Handbook

USG FLEX H Series

USG FLEX 100H / USG FLEX 100HP / USG FLEX 200H /
USG FLEX 200HP / USG FLEX 500H / USG FLEX 700H

Firmware Version: uOS1.20

04/2024

Default login Details	
Login IP Address	https://192.168.168.1
User Name	admin
Password	1234

Table of Content

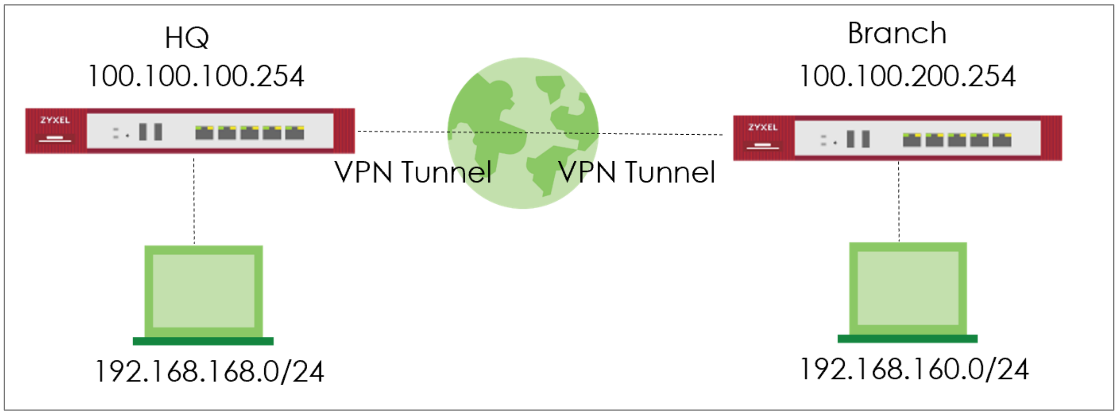
Chapter 1- VPN 4
How to Configure Site-to-site IPSec VPN Where the Peer has a Static IP Address..4
How to Configure Site-to-site IPSec VPN Where the Peer has a Dynamic IP Address.. 16
How to Configure IPSec Site to Site VPN while one Site is behind a NAT router 22
How to Configure Remote Access VPN with Zyxel VPN Client 34
How to Configure Site-to-site IPSec VPN between ZLD and uOS device................. 53
How to Configure Route-Based VPN.. 64
Chapter 2- Security Service 76
How to Block HTTPS Websites Using Content Filtering and SSL Inspection................ 76
How to Configure Content Filter with HTTPs Domain Filter 85
How to Block Facebook Using a Content Filter Block List 90
How to block YouTube access by Schedule 94
How to Control Access to Google Drive 103
How to Block the Spotify Music Streaming Service 111
How does Anti-Malware Work.. 114
How to Detect and Prevent TCP Port Scanning with DoS Prevention 117
How to block the client from accessing to certain country using Geo IP? 121
How to Use Sandbox to Detect Unknown Malware? 126
How to Configure Reputation Filter- IP Reputation.. 129
How to Configure Reputation Filter- URL Threat Filter 134
How to Configure Reputation Filter- DNS Threat Filter 138
How to Configure DNS Content Filter.. 142
External Block List for Reputation Filter 147

Chapter 3- Authentication 152
How to Use Two Factor with Google Authenticator for Admin Access 152
How to Use Two Factor with Google Authenticator for Remote Access VPN and SSL VPN 159
How to set up AD authentication with Microsoft AD 169
Chapter 4- Maintenance 174
How to Manage Configuration Files 174
How to Manage Firmware 178
Chapter 5- Others 180
How to Setup and Configure Daily Report 180
How to Setup and Send Logs to a Syslog Server 185
How to Setup and Send logs to the USB storage 188
How to Perform and Use the Packet Capture Feature 190
How to Allow Public Access to a Server Behind USG FLEX H 194
How to Configure DHCP Option 60 – Vendor Class Identifier 198
How to Configure Session Control 200
How to Configure Bandwidth Management for FTP Traffic 203
How to Configure WAN trunk for Spillover and Least Load First 206

Chapter 1- VPN

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

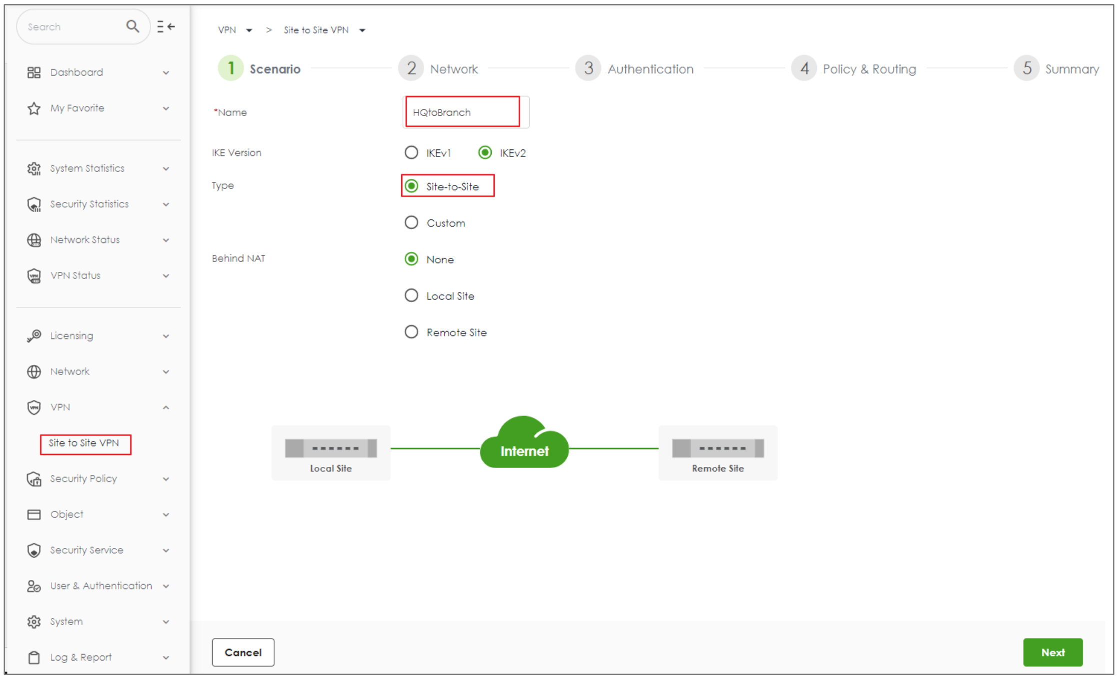
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Static IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPSec VPN Tunnel for HQ

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



VPN > Site to Site VPN

1 Scenario — 2 Network — 3 Authentication — 4 Policy & Routing — 5 Summary

*Name: HQtoBranch

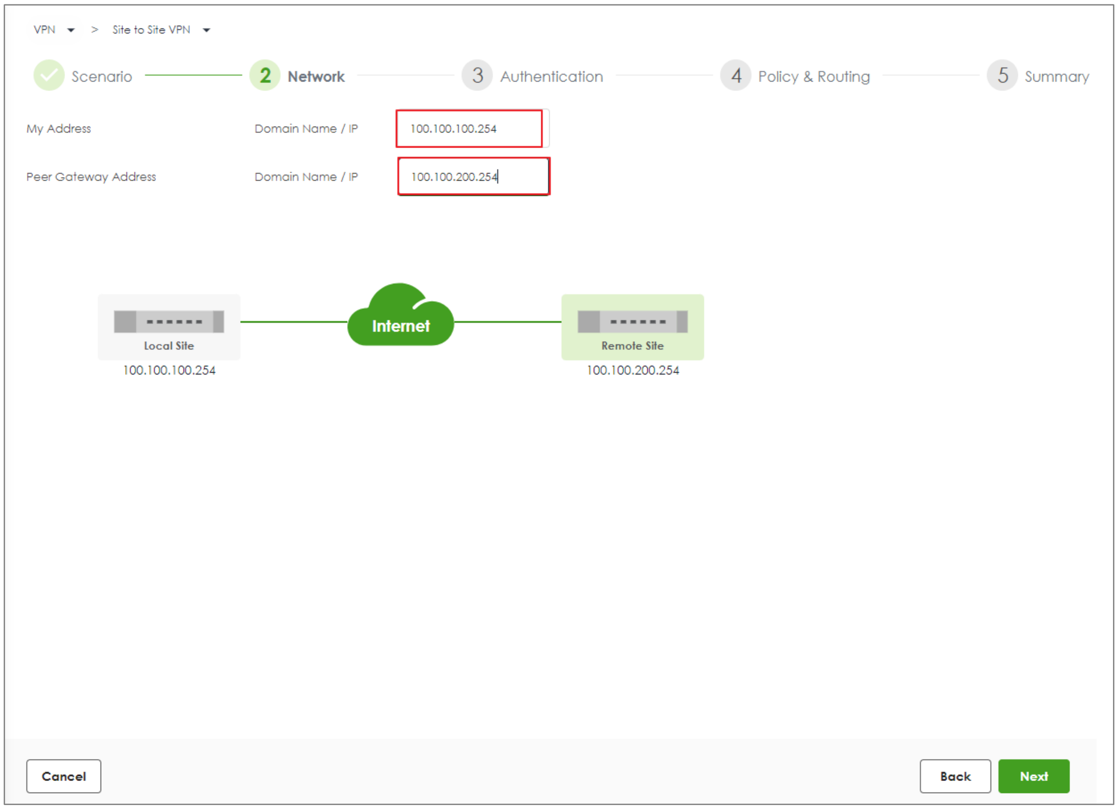
IKE Version: ○ IKEv1 ● IKEv2

Type: ● Site-to-Site ○ Custom

Behind NAT: ● None ○ Local Site ○ Remote Site

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next**.

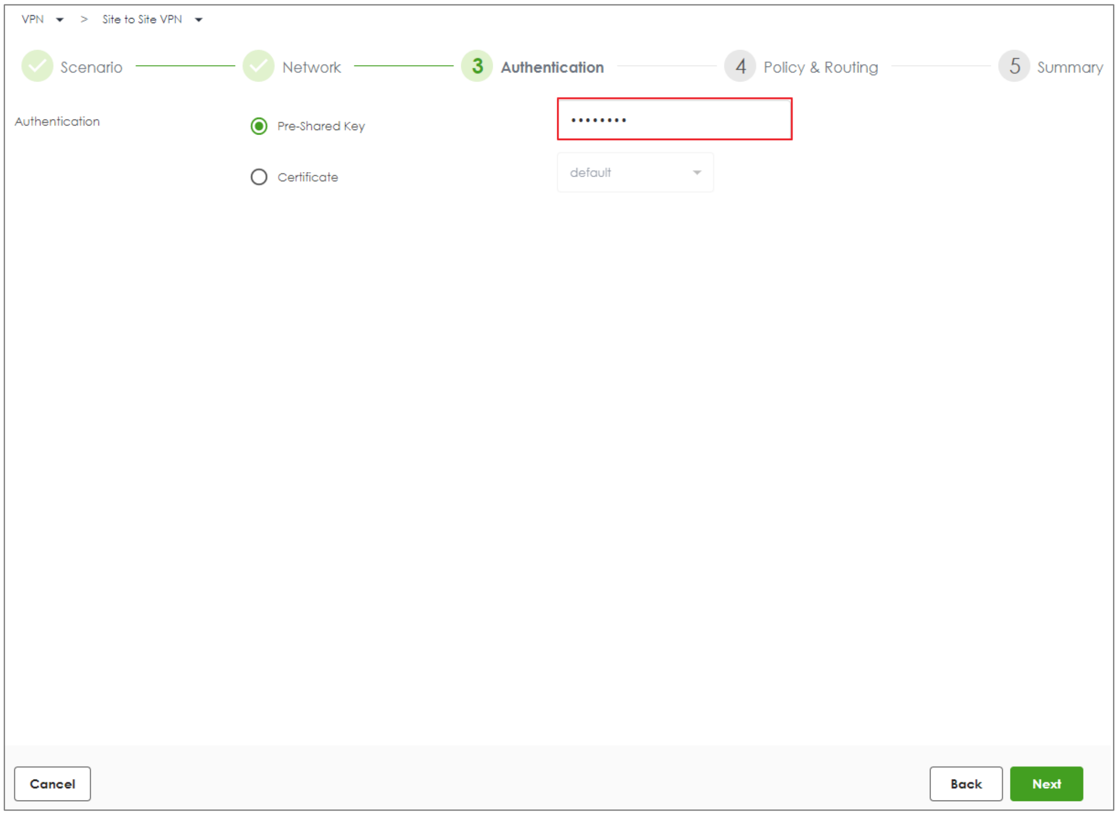


My Address Domain Name / IP 100.100.100.254

Peer Gateway Address Domain Name / IP 100.100.200.254

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**



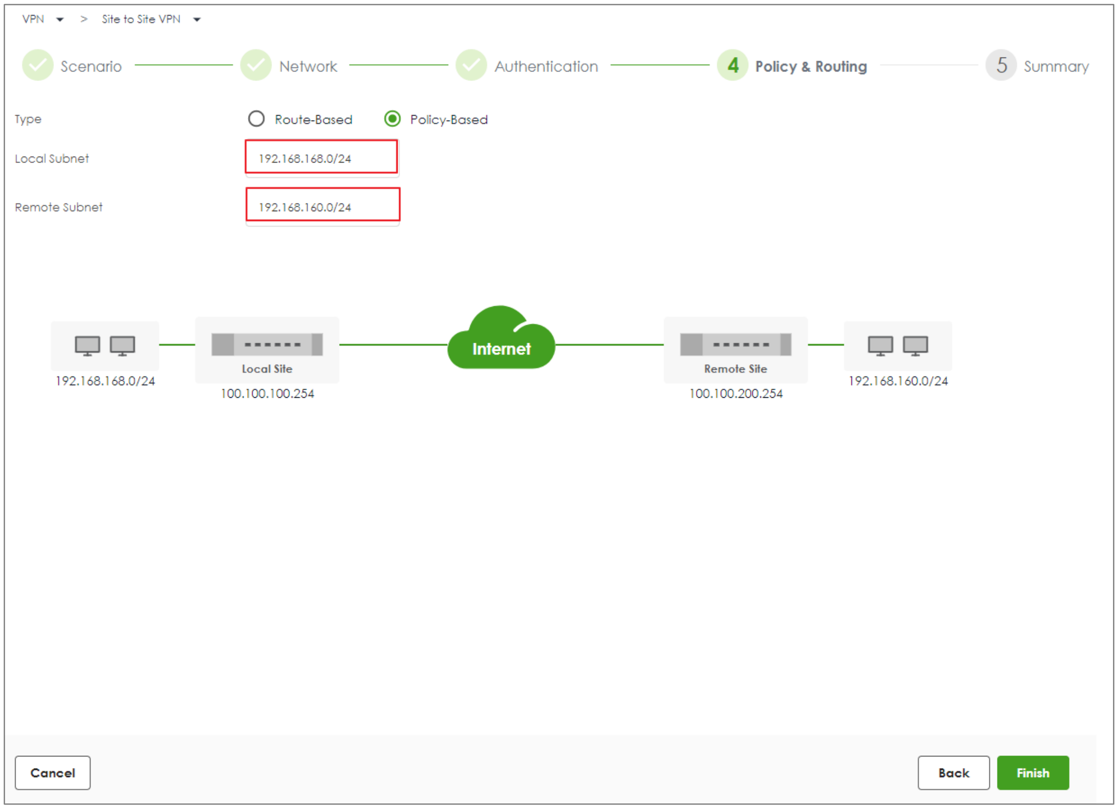
Authentication

● Pre-Shared Key ••••••••

○ Certificate default

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.



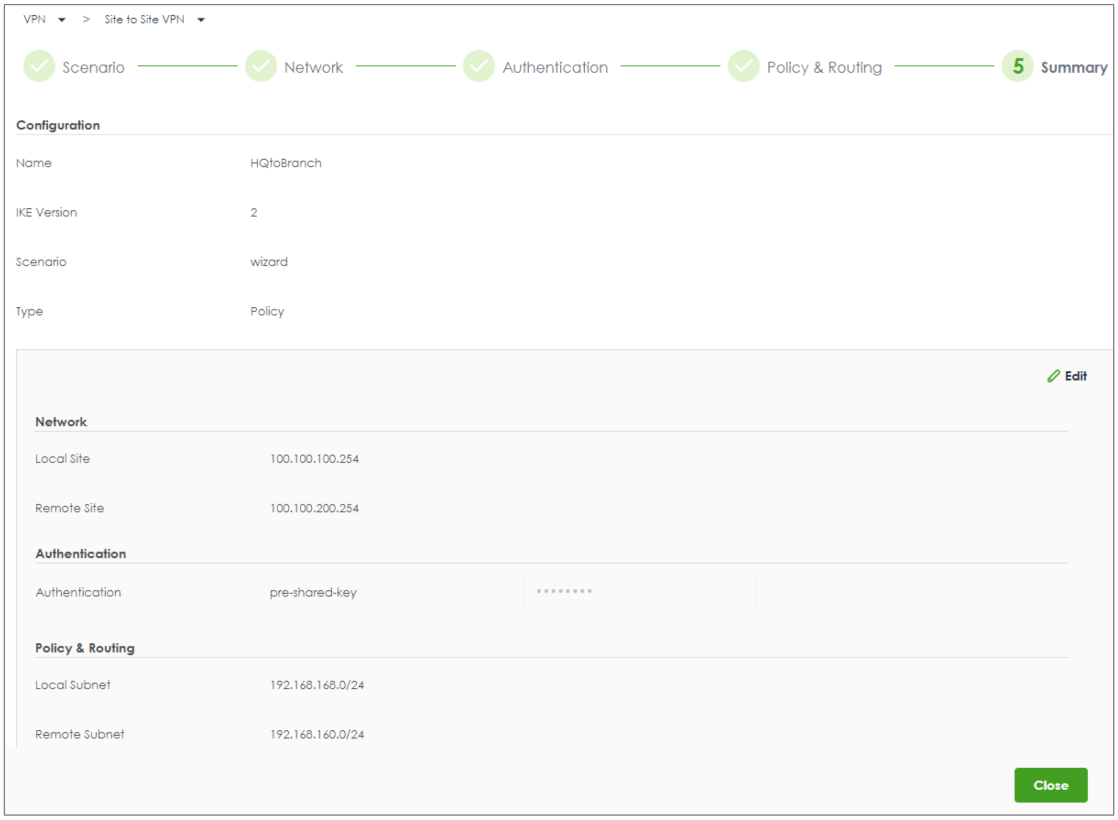
Type ○ Route-Based ● Policy-Based

Local Subnet 192.168.168.0/24

Remote Subnet 192.168.160.0/24

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



Configuration

Name	HQtoBranch
IKE Version	2
Scenario	wizard
Type	Policy

Network

Local Site	100.100.100.254
Remote Site	100.100.200.254

Authentication

Authentication	pre-shared-key	••••••••

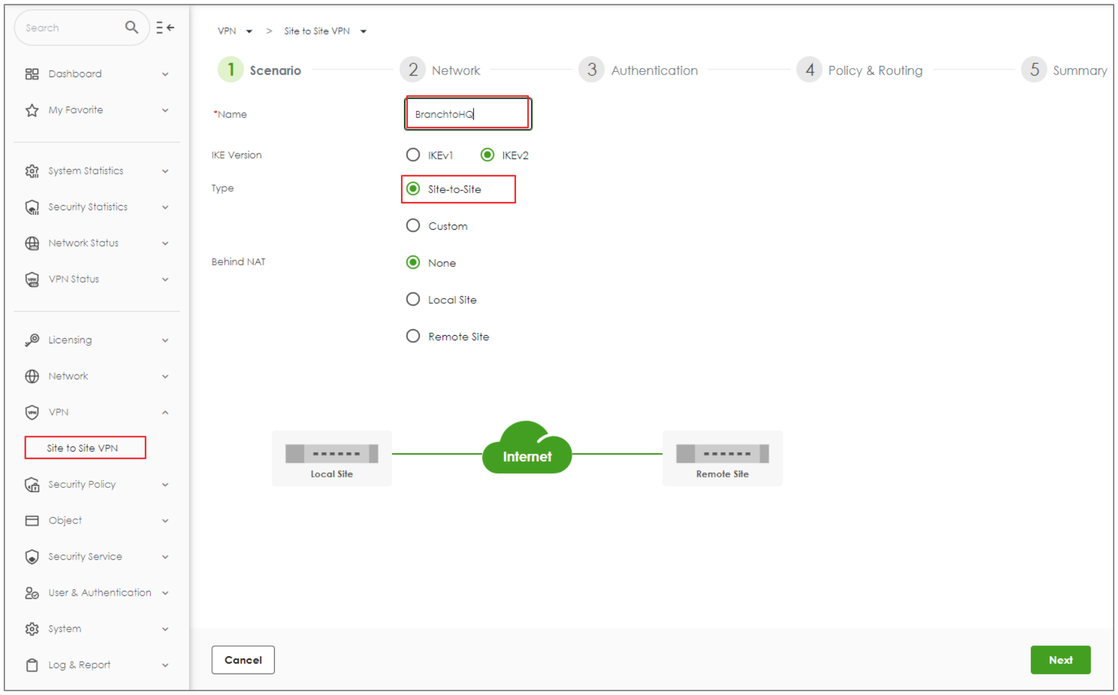
Policy & Routing

Local Subnet	192.168.168.0/24
Remote Subnet	192.168.160.0/24

Set up IPSec VPN Tunnel for Branch

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



*Name: BranchtoHQ

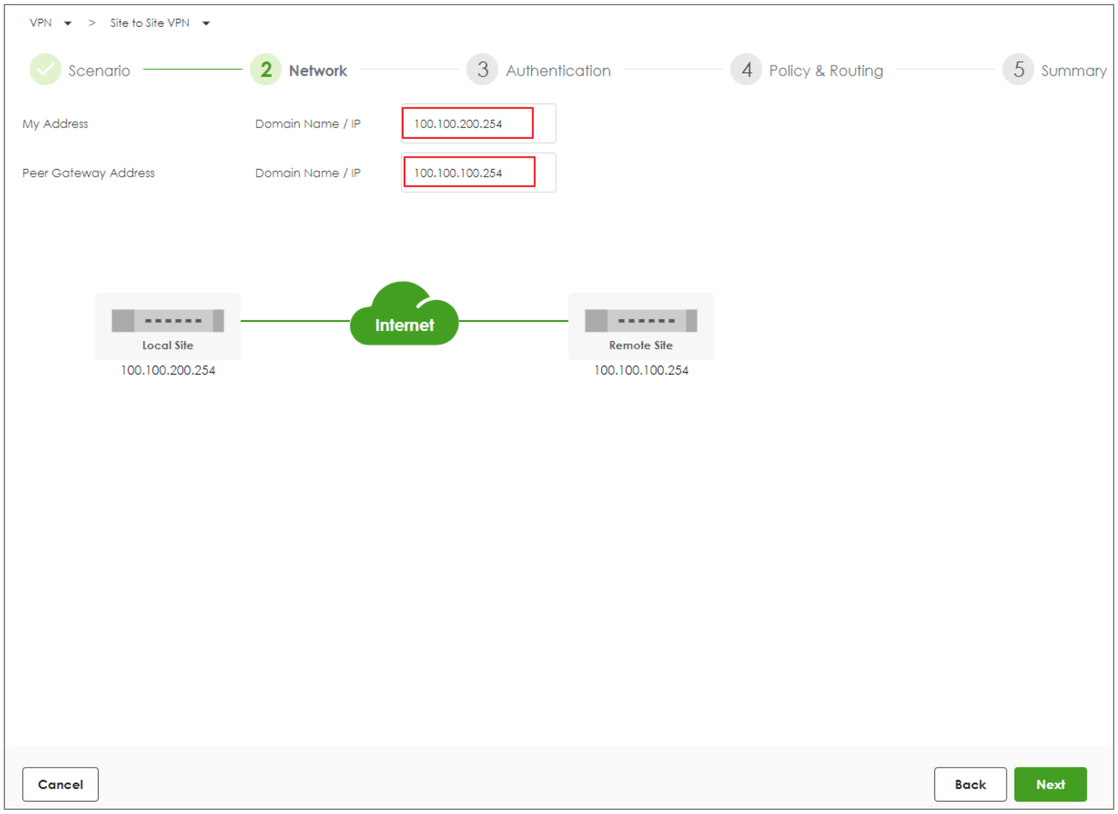
IKE Version: ○ IKEv1 ● IKEv2

Type: ● Site-to-Site ○ Custom

Behind NAT: ● None ○ Local Site ○ Remote Site

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next.**



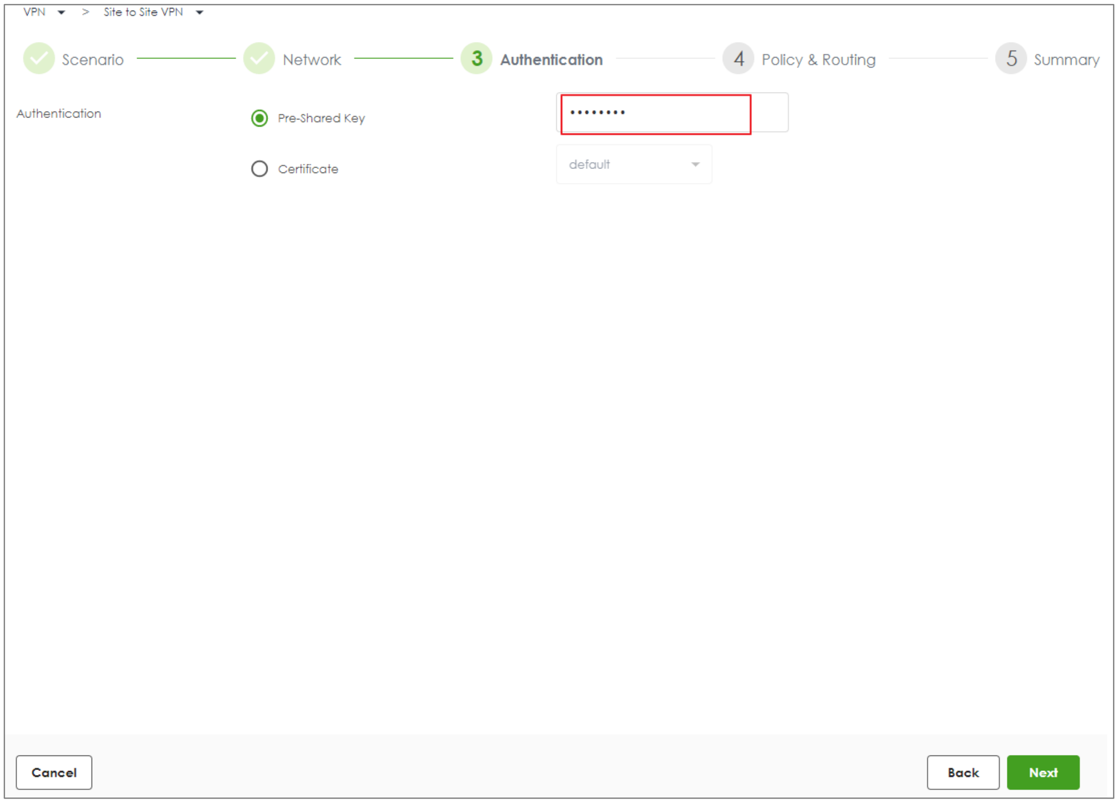
My Address	Domain Name / IP	100.100.200.254
Peer Gateway Address	Domain Name / IP	100.100.100.254

Local Site 100.100.200.254

Remote Site 100.100.100.254

VPN > Site to Site VPN > Scenario > Network > Authentication

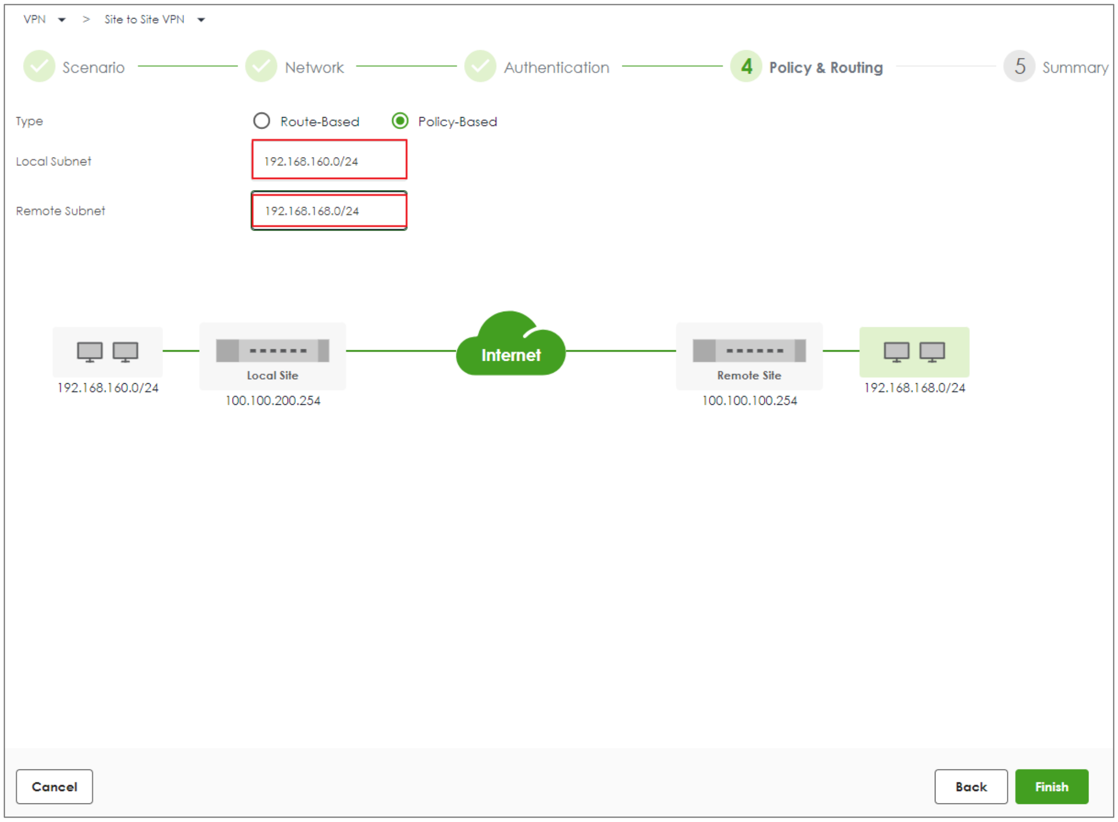
Type a secure Pre-Shared Key. Click **Next.**



Authentication ● Pre-Shared Key ••••••••• ○ Certificate default

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.



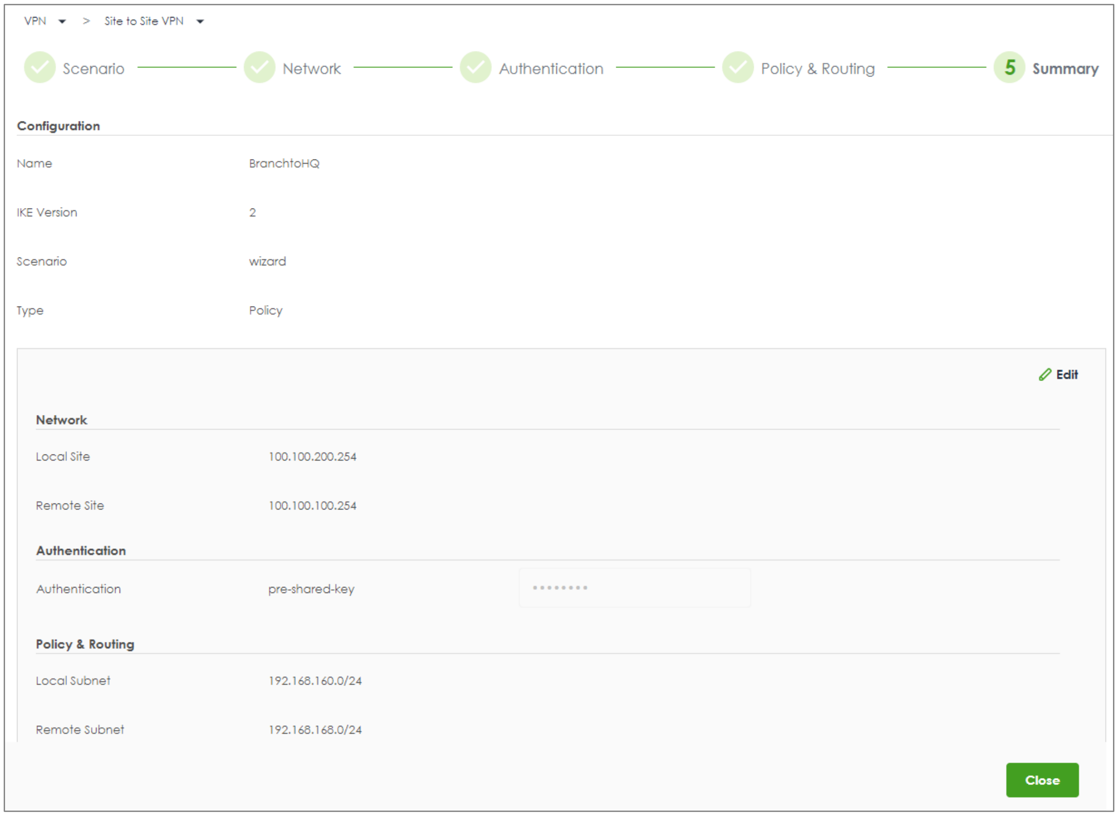
Type ○ Route-Based ● Policy-Based

Local Subnet 192.168.160.0/24

Remote Subnet 192.168.168.0/24

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



Configuration

Name	BranchtoHQ
IKE Version	2
Scenario	wizard
Type	Policy

Network

Local Site	100.100.200.254
Remote Site	100.100.100.254

Authentication

Authentication	pre-shared-key	••••••••

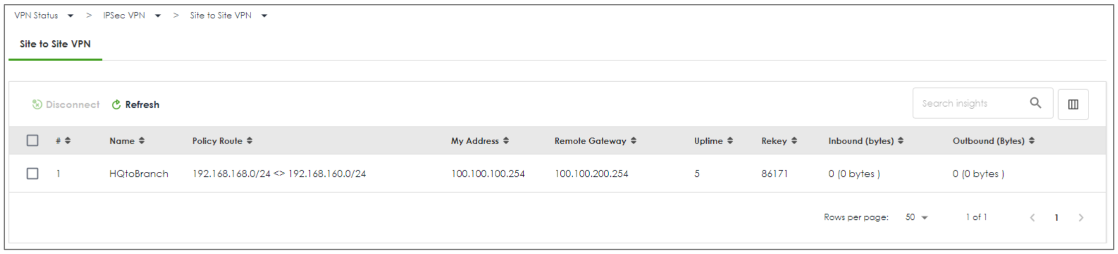
Policy & Routing

Local Subnet	192.168.160.0/24
Remote Subnet	192.168.168.0/24

Test IPSec VPN Tunnel

VPN Status > IPSec VPN

Verify the IPSec VPN status.



VPN Status > IPSec VPN > Site to Site VPN

Site to Site VPN

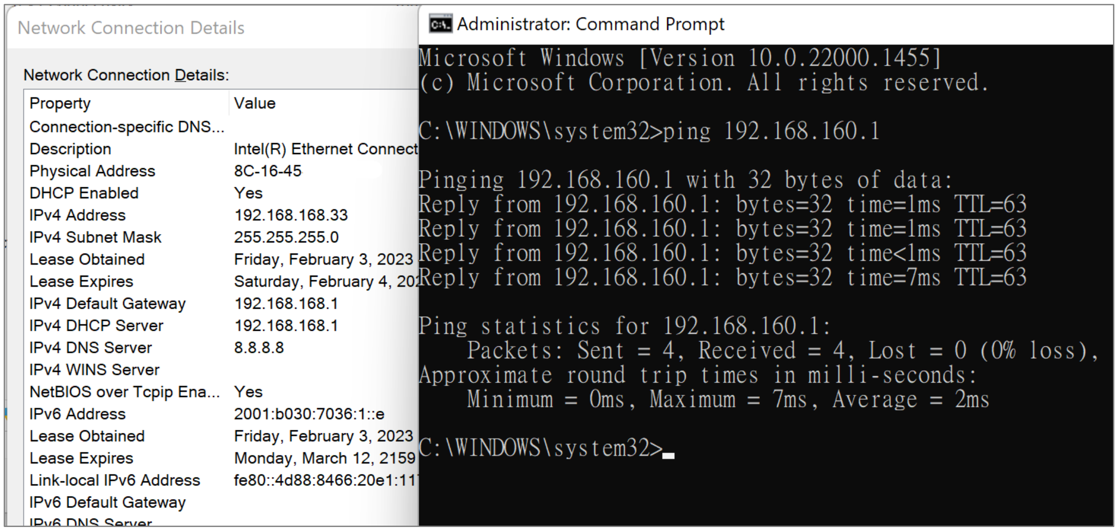
Disconnect Refresh Search insights

□	#	Name	Policy Route	My Address	Remote Gateway	Uptime	Rekey	Inbound (bytes)	Outbound (Bytes)
□	1	HQtoBranch	192.168.168.0/24 <> 192.168.160.0/24	100.100.100.254	100.100.200.254	5	86171	0 (0 bytes)	0 (0 bytes)

Rows per page: 50 1 of 1 1

Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



Network Connection Details

Network Connection Details:

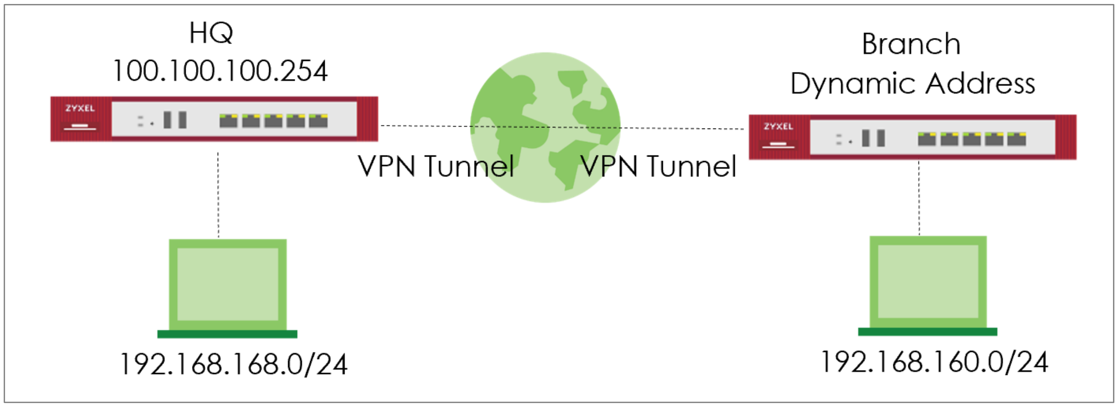
Property	Value
Connection-specific DNS...	
Description	Intel(R) Ethernet Connect
Physical Address	8C-16-45
DHCP Enabled	Yes
IPv4 Address	192.168.168.33
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, February 3, 2023
Lease Expires	Saturday, February 4, 20
IPv4 Default Gateway	192.168.168.1
IPv4 DHCP Server	192.168.168.1
IPv4 DNS Server	8.8.8.8
IPv4 WINS Server	
NetBIOS over Tcpip Ena...	Yes
IPv6 Address	2001:b030:7036:1::e
Lease Obtained	Friday, February 3, 2023
Lease Expires	Monday, March 12, 2159
Link-local IPv6 Address	fe80::4d88:8466:20e1:11
IPv6 Default Gateway	
IPv6 DNS Server	

Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping 192.168.160.1

Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time<1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=7ms TTL=63

Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\WINDOWS\system32>_
```

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

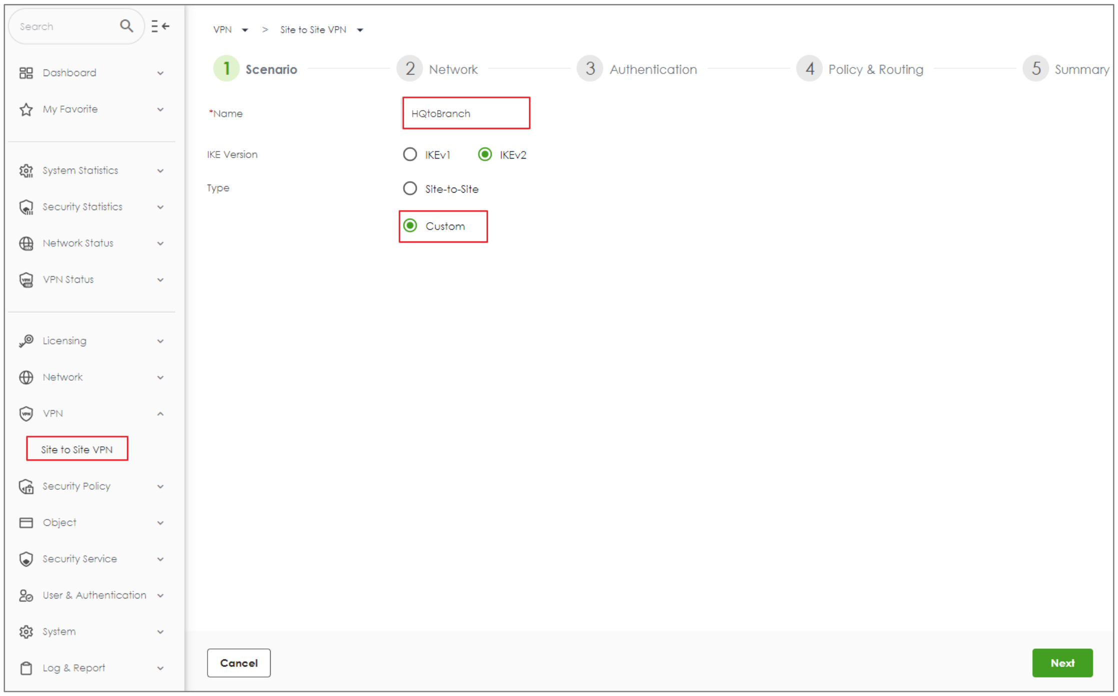
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Dynamic IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPSec VPN Tunnel for HQ

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Custom. Click **Next**.



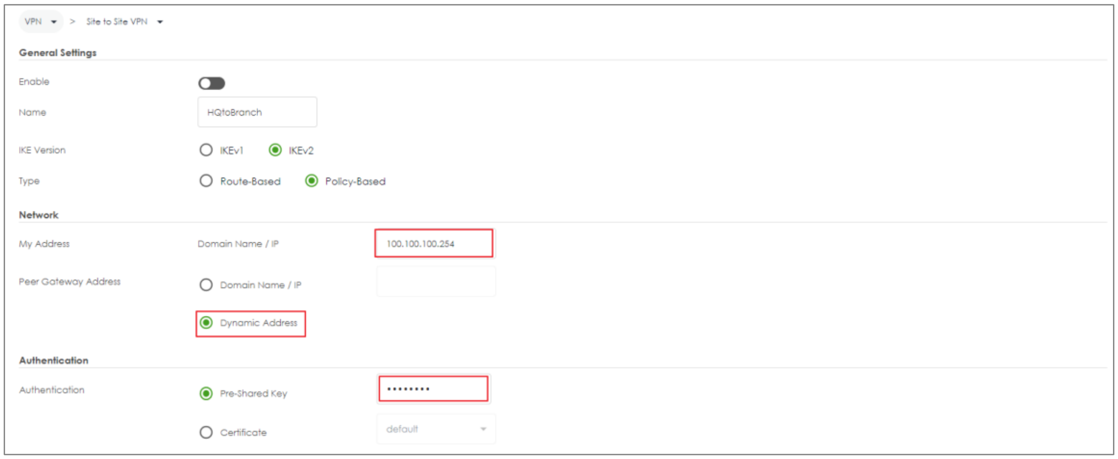
*Name: HQtoBranch

IKE Version: ○ IKEv1 ● IKEv2

Type: ○ Site-to-Site ● Custom

VPN > Site to Site VPN

Type My Address and select Peer Gateway Address as Dynamic Address. Type a secure Pre-shared key.



General Settings

Enable

Name: HQtoBranch

IKE Version: ○ IKEv1 ● IKEv2

Type: ○ Route-Based ● Policy-Based

Network

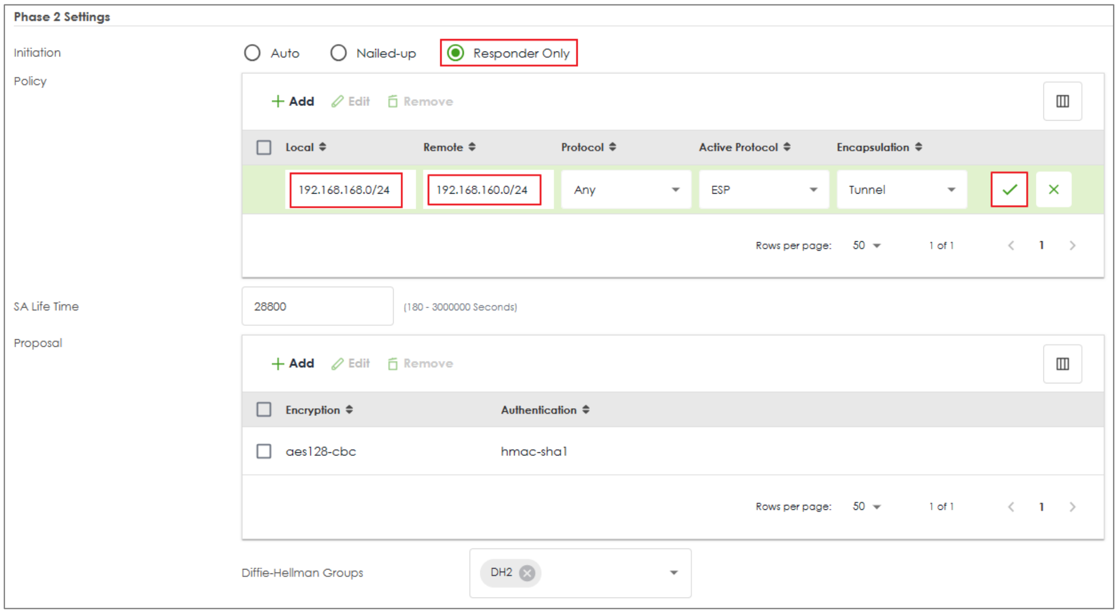
My Address: Domain Name / IP 100.100.100.254

Peer Gateway Address: ○ Domain Name / IP ● Dynamic Address

Authentication

Authentication: ● Pre-Shared Key •••••••• ○ Certificate default

Scroll down to find the Phase2 setting. Type Local and Remote Subnet and select Responder Only. Then click save change.



Phase 2 Settings

Initiation ○ Auto ○ Nailed-up ● Responder Only

Policy

+ Add Edit Remove

□	Local	Remote	Protocol	Active Protocol	Encapsulation
	192.168.168.0/24	192.168.160.0/24	Any	ESP	Tunnel

Rows per page: 50 1 of 1 1

SA Life Time 28800 (180 - 3000000 Seconds)

Proposal

+ Add Edit Remove

□	Encryption	Authentication
□	aes128-cbc	hmac-sha1

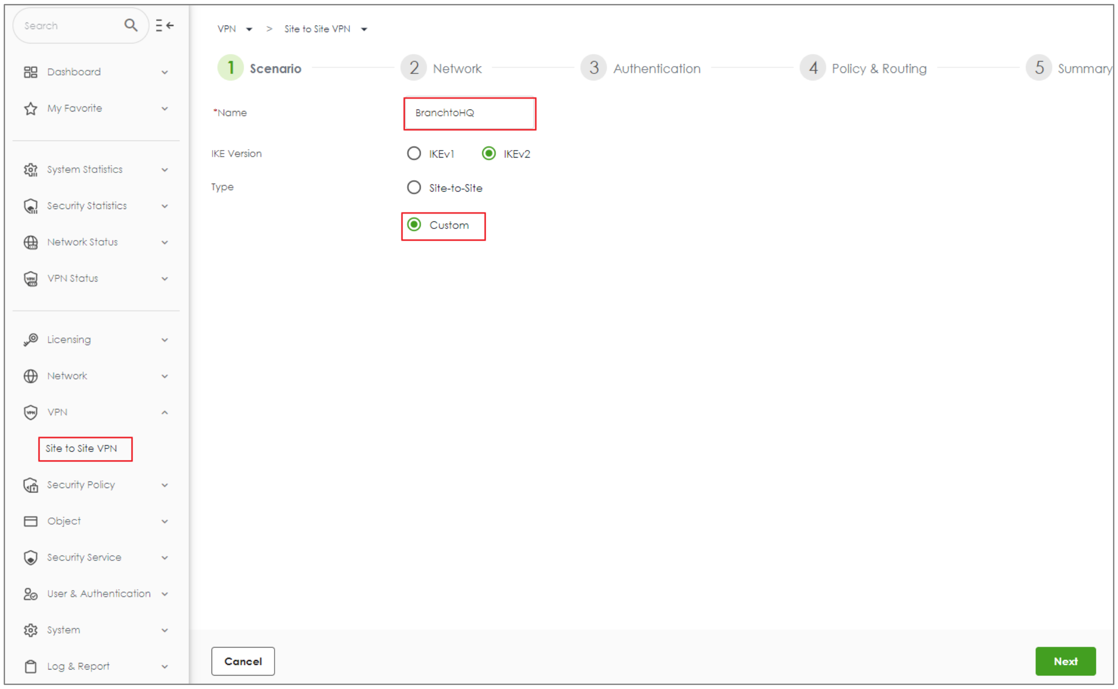
Rows per page: 50 1 of 1 1

Diffie-Hellman Groups DH2

Set up IPSec VPN Tunnel for Branch

VPN > Site to Site VPN > Scenario

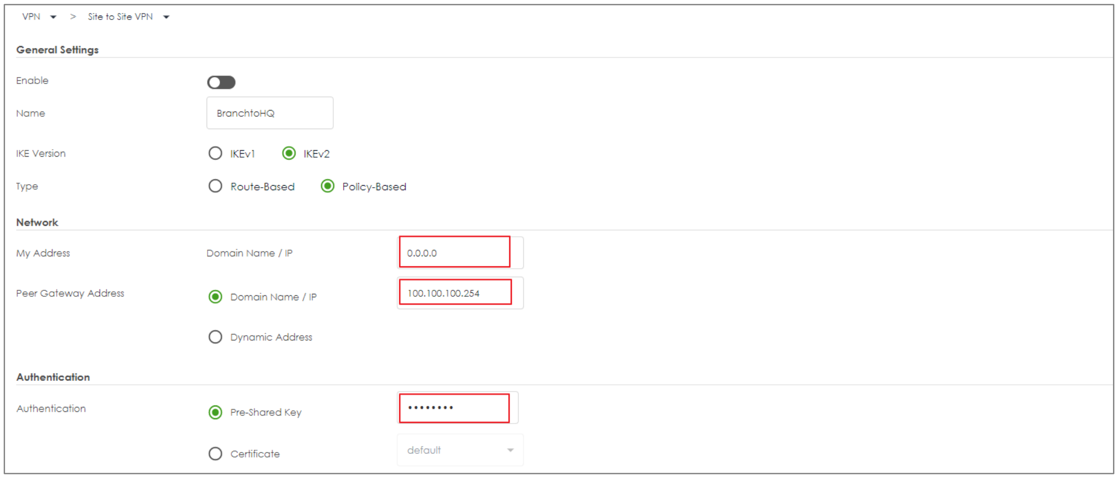
Type the VPN name used to identify this VPN connection. Select the type to the Custom. Click **Next.**



*Name	BranchtoHQ
IKE Version	○ IKEv1 ● IKEv2
Type	○ Site-to-Site ● Custom

VPN > Site to Site VPN

Type My Address as 0.0.0.0 and type Peer Gateway Address. Type a secure Pre-shared key.



General Settings

Enable		
Name	BranchtoHQ	
IKE Version	○ IKEv1 ● IKEv2	
Type	○ Route-Based ● Policy-Based	

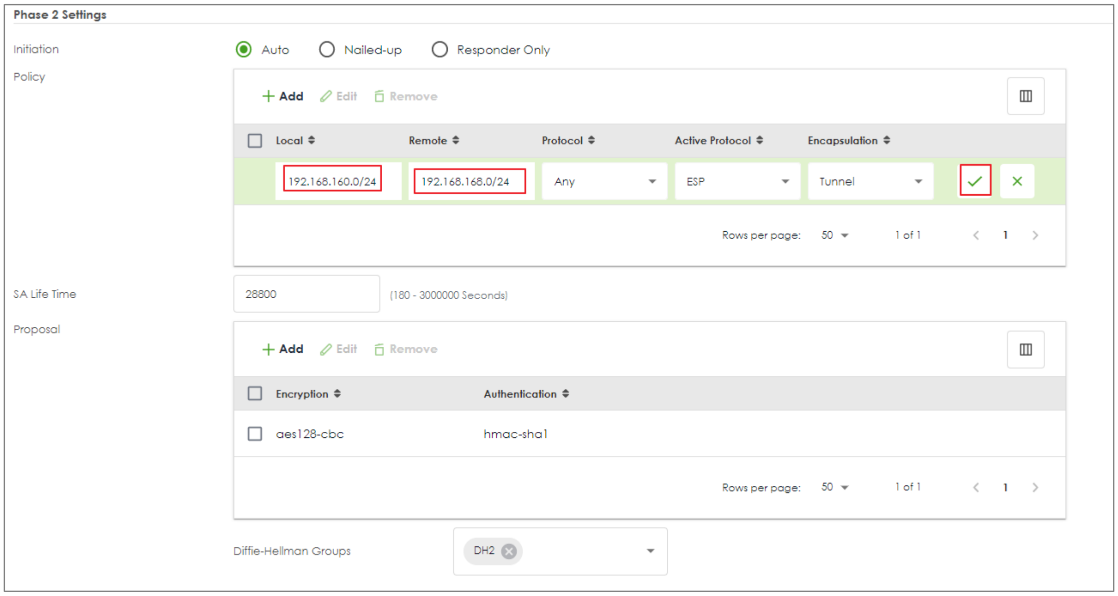
Network

My Address	Domain Name / IP	0.0.0.0
Peer Gateway Address	● Domain Name / IP	100.100.100.254
	○ Dynamic Address	

Authentication

Authentication	● Pre-Shared Key	••••••••
	○ Certificate	default

Scroll down to find the Phase2 setting, type Local and Remote Subnet. Then click save change.



Phase 2 Settings

Initiation ● Auto ○ Nailed-up ○ Responder Only

Policy

□	Local	Remote	Protocol	Active Protocol	Encapsulation
	192.168.160.0/24	192.168.168.0/24	Any	ESP	Tunnel

Rows per page: 50 1 of 1 1

SA Life Time 28800 (180 - 3000000 Seconds)

Proposal

□	Encryption	Authentication
□	aes128-cbc	hmac-sha1

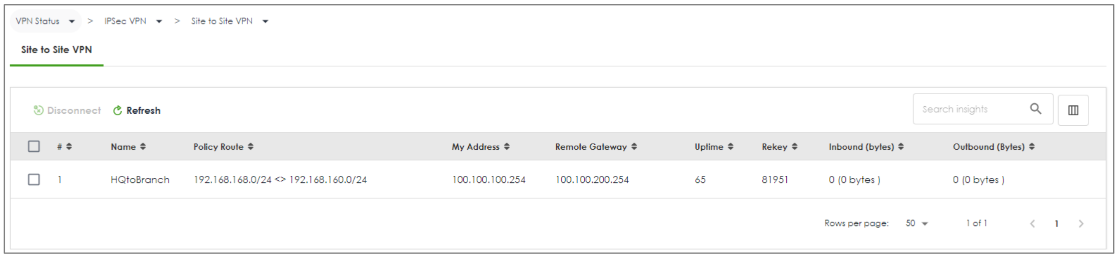
Rows per page: 50 1 of 1 1

Diffie-Hellman Groups DH2

Test IPSec VPN Tunnel

VPN Status > IPSec VPN

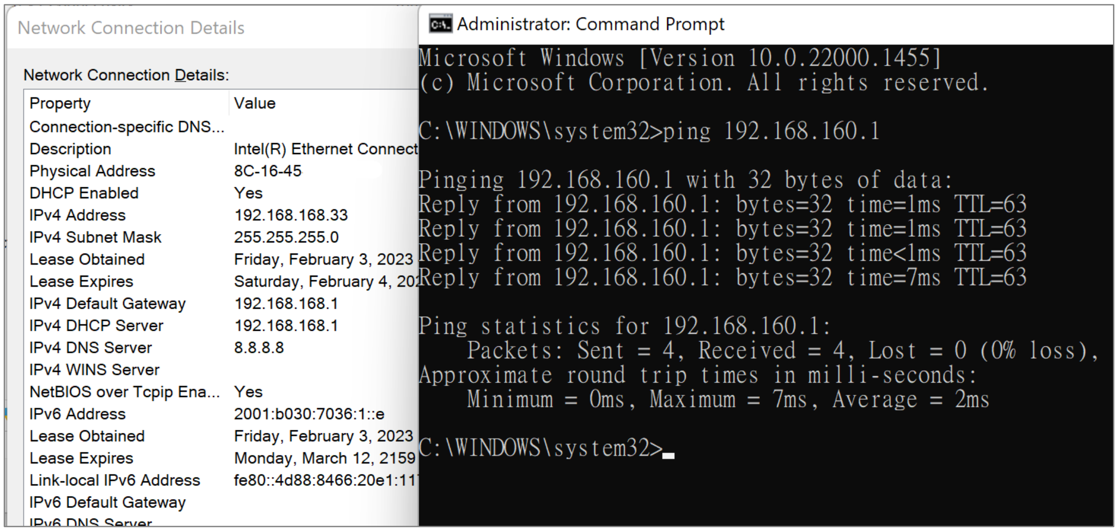
Verify the IPSec VPN status.



□	#	Name	Policy Route	My Address	Remote Gateway	Uptime	Rekey	Inbound (bytes)	Outbound (Bytes)
□	1	HQtoBranch	192.168.168.0/24 <> 192.168.160.0/24	100.100.100.254	100.100.200.254	65	81951	0 (0 bytes)	0 (0 bytes)

Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



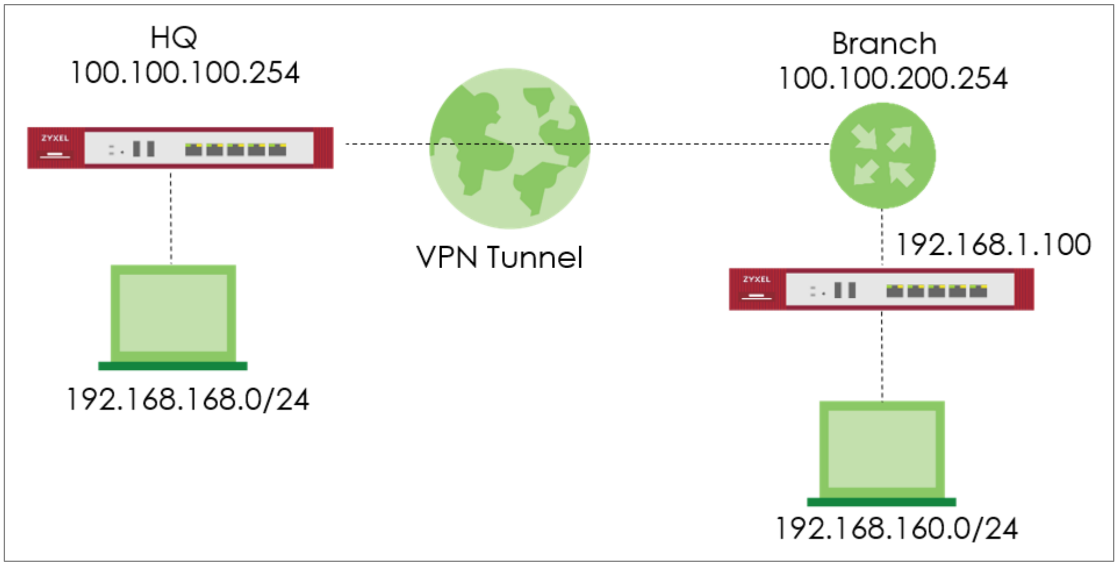
Network Connection Details:

Property	Value
Connection-specific DNS...	
Description	Intel(R) Ethernet Connect
Physical Address	8C-16-45
DHCP Enabled	Yes
IPv4 Address	192.168.168.33
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, February 3, 2023
Lease Expires	Saturday, February 4, 202
IPv4 Default Gateway	192.168.168.1
IPv4 DHCP Server	192.168.168.1
IPv4 DNS Server	8.8.8.8
IPv4 WINS Server	
NetBIOS over Tcpip Ena...	Yes
IPv6 Address	2001:b030:7036:1::e
Lease Obtained	Friday, February 3, 2023
Lease Expires	Monday, March 12, 2159
Link-local IPv6 Address	fe80::4d88:8466:20e1:11
IPv6 Default Gateway	
IPv6 DNS Server	

```
Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping 192.168.160.1

Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time<1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=7ms TTL=63

Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\WINDOWS\system32>
```

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 USG FLEX H 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.

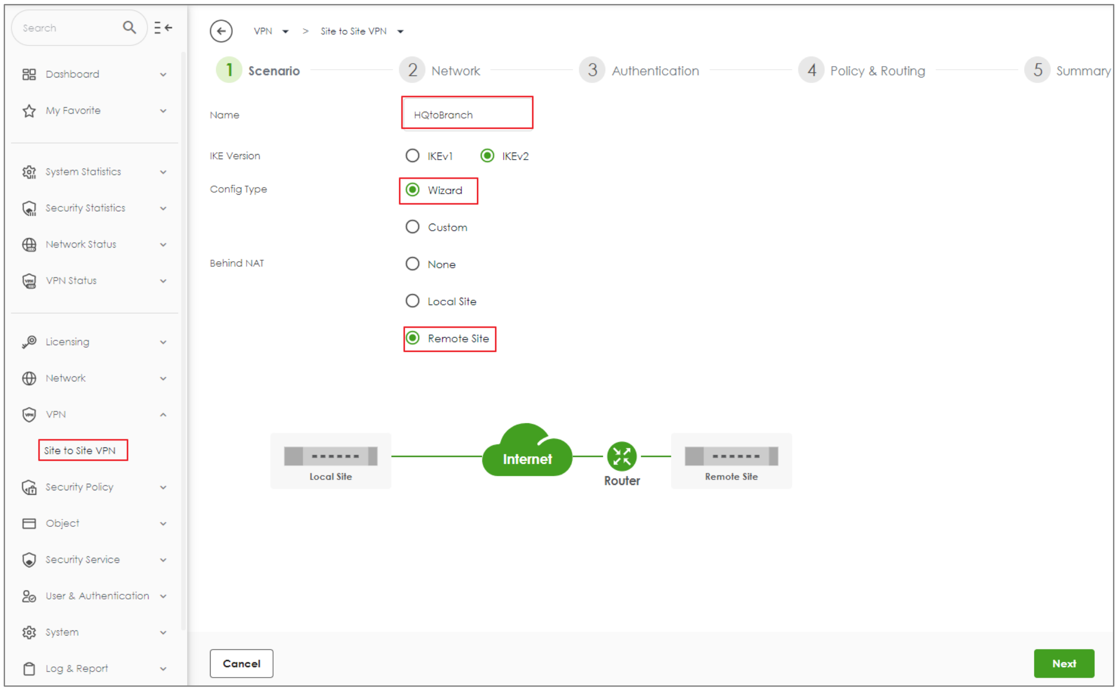


Note: Please ensure that you have NAT mapping UDP port 4500 to USG FLEX H device.

Set up IPSec VPN Tunnel for HQ

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the Behind NAT to the Remote Site. Click **Next**.



VPN > Site to Site VPN

1 Scenario — 2 Network — 3 Authentication — 4 Policy & Routing — 5 Summary

Name: HQtoBranch

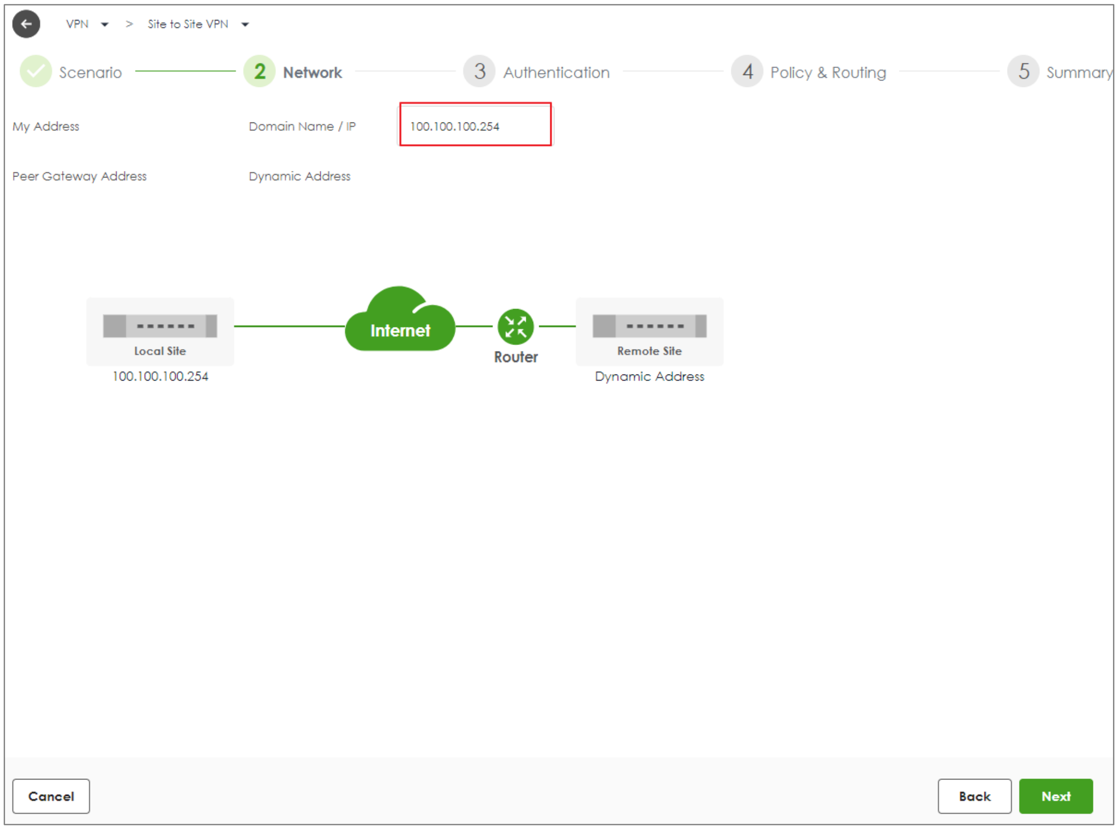
IKE Version: ○ IKEv1 ● IKEv2

Config Type: ● Wizard ○ Custom

Behind NAT: ○ None ○ Local Site ● Remote Site

VPN > Site to Site VPN > Scenario > Network

Configure My Address. Click **Next.**

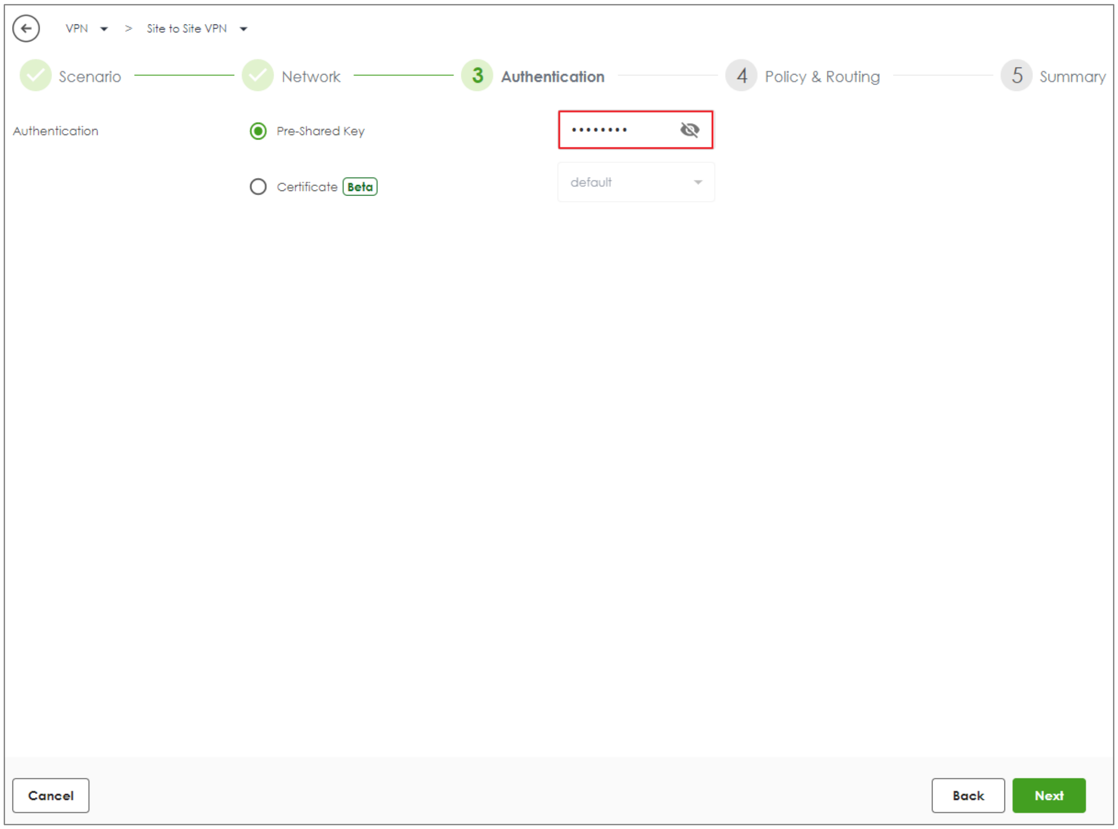


My Address — Domain Name / IP — 100.100.100.254

Peer Gateway Address — Dynamic Address

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**

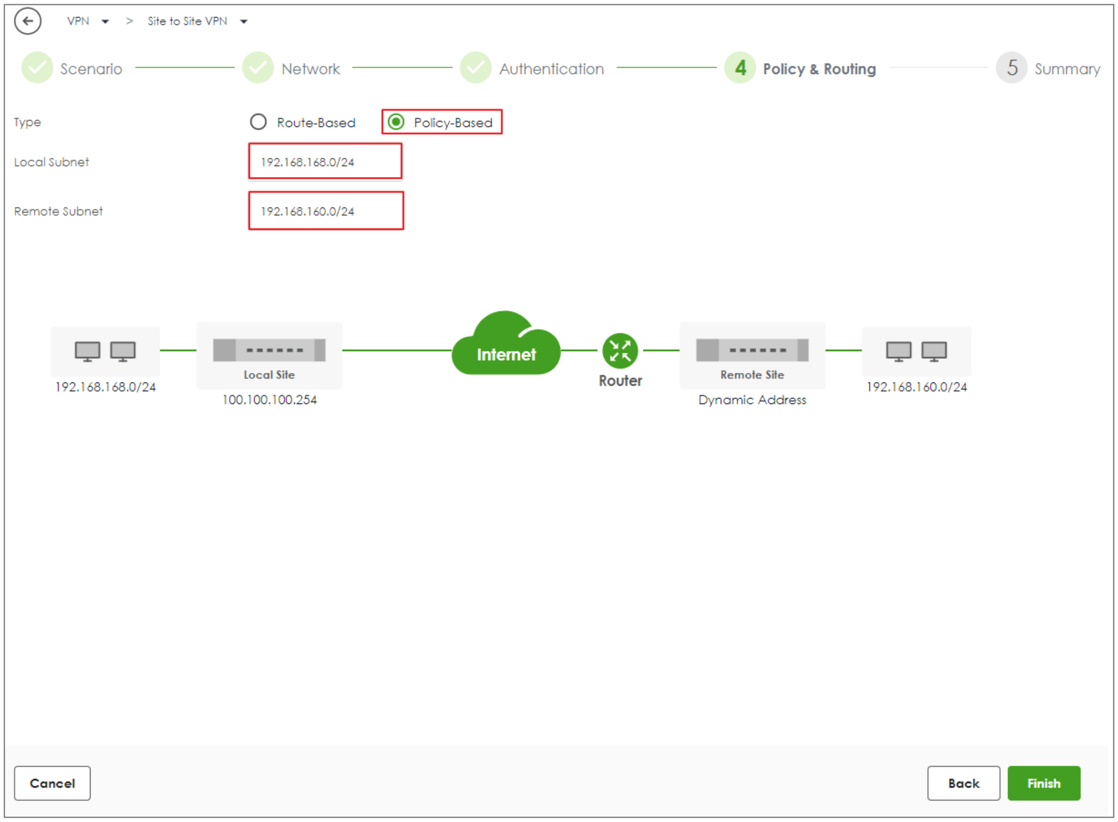


Authentication ● Pre-Shared Key ••••••••

○ Certificate Beta default

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.



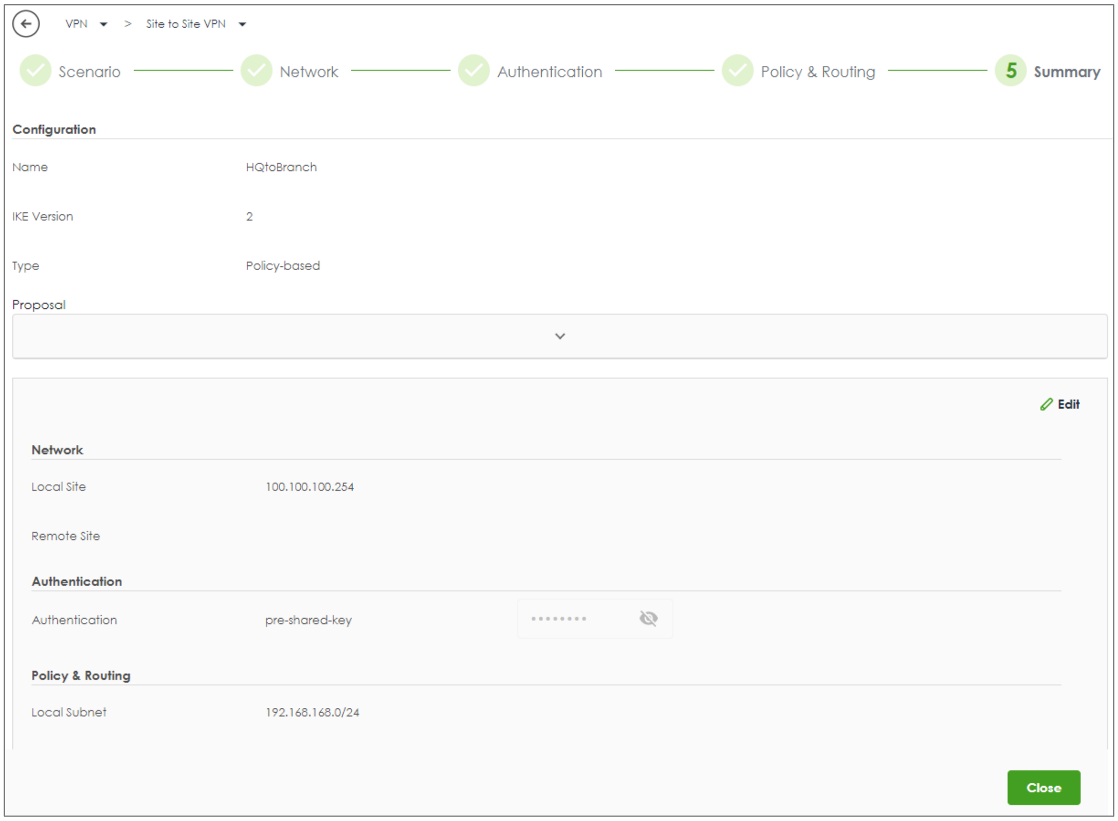
Type ○ Route-Based ● Policy-Based

Local Subnet 192.168.168.0/24

Remote Subnet 192.168.160.0/24

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



Configuration

Name HQtoBranch

IKE Version 2

Type Policy-based

Proposal

Network

Local Site 100.100.100.254

Remote Site

Authentication

Authentication pre-shared-key ••••••••

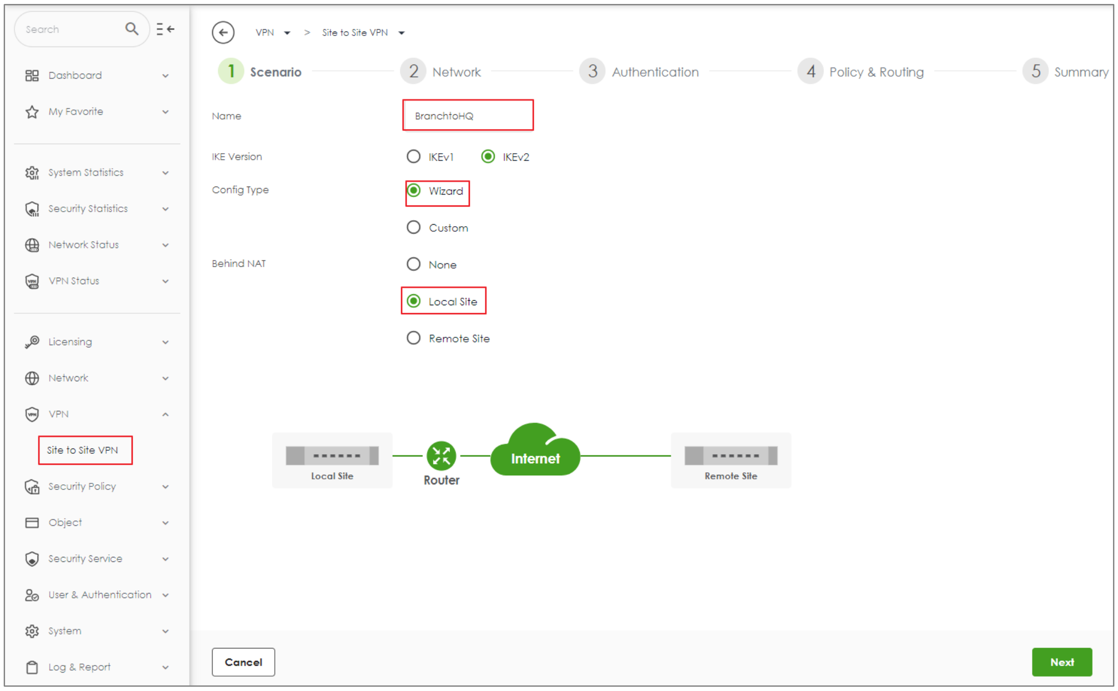
Policy & Routing

Local Subnet 192.168.168.0/24

Set up IPSec VPN Tunnel for Branch

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the Behind NAT to the Local Site. Click **Next.**



Name: BranchtoHQ

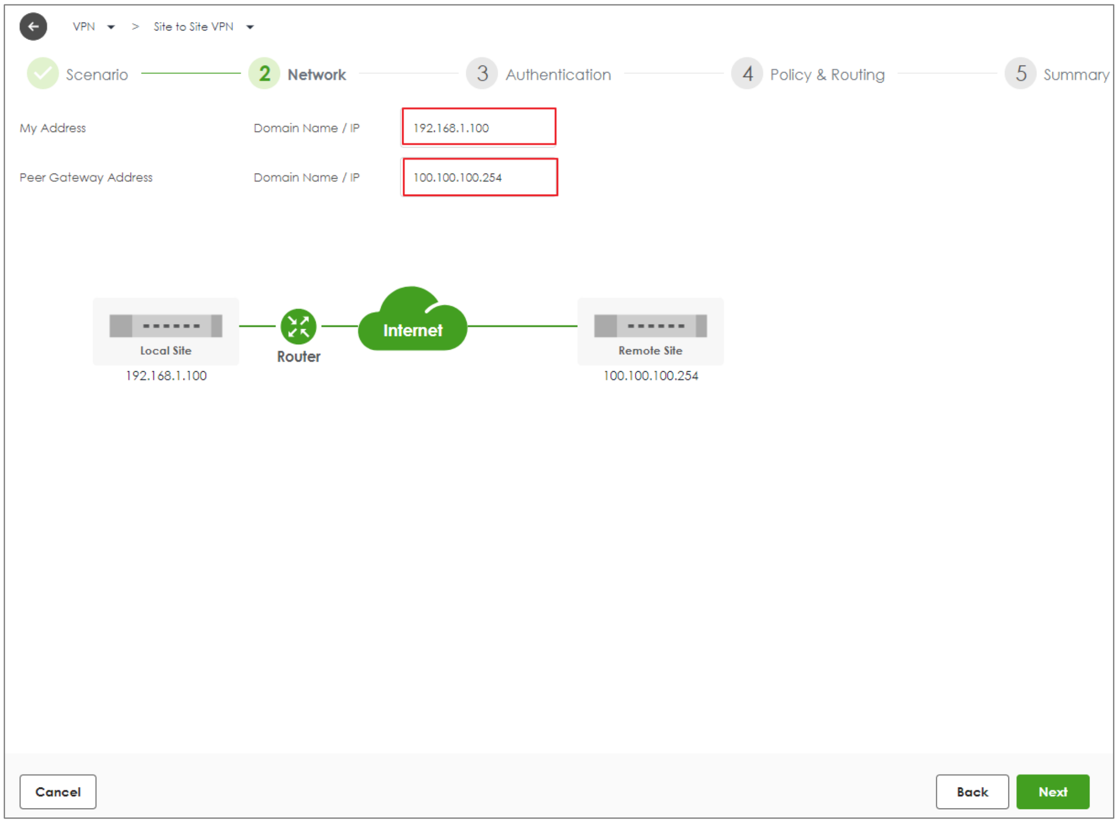
IKE Version: ○ IKEv1 ● IKEv2

Config Type: ● Wizard ○ Custom

Behind NAT: ○ None ● Local Site ○ Remote Site

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next.**



VPN > Site to Site VPN

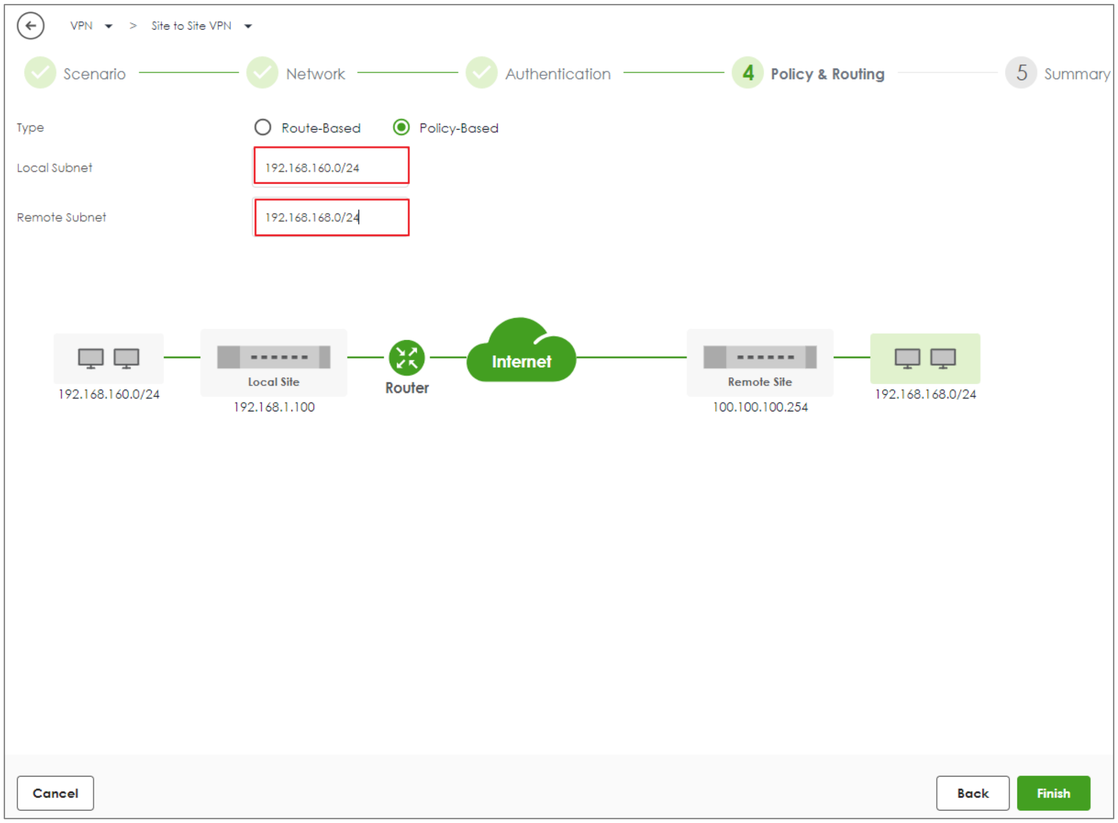
Scenario — 2 Network — 3 Authentication — 4 Policy & Routing — 5 Summary

My Address — Domain Name / IP: 192.168.1.100

Peer Gateway Address — Domain Name / IP: 100.100.100.254

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Local Subnet to be the IP address of the network connected to the gateway and Remote Subnet to be the IP address of the network connected to the peer gateway.



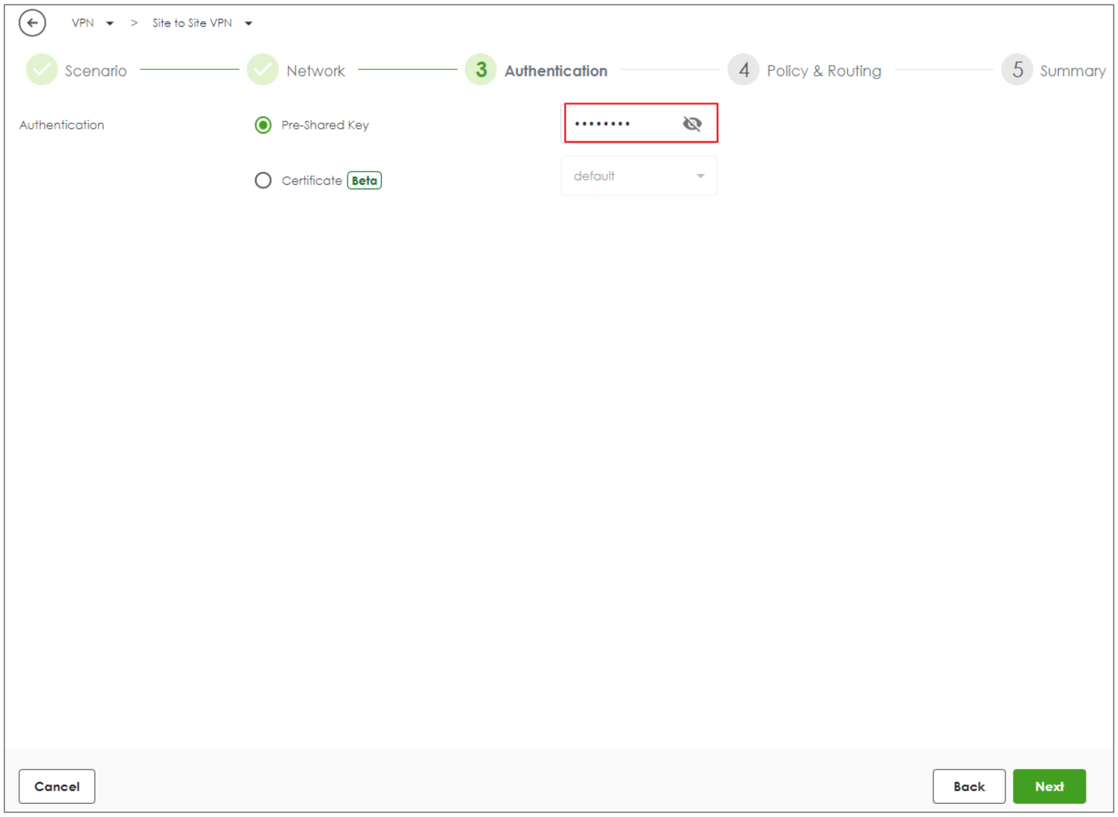
Type ○ Route-Based ● Policy-Based

Local Subnet 192.168.160.0/24

Remote Subnet 192.168.168.0/24

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**

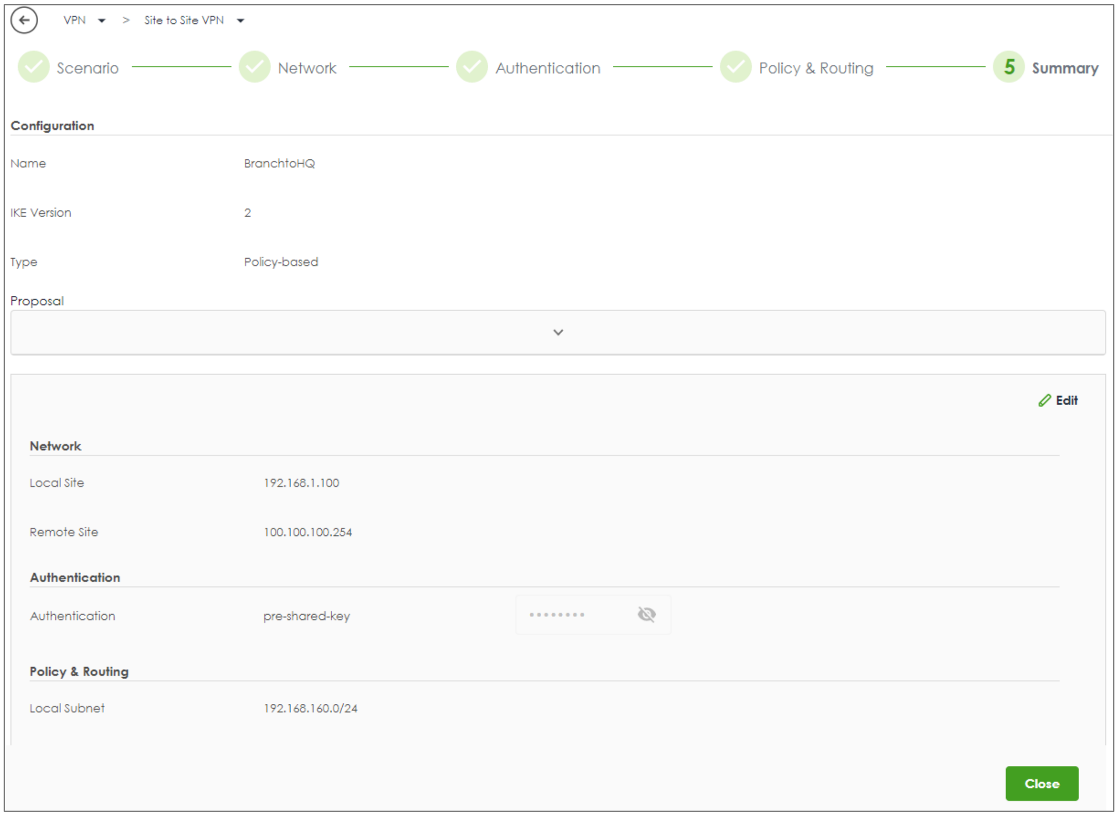


Authentication ● Pre-Shared Key ••••••••

○ Certificate Beta default

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



Configuration

Name	BranchtoHQ
IKE Version	2
Type	Policy-based

Proposal

Network

Local Site	192.168.1.100
Remote Site	100.100.100.254

Authentication

Authentication	pre-shared-key	••••••••

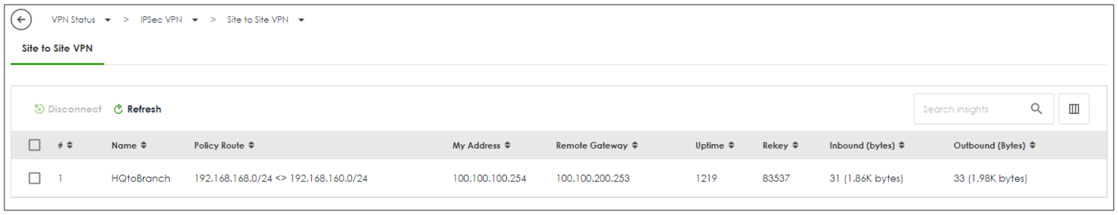
Policy & Routing

Local Subnet	192.168.160.0/24

Test IPSec VPN Tunnel

VPN Status > IPSec VPN

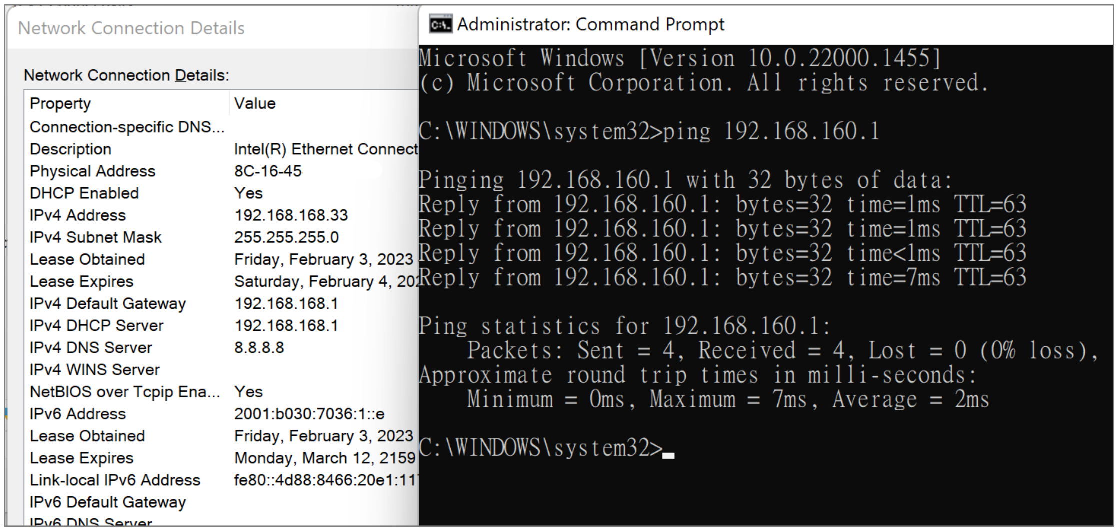
Verify the IPSec VPN status.



□	#	Name	Policy Route	My Address	Remote Gateway	Uptime	Rekey	Inbound (bytes)	Outbound (Bytes)
□	1	HQtoBranch	192.168.168.0/24 <> 192.168.160.0/24	100.100.100.254	100.100.200.253	1219	83537	31 (1.86K bytes)	33 (1.98K bytes)

Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



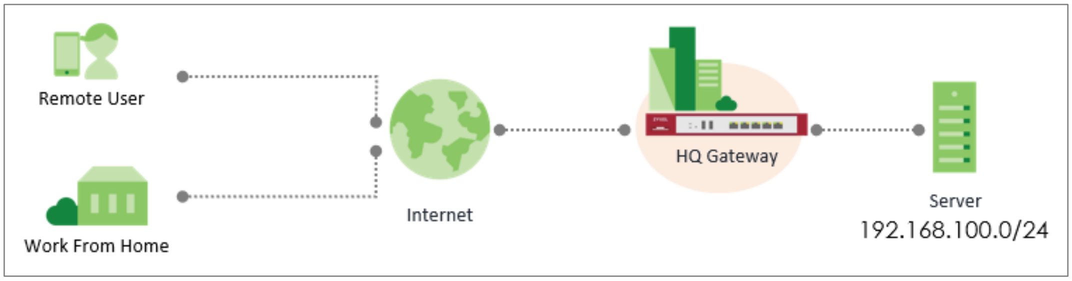
Network Connection Details:

Property	Value
Connection-specific DNS...	
Description	Intel(R) Ethernet Connect
Physical Address	8C-16-45
DHCP Enabled	Yes
IPv4 Address	192.168.168.33
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, February 3, 2023
Lease Expires	Saturday, February 4, 202
IPv4 Default Gateway	192.168.168.1
IPv4 DHCP Server	192.168.168.1
IPv4 DNS Server	8.8.8.8
IPv4 WINS Server	
NetBIOS over Tcpip Ena...	Yes
IPv6 Address	2001:b030:7036:1::e
Lease Obtained	Friday, February 3, 2023
Lease Expires	Monday, March 12, 2159
Link-local IPv6 Address	fe80::4d88:8466:20e1:11
IPv6 Default Gateway	
IPv6 DNS Server	

```
Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping 192.168.160.1

Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time<1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=7ms TTL=63

Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\WINDOWS\system32>_
```

How to Configure Remote Access VPN with Zyxel VPN Client

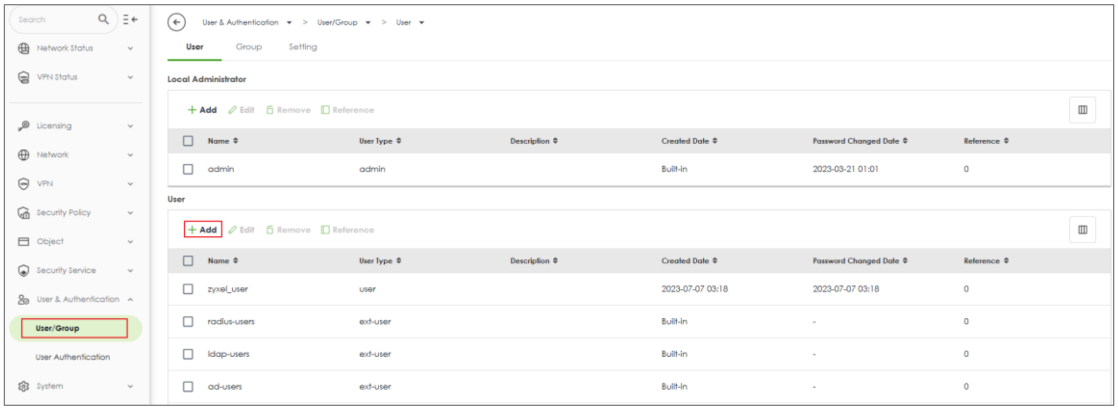
This example shows how to setup Remote Access VPN on USG FLEX H and Zyxel VPN Client. The example instructs how to implement Remote Access VPN by SSLVPN and IPSec VPN.



Before Begin

User & Authentication > User/Group > User

Create local user for remote access authentication.

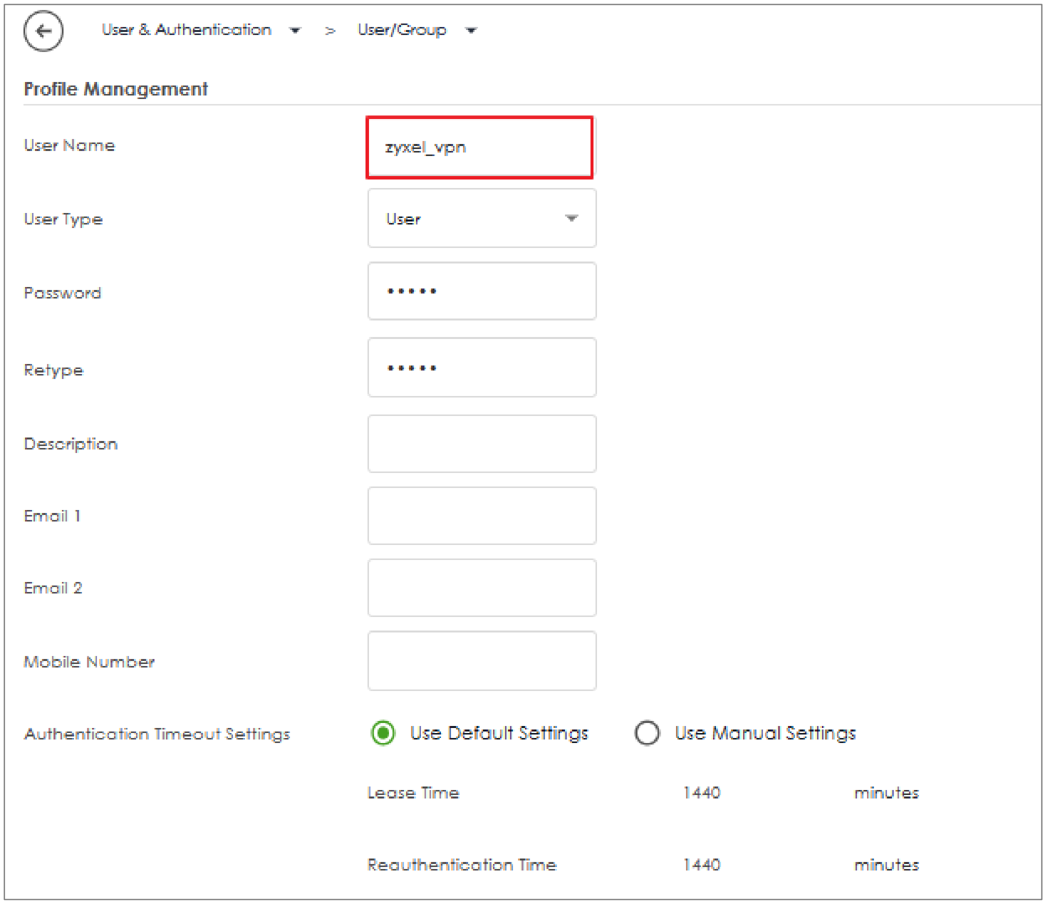


Local Administrator

	Name	User Type	Description	Created Date	Password Changed Date	Reference
□	admin	admin		Built-in	2023-03-21 01:01	0

User

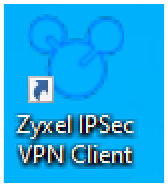
	Name	User Type	Description	Created Date	Password Changed Date	Reference
□	zyxel_user	user		2023-07-07 03:18	2023-07-07 03:18	0
□	radius-users	ext-user		Built-in	-	0
□	ldap-users	ext-user		Built-in	-	0
□	ad-users	ext-user		Built-in	-	0



Profile Management

User Name	zyxel_vpn
User Type	User
Password	•••••
Retype	•••••
Description	
Email 1	
Email 2	
Mobile Number	
Authentication Timeout Settings	● Use Default Settings ○ Use Manual Settings
	Lease Time 1440 minutes
	Reauthentication Time 1440 minutes

Download and install the new TGB Client

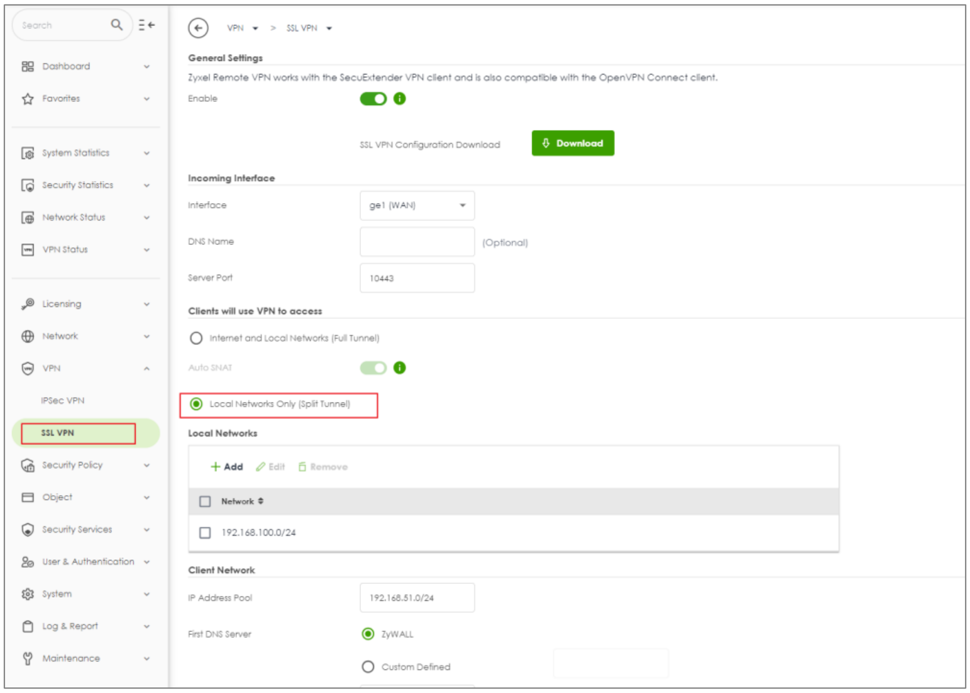


Set up SSL VPN

VPN > SSL VPN

Select the incoming interface, the default port is 10443. And up to your requirement to select Full Tunnel or Split Tunnel. And we now support OpenVPN config file.

For example: We pick up Split Tunnel and allows to access 192.168.100.0/24



General Settings

Zyxel Remote VPN works with the SecuExtender VPN client and is also compatible with the OpenVPN Connect client.

Enable: On

SSL VPN Configuration Download: Download

Incoming Interface

Interface: ge1 (WAN)

DNS Name: (Optional)

Server Port: 10443

Clients will use VPN to access

○ Internet and Local Networks (Full Tunnel)

Auto SNAT: On

● Local Networks Only (Split Tunnel)

Local Networks

+ Add   Edit   Remove

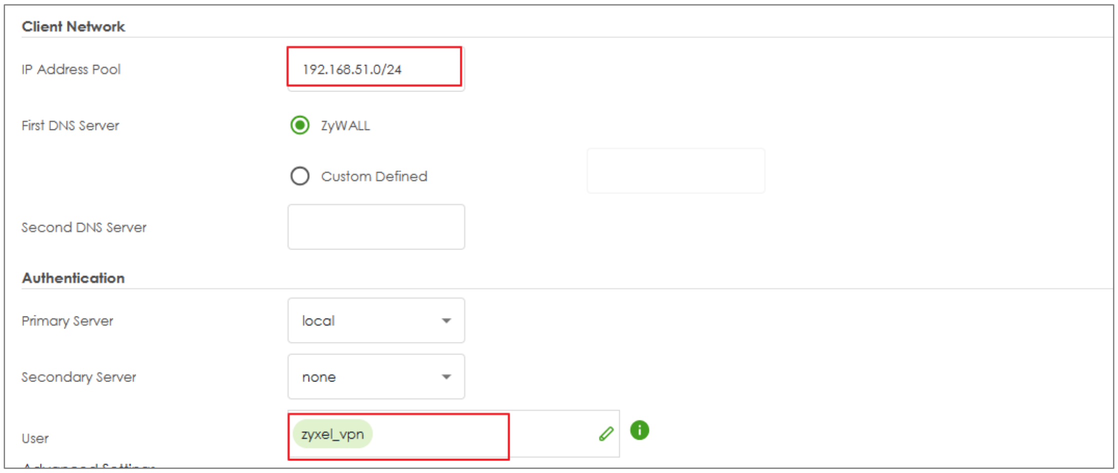
□	Network
□	192.168.100.0/24

Client Network

IP Address Pool: 192.168.51.0/24

First DNS Server: ● ZyWALL ○ Custom Defined

The default Address Pool is 192.168.51.0/24 and select the User who can access SSL VPN.



Client Network

IP Address Pool: 192.168.51.0/24

First DNS Server: ● ZyWALL ○ Custom Defined

Second DNS Server:

Authentication

Primary Server: local

Secondary Server: none

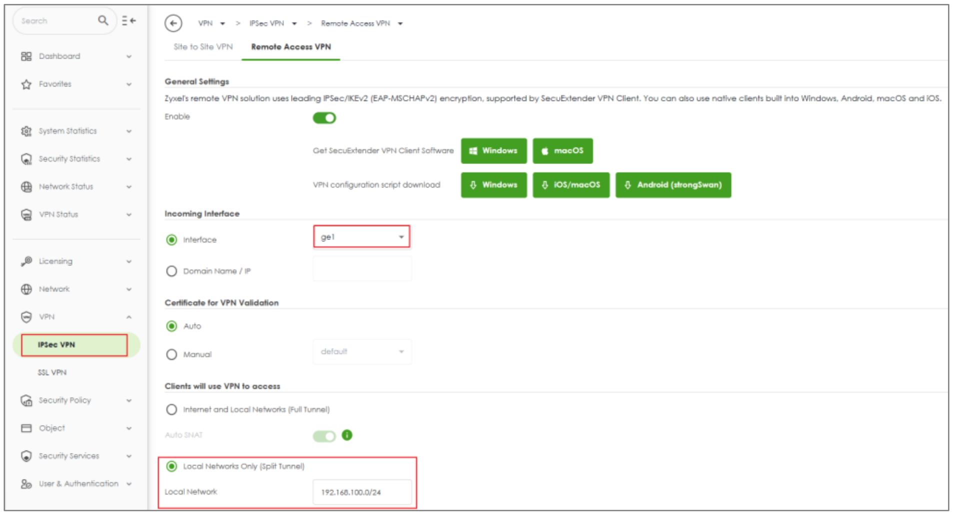
User: zyxel_vpn

Set up IKEv2 VPN

VPN > IPSec VPN > Remote Access VPN

Select the incoming interface. And up to your requirement to select Full Tunnel or Split Tunnel.

For example: We pick up Split Tunnel and allows to access 192.168.100.0/24



General Settings

Zyxel's remote VPN solution uses leading IPSec/IKEv2 (EAP-MSCHAPv2) encryption, supported by SecuExtender VPN Client. You can also use native clients built into Windows, Android, macOS and iOS.

Enable: on

Get SecuExtender VPN Client Software

VPN configuration script download

Incoming Interface

● Interface: ge1

○ Domain Name / IP

Certificate for VPN Validation

● Auto

○ Manual: default

Clients will use VPN to access

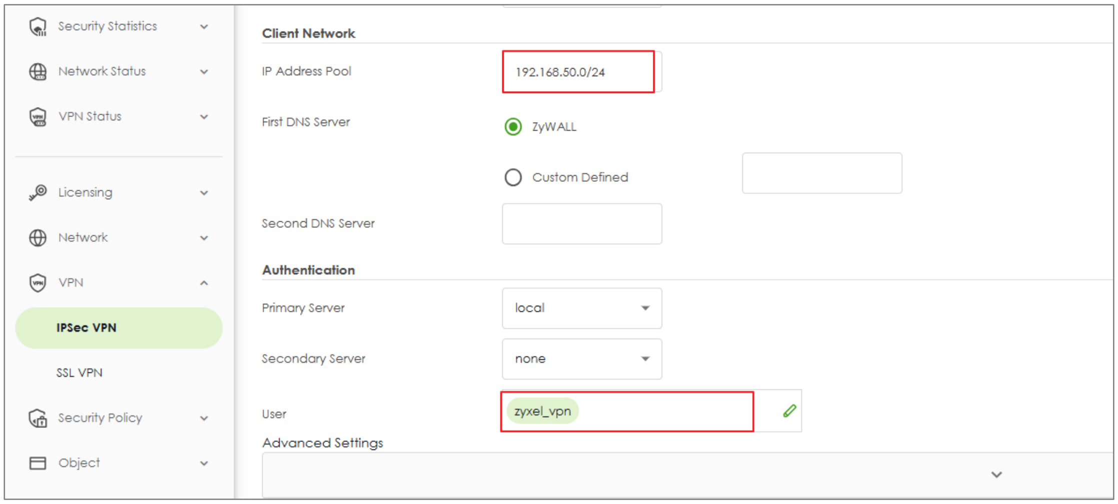
○ Internet and Local Networks (Full Tunnel)

Auto SNAT

● Local Networks Only (Split Tunnel)

Local Network: 192.168.100.0/24

The default Address Pool is 192.168.50.0/24 and select the User who can access IKEv2 VPN.



Client Network

IP Address Pool: 192.168.50.0/24

First DNS Server: ● ZyWALL ○ Custom Defined

Second DNS Server:

Authentication

Primary Server: local

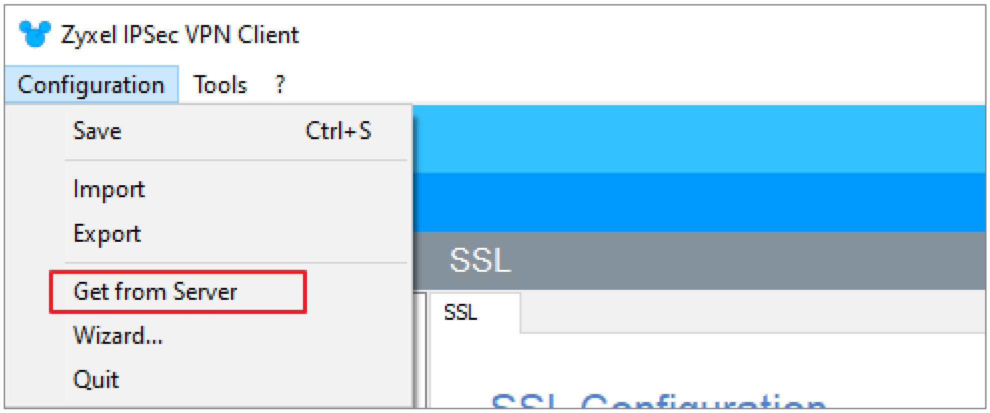
Secondary Server: none

User: zyxel_vpn

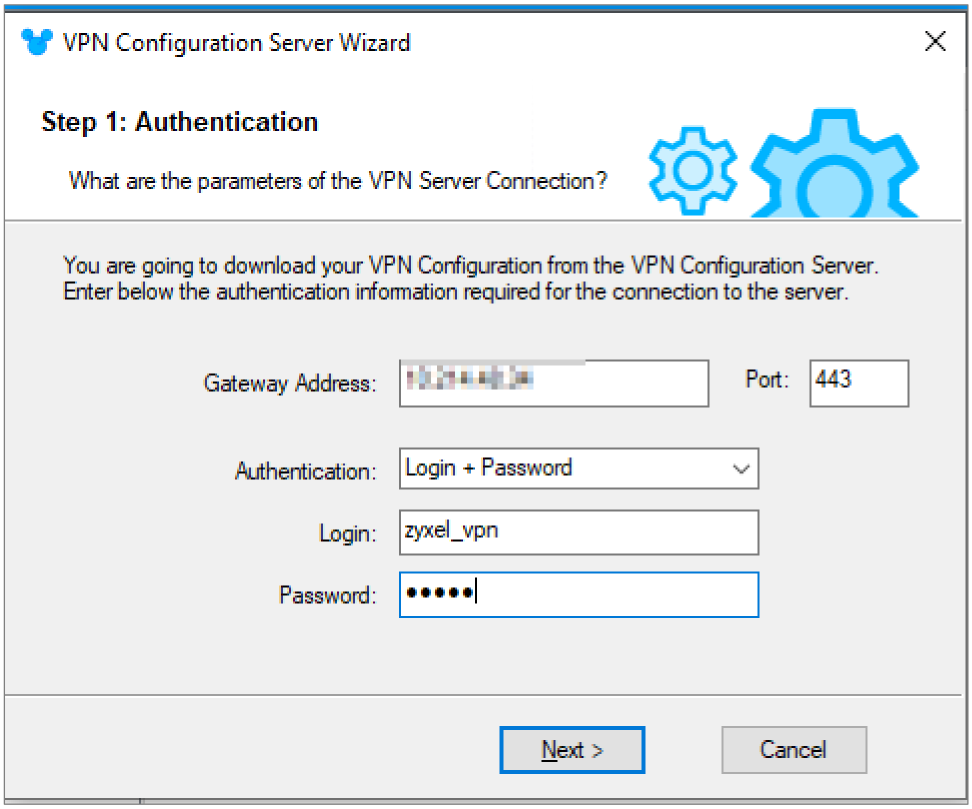
Advanced Settings

Set up Remote Access on TGB Client

The new TGB Client merge SSL VPN and IKEv2 VPN. You don't need additional software for each other.



Input the Gateway Address, Username and password to fetch configuration file.



VPN Configuration Server Wizard

Step 1: Authentication

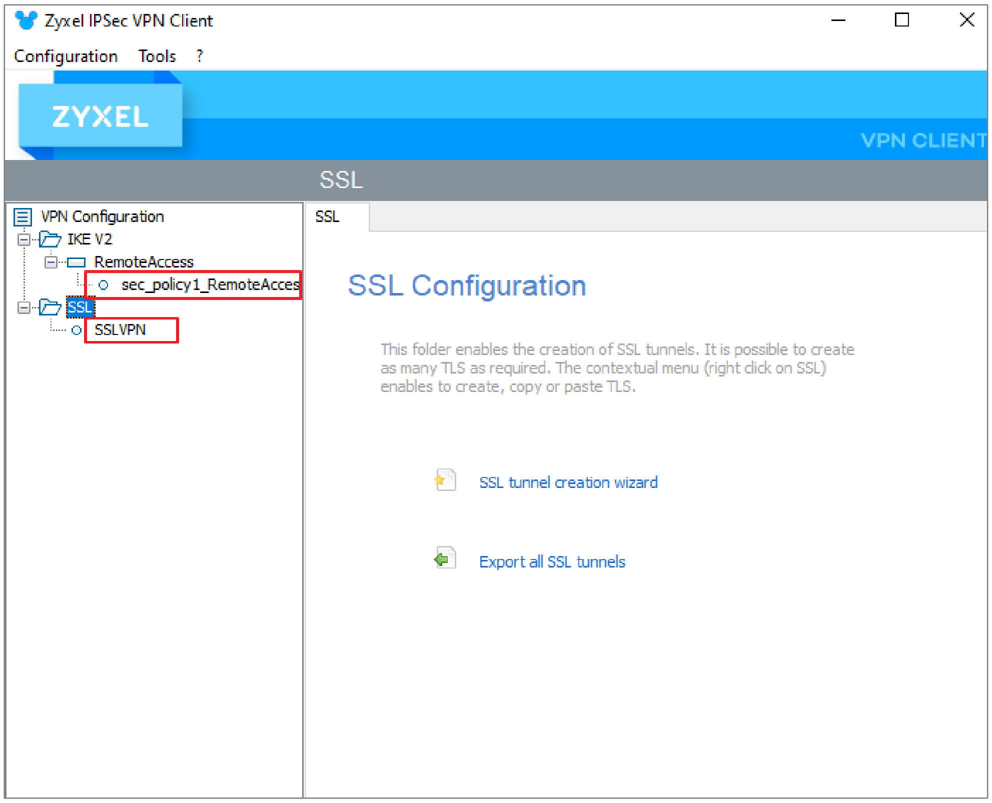
What are the parameters of the VPN Server Connection?

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: [redacted]
Port: 443

Authentication: Login + Password
Login: zyxel_vpn
Password: •••••

You will obtain IKEv2 as well as SSLVPN settings.



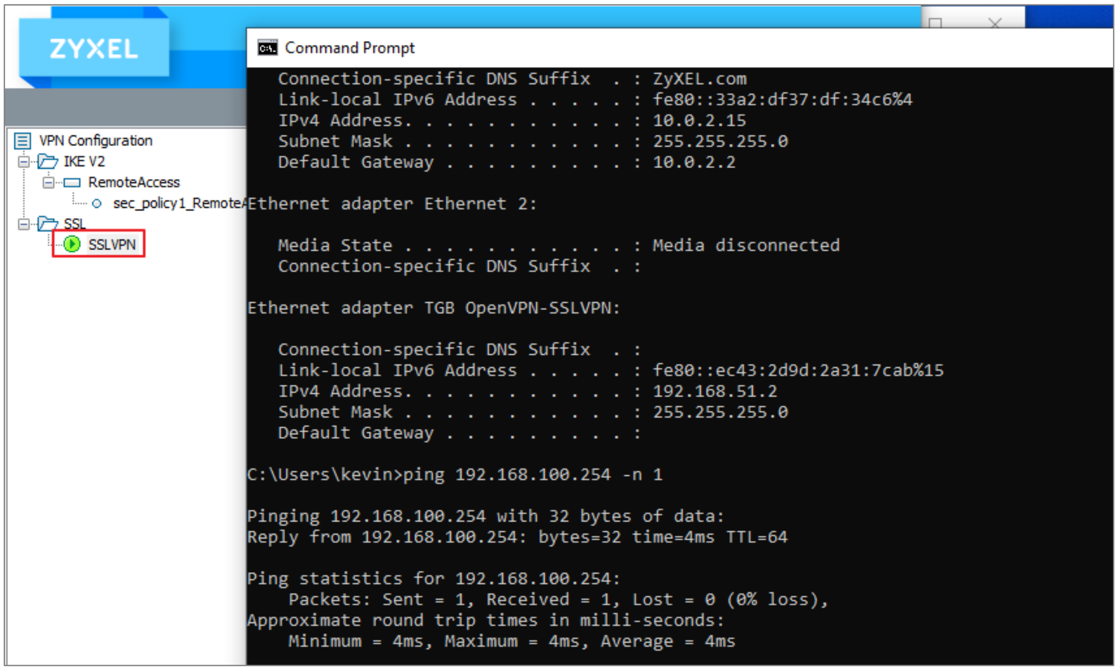
SSL Configuration

This folder enables the creation of SSL tunnels. It is possible to create as many TLS as required. The contextual menu (right click on SSL) enables to create, copy or paste TLS.

Test SSLVPN Tunnel on TGB Client

Right click the profile and “Open Tunnel” and log in.

You will see the profile being green and can access internal resource now.

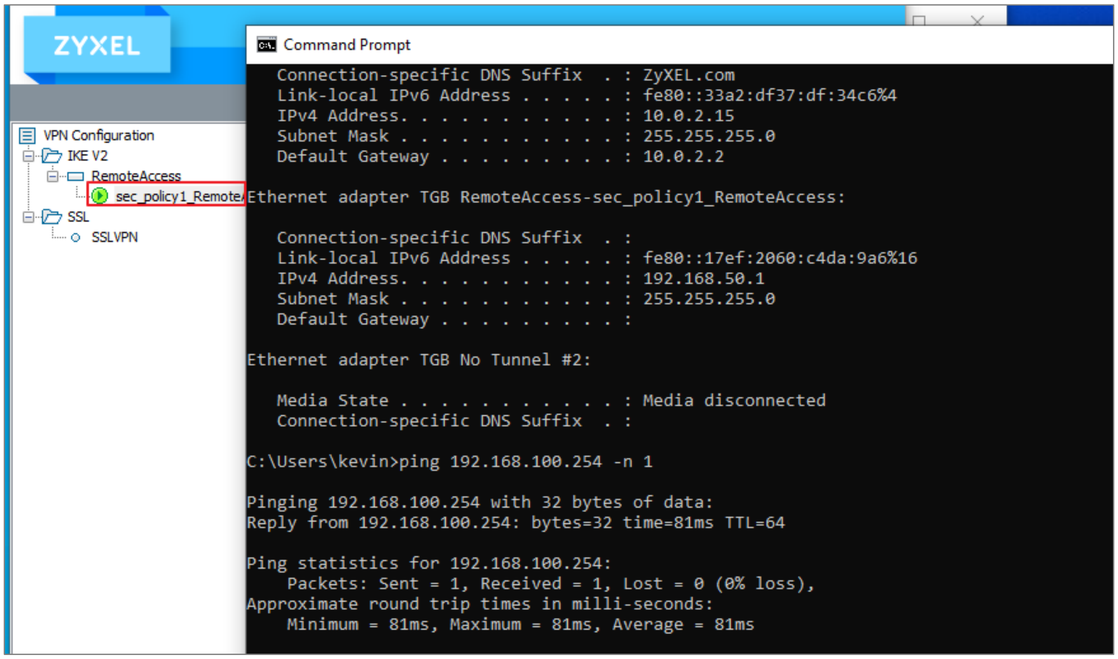


```
   Connection-specific DNS Suffix  . : ZyXEL.com
   Link-local IPv6 Address . . . . . : fe80::33a2:df37:df:34c6%4
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2

Ethernet adapter Ethernet 2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter TGB OpenVPN-SSLVPN:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ec43:2d9d:2a31:7cab%15
   IPv4 Address. . . . . . . . . . . : 192.168.51.2
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

C:\Users\kevin>ping 192.168.100.254 -n 1

Pinging 192.168.100.254 with 32 bytes of data:
Reply from 192.168.100.254: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.100.254:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 4ms, Average = 4ms
```

Test IKEv2 Tunnel on TGB Client

Right click the profile and "Open Tunnel" and log in.

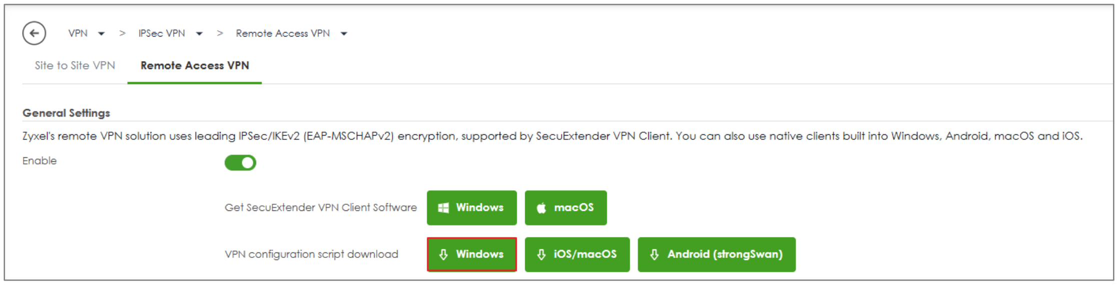
You will see the profile being green and can access internal resource now.



```
   Connection-specific DNS Suffix  . : ZyXEL.com
   Link-local IPv6 Address . . . . . : fe80::33a2:df37:df:34c6%4
   IPv4 Address. . . . . . . . . . . : 10.0.2.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.0.2.2

Ethernet adapter TGB RemoteAccess-sec_policy1_RemoteAccess:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::17ef:2060:c4da:9a6%16
   IPv4 Address. . . . . . . . . . . : 192.168.50.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter TGB No Tunnel #2:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\kevin>ping 192.168.100.254 -n 1

Pinging 192.168.100.254 with 32 bytes of data:
Reply from 192.168.100.254: bytes=32 time=81ms TTL=64

Ping statistics for 192.168.100.254:
    Packets: Sent = 1, Received = 1, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 81ms, Maximum = 81ms, Average = 81ms
```

Test IKEv2 Tunnel on Windows Client

Download Windows VPN configuration script

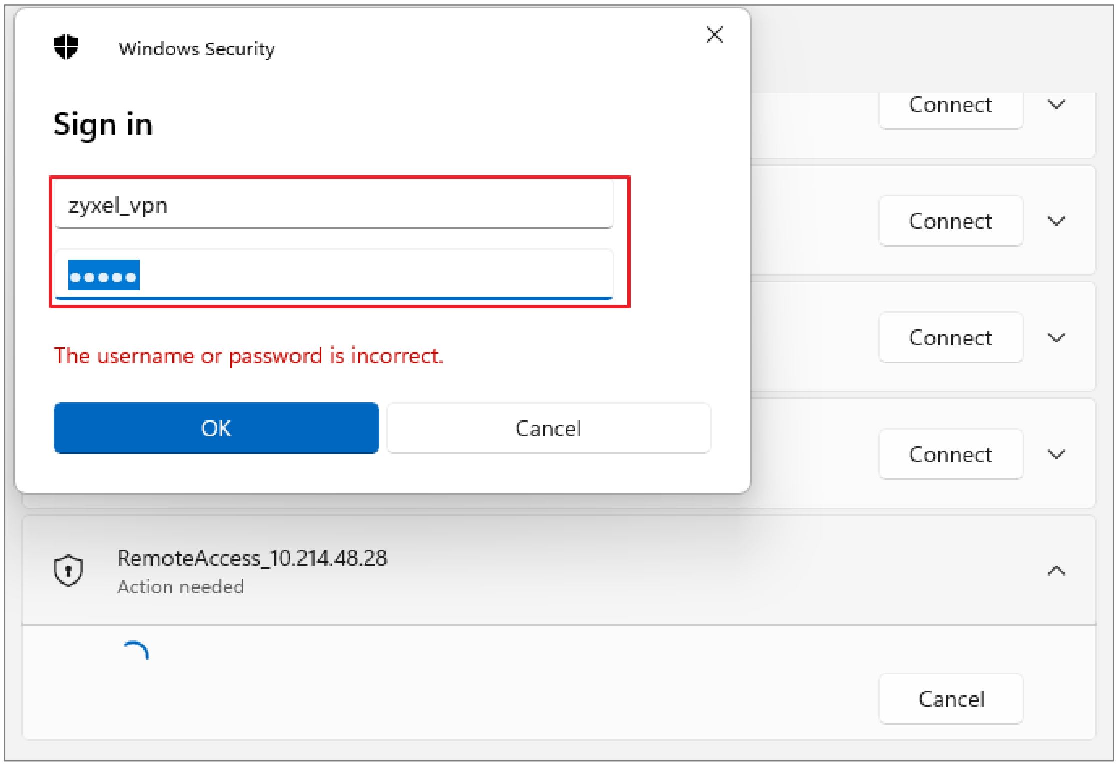

VPN > IPSec VPN > Remote Access VPN
Site to Site VPN
Remote Access VPN
Get SecuExtender VPN Client Software
Windows
macOS
VPN configuration script download
Windows
iOS/macOS
Android (strongSwan)

General Settings

Zyxel's remote VPN solution uses leading IPSec/IKEv2 (EAP-MSCHAPv2) encryption, supported by SecuExtender VPN Client. You can also use native clients built into Windows, Android, macOS and iOS.

Enable ●

Perform the windows bat file and input credentials.



Windows Security

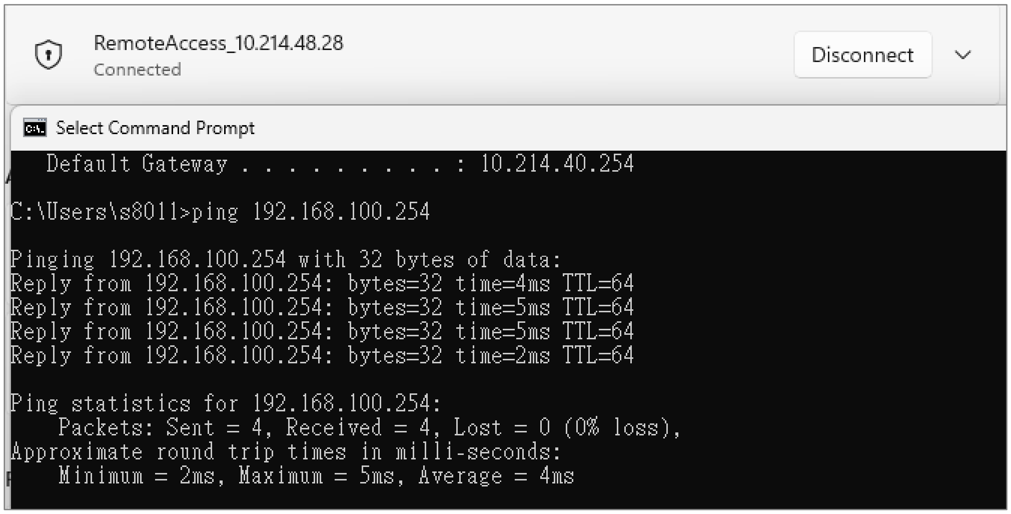
Sign in

zyxel_vpn

●●●●●

The username or password is incorrect.

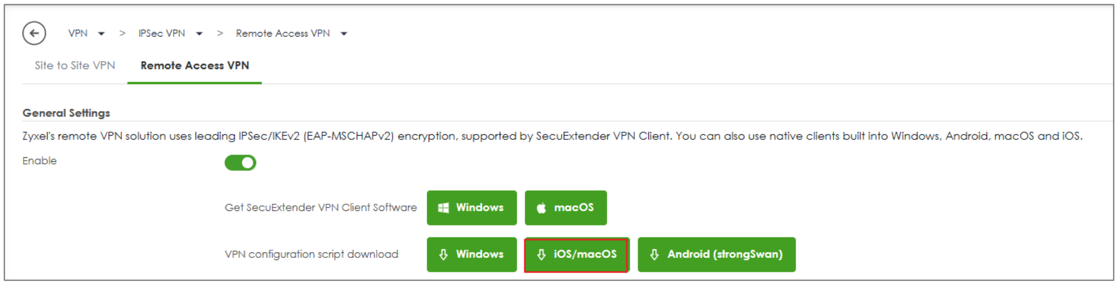
VPN is connected and can access internal resource.



```
   Default Gateway . . . . . . . . . : 10.214.40.254

C:\Users\s8011>ping 192.168.100.254

Pinging 192.168.100.254 with 32 bytes of data:
Reply from 192.168.100.254: bytes=32 time=4ms TTL=64
Reply from 192.168.100.254: bytes=32 time=5ms TTL=64
Reply from 192.168.100.254: bytes=32 time=5ms TTL=64
Reply from 192.168.100.254: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.100.254:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 5ms, Average = 4ms
```

Test IKEv2 Tunnel on iOS Client

Download iOS/macOS VPN configuration script.


VPN > IPSec VPN > Remote Access VPN
Site to Site VPN
Remote Access VPN

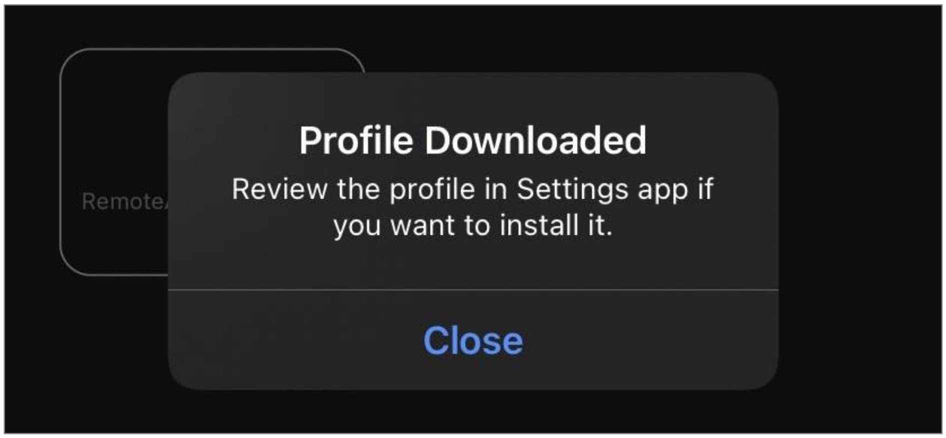
General Settings

Zyxel's remote VPN solution uses leading IPSec/IKEv2 (EAP-MSCHAPv2) encryption, supported by SecuExtender VPN Client. You can also use native clients built into Windows, Android, macOS and iOS.

Enable: on

Get SecuExtender VPN Client Software
Windows
macOS
VPN configuration script download
Windows
iOS/macOS
Android (strongSwan)

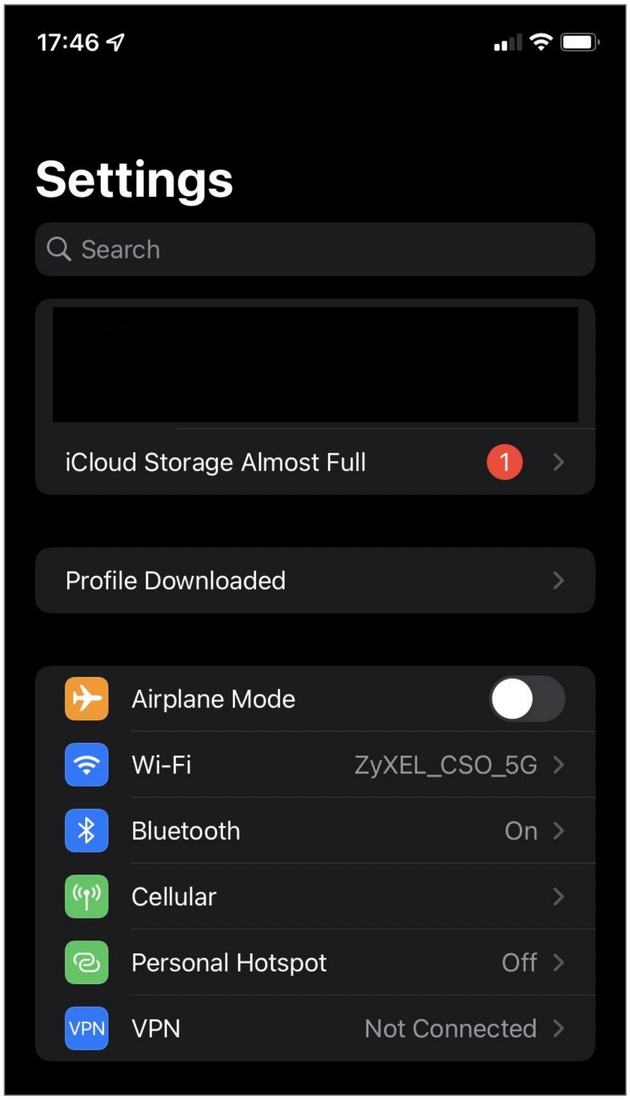
Send the script to Device.



Profile Downloaded

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

Settings > Profile Downloaded



17:46

Settings

Search

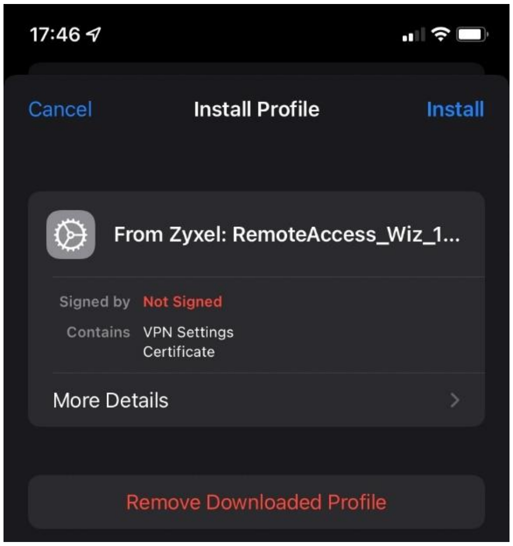
[redacted]

iCloud Storage Almost Full 1

Profile Downloaded

Airplane Mode	○
Wi-Fi	ZyXEL_CSO_5G
Bluetooth	On
Cellular	
Personal Hotspot	Off
VPN	Not Connected

Press Install.

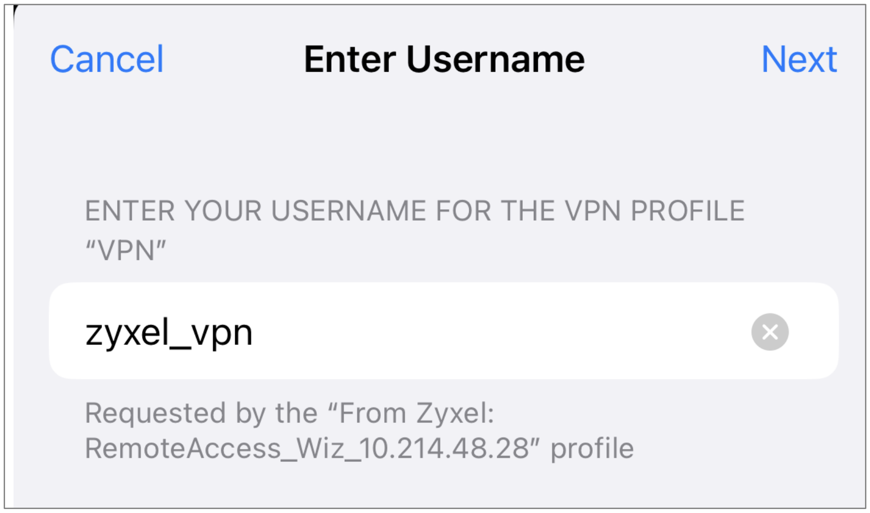


From Zyxel: RemoteAccess_Wiz_1...

Signed by Not Signed

Contains VPN Settings
Certificate

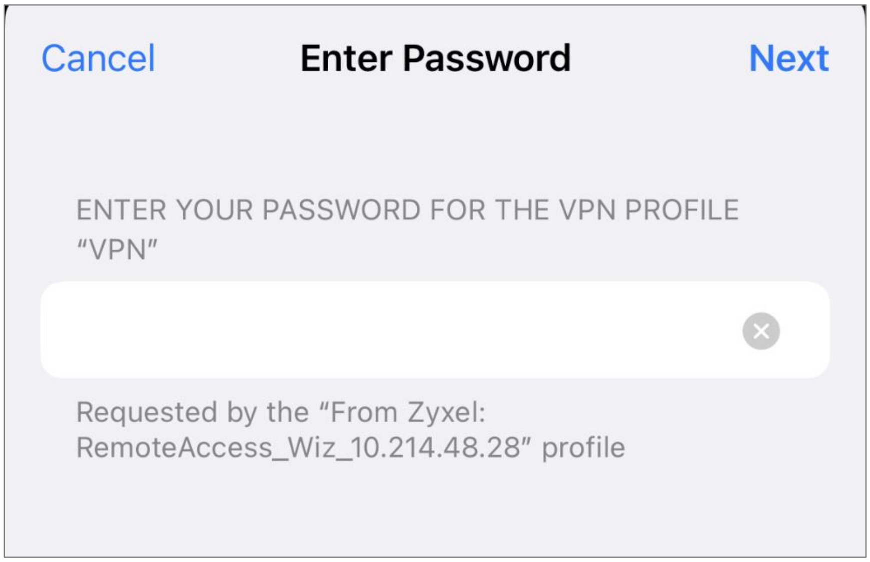
Enter Username and Password.



ENTER YOUR USERNAME FOR THE VPN PROFILE "VPN"

zyxel_vpn

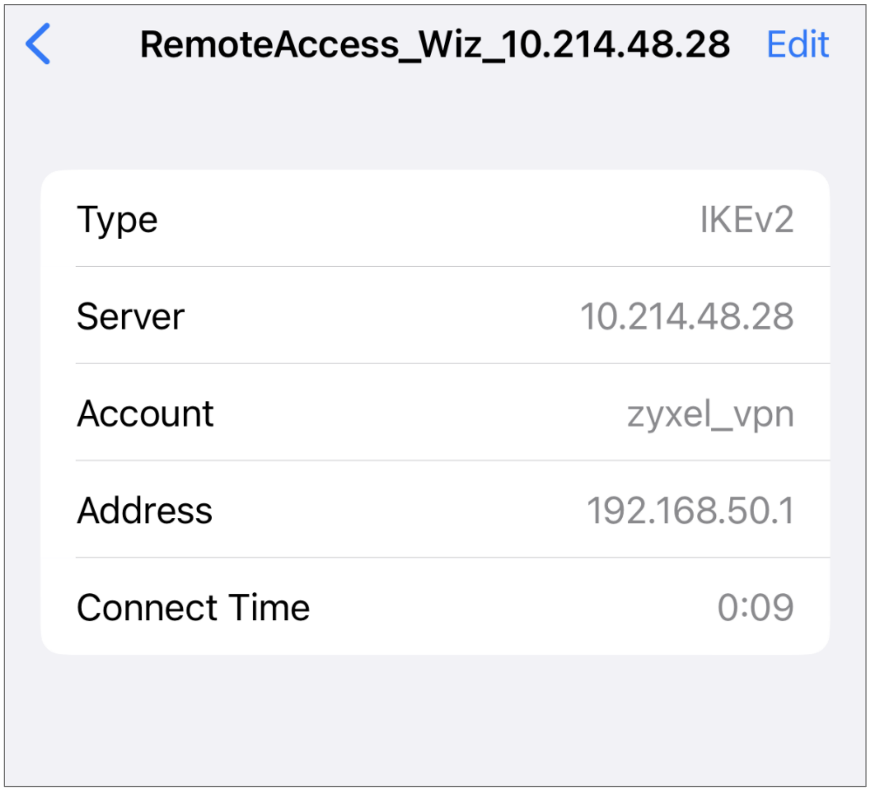
Requested by the "From Zyxel: RemoteAccess_Wiz_10.214.48.28" profile



ENTER YOUR PASSWORD FOR THE VPN PROFILE "VPN"

Requested by the "From Zyxel: RemoteAccess_Wiz_10.214.48.28" profile

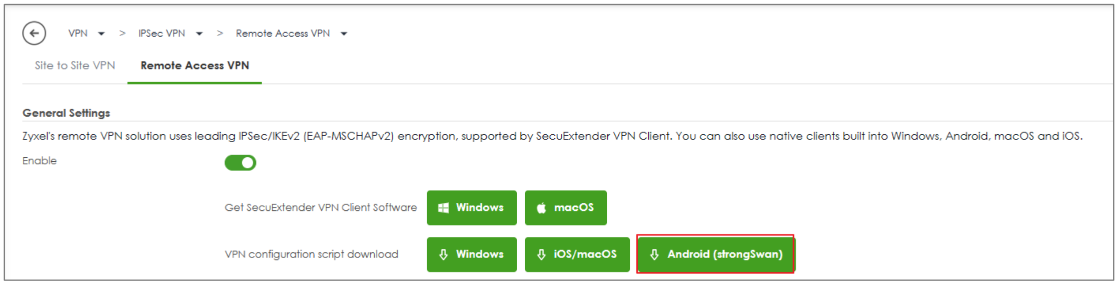
Now, it can connect.



Type	IKEv2
Server	10.214.48.28
Account	zyxel_vpn
Address	192.168.50.1
Connect Time	0:09

Test IKEv2 Tunnel on Android Client

Download Android(strongSwan) VPN configuration script.



VPN > IPSec VPN > Remote Access VPN

Site to Site VPN | **Remote Access VPN**

General Settings

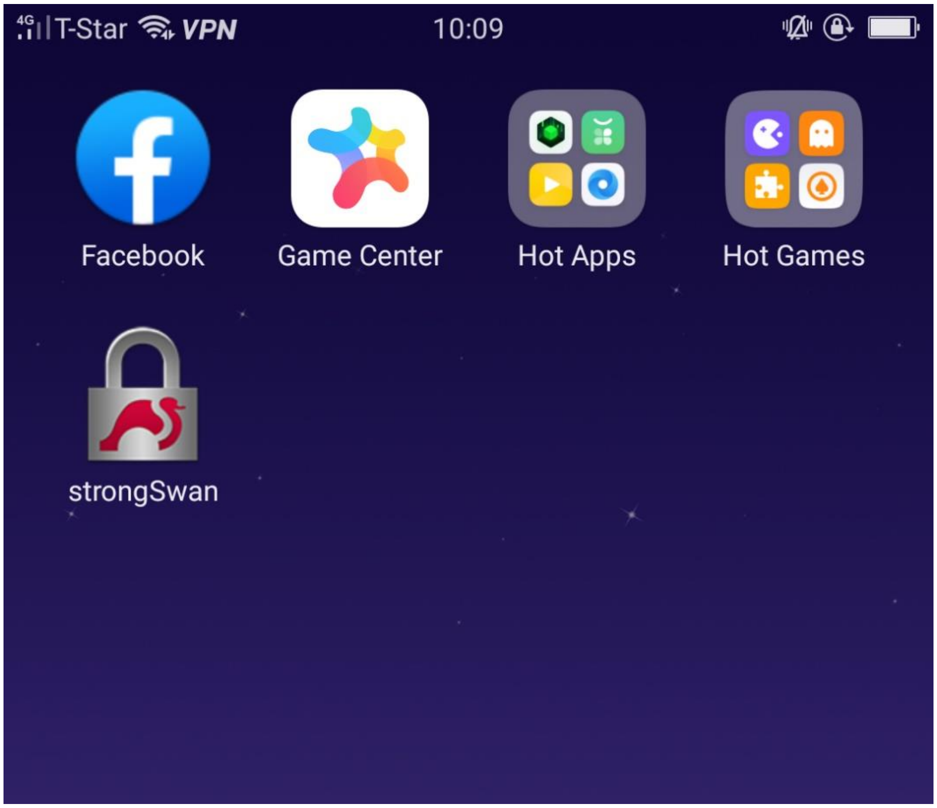
Zyxel's remote VPN solution uses leading IPSec/IKEv2 (EAP-MSCHAPv2) encryption, supported by SecuExtender VPN Client. You can also use native clients built into Windows, Android, macOS and iOS.

Enable ●

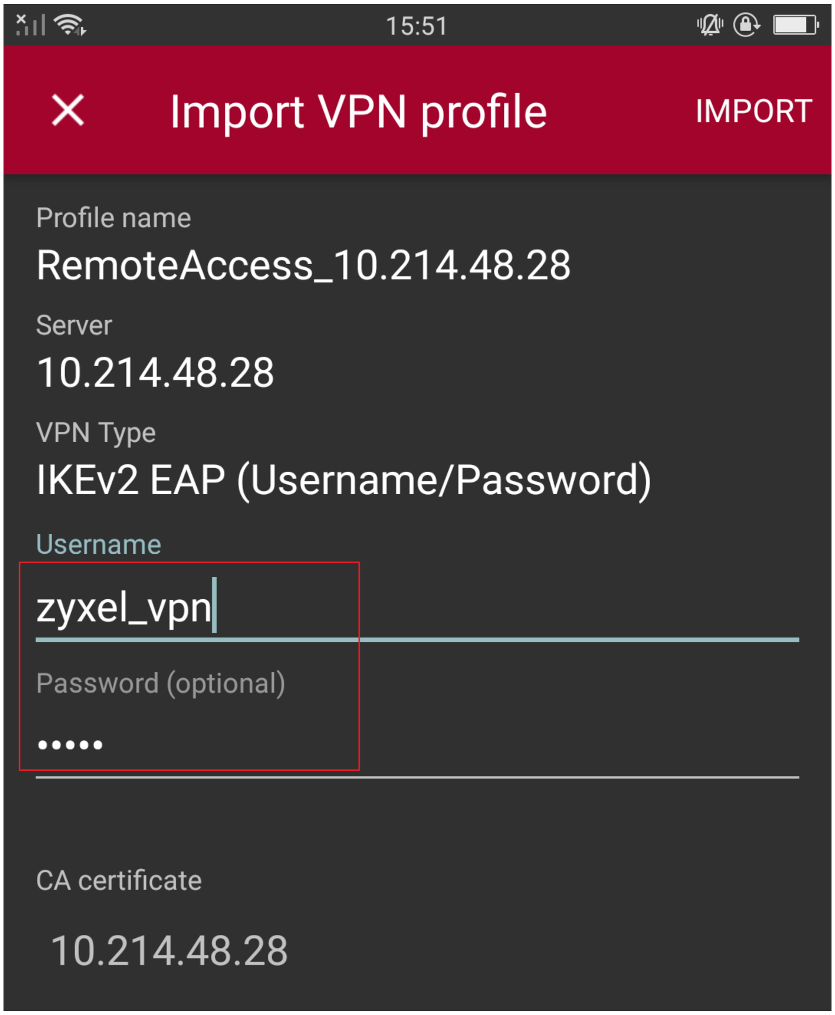
Get SecuExtender VPN Client Software: Windows | macOS

VPN configuration script download: Windows | iOS/macOS | Android (strongSwan)

Download strongSwan from Google Play Store.



Send the script to device then Install and Import strongSwan profile.



15:51

Profile name
RemoteAccess_10.214.48.28

Server
10.214.48.28

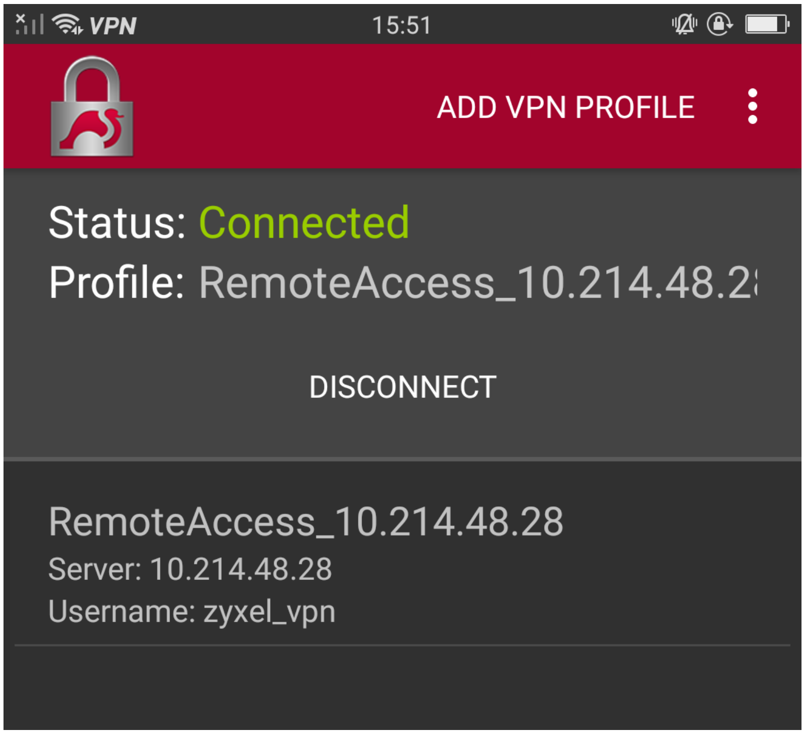
VPN Type
IKEv2 EAP (Username/Password)

Username
zyxel_vpn

Password (optional)
•••••

CA certificate
10.214.48.28

VPN is connected.



Status: Connected

Profile: RemoteAccess_10.214.48.2

RemoteAccess_10.214.48.28

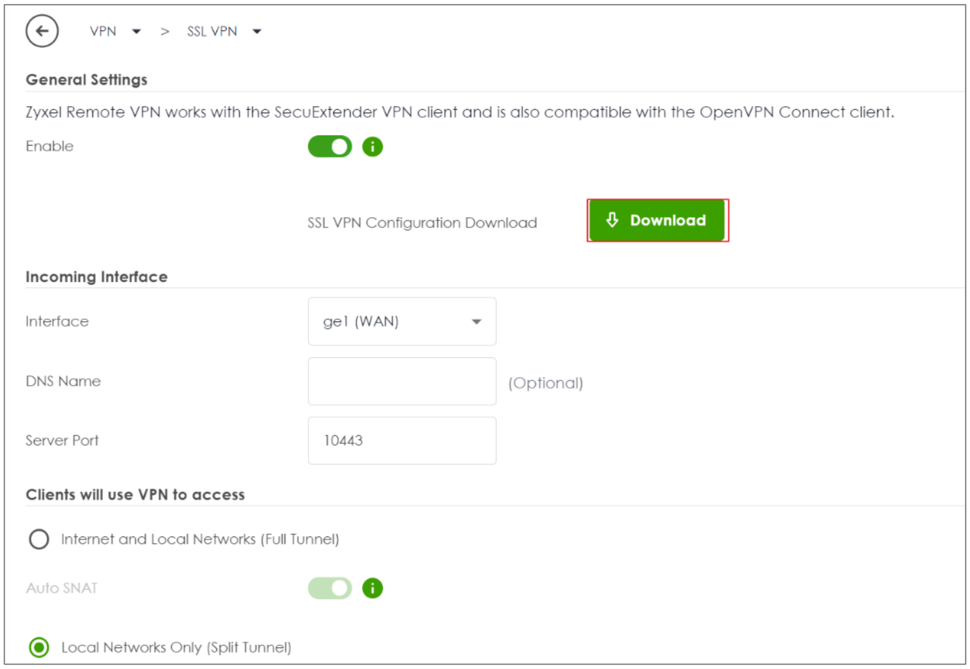
Server: 10.214.48.28

Username: zyxel_vpn

Test OpenVPN

VPN > SSL VPN

We now support OpenVPN config file, Click Download to obtain the ovpn file.



General Settings

Zyxel Remote VPN works with the SecuExtender VPN client and is also compatible with the OpenVPN Connect client.

Enable	●
SSL VPN Configuration Download	Download

Incoming Interface

Interface	ge1 (WAN)	
DNS Name		(Optional)
Server Port	10443	

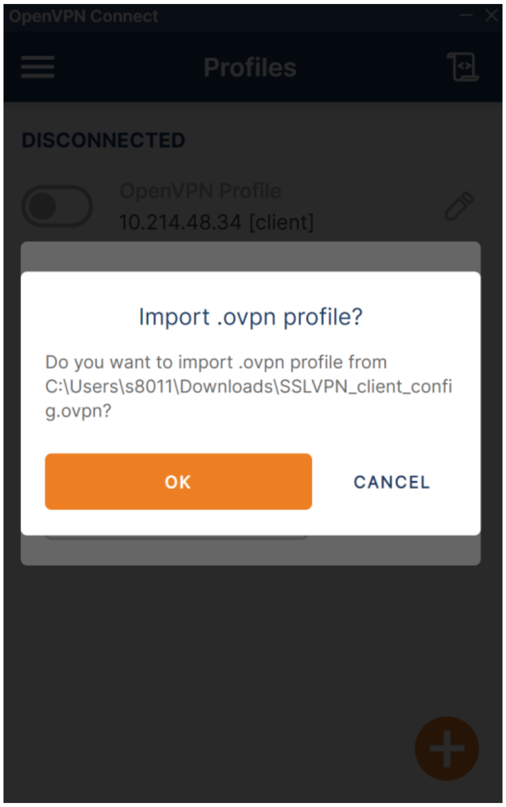
Clients will use VPN to access

○ Internet and Local Networks (Full Tunnel)

Auto SNAT

● Local Networks Only (Split Tunnel)

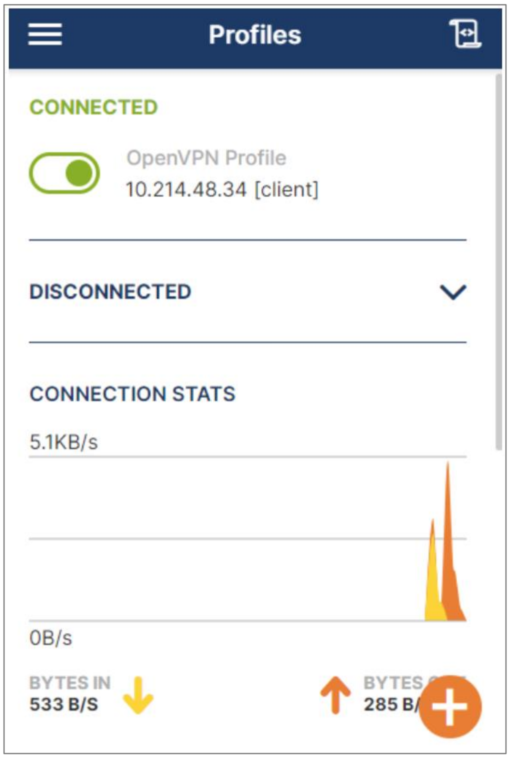
Import the config file.



Import .ovpn profile?

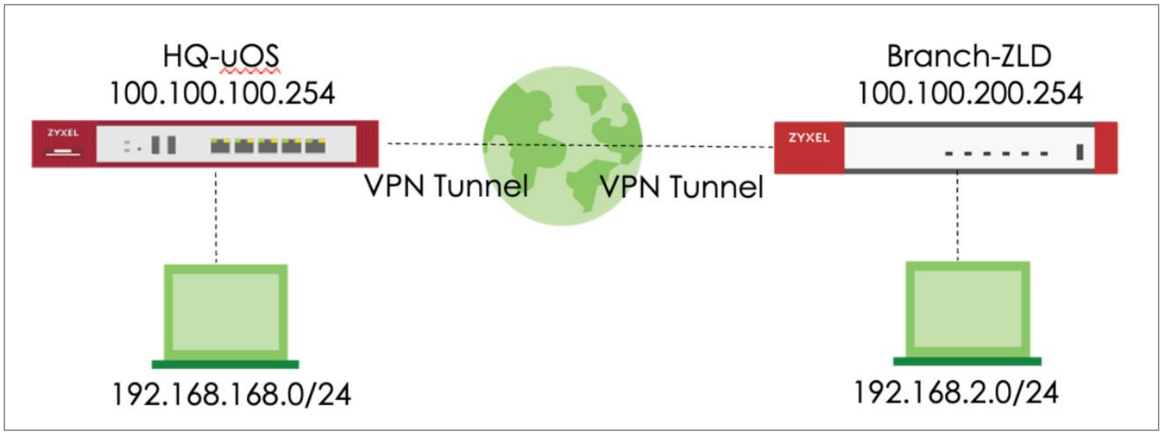
Do you want to import .ovpn profile from C:\Users\s8011\Downloads\SSLVPN_client_config.ovpn?

VPN is connected.



How to Configure Site-to-site IPSec VPN between ZLD and uOS device

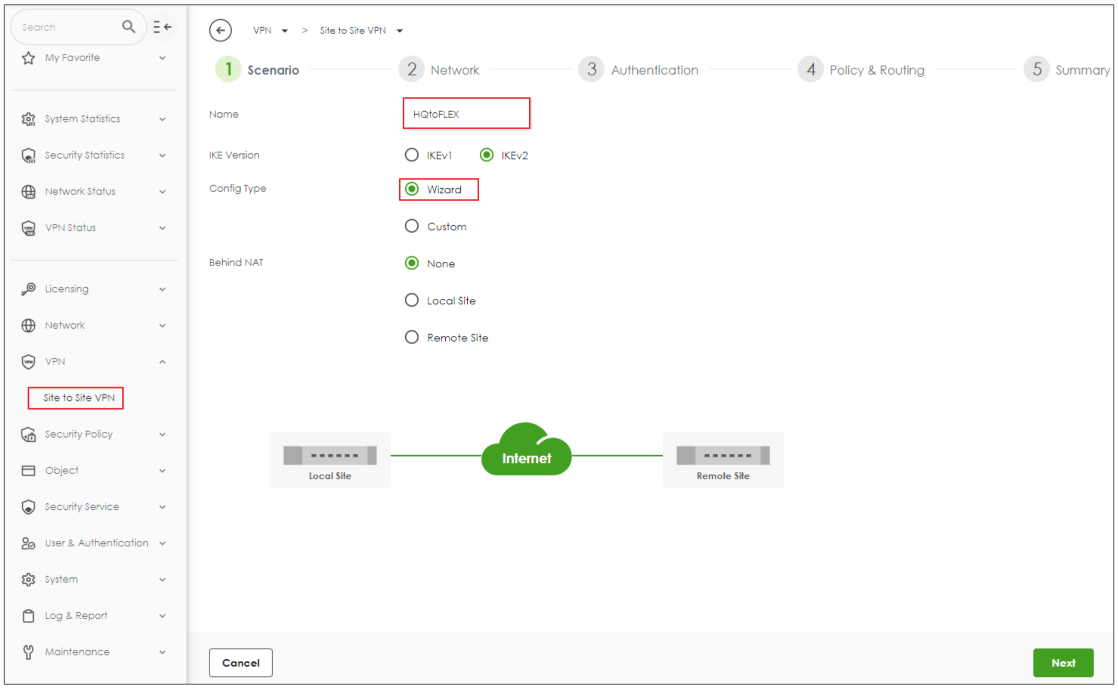
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer gateway is ZLD device. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPSec VPN Tunnel for uOS

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



1 Scenario — 2 Network — 3 Authentication — 4 Policy & Routing — 5 Summary

Name: HQtoFLEX

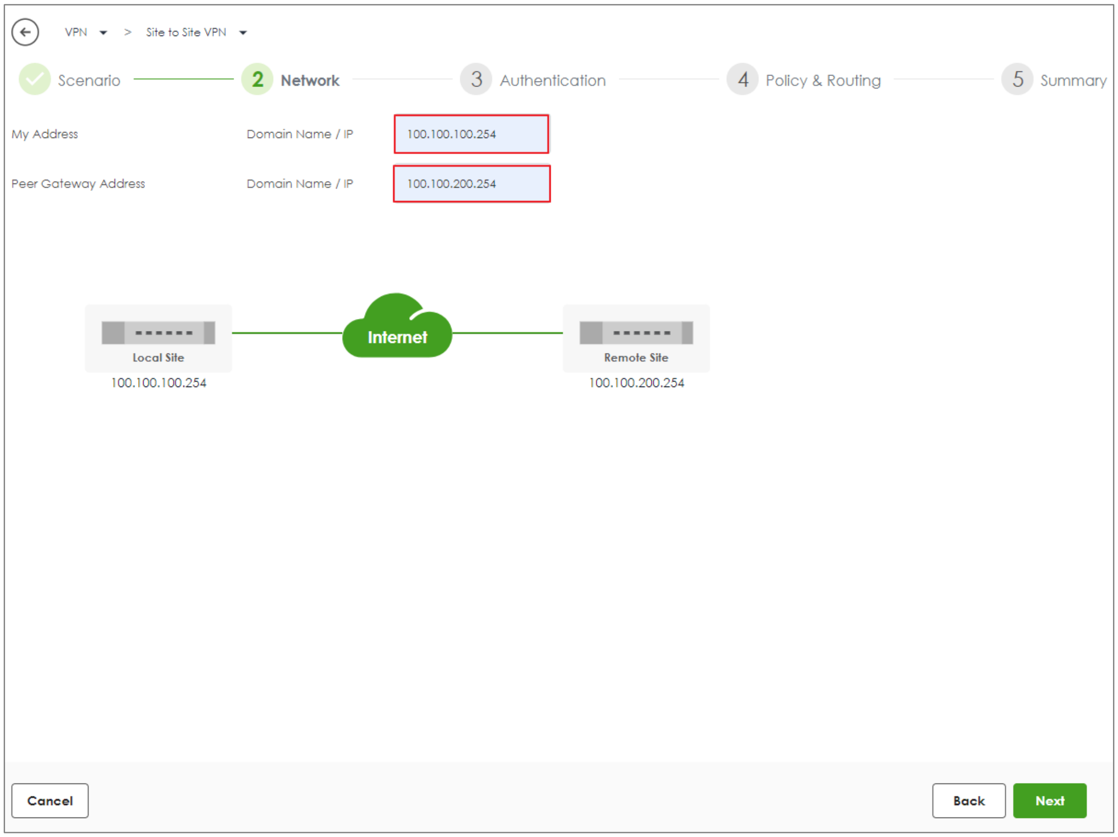
IKE Version: ○ IKEv1 ● IKEv2

Config Type: ● Wizard ○ Custom

Behind NAT: ● None ○ Local Site ○ Remote Site

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next.**

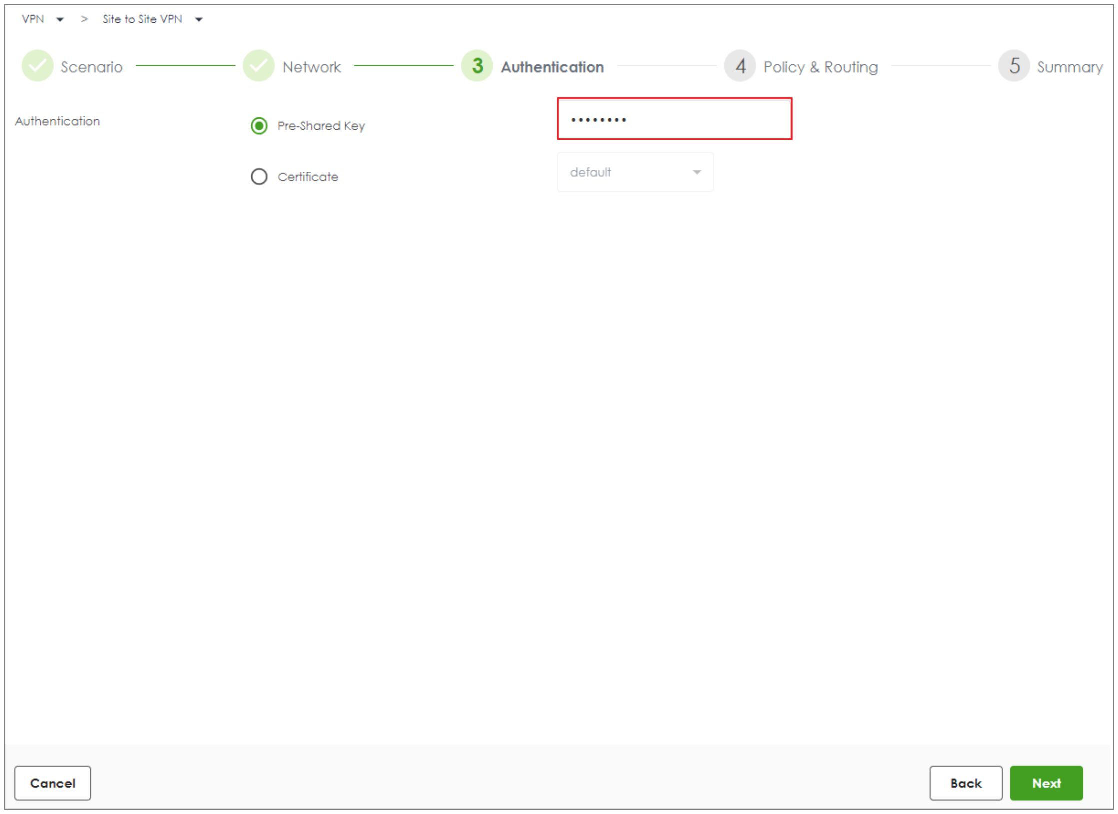


My Address Domain Name / IP 100.100.100.254

Peer Gateway Address Domain Name / IP 100.100.200.254

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**



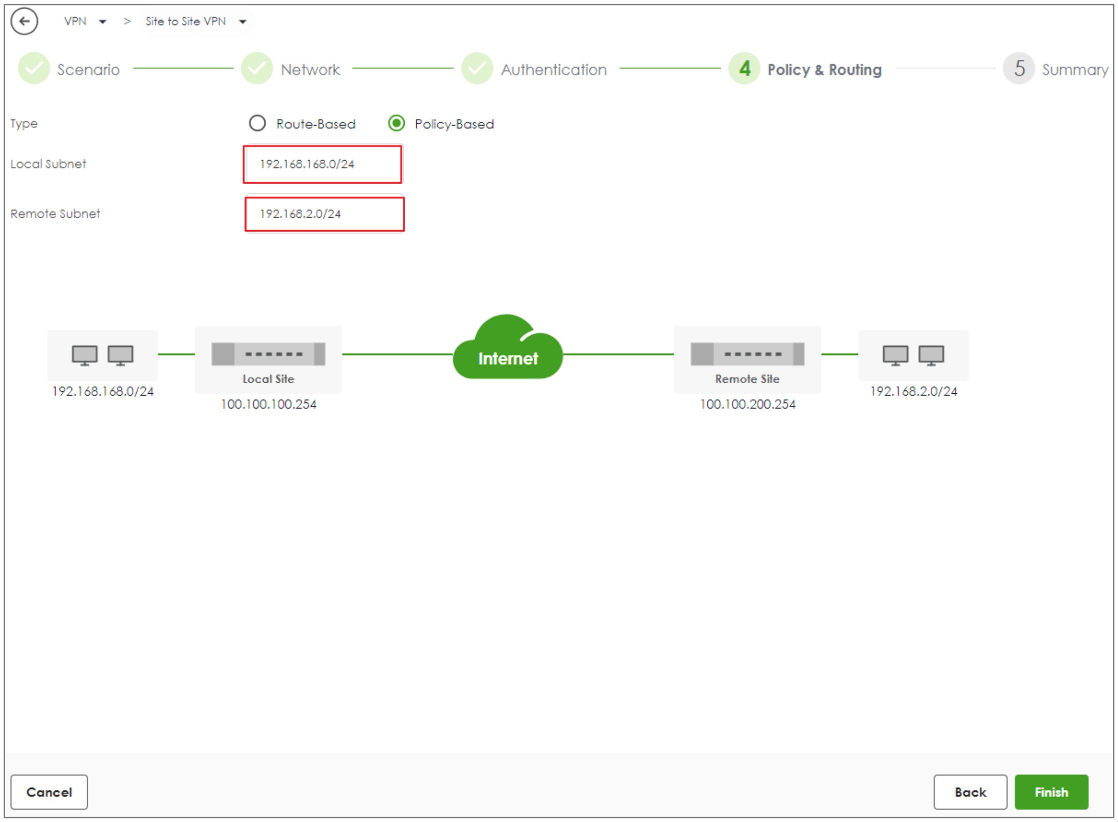
Authentication

● Pre-Shared Key ••••••••

○ Certificate default

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Local Subnet to be the IP address of the network connected to USG FLEX H and Remote Subnet to be the IP address of the network connected to the peer ZyWALL.



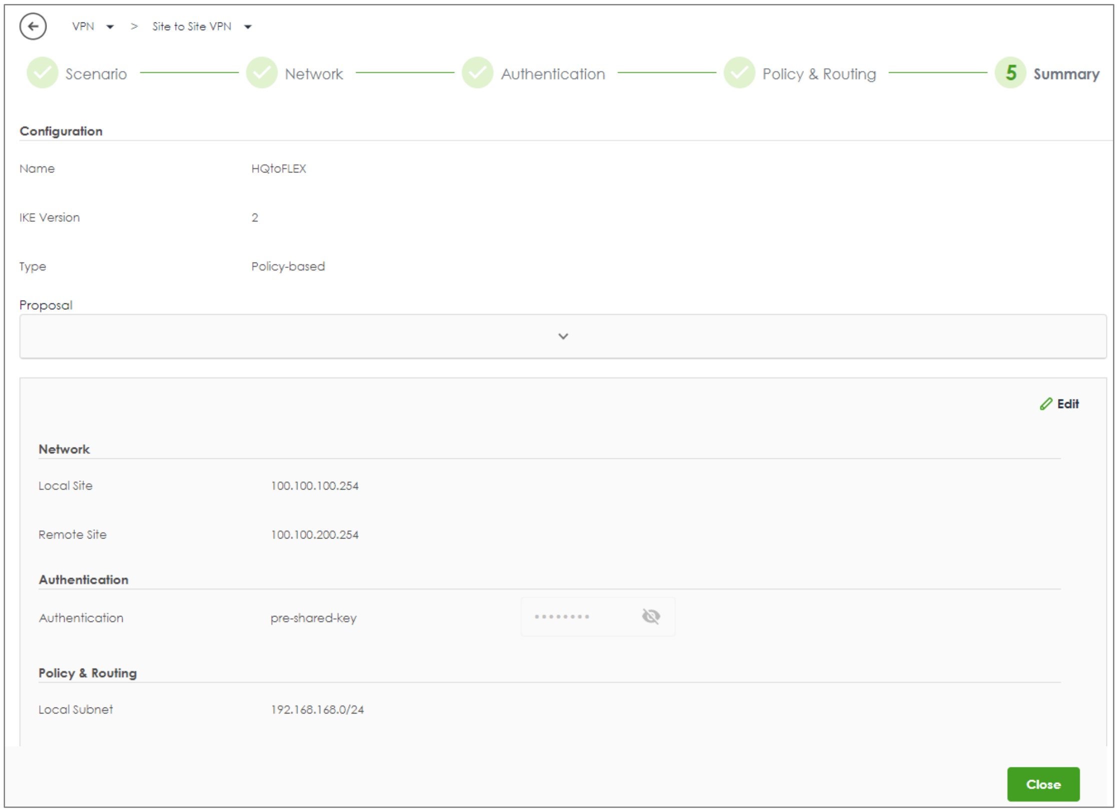
Type ○ Route-Based ● Policy-Based

Local Subnet 192.168.168.0/24

Remote Subnet 192.168.2.0/24

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



Configuration

Name HQtoFLEX

IKE Version 2

Type Policy-based

Proposal

Network

Local Site 100.100.100.254

Remote Site 100.100.200.254

Authentication

Authentication pre-shared-key ••••••••

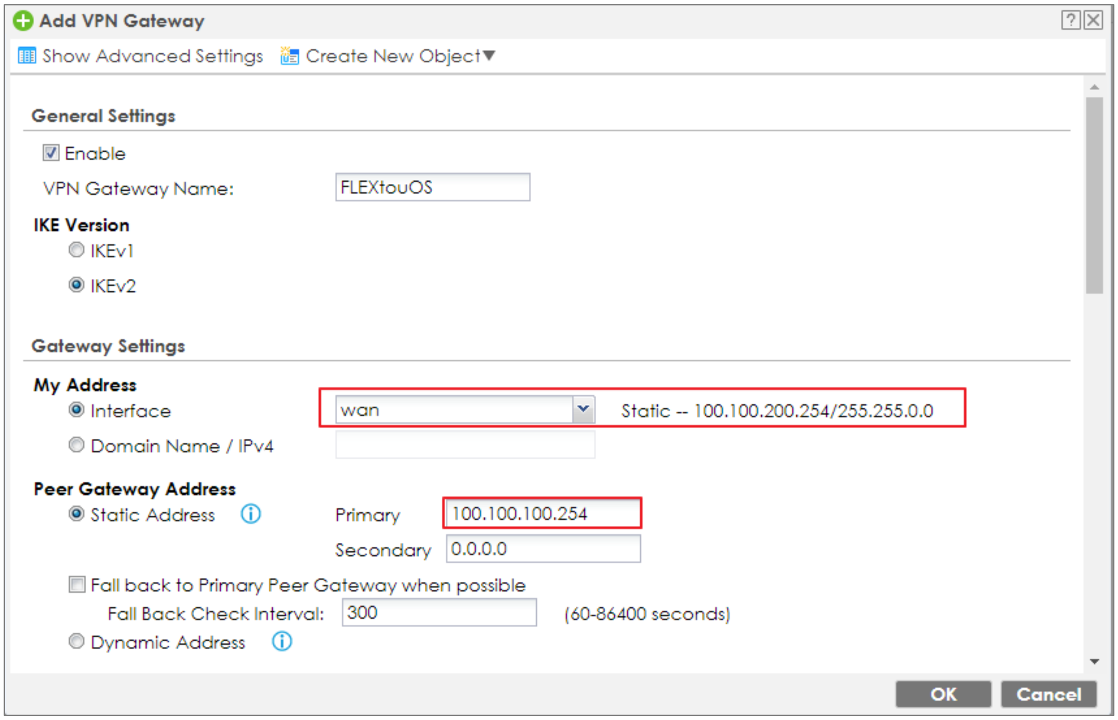
Policy & Routing

Local Subnet 192.168.168.0/24

Set up IPSec VPN Tunnel for ZLD

VPN > IPSec VPN > VPN Gateway

Select the WAN interface and type the Peer Gateway Address.



General Settings

☑ Enable

VPN Gateway Name: FLEXtouOS

IKE Version

○ IKEv1

● IKEv2

Gateway Settings

My Address

● Interface wan Static -- 100.100.200.254/255.255.0.0

○ Domain Name / IPv4

Peer Gateway Address

● Static Address Primary 100.100.100.254

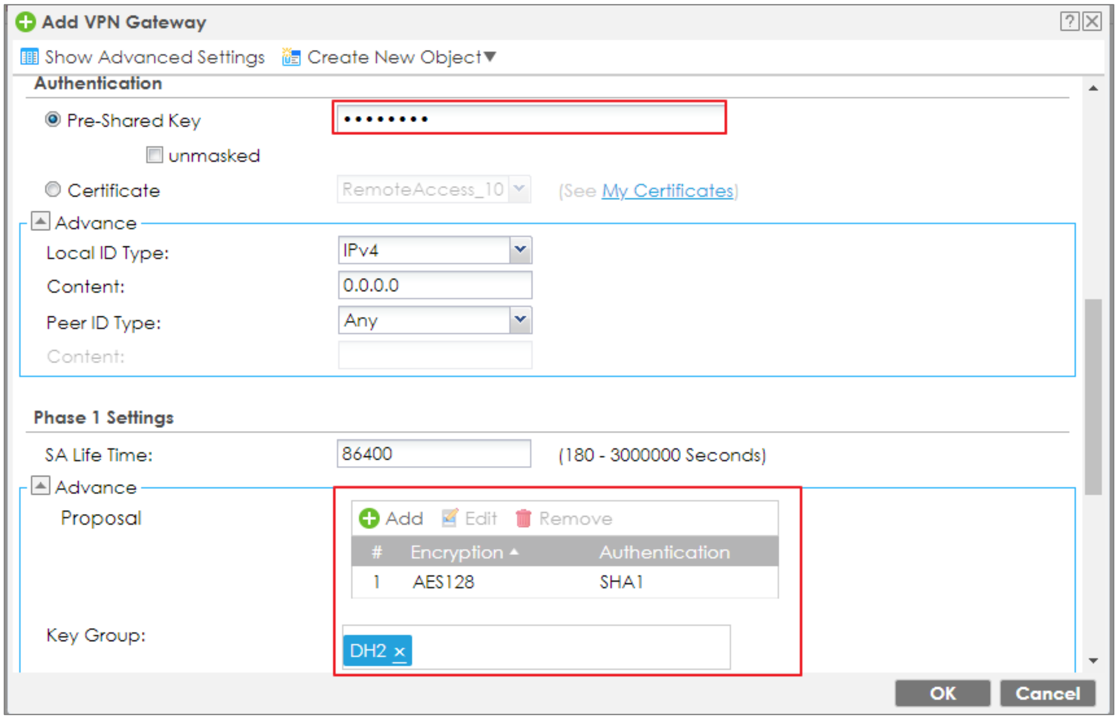
Secondary 0.0.0.0

□ Fall back to Primary Peer Gateway when possible

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

○ Dynamic Address

Type Pre-shared Key. The default proposal which created by wizard is "Encryption:AES128, Authentication:SHA1, Key Group:DH2". Those are the same as uOS.



Add VPN Gateway

Show Advanced Settings | Create New Object▼

Authentication

● Pre-Shared Key: •••••••••

□ unmasked

○ Certificate: RemoteAccess_10 (See My Certificates)

Advance

Local ID Type: IPv4

Content: 0.0.0.0

Peer ID Type: Any

Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Advance

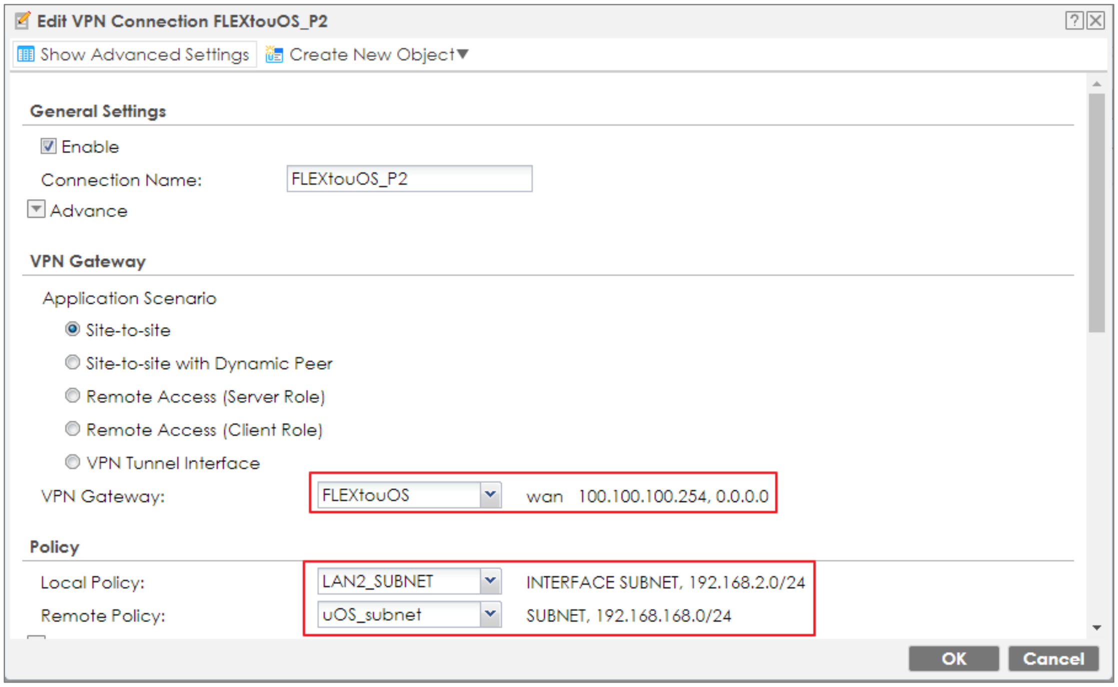
Proposal

#	Encryption ▲	Authentication
1	AES128	SHA1

Key Group: DH2

VPN > IPSec VPN > VPN Connection

Select VPN Gateway and set Local Subnet to be the IP address of the network connected to be ZyWALL and Remote Subnet to be the IP address of the network connected to the peer USG FLEX H.



Edit VPN Connection FLEXtouOS_P2

General Settings

☑ Enable

Connection Name: FLEXtouOS_P2

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

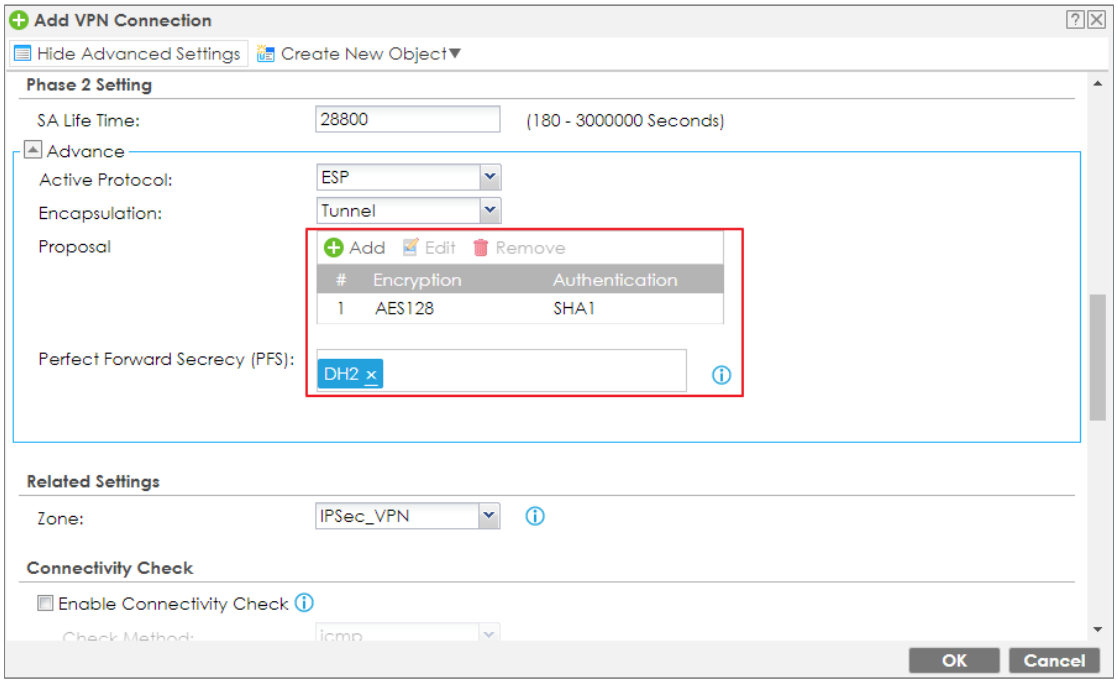
VPN Gateway: FLEXtouOS wan 100.100.100.254, 0.0.0.0

Policy

Local Policy: LAN2_SUBNET INTERFACE SUBNET, 192.168.2.0/24

Remote Policy: uOS_subnet SUBNET, 192.168.168.0/24

The default proposal which created by wizard is “Encryption: AES128, Authentication: SHA1, Key Group: DH2”. Those are the same as uOS.



Add VPN Connection

Hide Advanced Settings | Create New Object▼

Phase 2 Setting

SA Life Time: 28800 (180 - 3000000 Seconds)

Advance

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

Add | Edit | Remove

#	Encryption	Authentication
1	AES128	SHA1

Perfect Forward Secrecy (PFS): DH2 ×

Related Settings

Zone: IPSec_VPN

Connectivity Check

□ Enable Connectivity Check

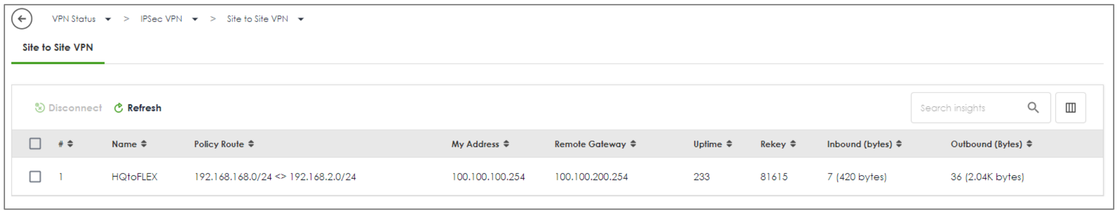
Check Method: icmp

OK | Cancel

Test IPSec VPN Tunnel

VPN Status > IPSec VPN

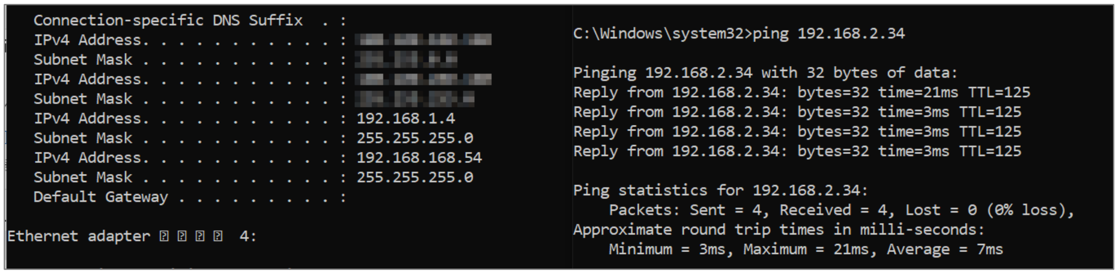
Verify the IPSec VPN status on uOS device.



□	#	Name	Policy Route	My Address	Remote Gateway	Uptime	Rekey	Inbound (bytes)	Outbound (Bytes)
□	1	HQtoFLEX	192.168.168.0/24 <> 192.168.2.0/24	100.100.100.254	100.100.200.254	233	81615	7 (420 bytes)	36 (2.04K bytes)

Ping the PC that is connected to ZLD device

Win 11 > cmd > ping 192.168.2.34

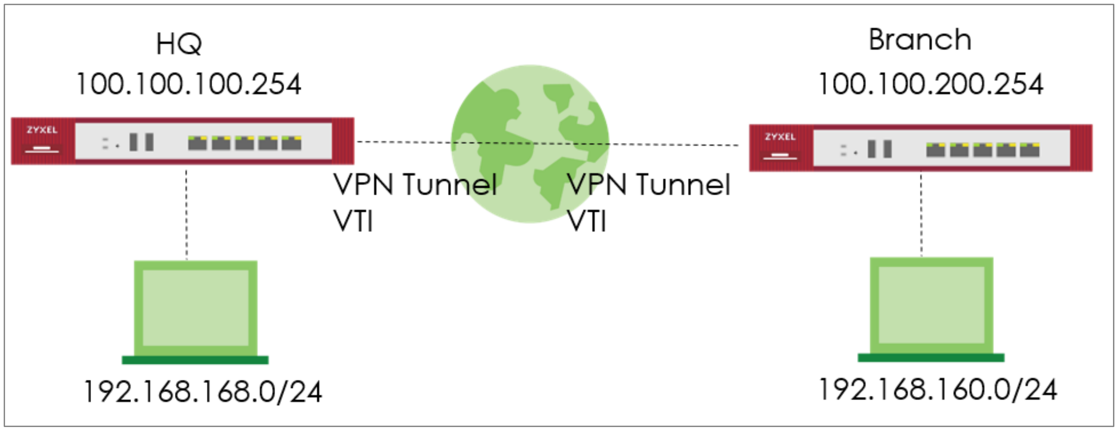


```
   Connection-specific DNS Suffix  . :
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : [redacted]
   Subnet Mask . . . . . . . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : 192.168.1.4
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 192.168.168.54
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter ⍰ ⍰ ⍰ ⍰  4:
```

```
C:\Windows\system32>ping 192.168.2.34

Pinging 192.168.2.34 with 32 bytes of data:
Reply from 192.168.2.34: bytes=32 time=21ms TTL=125
Reply from 192.168.2.34: bytes=32 time=3ms TTL=125
Reply from 192.168.2.34: bytes=32 time=3ms TTL=125
Reply from 192.168.2.34: bytes=32 time=3ms TTL=125

Ping statistics for 192.168.2.34:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 21ms, Average = 7ms
```

How to Configure Route-Based VPN

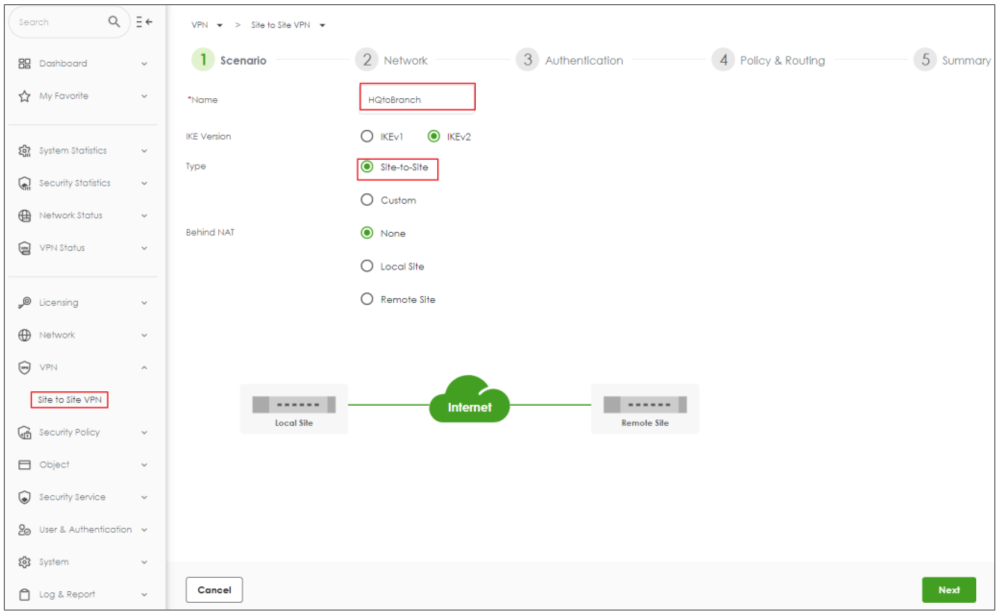
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Static IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPSec VPN Tunnel for HQ

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



*Name: HQtoBranch

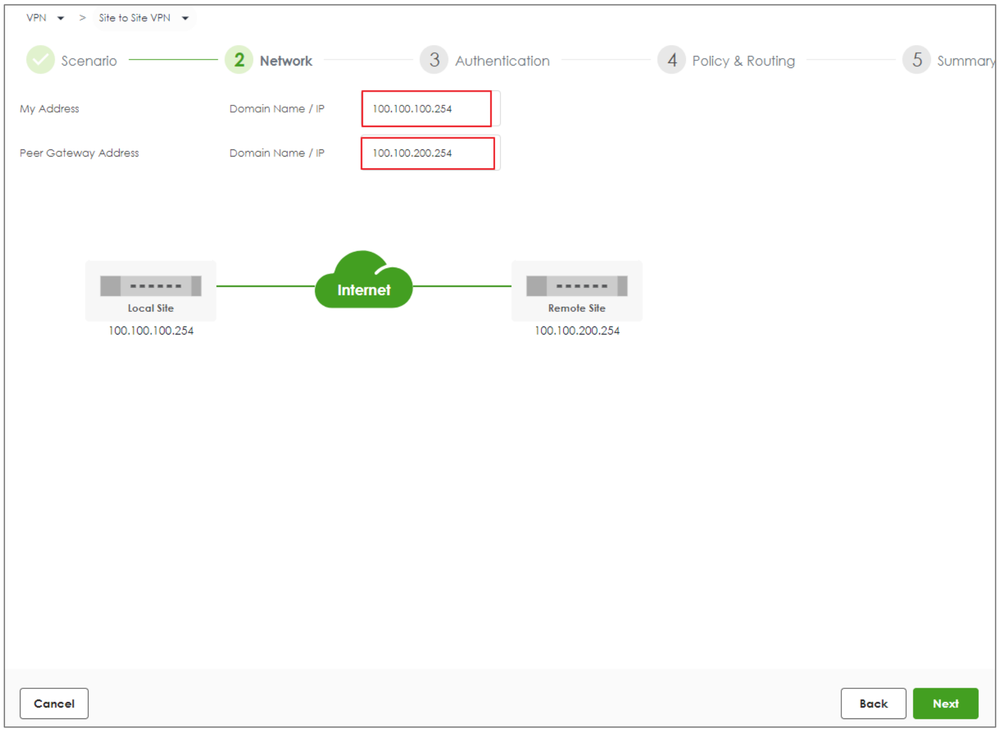
IKE Version: ○ IKEv1 ● IKEv2

Type: ● Site-to-Site ○ Custom

Behind NAT: ● None ○ Local Site ○ Remote Site

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next.**



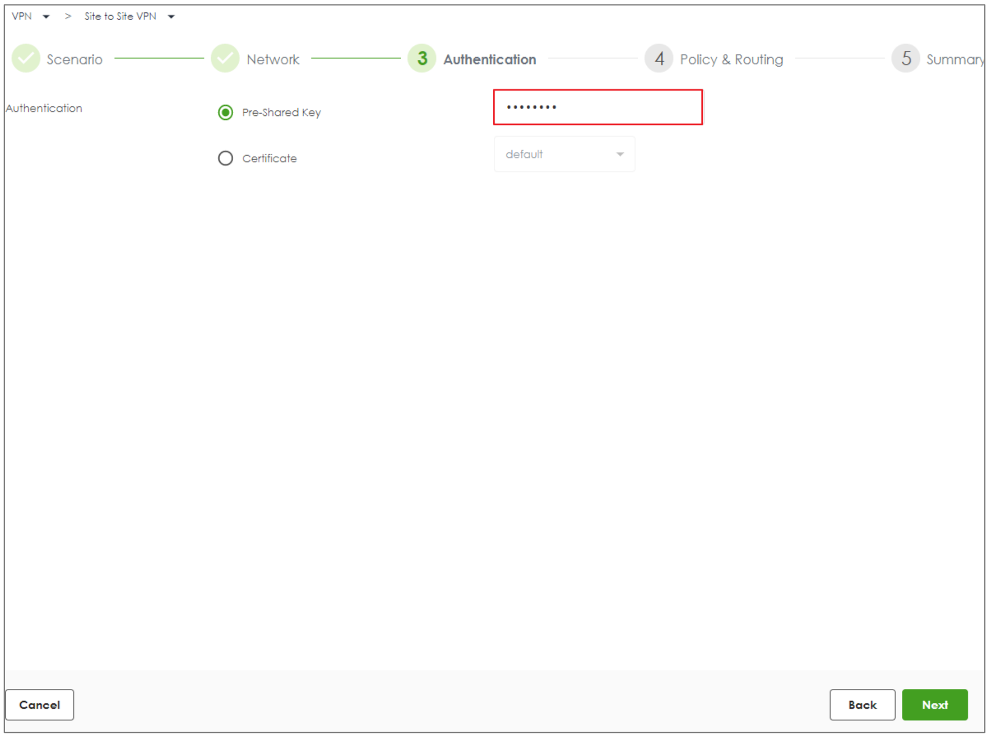
VPN > Site to Site VPN

My Address Domain Name / IP 100.100.100.254

Peer Gateway Address Domain Name / IP 100.100.200.254

VPN > Site to Site VPN > Scenario > Network > Authentication

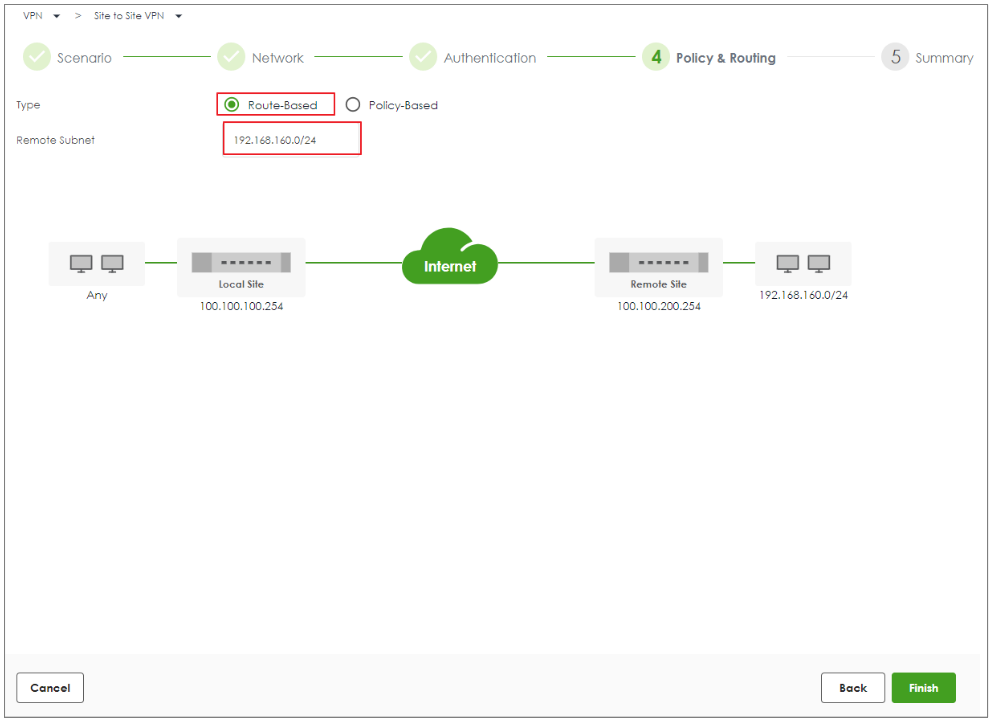
Type a secure Pre-Shared Key. Click **Next**



Authentication
● Pre-Shared Key ••••••••
○ Certificate default

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Type to Route-Based and configure the Remote Subnet.

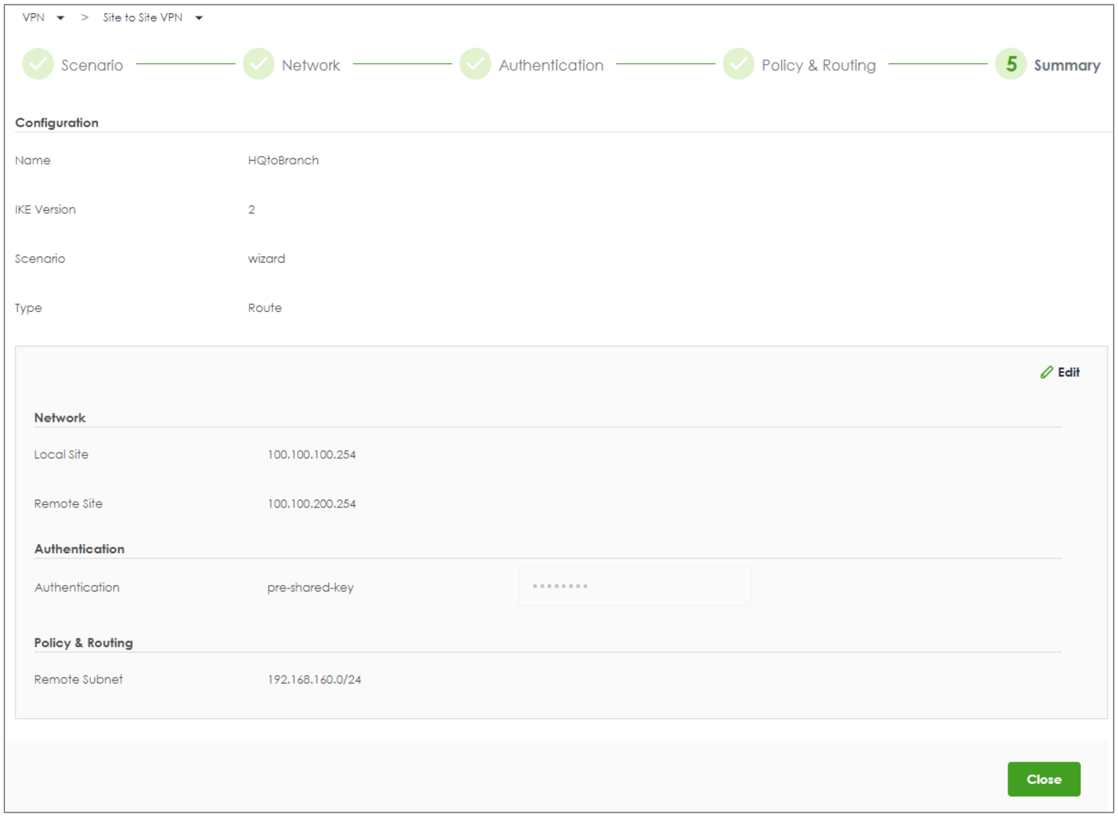


Type ● Route-Based ○ Policy-Based

Remote Subnet 192.168.160.0/24

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



Configuration

Name	HQtoBranch
IKE Version	2
Scenario	wizard
Type	Route

Network

Local Site	100.100.100.254
Remote Site	100.100.200.254

Authentication

Authentication	pre-shared-key	••••••••

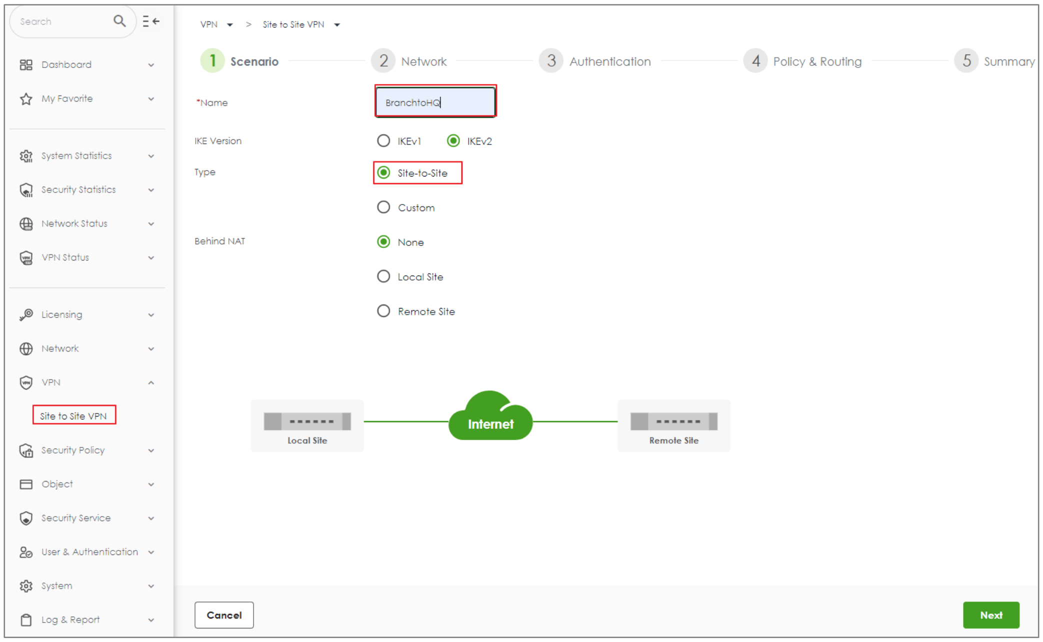
Policy & Routing

Remote Subnet	192.168.160.0/24

Set up IPSec VPN Tunnel for Branch

VPN > Site to Site VPN > Scenario

Type the VPN name used to identify this VPN connection. Select the type to the Site-to-Site. Click **Next**.



1 Scenario — 2 Network — 3 Authentication — 4 Policy & Routing — 5 Summary

*Name: BranchtoHQ

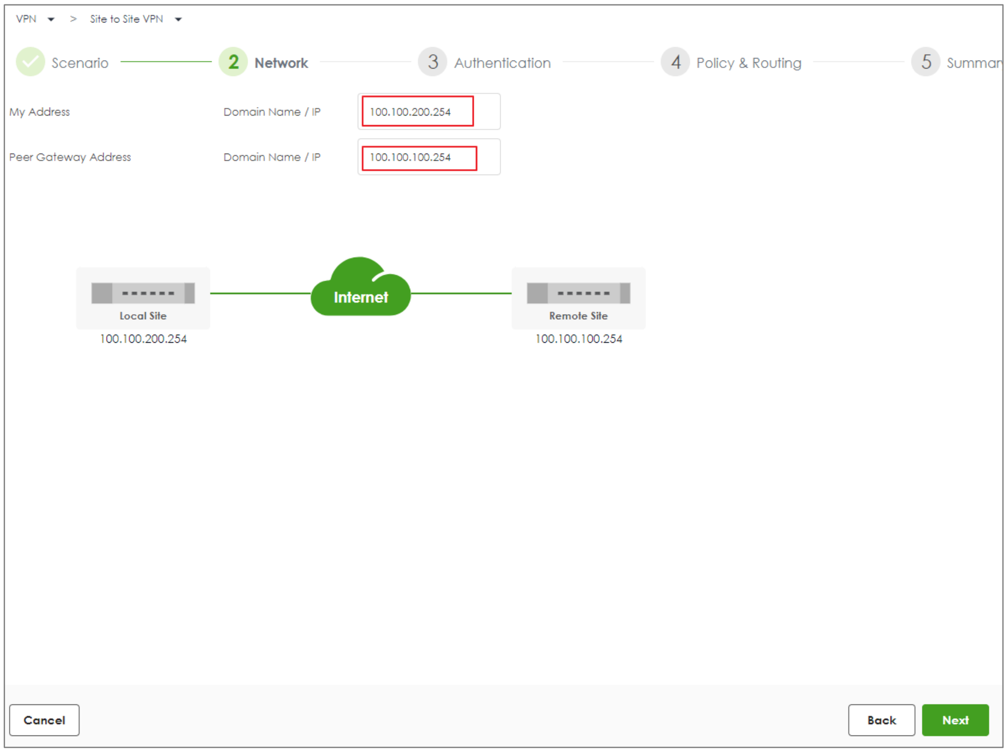
IKE Version: ○ IKEv1 ● IKEv2

Type: ● Site-to-Site ○ Custom

Behind NAT: ● None ○ Local Site ○ Remote Site

VPN > Site to Site VPN > Scenario > Network

Configure My Address and Peer Gateway Address. Click **Next.**



VPN > Site to Site VPN

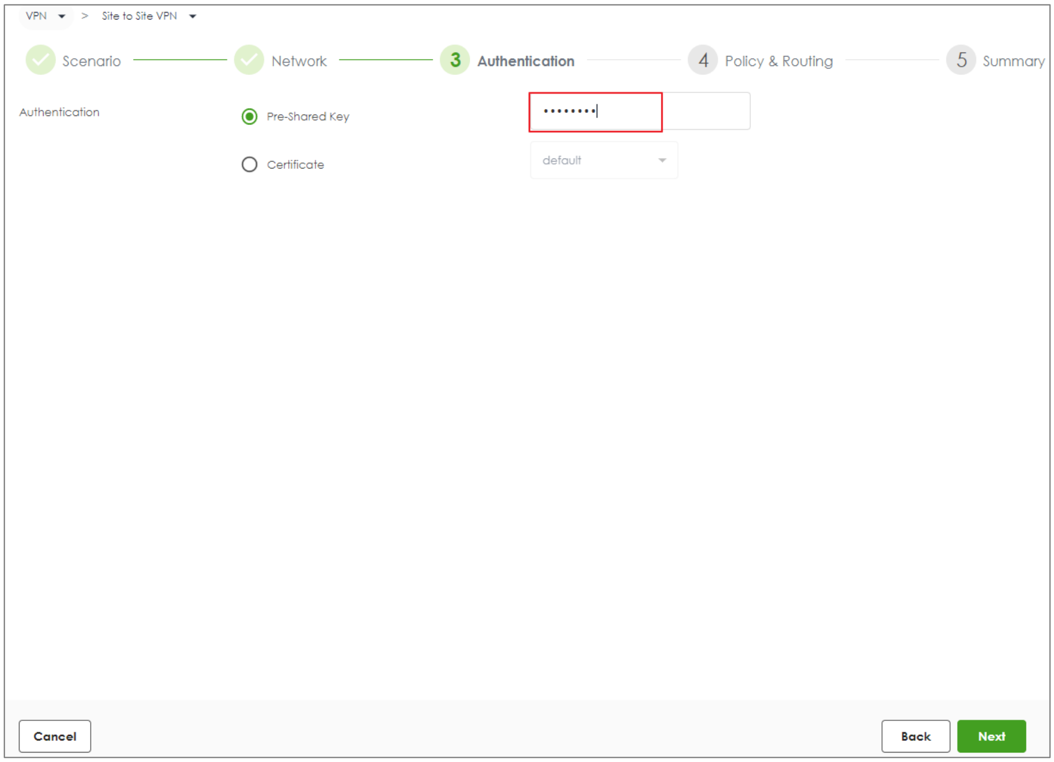
✓ Scenario — 2 Network — 3 Authentication — 4 Policy & Routing — 5 Summar

My Address: Domain Name / IP: 100.100.200.254

Peer Gateway Address: Domain Name / IP: 100.100.100.254

VPN > Site to Site VPN > Scenario > Network > Authentication

Type a secure Pre-Shared Key. Click **Next**



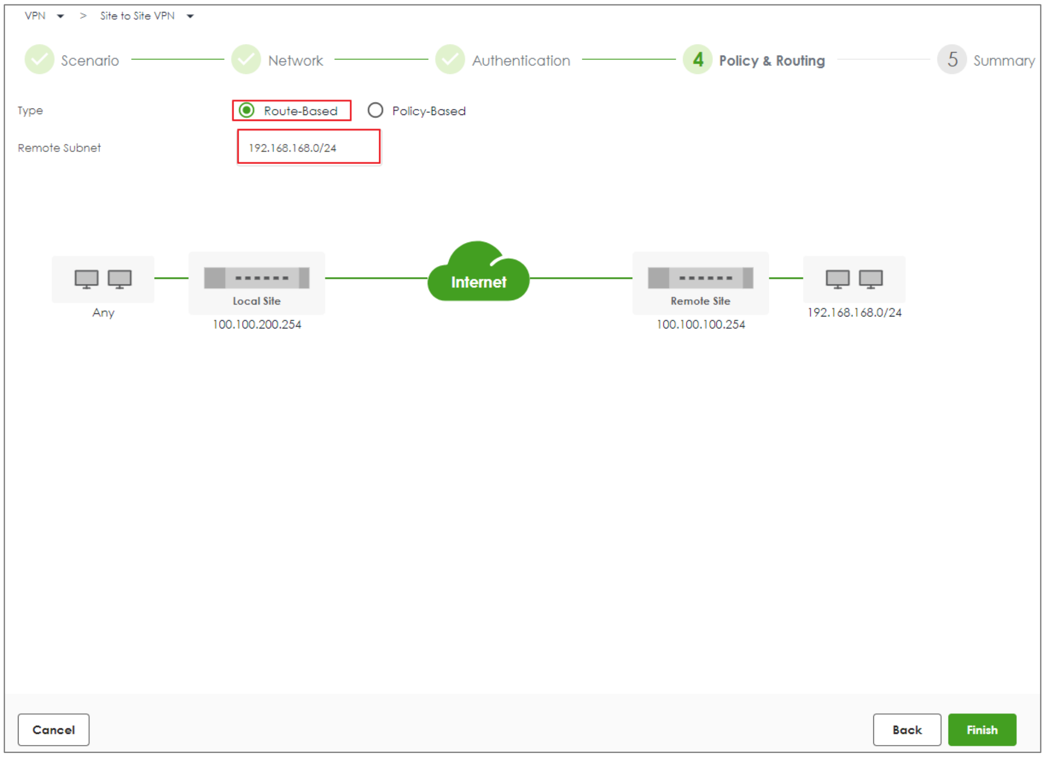
Authentication

● Pre-Shared Key ••••••••

○ Certificate default

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing

Set Type to Route-Based and Remote Subnet.



VPN > Site to Site VPN

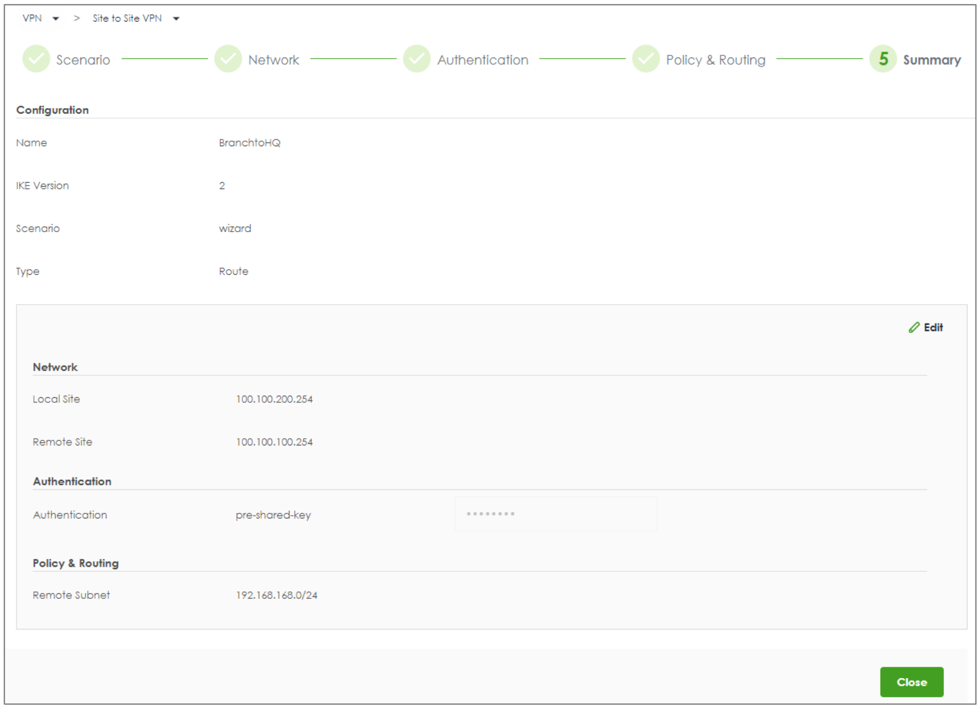
✓ Scenario — ✓ Network — ✓ Authentication — 4 Policy & Routing — 5 Summary

Type: ● Route-Based ○ Policy-Based

Remote Subnet: 192.168.168.0/24

VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing > Summary

The screen provides a summary of the VPN tunnel. You can Edit it if you want to modify.



Configuration

Name BranchtoHQ

IKE Version 2

Scenario wizard

Type Route

Network

Local Site 100.100.200.254

Remote Site 100.100.100.254

Authentication

Authentication pre-shared-key ••••••••

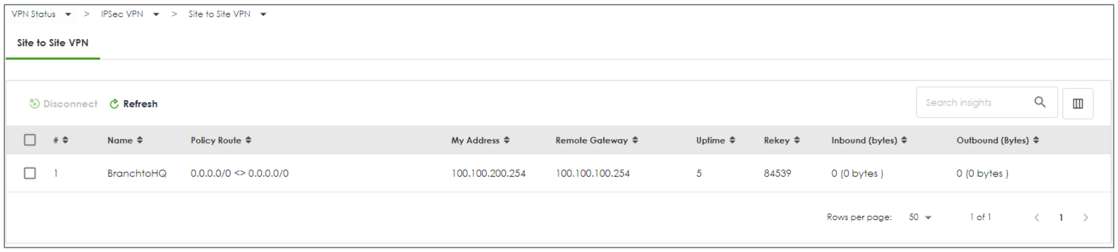
Policy & Routing

Remote Subnet 192.168.168.0/24

Test IPSec VPN Tunnel

VPN Status > IPSec VPN

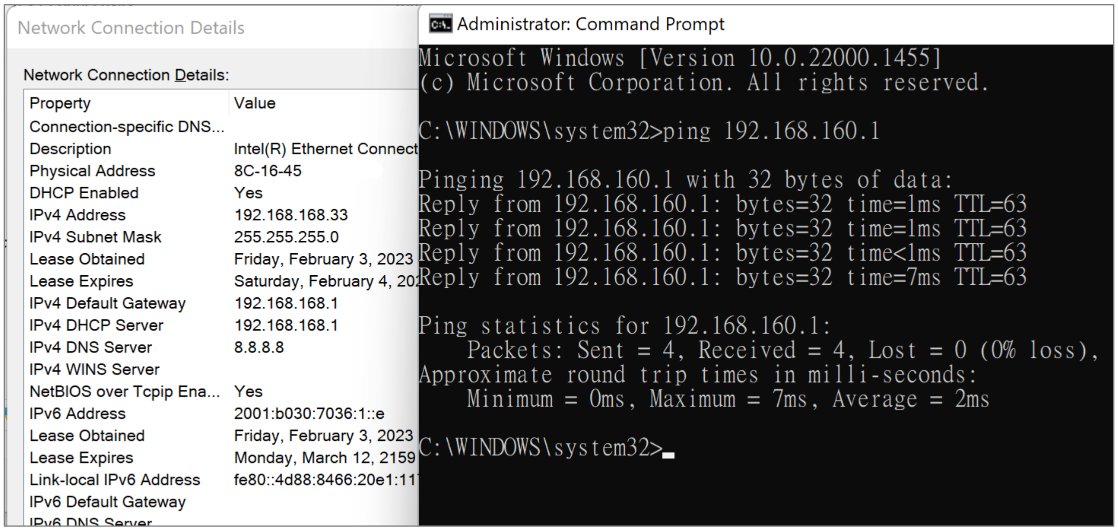
Verify the IPSec VPN status.



□	#	Name	Policy Route	My Address	Remote Gateway	Uptime	Rekey	Inbound (bytes)	Outbound (Bytes)
□	1	BranchtoHQ	0.0.0.0/0 <> 0.0.0.0/0	100.100.200.254	100.100.100.254	5	84539	0 (0 bytes)	0 (0 bytes)

Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



Network Connection Details

Network Connection Details:

Property	Value
Connection-specific DNS...	
Description	Intel(R) Ethernet Connect
Physical Address	8C-16-45
DHCP Enabled	Yes
IPv4 Address	192.168.168.33
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Friday, February 3, 2023
Lease Expires	Saturday, February 4, 202
IPv4 Default Gateway	192.168.168.1
IPv4 DHCP Server	192.168.168.1
IPv4 DNS Server	8.8.8.8
IPv4 WINS Server	
NetBIOS over Tcpip Ena...	Yes
IPv6 Address	2001:b030:7036:1::e
Lease Obtained	Friday, February 3, 2023
Lease Expires	Monday, March 12, 2159
Link-local IPv6 Address	fe80::4d88:8466:20e1:11
IPv6 Default Gateway	
IPv6 DNS Server	

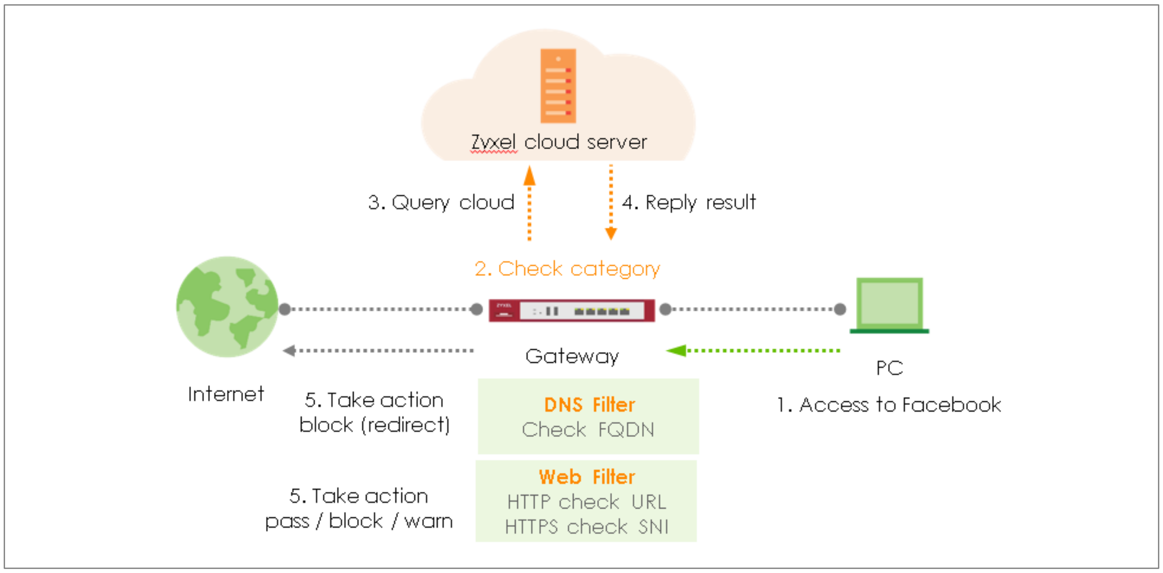
Administrator: Command Prompt

```
Microsoft Windows [Version 10.0.22000.1455]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>ping 192.168.160.1

Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time<1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=7ms TTL=63

Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\WINDOWS\system32>_
```

Chapter 2- Security Service

How to Block HTTPS Websites Using Content Filtering and SSL Inspection

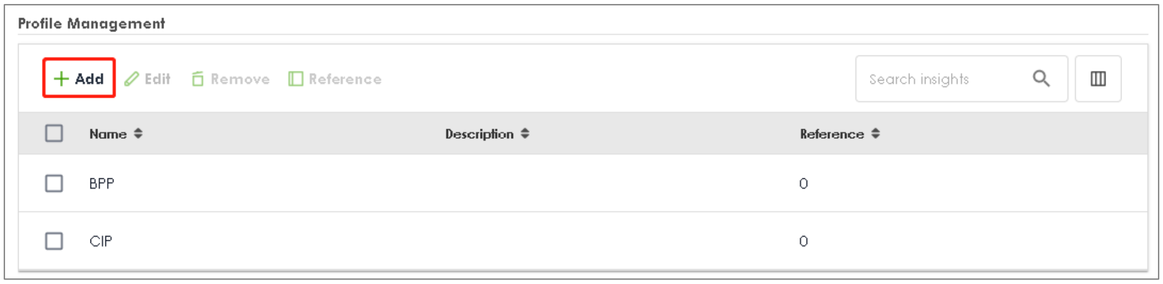
This is an example of using a FLEX Content Filtering, SSL Inspection and Security Policy to block access to malicious or not business-related websites.



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 USG FLEX 200H (Firmware Version: uOS 1.10).

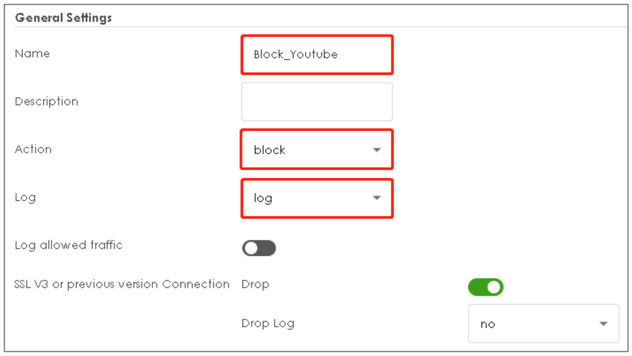
Set Up Content Filter

Go to Security Service > Content Filtering. Click Add to create a content filtering profile in Profile Management.



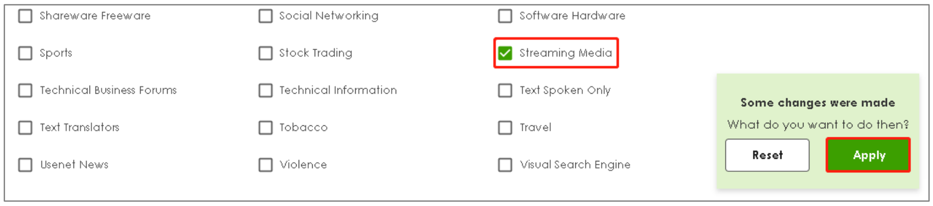
☐	Name	Description	Reference
☐	BPP		0
☐	CIP		0

Type profile name and enable log for block action in General Settings.


General Settings

Name	Block_Youtube	
Description		
Action	block	
Log	log	
Log allowed traffic	○	
SSL V3 or previous version Connection	Drop	●
	Drop Log	no

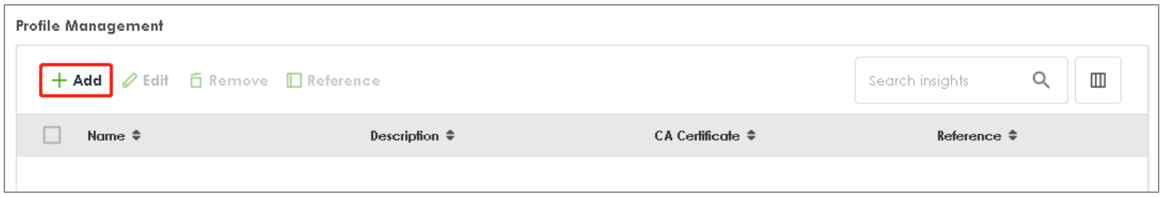
Tick Streaming Media category in Managed Categories, and click Apply.


☐ Shareware Freeware
☐ Sports
☐ Technical Business Forums
☐ Text Translators
☐ Usenet News
☐ Social Networking
☐ Stock Trading
☐ Technical Information
☐ Tobacco
☐ Violence
☐ Software Hardware
☑ Streaming Media
☐ Text Spoken Only
☐ Travel
☐ Visual Search Engine

Some changes were made
What do you want to do then?

Set Up SSL Inspection

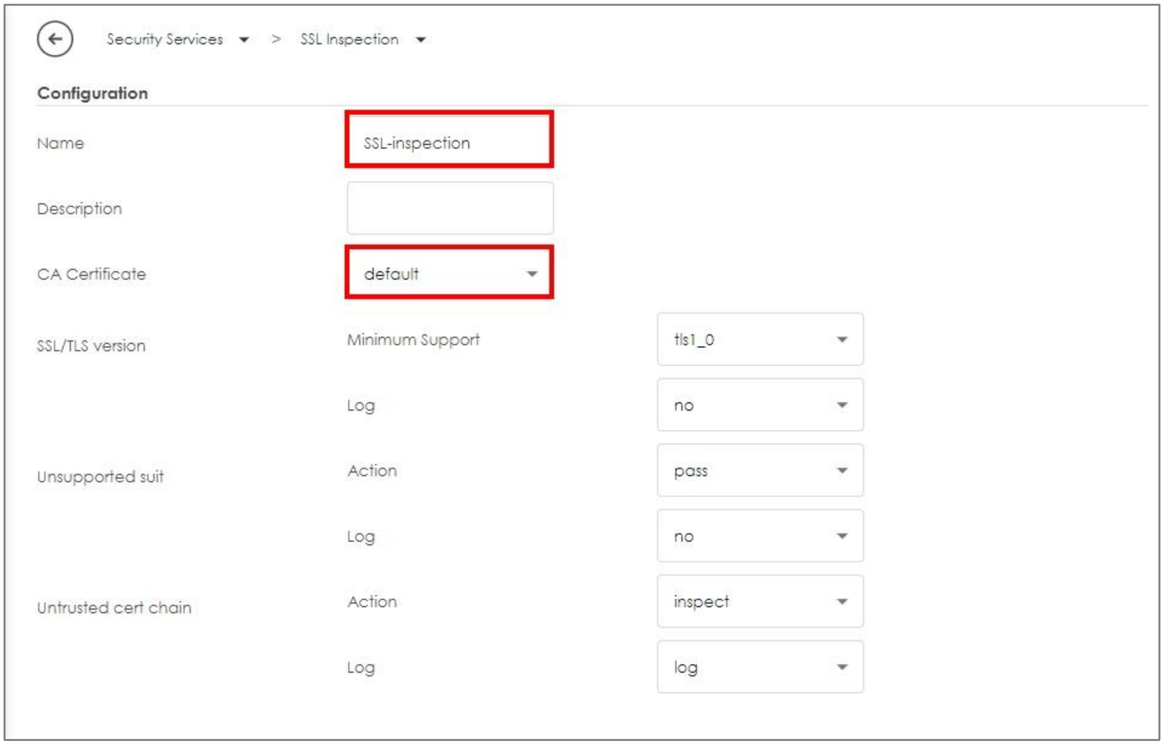
In the FLEX, go to Security Service > SSL inspection > profile > Profile Management, and click Add to create profile



Profile Management

□	Name	Description	CA Certificate	Reference

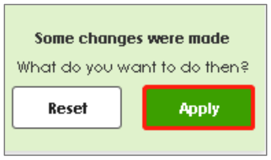
Type profile Name, and select the CA Certificate to be the certificate used in this profile. Leave other actions as default settings.



Configuration

Name	SSL-inspection	
Description		
CA Certificate	default	
SSL/TLS version	Minimum Support	tls1_0
	Log	no
Unsupported suit	Action	pass
	Log	no
Untrusted cert chain	Action	inspect
	Log	log

Click Apply to add SSL Inspection profile.



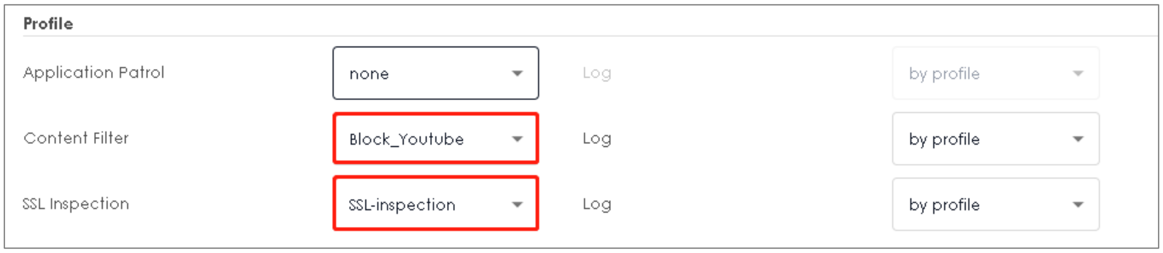
Some changes were made

What do you want to do then?

Set Up the Security Policy

Go to Security Policy > Policy control. Edit LAN_Outgoing, and scroll down to profile section.

Select Content Filtering, and SSL Inspection. Click Apply to save.



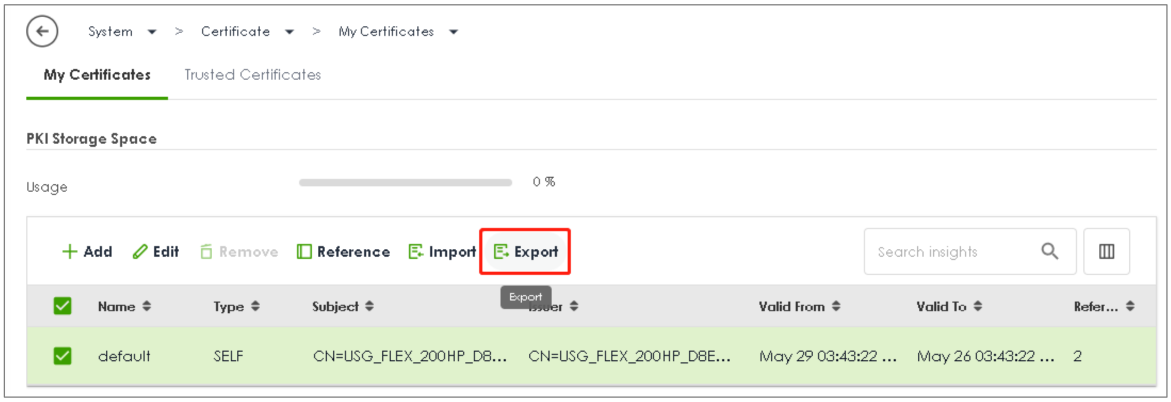
Profile

Application Patrol	none	Log	by profile
Content Filter	Block_Youtube	Log	by profile
SSL Inspection	SSL-inspection	Log	by profile

Export Certificate from FLEX and Import it to Windows

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

Go to System > Certificate > My Certificates to export default certificate from FLEX.

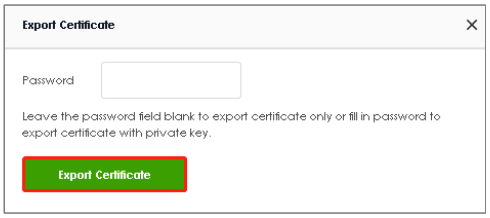


PKI Storage Space

Usage 0 %

☑	Name	Type	Subject	Issuer	Valid From	Valid To	Refer...
☑	default	SELF	CN=USG_FLEX_200HP_D8...	CN=USG_FLEX_200HP_D8E...	May 29 03:43:22 ...	May 26 03:43:22 ...	2

Click Export Certificate to export certificate file, and Save default certificate as default.crt file to Windows OS.

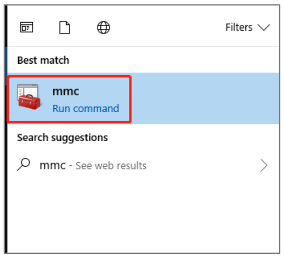


Export Certificate

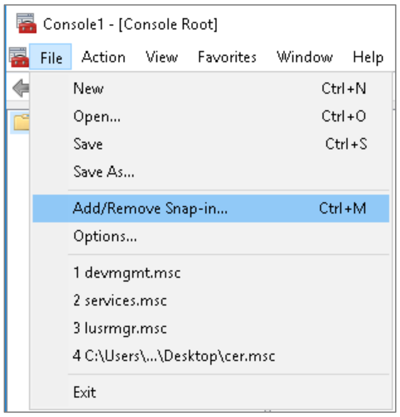
Password

Leave the password field blank to export certificate only or fill in password to export certificate with private key.

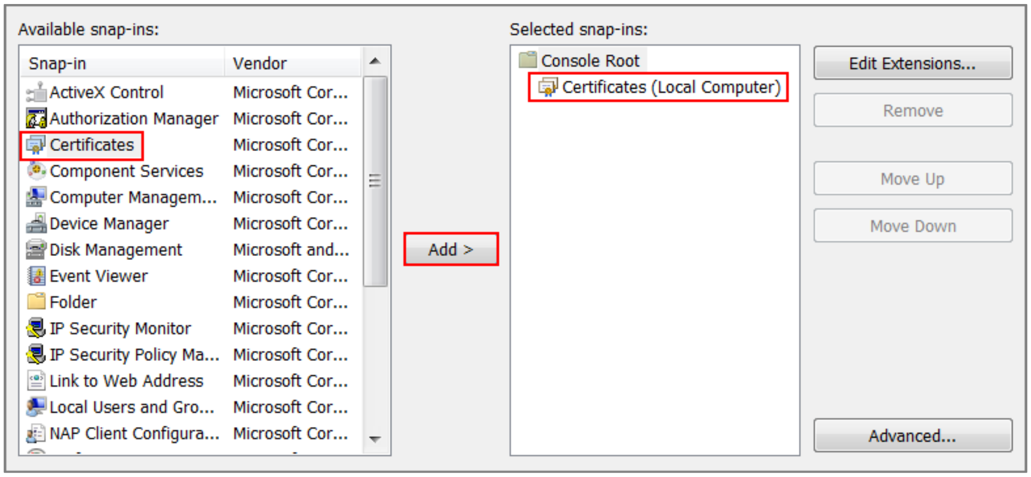
In Windows Start Menu > Search Box, type MMC and press Enter.



In the mmc console window, click 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:

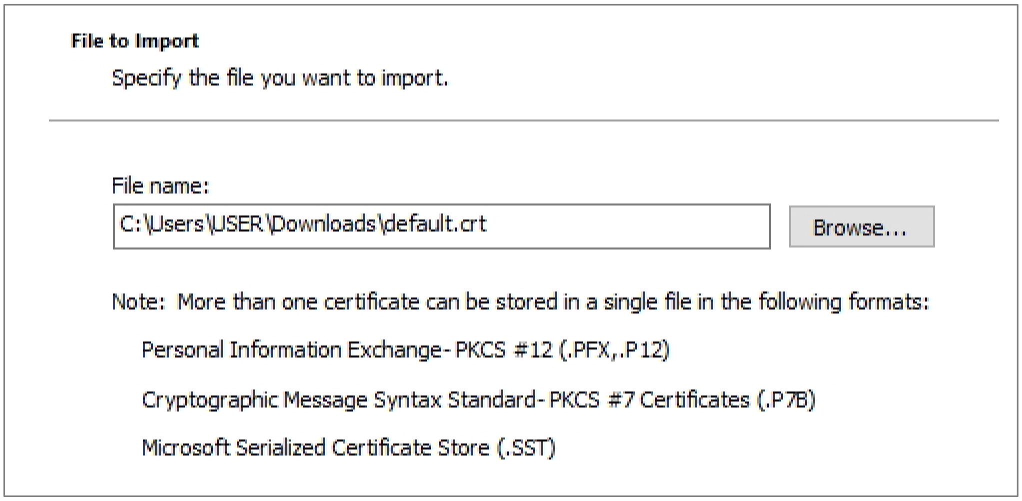
Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
NAP Client Configura...	Microsoft Cor...

Selected snap-ins:

Console Root
Certificates (Local Computer)

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

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



File to Import

Specify the file you want to import.

File name:

C:\Users\USER\Downloads\default.crt

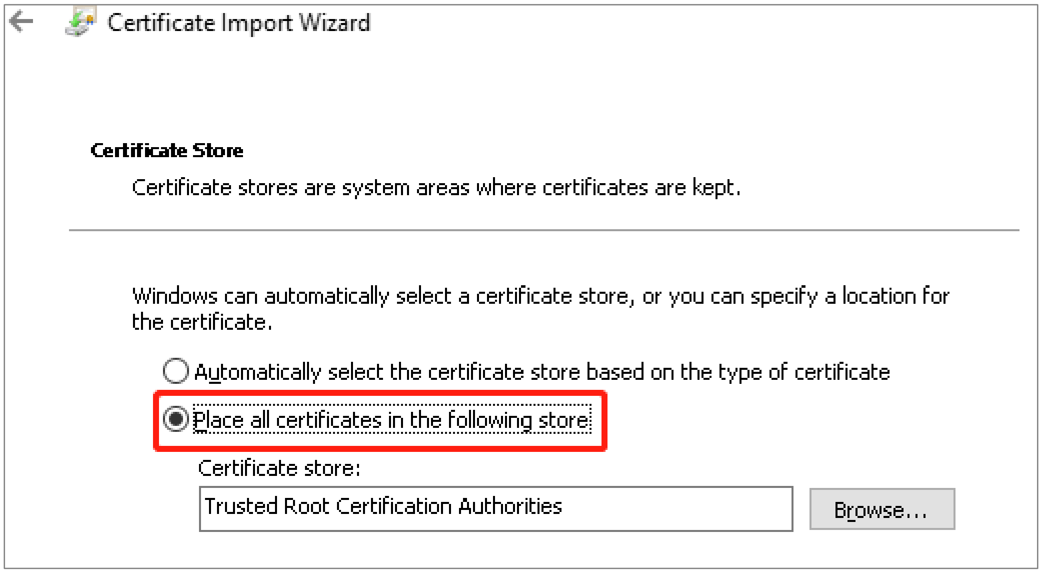
Note: More than one certificate can be stored in a single file in the following formats:

Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

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



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

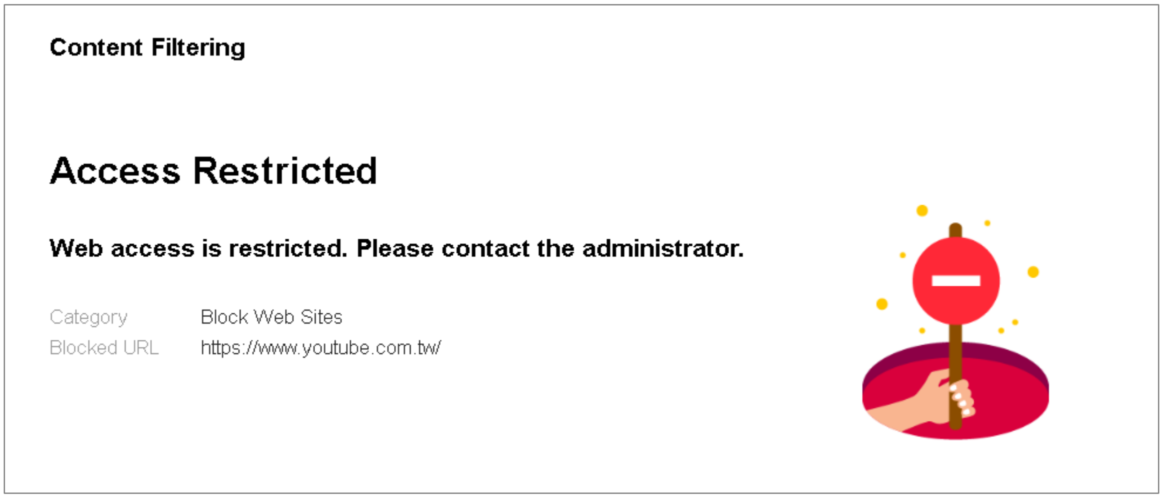
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Test the Result

Using Web Browser to access the YouTube. The gateway will redirect you to a blocked page.



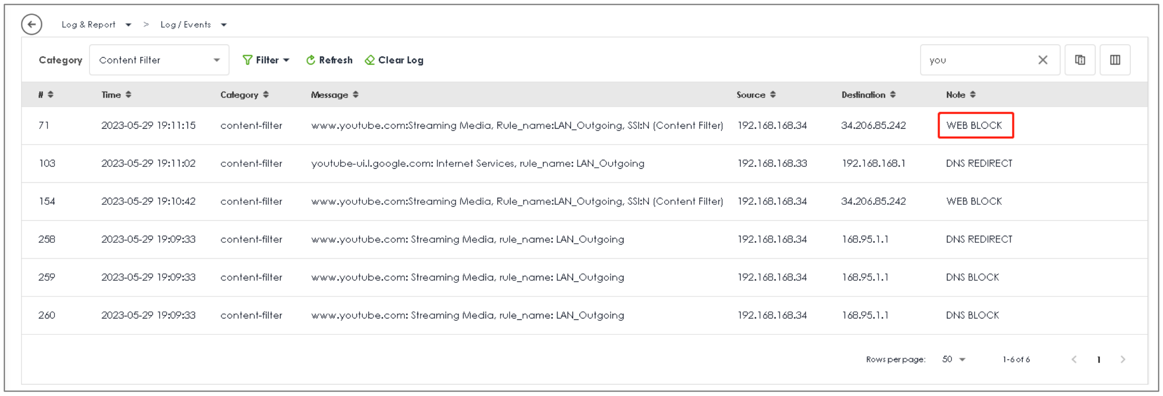
Content Filtering

Access Restricted

Web access is restricted. Please contact the administrator.

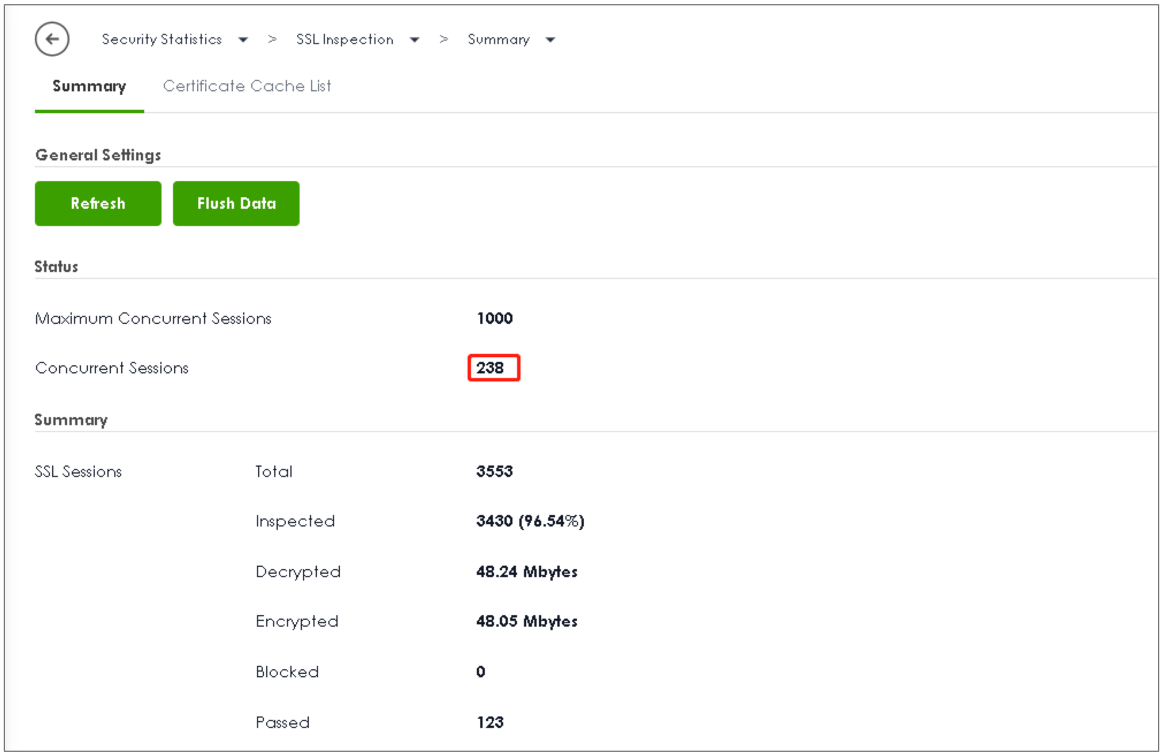
Category	Block Web Sites
Blocked URL	https://www.youtube.com.tw/

Go to Log & Report > Log/Events and select Content Filtering to check the logs.



#	Time	Category	Message	Source	Destination	Note
71	2023-05-29 19:11:15	content-filter	www.youtube.com:Streaming Media, Rule_name:LAN_Outgoing, SSI:N (Content Filter)	192.168.168.34	34.206.85.242	WEB BLOCK
103	2023-05-29 19:11:02	content-filter	youtube-ui.l.google.com: Internet Services, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS REDIRECT
154	2023-05-29 19:10:42	content-filter	www.youtube.com:Streaming Media, Rule_name:LAN_Outgoing, SSI:N (Content Filter)	192.168.168.34	34.206.85.242	WEB BLOCK
258	2023-05-29 19:09:33	content-filter	www.youtube.com: Streaming Media, rule_name: LAN_Outgoing	192.168.168.34	168.95.1.1	DNS REDIRECT
259	2023-05-29 19:09:33	content-filter	www.youtube.com: Streaming Media, rule_name: LAN_Outgoing	192.168.168.34	168.95.1.1	DNS BLOCK
260	2023-05-29 19:09:33	content-filter	www.youtube.com: Streaming Media, rule_name: LAN_Outgoing	192.168.168.34	168.95.1.1	DNS BLOCK

Go to Security Statistics > SSL Inspection > Summary. Traffic is inspected by SSL inspection.



General Settings

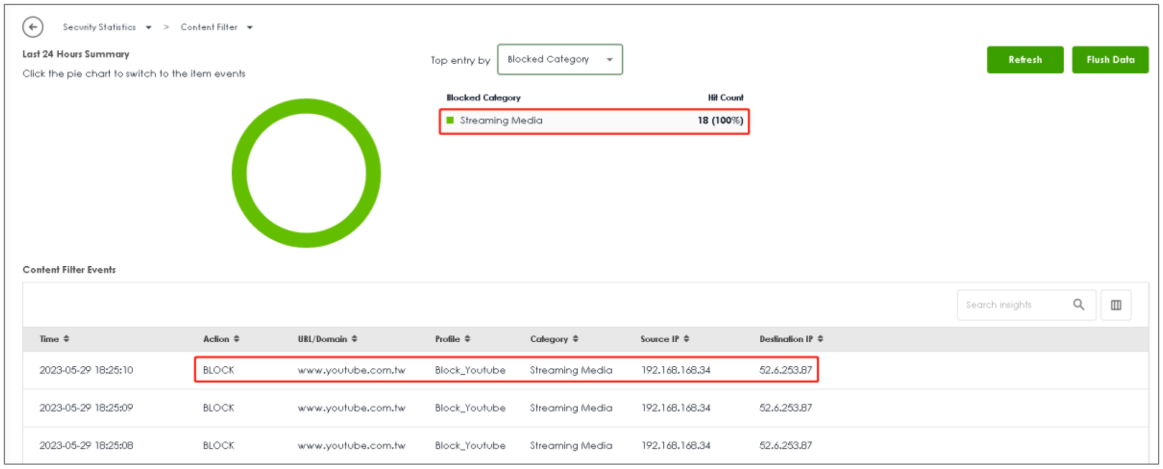
Status

Maximum Concurrent Sessions	1000
Concurrent Sessions	238

Summary

SSL Sessions	Total	3553
	Inspected	3430 (96.54%)
	Decrypted	48.24 Mbytes
	Encrypted	48.05 Mbytes
	Blocked	0
	Passed	123

Go to Security Statistics > Content Filter to check summary of all events.



Last 24 Hours Summary

Click the pie chart to switch to the item events

Top entry by Blocked Category

Blocked Category	Hit Count
🟩 Streaming Media	18 (100%)

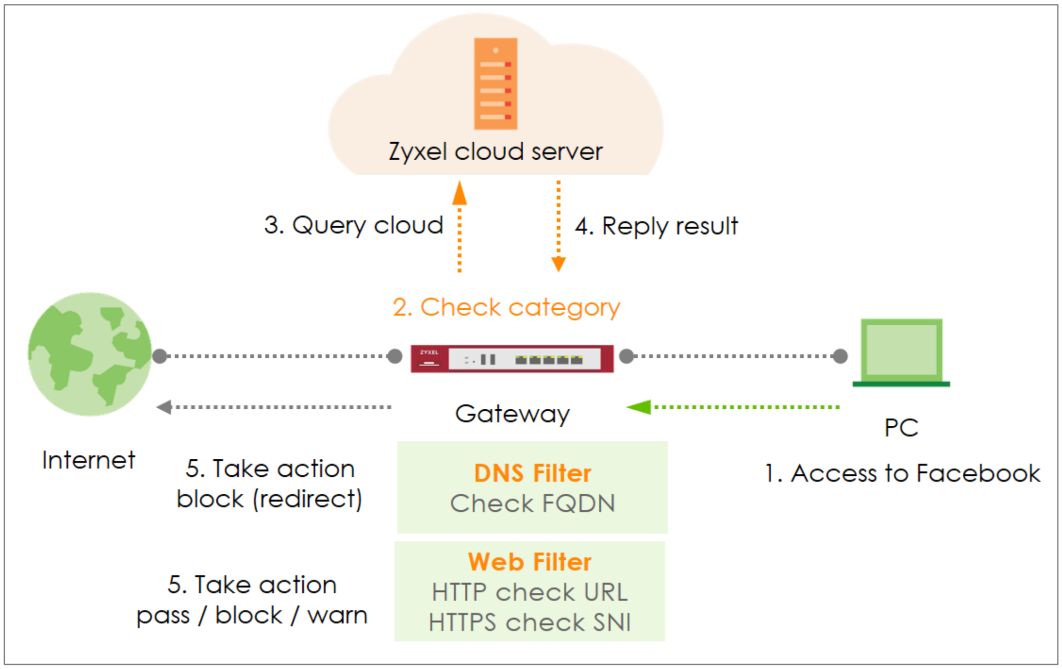
Content Filter Events

Time	Action	URL/Domain	Profile	Category	Source IP	Destination IP
2023-05-29 18:25:10	BLOCK	www.youtube.com.tw	Block_Youtube	Streaming Media	192.168.168.34	52.6.253.87
2023-05-29 18:25:09	BLOCK	www.youtube.com.tw	Block_Youtube	Streaming Media	192.168.168.34	52.6.253.87
2023-05-29 18:25:08	BLOCK	www.youtube.com.tw	Block_Youtube	Streaming Media	192.168.168.34	52.6.253.87

How to Configure Content Filter with HTTPs Domain Filter

The Content Filter with HTTPs Domain Filter allows you to block HTTPs websites by category service. The filtering feature is based on over 100 categories that is built in USG Flex H such as pornography, gambling, hacking, etc.

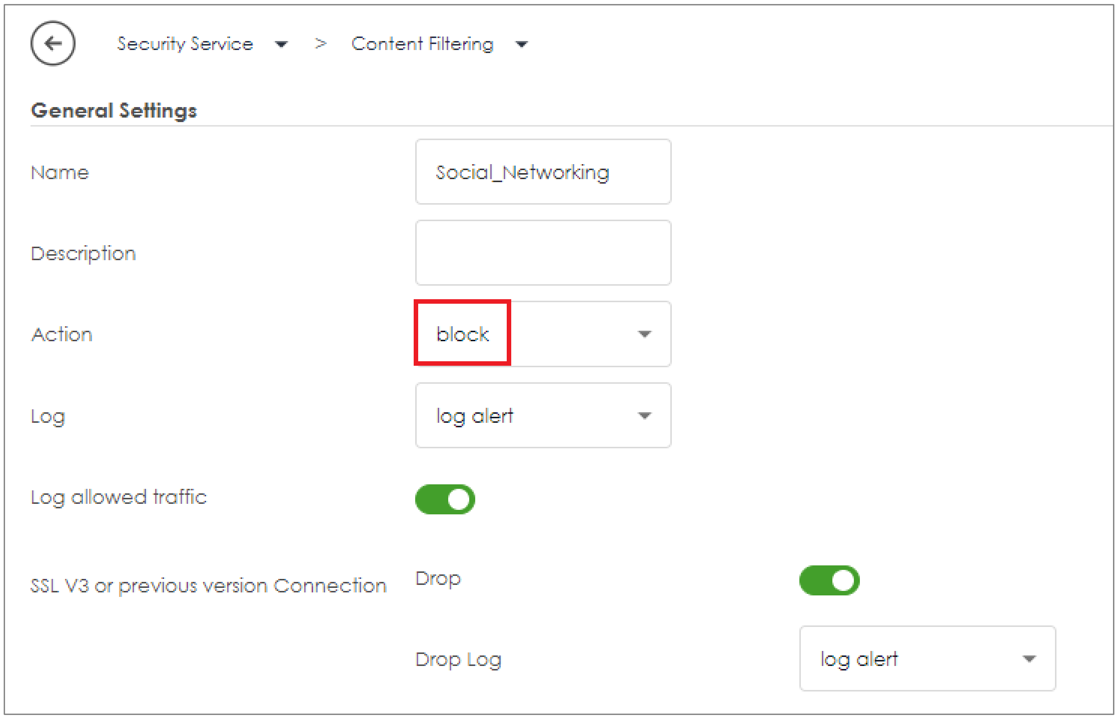
When the user makes an HTTPS request, the information contains a Server Name Indication (SNI) extension fields in server FQDN. Using the SNI to query category from local cache then the cloud database, then take action when it matches the block category in the Content Filter profile.



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 500H (Firmware Version: uOS 1.10).

Set Up the Content Filter

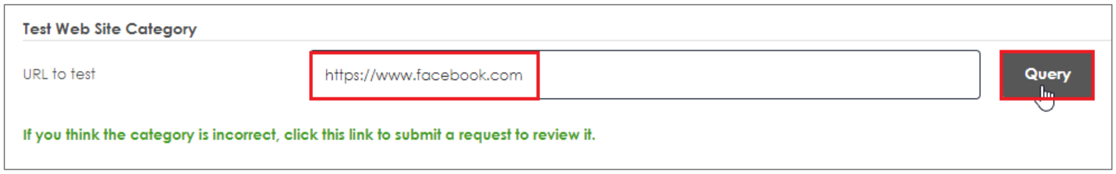
Go to **Security Service > Content Filtering > Profile Management > Add a Content Filter profile**. Configure a **Name** for you to identify the **Content Filter profile** such as "Social_Networking". Configure the **Action** to block when the Content Filter detects events.



General Settings

Name	Social_Networking
Description	
Action	block
Log	log alert
Log allowed traffic	●
SSL V3 or previous version Connection	Drop ●
	Drop Log: log alert

Navigate to **Test Web Site Category** and type URL to test the category and click **Query**.

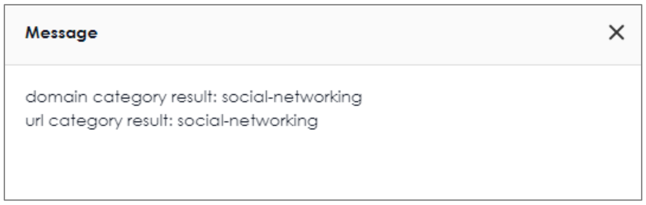


Test Web Site Category

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

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

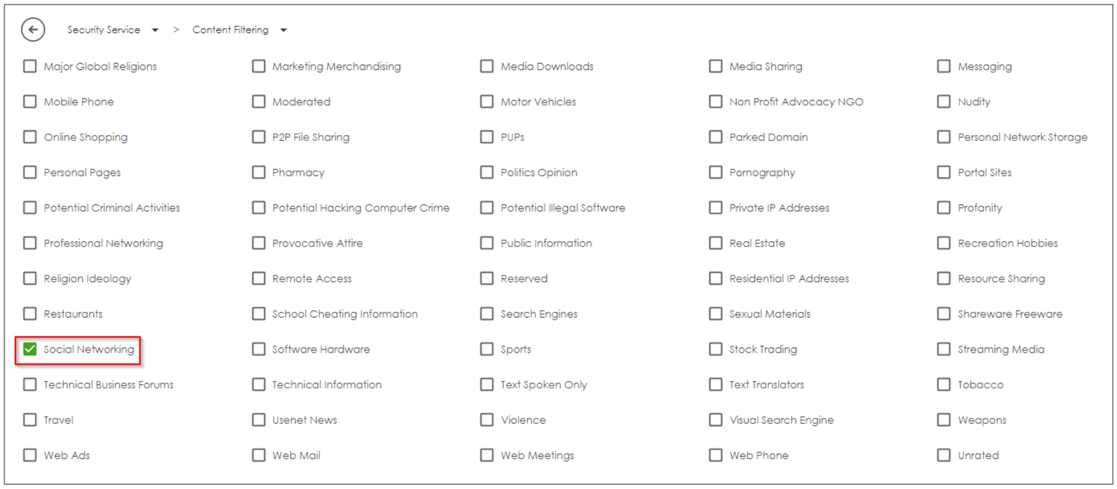
You will see the category recorded in the external content filter server's database for both HTTP and HTTPS Domain you specified.



Message

domain category result: social-networking
url category result: social-networking

Scroll to the **Managed Categories** section, and select categories in this section to control access to specific types of Internet content.

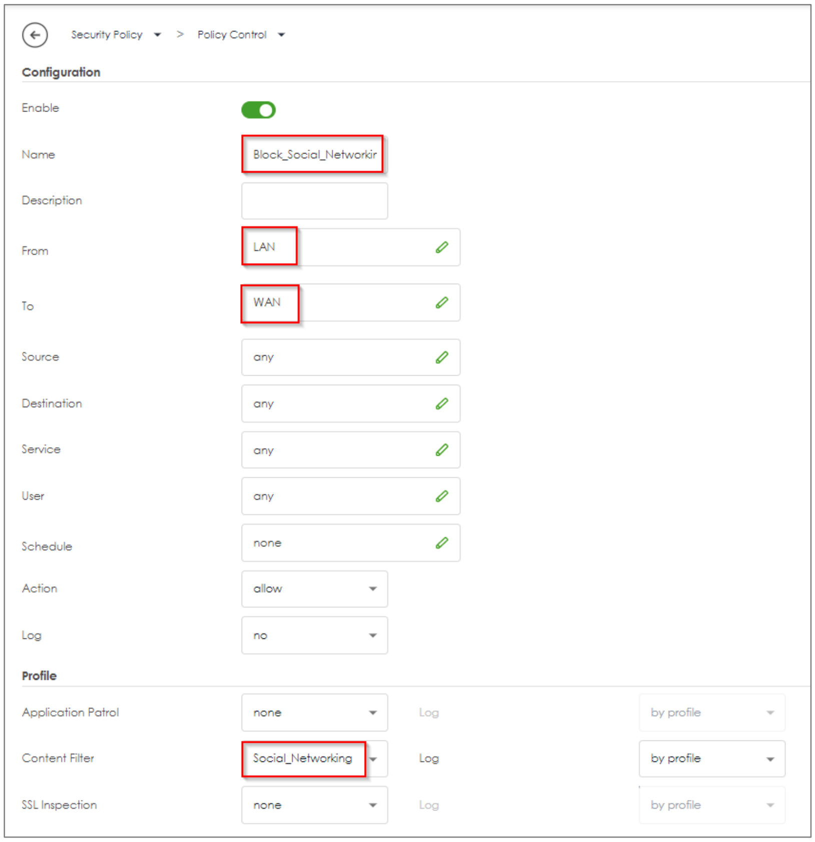


Security Service ▾ > Content Filtering ▾

☐ Major Global Religions	☐ Marketing Merchandising	☐ Media Downloads	☐ Media Sharing	☐ Messaging
☐ Mobile Phone	☐ Moderated	☐ Motor Vehicles	☐ Non Profit Advocacy NGO	☐ Nudity
☐ Online Shopping	☐ P2P File Sharing	☐ PUPs	☐ Parked Domain	☐ Personal Network Storage
☐ Personal Pages	☐ Pharmacy	☐ Politics Opinion	☐ Pornography	☐ Portal Sites
☐ Potential Criminal Activities	☐ Potential Hacking Computer Crime	☐ Potential Illegal Software	☐ Private IP Addresses	☐ Profanity
☐ Professional Networking	☐ Provocative Attire	☐ Public Information	☐ Real Estate	☐ Recreation Hobbies
☐ Religion Ideology	☐ Remote Access	☐ Reserved	☐ Residential IP Addresses	☐ Resource Sharing
☐ Restaurants	☐ School Cheating Information	☐ Search Engines	☐ Sexual Materials	☐ Shareware Freeware
☑ Social Networking	☐ Software Hardware	☐ Sports	☐ Stock Trading	☐ Streaming Media
☐ Technical Business Forums	☐ Technical Information	☐ Text Spoken Only	☐ Text Translators	☐ Tobacco
☐ Travel	☐ Usenet News	☐ Violence	☐ Visual Search Engine	☐ Weapons
☐ Web Ads	☐ Web Mail	☐ Web Meetings	☐ Web Phone	☐ Unrated

Set Up the Security Policy

Go to **Security Policy > Policy Control** to 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 and apply the **Profile > Content Filter** "Social_Networking" on this security policy.



Security Policy > Policy Control

Configuration

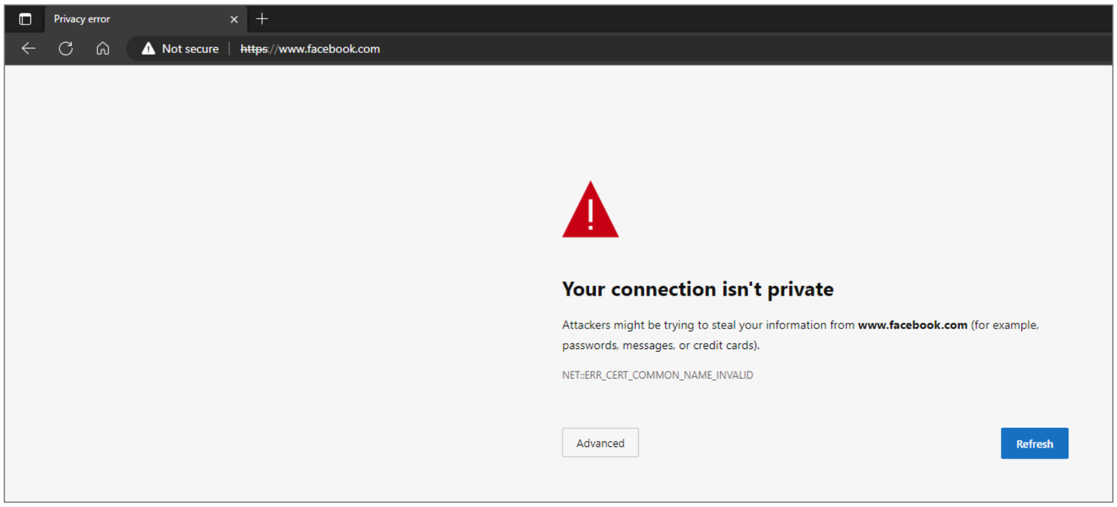
Enable	●
Name	Block_Social_Networkir
Description	
From	LAN
To	WAN
Source	any
Destination	any
Service	any
User	any
Schedule	none
Action	allow
Log	no

Profile

Application Patrol	none	Log	by profile
Content Filter	Social_Networking	Log	by profile
SSL Inspection	none	Log	by profile

Test Result

Type the URL http://www.facebook.com/ or https://www. facebook.com/ onto the browser and cannot browse facebook.

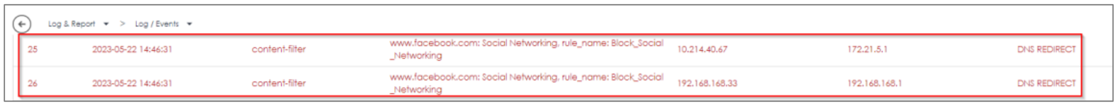


Your connection isn't private

Attackers might be trying to steal your information from **www.facebook.com** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_COMMON_NAME_INVALID

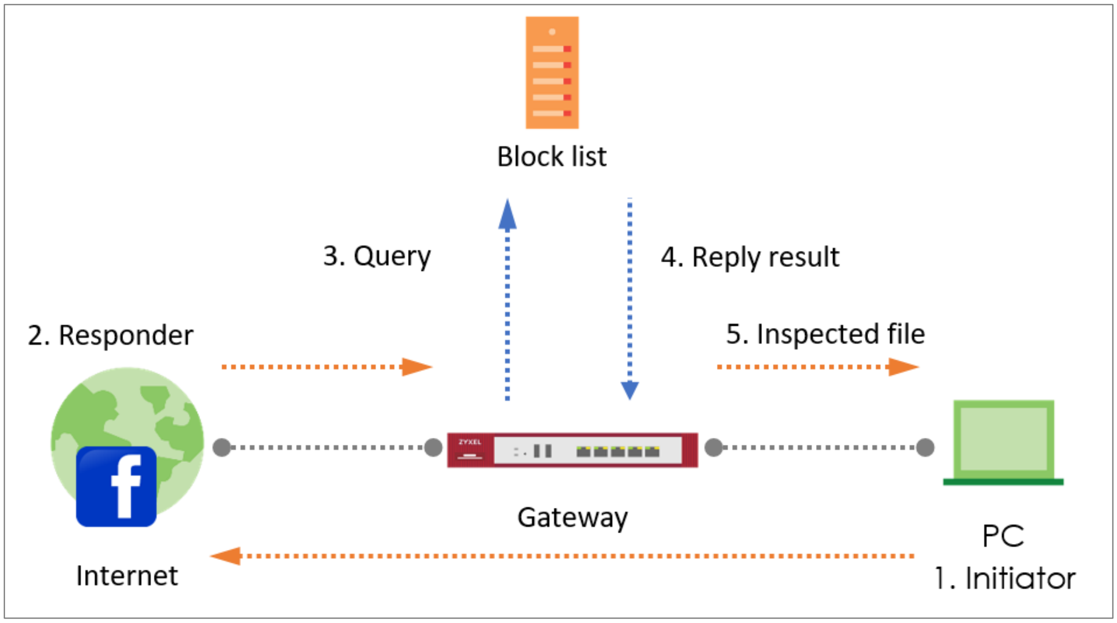
Navigate to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.



25	2023-05-22 14:46:31	content-filter	www.facebook.com: Social Networking, rule_name: Block_Social _Networking	10.214.40.67	172.21.5.1	DNS REDIRECT
26	2023-05-22 14:46:31	content-filter	www.facebook.com: Social Networking, rule_name: Block_Social _Networking	192.168.168.33	192.168.168.1	DNS REDIRECT

How to Block Facebook Using a Content Filter Block List

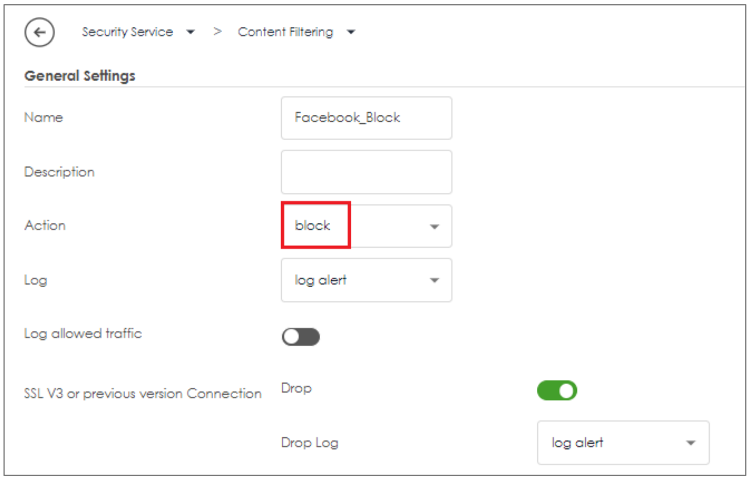
This is an example of using USG Flex H UTM Profile in a Security Policy to block access to a specific social network service. You can use Content Filter and Policy Control to make sure that a certain web page cannot be accessed through both HTTP and HTTPS protocols.



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 500H (Firmware Version: uOS 1.10).

Set Up the Content Filter

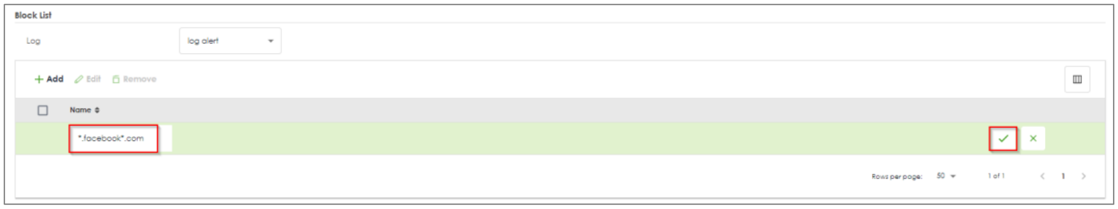
In the USG Flex H, go to **Security Service > Content Filtering > Profile Management > Add a Content Filter profile**. Configure a **Name** for you to identify the **Content Filter profile** such as "Facebook_Block". Configure the **Action** to block when the Content Filter detects events.



General Settings

Name	Facebook_Block
Description	
Action	block
Log	log alert
Log allowed traffic	○
SSL V3 or previous version Connection	Drop ●
	Drop Log: log alert

Go to **Block List** and type URL "*.facebook*.com" to add the URL that you want to block.



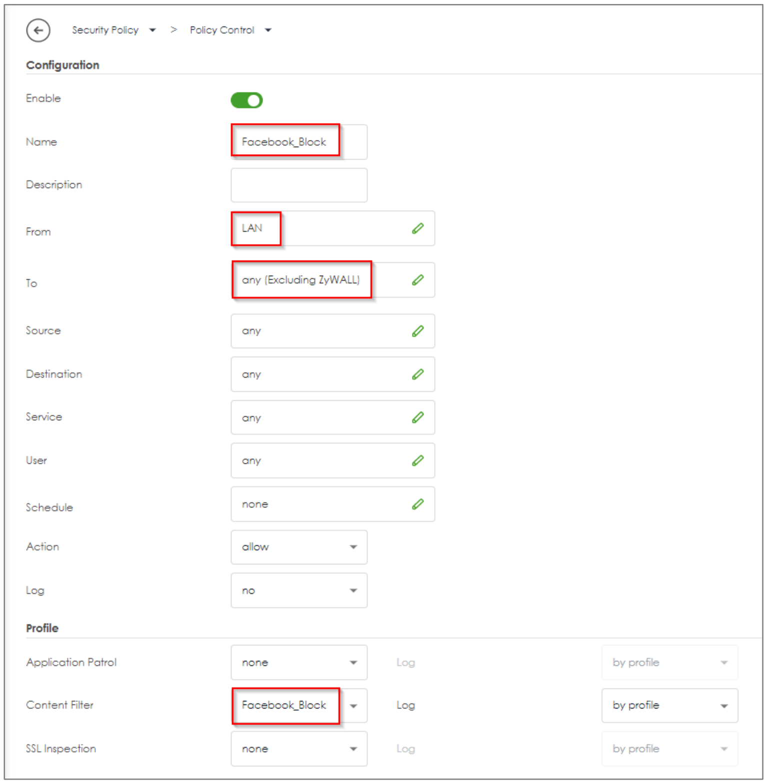
Block List

Log: log alert

☐	Name
	.facebook.com

Set Up the Security Policy

Go to **Security Policy > Policy Control** to 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 and apply the **Profile > Content Filter** "Facebook_Block" on this security policy.


Security Policy > Policy Control

Configuration

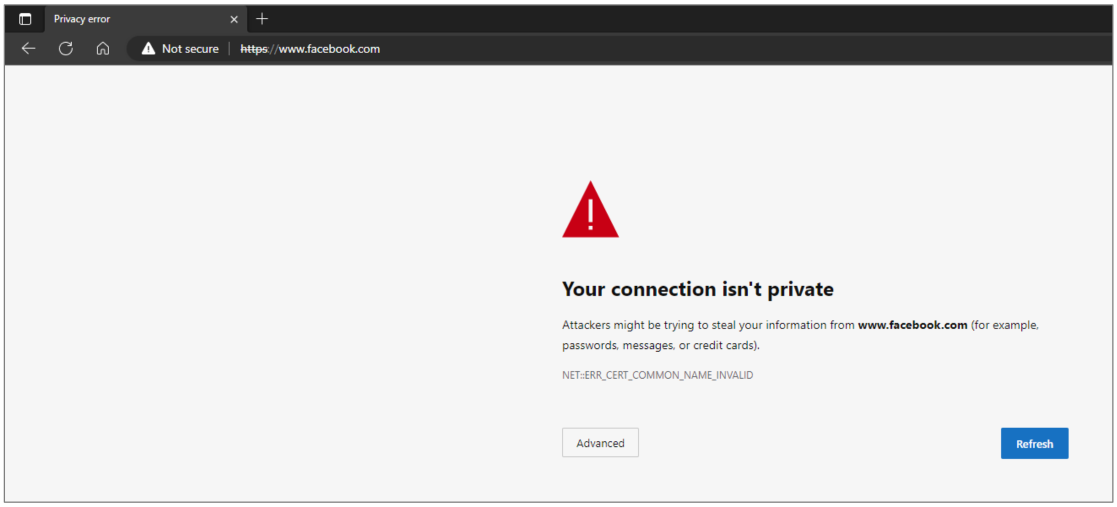
Enable	●
Name	Facebook_Block
Description	
From	LAN
To	any (Excluding ZyWALL)
Source	any
Destination	any
Service	any
User	any
Schedule	none
Action	allow
Log	no

Profile

Application Patrol	none	Log	by profile
Content Filter	Facebook_Block	Log	by profile
SSL Inspection	none	Log	by profile

Test the Result

Type the URL http://www.facebook.com/ or https://www. facebook.com/ onto the browser and cannot browse facebook.

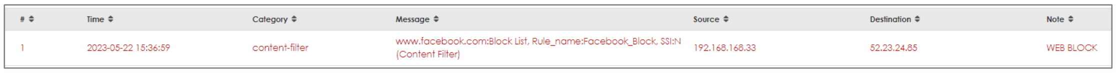


Your connection isn't private

Attackers might be trying to steal your information from **www.facebook.com** (for example, passwords, messages, or credit cards).

NET::ERR_CERT_COMMON_NAME_INVALID

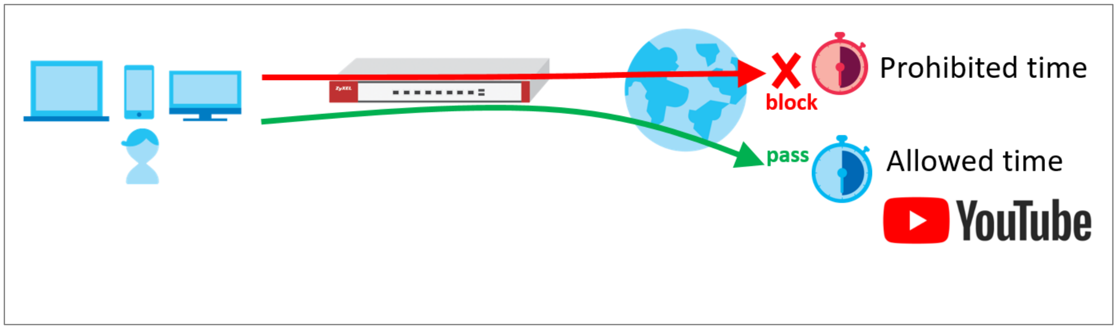
Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.



#	Time	Category	Message	Source	Destination	Note
1	2023-05-22 15:36:59	content-filter	www.facebook.com:Block List, Rule_name:Facebook_Block, SSI:N (Content Filter)	192.168.168.33	52.23.24.85	WEB BLOCK

How to block YouTube access by Schedule

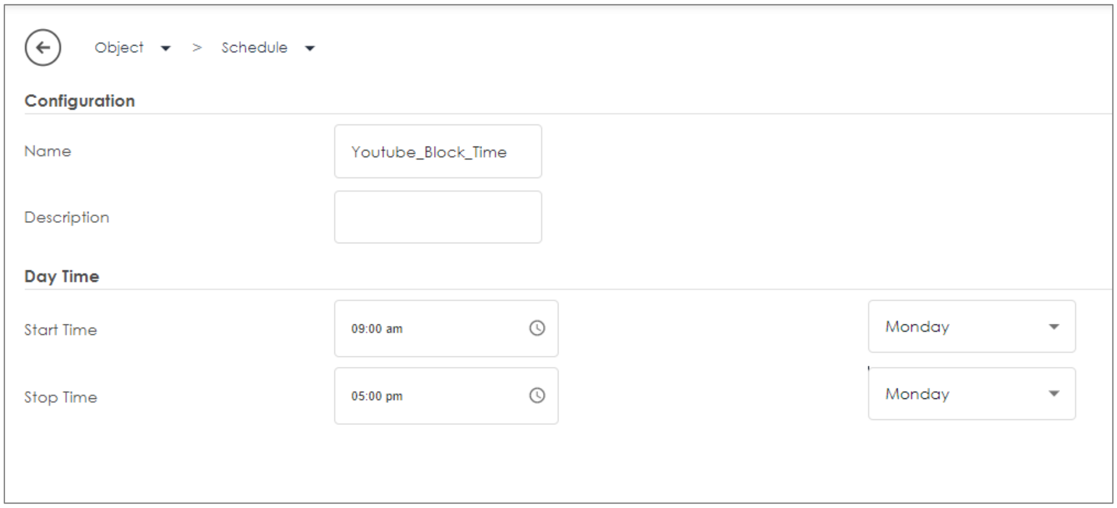
This is an example of using the USG Flex H to block access YouTube access by schedule. You can use Application Patrol and security policy with schedule settings to make sure that YouTube cannot be accessed in your network at a specific prohibited time. This article will guide you on how to deploy it.



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 500H (Firmware Version: uOS 1.10).

Set Up the Schedule

Go to **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.



Configuration

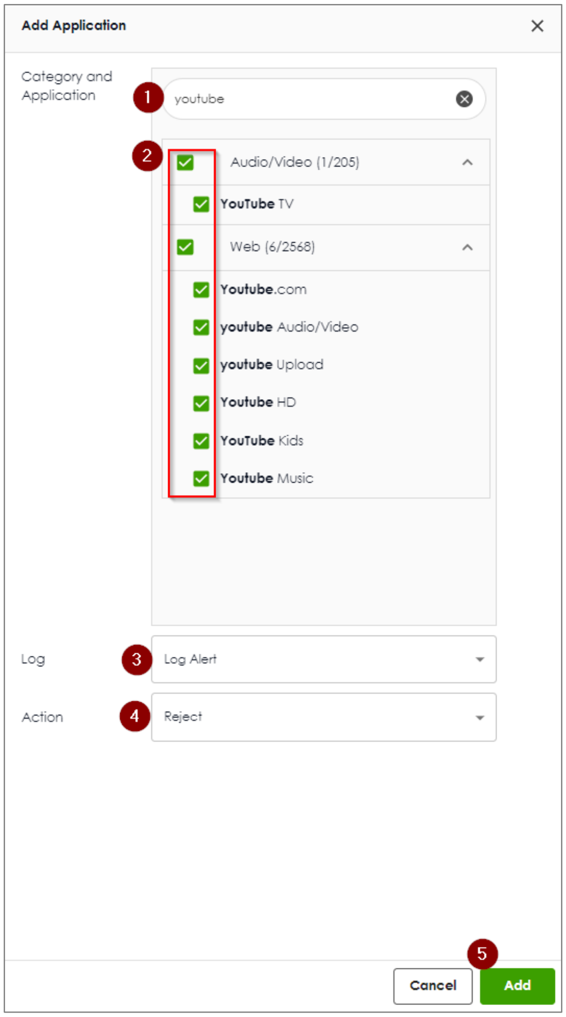
Name	Youtube_Block_Time	
Description		

Day Time

Start Time	09:00 am	Monday
Stop Time	05:00 pm	Monday

Create the Application Patrol profile

In the USG Flex H, go to **Security Service > App Patrol > General Settings > Application Management**. To add an App Patrol profile, configure the profile name and select "**Search Application**". Then enter the keyword "youtube" to search the key-related results and select all YouTube-related apps and click **Add.**



Add Application

Category and Application: youtube

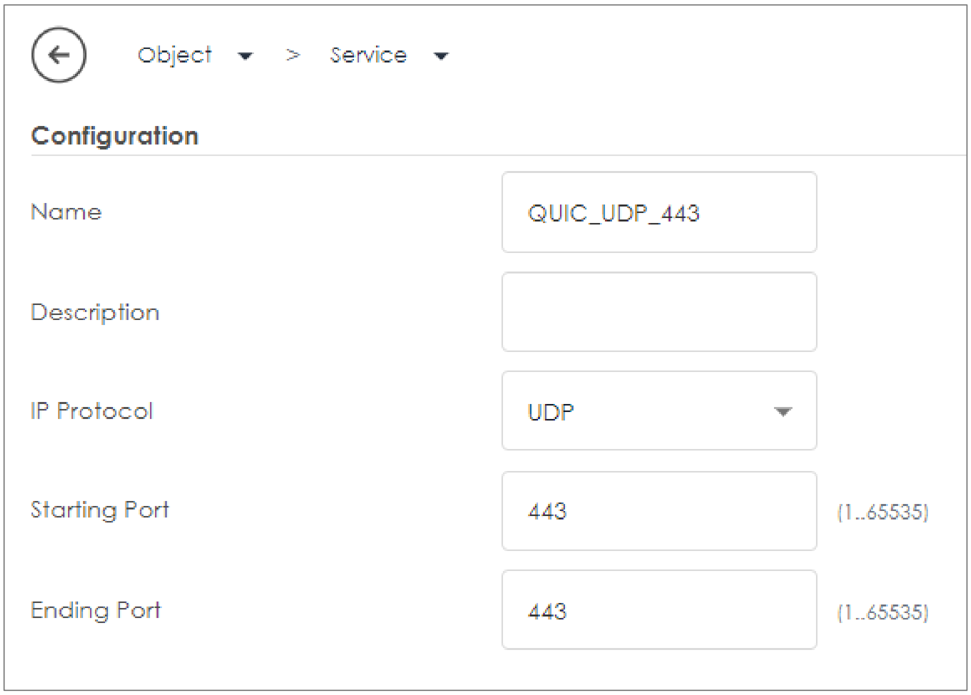
- ☑ Audio/Video (1/205)
  - ☑ YouTube TV
- ☑ Web (6/2568)
  - ☑ Youtube.com
  - ☑ youtube Audio/Video
  - ☑ youtube Upload
  - ☑ Youtube HD
  - ☑ YouTube Kids
  - ☑ Youtube Music

Log: Log Alert

Action: Reject

Set Up the Security Policy

Go to **Object > Service** to add a UDP 443 service object.

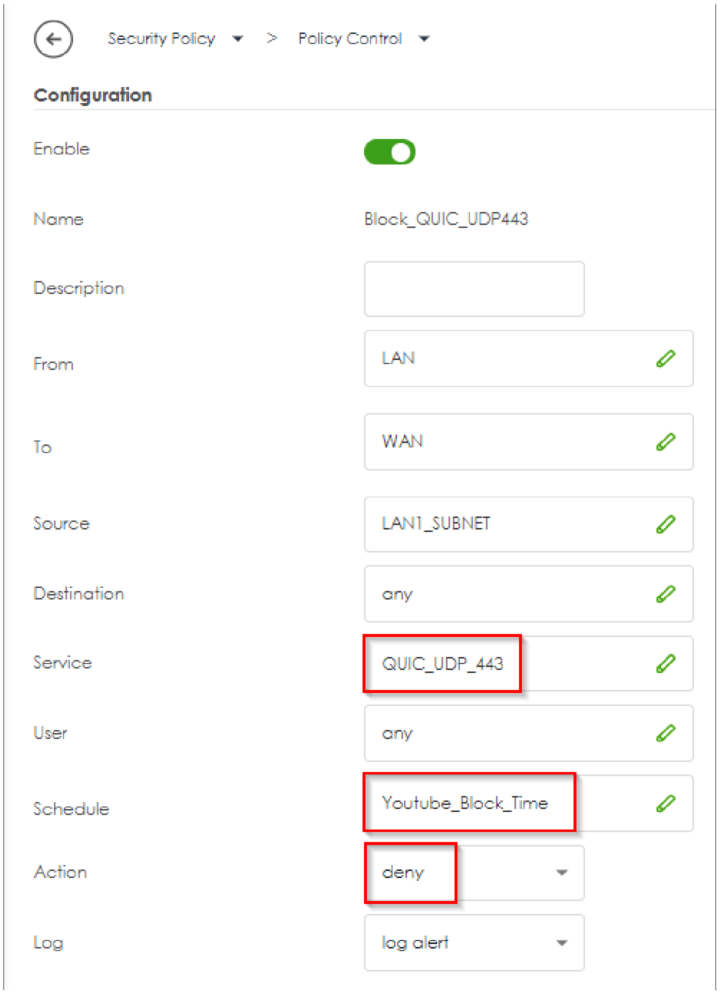


Configuration

Name	QUIC_UDP_443	
Description		
IP Protocol	UDP	
Starting Port	443	(1..65535)
Ending Port	443	(1..65535)

Go to **Security Policy > Policy Control** to 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 **service** QUIC_UDP443 and select the **Schedule** that defines when the policy would be applied.

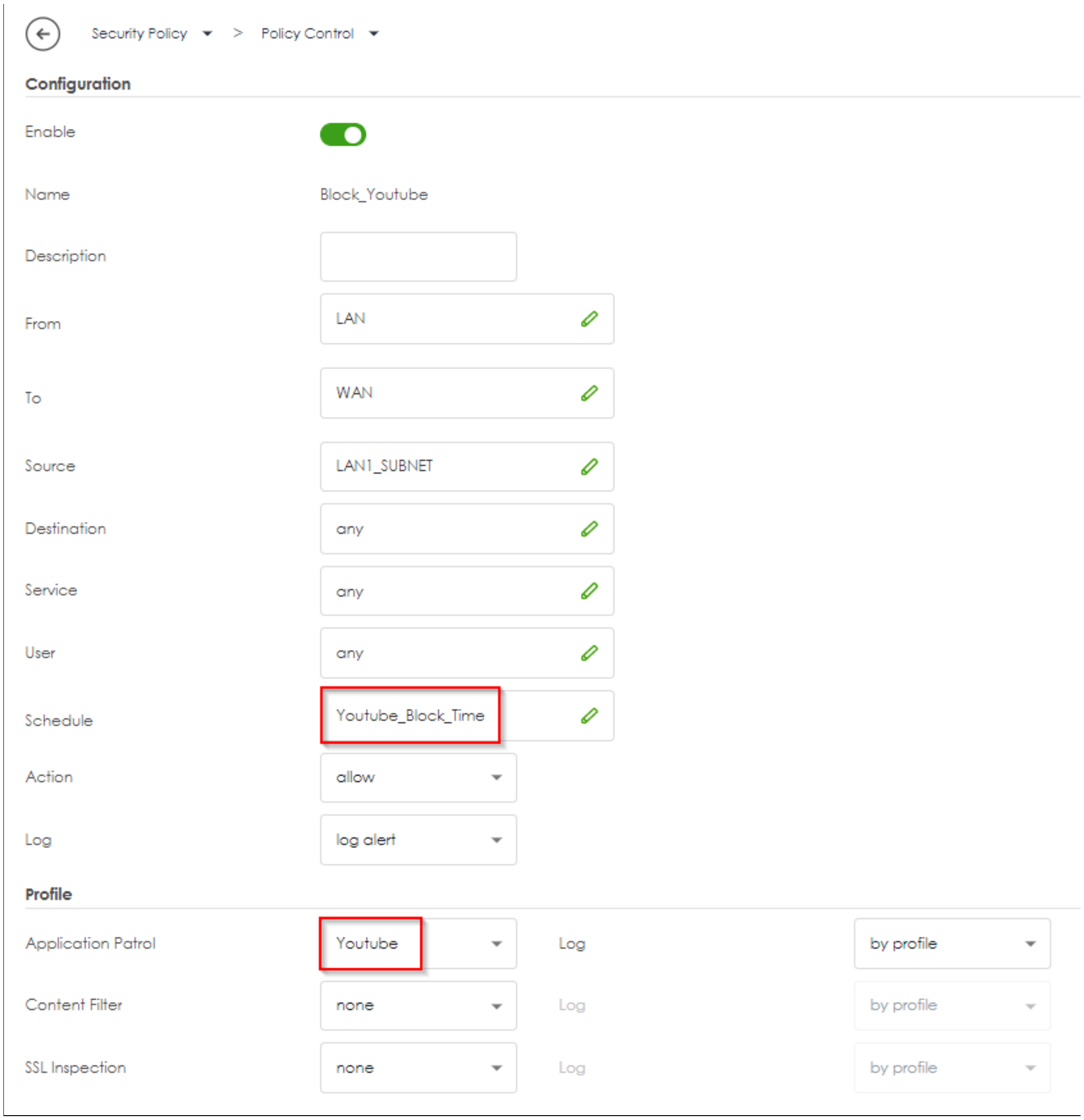
In this example, select "Youtube_Blocked_Time".



Configuration

Enable	●
Name	Block_QUIC_UDP443
Description	
From	LAN
To	WAN
Source	LAN1_SUBNET
Destination	any
Service	QUIC_UDP_443
User	any
Schedule	Youtube_Block_Time
Action	deny
Log	log alert

Add another security policy to block YouTube by schedule. To configure a **Name** and the **From**, **To** traffic direction. Select the **Schedule** that defines when the policy would be applied. Finally, to scroll down the **Profile**, check **Application Patrol** and select a profile from the list box. In this example, **Schedule**: Youtube_Block_Time; **Application Patrol**: Youtube.



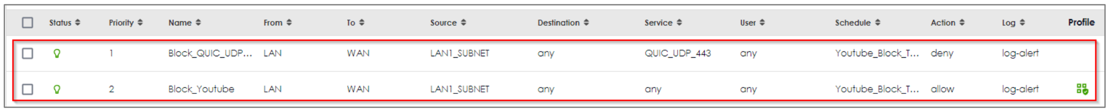
Configuration

Enable	●
Name	Block_Youtube
Description	
From	LAN
To	WAN
Source	LAN1_SUBNET
Destination	any
Service	any
User	any
Schedule	Youtube_Block_Time
Action	allow
Log	log alert

Profile

Application Patrol	Youtube	Log	by profile
Content Filter	none	Log	by profile
SSL Inspection	none	Log	by profile

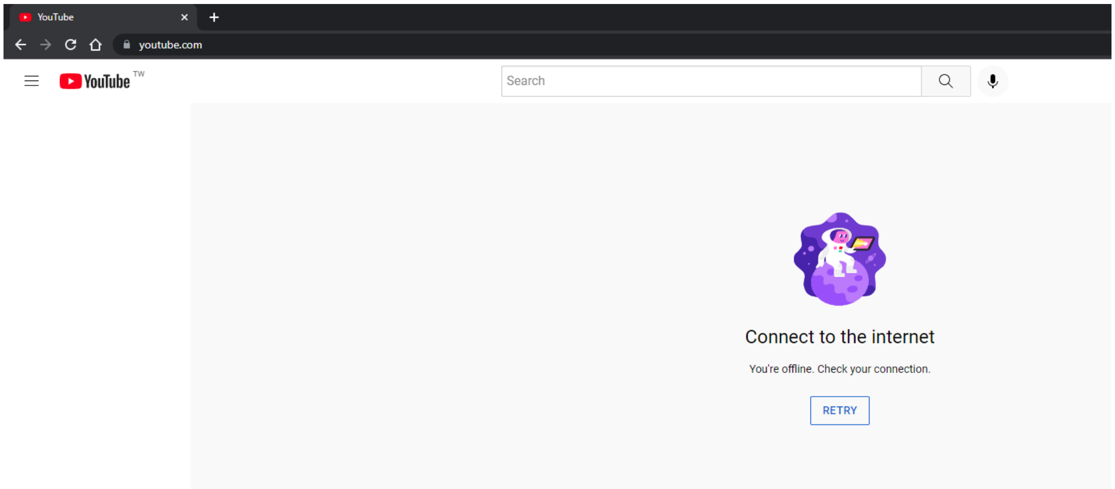
Then go back to the security policy page and move the security priority of block UDP 443 is higher than block YouTube by schedule.



□	Status	Priority	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log	Profile
□	●	1	Block_QUIC_UDP...	LAN	WAN	LAN1_SUBNET	any	QUIC_UDP_443	any	Youtube_Block_T...	deny	log-alert	
□	●	2	Block_Youtube	LAN	WAN	LAN1_SUBNET	any	any	any	Youtube_Block_T...	allow	log-alert	✓

Test the Result

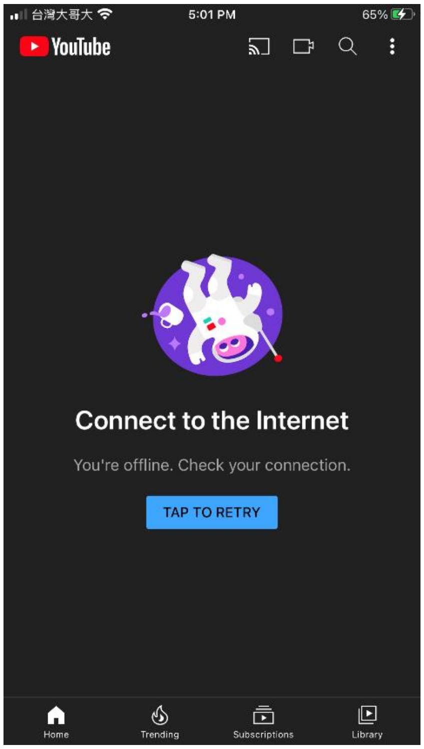
Type the URL http://www.youtube.com/ or https://www.youtube.com/ onto the browser and cannot browse YouTube.



Connect to the internet

You're offline. Check your connection.

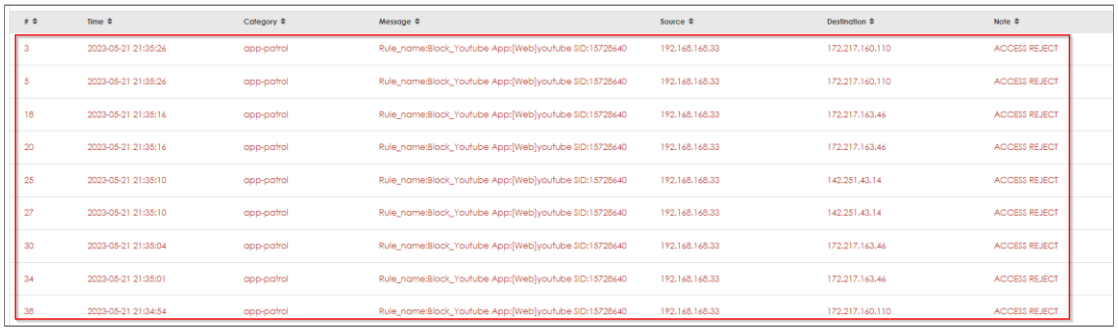
Open the YouTube APP on the phone and cannot access to YouTube.



Connect to the Internet

You're offline. Check your connection.

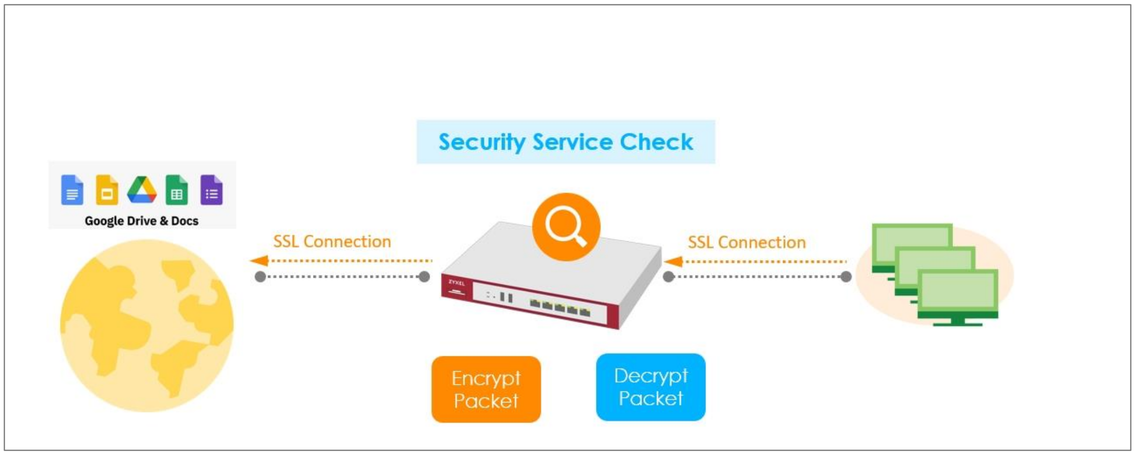
Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.



# ⇕	Time ⇕	Category ⇕	Message ⇕	Source ⇕	Destination ⇕	Note ⇕
3	2023-05-21 21:35:26	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.160.110	ACCESS REJECT
5	2023-05-21 21:35:26	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.160.110	ACCESS REJECT
18	2023-05-21 21:35:16	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.163.46	ACCESS REJECT
20	2023-05-21 21:35:16	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.163.46	ACCESS REJECT
25	2023-05-21 21:35:10	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	142.251.43.14	ACCESS REJECT
27	2023-05-21 21:35:10	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	142.251.43.14	ACCESS REJECT
30	2023-05-21 21:35:04	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.163.46	ACCESS REJECT
34	2023-05-21 21:35:01	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.163.46	ACCESS REJECT
38	2023-05-21 21:34:54	app-patrol	Rule_name:Block_Youtube App:[Web]youtube SID:15728640	192.168.168.33	172.217.160.110	ACCESS REJECT

How to Control Access to Google Drive

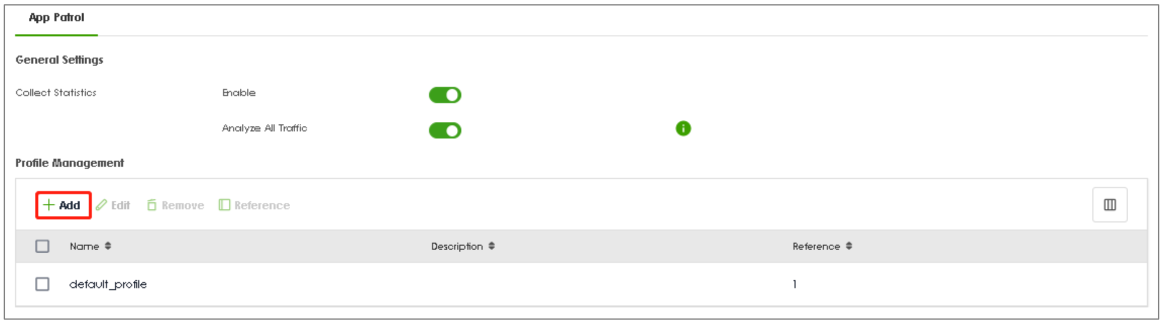
This is an example of using a FLEX UTM Profile in a Security Policy to block access to a specific file transfer service. You can use Application Patrol and Policy Control to make sure that a certain file transfer service cannot be accessed through both HTTP and HTTPS protocols.



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 200H (Firmware Version: uOS 1.10).

Create app patrol profile

Go to Security Service > App patrol > Profile management, and click Add to create profile

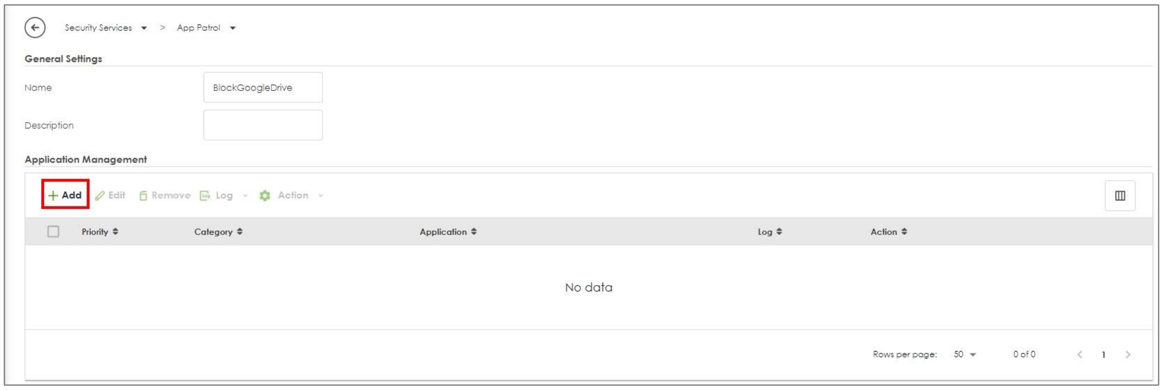


Collect Statistics — Enable: on

Analyze All Traffic: on

Name	Description	Reference
default_profile		1

Click add to add application in this profile.



Name: BlockGoogleDrive

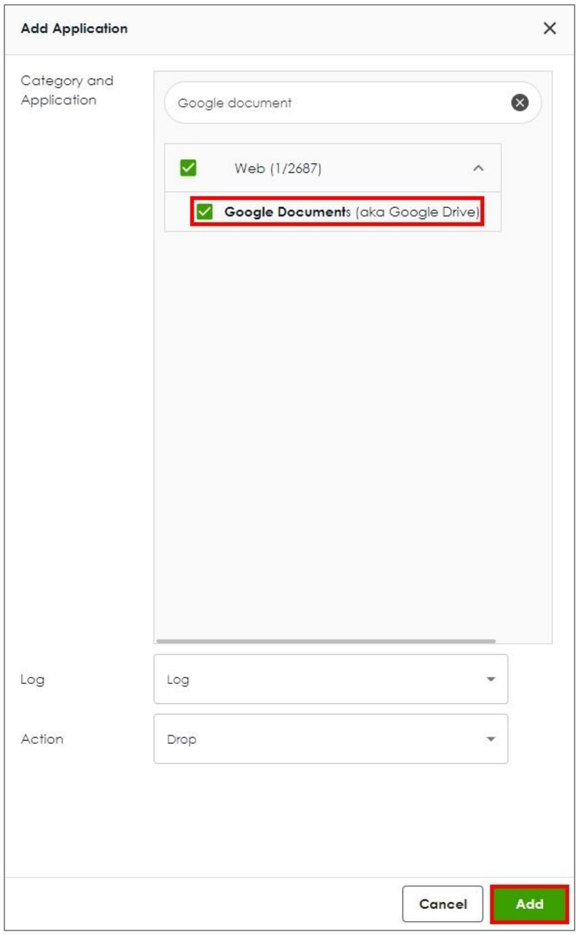
Description:

Priority	Category	Application	Log	Action

No data

Search **Google Documents(aka Google Drive)**, and select this Application.

Action set to Drop, and click Add.



Add Application

Category and Application: Google document

☑ Web (1/2687)

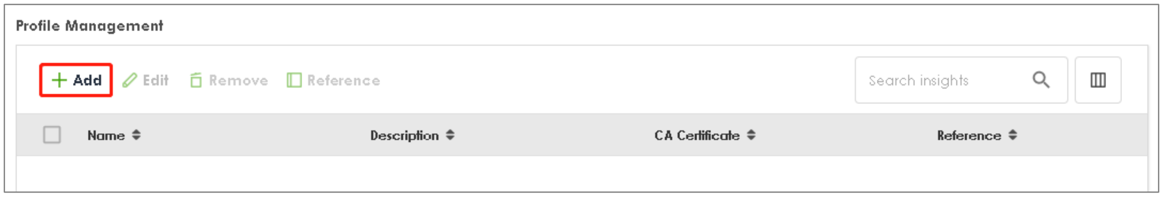
☑ **Google Documents** (aka Google Drive)

Log: Log

Action: Drop

Set Up SSL Inspection on the FLEX

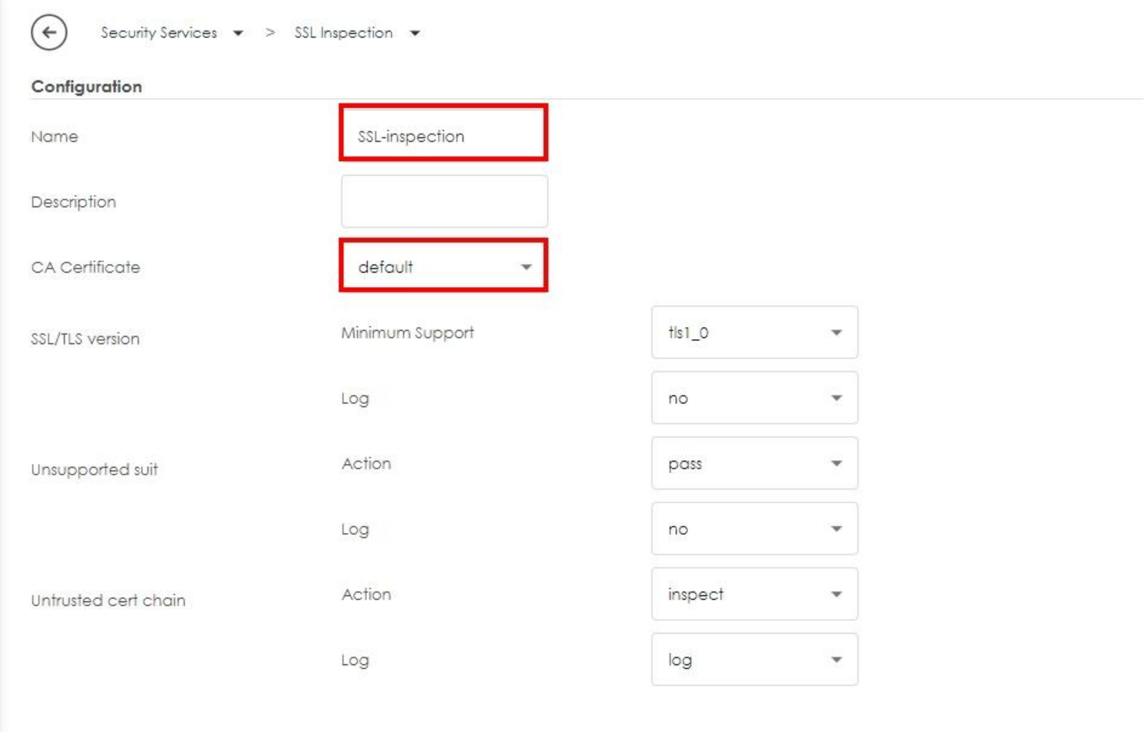
In the FLEX, go to Security Service > SSL inspection > profile > Profile Management, and click Add to create profile



Profile Management

□	Name	Description	CA Certificate	Reference

Type profile Name, and select the CA Certificate to be the certificate used in this profile. Leave other actions as default settings.



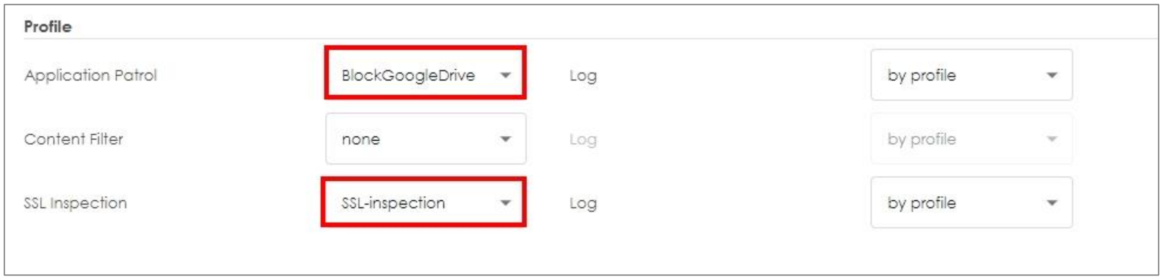
Configuration

Name	SSL-inspection	
Description		
CA Certificate	default	
SSL/TLS version	Minimum Support	tls1_0
	Log	no
Unsupported suit	Action	pass
	Log	no
Untrusted cert chain	Action	inspect
	Log	log

Apply profile to security policy

Go to Security Policy > Policy control. Edit LAN_Outgoing, and scroll down to profile section.

Select Application Patrol, and SSL Inspection.



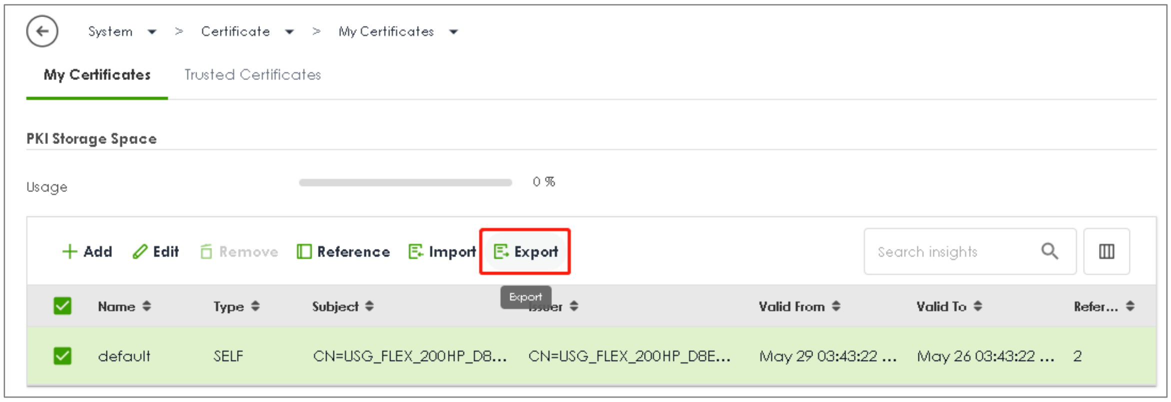
Profile

Application Patrol	BlockGoogleDrive	Log	by profile
Content Filter	none	Log	by profile
SSL Inspection	SSL-inspection	Log	by profile

Export Certificate from FLEX and import to Lan hosts

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

Go to System > Certificate > My Certificates to export default certificate from FLEX.

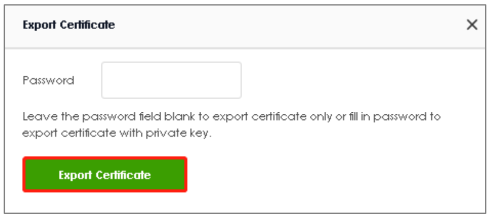


PKI Storage Space

Usage 0 %

	Name	Type	Subject	Issuer	Valid From	Valid To	Refer...
☑	default	SELF	CN=USG_FLEX_200HP_DB...	CN=USG_FLEX_200HP_DBE...	May 29 03:43:22 ...	May 26 03:43:22 ...	2

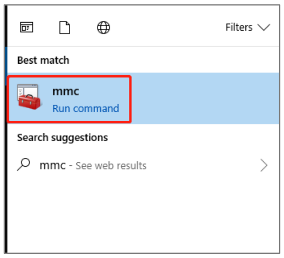
Click Export Certificate to export certificate file, and Save default certificate as default.crt file to Windows OS.



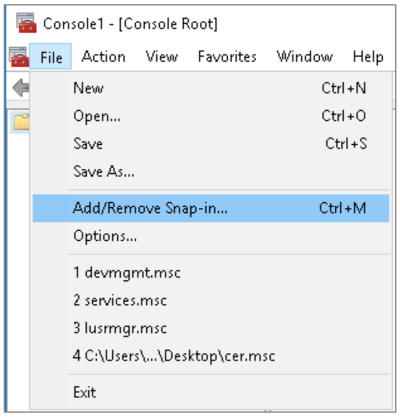
Password

Leave the password field blank to export certificate only or fill in password to export certificate with private key.

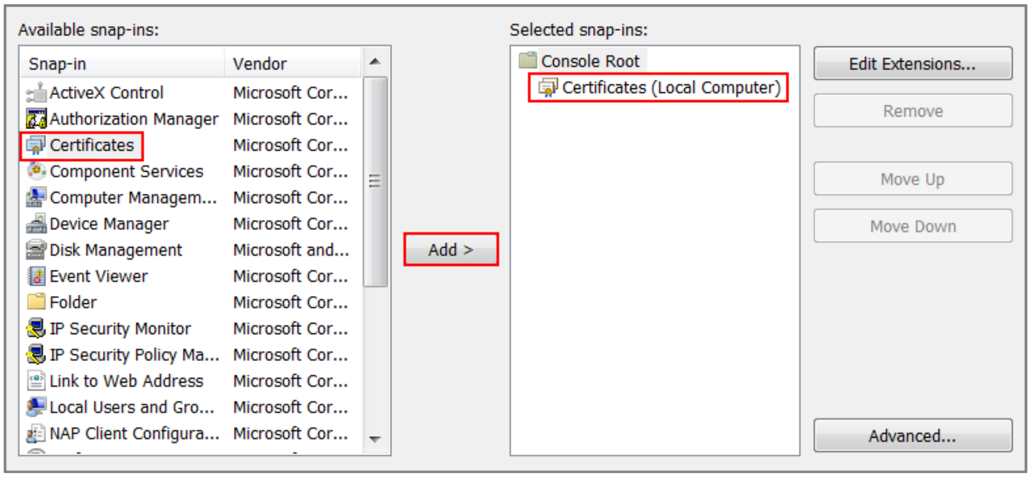
In Windows Start Menu > Search Box, type MMC and press Enter.



In the mmc console window, click 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.

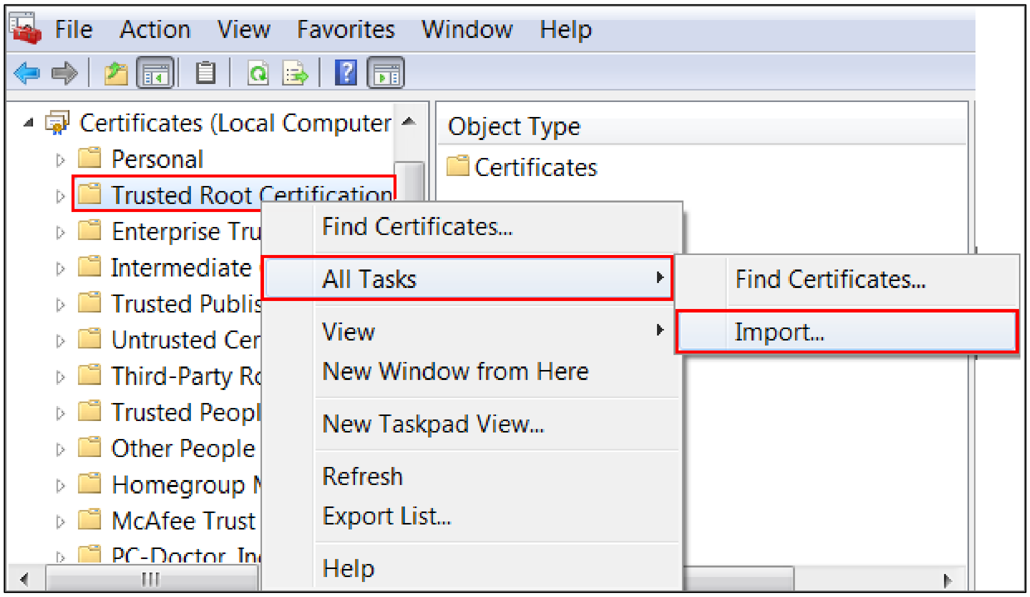

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
IP Security Monitor	Microsoft Cor...
IP Security Policy Ma...	Microsoft Cor...
Link to Web Address	Microsoft Cor...
Local Users and Gro...	Microsoft Cor...
NAP Client Configura...	Microsoft Cor...

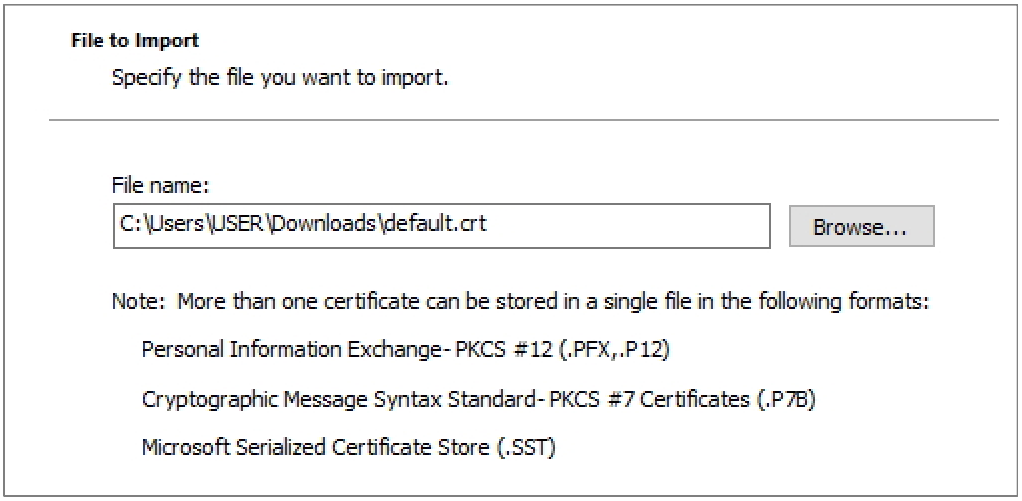
Selected snap-ins:

Console Root
Certificates (Local Computer)

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



Click Next. Then, Browse..., and locate the default.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...

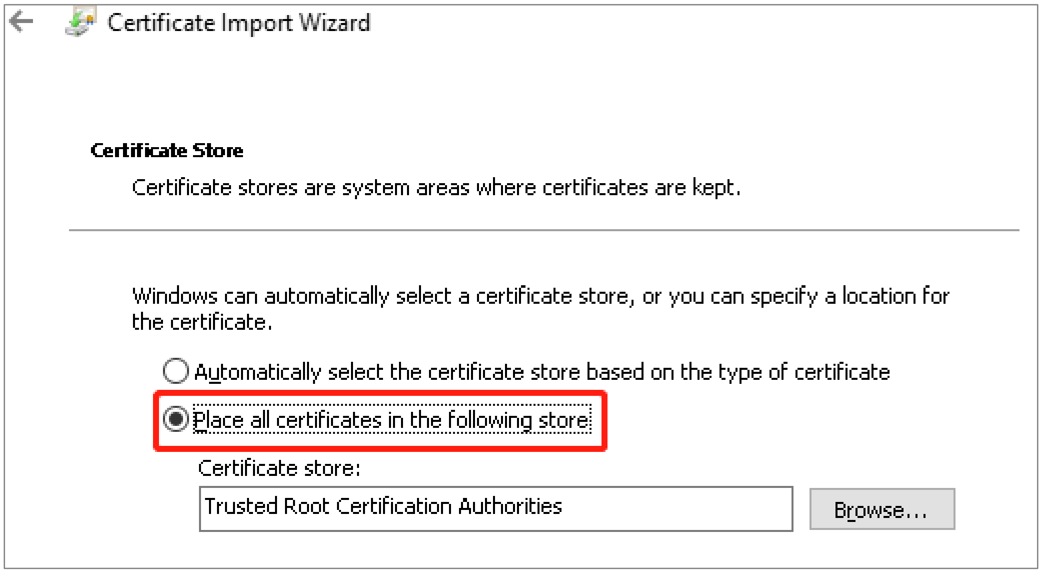
Note: More than one certificate can be stored in a single file in the following formats:

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 Import Wizard

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

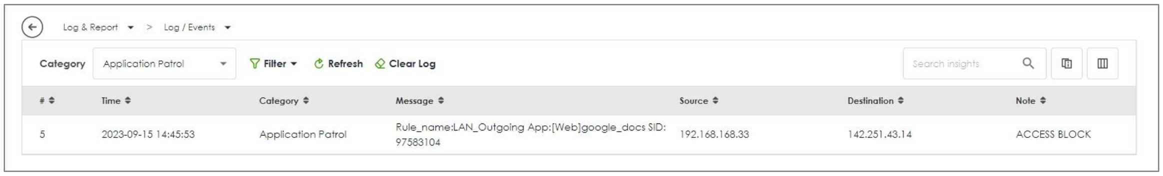
● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Test the Result

Access to Google drive from Lan host to verify if it is blocked by firewall Application patrol.

Go to Log & Report > Log/Events and select Application Patrol to check the logs.

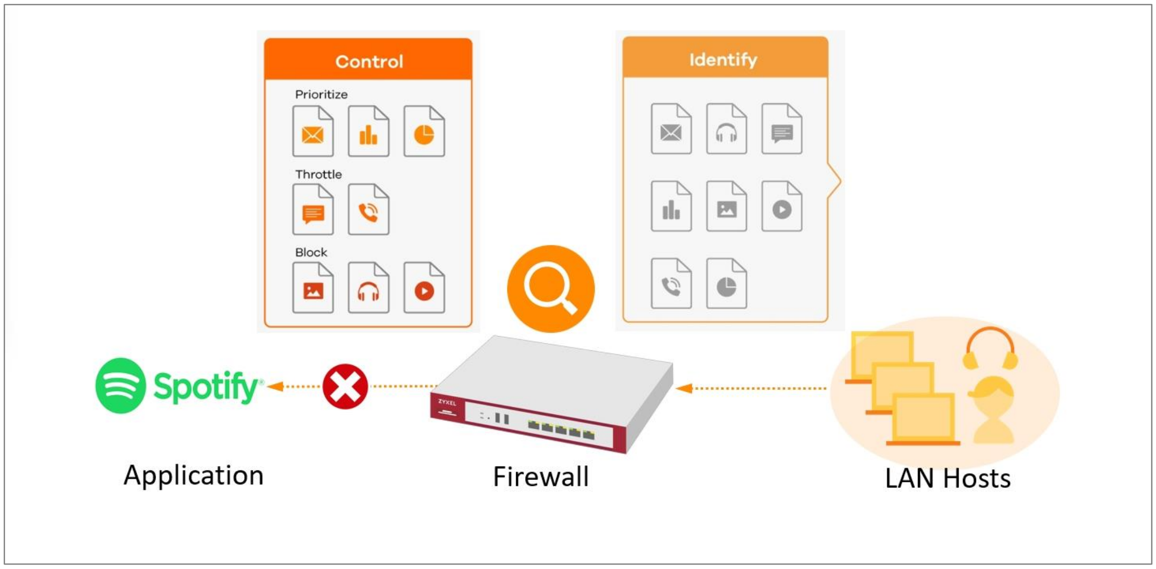


Category: Application Patrol

#	Time	Category	Message	Source	Destination	Note
5	2023-09-15 14:45:53	Application Patrol	Rule_name:LAN_Outgoing App:[Web]google_docs SID: 97583104	192.168.168.33	142.251.43.14	ACCESS BLOCK

How to Block the Spotify Music Streaming Service

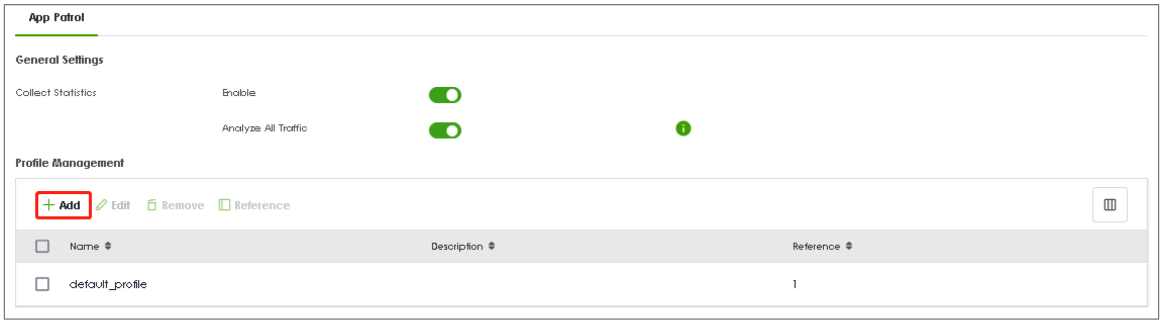
This is an example of using a FLEX UTM App Patrol Profile in a Security Policy to block the Spotify Music Streaming Service. You can use Application Patrol and Policy Control to ensure that the Spotify Music Streaming Service cannot be accessed on the LAN.



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 200H (Firmware Version: uOS 1.10).

Create a App Patrol profile

Go to Security Service > App patrol > Profile management, and click Add to create profile.



General Settings

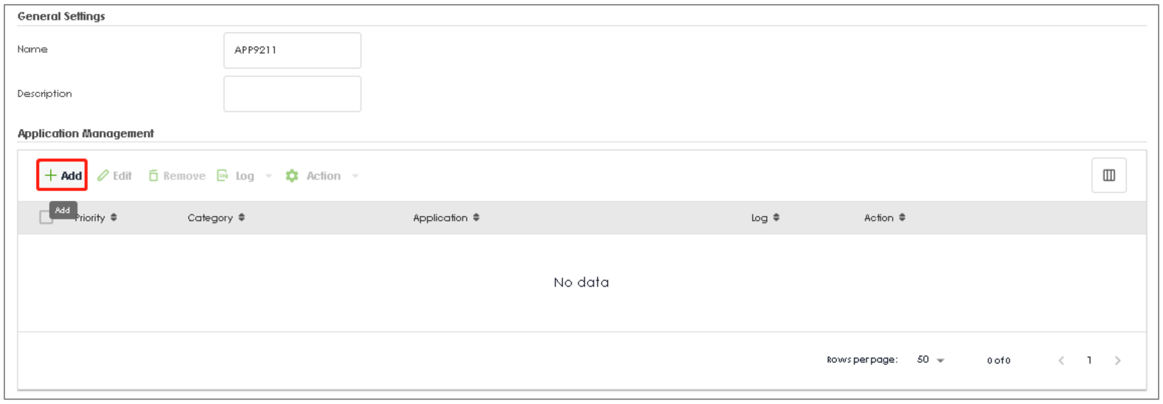
Collect Statistics — Enable: on

Analyze All Traffic: on

Profile Management

□	Name	Description	Reference
□	default_profile		1

Click add to add application in this profile.



General Settings

Name: APP9211

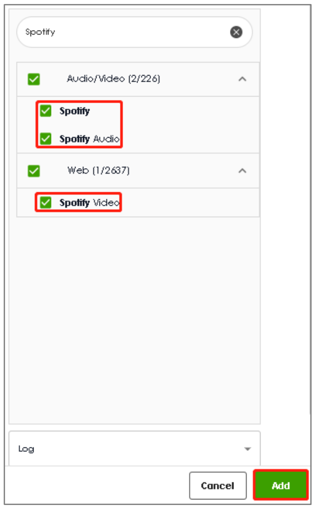
Description:

Application Management

□	Priority	Category	Application	Log	Action
No data					

Rows per page: 50 0 of 0 1

Search Spotify, and select this Application. Action set to Drop, and click Add.



☑ Audio/Video (2/226)

☑ Spotify

☑ Spotify Audio

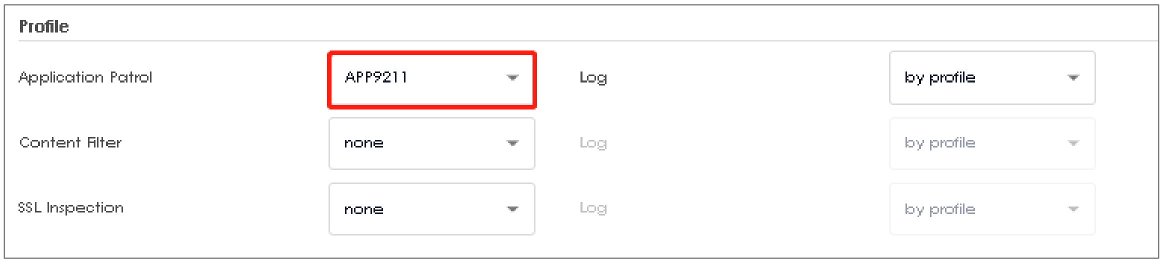
☑ Web (1/2637)

☑ Spotify Video

Apply profile to security policy

Go to Security Policy > Policy control. Edit LAN_Outgoing, and scroll down to profile section.

Apply Application Patrol profile to Security policy.



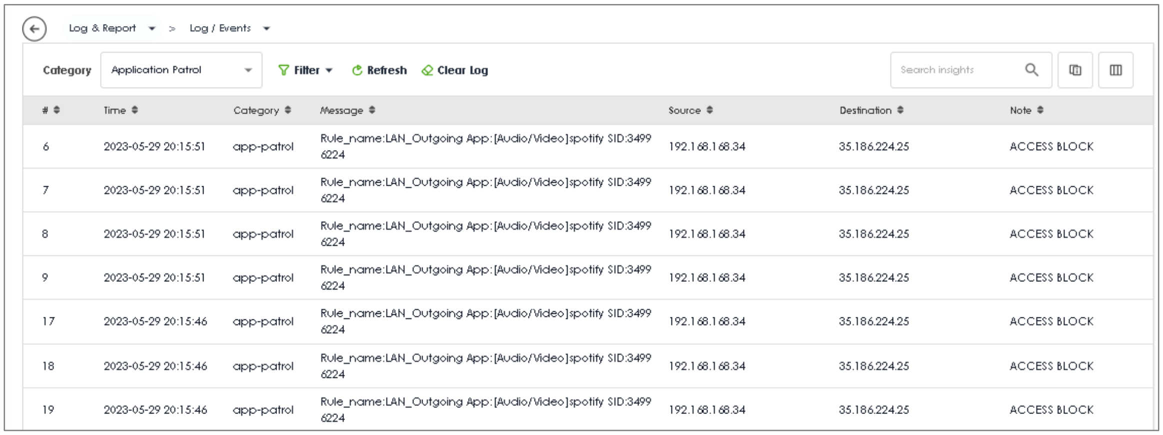
Profile

Application Patrol	APP9211	Log	by profile
Content Filter	none	Log	by profile
SSL Inspection	none	Log	by profile

Test the Result

Access to Spotify from Lan host to verify if it is blocked by firewall Application patrol.

Go to Log & Report > Log/Events and select Application Patrol to check the logs.

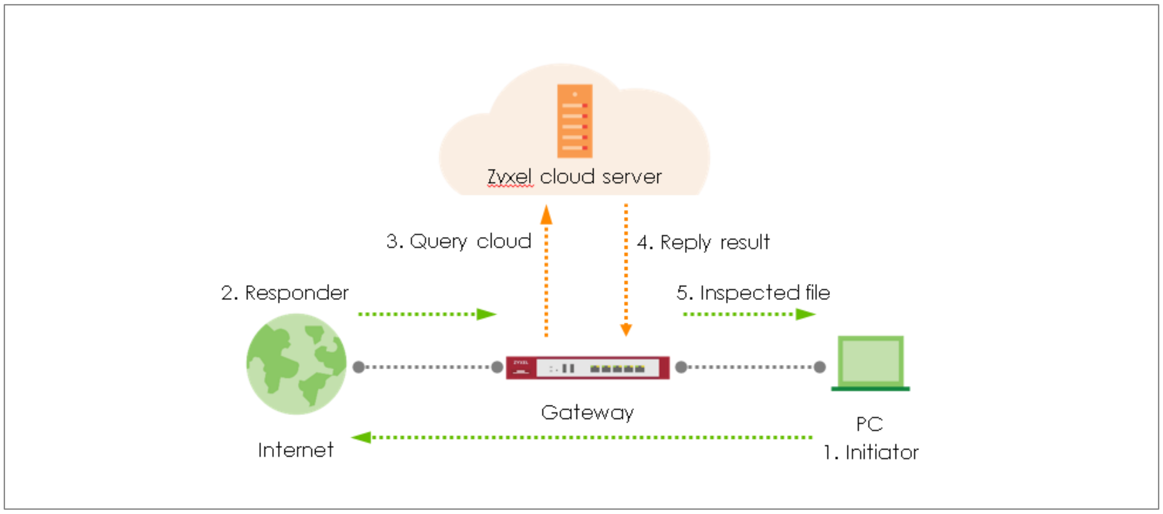


Category: Application Patrol

#	Time	Category	Message	Source	Destination	Note
6	2023-05-29 20:15:51	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.168.34	35.186.224.25	ACCESS BLOCK
7	2023-05-29 20:15:51	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.168.34	35.186.224.25	ACCESS BLOCK
8	2023-05-29 20:15:51	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.168.34	35.186.224.25	ACCESS BLOCK
9	2023-05-29 20:15:51	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.168.34	35.186.224.25	ACCESS BLOCK
17	2023-05-29 20:15:46	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.168.34	35.186.224.25	ACCESS BLOCK
18	2023-05-29 20:15:46	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.168.34	35.186.224.25	ACCESS BLOCK
19	2023-05-29 20:15:46	app-patrol	Rule_name:LAN_Outgoing App:[Audio/Video]spotify SID:3499 6224	192.168.168.34	35.186.224.25	ACCESS BLOCK

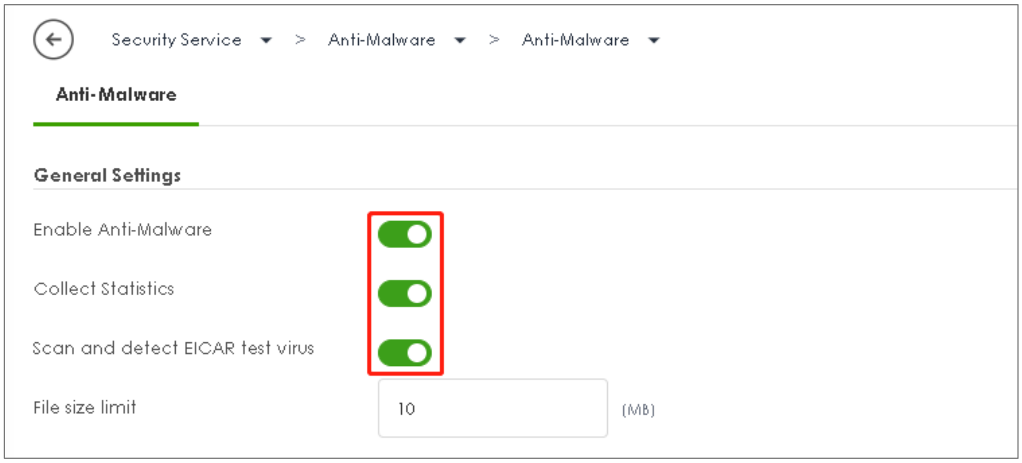
How does Anti-Malware Work

There are many viruses 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.



Enable Anti-Malware function to protecting your traffic

Go to Security Service > Anti-Malware. Turn on this feature. Select Collect Statistics and Scan and detect EICAR test virus.



Security Service > Anti-Malware > Anti-Malware

Anti-Malware

General Settings

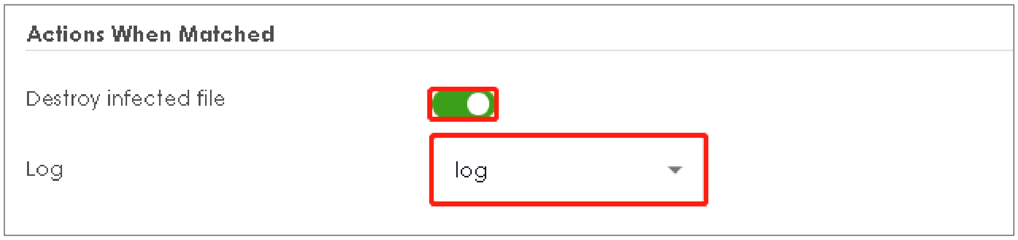
Enable Anti-Malware: on

Collect Statistics: on

Scan and detect EICAR test virus: on

File size limit: 10 (MB)

Select Destroy infected file and log in Actions When Matched



Actions When Matched

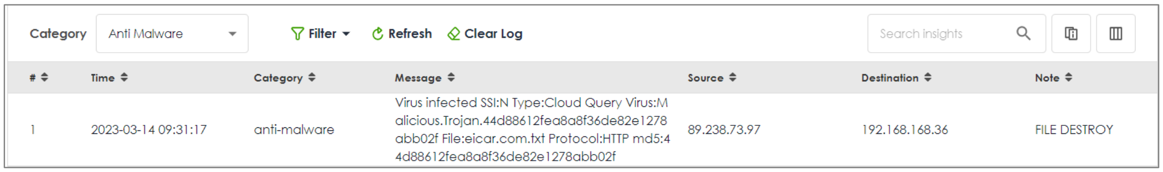
Destroy infected file: on

Log: log

Test the Result

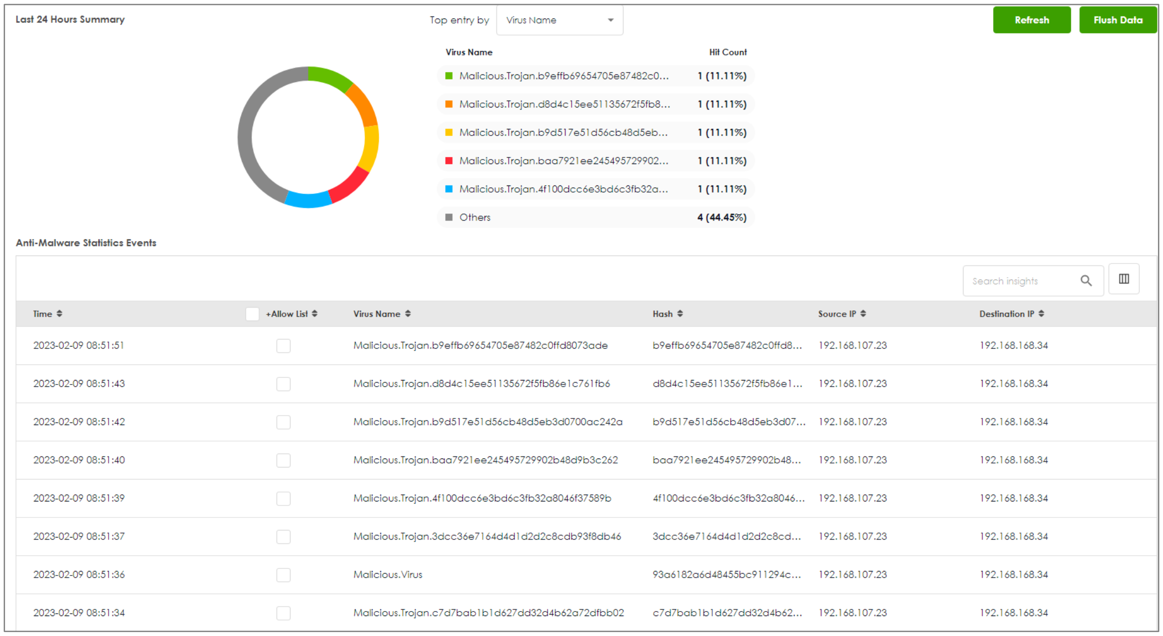
Download EIACR file from a LAN host to verify if Anti-malware works for detection.

Go to Log & Report > Log/Events and select Anti Malware to check the logs.



#	Time	Category	Message	Source	Destination	Note
1	2023-03-14 09:31:17	anti-malware	Virus infected SSI:N Type:Cloud Query Virus:Malicious.Trojan.44d88612fea8a8f36de82e1278abb02f File:eicar.com.txt Protocol:HTTP md5:44d88612fea8a8f36de82e1278abb02f	89.238.73.97	192.168.168.36	FILE DESTROY

Go to Security Statistics > Anti-Malware to check summary of all events.



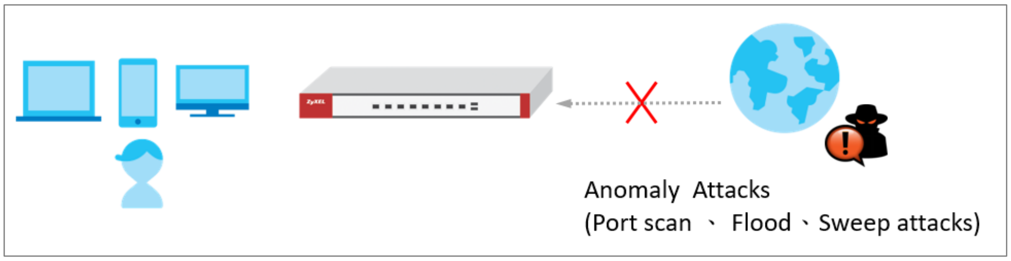
Virus Name	Hit Count
🟩 Malicious.Trojan.b9effb69654705e87482c0...	1 (11.11%)
🟧 Malicious.Trojan.d8d4c15ee51135672f5fb8...	1 (11.11%)
🟨 Malicious.Trojan.b9d517e51d56cb48d5eb...	1 (11.11%)
🟥 Malicious.Trojan.baa7921ee245495729902...	1 (11.11%)
🟦 Malicious.Trojan.4f100dcc6e3bd6c3fb32a...	1 (11.11%)
⬛ Others	4 (44.45%)

Anti-Malware Statistics Events

Time	□ +Allow List	Virus Name	Hash	Source IP	Destination IP
2023-02-09 08:51:51	□	Malicious.Trojan.b9effb69654705e87482c0ffd8073ade	b9effb69654705e87482c0ffd8...	192.168.107.23	192.168.168.34
2023-02-09 08:51:43	□	Malicious.Trojan.d8d4c15ee51135672f5fb86e1c761fb6	d8d4c15ee51135672f5fb86e1...	192.168.107.23	192.168.168.34
2023-02-09 08:51:42	□	Malicious.Trojan.b9d517e51d56cb48d5eb3d0700ac242a	b9d517e51d56cb48d5eb3d07...	192.168.107.23	192.168.168.34
2023-02-09 08:51:40	□	Malicious.Trojan.baa7921ee245495729902b48d9b3c262	baa7921ee245495729902b48...	192.168.107.23	192.168.168.34
2023-02-09 08:51:39	□	Malicious.Trojan.4f100dcc6e3bd6c3fb32a8046f37589b	4f100dcc6e3bd6c3fb32a8046...	192.168.107.23	192.168.168.34
2023-02-09 08:51:37	□	Malicious.Trojan.3dcc36e7164d4d1d2d2c8cdb93f8db46	3dcc36e7164d4d1d2d2c8cd...	192.168.107.23	192.168.168.34
2023-02-09 08:51:36	□	Malicious.Virus	93a6182a6d48455bc911294c...	192.168.107.23	192.168.168.34
2023-02-09 08:51:34	□	Malicious.Trojan.c7d7bab1b1d627dd32d4b62a72dfbb02	c7d7bab1b1d627dd32d4b62...	192.168.107.23	192.168.168.34

How to Detect and Prevent TCP Port Scanning with DoS Prevention

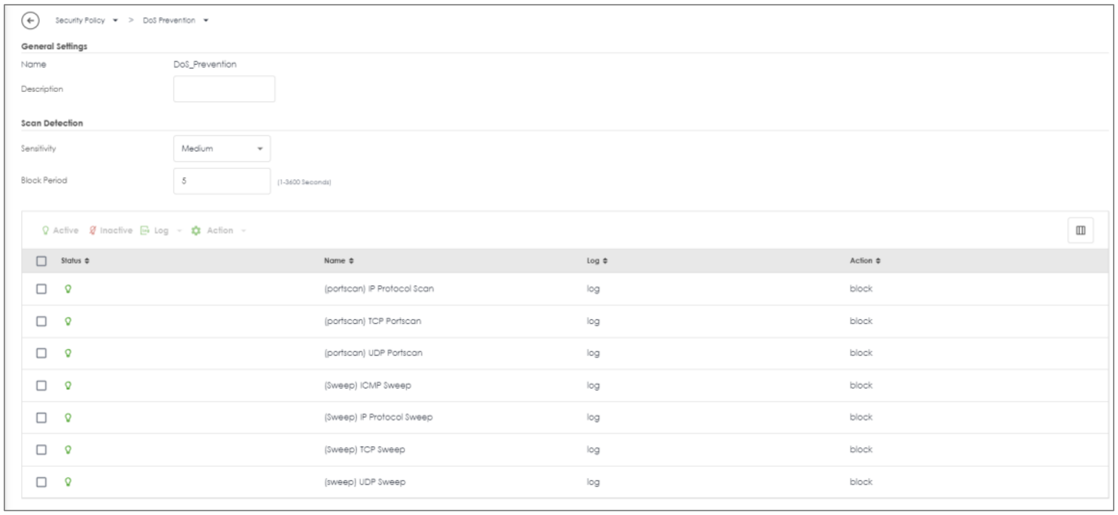
This is an example of using a USG Flex H DoS Prevention Profile to protect against anomalies based on violations of protocol standards (RFCs Requests for Comments) and abnormal traffic flows such as port scans.



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 500H (Firmware Version: uOS 1.10).

Set Up the DoS Prevention

In the USG Flex H, go to **Security Policy > Dos Prevention > Add a profile**. Configure a **Name** for you to identify the **profile** such as "DoS_Prevention". Configure the **Scan Detection** and **Flood Detection** to block when the Dos prevention events were detected.



General Settings

Name: DoS_Prevention

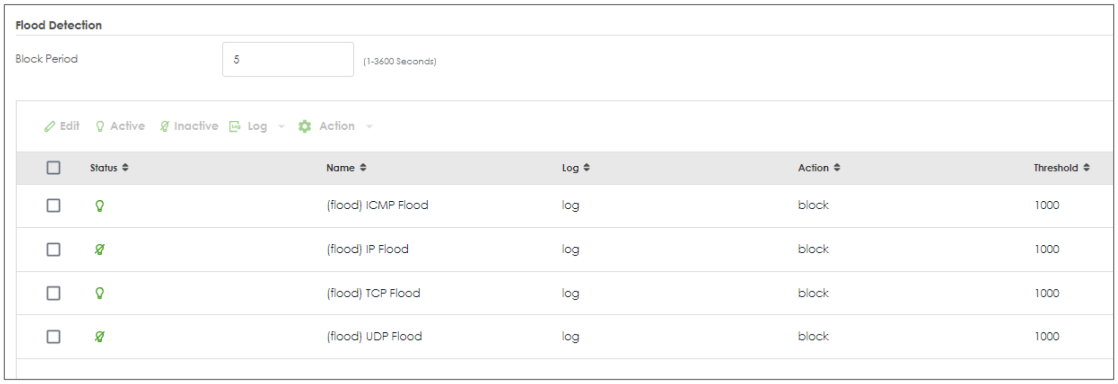
Description:

Scan Detection

Sensitivity: Medium

Block Period: 5 (1-3600 Seconds)

□	Status	Name	Log	Action
□	✓	(portscan) IP Protocol Scan	log	block
□	✓	(portscan) TCP Portscan	log	block
□	✓	(portscan) UDP Portscan	log	block
□	✓	(Sweep) ICMP Sweep	log	block
□	✓	(Sweep) IP Protocol Sweep	log	block
□	✓	(Sweep) TCP Sweep	log	block
□	✓	(sweep) UDP Sweep	log	block



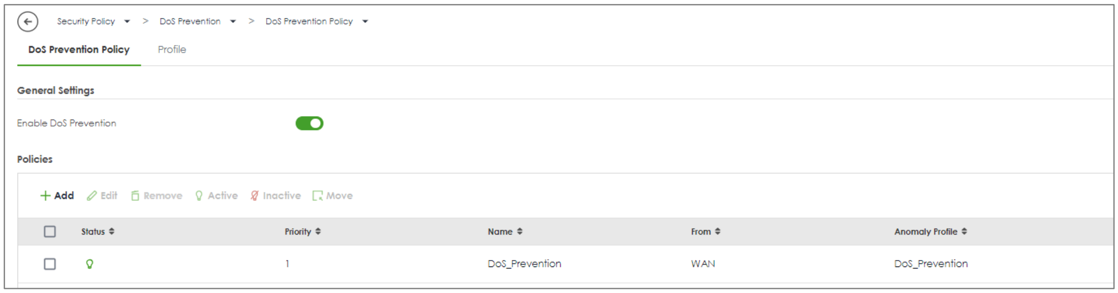
Flood Detection

Block Period: 5 (1-3600 Seconds)

□	Status	Name	Log	Action	Threshold
□	✓	(flood) ICMP Flood	log	block	1000
□	✗	(flood) IP Flood	log	block	1000
□	✓	(flood) TCP Flood	log	block	1000
□	✗	(flood) UDP Flood	log	block	1000

Set Up the DoS Prevention Policy

In the USG Flex H, go to **Security Policy > Dos Prevention > DoS Prevention Policy** Configure a **Name** for you to identify the **policy** such as "DoS_Prevention". Configure the **From** and **Anomaly Profile** to block when the DoS prevention events were detected.


Security Policy ▾ > DoS Prevention ▾ > DoS Prevention Policy ▾
DoS Prevention Policy
Profile
+ Add
Edit
Remove
Active
Inactive
Move

General Settings

Enable DoS Prevention ●

Policies

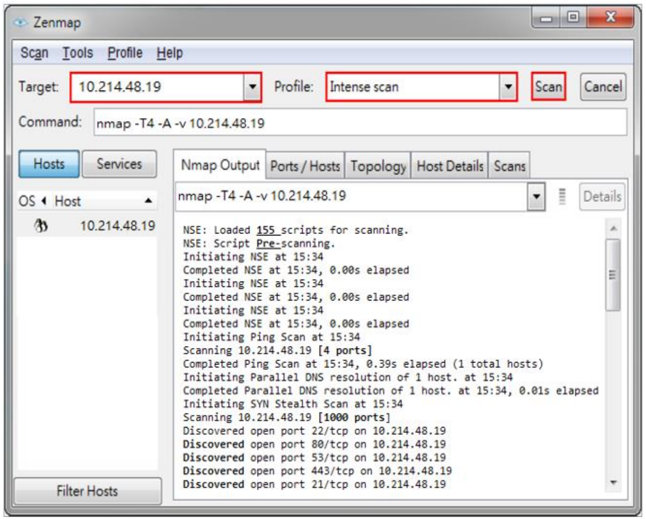
□	Status	Priority	Name	From	Anomaly Profile
□	💡	1	DoS_Prevention	WAN	DoS_Prevention

Test the Result

Using the port scan tool Nmap or hping3 to scan the wan interface.

For example, using Nmap security scanner for testing the result:

Open the Nmap GUI, set the Target to be the WAN IP of USG Flex H (10.214.48.19 in this example) and set Profile to be Intense Scan and click Scan.



Target: 10.214.48.19

Profile: Intense scan

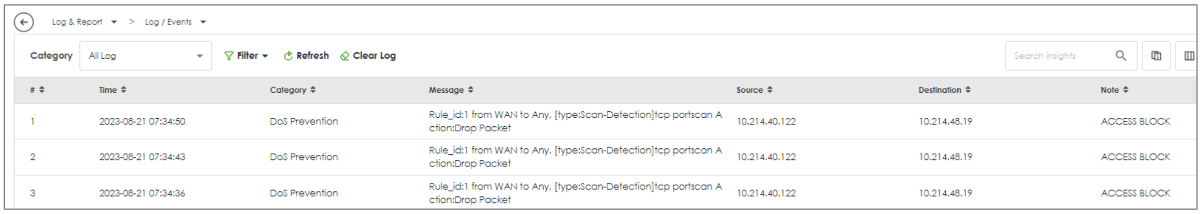
Command: nmap -T4 -A -v 10.214.48.19

Host: 10.214.48.19

```
nmap -T4 -A -v 10.214.48.19
```

```
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Initiating NSE at 15:34
Completed NSE at 15:34, 0.00s elapsed
Initiating Ping Scan at 15:34
Scanning 10.214.48.19 [4 ports]
Completed Ping Scan at 15:34, 0.39s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:34
Completed Parallel DNS resolution of 1 host. at 15:34, 0.01s elapsed
Initiating SYN Stealth Scan at 15:34
Scanning 10.214.48.19 [1000 ports]
Discovered open port 22/tcp on 10.214.48.19
Discovered open port 80/tcp on 10.214.48.19
Discovered open port 53/tcp on 10.214.48.19
Discovered open port 443/tcp on 10.214.48.19
Discovered open port 21/tcp on 10.214.48.19
```

Navigate to **Log & Report > Log / Events**, you will see log of blocked messages.



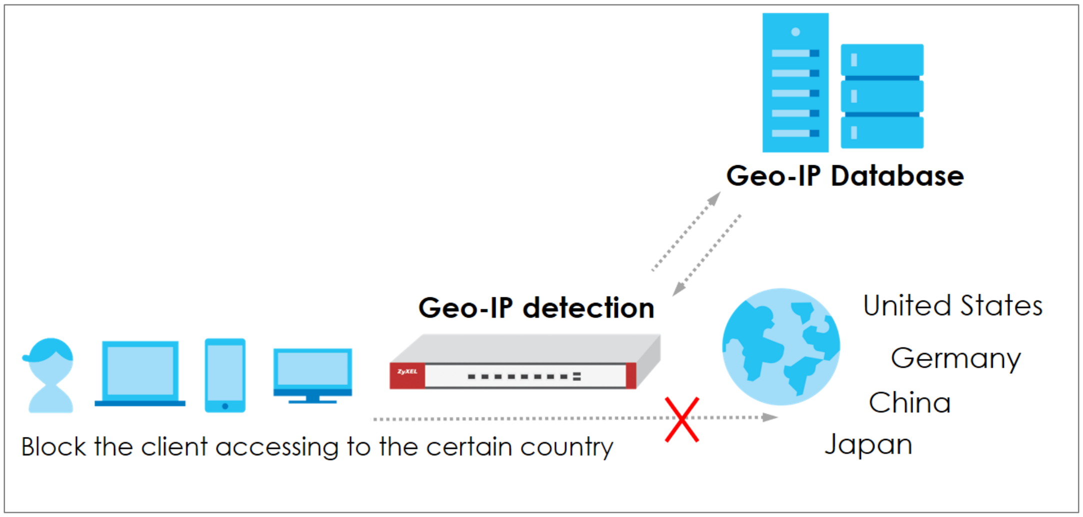
Category: All Log

#	Time	Category	Message	Source	Destination	Note
1	2023-08-21 07:34:50	DoS Prevention	Rule_id:1 from WAN to Any, [type:Scan-Detection]tcp portscan Action:Drop Packet	10.214.40.122	10.214.48.19	ACCESS BLOCK
2	2023-08-21 07:34:43	DoS Prevention	Rule_id:1 from WAN to Any, [type:Scan-Detection]tcp portscan Action:Drop Packet	10.214.40.122	10.214.48.19	ACCESS BLOCK
3	2023-08-21 07:34:36	DoS Prevention	Rule_id:1 from WAN to Any, [type:Scan-Detection]tcp portscan Action:Drop Packet	10.214.40.122	10.214.48.19	ACCESS BLOCK

How to block the client from accessing to certain country using Geo IP?

The Geo IP offers to identify the country-based IP addresses; it allows you to block the client from accessing a certain country based on the security policy.

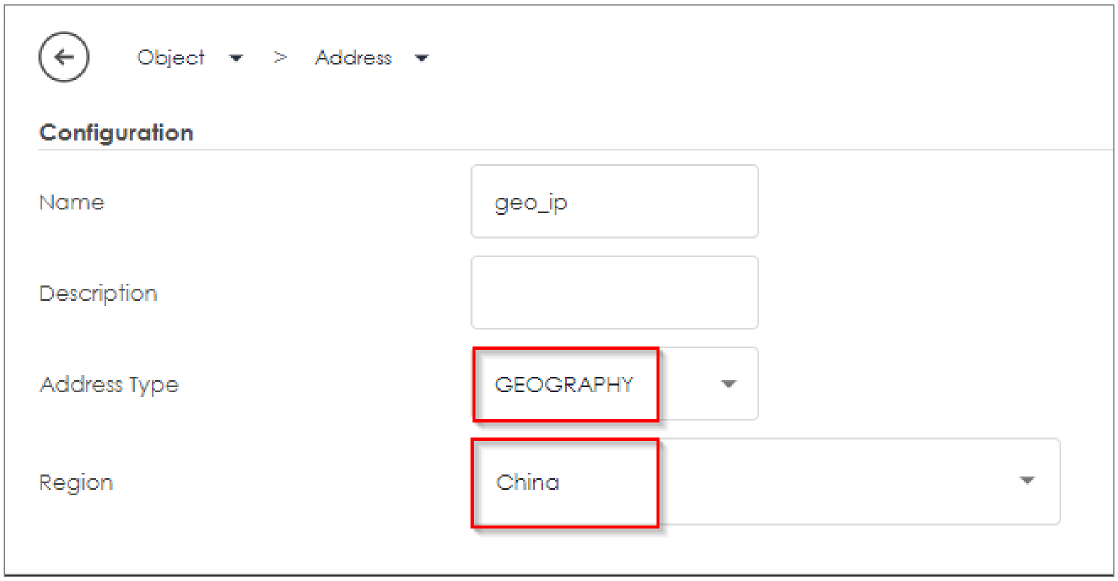
When the user makes HTTP or HTTPS request, USG Flex H queries the IP address from the cloud database, then takes action when it matches the block country in the security policy.



💡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 500H (Firmware Version: uOS 1.10)

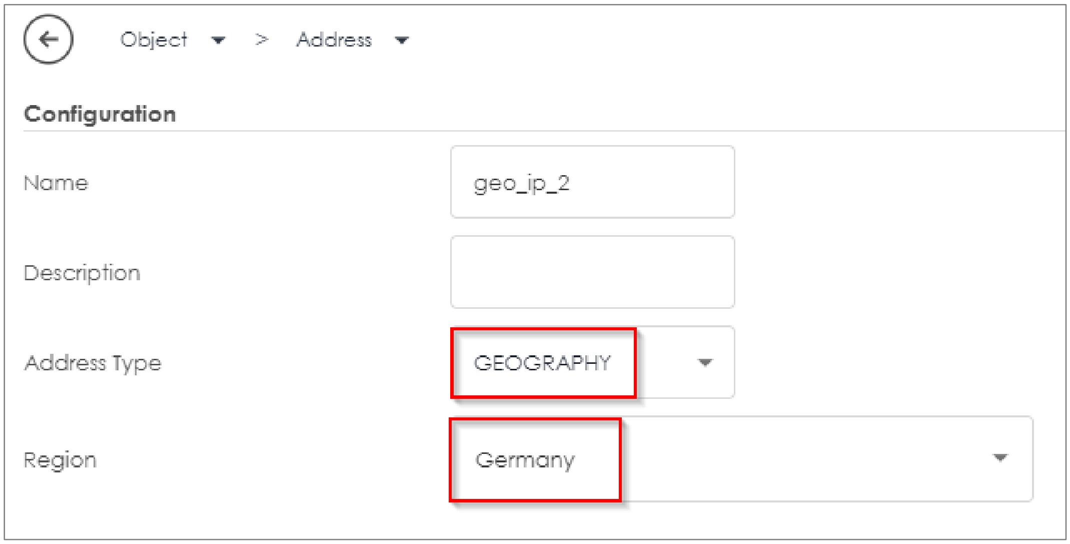
Set Up the Address Objet with Geo IP

Navigate to **Object > Address > Geo IP > Add geo IP related objects.**



Configuration

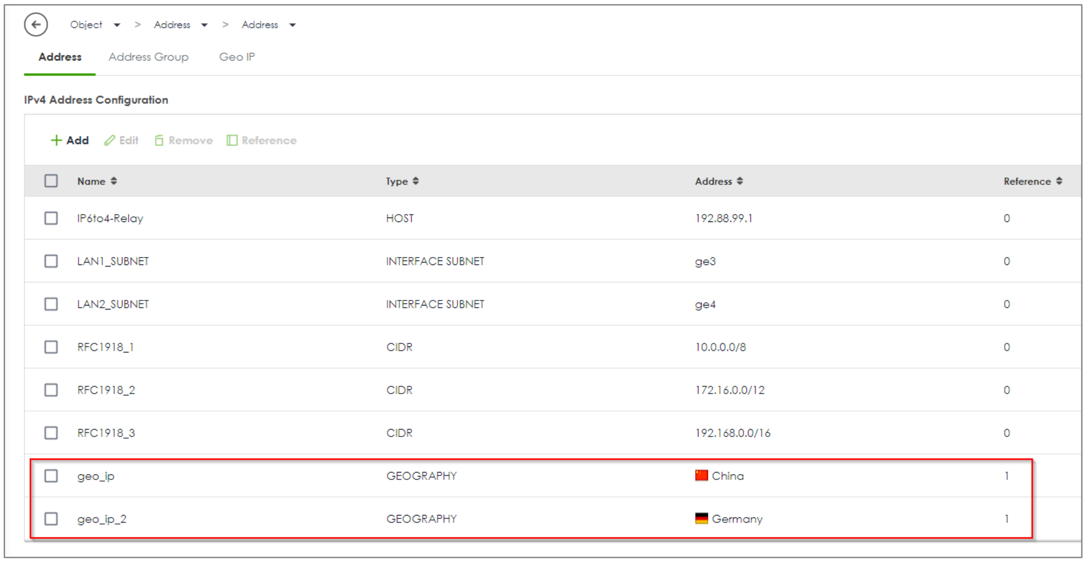
Name	geo_ip
Description	
Address Type	GEOGRAPHY
Region	China



Configuration

Name	geo_ip_2
Description	
Address Type	GEOGRAPHY
Region	Germany

Navigate to **Object > Address > Address**, you can see the customized GEOGRAPHY address object.



Object > Address > Address

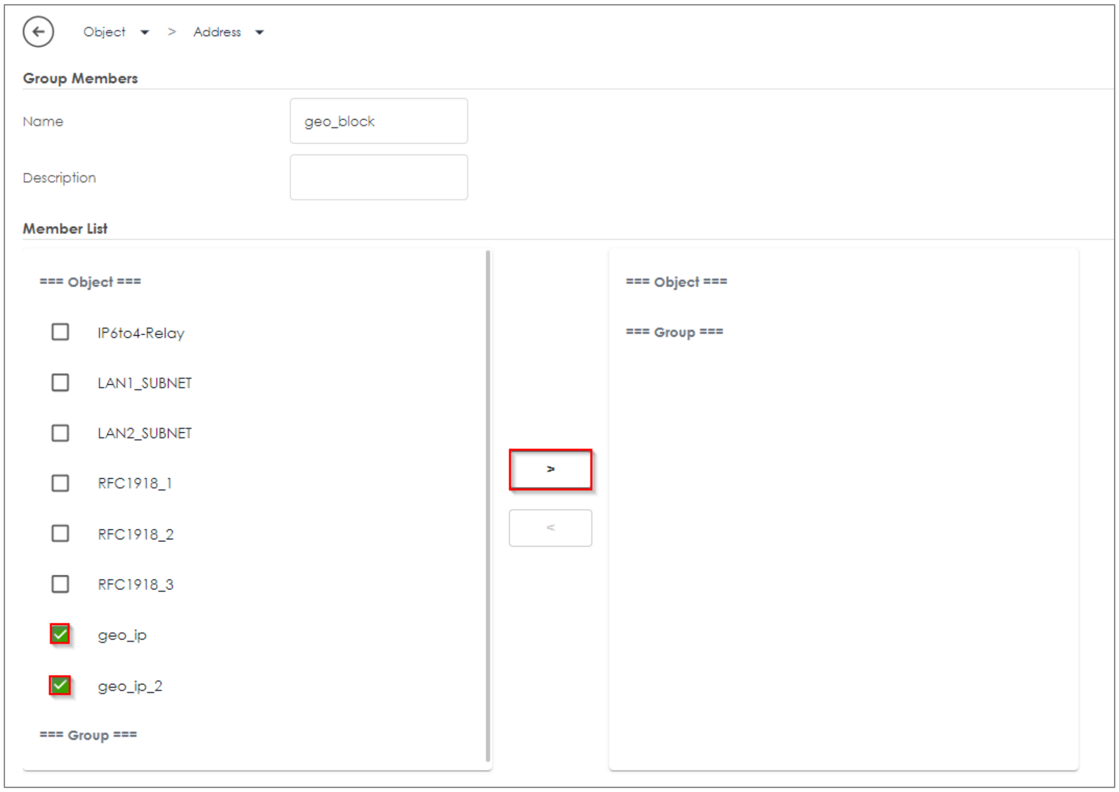
Address | Address Group | Geo IP

IPv4 Address Configuration

+ Add | Edit | Remove | Reference

□	Name	Type	Address	Reference
□	IP6to4-Relay	HOST	192.88.99.1	0
□	LAN1_SUBNET	INTERFACE SUBNET	ge3	0
□	LAN2_SUBNET	INTERFACE SUBNET	ge4	0
□	RFC1918_1	CIDR	10.0.0.0/8	0
□	RFC1918_2	CIDR	172.16.0.0/12	0
□	RFC1918_3	CIDR	192.168.0.0/16	0
□	geo_ip	GEOGRAPHY	China	1
□	geo_ip_2	GEOGRAPHY	Germany	1

Go to **Object > Address > Address Group> Add Address Group Rule**, add all customized GEOGRAPHY addresses into the same **Member** object.



Object > Address

Group Members

Name: geo_block

Description:

Member List

=== Object ===
- □ IP6to4-Relay
- □ LAN1_SUBNET
- □ LAN2_SUBNET
- □ RFC1918_1
- □ RFC1918_2
- □ RFC1918_3
- ☑ geo_ip
- ☑ geo_ip_2

=== Group ===

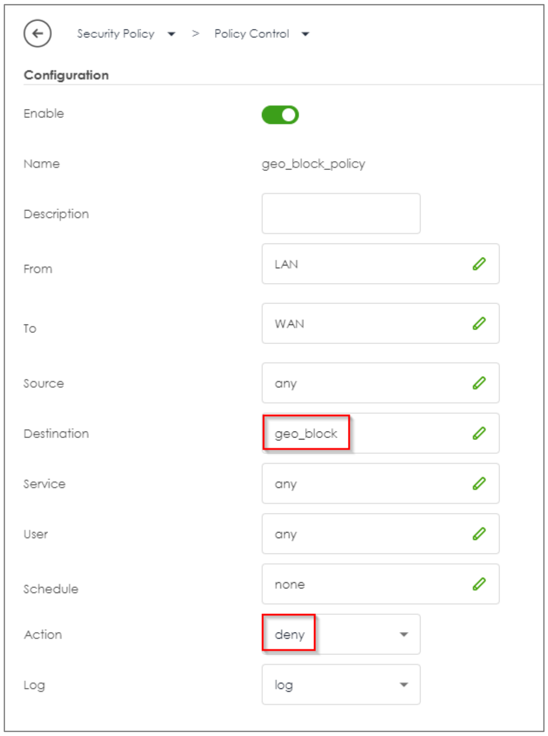
> | <

=== Object ===

=== Group ===

Set Up the Security Policy

Go to **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).

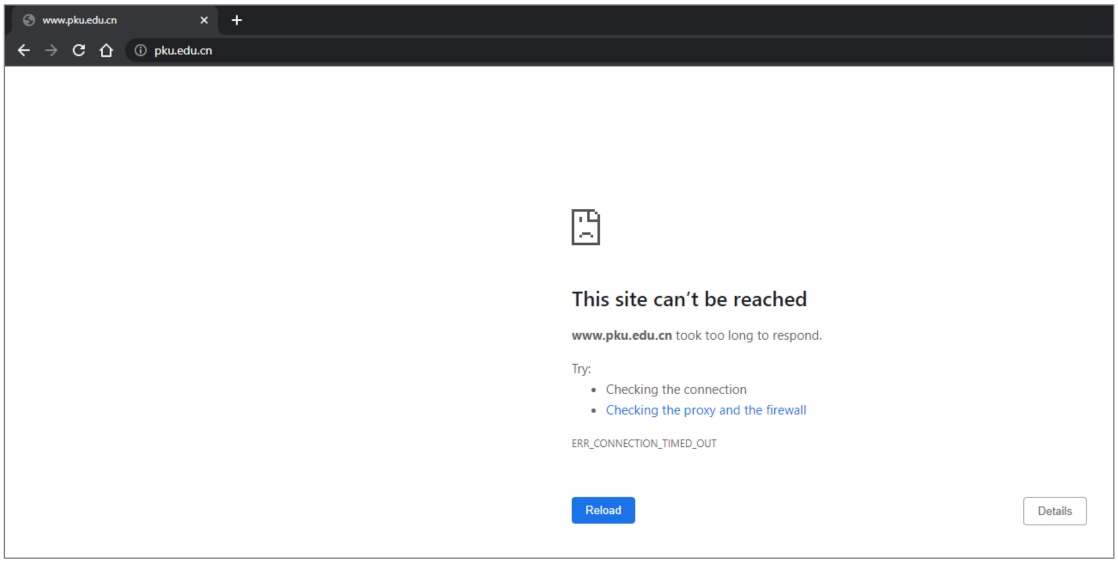


Configuration

Enable	●
Name	geo_block_policy
Description	
From	LAN
To	WAN
Source	any
Destination	geo_block
Service	any
User	any
Schedule	none
Action	deny
Log	log

Test the Result

When the LAN PC tries to access a website that matches the blocked geographical location, it is unable to reach those sites.



This site can’t be reached

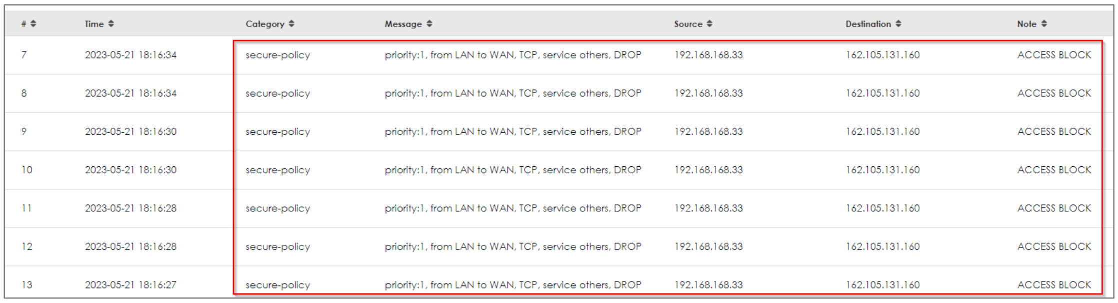
www.pku.edu.cn took too long to respond.

Try:

- Checking the connection
- Checking the proxy and the firewall

ERR_CONNECTION_TIMED_OUT

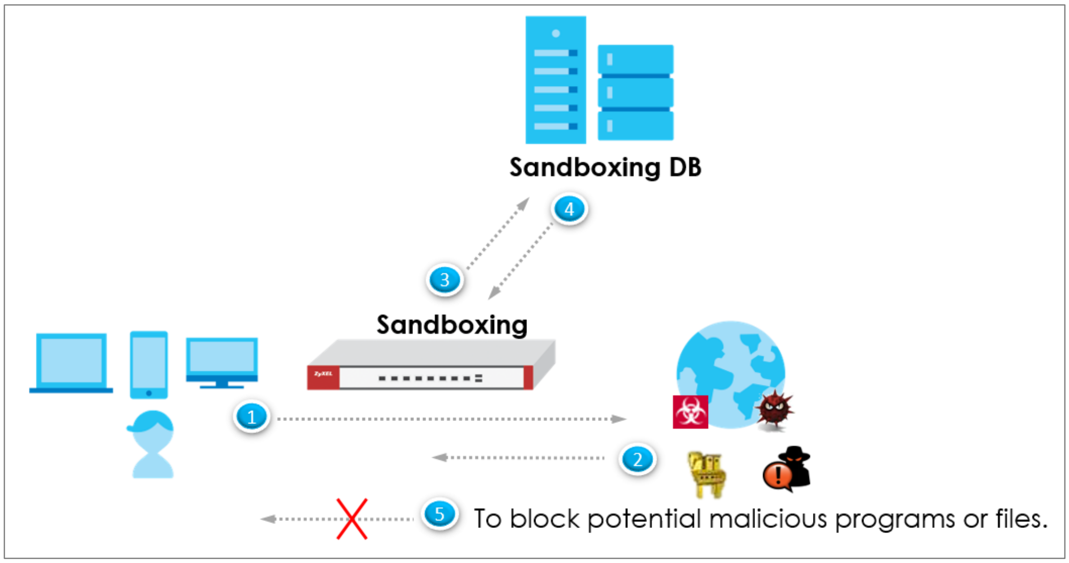
To view the log message, go to USG Flex H **Log & Report > Log / Events**. You will find log messages similar to the following. Any traffic that matches the Geo IP policy will be blocked, and the details will be displayed in the Message field.



#	Time	Category	Message	Source	Destination	Note
7	2023-05-21 18:16:34	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
8	2023-05-21 18:16:34	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
9	2023-05-21 18:16:30	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
10	2023-05-21 18:16:30	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
11	2023-05-21 18:16:28	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
12	2023-05-21 18:16:28	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK
13	2023-05-21 18:16:27	secure-policy	priority:1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	162.105.131.160	ACCESS BLOCK

How to Use Sandbox to Detect Unknown Malware?

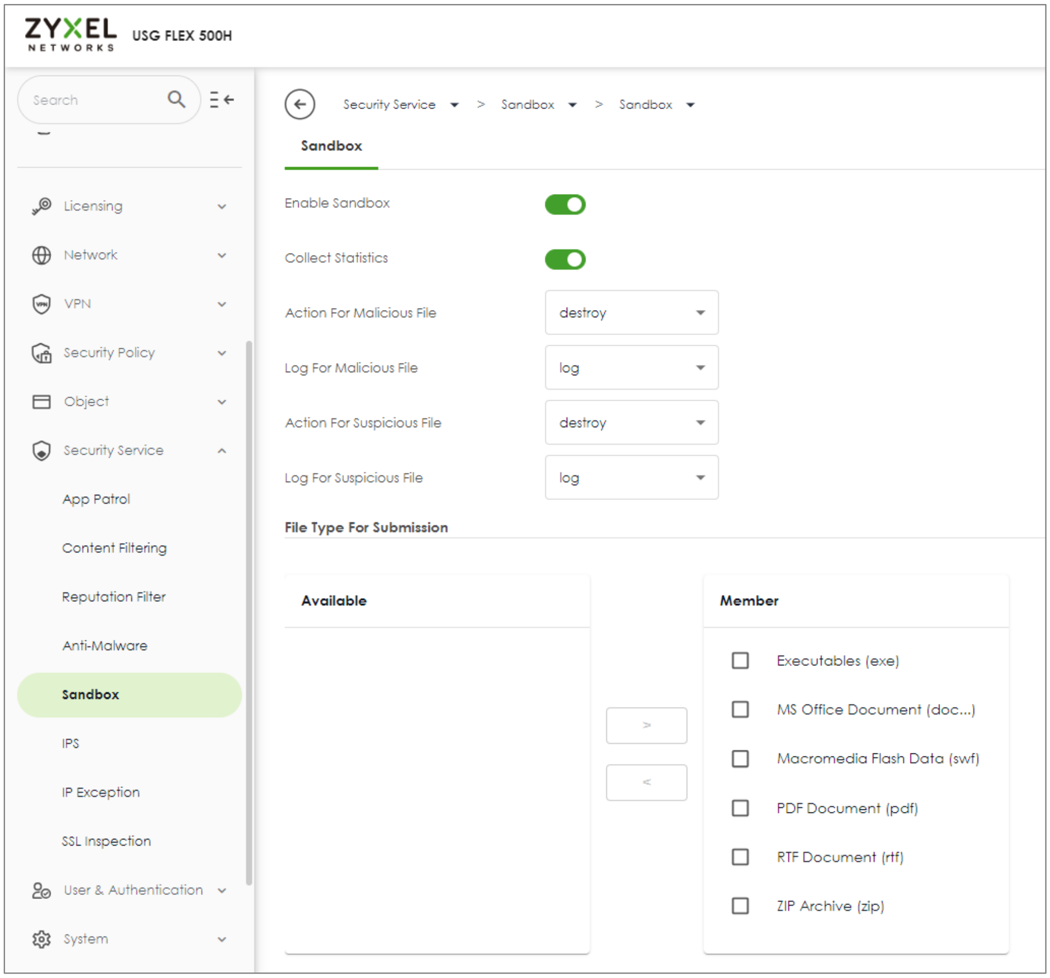
This is an example of using the USG Flex H to employ Sandboxing for detecting unknown malware. To achieve this goal, you can configure the Sandboxing profile within the security service path, and this article will guide you on its deployment.



> 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 500H (Firmware Version: uOS 1.10).

Set Up the Sandbox

Navigate to **Security Service > Sandbox**. Enable Sandbox option and choose the desired action when the Sandbox detects malicious and suspicious files. Additionally, select the desired file type for submission; currently, we support the following file types: Executables (exe), MS Office Document (doc...), Macromedia Flash Data (swf), PDF Document (pdf), RTF Document (rtf), and ZIP Archive (zip).



Enable Sandbox: On

Collect Statistics: On

Action For Malicious File: destroy

Log For Malicious File: log

Action For Suspicious File: destroy

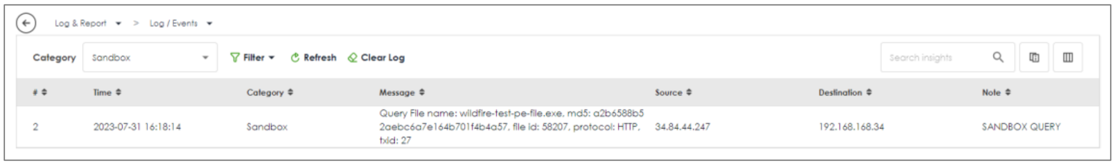
Log For Suspicious File: log

File Type For Submission

Available	Member
	□ Executables (exe)
	□ MS Office Document (doc...)
	□ Macromedia Flash Data (swf)
	□ PDF Document (pdf)
	□ RTF Document (rtf)
	□ ZIP Archive (zip)

Test the Result

When downloading the file, the firewall will query the Sandbox DB to detect whether it is a malicious or suspicious file. You can navigate to **Log & Report** > **Log/Events** to see the sandbox related logs.



#	Time	Category	Message	Source	Destination	Note
2	2023-07-31 16:18:14	Sandbox	Query File name: wildfire-test-pe-file.exe, md5: a2b6588b5 2aebc6a7e164b701f4b4a57, file id: 58207, protocol: HTTP, txid: 27	34.84.44.247	192.168.168.34	SANDBOX QUERY

How to Configure Reputation Filter- IP Reputation

As cyber threats such as scanners, botnets, phishing, etc. grow increasingly, how to identify suspect IP addresses of threats efficiently becomes a crucial task.

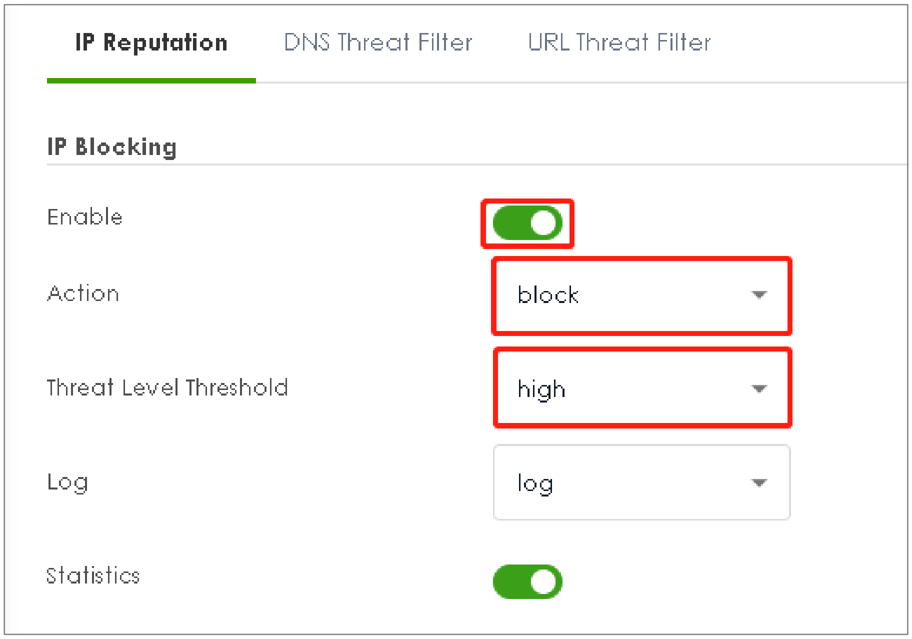
With regularly updated IP database, FLEX prevents threats by blocking connection to/from known IP addresses based on signature database. It filters source and destination addresses in your network traffic to take the proper risk prevention actions.

This example illustrates how to configure IP Reputation on FLEX gateway to detect cyber threats for both incoming and outgoing traffic.

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 200H (Firmware Version: uOS 1.10).

Set Up the IP reputation filter

Go to Security Service > Reputation Filter > IP reputation. Turn on this feature. Select Block on Action field. The threat level threshold is measured by the query score of IP signature database.



IP Blocking

Enable: ON

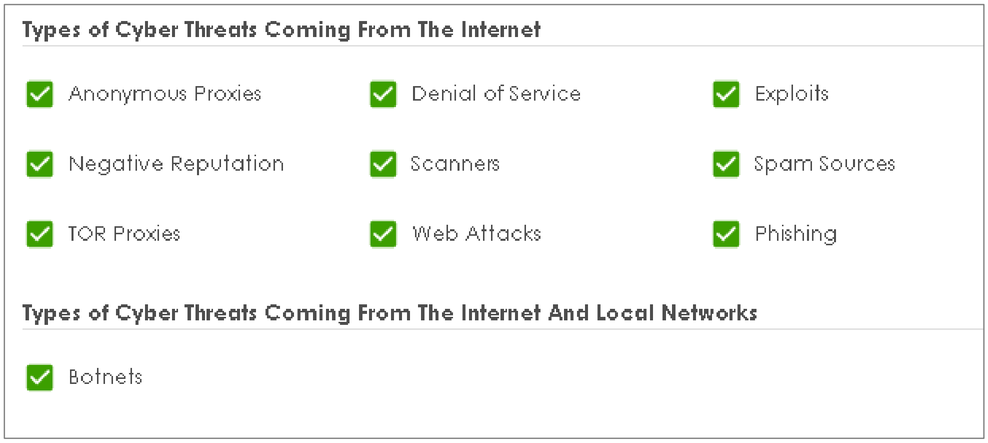
Action: block

Threat Level Threshold: high

Log: log

Statistics: ON

Select categories in Types of Cyber Threats Coming from the Internet, and Types of Cyber Threats Coming from The Internet and Local Networks.



Types of Cyber Threats Coming From The Internet

☑ Anonymous Proxies ☑ Denial of Service ☑ Exploits

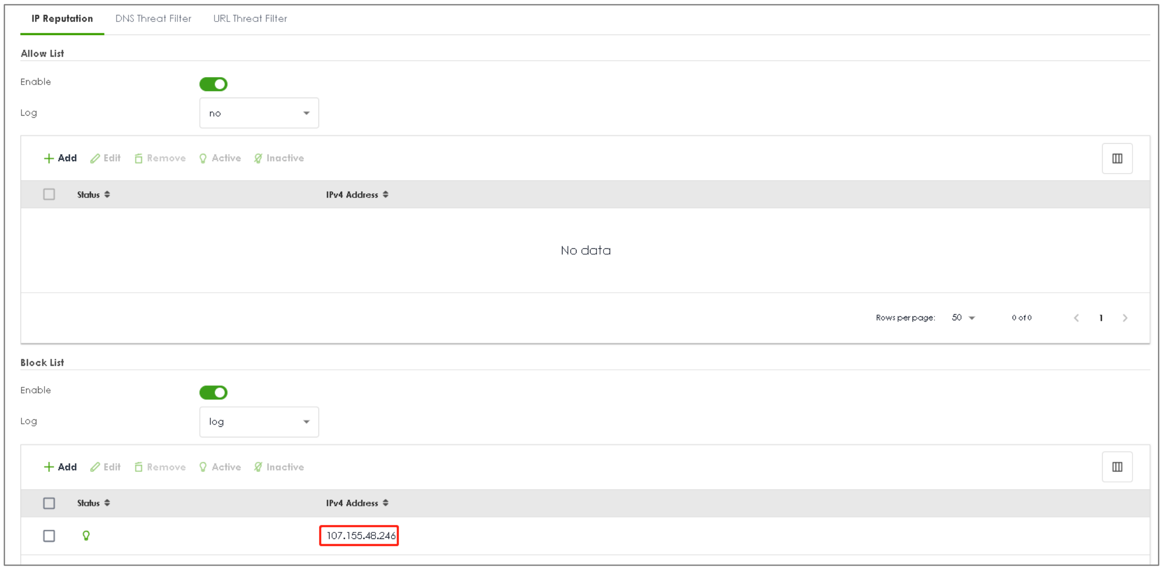
☑ Negative Reputation ☑ Scanners ☑ Spam Sources

☑ TOR Proxies ☑ Web Attacks ☑ Phishing

Types of Cyber Threats Coming From The Internet And Local Networks

☑ Botnets

Go to Security Service > Reputation Filter > IP reputation > White List and Black List to manually adding IP addresses to Black List.



Allow List

Enable

Log: no

☐	Status	IPv4 Address
	No data	

Rows per page: 50 0 of 0 1

Block List

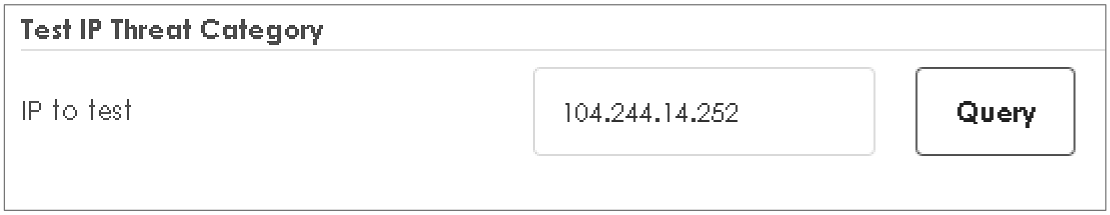
Enable

Log: log

☐	Status	IPv4 Address
☐		107.155.48.246

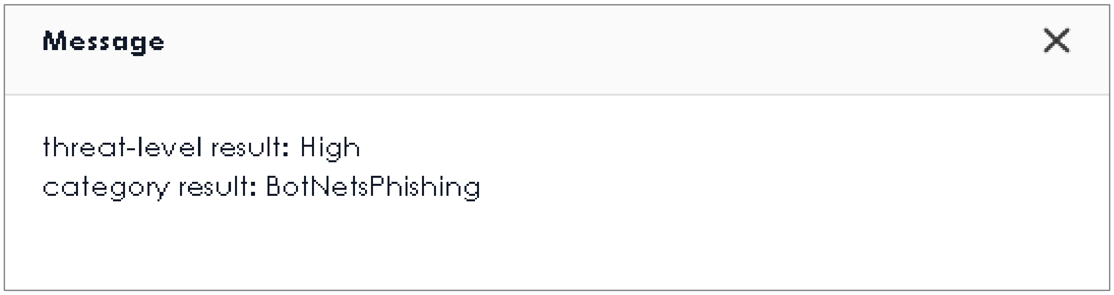
Test the Result

Verify an IP in Test IP Threat Category. In Test IP Threat Category, enter a malicious IP and query the result.



Test IP Threat Category

IP to test: 104.244.14.252

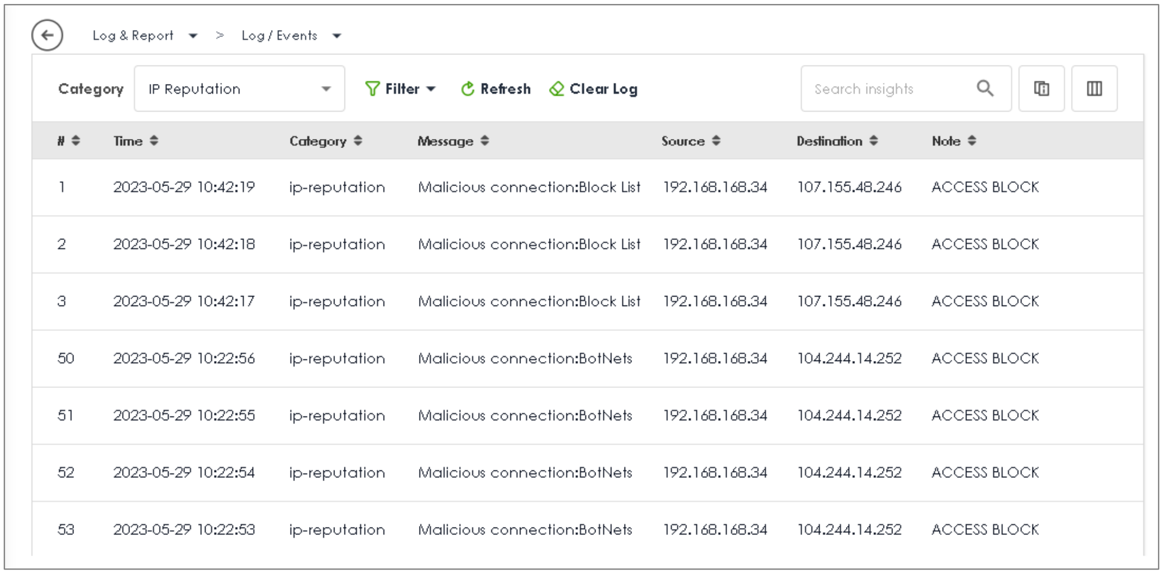


Message

threat-level result: High
category result: BotNetsPhishing

Try to generate ICMP packet from LAN to destination IP 107.155.48.246, and 104.244.14.252

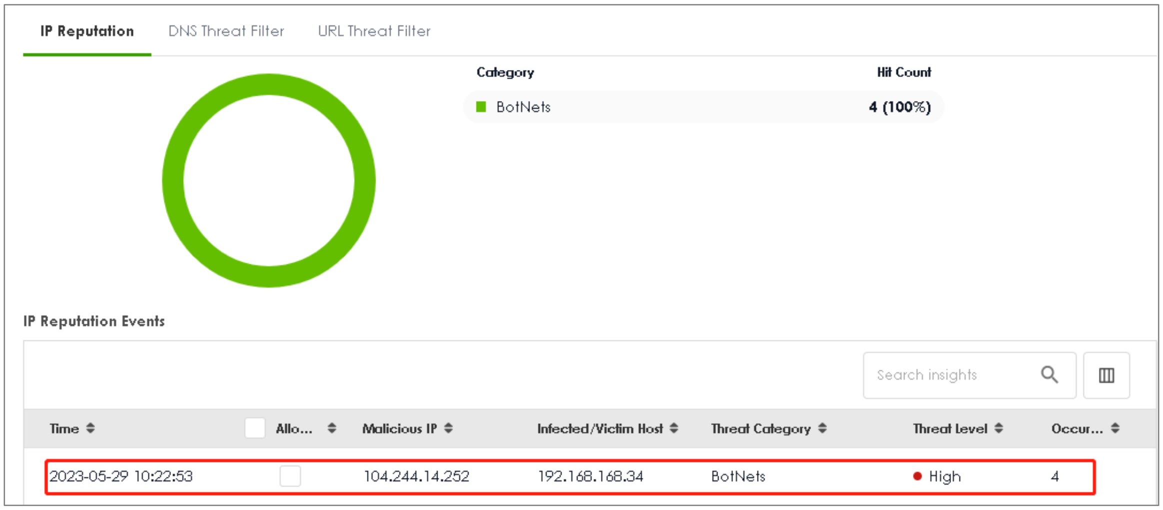
Go to Log & Report > Log/Events and select IP reputation Filter to check the logs.



Category: IP Reputation

#	Time	Category	Message	Source	Destination	Note
1	2023-05-29 10:42:19	ip-reputation	Malicious connection:Block List	192.168.168.34	107.155.48.246	ACCESS BLOCK
2	2023-05-29 10:42:18	ip-reputation	Malicious connection:Block List	192.168.168.34	107.155.48.246	ACCESS BLOCK
3	2023-05-29 10:42:17	ip-reputation	Malicious connection:Block List	192.168.168.34	107.155.48.246	ACCESS BLOCK
50	2023-05-29 10:22:56	ip-reputation	Malicious connection:BotNets	192.168.168.34	104.244.14.252	ACCESS BLOCK
51	2023-05-29 10:22:55	ip-reputation	Malicious connection:BotNets	192.168.168.34	104.244.14.252	ACCESS BLOCK
52	2023-05-29 10:22:54	ip-reputation	Malicious connection:BotNets	192.168.168.34	104.244.14.252	ACCESS BLOCK
53	2023-05-29 10:22:53	ip-reputation	Malicious connection:BotNets	192.168.168.34	104.244.14.252	ACCESS BLOCK

Go to Security Statistics > Reputation Filter > IP reputation to check summary of all events.



Category	Hit Count
🟩 BotNets	4 (100%)

IP Reputation Events

Time	□ Allo...	Malicious IP	Infected/Victim Host	Threat Category	Threat Level	Occur...
2023-05-29 10:22:53	□	104.244.14.252	192.168.168.34	BotNets	● High	4

How to Configure Reputation Filter- URL Threat Filter

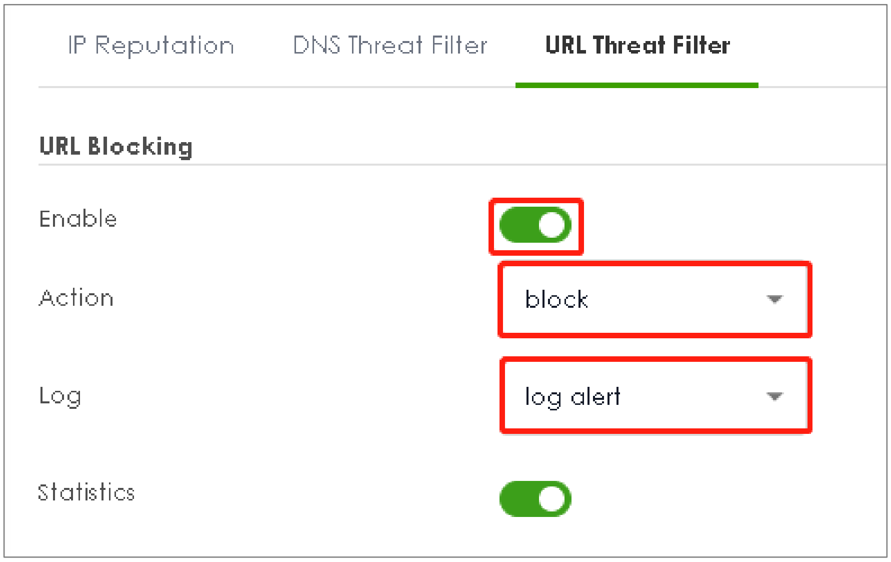
URL Threat Filter can avoid users to browse some malicious URLs (such as anonymizers, browser exploits, phishing sites, spam URLs, spyware) and allows administrator to manage which URLs can be browsed or not.

This example demonstrates how to configure the URL Threat Filter to redirect web access after the client hits the URL Threat Filter categories.

💡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 200H (Firmware Version: uOS 1.10).

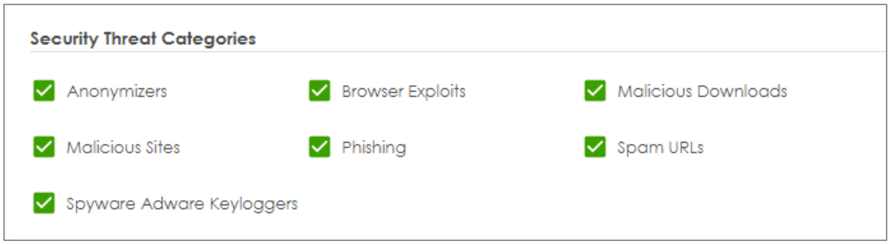
Set Up the URL Threat Filter

Go to Security Service > Reputation Filter > URL Threat Filter. Turn on this feature. Select Block on Action field. When a client hits URL Threat Filter, the page will be Blocked. Choose Log-alert on Log field.



URL Blocking

Enable	●
Action	block
Log	log alert
Statistics	●

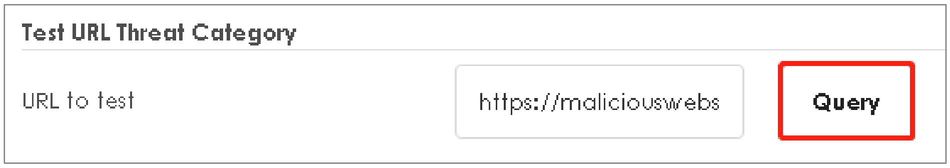


Security Threat Categories

☑ Anonymizers	☑ Browser Exploits	☑ Malicious Downloads
☑ Malicious Sites	☑ Phishing	☑ Spam URLs
☑ Spyware Adware Keyloggers		

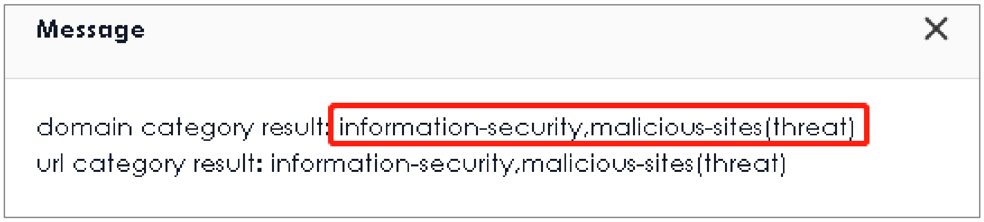
Test the Result

Verify a URL in the Security Threat Categories. In Test URL Threat Category, enter a malicious URL and query the result.



Test URL Threat Category

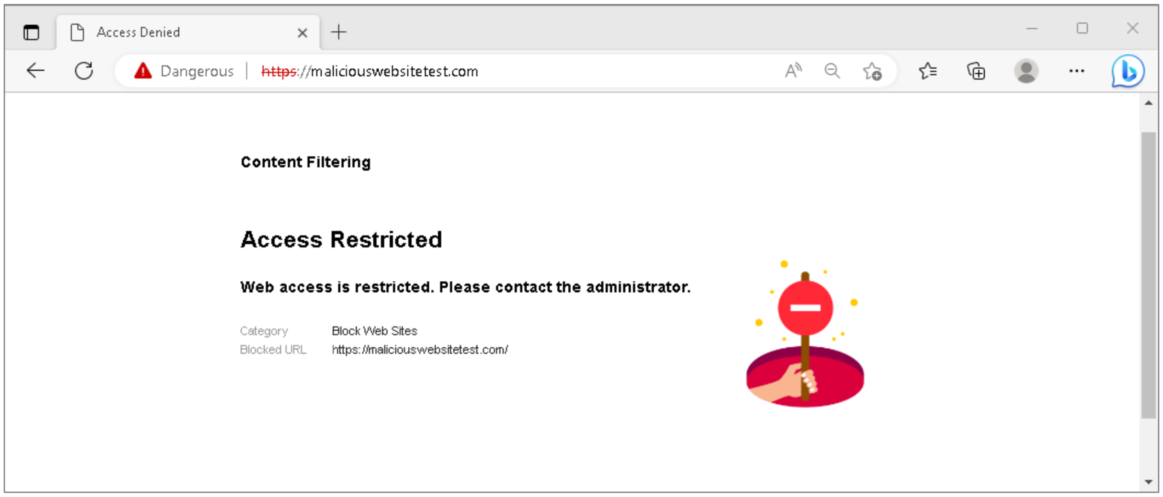
URL to test https://maliciouswebs



Message

domain category result: information-security,malicious-sites(threat)
url category result: information-security,malicious-sites(threat)

Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.



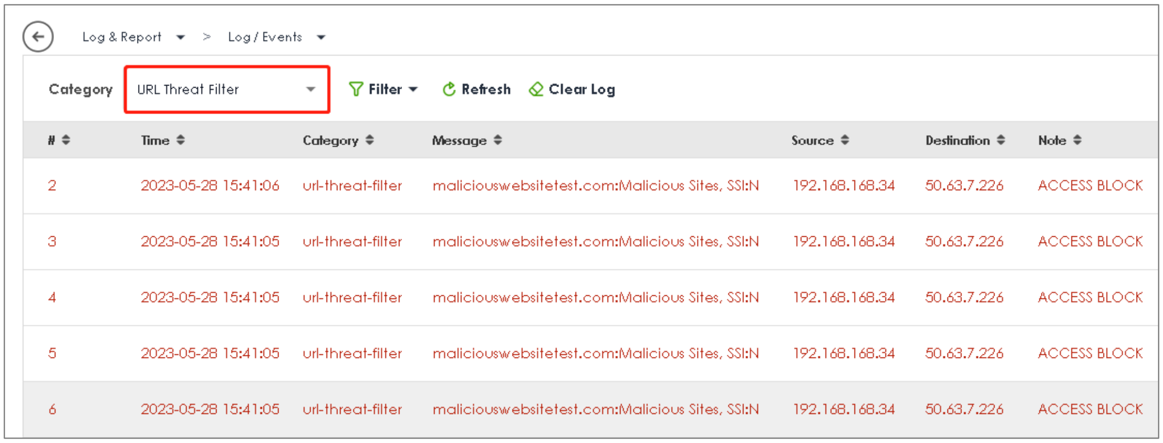
Content Filtering

Access Restricted

Web access is restricted. Please contact the administrator.

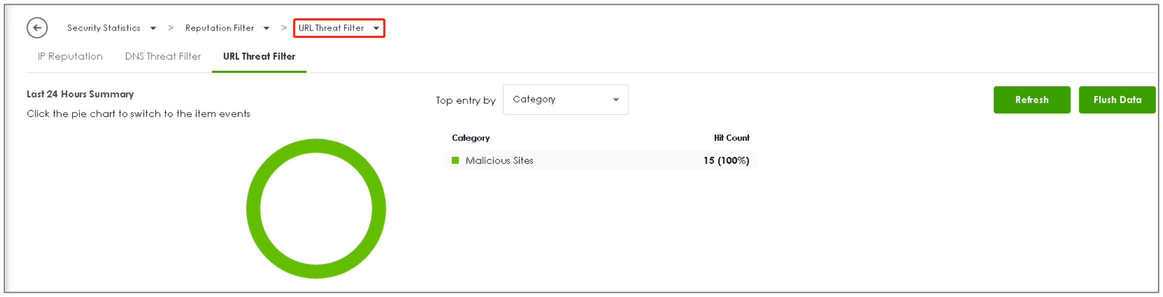
Category	Block Web Sites
Blocked URL	https://maliciouswebsitetest.com/

Go to Log & Report > Log/Events and select URL Threat Filter to check the logs.



#	Time	Category	Message	Source	Destination	Note
2	2023-05-28 15:41:06	url-threat-filter	maliciouswebsitetest.com:Malicious Sites, SSI:N	192.168.168.34	50.63.7.226	ACCESS BLOCK
3	2023-05-28 15:41:05	url-threat-filter	maliciouswebsitetest.com:Malicious Sites, SSI:N	192.168.168.34	50.63.7.226	ACCESS BLOCK
4	2023-05-28 15:41:05	url-threat-filter	maliciouswebsitetest.com:Malicious Sites, SSI:N	192.168.168.34	50.63.7.226	ACCESS BLOCK
5	2023-05-28 15:41:05	url-threat-filter	maliciouswebsitetest.com:Malicious Sites, SSI:N	192.168.168.34	50.63.7.226	ACCESS BLOCK
6	2023-05-28 15:41:05	url-threat-filter	maliciouswebsitetest.com:Malicious Sites, SSI:N	192.168.168.34	50.63.7.226	ACCESS BLOCK

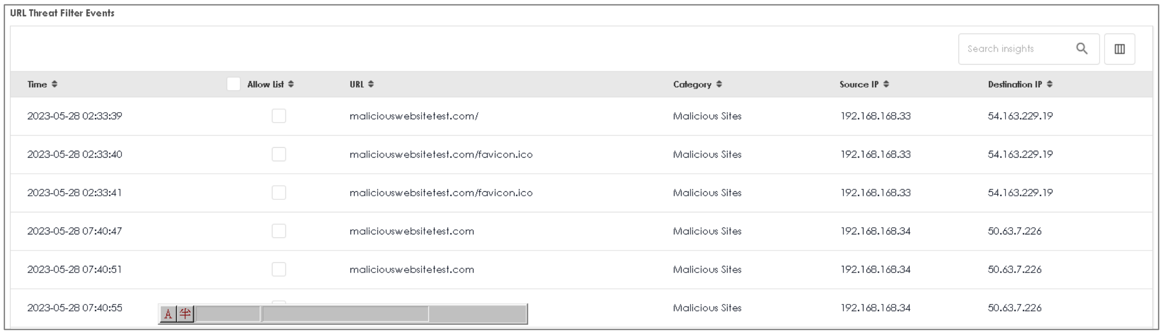
Go to Security Statistics > Reputation Filter > URL Threat Filter to check summary of all events.



Last 24 Hours Summary

Click the pie chart to switch to the item events

Category	Hit Count
🟩 Malicious Sites	15 (100%)



URL Threat Filter Events

Time	☐ Allow list	URL	Category	Source IP	Destination IP
2023-05-28 02:33:39	☐	maliciouswebsitetest.com/	Malicious Sites	192.168.168.33	54.163.229.19
2023-05-28 02:33:40	☐	maliciouswebsitetest.com/favicon.ico	Malicious Sites	192.168.168.33	54.163.229.19
2023-05-28 02:33:41	☐	maliciouswebsitetest.com/favicon.ico	Malicious Sites	192.168.168.33	54.163.229.19
2023-05-28 07:40:47	☐	maliciouswebsitetest.com	Malicious Sites	192.168.168.34	50.63.7.226
2023-05-28 07:40:51	☐	maliciouswebsitetest.com	Malicious Sites	192.168.168.34	50.63.7.226
2023-05-28 07:40:55			Malicious Sites	192.168.168.34	50.63.7.226

How to Configure Reputation Filter- DNS Threat Filter

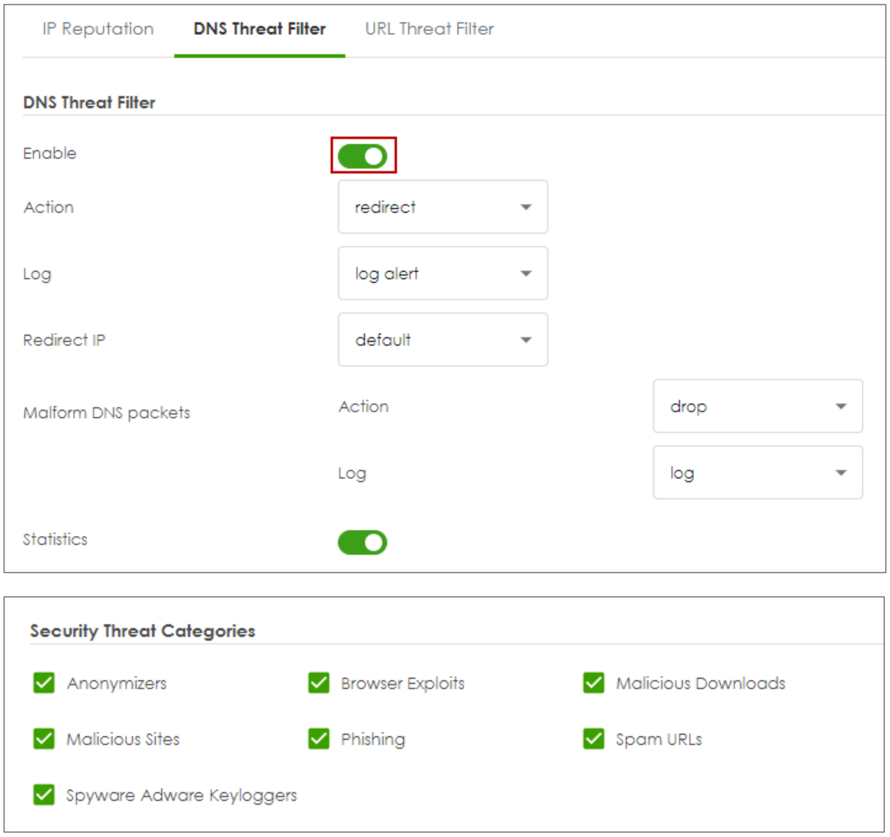
DNS Threat Filter is a mechanism aimed at protecting users by intercepting DNS request attempting to connect to known malicious or unwanted domains and returning a false, or rather controlled IP address. The controlled IP address points to a sinkhole server defined by the administrator.

When a client wants to access a malicious domain, the query is sent to the DNS server for getting the domain name details. All of the traffic now here gateway intercepts this query which is outgoing. The cloud server 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 shows how to configure DNS Threat Filter to redirect web access after client hit the filter profile.

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 200H (Firmware Version: uOS 1.10).

Set Up the DNS Threat Filter

Go to Security Service > Reputation Filter > DNS Threat Filter. Turn on this feature. Select Redirect on Action field. When a client hits DNS Threat Filter, the page will be redirected to the default blocked page or a custom IP address. Choose Log-alert on Log field. Configure Default on Redirect IP field to allow gateway redirect to the default blocked page.



DNS Threat Filter

Enable: ●

Action: redirect

Log: log alert

Redirect IP: default

Malform DNS packets: Action: drop; Log: log

Statistics: ●

Security Threat Categories

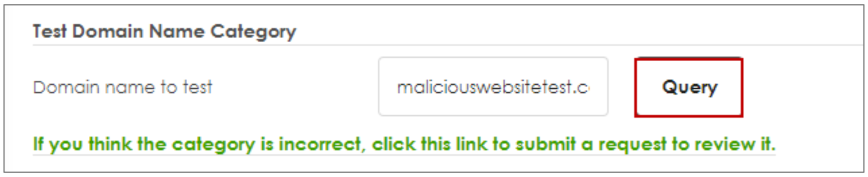
☑ Anonymizers ☑ Browser Exploits ☑ Malicious Downloads

☑ Malicious Sites ☑ Phishing ☑ Spam URLs

☑ Spyware Adware Keyloggers

Test the Result

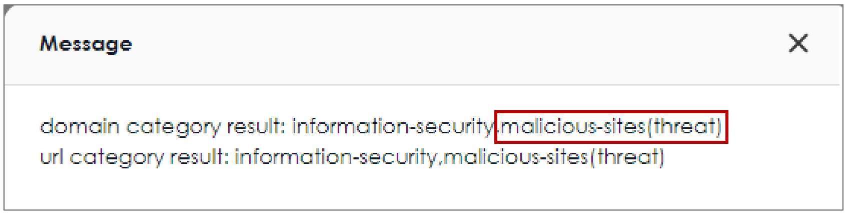
Verify a domain name in the Security Threat Categories. In Test Domain Name Category, enter a malicious domain and query the result.



Test Domain Name Category

Domain name to test: maliciouswebsitetest.c

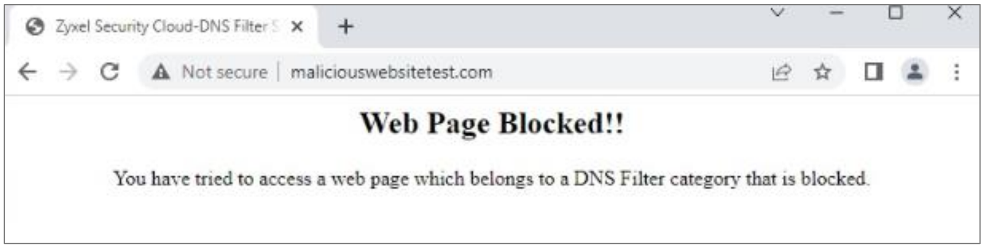
If you think the category is incorrect, click this link to submit a request to review it.



Message

domain category result: information-security,malicious-sites(threat)
url category result: information-security,malicious-sites(threat)

Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.

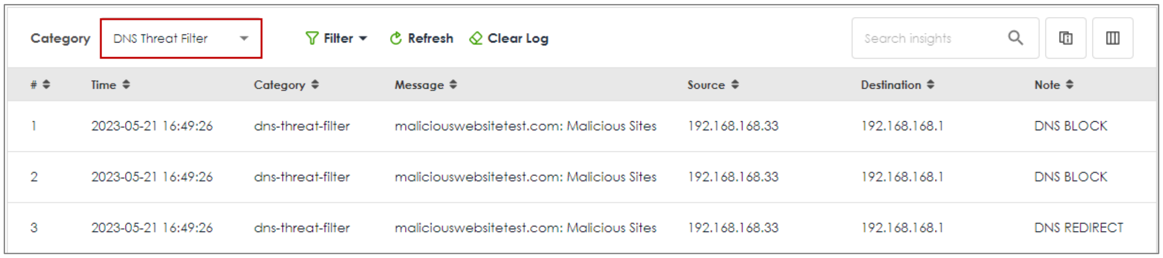


Zyxel Security Cloud-DNS Filter S
Not secure | maliciouswebsitetest.com

Web Page Blocked!!

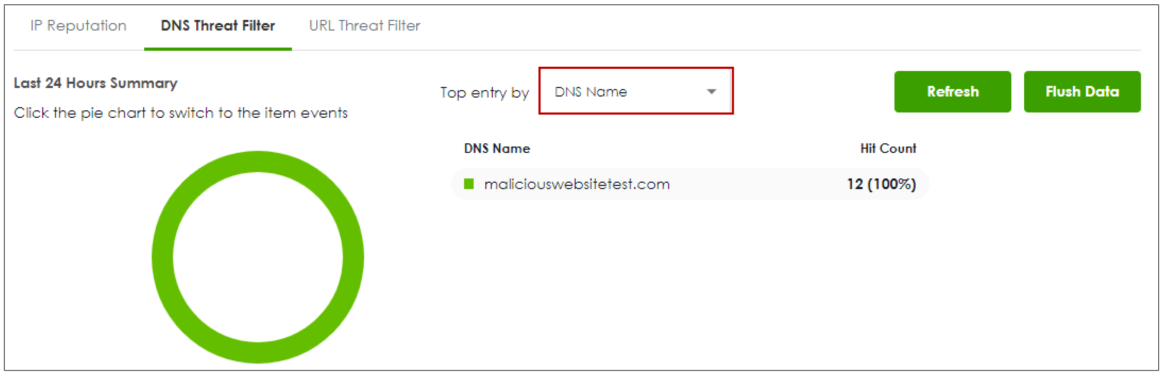
You have tried to access a web page which belongs to a DNS Filter category that is blocked.

Go to Log & Report > Log/Events and select DNS Threat Filter to check the logs.



#	Time	Category	Message	Source	Destination	Note
1	2023-05-21 16:49:26	dns-threat-filter	maliciouswebsitetest.com: Malicious Sites	192.168.168.33	192.168.168.1	DNS BLOCK
2	2023-05-21 16:49:26	dns-threat-filter	maliciouswebsitetest.com: Malicious Sites	192.168.168.33	192.168.168.1	DNS BLOCK
3	2023-05-21 16:49:26	dns-threat-filter	maliciouswebsitetest.com: Malicious Sites	192.168.168.33	192.168.168.1	DNS REDIRECT

Go to Security Statistics > Reputation Filter > DNS Threat Filter to check summary of all events.

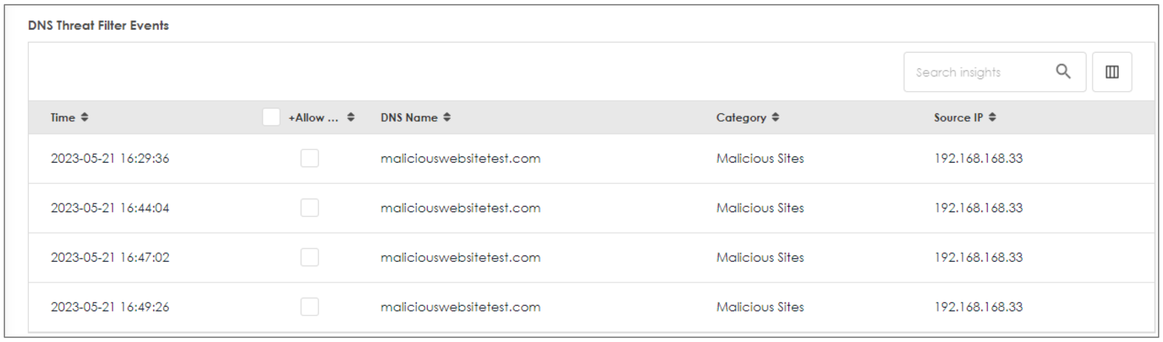


Last 24 Hours Summary

Click the pie chart to switch to the item events

Top entry by: DNS Name

DNS Name	Hit Count
🟩 maliciouswebsitetest.com	12 (100%)



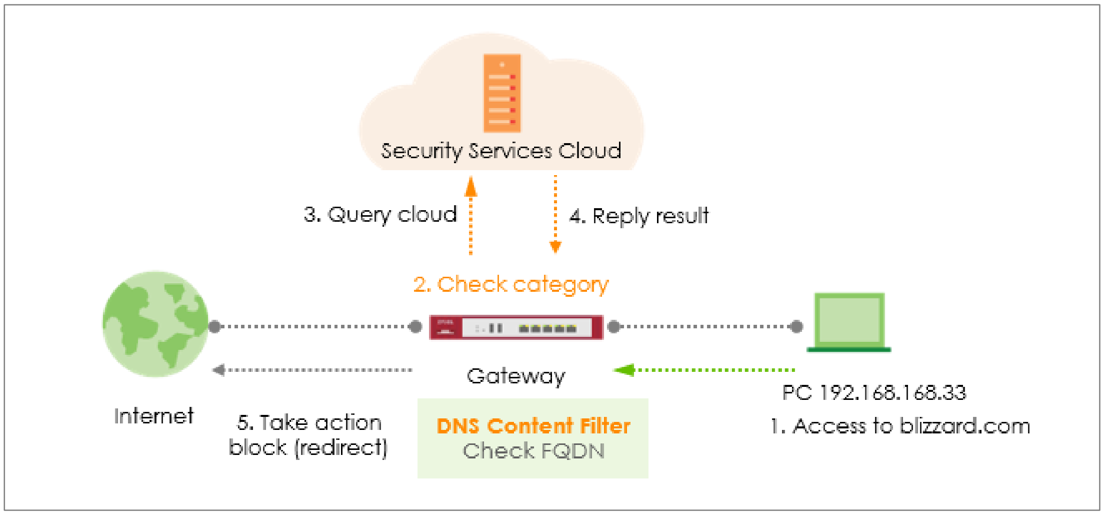
DNS Threat Filter Events

Time	□ +Allow ...	DNS Name	Category	Source IP
2023-05-21 16:29:36	□	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:44:04	□	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:47:02	□	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:49:26	□	maliciouswebsitetest.com	Malicious Sites	192.168.168.33

How to Configure DNS Content Filter

Compared to web content filter, DNS content filter is a stronger tool for SMB because it can restrict the number of attacks faced by network access, thereby helping to reduce the remediation workload of IT professionals.

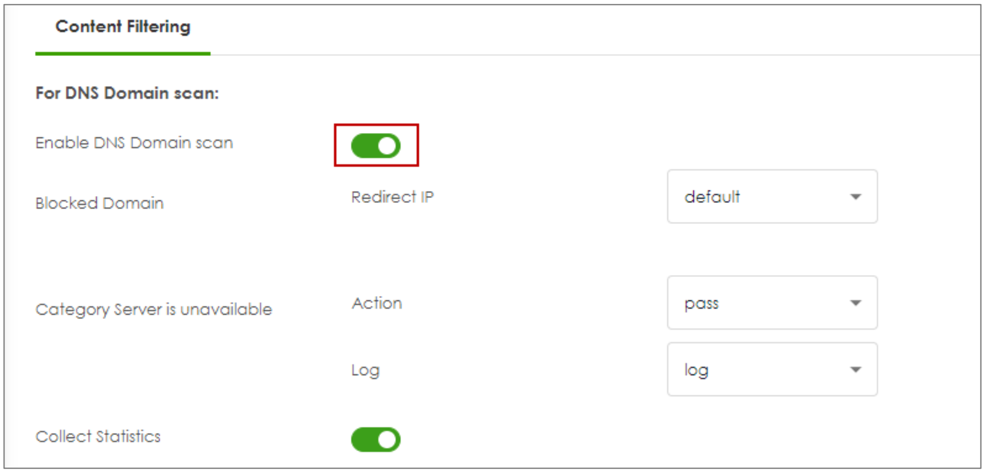
DNS content filter intercept DNS request from client, check the domain name category and takes a corresponding action, reducing the risk of phishing attacks, and obfuscate source IPs using hijacked domain names. Fully customizable blacklist to ban access to any unwanted domains and prevent reaching those known domains hosting malicious content. This example shows how to configure DNS Content Filter to block users in the local network to access the gaming 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 USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up the DNS Content Filter

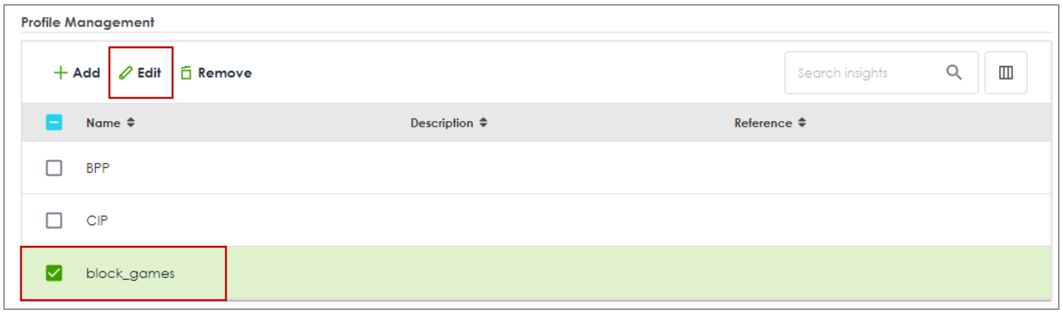
Go to Security Service > Content Filtering > For DNS Domain scan. Turn on this feature. Select Redirect IP for the Blocked Domain. If user selects the default, when client hits DNS Content Filter profile, the page will be redirected to block page http://dnsft.cloud.zyxel.com/.



For DNS Domain scan:

Enable DNS Domain scan	● On	
Blocked Domain	Redirect IP	default
Category Server is unavailable	Action	pass
	Log	log
Collect Statistics	● On	

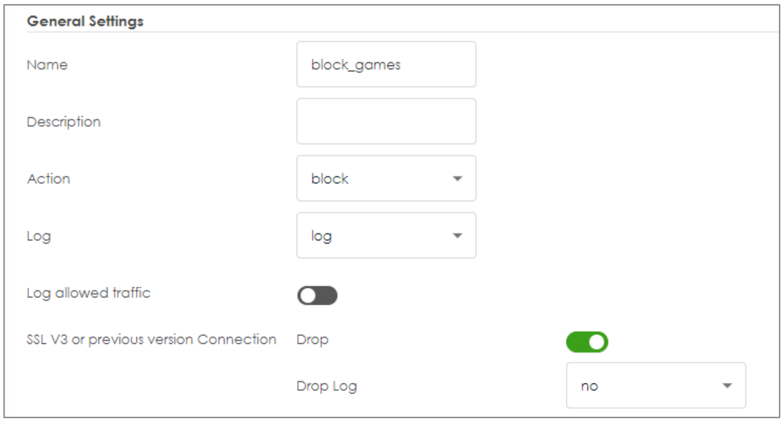
Add a new profile in Profile Management to block gaming websites.



	Name	Description	Reference
□	BPP		
□	CIP		
☑	block_games		

Action: block

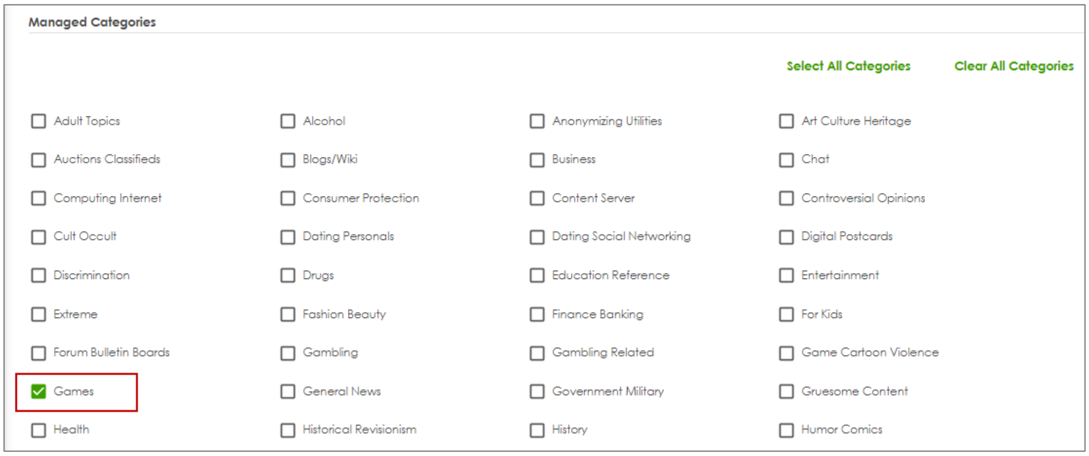
Log: log or log alert



General Settings

Name	block_games
Description	
Action	block
Log	log
Log allowed traffic	off
SSL V3 or previous version Connection	Drop: on
	Drop Log: no

Enable the checkbox of "Games" in managed categories.

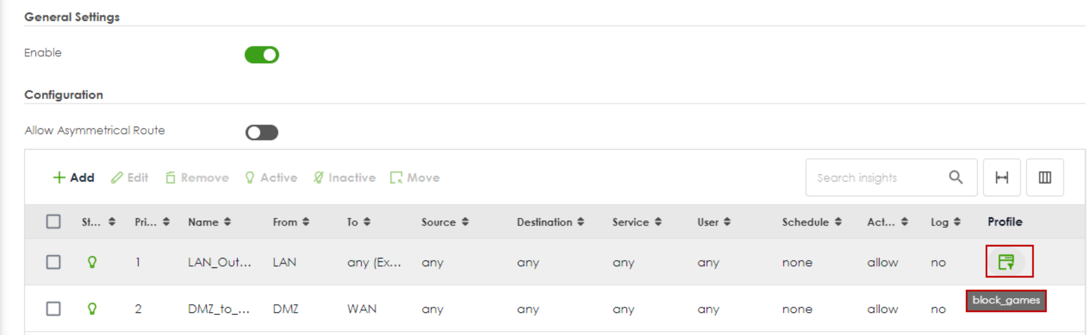


Managed Categories

Select All Categories Clear All Categories

☐ Adult Topics	☐ Alcohol	☐ Anonymizing Utilities	☐ Art Culture Heritage
☐ Auctions Classifieds	☐ Blogs/Wiki	☐ Business	☐ Chat
☐ Computing Internet	☐ Consumer Protection	☐ Content Server	☐ Controversial Opinions
☐ Cult Occult	☐ Dating Personals	☐ Dating Social Networking	☐ Digital Postcards
☐ Discrimination	☐ Drugs	☐ Education Reference	☐ Entertainment
☐ Extreme	☐ Fashion Beauty	☐ Finance Banking	☐ For Kids
☐ Forum Bulletin Boards	☐ Gambling	☐ Gambling Related	☐ Game Cartoon Violence
☑ Games	☐ General News	☐ Government Military	☐ Gruesome Content
☐ Health	☐ Historical Revisionism	☐ History	☐ Humor Comics

Apply the profile to security policy. In this example, the profile is applied to security policy rule "LAN_Outgoing".



General Settings

Enable: on

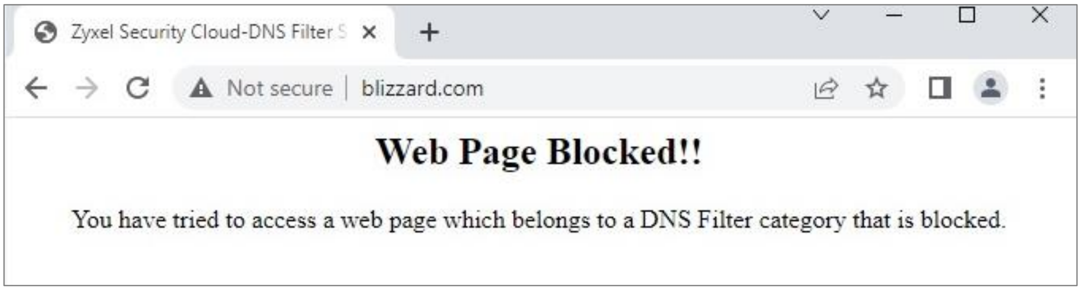
Configuration

Allow Asymmetrical Route: off

☐	St...	Pri...	Name	From	To	Source	Destination	Service	User	Schedule	Act...	Log	Profile
☐		1	LAN_Out...	LAN	any (Ex...	any	any	any	any	none	allow	no	
☐		2	DMZ_to_...	DMZ	WAN	any	any	any	any	none	allow	no	block_games

Test the Result

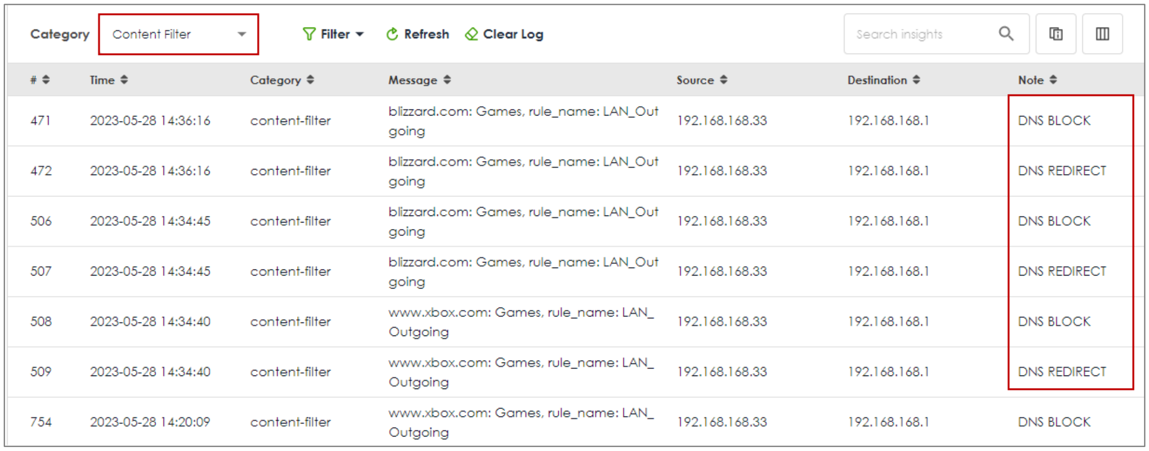
Access a gaming website blizzard.com. The gateway will redirect you to a blocked page.



Web Page Blocked!!

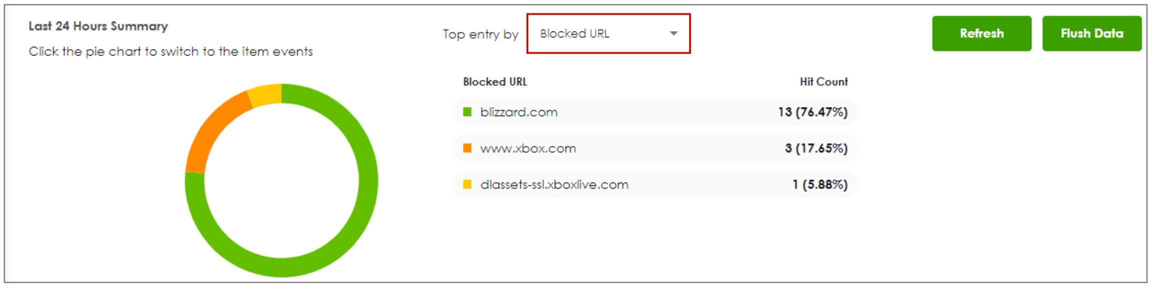
You have tried to access a web page which belongs to a DNS Filter category that is blocked.

Go to Log & Report > Log/Events and select Content Filter to check the logs.



#	Time	Category	Message	Source	Destination	Note
471	2023-05-28 14:36:16	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS BLOCK
472	2023-05-28 14:36:16	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS REDIRECT
506	2023-05-28 14:34:45	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS BLOCK
507	2023-05-28 14:34:45	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS REDIRECT
508	2023-05-28 14:34:40	content-filter	www.xbox.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS BLOCK
509	2023-05-28 14:34:40	content-filter	www.xbox.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS REDIRECT
754	2023-05-28 14:20:09	content-filter	www.xbox.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS BLOCK

Go to Security Statistics > Content Filter to check summary of all events.

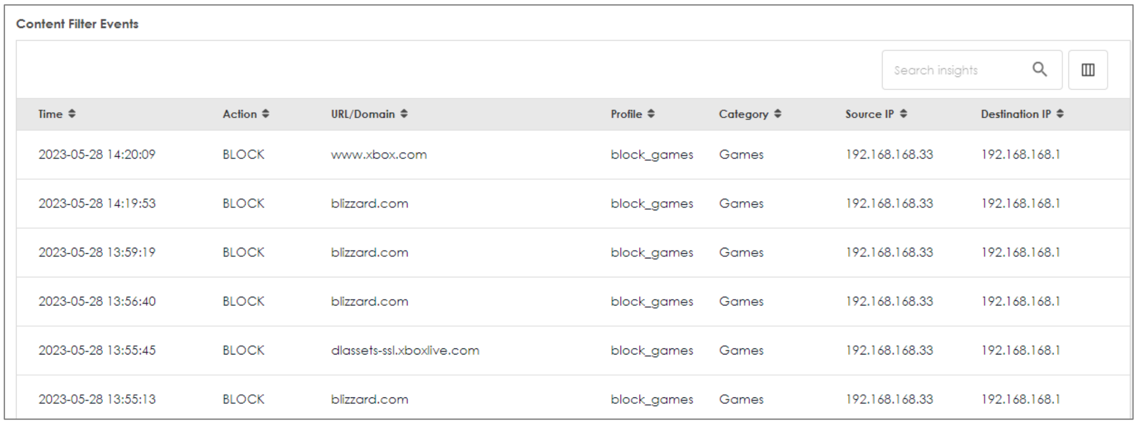


Last 24 Hours Summary

Click the pie chart to switch to the item events

Top entry by: Blocked URL

Blocked URL	Hit Count
🟩 blizzard.com	13 (76.47%)
🟧 www.xbox.com	3 (17.65%)
🟨 dlassets-ssl.xboxlive.com	1 (5.88%)

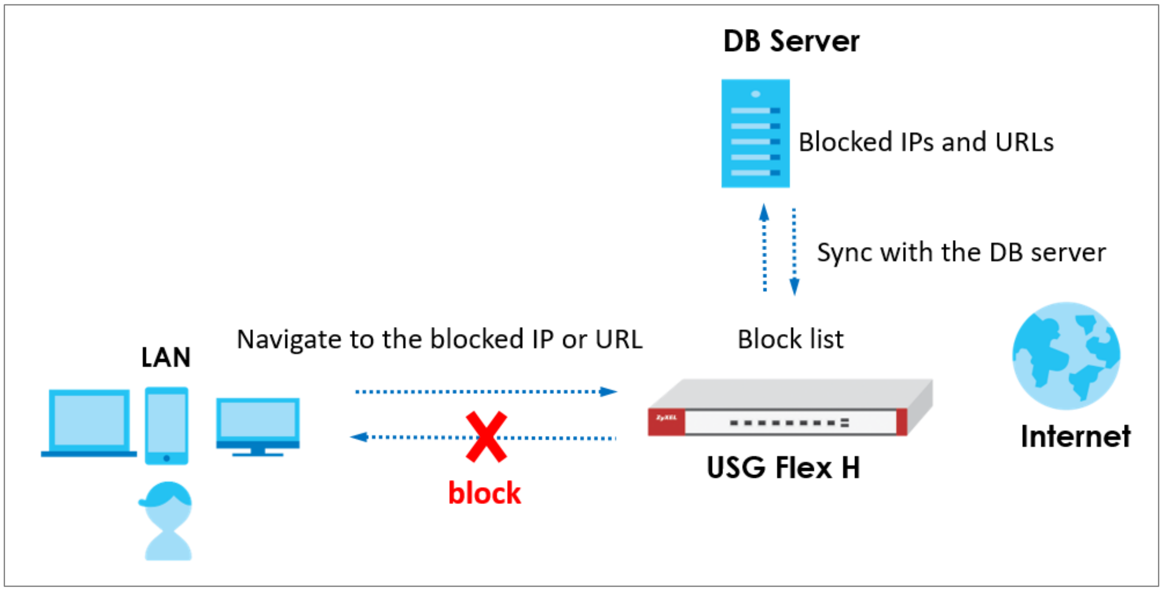


Content Filter Events

Time	Action	URL/Domain	Profile	Category	Source IP	Destination IP
2023-05-28 14:20:09	BLOCK	www.xbox.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-28 14:19:53	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-28 13:59:19	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-28 13:56:40	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-28 13:55:45	BLOCK	dlassets-ssl.xboxlive.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-28 13:55:13	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1

External Block List for Reputation Filter

The administrator can configure an external block list for the Reputation Filter to expand its usage. This article will provide guidance on setting up the external block list for the IP Reputation and DNS Threat Filter/URL Threat Filter.

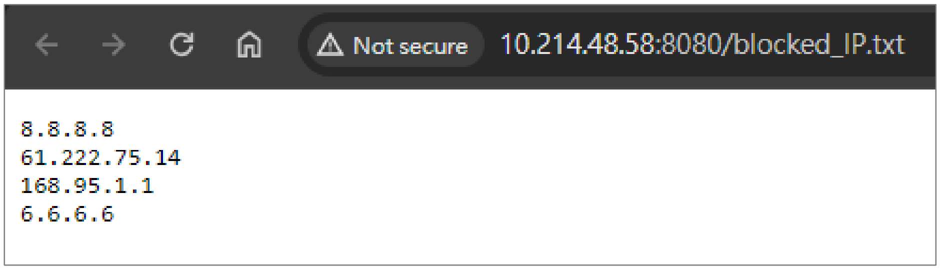


Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).

Set Up the DB server

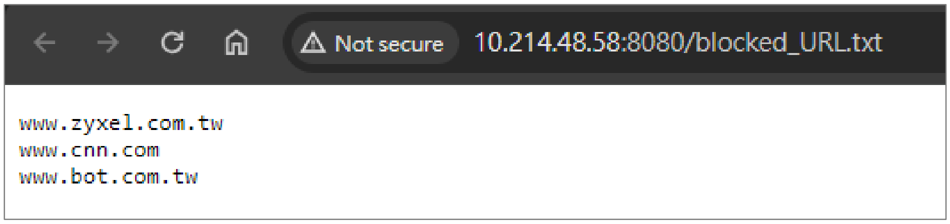
The administrator can set up websites to maintain external block lists. The USG Flex H firewall can update the external block list via a URL. For example,

http://10.214.48.58:8080/blocked_IP.txt



```
8.8.8.8
61.222.75.14
168.95.1.1
6.6.6.6
```

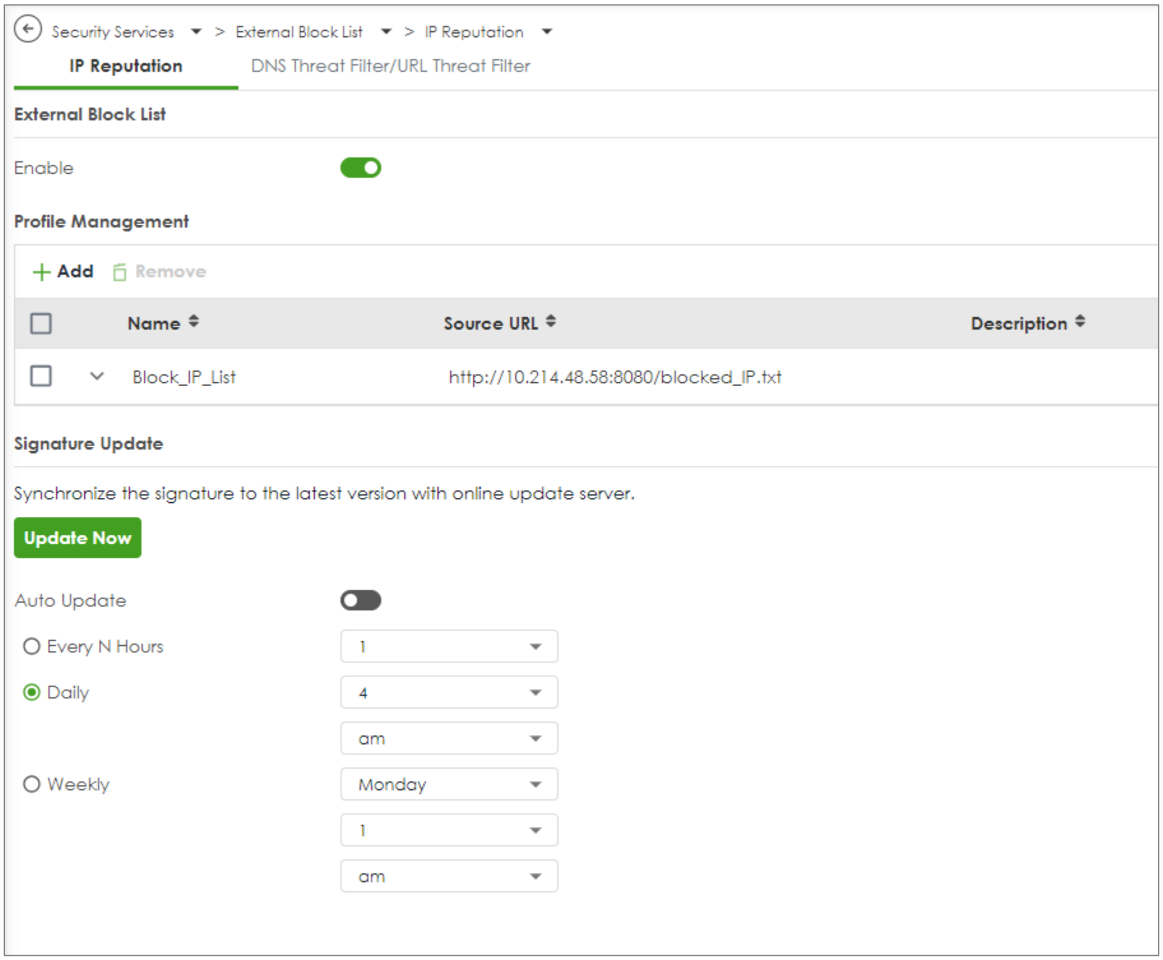
http://10.214.48.58:8080/blocked_URL.txt



```
www.zyxel.com.tw
www.cnn.com
www.bot.com.tw
```

Set Up the External Block List of IP Reputation

Navigate to Security Services > External Block List > IP Reputation and add a service URL such as http://10.214.48.58:8080/blocked_IP.txt and then click “Update Now” to update the block list.



Security Services > External Block List > IP Reputation
IP Reputation
DNS Threat Filter/URL Threat Filter

External Block List

Enable ●

Profile Management

□	Name	Source URL	Description
□	Block_IP_List	http://10.214.48.58:8080/blocked_IP.txt	

Signature Update

Synchronize the signature to the latest version with online update server.

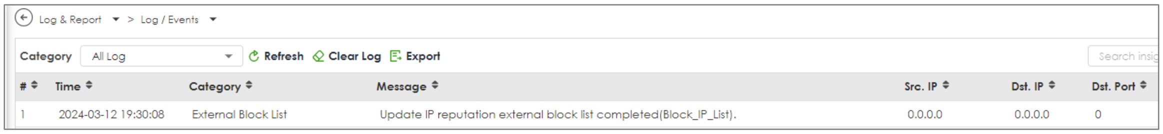
Auto Update ○

○ Every N Hours 1

● Daily 4 am

○ Weekly Monday 1 am

If the IP Reputation external block list is updated successfully and you can observe the corresponding log message.

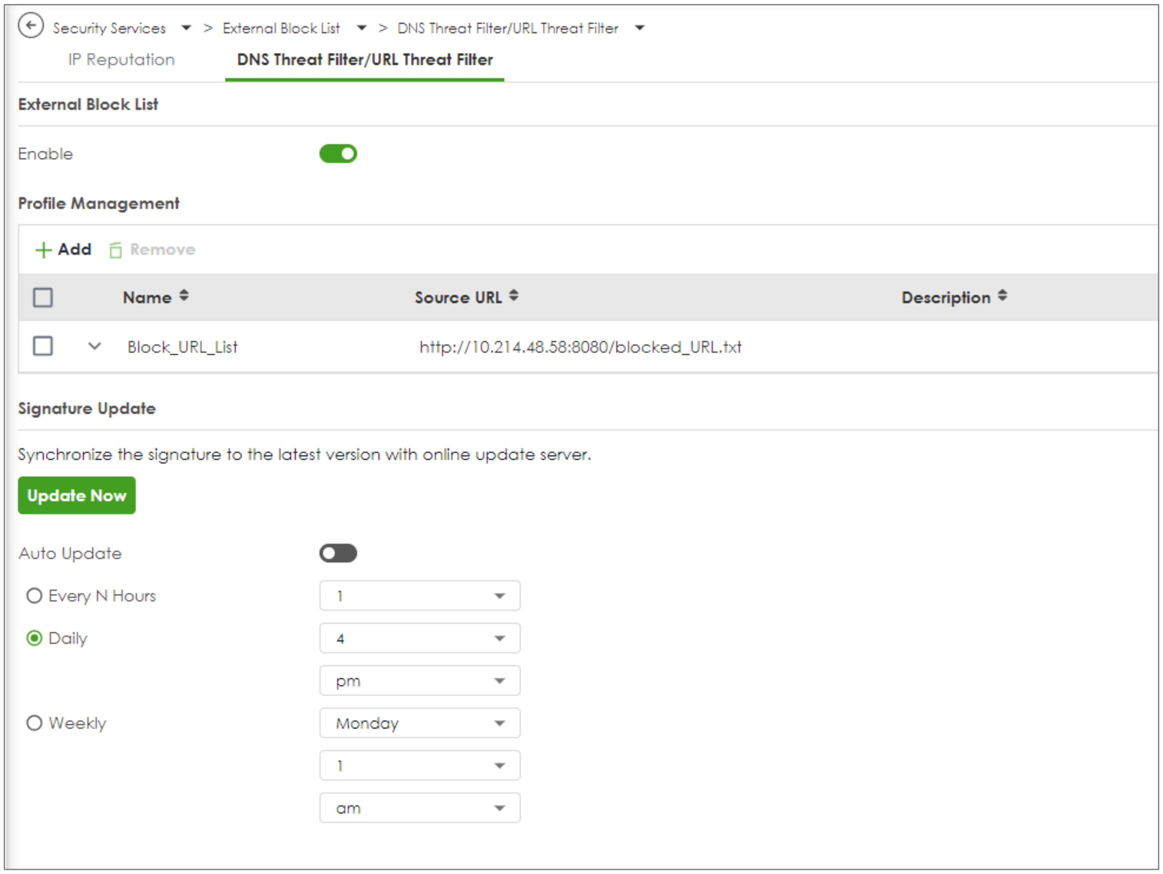


Category All Log

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port
1	2024-03-12 19:30:08	External Block List	Update IP reputation external block list completed(Block_IP_List).	0.0.0.0	0.0.0.0	0

Set Up the External Block List of DNS Threat Filter/URL Threat Filter

Navigate to Security Services > External Block List > DNS Threat Filter/URL Threat Filter and add a service URL such as http://10.214.48.58:8080/blocked_URL.txt and then click "Update Now" to update the block list.



Security Services > External Block List > DNS Threat Filter/URL Threat Filter

IP Reputation | **DNS Threat Filter/URL Threat Filter**

External Block List

Enable: ●

Profile Management

+ Add | Remove

□	Name	Source URL	Description
□	Block_URL_List	http://10.214.48.58:8080/blocked_URL.txt	

Signature Update

Synchronize the signature to the latest version with online update server.

Update Now

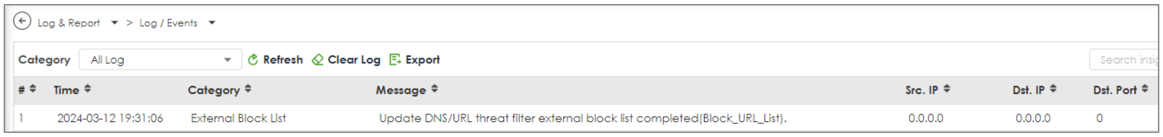
Auto Update: ○

○ Every N Hours: 1

● Daily: 4 pm

○ Weekly: Monday 1 am

If the DNS/URL threat filter external block list is updated successfully and you can observe the corresponding log message.



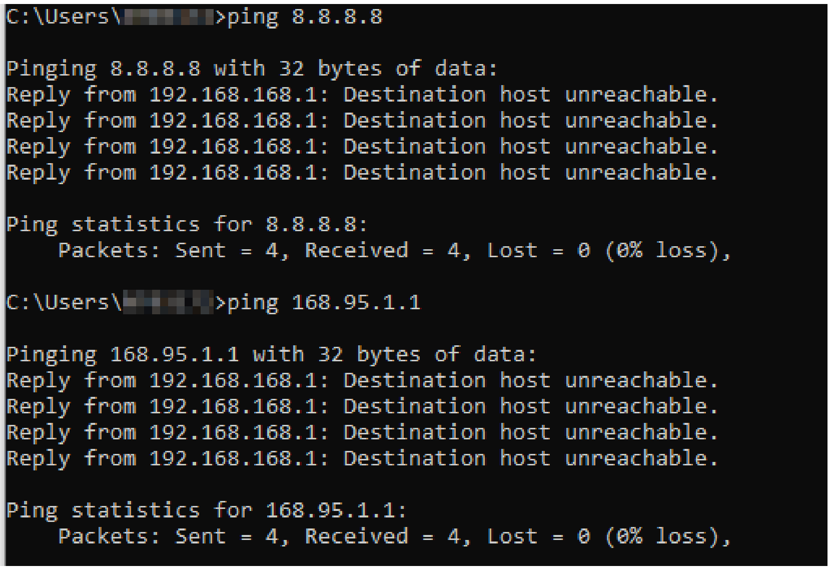
Log & Report > Log / Events

Category: All Log | Refresh | Clear Log | Export

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port
1	2024-03-12 19:31:06	External Block List	Update DNS/URL threat filter external block list completed(Block_URL_List).	0.0.0.0	0.0.0.0	0

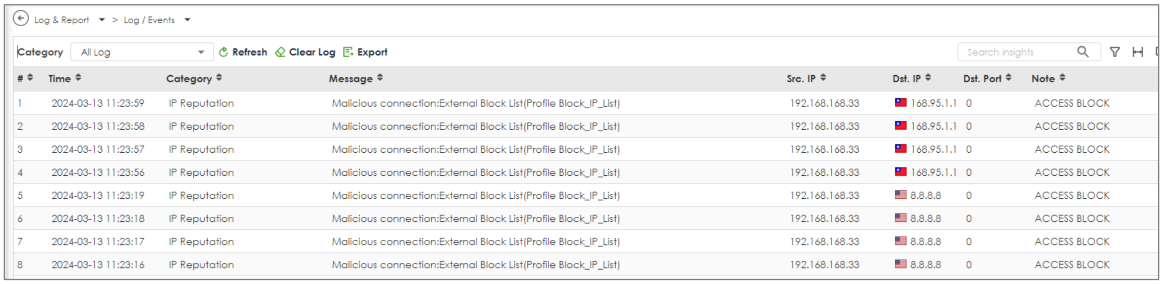
Test the Result

For instance, if the IP addresses 8.8.8.8 and 168.95.1.1 exist in the external block list, attempts to access these blocked IPs will be blocked as expected.



```
C:\Users\[redacted]>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.

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

C:\Users\[redacted]>ping 168.95.1.1

Pinging 168.95.1.1 with 32 bytes of data:
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.
Reply from 192.168.168.1: Destination host unreachable.

Ping statistics for 168.95.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

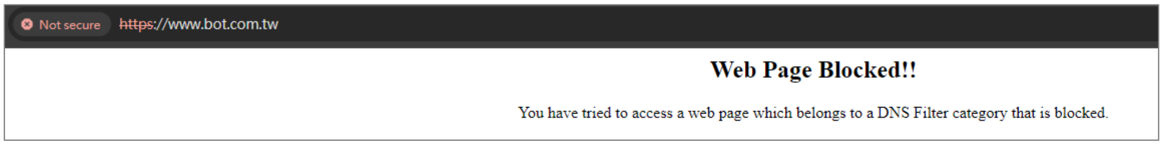
Go to Log & Report > Log / Events to observe block messages.



Category: All Log

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2024-03-13 11:23:59	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	168.95.1.1	0	ACCESS BLOCK
2	2024-03-13 11:23:58	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	168.95.1.1	0	ACCESS BLOCK
3	2024-03-13 11:23:57	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	168.95.1.1	0	ACCESS BLOCK
4	2024-03-13 11:23:56	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	168.95.1.1	0	ACCESS BLOCK
5	2024-03-13 11:23:19	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	8.8.8.8	0	ACCESS BLOCK
6	2024-03-13 11:23:18	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	8.8.8.8	0	ACCESS BLOCK
7	2024-03-13 11:23:17	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	8.8.8.8	0	ACCESS BLOCK
8	2024-03-13 11:23:16	IP Reputation	Malicious connection:External Block List(Profile Block_IP_List)	192.168.168.33	8.8.8.8	0	ACCESS BLOCK

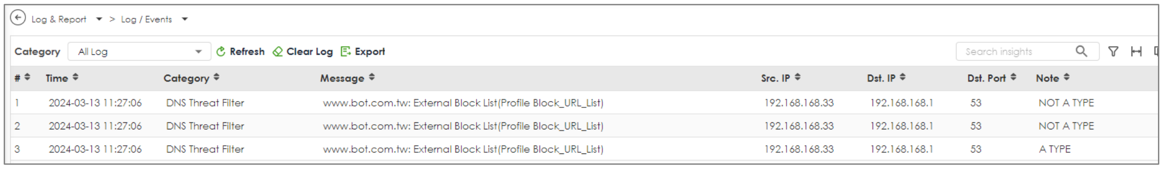
Attempts to access URLs that exist in the block list will also be blocked as expected.



Web Page Blocked!!

You have tried to access a web page which belongs to a DNS Filter category that is blocked.

Go to Log & Report > Log / Events to observe block messages.



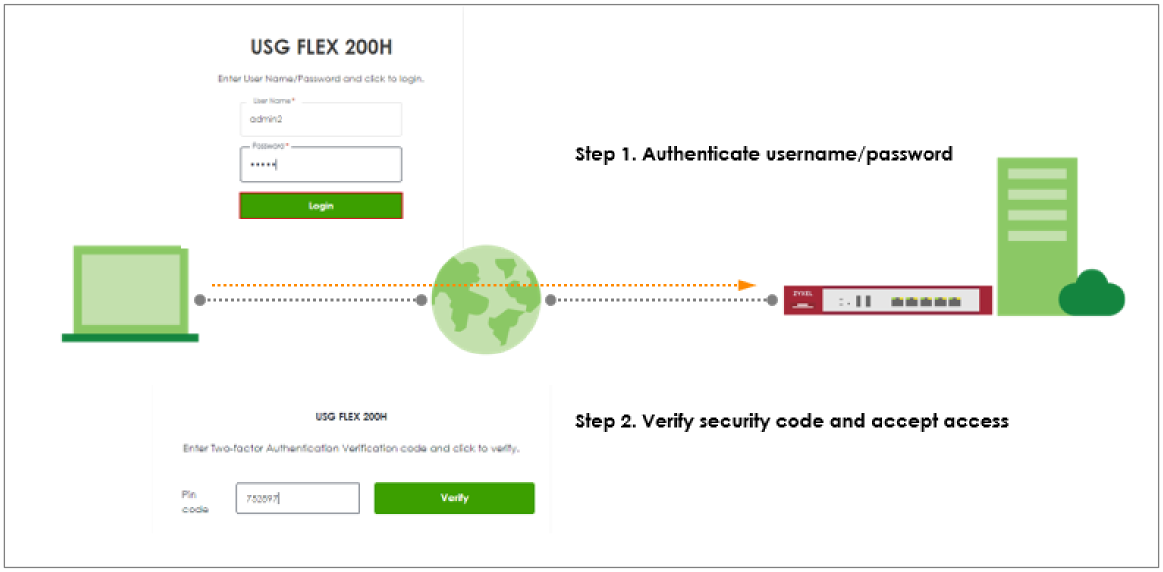
Category: All Log

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2024-03-13 11:27:06	DNS Threat Filter	www.bot.com.tw: External Block List(Profile Block_URL_List)	192.168.168.33	192.168.168.1	53	NOT A TYPE
2	2024-03-13 11:27:06	DNS Threat Filter	www.bot.com.tw: External Block List(Profile Block_URL_List)	192.168.168.33	192.168.168.1	53	NOT A TYPE
3	2024-03-13 11:27:06	DNS Threat Filter	www.bot.com.tw: External Block List(Profile Block_URL_List)	192.168.168.33	192.168.168.1	53	A TYPE

Chapter 3- Authentication

How to Use Two Factor with Google Authenticator for Admin Access

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.



USG FLEX 200H

Enter User Name/Password and click to login.

User Name*: admin2

Password*: •••••

Step 1. Authenticate username/password

USG FLEX 200H

Enter Two-factor Authentication Verification code and click to verify.

Pin code: 752597

Step 2. Verify security code and accept access

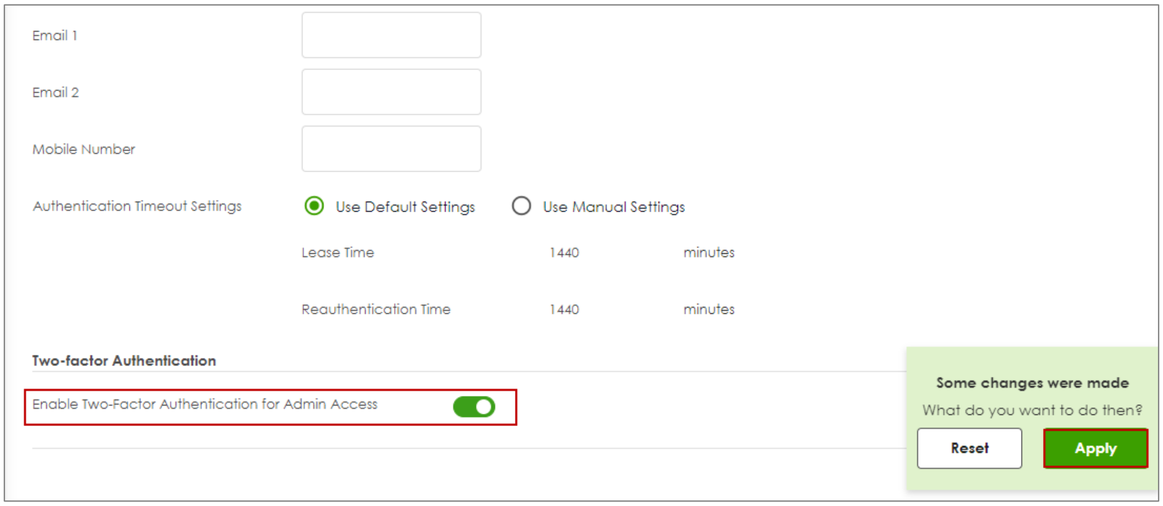
Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

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

Go to User & Authentication > User/Group. Select a specific local administrator and enable Two-factor authentication.



Email 1

Email 2

Mobile Number

Authentication Timeout Settings ● Use Default Settings ○ Use Manual Settings

Lease Time 1440 minutes

Reauthentication Time 1440 minutes

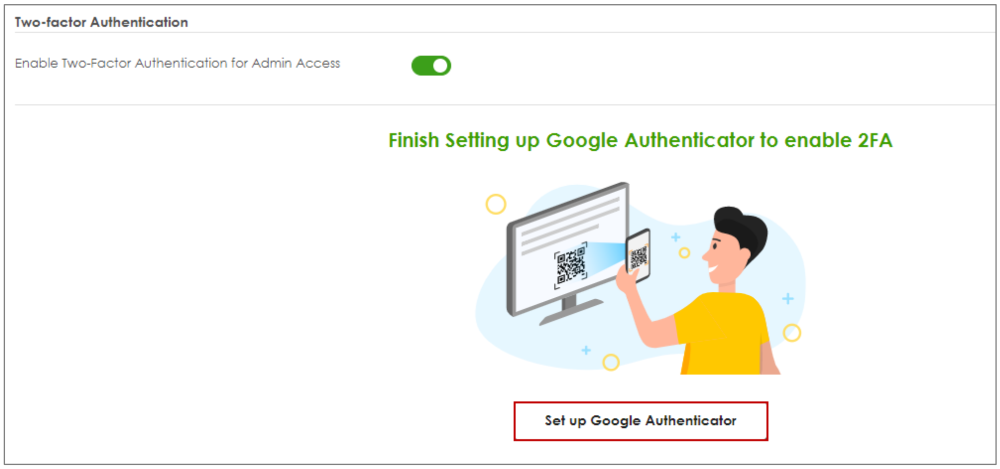
Two-factor Authentication

Enable Two-Factor Authentication for Admin Access

Some changes were made

What do you want to do then?

Click "Set up Google Authenticator" to start setting up Google Authenticator on your mobile phone.

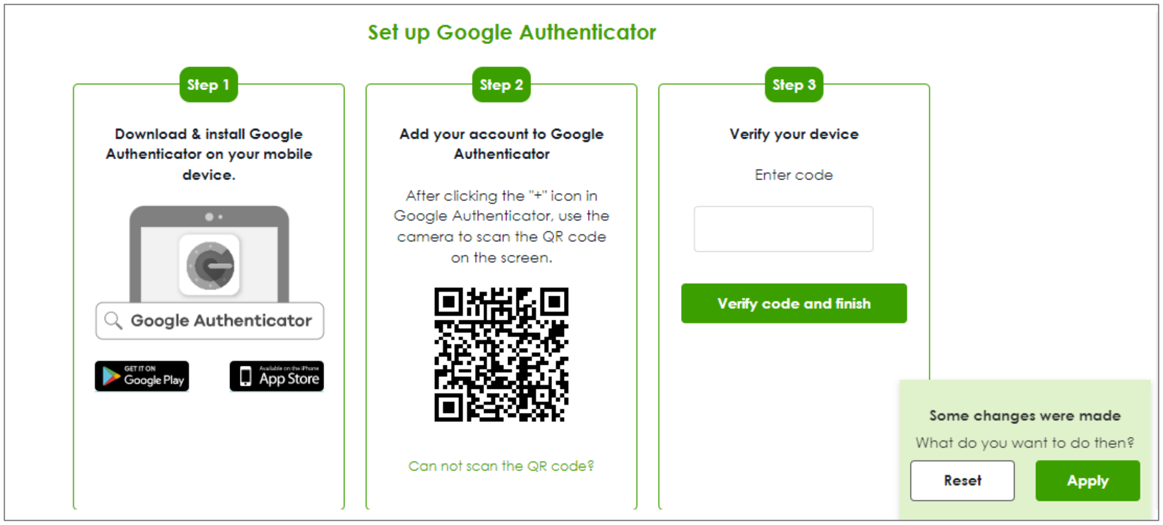


Two-factor Authentication

Enable Two-Factor Authentication for Admin Access

Finish Setting up Google Authenticator to enable 2FA

Set up Google Authenticator



Set up Google Authenticator

Step 1

Download & install Google Authenticator on your mobile device.

Step 2

Add your account to Google Authenticator

After clicking the "+" icon in Google Authenticator, use the camera to scan the QR code on the screen.

Can not scan the QR code?

Step 3

Verify your device

Enter code

Verify code and finish

Some changes were made

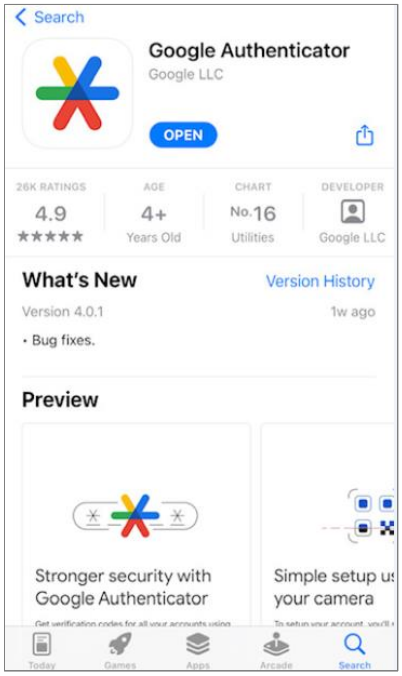
What do you want to do then?

Reset

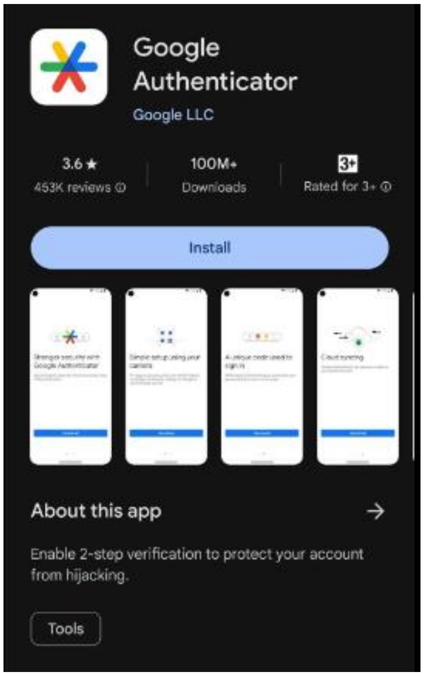
Apply

1. Download and install Google Authenticator on your mobile device.

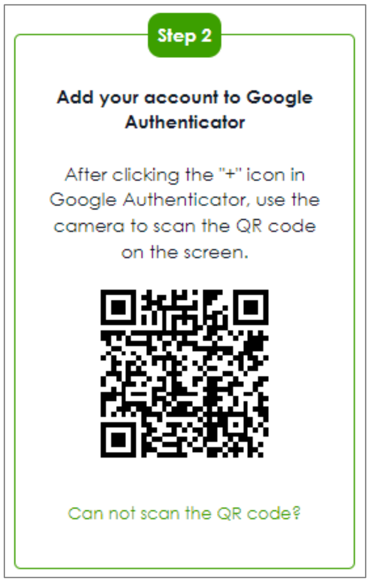
Apple Store



Google Play

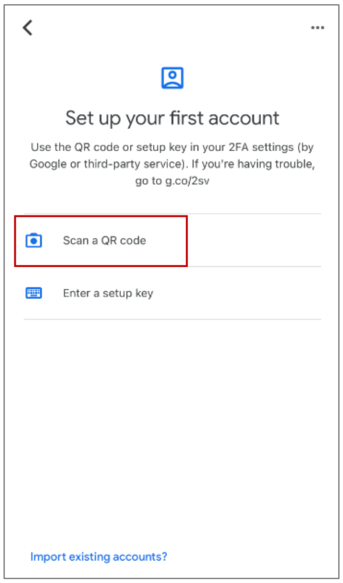


2. Register the admin account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.



Add your account to Google Authenticator

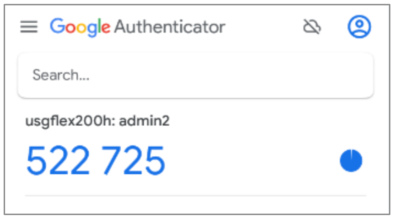
After clicking the "+" icon in Google Authenticator, use the camera to scan the QR code on the screen.



Set up your first account

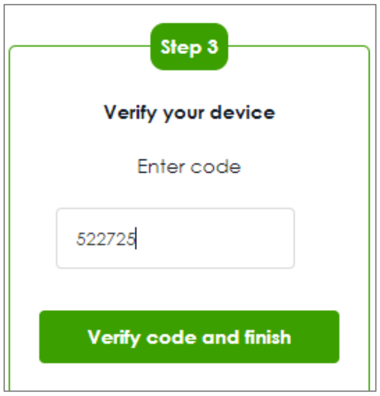
Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

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.



usgflex200h: admin2

522 725

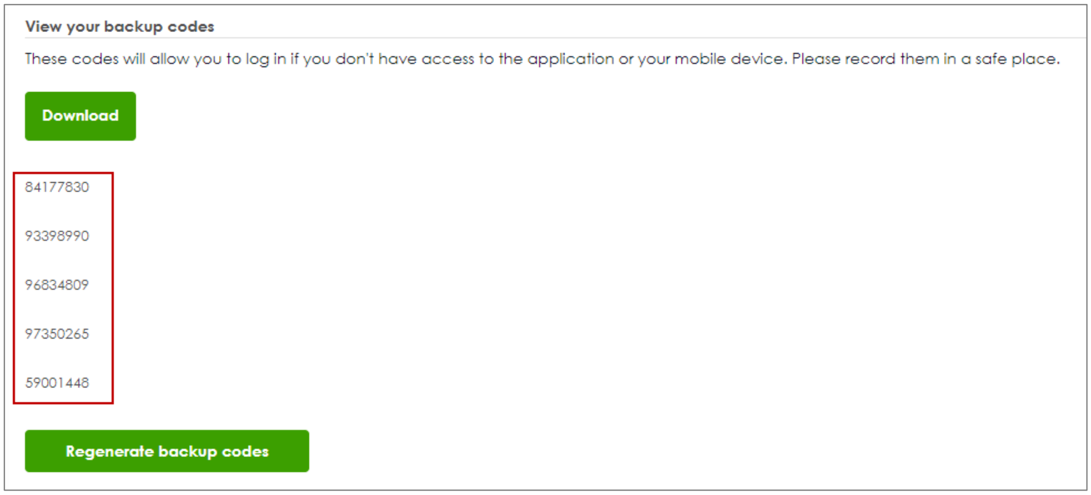


Verify your device

Enter code

522725

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.



View your backup codes

These codes will allow you to log in if you don't have access to the application or your mobile device. Please record them in a safe place.

84177830

93398990

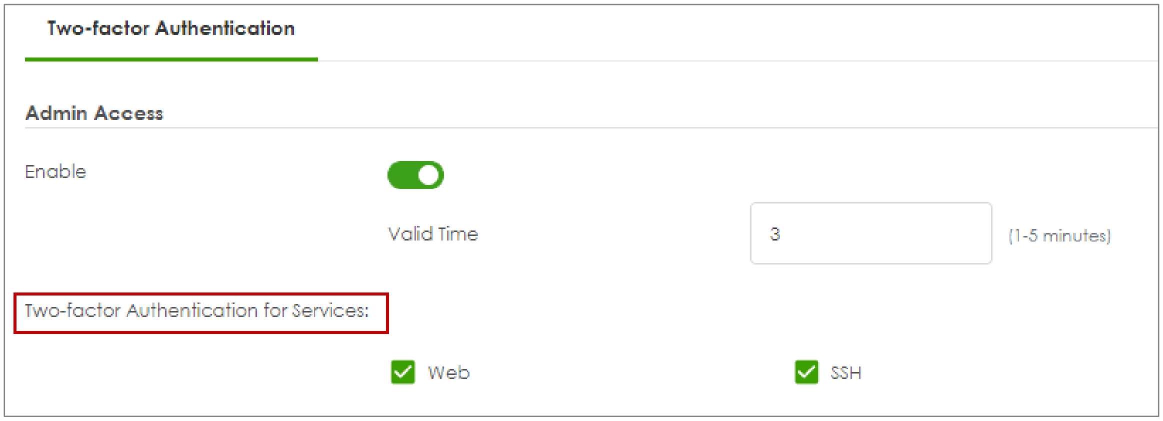
96834809

97350265

59001448

Configure valid time and login service types

Go to User & Authentication > User Authentication. Two factor authentication for admin access is enabled by default. You need to select which services require two-factor authentication for admin user manually. 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.



Two-factor Authentication

Admin Access

Enable: on

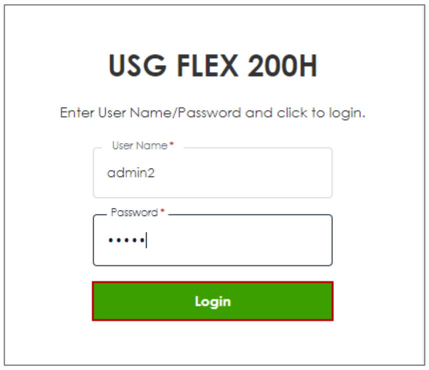
Valid Time: 3 (1-5 minutes)

Two-factor Authentication for Services:

☑ Web ☑ SSH

Test the Result

1. Login with the admin account "admin2".

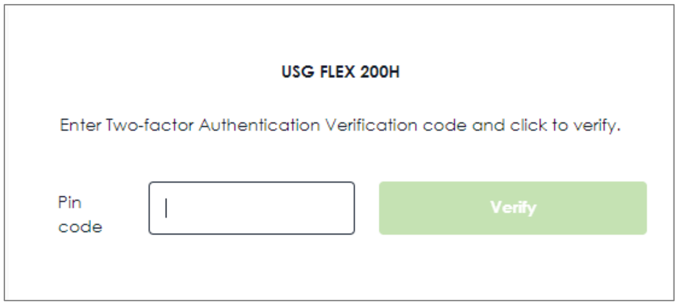

USG FLEX 200H

Enter User Name/Password and click to login.

User Name * admin2

Password * •••••

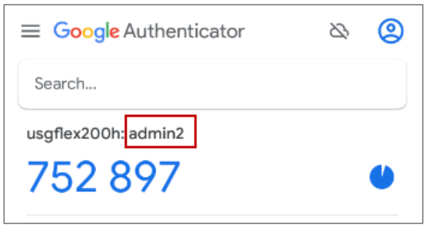
2. A pop-up window appears for administrator to enter the verification code.


USG FLEX 200H

Enter Two-factor Authentication Verification code and click to verify.

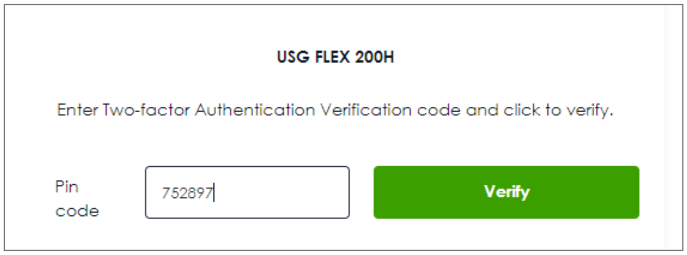
Pin code

3. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.



usgflex200h:admin2

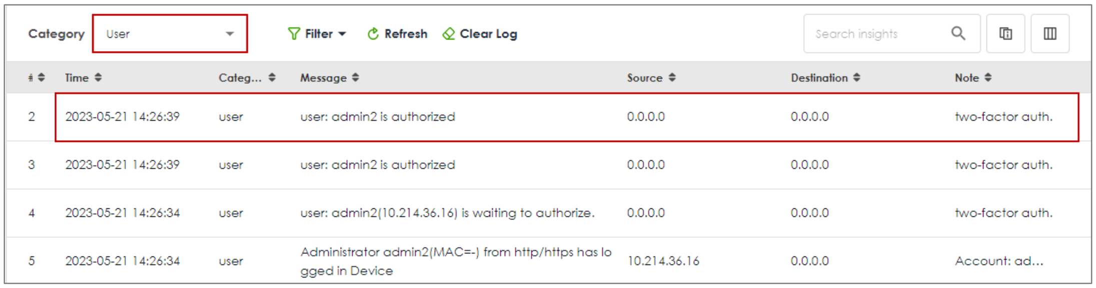
752 897


USG FLEX 200H

Enter Two-factor Authentication Verification code and click to verify.

Pin code 752897

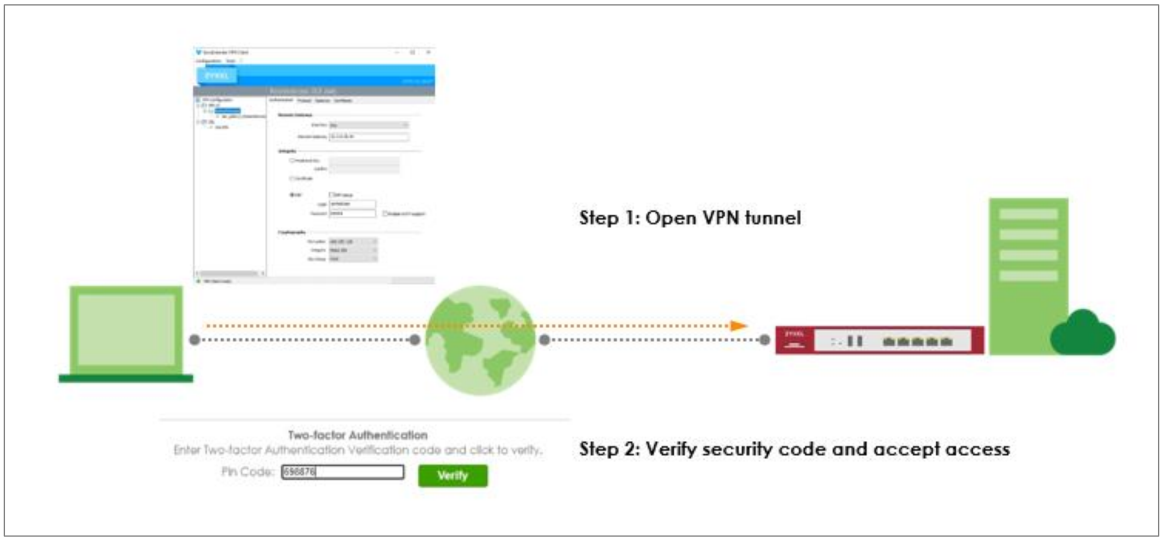
4. Authorize with username, password and the token code successfully. Go to Log & Report > Log/Events and select "User" to check the login status.



#	Time	Categ...	Message	Source	Destination	Note
2	2023-05-21 14:26:39	user	user: admin2 is authorized	0.0.0.0	0.0.0.0	two-factor auth.
3	2023-05-21 14:26:39	user	user: admin2 is authorized	0.0.0.0	0.0.0.0	two-factor auth.
4	2023-05-21 14:26:34	user	user: admin2(10.214.36.16) is waiting to authorize.	0.0.0.0	0.0.0.0	two-factor auth.
5	2023-05-21 14:26:34	user	Administrator admin2(MAC=-) from http/https has lo gged in Device	10.214.36.16	0.0.0.0	Account: ad...

How to Use Two Factor with Google Authenticator for Remote Access VPN and SSL VPN

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 Remote Access VPN and SSL VPN.



Two-factor Authentication

Enter Two-factor Authentication Verification code and click to verify.

Pin Code: 698876

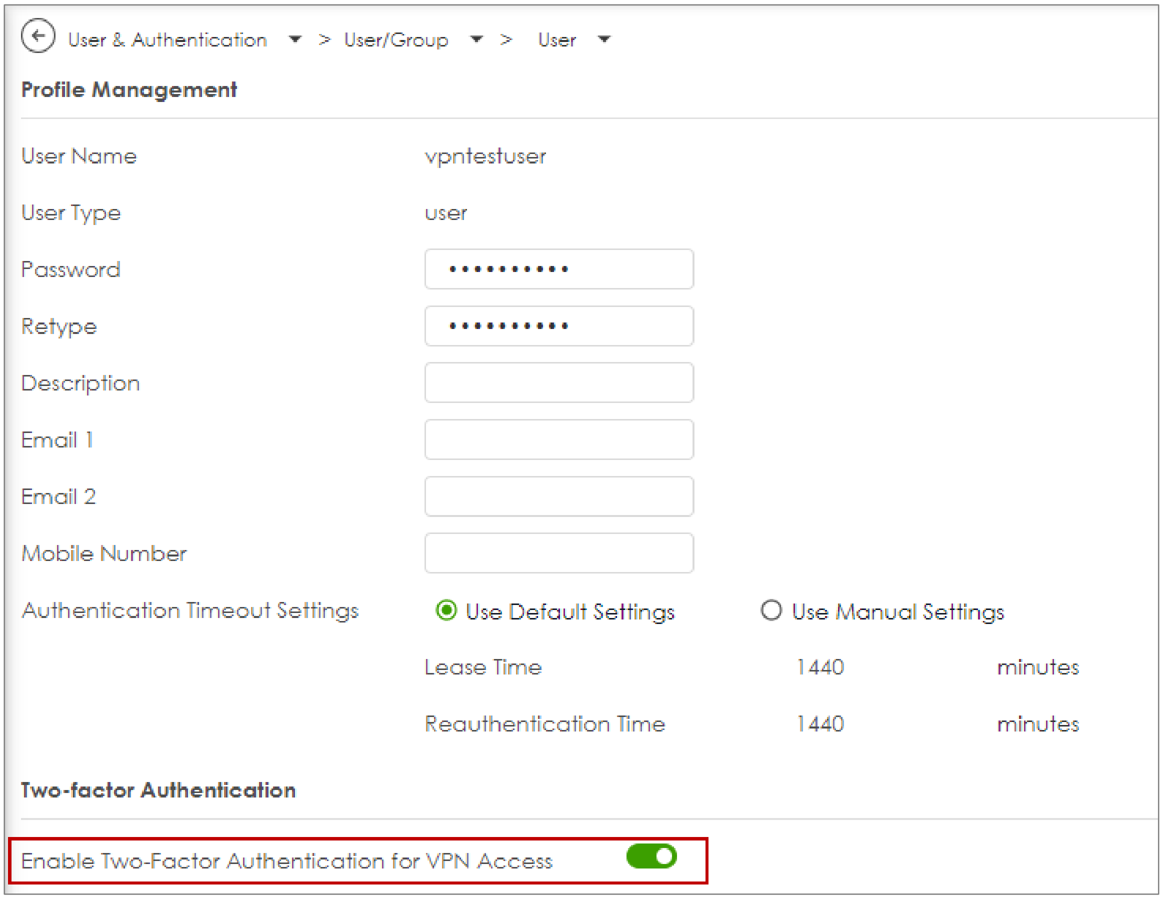
💡Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).

Two Factor with Google Authenticator Flow

4. Enable Google Authentication on a user.
5. Set up Google Authenticator.
6. Configure valid time and VPN types.

Enable Google Authentication on a User

Go to User & Authentication > User/Group. Select a local user and enable Two-factor authentication.



User & Authentication ▾ > User/Group ▾ > User ▾

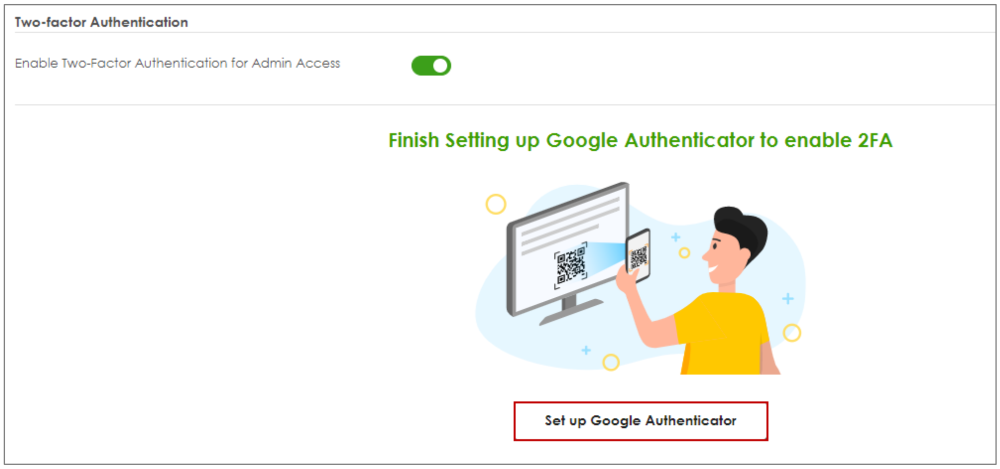
Profile Management

User Name	vpntestuser		
User Type	user		
Password	•••••••••••		
Retype	•••••••••••		
Description			
Email 1			
Email 2			
Mobile Number			
Authentication Timeout Settings	● Use Default Settings	○ Use Manual Settings	
	Lease Time	1440	minutes
	Reauthentication Time	1440	minutes

Two-factor Authentication

Enable Two-Factor Authentication for VPN Access ●

Click "Set up Google Authenticator" to start setting up Google Authenticator on your mobile phone.

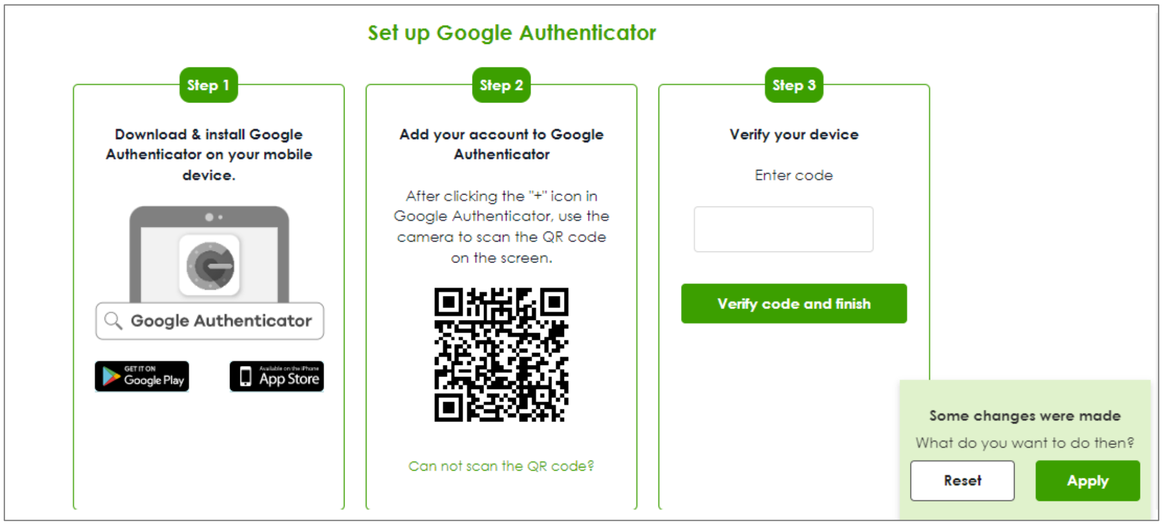


Two-factor Authentication

Enable Two-Factor Authentication for Admin Access

Finish Setting up Google Authenticator to enable 2FA

Set up Google Authenticator



Set up Google Authenticator

Step 1

Download & install Google Authenticator on your mobile device.

Step 2

Add your account to Google Authenticator

After clicking the "+" icon in Google Authenticator, use the camera to scan the QR code on the screen.

Can not scan the QR code?

Step 3

Verify your device

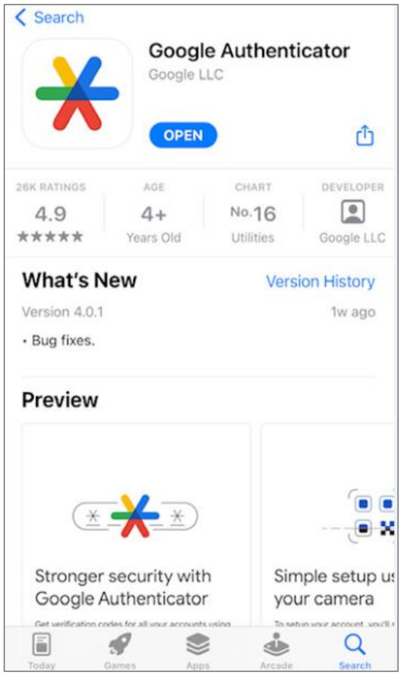
Enter code

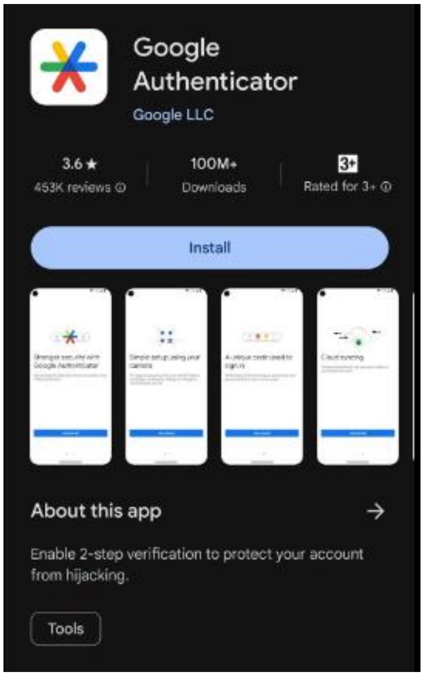
Some changes were made

What do you want to do then?

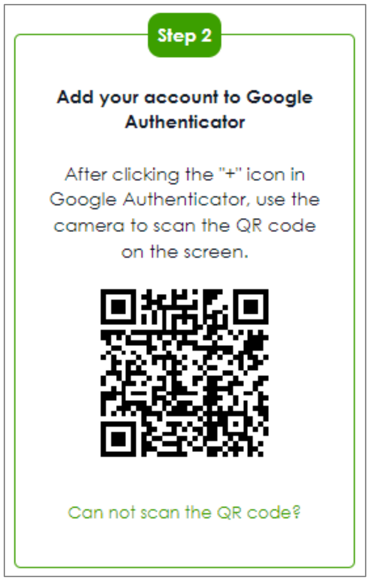
5. Download and install Google Authenticator on your mobile device.

Apple Store **Google Play**





6. Register the user account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.

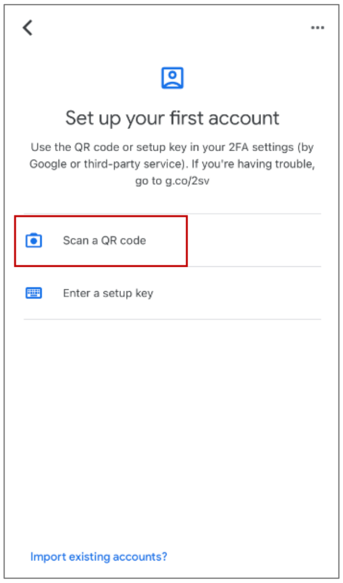


Step 2

Add your account to Google Authenticator

After clicking the "+" icon in Google Authenticator, use the camera to scan the QR code on the screen.

Can not scan the QR code?



Set up your first account

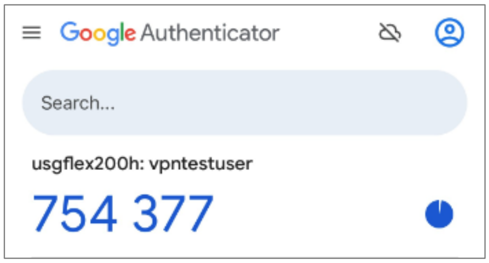
Use the QR code or setup key in your 2FA settings (by Google or third-party service). If you're having trouble, go to g.co/2sv

Scan a QR code

Enter a setup key

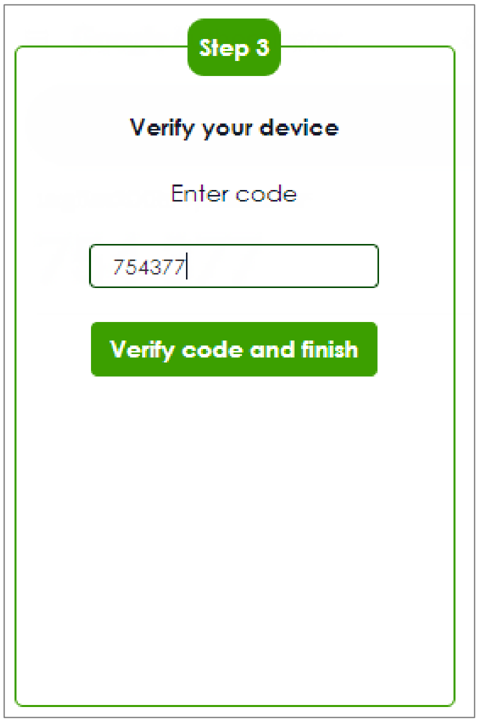
Import existing accounts?

7. Enter the token code which displays on Google Authenticator to "Step 3" and click "Verify code and finish" to submit and verify the code.



usgflex200h: vpntestuser

754 377

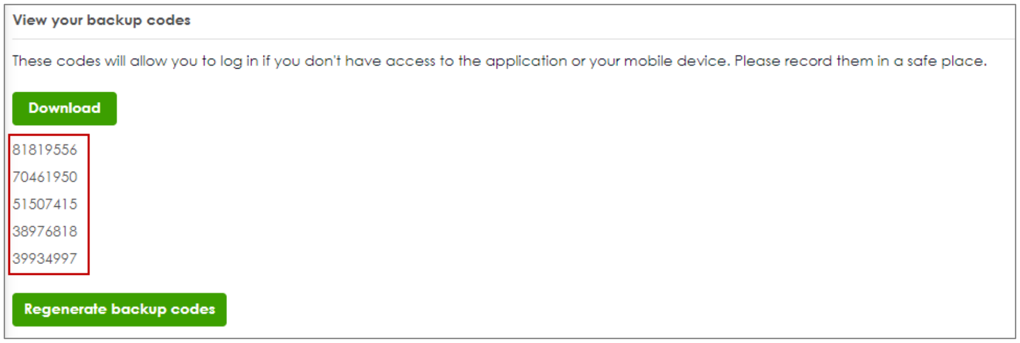


Verify your device

Enter code

754377

8. 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.

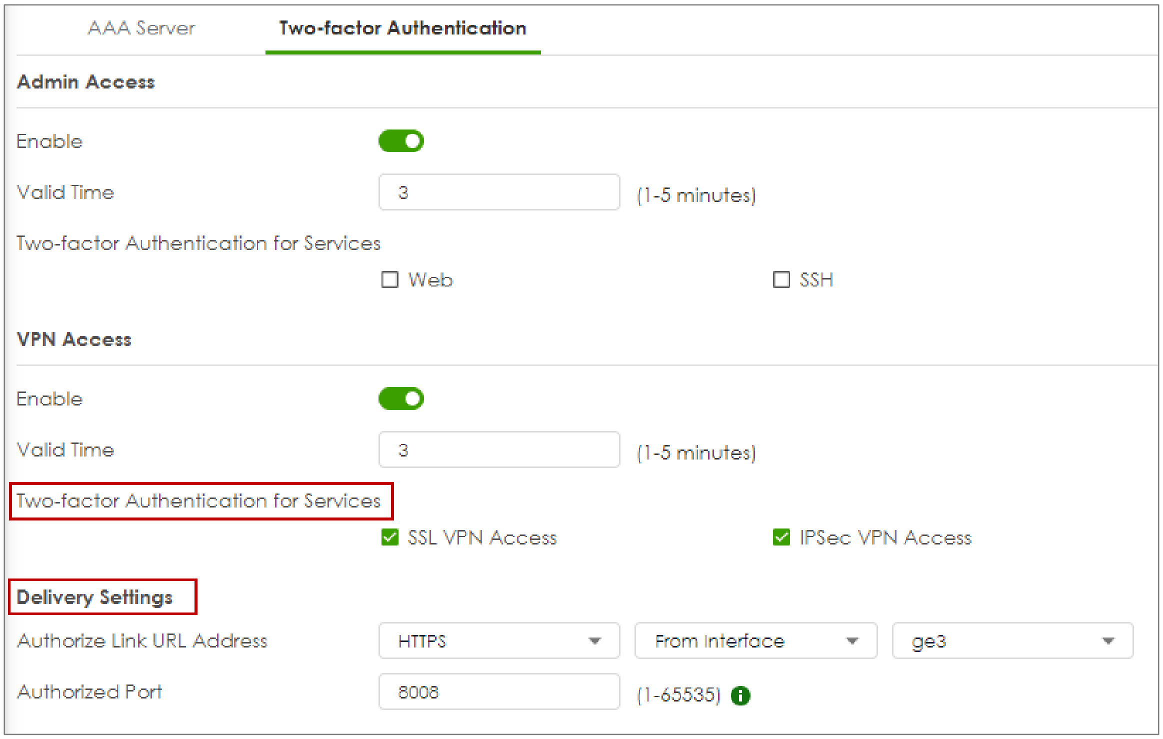

View your backup codes

These codes will allow you to log in if you don't have access to the application or your mobile device. Please record them in a safe place.

81819556
70461950
51507415
38976818
39934997

Configure valid time and login service types

Enable two factor authentication for VPN access. Configure valid time and select which VPN type requires two-factor authentication for VPN user. The valid time is the deadline that user needs to submit the two-factor authentication code to get the VPN access. The request is rejected if submitting the code later than valid time. By default, the valid time is 3 minutes. The authentication page is working on specific service port. After building up VPN tunnel, user have to enter the code in the Web GUI.



Admin Access

Enable: ●

Valid Time: 3 (1-5 minutes)

Two-factor Authentication for Services

□ Web □ SSH

VPN Access

Enable: ●

Valid Time: 3 (1-5 minutes)

Two-factor Authentication for Services

☑ SSL VPN Access ☑ IPSec VPN Access

Delivery Settings

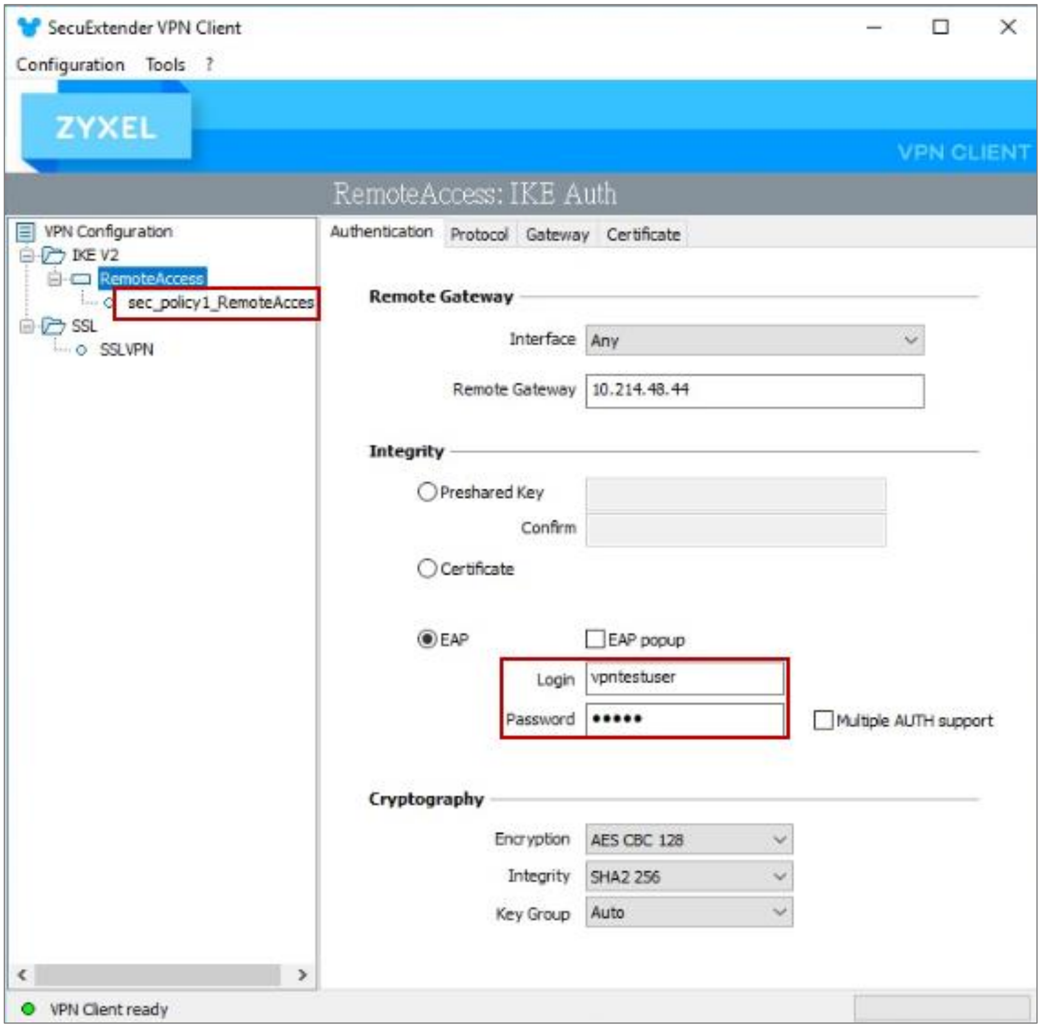
Authorize Link URL Address: HTTPS, From Interface, ge3

Authorized Port: 8008 (1-65535)

Test the Result

Remote Access VPN (IKEv2)

1. Open Remote Access VPN tunnel on SecuExtender VPN Client.



RemoteAccess: IKE Auth

Remote Gateway

Interface: Any

Remote Gateway: 10.214.48.44

Integrity

○ Preshared Key

Confirm

○ Certificate

● EAP □ EAP popup

Login: vpntestuser

Password: •••••

□ Multiple AUTH support

Cryptography

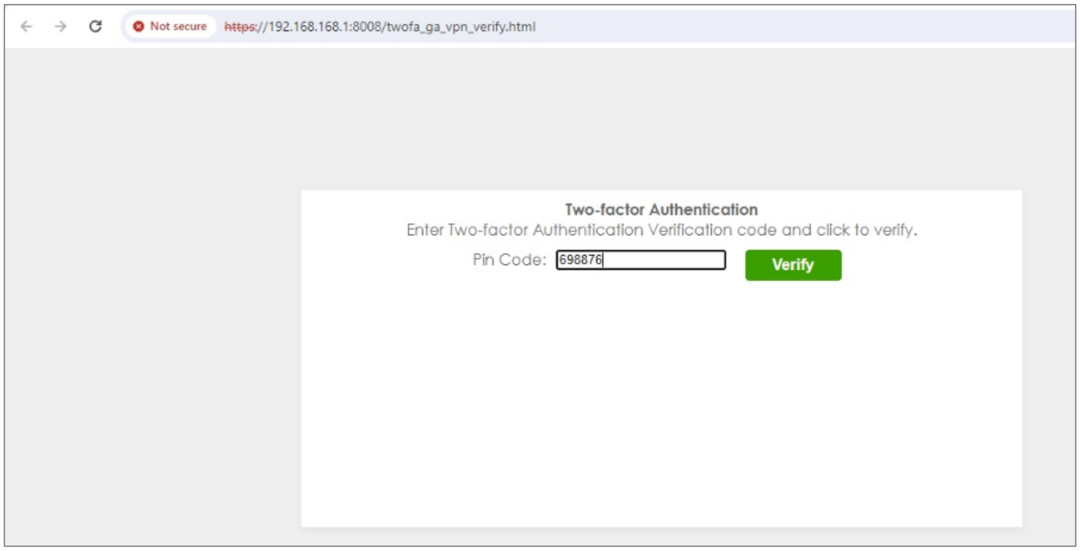
Encryption: AES CBC 128

Integrity: SHA2 256

Key Group: Auto

VPN Client ready

2. The browser will pop up authentication page to enter the verification code. 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.



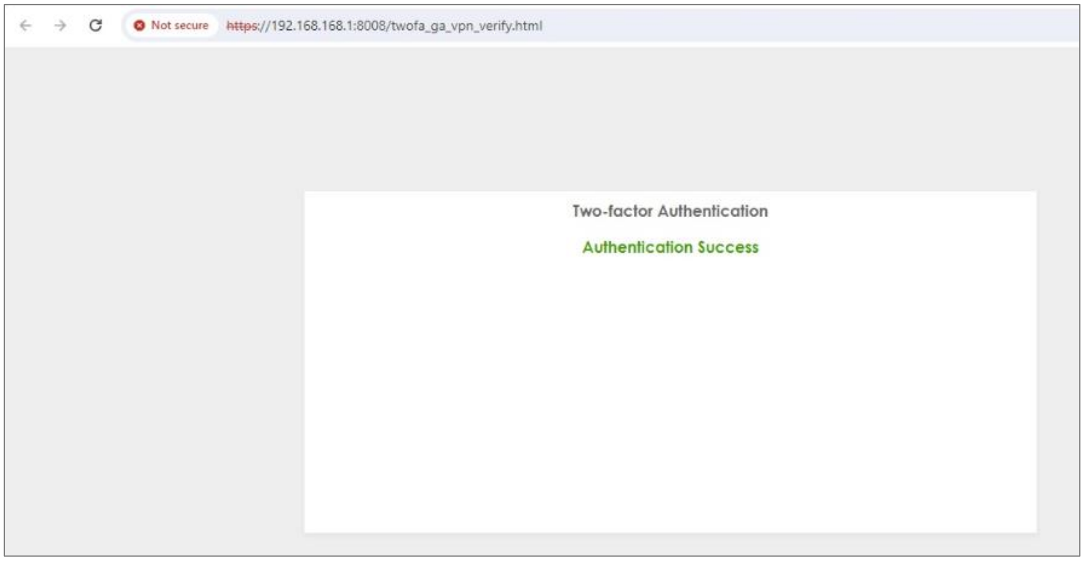
Not secure ~~https~~://192.168.168.1:8008/twofa_ga_vpn_verify.html

Two-factor Authentication

Enter Two-factor Authentication Verification code and click to verify.

Pin Code: 698876

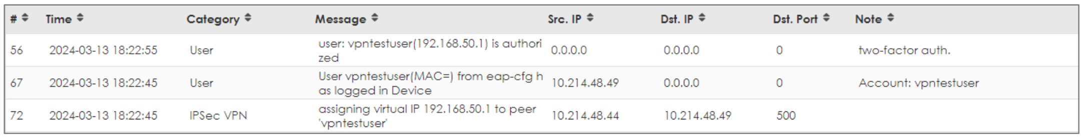
3. Authorize with username, password and the token code successfully.



Not secure ~~https~~://192.168.168.1:8008/twofa_ga_vpn_verify.html

Two-factor Authentication

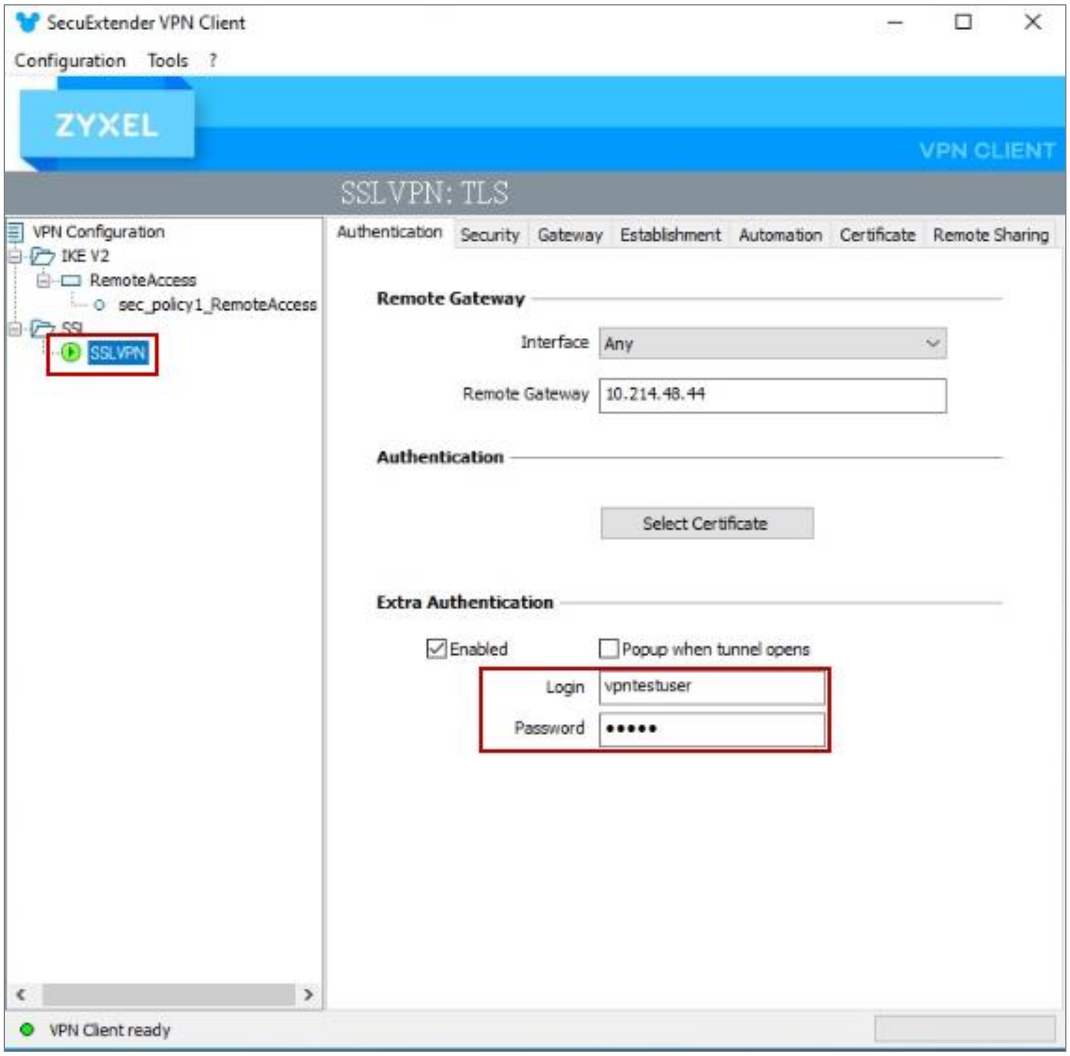
Authentication Success



#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
56	2024-03-13 18:22:55	User	user: vpntestuser(192.168.50.1) is authorized	0.0.0.0	0.0.0.0	0	two-factor auth.
67	2024-03-13 18:22:45	User	User vpntestuser(MAC=) from eap-cfg has logged in Device	10.214.48.49	0.0.0.0	0	Account: vpntestuser
72	2024-03-13 18:22:45	IPSec VPN	assigning virtual IP 192.168.50.1 to peer 'vpntestuser'	10.214.48.44	10.214.48.49	500	

SSL VPN

1. Open SSL VPN tunnel on SecuExtender VPN Client.



Remote Gateway

Interface: Any

Remote Gateway: 10.214.48.44

Authentication

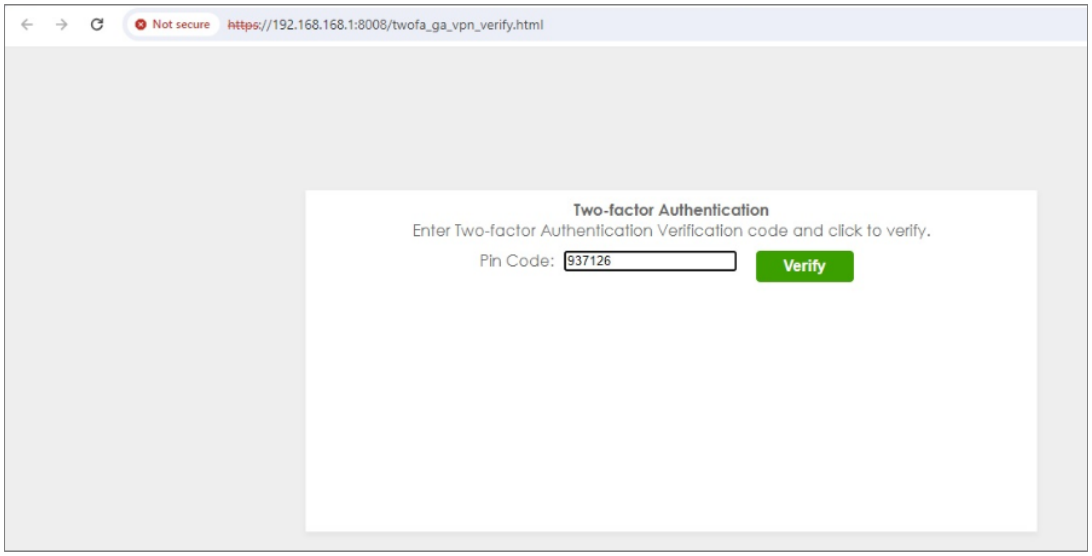
Extra Authentication

☑ Enabled ☐ Popup when tunnel opens

Login: vpntestuser

Password: •••••

2. The browser will pop up authentication page to enter the verification code. 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.



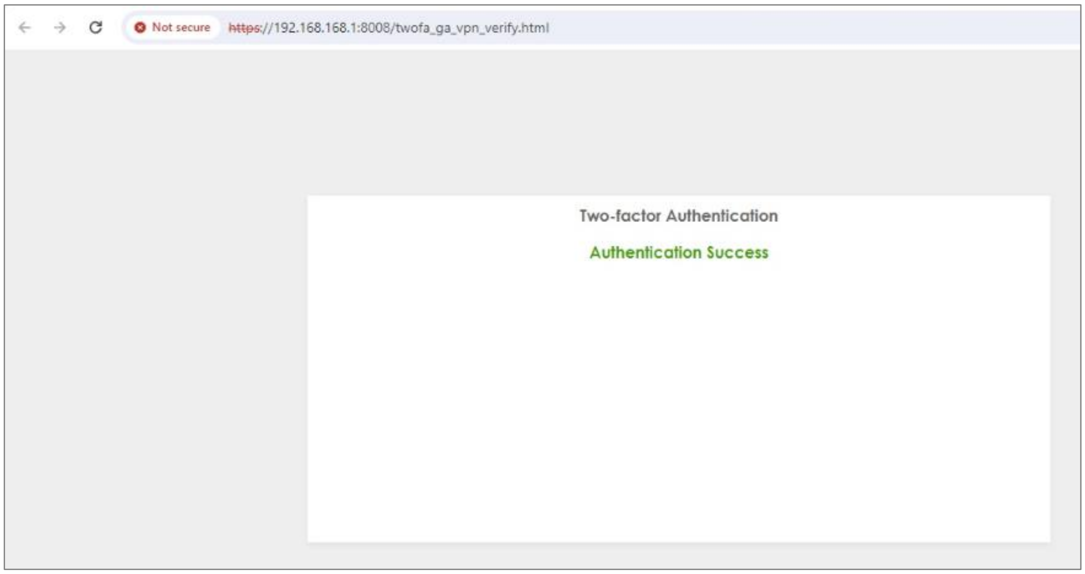
Not secure ~~https~~://192.168.168.1:8008/twofa_ga_vpn_verify.html

Two-factor Authentication

Enter Two-factor Authentication Verification code and click to verify.

Pin Code: 937126

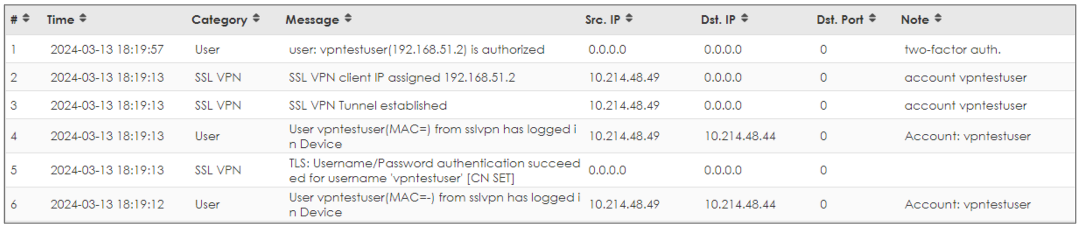
3. Authorize with username, password and the token code successfully.



Not secure ~~https~~://192.168.168.1:8008/twofa_ga_vpn_verify.html

Two-factor Authentication

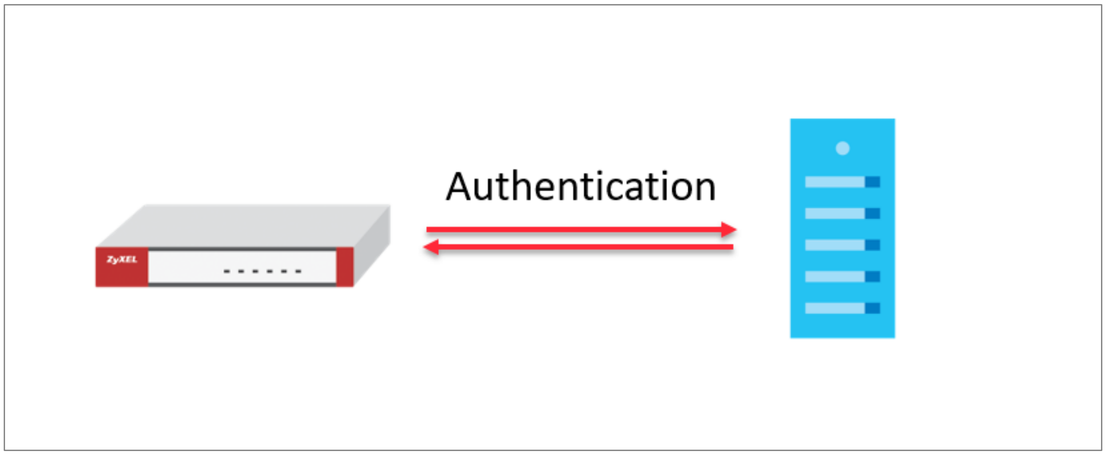
Authentication Success



#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2024-03-13 18:19:57	User	user: vpntestuser(192.168.51.2) is authorized	0.0.0.0	0.0.0.0	0	two-factor auth.
2	2024-03-13 18:19:13	SSL VPN	SSL VPN client IP assigned 192.168.51.2	10.214.48.49	0.0.0.0	0	account vpntestuser
3	2024-03-13 18:19:13	SSL VPN	SSL VPN Tunnel established	10.214.48.49	0.0.0.0	0	account vpntestuser
4	2024-03-13 18:19:13	User	User vpntestuser(MAC=) from sslvpn has logged in Device	10.214.48.49	10.214.48.44	0	Account: vpntestuser
5	2024-03-13 18:19:13	SSL VPN	TLS: Username/Password authentication succeeded for username 'vpntestuser' [CN SET]	0.0.0.0	0.0.0.0	0	
6	2024-03-13 18:19:12	User	User vpntestuser(MAC=-) from sslvpn has logged in Device	10.214.48.49	10.214.48.44	0	Account: vpntestuser

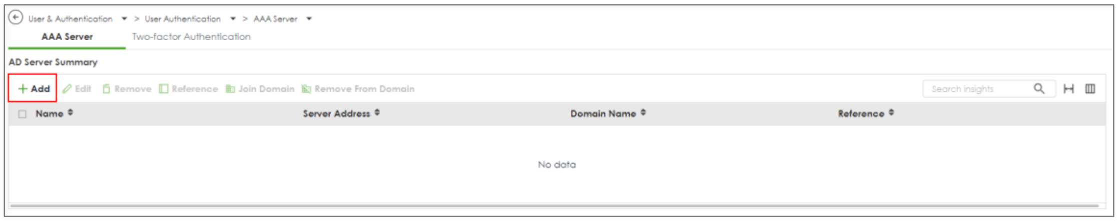
How to set up AD authentication with Microsoft AD

This is an example of using USG FLEX H to configure AD authentication with Microsoft Active Directory(AD). The article briefly explains the parameters for the AD configuration and guides how to join domain to the AD server.



Set Up a profile for AD server

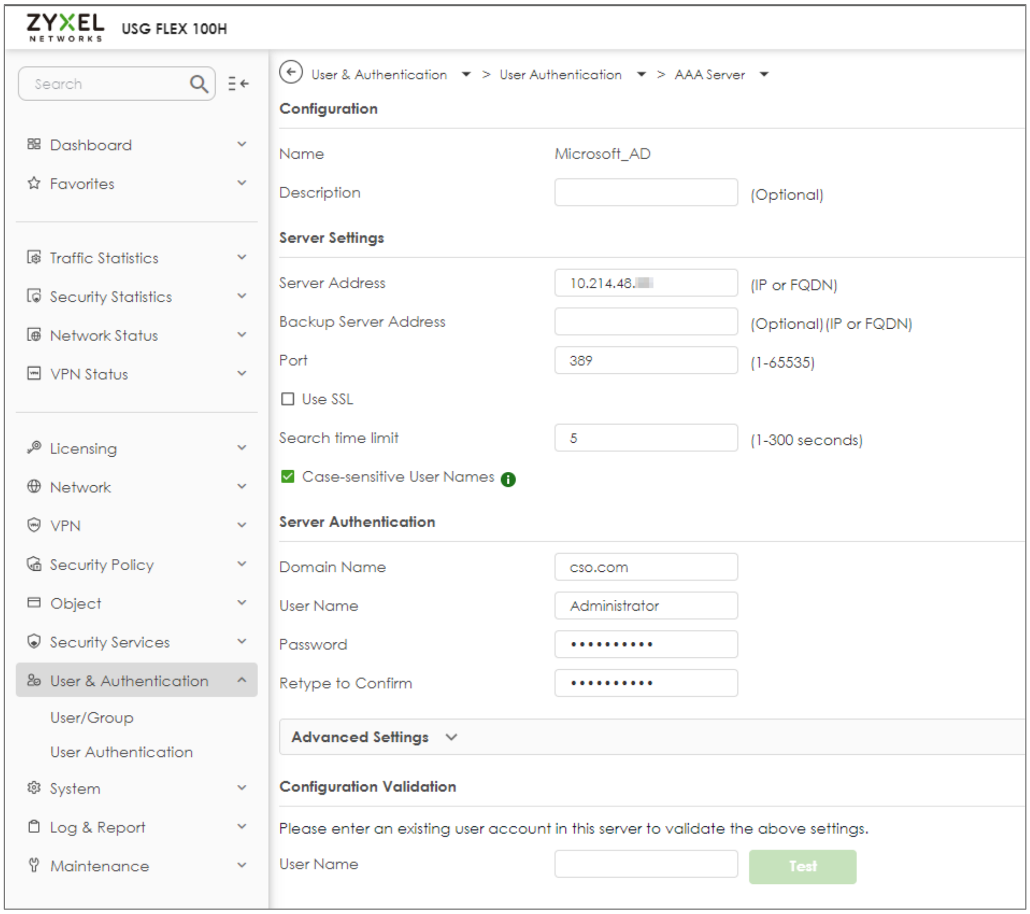
Go to User & Authentication > User Authentication > AAA Server > AD. Click +Add to create a new profile


User & Authentication > User Authentication > AAA Server
AAA Server
Two-factor Authentication
+ Add
Edit
Remove
Reference
Join Domain
Remove From Domain
Search insights

AD Server Summary

Name	Server Address	Domain Name	Reference
No data			

Enter the Server Address and port for Server settings. (10.214.48.XX:389 in this example). Enter the domain name and the credentials for logging into the AD server, and click Apply.



Configuration

Name	Microsoft_AD	
Description		(Optional)

Server Settings

Server Address	10.214.48.[redacted]	(IP or FQDN)
Backup Server Address		(Optional) (IP or FQDN)
Port	389	(1-65535)
☐ Use SSL		
Search time limit	5	(1-300 seconds)
☑ Case-sensitive User Names		

Server Authentication

Domain Name	cso.com
User Name	Administrator
Password	••••••••••
Retype to Confirm	••••••••••

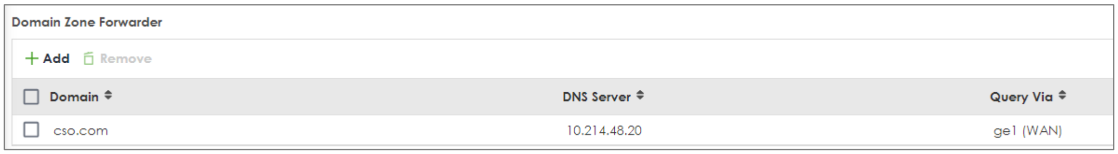
Configuration Validation

Please enter an existing user account in this server to validate the above settings.

User Name

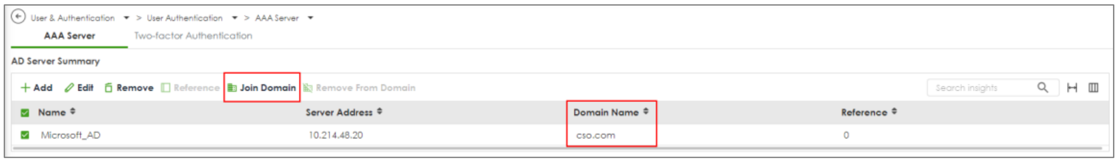
Join Domain

After the profile is created, go to System > DNS & DDNS > DNS, create a domain zone forwarder, and configure the DNS server IP as the IP address for the domain controller.



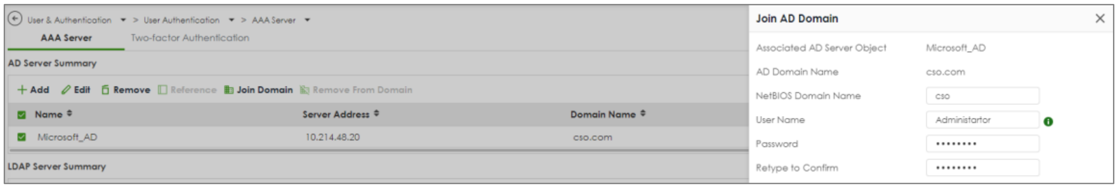
□ Domain	DNS Server	Query Via
□ cso.com	10.214.48.20	ge1 (WAN)

After the action above, go back to the profile page, tick it and click **Join Domain**



☑ Name	Server Address	Domain Name	Reference
☑ Microsoft_AD	10.214.48.20	cso.com	0

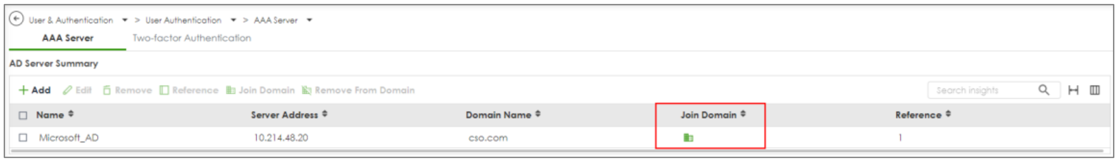
Enter NetBIOS Domain Name, Username and Password, click Apply.



☑ Name	Server Address	Domain Name
☑ Microsoft_AD	10.214.48.20	cso.com

Associated AD Server Object	Microsoft_AD
AD Domain Name	cso.com
NetBIOS Domain Name	cso
User Name	Administartor
Password	••••••••
Retype to Confirm	••••••••

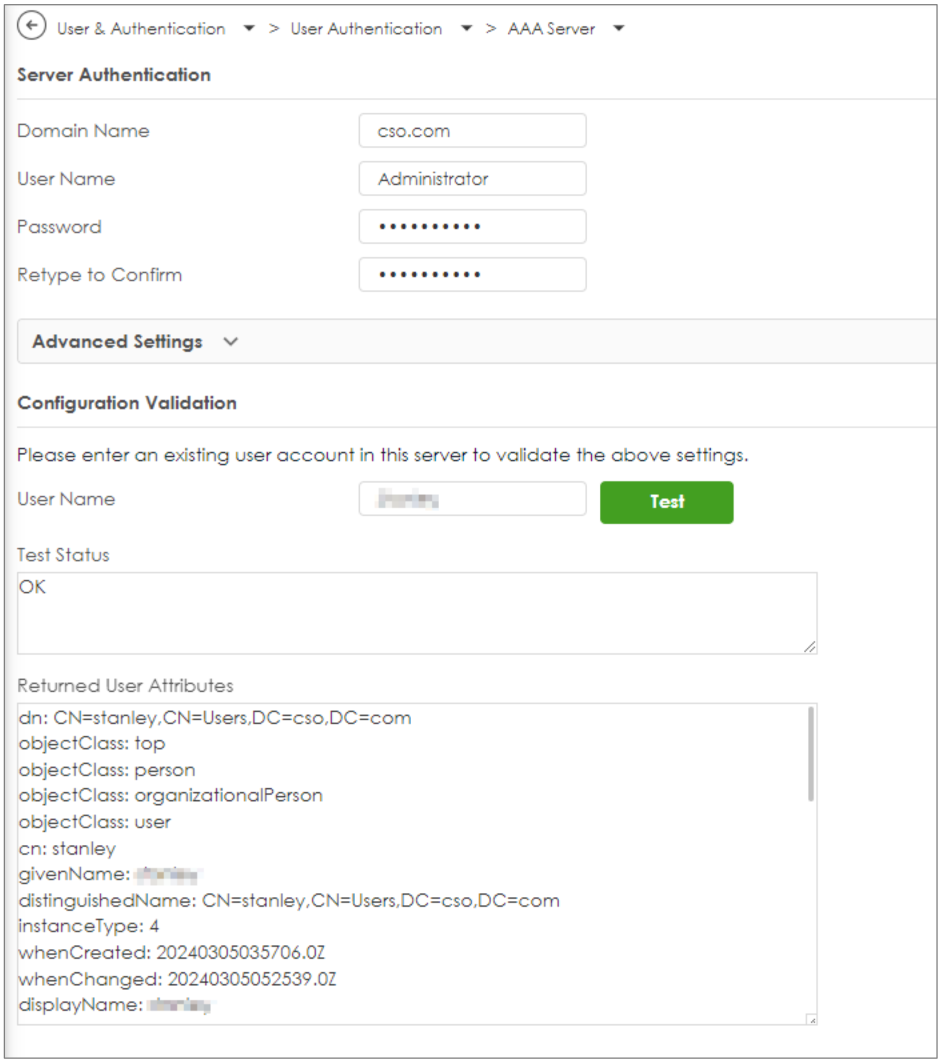
After join domain successfully, you can see this icon.



□ Name	Server Address	Domain Name	Join Domain	Reference
□ Microsoft_AD	10.214.48.20	cso.com	🟩	1

Test the Result

Scroll down to the bottom of the profile, you will see the Configuration Validation section, using a user account from the server specified above to test if the configuration is correct.



Server Authentication

Domain Name: cso.com
User Name: Administrator
Password: ••••••••••••
Retype to Confirm: ••••••••••••

Advanced Settings

Configuration Validation

Please enter an existing user account in this server to validate the above settings.

User Name: [redacted]

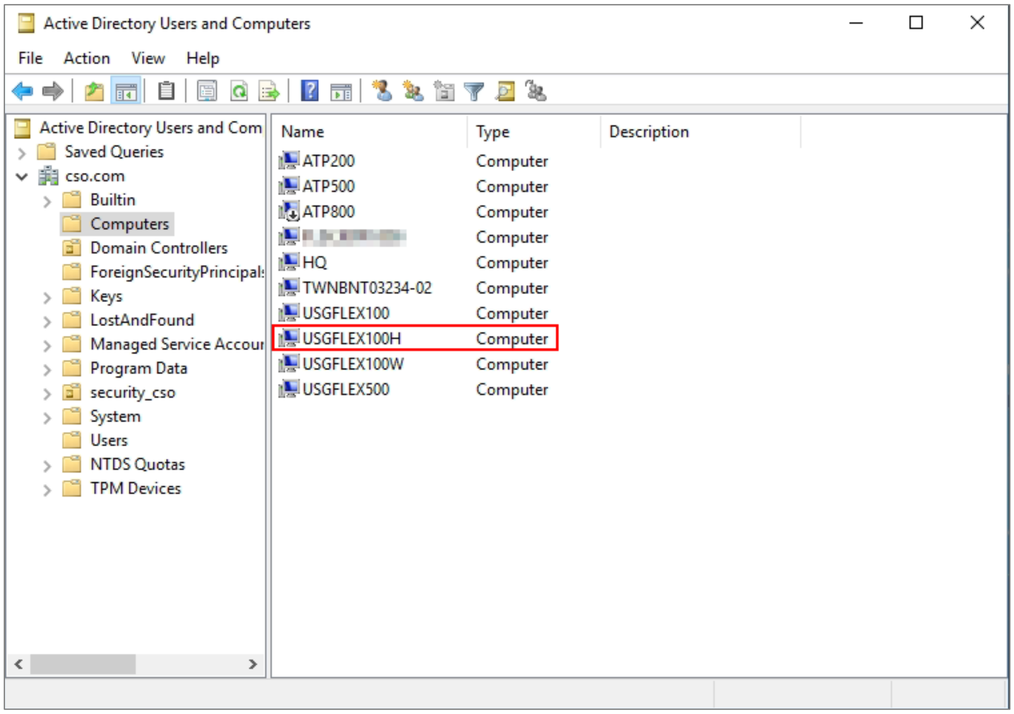
Test Status

```
OK
```

Returned User Attributes

```
dn: CN=stanley,CN=Users,DC=cso,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: stanley
givenName: [redacted]
distinguishedName: CN=stanley,CN=Users,DC=cso,DC=com
instanceType: 4
whenCreated: 20240305035706.0Z
whenChanged: 20240305052539.0Z
displayName: [redacted]
```

Check **computers** on Microsoft AD, you can see your firewall means join domain successfully.



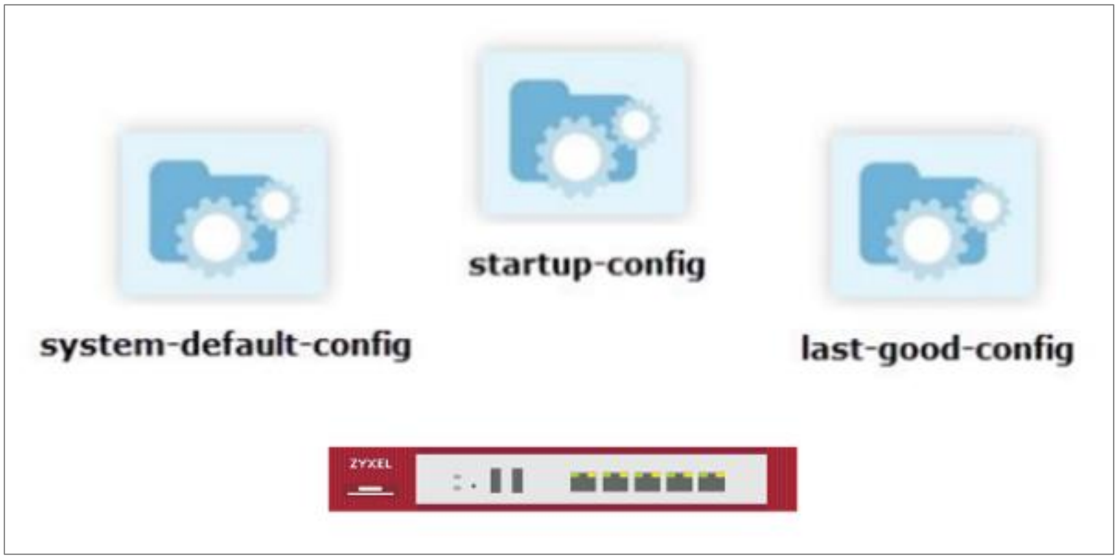
Active Directory Users and Com
- Saved Queries
- cso.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipal
  - Keys
  - LostAndFound
  - Managed Service Accour
  - Program Data
  - security_cso
  - System
  - Users
  - NTDS Quotas
  - TPM Devices

Name	Type	Description
ATP200	Computer	
ATP500	Computer	
ATP800	Computer	
[redacted]	Computer	
HQ	Computer	
TWNBNT03234-02	Computer	
USGFLEX100	Computer	
USGFLEX100H	Computer	
USGFLEX100W	Computer	
USGFLEX500	Computer	

Chapter 4- Maintenance

How to Manage Configuration Files

This is an example of how to rename, download, copy, apply and upload configuration files. Once your USG FLEX H device 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.



Note: The **system-default.conf** file contains the ZyWALL default settings. This configuration file is included when you upload a firmware package.

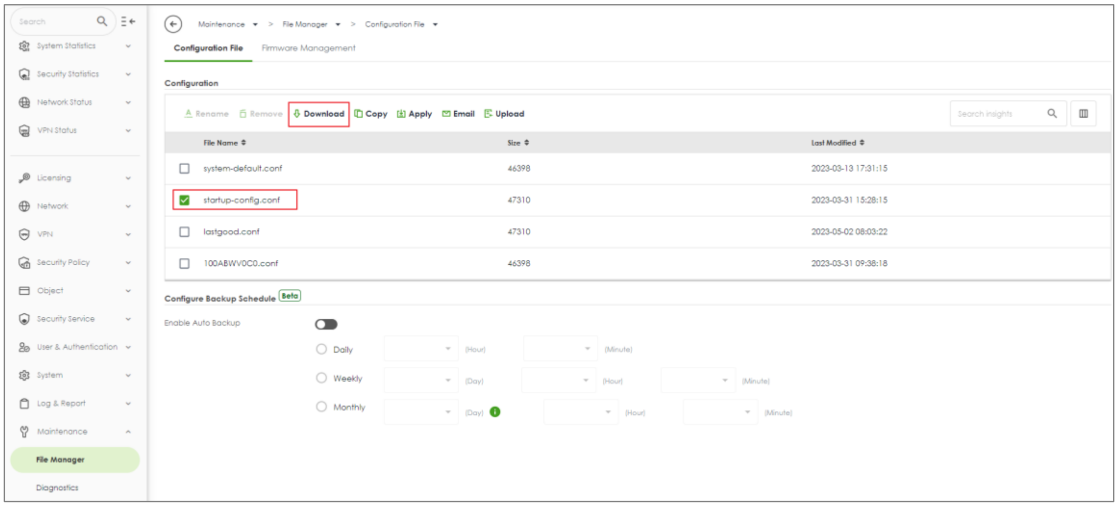
The **startup-config.conf** file is the configuration file that the ZyWALL is currently using. If you make and save changes during your management session, the changes are applied to this configuration file.

The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted.

Download the Configuration Files

Maintenance > File Manager > Configuration File

Select the statup-config.conf and click “Download”.



	File Name	Size	Last Modified
□	system-default.conf	46398	2023-03-13 17:31:15
☑	startup-config.conf	47310	2023-03-31 15:28:15
□	lastgood.conf	47310	2023-05-02 08:03:22
□	100ABWV0C0.conf	46398	2023-03-31 09:38:18

Configure Backup Schedule Beta

Enable Auto Backup

○ Daily (Hour) (Minute)

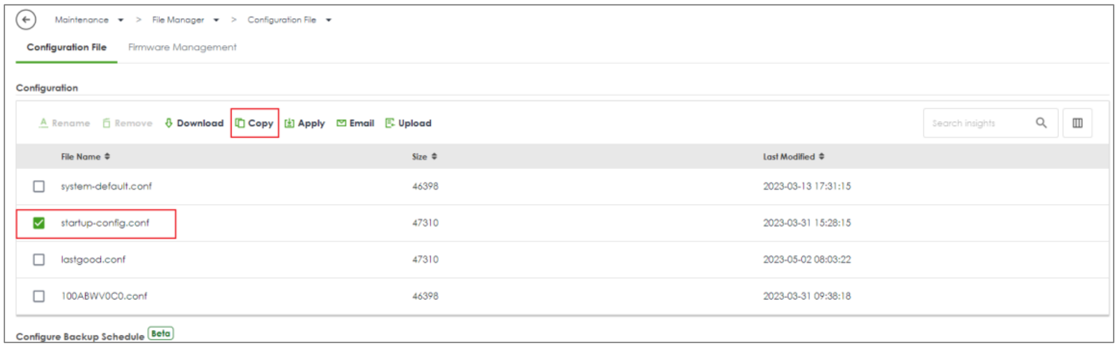
○ Weekly (Day) (Hour) (Minute)

○ Monthly (Day) (Hour) (Minute)

Copy the Configuration Files

Maintenance > File Manager > Configuration File

Select the file and click “Copy”.

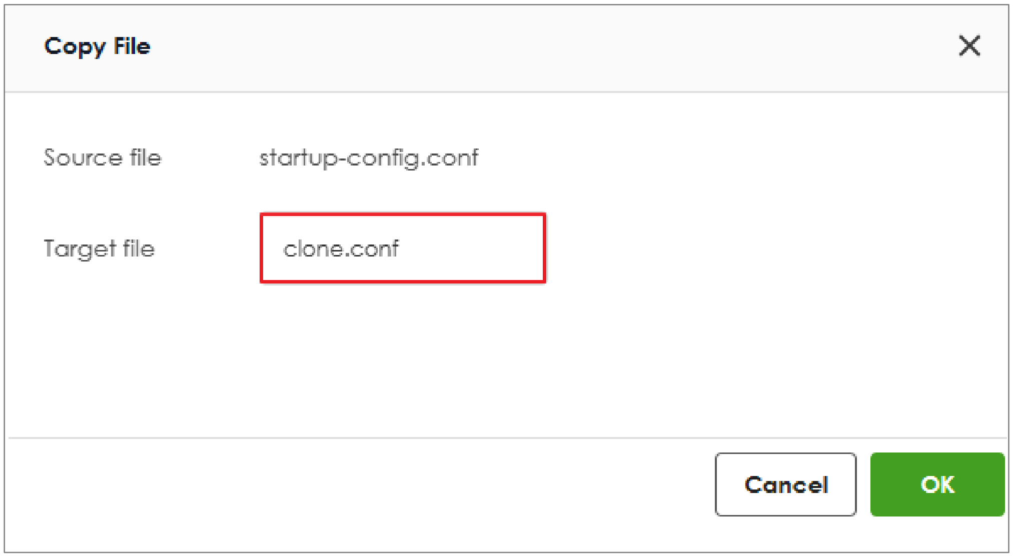


	File Name	Size	Last Modified
□	system-default.conf	46398	2023-03-13 17:31:15
☑	startup-config.conf	47310	2023-03-31 15:28:15
□	lastgood.conf	47310	2023-05-02 08:03:22
□	100ABWV0C0.conf	46398	2023-03-31 09:38:18

Configure Backup Schedule Beta

A pop-up screen will appear allowing you to edit the Target file name.

The file as format: [a-zA-Z0-9~_.=-]{1,63}.conf



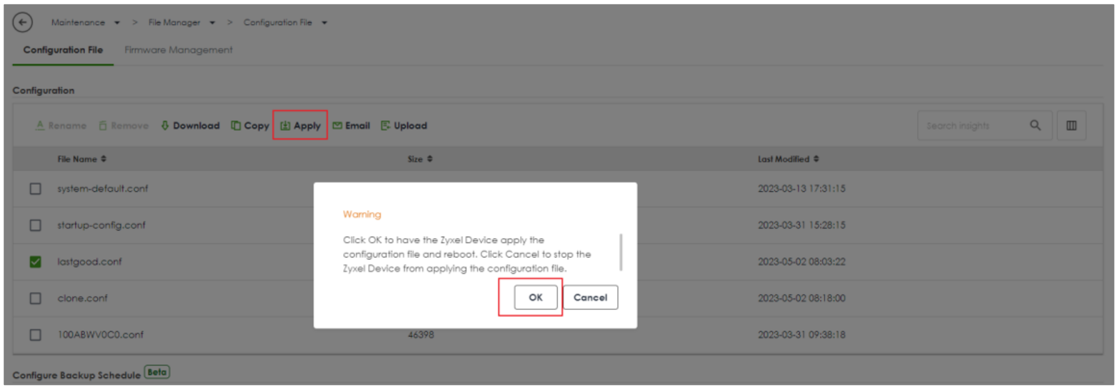
Copy File

Source file	startup-config.conf
Target file	clone.conf

Apply the Configuration Files

Maintenance > File Manager > Configuration File

Select a specific configuration file to have ZyWALL use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL 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 the valid configuration. Click "OK", ZyWALL will reboot automatically.



	File Name	Size	Last Modified
□	system-default.conf		2023-03-13 17:31:15
□	startup-config.conf		2023-03-31 15:28:15
☑	lastgood.conf		2023-05-02 08:03:22
□	clone.conf		2023-05-02 08:18:00
□	100ABWV0C0.conf	46398	2023-03-31 09:38:18

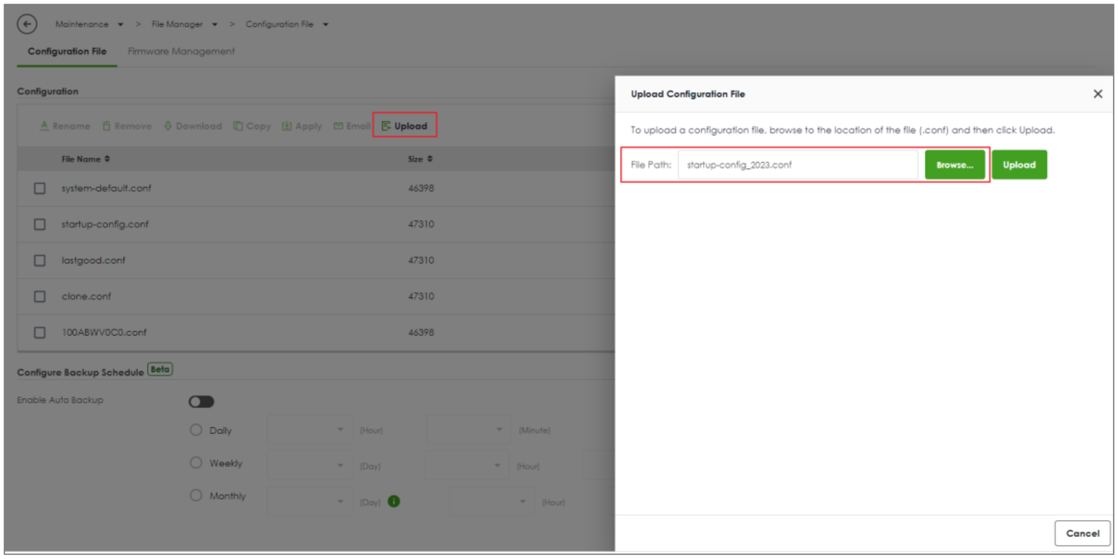
Warning

Click OK to have the Zyxel Device apply the configuration file and reboot. Click Cancel to stop the Zyxel Device from applying the configuration file.

Upload the Configuration Files

Maintenance > File Manager > Configuration File

Select Upload and Browse a new or previously saved configuration file from your computer to the USG FLEX H device. You cannot upload a configuration file which has the same name in the device.



	File Name	Size
□	system-default.conf	46398
□	startup-config.conf	47310
□	lastgood.conf	47310
□	clone.conf	47310
□	100ABWV0C0.conf	46398

Enable Auto Backup

○ Daily (Hour) (Minute)

○ Weekly (Day) (Hour)

○ Monthly (Day) (Hour)

To upload a configuration file, browse to the location of the file (.conf) and then click Upload.

File Path: startup-config_2023.conf

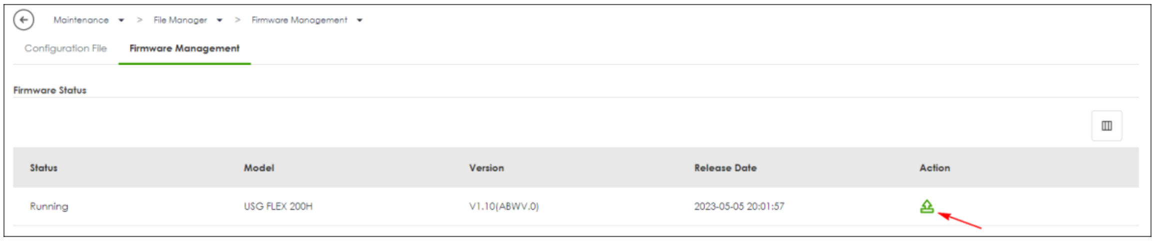
How to Manage Firmware

For management convenience, administrators have the capability to upgrade the firmware effortlessly either from a PC or using the cloud firmware upgrade function. Additionally, the firmware upgrade can be scheduled to occur automatically within a preconfigured timeframe.

Local Firmware Upgrade

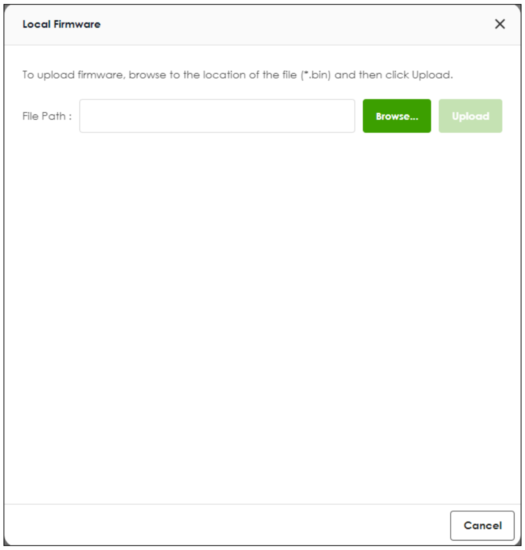
You can click the green button to upgrade firmware by browsing the .bin file from your PC.

Note: You can download the latest firmware version from myZyxel.com portal. (https://portal.myzyxel.com/my/firmwares)



Firmware Status

Status	Model	Version	Release Date	Action
Running	USG FLEX 200H	V1.10(ABWV.0)	2023-05-05 20:01:57	



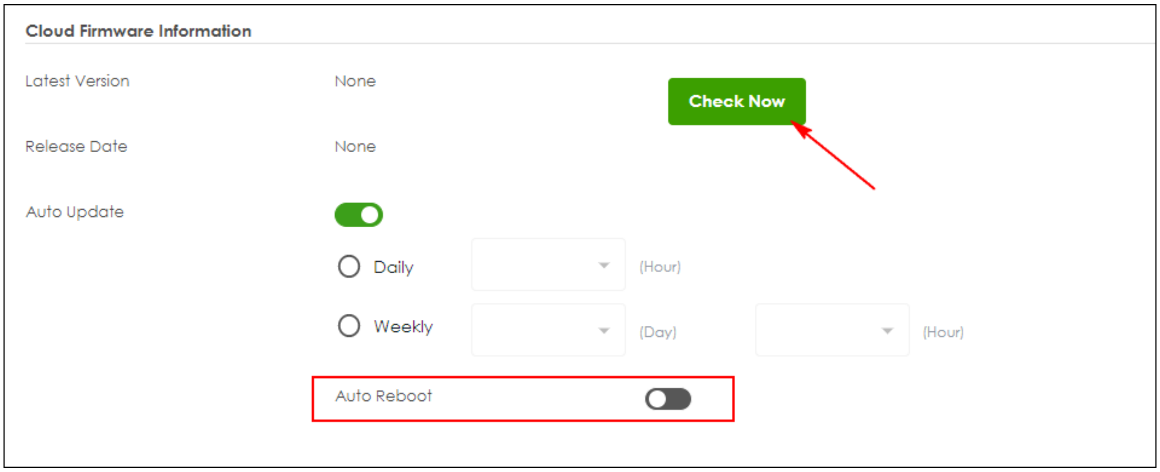
To upload firmware, browse to the location of the file (*.bin) and then click Upload.

File Path :

Cloud Firmware Upgrade

The cloud firmware upgrade function allows you to verify the most recent firmware version by clicking the "Check New" button.

Furthermore, the "Auto Update" feature can be activated to automatically download firmware to your firewall first and reboot your device within a specified time frame.



Cloud Firmware Information

Latest Version None

Release Date None

Auto Update ●

○ Daily (Hour)

○ Weekly (Day) (Hour)

Auto Reboot ○

Chapter 5- Others

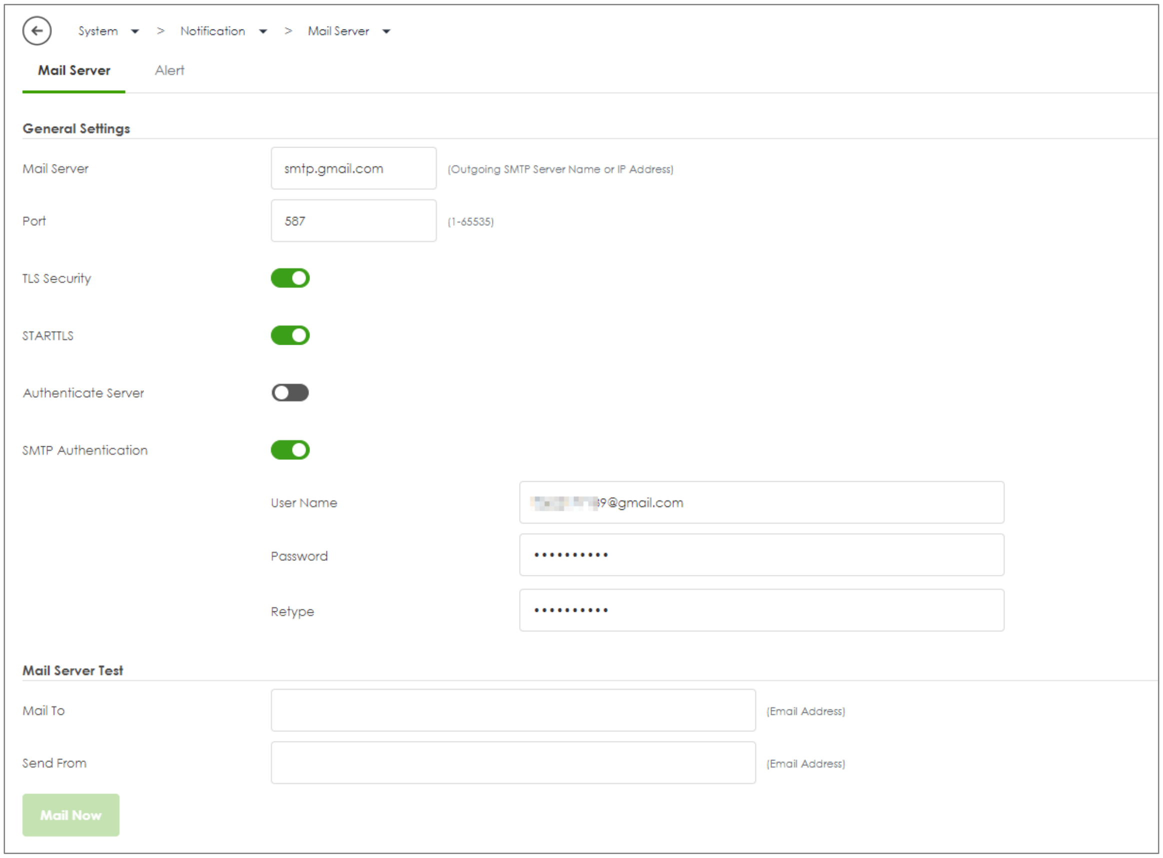
How to Setup and Configure Daily Report

Administrators can efficiently oversee gateway events by reviewing the Daily Report for management purposes. This example demonstrates how to set up the Daily Report, including the option to select specific log messages for inclusion. Once configured, you can utilize "Send Report Now" to assess your device's current status and establish a schedule for receiving the 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 USG FLEX 500H (Firmware Version: uOS 1.10).

Set Up the Mail Server

Before setting up the Email Daily Report, we will be required to set up a mail server. Navigate to the System > Notification > Mail Server. Input your Mail Server and port, and activate TLS Security and STARTTLS in their respective fields. Next, complete your account and password for SMTP Authentication as the Sender.



General Settings

Mail Server: smtp.gmail.com (Outgoing SMTP Server Name or IP Address)

Port: 587 (1-65535)

TLS Security: On

STARTTLS: On

Authenticate Server: Off

SMTP Authentication: On

User Name: [redacted]9@gmail.com

Password: ••••••••••

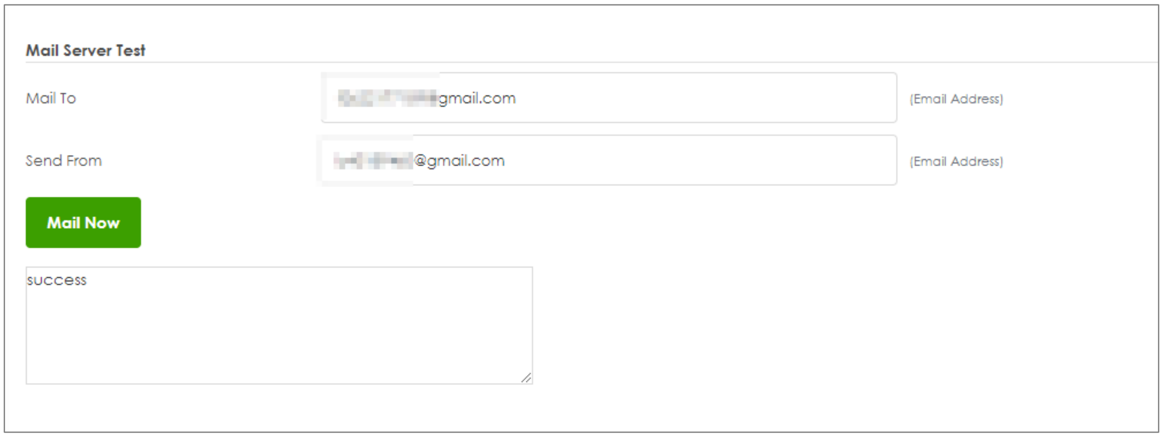
Retype: ••••••••••

Mail Server Test

Mail To: (Email Address)

Send From: (Email Address)

You can verify the correctness of the settings by using the Mail Server Test below. If it is successful, you will receive an email.

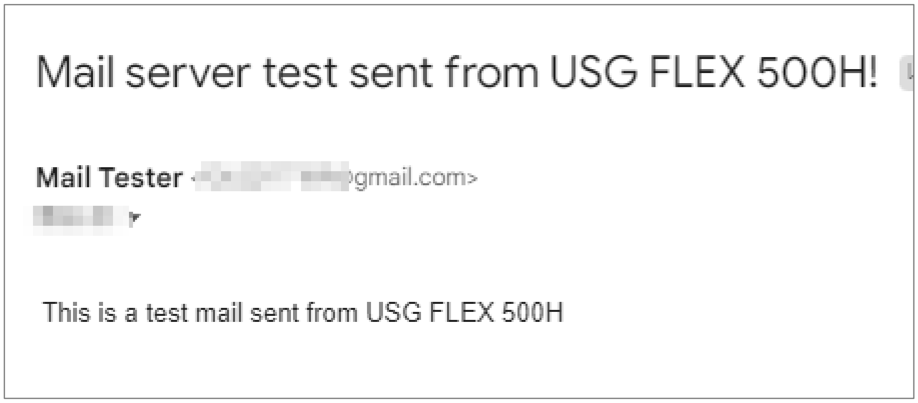


Mail Server Test

Mail To: [redacted]gmail.com (Email Address)

Send From: [redacted]@gmail.com (Email Address)

success



Mail server test sent from USG FLEX 500H!

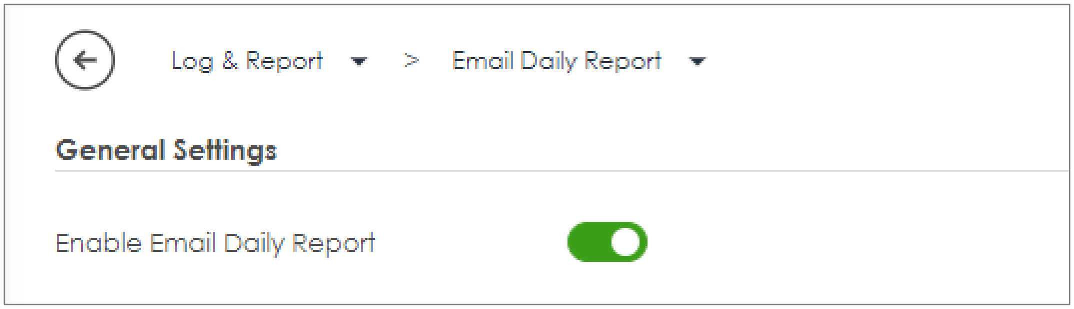
Mail Tester <[redacted]gmail.com>

[redacted]

This is a test mail sent from USG FLEX 500H

Set Up Email Daily Report

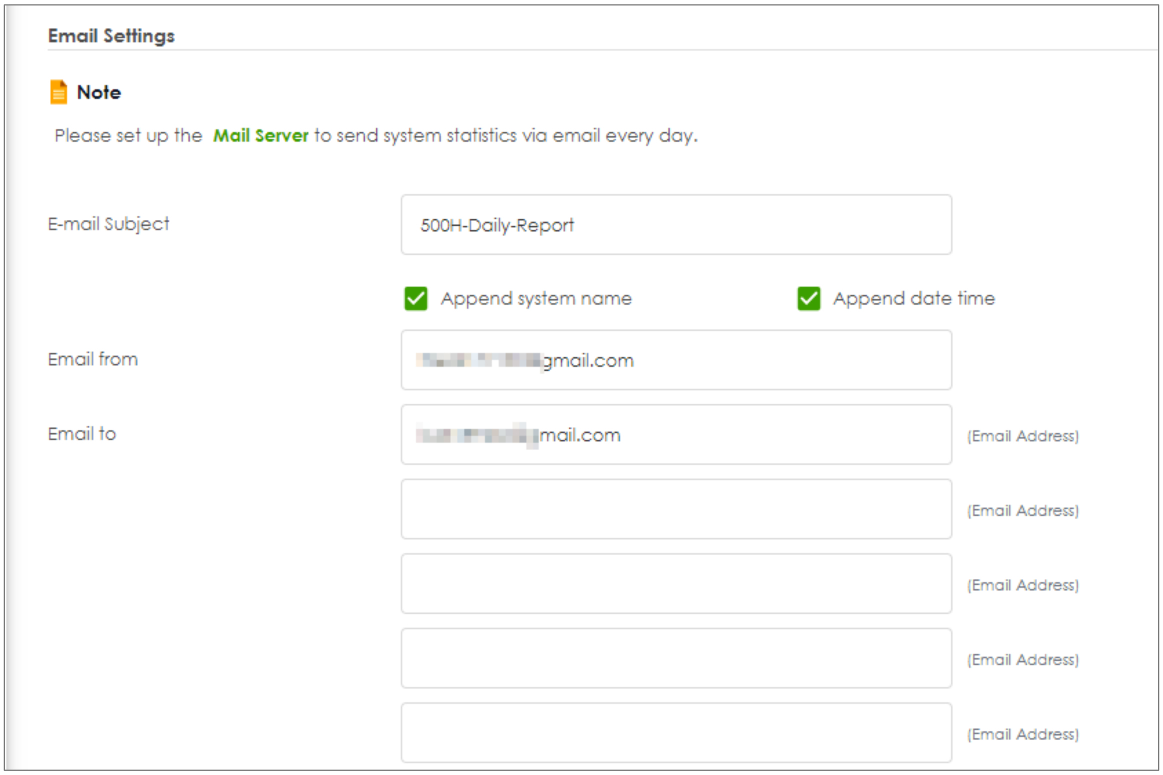
Navigate to Log & Report > Email Daily Report. Enable your Email Daily Report



General Settings

Enable Email Daily Report: on

Type your Email Subject and your Sender and Receiver in the field.



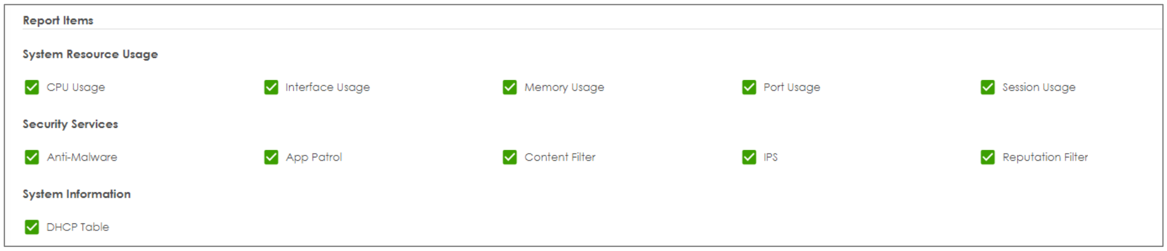
Email Settings

Note

Please set up the **Mail Server** to send system statistics via email every day.

E-mail Subject	500H-Daily-Report
	☑ Append system name ☑ Append date time
Email from	[redacted]gmail.com
Email to	[redacted]mail.com (Email Address)
	(Email Address)
	(Email Address)
	(Email Address)
	(Email Address)

Scroll down the page and go to Report Items to set up which messages you would like to include in the daily report



Report Items

System Resource Usage

☑ CPU Usage ☑ Interface Usage ☑ Memory Usage ☑ Port Usage ☑ Session Usage

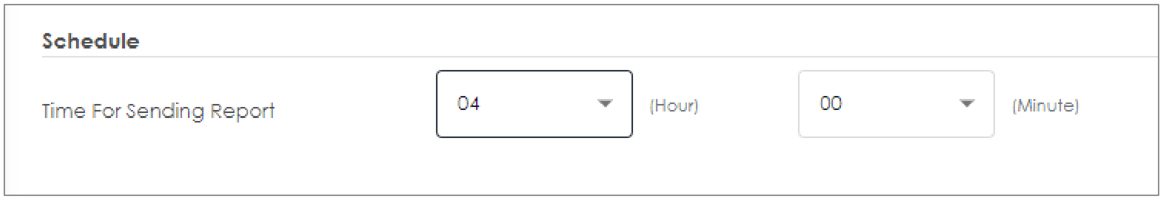
Security Services

☑ Anti-Malware ☑ App Patrol ☑ Content Filter ☑ IPS ☑ Reputation Filter

System Information

☑ DHCP Table

You can set up a Schedule at the bottom of the page

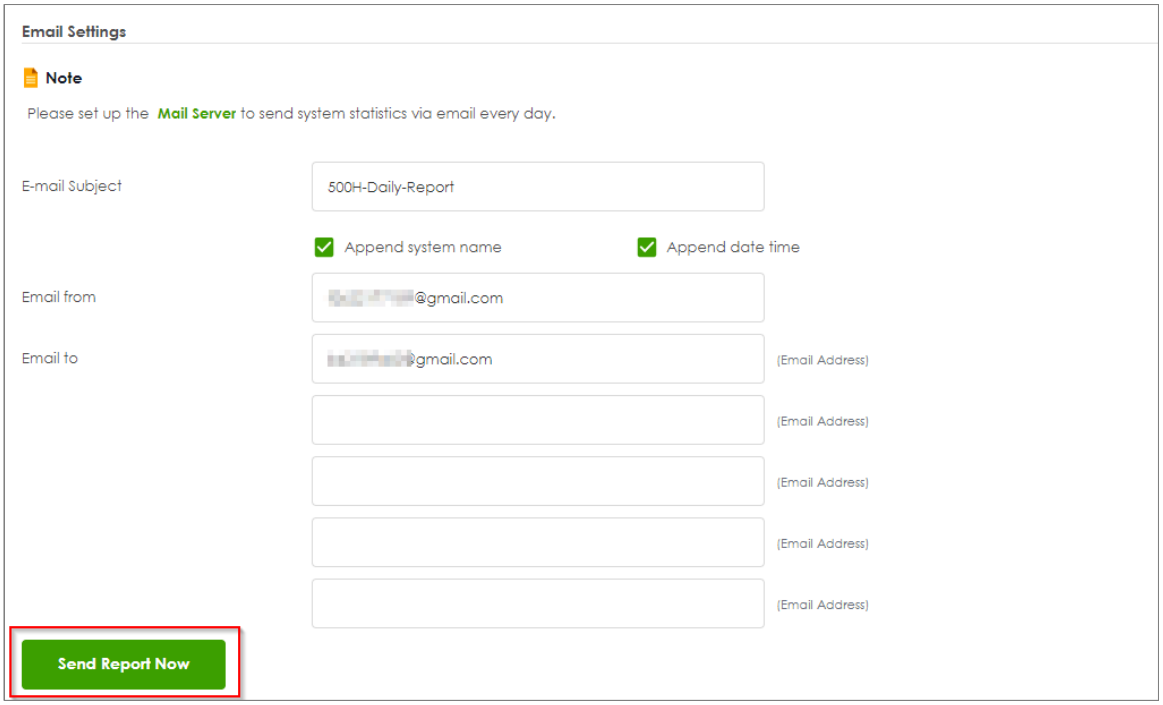


Schedule

Time For Sending Report: 04 (Hour) 00 (Minute)

Test the Email Daily Report

To confirm if the daily report has been set up successfully, click "Send Report Now."

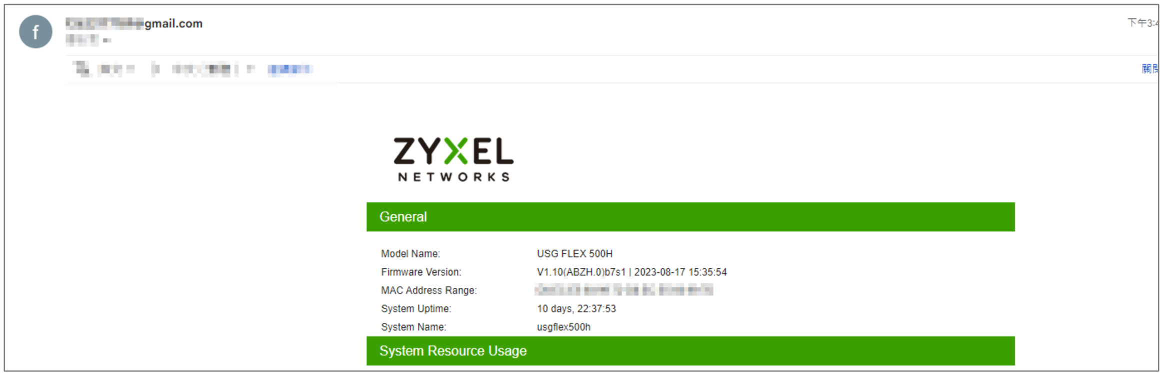


Email Settings

Note

Please set up the **Mail Server** to send system statistics via email every day.

E-mail Subject	500H-Daily-Report	
	☑ Append system name ☑ Append date time	
Email from	[redacted]@gmail.com	
Email to	[redacted]gmail.com	(Email Address)
		(Email Address)
		(Email Address)
		(Email Address)
		(Email Address)



[redacted]gmail.com [redacted]

[redacted]

下午3:

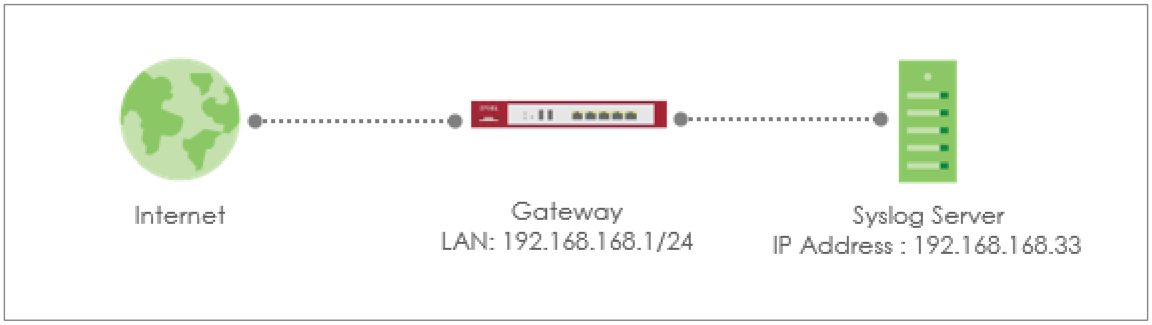
General

Model Name:	USG FLEX 500H
Firmware Version:	V1.10(ABZH.0)b7s1 | 2023-08-17 15:35:54
MAC Address Range:	[redacted]
System Uptime:	10 days, 22:37:53
System Name:	usgflex500h

System Resource Usage

How to Setup and Send Logs to a Syslog Server

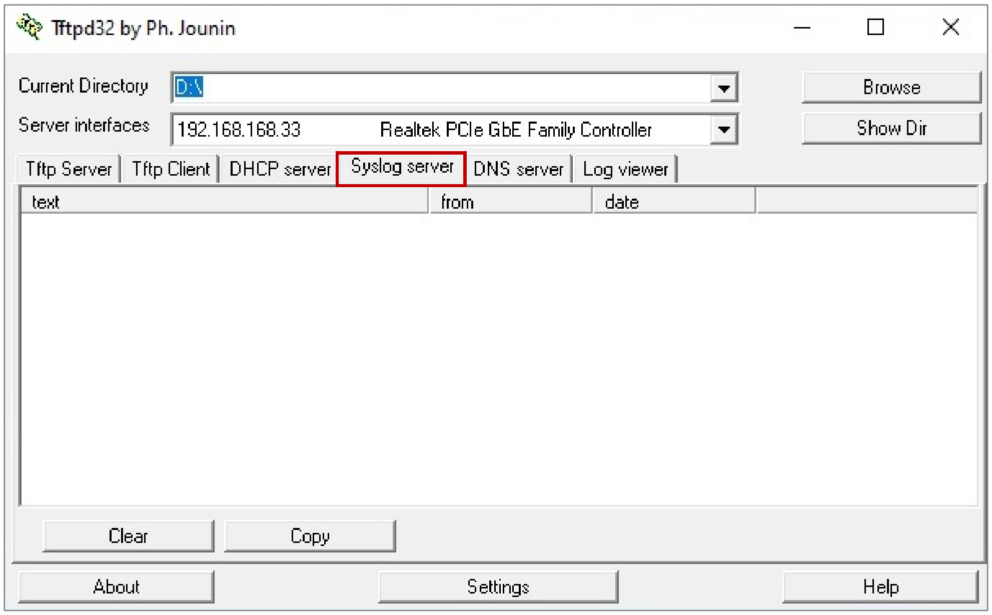
For management purposes, administrators can easily monitor events occurring on the gateway by reading the syslog. This example shows how to send logs to a syslog server. You can also specify which log messages to syslog server. When the syslog server is configured, you will receive the real time system 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 USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up the Syslog Server

Install the syslog server. In this example, we use tftpd32 as the syslog server.



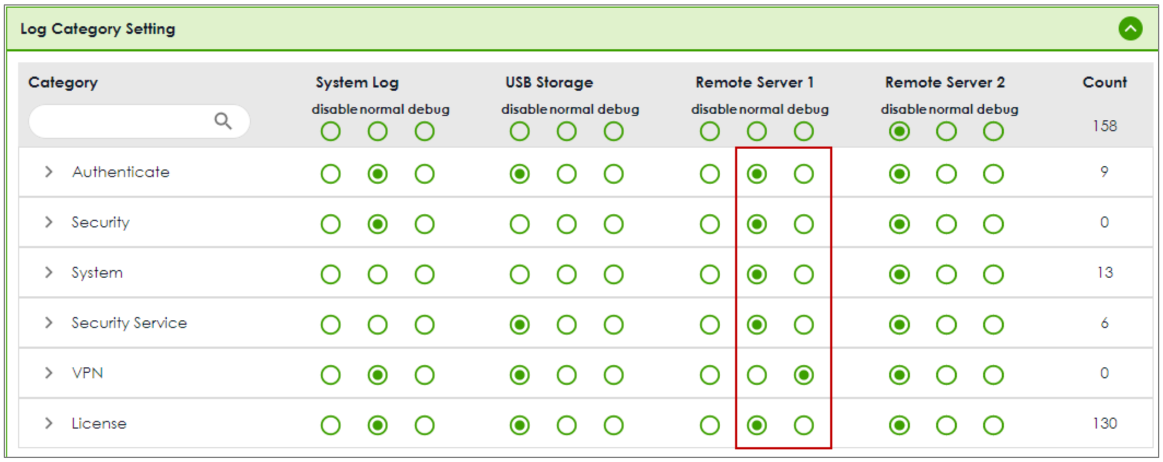
Tftpd32 by Ph. Jounin

Current Directory: D:\

Server interfaces: 192.168.168.33 Realtek PCIe GbE Family Controller

Set Up Remote Server Setting on the Gateway

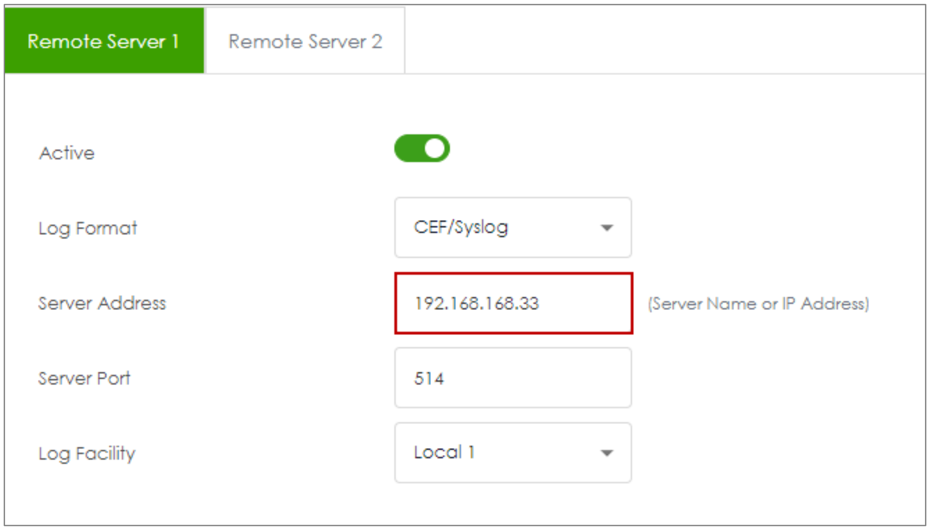
Go to Log & Report > Log Settings > Log Category Setting. Use the drop-down list to select what information you want to log from each log category.



Log Category Setting

Category	System Log			USB Storage			Remote Server 1			Remote Server 2			Count
	disable	normal	debug	disable	normal	debug	disable	normal	debug	disable	normal	debug	
	○	○	○	○	○	○	○	○	○	●	○	○	158
Authenticate	○	●	○	●	○	○	○	●	○	●	○	○	9
Security	○	●	○	○	○	○	○	●	○	●	○	○	0
System	○	○	○	○	○	○	○	●	○	●	○	○	13
Security Service	○	○	○	●	○	○	○	●	○	●	○	○	6
VPN	○	●	○	●	○	○	○	○	●	●	○	○	0
License	○	●	○	●	○	○	○	●	○	●	○	○	130

Go to Log & Report > Log Settings > Remote Syslog Server. Set Log Format to be CEF/Syslog and type the server name or the IP address of the syslog server. Turn on "Active" to send log information to the server.



Active ●

Log Format: CEF/Syslog

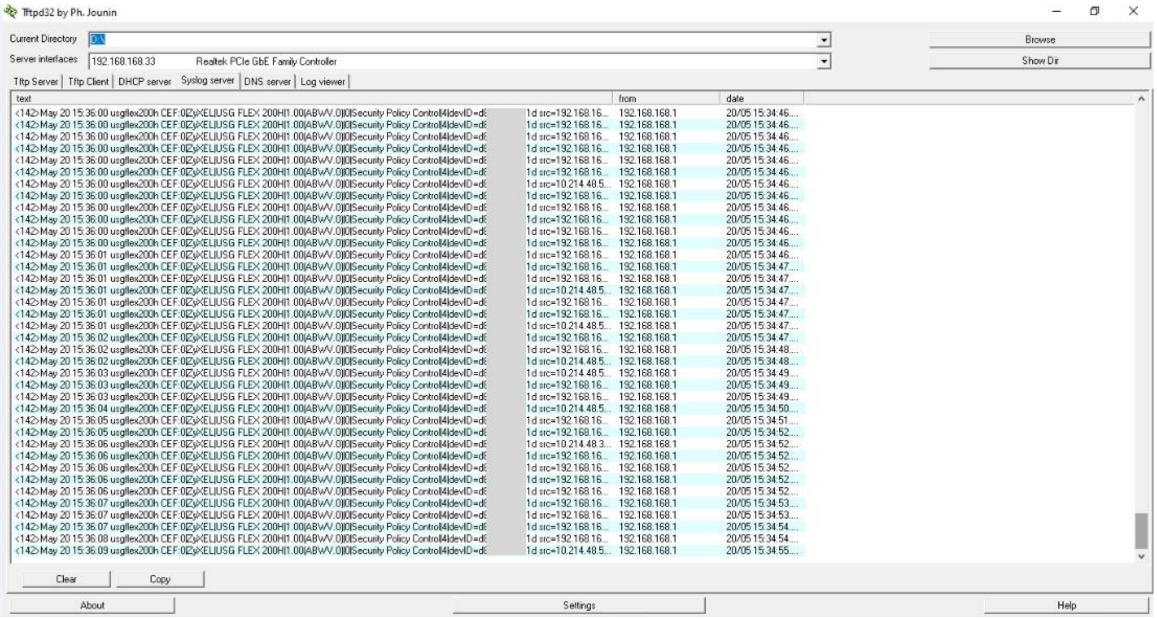
Server Address: 192.168.168.33 (Server Name or IP Address)

Server Port: 514

Log Facility: Local 1

Test the Remote Syslog Server

Check logs on the syslog server.



Current Directory: D:\

Server interfaces: 192.168.168.33 Realtek PCIe GbE Family Controller

```
text                                                                                                                   from           date
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=10.214.48.5...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:00 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:01 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:46....
<142>May 20 15:36:01 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:47....
<142>May 20 15:36:01 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:47....
<142>May 20 15:36:01 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=10.214.48.5...  192.168.168.1  20/05 15:34:47....
<142>May 20 15:36:01 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:47....
<142>May 20 15:36:01 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:47....
<142>May 20 15:36:01 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=10.214.48.5...  192.168.168.1  20/05 15:34:47....
<142>May 20 15:36:02 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:47....
<142>May 20 15:36:02 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:48....
<142>May 20 15:36:02 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=10.214.48.5...  192.168.168.1  20/05 15:34:48....
<142>May 20 15:36:03 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=10.214.48.5...  192.168.168.1  20/05 15:34:49....
<142>May 20 15:36:03 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:49....
<142>May 20 15:36:03 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:49....
<142>May 20 15:36:04 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=10.214.48.5...  192.168.168.1  20/05 15:34:50....
<142>May 20 15:36:05 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:51....
<142>May 20 15:36:05 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:52....
<142>May 20 15:36:06 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=10.214.48.3...  192.168.168.1  20/05 15:34:52....
<142>May 20 15:36:06 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:52....
<142>May 20 15:36:06 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:52....
<142>May 20 15:36:06 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:52....
<142>May 20 15:36:06 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:52....
<142>May 20 15:36:07 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:53....
<142>May 20 15:36:07 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:53....
<142>May 20 15:36:07 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:54....
<142>May 20 15:36:08 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=192.168.16...  192.168.168.1  20/05 15:34:54....
<142>May 20 15:36:09 usgflex200h CEF:0|ZyXEL|USG FLEX 200H|1.00|ABWV.0|0|Security Policy Control|4|devID=d[redacted]1d src=10.214.48.5...  192.168.168.1  20/05 15:34:55....
```

How to Setup and Send logs to the USB storage

The USG FLEX H Series device can use a connected USB device to store the system log and other diagnostic information. This example shows how to use the USB device to store the system log information.

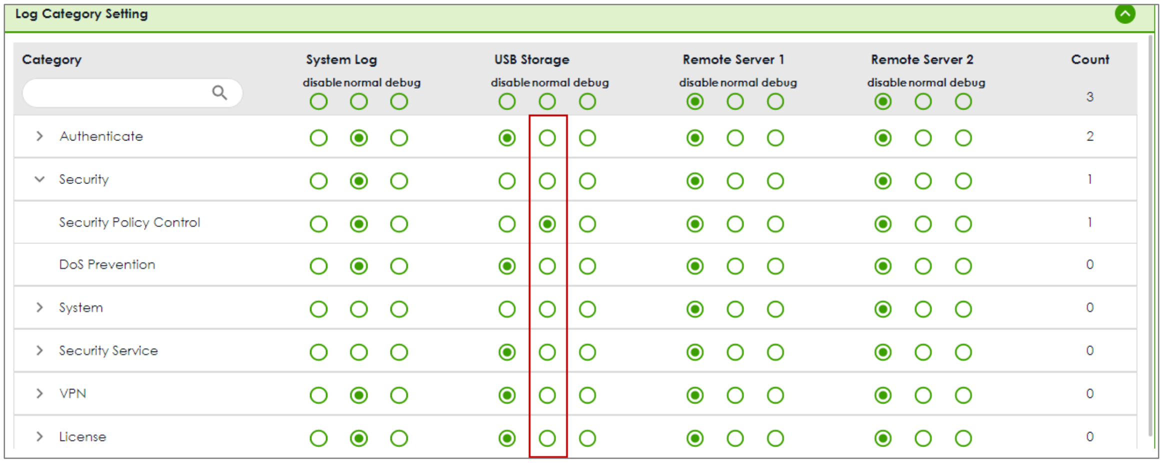
Note: The USB storage must allow writing (it cannot be read-only) and use the FAT16, FAT32, EXT2, or EXT3 file system. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10). The USB port can provide max. 900mA output power. You might need to connect external power for the USB storage device.

USB Storage device

Plug in an external USB storage device. USB storage devices with FAT16, FAT32, EXT2, or EXT3 file systems are supported to be connected to the USB port of the gateway.

Set Up the USB storage on the Gateway

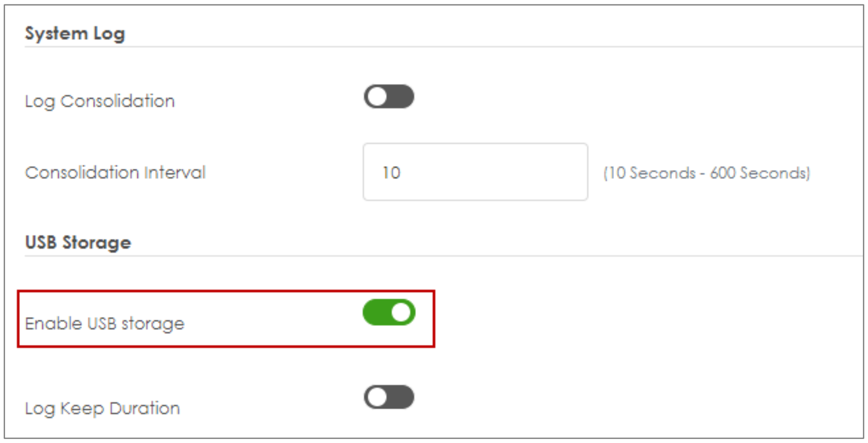
Go to Log & Report > Log Settings > Log Category Setting. Use the drop-down list to select what information you want to log from each log category.



Log Category Setting

Category	System Log			USB Storage			Remote Server 1			Remote Server 2			Count
	disable	normal	debug	disable	normal	debug	disable	normal	debug	disable	normal	debug	
	○	○	○	○	○	○	●	○	○	●	○	○	3
› Authenticate	○	●	○	●	○	○	●	○	○	●	○	○	2
⌄ Security	○	●	○	○	○	○	●	○	○	●	○	○	1
Security Policy Control	○	●	○	○	●	○	●	○	○	●	○	○	1
DoS Prevention	○	●	○	●	○	○	●	○	○	●	○	○	0
› System	○	○	○	○	○	○	●	○	○	●	○	○	0
› Security Service	○	○	○	●	○	○	●	○	○	●	○	○	0
› VPN	○	●	○	●	○	○	●	○	○	●	○	○	0
› License	○	●	○	●	○	○	●	○	○	●	○	○	0

Go to Log & Report > Log Settings > USB Storage. Turn on "Enable USB storage" to store the system logs on a USB device.



System Log

Log Consolidation: off

Consolidation Interval: 10 (10 Seconds - 600 Seconds)

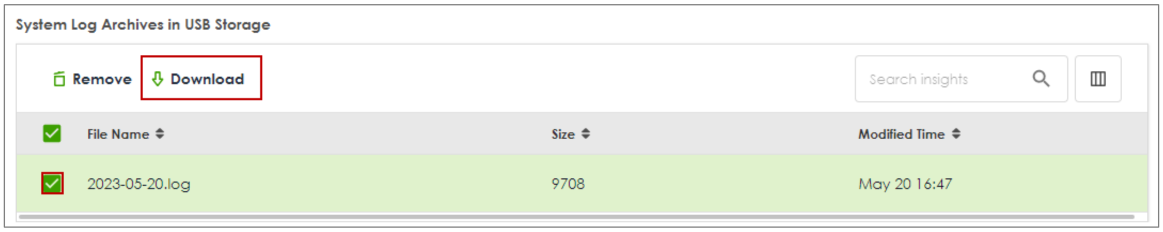
USB Storage

Enable USB storage: on

Log Keep Duration: off

Check the USG Log Files

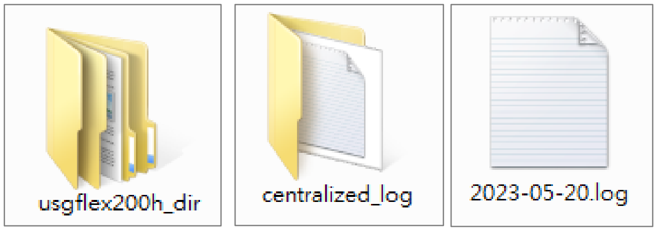
Go to Maintenance > Diagnostics > System Log. Select a file and click "Download" to view the log.



System Log Archives in USB Storage

☑	File Name	Size	Modified Time
☑	2023-05-20.log	9708	May 20 16:47

You can also connect the USB storage to PC and find the files in the following path.
\Model Name_dir\centralized_log\YYYY-MM-DD.log



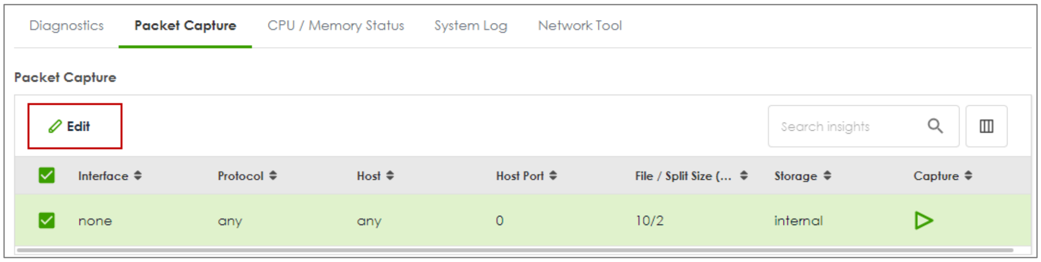
How to Perform and Use the Packet Capture Feature

This example shows how to use the Packet Capture feature to capture network traffic going through the device's interfaces. Studying these packet captures may help you analyze network problems.

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 200H (Firmware Version: uOS 1.10).

Set Up the Packet Capture Feature

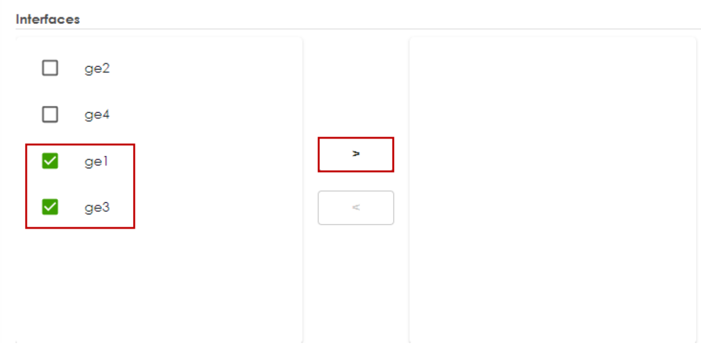
7. Go to Maintenance > Diagnostics > Packet Capture. Select "none" and click "Edit".



Packet Capture

☑	Interface	Protocol	Host	Host Port	File / Split Size (...	Storage	Capture
☑	none	any	any	0	10/2	internal	▷

8. In Interfaces, select interfaces for which to capture packets and click the right arrow button to move them to the list.



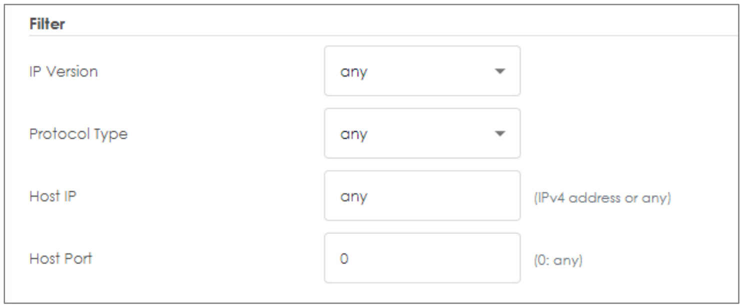
Interfaces

☐ ge2
☐ ge4
☑ ge1
☑ ge3

9. In Filter, select IP Version for which to capture packets. Select any to capture packets for all IP versions.

   Select the Protocol Type of traffic for which to capture packets. Select any to capture packets for all types of traffic.

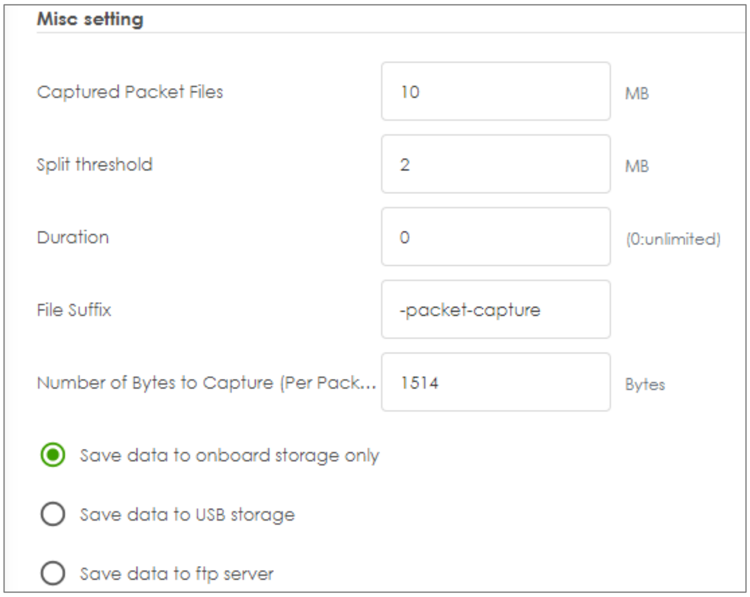
   Select a Host IP address object for which to capture packets. Select any to capture packets for all hosts. Select User Defined to be able to enter an IP address.



Filter

IP Version	any	
Protocol Type	any	
Host IP	any	(IPv4 address or any)
Host Port	0	(0: any)

10. In Misc setting, select "Save data to onboard storage only", "Save data to USB storage" or "Save data to ftp server".



Misc setting

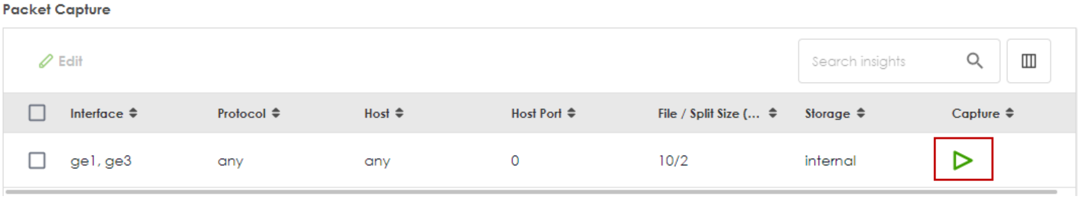
Captured Packet Files	10	MB
Split threshold	2	MB
Duration	0	(0:unlimited)
File Suffix	-packet-capture	
Number of Bytes to Capture (Per Pack...	1514	Bytes

● Save data to onboard storage only

○ Save data to USB storage

○ Save data to ftp server

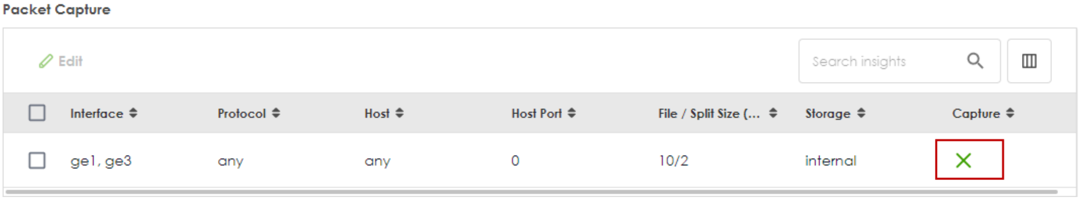
11. Click the icon to start capturing packets.



Packet Capture

□	Interface	Protocol	Host	Host Port	File / Split Size (...	Storage	Capture
□	ge1, ge3	any	any	0	10/2	internal	▷

12. Click the icon to stop capturing packets.

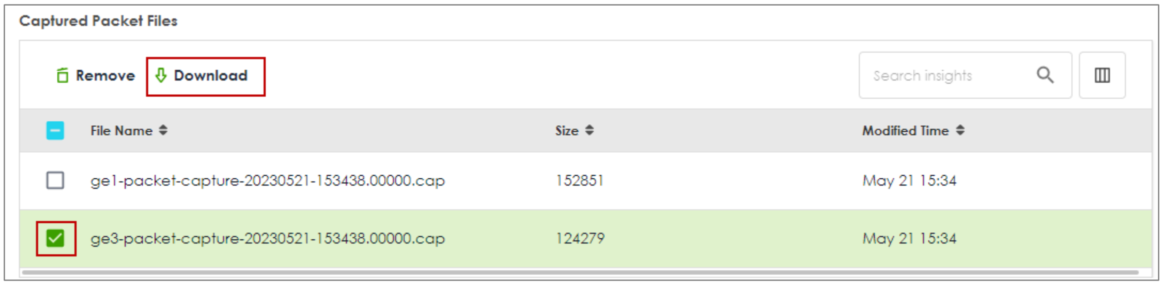


Packet Capture

□	Interface	Protocol	Host	Host Port	File / Split Size (...	Storage	Capture
□	ge1, ge3	any	any	0	10/2	internal	✕

Download the Captured Packet Files

In Captured Packet Files, select the file and click Download. You can download one file only at once. The captured files are named according to the date and time of capture, so new files will not overwrite existing ones.



Captured Packet Files

☐	File Name	Size	Modified Time
□	ge1-packet-capture-20230521-153438.00000.cap	152851	May 21 15:34
☑	ge3-packet-capture-20230521-153438.00000.cap	124279	May 21 15:34

Check Real-Time traffic using command

Traffic-capture is a CLI-based packet capturing tool on the device. It can be used to sniffer and analyze network traffic by intercepting and displaying packets transmitted in the network interface.

Syntax:

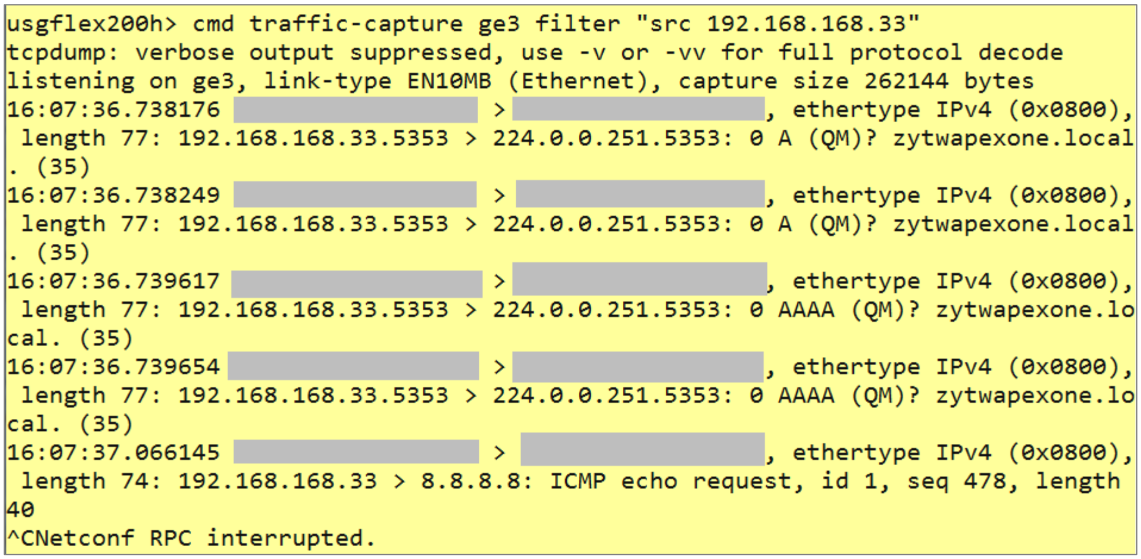
cmd traffic-capture <interface name>

cmd traffic-capture <interface name> filter <icmp | tcp | udp | arp | esp>

cmd traffic-capture <interface name> filter “src <ip address>”

cmd traffic-capture <interface name> filter “port <port number>”

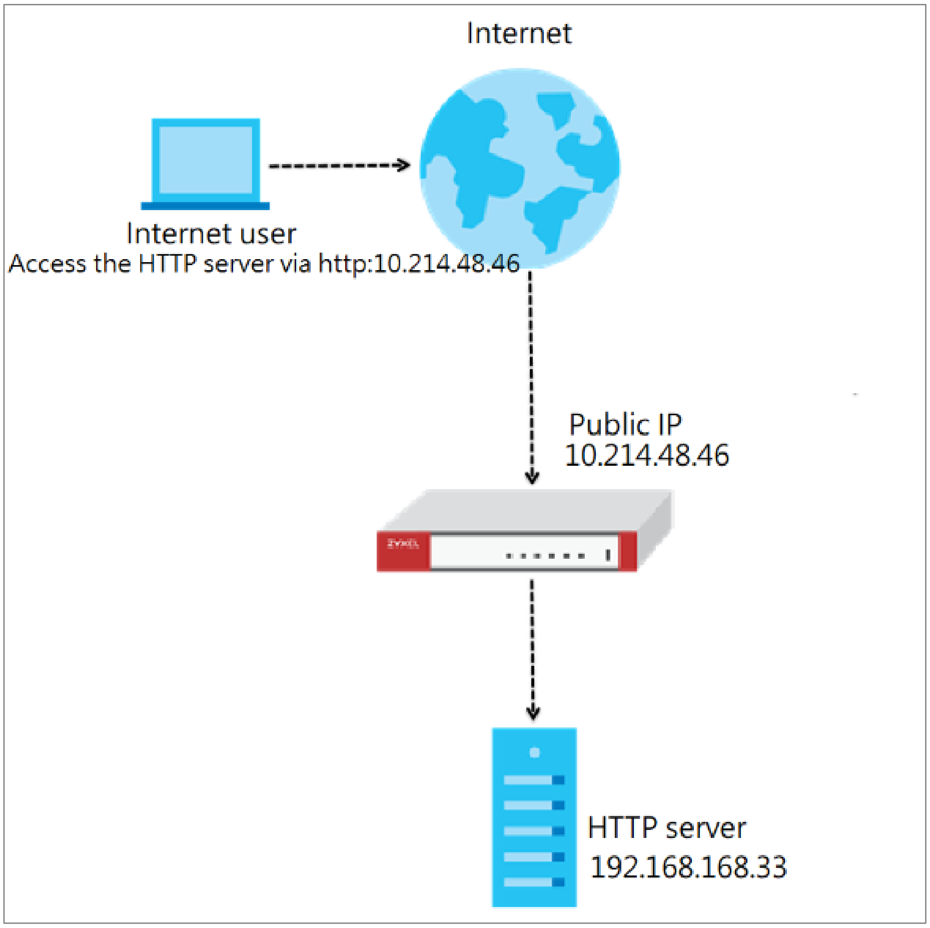
cmd traffic-capture <interface name> filter “host <ip address> and port <port number>”



```
usgflex200h> cmd traffic-capture ge3 filter "src 192.168.168.33"
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge3, link-type EN10MB (Ethernet), capture size 262144 bytes
16:07:36.738176 [redacted] > [redacted], ethertype IPv4 (0x0800),
 length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 A (QM)? zytwapexone.local
. (35)
16:07:36.738249 [redacted] > [redacted], ethertype IPv4 (0x0800),
 length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 A (QM)? zytwapexone.local
. (35)
16:07:36.739617 [redacted] > [redacted], ethertype IPv4 (0x0800),
 length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 AAAA (QM)? zytwapexone.lo
cal. (35)
16:07:36.739654 [redacted] > [redacted], ethertype IPv4 (0x0800),
 length 77: 192.168.168.33.5353 > 224.0.0.251.5353: 0 AAAA (QM)? zytwapexone.lo
cal. (35)
16:07:37.066145 [redacted] > [redacted], ethertype IPv4 (0x0800),
 length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 478, length
40
^CNetconf RPC interrupted.
```

How to Allow Public Access to a Server Behind USG FLEX H

Here is an example of allowing access to the internal server behind a USG FLEX H device with network address translation (NAT). Internet users can access the server directly by its public IP address and a NAT rule will forward traffic from the internet to the local server in the intranet.



Set Up the NAT

Go to Network > NAT, and click +Add to create a NAT rule.

- Input the rule name

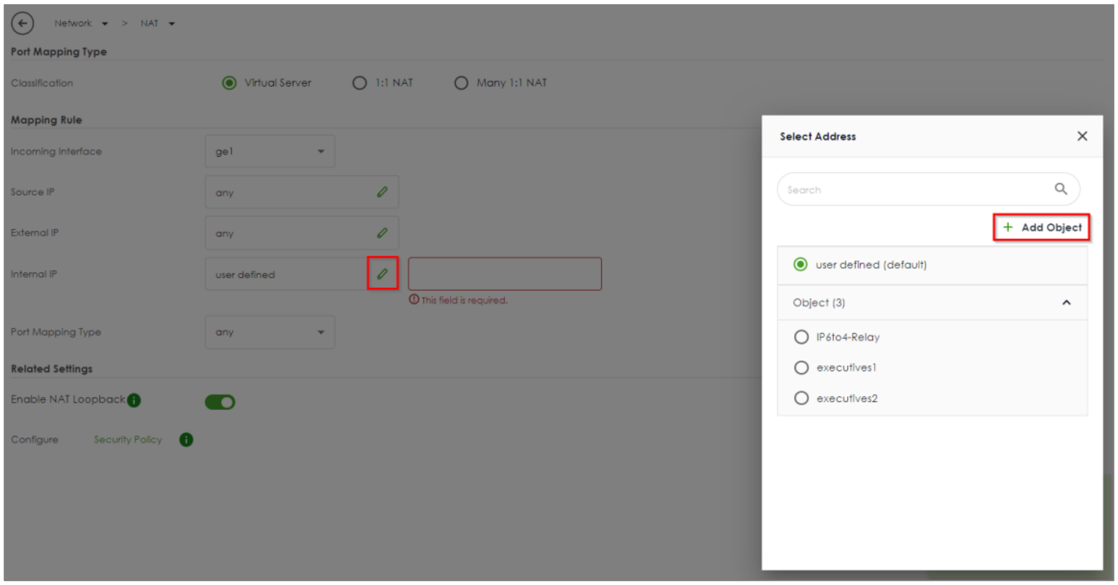
- select Virtual Server

- Incoming Interface: ge1

- Configure the Source IP to limit the access by the Source IP. You may select Any

- Configure the External IP. Select Any to choose the ge1 interface IP as the external IP.

- Configure the internal IP. Click +Add Object to create an address object as a host 192.168.168.33 which is the IP address of the internal server.



Network > NAT

Port Mapping Type

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

Mapping Rule

Incoming Interface: ge1

Source IP: any

External IP: any

Internal IP: user defined

This field is required.

Port Mapping Type: any

Related Settings

Enable NAT Loopback: on

Configure Security Policy

Select Address

Search

+ Add Object

● user defined (default)

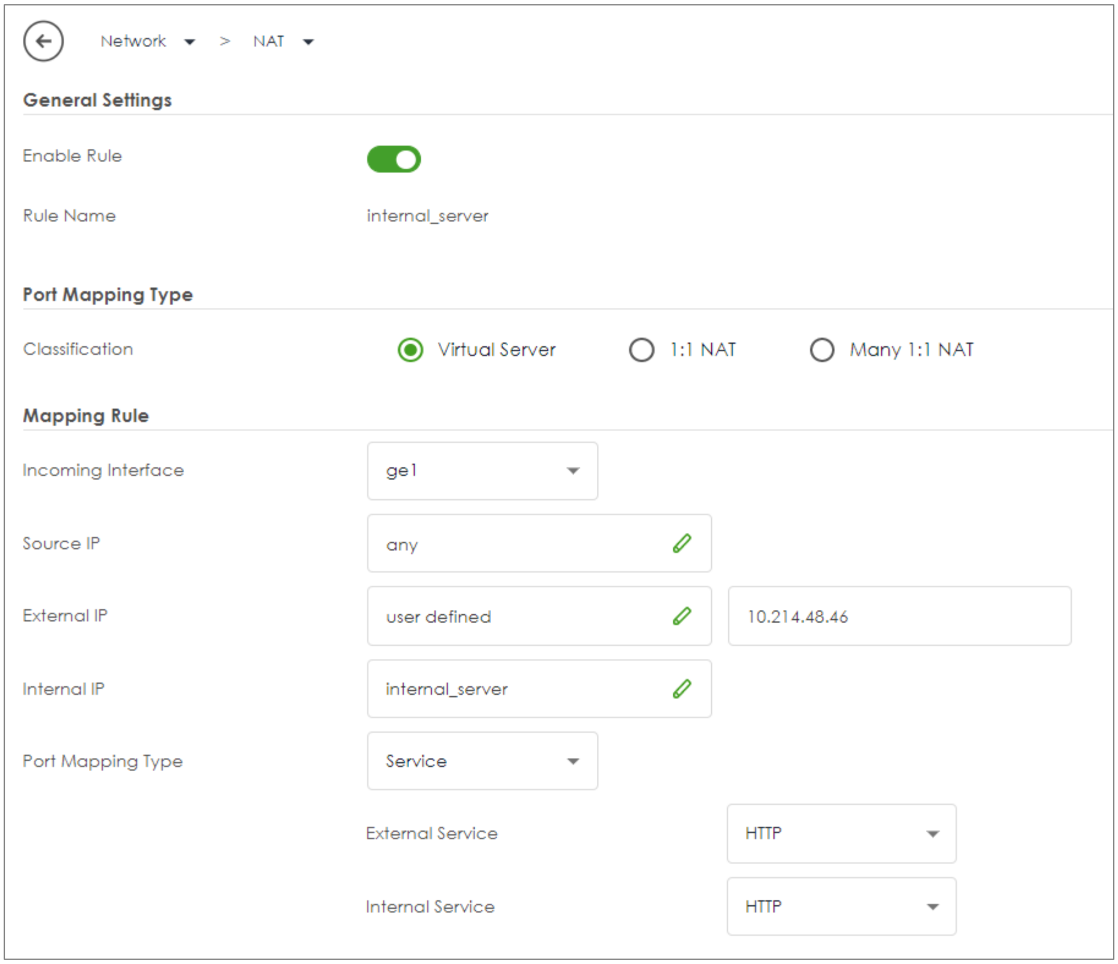
Object (3)

○ IP6to4-Relay

○ executives1

○ executives2

- Port Mapping Type: Select HTTP for both external and internal service.



General Settings

Enable Rule

Rule Name internal_server

Port Mapping Type

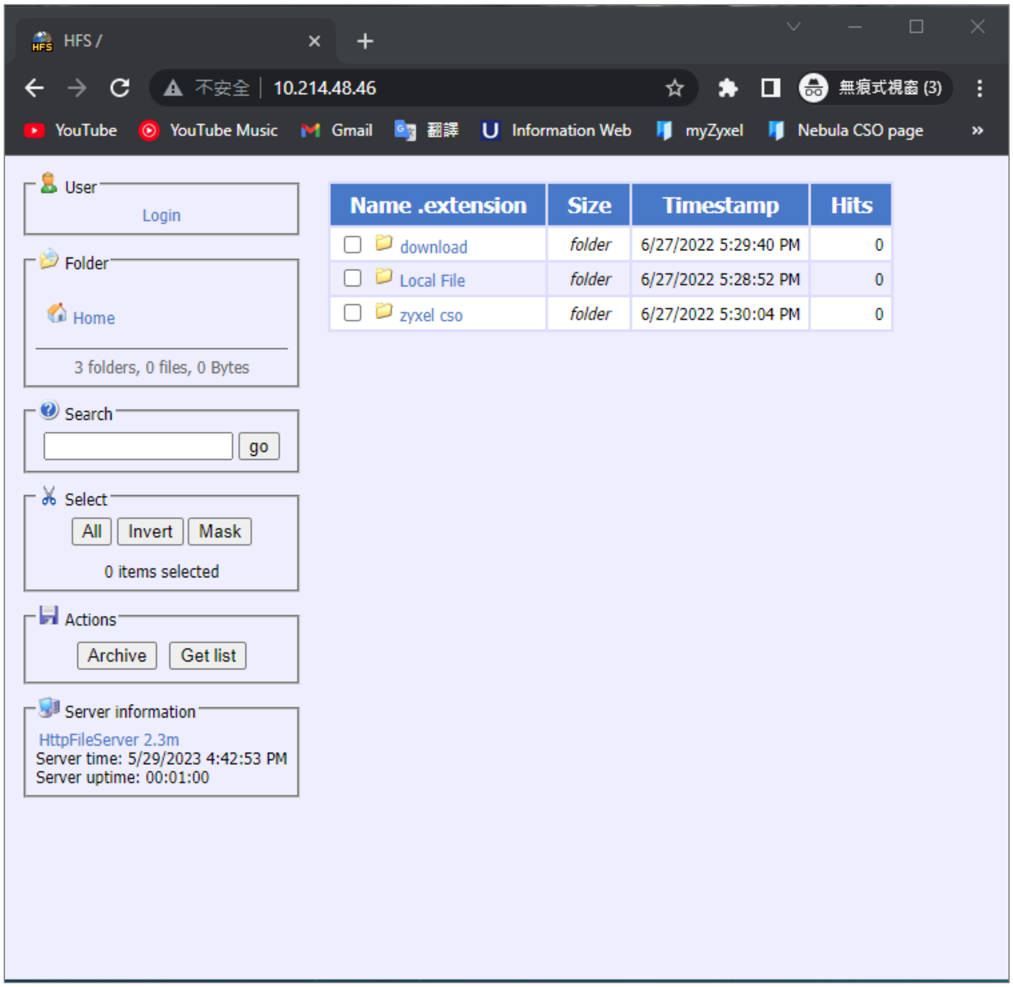
Classification ● Virtual Server ○ 1:1 NAT ○ Many 1:1 NAT

Mapping Rule

Incoming Interface	ge1
Source IP	any
External IP	user defined 10.214.48.46
Internal IP	internal_server
Port Mapping Type	Service
External Service	HTTP
Internal Service	HTTP

Test the Result

Type http://10.214.48.46 into the browser, and it display the HTTP service page.



3 folders, 0 files, 0 Bytes

0 items selected

HttpFileServer 2.3m
Server time: 5/29/2023 4:42:53 PM
Server uptime: 00:01:00

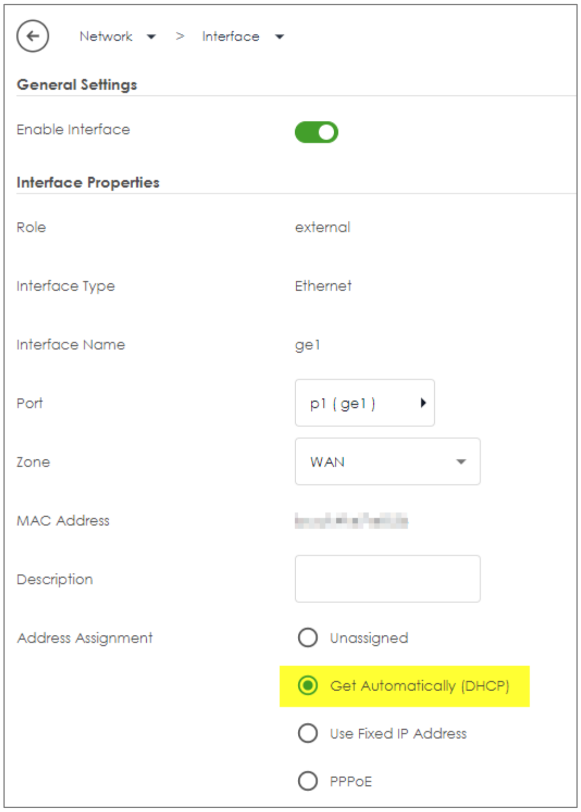
Name .extension	Size	Timestamp	Hits
☐ download	*folder*	6/27/2022 5:29:40 PM	0
☐ Local File	*folder*	6/27/2022 5:28:52 PM	0
☐ zyxel cso	*folder*	6/27/2022 5:30:04 PM	0

How to Configure DHCP Option 60 – Vendor Class Identifier

USG FLEX H series supports DHCP option 60. By VCI string matching, a DHCP client can select a specific DHCP server within the WAN network. This feature proves beneficial in network environments where multiple DHCP servers offer services. Clients that need Internet service can be directed to the DHCP server that provides corresponding Internet connection details via the identical option 60 string. On the other hand, IPTV clients can relay to another DHCP server for obtaining IPTV service information.

Set Up DHCP 60 on the USG FLEX H

1. Go to Network > Interface > External, and edit the WAN interface.
2. Make sure the WAN interface is set as a DHCP client. Select **Get Automatically (DHCP)** for Address Assignment.



Network > Interface

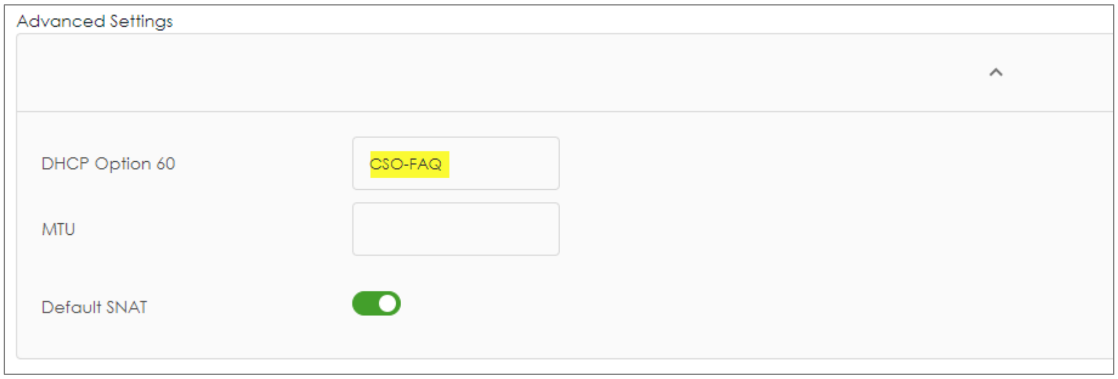
General Settings

Enable Interface	●

Interface Properties

Role	external
Interface Type	Ethernet
Interface Name	ge1
Port	p1 (ge1)
Zone	WAN
MAC Address	[redacted]
Description	
Address Assignment	○ Unassigned ● Get Automatically (DHCP) ○ Use Fixed IP Address ○ PPPoE

3. Scroll down and expand the Advanced Settings: DHCP Option 60
4. Enter the VCI string in the field of DHCP Option 60, and click **Apply**



Advanced Settings

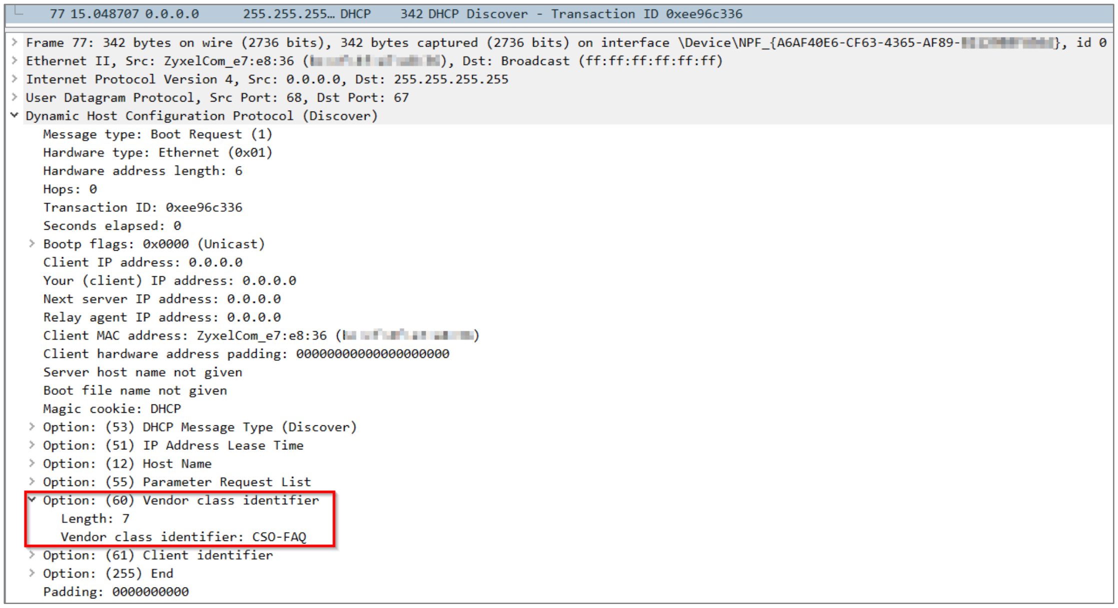
DHCP Option 60: CSO-FAQ

MTU:

Default SNAT: ON

Test DHCP Option 60

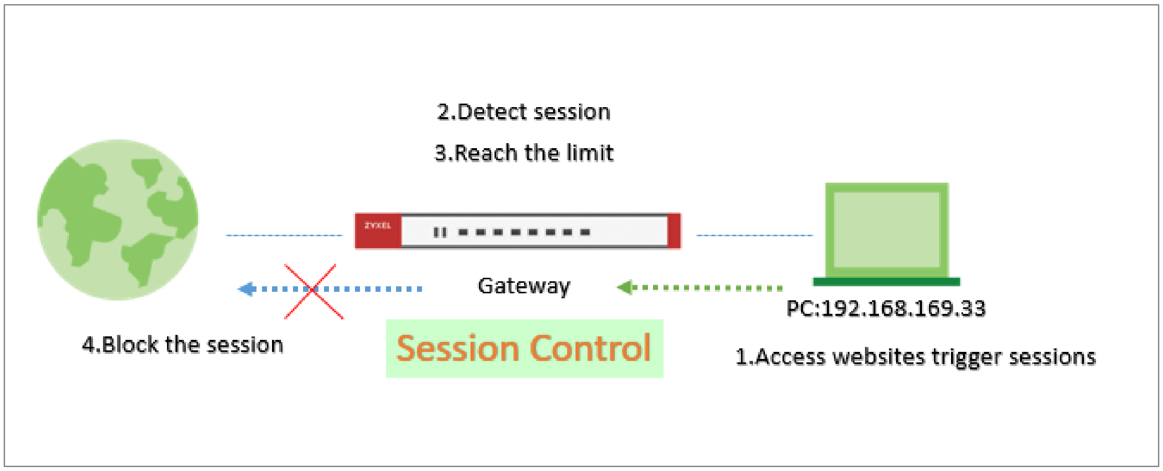
To check the functionality of DHCP Option 60, we can use packet capture software to check if option 60 string exists in the DHCP discover message that is sent from the USG FLEX H.



```
   77 15.048707 0.0.0.0       255.255.255… DHCP     342 DHCP Discover - Transaction ID 0xee96c336

> Frame 77: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{A6AF40E6-CF63-4365-AF89-[redacted]}, id 0
> Ethernet II, Src: ZyxelCom_e7:e8:36 ([redacted]), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0xee96c336
    Seconds elapsed: 0
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
    Client MAC address: ZyxelCom_e7:e8:36 ([redacted])
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (51) IP Address Lease Time
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  v Option: (60) Vendor class identifier
      Length: 7
      Vendor class identifier: CSO-FAQ
  > Option: (61) Client identifier
  > Option: (255) End
    Padding: 0000000000
```

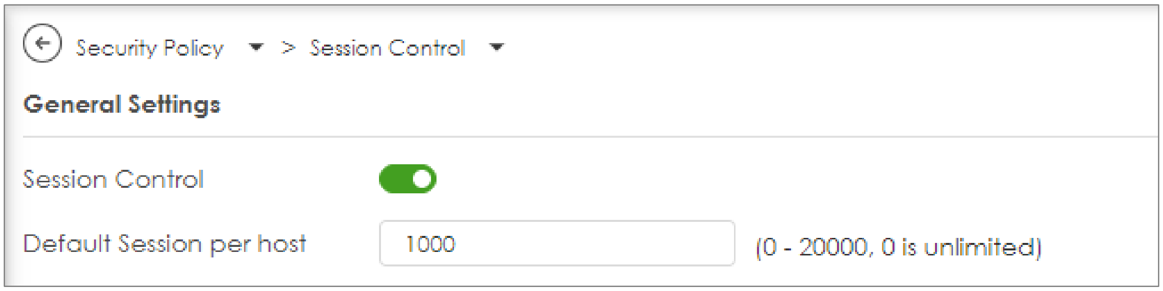
How to Configure Session Control

Session control can address abnormal user behavior. By monitoring session activities, the firewall can detect deviations from normal usage, such as sudden traffic spikes or unauthorized access attempts. This proactive approach enables prompt action to be taken to investigate and mitigate potential security threats .



Set Up the Session Control

Go to Security Policy > Session Control. Turn on this feature.



Security Policy > Session Control

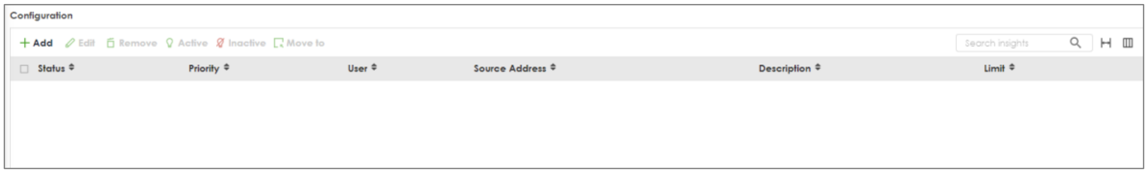
General Settings

Session Control: On

Default Session per host: 1000 (0 - 20000, 0 is unlimited)

You can field in the value of the Session per hosts you would like to limit.

The field here is for the client who is not in the rule under the list

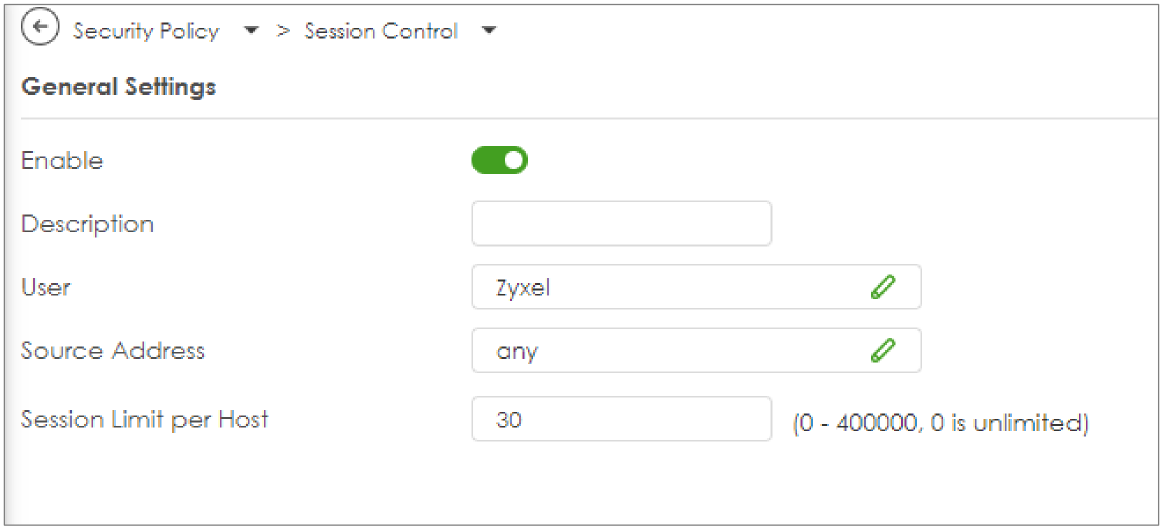


Configuration

□	Status	Priority	User	Source Address	Description	Limit

To limit a user's session. You can set up specific rules for each user

Click Add >Select one of the user and field in the Session limit for the user and click save.



Security Policy > Session Control

General Settings

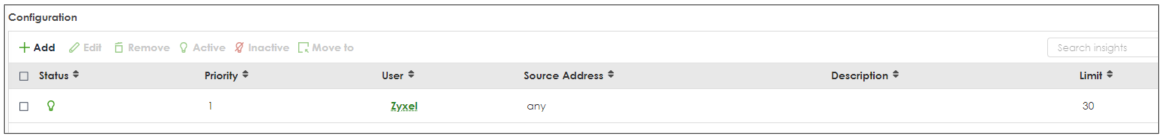
Enable: On

Description:

User: Zyxel

Source Address: any

Session Limit per Host: 30 (0 - 400000, 0 is unlimited)

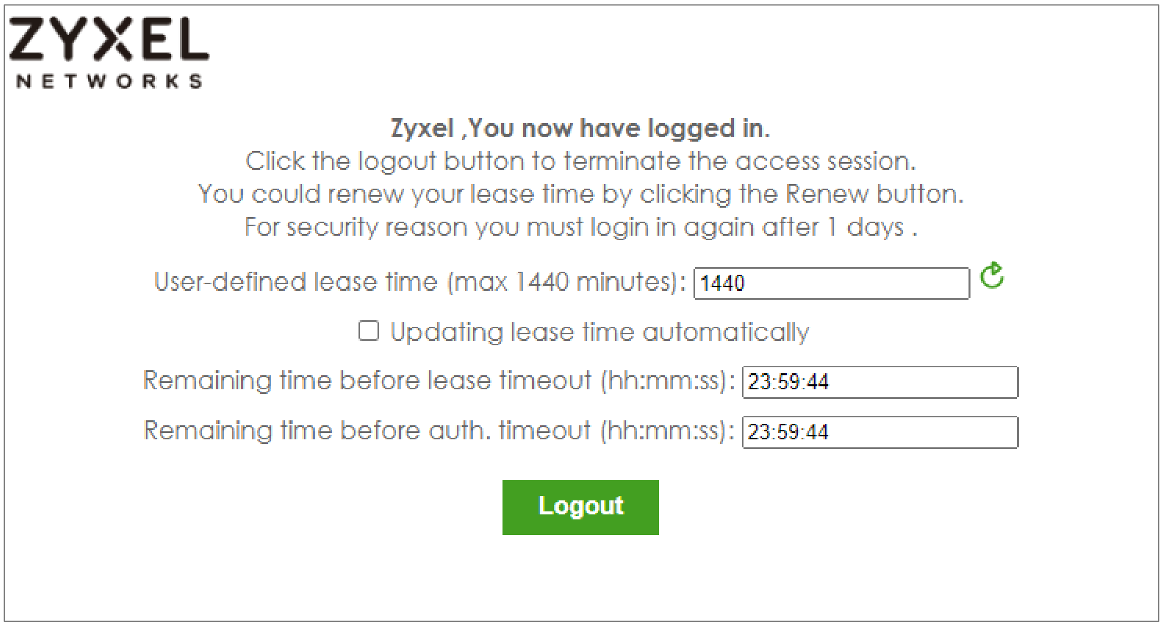


Configuration

□	Status	Priority	User	Source Address	Description	Limit
□	💡	1	Zyxel	any		30

Test the Result

Log in as User: Zyxel



Zyxel ,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 1 days .

User-defined lease time (max 1440 minutes): 1440

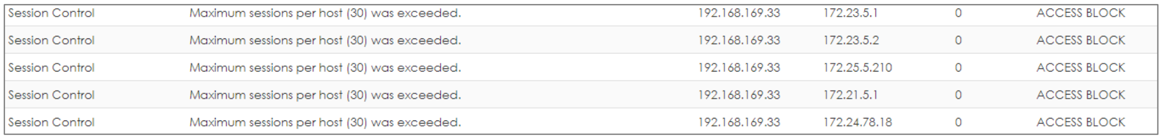
□ Updating lease time automatically

Remaining time before lease timeout (hh:mm:ss): 23:59:44

Remaining time before auth. timeout (hh:mm:ss): 23:59:44

Try to access web browser to hit the session limit

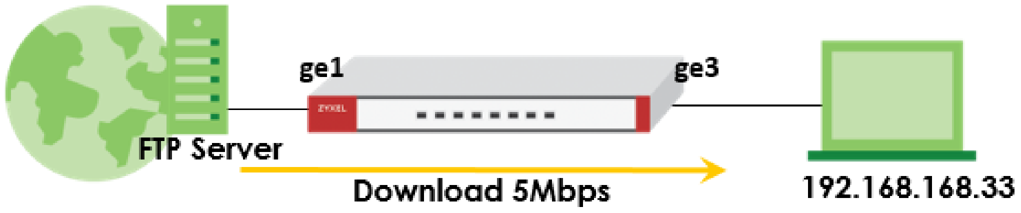
Go to Log & Report > Log/Events and select Session Control to check the logs.



```
Session Control   Maximum sessions per host (30) was exceeded.   192.168.169.33   172.23.5.1     0   ACCESS BLOCK
Session Control   Maximum sessions per host (30) was exceeded.   192.168.169.33   172.23.5.2     0   ACCESS BLOCK
Session Control   Maximum sessions per host (30) was exceeded.   192.168.169.33   172.25.5.210   0   ACCESS BLOCK
Session Control   Maximum sessions per host (30) was exceeded.   192.168.169.33   172.21.5.1     0   ACCESS BLOCK
Session Control   Maximum sessions per host (30) was exceeded.   192.168.169.33   172.24.78.18   0   ACCESS BLOCK
```

How to Configure Bandwidth Management for FTP Traffic

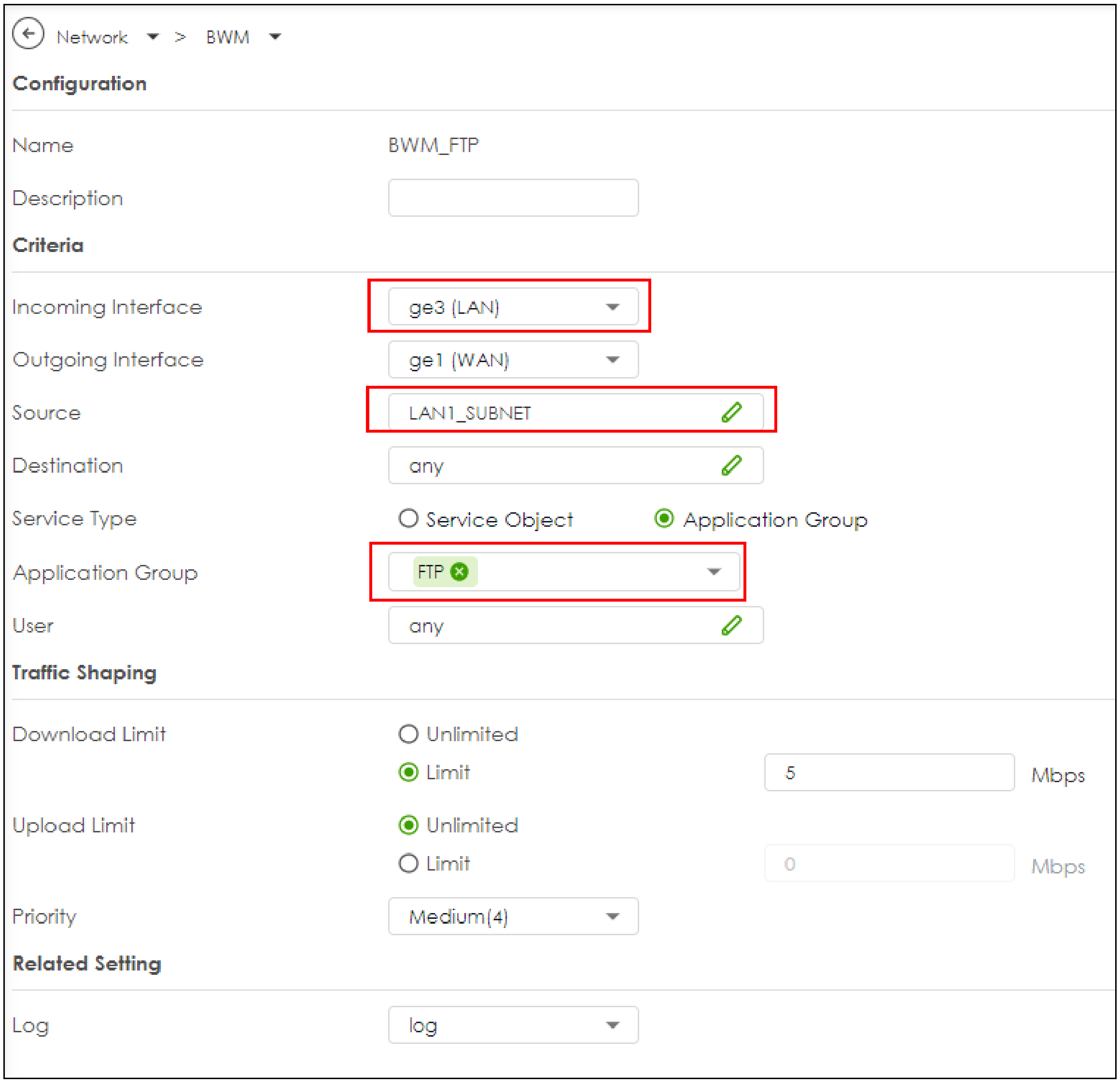
This example illustrates how to use USG Bandwidth Management (BWM) for controlling FTP traffic bandwidth allocation. By specifying criteria such as incoming interface, outgoing interface, source address, destination address, service objects, application group, and user, you can create a sequence of conditions to allocate bandwidth for packets that match these criteria. Once BWM is set up, it allows you to limit bandwidth for high-consumption services like FTP, ensuring bandwidth guarantees. This is a practical example of implementing BWM for FTP traffic with a USG device.



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 5Mbps. This example was tested using USG FLEX 500H

Set Up the BWM rule for FTP download.

Go to Network > BWM scan. Click on “Add” button to create a new BWM rule.



Network > BWM

Configuration

Name	BWM_FTP	
Description		

Criteria

Incoming Interface	ge3 (LAN)	
Outgoing Interface	ge1 (WAN)	
Source	LAN1_SUBNET	
Destination	any	
Service Type	○ Service Object	● Application Group
Application Group	FTP	
User	any	

Traffic Shaping

Download Limit	○ Unlimited		
	● Limit	5	Mbps
Upload Limit	● Unlimited		
	○ Limit	0	Mbps
Priority	Medium(4)		

Related Setting

Log	log

Incoming Interface: ge3

Outgoing Interface: ge1

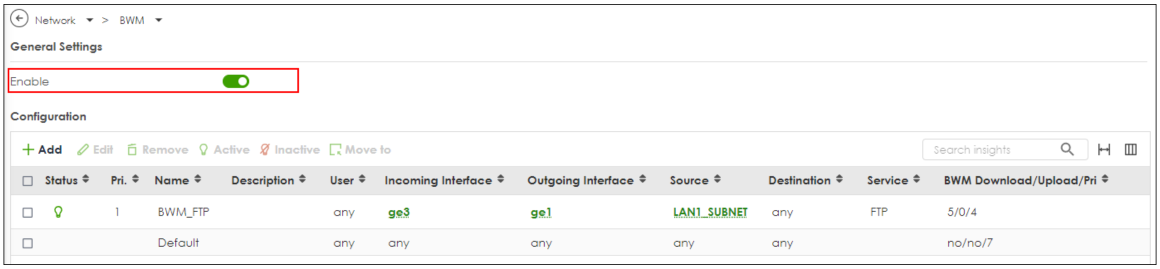
Source: LAN1 IP Subnet

Application Group: FTP

Traffic Shaping: Download Limit 5 Mbps.

Note: The terms "incoming interface" and "destination interface" indicate the direction of traffic that the client initiates during a session. The term "Source IP information" denotes the initial IP address. Furthermore, the Application Group function identifies client traffic types based not only on the service port but on other criteria as well.

Turn on this feature. It will enable BWM function to allowing the rules to be effectively applied.

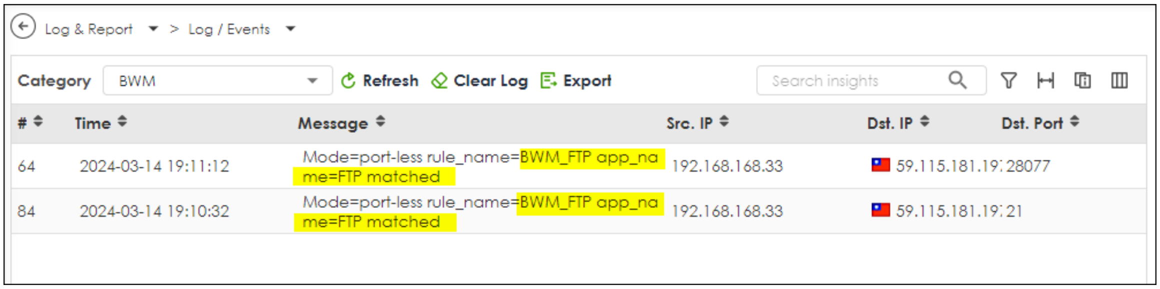


Enable ●

□	Status	Pri.	Name	Description	User	Incoming Interface	Outgoing Interface	Source	Destination	Service	BWM Download/Upload/Pri
□	💡	1	BWM_FTP		any	ge3	ge1	LAN1_SUBNET	any	FTP	5/0/4
□			Default		any	any	any	any	any		no/no/7

Test the Result

Go to Log & Report > Log/Events and select BWM to check the logs.

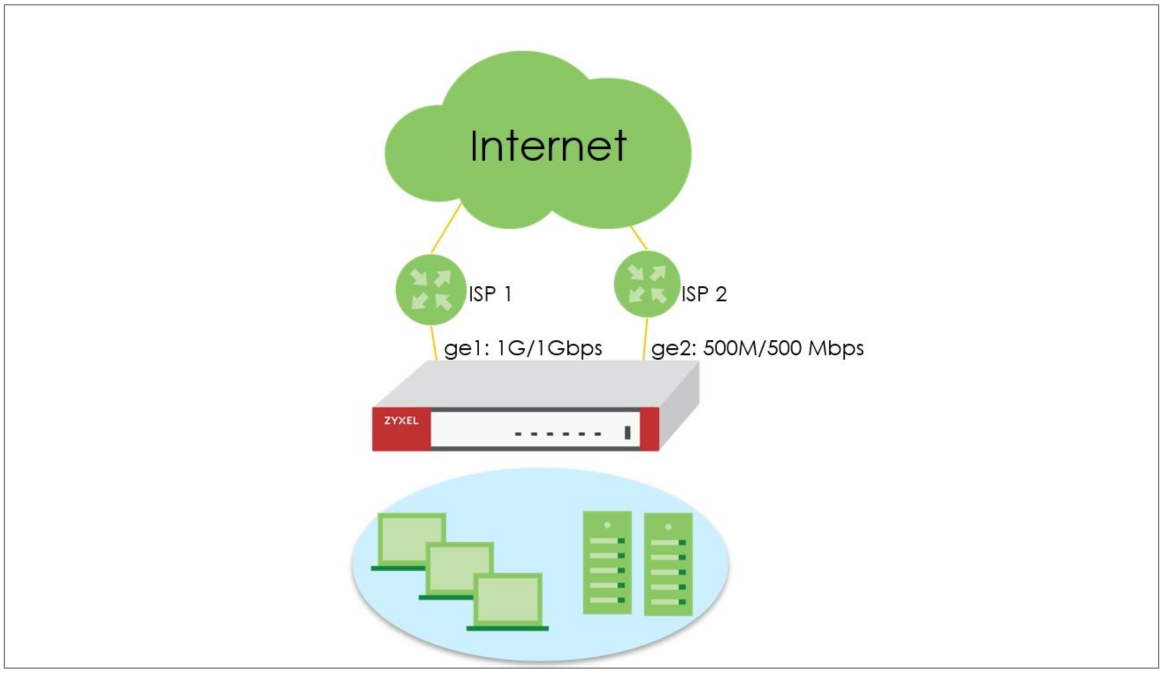


Category: BWM

#	Time	Message	Src. IP	Dst. IP	Dst. Port
64	2024-03-14 19:11:12	Mode=port-less rule_name=BWM_FTP app_name=FTP matched	192.168.168.33	59.115.181.19:	28077
84	2024-03-14 19:10:32	Mode=port-less rule_name=BWM_FTP app_name=FTP matched	192.168.168.33	59.115.181.19:	21

How to Configure WAN trunk for Spillover and Least Load First

In the realm of network management, WAN trunk spillover and the Least Load First (LLF) algorithm are vital for optimizing resource utilization and enhancing network performance. WAN trunk spillover ensures seamless connectivity by distributing traffic across multiple WAN connections, preventing bottlenecks, and maximizing bandwidth usage. The LLF algorithm intelligently balances traffic load by prioritizing the least loaded WAN links, minimizing latency, and improving overall network efficiency. This is an example of using the FLEX H series for two spillovers and the Least Load First configuration. The following example is based on GE1 1G/1G and GE2 500/500 Mbps for illustration.



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 500H (Firmware Version: uOS 1.20).

Least Load First

The “Least Load First” algorithm allocates new session traffic based on the current outbound bandwidth utilization of each trunk member interface. This utilization, measured as outbound throughput over available bandwidth, serves as the load balancing index. For instance, if WAN 1 has a throughput of 1000K and WAN 2 has 5K, the Zyxel Device calculates the load balancing index accordingly. With WAN 2 showing a lower utilization, indicating lesser utilization compared to WAN 1, subsequent new session traffic is routed through WAN 2 for optimal load distribution.

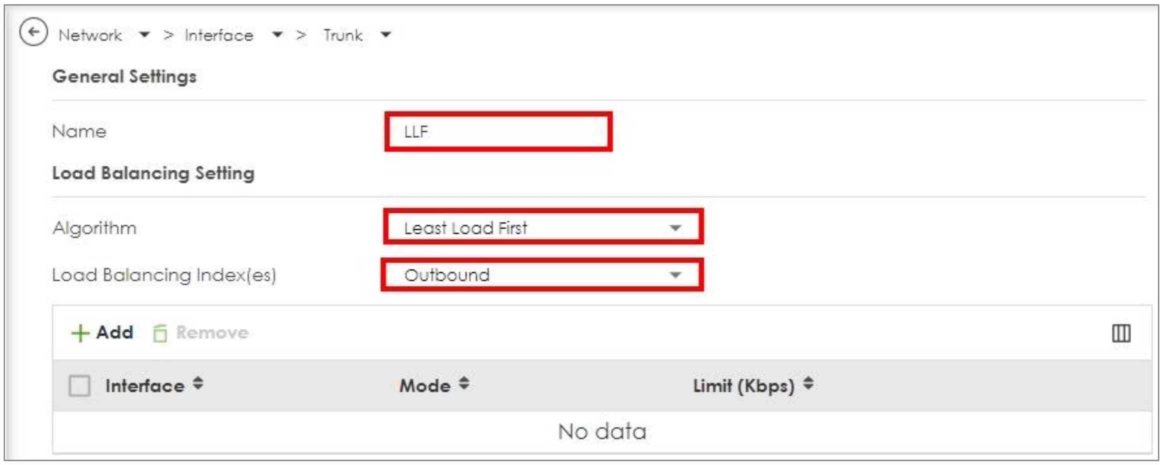
Spillover

The “Spillover” load balancing algorithm prioritizes the first interface in the trunk member list until its maximum load capacity is reached. Any excess traffic from new sessions is then directed to subsequent interfaces in the list, continuing until all member interfaces are utilized or traffic demands are met. For example, if the first interface offers unlimited access while the second incurs usage-based billing, the algorithm only activates the second interface when traffic surpasses the threshold of the first. This approach optimizes bandwidth usage on the first interface, minimizing Internet fees and preventing overload situations on individual interfaces.

Set Up the User-Defined Trunk

Spillover and Least Load First

Go to Network > Interface > Trunk page, and click **Add** button to create user-defined Trunk. In the general settings, we can configure the following settings;
Name: Least Load First (Enter a descriptive name for this trunk)
Algorithm: LLF
Load Balancing Index: Outbound
Note: *This field is available if you selected to use the* ***Least Load First*** *or* ***Spillover*** *method.*



Network > Interface > Trunk

General Settings

Name: LLF

Load Balancing Setting

Algorithm: Least Load First

Load Balancing Index(es): Outbound

□ Interface	Mode	Limit (Kbps)
No data		

Click **Add** to add a member interface to the trunk, in this scenario, we have ge1, and ge2 for Internet access.

Member: ge1(Wan)

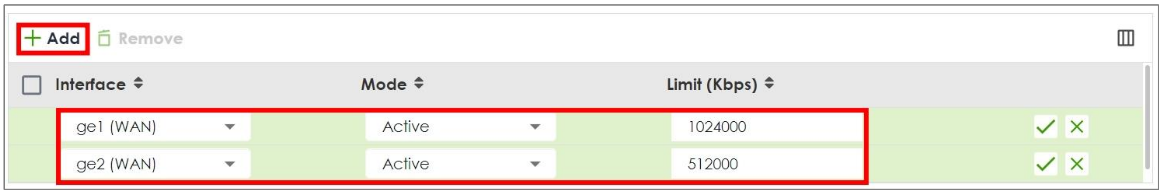
Mode: Active

Limit(Kbps): 1024000

Member: ge2(Wan)

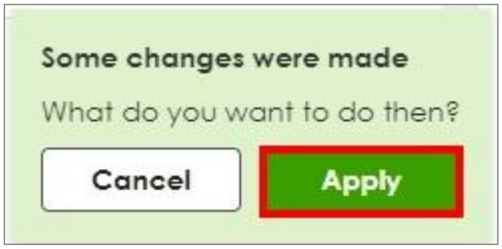
Mode: Active

Limit(Kbps): 512000



□ Interface	Mode	Limit (Kbps)	
ge1 (WAN)	Active	1024000	✓ ✕
ge2 (WAN)	Active	512000	✓ ✕

Click **Apply** to save changes.



Some changes were made

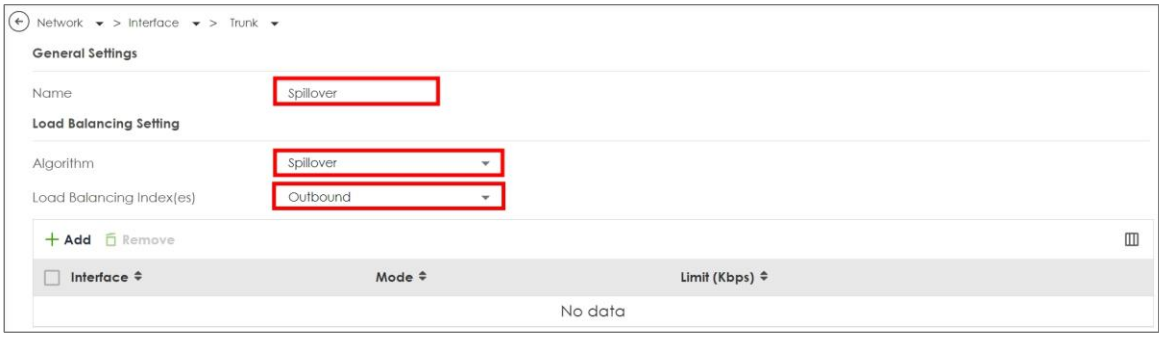
What do you want to do then?

After the Trunk LLF is created, let's create a second WAN trunk for spillover testing, click **Add** button to create 2nd user-defined Trunk.

Name: Spillover (Enter a descriptive name for this trunk)

Algorithm: Spillover

Load Balancing Index: Outbound



Click **Add** to add a member interface to the trunk.

Member: ge1(Wan)

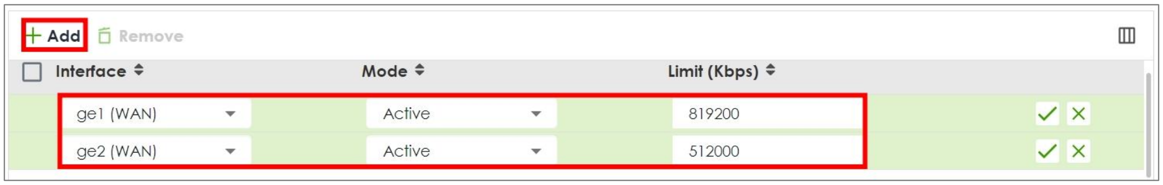
Mode: Active

Limit(Kbps): 819200

Member: ge2(Wan)

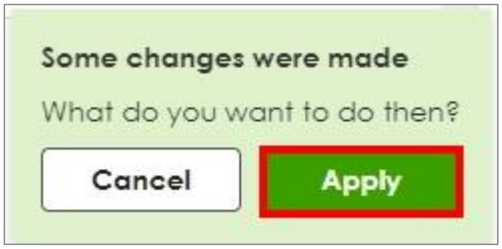
Mode: Active

Limit(Kbps): 512000



Interface	Mode	Limit (Kbps)
ge1 (WAN)	Active	819200
ge2 (WAN)	Active	512000

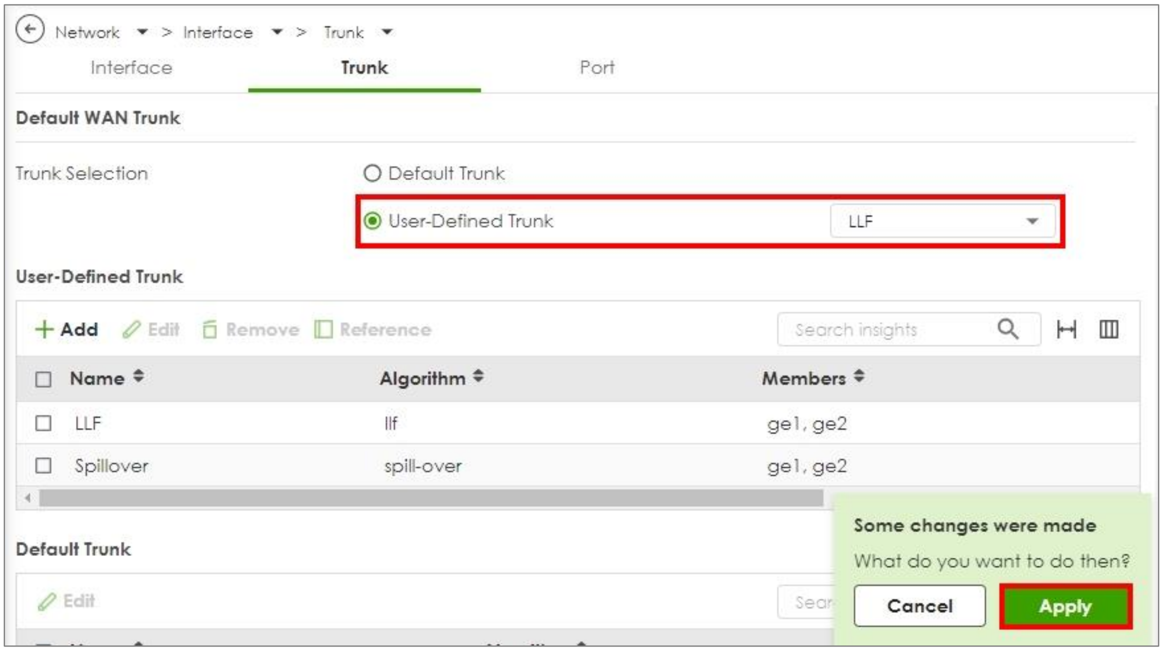
Click **Apply** to save changes.



Some changes were made

What do you want to do then?

Go to Default WAN Trunk section, select User-Defined Trunk and select the newly created (LLF or Spillover) Trunk from the list box. Click **Apply** to save changes.



Network > Interface > Trunk

Interface | **Trunk** | Port

Default WAN Trunk

Trunk Selection ○ Default Trunk

● User-Defined Trunk LLF

User-Defined Trunk

□	Name	Algorithm	Members
□	LLF	llf	ge1, ge2
□	Spillover	spill-over	ge1, ge2

Default Trunk

Some changes were made

What do you want to do then?

Test the Result

Spillover

1) Apply Spillover in User-Defined Trunk.

2) Connect two hosts on the LAN side. Host A upload a large file to an FTP server.

3) Go to Traffic Statistics > Port to check interface utilization. Upload traffic should go to ge1 as this interface is the first member interface in Trunk Spillover. Check if maximum load capacity 819200bps is reached. Any excess traffic from new sessions is then directed to subsequent interfaces in the list

4) Host B generates ICMP traffic to 8.8.8.8.

5) Capture packets on the interface ge2 to see if new sessions are captured on ge2.

Least Load First

1) Apply LLF in User-Defined Trunk

2) Connect two hosts on the LAN side. Host A upload a large file to an FTP server.

3) Go to Traffic Statistics > Port to check interface utilization.

4) Host B generates ICMP traffic to 8.8.8.8.

5) Capture packets on the interface with lower traffic load to verify if the ICMP traffic is routed through the less congested interface.