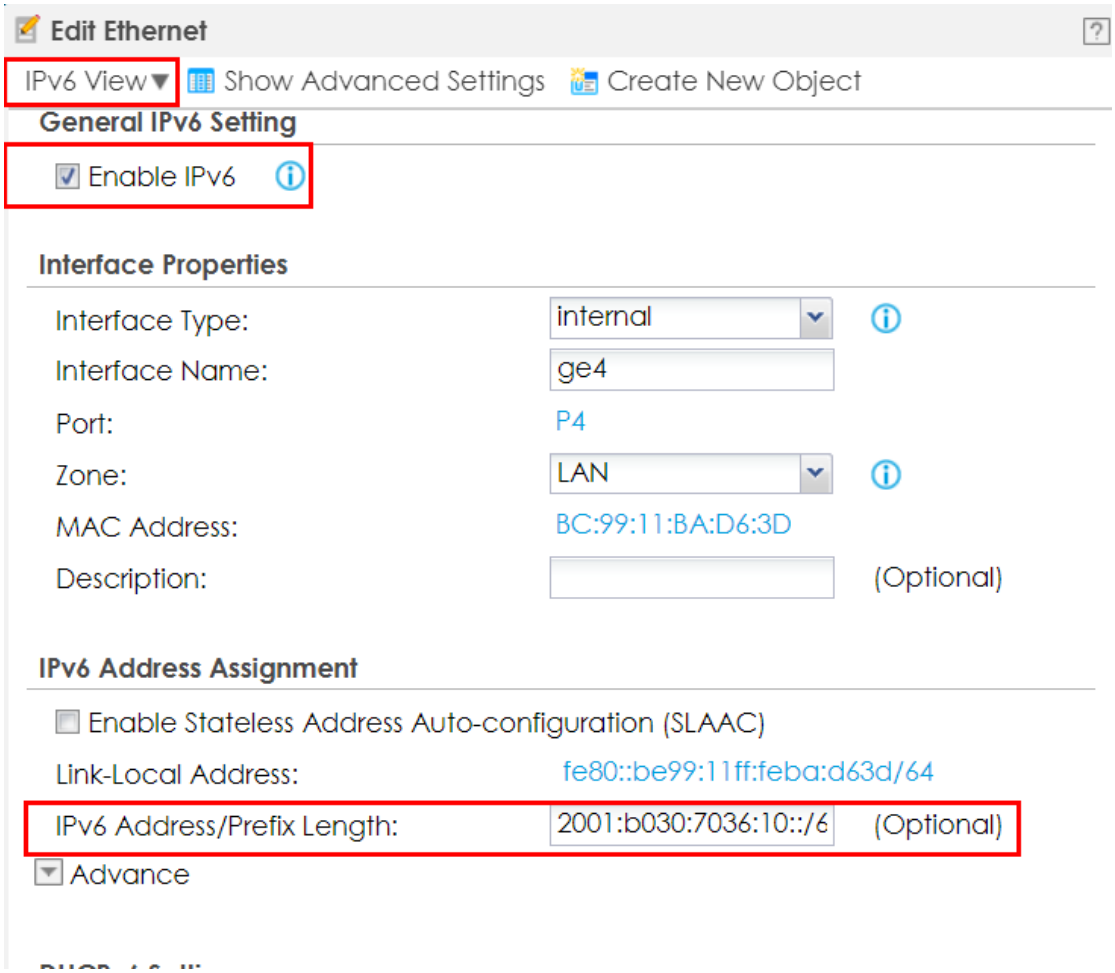
2. Create IPv6 DHCP DNS Server object. (Configuration > Object > DHCPv6 > Lease > Add)



In the Configuration > Ethernet > IPv6 Configuration section, double-click the LAN interface you want to modify.

3. Enable Interface and Enable IPv6.

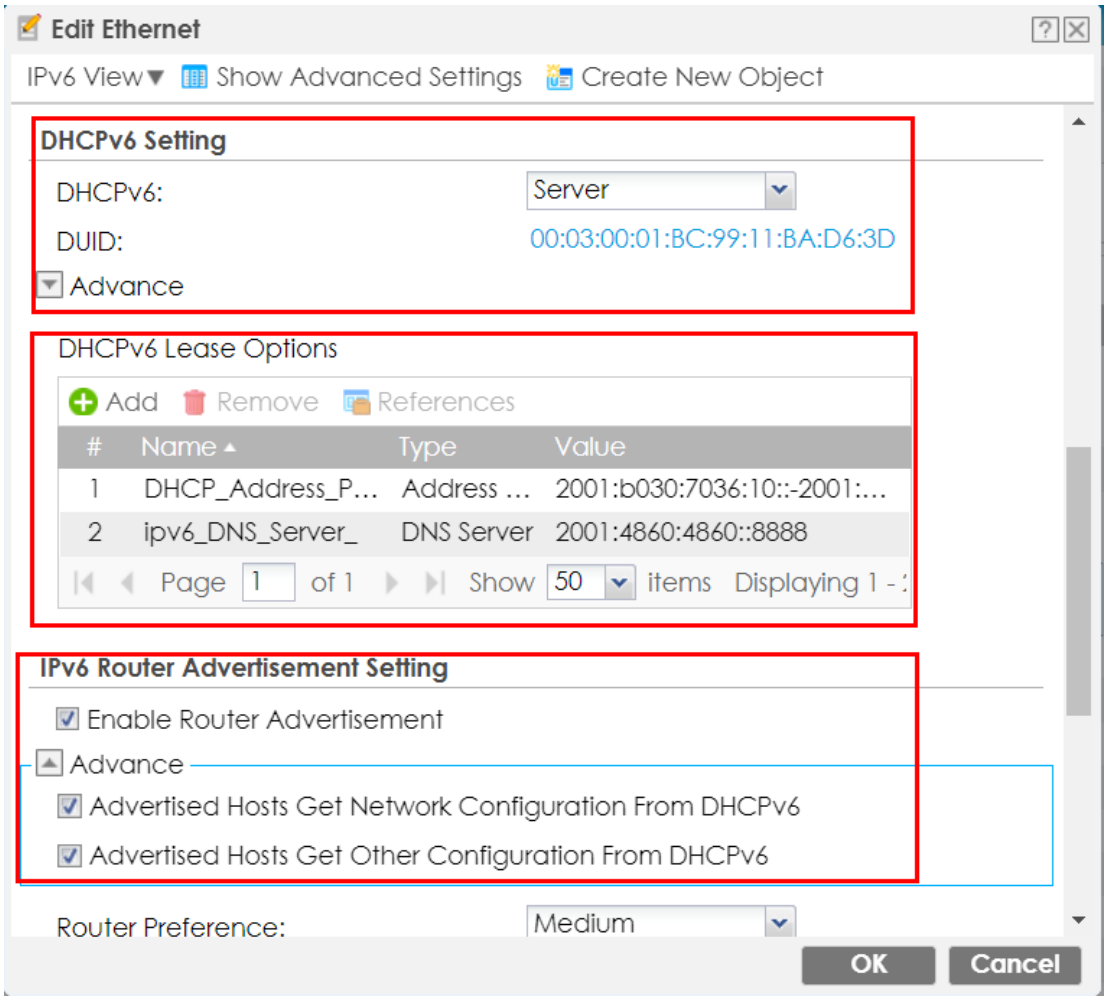
Key in IPv6 Address/Prefix Length



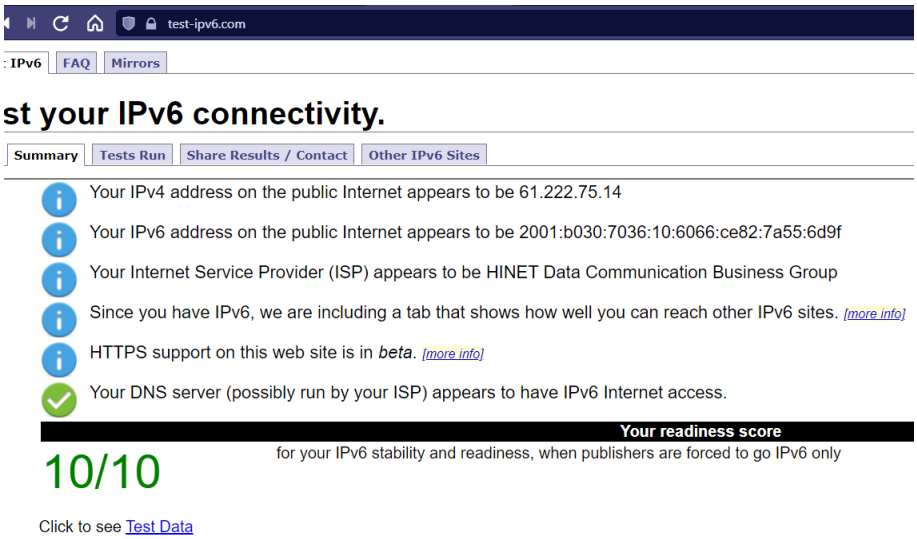
4. Scroll down and choose Server for DHCPv6 dropdown menu.

Navigate to IPv6 Router Advertisement Setting.

5. Enable Router Advertisement, Host Get Network Configuration From DHCPv6 and Hosts Get Other Configuration From DHCPv6 checkboxes.



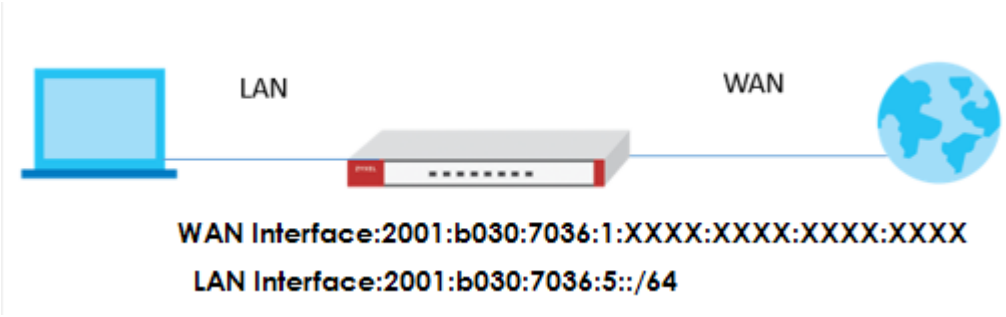
Test The Result



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



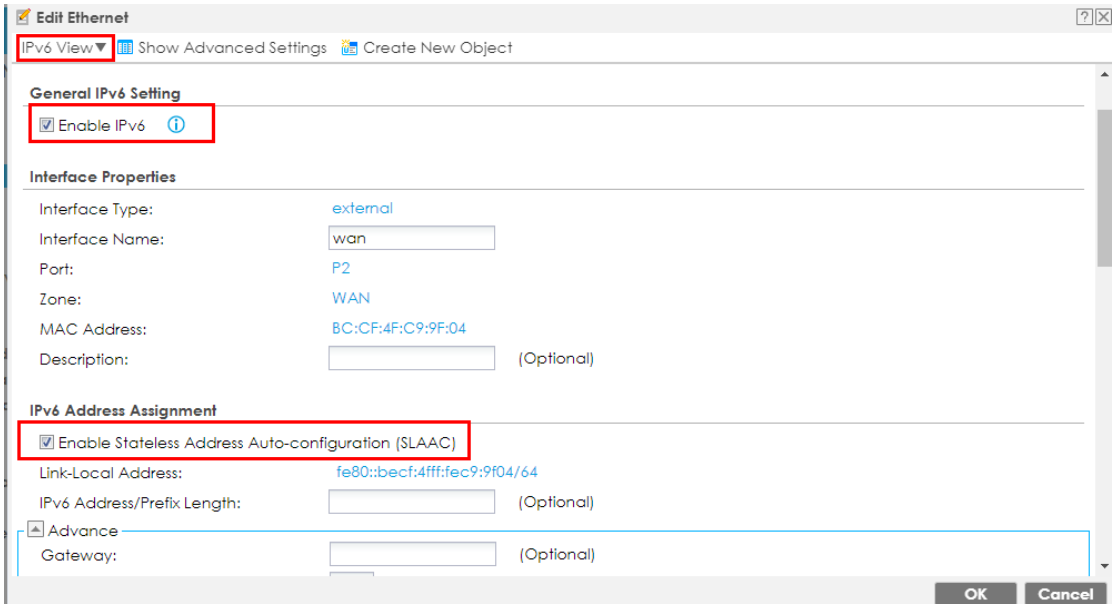
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP/USG Flex (Firmware Version: 5.00)

Setting Up the IPv6 Interfaces

Wan

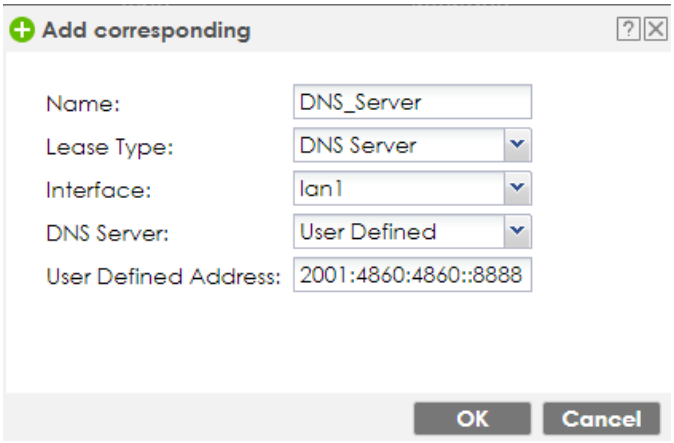
1. In the Configuration > Ethernet > IPv6 Configuration section, double-click the WAN interface you want to modify.

2. Choose IPv6 View, Enable Interface and Enable IPv6. In IPv6Address Assignment text box, enable Stateless Address Auto-configuration (SLAAC)



Lan

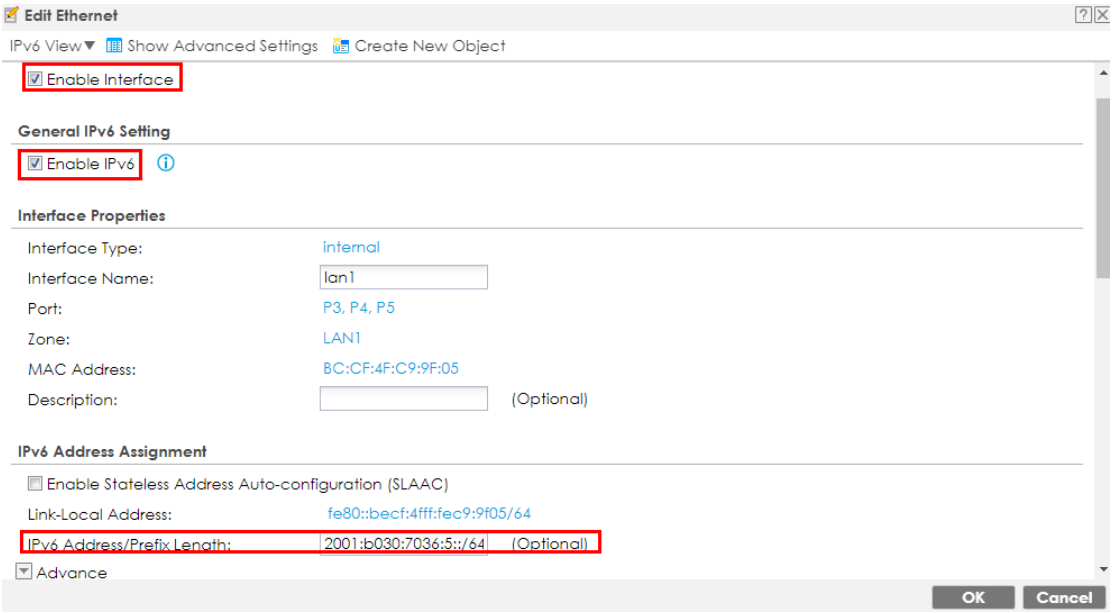
1. Create IPv6 DHCP DNS Server object. (Configuration > Object > DHCPv6 > Lease > Add)



In the Configuration > Ethernet > IPv6 Configuration section, double-click the LAN interface you want to modify.

2. Enable Interface and Enable IPv6.

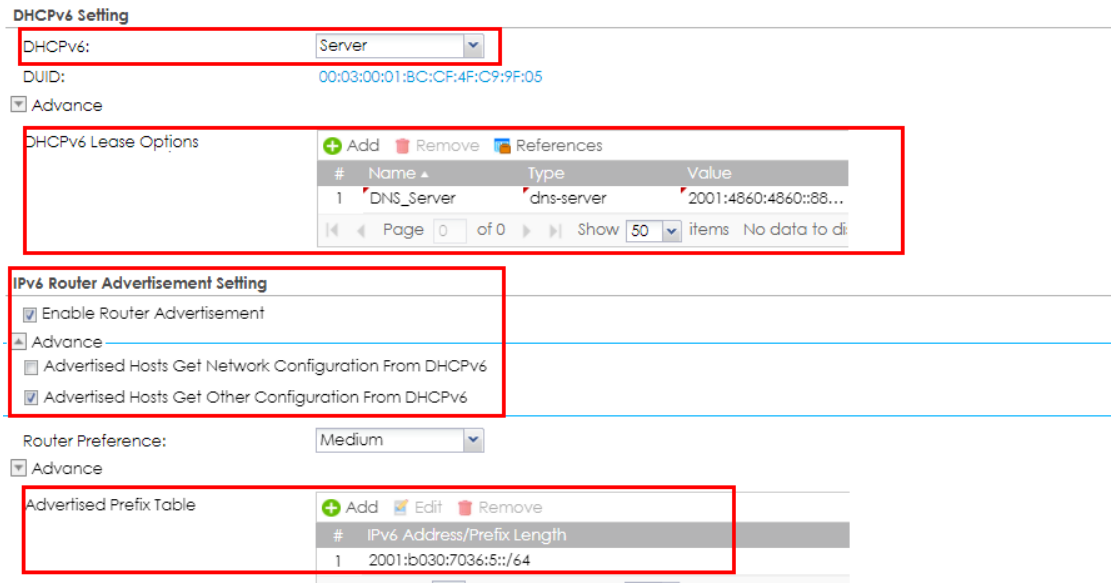
Key in IPv6 Address/Prefix Length.



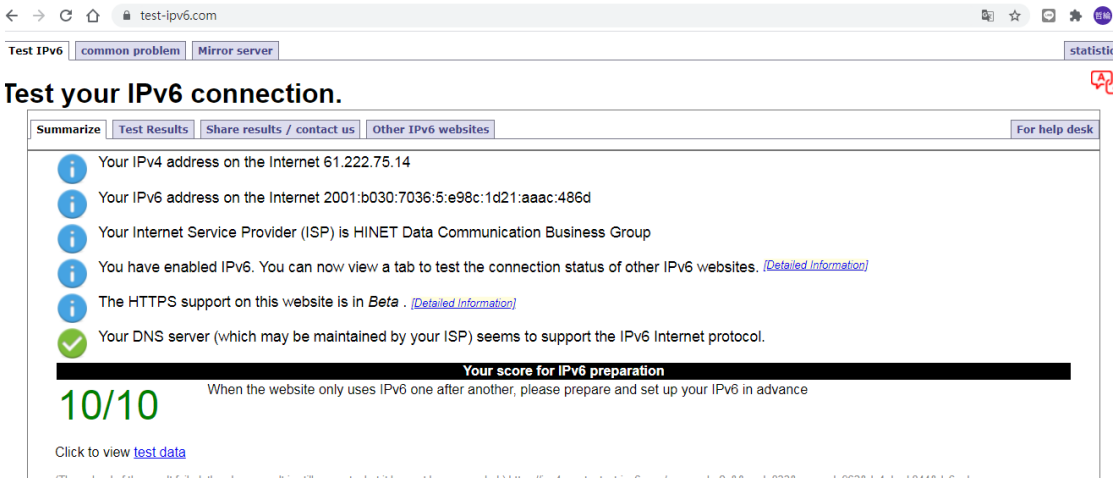
3. Assign IPv6 DNS Server into DHCPv6 Lease Options.

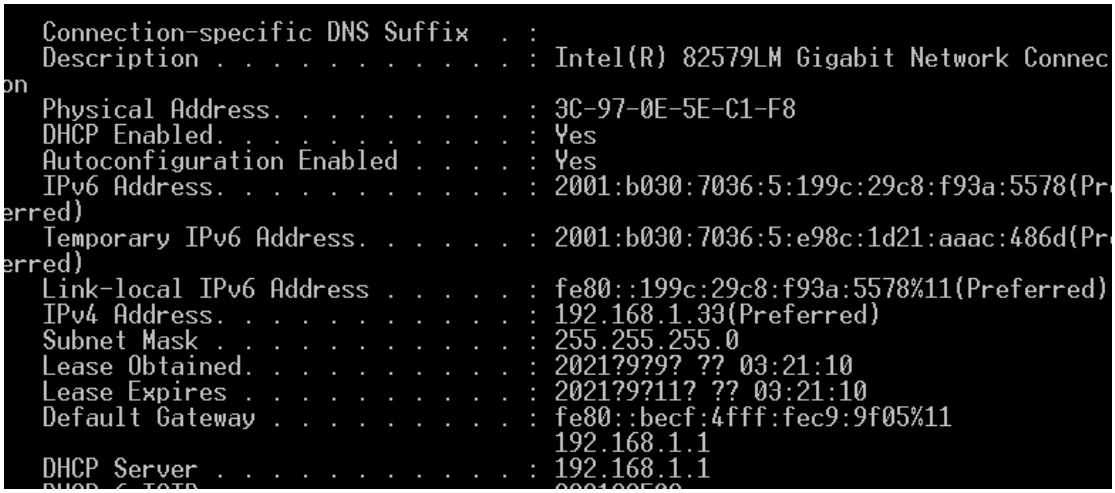
Enable Router Advertisement and enable Advertised Host Get Other Configuration From DHCPv6 checkboxes.

Key in Advertised Prefix Table.



Test the Result

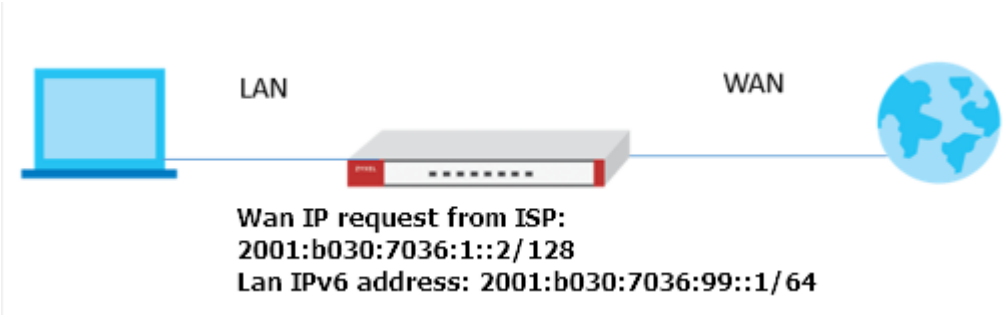




How to Set Up DHCPv6 with prefix delegation on the WAN and DHCPv6 on the LAN

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**

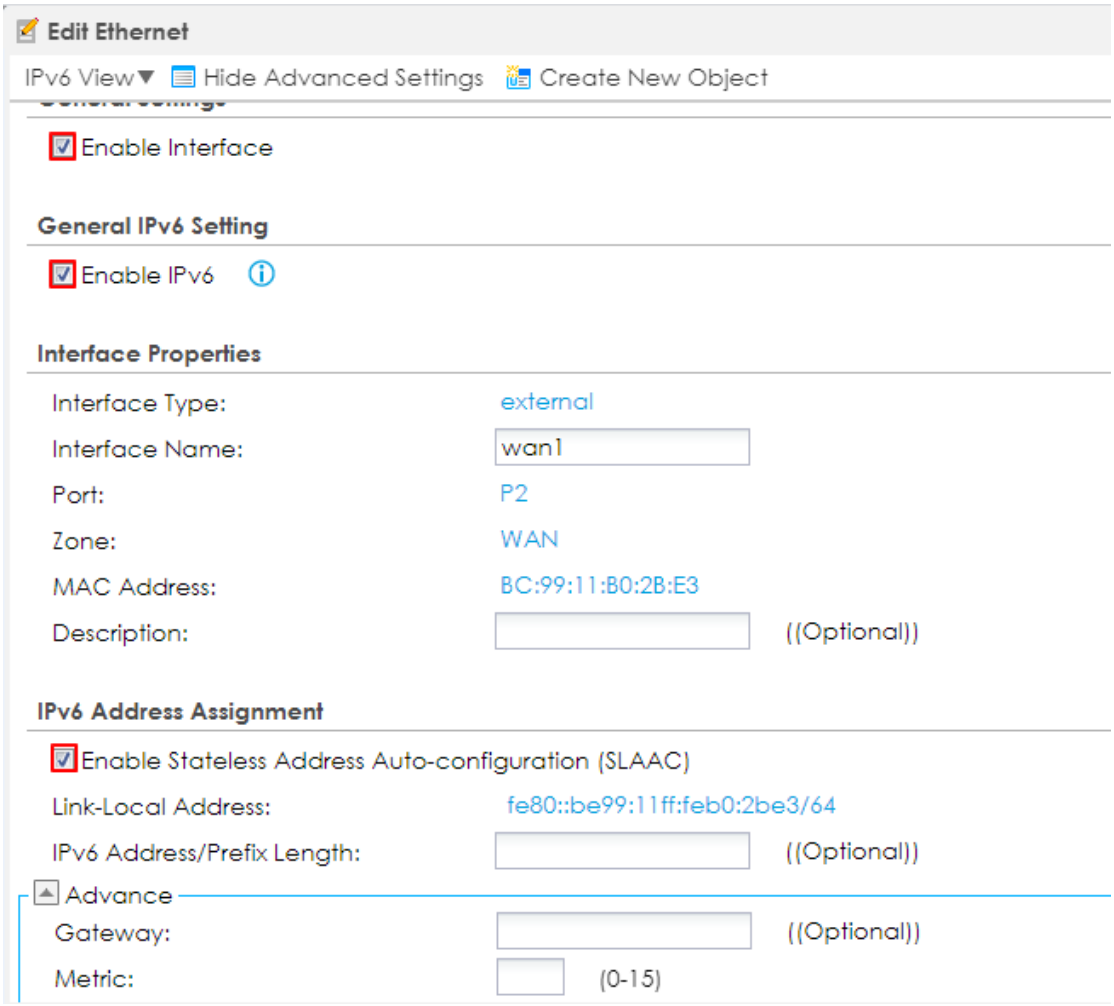


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP/USG Flex (Firmware Version: 5.00)

Configure on the Wan IPv6 interface

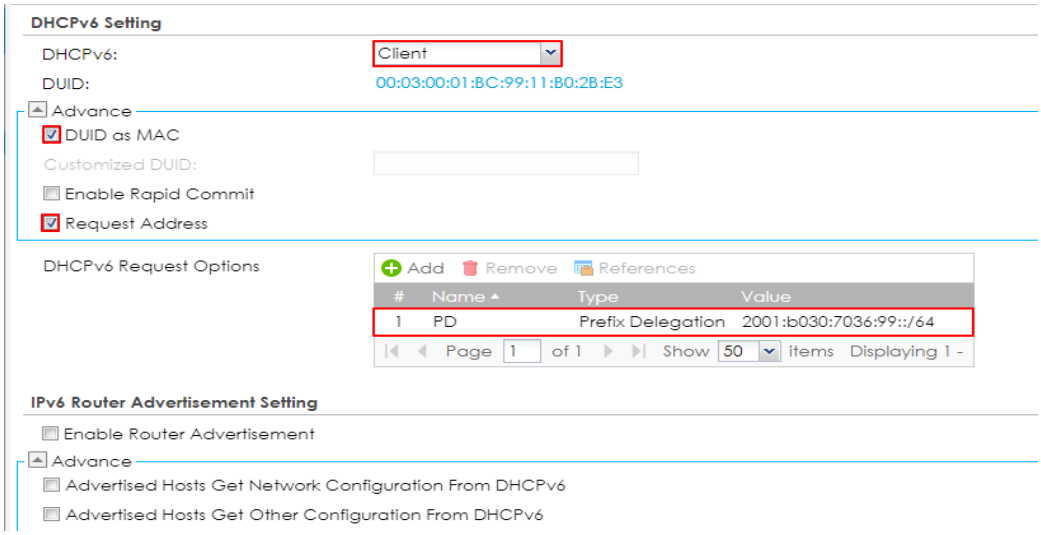
In the Configuration > Ethernet > IPv6 Configuration section, double-click the WAN interface you want to modify.

Choose IPv6 View, Enable Interface and Enable IPv6. In IPv6Address Assignment text box, enable Stateless Address Auto-configuration (SLAAC)



On DHCPv6, select **Client**, then Enable **DUID as MAC**, and tick **Request Address**

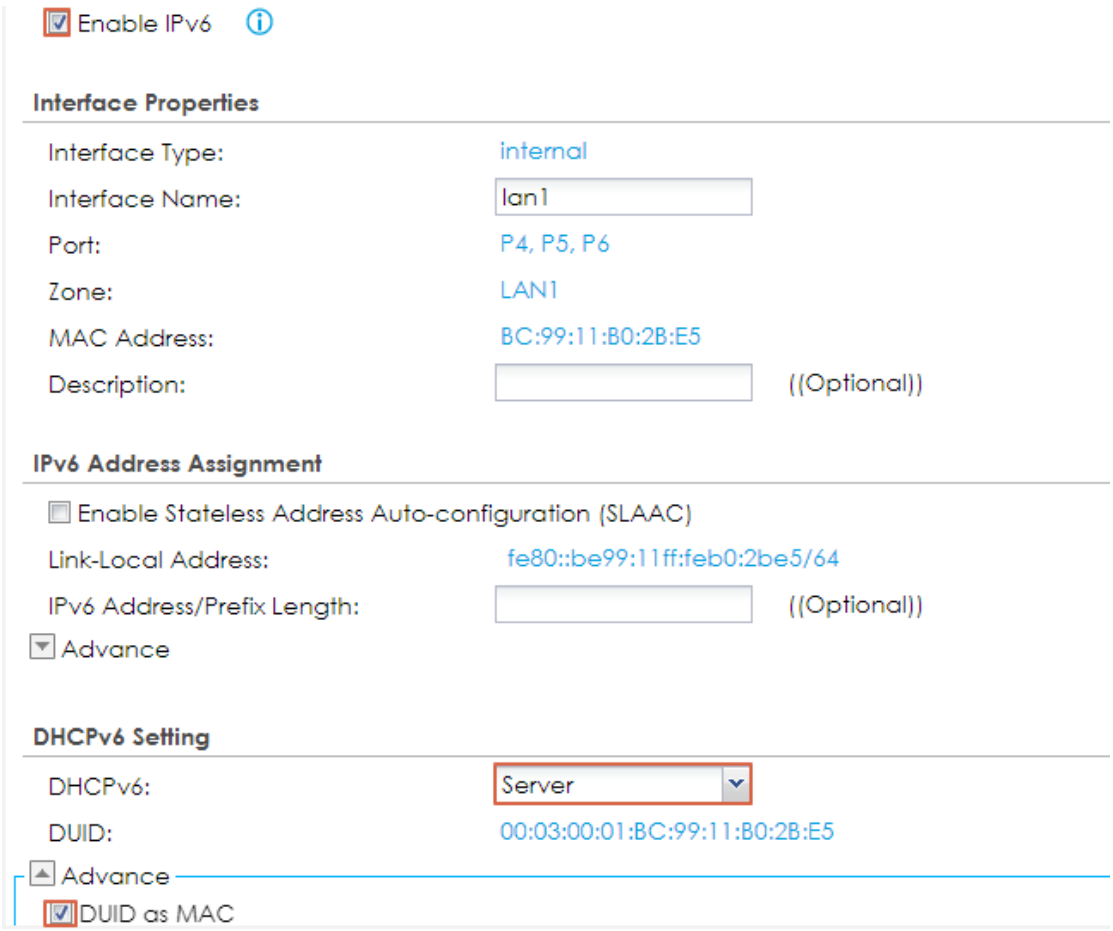
Next, create PD on DHCPv6 Request Options, and PD's Value: **2001:b030:7036:99::/64**



Configure on the Lan IPv6 interface

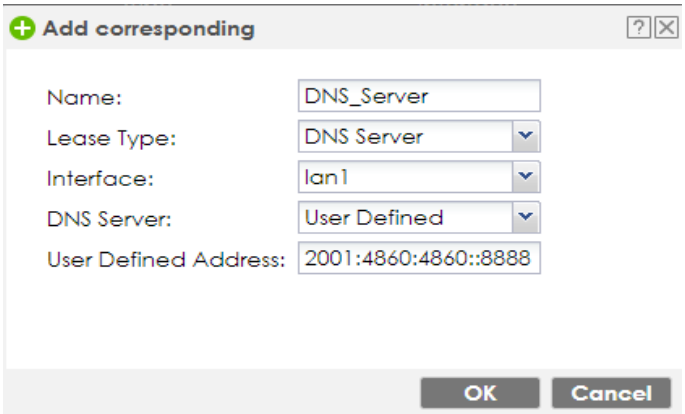
Tick **Enable IPv6**, then fill IPv6 address which provide from ISP:

Select **Server** as DHCPv6. Enable **DUID as MAC**.



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

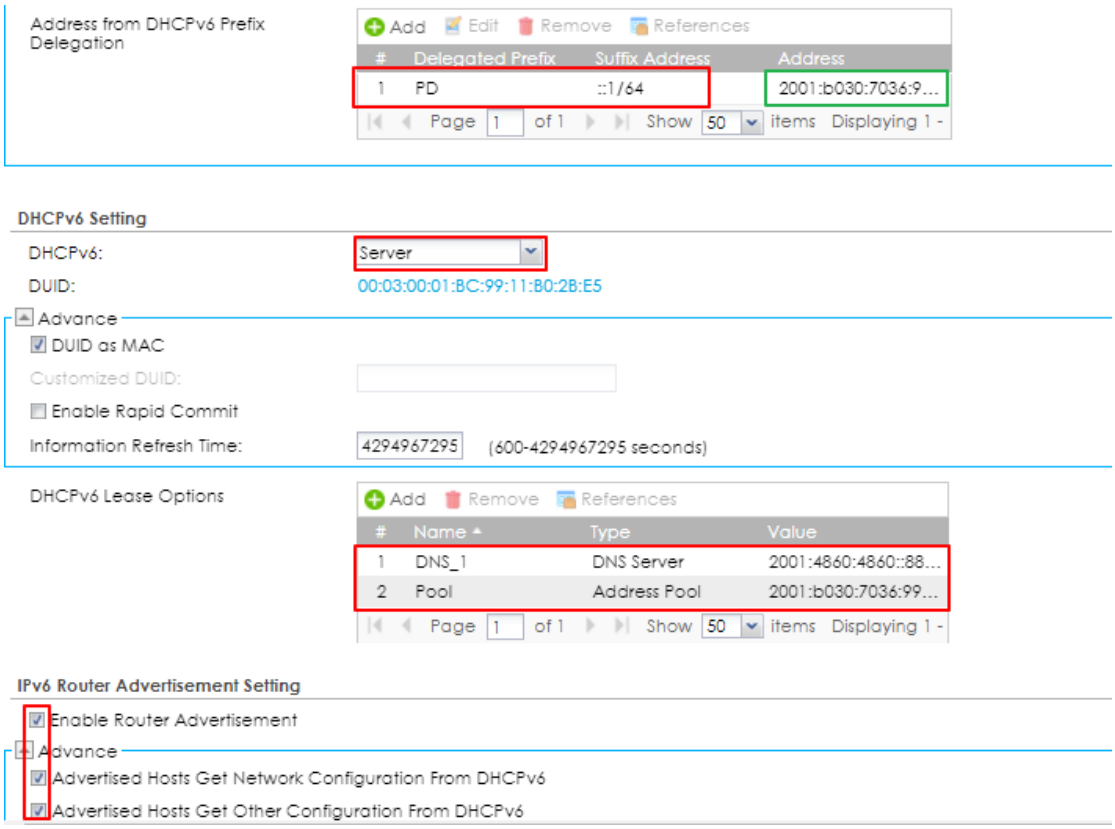


On Address from DHCPv6 Prefix Delegation, fill **::1/64 as PD.**

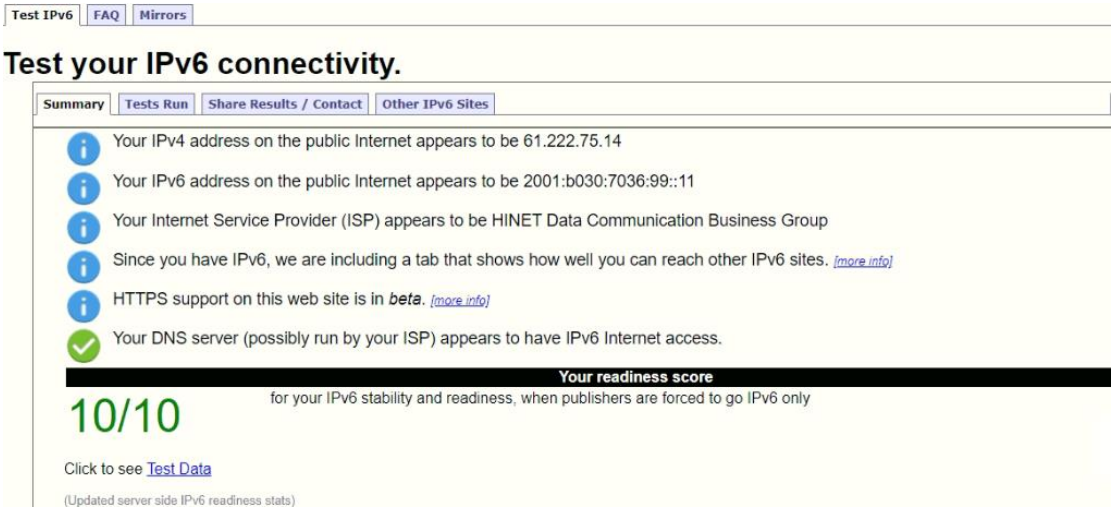
Enable **Router Advertisement** then enable **Advertised Hosts Get Network**

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.



Test the Result




```
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

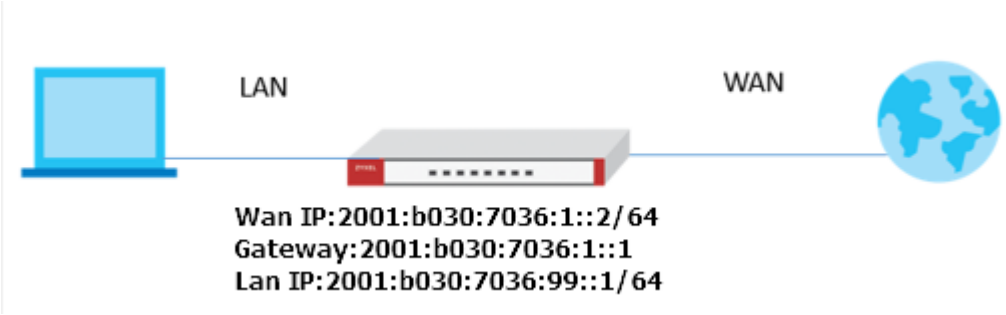
This example shows how to configure your ATP/USG Flex's WAN as Autoconf on the WAN and DHCPv6 on the LAN

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

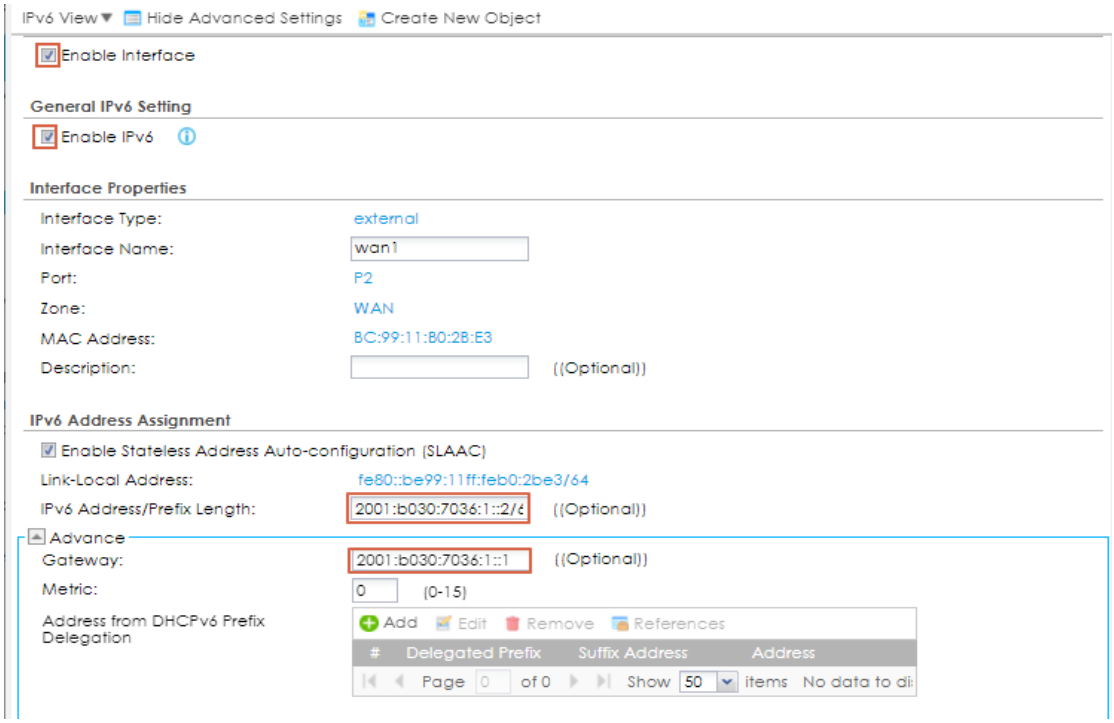


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP/USG Flex (Firmware Version: 5.00)

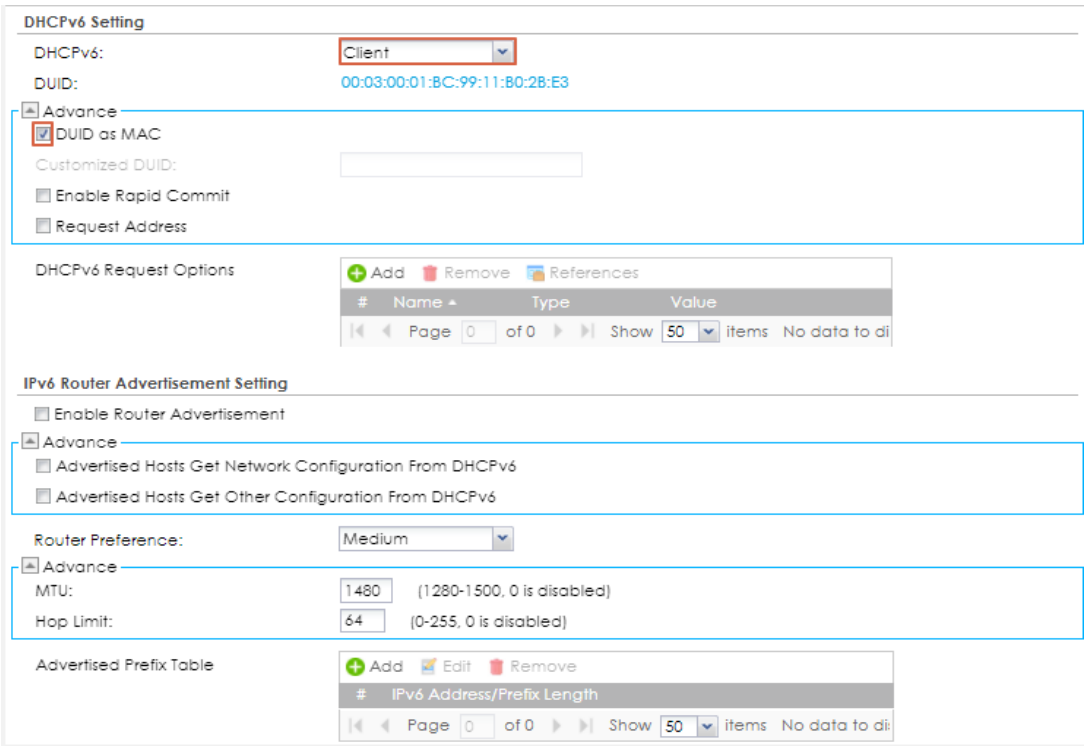
Configure on the Wan IPv6 interface

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



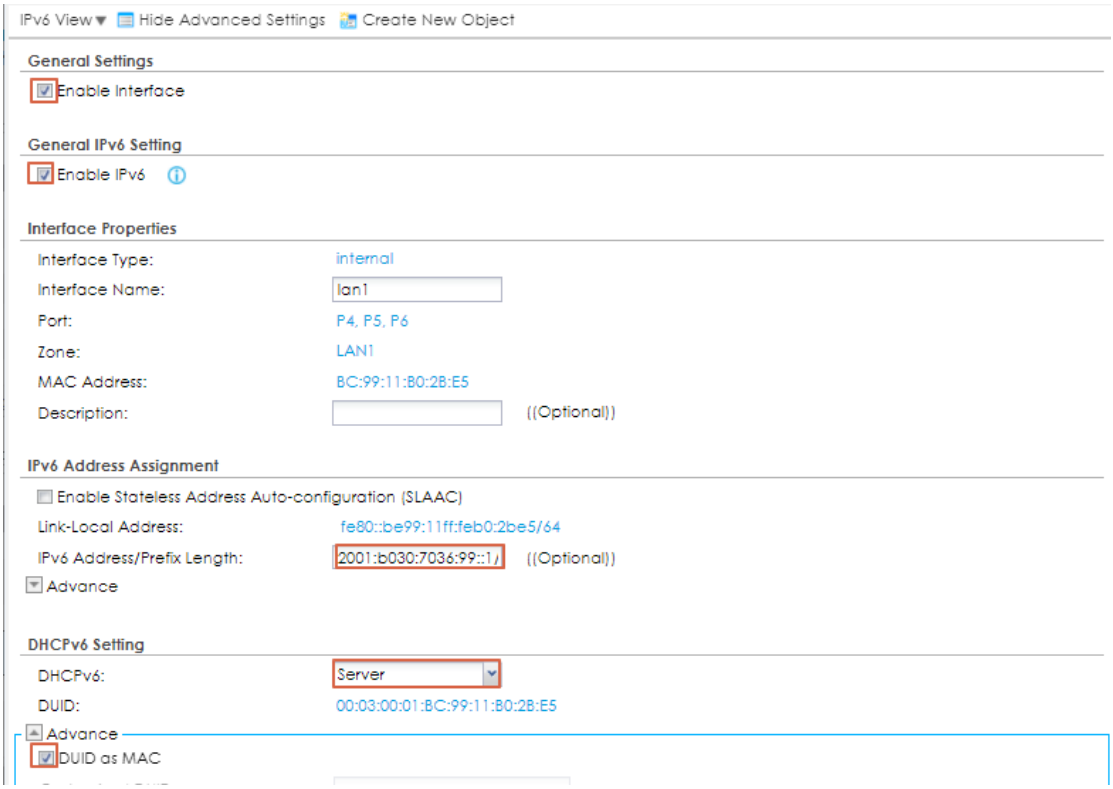
On DHCPv6, select **Client**, then Enable **DUID as MAC**



Configure on the Lan IPv6 interface

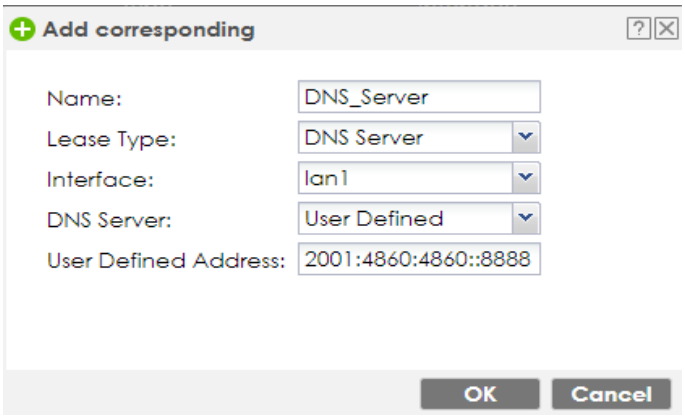
Tick **Enable IPv6**, then fill IPv6 address: **2001:b030:7036:99::1/64** which provide from ISP.

Select **Server** as DHCPv6. Enable **DUID as MAC**.

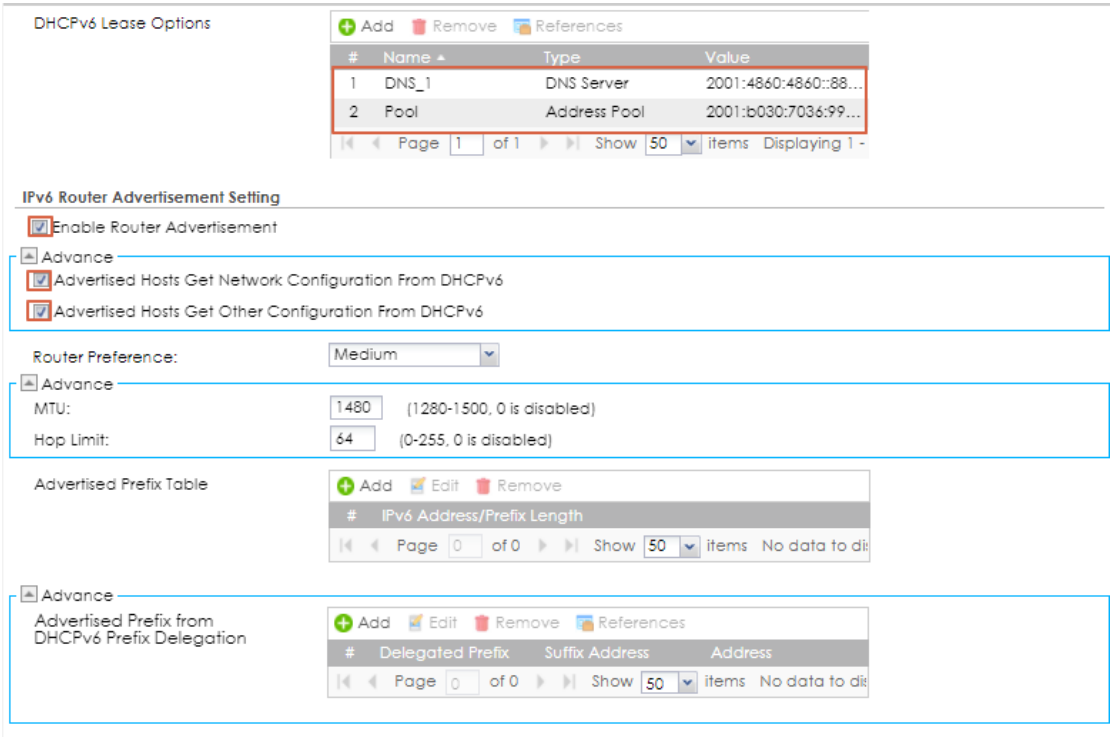


Next, On the DHCPv6 Lease Options, add **2001:4860:4860::8888** as DNS server

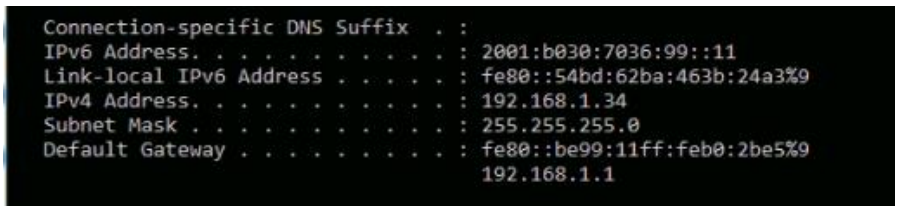
Add the **2001:b030:7036:99::10-2001:b030:7036:99::100** as Address Pool



Next, Enable **Router Advertisement**, **Advertised Hosts Get Network Configuration From DHCPv6** and **Advertised Hosts Get Other Configuration From DHCPv6**



Test the Result



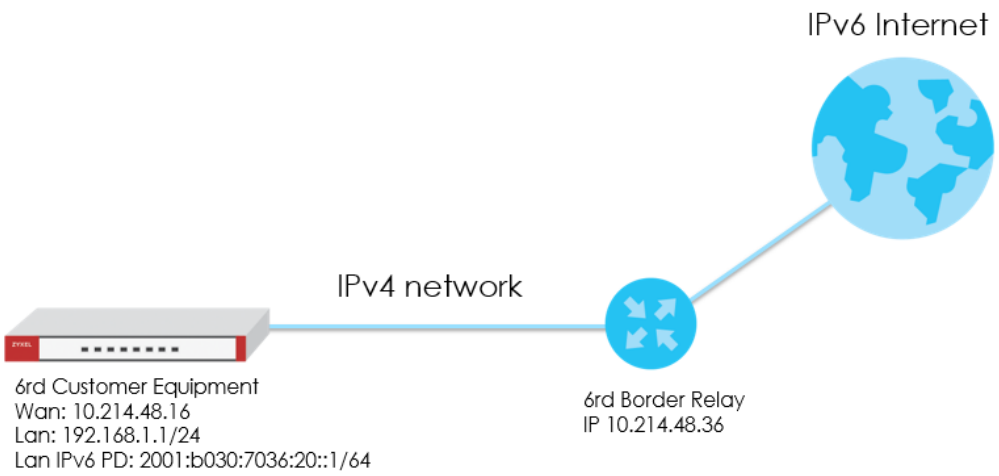
How to Set Up 6rd on the WAN and autoconf on the LAN

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.

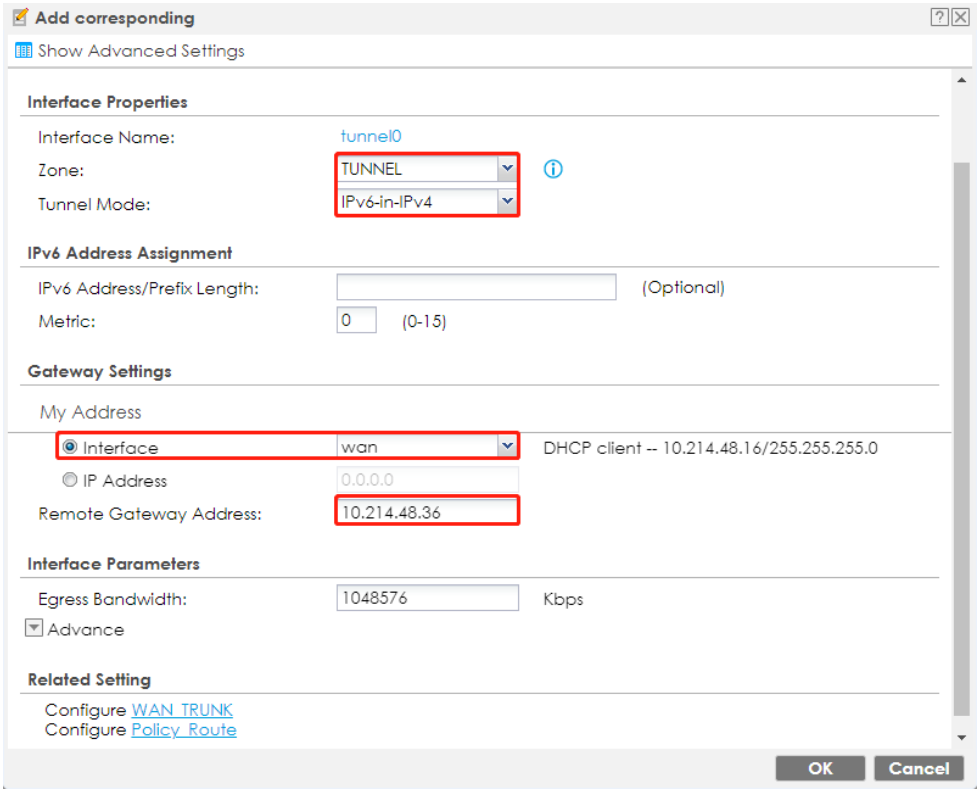
   Interface name: Tunnel0

   Zone: Tunnel

   Tunnel mode: IPv6-in-IPv4

   My address: Wan interface

   Remote Gateway address : 10.214.48.36 （Border Relay）



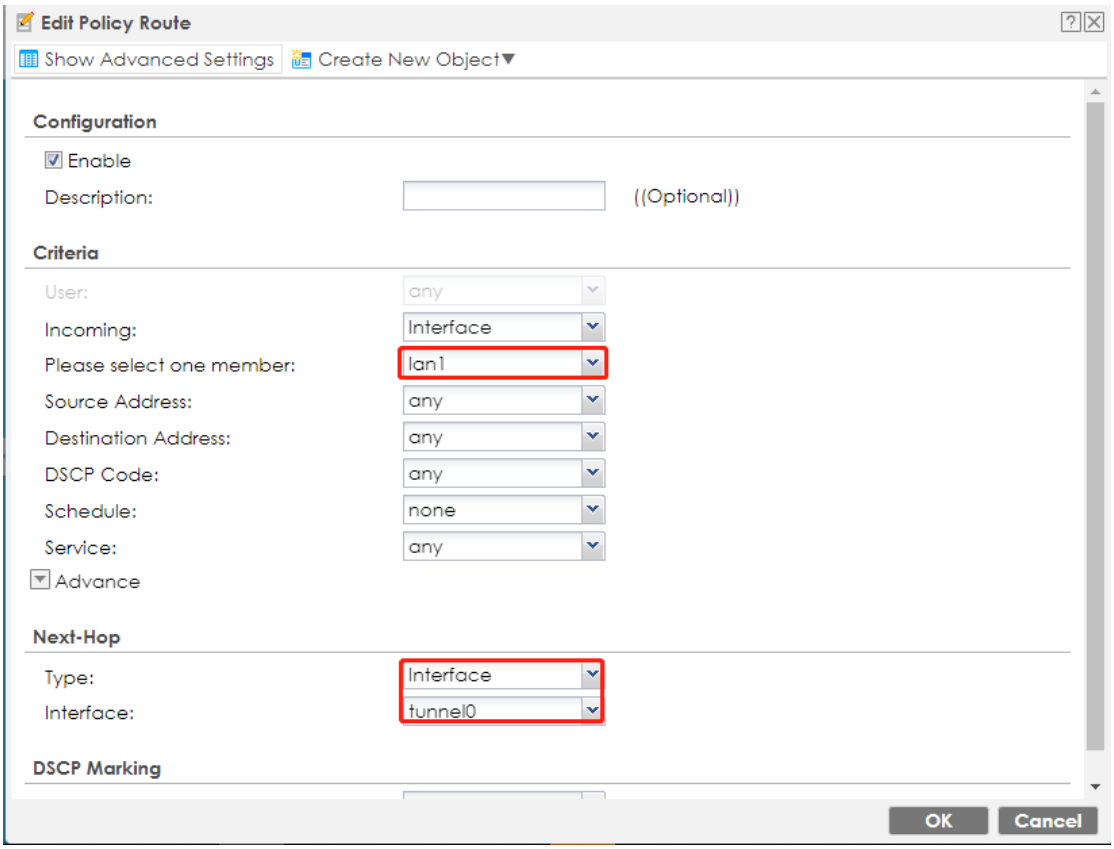
Policy route

Go to Configuration > Network > Routing > Policy route. click Add to create a policy route for V6 routing.

Incoming interface: lan1

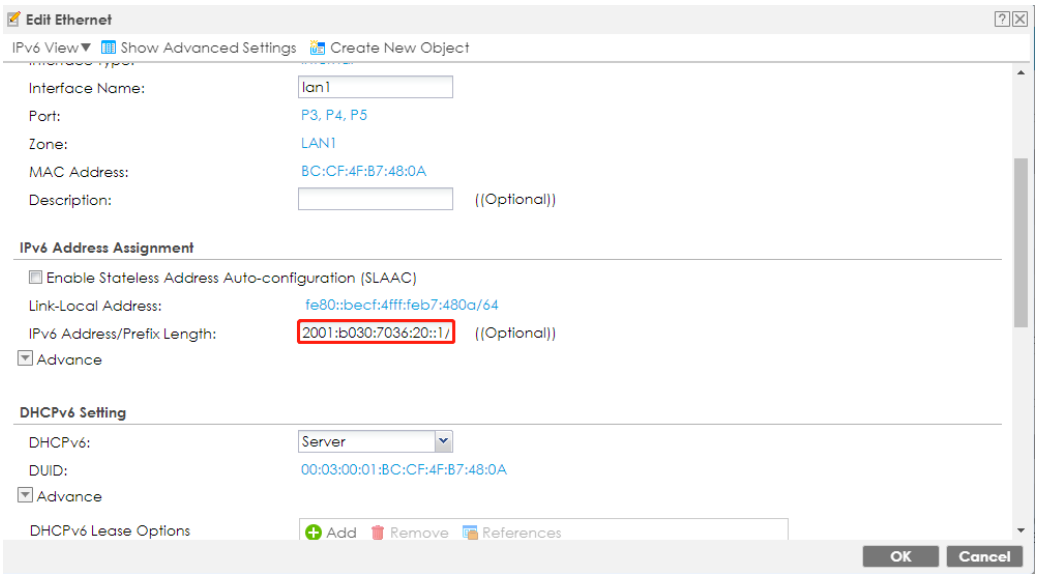
Destination Address: any

Next hop: Tunnel0

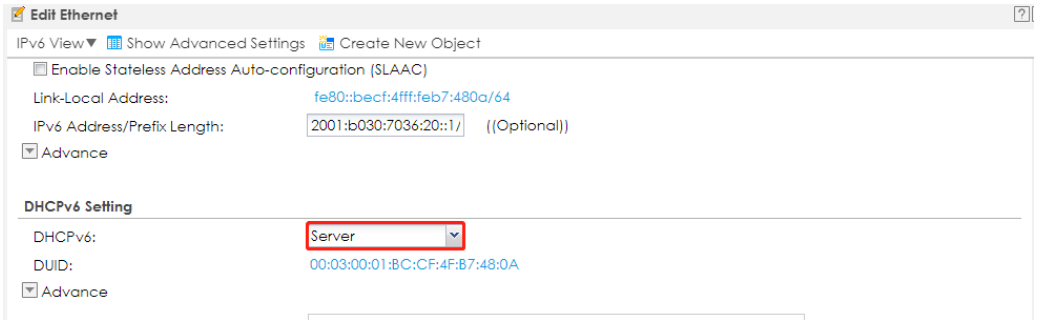


Lan

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

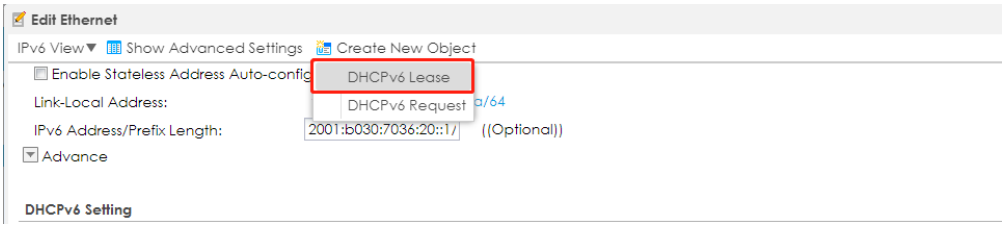


3. Enable IPv6 DHCP server.

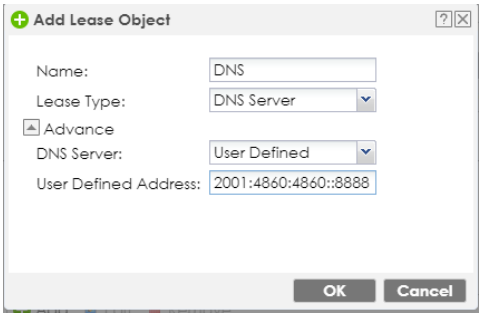


4. Add DHCP release object for LAN DNS setting.

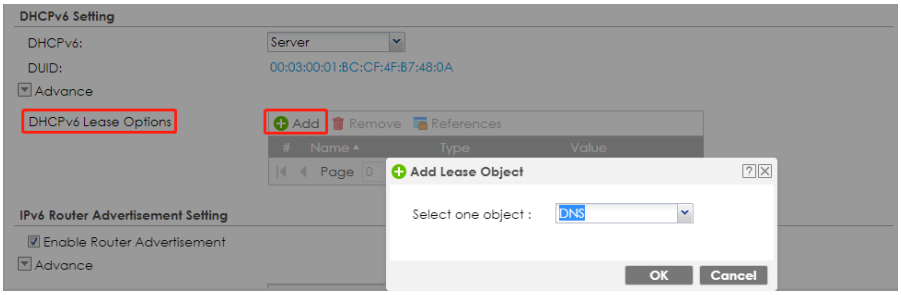
   Create New Object > DHCPv6 Lease



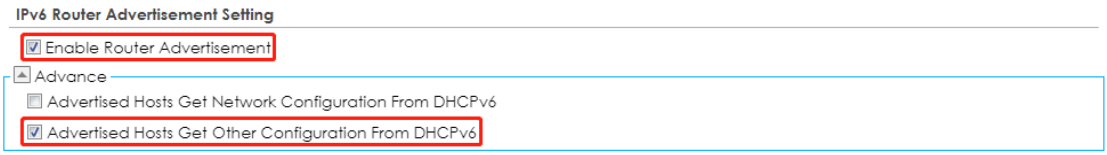
   In this scenario, we use Google V6 DNS server for LAN client. Click OK to save.



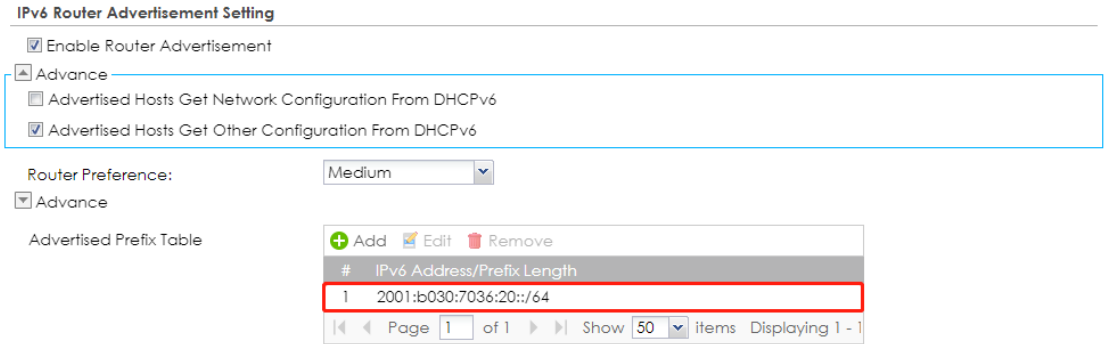
Add this Lease object in DHCPv6 Lease options.



5. Tick “Enable Router Advertisement”, and "Advertised Hosts Get Other Configuration From DHCPv6".

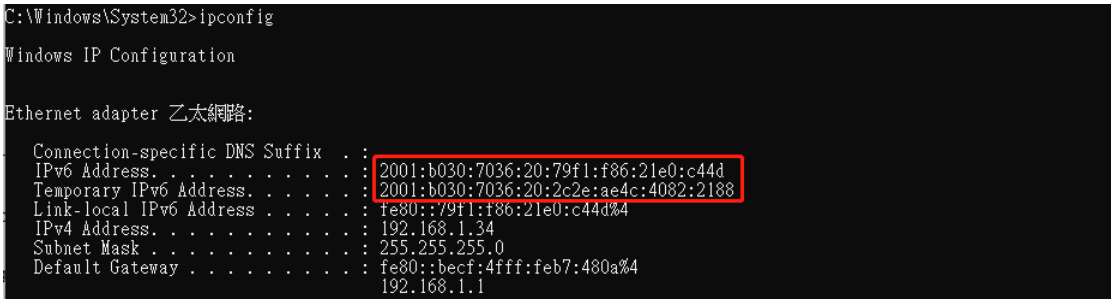


6. Set up Advertised Prefix from DHCPv6 Prefix Delegation. In this scenario, we set 2001:b030:7036:20::/64 for LAN prefix.

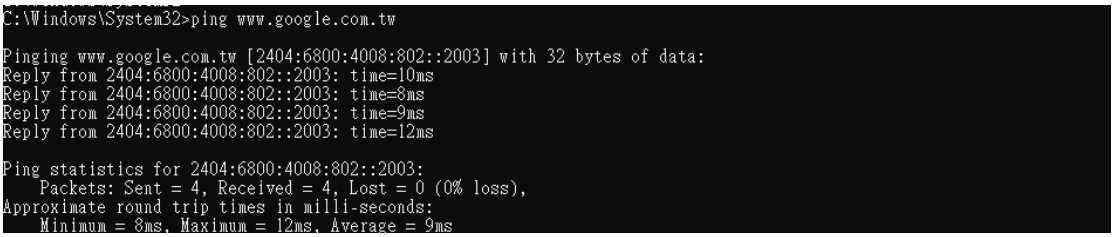


Test the Result

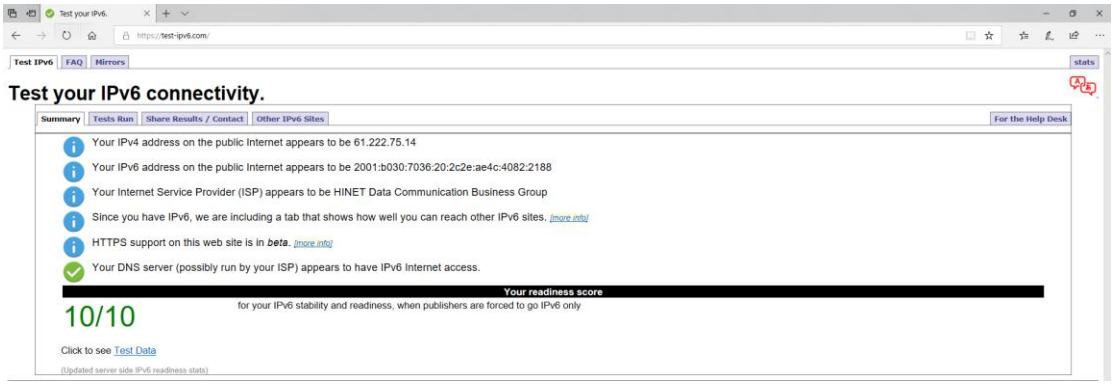
Client IPv6 address.



Ping to Google web site.



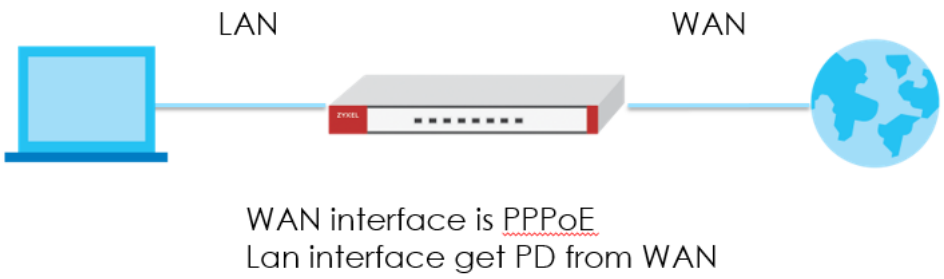
Test Your IPv6 connection.



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.



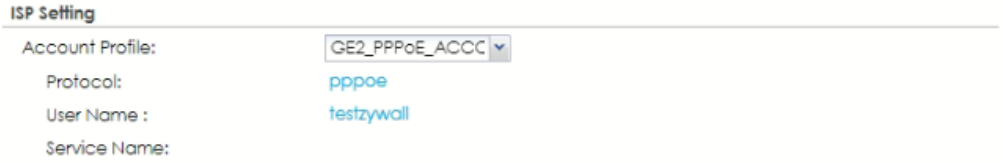
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP/USG Flex (Firmware Version: 5.00)

Setting Up the IPv6 Interfaces

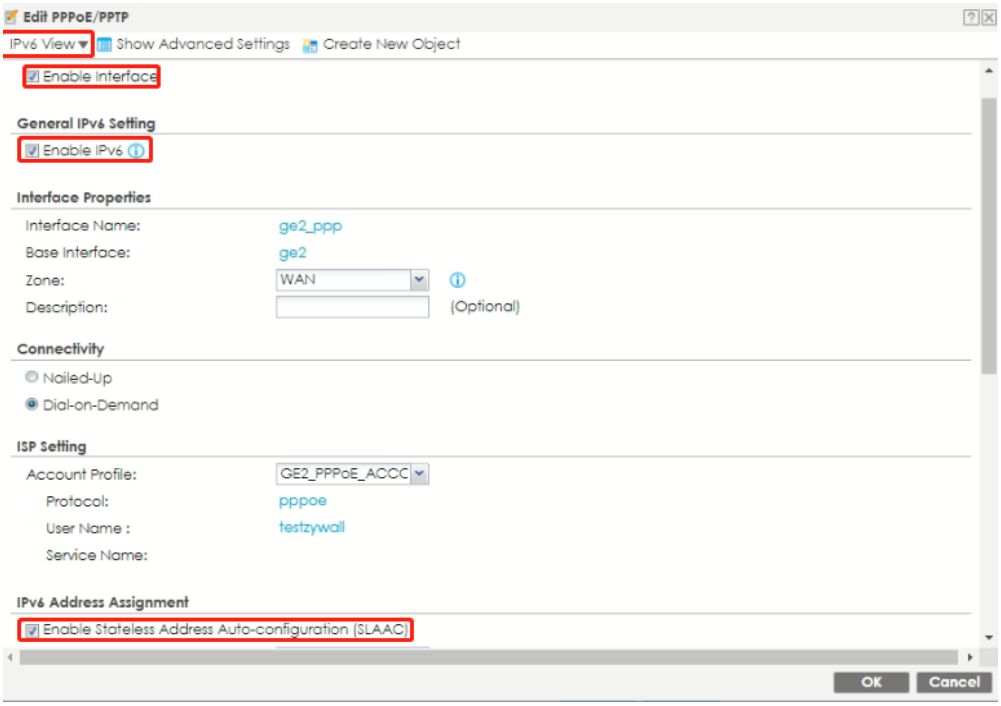
Wan

1. In the Configuration > Network > Interface > PPP Configuration section, double-click the PPP interface you want to modify.

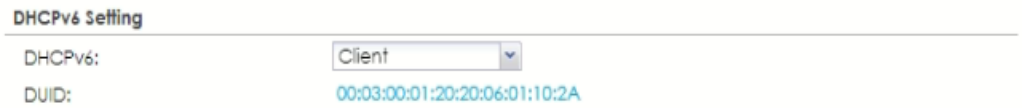
2. Select account profile in ISP Setting.



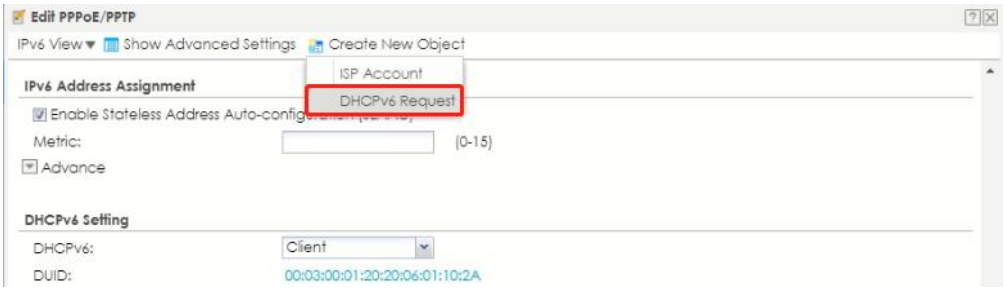
3. Choose IPv6 View, Enable Interface and Enable IPv6. In IPv6Address Assignment text box, enable Stateless Address Auto-configuration (SLAAC)



4. Set up interface as V6 client.

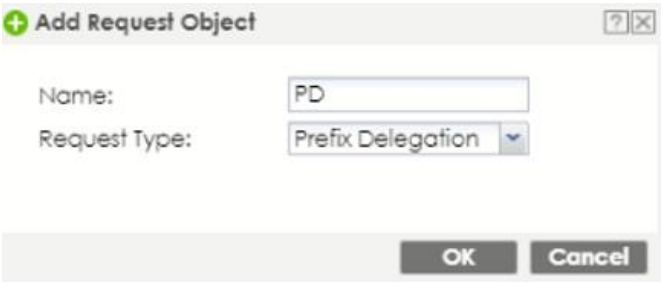


5. Create DHCPv6 Request object to get Prefix Delegation and DNS from ISP.

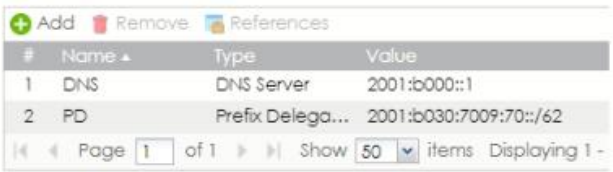


DNS object

Prefix delegation

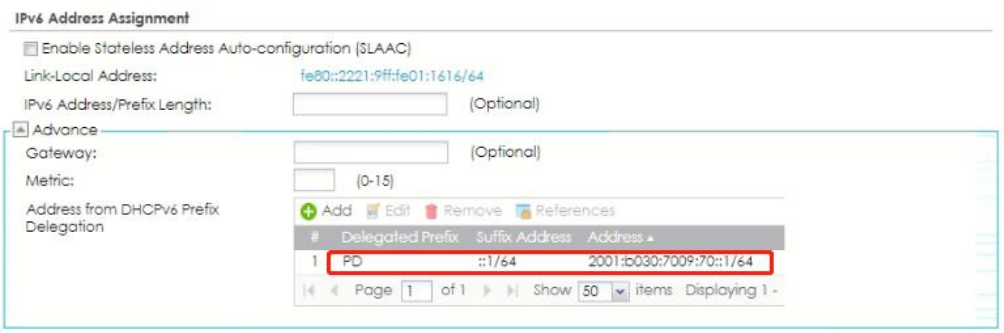


6. Tick Request Address.



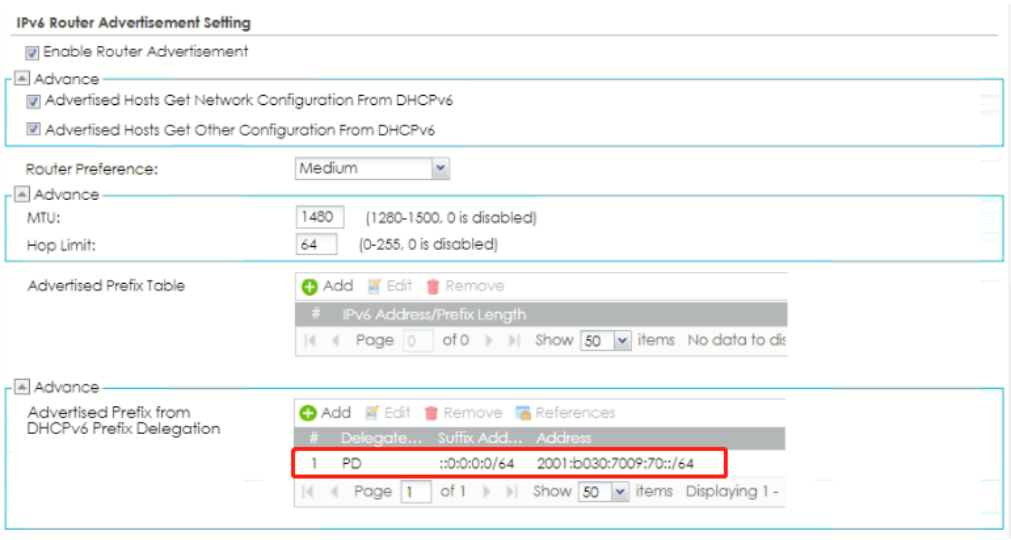
Lan

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



3. Tick “Enable Router Advertisement”, "Advertised Hosts Get Network Configuration From DHCPv6", and "Advertised Hosts Get Other Configuration From DHCPv6".

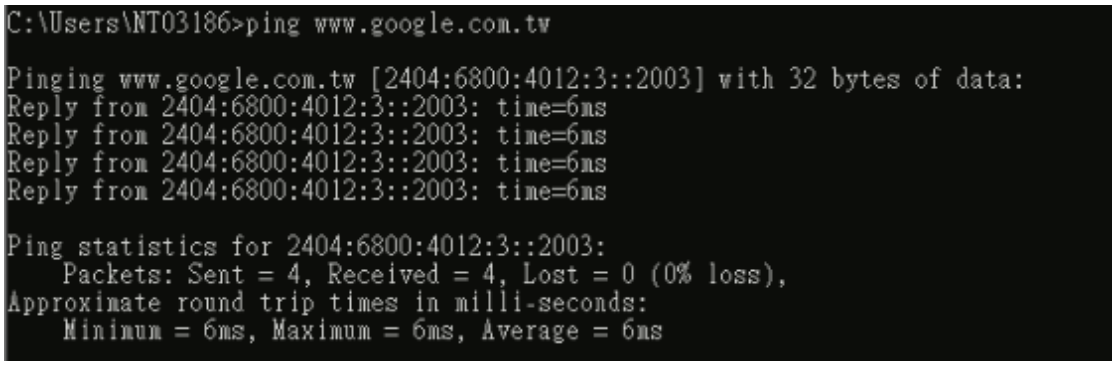
4. Set up Advertised Prefix from DHCPv6 Prefix Delegation.



Test Result

Client IPv6 address.

Ping to Google web site.



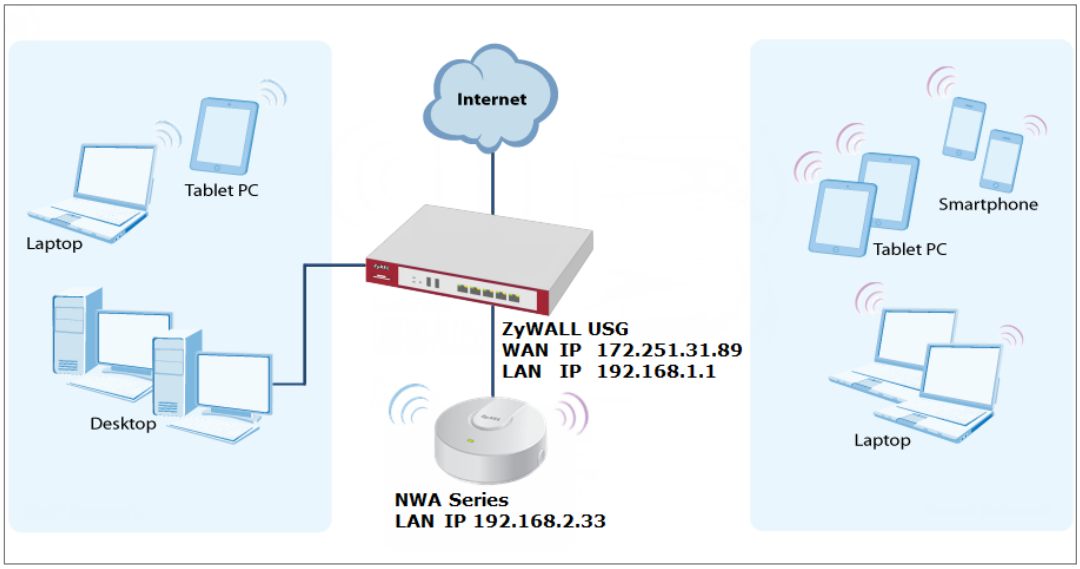
Test Your IPv6 connection.

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



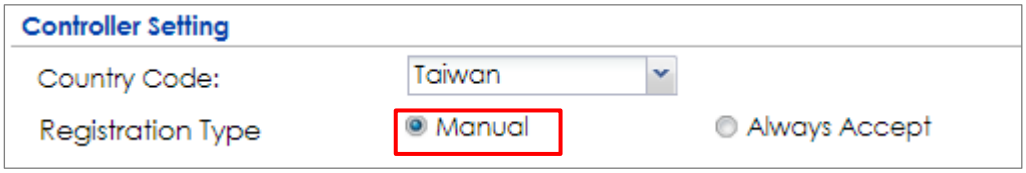
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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.

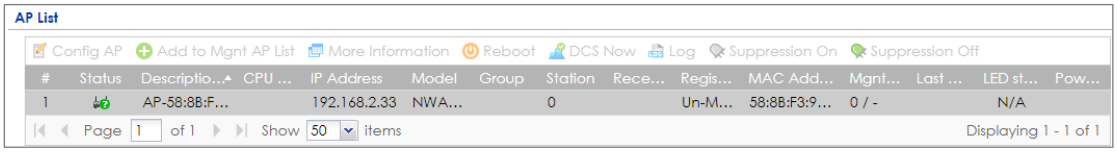
CONFIGURATION > Wireless > Controller > Configuration



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.

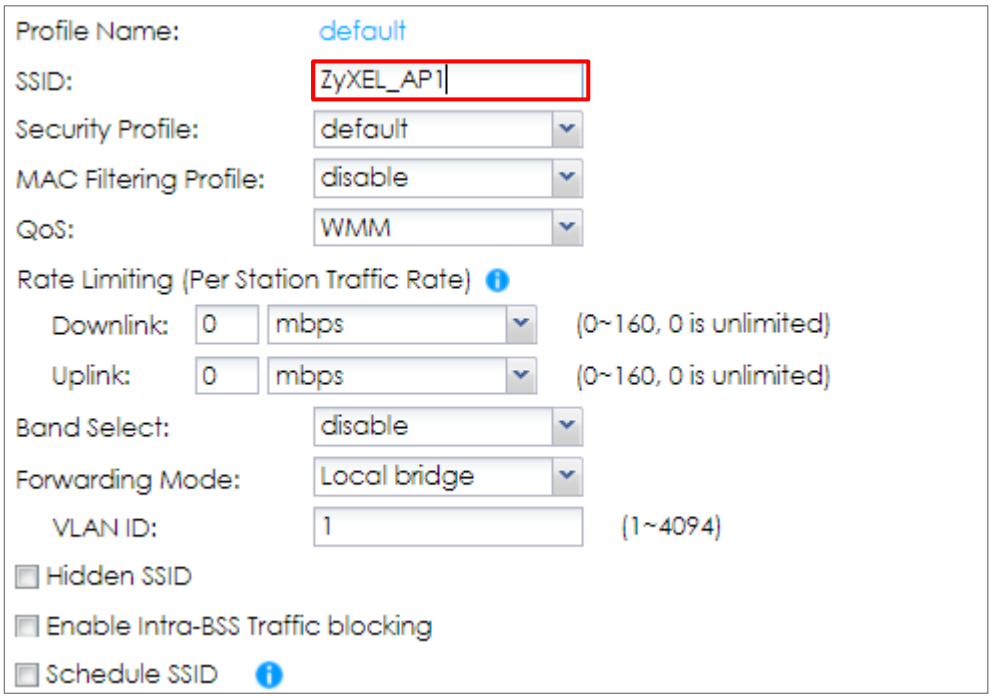
Monitor > Wireless > AP Information > AP List



Note: The APs may take few minutes to appear in the AP List.

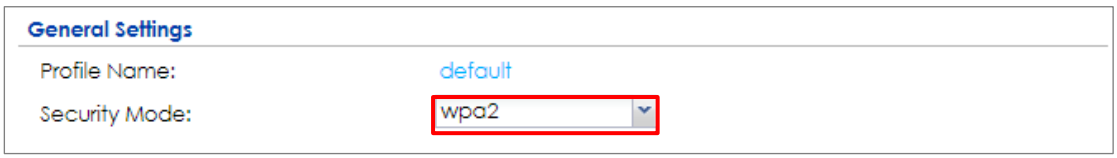
Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List** to configure a name to identify the **SSID**.

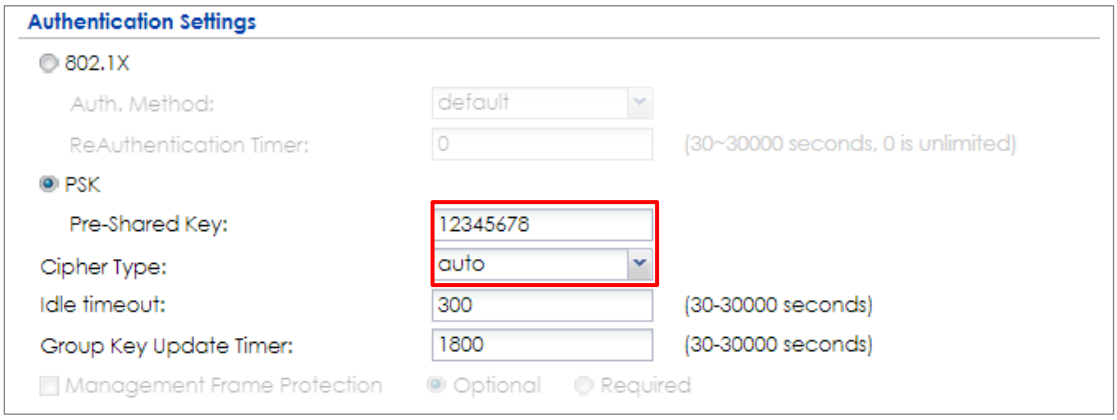
CONFIGURATION > Object > AP Profile > SSID > SSID List



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

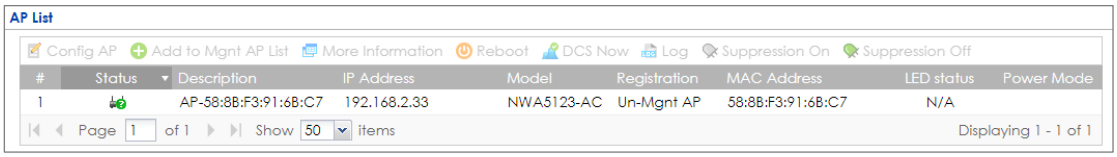




Test the Result

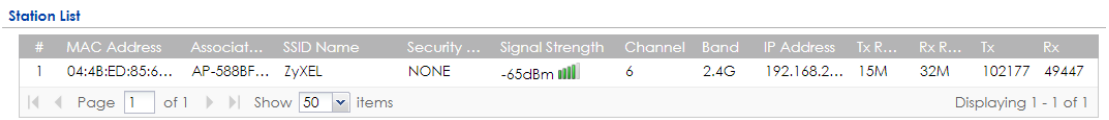
Go to the ZyWALL/USG **Monitor > Wireless > AP Information > AP List**, you can check the list of APs which are currently connected to it and the details information such as **Registration** type, **Model** and **Recent On-line Time /Last Off-line Time**.

MONITOR > Wireless > AP Information > AP List



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



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.

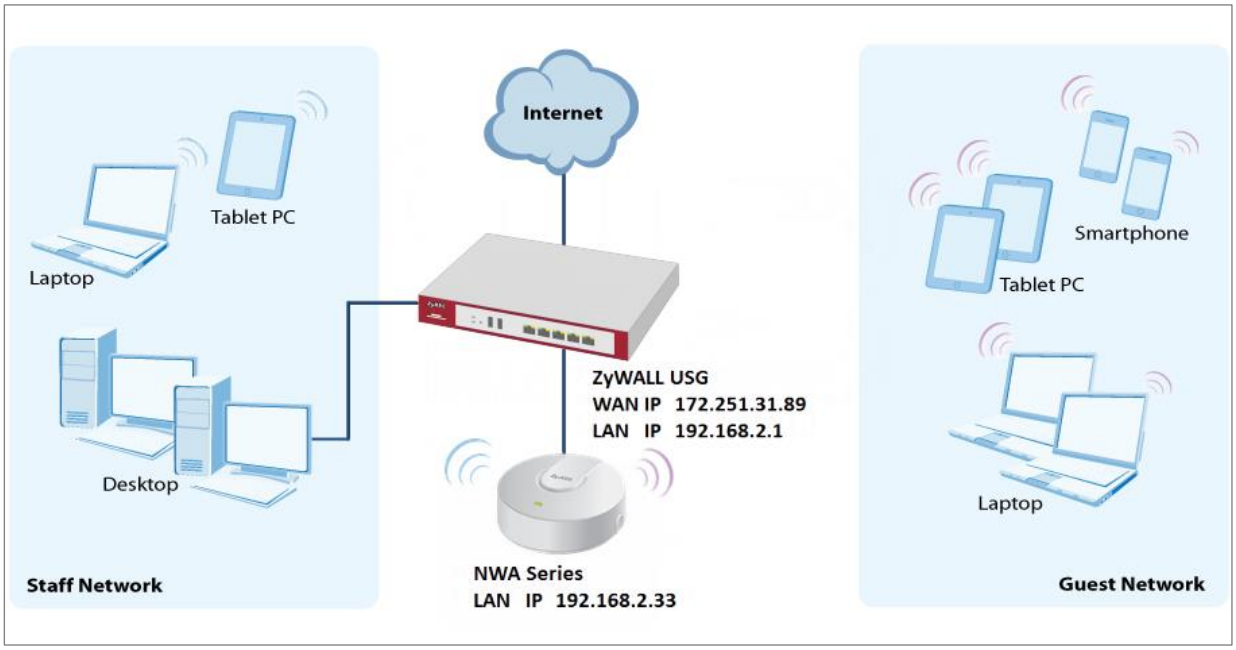
MONITOR > Log

#	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



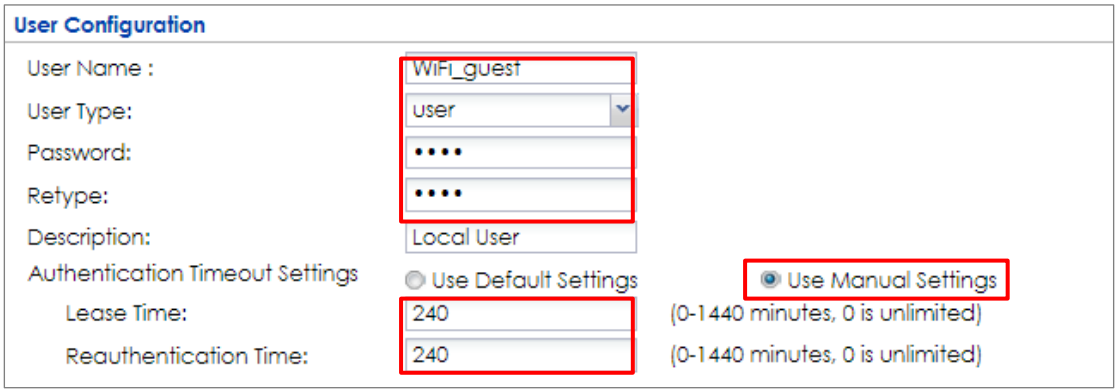
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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.

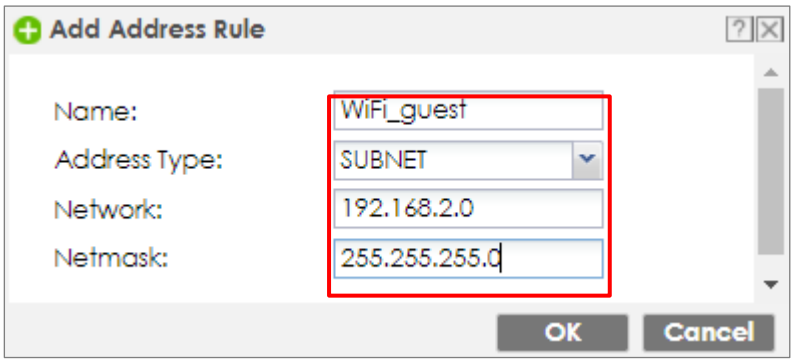
Set the **Authentication Timeout Settings** to be **Use Manual Settings** to enter the number of minutes this user has to renew the current session before the user is logged out.

CONFIGURATION > Object > User/Group > User > Add A User



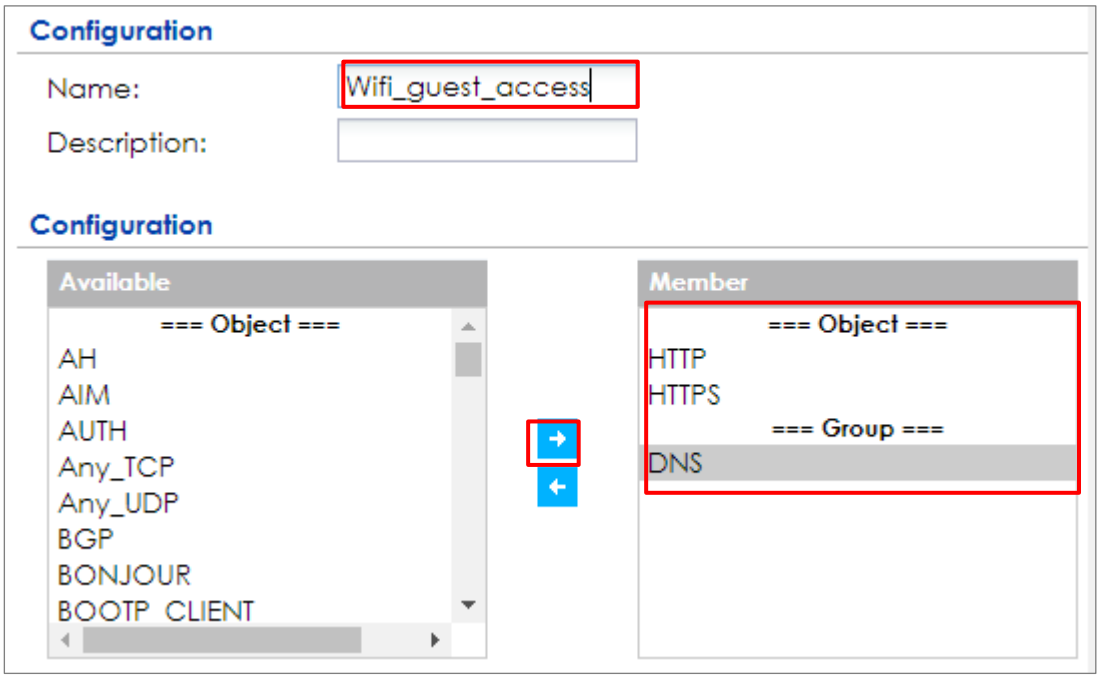
In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create the guest Wi-Fi user access subnet. In this example, AP is connected to ZyWALL/USG LAN interface 192.168.2.0/24. Configure the **Name** for you to identify the Wi-Fi guest subnet. Set the **Network** to be 192.168.2.0 and set the **Netmask** to be 255.255.255.0. Click **OK**.

CONFIGURATION > Object > Address > Add Address Rule



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**.

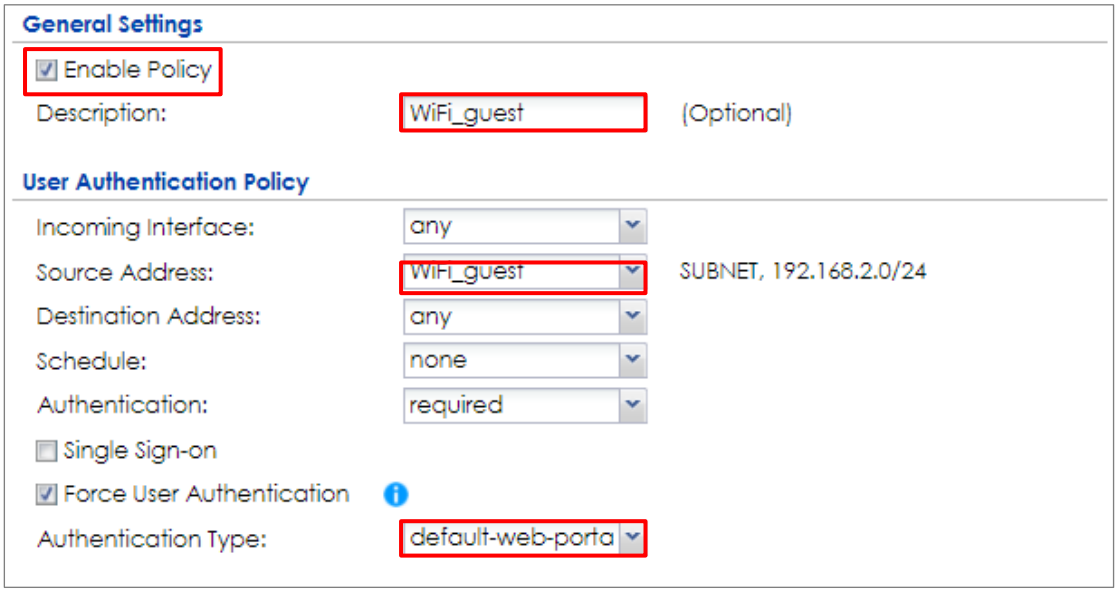
CONFIGURATION > Object > Service > Service Group > Add Service Group Rule



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



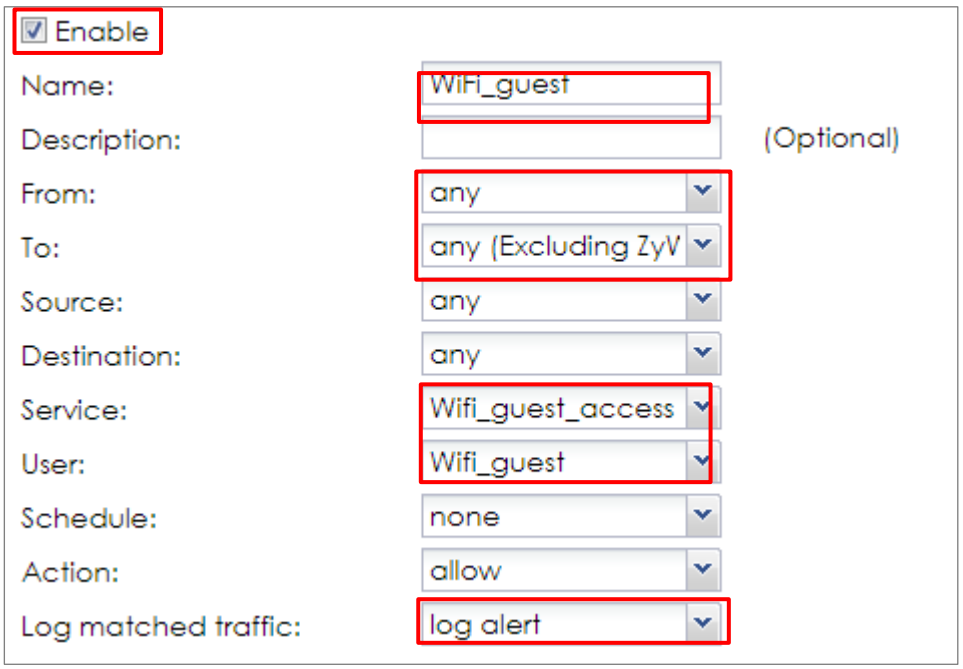
In the ZyWALL/USG, go to **CONFIGURATION > Web Authentication > General Settings** and select **Enable Web Authentication**.

CONFIGURATION > Web Authentication > General Settings

Set Up the Security Policy on the ZyWALL/USG

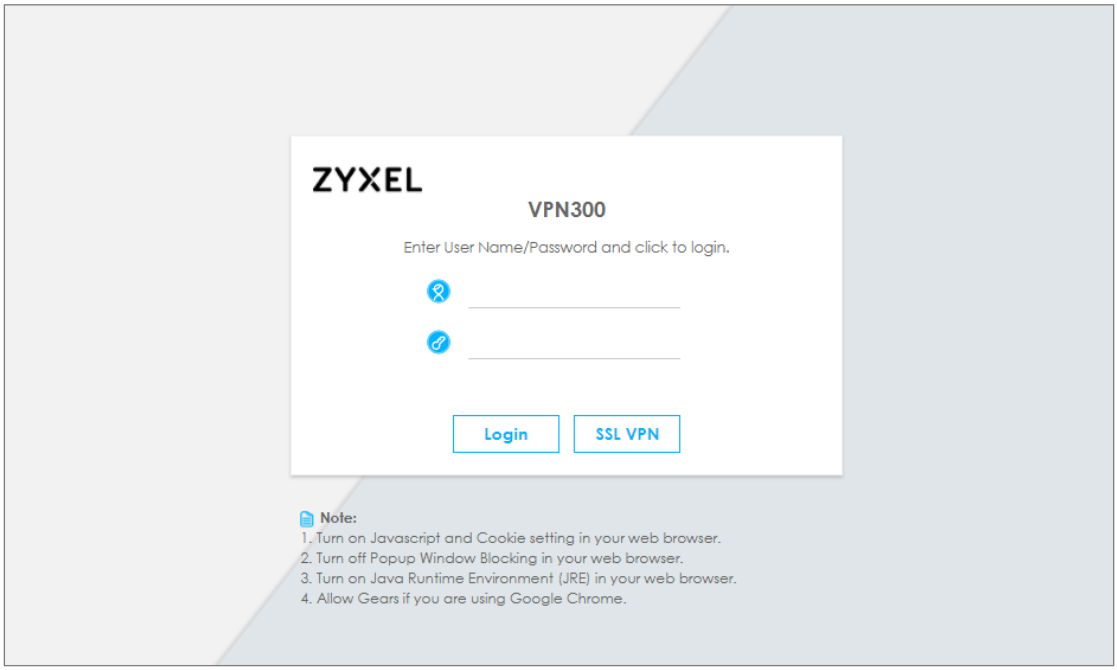
In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy > Add corresponding**. Configure a **Name** for you to identify the **Security Policy** profile. Set **From: LAN** and **To: any (Excluding ZyWALL)**. Set **Service** to be the Service Group Rule (wifi_guest_access in this example). 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

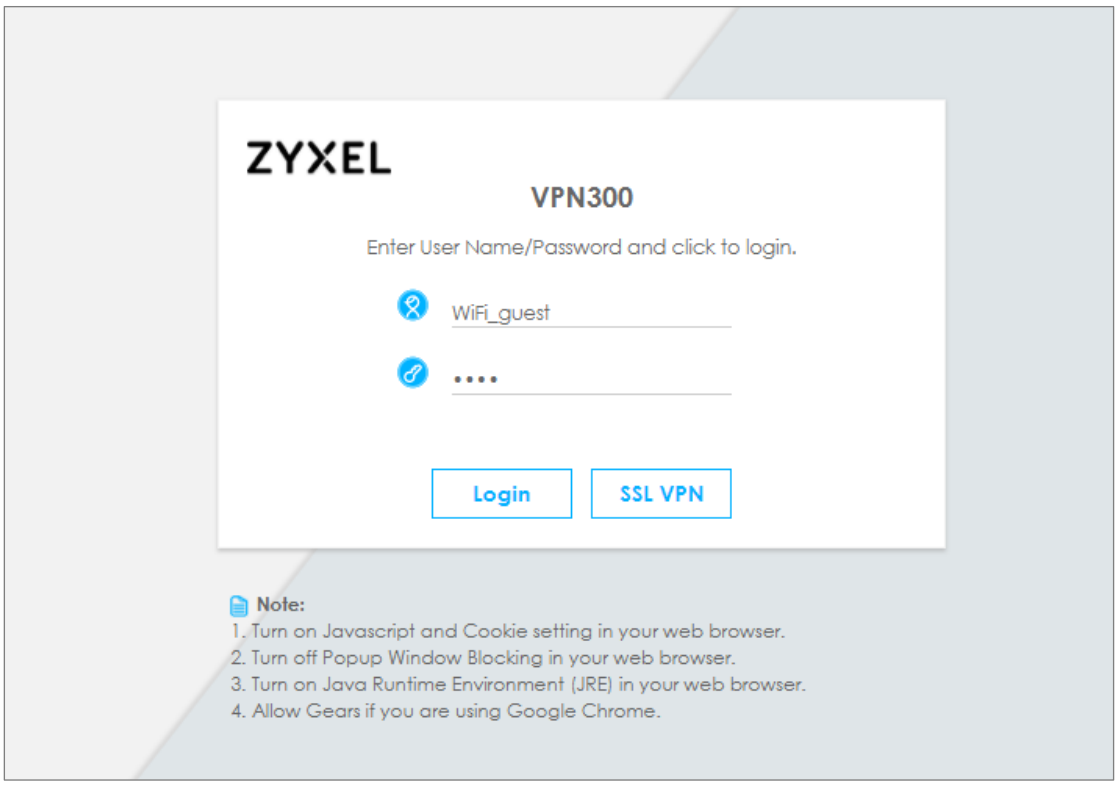


Test the Result

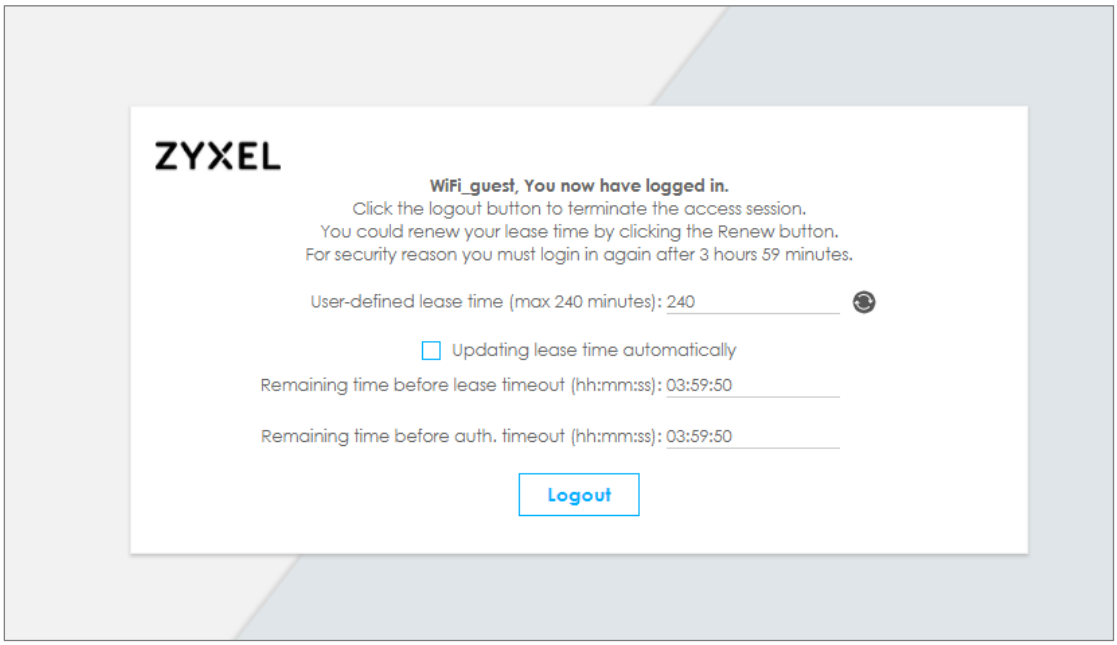
Using a mobile device to connect to the AP which is connected to the ZyWALL/USG. When you try to access the Internet, it will redirect to the user login screen.



Type the Wi-Fi guest **User Name** and **Password**, click **Login**.



The access session page will appear.



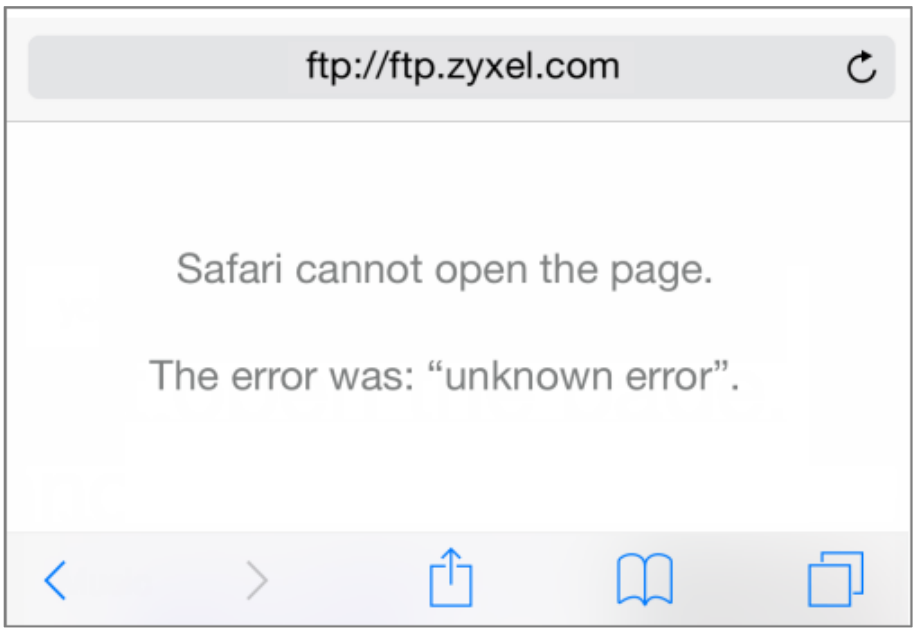
Go to the ZyWALL/USG **Monitor > System Status > Login Users**, you will see current login user list shown as below.

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.



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.

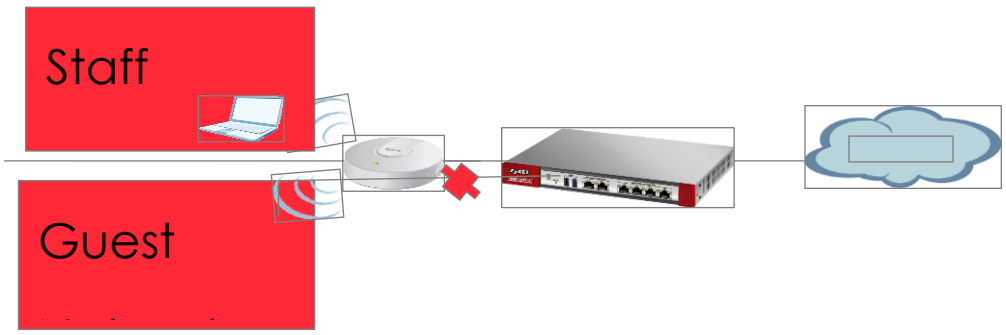
Monitor > Log

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

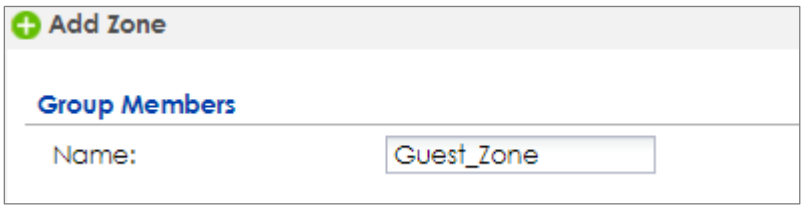
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG210 (Firmware Version: ZLD 4.25)

Set up Wi-Fi VLAN interfaces

Create VLAN interfaces

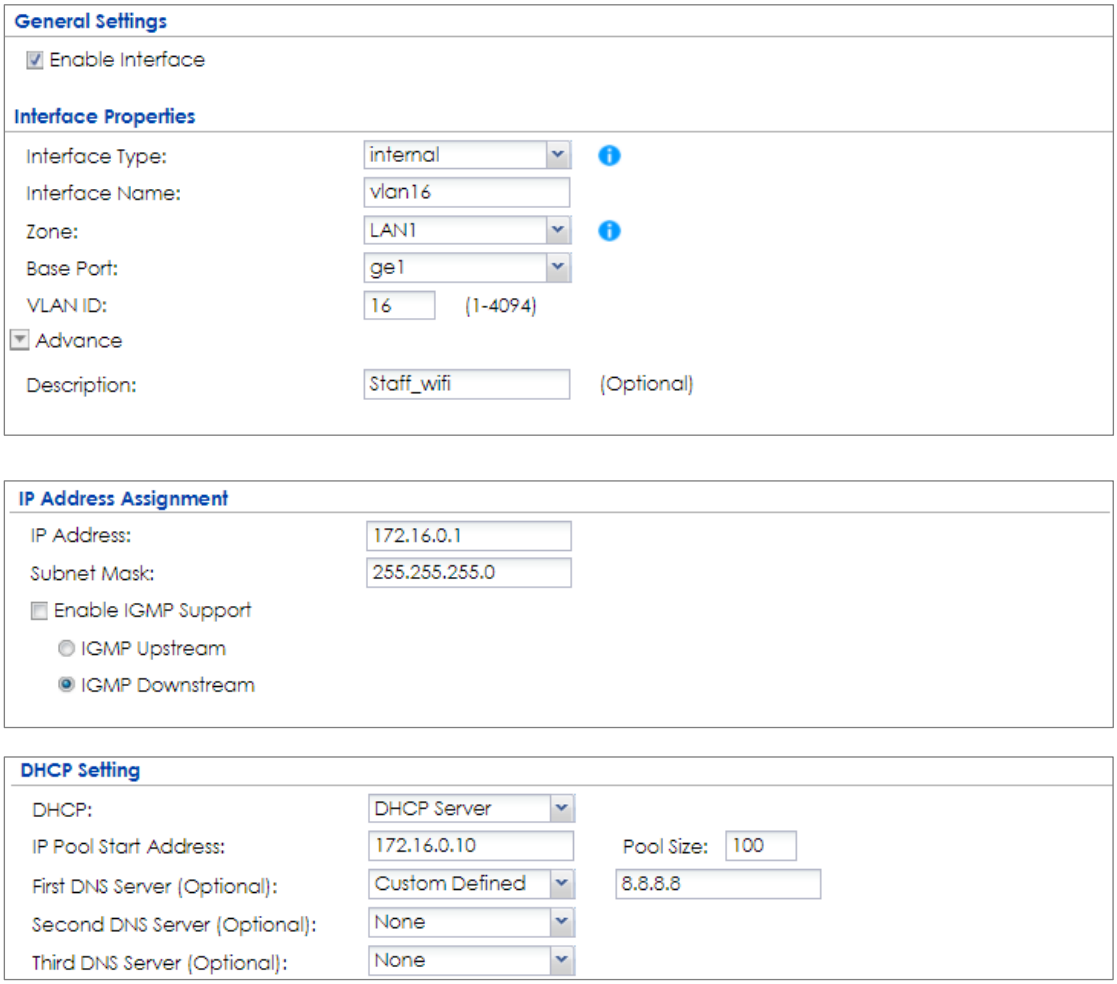
Go to **CONFIGURATION > Object > Zone**. Create a zone for the guest.

CONFIGURATION > Object > Zone

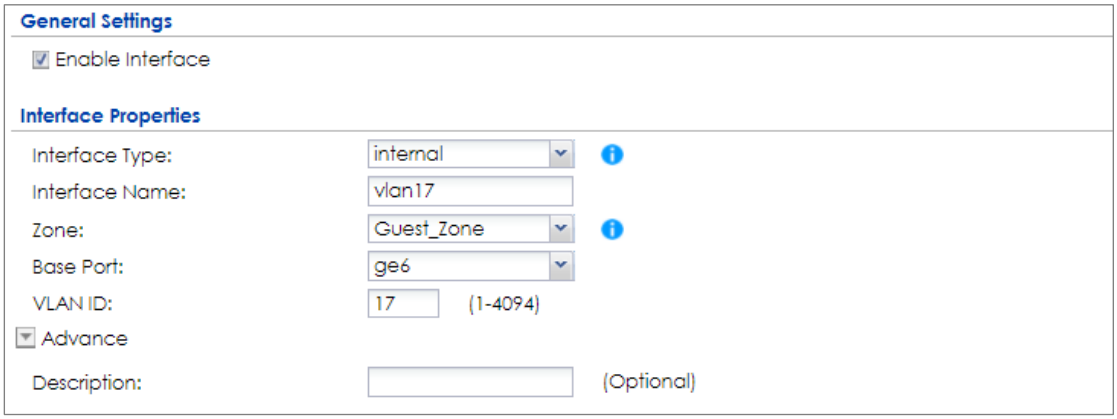


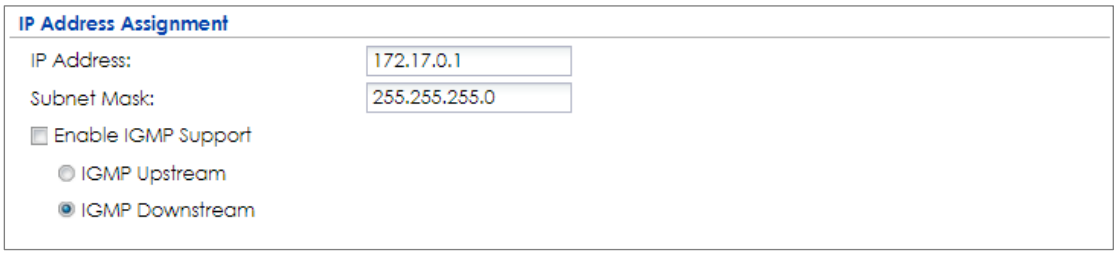
Go to **CONFIGURATION > Network > Interface > VLAN.** Create VLAN16 for Staff_WiFi and VLAN17 for Guest_WiF

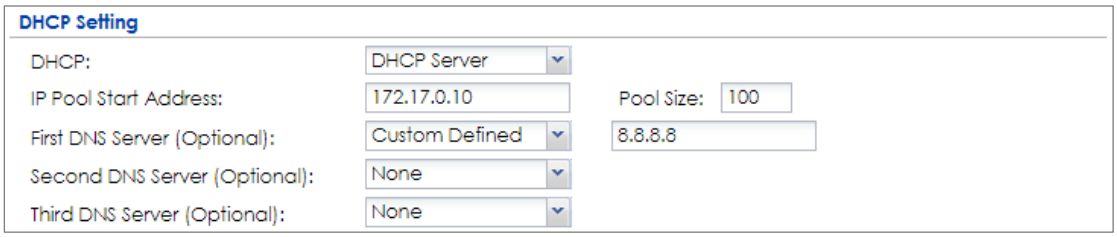
CONFIGURATION > Network > Interface > VLAN > VLAN16



CONFIGURATION > Network > Interface > VLAN > VLAN17

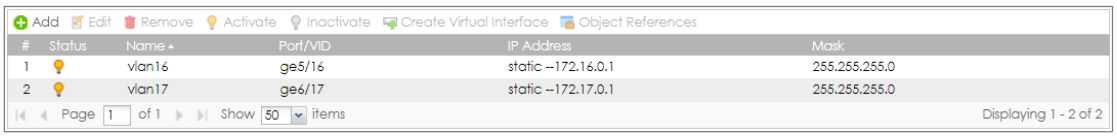






There will be two VLAN interfaces.

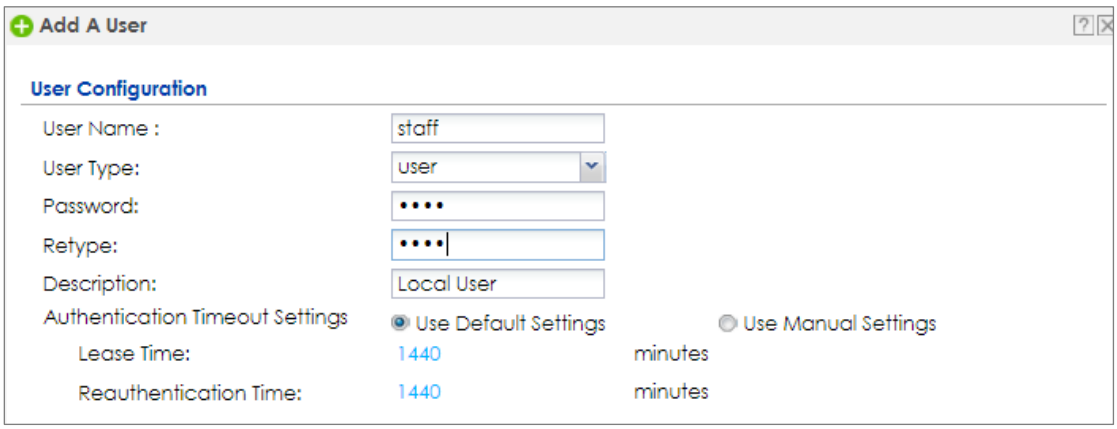
CONFIGURATION > Network > Interface > VLAN



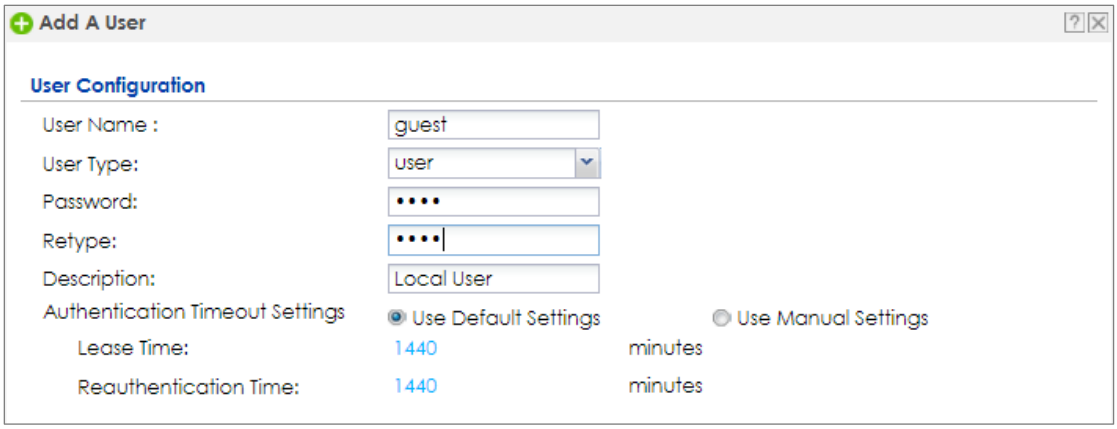
Set Up the User

Go to **Configuration > Object > User/Group > User**, and create users for the staff and the guest

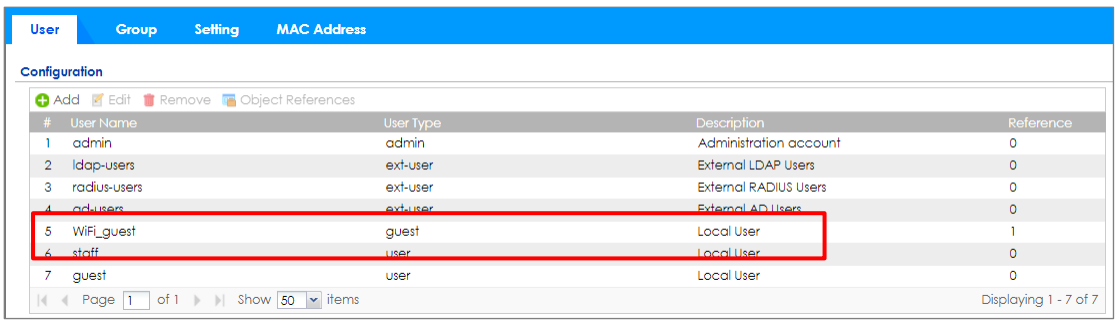
Configuration > Object > User/Group > User > staff



Configuration > Object > User/Group > User > guest



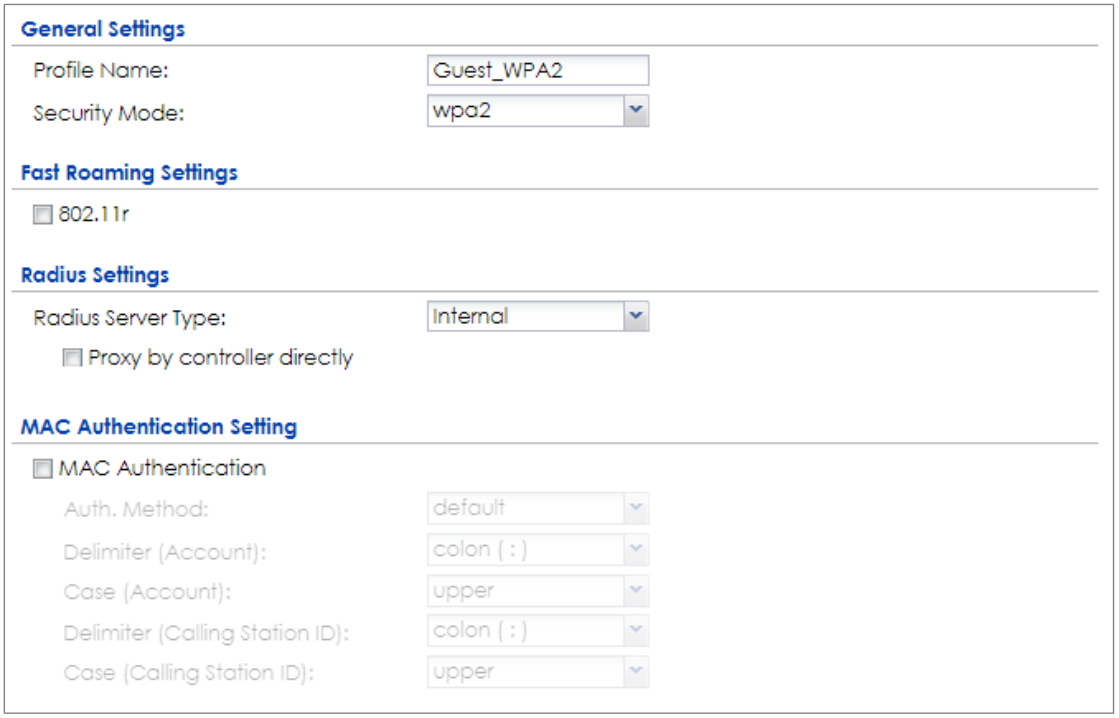
There will be two users.

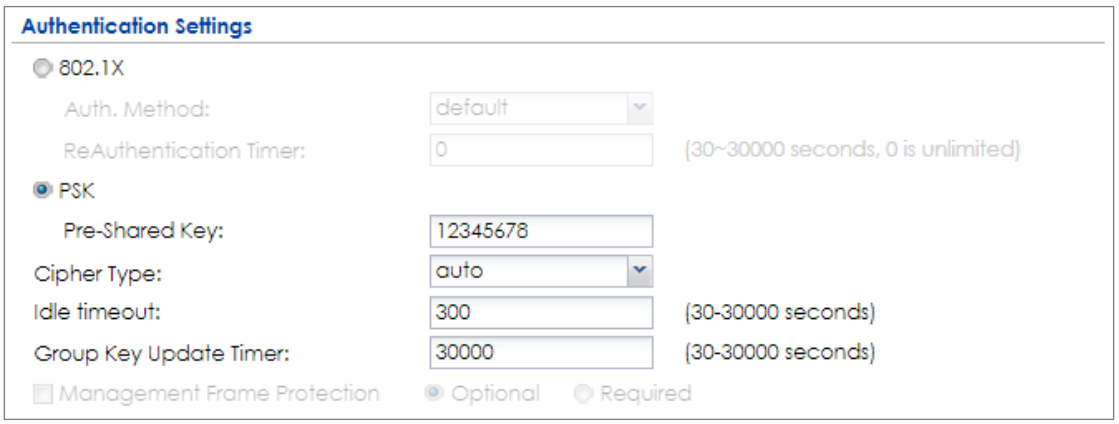


Set Up the AP Profile

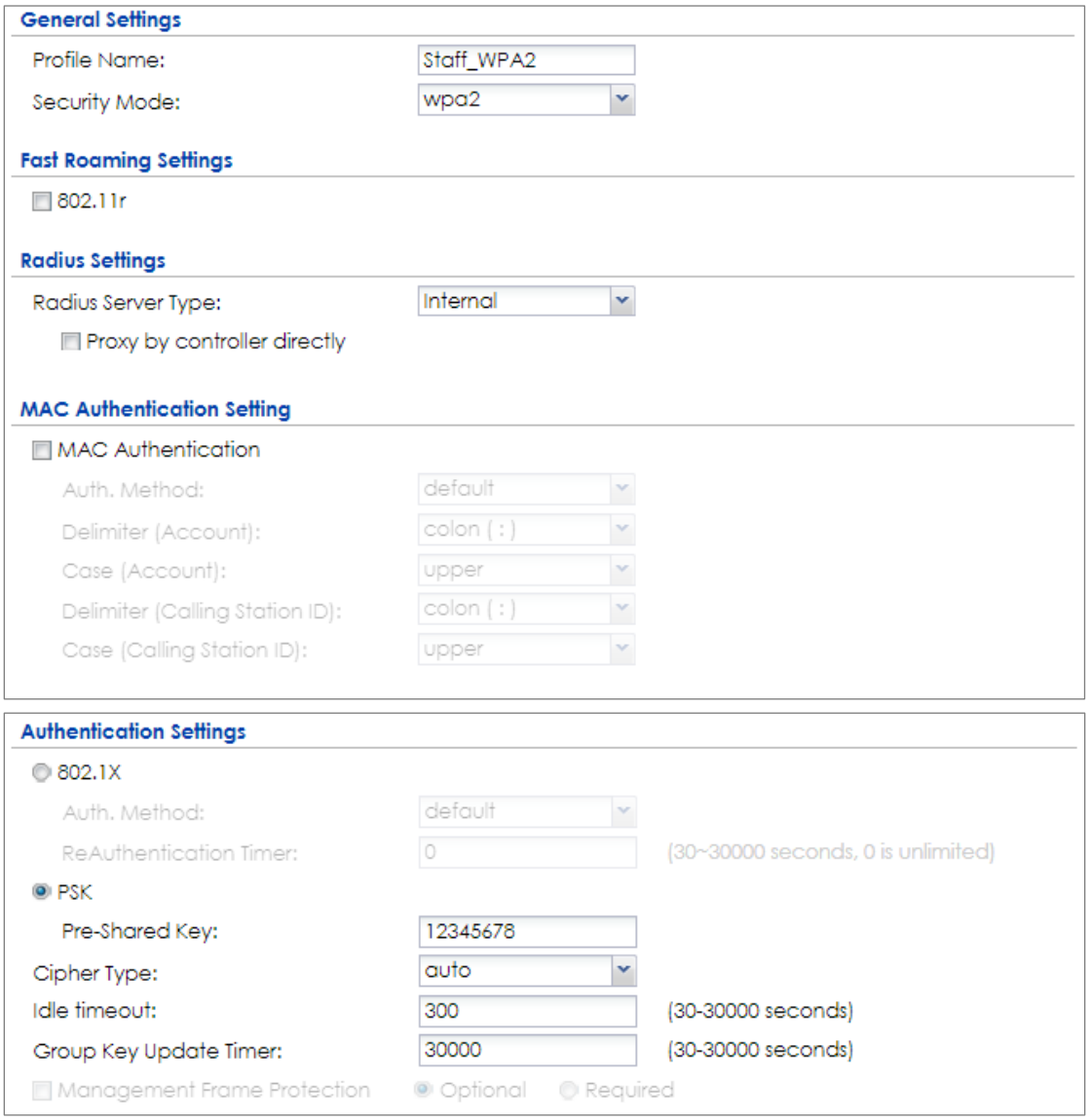
Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, and create two security profiles.

CONFIGURATION > Object > AP Profile > SSID > Security List > Guest_WPA2



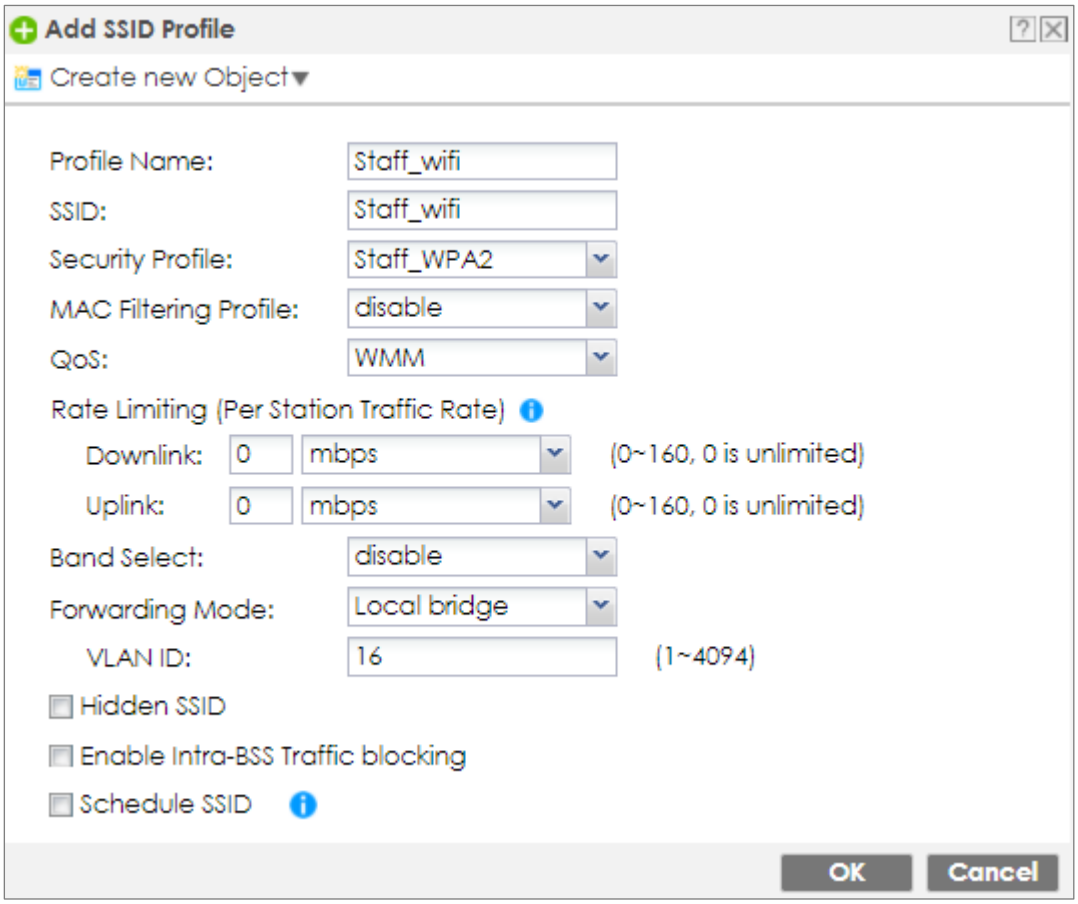


CONFIGURATION > Object > AP Profile > SSID > Security List > Staff_WPA2

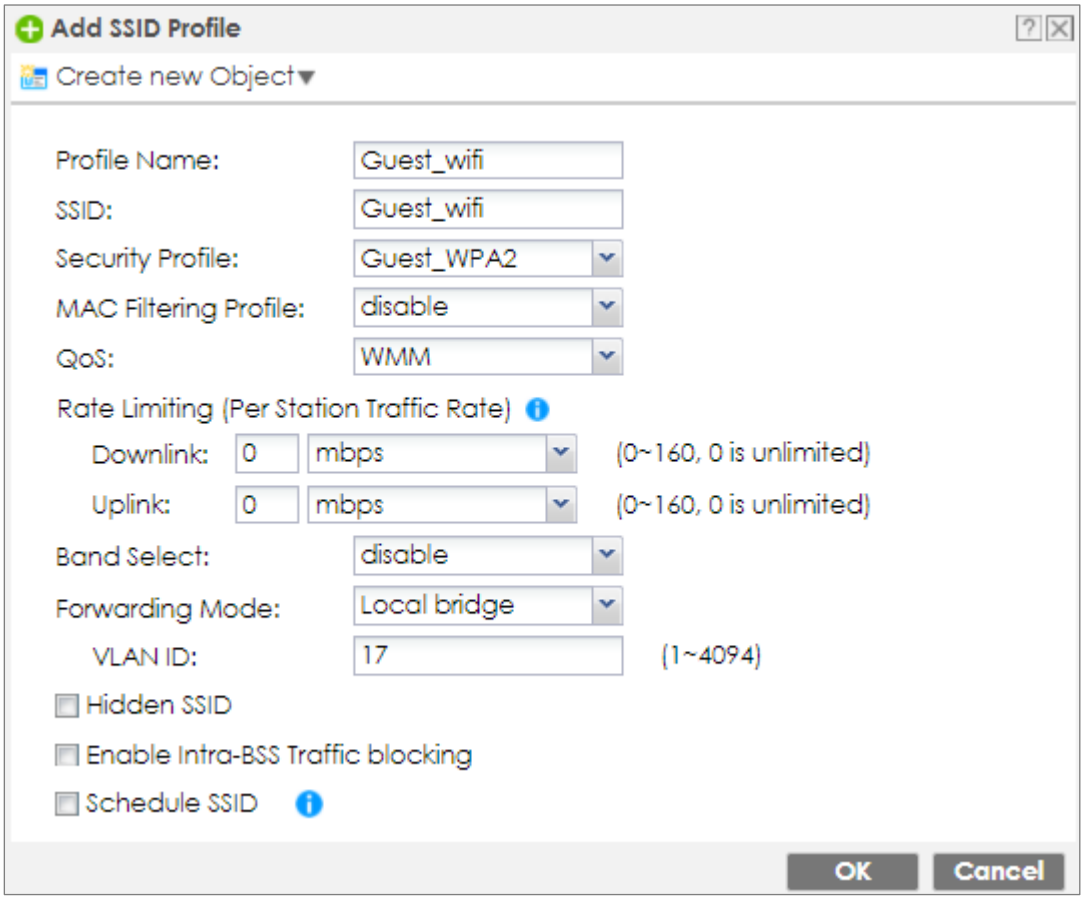


Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List,** and create two SSID profiles.

CONFIGURATION > Object > AP Profile > SSID > SSID List > Staff_Wifi

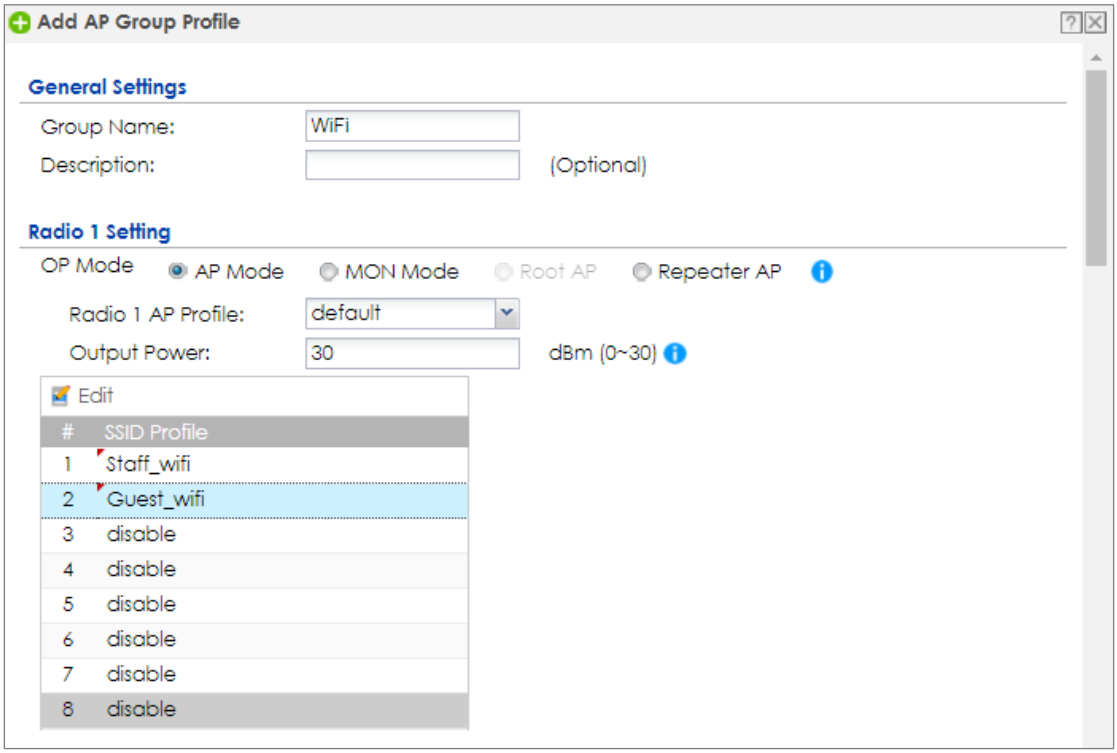


CONFIGURATION > Object > AP Profile > SSID > SSID List > Guest_Wifi



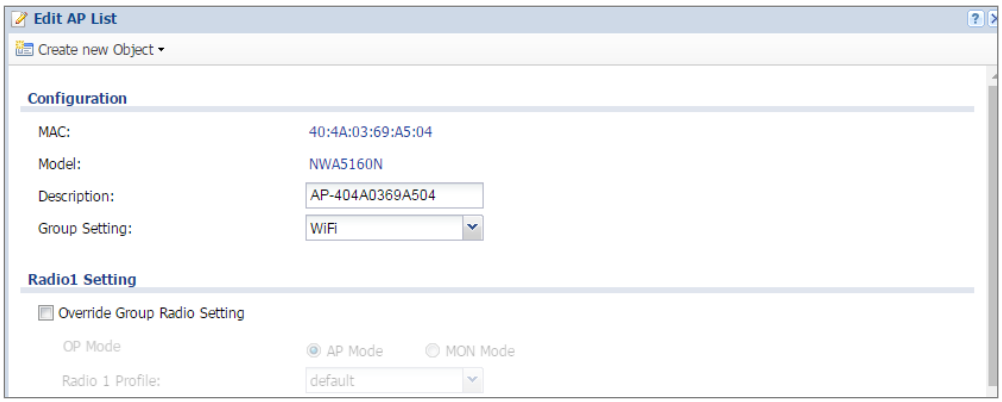
Go to **CONFIGURATION > Wireless > AP Management > AP Group**, and add an AP Group as **WiFi**.

CONFIGURATION > Wireless > AP Management > AP Group



Go to **CONFIGURATION > Wireless > AP Management > Mgnt. AP List**, and Edit the AP List. Change the Group setting as **WiFi**

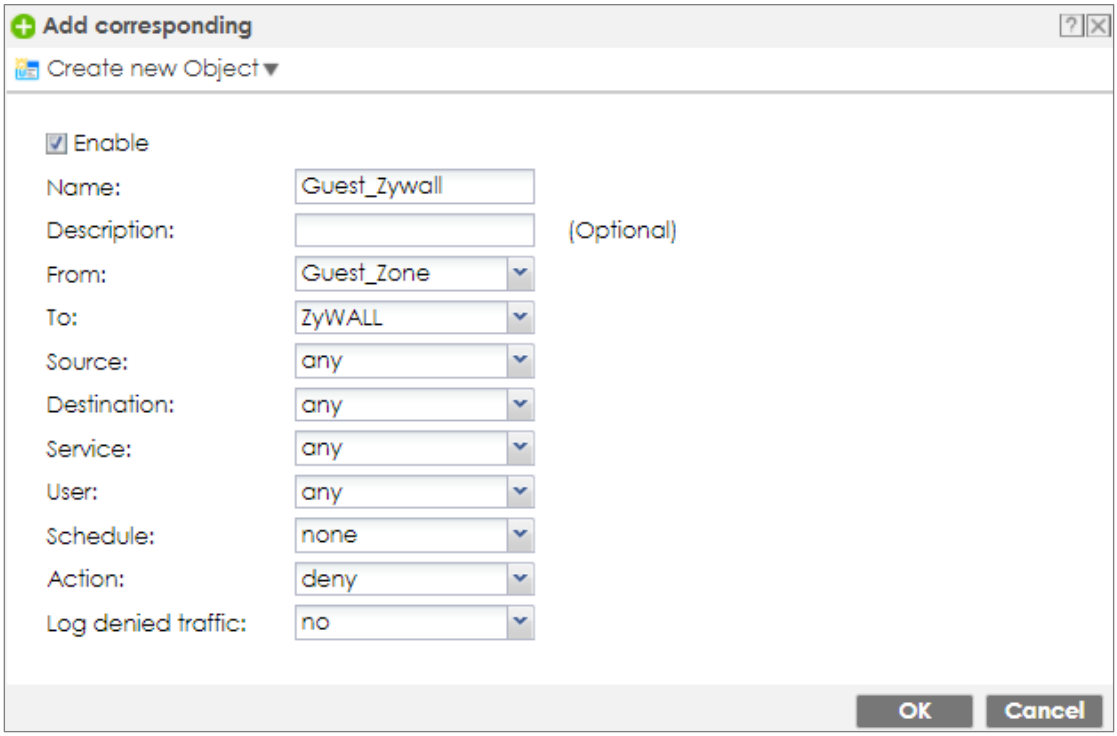
CONFIGURATION > Wireless > AP Management > Mgnt. AP List,



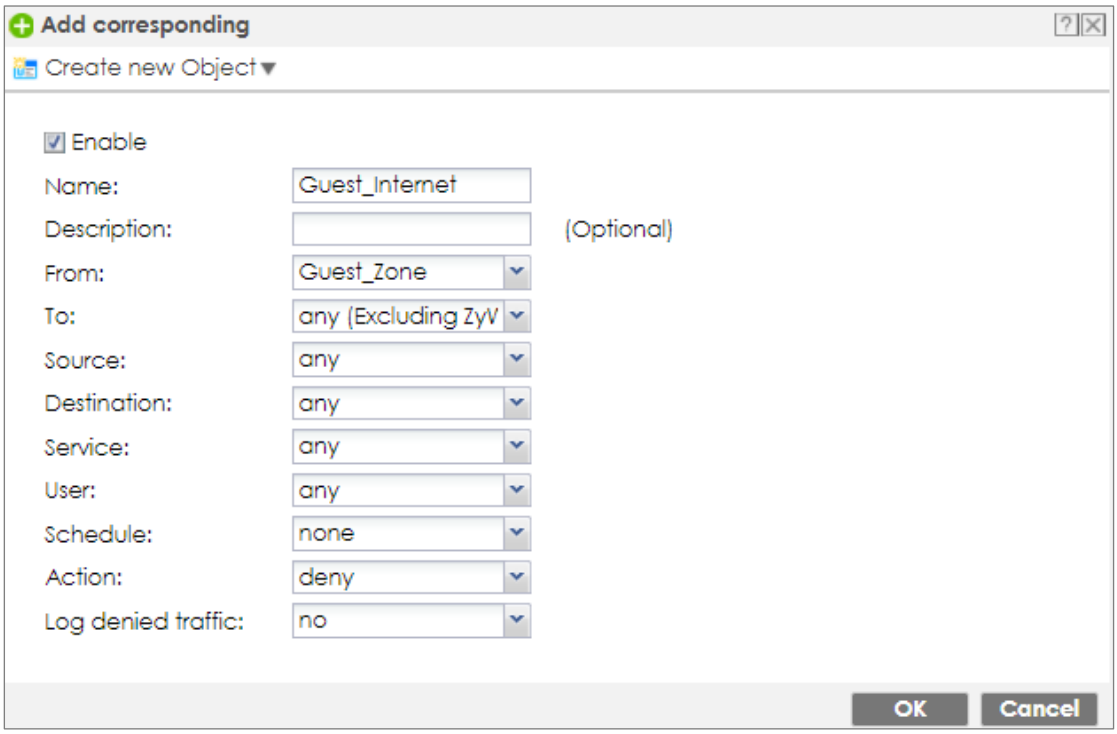
Set Up the Security policy rule

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

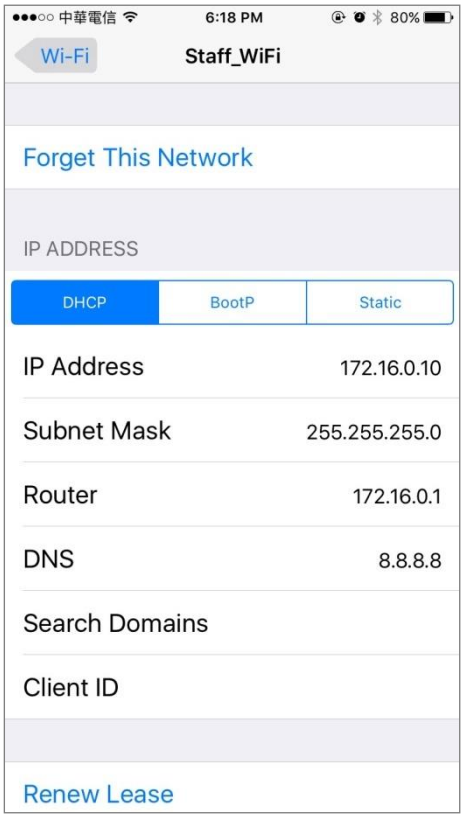


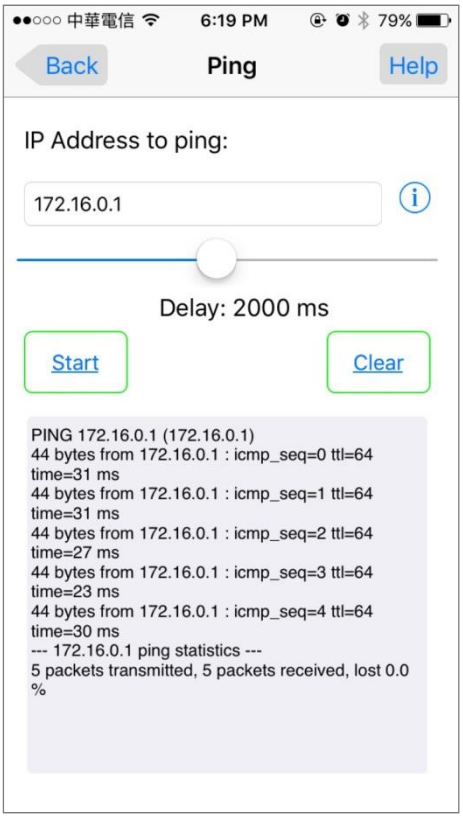
CONFIGURATION > Security Policy > Policy Control > Policy > Guest_Internet



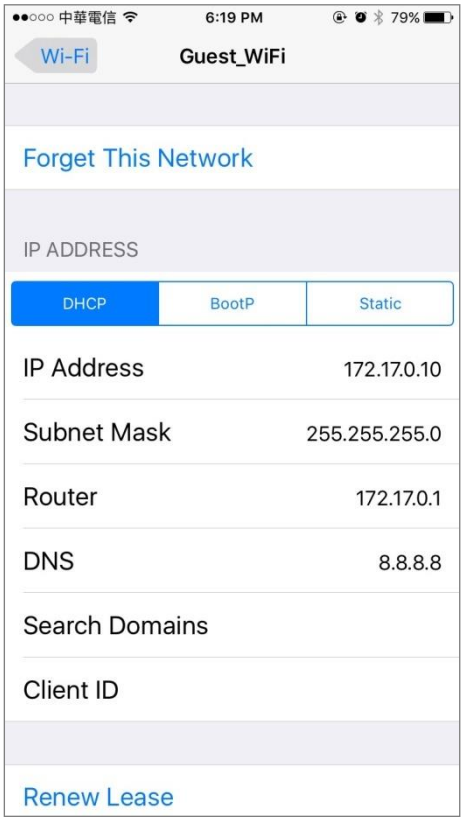
Test result

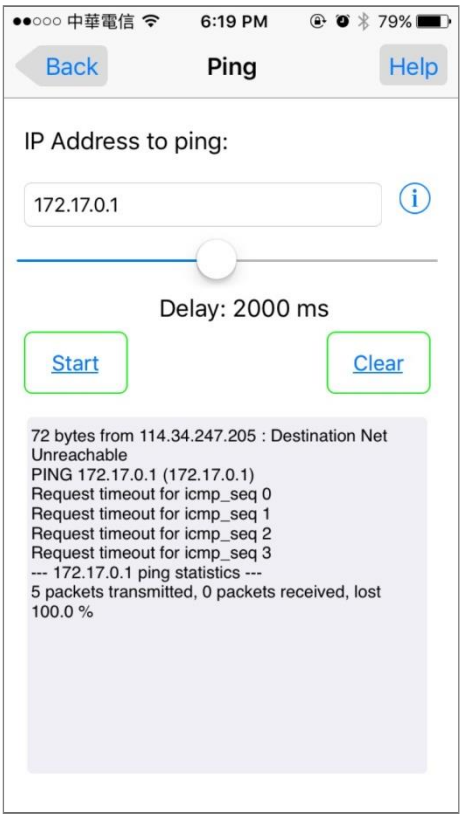
Connect to the SSID Staff_WiFi, and ping the USG interface.





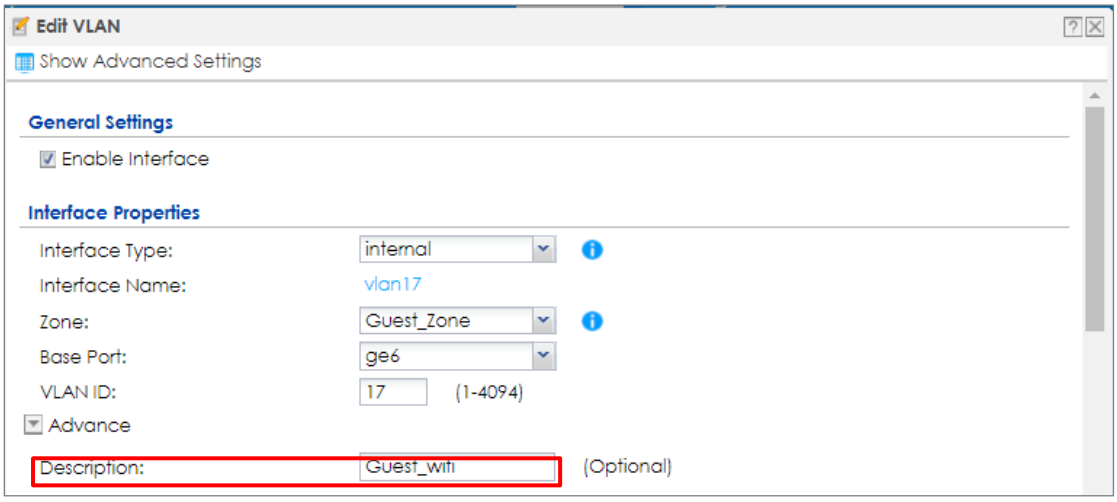
Connect to the SSID Guest_WiFi, and ping the USG interface



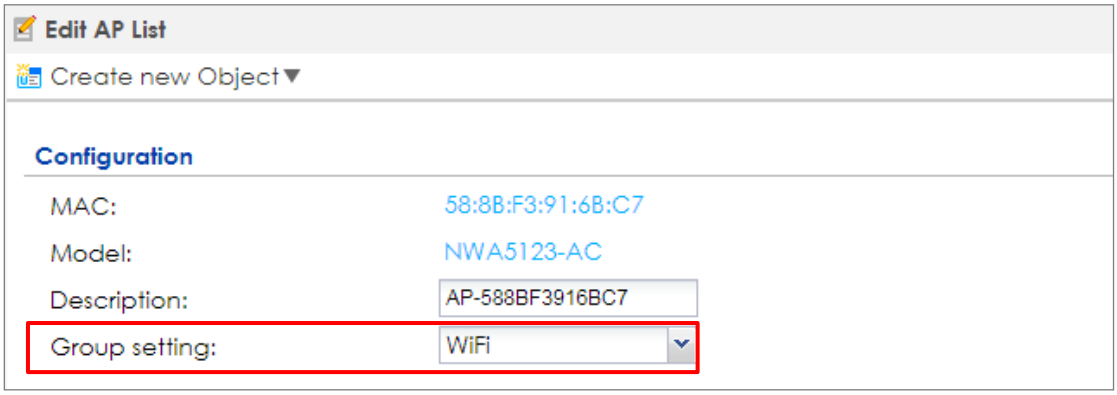


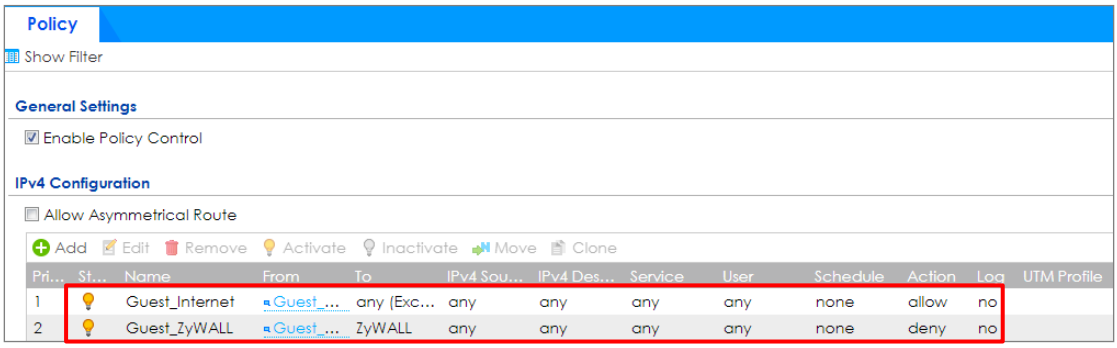
What could go wrong

Choose the wrong zone for the Guest VLAN interface.



Not change the AP to the correct group

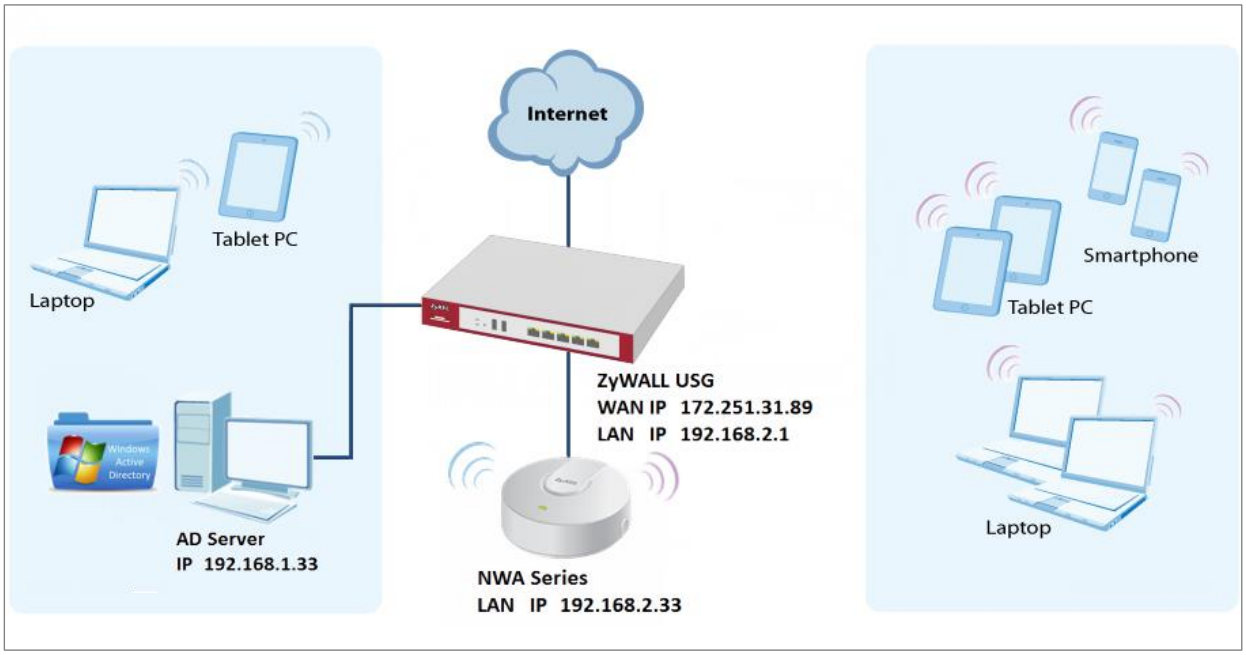

Edit AP List
Create new Object
Configuration
MAC:
58:8B:F3:91:6B:C7
Model:
NWA5123-AC
Description:
AP-588BF3916BC7
Group setting:
WiFi


Policy
Show Filter
General Settings
Enable Policy Control
IPv4 Configuration
Allow Asymmetrical Route
Add
Edit
Remove
Activate
Inactivate
Move
Clone
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

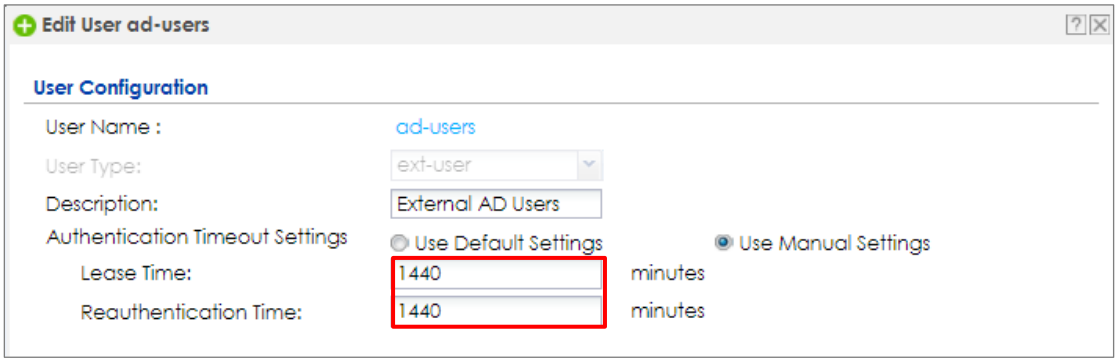


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Wi-Fi Guest Account and Authentication Method on the ZyWALL/USG

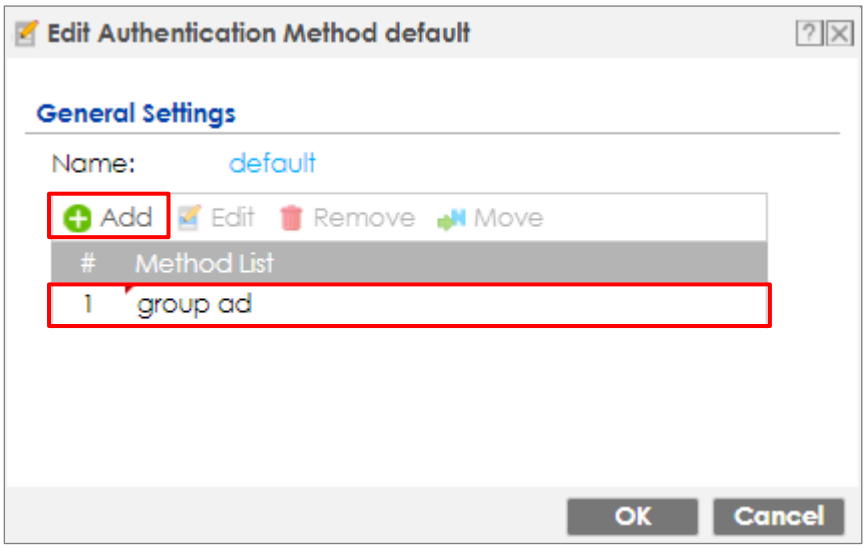
In the ZyWALL/USG, go to **CONFIGURATION > Object > User/Group > User > ad-users**, set the **Authentication Timeout Settings** to **Use Manual Settings** and enter the number of minutes this user has to renew the current session before the user is logged out.

CONFIGURATION > Object > User/Group > User > ad-users



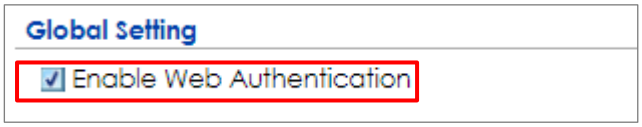
In the ZyWALL/USG, go to **CONFIGURATION > Object > Authentication Method > default > Edit Authentication Method default**, click **Add** to insert group ad in the table. Click **OK**.

CONFIGURATION > Object > User/Group > User > ad-users



In the ZyWALL/USG, go to **CONFIGURATION > Web Authentication > General Settings** and select **Enable Web Authentication**.

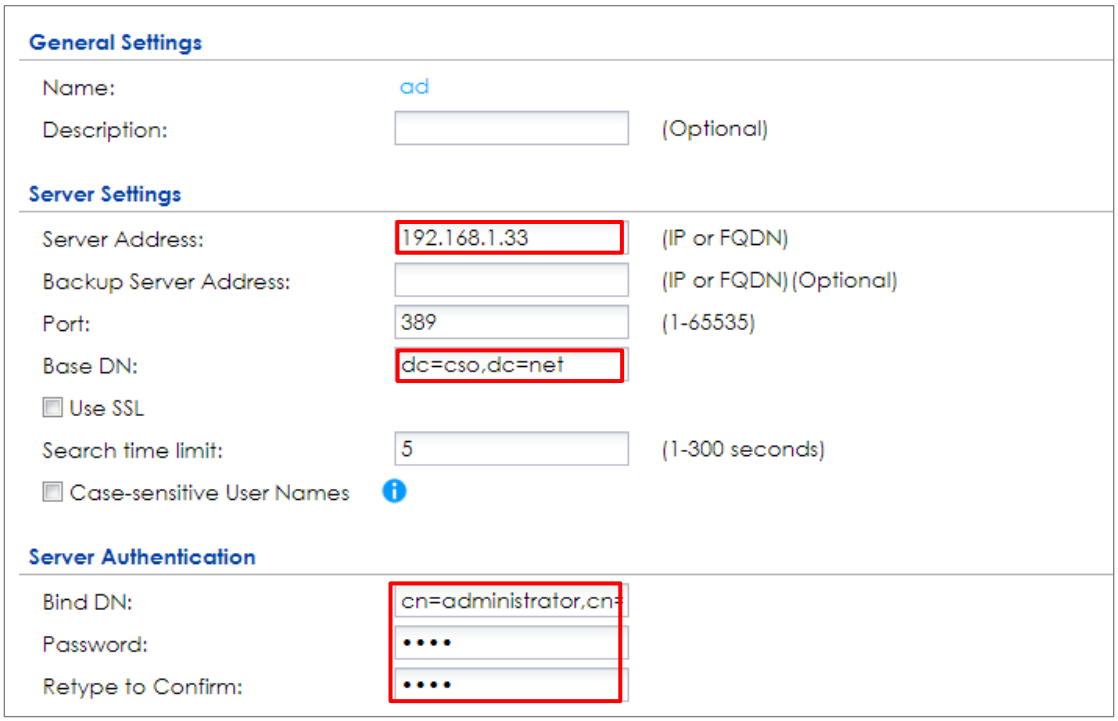
CONFIGURATION > Web Authentication > General Settings



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.

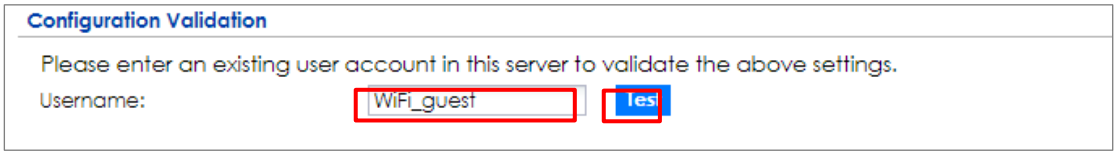
CONFIGURATION > Object > AAA Server > Active Directory > Add Active Directory

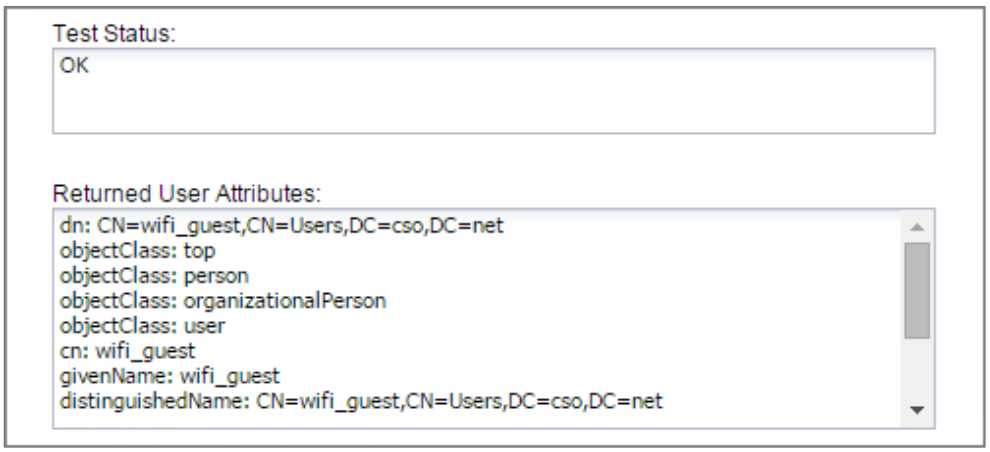


Scroll down to the **Configuration Validation** section, use a user account from the server specified above to test if the configuration is correct. Enter the account's user name (wifi_guest in this example) in the **Username** field and click **Test**. A pop-

up 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





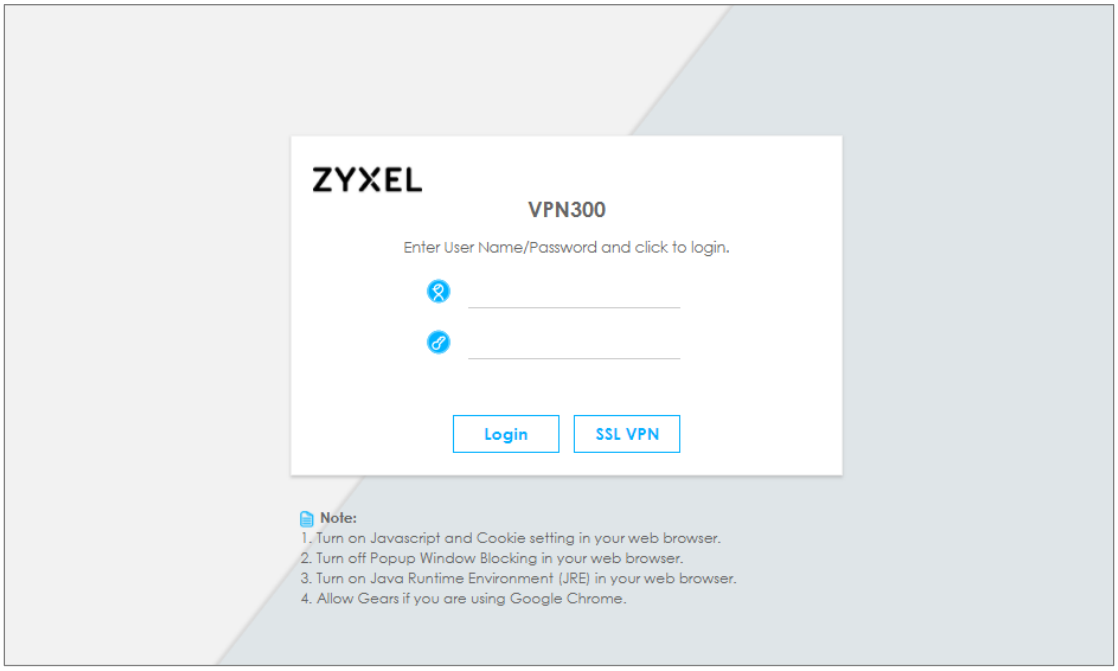
Set Up the Security Policy on the ZyWALL/USG

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.

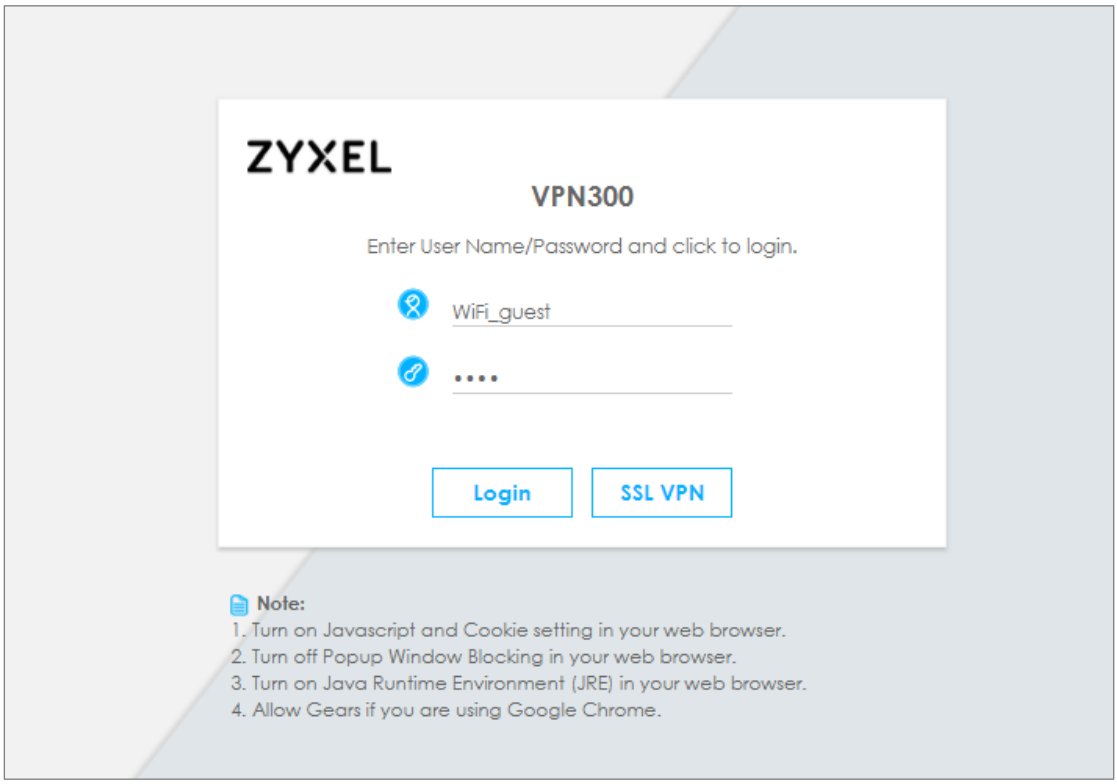
CONFIGURATION > Security Policy > Policy > Add corresponding

Test the Result

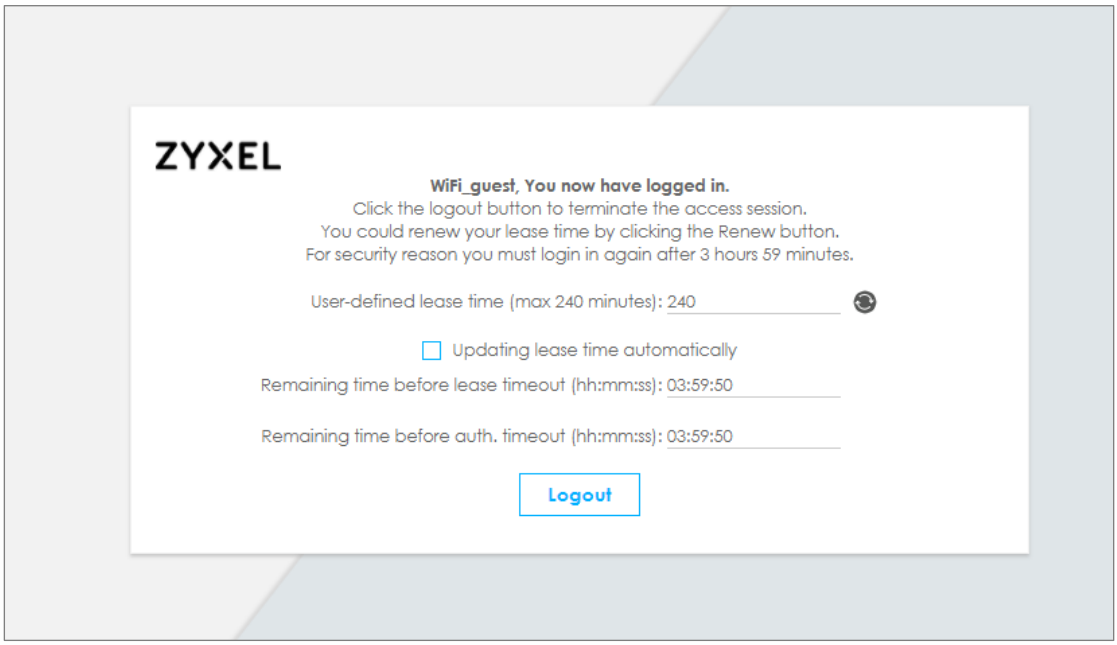
Using a mobile device to connect to the AP which is connected to the ZyWALL/USG. When you try to access the Internet, it will redirect to the user login screen.



Type the Wi-Fi guest **User Name** and **Password**, click **Login**.



The access session page will appear.



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.

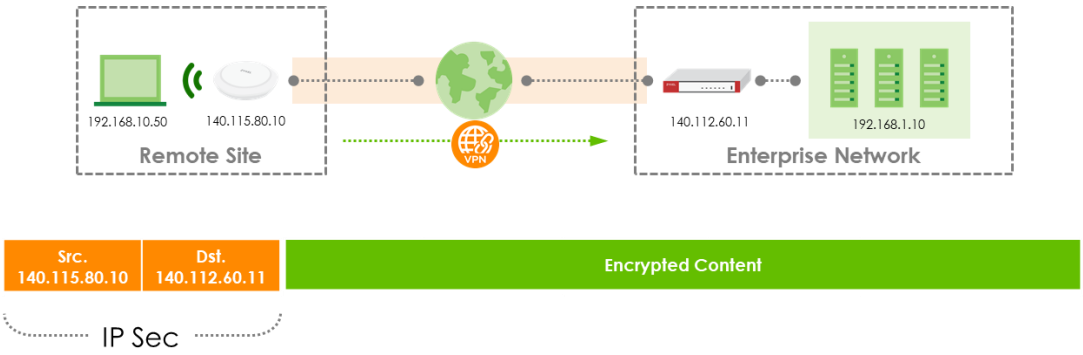
Monitor > Log

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.

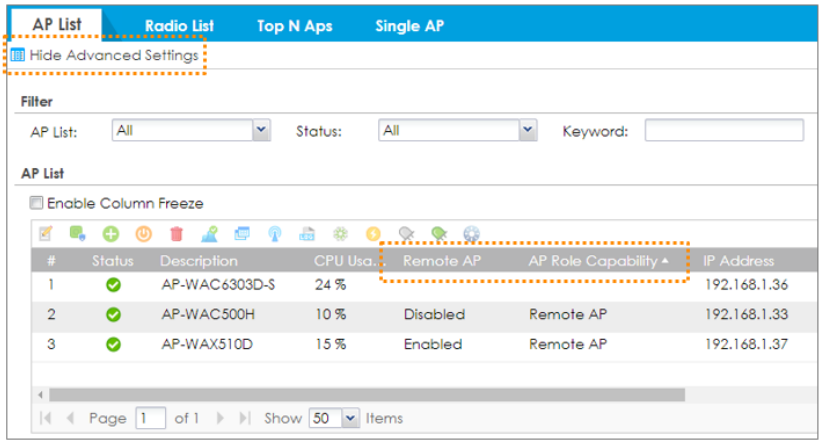


Secure Wi-Fi supported models:

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.**



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

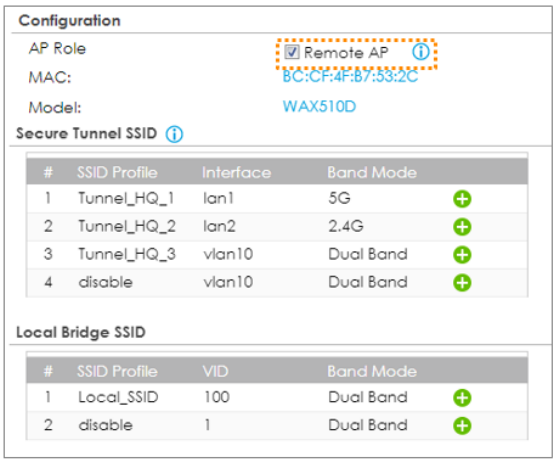
Stage two, remote users power up the AP, and then the IP Sec tunnel will be established automatically.

- 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.

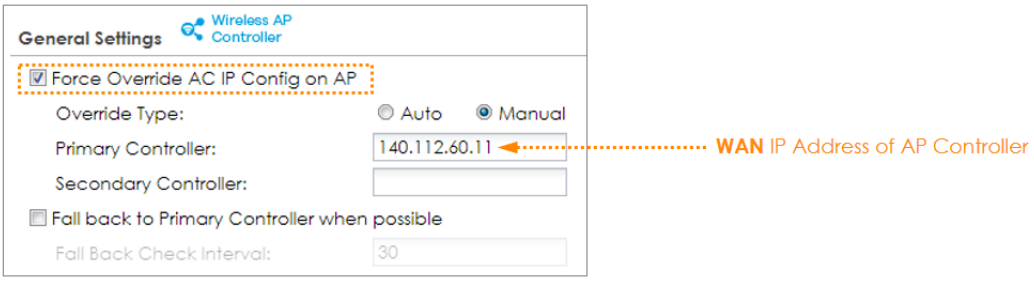


NOTE: Secure Tunnel can be only applied to SSID, Ethernet traffic from clients connecting to AP's LAN port won't be tunneled back to Controller.

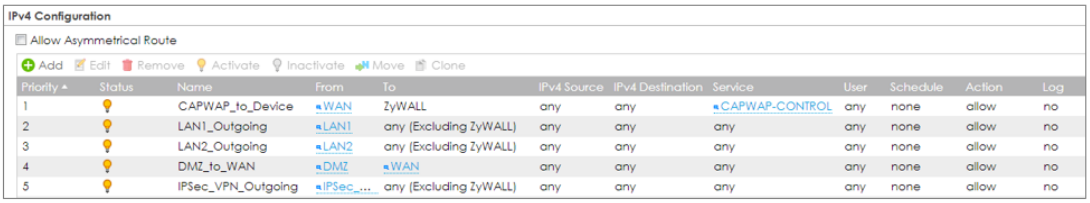
Update the Controller IP as the USG's WAN IP

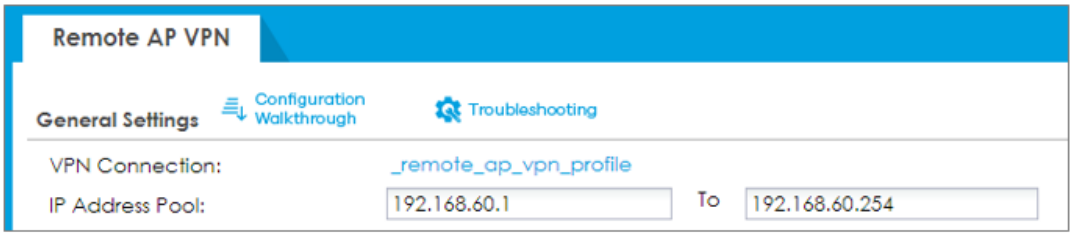
Besides setting the SSID also need to override the Controller's IP address on AP to let it connect back to HQ's Gateway after booting up in remote site. If Gateway supports dual WAN, add another WAN IP in the "secondary controller" column. FQDN is also an available input option for dynamic WAN IP, but requires corresponding DNS settings.

Assign Gateway's WAN IP as AP's Controller IP at: **Configuration > Wireless > AP Management > AP Policy**

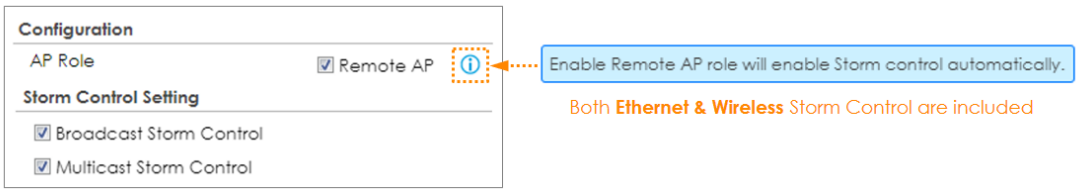


Firewall Policy Rule that is for CAPWAP connection and Remote AP VPN IP Address Pool that is a new subnet (192.168.60.1/24) for Remote AP VPN Client use will be auto-added when Remote AP is enabled.





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.



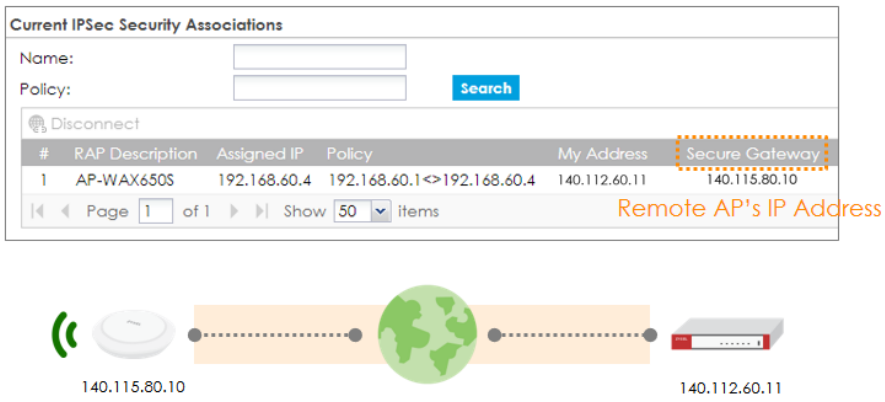
Power up remote APs at remote side

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



What can go wrong

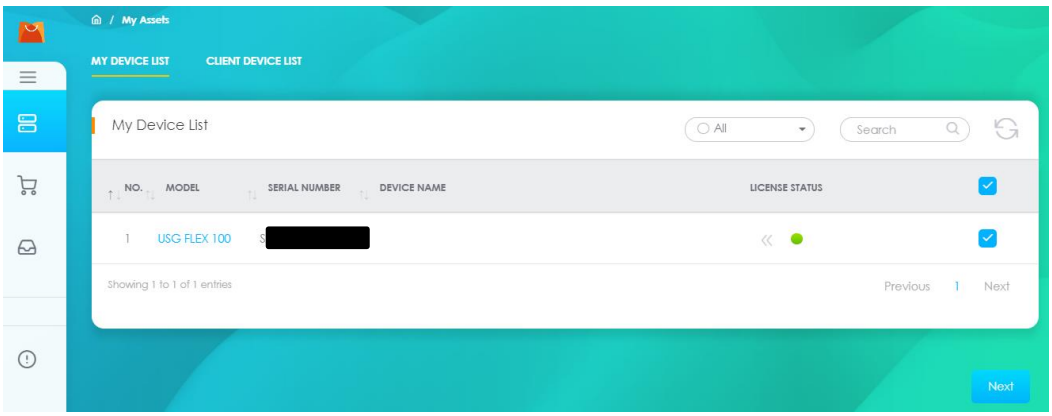
1. Configure all the corresponding setting on interface before you connect the link.
2. Maximum Remote AP number is limited by Device's capability of "Max. Concurrent IPsec Tunnel" and 25% of Maximum managed AP number.
3. Secure Wi-Fi requires specific license on AP.

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.



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

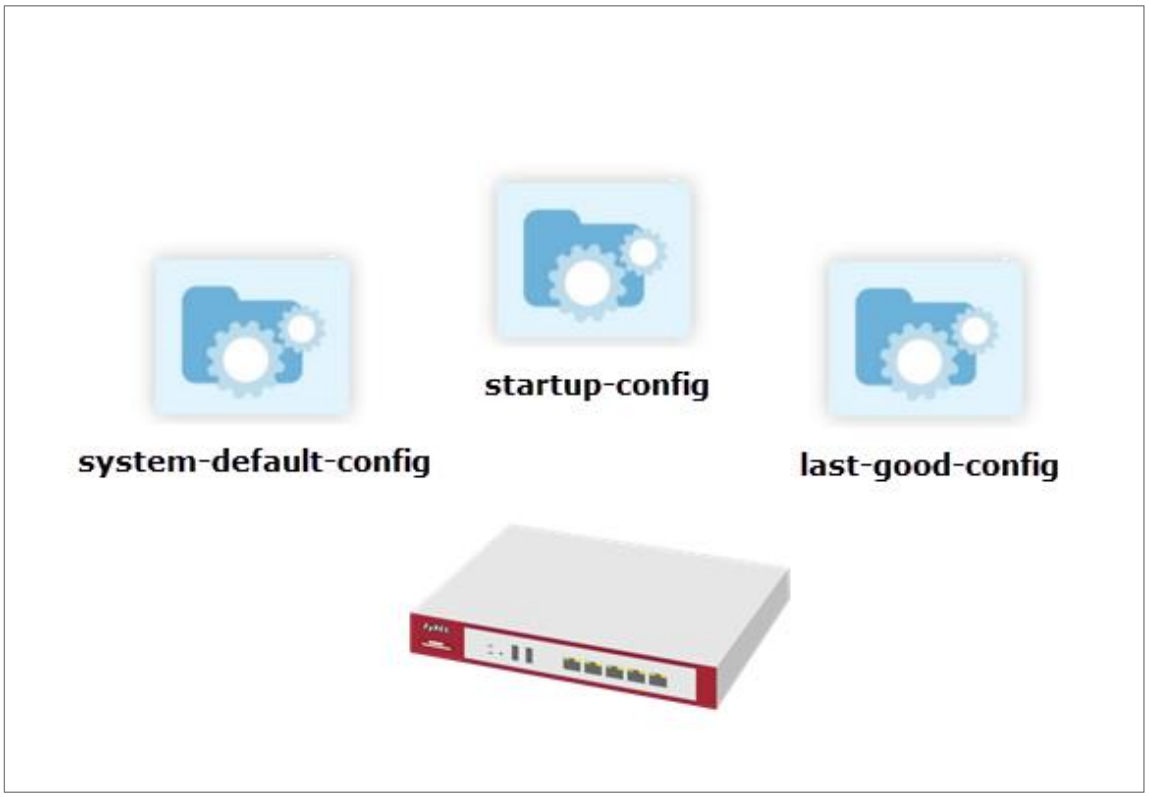
This is an example of how to rename, download, copy, apply and upload configuration files. Once your ZyWALL/USG is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be 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

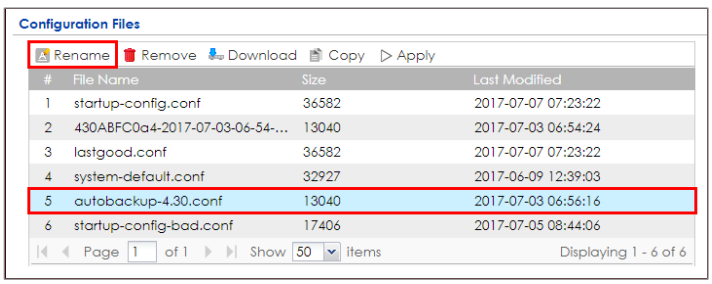


Note: This example was using USG310 (Firmware Version: ZLD 4.25).

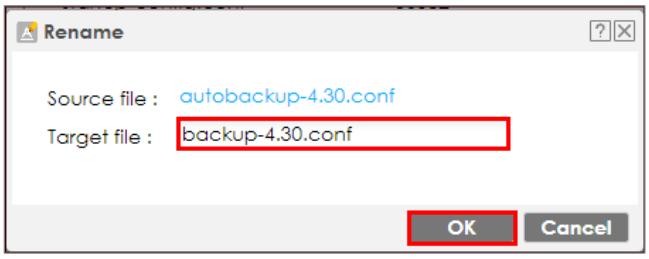
Rename the Configuration Files from the ZyWALL/USG

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



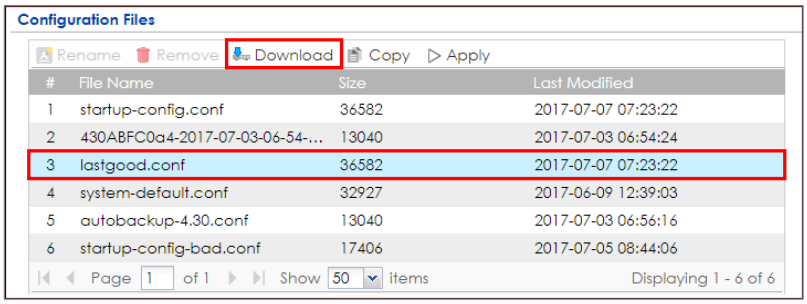
MAINTENANCE > File Manager > Configuration File > Rename



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.

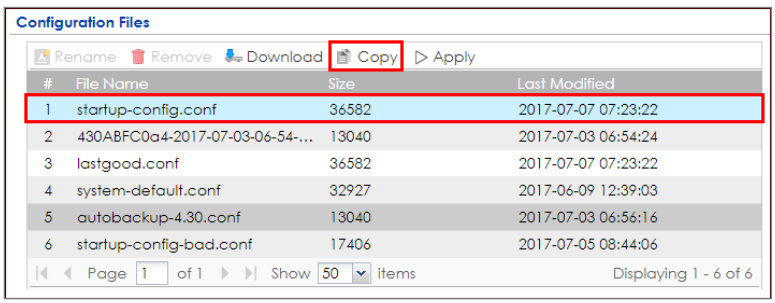
MAINTENANCE > File Manager > Configuration File



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

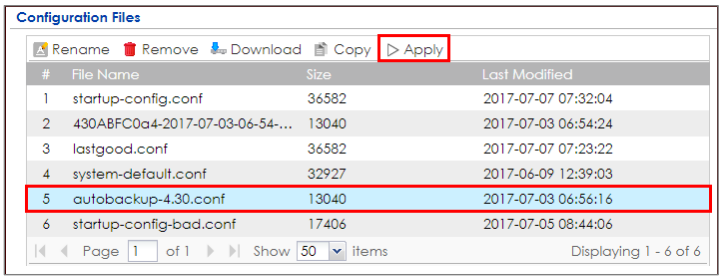


MAINTENANCE > File Manager > Configuration File > Copy

Apply the Configuration Files on the ZyWALL/USG

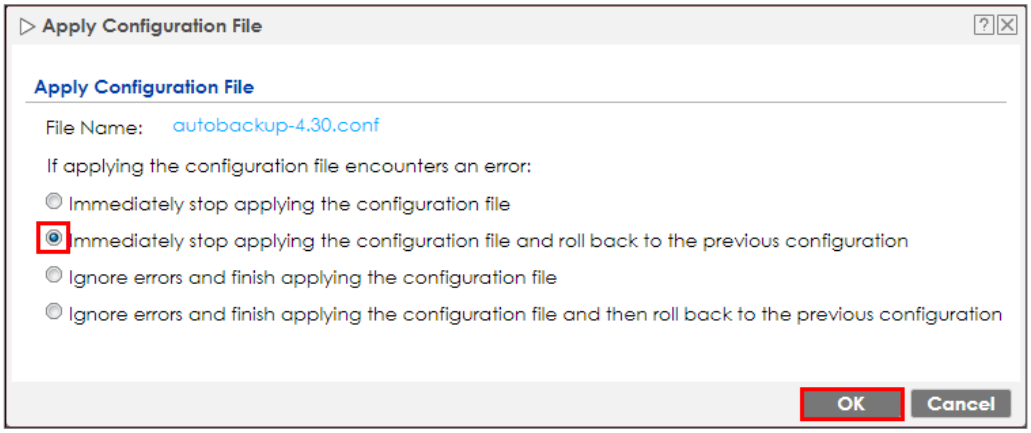
In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File**, select a specific configuration file to have ZyWALL/USG use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL/USG settings to the factory defaults. Or select the **lastgood.conf** 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



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

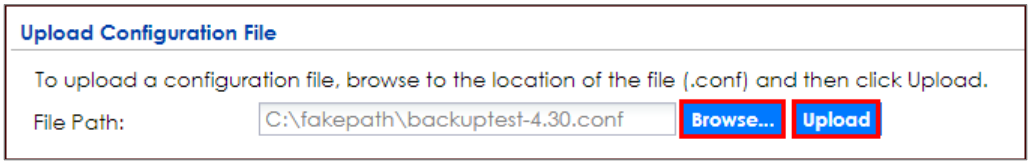


Note: Do not shut down the ZyWALL/USG while the configuration file is being applied.

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.

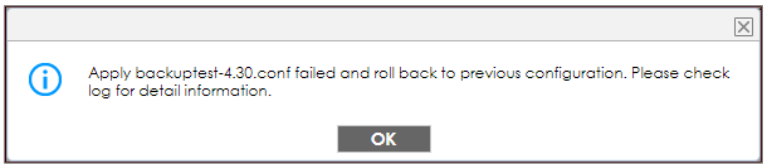
MAINTENANCE > File Manager > Configuration File



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



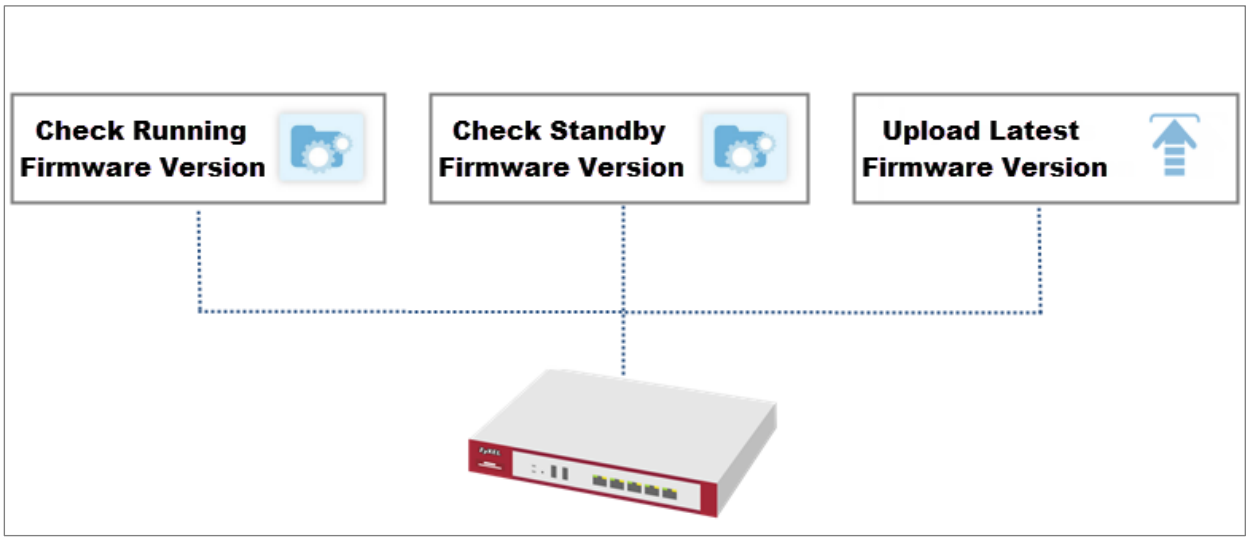
Monitor > Log

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.

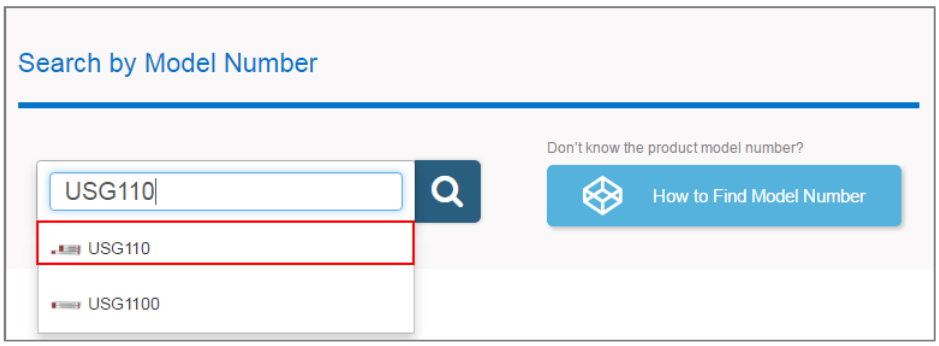
ZyWALL/USG with Firmware Management Example

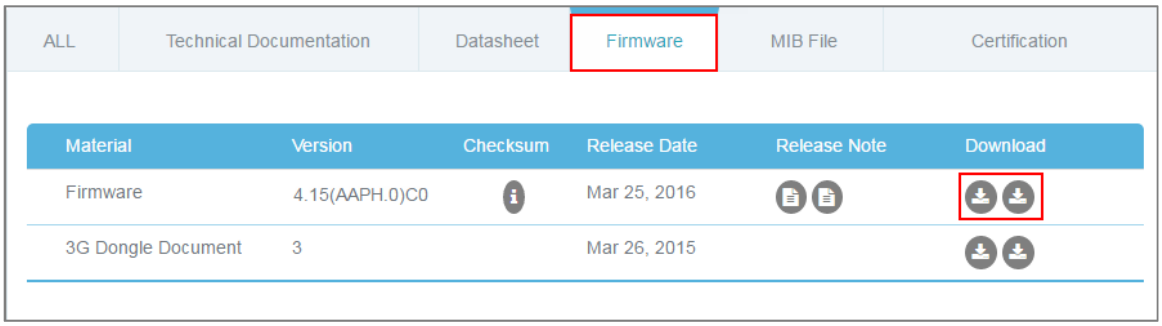


Note: The firmware update can take up to five minutes. Do not turn off or reset the ZyWALL/USG while the firmware update is in progress. This example was using USG110 (Firmware Version: ZLD 4.25).

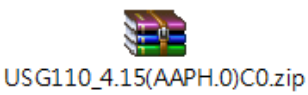
Download the Current Firmware Version from ZyXEL.com

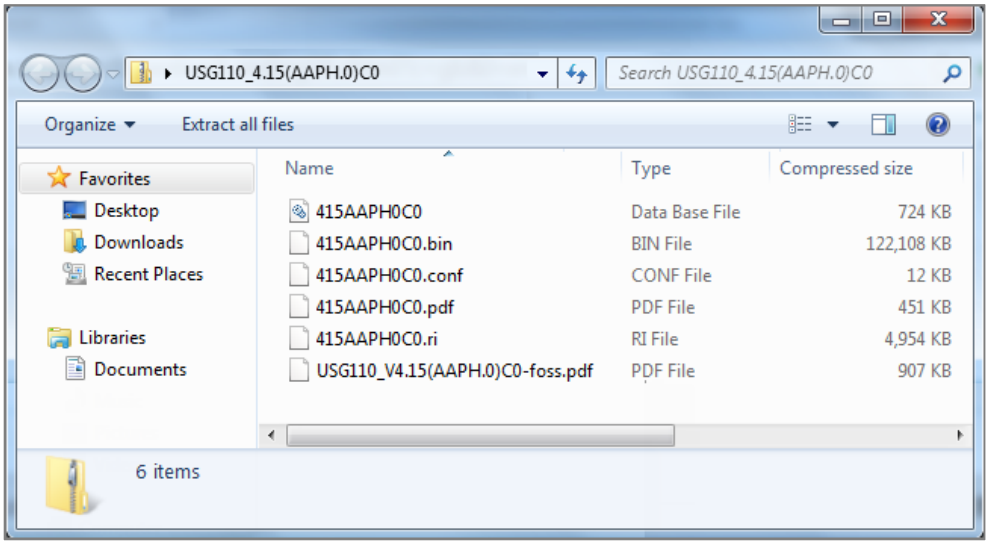
Go to www.zyxel.com/support/download_landing.shtml and download the current firmware package.





Extract firmware zip file.



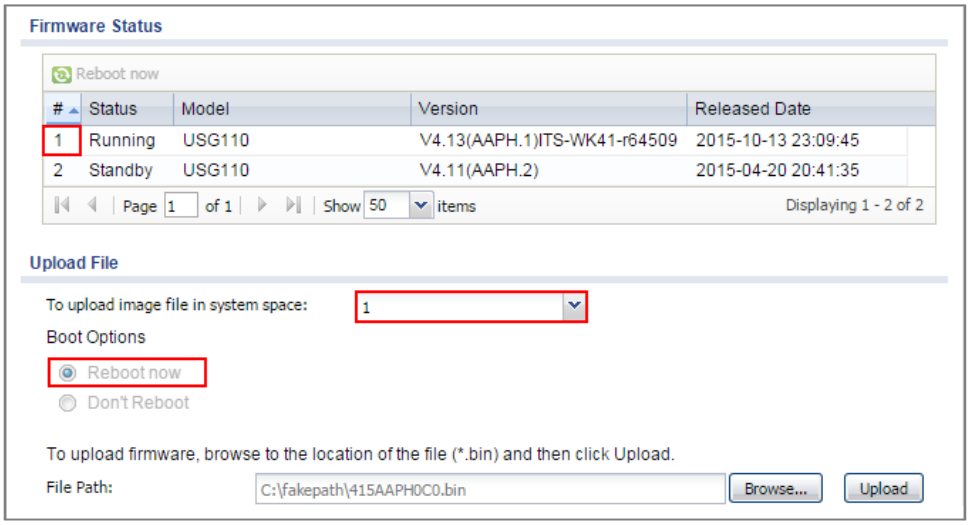


Upload the Firmware on the ZyWALL/USG

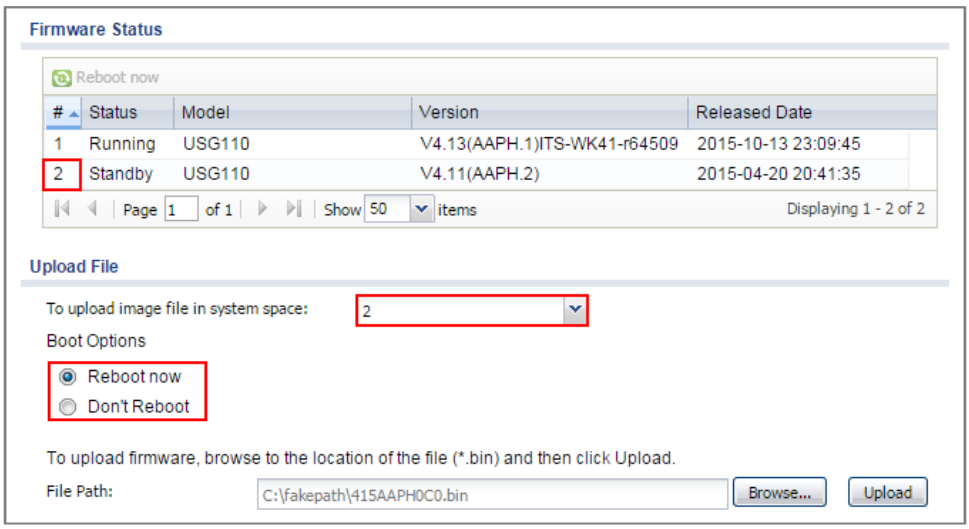
In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Firmware Package > Upload File**. Click the **To upload image file in system space** pull-down menu and select (**1**) or (**2**). The default **Standby** system space is (**2**), so if you want to upload new firmware to be the **Running** firmware, 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**.

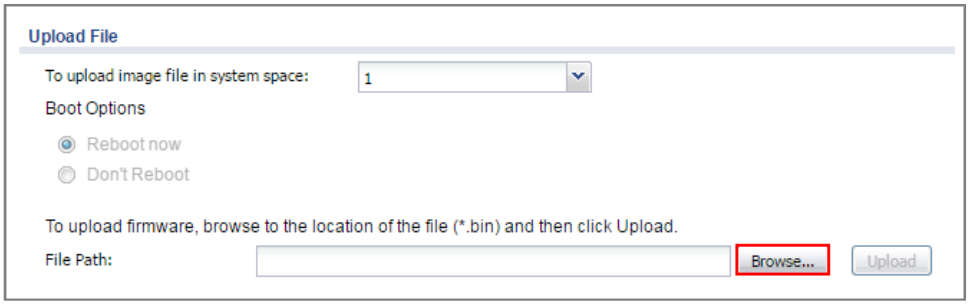
MAINTENANCE > File Manager > Firmware Package > Upload File > (1)

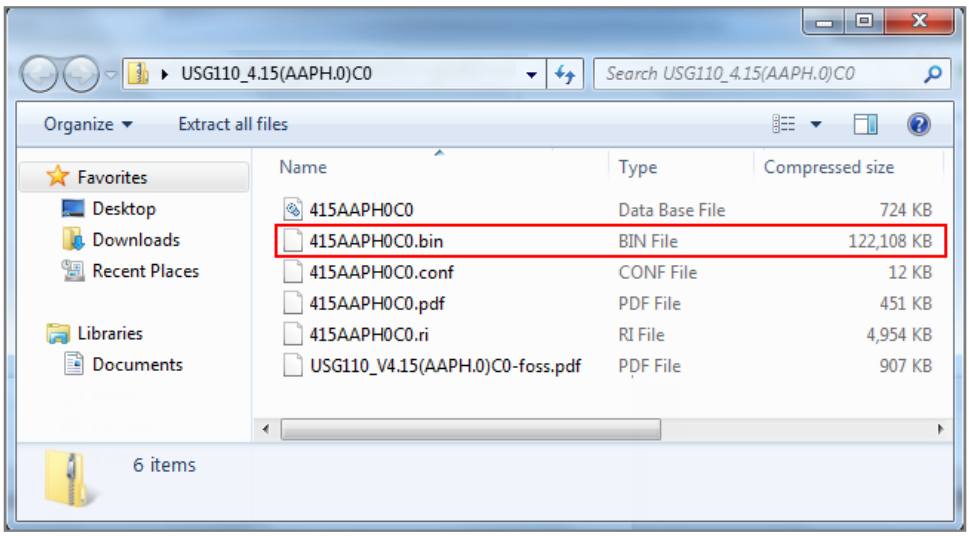


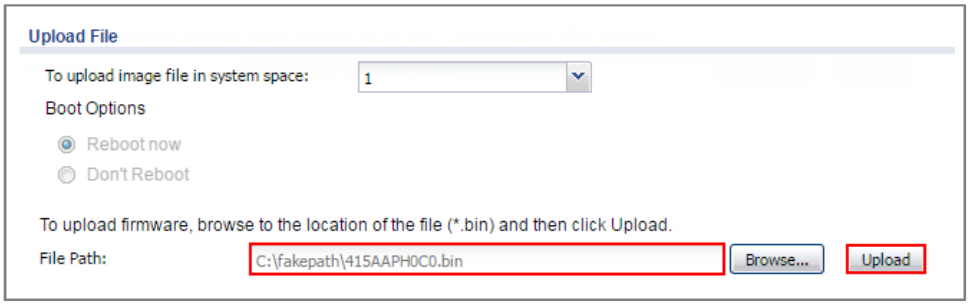
MAINTENANCE > File Manager > Firmware Package > Upload File > (2)



To upload firmware, click **Browse** to the location of the file (*.bin) and then click **Upload**.







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).

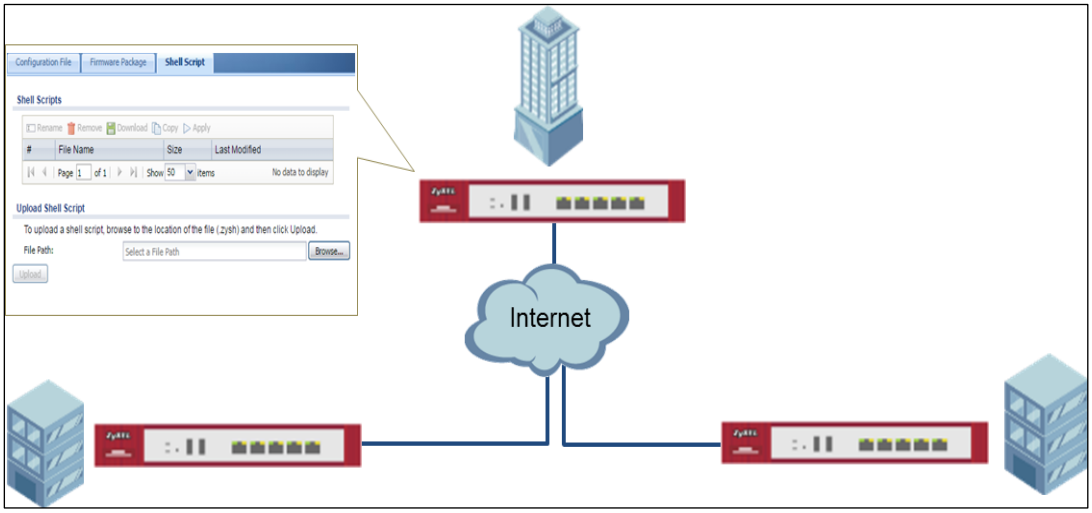
What Could Go Wrong?

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.

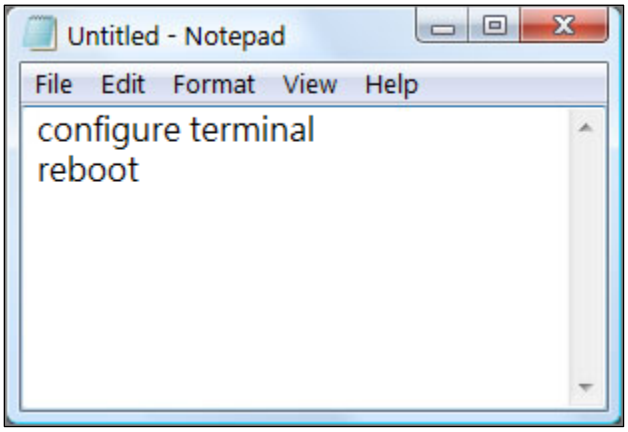


ZyWALL/USG Auto Schedule Reboot Settings

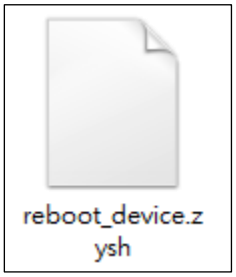
Note: This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the Shell Script

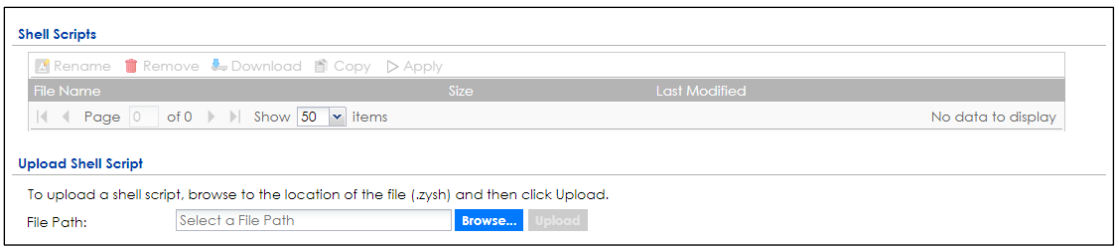
1 Run Windows Notepad application and input below command:



2 Save this file as "reboot_device.zysh"

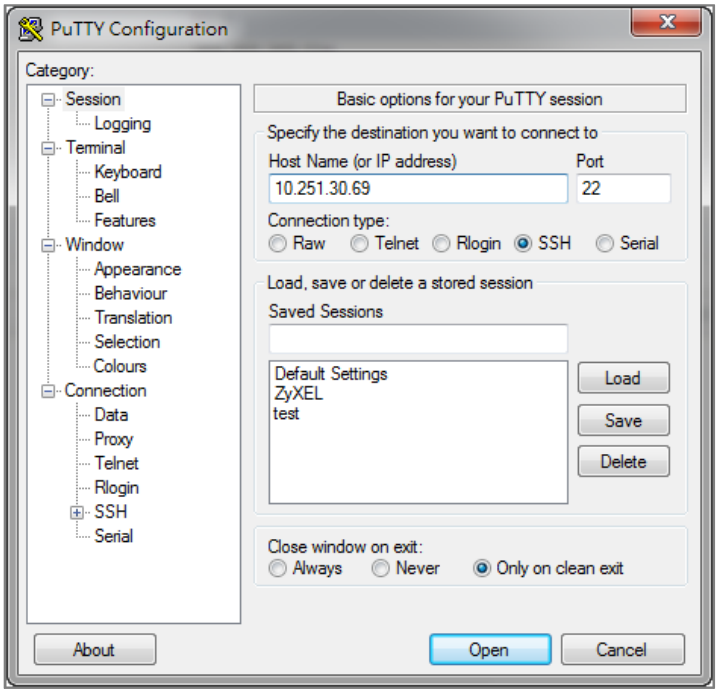


3 In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Shell Script**. Click **Browse**... to find the reboot_device.zysh file. Click **Upload** to begin the upload process.



Set Up the Schedule Run

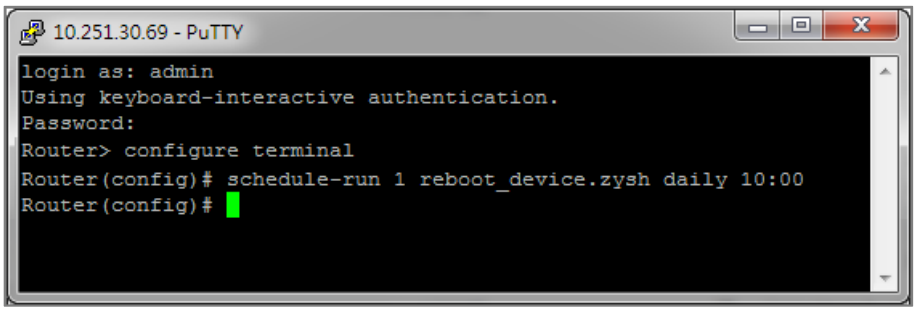
1 Login the device via console/telnet/SSH (using PuTTY in this example)



2 Issuing below commands based on three different (daily, weekly and monthly) user scenarios:

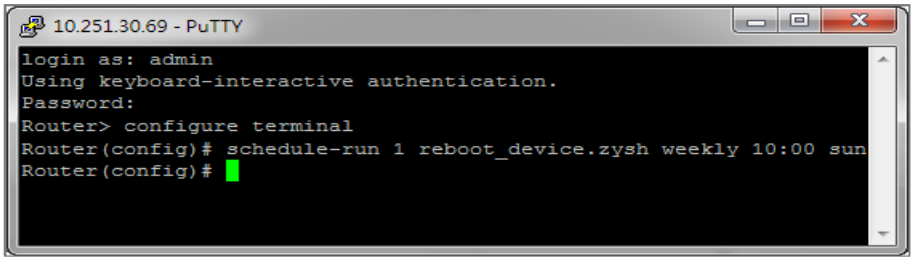
a. Router(config)# schedule-run 1 reboot_device.zysh daily 10:00

(The device will reboot at 10:00 everyday)



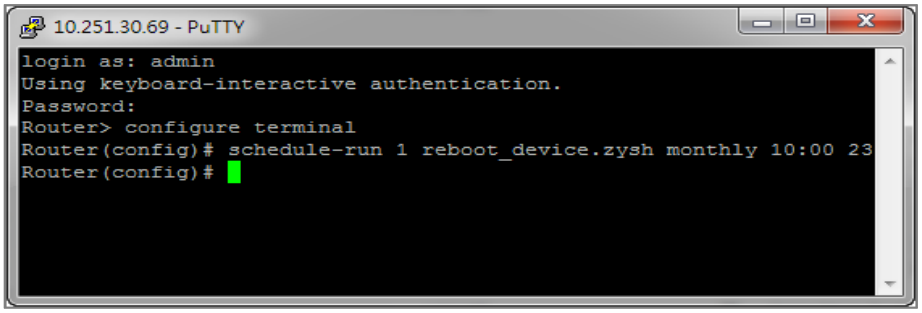
b. Router(config)# schedule-run 1 reboot_device.zysh weekly 10:00 sun

(The device will reboot at 10:00 every Sunday)



c. Router(config)# schedule-run 1 reboot_device.zysh monthly 10:00 23

(The device will reboot at 10:00 every month on 23th)

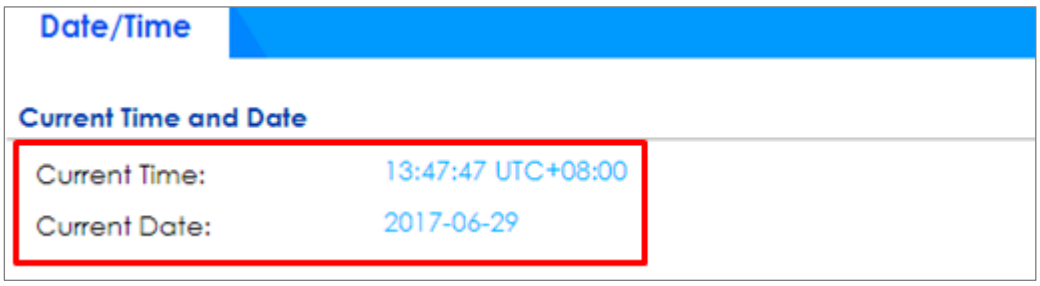


Check the Reboot Status

3 Login the device via console/telnet/SSH, the reboot runs as scheduled

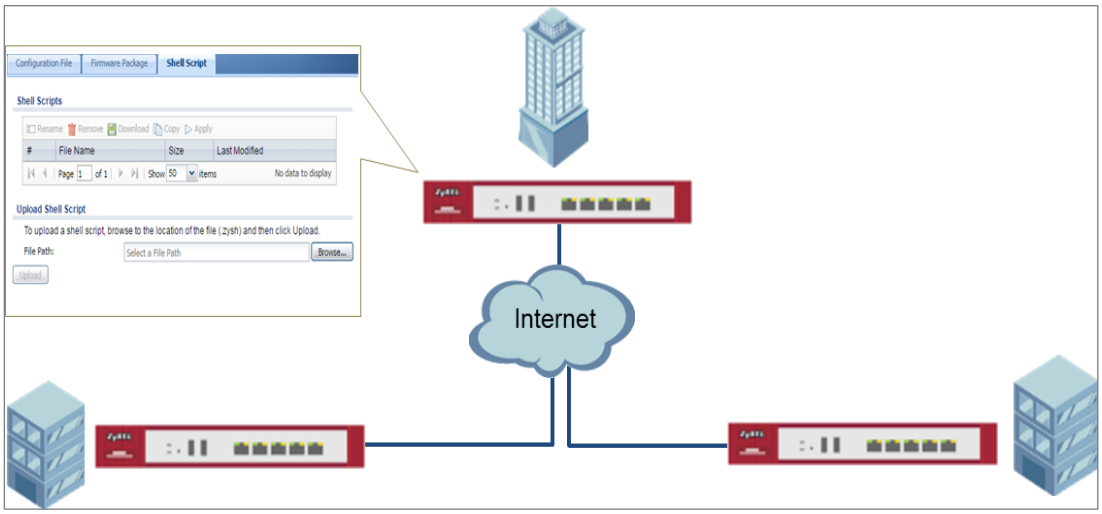
4 Go to **Configuration > System> Date/Time**, check **Current Date/Time**.

Figure Configuration > System >Date/Time



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.

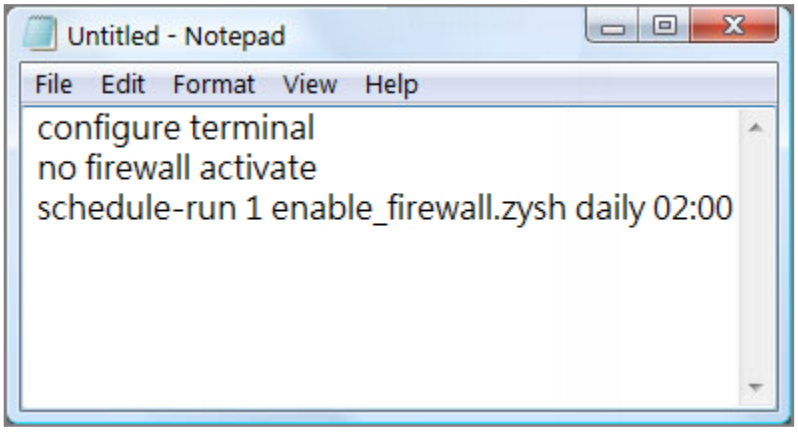


ZyWALL/USG continuously run a ZySH script Settings

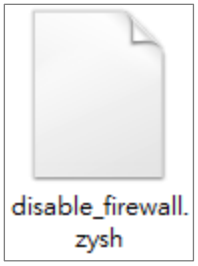
Note: This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the Shell Script

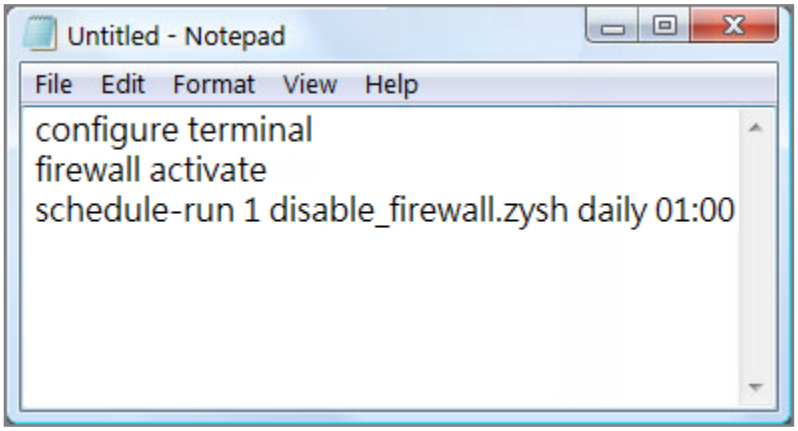
1 Run Windows Notepad application and input below command:



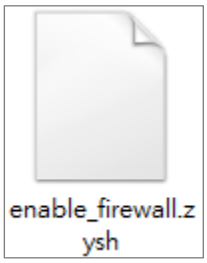
2 Save this file as "disable_firewall.zysh"



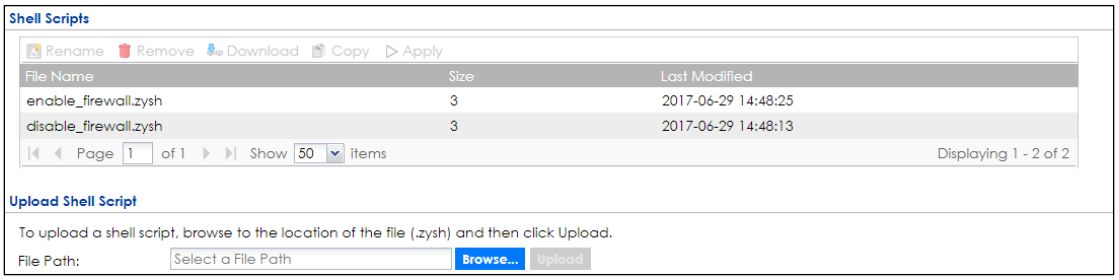
3 Run Windows Notepad application and input below command:



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.

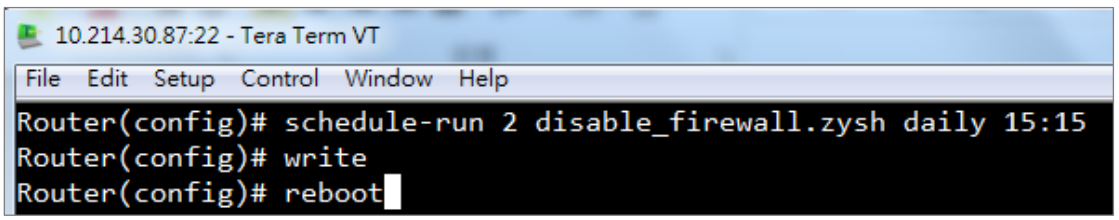


Set Up the Schedule Run

6 Issuing below commands:

Router> configure terminal

Router(config)# schedule-run 1 disable_firewall.zysh daily 15:15



Check the Result

1 In the ZyWALL/USG, go to **DASHBOARD**.

DASHBOARD

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.

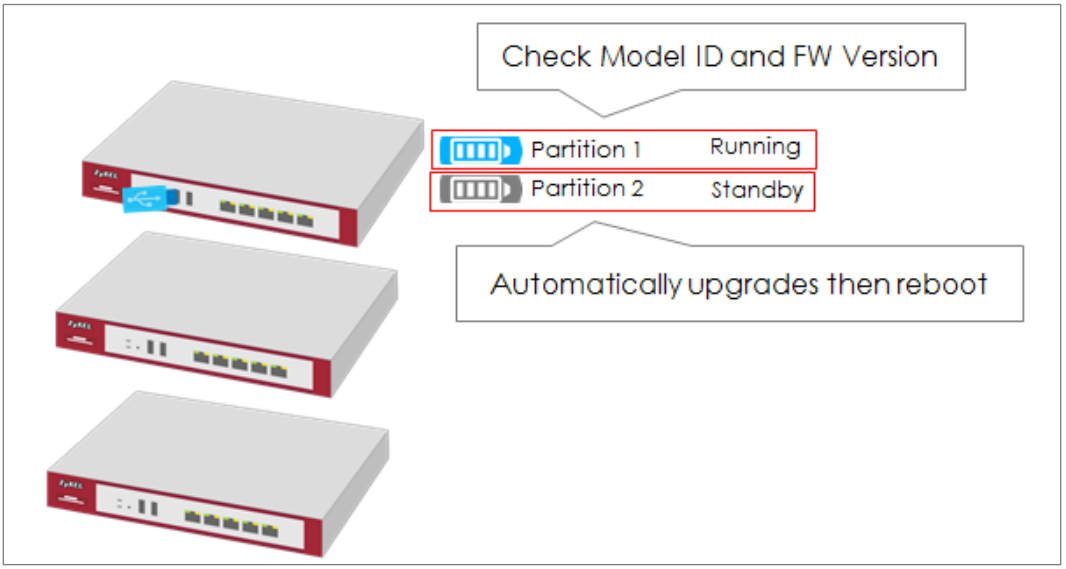


Figure 1 Automatic USB Firmware Upgrade

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:

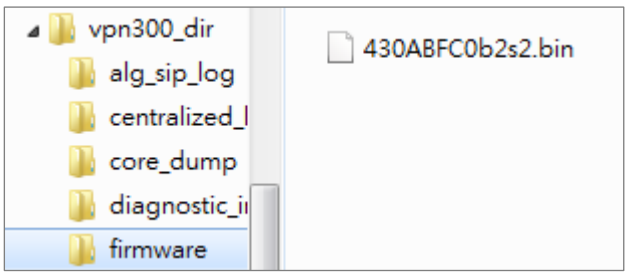
Router(config)# usb-storage update-firmware enable

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

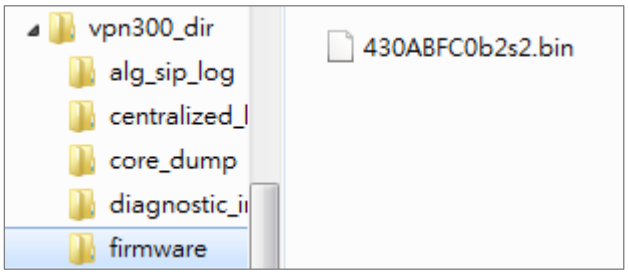
core_dump

diagnostic_info

firmware

packet_trace

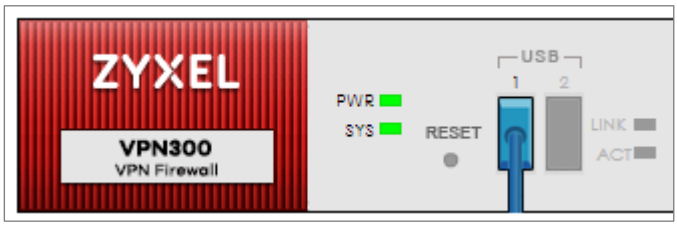
Firmware Folder is Created Automatically



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.

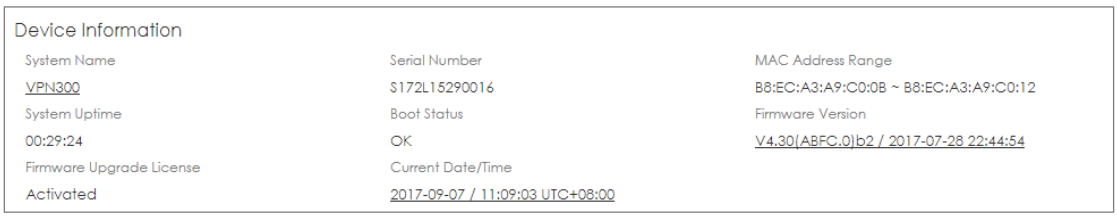
Check Model ID and Firmware Version

```
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!!
```

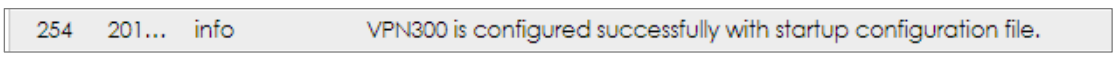
Check Firmware Status

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



MONITOR > Log > View log



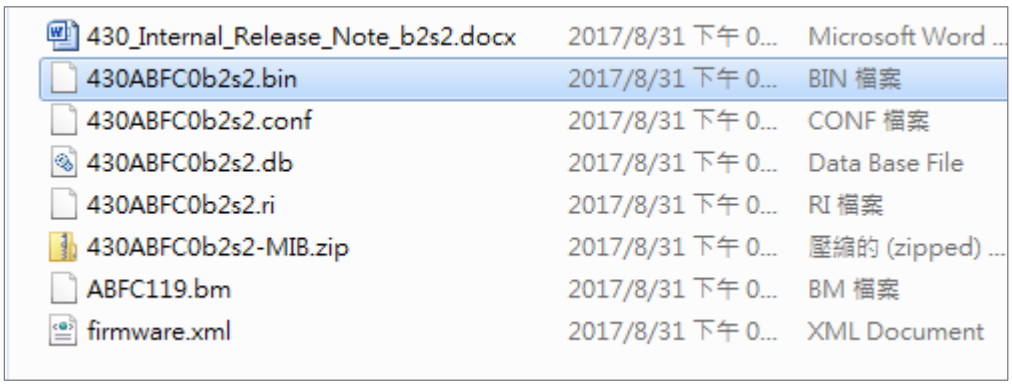
What Can Go Wrong?

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.



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

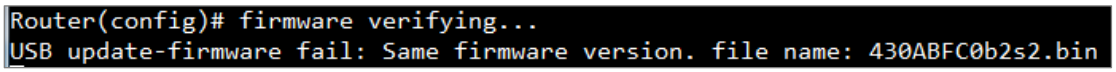
```
Router(config)# firmware verifying...
Product model id is not compatible!!
This product's model id is E134
The ZLD-current image supports the following product model id :
E10B
USB update-firmware fail: File damaged. file name: 430AALA0a1.bin
```

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...

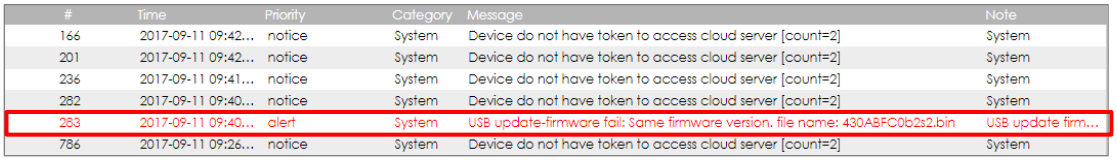
5 Make sure the version of the USB firmware is different from that of the running partition. The device writes logs on the console and device log if the firmware version is the same as the running firmware.

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

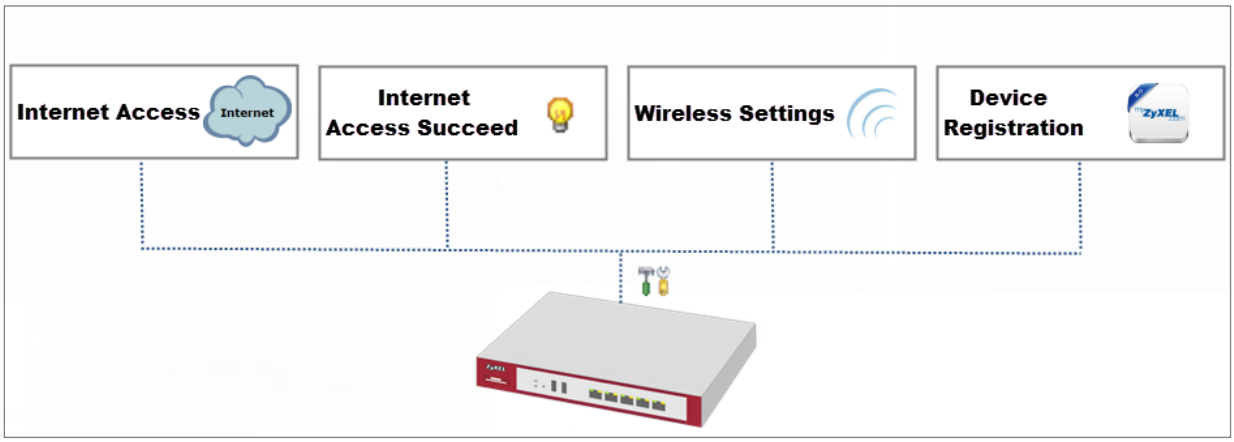
6 This feature does not support the Device HA Pro firmware auto upgrade to passive devices. Do not use USB firmware upgrade on devices with Device HA Pro function activated. When using USB firmware upgrade on a device HA or in a device HA Pro scenario, make sure you plug the USB storage to the passive 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



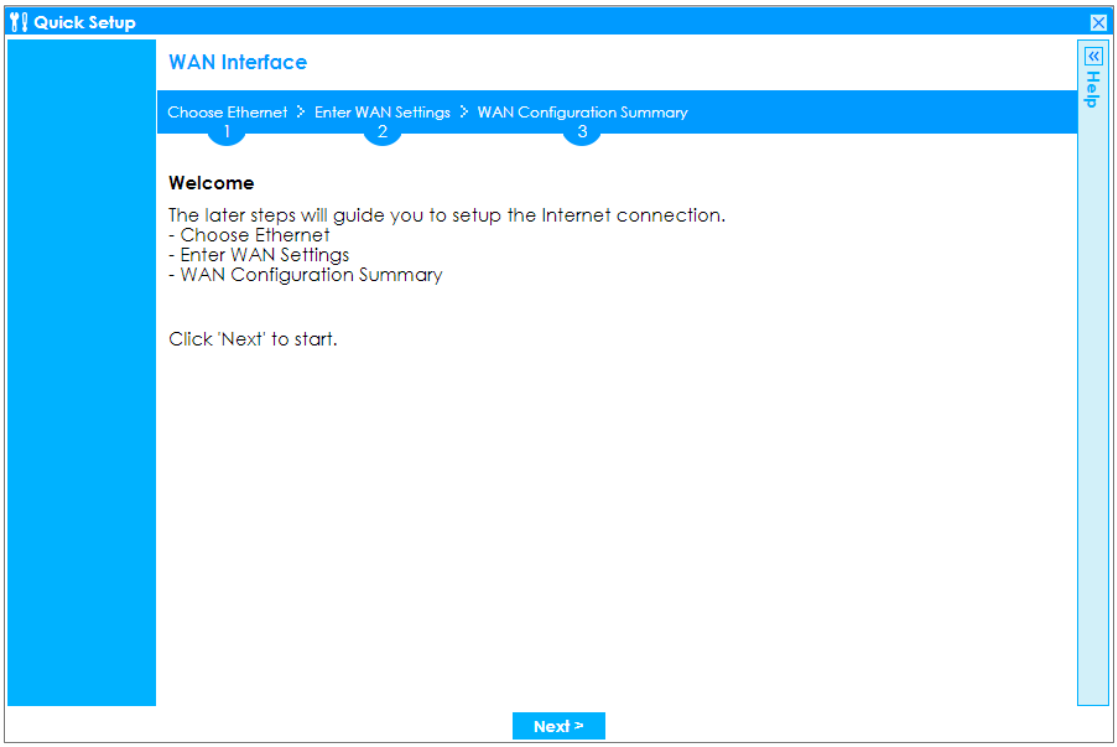
Note: You need internet access to activate your ZyWALL/USG subscription services. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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

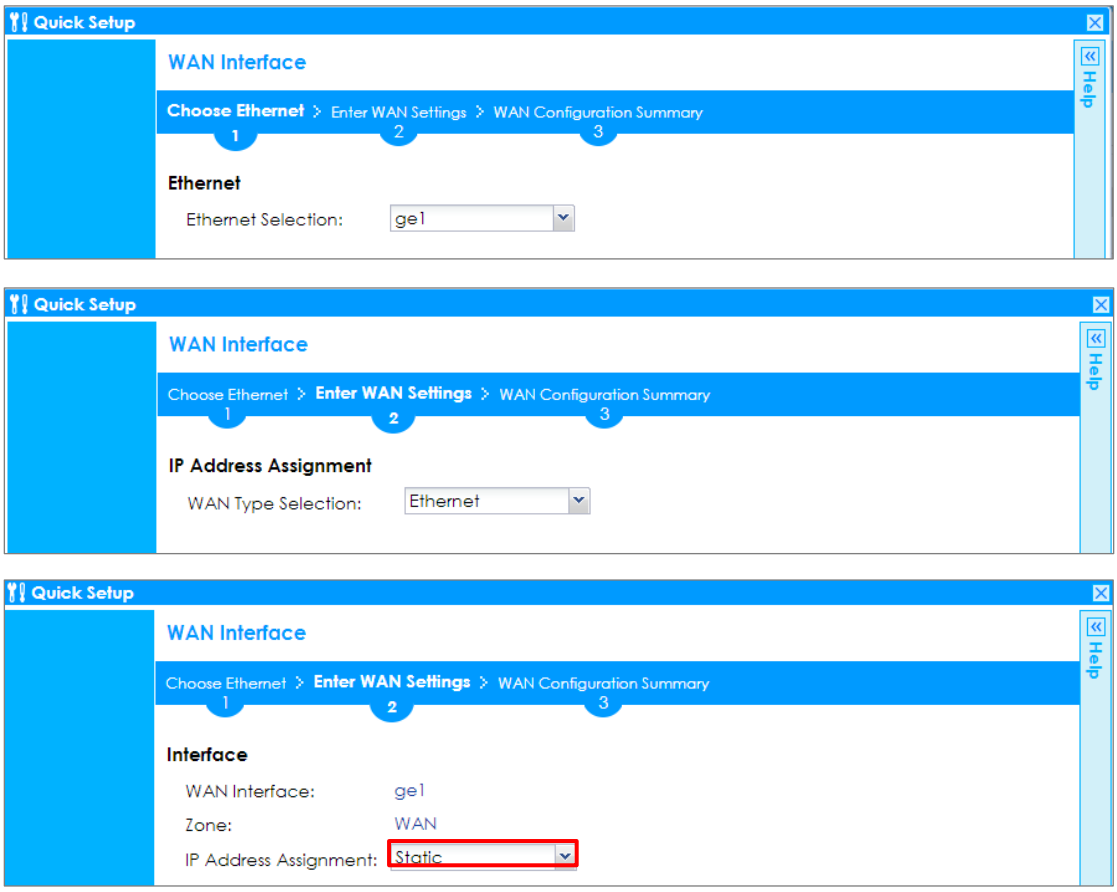


In the **Internet Access** page, you can configure Internet connections from two Internet service providers (ISPs). Connect your ISP devices to your ZyWALL/USG WAN port, select **I have two ISPs** if you want to configure two Internet connections or leave it cleared to configure just one.

Choose the **Encapsulation** option to be **Ethernet**, leave **Zone** as default setting Internet connection belongs to the WAN zone.

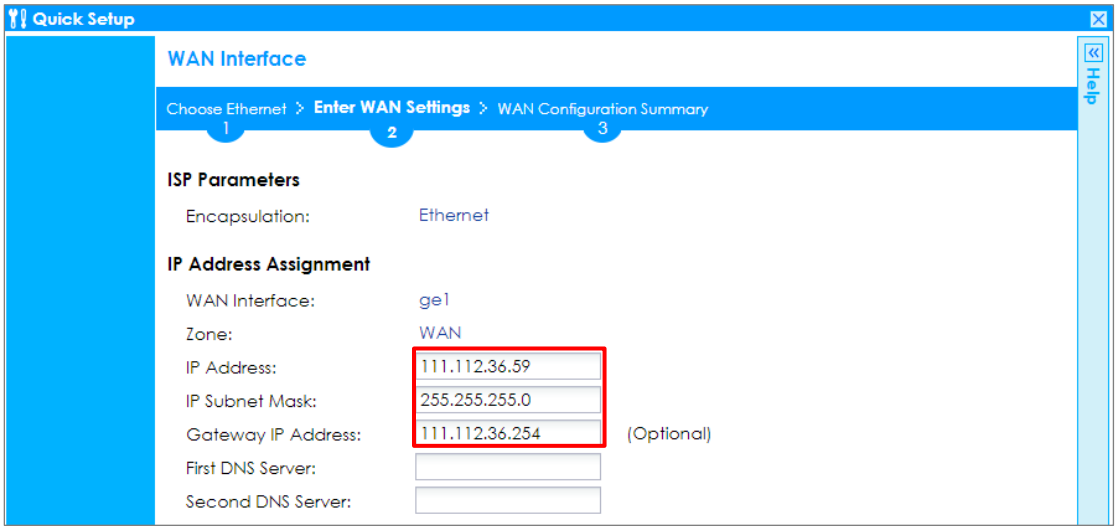
In the **IP Address Assignment** section, select **Auto** if your ISP did not assign you a fixed IP address or select **Static** if your ISP did assign you a fixed IP address. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access



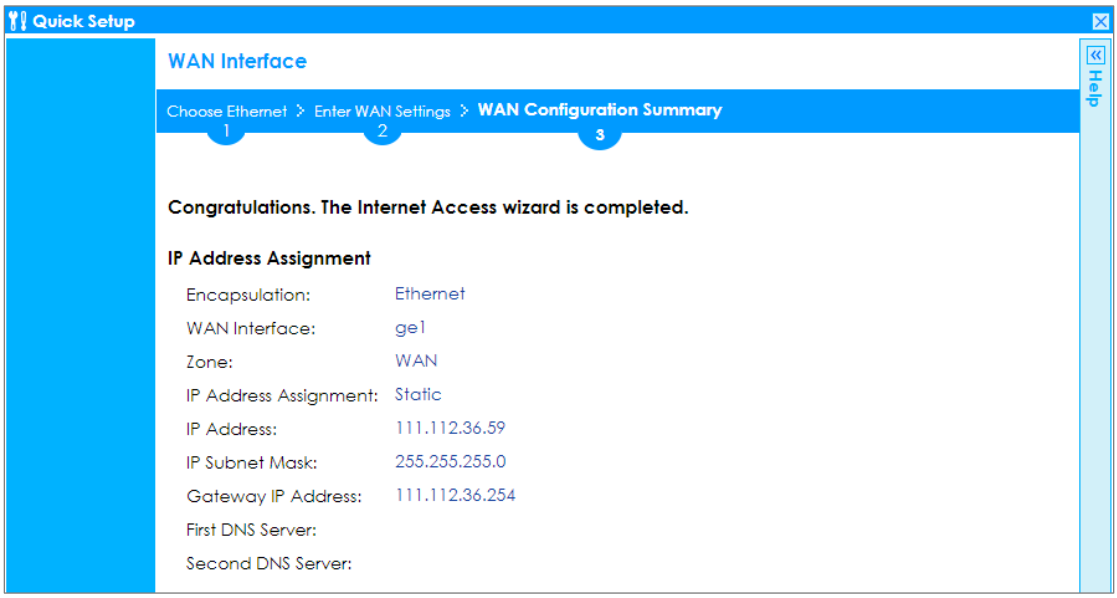
Enter the **IP Address**, **IP Subnet Mask** and **Gateway IP Address** exactly as given by your ISP or network administrator. First/Second DNS Servers are optional. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access



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.

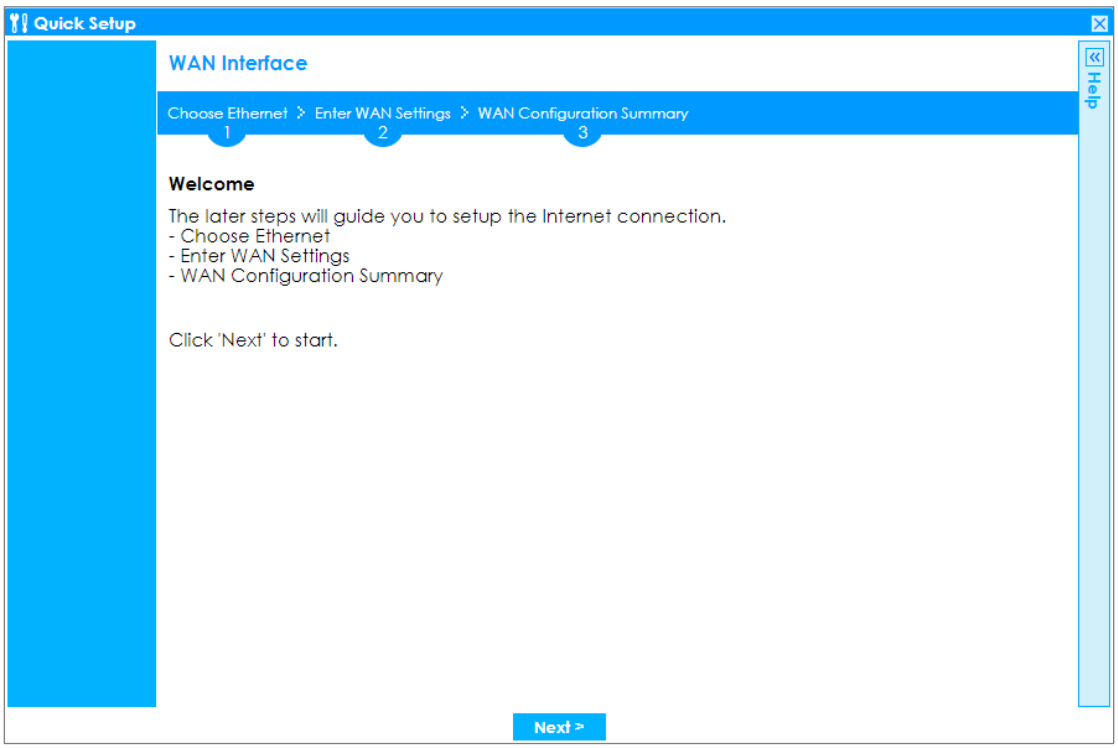
Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed



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.

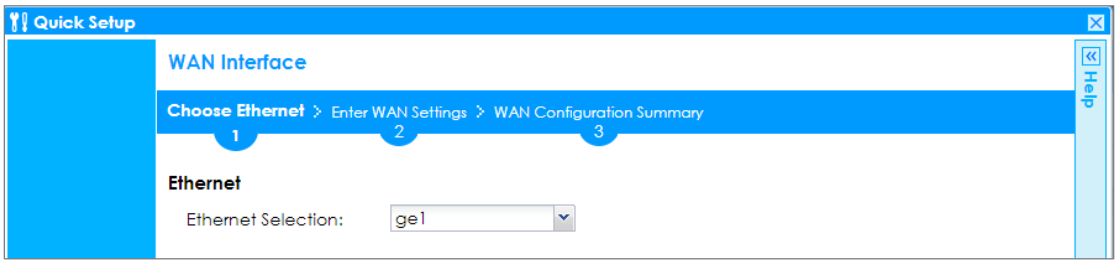
Installation Setup Wizard > Welcome

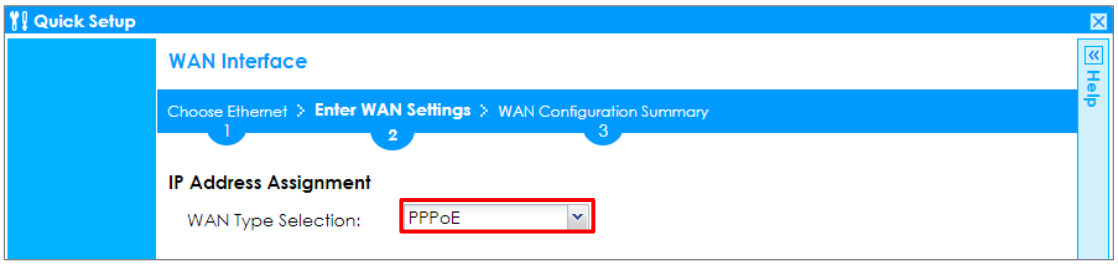


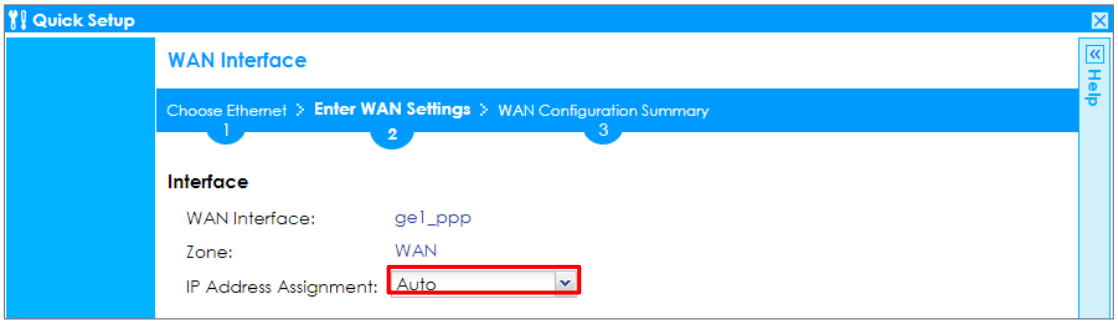
In the **Internet Access** page, you can configure Internet connections from two Internet service providers (ISPs). Connect your ISP devices to your ZyWALL/USG WAN port, select **I have two ISPs** if you want to configure two Internet connections or leave it cleared to configure just one.

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

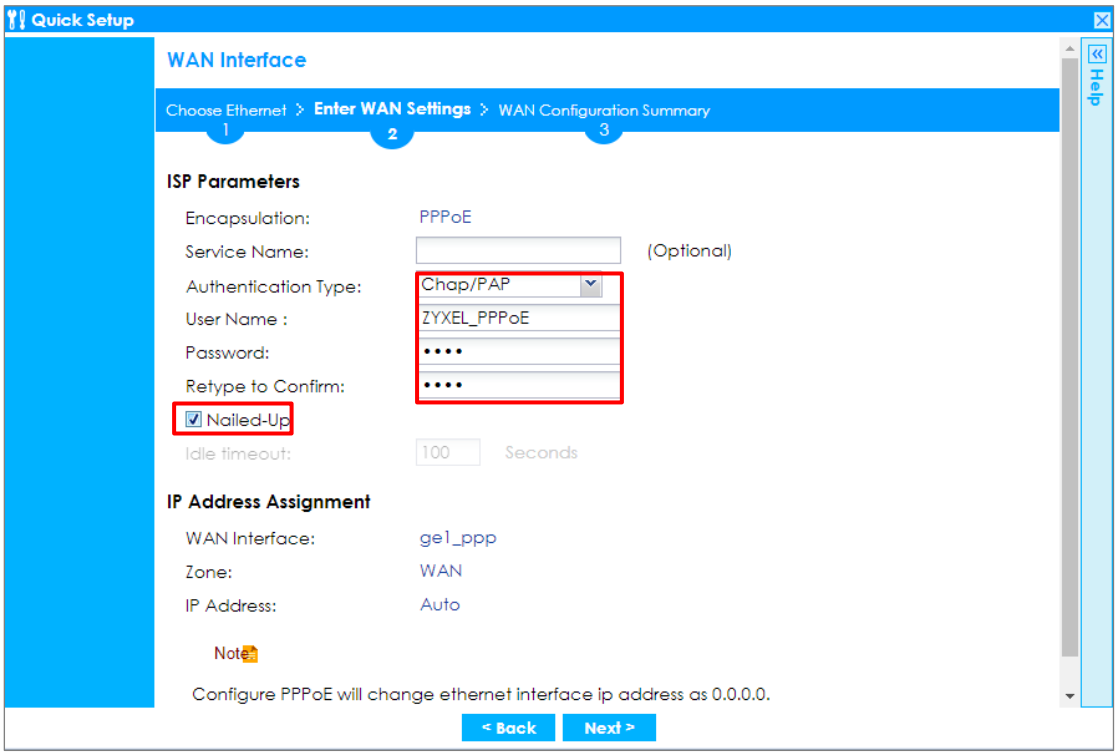






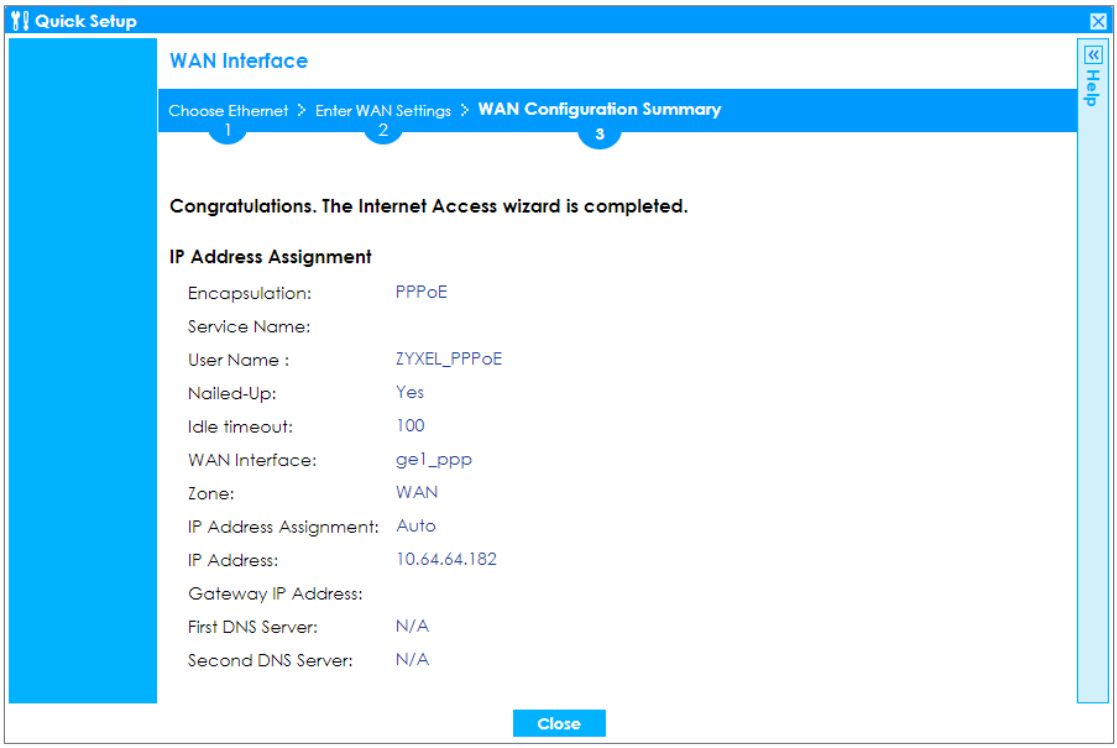
Select the **Authentication Type** to be the authentication method by the remote node. Enter the **User Name** and **Password** exactly as given by your ISP or network administrator. Select **Nailed-UP** if you want to keep the connection always up or type the desired **Idle Timeout** value in seconds. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access



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.

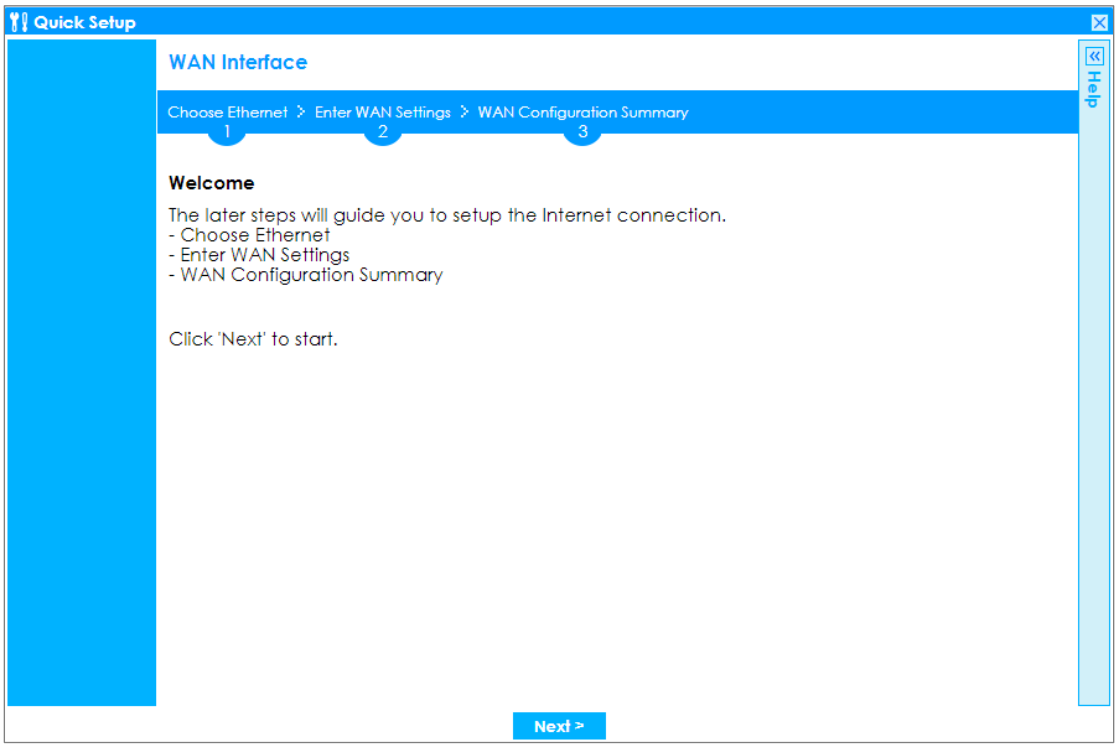
Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed



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.

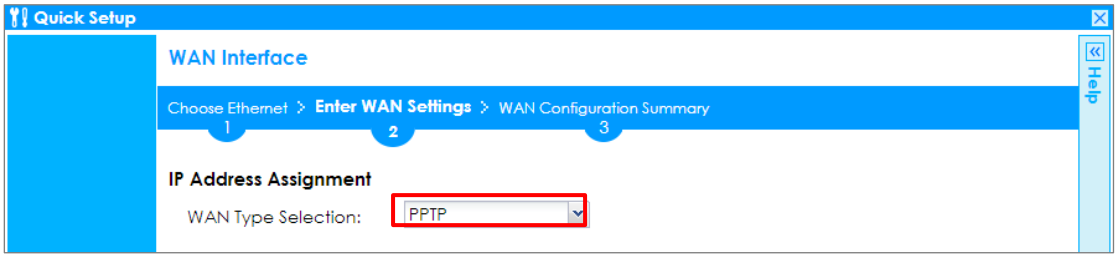
Installation Setup Wizard > Welcome

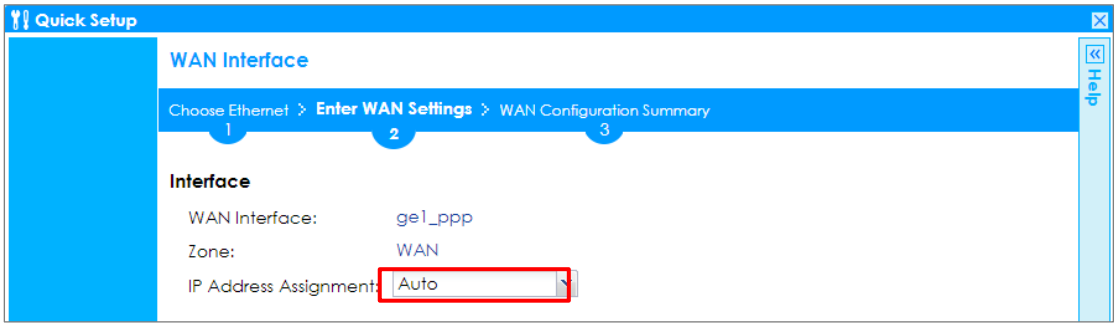


In the **Internet Access** page, you can configure Internet connections from two Internet service providers (ISPs). Connect your ISP devices to your ZyWALL/USG WAN port, select **I have two ISPs** if you want to configure two Internet connections or leave it cleared to configure just one.

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

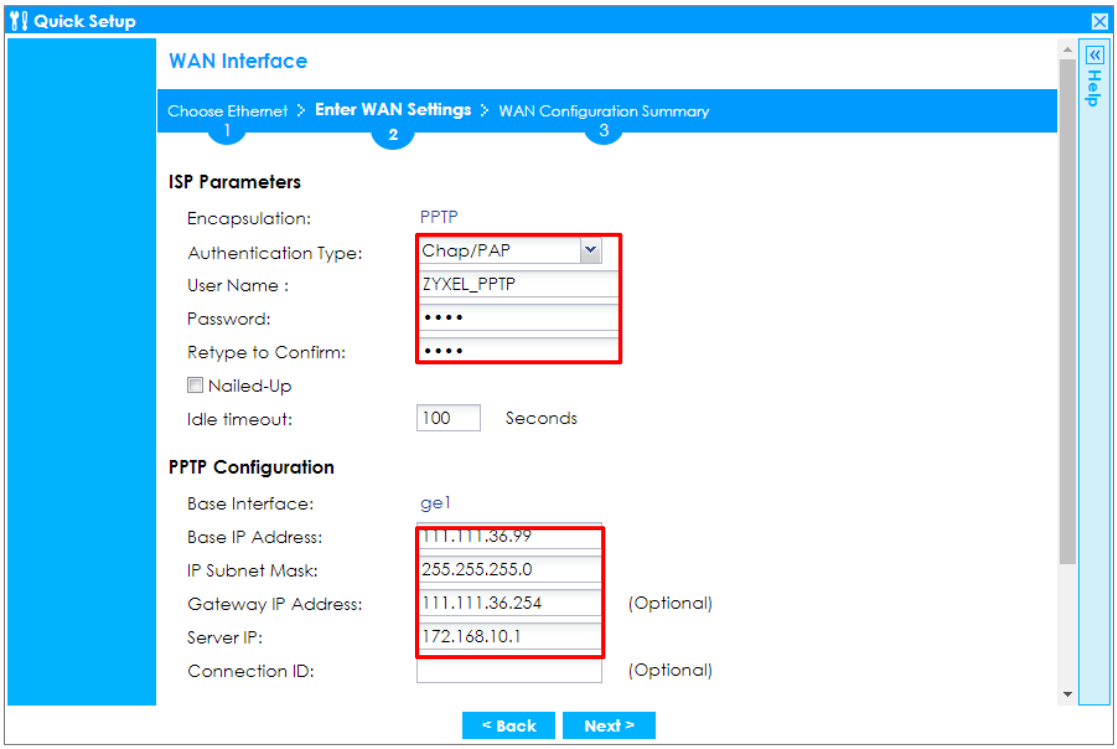




Select the **Authentication Type** to be the authentication method by the remote node. Enter the **User Name** and **Password** exactly as given by your ISP or network administrator. Select **Nailed-UP** if you want to keep the connection always up or type the desired **Idle Timeout** value in seconds. Click **Next**.

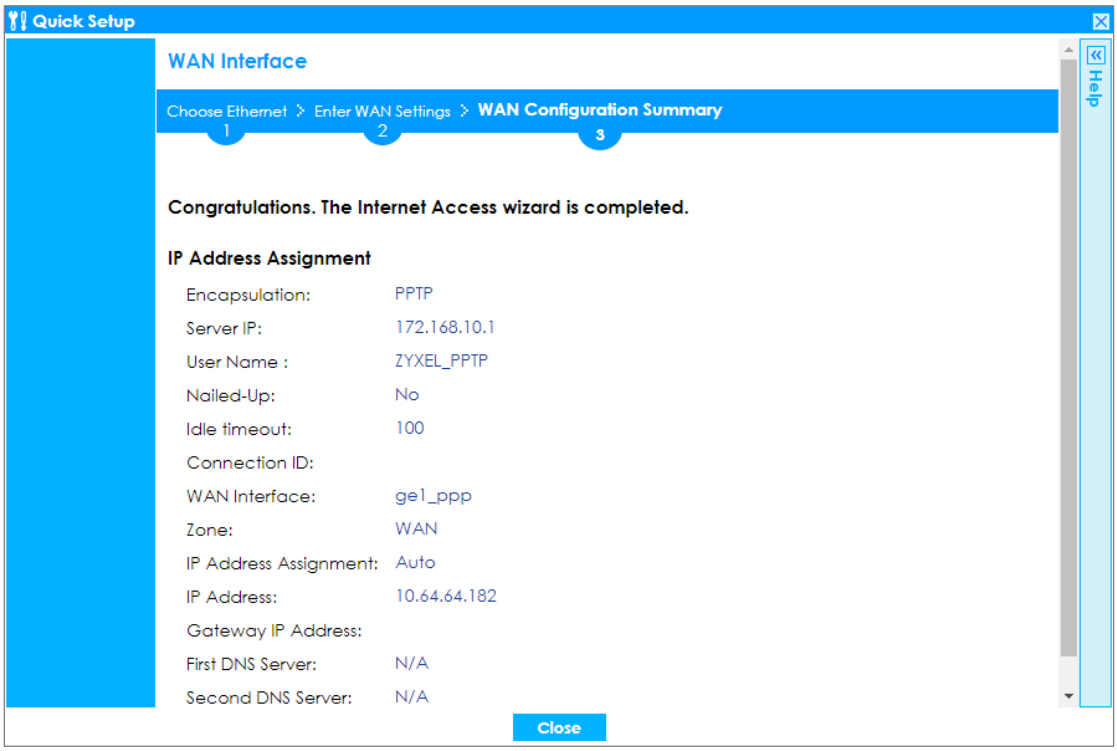
Enter the **Base IP Address**, **IP Subnet Mask**, **Gateway IP Address** assigned to you by your ISP. Type the **Server IP** address of the **PPTP Server**. Click **Next.**

Installation Setup Wizard > Welcome > Internet Access



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.

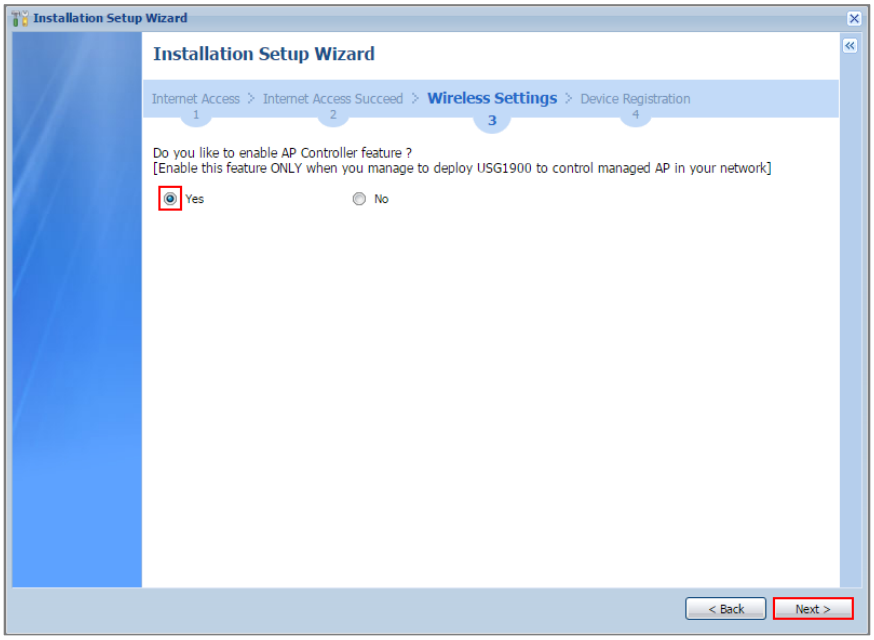
Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed



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



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.

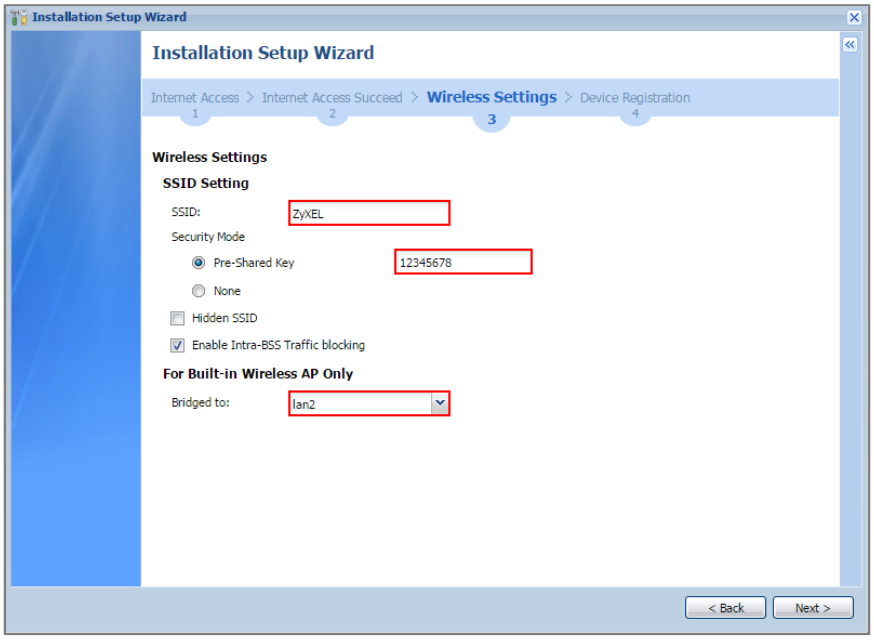
Select **Hidden SSID** to hide the SSID from site tool scanning.

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

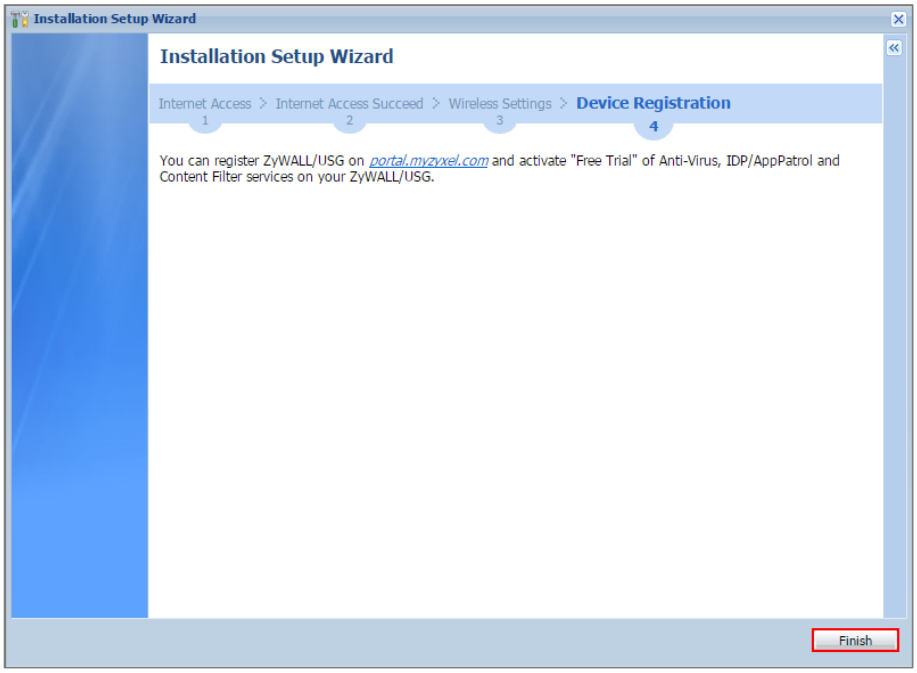


Set Up the Device Registration on the ZyWALL/USG

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 > Internet Access Succeed > Wireless Settings > Device Registration
1
2
3
4
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.
Finish

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.

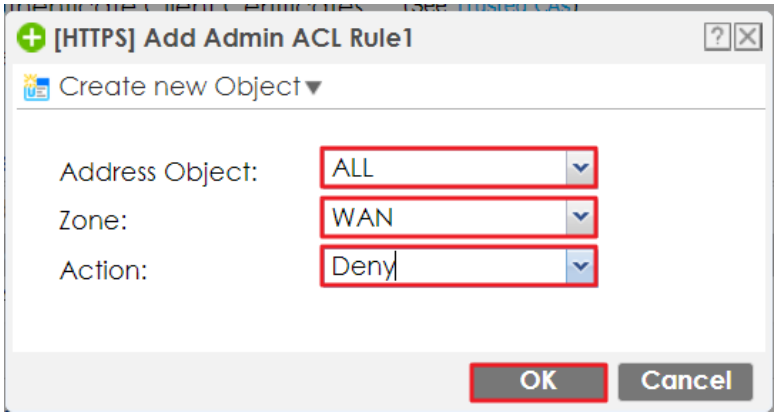
ZyWALL/USG Restrict Web Portal Access from the Internet

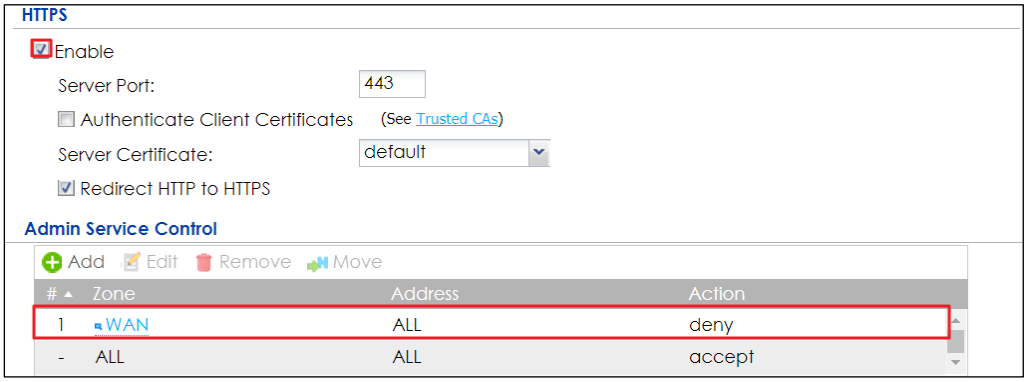
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG60 (Firmware Version: ZLD 4.25).

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

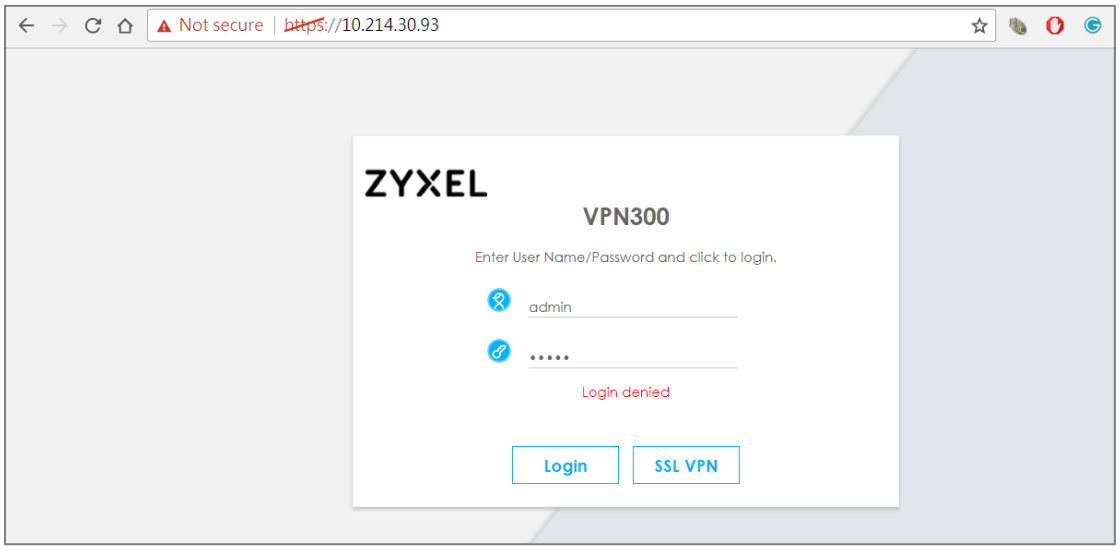




Test the Web Access

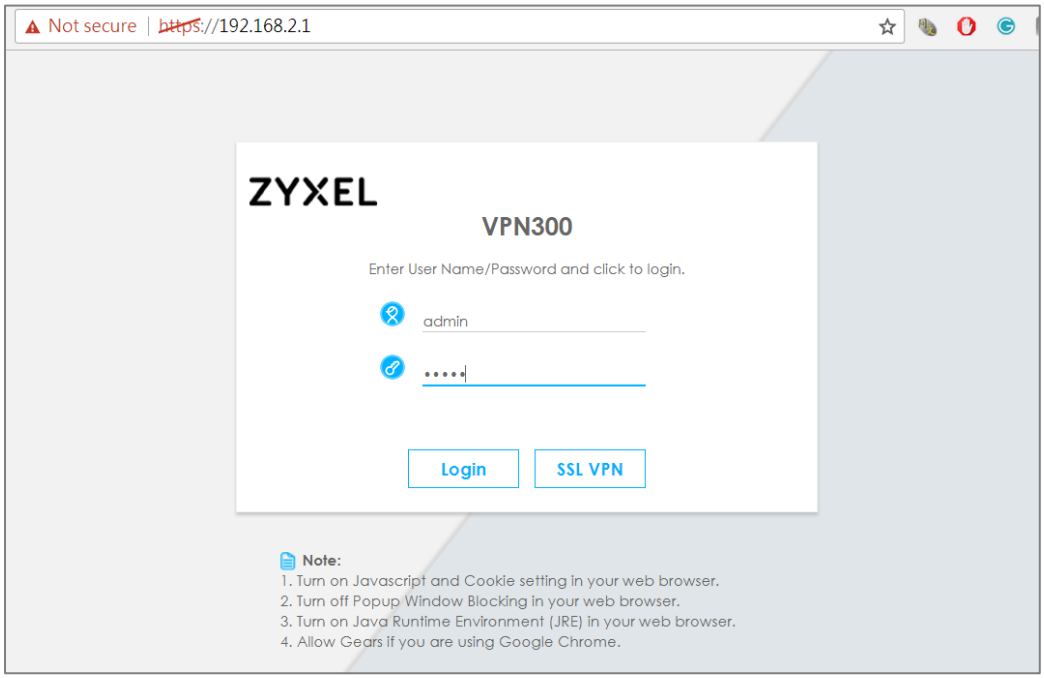
Login to the device via the WAN interface with the administrator's user name and password. The screen will show **Login denied**.

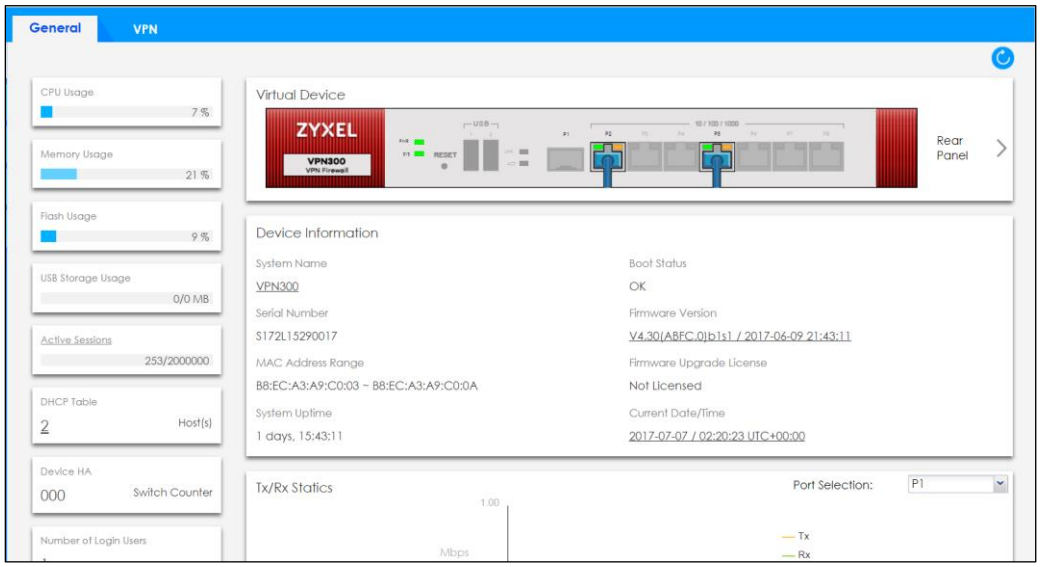
Login to the device via the WAN interface



Login to the device via the LAN interface with the administrator's user name and password. The management portal will be displayed.

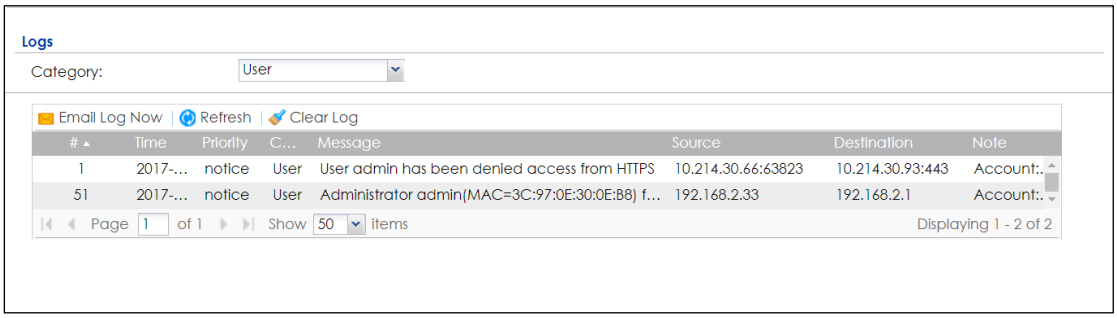
Login to the device via the LAN interface





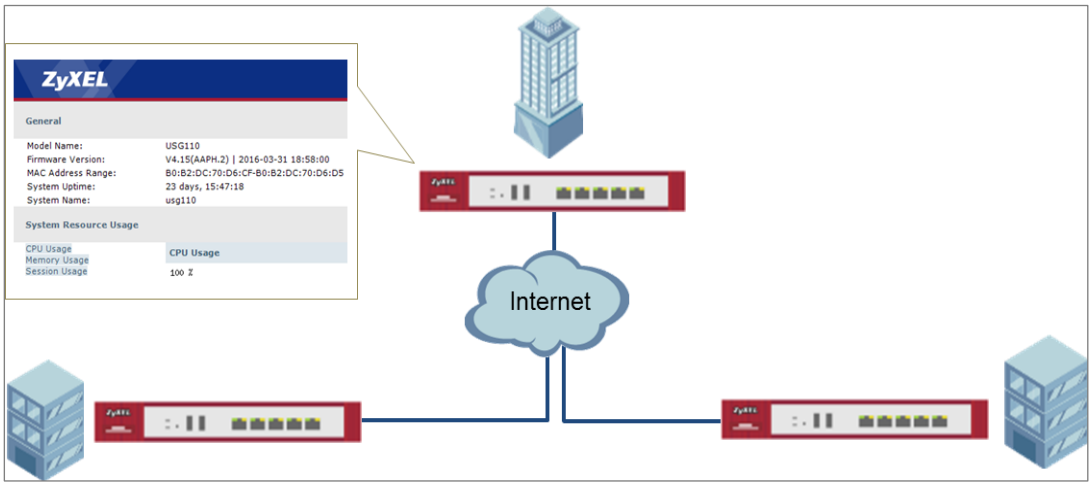
Go to **MONITOR > Log**. You can see that the admin login has been denied access from the WAN interface but it is allowed from the LAN interface.

MONITOR > Log


Logs
Category:
User
Email Log Now
Refresh
Clear Log
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.



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).

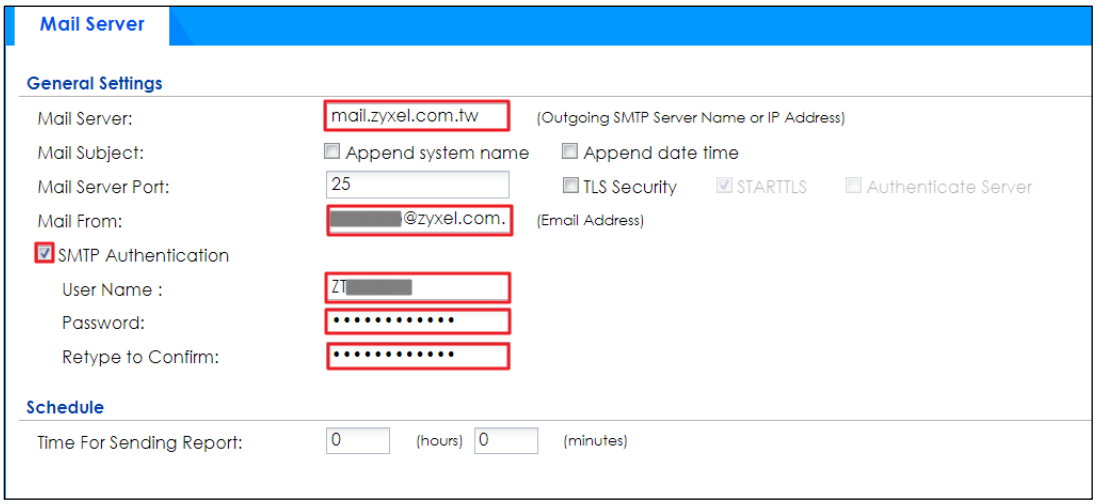
Set Up the ZyWALL/USG Email Daily Report Setting

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

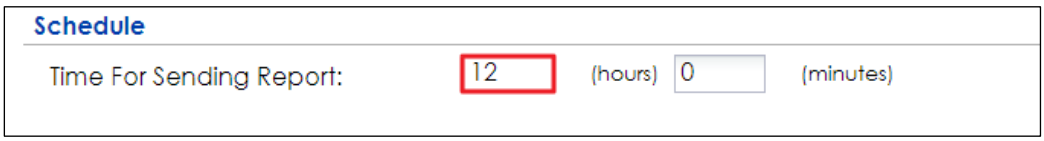
Type the SMTP server name or IP address. In **Mail From**, type the e-mail address from which the outgoing e-mail is delivered. In **Mail To**, type the e-mail address to which the outgoing e-mail is delivered. Select **SMTP Authentication** if it is necessary to provide a user name and password to the SMTP server.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings



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



Select the information to include in the report. Types of information include **System Resource Usage**, **Wireless Report**, **Threat Report**, and **Interface Traffic Statistics**.

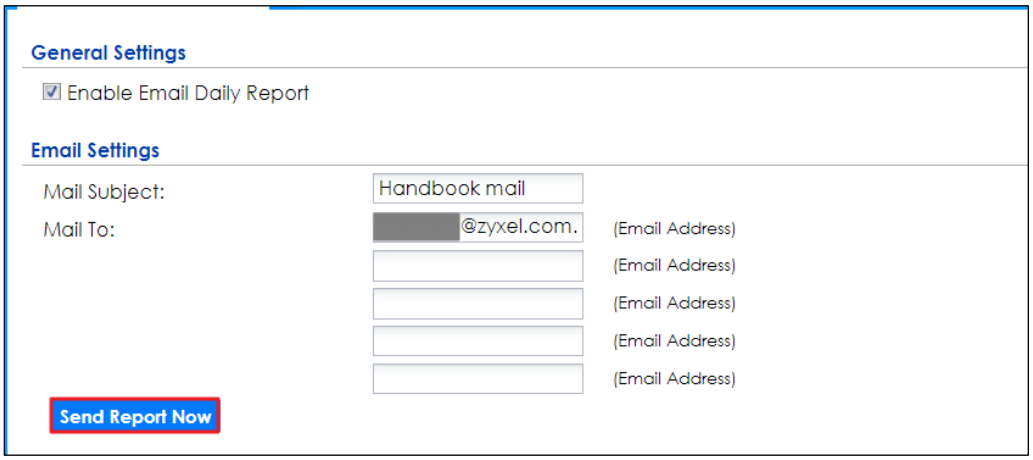
Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period.

CONFIGURATION > Log & Report > Email Daily Report > Report Items

Test the Daily Log Report

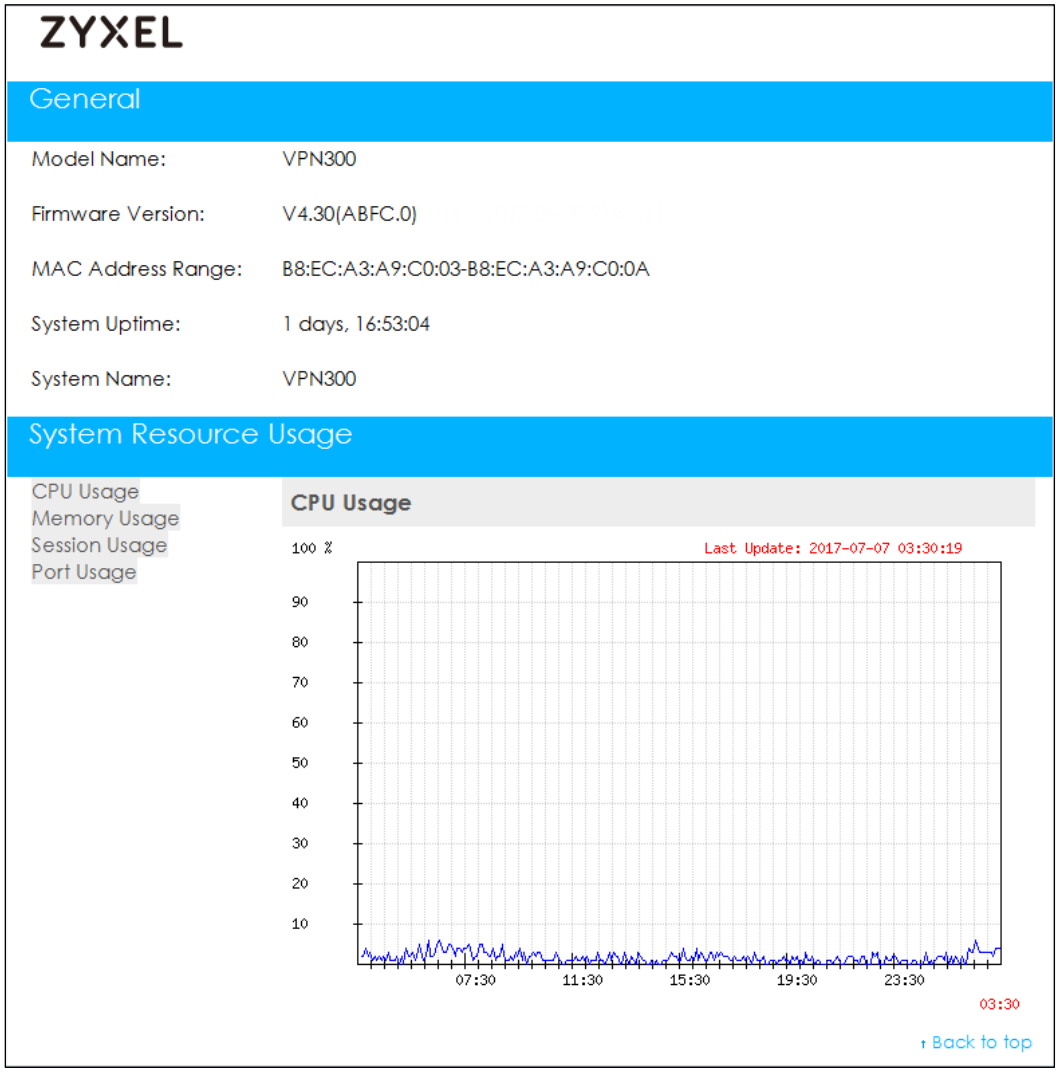
Click **Send Report Now** to have the ZyWALL/USG send the daily e-mail report immediately.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings



You will receive a daily report mail.

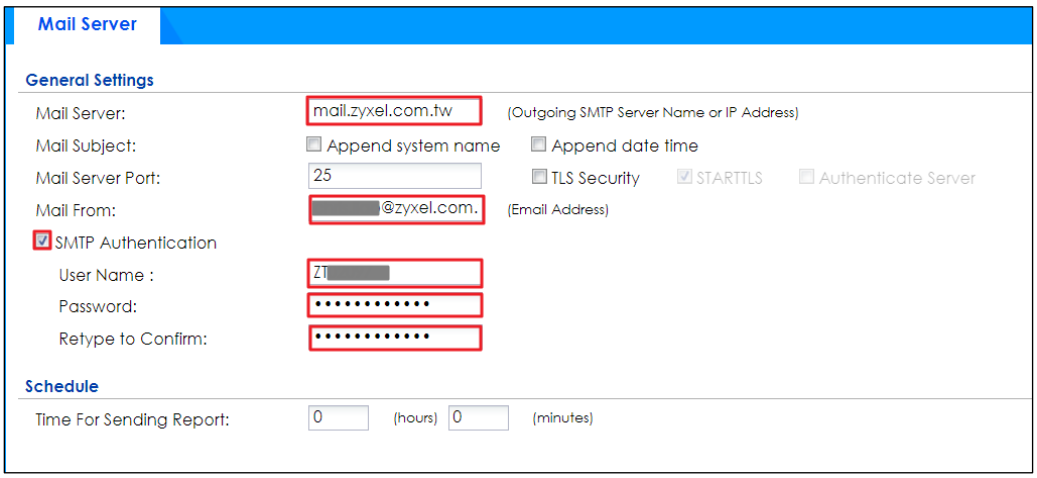
ZyXEL Daily Report Mail



What Could Go Wrong?

Make sure your Email settings are all correct.

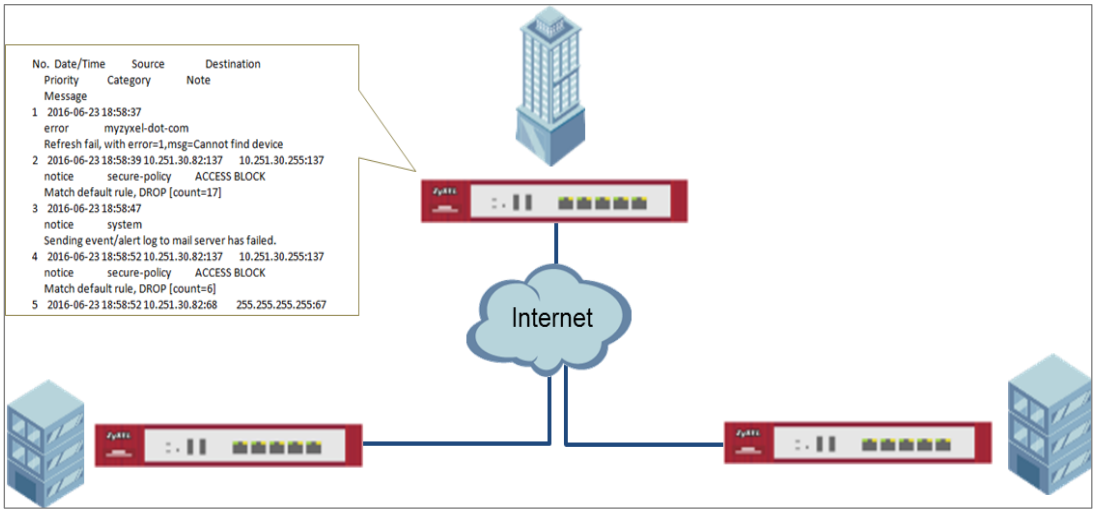
CONFIGURATION > Log & Report > Email Daily Report > Email Settings



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.



ZyWALL/USG Setup and Configure E-mail Logs

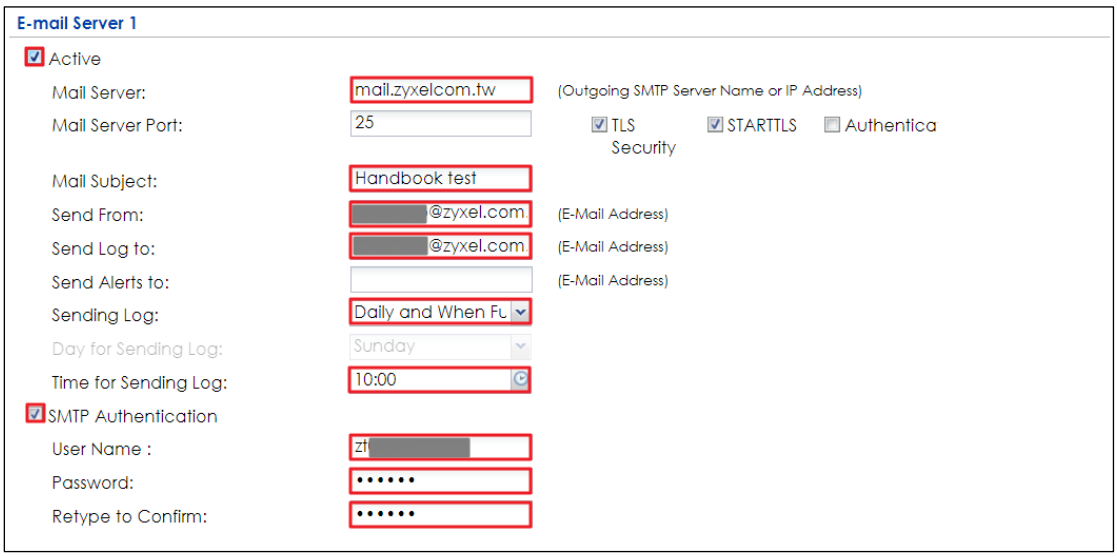
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

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.

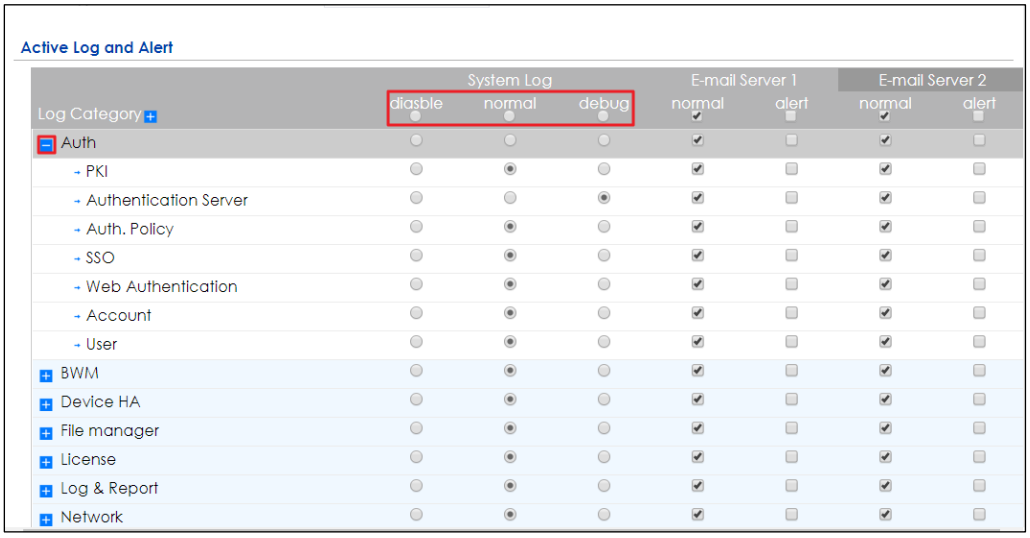
4. Select **SMTP Authentication** if it is necessary to provide a user name and password to the SMTP server.

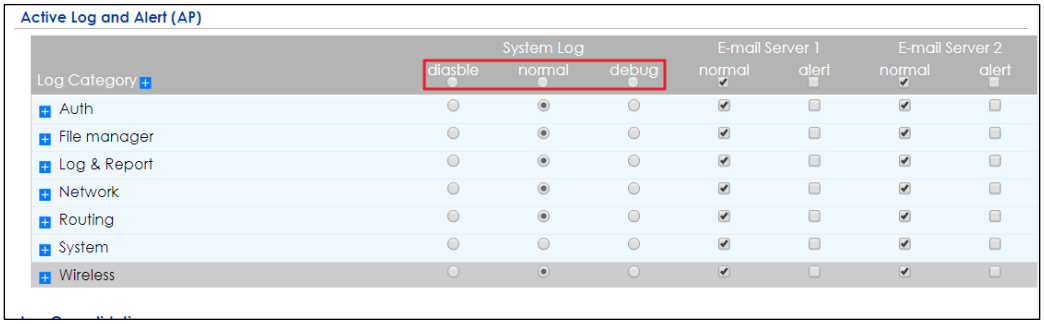
CONFIGURATION > Log & Report > Log Settings > System Log > Edit > E-mail Server 1



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.

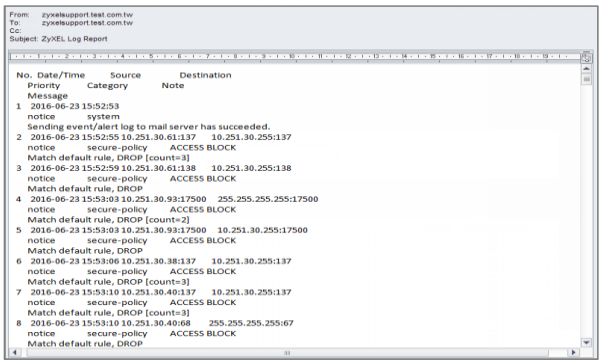




Test the Email Log

You will receive a log mail depends on the time you set in the E-mail Server.

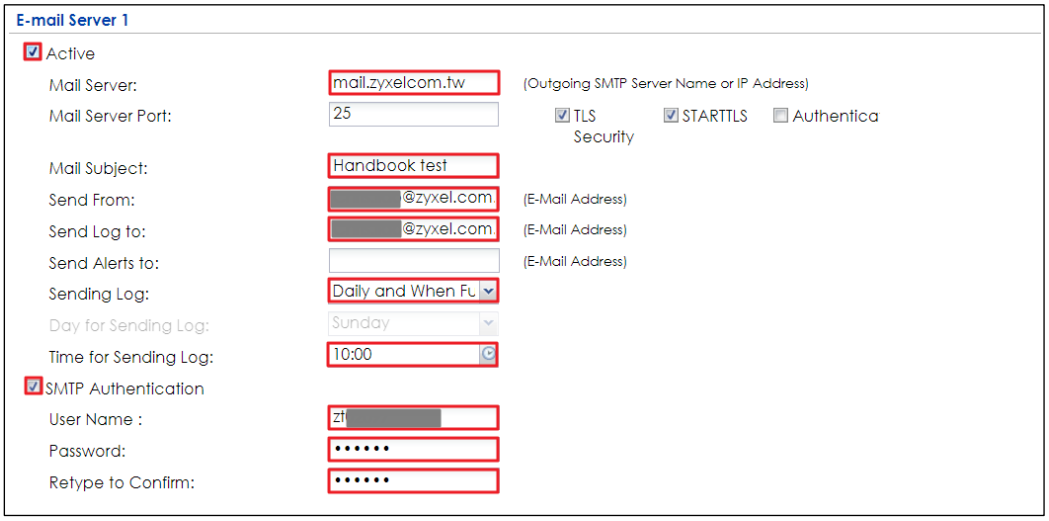
ZyXEL Log Mail



What Could Go Wrong?

Make sure your Email settings are all correct.

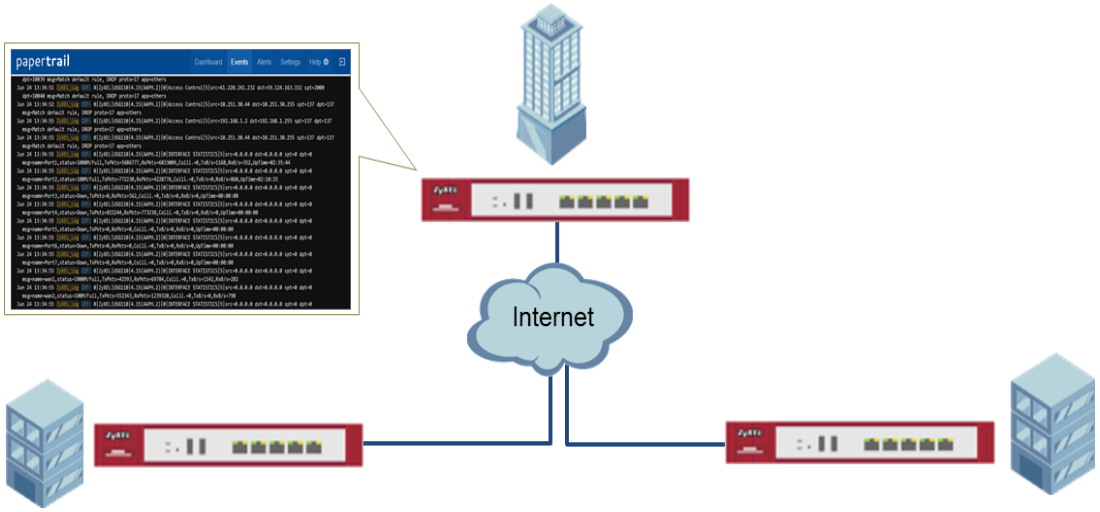
CONFIGURATION > Log & Report > Email Daily Report > Email Settings



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.



ZyWALL/USG Setup and Configure sending logs to a syslog and Vantage Reports Server

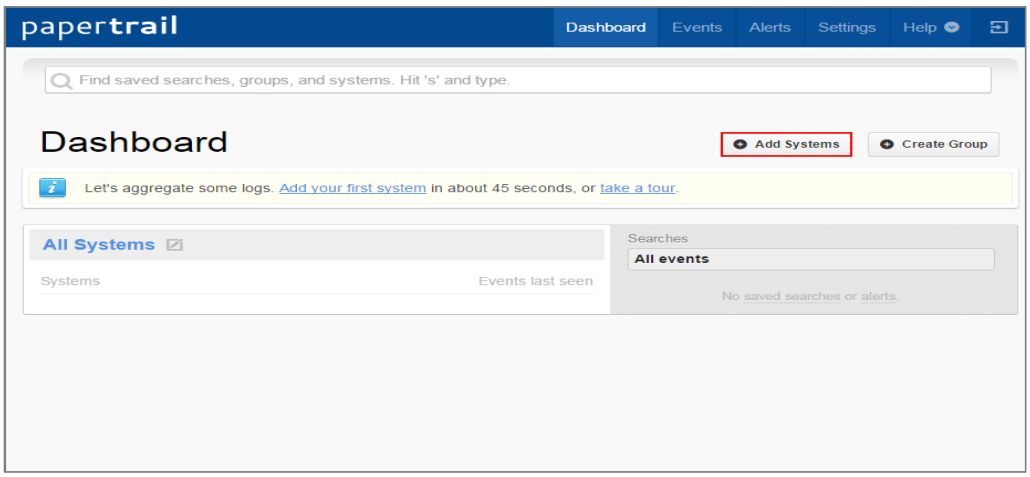
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the Syslog Server (Use Papertrail syslog in this example)

Register an account on Papertrail: https://papertrailapp.com

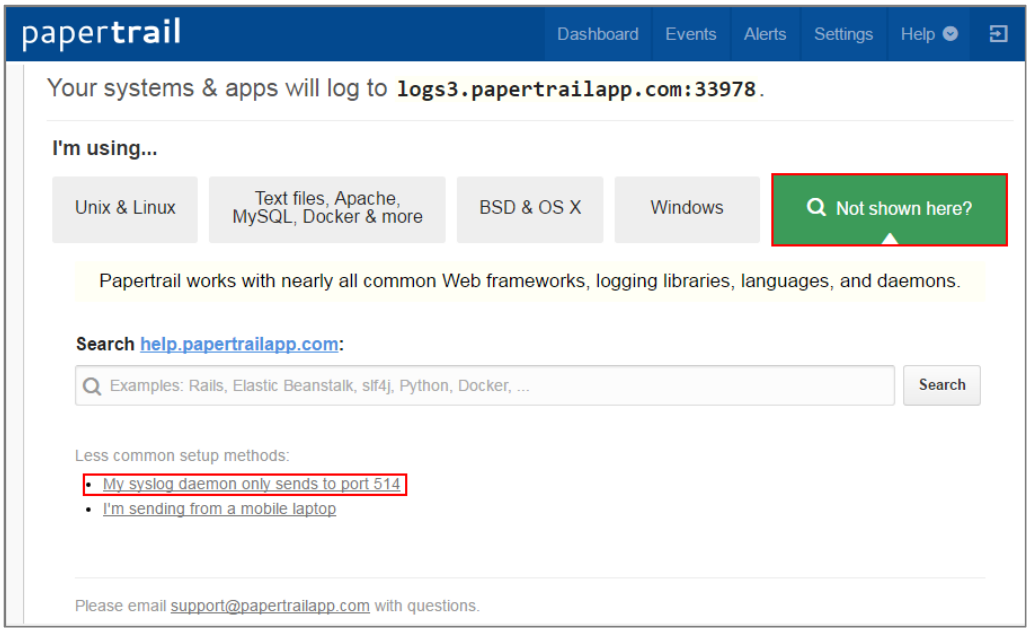
Go to **Dashboard > Add Systems**.

Dashboard > Add Systems



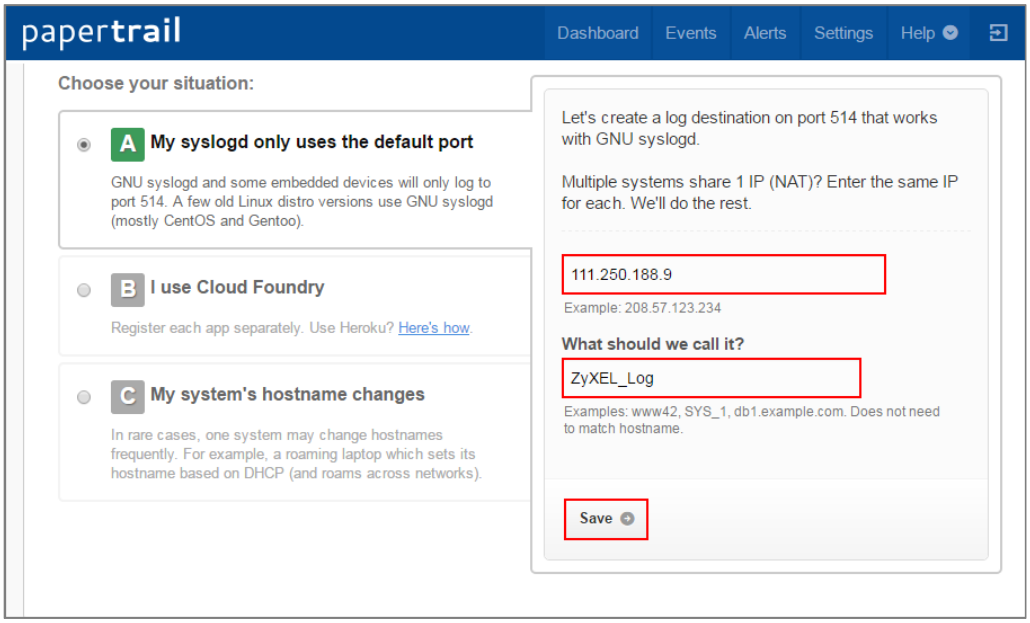
Select **Not shown here?** and **My syslog daemon only sends to port 514**.

Dashboard > Add Systems > I'm using



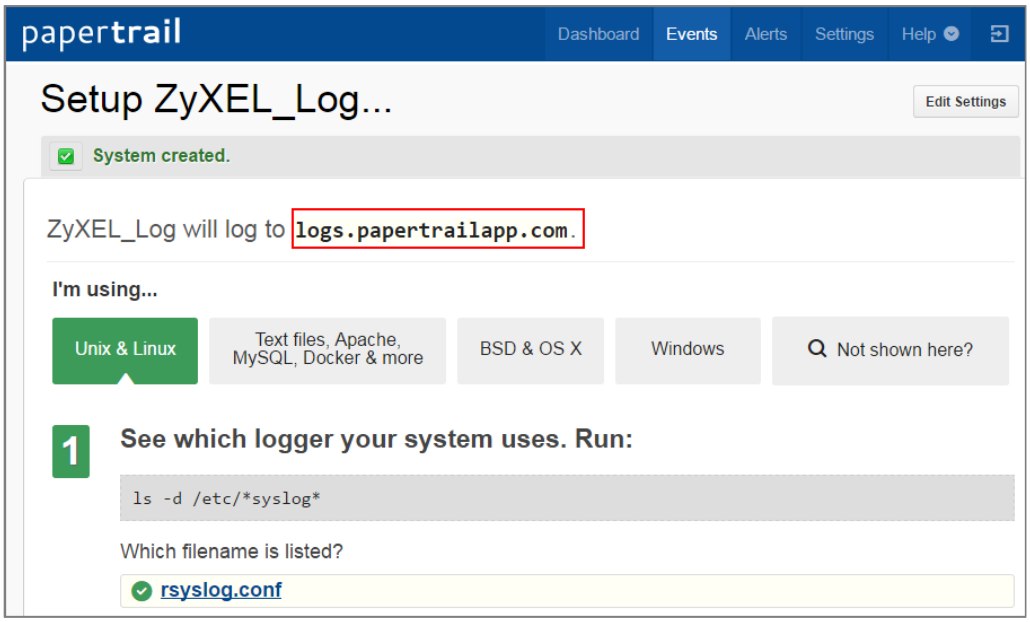
Select **My syslogd only uses the default port**, set ZyWALL/USG public IP address (111.250.188.9 in this example) and name the log system. Click **Save**.

Dashboard > Add Systems > > I'm using > Choose your situation



Write down the Papertrail-provided domain name (logs.papertrialpp.com in this example).

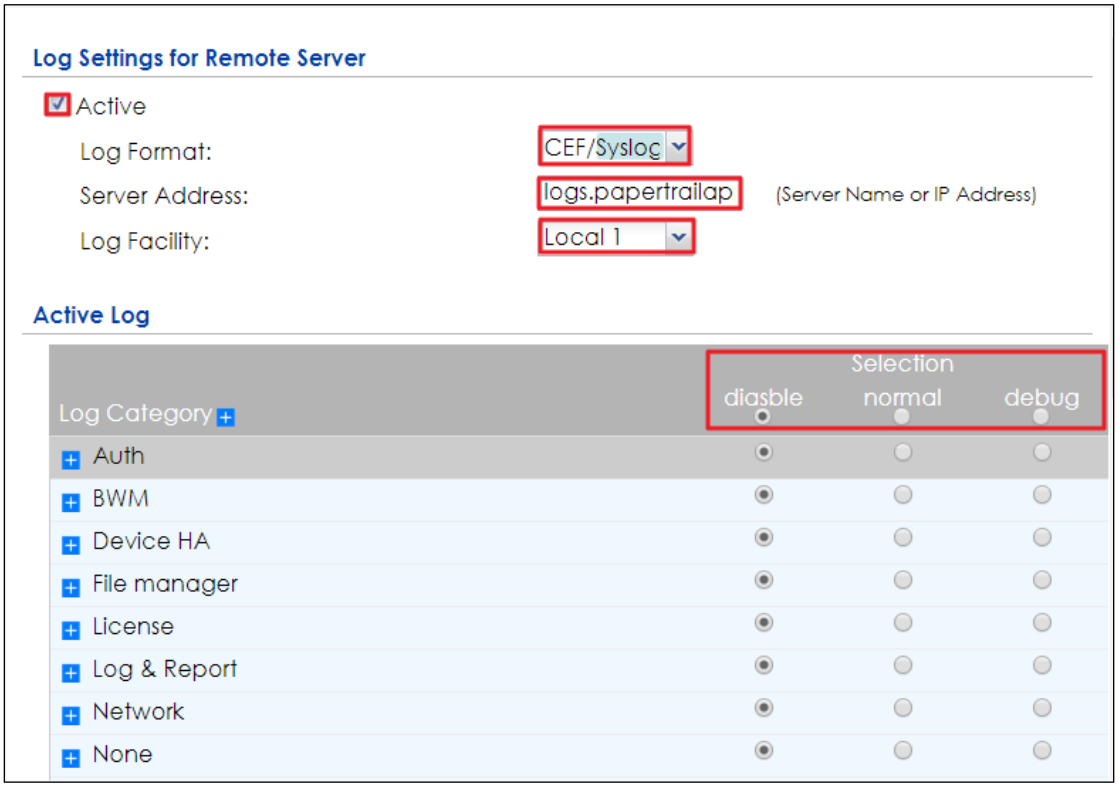
Dashboard > Add Systems > > I'm using > Choose your situation > System Created



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.

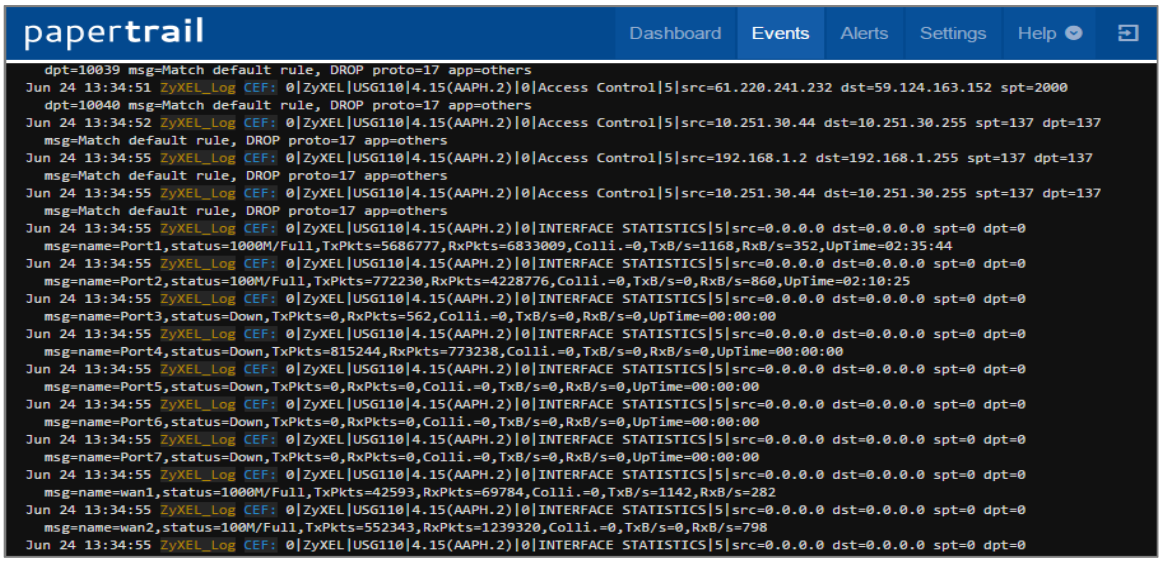
CONFIGURATION > Log & Report > Log Settings > Remote Server > Edit



Test the Remote Server

You will receive a log mail depends on the time you set in the E-mail Server.

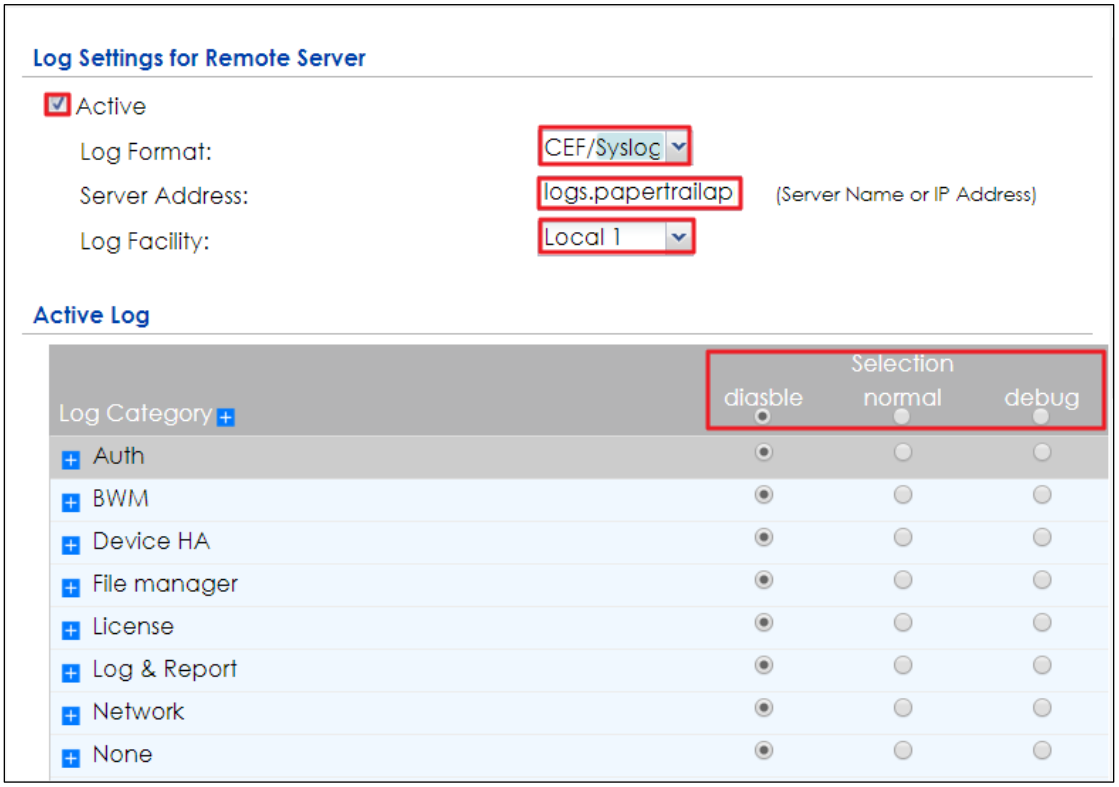
ZyXEL Log Mail



What Could Go Wrong?

Make sure your **Log settings for Remote Server** are all correct.

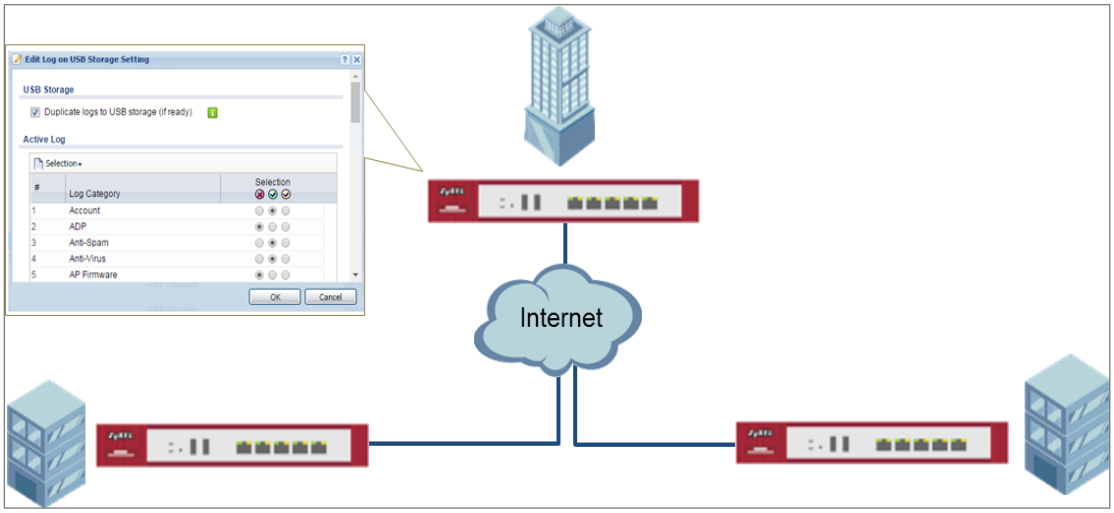
CONFIGURATION > Log & Report > Log Settings > Remote Server



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.



ZyWALL/USG enable and send logs to the USB storage

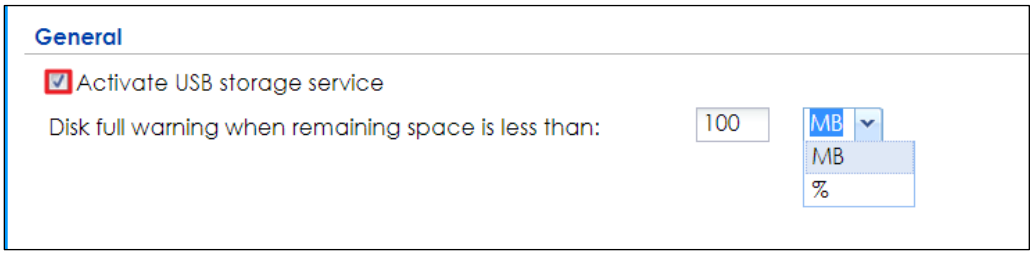
Note: Only connect one USB device. It must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system. This example was tested using USG110 (Firmware Version: ZLD 4.25).

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.

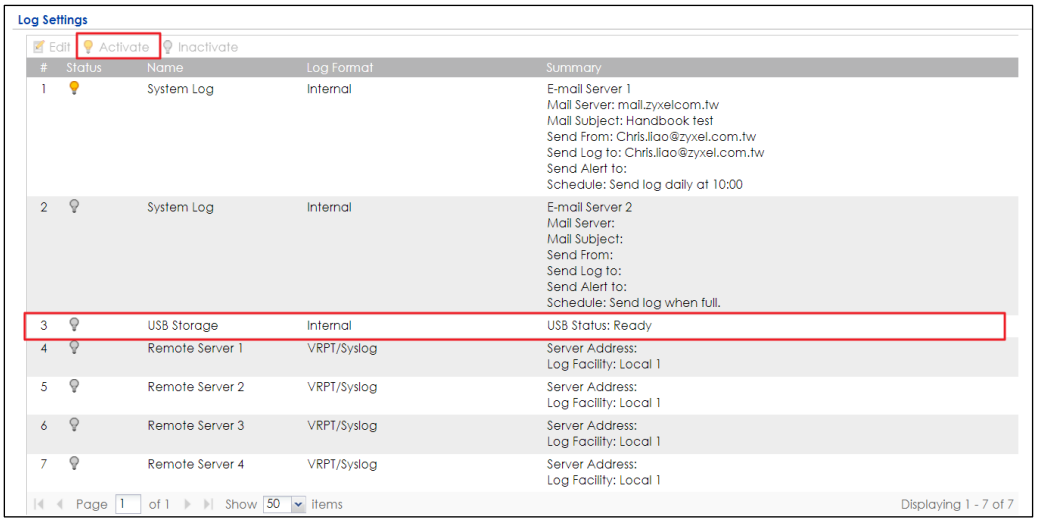
CONFIGURATION > System > USB Storage > Settings > General



Set Up the USB Log Storage

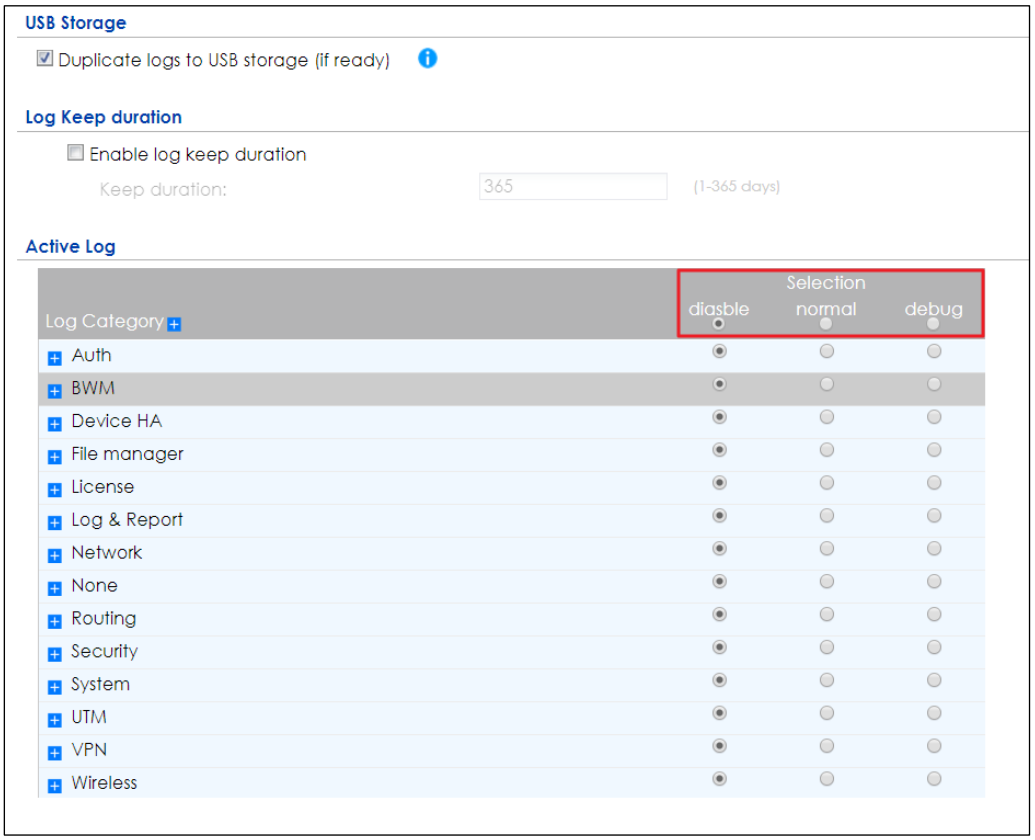
Go to **CONFIGURATION > Log & Report > Log Settings**, select **USB Storage** and click **Activate**. Click **Apply** to save your changes.

CONFIGURATION > Log & Report > Log Settings



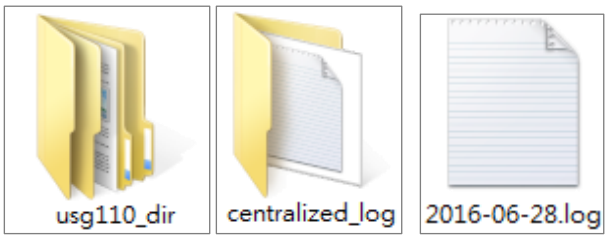
Go to **CONFIGURATION > Log & Report > Log Settings > USB Storage > Edit**. Select **Duplicate logs to USB storage (if ready)** to have the ZyWALL/USG save a copy of its system logs to a connected USB storage device. Use the **Selection** drop-down list to change the log settings for all of the log categories.

CONFIGURATION > Log & Report > Log Settings



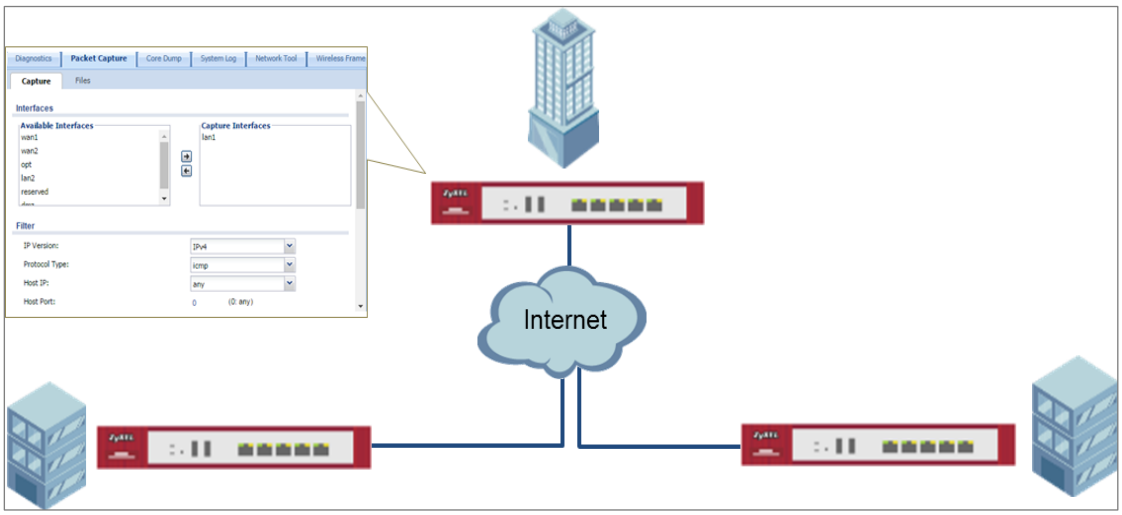
Check the USG Log Files

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.

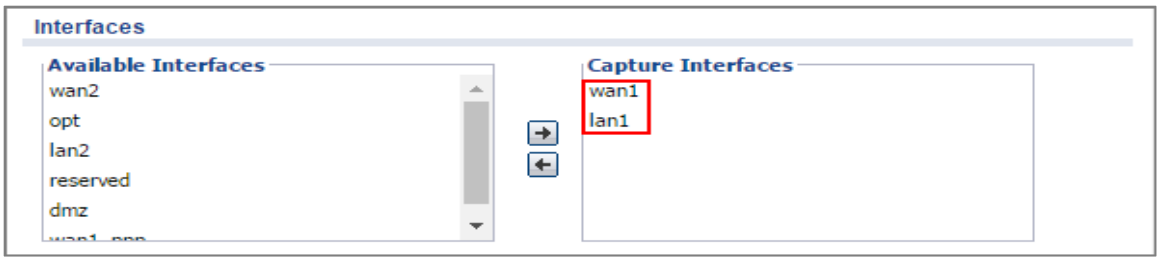


ZyWALL/USG Packet Capture Feature Settings

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.

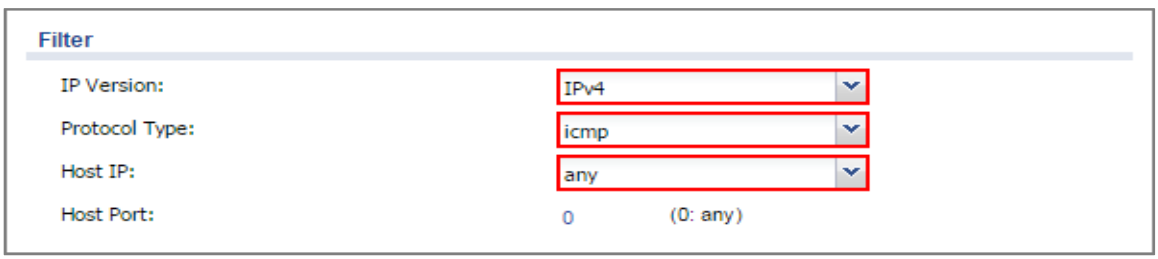


8 Go to **MAINTENANCE > Diagnostics > Packet Capture > Capture > Filter**.

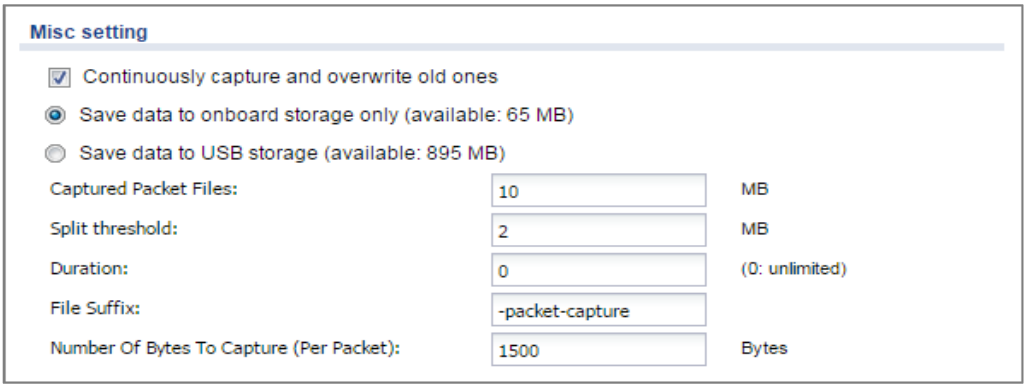
Select **IP Version** (IPv4 or IPv6) for which to capture packets or select **any** to capture packets for all IP versions.

Select the **Protocol Type** of traffic for which to capture packets. Select **any** to capture packets for all types of traffic.

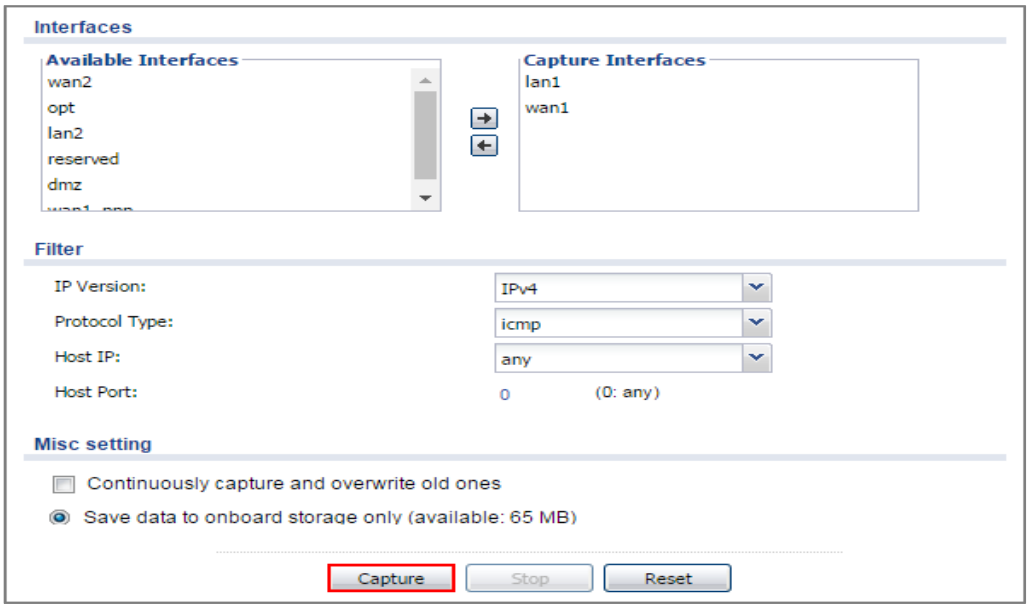
Select a **Host IP** address object for which to capture packets. Select **any** to capture packets for all hosts. Select **User Defined** to be able to enter an IP address.



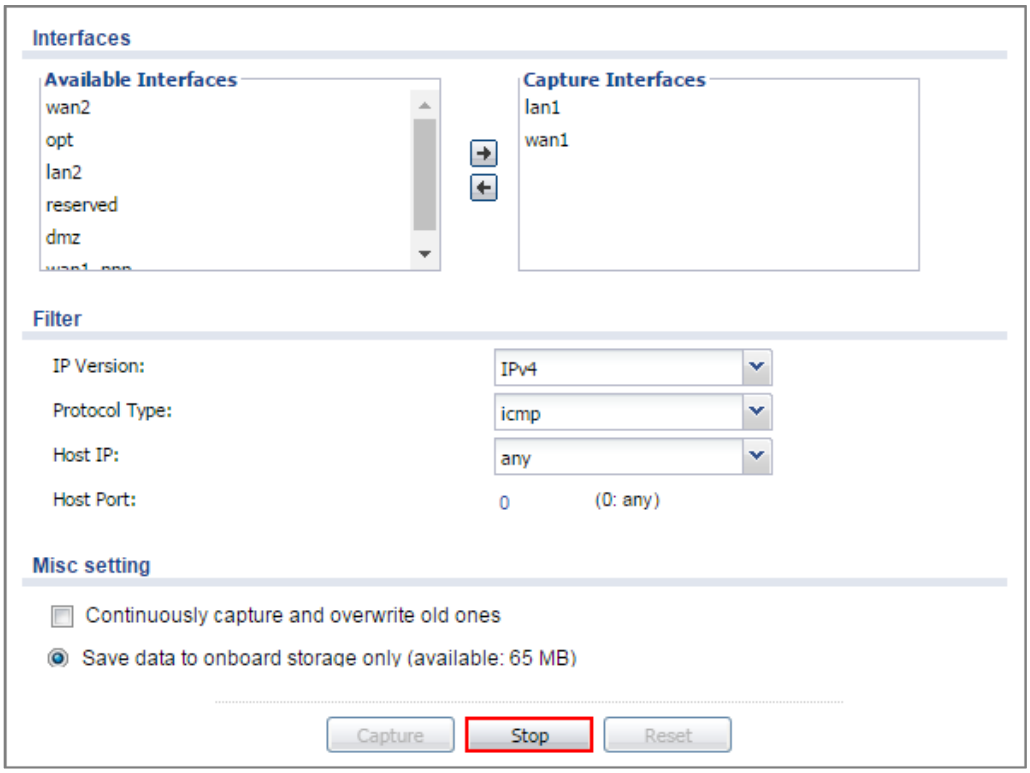
9 Go to **MAINTENANCE > Diagnostics > Packet Capture > Capture > Misc setitng**. Select **Continuously capture and overwrite old ones** to have the ZyWALL/USG keep capturing traffic and overwriting old packet capture entries when the available storage space runs out. Select **Save data to onboard storage only** or **Save data to USB storage** (If status shows service deactivated, go to **CONFIGURATION > Object > USB Storage**, select Activate USB storage service)



10 Click **Capture**.

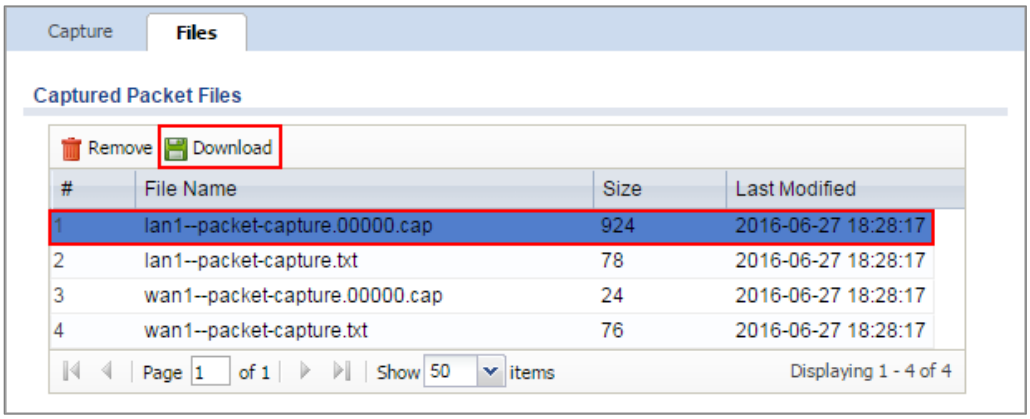


11 Click **Stop** when collection is done.

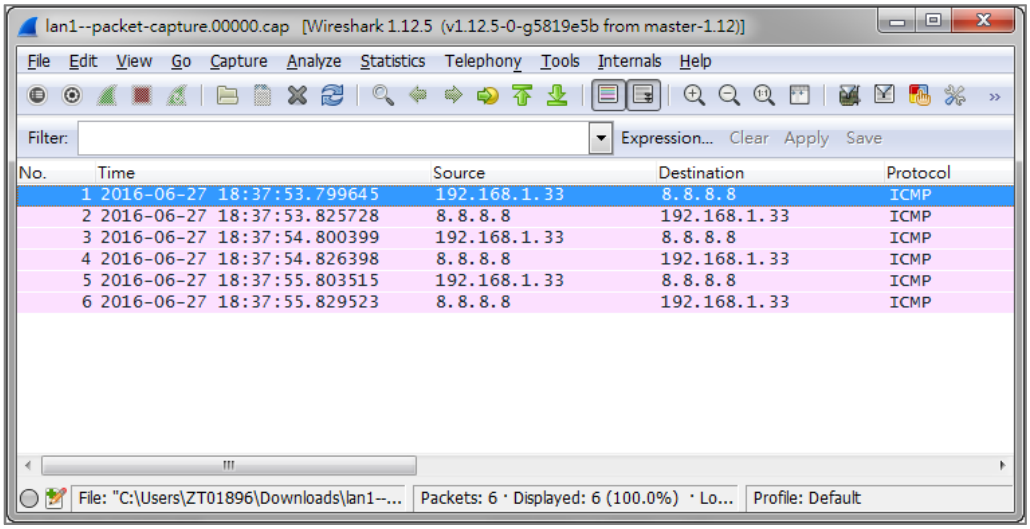


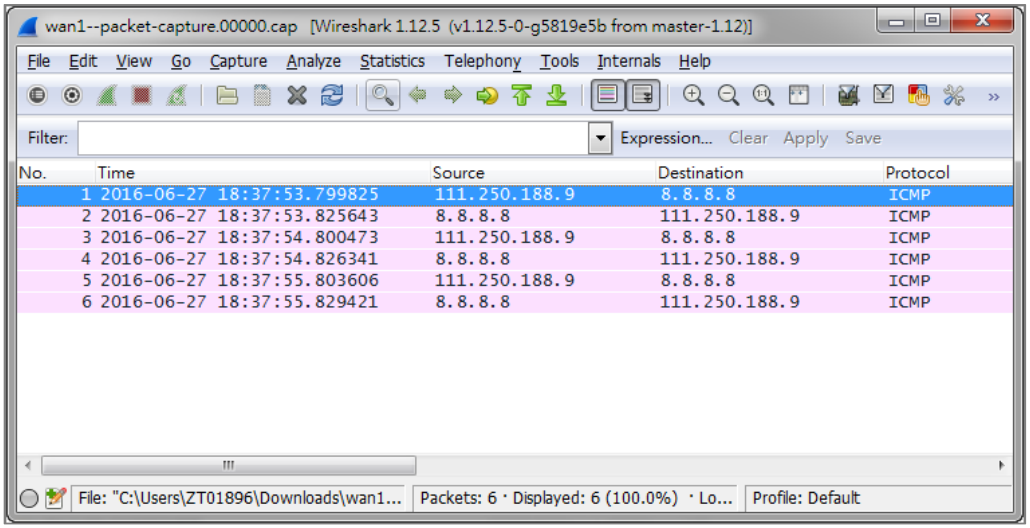
Check the Capture Files

12 Go to **MAINTENANCE > Diagnostics > Packet Capture > Files**, select the .cap file and click **Download**.



13 Open .cap files with Wireshark

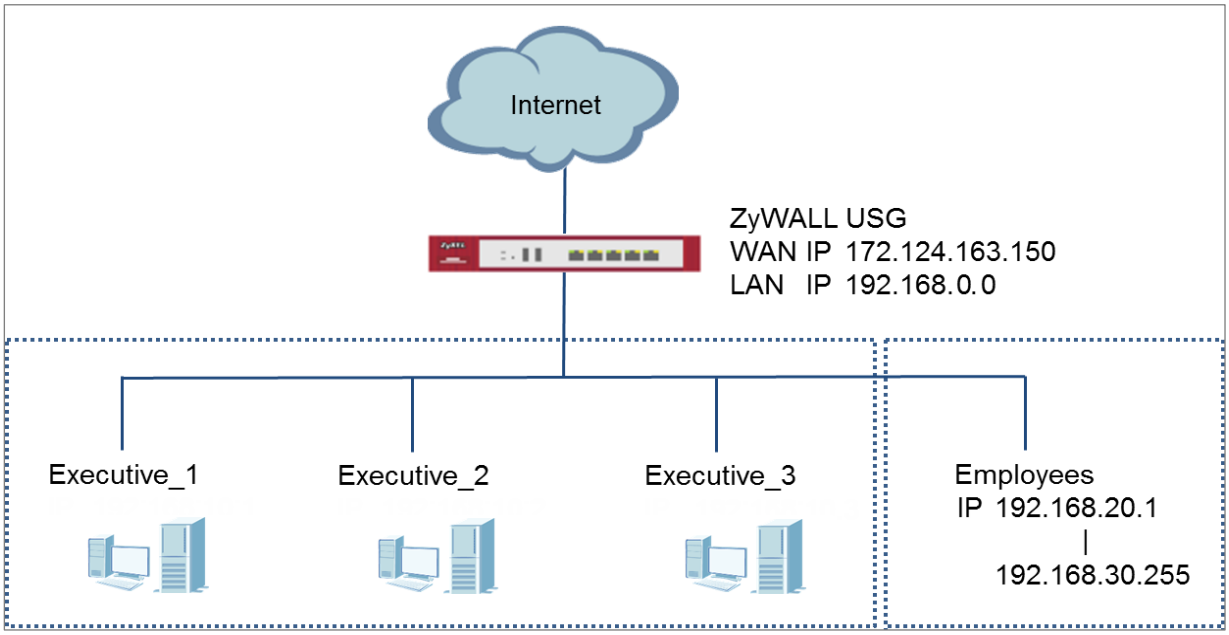




How to Exempt Specific Users from Security Control

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

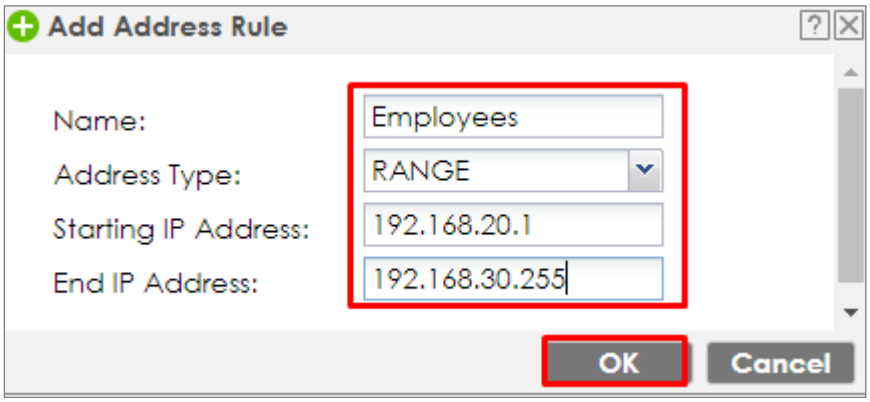


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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

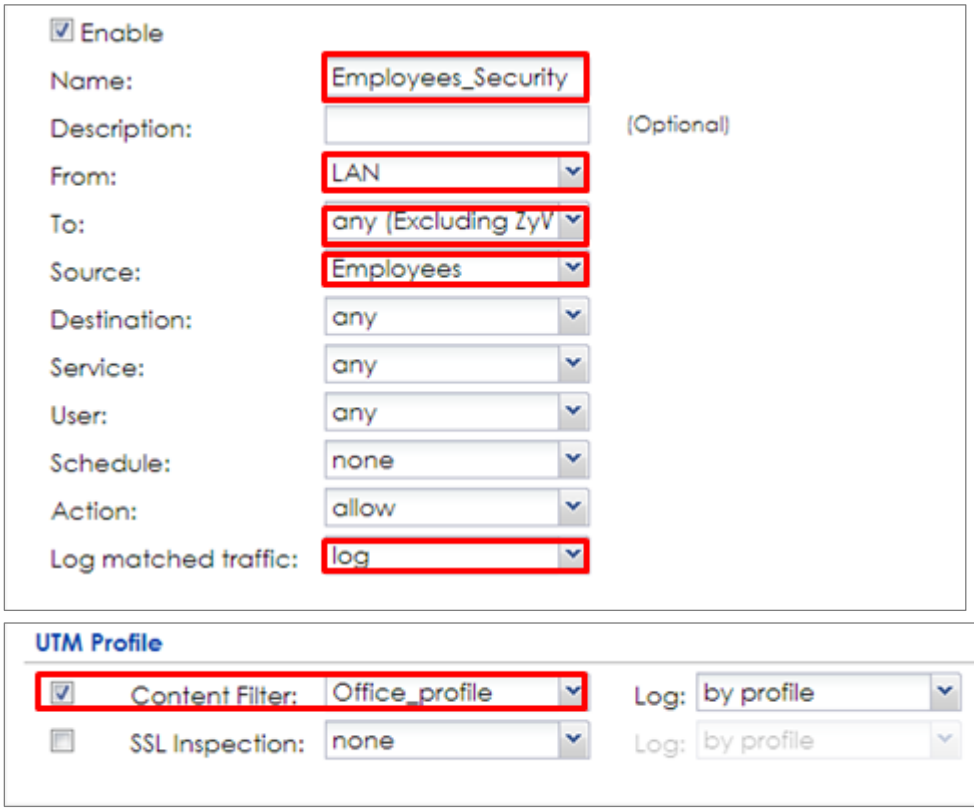


Set up **Security Policy** for employees, go to **CONFIGURATION > Security Policy > Policy Control > Add corresponding**, configure a **Name** for you to identify the employees' **Security Policy** profile.

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



Set Up the Security Policy on the ZyWALL/USG for Executives

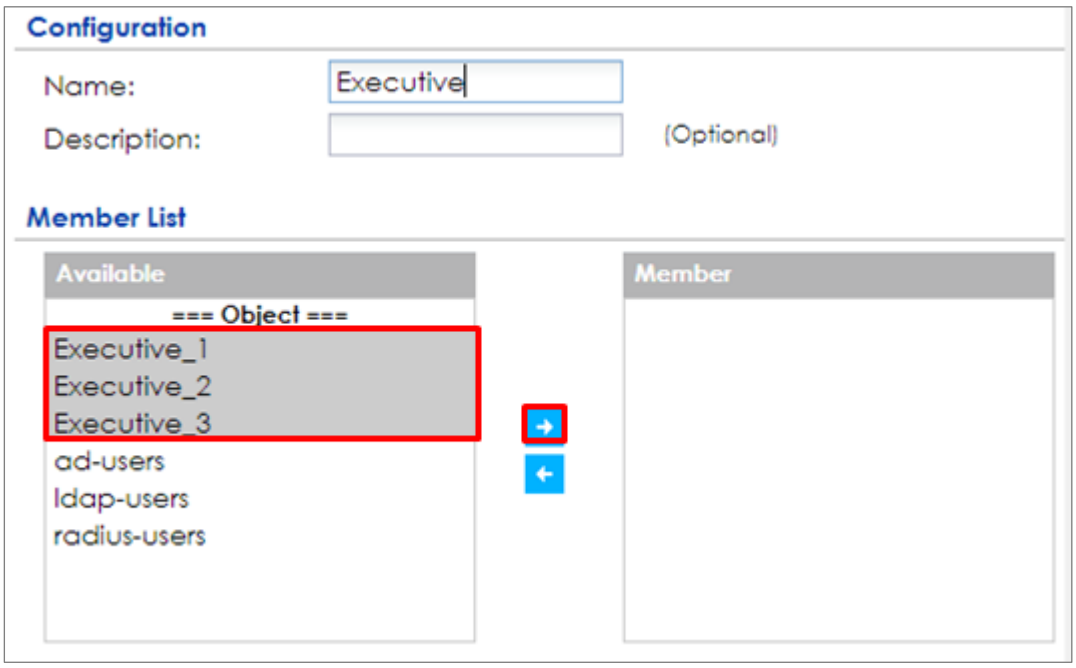
In the ZyWALL/USG, go to **CONFIGURATION > Object > User/Group > Add A User**

to create **User Name/Password** for each executive.

CONFIGURATION > Object > User/Group > Add A User

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



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

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.

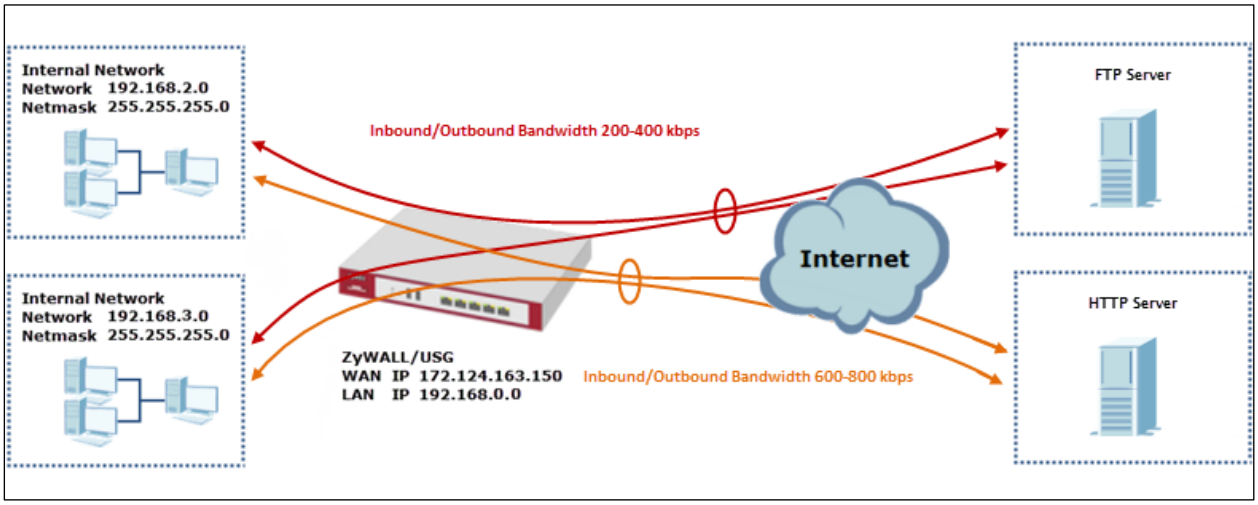
You have subscribed for the **UTM** service but the license is expired.

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

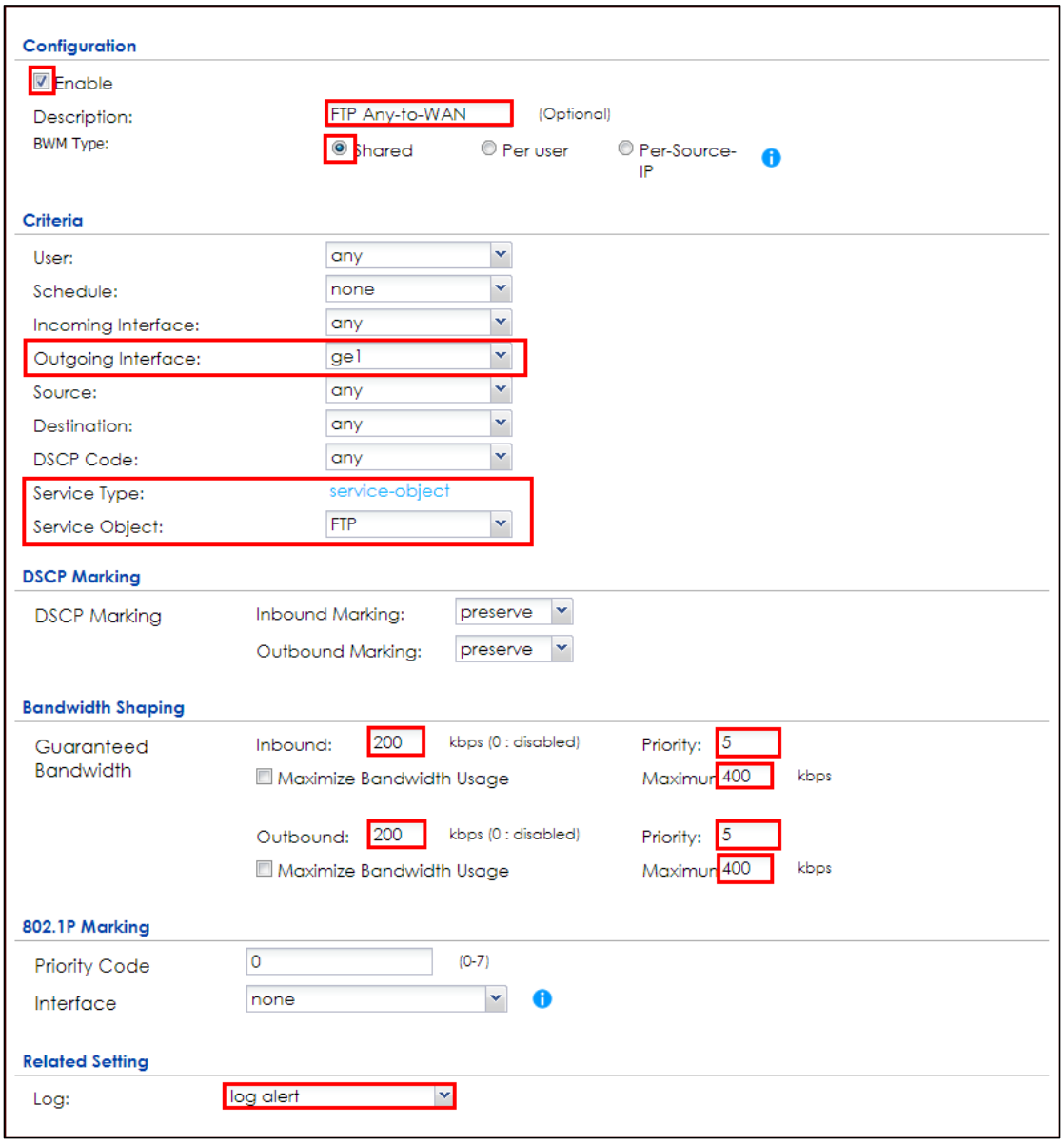
In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **FTP Any-to-WAN** as the policy's **Description**.

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



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

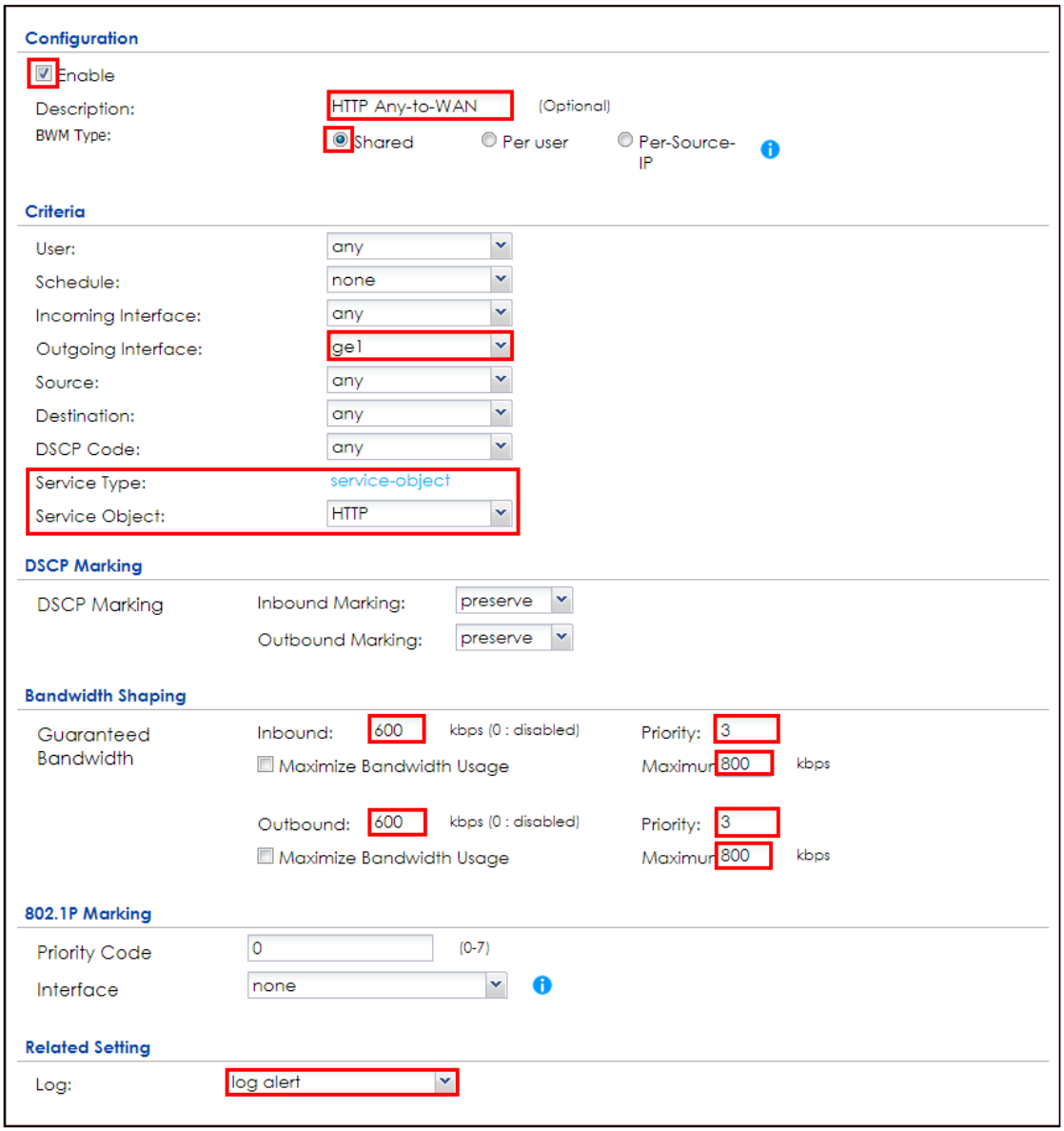
In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **HTTP Any-to-WAN** as the policy's Description (Optional).

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



Note: In Bandwidth Management, the highest priority is (1) the lowest priority is (7).

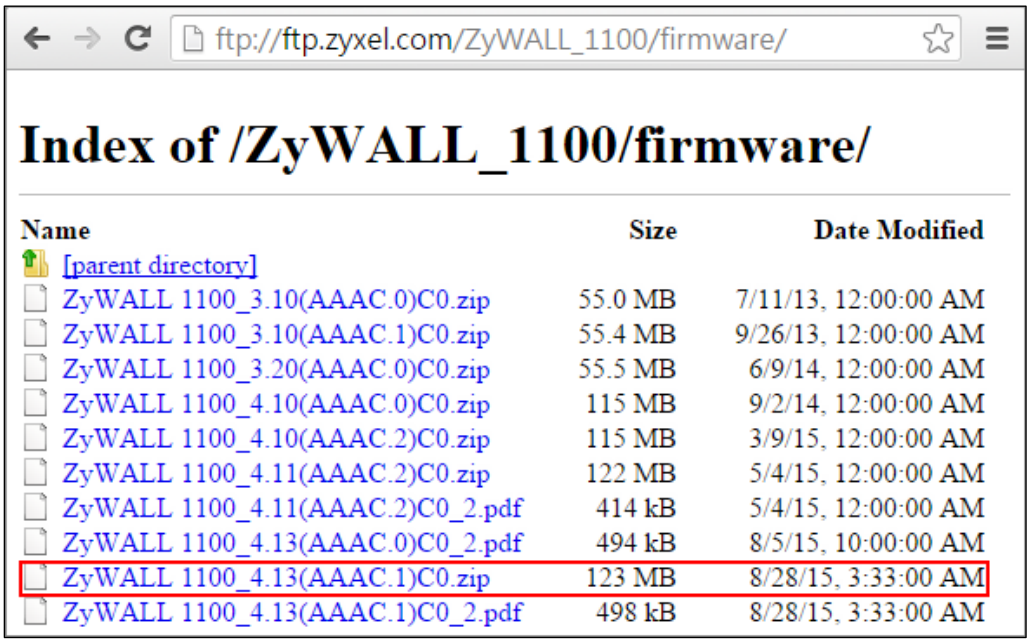
Set Up the Bandwidth Management Global Setting on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > BWM Global Setting**, select **Enable**.

CONFIGURATION > BWM > BWM Global Setting

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.



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

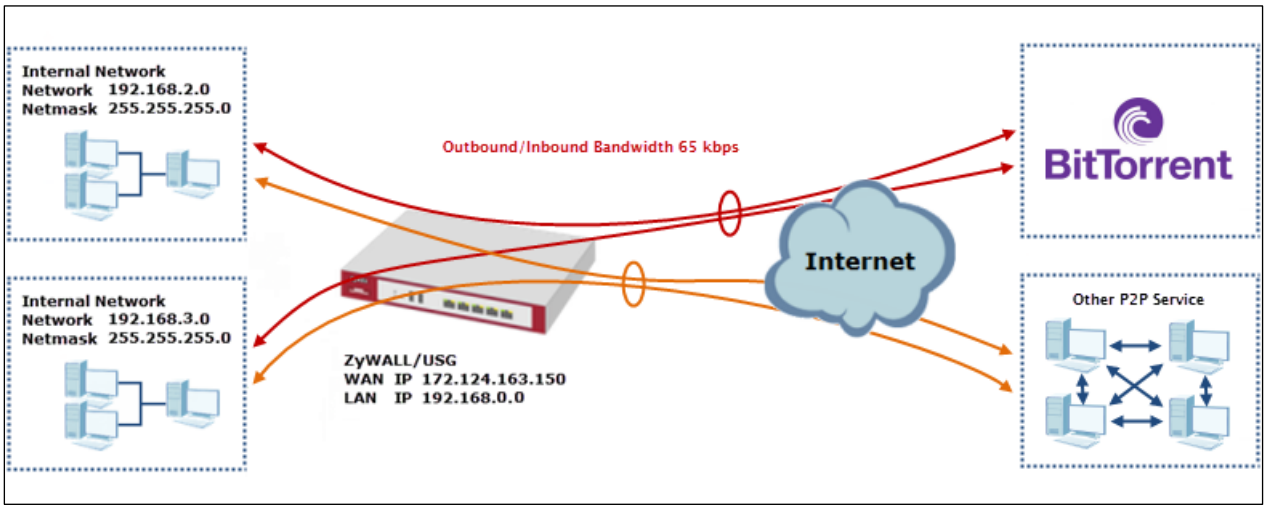
What Could Go Wrong?

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

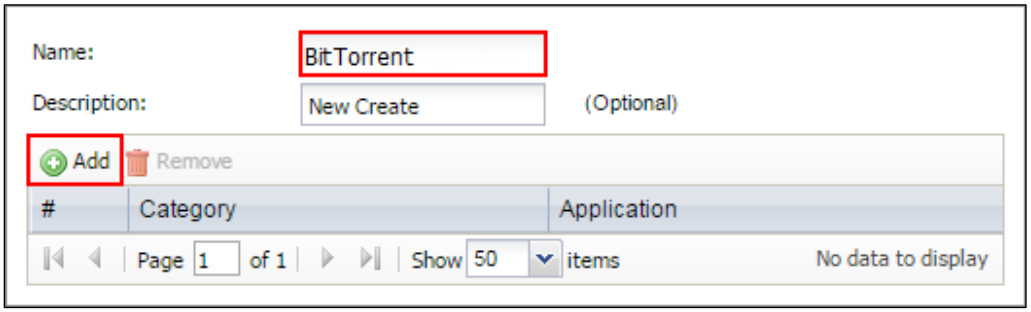


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. The total available bandwidth assumption is 1,600 kbps. This example was tested using USG310

Set Up the Application Patrol Profile on the ZyWALL/USG

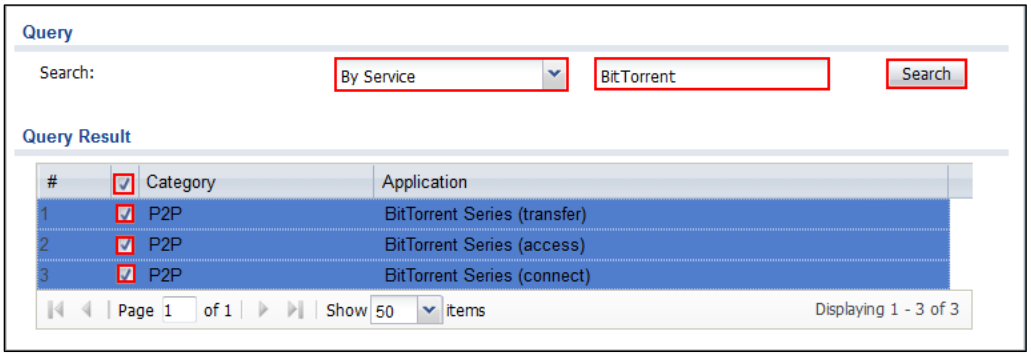
In the ZyWALL/USG, go to **CONFIGURATION > Object > Application > Add Application Rule**. Configure a **Name** for you to identify the **Application Profile**. Then, click **Add** to create an **Application Object**.

CONFIGURATION > Object > Application > Add Application Rule



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



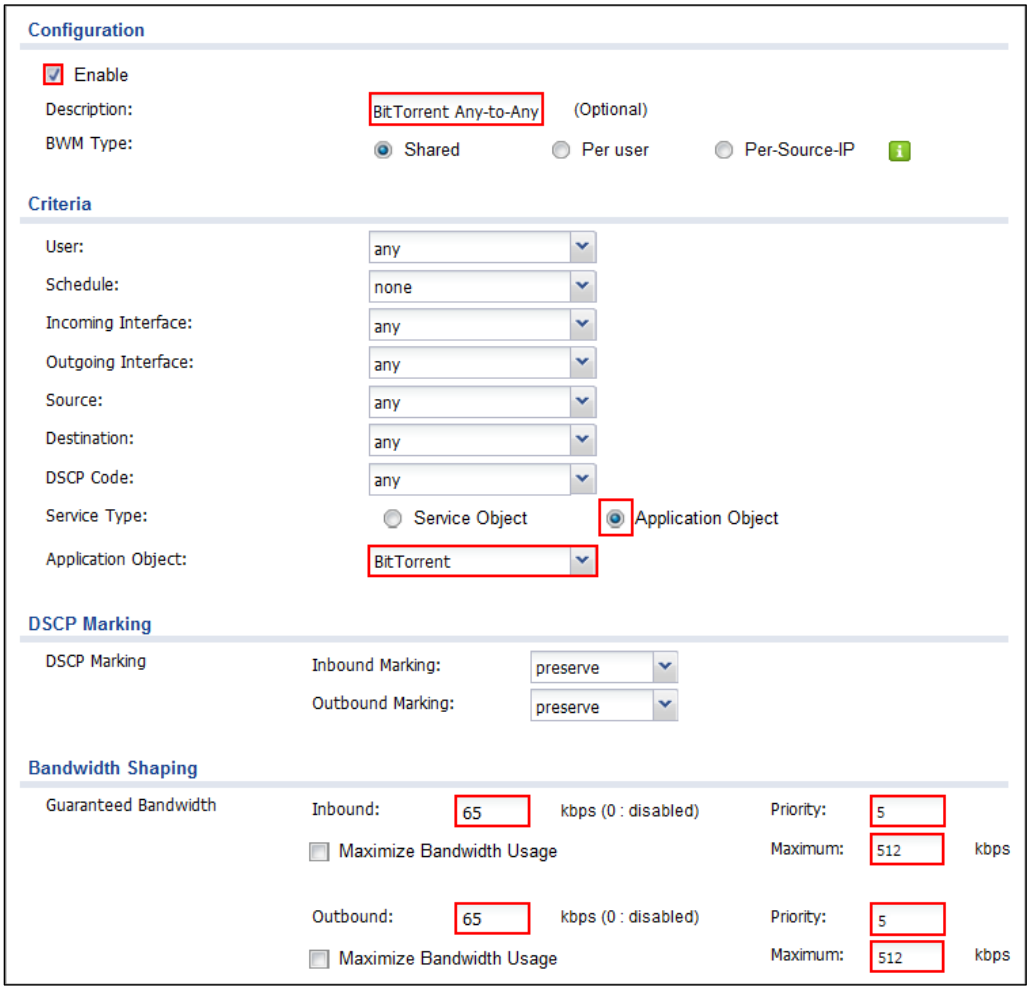
Set Up the Bandwidth Management for BitTorrent on the ZyWALL/USG

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

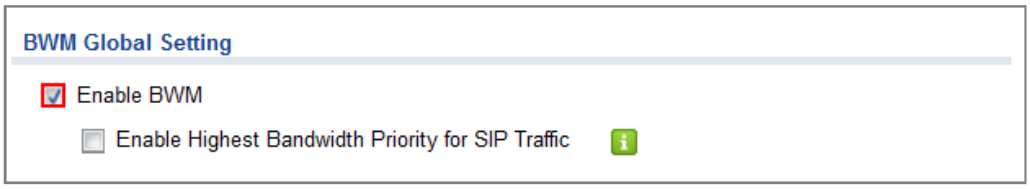


Note: In Bandwidth Management, the highest priority is (1) the lowest priority is (7).

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

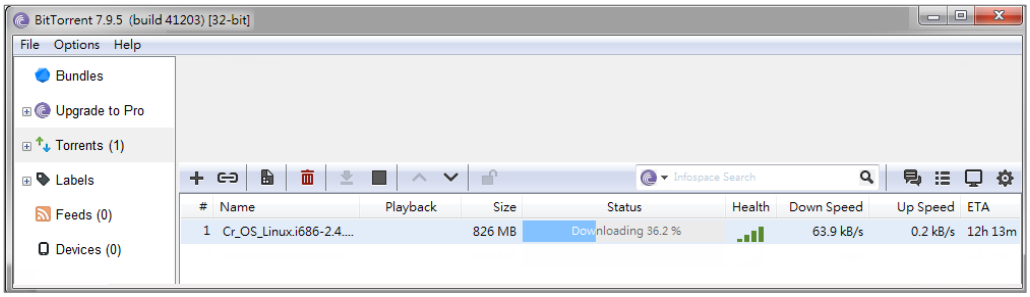


Test the Result

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.



Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

Monitor > Log

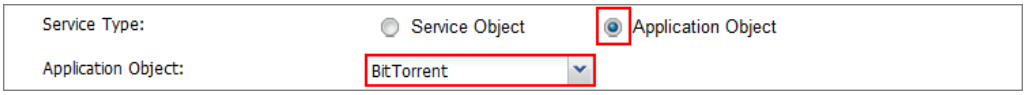
Priority	Category	Message	Source	Destination	Protocol
alert	BWM	Mode=port-less Rule=1 matched	192.168.1.33:53722	187.34.56.190:13867	udp
alert	BWM	Mode=port-less Rule=1 matched	192.168.1.33:53722	84.250.209.195:51413	udp
alert	BWM	Mode=port-less Rule=1 matched	192.168.1.33:53722	89.43.62.55:51016	udp

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.

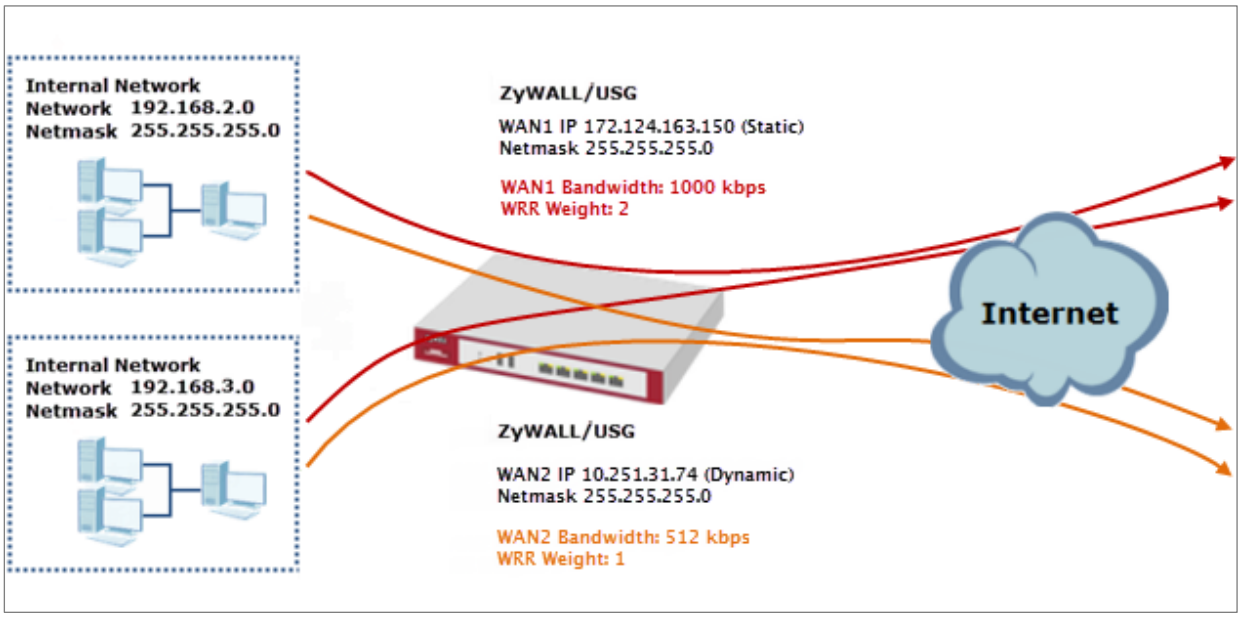


You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (https://portal.myzyxel.com/) to register or extend your **Application Patrol** license.

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

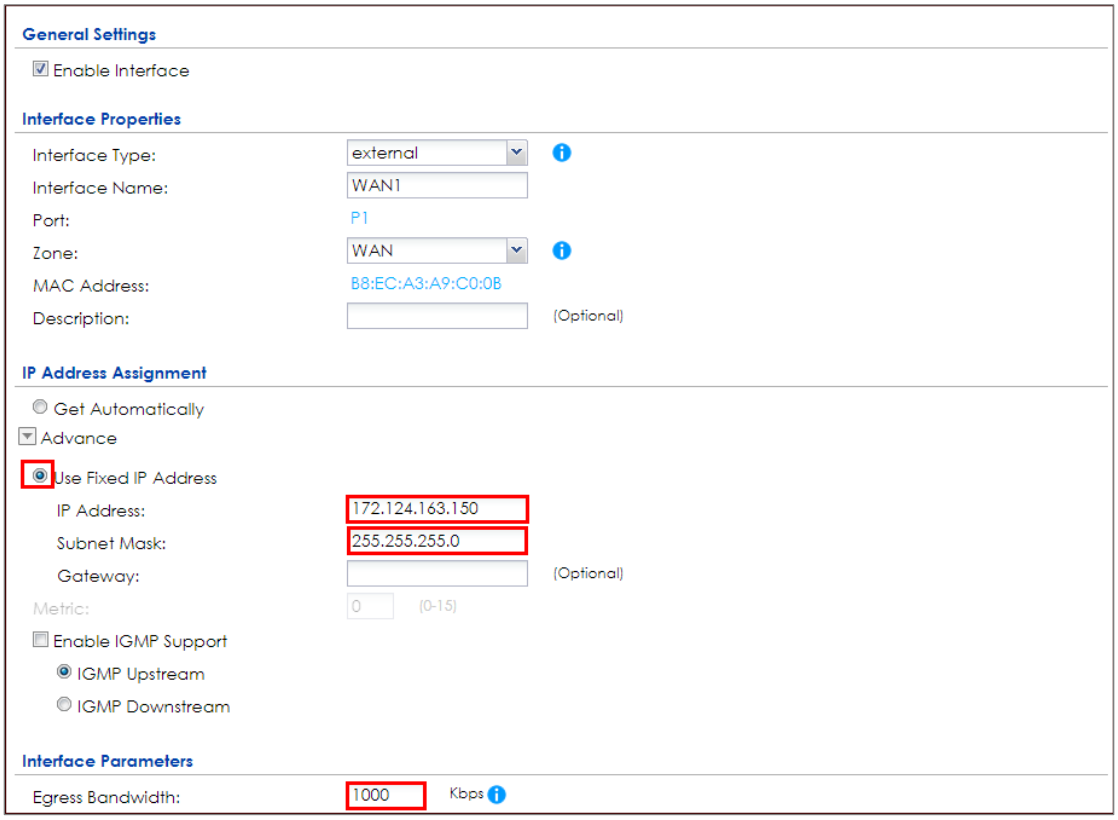


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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

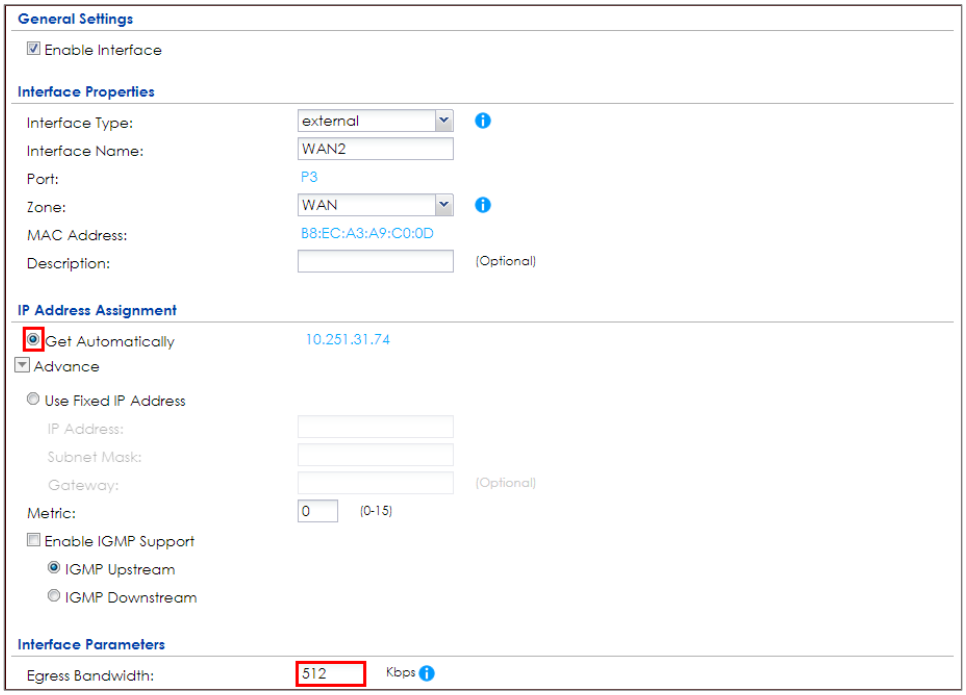


Set Up the Available Bandwidth on WAN2 Interfaces on the ZyWALL/USG

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

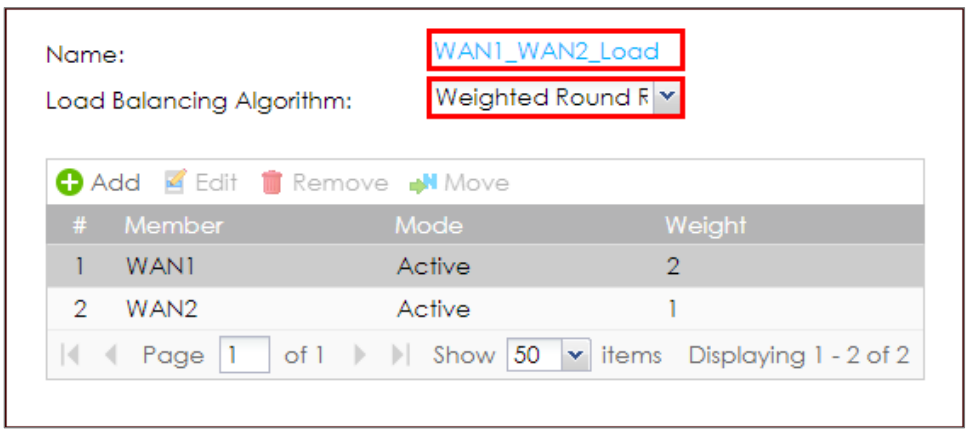


Set Up the WAN Trunk on the ZyWALL/USG

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**.

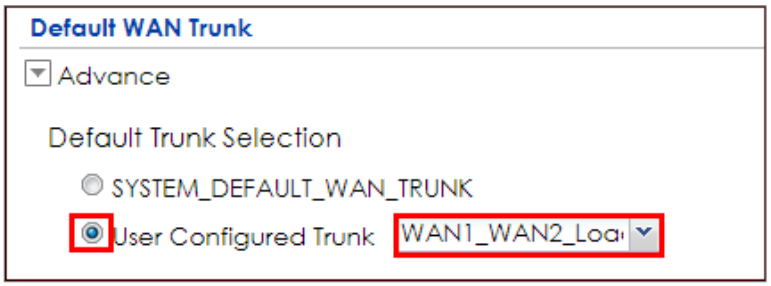
Add **WAN1** and enter **2** in the **Weight** column. Add **WAN2** and enter **1** in the **Weight** column. Click **OK** to return to the **Configuration** screen.

CONFIGURATION > Interface > Trunk > User Configuration > Add Trunk



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

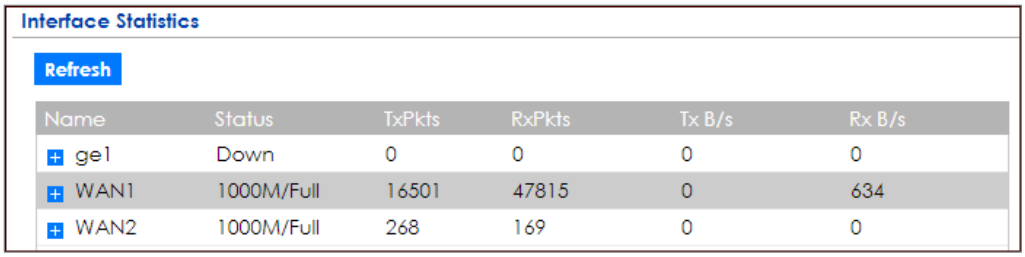


Test the Result

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



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.

ZYXEL

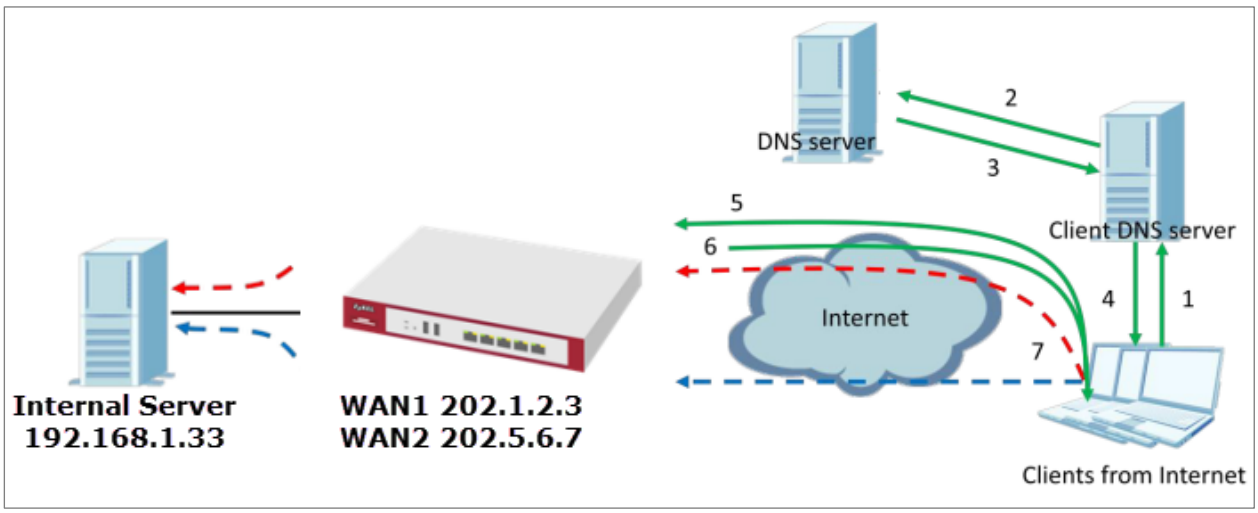
www.zyxel.com

805/865

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

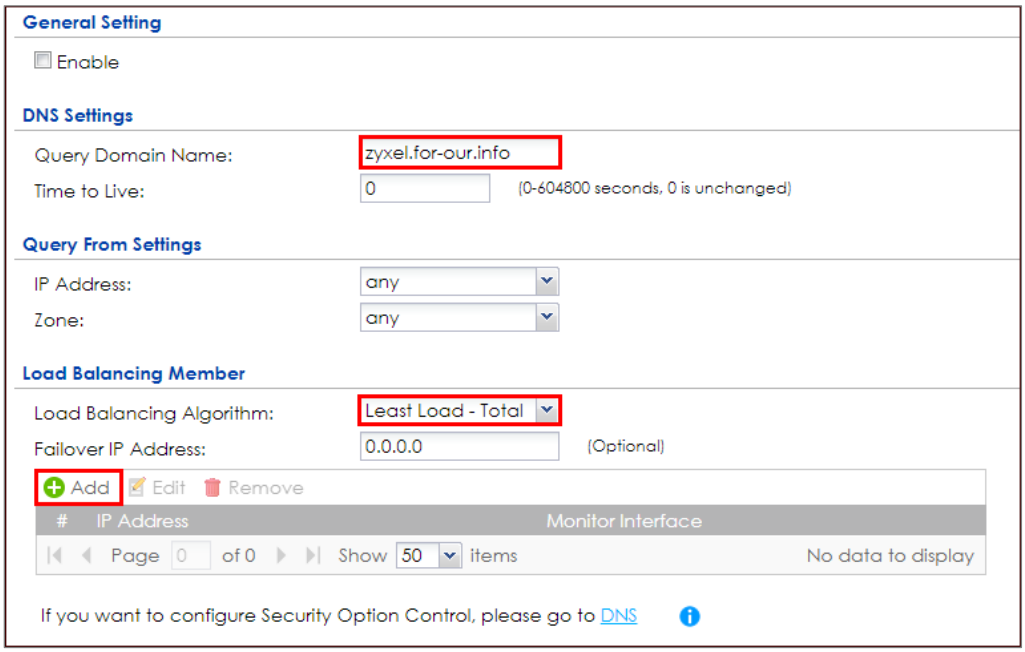


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

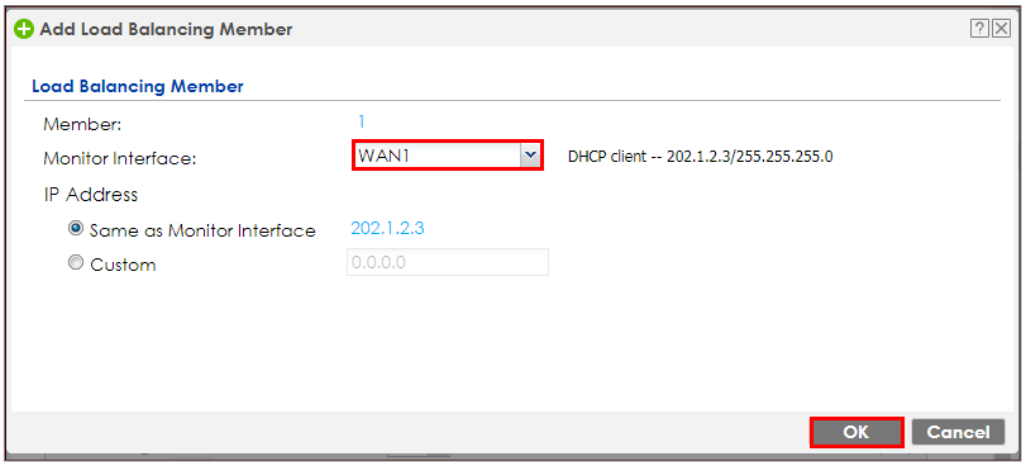
Set Up the DNS Inbound Load Balancing on the ZyWALL/USG

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**.

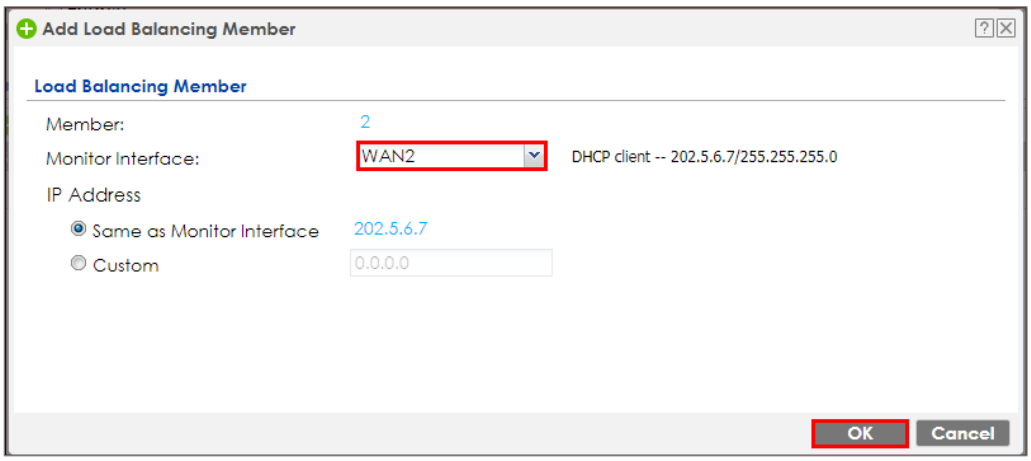
CONFIGURATION > Network > DNS Inbound LB



CONFIGURATION > Network > DNS Inbound LB

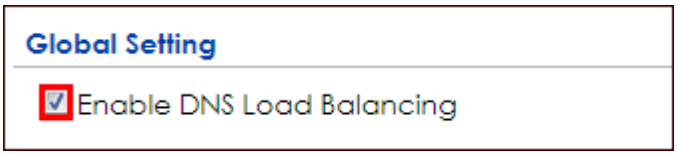


CONFIGURATION > Network > DNS Inbound LB



Go to **the Global Setting page to select Enable DNS Load Balancing.**

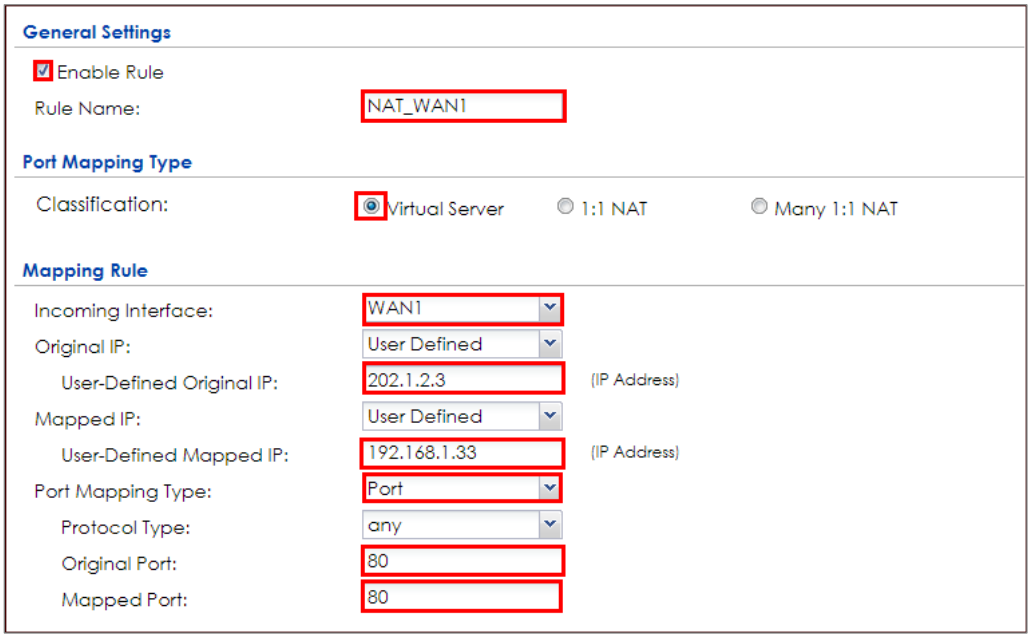
CONFIGURATION > Network > DNS Inbound LB



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



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...

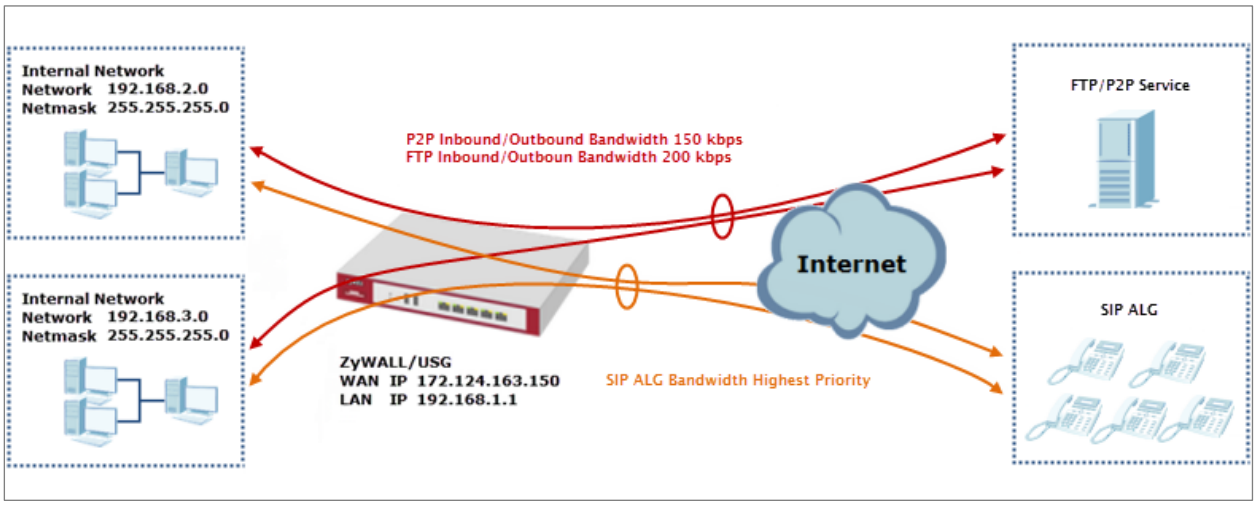
What Could Go Wrong?

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

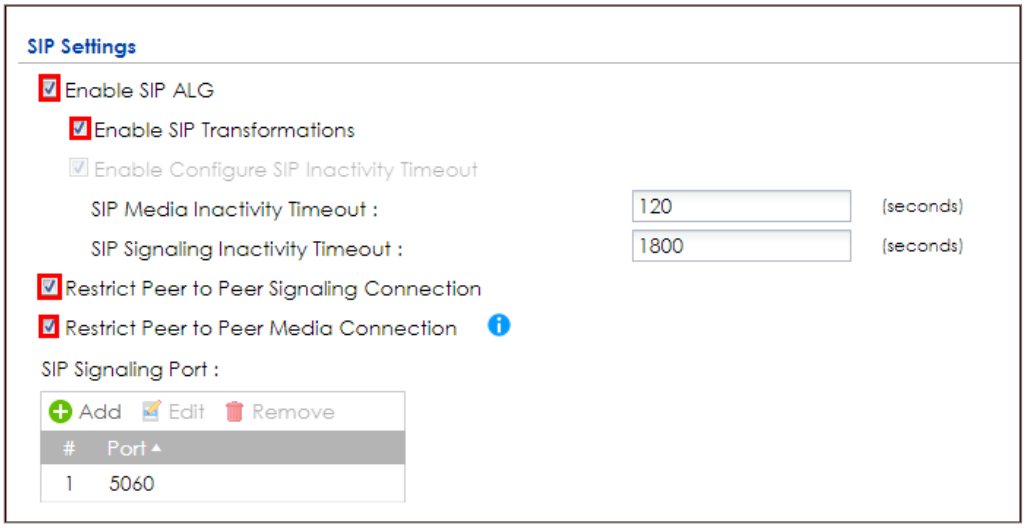


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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

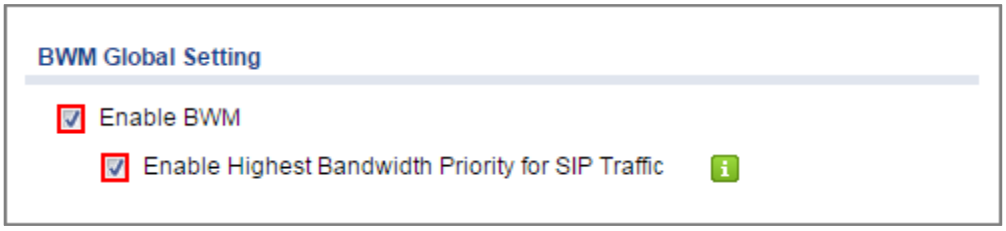


Note: If you are using a custom or additional UDP port number (not 5060) for SIP traffic, use the **Add** icon to add **SIP Signaling Port** numbers.

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



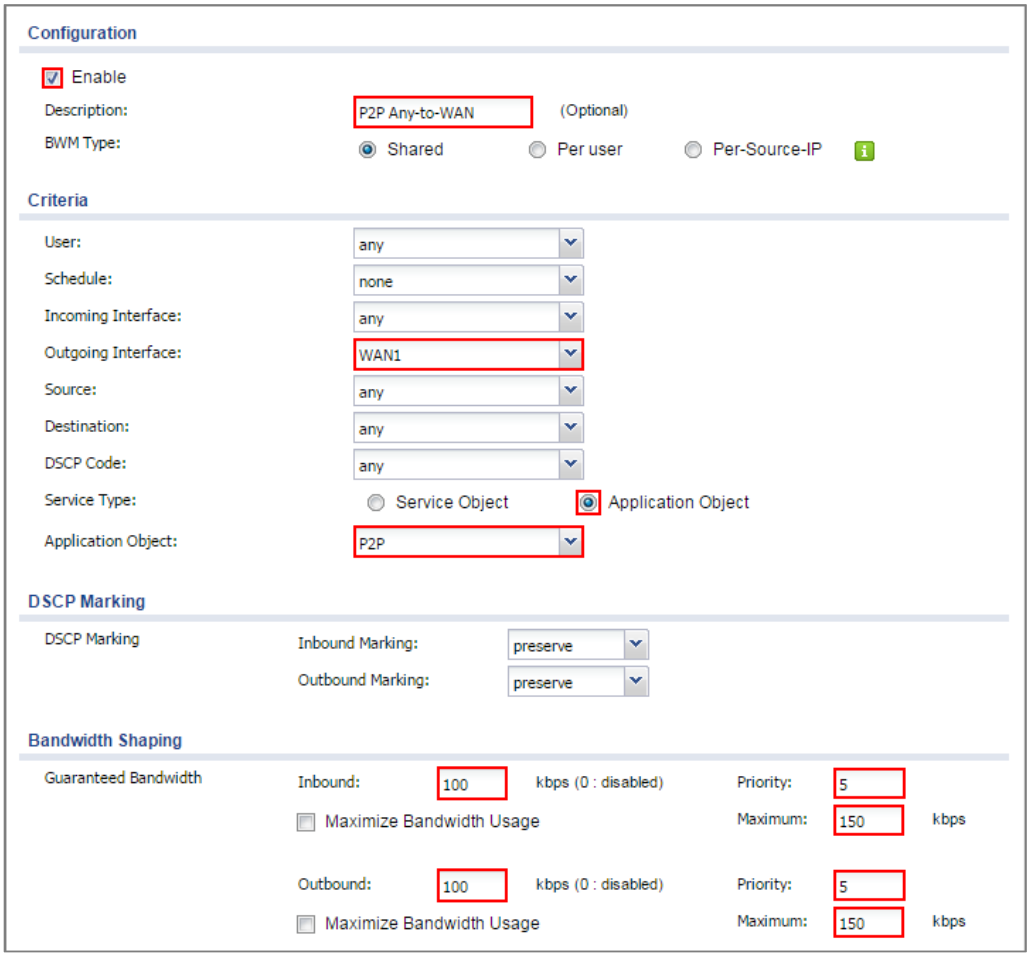
Set Up the Bandwidth Management for P2P on the ZyWALL/USG

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



Note: In Bandwidth Shaping, the highest priority is (1) the lowest priority is (7).

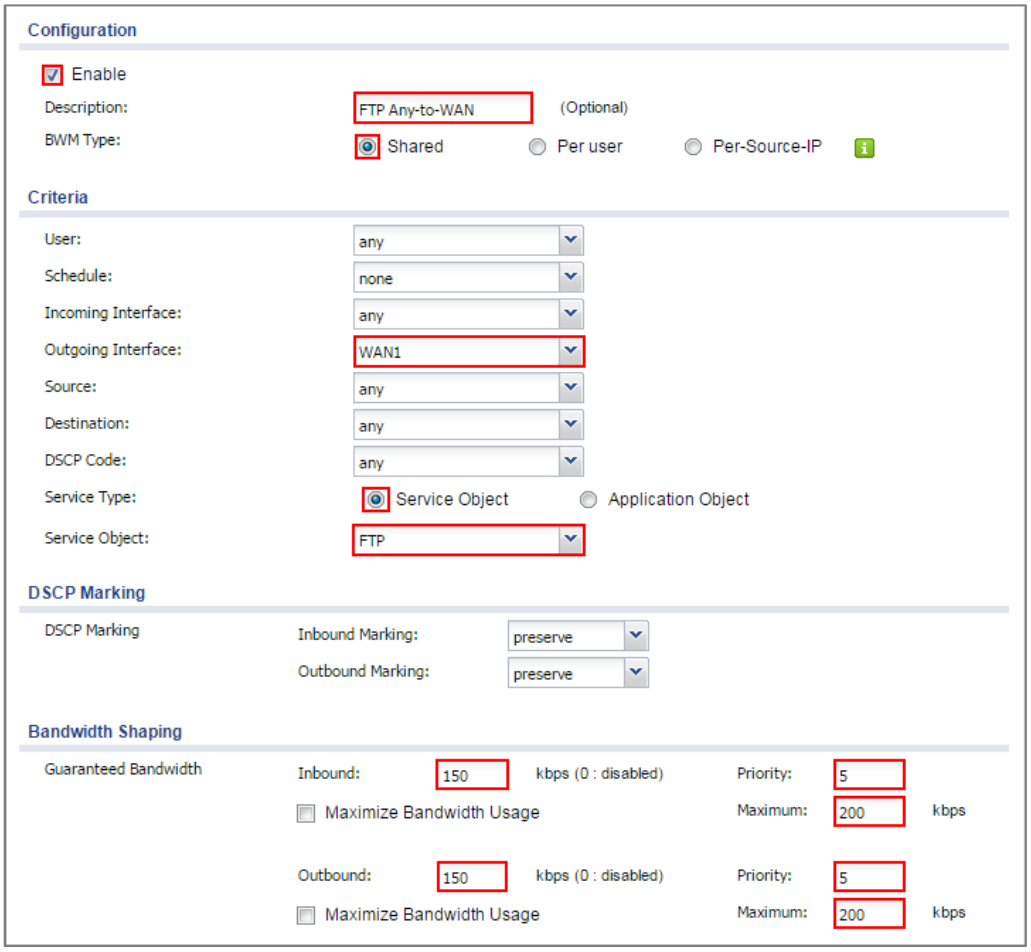
Set Up the Bandwidth Management for FTP on the ZyWALL/USG

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

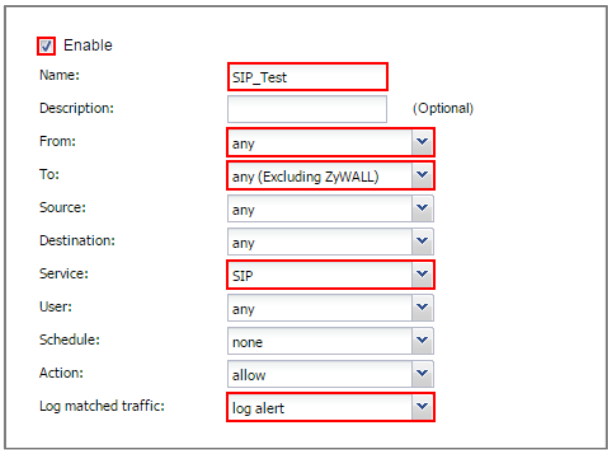


Note: In Bandwidth Shaping, the highest priority is (1) the lowest priority is (7).

Test the Result

Add a **Security Policy** rule to view the SIP log:

CONFIGURATION > BWM > Configuration > Add Policy



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.

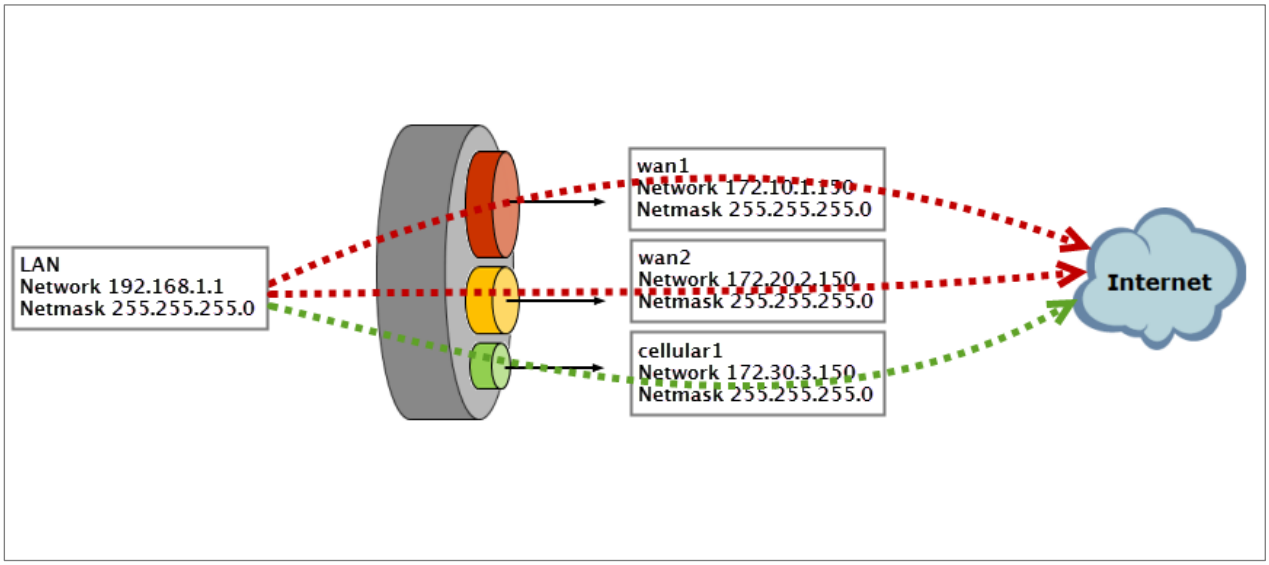
Monitor > Log

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.

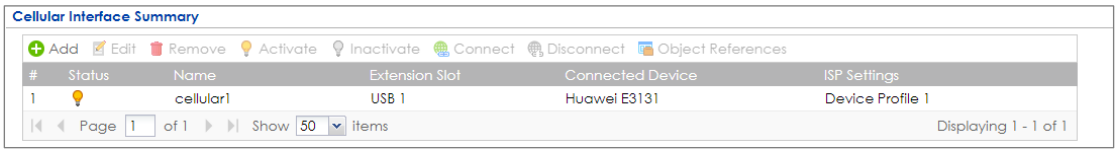
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the 3G/LTE Interface on the ZyWALL/USG

Connect a compatible mobile broadband USB device to use a cellular connection.

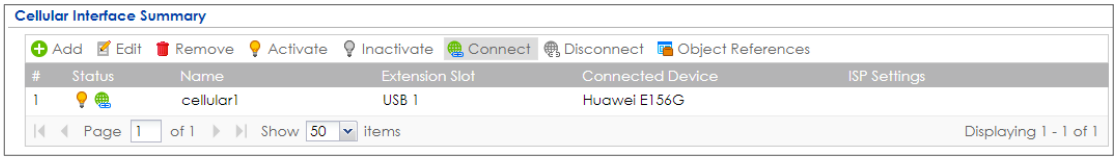
In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Cellular**, the connected device will automatically display in the **Cellular Interface Summary**. Click **Activate** and then the **Apply** button at the bottom of this page.

CONFIGURATION > Network > Interface > Cellular > Activate

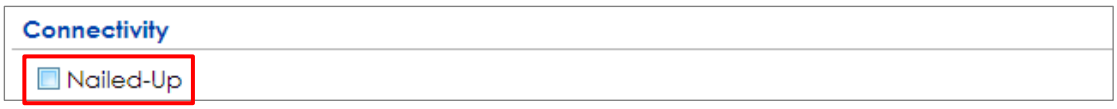


The default **Connectivity** method is **Nailed-Up**. The connection should always be up after you activate the cellular interface. You can click **Edit** and go to the **Connectivity** section to clear the **Nailed-Up** check box to have the ZyWALL/USG to establish the connection only when there is traffic.

CONFIGURATION > Network > Interface > Cellular > Connect



CONFIGURATION > Network > Interface > Cellular > Edit

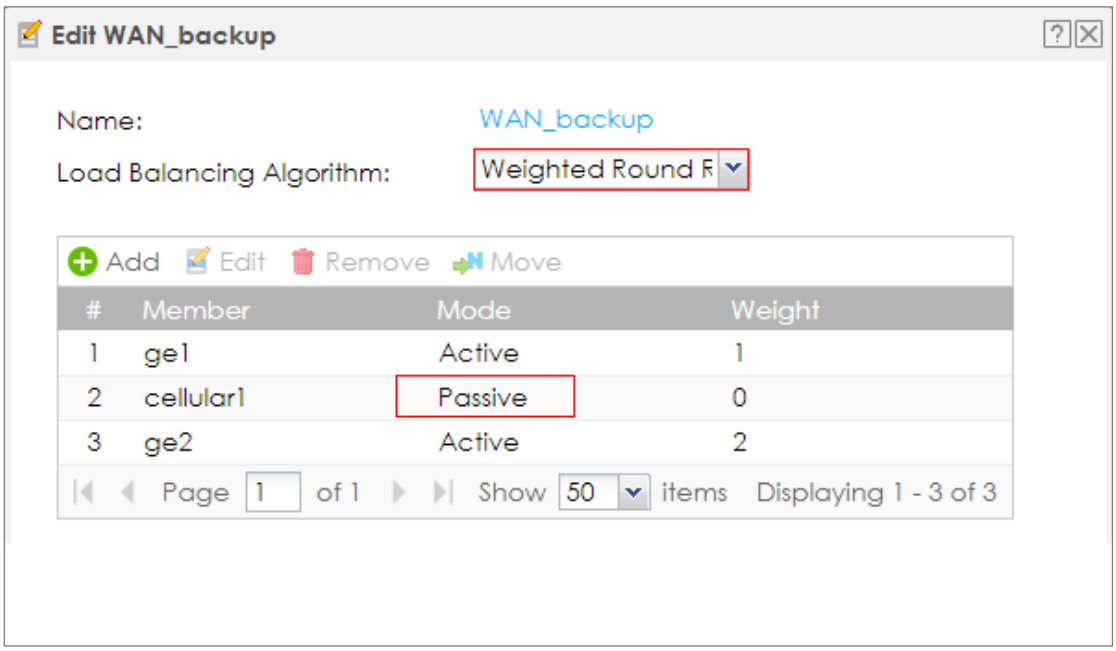


Set Up the Trunk on the ZyWALL/USG

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**.

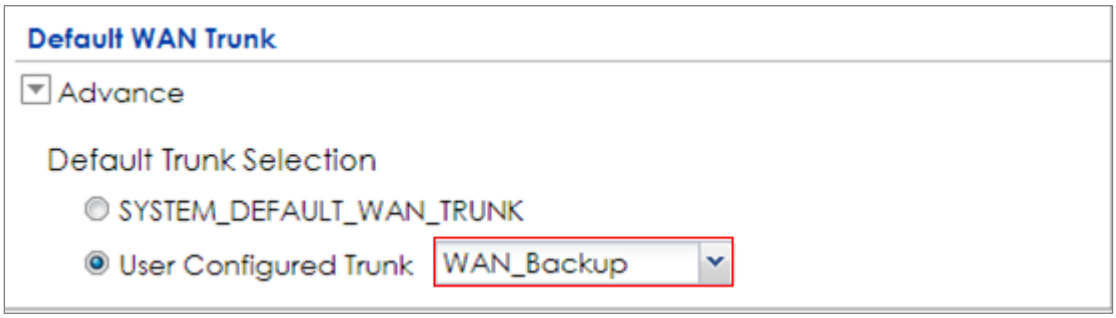
Add **wan1** and enter **3** in the **Weight** column. Add **wan2** and enter **2** in the **Weight** column. Add **cellular1**, change **Mode** to be the **Passive** mode, enter **1** in the **Weight** column. Click **OK** to return to the **Configuration** screen.

CONFIGURATION > Network > Interface > Trunk > User Configuration > Add Trunk



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**.

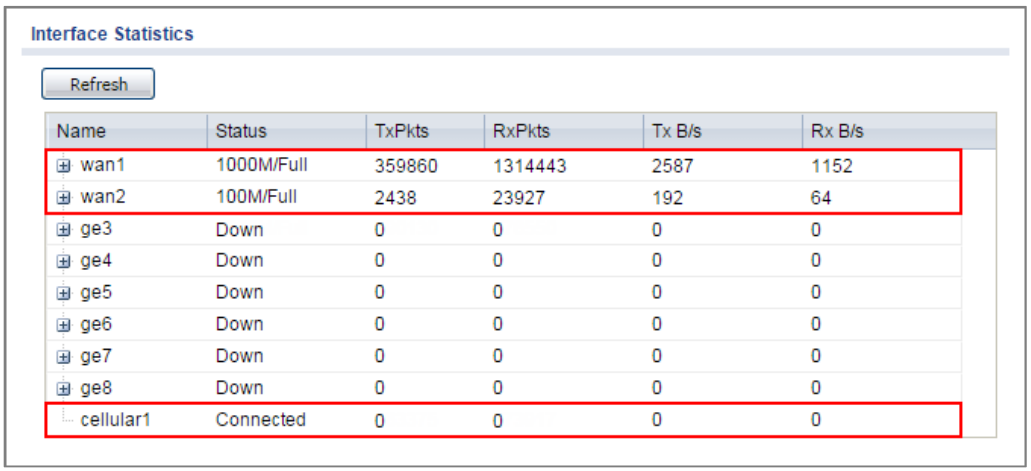
CONFIGURATION > Network > Interface > Trunk > Default WAN Trunk > User Configured Trunk



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



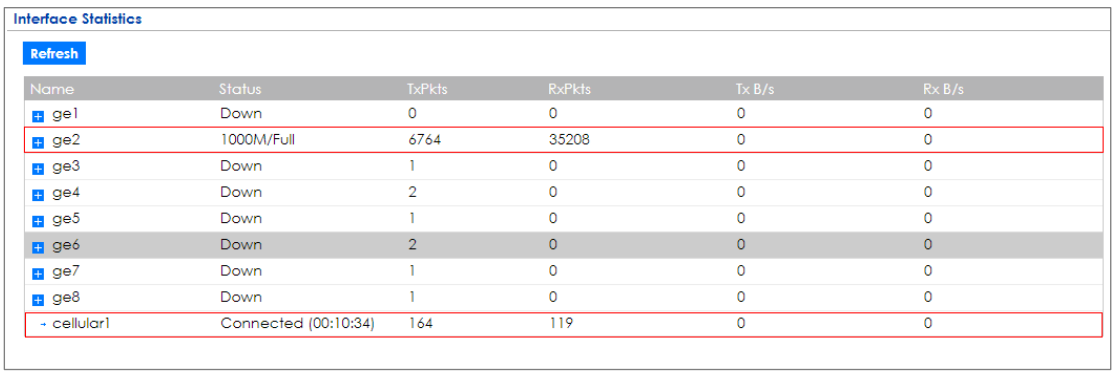
Interface Statistics

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

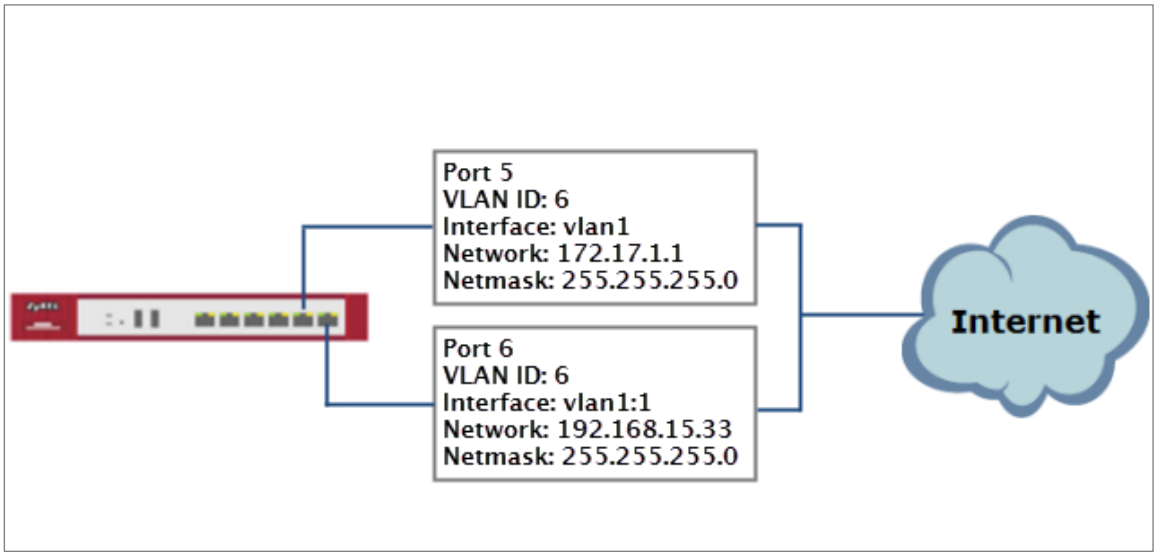
What Could Go Wrong?

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

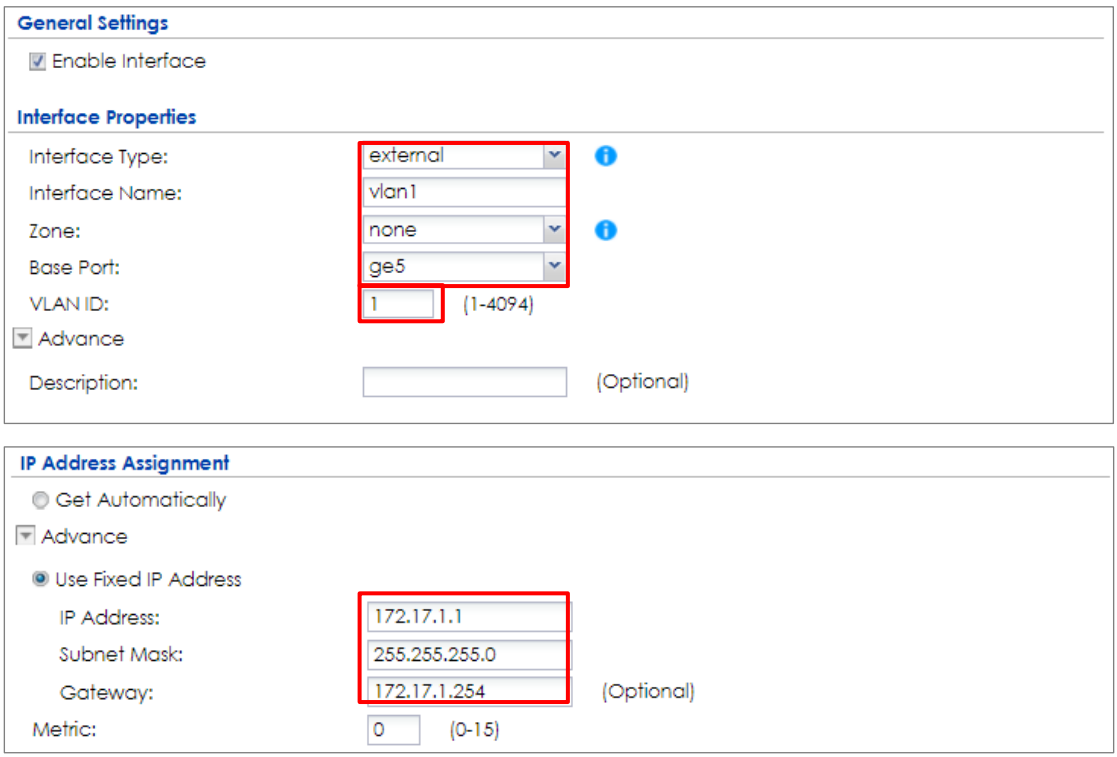
In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Port Grouping**, select the ports that you want to assign to a representative Interface (in this example, **Port 4** and **Port 5** are configured as **ge5**).

CONFIGURATION > Network > Interface > Port Grouping

Set Up the VLAN on the ZyWALL/USG

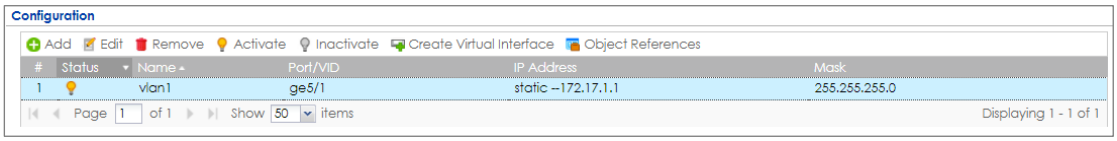
In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > VLAN**. Set **Interface Type** to be **External**. Set **Zone** to be **WAN**, configure **Base Port** to be **ge5**. Enter the **VLAN ID** and configure the fixed IP address (172.17.1.1/24 in this example). Click **OK** to go back to the **Configuration** page.

CONFIGURATION > Network > Interface > VLAN

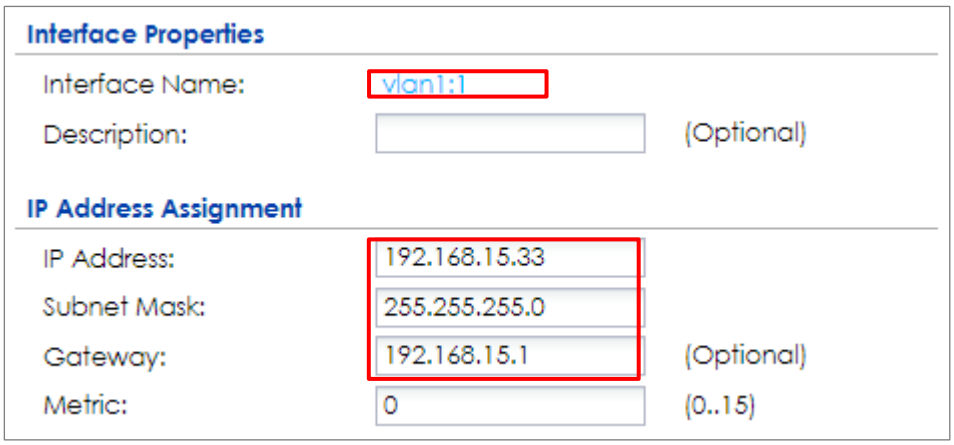


In the **Configuration** page, select the **vlan1** entry and click **Create Virtual Interface** on the upper bar. Configure the Fixed IP address (192.168.15.33/24 in this example). Click **OK**.

CONFIGURATION > Network > Interface > VLAN > vlan1



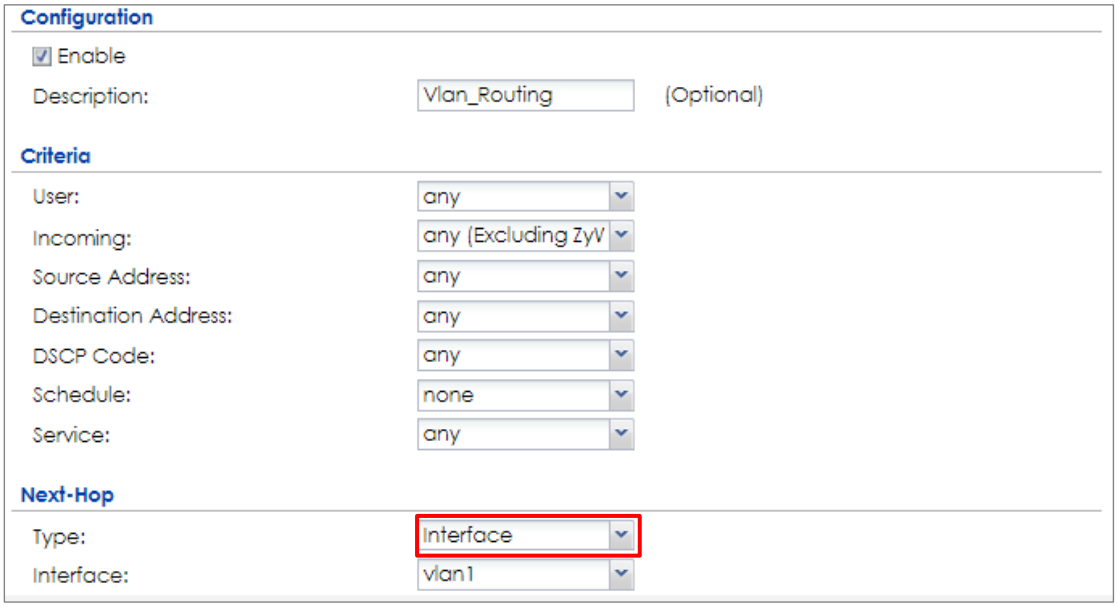
CONFIGURATION > Network > Interface > VLAN > vlan1:1



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**.

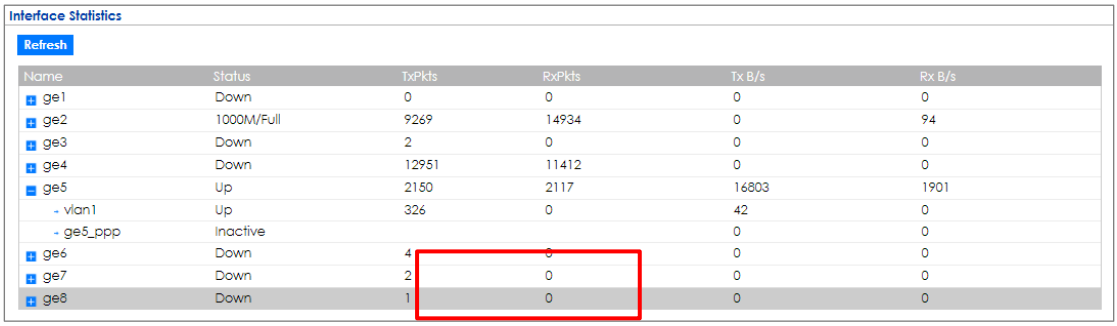
CONFIGURATION > Network > Routing



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



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

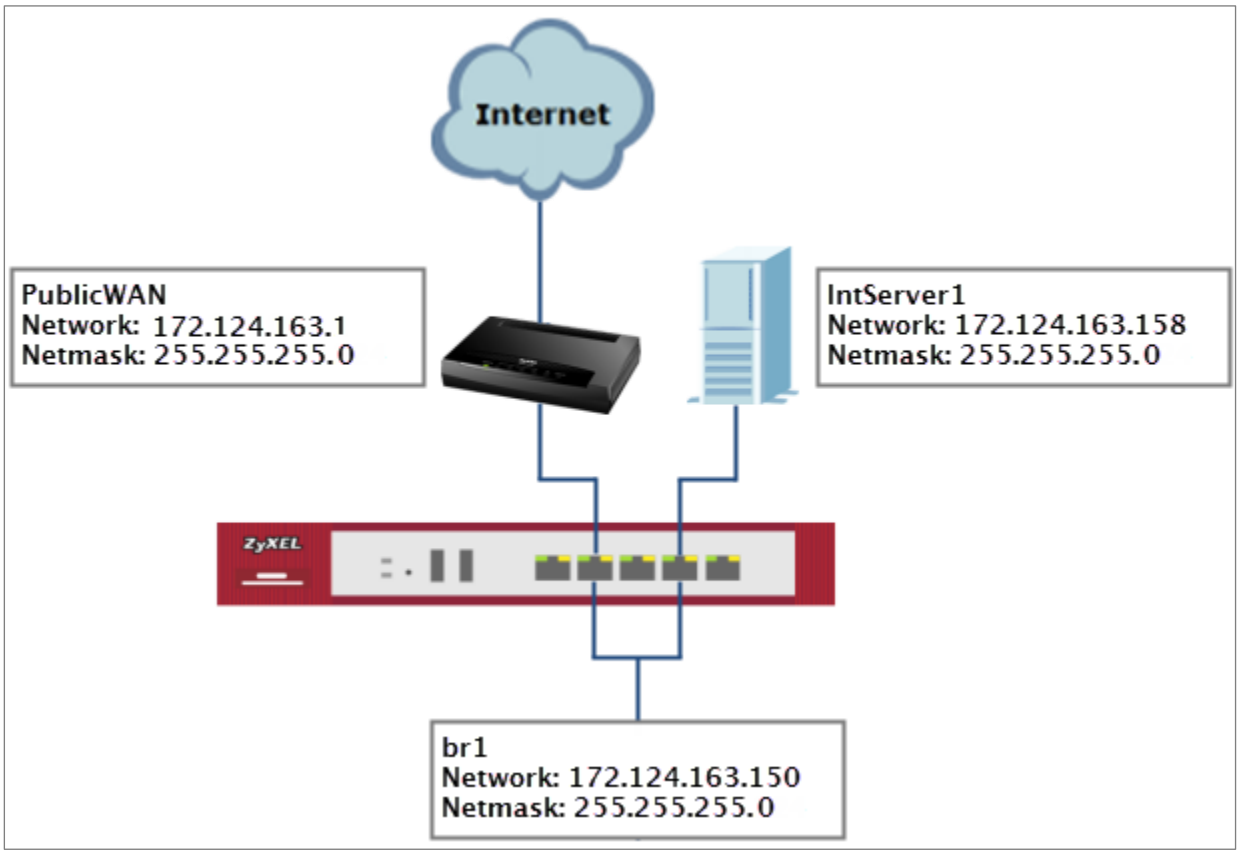
What Could Go Wrong?

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



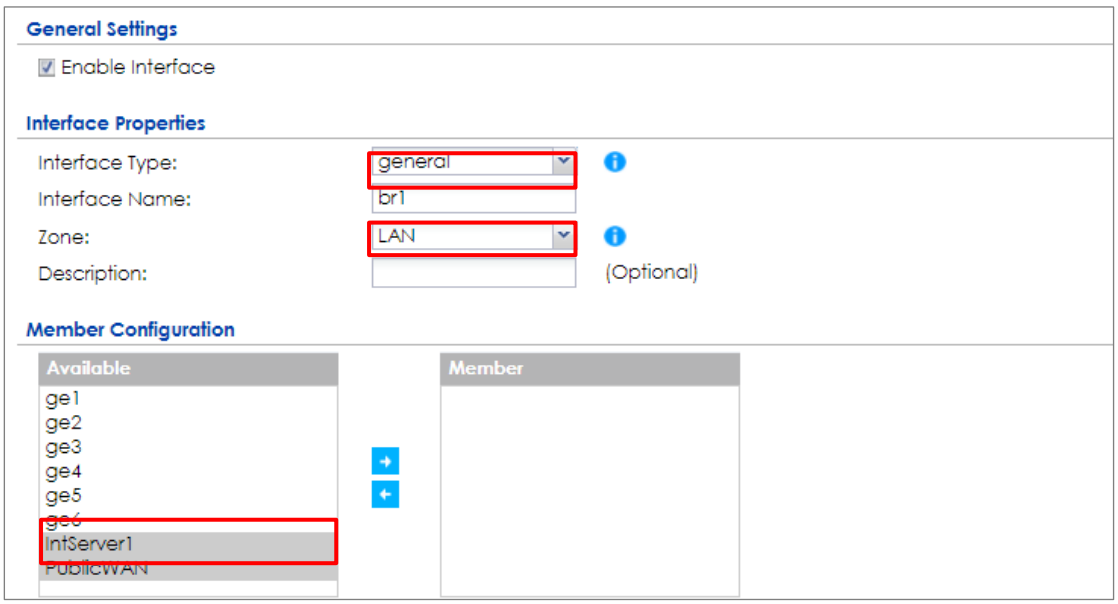
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

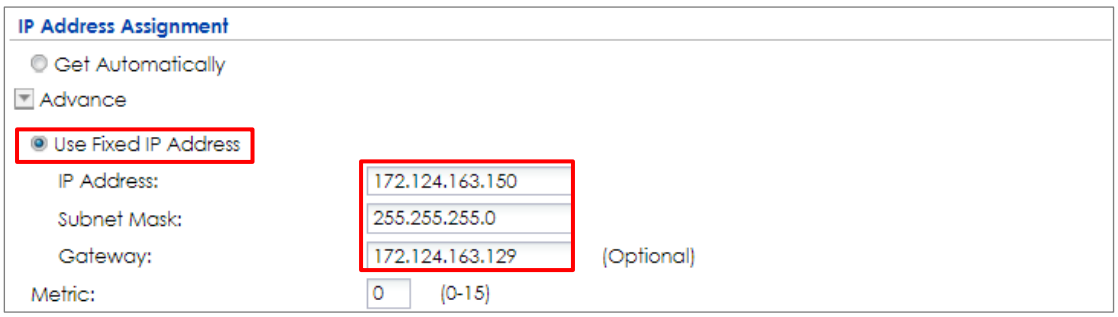
Set Up the Bridge Interface on the ZyWALL/USG

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





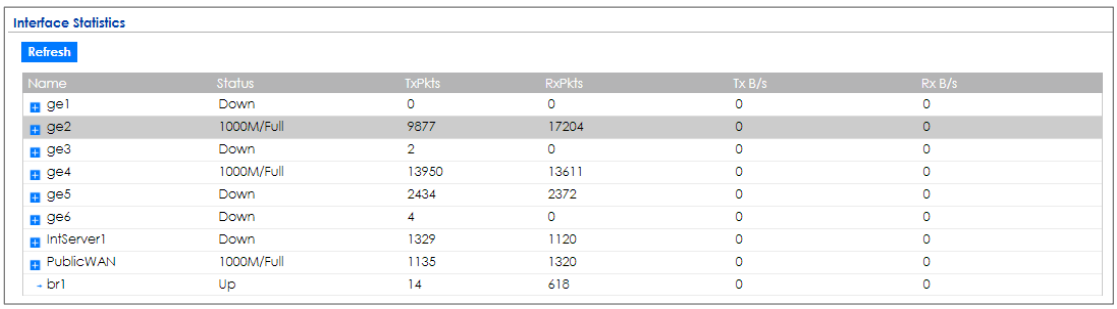
After creating the bridge interface, connect the server's network cable to **IntServer1** port and set the server's IP to be in the same subnet (172.124.163.158 in

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.

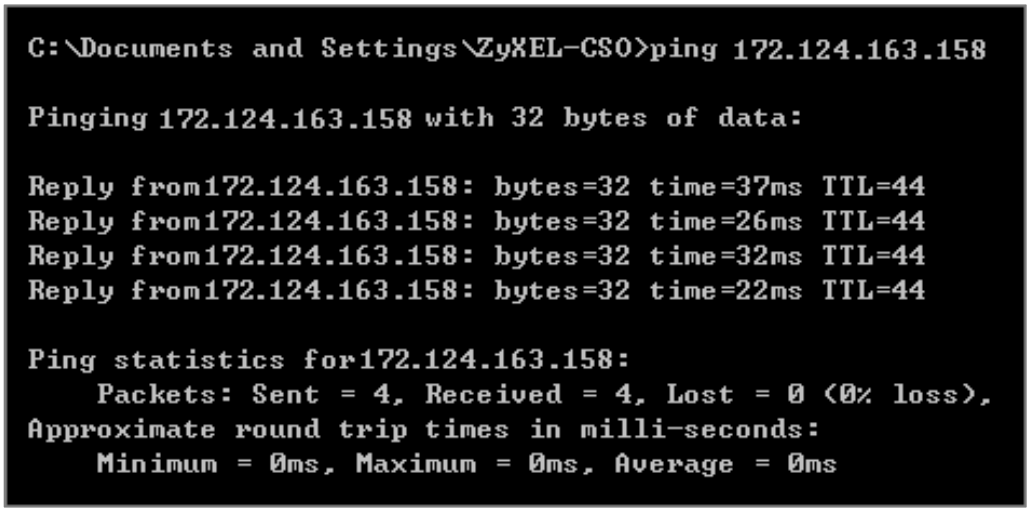
MONITOR > Interface Status > Interface Statistics



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



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.

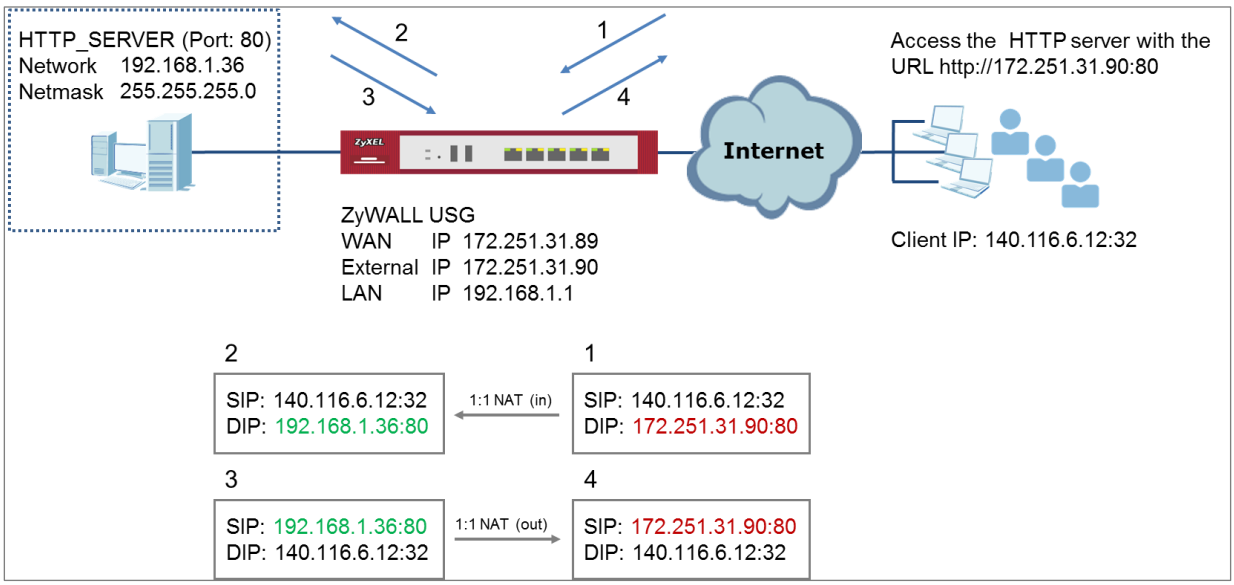
ZYXEL

www.zyxel.com

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

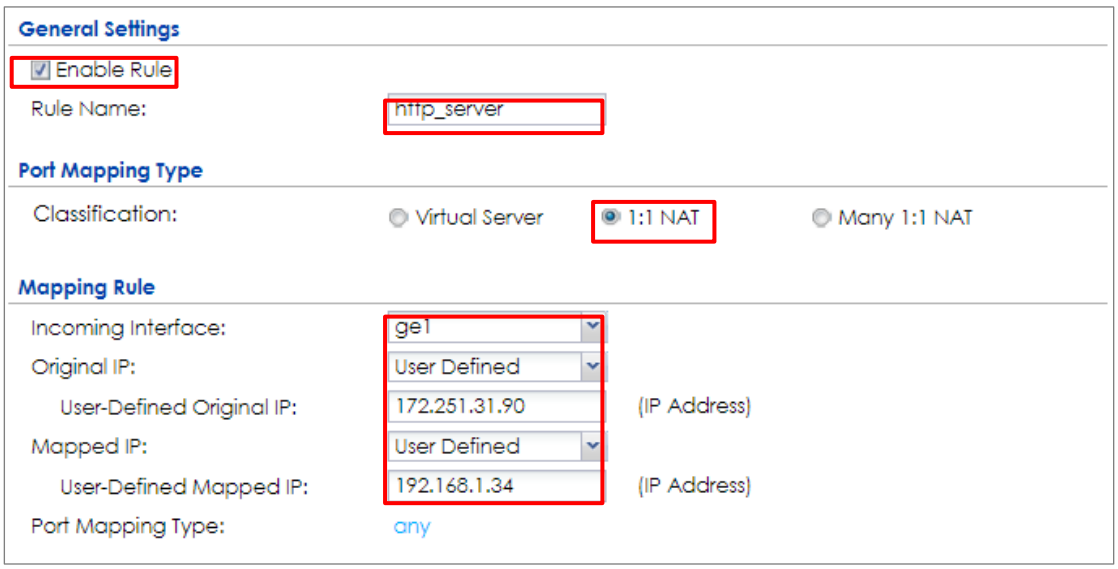


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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**.

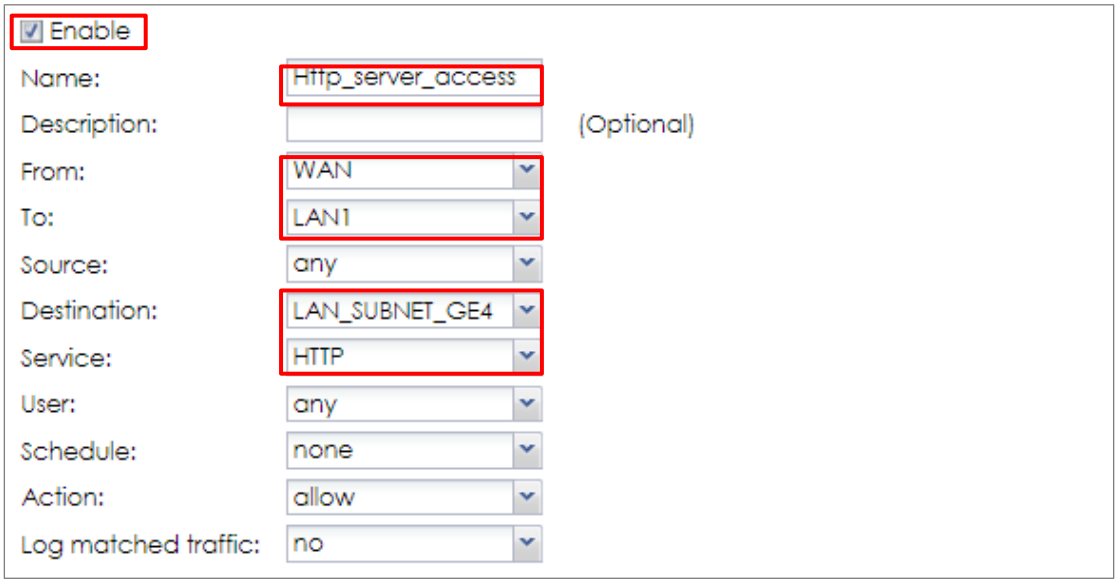
CONFIGURATION > Network > NAT > add NAT



Set Up the Security Policy on the ZyWALL/USG

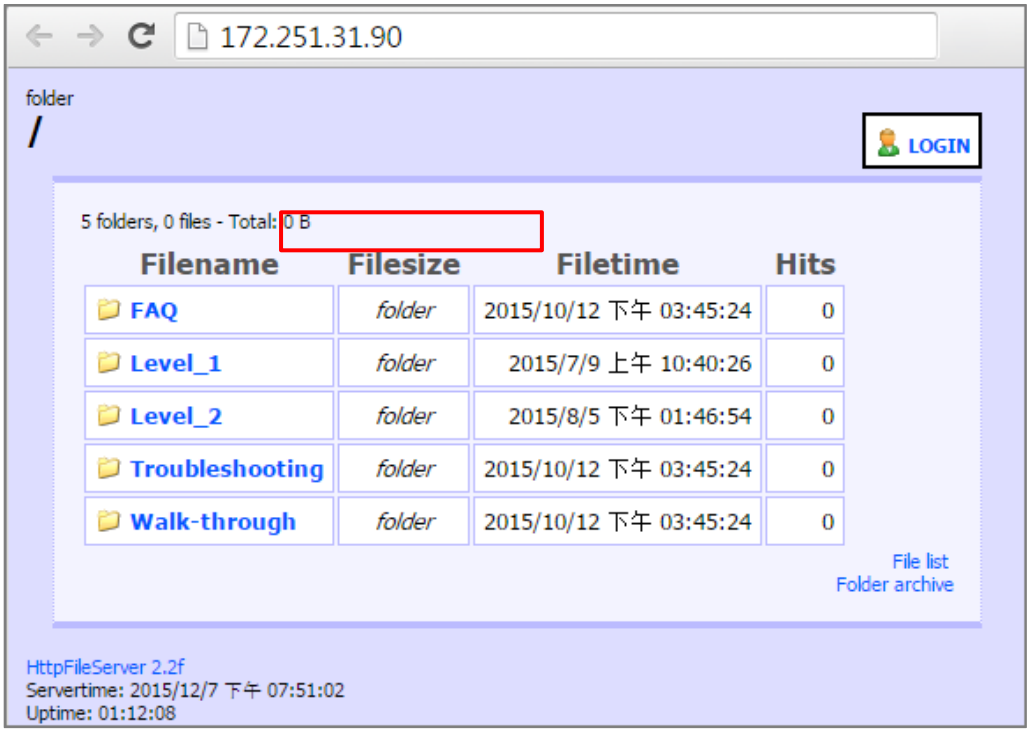
In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control > add corresponding**, select **Enable**. Configure a Name for your to identify the security policy (http_server_access in this example). Set **From: WAN** and **To: LAN1**. Set **Destination** to the lan subnet where your server is (LAN_SUBNET_GE3 in this example). Set **Service** to **HTTP**, set **Action** to **allow**. Click **OK**.

CONFIGURATION > Security Policy > Policy Control > add corresponding



Test the Result

Type http://172.251.31.90/ into the browser, it displays the HTTP service page.



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.

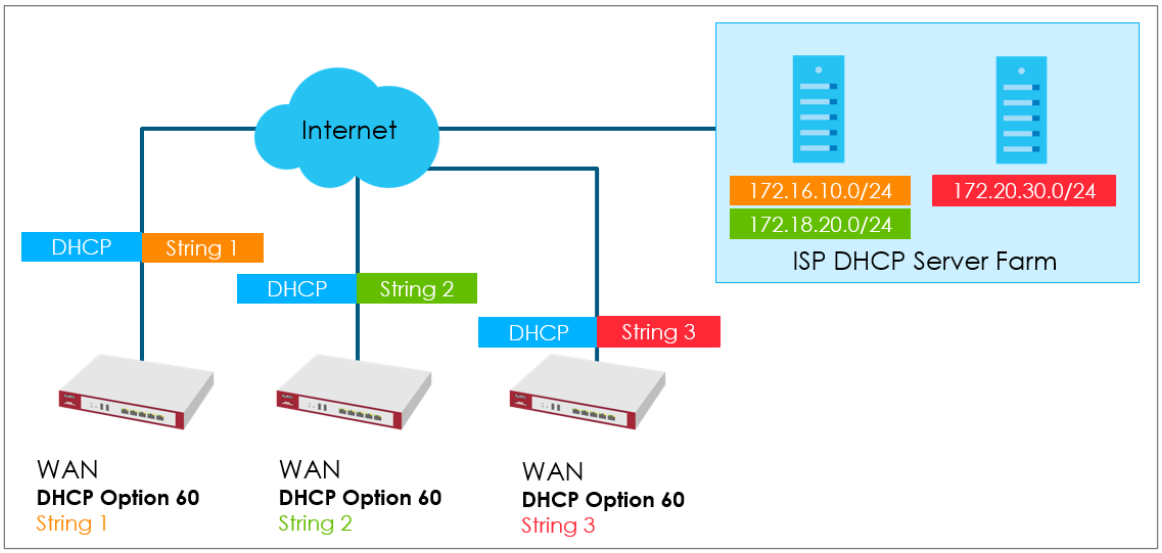


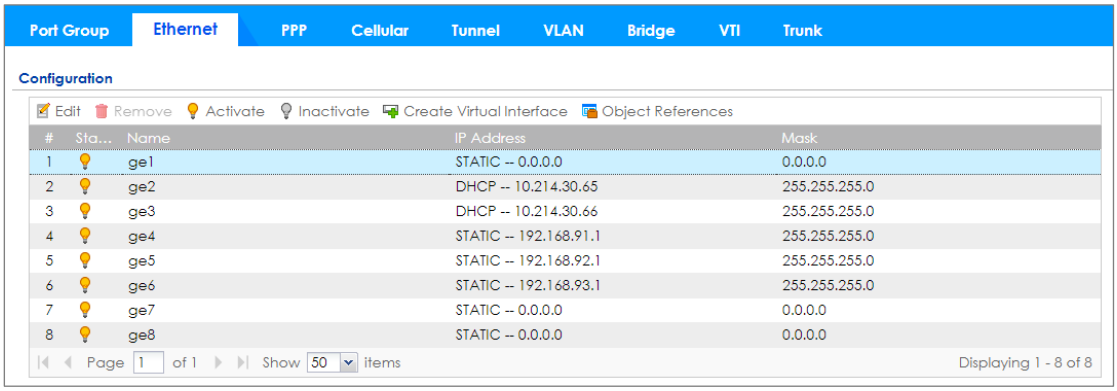
Figure 1 DHCP Option 60 Vendor Class Identifier

DHCP Option 60 Deployment Flow

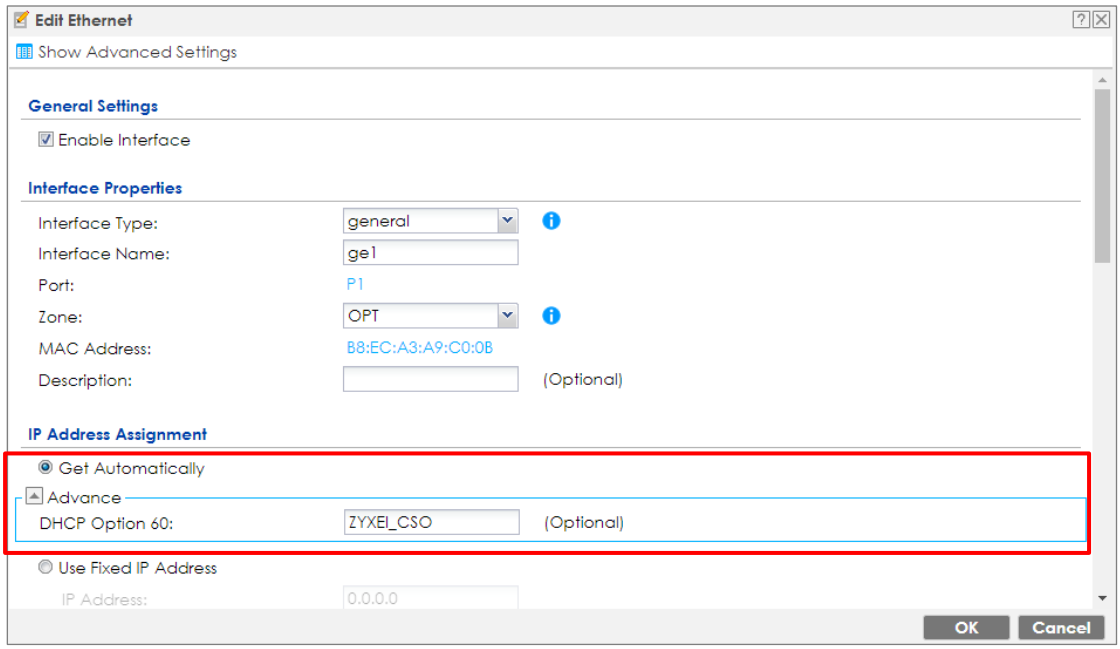
1. Enable the WAN ports as DHCP clients (enabled by default).
2. Navigate to the WAN interface configuration screen.
3. Type in user defined option 60 string in the **Advance** setting section.

Setting Up DHCP Option 60 on the Web GUI

1 In the ZyWALL/USG's navigation panel, go to **Configuration > Network > Interface**.



2 Click the **Ethernet** tab, go to **WAN > Edit**. Enter the VCI string in the **Advance** section of **DHCP Option 60**.



Setting Up DHCP Option 60 on the CLI

Under the specific interface path, use these commands to:

Enable option 60

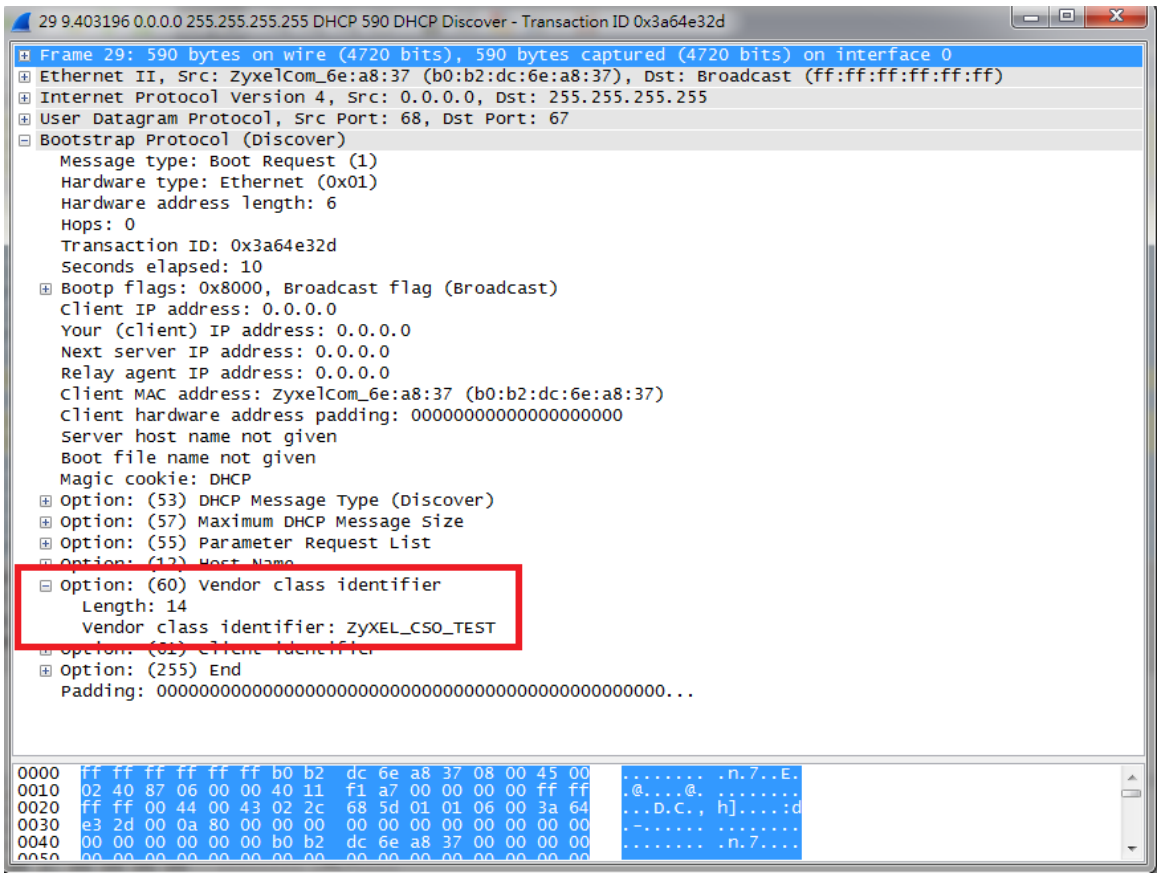
Router(config-if-wan1)# ip address dhcp option-60 {VCI_STRING}

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.



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.

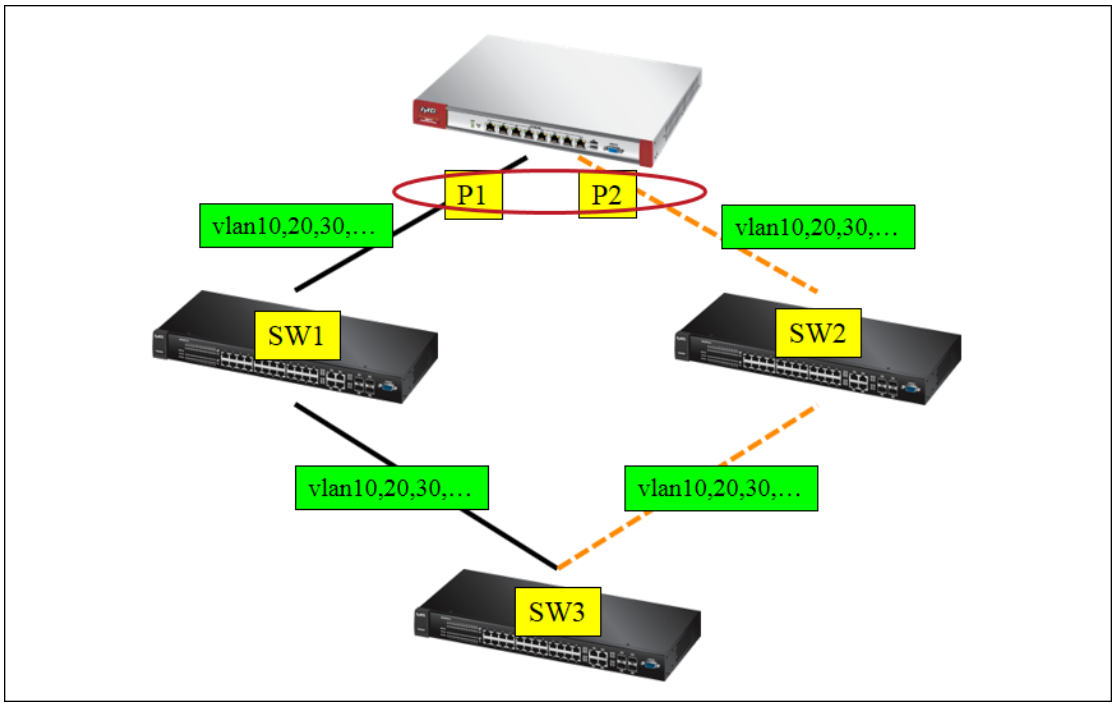
The link aggregation supported models have Active-backup, 802.3ad (LACP), and Balance-alb modes. Link aggregation supports IPSec tunnel, VLAN, and bridge interface.

Device HA Pro is supported on the LAG interface.

Set up the Active-backup, 802.3ad, Balance-alb

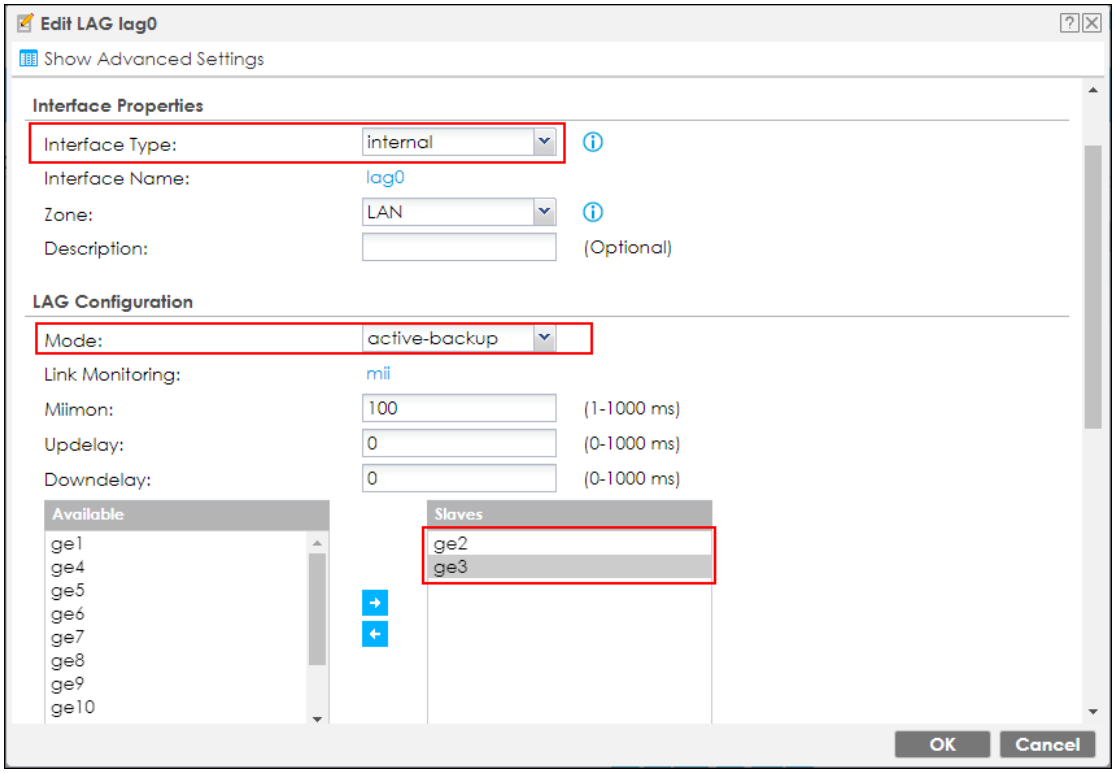
Active-backup Mode:

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



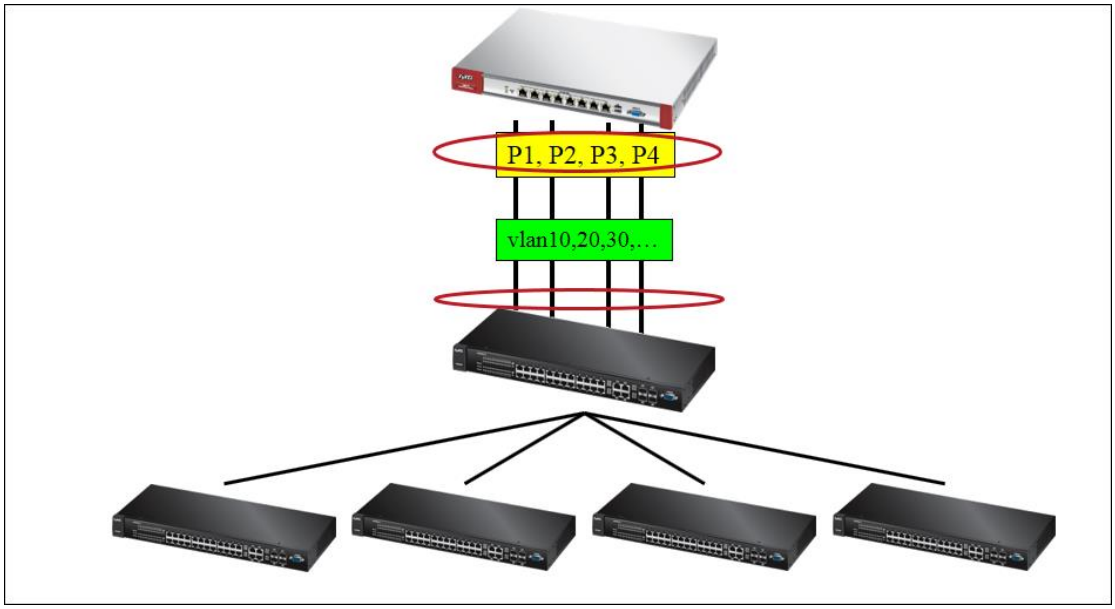
Only the USG needs to be configured. You do not need to change any settings on the switch.

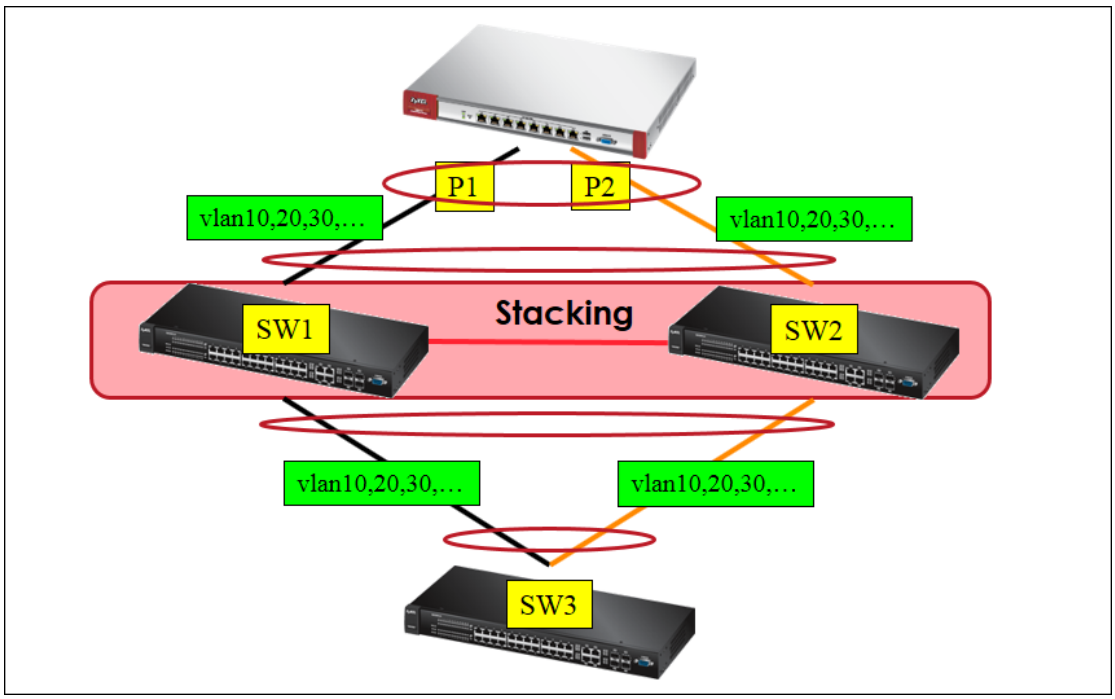
On the USG, go to **Configuration > Network > Interface > LAG**.
Choose the proper interface type and zone depending on the case. Also, select the slave ports that will be added in the LAG interface.



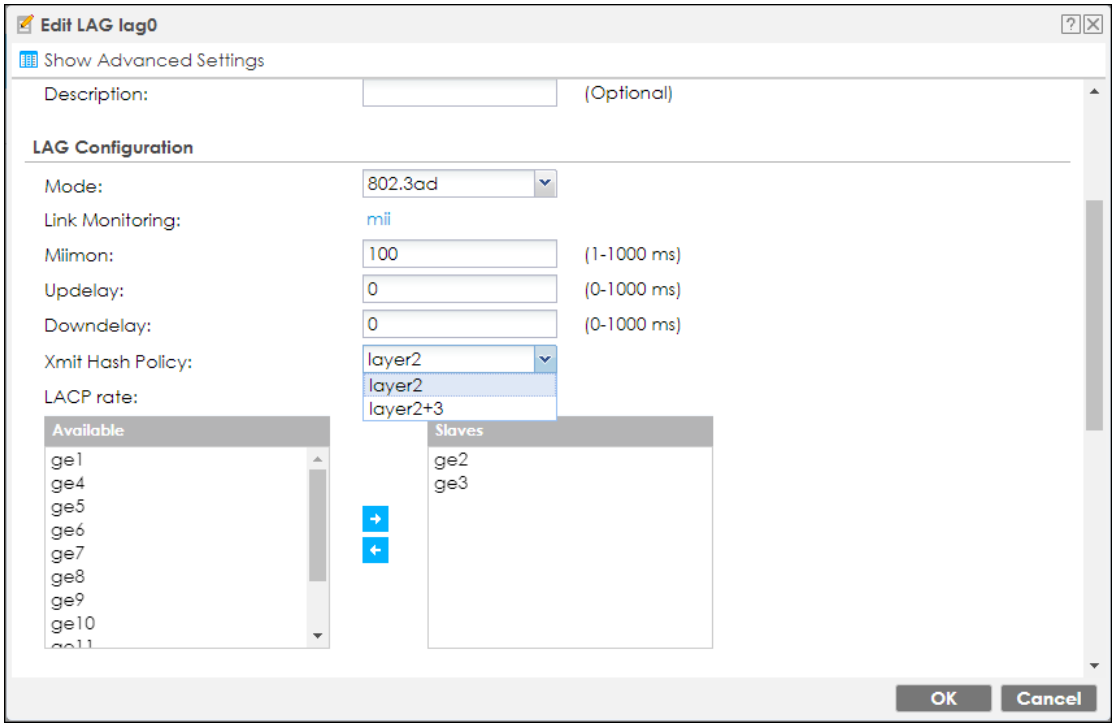
Link Monitoring: Mii monitoring monitors the state of the local interface.
Updelay is the time to wait to enable the slave port after the device detects the link recovery.
Downdelay is the time to wait to disable the slave port after the device detects the link failure.

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.

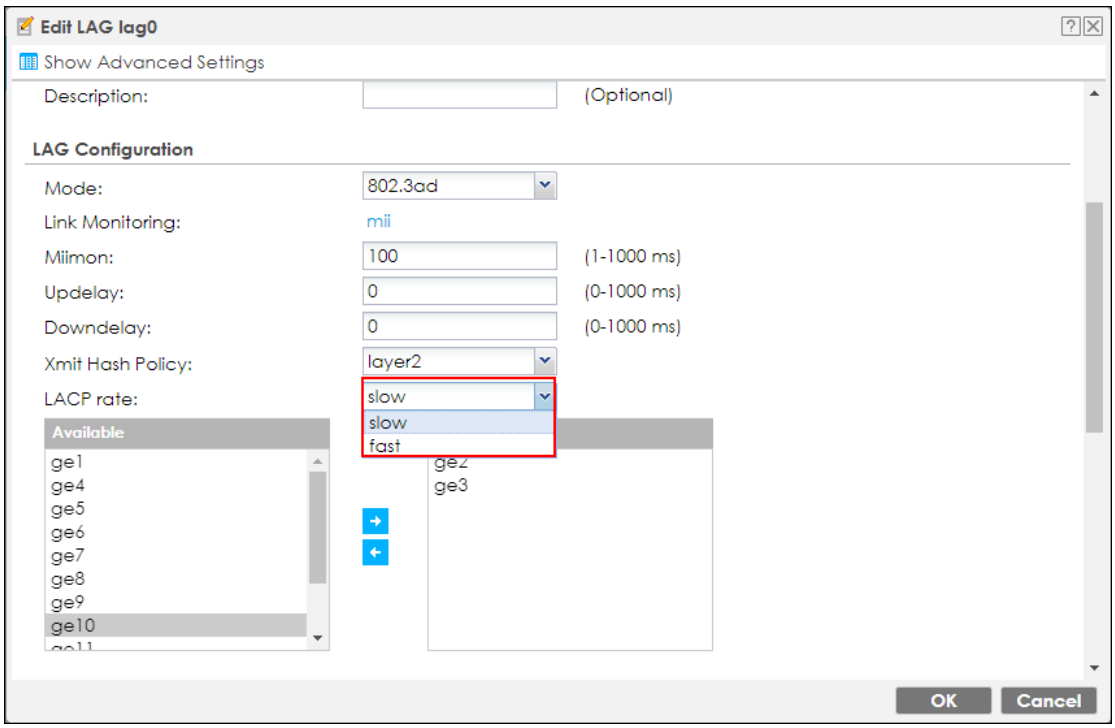


Xmit Hash Policy:

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.

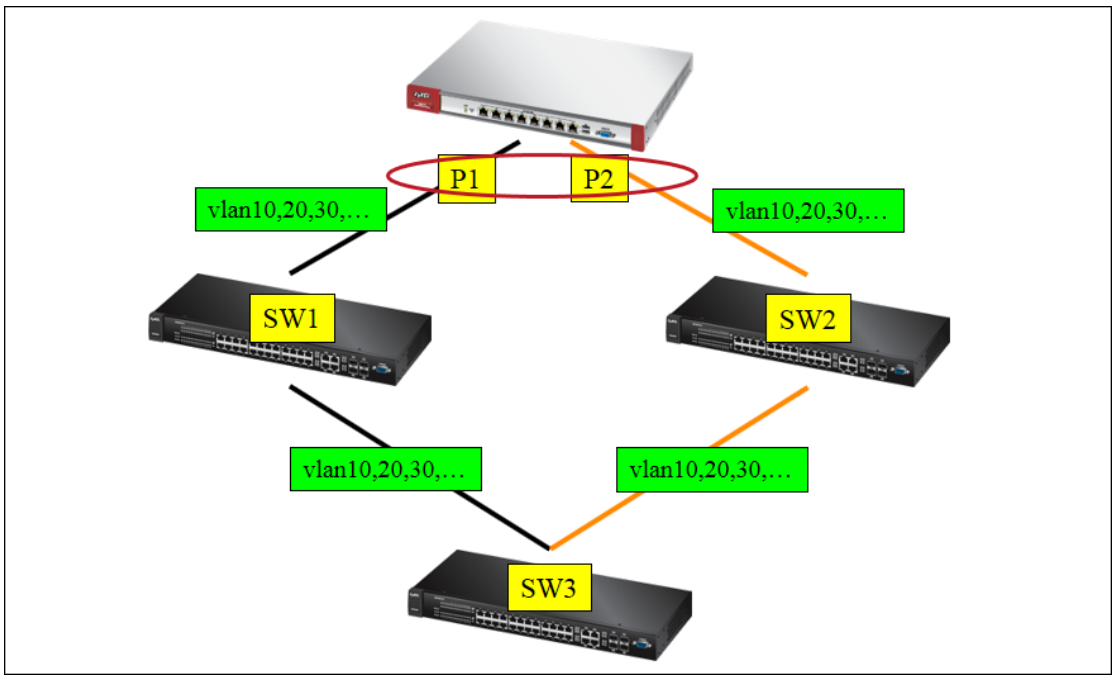


LACP rate:

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

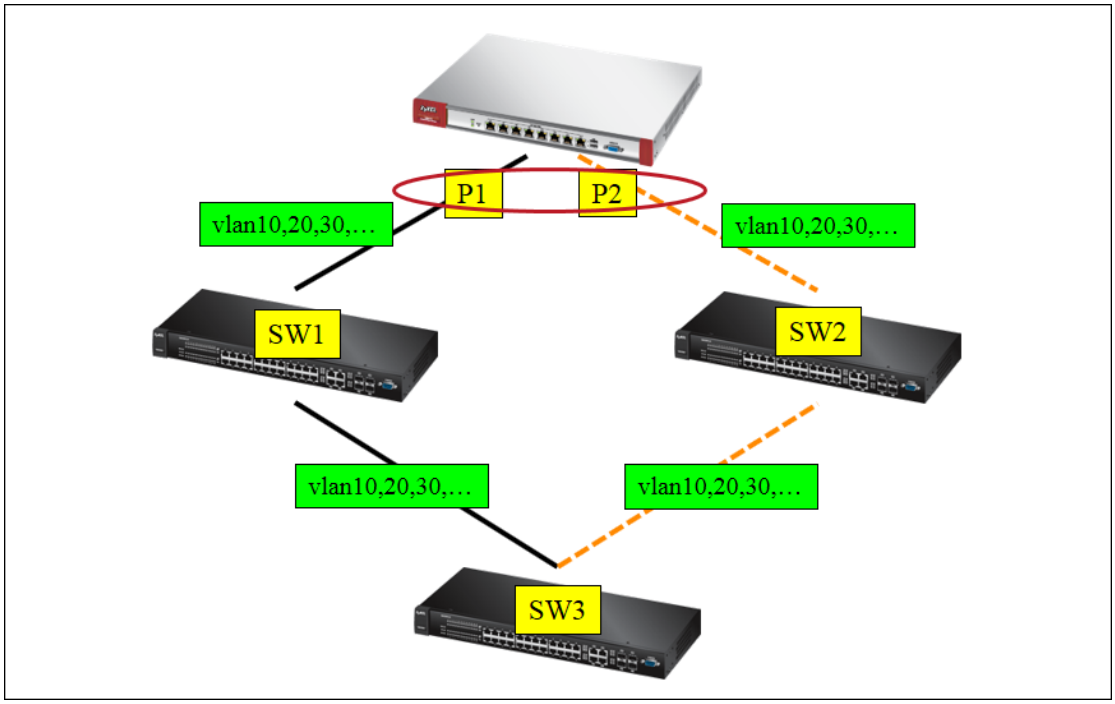
Balance-alb Mode:

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

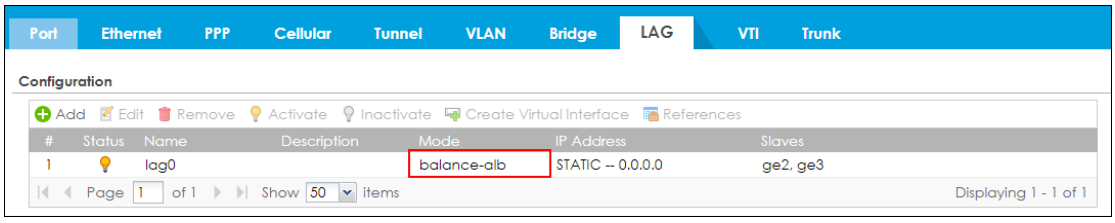


Set up the balance-alb mode.

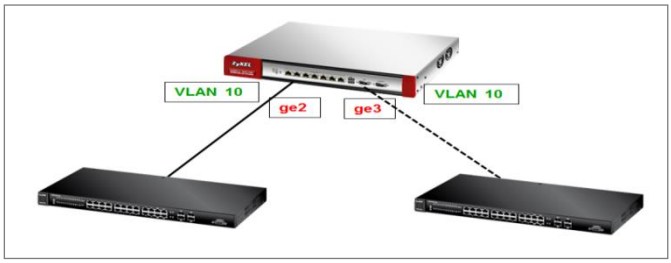
The VLAN interface is cross-connected to different switches and the link statuses on both switches are active.



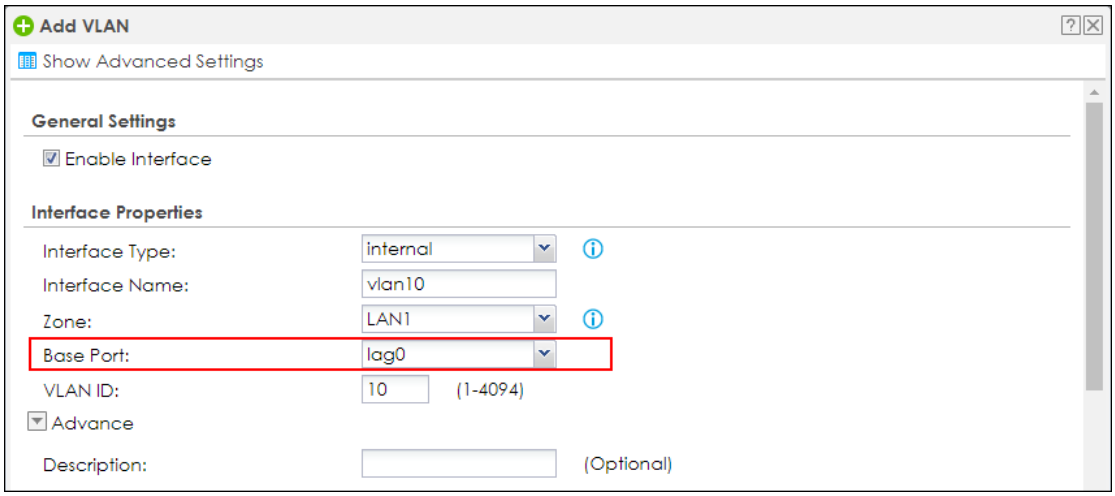
In this case, the LAG interface mode must be set to **Balance-alb**.



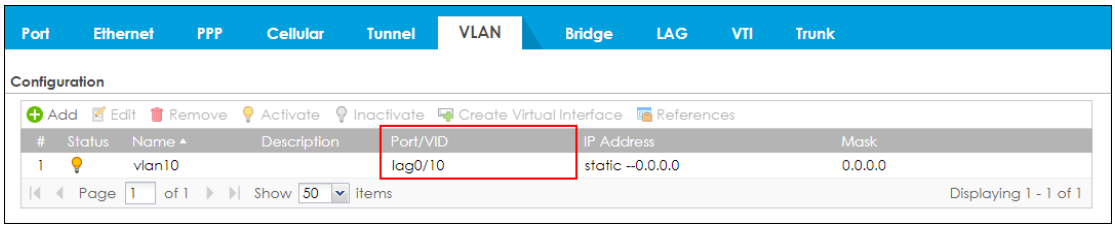
The VLAN interface is cross-connected to different switches (fault tolerance).



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



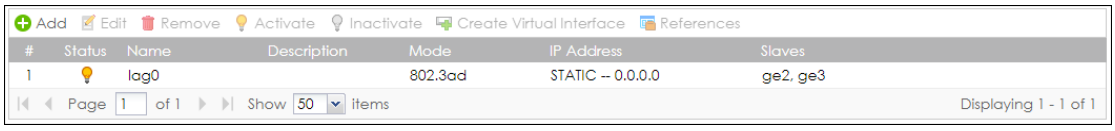
You can find the LAG interface in the VLAN interface.

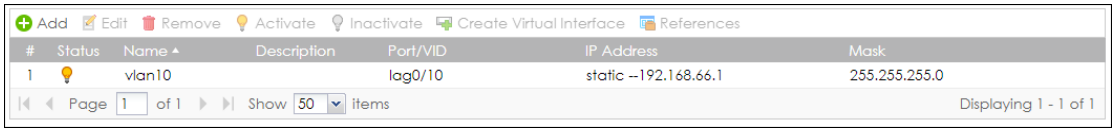


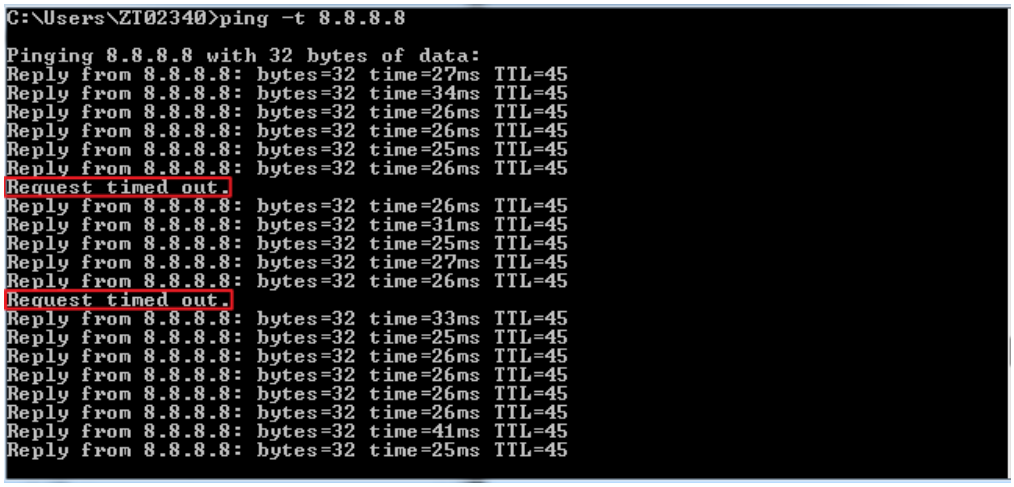
Test the Result

After the deployment you can see the interface status through **Monitor>interface Status**

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.





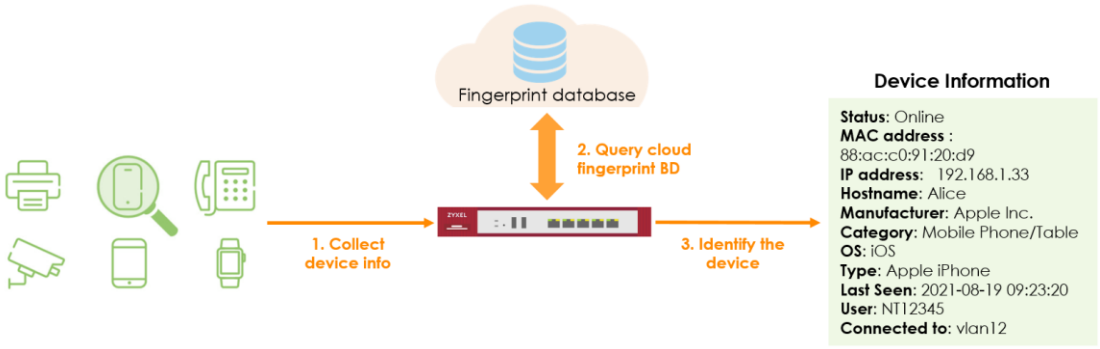


What can go wrong

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.

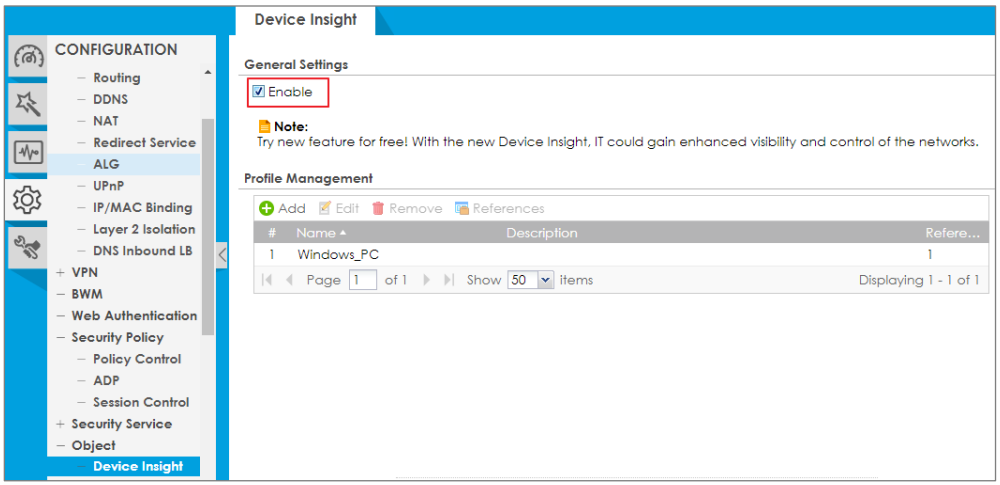
How to configure Device Insight

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.

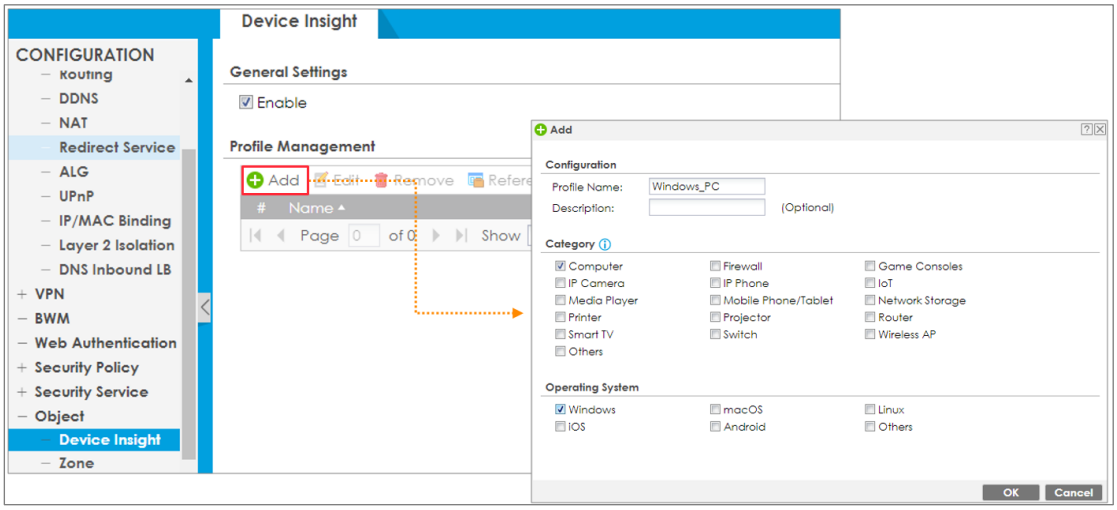


Enable Device Insight and create profile

In the Web GUI, go to **Configuration > Object > Device Insight**, enable the checkbox

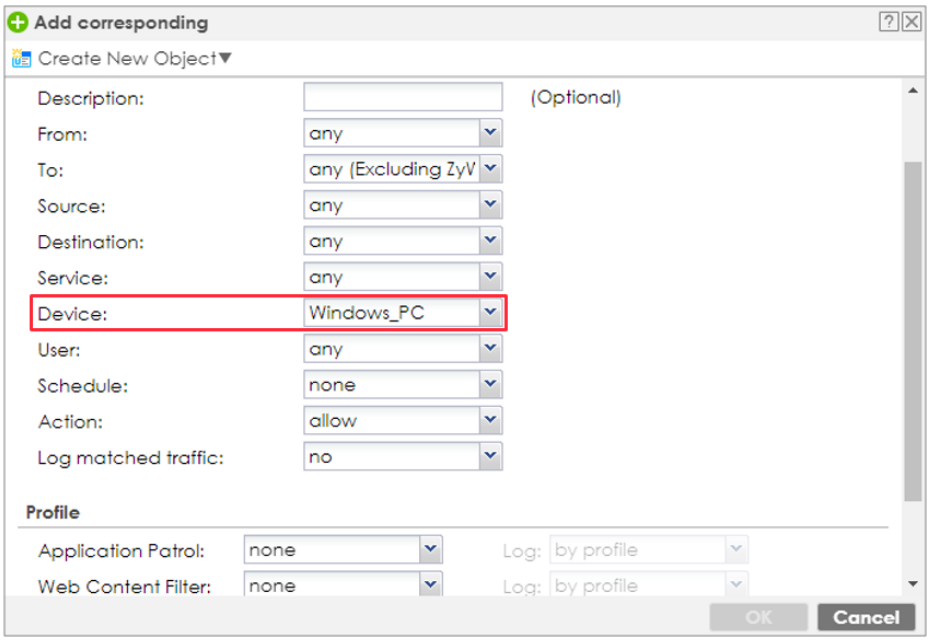


Then, click to Add button to create a new profile, select the device based on category and operating system you want to manage.



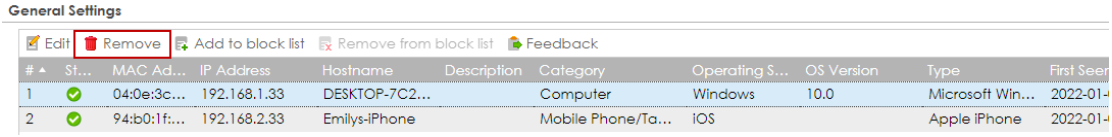
Apply the Device Insight profile to policy control

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.



Remove selected device from the table

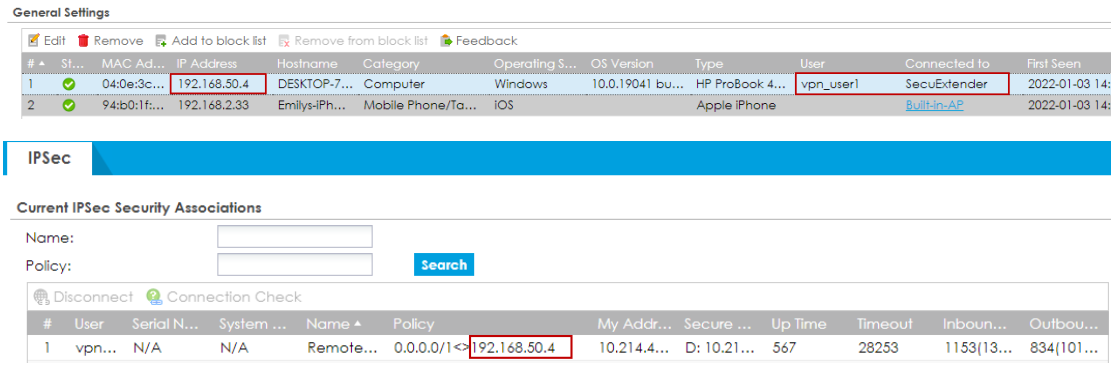
Go to **Monitor > Network Status > Device Insight**. Select one or more rules and click **Remove** to remove devices from the table. If the device is on the block list, it cannot be removed.



Online status of IPSec VPN client

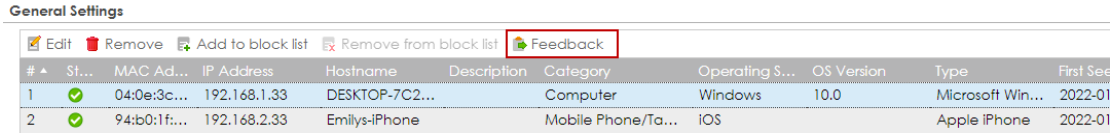
Once the IPSec VPN client is connected and shows on **MONITOR > VPN Monitor > IPSec**, the online status and user name of IPSec VP client display in **MONIOR > Device Insight**.

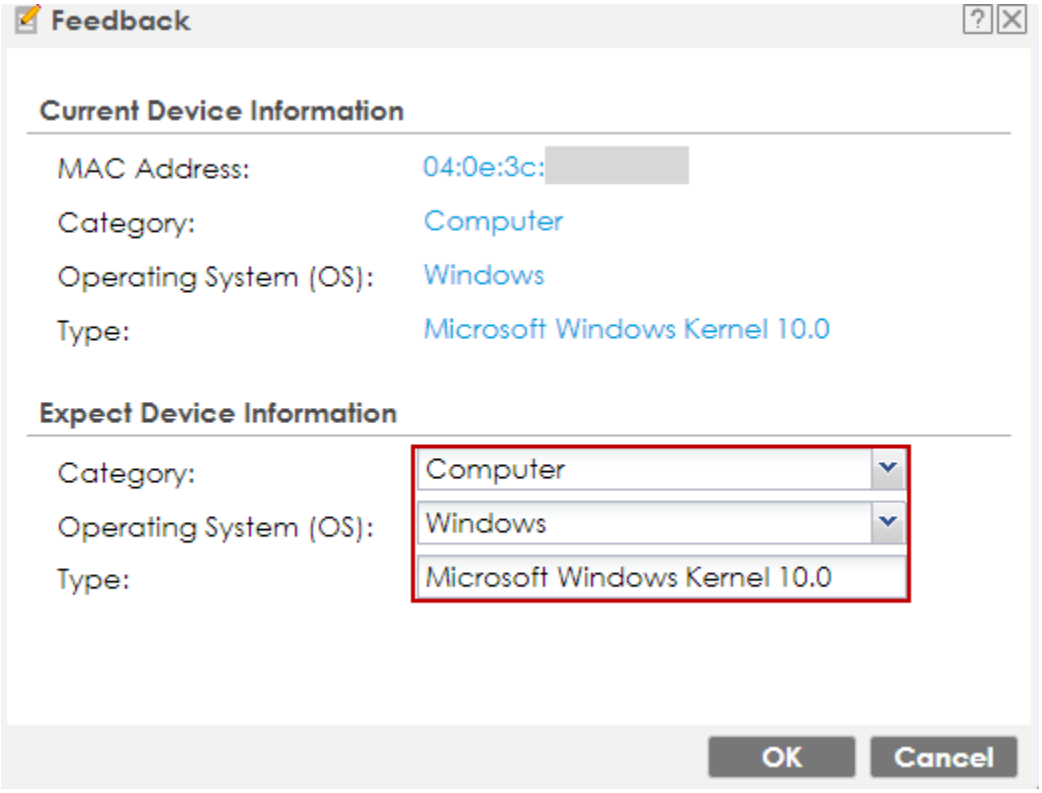
> Note: The version of IPSec VPN client must be IPSec_6.6.86.016(subscription_based) and later version.



Feedback button for Category/OS/Type

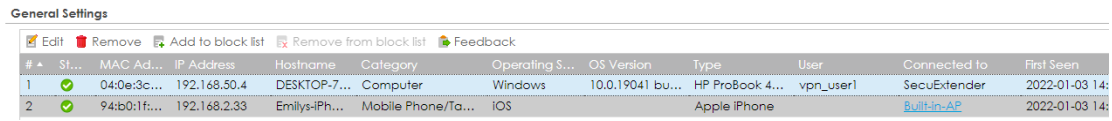
Select one rule and click Feedback to submit the request if Category/OS/Type of the device is incorrect.





Test result

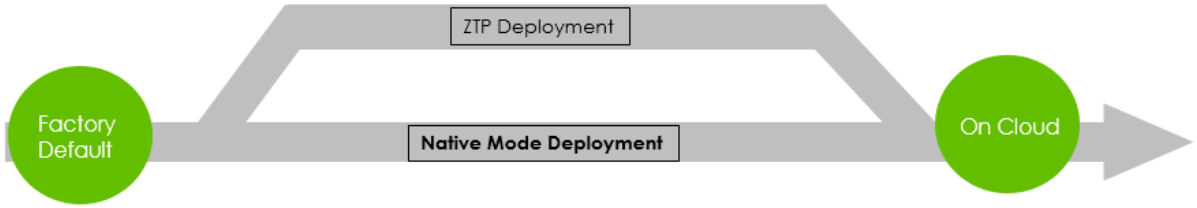
Once you enable Device Insight, gateway starts to collect client device's information, and query the fingerprint database to deeply identify. Go to **Monitor > Network Status > Device Insight**, you can monitor the client device list with their detail information. Based on device info, you also can restrict access by adding to block list.



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

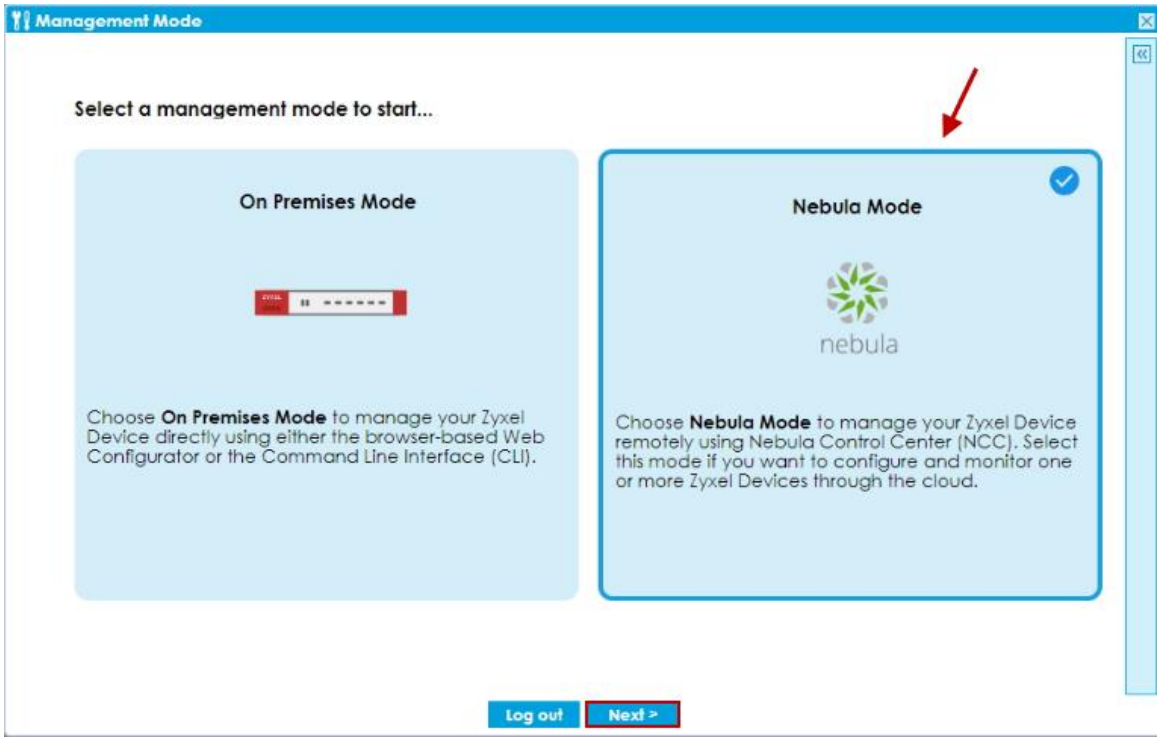
Administrator must locally apply factory default settings by pressing reset button of firewall panel before switching to cloud mode. Only the following settings may be changed and still allow firewall to switch to cloud mode:

1. Default admin account's password
2. WAN settings

Select a management mode: Nebula Mode

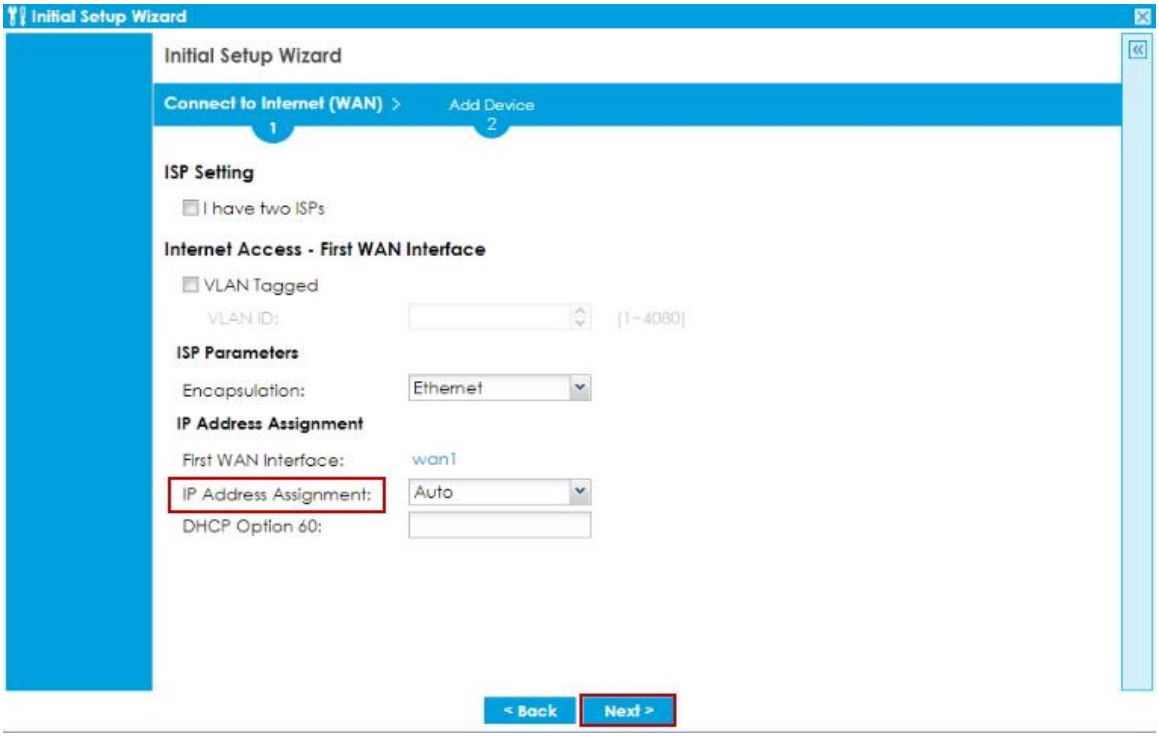
After the device is reset to factory default, access the Setup Wizard via https://192.168.1.1.

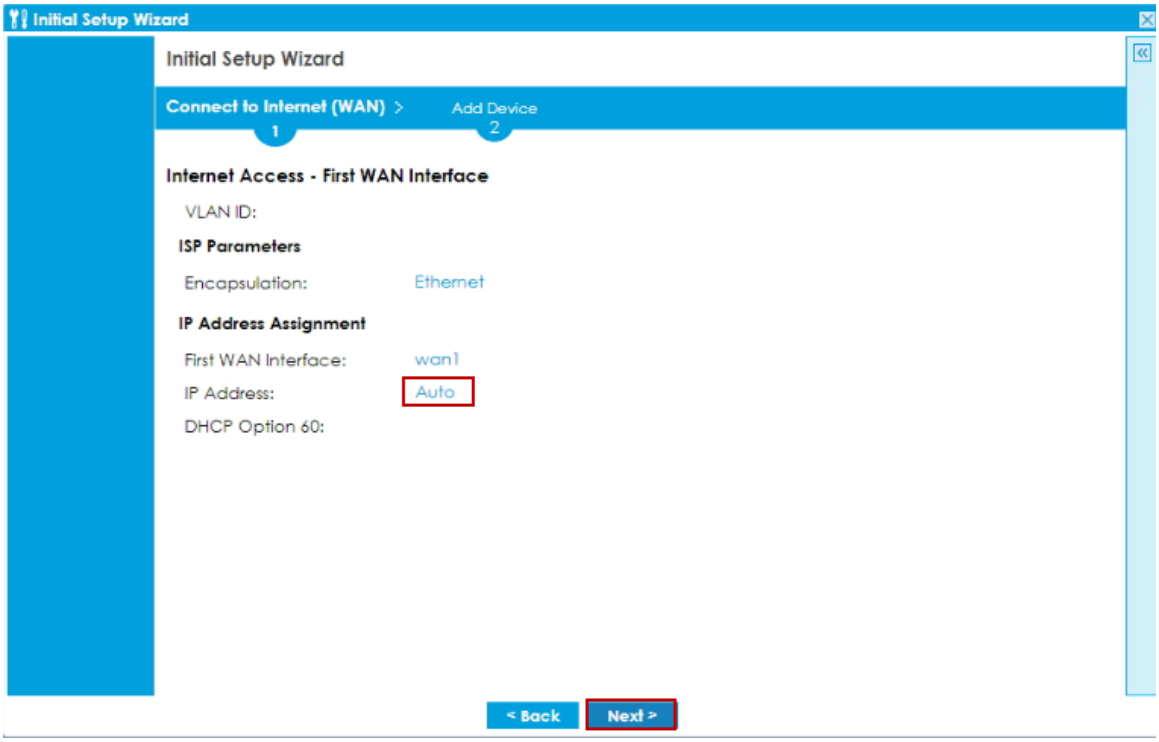
Select **Nebula Mode** and click **Next**.



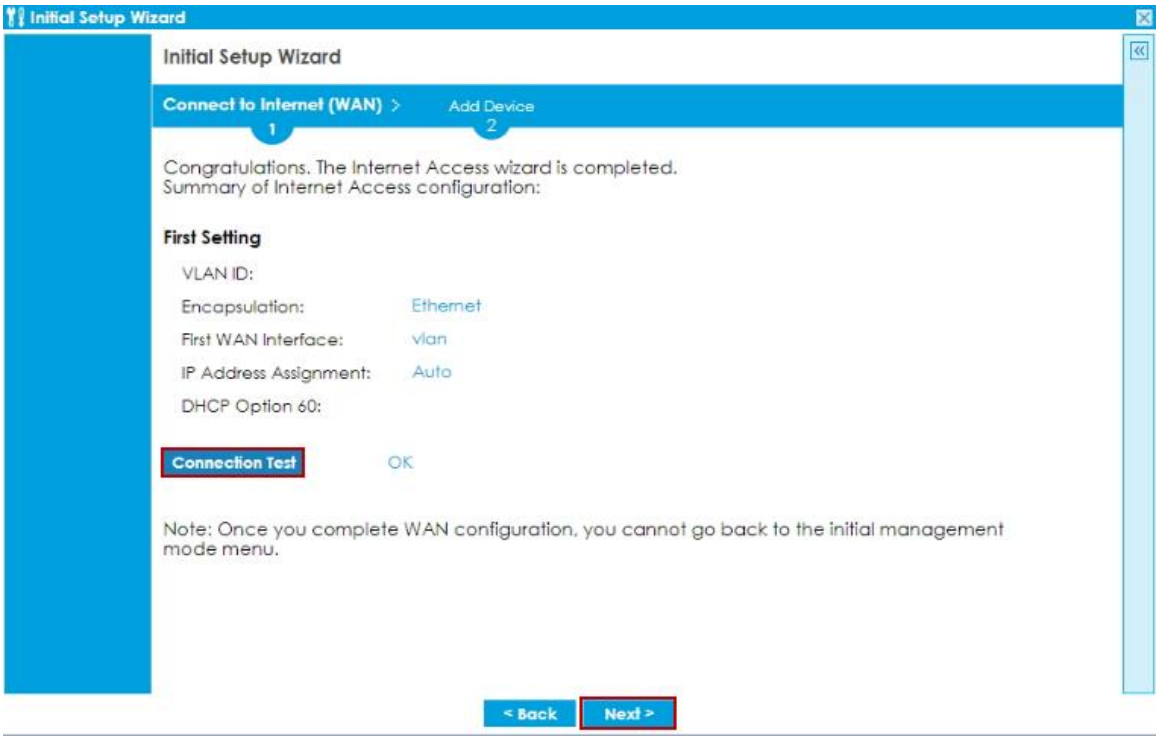
Note: Only device with factory default setting supports management mode selection for the first time login.

Configure WAN settings and click **Next**.

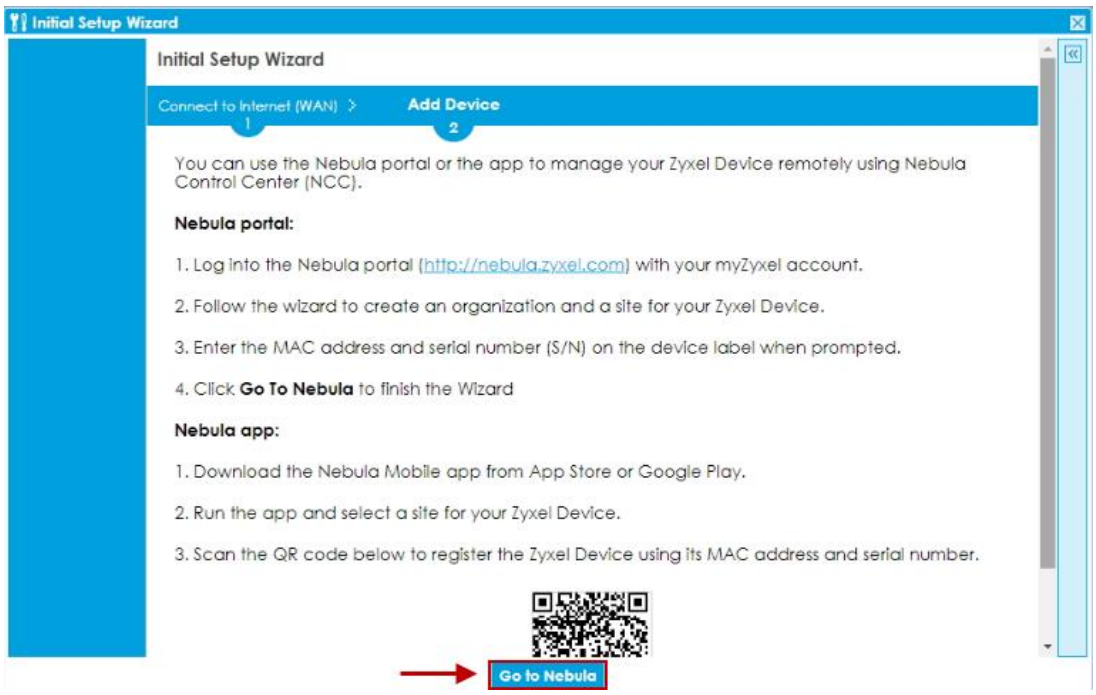




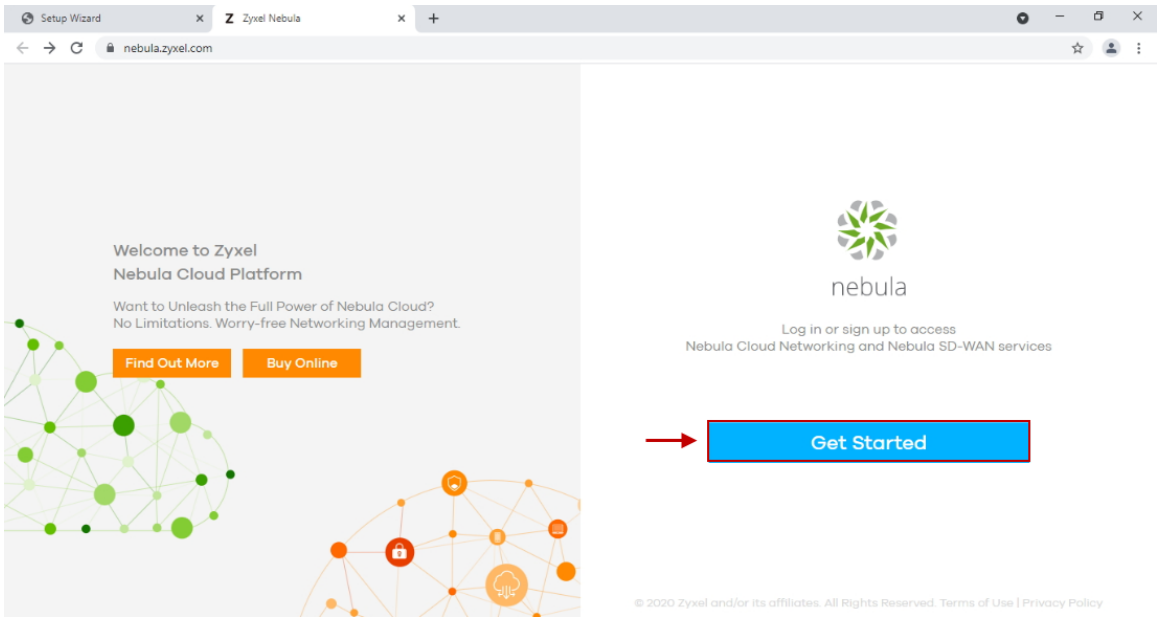
Test wan connection and click **Next**.



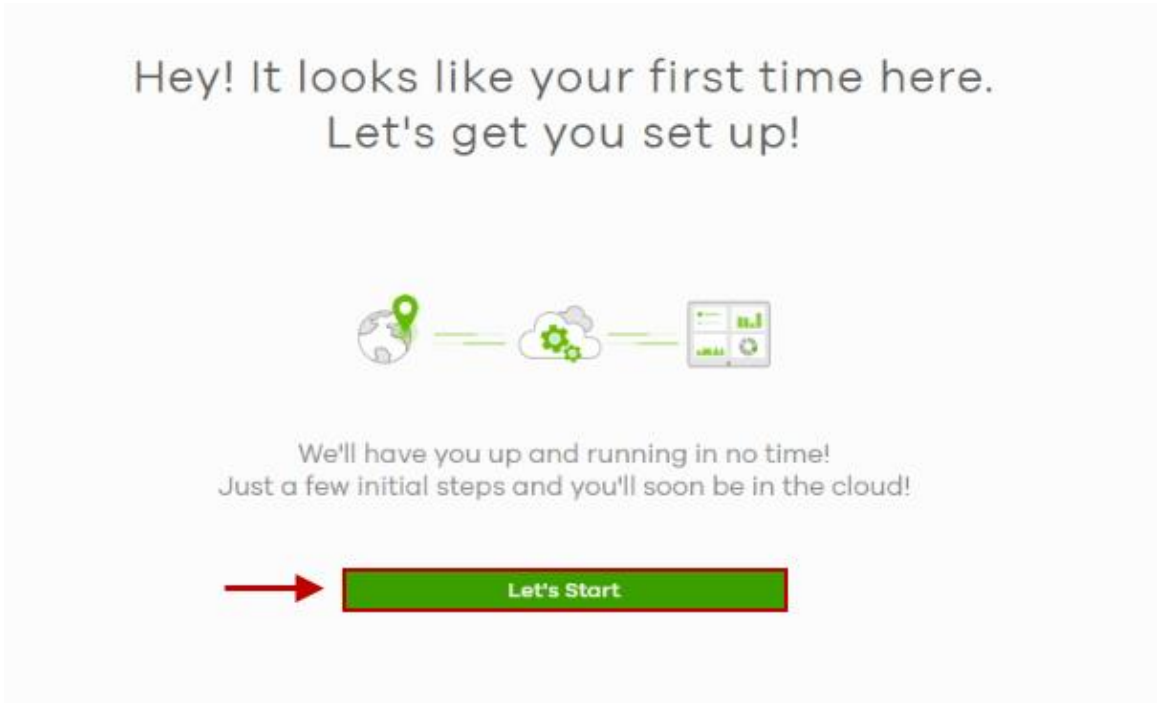
Click **Go to Nebula** to create Organization and Site.



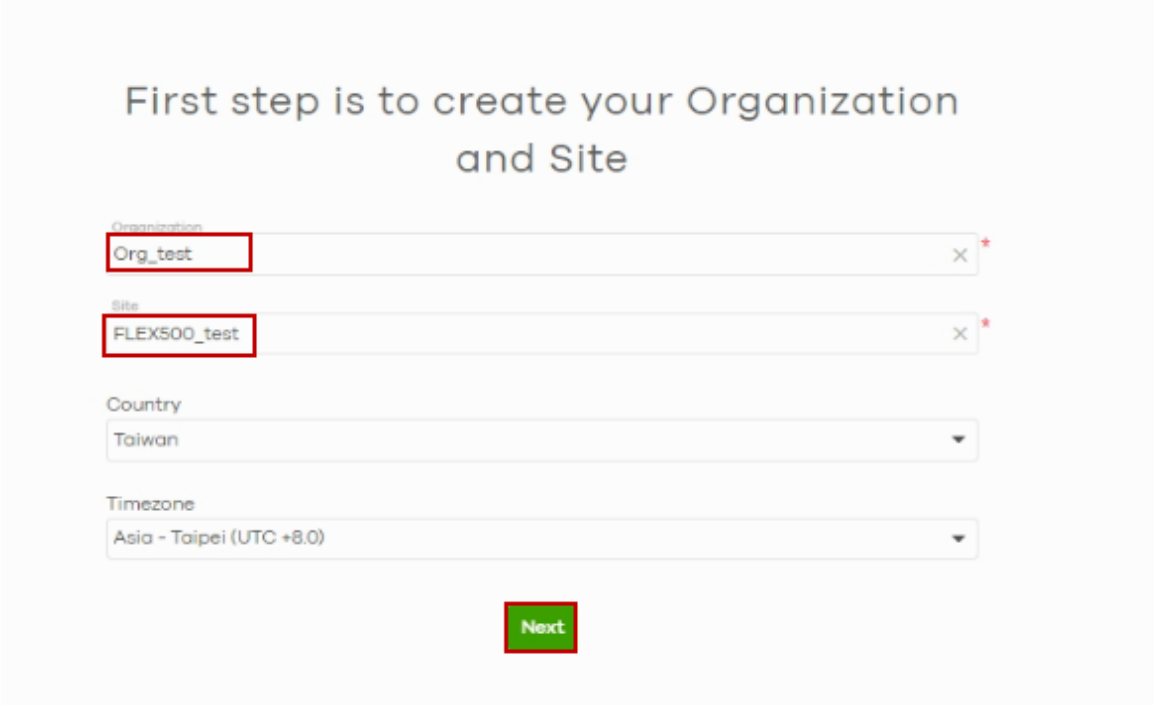
You will be redirected to nebula.zyxel.com. Click **Get Started**.



Start the Nebula wizard and click **Let's Start**.

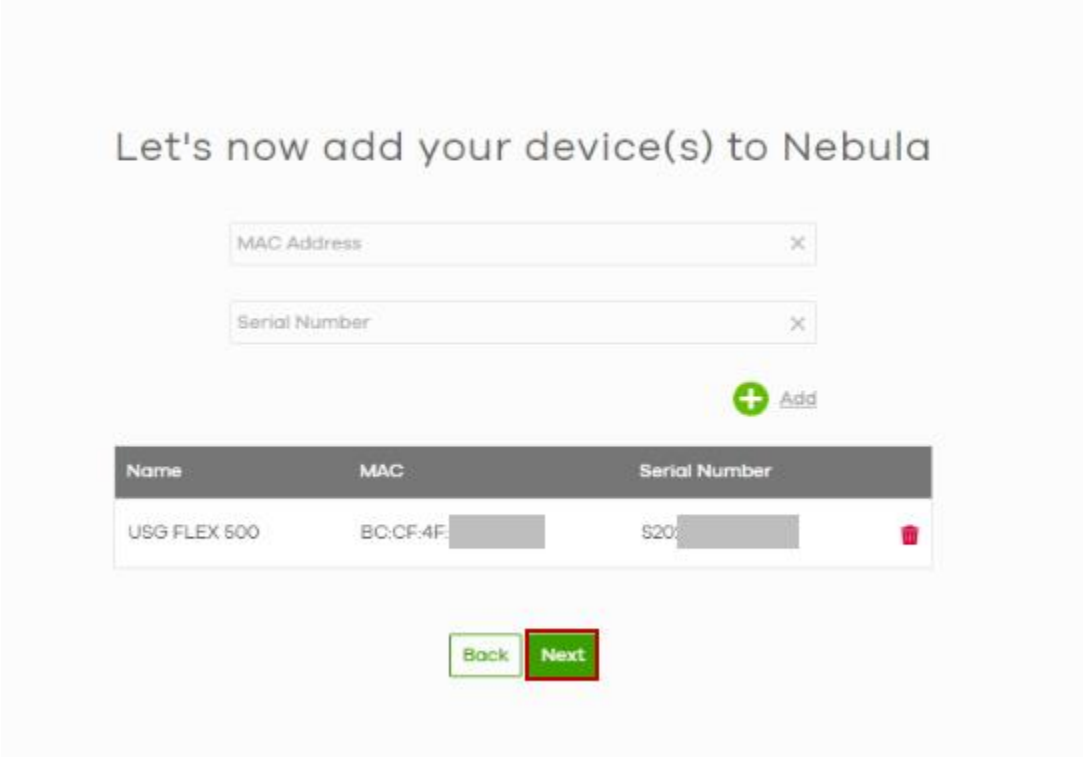


Create the organization and site.

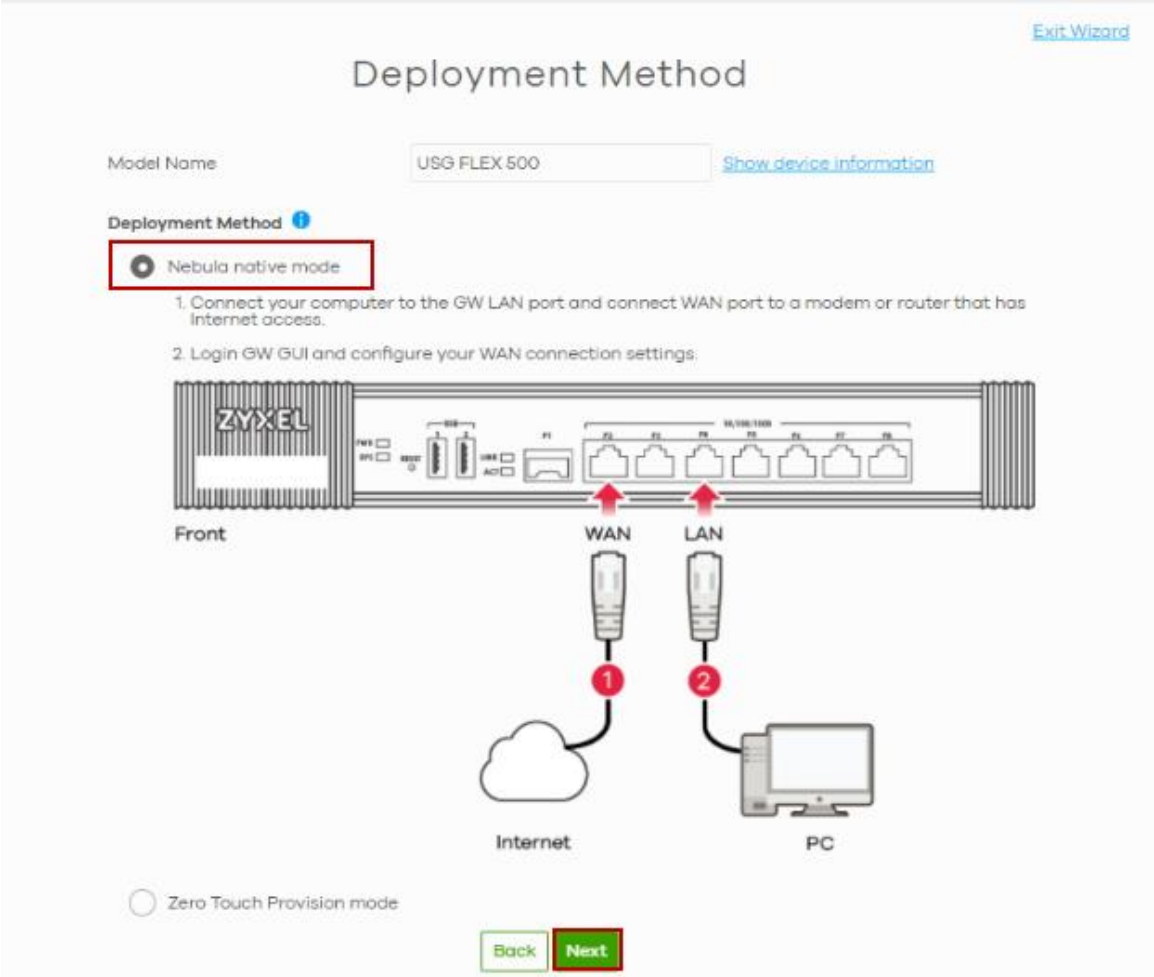


Enter MAC address and Serial number to add device.

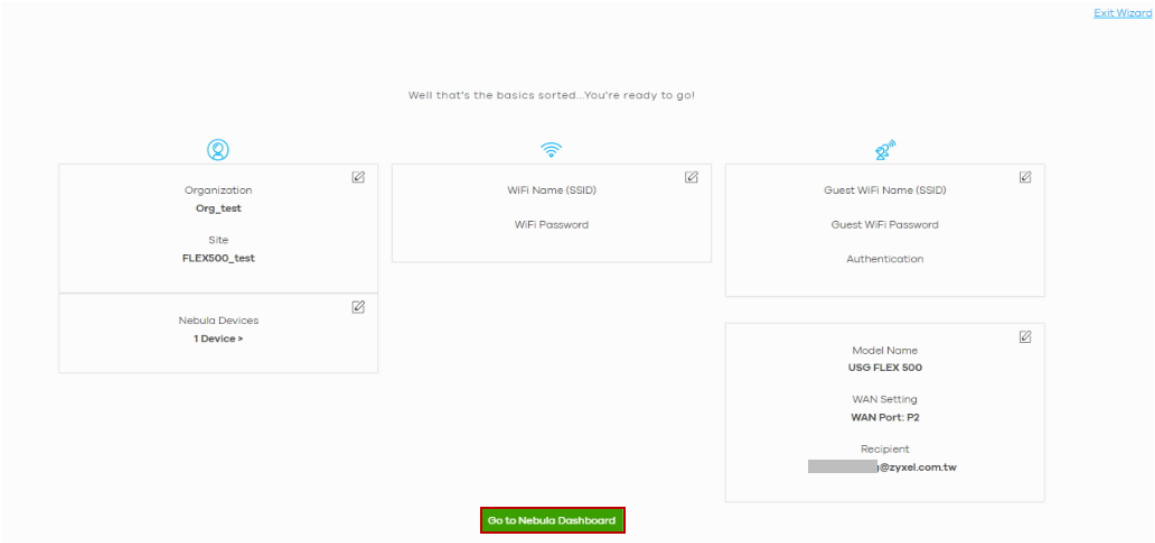
Click **Next**.


Let's now add your device(s) to Nebula
MAC Address
Serial Number
Add
Name
MAC
Serial Number
USG FLEX 500
BC:CF:4F
S20
Back
Next

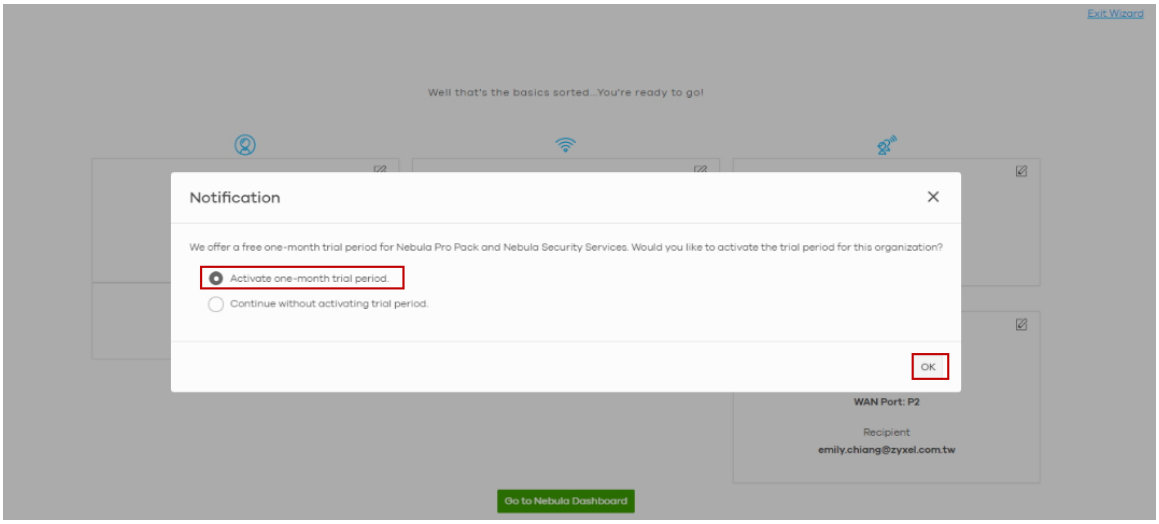
Select **Nebula native mode** and click **Next**.



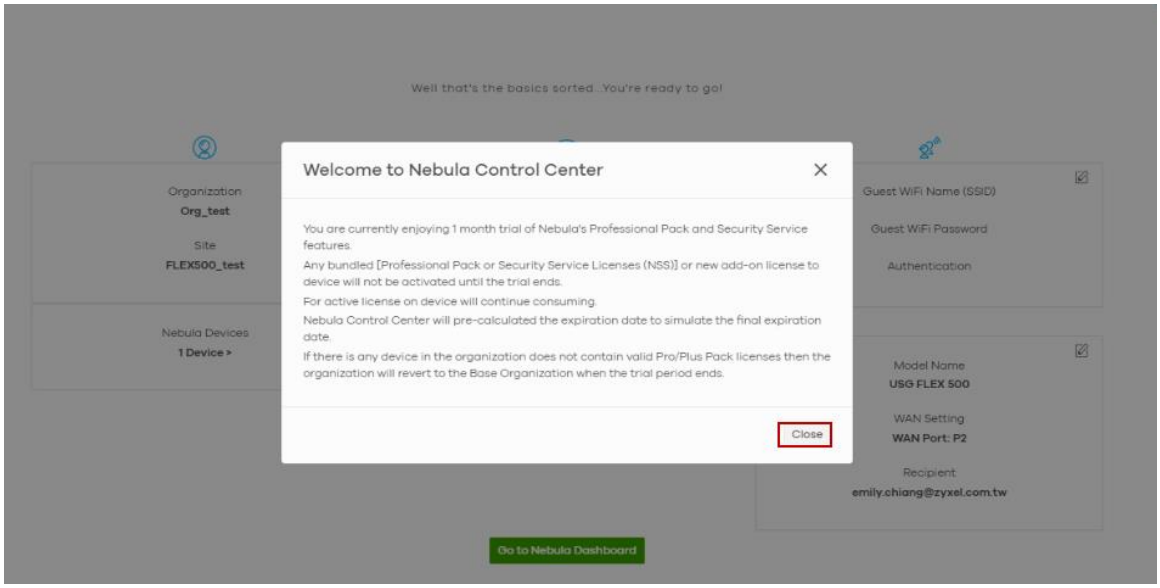
Check the information of the device and click **Go to Nebula Dashboard**.



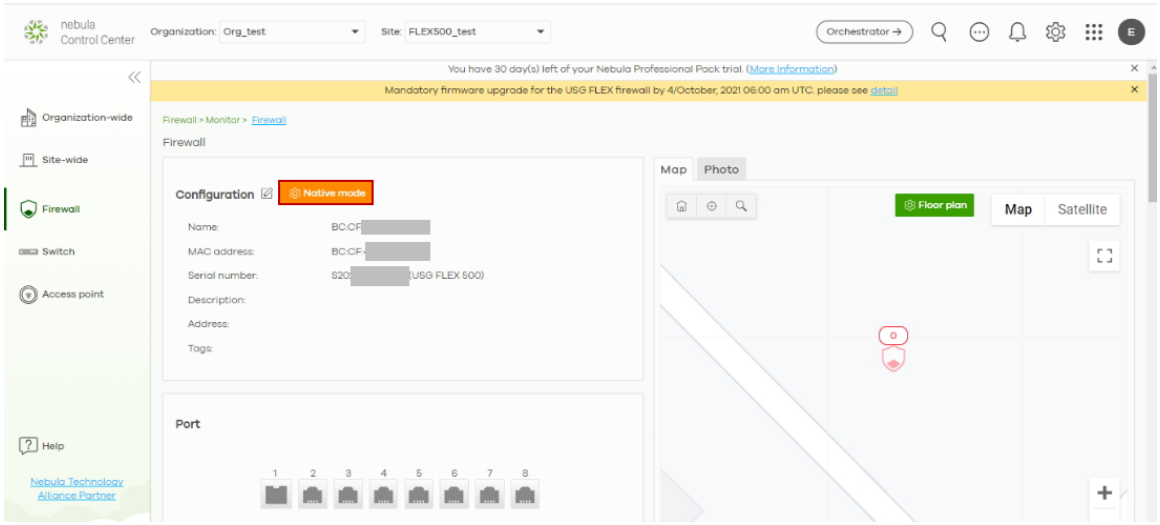
Select if you'd like to activate trial period of the license.



Click **Close**.

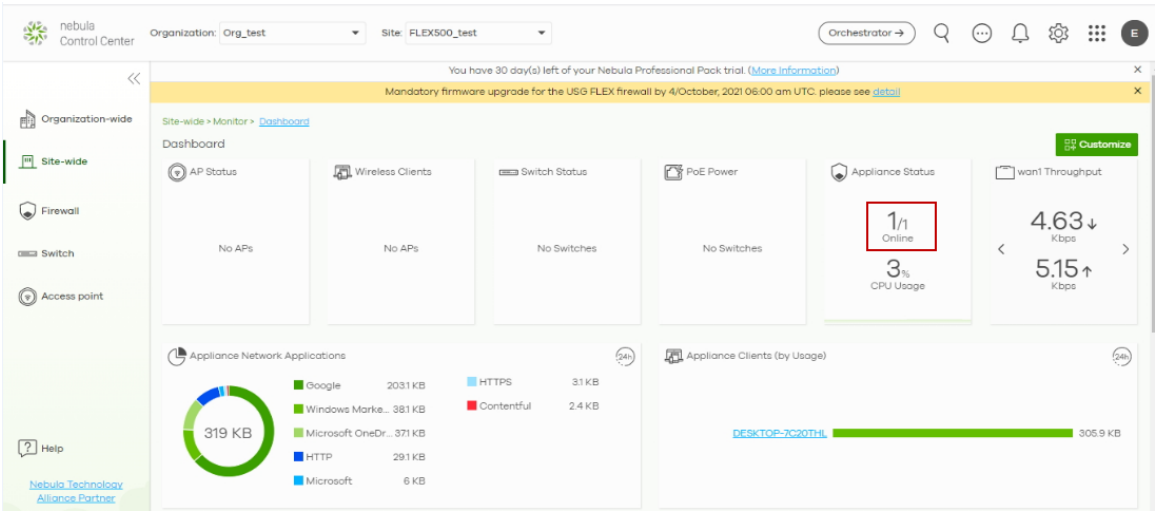


You will be redirected to Nebula Dashboard. The device is going online.



Test the Result

Go to **Site-wide > Monitor > Dashboard** and check if the device is online.



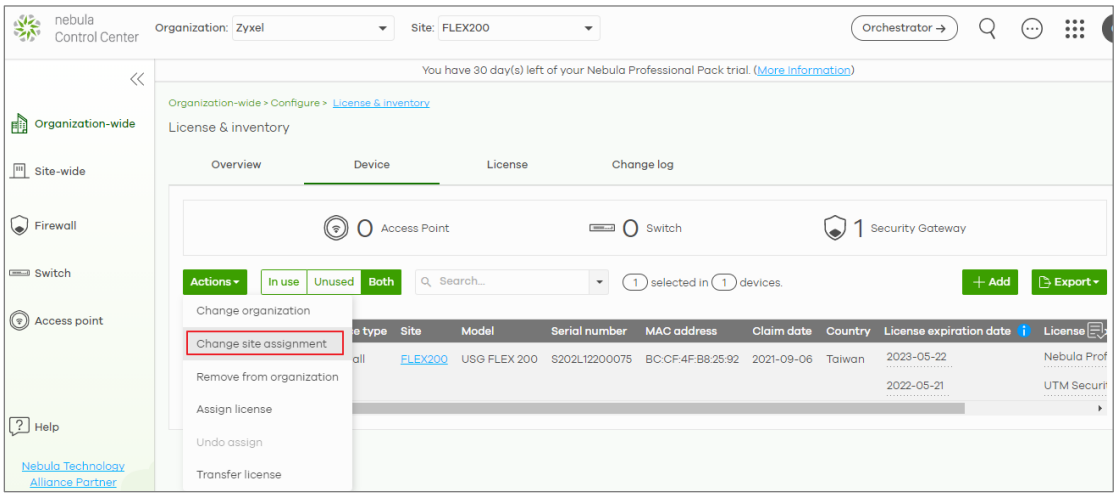
Change Site and Organization without Doing ZTP

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).

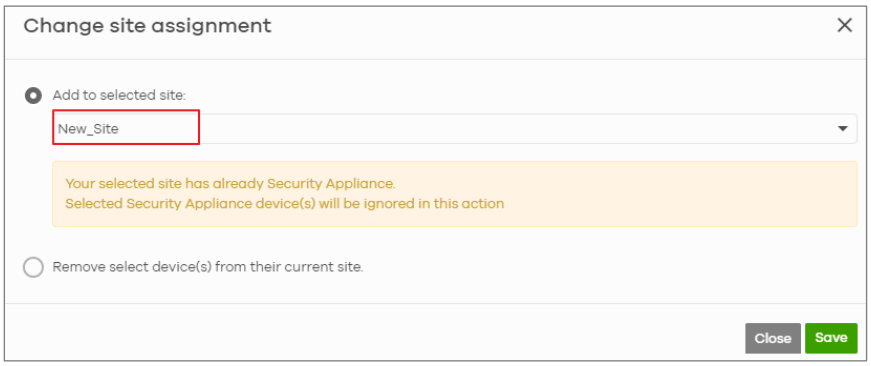
Change to the other site within the Organization

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**



Select **Add to selected site**, and choose target site



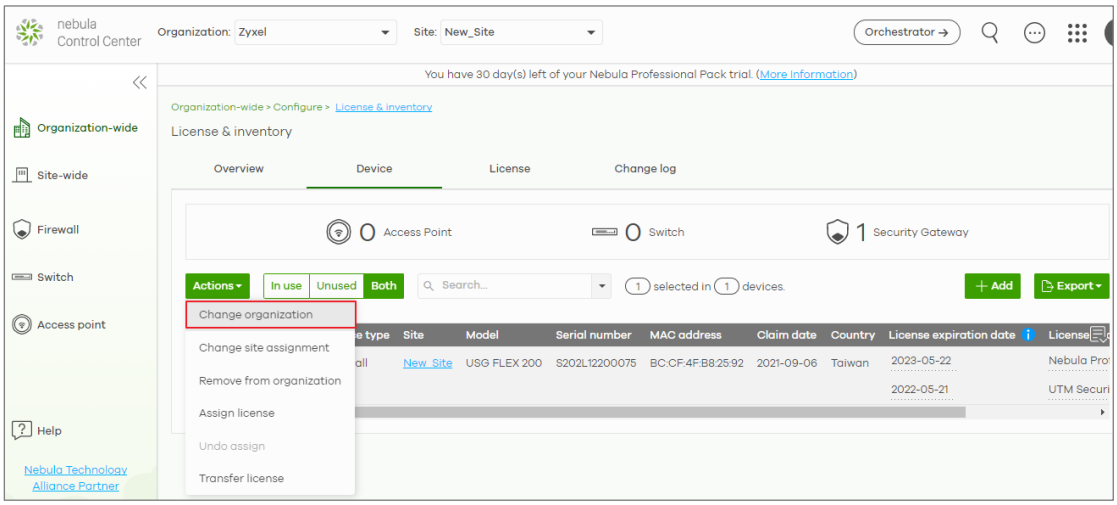
After change the site, gateway receive the request to reset to default setting but keep WAN settings from Nebula. It takes several minutes for device to reboot and get up. Then gateway will be managed by new Site on Nebula without do ZTP again.

Change to the other Organization

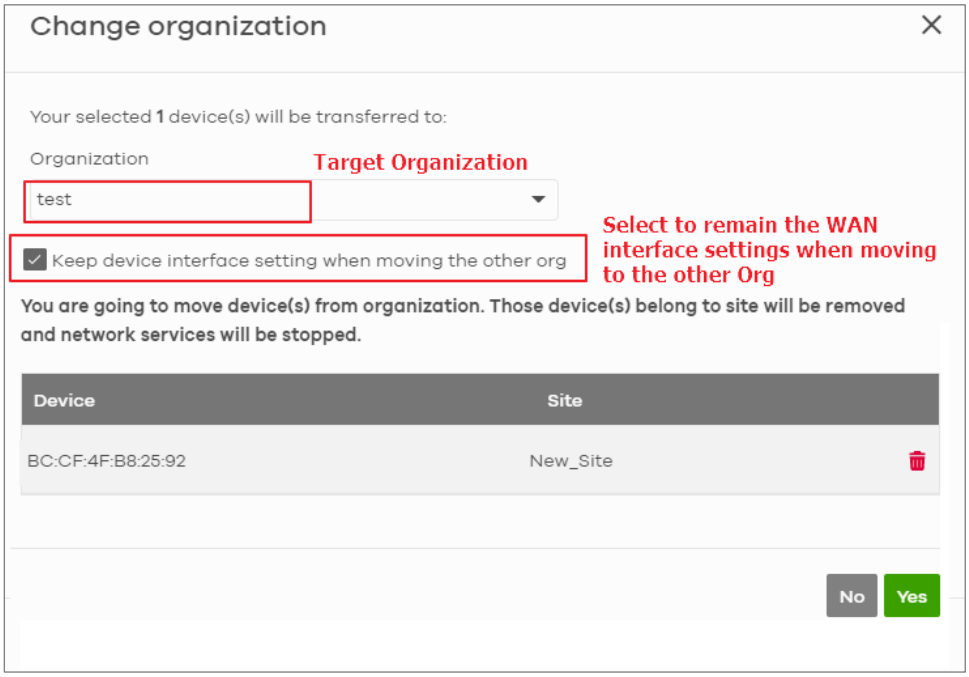
If you are MSP (require MSP license), you have multiple Organization. You wish to change the gateway to other Organization without repeating ZTP when your network environment doesn't change.

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.**



Select the target organization, and select **Keep device interface setting when moving the other org.**



After moving the device to the new organization, you can assign the device to specific site