

ATP/USG FLEX/VPN Series

ATP200/ ATP500/ ATP800

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

VPN50 / VPN100 /VPN300 /VPN1000

Security Firewalls

Firmware Version 5.00
Edition 1, 04/2021

Handbook

Default Login Details

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

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
How to Configure IPSec VPN with ZyWALL IPSec VPN Client	147
How to Configure Site-to-site IPSec VPN with FortiGate	159
How to Configure Site-to-site IPSec VPN with WatchGuard	171
How to Configure Site-to-site IPSec VPN with Cisco	184
How to Configure Site-to-site IPSec VPN with a SonicWALL router.....	198
How to Configure IPSec VPN Failover	214
How to Configure L2TP over IPSec VPN while the ZyWALL/USG is behind a NAT router	229
How to Configure L2TP VPN with Android 5.0 Mobile Devices	242
How to Configure L2TP VPN with iOS 8.4 Mobile Devices.....	254
How to Import ZyWALL/USG Certificate for L2TP over IPsec in Windows 10.....	265
How to Import ZyWALL/USG Certificate for L2TP over IPsec in iOS mobile phone	283
How to Configure 2 factor for VPN connection?	294

How to Import ZyWALL/USG Certificate for L2TP over IPsec in Android mobile phone	310
How to Configure the L2TP VPN with Apple MAC OS X 10.11 Operating System.....	323
How to configure if I want user can only see SSL VPN Login button in web portal login page	335
How to Deploy SSL VPN with Apple Mac OS X 10.10 Operating System	342
How To Configure SSL VPN for Remote Access Mobile Devices	355
How to Configure an SSL VPN Tunnel (with SecuExtender version 4.0.0.1) on the Windows 10 Operating System	362
How to redirect multiple LAN interface traffic to the VPN tunnel.....	368
How to Create VTI and Configure VPN Failover with VTI.....	381
Remote access VPN Wizard	397
Remote access VPN Wizard-IKEv2 Client	405
Chapter 2- Security Service.....	418
How to block HTTPS websites by Domain Filter without applying SSL Inspection.....	418
How to Configure Content Filter 2.0 with Geo IP Blocking	425
How to Configure Content Filter 2.0 with HTTPs Domain Filter	429
How to block the client accessing to certain country using Geo IP and Content Filter.....	435
How To Schedule YouTube Access	442
How to Detect and Prevent TCP Port Scanning with ADP	452
How to Block Facebook.....	458
How to Exempt Specific Users from a Blocked Website	468
How to Control Access To Google Drive.....	476
How to Block HTTPS Websites Using Content Filtering and SSL Inspection	484

How to Block the Spotify Music Streaming Service	495
How does Anti-Malware work	499
How to Configure an Email Security Policy with Mail Scan and DNSBL	503
How to Configure Botnet Filter on ATP series?	508
How to Use Sandboxing to Detect Unknown Malware	514
How to configure Email Security for Phishing mail?	521
How to Use IP Reputation to Detect Threats.....	525
How to Configure Reputation Filter- DNS Filter	531
How to customize external block list in Reputation Filter	535
How to Configure DNS Content Filter (On-Premises)	541
How to Configure DNS Content Filter (On-Cloud)	546
How to configure Collaborative Detection & Response to identify and quarantine compromised devices from your network.....	550
Chapter 3- Authentication	559
How to setup Two-Factor Authentication for admin login	559
How to setup Email to SMS	566
How to Use Two Factor with Google Authenticator for Admin Access?	572
Chapter 4- Device HA	582
How to Configure Device HA Pro	582
How to Configure Schedule Reboot in Device HA	592
Chapter 5- IPv6.....	595
How to Set Up IPv6 Interfaces for Pure IPv6 Routing	595
How to Set Up an IPv6 6to4 Tunnel	606
How to Set Up an IPv6-in-IPv4 Tunnel.....	611
Chapter 6- Wireless.....	616
How to Set Up a WiFi Network with ZyXEL APs	616

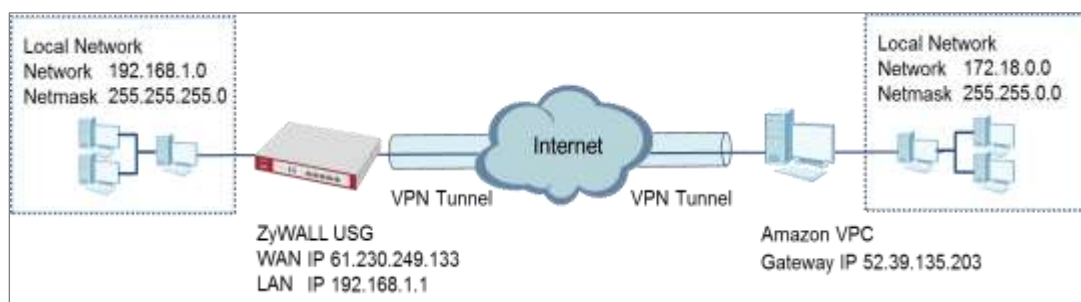
How to Set Up Guest WiFi Network Accounts.....	621
How to create a Wi-Fi VLAN interfaces to separate staff network and Guest network.....	630
How to Set Up WiFi Networks with Microsoft Active Directory Authentication.....	645
How to Configure Secure Wi-Fi to Secure the Wireless Environment?	653
Chapter 7- Maintenance.....	658
How to Manage ZyWALL/USG Configuration Files.....	658
How to Manage ZyWALL/USG Firmware.....	664
How to Automatically Reboot the ZyWALL/USG by Schedule	670
How to continuously run a ZySH script	675
How to Update Firmware Automatically from a USB Storage	679
Chapter 8- Others.....	686
How to Get Started Using the Wizards.....	686
How to Restrict Web Portal access from the Internet	701
How to Setup and Configure Daily Report	705
How to Setup and Configure Email Logs	711
How to Setup and send logs to a Syslog Server	715
How to Setup and send logs to the USB storage.....	721
How to Perform and Use the Packet Capture Feature on the ZyWALL/USG.....	725
How to Exempt Specific Users from Security Control	730
How to Configure Bandwidth Management for FTP and HTTP Traffic.	737
How to Limit BitTorrent or Other Peer-to-Peer Traffic	744
How to Configure a Trunk for WAN Load Balancing with a Static or Dynamic IP Address.....	750
How to Configure DNS Inbound Load Balancing to balance DNS Queries Among Interfaces.....	755

How to Manage Voice Traffic	760
How to Configure the 3G/LTE Interface on the ZyWALL/USG as a WAN Backup.....	767
How to Configure Two Different WAN Interfaces with Different IP Addresses in the Same VLAN	772
How to Let a Server Use the Same Public IP Address as the WAN Interface Using the Bridge Interface	777
How to Allow Public Access to a Server Behind ZyWALL/USG	780
How to Configure DHCP Option 60 – Vendor Class Identifier	784
How to set up Link Aggregation Group (LAG)	788

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



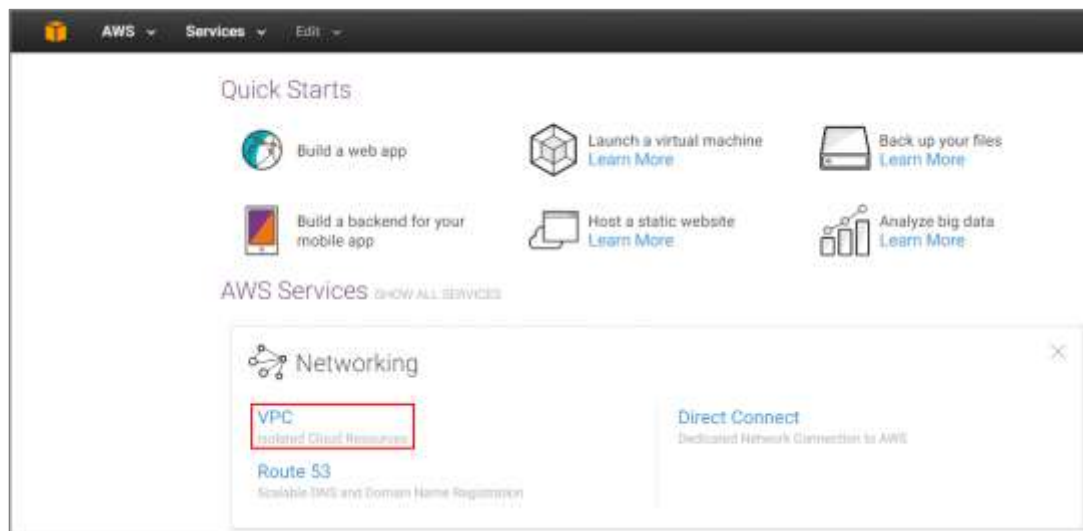
Note:

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

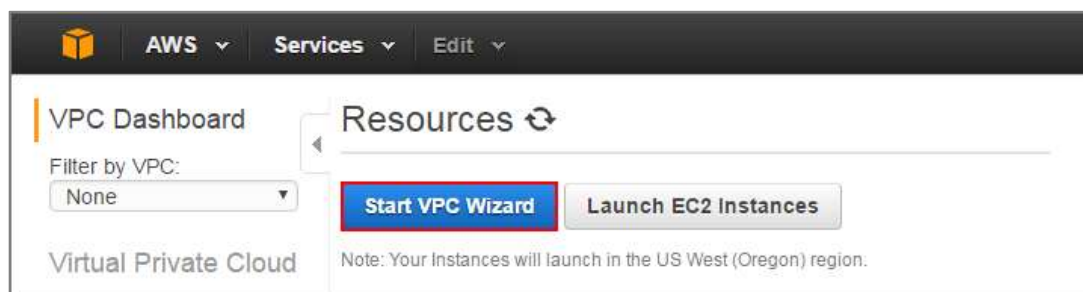
- 1 Sign into the Amazon AWS Management Console. Go to Networking > VPC.

Amazon AWS Management Console > Networking > VPC



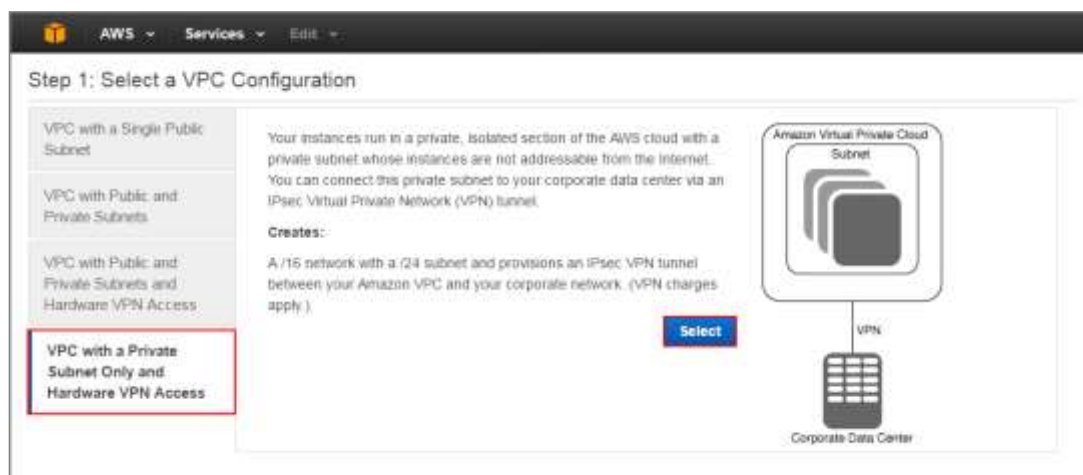
- 2 In the upper left-hand of the screen, click **Start VPC Wizard**.

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

The screenshot shows the AWS Management Console interface for Step 2: VPC with a Private Subnet Only and Hardware VPN Access. The form contains several input fields and options. The 'IP CIDR block' field is highlighted with a red rectangular box and contains the value '172.18.0.0/16' with '(65531 IP addresses available)' next to it. Below it is the 'VPC name' field. The 'Private subnet' field is also highlighted with a red rectangular box and contains the value '172.18.0.0/24' with '(251 IP addresses available)' next to it. Below it is the 'Availability Zone' dropdown menu, which is set to 'No Preference'. The 'Private subnet name' field contains the text 'Private subnet'. Below this, there is a note: 'You can add more subnets after AWS creates the VPC.' The 'Add endpoints for S3 to your subnets' section has a 'Subnet' dropdown menu set to 'None'. The 'Enable DNS hostnames' section has a radio button selected for 'Yes'. The 'Hardware tenancy' dropdown menu is set to 'Default'. At the bottom right, there are three buttons: 'Cancel and Exit', 'Back', and 'Next'.

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

Configure your VPN

Step 3: Configure your VPN

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

Customer Gateway IP: 61.230.249.133

Customer Gateway name: GW_to_ZyWALL/USG

VPN Connection name: CN_to_ZyWALL/USG

Note: VPN Connection rates apply.

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

Routing Type: Dynamic (requires BGP)

Buttons: Cancel and Exit, Back, Create VPC

Step 3: Configure your VPN

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

Customer Gateway IP: 61.230.249.133

Customer Gateway name: GW_to_ZyWALL/USG

VPN Connection name: CN_to_ZyWALL/USG

Note: VPN Connection rates apply.

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

Routing Type: Dynamic (requires BGP)

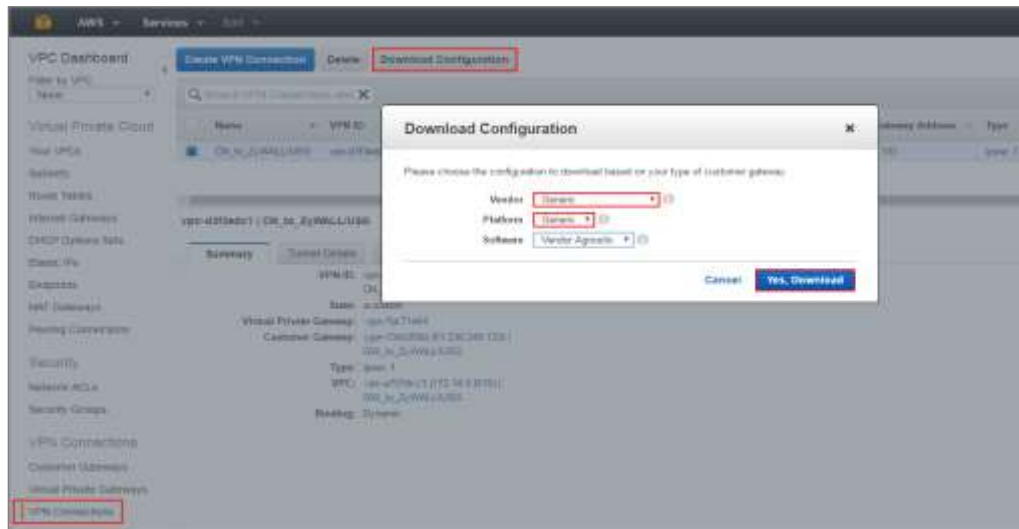
Progress: 47%

Creating VPN (This may take a few minutes)

Buttons: Cancel and Exit, Back, Create VPC

- 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            : 2EMrEASWT6QFMEBaaP2TibBmnoUaCLhW
- Authentication Algorithm   : sha1
- Encryption Algorithm       : aes-128-cbc
- Lifetime                   : 28800 seconds
- Phase 1 Negotiation Mode   : main
- Perfect Forward Secrecy    : Diffie-Hellman Group 2

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

IPSec Dead Peer Detection (DPD) will be enabled on the AWS Endpoint. We
recommend configuring DPD on your endpoint as follows:
- DPD Interval               : 10
- DPD Retries                 : 3

#3: Tunnel Interface Configuration
Outside IP Addresses:
- Customer Gateway           : 61.230.249.133
- Virtual Private Gateway    : 52.39.135.203
```

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

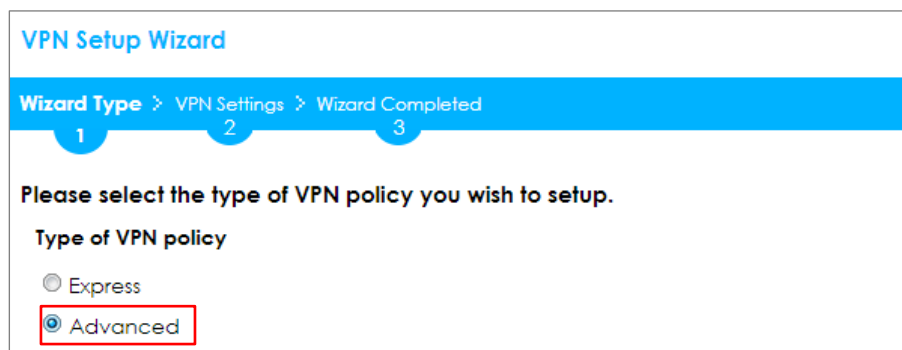
123

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

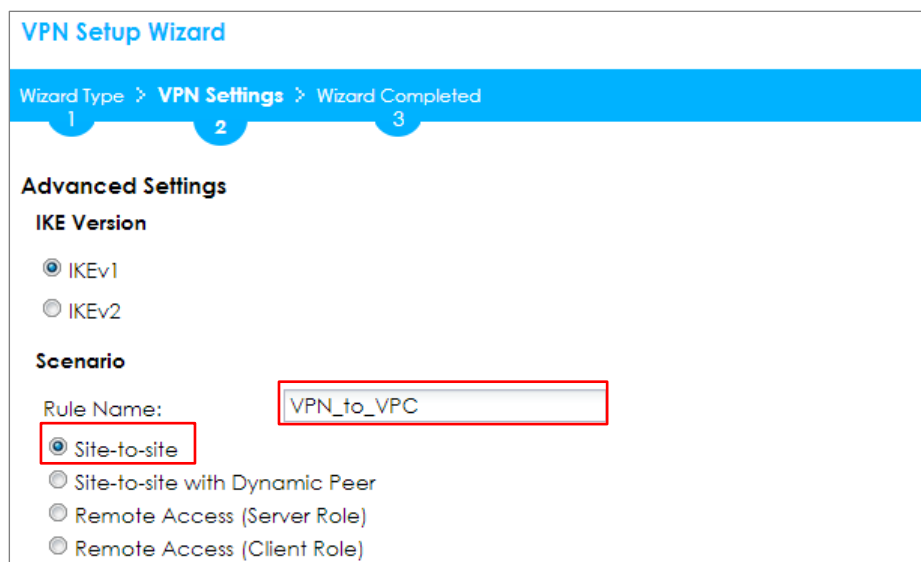
Type of VPN policy

☐ Express

☒ Advanced

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

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



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Advanced Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: VPN_to_VPC

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Advanced Settings

Phase 1 Setting

Secure Gateway: 52.39.135.203 (IP or FQDN)

My Address (interface): ge1

Negotiation Mode: Main

Encryption Algorithm: AES128

Authentication Algorithm: SHA1

Key Group: DH2

SA Life Time: 86400 (180 - 3000000 seconds)

☒ NAT Traversal

☒ Dead Peer Detection (DPD)

Authentication Method

☒ Pre-Shared Key 12345678

☐ Certificate default

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 2 Setting

Active Protocol:

ESP

Encapsulation:

Tunnel

Encryption Algorithm:

AES128

Authentication Algorithm:

SHA1

SA Life Time:

86400

(180 - 3000000 seconds)

Perfect Forward Secrecy (PFS):

None

Policy Setting

Local Policy (IP/Mask):

192.168.1.0

/255.255.255.0

Remote Policy (IP/Mask):

172.18.0.0

/255.255.0.0

Property

☒ Nailed-Up

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

Wizard Type > VPN Settings > Wizard Completed
 1 2 3

Advanced Settings

Summary

Rule Name:	VPN_to_VPC
Secure Gateway:	52.39.135.203
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	172.18.0.0 / 255.255.255.0

Phase 1

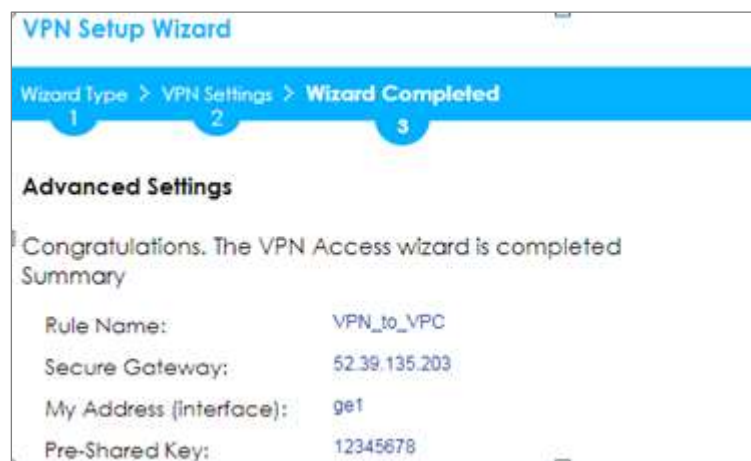
Negotiation Mode:	main
Encryption Algorithm:	aes128
Authentication Algorithm:	sha
Key Group:	DH2

Phase 2

Active Protocol:	esp
Encapsulation:	tunnel
Encryption Algorithm:	aes128
Authentication Algorithm:	sha

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

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



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

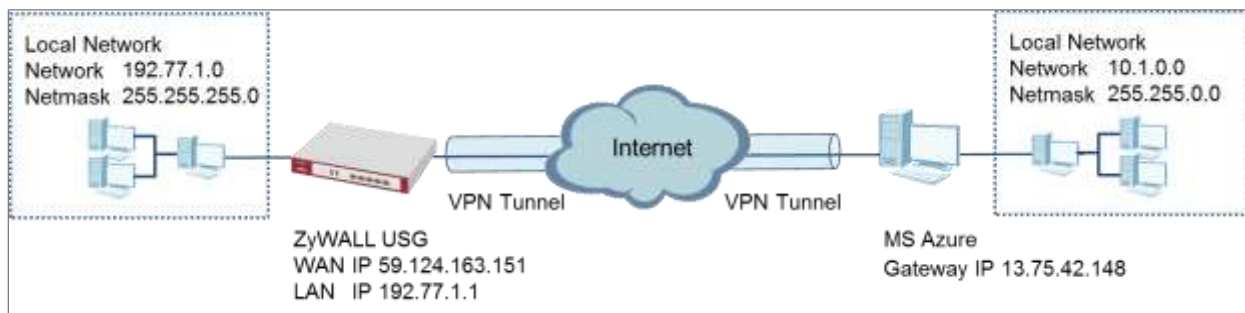
If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Make sure your ZyWALL/USG Phase 2 Settings are supported in the Amazon VPC IKE Phase 2 setup list.

MONITOR > Log

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

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

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



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



Note:

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

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

- ☐ Express
- ☒ Advanced

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

IKE Version

☒ IKEv1
☐ IKEv2

Scenario

Rule Name:

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

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 1 Setting

Secure Gateway: 13.75.42.148 (IP or FQDN)

My Address (interface): ge1

Negotiation Mode: Main

Encryption Algorithm: AES256

Authentication Algorithm: SHA1

Key Group: DH2

SA Life Time: 86400 (180 - 3000000 seconds)


☒ NAT Traversal

☐ Dead Peer Detection (DPD)

Authentication Method

☒ Pre-Shared Key 12345678

☐ Certificate default

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

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 2 Setting

Active Protocol: ESP

Encapsulation: Tunnel

Encryption Algorithm: AES128

Authentication Algorithm: SHA1

SA Life Time: 86400 (180 - 3000000 seconds)

Perfect Forward Secrecy (PFS): None

Policy Setting

Local Policy (IP/Mask): 192.77.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 10.1.0.0 / 255.255.0.0

Property

☒ Nailed-Up



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

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

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

Wizard Type > **VPN Settings** > Wizard Completed

123

Advanced Settings

Summary

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

Phase 1

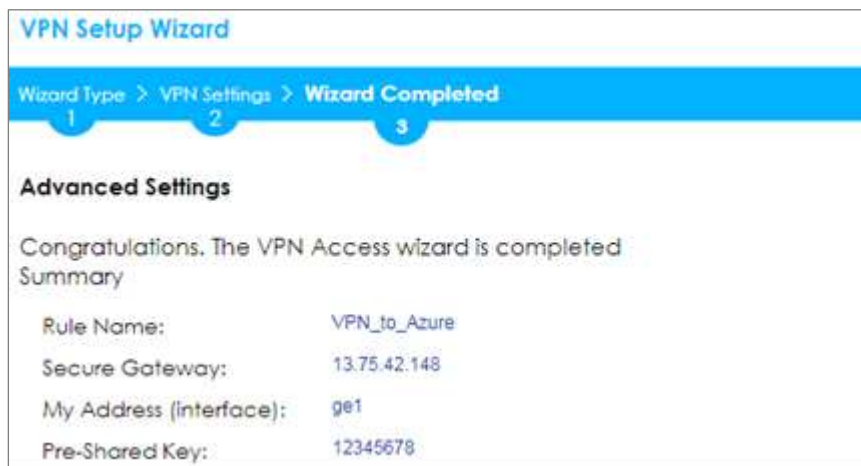
Negotiation Mode:	main
Encryption Algorithm:	aes128
Authentication Algorithm:	sha
Key Group:	DH2

Phase 2

Active Protocol:	esp
Encapsulation:	tunnel
Encryption Algorithm:	aes128

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

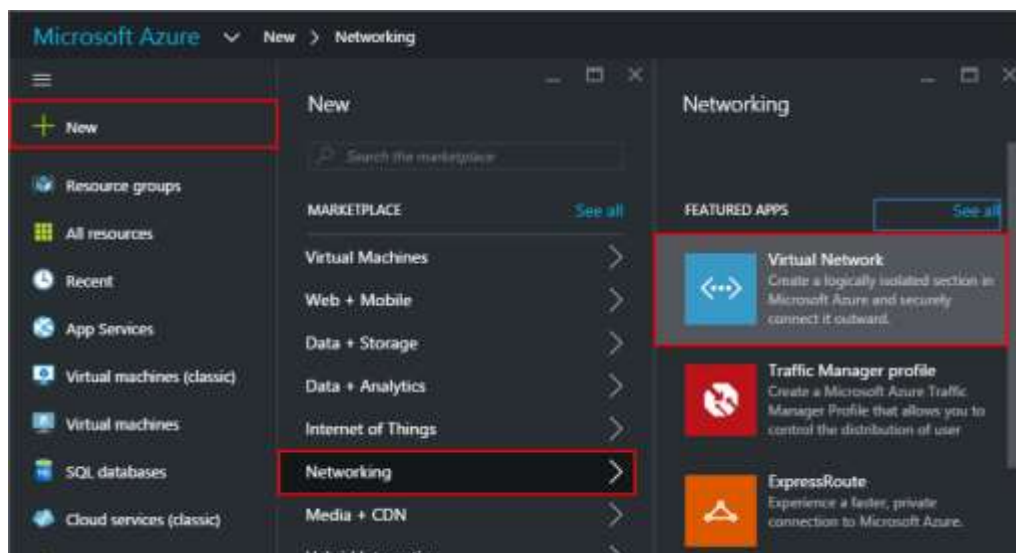
Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings > Wizard Completed



Set Up the IPSec VPN Tunnel on the MS Azure

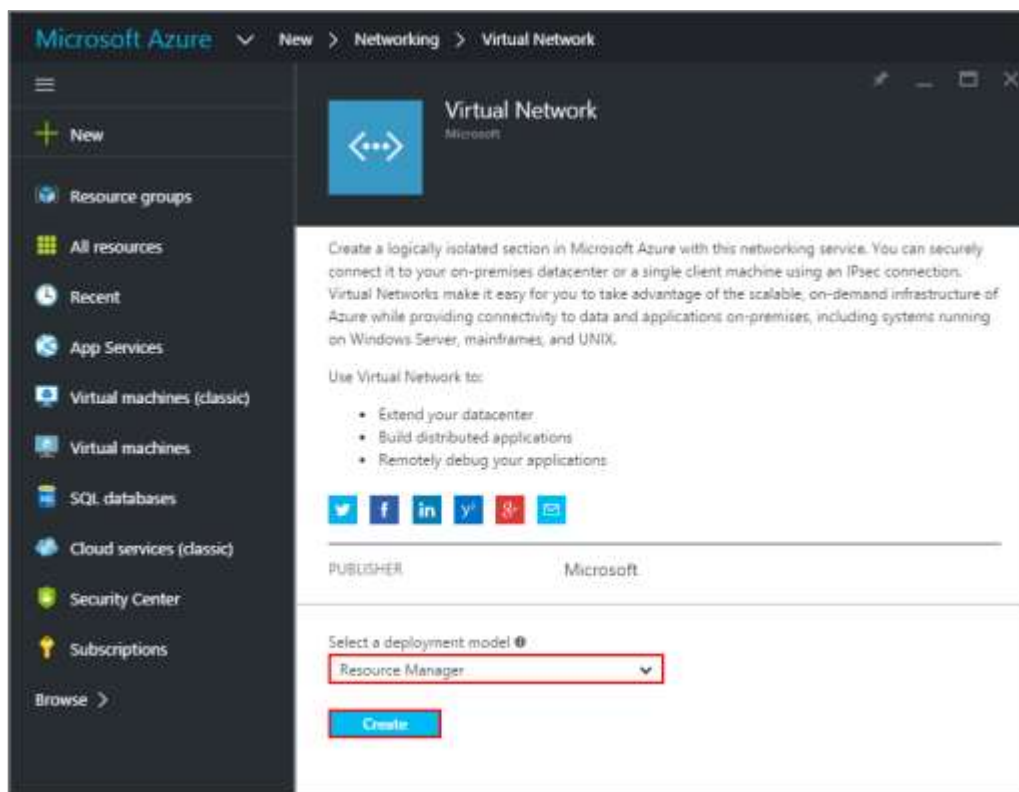
Sign into the **Windows Azure Management Portal**. In the upper left-hand corner of the screen, click **+New > Networking > Virtual Network**.

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

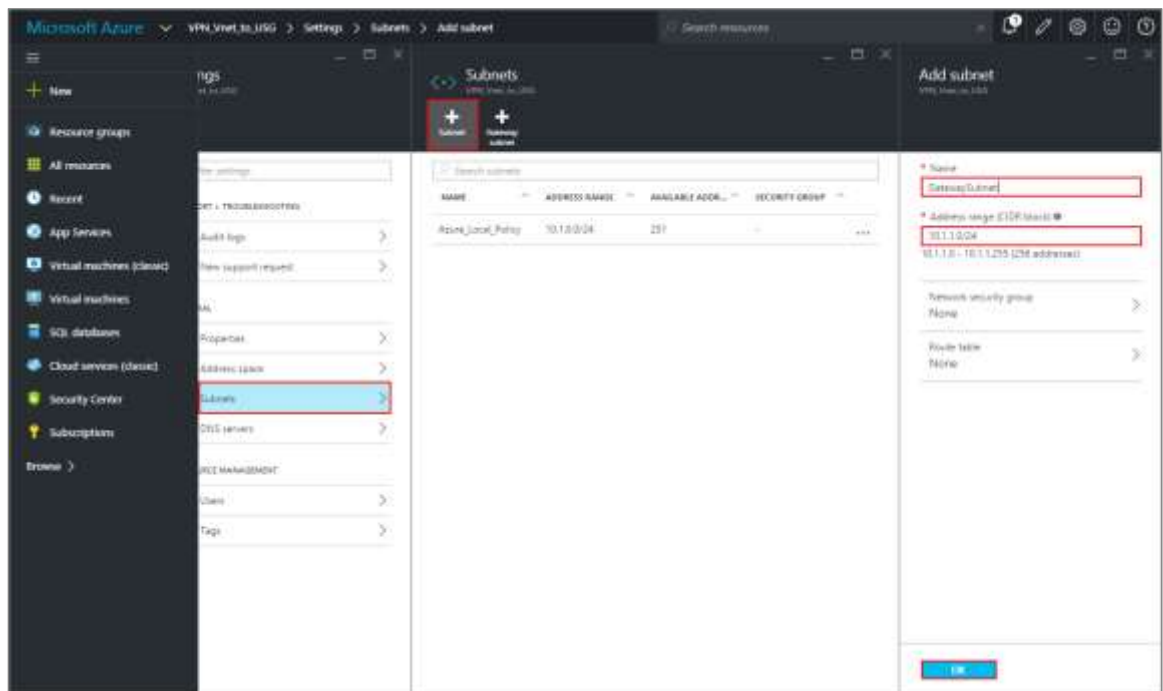
Microsoft Azure > New > Networking > Virtual Network > Create virtual network

Create virtual network

- * Name: VPN_Vnet_to_USG ✓
- * Address space ⓘ: 10.1.0.0/16 ✓
10.1.0.0 - 10.1.255.255 (65536 addresses)
- * Subnet name: Azure_Local_Policy ✓
- * Subnet address range ⓘ: 10.1.0.0/24 ✓
10.1.0.0 - 10.1.0.255 (256 addresses)
- Subscription: Free Trial
- * Resource group: + New
- New resource group name: RG_USG ✓
- Location: East Asia
- ☒ Pin to dashboard
- [Create](#)

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

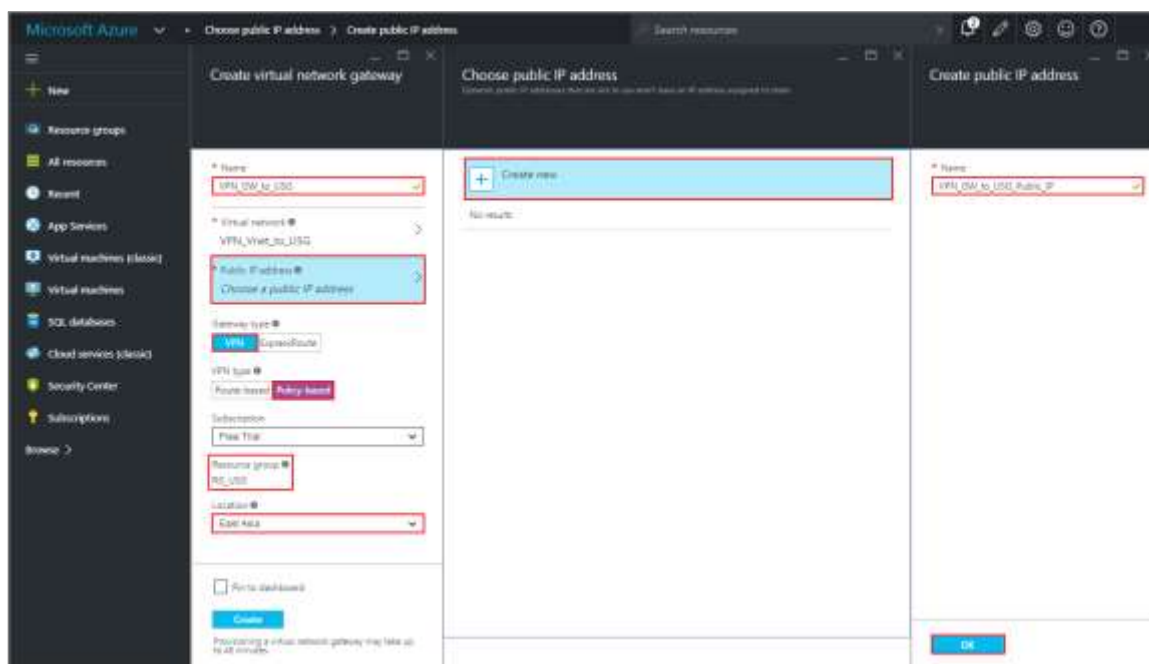


In the portal, go to **New**, then Networking. Select **Virtual network gateway** from the list. On the **Create virtual network gateway** blade **Name** field, name your gateway. Next, choose the **Virtual network** that you want to deploy this gateway to.

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

Microsoft Azure > New > Networking > Create local network gateway

Create local network gateway

* Name: ✓

* IP address ⓘ: ✓

Address space ⓘ: ...

...

Subscription: ▼

* Resource group ⓘ: ▼

Location: ▼

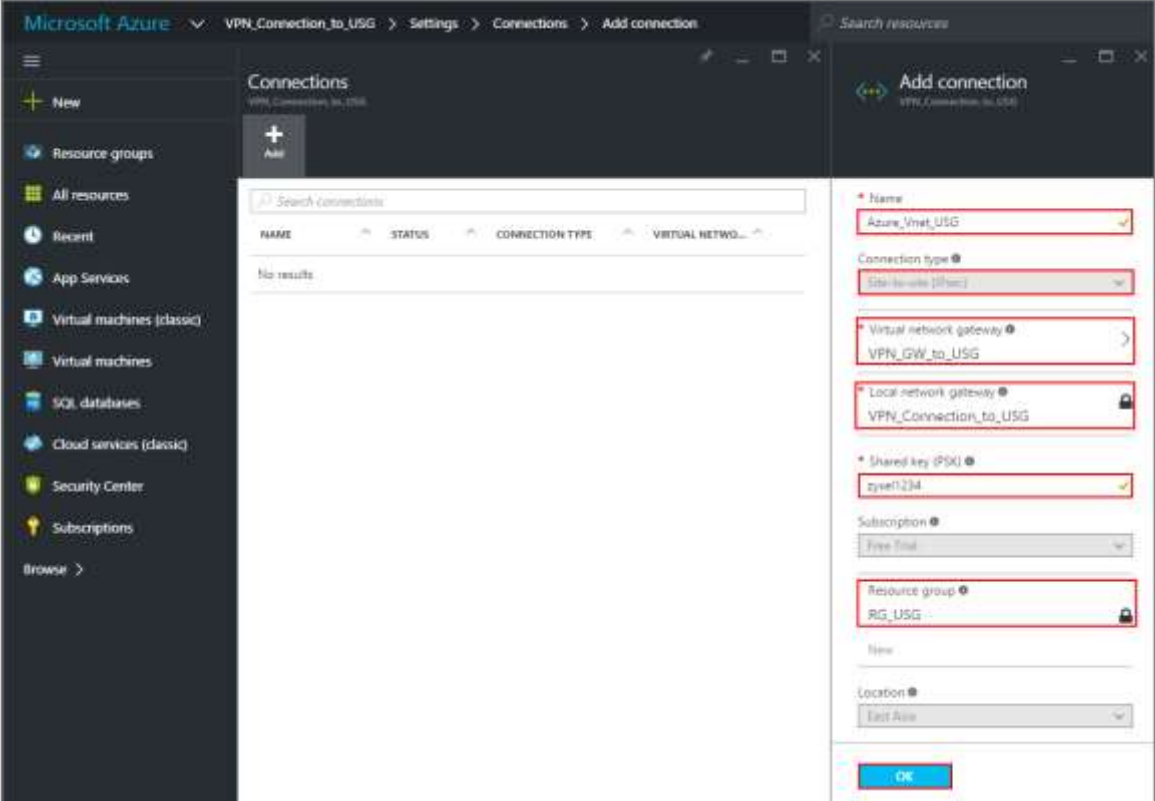
☒ Pin to dashboard

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



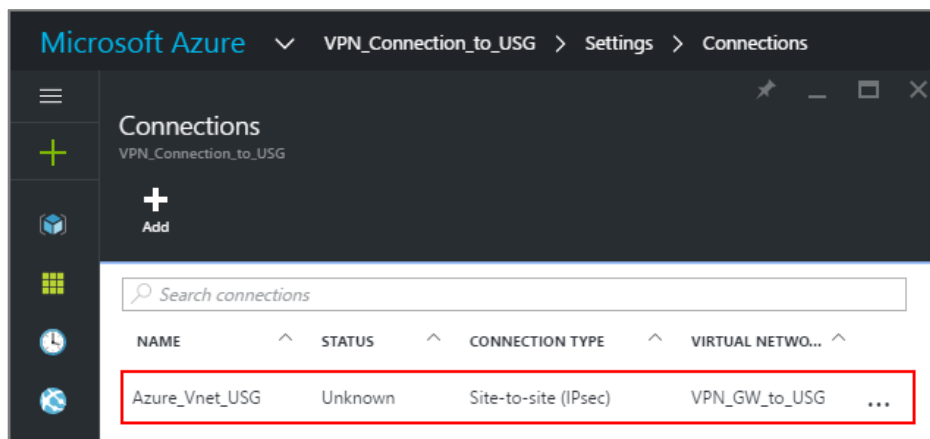
The screenshot shows the Microsoft Azure portal interface. The breadcrumb navigation at the top reads: **VPN_Connection_to_USG > Settings > Connections > Add connection**. The left sidebar contains a navigation menu with options like 'New', 'Resource groups', 'All resources', 'Recent', 'App Services', 'Virtual machines (classic)', 'Virtual machines', 'SQL databases', 'Cloud services (classic)', 'Security Center', and 'Subscriptions'. The main area is divided into two panes. The left pane, titled 'Connections', shows a table with columns 'NAME', 'STATUS', 'CONNECTION TYPE', and 'VIRTUAL NETWO...', and it displays 'No results'. The right pane, titled 'Add connection', contains the following fields:

- Name:** A dropdown menu with 'Azure_Vnet_USG' selected.
- Connection type:** A dropdown menu with 'Site-to-site (IPsec)' selected.
- Virtual network gateway:** A dropdown menu with 'VPN_GW_to_USG' selected.
- Local network gateway:** A dropdown menu with 'VPN_Connection_to_USG' selected.
- Shared key (PSK):** A text input field containing 'zyxel1234'.
- Subscription:** A dropdown menu with 'Free Trial' selected.
- Resource group:** A dropdown menu with 'RG_USG' selected.
- Name:** A text input field (empty).
- Location:** A dropdown menu with 'East Asia' selected.

 At the bottom of the right pane is a blue 'OK' button.

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

Add Edit Remove Activate Inactivate Connect Disconnect Object References				
Status	Name	VPN Gateway	Gateway IP Version	Policy
1	VPN_to_Azure	VPN_to_Azure	IPv4	VPN_to_Azure_LOCAL/VPN_to_Azure_REMOTE

Page 1 of 1 Show 50 Items Displaying 1 of 1

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

MONITOR > VPN Monitor > IPSec

Disconnect		Connection Check						
Name	Policy	My Address	Secure Gateway	Up time	Timeout	Inbound(B...	Outbound...	
1	WZ_VPN_Azure	192.77.1.0/24<10.1.0.0/16	59.124.163.151	P: 13.75.42.148;4500	14	86406	0(0 bytes)	

Page 1 of 1

Show 50 items

Displaying 1 - 1 of 1

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

VPN > VPN Settings > Currently Active VPN Tunnels

Microsoft Azure

Azure_Vnet_USG > Settings

Azure_Vnet_USG

Connection

Settings Delete

Essentials

Resource group

RG_USG

Status

Connected

Location

East Asia

Subscription name

Free Trial

Subscription ID

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

Data in

0 B

Data out

576 B

Virtual network

VPN_Vnet_to_USG

Virtual network gateway

VPN_GW_to_USG (13.75.42.148)

Local network gateway

VPN_Connection_to_USG (59.124.163.151)

All settings →

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

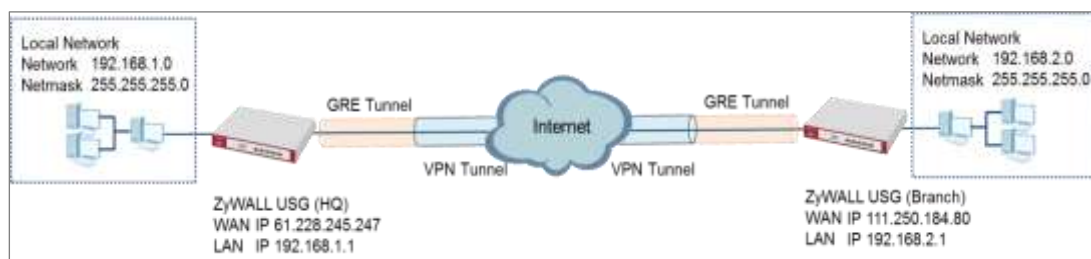
If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Make sure your ZyWALL/USG Phase 2 Settings are supported in the MS Azure IKE Phase 2 setup list.

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][CID]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

How to Configure GRE over IPsec VPN Tunnel

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



ZyWALL/USG GRE over IPsec VPN



Note:

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

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

- ☒ Express
- ☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

WIZ_VPN_HQ

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the 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)

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway:

111.250.184.80

(IP or FQDN)

Pre-Shared Key:

12345678

Local Policy (IP/Mask):

192.168.1.0

255.255.255.0

Remote Policy (IP/Mask):

192.168.2.0

255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_HQ

Secure Gateway: 111.250.184.80

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.2.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name: WIZ_VPN_HQ

Secure Gateway: 111.250.184.80

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.2.0 / 255.255.255.0

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

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

Authentication

☒ Pre-Shared Key ☐ unmasked

☐ Certificate (See [My Certificates](#))

☐ User Based PSK [i](#)

☒ Advance

Local ID Type:

Content:

Peer ID Type: [i](#)

Content:

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

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

Policy

Local policy: SUBNET, 192.168.1.0/24

Remote policy: SUBNET, 192.168.2.0/24


☒ Advance

☒ Enable GRE over IPSec [i](#)

☐ Policy Enforcement

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

CONFIGURATION > Network > Interface > Tunnel > Add

General Settings		
<input checked="" type="checkbox"/> Enable		
Interface Properties		
Interface Name:	<input type="text" value="tunnel1"/>	
Zone:	<input type="text" value="TUNNEL"/>	
Tunnel Mode:	<input type="text" value="GRE"/>	
IP Address Assignment		
IP Address:	<input type="text" value="10.0.0.1"/>	
Subnet Mask:	<input type="text" value="255.255.255.0"/>	
Metric:	<input type="text" value="0"/> (0-15)	
Gateway Settings		
My Address		
<input checked="" type="radio"/> Interface	<input type="text" value="ge1"/>	Static -- 61.226.245.247/255.255.255.255
<input type="radio"/> IP Address	<input type="text" value="0.0.0.0"/>	
Remote Gateway Address:	<input type="text" value="111.250.184.80"/>	

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

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

- ☒ Express
- ☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings
IKE Version
☒ IKEv1
☐ IKEv2
Scenario
Rule Name:
☒ Site-to-site
☐ Site-to-site with Dynamic Peer
☐ Remote Access (Server Role)
☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings
Configuration
Secure Gateway: (IP or FQDN)
Pre-Shared Key:
Local Policy (IP/Mask):
Remote Policy (IP/Mask):

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name:	WIZ_VPN_Branch
Secure Gateway:	61.228.245.247
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.2.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.1.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_VPN_Branch
Secure Gateway:	61.228.245.247
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.2.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.1.0 / 255.255.255.0

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

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

The screenshot shows the 'Authentication' section of the ZyXEL VPN Gateway configuration. The 'Pre-Shared Key' is selected and masked with dots. The 'Certificate' and 'User Based PSK' options are unselected. The 'Advance' section is expanded, showing 'Local ID Type' set to 'IPv4', 'Content' set to '0.0.0.0', and 'Peer ID Type' set to 'Any' (highlighted with a red box). The 'Content' field for 'Peer ID Type' is empty.

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 screenshot shows the 'Policy' section of the ZyXEL VPN Connection configuration. The 'Local policy' is set to 'WIZ_VPN_Branch_L' and the 'Remote policy' is set to 'WIZ_VPN_Branch_F'. Both are associated with the subnet 'SUBNET, 192.168.2.0/24'. The 'Advance' section is expanded, showing 'Enable GRE over IPsec' checked (highlighted with a red box) and 'Policy Enforcement' unchecked.

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

CONFIGURATION > Network > Interface > Tunnel > Add

General Settings	
<input checked="" type="checkbox"/> Enable	
Interface Properties	
Interface Name:	tunnel2
Zone:	TUNNEL ?
Tunnel Mode:	GRE
IP Address Assignment	
IP Address:	10.0.0.2
Subnet Mask:	255.255.255.0
Metric:	0 (0-15)
Gateway Settings	
My Address	
<input checked="" type="radio"/> Interface	ge1 Static -- 111.250.184.80/255.255.255.255
<input type="radio"/> IP Address	0.0.0.0
Remote Gateway Address:	61.228.245.247

Test the GRE over IPSec VPN Tunnel

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

CONFIGURATION > VPN > IPSec VPN > VPN Connection

IPv4 Configuration				
<div> Add Edit Remove Activate Inactivate Connect Disconnect Object References </div>				
Status	Name	VPN Gateway	Gateway IP Version	Policy
1	WIZ_VPN_HQ	WIZ_VPN_HQ	IPv4	WIZ_VPN_HQ_LOCAL...
<div> Page 1 of 1 Show 30 items Displaying 1 - 1 of 1 </div>				

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(Byte)	Outbound(Byte)
1	WZ_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

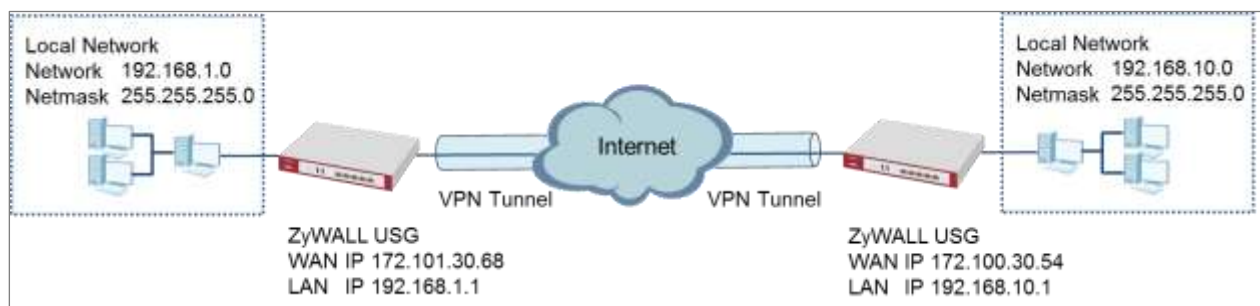
If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Make sure your ZyWALL/USG Phase 2 Settings are supported in the Amazon VPC IKE Phase 2 setup list.

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][C]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

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

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



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

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

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

☒ VPN Settings

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for Configuration Provisioning

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for L2TP VPN Settings

- VPN Settings
- General Settings
- Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

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

Type of VPN policy

☒ Express

☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway).

You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1
☐ IKEv2

Scenario

Rule Name:

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

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.100.30.54 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_HQ

Secure Gateway: 172.100.30.54

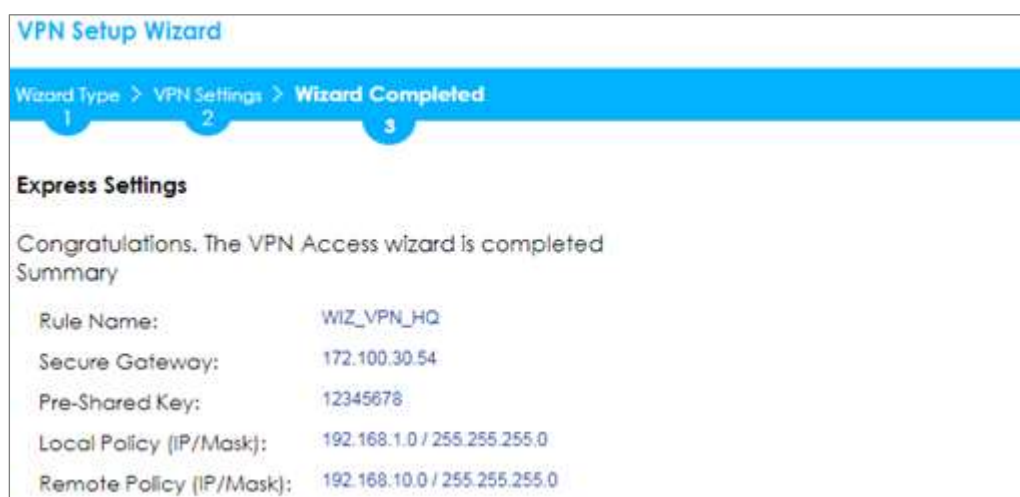
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

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

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



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

Express Settings

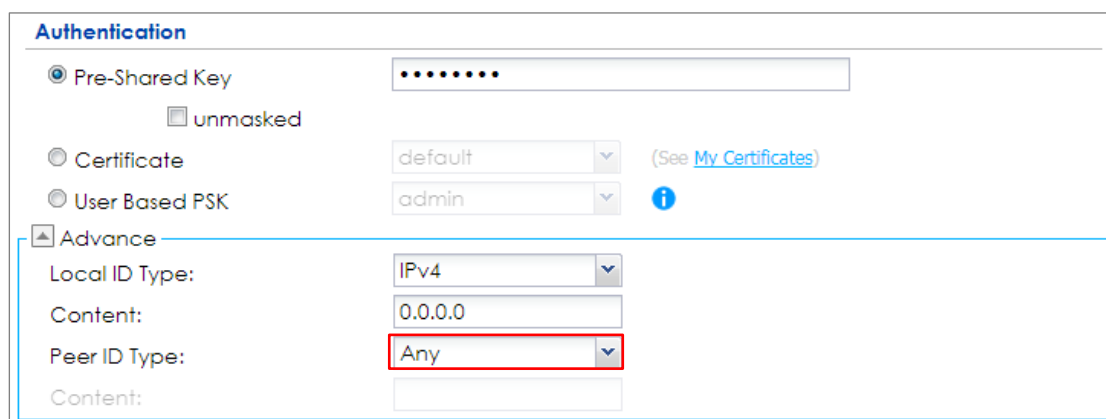
Congratulations. The VPN Access wizard is completed

Summary

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

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

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



Authentication

☒ Pre-Shared Key ☐ unmasked

☐ Certificate (See [My Certificates](#))

☐ User Based PSK [i](#)

Advance

Local ID Type:

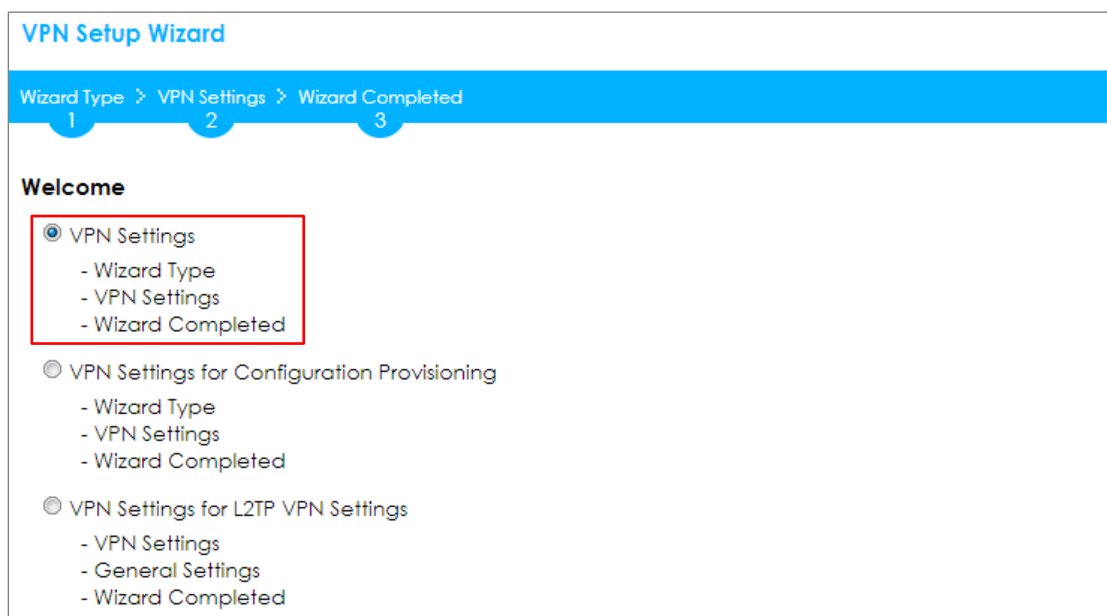
Content:

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



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type

VPN Settings

Wizard Completed

123

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

Type of VPN policy

☒ Express

☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway).

You may use 1-31 alphanumeric characters. This value is case-sensitive. Click **Next**.

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

VPN Setup Wizard

Wizard Type

VPN Settings

Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.101.30.68 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_Branch

Secure Gateway: 172.101.30.68

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

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

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

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

Authentication

☒ Pre-Shared Key ☐ unmasked

☐ Certificate (See [My Certificates](#))

☐ User Based PSK

☒ Advance

Local ID Type:

Content:

Peer ID Type:

Content:

Test the IPSec VPN Tunnel

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

CONFIGURATION > VPN > IPsec VPN > VPN Connection

Add Edit Remove Activate Inactivate Connect Disconnect Object References				
#	Status	Name	VPN Gateway	Gateway IP Version Policy
1		VPN_to_Azure	VPN_to_Azure	IPV4
*WG_VPN_HQ_LOCAL/*WG_VPN_HQ_REMOTE				
Page 1 of 1 Show 50 items				

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...	Outbou...
1	Hub_HQ-to-Branch_A	192.168.1.0/24<=>192.168.10.0/24	172.101.30.68	P:172.100.30.54	101	86319	0(0 bytes)	0(0 bytes)
Page 1 of 1 Show 50 items								

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

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

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

Pinging 192.168.10.33 with 32 bytes of data:

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

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

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

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

Pinging 192.168.1.33 with 32 bytes of data:

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

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

What Could Go Wrong?

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

MONITOR > Log

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

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

MONITOR > Log

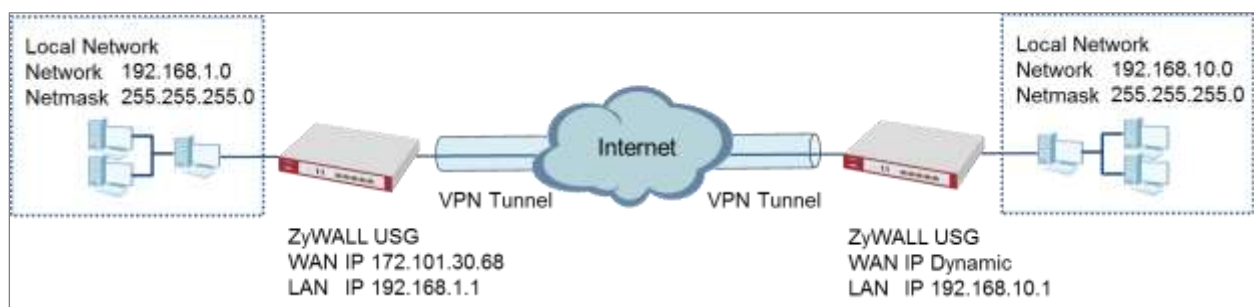
19	2017-09-11 ...	info	IKE	[SA] : No proposal chosen	IKE_LOG
20	2017-09-11 ...	info	IKE	[ID] : Tunnel [server] Phase 2 Local policy mismatch	IKE_LOG
31	2017-09-11 ...	info	IKE	Send:[HASH][SA][NONCE][ID][C]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

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


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

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

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



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

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

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

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

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

Type of VPN policy

- ☒ Express
- ☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1
☐ IKEv2

Scenario

Rule Name:

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

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: Any

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Summary

Rule Name: WIZ_VPN_HQ

Secure Gateway: Any

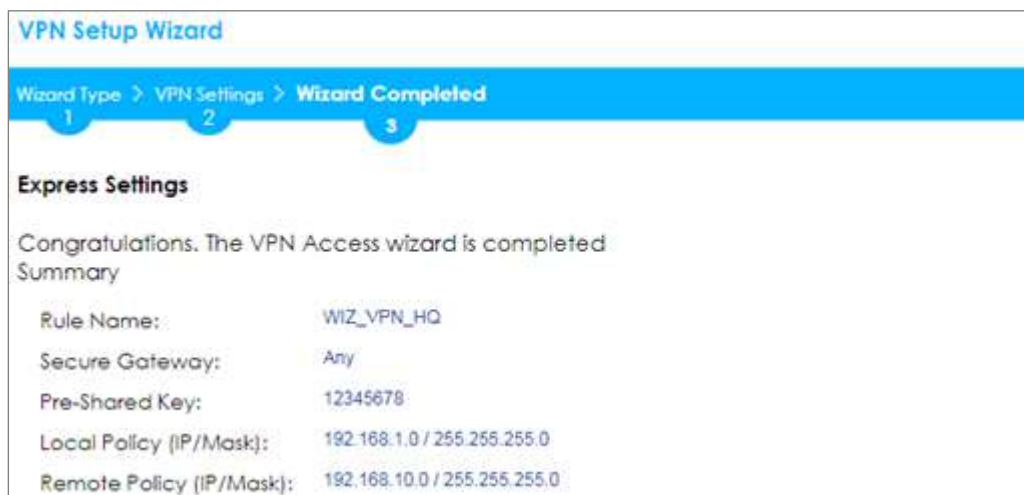
Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

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

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



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

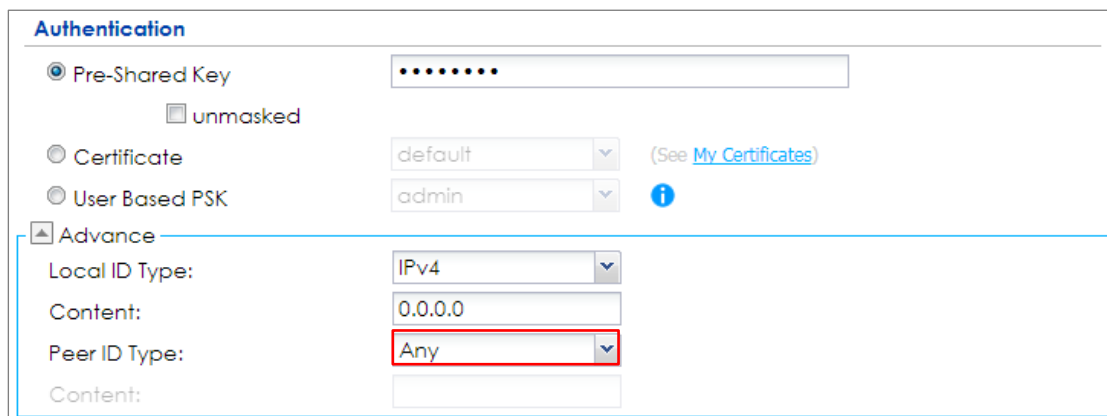
Congratulations. The VPN Access wizard is completed

Summary

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

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


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



Authentication

☒ Pre-Shared Key ☐ unmasked

☐ Certificate (See [My Certificates](#))

☐ User Based PSK 

☒ **Advance**

Local ID Type:

Content:

Peer ID Type:

Content:

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

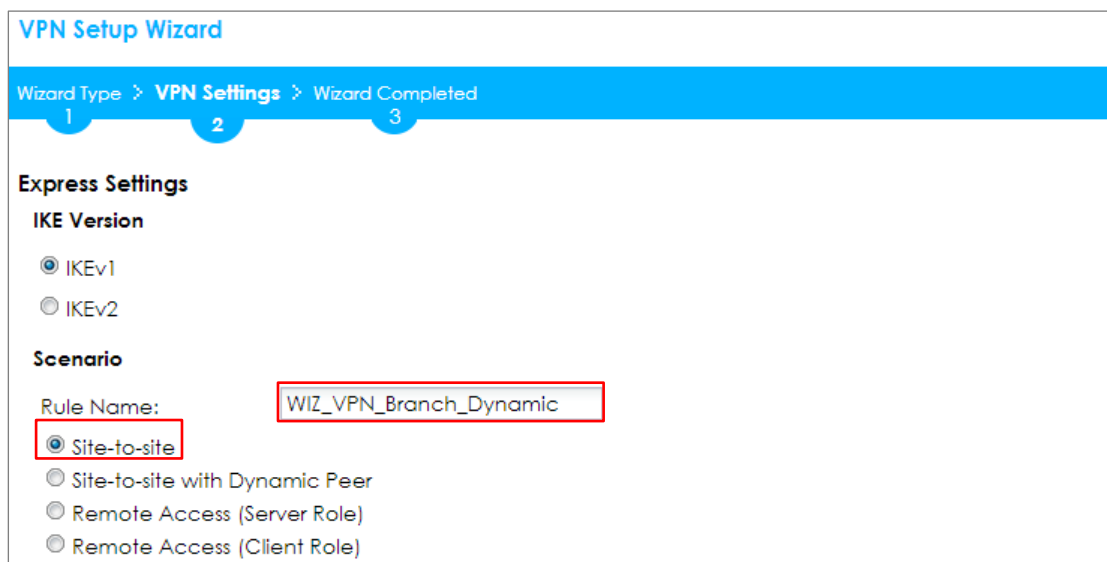
Please select the type of VPN policy you wish to setup.

Type of VPN policy

- ☒ Express
- ☐ Advanced

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

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



VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.101.30.68 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_Branch_Dynamic

Secure Gateway: 172.101.30.68

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

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

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

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

Authentication

☒ Pre-Shared Key

.....

☐ unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

admin

i

☒ Advance

Local ID Type:

IPv4

Content:

0.0.0.0

Peer ID Type:

Any

Content:

Test the IPSec VPN Tunnel

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

CONFIGURATION > VPN > IPsec VPN > VPN Connection

Add Edit Remove Activate Inactivate Connect Disconnect Object References				
Status	Name	VPN Gateway	Gateway IP Version	Policy
1	WIZ_VPN_Bro...	WIZ_VPN_Bro...	IPv4	WIZ_VPN_Branch_Dynamic_LOCAL/WIZ_VPN_Branch_Dyna...
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1				

Go to **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 By...	Outbound...
1	WIZ_VPN_Branch_Dynamic	192.168.1.0/24<>...	172.101.30.68	D: 172.100.30.54	15	86402	0(0 bytes)	0(0 bytes)
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1								

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 192.168.1.33

```
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 192.168.1.33

```
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

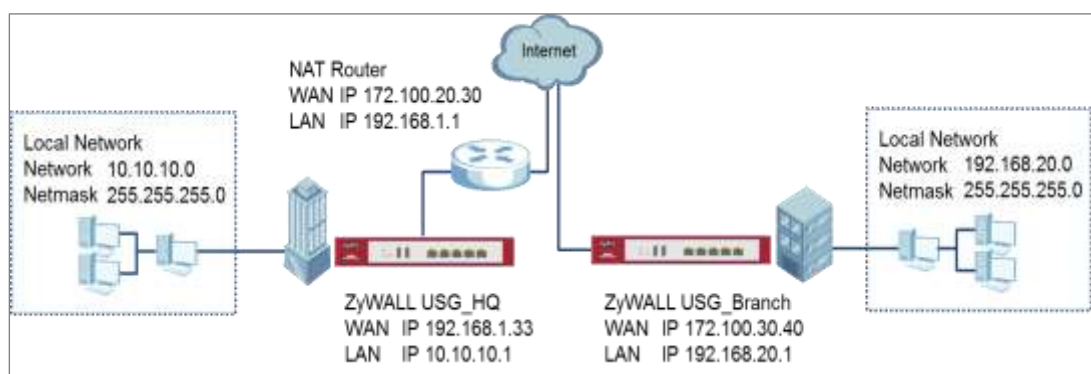
19	2017-09-11 ...	info	IKE	[SA] : No proposal chosen	IKE_LOG
20	2017-09-11 ...	info	IKE	[ID] : Tunnel [server] Phase 2 Local policy mismatch	IKE_LOG
31	2017-09-11 ...	info	IKE	Send:[HASH][SA][NONCE][ID][C]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

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

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

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

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



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

Note:

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

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

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

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

Type of VPN policy

- ☒ Express
- ☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1
☐ IKEv2

Scenario

Rule Name:

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

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: (IP or FQDN)

Pre-Shared Key:

Local Policy (IP/Mask):

Remote Policy (IP/Mask):

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

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

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

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

Authentication

☒ Pre-Shared Key

☐ unmasked

☐ Certificate
 (See [My Certificates](#))

☐ User Based PSK

☒ Advance

Local ID Type:

 Content:

 Peer ID Type:

 Content:

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

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

☒ Express

☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: 172.100.20.30 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.20.0 / 255.255.255.0

Remote Policy (IP/Mask): 10.10.10.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

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

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

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

Authentication

☒ Pre-Shared Key

☐ unmasked

☐ Certificate

(See [My Certificates](#))

☐ User Based PSK

[i](#)

☒ Advance

Local ID Type:

Content:

Peer ID Type:

Content:

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

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

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

CONFIGURATION > Network > NAT > Add

General Settings	
<input checked="" type="checkbox"/> Enable Rule	
Rule Name:	VPN_NAT
Port Mapping Type	
Classification:	<input type="radio"/> Virtual Server <input checked="" type="radio"/> 1:1 NAT <input type="radio"/> Many 1:1 NAT
Mapping Rule	
Incoming Interface:	ge1
Original IP:	User Defined
User-Defined Original IP:	172.100.20.30 (IP Address)
Mapped IP:	User Defined
User-Defined Mapped IP:	192.168.1.33 (IP Address)
Port Mapping Type:	any

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

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

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

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

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

CONFIGURATION > Security Policy > Policy Control

General Settings

☒ Enable Policy Control

IPv4 Configuration

☒ Allow Asymmetrical Route

[Add](#)
[Edit](#)
[Remove](#)
[Activate](#)
[Inactivate](#)
[Move](#)
[Clone](#)

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

[Default_Allow_WAN_To_ZyWALL](#)
 Description: System Default Allow From WAN To ZyWALL
 Members:
 AH
 ESP
 IKE
 NATT
 GRE
 VRRP

[Apply](#)
[Reset](#)

Test the IPSec VPN Tunnel

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

CONFIGURATION > VPN > IPSec VPN > VPN Connection

[Add](#)
[Edit](#)
[Remove](#)
[Activate](#)
[Inactivate](#)
[Connect](#)
[Disconnect](#)
[Object References](#)

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

Page 1 of 1 Show 50 items

Displaying 1 of 1

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

MONITOR > VPN Monitor > IPSec

Disconnect		Connection Check									
#	Name	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound(Byte)	Outbound(Byte)			
1	WLT_VPN_HQ	10.10.10.0/24<>192.168.20.0/24	192.168.1.33	P: 172.100.30.40:4500	14	8640s	0(0 bytes)	0(0 bytes)			
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1											

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][C]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

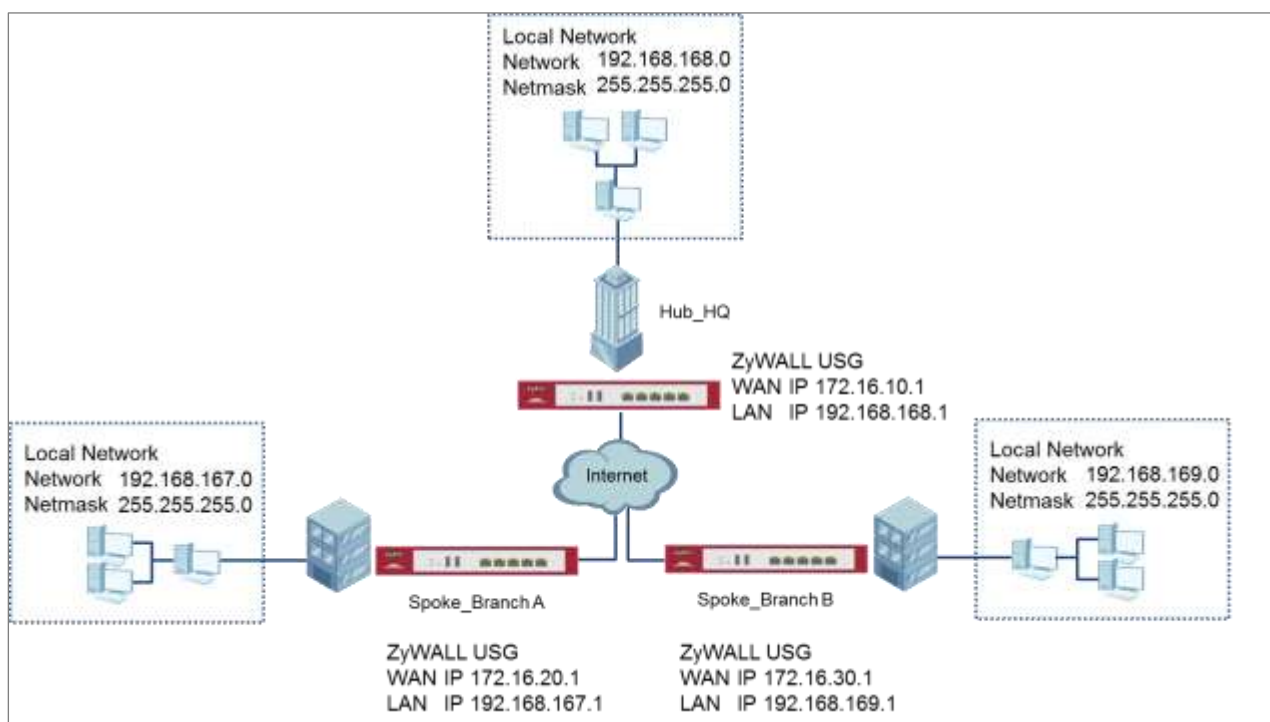
Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


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

How to Configure Hub-and-Spoke IPSec VPN

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

ZyWALL/USG Hub-and-Spoke VPN Example

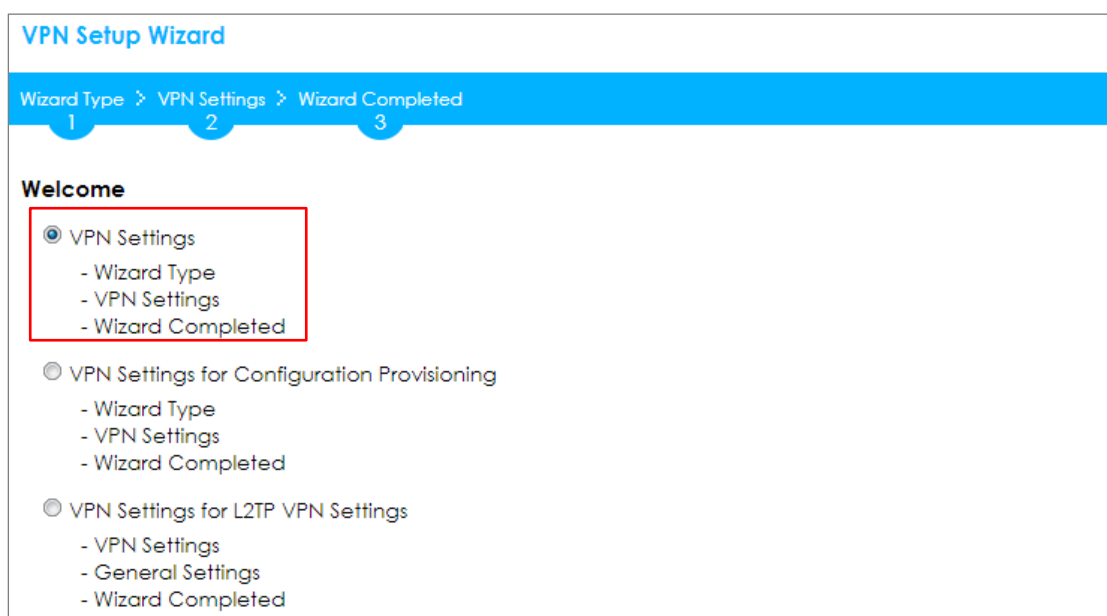


 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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

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

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

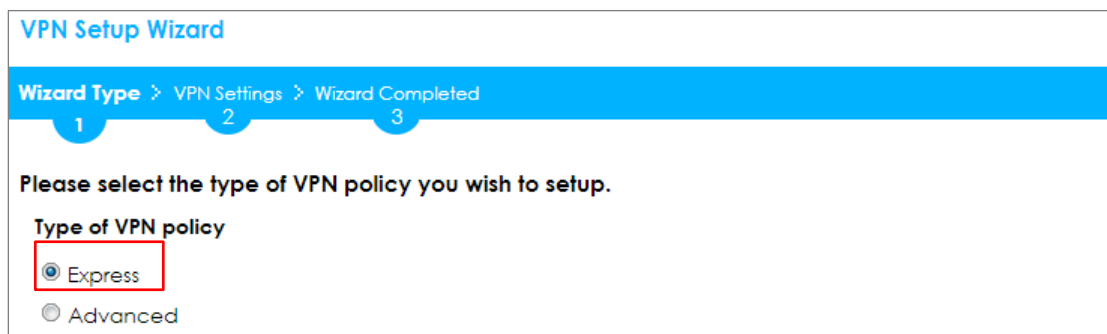
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

- ☒ Express
- ☐ Advanced

Type the **Rule Name** used to identify this VPN connection (and VPN gateway).

You may use 1-31 alphanumeric characters. This value is case-sensitive. Select the rule to be **Site-to-site**. Click **Next**.

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

Hub_HQ-to-Branch_A

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.16.20.1 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.167.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: Hub_HQ-to-Branch_A

Secure Gateway: 172.16.20.1

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.167.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

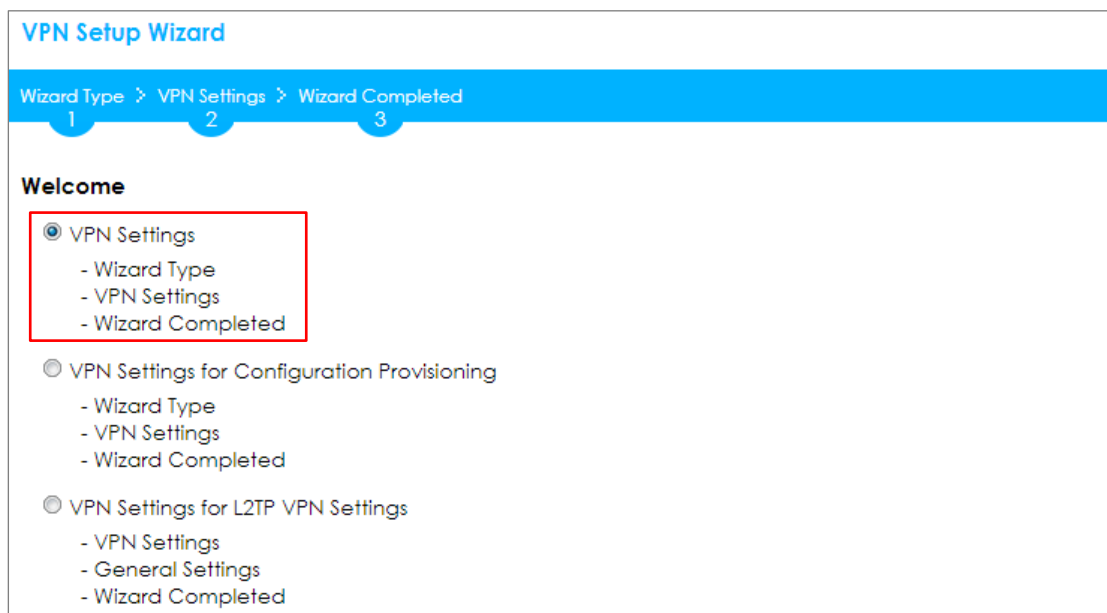
Summary

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

Hub_HQ-to-Branch_B

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

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

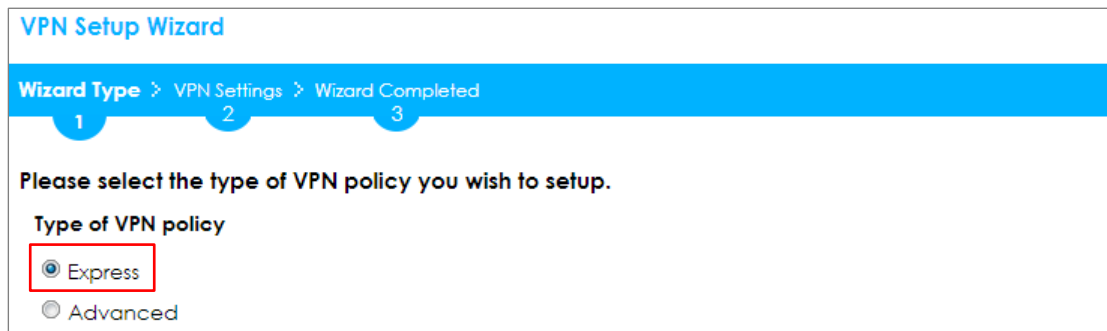
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

- ☒ Express
- ☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

Hub_HQ-to-Branch_B

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.16.30.1 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 255.255.255.0

Remote Policy (IP/Mask): 192.168.169.0 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

Summary

Rule Name: Hub_HQ-to-Branch_B

Secure Gateway: 172.16.30.1

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.169.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

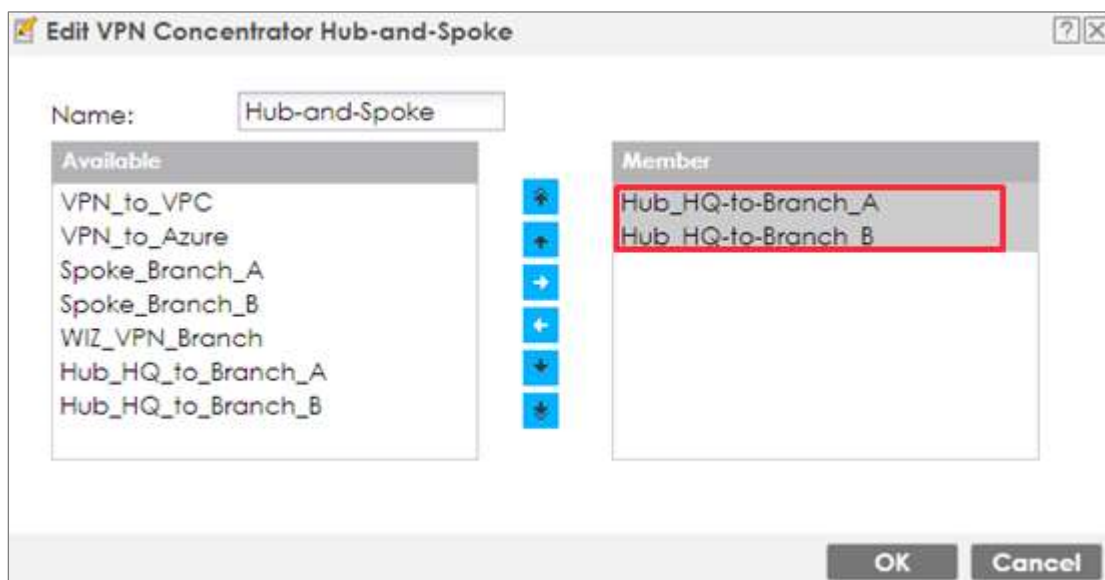
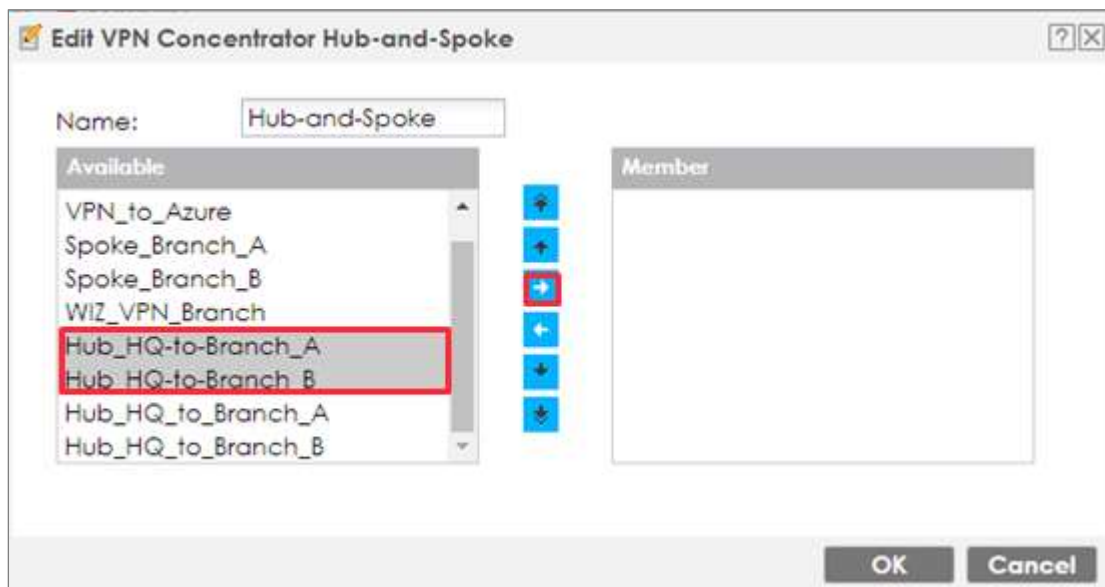
Congratulations. The VPN Access wizard is completed

Summary

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

Hub_HQ Concentrator

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



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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Welcome

☒ VPN Settings

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for Configuration Provisioning

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for L2TP VPN Settings

- VPN Settings
- General Settings
- Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

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

Type of VPN policy

☒ Express

☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

Spoke_Branch_A

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.16.10.1 (IP or FQDN)

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.167.0 255.255.255.0

Remote Policy (IP/Mask): 192.168.168.0 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: Spoke_Branch_A

Secure Gateway: 172.16.10.1

Pre-Shared Key: 12345678

Local Policy (IP/Mask): 192.168.167.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

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

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

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

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

Network > Routing > Policy Route

+

Add Policy Route

Show Advanced Settings

Create new Object ▼

Criteria

User:

any ▼

Incoming:

any (Excluding ZyV ▼

Source Address:

Spock_Branch_A_L ▼

Destination Address:

Spock_Branch_B_L ▼

DSCP Code:

any ▼

Schedule:

none ▼

Service:

any ▼

Next-Hop

Type:

VPN Tunnel ▼

VPN Tunnel:

Spoke_Branch_A ▼

Spoke_Branch_B

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

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

Type of VPN policy

- ☒ Express
- ☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Configuration

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

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Summary

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

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

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

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

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

Network > Routing > Policy Route

+

Add Policy Route

Show Advanced Settings

Create new Object

Criteria

User:

any

Incoming:

any (Excluding ZyV

Source Address:

Spock_Branch_B_L

Destination Address:

Spock_Branch_A_L

DSCP Code:

any

Schedule:

none

Service:

any

Next-Hop

Type:

VPN Tunnel

VPN Tunnel:

Spoke_Branch_B

Test the IPSec VPN Tunnel

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

Hub_HQ > CONFIGURATION > VPN > IPsec VPN > VPN Connection

IPv4 Configuration				
Add Edit Remove Activate Inactivate Connect Disconnect Object References				
#	Status	Name	VPN Gateway	Policy
1		Hub_HQ-to-Branch_A	Hub_HQ-to-Branch_A	Hub_HQ-to-Branch_A_LOCAL/Hub_HQ-to-Branch_A_REMOTE
2		Hub_HQ-to-Branch_B	Hub_HQ-to-Branch_B	Hub_HQ-to-Branch_B_LOCAL/Hub_HQ-to-Branch_B_REMOTE
Page 1 of 1 Show 50 items Displaying 1 - 2 of 2				

Spoke_Branch_A > CONFIGURATION > VPN > IPsec VPN > VPN Connection

IPv4 Configuration				
Add Edit Remove Activate Inactivate Connect Disconnect Object References				
#	Status	Name	VPN Gateway	Policy
1		Spoke-Branch_A	Spoke-Branch_A	Spoke-Branch_A_LOCAL/Spoke-Branch_A_REMOTE
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1				

Spoke_Branch_B > CONFIGURATION > VPN > IPsec VPN > VPN Connection

IPv4 Configuration				
Add Edit Remove Activate Inactivate Connect Disconnect Object References				
#	Status	Name	VPN Gateway	Policy
1		Spoke-Branch_B	Spoke-Branch_B	Spoke-Branch_B_LOCAL/Spoke-Branch_B_REMOTE
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1				

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

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

Disconnect		Connection Check						
#	Name	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound	Outbound
1	Hub_HQ-to-Branch_A	192.168.168.0/24<->192.168.167.0/24	172.16.10.1	P: 172.16.20.1	253	86167	0[0 bytes]	0[0 bytes]
2	Hub_HQ-to-Branch_B	192.168.168.0/24<->192.168.169.0/24	172.16.10.1	P: 172.16.30.1	68	86352	1[78 bytes]	0[0 bytes]

Page 1 of 1

Show 30 Items

Displaying 1 - 2 of 2


Connectivity Check

Connectivity Check

IP Address:

OK Cancel

Result

 ICMP Connectivity Check PASS on Hub_HQ-to-Branch_A

OK

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

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

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

?

X

Connectivity Check


Connectivity Check

IP Address:

OK Cancel

X

Result

 ICMP Connectivity Check PASS on Hub_HQ-to-Branch_B

OK

Spoke_Branch_A > MONITOR > VPN Monitor > IPsec

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

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

?

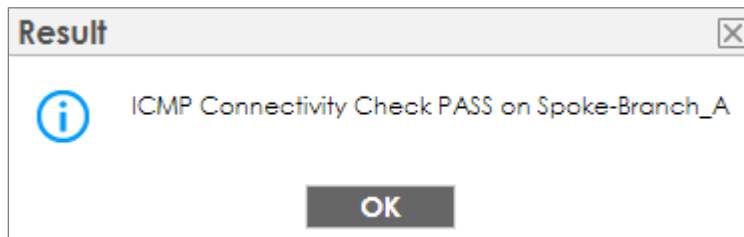
X

Connectivity Check

Connectivity Check

IP Address:

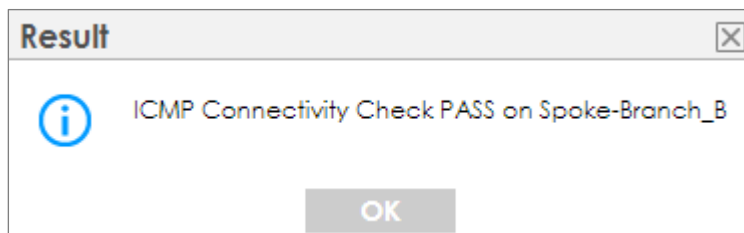
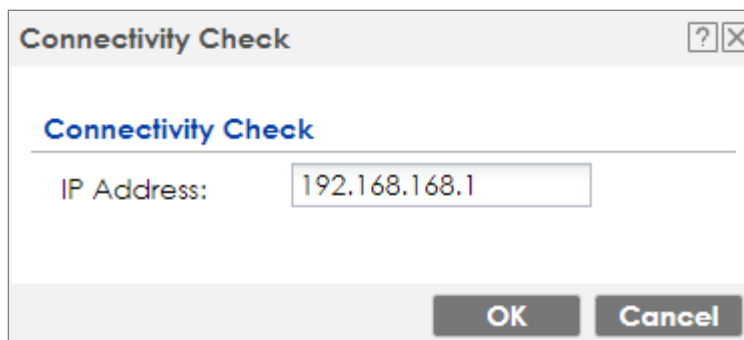
OK Cancel



Spoke_Branch_B > MONITOR > VPN Monitor > IPSec

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

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



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	SPt: 0x0 (0) SEQ: 0x0 (0) No rule found, Dropping TCP packet	IPSec
error	IPSec	SPt: 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][C]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

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

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

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

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

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

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name: Hub_HQ-to-Branch_A

IKE Version

☒ IKEv1
 ☐ IKEv2

Gateway Settings

My Address

☒ Interface ge2 DHCP client -- 172.16.10.1/255.255.255.
 ☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary 172.16.20.1
 Secondary 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

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

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

.....

unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

admin

☒ Advance

Phase 1 Settings

SA Life Time:

86400

(180 - 3000000 Seconds)

Negotiation Mode:

Main

☒ Advance

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** and select **Enable**.

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

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

General Settings

☒ Enable

Connection Name:

Hub_HQ-to-Branch_A

☒ Advance

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway:

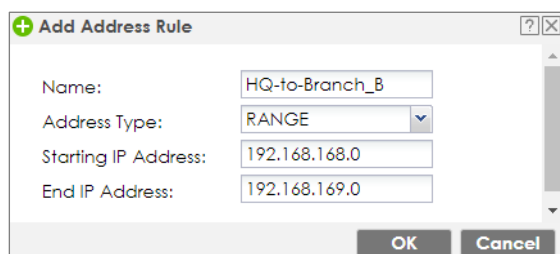
Hub_HQ-to-Branch

ge2 172.16.20.1, 0.0.0.0

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

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

Local Policy

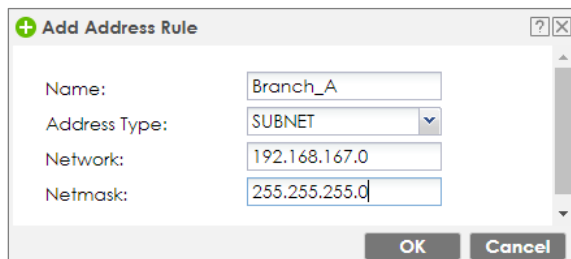


The 'Add Address Rule' dialog box is shown with the following fields:

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

Buttons: OK, Cancel

Remote Policy



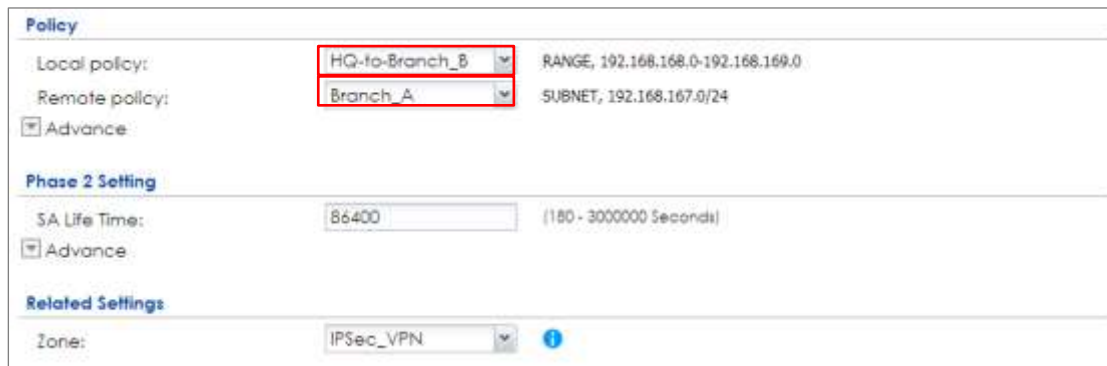
The 'Add Address Rule' dialog box is shown with the following fields:

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

Buttons: OK, Cancel

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



The 'Policy' configuration page is shown with the following settings:

- Local policy: HQ-to-Branch_B (highlighted with a red box)
- Remote policy: Branch_A (highlighted with a red box)
- Advance: (checkbox)
- Phase 2 Setting:
 - SA Life Time: 86400 (180 - 3000000 Seconds)
 - Advance: (checkbox)
- Related Settings:
 - Zone: IPSec_VPN

Hub_HQ-to-Branch_B

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

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

CONFIGURATION > VPN > IPsec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name: Hub_HQ-to-Branch_B

IKE Version

☒ IKEv1
 ☐ IKEv2

Gateway Settings

My Address

☒ Interface ge2 DHCP client -- 172.16.10.1/255.255.255.
 ☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary 172.16.30.1
 Secondary 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

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

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

☐ unmasked

☐ Certificate default (See [My Certificates](#))

☐ User Based PSK admin

☒ Advance

Go to **CONFIGURATION > VPN > IPsec VPN > VPN Connection** and select **Enable**.

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

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

General Settings

☒ Enable

Connection Name:

Hub_HQ-to-Branch_B

☐ Advance

VPN Gateway

Application Scenario

☒ Site-to-site
 ☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway:

Hub_HQ-to-Branch

ge2 172.16.30.1, 0.0.0.0

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

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

Local Policy



The 'Add Address Rule' dialog box is shown with the following fields:

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

Buttons: OK, Cancel

Remote Policy



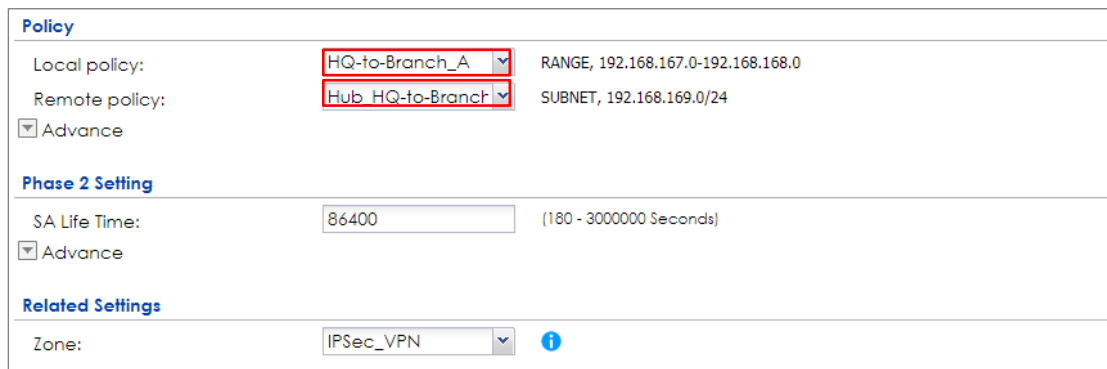
The 'Add Address Rule' dialog box is shown with the following fields:

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

Buttons: OK, Cancel

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



The 'Policy' configuration page is shown with the following settings:

- Local policy:** HQ-to-Branch_A (Range, 192.168.167.0-192.168.168.0)
- Remote policy:** Hub_HQ-to-Branch (Subnet, 192.168.169.0/24)
- Phase 2 Setting:** SA Life Time: 86400 (180 - 3000000 Seconds)
- Related Settings:** Zone: IPSec_VPN

Spoke_Branch_A

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

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

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name:

IKE Version
☒ IKEv1
☐ IKEv2

Gateway Settings

My Address
☒ Interface DHCP client -- 172.16.20.1/255.255.255.
☐ Domain Name / IPv4

Peer Gateway Address
☒ Static Address Primary
Secondary
☐ Fall back to Primary Peer Gateway when possible
 Fail Back Check Interval: (60-86400 seconds)
☐ Dynamic Address

Authentication

☒ Pre-Shared Key
☐ unmasked

☐ Certificate (See [My Certificates](#))
☐ User Based PSK

☒ Advance

Phase 1 Settings

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

Go to **CONFIGURATION > VPN > IPsec VPN > VPN Connection** and select **Enable**.

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

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

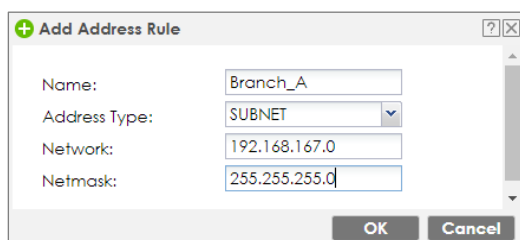


The screenshot shows the 'General Settings' and 'VPN Gateway' sections of the VPN Connection configuration page. In the 'General Settings' section, the 'Enable' checkbox is checked, and the 'Connection Name' is set to 'Spoke_Branch_A'. The 'Advance' checkbox is also checked. In the 'VPN Gateway' section, the 'Application Scenario' is set to 'Site-to-site'. The 'VPN Gateway' dropdown is set to 'Spoke_Branch_A', and the 'ge2' interface is selected with the IP address '172.16.10.1, 0.0.0.0'.

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

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Create new Object

Local Policy



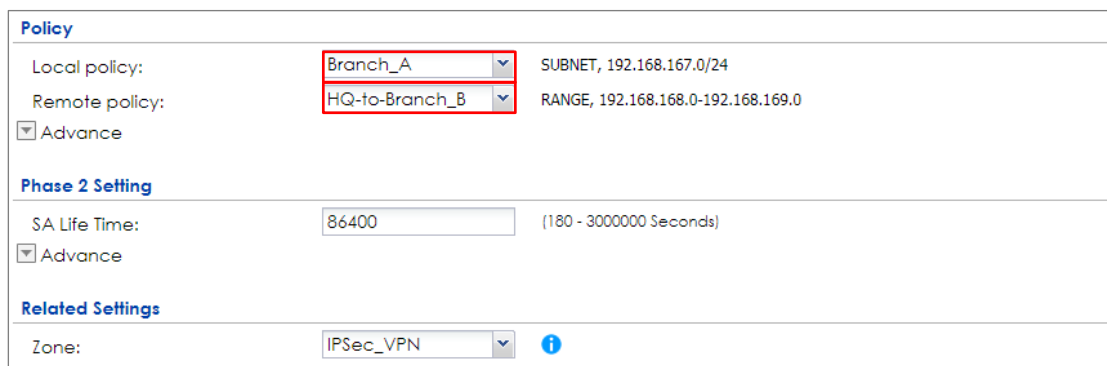
The screenshot shows the 'Add Address Rule' dialog box. The 'Name' field is set to 'Branch_A'. The 'Address Type' dropdown is set to 'SUBNET'. The 'Network' field is set to '192.168.167.0' and the 'Netmask' field is set to '255.255.255.0'. The 'OK' and 'Cancel' buttons are at the bottom.

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

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1
 ☐ IKEv2

Gateway Settings

My Address

☒ Interface DHCP client -- 172.16.30.1/255.255.255.
 ☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary
Secondary

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

☐ unmasked

☐ Certificate (See [My Certificates](#))
 ☐ User Based PSK

☒ Advance

Phase 1 Settings

SA Life Time: (180 - 3000000 Seconds)

Negotiation Mode:

☒ Advance

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

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

General Settings

☒ Enable

Connection Name:

☐ Advance

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway: ge2 172.16.10.1, 0.0.0.0

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

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

Local Policy

Add Address Rule

Name:

Address Type:

Network:

Netmask:

Remote Policy



Add Address Rule

Name:

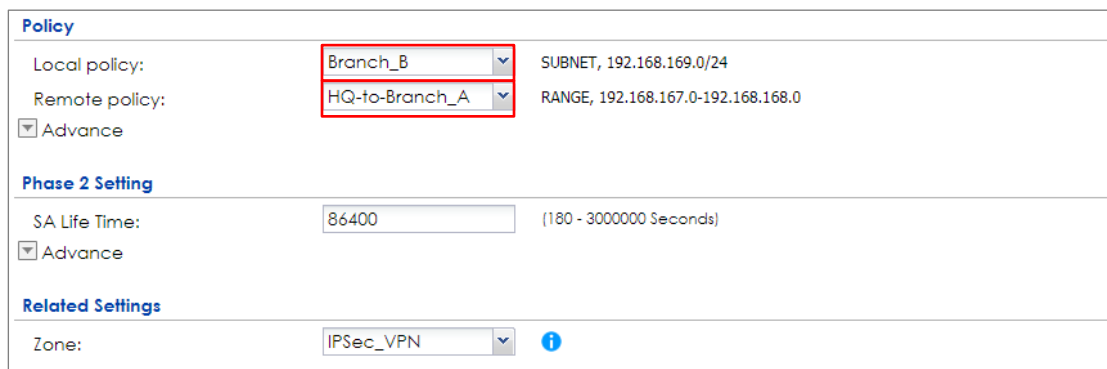
Address Type:

Starting IP Address:

End IP Address:

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

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Policy



Policy

Local policy: SUBNET, 192.168.169.0/24

Remote policy: RANGE, 192.168.167.0-192.168.168.0

☐ Advance

Phase 2 Setting

SA Life Time: (180 - 3000000 Seconds)

☐ Advance

Related Settings

Zone: ⓘ

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



IPv4 Configuration

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

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

Spoke_Branch_A > CONFIGURATION > VPN > IPSec VPN > VPN Connection

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

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

Spoke_Branch_B > CONFIGURATION > VPN > IPSec VPN > VPN Connection

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

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

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

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

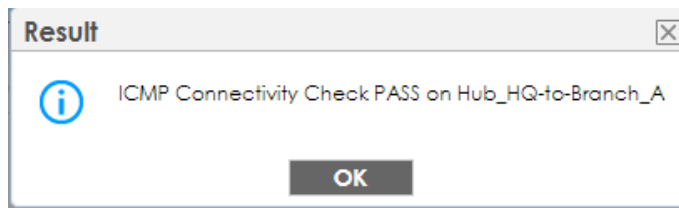
#	Name	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound	Outbound
1	Hub_HQ-to-Branch_A	192.168.168.0-192.168.169.0<->192.168.167.0/24	172.16.10.1	P: 172.16.20.1	584	85836	0/0 by...	0/0 by...
2	Hub_HQ-to-Branch_B	192.168.167.0-192.168.168.0<->192.168.169.0/24	172.16.10.1	P: 172.16.30.1	23	86397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

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

Connectivity Check

Connectivity Check

IP Address:



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

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

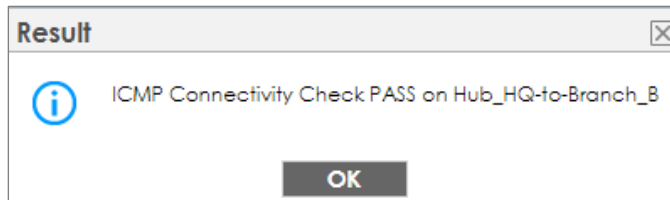
Page 1 of 1 Show 50 Items Displaying 1 - 2 of 2

Connectivity Check

Connectivity Check

IP Address: 192.168.169.1

OK Cancel



Spoke_Branch_A > MONITOR > VPN Monitor > IPSec

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

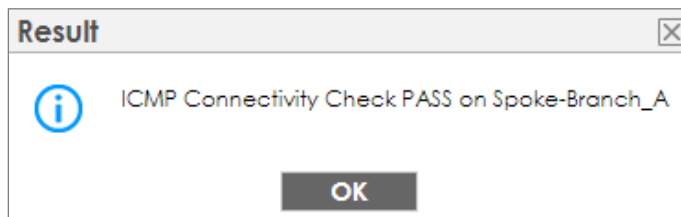
Page 1 of 1 Show 50 Items Displaying 1 - 1 of 1

Connectivity Check

Connectivity Check

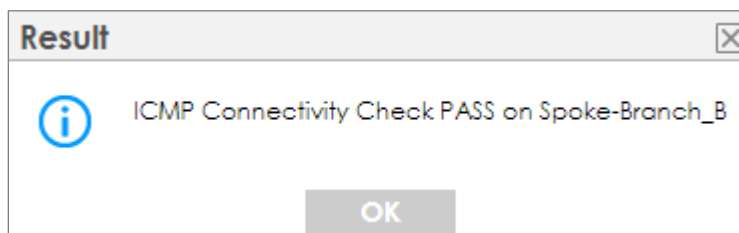
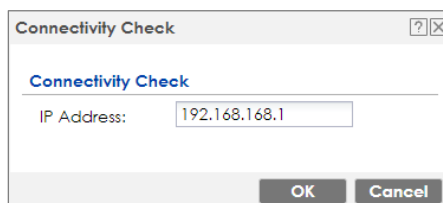
IP Address: 192.168.168.1

OK Cancel



Spoke_Branch_B > MONITOR > VPN Monitor > IPSec

Disconnect		Connection Check						
#	Name	Policy	My Address	Secure Gateway	Sp. ID	Time	In...	Out...
1	Spoke_Branch_B	192.168.169.0/24<>192.168.167.0-192.168.168.0	172.16.30.1	P: 172.16.10.1	115	86305	0/0 b...	0/0 b...
Page 1 of 1		Show 50 Items		Displaying 1 of 1				



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.

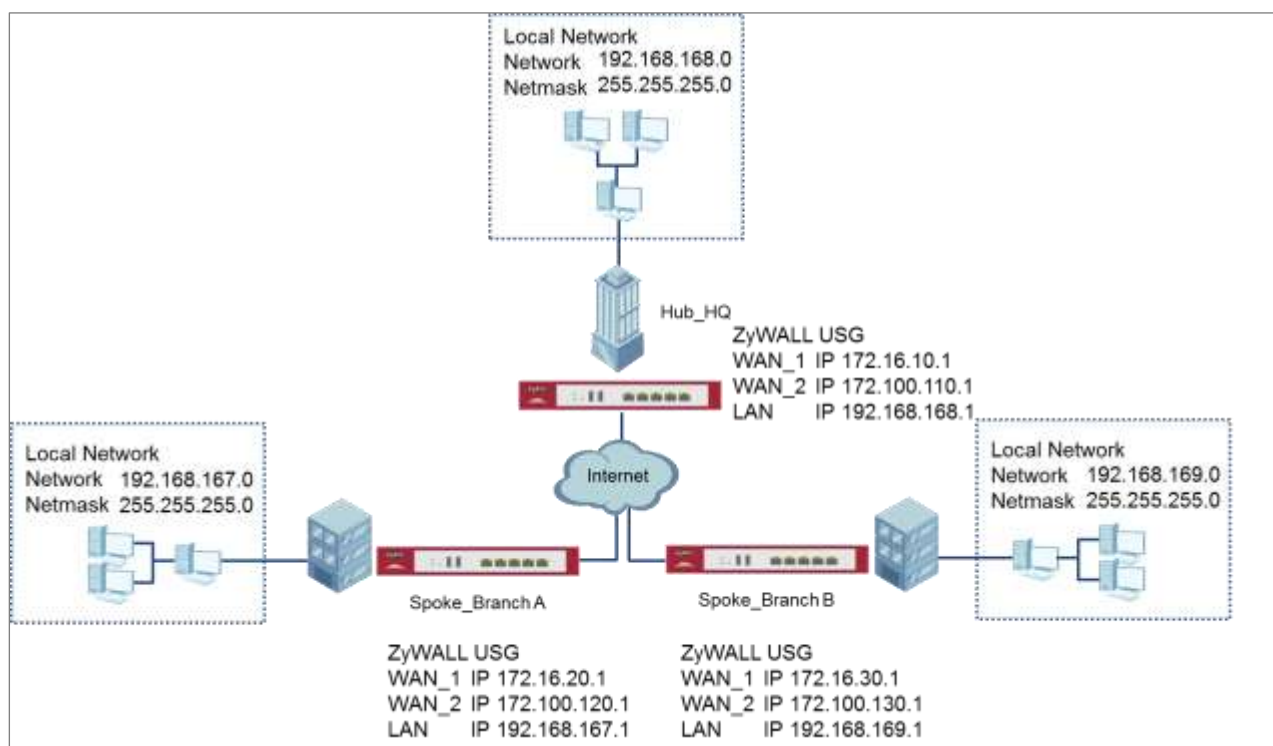
19	2017-09-11 ...	info	IKE	[SA] : No proposal chosen	IKE_LOG
20	2017-09-11 ...	info	IKE	[ID] : Tunnel [Server] Phase 2 Local policy mismatch	IKE_LOG
31	2017-09-11 ...	info	IKE	Send:[HASH][SA][NONCE][ID][C]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG

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

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

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

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

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

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

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name: Hub_HQ-to-Branch_A

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface

ge2

DHCP client -- 172.16.10.1/255.255.255.

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary

172.16.20.1

Secondary

172.100.120.1

☒ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval:

300

(60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

.....

unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

admin

☒ Advance

Phase 1 Settings

SA Life Time:

86400

(180 - 3000000 Seconds)

Negotiation Mode:

Main

☒ Advance

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

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

General Settings

☒ Enable

Connection Name:

Hub_HQ-to-Branch_A

☒ Advance

VPN Gateway

Application Scenario

☒ Site-to-site
 ☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway:

Hub_HQ-to-Branch_A

ge2 172.16.20.1, 172.100.120.1

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

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

Local Policy



The 'Add Address Rule' dialog box is shown with the following fields:

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

Buttons: OK, Cancel

Remote Policy



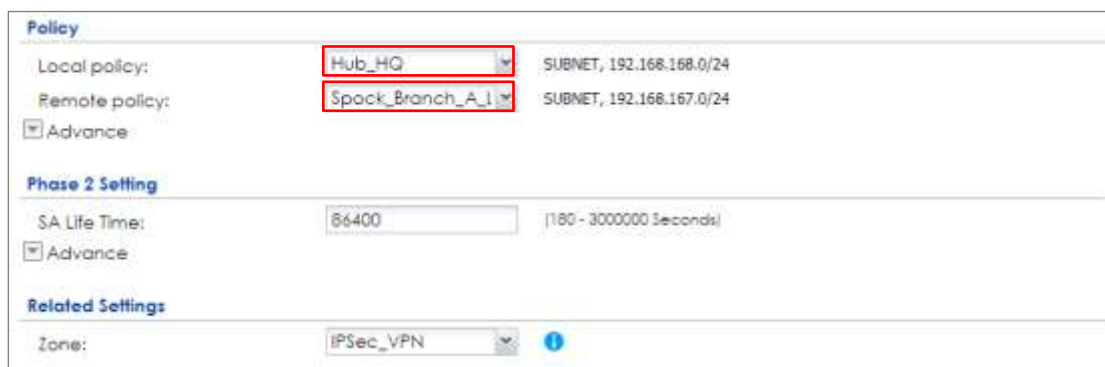
The 'Add Address Rule' dialog box is shown with the following fields:

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

Buttons: OK, Cancel

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



The 'Policy' configuration page is shown with the following settings:

- Local policy: Hub_HQ (highlighted with a red box)
- Remote policy: Spoke_Branch_A_LO (highlighted with a red box)
- Advance: [X] (checked)
- Phase 2 Setting:
 - SA Life Time: 86400 (180 - 3000000 Seconds)
 - Advance: [X] (checked)
- Related Settings:
 - Zone: IPSec_VPN

Hub_HQ-to-Branch_B

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

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

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

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name:

Hub_HQ-to-Branch_B

IKE Version

☒ IKEv1
 ☐ IKEv2

Gateway Settings

My Address

☒ Interface

ge2

DHCP client -- 172.16.10.1/255.255.255.

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary

172.16.30.1

Secondary

172.100.130.1

☒ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval:

300

(60-86400 seconds)

Authentication

☒ Pre-Shared Key

.....

☐ unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

admin

☐ Advance

Phase 1 Settings

SA Life Time:

86400

(180 - 3000000 Seconds)

Negotiation Mode:

Main

☐ Advance

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

General Settings

☒ Enable

Connection Name:

Hub_HQ-to-Branch_B

☐ Advance

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer
 ☐ Remote Access (Server Role)
 ☐ Remote Access (Client Role)
 ☐ Vpn Tunnel Interface

VPN Gateway:

Hub_HQ-to-Branch

ge2 172.16.30.1, 172.100.130.1

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

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

Local Policy



The 'Add Address Rule' dialog box is shown with the following fields:

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

Buttons: OK, Cancel

Remote Policy



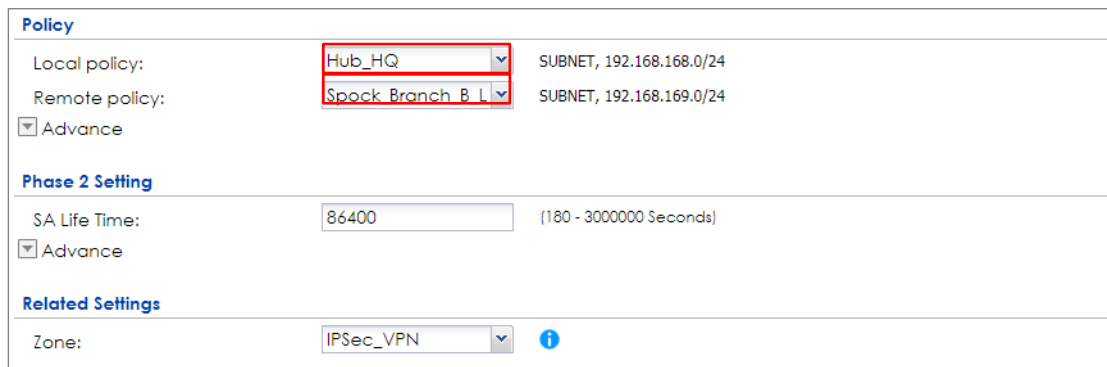
The 'Add Address Rule' dialog box is shown with the following fields:

- Name: Spoke_Branch_B_LOC
- Address Type: SUBNET
- Network: 192.168.169.0
- Netmask: 255.255.255.0

Buttons: OK, Cancel

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

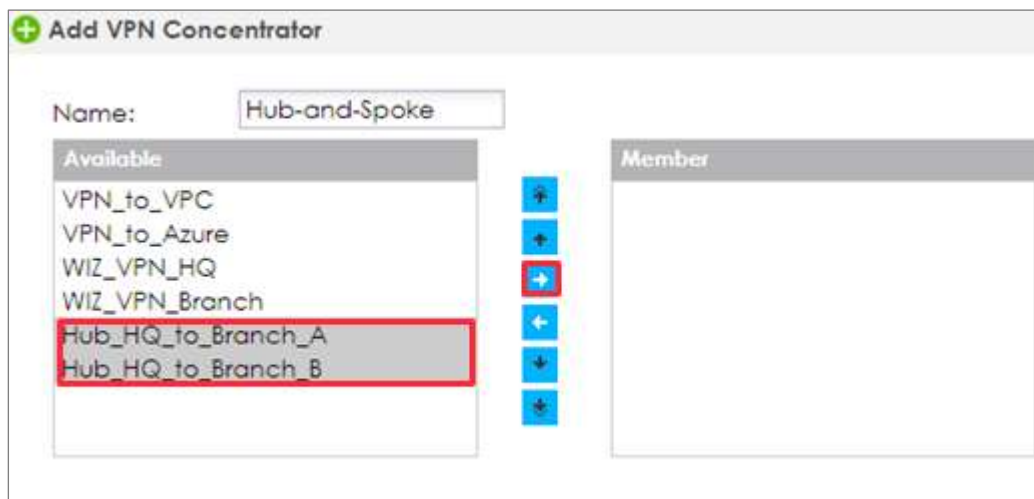


The 'Policy' configuration page is shown with the following settings:

- Local policy:** Hub_HQ (selected from dropdown)
- Remote policy:** Spoke_Branch_B_L (selected from dropdown)
- Advance:** (checkbox checked)
- Phase 2 Setting:**
 - SA Life Time:** 86400 (180 - 3000000 Seconds)
 - Advance:** (checkbox checked)
- Related Settings:**
 - Zone:** IPSec_VPN (selected from dropdown)

Hub_HQ Concentrator

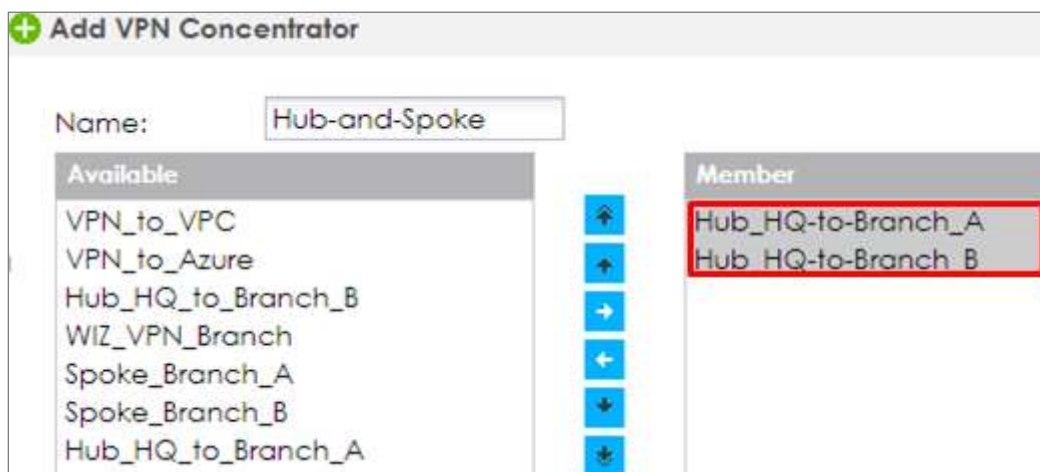
In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPSec VPN > Concentrator**, add a VPN Concentrator rule. Select VPN tunnels to the same member group and click **Save**.



+ Add VPN Concentrator

Name:

Available		Member
VPN_to_VPC	⬆	
VPN_to_Azure	+	
WIZ_VPN_HQ	➡	
WIZ_VPN_Branch	⬅	
Hub_HQ_to_Branch_A	+	
Hub_HQ_to_Branch_B	⬇	



+ Add VPN Concentrator

Name:

Available		Member
VPN_to_VPC	⬆	Hub_HQ-to-Branch_A
VPN_to_Azure	+	Hub HQ-to-Branch B
Hub_HQ_to_Branch_B	➡	
WIZ_VPN_Branch	⬅	
Spoke_Branch_A	+	
Spoke_Branch_B	⬇	
Hub_HQ_to_Branch_A		

Spoke_Branch_A

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

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

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

CONFIGURATION > VPN > IPSec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface DHCP client -- 172.16.20.1/255.255.255.

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary

Secondary

☒ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key

.....

unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

Remote_Client

☐ Advance

Phase 1 Settings

SA Life Time:

86400

(180 - 3000000 Seconds)

Negotiation Mode:

Main

☐ Advance

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

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

General Settings

☒ Enable

Connection Name:

Spoke_Branch_A

☐ Advance

VPN Gateway

Application Scenario

☒ Site-to-site

☐ Site-to-site with Dynamic Peer
☐ Remote Access (Server Role)
☐ Remote Access (Client Role)
☐ Vpn Tunnel Interface

VPN Gateway:

Spoke_Branch_A

ge2 172.16.10.1, 172.100.110.1

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

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

Local Policy



The 'Add Address Rule' dialog box is shown with the following fields:

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

Buttons: OK, Cancel

Remote Policy



The 'Add Address Rule' dialog box is shown with the following fields:

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

Buttons: OK, Cancel

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



The 'Policy' configuration page is shown with the following settings:

- Local policy:** Spoke_Branch_A_LO (highlighted with a red box)
- Remote policy:** Hub_HQ (highlighted with a red box)
- Advance:** (expanded)
- Phase 2 Setting:**
 - SA Life Time: 86400 (180 - 3000000 Seconds)
- Related Settings:**
 - Zone: IPSec_VPN

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

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

Network > Routing > Policy Route

Criteria	
User:	any
Incoming:	any (Excluding ZyV)
Source Address:	Spoke_Branch_A_L
Destination Address:	Spoke_Branch_B_L
DSCP Code:	any
Schedule:	none
Service:	any
Next-Hop	
Type:	VPN Tunnel
VPN Tunnel:	Spoke_Branch_A

Spoke_Branch_B

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

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

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

CONFIGURATION > VPN > IPsec VPN > VPN Gateway

General Settings

☒ Enable

VPN Gateway Name:

IKE Version
☐ IKEv1
☐ IKEv2

Gateway Settings

My Address
☒ Interface DHCP client -- 172.16.30.1/255.255.255.
☐ Domain Name / IPv4

Peer Gateway Address
☒ Static Address ?
 Primary
 Secondary
☒ Fall back to Primary Peer Gateway when possible
 Fall Back Check Interval: (60-86400 seconds)
☐ Dynamic Address ?

Authentication

☒ Pre-Shared Key
☐ unmasked
☐ Certificate (See [My Certificates](#))
☐ User Based PSK ?
☒ Advance

Phase 1 Settings
 SA Life Time: (180 - 3000000 Seconds)
 Negotiation Mode:
☒ Advance

Go to **CONFIGURATION > VPN > IPsec VPN > VPN Connection** and select **Enable**.

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

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



General Settings

☒ Enable

Connection Name:

☐ Advance

VPN Gateway

Application Scenario:

- ☒ Site-to-site
- ☐ Site-to-site with Dynamic Peer
- ☐ Remote Access (Server Role)
- ☐ Remote Access (Client Role)
- ☐ Vpn Tunnel Interface

VPN Gateway: ge2 172.16.10.1, 172.100.110.1

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

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



Add Address Rule

Name:

Address Type:

Network:

Netmask:

Remote Policy



Add Address Rule

Name:

Address Type:

Network:

Netmask:

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

CONFIGURATION > VPN > IPSec VPN > VPN Connection > Policy

Policy	
Local policy:	Spoke_Branch_B_L SUBNET, 192.168.169.0/24
Remote policy:	Hub_HQ SUBNET, 192.168.168.0/24
<input type="checkbox"/> Advance	
Phase 2 Setting	
SA Life Time:	86400 (180 - 3000000 Seconds)
<input type="checkbox"/> Advance	
Related Settings	
Zone:	IPSec_VPN

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

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


Network > Routing > Policy Route

Criteria	
User:	any
Incoming:	any (Excluding ZyV)
Source Address:	Spoke_Branch_B_L
Destination Address:	Spoke_Branch_A_L
DSCP Code:	any
Schedule:	none
Service:	any
Next-Hop	
Type:	VPN Tunnel
VPN Tunnel:	Spoke_Branch_B

Test the IPSec VPN Tunnel

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

Hub_HQ > CONFIGURATION > VPN > IPsec VPN > VPN Connection



The screenshot shows the 'IPv4 Configuration' window with a table of VPN connections. The table has columns for #, Status, Name, VPN Gateway, and Policy. There are two entries: 1. Hub_HQ-to-Branch_A and 2. Hub_HQ-to-Branch_B. Both have a green 'Connect' icon in the Status column. The Policy column shows 'Hub_HQ/*Spoke_Branch_A_LOCAL' and 'Hub_HQ/*Spoke_Branch_B_LOCAL' respectively. The bottom of the window shows 'Page 1 of 1' and 'Show 50 Items'.

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

Spoke_Branch_A > CONFIGURATION > VPN > IPsec VPN > VPN Connection



The screenshot shows the 'IPv4 Configuration' window for Spoke_Branch_A. The table has one entry: 1. Spoke-Branch_A. The Status column shows a green 'Connect' icon. The Policy column shows 'Spoke-Branch_A_LOCAL/*Hub_HQ'. The bottom of the window shows 'Page 1 of 1' and 'Show 50 Items'.

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

Spoke_Branch_B > CONFIGURATION > VPN > IPsec VPN > VPN Connection



The screenshot shows the 'IPv4 Configuration' window for Spoke_Branch_B. The table has one entry: 1. Spoke-Branch_B. The Status column shows a green 'Connect' icon. The Policy column shows 'Spoke-Branch_B_LOCAL/*Hub_HQ'. The bottom of the window shows 'Page 1 of 1' and 'Show 50 Items'.

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

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

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

		Disconnect		Connection Check							
#	Name	Policy	My Addr...	Secure Gateway...	Up Time	Timeout	Inbound...	Outbound...			
1	Hub_HQ-to-Branch_A	192.168.168.0/24<>192.168.167.0/24	172.16.10.1	P: 172.16.20.1	690	85730	1(46 bytes)	1(80 bytes)			
2	Hub_HQ-to-Branch_B	192.168.168.0/24<>192.168.169.0/24	172.16.10.1	P: 172.16.30.1	505	85915	1(78 bytes)	0(0 bytes)			

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

Connectivity Check

Connectivity Check

IP Address: 192.168.167.1

OK Cancel

Result

ICMP Connectivity Check PASS on Hub_HQ-to-Branch_A

OK

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

		Disconnect		Connection Check							
#	Name	Policy	My Addr...	Secure Gateway...	Up Time	Timeout	Inbound...	Outbound...			
1	Hub_HQ-to-Branch_A	192.168.168.0/24<>192.168.167.0/24	172.16.10.1	P: 172.16.20.1	690	85730	1(46 bytes)	1(80 bytes)			
2	Hub_HQ-to-Branch_B	192.168.168.0/24<>192.168.169.0/24	172.16.10.1	P: 172.16.30.1	505	85915	1(78 bytes)	0(0 bytes)			

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

Connectivity Check

Connectivity Check

IP Address: 192.168.169.1

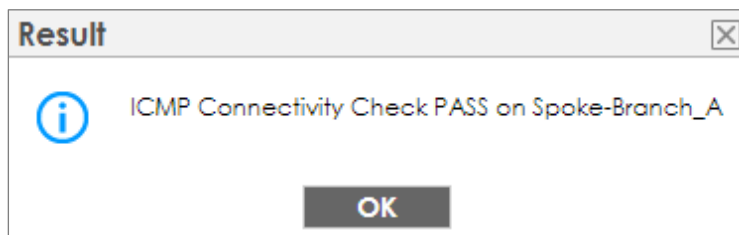
OK Cancel

Result

ICMP Connectivity Check PASS on Hub_HQ-to-Branch_B

OK

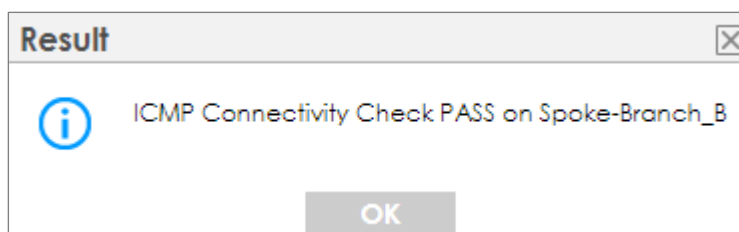
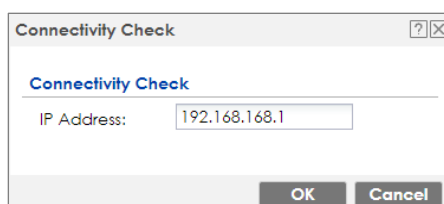
Spoke_Branch_A > MONITOR > VPN Monitor > IPSec



Spoke_Branch_B > MONITOR > VPN Monitor > IPSec

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

Page 1 of 1 | Show 30 Items | Displaying 1 - 1 of 1



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.

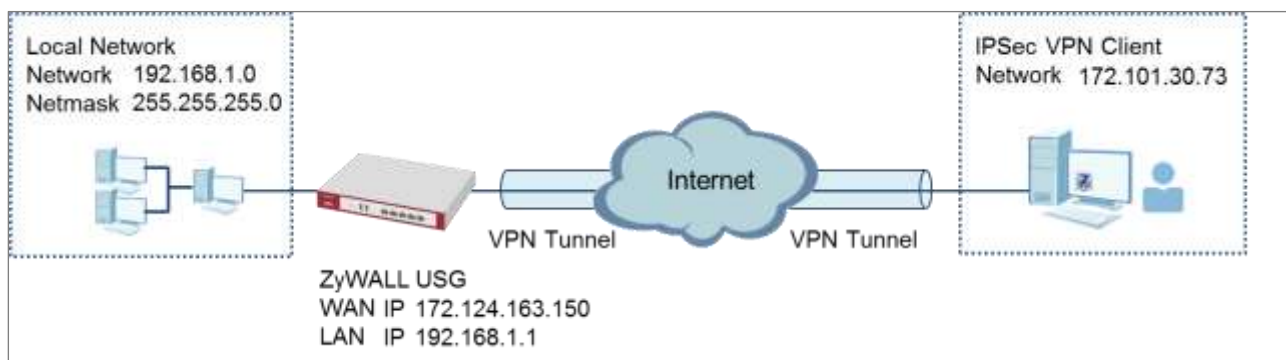
19	2017-09-11 ...	info	IKE	[SA] : No proposal chosen	IKE_LOG
20	2017-09-11 ...	info	IKE	[ID] : Tunnel [server] Phase 2 Local policy mismatch	IKE_LOG
31	2017-09-11 ...	info	IKE	Send:[HASH][SA][NONCE][ID][C]	IKE_LOG
32	2017-09-11 ...	info	IKE	Phase 1 IKE SA process done	IKE_LOG


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 Configure IPSec VPN with ZyWALL IPSec VPN Client

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



 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 ZyWALL IPSec VPN

ZyWALL IPSec VPN Client with VPN Tunnel Connected

Set Up the ZyWALL/USG IPSec VPN Tunnel

In the ZyWALL/USG, go to **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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☐ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☒ **VPN Settings for Configuration Provisioning**
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3


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

Type of VPN policy

- ☒ **Express**
- ☐ Advanced

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

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



VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: **WIZ_VPN_PROVISIONING**

Application Scenario: Remote Access (Server Role)

Type a secure **Pre-Shared Key** (8-32 characters). Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-2



VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: Any

Pre-Shared Key: **zyx12345**

Local Policy (IP/Mask): **192.168.1.33 / 255.255.255.0**

Remote Policy (IP/Mask): Any

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_PROVISIONING

Secure Gateway: Any

Pre-Shared Key: zyx12345

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): Any

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name: WIZ_VPN_PROVISIONING

Secure Gateway: Any

Pre-Shared Key: zyx12345

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): Any

Go to **CONFIGURATION > Object > User/Group > Add A User** and create a user account for the ZyWALL IPSec VPN Client user.

CONFIGURATION > Object > User/Group > Add A User

User Configuration

User Name :

Remote_Client

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

Go to **CONFIGURATION > VPN > IPSec VPN > Configuration Provisioning**. In the **General Settings** section, select the **Enable Configuration Provisioning**. Then, go to the **Configuration** section and click **Add** to bind a configured **VPN Connection** to **Allowed User**. Click **Activate** and **Apply** to save the configuration.

CONFIGURATION > VPN > IPSec VPN > Configuration Provisioning

General Settings

☒ Enable Configuration Provisioning

Authentication

Client Authentication Method:

default

Configuration

Add

Edit

Remove

Activate

Inactivate

Move

ID	Status	Priority	Type	VPN Connection	Allowed User
1		1	4in4	WIZ_VPN_PROVISIONING	Remote_Client

Page 1 of 1

Show 50 Items

Displaying 1 - 1 of 1

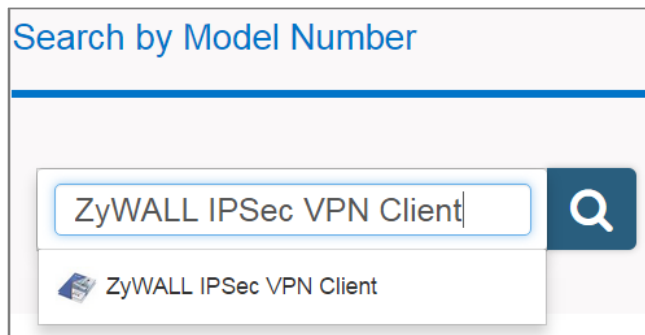
Apply

Reset

Set Up the ZyWALL IPSec VPN Client

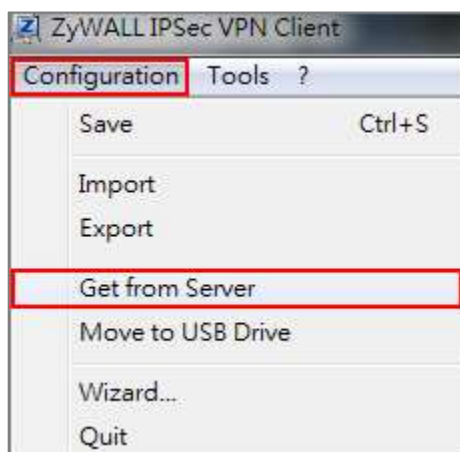
Download **ZyWALL IPSec VPN Client** software from ZyXEL Download Library:

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



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: Port:

Authentication:

Login:

Password:

CONFIGURATION > Get from Server > Step 2: Processing



VPN Configuration Server Wizard

Step 2: Processing...

Requesting the VPN Configuration.

Downloading the VPN Configuration from the server:

- ☒ Init Ok.
- ☒ Init crx server (172.124.163.150) Ok.
- ☐ Send https request...
 - Receive Config. from Server...
 - Write Config. file...
 - Apply Config. file...

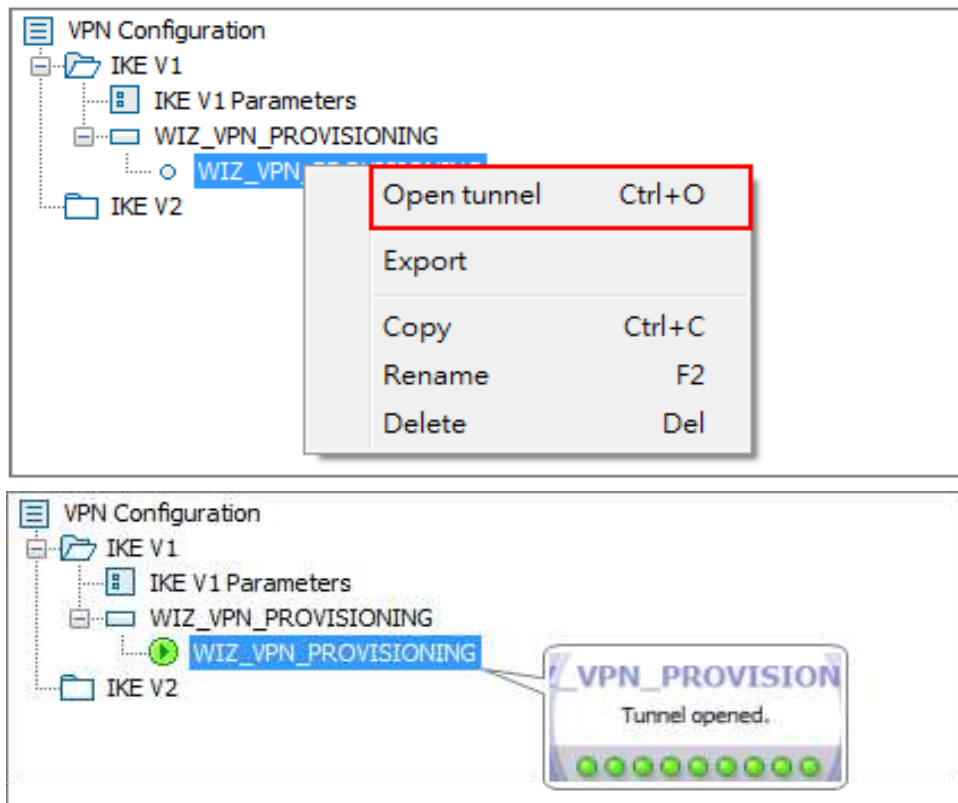
Then, you will see the **Configuration successful** page, click **OK** to exit the wizard.

CONFIGURATION > Get from Server > Configuration successful



Go to **VPN Configuration > IKEv1**, right click the **WIZ_VPN_PROVISIONING** and select **Open tunnel**. You will see the **Tunnel opened** on the bottom right of the screen.

VPN CONFIGURATION > IKE V1 > WIZ_VPN_PROVISIONING > Open tunnel



Test the 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 **Inbound(Bytes)/Outbound(Bytes)** Traffic.

MONITOR > VPN Monitor > IPSec

#	ID	Device	IPsec	My Address	Remote Gateway	Up Time	Download	Upload/Byte/s	Count/Byte/s
1	N/A	N/A	WS_VPN_PROVIDING	192.168.1.0/24	172.101.30.73	172.101.30.150	0	854/4	211854/bytes

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

PC with ZyWALL IPSec VPN Client installed > 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 behind ZyWALL/USG > Window 7 > cmd > ping 172.101.30.73

```
C:\Documents and Settings\ZYXEL>ping 172.101.30.73

Pinging 172.101.30.73 with 32 bytes of data:

Reply from 172.101.30.73: bytes=32 time=18ms TTL=54
Reply from 172.101.30.73: bytes=32 time=17ms TTL=54
Reply from 172.101.30.73: bytes=32 time=17ms TTL=54
Reply from 172.101.30.73: bytes=32 time=16ms TTL=54

Ping statistics for 172.101.30.73:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

What Can Go Wrong?

If you see [info] log message such as below, please make sure both ZyWALL/USG and ZyWALL IPSec VPN Client use the same **Pre-Shared Key** to establish the IKE SA.

MONITOR > Log

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 [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. ZyWALL/USG and ZyWALL IPsec VPN Client must use the same Encryption, Authentication method, DH key group and ID Type/Content to establish the IKE SA.

MONITOR > Log

Info	IKE	[SA] : No proposal chosen	IKE_LOG
Info	IKE	[SA] : Tunnel [WIZ_VPN_PROVISIONING] Phase 1 proposal mismatch	IKE_LOG

If you see that Phase 1 IKE SA process done but still get [alert] or [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG and ZyWALL IPsec VPN Client must use the same Active Protocol, Encapsulation, Proposal, PFS and set correct Local Policy to establish the IKE SA.

MONITOR > Log

Info	IKE	[SA] : No proposal chosen	IKE_LOG
Info	IKE	[SA] : Tunnel [WIZ_VPN_PROVISIONING] Phase 2 proposal mismatch	IKE_LOG

Info	IKE	[SA] : No proposal chosen	IKE_LOG
Info	IKE	[ID] : Tunnel [WIZ_VPN_PROVISIONING] Phase 2 Local policy mismatch	IKE_LOG

If you see [alert] log message as below, please make sure you create a user account for the ZyWALL IPsec VPN Client user on ZyWALL/USG or the external authentication server. Or please check your password matches the settings in the user account.

MONITOR > Log

Priority	Category	Message	Note
Alert	User	Failed login attempt to Device from http/https (incorrect password or inexistent username)	Account: Remote_Client

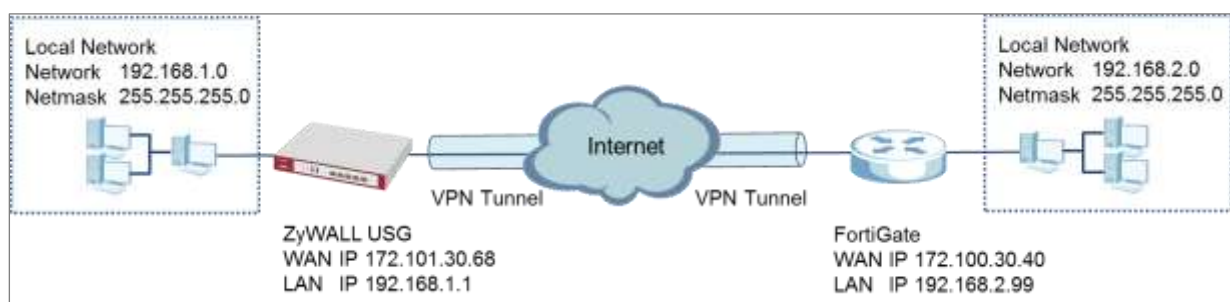
Make sure the service HTTPS **Port** on IPsec VPN Client application is available.

Make sure the To-ZyWALL security policies allow IPsec VPN traffic to the ZyWALL/USG. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


The ZyWALL/USG supports UDP port 500 and UDP port 4500 for NAT traversal. If you enable this, make sure the To-ZyWALL security policies allow UDP port 4500 too.

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: 6.2.0).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

- ☒ Express
- ☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: (IP or FQDN)

Pre-Shared Key:

Local Policy (IP/Mask): /

Remote Policy (IP/Mask): /

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

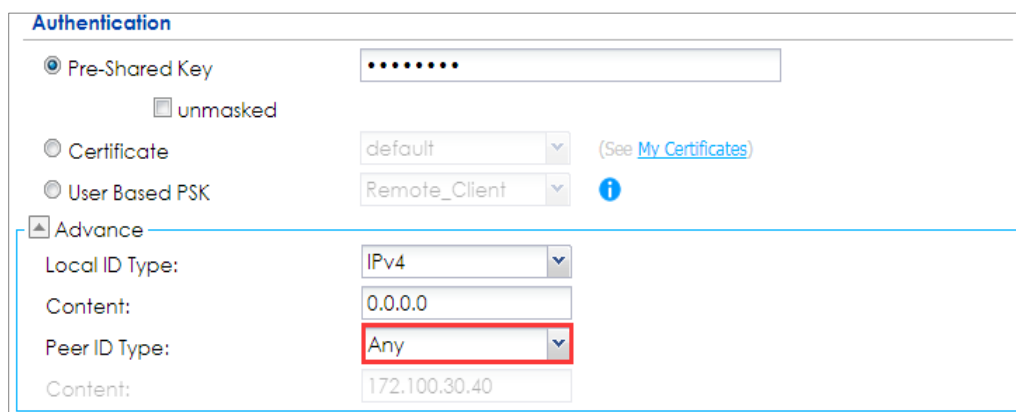
Rule Name:	WIZ_VPN_Fortigate
Secure Gateway:	172.100.30.40
Pre-Shared Key:	ZyXEL123
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.2.0 / 255.255.255.0

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

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

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

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



Authentication

☒ Pre-Shared Key
☐ unmasked

☐ Certificate (See [My Certificates](#))

☐ User Based PSK ⓘ

Advance

Local ID Type:

Content:

Peer ID Type: (highlighted with a red box)

Content:

Set Up the IPsec VPN Tunnel on the FortiGate

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

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



1 VPN Setup

Name: (highlighted with a red box)

Template:

- ☐ Dialup - FortiClient (Windows, Mac OS, Android)
- ☐ Site to Site - FortiGate
- ☐ Dialup - iOS (Native)
- ☐ Dialup - Android (Native L2TP/IPsec)
- ☐ Dialup - Cisco Firewall
- ☐ Site to Site - Cisco
- ☒ Custom VPN Tunnel (No Template) (highlighted with a red box)

< Back Next > Cancel

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

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

Name: **WIZ_VPN_ZyWALL**

Comments: Comments

Network

IP Version: ☒ IPv4 ☐ IPv6

Remote Gateway: **Static IP Address**

IP Address: **172.101.30.68**

Interface: **wan1**

Mode Config: ☐

NAT Traversal: ☒

Keepalive Frequency: 10

Dead Peer Detection: ☒

Static IP Address
Dialup User
Dynamic DNS

dmz
ha1
ha2
lan
wan1
wan2

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

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

Authentication

Method: **Pre-shared Key**

Pre-shared Key: **ZyXEL123** ☒ Show Key

IKE

Version: ☒ 1 ☐ 2

Mode: ☐ Aggressive ☒ **Main (ID protection)**

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

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

Phase 1 Proposal

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

Diffie-Hellman Group: ☐ 21 ☐ 20 ☐ 19 ☐ 18 ☐ 17 ☐ 16 ☐ 15 ☐ 14 ☐ 5 ☐ 2 ☒ 1

Key Lifetime (seconds): 86400

Local ID:

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

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

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

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

Phase 2 Selectors

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

Edit Phase 2

Name

WIZ_VPN_ZyWALL

Comments

Comments

Local Address

Subnet

192.168.2.0/255.255.255.0

Remote Address

Subnet

192.168.1.0/255.255.255.0

Advanced...

Phase 2 Proposal

Encryption

DES

Authentication

SHA1

Remove

Encryption

AES256

Authentication

SHA1

Remove

Encryption

3DES

Authentication

SHA1

Remove

Encryption

AES128

Authentication

SHA256

Remove

Encryption

AES256

Authentication

SHA256

Remove

Encryption

3DES

Authentication

SHA256

Remove

Enable Replay Detection

☒

Enable Perfect Forward Secrecy (PFS)

☐

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

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

Name

WIZ_VPN_ZyWALL

Comments

Comments

Network

IP Version

☒ IPv4 ☐ IPv6

Remote Gateway

Static IP Address

IP Address

172.101.30.68

Interface

wan1

Mode Config

☐

NAT Traversal

☒

Keepalive Frequency

10

Dead Peer Detection

☒

Authentication

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

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

Phase 1 Proposal

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

Diffie-Hellman Group : 1

XAUTH

Type : Disabled

Phase 2 Selectors

Name	Local Address	Remote Address	
WIZ_VPN_ZyWALL	192.168.2.99/255.255.255.0	192.168.1.1/255.255.255.0	<div>Add</div> <div></div>

OK

Cancel

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

Disconnect		Connection Check								
#	Serial Number	System Name	Name	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound	Outbound
1	N/A	N/A	WIZ_VPN_FortiGate	192.168.1.0/...	172.101.30.68	P: 172.100.30.40	68	79132	0(0 bytes)	0(0 bytes)
Page 1 of 1 Show 50 Items Displaying 1 - 1 of 1										

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

VPN > Monitor > IPsec Monitor

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

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

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

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

Pinging 192.168.2.33 with 32 bytes of data:

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

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

PC behind FortiGate> Window 7 > cmd > ping 192.168.1.33

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

Pinging 192.168.1.33 with 32 bytes of data:

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

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

What Could Go Wrong?

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

MONITOR > Log

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

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

Authentication method and PFS to establish the IKE SA.

MONITOR > Log

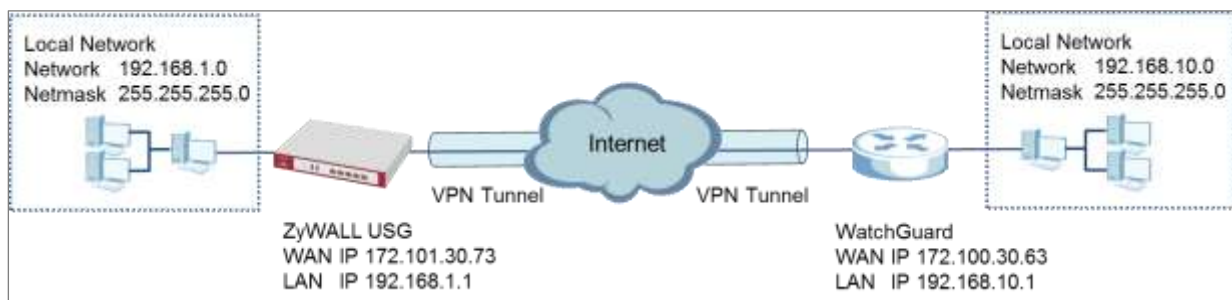
Info	IKE	[SA] : No proposal chosen	IKE_LOG
Info	IKE	[SA] : Tunnel [WIZ_VPN_FortiGate] Phase 2 proposal mismatch	IKE_LOG
Info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
Info	IKE	Phase 1 IKE SA process done	IKE_LOG

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


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

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

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



ZyWALL Site-to-site IPSec VPN with WatchGuard Connected

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and WatchGuard XTM 515 (Firmware Version: 11.10.4).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

- ☒ Express
- ☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Configure **Secure Gateway** IP as the WatchGuard's WAN IP address (in the example, 172.100.30.63). Then, type a secure **Pre-Shared Key** (8-32 characters).

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: (IP or FQDN)

Pre-Shared Key:

Local Policy (IP/Mask):

Remote Policy (IP/Mask):

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: VPN_to_WatchGuard

Secure Gateway: 172.100.30.63

Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name: VPN_to_WatchGuard

Secure Gateway: 172.100.30.63

Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway**, click **Show Advanced Settings**. Configure **Authentication > Local ID Type** as **IPv4** and set the **Content** as your ZyWALL/USG's **WAN IP Address** (in the example, 172.101.30.73). Then, configure **Authentication > Remote ID Type** as **IPv4** and set the **Content** as your WatchGuard's **External IP Address** (in the example, 172.100.30.63). Click **OK**.

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

Authentication

☒ Pre-Shared Key: [masked password] ☐ unmasked

☐ Certificate: default (See [My Certificates](#))

☐ User Based PSK: Remote_Client (i)

Advance

Local ID Type: IPv4
Content: 172.101.30.73

Peer ID Type: IPv4
Content: 172.100.30.63

Set Up the IPsec VPN Tunnel on the WatchGuard

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

Dashboard > Network Interfaces

Link Status	Alias	IPv4 Address	Gateway
Up	External	172.100.30.63/24	172.100.30.1
Up	Trusted	192.168.10.1/24	0.0.0.0
Down	Optional-1	0.0.0.0/0	0.0.0.0
Down	Optional-2	0.0.0.0/0	0.0.0.0
Down	Optional-3	0.0.0.0/0	0.0.0.0
Down	Optional-4	0.0.0.0/0	0.0.0.0
Down	Optional-5	0.0.0.0/0	0.0.0.0

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

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

Gateway Name **VPN_to_ZyWALL**

General Settings Phase 1 Settings

Credential Method

☒ Use Pre-Shared Key *********

☐ Use IPSec Firebox Certificate

ID	Certificate Name	Algorithm

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

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

Gateway Endpoints

Local Type	Local ID	Local Interface▲	Remote IP	Remote Type	Remote ID

Add
Edit
Remove

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.

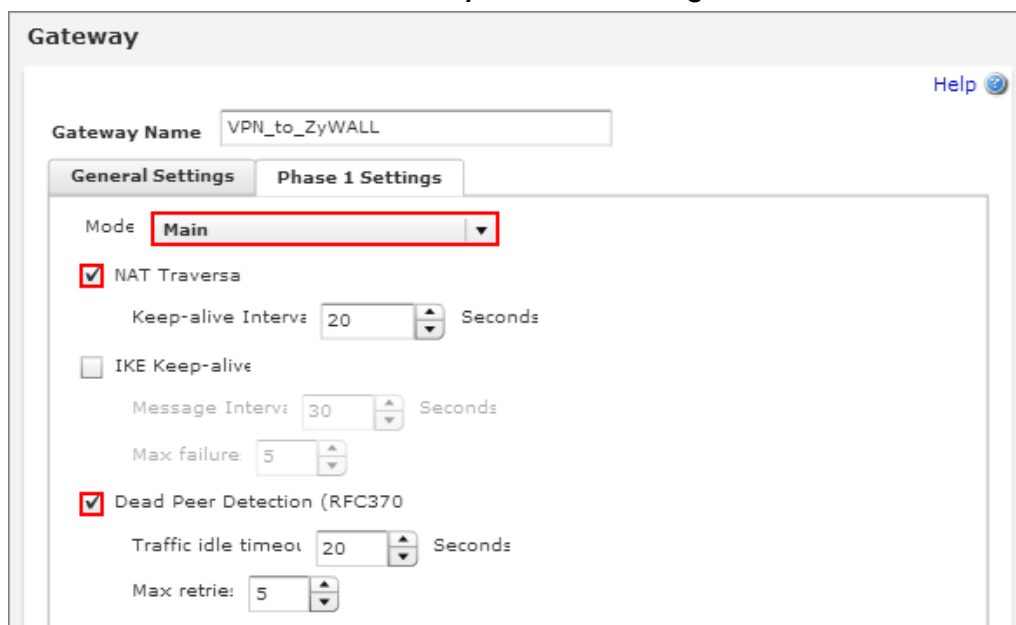
☒ By IP Address 172.101.30.73
 ☐ By Domain Name
 ☐ By User ID on Domain
 ☐ By x500 Name

☐ 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 Traversal** and **Dead Peer Detection** options if both options are enabled in the ZyWALL/USG.

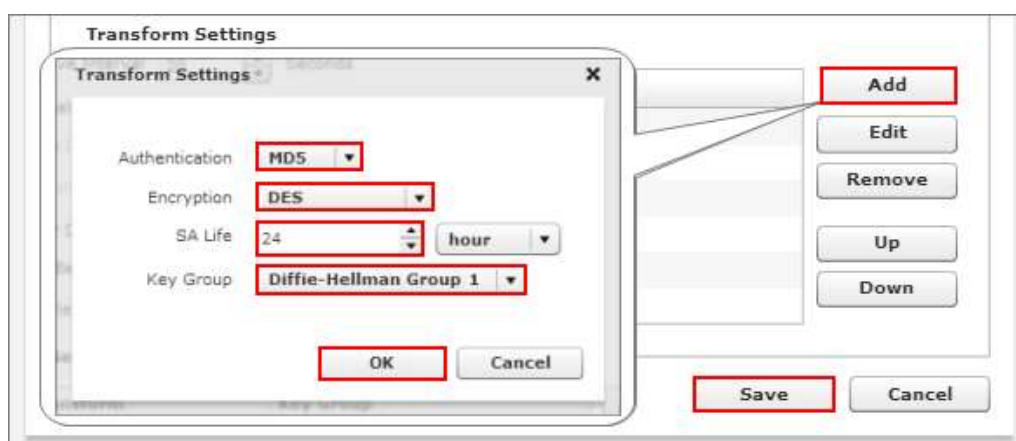
VPN > Branch Office VPN > Gateway > Phase 1 Settings



The screenshot shows the 'Gateway' configuration window with the 'Phase 1 Settings' tab selected. The 'Gateway Name' is 'VPN_to_ZyWALL'. Under 'General Settings', the 'Mode' is set to 'Main'. The 'NAT Traversal' checkbox is checked, with 'Keep-alive Interval' set to 20 seconds. The 'IKE Keep-alive' checkbox is unchecked, with 'Message Interval' set to 30 seconds and 'Max failure' set to 5. The 'Dead Peer Detection (RFC370)' checkbox is checked, with 'Traffic idle timeout' set to 20 seconds and 'Max retries' set to 5.

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

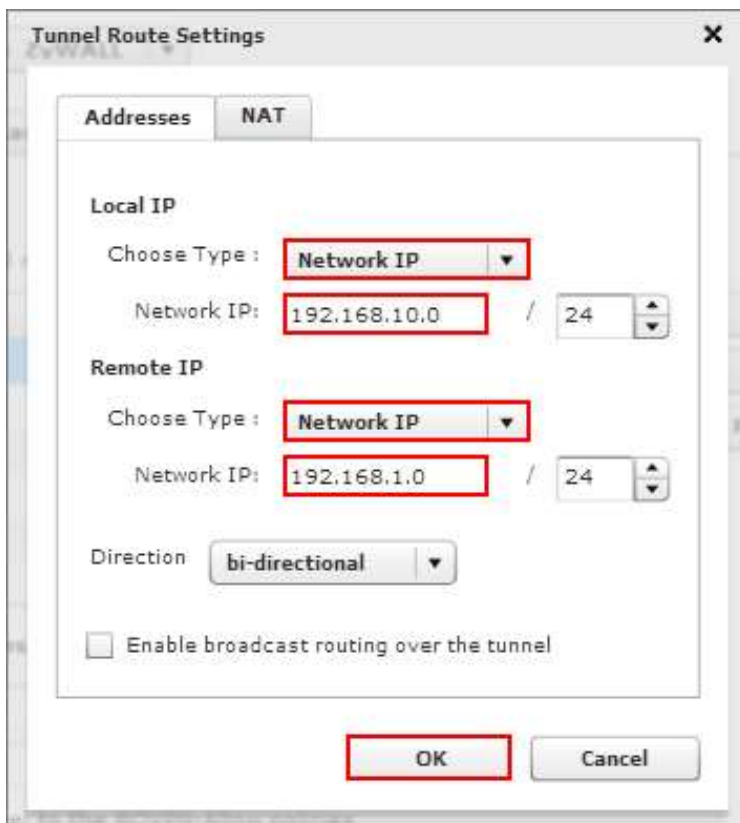
VPN > Branch Office VPN > Gateway > Phase 1 Settings > Transform Settings



The screenshot shows the 'Transform Settings' dialog box. The 'Authentication' is set to 'MD5', 'Encryption' is set to 'DES', 'SA Life' is set to 24 hours, and 'Key Group' is set to 'Diffie-Hellman Group 1'. The 'Add' button is highlighted with a red box. The 'OK' and 'Cancel' buttons are at the bottom of the dialog. The 'Save' and 'Cancel' buttons are at the bottom of the main window.

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

VPN > Branch Office VPN > Tunnel > Address



Tunnel Route Settings

Addresses NAT

Local IP

Choose Type: **Network IP**

Network IP: **192.168.10.0** / 24

Remote IP

Choose Type: **Network IP**

Network IP: **192.168.1.0** / 24

Direction: **bi-directional**

☐ Enable broadcast routing over the tunnel

OK Cancel

Go to **VPN > Branch Office VPN > Tunnel > Phase 2 Settings** to create a **Tunnel Name**. Then, select the **Gateway**. Make sure you enable **Perfect Forward Secrecy** and select **Diffie-Hellman Group 2**. Then, scroll down **Phase 2 Proposals** and add the encryption types to match your ZyWALL/USG's **VPN Connection > Phase 2 Settings**. Click **Save**.

VPN > Branch Office VPN > Tunnel > Phase 2 Settings

Tunnel

Tunnel Name: VPN_to_ZyWALL

Gateway: VPN to ZyWALL

Addresses | **Phase 2 Settings** | Multicast Settings

Perfect Forward Secrecy

☒ Enable Perfect Forward Secrecy | Diffie-Hellman Group 2

IPSec Proposals

Phase 2 Proposals	Remove	Up	Down

ESP-3DES-MD5 | Add

ESP-AES-SHA1

ESP-AES-MD5

ESP-3DES-SHA1

ESP-DES-SHA1

Save | Cancel

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

#	Serial Num.	System ID	Name	Policy	My Address	Remote Gateway	Up Time	Timeout	Inbound(B...	Outbound(B...
1	N/A	N/A	VPN_to_WatchGuard	192.168.1.0/24...	172.101.30.73	P:172.100.30.63	97	76200	0(0 bytes)	0(0 bytes)

Go to WatchGuard **System Status > VPN Statistics > Branch Office VPN** and check the tunnel **Status** is up and **Bytes In** (Incoming Data) and **Bytes Out** (Outgoing Data).

System Status > VPN Statistics > Branch Office

VPN Statistics									
Refresh Interval (30s): 5 120									
Branch Office VPN									
Name	Local	Remote	Gateway	Packets In	Bytes In	Packets Out	Bytes Out	Rekeys	
VPN_to_ZyWALL	192.168.10.0/24	192.168.1.0/24	172.100.30.63 - 172.101.30.73	265	15900	384	23635	0	

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

PC behind ZyWALL/USG > Window 7 > cmd > ping 192.168.10.33

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

Pinging 192.168.10.33 with 32 bytes of data:

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

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

PC behind WatchGuard> Window 7 > cmd > ping 192.168.1.33

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

Pinging 192.168.1.33 with 32 bytes of data:

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

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

What Could Go Wrong?

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

MONITOR > Log

Priority	Category	Message	Source	Destination	Note
info	IKE	Send [NOTIFY] NO_PROPOSAL_CHOSEN	172.101.30.73:500	172.100.30.63:500	WE_LOG
info	IKE	[SA]: No proposal chosen	172.101.30.73:500	172.100.30.63:500	WE_LOG
info	IKE	[SA]: Tunnel [VPN_to_WatchGuard] Phase 1 proposal mismatch	172.101.30.73:500	172.100.30.63:500	WE_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

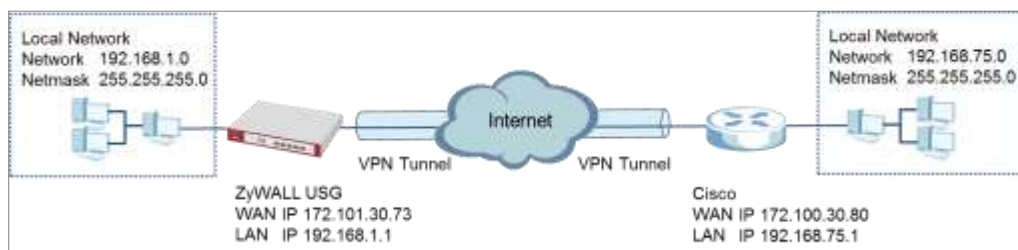
info	IKE	[SA] : No proposal chosen	172.101.30.73:500	172.100.30.63:500	IKE_LOG
info	IKE	[SA] : Tunnel [VPN_to_WatchGuard] Phase 2 proposal mismatch	172.101.30.73:500	172.100.30.63:500	IKE_LOG
info	IKE	Recv[HASH][SA][NONCE][ID]	172.100.30.63:500	172.101.30.73:500	IKE_LOG
info	IKE	Phase 1 IKE SA process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

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


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

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

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



ZyWALL Site-to-site IPSec VPN with Cisco Connected

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25) and ISA500 (Firmware Version: 1.0.3).

Set Up the IPSec VPN Tunnel on the ZyWALL/USG

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

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

Type of VPN policy

- ☐ Express
- ☒ Advanced

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

IKE Version

☒ IKEv1
☐ IKEv2

Scenario

Rule Name:

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

Then, configure the **Secure Gateway** IP as the Cisco's Gateway IP address (in the example, 172.100.30.80); select **My Address** to be the interface connected to the Internet.

Set the desired **Negotiation**, **Encryption**, **Authentication**, **Key Group** and **SA Life Time** settings. Type a secure **Pre-Shared Key** (8-32 characters) which must match your Cisco **Pre-Shared Key**. Click **OK**.

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 1 Setting

Secure Gateway: (IP or FQDN)

My Address (Interface):

Negotiation Mode:

Encryption Algorithm:

Authentication Algorithm:

Key Group:

SA Life Time: (180 - 3000000 seconds)

☒ NAT Traversal

☒ Dead Peer Detection (DPD)

Authentication Method

☒ Pre-Shared Key

☐ Certificate

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 2 Setting

Active Protocol: ESP

Encapsulation: Tunnel

Encryption Algorithm: 3DES

Authentication Algorithm: MD5

SA Life Time: 86400 (180 - 3000000 seconds)

Perfect Forward Secrecy (PFS): DH2

Policy Setting

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.75.0 / 255.255.255.0

Property

☒ Nailed-Up

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Summary

Rule Name: VPN_to_Cisco

Secure Gateway: 172.100.30.80

Pre-Shared Key: ZyxEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.75.0 / 255.255.255.0

Phase 1

Negotiation Mode: main

Encryption Algorithm: des

Authentication Algorithm: md5

Key Group: DH2

Phase 2

Active Protocol: esp

Encapsulation: tunnel

Encryption Algorithm: 3des

Authentication Algorithm: md5

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	VPN_to_Cisco
Secure Gateway:	172.100.30.80
My Address (Interface):	ge1
Pre-Shared Key:	ZyXEL123

Phase 1

Negotiation Mode:	main
Encryption Algorithm:	des
Authentication Algorithm:	md5
Key Group:	DH2
SA Life Time:	86400
NAT Traversal:	true
Dead Peer Detection (DPD):	true

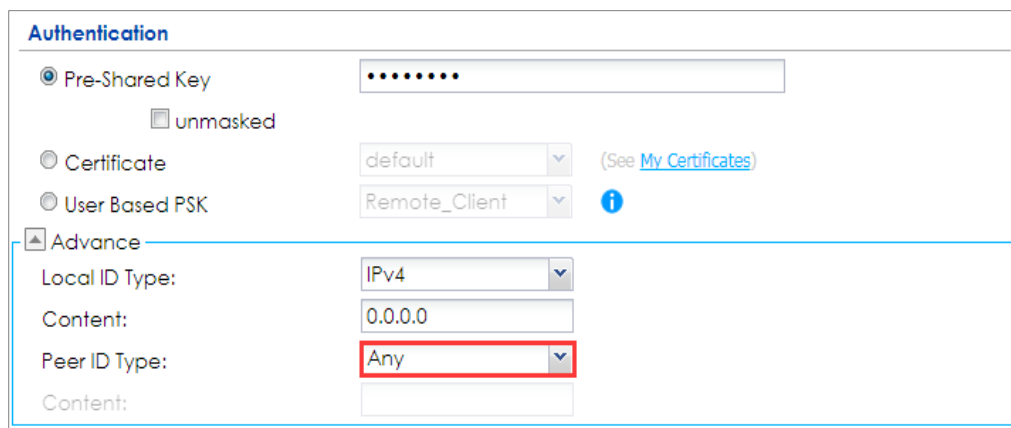
Phase 2

Active Protocol:	esp
Encapsulation:	tunnel
Encryption Algorithm:	3des
Authentication Algorithm:	md5
SA Life Time:	86400
Perfect Forward Secrecy (PFS):	DH2

Policy

Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.75.0 / 255.255.255.0
Nailed-Up:	true

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



Authentication

☒ Pre-Shared Key ☐ unmasked

☐ Certificate (See [My Certificates](#))

☐ User Based PSK [i](#)

☒ Advance

Local ID Type:

Content:

Peer ID Type: [i](#)

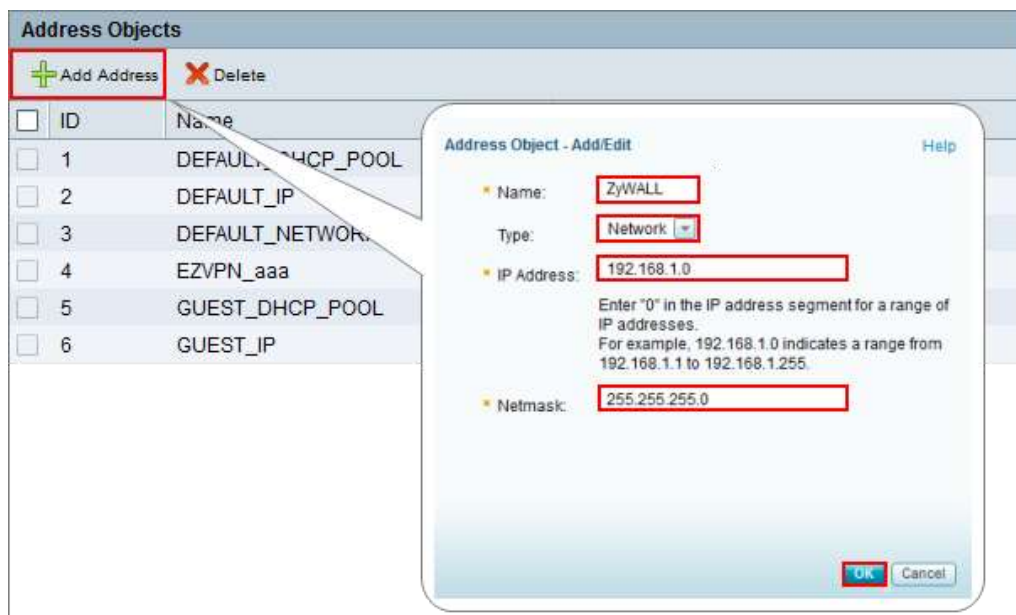
Content:

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

Set Up the IPSec VPN Tunnel on the Cisco

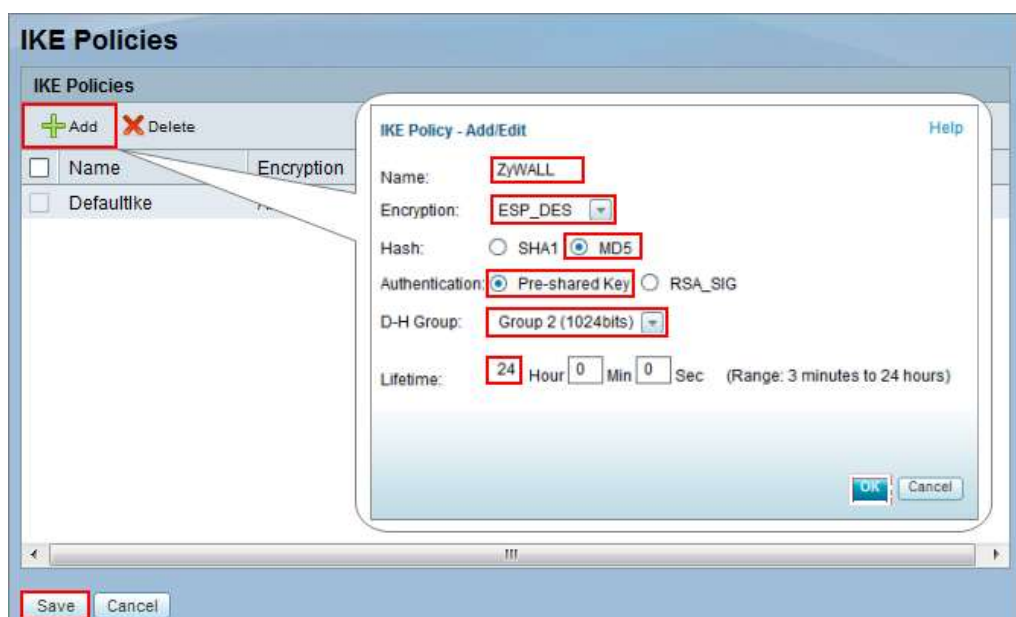
To create an **Address Object Name** of your peer ZyWALL/USG Local IP address, go to **Networking > Address Management > Address Objects** and click **Add Address**. Select **Network** as the **Type**. Configure **IP Address** and **Netmask** to be the IP address range of the network connected to the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

Networking > Address Management > Address Objects



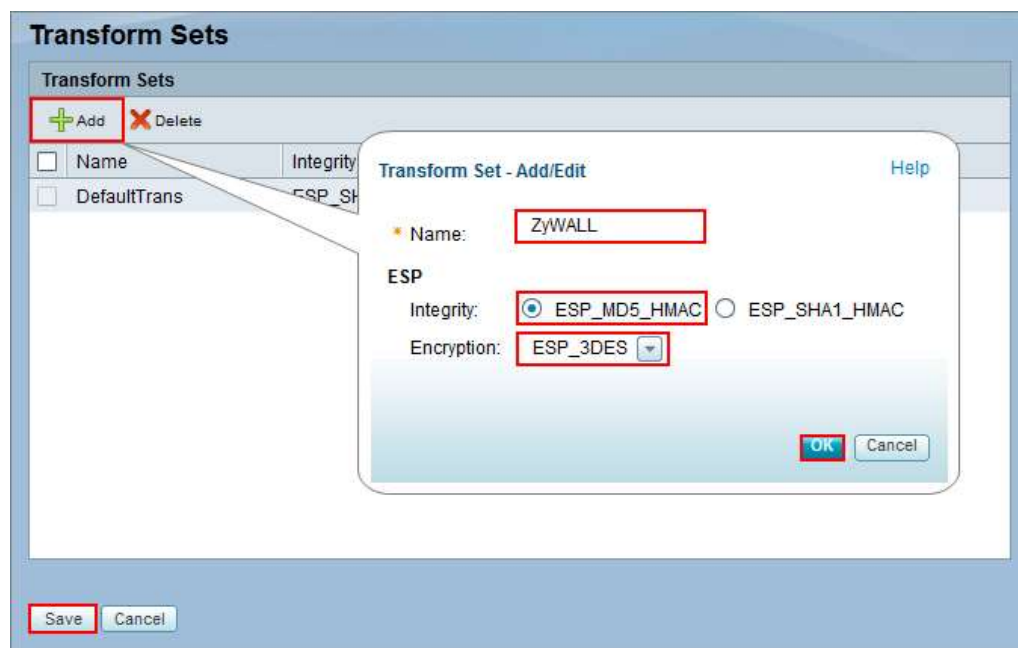
Go to **VPN > Site-to-site > IKE Policies**, click **Add** to create a new IKE Policy **Name**. Then, select **Encryption**, **Hash**, **Pre-shared Key** and **D-H Group** to match your ZyWALL/USG's **VPN Gateway > Phase 1 Settings**. Set **Lifetime** to **24** hours and click **OK** then click **Save**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

IPsec Policies - Add/Edit Help

Basic Settings | Advanced Settings | VPN Failover

* Description:

* IPsec Policy Enable: ☒ On ☐ Off

* Remote Type:

Remote Address:

* Authentication Method: ☒ Pre-Shared Key

* Key:

☐ Certificate

Local Certificate:

Remote Certificate:

WAN Interface:

* Local network:

* Remote network:

OK Cancel

Then, go to **Advanced Settings** enable **PFS** and **DPD** if you enable both options in the ZyWALL/USG. Set **IKE Policy** to be the **IKE Policy** created in Step 2 (found under **IKE Policy Link**); set **Transform** to be the **Transform Set** created in Step 3 (found under **Transform Link**) and **SA-Lifetime** to be **24** hours.

Click **OK**. The connection active dialog box appears. Click **Activate Connection**.


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

IPsec Policies - Add/Edit
[Help](#)

Basic Settings
Advanced Settings
VPN Failover

PFS Enable: ☒ On ☐ Off
DPD Enable: ☒ On ☐ Off
Delay Time: (Range: 10-300 s)
Detection Timeout: (Range: 30-1800 s)
DPD Action:

Apply NAT Policies: ☐ On ☒ Off
Translates Local Network:
Translates Remote Network:
IKE Policy: [IKE Policy Link](#)
Transform: [Transform Link](#)
SA-Lifetime: Hour Min Sec (Range: 3 minutes to 24 hours)


Do you want to make this connection active when the settings are saved?

Test the IPsec VPN Tunnel

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

CONFIGURATION > VPN > IPsec VPN > VPN Connection



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

MONITOR > VPN Monitor > IPsec

Serial Number	System Name	Remote ID	Policy	My Address	Remote Peer	Up Time	Inbound	Outbound	Inbound(Bytes)	Outbound(Bytes)
1	N/A	N/A	VPN_to_Cisco	192.168.1.0/24	172.101.30.73	791s7	0B	0B	0B	0B

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

Name	Status	VPN Type	WAN Interface	Remote Gateway	Local Network	Remote Network	Connect
VPN_to_ZyWALL	Up	Site to Site	WAN1	172.101.30.73	192.168.75.0/24	192.168.1.0/24	

Go to Cisco **VPN > VPN Status > IPsec VPN Status > Statics** and check the **Tx Packets** (Transmit data) and **Rx Packets** (Receive data).

VPN > VPN Status > IPsec VPN Status > Statistics

Name	VPN Type	WAN Interface	Remote Gateway	Tx Bytes	Rx Bytes	Tx Packets	Rx Packets
VPN_to_ZyWALL	Site to Site	WAN1	172.101.30.73	60665	45180	758	753

To test whether a tunnel is working, ping from a computer at one site to a computer at the other. Ensure that both computers have Internet access (via the IPSec devices).

PC behind ZyWALL/USG > Window 7 > cmd > ping 192.168.75.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.75.33

Pinging 192.168.75.33 with 32 bytes of data:

Reply from 192.168.75.33: bytes=32 time=18ms TTL=54
Reply from 192.168.75.33: bytes=32 time=17ms TTL=54
Reply from 192.168.75.33: bytes=32 time=17ms TTL=54
Reply from 192.168.75.33: bytes=32 time=16ms TTL=54

Ping statistics for 192.168.75.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 16ms, Maximum = 18ms, Average = 17ms
```

PC behind Cisco > Window 7 > cmd > ping 192.168.1.33

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

Pinging 192.168.1.33 with 32 bytes of data:

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

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

What Could Go Wrong?

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

IKE SA.

MONITOR > Log

Priority	Category	Message	Source	Destination	Note
Info	IKE	Send:[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 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

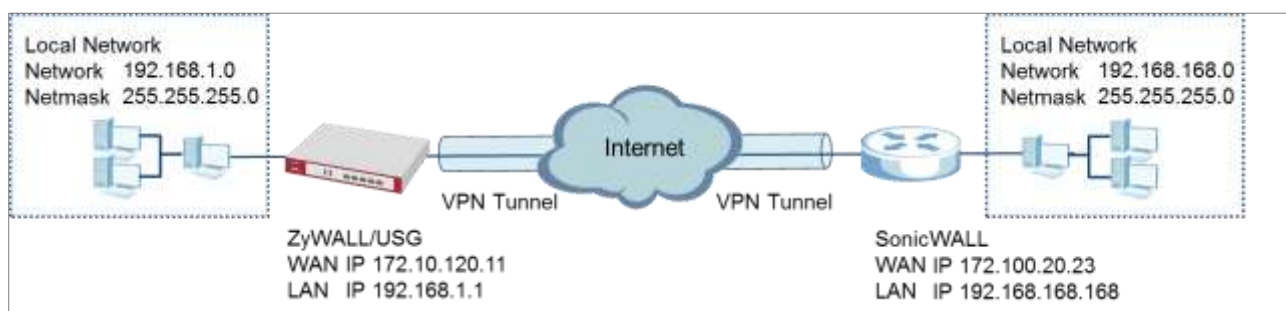
Info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	172.101.30.73:500	172.100.30.80:500	IKE_LOG
Info	IKE	[SA]: No proposal chosen	172.101.30.73:500	172.100.30.80:500	IKE_LOG
Info	IKE	[SA]: Tunnel [VPN_to_Cisco] Phase 2 proposal mismatch	172.101.30.73:500	172.100.30.80:500	IKE_LOG
Info	IKE	Recv:[HASH][SA][NO/HCE][ID][ID]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



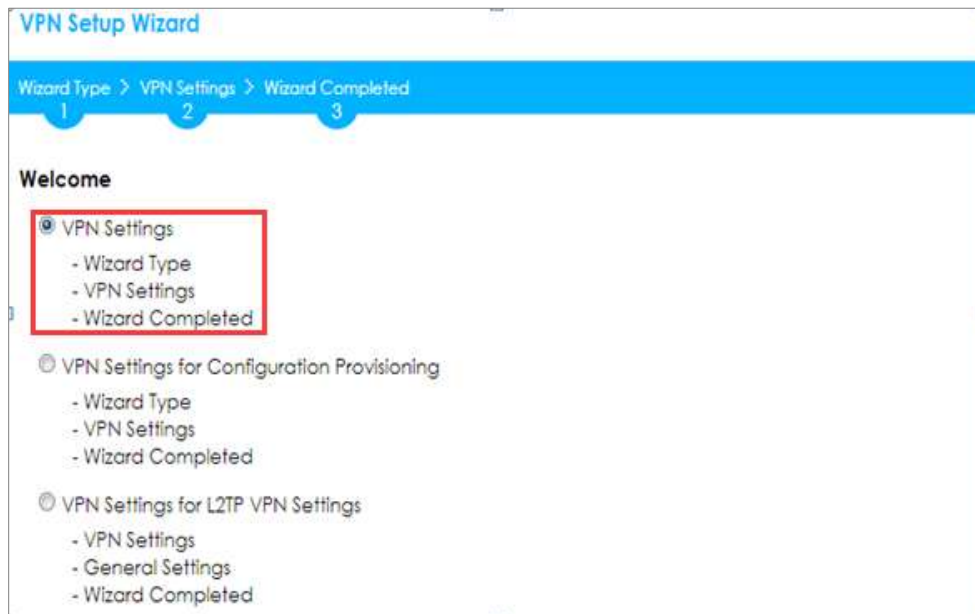
ZyWALL/USG Site-to-site IPsec VPN with SonicWALL

 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

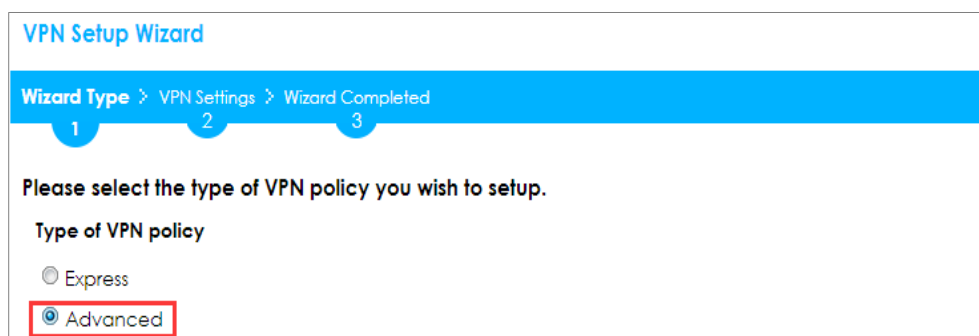
In the ZyWALL/USG, go to **Quick Setup > VPN Setup Wizard**, use the **VPN Settings** wizard to create a VPN rule that can be used with the SonicWALL. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome



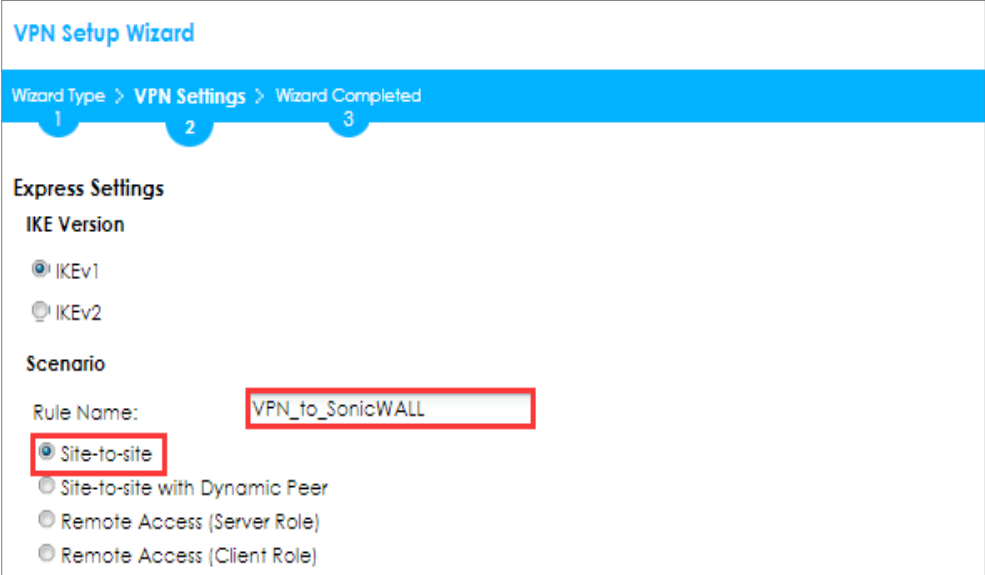
Choose **Advanced** to create a VPN rule with the customize phase 1, phase 2 settings and authentication method. Click **Next**.

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)



VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ **Site-to-site**

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

Then, configure the **Secure Gateway** IP as the SonicWALL's Gateway IP address (in the example, 172.100.20.23); select **My Address** to be the interface connected to the Internet.

Set the desired **Negotiation**, **Encryption**, **Authentication**, **Key Group** and **SA Life Time** settings. Type a secure **Pre-Shared Key** (8-32 characters) which must match your SonicWALL **Shared Secret**.

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Advanced Settings

Phase 1 Setting

Secure Gateway: (IP or FQDN)

My Address (interface):

Negotiation Mode:

Encryption Algorithm:

Authentication Algorithm:

Key Group:

SA Life Time: (180 - 3000000 seconds)

☒ NAT Traversal

☒ Dead Peer Detection (DPD)

Authentication Method

☒ Pre-Shared Key

☐ Certificate

Continue to **Phase 2 Settings** to select the desired **Encapsulation**, **Encryption**, **Authentication**, and **SA Life Time** settings.

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Phase 2 Setting

Active Protocol: ESP

Encapsulation: Tunnel

Encryption Algorithm: AES128

Authentication Algorithm: SHA1

SA Life Time: 86400 (180 - 3000000 seconds)

Perfect Forward Secrecy (PFS): None

Policy Setting

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Property

☒ Nailed-Up

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1

2

3

Advanced Settings

Summary

Rule Name: VPN_to_SonicWall
 Secure Gateway: 172.100.20.23
 Pre-Shared Key: 5k4u;4e.40fm06xk7187!
 Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0
 Remote Policy (IP/Mask): 192.168.168.0 / 255.255.255.0

Phase 1

Negotiation Mode: main
 Encryption Algorithm: aes256
 Authentication Algorithm: sha
 Key Group: DH2

Phase 2

Active Protocol: esp
 Encapsulation: tunnel
 Encryption Algorithm: aes128
 Authentication Algorithm: sha



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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Advanced Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	VPN_to_SonicWall
Secure Gateway:	172.100.20.23
My Address (interface):	ge1
Pre-Shared Key:	5k4u;4e.40fm08xx7187!

Phase 1

Negotiation Mode:	main
Encryption Algorithm:	aes256
Authentication Algorithm:	sha
Key Group:	DH2
SA Life Time:	86400
NAT Traversal:	true
Dead Peer Detection (DPD):	true

Phase 2

Active Protocol:	esp
Encapsulation:	tunnel
Encryption Algorithm:	aes128
Authentication Algorithm:	sha
SA Life Time:	86400
Perfect Forward Secrecy (PFS):	None

Policy

Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.168.0 / 255.255.255.0
Nailed-Up:	true

Go to **VPN Gateway > Show Advanced Settings > Authentication** to configure **your Local ID Type** and **Peer ID Type** to match your SonicWALL's **VPN > Settings > VPN Policies > General > IKE Authentication > Local IKE ID** and **Peer IKE ID**.

VPN Gateway > Show Advanced Settings > Authentication

Authentication


☒ Pre-Shared Key

☒ unmasked

☐ Certificate

[\(See My Certificates\)](#)

☐ User Based PSK



☒ Advance

Local ID Type:

Content:

Peer ID Type:

Content:

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

SONICWALL | Network Security Appliance

General | Network | Proposals | Advanced

Security Policy

Policy Type: Site to Site

Authentication Method: IKE using Preshared Secret

Name: VPN_to_ZyWALL

IPsec Primary Gateway Name or Address: 172.10.120.11

IPsec Secondary Gateway Name or Address: 0.0.0.0

IKE Authentication

Shared Secret: 5k4u;4e.40fm06xk7187!

Confirm Shared Secret: 5k4u;4e.40fm06xk7187!

☒ Mask Shared Secret

Local IKE ID: IP Address 192.168.168.0

Peer IKE ID: IP Address 192.168.1.0

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

Go to **Remote Network** and create a new address IP address range of the network connected to the ZyWALL/USG. Then, scroll down the list to choose the newly created **Address Object** to be the **Remote Network**.

VPN > Settings > VPN Policies > Network

SONICWALL Network Security Appliance

General Network Proposals Advanced

Local Networks

- ☒ Choose local network from list
- ☐ Local network obtains IP addresses using DHCP through this VPN Tunnel
- ☐ Any address

--Select Local Network--
 ==== Address Objects ====
 X0 IP
X0 Subnet
 X1 Default Gateway
 X1 IP
 ==== Address Objects ====

Remote Networks

- ☐ Use this VPN Tunnel as default route for all Internet traffic
- ☐ Destination network obtains IP addresses using DHCP through this VPN Tunnel
- ☒ Choose destination network from list

--Select Remote Network--
 --Select Remote Network--
Create new address object...
 Create new address group...
 ==== Address Groups ====
 allIP
 relayagent
 ==== Address Objects ====

SONICWALL Network Security Appliance

Name: ZyWALL
 Zone Assignment: LAN
 Type: Network
 Network: 192.168.1.0
 Netmask: 255.255.255.0

Remote Networks

- ☐ Use this VPN Tunnel as default route for all Internet traffic
- ☐ Destination network obtains IP addresses using DHCP through this VPN Tunnel
- ☒ Choose destination network from list

ZyWALL
 --Select Remote Network--
 Create new address object...
 Create new address group...
 ==== Address Groups ====
 allIP
 relayagent
 ==== Address Objects ====
ZyWALL

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

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

VPN > Settings > VPN Policies > Proposals

SONICWALL | Network Security Appliance

General | Network | **Proposals** | Advanced

IKE (Phase 1) Proposal

Exchange: Main Mode

DH Group: Group 2

Encryption: AES-256

Authentication: SHA1

Life Time (seconds): 28800

Ipssec (Phase 2) Proposal

Protocol: ESP

Encryption: AES-128

Authentication: SHA1

☐ Enable Perfect Forward Secrecy

Life Time (seconds): 28800

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

VPN > Settings > VPN Global Settings

VPN Global Settings

☒ Enable VPN

Unique Firewall Identifier:

VPN Policies

Refresh Interval (secs) 10 Items per page 50 Items 3 to 3

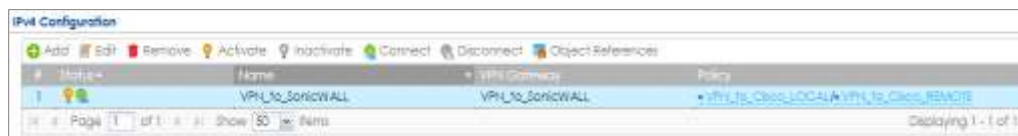
	Name	Gateway	Destinations	Crypto Suite	Enable
3	VPN_to_ZyWALL	172.10.120.11	192.168.1.0 - 192.168.1.255	ESP: DES/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>

Refresh Active

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.

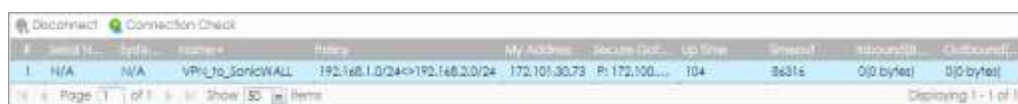
CONFIGURATION > VPN > IPSec VPN > VPN Connection



#	Name	VPN Gateway	Policy
1	VPN_to_SonicWALL	VPN_to_SonicWALL	VPN_to_SonicWALL

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

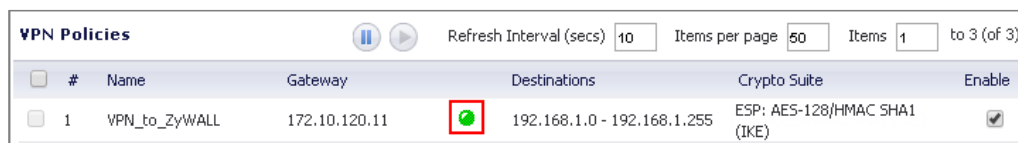
MONITOR > VPN Monitor > IPSec



#	Name	Rating	My Address	Secure Port	Up Time	Inbound	Outbound
1	VPN_to_SonicWALL	192.168.1.0/24<->192.168.2.0/24	172.10.30.73	172.100.104	104	0/0 bytes	0/0 bytes

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

VPN > VPN Settings > VPN Policies



#	Name	Gateway	Destinations	Crypto Suite	Enable
1	VPN_to_ZyWALL	172.10.120.11	192.168.1.0 - 192.168.1.255	ESP: AES-128/HMAC SHA1 (IKE)	<input checked="" type="checkbox"/>

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

Currently Active VPN Tunnels					
#	Created	Name	Local	Remote	
1	10/04/2015 15:07:06	VPN_to_ZyWALL	192.168.168.0 - 192.168.168.255	192.168.1.0 - 192.168.1.255	172.10.120.11 Renegotiate

VPN Tunnel Statistics
 Create Time: 10/04/2015 15:07:06
 Tunnel valid until: 10/04/2015 23:07:06
 Packets In: 378
 Packets Out: 370
 Bytes In: 20080
 Bytes Out: 16640
 Fragments In: 0
 Fragments Out: 0

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:[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 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

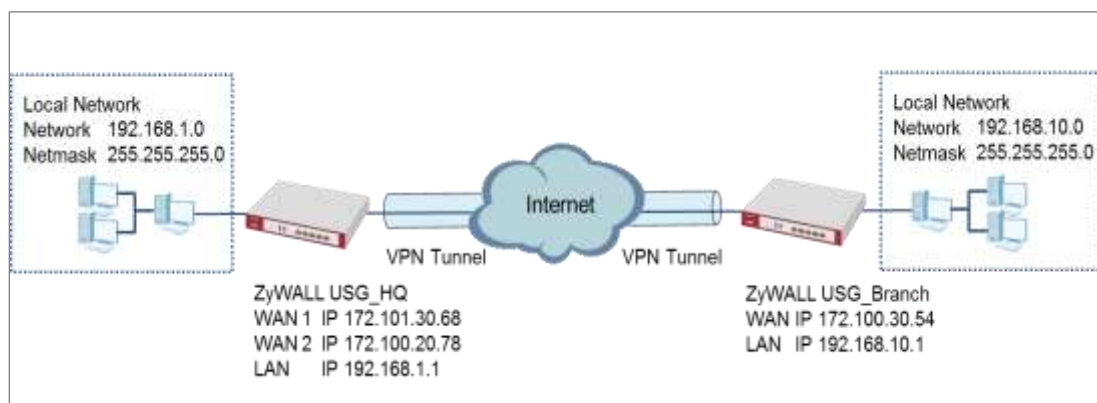
Priority	Category	Message	Source	Destination	Note
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	172.101.30.73...	172.100.30.80...	IKE_LOG
info	IKE	[SA] : No proposal chosen	172.101.30.73...	172.100.30.80...	IKE_LOG
info	IKE	[SA] : Tunnel [VPN_to_SonicWALL] Phase 2 proposal mismatch	172.101.30.73...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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

- ☒ Express
- ☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1
☐ IKEv2

Scenario

Rule Name:

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

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.100.30.54 (IP or FQDN)

Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_HQ

Secure Gateway: 172.100.30.54

Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_VPN_HQ
Secure Gateway:	172.100.30.54
Pre-Shared Key:	ZyXEL123
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.10.0 / 255.255.255.0

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

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

Authentication

☒ Pre-Shared Key

.....

☐ unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

Remote_Client

i

☒ Advance

Local ID Type:
IPv4

Content:
0.0.0.0

Peer ID Type:
Any

Content:
172.100.30.54

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

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

☒ VPN Settings

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for Configuration Provisioning

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for L2TP VPN Settings

- VPN Settings
- General Settings
- Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

☒ Express

☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name: WIZ_VPN_Branch

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 172.101.30.68 (IP or FQDN)

Pre-Shared Key: ZyXEL123

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings
Summary

Rule Name:	WIZ_VPN_Branch
Secure Gateway:	172.101.30.68
Pre-Shared Key:	ZyXEL123
Local Policy (IP/Mask):	192.168.10.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.1.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > **Wizard Completed**

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_VPN_Branch
Secure Gateway:	172.101.30.68
Pre-Shared Key:	ZyXEL123
Local Policy (IP/Mask):	192.168.10.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.1.0 / 255.255.255.0

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

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

Authentication

☒ Pre-Shared Key

.....

unmasked

☐ Certificate

default

(See [My Certificates](#))

☐ User Based PSK

Remote_Client

☒ Advance

Local ID Type: IPv4

Content: 0.0.0.0

Peer ID Type: Any

Content: 172.101.30.68

Go to **Configuration > VPN > IPSec VPN > VPN Gateway > Gateway Settings**. Set **My Address** to be **Domain Name/IP** "0.0.0.0" (ZyWALL/USG will dial-up with the active WAN interface first). Set **Peer Gateway Address > Static Address > Primary** to be ZyWALL/USG_HQ WAN1 IP address and **Secondary** to be ZyWALL/USG_HQ WAN2 IP address.

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

General Settings

☒ Enable

VPN Gateway Name: WIZ_VPN_Branch

IKE Version

☒ IKEv1
 ☐ IKEv2

Gateway Settings

My Address

☐ Interface

ge1

Static -- 0.0.0.0/0.0.0.0

☒ Domain Name / IPv4

0.0.0.0

Peer Gateway Address

☒ Static

Primary 172.101.30.68

Secondary 172.100.20.78

☒ Fall back to Primary Peer Gateway when possible

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

☐ Dynamic Address

Set up the WAN Trunk (ZyWALL/USG_HQ)

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

CONFIGURATION > Interface > Trunk > User Configuration > Add

+ Add Trunk

Name: Multi_WAN_Failover

Load Balancing Algorithm: Least Load First

Load Balancing Index(es): Outbound

#	Member	Mode	Egress Bandwidth
1	wan1	Active	1048576 kbps
2	wan2	Passive	1048576 kbps

Page 0 of 0 Show 50 items No data to display

OK Cancel

Go to **CONFIGURATION > Interface > Trunk > Configuration**. Select **Disconnect Connection before Falling Back**. In the **Default WAN Trunk**, select **User Configured Trunk** to be the customized WAN trunk added in the previous step (Multi_WAN_Failover in this example).

CONFIGURATION > Interface > Trunk > User Configuration > Add

Configuration

☒ Disconnect Connections Before Failing Back

Default WAN Trunk

Advance

Default Trunk Selection:

☐ SYSTEM_DEFAULT_WAN_TRUNK

☒ User Configured Trunk: **Mult_WAN_Failover**

User Configuration

Name	Algorithm
1 Mult_WAN_Failover	#

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

Set up the Failover Command Line (ZyWALL/USG HQ)

Go to **CONFIGURATION > Security Policy > Policy Control** and add a **To ZyWALL** rule to allow **SSH** service.

CONFIGURATION > Security Policy > Policy Control > Add corresponding

+ Add corresponding

Create new Object ▼

☒ Enable

Name: **Any_to_ZyWall_SSH**

Description: (Optional)

From: **any**

To: **ZyWALL**

Source: **any**

Destination: **any**

Service: **SSH**

User: **any**

Schedule: **none**

Action: **allow**

Log matched traffic: **no**

OK **Cancel**

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



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

MONITOR > VPN Monitor > IPSec

#	Name	Policy	My Address	Secure Gateway	Up Time	Timeout	Inbound(Bytes)	Outbound(Bytes)
1	test	192.168.10.0/24 <-> 192.168.	172.100.20.54	P: 172.101.30.68	18	79190	0(0 bytes)	0(0 bytes)

- Go to ZyWALL/USG_Branch **MONITOR > Log**. Try to disconnect WAN1 interface (172.1.1.30.68) and you will see the VPN tunnel failover to WAN2 interface (172.100.20.78).

MONITOR > Log

#	Time	Source	Destination	Protocol	Port	Source	Destination	Protocol	Port
1	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
2	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
3	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
4	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
5	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
6	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
7	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
8	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
9	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
10	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
11	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
12	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
13	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
14	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
15	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
16	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
17	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
18	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
19	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
20	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
21	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
22	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
23	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
24	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
25	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
26	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
27	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
28	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
29	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
30	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
31	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
32	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
33	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
34	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
35	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
36	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
37	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
38	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
39	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
40	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
41	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
42	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
43	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
44	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
45	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500
46	2017-07-19 10:40:00	192.168.10.0/24	172.100.20.54	IPSec	500	172.100.20.54	172.100.20.54	IPSec	500

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:[HASH]:NO_PROPOSAL_CHOSEN	IKE_LOG
Info	IKE	[SA] : No proposal chosen	IKE_LOG
Info	IKE	[SA] : Tunnel [WIZ_VPN_HQ] Phase 1 proposal mismatch	IKE_LOG

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

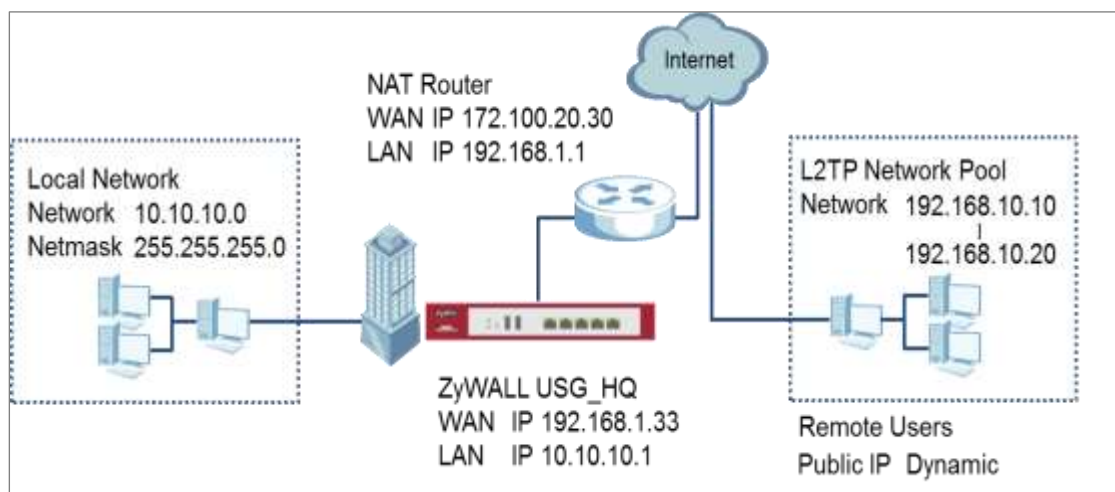
MONITOR > Log

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

- 13 Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- 14 Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

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

This example shows how to use the VPN Setup Wizard to create a L2TP over IPsec VPN tunnel between ZyWALL/USG devices. The example instructs how to configure the VPN tunnel between each site while the ZyWALL/USG is behind a NAT router. When the L2TP over IPsec VPN tunnel is configured, each site can be accessed securely.



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



Note:

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

Set Up the L2TP VPN Tunnel on the ZyWALL/USG_HQ

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☒ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

Rule Name: WIZ_L2TP_VPN

Phase 1 Setting

My Address (interface): wan1

Authentication Method

Pre-Shared Key: xyz12345

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

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

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

IP Address Pool: RANGE ⓘ

Starting IP Address: 192.168.10.10

End IP Address: 192.168.10.20

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

L2TP VPN Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_L2TP_VPN
My Address (Interface):	wan1
Pre-Shared Key:	xyz12345
IP Address Pool:	RANGE, 192.168.10.10 - 192.168.10.20

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

CONFIGURATION > VPN Connection > Create new Object > Create Address

+ Add Address Rule

Name: NAT_WAN_IP

Address Type: HOST

IP Address: 172.100.20.30

OK Cancel

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

CONFIGURATION > VPN Connection > Policy > Local Policy

General Settings

☒ Enable
 Connection Name:
☒ Advance

VPN Gateway

Application Scenario
☐ Site-to-site
☐ Site-to-site with Dynamic Peer
☒ Remote Access (Server Role)
☐ Remote Access (Client Role)
☐ Vpn Tunnel Interface
 VPN Gateway:

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

The image shows two screenshots from the ZyXEL web management interface. The top screenshot is the 'L2TP VPN' configuration page. It has a blue header with 'L2TP VPN' and a 'Create new Object' button. Below the header, there are tabs for 'General Settings', 'Config Walkthrough', 'Address', and 'Reshooting'. The 'General Settings' tab is active. It contains the following fields: 'Enable L2TP Over IPSec' (checked), 'VPN Connection' (WIZ_L2TP_VPN), 'IP Address Pool' (WIZ_L2TP_VPN_IP_A), 'Authentication Method' (default), 'Advance' (expanded), 'Allowed User' (any), 'Keep Alive Timer' (60), 'First DNS Server (Optional)' (Custom Defined), 'Second DNS Server (Optional)' (Custom Defined), 'First WINS Server (Optional)', and 'Second WINS Server (Optional)'. The bottom screenshot is the 'Add A User' dialog box. It has a 'User Configuration' section with fields for 'User Name' (L2TP_Remote_User), 'User Type' (user), 'Password' (masked), 'Ratatype' (masked), 'Description' (Local User), 'Authentication Timeout Settings' (Use Default Settings), 'Use Manual Settings' (unchecked), 'Lease Time' (1440 minutes), and 'Reauthentication Time' (1440 minutes). There are 'OK' and 'Cancel' buttons at the bottom.

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

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

CONFIGURATION > Network > NAT > Add

General Settings

☒ Enable Rule

Rule Name: VPN_NAT

Port Mapping Type

Classification:
 ☐ Virtual Server
 ☒ 1:1 NAT
 ☐ Many 1:1 NAT

Mapping Rule

Incoming Interface: wan1

Original IP: User Defined

User-Defined Original IP: 172.100.20.30 (IP Address)

Mapped IP: User Defined

User-Defined Mapped IP: 192.168.1.33 (IP Address)

Port Mapping Type: any

Go to **CONFIGURATION > Object > Address > Add**, create an address object as the ZyWALL/USU_HQ's WAN IP address (in the example, 192.168.1.33).

CONFIGURATION > Object > Address

+ Add Address Rule

Name: L2TP_WAN_IP

Address Type: HOST

IP Address: 192.168.1.33

OK Cancel

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

UDP Port Number = 1701 → Used by L2TP

UDP Port Number = 500 → Used by IKE

UDP Port Number = 4500 → Used by NAT-T

CONFIGURATION > Service > Service Group

+ Add Service Group Rule

Configuration

Name: **L2TP-Allow**

Description:

Configuration

Available

=== Object ===

- AH
- AIM
- AUTH
- Any_TCP
- Any_UDP
- BGP
- BONJOUR
- BOOTP_CLIENT

Member

=== Object ===

- NATT
- IKE
- L2TP-UDP**

OK **Cancel**

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

CONFIGURATION > Security Policy > Policy Control

+ Add corresponding

Create new Object ▼

☒ **Enable**

Name: **L2TP-Allow**

Description: (Optional)

From: any

To: any (Excluding ZyV)

Source: any

Destination: **L2TP_WAN_IP**

Service: **L2TP-Allow**

User: **L2TP_Remote_User**

Schedule: none

Action: allow

Log matched traffic: no

Test the L2TP over IPSec VPN Tunnel

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

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

Description is for you to identify the VPN configuration.

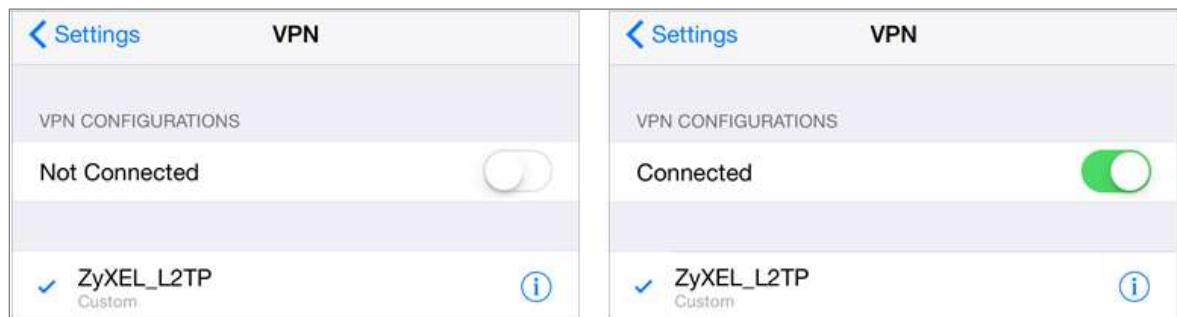
Set **Server** to the ZyWALL/USG's WAN IP address (172.100.20.30 in this example).

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

Set **Secret** to the **Pre-Shared Key** of the IPsec VPN gateway the ZyWALL/USG uses for L2TP VPN over IPsec (xyz12345 in this example).

ZyXEL_L2TP	
Type	L2TP
Description	ZyXEL_L2TP
Server	172.100.20.30
Account	L2TP_Remote_Users
RSA SecurID	<input type="checkbox"/>
Password	••••••
Secret	••••••••
Send All Traffic	<input checked="" type="checkbox"/>

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

< VPN
ZyXEL_L2TP

Type	L2TP
Server	172.100.20.30
Assigned IP Address	192.168.10.10
Connect Time	0:06

Description ZyXEL_L2TP

Server	172.100.20.30
Account	L2TP_Remote_Users
RSA SecurID	<input type="checkbox"/>
Password	••••••
Secret	••••••••
Send All Traffic	<input checked="" type="checkbox"/>

What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP

Allowed User or **User/Group Settings**. iOS Mobile users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.

Priority	Category	Message	Note
alert	L2TP Over IPsec	User L2TP_Remote_Users has been denied from L2TP service. (Incorrect Username or Password)	L2TP_LOG

If you see [info] or [error] log message such as below, please check ZyWALL/USG Phase 1 Settings. iOS Mobile users must use the same **Secret** as configured in ZyWALL/USG to establish the IKE SA.

Priority	Category	Message	Note
Info	IKE	Send:[NOTIFY:INVALID_PAYLOAD_TYPE]	IKE_LOG
Info	IKE	Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys	IKE_LOG

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.

Priority	Category	Message	Note
Info	IKE	ISAKMP SA [WIZ_L2TP_VPN] is disconnected	IKE_LOG
Info	IKE	Received delete notification	IKE_LOG
Info	IKE	Recv:[HASH][DEL]	IKE_LOG
Info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
Info	IKE	[SA] : No proposal chosen	IKE_LOG
Info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch	IKE_LOG

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

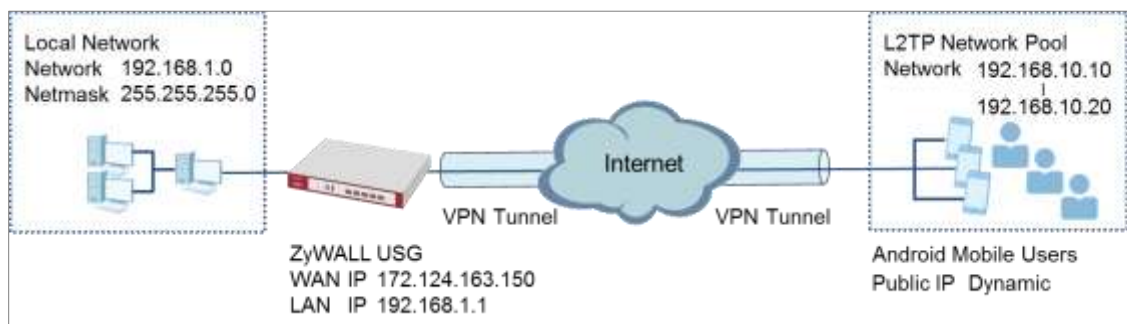
If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

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


Verify that the **Zone** is set correctly in the **Zone** object. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Configure L2TP VPN with Android 5.0 Mobile Devices

This example shows how to use the VPN Setup Wizard to create a L2TP VPN between a ZyWALL/USG and an Android 5.0 Mobile Device. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely and allow traffic from L2TP clients to go to the Internet.



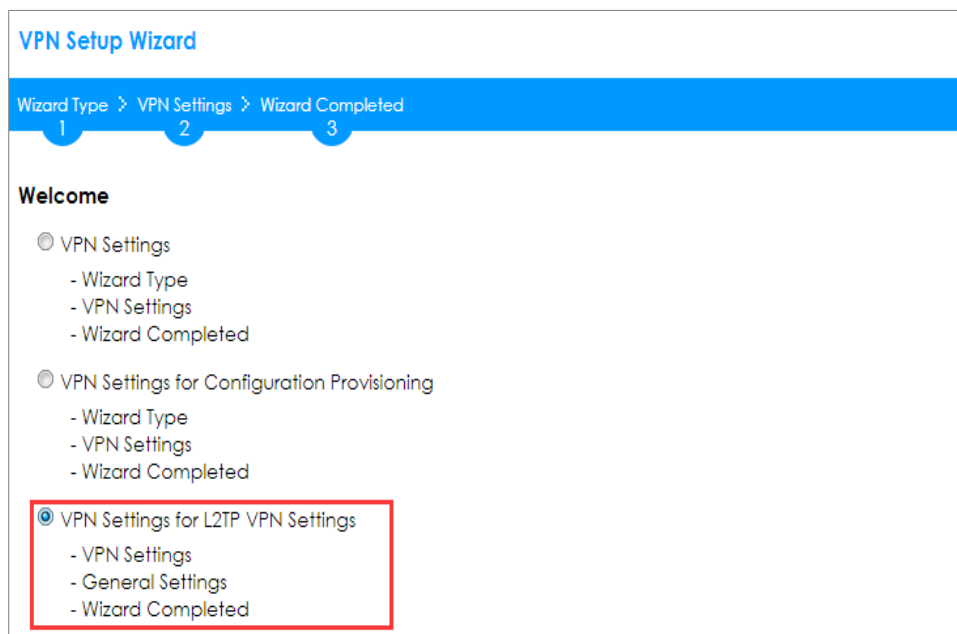
ZyWALL/USG L2TP VPN with Android Mobile Devices Example

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and Android version (Firmware Version: 5.0)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

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

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☐ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☒ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

Rule Name:

Phase 1 Setting

My Address (interface):

Authentication Method

Pre-Shared Key:

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

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

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

IP Address Pool: ⓘ

Starting IP Address:

End IP Address:

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > **Wizard Completed**

1 2 3

L2TP VPN Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name: WIZ_L2TP_VPN

My Address (interface): wan1

Pre-Shared Key: xyz12345

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

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

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

The screenshot shows the 'L2TP VPN' configuration page. At the top, there's a blue header with 'L2TP VPN'. Below it, a navigation bar includes 'Show Advanced Settings' and 'Create new Object'. A dropdown menu is open under 'Create new Object', showing 'User' (highlighted with a red box), 'Address', and 'Reshooting'. The 'General Settings' section is active, showing 'Enable L2TP Over IPSec' checked. Other settings include 'VPN Connection' (WIZ_L2TP_VPN), 'IP Address Pool' (WIZ_L2TP_VPN_IP_1), 'Authentication Method' (default), 'Allowed User' (any), 'Keep Alive Timer' (60 seconds), and optional DNS and WINS servers. The 'Advance' section is collapsed.

The screenshot shows the 'User Configuration' dialog box. It has fields for 'User Name' (L2TP_Remote_User), 'User Type' (User), 'Password' (masked with asterisks), and 'Retype' (masked with asterisks). The 'Description' field contains 'Local User'. There are two radio buttons: 'Use Default Settings' (selected) and 'Use Manual Settings'. Below these are 'Lease Time' and 'Reauthentication Time' fields, both set to 1:40 minutes. At the bottom are 'OK' and 'Cancel' buttons.

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

Edit Policy Route

Show Advanced Settings
Create new Object ▼

Configuration

☒ Enable

Description:
L2TP_VPN_to_Internet (Optional)

Criteria

User:
L2TP_Remote_User ▼

Incoming:
Tunnel ▼

Please select one member:
WIZ_L2TP_VPN ▼

Source Address:
WIZ_L2TP_VPN_IP_1 ▼

Destination Address:
any ▼

DSCP Code:
any ▼

Schedule:
none ▼

Service:
any ▼

Next-Hop

Type:
Trunk ▼


Trunk:
SYSTEM_DEFAULT_VPN ▼

OK Cancel

Set Up the L2TP VPN Tunnel on the Android Device

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

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



VPN name

ZyXEL_L2TP

OK Cancel

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

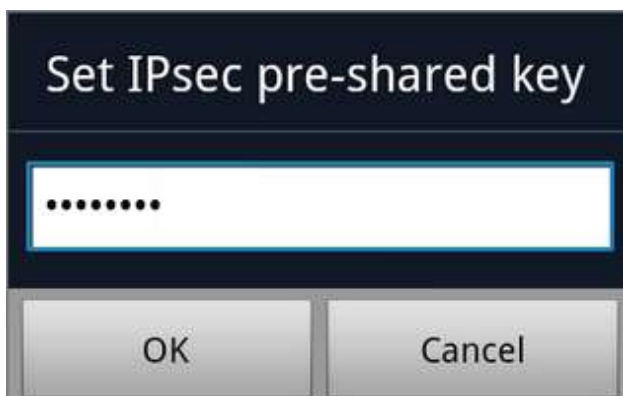


Set VPN server

172.124.163.150

OK Cancel

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



Set IPsec pre-shared key

.....

OK Cancel

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

Add L2TP/IPSec PSK VPN

VPN name
ZyXEL_L2TP

Set VPN server
172.124.163.150

Set IPsec pre-shared key
IPsec pre-shared key is set

Enable L2TP secret
L2TP secret disabled

Set L2TP secret
L2TP secret not set

DNS search domains
DNS search domains not set

Save **Cancel**

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

VPN settings

Add VPN

VPNs

ZyXEL_L2TP
Connect to network

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



Test the L2TP over IPSec VPN Tunnel

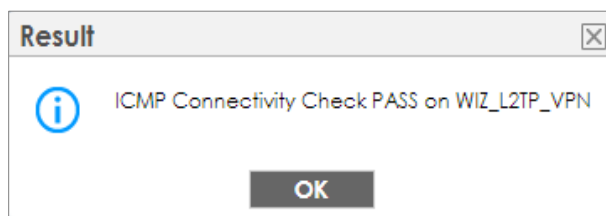
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

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



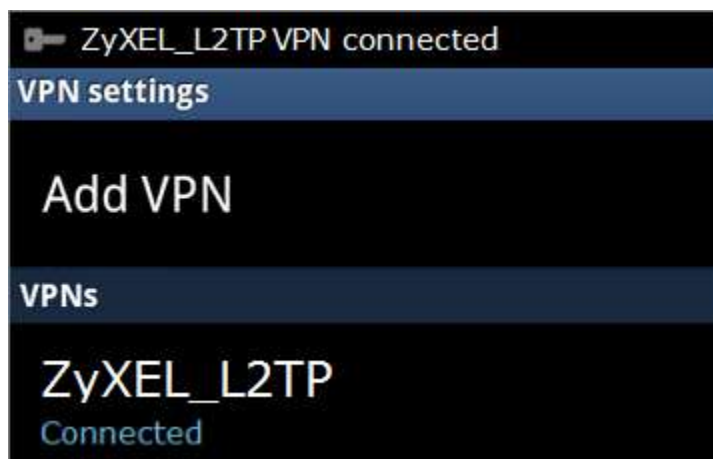
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPsec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPsec > L2TP_Remote_Users

Current L2TP Session				
<div> Disconnect Refresh </div>				
Index	User Name	Host Name	Assigned IP	Public IP
1	L2TP_Remote_Users	Android	192.168.10.10	172.124.163.254

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

Menu > Settings > Wireless & Networks > VPN



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_User 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	\$end:[NOTIFY:INVALID_PAYLOAD_TYPE]	IKE_LOG
Info	IKE	Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys	IKE_LOG

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.

Priority	Category	* Message	Note
Info	IKE	ISAKMP SA [WIZ_L2TP_VPN] is disconnected	IKE_LOG
Info	IKE	Received delete notification	IKE_LOG
Info	IKE	Recv:[HASH][DEL]	IKE_LOG
Info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
Info	IKE	[SA] : No proposal chosen	IKE_LOG
Info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch	IKE_LOG

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

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

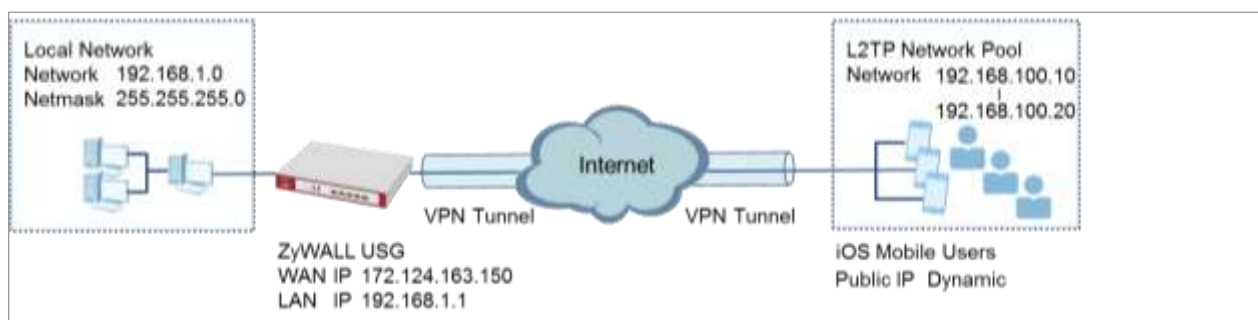
Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


Verify that the **Zone** is set correctly in the **Zone** object. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Configure L2TP VPN with iOS 8.4 Mobile Devices

This example shows how to use the VPN Setup Wizard to create a L2TP VPN between a ZyWALL/USG and an iOS 8.4 Mobile Device. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely and allow traffic from L2TP clients to go to the Internet.

ZyWALL/USG L2TP VPN with iOS Mobile Devices Example



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

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☐ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☒ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

Rule Name:

Phase 1 Setting

My Address (interface):

Authentication Method

Pre-Shared Key:

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)

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

IP Address Pool: RANGE ⓘ

Starting IP Address: 192.168.100.10

End IP Address: 192.168.100.20

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

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

VPN Setup Wizard

Wizard Type

VPN Settings

Wizard Completed

1

2

3

L2TP VPN Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_L2TP_VPN
My Address (interface):	wan1
Pre-Shared Key:	xyz12345
IP Address Pool:	RANGE, 192.168.100.10 - 192.168.100.20

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

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

The screenshot shows the 'L2TP VPN' configuration page. At the top, there's a blue header with 'L2TP VPN'. Below it, a tabbed interface shows 'Create new Object' with a dropdown menu open, highlighting 'User'. The 'General Settings' tab is active. It includes a 'Show Advanced Settings' link and a 'Config Walkthrough' icon. The main configuration area has the following fields:

- ☒ Enable L2TP Over IPSec
- VPN Connection: WIZ_L2TP_VPN
- IP Address Pool: WIZ_L2TP_VPN_IP_1 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):

The screenshot shows the 'User Configuration' dialog box. It contains the following fields and options:

- User Name: L2TP_Remote_User
- User Type: user
- Password: *****
- Retype: *****
- Description: Local User
- Authentication Timeout Settings:
 - ☒ Use Default Settings
 - ☐ Use Manual Settings
- Lease Time: 1:40 minutes
- Reauthentication Time: 1:40 minutes

At the bottom, there are 'OK' and 'Cancel' buttons.

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

Edit Policy Route

Show Advanced Settings
Create new Object ▼

Configuration

☒ Enable

Description: L2TP_VPN_to_Internet (Optional)

Criteria

User: L2TP_Remote_User ▼

Incoming: Tunnel ▼

Please select one member: WIZ_L2TP_VPN ▼

Source Address: WIZ_L2TP_VPN_IP_1 ▼

Destination Address: any ▼

DSCP Code: any ▼

Schedule: none ▼

Service: any ▼

Next-Hop

Type: Trunk ▼

Trunk: SYSTEM_DEFAULT_V ▼

OK Cancel

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).

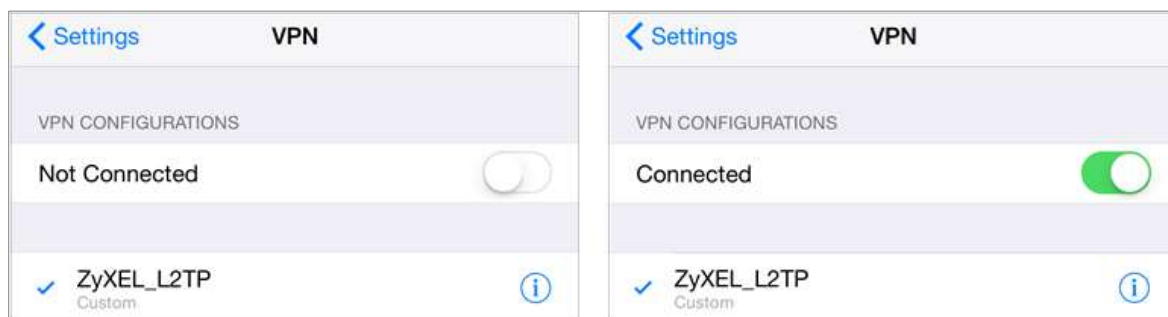
Enter **Account** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).

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).



ZyXEL_L2TP	
Type	L2TP
Description	ZyXEL_L2TP
Server	172.124.163.150
Account	L2TP_Remote_Users
RSA SecurID	<input type="checkbox"/>
Password	••••••
Secret	••••••••
Send All Traffic	<input checked="" type="checkbox"/>

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.

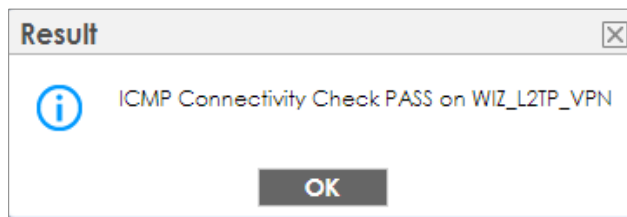
CONFIGURATION > VPN > IPSec VPN > VPN Connection



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

Current L2TP Session				
<div> Disconnect Refresh </div>				
#	User Name	Host Name	Assigned IP	Public IP
1	L2TP_Remote_Users	iPhone	192.168.100.10	10.214.30.69

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

Menu > Settings > VPN > ZyXEL_L2TP

VPN

ZyXEL_L2TP

Type

L2TP

Server

172.124.163.150

Assigned IP Address

192.168.100.10

Connect Time

0:06

Description

ZyXEL_L2TP

Server

172.124.163.150

Account

L2TP_Remote_Users

RSA SecurID

Password

••••••

Secret

••••••••

Send All Traffic

What Could Go Wrong?

If you see [alert] log message such as below, please check ZyWALL/USG L2TP **Allowed User** or **User/Group Settings**. iOS Mobile users must use the same Username and Password as configured in ZyWALL/USG to establish the L2TP VPN.

Priority	Category	Message	Notes
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 [WZ_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 [WZ_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.

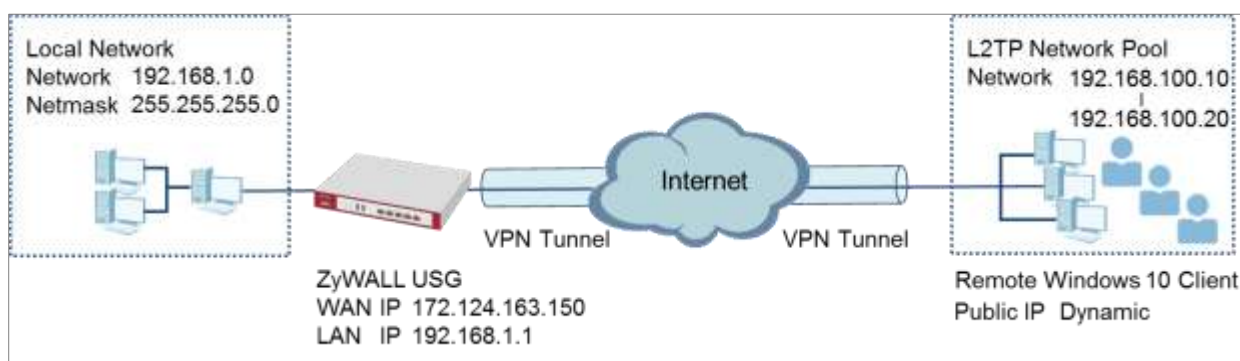
Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


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 Windows 10 clients. Click **Next**.

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

- ☐ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☒ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

Rule Name:

Phase 1 Setting

My Address (interface):

Authentication Method

Pre-Shared Key:

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

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

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

IP Address Pool: RANGE ⓘ

Starting IP Address: 192.168.100.10

End IP Address: 192.168.100.20

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

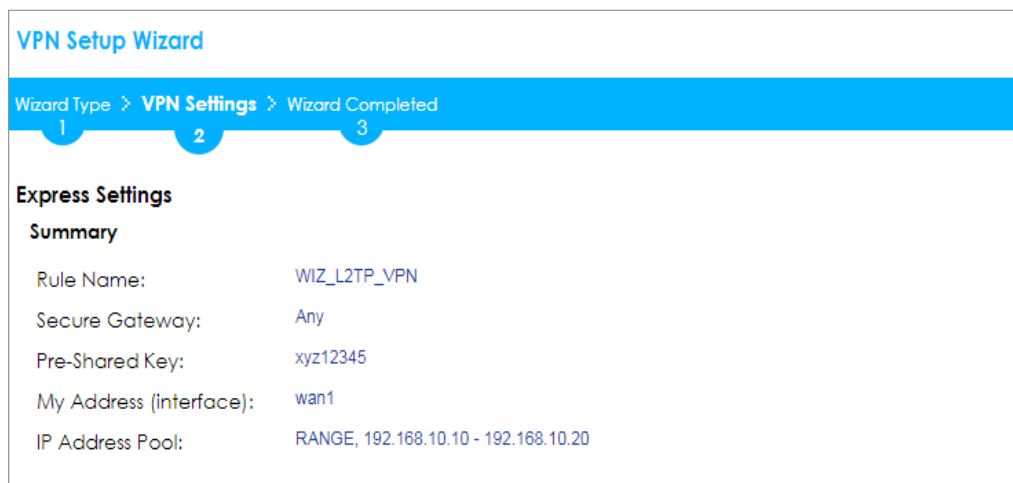
Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

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

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



VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

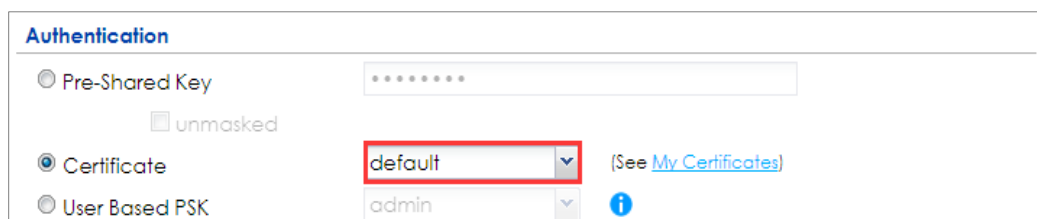
Express Settings

Summary

Rule Name:	WIZ_L2TP_VPN
Secure Gateway:	Any
Pre-Shared Key:	xyz12345
My Address (interface):	wan1
IP Address Pool:	RANGE, 192.168.10.10 - 192.168.10.20

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

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



Authentication

☐ Pre-Shared Key

☐ unmasked

☒ Certificate default (See [My Certificates](#))

☐ User Based PSK admin

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

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

The screenshot displays the 'L2TP VPN' configuration page. At the top, there is a blue header with 'L2TP VPN' and a 'Create new Object' dropdown menu. Below this, a 'User' button is highlighted with a red box. The 'General Settings' section includes options for 'Enable L2TP Over IPSec' (checked), 'VPN Connection' (WIZ_L2TP_VPN), 'IP Address Pool' (WIZ_L2TP_VPN_IP_1), 'Authentication Method' (default), and 'Advance' settings. The 'Advance' section includes 'Allowed User' (any), 'Keep Alive Timer' (60), and DNS/WINS server settings. Below the main configuration area, a 'User Configuration' dialog box is shown, containing fields for 'User Name' (L2TP_Remote_User), 'User Type' (User), 'Password' (masked), 'Retype' (masked), 'Description' (Local User), and 'Authentication Timeout Settings' (Lease Time: 1440 minutes, Reauthentication Time: 1440 minutes). The 'OK' button is highlighted with a red box.

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

Edit Policy Route

Show Advanced Settings
Create new Object ▼

Configuration

☒ Enable

Description: L2TP_VPN_to_Internet (Optional)

Criteria

User: L2TP_Remote_User ▼

Incoming: Tunnel ▼

Please select one member: WIZ_L2TP_VPN ▼

Source Address: WIZ_L2TP_VPN_IP_1 ▼

Destination Address: any ▼

DSCP Code: any ▼

Schedule: none ▼

Service: any ▼

Next-Hop

Type: Trunk ▼

Trunk: SYSTEM_DEFAULT_V1 ▼

OK Cancel

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

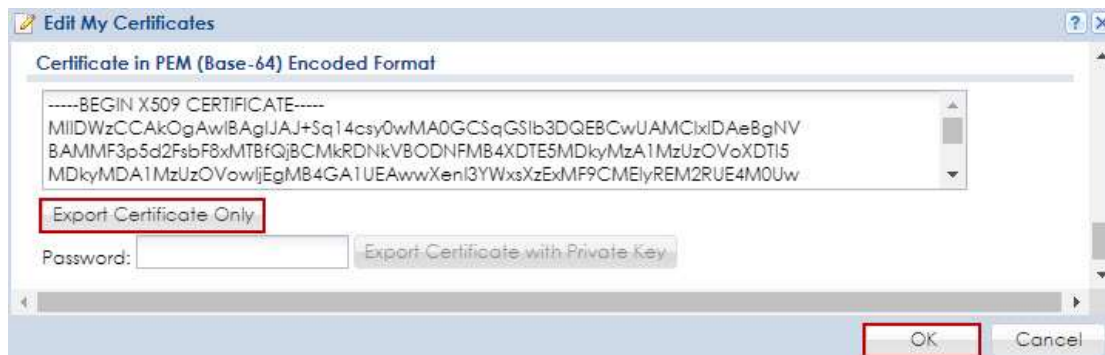
Go to ZyWALL/USG **CONFIGURATION > Object > Certificate**, select the certificate (default in this example) and click **Edit**.

CONFIGURATION > Object > Certificate > default

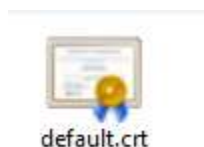
My Certificates Setting						
Add Edit Remove Object References						
#	Name *	Type	Subject	Issuer	Valid From	Valid To
1	default	SELF	CN=vpn50_88ECA31E2398	CN=vpn50_88ECA31E2398	2017-01-07 10:19:45 GMT	2027-01-05 10:19:45 GMT

Export default certificate from ZyWALL/USG.

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

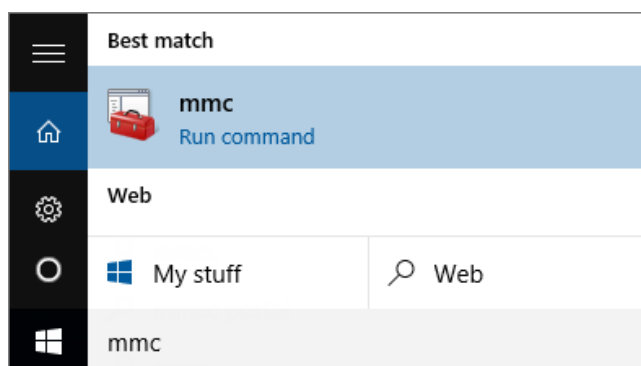


Save **default** certificate as ***.crt** file to Windows 10 computer.



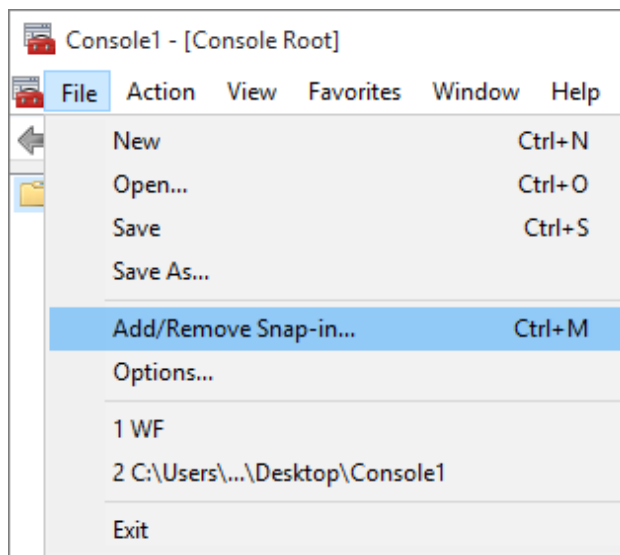
In Windows 10 Operating System, go to **Start Menu > Search Box**. Type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



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

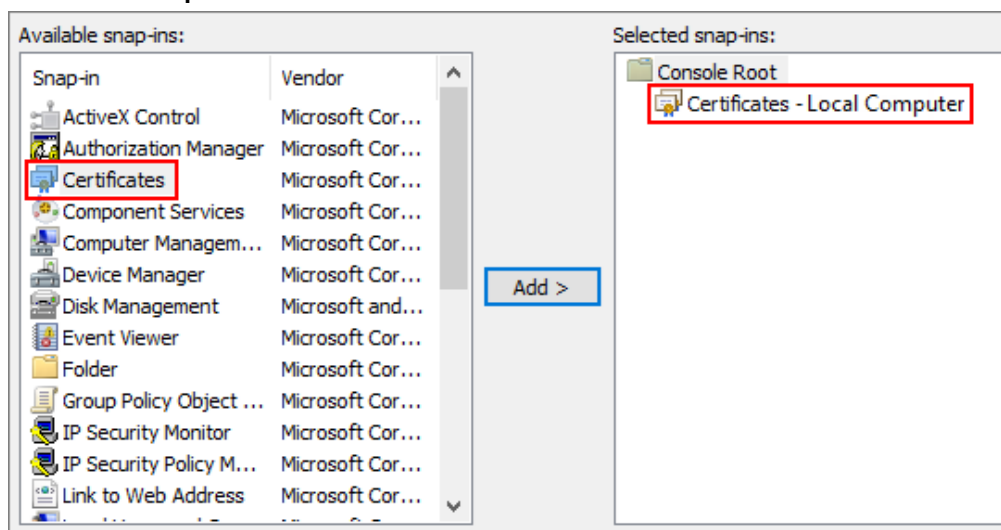
File > Add/Remove Snap-in...



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

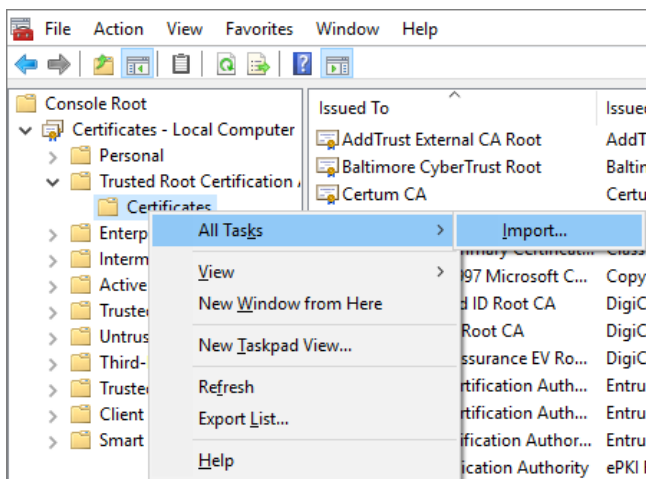
Press **OK** to close the Snap-ins window.

Available snap-ins > Certificates > Add

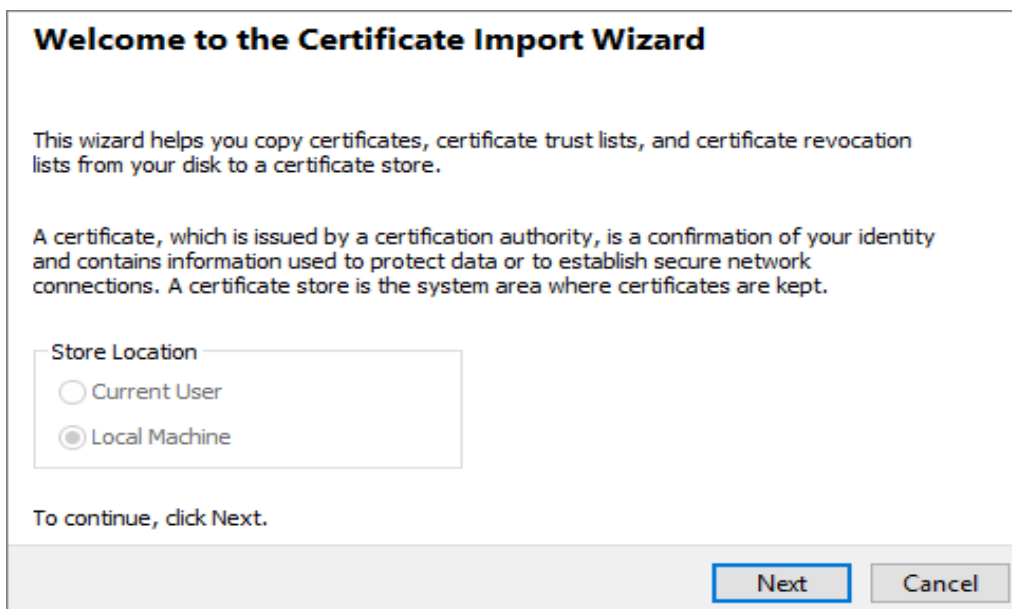


In the mmc console window, go to **Certificates (Local Computer) > Trusted Root**

Certification Authorities, right click **Certificate > All Tasks > Import...**



Click **Next**.



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

File to Import

Specify the file you want to import.

File name:

C:\Users\USER\Downloads\default.crt

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate
☒ Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities
Browse...

Next
Cancel



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

Set Up the L2TP VPN Tunnel on the Windows 10

To configure L2TP VPN in Windows 10 operating system, go to **Start > Settings > Network & Internet > VPN > Add a VPN Connection** and configure as follows.

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

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

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

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

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

Add a VPN connection

VPN provider
Windows (built-in)

Connection name
ZyXEL_L2TP_VPN

Server name or address
172.124.163.150

VPN type
Layer 2 Tunneling Protocol with IPsec (L2TP/I

Type of sign-in info
User name and password

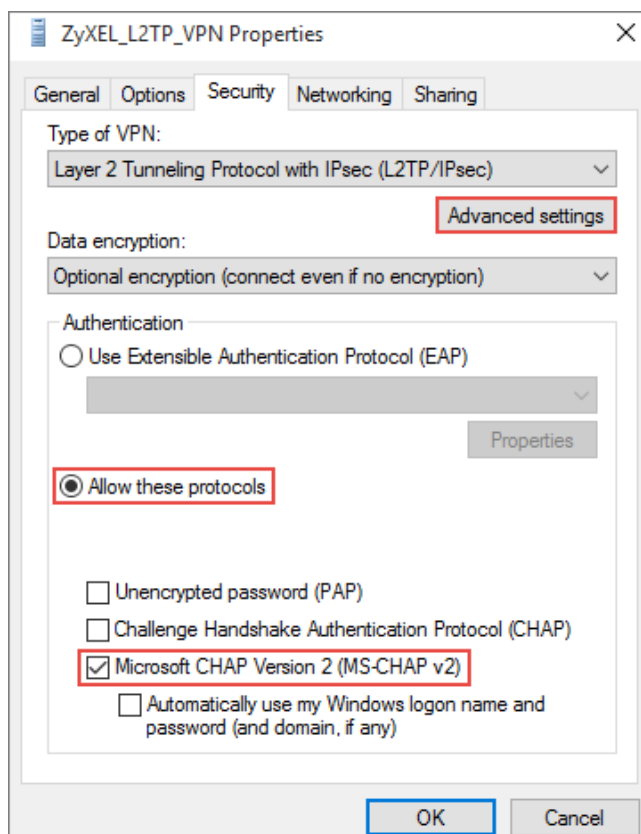
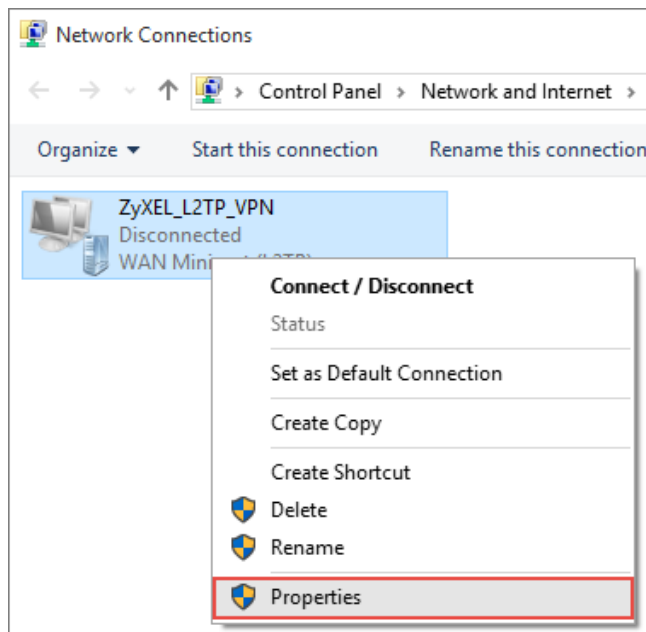
User name (optional)
L2TP_Remote_Users

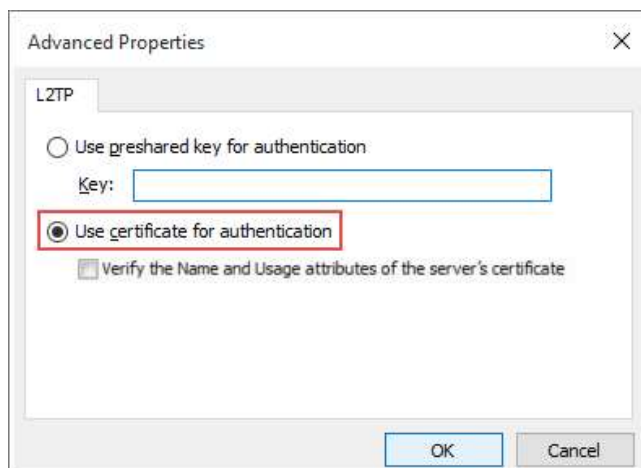
Password (optional)

☒ Remember my sign-in info

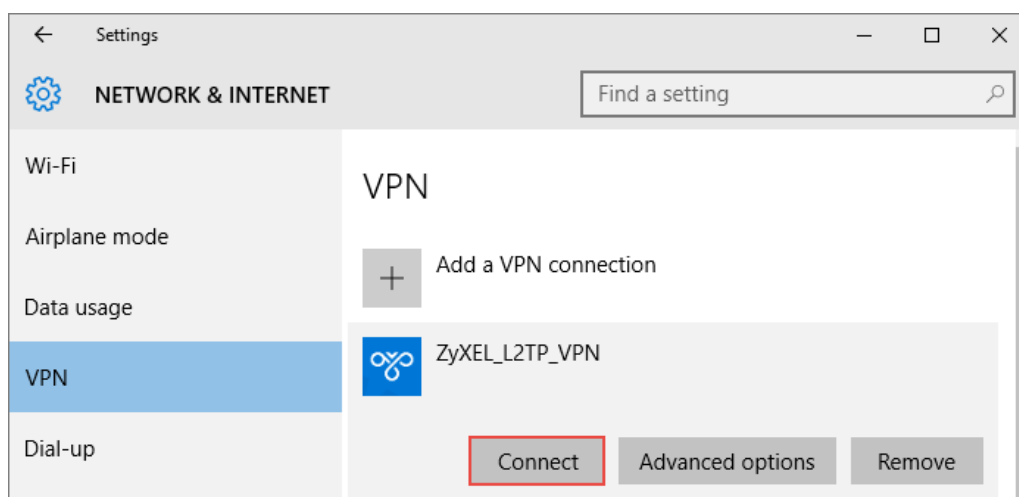
Save
Cancel

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





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.

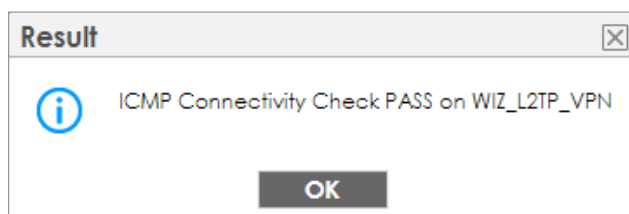
CONFIGURATION > VPN > IPSec VPN > VPN Connection



Status	Name	VPN Gateway	Policy
	WIZ_L2TP_VPN	WIZ_L2TP_VPN	WIZ_L2TP_VPN_LOCAL

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

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



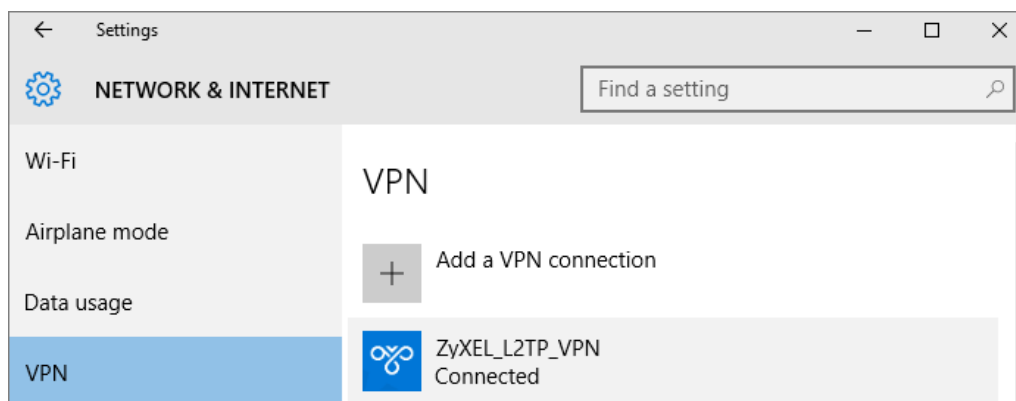
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

Current L2TP Session				
Disconnect Refresh				
#	User Name	Host Name	Assigned IP	Public IP
1	L2TP_Remote_User	ellen-PC	192.168.100.10	10.214.30.69
Page 1 of 1 Show 50 Items Displaying 1 of 1				

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 : 0x0103273f03f379ad / 0x05efcd54196dc6cd6	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.

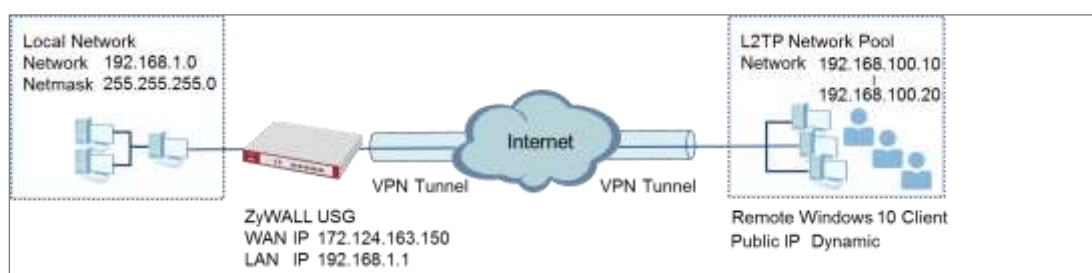
Make sure the ZyWALL/USG units' security policies allow IPsec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.


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

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

Rule Name:

Phase 1 Setting

My Address (interface):

Authentication Method

Pre-Shared Key:

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

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

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1 2 3

L2TP VPN Settings

IP Address Pool: RANGE ⓘ

Starting IP Address: 192.168.100.10

End IP Address: 192.168.100.20

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

Summary

Rule Name:	WIZ_L2TP_VPN
Secure Gateway:	Any
Pre-Shared Key:	xyz12345
My Address (interface):	wan1
IP Address Pool:	RANGE, 192.168.10.10 - 192.168.10.20

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_L2TP_VPN

Secure Gateway: Any

Pre-Shared Key: xyz12345

My Address (interface): wan1

IP Address Pool: RANGE, 192.168.10.10 - 192.168.10.20

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

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

Authentication

☐ Pre-Shared Key

☐ unmasked

☒ Certificate

☐ User Based PSK

default

(See [My Certificates](#))

admin

i

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

troubleshooting

General Settings

☒ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_1 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

☒ Use Default Settings
 ☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

OK

Cancel

L2TP VPN

Show Advanced Settings

Create new Object

Configuration Walkthrough

Troubleshooting

General Settings

☒ Enable L2TP Over IPSec

VPN Connection: WIZ_L2TP_VPN

IP Address Pool: WIZ_L2TP_VPN_IP_1 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**.

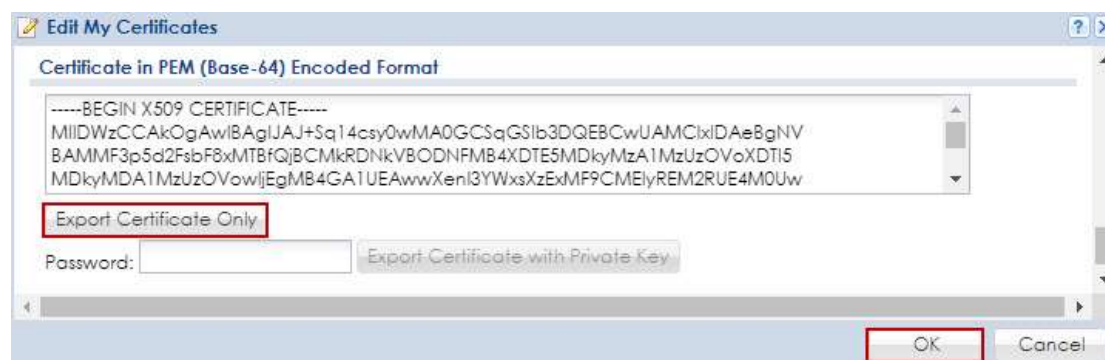
CONFIGURATION > Object > Certificate > default



#	Name	Type	Subject	Issuer	Valid From	Valid To
1	default	SELF	CN=vpn50_BBECA31E2398	CN=vpn50_BBECA31E2398	2017-01-07 10:19:45 GMT	2027-01-05 10:19:45 GMT

Export default certificate from ZyWALL/USG.

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



Save **default** certificate as ***.crt** file to Android mobile phone computer.



Set Up the L2TP VPN Tunnel on the iOS Mobile Device

- 1 To configure L2TP VPN in iOS operating system, go to **Start > Settings > Network & Internet > VPN > Add a VPN Connection** and configure as follows.
- 2 VPN Provider set to Windows (built-in).
- 3 Configure **Connection name** for you to identify the VPN configuration.

- 4 Set **Server** name or address to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).
- 5 Select VPN type to Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec).
- 6 Enter **User name** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).

Add a VPN connection

VPN provider
Windows (built-in) ▾

Connection name
ZyXEL_L2TP_VPN

Server name or address
172.124.163.150

VPN type
Layer 2 Tunneling Protocol with IPsec (L2TP/I ▾

Type of sign-in info
User name and password ▾

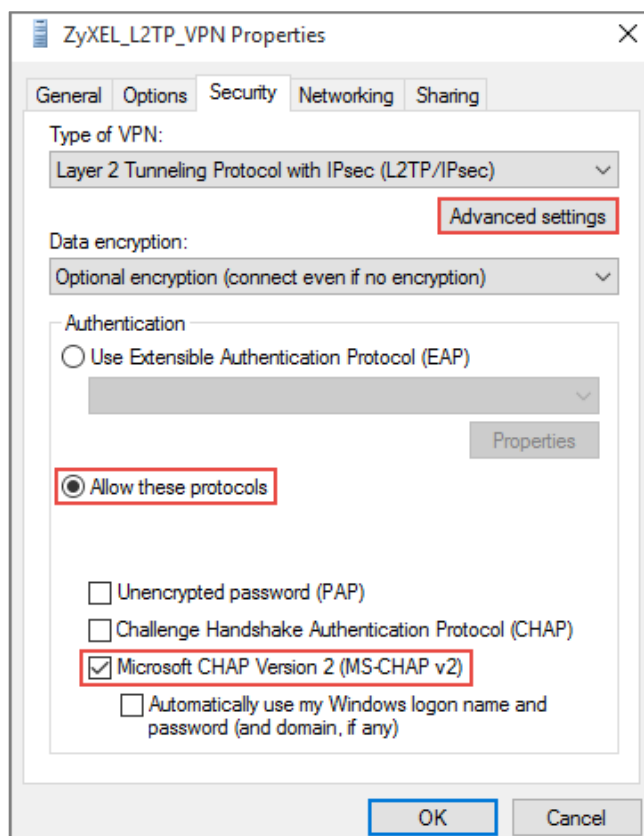
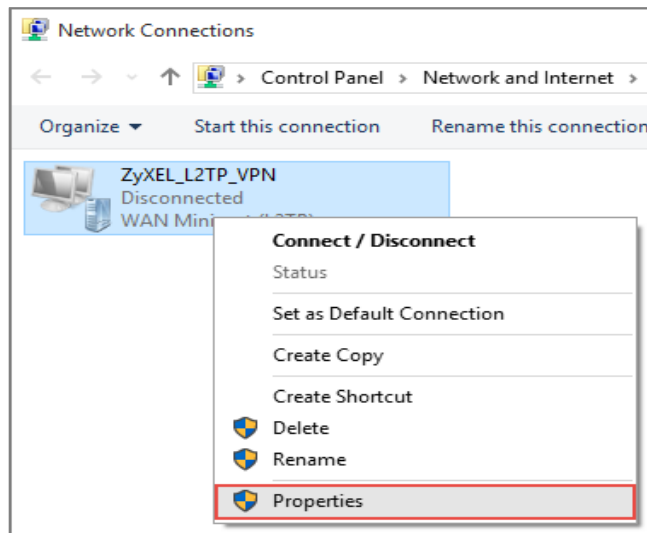
User name (optional)
L2TP_Remote_Users

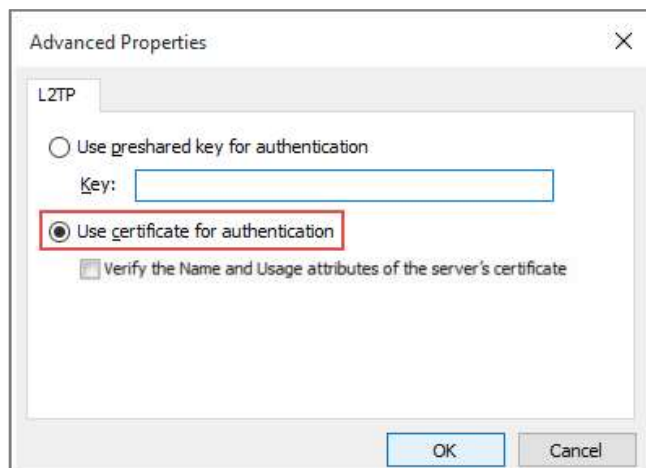
Password (optional)
•••••

☒ Remember my sign-in info

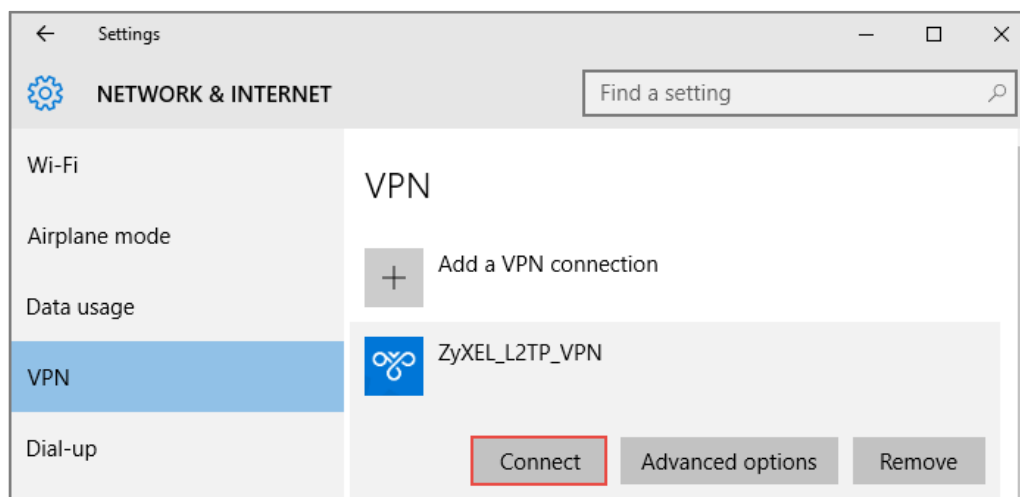
Save Cancel

- 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.





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



Test the L2TP over IPSec VPN Tunnel

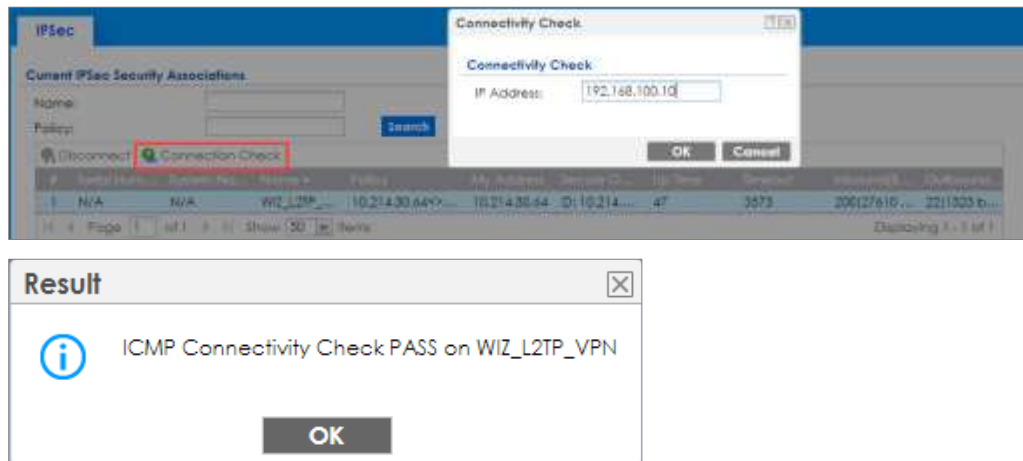
1. Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection



- 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



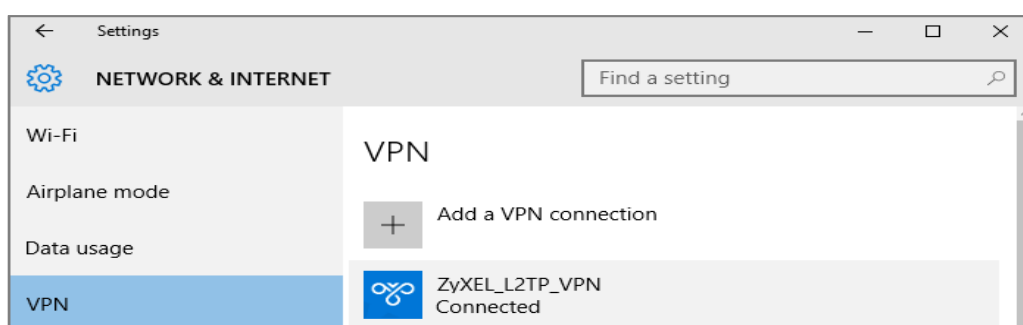
- Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

Current L2TP Session				
<div> Disconnect Refresh </div>				
User Name	Host Name	Assigned IP	Public IP	
L2TP_Remote_Users	ellen-PC	192.168.100.10	10.214.30.69	

- 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.

#	Seq	Priority	Category	Message	Note
1	2...	Info	IKE	ISAKMP SA [WZ_L2TP_VPN] is disconnected	IKE_LOG
2	2...	Info	IKE	Send:[HASH][DEL] [counters]	IKE_LOG
3	2...	Info	IKE	Tunnel [WZ_L2TP_VPN:WZ_L2TP_VPN:0x080ad2b4] is disconnected	IKE_LOG
4	2...	alert	L2TP Over IPSec	User [L2TP_Remote_User] 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.

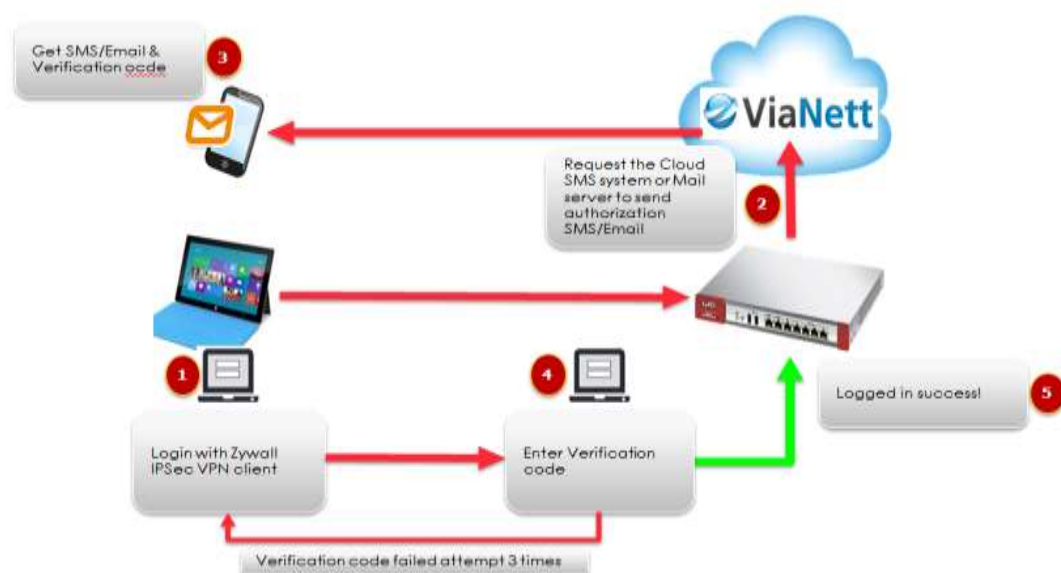
Priority	Category	Message	Note
Info	IKE	ISAKMP SA [WZ_L2TP_VPN] is disconnected	IKE_LOG
Info	IKE	Received delete notification	IKE_LOG
Info	IKE	Recv:[HASH][DEL]	IKE_LOG
Info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
Info	IKE	[SA] : No proposal chosen	IKE_LOG
Info	IKE	[ID] : Tunnel [WZ_L2TP_VPN] 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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☐ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☒ **VPN Settings for Configuration Provisioning**
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

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

Type of VPN policy

- ☒ **Express**
- ☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Scenario

Rule Name:

WIZ_VPN_PROVISIONING

Application Scenario:

Remote Access (Server Role)

Type a secure **Pre-Shared Key** (8-32 characters). Set **Local Policy** to be the IP address range of the network connected to the ZyWALL/USG.

Quick Setup > VPN Setup Wizard > Welcome > Wizard Type > VPN Settings-2

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Configuration

Secure Gateway:

Any

Pre-Shared Key:

zyx12345

Local Policy (IP/Mask)

192.168.1.33

/

255.255.255.0

Remote Policy (IP/Mask):

Any

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

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

VPN Setup Wizard

[Wizard Type](#) > **VPN Settings** > [Wizard Completed](#)

1

2

3

Express Settings

Summary

Rule Name:	WIZ_VPN_PROVISIONING
Secure Gateway:	Any
Pre-Shared Key:	zyx12345
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	Any

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

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

VPN Setup Wizard

[Wizard Type](#) > [VPN Settings](#) > **Wizard Completed**

1

2

3

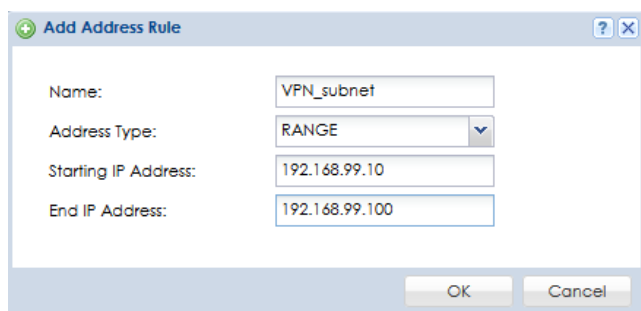
Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_VPN_PROVISIONING
Secure Gateway:	Any
Pre-Shared Key:	zyx12345
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	Any

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

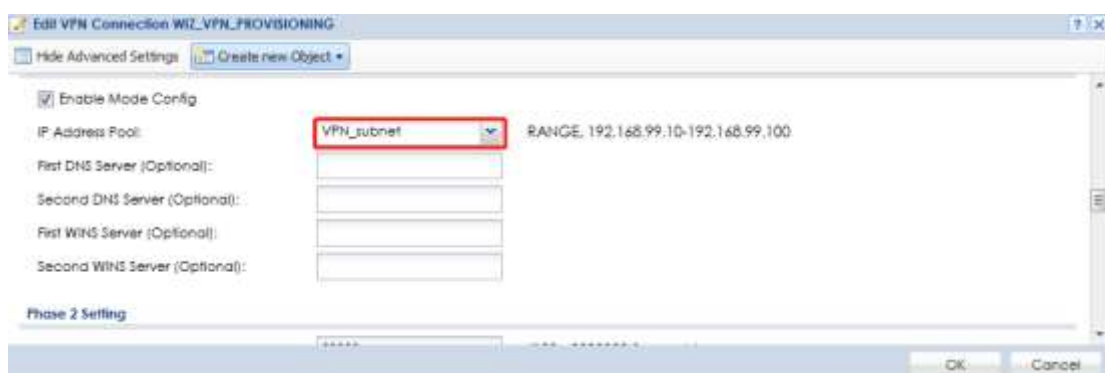


The 'Add Address Rule' dialog box contains the following fields:

- Name: VPN_subnet
- Address Type: RANGE
- Starting IP Address: 192.168.99.10
- End IP Address: 192.168.99.100

Buttons: OK, Cancel

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



The 'Edit VPN Connection WIZ_VPN_PROVISIONING' dialog box shows the following settings:

- ☒ Enable Mode Config
- IP Address Pool: VPN_subnet (highlighted with a red box) RANGE, 192.168.99.10-192.168.99.100
- First DNS Server (Optional):
- Second DNS Server (Optional):
- First WINS Server (Optional):
- Second WINS Server (Optional):

Section: Phase 2 Setting

Buttons: OK, Cancel

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

General Settings

☒ Enable Configuration Provisioning

Authentication

Client Authentication Method: default

Configuration

Status	Priority	Type	VPN Connection	Allowed User
1	1	404	WT_VPN_PROVISIONING	Remote_Client

Page 1 of 1 | Show 50 items | Deploying 1 of 1

Apply Reset

Set up the ZyWALL IPsec VPN Client

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

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

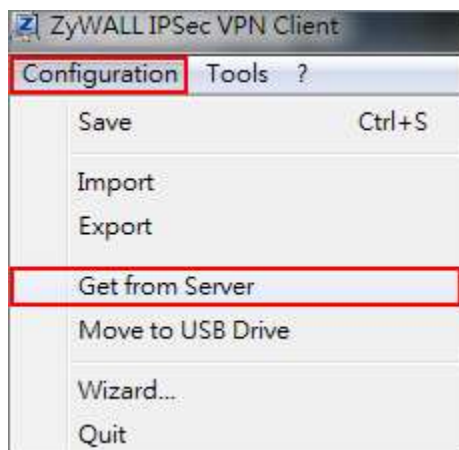
Search by Model Number

ZyWALL IPsec VPN Client

ZyWALL IPsec VPN Client

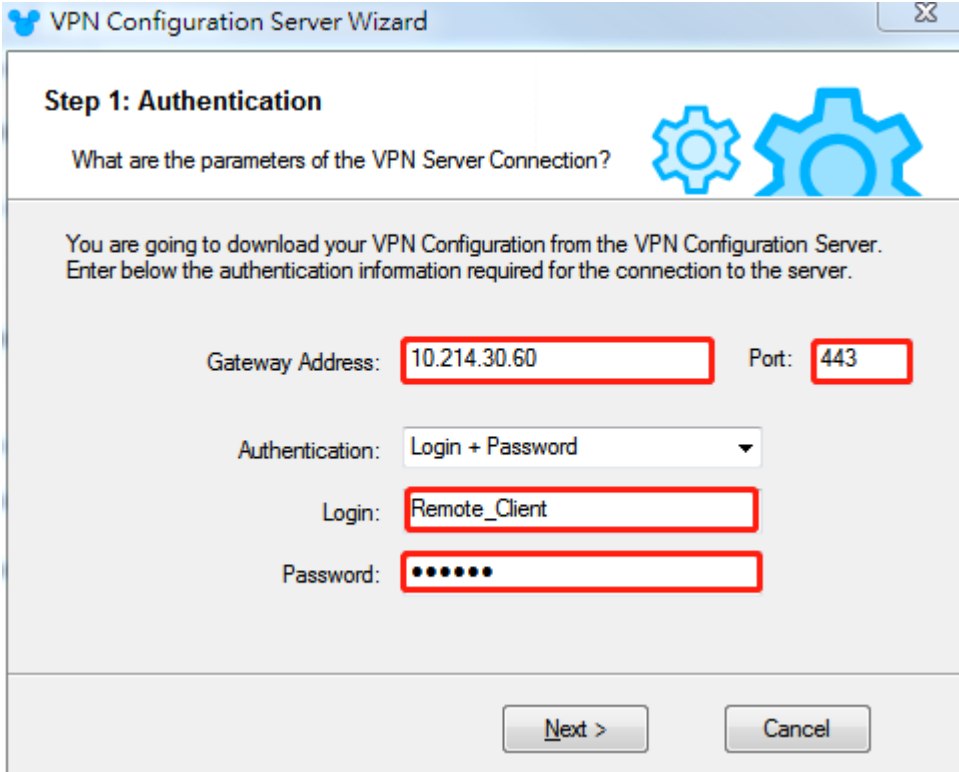
Open ZyWALL IPsec VPN Client, select **CONFIGURATION > Get from Server**.

CONFIGURATION > Get from Server



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

CONFIGURATION > Get from Server > Step 1: Authentication



VPN Configuration Server Wizard

Step 1: Authentication

What are the parameters of the VPN Server Connection?

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


Gateway Address: Port:

Authentication:

Login:

Password:

CONFIGURATION > Get from Server > Step 2: Processing



VPN Configuration Server Wizard

Step 2: Processing...

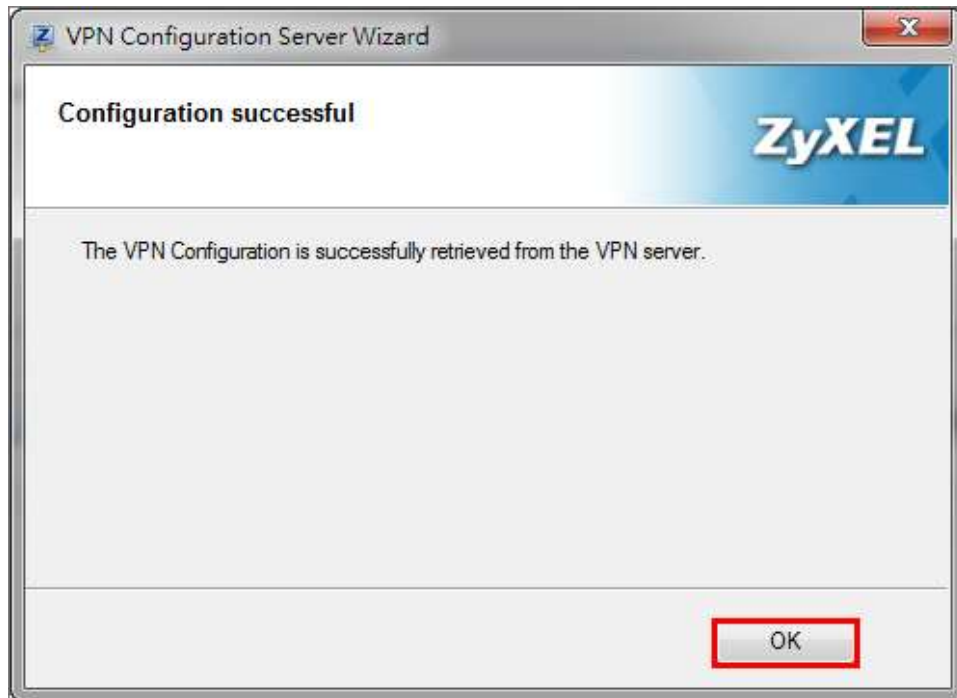
Requesting the VPN Configuration.

Downloading the VPN Configuration from the server:

- ☒ Init Ok.
- ☒ Init cnx server (10.214.30.60) Ok.
- ☐ Send https request...
 - Receive Config. from Server...
 - Write Config. file...
 - Apply Config. file...

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

CONFIGURATION > Get from Server > Configuration successful



VPN CONFIGURATION > 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.

The screenshot shows the 'Mail Server' configuration page in the ZyXel web interface. The 'General Settings' tab is selected. The following fields are highlighted with red boxes:

- Mail Server:** smtp.pchome.com.tw (Outgoing SMTP Server Name or IP Address)
- Mail Subject:** ☐ Append system name ☐ Append date time
- Mail Server Port:** 25
- Mail From:** cooldia@pchome.com.tw (Email Address)
- SMTP Authentication:** ☒
- User Name:** cooldia
- Password:** [masked with dots]
- Retype to Confirm:** [masked with dots]

The **Schedule** section at the bottom shows 'Time For Sending Report' set to 0 (hours) and 0 (minutes).

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

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

The screenshot shows the ZyXel web interface with the 'SMS' tab selected. The 'General Settings' section includes a checked 'Enable SMS' checkbox and a 'Default country code for phone number' field set to '886'. Below this is a link to 'Purchase SMS Voucher from Zyxel reseller'. The 'ViaNett Configuration' section contains three fields: 'User Name' (pd000245), 'Password' (masked with dots), and 'Retype to Confirm' (masked with dots). Red boxes highlight the 'Enable SMS' checkbox, the '886' country code, and the 'ViaNett Configuration' fields.

Set up authentication for 2 factor VPN connection

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

1. Select the check box **"Enable"** to enable 2 factor authentications.
2. Enter the maximum time (in minutes) that the user must click or tap the authorization link in the SMS or email in order to get authorization for the VPN connection.
3. Select which kinds of VPN tunnels require Two-Factor Authentication. in this scenario, we enable 2 factor authentication on IPSec VPN Access
4. This list displays the names of the users and user groups that can be selected for two-factor authentication.
5. Use this section to configure how to send an SMS or email for authorization.
We select both methods in this scenario.
6. Configure the link that the user will receive in the SMS or email. The user must be able to access the link.
7. You can either create a default message in the text box or upload a message file (Use Multilingual file) from your computer.
8. Click **"Apply"** button to save your changes to the Zyxel Device.

General Settings

☒ **Enable**

Valid Time: [1-15 minutes]

Two-Factor Authentication for Service:

☐ SSL VPN Access ☒ **IPSec VPN Access** ☐ L2TP/IPSec VPN Access

User/Group

Selectable User/Group Objects

admin
ldap-users
radius-users
ad-user
test

Selected User/Group Objects

any

Delivery Settings

Deliver Authorize Link Method: ☒ **SMS** ☒ **Email**

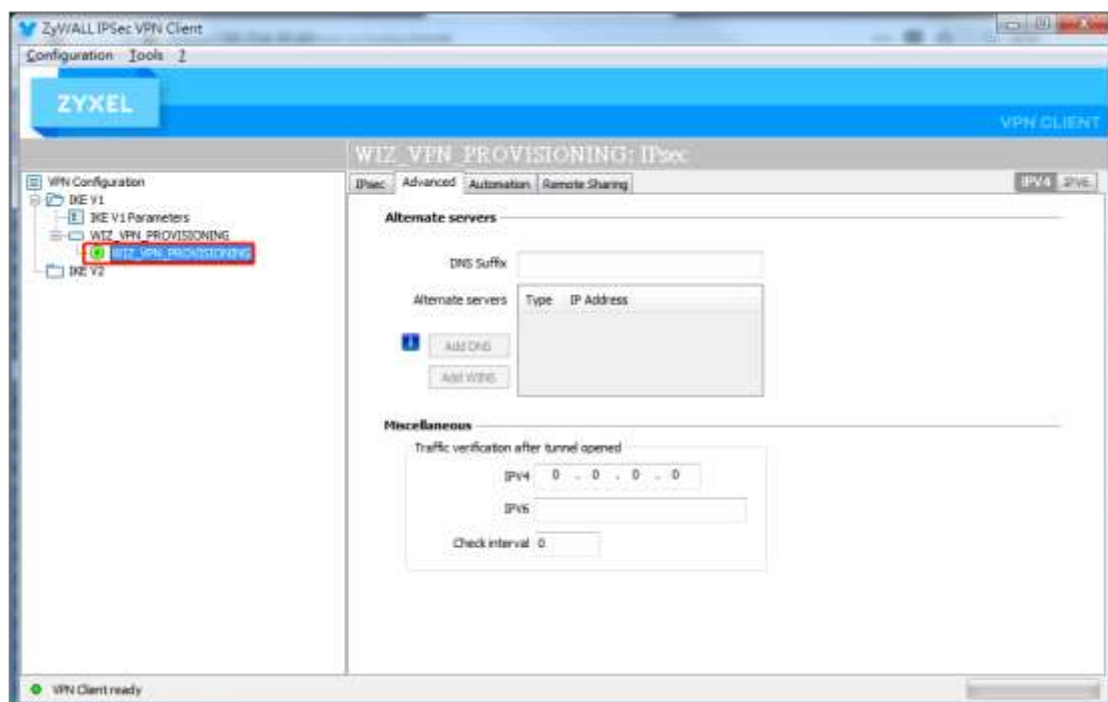
Authorize Link URL Address: [Domain Name or IP Address]

Message: ☒ Use Default Message ☐ Use Multilingual file

«user». You have initiated a VPN connection to a secured network behind the «host». Please click or tap the following link within «time» minutes to get authorization for the VPN connection. «url»

Test the Result

Go to **VPN Configuration > IKEv1**, right click the **WIZ_VPN_PROVISIONING** and select **Open tunnel**. You will see the **Tunnel opened** on ZyWALL IPSec VPN client



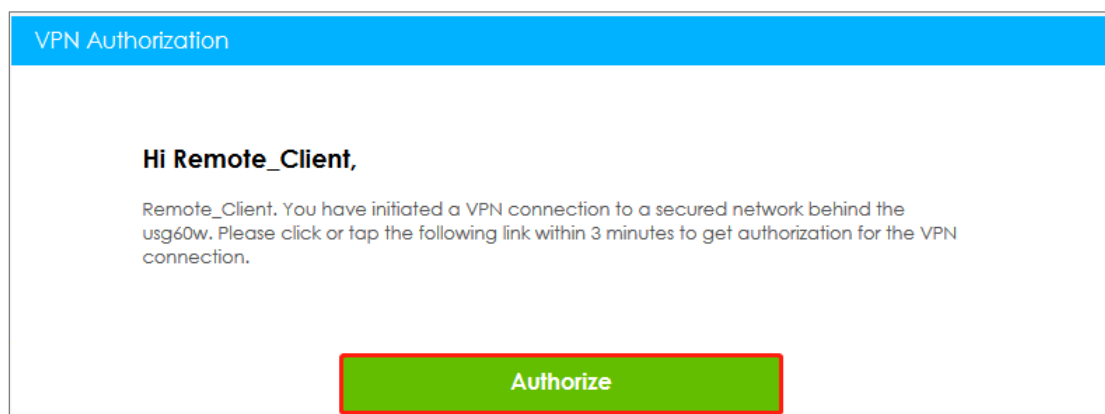
The VPN tunnel is created from the ZyWALL IPSec VPN client to the ZyWALL/USG, but we are still unable to access Intranet behind the ZyWALL/USG. The ZyWALL/USG send authorized link via phone number or email address in order to authenticate this user's

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.

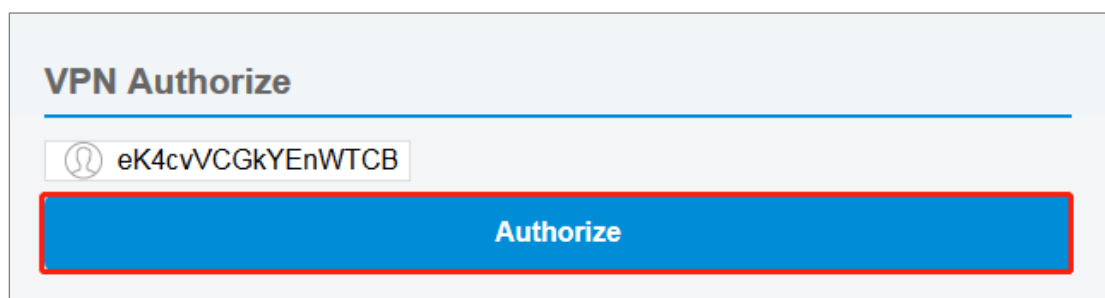
The following is authorized example by email and SMS

Authorized by email link

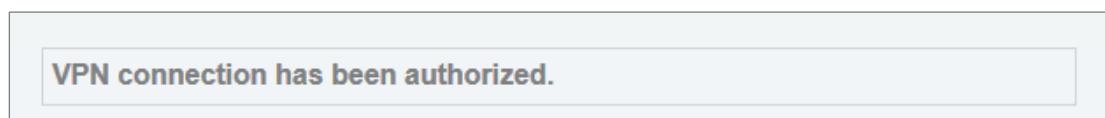
1. Received authorization mail with authorize link.



2. Click the “**Authorize**” to authorization.

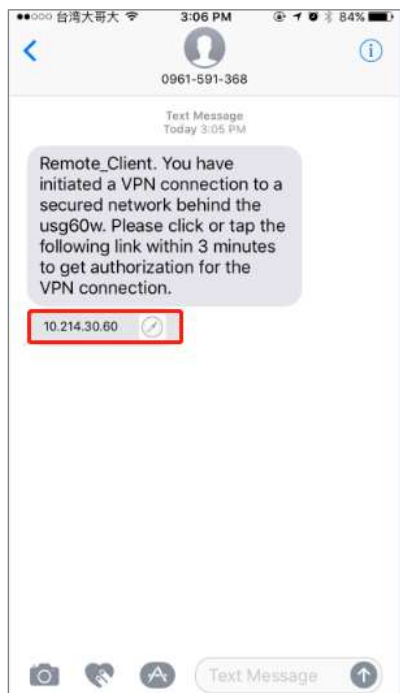


3. After we see “**VPN connection has been authorized**”, we can access the secured network behind the ZyWALL/USG.

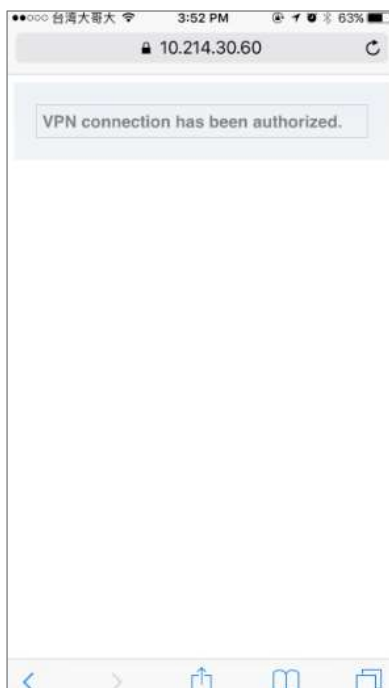
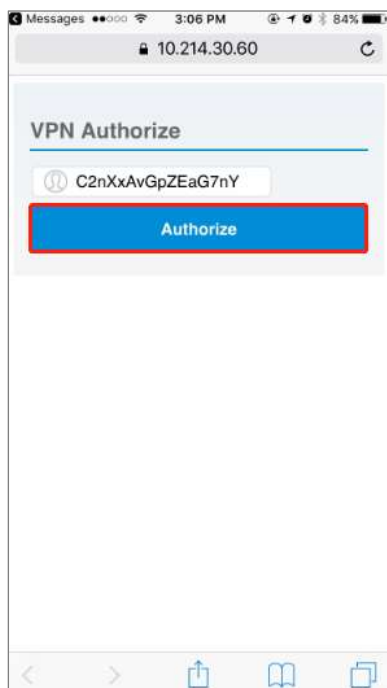


Authorized by SMS

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

General Settings

☒ Enable SMS

Default country code for phone number:

86

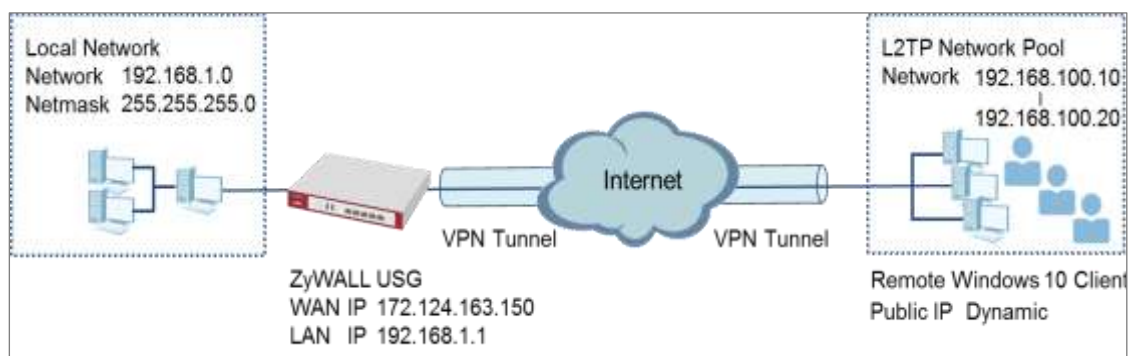
(1-4) digit


[Purchase SMS Voucher from Zyxel reseller](#)

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

This is an example of using the L2TP VPN and VPN client software included in Android mobile phone operating systems. When the VPN tunnel is configured, users can securely access the network behind the ZyWALL/USG and allow traffic from L2TP clients to go to the Internet from an Android mobile phone.

ZyWALL/USG L2TP VPN with Remote Android Mobile Phone Client Example

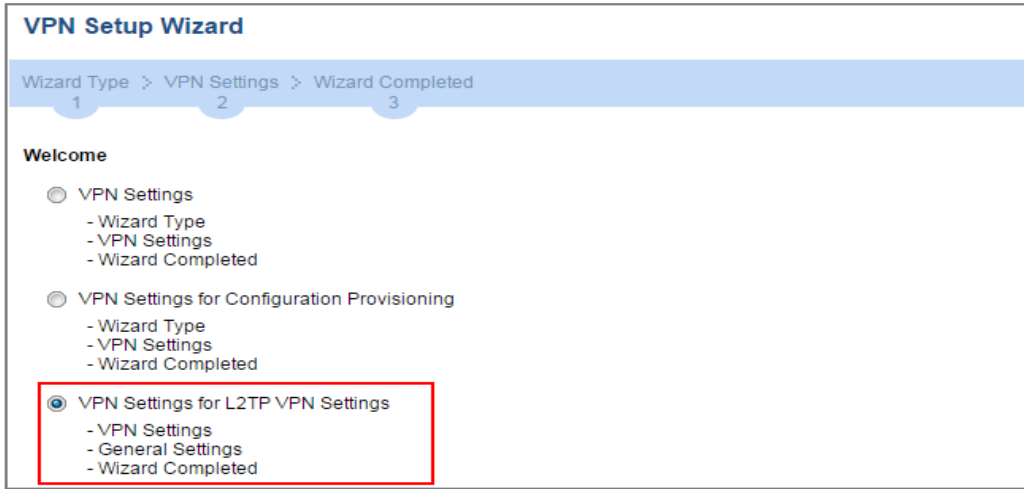


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25) and Android (Version: 10.0.10240)

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

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

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

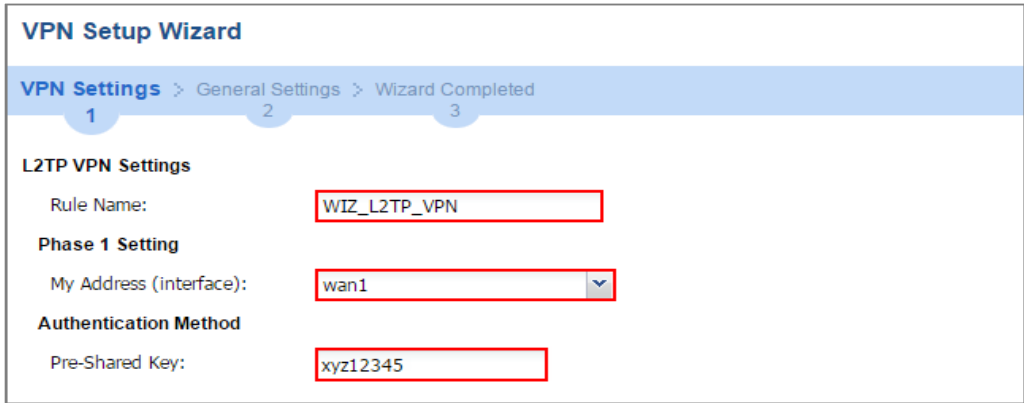
Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

- ☐ VPN Settings
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☐ VPN Settings for Configuration Provisioning
 - Wizard Type
 - VPN Settings
 - Wizard Completed
- ☒ VPN Settings for L2TP VPN Settings
 - VPN Settings
 - General Settings
 - Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings



VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed
1 2 3

L2TP VPN Settings

Rule Name:

Phase 1 Setting

My Address (interface):

Authentication Method

Pre-Shared Key:

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

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

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

123

L2TP VPN Settings

IP Address Pool: RANGE ⓘ
 Starting IP Address: 192.168.100.10
 End IP Address: 192.168.100.20
 First DNS Server (Optional):
 Second DNS Server (Optional):
☒ Allow L2TP traffic Through WAN

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Advanced Settings

Summary

Rule Name: WIZ_L2TP_VPN
 Secure Gateway: Any
 Pre-Shared Key: xyz12345
 My Address (interface): wan1
 IP Address Pool: RANGE, 192.168.100.10 - 192.168.100.20

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

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

VPN Setup Wizard

[Wizard Type](#) > [VPN Settings](#) > **Wizard Completed**

123

L2TP VPN Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_L2TP_VPN
My Address (interface):	wan1
Pre-Shared Key:	xyz12345
IP Address Pool:	RANGE, 192.168.100.10 - 192.168.100.20

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

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

Authentication

☐ Pre-Shared Key

☐ unmasked

☒ Certificate

default

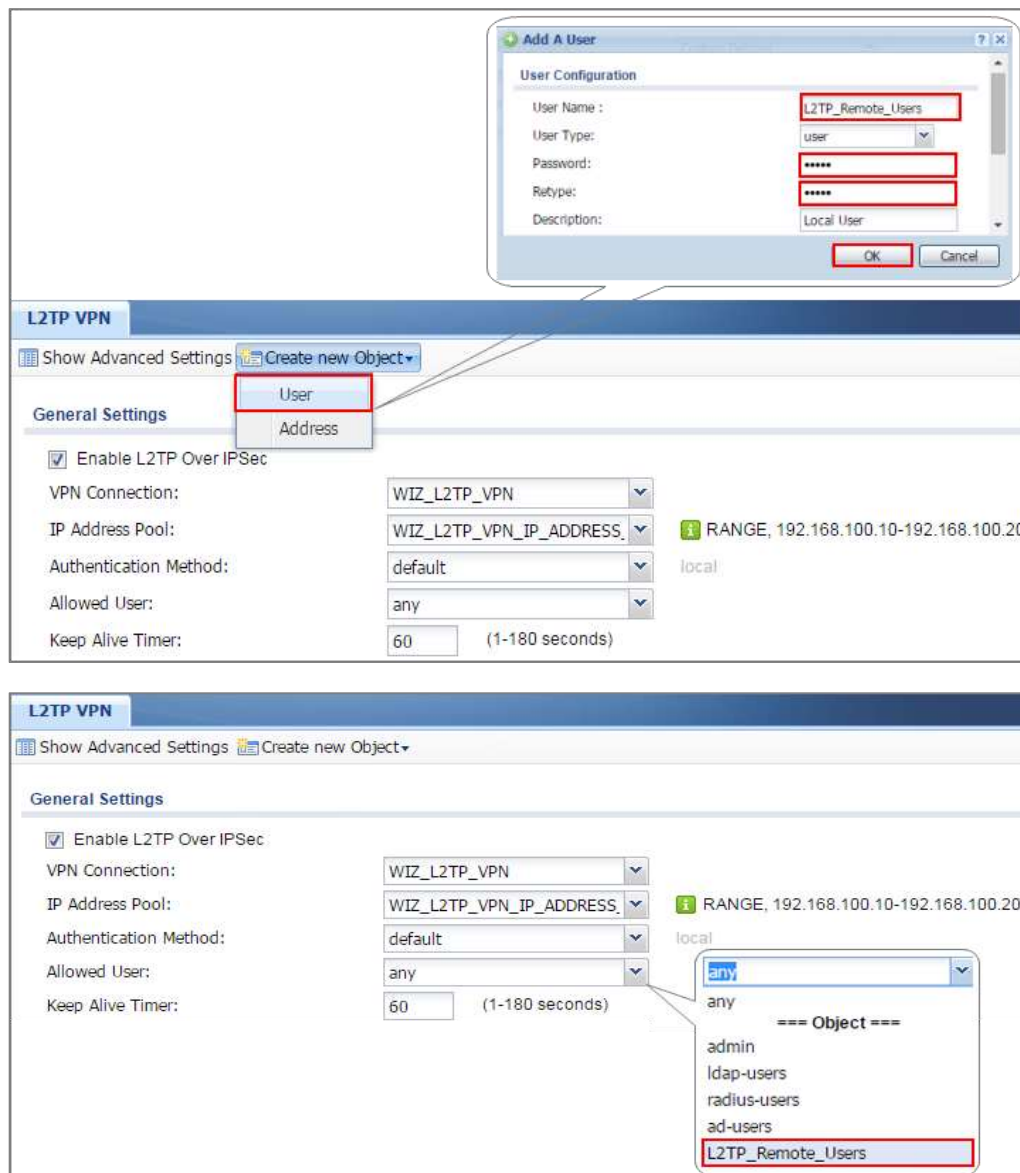
(See [My Certificates](#))

☐ User Based PSK

L2TP_Remote_Users

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

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



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**.

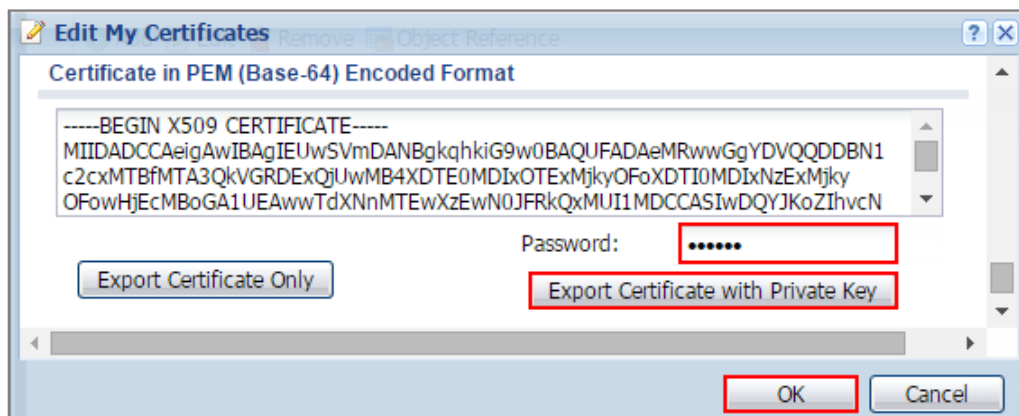
CONFIGURATION > **Object** > **Certificate** > **default**



#	Name	Type	Subject	Issuer	Valid From	Valid To
1	default	SELF	CN=usg110_107BEFD11B50	CN=usg110_107BEFD11B50	2014-02-19 11:29:28 GMT	2024-02-17 11:29:28 GMT

Export default certificate from ZyWALL/USG.

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



Edit My Certificates Remove Object Reference

Certificate in PEM (Base-64) Encoded Format

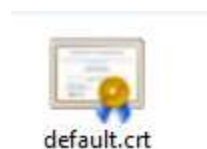
```
-----BEGIN X509 CERTIFICATE-----
MIIDADCCAeigAwIBAgIEUwSVmDANBgkqhkiG9w0BAQUFADAeMRwwGgYDVQQDDBN1
C2cxMTBfMTA3QkVGRDExQjUwMB4XDTE0MDIxOTExMjkyOFoXDTE0MDIxNzExMjky
OFowHjEcMBoGA1UEAwwTdXNnMTUwXzEwN0JFRkQxMUI1MDCCASIwDQYJKoZIhvcN

```

Export Certificate Only Password: [masked] Export Certificate with Private Key

OK Cancel

Save **default** certificate as ***.crt** file to Android mobile phone computer.



Set Up the L2TP VPN Tunnel on the Android Mobile Device

- 1** To configure L2TP VPN in Android, go to Start > Settings > Network & Internet > VPN > Add a VPN Connection and configure as follows.
- 2** VPN Provider set to Windows (built-in).
- 3** Configure **Connection name** for you to identify the VPN configuration.
- 4** Set **Server** name or address to be the ZyWALL/USG's WAN IP address (172.124.163.150 in this example).
- 5** Select VPN type to Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec).
- 6** Enter **User name** and **Password** which the same as **Allowed User** created in ZyWALL/USG (L2TP_Remote_Users/zyx168 in this example).

Add a VPN connection

VPN provider

Windows (built-in) ▾

Connection name

ZyXEL_L2TP_VPN

Server name or address

172.124.163.150

VPN type

Layer 2 Tunneling Protocol with IPsec (L2TP/I ▾

Type of sign-in info

User name and password ▾

User name (optional)

L2TP_Remote_Users

Password (optional)

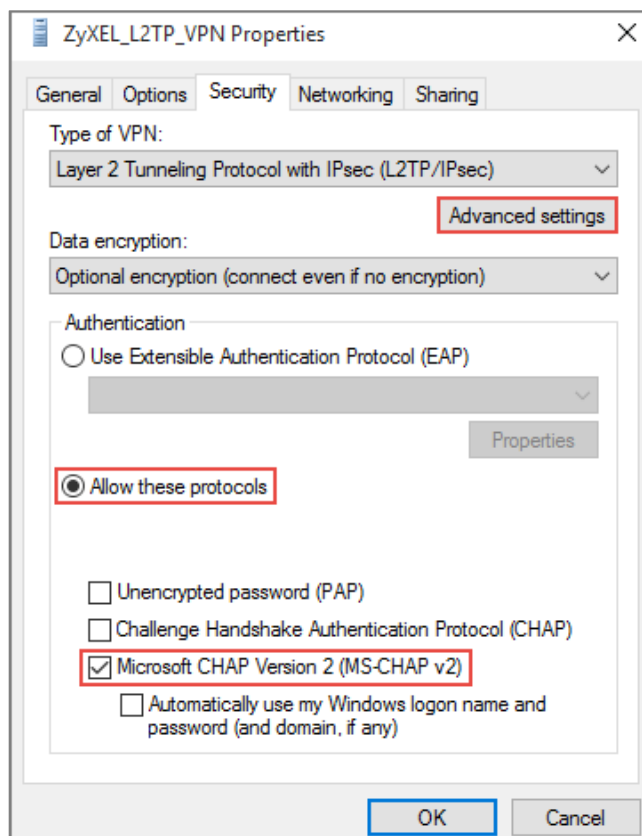
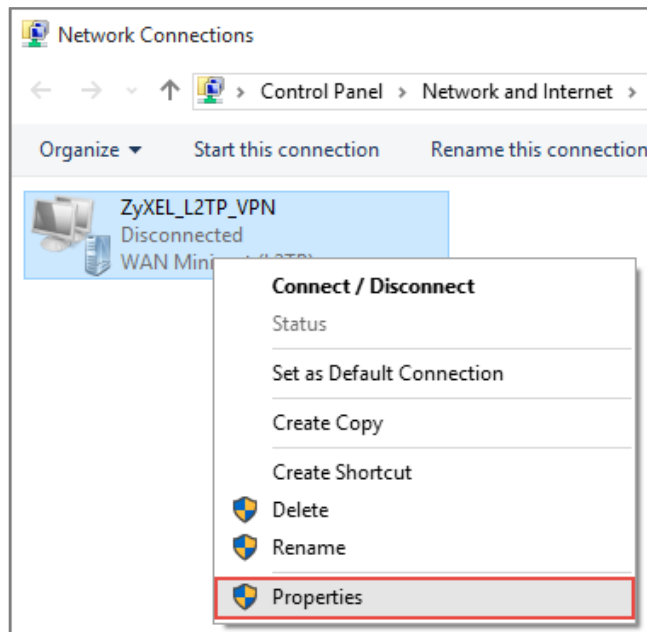
•••••

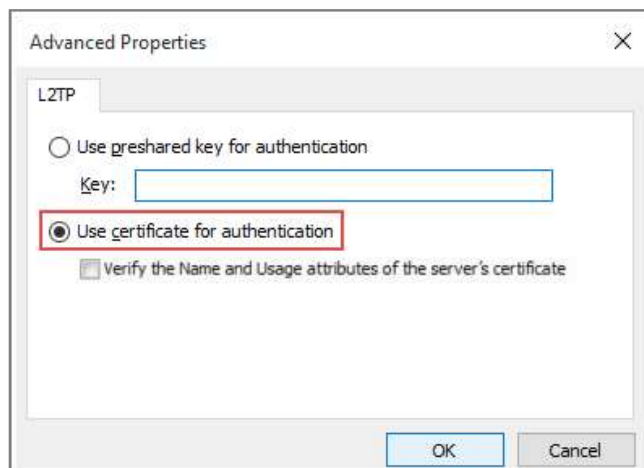
☒ Remember my sign-in info

Save

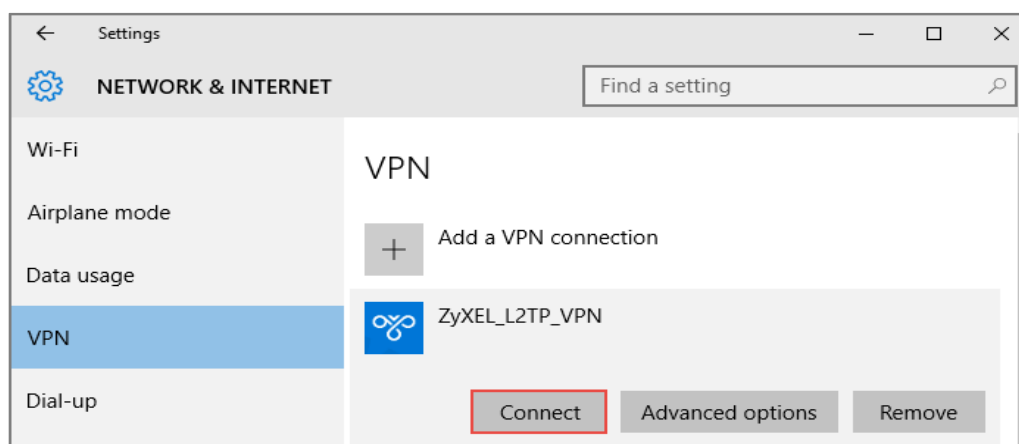
Cancel

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





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



Test the L2TP over IPSec VPN Tunnel

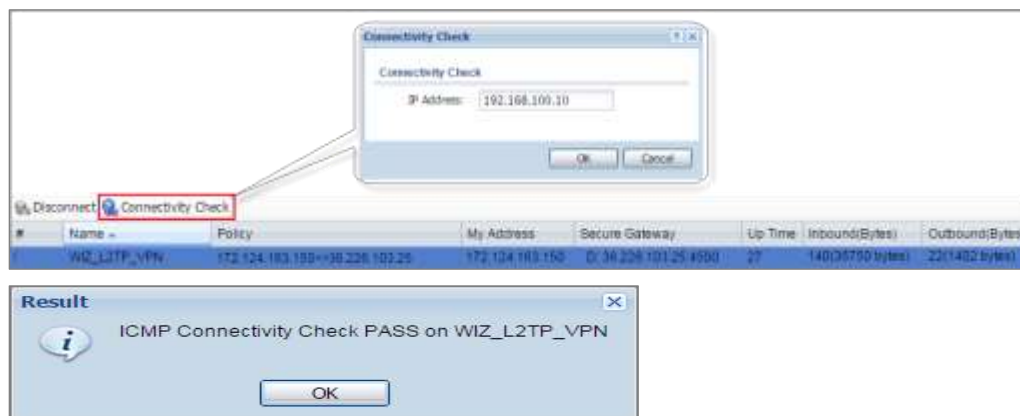
Go to ZyWALL/USG **CONFIGURATION > VPN > IPSec VPN > VPN Connection**, the **Status** connect icon is lit when the interface is connected.

CONFIGURATION > VPN > IPSec VPN > VPN Connection

IPv4 Configuration				
+ Add ✎ Edit 🗑 Remove 💡 Activate 🔇 Inactivate 🔗 Connect 🔌 Disconnect 📄 Object Reference				
#	Status	Name	VPN Gateway	Policy
1	💡	WIZ_L2TP_VPN	WIZ_L2TP_VPN	WIZ_L2TP_VPN_LOCAL/

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

Hub_HQ > MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



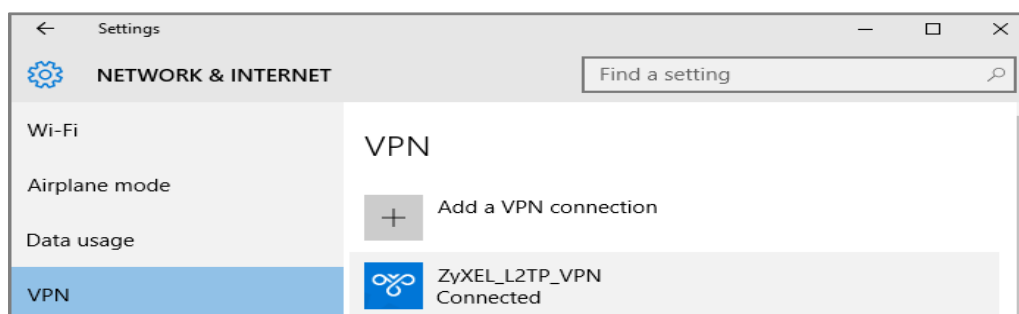
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

Current L2TP Session				
<div> Disconnect Refresh </div>				
#	User Name	Hostname	Assigned IP	Public IP
1	L2TP_Remote_Users	Windows_10	192.168.100.10	36.226.103.25

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

Menu > Settings > VPN > ZyXEL_L2TP



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	SP: 0x0 (0) SEQ: 0x0 (0) No rule found. Dropping TCP packet	IPSec
info	IKE	Send:[NOTIFY:INVALID_PAYLOAD_TYPE]	IKE_LOG
info	IKE	Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys	IKE_LOG
Priority	Category	Message	Note
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 1 Remote ID mismatch	IKE_LOG

- 9 If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.

Priority	Category	Message	Note
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch	IKE_LOG
Priority	Category	Message	Note
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [WIZ_L2TP_VPN] Phase 2 proposal mismatch	IKE_LOG

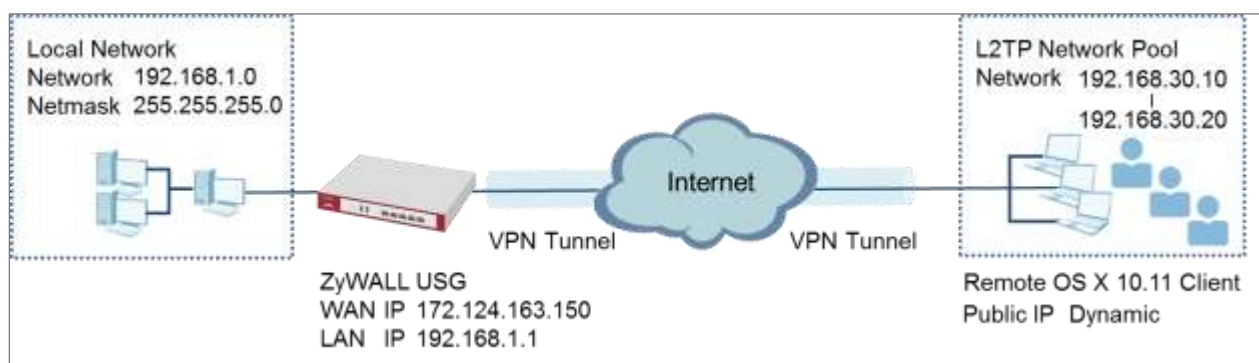
- 10 Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.
- 11 If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

- 12** Make sure the ZyWALL/USG units' security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- 13** Verify that the Zone is set correctly in the VPN Connection rule. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to Configure the L2TP VPN with Apple MAC OS X 10.11 Operating System

This is an example of using the L2TP VPN and VPN client software included in Apple MAC OS X 10.11 El Capitan operating systems. When the VPN tunnel is configured, users can securely access the network behind the ZyWALL/USG and allow traffic from L2TP clients to go to the Internet from an Apple computer.

ZyWALL/USG L2TP VPN with Apple MAC OS X 10.11 El Capitan



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

Set Up the L2TP VPN Tunnel on the ZyWALL/USG

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Welcome

☐ VPN Settings

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for Configuration Provisioning

- Wizard Type
- VPN Settings
- Wizard Completed

☒ VPN Settings for L2TP VPN Settings

- VPN Settings
- General Settings
- Wizard Completed

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

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

123

L2TP VPN Settings

Rule Name:

WIZ_L2TP_VPN

Phase 1 Setting

My Address (Interface):

ge1

Authentication Method

Pre-Shared Key:

xyz12345

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

Quick Setup > VPN Setup Wizard > Welcome > VPN Settings

VPN Setup Wizard

VPN Settings > General Settings > Wizard Completed

1

2

3

L2TP VPN Settings

IP Address Pool:

RANGE

Starting IP Address:

192.168.30.10

End IP Address:

192.168.30.20

First DNS Server (Optional):

Second DNS Server (Optional):

☒ Allow L2TP traffic Through WAN

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1

2

3

Express Settings

Summary

Rule Name:

WIZ_L2TP_VPN

Secure Gateway:

Any

Pre-Shared Key:

xyz12345

My Address (interface):

ge1

IP Address Pool:

RANGE, 192.168.30.10 - 192.168.30.20

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

L2TP VPN Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_L2TP_VPN2
My Address (interface):	ge1
Pre-Shared Key:	xyz12345
IP Address Pool:	RANGE, 192.168.30.10 - 192.168.30.20

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

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

L2TP VPN

Show Advanced Settings

Create new Object▼

User

Address

Reshooting

General Settings

Config Walkth

☒ 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

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_4 RANGE, 192.168.30.10-192.168.30.20

Authentication Method: default local

☒ Advance

Allowed User: any

Keep Alive Timer: 60 (1-180 seconds)

any

any

=== Object ===

Executive_1

Executive_2

Executive_3

ad-users

admin

ldap-users

radius-users

L2TP_Remote_Users

=== Group ===

Executive

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

To configure L2TP VPN in OS X 10.11 operation system, go to **System Preferences...**

> **Network**, click the "+" button at the bottom left of the connections to add a new connection and configure as follows.

Set the **Interface** to be **VPN**, select **VPN Type** to be **L2TP over IPSec**.

Configure **Service Name** for you to identify the VPN configuration. Click **Create**.

Select the interface and enter a name for the new service.

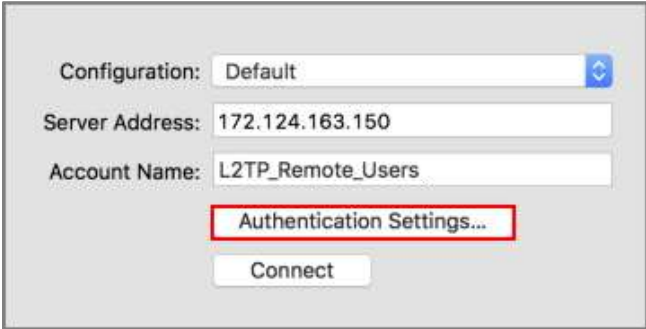
Interface: VPN

VPN Type: L2TP over IPSec

Service Name: ZyXEL_L2TP_VPN

Cancel 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....**

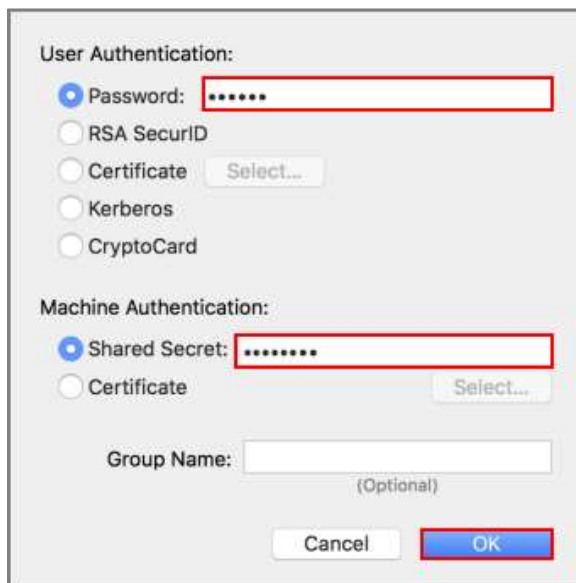


The screenshot shows a configuration window with the following fields and buttons:

- Configuration:** A dropdown menu set to "Default".
- Server Address:** A text field containing "172.124.163.150".
- Account Name:** A text field containing "L2TP_Remote_Users".
- Authentication Settings...:** A button highlighted with a red rectangle.
- Connect:** A button located below the "Authentication Settings..." button.

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

In the **Machine Authentication** section, enter **Shared Secret** to be the pre-shared key of the IPSec VPN gateway the ZyWALL/USG uses for L2TP VPN over IPSec (zyx12345 in this example). Click **OK**.



User Authentication:

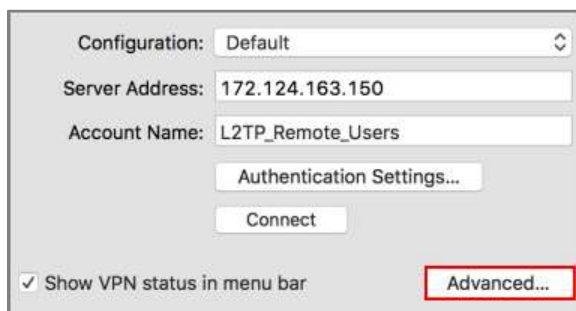
- ☒ Password:
- ☐ RSA SecurID
- ☐ Certificate
- ☐ Kerberos
- ☐ CryptoCard

Machine Authentication:

- ☒ Shared Secret:
- ☐ Certificate

Group Name:
(Optional)

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

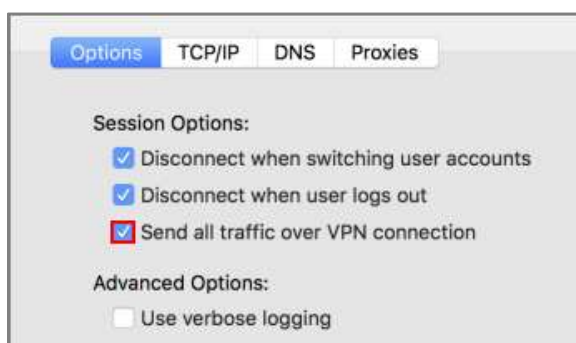


Configuration:

Server Address:

Account Name:

☒ Show VPN status in menu bar



Options TCP/IP DNS Proxies

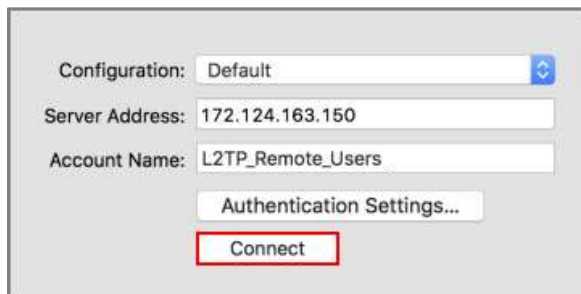
Session Options:

- ☒ Disconnect when switching user accounts
- ☒ Disconnect when user logs out
- ☒ Send all traffic over VPN connection

Advanced Options:

- ☐ Use verbose logging

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



Configuration: Default

Server Address: 172.124.163.150

Account Name: L2TP_Remote_Users

Authentication Settings...

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



#	Status	Home	VPN Gateway	Policy
1		VPN_to_VPC	VPN_to_VPC	VPN_to_VPC_LOCAL/VPN_to_V...
2		VPN_to_Azure	VPN_to_Azure	VPN_to_Azure_LOCAL/VPN_to_...
3		Hub_HQ_to_Branch_A	Hub_HQ_to_Branch_A	VPN_to_VPC_LOCAL/Spoke_Bra...
4		Hub_HQ_to_Branch_B	Hub_HQ_to_Branch_B	Hub_HQ/Spoke_Branch_B_LOCAL
5		Spoke_Branch_A	Spoke_Branch_A	Spoke_Branch_A_LOCAL/Hub_HQ
6		Spoke_Branch_B	Spoke_Branch_B	Spoke_Branch_B_LOCAL/Hub_HQ
7		WIZ_VPN_Branch	WIZ_VPN_Branch	WE_VPN_Branch_LOCAL/WE_V...
8		WIZ_L2TP_VPN	WIZ_L2TP_VPN	WE_L2TP_VPN_LOCAL/

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

MONITOR > VPN Monitor > IPSec > WIZ_L2TP_VPN



功能有問題無法截圖, connectivity check fail

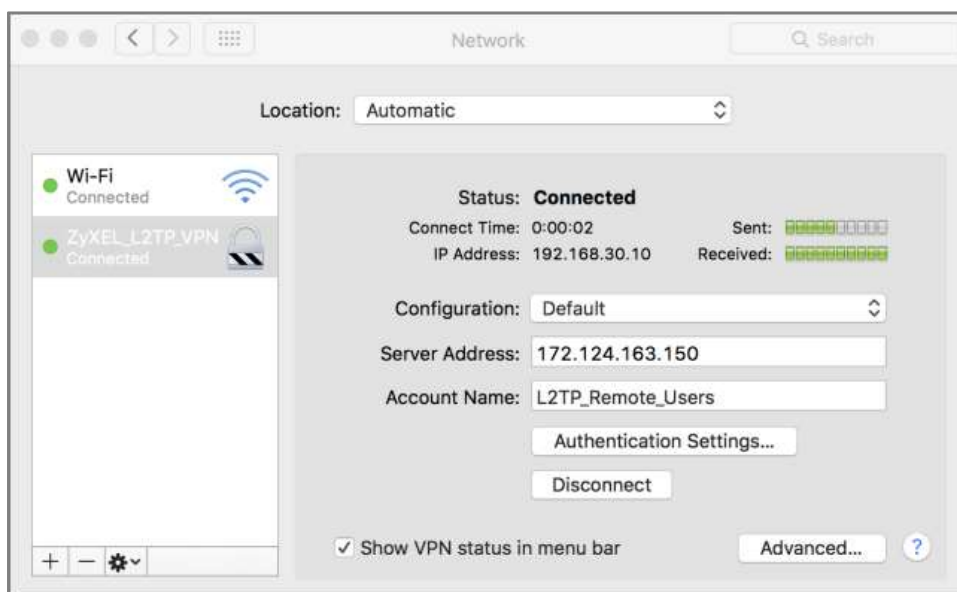
Go to ZyWALL/USG **MONITOR > VPN Monitor > L2TP over IPSec** and verify the **Current L2TP Session**.

MONITOR > VPN Monitor > L2TP over IPSec > L2TP_Remote_Users

Current L2TP Session				
<div> Disconnect Refresh </div>				
#	User Name	Hostname	Assigned IP	Public IP
1	L2TP_Remote_Users	Apple_MAC_OS_X	192.168.30.10	36.226.103.25

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

System Preferences... > Network



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	2017-06-15 10:10:10	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. 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	\$end:[NOTIFY:INVALID_PAYLOAD_TYPE]	IKE_LOG
info	IKE	Invalid payload type in encrypted payload chain, possibly because of different pre-shared keys	IKE_LOG

Priority	Category	Message	Note
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 1 Peer ID mismatch	IKE_LOG

If you see that Phase 1 IKE SA process has completed but still get [info] log message as below, please check ZyWALL/USG Phase 2 Settings. ZyWALL/USG unit must set correct **Local Policy** to establish the IKE SA.

Priority	Category	Message	Note
Info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
Info	IKE	[SA] : No proposal chosen	IKE_LOG
Info	IKE	[ID] : Tunnel [WIZ_L2TP_VPN] Phase 2 Local policy mismatch	IKE_LOG
Info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
Info	IKE	Phase 1 IKE SA process done	IKE_LOG

Priority	Category	Message	Note
Info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
Info	IKE	[SA] : No proposal chosen	IKE_LOG
Info	IKE	[SA] : Tunnel [WIZ_L2TP_VPN] Phase 2 proposal mismatch	IKE_LOG
Info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
Info	IKE	Phase 1 IKE SA process done	IKE_LOG

Ensure that the L2TP Address Pool does not conflict with any existing LAN1, LAN2, DMZ, or WLAN zones, even if they are not in use.

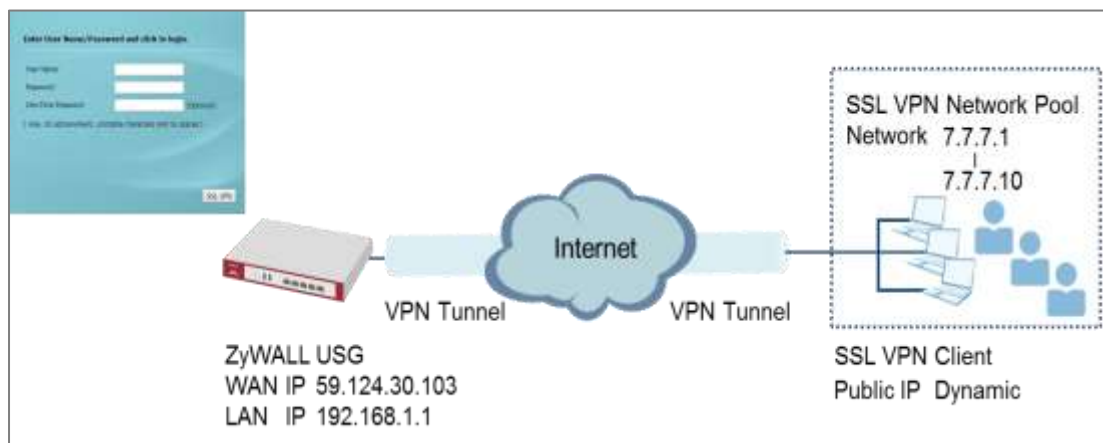
If you cannot access devices in the local network, verify that the devices in the local network set the USG's IP as their default gateway to utilize the L2TP tunnel.

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

Verify that the Zone is set correctly in the Zone object. This should be set to IPSec_VPN Zone so that security policies are applied properly.

How to configure if I want user can only see SSL VPN Login button in web portal login page

This example shows how to strict portal access for SSL VPN clients. The example instructs how to allow end users to only see the SSL VPN Login button in the web portal login screen and the administrator can only manage the device from LAN.



ZyWALL/USG only see SSL VPN Login button in web portal login page



Note:

All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG60 (Firmware Version: ZLD 4.25).

Set Up the DNS Service

In this scenario, you need to have a DNS host to fulfill the requirement. In this example, go to <https://www.noip.com/> to register an account and create a DNS host. The following mapping IP address is the public IP of the ZyWALL/USG's WAN IP address.

Set Up the ZyWALL/USG SSL VPN Setting

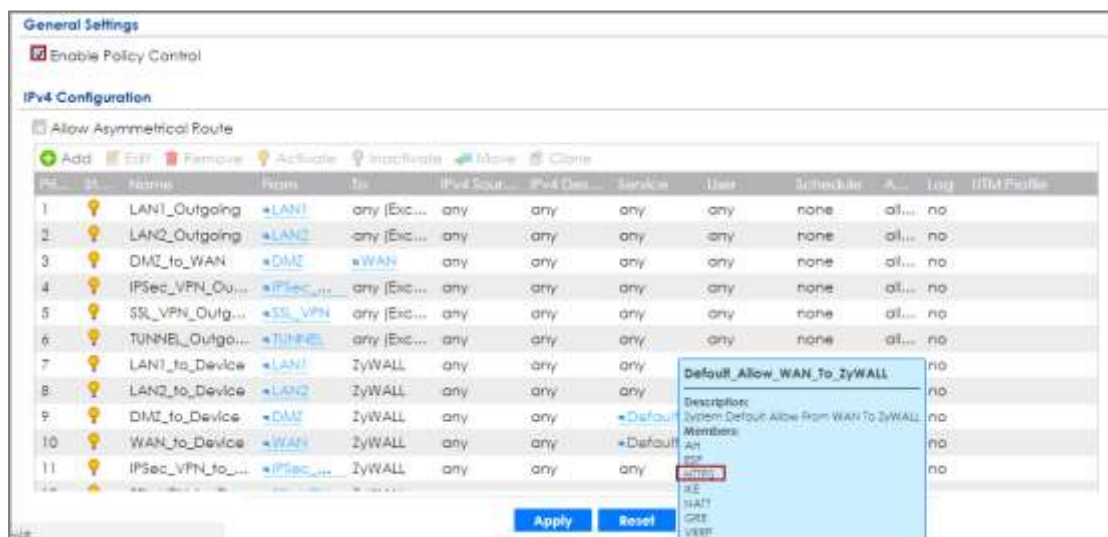
In the ZyWALL/USG, go to **CONFIGURATION > VPN > SSL VPN > Global Setting > SSL VPN Login Domain Name** and type in the DNS domain name.

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

Global Settings	
Network Extension Local IP:	<input type="text" value="192.168.200.1"/>
SSL VPN Login Domain Name	
SSL VPN Login Domain Name 1	<input type="text" value="zyxetestssl.ddns.net"/> (Optional)
SSL VPN Login Domain Name 2	<input type="text"/> (Optional)
Message	
Login Message:	<input type="text" value="Welcome to SSL VPN"/>
Logout Message:	<input type="text" value="Goodbye to SSL VPN"/>

Use SSL VPN, you need to allow users to access the **HTTPS** service. Go to **CONFIGURATION > Security Policy > Policy Control**. Make sure the security policy allows **HTTPS** traffic from the **WAN** interface to the **ZyWALL** (the example shows the default settings).

CONFIGURATION > Security Policy > Policy Control

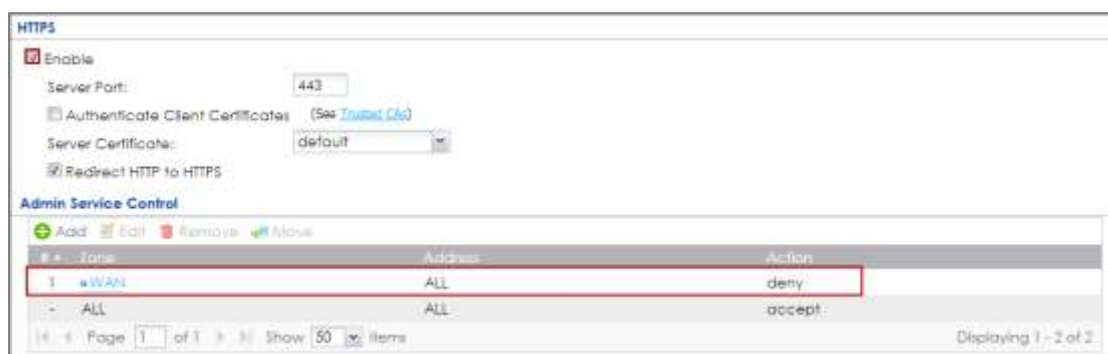
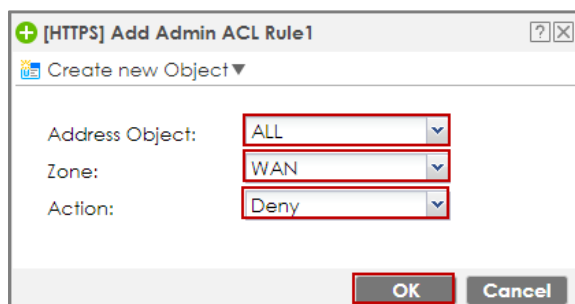


Set Up the ZyWALL/USG System Setting

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**.

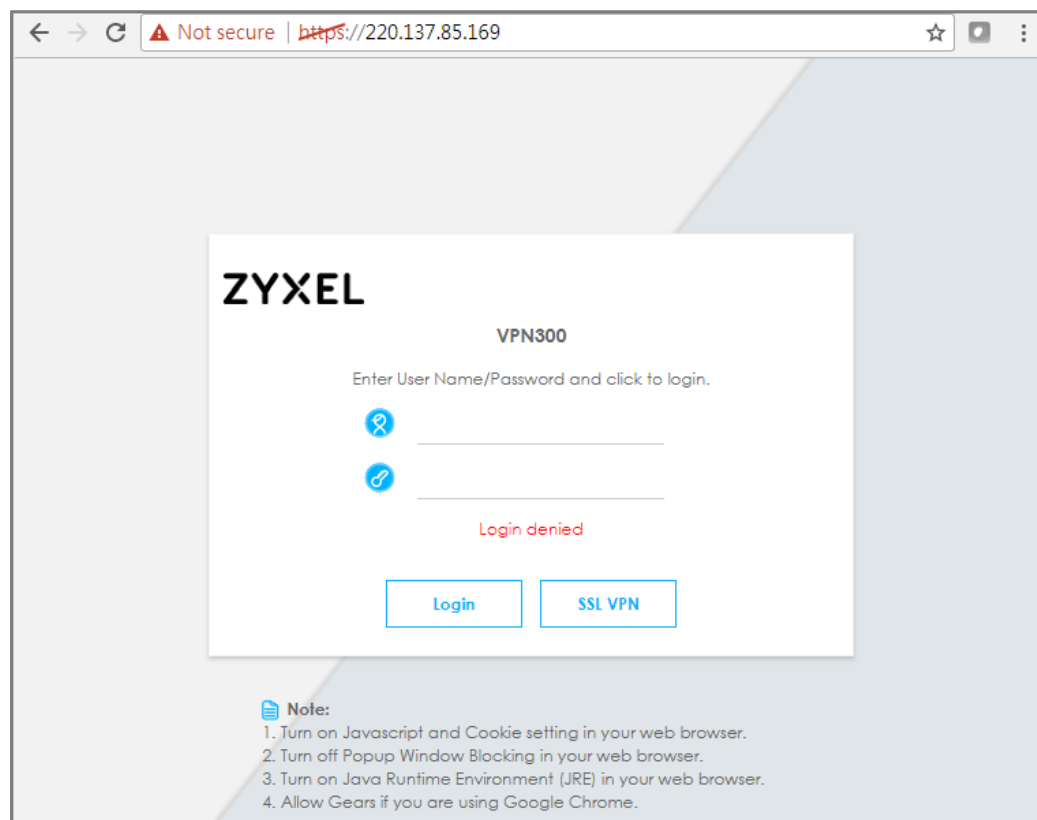
CONFIGURATION > System > WWW > Admin Service Control > Add Admin ACL Rule 1



Test the SSL VPN

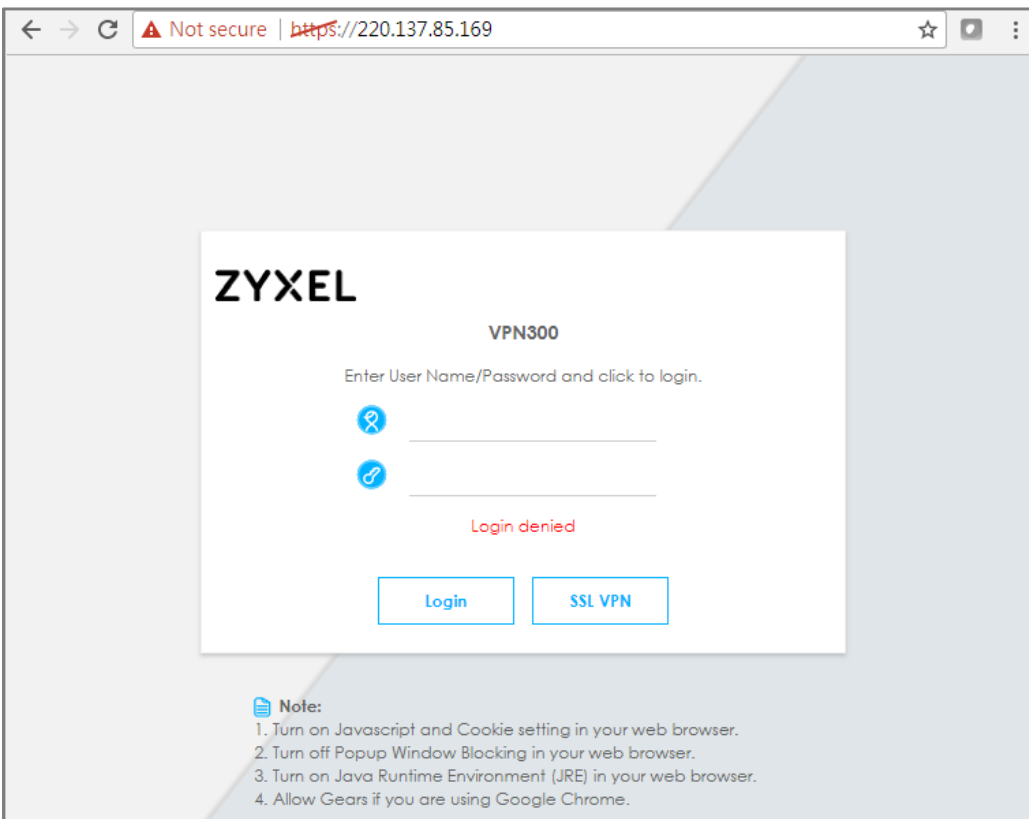
Type in the URL (<https://sslvpnzyxeltest.ddns.net>) and you will only see the **SSL VPN Login** button in the web portal screen.

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





← → ↻ ⚠ Not secure | <https://220.137.85.169> ☆ 📺 ⋮

ZYXEL

VPN300

Enter User Name/Password and click to login.





Login denied

LoginSSL VPN

Note:

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

Login to the device via the LAN interface with the administrator's user name and password. The management portal will be displayed.

Login to the device via the LAN interface

ZYXEL VPN300

Enter User Name/Password and click to login.

User Name:

Password:

Notice:

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

ZYXEL VPN300

Logout Help About Site Map Object Reference CLI

General VPN

System Status

- CPU Usage: 12%
- Memory Usage: 21%
- Flash Usage: 19%
- USB Storage Usage: 0/0 MB
- Active Session: 61/2000000
- DHCP Table: 2 Host(s)
- Device RA: 000 Switch Counter

Virtual Device

ZYXEL VPN300

Device Information

System Name	VPN300	Boot Status	OK
Serial Number	S172L15290016	Firmware Version	V4.30(A8FC.0)b1s1 / 2017-06-09 21:43:11
MAC Address Range	BB:EC:A3:A9:C0:08 - BB:EC:A3:A9:C0:12	Firmware Upgrade License	Not Licensed
System Uptime	02:57:33	Current Date/Time	2017-07-07 / 06:23:43 UTC+00:00

Tx/Rx Statics Port Selection: P1

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

MONITOR > Log

Log

Category:

Email Log Now

Refresh

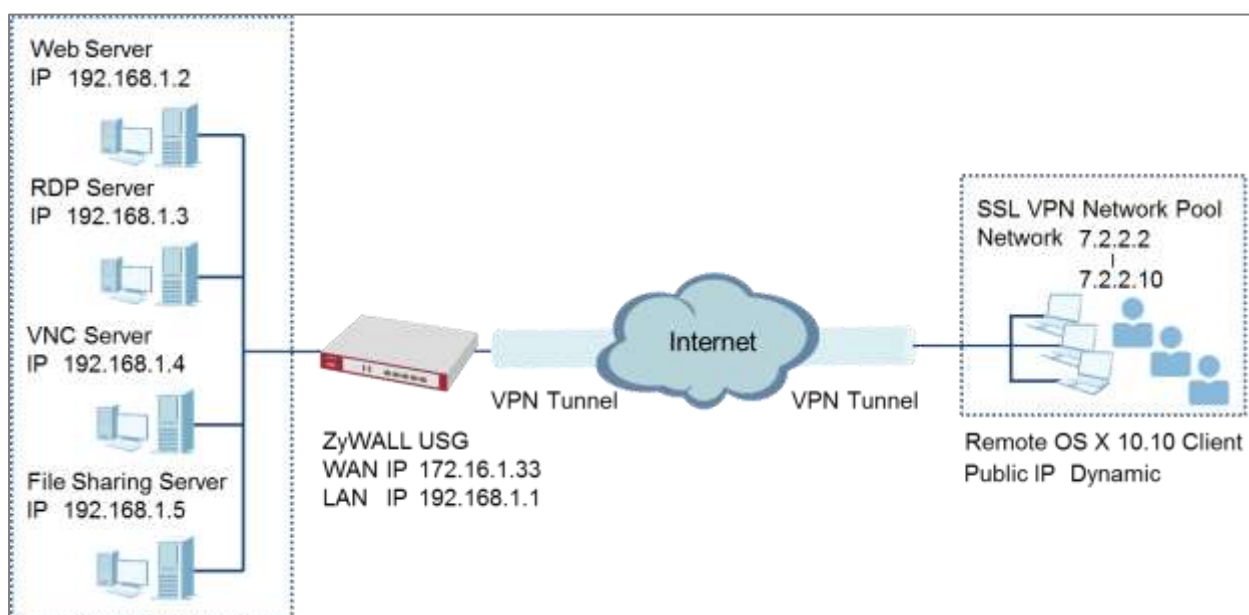
Clear Log


Priority	Category	Message	Source	Destination	Note
notice	User	Administrator admin(MAC=00:16:36:2B:B4:2F) from http/https has logged out Device	192.168.1.34	192.168.1.1	Account: admin
notice	User	Administrator admin(MAC=00:16:36:2B:B4:2F) from http/https has logged in Device	192.168.1.34	192.168.1.1	Account: admin
notice	User	User admin has been denied access from HTTPS	10.214.30.55:5...	10.214.30.90:443	Account: admin

How to Deploy SSL VPN with Apple Mac OS X 10.10 Operating System

This is an example of using the ZyWALL/USG SSL VPN client software in Apple MAC OS X 10.10 Yosemite operating systems for secure connections to the network behind the ZyWALL/USG. When the VPN tunnel is configured, users can securely access the network from a Mac OS X 10.11 Yosemite computer.

ZyWALL/USG SSL VPN with Apple MAC OS X 10.10 Yosemite



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

Set Up the SSL VPN Tunnel on the ZyWALL/USG

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

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

Configuration

☒ Enable Policy

Name:

Zone: ⓘ

Description: (Optional)

Go to **Create new Object > User** to add **User Name** (SSL_VPN_1_Users in this example) and **Password** (4-24 characters, zyx168 in this example), click **OK**.

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

+ Add Access Policy

Create new Object ▼

- User
- Application
- Address

Name:

Zone: ⓘ

Description: (Optional)

+ Add A User

User Configuration

User Name :

User Type:

Password:

Retype:

Description:

OK **Cancel**

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

User/Group

Selectable User/Group Objects

billing-users
 ua-users
 trial-users
 L2TP_Remote_Users
SSL_VPN_1_Users

Selected User/Group Objects

Selectable Application Objects

Internal_Server
 RDP
 VNC
File_Share

Selected Application Objects

Scroll down to **Network Extension (Optional)** to select **Enable Network Extension** to allow SSL VPN users to access the resources behind the ZyWALL/USG local network.

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

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

Network Extension (Optional)

☒ Enable Network Extension (Full Tunnel Mode)

☐ Force all client traffic to enter SSL VPN tunnel ⓘ

☐ NetBIOS broadcast over SSL VPN Tunnel

Assign IP Pool: SSL_VPN_POOL ⓘ RANGE 7.2.2.2-7.2.2.10

DNS Server 1: none

DNS Server 2: none

WINS Server 1: none

WINS Server 2: none

Network List

Selectable Address Objects

DMZ_SUBNET
IP6to4-Relay
LAN1_SUBNET
LAN2_SUBNET
RFC1918_1

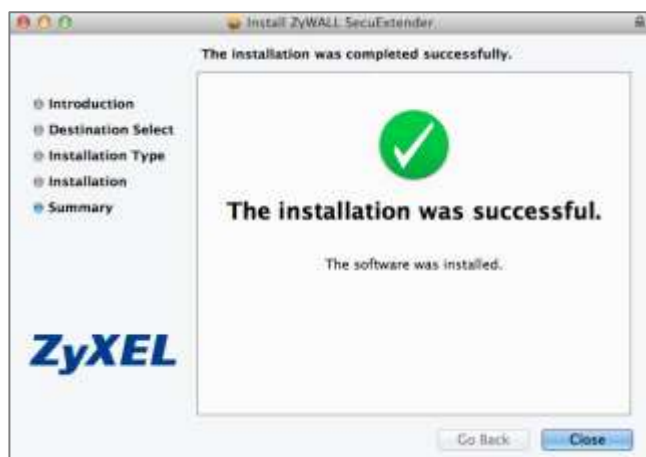
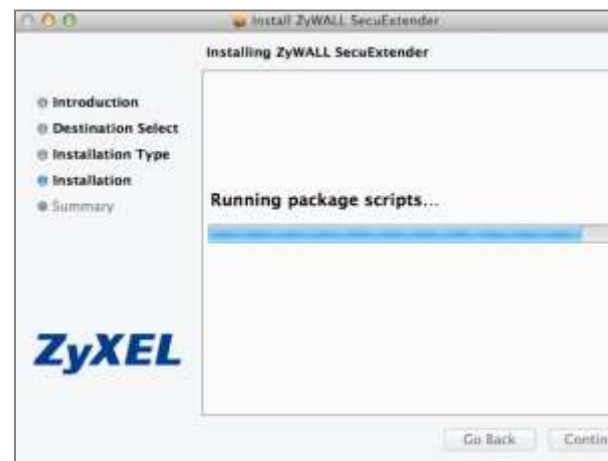
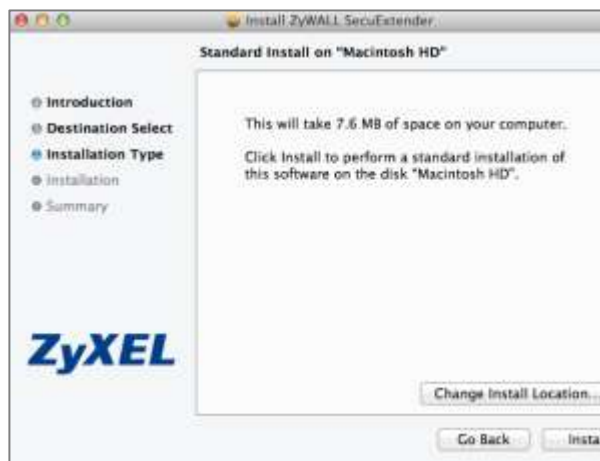
+
-

Selected Address Objects

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**.



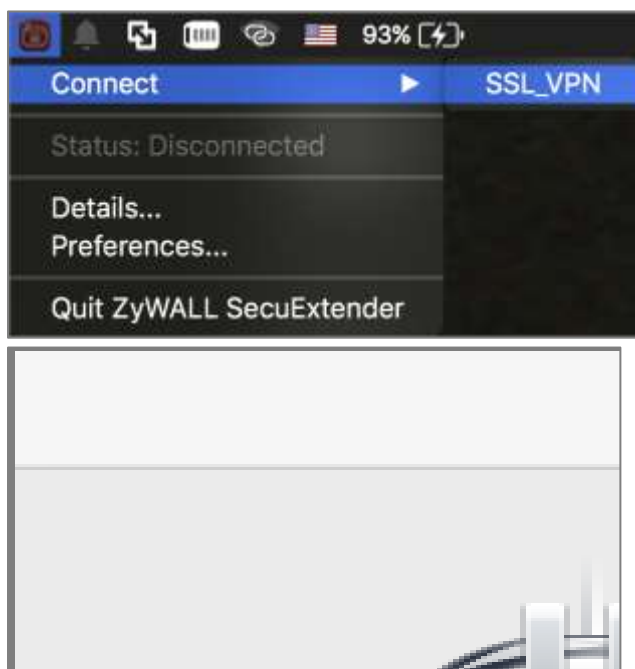
Here are two methods to initiate SSL VPN connections:

From ZyWALL SecuExtender

From a Web Browser

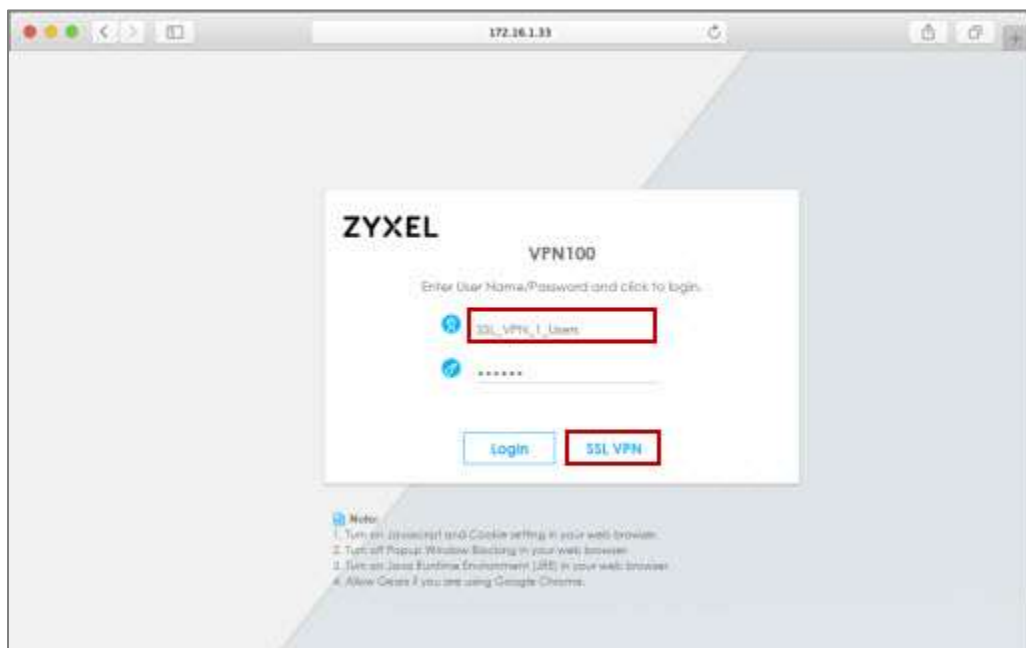
From ZyWALL SecuExtender

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

Current SSL VPN Connection						
Disconnect Refresh						
#	User	Access	Login Address	Connected Time	Inbound(Bytes)	Outbound(Bytes)
1	SSL_VPN_1_Users	Network-Extension	10.214.30.104	00:01:39	9390	503

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

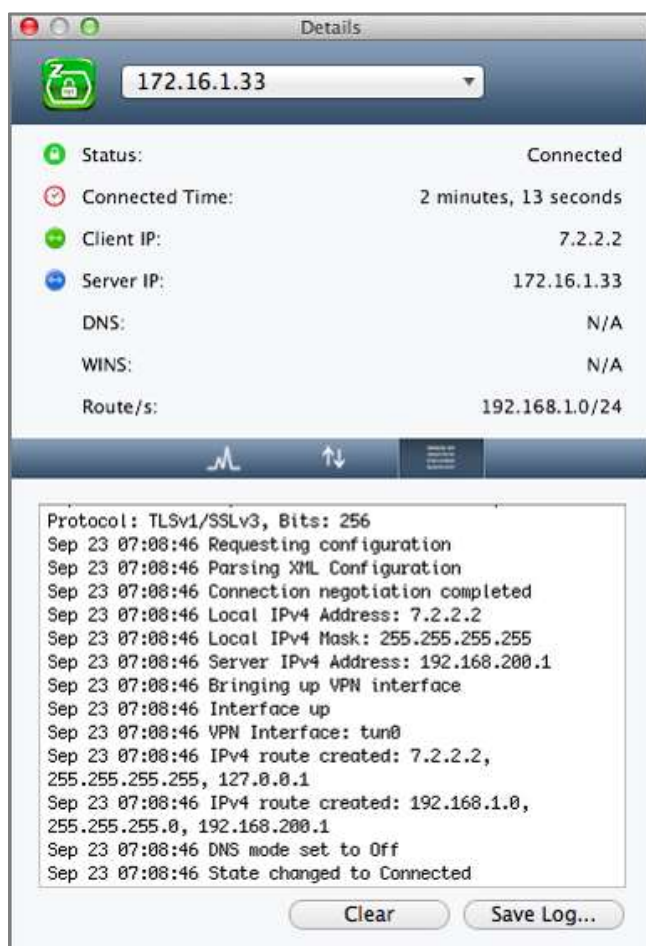
ZyWALL SecuExtender > Details > Traffic Graph



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.

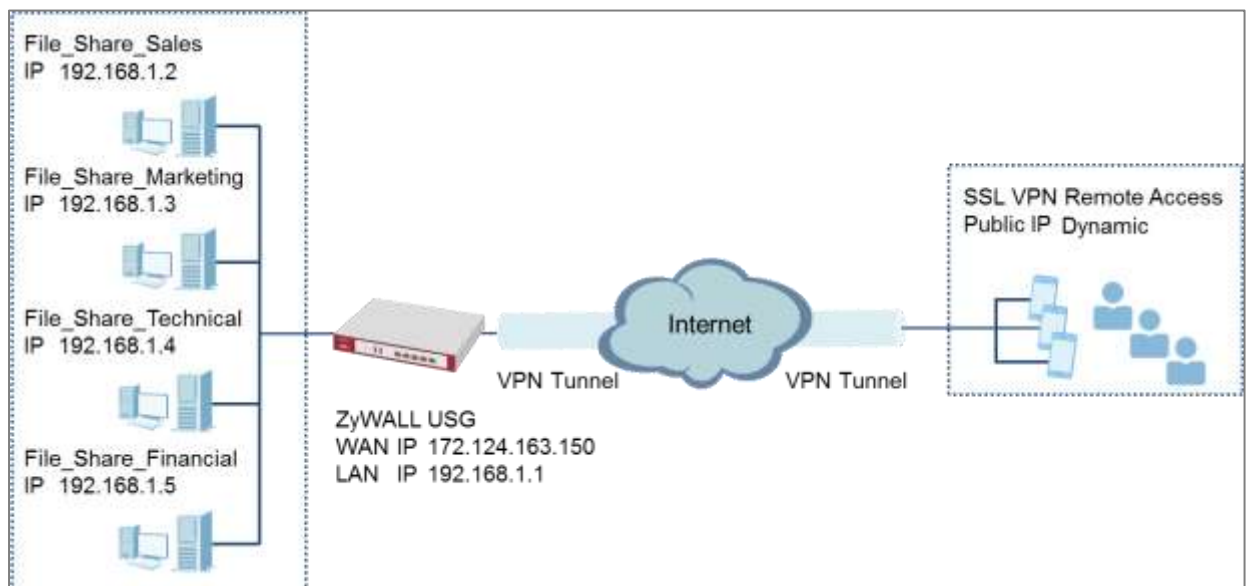
If the ZyWALL/USG redirects the user to the user aware screen, check whether the user account is included in an SSL VPN access policy or not.


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

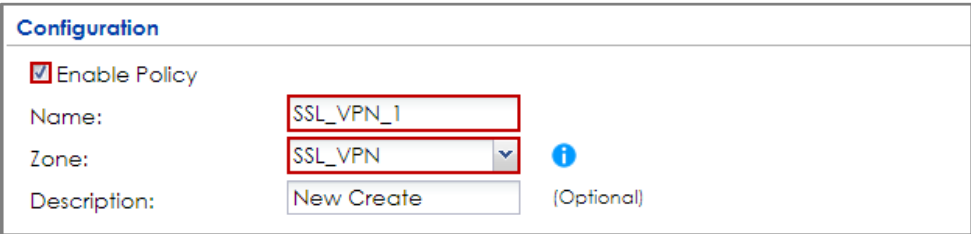


 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG1900 (Firmware Version: ZLD 4.25).

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



Configuration

☒ Enable Policy

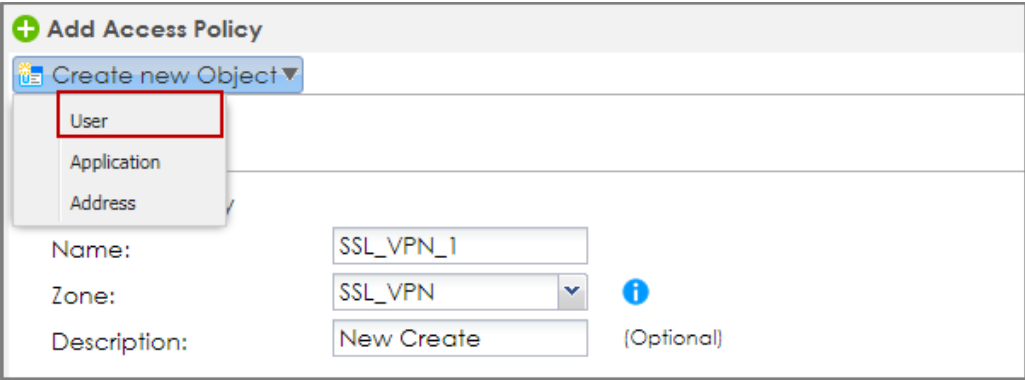
Name:

Zone: ⓘ

Description: (Optional)

Go to **Create new Object > User** to add **User Name** (SSL_VPN_1_Users in this example) and **Password** (4-24 characters, zyx168 in this example), click **OK**.

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



+ Add Access Policy

▼

- User
- Application
- Address

Name:

Zone: ⓘ

Description: (Optional)



+ Add A User

User Configuration

User Name :

User Type: ▼

Password:

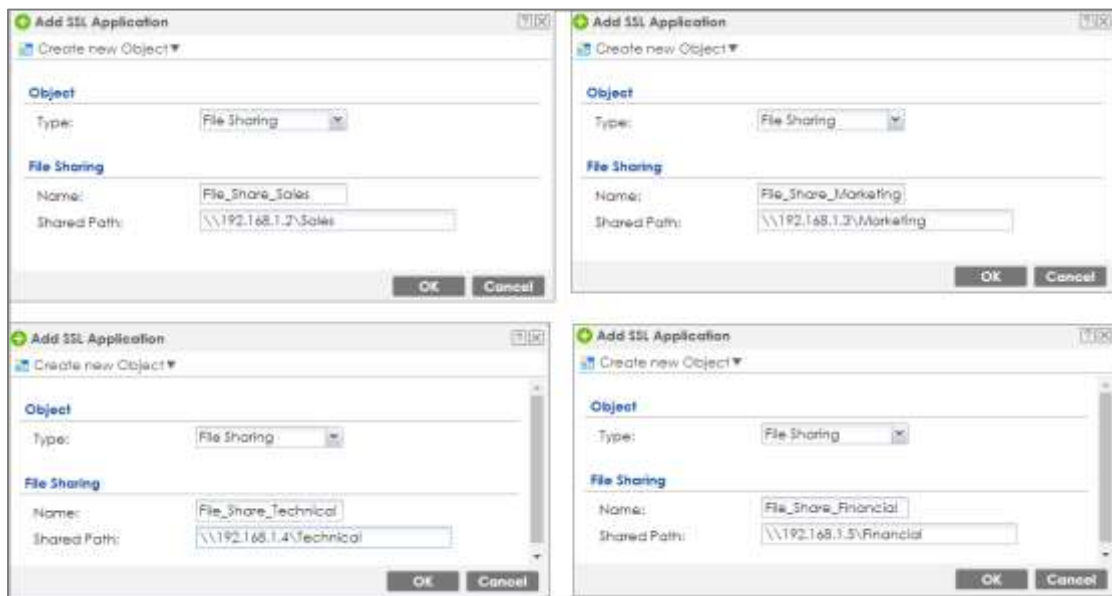
Retype:

Description:

OK Cancel

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

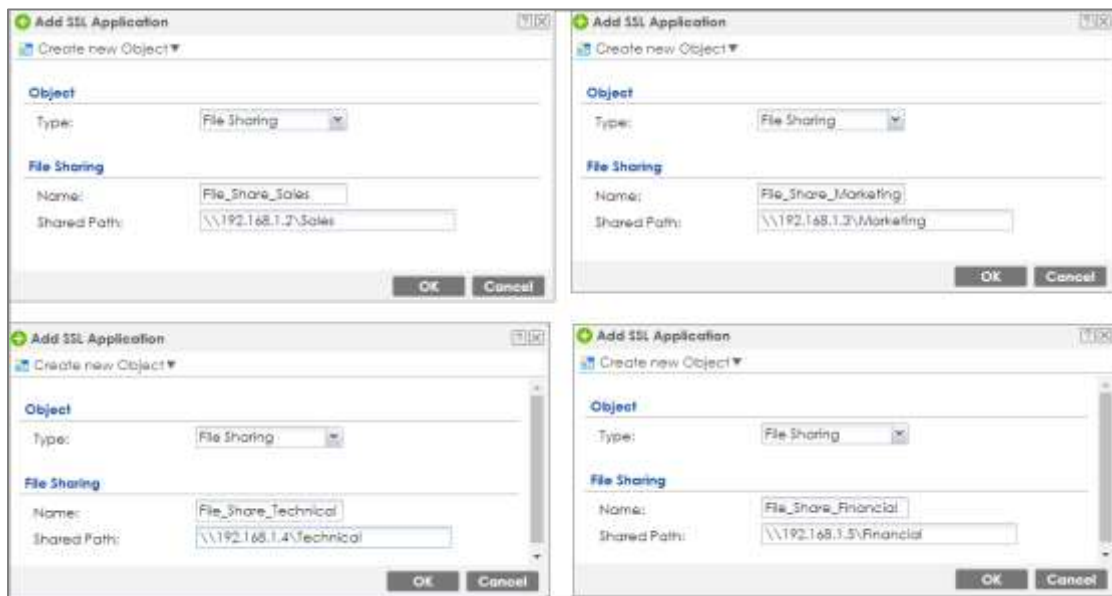
CONFIGURATION > VPN > SSL VPN > Access Privilege > Access Policy > Create new Object > Application



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

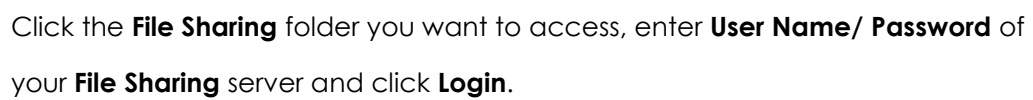



Test the SSL VPN Tunnel

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**.





File Sharing

Enter User Name/Password and click to login.

User Name:

Password:

(max. 31 alphanumeric, printable characters and no spaces)

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.

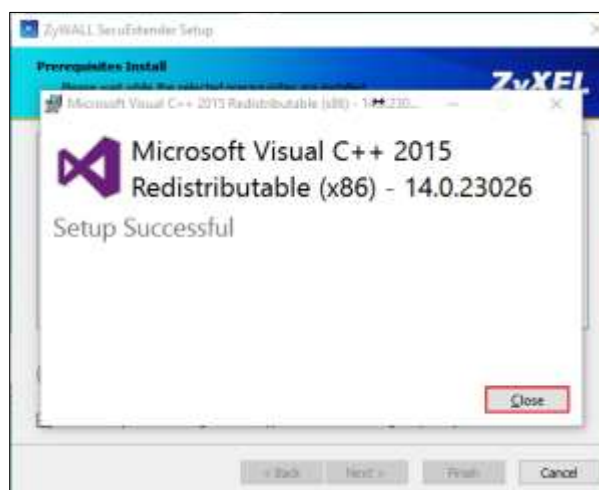
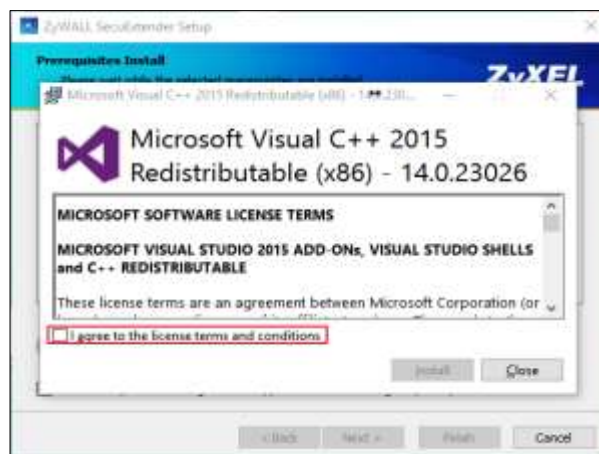
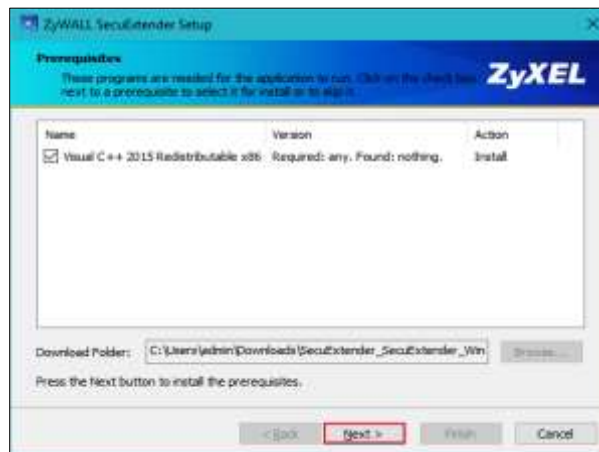
How to Configure an SSL VPN Tunnel (with SecuExtender version 4.0.0.1) on the Windows 10 Operating System

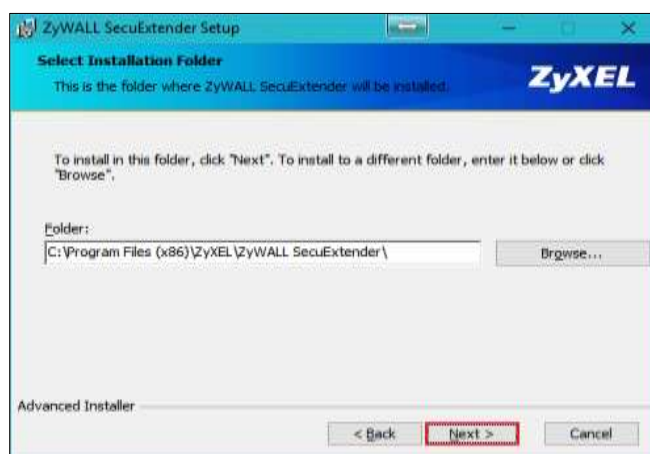
Set up the SSL VPN Tunnel with Windows 10

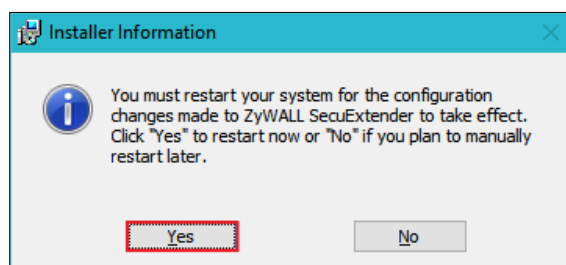
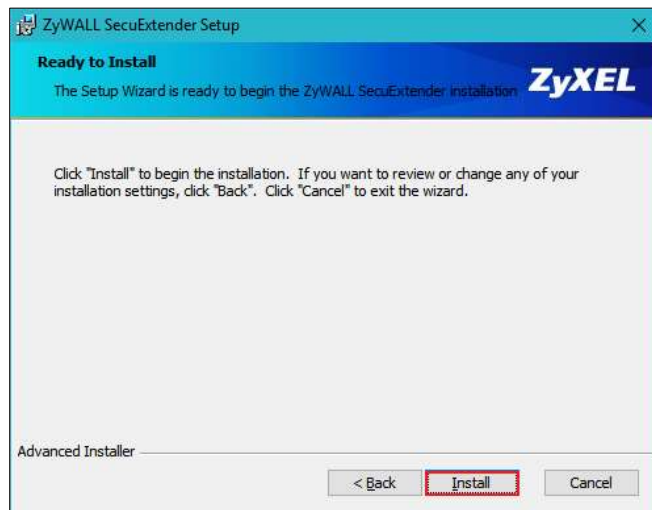
Please download SecuExtender version 4.0.0.1 from the download library of ZyXEL's official website.

Model	Material	Version	OS	Checksum	Release Date	Release Note	Download
ZyWALL IPSec VPN Client	Software	ZyWALLIPSecVPNClient3.7204.011	Windows 7 32bit/ Windows 7 64bit/ Windows 8 32bit/ Windows 8 64bit/ Windows 10 32bit/ Windows 10 64bit		May 24, 2017		
SecuExtender	Software	SecuExtender_MacOS3.11.5	Mac OS X/ Mac OS 10.6/ Mac OS 10.9/ Mac OS 10.10		Mar 15, 2017		
SecuExtender	Software	SecuExtender_Windows4.0.0.1	Windows XP/ Windows 7 32bit/ Windows 7 64bit/ Windows 8 32bit/ Windows 8 64bit/ Windows 10 32bit/ Windows 10 64bit		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.







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.

Current User List						
#	User ID	Reauth/Lease Time	Type	IP Address	MAC	User Info
1	SSL_user1	23:59:17 / 23:59:47	SSLVPN	10.251.30.56/7.7.7.1	3C:97:0E:30:0E:88	user(SSL_user1)

What Can Go Wrong?

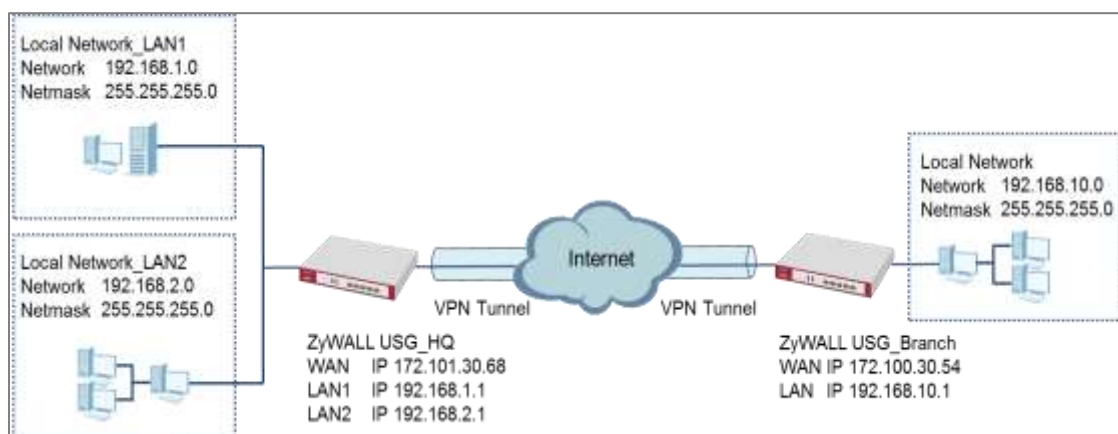
- 1 If you see a [notice] or [alert] log message such as shown below, please check the ZyWALL/USG SSL's **Selected User/Group Objects** settings. Windows 10 users must use the same **Username** and **Password** as configured in the ZyWALL/USG to establish the SSL VPN tunnel.

Priority	Category	Message	Note
notice	SSL VPN	Failed login attempt to SSLVPN from http/https (incorrect password or inexistent username)	Account: SSL_VPN_1_Users
alert	User	Failed login attempt to Device from http/https (incorrect password or inexistent username)	Account: SSL_VPN_1_Users


- 2 If you have uploaded a logo to show on the SSL VPN user screens but it does not display properly, check if the logo graphic is in GIF, JPG, or PNG format. The graphic should use a resolution of 103 x 29 pixels to avoid distortion when displayed. The ZyWALL/USG automatically resizes a graphic of a different resolution to 103 x 29 pixels. The file size must be 100 kilobytes or less. Transparent background is recommended.
- 3 If users can log into the SSL VPN but cannot see some of the resource links, check the SSL application object's configurations.
- 4 If the ZyWALL/USG redirects the user to the user aware screen, check whether the user account is included in an SSL VPN access policy or not.
- 5 If you have changed the HTTP/HTTPS configuration, the SSL VPN network extension sessions will be disconnected. The sessions need to be reconnected if this happens.

How to redirect multiple LAN interface traffic to the VPN tunnel

This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with multiple LAN access to the VPN tunnel. The example instructs how to configure the VPN tunnel between each site and redirect multiple LAN interface traffic to the VPN tunnel. When the VPN tunnel is configured, multiple LAN subnets can be accessed securely.



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

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

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

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

Quick Setup > VPN Setup Wizard > Welcome

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Welcome

☒ VPN Settings

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for Configuration Provisioning

- Wizard Type
- VPN Settings
- Wizard Completed

☐ VPN Settings for L2TP VPN Settings

- VPN Settings
- General Settings
- Wizard Completed

Upon completion of the Wizard Setup

i. VPN Tunnel and VPN Gateway are automatically configured/generated

ii. Policy Route is automatically configured/generated

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

☒ Express

☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1

☐ IKEv2

Scenario

Rule Name:

☒ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

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

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

1 2 3

Express Settings

Configuration

Secure Gateway: (IP or FQDN)

Pre-Shared Key:

Local Policy (IP/Mask): /

Remote Policy (IP/Mask): /

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings
Summary
Rule Name: WIZ_VPN_HQ
Secure Gateway: 10.214.30.77
Pre-Shared Key: zyxel123
Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

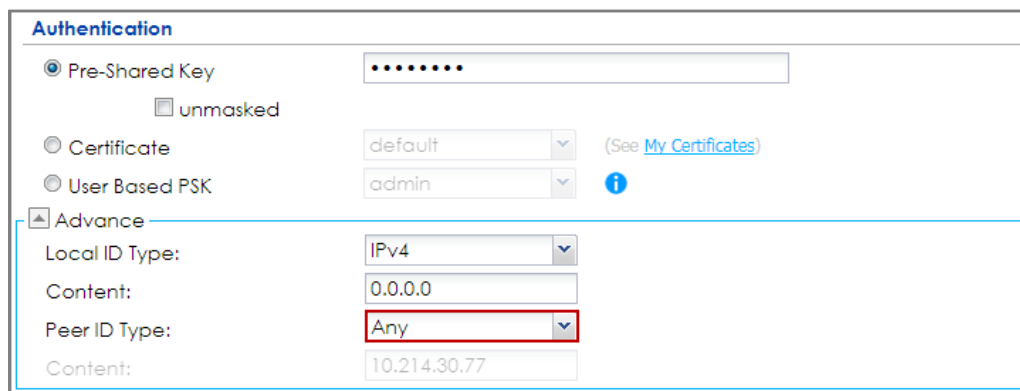
123

Express Settings
Congratulations. The VPN Access wizard is completed
Summary
Rule Name: WIZ_VPN_HQ
Secure Gateway: 10.214.30.77
Pre-Shared Key: zyxel123
Local Policy (IP/Mask): 192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway** and click **Show Advanced Settings**. Configure **Authentication > Peer ID Type** as **Any** to let the

ZyWALL/USG does not require to check the identity content of the remote IPSec router.

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



Authentication

☒ Pre-Shared Key
☐ unmasked

☐ Certificate (See [My Certificates](#))

☐ User Based PSK [i](#)

☒ Advance

Local ID Type:

Content:

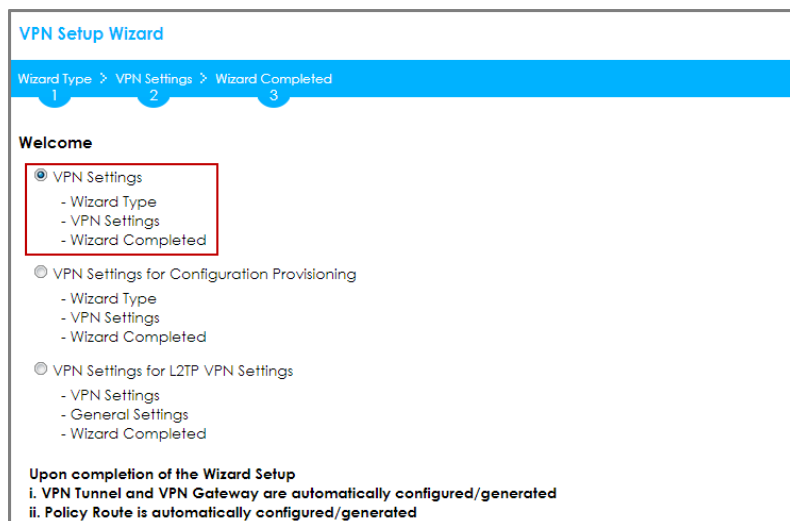
Peer ID Type: (highlighted with a red box)

Content:

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

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

Quick Setup > VPN Setup Wizard > Welcome



VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed
1 2 3

Welcome

☒ VPN Settings
- Wizard Type
- VPN Settings
- Wizard Completed

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

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

Upon completion of the Wizard Setup
i. VPN Tunnel and VPN Gateway are automatically configured/generated
ii. Policy Route is automatically configured/generated

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

Quick Setup > VPN Setup Wizard > Wizard Type

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

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

Type of VPN policy

☒ Express
 ☐ Advanced

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

1 2 3

Express Settings

IKE Version

☒ IKEv1
 ☐ IKEv2

Scenario

Rule Name:

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

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

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

Configuration

Secure Gateway: 10.214.30.106 (IP or FQDN)

Pre-Shared Key: zyxel123

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > **VPN Settings** > Wizard Completed

123

Express Settings

Summary

Rule Name: WIZ_VPN_Branch

Secure Gateway: 10.214.30.106

Pre-Shared Key: zyxel123

Local Policy (IP/Mask): 192.168.10.0 / 255.255.255.0

Remote Policy (IP/Mask): 192.168.1.0 / 255.255.255.0

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

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

VPN Setup Wizard

Wizard Type > VPN Settings > Wizard Completed

123

Express Settings

Congratulations. The VPN Access wizard is completed

Summary

Rule Name:	WIZ_VPN_Branch
Secure Gateway:	10.214.30.106
Pre-Shared Key:	zyxel123
Local Policy (IP/Mask):	192.168.10.0 / 255.255.255.0
Remote Policy (IP/Mask):	192.168.1.0 / 255.255.255.0

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

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

Authentication

☒ Pre-Shared Key

.....

☐ unmasked

☐ Certificate

default
(See [My Certificates](#))

☐ User Based PSK

admin

☒ Advance

Local ID Type:
IPv4
Content:
0.0.0.0
Peer ID Type:
Any
Content:
10.214.30.77

Set up the Policy Route (ZyWALL/USG_HQ)

Go to ZyWALL/USG_HQ **CONFIGURATION > Network > Routing > Add**. Set **Source Address** to be the subnet (192.168.2.0/24 in this example) allows joining the VPN

tunnel. Set **Destination Address** to be the remote LAN subnet (192.168.10.0/24 in this example).

CONFIGURATION > Network > Routing > Add

Add Policy Route

Show Advanced Settings Create new Object ▼

Configuration

☒ Enable

Description: (Optional)

Criteria

User: any ▼

Incoming: any (Excluding ZyV) ▼

Source Address: LAN2_SUBNET ▼

Destination Address: WIZ_VPN_HQ_REM ▼

DSCP Code: any ▼

Schedule: none ▼

Service: any ▼

Next-Hop

Type: VPN Tunnel ▼

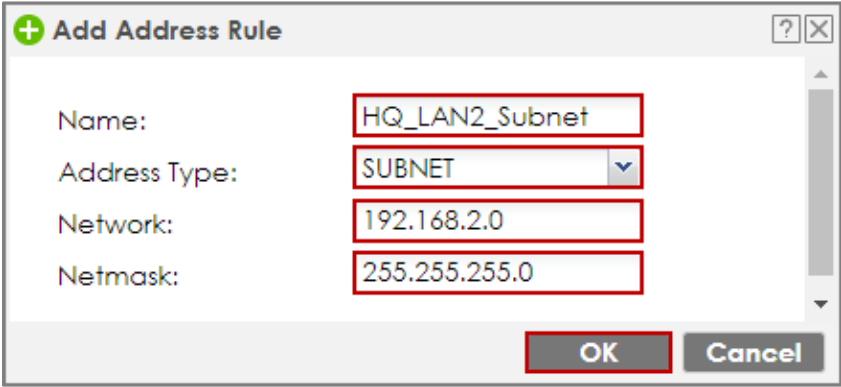
VPN Tunnel: WIZ_VPN_HQ ▼

OK Cancel

Set up the Policy Route (ZyWALL/USG_Branch)

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

CONFIGURATION > Object > Address > Add



+ Add Address Rule

Name:

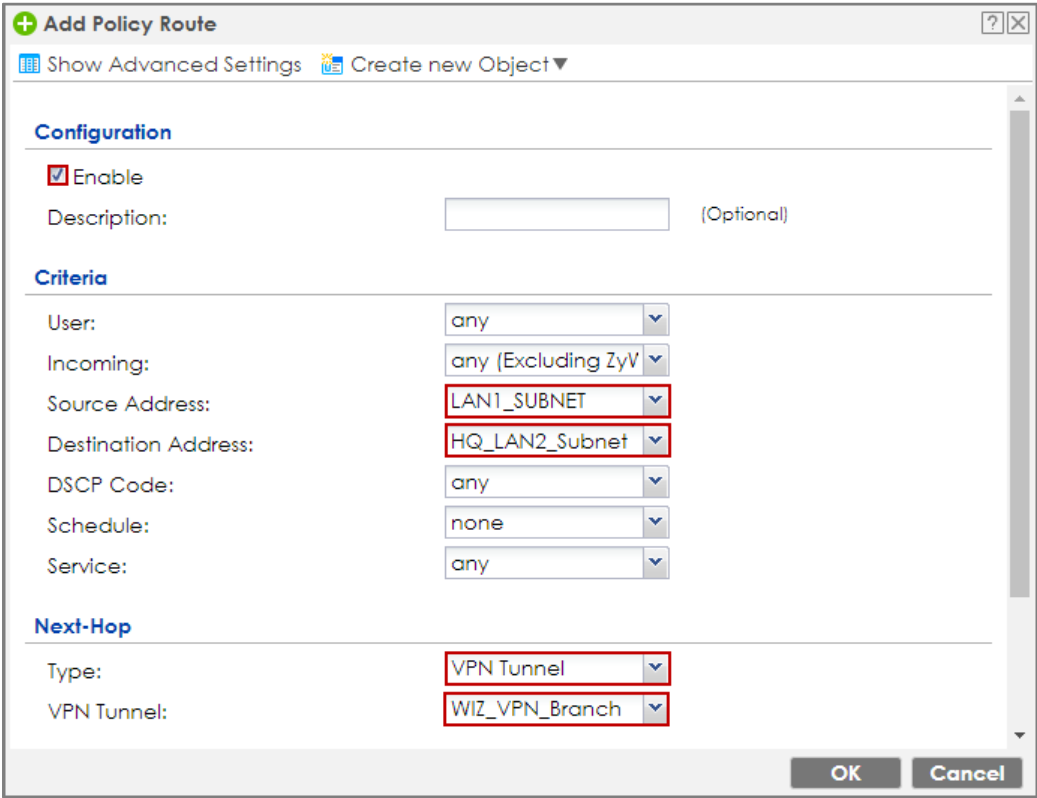
Address Type:

Network:

Netmask:

Go to ZyWALL/USG_Branch **CONFIGURATION > Network > Routing > Add**. Set **Source Address** to be the local subnet (192.168.10.0/24 in this example). Set **Destination Address** to be the remote LAN subnet (192.168.2.0/24 in this example) allows joining the VPN tunnel.

CONFIGURATION > Network > Routing > Add



+ Add Policy Route

Configuration

☒ Enable

Description: (Optional)

Criteria

User:

Incoming:

Source Address:

Destination Address:

DSCP Code:

Schedule:

Service:

Next-Hop

Type:

VPN Tunnel:

Test the IPSec VPN Tunnel

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

CONFIGURATION > VPN > IPSec VPN > VPN Connection



#	Status	Name	VPN Gateway	Policy
1		WIZ_VPN_HQ	WIZ_VPN_HQ	WIZ_VPN_HQ_LOCAL_WIZ_VPN...

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

MONITOR > VPN Monitor > IPSec



#	Serial Num...	System No...	Name	Policy	My Address	Secure G...	Up Time	Timeout	Inbound(B...	Outbound...
1	5162L44290	VPN100	WIZ_VPN_...	192.168.1.0/24<...	10.214.30...	P: 10.214.3...	1260	72180	31(1674 b...	31(1860 b...

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

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

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

Pinging 192.168.10.33 with 32 bytes of data:

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

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

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

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

Pinging 192.168.1.33 with 32 bytes of data:

Reply from 192.168.1.33: bytes=32 time=27ms TTL=43
Reply from 192.168.1.33: bytes=32 time=32ms TTL=43
Reply from 192.168.1.33: bytes=32 time=26ms TTL=43
Reply from 192.168.1.33: bytes=32 time=27ms TTL=43

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

PC at Branch Office > Window 7 > cmd > ping 192.168.2.33

```
C:\Documents and Settings\ZyXEL>ping 192.168.2.33

Pinging 192.168.2.33 with 32 bytes of data:

Reply from 192.168.2.33: bytes=32 time=27ms TTL=43
Reply from 192.168.2.33: bytes=32 time=27ms TTL=43
Reply from 192.168.2.33: bytes=32 time=26ms TTL=43
Reply from 192.168.2.33: bytes=32 time=32ms TTL=43

Ping statistics for 192.168.2.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 26ms, Maximum = 32ms, Average = 28ms
```

What Could Go Wrong?

If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

Priority	Category	Message	Note
info	IKE	[COOKIE] Invalid cookie, no sa found	IKE_LOG
Priority	Category	Message	Note
info	IKE	Recv:[NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : Tunnel [HQ1] Phase 1 proposal mismatch	IKE_LOG

If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log

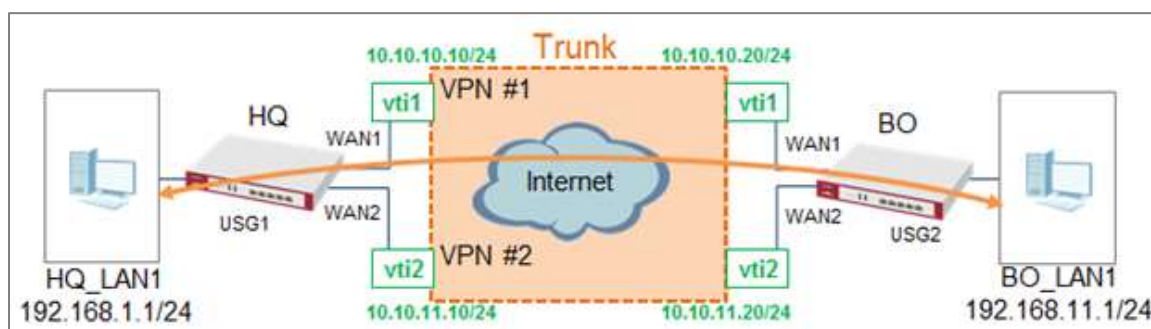
Priority	Cate...	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [BO1] Phase 2 proposal mismatch	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Phase 1 IKE SA process done	IKE_LOG

Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPSec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.

Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPSec device must also have NAT traversal enabled.

How to Create VTI and Configure VPN Failover with VTI

This example illustrates how to create a VTI object and configure a policy route with the VTI. Furthermore, it applies the VTI to the WAN trunk to achieve VPN load balancing.



VPN Load Balance with VTI

Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

VTI Deployment Flow

- 1 Configure the VPN gateways.
- 2 Configure a VPN tunnel for each VPN gateway with the application scenario VPN Tunnel Interface.
- 3 Create a VTI for each VPN tunnel.
- 4 Create a trunk with the VTIs.
- 5 Configure a policy route.
- 6 Connect the VPN tunnels.

Set Up the ZyWALL/USG VTI of Corporate Network (HQ)

- 1 In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add** to create the VPN gateway **HQ1** with **wan1**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface: DHCP client -- 10.214.30.106/255.255.252

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address: Primary
Secondary:

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key:

- 2 In the same screen, create the VPN gateway **HQ2** with **wan2**.

CONFIGURATION > VPN > IPSec VPN > VPN Gateway > Add

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface: DHCP client -- 10.214.30.107/255.255.252

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address: Primary
Secondary:

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key:

- Go to **CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add** and configure a VPN tunnel for the VPN gateway **HQ1**. Select **VPN Tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add

General Settings	
<input checked="" type="checkbox"/> Enable	
Connection Name:	HQ1
<input type="checkbox"/> Advance	
VPN Gateway	
Application Scenario	
<input type="radio"/> Site-to-site	
<input type="radio"/> Site-to-site with Dynamic Peer	
<input type="radio"/> Remote Access (Server Role)	
<input type="radio"/> Remote Access (Client Role)	
<input checked="" type="radio"/> Vpn Tunnel Interface	
VPN Gateway:	HQ1 wan1 10.214.30.77, 0.0.0.0
Phase 2 Setting	
SA Life Time:	86400 (180 - 3000000 Seconds)

- In the same screen, create a VPN tunnel for the VPN gateway **HQ2**. Select **VPN tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add

General Settings	
<input checked="" type="checkbox"/> Enable	
Connection Name:	HQ2
<input type="checkbox"/> Advance	
VPN Gateway	
Application Scenario	
<input type="radio"/> Site-to-site	
<input type="radio"/> Site-to-site with Dynamic Peer	
<input type="radio"/> Remote Access (Server Role)	
<input type="radio"/> Remote Access (Client Role)	
<input checked="" type="radio"/> Vpn Tunnel Interface	
VPN Gateway:	HQ2 wan2 10.214.30.84, 0.0.0.0
Phase 2 Setting	
SA Life Time:	86400 (180 - 3000000 Seconds)

- 5 Go to **CONFIGURATION > Network > Interface > VTI > Add** to create a VTI for the VPN tunnel **HQ1**. Enable the connectivity check. Enter the IP address of **vti1**, which is configured on **USG2**.

CONFIGURATION > Network > Interface > VTI > Add

General Settings	
<input checked="" type="checkbox"/> Enable	
Interface Properties	
Interface Name:	vti1
Zone:	IPSec_VPN
vpn-rule:	HQ1
IP Address Assignment	
IP Address:	10.10.10.10
Subnet Mask:	255.255.255.0
Metric:	0 (0-15)

CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check

Connectivity Check	
<input checked="" type="checkbox"/> Enable Connectivity Check	
Check Method:	icmp
Check Period:	30 (5-600 seconds)
Check Timeout:	5 (1-10 seconds)
Check Fail Tolerance:	5 (1-10)
Check this address:	10.10.10.20

- 6 In the same screen, create a VTI for the VPN tunnel **HQ2**.

CONFIGURATION > Network > Interface > VTI > Add

General Settings	
<input checked="" type="checkbox"/> Enable	
Interface Properties	
Interface Name:	vti2
Zone:	IPSec_VPN
vpn-rule:	HQ2
IP Address Assignment	
IP Address:	10.10.11.10
Subnet Mask:	255.255.255.0
Metric:	0 (0-15)

CONFIGURATION > Network > Interface > VTI > vti2 > Connectivity Check

Connectivity Check

☒ Enable Connectivity Check

Check Method:

Check Period: (5-600 seconds)

Check Timeout: (1-10 seconds)

Check Fail Tolerance: (1-10)

Check this address:

7 Go to CONFIGURATION > Network > Interface > Trunk > User

Configuration > Add to create a new trunk. Add **vti1** and **vti2** to the new trunk.

CONFIGURATION > Network > Interface > Trunk > User Configuration > Add

Name:

Load Balancing Algorithm:

Load Balancing Index(es):

#	Member	Mode	Egress Bandwidth
1	vti1	Active	1048576 kbps
2	vti2	Active	1048576 kbps

No data to display

8 Go to CONFIGURATION > Network > Routing > Policy Route > Add to configure a policy route.

Source Address: LAN1_SUBNET (192.168.1.0/24)

Destination Address: BO_subnet (192.168.11.0/24)

Next-Hop: HQ_vti_trunk

SNAT: none

CONFIGURATION > Network > Routing > Policy Route > Add

Configuration

☒ Enable

Description: (Optional)

Criteria

User:

Incoming:

Source Address:

Destination Address:

DSCP Code:

Schedule:

Service:

Next-Hop

Type:

Trunk:

DSCP Marking

DSCP Marking:

Address Translation

Source Network Address Translation:

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

VPN Connection

[VPN Gateway](#)
[Concentrator](#)
[Configuration Provisioning](#)

[Global Setting](#)
[Configuration Walkthrough](#)
[Troubleshooting](#)
[Download VPN Client](#)
[VPN](#)

☐ Use Policy Route to control dynamic IPsec rules

☐ Ignore "Don't Fragment" setting in IPv4 header

IPv4 Configuration

[Add](#)
[Edit](#)
[Remove](#)
[Activate](#)
[Deactivate](#)
[Connect](#)
[Disconnect](#)
[Object References](#)

#	Status	Name	VPN Gateway	Policy
1		HQ1	HQ1	any/any
2		HQ2	HQ2	any/any

Page 1 of 1
 Show 50 Items
 Displaying 1 - 2 of 2

10 Go to **CONFIGURATION > Network > Interface > VTI**. You will see that the status of the VTI is up when the corresponding VPN tunnel is established.

CONFIGURATION > Network > Interface > VTI

Port Role Ethernet PPP Cellular Tunnel VLAN Bridge VTI Trunk				
Configuration				
Add Edit Remove Activate Inactivate Object References				
#	Status	Name	IP Address	vpn rule
1		vtf1	10.10.10.10/24	HQ1
2		vtf2	10.10.11.10/24	HQ2
Page 1 of 1 Show 50 Items Displaying 1 - 2 of 2				

Set Up the ZyWALL/USG VTI of Corporate Network (Branch)

- 1 In the ZyWALL/USG, go to **CONFIGURATION > VPN > IPsec VPN > VPN Gateway > Add** to create the VPN gateway **BO1** with **wan1**.

CONFIGURATION > VPN > IPsec VPN > VPN Gateway > Add

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface: DHCP client — 10.214.30.77/255.255.255.255

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address

Primary:

Secondary:

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-60400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key:

- 2 In the same screen, create the VPN gateway **BO2** with **wan2**.

CONFIGURATION > VPN > IPsec VPN > VPN Gateway > Add

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☒ IKEv1

☐ IKEv2

Gateway Settings

My Address

☒ Interface: DHCP client -- 10.214.30.84/255.255.255.255

☐ Domain Name / IPv4:

Peer Gateway Address

☒ Static Address

Primary: Secondary:

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

☐ Dynamic Address

Authentication

☒ Pre-Shared Key:

- Go to **CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add** and configure a VPN tunnel for the VPN gateway **BO1**. Select **VPN Tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add

General Settings

☒ Enable

Connection Name:

☐ Advance

VPN Gateway

Application Scenario

☐ Site-to-site

☐ Site-to-site with Dynamic Peer

☐ Remote Access (Server Role)

☐ Remote Access (Client Role)

☒ Vpn Tunnel Interface

VPN Gateway: wan1: 10.214.30.106, 0.0.0.0

Phase 2 Setting

SA Life Time: (180 - 3000000 Seconds)

- 4 In the same screen, create a VPN tunnel for the VPN gateway **BO2**.
Select **VPN tunnel Interface** as the application scenario.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Add

General Settings

☒ Enable

Connection Name:

☐ Advance

VPN Gateway

Application Scenario

- ☐ Site-to-site
- ☐ Site-to-site with Dynamic Peer
- ☐ Remote Access (Server Role)
- ☐ Remote Access (Client Role)
- ☒ Vpn Tunnel Interface

VPN Gateway: wan2 10.214.30.107, 0.0.0.0

Phase 2 Setting

SA Life Time: (180 - 3000000 Seconds)

- 5 Go to **CONFIGURATION > Network > Interface > VTI > Add** to create a VTI for the VPN tunnel **BO1**. Be aware that the IP address of this VTI must be in the same subnet as **vti1** on **USG1**.

In this example, the IP address and subnet mask of **vti1** on **USG1** is **10.10.10.10** and **255.255.255.0** respectively. The IP address of **vti1** on **USG2** must be in the subnet of **10.10.10.0/24**. Enable the connectivity check. Enter the IP address of **vti1**, which is configured on **USG1**.

CONFIGURATION > Network > Interface > VTI > Add

General Settings	
<input checked="" type="checkbox"/> Enable	
Interface Properties	
Interface Name:	<input type="text" value="vti1"/>
Zone:	<input type="text" value="IPSec_VPN"/> ⓘ
vpn-rule:	<input type="text" value="BO1"/> ⓘ
IP Address Assignment	
IP Address:	<input type="text" value="10.10.10.20"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>
Metric:	<input type="text" value="0"/> (0-15)

CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check

Connectivity Check	
<input checked="" type="checkbox"/> Enable Connectivity Check	
Check Method:	<input type="text" value="icmp"/>
Check Period:	<input type="text" value="30"/> (5-600 seconds)
Check Timeout:	<input type="text" value="5"/> (1-10 seconds)
Check Fail Tolerance:	<input type="text" value="5"/> (1-10)
Check this address:	<input type="text" value="10.10.10.10"/>

6 In the same screen, create a VTI for the VPN tunnel **BO2**. Be aware that the IP address of this VTI must be in the same subnet as **vti2** on **USG1**. In this example, the IP address and subnet mask of **vti2** on **USG1** is **10.10.11.10** and **255.255.255.0** respectively. The IP address of **vti2** on **USG2** must be in the subnet of **10.10.11.0/24**. Enable the connectivity check. Enter the IP address of **vti2**, which is configured on **USG1**.

CONFIGURATION > Network > Interface > VTI > Add

General Settings

☒ Enable

Interface Properties

Interface Name:

Zone: ⓘ

vpn-rule: ⓘ

IP Address Assignment

IP Address:

Subnet Mask:

Metric: (0-15)

CONFIGURATION > Network > Interface > VTI > vti1 > Connectivity Check

Connectivity Check

☒ Enable Connectivity Check

Check Method:

Check Period: (5-600 seconds)

Check Timeout: (1-10 seconds)

Check Fail Tolerance: (1-10)

Check this address:

7 Go to **CONFIGURATION > Network > Interface > Trunk > User Configuration > Add** to create a new trunk. Add **vti1** and **vti2** to the new trunk.

CONFIGURATION > Network > Interface > Trunk > User Configuration > Add

Name:

Load Balancing Algorithm:

Load Balancing Index(es):

#	Member	Mode	Egress Bandwidth
1	<input type="text" value="vti1"/>	Active	1048576 kbps
2	<input type="text" value="vti2"/>	Active	1048576 kbps

Page 0 of 0 Show 50 items No data to display

- 8 Go to **CONFIGURATION > Network > Routing > Policy Route > Add** to configure a policy route.

Source Address: LAN1_SUBNET (192.168.11.0/24)

Destination Address: HQ_subnet (192.168.1.0/24)

Next-Hop: BO_vti_trunk

SNAT: none

CONFIGURATION > Network > Routing > Policy Route > Add

Configuration	
<input checked="" type="checkbox"/> Enable	
Description:	<input type="text"/> (Optional)
Criteria	
User:	any
Incoming:	any (Excluding ZyV)
Source Address:	LAN1_SUBNET
Destination Address:	HQ_subnet
DSCP Code:	any
Schedule:	none
Service:	any
Next-Hop	
Type:	Trunk
Trunk:	BO_vti_trunk
DSCP Marking	
DSCP Marking:	preserve
Address Translation	
Source Network Address Translation:	none

- 9 Connect the VPN tunnels when the VTIs are ready. Go to **CONFIGURATION > VPN > IPSec VPN > VPN Connection** to connect the VPN tunnels.

CONFIGURATION > VPN > IPsec VPN > VPN Connection > Connect

Configuration

☒ Enable
 Description: (Optional)

Criteria

User: any
 Incoming: any (Excluding ZyV
 Source Address: LAN1_SUBNET
 Destination Address: HQ_subnet
 DSCP Code: any
 Schedule: none
 Service: any

Next-Hop

Type: Trunk
 Trunk: BO_vti_trunk

DSCP Marking

DSCP Marking: preserve

Address Translation

Source Network Address Translation: none

10 Go to **CONFIGURATION > Network > Interface > VTI**. You will see that the status of the VTI is up when the corresponding VPN tunnel is established.

CONFIGURATION > Network > Interface > VTI

Port Role	Ethernet	PPP	Cellular	Tunnel	VLAN	Bridge	VTI	trunk
Configuration								
<div><div><div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div></div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div></div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div><div><div></div><div></div><div></div></div></div> <div>AddEditRemoveActivateImport/ExportObject Relationship</div>								
#	Status	Name	IP Address	VPN rule				
1	<div><div></div><div></div><div></div></div>	vti1	10.10.10.20/24	801				
2	<div><div></div><div></div><div></div></div>	vti2	10.10.11.20/24	802				
<div><div>1</div><div>Page 1 of 1</div><div>Show 50 items</div><div>Displaying 1 - 2 of 2</div></div>								

Test the IPsec VPN Tunnel

1 To test whether or not a tunnel is working, ping from a PC in LAN1 of USG1 to a PC in LAN1 of USG2 and vice versa.

PC of USG1 (192.168.1.34) > Window 7 > cmd > ping 192.168.11.33

```
C:\Users>ping 192.168.11.33 -t

Ping 192.168.11.33 <使用 32 位元組的資料>:
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
```

PC of USG2 (192.168.11.33) > Window 7 > cmd > ping 192.168.1.34

```
C:\Users>ping 192.168.1.34 -t

Ping 192.168.1.34 <使用 32 位元組的資料>:
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
```

- 2 To test whether or not VPN failover is working, unplug wan1 of USG1. Then ping from a PC in LAN1 of USG1 to a PC in LAN1 of USG2 and vice versa.

Check the VPN status of the USG1 in the MONITOR > VPN Monitor > IPSec screen.

#	Serial No...	System N...	Name	Policy	My Address	Secure Gate...	Up Time	Timeout	Inbound[...	Outbound...
1	5162L44290	VPN100	HQ2	0.0.0.0/1 <0.0...	10.214.30.107	P: 10.214.30.84	562	72878	205(11070...	285(17100...

PC of USG1 (192.168.1.34) > Window 7 > cmd > ping 192.168.11.33

```
C:\Users>ping 192.168.11.33 -t

Ping 192.168.11.33 <使用 32 位元組的資料>:
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=125
回覆自 192.168.11.33: 位元組=32 時間=1ms TTL=124
```

Check the VPN status of the USG2 in the **MONITOR > VPN Monitor > IPSec** screen.

Connection Check									
#	Serial No...	System N...	Name	Policy	My Address	Secure Gate...	Up Time	Timeout	Inbound/...
1	3162L44290	VPN100	HQ2	0.0.0.0/1<->0.0...	10.214.30.107	P: 10.214.30.84	562	72878	205(11070...

PC of USG2 (192.168.11.33) > Window 7 > cmd > ping 192.168.1.34

```
C:\Users>ping 192.168.1.34 -t

Ping 192.168.1.34 <使用 32 位元組的資料>:
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=124
回覆自 192.168.1.34: 位元組=32 時間=1ms TTL=125
```

What Can Go Wrong?

- 1 If you see below [info] or [error] log message, please check ZyWALL/USG Phase 1 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Pre-Shared Key, Encryption, Authentication method, DH key group and ID Type to establish the IKE SA.

MONITOR > Log

Priority	Category	Message	Note
Info	IKE	[COOKIE] Invalid cookie, no sa found	IKE_LOG
Priority	Category	Message	Note
Info	IKE	Recv:[NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
Info	IKE	[SA] : Tunnel [HQ1] Phase 1 proposal mismatch	IKE_LOG

- 2 If you see that Phase 1 IKE SA process done but still get below [info] log message, please check ZyWALL/USG Phase 2 Settings. Both ZyWALL/USG at the HQ and Branch sites must use the same Protocol, Encapsulation, Encryption, Authentication method and PFS to establish the IKE SA.

MONITOR > Log

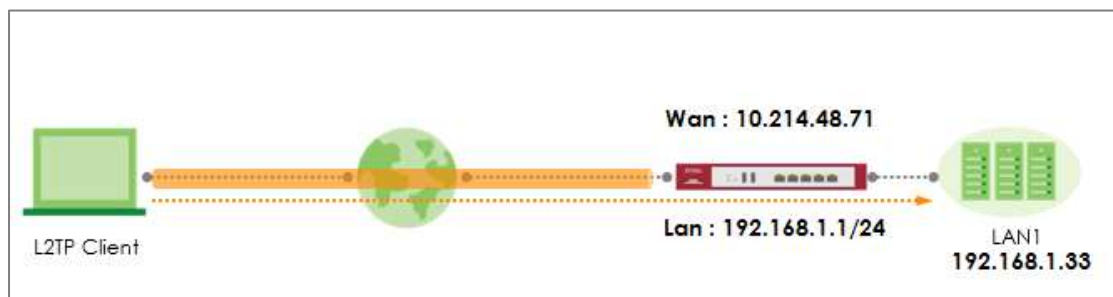
Priority	Cate...	Message	Note
info	IKE	Recv:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	Send:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Send:[HASH][NOTIFY:NO_PROPOSAL_CHOSEN]	IKE_LOG
info	IKE	[SA] : No proposal chosen	IKE_LOG
info	IKE	[SA] : Tunnel [BO1] Phase 2 proposal mismatch	IKE_LOG
info	IKE	Recv:[HASH][SA][NONCE][ID][ID]	IKE_LOG
info	IKE	Phase 1 IKE SA process done	IKE_LOG

- 3 Make sure the both ZyWALL/USG at the HQ and Branch sites security policies allow IPsec VPN traffic. IKE uses UDP port 500, AH uses IP protocol 51, and ESP uses IP protocol 50.
- 4 Default NAT traversal is enable on ZyWALL/USG, please make sure the remote IPsec device must also have NAT traversal enabled.
- 5 Make sure the both ZyWALL/USG at the HQ and Branch sites use static IP address because VPN Tunnel Interface does not support dynamic peer.
- 6 Make sure policy routes are configured to control traffic between the subnet of HQ and Branch through VTI.
- 7 Make sure that the IP address of VTI at the Branch must be in the same subnet as vti1 on HQ. For example, the IP address and subnet mask of vti1 on HQ is 10.10.10.10 and 255.255.255.0 respectively. The IP address of vti1 on the Branch must be in the subnet of 10.10.10.0/24; the IP address and subnet mask of vti2 on HQ is 10.10.11.10 and 255.255.255.0 respectively. The IP address of vti2 on the Branch must be in the subnet of 10.10.10.0/24, and so on.

Remote access VPN Wizard

The following is a sample configuration how to build up VPN tunnel with the remote access VPN wizard.

Remote access VPN Wizard is an easy way to quick set up VPN tunnel. Do not need complex configuration to build up VPN tunnel, all you need is to follow the steps on the VPN Wizard. Here are the steps to build L2TP over IPSec VPN tunnel for example.



Set up VPN Tunnel

1. In the ZyWALL/USG, Click Quick Setup, then click Remote Access VPN Setup build up VPN tunnel with the Wizard.



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-Shared Key
 - (2) Choose the Incoming interface
 - (3) Select the tunnel type, L2TP over IPsec VPN only support full tunnel type.
Enable the check box of "Allow L2TP traffic Through WAN".

Remote Access VPN Setup - L2TP over IPSec Client (iOS, Windows, Android)

1 VPN Configuration

2 VPN Configuration

3 Summary

4 Config Provision

VPN Authentication Method

Pre-Shared Key: 12345678

Incoming Interface

Interface: ge2 10.214.48.71/255.255.255.0

Domain Name / IPv4

Local Network

Full Tunnel

☒ Allow L2TP traffic Through WAN

Close < Back Next >

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.

Remote Access VPN Setup - L2TP over IPSec Client (iOS, Windows, Android)

1 VPN Configuration

2 User Authentication

3 Summary

4 Config Preview

Client Network

IP Address Pool : ☒ 192.168.50.1-192.168.50.250

☐ Custom Defined

Starting IP Address:

End IP Address:

First DNS Server : ☒ ZyWALL

☐ Custom Defined:

Second DNS Server:

Close < Back Next >

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.

Remote Access VPN Setup - L2TP over IPSec Client (iOS, Windows, Android)

1 VPN Configuration

2 User Authentication

3 Summary

4 Config Preview

Allowed Local User

Select user from the available user list and move it to the member list.

Available

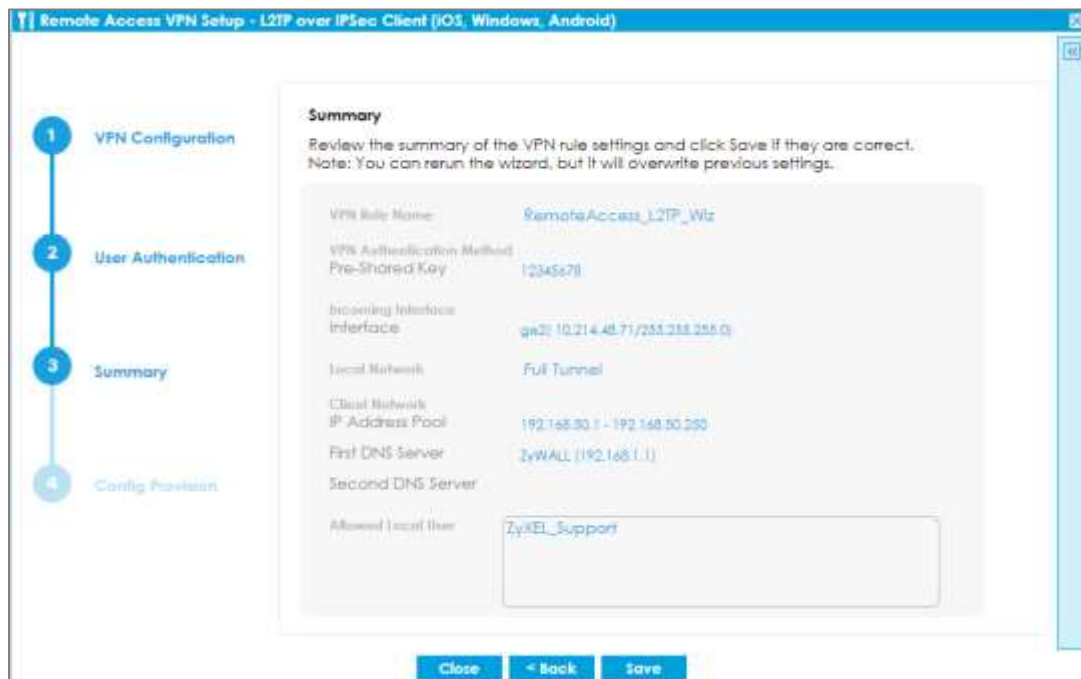
--- Object ---

ZyXEL_Support

Member

Close < Back Next >

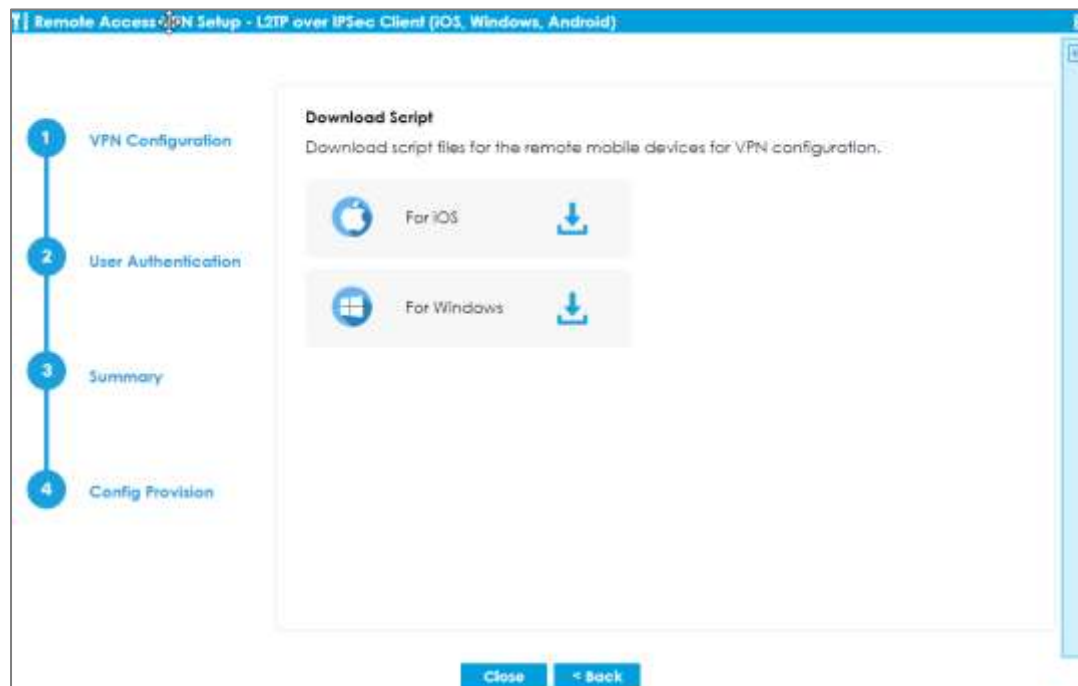
6. After done all the steps in the wizard, you can check the settings at the final step, if there is any settings wrong, you can click back to reset the configuration.
If the settings are all correct, click save to go next step.



7. Download script for Windows or IOS

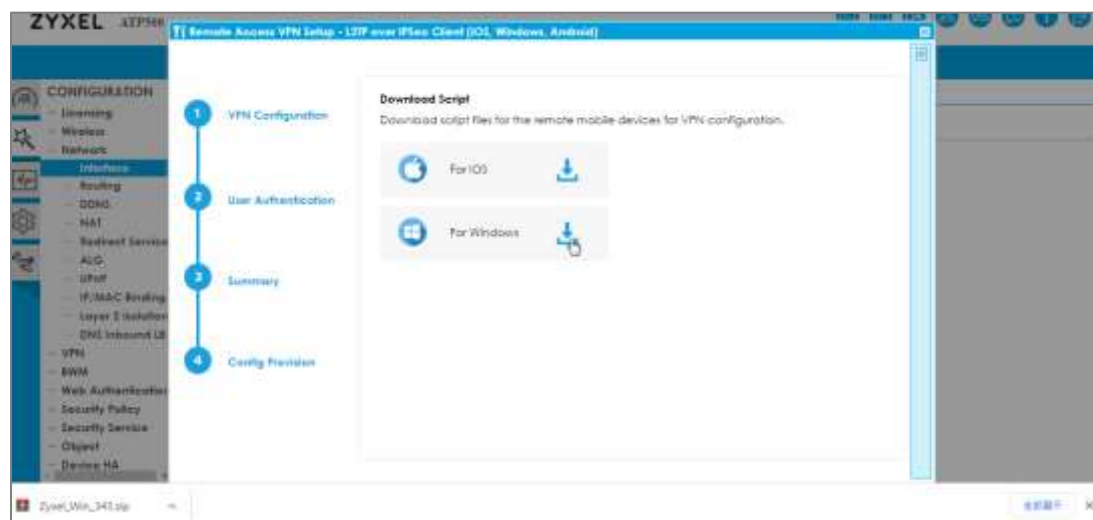
To quick connect to the device from client, we support scripts to run on IOS and Windows system.

Note: We do not support the script for Android system.



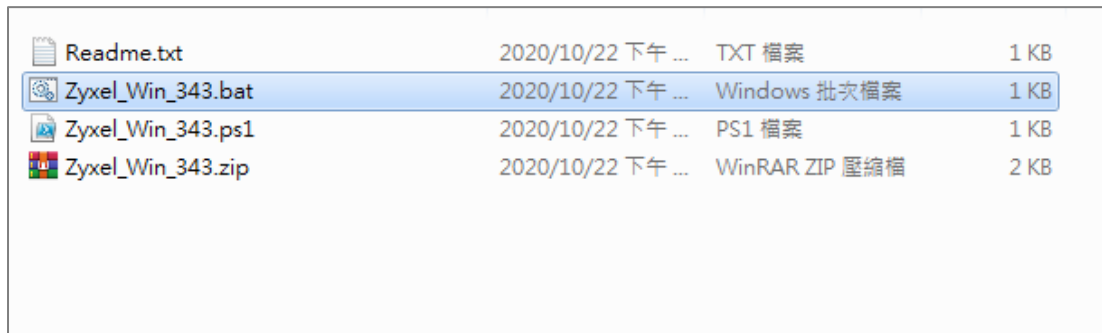
8. Download the scripts to quick build up VPN tunnel to the device on the client.

Note: Script file on windows support for Window8/ Window10



Test the result

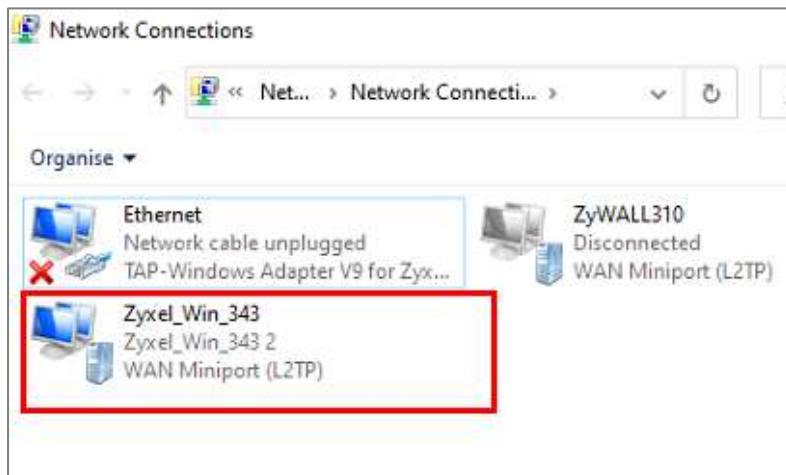
1. Extract the download script on windows, and run the scripts



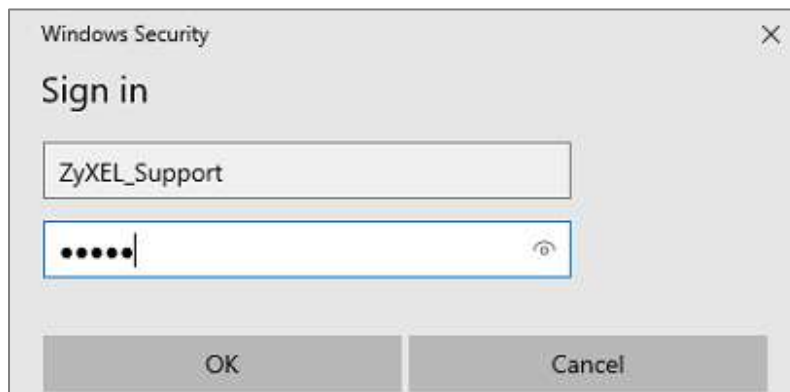
2. Using PowerShell to run the scripts



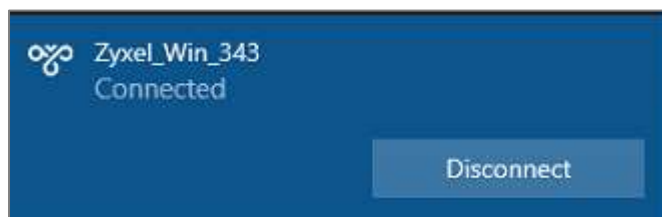
3. It will generate a site to connect to the device



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

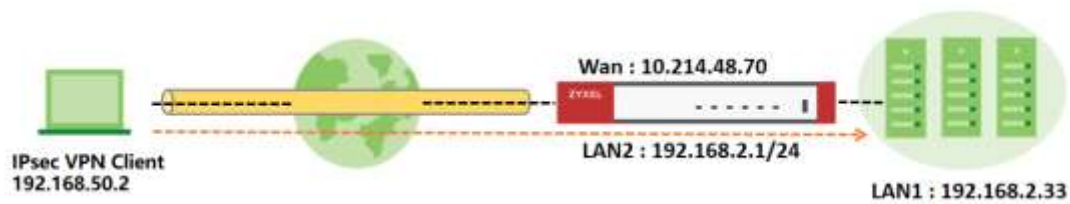
Pinging 192.168.1.33 with 32 bytes of data:
Reply from 192.168.1.33: bytes=32 time=1ms TTL=126
Reply from 192.168.1.33: bytes=32 time=1ms TTL=126
Reply from 192.168.1.33: bytes=32 time=1ms TTL=126
Reply from 192.168.1.33: bytes=32 time=2ms TTL=126

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.

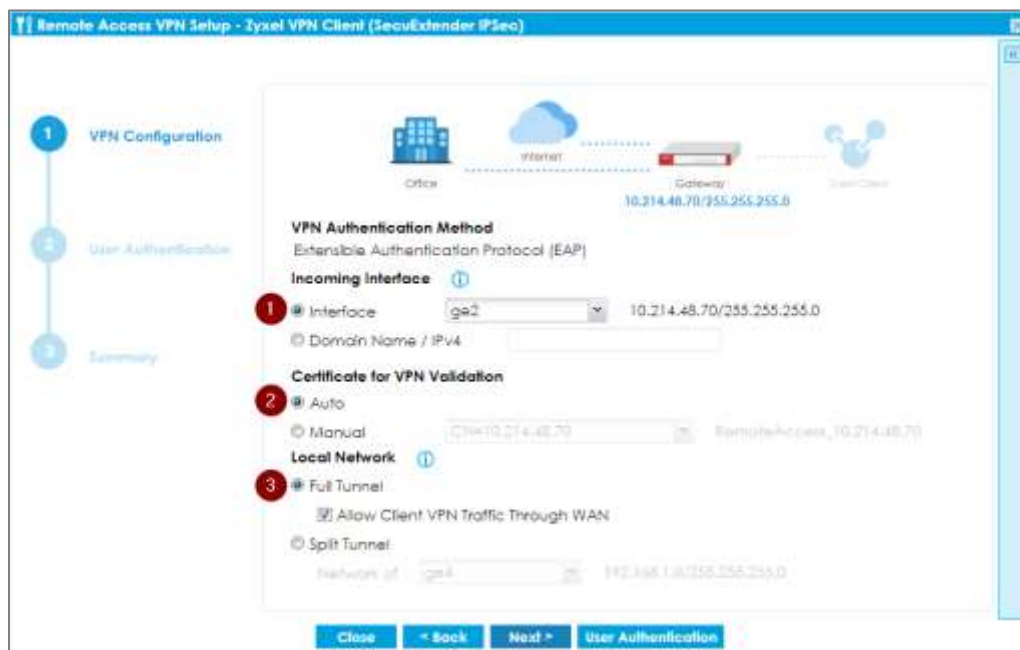


2. Select remote VPN scenarios, **ZyXEL VPN Client (SecuExtender IPSec)**.



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".

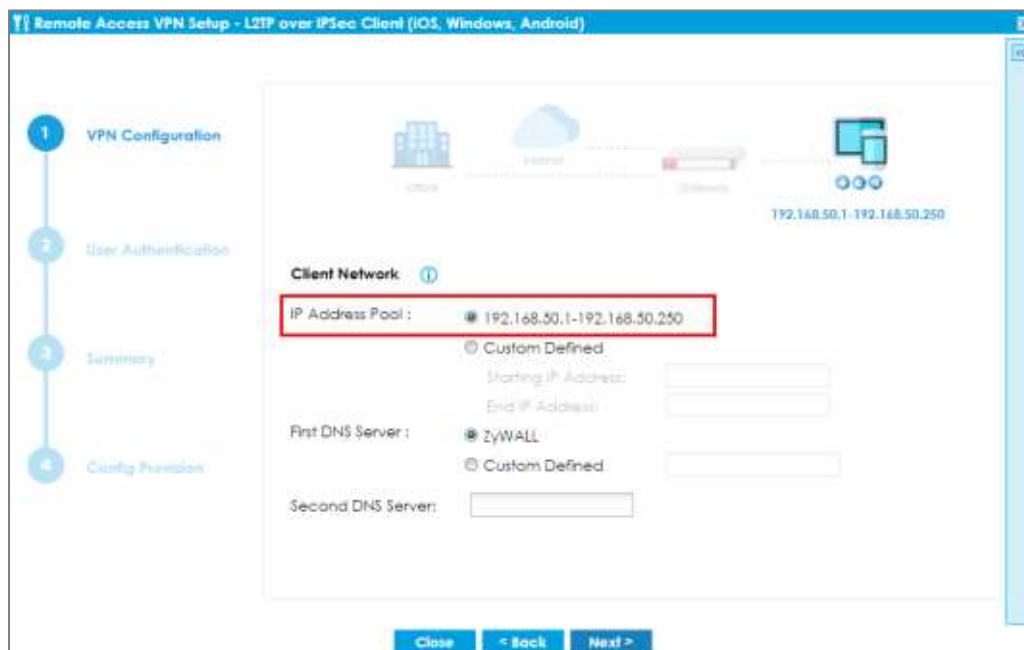


4. Configure the IP Address Pool for the client

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

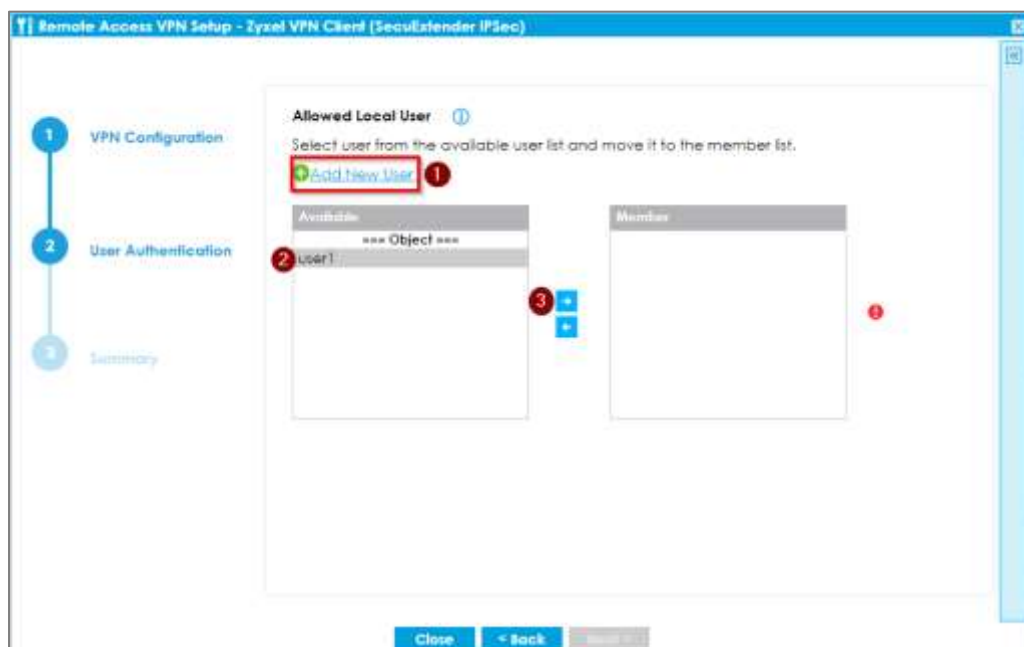
If there is 192.168.50.1 subnet exist in the gateway settings, the IP address pool will auto change to 192.168.51.1 subnet.

Note: the gateway only checks overlapped subnets in /24, not check the other subnet mask.

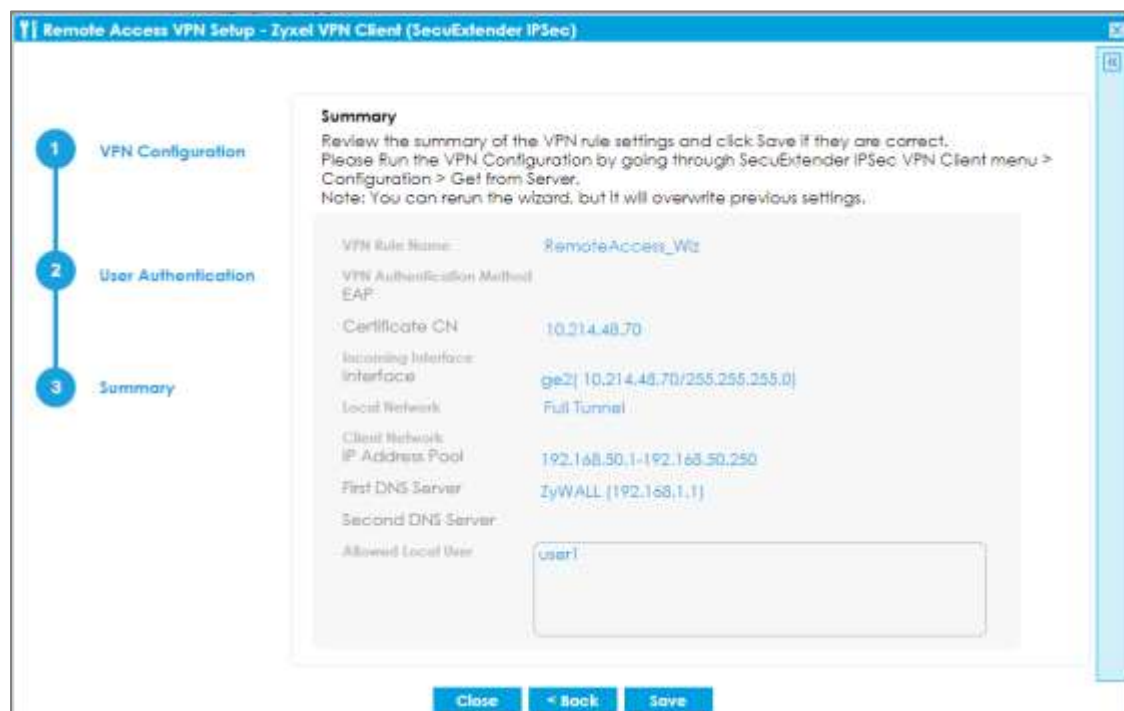


5. Allow local user to access the device

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.

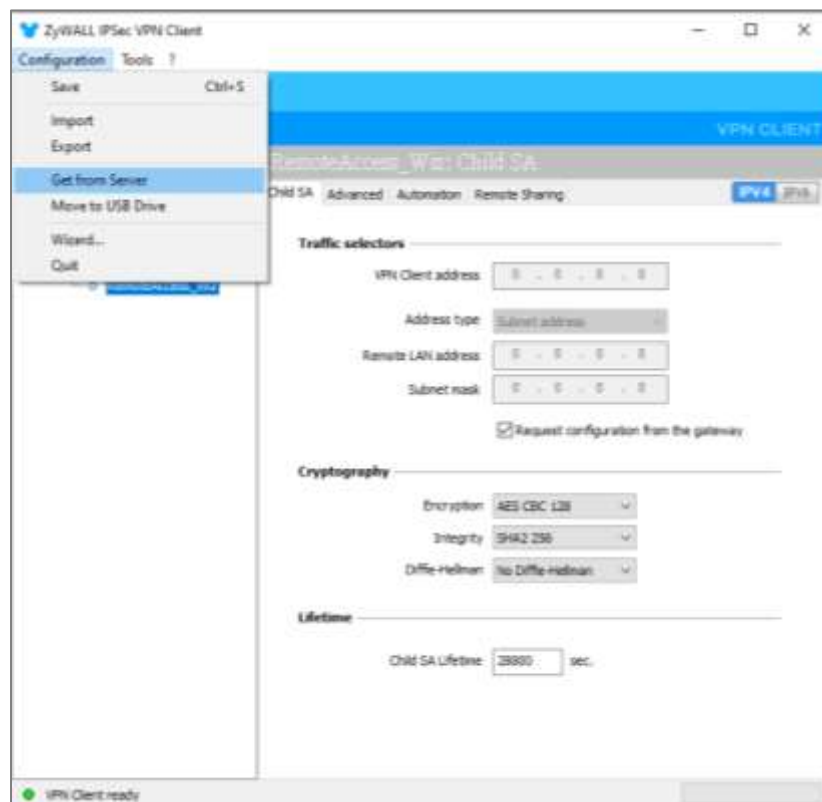


6. After done all the steps in the wizard, you can check the settings at the final step, if there is any settings wrong, you can click back to reset the configuration. If the settings are all correct, click save to go next step.

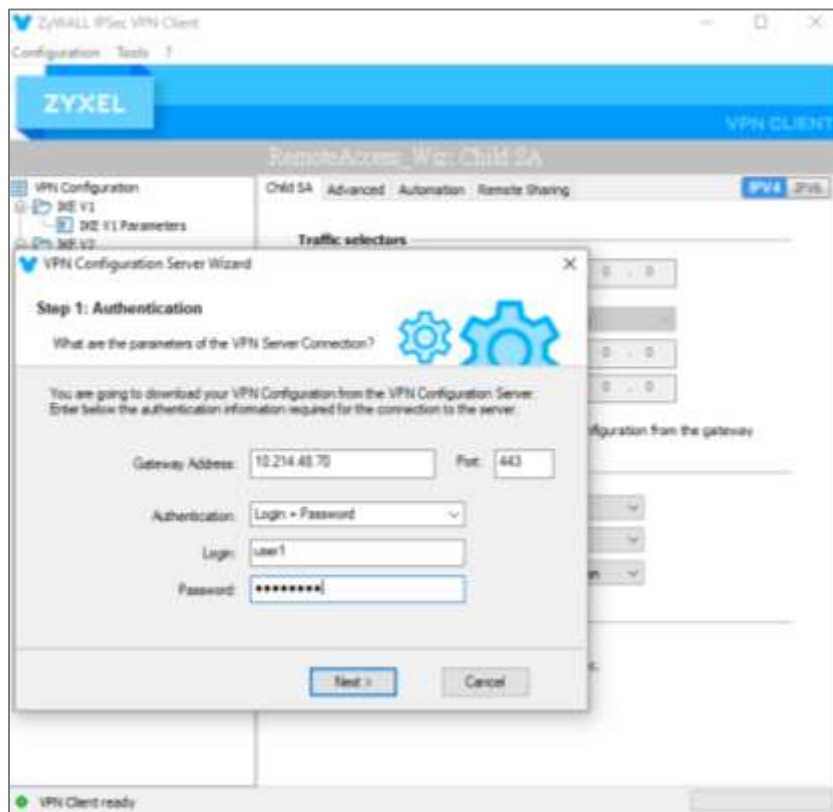


Test the result

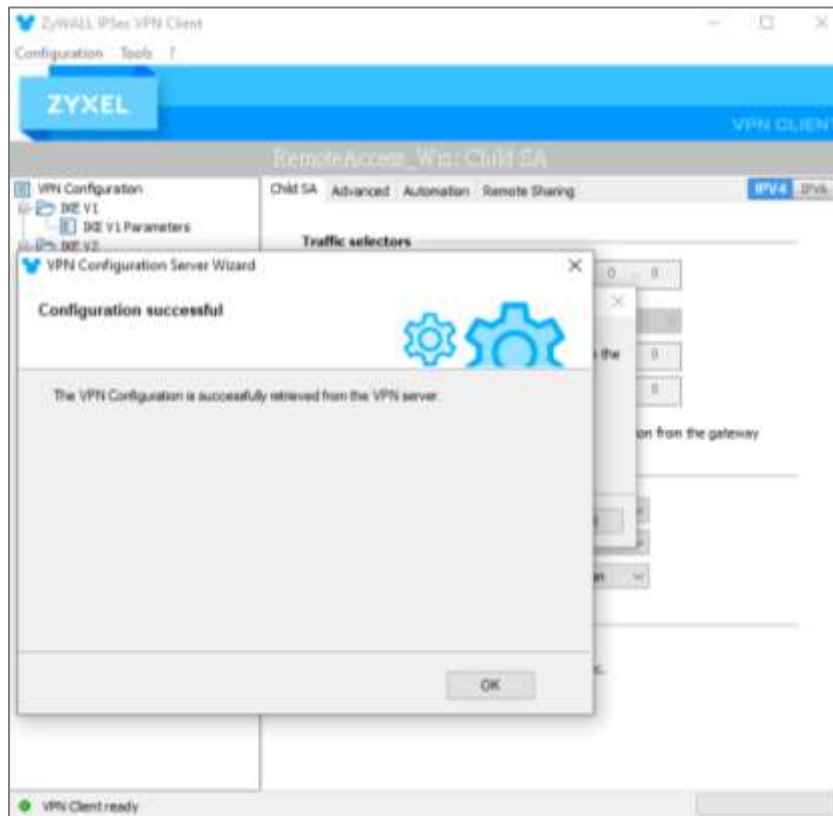
1. Open **ZyWALL IPsec VPN Client**, go to **Configuration > Get from Server**



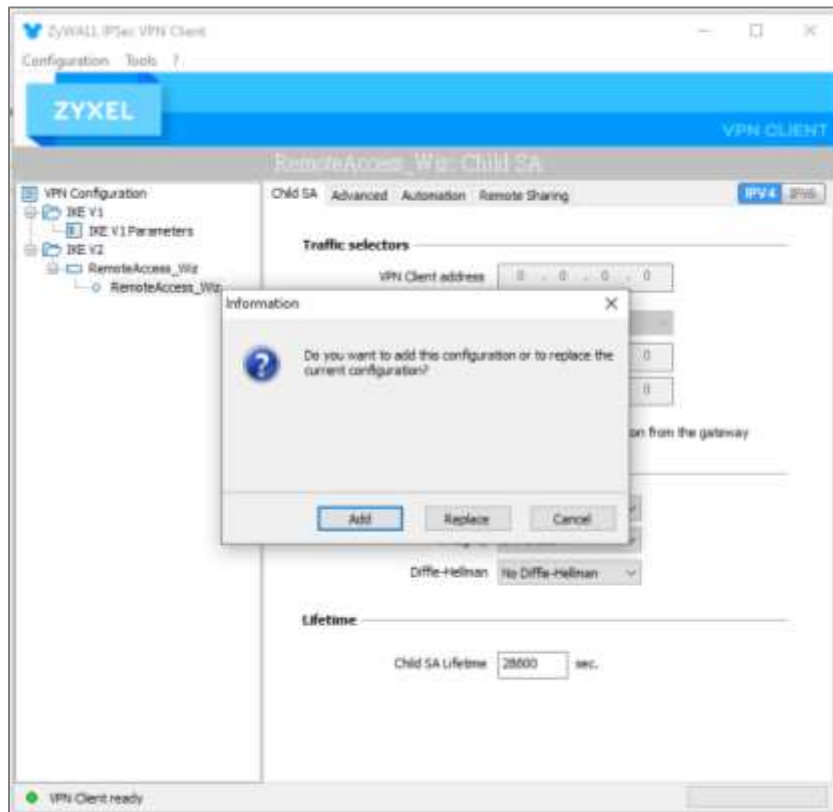
2. Typing the IP address of server, user account, and password. Then click on **Next**



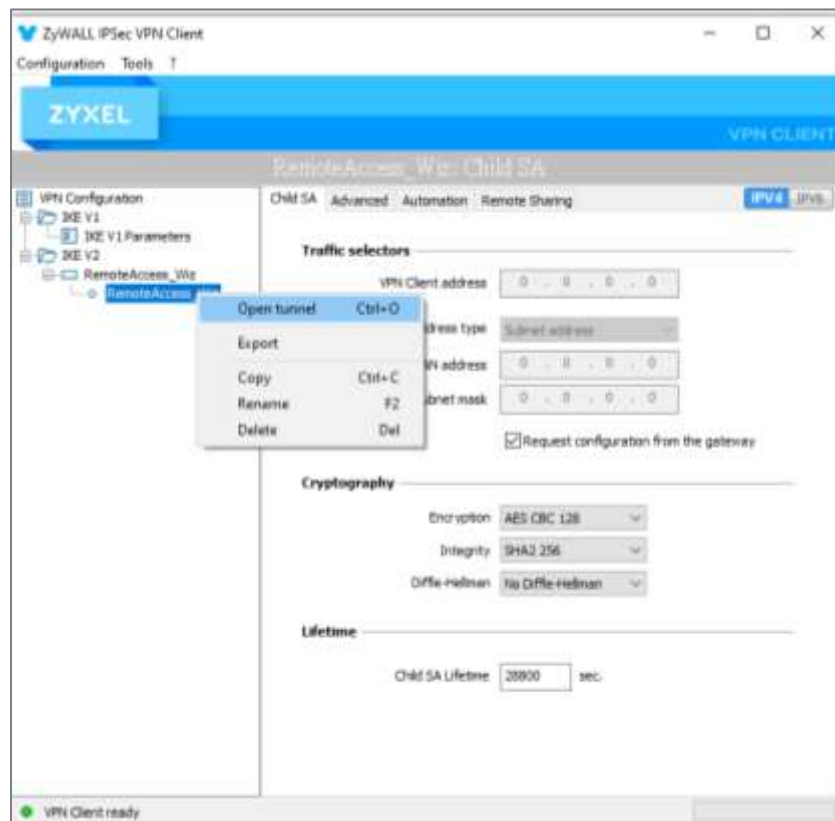
3. Wait until the VPN Client download successfully the configuration from server.



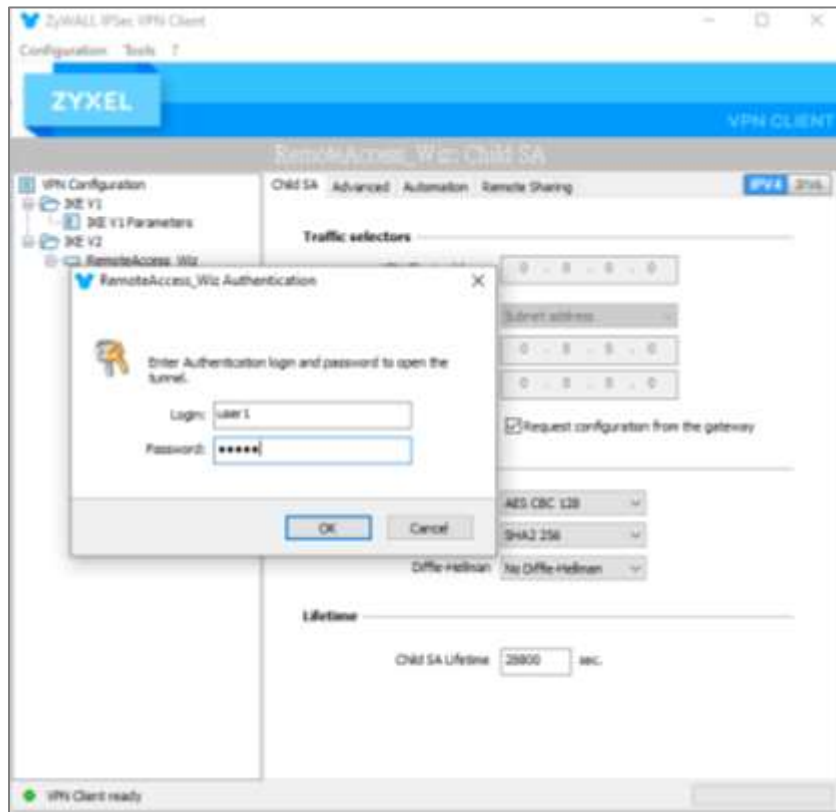
4. If you have an existing VPN configuration on the VPN client, click **Add** to replace.



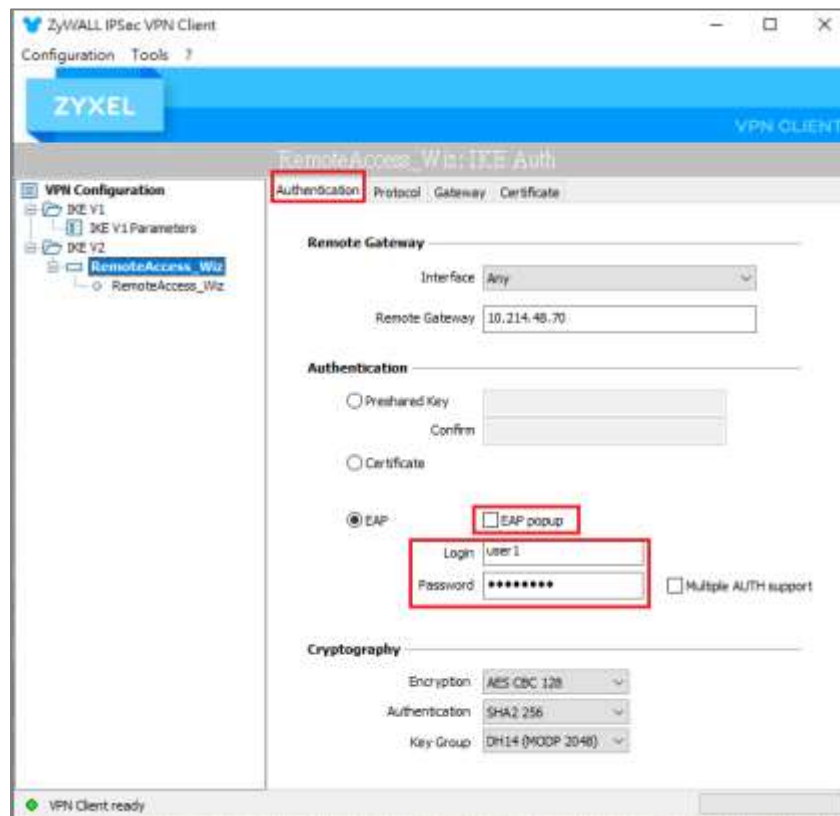
5. Right-click this configuration and press Open tunnel.



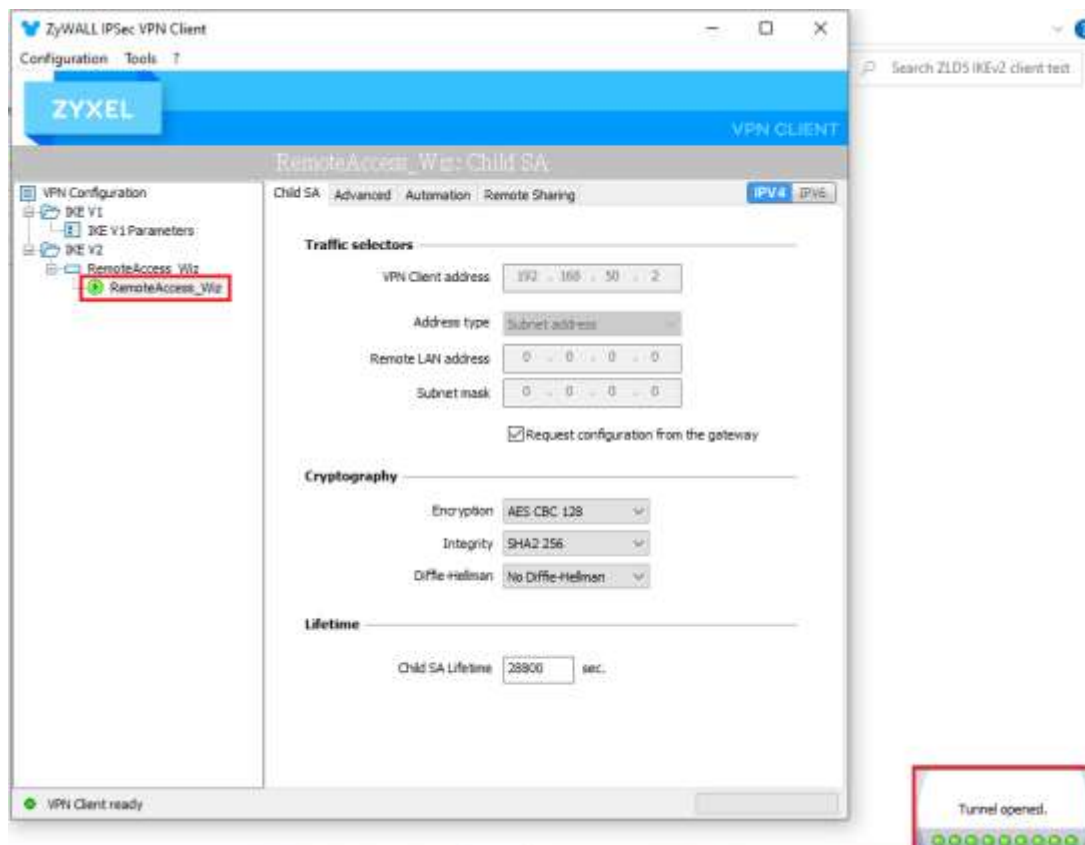
6. Popup window then typing login account and password.



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.

```

C:\Users\USER>ping 192.168.2.33

Pinging 192.168.2.33 with 32 bytes of data:
Reply from 192.168.2.33: bytes=32 time=9ms TTL=126
Reply from 192.168.2.33: bytes=32 time=6ms TTL=126
Reply from 192.168.2.33: bytes=32 time=8ms TTL=126
Reply from 192.168.2.33: bytes=32 time=12ms TTL=126

Ping statistics for 192.168.2.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 6ms, Maximum = 12ms, Average = 8ms
    
```

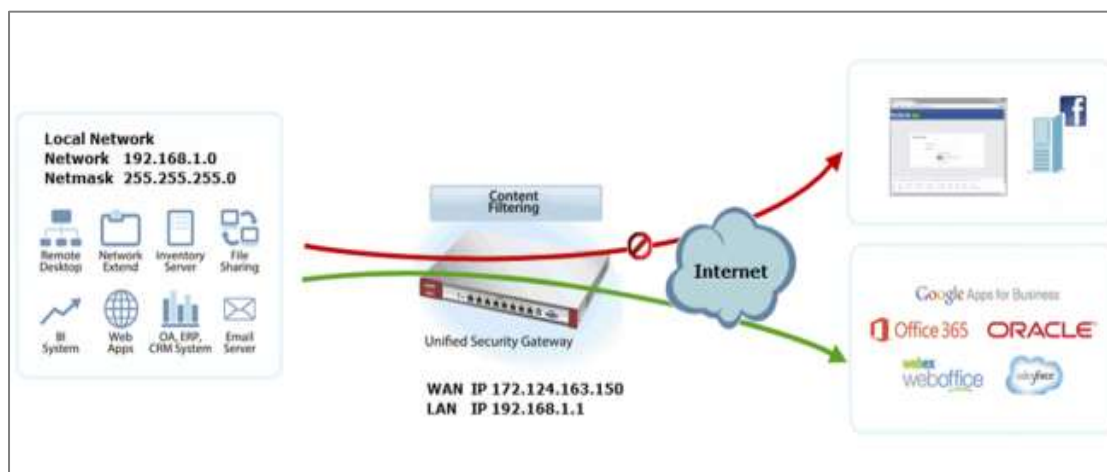
Chapter 2- Security Service

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.

General Settings

License Status:	Licensed		
License Type:	Standard		
Name:	Social_Net_Block		
Description:		(Optional)	

☐ Enable SafeSearch

☒ Enable Content Filter Category Service

☐ Log all web pages

Action for Unsafe Web Pages:	Block	<input type="checkbox"/> Log
Action for Managed Web Pages:	Block	<input checked="" type="checkbox"/> Log
Action for Unrated Web Pages:	Warn	<input type="checkbox"/> Log
Action When Category Server Is Unavailable:	Warn	<input type="checkbox"/> Log

Scroll down to the **Managed Categories** section, select categories in this section to control access to specific types of Internet content. You must have the Content Filtering license to filter these categories.

Managed Categories		
<input type="checkbox"/> Advertisements & Pop-Ups	<input type="checkbox"/> Alcohol/Tobacco	<input type="checkbox"/> Arts
<input type="checkbox"/> Business	<input type="checkbox"/> Transportation	<input type="checkbox"/> Chat
<input type="checkbox"/> Forums & Newsgroups	<input type="checkbox"/> Computers & Technology	<input type="checkbox"/> Criminal Activity
<input type="checkbox"/> Dating & Personals	<input type="checkbox"/> Download Sites	<input type="checkbox"/> Education
<input type="checkbox"/> Entertainment	<input type="checkbox"/> Finance	<input type="checkbox"/> Gambling
<input type="checkbox"/> Games	<input type="checkbox"/> Government	<input type="checkbox"/> Hate & Intolerance
<input type="checkbox"/> Health & Medicine	<input type="checkbox"/> Illegal Drugs	<input type="checkbox"/> Job Search
<input type="checkbox"/> Streaming Media & Downloads	<input type="checkbox"/> News	<input type="checkbox"/> Non-profits & NGOs
<input type="checkbox"/> Nudity	<input type="checkbox"/> Personal Sites	<input type="checkbox"/> Politics
<input type="checkbox"/> Pornography/Sexually Explicit	<input type="checkbox"/> Real Estate	<input type="checkbox"/> Religion
<input type="checkbox"/> Restaurants & Dining	<input type="checkbox"/> Search Engines/Portals	<input type="checkbox"/> Shopping
<input checked="" type="checkbox"/> Social Networking	<input type="checkbox"/> Sports	<input type="checkbox"/> Translators
<input type="checkbox"/> Travel	<input type="checkbox"/> Violence	<input type="checkbox"/> Weapons
<input type="checkbox"/> Web-based Email	<input type="checkbox"/> General	<input type="checkbox"/> Leisure & Recreation
<input type="checkbox"/> Cults	<input type="checkbox"/> Fashion & Beauty	<input type="checkbox"/> Greeting Cards
<input type="checkbox"/> Hacking	<input type="checkbox"/> Illegal Software	<input type="checkbox"/> Image Sharing
<input type="checkbox"/> Information Security	<input type="checkbox"/> Instant Messaging	<input type="checkbox"/> Peer to Peer
<input type="checkbox"/> Private IP Addresses	<input type="checkbox"/> School Cheating	<input type="checkbox"/> Sex Education
<input type="checkbox"/> Tasteless	<input type="checkbox"/> Child Abuse Images	

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).

<input checked="" type="checkbox"/> Enable	
Name:	Social_Network_Polic
Description:	(Optional)
From:	LAN1
To:	WAN
Source:	any
Destination:	any
Service:	any
User:	any
Schedule:	none
Action:	allow
Log matched traffic:	no
UTM Profile	
<input checked="" type="checkbox"/> Content Filter:	Social_Net_Block
<input type="checkbox"/> SSL Inspection:	none
Log:	by profile
Log:	by profile

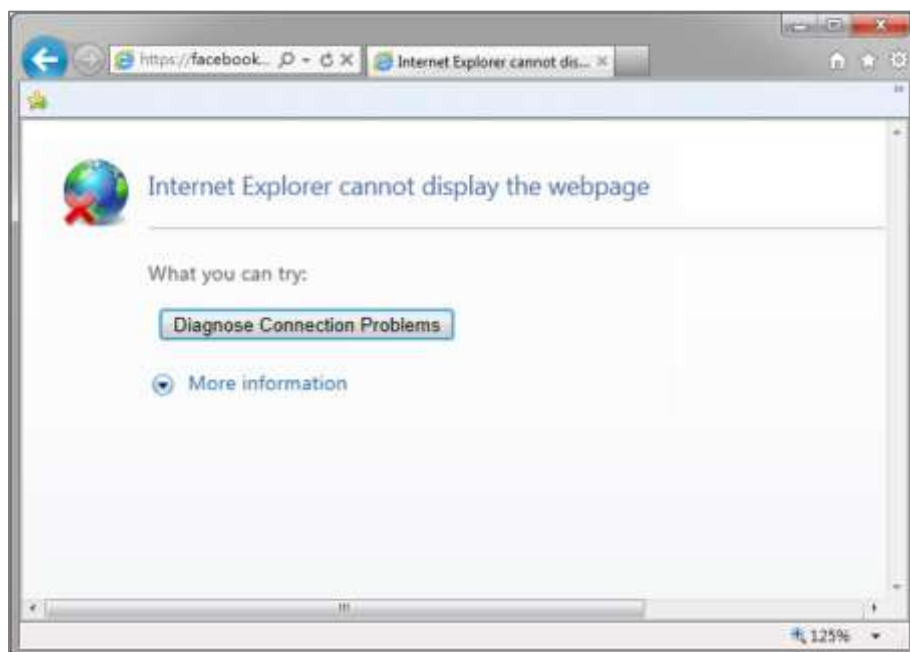
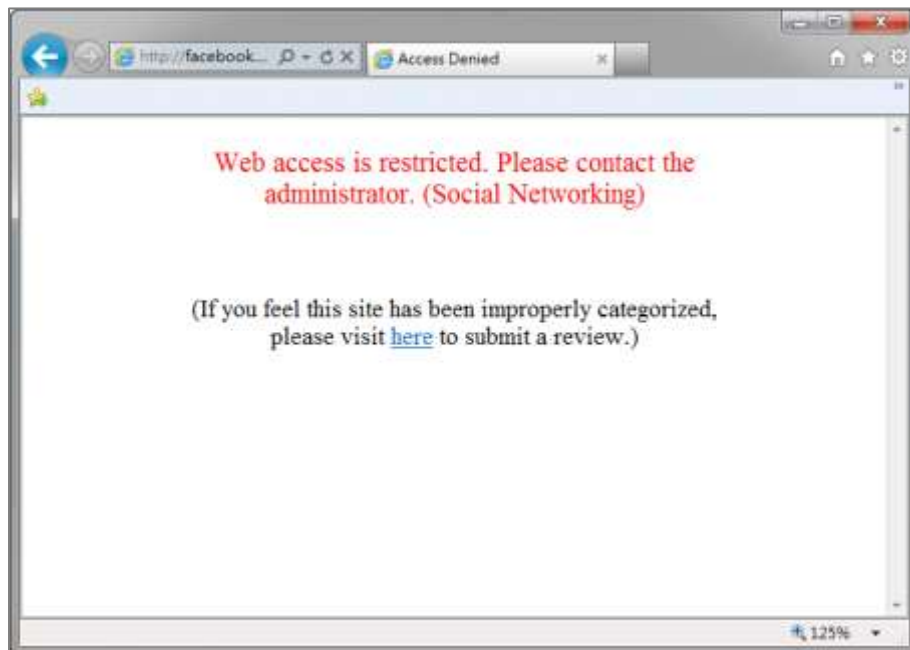
Set Up the System Policy on the ZyWALL/USG

Go to **CONFIGURATION > System > WWW > Show Advanced Settings > Other**, click **Enable Content Filter HTTPS Domain Filter Block/Warn Page**.

Other	
<input checked="" type="checkbox"/> Enable Content Filter HTTPS Domain Filter Block/Warn Page	
Block/Warn Page Port:	54088
<div> <div>Apply</div> <div>Reset</div> </div>	

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

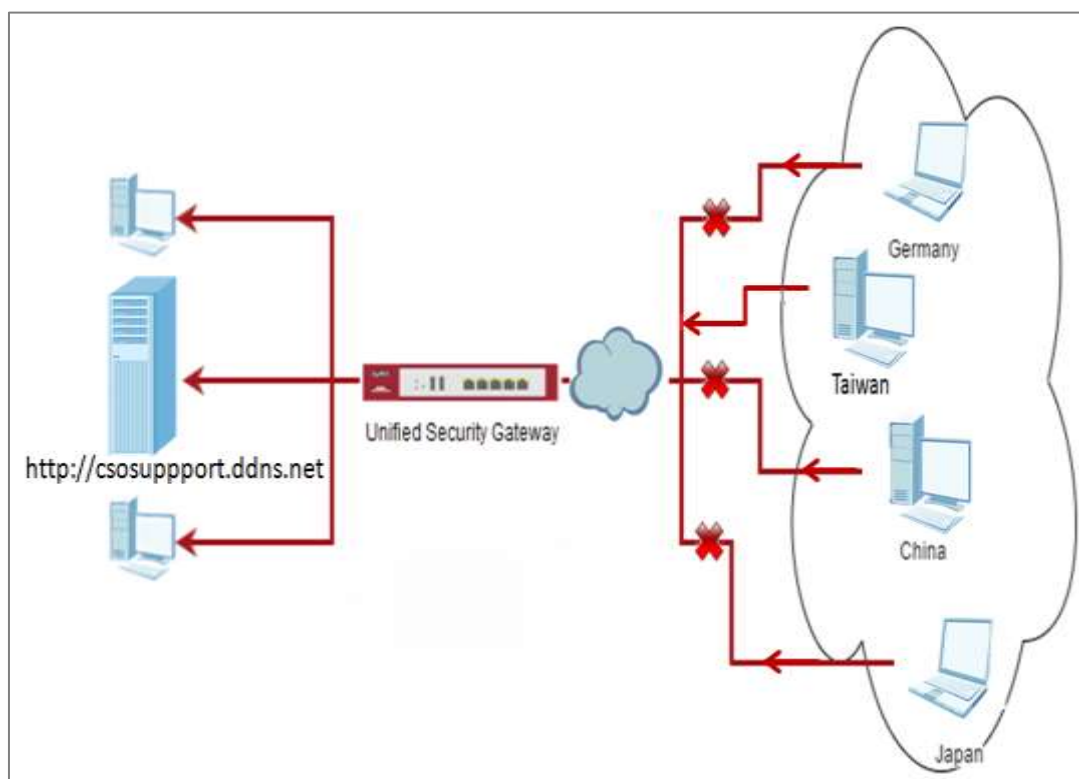
#	Time	Priority	Category	Message	Source	Destination	Note
1	2016-03-17 02:22:38	notice	Security Policy Control	Match default rule, DROP [count=1]	10.251.31.91:17500	255.255.255.255:17500	ACCESS BLOCK
2	2016-03-17 02:33:08	alert	Blocked web sites	facebook.com : Social Networking, Rule_id=1 (Content Filter)	192.168.1.33:18424	88.220.150.60:80	WEB BLOCK
3	2016-03-17 02:22:38	alert	Blocked web sites	www.facebook.com : Social Networking, Rule_id=1 (HTTPS Domain Filter)	192.168.1.33:81728	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 Object with Geo IP on the ZyWALL/USG

Go to **CONFIGURATION > Object > Address/Geo IP > Address > Add Address Rule**.



Edit Address Rule Taiwan

Name:

Address Type:

Country:

OK Cancel

Go to **CONFIGURATION > Object > Address/Geo IP > Address**, you can see the customized GEOGRAPHY address.

Address			
Address Group			
Geo IP			
IPv4 Address Configuration			
Add Edit Remove Object References			
#	Name	Type	IPv4 Address
1	wan2	INTERFACE IP	wan2-10.251.30.90
2	LAN2_SUBNET	INTERFACE SUBNET	lan2-192.168.2.0/24
3	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.1.0/24
4	DMZ_SUBNET	INTERFACE SUBNET	dmz-192.168.3.0/24
5	Taiwan	GEOGRAPHY	Taiwan-All
6	IP6to4-Relay	HOST	192.88.99.1
7	l2tp_pool	RANGE	192.168.10.10-192.168.10.20
8	RFC1918_3	SUBNET	192.168.0.0/16
9	RFC1918_2	SUBNET	172.16.0.0/12

Set Up the Security Policy on the ZyWALL/USG

Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set Geo IP traffic from WAN to LAN allow source from local country (geo_allow_policy in this example).

Edit Policy1

Create new Object ▾

☒ Enable

Name: geo_allow_policy

Description: (Optional)

From: WAN

To: LAN1

Source: Taiwan

Destination: any

Service: any

User: any

Schedule: none

Action: allow

Log matched traffic: log

Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Set traffic from WAN to LAN deny (geo_block_policy in this example).

Add corresponding

Create new Object ▾

☒ Enable

Name: geo_block_policy

Description: (Optional)

From: WAN

To: LAN1

Source: any

Destination: any

Service: any

User: any

Schedule: none

Action: deny

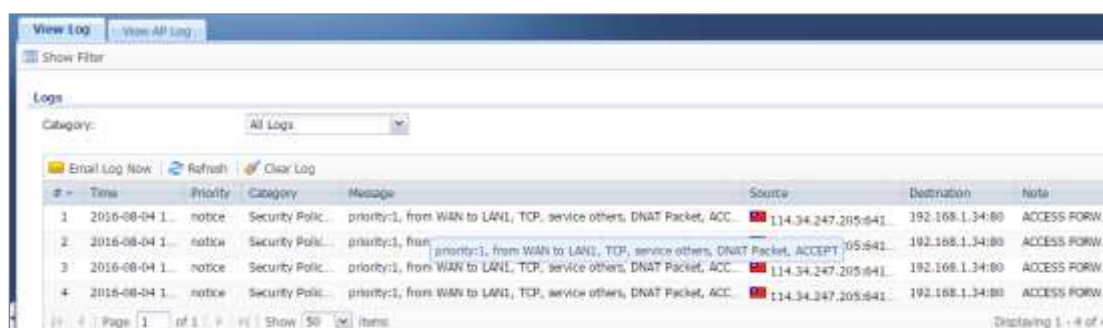
Log denied traffic: no

Test the Result

Type <http://csosupport.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.

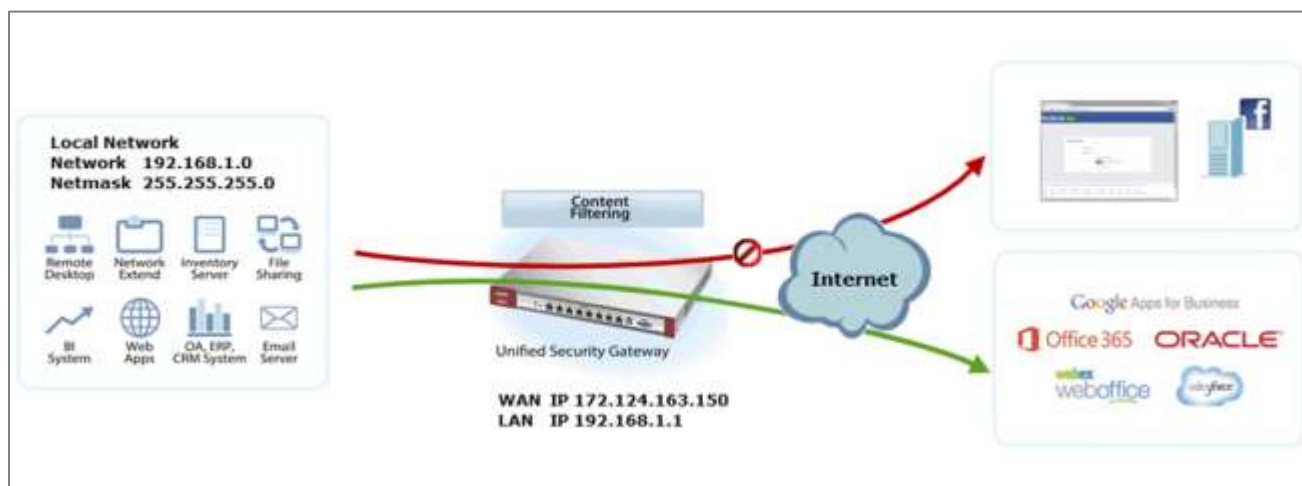
#	Time	Priority	Category	Message	Source	Destination	Note
5	2016-08-19 1...	alert	Security Polic...	Match default rule, DNAT Packet, DROP [count=3]	114.34.247.205...	192.168.1.34:80	ACCESS BLOCK
6	2016-08-19 1...	alert	Security Polic...	Match default rule, DNAT Packet, DROP [count=3]	114.34.247.205...	192.168.1.34:80	ACCESS BLOCK

2. The Content-Filter service is 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**.

The screenshot shows the 'General Settings' tab for the Content Filter. The 'Enable Content Filter Report Service' checkbox is unchecked, with a 'Report Server' link and an information icon. The 'Enable HTTPS Domain Filter for HTTPS traffic' checkbox is checked, with an information icon. The 'Drop connection when HTTPS connection with SSL V3 or previous version' checkbox is checked. The 'Content Filter Category Service Timeout' is set to 10 seconds, with a note '(1~60 Seconds)'.

Go to **CONFIGURATION > UTM Profile> Content Filter > Profile Management > Add Filter**

Profile > Test Web Site Category. Type URL to test the category and click **Test Against Content Filter Category Server.**

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.

Category Service	Custom Service	
<input type="checkbox"/> Advertisements & Pop-Ups	<input type="checkbox"/> Alcohol/Tobacco	<input type="checkbox"/> Arts
<input type="checkbox"/> Business	<input type="checkbox"/> Transportation	<input type="checkbox"/> Chat
<input type="checkbox"/> Forums & Newsgroups	<input type="checkbox"/> Computers & Technology	<input type="checkbox"/> Criminal Activity
<input type="checkbox"/> Dating & Personals	<input type="checkbox"/> Download Sites	<input type="checkbox"/> Education
<input type="checkbox"/> Entertainment	<input type="checkbox"/> Finance	<input type="checkbox"/> Gambling
<input type="checkbox"/> Games	<input type="checkbox"/> Government	<input type="checkbox"/> Hate & Intolerance
<input type="checkbox"/> Health & Medicine	<input type="checkbox"/> Illegal Drugs	<input type="checkbox"/> Job Search
<input type="checkbox"/> Streaming Media & Downloads	<input type="checkbox"/> News	<input type="checkbox"/> Non-profits & NGOs
<input type="checkbox"/> Nudity	<input type="checkbox"/> Personal Sites	<input type="checkbox"/> Politics
<input type="checkbox"/> Pornography/Sexually Explicit	<input type="checkbox"/> Real Estate	<input type="checkbox"/> Religion
<input type="checkbox"/> Restaurants & Dining	<input type="checkbox"/> Search Engines/Portals	<input type="checkbox"/> Shopping
<input checked="" type="checkbox"/> Social Networking	<input type="checkbox"/> Sports	<input type="checkbox"/> Translators
<input type="checkbox"/> Travel	<input type="checkbox"/> Violence	<input type="checkbox"/> Weapons
<input type="checkbox"/> Web-based Email	<input type="checkbox"/> General	<input type="checkbox"/> Leisure & Recreation
<input type="checkbox"/> Cults	<input type="checkbox"/> Fashion & Beauty	<input type="checkbox"/> Greeting Cards
<input type="checkbox"/> Hacking	<input type="checkbox"/> Illegal Software	<input type="checkbox"/> Image Sharing
<input type="checkbox"/> Information Security	<input type="checkbox"/> Instant Messaging	<input type="checkbox"/> Peer to Peer

Set Up the Security Policy on the ZyWALL/USG

Go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Social_Net_Block in this example).

Create new Object ▼

☒ Enable

Name:

Description: (Optional)

From:

To:

Source:

Destination:

Service:

User:

Schedule:

Action:

Log matched traffic:

UTM Profile

☒ Content Filter: Log:

Set Up the System Policy on the ZyWALL/USG

Go to **CONFIGURATION > System > WWW > Show Advanced Settings > Other**, click **Enable Content Filter HTTPS Domain Filter Block/Warn Page**.

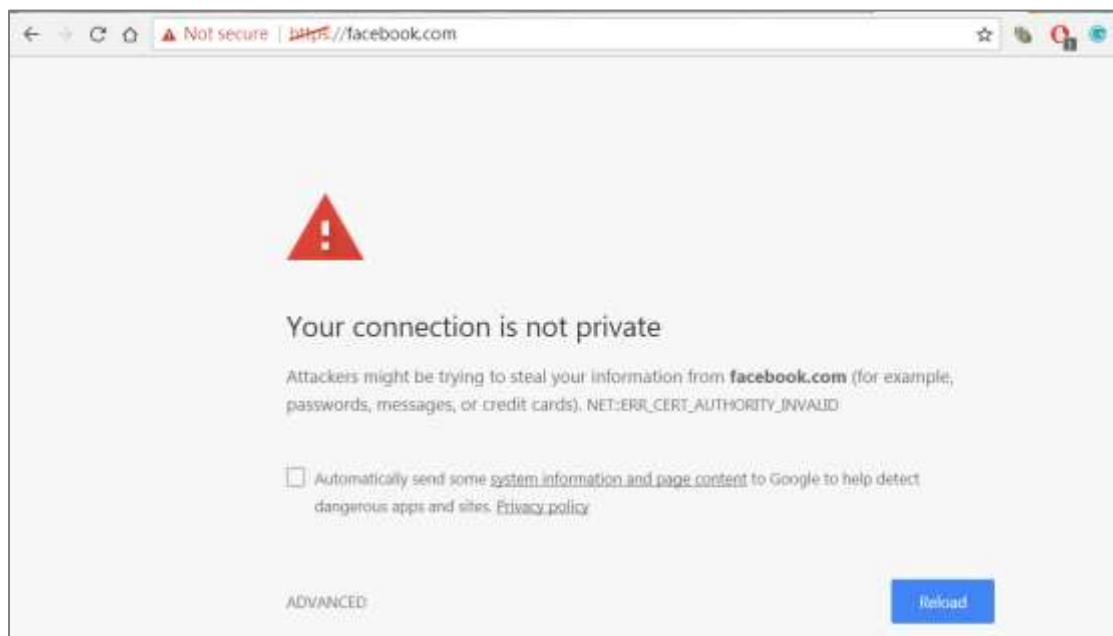
Other

☒ Enable Content Filter HTTPS Domain Filter Block/Warn Page

Block/Warn Page Port:

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	PL	Category	Message	Source	Dest	Alert
28	20...	alert	Blocked w...	facebook.com : Social Networking, Rule_id=1, SSL=N (HTTPS Domain...	192.168.2.3...	31...	WEB BLOCK
29	20...	alert	Blocked w...	facebook.com : Social Networking, Rule_id=1, SSL=N (HTTPS Domain...	192.168.2.3...	31...	WEB BLOCK
30	20...	alert	Blocked w...	facebook.com : Social Networking, Rule_id=1, SSL=N (HTTPS Domain...	192.168.2.3...	31...	WEB BLOCK

What Could Wrong?

1. "Enable HTTPS Domain Filter for HTTPS traffic" is not checked.

Profile	Trusted Web Sites	Forbidden Web Sites
General Settings Configuration Walkthrough Troubleshooting Content Filter		
<input type="checkbox"/> Enable Content Filter Report Service Report Server		
<input type="checkbox"/> Enable HTTPS Domain Filter for HTTPS traffic i		
<input checked="" type="checkbox"/> Drop connection when HTTPS connection with SSL V3 or previous version i		
Content Filter Category Service Timeout:	<input type="text" value="10"/>	(1~60 Seconds)

HTTPs traffic will pass.

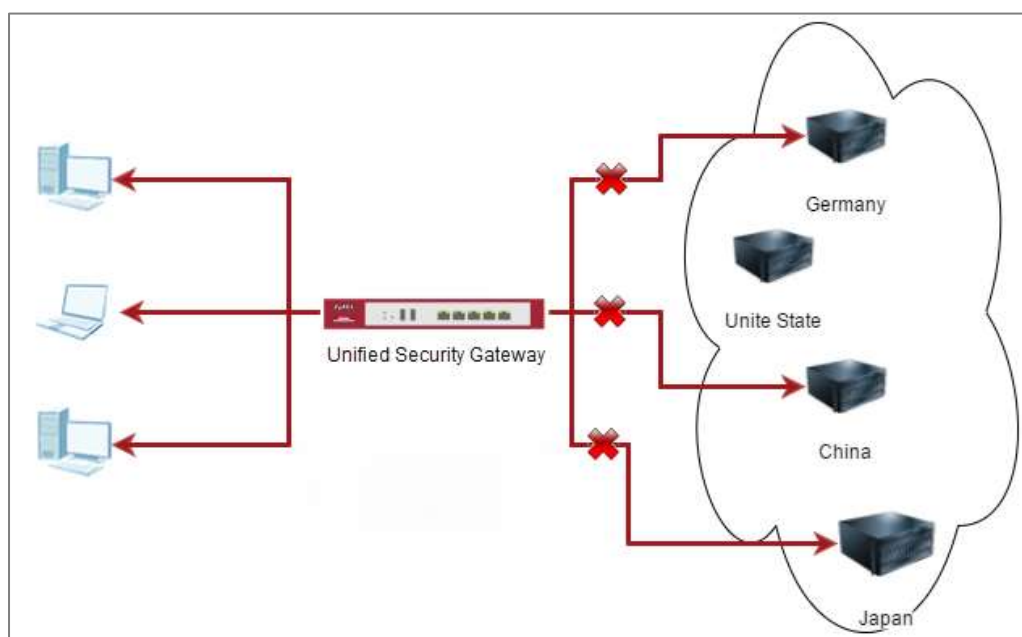
https://www.facebook.com
<div>  <input type="text" value="搜尋人、地點和事物"/> <input type="button" value="Q"/> </div>


How to block the client accessing to certain country using Geo IP and Content Filter

The Content Filter with Geo IP offers identify the country based on IP address, it allows you to block the client accessing to certain country based on organizational policy.

When user makes HTTP or HTTPS request, ZyWALL/USG query IP address from MaxMind database, then take action when it matches the block country in Content Filter profile.

ZyWALL/USG Geo IP Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: 4.25)

Check Geo IP License Status on the ZyWALL/USG

Go to **CONFIGURATION > Licensing > Registration > Service**, the **Geo IP Service** should be **Licensed** to configure this feature.

#	Service	Status	Service Type	Expiration ...	Count	Action
1	Content Filter 2.0	Licensed	Standard	2018-7-6	N/A	Renew
2	SSL VPN Service	Licensed	Standard		60	Buy
3	Managed AP Service	Default	Standard		4	Buy
4	Zymesh Service	Not Licens...			N/A	
5	Concurrent Device Upgr...	Default	Standard		200	Buy
6	Device HA Pro	Not Licens...			N/A	Buy
7	Firmware Upgrade Service	Not Licens...			N/A	
8	SecuReporter	Not Licens...			N/A	Buy

Set Up the Address Objet with Geo IP on the ZyWALL/USG

Go to **CONFIGURATION > Object > Address/Geo IP > Address > Add Address Rule**.

Add Address Rule

Name:

Address Type:

Country:

Go to **CONFIGURATION > Object > Address/Geo IP > Address**, you can see the customized GEOGRAPHY address.

+ Add Edit Remove Object References				
#	Name	Type	IPv4 Address	Refer...
1	DMZ_SUBNET	INTERFACE SUBNET	ge6-192.168.3.0/24	0
2	IP6to4-Relay	HOST	192.88.99.1	0
3	LAN_SUBNET_GE4	INTERFACE SUBNET	ge4-192.168.1.0/24	0
4	LAN_SUBNET_GE5	INTERFACE SUBNET	ge5-192.168.2.0/24	0
5	RFC1918_1	SUBNET	10.0.0.0/8	1
6	RFC1918_2	SUBNET	172.16.0.0/12	1
7	RFC1918_3	SUBNET	192.168.0.0/16	1
8	Taiwan	GEOGRAPHY	Taiwan-All	1
9	geo1	GEOGRAPHY	China-All	0
10	geo2	GEOGRAPHY	Germany-All	0

Go to **CONFIGURATION > Object > Address/Geo IP > Address Group > Add Address Group Rule**, add all customized GEOGRAPHY address into the same **Member** object.

+

Add Address Group Rule

Group members

Name:

geo_block

Description:

Address Type:

GEOGRAPHY

Member List

Available

=== Object ===

Taiwan

geo1

geo2

Member

→

←

OK

Cancel

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).

Add corresponding

Create new Object ▼

☒ Enable

Name:

Description: (Optional)

From:

To:

Source:

Destination:

Service:

User:

Schedule:

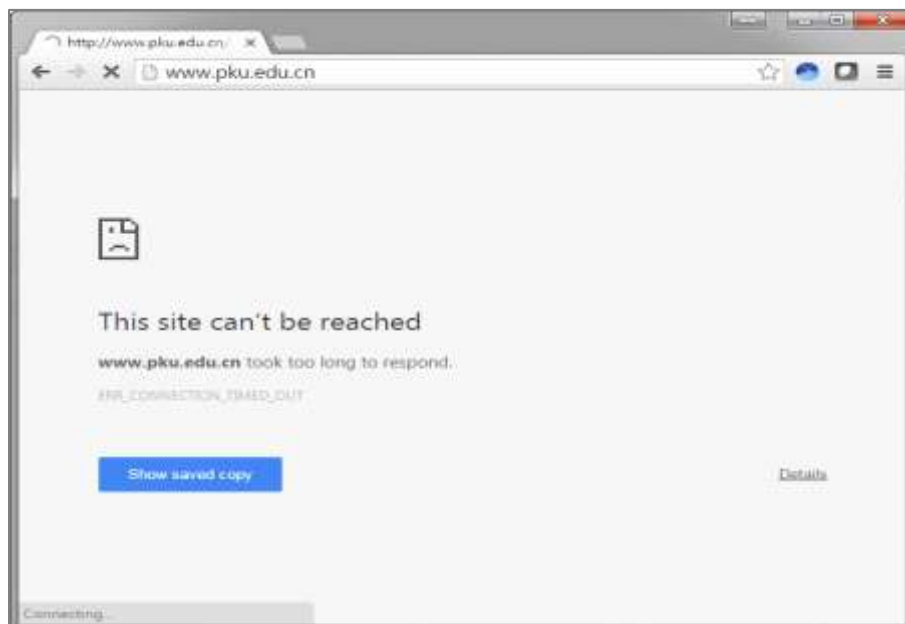
Action:

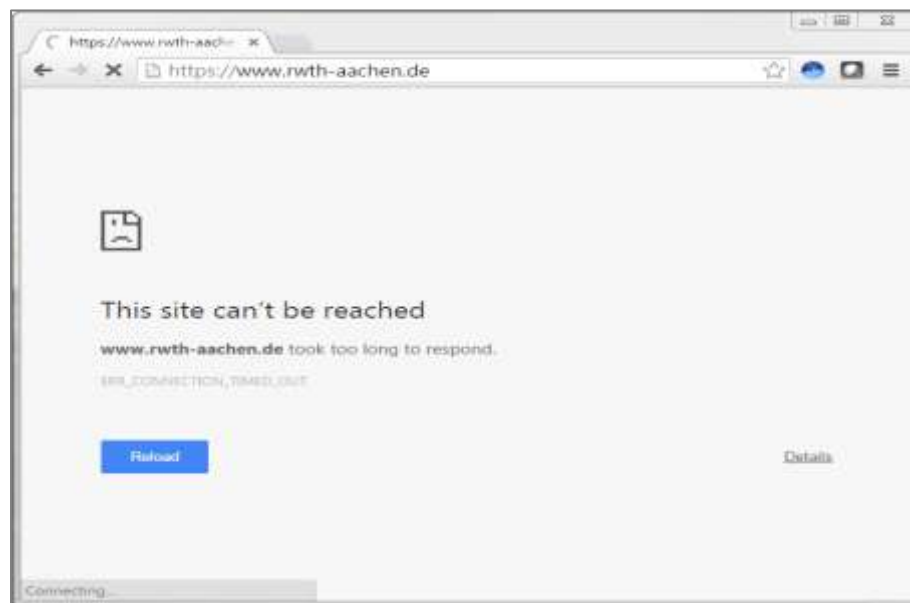
Log denied traffic:

OK Cancel

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.

Logs

Category:

All Logs

Email Log Now

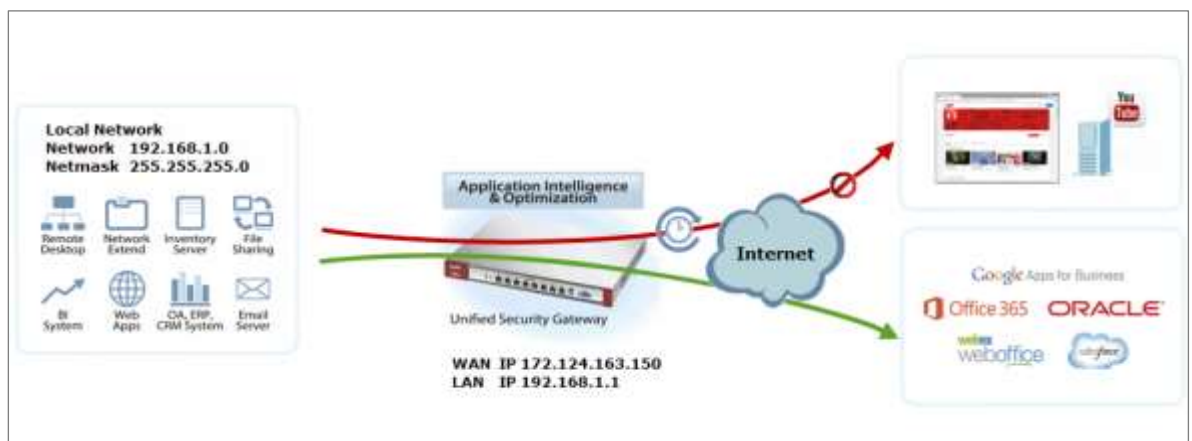
Refresh

Clear Log


#	Time	Port	Category	Message	Source	Destin...	Note
1	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2]	192.168.2.3...	61...	ACCESS BLOCK
2	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2]	192.168.2.3...	115...	ACCESS BLOCK
3	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2]	192.168.2.3...	61...	ACCESS BLOCK
4	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=2]	192.168.2.3...	115...	ACCESS BLOCK
5	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	137...	ACCESS BLOCK
6	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	137...	ACCESS BLOCK
7	2...	al...	Security P...	Match default rule, DROP [count=6]	10.214.30.3...	10.214...	ACCESS BLOCK
8	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	61...	ACCESS BLOCK
9	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	61...	ACCESS BLOCK
10	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	61...	ACCESS BLOCK
11	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	61...	ACCESS BLOCK
12	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	61...	ACCESS BLOCK
13	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	61...	ACCESS BLOCK
14	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	162...	ACCESS BLOCK
15	2...	al...	Security P...	priority:1, from LAN2 to WAN, TCP, service others, DROP [count=3]	192.168.2.3...	162...	ACCESS BLOCK

How To Schedule YouTube Access

This is an example of using the ZyWALL/USG UTM Profile and Security Policy to control access to the network. If an application should not have network access during certain hours, you can use Application Patrol, SSL Inspection and Schedule settings to make sure that these applications cannot access the Internet.



ZyWALL/USG with Scheduled YouTube Access Settings Example

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Schedule on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > Schedule > Recurring > Add Schedule Recurring Rule**. Configure a **Name** for you to identify the **Schedule Recurring Rule**. Specify the **Day Time** hour and minute when the schedule begins and ends each day. In the **Weekly** schedule, select each day of the week that the recurring schedule is effective.

CONFIGURATION > Object > Schedule > Recurring



Add Schedule Recurring Rule

Configuration

Name:

Day Time

Start Time:

Stop Time:

Weekly

Week Days:

<input checked="" type="checkbox"/> Monday	<input checked="" type="checkbox"/> Tuesday	<input checked="" type="checkbox"/> Wednesday
<input checked="" type="checkbox"/> Thursday	<input checked="" type="checkbox"/> Friday	<input type="checkbox"/> Saturday
<input type="checkbox"/> Sunday		

Create the Application Objects on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > Application > Add Application Rule**. Configure a **Name** for you to identify the **Application Profile**. Then, click **Add** to create an **Application Object**.

CONFIGURATION > Object > Application > Add Application Rule

In the **Application Object**, select **By Service**, type a keyword and click **Search** to display all signatures containing that keyword. Check all **Query Result** and Click **OK**.

CONFIGURATION > Object > Application > Add Application Rule > Add Application Object

Set Up SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select **Block** to **Action for Connection with SSL v3** and select **Log** type to be **log alert**. Leave

other actions as default settings.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule

General Settings			
Name:	Youtube_Profile		
Description:			
CA Certificate:	default		
SSL/TLS version supported minimum:	ssl3	Log:	log alert
Action for connection with unsupported suit:	pass	Log:	no
Action for connection with untrusted cert chain:	pass	Log:	log

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select the **Schedule** that defines when the policy applies (Youtube_Schedule in this example).

Scroll down to **UTM Profile**, check **Application Patrol** and select a profile from the list box (Youtube_profile in this example). Then, check **SSL Inspection** and select a profile from the list box (Youtube in this example).

CONFIGURATION > Security Policy > Policy Control

<input checked="" type="checkbox"/> Enable		
Name:	Youtube_Schedule	
Description:		[Optional]
From:	[LAN]	
To:	any (Excluding ZyV)	
Source:	any	
Destination:	any	
Service:	any	
User:	any	
Schedule:	Youtube_Schedule	
Action:	allow	
Log matched traffic:	no	

UTM Profile		
<input type="checkbox"/> Content Filter:	none	Log: by profile
<input checked="" type="checkbox"/> SSL Inspection:	Youtube_Profile	Log: by profile

Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

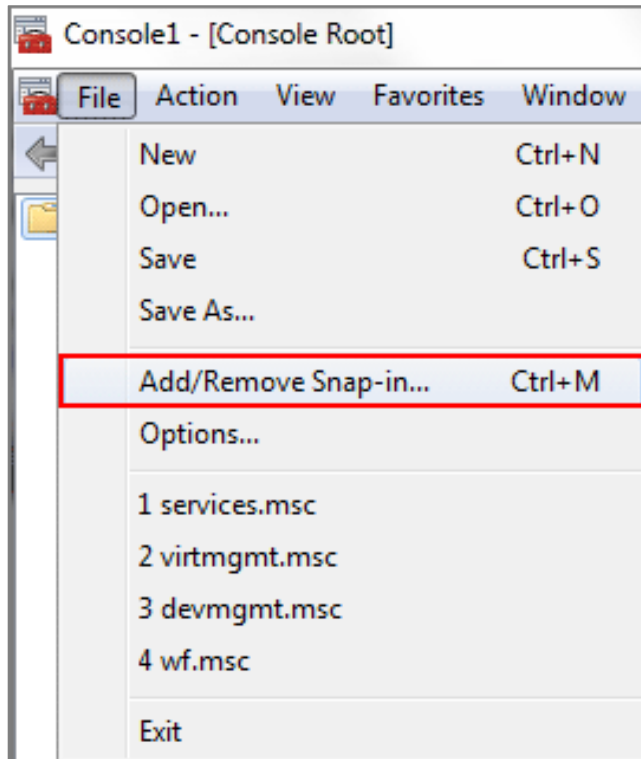
When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG.

CONFIGURATION > Object > Certificate > default

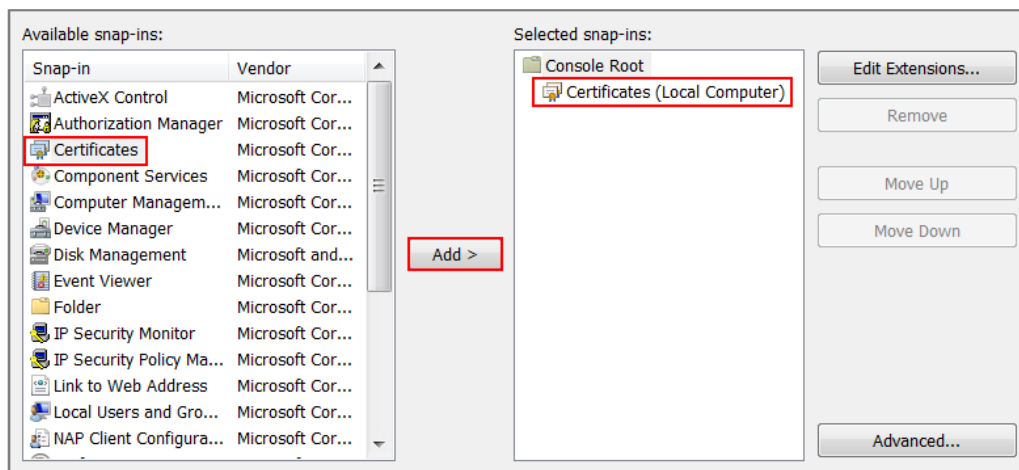
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

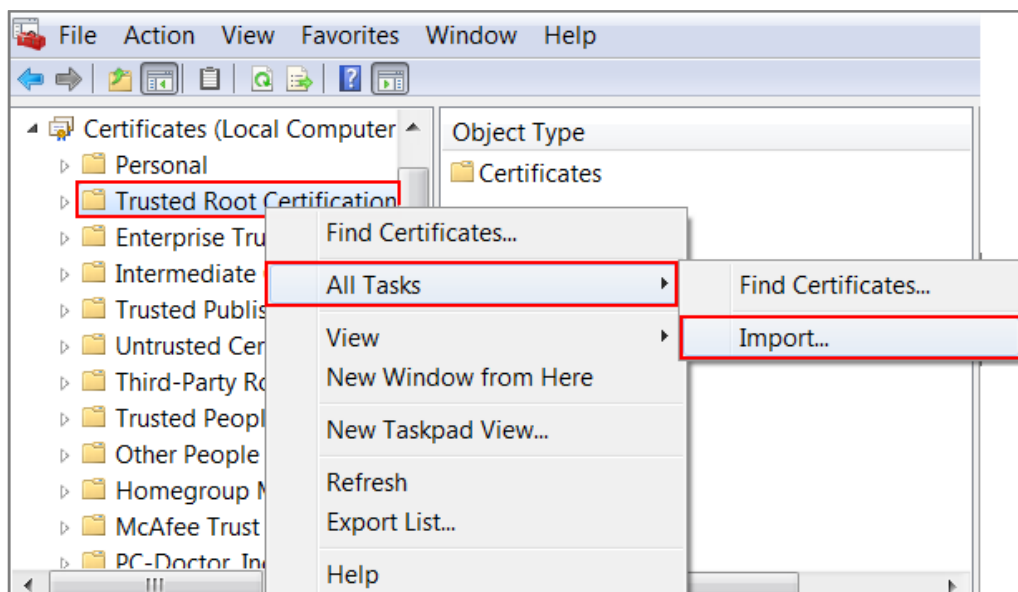


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

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**.

File to Import

Specify the file you want to import.

File name:

C:\Users\USER\Downloads\default.crt

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities**. Click **Next**, then click **Finish**.

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Browse...

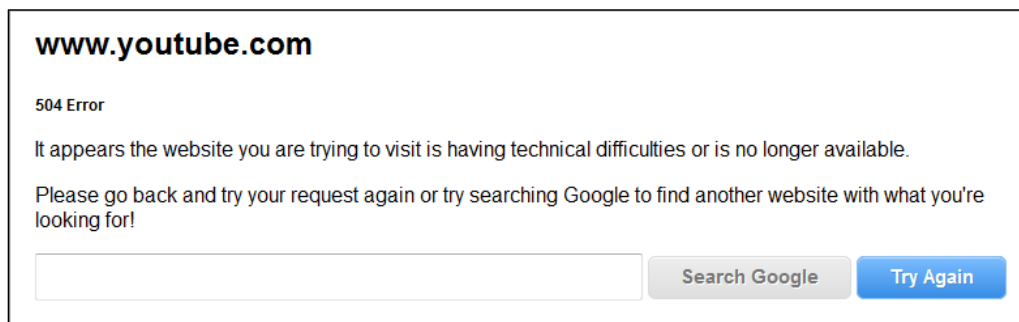


Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to the default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

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 SS=Y App=(Streaming Media)Youtube access Action=reject SID=67137542	ACCESS BLOCK
alert	Application Patrol	Rule_id=1 SS=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.

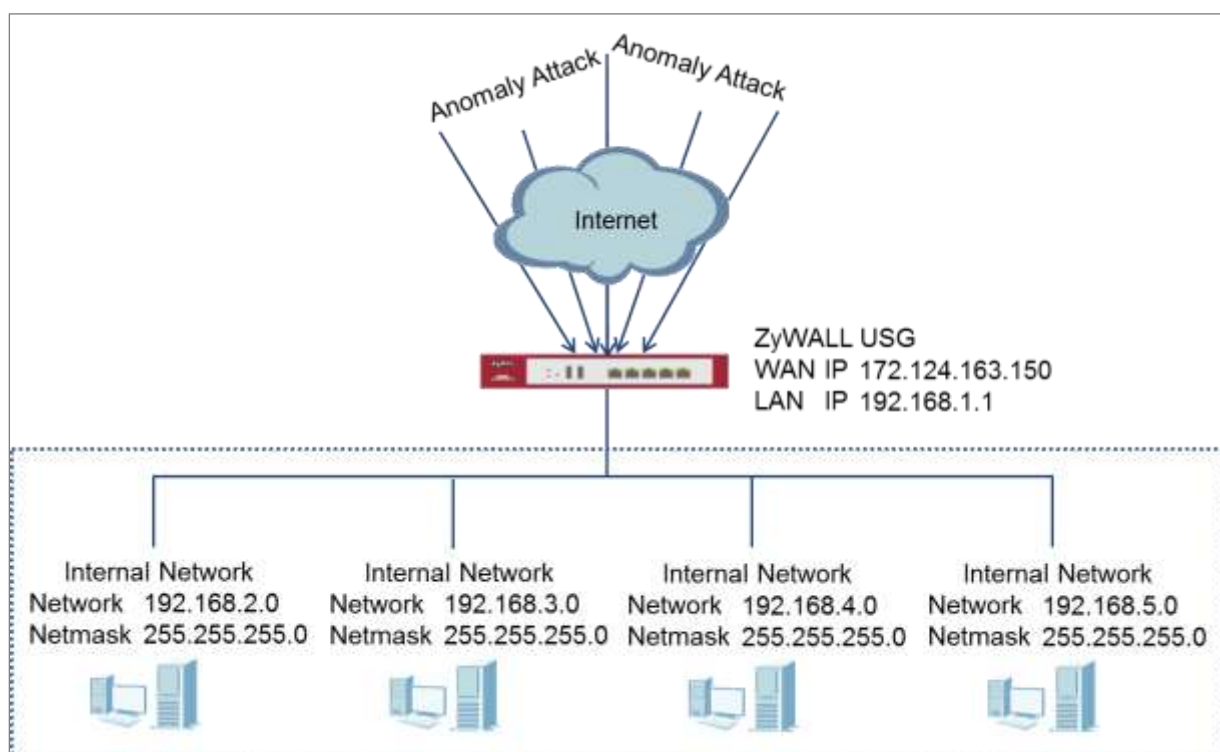
You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **Application Patrol** license.


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

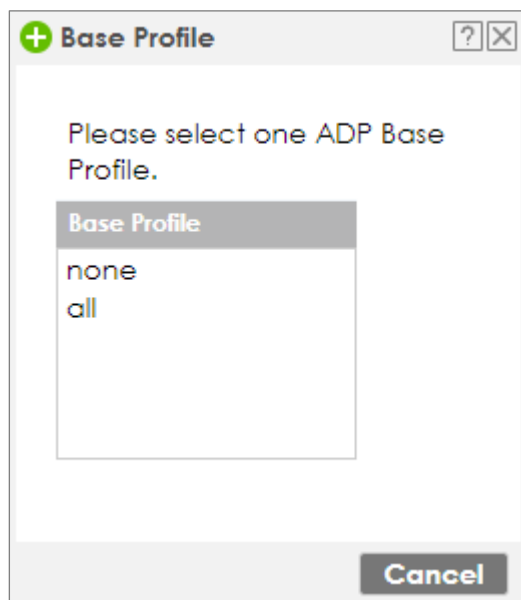


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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

General

Name: **APF1895**

Description:

Scan Detection

Sensitivity: medium

Block Period: **10** (1-3600 seconds)

☐ Activate
 ☐ Inactivate
 ☐ Log
 ☐ Action

#	Status	Name *	Log	Action
1		(portscan) IP Protocol Scan	no	none
2		(portscan) TCP Portscan	no	none
3		(portscan) UDP Portscan	no	none
4		(sweep) ICMP Sweep	no	none
5		(sweep) IP Protocol Sweep	no	none
6		(sweep) TCP Port Sweep	no	none
7		(sweep) UDP Port Sweep	no	none

Page 1 of 1
 Show 50 Items
 Displaying 1 - 7 of 7

Flood Detection

Block Period: **5** (1-3600 seconds)

☐ Edit
 ☐ Activate
 ☐ Inactivate
 ☐ Log
 ☐ Action

#	Status	Name *	Log	Action	Threshold/p...
1		(flood) ICMP Flood	no	none	1000
2		(flood) IP Flood	no	none	1000
3		(flood) TCP Flood	no	none	1000
4		(flood) UDP Flood	no	none	1000

Page 1 of 1
 Show 50 Items
 Displaying 1 - 4 of 4

Click the **Protocol Anomaly** tab. A **Name** is automatically generated that you can edit. Enable or disable individual rules by selecting a row and clicking **Activate** or **Inactivate**. Edit the default log options and actions by selecting a row and making a selection in the **Log** or **Action** drop-down menus. Click **OK**.

CONFIGURATION > Security Policy > ADP > Profile > Base Profile > Protocol Anomaly

General

Name:

Description:

TCP Decoder

☒ Activate
 ☐ Inactivate

#	Status	Name	Log	Action
1		(tcp_decoder) BAD-LENGTH-OPTI...	no	none
2		(tcp_decoder) EXPERIMENTAL-OP...	no	none
3		(tcp_decoder) OBSOLETE-OPTION...	no	none
4		(tcp_decoder) OVERSIZE-OFFSET A...	no	none
5		(tcp_decoder) TRUNCATED-OPTIO...	no	none
6		(tcp_decoder) TTCP-DETECTED AT...	no	none
7		(tcp_decoder) UNDERSIZE-LEN ATT...	no	none
8		(tcp_decoder) UNDERSIZE-OFFSET ...	no	none
9		(tcp_decoder) tcp-fragment ATTA...	no	none

Page 1 of 1 Show 50 Items Displaying 1 - 9 of 9

UDP Decoder

☒ Activate
 ☐ Inactivate

#	Status	Name	Log	Action
1		(udp_decoder) OVERSIZE-LEN ATT...	no	none
2		(udp_decoder) TRUNCATED-HEAD...	no	none
3		(udp_decoder) UNDERSIZE-LEN AT...	no	none

Page 1 of 1 Show 50 Items Displaying 1 - 3 of 3

ICMP Decoder

☒ Activate
 ☐ Inactivate

#	Status	Name	Log	Action
1		(icmp_decoder) TRUNCATED-ADD...	no	none
2		(icmp_decoder) TRUNCATED-HEA...	no	none
3		(icmp_decoder) TRUNCATED-TIME...	no	none
4		(icmp_decoder) icmp-fragment ...	no	none

Page 1 of 1 Show 50 Items Displaying 1 - 4 of 4

IP Decoder

☒ Activate
 ☐ Inactivate

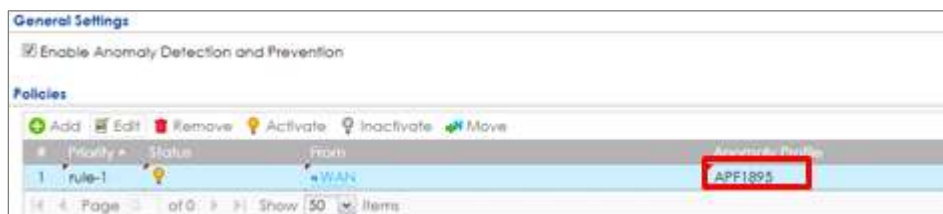
#	Status	Name	Log	Action
1		(ip_decoder) BAD-LENGTH-OPTIO...	no	none
2		(ip_decoder) IP-land ATTACK	no	none
3		(ip_decoder) TRUNCATED-OPTION...	no	none
4		(ip_decoder) UNDERSIZE-LEN ATTA...	no	none
5		(ip_decoder) ip-spoof ATTACK	no	none
6		(ip_decoder) ip-teardrop ATTACK	no	none

Page 1 of 1 Show 50 Items Displaying 1 - 6 of 6

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

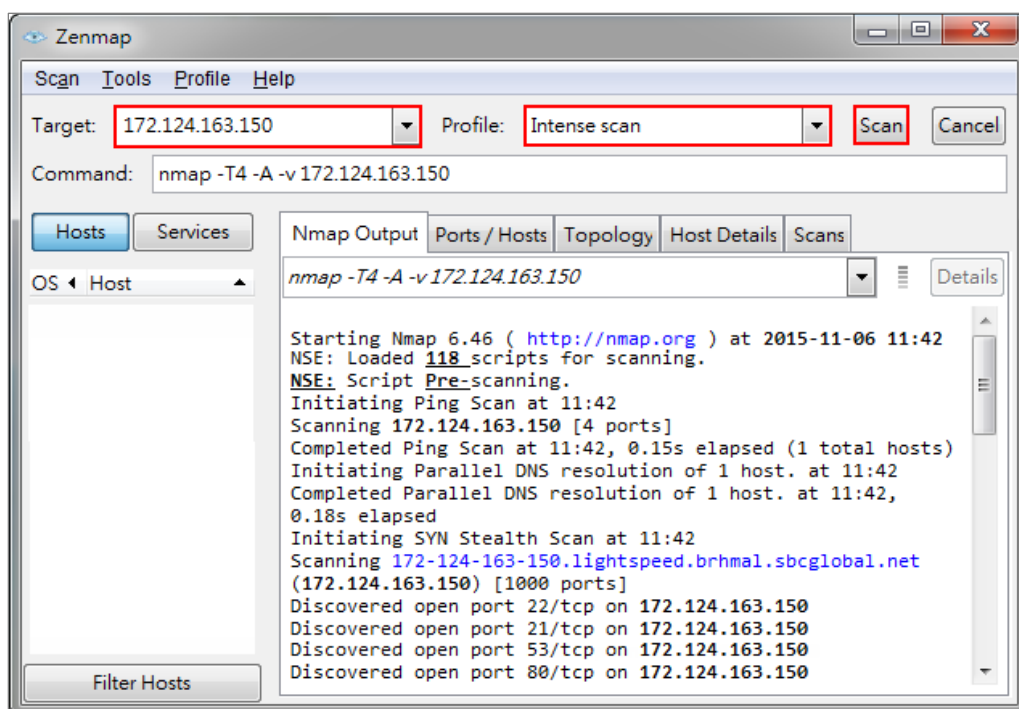


Test the Result

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

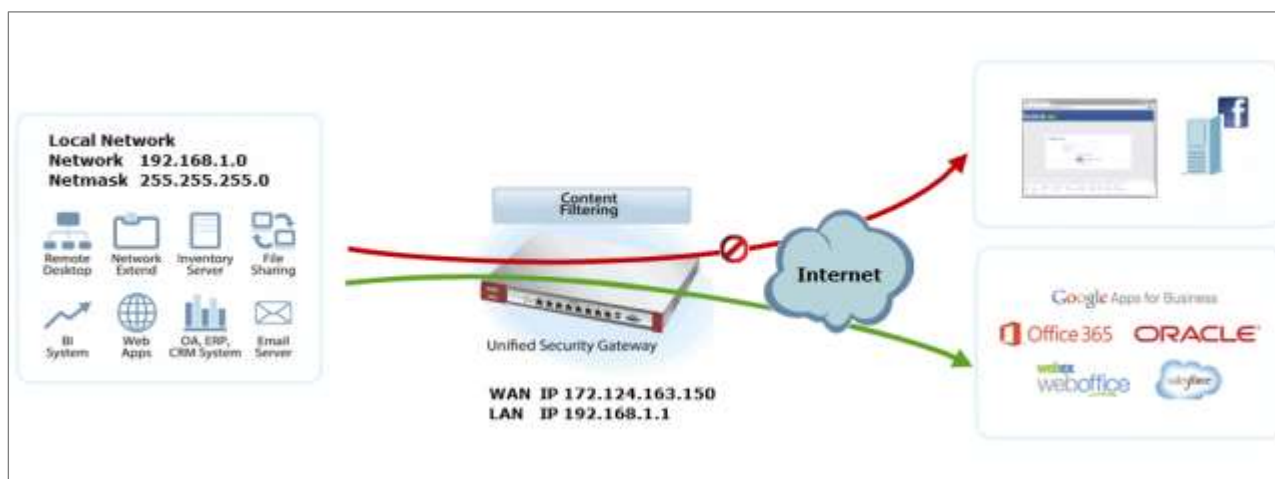
What Could Go Wrong?


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

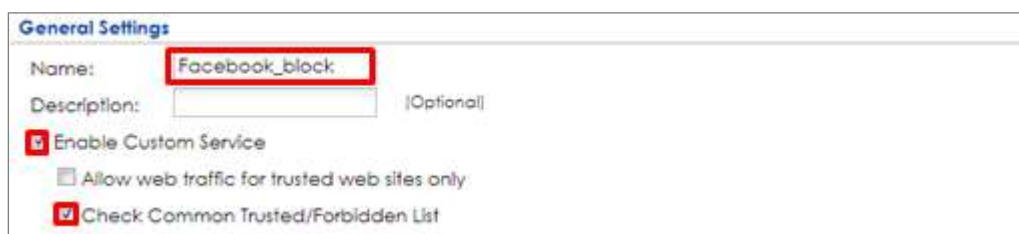


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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



General Settings

Name: **Facebook_block**

Description: [Optional]

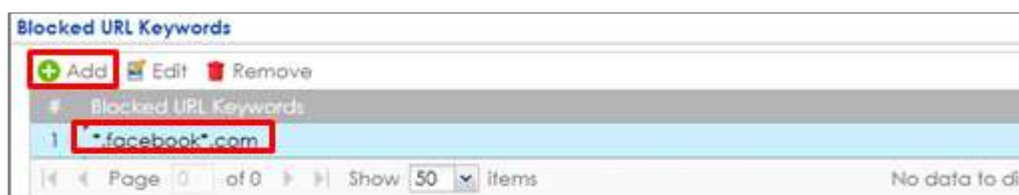
☒ Enable Custom Service

☐ Allow web traffic for trusted web sites only

☒ Check Common Trusted/Forbidden List

Scroll down to the **Blocked URL Keywords** section, click **Add** and use "*" as a wildcard to match any string in trusted/forbidden web sites and blocked URL keywords (*.facebook*.com in this example). Click **OK**.

CONFIGURATION > UTM Profile > Content Filter > Profile > Profile Management > Add Filter File > Custom Service > Blocked URL Keywords



Blocked URL Keywords

Add Edit Remove

ID	Blocked URL Keywords	Action
1	*.facebook*.com	

Page 0 of 0 Show 50 items No data to display

Set Up the SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select **Block** to **Action for Connection with SSL v3** and select **Log** type to be **log alert**. Leave other actions as default settings.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule

General Settings			
Name:	Facebook_Block		
Description:			
CA Certificate:	default		
SSL/TLS version supported minimum:	ssl3	Log:	no
Action for connection with unsupported suit:	pass	Log:	no
Action for connection with untrusted cert chain:	pass	Log:	log

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select the **Schedule** that defines when the policy applies (Facebook_Block in this

example).

Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Facebook_Block in this example). Then, select **SSL Inspection** and select a profile from the list box (Facebook_Block in this example).

CONFIGURATION > Security Policy > Policy Control

<input checked="" type="checkbox"/> Enable		
Name:	Facebook_Block	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyV)	
Source:	any	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	no	

UTM Profile		
<input checked="" type="checkbox"/> Content Filter:	Facebook_Block	Log: by profile
<input checked="" type="checkbox"/> SSL Inspection:	Facebook_Block	Log: by profile

Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG.

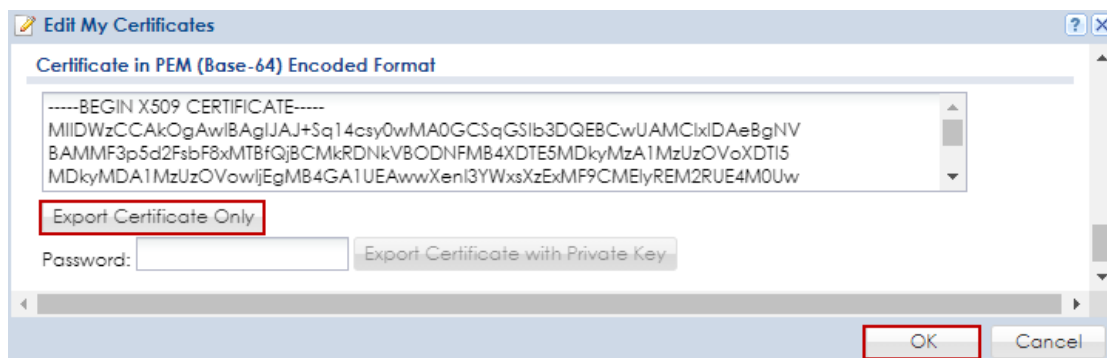
CONFIGURATION > Object > Certificate > default



#	Name	Type	Subject	Issuer	Valid From	Valid To
1	default	SELF	CN=vpn300_B8ECA3A9C...	CN=vpn300_B8ECA3A9C...	2017-04-25 12:41:25 GMT	2027-04-23 12:41:25 GMT

Page 1 of 1 | Show 50 Items | Displaying 1 - 1 of 1

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only



Edit My Certificates

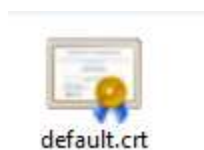
Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN X509 CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIJUJ+Sq14csyOwMA0GCSqGSIb3DQEBCwUAMCxiDAeBgNV
BAMMF3p5d2FsbF8xMTBfQjBjCMkRDnkVBODNFMB4XDTE5MDkyMzA1MzUzOV0XDTI5
MDkyMDA1MzUzOV0wIjEgMB4GA1UEAwwXenl3YWxsXzExMF9CMEl5REM2RUE4M0Uw
-----
```

Export Certificate Only

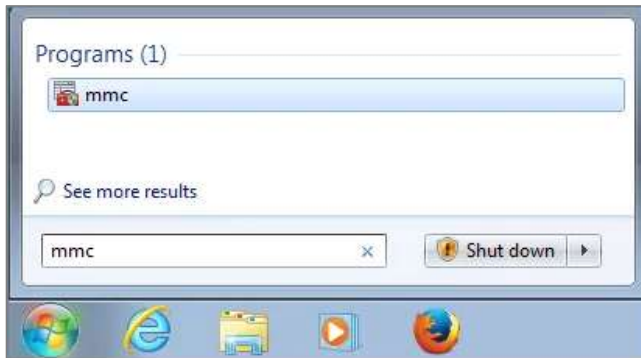
Password:

Save default certificate as *.crt file to Windows 7 Operation System.



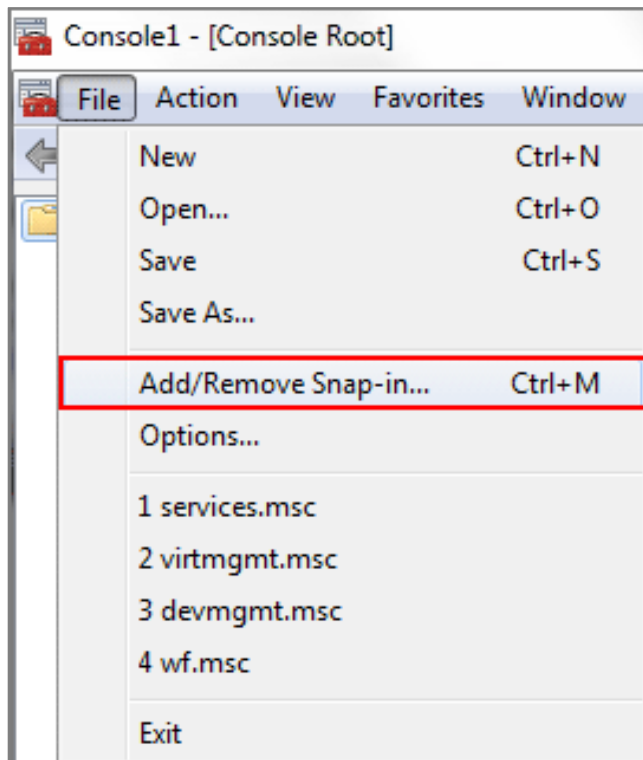
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



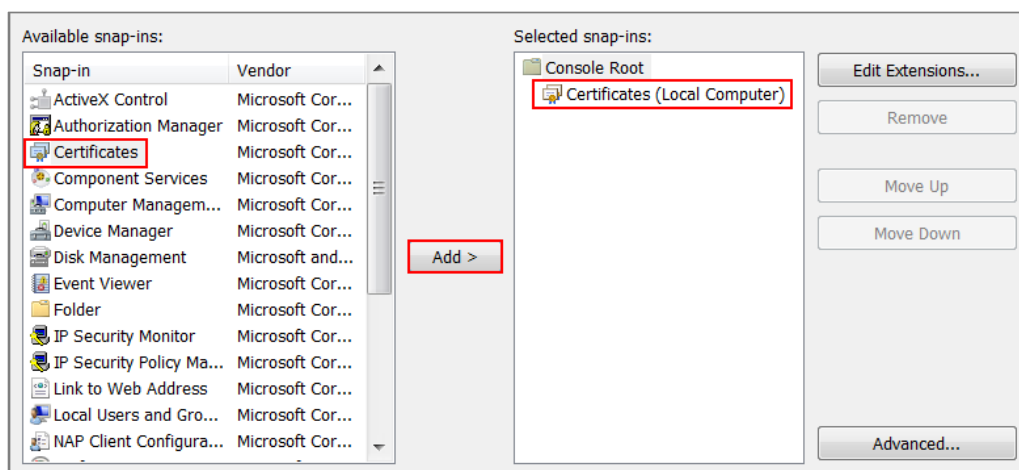
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

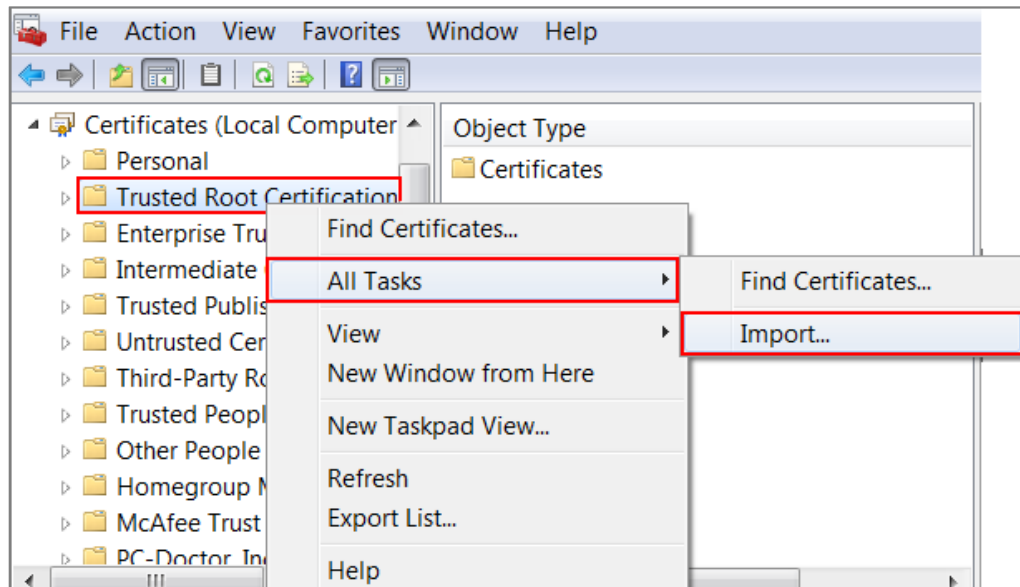


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

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**.

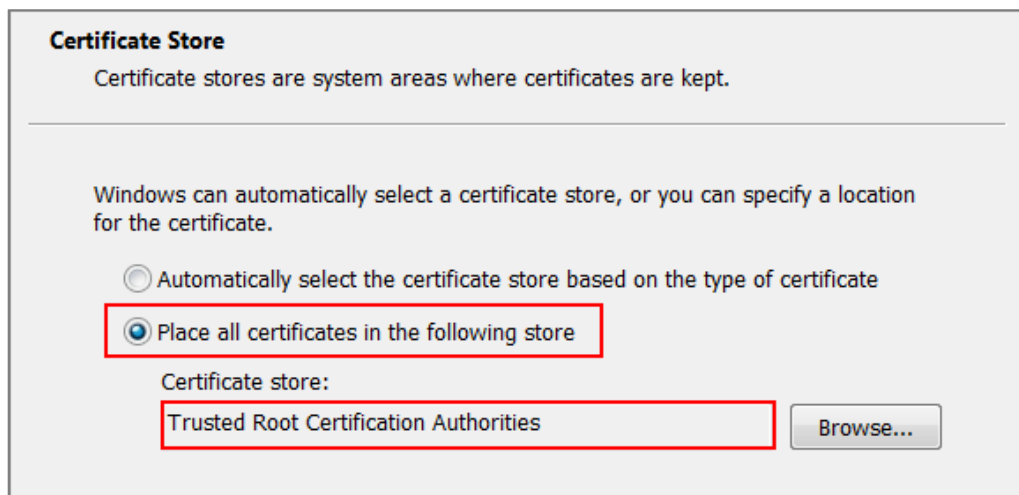
File to Import
Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities**. Click **Next**, then click **Finish**.



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.

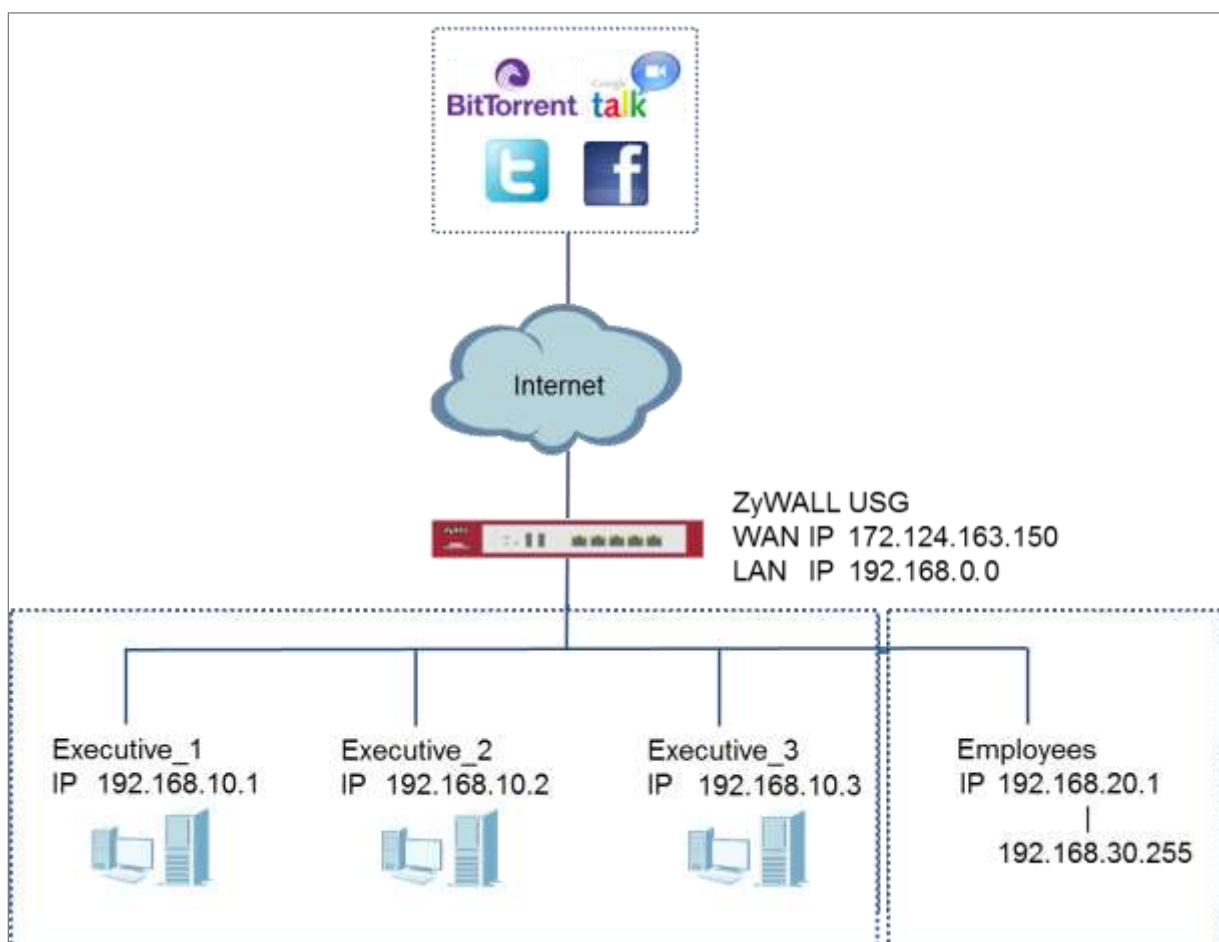
You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **Content Filter** license.


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

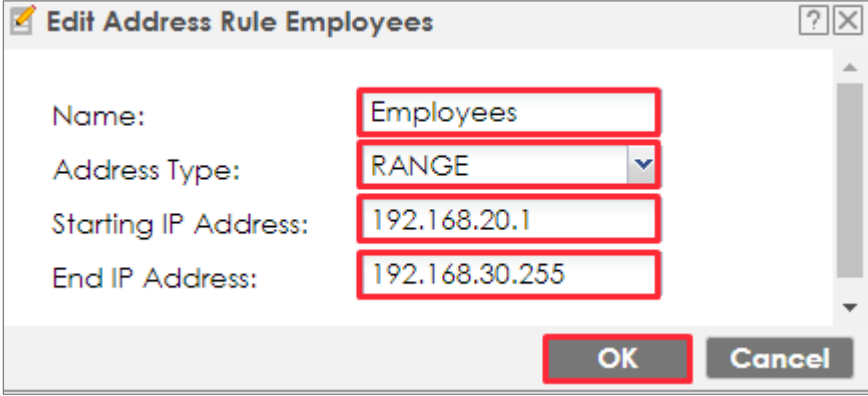


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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

<input checked="" type="checkbox"/> Enable		
Name:	Employees Security	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyV	
Source:	Employees	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	log	

UTM Profile		
<input checked="" type="checkbox"/>	Content Filter:	Office profile
<input type="checkbox"/>	SSL Inspection:	none
	Log:	by profile
	Log:	by profile

Set Up the Security Policy on the ZyWALL/USG for Executives

In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create address for each executives.

CONFIGURATION > Object > Address > Add Address Rule

+

Add Address Rule

?

✕

Name:

Executive_1

Address Type:

HOST

▼

IP Address:

192.168.10.1

OK

Cancel

+

Add Address Rule

?

✕

Name:

Executive_2

Address Type:

HOST

▼

IP Address:

192.168.10.2

OK

Cancel

+

Add Address Rule

?

✕

Name:

Executive_3

Address Type:

HOST

▼

IP Address:

192.168.10.3

OK

Cancel

Then, go to **CONFIGURATION > Object > Address Group > Add Address Group Rule** to create a **Group Members' Name** and move the just created executives address object to **Member**.

CONFIGURATION > Object > Address Group > Add Address Group Rule

Configuration

Name:

Description: (Optional)

Member List

Available		Member
=== Object ===		
ad-users		
ldap-users		
radius-users		
Executive_1	<input checked="" type="checkbox"/>	
Executive_2	<input checked="" type="checkbox"/>	
Executive_3	<input checked="" type="checkbox"/>	

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

<input checked="" type="checkbox"/> Enable	
Name:	Executive_Security
Description:	(Optional)
From:	LAN
To:	any (Excluding ZyV)
Source:	any
Destination:	any
Service:	any
User:	Executive
Schedule:	none
Action:	allow
Log matched traffic:	log

Test the Result

Connect to the Internet from two computers: one from executive_2 address (192.168.10.2) and one from an employee address (192.168.20.1) and both access to <https://hangouts.google.com/>.

Go to the ZyWALL/USG **Monitor > Log**, you will see [notice] and [info] log message such as below. In this example result, connections from executive_2 address (192.168.10.2) use **Security Policy** priority: 1. Connections from employee address (192.168.20.1) use **Security Policy** priority: 2 and **UTM Profile** Rule_id=2.

Priority	Category	Message	Source	Destination	Note
notice	Security Policy Control	priority:1, from LAN to ANY, TCP, service others, ACCEPT	192.168.10.2:52549	172.23.6.115:5088	ACCESS FORWARD
notice	Security Policy Control	priority:1, from LAN to ANY, TCP, service others, ACCEPT	192.168.10.2:54956	64.233.189.125:5222	ACCESS FORWARD

Priority	Category	Message	Source	Destination	Note
info	Application Patrol	Rule_id=2 SSN 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 SSN App=(Social Network)Google-plus authority Action=reject SID=402692087	192.168.20.1:53688	74.125.203.102:443	ACCESS BLOCK

What Could Go Wrong?

If you are not be able to configure any **UTM** policies or it's not working, there are two possible reasons:

You have not subscribed for the **UTM** service.

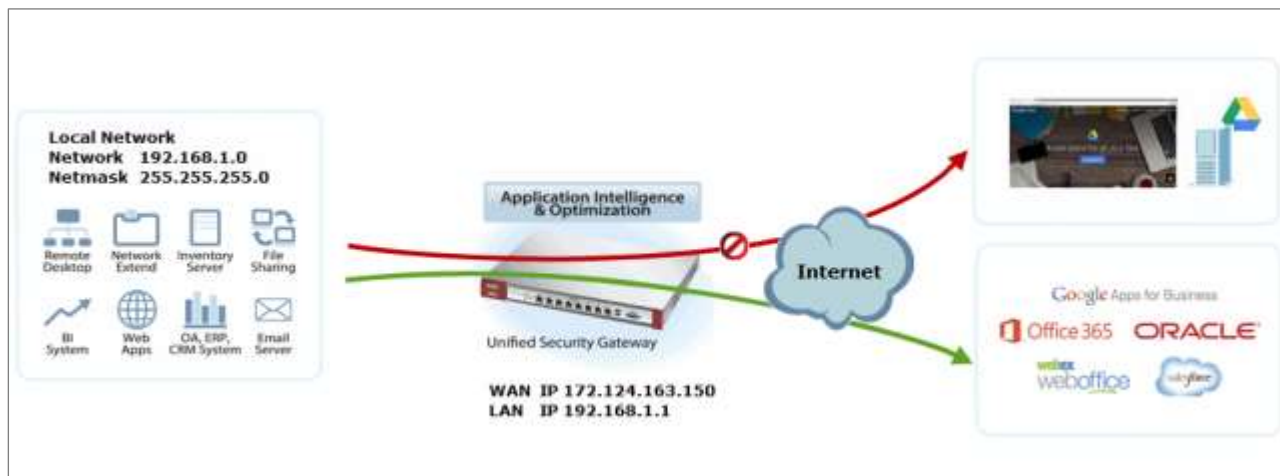
You have subscribed for the **UTM** service but the license is expired.


You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **UTM** license.

How to Control Access To Google Drive

This is an example of using a ZyWALL/USG UTM Profile in a Security Policy to block access to a specific file transfer service. You can use Application Patrol and Policy Control to make sure that a certain file transfer service cannot be accessed through both HTTP and HTTPS protocols.

ZyWALL/USG with Control Access To Google Drive Settings Example



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select **Block** to **Action for Connection with SSL v3** and select **Log** type to be **log alert**. Leave other actions as default settings.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule

General Settings			
Name:	Google Drive Contr		
Description:			
CA Certificate:	default		
SSL/TLS version supported minimum:	ssl3	Log:	log alert
Action for connection with unsupported suit:	pass	Log:	no
Action for connection with untrusted cert chain:	pass	Log:	log

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies.

Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Facebook_Block in this example). Then, select **SSL Inspection** and select a profile from the list box (Facebook_Block in this example).

CONFIGURATION > Security Policy > Policy Control

<input checked="" type="checkbox"/> Enable		
Name:	Google_Drive_Contr	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyV	
Source:	any	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	no	

UTM Profile		
<input type="checkbox"/>	Content Filter:	none
<input checked="" type="checkbox"/>	SSL Inspection:	Google_Drive_Cor

Export Certificate from ZyWALL/USG and Import it to Windows 7 Operation System

When SSL inspection is enabled and an access website does not trust the ZyWALL/USG certificate, the browser will display a warning page of security certificate problems.

Go to ZyWALL/USG **CONFIGURATION > Object > Certificate > default > Edit** to export default certificate from ZyWALL/USG.

CONFIGURATION > Object > Certificate > default

My Certificates Setting					
Add Edit Remove Object References					
Name	Type	Subject	Issuer	Valid from	Valid to
1 default	SELF	CN=vpn300_B8ECA3A9C...	CN=vpn300_B8ECA3A9C...	2017-04-25 12:41:25 GMT	2027-04-23 12:41:25 GMT
Page 1 of 1 Show 50 Items Displaying 1 of 1					

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only

Edit My Certificates

Certificate in PEM (Base-64) Encoded Format

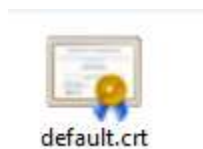
```
-----BEGIN X509 CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIJAJ+Sq14csyOwMA0GCSqGSIb3DQEBCwUAMCxiDAeBgNV
BAMMF3p5d2FsbF8xMTBfGjBCMkRDNkVBODNFMB4XDTE5MDkyMzA1MzUzOVoXDTE5
MDkyMDA1MzUzOVowIjEgMB4GA1UEAwwXenI3YWxsXzExMF9CMElyREM2RUE4M0Uw
```

Export Certificate Only

Password: Export Certificate with Private Key

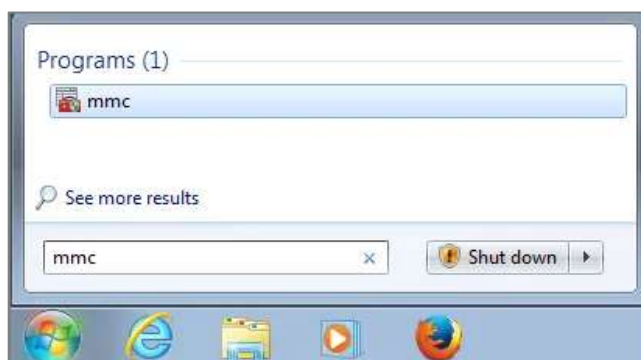
OK Cancel

Save default certificate as *.crt file to Windows 7 Operation System.



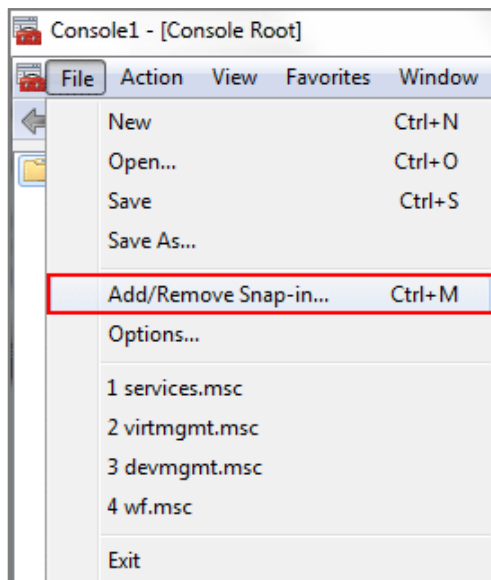
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



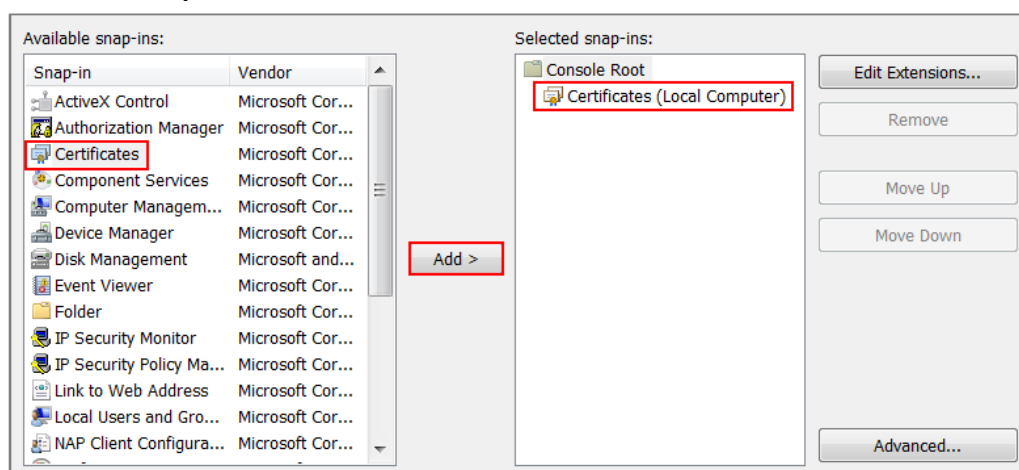
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

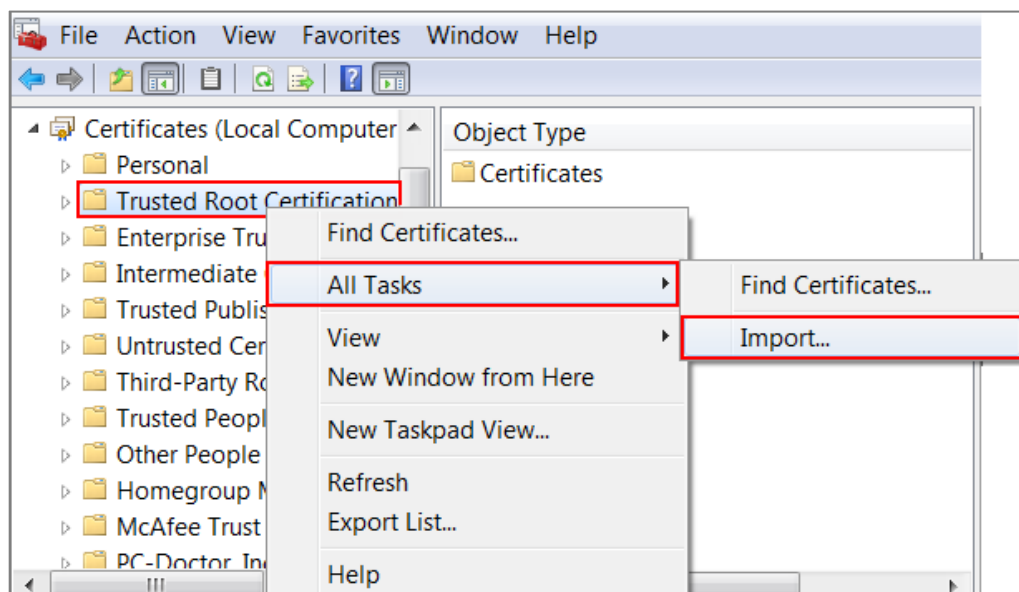


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

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**.

File to Import
Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities**. Click **Next**, then click **Finish**.

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.


☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Browse...

 Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

Test the Result

Type <http://drive.google.com/> or <https://drive.google.com/> into the browser, the error message occurs.

google.drive

502 Error

It appears the website you are trying to visit is having technical difficulties or is no longer available.

Please go back and try your request again or try searching Google to find another website with what you're looking for!

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

Monitor > Log

Priority	Category	Message	Note
alert	Application Patrol	Rule_id=1 SSI=Y App=[File Transfer]Google-drive:access Action=reject SID=50335494	ACCESS BLOCK
alert	Application Patrol	Rule_id=1 SSI=Y App=[File Transfer]Google-drive:access Action=reject SID=50335494	ACCESS BLOCK

What Could Go Wrong?

If you are not be able to configure any **Application Patrol** policies or it's not working, there are two possible reasons:

You have not subscribed for the **Application Patrol** service.

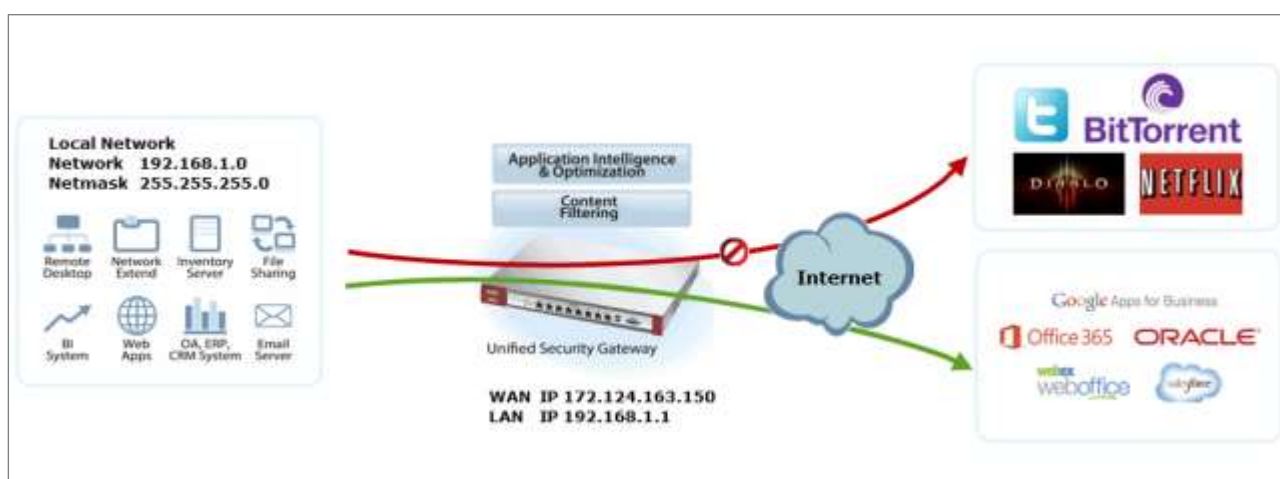
You have subscribed for the **Application Patrol** service but the license is expired.


You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **Application Patrol** license.

How to Block HTTPS Websites Using Content Filtering and SSL Inspection

This is an example of using a ZyWALL/USG Content Filtering, SSL Inspection and Security Policy to block access to malicious or not business-related websites.

ZyWALL/USG with Block HTTPS Websites Using Content Filtering and SSL Inspection Settings Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Content Filter on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > Content Filter > Profile Management > Add Filter File > Category Service**. Configure a **Name** for you to identify the **Content Filter Profile** and select **Enable Custom Service**.

CONFIGURATION > UTM Profile > Content Filter > Profile > Profile Management > Add > Category Service > General Settings

General Settings

License Status: Licensed
License Type: Standard
Name: Office_Profile
Description: (Optional)

☐ Enable SafeSearch
☒ Enable Content Filter Category Service

☐ Log all web pages

Action for Unsafe Web Pages: Block

☐ Log

Action for Managed Web Pages: Block

☐ Log

Action for Unrated Web Pages: Warn

☐ Log

Action When Category Server Is Unavailable: Warn

☐ Log

Scroll down to the **Security Threat (unsafe)** section and select all categories of web pages that are known to pose a threat to your computers.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Category Service > Security Threat (unsafe)

Security Threat (unsafe)		
<input checked="" type="checkbox"/> Anonymizers	<input checked="" type="checkbox"/> Botnets	<input checked="" type="checkbox"/> Compromised
<input checked="" type="checkbox"/> Malware	<input checked="" type="checkbox"/> Network Errors	<input checked="" type="checkbox"/> Parked Domains
<input checked="" type="checkbox"/> Phishing & Fraud	<input checked="" type="checkbox"/> Spam Sites	

Scroll down to the **Managed Categories** section and select the categories that are not business-related. Click **OK**.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Category Service > Managed Categories

Managed Categories		
<input checked="" type="checkbox"/> Advertisements & Pop-Ups	<input checked="" type="checkbox"/> Alcohol/Tobacco	<input type="checkbox"/> Arts
<input type="checkbox"/> Business	<input type="checkbox"/> Transportation	<input type="checkbox"/> Chat
<input type="checkbox"/> Forums & Newsgroups	<input type="checkbox"/> Computers & Technology	<input checked="" type="checkbox"/> Criminal Activity
<input checked="" type="checkbox"/> Dating & Personals	<input type="checkbox"/> Download Sites	<input type="checkbox"/> Education
<input type="checkbox"/> Entertainment	<input type="checkbox"/> Finance	<input checked="" type="checkbox"/> Gambling
<input checked="" type="checkbox"/> Games	<input type="checkbox"/> Government	<input checked="" type="checkbox"/> Hate & Intolerance
<input type="checkbox"/> Health & Medicine	<input checked="" type="checkbox"/> Illegal Drugs	<input type="checkbox"/> Job Search
<input checked="" type="checkbox"/> Streaming Media & Downloads	<input type="checkbox"/> News	<input type="checkbox"/> Non-profits & NGOs
<input checked="" type="checkbox"/> Nudity	<input type="checkbox"/> Personal Sites	<input type="checkbox"/> Politics
<input checked="" type="checkbox"/> Pornography/Sexually Explicit	<input type="checkbox"/> Real Estate	<input type="checkbox"/> Religion
<input type="checkbox"/> Restaurants & Dining	<input type="checkbox"/> Search Engines/Portals	<input type="checkbox"/> Shopping
<input checked="" type="checkbox"/> Social Networking	<input type="checkbox"/> Sports	<input type="checkbox"/> Translators
<input type="checkbox"/> Travel	<input checked="" type="checkbox"/> Violence	<input checked="" type="checkbox"/> Weapons
<input type="checkbox"/> Web-based Email	<input type="checkbox"/> General	<input type="checkbox"/> Leisure & Recreation
<input checked="" type="checkbox"/> Cults	<input type="checkbox"/> Fashion & Beauty	<input type="checkbox"/> Greeting Cards
<input checked="" type="checkbox"/> Hacking	<input checked="" type="checkbox"/> Illegal Software	<input type="checkbox"/> Image Sharing
<input type="checkbox"/> Information Security	<input type="checkbox"/> Instant Messaging	<input checked="" type="checkbox"/> Peer to Peer
<input type="checkbox"/> Private IP Addresses	<input checked="" type="checkbox"/> School Cheating	<input checked="" type="checkbox"/> Sex Education
<input checked="" type="checkbox"/> Tasteless	<input checked="" type="checkbox"/> Child Abuse Images	

If you are not sure which category a web page belongs to, you can enter a web site URL in the text box of **Test Web Site Category**.

CONFIGURATION > UTM Profile> Content Filter > Profile > Profile Management > Add Filter File > Category Service > Test Web Site Category

Test Web Site Category	
URL to test:	<input type="text" value="https://www.youtube.com"/>
<input type="button" value="Test Against Content Filter Category Server"/>	

Set Up SSL Inspection on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > SSL Inspection > Add rule**, and configure a **Name** for you to identify the **SSL Inspection** profile.

Then, select the **CA Certificate** to be the certificate used in this profile. Select to **pass** or **block** SSLv2/unsupported suit/untrusted cert chain traffic that matches traffic bound to this policy here.

Select desired **Log** type whether to have the ZyWALL/USG generate a log (log), log and alert (log alert) or neither (no) by default when traffic matches this policy.

CONFIGURATION > UTM Profile > SSL Inspection > Add rule

General Settings			
Name:	<input type="text" value="Office_Control"/>		
Description:	<input type="text"/>		
CA Certificate:	<input type="text" value="default"/>		
SSL/TLS version supported minimum:	<input type="text" value="ssl3"/>	Log:	<input type="text" value="no"/>
Action for connection with unsupported suit:	<input type="text" value="pass"/>	Log:	<input type="text" value="no"/>
Action for connection with untrusted cert chain:	<input type="text" value="pass"/>	Log:	<input type="text" value="log"/>

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control**, configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies.

Scroll down to **UTM Profile**, select **Content Filter** and select a profile from the list box (Office_profile in this example). Then, select **SSL Inspection** and select a profile from the list box (Office_Control in this example).

CONFIGURATION > Security Policy > Policy Control

<input checked="" type="checkbox"/> Enable		
Name:	Office_Control	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyV	
Source:	any	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	no	

UTM Profile		
<input checked="" type="checkbox"/>	Content Filter:	Office_profile
<input checked="" type="checkbox"/>	SSL Inspection:	Office_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.

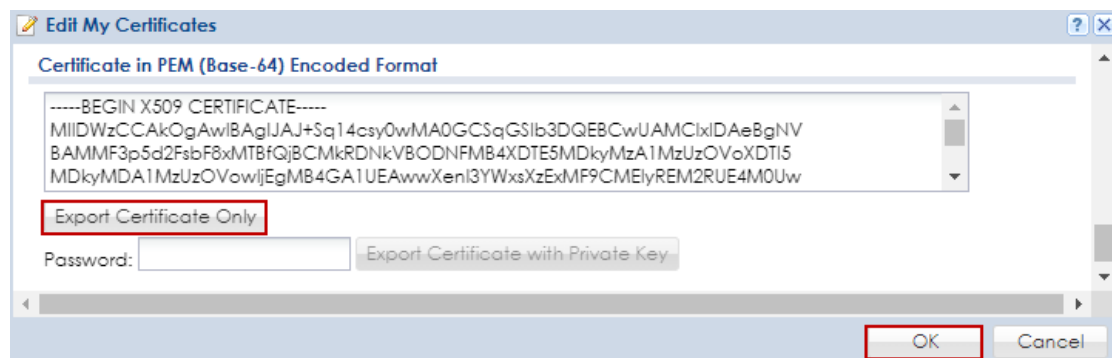
CONFIGURATION > Object > Certificate > default



#	Name	Type	Subject	Issuer	Valid from	Valid To
1	default	SELF	CN=vpn300_88ECA3A9C...	CN=vpn300_88ECA3A9C...	2017-04-25 12:41:25 GMT	2027-04-23 12:41:25 GMT

Page 1 of 1 | Show 50 items | Displaying 1 - 1 of 1

CONFIGURATION > Object > Certificate > default > Edit > Export Certificate Only



Edit My Certificates

Certificate in PEM (Base-64) Encoded Format

```
-----BEGIN X509 CERTIFICATE-----
MIIDWzCCAkOgAwIBAgIJAJ+Sq14csy0wMA0GCSqGSIb3DQEBCwUAMCxlDAe8gNV
BAMMF3p5d2FsbF8xMTBfQjBCMkRDnkVBODNFMB4XDTE5MDkyMzA1MzUzOVoXDTI5
MDkyMDA1MzUzOVowijEgMB4GA1UEAwwXenI3YWxsXzExMF9CMEl5REM2RUE4M0Uw
-----
```

Export Certificate Only

Password: Export Certificate with Private Key

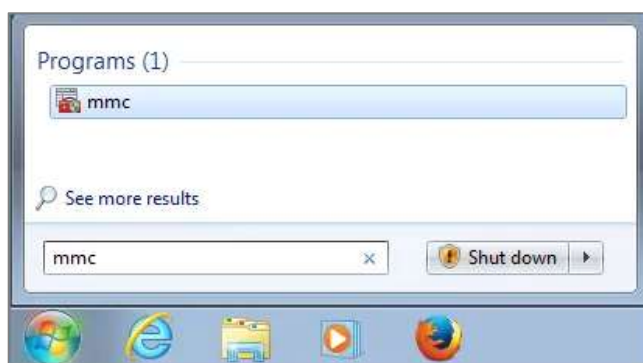
OK Cancel

Save default certificate as *.crt file to Windows 7 Operation System.



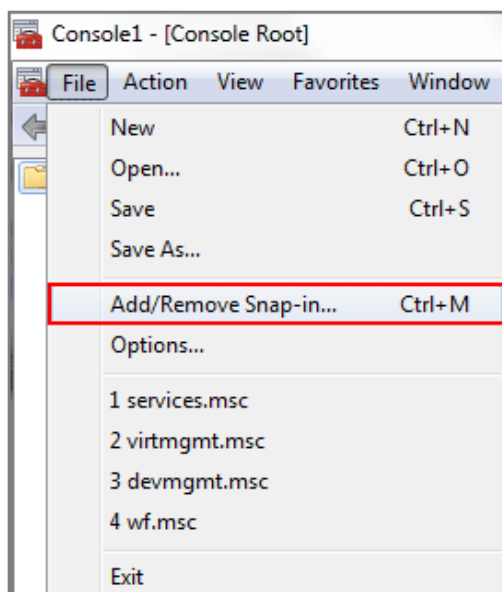
In Windows 7 Operating System **Start Menu > Search Box**, type **mmc** and press **Enter**.

Start Menu > Search Box > mmc



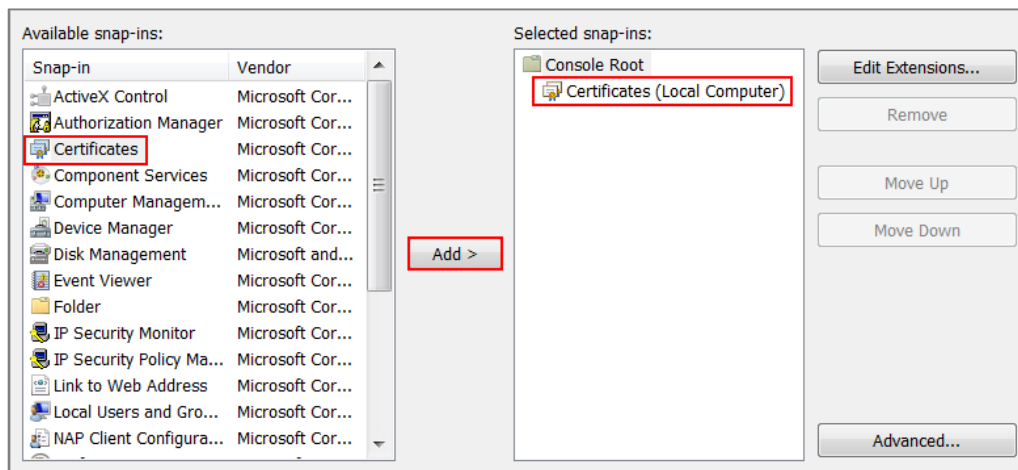
In the mmc console window, click **File > Add/Remove Snap-in...**

File > Add/Remove Snap-in...

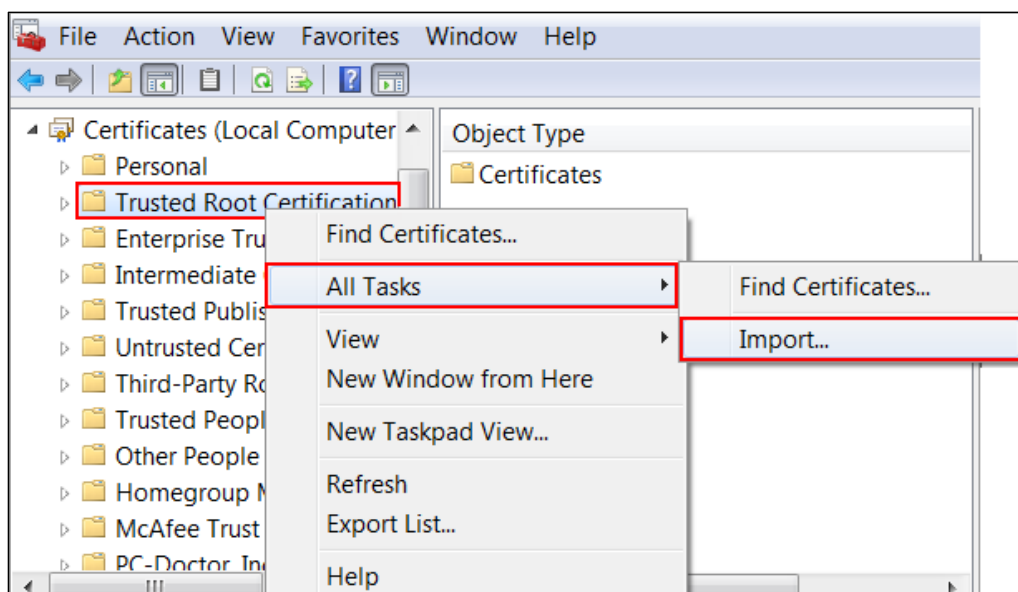


In the **Available snap-ins**, select the **Certificates** and click **Add** button. Select **Computer account > Local Computer**. Then, click **Finished** and **OK** to close the **Snap-ins** window.

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**.

File to Import

Specify the file you want to import.

File name:

C:\Users\USER\Downloads\default.crt

Browse...

Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Select **Place all certificates in the following store** and then click **Browse** and find **Trusted Root Certification Authorities**. Click **Next**, then click **Finish**.

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

☐ Automatically select the certificate store based on the type of certificate

☒ Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

Browse...

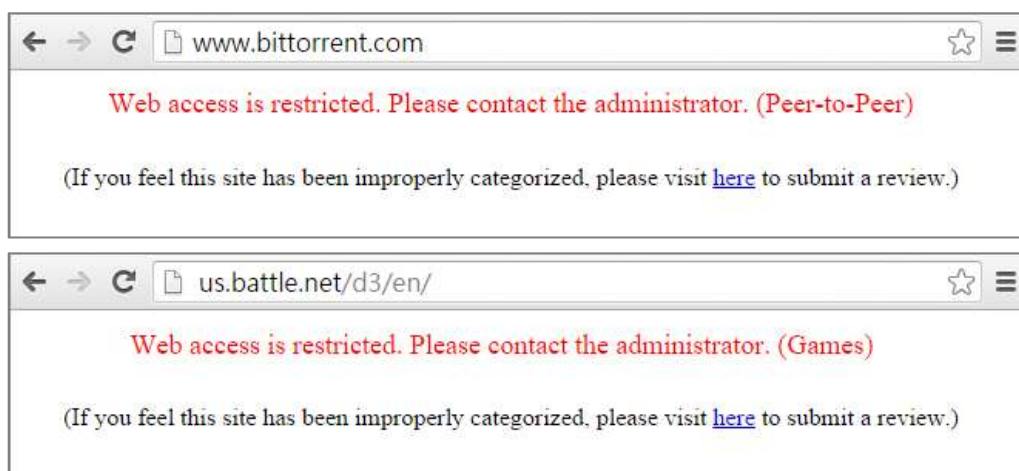


Note: Each ZyWALL/USG device has its own self-signed certificate by factory default. When you reset to default configuration file, the original self-signed certificate is erased, and a new self-signed certificate will be created when the ZyWALL/USG boots the next time.

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.

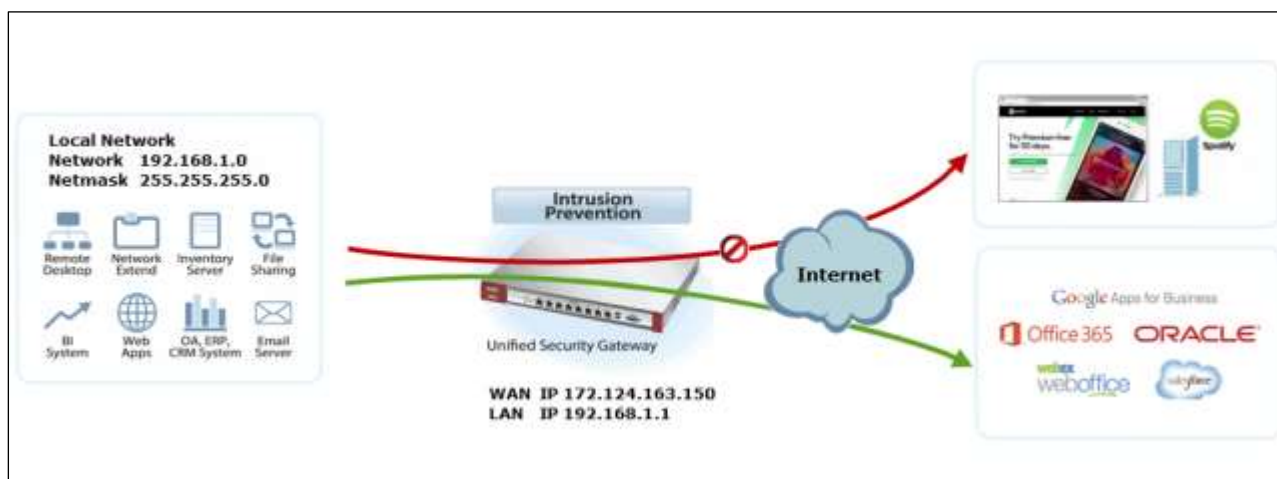
You have subscribed for the **Content Filter** service but the license is expired.


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 Spotify's public server. In this example, you can create a custom IDP to block DNS query packet if this packet includes the Spotify signature.

ZyWALL/USG with Block the Spotify Service Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up IDP Profile on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > IDP > Custom Signatures > Add Custom Signatures**, configure a **Name** for you to identify the IDP Profile. Select **medium** as the **Severity** level. Select all **Platform**. Select **Policy Type** to be **Access-Control** here to limit access network resources such as servers.

CONFIGURATION > Security Policy > IDP > Custom Signatures > Add Custom Signatures > Setup & Information

Setup

Name: Spotify
Signature ID: 9986234

Information

Severity: medium

Platform:

- ☒ Windows
- ☒ Linux
- ☒ FreeBSD
- ☒ Solaris
- ☒ Other-Unix
- ☒ Network-Device
- ☒ MAC
- ☒ iOS
- ☒ Android
- ☒ Windows-Mobile
- ☒ Symbian
- ☒ Others

Policy Type: Access-Control

Scroll down to the **Payload Options** section, the type Spotify's software signature: |73||70||6F||74||69||66||79| into the **Content** field. Click **OK**.

CONFIGURATION > Security Policy > IDP > Custom Signatures > Add Custom Signatures > Payload Options

Payload Options

Payload Size: [] Bytes

#	Offset	Content	Case-insensitive	Decode as URI
1	0	73 70 6F 74 69 66 79	no	no

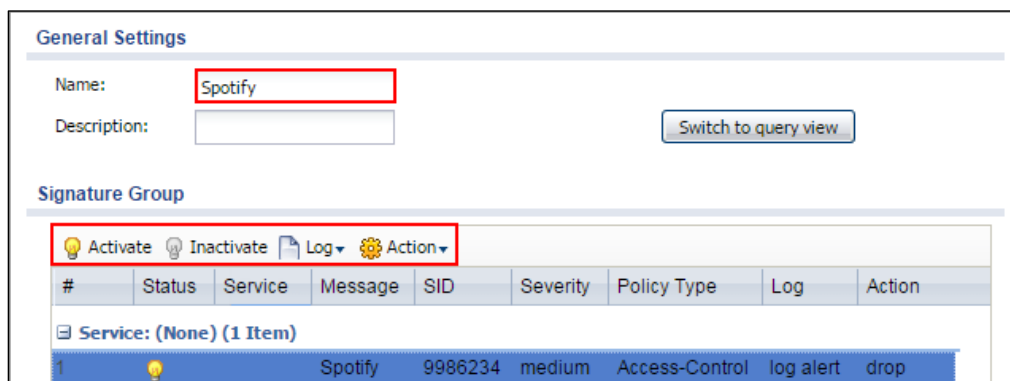
In the ZyWALL/USG, go to **CONFIGURATION > UTM Profile > IDP > Profile > Base Profile**. A pop-up screen will appear and select a **Base Profile** to go to the profile details screen.

CONFIGURATION > UTM Profile > IDP > Profile > Base Profile



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.

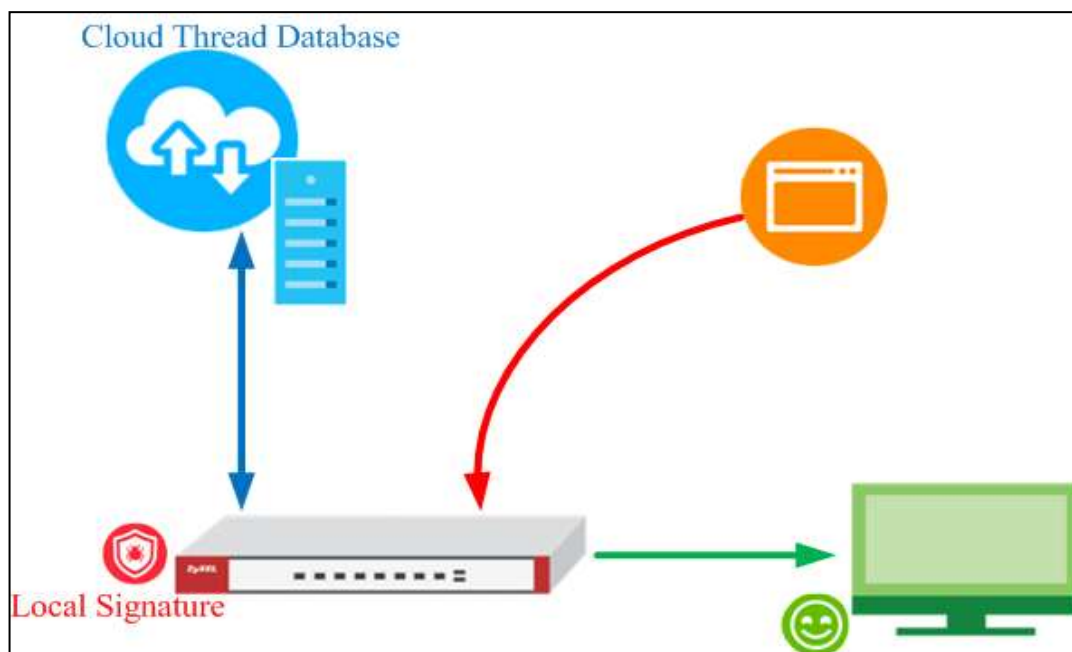
You have subscribed for the **IDP** service but the license is expired.

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

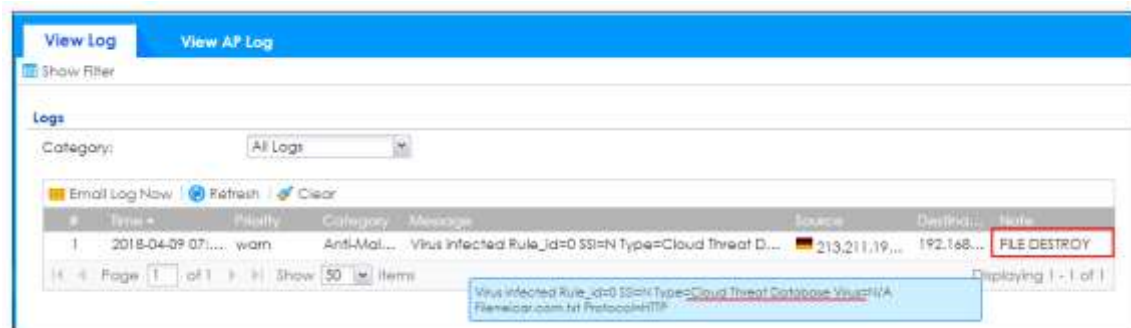
The screenshot shows the ZyXel Anti-Malware configuration interface. The 'General Settings' tab is active. Under 'General Settings', the 'Enable' checkbox is checked and highlighted with a red box. Below it, the 'Scan and detect EICAR test virus' checkbox is also checked. The 'Actions When Matched' section shows 'Destroy infected file' checked, with a 'Log' dropdown menu set to 'log'. 'Check White List' is checked, and 'Check Black List' is also checked. Both lists are currently empty. The 'File decompression' section has 'Enable file decompression (ZIP and RAR)' checked. The 'Signature Information' section shows details for 'Anti-Malware' and 'Cloud Threat Database' signatures, including version, signature number, and release date. At the bottom, there are 'Apply' and 'Reset' buttons.

 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. Your 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 database is enabled. You can use the CLI command to activate/deactivate cloud base service. It means the scanning priority will been changed.
 - a. **Router(config)# debug anti-virus ctdb activate**
 - b. **Router(config)# debug anti-virus ctdb deactivate**

How to Configure an Email Security Policy with Mail Scan and DNSBL

This is an example of using ATP Series' UTM Profile to mark or discard spam (unsolicited commercial or junk e-mail). Use the Email Security white list to identify legitimate e-mail. Use the Email Security black list to identify spam e-mail. The ATP Series can also check e-mail against a DNS Black List (DNSBL) of IP addresses of servers that are suspected of being used by spammers.

ATP Series with Email Security Profile to mark or discard spam e-mail
Example



Figure 1 Using Email Security to Detect Spam



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ATP200 (Firmware Version: ZLD 4.32).

Set Up the Email Security on ATP Series

In the ATP Series, go to **CONFIGURATION > Security Service > Email Security**; Enable this feature on General Settings page. Select **Check IP Reputation (SMTP only)** to have the ATP Series scan for spam e-mail by IP Reputation. Select **Check Mail Content** to identify Spam Email by content, such as malicious content. Select **Check Virus Outbreak** to scan viruses attached in emails. On advance section, leave Query Timeout Settings to be the default settings.

Select from the list of available **Scan Options** and desired Log type whether to have the ATP Series generate a log (**log**), log and alert (**log alert**) or neither (**no**) by default when traffic matches this policy. Click **Apply** to save the configuration

CONFIGURATION > Security Service > Email Security

☒ Enable

☒ Check White List
☒ Check Black List
☒ Check IP Reputation (SMTP only)
☒ Check Mail Content
☒ Check Virus Outbreak
☒ Check Mail Phishing
☒ Check DNSBL

Black List Spam Tag: (Optional)
 Mail Content Spam Tag: (Optional)
 Virus Outbreak Tag: (Optional)
 Mail Phishing Tag: (Optional)
 DNSBL Spam Tag: (Optional)

DNSBL Domain List

[+ Add](#)
[Edit](#)
[Remove](#)
[Activate](#)
[Inactivate](#)

Status	#	DNSBL Domain
Page 0 of 0 Show 50 items No data to display		

Action

Actions For Spam Mail ⓘ

SMTP:
 POP3:
 Log: ⓘ

 Action taken when mail session threshold is reached

☒ Forward Session

1. Register the device to myZyxel.com.
2. Activate Application Security.

#	Service	Status	Service Type	Expiration Date	Count	Action
1	Web Security	Activated	Standard	2019-5-13	N/A	Renew
2	Application Security	Activated	Standard	2019-5-13	N/A	Renew
3	Malware Blocker	Activated	Standard	2019-5-13	N/A	Renew
4	Intrusion Prevention	Activated	Standard	2019-5-13	N/A	Renew
5	Geo Enforcer	Activated	Standard	2019-5-13	N/A	Renew
6	Sandboxing	Activated	Standard	2019-5-13	N/A	Renew
7	SecuReporter	Activated	Standard	2019-5-13	N/A	Renew
8	Managed AP Service	Activated	Standard	2019-5-13	8	Renew
9	Firmware Upgrade Service	Activated			N/A	

Page 1 of 1 Show 50 items Displaying 1 - 9 of 9

3. Go to **CONFIGURATION > Security Service> Email Security>Enable Check Black List** to have the ATP Series treat e-mail that matches (an active) black list entry as spam.

General Settings Email Security

☒ Enable

☒ Check White List

☒ Check Black List

Black List Spam Tag: (Optional)

4. Continue to **Rule Summary on Black/White List**, click the **Add** icon. A pop-up screen will appear allowing you to configure **Content (Subject, IP/IPv6 Address, E-Mail Address and Mail Header)**, Use wildcards (*) to configure **Mail Subject Keyword**. (*sell* in this example). Click **OK** to return to the **General** screen.

CONFIGURATION > Security Service> Black/White List

+ Add Rule

☒ Enable Rule

Type:

Mail Subject Keyword:

OK **Cancel**

5. In the ATP Series, go to **CONFIGURATION > Security Service> Email Security>Enable Check DNSBL**
Press **Add** and enter the **DNSBL Domain** for a DNSBL service (zen.spamhaus.org in this example). Click **Apply**.

☒ Check DNSBL

DNSBL Spam Tag: [Spam] (Optional)

Status	#	DNSBL Domain
		zen.spamhaus.org

No data to display

Test the result

1. Send the mail subject with "sell".

From: zyxelsupport@zyxel.com.tw
 To: zyxelsupport@zyxel.com.tw;
 Cc:
 Bcc:
 Subject: Now on sell!!!
 Anti-Spam test

2. You will receive the mail subject with [Spam] tag.

From: zyxelsupport <zyxelsupport@zyxel.com.tw>
 To: zyxelsupport@zyxel.com.tw
 Cc:
 Subject: [Spam][Spam]Now on sell!!!
 Anti-Spam test

What can go wrong

1. If Email Security is not working, there are two possible reasons:
 You have not subscribed for the **Email Security** service.

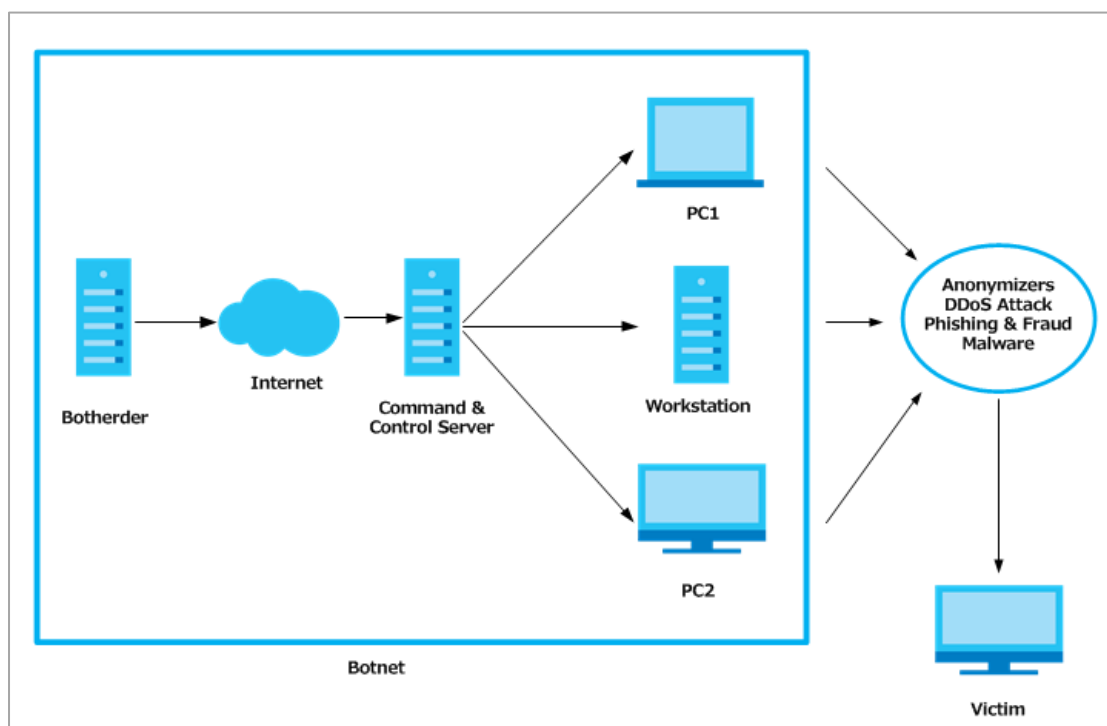
You have subscribed for the **Email Security** service but the license (**Application Security**) is expired.

2. You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **Application Security** license.

How to Configure Botnet Filter on ATP series?

Botnets are organized groups of infected computers. Those infected PCs will try to connect to the command-and-control server and ask for commands. When the attacker sends command to the command-and-control server, it will relay those commands to the clients (infected computers) and perform attacks on particular targets.

The following steps will walk you through an example of how to configure Botnet Filter (IP blocking and URL blocking) on the ATP.



Prerequisites before setting up Botnet Filter function

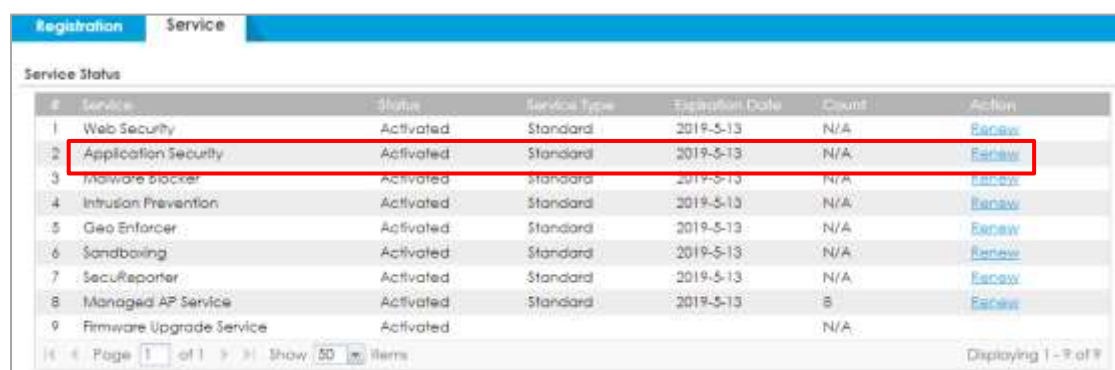
1. License status check
2. Update the Botnet Filter signature

License activation

Before setting up the Botnet Filter function, users need to make sure their licenses are purchased and activated.

To check the license activation status:

Go to configuration > Licensing > Registration > Service and check on the “Application Security” service which includes the Botnet Filtering function.



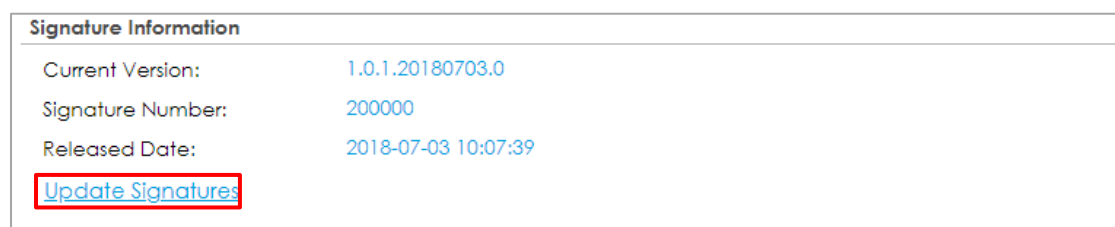
#	Service	Status	Service Type	Expiration Date	Count	Action
1	Web Security	Activated	Standard	2019-5-13	N/A	Renew
2	Application Security	Activated	Standard	2019-5-13	N/A	Renew
3	Malware blocker	Activated	Standard	2019-5-13	N/A	Renew
4	Intrusion Prevention	Activated	Standard	2019-5-13	N/A	Renew
5	Geo Enforcer	Activated	Standard	2019-5-13	N/A	Renew
6	Sandboxing	Activated	Standard	2019-5-13	N/A	Renew
7	SecuReporter	Activated	Standard	2019-5-13	N/A	Renew
8	Managed AP Service	Activated	Standard	2019-5-13	8	Renew
9	Firmware Upgrade Service	Activated			N/A	

Update Botnet Filter Signatures


To make sure the device has the most updated signature, we suggest users to update their Botnet Filter signature before using this function.

To update the Botnet Filter signature:

Go to **Configuration > Security Service > Botnet Filter**. Then click “**Update Signatures**”

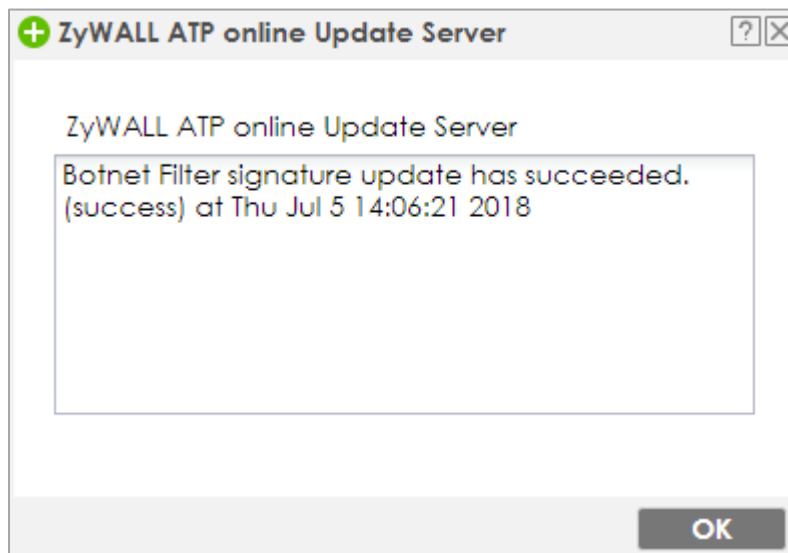


Signature Information	
Current Version:	1.0.1.20180703.0
Signature Number:	200000
Released Date:	2018-07-03 10:07:39
Update Signatures	

Then the device will redirect users to the “**Service Status**” page. Click on the cloud icon  and the device will start signature downloading process

Signature					
Service Status					
Feature	Type	Current Version	Released Date	Last Sync	Action
Anti-Malware	Anti-Malware Signature	2.0.1.20180627.0	2018-06-27 09:31:58 (UTC+08:00)	2018-07-04 23:55:01	
	Cloud Threat Databa...	1.0.0.20180704.0	2018-07-04 02:15:03 (UTC+08:00)		
App-Patrol	App-Patrol	1.0.0.20180517.0	2018-05-17 09:43:17 (UTC+08:00)	2018-06-20 04:52:18	
IDP	IDP	4.0.1.20180626.0	2018-06-26 13:10:00 (UTC+08:00)	2018-07-01 00:27:01	
Botnet Filter	Botnet Filter	1.0.1.20180703.0	2018-07-03 10:07:39 (UTC+08:00)	2018-07-05 02:59:01	

Once the signature updating process was done. The GUI will pop up the following message to notify users.

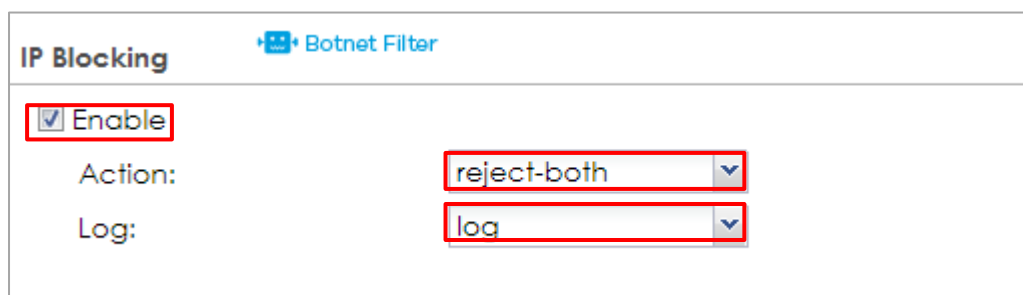


Now the Botnet Filtering function is ready to go.

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.



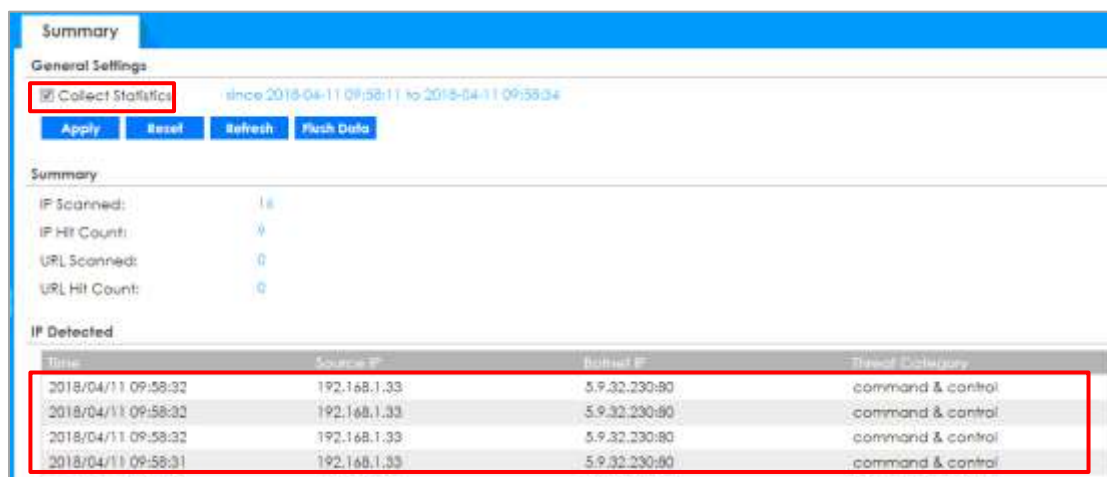
The screenshot shows the 'Botnet Filter' configuration page. Under the 'IP Blocking' section, the 'Enable' checkbox is checked. The 'Action' dropdown menu is set to 'reject-both', and the 'Log' dropdown menu is set to 'log'.

Test the Result

User access IP: 5.9.32.230

Go to **Monitor > Security Statistics > Botnet Filter** to check summary.

IP: 5.9.32.230 is blocked due to command & control.



The screenshot shows the 'Summary' page of the Botnet Filter. The 'Collect Statistics' checkbox is checked. The summary table shows 1 IP scanned, 0 IP hit counts, 0 URL scanned, and 0 URL hit counts. The 'IP Detected' table lists four entries, all identified as 'command & control' threats.

Time	Source IP	Botnet IP	Threat Category
2018/04/11 09:58:32	192.168.1.33	5.9.32.230:80	command & control
2018/04/11 09:58:32	192.168.1.33	5.9.32.230:80	command & control
2018/04/11 09:58:32	192.168.1.33	5.9.32.230:80	command & control
2018/04/11 09:58:31	192.168.1.33	5.9.32.230:80	command & control

Set up the URL Blocking on the ATP series

Go to **Configuration > Security Service > Botnet Filter**.

Select the **Enable URL Blocking** check box, check the categories that need to be blocked. Users can only check those categories as their requirement. Choose the Action the device will take (In this example we select “block” to block certain URLs) and if they want to Log those events on the device.

URL Blocking

☒ **Enable**

☒ Anonymizers
 ☒ Botnet C&C
 ☒ Compromised

☒ Malware
 ☒ Phishing & Fraud
 ☒ Spam Sites

Action: **block**

Log: **log**

Message to display when a site is blocked

Denied Access Message: Web access is restricted. Please contact the administrator.

Redirect URL:

Test the Result

Browse the Phishing website URL from the host browser. Users will be redirected to an error page in the browser that notifies 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
<div> <div>Page 1 of 1</div> <div>Show 50 Items</div> <div>No data to display</div> </div>			

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.

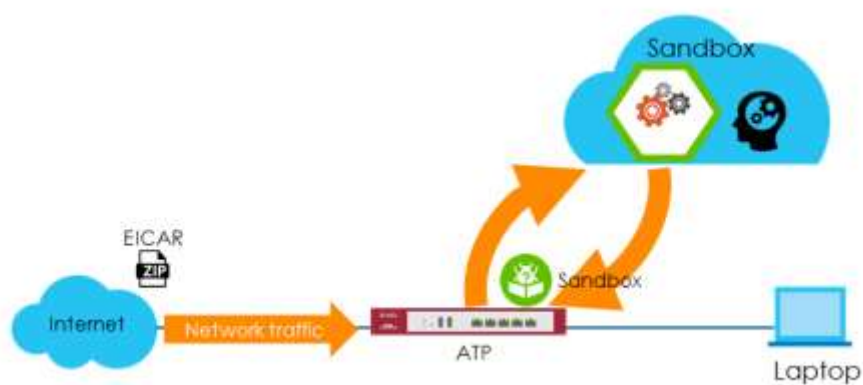


Figure 1 Using Sandboxing to Detect Unknown Malware



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 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.

File Submission Options

- ☒ Archives(.zip)
- ☒ Executables
- ☒ MS Office Documents
- ☒ Macromedia Flash Data
- ☒ PDF
- ☒ RTF

Use the command to check the status of each file type. If the status is "no", the file type is not scanned by Sandboxing.

Router> show sandbox file-type all

```
Router> show sandbox file-type all
```

No.	Show_name	Name	Status
1	Archives(.zip)	archives	yes
2	CHM	chm	no
3	EICAR	eicar	no
4	Executables	executables	yes
5	Macromedia Flash Data	macromedia-flash-data	yes
6	MS Office Documents	ms-office-document	yes
7	PDF	pdf	yes
8	RTF	rtf	yes
9	Unknow Type	unknow-type	no

Use the following commands to make Sandboxing access and check a certain file type.

```
Router> configure terminal
```

```
Router(config)# sandbox file-type eicar
```

```
Router(config)# write
```

```
Router> configure terminal
Router(config)# sandbox file-type eicar
Router(config)# write
Router(config)# show sandbox file-type all
```

No.	Show_name	Name	Status
1	Archives(.zip)	archives	yes
2	CHM	chm	no
3	EICAR	eicar	yes
4	Executables	executables	yes
5	Macromedia Flash Data	macromedia-flash-data	yes
6	MS Office Documents	ms-office-document	yes
7	PDF	pdf	yes
8	RTF	rtf	yes
9	Unknow Type	unknow-type	no

- Go to **CONFIGURATION > Security Service > Sandboxing > General**, enable Sandboxing and select action and log for malicious and suspicious files to monitor the result.

General

☒ Enable Sandboxing

Action For Malicious File:

Log For Malicious File:

Action For Suspicious File:

Log For Suspicious File:

5. Enable Collect Statistics to monitor the scan results and statistics.

MONITOR > Security Statistics > Sandboxing

General Settings

☒ Collect Statistics
 show 2018-07-03 10:41:08 to 2018-07-03 10:41:08

Submission Summary

Total:	0
Scannings:	0
Scanned:	0
Destroyed Files:	0

Scan Result

Malicious Files:	0
Suspicious Files:	0
Safe Files:	0
Other:	0

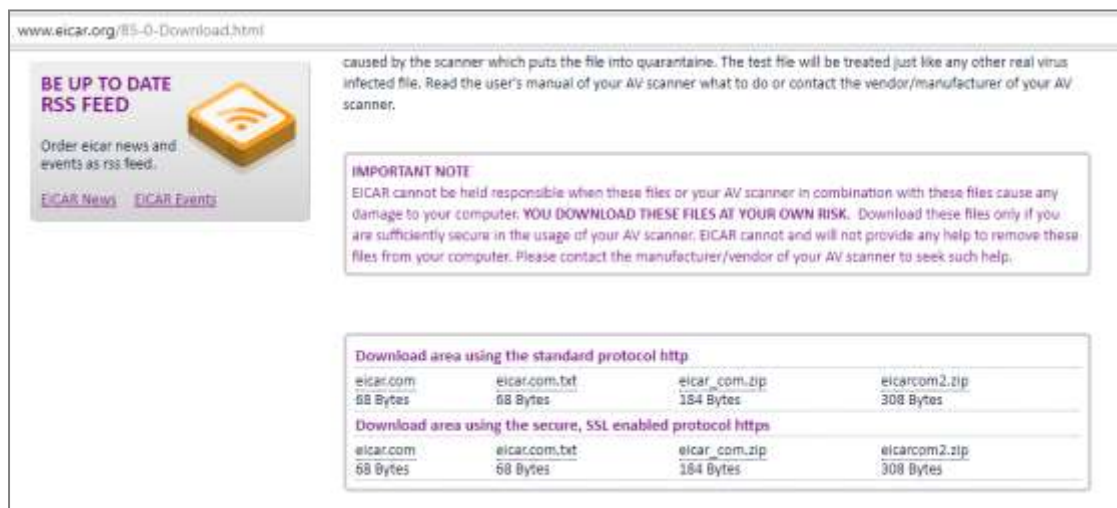
Statistics

#	File Name	Hash	Type	Occurrence	Update Time
<div> <div>14</div> <div>Page 1 of 0</div> <div>Show 50 Items</div> </div>					

No data to display

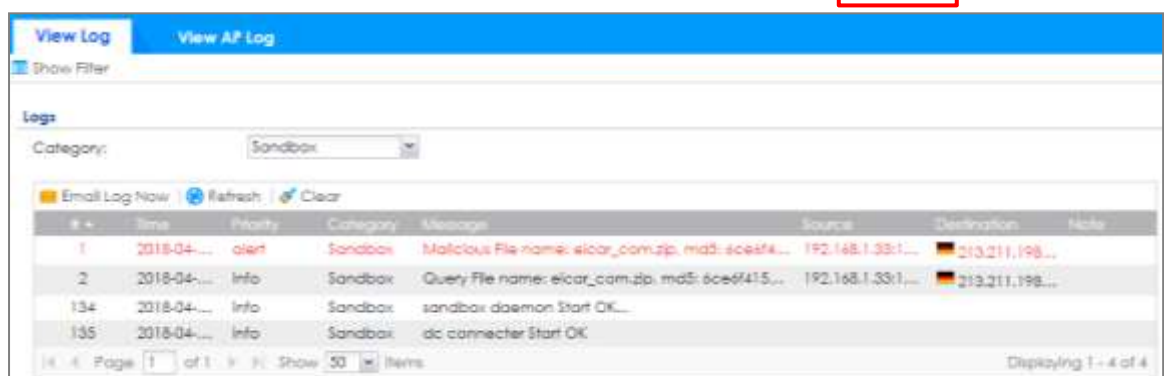
Test the Result

- 3 Go to <http://www.eicar.org/85-0-Download.html> to download eicar_com.zip file.



- 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

Summary

General Settings

Collect Statistics

since 2018-04-27 18:55:12 to 2018-04-27 17:04:09

Apply

Reset

Refresh

Flush Data

Submission Summary

Total:

1

Scanning:

0

Scanned:

1

Destroyed File:

0

Scan Result

Malicious File:

1

Suspicious File:

0

Clean File:

0

Other:

0

Statistics

#	File Name	Hash	Type	Occurrence	Update Time
1	eicar_com.zip	6ce6f413d8475545be5ba114208e0ff	Malicious	1	2018-04-27 17:03:18



Note: Disable anti-virus software on your laptop in order to test Sandbox.

- 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

View Log							
View All Log							
Show Filter							
Logs							
Category: Sandbox							
Email Log Now Refresh Clear							
#	Time	Priority	Category	Message	Source	Destination	Note
1	2018-04-27...	crit	Sandbox	Malicious infected (Stichfile:eicar_com.zip, md5: 6ce6f413d8475545be5ba114208e0ff)	192.168.1.33:1845	213.211.198...	FILE DESTROY
4	2018-04-27...	alert	Sandbox	Malicious File name: eicar_com.zip, md5: 6ce6f413d8475545be5ba114208e0ff	192.168.1.33:1845	213.211.198...	
5	2018-04-27...	info	Sandbox	Query File name: eicar_com.zip, md5: 6ce6f413d8475545be5ba114208e0ff	192.168.1.33:1845	213.211.198...	
137	2018-04-27...	info	Sandbox	sandbox daemon Start OK			
138	2018-04-27...	info	Sandbox	dc connector Start OK			
Page 1 of 1 Show 50 Items							
Displaying 1 - 5 of 5							

MONITOR > Security Statistics > Sandboxing

Summary

General Settings

☒ Collect Statistics since 2018-04-27 16:55:11 to 2018-04-27 17:11:14

ApplyResetRefreshFlush Data

Submission Summary

Total: 2

Scanning: 0

Scanned: 0

Destroyed File: 1

Scan Result

Malicious File: 2

Suspicious File: 0

Clean File: 0

Other: 0

Statistics

#	File Name	Hash	Type	Occurrence	Update Time
1	elcar_com.zip	6ce6f415d8475545be5ba114f208b0ff	Malicious	2	2018-04-27 17:08:26

« Page 1 of 1 » Show 50 Items

Displaying 1 - 1 of 1

What Can Go Wrong?

- 6 SSL inspection needs to be enabled and applied to the corresponding security policy rule for HTTPS traffic.
- 7 Only Windows (Win XP, Win 7, Win 10) and Mac OSX operating system are supported.
- 8 The local cache of the analysis result will be deleted when the device reboots.

How to configure Email Security for Phishing mail?

(This feature is only supported on ATP series)

The following depicts a sample configuration of Email security for Phishing mail.

Phishing is a type of online scam where criminals send an email with a fake website and asking you to provide sensitive information.

An example of phishing attack:

1. Attacker creates an fake banking websites which copy the content from real banking website
2. Attacker sends user an phishing emails with an embed URLs to ask change the new banking password
3. User opens the mail then click to the embed URLs, it redirects user access to fake banking websites.
4. User enters the current banking account when they attempt change the password
5. Attacker gets the user's banking account and can steal user's money

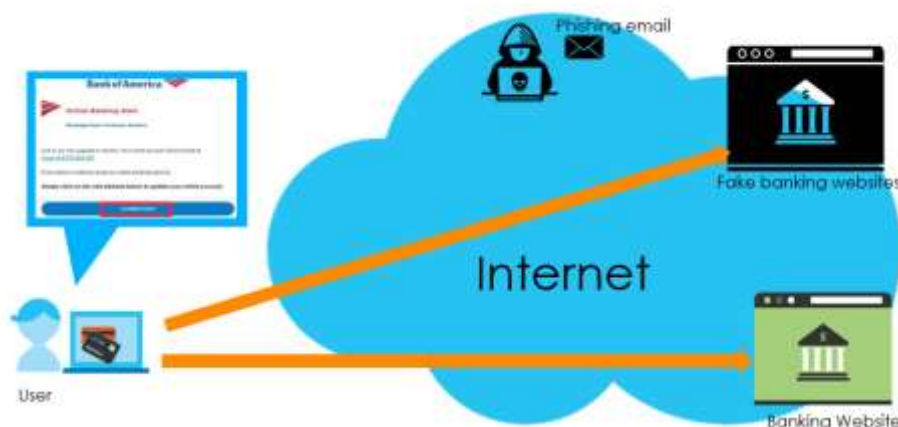


Figure 1 Using Sandboxing to Detect Unknown Malware

How it works

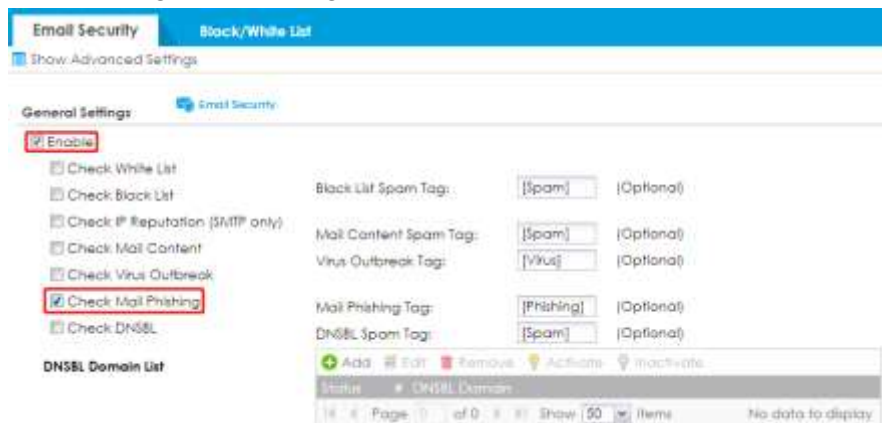
Gateway inspects the email content to detect the embedded URLs. With Anti-phishing enhancement, ATP gateway inspects the mail content to detect the embedded URLs.



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:bbs@ssdkkk.com/tw phishing host:websectest.ctmail.com	192.168.2.33:1756	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

Summary

Status

General Settings

☒ Collect Statistics

Apply

Reset

Refresh

Flush Data

Email Summary

Total Mails Scanned:	1
Clear Mails:	0
Clear Mails Detected by White List:	0
Spam Mails:	0
Spam Mails Detected by Black List:	0
Spam Mails Detected by IP Reputation:	0
Spam Mails Detected by Mail Content:	0
Spam Mails Detected by Mail Phishing:	1
Spam Mails Detected by DNSBL:	0
Spam Mails with Virus Detected by Mail Content:	0
Virus Mails:	0
Query Timeout:	0

What Can Go Wrong?

- 1 Make sure the Anti-Spam default service port is SMTP or POP3 by CLI

Router# show utm-manager anti-spam defaultport

```
Router# show utm-manager anti-spam defaultport
```

No.	Proto	Port
1	smtp	25
2	pop-3	110

- 2 It does not support SSL inspection.
- 3 The ATP can inspect email up to 50KB. If the mail size greater than 50KB, gateway will inspect the first 50KB from the header

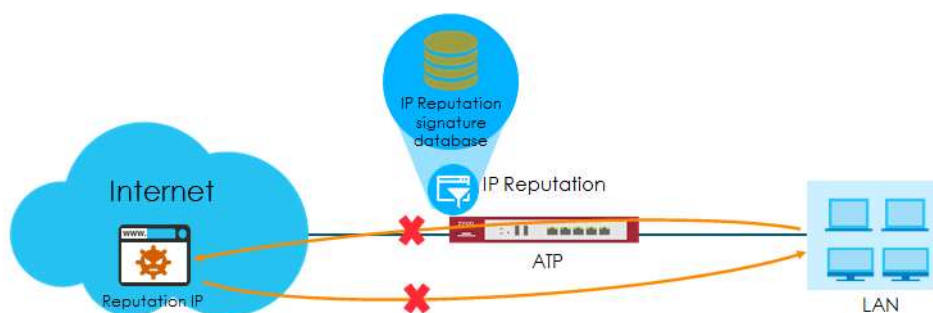
How to Use IP Reputation to Detect Threats

(This feature is only supported on ATP series)


As cyber threats such as scanners, botnets, phishing, etc. grow increasingly, how to identify suspect IP addresses of threats efficiently becomes a crucial task.

With regularly updated IP database, ATP prevents threats by blocking connection to/from known IP addresses based on signature database. It filters source and destination addresses in your network traffic to take the proper risk prevention actions.

This example illustrates how to configure IP Reputation on ATP gateway to detect cyber threats for both incoming and outgoing traffic.



Figure

 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses. This example was tested using the ATP500 (Firmware Version: ZLD 4.35).

Activating Reputation Filter Service

- 1 Register ATP gateway to myZyxel.com.
- 2 Activate Reputation Filter license.

#	Service	Status	Service Type	Expiration Date	Count	Action
1	Web Security	Activated	Standard	2020-3-31	N/A	Refresh
2	Application Security	Activated	Standard	2020-3-31	N/A	Refresh
3	Malware Blocker	Activated	Standard	2020-3-31	N/A	Refresh
4	Intrusion Prevention	Activated	Standard	2020-3-31	N/A	Refresh
5	Geo Enforcer	Activated	Standard	2020-3-31	N/A	Refresh
6	Sandboxing	Activated	Standard	2020-3-31	N/A	Refresh
7	Reputation Filter	Activated	Standard	2020-3-31	N/A	Refresh
8	SecuReporter	Activated	Standard	2020-3-31	N/A	Refresh
9	Managed AP Service	Activated	Standard	2020-3-31	34	Refresh
10	Device HA Pro	Activated	Standard		N/A	
11	Firmware Upgrade Service	Activated			N/A	

Page 1 of 1 | Show 50 Items | Displaying 1 - 11 of 11

- 3 On ATP, go to **CONFIGURATION > Licensing > Signature Update**. Click the **Update** icon to check for new signatures.

Feature	Type	Client Version	Refresh Date	Last Sync	Action
Anti-Malware	Anti-Malware Signature	2.0.2.20190601.0	2019-06-01 09:35:37 (UTC+08:00)		Refresh
	Cloud Threat Database	1.0.0.20190601.0	2019-06-01 02:15:03 (UTC+08:00)	2019-06-13 23:49:01	Refresh
App-Patrol	App-Patrol	1.0.0.20190518.0	2019-05-18 09:45:23 (UTC+08:00)	2019-06-02 00:15:01	Refresh
ICP	ICP	4.0.0.20190524.0	2019-05-24 10:10:00 (UTC+08:00)	2019-06-02 01:03:01	Refresh
Botnet Filter	Botnet Filter	1.0.0.20190601.0	2019-06-01 10:20:30 (UTC+08:00)	2019-06-14 02:50:01	Refresh
IP Reputation	IP Reputation	1.0.0.20190601.0	2019-06-01 10:30:10 (UTC+08:00)	2019-06-17 14:55:03	Refresh

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.

General
White List
 Black List

IP Blocking

☒ **Enable**

Action: block

Threat Level Threshold: high

High
Medium and above
Low and above

Log: log

Selecting specific type of IP addresses to block

In Types of Cyber Threats Coming From The Internet, select the type of threats that are known to pose a security threat for incoming traffic.

In Types of Cyber Threats Coming From The Internet And Local Networks, select the type of threats that are known to pose a security threat for both incoming

and outgoing traffic.

Types of Cyber Threats Coming From The Internet		
<input checked="" type="checkbox"/> Anonymous Proxies	<input checked="" type="checkbox"/> Denial of Service	<input checked="" type="checkbox"/> Exploits
<input checked="" type="checkbox"/> Negative Reputation	<input checked="" type="checkbox"/> Scanners	<input checked="" type="checkbox"/> Spam Sources
<input checked="" type="checkbox"/> TOR Proxies	<input checked="" type="checkbox"/> Web Attacks	
Types of Cyber Threats Coming From The Internet And Local Networks		
<input checked="" type="checkbox"/> Botnets	<input checked="" type="checkbox"/> Phishing	
Test IP Threat Category		
IP to test:	<input type="text"/>	<input type="button" value="Search"/>
Signature Information		
Current Version:	1.0.0.20190601.0	
Signature Number:	752104	
Released Date:	2019-06-01 10:30:10	
Update Signatures		

Adding IP addresses to white list and black list

Go to **CONFIGURATION > Security Service > Reputation Filter > IP Reputation > White List** and **Black List** to manually adding IP addresses to the White List and Black List.

General	White List	Black List
White List		
<input checked="" type="checkbox"/> Check White List		
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/> <input type="button" value="Activate"/> <input type="button" value="Inactivate"/>		
#	Status	IPv4 Address
1	<input checked="" type="radio"/>	1.1.1.1
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1		
Black List		
<input checked="" type="checkbox"/> Check Black List		
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Remove"/> <input type="button" value="Activate"/> <input type="button" value="Inactivate"/>		
#	Status	IPv4 Address
1	<input checked="" type="radio"/>	9.9.9.9
Page 1 of 1 Show 50 items Displaying 1 - 1 of 1		

Monitoring statistics for IP detection

Enable Collect Statistics to monitor the scanned result and detected IP.

MONITOR > Security Statistics > Reputation Filter

General Settings

☒ Collect Statistics since 2019-06-18 13:30:56 to 2019-06-18 13:30:56

Refresh Flush Data

Summary

IP Scanned: 0
IP Hit Count: 0
URL Scanned: 0
URL Hit Count: 0

IP Detected

☐ Add to white list ☐ Remove from white list

Time	Malicious IP	Infected/Victim Host	Threat Category	Threat Level
Page 1 of 0 at 0 Show 50 Items No data to display				

URL Detected

☐ Add to white list ☐ Remove from white list

Time	Source IP	Destination IP	Botnet URL	Threat Category
Page 1 of 0 at 0 Show 50 Items No data to display				

Test the Result

- 1 Select Anonymous Proxies for detecting incoming traffic and Botnet for outgoing traffic.

IP Blocking

☒ Enable

Action: block

Threat Level Threshold: high

Log: log

Types of Cyber Threats Coming From The Internet

☒ Anonymous Proxies ☒ Denial of Service ☒ Exploits
☒ Negative Reputation ☒ Scanners ☒ Spam Sources
☒ TOR Proxies ☒ Web Attacks

Types of Cyber Threats Coming From The Internet And Local Networks

☒ Botnets ☒ Phishing

- 2 For incoming traffic, set a NAT rule and add a security policy rule for allowing traffic from WAN to LAN.

General Settings										
<input checked="" type="checkbox"/> Enable Policy Control										
IPv4 Configuration										
<input checked="" type="checkbox"/> Allow Asymmetrical Route										
<div> + Add ✖ Edit ✖ Remove 🔔 Activate 🔍 Track/Update ↔ Move ✖ Delete </div>										
Id	Name	From	To	IPv4 Src	IPv4 Dest	Service	User	Schedule	Action	Log Profile
1	test	WAN	LAN	any	any	RDP	any	none	allow	no
2	LAN_Outgoing	LAN	any (Ex...	any	any	any	any	none	allow	no
3	DMZ_To_WAN	DMZ	WAN	any	any	any	any	none	allow	no

For outgoing traffic, ping an IP address in the threat category "Botnets" from LAN.

- 3 Check statistics for detected IPs.

MONITOR > Security Statistics > Reputation Filter

General Settings

☒ Collect Statistics since 2019-06-17 16:16:45 to 2019-06-17 16:22:50

Refresh

Refresh Data

Summary

IP Scanned:197

IP Hit Count:7

URL Scanned:0

URL Hit Count:0

IP Detected

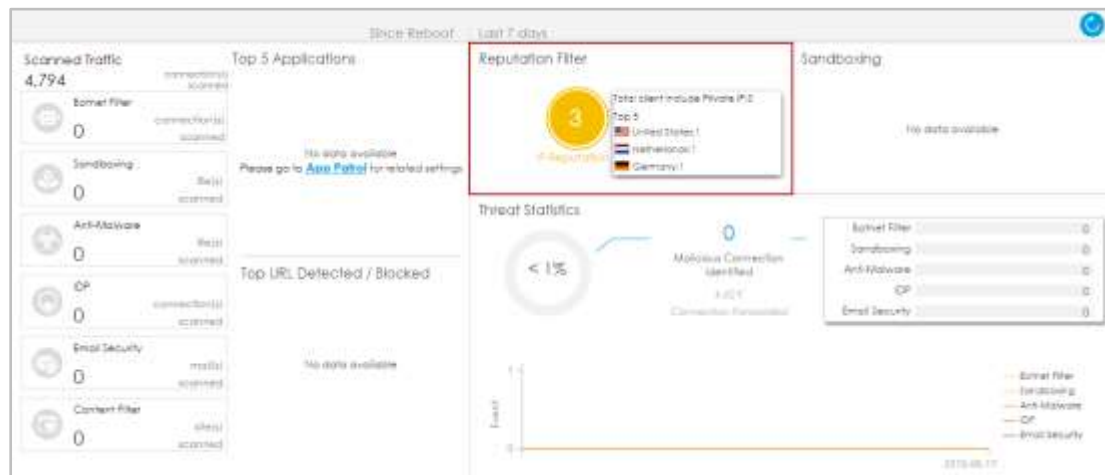
☒ Add to white list

☒ Remove from white list

Time	Malicious IP	Infected/Victim IP	Threat Category	Threat Level
2019/06/17 16:23:33	<input type="checkbox"/> 195.20.42.1	192.168.1.33	Botnets	High
2019/06/17 16:23:32	<input type="checkbox"/> 195.20.42.1	192.168.1.33	Botnets	High
2019/06/17 16:23:00	<input type="checkbox"/> 195.20.42.1	192.168.1.33	Botnets	High
2019/06/17 16:22:59	<input type="checkbox"/> 195.20.42.1	192.168.1.33	Botnets	High
2019/06/17 16:21:45	<input type="checkbox"/> 148.251.232.132	192.168.1.34	Anonymous Proxies	High
2019/06/17 16:21:45	<input type="checkbox"/> 148.251.232.132	192.168.1.34	Anonymous Proxies	High
2019/06/17 16:21:44	<input type="checkbox"/> 148.251.232.132	192.168.1.34	Anonymous Proxies	High

On dashboard, you can find top 5 countries that are detected the most by IP Reputation.

Dashboard > Advanced Threat Protection



What Can Go Wrong?

1. For device HA or HA Pro, signature synchronization is required.
2. Cloud query is not supported.
3. It doesn't support for IPv6.

How to Configure Reputation Filter- DNS Filter

DNS Filter is a mechanism aimed at protecting users by intercepting DNS request attempting to connect to known malicious or unwanted domains and returning a false, or rather controlled IP address. The controlled IP address points to a sinkhole server defined by the administrator.

Suppose of there a client who wants to access malicious domain. This will send query to the DNS server for getting the domain name details. All of the traffic now here gateway intercepts this query which is outgoing. Gateway contains DNS signatures and identifies that this is bad site. What gateway can do here is send the redirect IP address where we deploy a blocked page to the client. The client will connect to redirect IP address instead of the real IP address of malicious domain, and get the blocked page with the web access. This example will show you how to configure DNS Filter to redirect web access after client hit the filter profile.

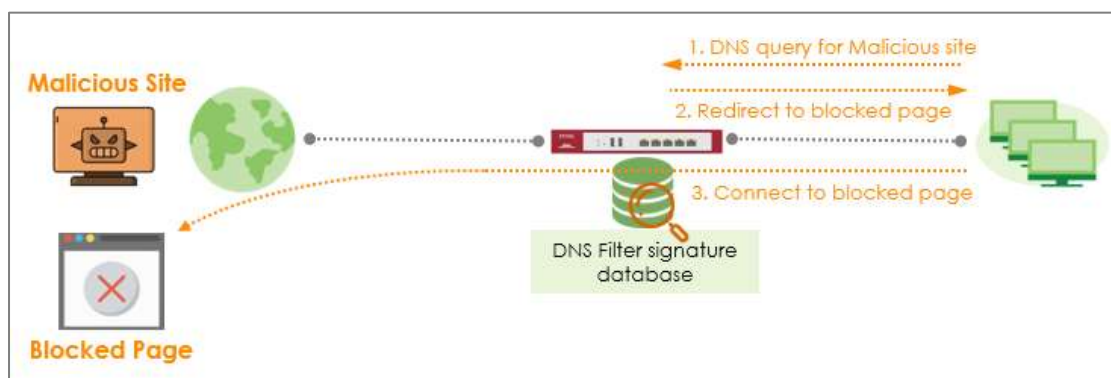


Figure. DNS Filter protects user from malicious websites



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).

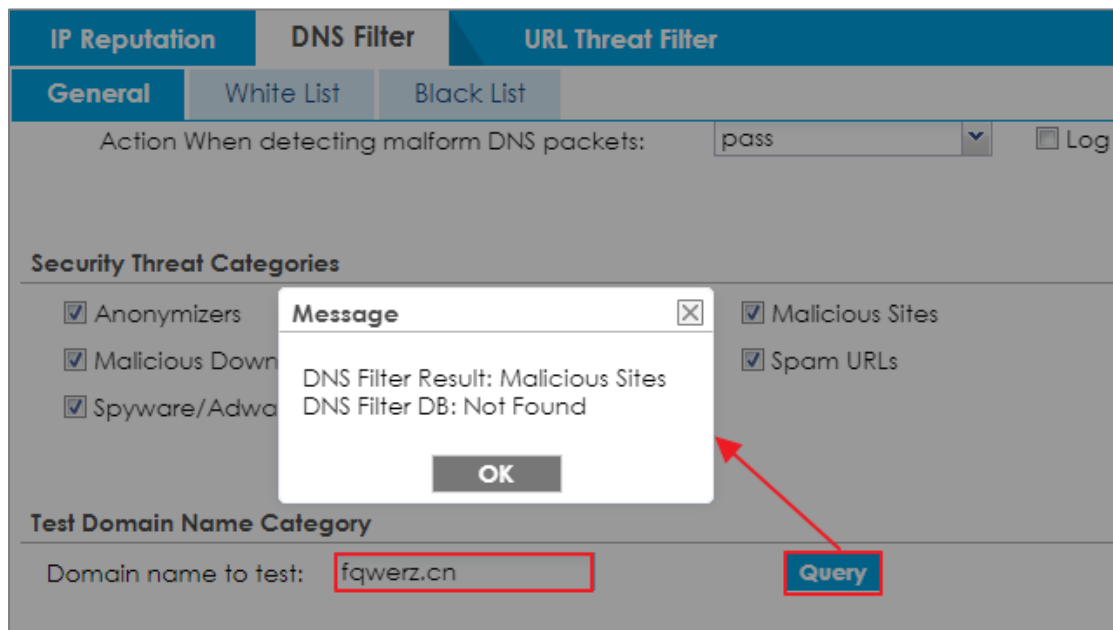
Set Up the DNS Filter on ATP Series

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.

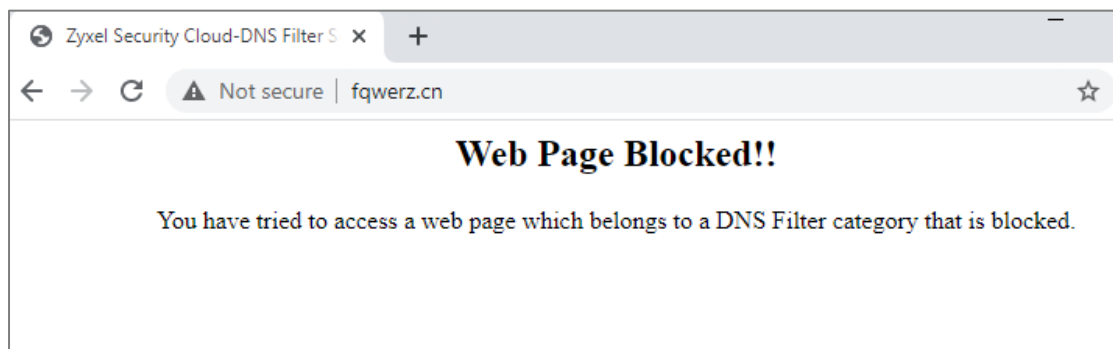
IP Reputation	DNS Filter	URL Threat Filter
General	White List	Black List
<h3>DNS Filter</h3> <p><input checked="" type="checkbox"/> Enable</p> <p>Action: redirect</p> <p>Log: log-alert</p> <p>Redirect IP: default</p> <p>Action When detecting malformed DNS packets: pass <input type="checkbox"/> Log</p> <h3>Security Threat Categories</h3> <p> <input checked="" type="checkbox"/> Anonymizers <input checked="" type="checkbox"/> Browser Exploits <input checked="" type="checkbox"/> Malicious Sites </p> <p> <input checked="" type="checkbox"/> Malicious Downloads <input checked="" type="checkbox"/> Phishing <input checked="" type="checkbox"/> Spam URLs </p> <p> <input checked="" type="checkbox"/> Spyware/Adware/Keyloggers </p>		

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.

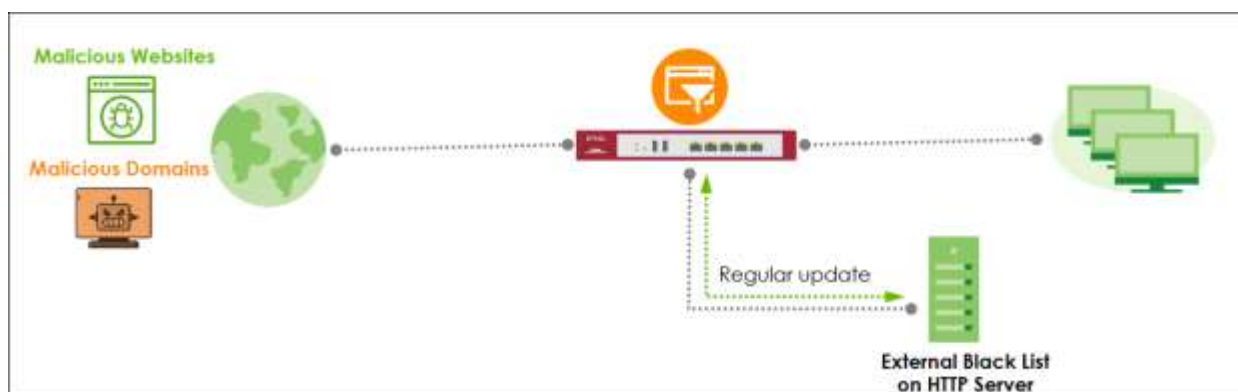
How to customize external block list in Reputation Filter

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:0000:0000:0000:0e13 (IPv6 Single Host)
 2001:DB8:2de::e14/32 (IPv6 CIDR)

URL Threat Filter format

https://example.com (URL)
 www.example.com (Hostname)
 example.com (Domain name)
 *.example.com (Wildcard domain name)

After configured list completely, you can save your .txt file on your HTTP server.
 (e.g. Software: HTTP File Server)

Configure External Block list setting

IP Reputation

Go to Configuration > Security Service > Reputation Filter > IP Reputation > External Black List.

Click Add button to download source on your HTTP Server.

+ Add Rule

General Settings

Name:

Description:

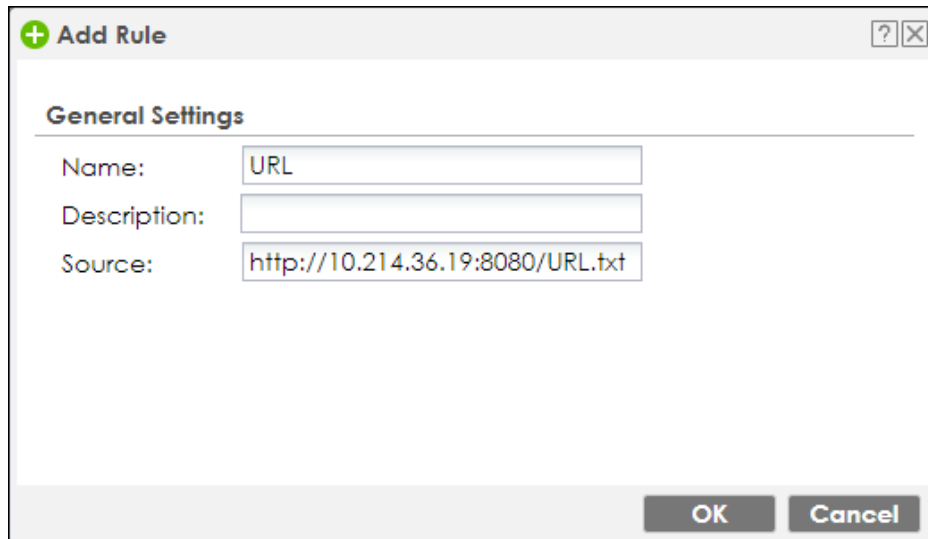
Source:

OK Cancel

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.



+ Add Rule

General Settings

Name:

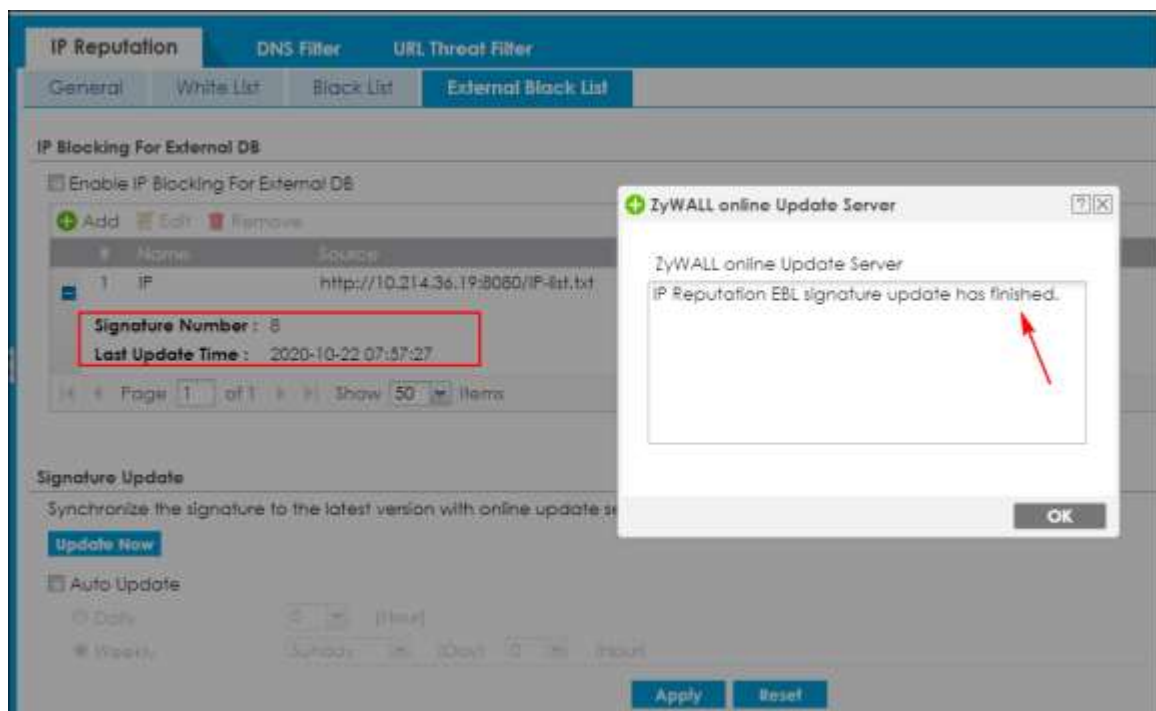
Description:

Source:

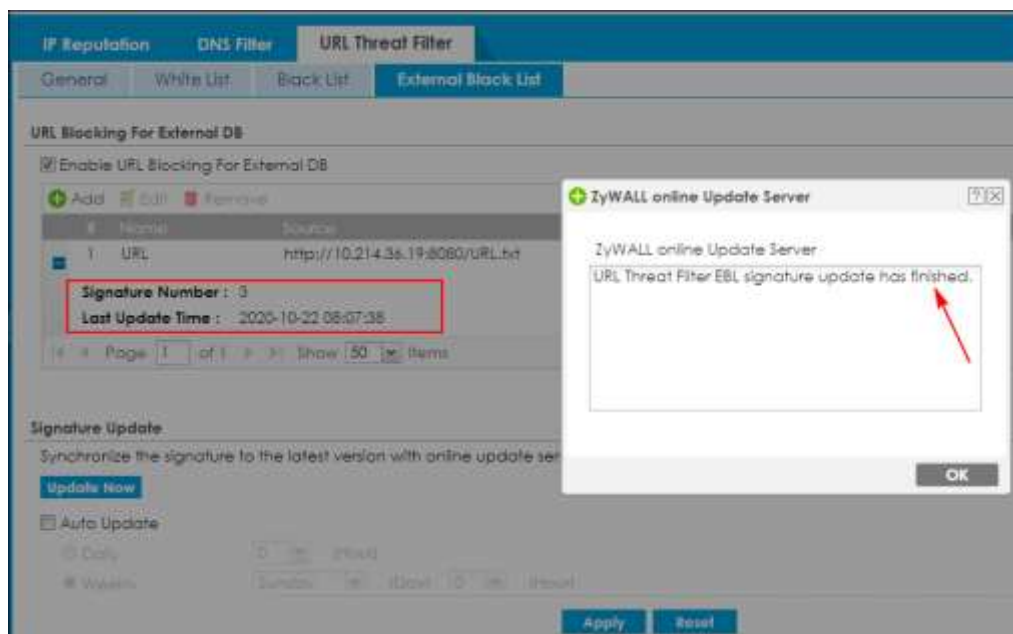
OK Cancel

Check External Block List update status

IP Reputation



URL Threat Filter

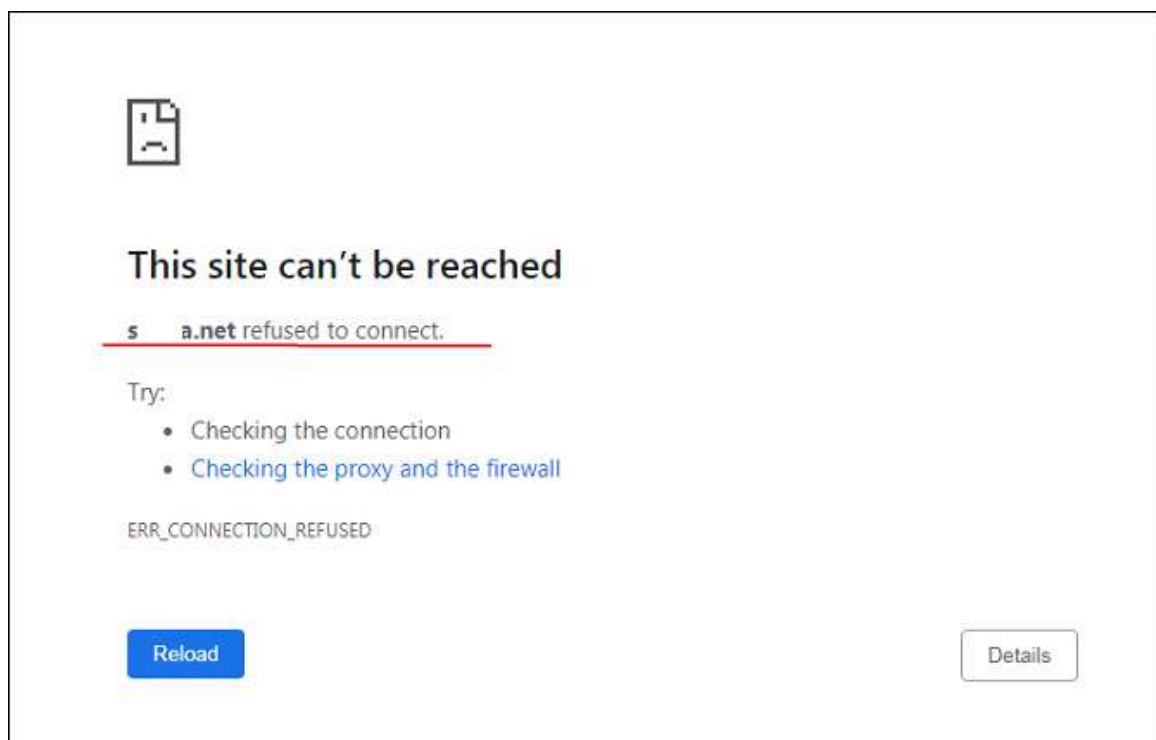


Note: Please must make sure **block list format** in your ".txt" file correct. Otherwise the data will unable import to system completely. You can check "**Signature Number**" if amount is the same as your list.

Verification

IP Reputation block page

If client traffic is blocked by IP Reputation, website will unable to access to will display it.



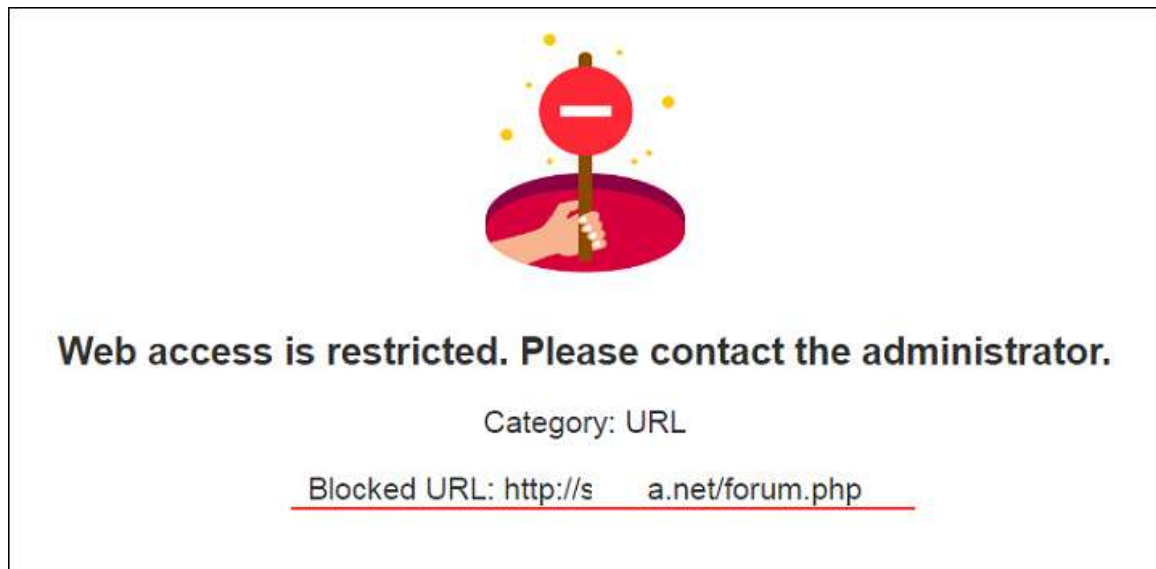
IP Reputation Log

Email Log Now Refresh Clear						
#	Time	File	Category	Message	Source	Destination
1	202...	alert	IP Reputation	Malicious connection:IP [count=3]	192.168.1.50:49638	104.31.95.74:80
2	202...	alert	IP Reputation	Malicious connection:IP	192.168.1.50:49639	104.31.94.74:80
3	202...	alert	IP Reputation	Malicious connection:IP [count=3]	192.168.1.50:49637	104.31.95.74:80
4	202...	alert	IP Reputation	Malicious connection:IP	192.168.1.50:49634	104.31.94.74:80
5	202...	alert	IP Reputation	Malicious connection:IP [count=3]	192.168.1.50:49636	104.31.95.74:80
6	202...	alert	IP Reputation	Malicious connection:IP	192.168.1.50:49633	104.31.94.74:80

Page 1 of 1 Show 50 Items Displaying 1 - 6 of 6

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

Email Log Now Refresh Clear							
#	Time	Priority	Category	Message	Source	Destination	Note
2	202...	alert	URL Threat Filter	s a.net/URL SSID=N	192.168.1.50:49747	[104.31.94.74:80]	ACCESS BLOCK
Page 1 of 1				Show 50 Items	Displaying 1 - 1 of 1		

What Can Go Wrong

1. Must make sure IP/FDQN format in Block List file. Otherwise system will stop to import data into system.
2. Must make sure your HTTP server is reachable from device.
3. If destination server working in HTTPS, Block page may only display certificate error.

How to Configure DNS Content Filter (On-Premises)

There are more browser support and users are encouraged to switch to TLS 1.3 because of its increased security, but websites using TLS 1.3 may not be categorized by URL content filtering without SSL inspection. For that, we need a solution to have early check on categorizations by DNS query instead. Compared to traditional content filter, DNS content filter is a stronger tool for SMB(s), because it can restrict the number of attacks faced by network access, thereby helping to reduce the remediation workload of IT professionals. Effective DNS content filter can even prevent up to 88% of Internet-spread malware.

DNS content filter intercept DNS request from client, check the domain name category and takes a corresponding action, reducing the risk of phishing attacks, and obfuscate source IPs using hijacked domain names. Fully customizable blacklist to ban access to any unwanted domains and prevent reaching those known domains hosting malicious content.

In this scenario, gateway works in on-premises mode, we configure DNS Content Filter via device Web GUI to block users in the local network to access the social networking site such as Facebook.

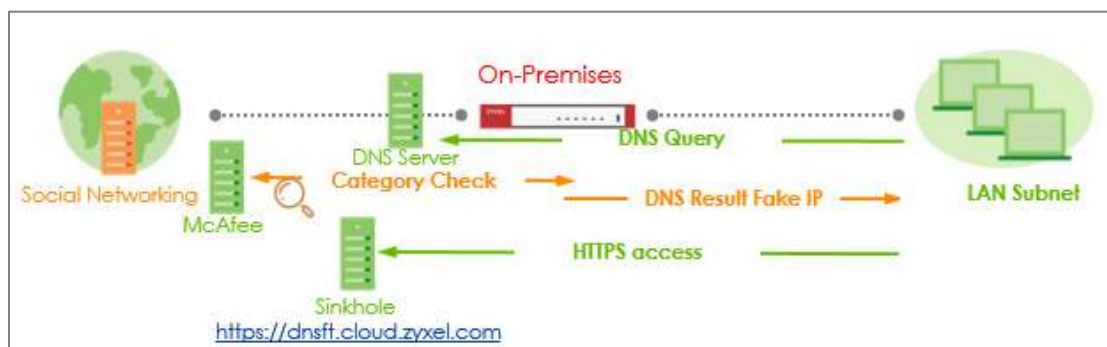


Figure: DNS Content Filter protects user to inappropriate website

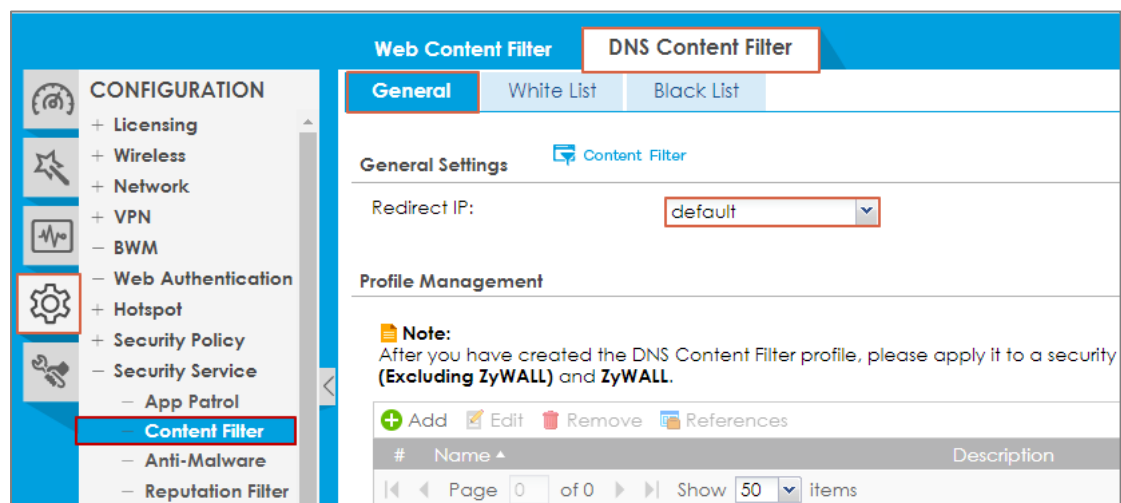


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG Flex 500 (Firmware Version: ZLD 5.00).

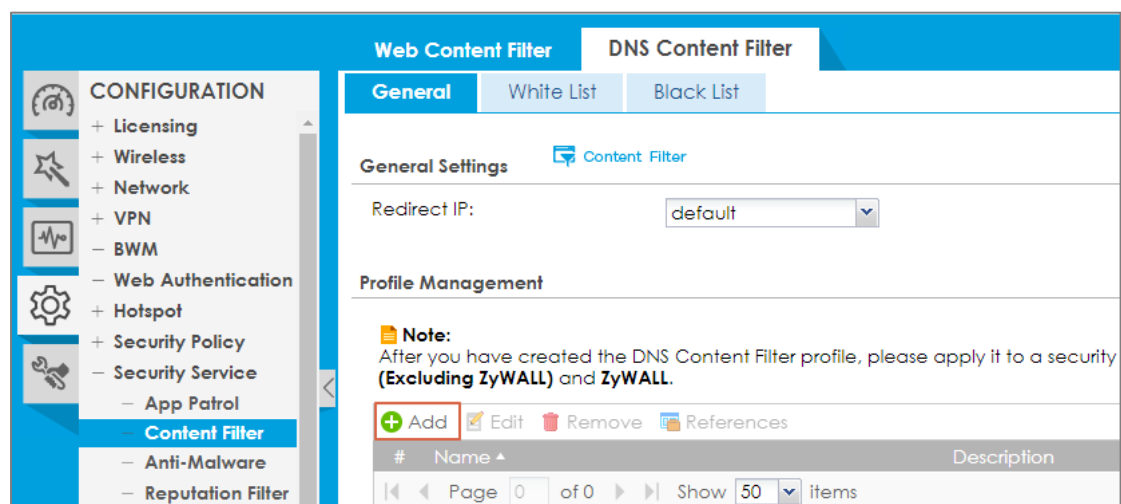
Set Up the DNS Content Filter on USG Flex Series

In the USG Flex Web GUI, go to **Configuration > Security Service > Content Filter > DNS Content Filter**; Select Redirect IP to indicated IP address or default one. If user selects the default, when client hit DNS Content Filter profile, the page will be redirect to block page <http://dnsft.cloud.zyxel.com/>.

If user selects the custom defined, the page will be redirect indicated IP address.



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.



Add

General Settings

Name:

Description: (Optional)

Action:

Log:

Scan Option

☒ Check White List

☒ Check Black List

Select Categories

☐ Select All Categories ☐ Clear All Categories

Clone Categories Setting From Profile:

Test Domain Name Category

Domain name to test:

[If you think the category is incorrect, click this link to submit a request to review it.](#)

Once the DNS Content Filter profile is created, a windows shows up to instruct you to apply this profile to security policy. Click **Yes** to continue

Web Content Filter **DNS Content Filter**

General **White List** **Black List**

General Settings ☒ Content Filter

Redirect IP:

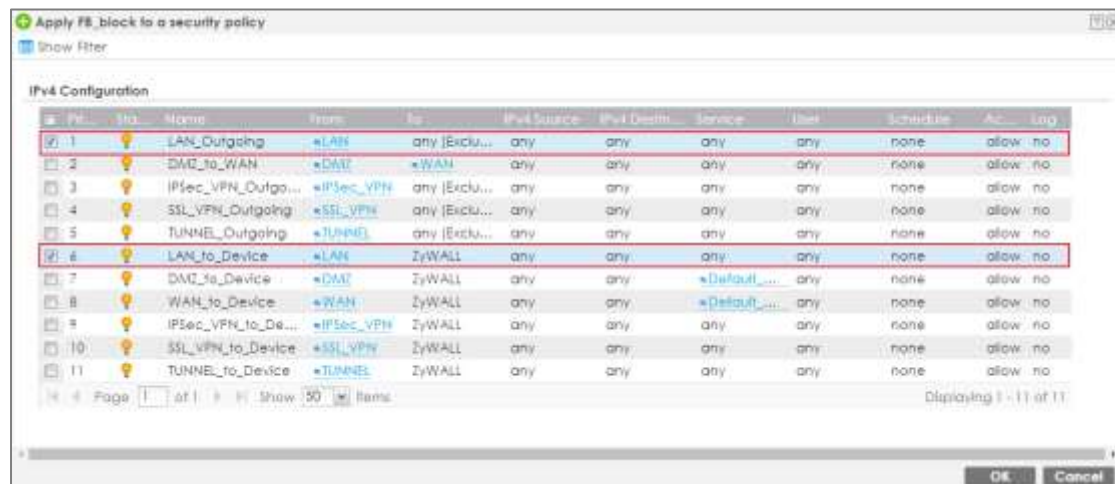
Profile Management

Note:
After you have created the DNS Content Filter profile, please apply it to a security policy going from your internal network (LAN, DMZ, VPN) to both **Any** (Excluding ZyWALL) and **ZyWALL**.

Info

Profile FB_block has been saved. A profile takes effect only when it is applied to a security policy. Apply this profile to a security policy now?

Please apply this profile to a security policy going from your internal network to both **Any (Excluding ZyWALL)** and **ZyWALL**.



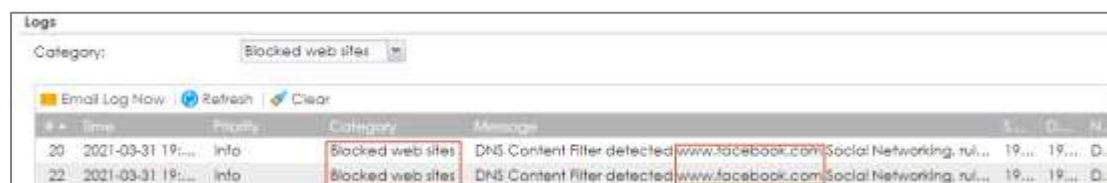
Test the Result

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.

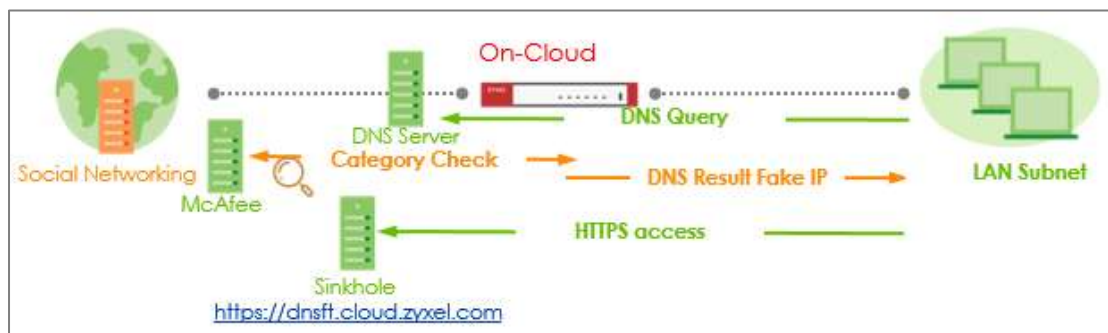



Figure: DNS Content Filter protects user to inappropriate website

 **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

Create content filtering profile

Add profile

Name

FB_block

Description (Optional)

Log

☒

DNS content filtering

Enabled

☒

Click the **category list**, select **Social Networking**, then press **Create** button

Make sure this profile is applied to the security policy


Security policy							
Enabled	Name	Action	Application Profile / Content Filtering Policy	Protocol	Source	Destination	Out Port
<input checked="" type="checkbox"/>	IP_FQ_block	Allow	IP_Block	Any	Any	Any	Any

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.



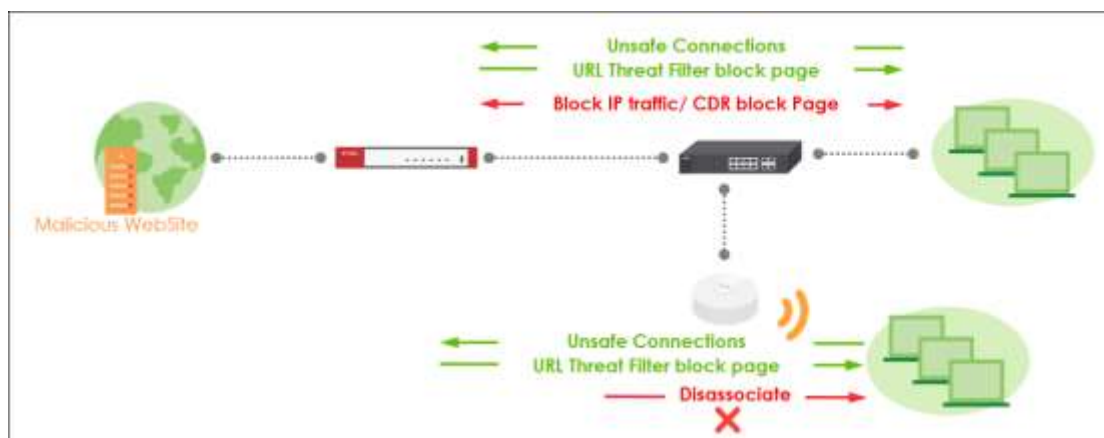
The screenshot shows the 'Content Filter' event log in the Nebula interface. The search bar contains 'facebook'. The log shows 3 matches in 5001 events. The table below lists the blocked access events.

Time	Category	Source	Destination	Detail
2021-04-01 12:20:47	Content Filter	192.168.1.34	192.168.1.1	DNS Content Filter detected zh-hk.facebook.com Social Networking, Rule_name SF_FB_block1
2021-04-01 12:48:52	Content Filter	192.168.1.34	192.168.1.1	DNS Content Filter detected zh-hk.facebook.com Social Networking, Rule_name SF_FB_block1
2021-04-01 12:47:05	Content Filter	192.168.1.34	192.168.1.1	DNS Content Filter detected www.facebook.com Social Networking, Rule_name SF_FB_block1

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:

Policy				
Category	Event type	Occurrence (1-1000 #)	Duration (1-1440 min)	Containment
Malware	Malware detected	2	60	Alert
IDS	Vulnerability exploit detected	2	10	Alert
Web Threat	Connections to malicious web sites detected	2	30	Alert

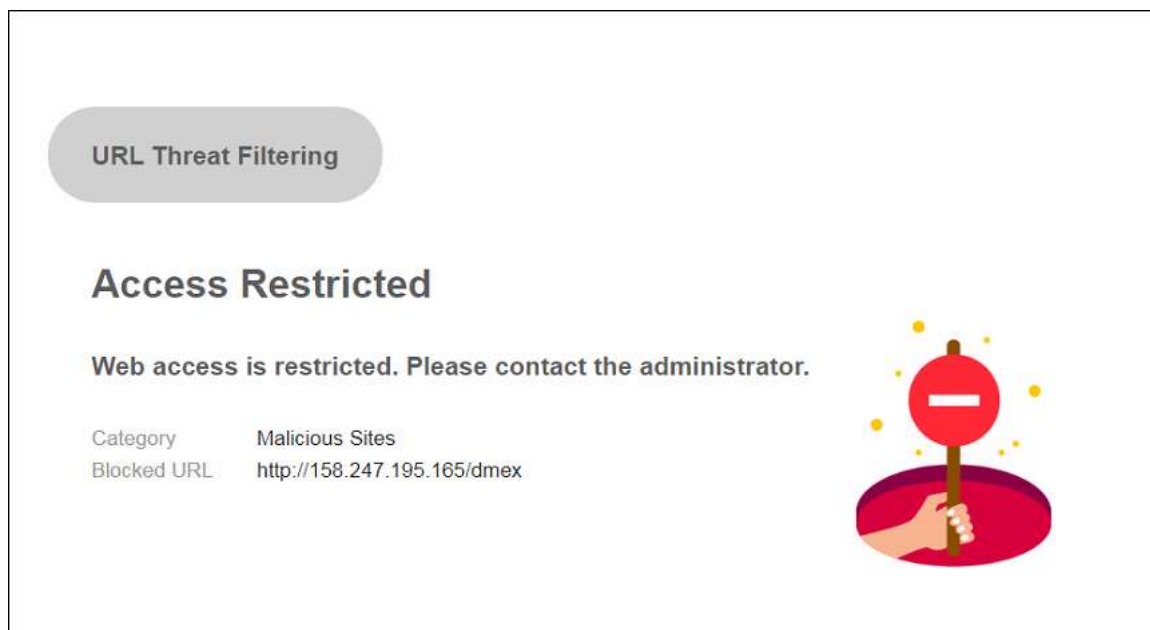
Page 1 of 1 | Show 30 items | Deploying 1 - 3 of 3

Containment

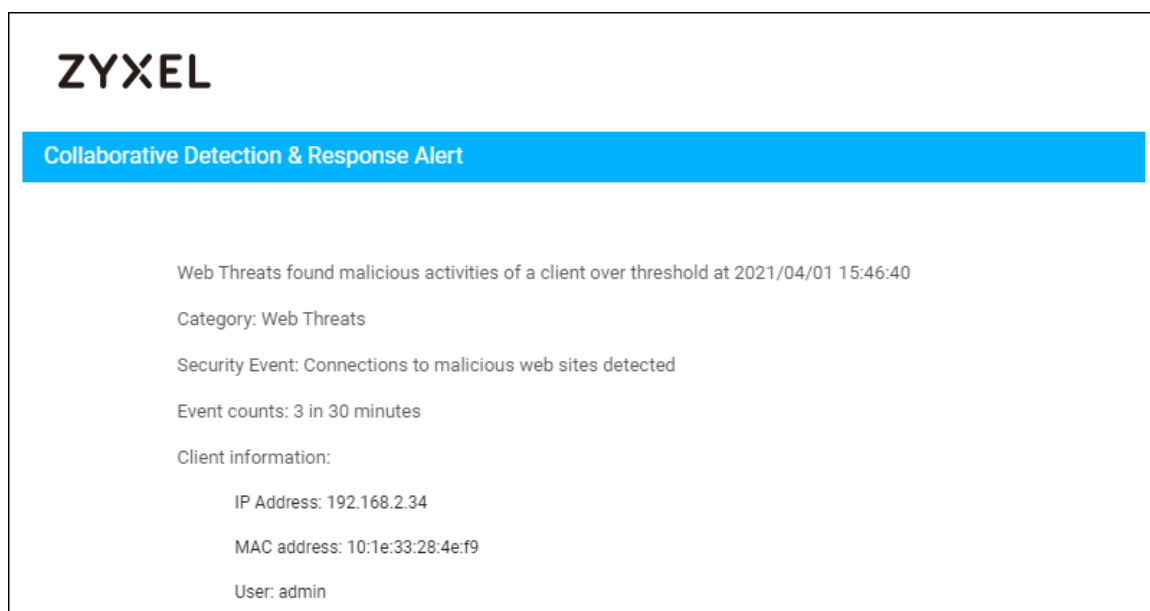
Alert

Email: test@zyxel.com.tw

If client access to malicious website. The connection will be detected by Web Threat Filter service. So browser will display Web Threat Filter page first.



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

View Log

View AP Log

Show Filter

Logs

Category: All Logs

Email Log Now Refresh Clear

#	Time	Priority	Category	Message	Source	Destination	Note
1	2021...	info	CDR	CDR alert mail has been sent successfully.			
2	2021...	alert	CDR	client:192.168.2.34 user:admin from:ge5 security event:Web Thre...			CDR
3	2021...	warn	URL Thre...	158.247.195.165:Malicious Sites, \$StN	192.168.2.34:...	158.247.19...	ACCESS...
4	2021...	warn	URL Thre...	158.247.195.165:Malicious Sites, \$StN	192.168.2.34:...	158.247.19...	ACCESS...
5	2021...	notice	Security ...	Match default rule, DROP (count=3)	10.214.48.26:...	10.214.48.255...	ACCESS...

Page 1 of 1 Show 200 Items

Displaying 1 - 5 of 5

In system log, client traffic will block by Web Threat Filter first. If connection over threshold, it will trigger CDR to send email.



Note: If CDR is configured as "Alert", CDR will only send alert mail without additional action, but client traffic still protected by others UTM services.

Block:

Policy				
Edit				
Category	Event Type	Occurrence (1-100) *	Duration (1-1440 mins)	Containment
Malware	Malware detected	2	60	Block
CDP	Vulnerability exploit detected	2	10	Block
Web Threat	Connections to malicious web sites detected	2	30	Block
Page 1 of 1 Show 50 items Displaying 1 - 3 of 3				
Containment ⓘ				
Alert				
Email: test@zyxel.com.tw				
Block & Quarantine				
Notification Page: <input checked="" type="radio"/> Denied access message <input type="radio"/> Redirect external URL				
There are malicious network activities found on your device. Please contact network administrator.				
Containment Period: 60 [infinite, 1-1440 mins]				

If client accesses to malicious website. The connection will be detected by Web Threat Filter service. So browser will display block page of Web Threat Filter page first. When connection reaches threshold, then all of client IP traffic will be blocked by CDR function in a period time. On client browser, it will display CDR block page.

Collaborative Detection & Response

Limited Network Access

There are malicious network activities found on your device. Please contact network administrator.

Category	Web Threats
Security Event	Connections to malicious web sites detected
Event Counts	3 in 30 minutes
Containment	Block
User IP address	192.168.2.34
User MAC address	10:1e:33:28:4e:f9
User Name	-



In block page, it will show block reason and client IP/MAC information.

System log:

Email Log Now Refresh Clear							
#	Time	Priority	Category	Message	Source	Destination	Note
1	2021/04/01 16:16:17	alert	CDR	client:192.168.2.34 user: from:ge5 security event:Web Threats thresh...	192.168.2.34	158.247.1...	CDR
2	2021/04/01 16:16:17	warn	URL Thr...	158.247.195.165:Malicious Sites. \$SIPN	192.168.2.34	158.247.1...	ACCES...

Page 1 of 1 | Show 200 items | Displaying 1 - 2 of 2

You can also check containment list:

Monitor > Security Statistics > CDR

Containment List							
Add to whitelist Release							
Time	IP Address	MAC Address	User	Security Events	Containment	Time Re... (seconds)	Connect to
2021/04/01 16:16:17	192.168.2.34	10:1e:33:28:4e:f9	-	Connections to malicious we...	Block	3519	ge5

If client is blocked by CDR, client will be added into containment list. In this list, you can check the remaining time of block period. Client will be automatically released once the remaining time is countdown to 0. Or you can click release button to release client manually.

For wireless client. You can enable "Block Wireless client" checkbox to prevent the

wireless client re-associates to the AP.

Block
☒ Block wireless client

Quarantine
 Quarantine VLAN ID:

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 Def...	
15	202...	Alert	CDR	client:192.168.1.39 user: from:AP-BCCF4F65E156 security event:...	CDR



Note: If "Block Wireless Client" checkbox is disabled, the wireless client still keep connection with AP but traffic is blocked by CDR.

Quarantine:

Policy

Category	Event type	Occurrence (1-100) *	Duration (1-1440 mins)	Containment
Malware	Malware detected	2	60	Quarantine
IDP	Vulnerability exploit detected	2	10	Quarantine
Web threat	Connections to malicious web sites detected	2	30	Quarantine

Containment
 Alert
 Email:
 Block & Quarantine
 Notification Page: ☒ Denied access message ☐ Redirect external URL
 Containment Period: (Infinite, 1-1440 mins)
 Block
☒ Block wireless client
 Quarantine
 Quarantine VLAN ID:

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.

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.

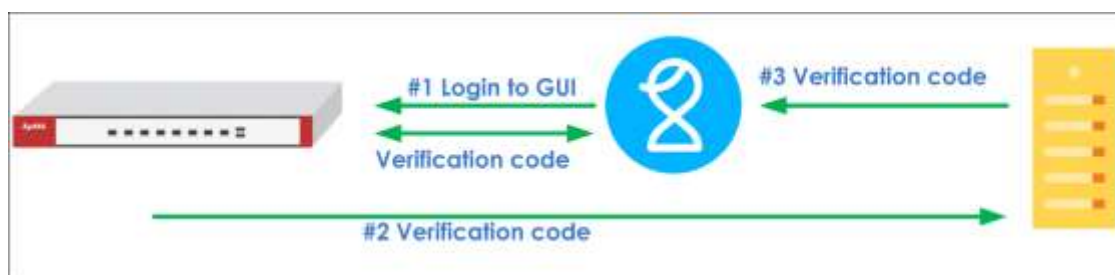
Router(config)# cdr blocked-by ip | mac

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 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.

- Mail server
- Mail server ports
- Mail From
- SMTP Authentication

Mail Server

SMS

General Settings

Mail Server:

smtp.gmail.com

(Outgoing SMTP Server Name or IP Address)

Mail Subject:

☐ Append system name
 ☐ Append date time

Mail Server Port:

587

☒ TLS Security
 ☒ STARTTLS
 ☐ Authenticate Server

Mail From:

s.y@gn

(Email Address)

☒ SMTP Authentication

User Name :

s.y

Password:

.....

Retype to Confirm:

.....

Schedule

Time For Sending Report:

0

(hours)

0

(minutes)

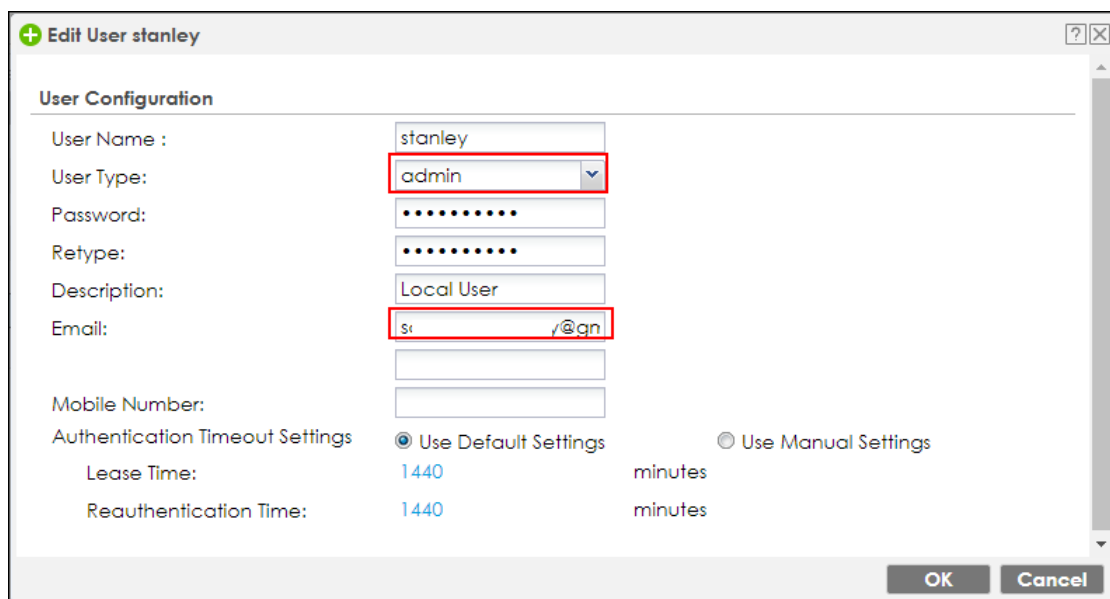


Note: Must make sure SMTP Server configuration is correct otherwise user will unable receive mail successfully.

Create admin type user on device

Go to **Configuration > Object > User/Group > User Click** Add button to create an user and user type is admin.

And also entered email address of this user.



Edit User stanley

User Configuration

User Name : stanley

User Type: admin

Password:

Retype:

Description: Local User

Email: st...@qn...

Mobile Number:

Authentication Timeout Settings

☒ Use Default Settings ☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

OK Cancel

Setup Two-Factor Authentication for admin on your device

Go to **Configuration > Object > Auth Method > Two-Factor Authentication > Admin Access**

Enable the function and add admin user which you added in step2 in the rule, and you can select what services are 2 Factor authentication needed.

Authentication Method

Two-factor Authentication

VPN Access

Admin Access

General Settings

☒ Enable

Valid Time: (1-5 minutes)

Two-factor Authentication for Services:

☒ Web
 ☒ SSH
 ☒ TELNET

User

Selectable User Objects

=== Object ===

admin

Selectable User Objects

=== Object ===

stanley

Delivery Settings

Deliver Authorize Link Method: ☐ SMS ☒ Email

Test the Result

After setup these steps and login to device by admin user, the verification code is required.

Web Service:

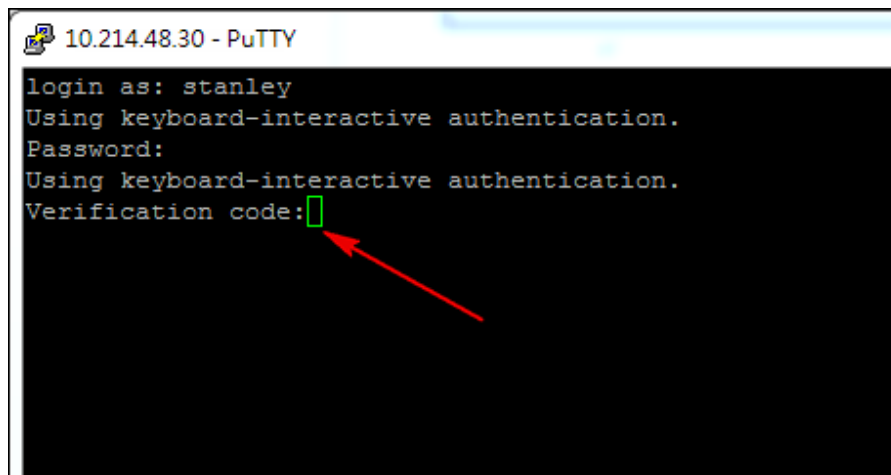
ZYXEL

ATP500

Enter Two-factor Authentication Verification code and click to verify.

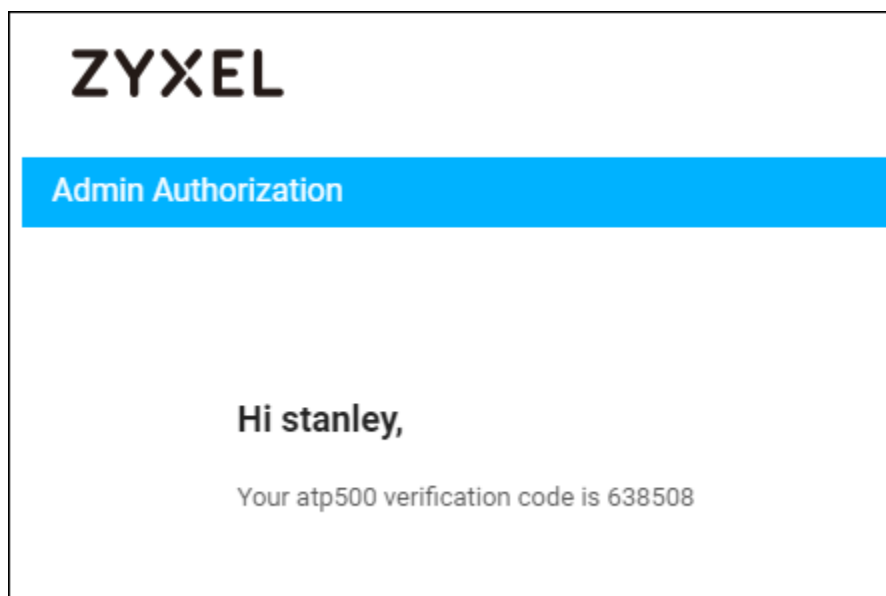
Verify

SSH Service:



A screenshot of a PuTTY terminal window titled "10.214.48.30 - PuTTY". The terminal shows the following text: "login as: stanley", "Using keyboard-interactive authentication.", "Password:", "Using keyboard-interactive authentication.", and "Verification code:". A green rectangular cursor is positioned at the end of the "Verification code:" line, and a red arrow points to it from the right.

You will receive verification code by Email.

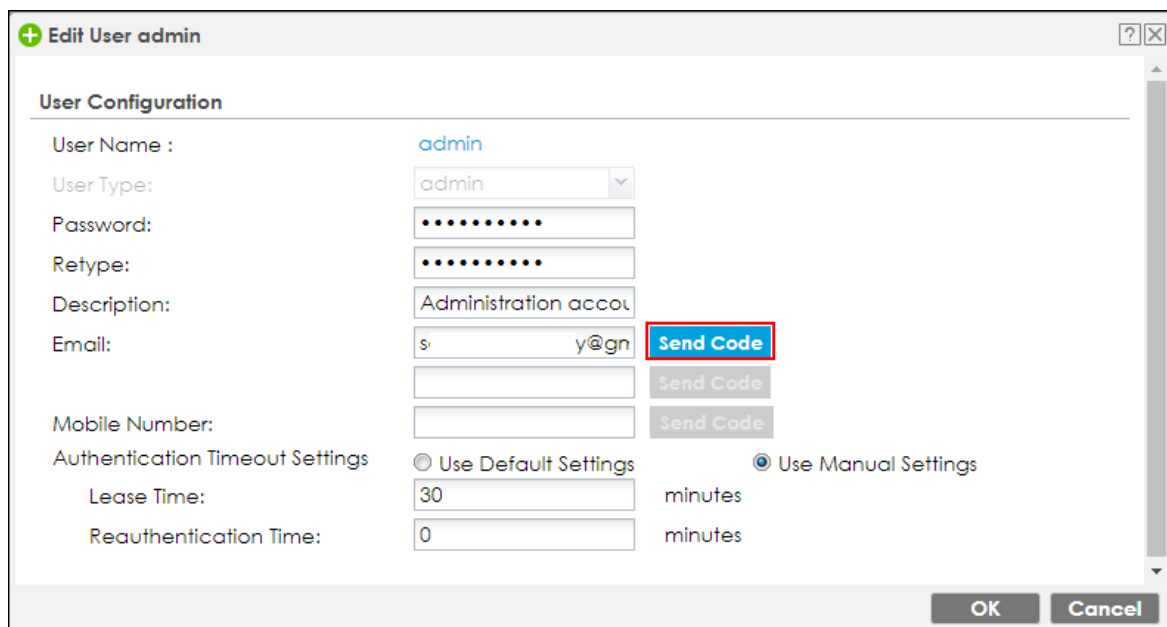


What Can Go Wrong?

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



Edit User admin

User Configuration

User Name : admin

User Type: admin

Password:

Retype:

Description: Administration accou

Email: s. y@gn **Send Code**

Mobile Number:

Authentication Timeout Settings: ☐ Use Default Settings ☒ Use Manual Settings

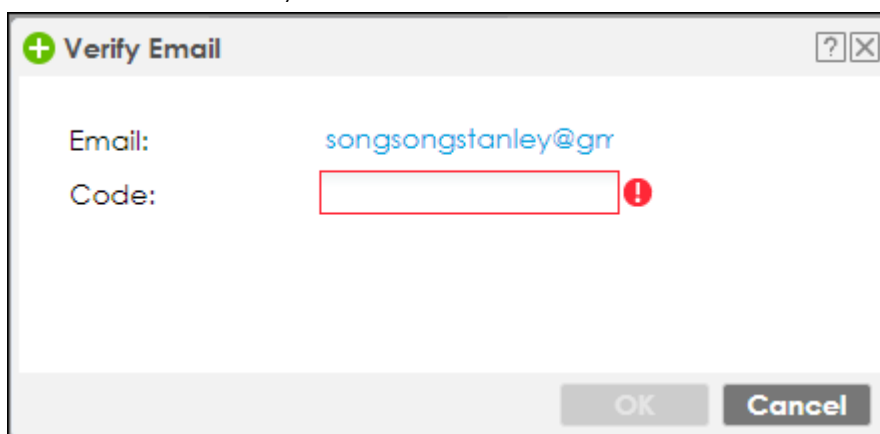
Lease Time: 30 minutes

Reauthentication Time: 0 minutes

OK Cancel

2.2 After clicked “Send Code”, you will receive code by Email.

2.3 Enter code that you received.



Verify Email

Email: songsongstanley@gn

Code:

OK Cancel

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

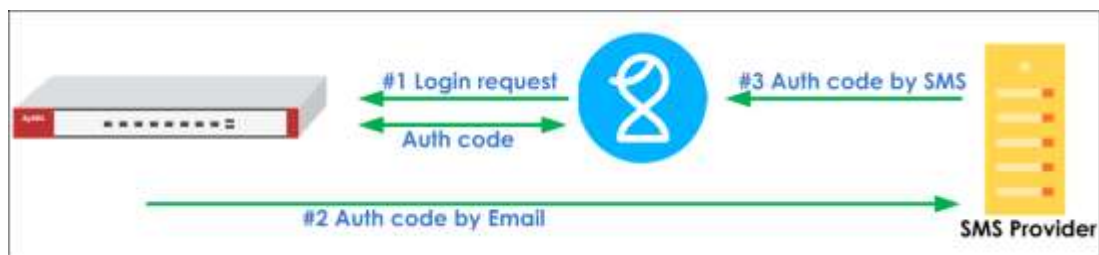
minutes

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 initiated 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

Mail Server

SMS

General Settings

Mail Server:

smtp.gmail.com

(Outgoing SMTP Server Name or IP Address)

Mail Subject:

☐ Append system name
 ☐ Append date time

Mail Server Port:

587

☒ TLS Security
 ☒ STARTTLS
 ☐ Authenticate Server

Mail From:

s.y@gn

(Email Address)

☒ SMTP Authentication

User Name :

s.y

Password:

.....

Retype to Confirm:

.....

Schedule

Time For Sending Report:

0

(hours)

0

(minutes)



Note: Must make sure SMTP Server configuration is correct otherwise message will unable send to SMS provider successfullv.

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”

Mail Server

SMS

General Settings

☒ Enable SMS

Default country code for phone number:

0

(1-4 digit)

SMS Provider:

Email-to-SMS Provider

Provider Domain:

email.smsglobal.com

SMS Provider Email domain

☒ auto append to "Mail to"

Mail Subject:

SMS Message

(Optional)

Mail From:

s.y@gmail.com

Email address

(Optional)

Mail To:

\$mobile_number\$@email.smsglobal.com

Note

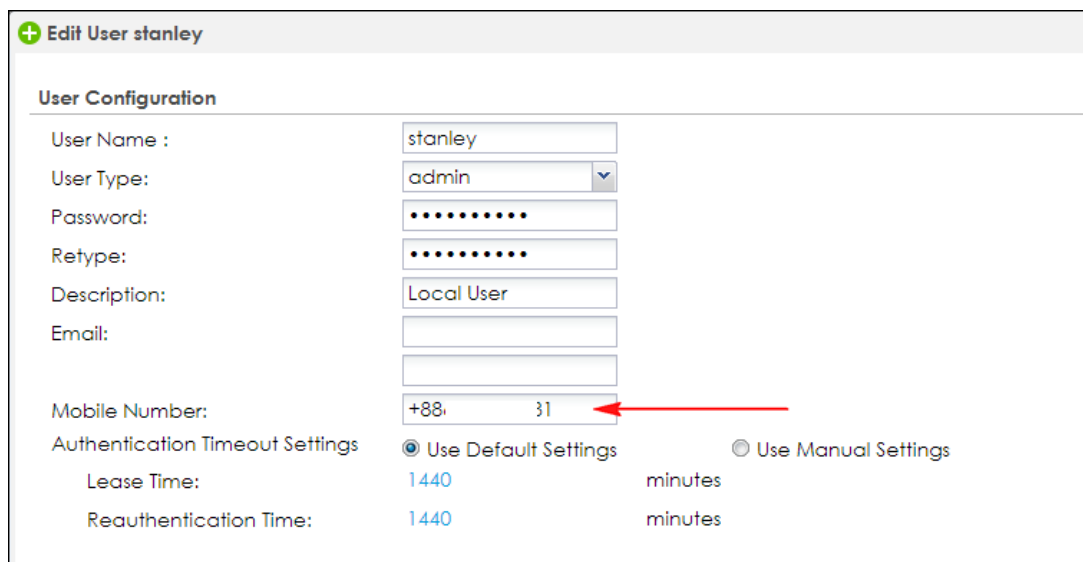
1. If you select to use an Email-to-SMS provider, configure a mail server before you enable SMS.
2. If you leave the Mail From field blank here, the system automatically uses the mail address configured in the Mail Server screen.
3. "Mail To" default format is "\$mobile_number\$@provider domain" and some Service Providers might require prefix symbol like "+" added before \$mobile_number\$.



Note: Your SMS provider has to allow the email address which configured in “Mail From” to prevent the email is denied by SMS provider's mailbox.

Create admin type user on device

Go to **Configuration > Object > User/Group > User** Click Add button to create an user and user type is admin. And also entered phone number of this user.



Edit User stanley

User Configuration

User Name : stanley

User Type: admin

Password:

Retype:

Description: Local User

Email:

Mobile Number: +88, 31

Authentication Timeout Settings

☒ Use Default Settings ☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

Setup Two-Factor Authentication for admin on your device

Go to **Configuration > Object > Auth Method > Two-Factor Authentication > Admin Access**

Enable the function and add admin user which you added in step3 in the rule, and you can select what services are 2 Factor authentication needed. Enable SMS function to send verification code by SMS.

Authentication Method

Two-factor Authentication

VPN Access

Admin Access

General Settings

☒ Enable

Valid Time: (1-5 minutes)

Two-factor Authentication for Services:

☒ Web
 ☒ SSH
 ☒ TELNET

User

Selectable User Objects

=== Object ===

admin

+

-

Selectable User Objects

=== Object ===

stanley

Delivery Settings

Deliver Authorize Link Method: ☒ SMS ☐ Email

Test the Result


After setup these steps and login to device by admin user, the verification code is required.


Web Service:

ZYXEL

ATP500

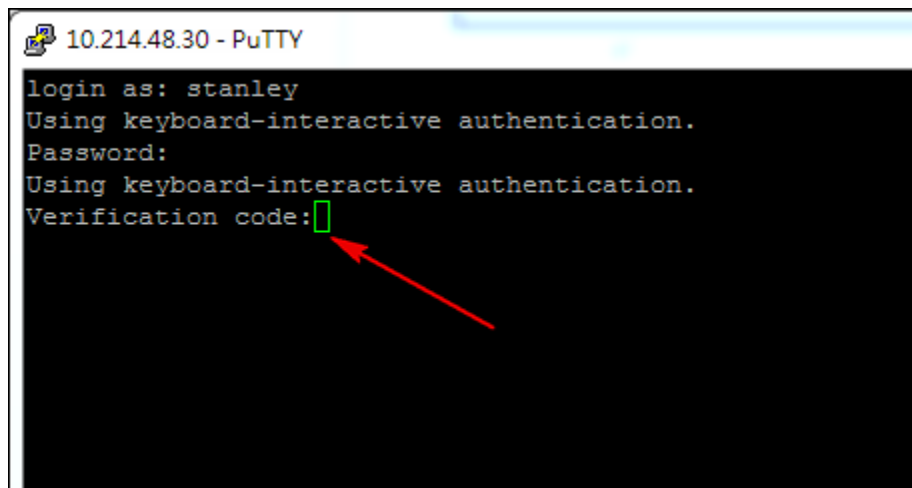
Enter Two-factor Authentication Verification code and click to verify.



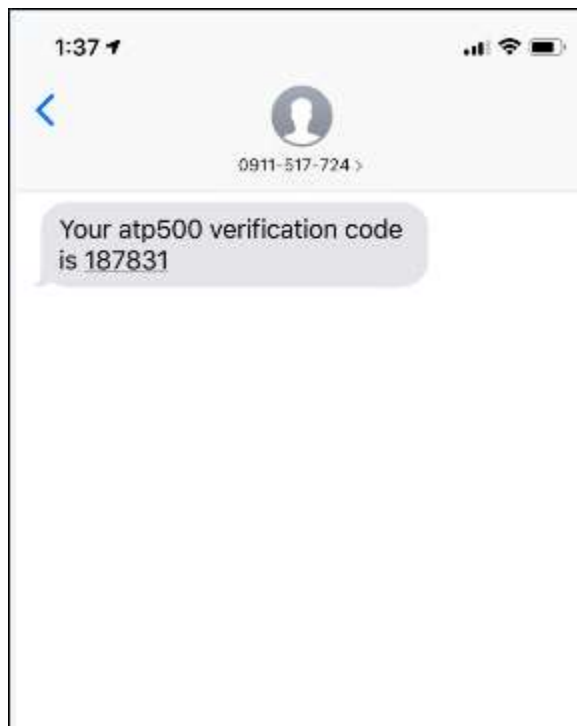


Verify

SSH Service:



You will receive verification code by SMS.



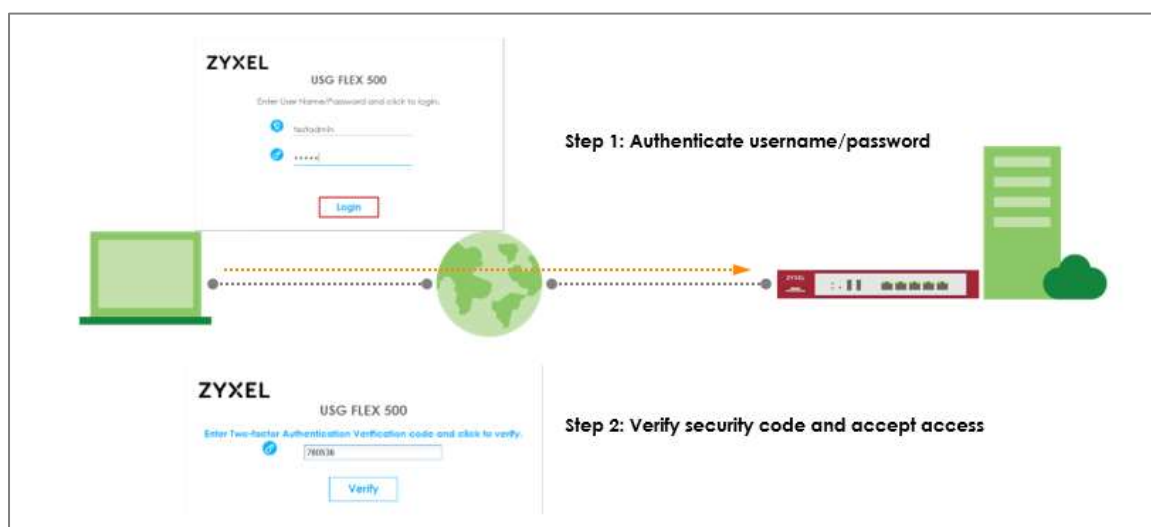
What Can Go Wrong?

- 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

Edit User testadmin

General **Two-factor Authentication**

User Configuration

User Name : testadmin

User Type: admin

Password:

Retype:

Description: Local User

Email: Send Code

Mobile Number: Send Code

Authentication Timeout Settings

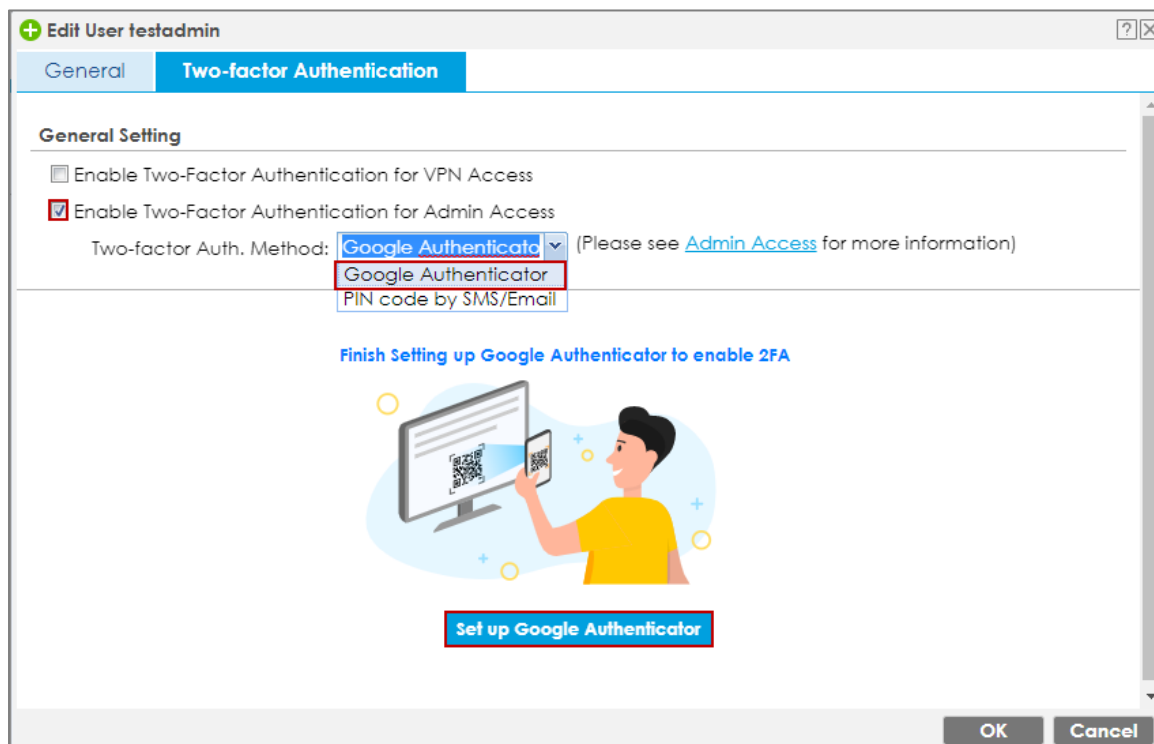
☒ Use Default Settings ☐ Use Manual Settings

Lease Time: 1440 minutes

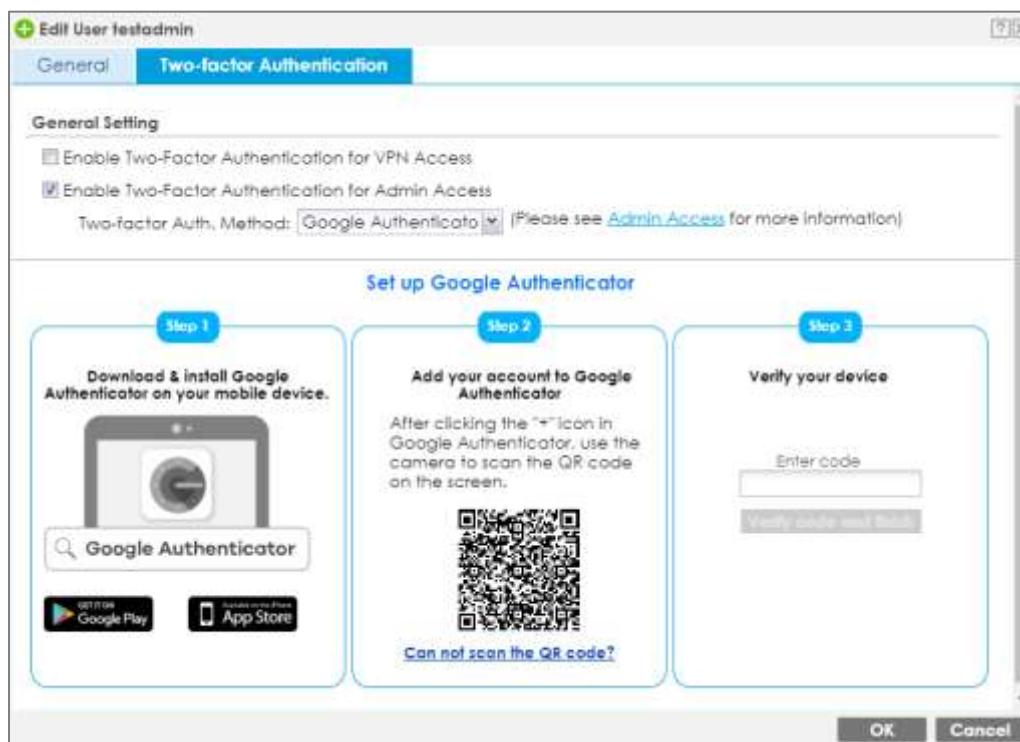
Reauthentication Time: 1440 minutes

OK Cancel

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.

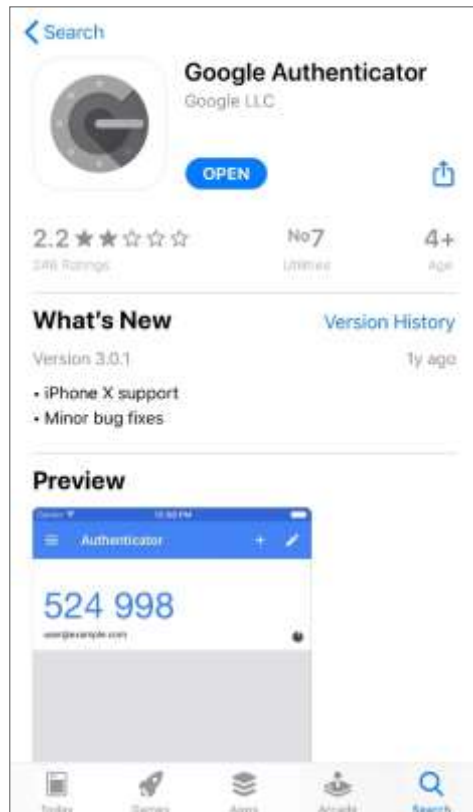


Set up Google Authenticator

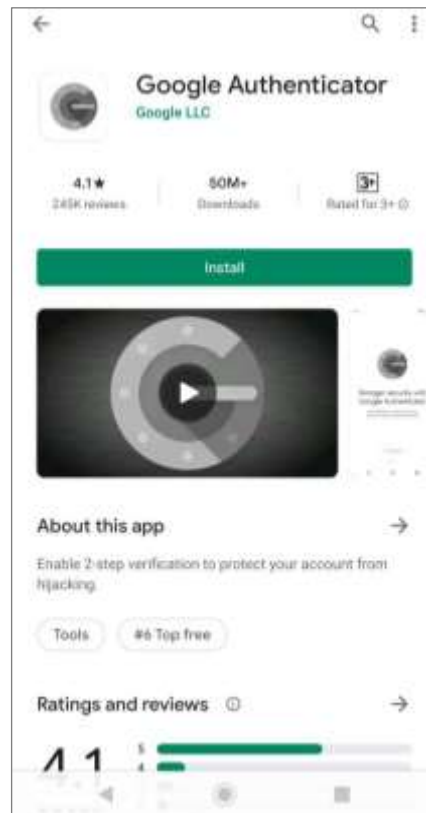


1. Download and install Google Authenticator on your mobile device.

Apple Store



Google Play

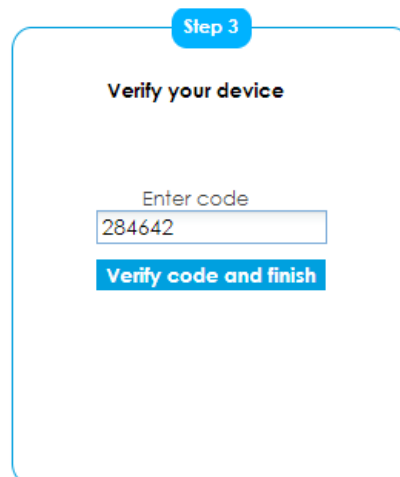
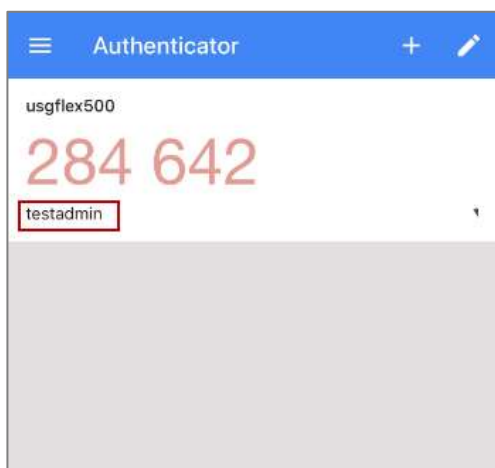


2. Register the admin account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.

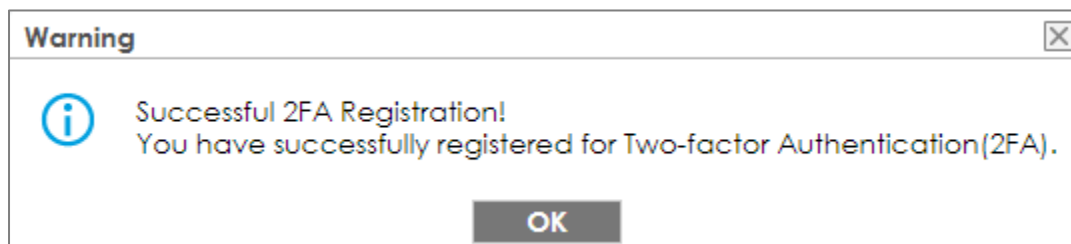




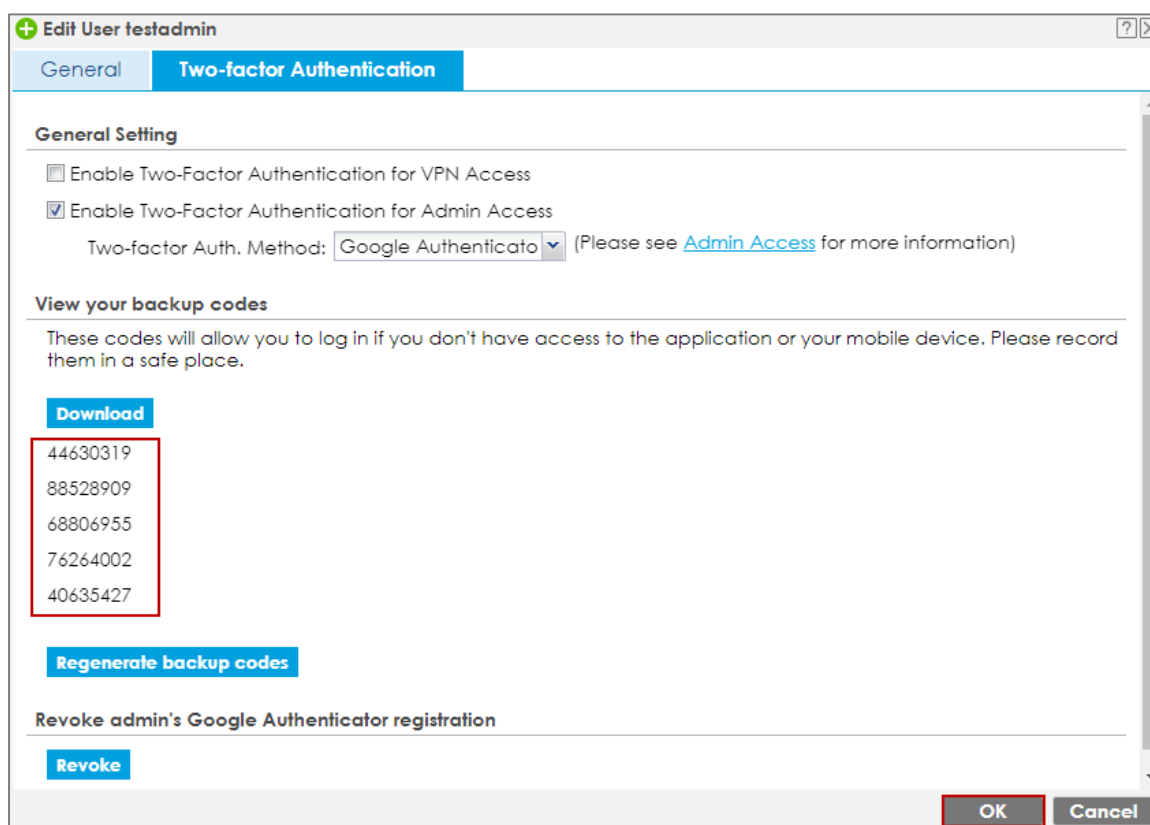
3. Enter the token code which displays on Google Authenticator to "Step 3" and click "Verify code and finish" to submit and verify the code.



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

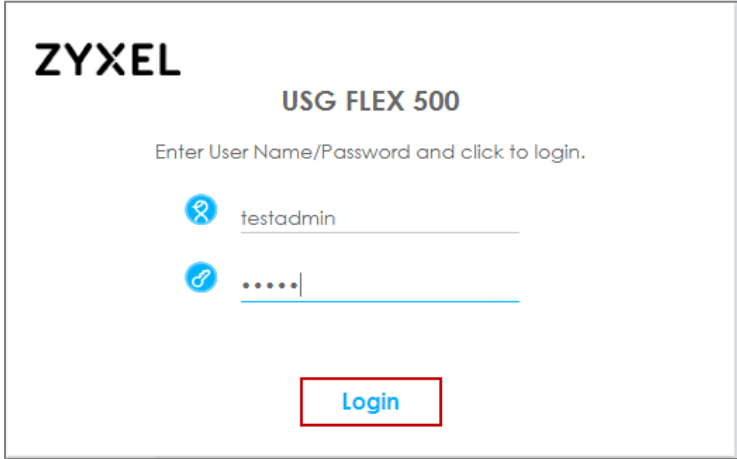
Enable two factor authentication for admin access. Configure valid time and select which services require two-factor authentication for admin user. The valid time is the deadline that admin needs to submit the two-factor authentication code to get the access. The access request is rejected if submitting the code later than valid time. By default, the valid time is 3 minutes.

CONFIGURATION > Object > Auth. Method > Two-factor Authentication > Admin Access

Authentication Method		Two-factor Authentication
VPN Access	Admin Access	
General Settings		
<input checked="" type="checkbox"/> Enable Valid Time: <input type="text" value="3"/> (1-5 minutes) Two-factor Authentication for Services: <input checked="" type="checkbox"/> Web <input checked="" type="checkbox"/> SSH <input type="checkbox"/> TELNET		
Delivery Settings		
Verification Code Delivery Method:		<input type="text" value="Email"/> ▼

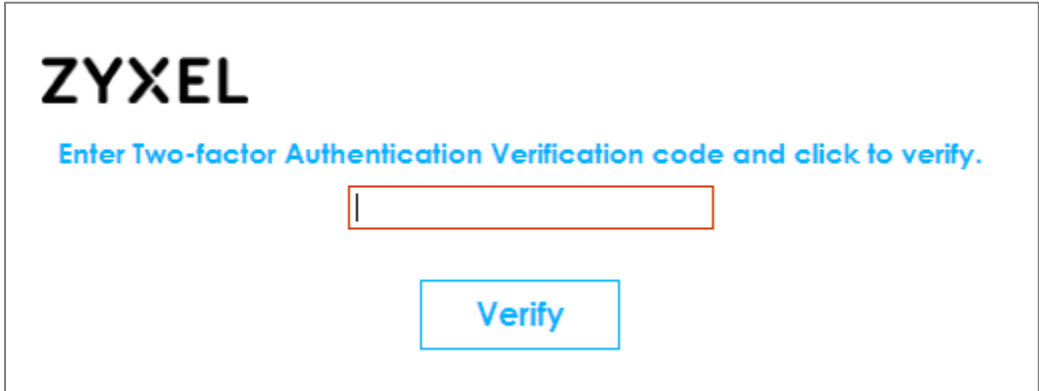
Test the Result

1. Login with the admin account "testadmin".



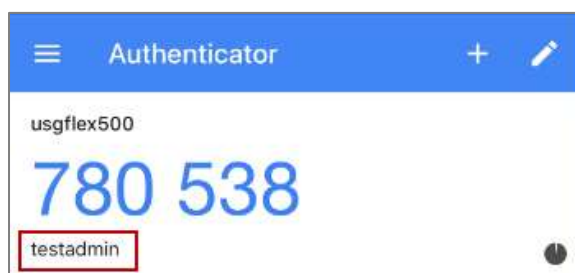
The image shows the login page for a ZYXEL USG FLEX 500 device. At the top left is the ZYXEL logo. To its right, the text "USG FLEX 500" is displayed. Below this, a prompt reads "Enter User Name/Password and click to login." There are two input fields: the first is for the username, containing "testadmin", and the second is for the password, shown as five dots. A blue "Login" button is located at the bottom right of the form area.

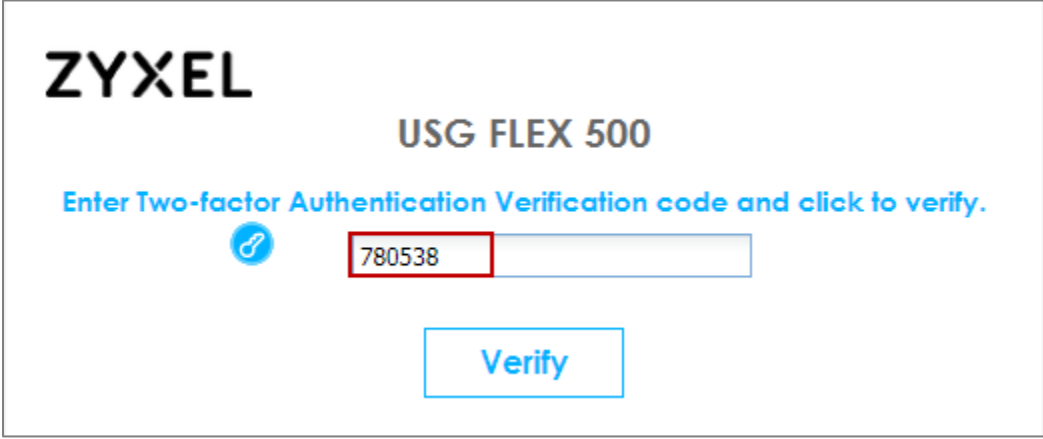
2. A pop-up window appears for administrator to enter the verification code.



The image shows a verification page for two-factor authentication. It features the ZYXEL logo at the top left. Below the logo, a blue prompt reads "Enter Two-factor Authentication Verification code and click to verify." There is a single text input field for the verification code. A blue "Verify" button is positioned at the bottom right of the page.

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.






ZYXEL

USG FLEX 500

Enter Two-factor Authentication Verification code and click to verify.



Verify

4. Authorize with username, password and the token code successfully.

MONITOR > Log > View Log > Category and select "Authentication Server"



View Log | View AP Log | Dynamic Users Log

Show Filter

Logs

Category: **Authentication Server**

Email Log Now | Refresh | Clear

#	Time	Priority	Category	Message	Source	Host
2	202...	notice	Authentication Server	user: testadmin is authorized [count=2]		two-factor auth.
3	202...	notice	Authentication Server	user: testadmin(10.214.36.16) is waiting to authorize.		two-factor auth.
59	202...	Info	Authentication Server	user: testadmin's secret-file is verified.		two-factor auth.

What Can Go Wrong?

1. An admin user only can be registered on one Google Authenticator. If you would like to use another mobile device to authenticate the same admin user, click "Revoke" to revoke registered user and user another mobile device to set up Google Authenticator again.



Revoke admin's Google Authenticator registration

Revoke

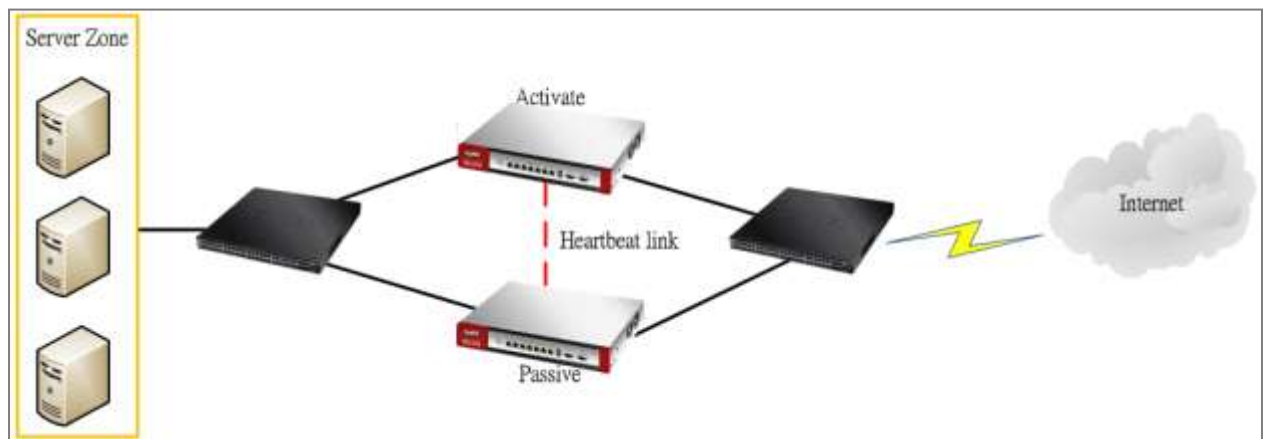
OK **Cancel**

2. Each admin user has 5 backup codes and each backup code could be used only once for login.

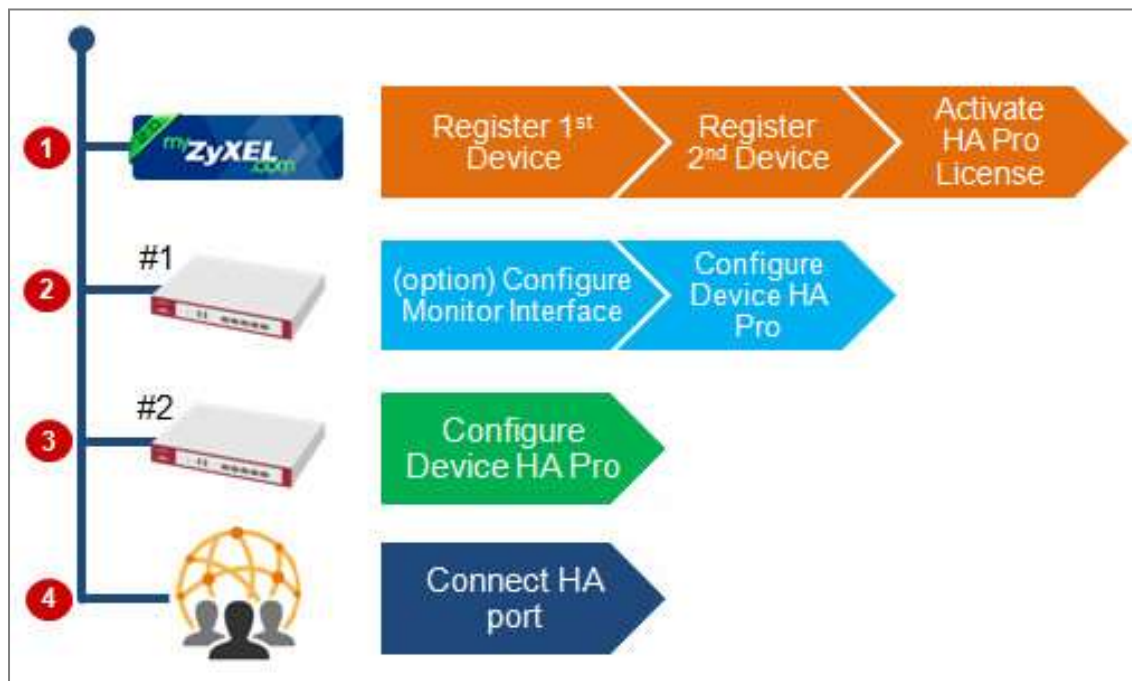
Chapter 4- Device HA

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.



Device HA Pro License

The Device HA Pro feature is license required. You must register both of your devices on the **myZyXEL.com** server first. Then make sure the Device HA Pro license is available on both of your devices.

Registration Service					
Service Status					
#	Service	Status	Service Type	Expiration Date	Count
1	Content Filter 2.0	Activated	Trial	2017-10-20	N/A
2	Geo Enforcer	Activated	Standard	2018-10-21	N/A
3	Managed AP Service	Default	Standard		4
4	SSL VPN Service	Default			50
5	Zymesh Service	Not Licensed			N/A
6	Hotspot Management Subscription Ser...	Activated	Trial	2017-10-20	N/A
7	Concurrent Device Upgrade	Default	Standard		200
8	Device HA Pro	Activated	Standard		N/A
9	Firmware Upgrade Service	Activated			N/A

Page 1 of 1 Show 50 items

Service Refresh

Service License Refresh

Note: Update device license information from myZyXEL.com server. If you want to activate license, please go to portal.myzyxel.com

Behavior of the Device HA Pro

The behavior of the Device HA Pro includes a heartbeat link to monitor the

“activate” device’s interface status. If one of the monitored interfaces is dead or fails, the “passive” device’s status will 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.

Device HA Status	Device HA Pro	View Log
Configuration		
<input checked="" type="checkbox"/> Enable Configuration Provisioning From Active Device.		
Serial Number of Licensed Device for License Synchronization:	<input type="text" value="S172L15290017"/>	
Active Device Management IP:	<input type="text" value="20.20.20.1"/>	
Passive Device Management IP:	<input type="text" value="20.20.20.2"/>	
Subnet Mask:	<input type="text" value="255.255.255.0"/>	
Password:	<input type="password" value="...."/>	
Retype to Confirm:	<input type="password" value="...."/>	
Heartbeat Interval:	<input type="text" value="2"/>	seconds (1-10)
Heartbeat Lost Tolerance:	<input type="text" value="2"/>	(1-10)

Monitor Interface

Available Interfaces

=== Object ===

ge3

ge4

ge5

ge6

Monitor Interface

=== Object ===

ge1

ge2

Failover Detection

☒ Enable Failover When Interface Failure (Option)

☐ Enable Failover When Device Service Fails (Option)

The Main Function of the Device HA Pro

Device HA Status

Device HA Pro

View Log

General Settings

Configuration Walkthrough

Troubleshooting

☒ Enable Device HA

Heartbeat Link

The heartbeat port is a new physical port on the device.

After you have enabled Device HA Pro, the devices will transmit multicast packets (UDP 694) to check each device's status.

When the passive device is working properly, the system LED light will be on. Only the heartbeat port's LED light can be on.

Suggestions

1. Transfer all the licenses to the primary device. This helps to avoid the system from recounting licenses every time.
2. Enable the connectivity check function on the monitored interfaces. When an interface doesn't receive any response from the remote server for a certain period of time, the device will consider the interface status as fail. Then the Device HA Pro feature will change the status of the interface.

How do I Configure Device HA Pro in My Current Environment?



License

The Device HA Pro feature is license required. Please go to register both of your devices on **myZyXEL.com** and make sure the devices have the license after syncing with the **myZyXEL.com** server.

Registration					
Service					
Service Status					
#	Service	Status	Service Type	Expiration Date	Count
1	Content Filter 2.0	Activated	Trial	2017-10-20	N/A
2	Geo Enforcer	Activated	Standard	2018-10-21	N/A
3	Managed AP Service	Default	Standard		4
4	SSL VPN Service	Default			50
5	Zymesh Service	Not Licensed			N/A
6	Hotspot Management Subscription Ser...	Activated	Trial	2017-10-20	N/A
7	Concurrent Device Upgrade	Default	Standard		200
8	Device HA Pro	Activated	Standard		N/A
9	Firmware Upgrade Service	Activated			N/A

< < Page 1 of 1 > > Show 50 items

Service Refresh
 Service License Refresh

Note:
 Update device license information from myZyXEL.com server. If you want to activate license, please go to portal.myzyxel.com

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**.

Device HA Status

Device HA Pro

View Log

Configuration

☐ Enable Configuration Provisioning From Active Device.

Serial Number of Licensed Device for License Synchronization:

S172L15290017

Active Device Management IP:

20.20.20.1

Passive Device Management IP:

20.20.20.2

Subnet Mask:

255.255.255.0

Password:

....

Retype to Confirm:

....

Heartbeat Interval:

2

seconds (1-10)

Heartbeat Lost Tolerance:

2

(1-10)

Monitor Interface

Available Interfaces

=== Object ===

ge3

ge4

ge5

ge6

→

←

Monitor Interface

=== Object ===

ge1

ge2

Failover Detection

☒ Enable Failover When Interface Failure (Option)

☐ Enable Failover When Device Service Fails (Option)

Go to the **Configuration > Device HA > General** screen.

Select **Enable Device HA** and click **Apply** to enable Device HA Pro.

Device HA Status

Device HA Pro

View Log

General Settings

Configuration Walkthrough

Troubleshooting

☒ Enable Device HA

Configurations on the Secondary Device

Go to the **Configuration > Device HA > Device-HA Pro** screen.

Select **Enable Configuration Provisioning from Active Device**.

Click **Apply**.

Device HA Status

Device HA Pro

View Log

Configuration

☒ Enable Configuration Provisioning From Active Device

Serial Number of Licensed Device for License Synchronization:

Active Device Management IP:

Passive Device Management IP:

Subnet Mask:

Password:

Retype to Confirm:

Heartbeat Interval:
 seconds (1-10)

Heartbeat Lost Tolerance:
 (1-10)

Monitor Interface

Available Interfaces

=== Object ===

ge1
 ge2
 ge3
 ge4

+

+

Monitor Interface

Failover Detection

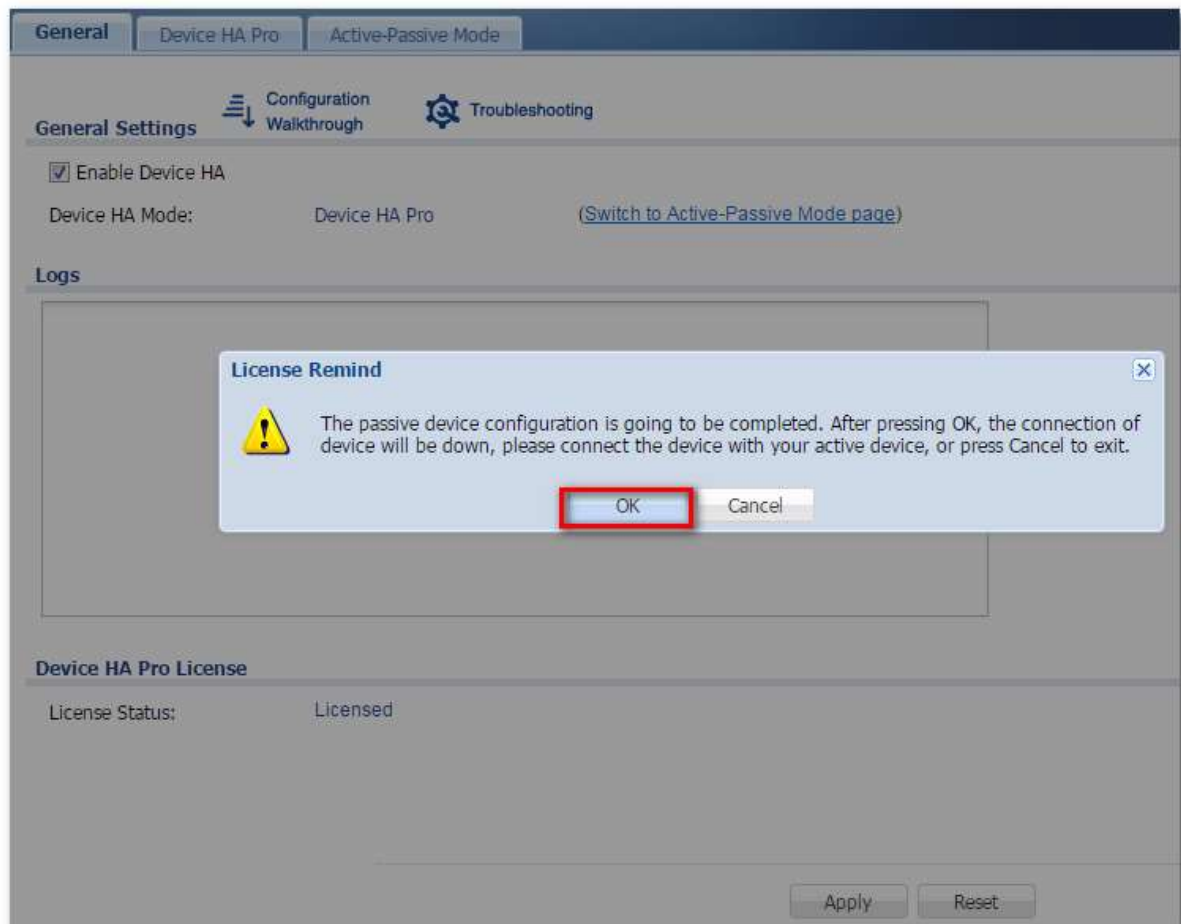
☐ Enable Failover When Interface Failure (Option)

☐ Enable Failover When Device Service Fails (Option)

Go to the **Configuration > Device HA > General** screen.

Select **Enable Device HA** and click **Apply**.

Before the Device HA Pro feature is enabled on the secondary device, a **warning message** will pop-up for you to confirm. Click **OK** to enable it.



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 entering 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.

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.

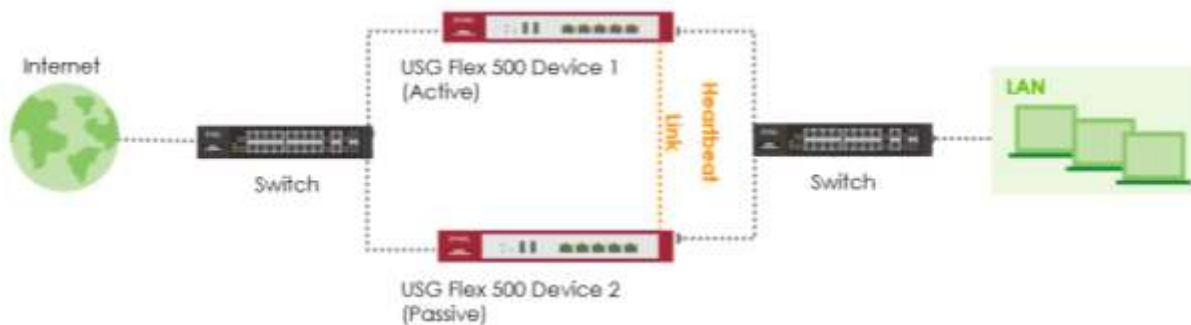
3. Why after Device-HA failover to secondary device, it will not fallback to primary device?

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.

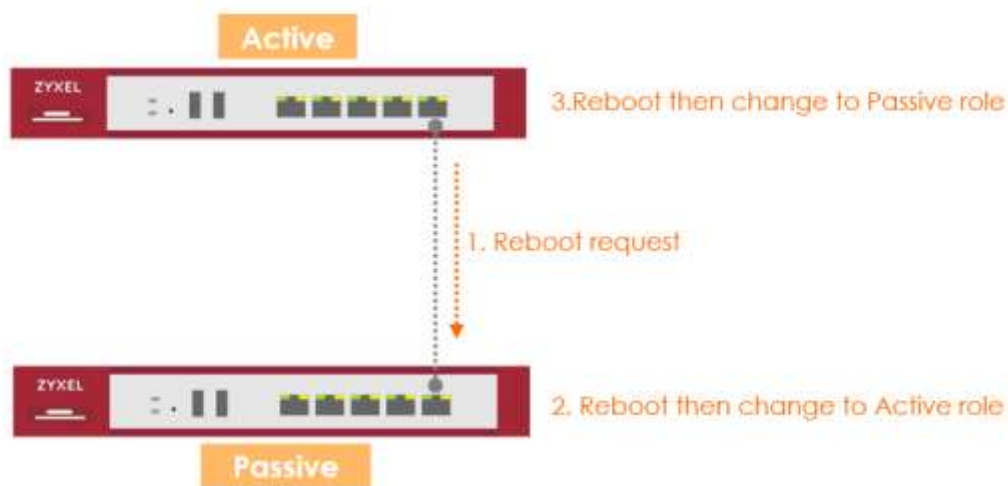


Verification

When you enable schedule reboot in Device HA mode, the active device will send reboot request to passive device first.

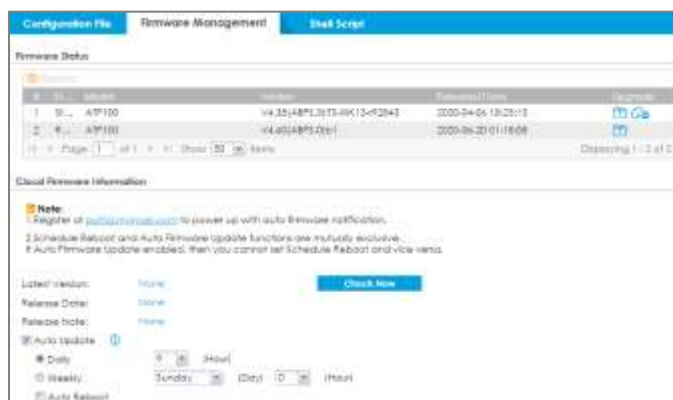
After passive device reboot successfully, the passive device changes to active role.

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 Upgrade 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 reboot the device. Please wait a minute until the logon page appears in your web 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.

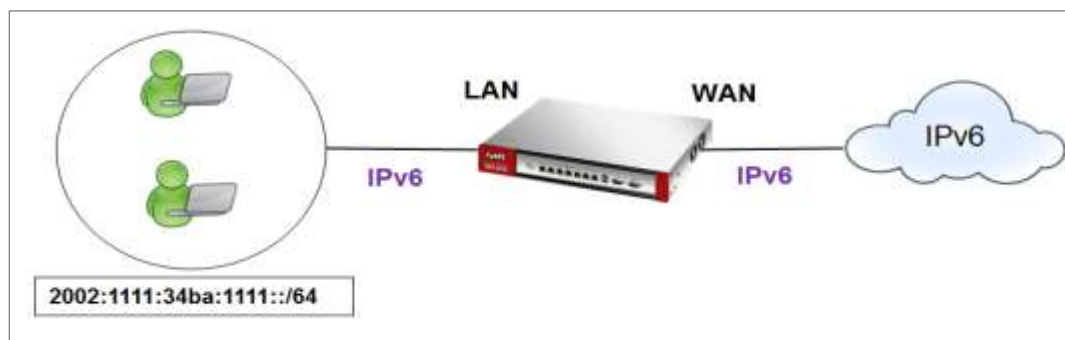
OK

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 IPv6 Interfaces for Pure IPv6 Routing

This example shows how to configure your USG Z's WAN and LAN interfaces which connects two IPv6 networks. USG Z periodically advertises a network prefix of 2006:1111:1111:1111::/64 to the LAN through router advertisements.



ZyWALL/USG access the internet via IPv6

Note:

Instead of using router advertisement, you can use DHCPv6 to pass the network settings to the computers on the LAN.

This example was tested using USG110 (Firmware Version: ZLD 4.25) and ZyWALL 310 (Firmware Version: ZLD 4.25).

Setting Up the IPv6 Interface

Wan

1. In the CONFIGURATION > Network > Interface > Ethernet screen's IPv6 Configuration section, double-click the wan1.
2. The Edit Ethernet screen appears. Select Enable Interface and Enable IPv6. Select Enable Auto-Configuration. Click OK.

Note: Your ISP or uplink router should enable router advertisement.

The screenshot shows the 'Edit Ethernet' configuration page for an IPv6 interface. The page is divided into several sections:

- General Settings:** Includes a checkbox for 'Enable Interface' which is checked.
- General IPv6 Setting:** Includes a checkbox for 'Enable IPv6' which is checked.
- Interface Properties:**
 - Interface Type: external
 - Interface Name: ge2
 - Port: P2
 - Zone: WAN
 - MAC Address: 88EC:A3A9:C034
 - Description: (Optional)
- IPv6 Address Assignment:**
 - Enable Stateless Address Auto-configuration (SLAAC): checked
 - Link-Local Address: n/a
 - IPv6 Address/Prefix Length: (Optional)
 - Advanced: expanded
- DHCPv6 Setting:**
 - DHCPv6: N/A
- IPv6 Router Advertisement Setting:**
 - Enable Router Advertisement: checked
 - Advanced: expanded
 - Router Preference: Medium

Lan

1. In the CONFIGURATION > Network > Interface > Ethernet screen, double-click the lan1 in the IPv6 Configuration section.
2. The Edit Ethernet screen appears. Select Enable Interface and Enable IPv6. Select Enable Router Advertisement and click Add and configure a network prefix for the LAN1 (2006:1111:34ba:1111::/64 in this example). Click **OK**.

General Settings

☒ Enable Interface

General IPv6 Setting

☒ Enable IPv6 ?

Interface Properties

Interface Type: Internal ?

Interface Name: ge4

Port: P4

Zone: LAN1 ?

MAC Address: BB:EC:A3:A9:C8:D6

Description: (Optional)

IPv6 Address Assignment

☐ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: n/a

IPv6 Address/Prefix Length: (Optional)

☒ Advance

IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

☒ Advance

Router Preference: Medium

☒ Advance

Advertised Prefix Table

	IPv6 Address/Prefix Length
1	2002:1111:34ba:1111::/64

Page 1 of 1 | Show 50 items | No data to display

☒ Advance

3. Using command line ipconfig to check.

```

C:\Windows\system32\cmd.exe
Windows IP Configuration

Wireless LAN adapter Wireless Network Connection:

    Connection-specific DNS Suffix . : 
    Link-local IPv6 Address . . . . . : fe80::5138:dc32:ff2f:6a34%12
    IPv4 Address. . . . . : 10.251.61.91
    Subnet Mask . . . . . : 255.255.254.0
    Default Gateway . . . . . : 10.251.61.253

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : 
    IPv6 Address. . . . . : 2002::1111:34ba:1111:d1b3:8580:1506:4d72
    Temporary IPv6 Address. . . . . : 2002::1111:34ba:1111:5cdd:2779:4c5e:9fe
    Link-local IPv6 Address . . . . . : fe80::d1b3:8580:1506:4d72%11
    IPv4 Address. . . . . : 192.168.2.34
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::5ef4:abff:fef9:d4d4%11
                                192.168.2.1

Tunnel adapter isatap.{1C5CCB06-45A8-4C5E-AB6A-32D5DE7DA785}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

Tunnel adapter isatap.{7824C2F6-F6C2-4A7C-BBF5-10CF6F23CEE3}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . : 

C:\Users\ZT02340>

```

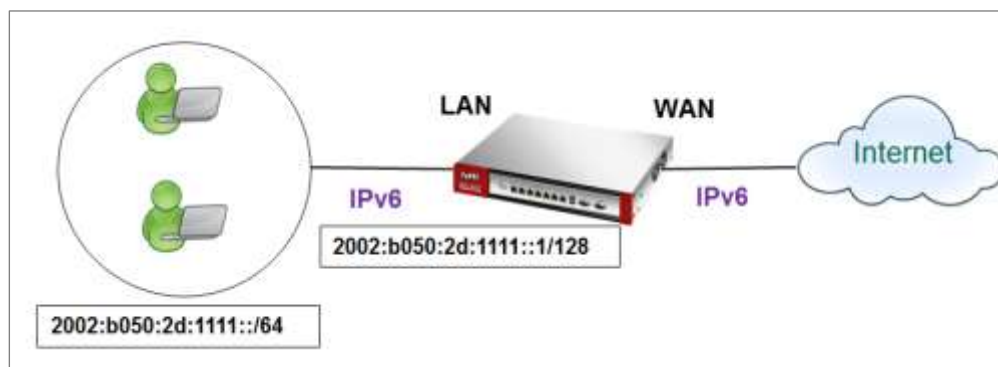
Set up the Prefix Delegation and Router Advertisement

This example shows how to configure prefix delegation on the ZyWALL's WAN and router advertisement on the LAN.

Apply a network Prefix From Your ISP

First of all, you have to apply a network prefix from your ISP or the uplink router's administrator. The WAN port's DUID is required when you apply the prefix. You can check the DUID information in the **WAN IPv6 Interface Edit** screen.

This example assumes that you were given a network prefix of 2001:b050:2d::/48 and you decide to divide it and give 2001:b050:2d:1111::/64 to the LAN network. LAN1's IP address is 2001:b050:2d:1111::1/128.



Setting Up the WAN IPv6 Interface

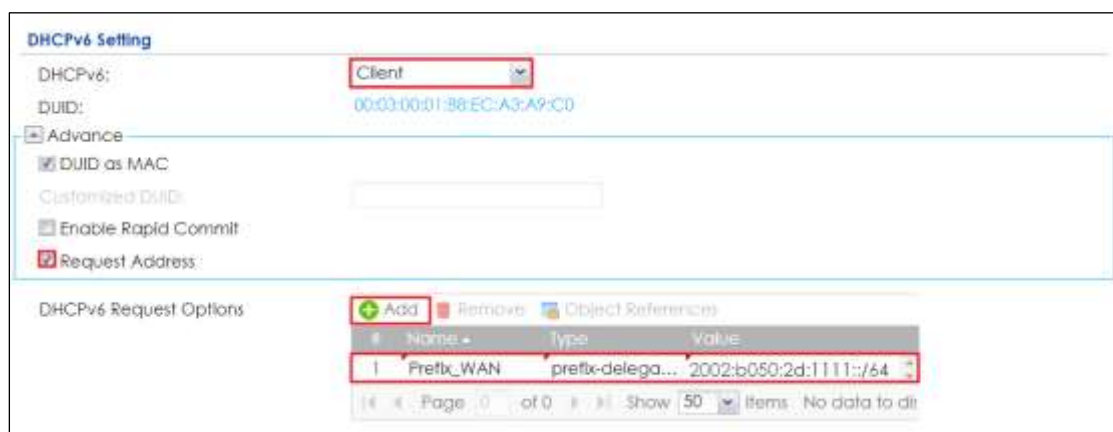
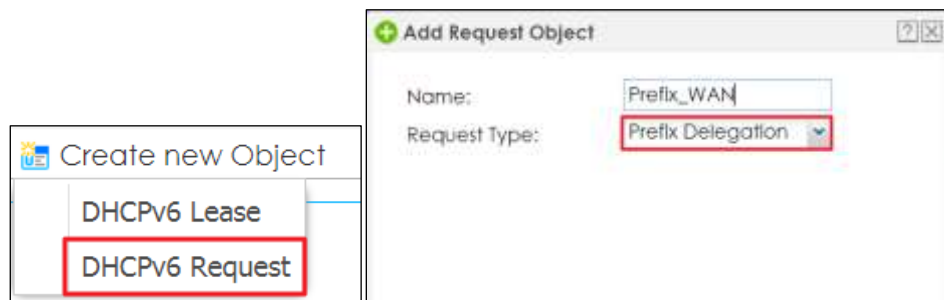
1. In the **Configuration > Network > Interface > Ethernet** screen's **IPv6 Configuration** section,
double-click the **WAN** interface.
2. The Edit Ethernet screen appears. Select **Enable Interface** and **Enable IPv6**.
Click **Create new Object** to add a DHCPv6 Request object with the Prefix Delegation type.
Select **Enable Auto-Configuration**.
Select **Client** in the DHCPv6 field. (WAN1's DUID appears.)

Click **Add** in the DHCPv6 Request Options table and select the DHCPv6 request object you just created. You cannot see the prefix your ISP gave you in the Value field until you click **OK** and then come back to this screen again. It is 2001:b050:2d::/48 in this example.

Note: Your ISP or a DHCPv6 server in the same network as the WAN should assign an IPv6 IP address for the WAN interface.

The screenshot shows the 'Edit Ethernet' configuration screen for the WAN interface. It is divided into three sections: 'General Settings', 'General IPv6 Setting', and 'Interface Properties'.

- General Settings:** The 'Enable Interface' checkbox is checked.
- General IPv6 Setting:** The 'Enable IPv6' checkbox is checked.
- Interface Properties:**
 - Interface Type: external
 - Interface Name: ge2
 - Port: P2
 - Zone: WAN
 - MAC Address: B8:EC:A3:A9:C0:04
 - Description: (Optional)



Setting Up the WAN IPv6 Interface

1. In the Configuration > Network > Interface > Ethernet screen, double-click the lan interface in the IPv6 Configuration section.
2. The Edit Ethernet screen appears. Click Show Advanced Settings to display more settings on this screen.

Select Enable Interface and Enable IPv6.

In the Address from DHCPv6 Prefix Delegation table, click Add and select the DHCPv6 request object from the drop-down list, type ::1111:0:0:1/128 in the Suffix Address field. (The combined address 2001:b050:2d:1111::1/128 will display as LAN1's IPv6 address after you click OK and come back to this screen again).

DHCPv6 Setting is **N/A**

Note: You can configure the IPv6 Address/Prefix Length field instead if the delegated prefix is never changed.

3. In the Advertised Prefix from DHCPv6 Prefix Delegation table, click Add and select the DHCPv6 request object from the drop-down list, type ::1111/64 in the Suffix Address field. (The combined prefix 2001:b050:2d:1111::/64 will display for the LAN1's network prefix after you click OK and come back to this screen again)., please note that this is the USG LAN interface IP.

General Settings

☒ Enable Interface

General IPv6 Setting

☒ Enable IPv6

Interface Properties

Interface Type:

Interface Name:

Port:

Zone:

MAC Address:

Description: (Optional)

IPv6 Address Assignment

☐ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address:

IPv6 Address/Prefix Length: (Optional)

☒ Advance

Gateway: (Optional)

Metric: (0-15)

Address from DHCPv6 Prefix Delegation

#	Delegated Prefix	Suffix Address	Address
1	Prefix_WAN	::1111:0:0:1/64	2002:b050:2d:1111

of 0 50 items . No data to display

1. Navigate to IPv6 Router Advertisement Setting, enable Router Advertisement, it would advertise the prefix to the Lan host, also enable Advertised Hosts Get Other Configuration From DHCPv6, Lan hosts will get the DNS address from USG.
2. Configure Advertised Prefix from DHCPv6 Prefix Delegation, the Lan hosts will get the Prefix from USG, Suffix address can set 0~F

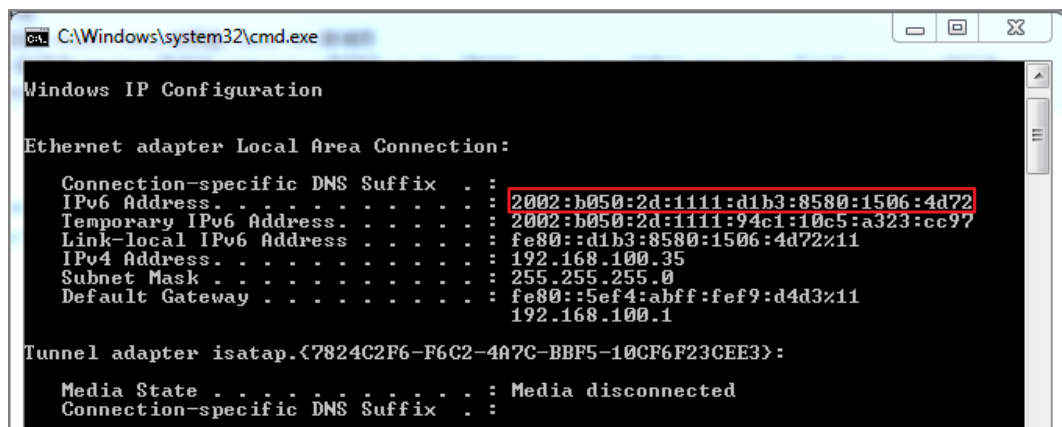
Test

1. Connect a computer to the ZyWALL's LAN interface.
2. Enable IPv6 support on you computer.

In Windows XP, you need to use the IPv6 install command in a Command Prompt.

In Windows 7, IPv6 is supported by default. You can enable IPv6 in the Control Panel > Network and Sharing Center > Local Area Connection screen.

3. Your computer should get an IPv6 IP address (starting with 2001:b050:2d:1111: for this example) from the ZyWALL.



4. Open a web browser and type <http://www.kame.net>. If your IPv6 settings are correct, you can see a dancing turtle in the website.

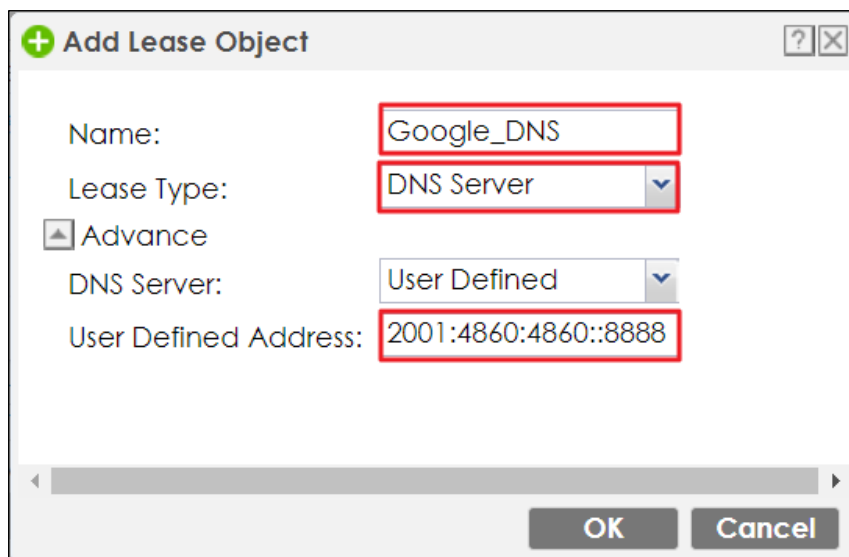
What Can Go Wrong?

1. If you forgot to enable Auto-Configuration on the WAN1 IPv6 interface, you will not have any default route to forward the LAN's IPv6 packets.
2. To use prefix delegation, you must set the WAN interface to a DHCPv6 client, enable router advertisements on the LAN interface as well as configure the Advertised Prefix from DHCPv6 Prefix Delegation table.
3. If the Value field in the WAN1's DHCPv6 Request Options table displays n/a, contact your ISP for further support.
4. In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

Assign the DNS address to the client

1. If you want to assign the DNS server address instead of ISP's , then please create the DNS server object.

Select DHCPv6 Lease and DNS server as lease type. For example set the Google DNS IPv6 address 2001:4860:4860::8888



+ Add Lease Object

Name: Google_DNS

Lease Type: DNS Server

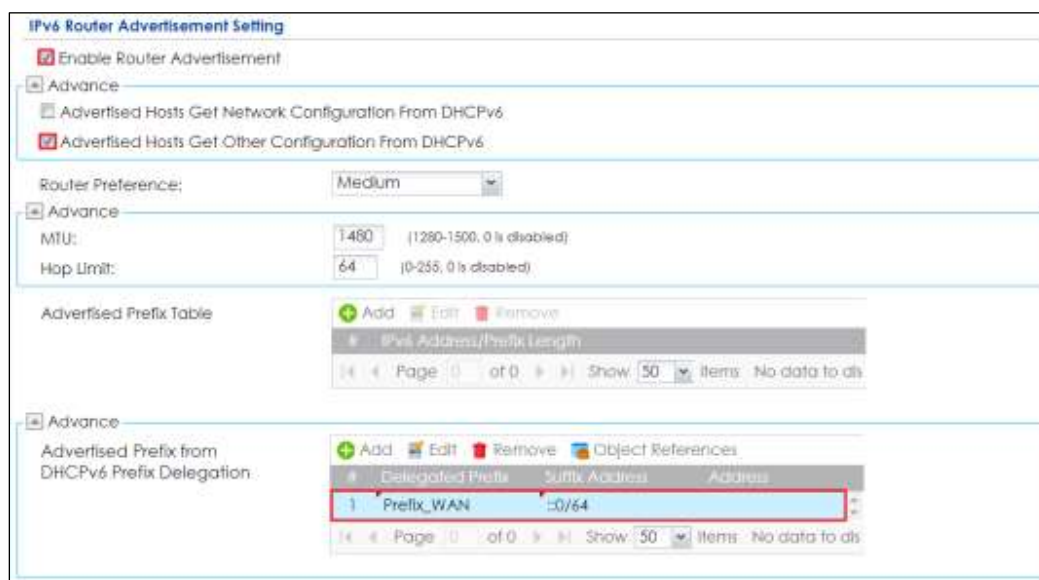
☐ Advance

DNS Server: User Defined

User Defined Address: 2001:4860:4860::8888

OK Cancel

2. Select the drop-down list DHCPv6 as server type, add the DNS server object in DHCPv6 lease options and enable **Router Advertisement**.



IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

☐ Advance

☐ Advertised Hosts Get Network Configuration From DHCPv6

☒ Advertised Hosts Get Other Configuration From DHCPv6

Router Preference: Medium

☐ Advance

MTU: 1480 (1280-1500, 0 is disabled)

Hop Limit: 64 (0-255, 0 is disabled)

Advertised Prefix Table

+ Add Edit Remove

IPv6 Address/Prefix Length

Page 0 of 0 Show 50 Items No data to display

☐ Advance

Advertised Prefix from DHCPv6 Prefix Delegation

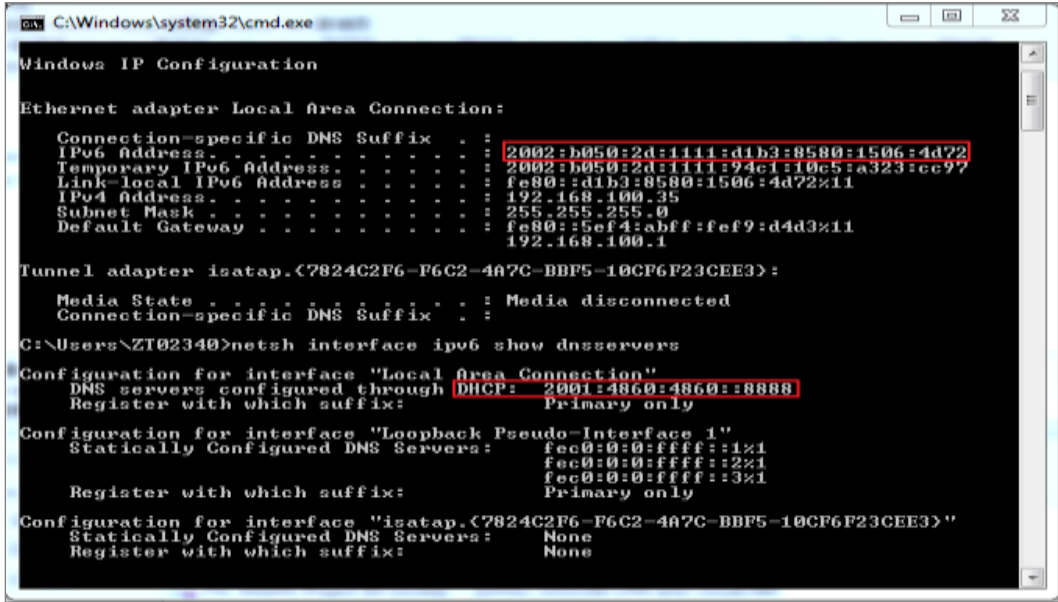
+ Add Edit Remove Object References

Delegated Prefix	Suffix Address	Address
1 Prefix_WAN	50/64	

Page 0 of 0 Show 50 Items No data to display

Test

You can use command "netsh interface ipv6 show dnsservers" to check the DNS server IP.



```

C:\Windows\system32\cmd.exe
Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2002:b050:2d:1111:d1b3:8580:1506:4d72
    Temporary IPv6 Address. . . . . : 2002:b050:2d:1111:94c1:10c5:a323:cc97
    Link-local IPv6 Address . . . . . : fe80::d1b3:8580:1506:4d72%11
    IPv4 Address. . . . . : 192.168.100.35
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::5ef4:abff:fef9:d4d3%11
                                192.168.100.1

Tunnel adapter isatap.{7824C2F6-F6C2-4A7C-BBF5-10CF6F23CEE3}:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : 

C:\Users\ZT02340>netsh interface ipv6 show dnsservers

Configuration for interface "Local Area Connection"
    DNS servers configured through DHCP: 2001:4860:4860::8888
    Register with which suffix: Primary only

Configuration for interface "Loopback Pseudo-Interface 1"
    Statically Configured DNS Servers: fec0:0:0:ffff::1%1
                                         fec0:0:0:ffff::2%1
                                         fec0:0:0:ffff::3%1
    Register with which suffix: Primary only

Configuration for interface "isatap.{7824C2F6-F6C2-4A7C-BBF5-10CF6F23CEE3}"
    Statically Configured DNS Servers: None
    Register with which suffix: None
  
```

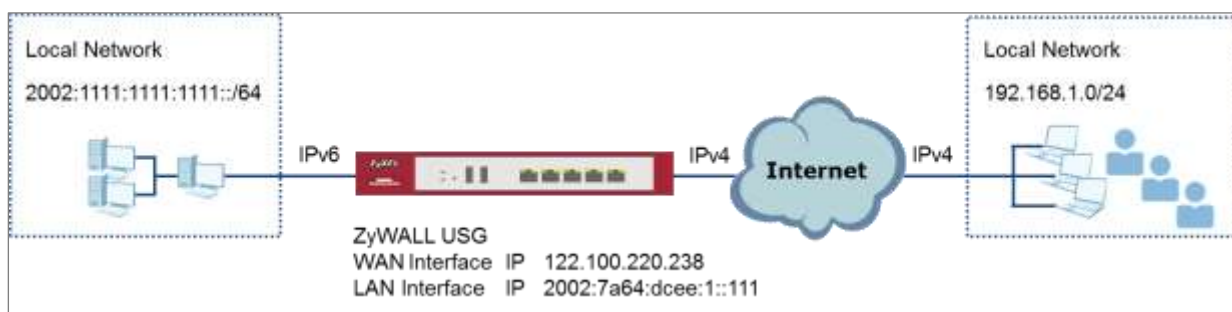
How to Set Up an IPv6 6to4 Tunnel


This example shows how to configure your ZyWALL/USG to create IPv6 6to4 Tunnel.

In this example, the ZyWALL/USG acts as a 6to4 router which connects the IPv4.

After configuration, the ZyWALL/USG can assign an IPv6 to clients behind it and pass IPv6 traffic through IPv4 environment to access remote IPv6 network.

ZyWALL/USG with IPv6 6to4 Tunnel 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 LAN IPv6 Interface on the ZyWALL/USG

The second and third sets of 16-bit IP address from the left must be converted from wan1 IP (122.100.220.238 in this example). It becomes 7a64:dcee in hexadecimal. (You can go to <https://isc.sans.edu/tools/ipv6.html#form> to convert an IPv4 address into it's default 6-to-4 equivalent). You are free to use the fourth set of 16-bit IP address from the left in order to allocate different network addresses (prefixes) to IPv6 interfaces. In this example, the LAN1 network address is assigned to use 2002:7a64:dcee:1::/64 and the LAN1 IP address is set to 2002:7a64:dcee:1::111/128.

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Ethernet > lan1**, Select **Enable Interface** and **Enable IPv6**. Type 2002:7a64:dcee:1::111/128 in the **IPv6 Address/Prefix Length** field for the LAN1's IP address.

Enable **Router Advertisement**. Then click **Add** in the **Advertised Prefix Table** to add **2002:7a64:dcee:1::/64**. The LAN1 hosts will get the network prefix through the router advertisement messages sent by the LAN1 IPv6 interface periodically. Click **OK**.

CONFIGURATION > Network > Interface > Ethernet > lan1 > General Settings

General Settings	
<input checked="" type="checkbox"/>	Enable Interface
General IPv6 Setting	
<input checked="" type="checkbox"/>	Enable IPv6 
Interface Properties	
Interface Type:	internal 
Interface Name:	Lan1
Port:	P5, P6
Zone:	LAN1 
MAC Address:	B8:EC:A3:A9:C0:0F
Description:	<input type="text"/> (Optional)
IPv6 Address Assignment	
<input type="checkbox"/>	Enable Stateless Address Auto-configuration (SLAAC)
Link-Local Address:	fe80::baec:a3ff:fea9:c00f/64
IPv6 Address/Prefix Length:	2002:7a64:dcee::111, (Optional)

CONFIGURATION > Network > Interface > Ethernet > lan1 > IPv6 Router

Advertisement Setting

IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

☐ Advance

Router Preference: Medium

☐ Advance

Advertised Prefix Table

Add

Edit

Remove

#	IPv6 Address/Prefix Length
	2002:7a64:dcee:1::/64

Page

1

of 1

Show

50

items

Displaying 1 -

Set Up the 6to4 Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go 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**.

CONFIGURATION > Network > Interface > Tunnel

General Settings

☒ Enable

Interface Properties

Interface Name: tunnel0
Zone: TUNNEL
Tunnel Mode: 6to4

IPv6 Address Assignment

Metric: 0 (0-15)

6to4 Tunnel Parameter

6to4 Prefix: 2002::/16
Relay Router: 192.88.99.1 (Optional)

NOTE: traffic destined to the non-6to4 prefix domain tunnels to the relay router

☐ Advance

Gateway Settings

My Address

☒ Interface
ge2 DHCP client -- 10.214.30.82/255.255.255.0

☐ IP Address
0.0.0.0

Remote Gateway Address: Automatic

Test the Result

Connect a computer to the ZyWALL/USG's LAN1.

Enable IPv6 support on your computer. In Windows XP, you need to use the IPv6 install command in a Command Prompt. In Windows 7, IPv6 is supported by default. You can enable IPv6 in the **Control Panel > Network and Sharing Center > Local Area Connection** screen.

Your computer should get an IPv6 IP address (starting with 2002:7a64:dcee:1: in this example) from the ZyWALL/USG.

Window 7 > cmd > ipconfig

```
C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    IPv6 Address. . . . . : 2002:7a64:dcee:1:dc9:e2ff:7d32:19c9
    Temporary IPv6 Address. . . . . : 2002:7a64:dcee:1:393c:37d8:5564:8f34
    Link-local IPv6 Address . . . . . : fe80::dc9:e2ff:7d32:19c9%12
    IPv4 Address. . . . . : 192.168.1.34
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::b2b2:dcff:fe70:c1d8%12
                                192.168.1.1
```

Type **ping -6 ipv6.google.com** in a Command Prompt to test. You should get a response.

Window 7 > cmd > ping -6 ipv6.google.com

```
C:\Windows\system32>ping -6 ipv6.google.com

Pinging ipv6.l.google.com [2404:6800:4001:801::1000] with 32 bytes of data:
Reply from 2404:6800:4001:801::1000: time=69ms
Reply from 2404:6800:4001:801::1000: time=69ms
Reply from 2404:6800:4001:801::1000: time=69ms
Reply from 2404:6800:4001:801::1000: time=69ms
Ping statistics for 2404:6800:4001:801::1000
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 69ms, Maximum = 69ms, Average = 69ms
```

What Could Go Wrong?

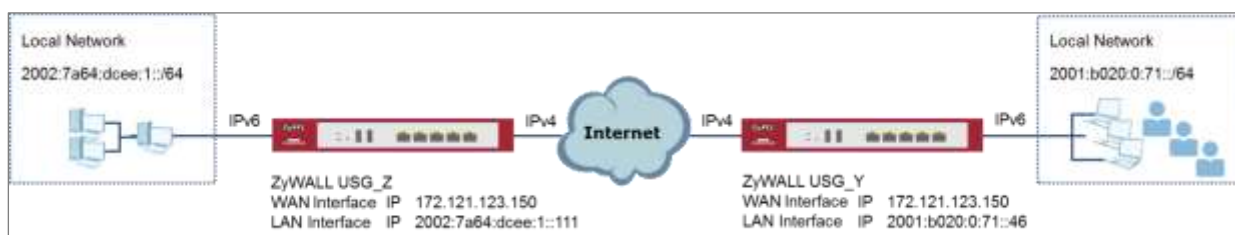
If your IPv6 connection is not working, please make sure you disable Auto-Configuration on the LAN1 IPv6 interface. Enabling it will cause two default routes, however, the ZyWALL/USG only needs a default route generated by your relay router setting. Also, make sure you enable the WAN1 IPv4 interface. In 6to4, the ZyWALL/USG uses the WAN1 IPv4 interface to forward your 6to4 packets over the IPv4 network.


In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.

How to Set Up an IPv6-in-IPv4 Tunnel

This example shows how to configure your ZyWALL/USG to create IPv6-in-IPv4 Tunnel. In this example, the ZyWALL/USG acts as IPv6-in-IPv4 routers which connect the IPv4 Internet and an individual IPv6 network. This configuration example only shows the settings on ZyWALL/USG_Z. You can use similar settings to configure ZyWALL/USG_Y.

ZyWALL/USG with IPv6-in-IPv4 Tunnel 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 LAN IPv6 Interface on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Ethernet >**

lan1. Select **Enable Interface** and **Enable IPv6**. Type **2002:7a64:dcee:1::111/128** in the **IPv6 Address/Prefix Length** field for the LAN1's IP address.

Enable **Router Advertisement**. Then click **Add** in the **Advertised Prefix Table** to add **2002:7a64:dcee:1::/64**. The LAN1 hosts will get the network prefix through the router advertisement messages sent by the LAN1 IPv6 interface periodically. Click **OK**.

CONFIGURATION > Network > Interface > Ethernet > lan1 > General Settings

General Settings

☒ Enable Interface

General IPv6 Setting

☒ Enable IPv6 ⓘ

Interface Properties

Interface Type: internal ⓘ

Interface Name: lan1

Port: P5, P6

Zone: LAN1 ⓘ

MAC Address: B8:EC:A3:A9:C0:0F

Description: (Optional)

IPv6 Address Assignment

☐ Enable Stateless Address Auto-configuration (SLAAC)

Link-Local Address: fe80::baec:a3ff:fea9:c00f/64

IPv6 Address/Prefix Length: 2002:7a64:dcee:1::111, (Optional)

CONFIGURATION > Network > Interface > Ethernet > lan1 > IPv6 Router Advertisement Setting

IPv6 Router Advertisement Setting

☒ Enable Router Advertisement

☐ Advance

Router Preference: Medium

☐ Advance

Advertised Prefix Table

#	IPv6 Address/Prefix Length	
1	2002:7a64:dcee:1::/64	

Page 1 of 1 Show 50 items Displaying 1 - 1

Set Up the 6to4 Tunnel on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Tunnel > Add** and select **Enable**. Enter **tunnel0** as the **Interface Name** and select **IPv6-in-IPv4** as

the **Tunnel Mode**. Select **wan1** as the gateway interface. Enter your **Remote Gateway Address** (172.121.123.150 in this example). Click **OK**.

CONFIGURATION > Network > Interface > Tunnel

General Settings

☒ Enable

Interface Properties

Interface Name: tunnel0

Zone: TUNNEL

Tunnel Mode: IPv6-in-IPv4

IPv6 Address Assignment

IPv6 Address/Prefix Length: (Optional)

Metric: 0 (0-15)

Gateway Settings

My Address

☒ Interface

ge2

DHCP client -- 10.214.30.82/255.255.255.0

☐ IP Address

0.0.0.0

Remote Gateway Address: 172.121.123.150

Set Up the Policy Route on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Routing > IPv6**

Configuration > Add, click **Create New Object** to create an IPv6 address object with the address prefix of **2002:7a64:dcee:1::/64**. Select **Enable**. Select the address object you just created in the **Source Address** field. Select **any** in the **Destination Address** field. Select **Interface** as the **next-hop** type and then **tunnel0** as the interface. Click **OK**.

CONFIGURATION > Network > Routing > Policy Route > IPv6 Configuration

+ Add IPv6 Address Rule

Name: Lan1_subnet

Object Type: SUBNET

IPv6 Address Prefix: 2002:7a64:dcee:1::/64

Add Policy Route

Show Advanced Settings Create new Object ▼

Configuration

☒ Enable

Description: (Optional)

Criteria

User: any

Incoming: any (Excluding ZyV

Source Address: Lan1_subnet

Destination Address: any

DSCP Code: any

Schedule: none

Service: any

▼ Advance

Next-Hop

Type: Interface

Interface: tunnel0

Test the Result

Connect a computer to the ZyWALL/USG's LAN1.

Enable IPv6 support on your computer. In Windows XP, you need to use the IPv6 install command in a Command Prompt. In Windows 7, IPv6 is supported by default. You can enable IPv6 in the **Control Panel > Network and Sharing Center > Local Area Connection** screen.

Your computer should get an IPv6 IP address (starting with 2002:7a64:dcee:1: for this example) from the ZyWALL/USG.

Window 7 > cmd > ipconfig

```
C:\Windows\system32>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . : localdomain
    IPv6 Address. . . . . : 2002:7a64:dcee:1:dc9:e2ff:7d32:19c9
    Temporary IPv6 Address. . . . . : 2002:7a64:dcee:1:393c:37d8:5564:8f34
    Link-local IPv6 Address . . . . . : fe80::dc9:e2ff:7d32:19c9%12
    IPv4 Address. . . . . : 192.168.1.34
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::b2b2:dcff:fe70:c1d8%12
                                192.168.1.1
```

Use the ping -6 [IPv6 IP address] command in a Command Prompt to test whether you can ping a computer behind ZyWALL/USG_Y. You should get a response.

Window 7 > cmd > ping -6 2001:b020:0:71::46

```
C:\Windows\system32>ping -6 2001:b020:0:71::46

Pinging 2001:b020:0:71::46 with 32 bytes of data:

Reply from 2001:b020:0:71::46: time=21ms
Reply from 2001:b020:0:71::46: time=21ms
Reply from 2001:b020:0:71::46: time=21ms
Reply from 2001:b020:0:71::46: time=21ms

Ping statistics for 2001:b020:0:71::46
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 21ms, Maximum = 21ms, Average = 21ms
```

What Could Go Wrong?

If your IPv6 connection is not working, please make sure you enable the WAN1 IPv4 interface. In IPv6-in-IPv4, the ZyWALL/USG uses the WAN1 IPv4 interface to forward your 6to4 packets to the IPv4 network.

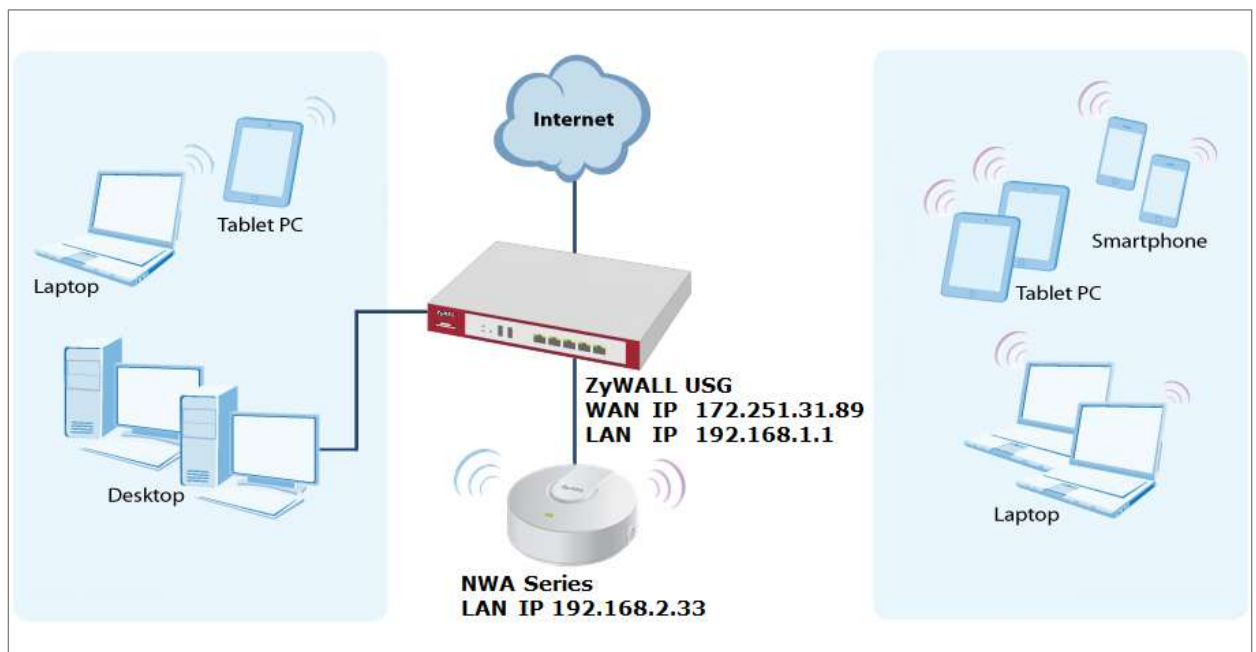
In Windows, some IPv6 related tunnels may be enabled by default such as Teredo and 6to4 tunnels. It may cause your computer to handle IPv6 packets in an unexpected way. It is recommended to disable those tunnels on your computer.


Chapter 6- Wireless

How to Set Up a WiFi Network with ZyXEL APs

This is an example of using ZyWALL/USG to manage the Access Points (APs) and allow wireless access to the network.

ZyWALL/USG as AP Controller Example

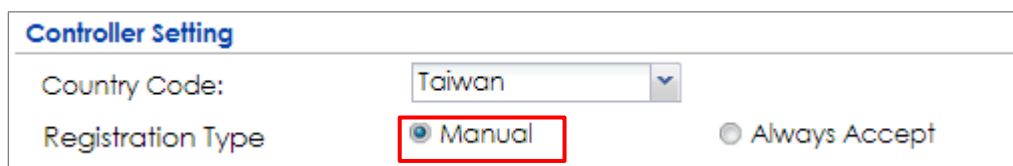


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the AP Management on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Wireless > Controller > Configuration**, set **Registration Type** to **Manual**. This is recommended as the registration mechanism cannot automatically differentiate between friendly and rogue APs.

CONFIGURATION > Wireless > Controller > Configuration



Controller Setting

Country Code: Taiwan

Registration Type: ☒ Manual ☐ Always Accept

Connect the ZyXEL AP unit to the lan interface.

Go to **MONITOR > Wireless > AP Information > AP List** and the ZyXEL AP is listed. A green question mark displays in the Status column since the AP is not yet managed by the ZyWALL/USG. Select the listed AP and click **Add to Mgmt AP List** on the upper bar.

Monitor > Wireless > AP Information > AP List



Status	Description	IP Address	Model	Group	Station	Face	Reg.	MAC-Add	Mgmt	Last	LED st.	Power
?	AP-38:86:F...	192.168.2.33	NWA...		0		Un-M...	38:86:F3:9...	0/-			N/A

Page 1 of 1 | Show 30 items | Deploying 1 - 1 of 1



Note: The APs may take few minutes to appear in the AP List.

Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List** to configure a name to identify the **SSID**.

CONFIGURATION > Object > AP Profile > SSID > SSID List

Profile Name:	default		
SSID:	<div style="border: 2px solid red; padding: 2px;">ZyXEL_AP1</div>		
Security Profile:	default	▼	
MAC Filtering Profile:	disable	▼	
QoS:	WMM	▼	
Rate Limiting (Per Station Traffic Rate) ⓘ			
Downlink:	0	mbps	▼ (0~160, 0 is unlimited)
Uplink:	0	mbps	▼ (0~160, 0 is unlimited)
Band Select:	disable	▼	
Forwarding Mode:	Local bridge	▼	
VLAN ID:	1	(1~4094)	
<input type="checkbox"/> Hidden SSID			
<input type="checkbox"/> Enable Intra-BSS Traffic blocking			
<input type="checkbox"/> Schedule SSID ⓘ			

Go to **CONFIGURATION > Object > AP Profile > SSID > Security List** to select the **Security Mode** to be the **wpa2**. Then, set a **Pre-Shared Key** (8-63 characters) and select the **Cipher Type** to be the **auto** to have ZyWALL/USG automatically chooses the best available cipher based on the cipher currently in use by the wireless network. Click **OK**.

CONFIGURATION > Object > AP Profile > SSID > Security List

General Settings	
Profile Name:	default
Security Mode:	<div style="border: 2px solid red; padding: 2px;">wpa2</div> ▼

Authentication Settings

☒ 802.1X

Auth. Method:
ReAuthentication Timer: (30~30000 seconds, 0 is unlimited)

☒ PSK

Pre-Shared Key:
Cipher Type:
Idle timeout: (30~30000 seconds)
Group Key Update Timer: (30~30000 seconds)

☐ Management Frame Protection
☒ Optional
☐ Required

Test the Result

Go to the ZyWALL/USG **Monitor > Wireless > AP Information > AP List**, you can check the list of APs which are currently connected to it and the details information such as **Registration** type, **Model** and **Recent On-line Time /Last Off-line Time**.

MONITOR > Wireless > AP Information > AP List

AP List

Config AP Add to Mgmt AP List More Information Refresh DCS Now Log Suppression On Suppression Off

#	Status	Description	IP Address	Model	Registration	MAC Address	LED status	Power Mode
1		AP-58:8B:F3:91:58:C7	192.168.2.33	NWA5123-AC	Un-Mgmt AP	58:8B:F3:91:58:C7	N/A	

Page 1 of 1 Show 30 items Displaying 1 - 1 of 1

Go to the ZyWALL/USG **Monitor > Wireless > Station Info > Station List**, you can check the list of wireless stations associated with a managed AP and the details information such as **SSID Name**, **Signal Strength** and the transmit (**Tx**)/receive (**Rx**) data rate.

MONITOR > Wireless > Station Info > Station List

Station List

#	MAC Address	Associated	SSID Name	Security	Signal Strength	Channel	Band	IP Address	Tx R...	Rx R...	Tx	Rx
1	04:4B:ED:85:16...	AP-588BF...	ZyXEL	NONE	-55dBm	6	2.4G	192.168.2...	15M	32M	102177	49447

Page 1 of 1 Show 50 items Displaying 1 - 1 of 1

Using a mobile device to connect to SSID: **ZyXEL_AP1** and type the password (zyxel123) for authentication. Go to the ZyWALL/USG **Monitor > Log**, you will see [info] log message as shown below. The ZyWALL/USG will assign an IP address to the mobile device and the mobile device can access the Internet.

MONITOR > Log

349	Info	DHCP	DHCP server assigned 192.168.1.33 to TWNBZT02643-02(30:65:EC:49:85:EA)... DHCP ACK
350	Info	DHCP	Requested 192.168.1.33 from TWNBZT02643-02(30:65:EC:49:85:EA) (count... DHCP Request

What Could Go Wrong?

If you can't see AP information in the AP List, please check the number of APs connected to the ZyWALL/USG has exceeded the maximum Managed AP number it can support. You can check the maximum support number of each ZyWALL/USG in the Datasheet from ZyXEL Download Library -

http://www.zyxel.com/support/download_landing.shtml

If your mobile device can't find the AP SSID you configured, please go to **CONFIGURATION > Object > AP Profile > SSID > SSID List** and check if the **Hidden SSID** option is enabled.

If your mobile device can't access to the Internet via AP connects to the ZyWALL/USG, please check if the LAN outgoing security policy allow access to the Internet.

If your mobile device is not connected to the AP automatically even you've joined the Wifi network before and you see [Wlan Station Info] log message as shown below, please check if this AP is removed from your mobile device's saved Wifi network list.

MONITOR > Log

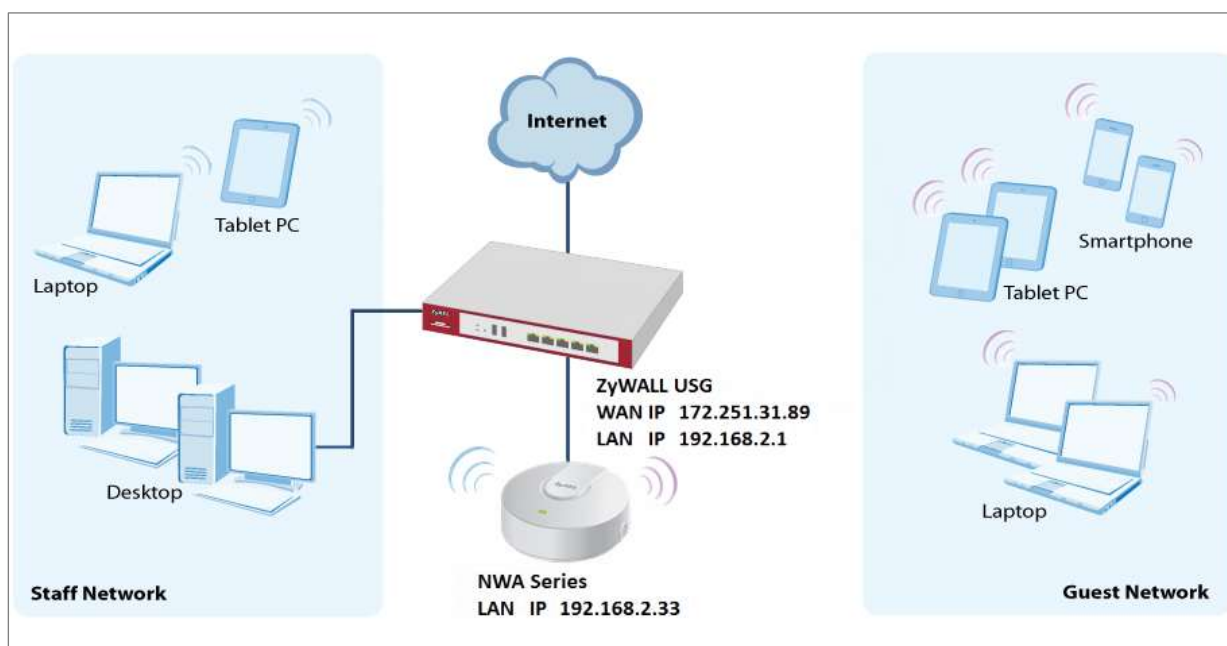
#	Priority	Category	Message *	Host
17	Info	Wlan Station Info	STA Disassociation(8-DISASSOC_STA_HAS_LEFT) by STA Logout, MA...	
100	Info	Wlan Station Info	STA Disassociation(3-DEAUTH_LEAVING) by STA Logout, MAC:D4:9...	
10	Info	Wlan Station Info	STA Disassociation(3-DEAUTH_LEAVING) by STA Logout, MAC:D4:9...	
105	Info	Wlan Station Info	STA Disassociation(3-DEAUTH_LEAVING) by STA Logout, MAC:D4:9...	


How to Set Up Guest WiFi Network Accounts

This is an example of using ZyWALL/USG to configure guest WiFi accounts to allow limited wireless access to the Internet using only HTTP, HTTPS, and DNS protocols.

For the wireless network setup, please see the tutorial about How to Set Up WiFi with ZyXEL AP.

ZyWALL/USG with Guest WiFi Accounts Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the WiFi Guest Account, Address Range and Service Rule on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > User/Group > User > Add A User** to configure the **User Name** the guest Wi-Fi user and set **User Type** to **guest**. Set a secured **Password** (4-31 characters) and enter it again for confirmation.

Set the **Authentication Timeout Settings** to be **Use Manual Settings** to enter the number of minutes this user has to renew the current session before the user is logged out.

CONFIGURATION > Object > User/Group > User > Add A User

User Configuration

User Name : WiFi_guest

User Type: user

Password:

Retype:

Description: Local User

Authentication Timeout Settings: ☐ Use Default Settings ☒ Use Manual Settings

Lease Time: 240 (0-1440 minutes, 0 is unlimited)

Reauthentication Time: 240 (0-1440 minutes, 0 is unlimited)

In the ZyWALL/USG, go to **CONFIGURATION > Object > Address > Add Address Rule** to create the guest Wi-Fi user access subnet. In this example, AP is connected to ZyWALL/USG LAN interface 192.168.2.0/24. Configure the **Name** for you to identify the Wi-Fi guest subnet. Set the **Network** to be 192.168.2.0 and set the **Netmask** to be 255.255.255.0. Click **OK**.

CONFIGURATION > Object > Address > Add Address Rule

+ Add Address Rule

Name: WiFi_guest

Address Type: SUBNET

Network: 192.168.2.0

Netmask: 255.255.255.0

OK Cancel

In the ZyWALL/USG, go to **CONFIGURATION > Object > Service > Service Group >**

Add Service Group Rule to create the allowed protocols for guest Wi-Fi user.

Configure the **Name** for you to identify the **Service Group**. Set **HTTP**, **HTTPS** and

DNS to be in the same member group and click **OK**.

CONFIGURATION > Object > Service > Service Group > Add Service Group Rule

Configuration

Name:

Description:

Configuration

Available	Member
<div>=== Object ===</div> <div> <div>AH</div> <div>AIM</div> <div>AUTH</div> <div>Any_TCP</div> <div>Any_UDP</div> <div>BGP</div> <div>BONJOUR</div> <div>BOOTP CLIENT</div> </div>	<div>=== Object ===</div> <div> <div>HTTP</div> <div>HTTPS</div> </div> <div>=== Group ===</div> <div> <div>DNS</div> </div>


Set Up the Web Authentication on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Web Authentication > Web**

Authentication Policy Summary > Auth. Policy Add to configure policy to redirect HTTP traffic to the user login screen. Configure the **Description (Optional)** for you to identify the auth. Policy. Then, scroll down the **Source Address** list to choose the newly created **wifi-guest**. Set the **Authentication** to be **required**. Select **Force User Authentication**.

CONFIGURATION > Web Authentication > Web Authentication Policy Summary >

Auth. Policy Add

General Settings		
<input checked="" type="checkbox"/> Enable Policy		
Description:	WiFi_guest	(Optional)
User Authentication Policy		
Incoming Interface:	any	
Source Address:	WiFi_guest	SUBNET, 192.168.2.0/24
Destination Address:	any	
Schedule:	none	
Authentication:	required	
<input type="checkbox"/> Single Sign-on		
<input checked="" type="checkbox"/> Force User Authentication		
Authentication Type:	default-web-porta	

In the ZyWALL/USG, go to **CONFIGURATION > Web Authentication > General Settings** and select **Enable Web Authentication**.

CONFIGURATION > Web Authentication > General Settings

Global Setting
<input checked="" type="checkbox"/> Enable Web Authentication

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy > Add corresponding**. Configure a **Name** for you to identify the **Security Policy** profile. Set **From: LAN** and **To: any (Excluding ZyWALL)**. Set **Service** to be the Service Group Rule (wifi_guest_access in this example). Set **User** to be the Wi-Fi guest user (wifi_guest_access in this example). Select Log type to **log alert** in order to view the result later.

CONFIGURATION > Security Policy > Policy > Add corresponding

<input checked="" type="checkbox"/> Enable	
Name:	Wifi_guest
Description:	(Optional)
From:	any
To:	any (Excluding ZyV
Source:	any
Destination:	any
Service:	Wifi_guest_access
User:	Wifi_guest
Schedule:	none
Action:	allow
Log matched traffic:	log alert


Test the Result


Using a mobile device to connect to the AP which is connected to the ZyWALL/USG. When you try to access the Internet, it will redirect to the user login screen.

ZYXEL

VPN300

Enter User Name/Password and click to login.

 _____

 _____

[login](#) [SSL VPN](#)

Note:


1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.


Type the Wi-Fi guest **User Name** and **Password**, click **Login**.

ZYXEL

VPN300

Enter User Name/Password and click to login.

 WiFi_guest _____

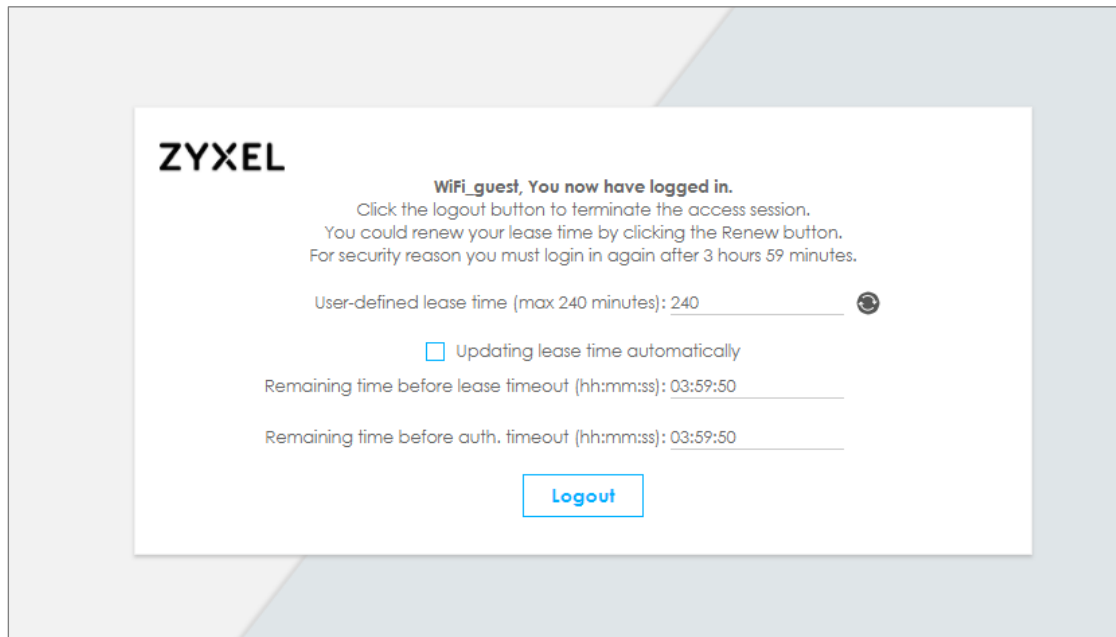
 _____

[login](#) [SSL VPN](#)

Note:

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.

The access session page will appear.



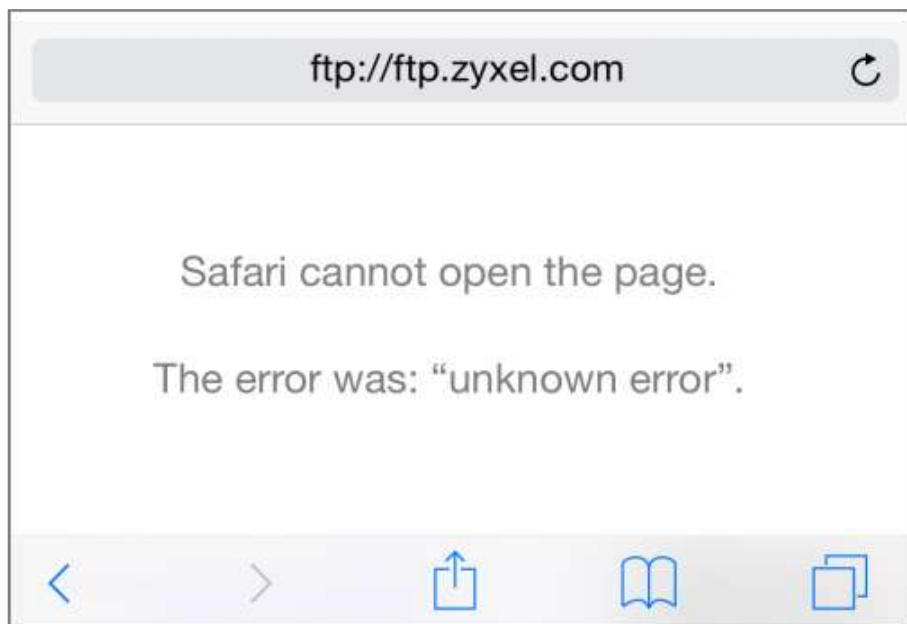
Go to the ZyWALL/USG **Monitor > System Status > Login Users**, you will see current login user list shown as below.

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:33:2B:4F:A2	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.

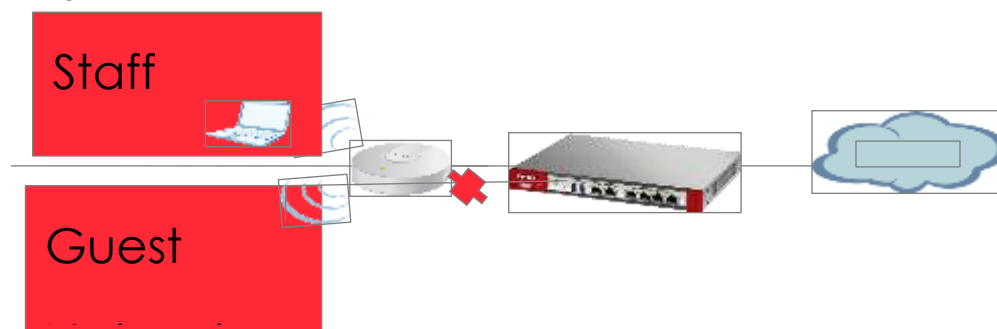
Monitor > Log

Priority	Category	Message	Source	Destination	Rule
notice	Security Policy Control	priority:1, from LAN to ANY, UDP, service WiF_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 WiF_guest, REJECT...	192.168.2.33:59691	36.139.161.14:17:443	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

+
Add Zone

Group Members

Name:

Go to **CONFIGURATION > Network > Interface > VLAN**. Create VLAN16 for Staff_WiFi and VLAN17 for Guest_WiF

CONFIGURATION > Network > Interface > VLAN > VLAN16

General Settings	
<input checked="" type="checkbox"/> Enable Interface	
Interface Properties	
Interface Type:	internal ?
Interface Name:	vlan16
Zone:	LAN1 ?
Base Port:	ge1
VLAN ID:	16 (1-4094)
<input checked="" type="checkbox"/> Advance	
Description:	Staff_wifi (Optional)

IP Address Assignment	
IP Address:	172.16.0.1
Subnet Mask:	255.255.255.0
<input type="checkbox"/> Enable IGMP Support	
<input type="radio"/> IGMP Upstream <input checked="" type="radio"/> IGMP Downstream	

DHCP Setting	
DHCP:	DHCP Server
IP Pool Start Address:	172.16.0.10
First DNS Server (Optional):	Custom Defined
Second DNS Server (Optional):	None
Third DNS Server (Optional):	None

Pool Size:	100
	8.8.8.8

CONFIGURATION > Network > Interface > VLAN > VLAN17

General Settings

☒ Enable Interface

Interface Properties

Interface Type: ⓘ
 Interface Name:
 Zone: ⓘ
 Base Port:
 VLAN ID: (1-4094)
☒ Advance
 Description: (Optional)

IP Address Assignment

IP Address:
 Subnet Mask:
☐ Enable IGMP Support
☐ IGMP Upstream
☒ IGMP Downstream

DHCP Setting

DHCP:
 IP Pool Start Address: Pool Size:
 First DNS Server (Optional):
 Second DNS Server (Optional):
 Third DNS Server (Optional):

There will be two VLAN interfaces.

CONFIGURATION > Network > Interface > VLAN

#	Status	Name	Port/VID	IP Address	Mask
1		vlan16	ge5/16	static --172.16.0.1	255.255.255.0
2		vlan17	ge6/17	static --172.17.0.1	255.255.255.0

Page 1 of 1 | Show 30 items | Deploying 1 - 2 of 2

Set Up the User

Go to **Configuration > Object > User/Group > User**, and create users for the staff and the guest

Configuration > Object > User/Group > User > staff

+ Add A User

User Configuration

User Name :

User Type:

Password:

Retype:

Description:

Authentication Timeout Settings

☒ Use Default Settings
☐ Use Manual Settings

Lease Time: minutes

Reauthentication Time: minutes

Configuration > Object > User/Group > User > guest

+ Add A User

User Configuration

User Name :

User Type:

Password:

Retype:

Description:

Authentication Timeout Settings

☒ Use Default Settings
☐ Use Manual Settings

Lease Time: minutes

Reauthentication Time: minutes

There will be two users.

User				
Group: Setting: MAC Address:				
Configuration				
Add Edit Remove Object Referenced				
#	User Name	User Type	Description	Reference
1	admin	admin	Administration account	0
2	ldap-users	ext-user	External LDAP Users	0
3	radius-users	ext-user	External RADIUS Users	0
4	ext-users	ext-user	External Ext Users	0
5	WIFI_guest	guest	Local User	1
6	staff	User	Local user	0
7	guest	User	Local User	0

Set Up the AP Profile

Go to **CONFIGURATION > Object > AP Profile > SSID > Security List**, and create two security profiles.

CONFIGURATION > Object > AP Profile > SSID > Security List > Guest_WPA2

General Settings	
Profile Name:	Guest_WPA2
Security Mode:	wpa2
Fast Roaming Settings	
<input type="checkbox"/> 802.11r	
Radius Settings	
Radius Server Type:	Internal
<input type="checkbox"/> Proxy by controller directly	
MAC Authentication Setting	
<input type="checkbox"/> MAC Authentication	
Auth. Method:	default
Delimiter (Account):	colon (:)
Case (Account):	upper
Delimiter (Calling Station ID):	colon (:)
Case (Calling Station ID):	upper
Authentication Settings	
<input type="radio"/> 802.1X	
Auth. Method:	default
ReAuthentication Timer:	0 (30~30000 seconds, 0 is unlimited)
<input checked="" type="radio"/> PSK	
Pre-Shared Key:	12345678
Cipher Type:	auto
Idle timeout:	300 (30~30000 seconds)
Group Key Update Timer:	30000 (30~30000 seconds)
<input type="checkbox"/> Management Frame Protection <input checked="" type="radio"/> Optional <input type="radio"/> Required	

CONFIGURATION > Object > AP Profile > SSID > Security List > Staff_WPA2

General Settings

Profile Name:

Security Mode:

Fast Roaming Settings

☐ 802.11r

Radius Settings

Radius Server Type:

☐ Proxy by controller directly

MAC Authentication Setting

☐ MAC Authentication

Auth. Method:

Delimiter (Account):

Case (Account):

Delimiter (Calling Station ID):

Case (Calling Station ID):

Authentication Settings

☐ 802.1X

Auth. Method:

ReAuthentication Timer: (30~30000 seconds, 0 is unlimited)

☒ PSK

Pre-Shared Key:

Cipher Type:

Idle timeout: (30~30000 seconds)

Group Key Update Timer: (30~30000 seconds)

☐ Management Frame Protection ☒ Optional ☐ Required

Go to **CONFIGURATION > Object > AP Profile > SSID > SSID List**, and create two SSID profiles.

CONFIGURATION > Object > AP Profile > SSID > SSID List > Staff_Wifi

Add SSID Profile
?
✕

Create new Object ▼

Profile Name:

SSID:

Security Profile:
 ▼

MAC Filtering Profile:
 ▼

QoS:
 ▼

Rate Limiting (Per Station Traffic Rate) ⓘ

Downlink:
 ▼
(0~160, 0 is unlimited)

Uplink:
 ▼
(0~160, 0 is unlimited)

Band Select:
 ▼

Forwarding Mode:
 ▼

VLAN ID:
(1~4094)

☐ Hidden SSID

☐ Enable Intra-BSS Traffic blocking

☐ Schedule SSID ⓘ

OK

Cancel

CONFIGURATION > Object > AP Profile > SSID > SSID List > Guest_Wifi

Add SSID Profile

Create new Object ▼

Profile Name:

SSID:

Security Profile:
 ▼

MAC Filtering Profile:
 ▼

QoS:
 ▼

Rate Limiting (Per Station Traffic Rate) ⓘ

Downlink:
 ▼
(0~160, 0 is unlimited)

Uplink:
 ▼
(0~160, 0 is unlimited)

Band Select:
 ▼

Forwarding Mode:
 ▼

VLAN ID:
(1~4094)

☐ Hidden SSID

☐ Enable Intra-BSS Traffic blocking

☐ Schedule SSID ⓘ

OK

Cancel

Go to **CONFIGURATION > Wireless > AP Management > AP Group**, and add an AP Group as **WiFi**.

CONFIGURATION > Wireless > AP Management > AP Group

+ Add AP Group Profile

General Settings

Group Name: WiFi

Description: (Optional)

Radio 1 Setting

OP Mode
☒ AP Mode
☐ MON Mode
☐ Root AP
☐ Repeater AP

Radio 1 AP Profile: default

Output Power: 30 dBm (0~30)

Edit

#	SSID Profile
1	Staff_wifi
2	Guest_wifi
3	disable
4	disable
5	disable
6	disable
7	disable
8	disable

Go to **CONFIGURATION > Wireless > AP Management > Mgmt. AP List**, and Edit the AP List. Change the Group setting as **WiFi**

CONFIGURATION > Wireless > AP Management > Mgmt. AP List,

Edit AP List

Create new Object *

Configuration

MAC: 40-4A:03:69:A5:04

Model: NWA5160N

Description: AP-404A0369A504

Group Setting: WiFi

Radio1 Setting

☐ Override Group Radio Setting

OP Mode
☒ AP Mode
☐ MON Mode

Radio 1 Profile: default

Set Up the Security policy rule

Go to **CONFIGURATION > Security Policy > Policy Control > Policy**. Add one rule to restrict Guest access USG, and another one to allow to access internet.

CONFIGURATION > Security Policy > Policy Control > Policy > Guest_ZyWALL

+

Add corresponding

?

×

Create new Object ▼

☒ Enable

Name:

Guest_Zywall

Description:

(Optional)

From:

Guest_Zone

▼

To:

ZyWALL

▼

Source:

any

▼

Destination:

any

▼

Service:

any

▼

User:

any

▼

Schedule:

none

▼

Action:

deny

▼

Log denied traffic:

no

▼

OK

Cancel

CONFIGURATION > Security Policy > Policy Control > Policy > Guest_Internet

+

Add corresponding

?

✕

Create new Object ▼

☒ Enable

Name:

Guest_Internet

Description:

(Optional)

From:

Guest_Zone

▼

To:

any (Excluding ZyV

▼

Source:

any

▼

Destination:

any

▼

Service:

any

▼

User:

any

▼

Schedule:

none

▼

Action:

deny

▼

Log denied traffic:

no

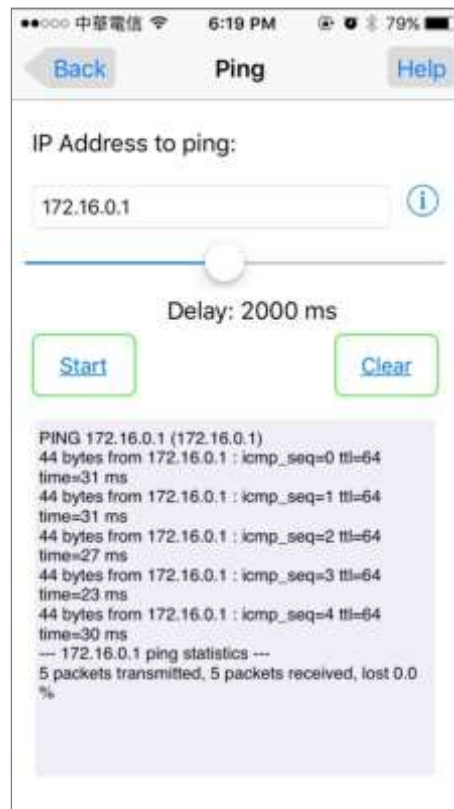
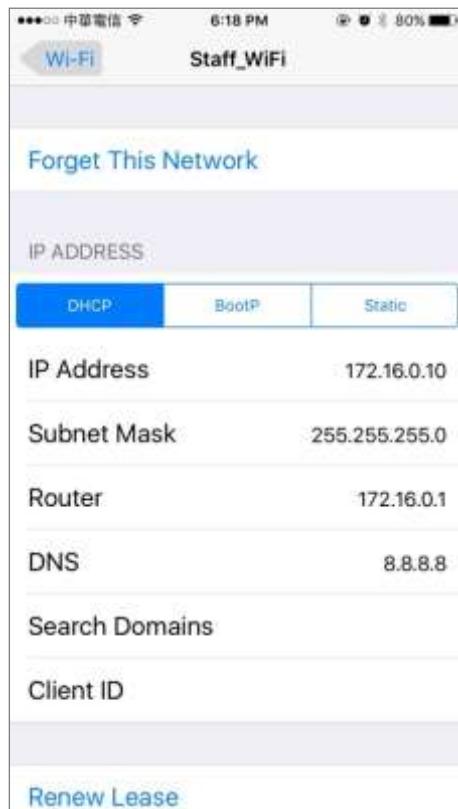
▼

OK

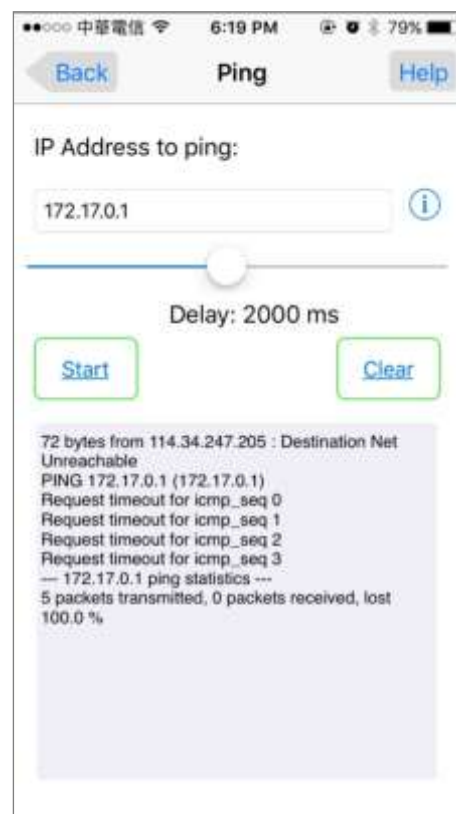
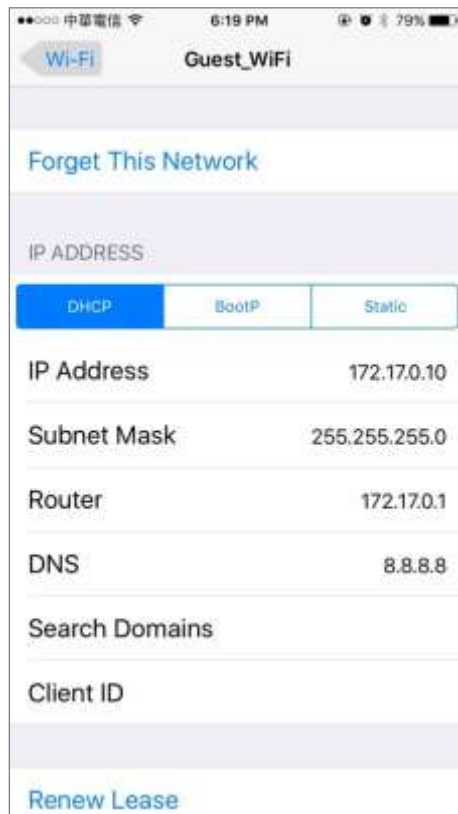
Cancel

Test result

Connect to the SSID Staff_WiFi, and ping the USG interface.

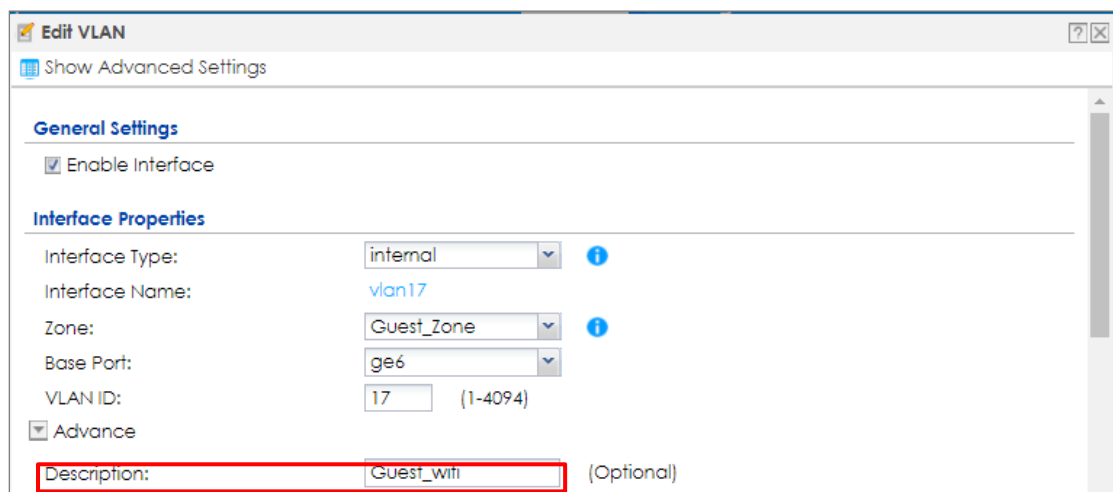


Connect to the SSID Guest_WiFi, and ping the USG interface



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

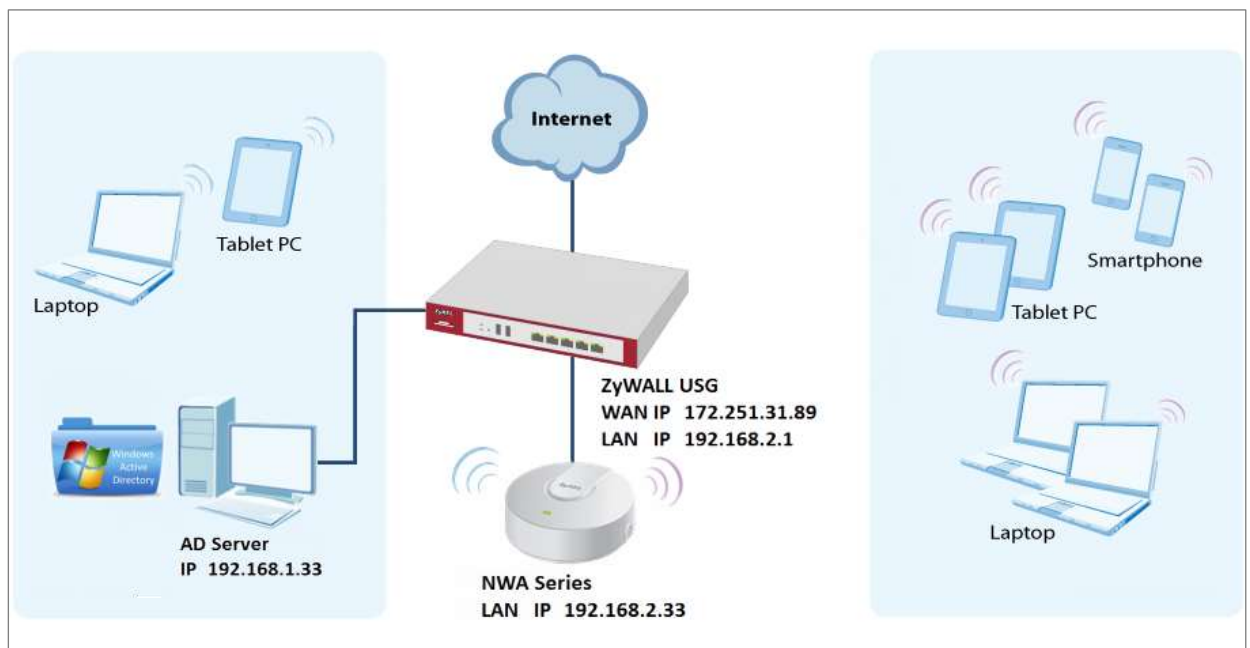
☐ Allow Asymmetrical Route


<

How to Set Up WiFi Networks with Microsoft Active Directory Authentication

This is an example of using ZyWALL/USG to configure guest WiFi accounts with Microsoft Active Directory (AD) to authenticate your WiFi guests. For the wireless network setup, please go to How to Set Up WiFi with ZyXEL AP.

ZyWALL/USG with AD Guest WiFi Accounts Example

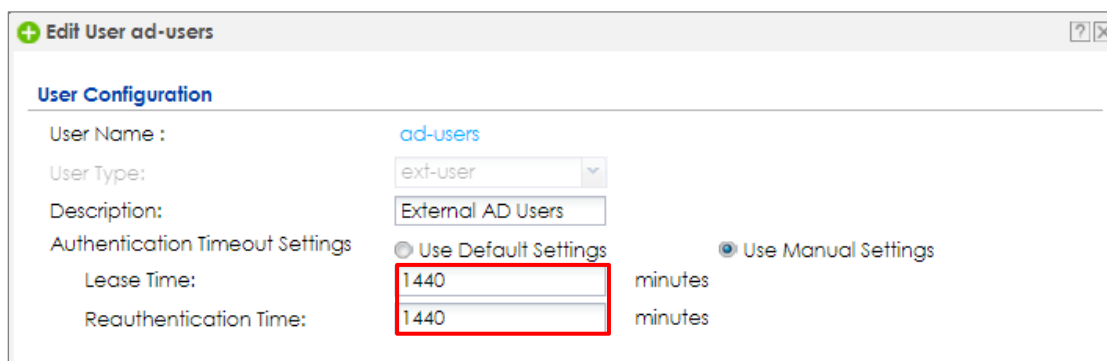


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Wi-Fi Guest Account and Authentication Method on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > User/Group > User > ad-users**, set the **Authentication Timeout Settings** to **Use Manual Settings** and enter the number of minutes this user has to renew the current session before the user is logged out.

CONFIGURATION > Object > User/Group > User > ad-users



Edit User ad-users

User Configuration

User Name : ad-users

User Type: ext-user

Description: External AD Users

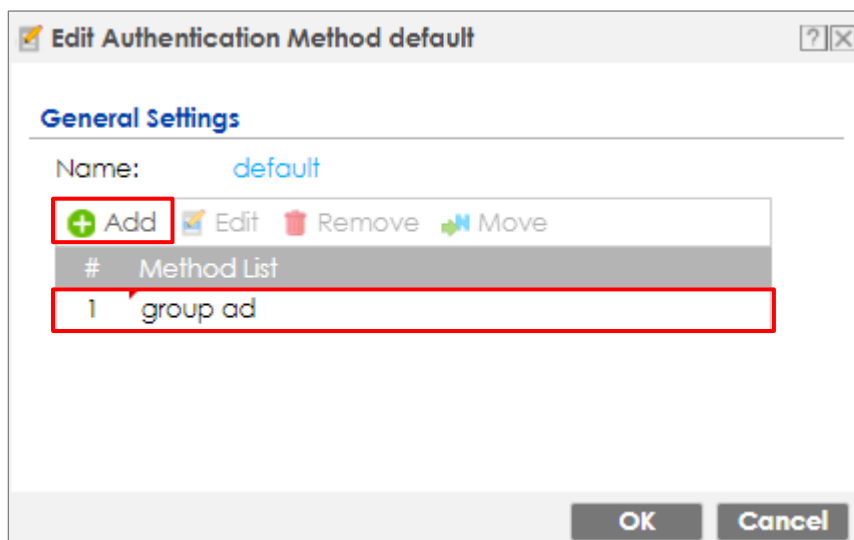
Authentication Timeout Settings: ☐ Use Default Settings ☒ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes

In the ZyWALL/USG, go to **CONFIGURATION > Object > Authentication Method > default > Edit Authentication Method default**, click **Add** to insert group ad in the table. Click **OK**.

CONFIGURATION > Object > User/Group > User > ad-users



Edit Authentication Method default

General Settings

Name: default

#	Method List
1	group ad

OK Cancel

In the ZyWALL/USG, go to **CONFIGURATION > Web Authentication > General Settings** and select **Enable Web Authentication**.


CONFIGURATION > Web Authentication > General Settings

Global Setting
<input checked="" type="checkbox"/> Enable Web Authentication

Set Up the Active Directory Server Account on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > AAA Server > Active Directory > Add Active Directory** to configure the AD sever. Enter the **Server Address** (192.168.1.33 in this example) and **Based DN** (dc=cso,dc=net in this example). Specify the **Bind DN** for logging into the AD server (cn=Administrator,cn=users,dc=cso,dc=net in this example). If required, enter the **Password** for the ZyWALL/USG to bind (or log in) to the AD server.

CONFIGURATION > Object > AAA Server > Active Directory > Add Active Directory

General Settings		
Name:	ad	
Description:	<input type="text"/>	(Optional)
Server Settings		
Server Address:	<input type="text" value="192.168.1.33"/>	(IP or FQDN)
Backup Server Address:	<input type="text"/>	(IP or FQDN) (Optional)
Port:	<input type="text" value="389"/>	(1-65535)
Base DN:	<input type="text" value="dc=cso,dc=net"/>	
<input type="checkbox"/> Use SSL		
Search time limit:	<input type="text" value="5"/>	(1-300 seconds)
<input type="checkbox"/> Case-sensitive User Names		
Server Authentication		
Bind DN:	<input type="text" value="cn=administrator,cn=users,dc=cso,dc=net"/>	
Password:	<input type="password" value="...."/>	
Retype to Confirm:	<input type="password" value="...."/>	

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

Configuration Validation

Please enter an existing user account in this server to validate the above settings.

Username:

Test Status:

OK

Returned User Attributes:

dn: CN=wifi_guest,CN=Users,DC=cso,DC=net
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: wifi_guest
givenName: wifi_guest
distinguishedName: CN=wifi_guest,CN=Users,DC=cso,DC=net

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy > Add corresponding**. Configure a **Name** for you to identify the **Security Policy** profile. Set **From: LAN** and **To: any (Excluding ZyWALL)**. Set **Service** to be the service rule for Wi-Fi guest (wifi_guest_access in this example). Set **User** to be the Wi-Fi guest user (ad-users in this example). Select Log type to be **log alert** in order to view the result later.

CONFIGURATION > Security Policy > Policy > Add corresponding

<input checked="" type="checkbox"/> Enable	
Name:	WiFi_Guest
Description:	(Optional)
From:	LAN
To:	any (Excluding ZyV
Source:	any
Destination:	any
Service:	Wifi_guest_access
User:	ad-users
Schedule:	none
Action:	allow
Log matched traffic:	log alert

Test the Result

Using a mobile device to connect to the AP which is connected to the ZyWALL/USG. When you try to access the Internet, it will redirect to the user login screen.

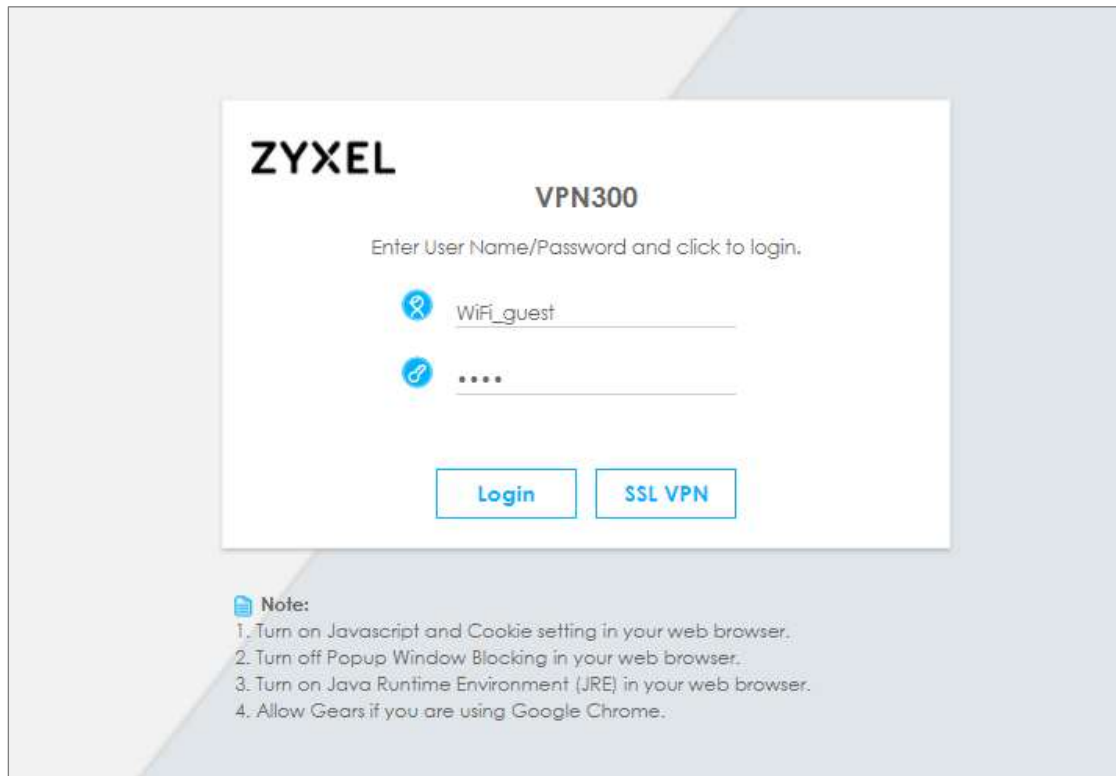
ZYXEL
VPN300

Enter User Name/Password and click to login.

Login
SSL VPN

Note:
1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Geart if you are using Google Chrome.

Type the Wi-Fi guest **User Name** and **Password**, click **Login**.



ZYXEL

VPN300

Enter User Name/Password and click to login.

WiFi_guest

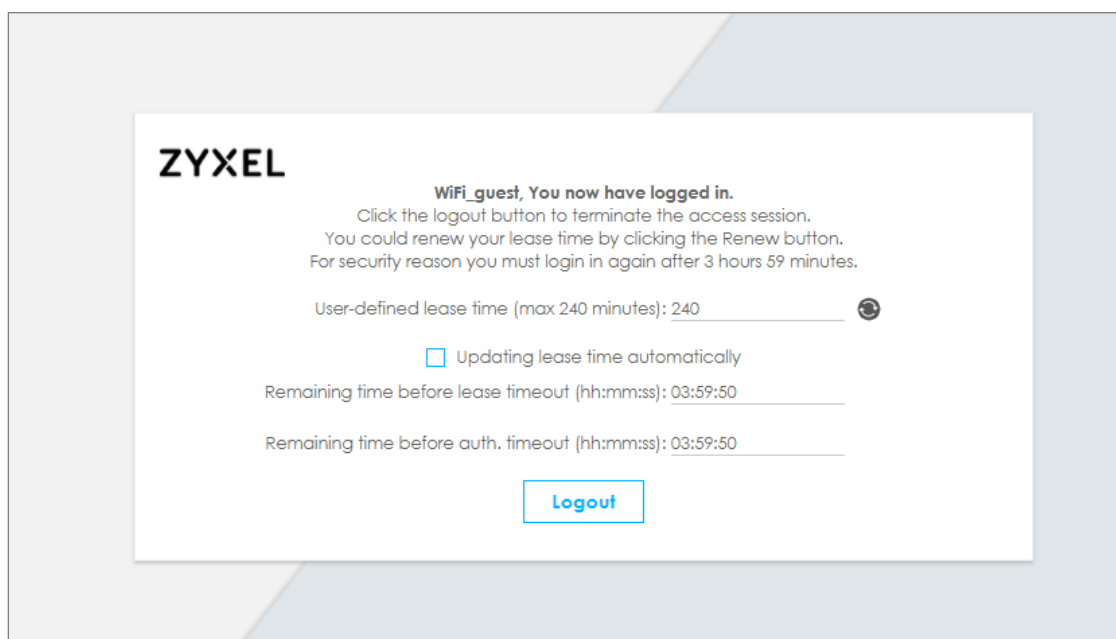
....

Login SSL VPN

Note:

1. Turn on Javascript and Cookie setting in your web browser.
2. Turn off Popup Window Blocking in your web browser.
3. Turn on Java Runtime Environment (JRE) in your web browser.
4. Allow Gears if you are using Google Chrome.

The access session page will appear.



ZYXEL

WiFi_guest, You now have logged in.

Click the logout button to terminate the access session.
You could renew your lease time by clicking the Renew button.
For security reason you must login in again after 3 hours 59 minutes.

User-defined lease time (max 240 minutes): 240

☐ Updating lease time automatically

Remaining time before lease timeout (hh:mm:ss): 03:59:50

Remaining time before auth. timeout (hh:mm:ss): 03:59:50

Logout

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

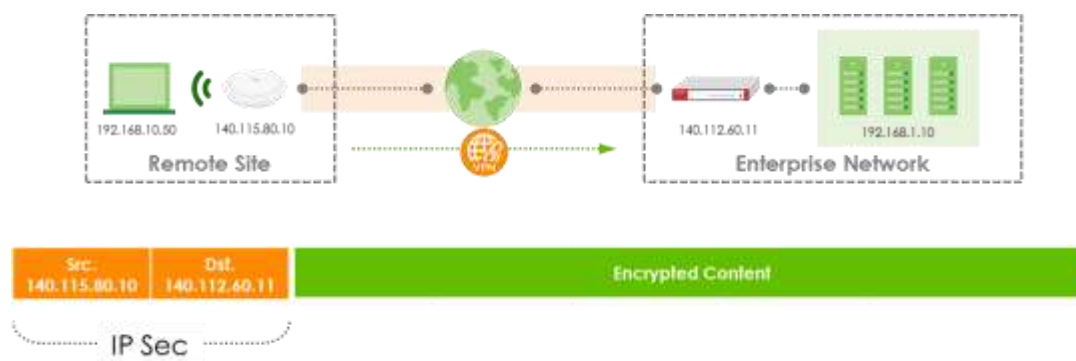
Priority	Category	Message	Note
alert	User	Failed login attempt to Device from http/https (incorrect passw...	Account: wifi_guest



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.**

#	Status	Description	CPU Util.	Remote AP	AP Role Capability	IP Address
1	✓	AP-WAC6303D-S	24 %			192.168.1.36
2	✓	AP-WAC500H	10 %	Disabled	Remote AP	192.168.1.33
3	✓	AP-WAX510D	15 %	Enabled	Remote AP	192.168.1.37

Note: To protect the Security Gateway from overloading due to handle too much tunnel traffic, only 25% of managed APs can be configured as Remote AP.

Set up Secure Wi-Fi on AP controller

There are two stages when deploying Secure Wi-Fi on AP managed by AP Controller and status is online.

Stage one, finish the configuration inside enterprise network.

- Configure AP role as Remote AP and SSID setting
- Update the Controller IP as the USG's WAN IP

Stage two, remote users power up the AP, and then the IP Sec tunnel will be established automatically.

- Power up remote APs at remote side

Configure AP role as Remote AP and SSID setting

Secure Wi-Fi is per AP setting at **Configuration > Wireless > AP Management > Mgmt.**

AP List > Specific AP.

Enable the AP Role to Remote AP. The maximum of Secure Tunnel SSIDs is up to four. Then define which interface the traffic will be tunneled to, and where to transmit the traffic at.

Configuration

AP Role: ☒ Remote AP ⓘ

MAC: 10:11:22:33:44:55

Model: WAX3100

Secure Tunnel SSID ⓘ

#	SSID Profile	Interface	Band Mode
1	Tunnel_HQ_1	lan1	5G +
2	Tunnel_HQ_2	lan2	2.4G +
3	Tunnel_HQ_3	vlan10	Dual Band +
4	disable	vlan10	Dual Band +

Local Bridge SSID

#	SSID Profile	VID	Band Mode
1	Local_SSID	100	Dual Band +
2	disable	1	Dual Band +

NOTE: Secure Tunnel can be only applied to SSID, Ethernet traffic from clients connecting to AP's LAN port won't be tunneled back to Controller.

Update the Controller IP as the USG's WAN IP

Besides setting the SSID also need to override the Controller's IP address on AP to let it connect back to HQ's Gateway after booting up in remote site. If Gateway supports dual WAN, add another WAN IP in the "secondary controller" column. FQDN is also an available input option for dynamic WAN IP, but requires corresponding DNS settings.

Assign Gateway's WAN IP as AP's Controller IP at: **Configuration > Wireless > AP Management > AP Policy**

General Settings Wireless AP Controller

☒ Force Override AC IP Config on AP

Override Type: ☐ Auto ☒ Manual

Primary Controller: 140.112.60.11 WAN IP Address of AP Controller

Secondary Controller:

☐ Fall back to Primary Controller when possible

Fall Back Check Interval: 30

Firewall Policy Rule that is for CAPWAP connection and Remote AP VPN IP Address Pool that is a new subnet (192.168.60.1/24) for Remote AP VPN Client use will be auto-added when Remote AP is enabled.

IPv4 Configuration

☒ Allow Asymmetrical Route

Policy #	Status	Name	From	To	IPv4 Source	IPv4 Destination	Service	Action	Schedule	Log
1	On	CAPWAP_to_Device	➔WAN	ZyWALL	any	any	➔CAPWAP-CONTROL	allow	none	no
2	On	LAN1_Outgoing	➔LAN1	any (Excluding ZyWALL)	any	any	any	allow	none	no
3	On	LAN2_Outgoing	➔LAN2	any (Excluding ZyWALL)	any	any	any	allow	none	no
4	On	DMZ_to_WAN	➔DMZ	➔WAN	any	any	any	allow	none	no
5	On	IPSec_VPN_Outgoing	➔IPSec_VPN	any (Excluding ZyWALL)	any	any	any	allow	none	no

Remote AP VPN

General Settings

Configuration Walkthrough

Troubleshooting

VPN Connection:

_remote_ap_vpn_profile

IP Address Pool:

192.168.60.1

To

192.168.60.254

On remote AP, Storm Control is automatically activated in order to avoid huge broadcast traffic flooding from wireless part to Gateway and to other Remote APs. Both Wireless and Ethernet Storm Control will be auto-enabled on Remote AP.

Configuration

AP Role

☒ Remote AP

Storm Control Setting

☒ Broadcast Storm Control

☒ Multicast Storm Control

Enable Remote AP role will enable Storm control automatically.

Both Ethernet & Wireless Storm Control are included

Power up remote APs at remote side

Remote users power up the AP, and then the IP Sec tunnel will be established automatically.

Test the Result

After Remote AP boots up in the remote site, AP will automatically establish the IPSec VPN connection with HQ. AP and tunnel information displays on the Web GUI at:

Monitor > VPN Monitor > Remote AP VPN > Remote AP VPN

Current IPSec Security Associations

Name:

Policy:

Search

Disconnect

#	RAP Description	Assigned IP	Policy	My Address	Secure Gateway
1	AP-WAX650S	192.168.60.4	192.168.60.1<=>192.168.60.4	140.112.60.11	140.115.80.10

Page 1 of 1

Show 50 Items

Remote AP's IP Address



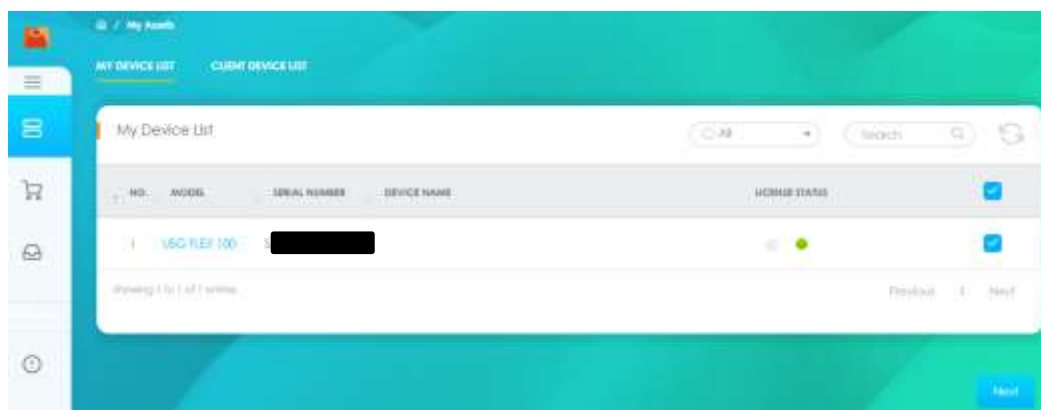
What can go wrong

1. Configure all the corresponding setting on interface before you connect the link.
2. Maximum Remote AP number is limited by Device's capability of "Max. Concurrent IPsec Tunnel" and 25% of Maximum managed AP number.
3. Secure Wi-Fi requires specific license on AP.

#	Service	Status	Service 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 Wi-Fi	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

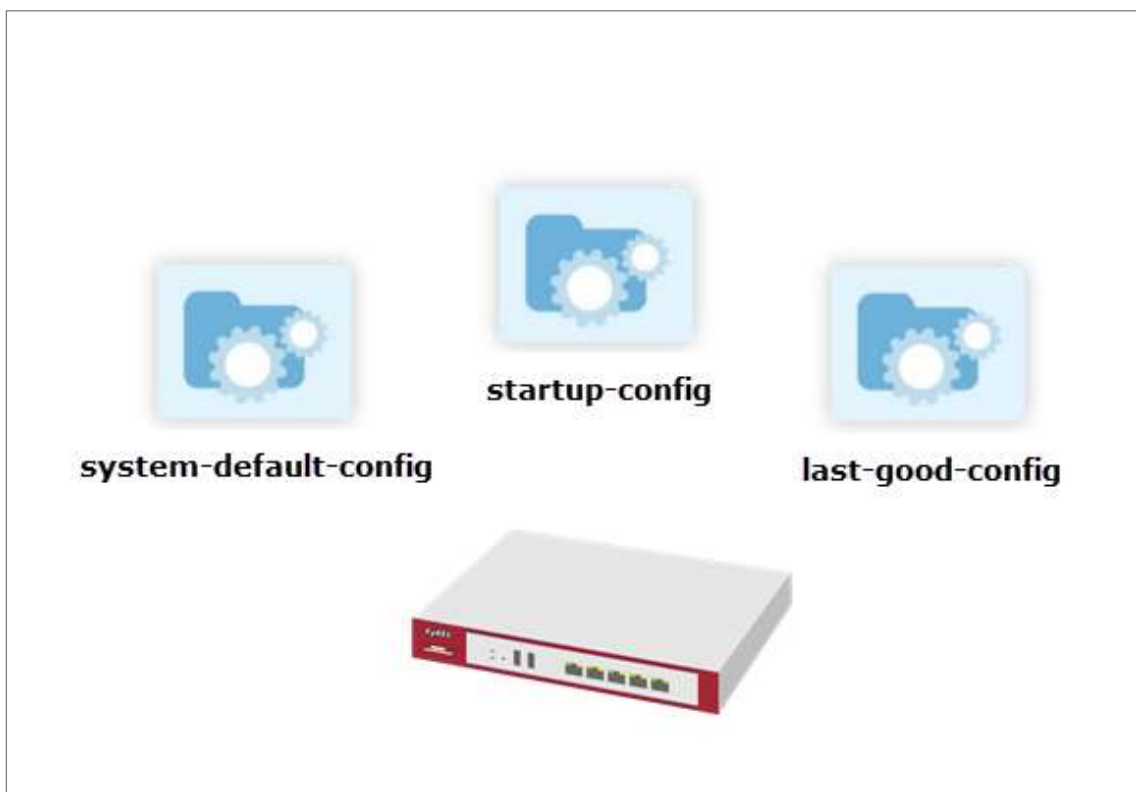
This is an example of how to rename, download, copy, apply and upload configuration files. Once your ZyWALL/USG is configured and functioning properly, it is highly recommended that you back up your configuration file before making further configuration changes. The backup configuration file will be 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

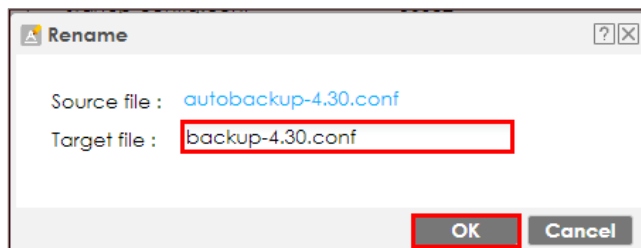
In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File**, select the configuration file and click **Rename**. A pop-up screen will appear allowing you to edit the **Target file** name. Click **OK** to save the **Rename** configuration.

MAINTENANCE > File Manager > Configuration File

Configuration Files			
<div>  Rename  Remove  Download  Copy  Apply </div>			
#	File Name	Size	Last Modified
1	startup-config.conf	36582	2017-07-07 07:23:22
2	430A8FC0a4-2017-07-03-06-54-...	13040	2017-07-03 06:54:24
3	lastgood.conf	36582	2017-07-07 07:23:22
4	system-default.conf	32927	2017-06-09 12:39:03
5	autobackup-4.35.conf	13040	2017-07-03 06:56:16
6	startup-config-bad.conf	17406	2017-07-05 08:44:06

Page 1 of 1 Show 30 Items Displaying 1 - 6 of 6

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

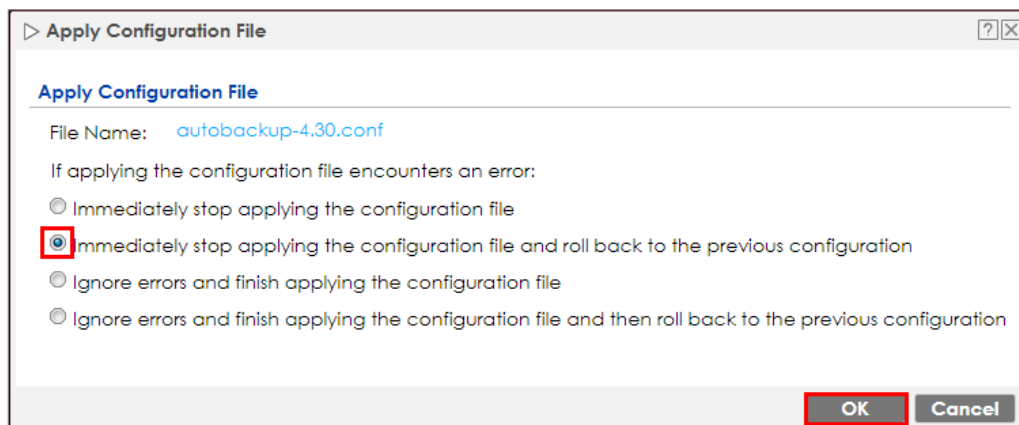
In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Configuration File**, select a specific configuration file to have ZyWALL/USG use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL/USG settings to the factory defaults. Or select the **lastgood.conf** 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

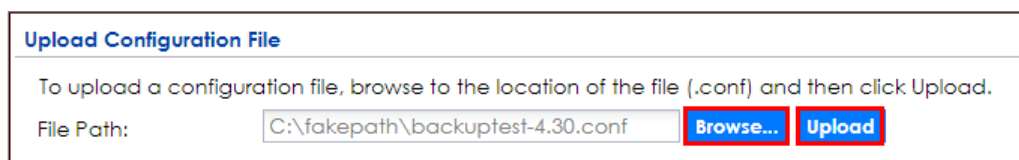


Note: Do not shut down the ZyWALL/USG while the configuration file is being applied.

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



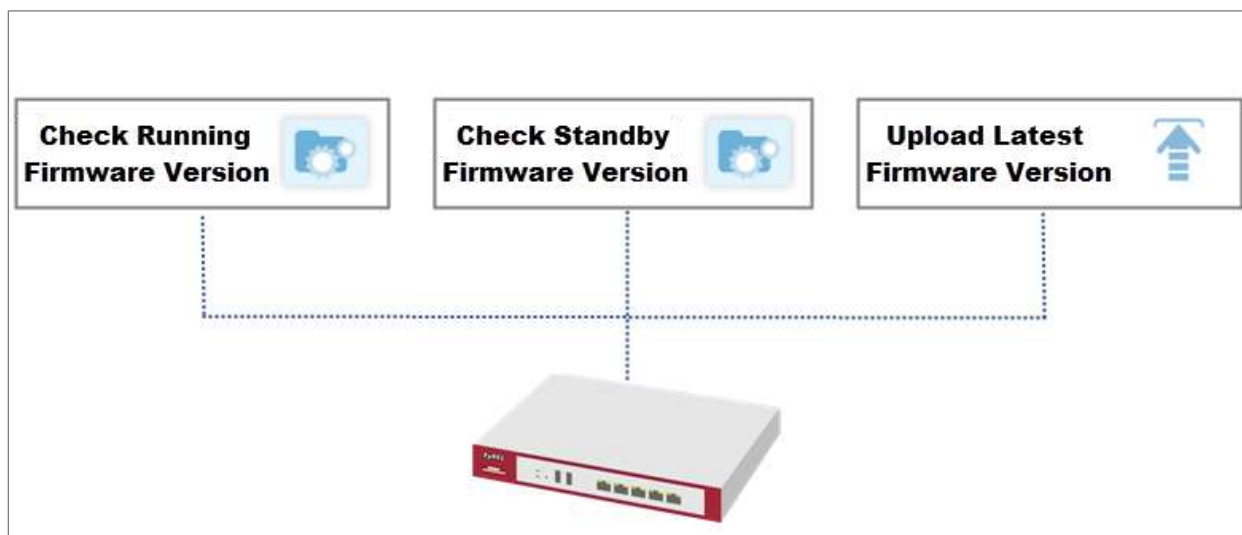
Monitor > Log


Priority	Category	Message	Note
alert	File Manager	Going to rollback previous running-config.	Apply Config
alert	File Manager	ERROR: #configure terminal interface _ether dntz 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.

Search by Model Number

Don't know the product model number?

USG110

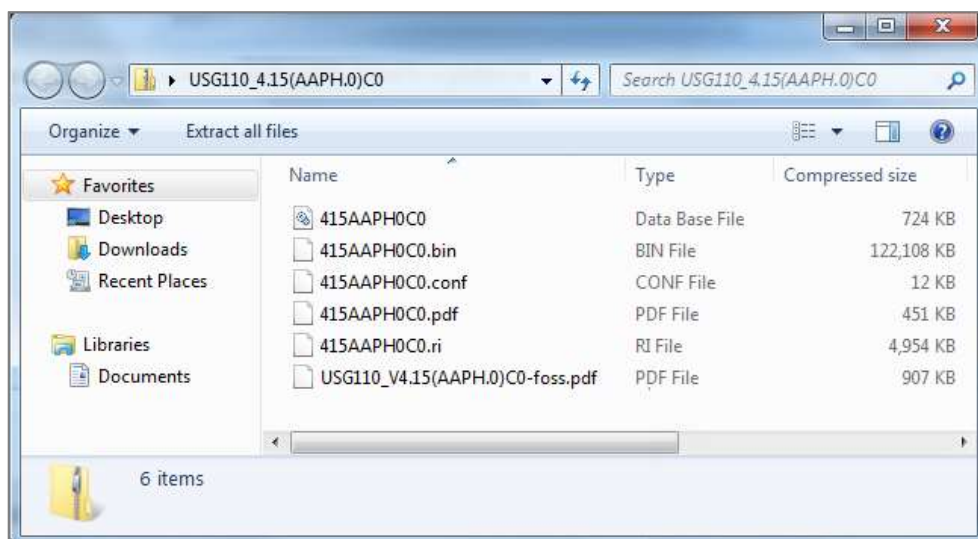
USG1100

ALL	Technical Documentation	Datasheet	Firmware	MIB File	Certification
Material	Version	Checksum	Release Date	Release Note	Download
Firmware	4.15(AAPH.0)C0		Mar 25, 2016		
3G Dongle Document	3		Mar 26, 2015		

Extract firmware zip file.



USG110_4.15(AAPH.0)C0.zip



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)

Firmware Status

#	Status	Model	Version	Released Date
1	Running	USG110	V4.13(AAPH.1)ITS-WK41-r64509	2015-10-13 23:09:45
2	Standby	USG110	V4.11(AAPH.2)	2015-04-20 20:41:35

Page 1 of 1 | Show 50 items | Displaying 1 - 2 of 2

Upload File

To upload image file in system space: 1

Boot Options

☒ Reboot now

☐ Don't Reboot

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path:

MAINTENANCE > File Manager > Firmware Package > Upload File > (2)

Firmware Status

Reboot now

#	Status	Model	Version	Released Date
1	Running	USG110	V4.13(AAPH.1)ITS-WK41-r64509	2015-10-13 23:09:45
2	Standby	USG110	V4.11(AAPH.2)	2015-04-20 20:41:35

Page 1 of 1 Show 50 items Displaying 1 - 2 of 2

Upload File

To upload image file in system space: 2

Boot Options

☒ Reboot now
☐ Don't Reboot

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path: C:\fakepath\415AAPH0C0.bin

To upload firmware, click **Browse** to the location of the file (*.bin) and then click **Upload**.

Upload File

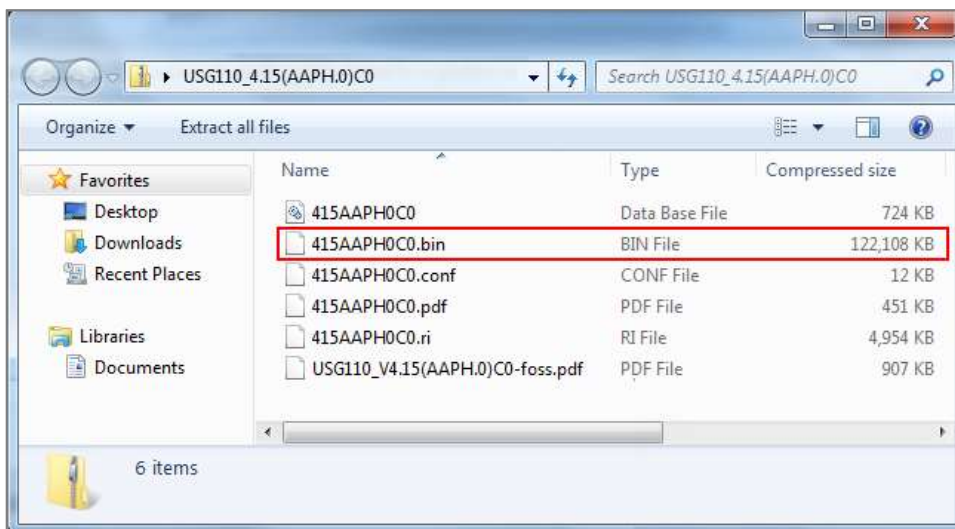
To upload image file in system space: 1

Boot Options

☒ Reboot now
☐ Don't Reboot

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path:



Upload File


To upload image file in system space: ▼

Boot Options

☒ Reboot now
☐ Don't Reboot

To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path:

 **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?

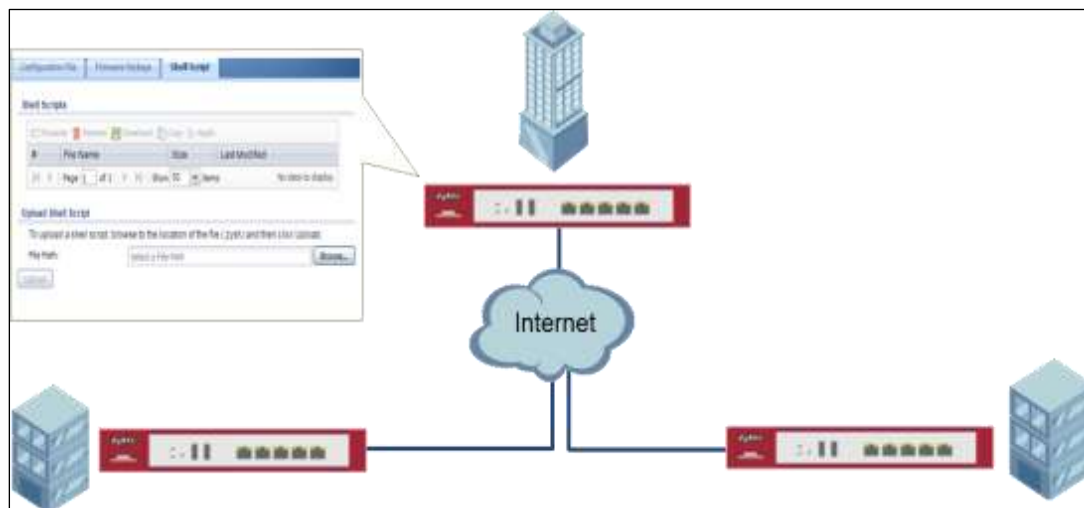
If you cannot download the firmware, please check if you enable the **Destroy compressed files that could not be decompressed** function in **Anti-Virus**.

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.



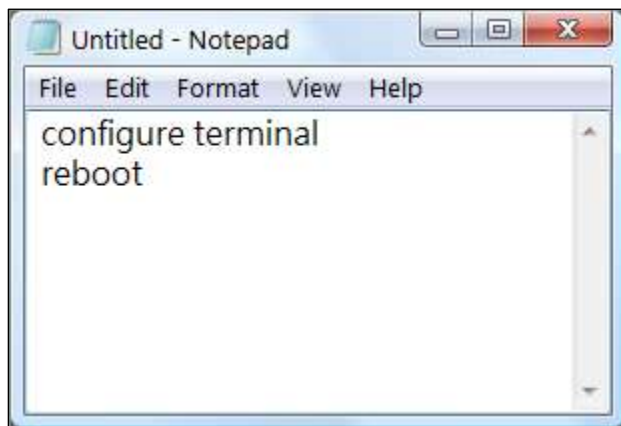
ZyWALL/USG Auto Schedule Reboot Settings



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"

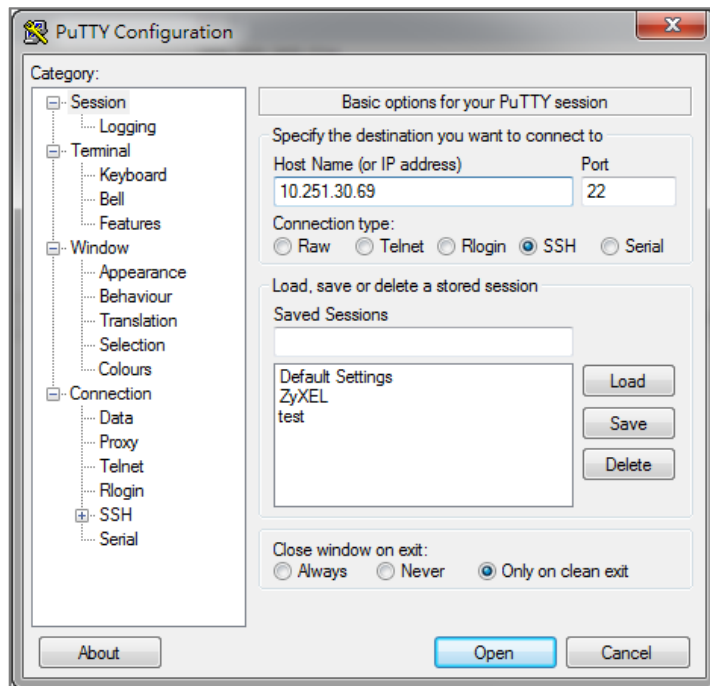


- 3 In the ZyWALL/USG, go to **MAINTENANCE > File Manager > Shell Script**. Click **Browse...** to find the reboot_device.zysh file. Click **Upload** to begin the upload process.



Set Up the Schedule Run

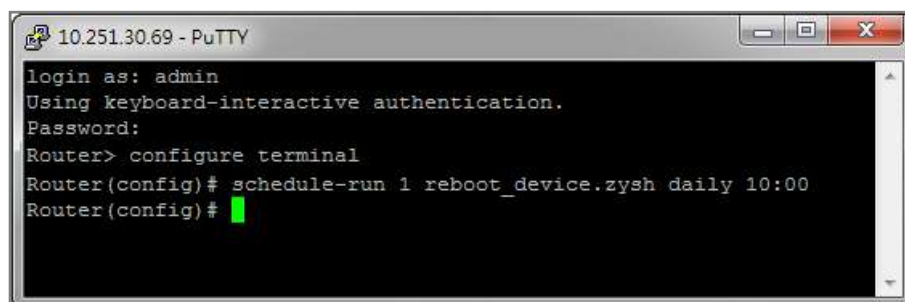
- 1 Login the device via console/telnet/SSH (using PuTTY in this example)



- 2 Issuing below commands based on three different (daily, weekly and monthly) user scenarios:

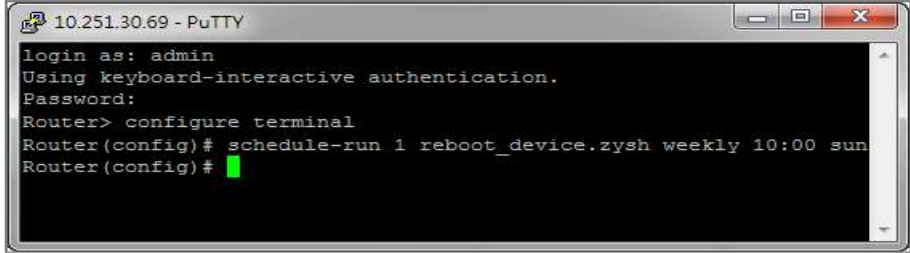
a. Router(config)# schedule-run 1 reboot_device.zysh daily 10:00

(The device will reboot at 10:00 everyday)



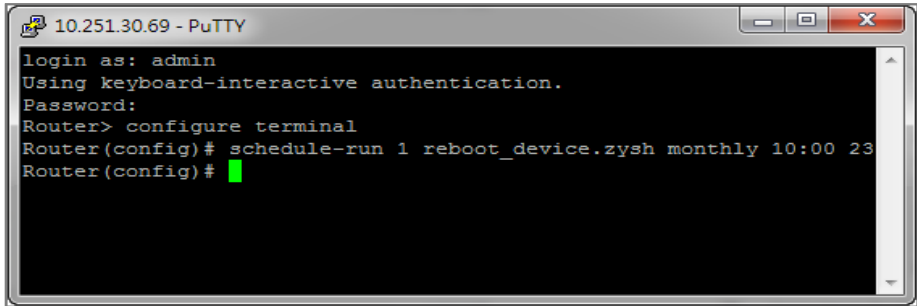
b. Router(config)# schedule-run 1 reboot_device.zysh weekly 10:00 sun

(The device will reboot at 10:00 every Sunday)



```
10.251.30.69 - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:
Router> configure terminal
Router(config)# schedule-run 1 reboot_device.zysh weekly 10:00 sun
Router(config)#
```

- c. Router(config)# schedule-run 1 reboot_device.zysh monthly 10:00 23
(The device will reboot at 10:00 every month on 23th)



```
10.251.30.69 - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:
Router> configure terminal
Router(config)# schedule-run 1 reboot_device.zysh monthly 10:00 23
Router(config)#
```

Check the Reboot Status

- 3 Login the device via console/telnet/SSH, the reboot runs as scheduled

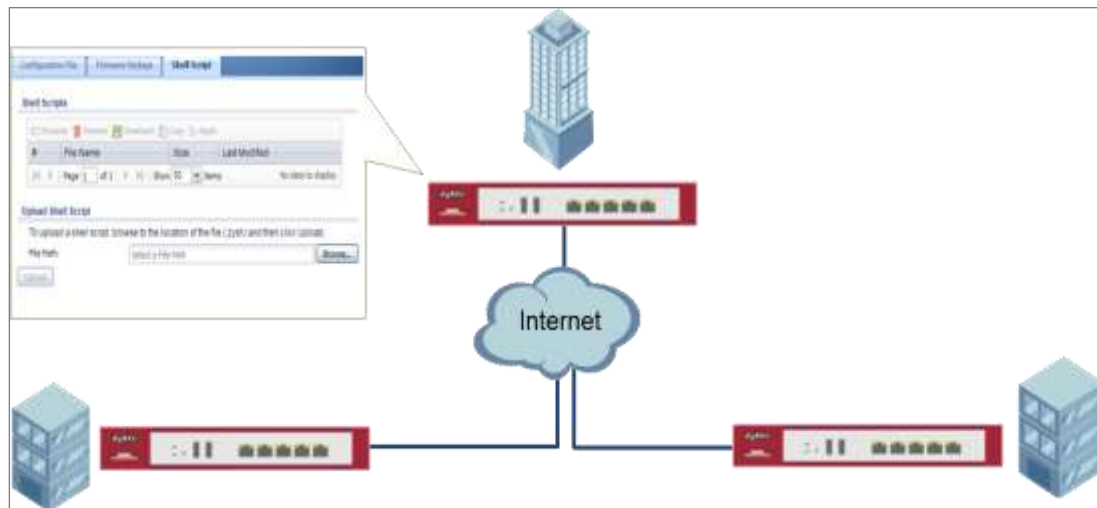
- 4 Go to **Configuration > System> Date/Time**, check **Current Date/Time**.

Figure Configuration > System >Date/Time

Date/Time	
Current Time and Date	
Current Time:	13:47:47 UTC+08:00
Current Date:	2017-06-29

How to continuously run a ZySH script

This example shows how to use shell script and continuously run a ZySH script automatically for maintenance purpose.

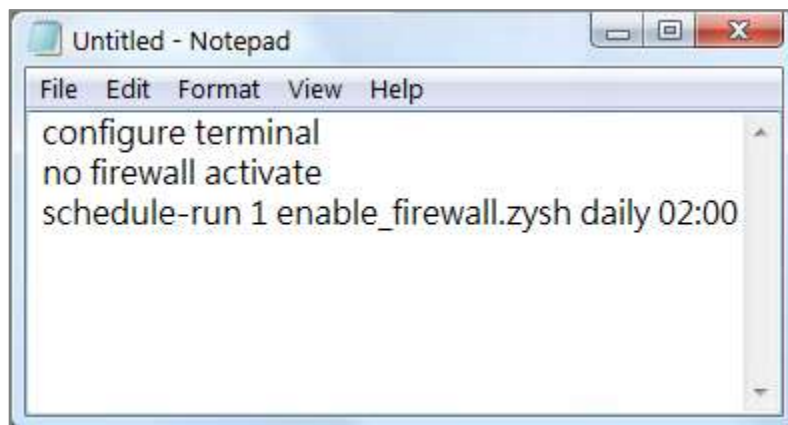


ZyWALL/USG continuously run a ZySH script Settings

 Note: This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the Shell Script

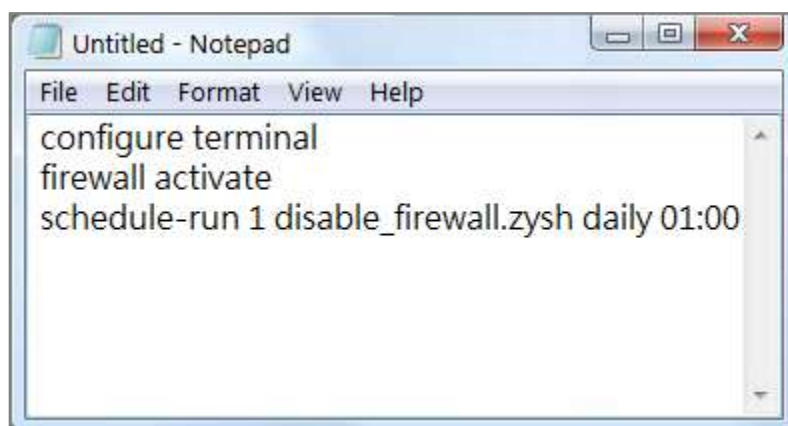
- 1 Run Windows Notepad application and input below command:



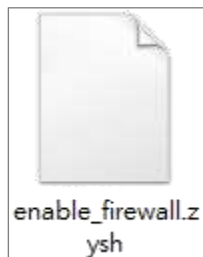
- 2 Save this file as "disable_firewall.zysh"



- 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.

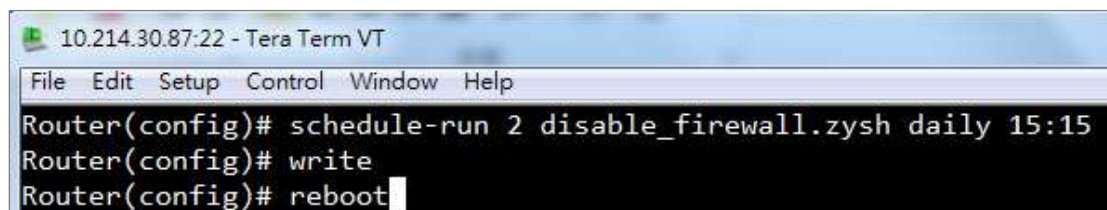


Set Up the Schedule Run

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

System Uptime	Current Date/Time
00:02:48	<u>2017-06-29 / 15:15:26 UTC+08:00</u>

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.

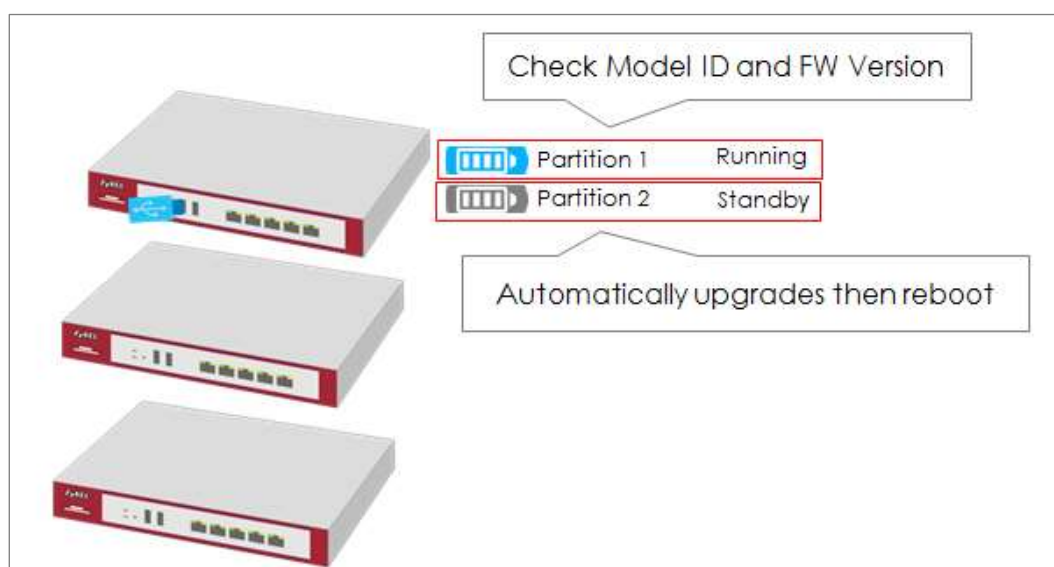



Figure 1 Automatic USB Firmware Upgrade

 **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:

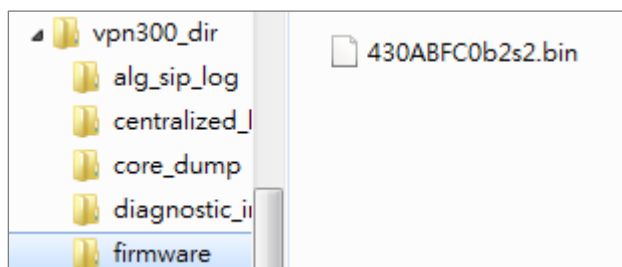
Router(config)# usb-storage update-firmware enable

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

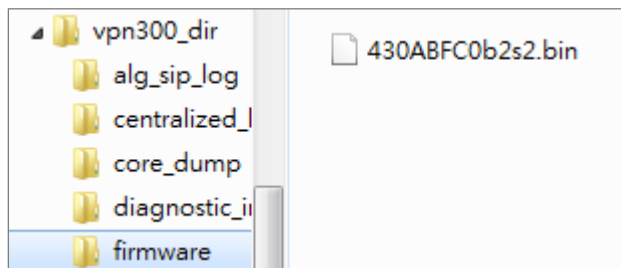
core_dump

diagnostic_info

firmware

packet_trace

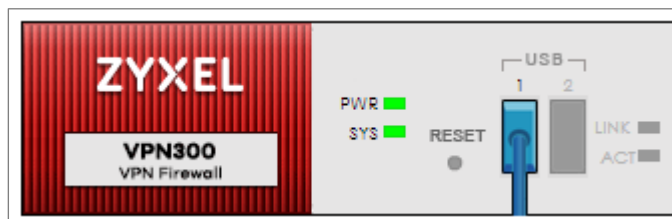
Firmware Folder is Created Automatically



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

Device Information		
System Name:	Serial Number:	MAC Address Range:
VPN300	S172L18290016	BB:EC:A3:AF:CD:08 - BB:EC:A3:AF:CD:12
System UpTime:	Boot Status:	Firmware Version:
00:29:24	OK	V4.30(A8FG.0)B2 / 2017-07-28 22:44:54
Firmware Upgrade License:	Current Date/Time:	
Activated	2017-09-07 / 11:08:03 UTC+08:00	









MONITOR > Log > View log

254	201...	info	VPN300 is configured successfully with startup configuration file.
-----	--------	------	--

What Can Go Wrong?

- 1 The USB storage must use the FAT16, FAT32, EXT2, or EXT3 file system.
Otherwise, it may not be detected by the ZyWALL/USG.
- 2 The device only checks the firmware under the specific folder.
Therefore, make sure the firmware is saved in the correct folder under the root directory: **\ProductName_dir\firmware**. For example:
\vpn300_dir\firmware
- 3 If there are multiple firmware files in the firmware folder of one model, the device only checks the first one in order.

Multiple firmware files of one model in the same folder is not supported.

	430_Internal_Release_Note_b2s2.docx	2017/8/31 下午 0...	Microsoft Word ...
	430ABFC0b2s2.bin	2017/8/31 下午 0...	BIN 檔案
	430ABFC0b2s2.conf	2017/8/31 下午 0...	CONF 檔案
	430ABFC0b2s2.db	2017/8/31 下午 0...	Data Base File
	430ABFC0b2s2.ri	2017/8/31 下午 0...	RI 檔案
	430ABFC0b2s2-MIB.zip	2017/8/31 下午 0...	壓縮的 (zipped) ...
	ABFC119.bm	2017/8/31 下午 0...	BM 檔案
	firmware.xml	2017/8/31 下午 0...	XML Document

- 4 Make sure the product model ID of the USB firmware is compatible with the device. The device writes logs on the console and device log if the firmware model ID is incompatible.

Console Message

```
Router(config)# firmware verifying...
Product model id is not compatible!!
This product's model id is E134
The ZLD-current image supports the following product model id :
E10B
USB update-firmware fail: File damaged. file name: 430AALA0a1.bin
```

MONITOR > Log > View log

#	Time	Priority	Category	Message	Note
20	2017-09-11 09:54...	error	System	USB update-firmware fail: file damaged, file name: 430AALA2011.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
144	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
234	2017-09-11 09:41...	notice	System	Device do not have token to access cloud server [count=2]	System
283	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...	error	System	USB update-firmware fail: Same firmware version. file name: 430ABFC0b2s2.bin	USB update firm...
784	2017-09-11 09:26...	notice	System	Device do not have token to access cloud server [count=2]	System

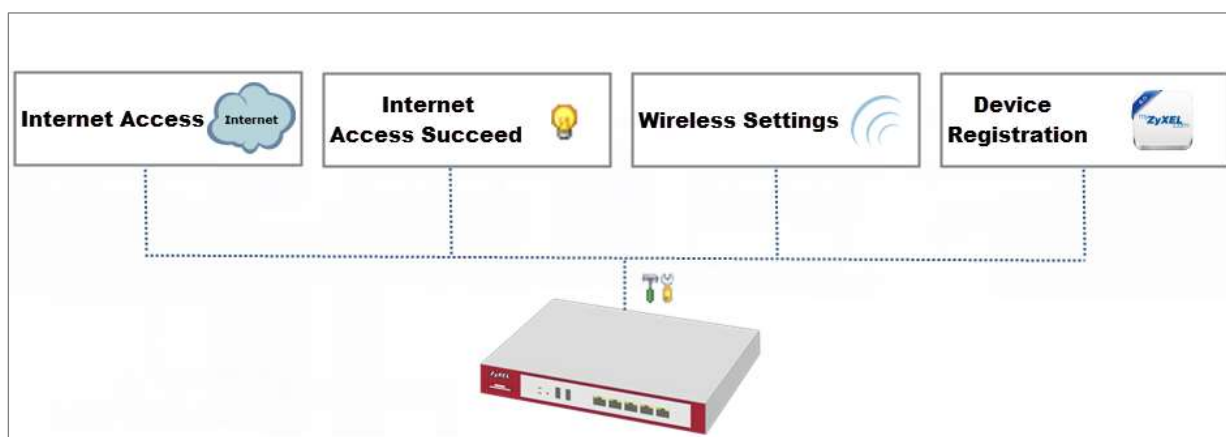
- 6 This feature does not support the Device HA Pro firmware auto upgrade to passive devices. Do not use USB firmware upgrade on devices with Device HA Pro function activated. When using USB firmware upgrade on a device HA or in a device HA Pro scenario, make sure you plug the USB storage to the passive 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



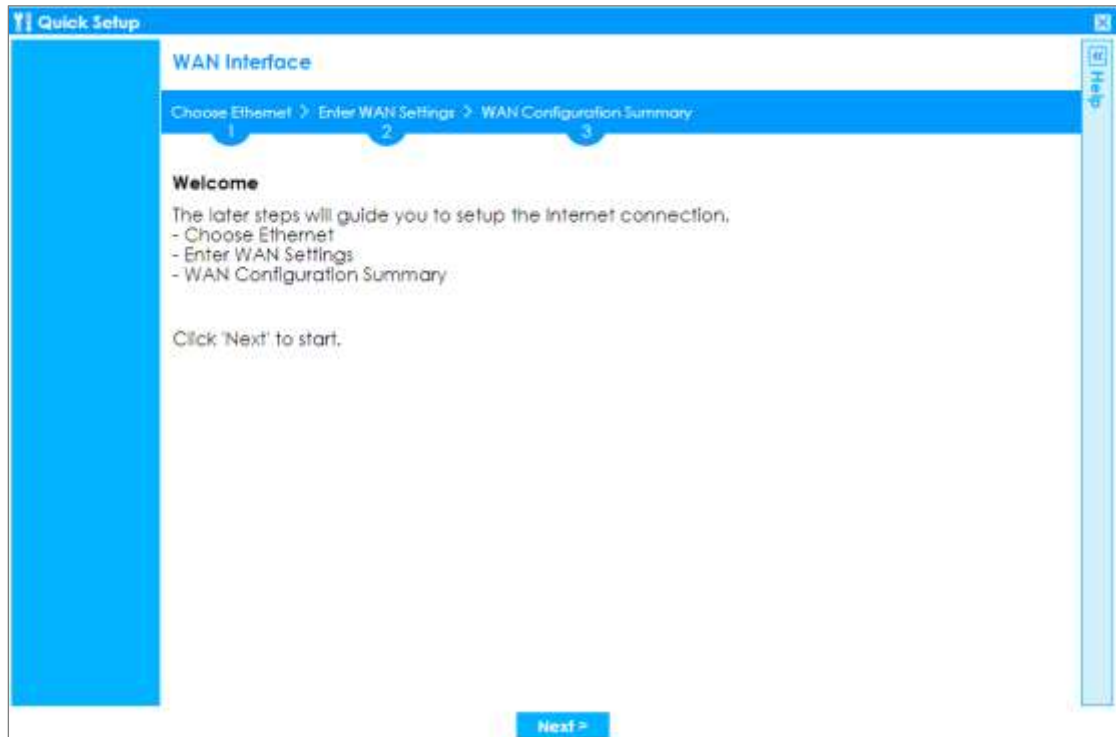
 Note: You need internet access to activate your ZyWALL/USG subscription services. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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



Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary

1 2 3

Ethernet

Ethernet Selection:



Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary

1 2 3

IP Address Assignment

WAN Type Selection:



Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary

1 2 3

Interface

WAN Interface:

Zone:

IP Address Assignment:

Enter the **IP Address**, **IP Subnet Mask** and **Gateway IP Address** exactly as given by your ISP or network administrator. First/Second DNS Servers are optional. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access

Quick Setup

WAN Interface

Choose Ethernet > **Enter WAN Settings** > WAN Configuration Summary

1 2 3

ISP Parameters

Encapsulation: Ethernet

IP Address Assignment

WAN Interface: ge1

Zone: WAN

IP Address: 111.112.36.59

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 111.112.36.254 (Optional)

First DNS Server:

Second DNS Server:

The **Internet Access Succeed** page will display the summary of Internet access of the **First Setting**. If you select **I have two ISPs** in **Internet Access > ISP Setting**, click **Next** to configure the second WAN interface or continue to the **Wireless Settings** page.

Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed

Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > **WAN Configuration Summary**

1 2 3

Congratulations. The Internet Access wizard is completed.

IP Address Assignment

Encapsulation: Ethernet

WAN Interface: ge1

Zone: WAN

IP Address Assignment: Static

IP Address: 111.112.36.59

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 111.112.36.254

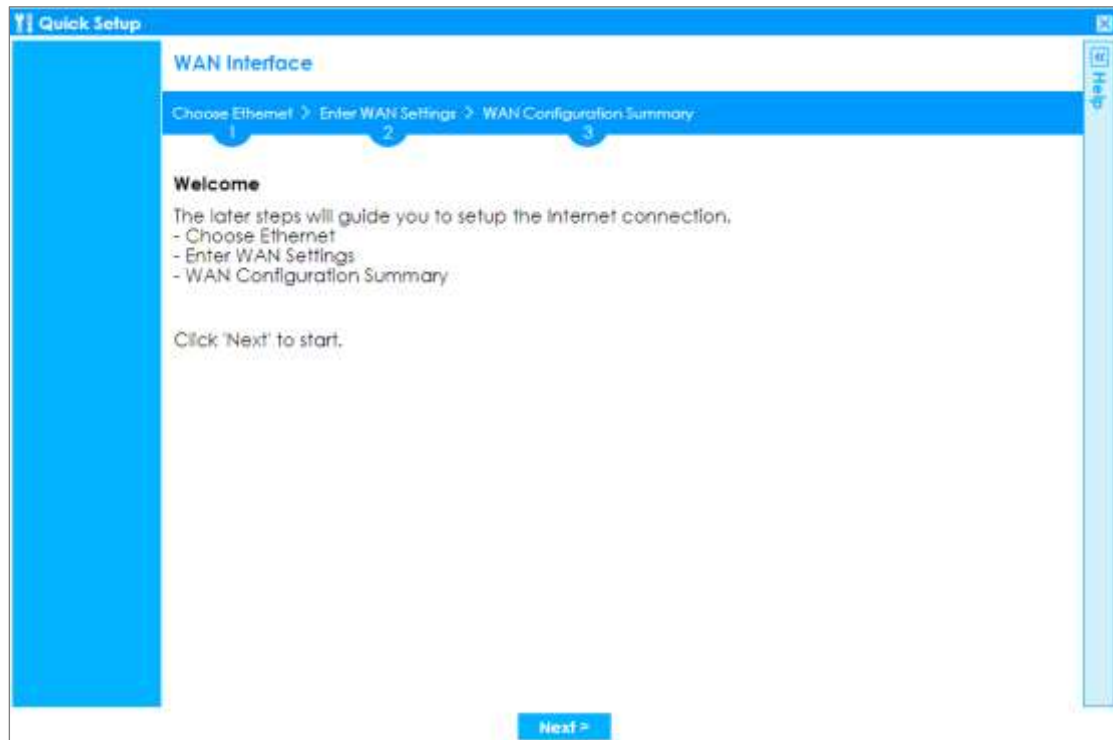
First DNS Server:

Second DNS Server:

Set Up the Internet Access (PPPoE) Wizard on the ZyWALL/USG

In the ZyWALL/USG **Installation Setup Wizard** Welcome page, click **Next** to start configuring for Internet. Click the double arrow in the upper right corner to display (<<) or hide (>>) the help.

Installation Setup Wizard > Welcome



In the **Internet Access** page, you can configure Internet connections from two Internet service providers (ISPs). Connect your ISP devices to your ZyWALL/USG WAN port, select **I have two ISPs** if you want to configure two Internet connections or leave it cleared to configure just one.

Choose the **Encapsulation** option to be **PPP over Ethernet**, leave **Zone** as default setting Internet connection belongs to the WAN zone. Leave the **IP Address Assignment** section to be the **Auto** and click **Next**.

Installation Setup Wizard > Welcome > Internet Access

Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary

1 2 3

Ethernet

Ethernet Selection:

Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary

1 2 3

IP Address Assignment

WAN Type Selection:

Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary

1 2 3

Interface

WAN Interface:

Zone:

IP Address Assignment:

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

Quick Setup

WAN Interface

Choose Ethernet > **Enter WAN Settings** > WAN Configuration Summary

1 2 3

ISP Parameters

Encapsulation: PPPoE

Service Name: (Optional)

Authentication Type: Chap/PAP

User Name : ZYXEL_PPPoE

Password: ****

Retype to Confirm: ****

☒ Nailed-Up

Idle timeout: 100 Seconds

IP Address Assignment

WAN Interface: ge1_ppp

Zone: WAN

IP Address: Auto

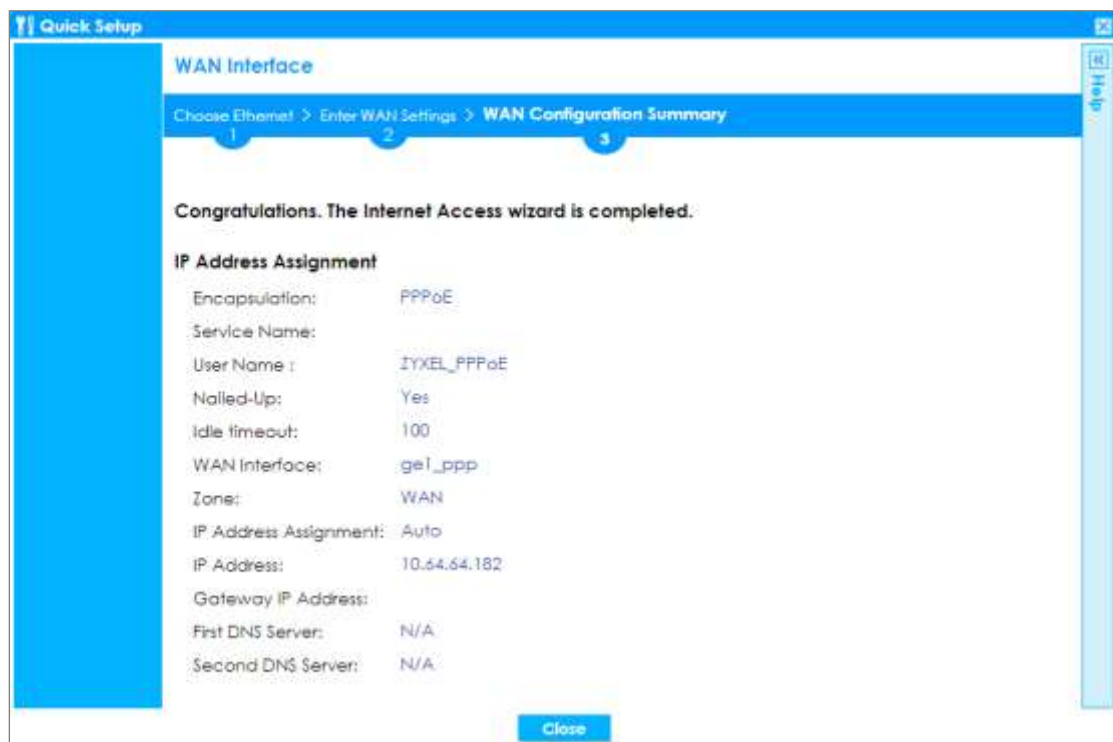
Note

Configure PPPoE will change ethernet interface ip address as 0.0.0.0.

[< Back](#) [Next >](#)

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.

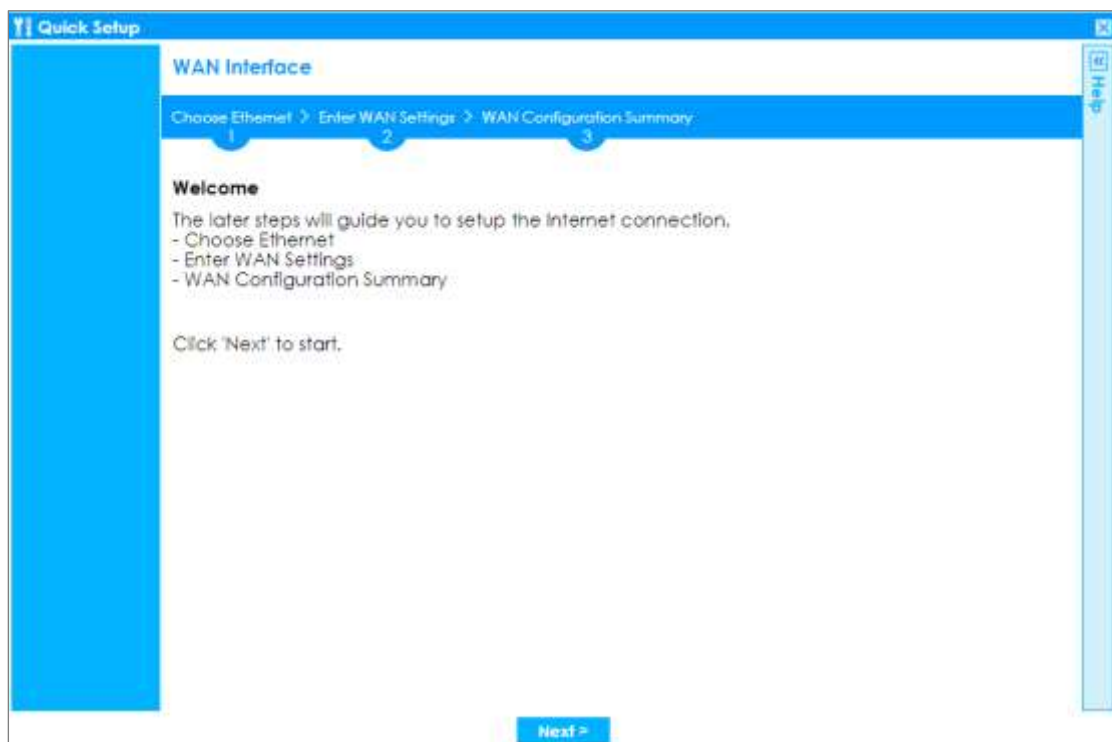
Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed



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.

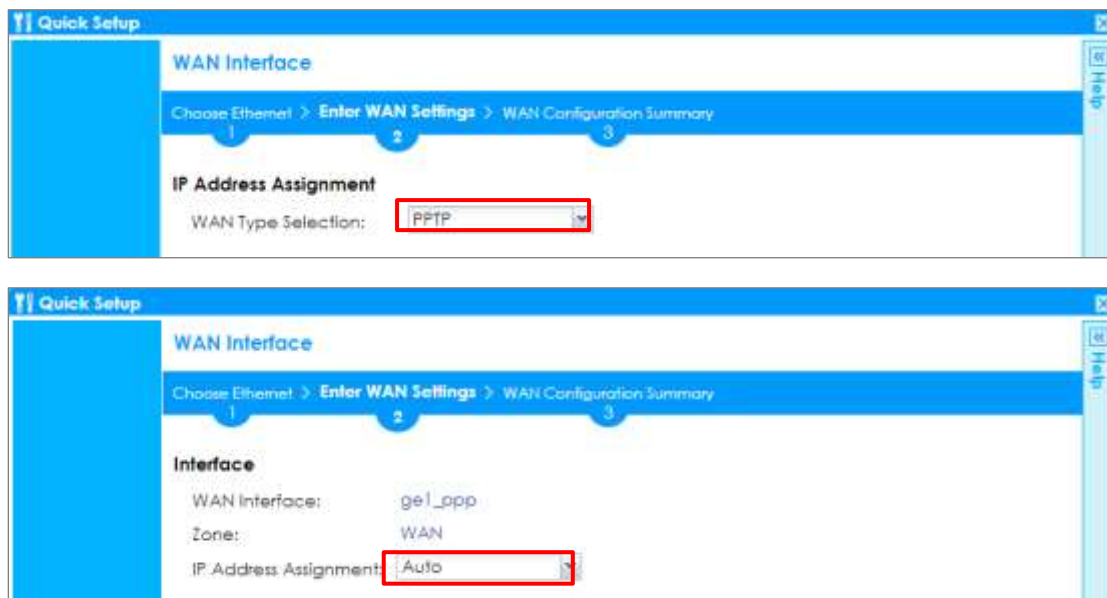
Installation Setup Wizard > Welcome



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



Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary

1 2 3

IP Address Assignment

WAN Type Selection: PPTP

Quick Setup

WAN Interface

Choose Ethernet > Enter WAN Settings > WAN Configuration Summary

1 2 3

Interface

WAN Interface: ge1_ppp

Zone: WAN

IP Address Assignment: Auto

Select the **Authentication Type** to be the authentication method by the remote node. Enter the **User Name** and **Password** exactly as given by your ISP or network administrator. Select **Nailed-UP** if you want to keep the connection always up or type the desired **Idle Timeout** value in seconds. Click **Next**.

Enter the **Base IP Address**, **IP Subnet Mask**, **Gateway IP Address** assigned to you by your ISP. Type the **Server IP** address of the **PPTP Server**. Click **Next**.

Installation Setup Wizard > Welcome > Internet Access

Quick Setup

WAN Interface

Choose Ethernet > **Enter WAN Settings** > WAN Configuration Summary

1 2 3

ISP Parameters

Encapsulation: PPTP

Authentication Type: Chap/PAP

User Name: ZYXEL_PPTP

Password: ****

Retype to Confirm: ****

☐ Nailed-Up

Idle timeout: 100 Seconds

PPTP Configuration

Base Interface: ge1

Base IP Address: 111.111.36.99

IP Subnet Mask: 255.255.255.0

Gateway IP Address: 111.111.36.254 (Optional)

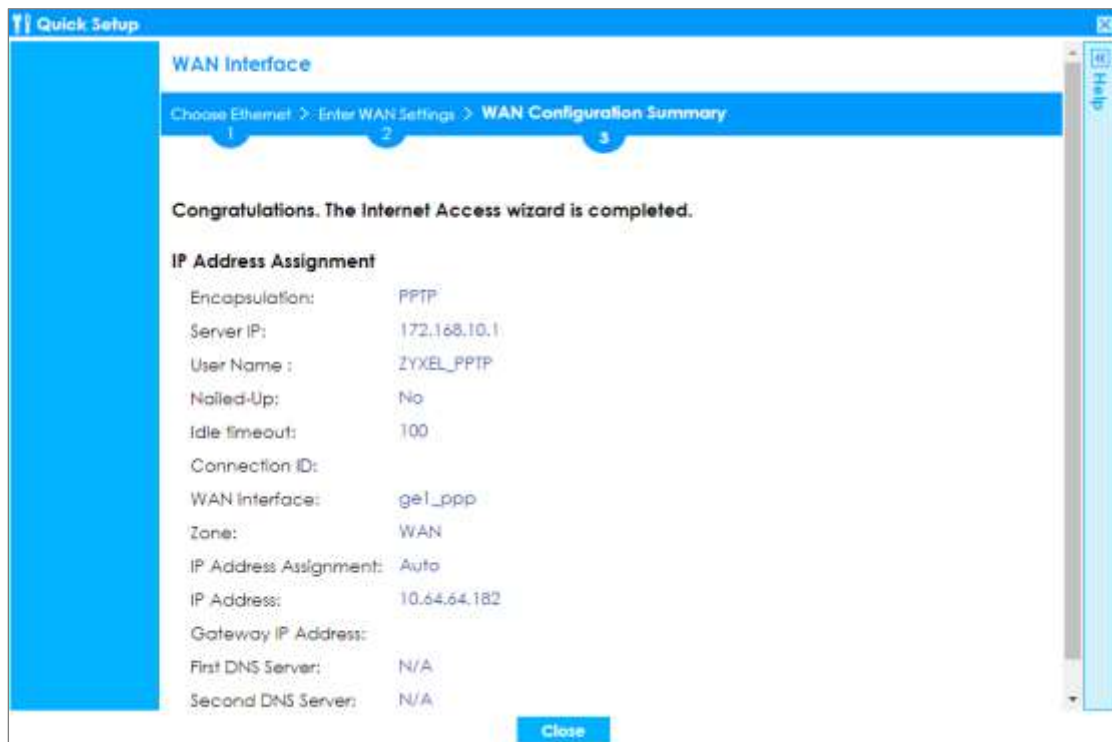
Server IP: 172.168.10.1 (Optional)

Connection ID: (Optional)

< Back Next >

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.

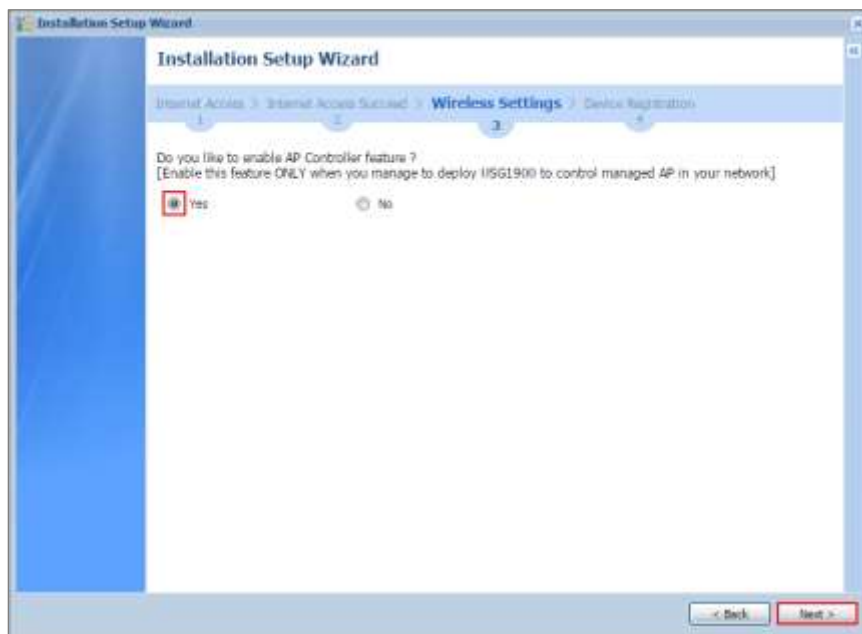
Installation Setup Wizard > Welcome > Internet Access > Internet Access Succeed



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.

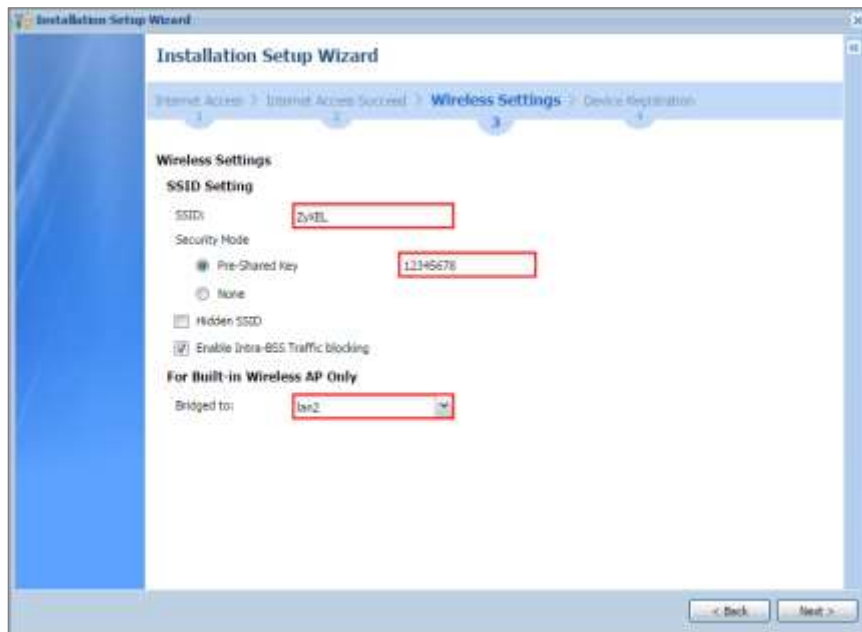
Select **Hidden SSID** to hide the SSID from site tool scanning.

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**



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



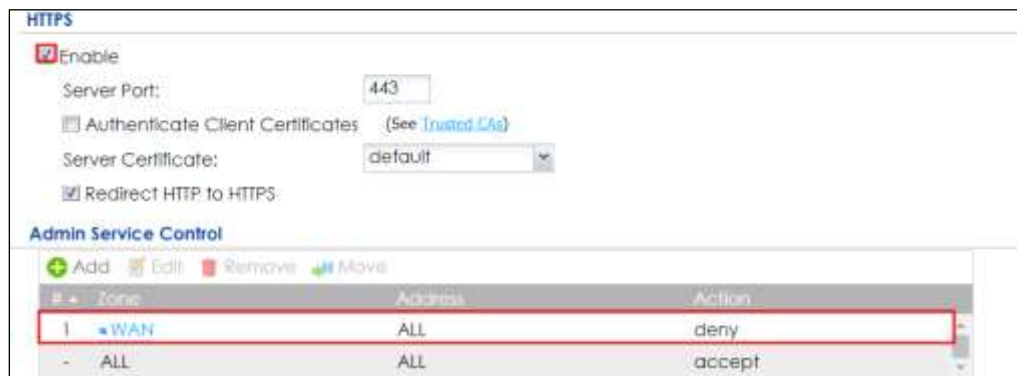
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG60 (Firmware Version: ZLD 4.25).

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**.

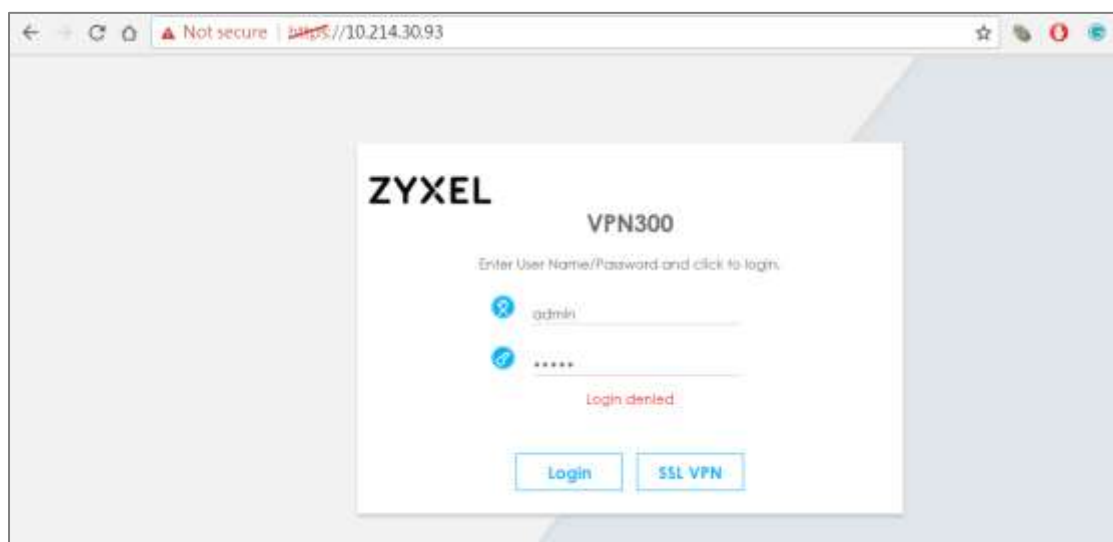
CONFIGURATION > System > WWW > Admin Service Control > Add Admin ACL Rule 1



Test the Web Access

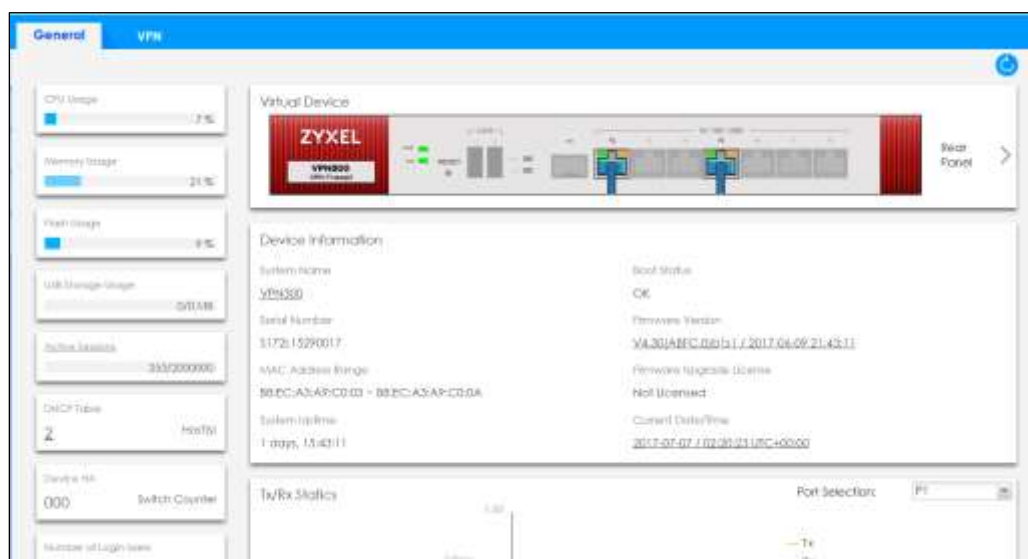
Login to the device via the WAN interface with the administrator's user name and password. The screen will show **Login denied**.

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:

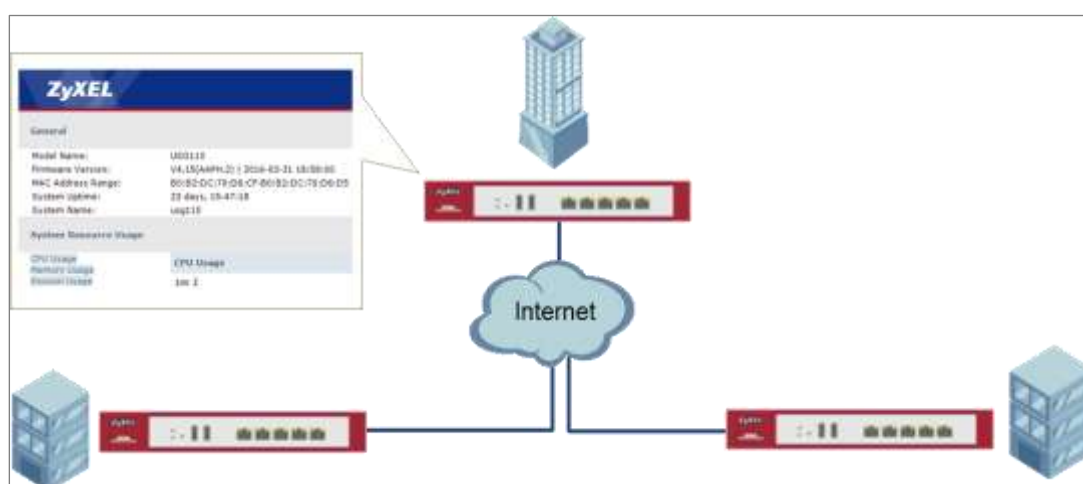
[Email Log Now](#)
[Refresh](#)
[Clear Log](#)

#	Time	Priority	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

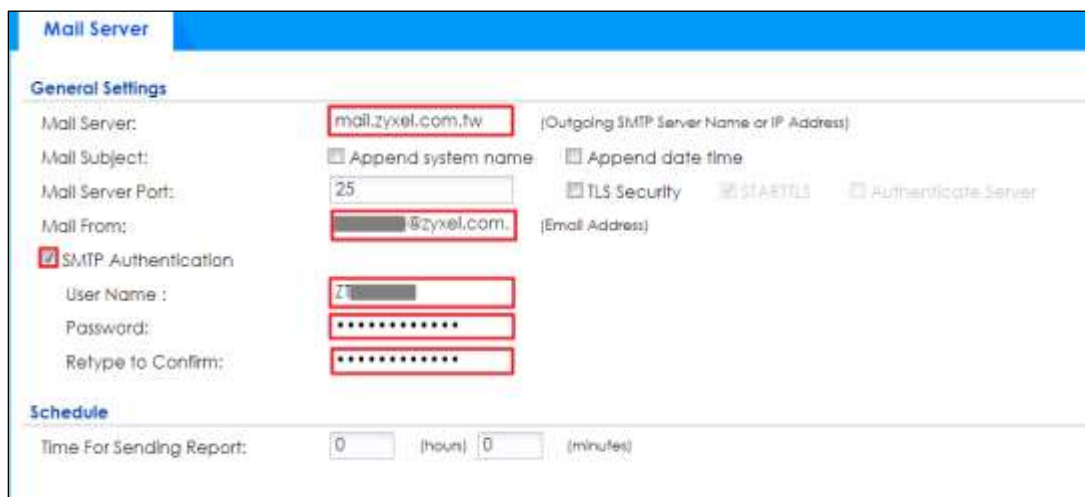


General Settings

☒ Enable Email Daily Report

Type the SMTP server name or IP address. In **Mail From**, type the e-mail address from which the outgoing e-mail is delivered. In **Mail To**, type the e-mail address to which the outgoing e-mail is delivered. Select **SMTP Authentication** if it is necessary to provide a user name and password to the SMTP server.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings



Mail Server

General Settings

Mail Server: mail.zyxel.com.tw (Outgoing SMTP Server Name or IP Address)

Mail Subject: ☐ Append system name ☐ Append date time

Mail Server Port: 25 ☐ TLS Security ☒ STARTTLS ☐ Authenticate Server

Mail From: admin@zyxel.com. (Email Address)

☒ SMTP Authentication

User Name: admin

Password: *****

Retype to Confirm: *****

Schedule

Time For Sending Report: 0 (hours) 0 (minutes)

In the **CONFIGURATION > Log & Report > Email Daily Report > Schedule**. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.

CONFIGURATION > Log & Report > Email Daily Report > Schedule

Schedule

Time For Sending Report:

12

(hours)

0

(minutes)

Select the information to include in the report. Types of information include **System Resource Usage**, **Wireless Report**, **Threat Report**, and **Interface Traffic Statistics**.

Select **Reset counters after sending report successfully** if you only want to see statistics for a 24 hour period.

CONFIGURATION > Log & Report > Email Daily Report > Report Items

Report Items

System Resource Usage :

☒ CPU Usage
 ☒ Memory Usage
 ☒ Session Usage
 ☒ Port Usage

Wireless Report :

☐ Station Count
 ☐ TX Statistics
 ☐ RX Statistics
 ☒ Content Filter

☒ Interface Traffic Statistics
 ☒ DHCP Table

☐ Reset counters after sending report successfully

Reset All Counters

Test the Daily Log Report

Click **Send Report Now** to have the ZyWALL/USG send the daily e-mail report immediately.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings

General Settings

☒ Enable Email Daily Report

Email Settings

Mail Subject:

Handbook mail

Mail To:

@zyxel.com.

(Email Address)

(Email Address)

(Email Address)

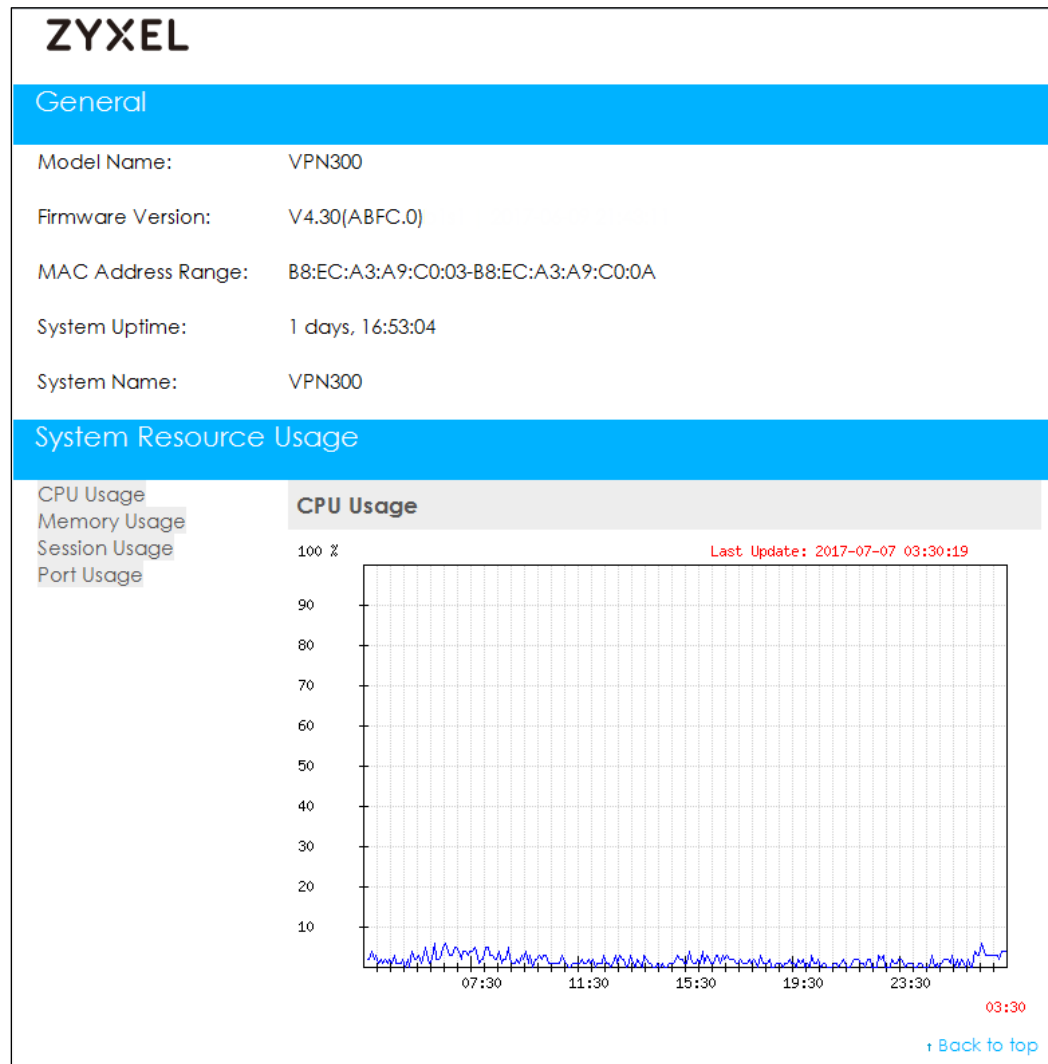
(Email Address)

(Email Address)

Send Report Now

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

Mail Server

General Settings

Mail Server: mail.zyxel.com.tw (Outgoing SMTP Server Name or IP Address)

Mail Subject: ☐ Append system name ☐ Append date time

Mail Server Port: 25 ☐ TLS Security ☒ STARTTLS ☐ Authenticate Server

Mail From: [redacted]@zyxel.com (Email Address)

☒ SMTP Authentication

User Name : [redacted]

Password: [redacted]

Retype to Confirm: [redacted]

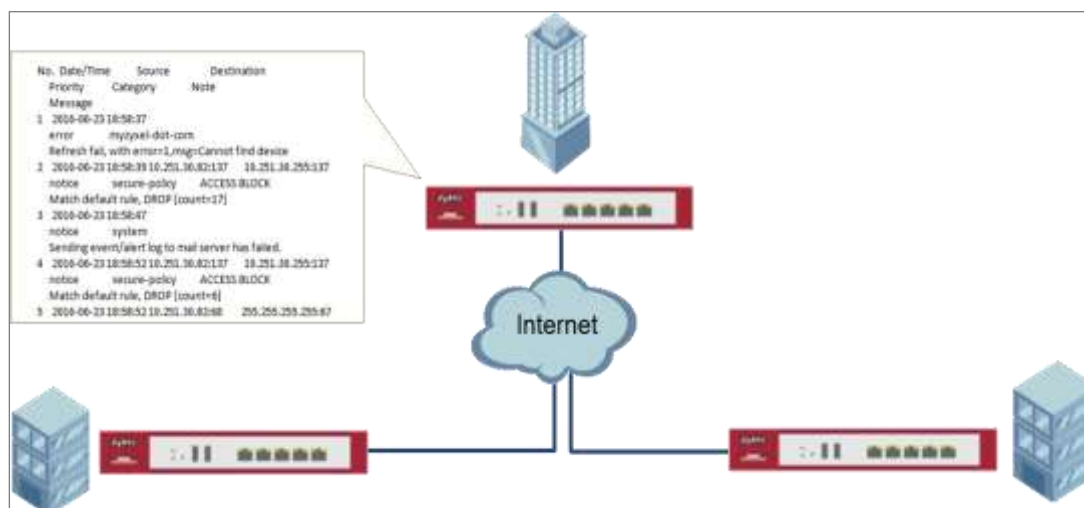
Schedule

Time For Sending Report: 0 (hours) 0 (minutes)

Make sure your ZyWALL to WAN security policy allow.

How to Setup and Configure Email Logs

This example shows how to set up the e-mail profiles to mail ZyWALL/USG log messages to the specific destinations. You can also specify which log messages to e-mail, and where and how often to e-mail them. When the Email Logs is configured, you will receive logs email report base on customized schedule.




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.
- Day for Sending Log** is available if the log is e-mailed weekly. Select the day of the week the log is e-mailed.
- Time for Sending Log** is available if the log is e-mailed weekly or daily. Select the time of day (hours and minutes) when the log is e-mailed. Use 24-hour notation.

4. Select **SMTP Authentication** if it is necessary to provide a user name and password to the SMTP server.

CONFIGURATION > Log & Report > Log Settings > System Log > Edit > E-mail Server 1



E-mail Server 1

☒ **Active**

Mail Server: (Outgoing SMTP Server Name or IP Address)

Mail Server Port: ☒ TLS ☒ STARTTLS ☐ Authentication Security

Mail Subject:

Send From: (E-Mail Address)

Send Log to: (E-Mail Address)

Send Alerts to: (E-Mail Address)

Sending Log:

Day for Sending Log:

Time for Sending Log:

☒ **SMTP Authentication**

User Name:

Password:

Retype to Confirm:

5. Go to **CONFIGURATION > Log & Report > Log Settings > System Log > Edit > Active Log and Alert**. Use the **System Log** drop-down list to change the log settings for all of the log categories.

CONFIGURATION > Log & Report > Log Settings > System Log > Edit > Active Log and Alert.

Active Log and Alert

Log Category +	System Log			Email Server 1		Email Server 2	
	disable	normal	debug	normal	debug	normal	debug
Auth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- PKI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- Authentication Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- Auth. Policy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- SSO	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- Web Authentication	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- Account	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
- User	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
BWM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Device HA	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
License	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Log & Report	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Network	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Active Log and Alert (AP)

Log Category +	System Log			Email Server 1		Email Server 2	
	disable	normal	debug	normal	debug	normal	debug
Auth	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
File manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Log & Report	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Network	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Routing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
System	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Wireless	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Test the Email Log

You will receive a log mail depends on the time you set in the E-mail Server.

ZyXEL Log Mail

From: ZyXEL Support [mailto:zyxel.support@zyxel.com]
 To: jaymiller@zyxel.com
 Subject: ZyXEL Log Mail

Content-Type: text/html; charset="utf-8"

No.	Time	Source	Destination
Priority	Category	Source	Dest
1	2018-08-22 15:02:03	192.168.1.1	192.168.1.1
2	2018-08-22 15:02:03	192.168.1.1	192.168.1.1
3	2018-08-22 15:02:03	192.168.1.1	192.168.1.1
4	2018-08-22 15:02:03	192.168.1.1	192.168.1.1
5	2018-08-22 15:02:03	192.168.1.1	192.168.1.1
6	2018-08-22 15:02:03	192.168.1.1	192.168.1.1
7	2018-08-22 15:02:03	192.168.1.1	192.168.1.1
8	2018-08-22 15:02:03	192.168.1.1	192.168.1.1
9	2018-08-22 15:02:03	192.168.1.1	192.168.1.1

What Could Go Wrong?

Make sure your Email settings are all correct.

CONFIGURATION > Log & Report > Email Daily Report > Email Settings

E-mail Server 1

☒ Active

Mail Server:

mail.zyxel.com.tw

(Outgoing SMTP Server Name or IP Address)

Mail Server Port:

25

☒ TLS
 ☒ STARTTLS
 ☐ Authentica
 Security

Mail Subject:

Handbook test

Send From:

zyxel.com

(E-Mail Address)

Send Log to:

zyxel.com

(E-Mail Address)

Send Alerts to:

(E-Mail Address)

Sending Log:

Daily and When Full

Day for Sending Log:

Sunday

Time for Sending Log:

10:00

☒ SMTP Authentication:

User Name :

zt

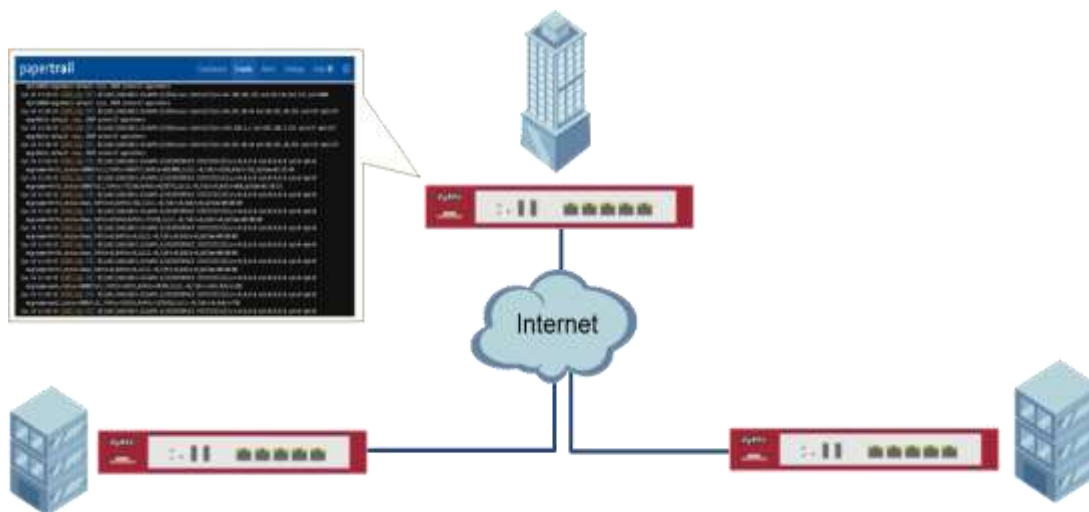
Password:

Retype to Confirm:


Make sure your ZyWALL to WAN security policy allow.

How to Setup and send logs to a Syslog Server

This example shows how to set up the syslog server profiles to mail ZyWALL/USG log messages to the specific destinations. You can also specify which log messages to syslog server. When the syslog server is configured, you will receive the real time system logs.



ZyWALL/USG Setup and Configure sending logs to a syslog and Vantage Reports Server

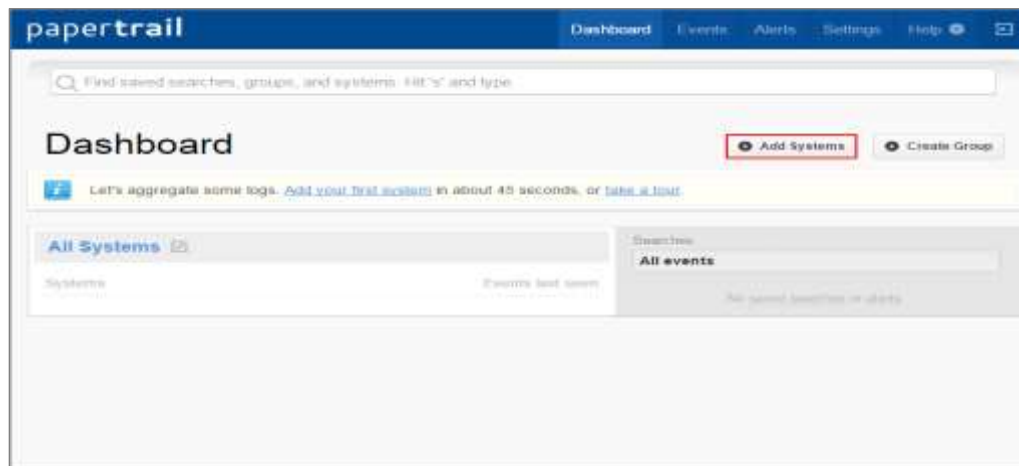
 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG110 (Firmware Version: ZLD 4.25).

Set Up the Syslog Server (Use Papertrail syslog in this example)

Register an account on Papertrail: <https://papertrailapp.com>

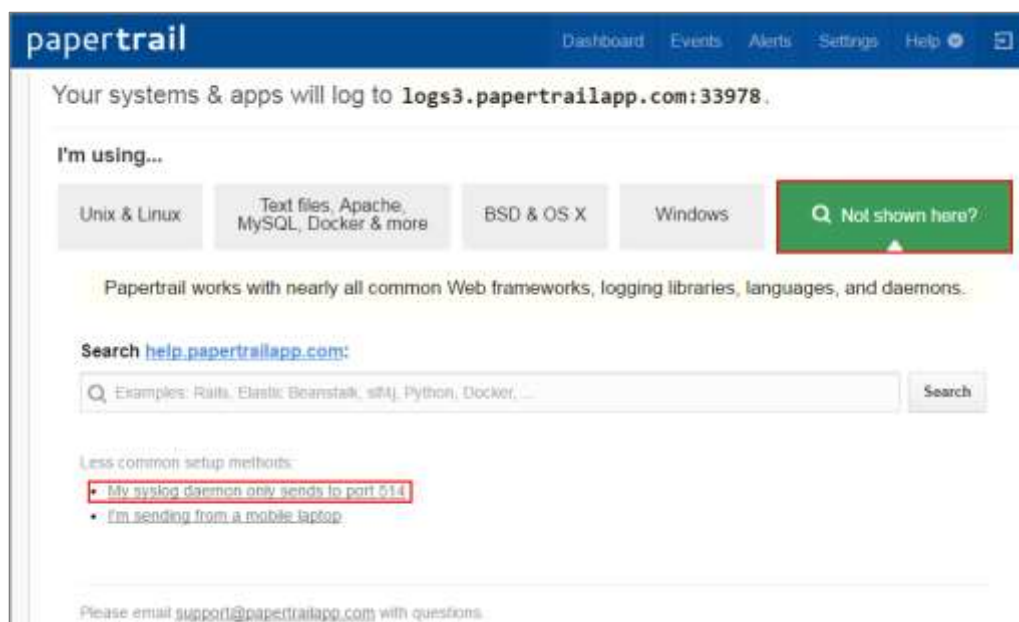
Go to **Dashboard > Add Systems**.

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

papertrail Dashboard Events Alerts Settings Help

Choose your situation:

- A My syslogd only uses the default port**
GNU syslogd and some embedded devices will only log to port 514. A few old Linux distro versions use GNU syslogd (mostly CentOS and Gentoo).
- B I use Cloud Foundry**
Register each app separately. Use Heroku? [Here's how](#)
- C My system's hostname changes**
In rare cases, one system may change hostnames frequently. For example, a roaming laptop which sets its hostname based on DHCP (and roams across networks).

Let's create a log destination on port 514 that works with GNU syslogd.

Multiple systems share 1 IP (NAT)? Enter the same IP for each. We'll do the rest.

111.250.188.9
Example: 208.57.123.234

What should we call it?
ZyXEL_Log
Examples: www42, SY8_1, bb1.example.com. Does not need to match hostname

Save

Write down the Papertrail-provided domain name (logs.papertrailapp.com in this example).

Dashboard > Add Systems > > I'm using > Choose your situation > System Created

papertrail Dashboard Events Alerts Settings Help

Setup ZyXEL_Log...

[Edit Settings](#)

✓ System created.

ZyXEL_Log will log to **logs.papertrailapp.com**.

I'm using...

Unix & Linux Text files, Apache, MySQL, Docker & more BSD & OS X Windows 🔍 Not shown here?

1 See which logger your system uses. Run:

```
ls -ld /etc/*syslog*
```

Which filename is listed?

✓ **rsyslog.conf**

Set Up the ZyWALL/USG Remote Server Setting

1. Go to **CONFIGURATION > Log & Report > Log Settings > Remote Server > Edit**. Set **Log Format** to be **CEF/Syslog**. Type the **Server Address** to be the Papertrail- provided domain name (logs.papertrailpp.com in this example).
2. Use the **System Log** drop-down list to change the log settings for all of the log categories.

CONFIGURATION > Log & Report > Log Settings > Remote Server > Edit

Log Settings for Remote Server

☒ Active

Log Format: CEF/Syslog

Server Address: logs.papertrailpp (Server Name or IP Address)

Log Facility: Local 1

Active Log

Log Category +	disable	normal	debug
+ Auth	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ BWM	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ Device HA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ File manager	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ License	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ Log & Report	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ Network	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Test the Remote Server

You will receive a log mail depends on the time you set in the E-mail Server.

ZyXEL Log Mail

The screenshot shows the 'papertrail' interface with a navigation bar containing 'Dashboard', 'Events', 'Alerts', 'Settings', and 'Help'. The main area displays a log of events, including messages about default rules, interface statistics, and port status changes.

```

dpt=10039 msg=Match default rule, DROP proto=17 app=others
Jun 24 13:34:51 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=61.220.241.232 dst=59.124.163.152 spt=2800
dpt=10040 msg=Match default rule, DROP proto=17 app=others
Jun 24 13:34:52 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=10.251.30.44 dst=10.251.30.255 spt=137 dpt=137
msg=Match default rule, DROP proto=17 app=others
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=192.168.1.2 dst=192.168.1.255 spt=137 dpt=137
msg=Match default rule, DROP proto=17 app=others
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|Access Control|5|src=10.251.30.44 dst=10.251.30.255 spt=137 dpt=137
msg=Match default rule, DROP proto=17 app=others
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
msg=name=Port1,status=1000M/Full,TxPkts=5686777,RxPkts=6833009,Coll1.=0,TxB/s=1168,RxB/s=352,UpTime=02:35:44
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
msg=name=Port2,status=1000M/Full,TxPkts=772230,RxPkts=4228776,Coll1.=0,TxB/s=0,RxB/s=860,UpTime=02:10:25
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
msg=name=Port3,status=Down,TxPkts=0,RxPkts=562,Coll1.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
msg=name=Port4,status=Down,TxPkts=815244,RxPkts=773238,Coll1.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
msg=name=Port5,status=Down,TxPkts=0,RxPkts=0,Coll1.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
msg=name=Port6,status=Down,TxPkts=0,RxPkts=0,Coll1.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
msg=name=Port7,status=Down,TxPkts=0,RxPkts=0,Coll1.=0,TxB/s=0,RxB/s=0,UpTime=00:00:00
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
msg=name=wani,status=1000M/Full,TxPkts=42593,RxPkts=69784,Coll1.=0,TxB/s=1342,RxB/s=282
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
msg=name=wan2,status=100M/Full,TxPkts=552343,RxPkts=1239320,Coll1.=0,TxB/s=0,RxB/s=798
Jun 24 13:34:55 ZyXEL_Log CFFF 0|ZyXEL|USG110|4.15(AAPH.2)|0|INTERFACE STATISTICS|5|src=0.0.0.0 dst=0.0.0.0 spt=0 dpt=0
  
```

What Could Go Wrong?

Make sure your **Log settings for Remote Server** are all correct.

CONFIGURATION > Log & Report > Log Settings > Remote Server

Log Settings for Remote Server

☒ Active

Log Format: CEF/Syslog

Server Address: logs.papertrailapp (Server Name or IP Address)

Log Facility: Local 1

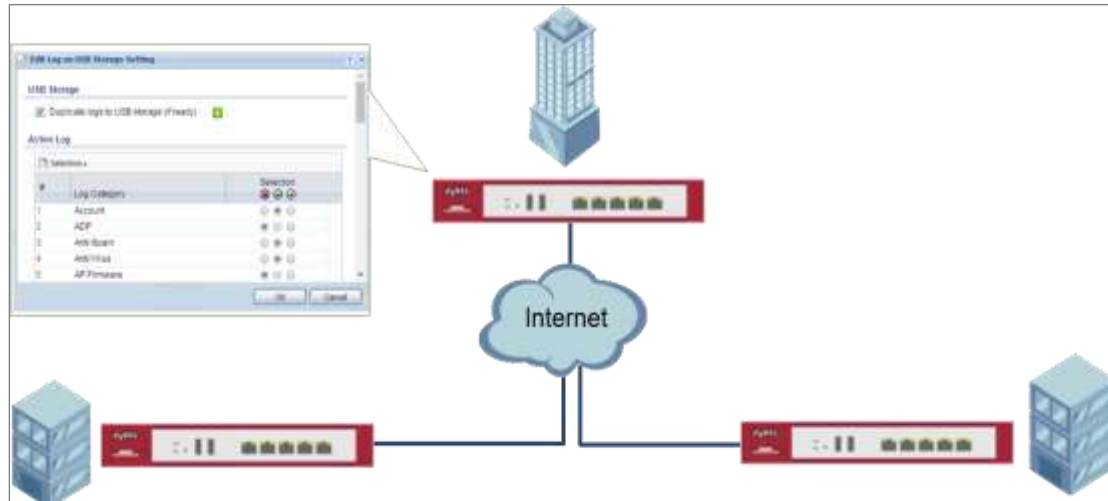
Active Log

Log Category +	disable	normal	debug
+ Auth	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ BWM	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ Device HA	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ File manager	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ License	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ Log & Report	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ Network	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
+ None	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>


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).

Go to **CONFIGURATION > System > USB Storage > Settings > General**. Select **Activate USB storage service** if you want to use the connected USB device(s).

Set a number and select a unit (MB or %) to have the ZyWALL/USG send a warning message when the remaining USB storage space is less than the value you set here.

CONFIGURATION > System > USB Storage > Settings > General

General

☒ Activate USB storage service

Disk full warning when remaining space is less than:

MB

MB

%

Set Up the USB Log Storage

Go to **CONFIGURATION > Log & Report > Log Settings**, select **USB Storage** and click **Activate**. Click **Apply** to save your changes.

CONFIGURATION > Log & Report > Log Settings

Log Settings

Icon	Name	Log Format	Summary
1	System Log	Internal	Email Server 1 Mail Server: mail.zyxel.com.tw Mail Subject: handbook test Send From: Chris.Liao@zyxel.com.tw Send Log to: Chris.Liao@zyxel.com.tw Send Alert to: Schedule: Send log daily at 10:00
2	System Log	Internal	Email Server 2 Mail Server: Mail Subject: Send From: Send Log to: Send Alert to: Schedule: Send log when full.
3	USB Storage	Internal	USB Status: Ready
4	Remote Server 1	VRPT/Syslog	Server Address: Log Facility: Local 1
5	Remote Server 2	VRPT/Syslog	Server Address: Log Facility: Local 1
6	Remote Server 3	VRPT/Syslog	Server Address: Log Facility: Local 1
7	Remote Server 4	VRPT/Syslog	Server Address: Log Facility: Local 1

Page 1 of 1 Show 50 items Displaying 1 - 7 of 7

Go to **CONFIGURATION > Log & Report > Log Settings > USB Storage > Edit**. Select **Duplicate logs to USB storage (if ready)** to have the ZyWALL/USG save a copy of its system logs to a connected USB storage device. Use the **Selection** drop-down list to change the log settings for all of the log categories.

CONFIGURATION > Log & Report > Log Settings

USB Storage
☒ Duplicate logs to USB storage (if ready) ⓘ

Log Keep duration

☐ Enable log keep duration

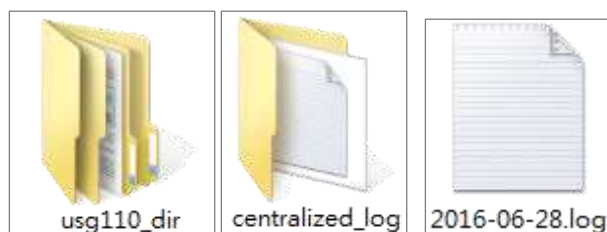
 Keep duration: (1-365 days)

Active Log

Log Category +	disable	normal	debug
<input checked="" type="checkbox"/> Auth	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> BWM	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Device HA	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> File manager	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> License	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Log & Report	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Network	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> None	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Routing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> System	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> UTM	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> VPN	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
<input checked="" type="checkbox"/> Wireless	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

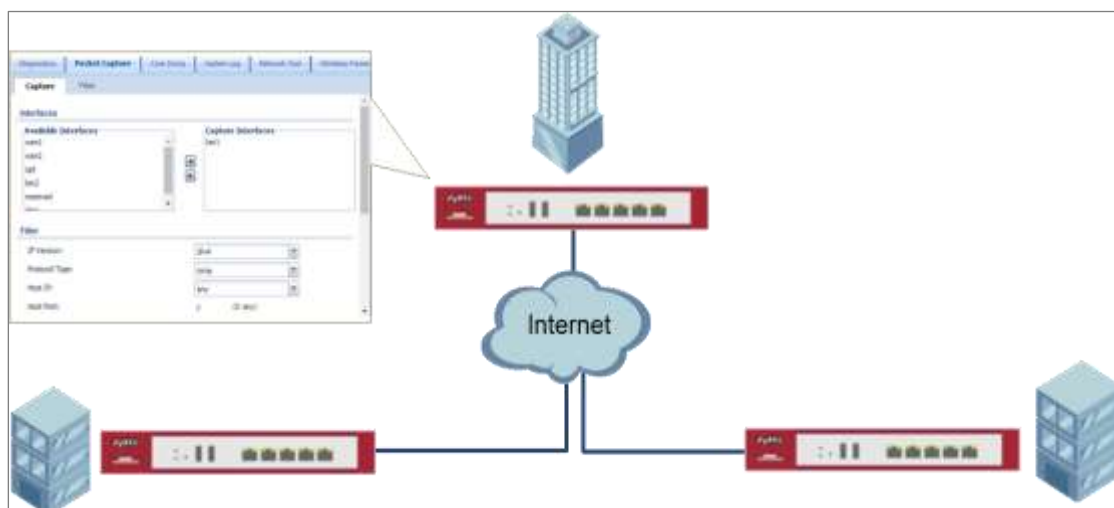
Check the USG Log Files

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 setting**.
Select **Continuously capture and overwrite old ones** to have the ZyWALL/USG keep capturing traffic and overwriting old packet capture entries when the available storage space runs out. Select **Save data to onboard storage only** or **Save data to USB storage** (If status shows service deactivated, go to **CONFIGURATION > Object > USB Storage**, select Activate USB storage service)

Misc setting

☒ Continuously capture and overwrite old ones

☒ Save data to onboard storage only (available: 65 MB)

☐ Save data to USB storage (available: 895 MB)

Captured Packet Files: MB

Split threshold: MB

Duration: (0: unlimited)

File Suffix:

Number Of Bytes To Capture (Per Packet): Bytes

- 10 Click **Capture**.

Interfaces

Available Interfaces

- wan2
- opt
- lan2
- reserved
- dmz
- wan1-eth

Capture Interfaces

- lan1
- wan1

Filter

IP Version:

Protocol Type:

Host IP:

Host Port: (0: any)

Misc setting

☐ Continuously capture and overwrite old ones

☒ Save data to onboard storage only (available: 65 MB)

Capture **Stop** **Reset**

- 11 Click **Stop** when collection is done.

Interfaces

Available Interfaces

- wan2
- opt
- lan2
- reserved
- dmz
- wan1

Capture Interfaces

- lan1
- wan1

Filter

IP Version: IPv4
Protocol Type: icmp
Host IP: any
Host Port: 0 (0: any)

Misc setting

☐ Continuously capture and overwrite old ones
☒ Save data to onboard storage only (available: 65 MB)

Capture Stop Reset



Check the Capture Files

- Go to **MAINTENANCE > Diagnostics > Packet Capture > Files**, select the .cap file and click **Download**.






Capture

Files

Captured Packet Files

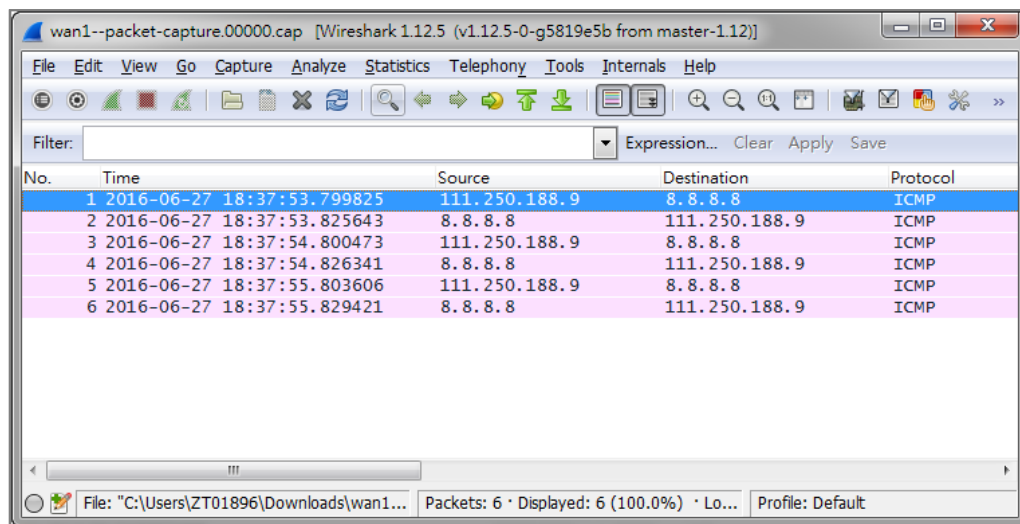
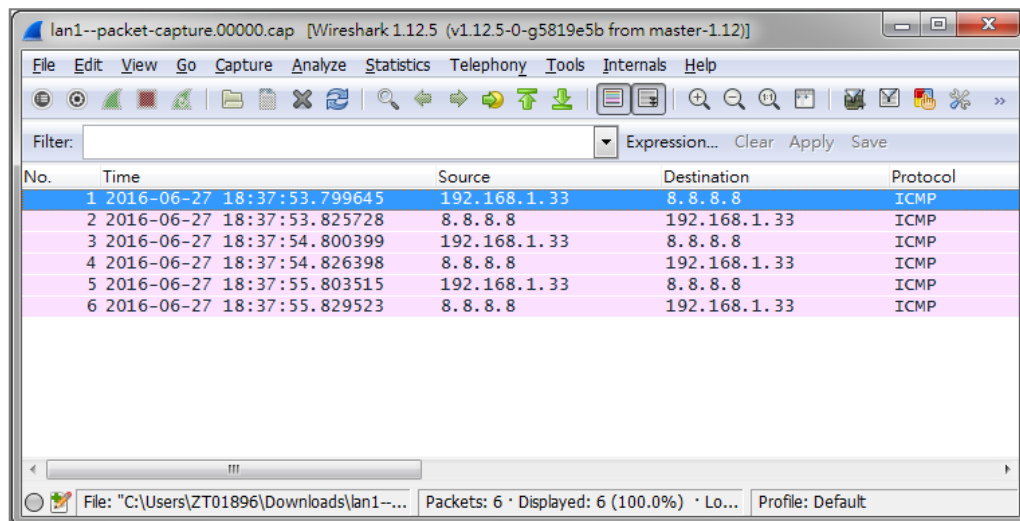
 Remove  Download

#	File Name	Size	Last Modified
1	lan1--packet-capture.00000.cap	924	2016-06-27 18:28:17
2	lan1--packet-capture.txt	78	2016-06-27 18:28:17
3	wan1--packet-capture.00000.cap	24	2016-06-27 18:28:17
4	wan1--packet-capture.txt	76	2016-06-27 18:28:17

  Page of   Show  items

Displaying 1 - 4 of 4

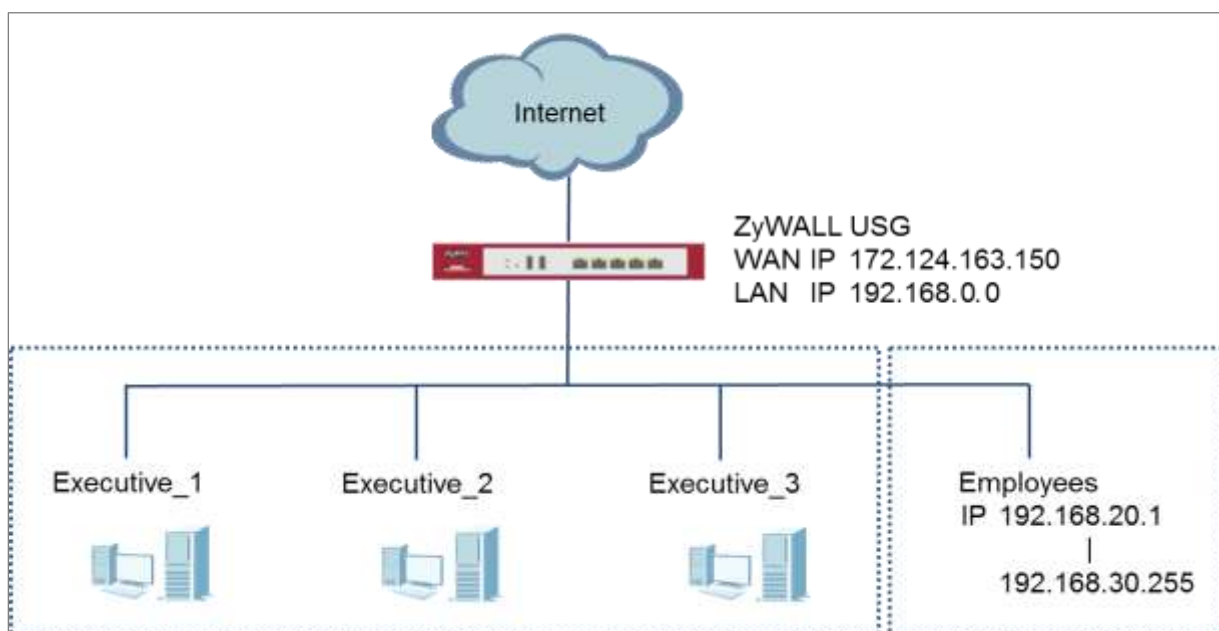
13 Open .cap files with Wireshark




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

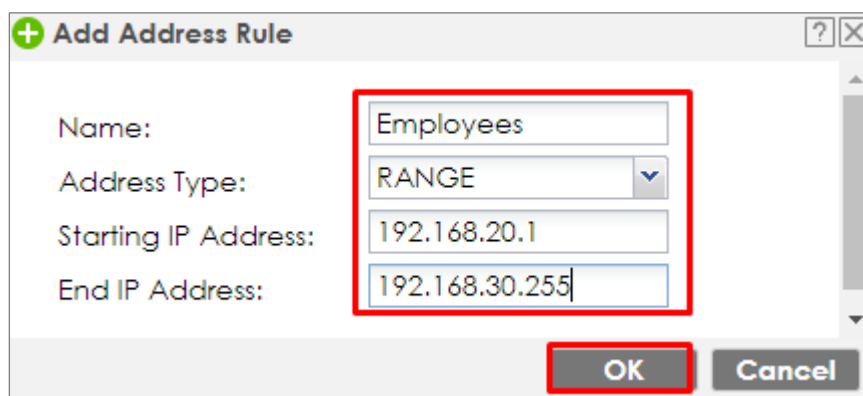


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

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

<input checked="" type="checkbox"/> Enable		
Name:	Employees_Security	
Description:		(Optional)
From:	LAN	
To:	any (Excluding ZyV	
Source:	Employees	
Destination:	any	
Service:	any	
User:	any	
Schedule:	none	
Action:	allow	
Log matched traffic:	log	

UTM Profile		
<input checked="" type="checkbox"/> Content Filter:	Office_profile	Log: by profile
<input type="checkbox"/> SSL Inspection:	none	Log: by profile

Set Up the Security Policy on the ZyWALL/USG for Executives

In the ZyWALL/USG, go to **CONFIGURATION > Object > User/Group > Add A User**

to create **User Name/Password** for each executive.

CONFIGURATION > Object > User/Group > Add A User

User Configuration	
User Name :	Executive_1
User Type:	user
Password:	****
Retype:	****
Description:	Local User

User Configuration	
User Name :	Executive_2
User Type:	user
Password:	****
Retype:	****
Description:	Local User

User Configuration	
User Name :	Executive_3
User Type:	user
Password:	****
Retype:	****
Description:	Local User

Then, go to **CONFIGURATION > Object > User/Group > Group > Add Group** to create a **Group Members' Name** and move the just created executives user object to **Member**.

CONFIGURATION > Object > Address Group > Add Address Group Rule

Configuration

Name:

Description: (Optional)

Member List

Available		Member
=== Object ===		
Executive_1	+	
Executive_2		
Executive_3	+	
ad-users		
ldap-users		
radius-users		

Set up **Security Policy** for executives, go to **CONFIGURATION > Security Policy > Policy Control > Add corresponding**, configure a **Name** for you to identify the executives' **Security Policy** profile.

For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select **User** to be the **Executives** to apply the policy to all traffic coming from them.

In order to view the test result later on, set **Log matched traffic** to be **log**.

Leave all **UTM Profiles** disabled.

CONFIGURATION > Security Policy > Policy Control > Add corresponding > Employees_Security

☒ Enable

Name: Executive_Security

Description: (Optional)

From: LAN

To: any (Excluding ZyV

Source: any

Destination: any

Service: any

User: Executive

Schedule: none

Action: allow

Log matched traffic: log

[UTM Profile](#)

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	59.124.193.66:443	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	59.124.193.150	Account: Executive_1

Priority	Category	Message	Source	Destination	Note
notice	Security Policy Control	priority:2, from LAN to ANY, TCP, service others, ACCEPT	192.168.30.9:50926	74.125.23.189:443	ACCESS FORWARD
info	Application Patrol	Rule_id=2 SSI=N App=[Social Network]Google-plus:authority Action=reject SID=402652097	192.168.30.9:50926	74.125.23.113:443	ACCESS BLOCK
info	Application Patrol	Rule_id=2 SSI=N App=[Social Network]Facebook:authority Action=reject SID=402653953	192.168.30.9:51041	66.220.158.19:443	ACCESS BLOCK

What Could Go Wrong?

If you are not be able to configure any **UTM** policies or it's not working, there are two possible reasons:

You have not subscribed for the **UTM** service.

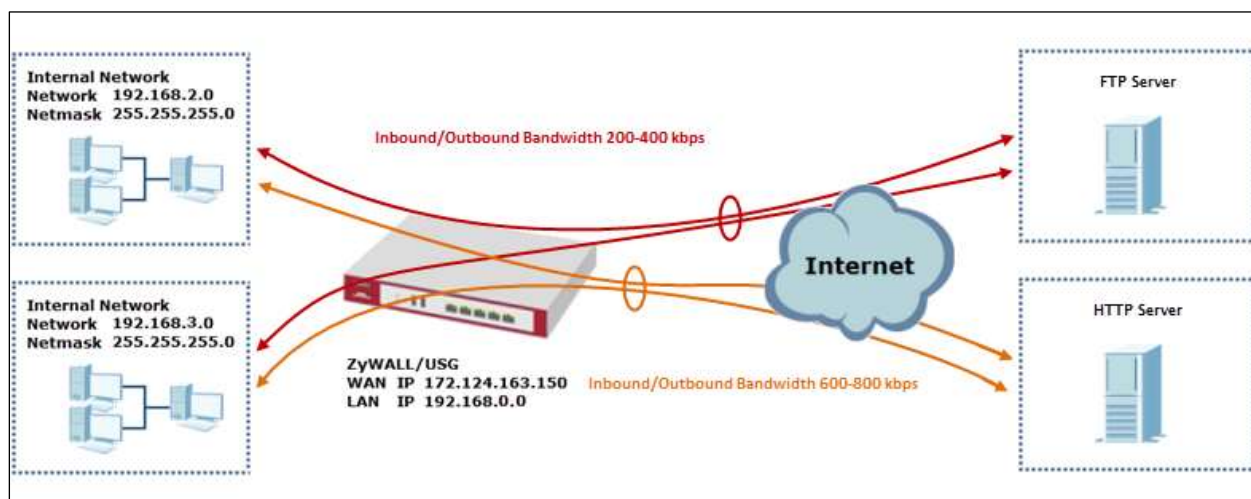
You have subscribed for the **UTM** service but the license is expired.


You can click the link from the **CONFIGURATION > Licensing > Registration** screen of your ZyXEL device's Web Configurator or click the myZyXEL.com 2.0 icon from the portal page (<https://portal.myzyxel.com/>) to register or extend your **UTM** license.

How to Configure Bandwidth Management for FTP and HTTP Traffic

This is an example of using ZyWALL/USG Bandwidth Management (BWM) to control the bandwidth allocation for FTP and HTTP traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions to allocate bandwidth for the matching packets. When the BWM is configured, you can limit bandwidth consuming services, such as FTP, while providing consistent HTTP service with bandwidth guarantees.

ZyWALL/USG with Bandwidth Management for HTTP and FTP Traffic Example



 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. The total available bandwidth assumption is 1,600 kbps. This example was tested using USG310

Set Up the Bandwidth Management for FTP on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **FTP Any-to-WAN** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **wan1**. Select **Service Type** to be the **Service Object** and select **FTP** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 200 (kbps) and set **Priority 5** (low-to-medium). Set the **Maximum** to 400 (kbps). Set the **Guaranteed Bandwidth Outbound** to 200 (kbps) and set **Priority 5**. Set the **Maximum** to 400 (kbps).

In order to view the result later, set the **Log** setting to be **log alert**. Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy

Configuration

☒ Enable
 Description: FTP Any-to-WAN (Optional)
 BWM Type: ☒ Shared ☐ Per user ☐ Per-Source-IP

Criteria

User: any
 Schedule: none
 Incoming Interface: any
 Outgoing Interface: ge1
 Source: any
 Destination: any
 DSCP Code: any
 Service Type: service-object
 Service Object: FTP

DSCP Marking

DSCP Marking
 Inbound Marking: preserve
 Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth	Inbound: 200 kbps (0 : disabled)	Priority: 5
	<input type="checkbox"/> Maximize Bandwidth Usage	Maximum 400 kbps
	Outbound: 200 kbps (0 : disabled)	Priority: 5
	<input type="checkbox"/> Maximize Bandwidth Usage	Maximum 400 kbps

802.1P Marking

Priority Code: 0 (0-7)
 Interface: none

Related Setting

Log: log alert



Note: In Bandwidth Management, the highest priority is (1) the lowest priority is (7).

Set Up the Bandwidth Management for HTTP on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **HTTP Any-to-WAN** as the policy's Description (Optional).

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **wan1**. Select **Service Type** to be the **Service Object** and select **HTTP** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 600 (kbps) and set higher **Priority 3**. Set the **Maximum** to 800 (kbps). Set the **Guaranteed Bandwidth Outbound Priority 3**.

In order to view the result later, set the **Log** setting to be **log alert**. Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy

Configuration

☒ Enable

Description: HTTP Any-to-WAN (Optional)

BWM Type: ☒ Shared ☐ Per user ☐ Per-Source-IP ⓘ

Criteria

User: any

Schedule: none

Incoming Interface: any

Outgoing Interface: ge1

Source: any

Destination: any

DSCP Code: any

Service Type: service-object

Service Object: HTTP

DSCP Marking

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth

Inbound: 600 kbps (0 : disabled)

☐ Maximize Bandwidth Usage

Priority: 3

Maximum: 800 kbps

Outbound: 600 kbps (0 : disabled)

☐ Maximize Bandwidth Usage

Priority: 3

Maximum: 800 kbps

802.1P Marking

Priority Code 0 (0-7)

Interface none ⓘ

Related Setting

Log: log alert



Note: In Bandwidth Management, the highest priority is (1) the lowest priority is (7).

Set Up the Bandwidth Management Global Setting on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > BWM Global Setting**, select **Enable**.

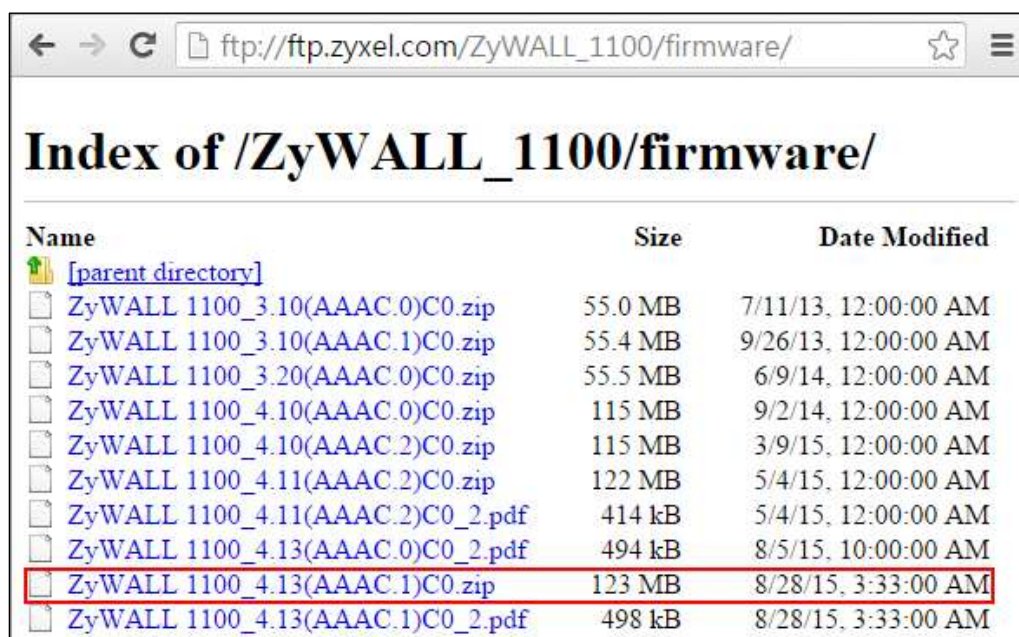
CONFIGURATION > BWM > BWM Global Setting

BWM Global Setting

☒ Enable BWM

Test the Result

Access the Internet to generate FTP traffic and HTTP traffic. In this example, a 123 MB file is downloading from an FTP server. The FTP file should download slowly.



Name	Size	Date Modified
[parent directory]		
ZyWALL 1100_3.10(AAAC.0)C0.zip	55.0 MB	7/11/13, 12:00:00 AM
ZyWALL 1100_3.10(AAAC.1)C0.zip	55.4 MB	9/26/13, 12:00:00 AM
ZyWALL 1100_3.20(AAAC.0)C0.zip	55.5 MB	6/9/14, 12:00:00 AM
ZyWALL 1100_4.10(AAAC.0)C0.zip	115 MB	9/2/14, 12:00:00 AM
ZyWALL 1100_4.10(AAAC.2)C0.zip	115 MB	3/9/15, 12:00:00 AM
ZyWALL 1100_4.11(AAAC.2)C0.zip	122 MB	5/4/15, 12:00:00 AM
ZyWALL 1100_4.11(AAAC.2)C0_2.pdf	414 kB	5/4/15, 12:00:00 AM
ZyWALL 1100_4.13(AAAC.0)C0_2.pdf	494 kB	8/5/15, 10:00:00 AM
ZyWALL 1100_4.13(AAAC.1)C0.zip	123 MB	8/28/15, 3:33:00 AM
ZyWALL 1100_4.13(AAAC.1)C0_2.pdf	498 kB	8/28/15, 3:33:00 AM

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below.

Monitor > Log

Priority	Category	Message	Source	Destination
alert	BWM	Mode=port-base Rule=2 matched	192.168.1.33:51495	216.241.54.88:54190
alert	BWM	Mode=port-base Rule=2 matched	192.168.1.33:51494	216.241.54.88:21
alert	BWM	Mode=port-base Rule=2 matched	192.168.1.33:51493	216.241.54.88:13700
alert	BWM	Mode=port-base Rule=2 matched	192.168.1.33:51492	216.241.54.88:21

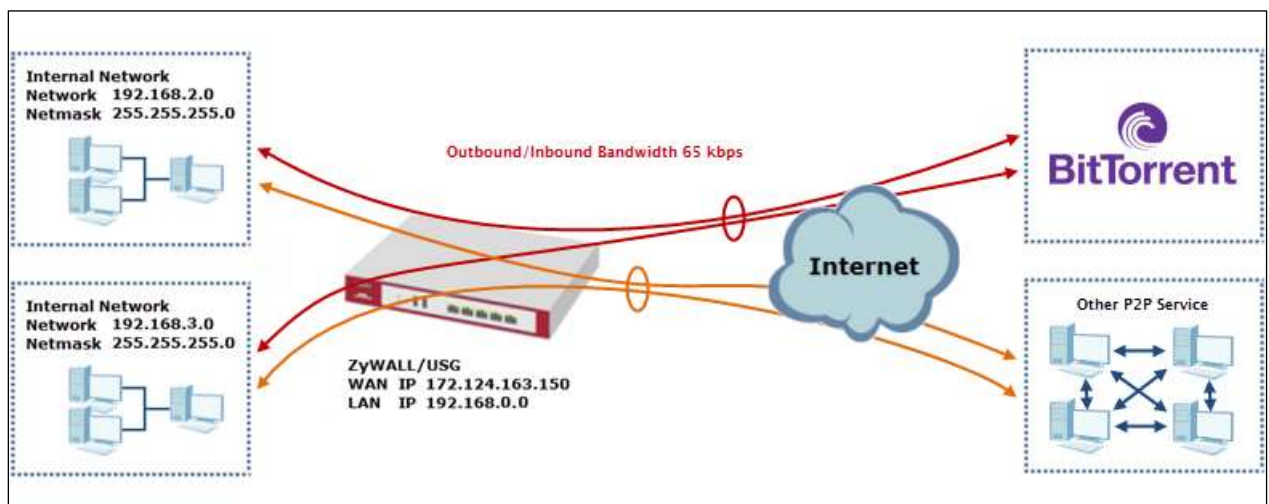
What Could Go Wrong?


If the "outbound" in the guaranteed bandwidth settings apply to traffic going from the connection initiator to the outgoing interface. "Inbound" refers to the reverse direction.

How to Limit BitTorrent or Other Peer-to-Peer Traffic

This is an example of using ZyWALL/USG Bandwidth Management (BWM) to control the bandwidth allocation for peer-to-peer traffic. You can use source interface, destination interface, destination port, schedule, user, source, destination information, DSCP code and service type as criteria to create a sequence of specific conditions to allocate bandwidth for the matching packets. When the BWM is configured, you can limit bandwidth consuming Application traffic, such as Peer-to-Peer (P2P) service.

ZyWALL/USG with Bandwidth Management for Peer-to-Peer Traffic Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. The total available bandwidth assumption is 1,600 kbps. This example was tested using USG310

Set Up the Application Patrol Profile on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Object > Application > Add Application Rule**. Configure a **Name** for you to identify the **Application Profile**. Then, click **Add** to create an **Application Object**.

CONFIGURATION > Object > Application > Add Application Rule

Name:

Description: (Optional)

☒ Add ☐ Remove

#	Category	Application
No data to display		

Page 1 of 1 | Show 50 items

In the **Application Object**, select **By Service**, type a keyword and click **Search** to display all signatures containing that keyword. Select all **Query Result** and Click **OK**.

CONFIGURATION > Object > Application > Add Application Rule > Add Application Object

Query

Search:

Query Result

#	<input checked="" type="checkbox"/>	Category	Application
1	<input checked="" type="checkbox"/>	P2P	BitTorrent Series (transfer)
2	<input checked="" type="checkbox"/>	P2P	BitTorrent Series (access)
3	<input checked="" type="checkbox"/>	P2P	BitTorrent Series (connect)

Page 1 of 1 | Show 50 items | Displaying 1 - 3 of 3

Set Up the Bandwidth Management for BitTorrent on the ZyWALL/USG


In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **BitTorrent Any-to-Any** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **wan1**. Select **Service Type** to be the **Service Object** and select **BitTorrent** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 65 (kbps) and set **Priority 5** (low-to-medium). Set the **Maximum** to 512(kbps). Set the **Guaranteed Bandwidth Outbound** to 65 (kbps) and set **Priority 5**. Set the **Maximum** to 512 (kbps). Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy

Configuration

☒ Enable
 Description: BitTorrent Any-to-Any (Optional)
 BWM Type:
 ☒ Shared
 ☐ Per user
 ☐ Per-Source-IP
 

Criteria

User: any
 Schedule: none
 Incoming Interface: any
 Outgoing Interface: any
 Source: any
 Destination: any
 DSCP Code: any
 Service Type:
 ☐ Service Object
 ☒ Application Object
 Application Object: BitTorrent

DSCP Marking

DSCP Marking
 Inbound Marking: preserve
 Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth	Inbound:	65	kbps (0 : disabled)	Priority:	5	
	<input type="checkbox"/> Maximize Bandwidth Usage			Maximum:	512	kbps
	Outbound:	65	kbps (0 : disabled)	Priority:	5	
	<input type="checkbox"/> Maximize Bandwidth Usage			Maximum:	512	kbps

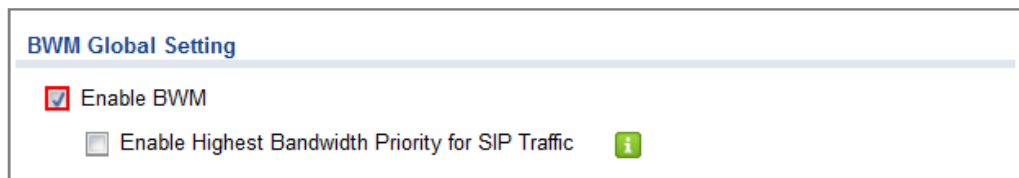


Note: In Bandwidth Management, the highest priority is (1) the lowest priority is (7).

Set Up the Bandwidth Management Global Setting on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > BWM Global Setting**, select **Enable**.

CONFIGURATION > BWM > BWM Global Setting

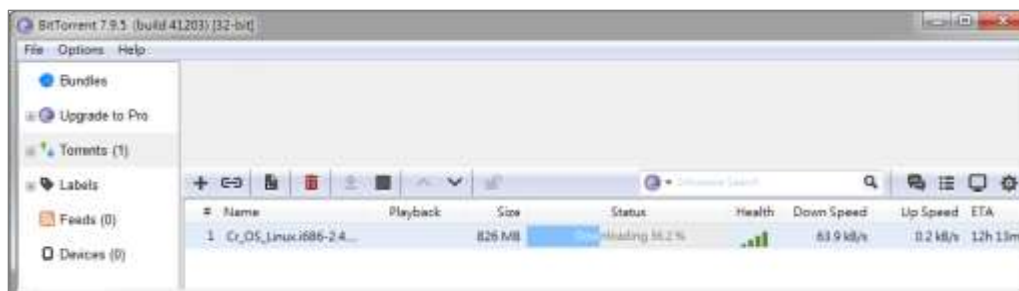


Test the Result

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.

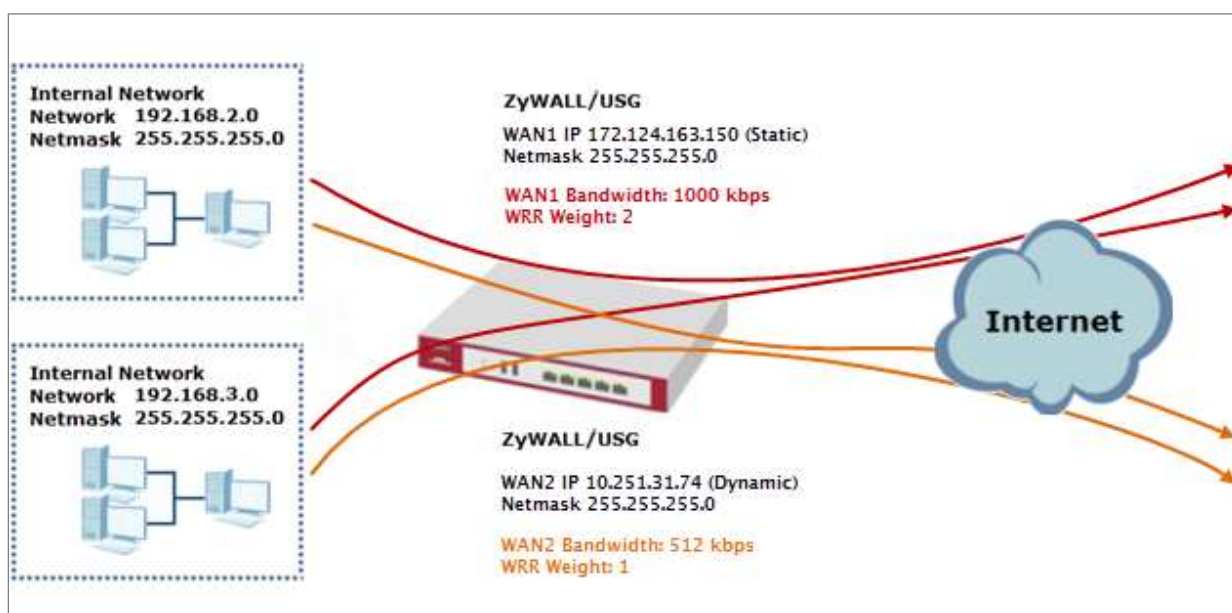
Service Type:	<input type="radio"/> Service Object <input checked="" type="radio"/> Application Object
Application Object:	<div>BitTorrent</div>


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

The screenshot displays the configuration page for the WAN1 interface. The 'General Settings' section includes 'Enable Interface' (checked). The 'Interface Properties' section shows 'Interface Type' as 'external', 'Interface Name' as 'WAN1', 'Port' as 'P1', 'Zone' as 'WAN', and 'MAC Address' as '88:EC:A3:A9:C0:0B'. The 'IP Address Assignment' section has 'Get Automatically' selected, but 'Use Fixed IP Address' is also shown with a red box around its radio button. Below it, 'IP Address' is '172.124.163.150' and 'Subnet Mask' is '255.255.255.0', both highlighted with red boxes. The 'Interface Parameters' section at the bottom shows 'Egress Bandwidth' set to '1000' Kbps, also highlighted with a red box.

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

#	Member	Mode	Weight
1	WAN1	Active	2
2	WAN2	Active	1

In the **Configuration** screen, go to **Default WAN Trunk** section, select **User Configured Trunk** and select the newly created Trunk from the list box. Click **Apply**.

CONFIGURATION > Interface > Trunk > Default WAN Trunk

Default WAN Trunk

☐ Advance

Default Trunk Selection

☐ SYSTEM_DEFAULT_WAN_TRUNK
 ☒ User Configured Trunk

WAN1_WAN2_Load

Test the Result

Browse any website to test the result.

The Weighted Round Robin (WRR) algorithm is best suited for situations where the bandwidths set for the two WAN interfaces are different. An interface with a larger weight (**WAN1**) gets more chances to transmit traffic than an interface with a smaller weight (**WAN2**).

MONITOR > Interface Summary > Interface Statistics

Interface Statistics					
Refresh					
Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s
+ ge1	Down	0	0	0	0
+ WAN1	1000M/Full	16501	47815	0	634
+ WAN2	1000M/Full	268	169	0	0

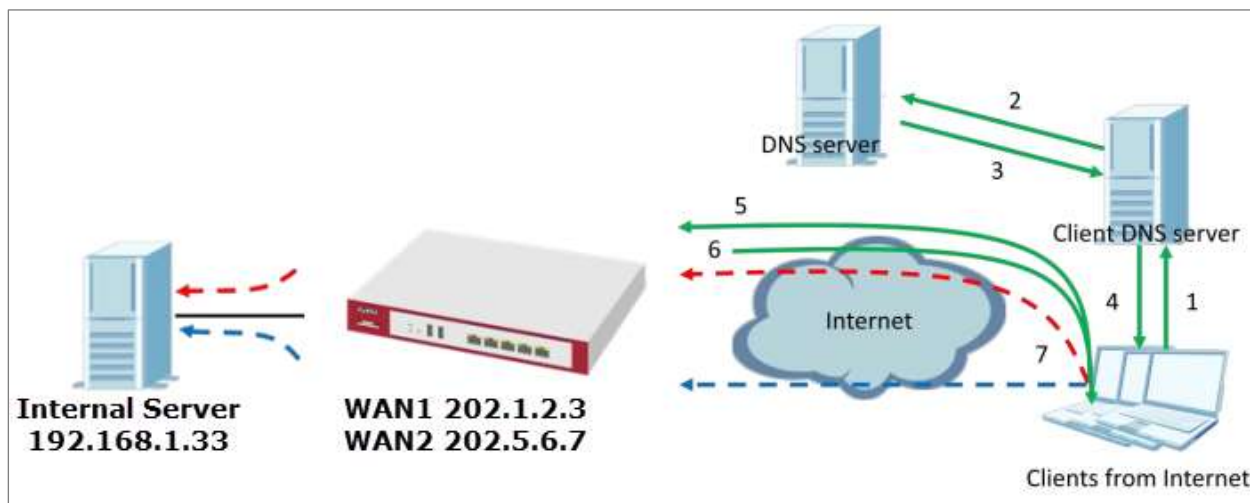
What Could Go Wrong?


If there is no traffic passing through either WAN1 or WAN2 interfaces, check that the **Mode** of both WAN1 & WAN2 should be **Active**. If a trunk is in **Passive** mode, the ZyWALL/USG will use this connection only when all of the connections set to **Active** mode are down.

How to Configure DNS Inbound Load Balancing to balance DNS Queries Among Interfaces

This is an example of using the ZyWALL/USG dynamically responding to DNS query messages with its least loaded interface's IP address. The DNS query senders will then transmit packets to that interface instead of an interface that has a heavy load. This example assumes that your company's domain name is `www.example.com`. You want your ZyWALL/USG's WAN1 (202.1.2.3) and WAN2 (202.5.6.7) to use DNS inbound load balancing to balance traffic loading coming from the Internet.

ZyWALL/USG with DNS Inbound Load Balancing Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the DNS Inbound Load Balancing on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > DNS Inbound LB**. Edit the **Query Domain Name**, set the **Load Balancing Algorithm** field to be the **Least Load - Total**. Click **Add** to create a new **Load Balancing Member**.

CONFIGURATION > Network > DNS Inbound LB

General Setting

☐ Enable

DNS Settings

Query Domain Name: zyxel.for-our.info

Time to Live: (0-604800 seconds, 0 is unchanged)

Query From Settings

IP Address:

Zone:

Load Balancing Member

Load Balancing Algorithm: Least Load - Total

Failover IP Address: (Optional)

+ Add ✎ Edit ✖ Remove

#	IP Address	Monitor Interface
No data to display		

If you want to configure Security Option Control, please go to [DNS](#) ⓘ

CONFIGURATION > Network > DNS Inbound LB

Add Load Balancing Member

Load Balancing Member

Member: 1

Monitor Interface: WANT DHCP client -- 202.1.2.3/255.255.255.0

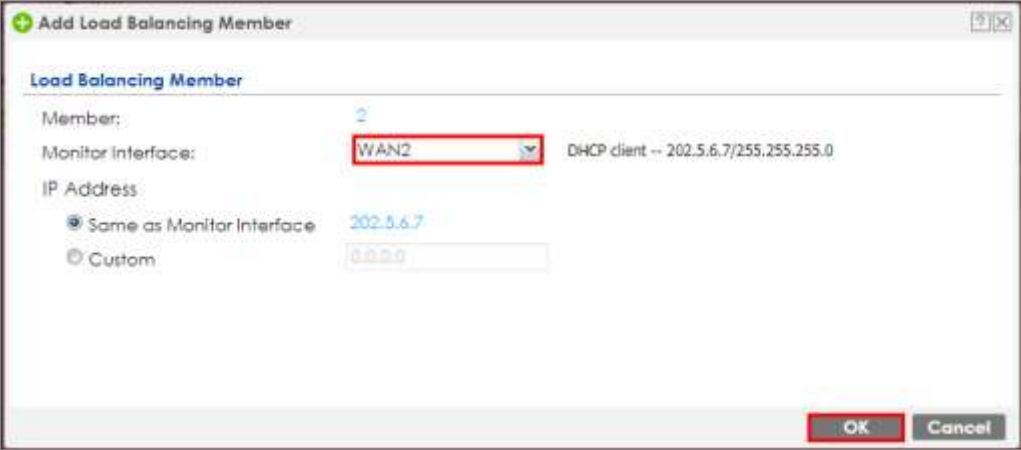
IP Address

☒ Same as Monitor Interface 202.1.2.3

☐ Custom

OK Cancel

CONFIGURATION > Network > DNS Inbound LB



Add Load Balancing Member

Load Balancing Member

Member: 2

Monitor Interface: WAN2 DHCP client -- 202.5.6.7/255.255.255.0

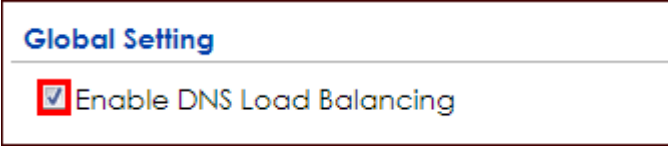
IP Address:

- ☒ Same as Monitor Interface 202.5.6.7
- ☐ Custom 0.0.0.0

OK **Cancel**

Go to the **Global Setting** page to select **Enable DNS Load Balancing**.

CONFIGURATION > Network > DNS Inbound LB



Global Setting

☒ **Enable DNS Load Balancing**

Set Up the NAT Rule on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > NAT**. Configure the **Virtual Server** to forward the traffic from WAN to Internal Server (192.168.1.33). Click **OK**.

CONFIGURATION > Network > NAT

General Settings	
<input checked="" type="checkbox"/> Enable Rule	
Rule Name:	NAT_WAN1
Port Mapping Type	
Classification:	<input checked="" type="radio"/> Virtual Server <input type="radio"/> 1:1 NAT <input type="radio"/> Many 1:1 NAT
Mapping Rule	
Incoming Interface:	WAN1
Original IP:	User Defined
User-Defined Original IP:	202.1.2.3 (IP Address)
Mapped IP:	User Defined
User-Defined Mapped IP:	192.168.1.33 (IP Address)
Port Mapping Type:	Port
Protocol Type:	any
Original Port:	80
Mapped Port:	80

General Settings	
<input checked="" type="checkbox"/> Enable Rule	
Rule Name:	NAT_WAN2
Port Mapping Type	
Classification:	<input checked="" type="radio"/> Virtual Server <input type="radio"/> 1:1 NAT <input type="radio"/> Many 1:1 NAT
Mapping Rule	
Incoming Interface:	WAN2
Original IP:	User Defined
User-Defined Original IP:	202.5.6.7 (IP Address)
Mapped IP:	User Defined
User-Defined Mapped IP:	192.168.1.33 (IP Address)
Port Mapping Type:	Port
Protocol Type:	any
Original Port:	80
Mapped Port:	80

Test the Result

Open the browser and query <http://zyxel.for-our.info/>.

Create a **Security Policy** in order to view the testing result. Set **Destination** to be

the Internal Server IP address (192.168.1.33 in this example) and set **Log** type to be the **Log Alert**.

Go to the ZyWALL/USG **Monitor > Log**, you will see [alert] log message such as below. The **Source Interface** is the WAN1 or WAN2 interface which is handling the least amount of outgoing and incoming traffic.

Prior...	Category	Message	Source	Source I...	Destination	Note
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52268	WAN2	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52267	WAN2	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52266	WAN1	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52265	WAN1	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52260	WAN1	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52259	WAN1	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52258	WAN2	192.168.1.33:80	ACCESS FORWA...
alert	Security Policy ...	priority:1, from ANY to ANY, TCP, service oth...	202.1.2.4:52257	WAN2	192.168.1.33:80	ACCESS FORWA...

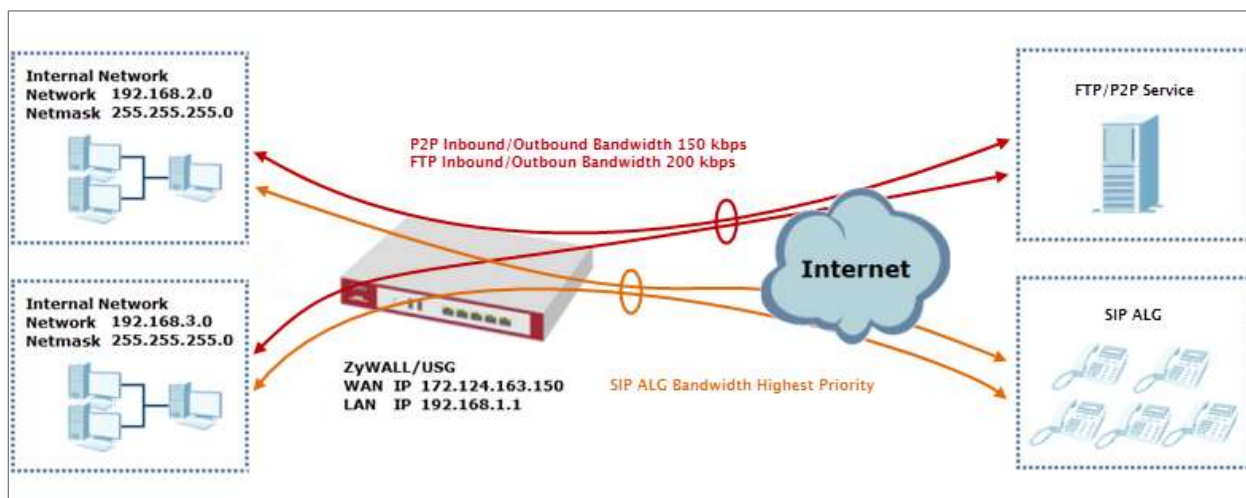
What Could Go Wrong?


If you cannot access the Internal Server, please check that the NAT configuration matches the Internal Server IP address and Port number. If the NAT configuration is correct, please check the system status of your Internal Server is up.

How to Manage Voice Traffic

This is an example of using Application Layer Gateway (ALG) to allow the SIP (Session Initiation Protocol) voice traffic through the ZyWALL/USG. To achieve high-quality voice transmissions, use ZyWALL/USG provides Bandwidth Management (BWM) function to effectively manage bandwidth according to flexible criteria. You can limit bandwidth consuming services, such as Peer-to-Peer (P2P) and FTP service while providing a higher priority and consistent bandwidth for voice traffic.

ZyWALL/USG with Voice Traffic Management Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the SIP ALG on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > SIP > SIP Settings**, select **Enable SIP ALG**, **Enable SIP Transformations** (optional), **Restrict Peer to Peer Signaling Connection** and **Restrict Peer to Peer Media Connection**. Make sure the **SIP Signaling Port** is configured the same as your VoIP phone SIP signaling port. Click **Apply**.

CONFIGURATION > BWM > Configuration > Add Policy

SIP Settings

☒ Enable SIP ALG

☒ Enable SIP Transformations

☒ Enable Configure SIP Inactivity Timeout

SIP Media Inactivity Timeout : (seconds)
 SIP Signaling Inactivity Timeout : (seconds)

☒ Restrict Peer to Peer Signaling Connection
 ☒ Restrict Peer to Peer Media Connection ⓘ

SIP Signaling Port :

+ Add
 Edit
 Remove

#	Port ▲
1	5060

 Note: If you are using a custom or additional UDP port number (not 5060) for SIP traffic, use the **Add** icon to add **SIP Signaling Port** numbers.

Set Up the Bandwidth Management for SIP on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > BWM Global Settings**, select **Enable BWM** and **Enable Highest Bandwidth Priority for SIP Traffic**.

CONFIGURATION > BWM > BWM Global Settings > Enable BWM

BWM Global Setting

☒ Enable BWM

☒ Enable Highest Bandwidth Priority for SIP Traffic ⓘ

Set Up the Bandwidth Management for P2P on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **P2P Any-to-WAN** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **WAN1**. Select **Service Type** to be the **Application Object** and select **P2P** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 100 (kbps) and set **Priority** 5. Set the **Maximum** to 150 (kbps). Set the **Guaranteed Bandwidth Outbound** to 100 (kbps) and set **Priority** 5. Set the **Maximum** to 150 (kbps). Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy

Configuration

☒ Enable

Description: P2P Any-to-WAN (Optional)

BWM Type: ☒ Shared ☐ Per user ☐ Per-Source-IP

Criteria

User: any

Schedule: none

Incoming Interface: any

Outgoing Interface: WAN1

Source: any

Destination: any

DSCP Code: any

Service Type: ☐ Service Object ☒ Application Object

Application Object: P2P

DSCP Marking

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth	Inbound:	100	kbps (0 : disabled)	Priority:	5
	<input type="checkbox"/> Maximize Bandwidth Usage			Maximum:	150 kbps
	Outbound:	100	kbps (0 : disabled)	Priority:	5
	<input type="checkbox"/> Maximize Bandwidth Usage			Maximum:	150 kbps



Note: In Bandwidth Shaping, the highest priority is (1) the lowest priority is (7).

Set Up the Bandwidth Management for FTP on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > BWM > Configuration > Add Policy**, select **Enable** and type **FTP Any-to-Any** as the policy's **Description**.

Leave the **Incoming Interface** to **any** and select the Outgoing Interface to be **WAN1**. Select **Service Type** to be the **Service Object** and select **FTP** from the list box.

Set the **Guaranteed Bandwidth Inbound** to 150 (kbps) and set **Priority** 5. Set the **Maximum** to 200 (kbps). Set the **Guaranteed Bandwidth Outbound** to 150 (kbps) and set **Priority** 5. Set the **Maximum** to 200 (kbps). Click **OK** to return to the **General** screen.

CONFIGURATION > BWM > Configuration > Add Policy

Configuration

☒ Enable

Description: FTP Any-to-WAN (Optional)

BWM Type: ☒ Shared ☐ Per user ☐ Per-Source-IP i

Criteria

User: any

Schedule: none

Incoming Interface: any

Outgoing Interface: WAN1

Source: any

Destination: any

DSCP Code: any

Service Type: ☒ Service Object ☐ Application Object

Service Object: FTP

DSCP Marking

DSCP Marking

Inbound Marking: preserve

Outbound Marking: preserve

Bandwidth Shaping

Guaranteed Bandwidth	Inbound:	150	kbps (0 : disabled)	Priority:	5
	<input type="checkbox"/> Maximize Bandwidth Usage			Maximum:	200 kbps
Outbound:	150	kbps (0 : disabled)	Priority:	5	
	<input type="checkbox"/> Maximize Bandwidth Usage			Maximum:	200 kbps



Note: In Bandwidth Shaping, the highest priority is (1) the lowest priority is (7).

Test the Result

Add a **Security Policy** rule to view the SIP log:

CONFIGURATION > BMW > 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	Rate
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.

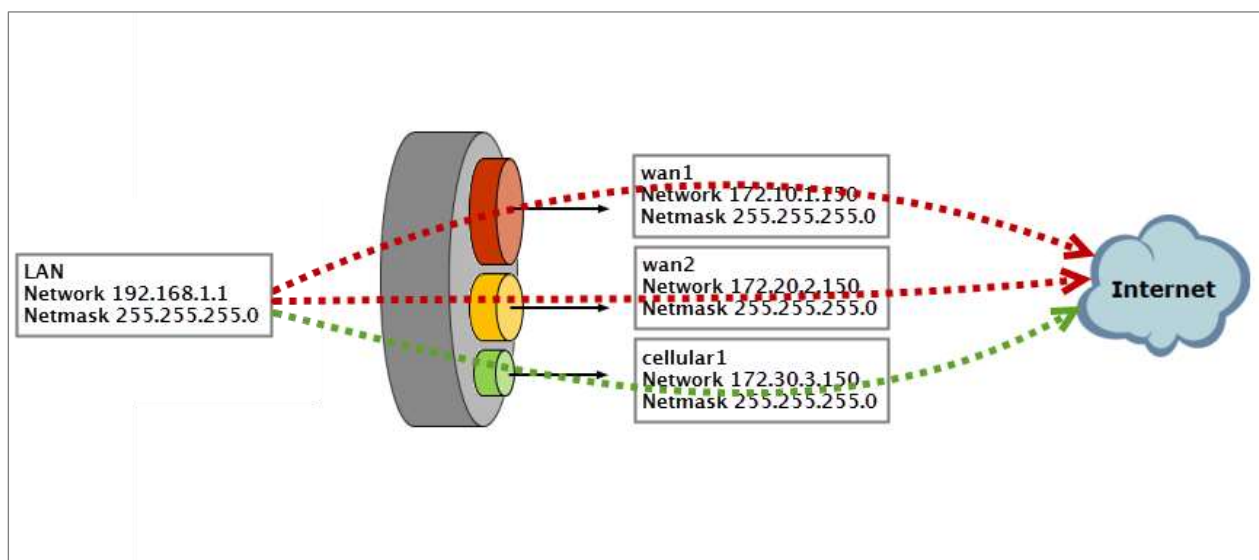
Monitor > Log

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

#	Status	Name	Extension Slot	Connected Device	ISP Settings
1		cellular1	USB 1	Huawei E3131	Device Profile 1

The default **Connectivity** method is **Nailed-Up**. The connection should always be up after you activate the cellular interface. You can click **Edit** and go to the **Connectivity** section to clear the **Nailed-Up** check box to have the ZyWALL/USG to establish the connection only when there is traffic.

CONFIGURATION > Network > Interface > Cellular > Connect

#	Status	Name	Extension Slot	Connected Device	ISP Settings
1		cellular1	USB 1	Huawei E156G	

CONFIGURATION > Network > Interface > Cellular > Edit

Connectivity
<input checked="" type="checkbox"/> Nailed-Up

Set Up the Trunk on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Trunk > User Configuration > Add Trunk**, configure a **Name** for you to identify the Trunk profile and set the **Load Balancing Algorithm** field to be the **Weighted Round Robin**.

Add **wan1** and enter **3** in the **Weight** column. Add **wan2** and enter **2** in the **Weight** column. Add **cellular1**, change **Mode** to be the **Passive** mode, enter **1** in the **Weight** column. Click **OK** to return to the **Configuration** screen.

CONFIGURATION > Network > Interface > Trunk > User Configuration > Add Trunk

Edit WAN_backup

Name: WAN_backup

Load Balancing Algorithm: Weighted Round Robin

#	Member	Mode	Weight
1	ge1	Active	1
2	cellular1	Passive	0
3	ge2	Active	2

Page 1 of 1 Show 50 items Displaying 1 - 3 of 3

In the **Configuration** screen, go to **Default WAN Trunk** section, select **User Configured Trunk** and select the newly created Trunk from the list box. Click **Apply**.

CONFIGURATION > Network > Interface > Trunk > Default WAN Trunk > User Configured Trunk

Default WAN Trunk

Advance

Default Trunk Selection

☐ SYSTEM_DEFAULT_WAN_TRUNK

☒ User Configured Trunk: WAN_Backup

Test the Result

Check the **Interface Statistics** when wan1 and wan2 connections are up. You can see both wan1 and wan2 **Status** are up, **Tx B/s** displays the transmission speed and **Rx B/s** displays the reception speed; cellular1 **Status** is connected but there is no traffic going through this interface.

MONITOR > Interface Status > Interface Statistics

Interface Statistics					
<button>Refresh</button>					
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					
<button>Refresh</button>					
Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s
ge1	Down	0	0	0	0
ge2	1000M/Full	6764	35208	0	0
ge3	Down	1	0	0	0
ge4	Down	2	0	0	0
ge5	Down	1	0	0	0
ge6	Down	2	0	0	0
ge7	Down	1	0	0	0
ge8	Down	1	0	0	0
cellular1	Connected (00:10:34)	164	119	0	0

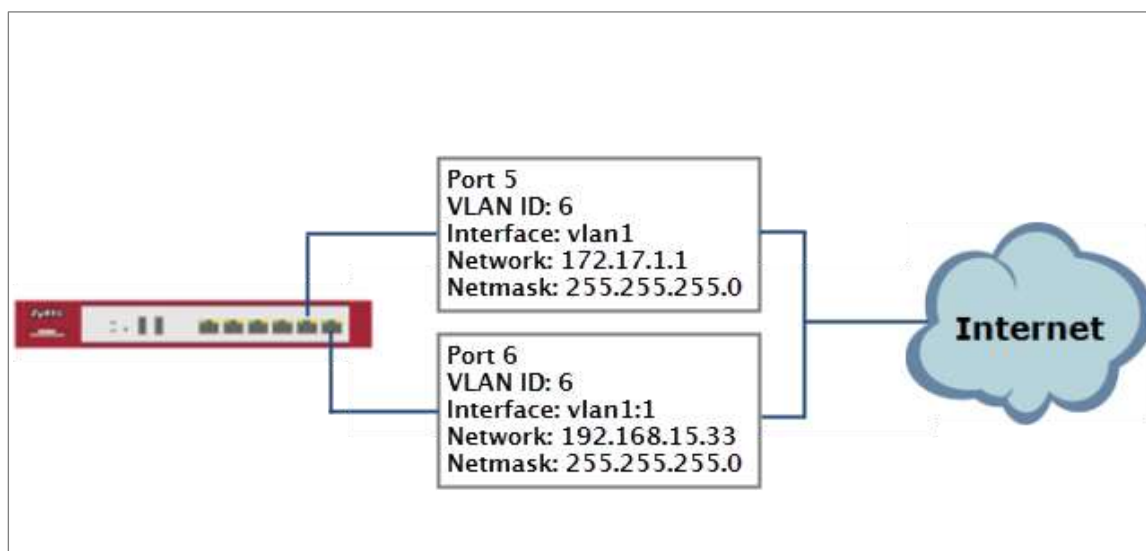
What Could Go Wrong?


If there is no traffic going through cellular interface when other interfaces are down, please make sure you have a compatible mobile broadband device installed or connected. Go to http://www.zyxel.com/support/download_landing.shtml and see the **3G Dongle Document** to check the compatible mobile broadband devices. Also, make sure the cellular interface is enabled and the cellular interface has the correct user name, password, and PIN code configured with the correct casing.

How to Configure Two Different WAN Interfaces with Different IP Addresses in the Same VLAN

This is an example of using ZyWALL/USG to configure two different WAN interfaces with different IP addresses in the same VLAN. After configuration, you can have the same VLAN ID for two different WAN interfaces.

ZyWALL/USG with Two Different WAN Interfaces with Different IP Addresses in the Same VLAN Example

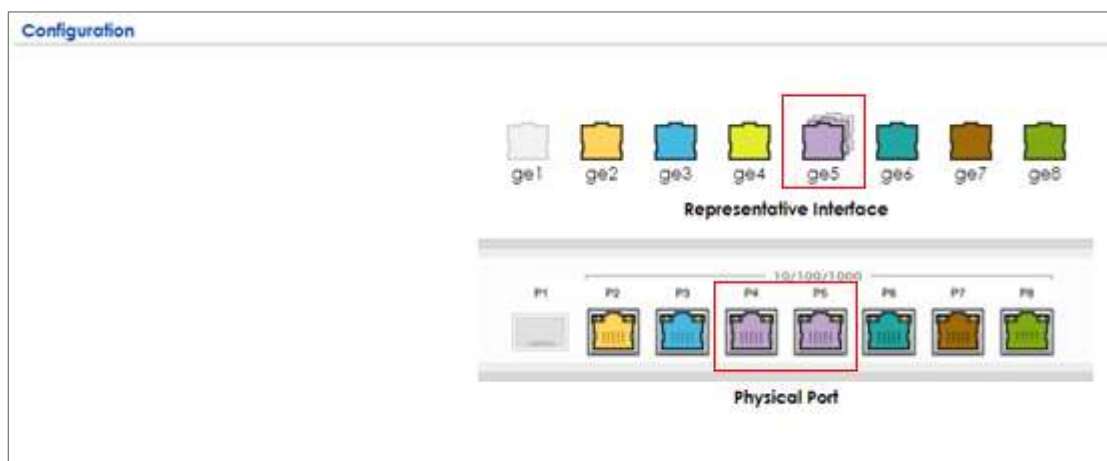


 Note: This example requires the ZyWALL/USG models which can apply port grouping. All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using ZyWALL USG300 (Firmware Version: ZLD 4.25).

Set Up the Port Grouping on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Port Grouping**, select the ports that you want to assign to a representative Interface (in this example, **Port 4** and **Port 5** are configured as **ge5**).

CONFIGURATION > Network > Interface > Port Grouping



Set Up the VLAN on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > VLAN**. Set **Interface Type** to be **External**. Set **Zone** to be **WAN**, configure **Base Port** to be **ge5**. Enter the **VLAN ID** and configure the fixed IP address (172.17.1.1/24 in this example). Click **OK** to go back to the **Configuration** page.

CONFIGURATION > Network > Interface > VLAN

General Settings

☒ Enable Interface

Interface Properties

Interface Type: external
 Interface Name: vlan1
 Zone: none
 Base Port: ge5
 VLAN ID: 1 (1-4094)
☒ Advance
 Description: (Optional)

IP Address Assignment

☐ Get Automatically
☒ Advance
☒ Use Fixed IP Address
 IP Address: 172.17.1.1
 Subnet Mask: 255.255.255.0
 Gateway: 172.17.1.254 (Optional)
 Metric: 0 (0-15)

In the **Configuration** page, select the **vlan1** entry and click **Create Virtual Interface** on the upper bar. Configure the Fixed IP address (192.168.15.33/24 in this example). Click **OK**.

CONFIGURATION > Network > Interface > VLAN > vlan1

Configuration				
<div> Add Edit Remove Activate Inactivate Create Virtual Interface Object References </div>				
#	Status	Name	Port/VID	IP Address
1		vlan1	ge5/1	static - 172.17.1.1
<div> Page 1 of 1 Show 50 Items Deploying 1 - 1 of 1 </div>				

CONFIGURATION > Network > Interface > VLAN > vlan1:1

Interface Properties

Interface Name: vlan1:1
 Description: (Optional)

IP Address Assignment

IP Address: 192.168.15.33
 Subnet Mask: 255.255.255.0
 Gateway: 192.168.15.1 (Optional)
 Metric: 0 (0..15)

Set Up the Routing on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Routing**, set **Next-Hop Type** to be **Interface** and set **Interface** to be the **vlan1**.

CONFIGURATION > Network > Routing

Configuration

☒ Enable

Description: (Optional)

Criteria

User:

Incoming:

Source Address:

Destination Address:

DSCP Code:

Schedule:

Service:

Next-Hop

Type:

Interface:

Test the Result

Check the **Interface Statistics**, you can see **vlan1 Status** is up, **Tx B/s** displays the transmission speed and **Rx B/s** displays the reception speed. Port 5 and Port 6 are configured in the same **vlan1** but use different IP addresses.

MONITOR > Interface Status > Interface Statistics

Interface Statistics						
Refresh						
Interface	Status	Tx Pkts	Rx Pkts	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	1603	1901	
- vlan1	Up	326	0	42	0	
- ge5_ppp	Inactive			0	0	
ge6	Down	4	0	0	0	
ge7	Down	2	0	0	0	
ge8	Down	1	0	0	0	

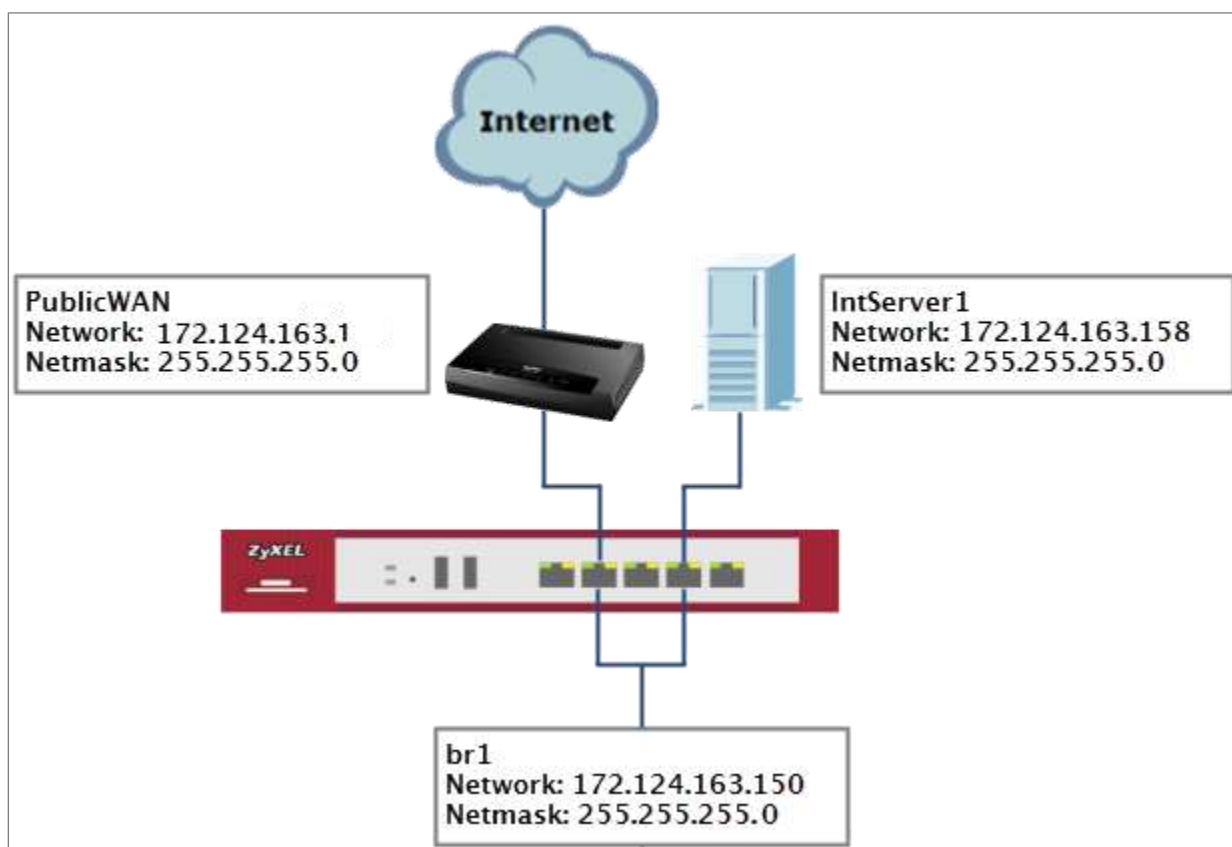
What Could Go Wrong?


If you cannot configure a particular VLAN interface on top of an Ethernet interface, please whether this VLAN has just been created on top of other Ethernet interface.

How to Let a Server Use the Same Public IP Address as the WAN Interface Using the Bridge Interface

This is an example of using ZyWALL/USG to configure an internal server in bridge mode without applying network address translation (NAT). The Internet users can reach this server directly by its public IP address.

ZyWALL/USG with Bridge Interface Example



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the Bridge Interface on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > Interface > Bridge > add Bridge**, select **Interface Type** to be the **general** type, select **Zone** to be the **LAN** zone. In the **Member Configuration**, select internal server (**IntServer1** interface in this example) and public IP address (**Public WAN** interface in this example) to be in the same member group.

In the **IP Address Assignment** section, select **Used Fixed IP Address** and configure br1 IP address (172.124.163.150/24 in this example).

CONFIGURATION > Network > Interface > Bridge > add Bridge

General Settings

☒ Enable Interface

Interface Properties

Interface Type:

general

br1

Zone:

LAN

Description:

(Optional)

Member Configuration

Available

ge1
ge2
ge3
ge4
ge5
ge6
IntServer1
PublicWAN

Member

IP Address Assignment

☐ Get Automatically

☒ Use Fixed IP Address

IP Address:

172.124.163.150

Subnet Mask:

255.255.255.0

Gateway:

172.124.163.129

Metric:

0

(Optional)

(0-15)

After creating the bridge interface, connect the server's network cable to **IntServer1** port and set the server's IP to be in the same subnet (172.124.163.158 in

this example).

Test the Result

Check the **Interface Statistics**, you can see br1 **Status** is up, **Tx B/s** displays the transmission speed and **Rx B/s** displays the reception speed. **IntServer1** and **PublicWAN** are configured in the same vlan1 but using different IP address.

MONITOR > Interface Status > Interface Statistics

Name	Status	TxPkts	RxPkts	Tx B/s	Rx B/s
ge1	Down	0	0	0	0
ge2	1000M/Full	9577	17204	0	0
ge3	Down	2	0	0	0
ge4	1000M/Full	13950	13611	0	0
ge5	Down	2434	2972	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

```
G:\Documents and Settings\ZyXEL-CS0>ping 172.124.163.158

Pinging 172.124.163.158 with 32 bytes of data:

Reply from 172.124.163.158: bytes=32 time=37ms TTL=44
Reply from 172.124.163.158: bytes=32 time=26ms TTL=44
Reply from 172.124.163.158: bytes=32 time=32ms TTL=44
Reply from 172.124.163.158: bytes=32 time=22ms TTL=44

Ping statistics for 172.124.163.158:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

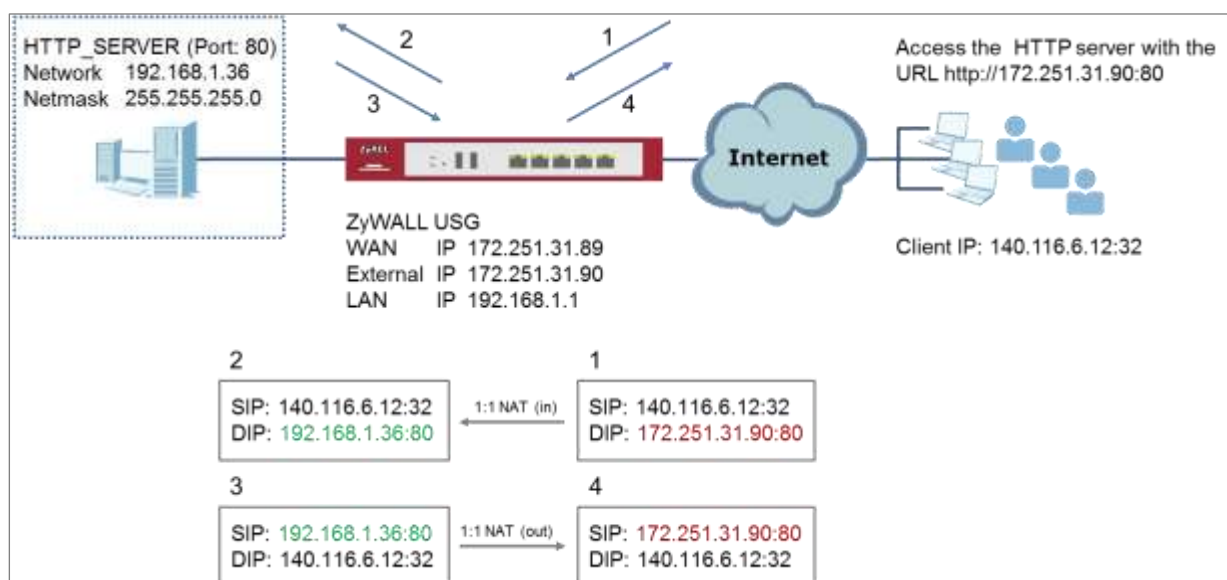
What Could Go Wrong?

If you cannot configure a particular bridge IP address, please check is this IP address already created on other Ethernet interface.

How to Allow Public Access to a Server Behind ZyWALL/USG

This is an example of using ZyWALL/USG to configure a securely access to internal server behind ZyWALL/USG with network address translation (NAT). The Internet users can reach this server directly by its public IP address and a NAT mapping rule will forward the traffic from the Internet to the Intranet. It provides security and decrease the number of IP addresses an organization needs.

ZyWALL/USG enables Public Access to a Server with NAT



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG310 (Firmware Version: ZLD 4.25).

Set Up the NAT on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Network > NAT > add NAT**, select **Enable Rule**. Select **1:1 NAT**. Set **Incoming Interface** to be the **wan1** interface. Type **User-Defined Original IP** (172.251.31.90 in this example) and type **User-Defined Mapped IP** (192.168.1.34 in this example). Set **Port Mapping Type** to **Service**, set **Original Service** and **Mapped Service** to **HTTP** in this example. Click **OK**.

CONFIGURATION > Network > NAT > add NAT

General Settings	
<input checked="" type="checkbox"/> Enable Rule	
Rule Name:	http_server
Port Mapping Type	
Classification:	<input type="radio"/> Virtual Server <input checked="" type="radio"/> 1:1 NAT <input type="radio"/> Many 1:1 NAT
Mapping Rule	
Incoming Interface:	ge1
Original IP:	User Defined
User-Defined Original IP:	172.251.31.90 (IP Address)
Mapped IP:	User Defined
User-Defined Mapped IP:	192.168.1.34 (IP Address)
Port Mapping Type:	any

Set Up the Security Policy on the ZyWALL/USG

In the ZyWALL/USG, go to **CONFIGURATION > Security Policy > Policy Control > add corresponding**, select **Enable**. Configure a Name for your to identify the security policy (http_server_access in this example). Set **From: WAN** and **To: LAN1**. Set **Destination** to the lan subnet where your server is (LAN_SUBNET_GE3 in this example). Set **Service** to **HTTP**, set **Action** to **allow**. Click **OK**.

CONFIGURATION > Security Policy > Policy Control > add corresponding

☒ Enable

Name:

Description: (Optional)

From:

To:

Source:

Destination:

Service:

User:

Schedule:

Action:

Log matched traffic:

Test the Result

Type <http://172.251.31.90/> into the browser, it displays the HTTP service page.

folder
/

5 folders, 0 files - Total: 0 B

Filename	Filesize	Filetime	Hits
FAQ	folder	2015/10/12 下午 03:45:24	0
Level_1	folder	2015/7/9 上午 10:40:26	0
Level_2	folder	2015/8/5 下午 01:46:54	0
Troubleshooting	folder	2015/10/12 下午 03:45:24	0
Walk-through	folder	2015/10/12 下午 03:45:24	0

[File list](#)
[Folder archive](#)

HttpFileServer 2.2f
 Servertime: 2015/12/7 下午 07:51:02
 Uptime: 01:12:08

What Could Go Wrong?

If you cannot access your server via public IP address, please make sure all your public IP addresses are routing properly. To do one by one assign them to the ZyWALL's WAN port. Test to make sure you have internet access with the public IP address.

If you cannot access the ZyWALL from the internet with any IP address on your public IP, this is a routing issue on the service end. Please contact the ISP to fix the routing for the public IPs.

If you see [notice] log message as below, the HTTPS traffic is blocked by the priority 1 Security Policy. The ZyWALL/USG checks the security policy in order and applies the first security policy the traffic matches. If the HTTPS traffic matches a policy that comes earlier in the list, it may be unexpectedly blocked. Please change your policy setting or move the policy to the higher priority.

Monitor > Log

#	Priority	Category	Message	Match
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.

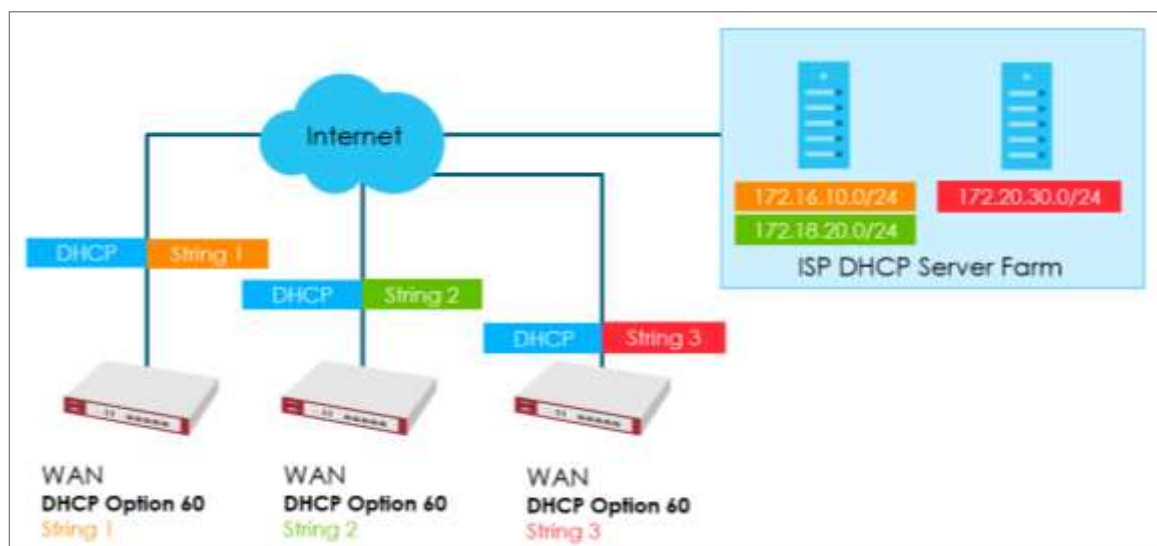


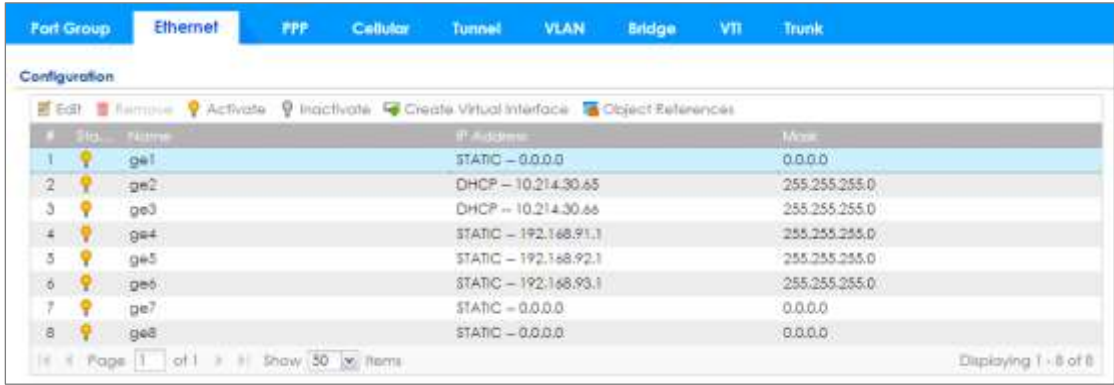
Figure 1 DHCP Option 60 Vendor Class Identifier

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.

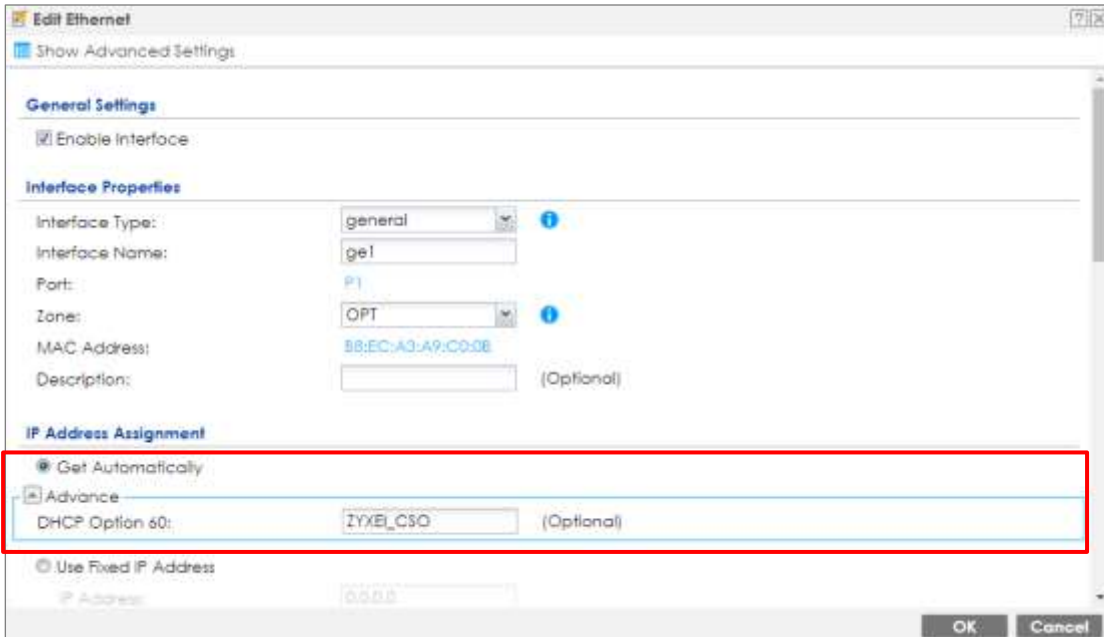
Setting Up DHCP Option 60 on the Web GUI

- 1 In the ZyWALL/USG's navigation panel, go to **Configuration > Network > Interface**.



#	ID	Name	IP Address	Mask
1	ge1	ge1	STATIC - 0.0.0.0	0.0.0.0
2	ge2	ge2	DHCP - 10.214.30.65	255.255.255.0
3	ge3	ge3	DHCP - 10.214.30.66	255.255.255.0
4	ge4	ge4	STATIC - 192.168.91.1	255.255.255.0
5	ge5	ge5	STATIC - 192.168.92.1	255.255.255.0
6	ge6	ge6	STATIC - 192.168.93.1	255.255.255.0
7	ge7	ge7	STATIC - 0.0.0.0	0.0.0.0
8	ge8	ge8	STATIC - 0.0.0.0	0.0.0.0

- 2 Click the **Ethernet** tab, go to **WAN > Edit**. Enter the VCI string in the **Advance** section of **DHCP Option 60**.



Edit Ethernet

Show Advanced Settings

General Settings

☒ Enable Interface

Interface Properties

Interface Type: general

Interface Name: ge1

Port: P1

Zone: OPT

MAC Address: 88:EC:A3:A9:C0:0E

Description: (Optional)

IP Address Assignment

☒ Get Automatically

☐ Advance

DHCP Option 60: ZYXEL_CSO (Optional)

☐ Use Fixed IP Address

IP Address: 0.0.0.0

OK Cancel

Setting Up DHCP Option 60 on the CLI

Under the specific interface path, use these commands to:

Engble option 60

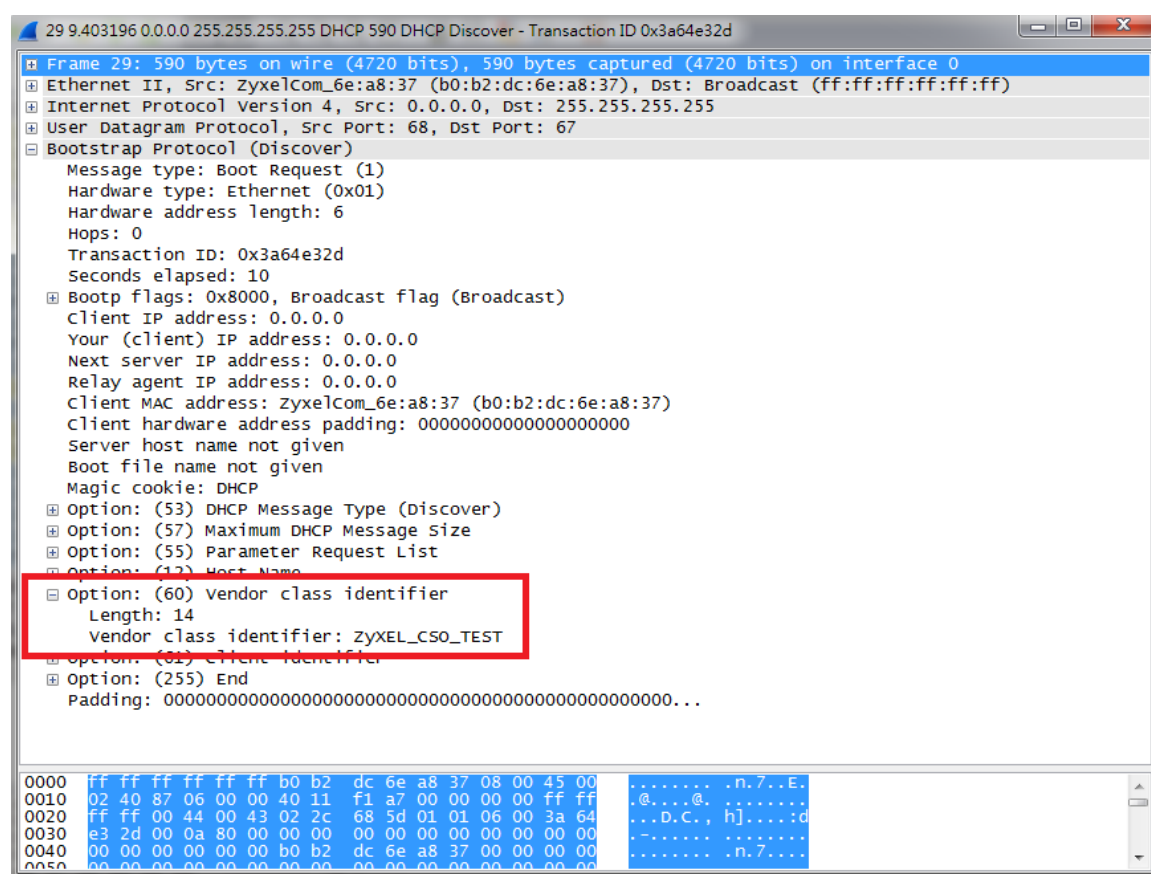
```
Router(config-if-wan1)# ip address dhcp option-60 {VCI STRING}
```

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.

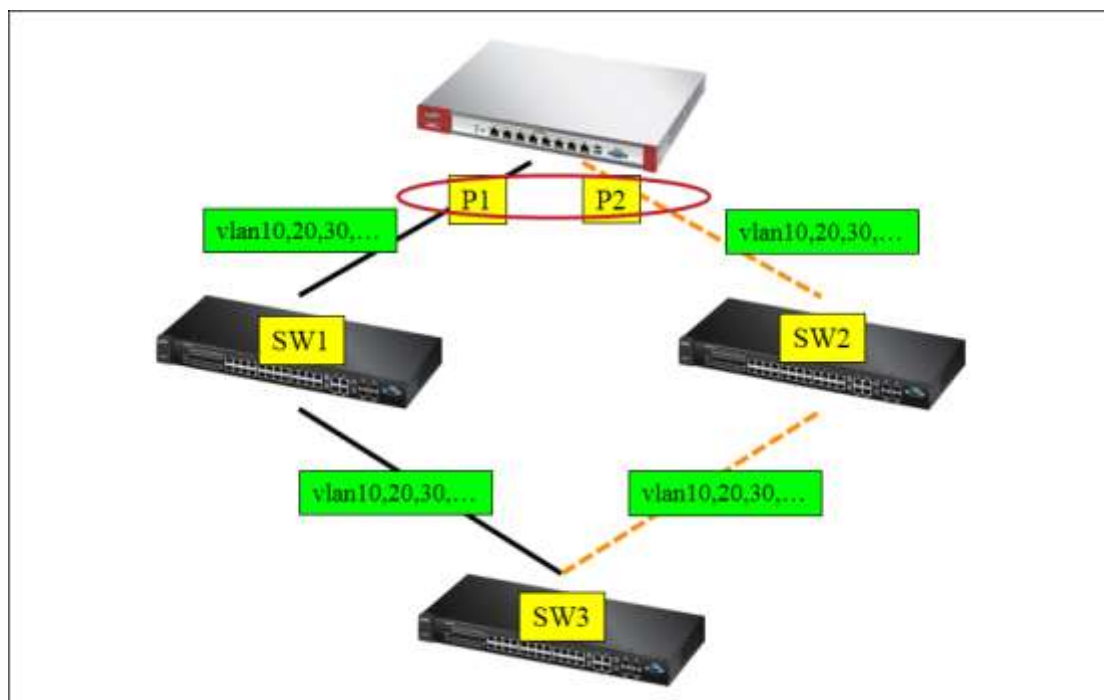
The link aggregation supported models have Active-backup, 802.3ad (LACP), and Balance-alb modes. Link aggregation supports IPsec tunnel, VLAN, and bridge interface.

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.

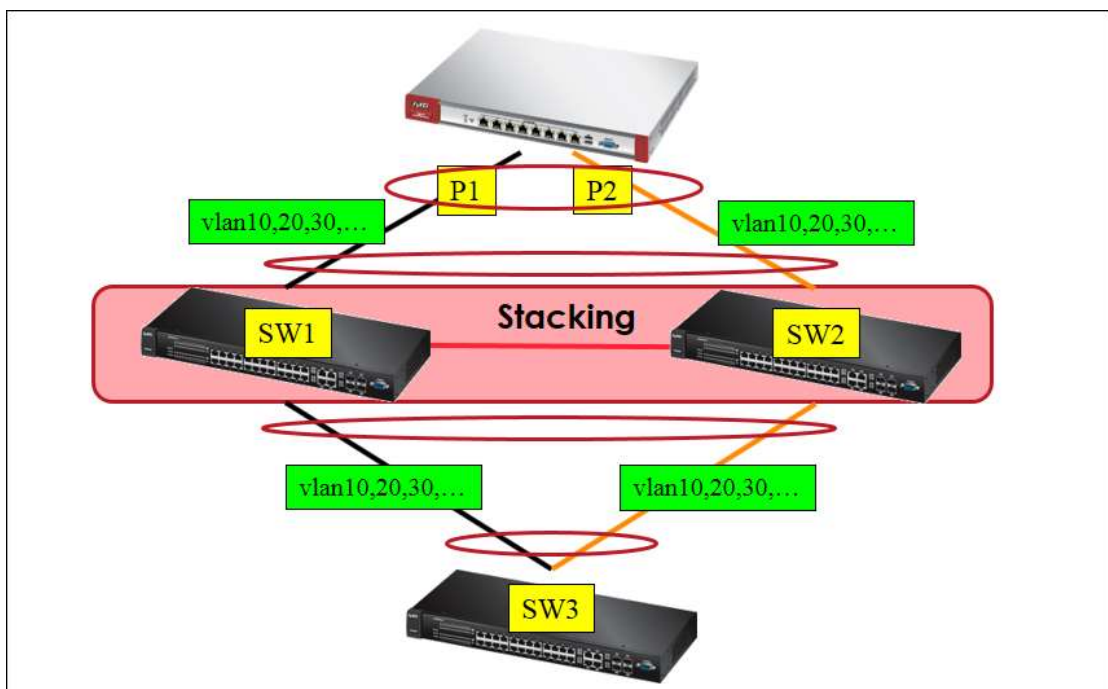
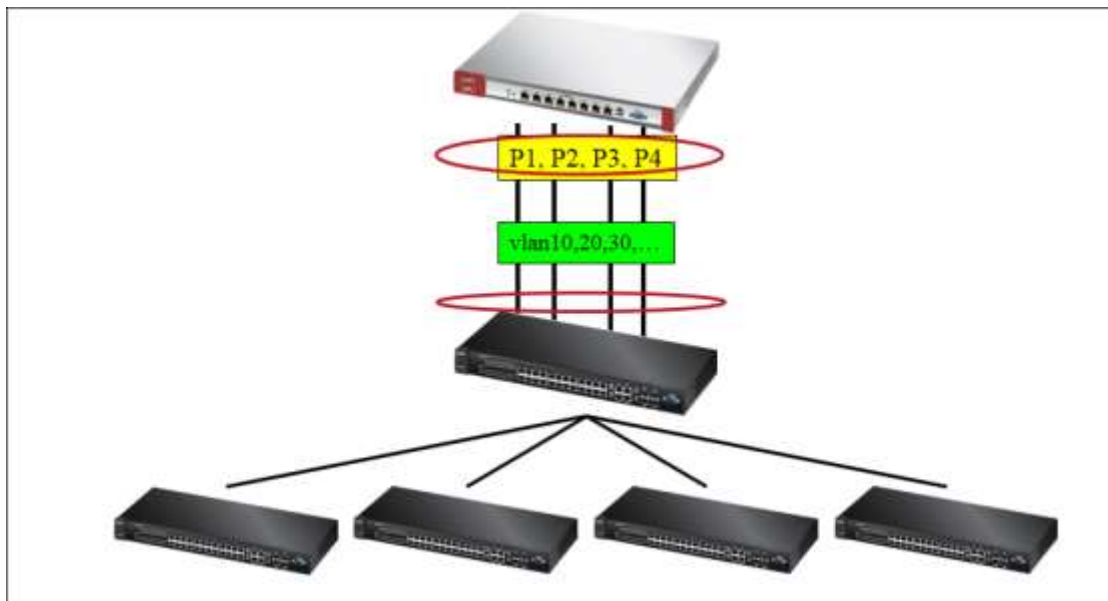
Link Monitoring: Mii monitoring monitors the state of the local interface.

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.

Edit LAG lag0

Show Advanced Settings

Description: (Optional)

LAG Configuration

Mode: 802.3ad

Link Monitoring: mii

Minmon: 100 (1-1000 ms)

Updelay: 0 (0-1000 ms)

Downdelay: 0 (0-1000 ms)

Xmit Hash Policy: layer2

LACP rate: layer2

Available: ge1, ge4, ge5, ge6, ge7, ge8, ge9, ge10, ge11

Slaves: ge2, ge3

OK Cancel

Xmit Hash Policy:

Xmit Hash policy: Select **layer2** or **layer2+3**.

Select **layer 2** if the LAG interface is connect to a layer 2 subnet.

Select **layer 2+3** if the LAG interface is connect to a network with a router or a L3 switch.

Edit LAG lag0

Show Advanced Settings

Description: (Optional)

LAG Configuration

Mode: 802.3ad

Link Monitoring: mii

Minmon: 100 (1-1000 ms)

Updelay: 0 (0-1000 ms)

Downdelay: 0 (0-1000 ms)

Xmit Hash Policy: layer2

LACP rate: slow

Available: ge1, ge4, ge5, ge6, ge7, ge8, ge9, ge10, ge11

Slaves: ge2, ge3

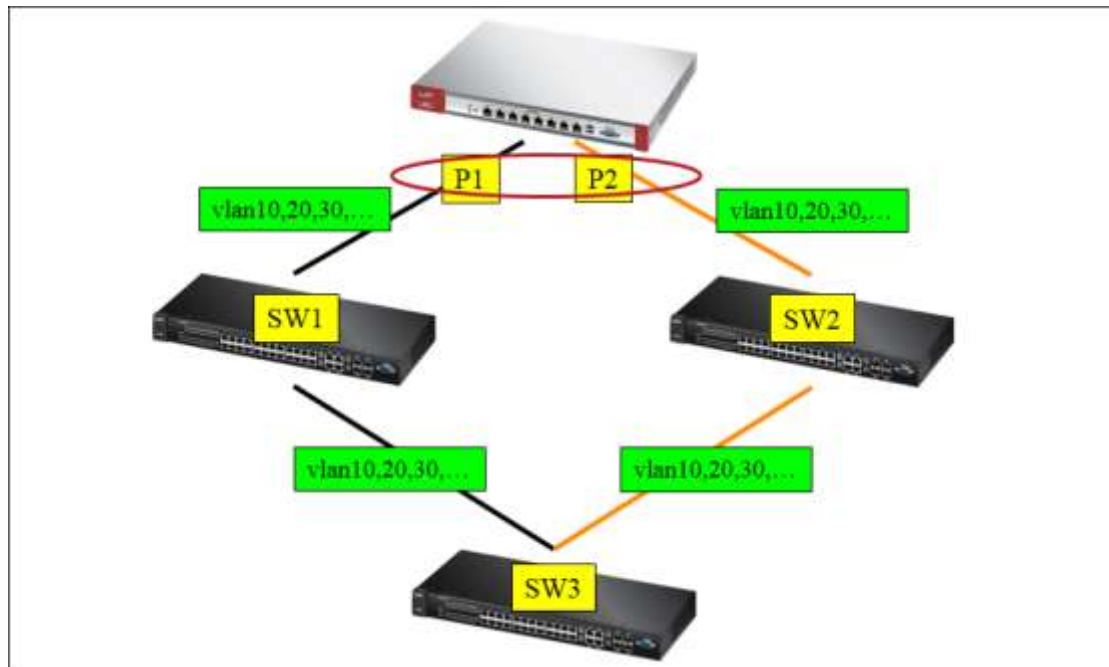
OK Cancel

LACP rate:

The interval can be fast (every second) or slow (every 30 seconds).

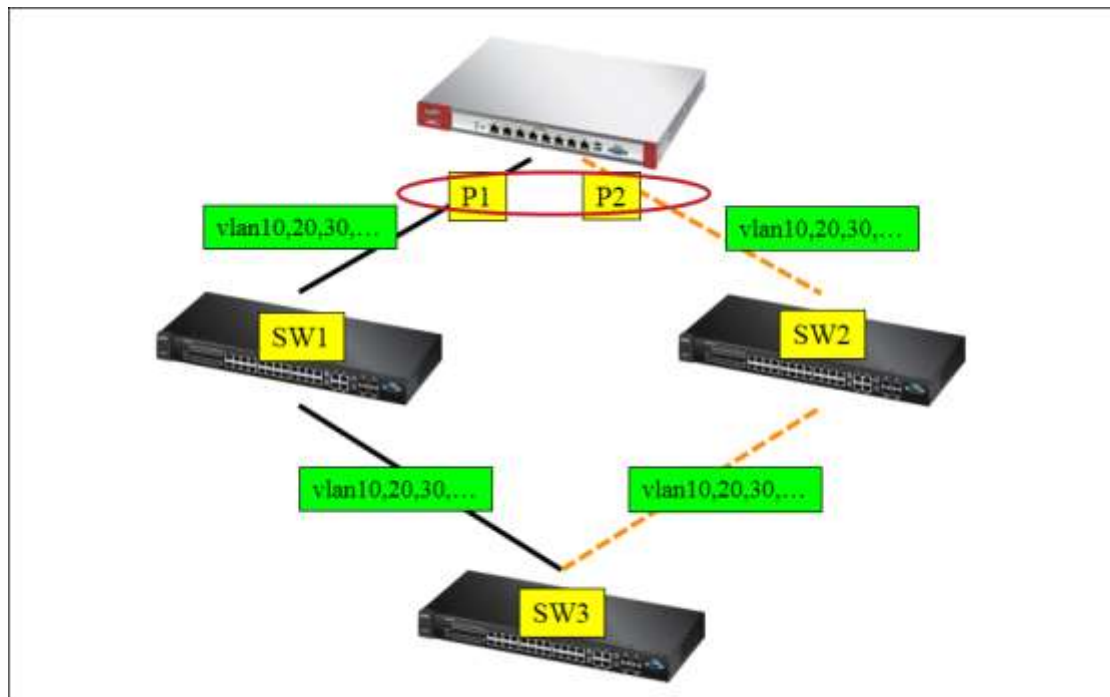
Balance-alb Mode:

(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**.

Port

Ethernet

PPP

Cellular

Tunnel

VLAN

Bridge

LAG

VTI

Trunk

Configuration

Add

Edit

Remove

Activate

Inactivate

Create Virtual Interface

References

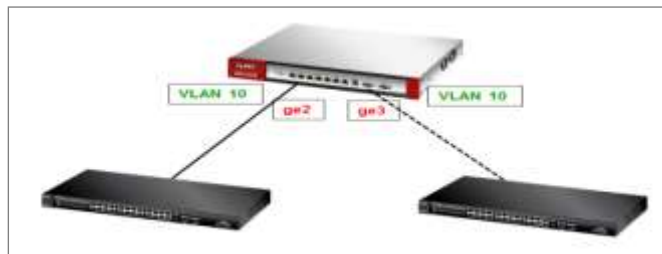
#	Status	Name	Description	Mode	IP Address	Slaves
1		lag0		balance-alb	STATIC - 0.0.0.0	ge2, ge3

Page 1 of 1

Show 50 items

Displaying 1 of 1

The VLAN interface is cross-connected to different switches (fault tolerance).



Only one link connection is up and the other is down. In this case, you will need to use the **active-backup** mode.

+ Add VLAN
Show Advanced Settings

General Settings

☒ Enable Interface

Interface Properties

Interface Type: Internal ⓘ
Interface Name: vlan10
Zone: LAN1 ⓘ
Base Port: lag0
VLAN ID: 10 (1-4094)
☒ Advance
Description: (Optional)

You can find the LAG interface in the VLAN interface.

Port
Ethernet
PPP
Cellular
Tunnel
VLAN
Bridge
LAG
VVI
Trunk

Configuration

Add
Edit
Remove
Activate
Inactivate
Create Virtual Interface
References

#	Status	Name	Description	Port/VID	IP Address	Mask
1		vlan10		lag0/10	static -0.0.0.0	0.0.0.0

Page 1 of 1
Show 50 Items

Displaying 1 - 1 of 1

Test the Result

After the deployment you can see the interface status through **Monitor>interface Status**

lag0	P2, P3	Down	n/a	LAN	0.0.0.0 / 0.0.0.0	Static	n/a	n/a
vlan10	lag0	Up	n/a	LAN1	192.168.66.1	Static	n/a	n/a

Below we are using 802.3ad LAG interface with Vlan66 for the example, unplug one of the network cable during the ping, the connection should still alive after one ping lost.

Add
Edit
Remove
Activate
Inactivate
Create Virtual Interface
References

#	Status	Name	Description	Mode	IP Address	Mask
1		lag0		802.3ad	STATIC - 0.0.0.0	ge2, ge3

Page 1 of 1
Show 50 Items

Displaying 1 - 1 of 1

Add
Edit
Remove
Activate
Inactivate
Create Virtual Interface
References

#	Status	Name	Description	Port/VID	IP Address	Mask
1		vlan10		lag0/10	static -192.168.66.1	255.255.255.0

Page 1 of 1
Show 50 Items

Displaying 1 - 1 of 1

```
C:\Users\ZT02340>ping -t 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=27ms TTL=45
Reply from 8.8.8.8: bytes=32 time=34ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=25ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Request timed out.
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=31ms TTL=45
Reply from 8.8.8.8: bytes=32 time=25ms TTL=45
Reply from 8.8.8.8: bytes=32 time=27ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Request timed out.
Reply from 8.8.8.8: bytes=32 time=33ms TTL=45
Reply from 8.8.8.8: bytes=32 time=25ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=26ms TTL=45
Reply from 8.8.8.8: bytes=32 time=41ms TTL=45
Reply from 8.8.8.8: bytes=32 time=25ms TTL=45
```

What can go wrong

1. Configure all the related setting on LAG interface before you connect the link.
2. Make sure you have the corresponding setting on your switch if using 802.3ad (LACP).
3. Check the Xmit Hash policy or the link monitoring method.
4. To adjust the sensitivity of the updelay and downdelay when using active-backup or balance-alb mode.