ZYXEL

www.zyxel.com

VPN2S

VPN2S

VPN

Firmware V1.12(ABLN.0)b9
Edition 1, 5/2018

Handbook

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

Copyright © 2018 ZyXEL Communications Corporation

Table of Content

How to Setup VPN2S connect with Android Mobile via L2TP tunnel........4

Set Up the PPPoE Connection On VPN2S Series.................................. 5
Set Up the L2TP VPN Tunnel on VPN2S.. 6
Configure the L2TP VPN Tunnel on Android Mobile (Version 5.0.2) ... 8
Test the L2TP over IPSec VPN Tunnel 9
What Could Go Wrong? 10

How to configure site to site VPN 11

Configuration the LAN IP on HQ Site... 12
Setup the VPN configuration on HQ Site.. 14
Configuration the LAN IP on Branch Site 16
Setup the VPN configuration on Branch Site..................................... 18
Test IPSec VPN on VPN2S Series 20

How to configure VPN with PC -Server Role..21

Set Up the IPSec VPN Tunnel on the VPN2S.. 21
Setup the Zywall IPsec VPN client.. 24
Test VPN2S as Server Role 27

How to setup scheduled rule via firewall on VPN2S...............................29

Setup the schedule rule on the VPN2S 30
Test scheduled rule via firewall on VPN2S 32

How to Configure Interface Group Bridge / Bundle WAN Interface (Triple play)...32

Set Up the Interface Group Bridge / Bundle WAN Interface Group on the VPN2S. 33

How to configure Multi-WAN 36

Set Up the Multi-WAN on the VPN2S. 37
Check the Multi-WAN status 37

How to Configure NAT Port Forwarding 38

Set Up the Port Forwarding on the VPN2S.. 39
Test the Port Forwarding 40

How to Configure NAT Port Triggering...42

Set Up the Port Triggering on the VPN2S... 43

How to Enable NAT ALG 44

Enable the ALG on the VPN2S 44

How to Configure NAT Default Server 45

Set Up the Default Server on the VPN2S 46

Test the Default Server 47

How to Configure NAT Address Mapping 48

Set Up the VPN2S Address Mapping (One-to-One) 49

Set Up the VPN2S Address Mapping (Many-to-Many) 50

Set Up the VPN2S Address Mapping (Many-to-one)......................... 51

How to setup policy route to force VPN2S clients following rules..........52

Set Up the policy route to force VPN2S clients following rules......... 53

How to Configure Content Filter by Category 55

Set up the Content Filter by Category 55

Test the Content Filter 57

How to Configure bypass website by Content Filter white list................58

Set up the Content Filter by Category 58

Set up the Content Filter white list 60

Test bypass website by Content Filter white list 60

How to Configure bypass website by Content Filter black list...............60

Set up the Content Filter by black list 61

Set up the Content Filter black list... 62

Test block website by Content Filter black list 62

How to Setup VPN2S connect with Android Mobile via L2TP tunnel

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 and allow traffic from L2TP clients to go to the Internet from an Android mobile phone.

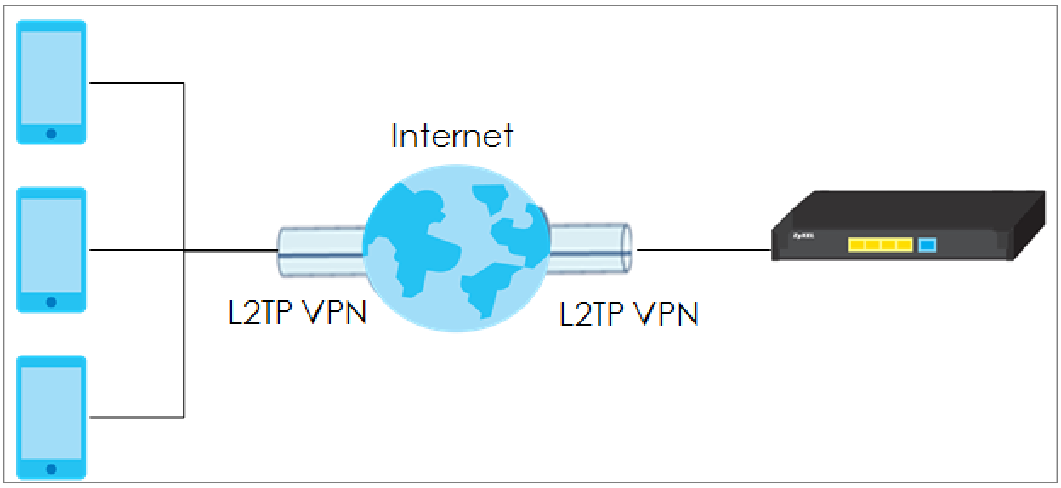
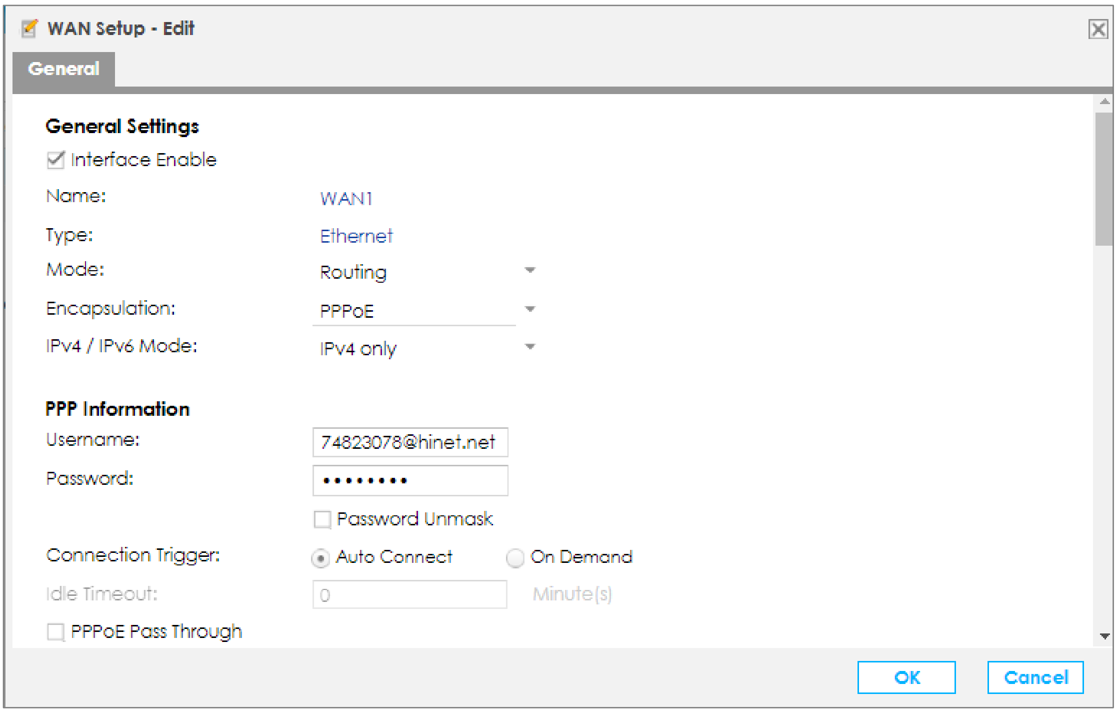


Figure VPN2S connect with Mobile through L2TP VPN Tunnel

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.

Set Up the PPPoE Connection On VPN2S Series

Go to **Configuration> Wan/Internet> WAN Setup> WAN1> Edit**, change the **Encapsulation** from default IPoE to PPPoE and fill the username/password on **PPP information.**



WAN Setup - Edit

General

General Settings

☑ Interface Enable

Name: WAN1

Type: Ethernet

Mode: Routing

Encapsulation: PPPoE

IPv4 / IPv6 Mode: IPv4 only

PPP Information

Username: 74823078@hinet.net

Password: ••••••••

□ Password Unmask

Connection Trigger: ● Auto Connect ○ On Demand

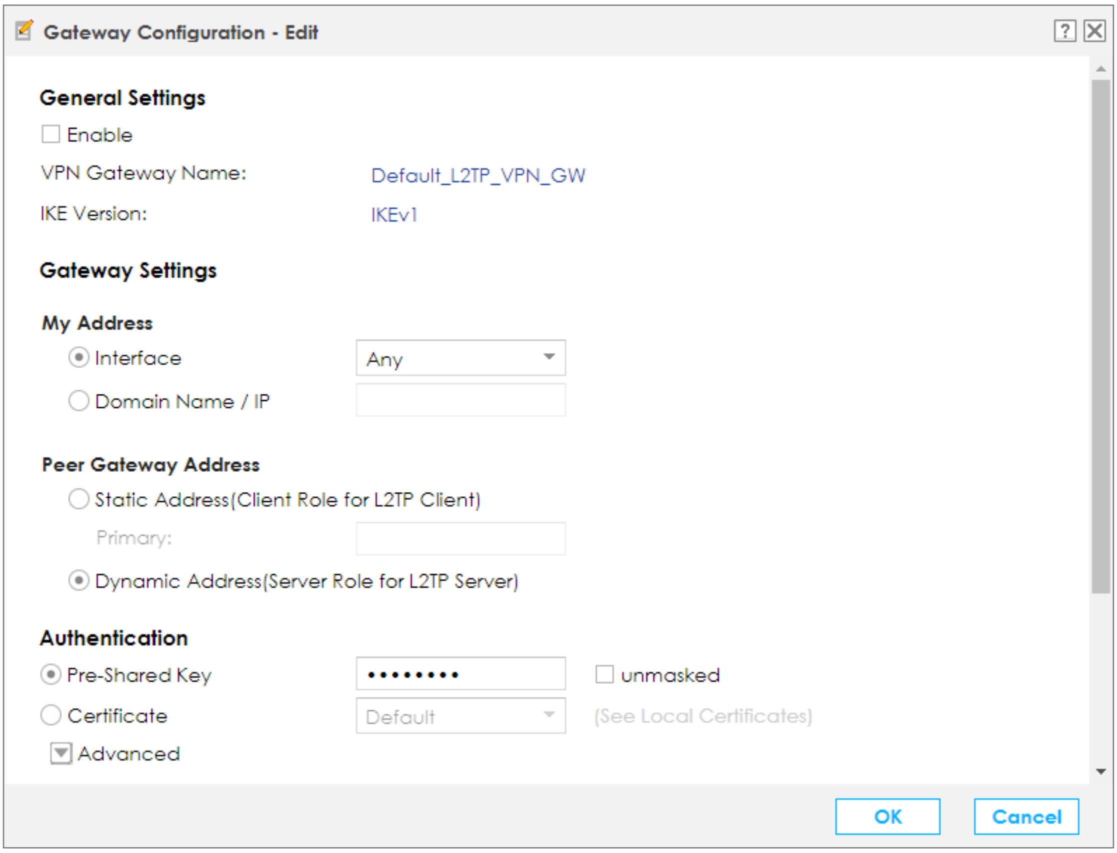
Idle Timeout: 0 Minute(s)

□ PPPoE Pass Through

Set Up the L2TP VPN Tunnel on VPN2S

Go to **Configuration> VPN> IPsec VPN > Default_L2TP_VPN_GW and Default_L2TP_VPN_Connection > Edit**, enable both of rule and fill the pre-share key on Default_L2TP_VPN_GW.

Figure Configuration> VPN> IPsec VPN > Default_L2TP_VPN_GW



Gateway Configuration - Edit

General Settings

□ Enable

VPN Gateway Name: Default_L2TP_VPN_GW

IKE Version: IKEv1

Gateway Settings

My Address

● Interface: Any

○ Domain Name / IP

Peer Gateway Address

○ Static Address(Client Role for L2TP Client)

Primary:

● Dynamic Address(Server Role for L2TP Server)

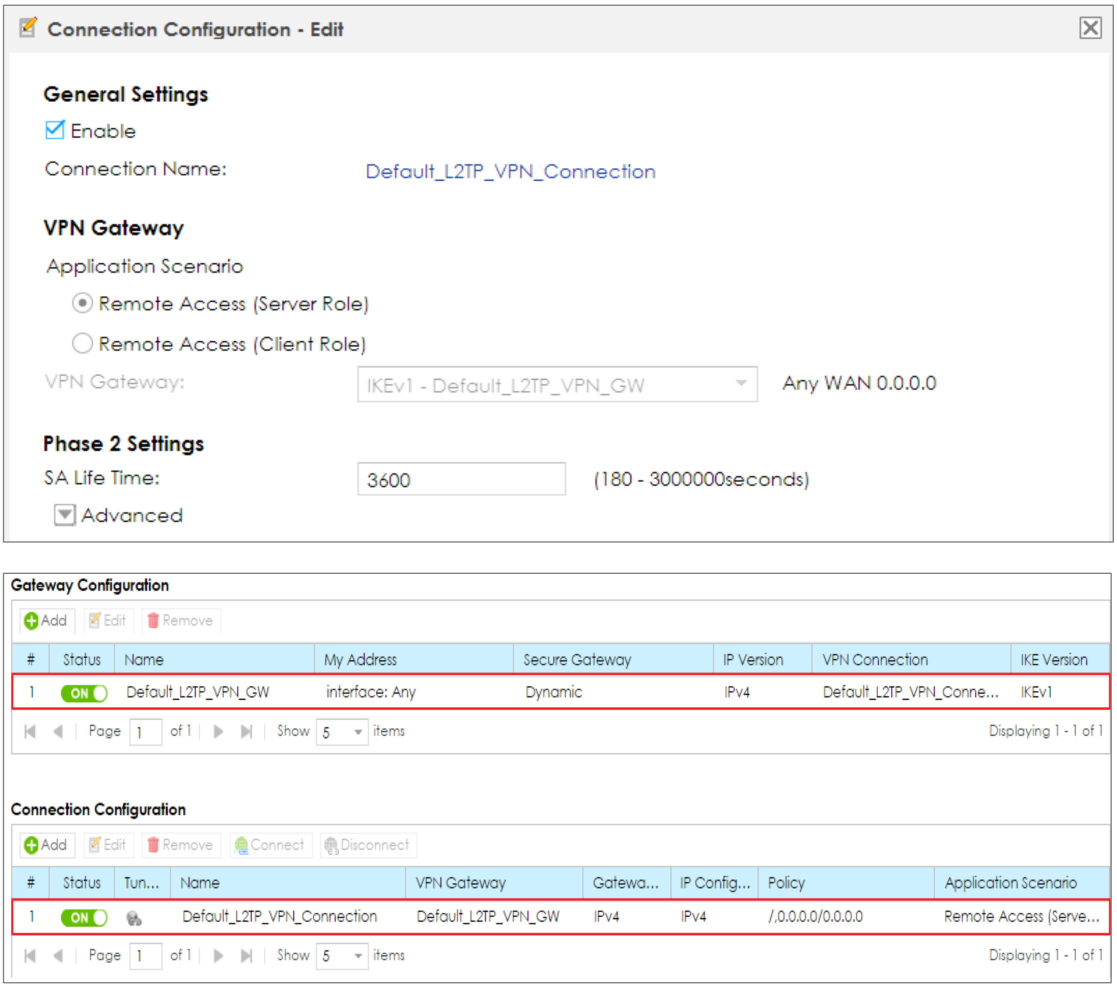
Authentication

● Pre-Shared Key: •••••••• □ unmasked

○ Certificate: Default (See Local Certificates)

Advanced

Figure Configuration> VPN> IPsec VPN > Default_L2TP_VPN_Connection



Connection Configuration - Edit

General Settings

☑ Enable

Connection Name: Default_L2TP_VPN_Connection

VPN Gateway

Application Scenario

● Remote Access (Server Role)

○ Remote Access (Client Role)

VPN Gateway: IKEv1 - Default_L2TP_VPN_GW Any WAN 0.0.0.0

Phase 2 Settings

SA Life Time: 3600 (180 - 3000000seconds)

Advanced

Gateway Configuration

#	Status	Name	My Address	Secure Gateway	IP Version	VPN Connection	IKE Version
1	ON	Default_L2TP_VPN_GW	interface: Any	Dynamic	IPv4	Default_L2TP_VPN_Conne...	IKEv1

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

Connection Configuration

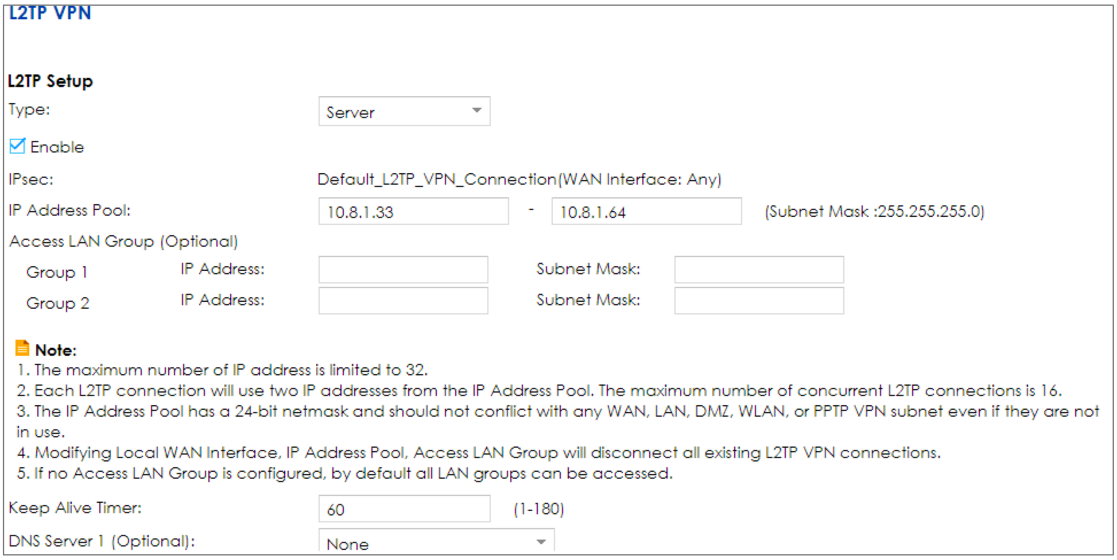
#	Status	Tun...	Name	VPN Gateway	Gatewa...	IP Config...	Policy	Application Scenario
1	ON		Default_L2TP_VPN_Connection	Default_L2TP_VPN_GW	IPv4	IPv4	/,0.0.0.0/0.0.0.0	Remote Access (Serve...

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

Move to **L2TP VPN, Enable** this feature, and select **Server** type.

Fill the IP Address which will be assigned to l2tp client on **IP Address Pool**.

Figure Configuration> VPN> L2TP VPN



L2TP VPN

L2TP Setup

Type: Server

☑ Enable

IPsec: Default_L2TP_VPN_Connection(WAN Interface: Any)

IP Address Pool: 10.8.1.33 - 10.8.1.64 (Subnet Mask :255.255.255.0)

Access LAN Group (Optional)

Group 1 IP Address: Subnet Mask:

Group 2 IP Address: Subnet Mask:

Note:

1. The maximum number of IP address is limited to 32.
2. Each L2TP connection will use two IP addresses from the IP Address Pool. The maximum number of concurrent L2TP connections is 16.
3. The IP Address Pool has a 24-bit netmask and should not conflict with any WAN, LAN, DMZ, WLAN, or PPTP VPN subnet even if they are not in use.
4. Modifying Local WAN Interface, IP Address Pool, Access LAN Group will disconnect all existing L2TP VPN connections.
5. If no Access LAN Group is configured, by default all LAN groups can be accessed.

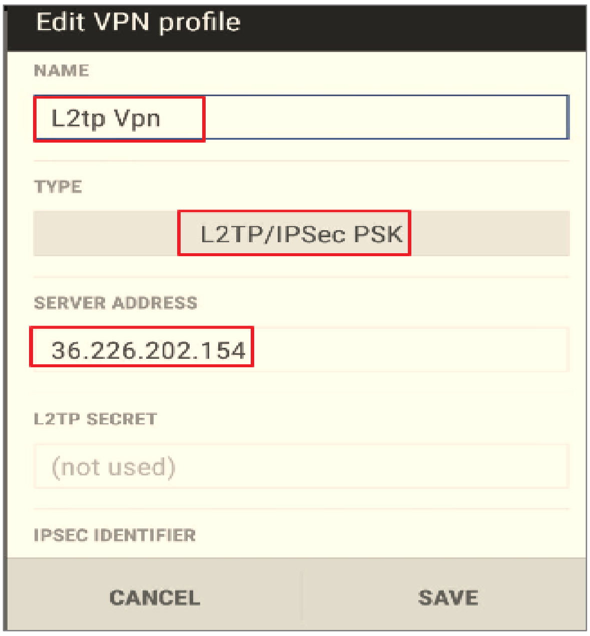
Keep Alive Timer: 60 (1-180)

DNS Server 1 (Optional): None

Configure the L2TP VPN Tunnel on Android Mobile (Version 5.0.2)

Go to **Setting> Wireless & Networks > VPN> Add VPN Profile,** and fill the name of profile.

Select L2TP/IPSec PSK on Type field, enter Server address and pre-shared key.



Edit VPN profile

NAME

L2tp Vpn

TYPE

L2TP/IPSec PSK

SERVER ADDRESS

36.226.202.154

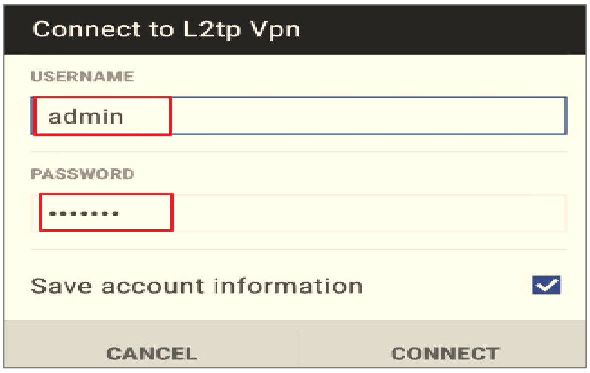
L2TP SECRET

(not used)

IPSEC IDENTIFIER

Test the L2TP over IPSec VPN Tunnel

Type the username and password, and click CONNECT



Connect to L2tp Vpn

USERNAME

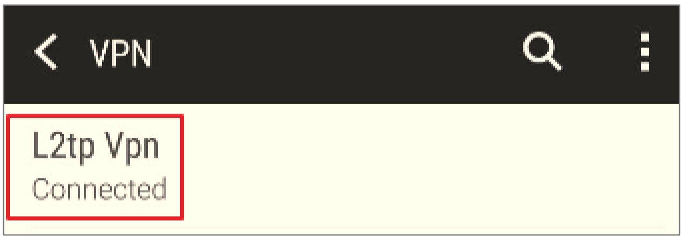
admin

PASSWORD

•••••••

Save account information ☑

The L2TP VPN session connected

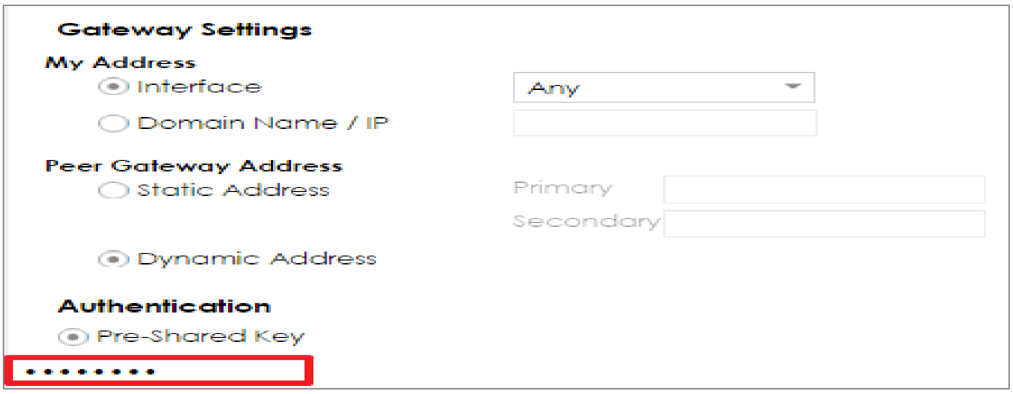


VPN

L2tp Vpn
Connected

What Could Go Wrong?

Make sure your Pre-shared key on VPN2S and Mobile are the same



Gateway Settings

My Address

● Interface — Any

○ Domain Name / IP

Peer Gateway Address

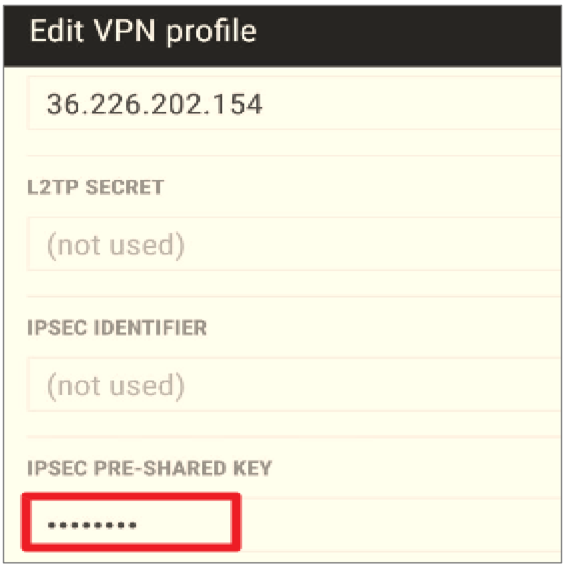
○ Static Address — Primary / Secondary

● Dynamic Address

Authentication

● Pre-Shared Key

•••••••••



Edit VPN profile

36.226.202.154

L2TP SECRET

(not used)

IPSEC IDENTIFIER

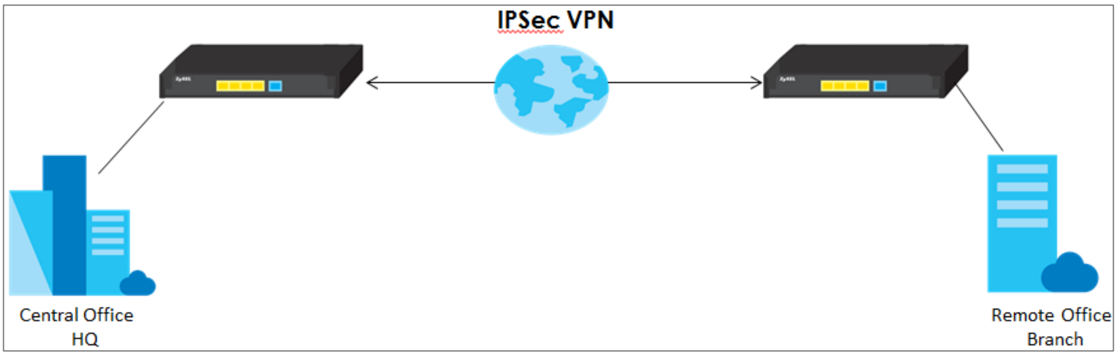
(not used)

IPSEC PRE-SHARED KEY

•••••••••

How to configure site to site VPN

The multinational corporations have many sites at each country, so if they want to communicate from HQ to branch under security, the client to Site VPN is the option they needed.



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 VPN2S.

This scenario uses two units of VPN2S to create an IPSec VPN connection.

Moreover, both USGs get their public IPs via PPPoE .

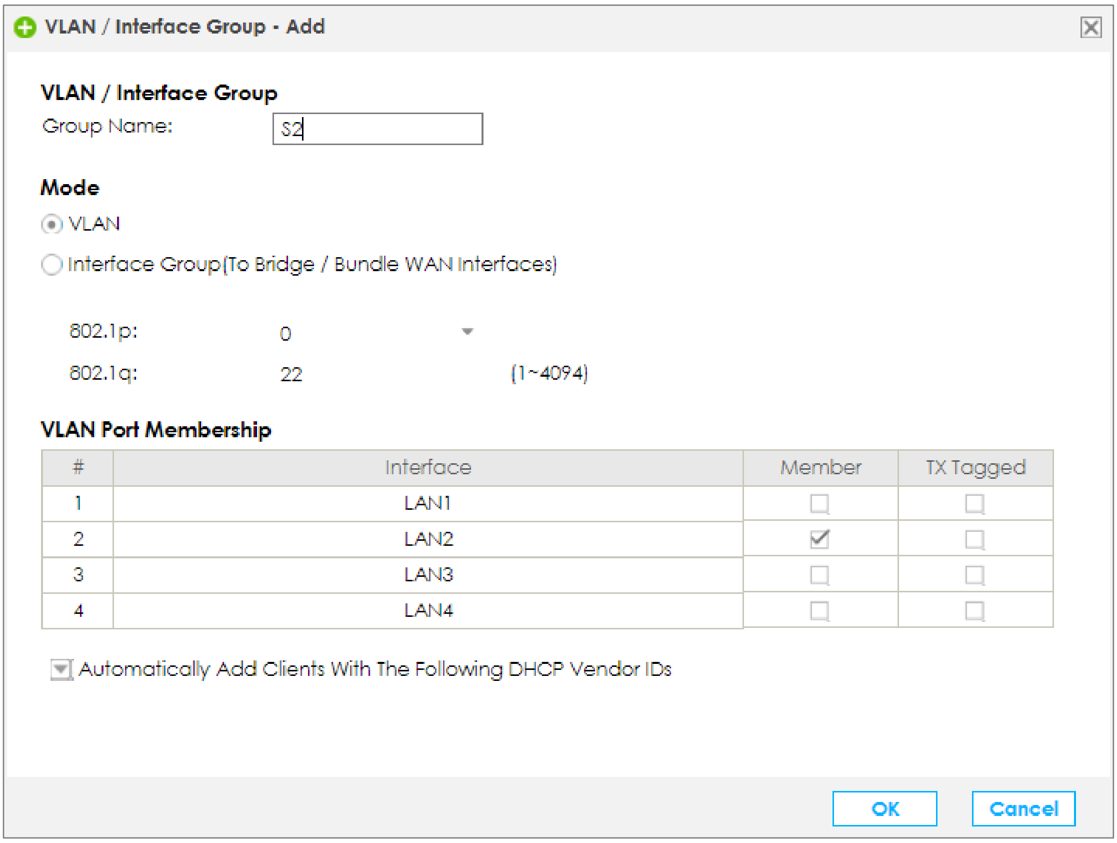
HQ WAN IP: 61.231.53.228, LAN IP: 192.168.2.1

Branch WAN IP: 36.226.203.74   LAN IP: 192.168.3.1

Configuration the LAN IP on HQ Site

Go to **Configuration > LAN/ Home network > VLAN/ Interface Group > Add**

Create the Lan Subnet: 192.168.2.X/24, first go to VLAN to separate the LAN2, and then change the subnet to 192.168.2.X/24



VLAN / Interface Group - Add

VLAN / Interface Group

Group Name: S2

Mode

● VLAN

○ Interface Group(To Bridge / Bundle WAN Interfaces)

802.1p: 0

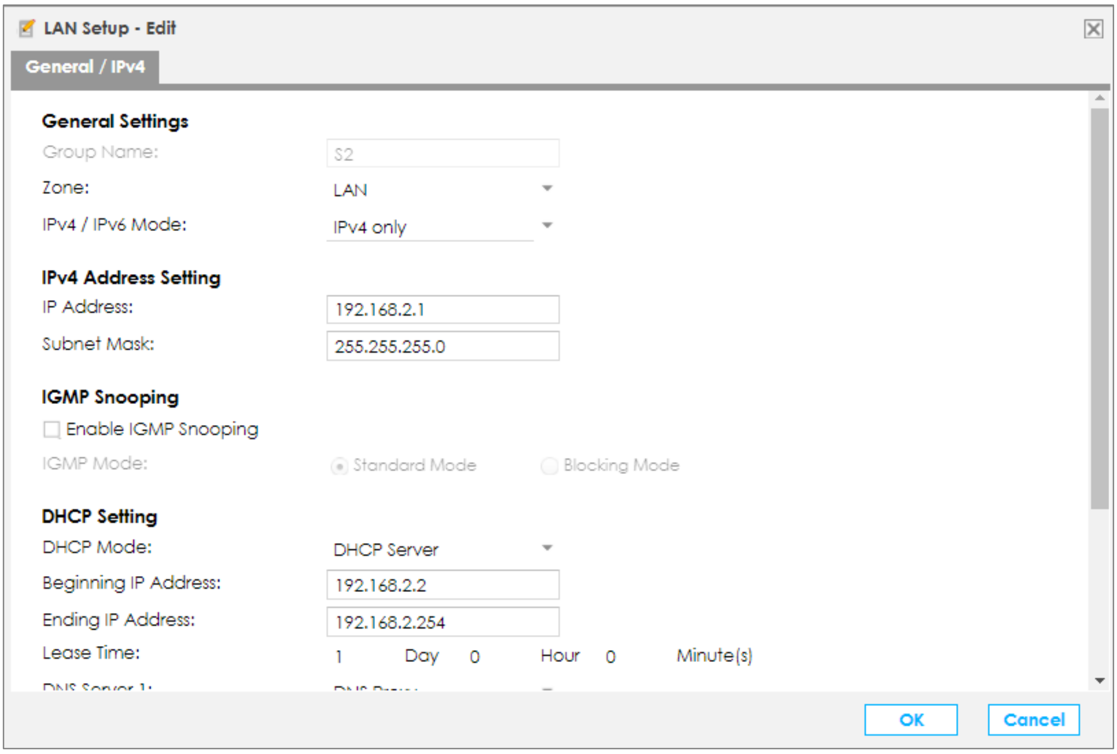
802.1q: 22 (1~4094)

VLAN Port Membership

#	Interface	Member	TX Tagged
1	LAN1	□	□
2	LAN2	☑	□
3	LAN3	□	□
4	LAN4	□	□

Automatically Add Clients With The Following DHCP Vendor IDs

Go to **Configuration > LAN Setup >Edit**



General Settings

Group Name: S2

Zone: LAN

IPv4 / IPv6 Mode: IPv4 only

IPv4 Address Setting

IP Address: 192.168.2.1

Subnet Mask: 255.255.255.0

IGMP Snooping

□ Enable IGMP Snooping

IGMP Mode: ● Standard Mode ○ Blocking Mode

DHCP Setting

DHCP Mode: DHCP Server

Beginning IP Address: 192.168.2.2

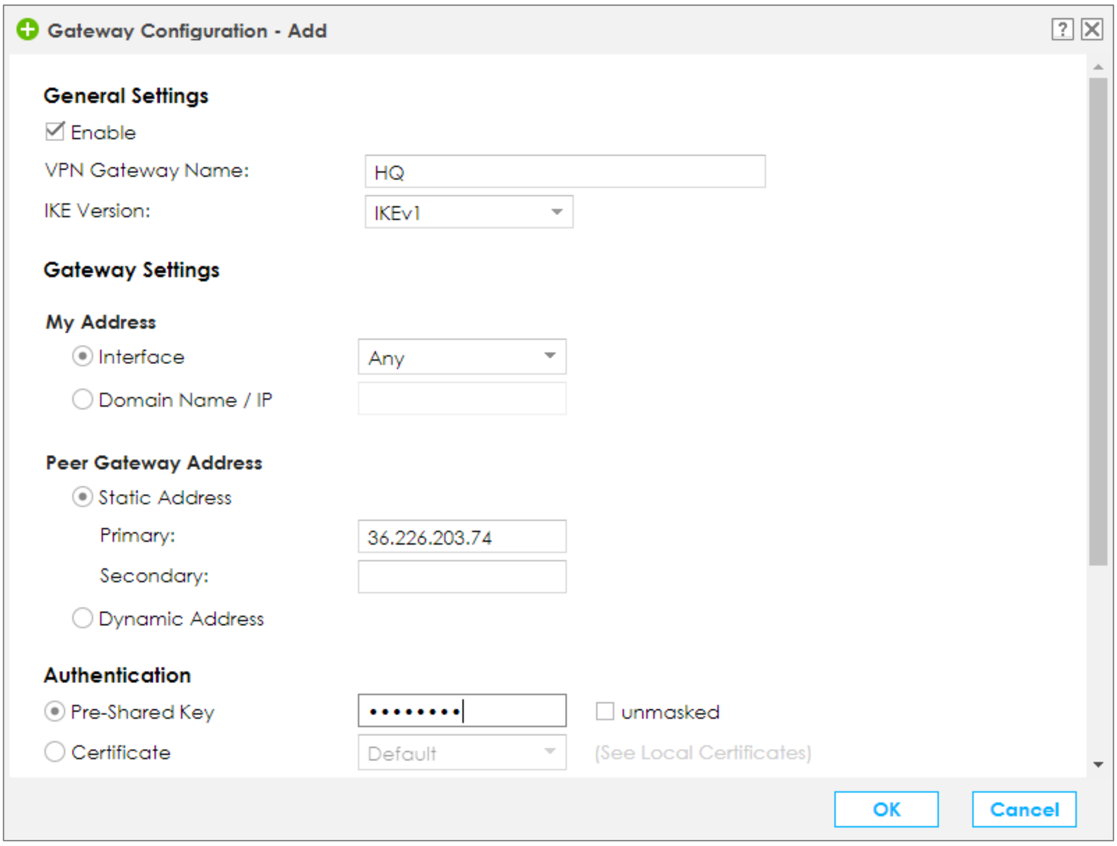
Ending IP Address: 192.168.2.254

Lease Time: 1 Day 0 Hour 0 Minute(s)

DNS Server 1: DNS Proxy

Setup the VPN configuration on HQ Site

Go to **Configuration > VPN > IPSec VPN > Add** the profile on **Gateway configuration** and **Connection configuration**
For the VPN gateway, please enter the VPN gateway name, select the Interface (for public IP), enter the peer's domain in the Primary field, and enter the Pre-Shared Key.



Gateway Configuration - Add

General Settings

☑ Enable

VPN Gateway Name: HQ

IKE Version: IKEv1

Gateway Settings

My Address

● Interface: Any

○ Domain Name / IP

Peer Gateway Address

● Static Address

Primary: 36.226.203.74

Secondary:

○ Dynamic Address

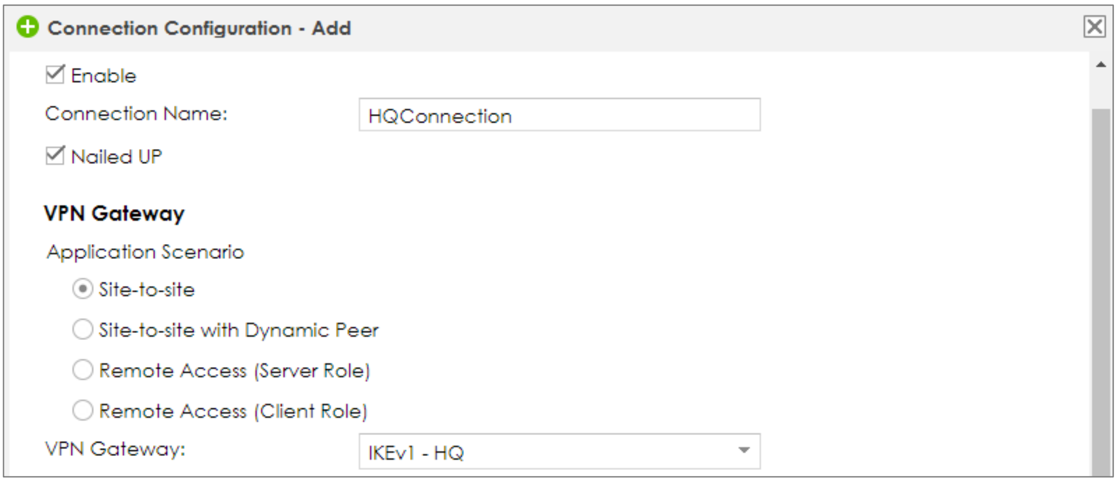
Authentication

● Pre-Shared Key: ••••••••• □ unmasked

○ Certificate: Default (See Local Certificates)

For the VPN connection (Phase 2):

1. Enter the **Connection Name**, select **Site-to-site** as the **Application Scenario**, and select the name of the phase 1 profile (**Branch**) in the **VPN Gateway** field.
2. For **Local policy**, choose the subnet that your PC is connected to.



Connection Configuration - Add

☑ Enable

Connection Name: HQConnection

☑ Nailed UP

VPN Gateway

Application Scenario

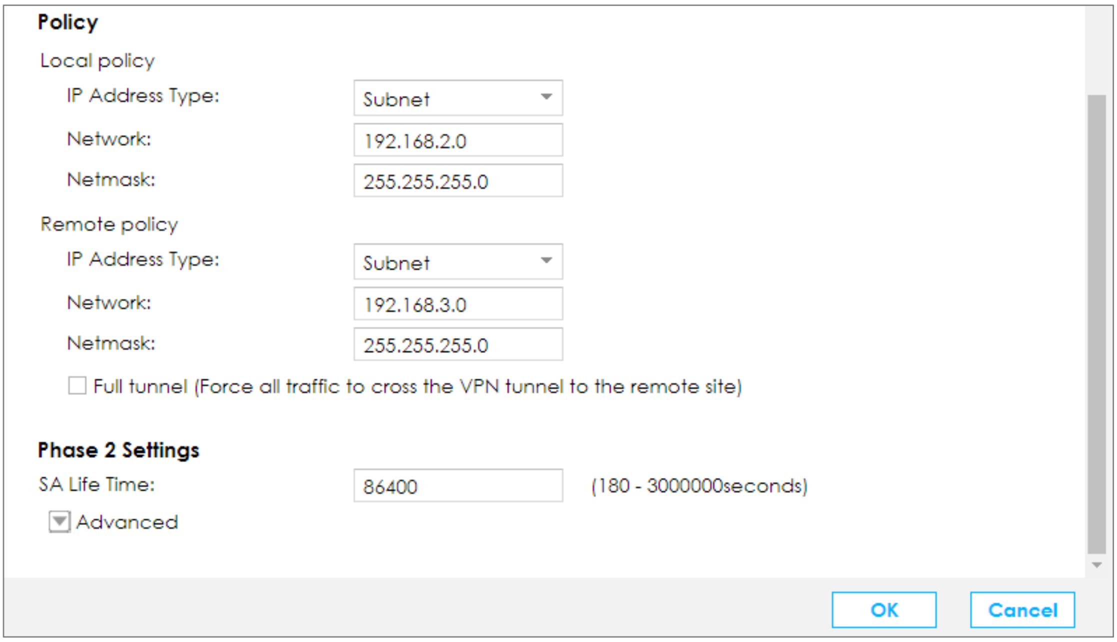
● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

VPN Gateway: IKEv1 - HQ



Policy

Local policy

IP Address Type: Subnet

Network: 192.168.2.0

Netmask: 255.255.255.0

Remote policy

IP Address Type: Subnet

Network: 192.168.3.0

Netmask: 255.255.255.0

□ Full tunnel (Force all traffic to cross the VPN tunnel to the remote site)

Phase 2 Settings

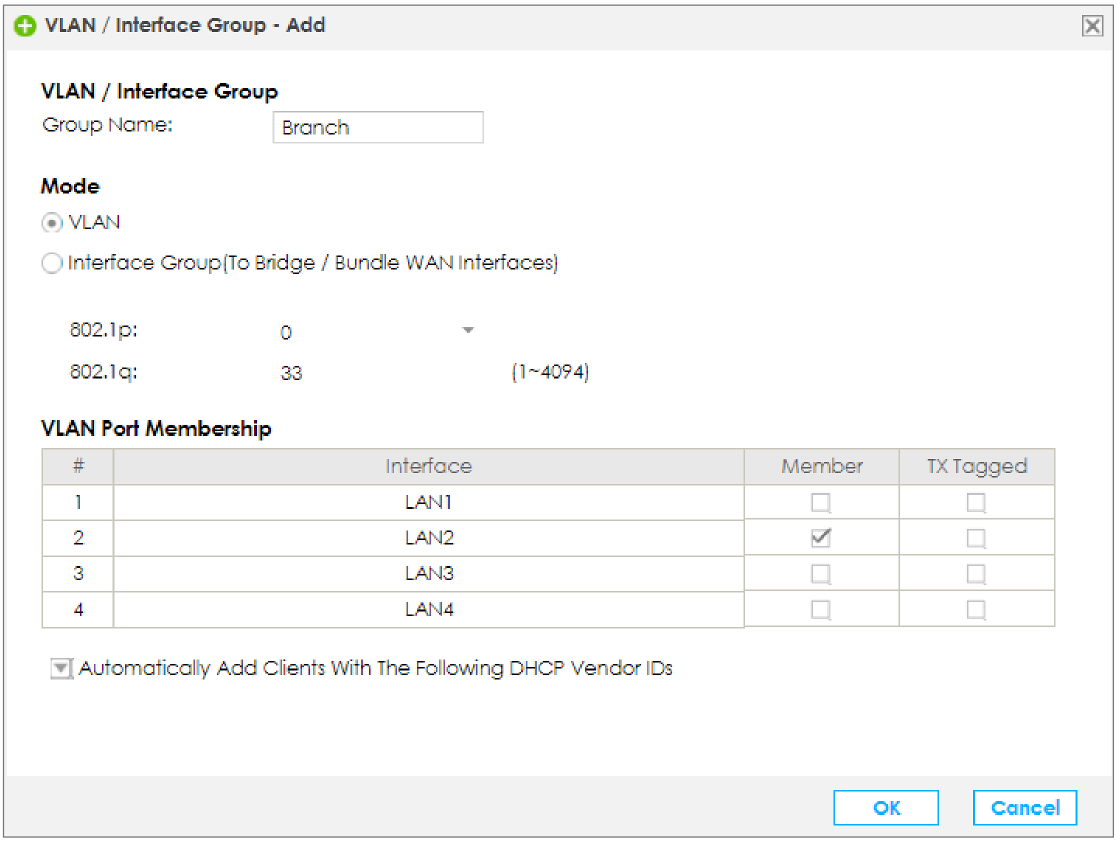
SA Life Time: 86400 (180 - 3000000seconds)

▾ Advanced

Configuration the LAN IP on Branch Site

Go to **Configuration > LAN/ Home network > VLAN/ Interface Group > Add**

Create the Lan Subnet: 192.168.3.X/24, first go to VLAN to separate the LAN2, and then change the subnet to 192.168.3.X/24



VLAN / Interface Group - Add

VLAN / Interface Group

Group Name: Branch

Mode

● VLAN

○ Interface Group(To Bridge / Bundle WAN Interfaces)

802.1p: 0

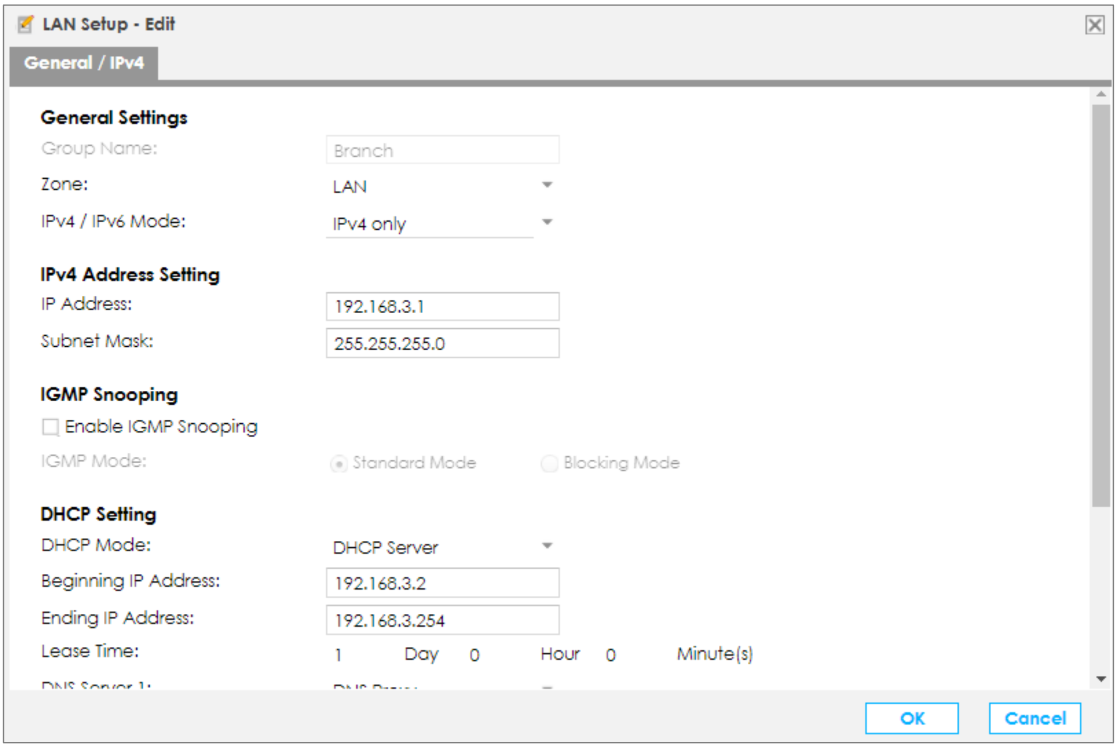
802.1q: 33 (1~4094)

VLAN Port Membership

#	Interface	Member	TX Tagged
1	LAN1	□	□
2	LAN2	☑	□
3	LAN3	□	□
4	LAN4	□	□

□ Automatically Add Clients With The Following DHCP Vendor IDs

Go to **Configuration > LAN Setup >Edit**



General Settings

Group Name: Branch

Zone: LAN

IPv4 / IPv6 Mode: IPv4 only

IPv4 Address Setting

IP Address: 192.168.3.1

Subnet Mask: 255.255.255.0

IGMP Snooping

□ Enable IGMP Snooping

IGMP Mode: ● Standard Mode ○ Blocking Mode

DHCP Setting

DHCP Mode: DHCP Server

Beginning IP Address: 192.168.3.2

Ending IP Address: 192.168.3.254

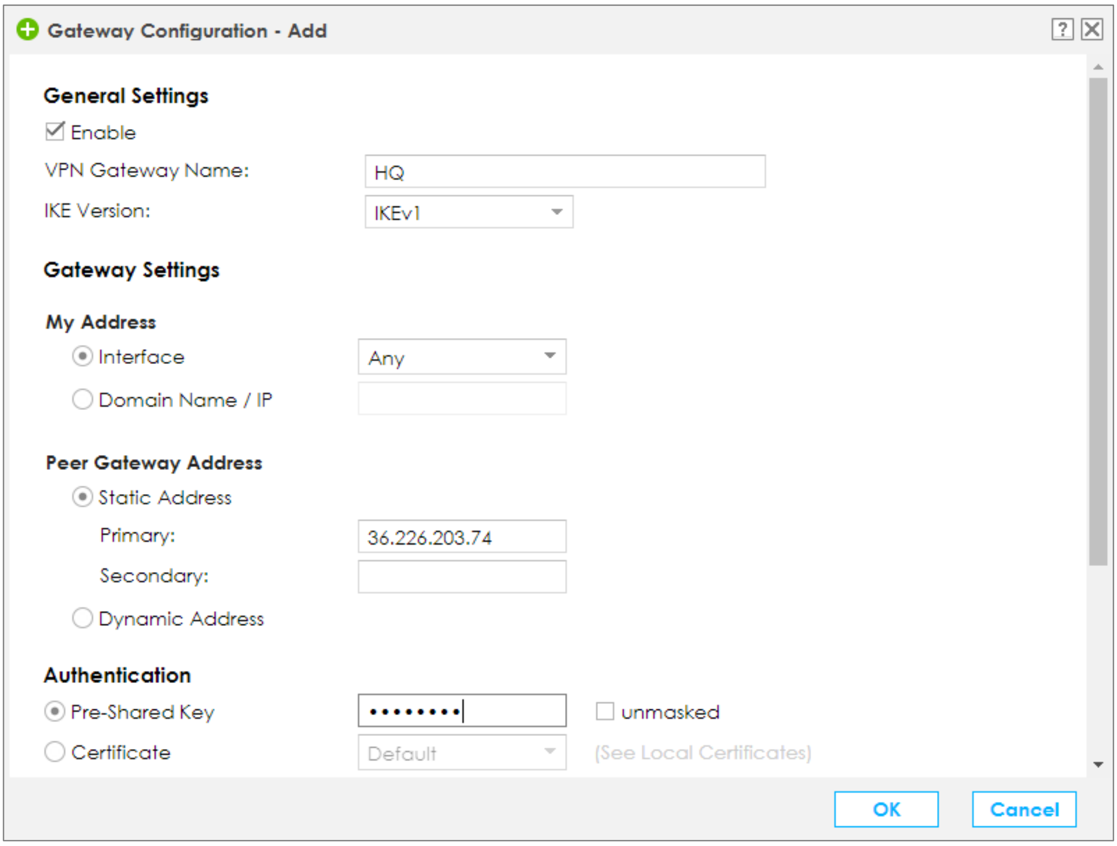
Lease Time: 1 Day 0 Hour 0 Minute(s)

DNS Server 1: DNS Proxy

Setup the VPN configuration on Branch Site

Go to **Configuration > VPN > IPSec VPN > Add** the profile on **Gateway configuration** and **Connection configuration**

For the VPN gateway, please enter the VPN gateway name, select the Interface (for public IP), enter the peer's domain in the Primary field, and enter the Pre-Shared Key.



Gateway Configuration - Add

General Settings

☑ Enable

VPN Gateway Name: HQ

IKE Version: IKEv1

Gateway Settings

My Address

● Interface: Any

○ Domain Name / IP

Peer Gateway Address

● Static Address

Primary: 36.226.203.74

Secondary:

○ Dynamic Address

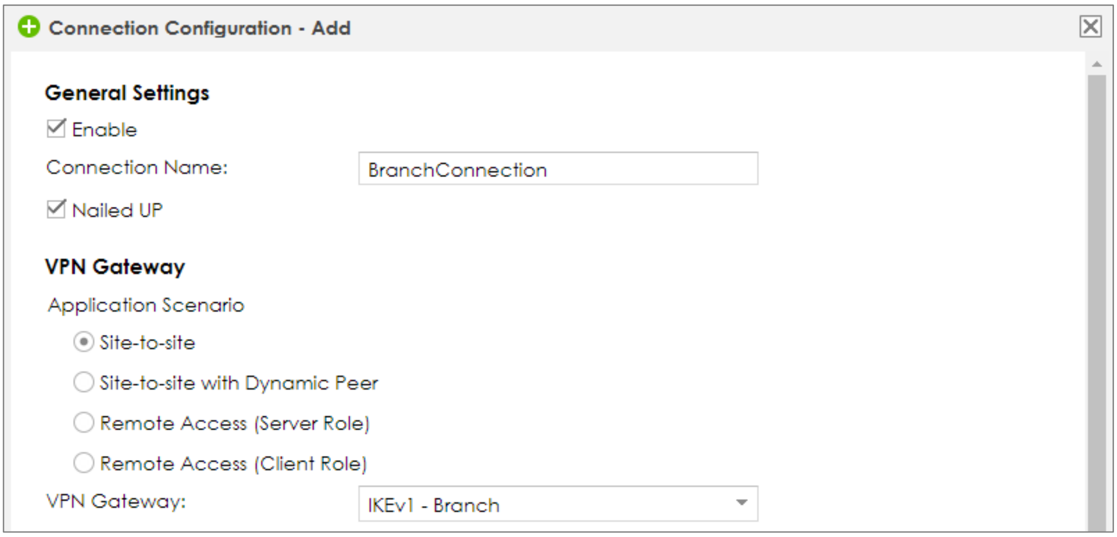
Authentication

● Pre-Shared Key: ••••••••• □ unmasked

○ Certificate: Default (See Local Certificates)

For the VPN connection (Phase 2):

3. Enter the **Connection Name**, select **Site-to-site** as the **Application Scenario**, and select the name of the phase 1 profile (**Branch**) in the **VPN Gateway** field.
4. For **Local policy**, choose the subnet that your PC is connected to.



Connection Configuration - Add

General Settings

☑ Enable

Connection Name: BranchConnection

☑ Nailed UP

VPN Gateway

Application Scenario

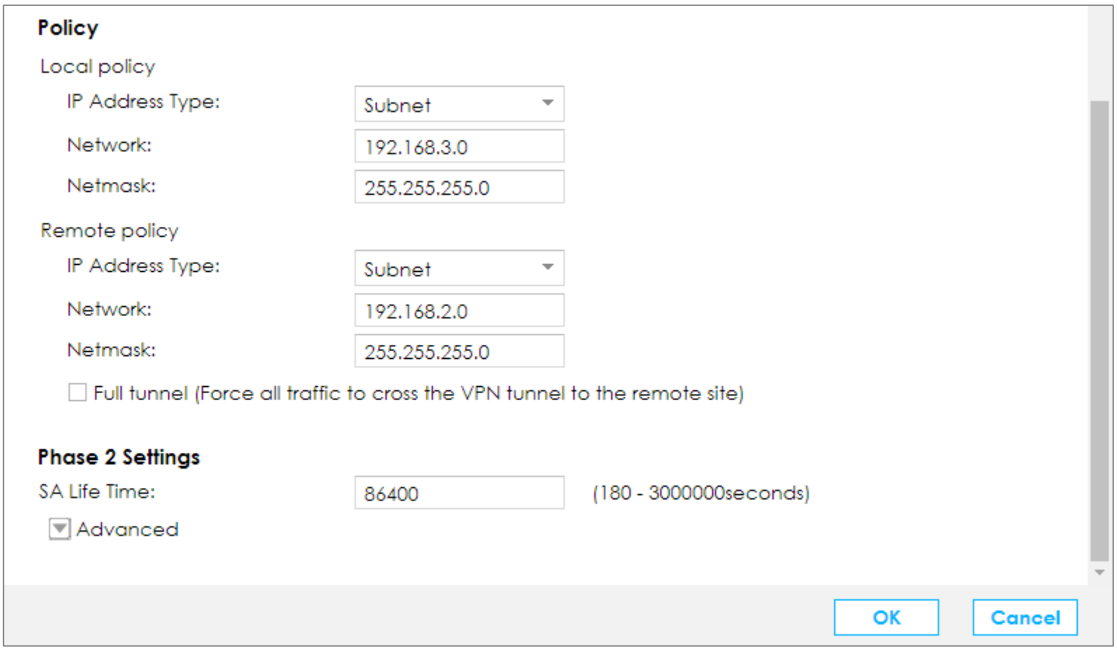
● Site-to-site

○ Site-to-site with Dynamic Peer

○ Remote Access (Server Role)

○ Remote Access (Client Role)

VPN Gateway: IKEv1 - Branch



Policy

Local policy

IP Address Type: Subnet

Network: 192.168.3.0

Netmask: 255.255.255.0

Remote policy

IP Address Type: Subnet

Network: 192.168.2.0

Netmask: 255.255.255.0

□ Full tunnel (Force all traffic to cross the VPN tunnel to the remote site)

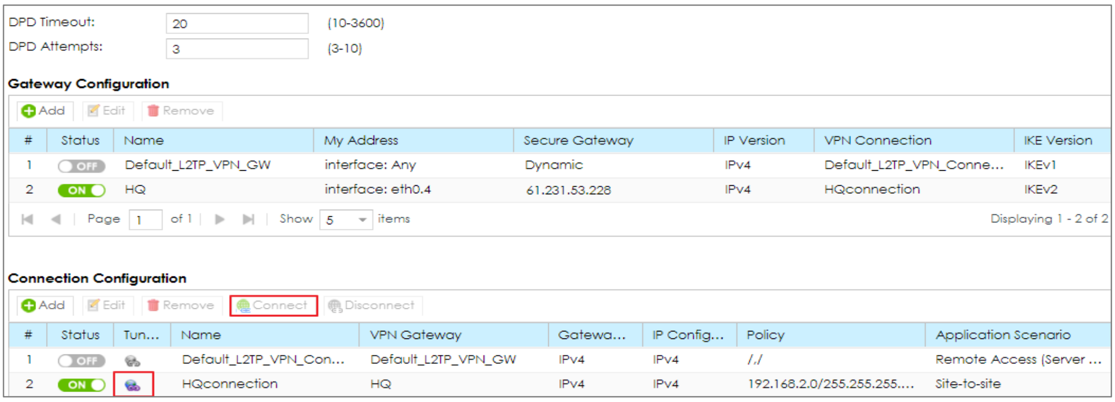
Phase 2 Settings

SA Life Time: 86400 (180 - 3000000seconds)

Advanced

Test IPSec VPN on VPN2S Series

Click the connect button, and the Icon will change from Gray to light



DPD Timeout: 20 (10-3600)

DPD Attempts: 3 (3-10)

Gateway Configuration

#	Status	Name	My Address	Secure Gateway	IP Version	VPN Connection	IKE Version
1	OFF	Default_L2TP_VPN_GW	interface: Any	Dynamic	IPv4	Default_L2TP_VPN_Conne...	IKEv1
2	ON	HQ	interface: eth0.4	61.231.53.228	IPv4	HQconnection	IKEv2

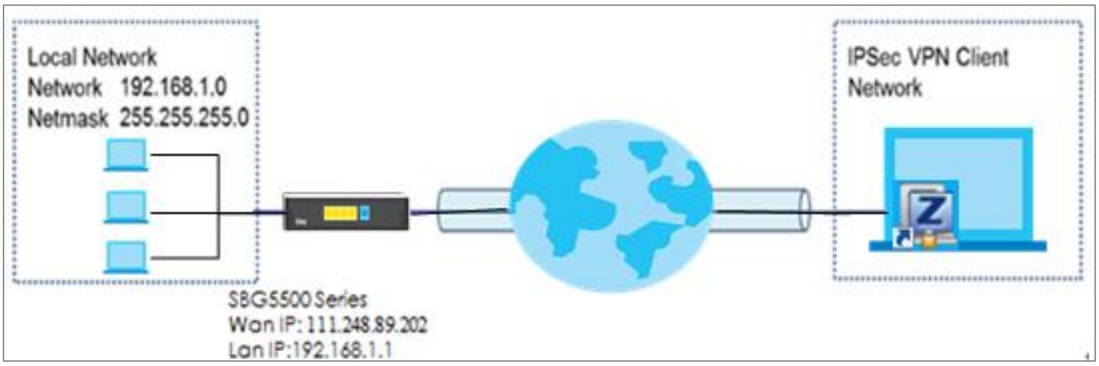
Page 1 of 1 | Show 5 items   Displaying 1 - 2 of 2

Connection Configuration

#	Status	Tun...	Name	VPN Gateway	Gatewa...	IP Config...	Policy	Application Scenario
1	OFF		Default_L2TP_VPN_Con...	Default_L2TP_VPN_GW	IPv4	IPv4	/./	Remote Access (Server ...
2	ON		HQconnection	HQ	IPv4	IPv4	192.168.2.0/255.255.255....	Site-to-site

How to configure VPN with PC -Server Role

This scenario shows how to use the VPN Setup to create a site-to-site VPN between a VPN2S 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.

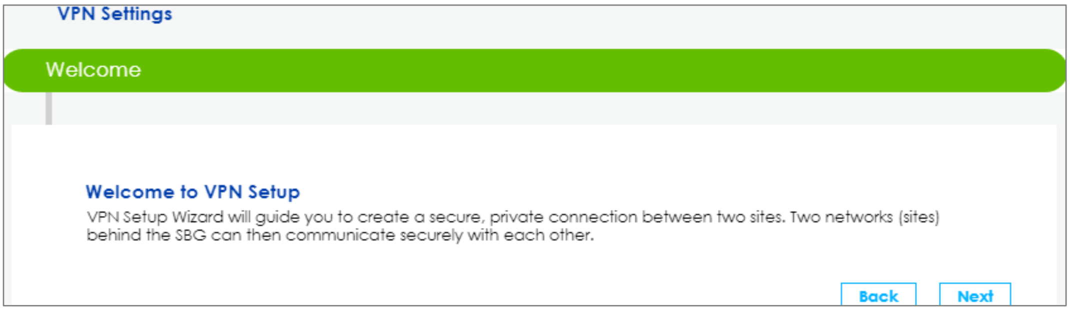


Note:
All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks.

Set Up the IPSec VPN Tunnel on the VPN2S

In the VPN2S, go to **Wizard > Welcome to IPsec VPN Setup**, 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**.

Figure Wizard > Welcome to IPsec VPN Setup



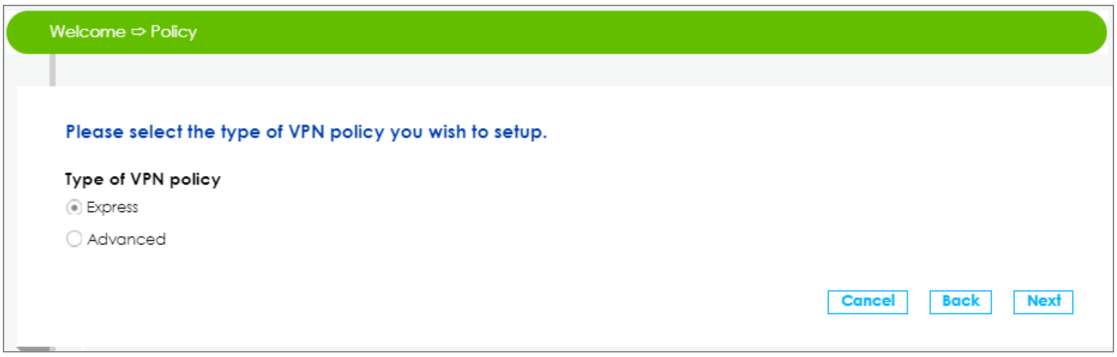
Welcome to VPN Setup

VPN Setup Wizard will guide you to create a secure, private connection between two sites. Two networks (sites) behind the SBG can then communicate securely with each other.

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**.

Figure Wizard > Welcome to IPsec VPN Setup



Welcome ⇨ Policy

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

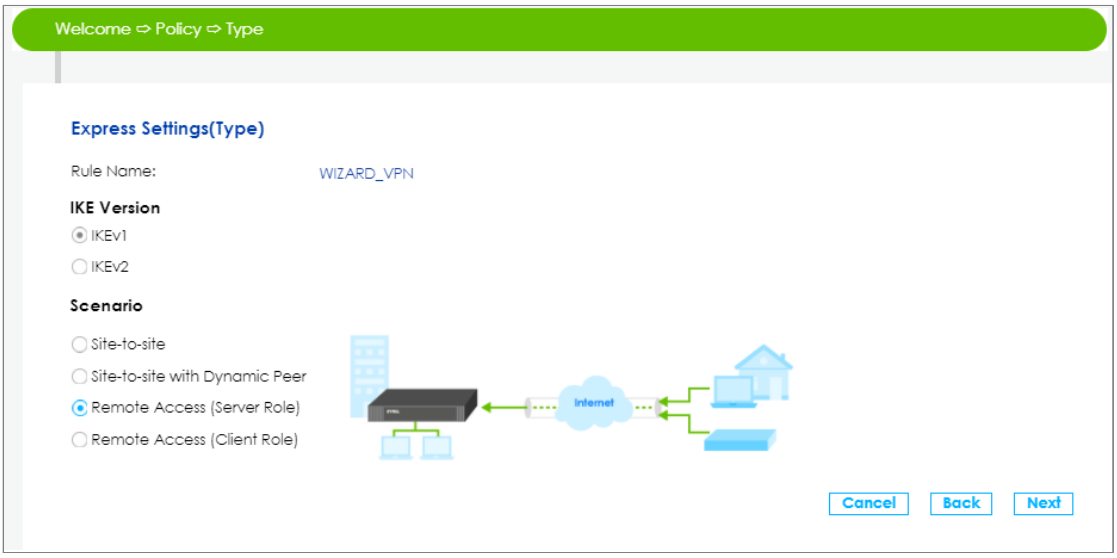
Type of VPN policy

● Express

○ Advanced

Select the Scenario which will be deployed. (Remote Access, Server Role), and click **Next.**

Figure Wizard > Welcome to IPsec VPN Setup



Welcome ⇨ Policy ⇨ Type

Express Settings(Type)

Rule Name: WIZARD_VPN

IKE Version

● IKEv1

○ IKEv2

Scenario

○ Site-to-site

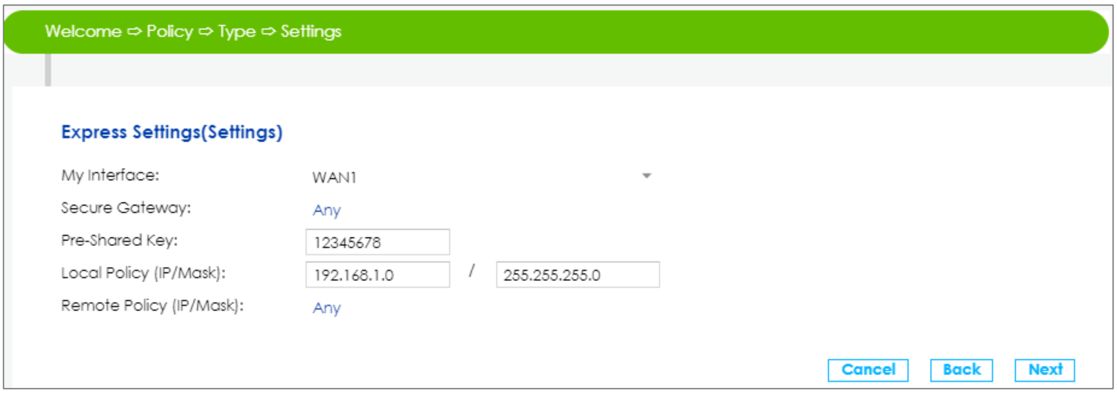
○ Site-to-site with Dynamic Peer

● Remote Access (Server Role)

○ Remote Access (Client Role)

Choose the **WAN1** for My Interface and fill pre-Shared Key and local IP Address.

Figure Wizard > Welcome to IPsec VPN Setup

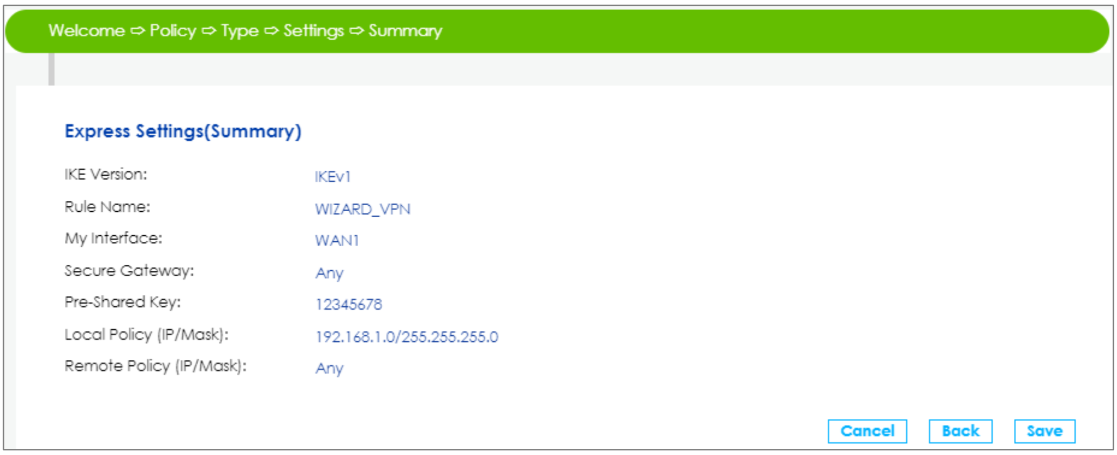


Welcome ⇨ Policy ⇨ Type ⇨ Settings

Express Settings(Settings)

My Interface:	WAN1
Secure Gateway:	Any
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.1.0 / 255.255.255.0
Remote Policy (IP/Mask):	Any

The configured result will be displayed. Click **Save**



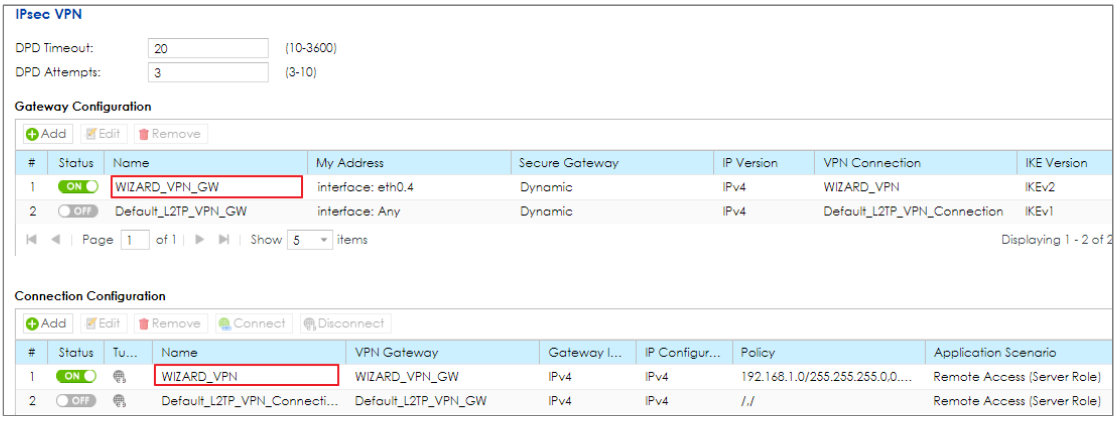
Welcome ⇨ Policy ⇨ Type ⇨ Settings ⇨ Summary

Express Settings(Summary)

IKE Version:	IKEv1
Rule Name:	WIZARD_VPN
My Interface:	WAN1
Secure Gateway:	Any
Pre-Shared Key:	12345678
Local Policy (IP/Mask):	192.168.1.0/255.255.255.0
Remote Policy (IP/Mask):	Any

And then Go to **Configuration > VPN > IPsec VPN**, the Server role already created on VPN.

Figure Configuration > VPN > IPsec VPN



IPsec VPN

DPD Timeout:	20	(10-3600)
DPD Attempts:	3	(3-10)

Gateway Configuration

#	Status	Name	My Address	Secure Gateway	IP Version	VPN Connection	IKE Version
1	ON	WIZARD_VPN_GW	interface: eth0.4	Dynamic	IPv4	WIZARD_VPN	IKEv2
2	OFF	Default_L2TP_VPN_GW	interface: Any	Dynamic	IPv4	Default_L2TP_VPN_Connection	IKEv1

Page 1 of 1 | Show 5 items Displaying 1 - 2 of 2

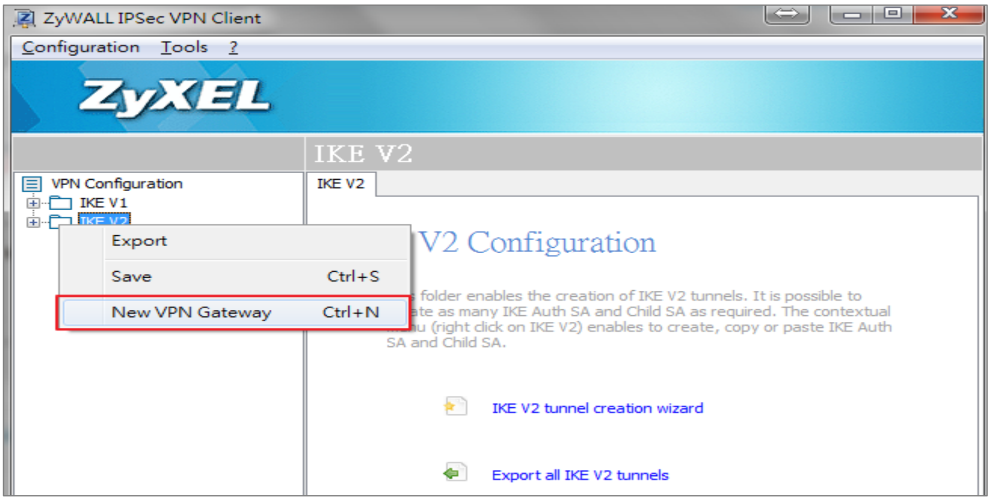
Connection Configuration

#	Status	Tu...	Name	VPN Gateway	Gateway I...	IP Configur...	Policy	Application Scenario
1	ON		WIZARD_VPN	WIZARD_VPN_GW	IPv4	IPv4	192.168.1.0/255.255.255.0,0....	Remote Access (Server Role)
2	OFF		Default_L2TP_VPN_Connecti...	Default_L2TP_VPN_GW	IPv4	IPv4	/,/	Remote Access (Server Role)

Setup the Zywall IPsec VPN client

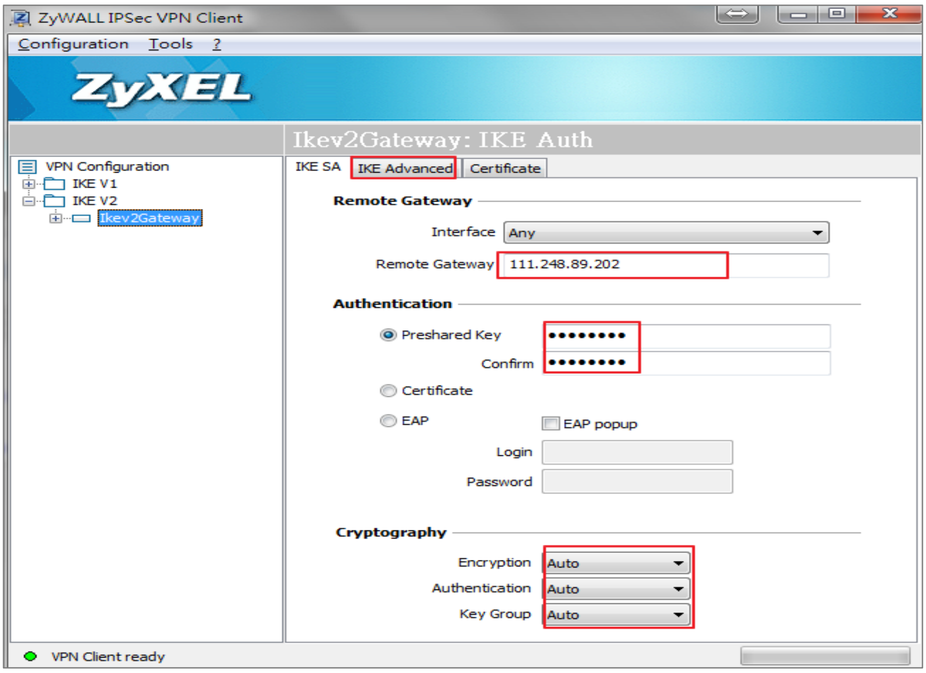
Since the IKE Version 2 is using, so the **New VPN Gateway** need to be added on IKEV2 on IPSec VPN Client.

Figure IPSec VPN Client



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

Fill **Remote Gateway** IP address and pre-shared key, and then move to **IKE Advance**



Remote Gateway

Interface: Any

Remote Gateway: 111.248.89.202

Authentication

● Preshared Key: ••••••••

Confirm: ••••••••

○ Certificate

○ EAP □ EAP popup

Login:

Password:

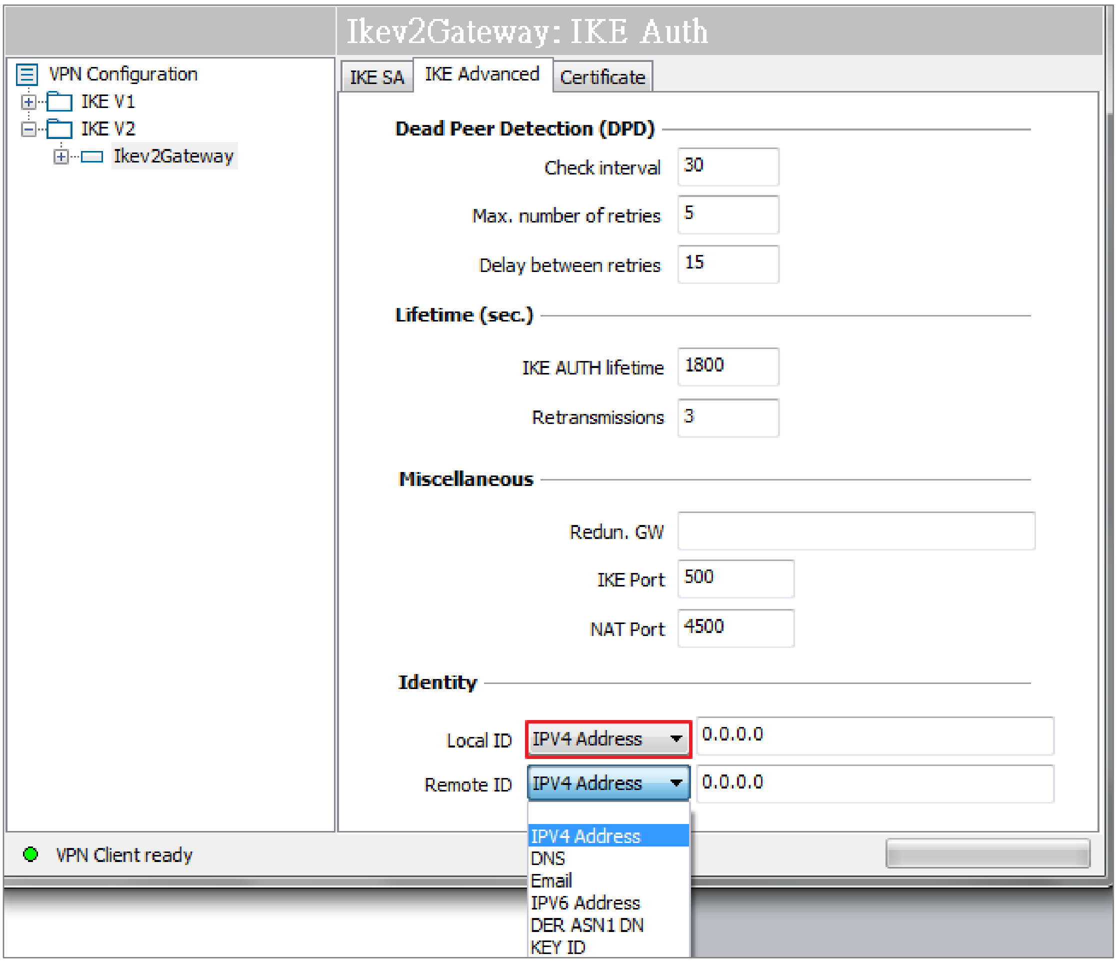
Cryptography

Encryption: Auto

Authentication: Auto

Key Group: Auto

On the IKE Advance page, Select **IPV4 Address** and fill **0.0.0.0** on **local and Remote ID.**



Ikev2Gateway: IKE Auth

Dead Peer Detection (DPD)

Check interval: 30

Max. number of retries: 5

Delay between retries: 15

Lifetime (sec.)

IKE AUTH lifetime: 1800

Retransmissions: 3

Miscellaneous

Redun. GW:

IKE Port: 500

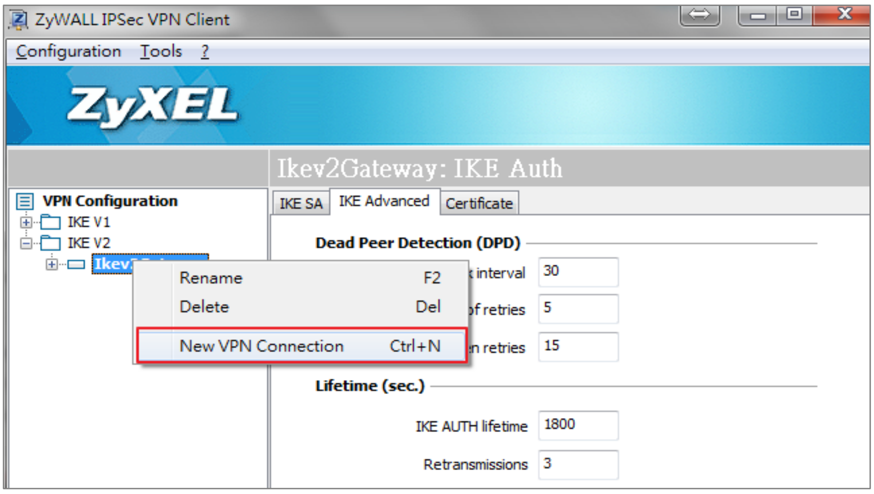
NAT Port: 4500

Identity

Local ID: IPV4 Address 0.0.0.0

Remote ID: IPV4 Address 0.0.0.0

After that, create the New VPN Connection



Dead Peer Detection (DPD)

interval: 30

of retries: 5

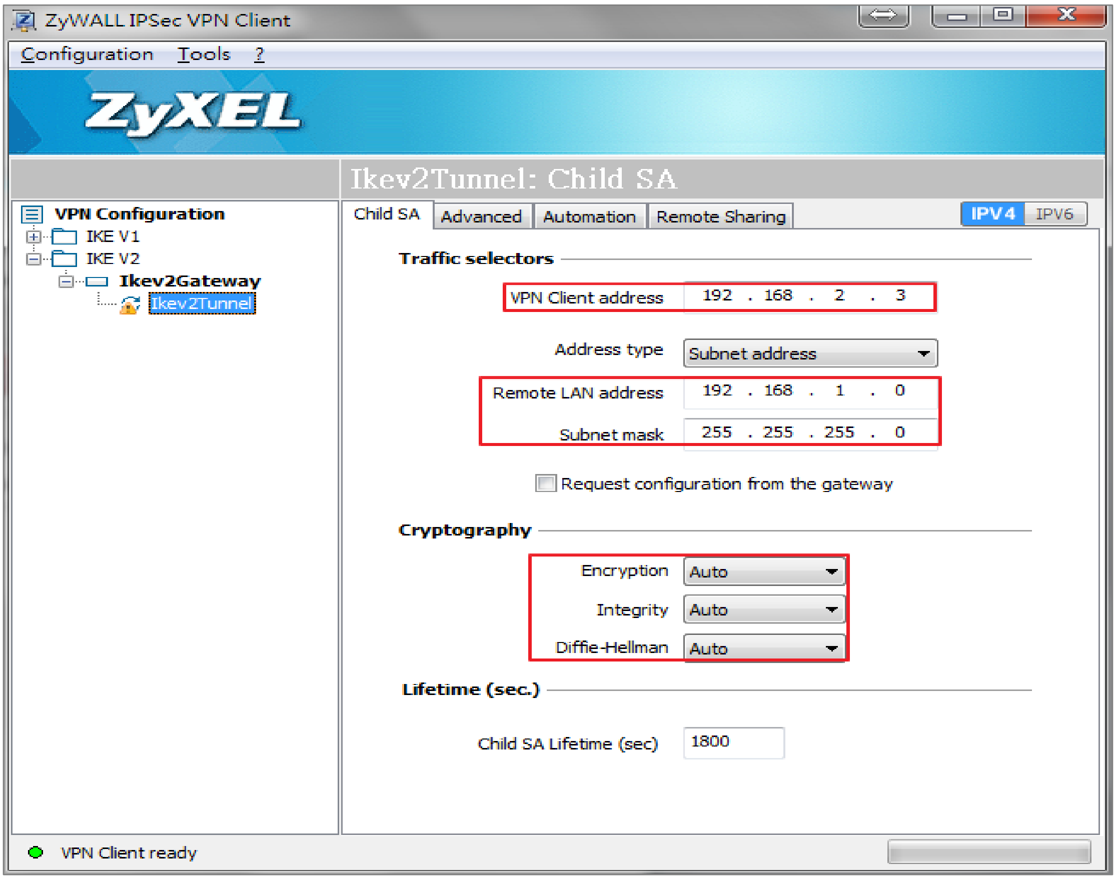
n retries: 15

Lifetime (sec.)

IKE AUTH lifetime: 1800

Retransmissions: 3

On the IKev2 Tunnel, please fill in **VPN Client address** and **Remote LAN address**



Ikev2Tunnel: Child SA

Traffic selectors

VPN Client address 192 . 168 . 2 . 3

Address type Subnet address

Remote LAN address 192 . 168 . 1 . 0

Subnet mask 255 . 255 . 255 . 0

□ Request configuration from the gateway

Cryptography

Encryption Auto

Integrity Auto

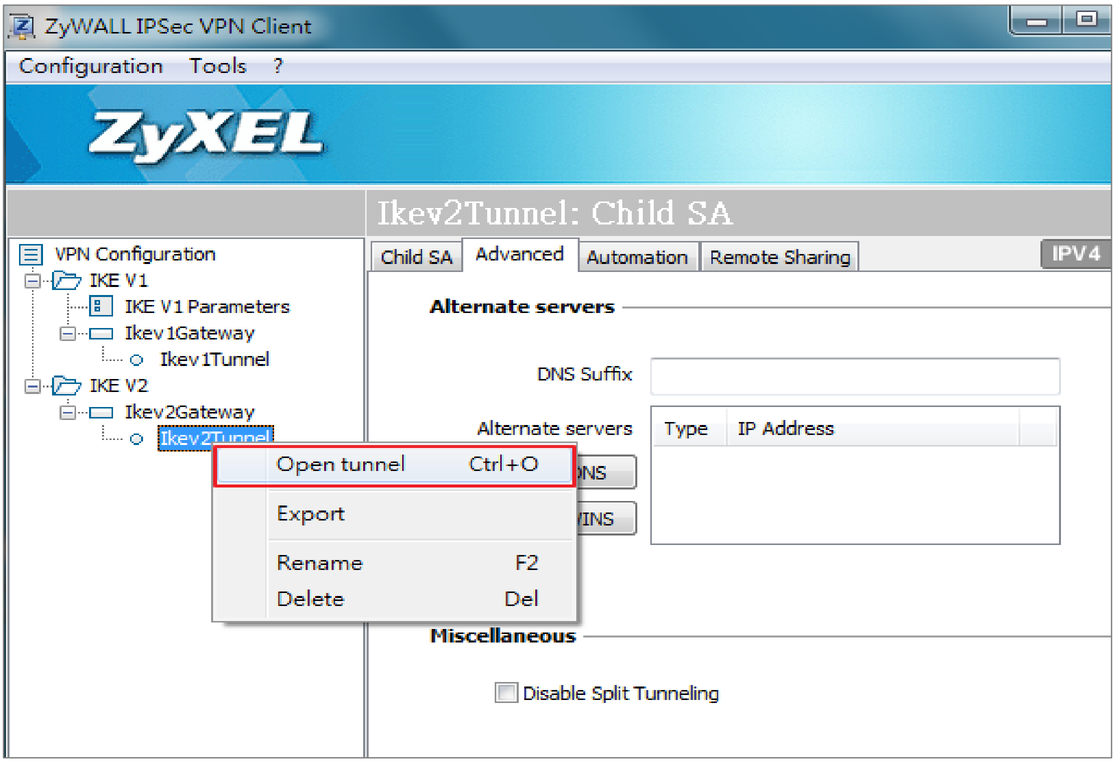
Diffie-Hellman Auto

Lifetime (sec.)

Child SA Lifetime (sec) 1800

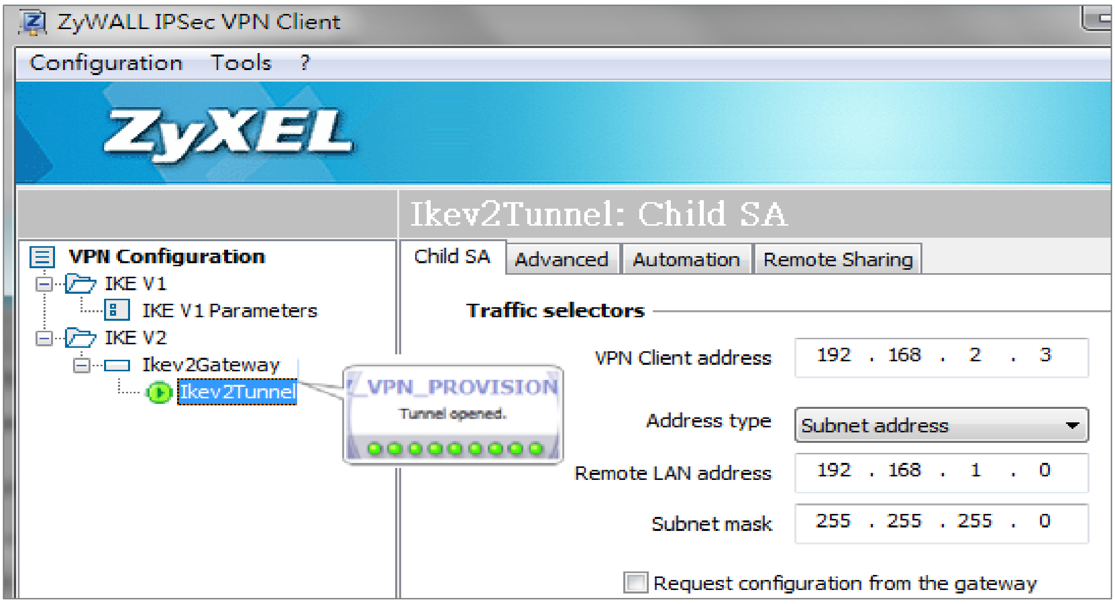
Test VPN2S as Server Role

Click Open Tunnel



□ Disable Split Tunneling

The Tunnel established



VPN Client address 192 . 168 . 2 . 3

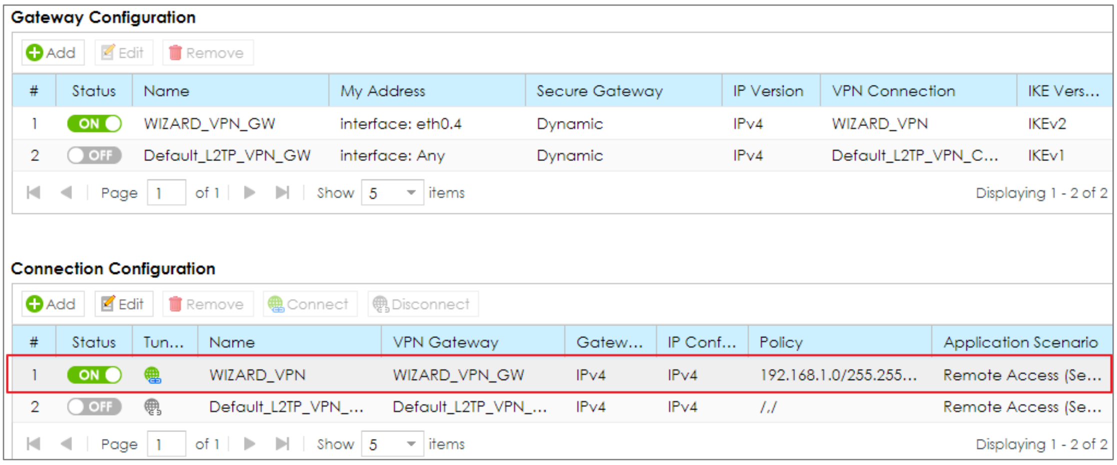
Address type Subnet address

Remote LAN address 192 . 168 . 1 . 0

Subnet mask 255 . 255 . 255 . 0

□ Request configuration from the gateway

The result is displayed on VPN on VPN2S



Gateway Configuration

#	Status	Name	My Address	Secure Gateway	IP Version	VPN Connection	IKE Vers...
1	ON	WIZARD_VPN_GW	interface: eth0.4	Dynamic	IPv4	WIZARD_VPN	IKEv2
2	OFF	Default_L2TP_VPN_GW	interface: Any	Dynamic	IPv4	Default_L2TP_VPN_C...	IKEv1

Connection Configuration

#	Status	Tun...	Name	VPN Gateway	Gatew...	IP Conf...	Policy	Application Scenario
1	ON		WIZARD_VPN	WIZARD_VPN_GW	IPv4	IPv4	192.168.1.0/255.255...	Remote Access (Se...
2	OFF		Default_L2TP_VPN_...	Default_L2TP_VPN_...	IPv4	IPv4	/./	Remote Access (Se...

How to setup scheduled rule via firewall on VPN2S

This example will illustrate the VPN2S User Access Control allows IT manager arrange Internet access schedule to limit specific or all LAN PC Internet access time.

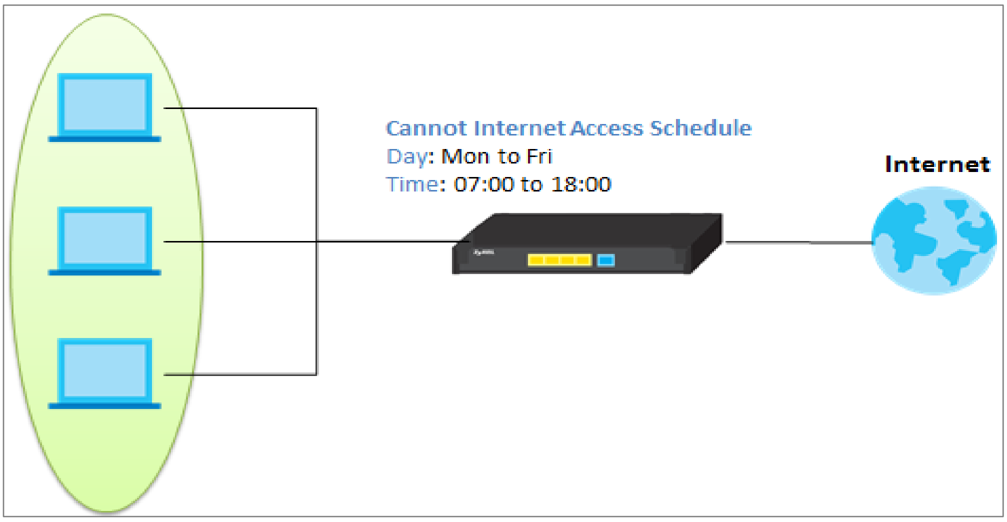


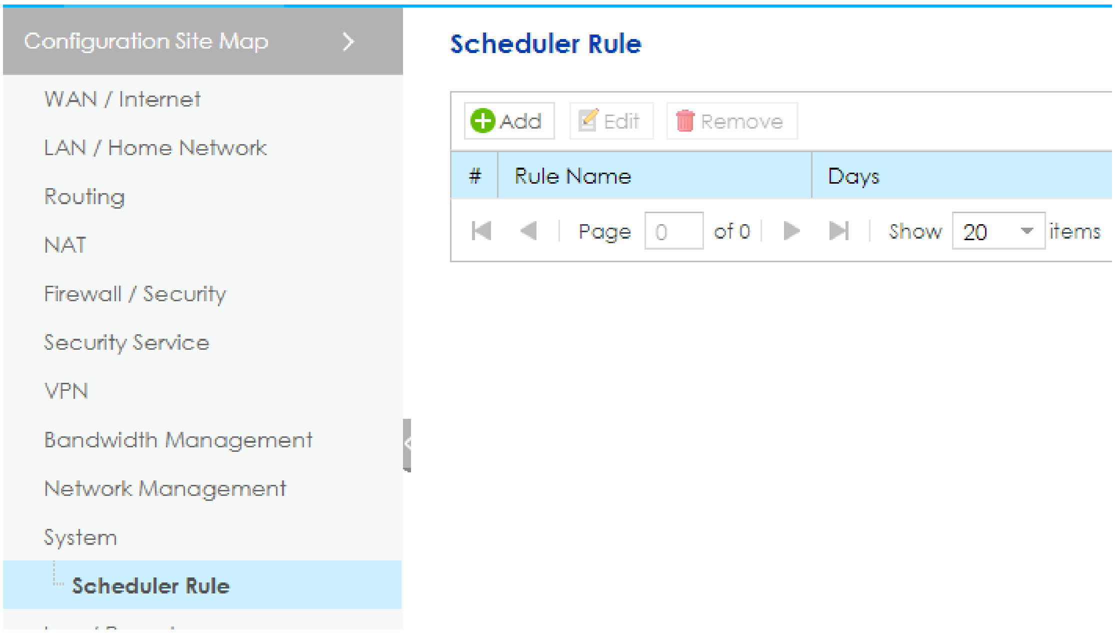
Figure User Access Control

Note:
The rules of internet access schedule related with device need to be double checked by IT Manager.

Setup the schedule rule on the VPN2S

Go to **System** > **Scheduler Rule** > **Add**
Fill the name of the schedule rule and tick **Mon to Fri** on the Days field.
On the Time of Day Range, enter **7:00 to 18:00**. Click **OK**.

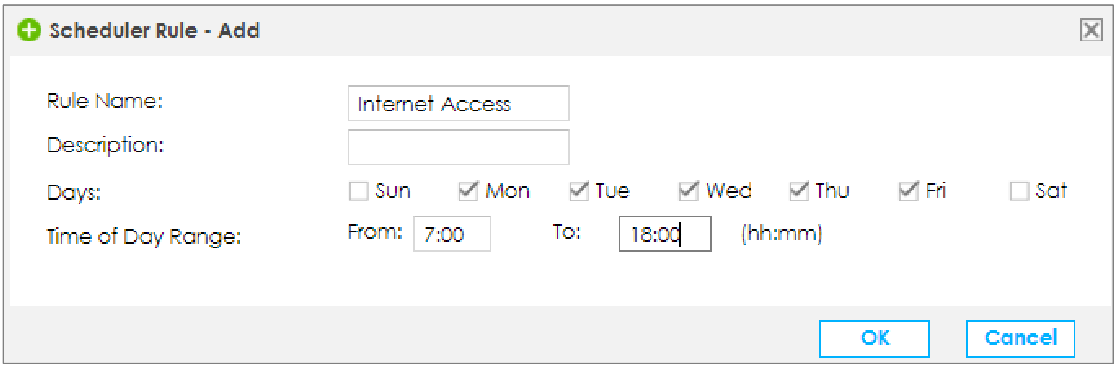
Figure Schedule Rule



#	Rule Name	Days

Page 0 of 0 Show 20 items

Figure Schedule Rule

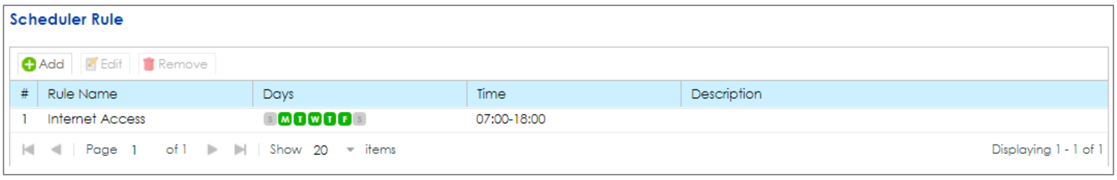


Rule Name: Internet Access

Description:

Days: □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Time of Day Range: From: 7:00 To: 18:00 (hh:mm)



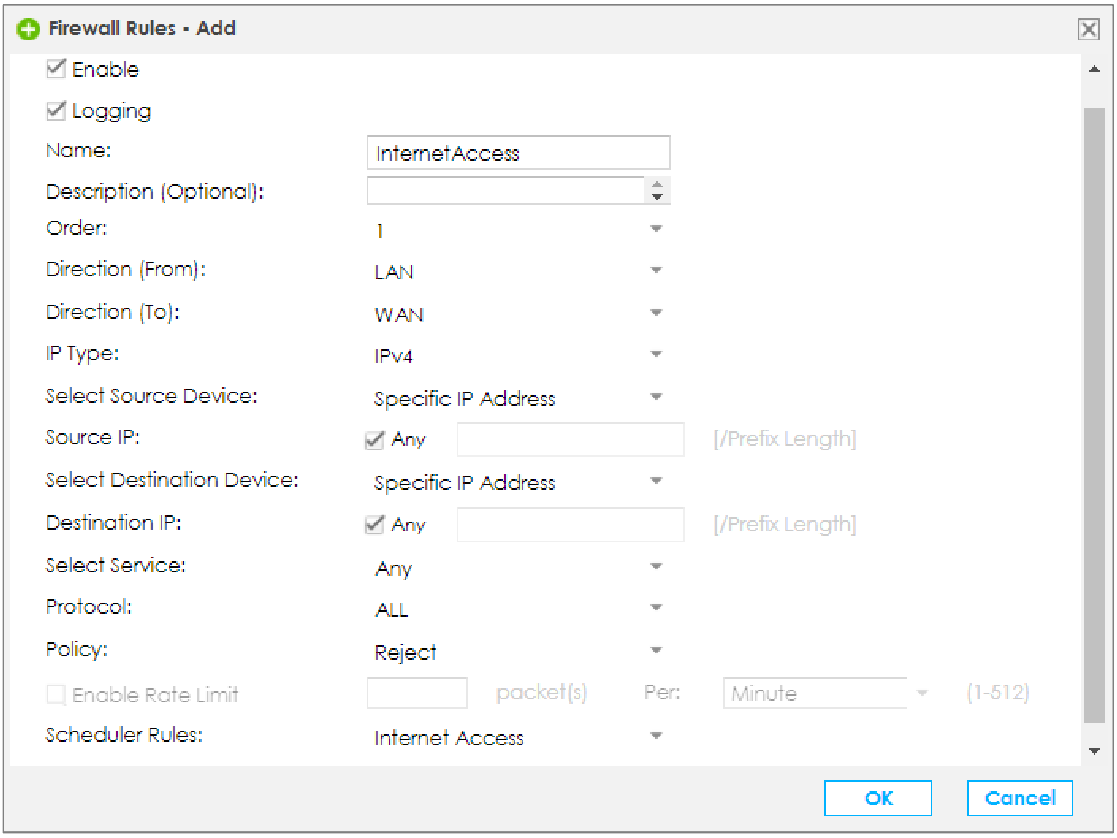
#	Rule Name	Days	Time	Description
1	Internet Access	S M T W T F S	07:00-18:00	

Page 1 of 1 Show 20 items Displaying 1 - 1 of 1

Move to **Firewall/Security >Firewall Rules > Add**, Create the Firewall Rule which related with Schedule rule.

Check **Enable**, fill the name of rule, and check **Any** to limit all device in the schedule. Choose **REJECT** as your policy. Select **Internet Access** which created on schedule rule.

Figure Firewall/Security >Firewall Rules > Add



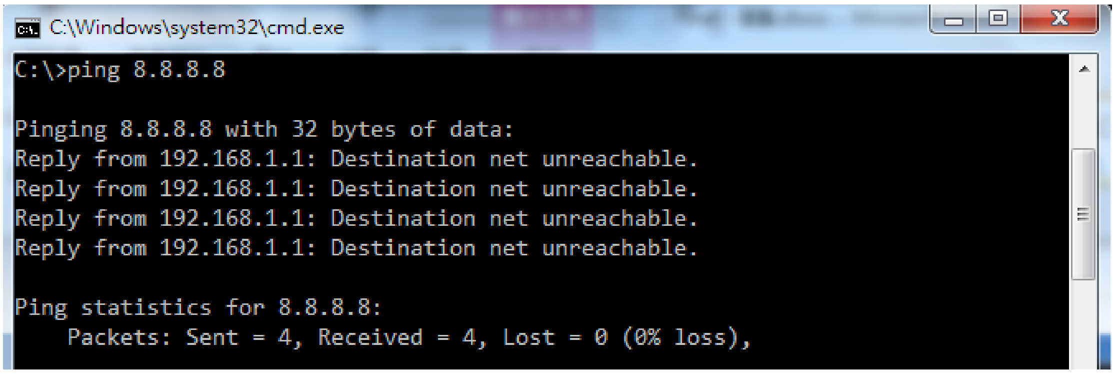
Firewall Rules - Add

☑ Enable

☑ Logging

Name:	InternetAccess
Description (Optional):	
Order:	1
Direction (From):	LAN
Direction (To):	WAN
IP Type:	IPv4
Select Source Device:	Specific IP Address
Source IP:	☑ Any [/Prefix Length]
Select Destination Device:	Specific IP Address
Destination IP:	☑ Any [/Prefix Length]
Select Service:	Any
Protocol:	ALL
Policy:	Reject
□ Enable Rate Limit	packet(s) Per: Minute (1-512)
Scheduler Rules:	Internet Access

Test scheduled rule via firewall on VPN2S

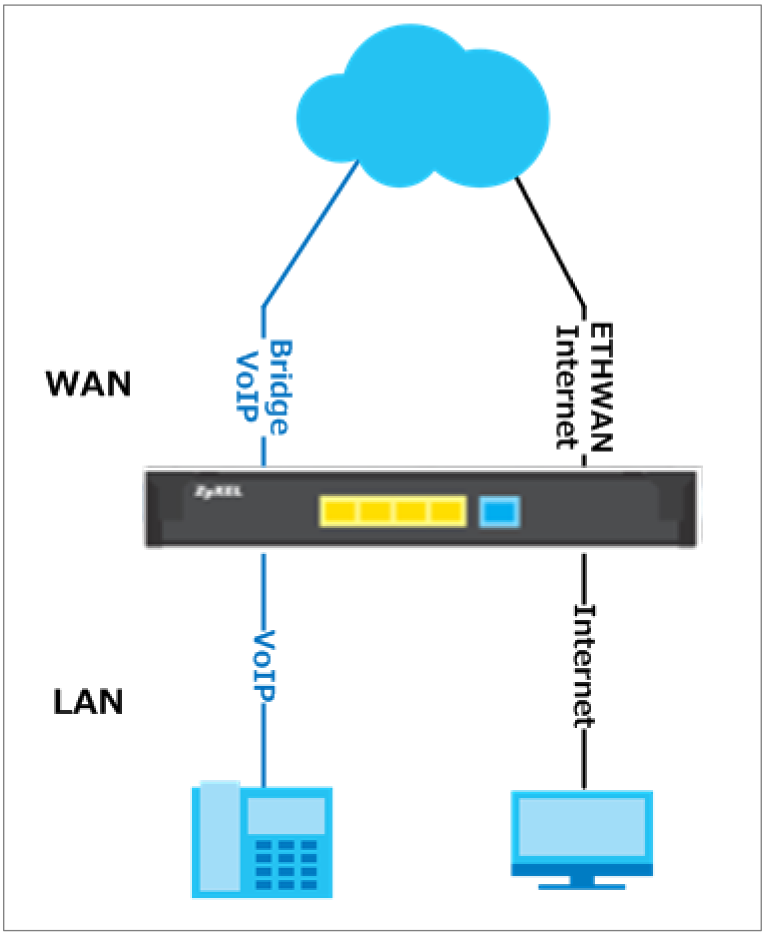


```
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.1.1: Destination net unreachable.
Reply from 192.168.1.1: Destination net unreachable.
Reply from 192.168.1.1: Destination net unreachable.
Reply from 192.168.1.1: Destination net unreachable.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

How to Configure Interface Group Bridge / Bundle WAN Interface (Triple play)

This example shows how to use the Interface Group. There are Internet and VoIP, connections. The Interface Group VoIP should be bridge to WAN interface VoIP. When the Interface Group is configured, Internet and VoIP traffic can be isolated and VoIP can be use L2 traffic to the WAN interface

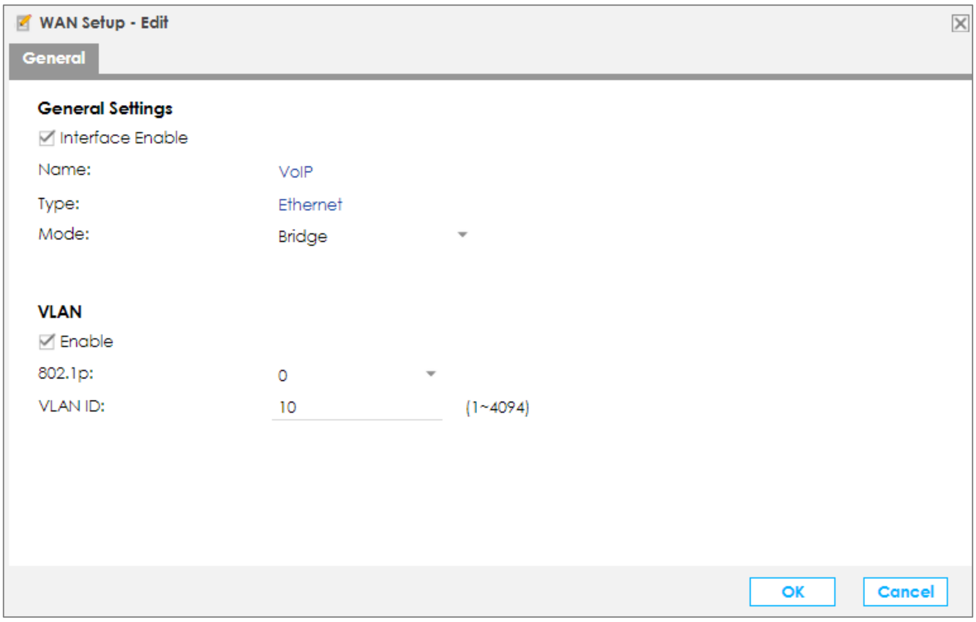
Figure Interface Group Bridge / Bundle WAN Interface



Set Up the Interface Group Bridge / Bundle WAN Interface Group on the VPN2S.

Sign into the VPN2S. Go to LAN / Home Network > VLAN / Interface Group

Click Configuration > WAN / Internet > WAN Setup > Add to open the follow screen.



WAN Setup - Edit

General

General Settings

☑ Interface Enable

Name: VoIP

Type: Ethernet

Mode: Bridge

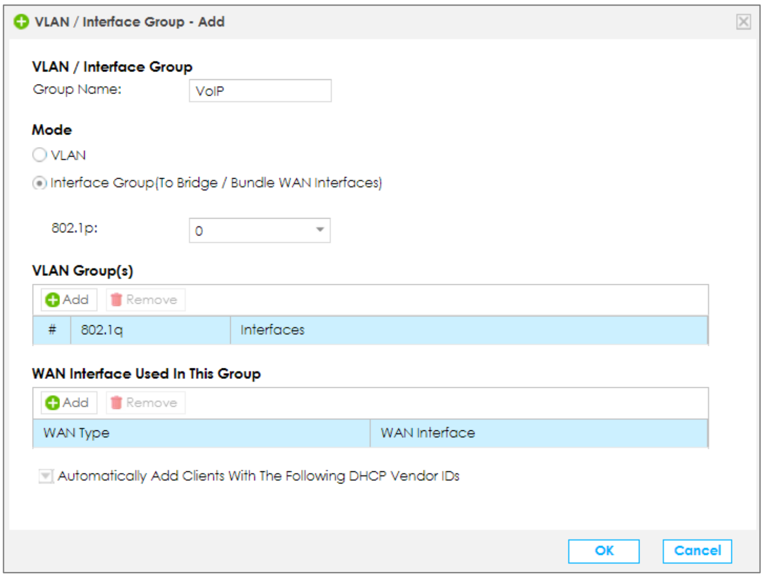
VLAN

☑ Enable

802.1p: 0

VLAN ID: 10 (1~4094)

Click Configuration > LAN / Home Network > VLAN / Interface Group > Add to open the follow screen.



VLAN / Interface Group - Add

VLAN / Interface Group

Group Name: VoIP

Mode

○ VLAN

● Interface Group(To Bridge / Bundle WAN Interfaces)

802.1p: 0

VLAN Group(s)

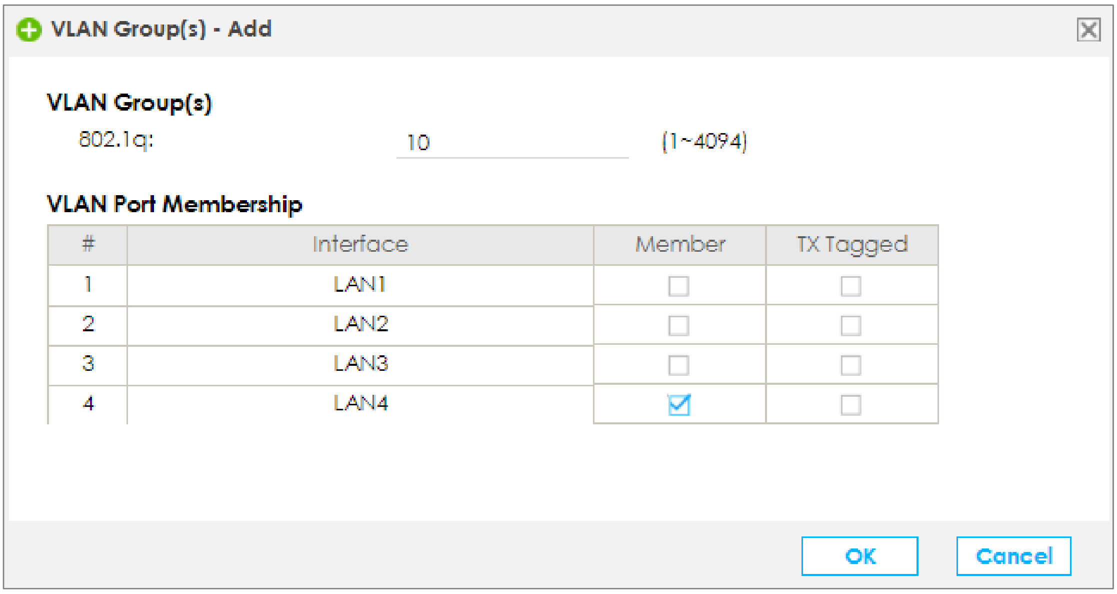
#	802.1q	Interfaces

WAN Interface Used In This Group

WAN Type	WAN Interface

□ Automatically Add Clients With The Following DHCP Vendor IDs

Click Configuration > LAN / Home Network > VLAN / Interface Group > Add > VLAN Group(s) Add to open the follow screen.



VLAN Group(s) - Add

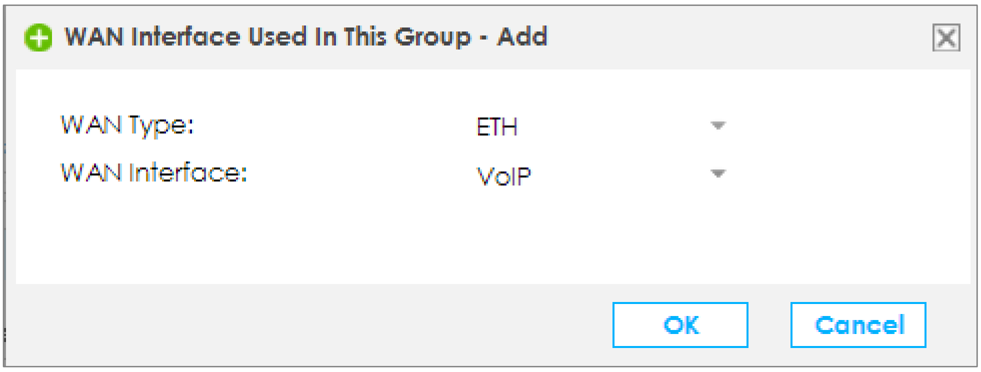
VLAN Group(s)

802.1q: 10 (1~4094)

VLAN Port Membership

#	Interface	Member	TX Tagged
1	LAN1	□	□
2	LAN2	□	□
3	LAN3	□	□
4	LAN4	☑	□

Click Configuration > LAN / Home Network > VLAN / Interface Group > Add > **WAN Interface Used In This Group** Add to open the follow screen.

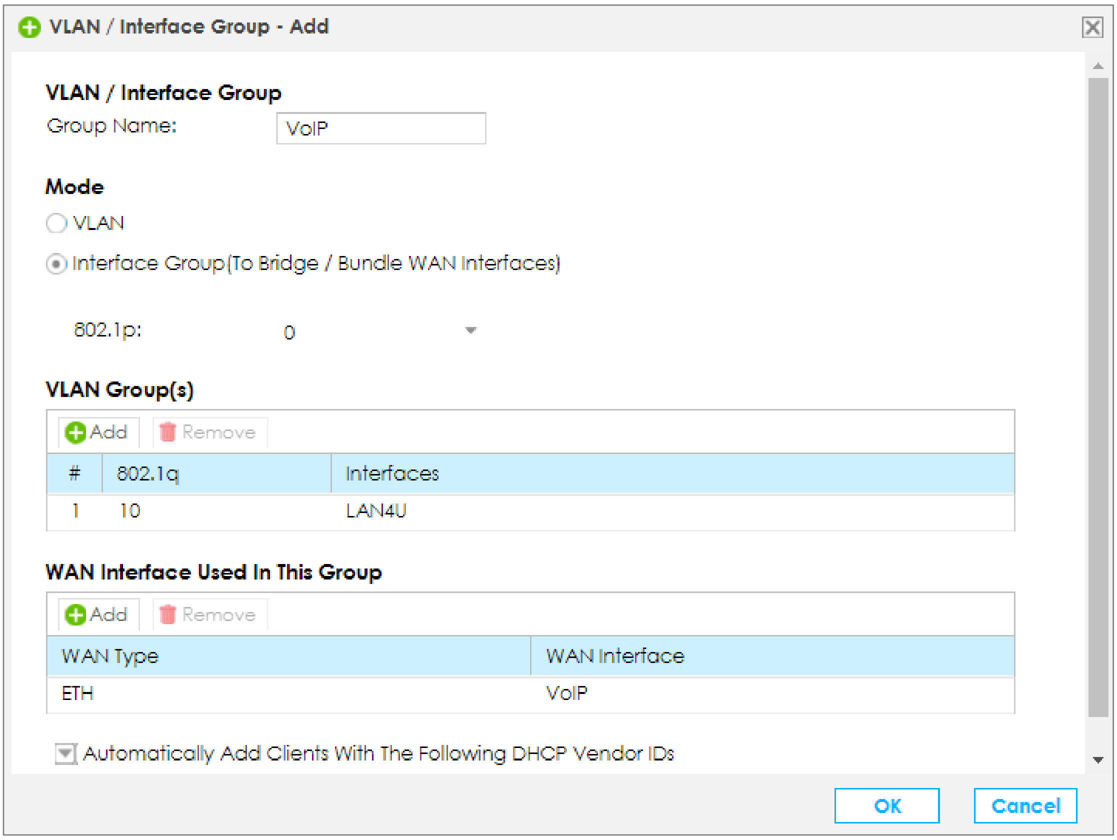


WAN Interface Used In This Group - Add

WAN Type: ETH

WAN Interface: VoIP

Click Configuration > LAN / Home Network > VLAN / Interface Group > Add to open the follow screen.



VLAN / Interface Group - Add

VLAN / Interface Group

Group Name: VoIP

Mode

○ VLAN

● Interface Group(To Bridge / Bundle WAN Interfaces)

802.1p: 0

VLAN Group(s)

#	802.1q	Interfaces
1	10	LAN4U

WAN Interface Used In This Group

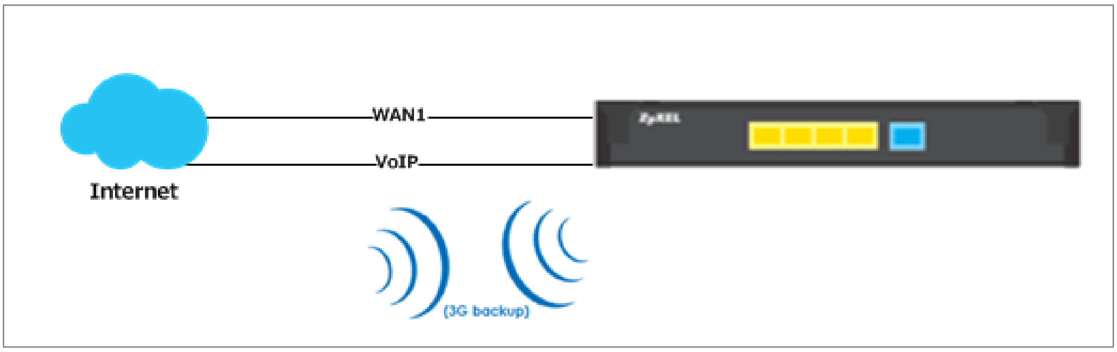
WAN Type	WAN Interface
ETH	VoIP

Automatically Add Clients With The Following DHCP Vendor IDs

How to configure Multi-WAN

This example shows how to use the Multi-WAN, there are WAN1, VoIP, Mobile connections. The bandwidth for the WAN1 :100M, VoIP:20M. The ratio should be 5:1 on WAN1 and VoIP. The Mobile connection is WAN backup, since most Mobile connection charge the user more cost.

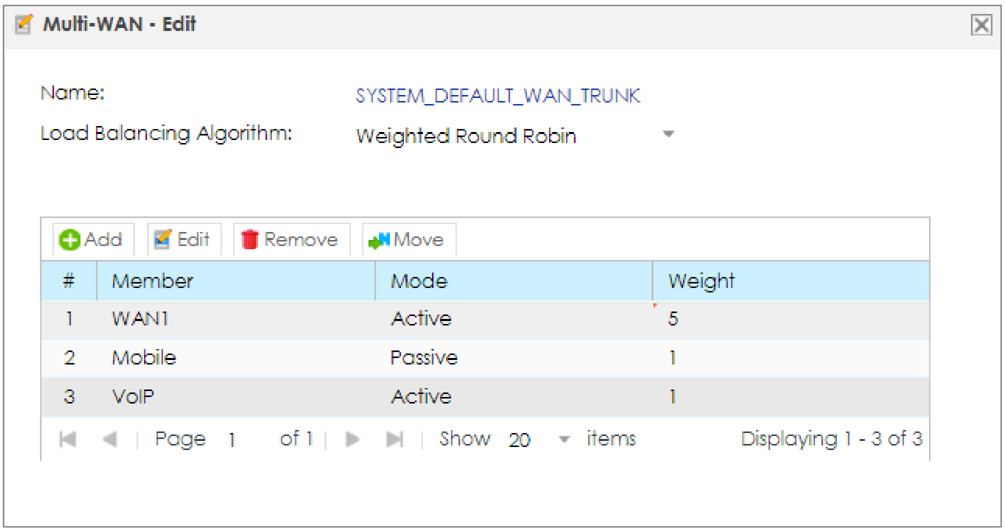
Figure Multi-WAN



Set Up the Multi-WAN on the VPN2S.

Sign into the VPN2S. Go to Configuration > WAN / Internet > Multi-WAN

Click Configuration > WAN / Internet > Multi-WAN > Edit open the follow screen.



Name: SYSTEM_DEFAULT_WAN_TRUNK

Load Balancing Algorithm: Weighted Round Robin

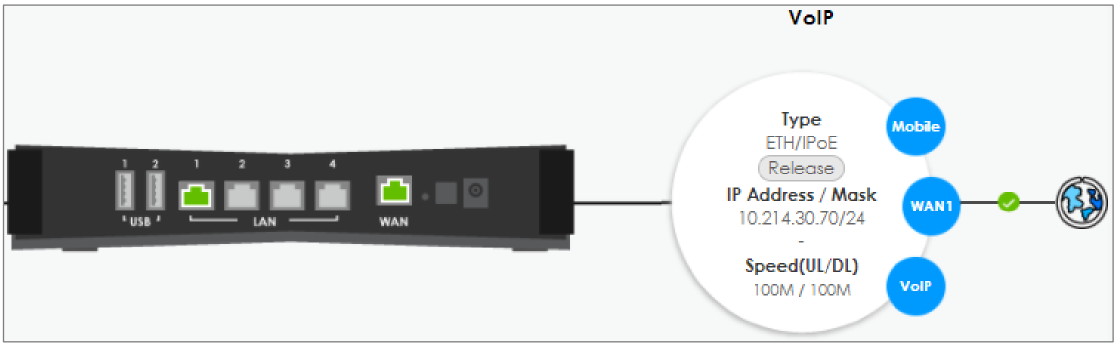
#	Member	Mode	Weight
1	WAN1	Active	5
2	Mobile	Passive	1
3	VoIP	Active	1

Page 1 of 1 | Show 20 items | Displaying 1 - 3 of 3

Check the Multi-WAN status

VoIP connection

Click Dashboard open the follow screen.

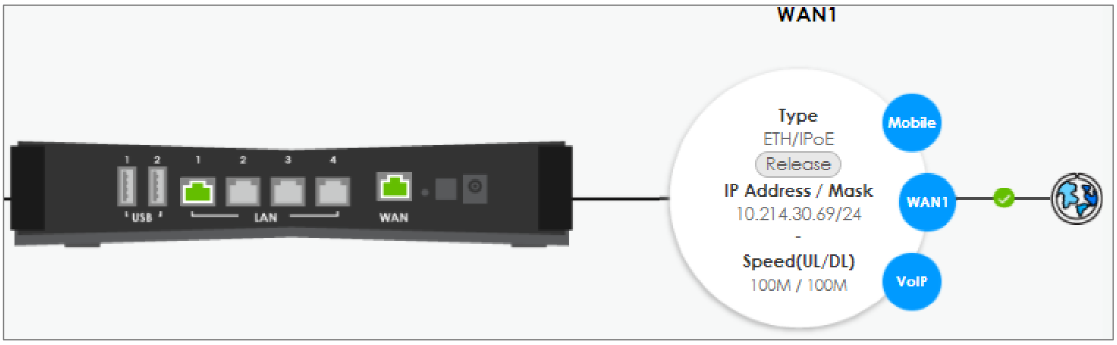


VoIP

Type
ETH/IPoE
Release
IP Address / Mask
10.214.30.70/24
-
Speed(UL/DL)
100M / 100M

WAN1 connection

Click Dashboard open the follow screen.

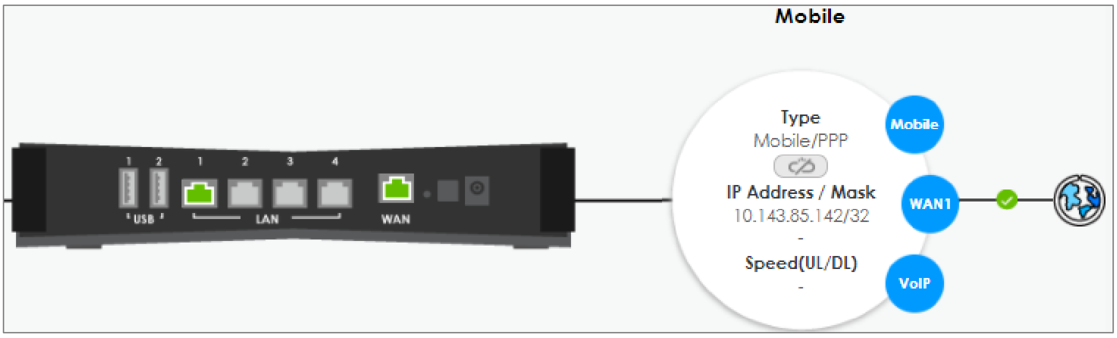


WAN1

Type
ETH/IPoE
Release
IP Address / Mask
10.214.30.69/24
-
Speed(UL/DL)
100M / 100M

Mobile 3G connection

Click Dashboard open the follow screen.



Mobile

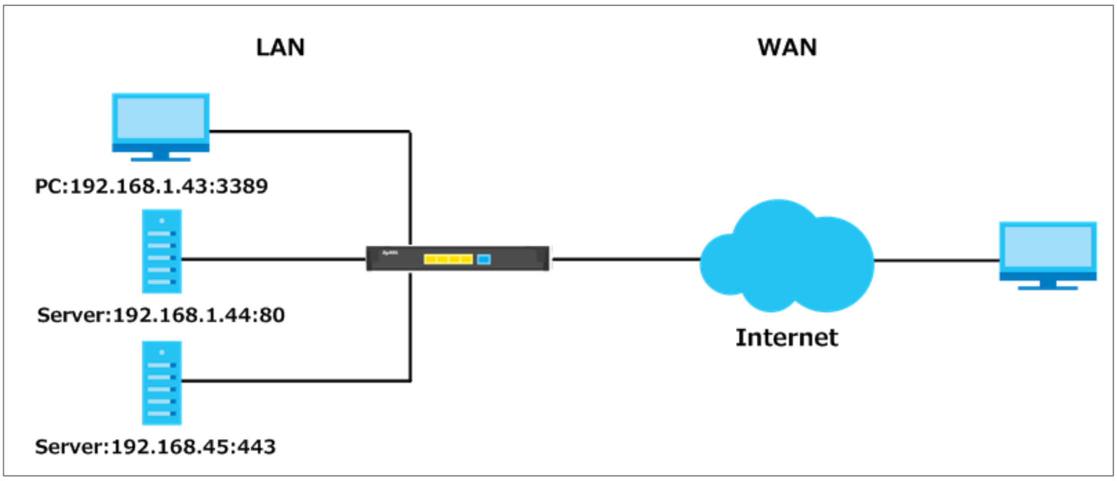
Type
Mobile/PPP
IP Address / Mask
10.143.85.142/32
-
Speed(UL/DL)
-

How to Configure NAT Port Forwarding

This example shows how to use the Port Forwarding to access local server. The example instructs how to configure the Port Forwarding. When the Port

Forwarding is configured, each server can be accessed from Internet.

Figure Multiple Servers Behind NAT Example



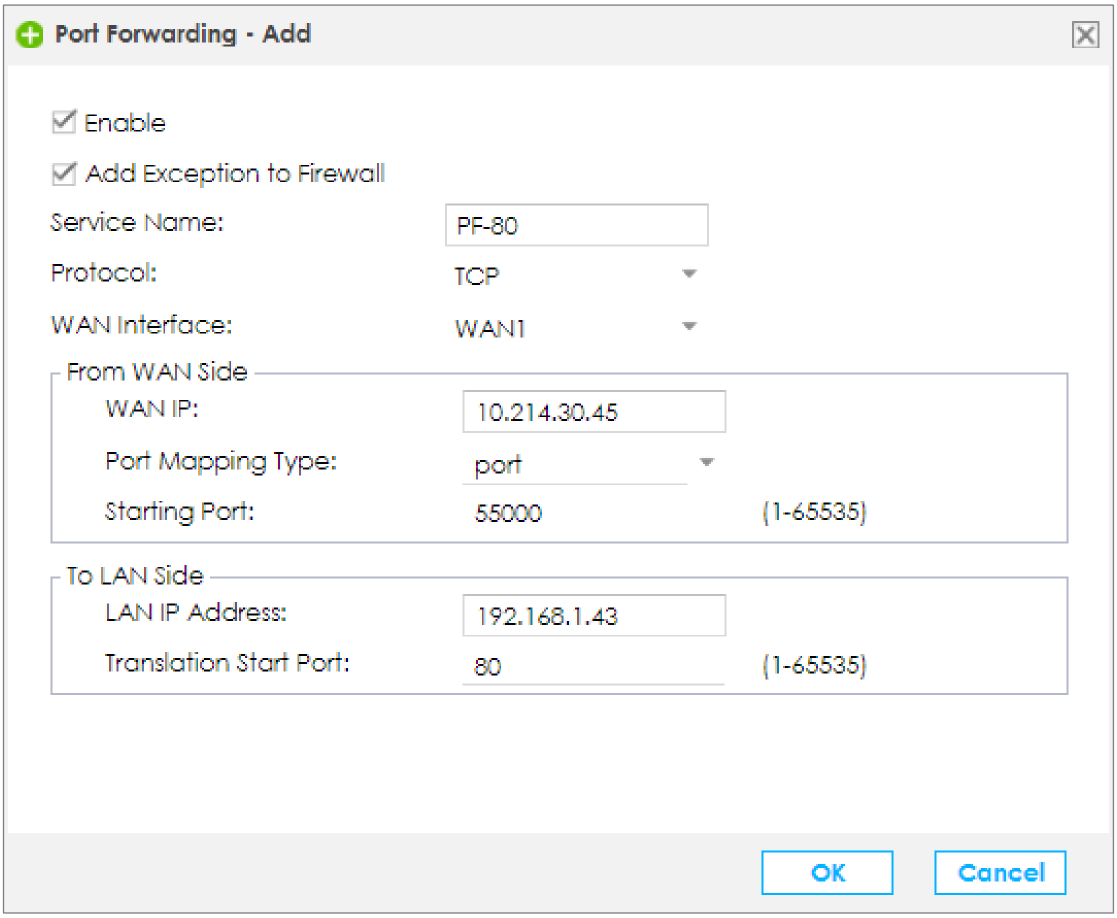
Note:

1. The TCP port is reserved for TR069 connection request port.

Set Up the Port Forwarding on the VPN2S.

Sign into the VPN2S. Go to NAT > Port Forwarding

Click Configuration > NAT > Port Forwarding > Add to open the follow screen.



Port Forwarding - Add

☑ Enable

☑ Add Exception to Firewall

Service Name:	PF-80	
Protocol:	TCP	
WAN Interface:	WAN1	

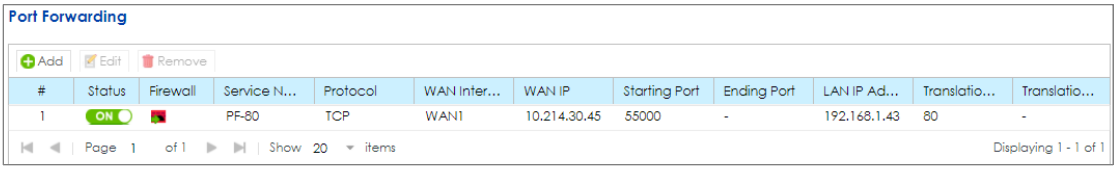
From WAN Side

WAN IP:	10.214.30.45	
Port Mapping Type:	port	
Starting Port:	55000	(1-65535)

To LAN Side

LAN IP Address:	192.168.1.43	
Translation Start Port:	80	(1-65535)

Click Configuration > NAT > Port Forwarding open the follow screen.



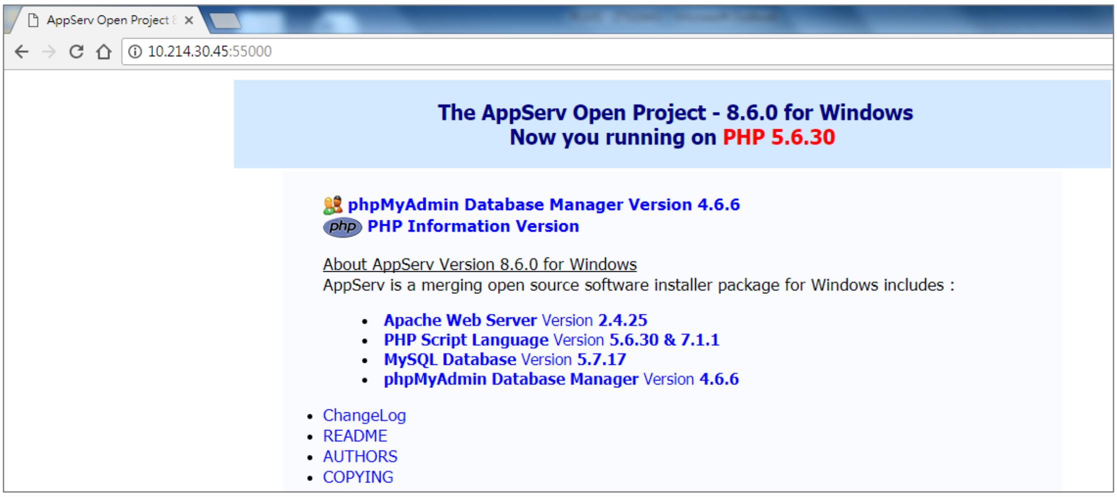
Port Forwarding

#	Status	Firewall	Service N...	Protocol	WAN Inter...	WAN IP	Starting Port	Ending Port	LAN IP Ad...	Translatio...	Translatio...
1	ON	🟥	PF-80	TCP	WAN1	10.214.30.45	55000	-	192.168.1.43	80	-

Page 1 of 1 | Show 20 items | Displaying 1 - 1 of 1

Test the Port Forwarding

Connect to http://10.214.30.45:55000 will access Server B 192.168.1.43:80



The AppServ Open Project - 8.6.0 for Windows
Now you running on PHP 5.6.30

phpMyAdmin Database Manager Version 4.6.6
PHP Information Version

About AppServ Version 8.6.0 for Windows
AppServ is a merging open source software installer package for Windows includes :

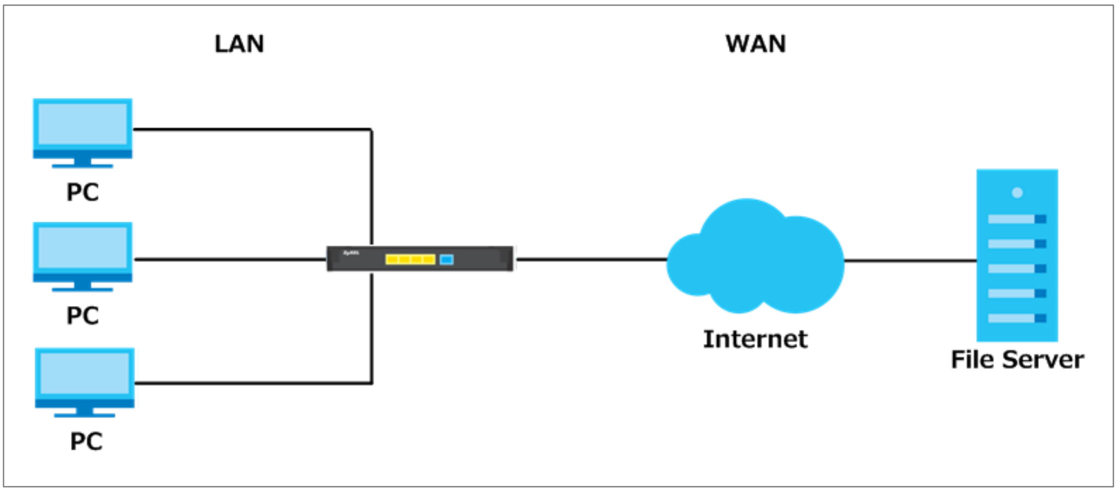
- Apache Web Server Version 2.4.25
- PHP Script Language Version 5.6.30 & 7.1.1
- MySQL Database Version 5.7.17
- phpMyAdmin Database Manager Version 4.6.6

- ChangeLog
- README
- AUTHORS
- COPYING

How to Configure NAT Port Triggering

This example shows how to create a Port Triggering on the VPN2S. The example instructs how to configure the Port Triggering. When Port Triggering is opened, File Server will forward to the open port. .

Trigger Port Forwarding Process: Example



Note:

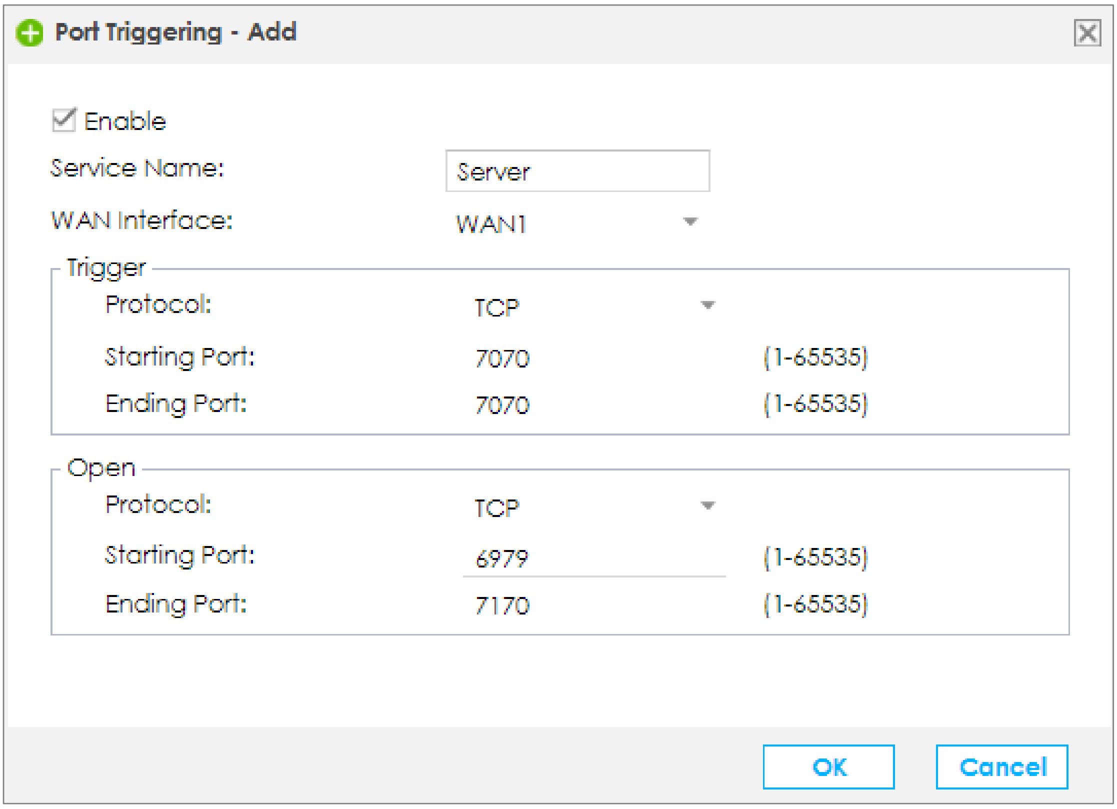
1. Only one PC can connect to the File Server until the connection is closed or time out.
2. The times out in three minutes with UDP or two hours with TCP/IP.

Set Up the Port Triggering on the VPN2S

In the VPN2S, go to NAT > Port Triggering.

.

Click Configuration > NAT > Port Triggering > Add to open the follow screen.



Port Triggering - Add

☑ Enable

Service Name: Server

WAN Interface: WAN1

Trigger

Protocol: TCP

Starting Port: 7070 (1-65535)

Ending Port: 7070 (1-65535)

Open

Protocol: TCP

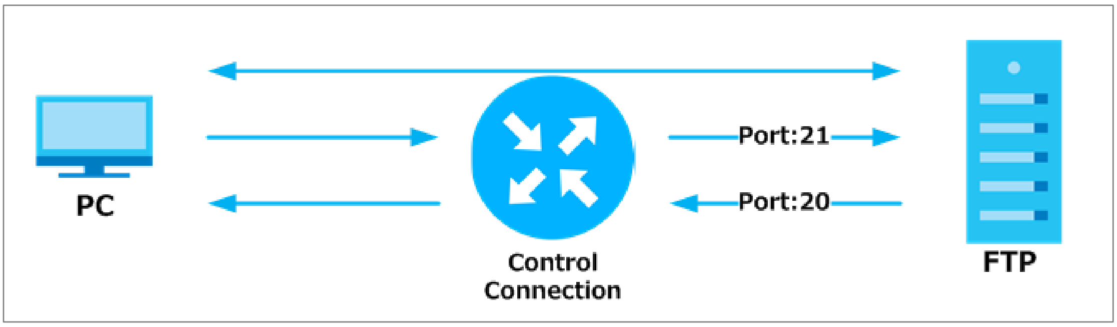
Starting Port: 6979 (1-65535)

Ending Port: 7170 (1-65535)

How to Enable NAT ALG

This example shows how to create NAT ALG on the VPN2S. The example instructs how to configure the NAT ALG. When the NAT ALG is configured, will solve major problem for peer-to-peer communication in NAT

Figure FTP ALG



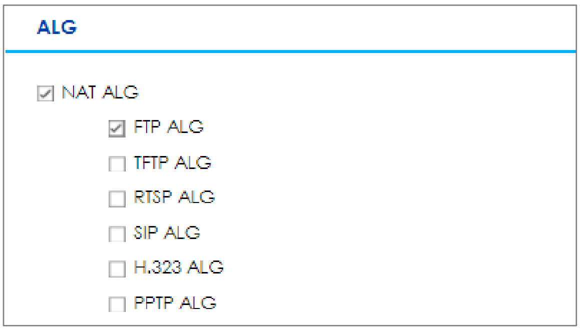
Note:

1. Mack sure ALG works correctly with port-forwarding and address mapping rules.

Enable the ALG on the VPN2S

1. In the VPN2S, go to NAT > ALG.

.Click Configuration > NAT > ALG open the follow screen.



ALG

☑ NAT ALG

☑ FTP ALG

□ TFTP ALG

□ RTSP ALG

□ SIP ALG

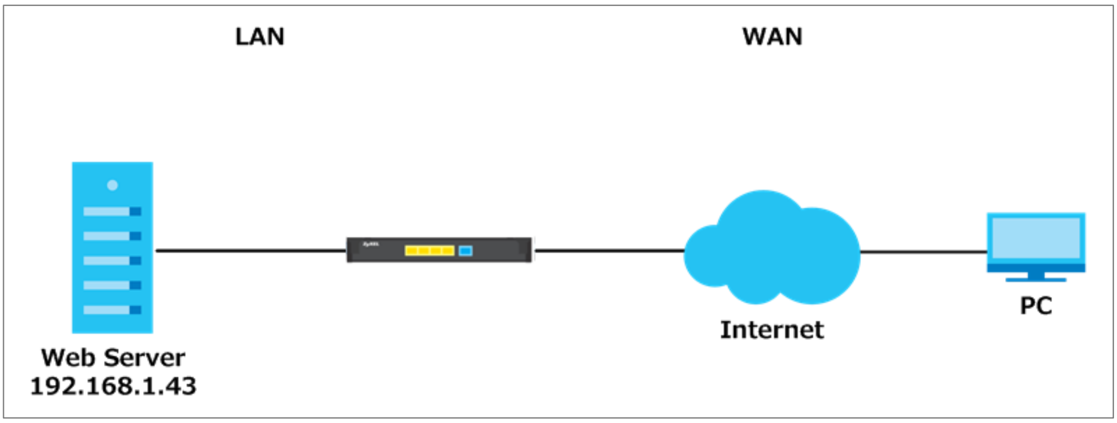
□ H.323 ALG

□ PPTP ALG

How to Configure NAT Default Server

This example shows how to create Default Server on the VPN2S. The example instructs how to configure the Default Server. When the Default Server is configured, each Internet PC can be accessed Web Server.

Figure Default Server



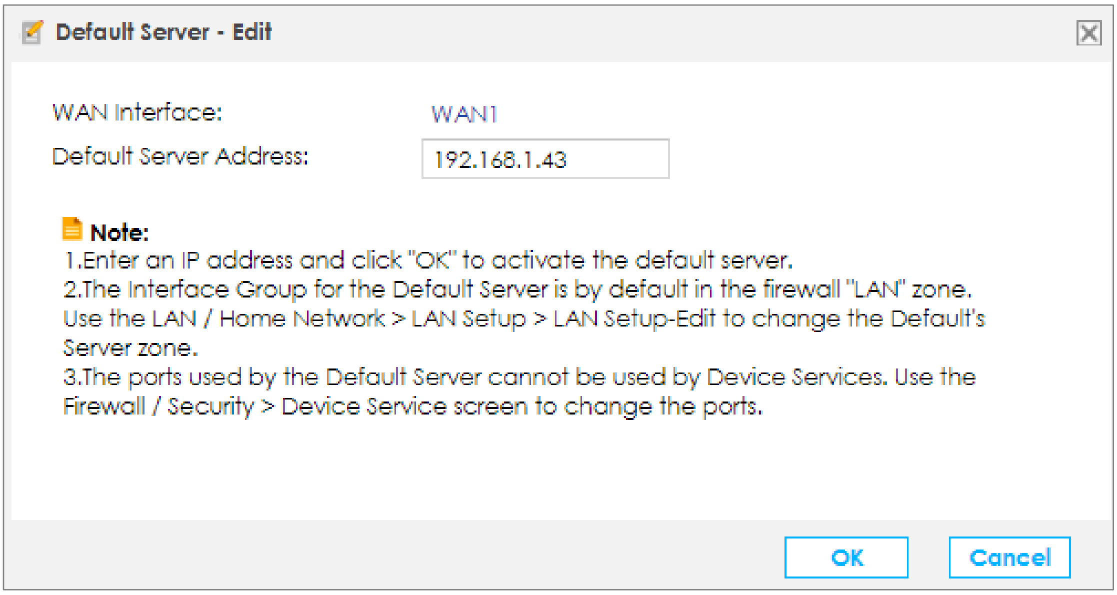
Note:

1. Enter IP address and click "OK" to activate the default server.
2. The Interface Group for the default server is by default on firewall "LAN" zone. Use LAN to configure it to other zone, if desired.
3. Some default ports of services are already used by device service. If you need the same ports for the default server, please change the ports used by device service from Firewall / Security > Device Service.

Set Up the Default Server on the VPN2S

1. In the VPN2S, go to NAT > Default Server.

Click Configuration > NAT > Default Server > Add to open the follow screen.



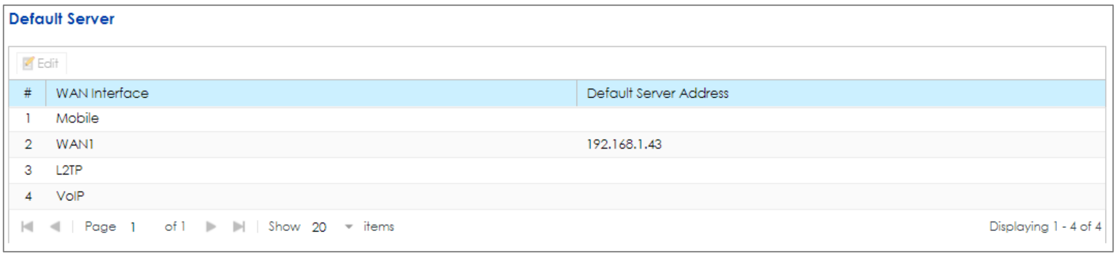
Default Server - Edit

WAN Interface: WAN1

Default Server Address: 192.168.1.43

Note:
1.Enter an IP address and click "OK" to activate the default server.
2.The Interface Group for the Default Server is by default in the firewall "LAN" zone. Use the LAN / Home Network > LAN Setup > LAN Setup-Edit to change the Default's Server zone.
3.The ports used by the Default Server cannot be used by Device Services. Use the Firewall / Security > Device Service screen to change the ports.

Click Configuration > NAT > Default Server open the follow screen.

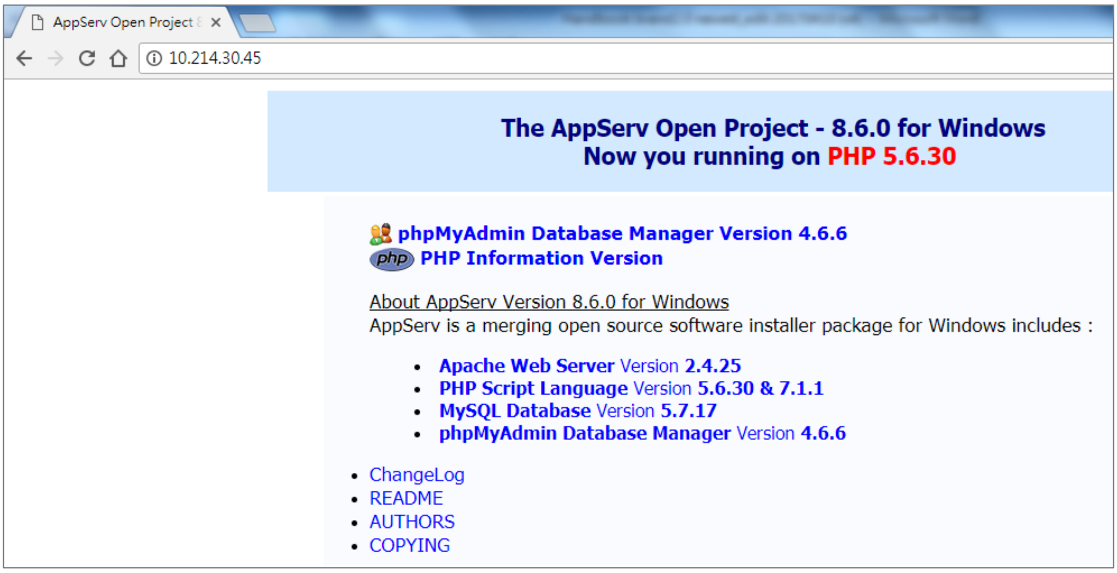


Default Server

#	WAN Interface	Default Server Address
1	Mobile	
2	WAN1	192.168.1.43
3	L2TP	
4	VoIP	

Test the Default Server

Connect to http://10.214.30.45 will access Server B 192.168.1.43



The AppServ Open Project - 8.6.0 for Windows
Now you running on PHP 5.6.30

phpMyAdmin Database Manager Version 4.6.6
PHP Information Version

About AppServ Version 8.6.0 for Windows
AppServ is a merging open source software installer package for Windows includes :

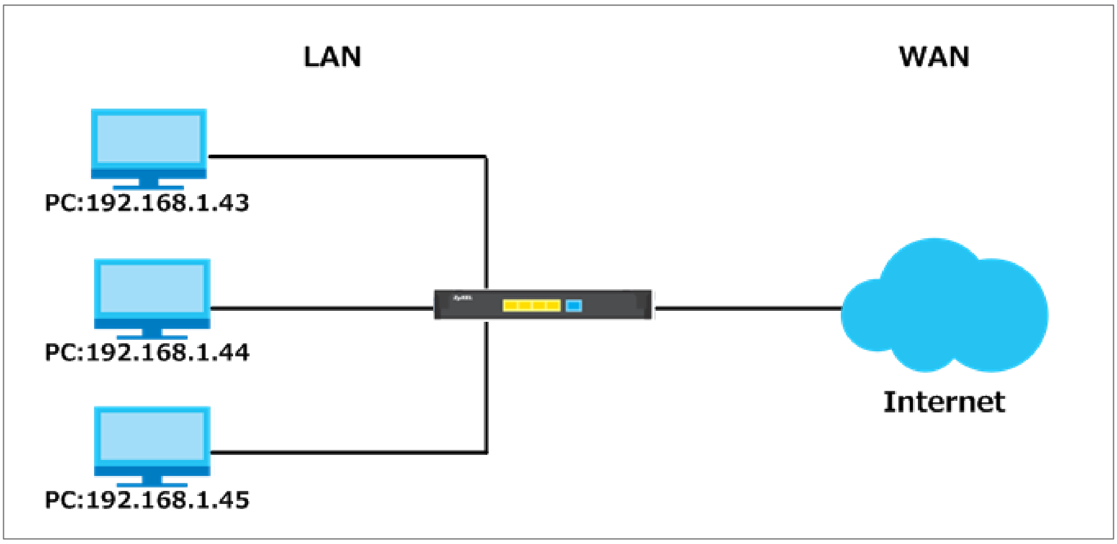
- **Apache Web Server** Version **2.4.25**
- **PHP Script Language** Version **5.6.30 & 7.1.1**
- **MySQL Database** Version **5.7.17**
- **phpMyAdmin Database Manager** Version **4.6.6**

- ChangeLog
- README
- AUTHORS
- COPYING

How to Configure NAT Address Mapping

This example shows how to create NAT Address Mapping. You want to LAN user browser Internet, but you don't have enough Public. So we can use Address Mapping to translate Private IP to Public IP. When the Address Mapping is configured, each user can be browser Internet.

Figure NAT Address Mapping



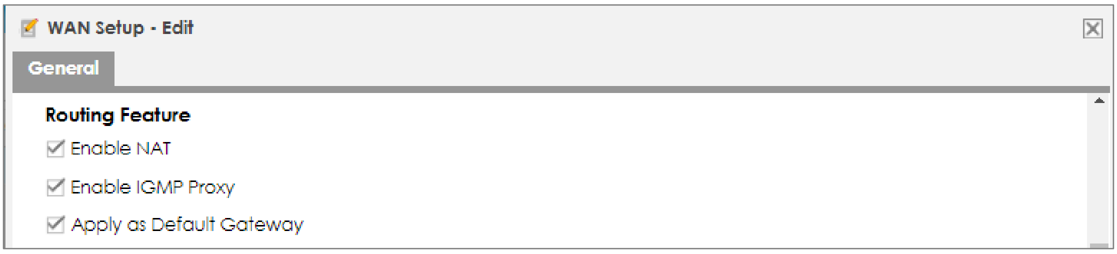
Note:

1. Address mapping rule sets do not have priority above each other, and might not give the desired result if the IP ranges overlap.

Set Up the VPN2S Address Mapping (One-to-One)

In the VPN2S, go to WAN / Internet > WAN Setup.

Click Configuration > WAN / Internet > WAN Setup > Choice WAN1 > Edit to open the follow screen.



Routing Feature

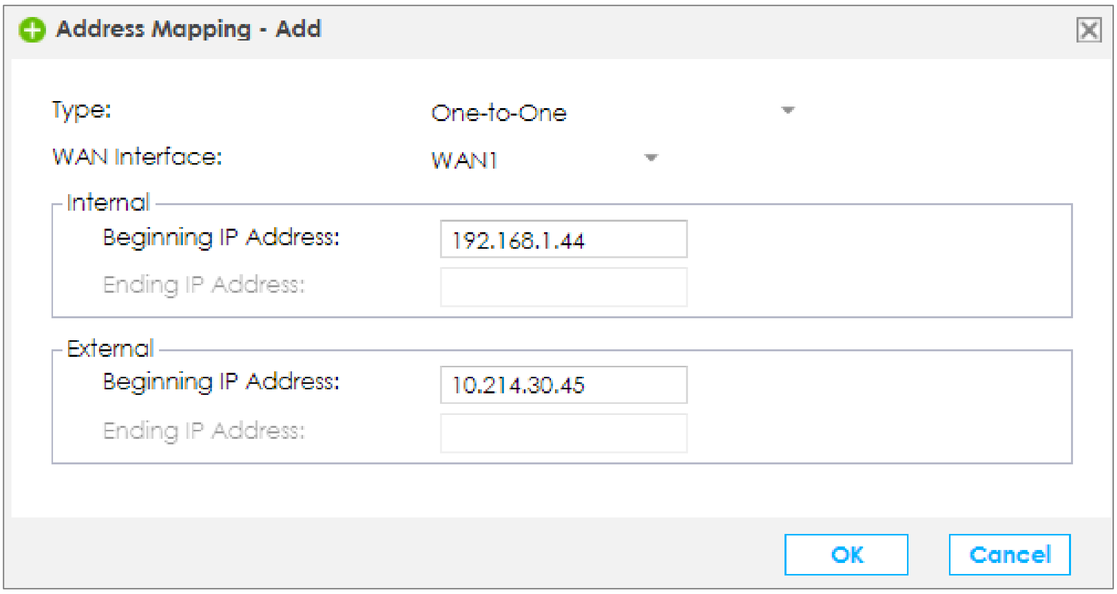
☑ Enable NAT

☑ Enable IGMP Proxy

☑ Apply as Default Gateway

2. In the VPN2S, go to NAT > Address Mapping.

Click Configuration > NAT > Address Mapping > Add to open the follow screen.



Type: One-to-One

WAN Interface: WAN1

Internal

Beginning IP Address: 192.168.1.44

Ending IP Address:

External

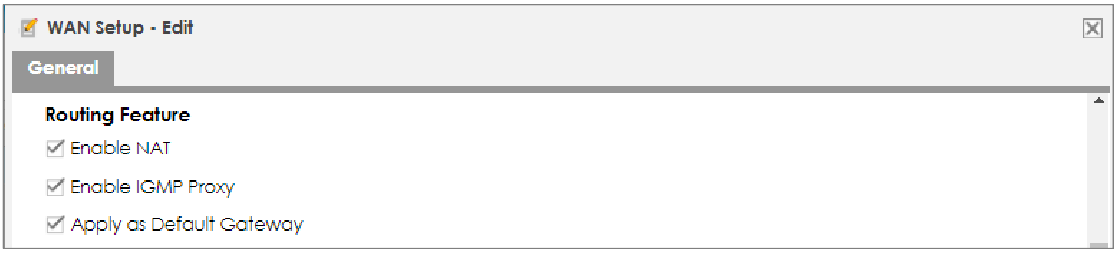
Beginning IP Address: 10.214.30.45

Ending IP Address:

Set Up the VPN2S Address Mapping (Many-to-Many)

In the VPN2S, go to WAN / Internet > WAN Setup.

Click Configuration > WAN / Internet > WAN Setup > Choice WAN1 > Edit to open the follow screen.


WAN Setup - Edit

General

Routing Feature

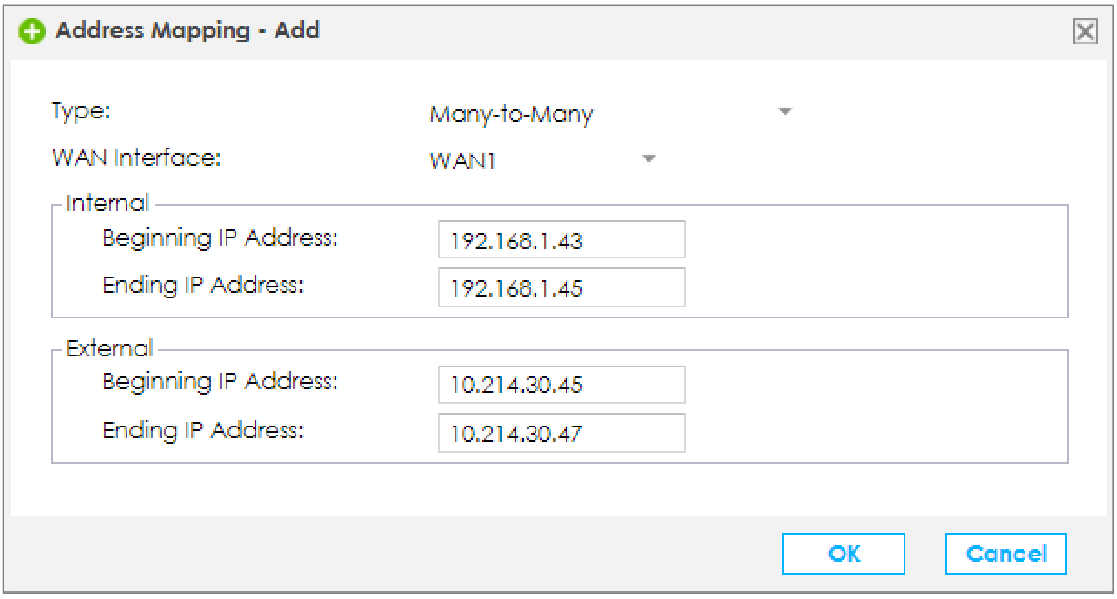
☑ Enable NAT

☑ Enable IGMP Proxy

☑ Apply as Default Gateway

3. In the VPN2S, go to NAT > Address Mapping.

Click Configuration > NAT > Address Mapping > Add to open the follow screen.


Address Mapping - Add

Type: Many-to-Many

WAN Interface: WAN1

Internal

Beginning IP Address: 192.168.1.43

Ending IP Address: 192.168.1.45

External

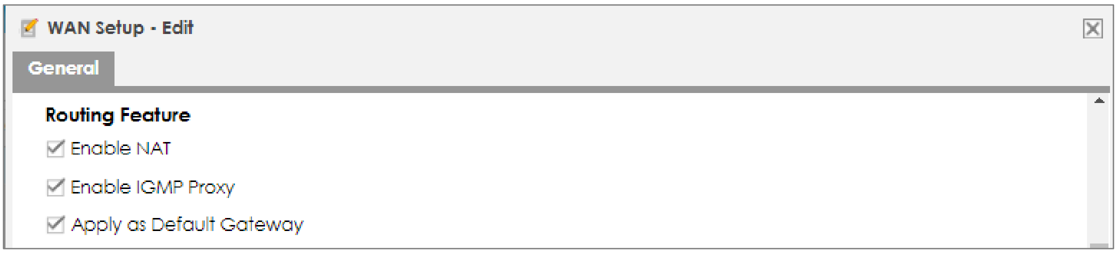
Beginning IP Address: 10.214.30.45

Ending IP Address: 10.214.30.47

Set Up the VPN2S Address Mapping (Many-to-one)

In the VPN2S, go to WAN / Internet > WAN Setup.

Click Configuration > WAN / Internet > WAN Setup > Choice WAN1 > Edit to open the follow screen.



Routing Feature

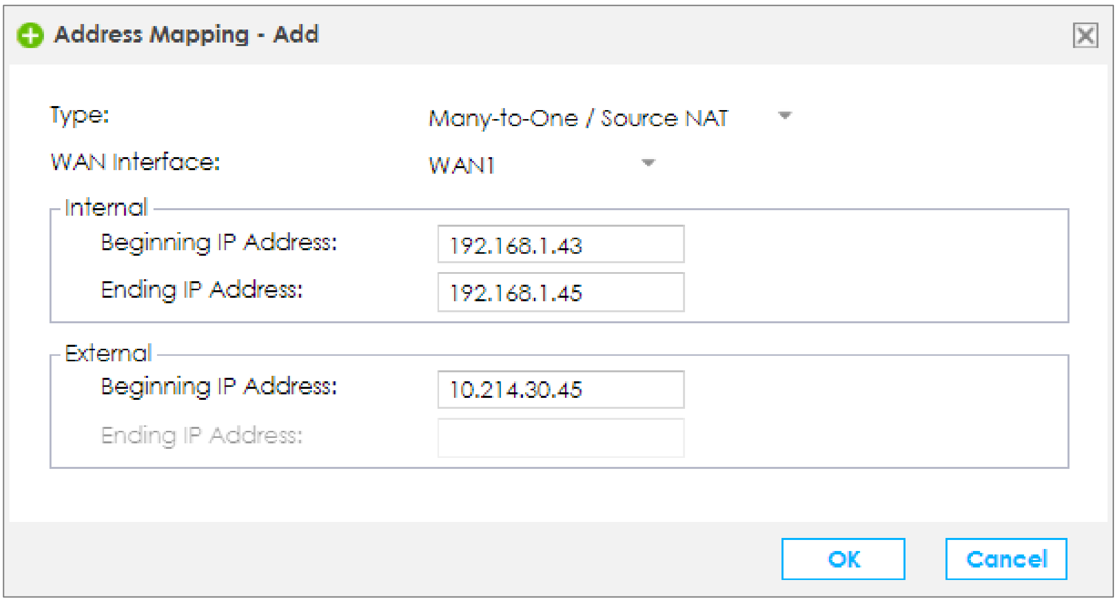
☑ Enable NAT

☑ Enable IGMP Proxy

☑ Apply as Default Gateway

4. In the VPN2S, go to NAT > Address Mapping.

Click Configuration > NAT > Address Mapping > Add to open the follow screen.



Type: Many-to-One / Source NAT

WAN Interface: WAN1

Internal

Beginning IP Address: 192.168.1.43

Ending IP Address: 192.168.1.45

External

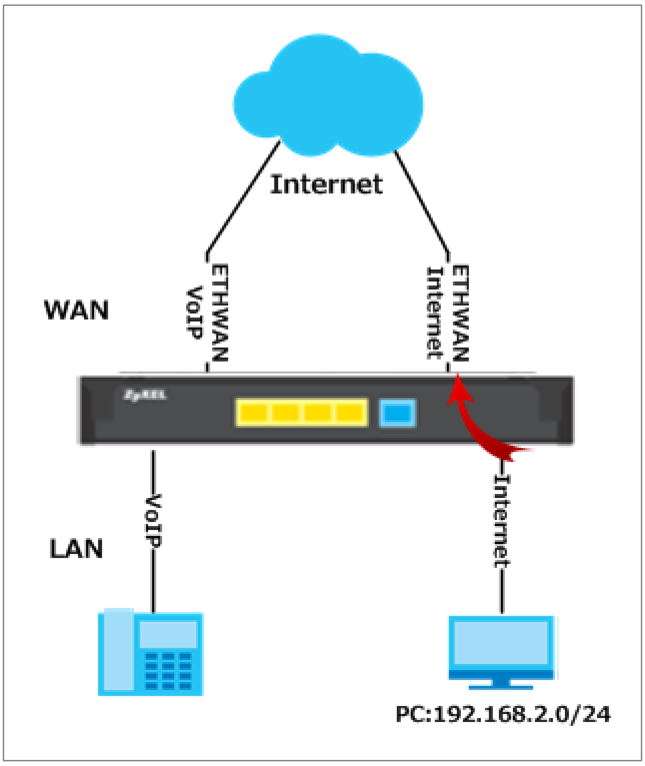
Beginning IP Address: 10.214.30.45

Ending IP Address:

How to setup policy route to force VPN2S clients following rules

This example shows how to create Policy Route. You want to LAN users bower Internet use different interface; however you won't to use static route. Therefore we can use Policy Route to reach this purpose. When the Policy Route is configured, each LAN user can be used different interface go to Internet.

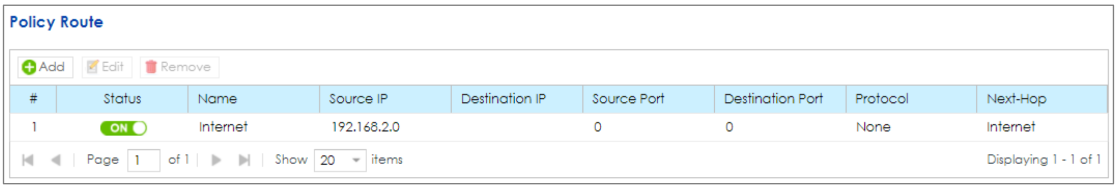
Figure NAT Address Mapping



Set Up the policy route to force VPN2S clients following rules

In the VPN2S, go to WAN / Internet > WAN Setup.

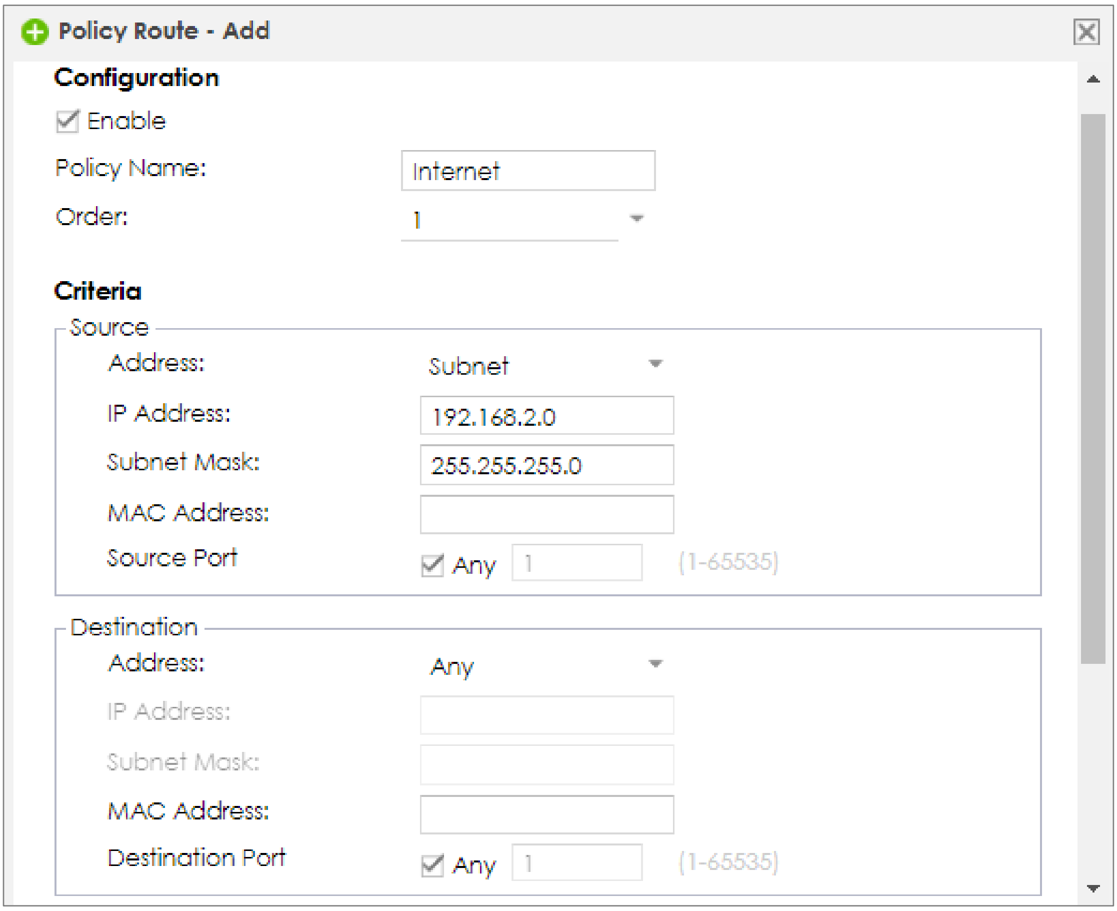
Click Configuration > Routing > Policy Route to open the follow screen.



Policy Route

#	Status	Name	Source IP	Destination IP	Source Port	Destination Port	Protocol	Next-Hop
1	ON	Internet	192.168.2.0		0	0	None	Internet

Click Configuration > Routing > Policy Route > Add to open the follow screen.



Policy Route - Add

Configuration

☑ Enable

Policy Name: Internet

Order: 1

Criteria

Source

Address: Subnet

IP Address: 192.168.2.0

Subnet Mask: 255.255.255.0

MAC Address:

Source Port ☑ Any 1 (1-65535)

Destination

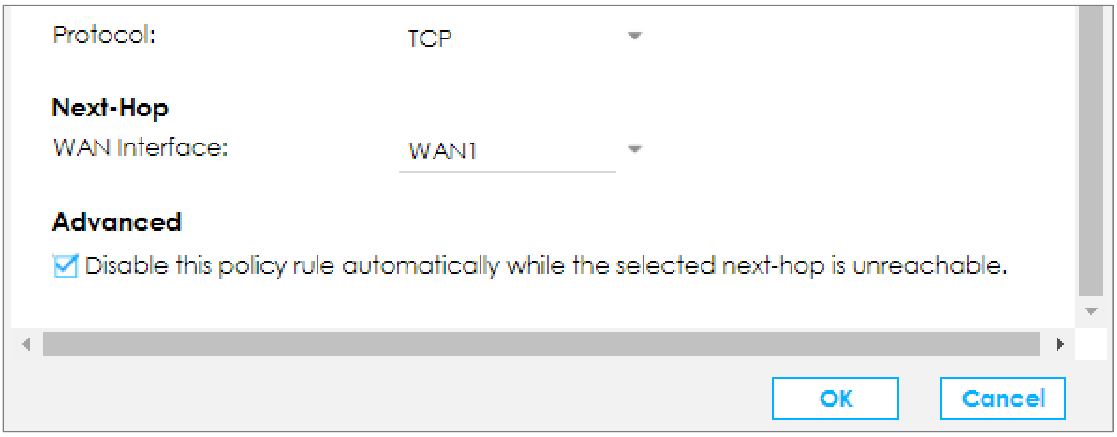
Address: Any

IP Address:

Subnet Mask:

MAC Address:

Destination Port ☑ Any 1 (1-65535)



Protocol: TCP

Next-Hop

WAN Interface: WAN1

Advanced

☑ Disable this policy rule automatically while the selected next-hop is unreachable.

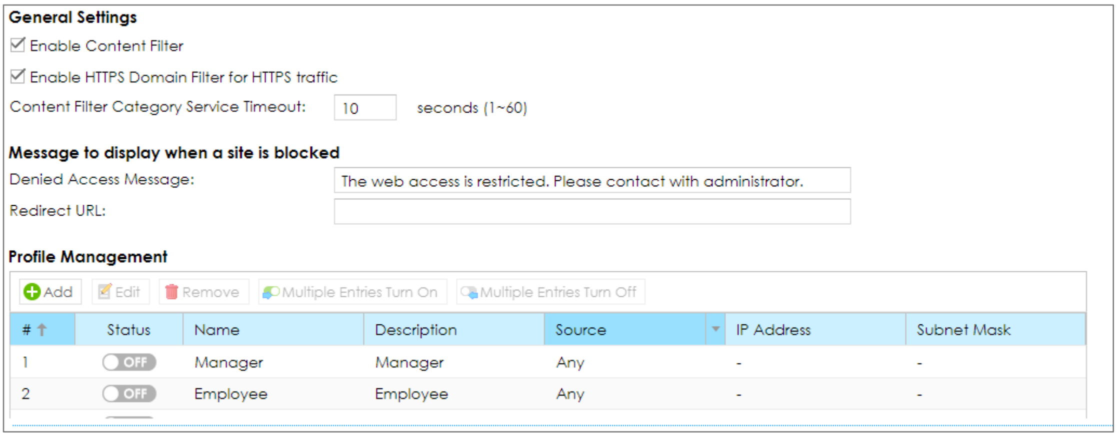
How to Configure Content Filter by Category

This example shows how to block website by Content Filter on the VPN2s. The example instructs how to configure Content Filter. When the Content Filter is configured, each PC can't not access media website.

Set up the Content Filter by Category

In the VPN2S, go to Security Service > Content Filter.

Click Configuration > Security Service > Content Filter to open the follow screen. Then check "Enable Content Filter" and "Enable HTTPS Domain Filter for HTTPs traffic"



General Settings

☑ Enable Content Filter

☑ Enable HTTPS Domain Filter for HTTPS traffic

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

Message to display when a site is blocked

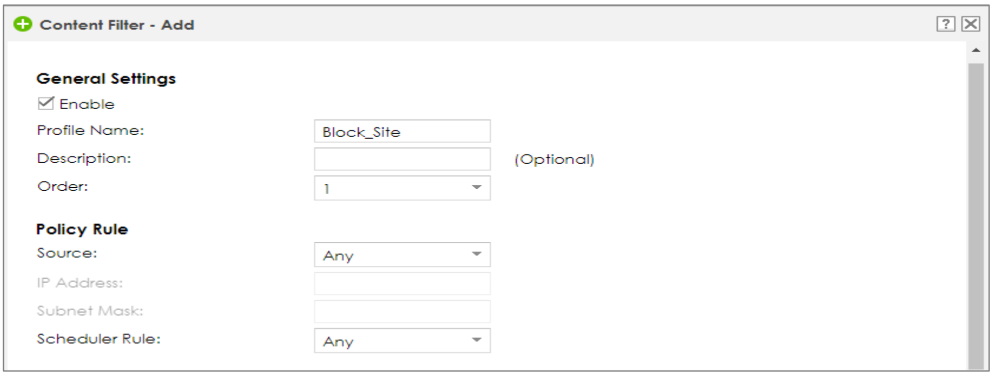
Denied Access Message: The web access is restricted. Please contact with administrator.

Redirect URL:

Profile Management

#	Status	Name	Description	Source	IP Address	Subnet Mask
1	OFF	Manager	Manager	Any	-	-
2	OFF	Employee	Employee	Any	-	-

Click Configuration > Security Service > Content Filter > Profile Management > Add to open the follow screen



Content Filter - Add

General Settings

☑ Enable

Profile Name: Block_Site

Description: (Optional)

Order: 1

Policy Rule

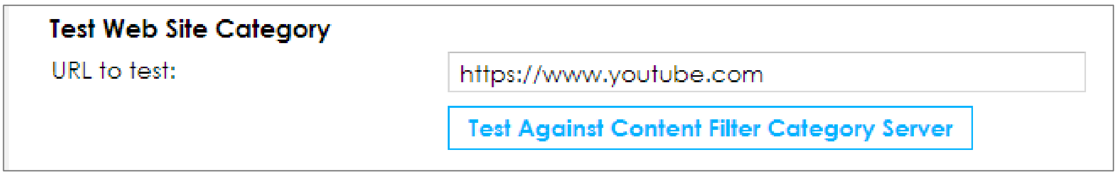
Source: Any

IP Address:

Subnet Mask:

Scheduler Rule: Any

To Test Against Content Filter Category Server

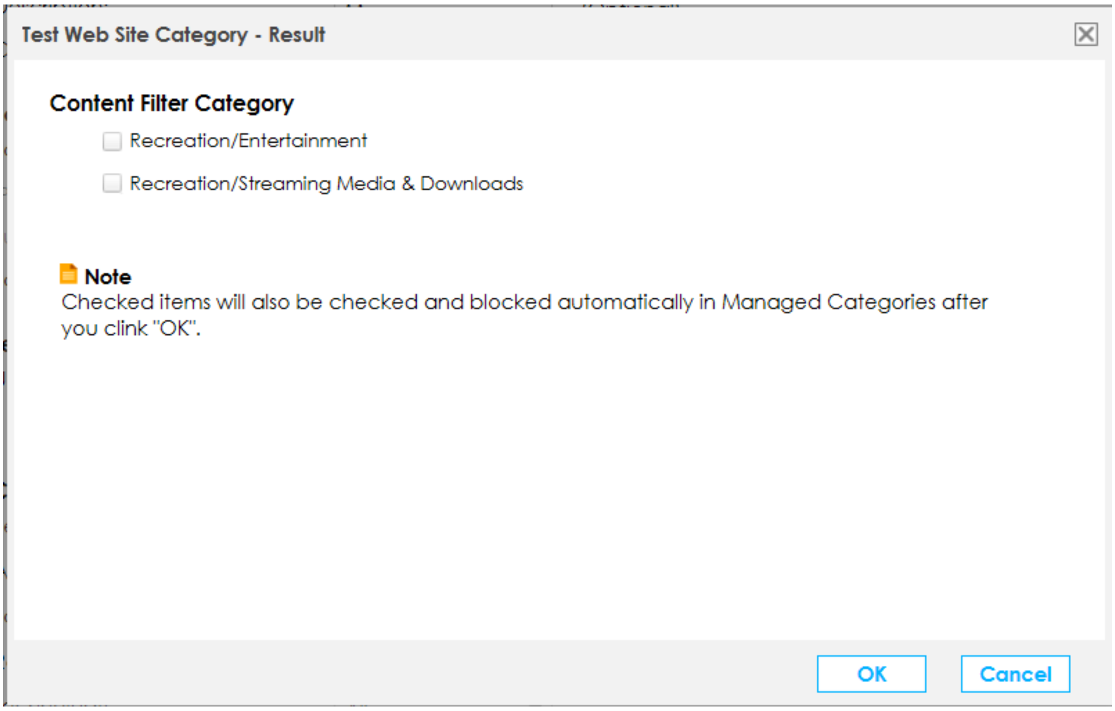


Test Web Site Category

URL to test: https://www.youtube.com

Click Configuration > Security Service > Content Filter > Profile Management > Add > Test Against Content Filter Category Server to open the follow screen

Youtube is Recreation/Entertainment and Streaming Media & Downloads



Test Web Site Category - Result

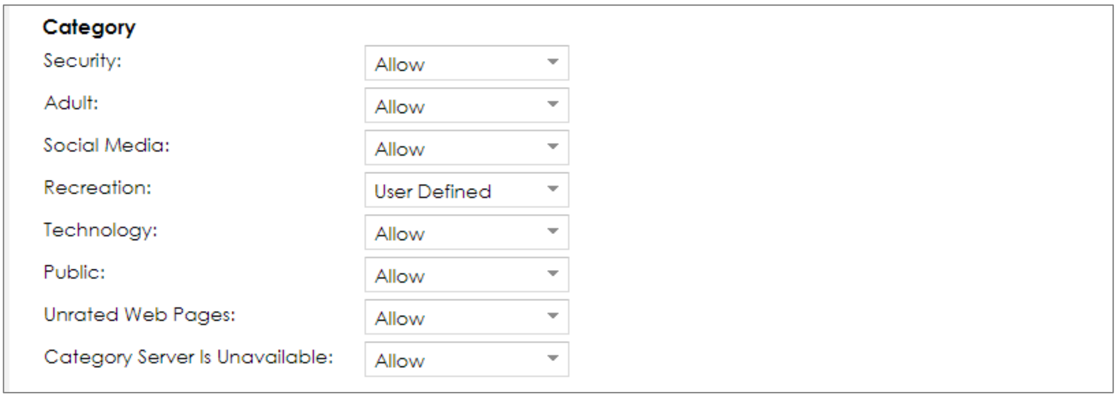
Content Filter Category

□ Recreation/Entertainment

□ Recreation/Streaming Media & Downloads

Note
Checked items will also be checked and blocked automatically in Managed Categories after you clink "OK".

Select “Block” in Recreation

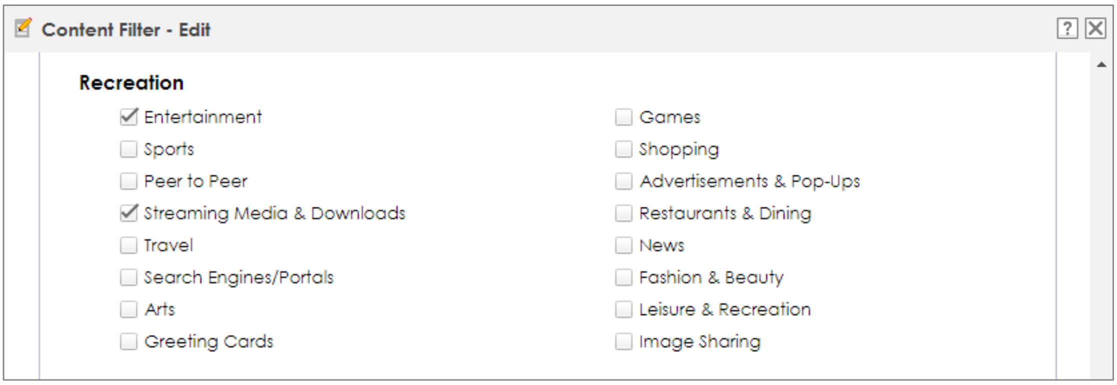


Category

Security:	Allow
Adult:	Allow
Social Media:	Allow
Recreation:	User Defined
Technology:	Allow
Public:	Allow
Unrated Web Pages:	Allow
Category Server Is Unavailable:	Allow

Click Configuration > Security Service > Content Filter > Profile Management > Add > Managed Categories to open the follow screen

To check "Entertainment" and "Streaming Media & Downloads" in Recreation



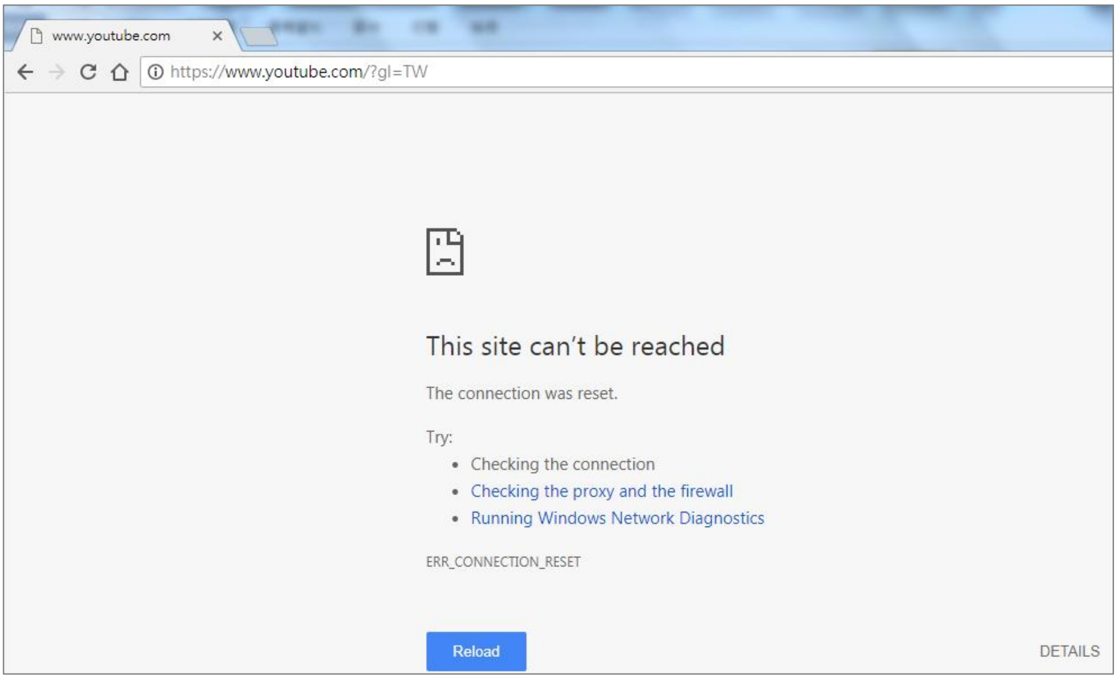
Content Filter - Edit

Recreation

☑ Entertainment
□ Sports
□ Peer to Peer
☑ Streaming Media & Downloads
□ Travel
□ Search Engines/Portals
□ Arts
□ Greeting Cards
□ Games
□ Shopping
□ Advertisements & Pop-Ups
□ Restaurants & Dining
□ News
□ Fashion & Beauty
□ Leisure & Recreation
□ Image Sharing

Test the Content Filter

Connect to https://www.youtube.com



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_RESET

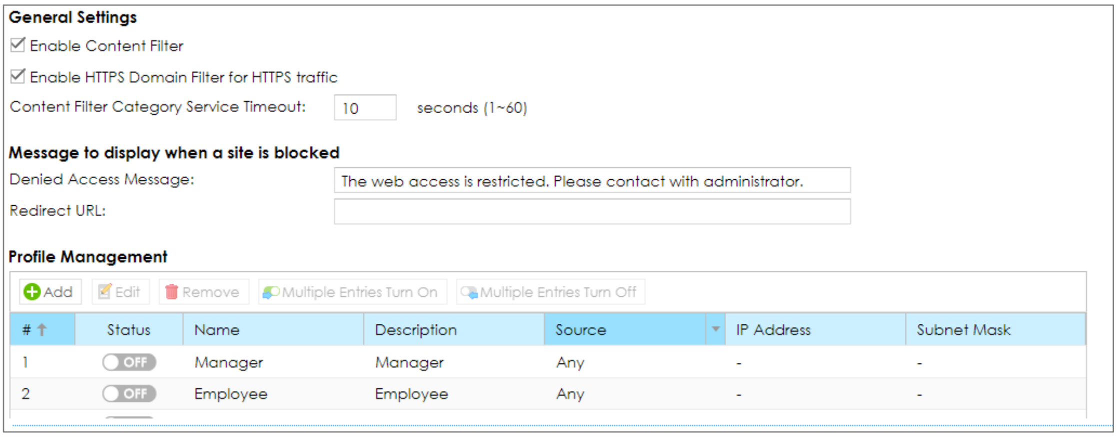
How to Configure bypass website by Content Filter white list

This example shows how to bypass website by Content Filter white list on the VPN2s. The example instructs how to configure Content Filter white list. When the Content Filter white list is configured, each PC cannot access media websites exclude white list web site.

Set up the Content Filter by Category

In the VPN2S, go to Security Service > Content Filter.

Click Configuration > Security Service > Content Filter to open the follow screen. Then check "Enable Content Filter" and "Enable HTTPS Domain Filter for HTTPs traffic"



General Settings

☑ Enable Content Filter

☑ Enable HTTPS Domain Filter for HTTPS traffic

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

Message to display when a site is blocked

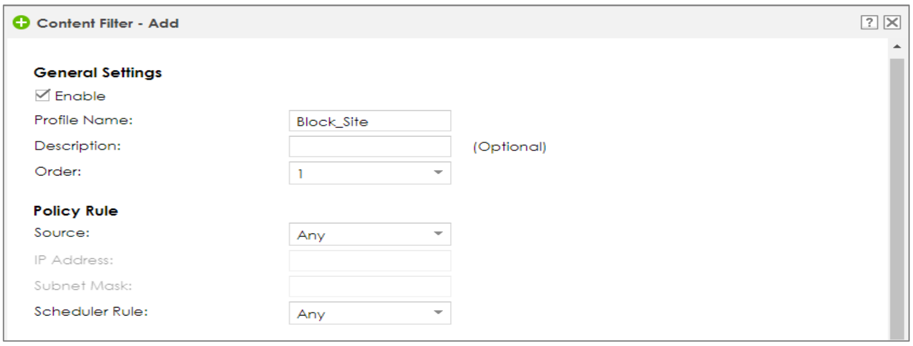
Denied Access Message: The web access is restricted. Please contact with administrator.

Redirect URL:

Profile Management

#	Status	Name	Description	Source	IP Address	Subnet Mask
1	OFF	Manager	Manager	Any	-	-
2	OFF	Employee	Employee	Any	-	-

Click Configuration > Security Service > Content Filter > Profile Management > Add to open the follow screen



Content Filter - Add

General Settings

☑ Enable

Profile Name: Block_Site

Description: (Optional)

Order: 1

Policy Rule

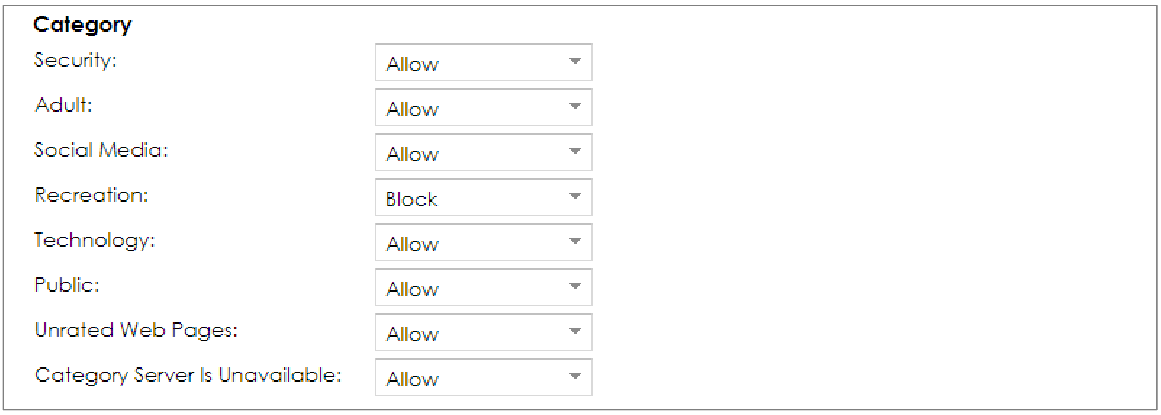
Source: Any

IP Address:

Subnet Mask:

Scheduler Rule: Any

Select “Block” in Recreation

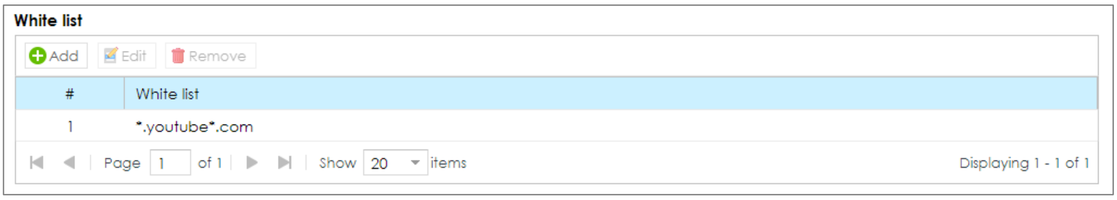


Category

Security:	Allow
Adult:	Allow
Social Media:	Allow
Recreation:	Block
Technology:	Allow
Public:	Allow
Unrated Web Pages:	Allow
Category Server Is Unavailable:	Allow

Set up the Content Filter white list

To add Youtube to White list

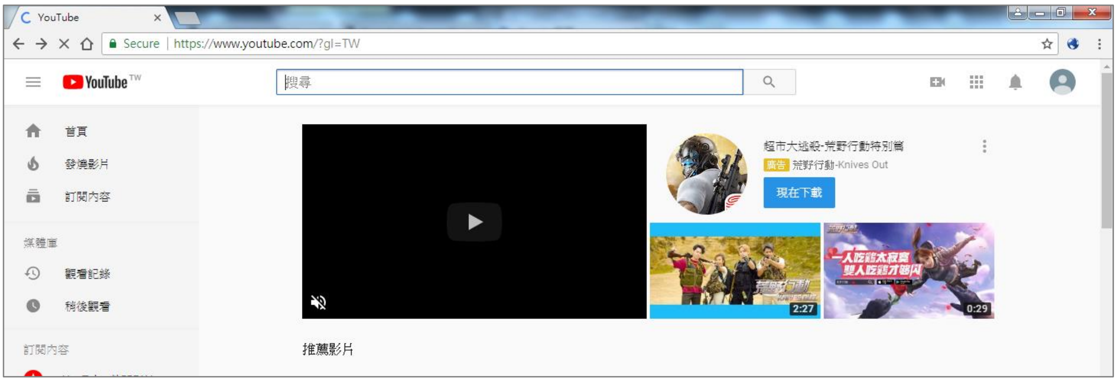


White list

#	White list
1	*.youtube*.com

Test bypass website by Content Filter white list

Connect to https://www.youtube.com



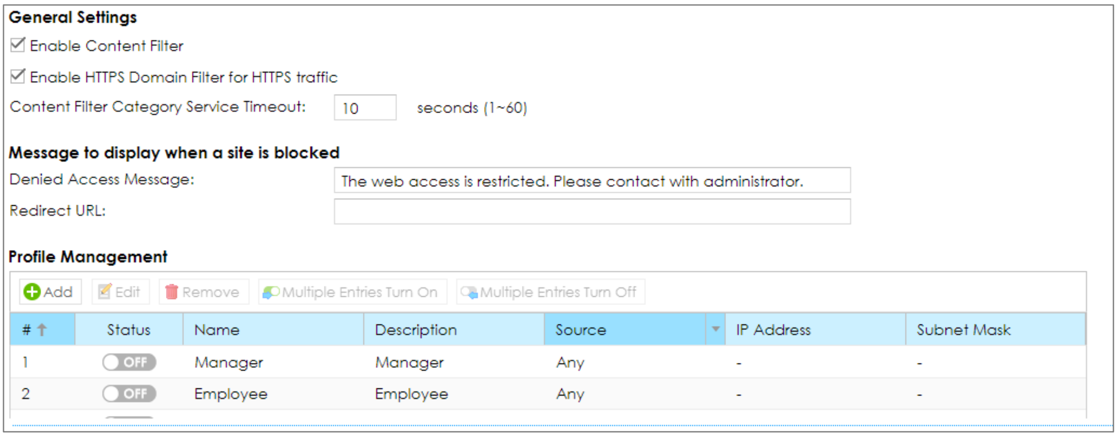
How to Configure bypass website by Content Filter black list

This example shows how to bypass website by Content Filter black list on the VPN2s. The example instructs how to configure Content Filter black list. When the Content Filter black list is configured, each PC cannot access those websites.

Set up the Content Filter by black list

In the VPN2S, go to Security Service > Content Filter.

Click Configuration > Security Service > Content Filter to open the follow screen. Then check "Enable Content Filter" and "Enable HTTPS Domain Filter for HTTPs traffic"



General Settings

☑ Enable Content Filter

☑ Enable HTTPS Domain Filter for HTTPS traffic

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

Message to display when a site is blocked

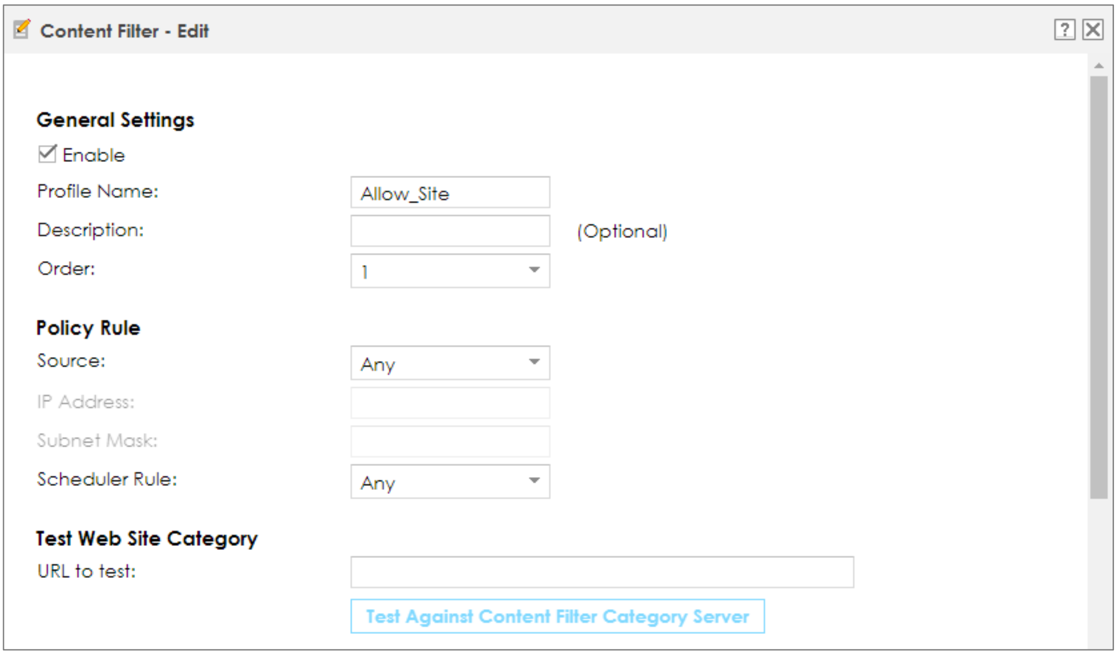
Denied Access Message: The web access is restricted. Please contact with administrator.

Redirect URL:

Profile Management

#	Status	Name	Description	Source	IP Address	Subnet Mask
1	OFF	Manager	Manager	Any	-	-
2	OFF	Employee	Employee	Any	-	-

Click Configuration > Security Service > Content Filter > Profile Management > Add to open the follow screen



Content Filter - Edit

General Settings

☑ Enable

Profile Name: Allow_Site

Description: (Optional)

Order: 1

Policy Rule

Source: Any

IP Address:

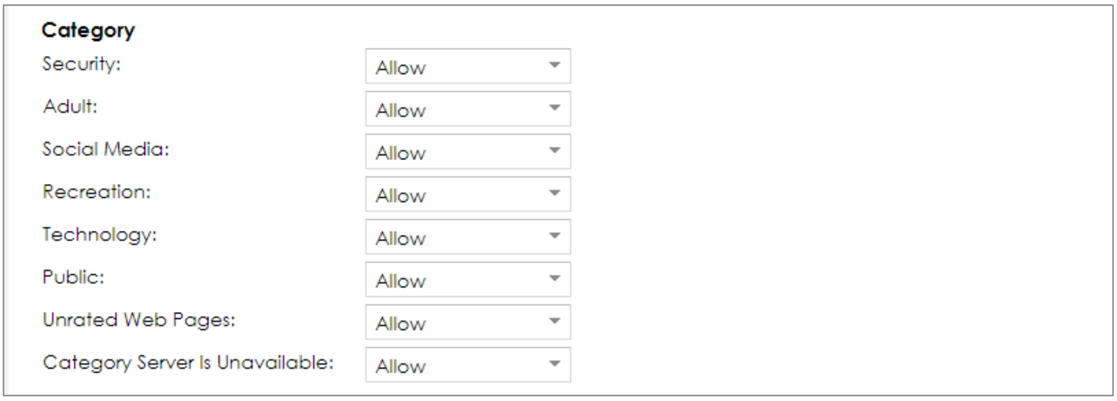
Subnet Mask:

Scheduler Rule: Any

Test Web Site Category

URL to test:

Select "Allow" in all Category

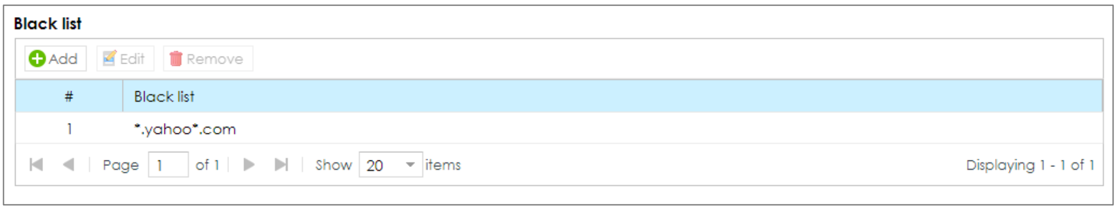


Category

Security:	Allow
Adult:	Allow
Social Media:	Allow
Recreation:	Allow
Technology:	Allow
Public:	Allow
Unrated Web Pages:	Allow
Category Server Is Unavailable:	Allow

Set up the Content Filter black list

To add Yahoo to black list

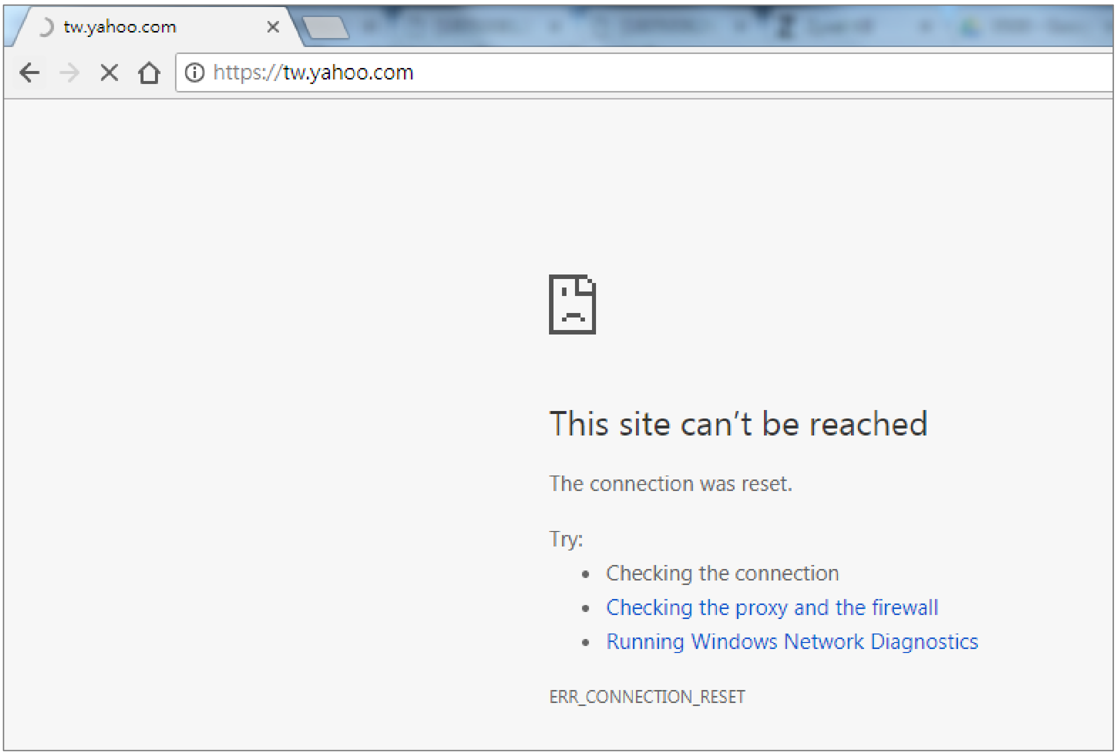


Black list

#	Black list
1	*.yahoo*.com

Test block website by Content Filter black list

Connect to https://tw.yahoo.com



This site can't be reached

The connection was reset.

Try:

- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_RESET