

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

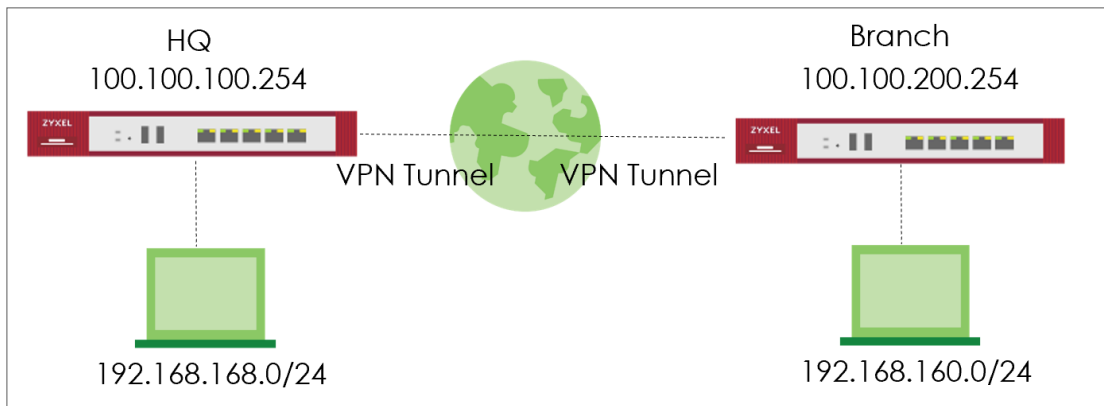
Chapter 1- VPN	4
How to Configure Site-to-site IPSec VPN Where the Peer has a Static IP Address.....	4
How to Configure Site-to-site IPSec VPN Where the Peer has a Dynamic IP Address.....	16
How to Configure IPSec Site to Site VPN while one Site is behind a NAT router	22
How to Configure Remote Access 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

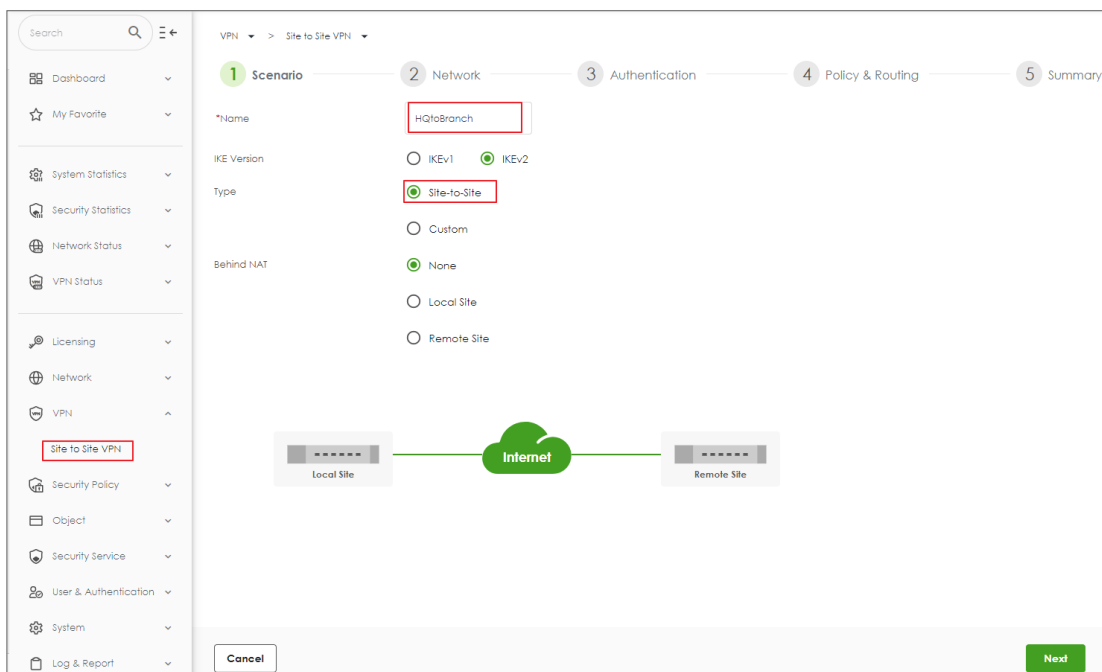
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Static IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



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**.



The screenshot shows the ZyXel VPN configuration interface. On the left is a sidebar menu with options: Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Site to Site VPN (highlighted with a red box), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main area displays the 'VPN > Site to Site VPN' configuration steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active. It includes a text field for '*Name' with the value 'HQtoBranch' (highlighted with a red box). Below this are radio button options for 'IKE Version' (IKEv1, IKEv2 - selected), 'Type' (Site-to-Site - selected, Custom), and 'Behind NAT' (None - selected, Local Site, Remote Site). At the bottom, there is a diagram showing a 'Local Site' connected to an 'Internet' cloud, which is then connected to a 'Remote Site'. At the bottom of the form are 'Cancel' and 'Next' buttons.

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

100.100.100.254

Peer Gateway Address

Domain Name / IP

100.100.200.254

Local Site

100.100.100.254

Internet

Remote Site

100.100.200.254

Cancel

Back

Next

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

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

VPN > Site to Site VPN

✓ Scenario

✓ Network

3 Authentication

4 Policy & Routing

5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate

.....

default

Cancel

Back

Next

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.

VPN > Site to Site VPN >

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

Type

☐ Route-Based
☒ Policy-Based

Local Subnet

192.168.168.0/24

Remote Subnet

192.168.160.0/24

192.168.168.0/24

Local Site
100.100.100.254

Internet

Remote Site
100.100.200.254

192.168.160.0/24

Cancel

Back

Finish

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.

VPN > Site to Site VPN >

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

Configuration

Name	HQtoBranch
IKE Version	2
Scenario	wizard
Type	Policy

Edit

Network

Local Site	100.100.100.254
Remote Site	100.100.200.254

Authentication

Authentication	pre-shared-key	*****
----------------	----------------	-------

Policy & Routing

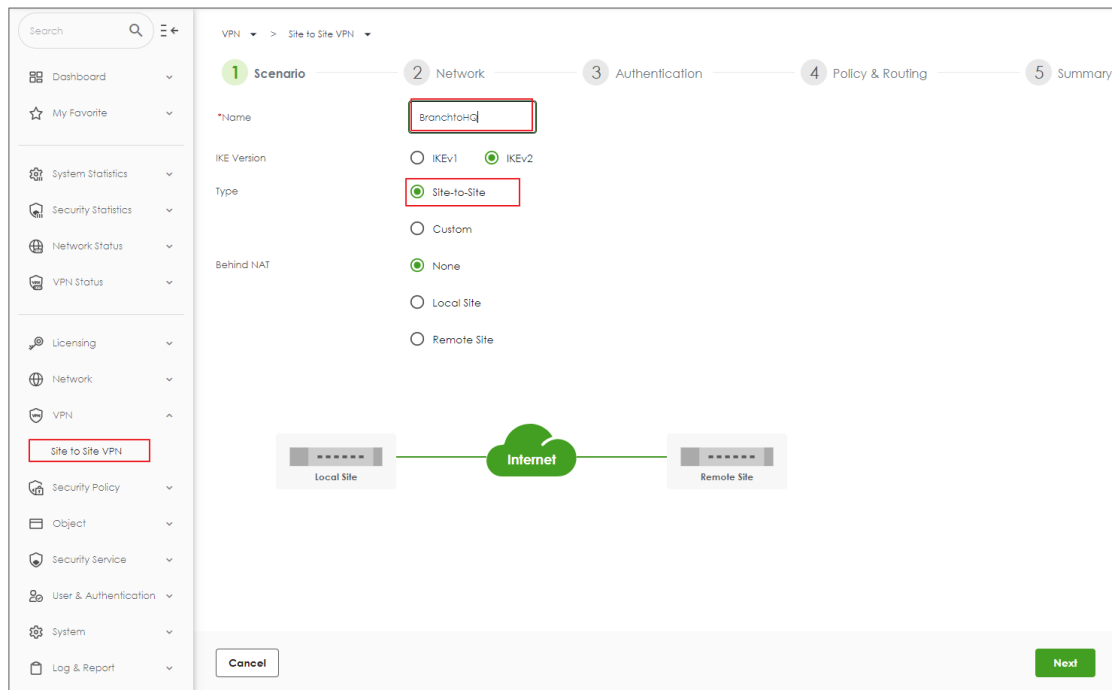
Local Subnet	192.168.168.0/24
Remote Subnet	192.168.160.0/24

Close

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**.



Search

VPN > Site to Site VPN

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

Local Site Internet Remote Site

Cancel Next

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

100.100.200.254

Peer Gateway Address

Domain Name / IP

100.100.100.254

Local Site

100.100.200.254

Internet

Remote Site

100.100.100.254

Cancel

Back

Next

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

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

VPN > Site to Site VPN

✓ Scenario — ✓ Network — **3 Authentication** — 4 Policy & Routing — 5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate

.....

default ▾

Cancel Back Next

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.

VPN > Site to Site VPN >

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

Type

☐ Route-Based
☒ Policy-Based

Local Subnet

192.168.160.0/24

Remote Subnet

192.168.168.0/24

192.168.160.0/24

Local Site

100.100.200.254

Internet

Remote Site

100.100.100.254

192.168.168.0/24

Cancel

Back

Finish

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.

VPN > > Site to Site VPN >

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

Configuration

Name	BranchtoHQ	
IKE Version	2	
Scenario	wizard	
Type	Policy	

Edit

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	

Close

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, 2023
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

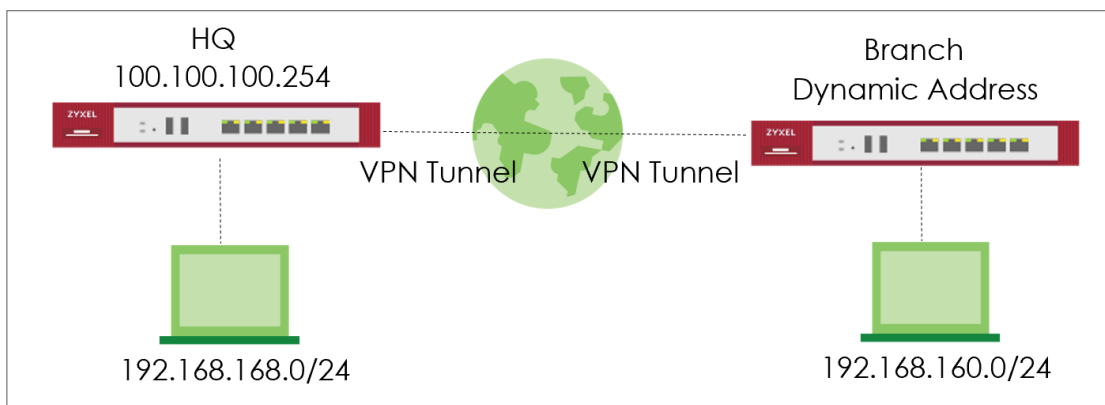
Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\WINDOWS\system32>

```

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

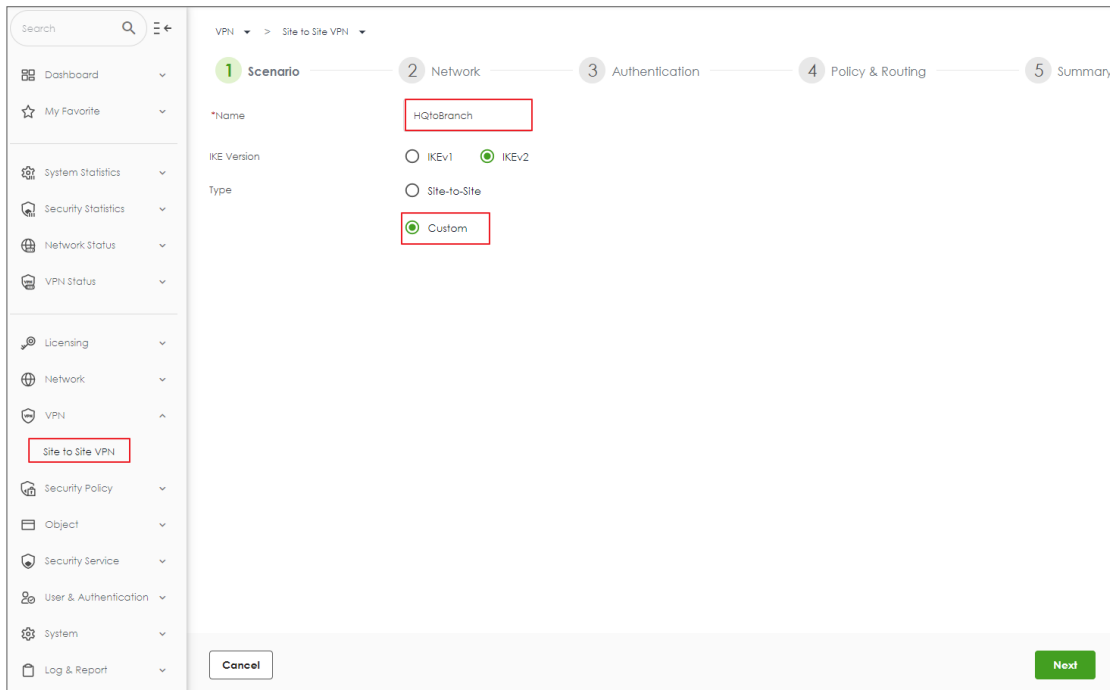
This example shows how to use the VPN Setup Wizard to create a site-to-site VPN with the Peer has a Dynamic IP Address. The example instructs how to configure the VPN tunnel between each site. When the VPN tunnel is configured, each site can be accessed securely.



Set up IPsec VPN Tunnel for HQ

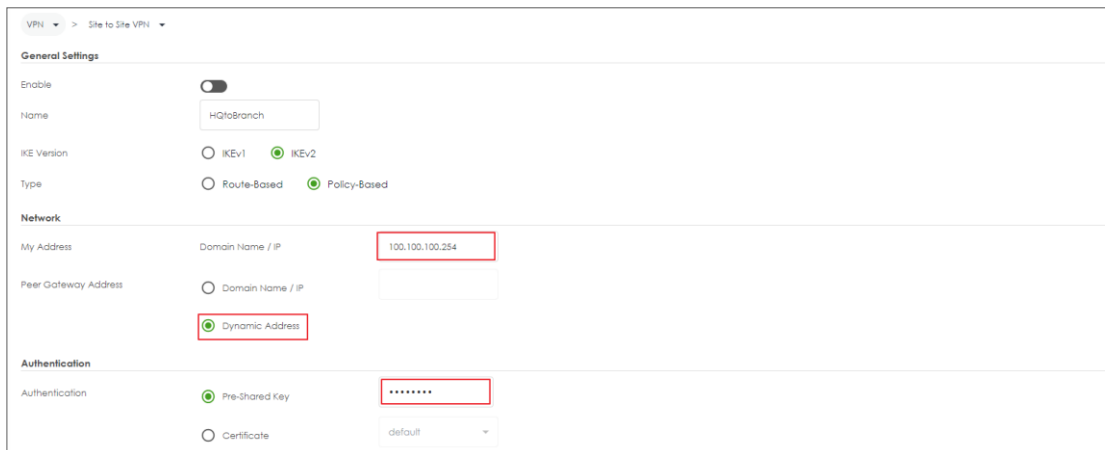
VPN > Site to Site VPN > Scenario

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



VPN > Site to Site VPN

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



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
☐ Nalled-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**.

VPN > Site to Site VPN

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

*Name: BranchtoHQ

IKE Version: ☐ IKEv1 ☒ IKEv2

Type: ☐ Site-to-Site ☒ Custom

Cancel Next

VPN > Site to Site VPN

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

VPN > Site to Site VPN

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

Policy

SA Life Time

Proposal

☒ Auto
 ☐ Nailed-up
 ☐ Responder Only

+ Add

Edit

Remove

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 >

28800 (180 - 3000000 Seconds)

+ Add

Edit

Remove

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.

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	65	81951	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, 2023
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

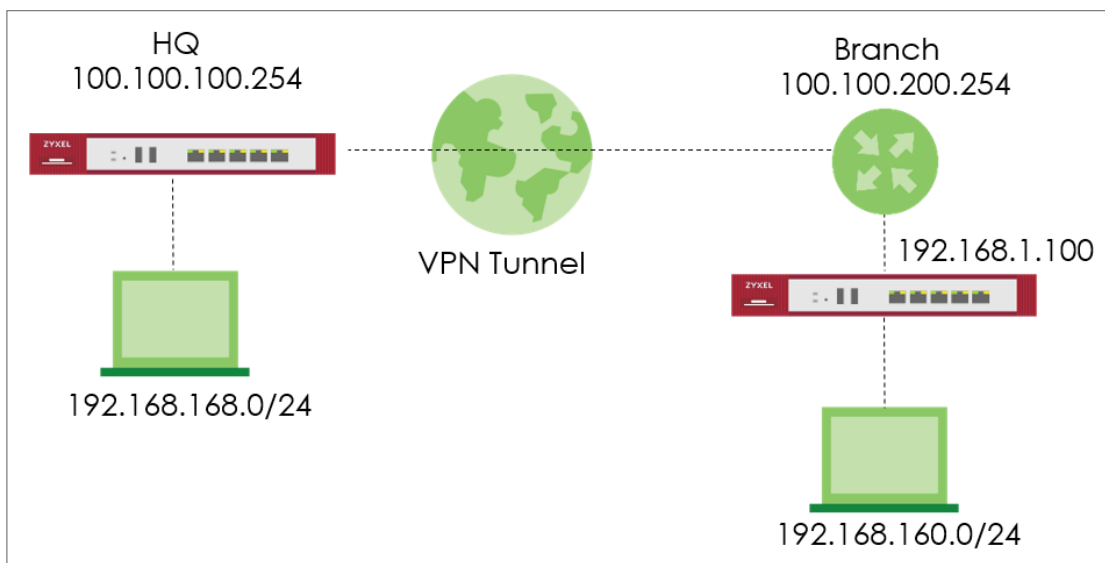
Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\WINDOWS\system32>

```

How to Configure 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.

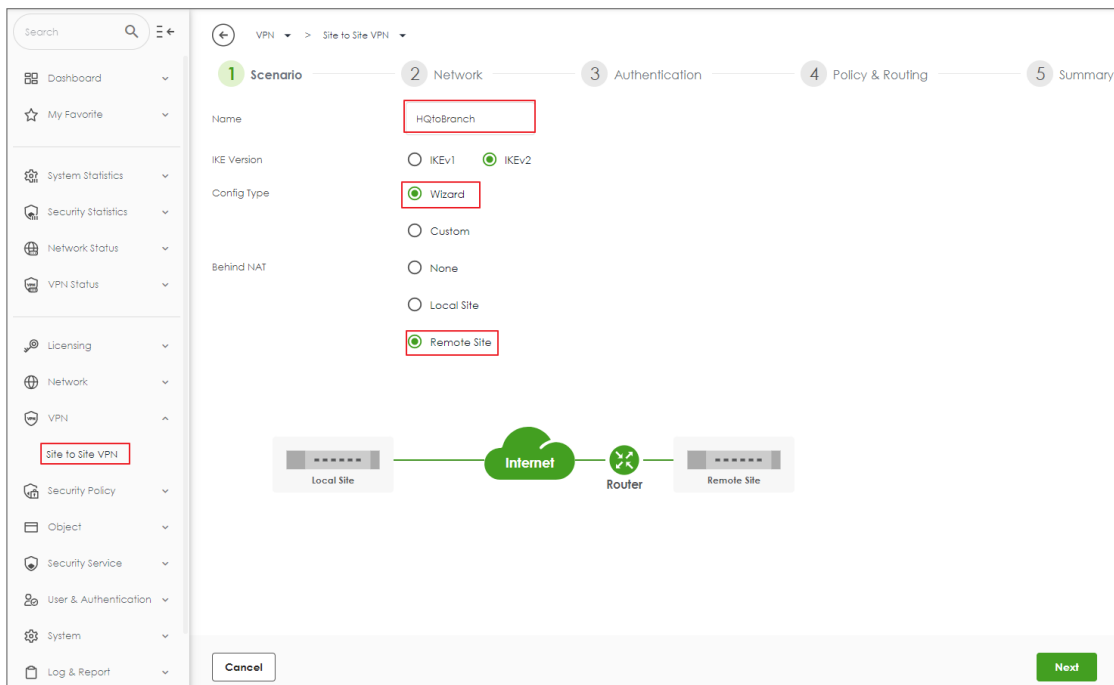


Note: Please ensure that you have NAT mapping UDP port 4500 to USG FLEX H device.

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**.



Search

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

Local Site Internet Router Remote Site

Cancel Next

VPN > Site to Site VPN > Scenario > Network

Configure My Address. Click **Next**.

VPN

>

Site to Site VPN

Scenario

2 Network

3 Authentication

4 Policy & Routing

5 Summary

My Address

Domain Name / IP

100.100.100.254

Peer Gateway Address

Dynamic Address

Local Site

100.100.100.254

Internet

Router

Remote Site

Dynamic Address

Cancel

Back

Next

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

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

VPN > Site to Site VPN

Scenario

Network

3 Authentication

4 Policy & Routing

5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate Beta

.....

default

Cancel

Back

Next

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.

The screenshot displays the ZyXel VPN configuration interface for a Site to Site VPN. The breadcrumb trail at the top indicates the current step: **VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing**. The configuration progress bar shows five steps: Scenario, Network, Authentication, Policy & Routing (current step, highlighted with a green circle and number 4), and Summary (highlighted with a grey circle and number 5).

Under the "Type" section, there are two radio buttons: "Route-Based" and "Policy-Based". The "Policy-Based" option is selected and highlighted with a red box.

Below the "Type" section, there are two input fields for subnets, both highlighted with red boxes:

- Local Subnet:** 192.168.168.0/24
- Remote Subnet:** 192.168.160.0/24

At the bottom of the form, there is a network diagram illustrating the Site to Site VPN setup:

- Local Site:** Represented by a server icon and the IP address 100.100.100.254.
- Internet:** Represented by a green cloud icon.
- Remote Site:** Represented by a server icon and the IP address 192.168.160.0/24.
- Router:** Represented by a router icon.

The diagram shows the Local Site connected to the Internet, which is connected to the Remote Site. The Router is positioned between the Internet and the Remote Site. The Local Site is also connected to the Router.

At the bottom of the interface, there are three buttons: "Cancel", "Back", and "Finish".

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.

←

VPN > Site to Site VPN

✓ Scenario

✓ Network

✓ Authentication

✓ Policy & Routing

5 Summary

Configuration

Name	HQtoBranch
IKE Version	2
Type	Policy-based
Proposal	▼

✎ Edit

Network

Local Site

100.100.100.254

Remote Site

Authentication

Authentication

pre-shared-key

🗨

Policy & Routing

Local Subnet

192.168.168.0/24

Close

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**.

Search

VPN > Site to Site VPN

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

Name: BranchtoHQ

IKE Version: ☐ IKEv1 ☒ IKEv2

Config Type: ☒ Wizard ☐ Custom

Behind NAT: ☐ None ☒ Local Site ☐ Remote Site

Local Site Router Internet Remote Site

Cancel Next

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

Local Site

192.168.1.100

Router

Internet

Remote Site

100.100.100.254

Cancel

Back

Next

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.

VPN

>

Site to Site VPN

✓ Scenario

✓ Network

✓ Authentication

4 Policy & Routing

5 Summary

Type

☐ Route-Based
 ☒ Policy-Based

Local Subnet

192.168.160.0/24

Remote Subnet

192.168.168.0/24

192.168.160.0/24

Local Site

192.168.1.100

Router

Internet

Remote Site

100.100.100.254

192.168.168.0/24

Cancel

Back

Finish

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

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

← VPN > Site to Site VPN

✓ Scenario

✓ Network

3 Authentication

4 Policy & Routing

5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate Beta

.....

default

Cancel

Back

Next

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.

←

VPN > Site to Site VPN

✓ Scenario

✓ Network

✓ Authentication

✓ Policy & Routing

5 Summary

Configuration

Name

BranchtoHQ

IKE Version

2

Type

Policy-based

Proposal

▼

✎ Edit

Network

Local Site

192.168.1.100

Remote Site

100.100.100.254

Authentication

pre-shared-key

🗑

Policy & Routing

Local Subnet

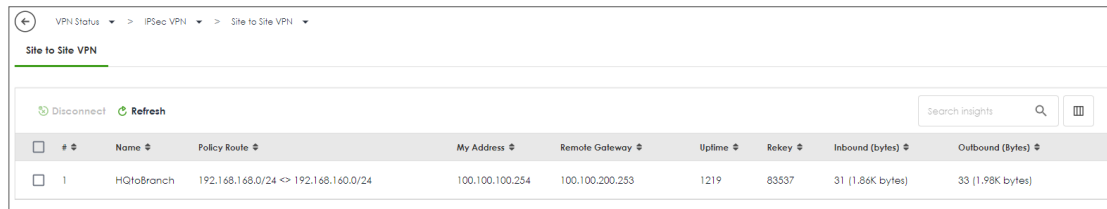
192.168.160.0/24

Close

Test IPsec VPN Tunnel

VPN Status > IPsec VPN

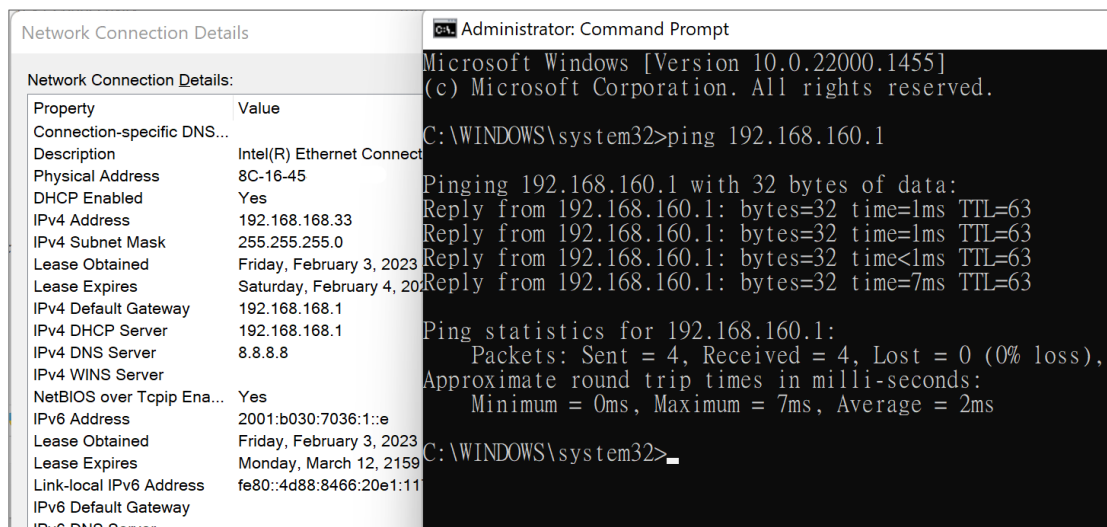
Verify the IPsec VPN status.



	#	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, 2023
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

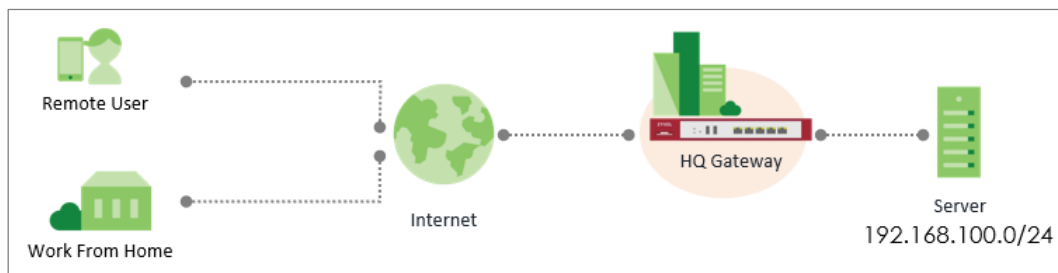
Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

C:\WINDOWS\system32>

```

How to Configure 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.

Search

Q

+

Network Status

VPN Status

Licensing

Network

VPN

Security Policy

Object

Security Service

User & Authentication

User/Group

User Authentication

System

User & Authentication > > User/Group > > User

User Group Setting

Local Administrator

+ Add Edit Remove Reference

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

User

+ Add Edit Remove Reference

☐	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

←

User & Authentication > User/Group >

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

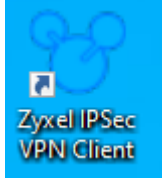
minutes

Reauthentication Time

1440

minutes

Download and install the new TGB Client

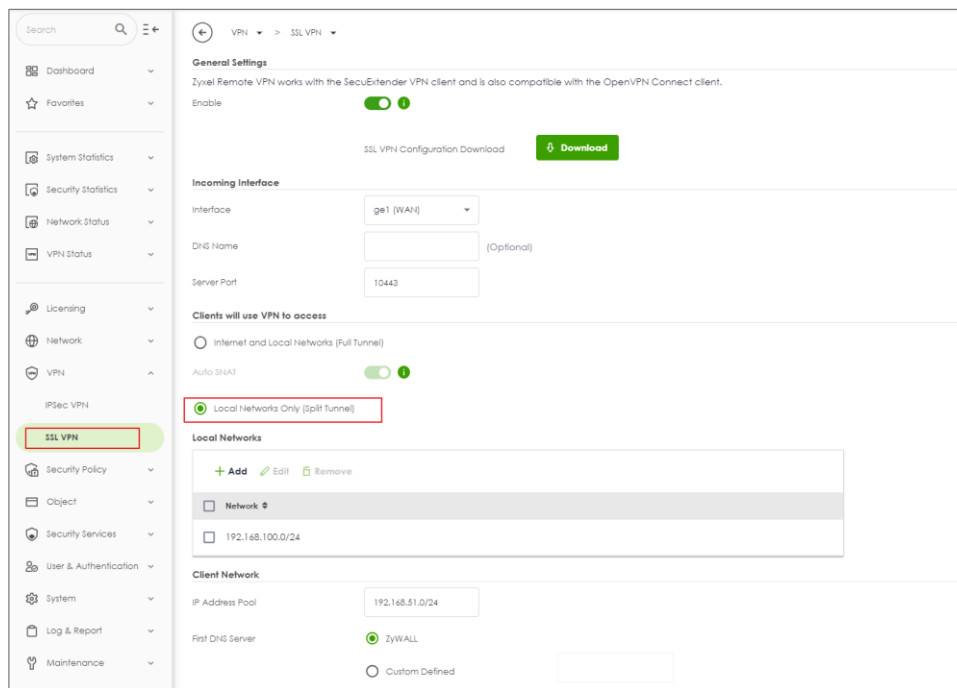


Set up SSL VPN

VPN > SSL VPN

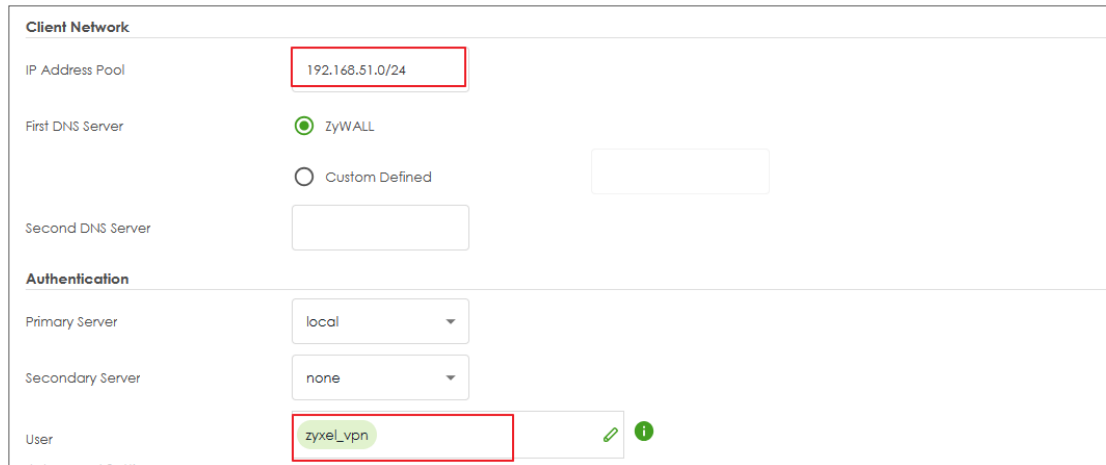
Select the incoming interface, the default port is 10443. And up to your requirement to select Full Tunnel or Split Tunnel. And we now support OpenVPN config file.

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



The screenshot shows the ZyXEL SSL VPN configuration page. The left sidebar contains a navigation menu with options like Dashboard, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, IPsec VPN, and SSL VPN (which is highlighted). The main content area is titled 'VPN > SSL VPN' and includes a 'General Settings' section with an 'Enable' toggle switch. Below this is a 'Download' button for the 'SSL VPN Configuration Download'. The 'Incoming Interface' section has a dropdown menu set to 'ge1 (WAN)' and a 'Server Port' field set to '10443'. The 'Clients will use VPN to access' section has two radio buttons: 'Internet and Local Networks (Full Tunnel)' and 'Local Networks Only (Split Tunnel)', with the latter being selected and highlighted by a red box. Below this is a 'Local Networks' table with columns for 'Add', 'Edit', and 'Remove', and a list of networks including '192.168.100.0/24'. The 'Client Network' section has an 'IP Address Pool' field set to '192.168.51.0/24' and a 'First DNS Server' dropdown set to 'ZyWALL'.

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

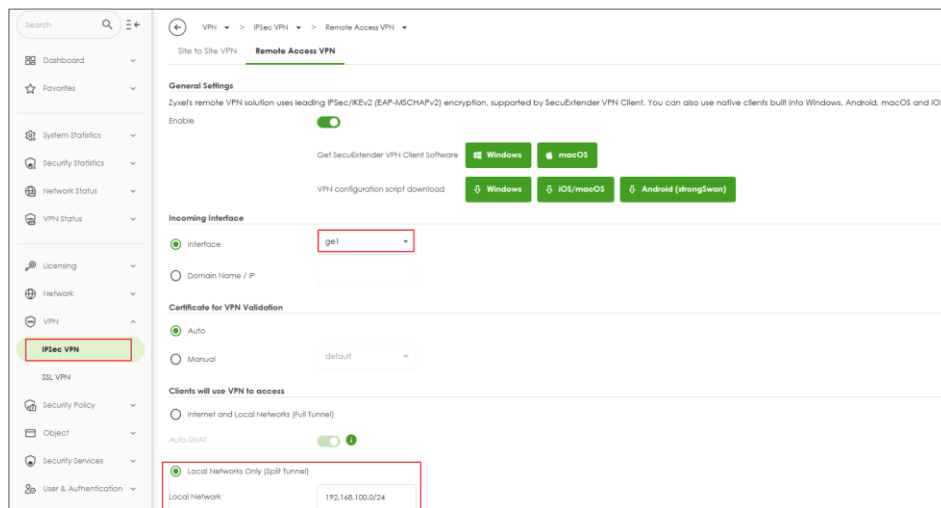
User: zyxel_vpn

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



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 \(zhongtuan\)](#)

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 NAT: ☒

☒ Local Networks Only (Split Tunnel)

Local Network: 192.168.100.0/24

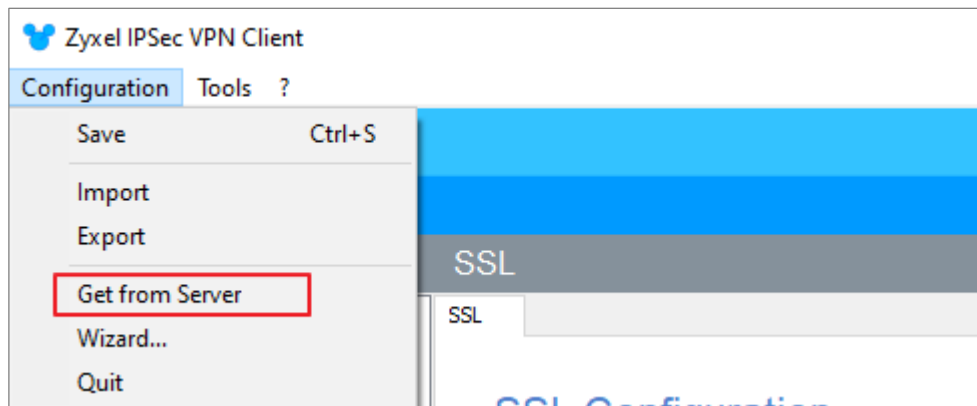
The default Address Pool is 192.168.50.0/24 and select the User who can access IKEv2 VPN.

The screenshot shows the ZyXEL VPN configuration interface. On the left is a sidebar with navigation options: Security Statistics, Network Status, VPN Status, Licensing, Network, VPN (expanded), IPsec VPN (highlighted), SSL VPN, Security Policy, and Object. The main panel is titled 'Client Network' and contains the following settings:

- IP Address Pool:** 192.168.50.0/24 (highlighted with a red box)
- First DNS Server:** ZyWALL (selected with a radio button)
- Custom Defined:** (empty text box)
- Second DNS Server:** (empty text box)
- Authentication:**
 - Primary Server:** local (dropdown menu)
 - Secondary Server:** none (dropdown menu)
 - User:** zyxel_vpn (highlighted with a red box and a green checkmark icon)
- Advanced Settings:** (expandable section)

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.

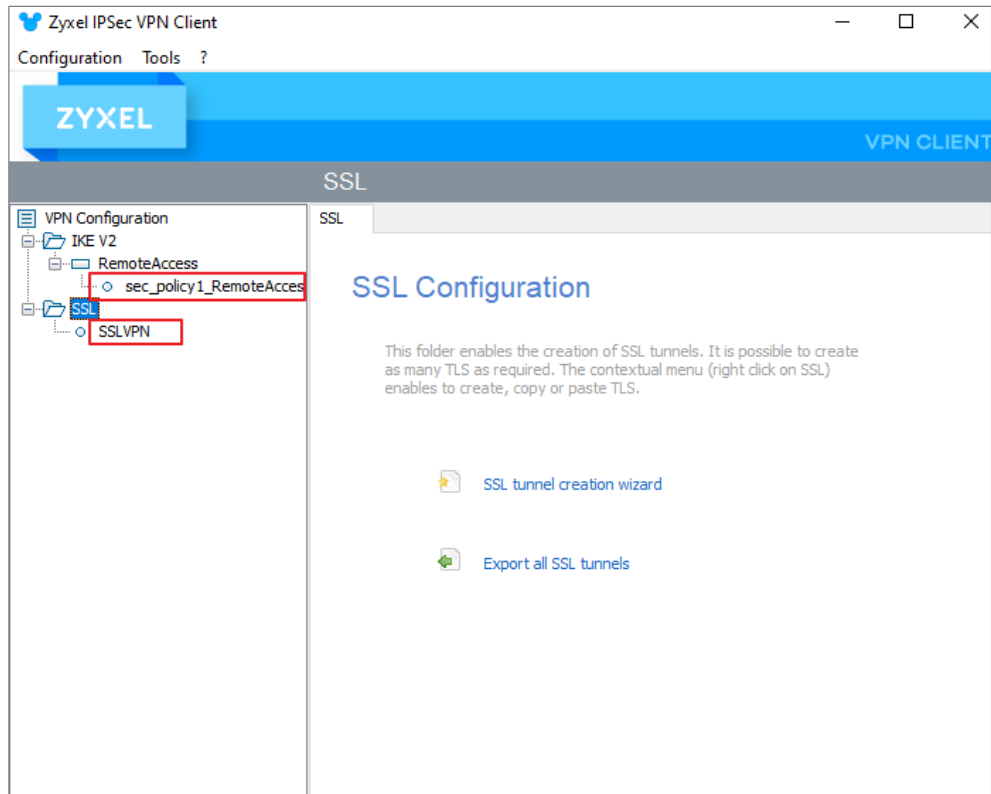
Gateway Address:
Port:

Authentication:

Login:

Password:

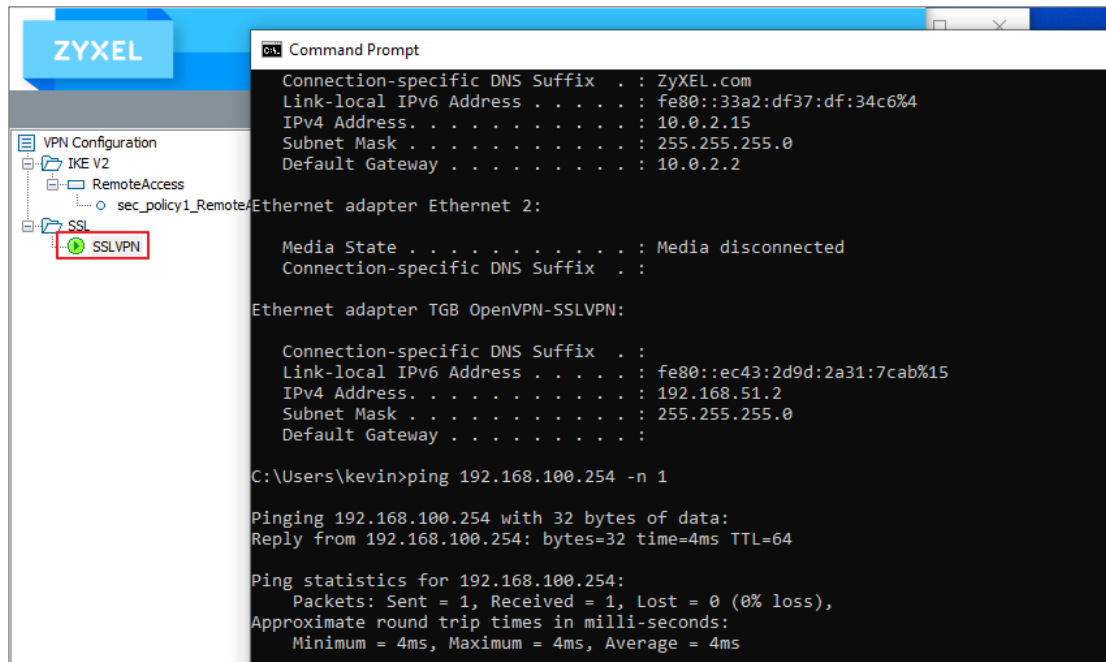
You will obtain IKEv2 as well as SSLVPN settings.



Test SSLVPN Tunnel on TGB Client

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

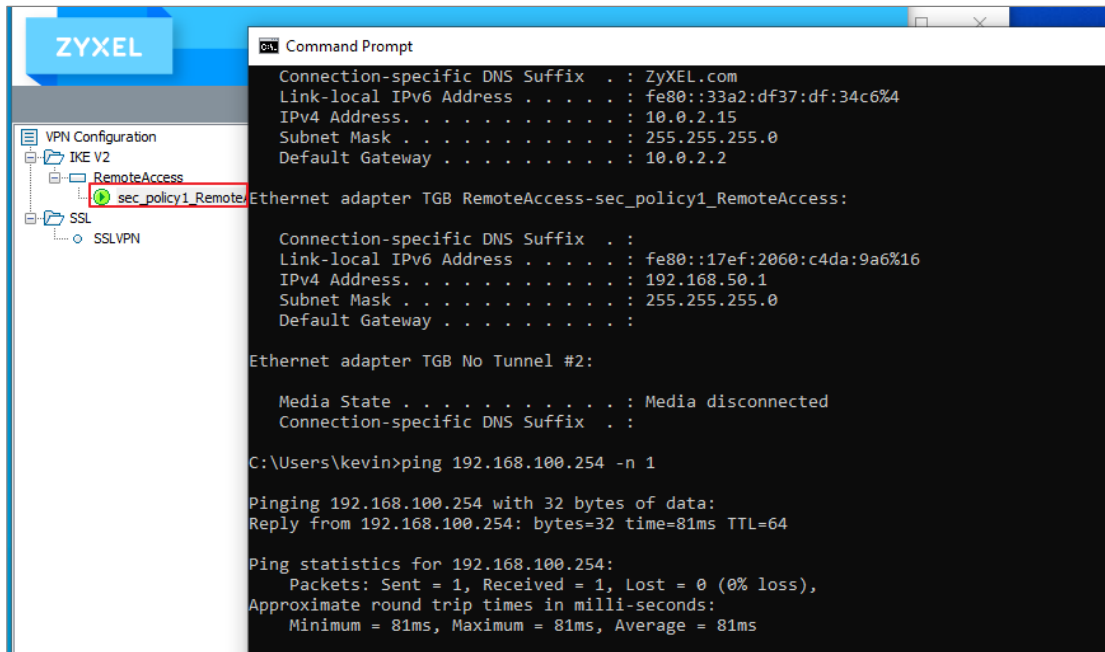
You will see the profile being green and can access internal resource now.



Test IKEv2 Tunnel on TGB Client

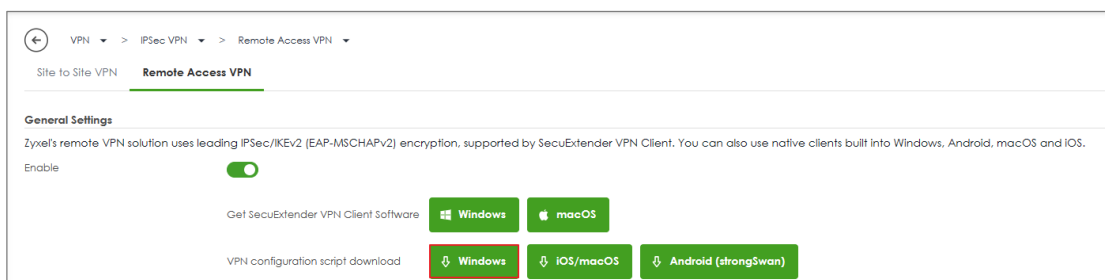
Right click the profile and "Open Tunnel" and log in.

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

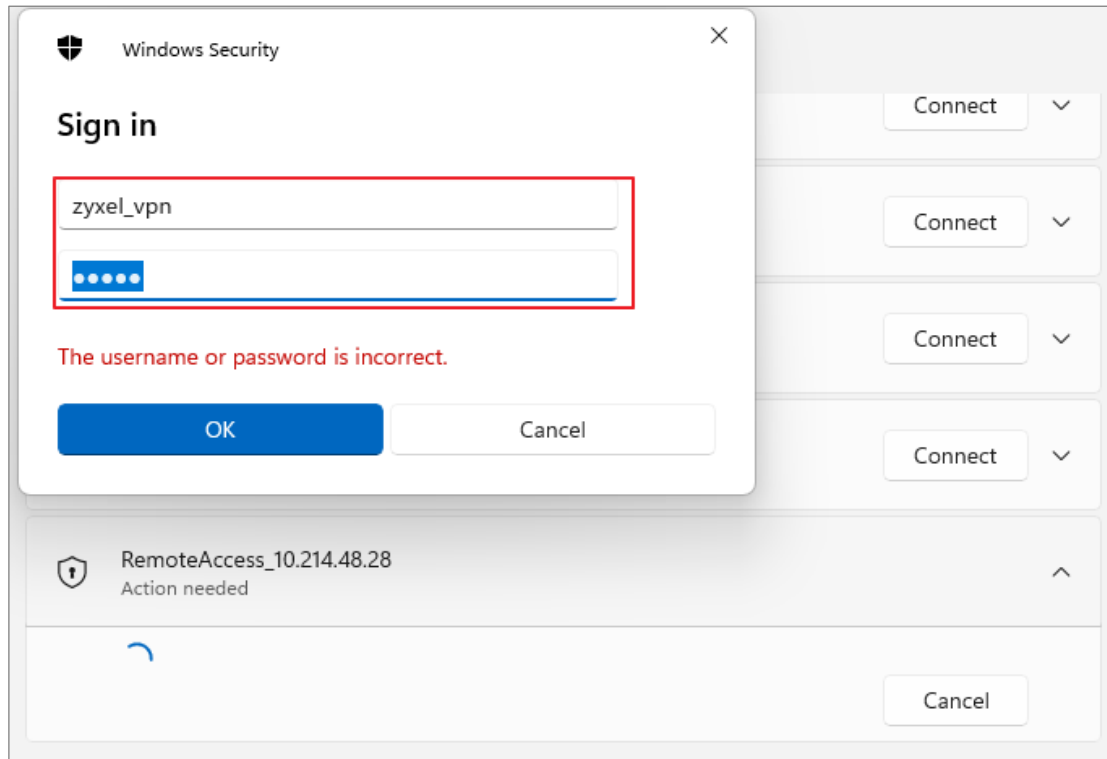


Test IKEv2 Tunnel on Windows Client

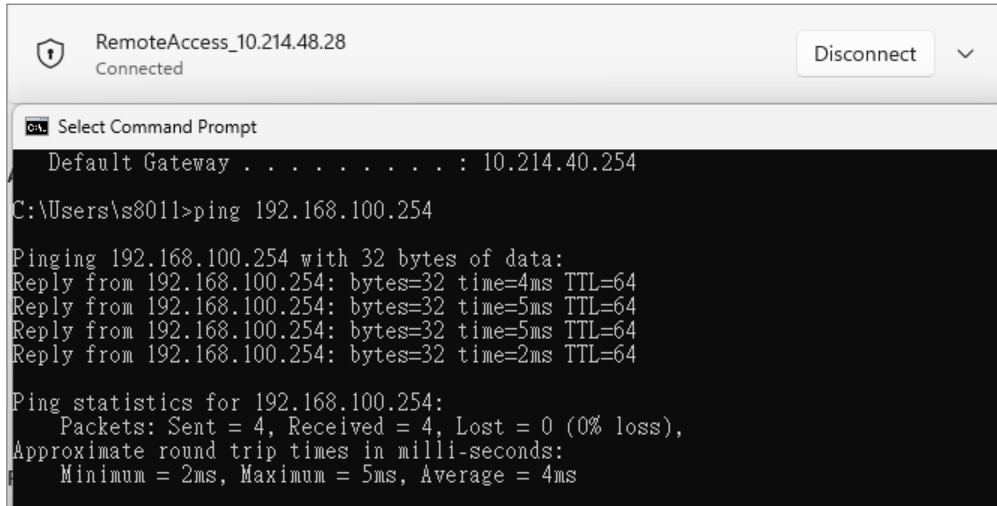
Download Windows VPN configuration script



Perform the windows bat file and input credentials.

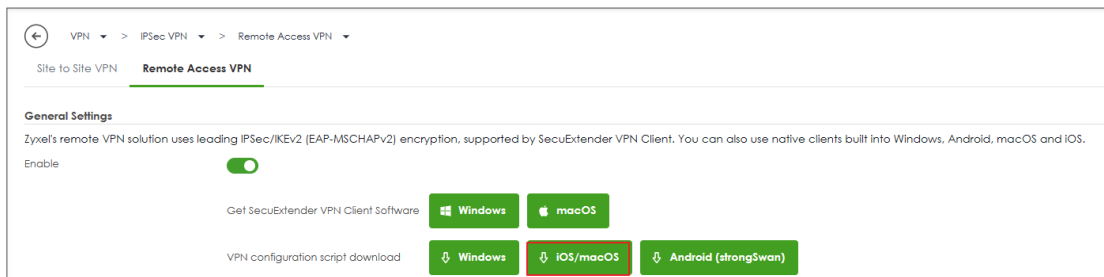


VPN is connected and can access internal resource.

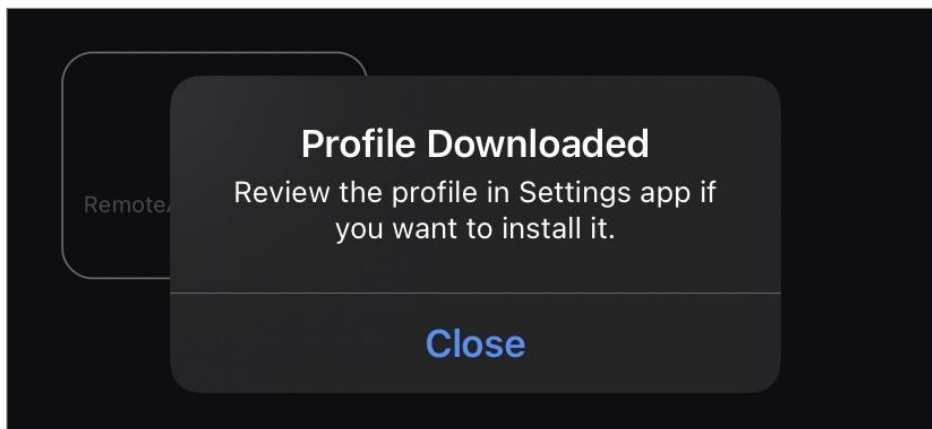


Test IKEv2 Tunnel on iOS Client

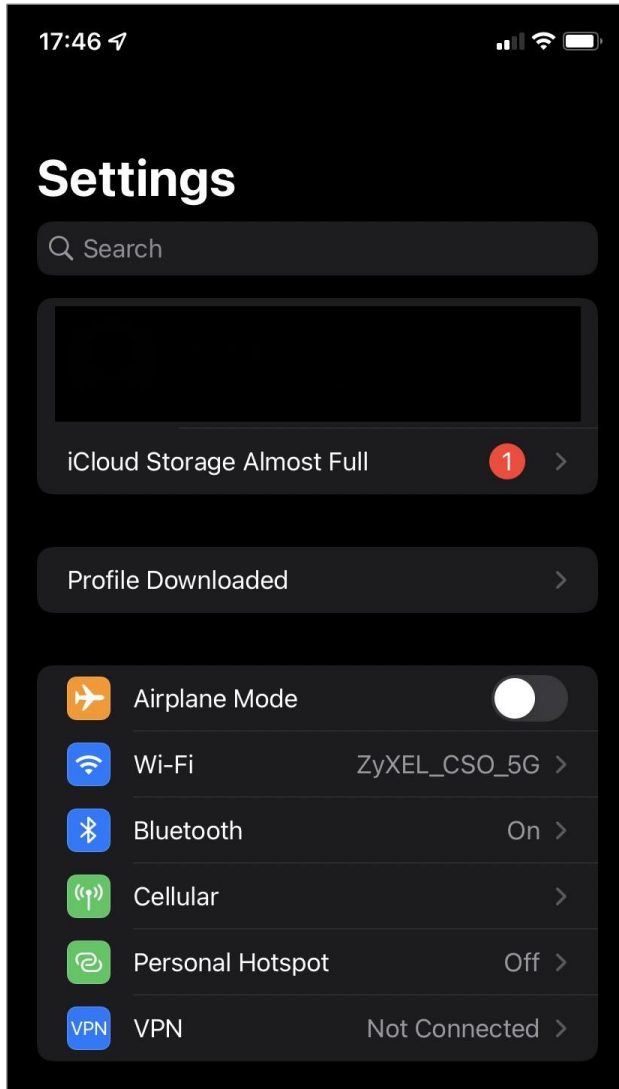
Download iOS/macOS VPN configuration script.



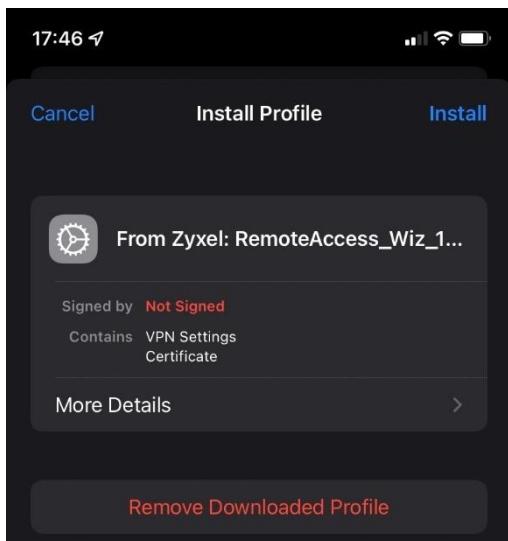
Send the script to Device.



Settings > Profile Downloaded



Press Install.



Enter Username and Password.

A screenshot of an iPhone screen showing the 'Enter Username' dialog. The status bar at the top shows the time 17:46 and signal indicators. The dialog has a light gray background with a title bar containing 'Cancel', 'Enter Username', and 'Next' buttons. The main content area has the text 'ENTER YOUR USERNAME FOR THE VPN PROFILE "VPN"'. Below this is a text input field containing 'zyxel_vpn' with a clear button (an 'x' in a circle) to its right. At the bottom, it says 'Requested by the "From Zyxel: RemoteAccess_Wiz_10.214.48.28" profile'.

[Cancel](#)
Enter Password
[Next](#)

ENTER YOUR PASSWORD FOR THE VPN PROFILE
"VPN"

✕

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

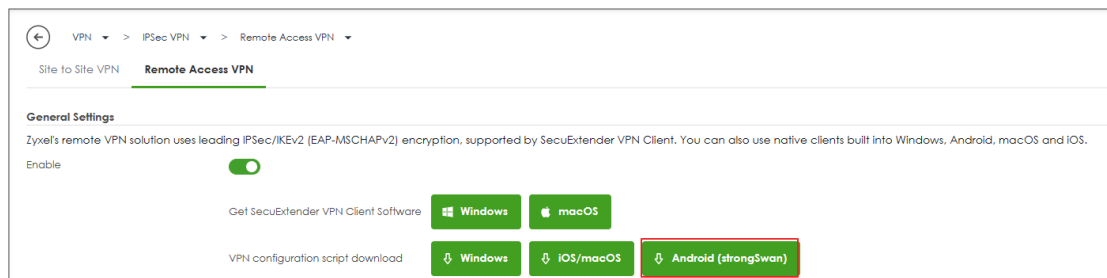
Now, it can connect.

[<](#)
RemoteAccess_Wiz_10.214.48.28
[Edit](#)

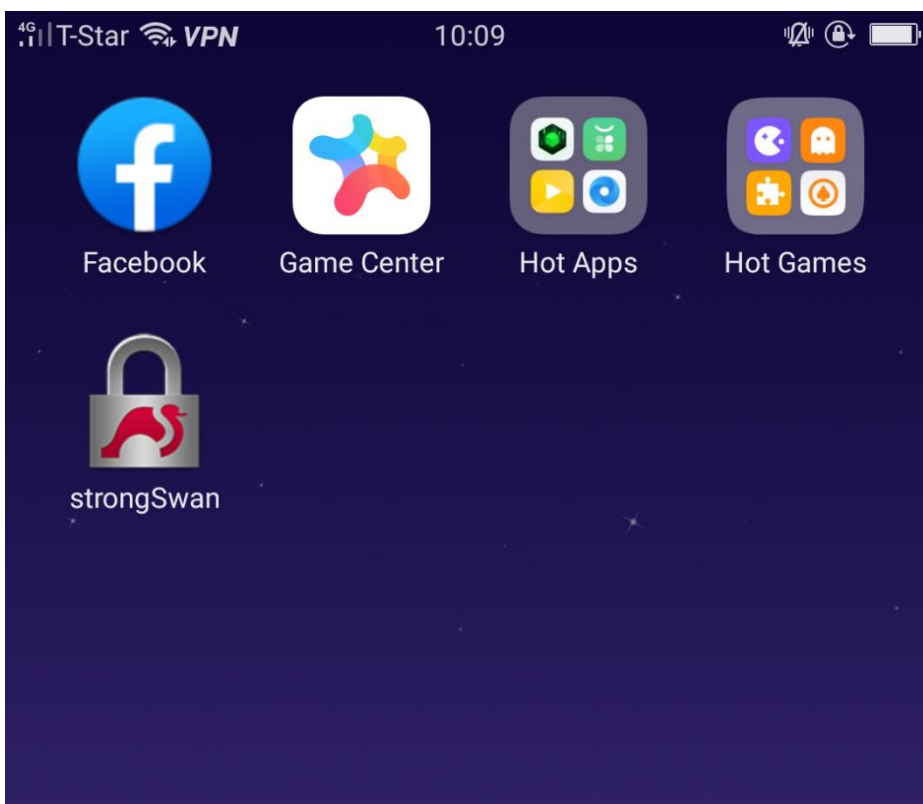
Type	IKEv2
Server	10.214.48.28
Account	zyxel_vpn
Address	192.168.50.1
Connect Time	0:09

Test IKEv2 Tunnel on Android Client

Download Android(strongSwan) VPN configuration script.



Download strongSwan from Google Play Store.



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

15:51

Import VPN profile **IMPORT**

Profile name
RemoteAccess_10.214.48.28

Server
10.214.48.28

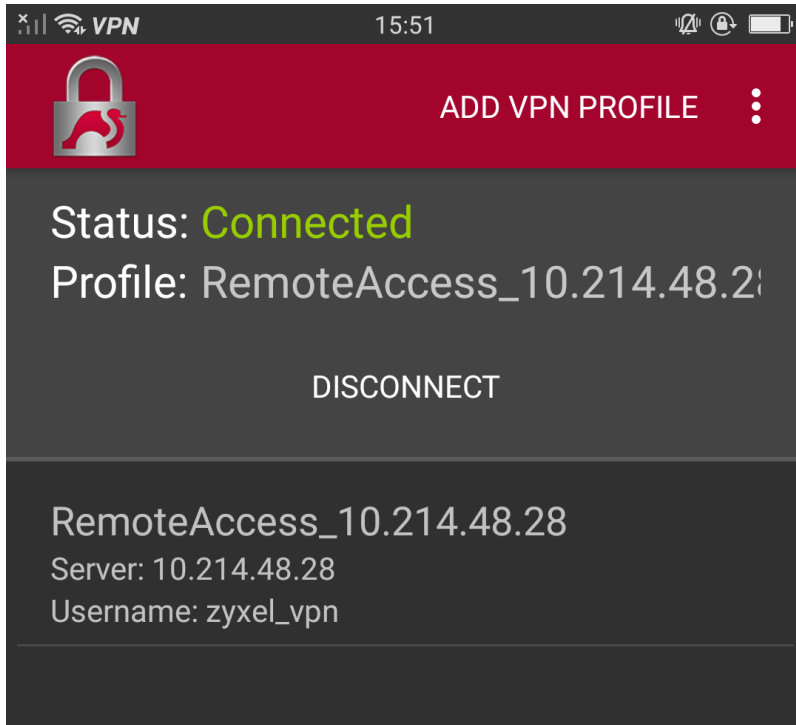
VPN Type
IKEv2 EAP (Username/Password)

Username
zyxel_vpn

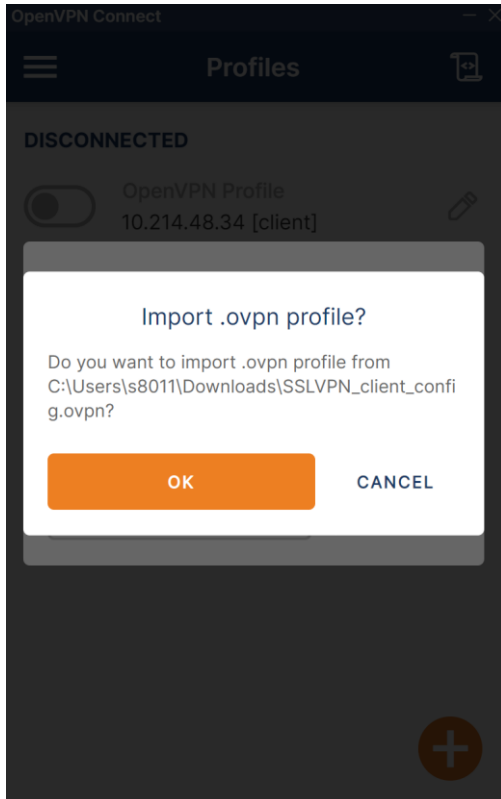
Password (optional)
.....

CA certificate
10.214.48.28

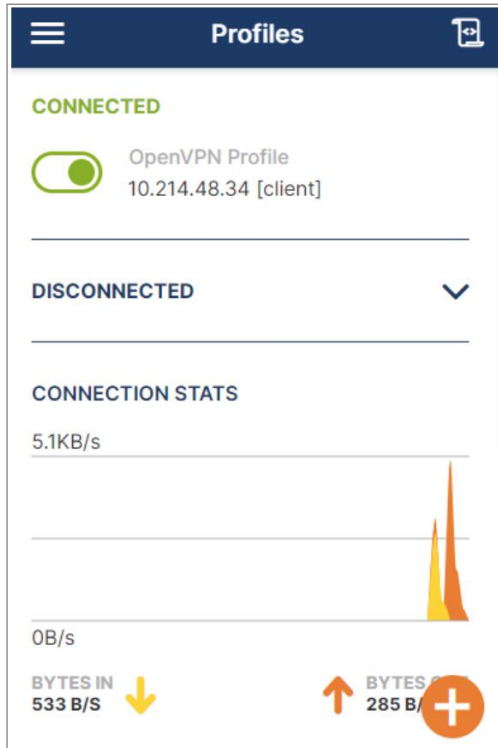
VPN is connected.



Import the config file.

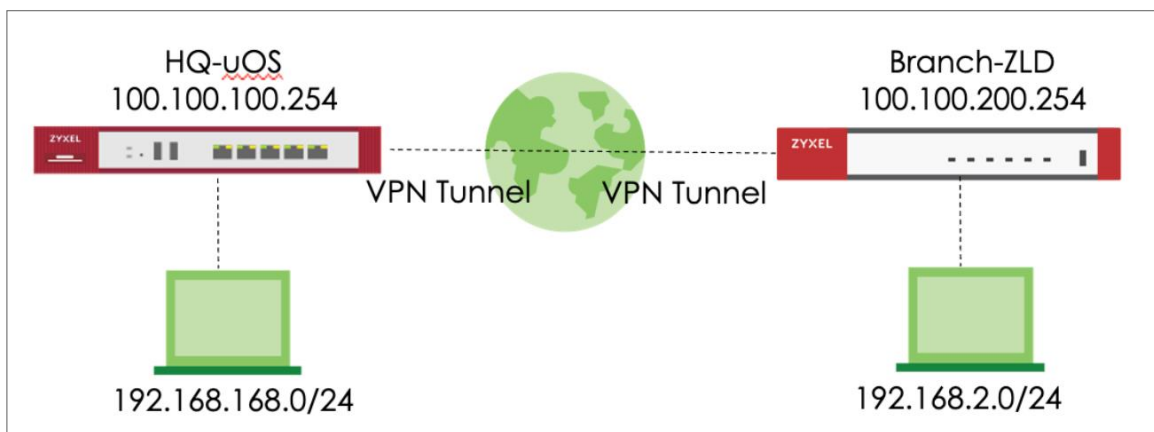


VPN is connected.



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**.

Search

My Favorite

System Statistics

Security Statistics

Network Status

VPN Status

Licensing

Network

VPN

Site to Site VPN

Security Policy

Object

Security Service

User & Authentication

System

Log & Report

Maintenance

VPN > Site to Site VPN

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

Local Site Internet Remote Site

Cancel Next

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	100.100.100.254
Peer Gateway Address	Domain Name / IP	100.100.200.254

Local Site

100.100.100.254

Internet

Remote Site

100.100.200.254

Cancel

Back

Next

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

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

VPN > Site to Site VPN

✓ Scenario — ✓ Network — **3 Authentication** — 4 Policy & Routing — 5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate

.....

default

Cancel Back Next

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.

VPN > Site to Site VPN

Scenario

Network

Authentication

4 Policy & Routing

5 Summary

Type

☐ Route-Based
 ☒ Policy-Based

Local Subnet

192.168.168.0/24

Remote Subnet

192.168.2.0/24

192.168.168.0/24

Local Site

100.100.100.254

Internet

Remote Site

100.100.200.254

192.168.2.0/24

Cancel

Back

Finish

Set up IPsec VPN Tunnel for ZLD

VPN > IPsec VPN > VPN Gateway

Select the WAN interface and type the Peer Gateway Address.

+ Add VPN Gateway [?] [X]

Show Advanced Settings Create New Object ▼

General Settings

☒ Enable

VPN Gateway Name:

IKE Version

☐ IKEv1

☒ IKEv2

Gateway Settings

My Address

☒ Interface Static -- 100.100.200.254/255.255.0.0

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address ⓘ

Primary

Secondary

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: (60-86400 seconds)

☐ Dynamic Address ⓘ

OK Cancel

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

OK Cancel

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

Show Advanced Settings Create New Object ▼

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

OK Cancel

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

+ Add VPN Connection [?] [X]

☐ Hide Advanced Settings ☐ Create New Object ▼

Phase 2 Setting

SA Life Time: (180 - 3000000 Seconds)

Advanced

Active Protocol:

Encapsulation:

Proposal

#	Encryption	Authentication
1	AES128	SHA1

Perfect Forward Secrecy (PFS): ⓘ

Related Settings

Zone: ⓘ

Connectivity Check

☒ Enable Connectivity Check ⓘ

Check Method:

OK Cancel

Test IPSec VPN Tunnel

VPN Status > IPSec VPN

Verify the IPSec VPN status on uOS device.

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	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. . . . . : 
Subnet Mask . . . . . : 
IPv4 Address. . . . . : 
Subnet Mask . . . . . : 
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:

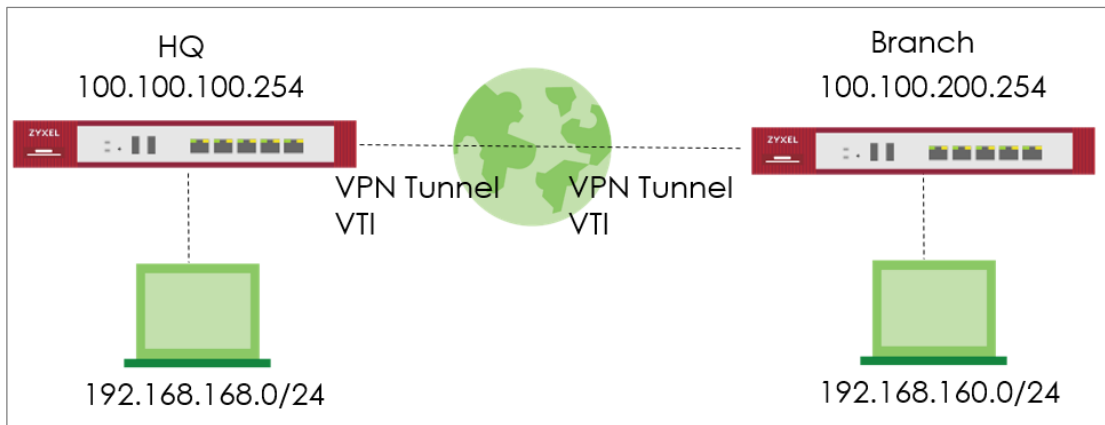
C:\Windows\system32>ping 192.168.2.34

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.



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

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

VPN > Site to Site VPN

✓ Scenario — ✓ Network — **3 Authentication** — 4 Policy & Routing — 5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate

.....

default

Cancel Back Next

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

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

VPN > Site to Site VPN

Scenario Network Authentication **4 Policy & Routing** 5 Summary

Type ☒ Route-Based ☐ Policy-Based

Remote Subnet 192.168.160.0/24

Any Local Site 100.100.100.254 Internet Remote Site 100.100.200.254 192.168.160.0/24

Cancel Back Finish

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
100.100.200.254

Peer Gateway Address

Domain Name / IP
100.100.100.254

Local Site
100.100.200.254

Internet

Remote Site
100.100.100.254

Cancel

Back

Next

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

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

VPN > Site to Site VPN

Scenario Network **3 Authentication** 4 Policy & Routing 5 Summary

Authentication

☒ Pre-Shared Key

☐ Certificate

.....

default

Cancel Back Next

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:

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.



The image shows a screenshot of the 'Certificate Import Wizard' window. The title bar includes a back arrow and the text 'Certificate Import Wizard'. The main content area is titled 'Certificate Store' and contains the text: 'Certificate stores are system areas where certificates are kept.' Below this, a horizontal line separates the header from the main options. The text 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' is followed by two radio button options. The first option, 'Automatically select the certificate store based on the type of certificate', is unselected. The second option, 'Place all certificates in the following store:', is selected and highlighted with a red rectangular box. Below the selected option, there is a text field labeled 'Certificate store:' containing the text 'Trusted Root Certification Authorities'. To the right of this text field is a 'Browse...' button.

← 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

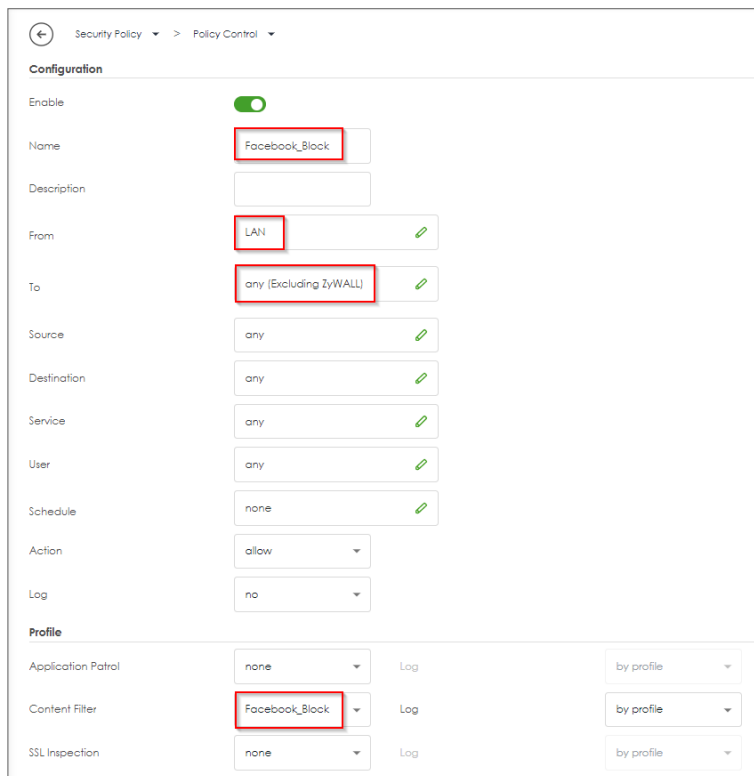
☒ Place all certificates in the following store:

Certificate store:
Trusted Root Certification Authorities

Browse...

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

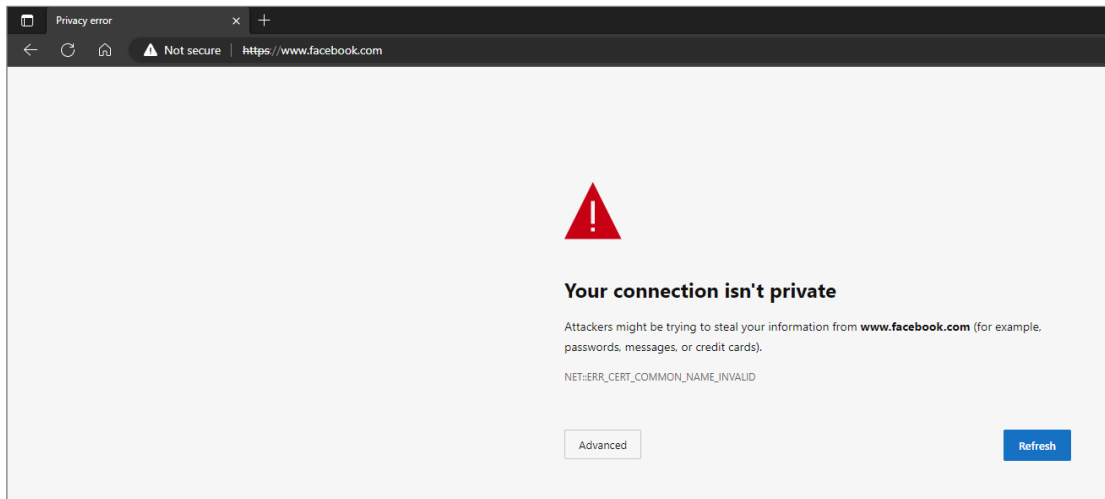
Content Filter: Facebook_Block

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.

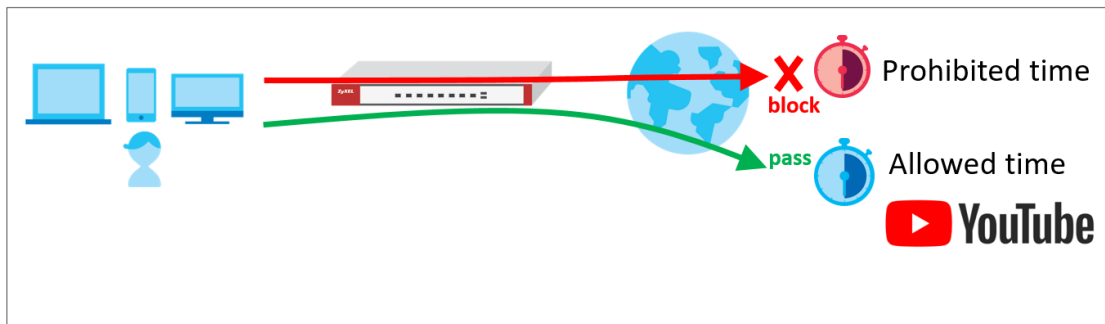


Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

#	Time	Category	Message	Source	Destination	Note
1	2023-05-22 15:36:59	content-filter	www.facebook.com:Block List, Rule_name:Facebook_Block, \$32IN (Content Filter)	192.168.168.33	52.23.24.55	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.


Object ▾ > Schedule ▾

Configuration

Name

Description

Day Time

Start Time  ▾

Stop Time  ▾

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 [X]

Category and Application

1 youtube [X]

2

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

Log 3 Log Alert v

Action 4 Reject v

5

Cancel Add

Set Up the Security Policy

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

←
Object ▾
>
Service ▾

Configuration

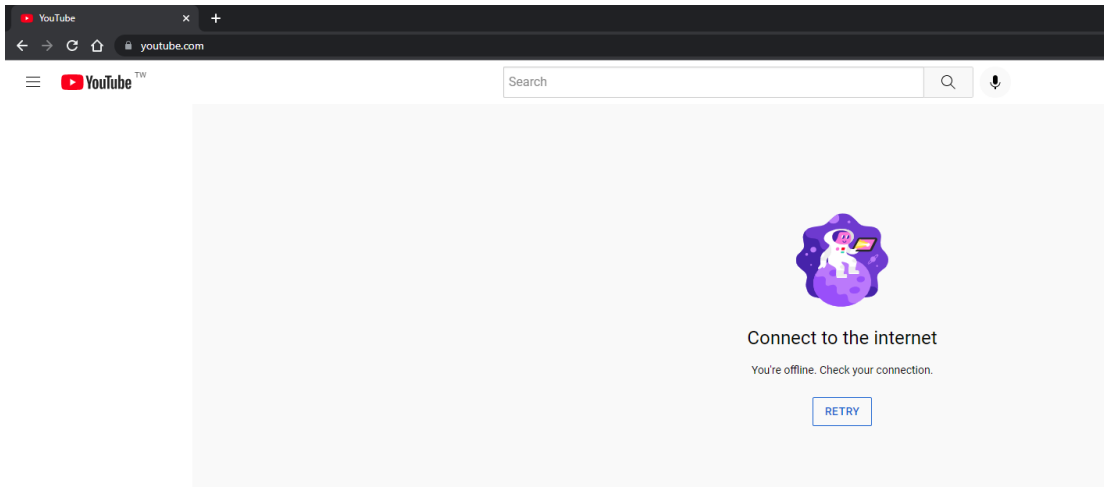
Name	QUIC_UDP_443	
Description		
IP Protocol	UDP ▾	
Starting Port	443	(1..65535)
Ending Port	443	(1..65535)

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

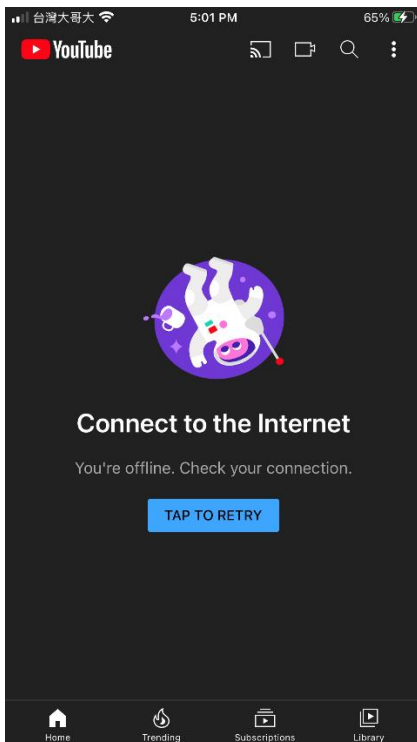
☐	Status	Priority	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log	Profile
☐		1	Block_QUIC_UDP...	LAN	WAN	LAN1_SUBNET	any	QUIC_UDP_443	any	Youtube_Block_T...	deny	log-alert	
☐		2	Block_YouTube	LAN	WAN	LAN1_SUBNET	any	any	any	Youtube_Block_T...	allow	log-alert	

Test the Result

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



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



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



App Patrol

General Settings

Collect Statistics: Enable ☒

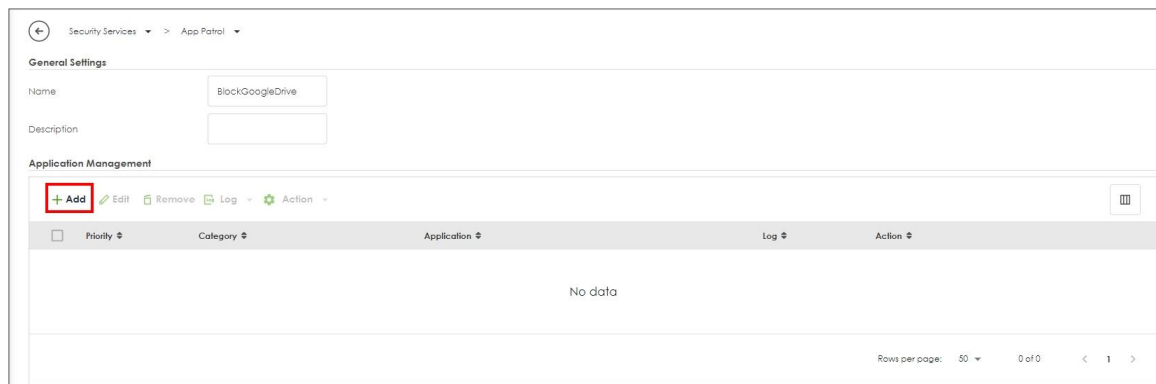
Analyze All Traffic: ☒ ⓘ

Profile Management

+ Add Edit Remove Reference

Name	Description	Reference
default_profile		1

Click add to add application in this profile.



Security Services > App Patrol

General Settings

Name: BlockGoogleDrive

Description:

Application Management

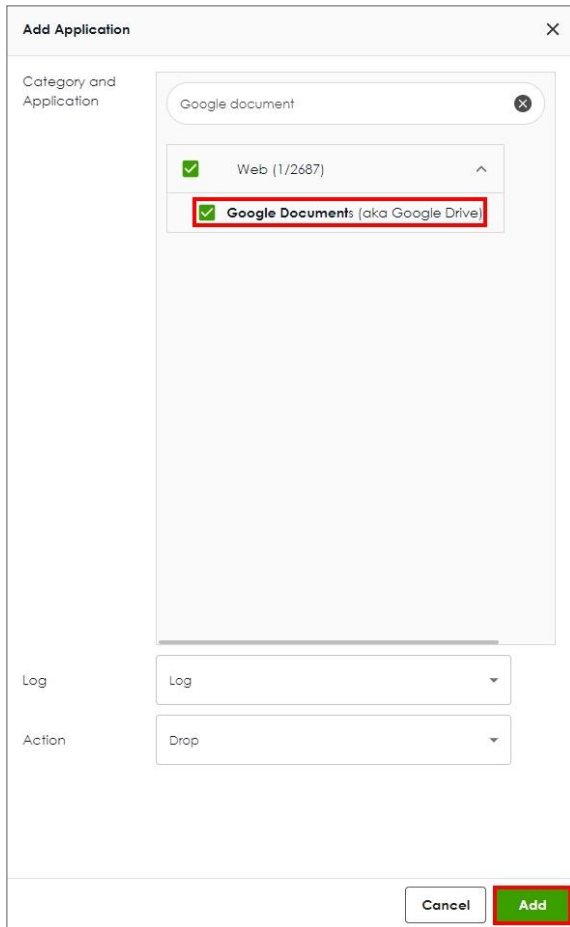
+ Add Edit Remove Log Action

Priority	Category	Application	Log	Action
No data				

Rows per page: 50 0 of 0 < 1 >

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

Cancel Add

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

+ Add Edit Remove Reference

Search insights

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.

Security Services > SSL Inspection

Configuration

Name	SSL-inspection		
Description			
CA Certificate	default		
SSL/TLS version	Minimum Support	f1s1_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.

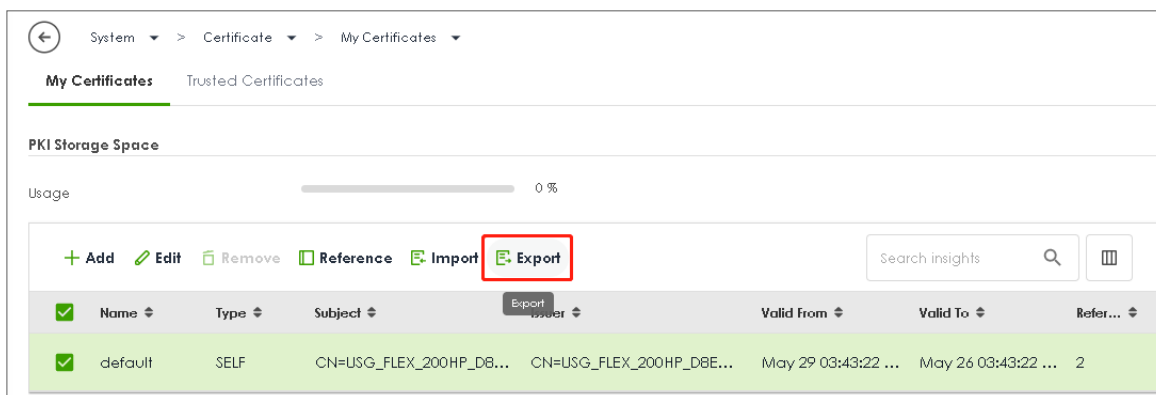
Profile

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

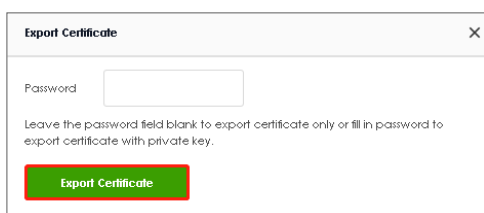
Export Certificate from FLEX and import to Lan hosts

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.

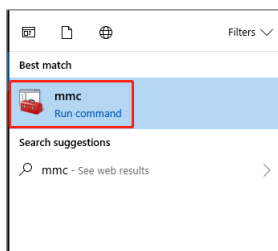
Go to System > Certificate > My Certificates to export default certificate from FLEX.



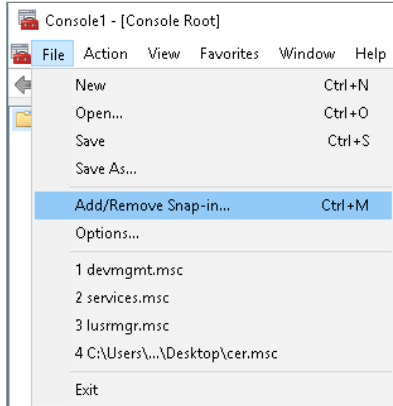
Click Export Certificate to export certificate file, and Save default certificate as default.crt file to Windows OS.



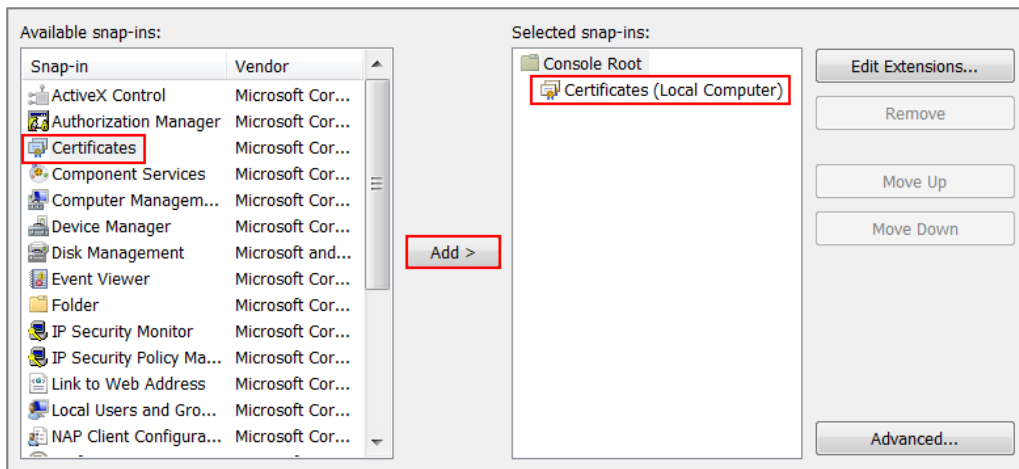
In Windows Start Menu > Search Box, type MMC and press Enter.



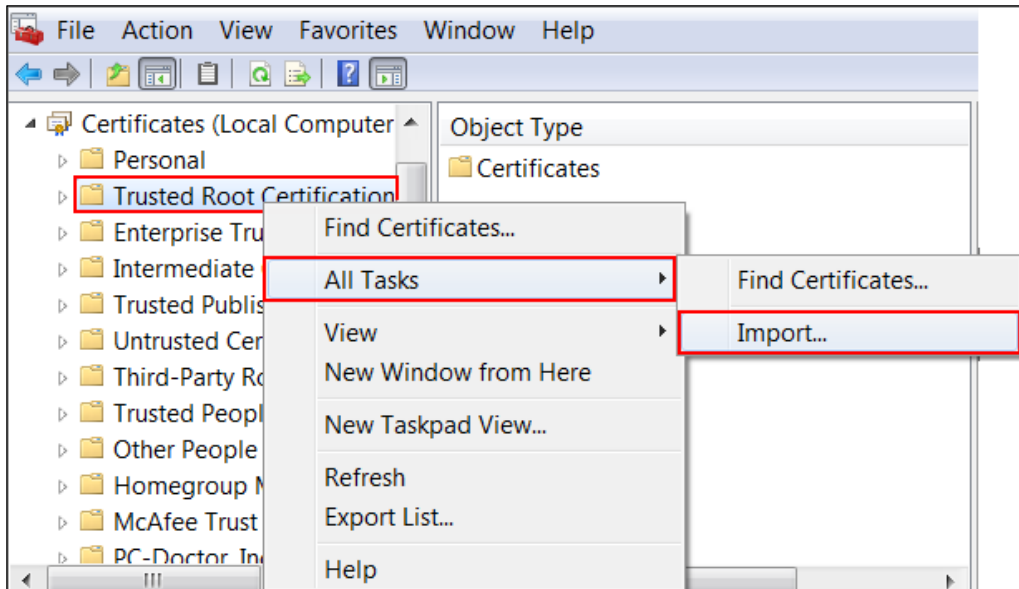
In the mmc console window, click File > Add/Remove Snap-in...



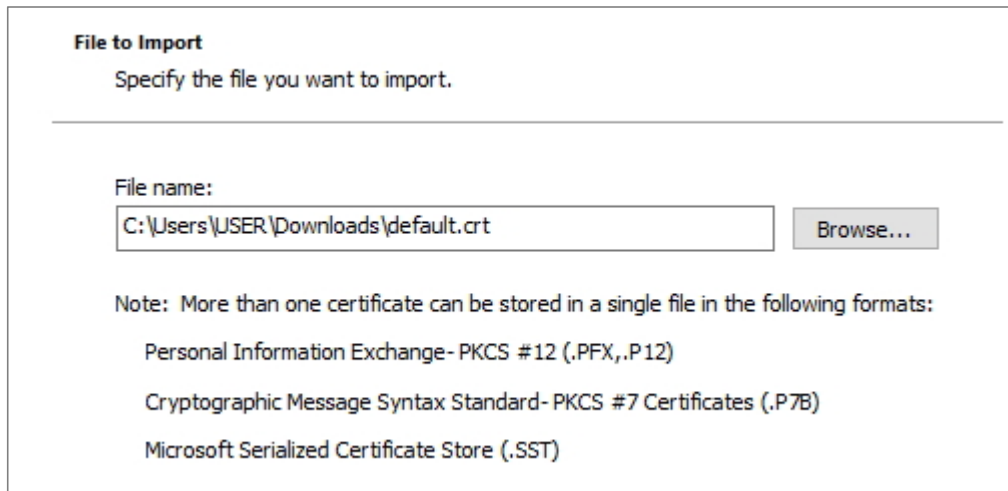
In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.



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.



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:

Test the Result

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

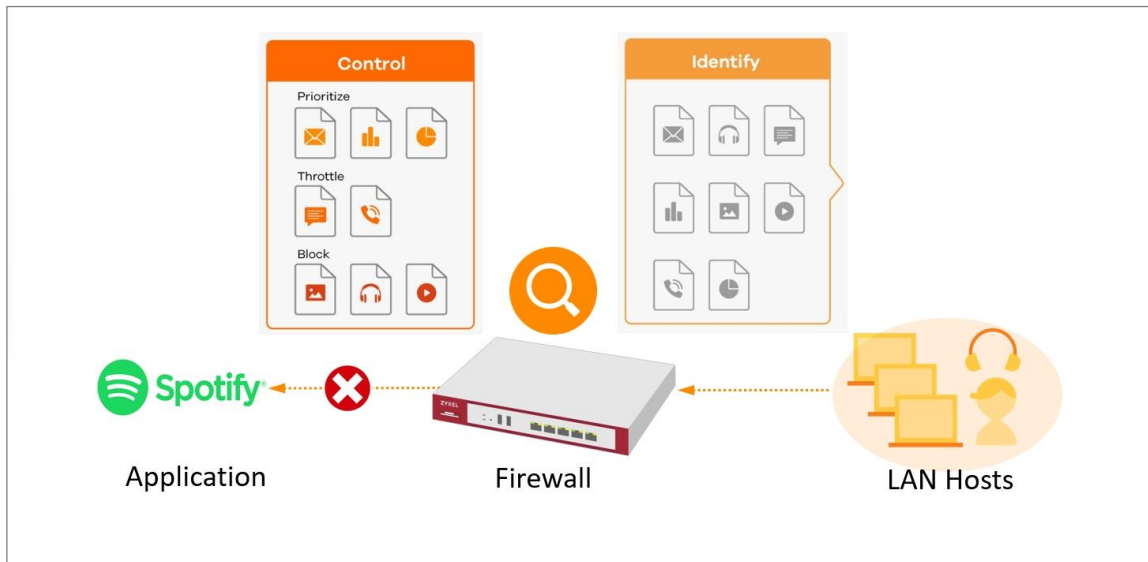
Go to Log & Report > Log/Events and select Application Patrol to check the logs.



#	Time	Category	Message	Source	Destination	Note
5	2023-09-15 14:45:53	Application Patrol	Rule_name:LAN_Outgoing App:[Web]google_docs \$ID: 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.



App Patrol

General Settings

Collect Statistics: Enable ☒

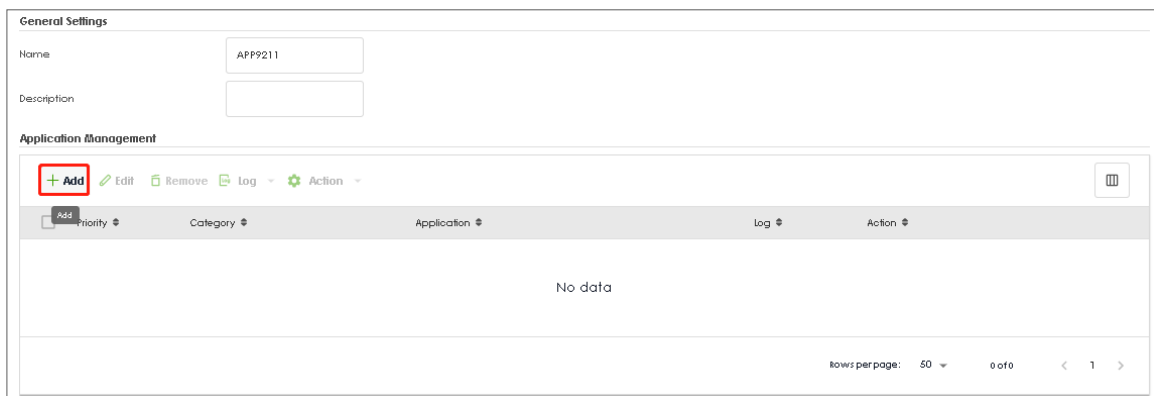
Analyze All Traffic: ☒ 1

Profile Management

+ Add Edit Remove Reference

Name	Description	Reference
default_profile		1

Click add to add application in this profile.



General Settings

Name: APP9211

Description:

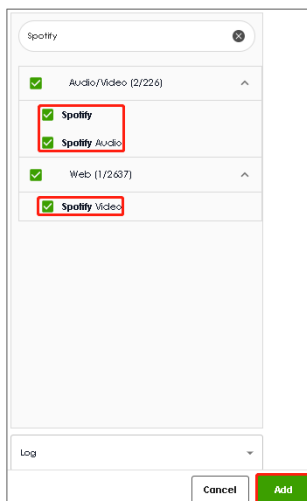
Application Management

+ Add Edit Remove Log Action

Add	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.



Spotify

Audio/Video (2/226)

- ☒ Spotify
- ☒ Spotify Audio

Web (1/2637)

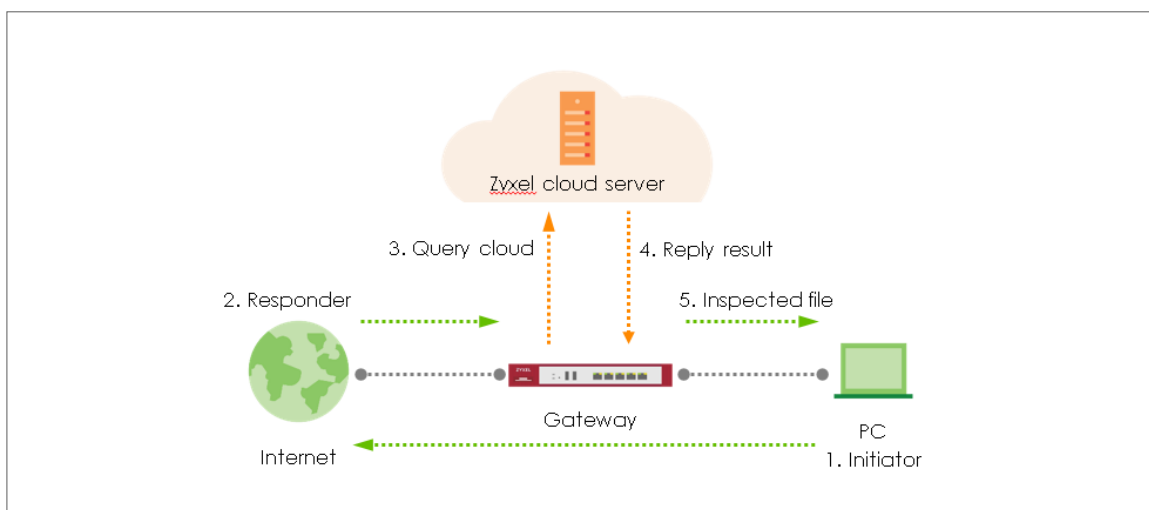
- ☒ Spotify Video

Log

Cancel Add

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.



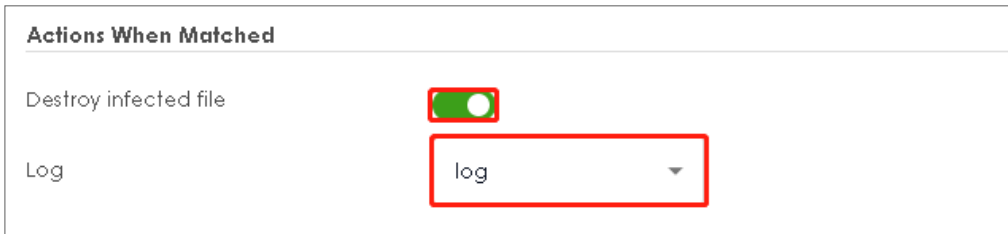
Security Service > Anti-Malware > Anti-Malware

Anti-Malware

General Settings

Enable Anti-Malware	☒
Collect Statistics	☒
Scan and detect EICAR test virus	☒
File size limit	10 (MB)

Select Destroy infected file and log in Actions When Matched



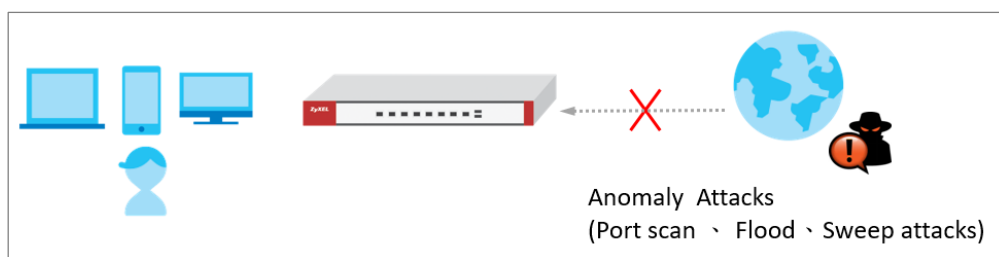
Actions When Matched

Destroy infected file	☒
Log	log

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.

Security Policy > Dos Prevention >

General Settings

Name: DoS_Prevention
Description:

Scan Detection

Sensitivity: Medium
Block Period: 5 (1-3600 seconds)

Active Inactive Log Action

Status	Name	Log	Action
☐ Active	(portscan) IP Protocol Scan	log	block
☐ Active	(portscan) TCP Portscan	log	block
☐ Active	(portscan) UDP Portscan	log	block
☐ Active	(Sweep) ICMP Sweep	log	block
☐ Active	(Sweep) IP Protocol Sweep	log	block
☐ Active	(Sweep) TCP Sweep	log	block
☐ Active	(Sweep) UDP Sweep	log	block

Flood Detection

Block Period: 5 (1-3600 seconds)

Edit Active Inactive Log Action

Status	Name	Log	Action	Threshold
☐ Active	(flood) ICMP Flood	log	block	1000
☐ Inactive	(flood) IP Flood	log	block	1000
☐ Active	(flood) TCP Flood	log	block	1000
☐ Inactive	(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

General Settings

Enable DoS Prevention ☒

Policies

+ Add Edit Remove Active Inactive Move

☐	Status	Priority	Name	From	Anomaly Profile
☐	Active	1	DoS_Prevention	WAN	DoS_Prevention

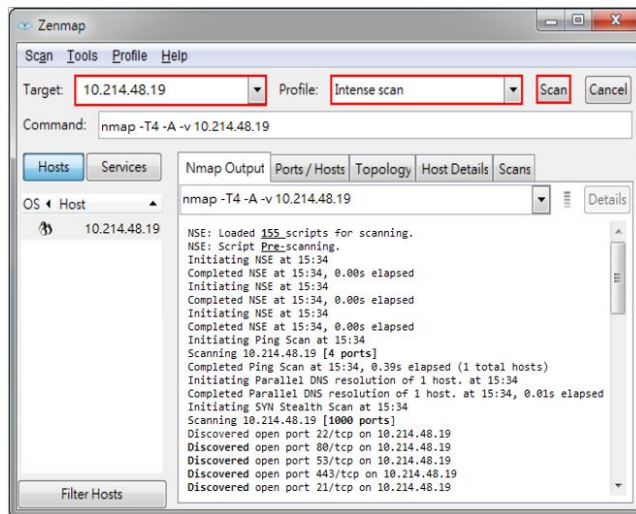
|

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.



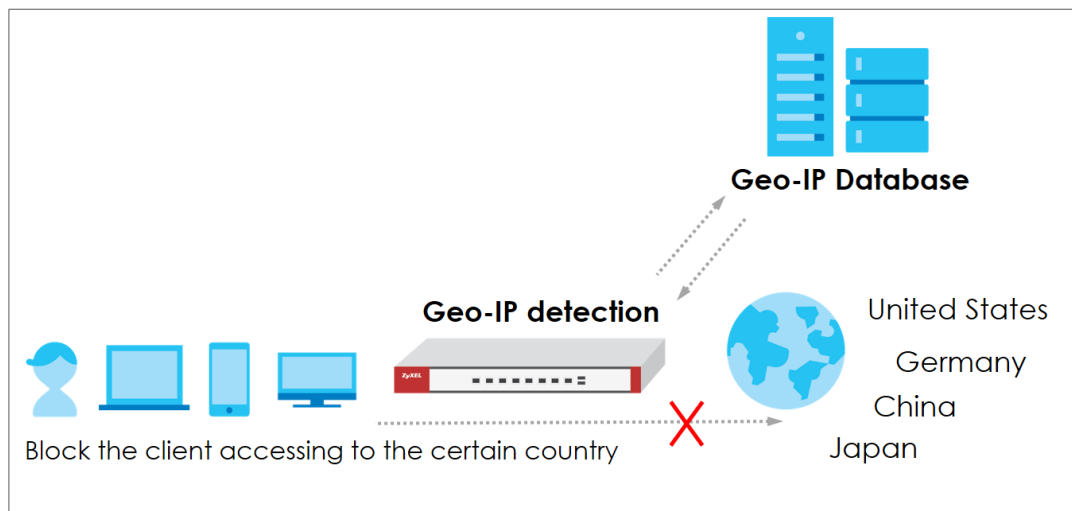
Navigate to **Log & Report > Log / Events**, you will see log of blocked messages.

Log & Report > Log / Events						
Category: All Log Filter Refresh Clear 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 Object with Geo IP

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

←
Object ▾
>
Address ▾

Configuration

Name

geo_ip

Description

Address Type

GEOGRAPHY ▾

Region

China ▾

←
Object ▾
>
Address ▾

Configuration

Name

geo_ip_2

Description

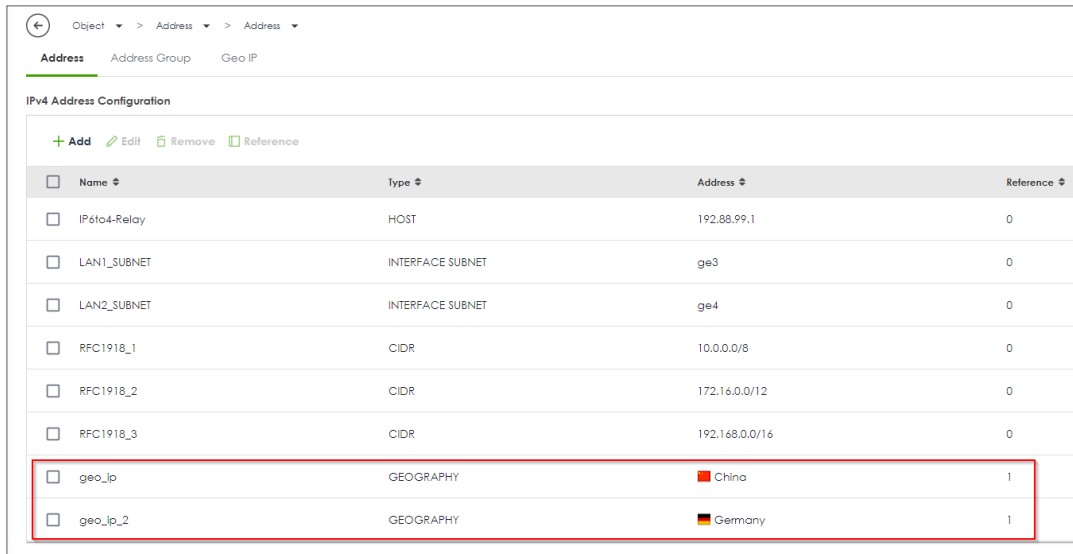
Address Type

GEOGRAPHY ▾

Region

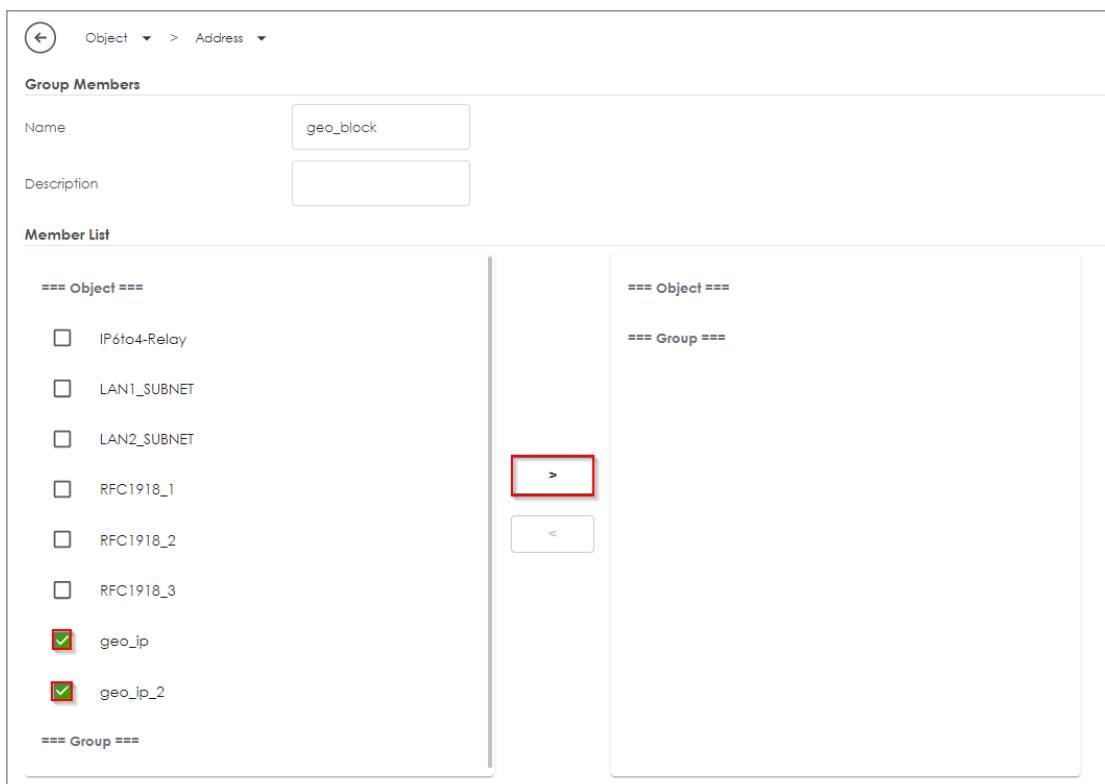
Germany ▾

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



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.



Group Members

Name:

Description:

Member List

=== Object ===

- ☐ IP6to4-Relay
- ☐ LAN1_SUBNET
- ☐ LAN2_SUBNET
- ☐ RFC1918_1
- ☐ RFC1918_2
- ☐ RFC1918_3
- ☒ geo_ip
- ☒ geo_ip_2

=== Group ===

=== Object ===

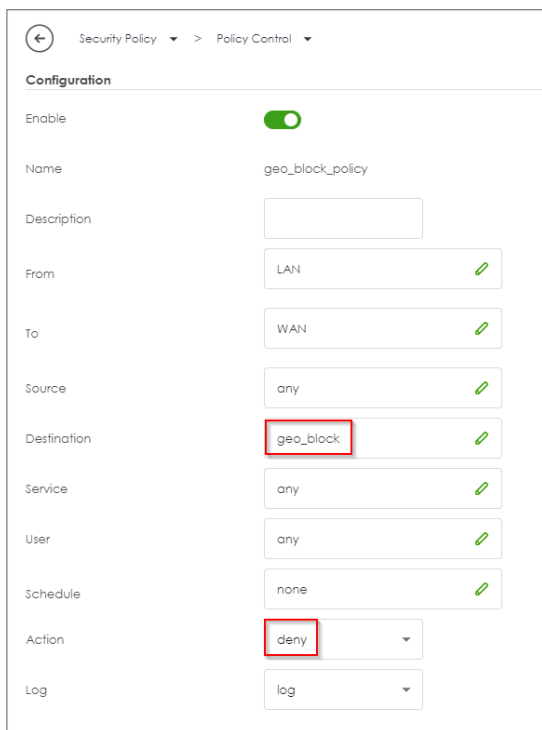
=== Group ===

>

<

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).



Security Policy > Policy Control

Configuration

Enable ☒

Name geo_block_policy

Description

From LAN

To WAN

Source any

Destination geo_block

Service any

User any

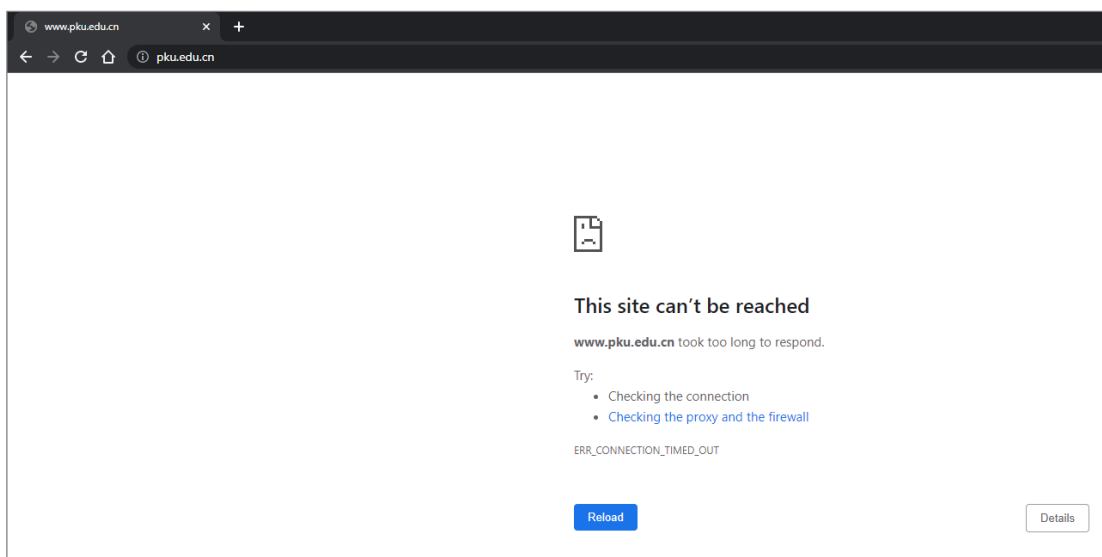
Schedule none

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.

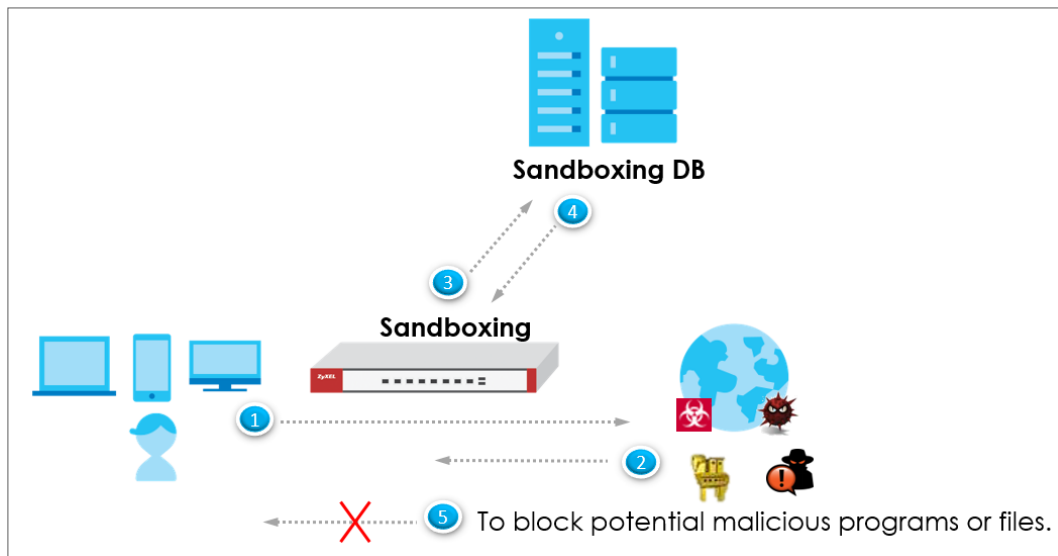


To view the log message, go to USG Flex H **Log & Report > Log / Events**. You will find log messages similar to the following. Any traffic that matches the Geo IP policy will be blocked, and the details will be displayed in the Message field.

#	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).

ZYXEL NETWORKS USG FLEX 500H

Search

Security Service > Sandbox > Sandbox

Sandbox

Enable Sandbox ☒

Collect Statistics ☒

Action For Malicious File

Log For Malicious File

Action For Suspicious File

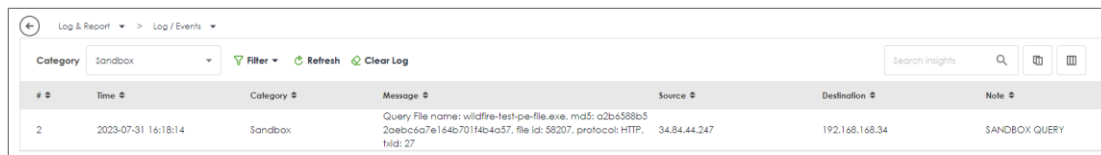
Log For Suspicious File

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: a2b6588b52aebc5a7e164b70114b4a57, file id: 58207, protocol: HTTP, tvid: 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 Reputation	DNS Threat Filter	URL Threat Filter
IP Blocking		
Enable	☒	
Action	block ▼	
Threat Level Threshold	high ▼	
Log	log ▼	
Statistics	☒	

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.

IP Reputation

DNS Threat Filter

URL Threat Filter

Allow List

Enable

Log

no

+ Add

Edit

Remove

Active

Inactive

Status

IPv4 Address

No data

Rows per page: 50

0 of 0

<

1

>

Block List

Enable

Log

log

+ Add

Edit

Remove

Active

Inactive

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

Query

Message

threat-level result: High

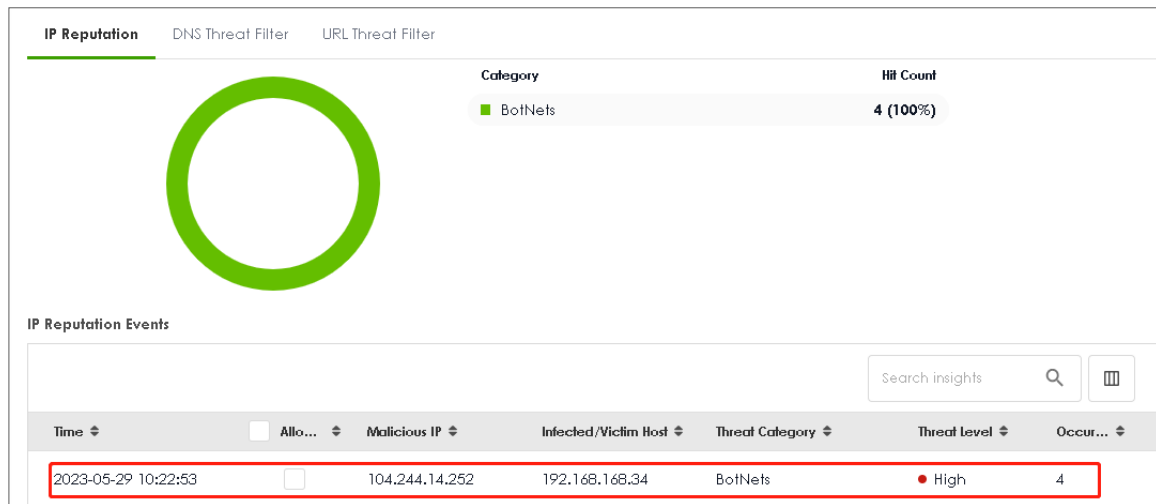
category result: BotNetsPhishing

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.

← Log & Report > Log / Events >							
Category		IP Reputation	Filter	Refresh	Clear Log		Search insights
#	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.



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.

IP Reputation
DNS Threat Filter
URL Threat Filter

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

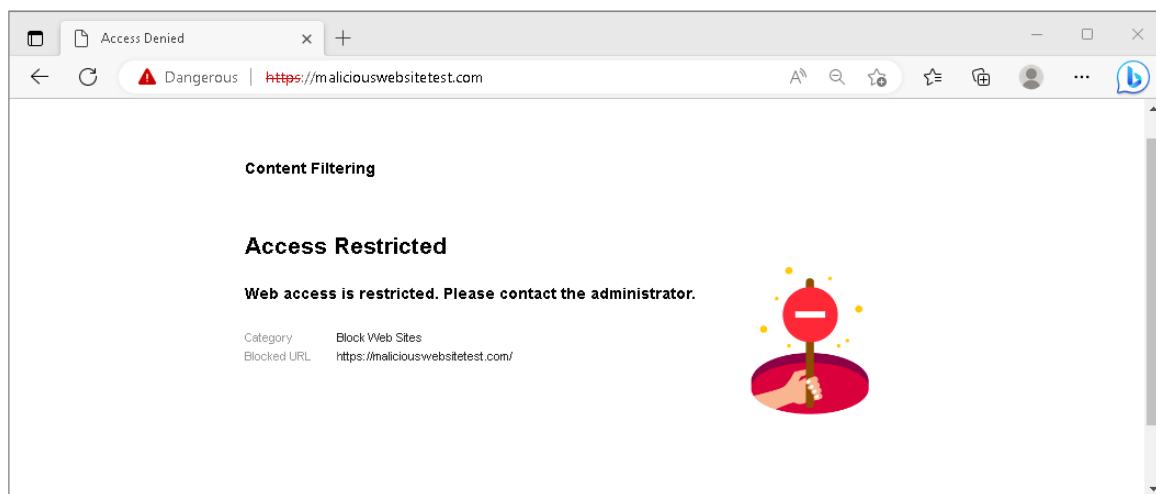
Query

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.



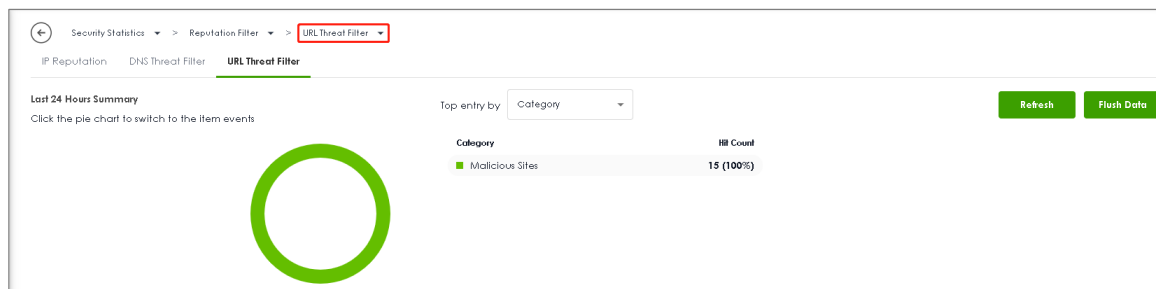
Go to Log & Report > Log/Events and select URL Threat Filter to check the logs.

Log & Report > Log / Events

Category: **URL Threat Filter** Filter Refresh Clear Log

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



URL Threat Filter Events

Search insights

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

IP Reputation
DNS Threat Filter
URL Threat Filter

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

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)

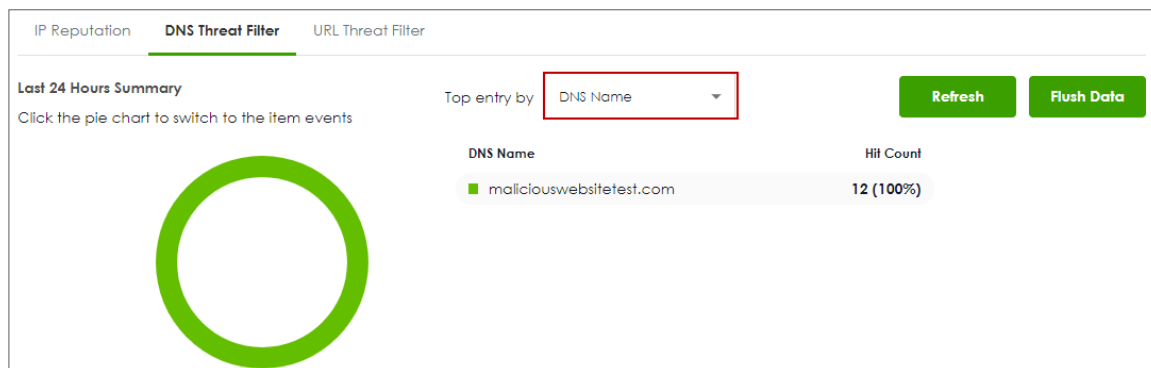
Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.



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

Category DNS Threat Filter Filter Refresh Clear Log Search insights						
#	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.



DNS Threat Filter Events

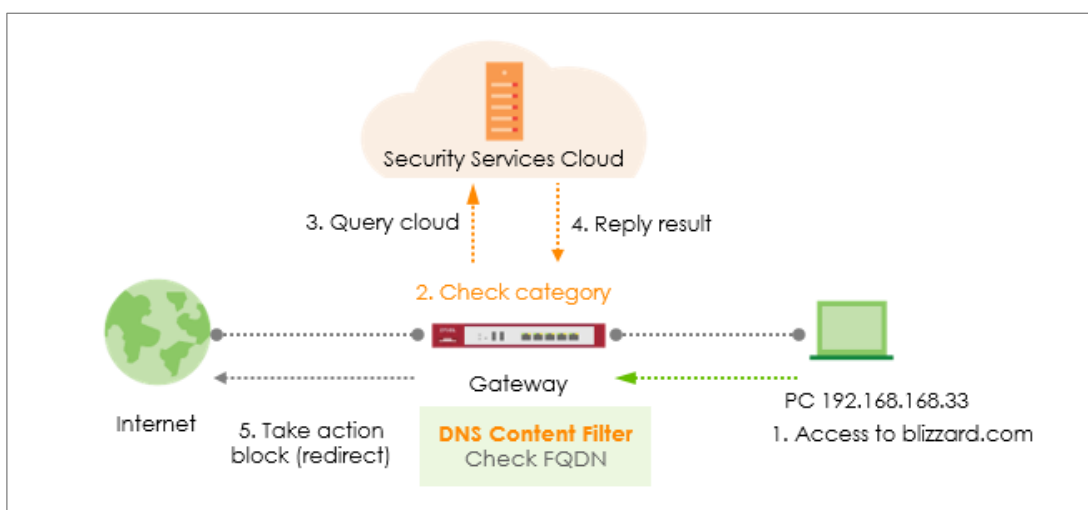
Search insights

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/>.

Content Filtering

For DNS Domain scan:

Enable DNS Domain scan
☒

Blocked Domain

Redirect IP

default

Category Server is unavailable

Action

pass

Log

log

Collect Statistics
☒

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

Profile Management

+ Add
Edit
Remove

Search insights

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

☐

SSL V3 or previous version Connection

Drop

☒

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
☐ Gruesome Content
☒ Games
☐ General News
☐ Government Military
☐ History
☐ Health
☐ Historical Revisionism
☐ Humor Comics

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

General Settings

Enable

☒

Configuration

Allow Asymmetrical Route

☐

+ Add
Edit
Remove
Active
Inactive
Move

Search insights

	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

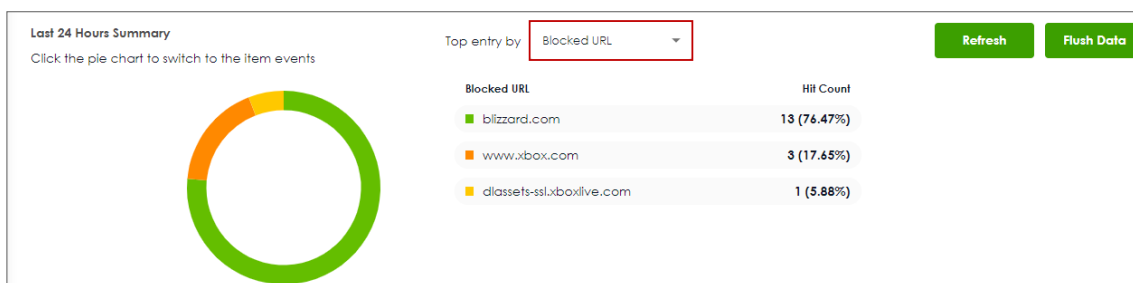
Access a gaming website blizzard.com. The gateway will redirect you to a blocked page.



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

Category: Content Filter Filter Refresh Clear Log						
#	Time	Category	Message	Source	Destination	Note
471	2023-05-28 14:36:16	content-filter	blizzard.com: Games, rule_name: LAN_Out going	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_Out going	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_Out going	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_Out going	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

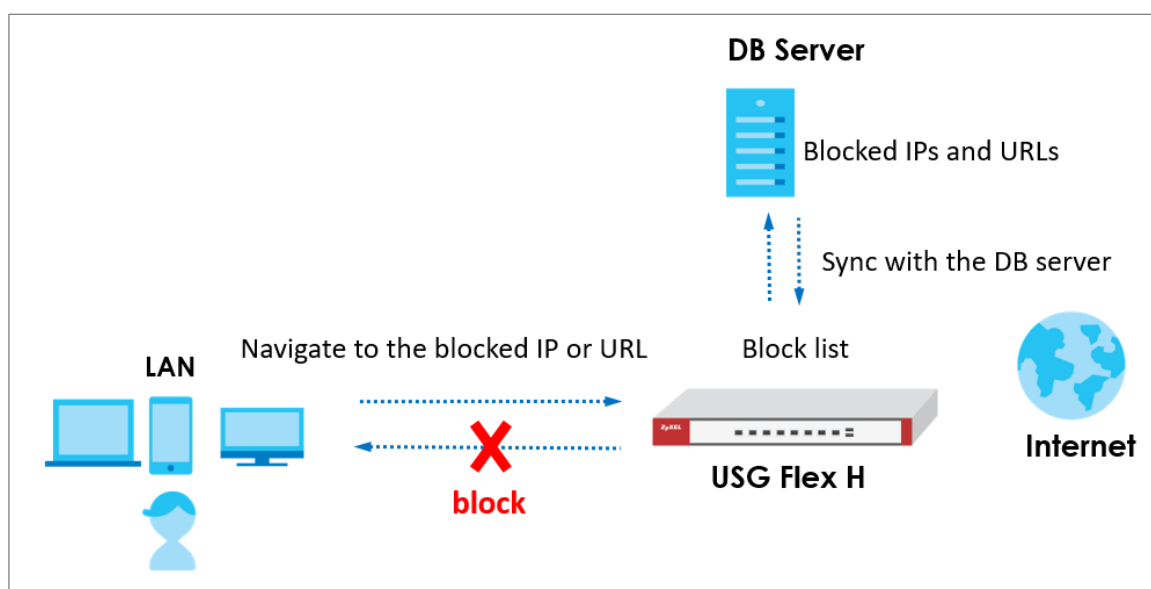
Go to Security Statistics > Content Filter to check summary of all events.



Content Filter Events						
Search insights						
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	dassets-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.

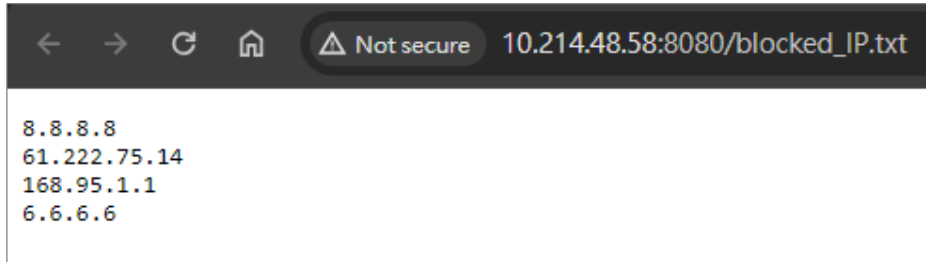


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).

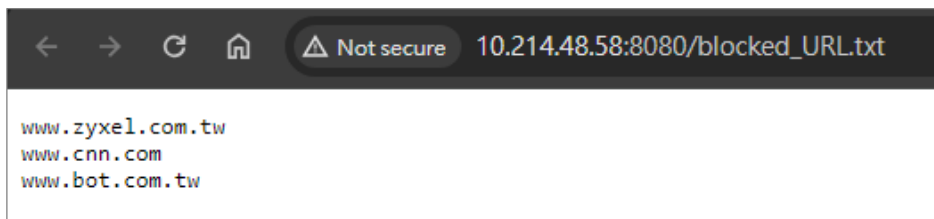
Set Up the DB server

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



http://10.214.48.58:8080/blocked_URL.txt



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

+ Add Remove

☐	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.

Update Now

Auto Update ☐

☐ Every N Hours

☒ Daily

☐ Weekly

If the IP Reputation 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

Search Inside

#	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

☒ Daily

☐ Weekly

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

Search inside

#	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.

Log & Report > Log / Events							
Category		All Log		Refresh Clear Log Export		Search insights	
#	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.

Not secure
https://www.bot.com.tw

Web Page Blocked!!

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

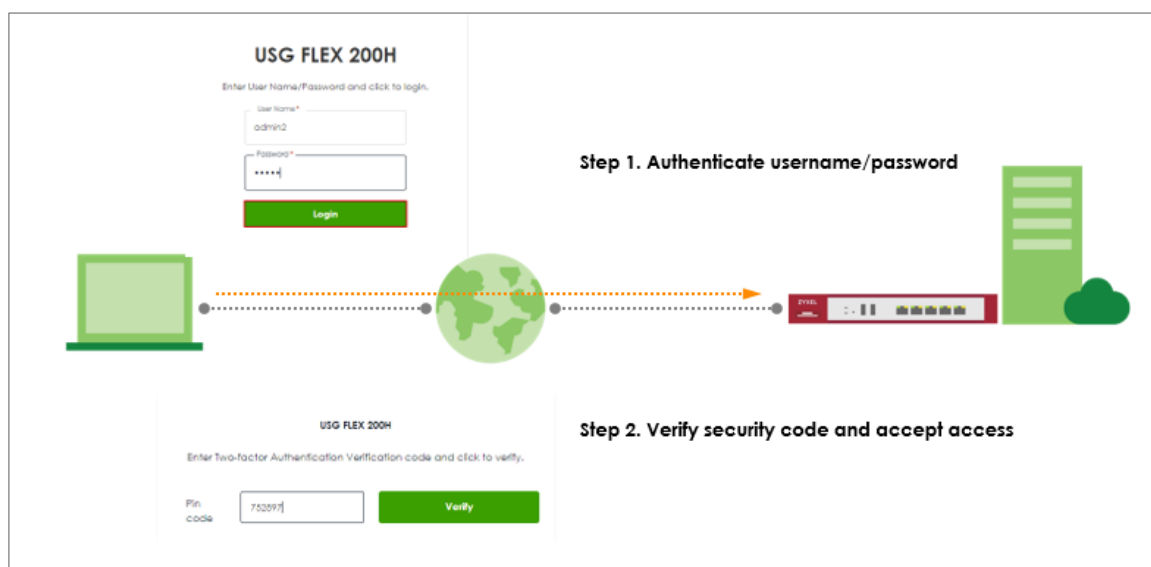
Go to Log & Report > Log / Events to observe block messages.

Log & Report > Log / Events							
Category		All Log		Refresh Clear Log Export		Search insights	
#	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.



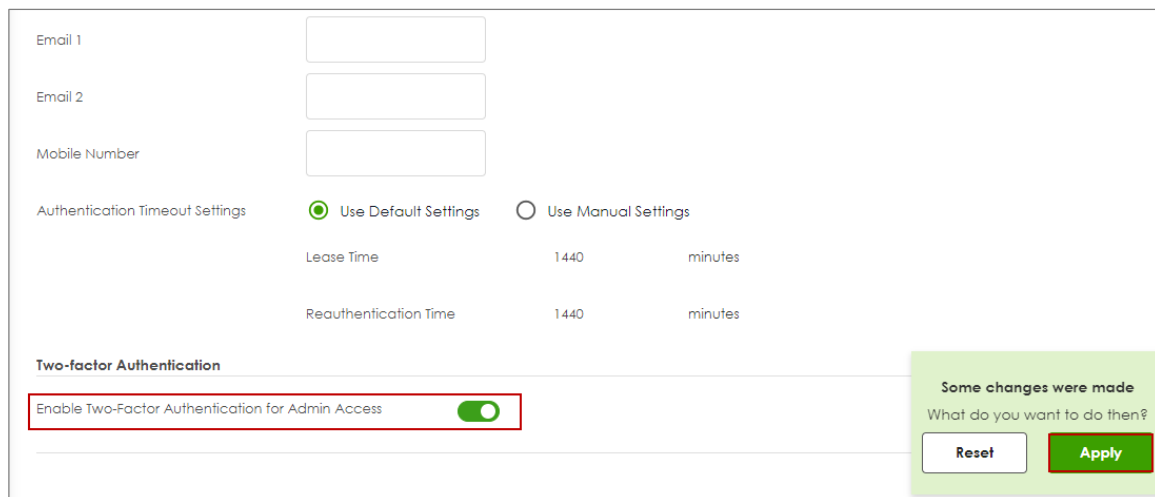
 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

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

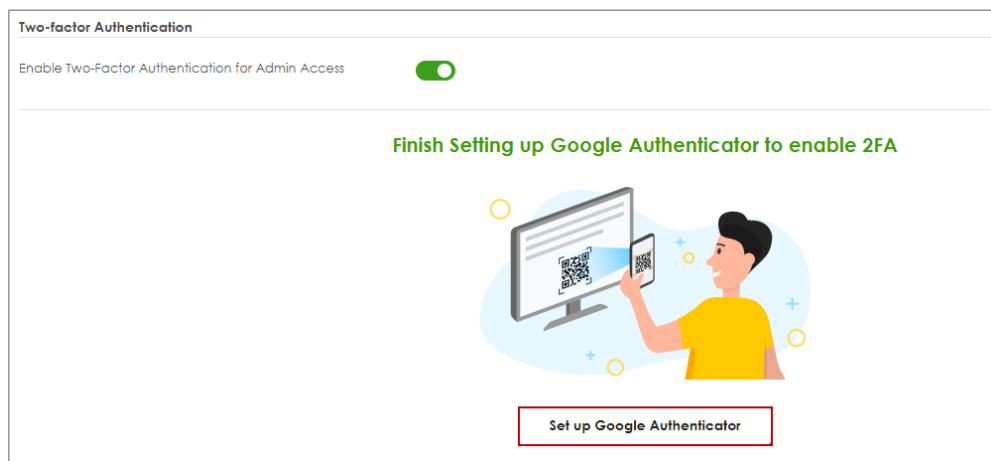
Reauthentication Time 1440 minutes

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.



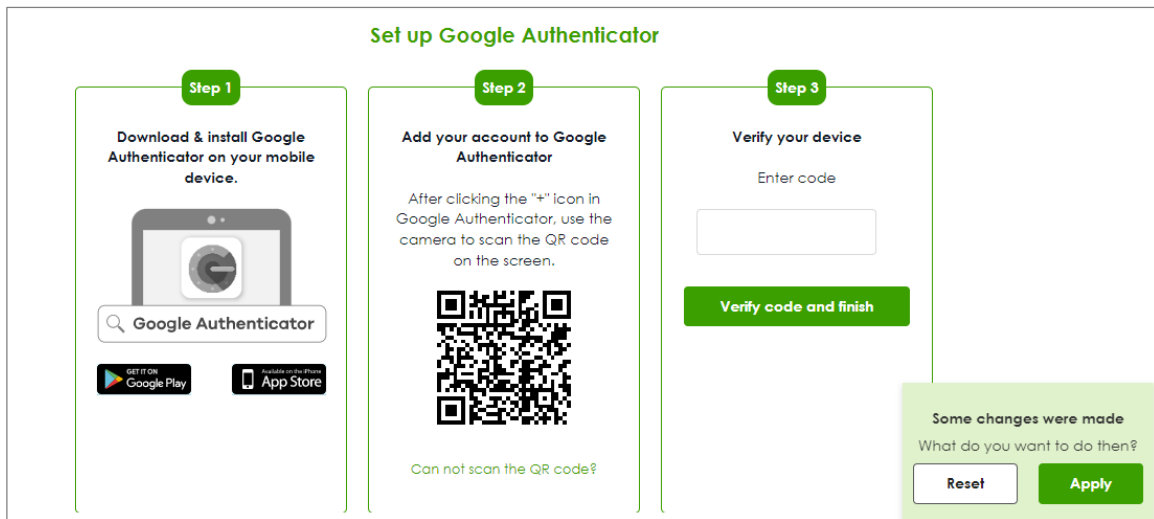
Two-factor Authentication

Enable Two-Factor Authentication for Admin Access ☒

Finish Setting up Google Authenticator to enable 2FA

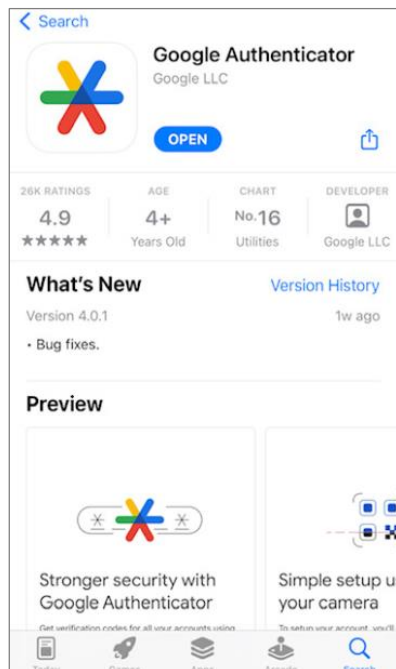
Set up Google Authenticator

Set up Google Authenticator

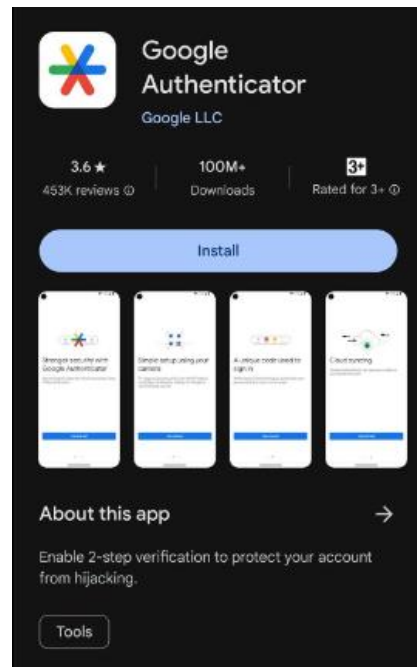


1. Download and install Google Authenticator on your mobile device.

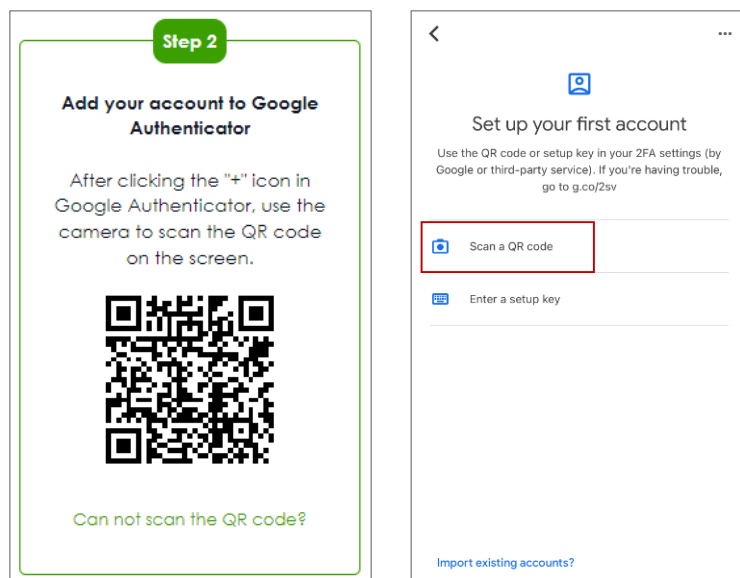
Apple Store



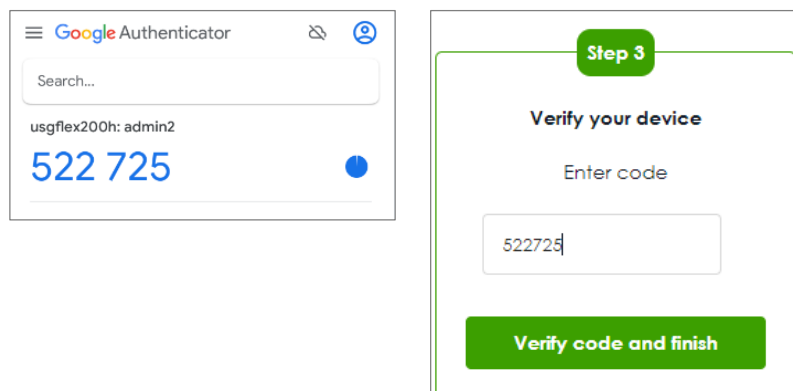
Google Play



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



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



- 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.

Download

84177830

93398990

96834809

97350265

59001448

Regenerate backup codes

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 ☒

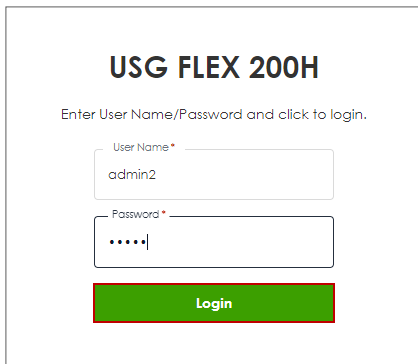
Valid Time (1-5 minutes)

Two-factor Authentication for Services:

☒ Web ☒ SSH

Test the Result

1. Login with the admin account "admin2".



USG FLEX 200H

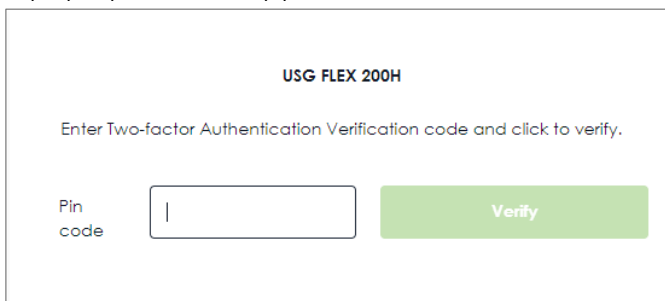
Enter User Name/Password and click to login.

User Name *
admin2

Password *
.....

Login

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



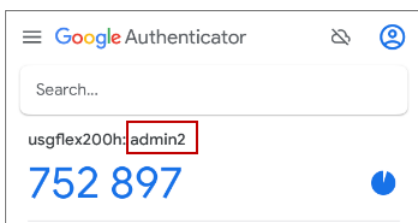
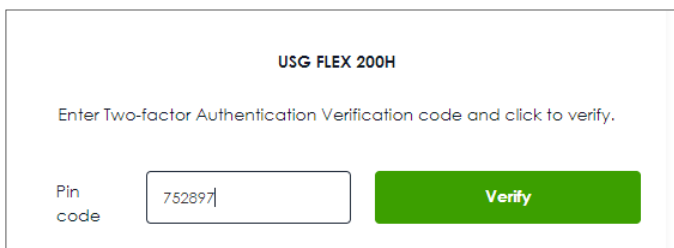
USG FLEX 200H

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

Pin code |

Verify

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

USG FLEX 200H

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

Pin code 752897

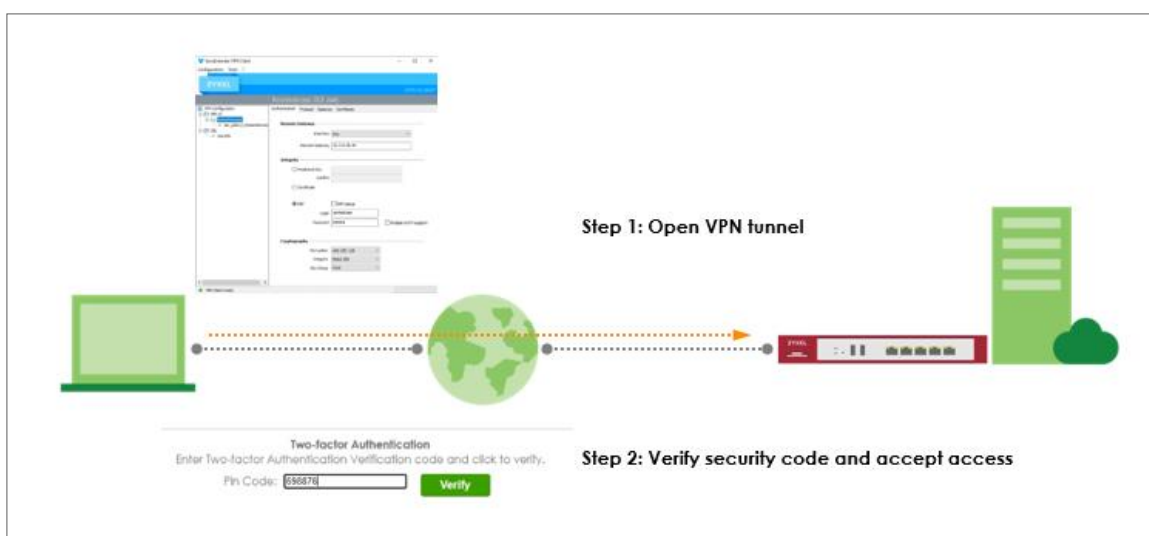
Verify

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

Category User Filter Refresh Clear Log Search insights						
#	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 logged 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.



 **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

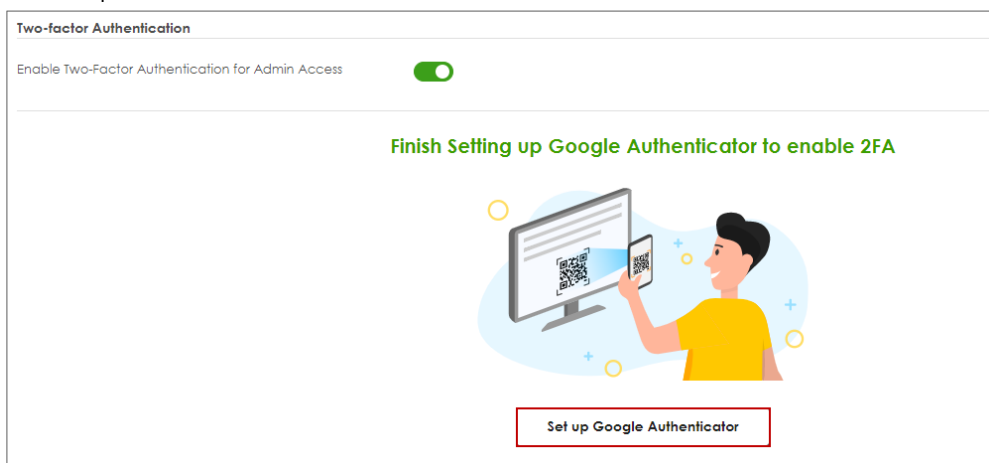
Profile Management

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

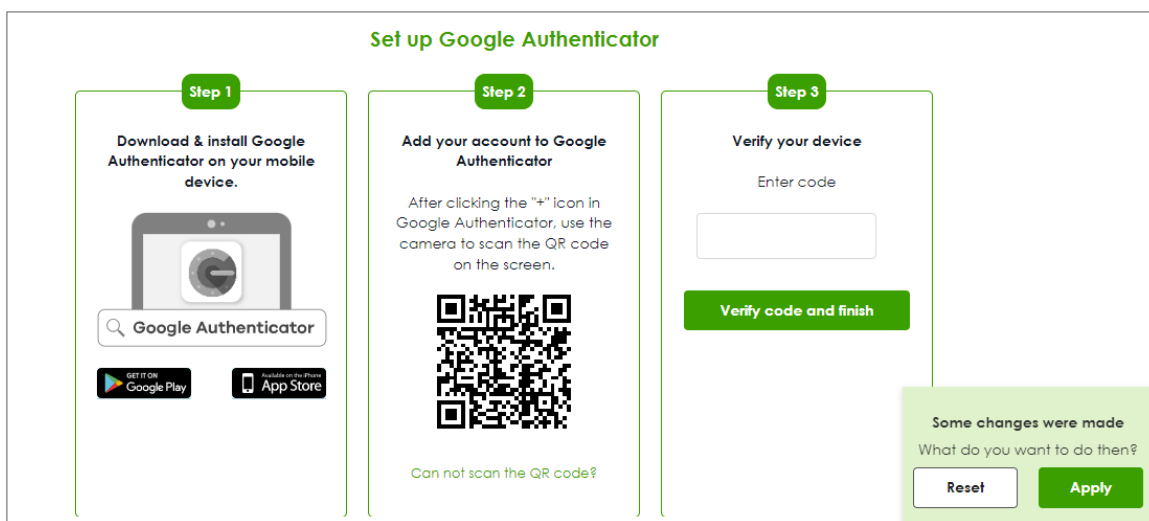
Two-factor Authentication

Enable Two-Factor Authentication for VPN Access ☒

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

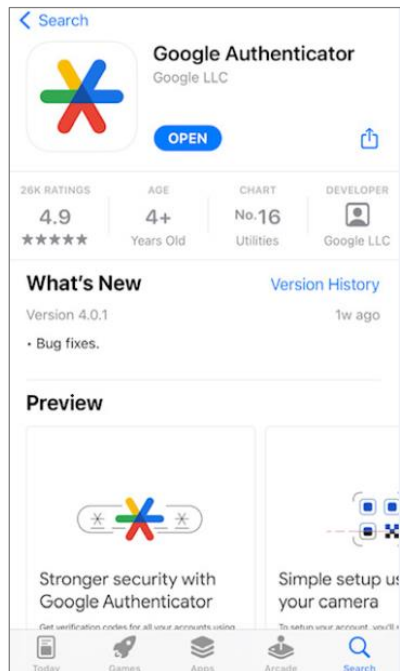


Set up Google Authenticator

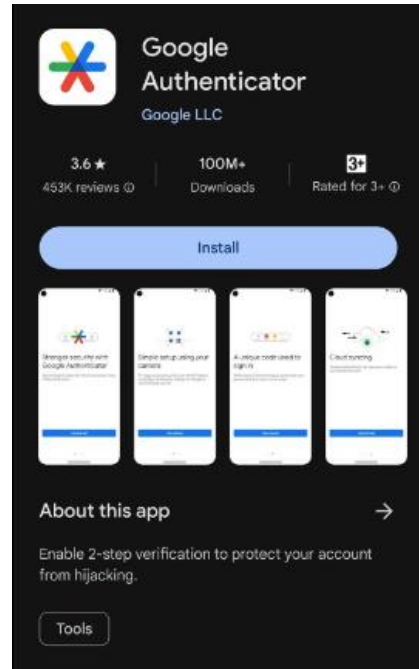


- Download and install Google Authenticator on your mobile device.

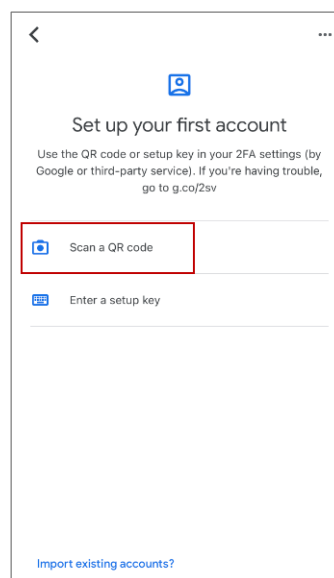
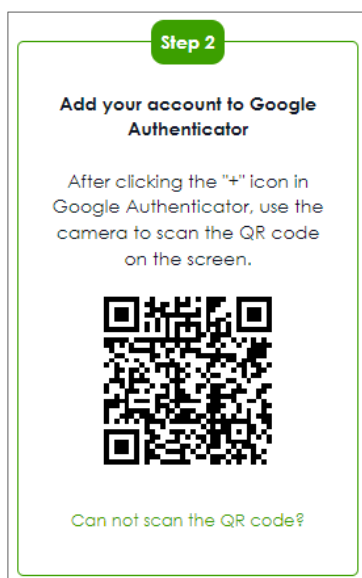
Apple Store



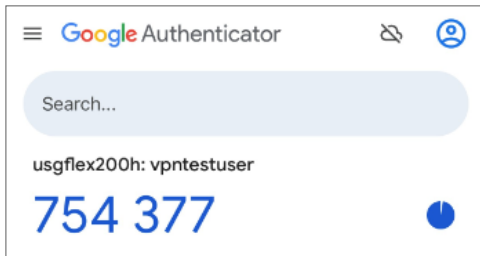
Google Play



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



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.



Step 3

Verify your device

Enter code

754377

Verify code and finish

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.

Download

81819556
70461950
51507415
38976818
39934997

Regenerate backup codes

Configure valid time and login service types

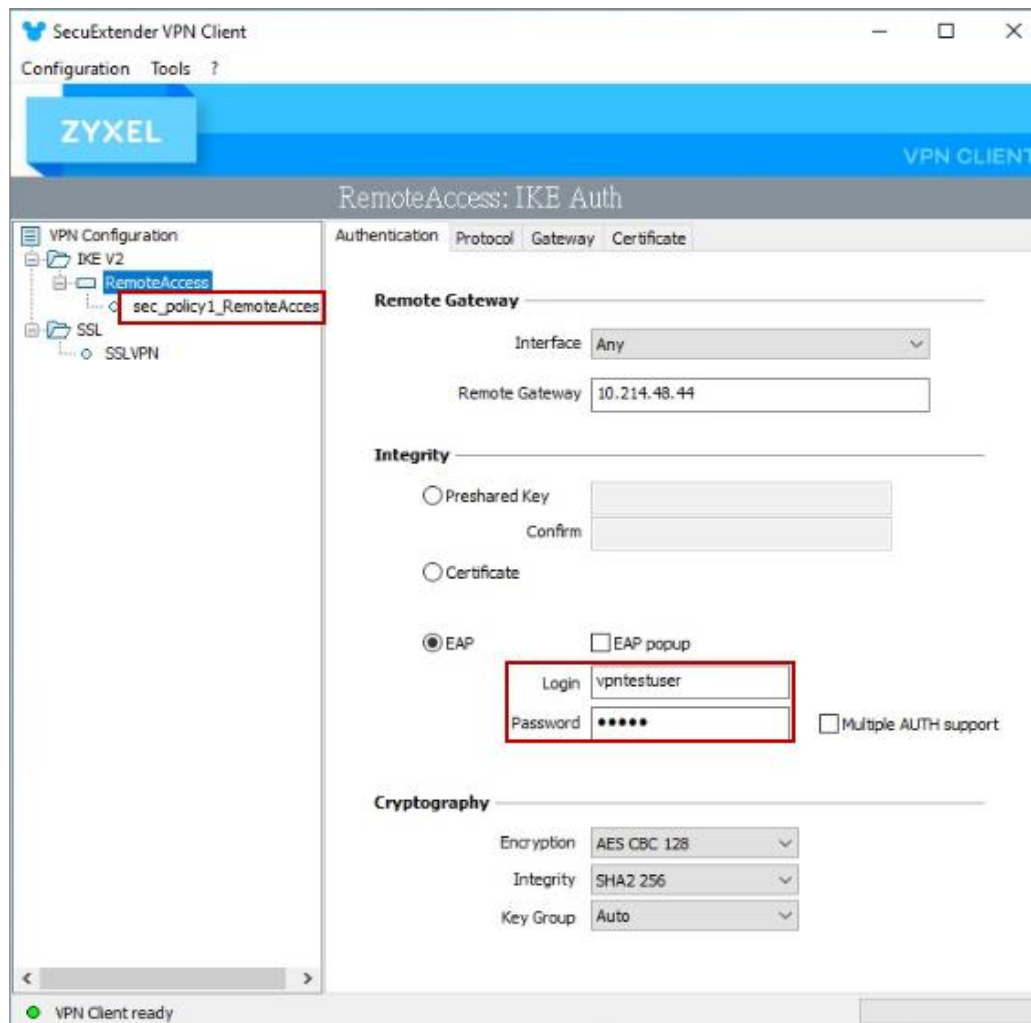
Enable two factor authentication for VPN access. Configure valid time and select which VPN type requires two-factor authentication for VPN user. The valid time is the deadline that user needs to submit the two-factor authentication code to get the VPN access. The request is rejected if submitting the 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.

AAA Server		Two-factor Authentication	
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.



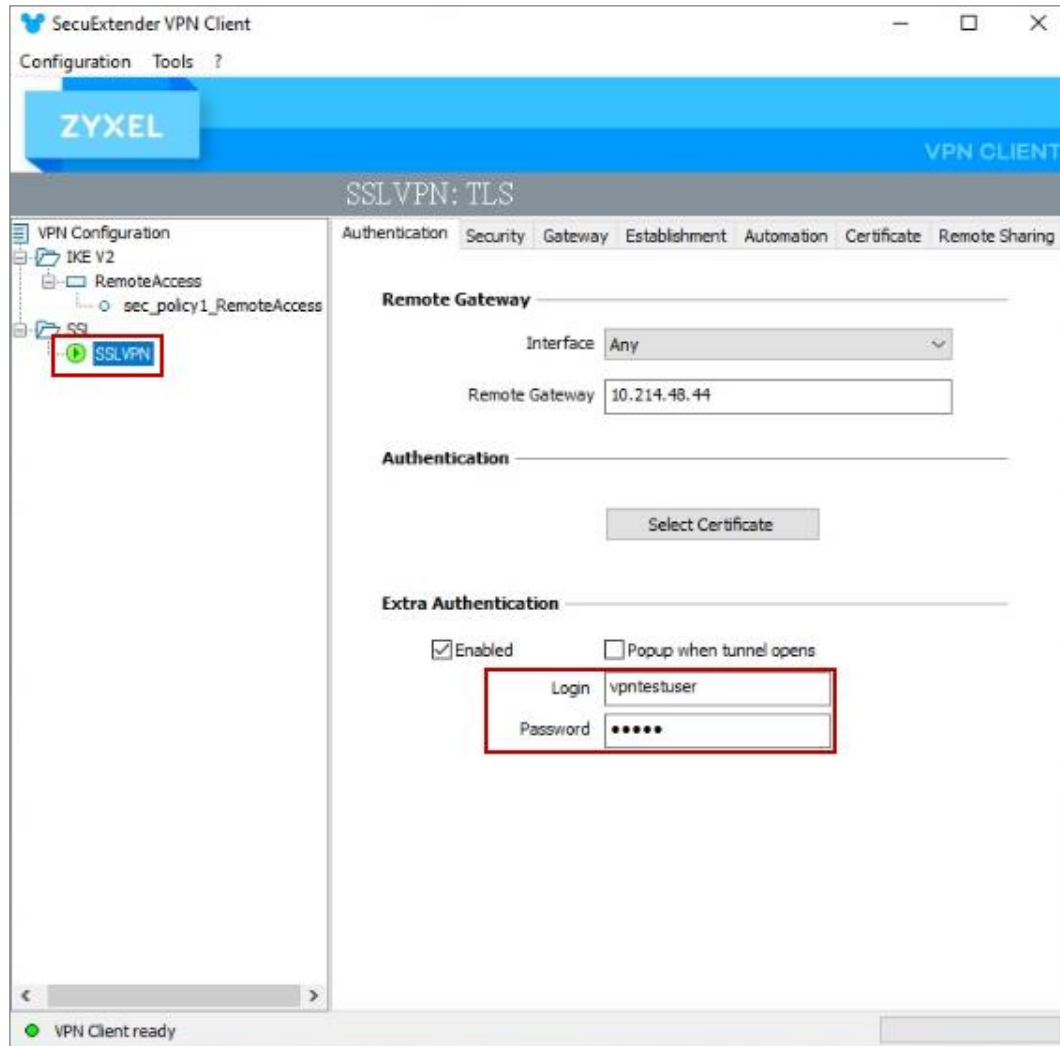
- The browser will pop up authentication page to enter the verification code. Enter the code shown on Google Authenticator and click "Verify". You can also enter the backup code if you don't have mobile device on hand.

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

#	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 h as 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.



- 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.

Two-factor Authentication

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

Pin Code:

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

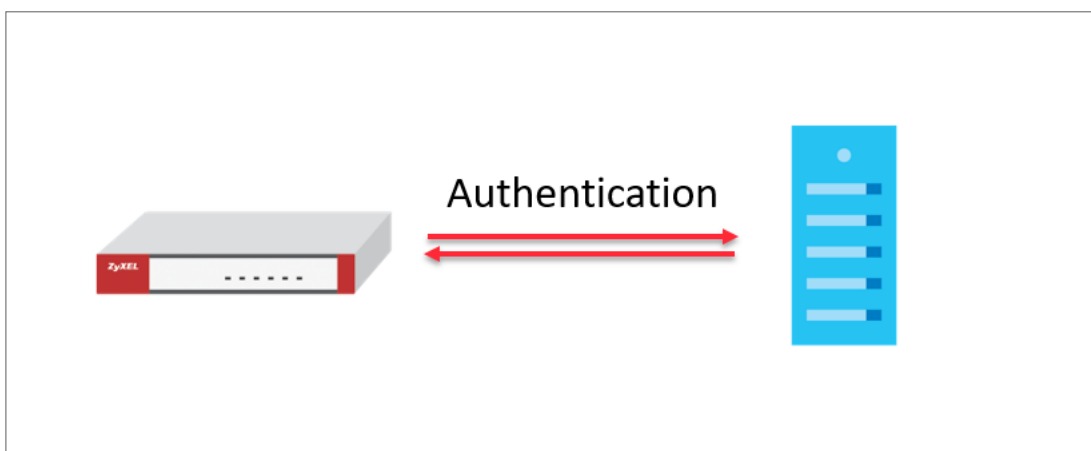
Two-factor Authentication

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

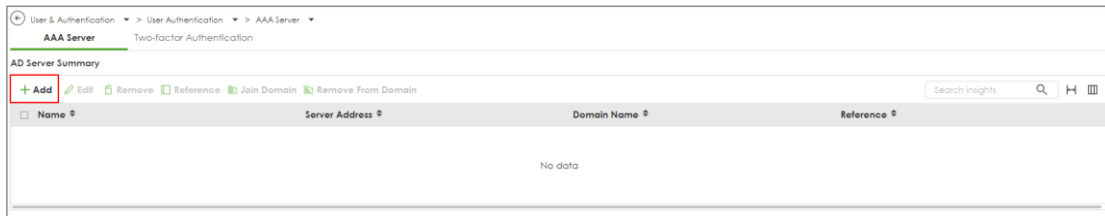
How to set up AD authentication with Microsoft AD

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



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.

The screenshot shows the 'ZYXEL USG FLEX 100H' configuration page. The left sidebar contains a navigation menu with options: Dashboard, Favorites, Traffic Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Security Policy, Object, Security Services, User & Authentication (expanded), System, Log & Report, and Maintenance. The 'User & Authentication' section is expanded, showing 'User/Group' and 'User Authentication'. The main content area shows the 'Configuration' page for the 'AAA Server' profile. The 'Name' field is set to 'Microsoft_AD'. The 'Description' field is empty. The 'Server Settings' section includes: 'Server Address' (10.214.48.XX), 'Backup Server Address' (empty), 'Port' (389), 'Use SSL' (unchecked), 'Search time limit' (5), and 'Case-sensitive User Names' (checked). The 'Server Authentication' section includes: 'Domain Name' (cso.com), 'User Name' (Administrator), 'Password' (masked), and 'Retype to Confirm' (masked). The 'Advanced Settings' section is collapsed. The 'Configuration Validation' section includes a 'Please enter an existing user account in this server to validate the above settings.' message and a 'Test' button.

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 Zone Forwarder		
+ Add Remove		
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**

User & Authentication > User Authentication > AAA Server				
AAA Server Two-factor Authentication				
AD Server Summary				
+ Add Edit Remove Reference Join Domain Remove From 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.

User & Authentication > User Authentication > AAA Server		Join AD Domain	
AAA Server Two-factor Authentication		Associated AD Server Object Microsoft_AD	
AD Server Summary		AD Domain Name cso.com	
+ Add Edit Remove Reference Join Domain Remove From Domain		NetBIOS Domain Name cso	
Name Server Address Domain Name		User Name Administrator	
☒ Microsoft_AD 10.214.48.20 cso.com		Password *****	
LDAP Server Summary		Retype to Confirm *****	

After join domain successfully, you can see this icon.

User & Authentication > User Authentication > AAA Server				
AAA Server Two-factor Authentication				
AD Server Summary				
+ Add Edit Remove Reference Join Domain Remove From Domain				
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.

← User & Authentication > User Authentication > AAA Server

Server Authentication

Domain Name	cs0.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	stanley	Test
-----------	---------	-------------

Test Status

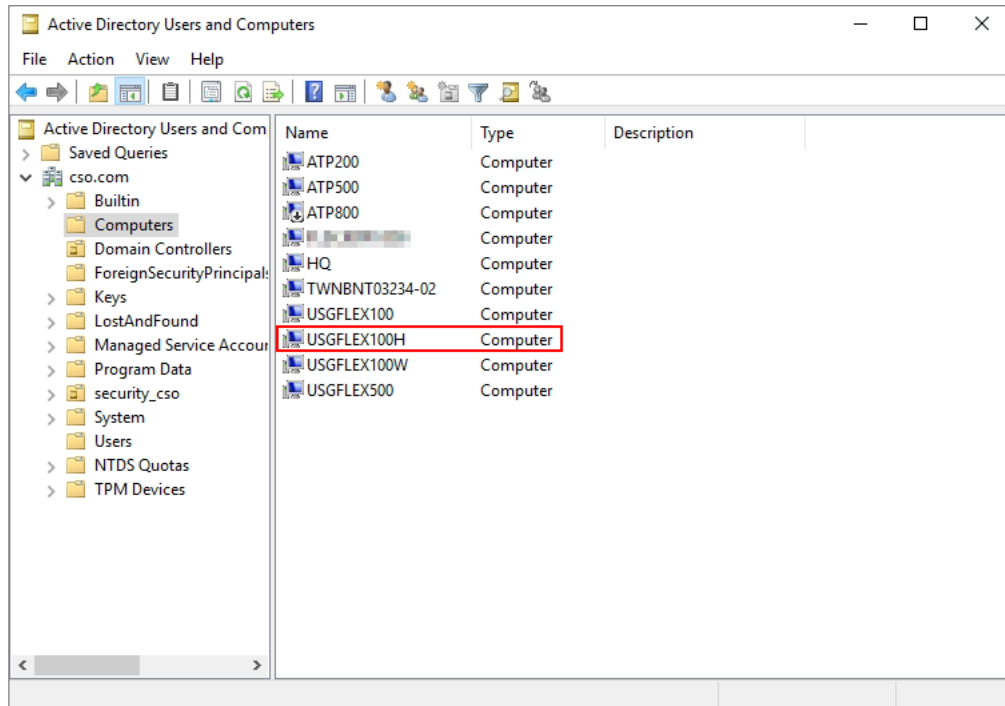
OK

Returned User Attributes

```

dn: CN=stanley,CN=Users,DC=cs0,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: stanley
givenName: Stanley
distinguishedName: CN=stanley,CN=Users,DC=cs0,DC=com
instanceType: 4
whenCreated: 20240305035706.0Z
whenChanged: 20240305052539.0Z
displayName: Stanley
    
```

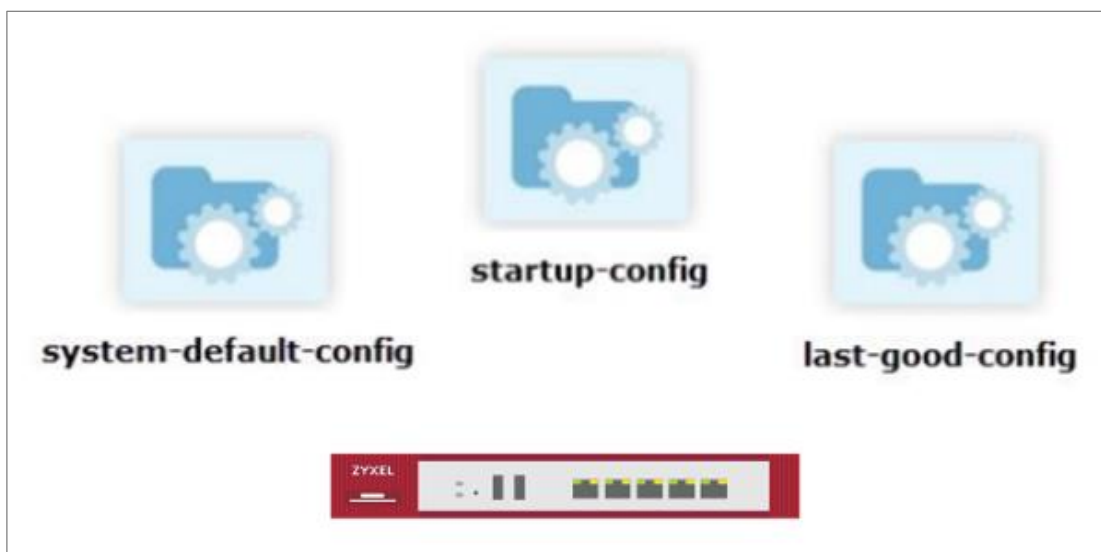
Check **computers** on Microsoft AD, you can see your firewall means join domain successfully.



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.

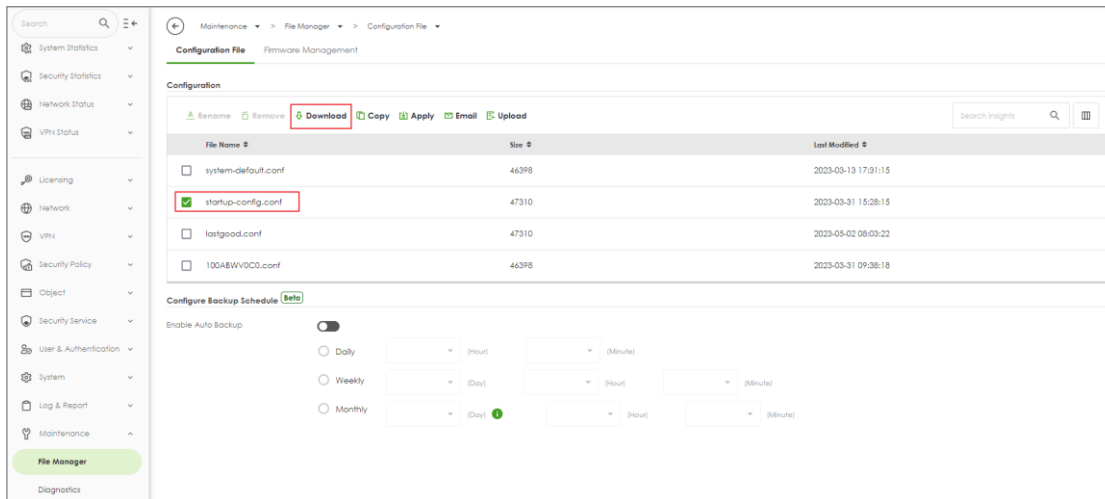
The **startup-config.conf** file is the configuration file that the ZyWALL is currently using. If you make and save changes during your management session, the changes are applied to this configuration file.

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 startup-config.conf and click "Download".



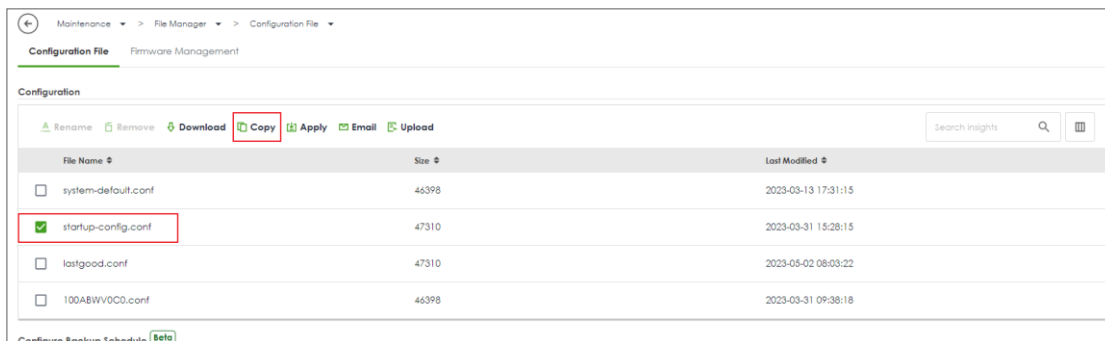
The screenshot shows the ZyXel File Manager interface. The left sidebar contains a navigation menu with options like System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Security Policy, Object, Security Service, User & Authentication, System, Log & Report, Maintenance, File Manager (highlighted), and Diagnostics. The main content area is titled 'Configuration File' and 'Firmware Management'. It features a 'Configuration' section with a table of files. The 'Download' button is highlighted in red. Below the table, there is a 'Configure Backup Schedule' section with a 'Beta' label and options to enable auto backup and set a schedule.

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

Copy the Configuration Files

Maintenance > File Manager > Configuration File

Select the file and click "Copy".

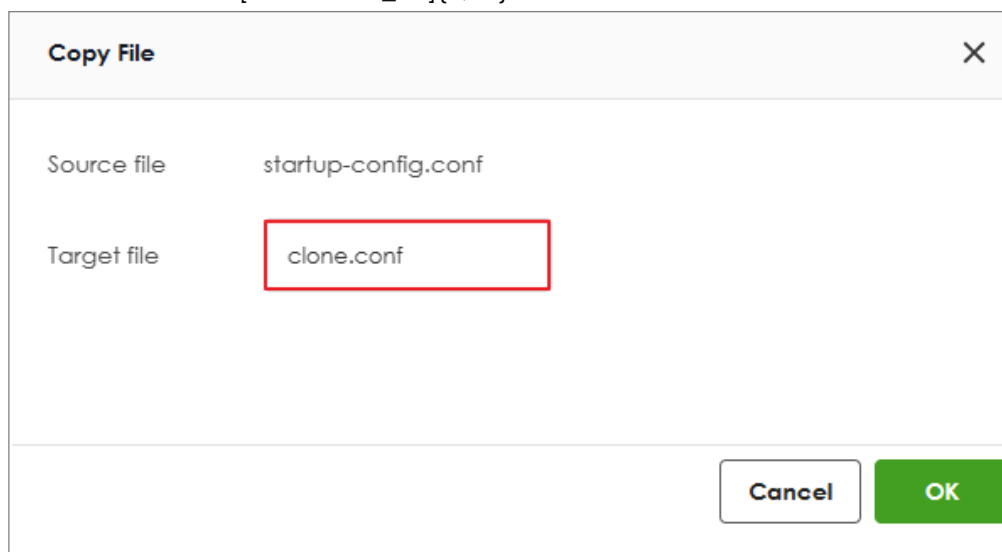


This screenshot is similar to the previous one, showing the same ZyXel File Manager interface. However, in this view, the 'Copy' button is highlighted with a red box instead of the 'Download' button. The 'startup-config.conf' file is also selected with a red box around its checkbox.

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

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

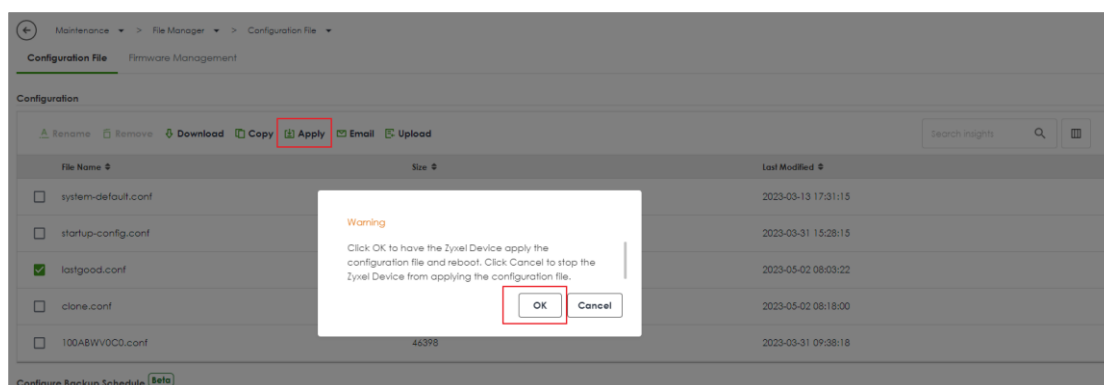


The image shows a 'Copy File' dialog box with a close button (X) in the top right corner. It contains two input fields: 'Source file' with the value 'startup-config.conf' and 'Target file' with the value 'clone.conf'. The 'Target file' field is highlighted with a red rectangular border. At the bottom right, there are two buttons: 'Cancel' and 'OK'.

Apply the Configuration Files

Maintenance > File Manager > Configuration File

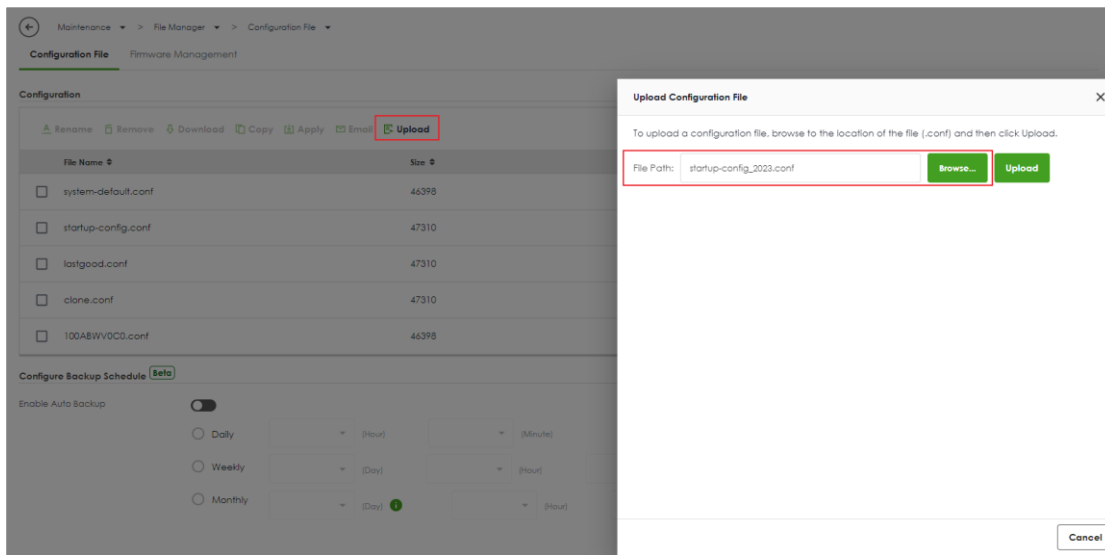
Select a specific configuration file to have ZyWALL use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL settings to the factory defaults. Or select the **lastgood.conf** which is the most recently used (valid) configuration file that was saved when 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.



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.



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.

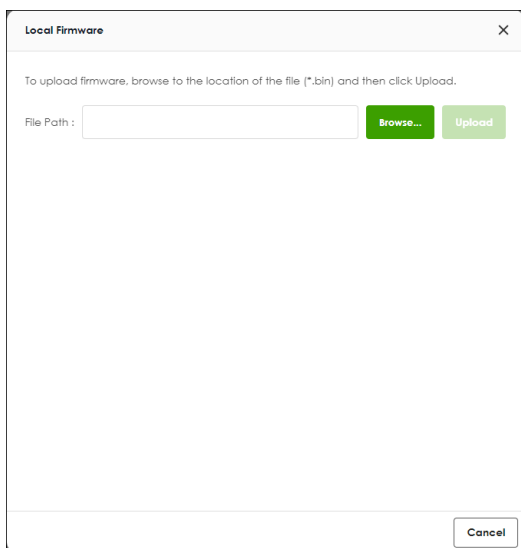
Local Firmware Upgrade

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](https://portal.myzyxel.com/my/firmwares) portal.
(<https://portal.myzyxel.com/my/firmwares>)



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



Local Firmware

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	Check Now
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.

←

System > Notification > Mail Server

Mail Server

Alert

General Settings

Mail Server

smtp.gmail.com

(Outgoing SMTP Server Name or IP Address)

Port

587

(1-65535)

TLS Security

☒

STARTTLS

☒

Authenticate Server

☐

SMTP Authentication

☒

User Name

9@gmail.com

Password

.....

Retype

.....

Mail Server Test

Mail To

(Email Address)

Send From

(Email Address)

Mail Now

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

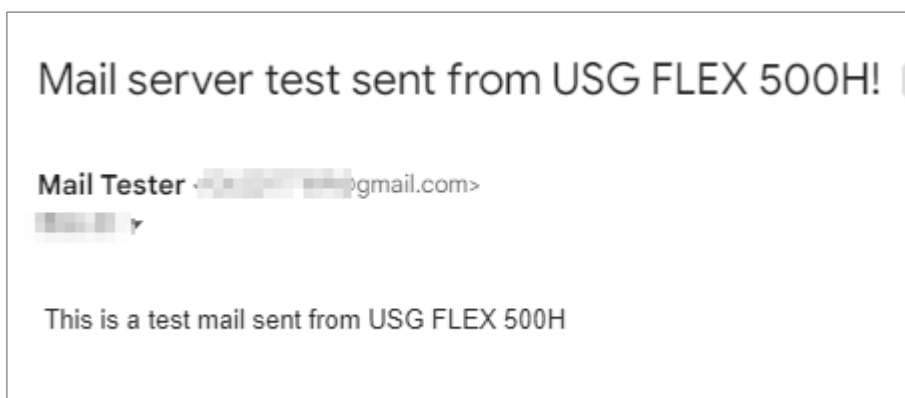
(Email Address)

Send From

(Email Address)

Mail Now

success



Set Up Email Daily Report

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

←

Log & Report ▾

>

Email Daily Report ▾

General Settings

Enable Email Daily Report

☒

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

gmail.com

Email to

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

@gmail.com

Email to

@gmail.com (Email Address)

(Email Address)

(Email Address)

(Email Address)

(Email Address)

Send Report Now

f

@gmail.com

下午3:24

ZYXEL

NETWORKS

General

Model Name:

USG FLEX 500H

Firmware Version:

V1.10(A82H.0)b7s1 | 2023-08-17 15:35:54

MAC Address Range:

08:00:27:00:00:00 - 08:00:27:00:00:00

System Uptime:

10 days, 22:37:53

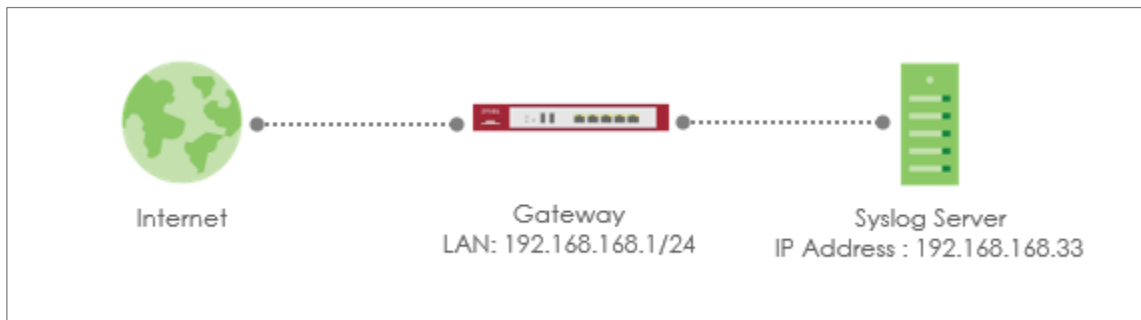
System Name:

usgflex500h

System Resource Usage

How to Setup and Send Logs to a Syslog Server

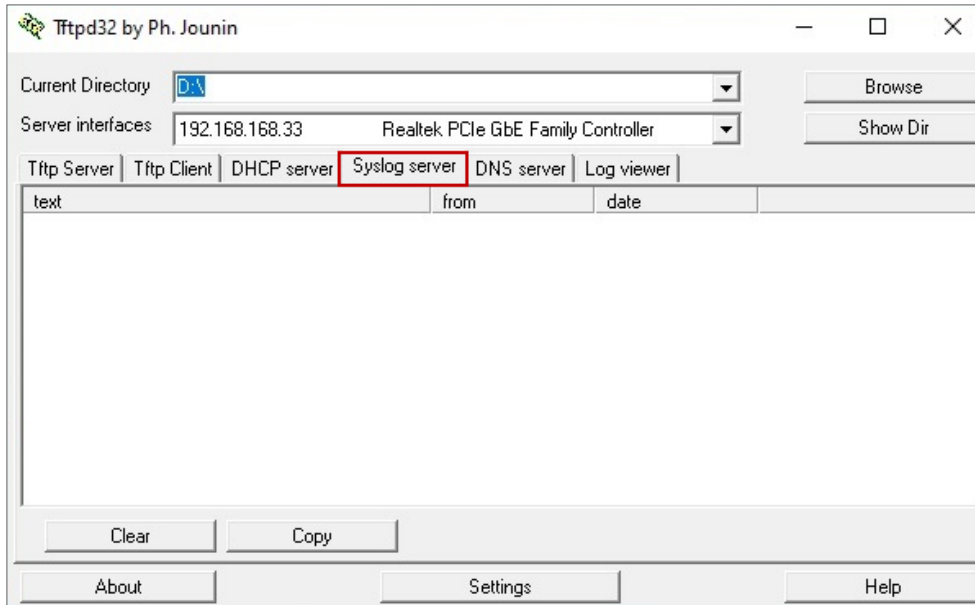
For management purposes, administrators can easily monitor events occurring on the gateway by reading the syslog. This example shows how to send logs to a syslog server. You can also specify which log messages to syslog server. When the syslog server is configured, you will receive the real time system 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.



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

disablenormaldebug

USB Storage

disablenormaldebug

Remote Server 1

disablenormaldebug

Remote Server 2

disablenormaldebug

Count

158

>Authenticate

<

Remote Server 1	Remote Server 2
Active	☒
Log Format	CEF/Syslog
Server Address	192.168.168.33 (Server Name or IP Address)
Server Port	514
Log Facility	Local 1

Check logs on the syslog server.



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	
> Authenticate													3
> Security													2
Security Policy Control													1
DoS Prevention													1
> 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 ☐

Consolidation Interval (10 Seconds - 600 Seconds)

USB Storage

Enable USB storage ☒

Log Keep Duration ☐

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

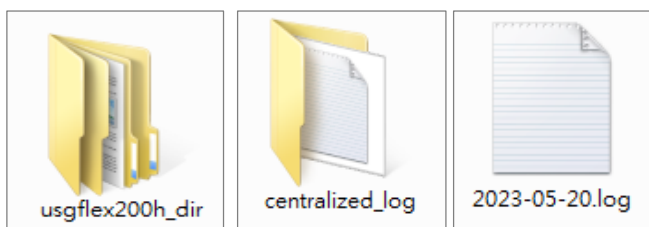
Remove Download

Search insights

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



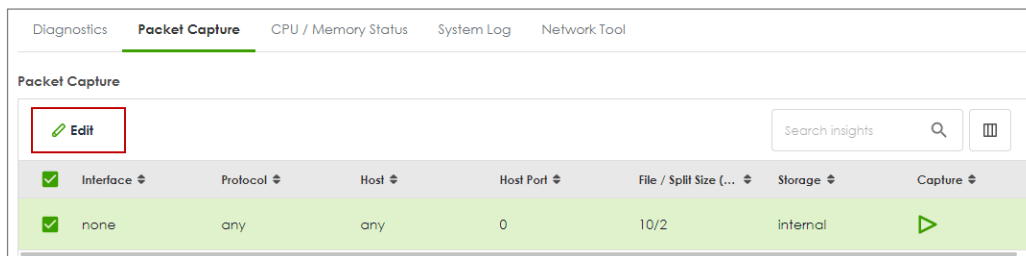
How to Perform and Use the Packet Capture Feature

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.

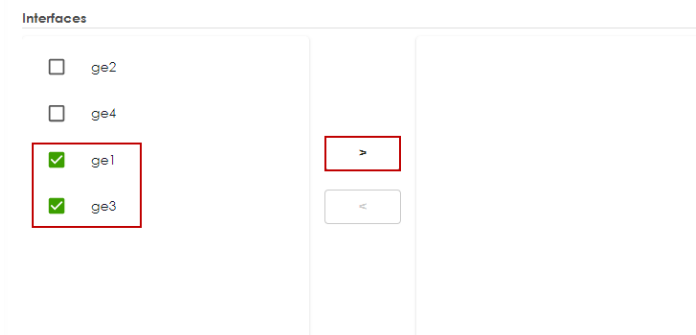
 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

Set Up the Packet Capture Feature

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



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



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.

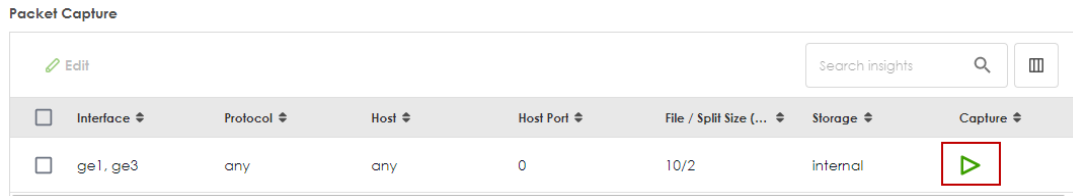
Select a Host IP address object for which to capture packets. Select any to capture packets for all hosts. Select User Defined to be able to enter an IP address.

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

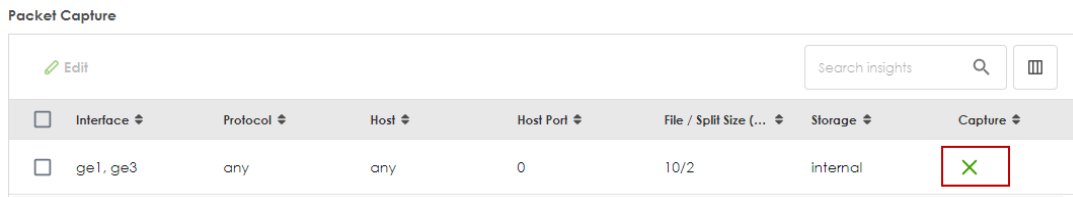
10. In Misc setting, select "Save data to onboard storage only", "Save data to USB storage" or "Save data to ftp server".

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.

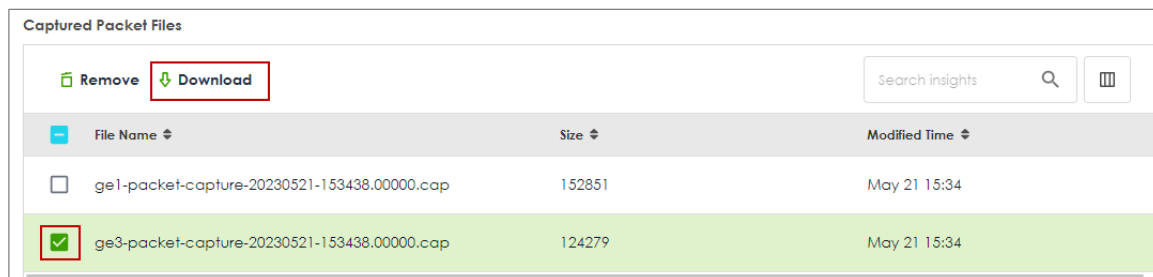


12. Click the icon to stop capturing packets.



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.



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>"

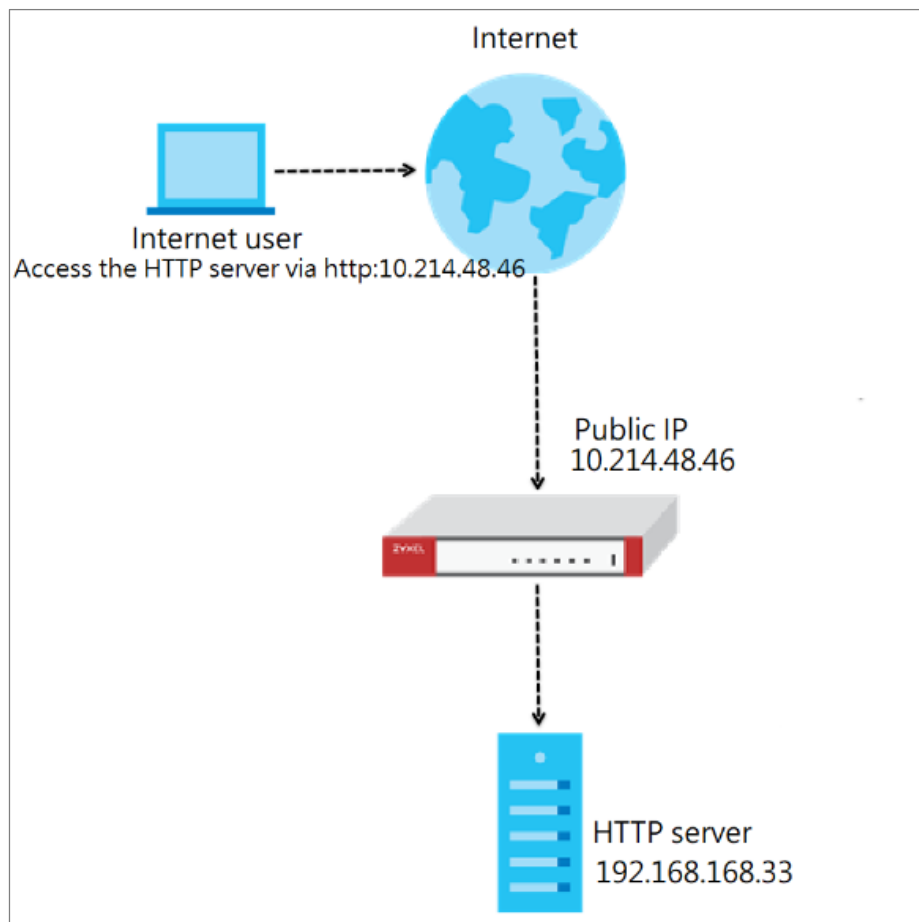
cmd traffic-capture <interface name> filter "port <port number>"

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.local. (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.local. (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.

The screenshot displays the ZyXEL web management interface for configuring NAT. The breadcrumb navigation shows 'Network > NAT'. The 'Port Mapping Type' section has three radio buttons: 'Virtual Server' (selected), '1:1 NAT', and 'Many 1:1 NAT'. Below this, the 'Mapping Rule' section contains several fields: 'Incoming Interface' is set to 'ge1'; 'Source IP' is set to 'any' with a green edit icon; 'External IP' is set to 'any' with a green edit icon; 'Internal IP' is set to 'user defined' with a red box around the green edit icon and a red error message 'this field is required.'; and 'Port Mapping Type' is set to 'any'. At the bottom, the 'Related Settings' section includes 'Enable NAT Loopback' (checked) and 'Configure Security Policy' (checked). A 'Select Address' dialog is open on the right, showing a search bar, a '+ Add Object' button (highlighted with a red box), and a list of objects: 'user defined (default)' (selected), 'IP6to4-Relay', 'executives1', and 'executives2'.

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

←
Network
>
NAT
▼

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 

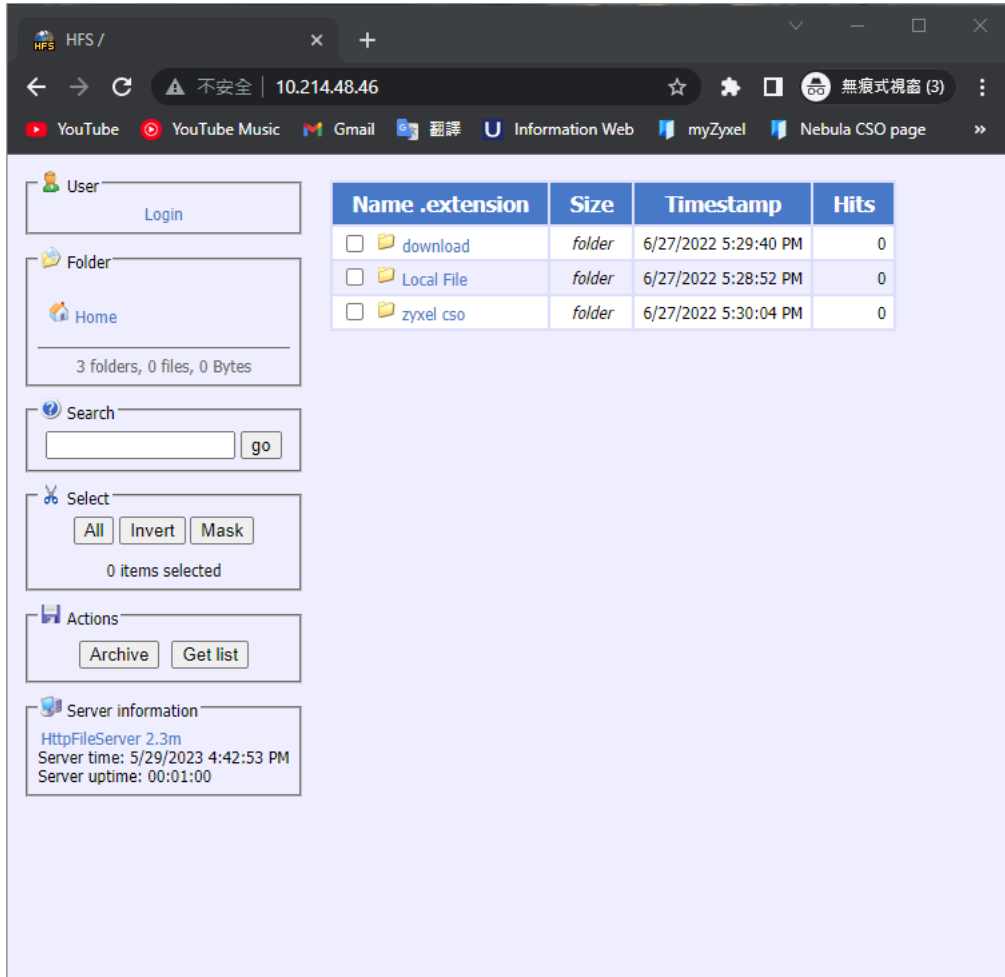
Port Mapping Type Service ▼

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.



The screenshot shows a web browser window with the address bar displaying `10.214.48.46`. The browser's address bar also shows "不安全" (Not Secure) and "無痕式視窗 (3)" (Incognito (3)). The browser's toolbar includes links to YouTube, YouTube Music, Gmail, 翻譯 (Translate), Information Web, myZyxel, and Nebula CSO page.

The main content area of the browser displays the HFS (HTTP File Server) interface. The interface is divided into a sidebar on the left and a main content area on the right.

Sidebar:

- User:** Login
- Folder:** Home (3 folders, 0 files, 0 Bytes)
- Search:** Search input field and go button
- Select:** Select input field, All, Invert, Mask buttons, 0 items selected
- Actions:** Archive, Get list buttons
- Server information:** HttpFileServer 2.3m, Server time: 5/29/2023 4:42:53 PM, Server uptime: 00:01:00

Main Content Area:

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.

The screenshot shows the configuration page for the WAN interface (ge1). The 'General Settings' section includes 'Enable Interface' (checked). The 'Interface Properties' section includes 'Role' (external), 'Interface Type' (Ethernet), 'Interface Name' (ge1), 'Port' (p1 (ge1)), 'Zone' (WAN), 'MAC Address' (randomly generated), and 'Description' (empty). The 'Address Assignment' section at the bottom shows three radio button options: 'Unassigned', 'Get Automatically (DHCP)' (selected and highlighted in yellow), and 'Use Fixed IP Address'. There is also a 'PPPoE' option at the very bottom.

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

MTU

Default SNAT
☒

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.

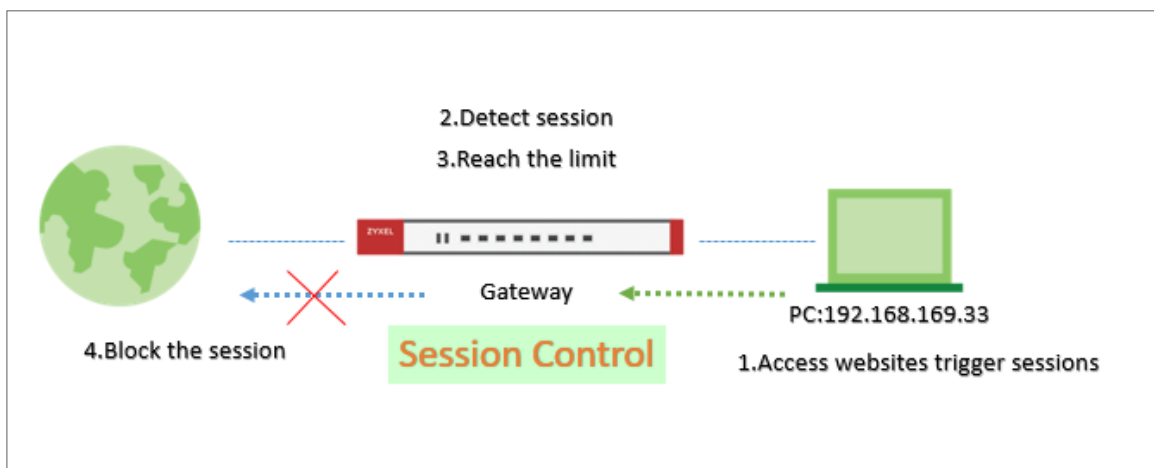
```

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-...}, id 0
> Ethernet II, Src: ZyxelCom_e7:e8:36 (08:00:27:08:00:36), 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
< 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 (08:00:27:08:00:36)
  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
  > Option: (60) Vendor class identifier
    Length: 7
    Vendor class identifier: CSO-FAQ
  > Option: (61) Client identifier
  > Option: (255) End
  Padding: 0000000000

```

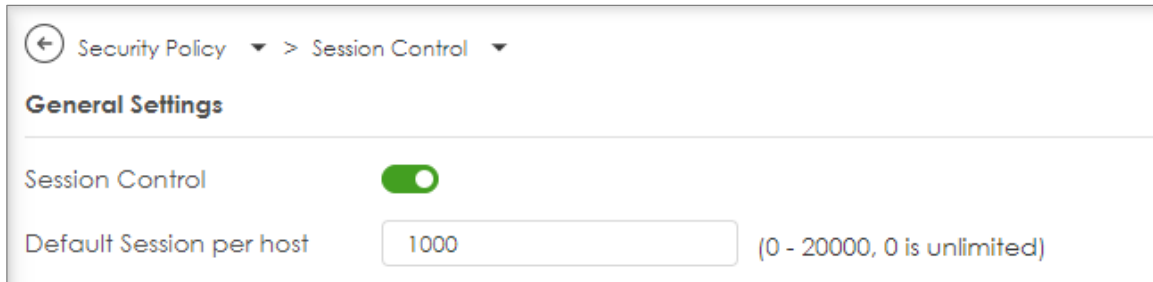
How to Configure Session Control

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 ☒

Default Session per host (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

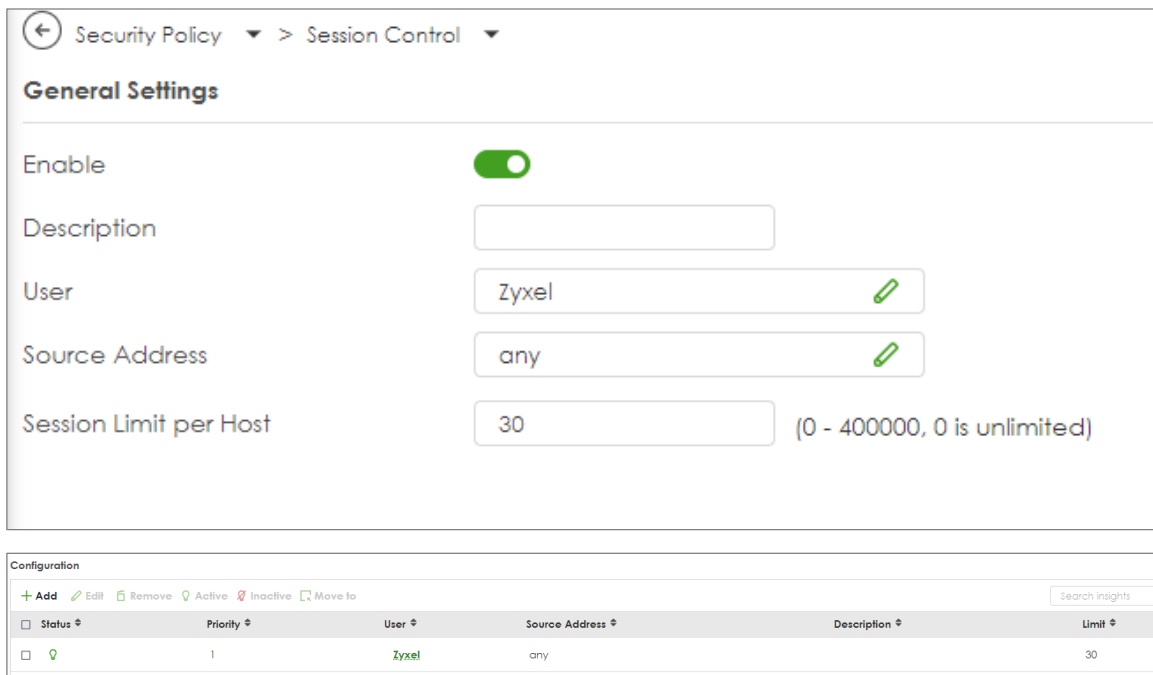
Configuration

+ Add Edit Remove Active Inactive Move to Search Insights

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 ☒

Description

User Edit

Source Address Edit

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

Configuration

+ Add Edit Remove Active Inactive Move to Search Insights

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): 

☐ Updating lease time automatically

Remaining time before lease timeout (hh:mm:ss):

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

Logout

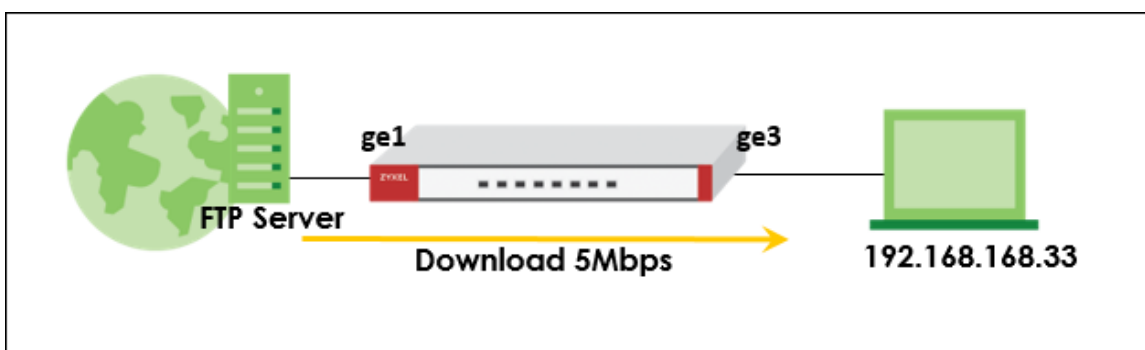
Try to access web browser to hit the session limit

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.

Network > BWM

General Settings

Enable ☒

Configuration

+ Add Edit Remove Active Inactive Move to

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.

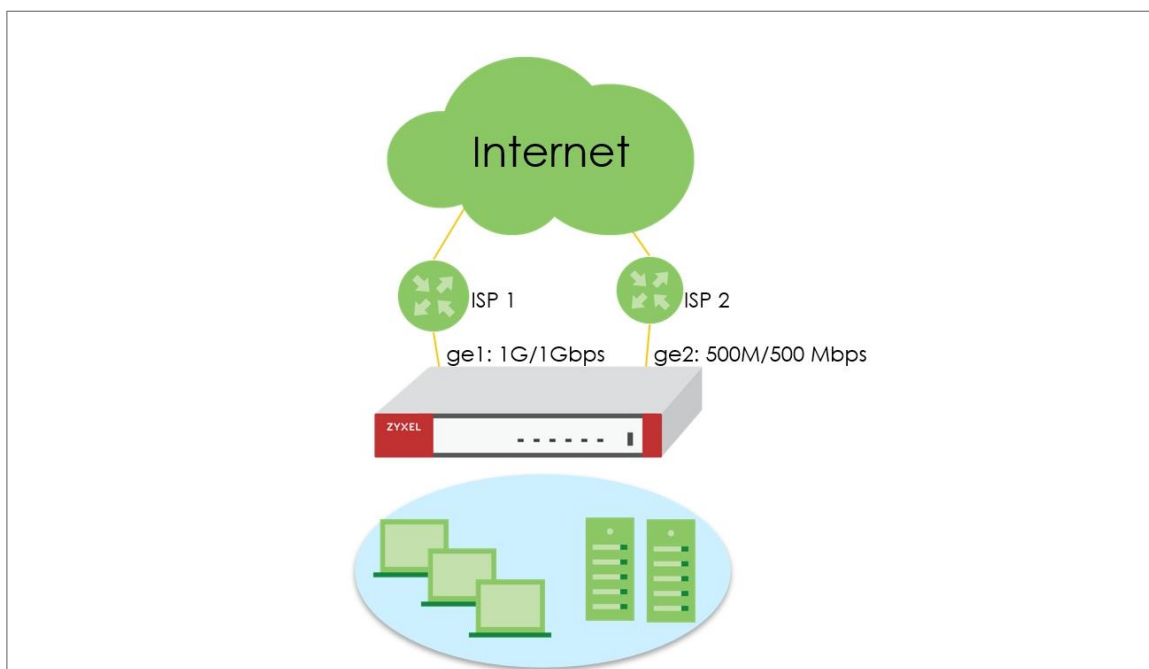
Log & Report > Log / Events

Category: BWM Refresh Clear Log Export

#	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

+ Add Remove

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

+ Add Remove

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?

Cancel Apply

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

Network > Interface > Trunk

General Settings

Name:

Load Balancing Setting

Algorithm:

Load Balancing Index(es):

+ Add Remove

Interface	Mode	Limit (Kbps)
No data		

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

+ Add Remove

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?

Cancel Apply

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

+ Add Edit Remove Reference Search insights

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

Default Trunk

Edit Search

Some changes were made

What do you want to do then?

Cancel **Apply**

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.