

# Handbook

## **USG FLEX H Series**

USG FLEX 50H / USG FLEX 50HP

USG FLEX 100H / USG 100HP / USG FLEX 200H /

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

Firmware Version: uOS1.32

Jun. 2025

**Table of Content**

**Chapter 1- VPN** .....5

How to Configure Site-to-site IPSec VPN Where the Peer has a Static IP Address.....5

How to Configure Site-to-site IPSec VPN Where the Peer has a Dynamic IP Address..... 17

How to Configure IPSec Site to Site VPN while one Site is behind a NAT router ..... 23

How to Configure Remote Access VPN with Zyxel VPN Client ..... 35

How to Configure Site-to-site IPSec VPN between ZLD and uOS device..... 56

How to Configure Route-Based VPN..... 67

How to Use Tailscale..... 79

**Chapter 2- Security Service** ..... 90

How to Block HTTPS Websites Using Content Filtering and SSL Inspection ..... 90

How to Configure Content Filter with HTTPs Domain Filter ..... 99

How to Block Facebook Using a Content Filter Block List ..... 104

How to block YouTube access by Schedule ..... 108

How to Control Access to Google Drive ..... 117

How to Block the Spotify Music Streaming Service ..... 125

How does Anti-Malware Work..... 128

How to Detect and Prevent TCP Port Scanning with DoS Prevention ..... 131

How to block the client from accessing to certain country using Geo IP? ..... 135

How to Use Sandbox to Detect Unknown Malware? ..... 140

How to Configure Reputation Filter- IP Reputation ..... 143

How to Configure Reputation Filter- URL Threat Filter ..... 148

How to Configure Reputation Filter- DNS Threat Filter ..... 152

How to Configure DNS Content Filter ..... 156

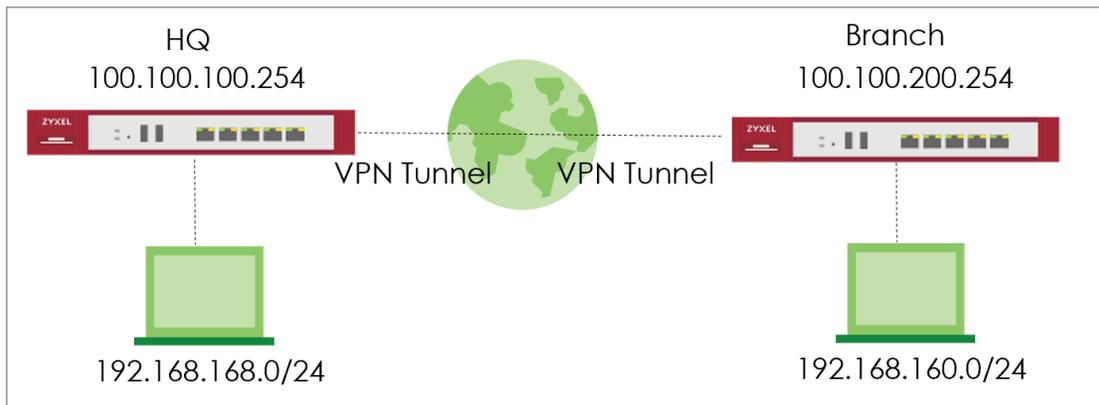
External Block List for Reputation Filter .....	161
<b>Chapter 3- Authentication</b> .....	166
How to Use Two Factor with Google Authenticator for Admin Access.....	166
How to Use Two Factor with Google Authenticator for Remote Access	
VPN and SSL VPN .....	173
How to set up AD authentication with Microsoft AD .....	183
How to Set Up Captive Portal?.....	188
<b>Chapter 4- Maintenance</b> .....	196
How to Manage Configuration Files.....	196
How to Manage Firmware .....	200
<b>Chapter 5- Others</b> .....	202
How to Setup and Configure Daily Report.....	202
How to Setup and Send Logs to a Syslog Server .....	207
How to Setup and Send logs to the USB storage .....	210
How to Perform and Use the Packet Capture Feature .....	212
How to Allow Public Access to a Server Behind USG FLEX H .....	216
How to Configure DHCP Option 60 – Vendor Class Identifier .....	220
How to Configure Session Control .....	222
How to Configure Bandwidth Management for FTP Traffic .....	225
How to Configure WAN trunk for Spillover and Least Load First.....	230
How Does SIP ALG Function Work on USG FLEX H? .....	236
How to Deploy Device HA .....	240
How to check Packet Flow Explorer.....	252
How to set up a Link Aggregation Group (LAG) interface.....	258
How to Set Up AP Control Service for Zyxel APs .....	264
<b>Chapter 6- Nebula</b> .....	269
How to Set Up Nebula site-to-site VPN on the USG FLEX H? .....	269

How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Hub site)? ..... 273  
How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Spoke site)? ..... 277

## 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 navigation menu with options like Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Site to Site VPN (highlighted), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main area displays the configuration steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active, showing a form with the following fields: \*Name (HQtoBranch), IKE Version (IKEv1, IKEv2), Type (Site-to-Site, Custom), and Behind NAT (None, Local Site, Remote Site). A diagram below the form illustrates a Local Site connected to an Internet cloud, which is then connected to a Remote Site. At the bottom, there 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.

The screenshot shows the 'Policy & Routing' configuration page for a Site to Site VPN. The breadcrumb trail is 'VPN > Site to Site VPN > Scenario > Network > Authentication > Policy & Routing'. The progress indicator shows five steps: Scenario, Network, Authentication, Policy & Routing (current), and Summary. The 'Type' is set to 'Policy-Based'. The 'Local Subnet' is '192.168.168.0/24' and the 'Remote Subnet' is '192.168.160.0/24'. A network diagram below shows a 'Local Site' (100.100.100.254) and a 'Remote Site' (100.100.200.254) connected via an 'Internet' cloud. The local site is associated with the subnet 192.168.168.0/24 and the remote site with 192.168.160.0/24. At the bottom, there are 'Cancel', 'Back', and 'Finish' buttons.

**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**.

The screenshot displays the ZyXEL VPN configuration interface. On the left is a navigation menu with options like Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Site to Site VPN (highlighted), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main area shows the configuration steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active, with the following settings: \*Name: BranchtoHQ, IKE Version: IKEv2, Type: Site-to-Site, Behind NAT: None, Local Site, and Remote Site. A diagram at the bottom shows a Local Site connected to an Internet cloud, which is 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

Peer Gateway Address Domain Name / IP



Local Site  
100.100.200.254

Internet

Remote Site  
100.100.100.254

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

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

The screenshot shows the ZyXel VPN configuration interface for Site to Site VPN. The breadcrumb path is VPN > Site to Site VPN. The configuration progress is shown as a series of steps: Scenario (checked), Network (checked), 3 Authentication (active), 4 Policy & Routing, and 5 Summary. Under the Authentication section, the Pre-Shared Key option is selected with a radio button. A text input field containing seven dots is highlighted with a red border. Below it is a dropdown menu set to 'default'. The Certificate option is unselected. At the bottom of the interface, there are three buttons: 'Cancel', 'Back', and '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 shows the 'Policy & Routing' configuration page for a Site to Site VPN. At the top, a progress bar indicates the current step is 4 out of 5: Scenario, Network, Authentication, Policy & Routing, and Summary. Below the progress bar, the 'Type' is set to 'Policy-Based' (indicated by a selected radio button). The 'Local Subnet' is configured as '192.168.160.0/24' and the 'Remote Subnet' is '192.168.168.0/24', both fields are highlighted with red boxes. A network diagram below shows a 'Local Site' (100.100.200.254) connected to an 'Internet' cloud, which is then connected to a 'Remote Site' (100.100.100.254). The local site is associated with the subnet 192.168.160.0/24, and the remote site is associated with 192.168.168.0/24. At the bottom of the page, there are 'Cancel', 'Back', and 'Finish' buttons.

**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	<input type="password" value="*****"/>
----------------	----------------	--

**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.

The screenshot shows the 'Site to Site VPN' status page. At the top, there are navigation tabs for 'VPN Status', 'IPsec VPN', and 'Site to Site VPN'. Below the tabs, there are 'Disconnect' and 'Refresh' buttons, and a search bar. A table lists the VPN tunnels with columns for Name, Policy Route, My Address, Remote Gateway, Uptime, Rekey, Inbound (bytes), and Outbound (bytes). One tunnel is listed with ID 1, Name HQtoBranch, Policy Route 192.168.168.0/24 <-> 192.168.160.0/24, My Address 100.100.100.254, Remote Gateway 100.100.200.254, Uptime 5, Rekey 86171, Inbound 0 (0 bytes), and Outbound 0 (0 bytes). At the bottom right, it shows 'Rows per page: 50' and '1 of 1'.

	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)

### Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1

The screenshot is split into two parts. On the left, the 'Network Connection Details' window shows the following information:

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	

On the right, the 'Administrator: Command Prompt' window shows the following output:

```

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

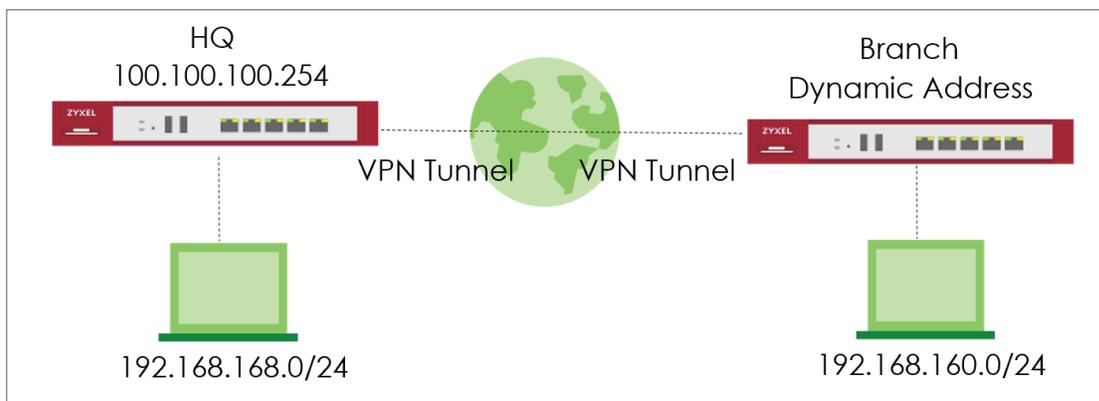
Ping statistics for 192.168.160.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 7ms, Average = 2ms

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**.

The screenshot shows the ZyXel VPN configuration interface. On the left is a navigation menu with 'Site to Site VPN' selected. The main area shows a progress bar with five steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active. The configuration fields are:
 

- \*Name: HQtoBranch
- IKE Version:  IKEv1,  IKEv2
- Type:  Site-to-Site,  Custom

 At the bottom, there are 'Cancel' and 'Next' buttons.

### VPN > Site to Site VPN

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

The screenshot shows the ZyXel VPN configuration interface for the 'Network' and 'Authentication' steps. The configuration fields are:
 

- General Settings:**
  - Enable:
  - Name: HQtoBranch
  - IKE Version:  IKEv1,  IKEv2
  - Type:  Route-Based,  Policy-Based
- Network:**
  - My Address: Domain Name / IP: 100.100.100.254
  - Peer Gateway Address:  Domain Name / IP,  Dynamic Address
- Authentication:**
  - Authentication:  Pre-Shared Key,  Certificate
  - Pre-Shared Key: [Redacted]
  - Certificate: default

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

**Phase 2 Settings**

Initiation  Auto  Nalled-up  Responder Only

Policy

[+ Add](#) [Edit](#) [Remove](#)

<input type="checkbox"/> Local	Remote	Protocol	Active Protocol	Encapsulation		
192.168.168.0/24	192.168.160.0/24	Any	ESP	Tunnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Rows per page: 50 1 of 1 < 1 >

SA Life Time  (180 - 3000000 Seconds)

Proposal

[+ Add](#) [Edit](#) [Remove](#)

<input type="checkbox"/> Encryption	Authentication
<input type="checkbox"/> aes128-cbc	hmac-sha1

Rows per page: 50 1 of 1 < 1 >

Diffie-Hellman Groups

## 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**.

The screenshot shows the 'Scenario' configuration step for a Site-to-Site VPN. The breadcrumb path is 'VPN > Site to Site VPN'. A progress bar at the top indicates five steps: 1. Scenario (active), 2. Network, 3. Authentication, 4. Policy & Routing, and 5. Summary. The configuration fields are as follows:

- Name:** BranchHQ
- IKE Version:** IKEv2 (selected)
- Type:** Custom (selected)

Buttons for 'Cancel' and 'Next' are visible at the bottom of the configuration area.

### VPN > Site to Site VPN

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

The screenshot shows the 'Network' configuration step for a Site-to-Site VPN. The breadcrumb path is 'VPN > Site to Site VPN'. The configuration fields are as follows:

- General Settings:**
  - Enable:** Disabled
  - Name:** BranchHQ
  - IKE Version:** IKEv2 (selected)
  - Type:** Policy-Based (selected)
- Network:**
  - My Address:** Domain Name / IP: 0.0.0.0
  - Peer Gateway Address:** Domain Name / IP: 100.100.100.254
- Authentication:**
  - Authentication:** Pre-Shared Key (selected)

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

**Phase 2 Settings**

Initiation:  Auto  Nailed-up  Responder Only

Policy

Local	Remote	Protocol	Active Protocol	Encapsulation		
192.168.160.0/24	192.168.168.0/24	Any	ESP	Tunnel	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Rows per page: 50 1 of 1 < 1 >

SA Life Time: 28800 (180 - 3000000 Seconds)

Proposal

Encryption	Authentication
<input type="checkbox"/> 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.

The screenshot shows the 'Site to Site VPN' status page. At the top, there are navigation links for 'VPN Status', 'IPsec VPN', and 'Site to Site VPN'. Below the navigation, there are 'Disconnect' and 'Refresh' buttons, and a search bar. The main content is a table with the following columns: #, Name, Policy Route, My Address, Remote Gateway, Uptime, Rekey, Inbound (Bytes), and Outbound (Bytes). There is one row in the table:

#	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)

At the bottom right of the table, it says 'Rows per page: 50' and '1 of 1'.

### Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1

The screenshot is split into two parts. On the left is the 'Network Connection Details' window, and on the right is the 'Administrator: Command Prompt' window.

**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

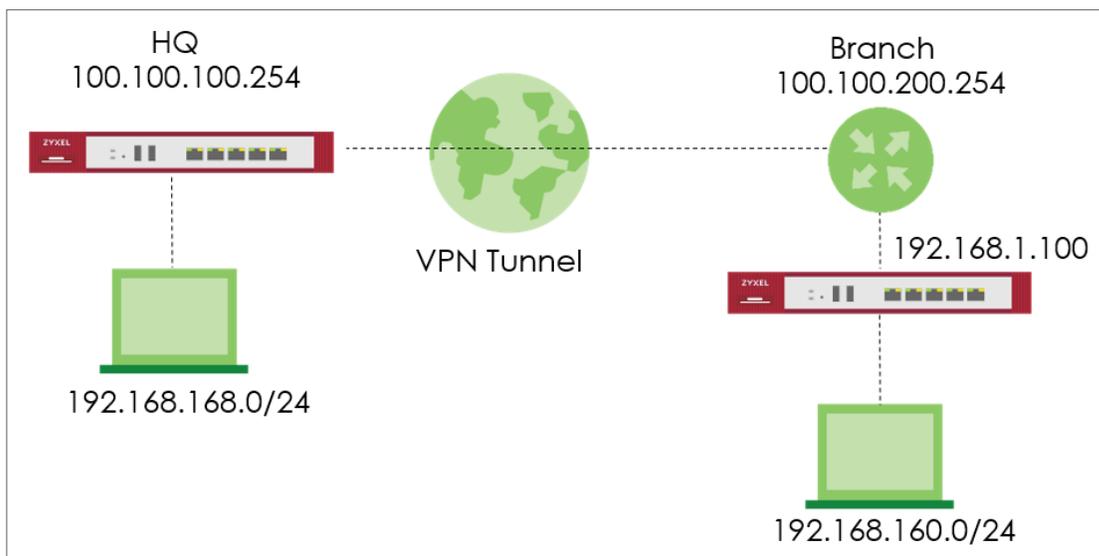
Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time<1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=7ms TTL=63

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**.

The screenshot displays the ZyXel VPN configuration wizard, Step 1: Scenario. The interface includes a search bar, a navigation menu on the left, and a progress indicator at the top showing five steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The main configuration area contains the following fields and options:

- Name: HQtoBranch
- IKE Version:  IKEv1,  IKEv2
- Config Type:  Wizard,  Custom
- Behind NAT:  None,  Local Site,  Remote Site

At the bottom of the form, there is a diagram illustrating the network topology: a Local Site is connected to an Internet cloud, which is connected to a Router, which is connected to a Remote Site. The 'Next' button is highlighted in green, and a 'Cancel' button is visible at the bottom left.

**VPN > Site to Site VPN > Scenario > Network**

Configure My Address. Click **Next**.

The screenshot displays the ZyXel VPN configuration interface for Site to Site VPN. At the top, a breadcrumb trail shows 'VPN > Site to Site VPN'. Below this, a progress indicator shows five steps: 1. Scenario (checked), 2. Network (active), 3. Authentication, 4. Policy & Routing, and 5. Summary.

The configuration fields are as follows:

- My Address:** A dropdown menu showing '100.100.100.254', which is highlighted with a red box.
- Domain Name / IP:** A text field containing '100.100.100.254', also highlighted with a red box.
- Peer Gateway Address:** A dropdown menu showing 'Dynamic Address'.
- Dynamic Address:** A text field containing 'Dynamic Address'.

Below the configuration fields is a network diagram illustrating the setup:

- A **Local Site** (represented by a server icon) with the IP address '100.100.100.254' is connected to the **Internet** (represented by a cloud icon).
- The **Internet** is connected to a **Router** (represented by a router icon).
- The **Router** is connected to a **Remote Site** (represented by a server icon) with the IP address 'Dynamic Address'.

At the bottom of the interface, there are three buttons: 'Cancel', 'Back', and 'Next'.

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

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

The screenshot shows the ZyXel configuration interface for Site to Site VPN Authentication. At the top, a breadcrumb trail reads 'VPN > Site to Site VPN'. Below this is a progress indicator with five steps: 'Scenario' (checked), 'Network' (checked), '3 Authentication' (active), '4 Policy & Routing', and '5 Summary'. The 'Authentication' section has two radio button options: 'Pre-Shared Key' (selected) and 'Certificate' (with a 'Beta' label). The 'Pre-Shared Key' field contains a masked key '.....' and a red box highlights this field along with a toggle icon. Below the key field is a dropdown menu set to 'default'. At the bottom of the interface are three buttons: 'Cancel', 'Back', and '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 shows the 'Policy & Routing' configuration page for a Site to Site VPN. The breadcrumb trail is 'VPN > Site to Site VPN'. The progress indicator 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, 'Policy-Based' is selected with a radio button, while 'Route-Based' is unselected. The 'Local Subnet' field contains '192.168.168.0/24' and the 'Remote Subnet' field contains '192.168.160.0/24'. Below the form is a network diagram showing a 'Local Site' (100.100.100.254) connected to an 'Internet' cloud, which is connected to a 'Router', which is connected to a 'Remote Site' (Dynamic Address, 192.168.160.0/24). At the bottom, there are 'Cancel', 'Back', and 'Finish' buttons.

**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**.

The screenshot displays the ZyXel VPN configuration wizard in the 'Scenario' step. The left sidebar contains a navigation menu with 'Site to Site VPN' highlighted. The main content area shows the following configuration options:

- Name: BranchtoHQ
- IKE Version:  IKEv2
- Config Type:  Wizard
- Behind NAT:  Local Site

Below the form is a network diagram illustrating the setup: a Local Site is connected to a Router, which is connected to the Internet, which is connected to a Remote Site. At the bottom of the wizard, there are 'Cancel' and 'Next' buttons, with 'Next' being highlighted in green.

**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

Peer Gateway Address Domain Name / IP



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.

The screenshot shows the 'Policy & Routing' configuration page for a Site to Site VPN. At the top, a progress bar indicates the current step is 4 out of 5, with steps labeled Scenario, Network, Authentication, Policy & Routing, and Summary. Below the progress bar, the 'Type' is set to 'Policy-Based' (selected with a radio button). The 'Local Subnet' is configured as '192.168.160.0/24' and the 'Remote Subnet' is '192.168.168.0/24', both fields are highlighted with red boxes. A network diagram below shows a 'Local Site' (192.168.1.100) connected to a 'Router', which is connected to the 'Internet' cloud, and another 'Router' connected to a 'Remote Site' (100.100.100.254). The Remote Site is further connected to a network with IP address 192.168.168.0/24. At the bottom of the page are 'Cancel', 'Back', and 'Finish' buttons.

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

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

The screenshot shows a configuration page for Site to Site VPN Authentication. At the top, there is a breadcrumb trail: VPN > Site to Site VPN. Below this is a progress indicator with five steps: Scenario (checked), Network (checked), Authentication (active, highlighted with a green circle and number 3), Policy & Routing (4), and Summary (5). The main content area is titled 'Authentication' and contains two radio button options: 'Pre-Shared Key' (selected) and 'Certificate Beta'. The 'Pre-Shared Key' option has a text input field containing seven dots, a red rectangular highlight around the dots, and a small eye icon to the right. Below the input field is a dropdown menu with 'default' selected. At the bottom of the page, there are three buttons: 'Cancel' on the left, 'Back' in the middle, and 'Next' on the right.

**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**

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

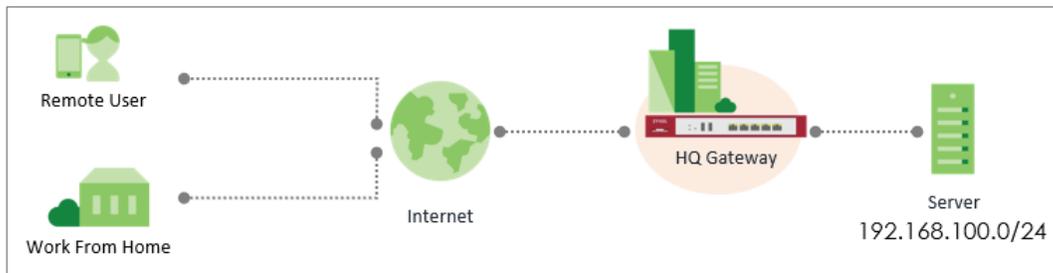
Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=1ms TTL=63
Reply from 192.168.160.1: bytes=32 time<1ms TTL=63
Reply from 192.168.160.1: bytes=32 time=7ms TTL=63

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 guide provides step-by-step instructions to set up Remote Access VPN on Zyxel USG FLEX H series devices using SSL VPN and IKEv2 VPN, with the new SecuExtender VPN Client. It's intended for IT administrators and support teams deploying secure remote access globally.



## Before You Begin

### 1. Create a Local User for VPN Authentication

Navigate to **User & Authentication > User/Group > User**

Create a local user account for remote access authentication.

- Enter a username and password.
- Save the settings.

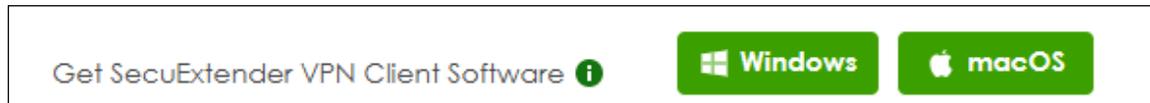
The screenshot shows the ZyXel management console interface. The left sidebar contains a search bar and a list of menu items: Network Status, VPN Status, Licensing, Network, VPN, Security Policy, Object, Security Service, User & Authentication (expanded), and System. Under 'User & Authentication', 'User/Group' is highlighted with a red box. The main content area shows the breadcrumb 'User & Authentication > User/Group > User'. Below the breadcrumb are tabs for 'User', 'Group', and 'Setting'. The 'User' tab is active. It displays two tables: 'Local Administrator' and 'User'. The 'Local Administrator' table has one entry: 'admin' with User Type 'admin'. The 'User' table has five entries: 'zyxel\_user' (User Type: user), 'radius-users' (User Type: ext-user), 'ldap-users' (User Type: ext-user), and 'ad-users' (User Type: ext-user). A red box highlights the '+ Add' button in the 'User' table.

The screenshot shows the 'Profile Management' form in the ZyXel management console. The breadcrumb is 'User & Authentication > User/Group'. The form has the following fields: 'User Name' (text input, value: 'zyxel\_vpn', highlighted with a red box), 'User Type' (dropdown menu, value: 'User'), 'Password' (password input, masked with dots), 'Retype' (password input, masked with dots), and 'Description' (text input, empty). A red box highlights the 'zyxel\_vpn' text in the 'User Name' field.

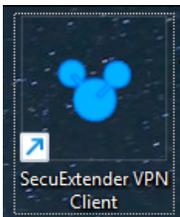
## 2. Download and Install the Latest SecuExtender VPN Client

You can download it from the device GUI or from the Zyxel official website.

[Download Link](#)



After installation, desktop shortcut icons will appear:



## Configure SSL VPN on the Device

1. Navigate to **VPN > SSL VPN**
2. Enable **SSL VPN**
3. Select the incoming interface (e.g., **ge1 (WAN)** or **ge4 (LAN)** ).
4. Choose the Port (Default port: **10443** ).
5. Choose the **tunnel type** based on your network policy:
  - **Internet and Local Networks (Full Tunnel)**: All traffic goes through VPN
  - **Local Networks Only (Split Tunnel)**: Only specified subnet(s) go through VPN
6. Define which internal network(s) VPN users can access.
  - Example: Allow access to **192.168.100.0/24**  
→ Add to **Local Networks**: 192.168.100.0/24
7. The default address pool for SSL VPN is **192.168.51.0/24**
8. Assign allowed users for SSL VPN access

\* This SSL VPN configuration is also compatible with standard OpenVPN clients. You can download the **.ovpn** file from the device and import it into an OpenVPN client to establish a connection.

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

Enable

SSL VPN Configuration Download [Download](#)

**Incoming Interface**

Interface:

DNS Name:  (Optional)

Server Port:

Zone:

**Clients will use VPN to access**

Internet and Local Networks (Full Tunnel)

Local Networks Only (Split Tunnel)

**Local Networks**

+ Add - Remove

Network
<input type="checkbox"/> 192.168.100.0/24

**Client Network**

IP Address Pool:

First DNS Server:  ZyWALL  Custom Defined

Second DNS Server:

**Authentication**

Primary Server:

Secondary Server:

User:

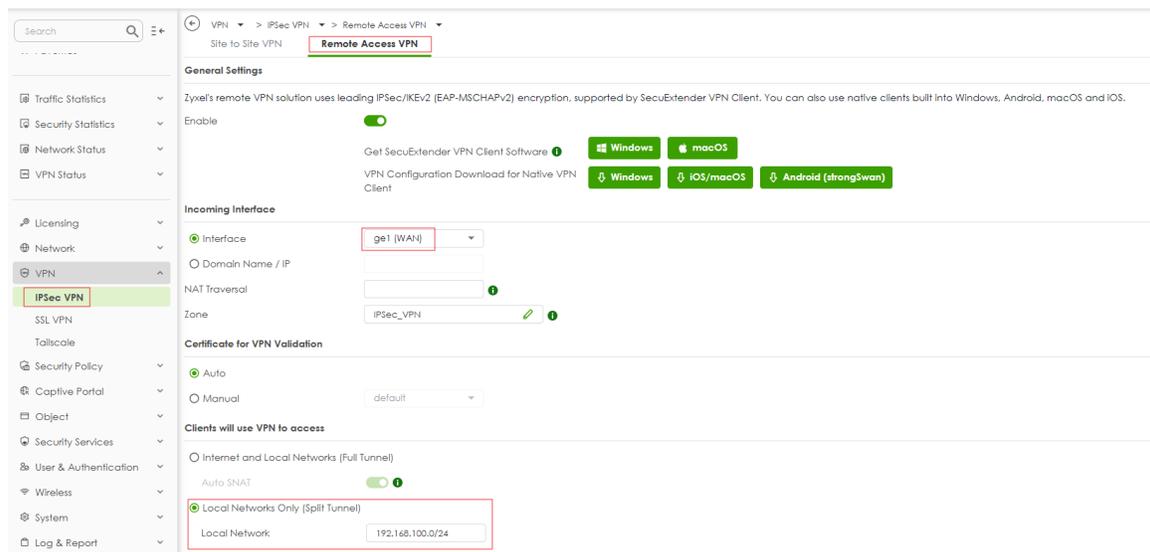
## Configure IKEv2 VPN on the Device

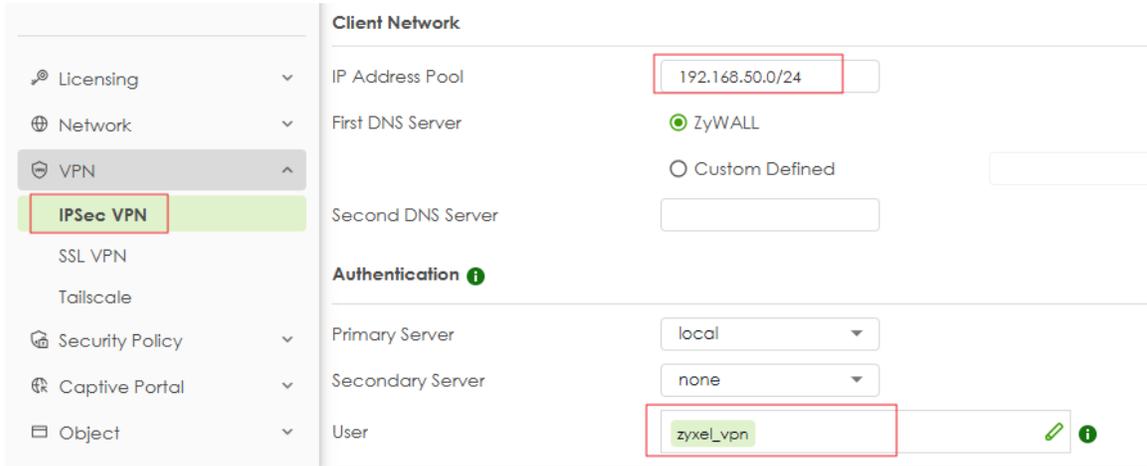
1. Navigate to **VPN > IPsec VPN > Remote Access VPN**
2. Enable **IPSev VPN**
3. Select the incoming interface (e.g., **ge1 (WAN)** or **ge4 (LAN)** )
4. Choose the **tunnel type** based on your network policy:
  - **Internet and Local Networks (Full Tunnel):** All traffic goes through VPN

- **Local Networks Only (Split Tunnel):** Only specified subnet(s) go through VPN
5. Define which internal network(s) VPN users can access.
    - *Example: Allow access to 192.168.100.0/24*  
→ Add to **Local Network:** 192.168.100.0/24
  6. The default address pool for IKEv2 VPN is **192.168.50.0/24**
  7. Assign allowed users for IKEv2 VPN access

 **Note:** When configuring IKEv2 VPN for use with the **Windows (Native IKEv2 Client)** and selecting Interface as the incoming interface, you must enter the **domain name** (as shown in the certificate) in the **NAT Traversal** field.

This allows the Windows client to correctly establish the VPN tunnel using the domain name instead of the IP address. (see **Self-Signed Certificate Scenario (For Windows Native IKEv2 Client)**)

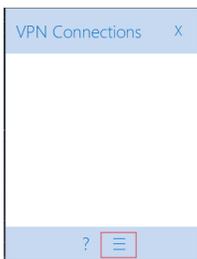




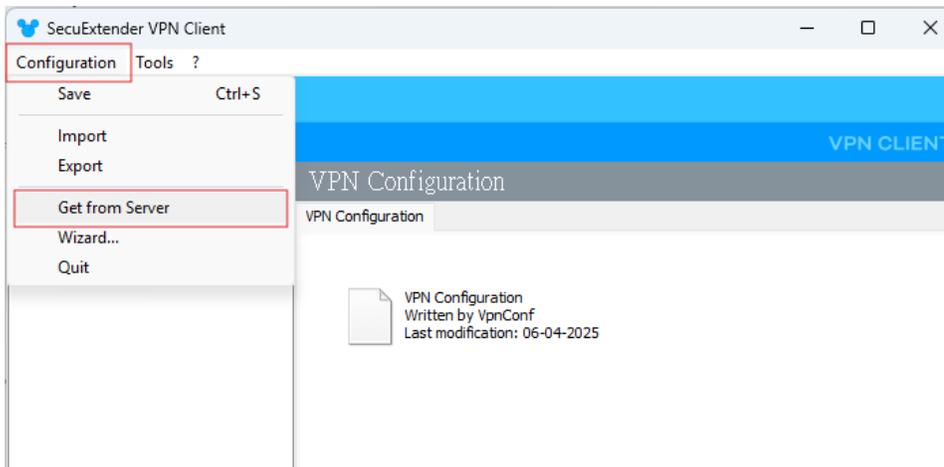
## Set Up Remote Access on SecuExtender VPN Client

The new SecuExtender VPN Client combines **SSL VPN** and **IKEv2 VPN** in a single application, eliminating the need for separate software.

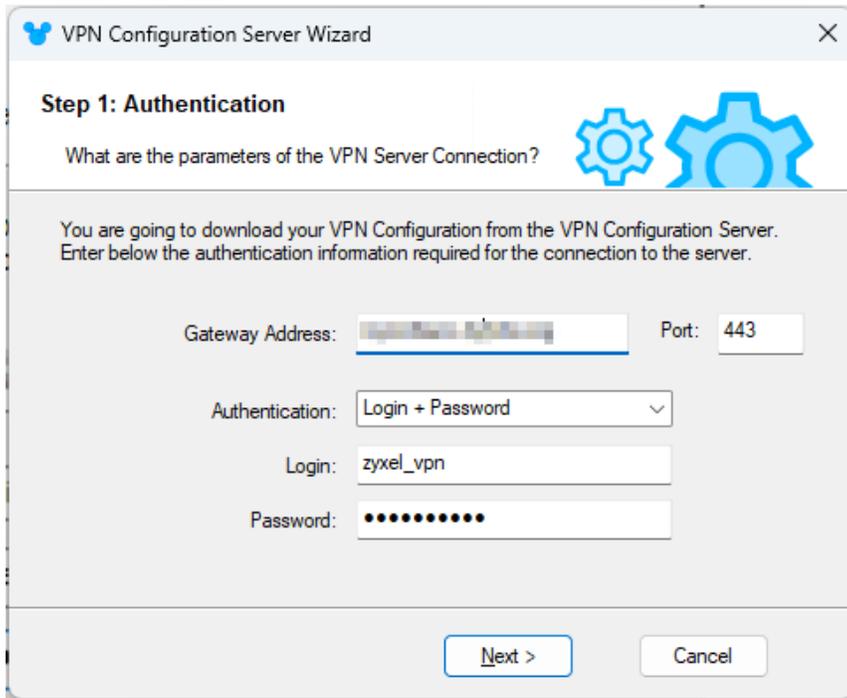
1. Launch the client



2. Navigate to **Menu > Configuration > Get from Server**

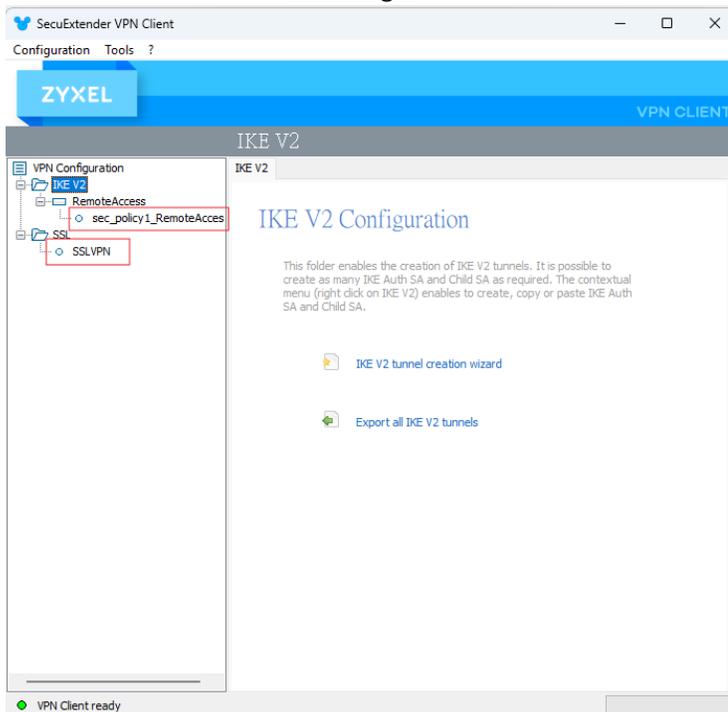


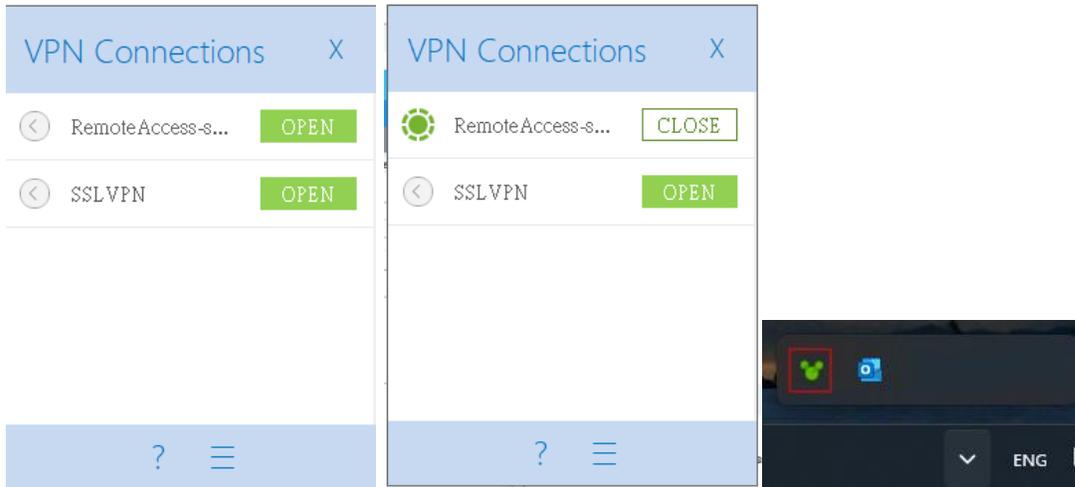
3. Enter the **Gateway Address**, **Username**, and **Password**
4. Click **Next** to fetch the VPN configuration file



The image shows a 'VPN Configuration Server Wizard' window. The title bar says 'VPN Configuration Server Wizard'. The main heading is 'Step 1: Authentication'. Below the heading is the question 'What are the parameters of the VPN Server Connection?' followed by two gear icons. A paragraph of text reads: '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.' There are four input fields: 'Gateway Address' (with a blurred value), 'Port' (with the value '443'), 'Authentication' (a dropdown menu with 'Login + Password' selected), 'Login' (with the value 'zyxel\_vpn'), and 'Password' (with masked characters). At the bottom, there are two buttons: 'Next >' and 'Cancel'.

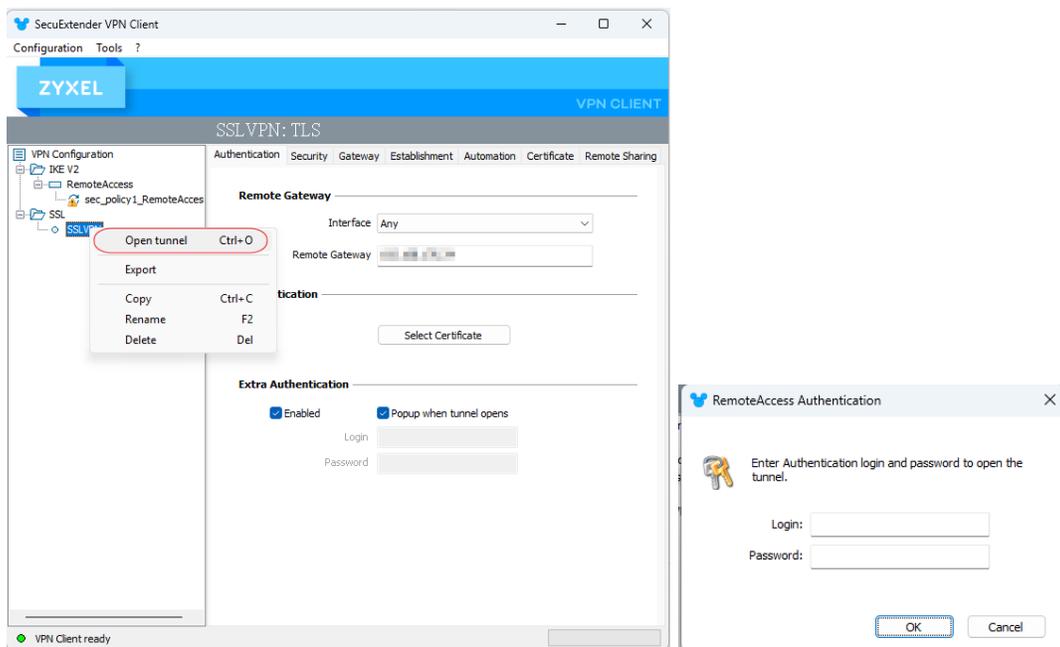
5. Both SSL VPN and IKEv2 settings will be available.





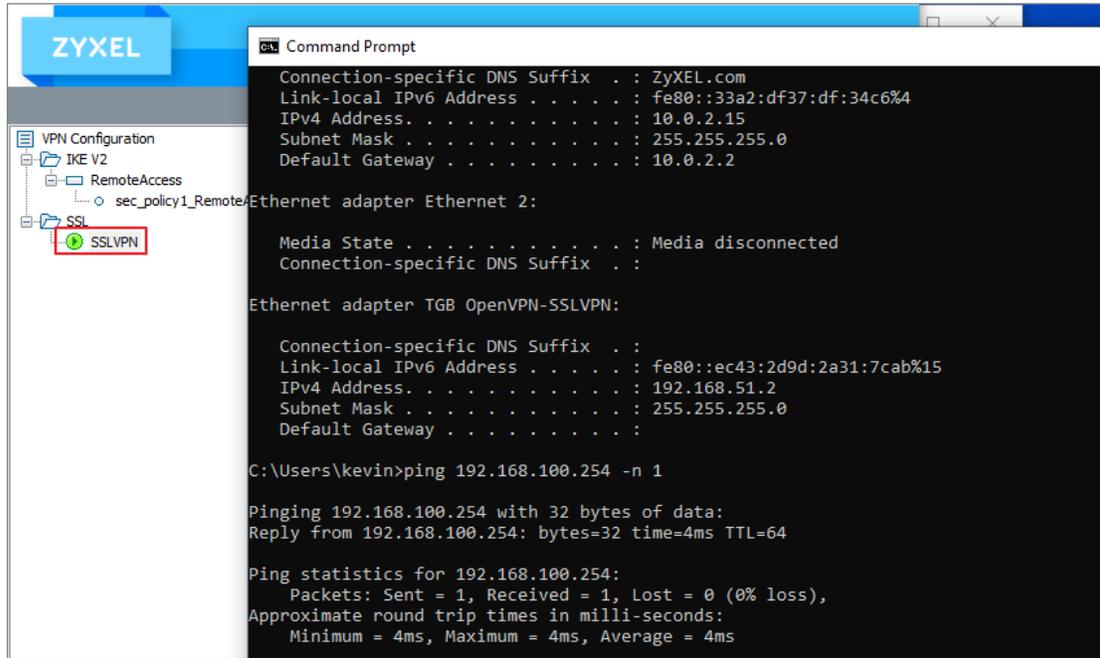
## Test SSL VPN Tunnel on SecuExtender VPN Client

1. Launch the SecuExtender VPN Client
2. Right-click the VPN profile and **“Open Tunnel”** and log in.



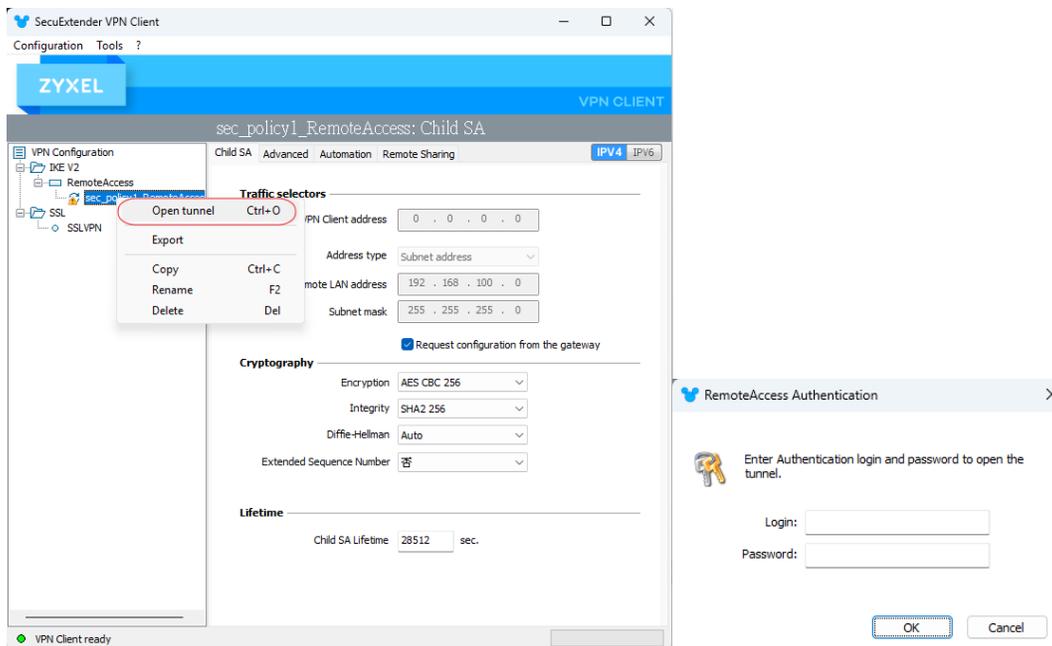
3. Once connected, the profile status will turn green, indicating an active tunnel.

4. You should now be able to access internal network resources.

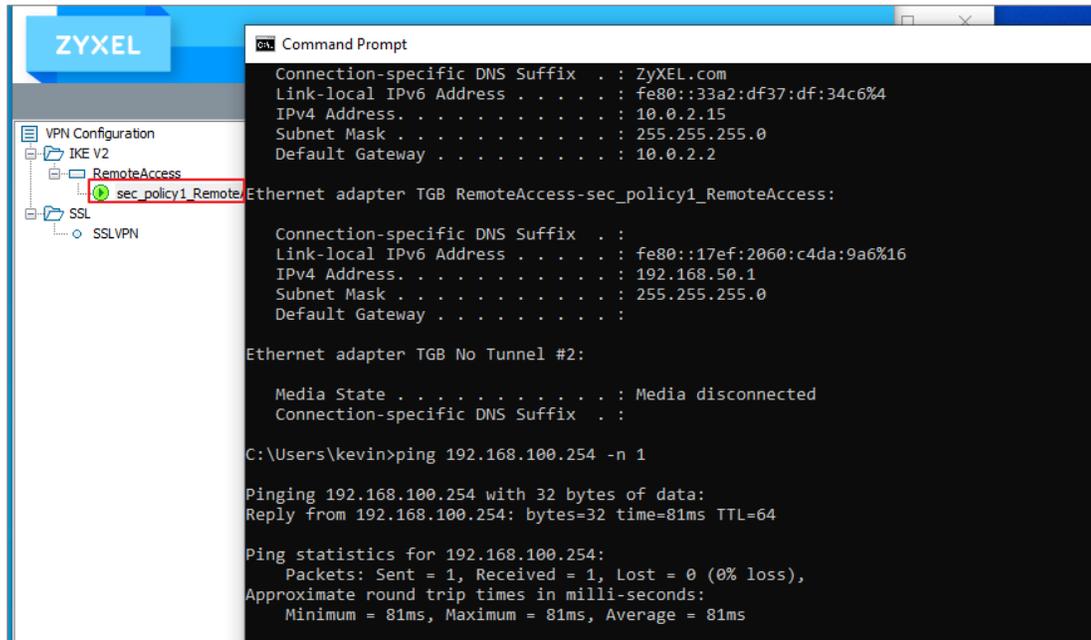


## Test IKEv2 VPN Tunnel on SecuExtender VPN Client

1. Launch the SecuExtender VPN Client
2. Right-click the VPN profile and **"Open Tunnel"** and log in.



- Once connected, the profile status will turn green, indicating an active tunnel.
- You should now be able to access internal network resources.

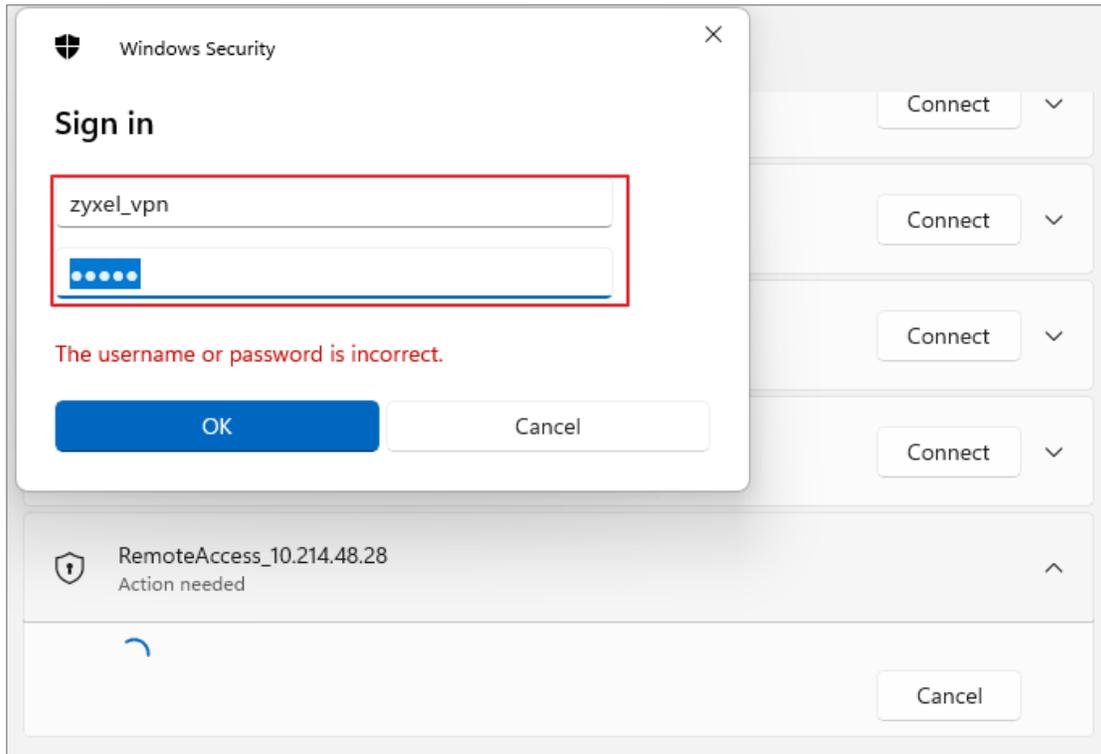


## Set Up IKEv2 VPN On Windows (Native IKEv2 Client)

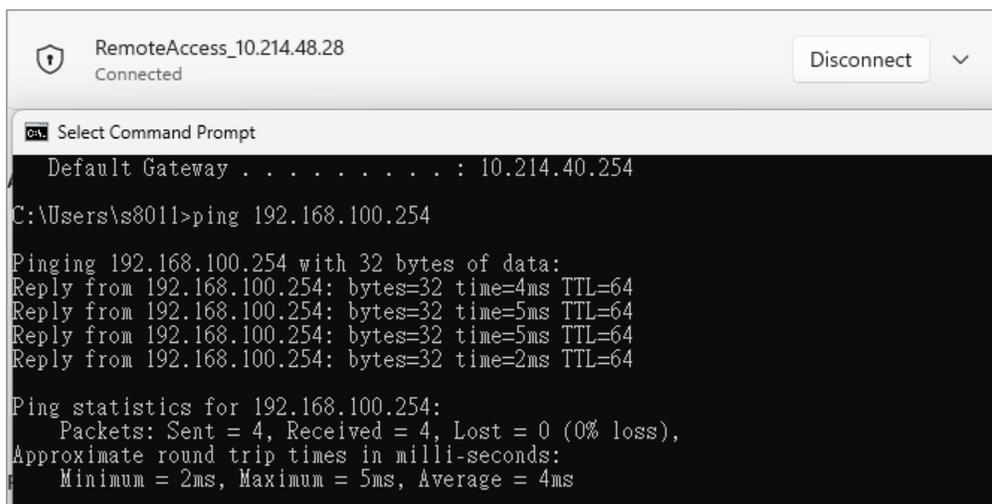
- Download the VPN configuration script from the USG FLEX H web configurator.



- Run the script (.bat file) and enter your credentials when prompted.

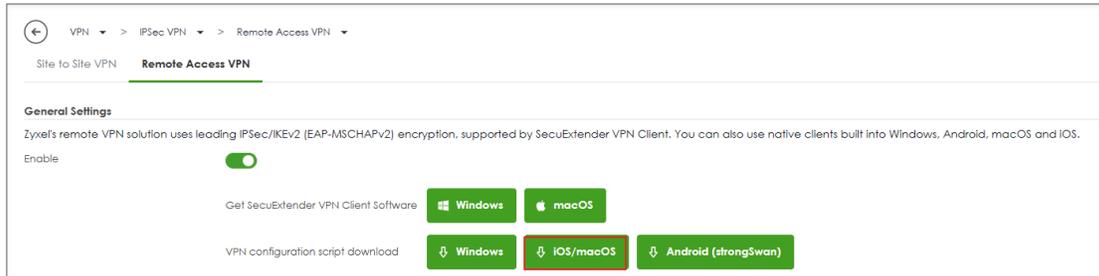


3. VPN will connect and access internal resources

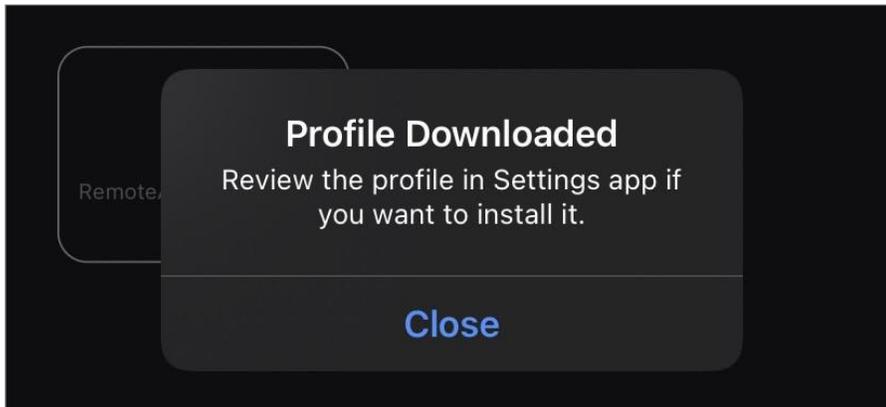


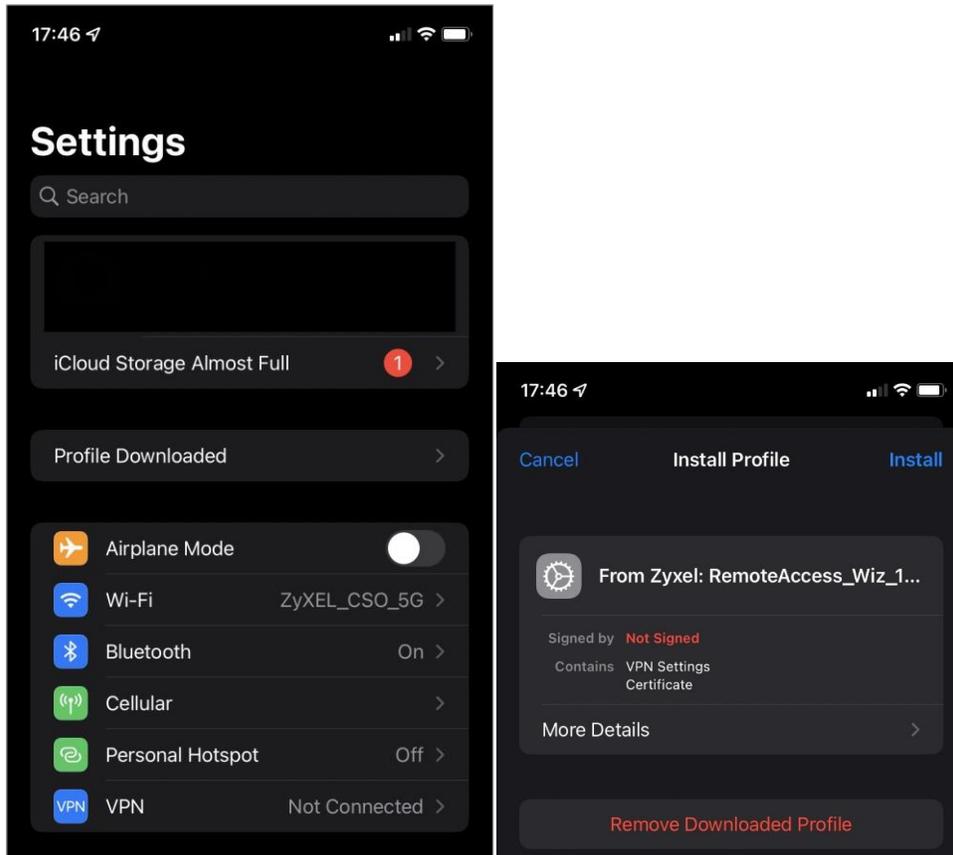
## Set Up IKEv2 VPN on iOS

1. Download the iOS/macOS VPN configuration script from the USG FLEX H web configurator.

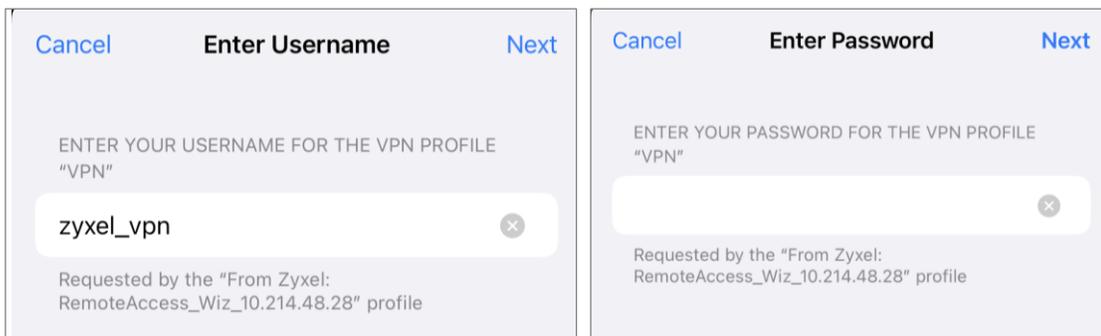


2. Send it to the iOS/macOS device.
3. Go to **Settings > Profile Downloaded**, then **Install**  
(Mac device: System Settings > Network / VPN )

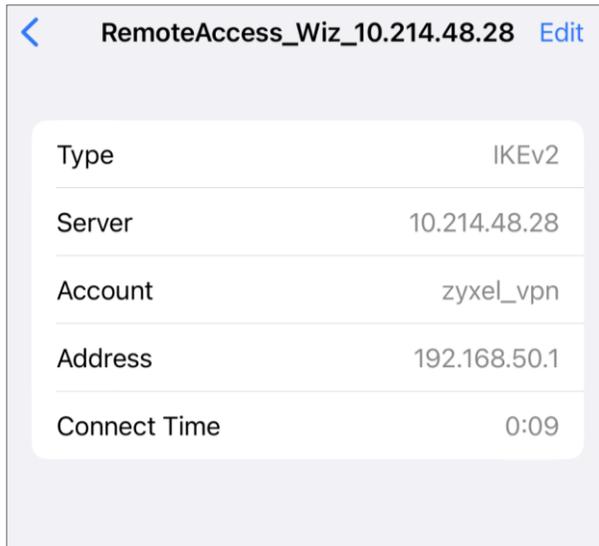




4. Enter your username and password.



5. Connect to the VPN from the **Settings** > **VPN** menu.

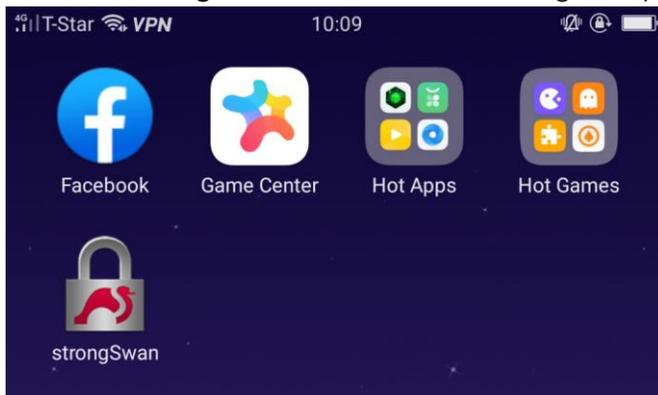


## Set Up IKEv2 VPN on Android (strongSwan App)

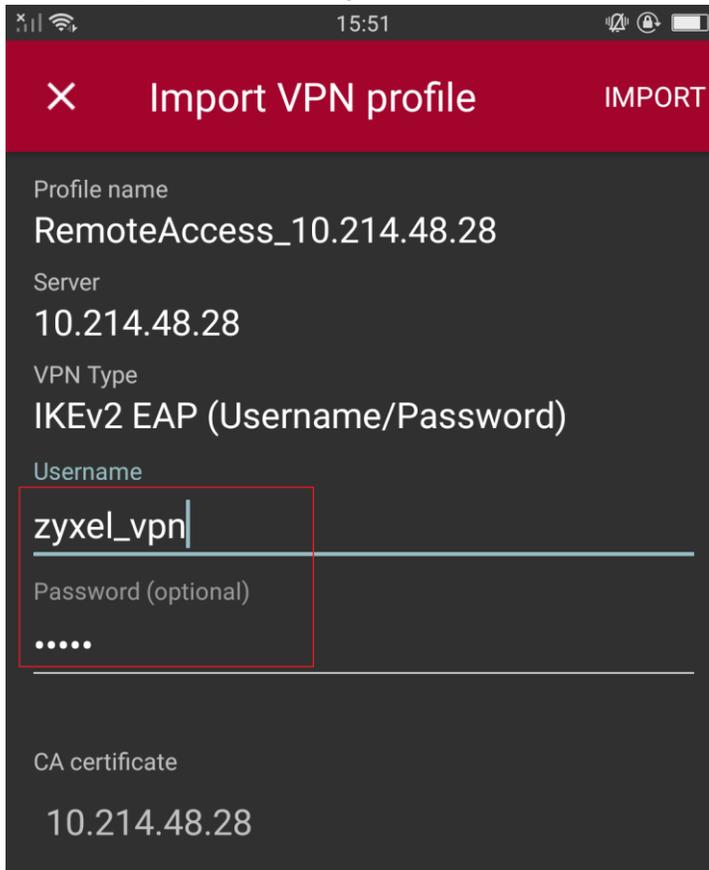
1. Download the Android VPN configuration script from the USG FLEX H web configurator.



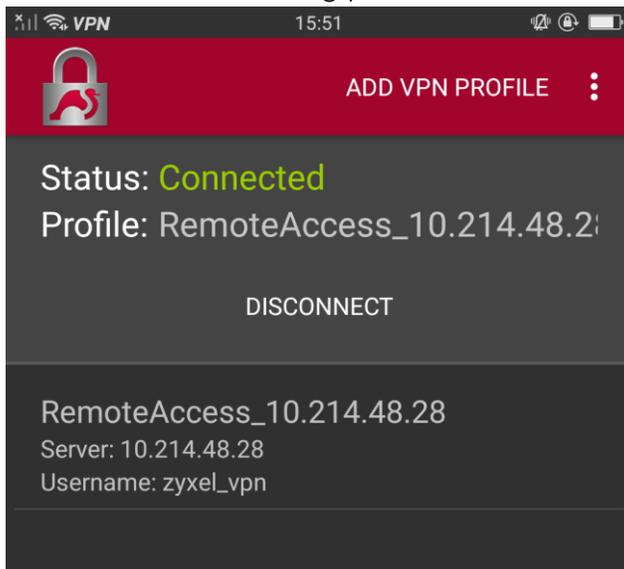
2. Install the **strongSwan VPN Client** from Google Play Store



3. Send the config script to the Android device.
4. Import the profile into strongSwan



5. Connect to the VPN using your credentials

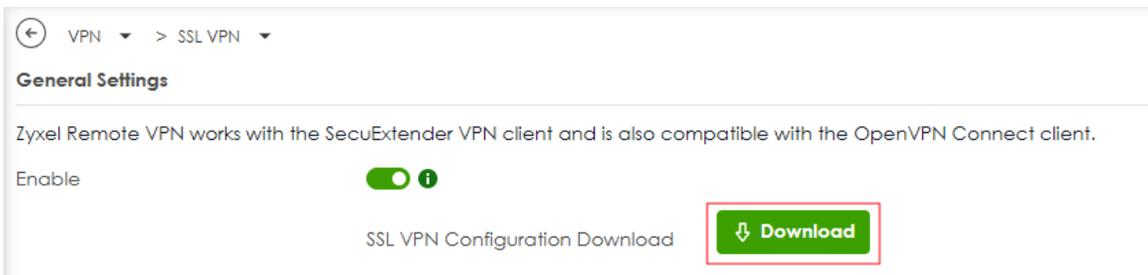


## Set Up OpenVPN Client

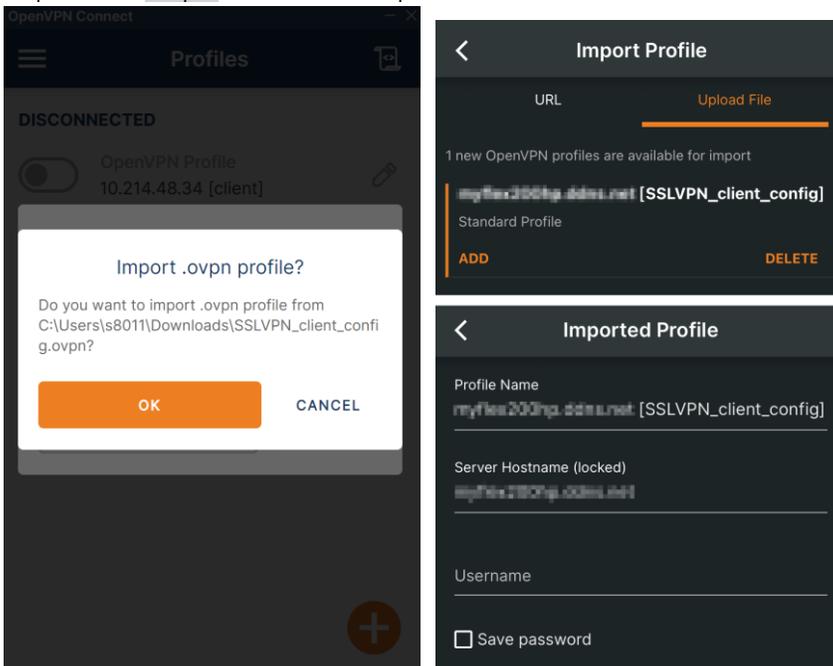
1. Download and install the **OpenVPN Connect** client from the OpenVPN official website or app store.



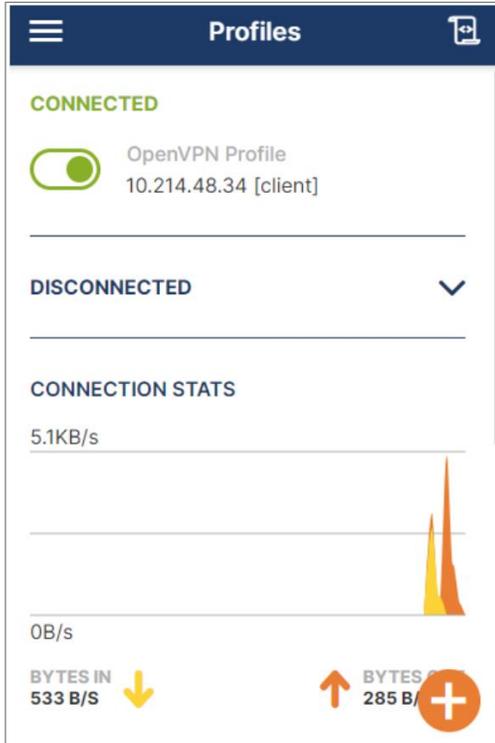
2. Download the SSL VPN configuration script from the USG FLEX H web configurator at **VPN > SSL VPN**



3. Import the `.ovpn` file into the OpenVPN client



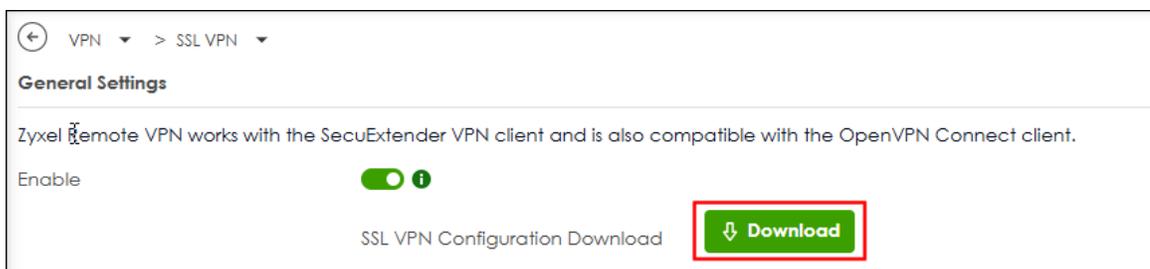
- Once connected, you can access internal resources.



## Configuring Split Routing for OpenVPN Connect Client

When the USG FLEX H is configured for **Full Tunnel** but you need **Split Tunnel** for specific clients, you can configure different split route settings by modifying the SSL VPN configuration file (.ovpn). This document explains the process:

- Download the SSL VPN configuration file (.ovpn) from the USG FLEX H.



2. Open the .ovpn file in a text editor.

```
client
dev tun
proto tcp
remote sslvpn.mydomain.local 10443
resolv-retry infinite
nobind
persist-key
persist-tun
auth sha256
cipher aes-256-cbc
auth-user-pass
verb 3
reneg-sec 28800
redirect-gateway
<key>
-----BEGIN PRIVATE KEY-----
```

3. Modify the file to enable split routing:

- a. Remove the **redirect-gateway** line to disable full routing.

```
client
dev tun
proto tcp
remote sslvpn.mydomain.local 10443
resolv-retry infinite
nobind
persist-key
persist-tun
auth sha256
cipher aes-256-cbc
auth-user-pass
verb 3
reneg-sec 28800
redirect-gateway
<key>
-----BEGIN PRIVATE KEY-----
```

- b. Add **route-nopull** to prevent pulling routes from the SSL VPN server.
- c. Add specific routes, e.g., **route 192.168.168.0/24** and **route 192.168.169.0/24**

**Add split routes**

- ➔ Add "route 192.168.168.0 255.255.255.0"
- ➔ Add "route 192.168.169.0 255.255.255.0"

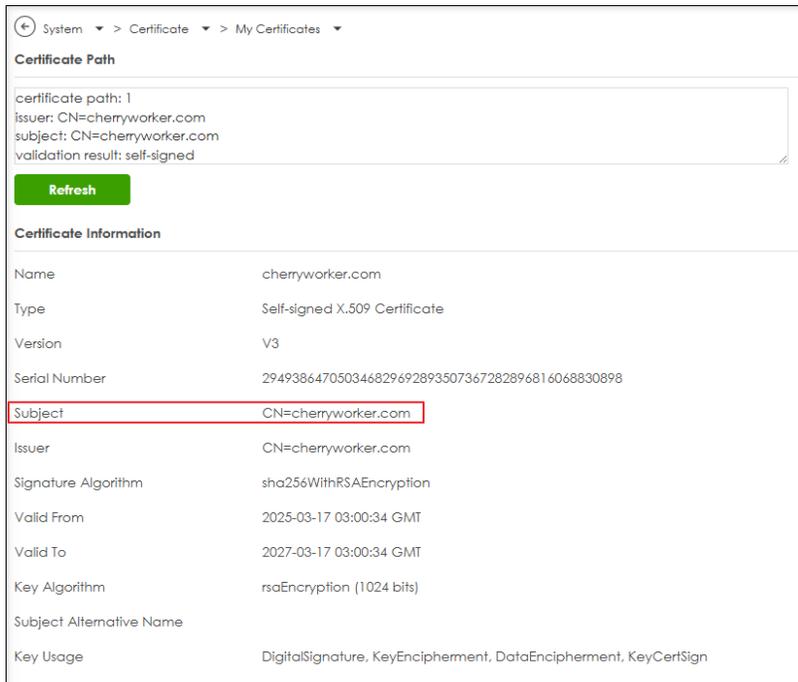
```
client
dev tun
proto tcp
remote sslvpn.mydomain.local 10443
resolv-retry infinite
nobind
persist-key
persist-tun
auth sha256
cipher aes-256-cbc
auth-user-pass
verb 3
reneg-sec 28800
route-nopull
route 192.168.168.0 255.255.255.0
route 192.168.169.0 255.255.255.0
<key>
-----BEGIN PRIVATE KEY-----
```

## Troubleshooting Self-Signed Certificates with Native Windows VPN Client

If using a self-signed certificate with a domain name and the incoming interface set to "Interface", you may encounter connection issues. Follow these steps to configure **NAT Traversal** to resolve this:

### Conditions

- (1) Incoming Interface set to "**Interface**".
- (2) The self-signed certificate subject name (Certificate for VPN Validation) set as a "**domain name**". (e.g., cherryworker.com)



## Solution: Configure NAT Traversal

- (1) Log in to the USG FLEX H management interface.
- (2) Navigate to **VPN > IPSec VPN > Remote Access VPN**.
- (3) Locate the **NAT Traversal** settings.
- (4) Set the **NAT Traversal** field to the same domain name as the certificate (e.g., cherryworker.com).
- (5) Save the settings.
- (6) Download the updated Windows VPN configuration script from the USG FLEX H web configurator.
- (7) The script will automatically use the domain name (e.g., cherryworker.com) instead of an IP address for the "ServerAddress".
- (8) The VPN should connect without manual changes to the script.

This ensures proper script generation and prevents connection failure.

More info: [Microsoft Troubleshooting Guide](https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/troubleshoot-always-on-vpn). ( <https://learn.microsoft.com/en-us/troubleshoot/windows-server/networking/troubleshoot-always-on-vpn> )

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 Download for Native VPN Client [Windows](#) [iOS/macOS](#) [Android \(strongSwan\)](#)

**Incoming Interface**

Interface  1.

Domain Name / IP  3. **Self-Signed Server Name:** **cherryworker.com**

NAT Traversal

Zone  [i](#)

**Certificate for VPN Validation**

Auto

Manual  2.

**Clients will use VPN to access**

Internet and Local Networks (Full Tunnel)

Auto SNAT  [i](#)

Local Networks Only (Split Tunnel)

Local Network:

**Client Network**

IP Address Pool

First DNS Server  ZyWALL

Script of "ServerAddress".

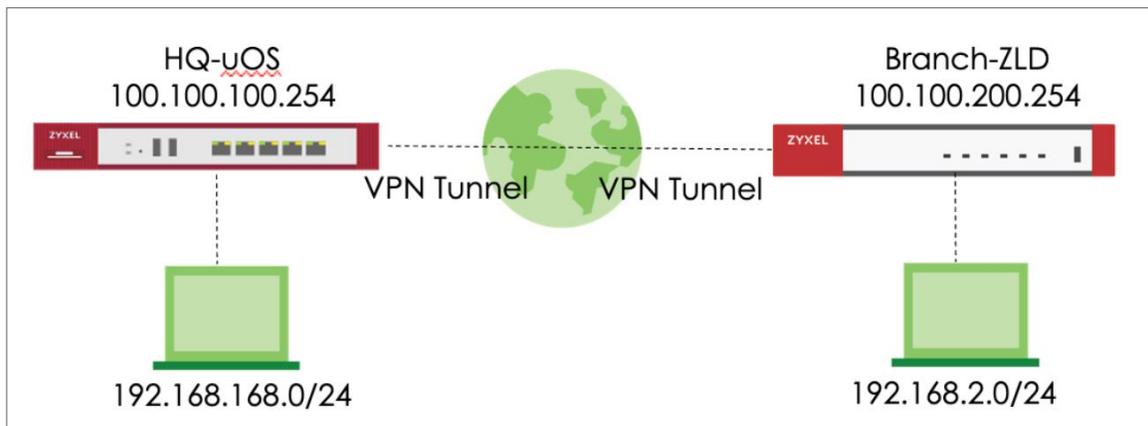
```

@echo off

set Name="RemoteAccess_cherryworker.com"
set ServerAddress="cherryworker.com"
set TunnelType="IKEv2"
set AuthenticationMethod="EAP"
set EncryptionLevel="Required"
set UseWinlogonCredential=$False
set RememberCredential=$False
set SplitTunneling=$True
set IKEEnc="AES256"
set IKEAuth="SHA256"
set IKEKey="ECP256"
set ESPEnc="AES256"
set ESPAuth="SHA256128"
set ESPPfs="None"
:: Installing CA certificate requires Administrator privileges.
call :isAdmin
  
```

## 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**.

The screenshot shows the configuration page for Site to Site VPN, Network tab. The breadcrumb trail is VPN > Site to Site VPN. The progress indicator shows five steps: Scenario (checked), 2 Network (active), 3 Authentication, 4 Policy & Routing, and 5 Summary. The configuration fields are as follows:

Field	Value
My Address	100.100.100.254
Peer Gateway Address	100.100.200.254

Below the form is a diagram showing a Local Site (100.100.100.254) connected to an Internet cloud, which is then connected to a Remote Site (100.100.200.254). At the bottom of the page are three buttons: Cancel, Back, and Next.

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

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

The screenshot shows a configuration wizard for a Site to Site VPN. The breadcrumb path is VPN > Site to Site VPN. The wizard has five steps: 1. Scenario (checked), 2. Network (checked), 3. Authentication (active), 4. Policy & Routing, and 5. Summary. Under the 'Authentication' step, there are two radio button options: 'Pre-Shared Key' (selected) and 'Certificate'. A text input field for the Pre-Shared Key is highlighted with a red box and contains seven dots. Below it is a dropdown menu set to 'default'. At the bottom of the form, there are three buttons: 'Cancel', 'Back', and '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.

The screenshot shows the 'Policy & Routing' configuration page for a Site to Site VPN. The breadcrumb trail is 'VPN > Site to Site VPN'. The progress indicator shows five steps: Scenario, Network, Authentication, Policy & Routing (current step, highlighted with a green '4'), and Summary (highlighted with a grey '5').

Under 'Type', the 'Policy-Based' radio button is selected. The 'Local Subnet' field contains '192.168.168.0/24' and the 'Remote Subnet' field contains '192.168.2.0/24', both highlighted with red boxes.

A network diagram below shows two sites connected via the Internet. The 'Local Site' has a ZyWALL icon and a local network of 192.168.168.0/24. The 'Remote Site' has a ZyWALL icon and a local network of 192.168.2.0/24. The Internet cloud is labeled 'Internet'.

At the bottom, there are 'Cancel', 'Back', and 'Finish' buttons.

**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	HQtoFLEX
IKE Version	2
Type	Policy-based
Proposal	<input type="text"/>

**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
--------------	------------------

[Edit](#)

[Close](#)

## 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**

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

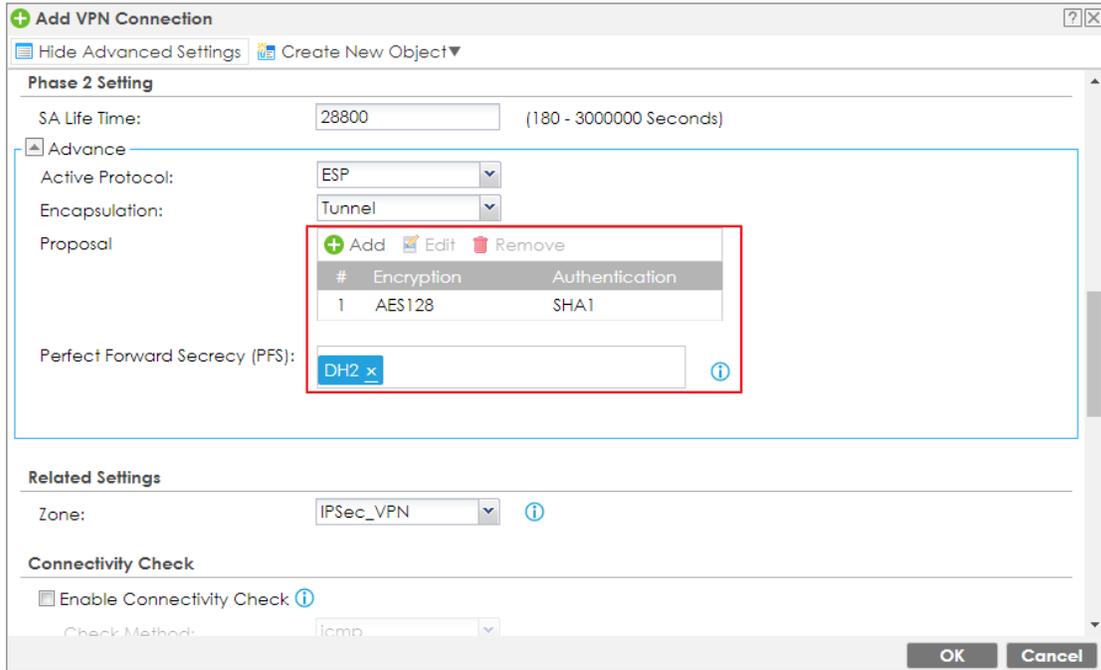
**Policy**

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.



## Test IPsec VPN Tunnel

### VPN Status > IPsec VPN

Verify the IPsec VPN status on uOS device.

The screenshot shows the 'Site to Site VPN' configuration page. At the top, there are buttons for 'Disconnect' and 'Refresh'. Below is a table with columns for Name, Policy Route, My Address, Remote Gateway, Uptime, Rekey, Inbound (bytes), and Outbound (Bytes). One tunnel is listed with the name 'HQtoFLEX' and a policy route of '192.168.168.0/24 <-> 192.168.2.0/24'. The 'My Address' is 100.100.100.254 and the 'Remote Gateway' is 100.100.200.254. The tunnel has been up for 233 seconds, with 81615 rekeys, 7 (420 bytes) inbound traffic, and 36 (2,04K bytes) outbound traffic.

	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:

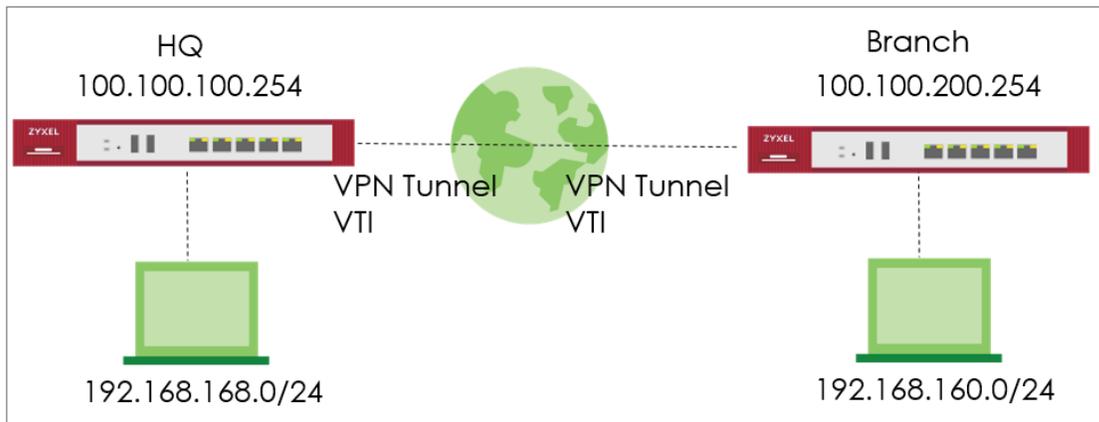
C:\Windows\system32>ping 192.168.2.34

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.



## 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 navigation menu with options like Dashboard, 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, and Log & Report. The main area is titled 'VPN > Site to Site VPN' and has a progress bar with five steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active. The configuration fields are: \*Name: HQtoBranch; IKE Version: IKEv2 (selected); Type: Site-to-Site (selected); Behind NAT: None (selected). Below the fields is a diagram showing a 'Local Site' and a 'Remote Site' connected via an 'Internet' cloud. At the bottom 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	<input type="text" value="100.100.100.254"/>
Peer Gateway Address	Domain Name / IP	<input type="text" value="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**

The screenshot shows the ZyXel VPN configuration interface for Site to Site VPN. The breadcrumb path is VPN > Site to Site VPN. The configuration progress is shown as a sequence of steps: 1. Scenario (checked), 2. Network (checked), 3. Authentication (active), 4. Policy & Routing, and 5. Summary. Under the Authentication step, there are two radio button options: Pre-Shared Key (selected) and Certificate. A text input field for the Pre-Shared Key is highlighted with a red border and contains seven asterisks. Below the input field is a dropdown menu currently set to 'default'. At the bottom of the interface, there are three buttons: 'Cancel', 'Back', and 'Next'.

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

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

The screenshot shows the 'Policy & Routing' configuration page for a Site to Site VPN. At the top, a progress bar indicates the current step is 4 out of 5, with steps: Scenario (checked), Network (checked), Authentication (checked), Policy & Routing (active), and Summary (disabled). Below the progress bar, the 'Type' is set to 'Route-Based' (selected with a radio button and highlighted by a red box) and 'Policy-Based' (unselected). The 'Remote Subnet' is configured as '192.168.160.0/24' (also highlighted by a red box). A network diagram below shows a 'Local Site' (100.100.100.254) connected to an 'Internet' cloud, which is then connected to a 'Remote Site' (100.100.200.254). The Remote Site is further connected to a subnet of '192.168.160.0/24'. At the bottom, there are 'Cancel', 'Back', and 'Finish' buttons.

**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	Route

[Edit](#)

**Network**

Local Site	100.100.100.254
Remote Site	100.100.200.254

**Authentication**

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

**Policy & Routing**

Remote Subnet	192.168.160.0/24
---------------	------------------

[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**.

The screenshot displays the ZyXel VPN configuration interface. On the left is a navigation menu with options like Dashboard, My Favorite, System Statistics, Security Statistics, Network Status, VPN Status, Licensing, Network, VPN, Site to Site VPN (highlighted), Security Policy, Object, Security Service, User & Authentication, System, and Log & Report. The main area shows the configuration steps: 1 Scenario, 2 Network, 3 Authentication, 4 Policy & Routing, and 5 Summary. The 'Scenario' step is active, with the following settings: \*Name: BranchtoHQ, IKE Version: IKEv2, Type: Site-to-Site, and Behind NAT: None. A diagram below shows a Local Site connected to an Internet cloud, which is then connected to a Remote Site. At the bottom, there are 'Cancel' and 'Next' buttons.

**VPN > Site to Site VPN > Scenario > Network**

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

The screenshot shows the configuration interface for a Site to Site VPN. At the top, there is a breadcrumb trail: VPN > Site to Site VPN. Below this is a progress indicator with five steps: 1. Scenario (checked), 2. Network (active), 3. Authentication, 4. Policy & Routing, and 5. Summary.

The main configuration area contains two rows of input fields:

- Row 1: "My Address" label, "Domain Name / IP" label, and a text input field containing "100.100.200.254".
- Row 2: "Peer Gateway Address" label, "Domain Name / IP" label, and a text input field containing "100.100.100.254".

Below the input fields is a network diagram showing a "Local Site" (represented by a server icon) and a "Remote Site" (represented by a server icon) connected to a central "Internet" cloud. The IP address "100.100.200.254" is associated with the Local Site, and "100.100.100.254" is associated with the Remote Site.

At the bottom of the interface, there are three buttons: "Cancel" on the left, "Back" in the center, and "Next" on the right (highlighted in green).

**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 Remote Subnet.

VPN > Site to Site VPN

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

Type  Route-Based  Policy-Based

Remote Subnet

Any 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	Route

[Edit](#)

**Network**

Local Site	100.100.200.254
Remote Site	100.100.100.254

**Authentication**

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

**Policy & Routing**

Remote Subnet	192.168.168.0/24
---------------	------------------

[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	BranchHQ	0.0.0.0/0 <-> 0.0.0.0/0	100.100.200.254	100.100.100.254	5	84539	0 (0 bytes)	0 (0 bytes)

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

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>

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	

## How to Use Tailscale

### What's Tailscale?

Tailscale is a secure, peer-to-peer VPN solution that simplifies connecting devices over the internet. Unlike traditional VPNs, Tailscale establishes direct connections between devices without requiring complex firewall configurations or static IP addresses. It uses a mesh network topology, allowing every device to communicate directly with every other device securely.

### Start to Tailscale and implement on Firewall

1. Please refer [TailScale KB](#) to create an account and start.
2. Navigate to "Settings -> Personal Settings -> Keys" and "Generate auth key".

The screenshot shows the Zyxel Tailnet Settings interface. At the top, there is a navigation bar with the following items: 'Machines', 'Apps', 'Services', 'Users', 'Access controls', 'Logs', 'DNS', 'Settings' (highlighted), and 'Get started'. The 'Settings' section is expanded, showing a sidebar with 'Personal Settings' (highlighted) and 'Keys' (highlighted). The main content area is titled 'Keys' and contains the following text: 'View and manage your Auth keys and API access tokens. Your private device keys are not included here: they are always private, stay on your device, and are never shared with Tailscale. [Learn more](#)'. Below this, there is a section for 'Auth keys' with the text 'Authenticate devices without an interactive login. [Learn more](#)' and a 'Generate auth key...' button. A message box states 'You don't have any valid auth keys' and a link '> 1 recently invalidated auth key' is visible.

3. Give a Description Name as you want and disable "Reusable" due to security reason then click "Generate key".

### Generate auth key ✕

**Description**  
Add an optional description for the key.

**Reusable**   
Use this key to authenticate more than one device.

**Expiration**  
Number of days until this auth key expires. This will not affect the [node key expiry](#) of any machine authenticated with this auth key.

90   days  
Must be between 1 and 90 days.

---

**DEVICE SETTINGS**  
These settings will apply to any devices authenticated using this key.

**Ephemeral**   
Devices authenticated by this key will be automatically removed after going offline. [Learn more ↗](#)

**Tags**   
Devices authenticated by this key will be automatically tagged. This will also disable node key expiry for the device. [Learn more ↗](#)

Copy the key.

### Generated new key ✕

Be sure to copy your new key below. It won't be shown in full again.

tskey-auth-kc5HbhKcQQ11CNTRL-



ⓘ This key will expire on Jun 2, 2025. If you'll then want to continue using an auth key, you'll need to generate a new one.

Done

4. Login Firewall and navigate to "VPN -> Tailscale", paste to the "Auth Keys".

The screenshot shows the 'VPN > Tailscale' configuration page. Under 'General Settings', the 'Enable' toggle is turned on. The 'Auth Keys' field contains a key and has a 'Logout' button next to it. The 'Server Port' is set to 41641. The 'Zone' is set to 'Tailscale'. Under 'Routing', the 'As an Exit Node' toggle is turned on.

Note:

- When you want to change the key, please click Logout.
- You can choose the zone by yourself. We recommend using Tailscale zone for some predefined rules.

5. Go back to the Tailscale admin page. You will see the Firewall device.

The screenshot shows the Tailscale admin interface for 'zyxel.com.tw'. At the top, there are navigation links for 'Machines', 'Apps', 'Services', 'Users', 'Access controls', 'Logs', 'DNS', and 'Settings'. Below the navigation is a search bar and a 'Filters' dropdown. A table lists the connected machines:

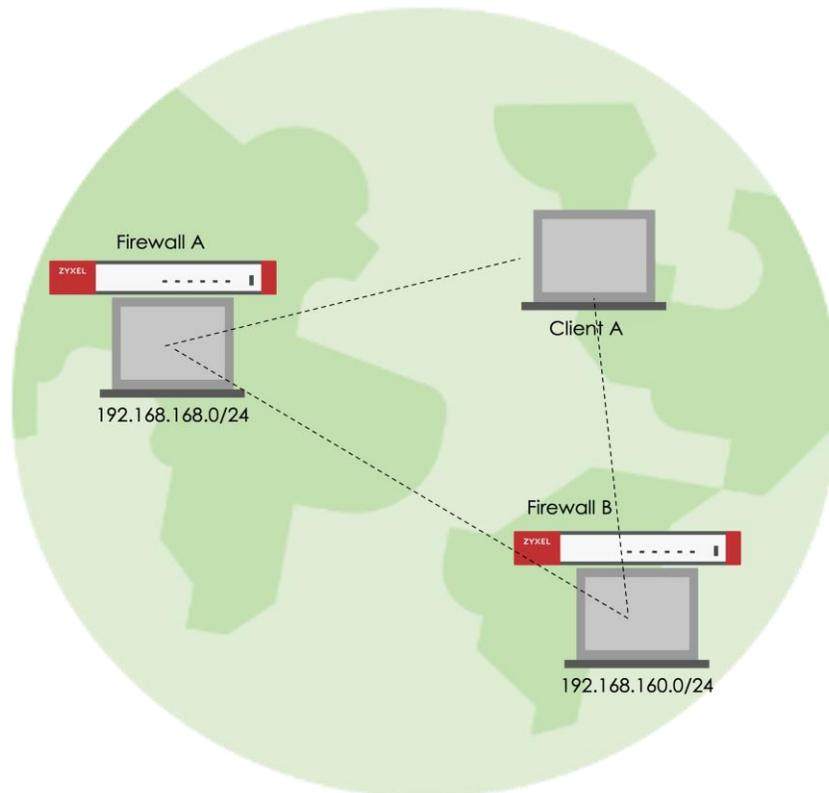
MACHINE	ADDRESSES	VERSION	LAST SEEN
twbnbt123234-01 Kevin.Wu4@zyxel.com.tw	100.95.1	1.80.2 Windows 11 22H2	Connected
<b>usgflex500h</b> Kevin.Wu4@zyxel.com.tw	100.115.1	1.75.16 Linux 4.14.207-10.3.7.0-2	Connected

Click "Disable key expiry" for all client to prevent lost connection while expire.

This screenshot shows a detailed view of the 'usgflex500h' machine. It displays the IP address '100.115.120.97', version '1.75.16', and OS 'Linux 4.14.207-10.3.7.0-2'. A dropdown menu is open, showing options: 'Edit machine name...', 'Edit machine IPv4...', 'Share...', and 'Disable key expiry'. The 'Disable key expiry' option is highlighted with a red box.

## Scenario

We have two subnets, 192.168.168.0/24 and 192.168.160.0/24, which are located behind firewalls. Both the firewalls and the Client A are part of the Tailscale VPN network. The objectives are as follows:



**Case1: Allow Client A to access the 192.168.168.0/24 and 192.168.160.0/24 subnets**

1. Advertised 192.168.168.0/24 in Firewall A.

VPN > Tailscale

**General Settings**

Zyxel's Tailscale VPN solution is compatible with the Tailscale VPN client, which is built into Windows, macOS, Android, and iOS, and can be managed through the Tailscale Portal.

Enable

Auth Keys

Server Port  (1-65535)

Zone

**Routing**

As an Exit Node

**Advertised Networks**

+ Add Remove

Network
<input type="checkbox"/> N_192_168_168

2. Advertised 192.168.160.0/24 in Firewall B.

VPN > Tailscale

**General Settings**

Zyxel's Tailscale VPN solution is compatible with the Tailscale VPN client, which is built into Windows, macOS, Android, and iOS, and can be managed through the Tailscale Portal.

Enable

Auth Keys

Server Port  (1-65535)

Zone

**Routing**

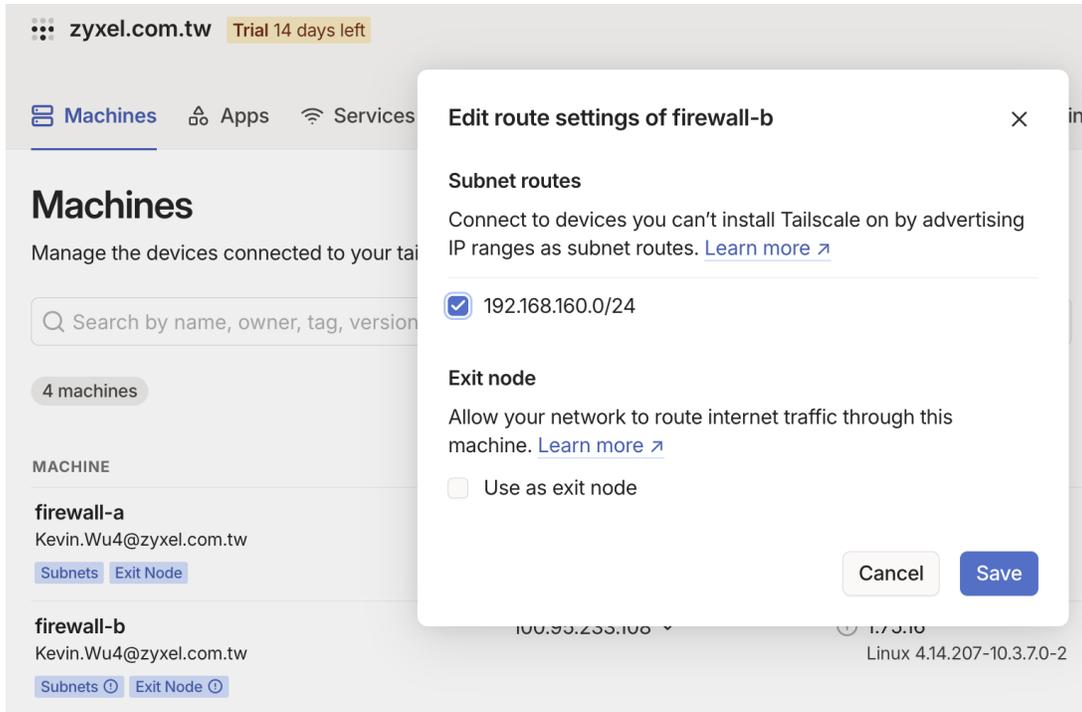
As an Exit Node

**Advertised Networks**

+ Add Remove

Network
<input type="checkbox"/> N_192_168_160

3. Ensure Both subnets have been approved from Tailscale portal.



## Test the Result

Now, Client A know how to route traffic and able to access 192.168.168.1 and 192.168.160.1.

```
C:\Users\NT03234\Downloads>route print | findstr "192.168.168.0 192.168.160.0"
192.168.160.0    255.255.255.0    100.100.100.100    100.95.1.123    0
192.168.168.0    255.255.255.0    100.100.100.100    100.95.1.123    0

C:\Users\NT03234\Downloads>ping -n 2 192.168.168.1

Pinging 192.168.168.1 with 32 bytes of data:
Reply from 192.168.168.1: bytes=32 time=80ms TTL=64
Reply from 192.168.168.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.168.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 80ms, Average = 41ms

C:\Users\NT03234\Downloads>ping -n 2 192.168.160.1

Pinging 192.168.160.1 with 32 bytes of data:
Reply from 192.168.160.1: bytes=32 time=258ms TTL=64
Reply from 192.168.160.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.160.1:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 258ms, Average = 130ms
```

## Case 2: Allow Client A to access internet through Firewall

1. Take Firewall A as example. Enable "Exit Node" and "Default SNAT".

VPN > Tailscale

### General Settings

Zyxel's Tailscale VPN solution is compatible with the Tailscale VPN client, which is built into Windows, macOS, Android, and iOS, and can be managed through the Tailscale Portal.

Enable

Auth Keys

Server Port  (1-65535)

Zone

### Routing

As an Exit Node

### Advised Networks

+ Add Remove

Network
<input type="checkbox"/> N_192_168_168

### Advanced Settings

Accept routes

Default SNAT

2. Ensure the Exit-Node have been enabled from Tailscale portal.

## Edit route settings of firewall-a



### Key expiry is enabled

If this machine's [key expires](#), your relayed traffic may be interrupted until you reauthenticate.

### Subnet routes

Connect to devices you can't install Tailscale on by advertising IP ranges as subnet routes. [Learn more](#) ↗

192.168.168.0/24

### Exit node

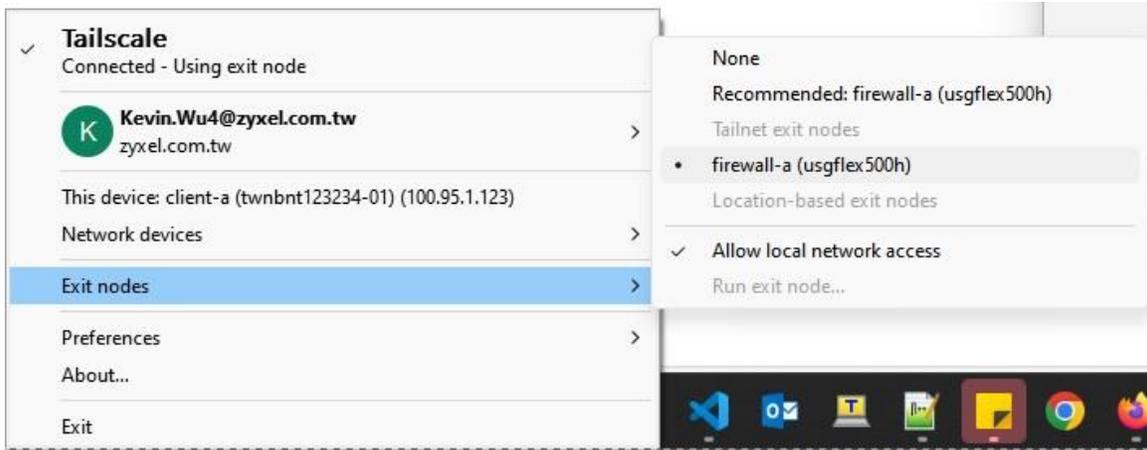
Allow your network to route internet traffic through this machine. [Learn more](#) ↗

Use as exit node

Cancel

Save

3. Client A need to select Firewall A as exit node.



## Test the Result

The internet traffic will send to Firewall A.

```
C:\Users\NT03234>route print | findstr "0.0.0.0"
     0.0.0.0          0.0.0.0          192.168.1.1        192.168.1.40      400
     0.0.0.0          0.0.0.0          100.100.100.100    100.95.1.123      0
    224.0.0.0        240.0.0.0         On-link           127.0.0.1         331
    224.0.0.0        240.0.0.0         On-link           192.168.56.1      281
    224.0.0.0        240.0.0.0         On-link           169.254.122.18    281
    224.0.0.0        240.0.0.0         On-link           192.168.1.40      456

C:\Users\NT03234>tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

  0  2 ms  2 ms  1 ms  100.115.120.97
  1  4 ms  2 ms  2 ms  10.214.48.254
```

**Case3: The devices within the 192.168.168.0/24 and 192.168.160.0/24 subnets can communicate with each other**

Once you completed advertised Networks, you can communicate each other.

## Test the Result

The ping test from Firewall A

```
[kevin@wujiaxuandeMacBook-Air 0219 % ifconfig en5
en5: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
  options=404<VLAN_MTU,CHANNEL_IO>
  ether 20:7b:d2:5f:c9:d5
  inet6 fe80::10:9bda:e5fd:a6c7%en5 prefixlen 64 secured scopeid 0x16
  inet 192.168.168.4 netmask 0xffffffff broadcast 192.168.168.255
  nd6 options=201<PERFORMNUD,DAD>
  media: autoselect (1000baseT <full-duplex>)
  status: active
[kevin@wujiaxuandeMacBook-Air 0219 % ping 192.168.160.33
PING 192.168.160.33 (192.168.160.33): 56 data bytes
64 bytes from 192.168.160.33: icmp_seq=0 ttl=126 time=3.301 ms
64 bytes from 192.168.160.33: icmp_seq=1 ttl=126 time=3.267 ms
--
```

The ping test from Firewall B

```
IPv4 Address. . . . . : 192.168.160.33
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : fe80::daec:e5ff:fe62:a7b9%23
                          192.168.160.1

Wireless LAN adapter Wi-Fi:

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

Ethernet adapter 藍牙網路連線:

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

C:\Users\NT03234\Downloads>ping 192.168.168.4 -n 2

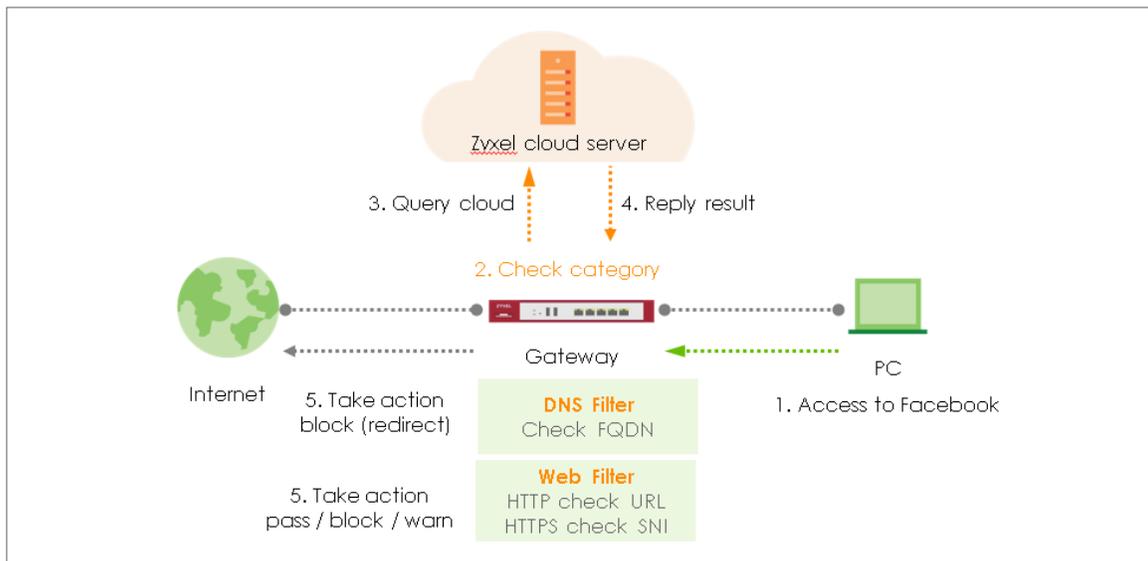
Pinging 192.168.168.4 with 32 bytes of data:
Reply from 192.168.168.4: bytes=32 time=3ms TTL=62
Reply from 192.168.168.4: bytes=32 time=3ms TTL=62

Ping statistics for 192.168.168.4:
    Packets: Sent = 2, Received = 2, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 3ms, Average = 3ms
```

## Chapter 2- Security Service

### How to Block HTTPS Websites Using Content Filtering and SSL Inspection

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



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

## Set Up Content Filter

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

Profile Management

+ Add Edit Remove Reference

Search insights

<input type="checkbox"/>	Name	Description	Reference
<input type="checkbox"/>	BPP		0
<input type="checkbox"/>	CIP		0

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

General Settings

Name: Block\_Youtube

Description:

Action: block

Log: log

Log allowed traffic:

SSL V3 or previous version Connection Drop:

Drop Log: no

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

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

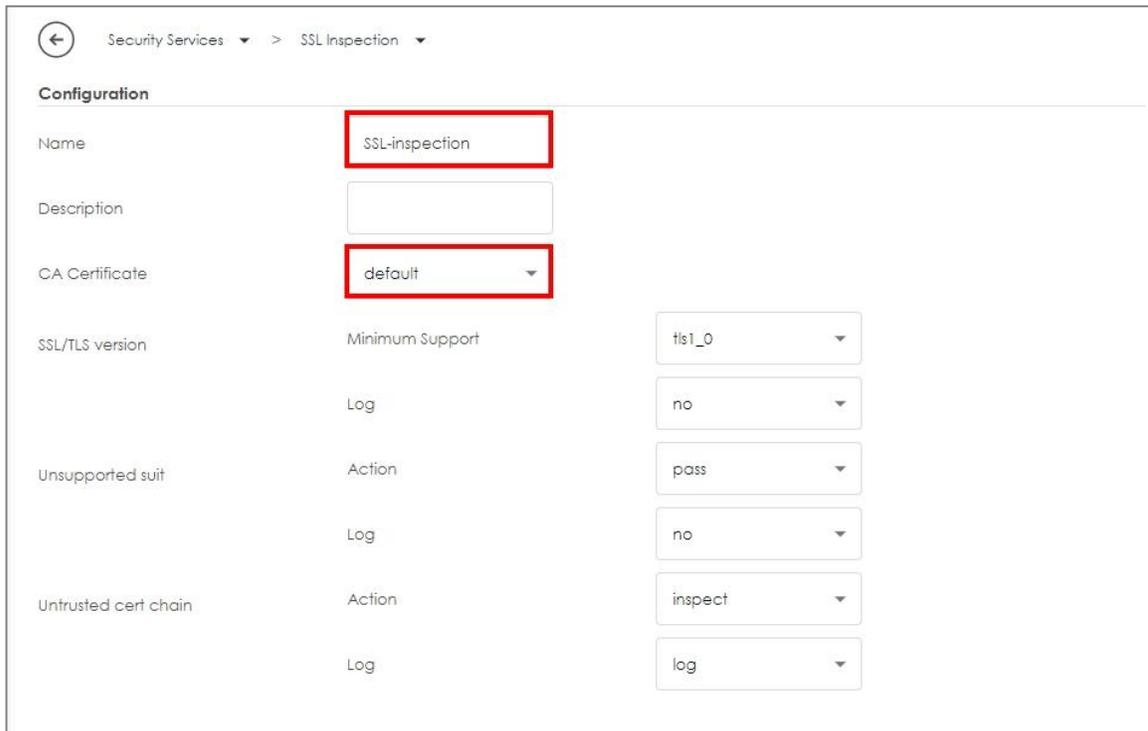
Some changes were made  
What do you want to do then?  
Reset Apply

## Set Up SSL Inspection

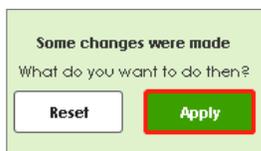
In the FLEX, go to Security Service > SSL inspection > profile > Profile Management, and click Add to create profile



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



Click Apply to add SSL Inspection profile.



## Set Up the Security Policy

Go to Security Policy > Policy control. Edit LAN\_Outgoing, and scroll down to profile section.

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

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

## Export Certificate from FLEX and Import it to Windows

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

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

System > Certificate > My Certificates

**My Certificates** Trusted Certificates

PKI Storage Space

Usage 0%

+ Add Edit Remove Reference Import **Export** Search insights

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

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

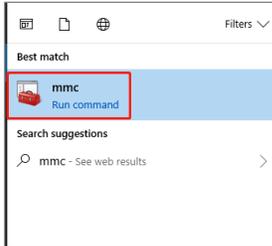
**Export Certificate** [X]

Password

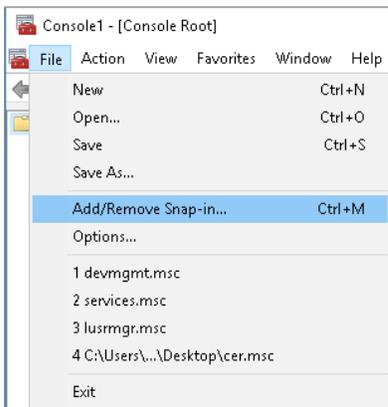
Leave the password field blank to export certificate only or fill in password to export certificate with private key.

**Export Certificate**

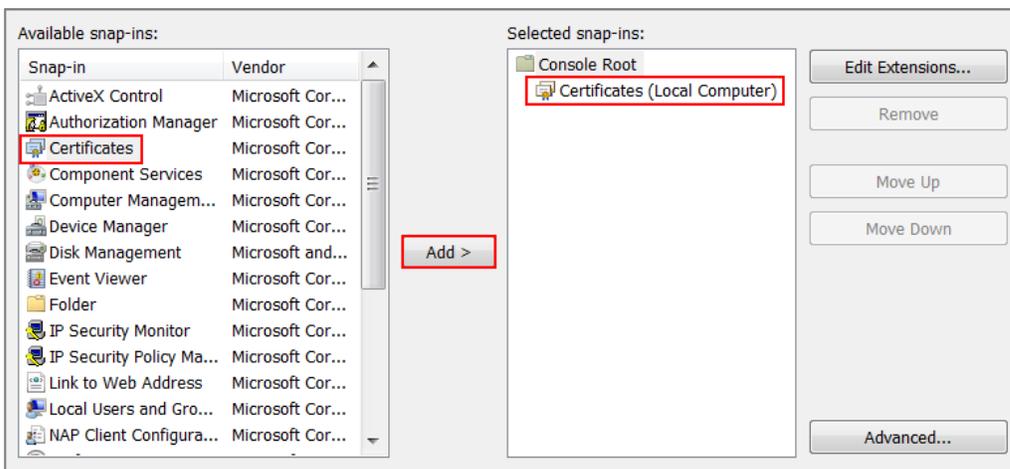
In Windows Start Menu > Search Box, type MMC and press Enter.



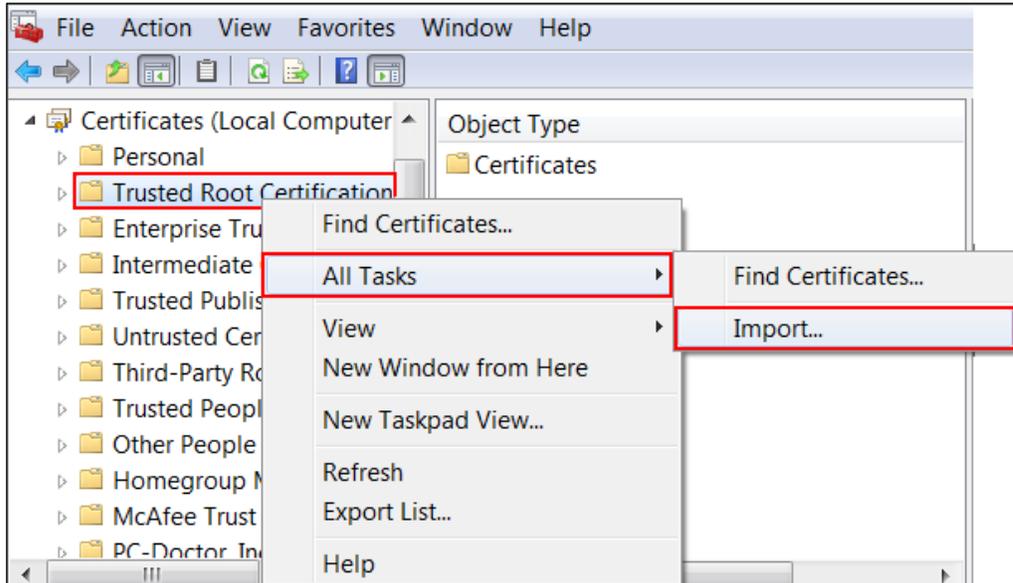
In the mmc console window, click File > Add/Remove Snap-in...



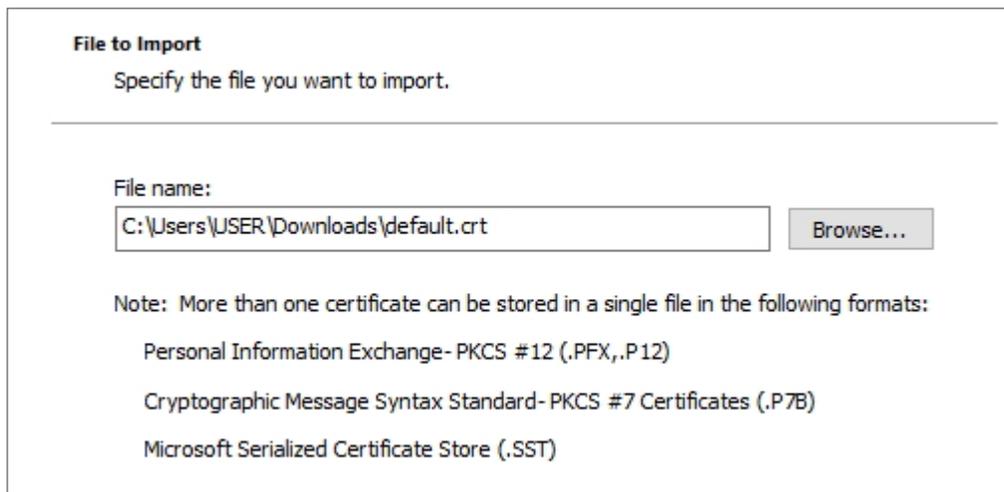
In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.



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 Import Wizard

**Certificate Store**  
Certificate stores are system areas where certificates are kept.

---

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

Automatically select the certificate store based on the type of certificate

Place all certificates in the following store:

Certificate store:  
Trusted Root Certification Authorities

## Test the Result

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

**Content Filtering**

## Access Restricted

**Web access is restricted. Please contact the administrator.**

Category        Block Web Sites

Blocked URL    <https://www.youtube.com.tw/>



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

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

Rows per page: 50    1-6 of 6

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

Security Statistics > SSL Inspection > Summary

**Summary** Certificate Cache List

**General Settings**

Refresh Flush Data

**Status**

Maximum Concurrent Sessions **1000**

Concurrent Sessions **238**

**Summary**

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

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

Security Statistics > Content Filter

Last 24 Hours Summary

Click the pie chart to switch to the item events

Top entry by Blocked Category

Refresh Flush Data

Blocked Category	Hit Count
Streaming Media	<b>18 (100%)</b>

**Content Filter Events**

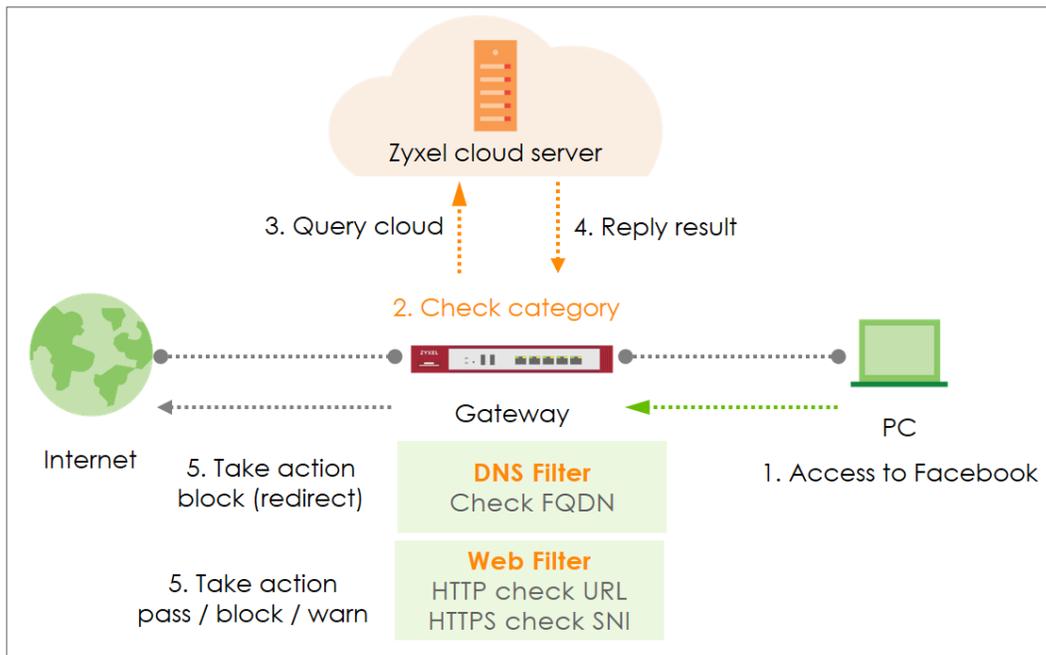
Search insights

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

## How to Configure Content Filter with HTTPs Domain Filter

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

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



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

## Set Up the Content Filter

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

The screenshot shows the configuration page for a Content Filter profile. The breadcrumb navigation is "Security Service > Content Filtering". The "General Settings" section includes the following fields:

- Name: Social\_Networking
- Description: (empty)
- Action: block (highlighted with a red box)
- Log: log alert
- Log allowed traffic:
- SSL V3 or previous version Connection Drop:
- Drop Log: log alert

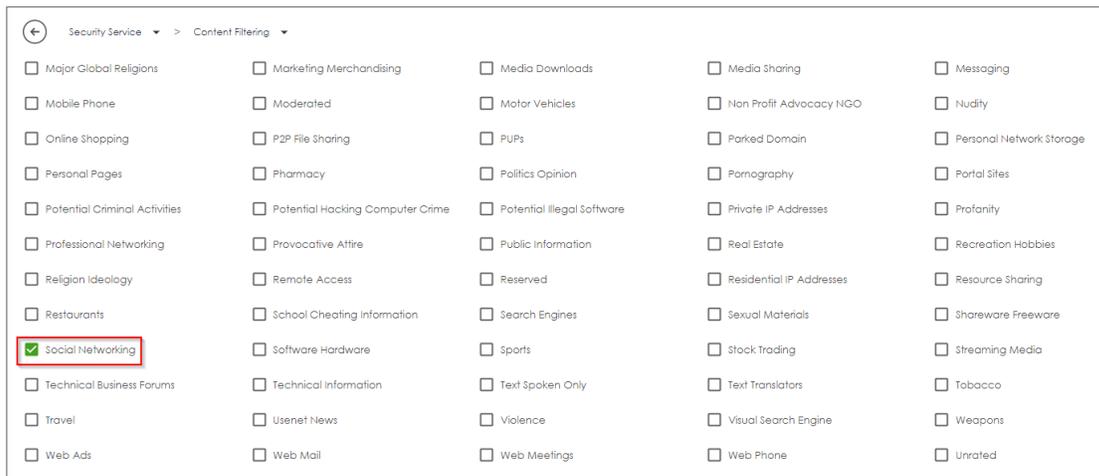
Navigate to **Test Web Site Category** and type URL to test the category and click **Query**.

The screenshot shows the "Test Web Site Category" form. The "URL to test" field contains "https://www.facebook.com". The "Query" button is highlighted with a red box. Below the form, there is a green link: "If you think the category is incorrect, click this link to submit a request to review it."

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



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



## Set Up the Security Policy

Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies and apply the **Profile > Content Filter** "Social\_Networking" on this security policy.

The screenshot displays the configuration page for a Security Policy. The breadcrumb navigation shows 'Security Policy > Policy Control'. The page is divided into two main sections: 'Configuration' and 'Profile'.

**Configuration Section:**

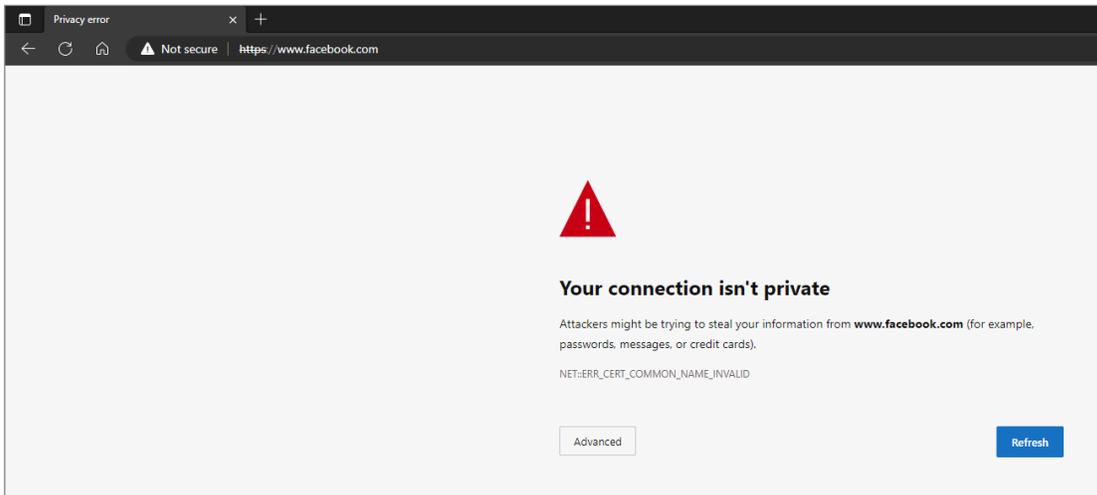
- Enable:** A green toggle switch is turned on.
- Name:** A text input field contains 'Block\_Social\_Networking'.
- Description:** An empty text input field.
- From:** A dropdown menu is set to 'LAN'.
- To:** A dropdown menu is set to 'WAN'.
- Source:** A dropdown menu is set to 'any'.
- Destination:** A dropdown menu is set to 'any'.
- Service:** A dropdown menu is set to 'any'.
- User:** A dropdown menu is set to 'any'.
- Schedule:** A dropdown menu is set to 'none'.
- Action:** A dropdown menu is set to 'allow'.
- Log:** A dropdown menu is set to 'no'.

**Profile Section:**

- Application Patrol:** A dropdown menu is set to 'none'. To its right is a 'Log' checkbox and a dropdown menu set to 'by profile'.
- Content Filter:** A dropdown menu is set to 'Social\_Networking'. To its right is a 'Log' checkbox and a dropdown menu set to 'by profile'.
- SSL Inspection:** A dropdown menu is set to 'none'. To its right is a 'Log' checkbox and a dropdown menu set to 'by profile'.

## Test Result

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

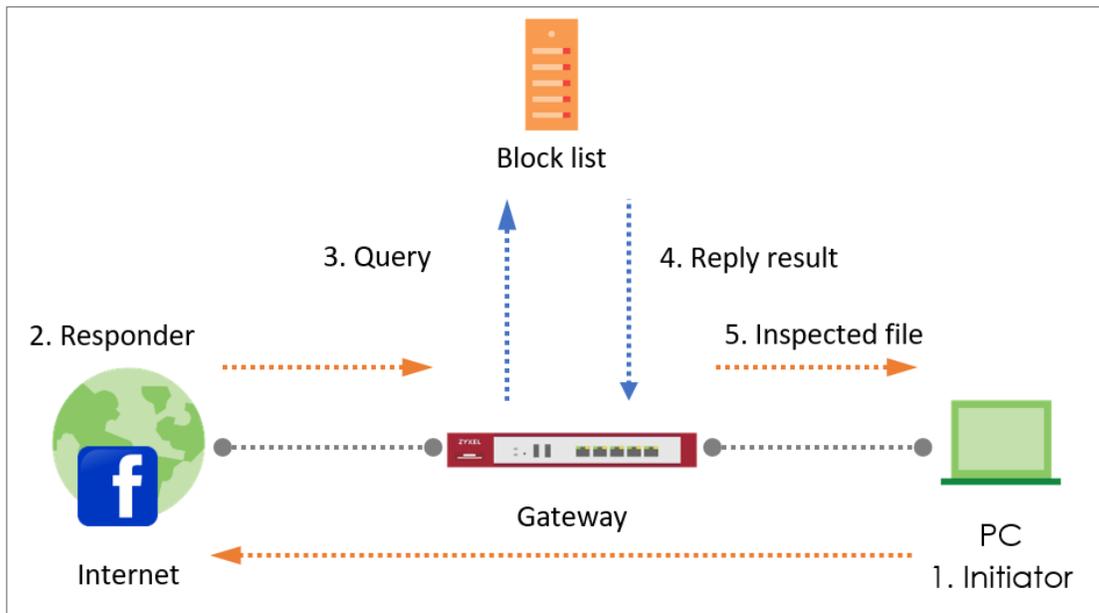


Navigate to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

Log & Report	Log / Events
25	2023-05-22 14:46:31 content-filter www.facebook.com: Social Networking; rule_name: Block_Social_Networking 10.214.40.67 172.21.5.1 DNS REDIRECT
25	2023-05-22 14:46:31 content-filter www.facebook.com: Social Networking; rule_name: Block_Social_Networking 192.168.168.33 192.168.168.1 DNS REDIRECT

## How to Block Facebook Using a Content Filter Block List

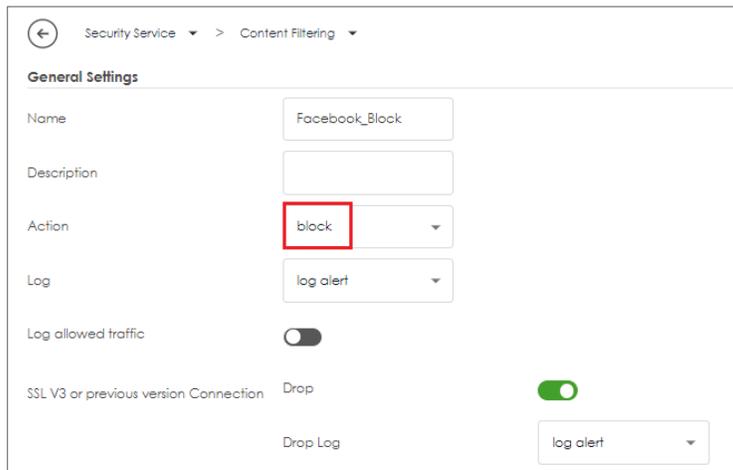
This is an example of using USG Flex H UTM Profile in a Security Policy to block access to a specific social network service. You can use Content Filter and Policy Control to make sure that a certain web page cannot be accessed through both HTTP and HTTPS protocols.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

## Set Up the Content Filter

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



The screenshot shows the configuration page for a Content Filter profile. The breadcrumb navigation is "Security Service > Content Filtering". Under "General Settings", the "Name" field contains "Facebook\_Block". The "Action" dropdown menu is set to "block" and is highlighted with a red box. The "Log" dropdown menu is set to "log alert". The "Log allowed traffic" toggle is turned off. The "SSL V3 or previous version Connection" section has a "Drop" toggle turned on and a "Drop Log" dropdown set to "log alert".

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



The screenshot shows the "Block list" configuration page. The "Log" dropdown is set to "log alert". Below the navigation buttons (+ Add, Edit, Remove), there is a table with one entry. The entry has a checkbox, the name "\*.facebook\*.com" (highlighted with a red box), and a status icon (a green checkmark in a box, also highlighted with a red box). The footer shows "Rows per page: 50" and "1 of 1".

## 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.

The screenshot displays the configuration interface for a Security Policy. The breadcrumb navigation shows 'Security Policy > Policy Control'. The 'Configuration' section includes the following fields:

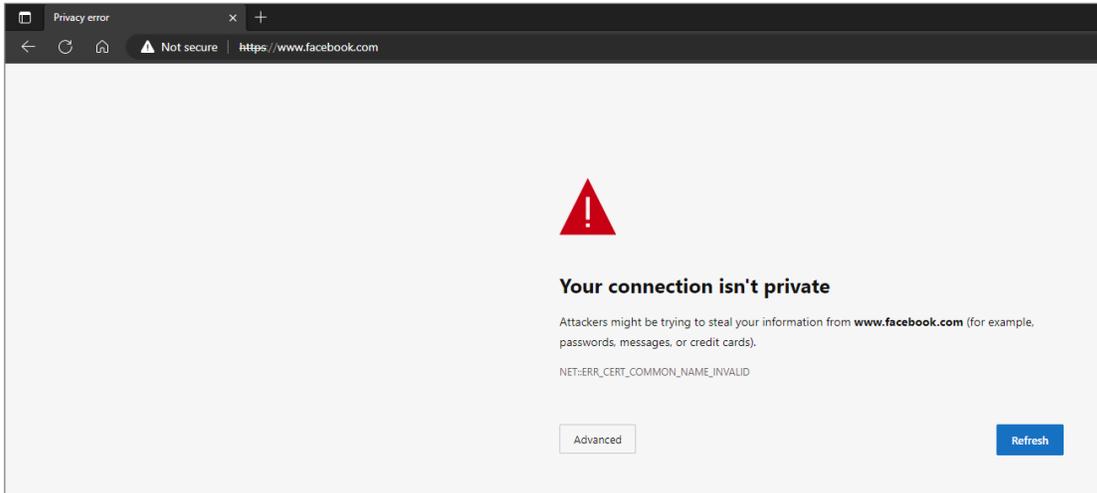
- Enable:** A toggle switch is turned on.
- Name:** A text input field containing 'Facebook\_Block'.
- Description:** An empty text input field.
- From:** A dropdown menu with 'LAN' selected.
- To:** A dropdown menu with 'any (Excluding ZyWALL)' selected.
- Source:** A dropdown menu with 'any' selected.
- Destination:** A dropdown menu with 'any' selected.
- Service:** A dropdown menu with 'any' selected.
- User:** A dropdown menu with 'any' selected.
- Schedule:** A dropdown menu with 'none' selected.
- Action:** A dropdown menu with 'allow' selected.
- Log:** A dropdown menu with 'no' selected.

The 'Profile' section includes the following fields:

- Application Patrol:** A dropdown menu with 'none' selected, with a 'Log' checkbox and a 'by profile' dropdown.
- Content Filter:** A dropdown menu with 'Facebook\_Block' selected, with a 'Log' checkbox and a 'by profile' dropdown.
- SSL Inspection:** A dropdown menu with 'none' selected, with a 'Log' checkbox and a 'by profile' dropdown.

## Test the Result

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

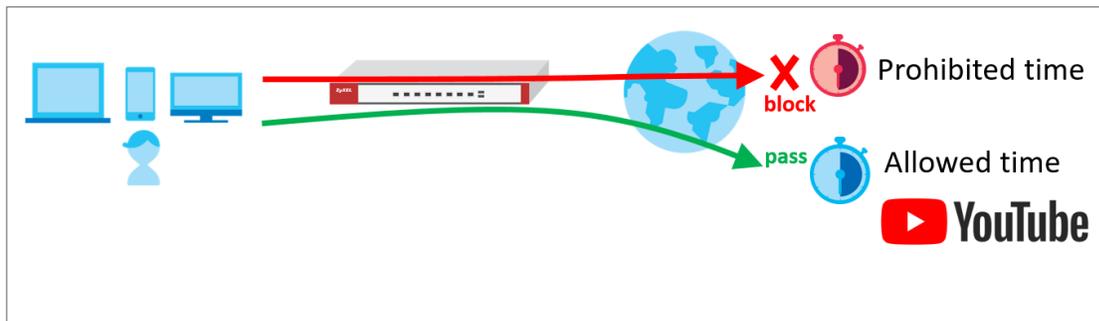


Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.

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

## How to block YouTube access by Schedule

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



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).

## Set Up the Schedule

Go to **Object > Schedule > Recurring > Add Schedule Recurring Rule**. Configure a **Name** for you to identify the **Schedule Recurring Rule**. Specify the **Day Time** hour and minute when the schedule begins and ends each day.

← 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**.

The screenshot shows the 'Add Application' dialog box with the following configuration:

- Category and Application:** Search term: youtube
- Results:**
  - Audio/Video (1/205):
    - YouTube TV
  - Web (6/2568):
    - Youtube.com
    - youtube Audio/Video
    - youtube Upload
    - Youtube HD
    - YouTube Kids
    - Youtube Music
- Log:** Log Alert
- Action:** Reject
- Buttons:** Cancel, Add

## Set Up the Security Policy

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

← Object ▾ > Service ▾

---

**Configuration**

Name	<input type="text" value="QUIC_UDP_443"/>
Description	<input type="text"/>
IP Protocol	<input type="text" value="UDP"/> ▾
Starting Port	<input type="text" value="443"/> (1..65535)
Ending Port	<input type="text" value="443"/> (1..65535)

Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies. Select the **service** QUIC\_UDP443 and select the **Schedule** that defines when the policy would be applied.

In this example, select "Youtube\_Blocked\_Time".

← Security Policy > Policy Control

**Configuration**

Enable	<input checked="" type="checkbox"/>
Name	Block_QUIC_UDP443
Description	<input type="text"/>
From	LAN
To	WAN
Source	LAN1_SUBNET
Destination	any
Service	QUIC_UDP_443
User	any
Schedule	Youtube_Block_Time
Action	deny ▼
Log	log alert ▼

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

← Security Policy > Policy Control

### Configuration

Enable

Name Block\_Youtube

Description

From LAN

To WAN

Source LAN1\_SUBNET

Destination any

Service any

User any

Schedule Youtube\_Block\_Time

Action allow ▼

Log log alert ▼

### Profile

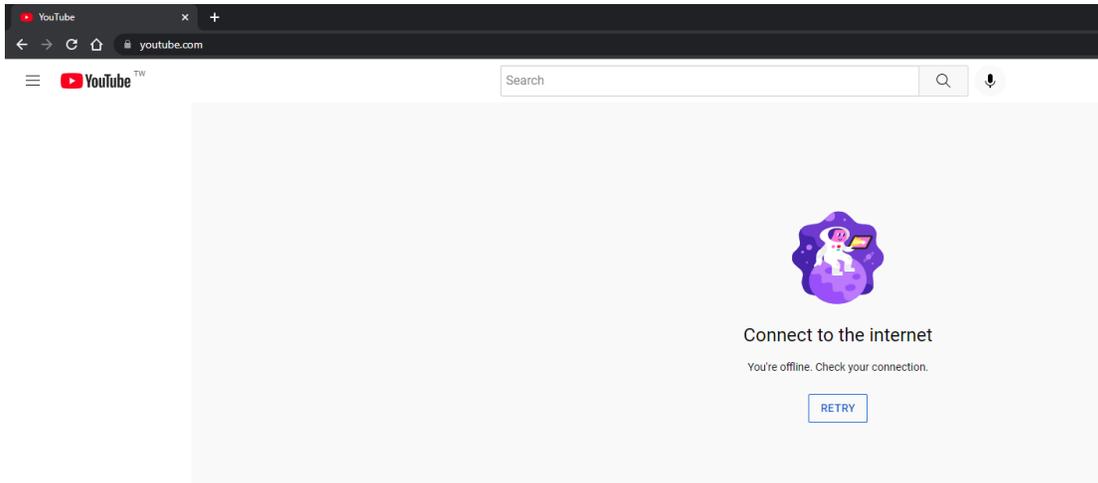
Application Patrol	Youtube ▼	Log	by profile ▼
Content Filter	none ▼	Log	by profile ▼
SSL Inspection	none ▼	Log	by profile ▼

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

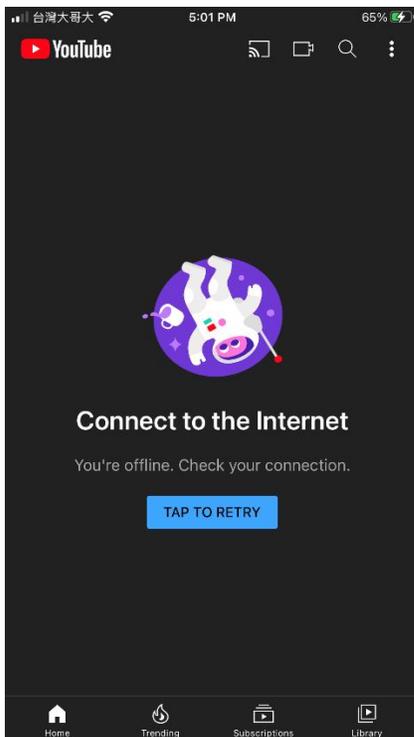
<input type="checkbox"/>	Status	Priority	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log	Profile
<input type="checkbox"/>	🟢	1	Block_QUIC_UDP...	LAN	WAN	LAN1_SUBNET	any	QUIC_UDP_443	any	Youtube_Block_T...	deny	log-alert	
<input type="checkbox"/>	🟢	2	Block_YouTube	LAN	WAN	LAN1_SUBNET	any	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.



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

#	Time	Category	Message	Source	Destination	Note
3	2023-05-21 21:35:26	app-patrol	Rule_name@lock_Youtube App(Web)youtube SID:1572640	192.168.168.33	172.217.160.110	ACCESS REJECT
5	2023-05-21 21:35:26	app-patrol	Rule_name@lock_Youtube App(Web)youtube SID:1572640	192.168.168.33	172.217.160.110	ACCESS REJECT
18	2023-05-21 21:35:16	app-patrol	Rule_name@lock_Youtube App(Web)youtube SID:1572640	192.168.168.33	172.217.163.46	ACCESS REJECT
20	2023-05-21 21:35:16	app-patrol	Rule_name@lock_Youtube App(Web)youtube SID:1572640	192.168.168.33	172.217.163.46	ACCESS REJECT
25	2023-05-21 21:35:10	app-patrol	Rule_name@lock_Youtube App(Web)youtube SID:1572640	192.168.168.33	142.251.43.14	ACCESS REJECT
27	2023-05-21 21:35:10	app-patrol	Rule_name@lock_Youtube App(Web)youtube SID:1572640	192.168.168.33	142.251.43.14	ACCESS REJECT
30	2023-05-21 21:35:04	app-patrol	Rule_name@lock_Youtube App(Web)youtube SID:1572640	192.168.168.33	172.217.163.46	ACCESS REJECT
34	2023-05-21 21:35:01	app-patrol	Rule_name@lock_Youtube App(Web)youtube SID:1572640	192.168.168.33	172.217.163.46	ACCESS REJECT
38	2023-05-21 21:34:54	app-patrol	Rule_name@lock_Youtube App(Web)youtube SID:1572640	192.168.168.33	172.217.160.110	ACCESS REJECT

## How to Control Access to Google Drive

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



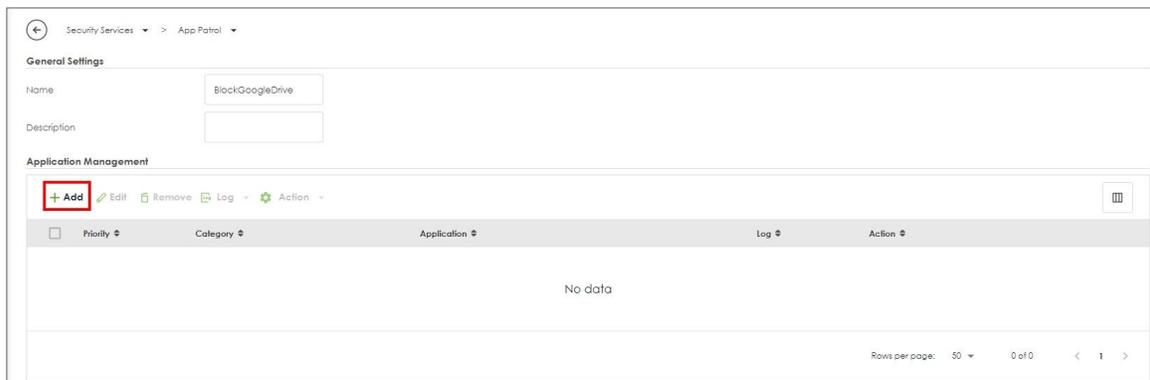
 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

## Create app patrol profile

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



Click add to add application in this profile.



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

Action set to Drop, and click Add.

The screenshot shows a dialog box titled "Add Application". On the left, there are labels for "Category and Application", "Log", and "Action". The "Category and Application" section has a search bar containing "Google document" and a list of results. The first result is "Web (1/2687)" and the second is "Google Documents (aka Google Drive)", which is highlighted with a red box. Below the list are two dropdown menus: "Log" and "Action" (set to "Drop"). At the bottom right, there are "Cancel" and "Add" buttons, with the "Add" button highlighted in red.

## 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

The screenshot shows the "Profile Management" interface. At the top, there are buttons for "+ Add", "Edit", "Remove", and "Reference". The "+ Add" button is highlighted with a red box. To the right, there is a search bar labeled "Search insights" and a trash icon. Below the buttons is a table with the following columns: "Name", "Description", "CA Certificate", and "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.

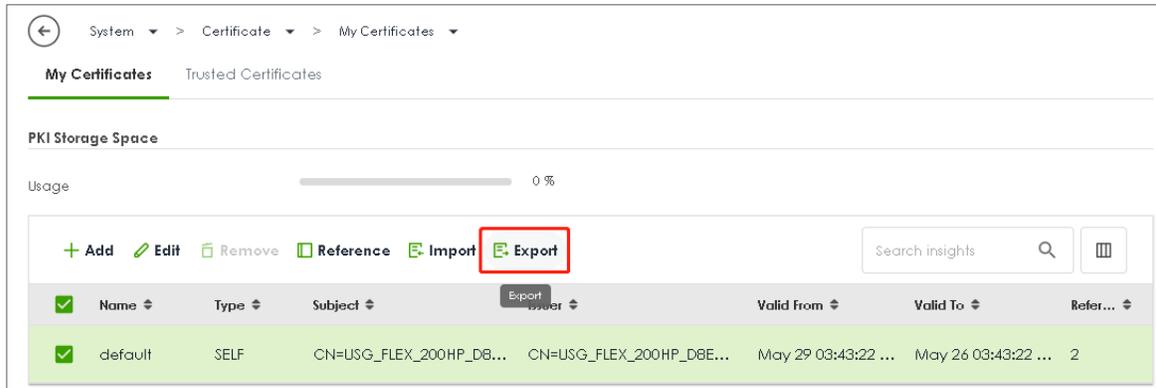
**Profile**

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

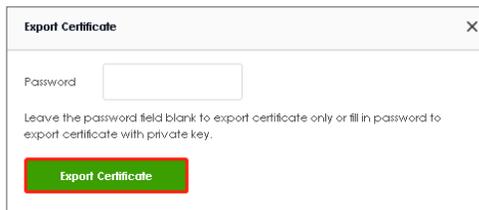
## Export Certificate from FLEX and import to Lan hosts

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.

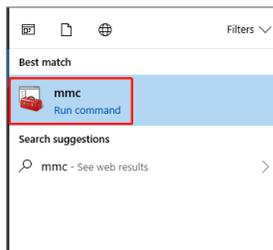
Go to System > Certificate > My Certificates to export default certificate from FLEX.



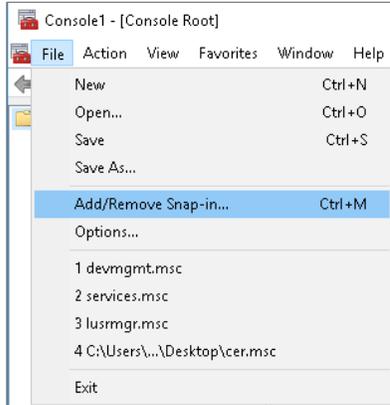
Click Export Certificate to export certificate file, and Save default certificate as default.crt file to Windows OS.



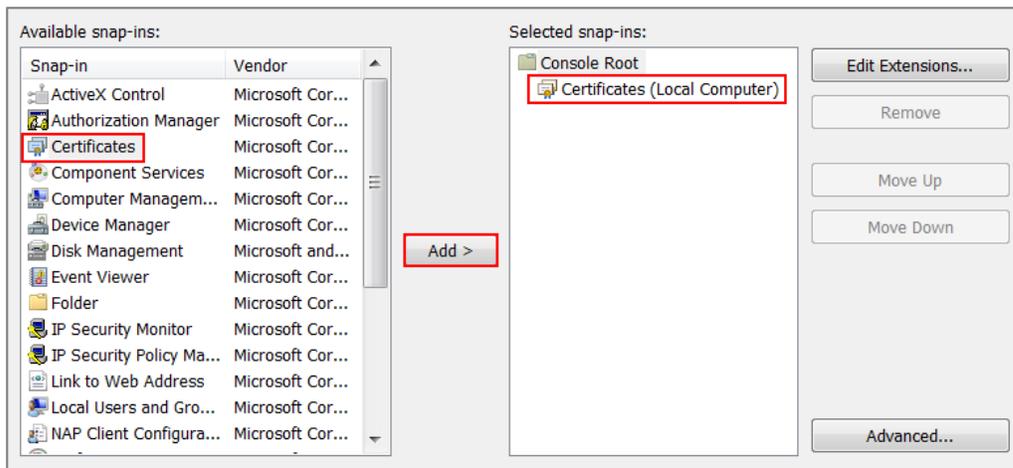
In Windows Start Menu > Search Box, type MMC and press Enter.



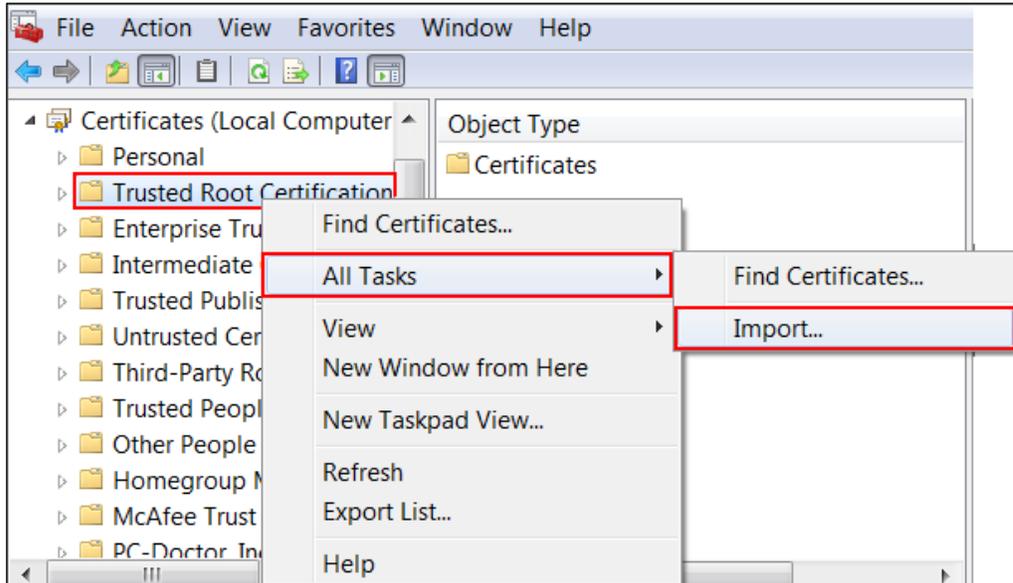
In the mmc console window, click File > Add/Remove Snap-in...



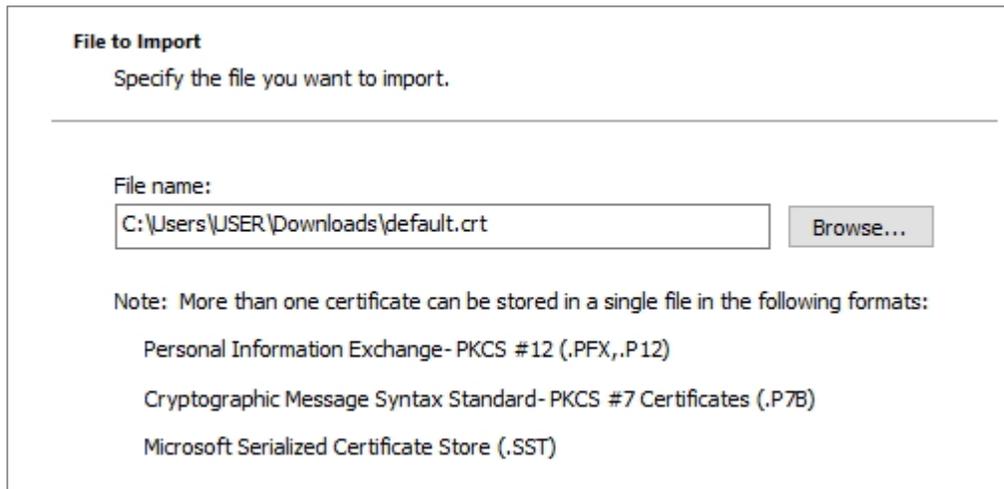
In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.



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.



## Test the Result

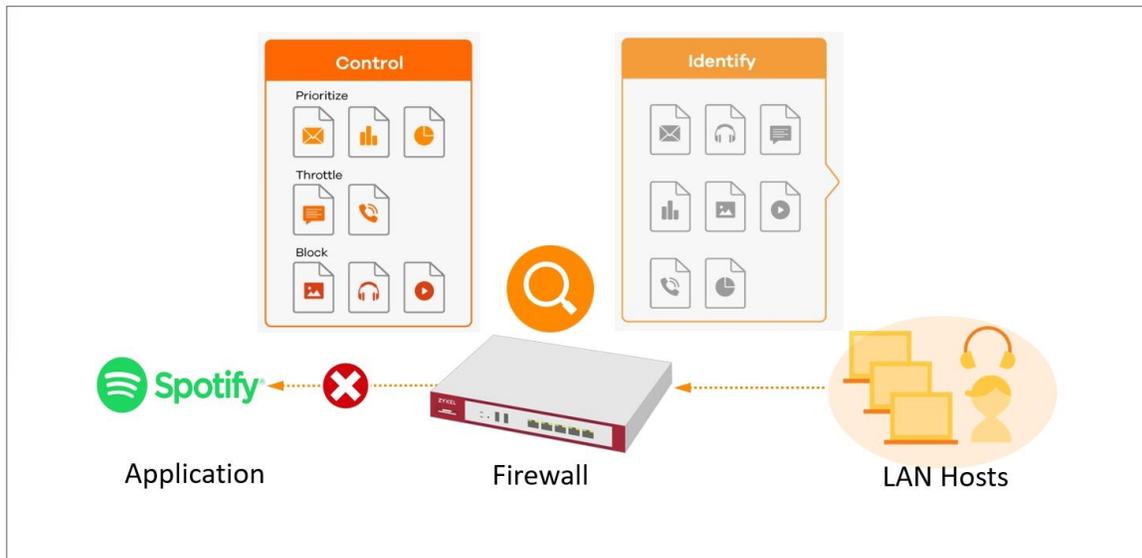
Access to Google drive from Lan host to verify if it is blocked by firewall Application patrol.

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.



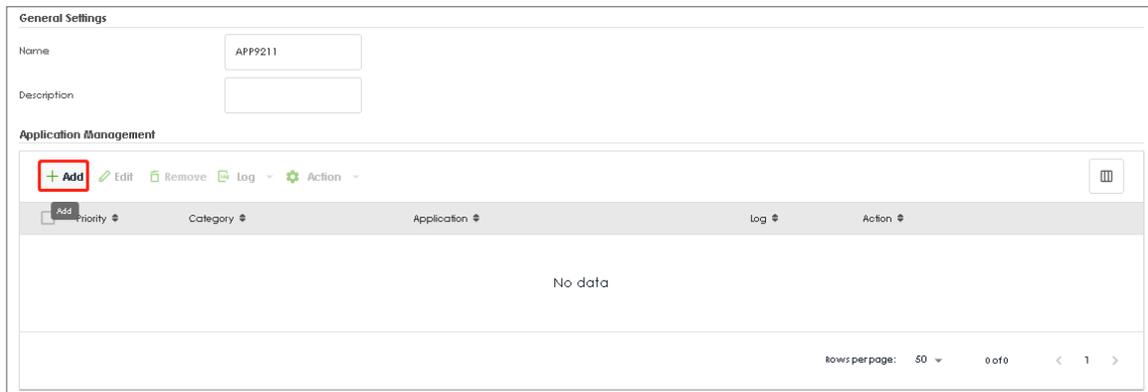
 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

## Create a App Patrol profile

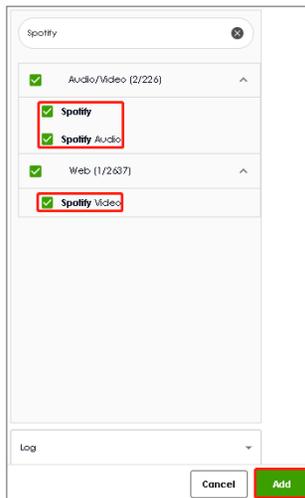
Go to Security Service > App patrol > Profile management, and click Add to create profile.



Click add to add application in this profile.



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



## Apply profile to security policy

Go to Security Policy > Policy control. Edit LAN\_Outgoing, and scroll down to profile section.

Apply Application Patrol profile to Security policy.

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

## Test the Result

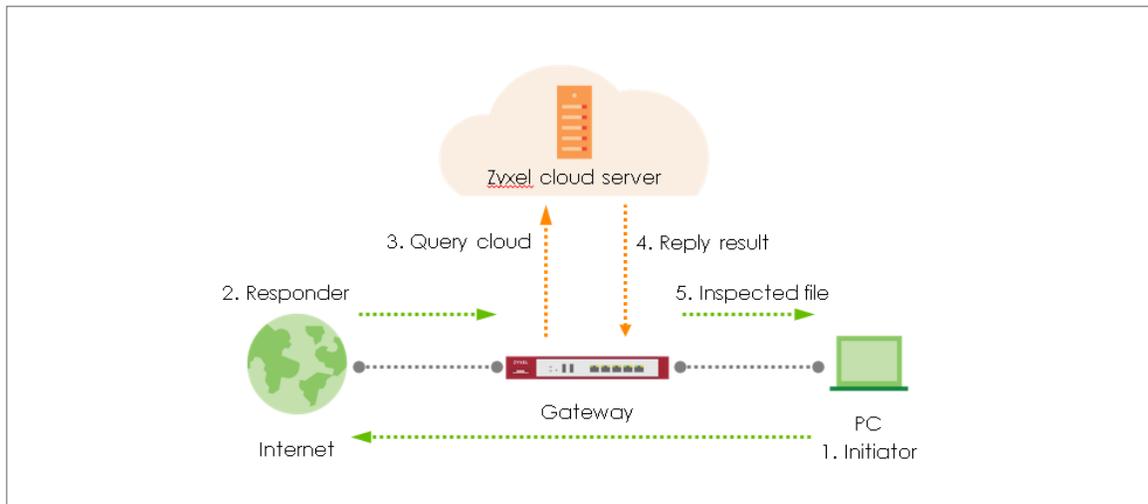
Access to Spotify from Lan host to verify if it is blocked by firewall Application patrol.

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

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

## How does Anti-Malware Work

There are many viruses exist on the internet. And it may auto-downloaded on unexpected situation when you surfing between websites. The Anti-Malware is a good choose to protecting your computer to downloads unsafe application or files.



## Enable Anti-Malware function to protecting your traffic

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

Security Service > Anti-Malware > Anti-Malware

### Anti-Malware

#### General Settings

Enable Anti-Malware	<input checked="" type="checkbox"/>
Collect Statistics	<input checked="" type="checkbox"/>
Scan and detect EICAR test virus	<input checked="" type="checkbox"/>
File size limit	<input type="text" value="10"/> (MB)

Select Destroy infected file and log in Actions When Matched

### Actions When Matched

Destroy infected file	<input checked="" type="checkbox"/>
Log	<input type="text" value="log"/>

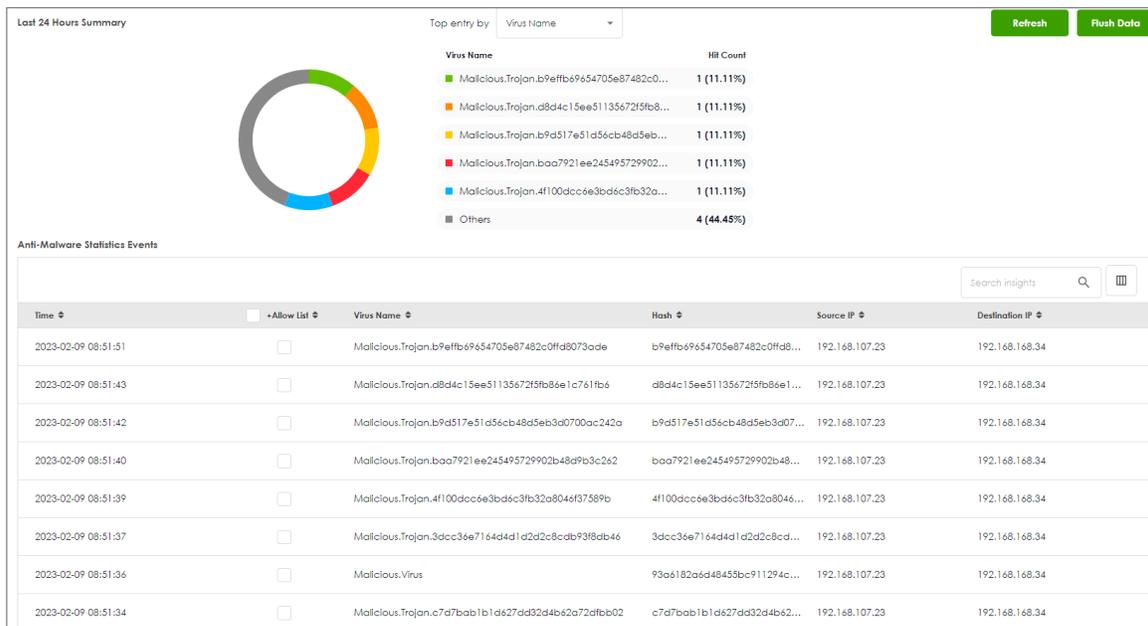
## Test the Result

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

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

#	Time	Category	Message	Source	Destination	Note
1	2023-03-14 09:31:17	anti-malware	Virus infected SSI:N Type:Cloud Query Virus:Malicious.Trojan.44d88612fea8af36de82e1278abb02f File:elcar.com.txt Protocol:HTTP md5:44d88612fea8af36de82e1278abb02f	89.238.73.97	192.168.168.36	FILE DESTROY

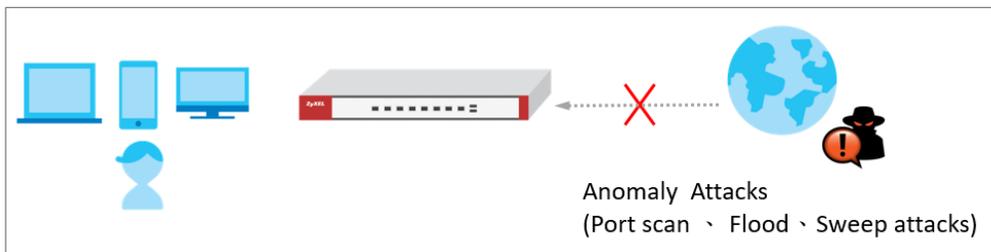
Go to Security Statistics > Anti-Malware to check summary of all events.



## 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
<input type="checkbox"/> Active	(partscan) IP Protocol Scan	log	block
<input type="checkbox"/> Active	(partscan) TCP Partscan	log	block
<input type="checkbox"/> Active	(partscan) UDP Partscan	log	block
<input type="checkbox"/> Active	(Sweep) ICMP Sweep	log	block
<input type="checkbox"/> Active	(Sweep) IP Protocol Sweep	log	block
<input type="checkbox"/> Active	(Sweep) TCP Sweep	log	block
<input type="checkbox"/> Active	(Sweep) UDP Sweep	log	block

**Flood Detection**

Block Period: 5 (1-3600 seconds)

Edit Active Inactive Log Action

Status	Name	Log	Action	Threshold
<input type="checkbox"/> Active	(flood) ICMP Flood	log	block	1000
<input type="checkbox"/> Active	(flood) IP Flood	log	block	1000
<input type="checkbox"/> Active	(flood) TCP Flood	log	block	1000
<input type="checkbox"/> Active	(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.

The screenshot shows the configuration page for a DoS Prevention Policy. Under 'General Settings', the 'Enable DoS Prevention' toggle is turned on. The 'Policies' section contains a table with the following data:

	Status	Priority	Name	From	Anomaly Profile
<input type="checkbox"/>	🔒	1	DoS_Prevention	WAN	DoS_Prevention

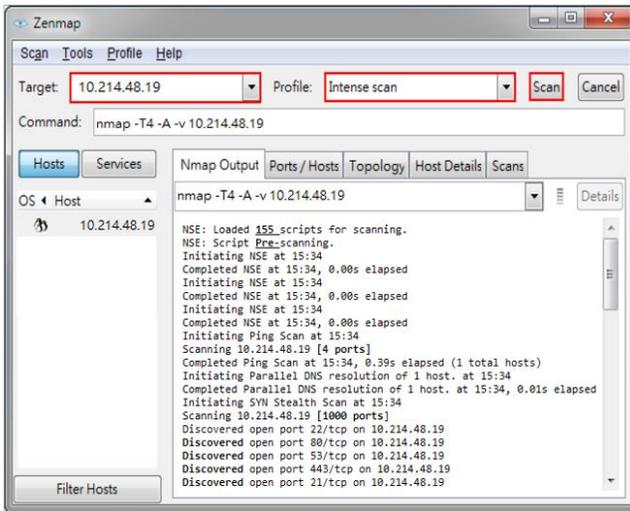
|

## 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.



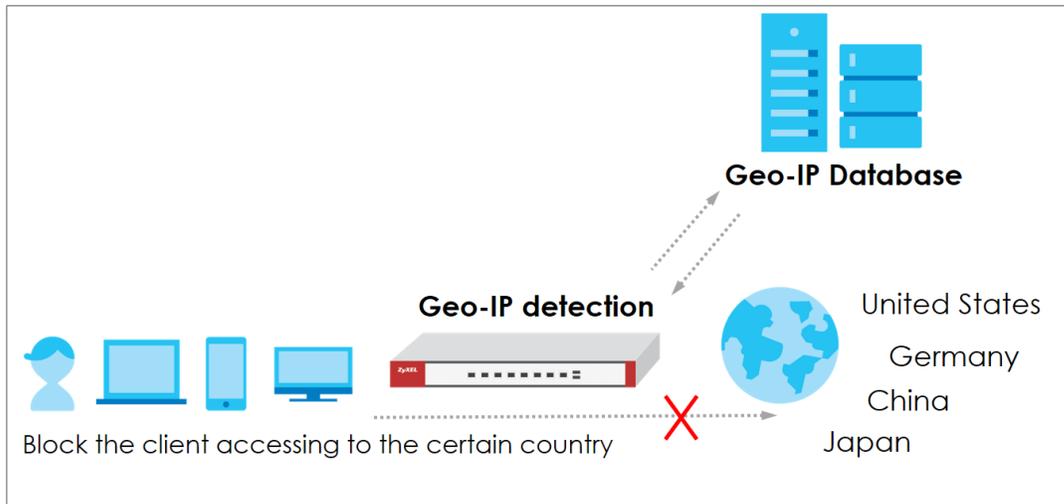
Navigate to **Log & Report > Log / Events**, you will see log of blocked messages.

#	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.**

The screenshot shows the configuration page for a Geo IP object. At the top, there is a breadcrumb navigation: Object > Address. Below this is a 'Configuration' section with the following fields:

- Name: geo\_ip
- Description: (empty)
- Address Type: GEOGRAPHY (highlighted with a red box)
- Region: China (highlighted with a red box)

The screenshot shows the configuration page for a second Geo IP object. At the top, there is a breadcrumb navigation: Object > Address. Below this is a 'Configuration' section with the following fields:

- Name: geo\_ip\_2
- Description: (empty)
- Address Type: GEOGRAPHY (highlighted with a red box)
- Region: Germany (highlighted with a red box)

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	10.0.0/8	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

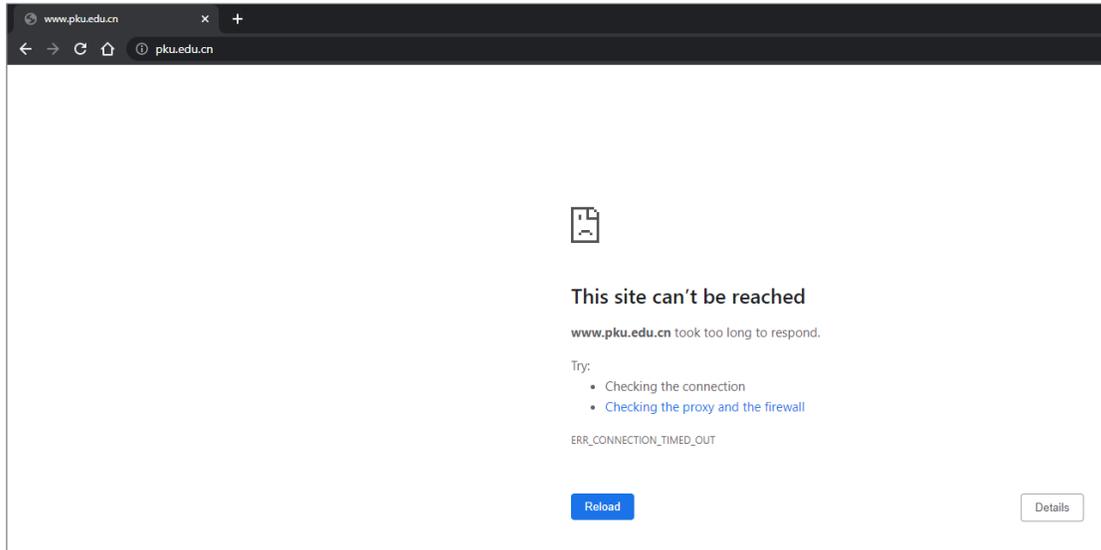
Schedule: none

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.

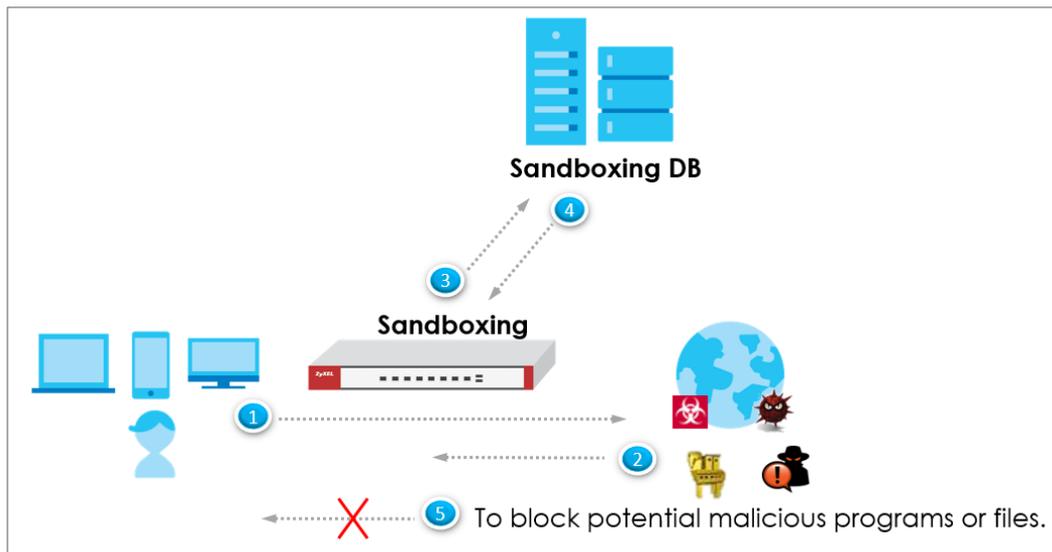


To view the log message, go to USG Flex H **Log & Report > Log / Events**. You will find log messages similar to the following. Any traffic that matches the Geo IP policy will be blocked, and the details will be displayed in the Message field.

#	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?

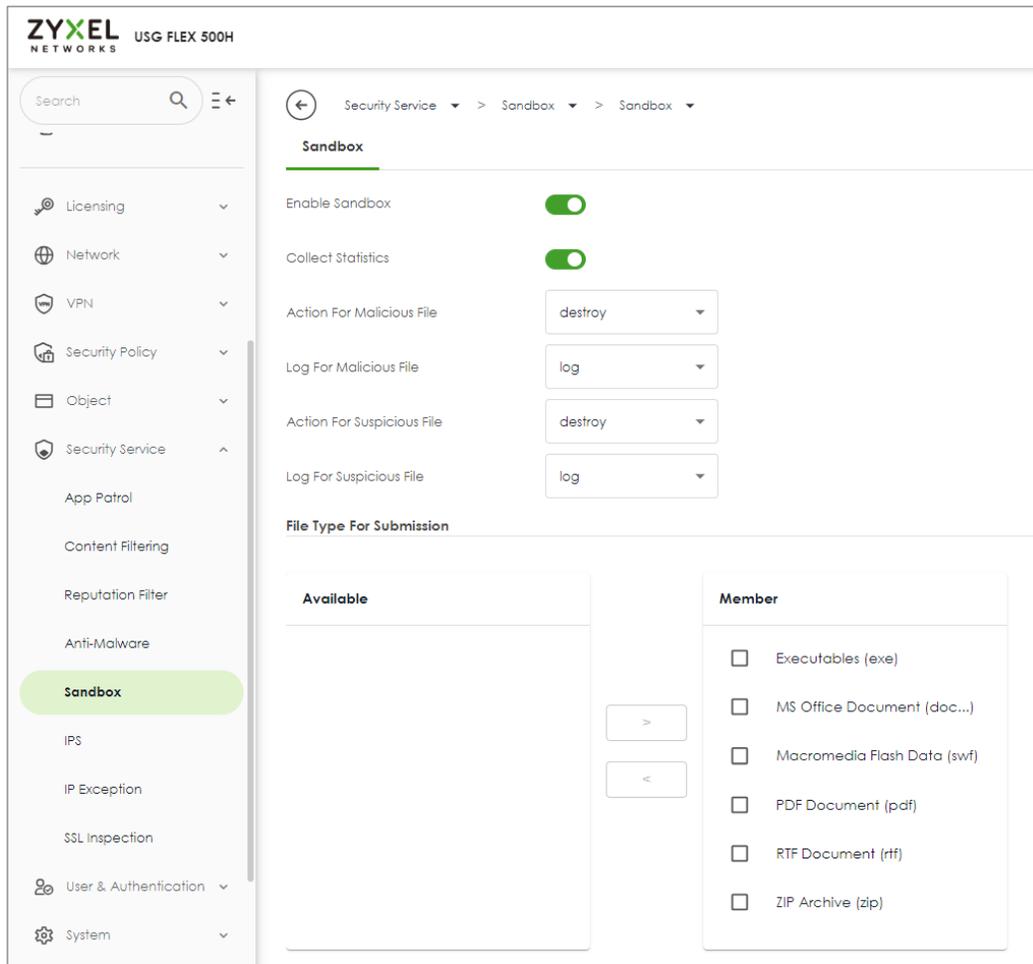
This is an example of using the USG Flex H to employ Sandboxing for detecting unknown malware. To achieve this goal, you can configure the Sandboxing profile within the security service path, and this article will guide you on its deployment.



 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).



## 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.

The screenshot shows the 'Log / Events' page in the ZyXel management interface. The 'Category' is set to 'Sandbox'. The log entry details are as follows:

#	Time	Category	Message	Source	Destination	Note
2	2023-07-31 16:18:14	Sandbox	Query File name: wildfire-test-pe-file.exe, md5: a2b6588b529a0c5a7e164b70114b4a57, 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
<b>IP Blocking</b>		
Enable	<input checked="" type="checkbox"/>	
Action	block	
Threat Level Threshold	high	
Log	log	
Statistics	<input checked="" type="checkbox"/>	

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		
<input checked="" type="checkbox"/> Anonymous Proxies	<input checked="" type="checkbox"/> Denial of Service	<input checked="" type="checkbox"/> Exploits
<input checked="" type="checkbox"/> Negative Reputation	<input checked="" type="checkbox"/> Scanners	<input checked="" type="checkbox"/> Spam Sources
<input checked="" type="checkbox"/> TOR Proxies	<input checked="" type="checkbox"/> Web Attacks	<input checked="" type="checkbox"/> Phishing
Types of Cyber Threats Coming From The Internet And Local Networks		
<input checked="" type="checkbox"/> Botnets		

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

The screenshot displays the 'IP Reputation' configuration page, which is divided into two main sections: 'Allow List' and 'Block List'. Both sections have an 'Enable' toggle set to 'on' and a 'Log' dropdown menu. The 'Allow List' section is currently empty, showing 'No data'. The 'Block List' section contains one entry with the IP address '107.155.48.246', which is highlighted with a red box. The interface includes various action buttons like '+ Add', 'Edit', 'Remove', 'Active', and 'Inactive' for each list.

Status	IPv4 Address
<input type="checkbox"/>	
<input type="checkbox"/>	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

**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

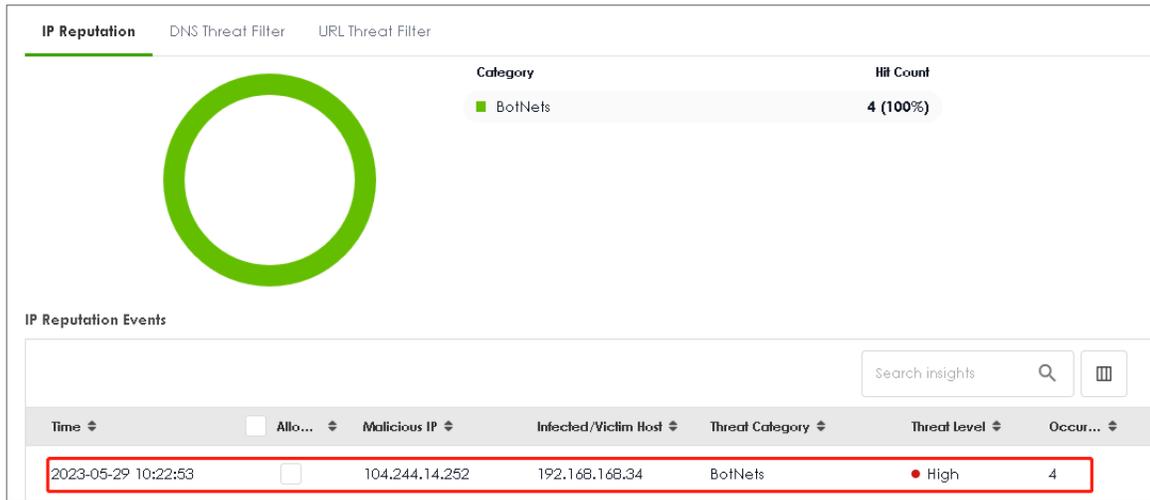
Go to Log & Report > Log/Events and select IP reputation Filter to check the logs.

← 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.

The screenshot shows the configuration interface for the URL Threat Filter. It is divided into two main sections: 'URL Blocking' and 'Security Threat Categories'.

**URL Blocking Configuration:**

- Enable:** A green toggle switch is turned on.
- Action:** A dropdown menu is set to 'block'.
- Log:** A dropdown menu is set to 'log alert'.
- Statistics:** A green toggle switch is turned on.

**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.

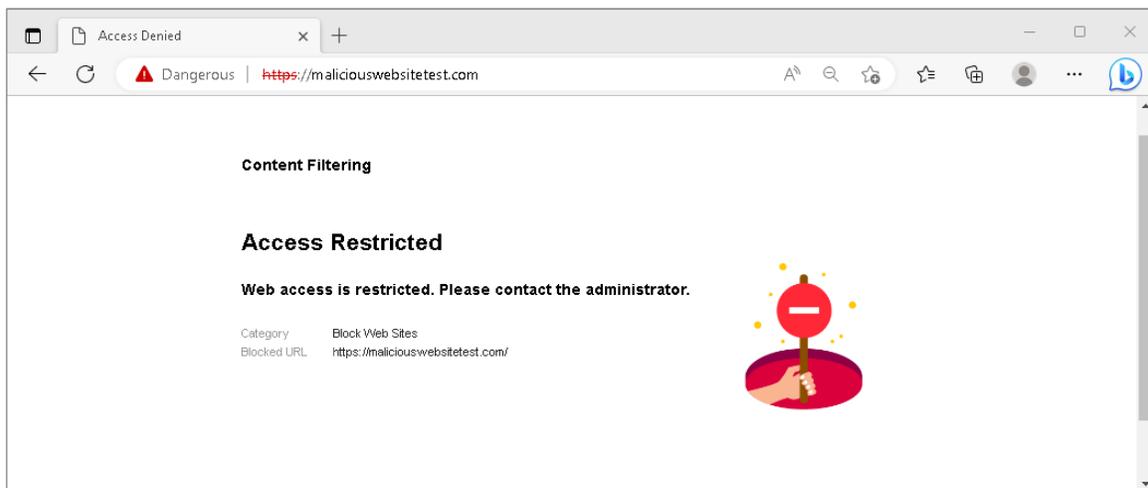
**Test URL Threat Category**

URL to test

**Message** ✕

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

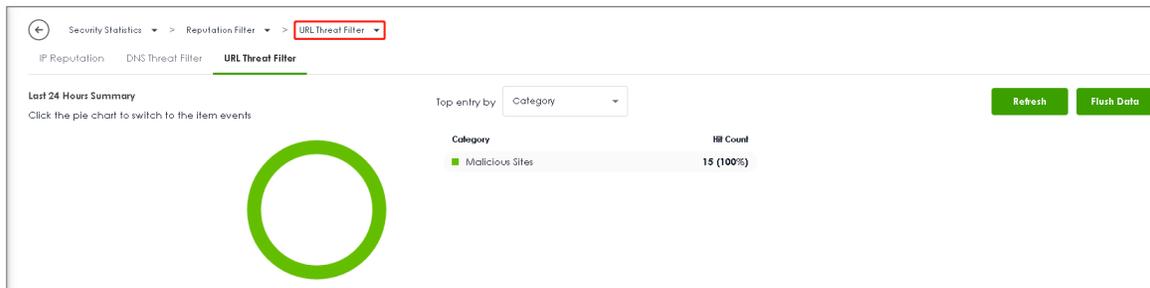
Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.



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

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

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



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

The screenshot shows the configuration page for the DNS Threat Filter. At the top, there are three tabs: 'IP Reputation', 'DNS Threat Filter' (which is selected and underlined), and 'URL Threat Filter'. Below the tabs, the 'DNS Threat Filter' section contains the following settings:

- Enable:** A green toggle switch is turned on, and it is highlighted with a red rectangular box.
- Action:** A dropdown menu is set to 'redirect'.
- Log:** A dropdown menu is set to 'log alert'.
- Redirect IP:** A dropdown menu is set to 'default'.
- Malform DNS packets:**
  - Action:** A dropdown menu is set to 'drop'.
  - Log:** A dropdown menu is set to 'log'.
- Statistics:** A green toggle switch is turned on.

Below the DNS Threat Filter section is the 'Security Threat Categories' section, which lists several categories with green checkmarks indicating they are enabled:

- 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  Query

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)

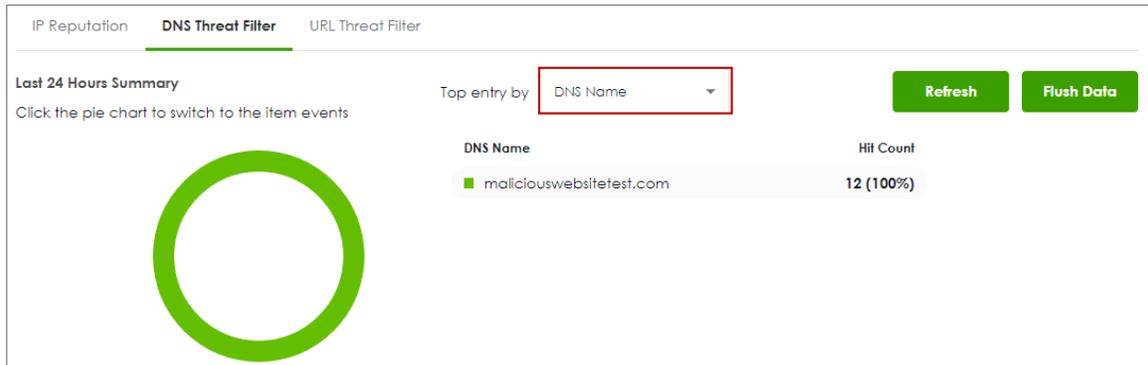
Using Web Browser to access the malicious site. The gateway will redirect you to a blocked page.



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

#	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**

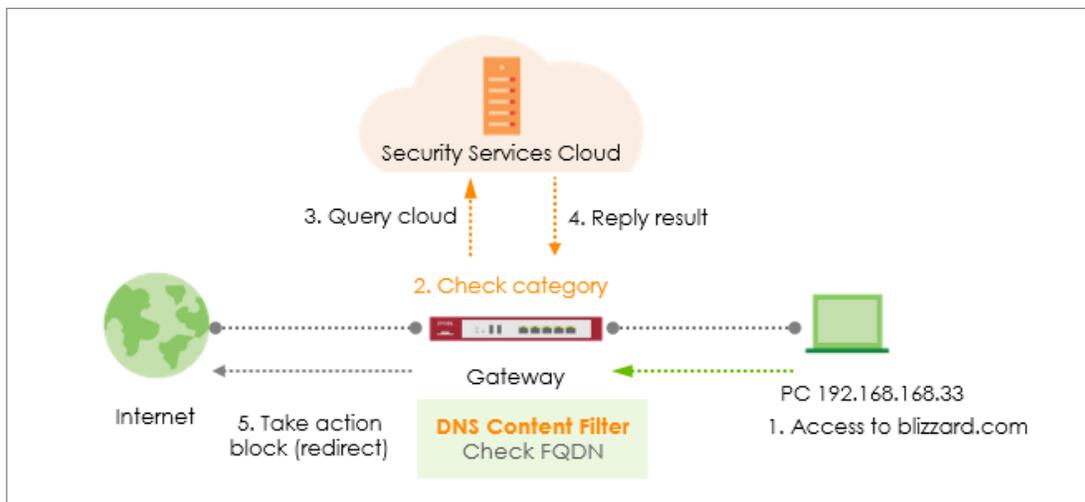
Search insights

Time	<input type="checkbox"/> +Allow ...	DNS Name	Category	Source IP
2023-05-21 16:29:36	<input type="checkbox"/>	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:44:04	<input type="checkbox"/>	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:47:02	<input type="checkbox"/>	maliciouswebsitetest.com	Malicious Sites	192.168.168.33
2023-05-21 16:49:26	<input type="checkbox"/>	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
<input type="checkbox"/> BPP		
<input type="checkbox"/> CIP		
<input checked="" type="checkbox"/> block_games		

Action: block

Log: log or log alert

**General Settings**

Name:

Description:

Action:

Log:

Log allowed traffic:

SSL V3 or previous version Connection Drop:

Drop Log:

Enable the checkbox of "Games" in managed categories.

**Managed Categories**

Select All Categories Clear All Categories

Adult Topics  Alcohol  Anonymizing Utilities  Art Culture Heritage

Auctions Classifieds  Blogs/Wiki  Business  Chat

Computing Internet  Consumer Protection  Content Server  Controversial Opinions

Cult Occult  Dating Personals  Dating Social Networking  Digital Postcards

Discrimination  Drugs  Education Reference  Entertainment

Extreme  Fashion Beauty  Finance Banking  For Kids

Forum Bulletin Boards  Gambling  Gambling Related  Game Cartoon Violence

Games  General News  Government Military  Gruesome Content

Health  Historical Revisionism  History  Humor Comics

Apply the profile to security policy. In this example, the profile is applied to security policy rule "LAN\_Outgoing".

**General Settings**

Enable:

**Configuration**

Allow Asymmetrical Route:

+ Add Edit Remove Active Inactive Move

Search insights

<input type="checkbox"/>	St...	Pri...	Name	From	To	Source	Destination	Service	User	Schedule	Act...	Log	Profile
<input type="checkbox"/>	1		LAN_Out...	LAN	any (Ex...	any	any	any	any	none	allow	no	<input checked="" type="checkbox"/>
<input type="checkbox"/>	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.

#	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.



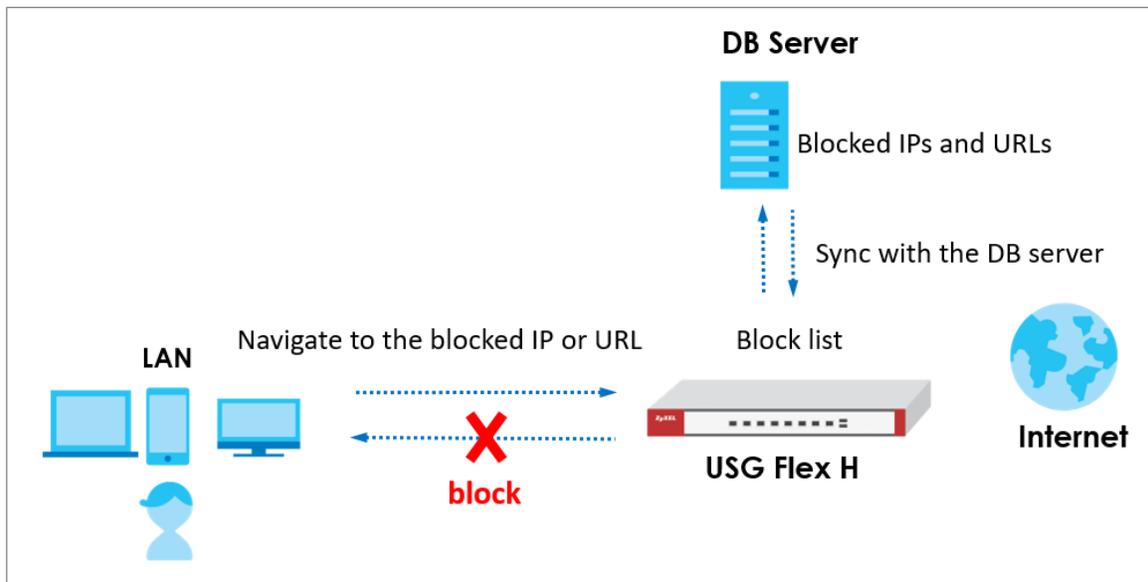
Content Filter Events

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.

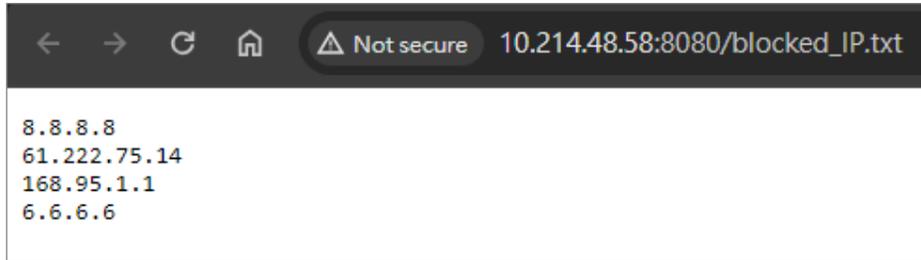


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).

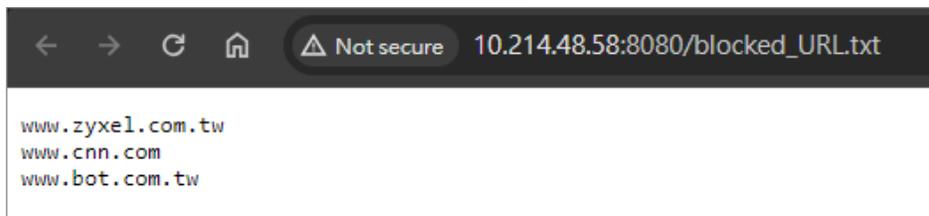
## Set Up the DB server

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_IP.txt)



[http://10.214.48.58:8080/blocked\\_URL.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](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

<input type="checkbox"/>	Name	Source URL	Description
<input type="checkbox"/>	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: 1  
 Daily: 4 am  
 Weekly: Monday, 1 am

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

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](http://10.214.48.58:8080/blocked_URL.txt) and then click "Update Now" to update the block list.

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

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

**External Block List**

Enable

**Profile Management**

+ Add    Remove

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

**Signature Update**

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

**Update Now**

Auto Update

Every N Hours    1
   
 Daily    4    pm
   
 Weekly    Monday    1    am

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

Log & Report > Log / Events

Category: All Log    Refresh    Clear Log    Export    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\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
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\>ping 168.95.1.1

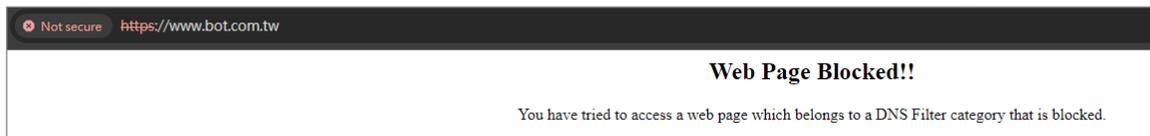
Pinging 168.95.1.1 with 32 bytes of data:
Reply from 192.168.168.1: Destination host unreachable.

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.

#	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.



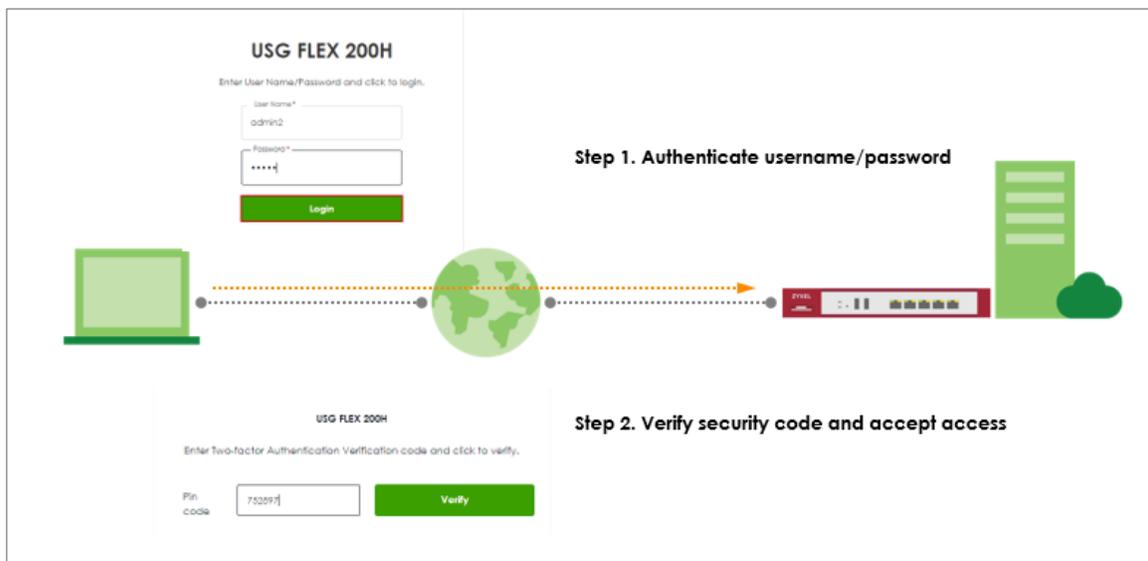
Go to Log & Report > Log / Events to observe block messages.

#	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?  
Reset Apply

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**

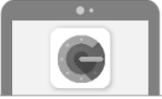
Set up Google Authenticator

## Set up Google Authenticator

Set up Google Authenticator

Step 1

**Download & install Google Authenticator on your mobile device.**



Google Authenticator




Step 2

**Add your account to Google Authenticator**

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



Can not scan the QR code?

Step 3

**Verify your device**

Enter code

Verify code and finish

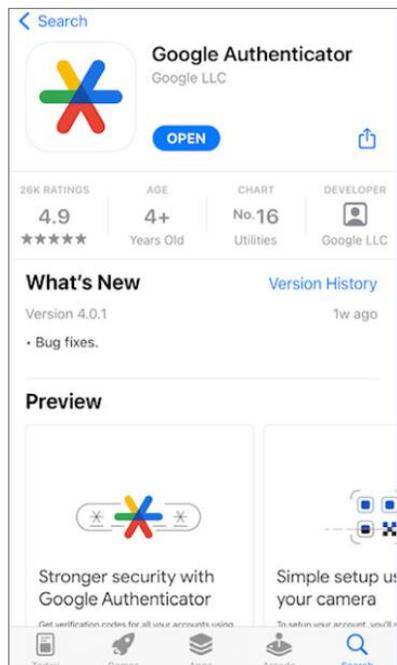
Some changes were made  
What do you want to do then?

Reset

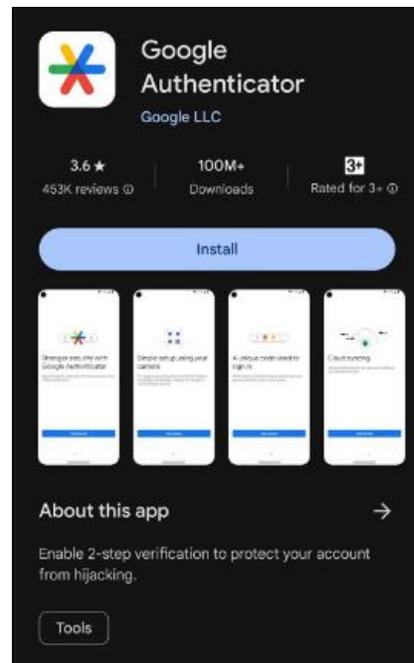
Apply

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

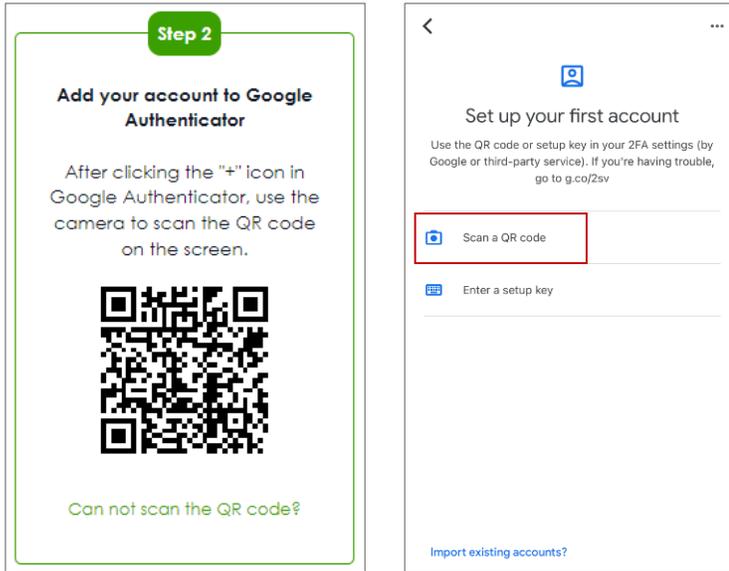
### Apple Store



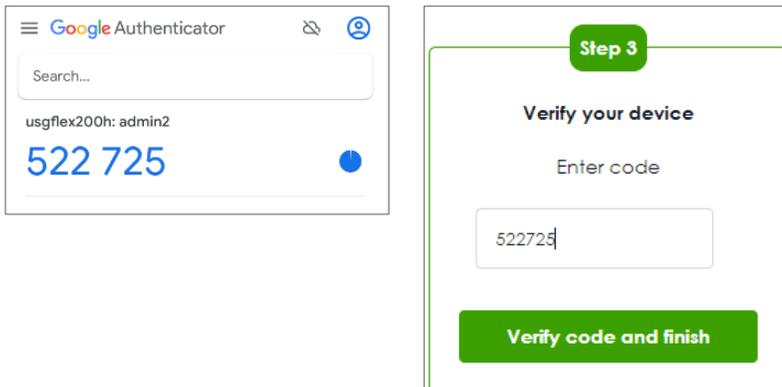
### Google Play



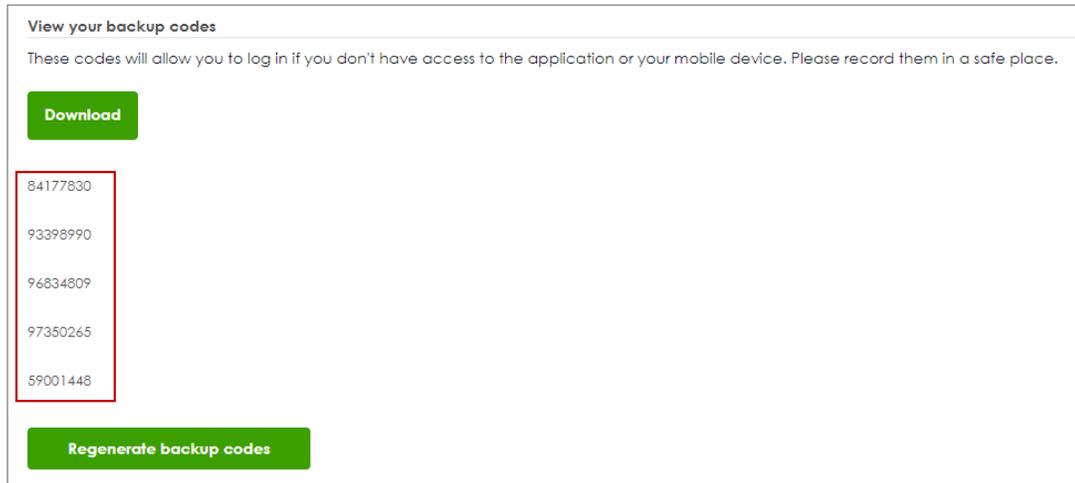
2. Register the admin account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.



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.

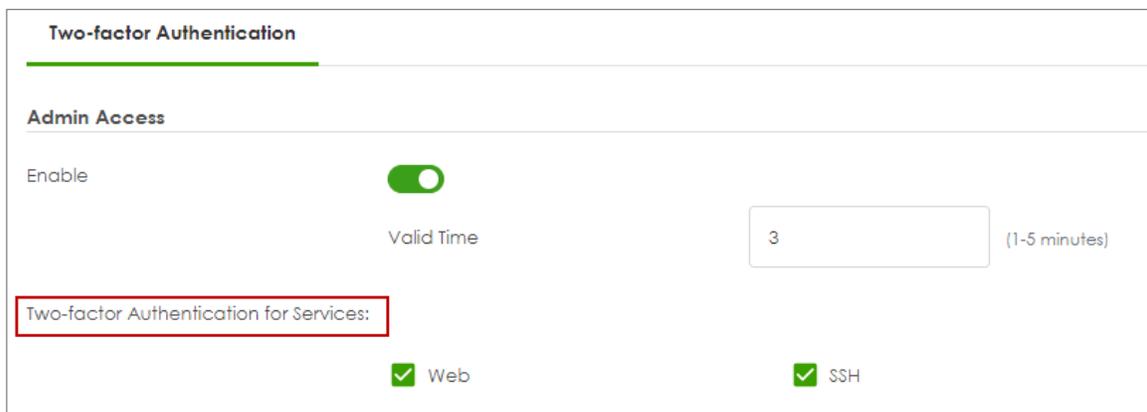


- After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.



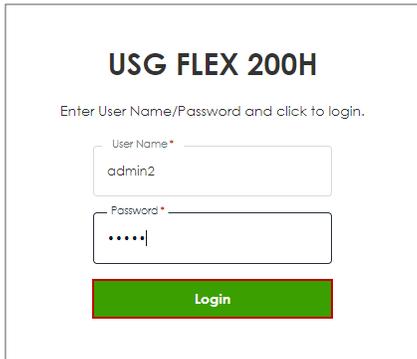
## Configure valid time and login service types

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.



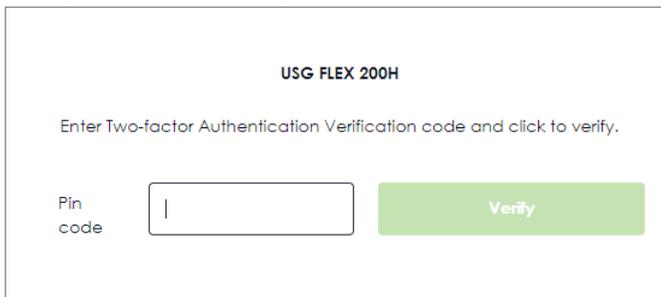
## Test the Result

1. Login with the admin account "admin2".



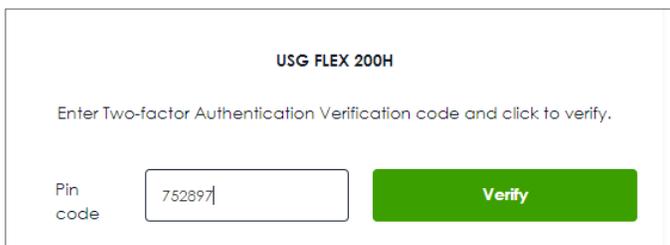
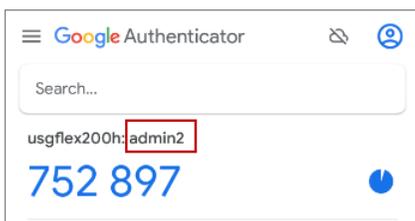
The image shows the login page for the USG FLEX 200H. The title is "USG FLEX 200H". Below the title, it says "Enter User Name/Password and click to login." There are two input fields: "User Name\*" with the value "admin2" and "Password\*" with masked characters ".....". A green "Login" button is at the bottom.

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



The image shows the verification page for the USG FLEX 200H. The title is "USG FLEX 200H". Below the title, it says "Enter Two-factor Authentication Verification code and click to verify." There is a "Pin code" input field with a vertical cursor and a green "Verify" button.

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.



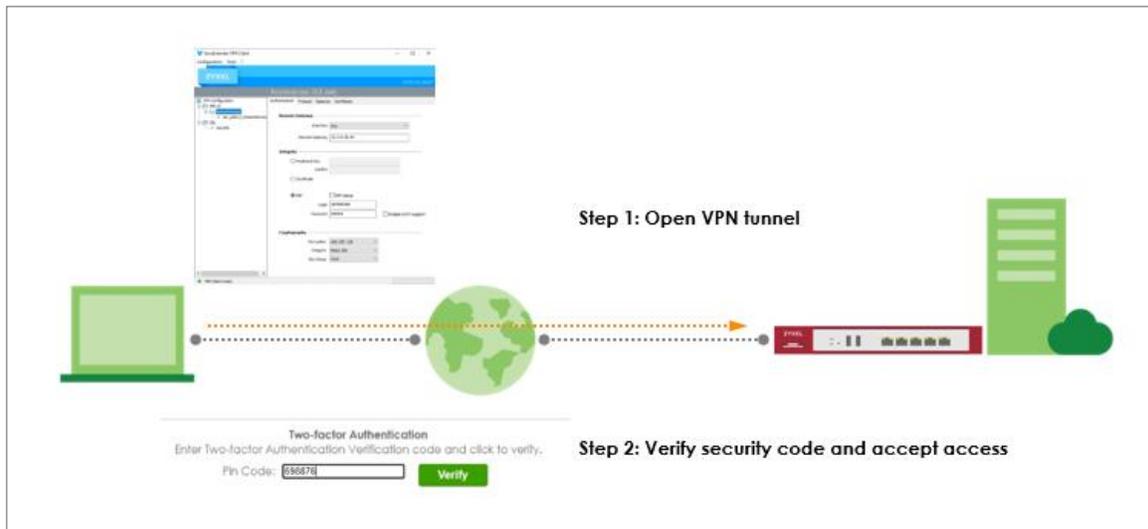
The image shows the verification page for the USG FLEX 200H, similar to the previous one, but the "Pin code" input field now contains the value "752897". The "Verify" button is still present.

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

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

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

Set up Google Authenticator

**Step 1**

Download & install Google Authenticator on your mobile device.



Google Authenticator

GET IT ON Google Play | Available on the App Store

**Step 2**

Add your account to Google Authenticator

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



Can not scan the QR code?

**Step 3**

Verify your device

Enter code

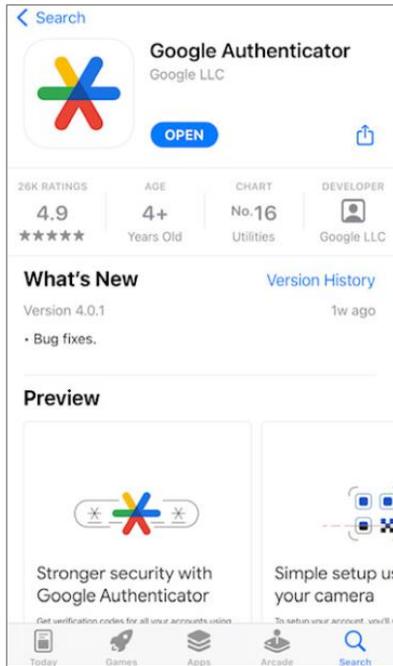
Verify code and finish

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

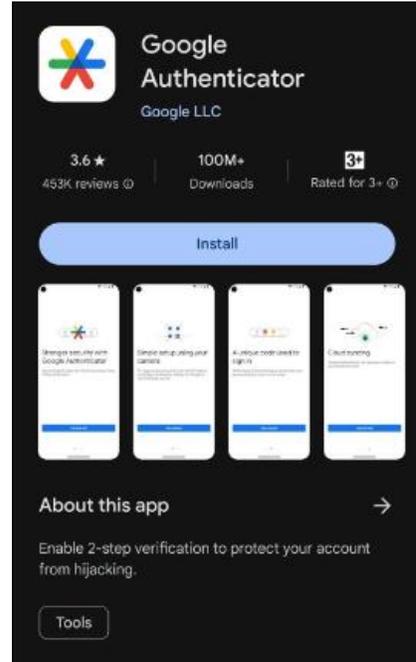
Reset Apply

- Download and install Google Authenticator on your mobile device.

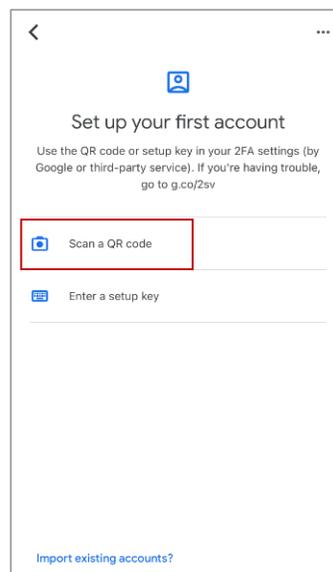
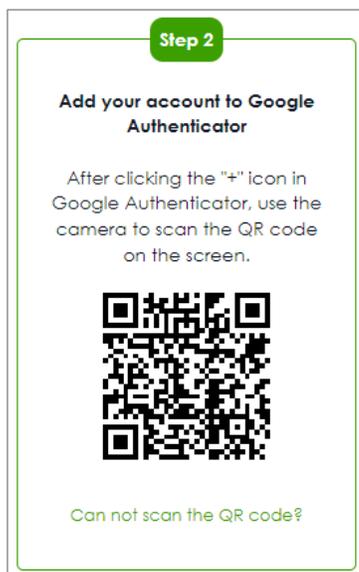
**Apple Store**



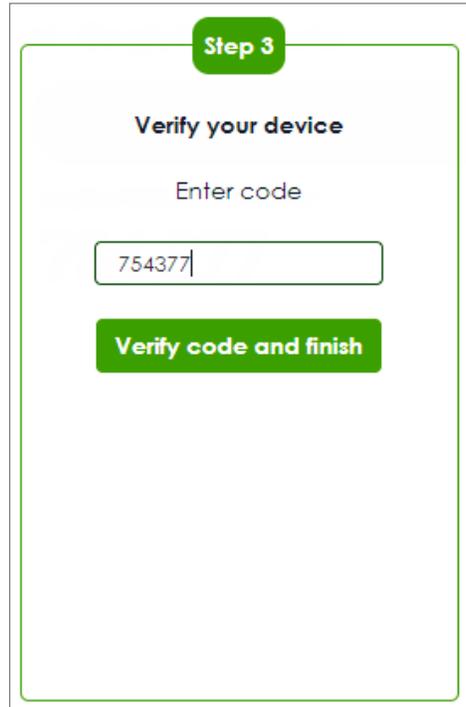
**Google Play**



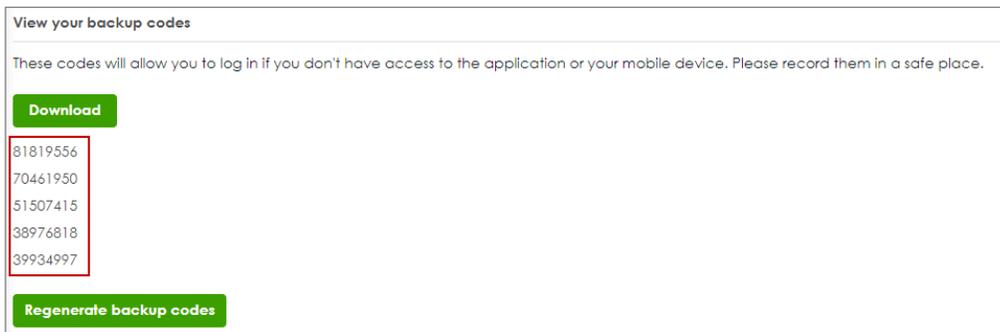
- Register the user account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.



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.



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.



## Configure valid time and login service types

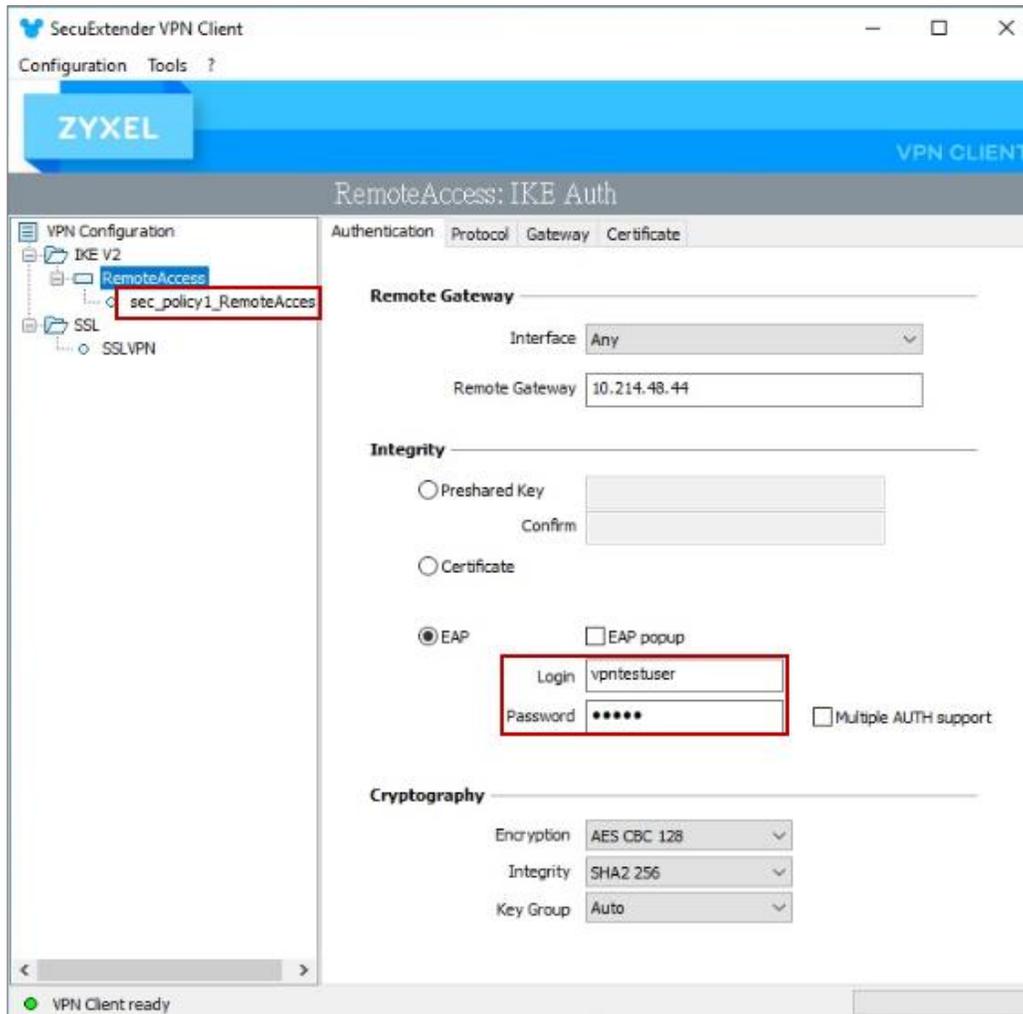
Enable two factor authentication for VPN access. Configure valid time and select which VPN type requires two-factor authentication for VPN user. The valid time is the deadline that user needs to submit the two-factor authentication code to get the VPN access. The request is rejected if submitting the 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		
<b>Admin Access</b>			
Enable	<input checked="" type="checkbox"/>		
Valid Time	<input type="text" value="3"/>	(1-5 minutes)	
Two-factor Authentication for Services			
	<input type="checkbox"/> Web	<input type="checkbox"/> SSH	
<b>VPN Access</b>			
Enable	<input checked="" type="checkbox"/>		
Valid Time	<input type="text" value="3"/>	(1-5 minutes)	
Two-factor Authentication for Services			
	<input checked="" type="checkbox"/> SSL VPN Access	<input checked="" type="checkbox"/> IPSec VPN Access	
<b>Delivery Settings</b>			
Authorize Link URL Address	<input type="text" value="HTTPS"/>	<input type="text" value="From Interface"/>	<input type="text" value="ge3"/>
Authorized Port	<input type="text" value="8008"/>	(1-65535) ⓘ	

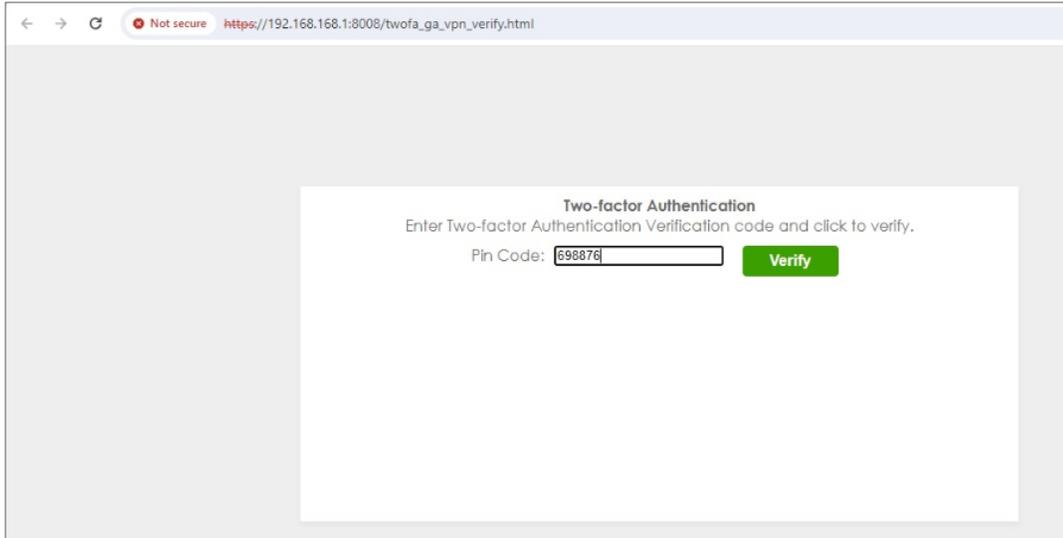
## Test the Result

### Remote Access VPN (IKEv2)

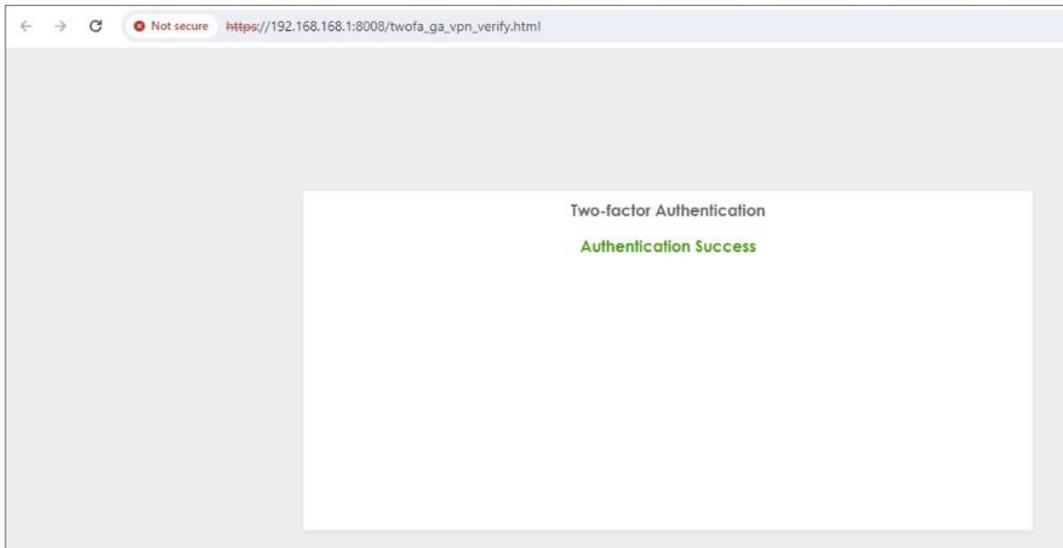
1. Open Remote Access VPN tunnel on SecuExtender VPN Client.



- 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.



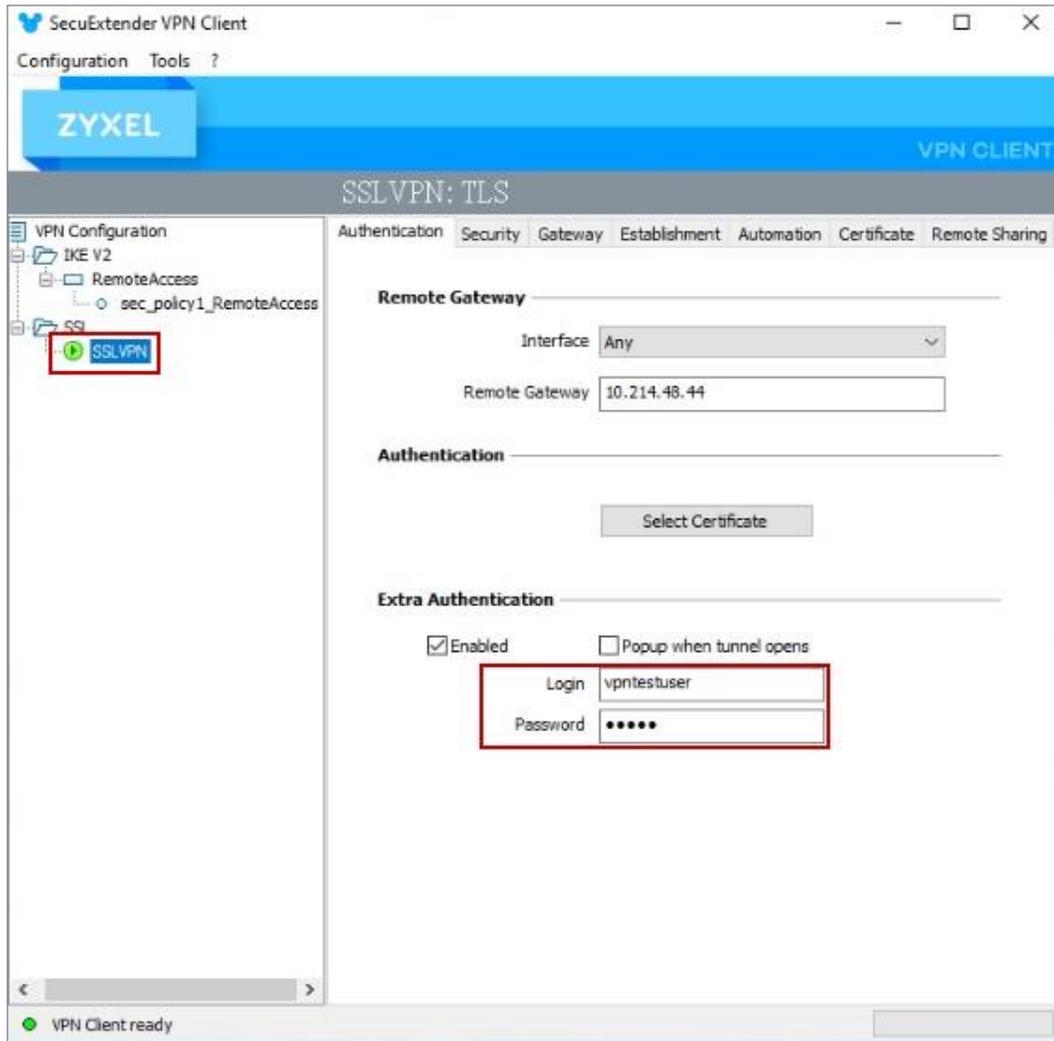
- Authorize with username, password and the token code successfully.



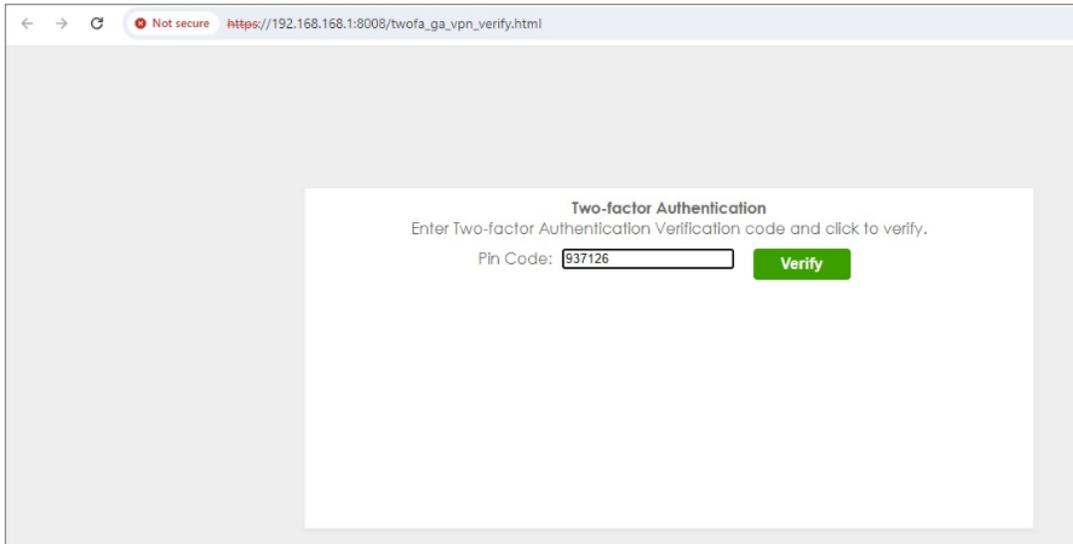
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
56	2024-03-13 18:22:55	User	user: vpntestuser[192.168.50.1] is authorized	0.0.0.0	0.0.0.0	0	two-factor auth.
67	2024-03-13 18:22:45	User	User vpntestuser(MAC=) from eap-cfg h as logged in Device	10.214.48.49	0.0.0.0	0	Account: vpntestuser
72	2024-03-13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

### SSL VPN

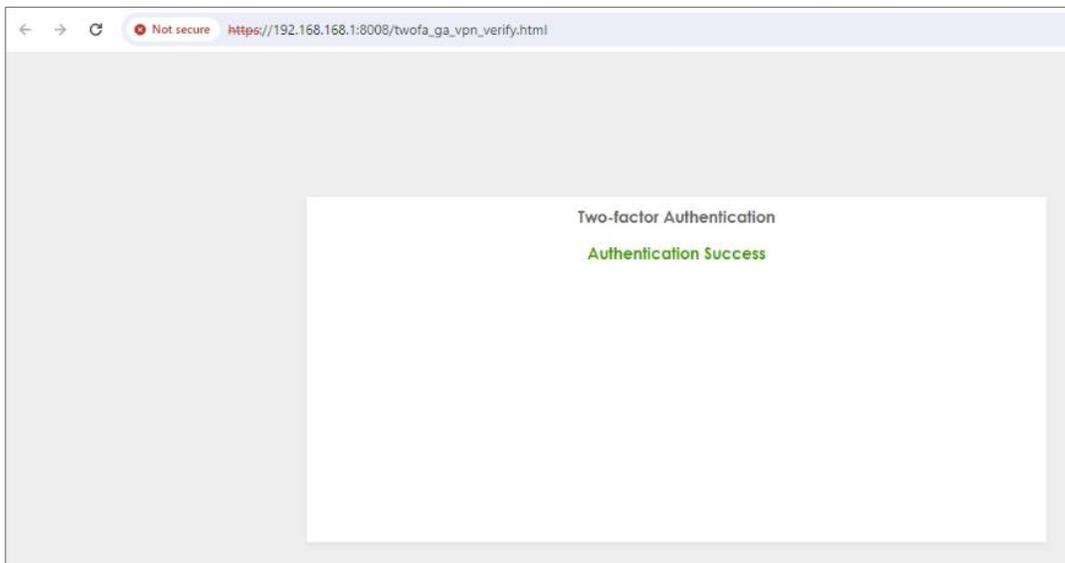
1. Open SSL VPN tunnel on SecuExtender VPN Client.



- 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.



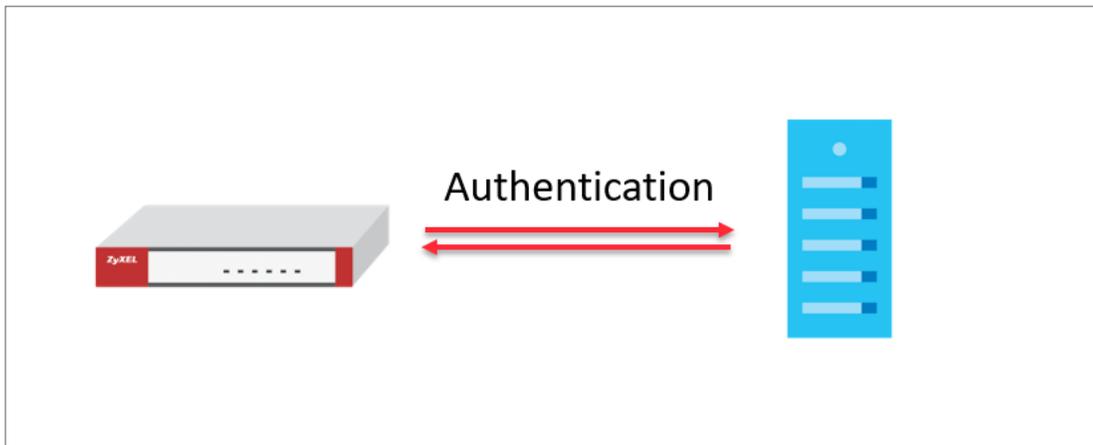
- Authorize with username, password and the token code successfully.



#	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.

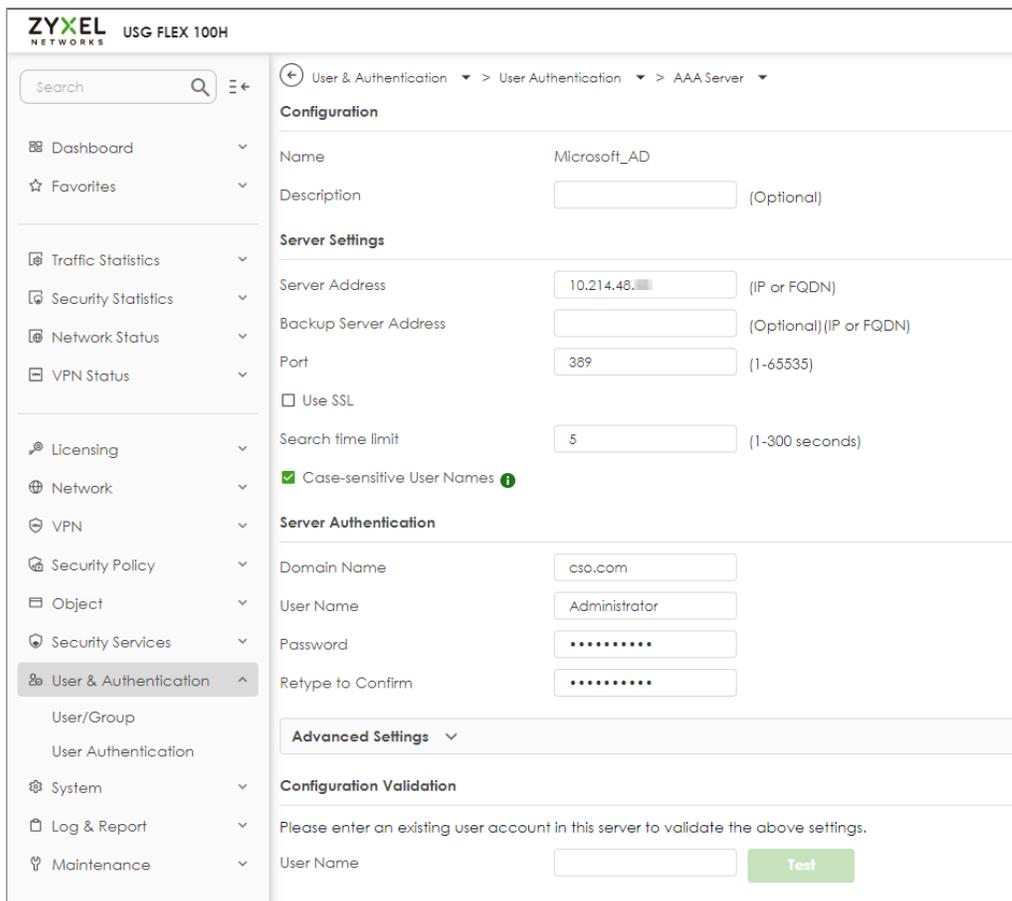


## Set Up a profile for AD server

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.



## Join Domain

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

Domain	DNS Server	Query Via
<input type="checkbox"/> cso.com	10.214.48.20	ge1 (WAN)

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

Name	Server Address	Domain Name	Reference
<input checked="" type="checkbox"/> Microsoft_AD	10.214.48.20	cso.com	0

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

Name	Server Address	Domain Name
<input checked="" type="checkbox"/> Microsoft_AD	10.214.48.20	cso.com

**Join AD Domain**

Associated AD Server Object: Microsoft\_AD

AD Domain Name: cso.com

NetBIOS Domain Name:

User Name:

Password:

Retype to Confirm:

After join domain successfully, you can see this icon.

Name	Server Address	Domain Name	Join Domain	Reference
<input checked="" type="checkbox"/> Microsoft_AD	10.214.48.20	cso.com	<input checked="" type="checkbox"/>	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.

The screenshot shows a web interface for configuring an AAA Server. The breadcrumb navigation is: User & Authentication > User Authentication > AAA Server. The main section is titled "Server Authentication" and contains the following fields:

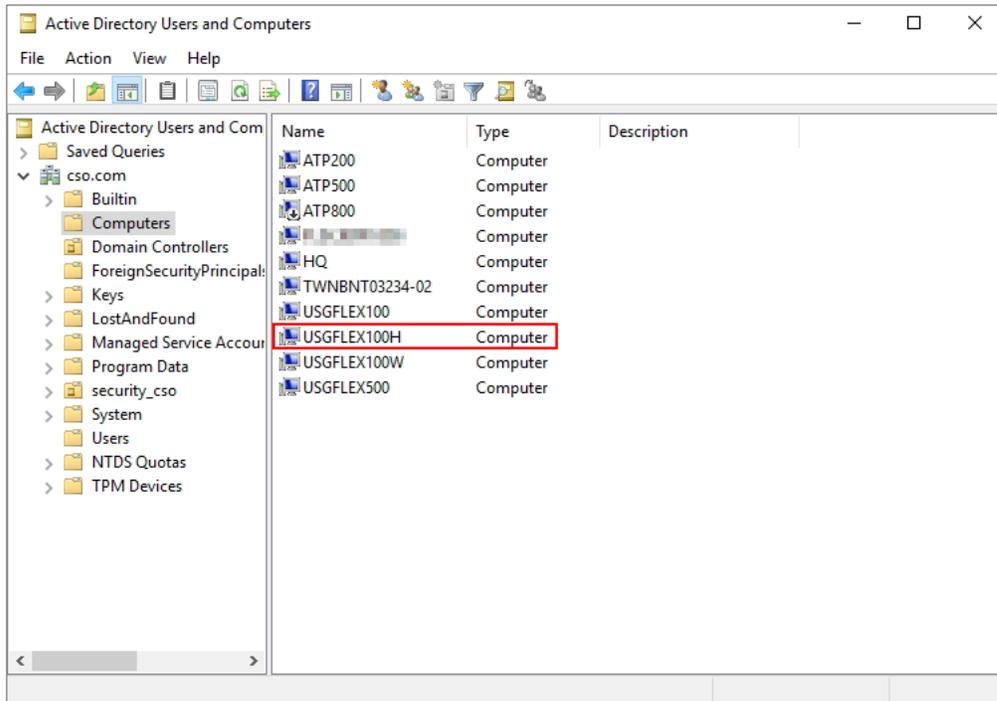
- Domain Name: cso.com
- User Name: Administrator
- Password: [Redacted]
- Retype to Confirm: [Redacted]

Below this is an "Advanced Settings" section, which is currently collapsed. Underneath is the "Configuration Validation" section, which includes the instruction: "Please enter an existing user account in this server to validate the above settings." It features a "User Name" field with "stanley" entered and a green "Test" button. The "Test Status" field displays "OK".

At the bottom, the "Returned User Attributes" section shows the following details:

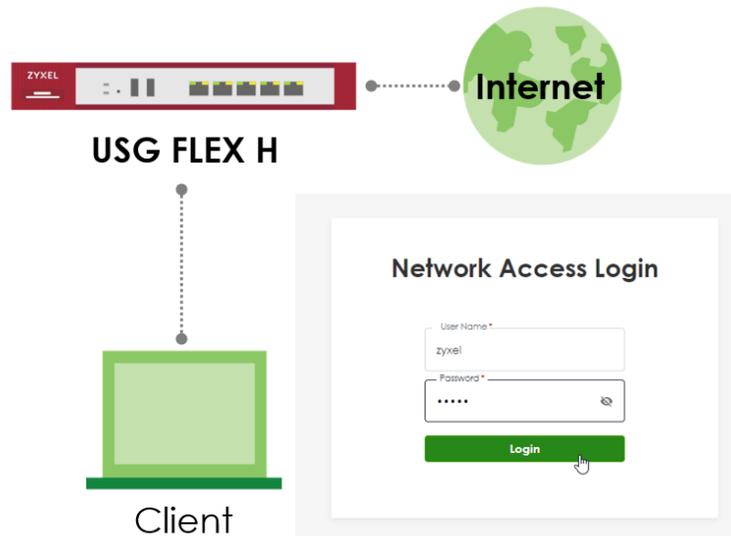
```
dn: CN=stanley,CN=Users,DC=cso,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: stanley
givenName: Stanley
distinguishedName: CN=stanley,CN=Users,DC=cso,DC=com
instanceType: 4
whenCreated: 20240305035706.0Z
whenChanged: 20240305052539.0Z
displayName: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

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



## How to Set Up Captive Portal?

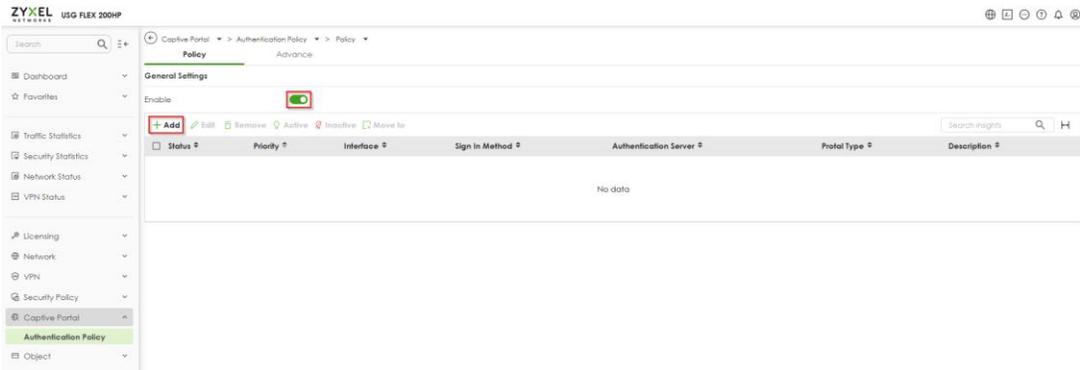
The Captive Portal feature provides functionality that requires LAN client users to complete the authentication procedure of Network Access Login page before accessing the internet. This article will guide users on how to set up and verify this feature.



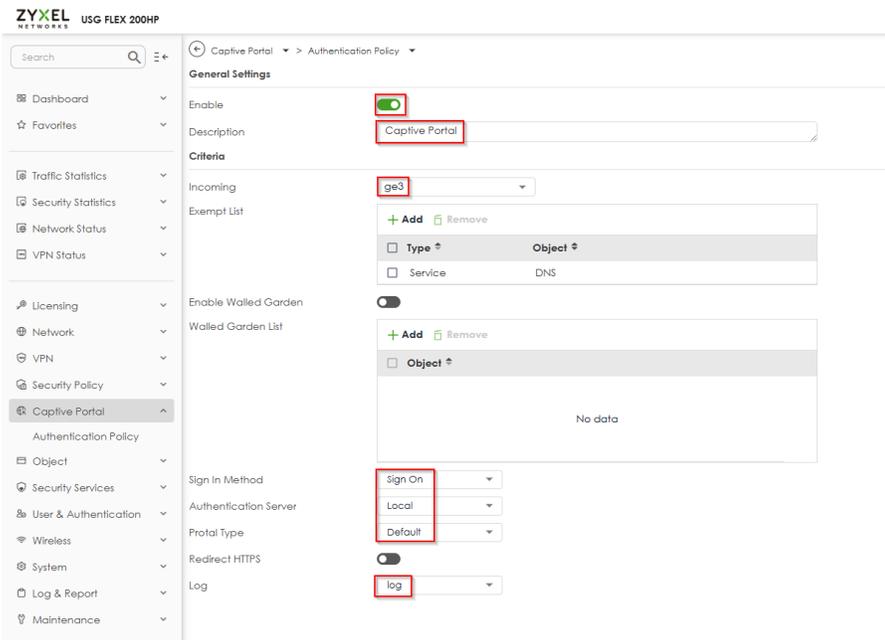
 Note: Captive Portal is supported on USG Flex 100H, USG FLEX 200H, USG FLEX 200HP, USG FLEX 500H, USG FLEX 700H. This example was tested using USG FLEX 200HP (Firmware Version: uOS 1.32).

## Configure the Captive Portal via the Web-GUI

1. **Enable the Captive Portal and add a policy** - Navigate to the Web-GUI path Captive Portal > Authentication Policy > Policy > To enable the **Captive Portal** function and add a policy.



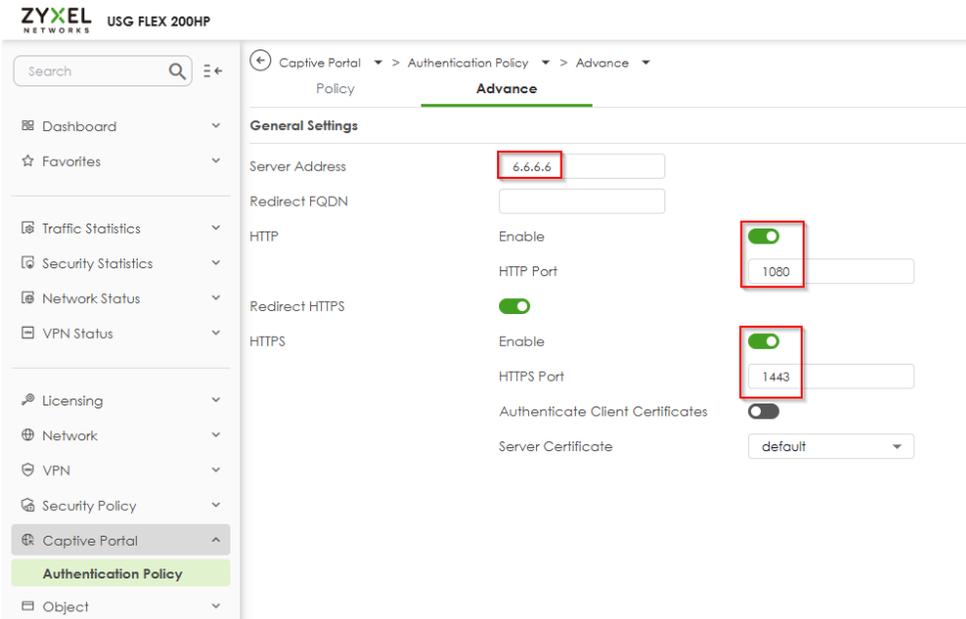
2. **Add an Authentication Policy** – Enable the Authentication Policy, provide a Description, select the Incoming interface, choose the Sign In Method, specify the Authentication Server and Portal Type, and enable Log.



3. **Check the settings** – Ensure the Captive Portal function and the Authentication Policy are enabled.



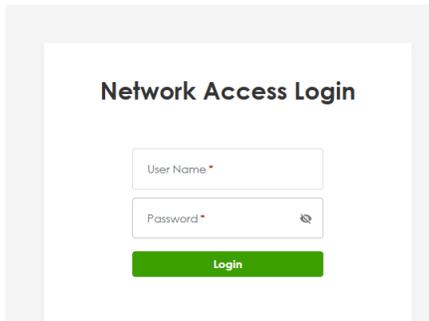
4. **Edit the Advance settings** – The default server address is 6.6.6.6, the default HTTP port is set to 1080, and the default HTTPS port is set to 1443.



## Verify the Captive Portal function

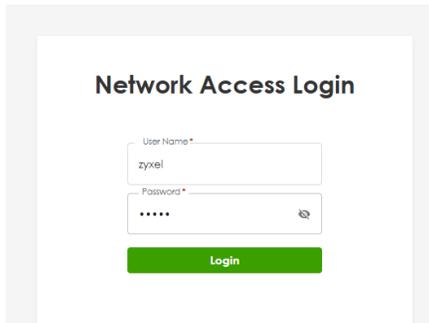
The PC client must complete the authentication process of the Captive Portal before gaining access to the internet.

1. The PC client connects to the LAN port and opens the browser, which will be redirected to the Network Access Login page.



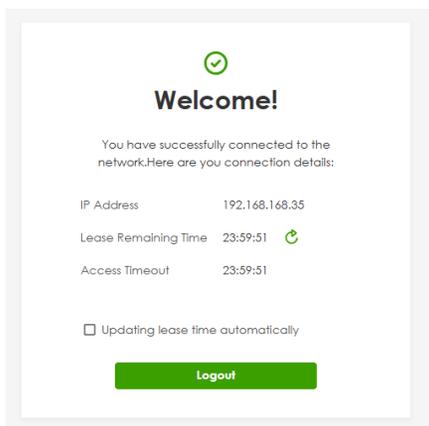
The screenshot shows the 'Network Access Login' page. It features a title 'Network Access Login' at the top. Below the title are two input fields: 'User Name \*' and 'Password \*'. The 'Password \*' field has a small eye icon to its right. At the bottom of the form is a green 'Login' button.

2. Enter the login User Name and Password.



The screenshot shows the 'Network Access Login' page with the 'User Name \*' field containing the text 'zyxel'. The 'Password \*' field contains masked characters (dots) and has the eye icon visible. The green 'Login' button is still present at the bottom.

3. Once successfully logged into the Network Access Login page, the client will be redirected to the Welcome page, which displays the client's IP address, lease remaining time, and access timeout.

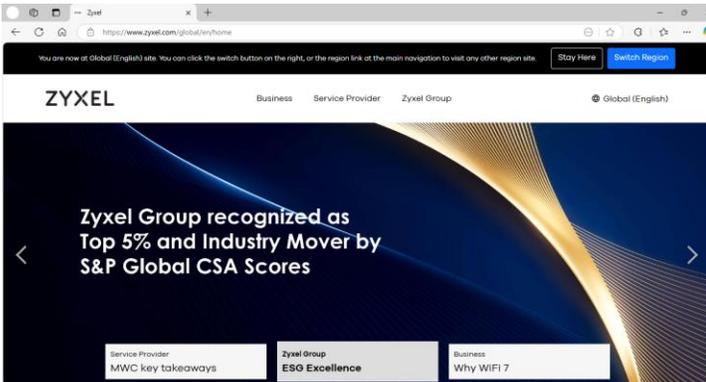


The screenshot shows the 'Welcome!' page. It features a green checkmark icon at the top. Below the title is a message: 'You have successfully connected to the network. Here are your connection details:'. This is followed by a table of connection details:

IP Address	192.168.168.35
Lease Remaining Time	23:59:51 
Access Timeout	23:59:51

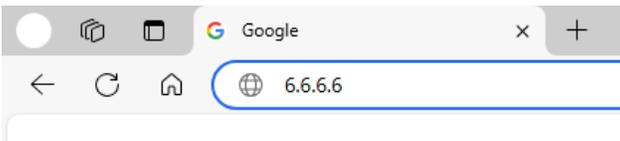
Below the table is a checkbox labeled 'Updating lease time automatically' which is currently unchecked. At the bottom is a green 'Logout' button.

- Eventually, the client can access the internet normally.

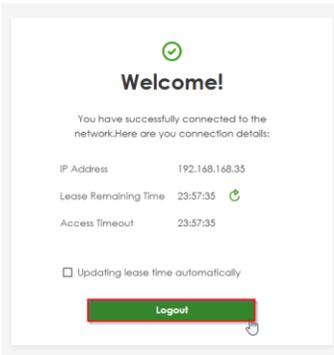


## How to logout the Captive Portal?

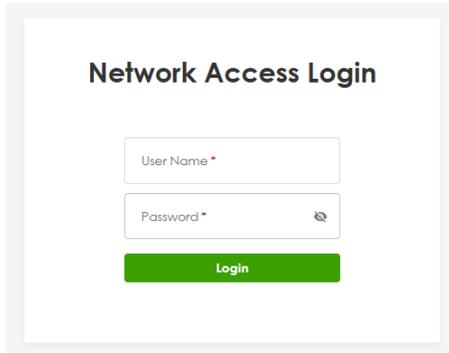
- Enter the defined server link. The default link is https://6.6.6.6.



- Enter the Welcome page and click 'Logout'.



- Redirect to the Network Access Login page. If the user needs to access the internet, they must re-enter the username and password to complete the Captive Portal authentication process.



## How to check the status?

When the user successfully logs into the Captive Portal page, they can navigate to the GUI path: Network Status > Login Users > Login Users, to check if the user account has already logged into the Captive Portal.

#	User ID	Role	From	Login Time	Type	Tunnel IP	Lease Time	User Info
1	admin	admin	console	0:19:35	console	0.0.0.0	23:40:52	admin(admin)
2	admin	admin	192.168.169.33	0:00:13	http/https	0.0.0.0	23:59:59	admin(admin)
3	zyxel	user	192.168.168.35	0:01:23	captive portal	0.0.0.0	23:58:37	user(zyxel)

They can also navigate to the GUI path: Log & Report > Log / Events > System, to verify the log message indicating that they have successfully logged into the captive portal.

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
4	2025-03-17 14:06:37	User	User zyxel(MAC=) from captive portal has logged in Device	192.168.168.35	192.168.168.1	0	Account: zyxel

When the user successfully logs out the Captive Portal page, they can navigate to the GUI path: Log & Report > Log / Events > System, to verify the log message indicating that they have successfully logged out the captive portal.

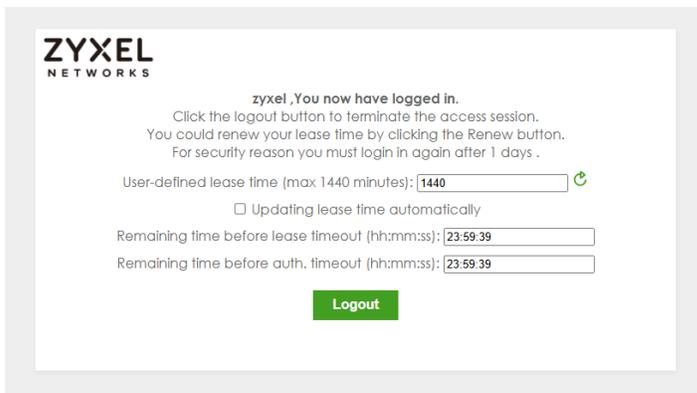
#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
59	2025-03-17 14:13:34	User	User zyxel from captive portal has logged out Device	192.168.168.35	192.168.168.1	0	Account: zyxel

## Feature Change:

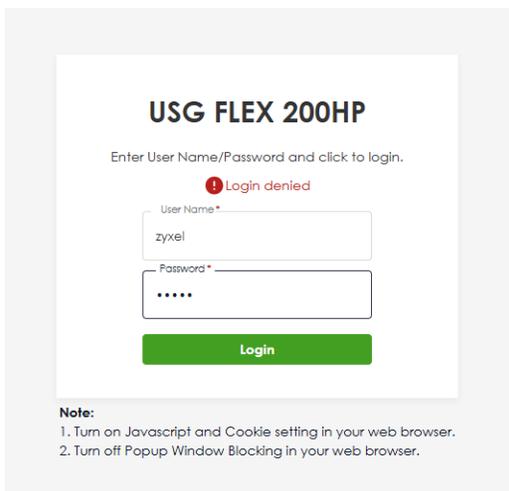


Starting from firmware version uOS 1.32, the user must log in to the Captive Portal before using the User Aware function for security policy or BWM policy utilization.

Prior to firmware version uOS 1.32, users were able to successfully log in to the device's GUI link to utilize security policies or BWM policies, as shown below:



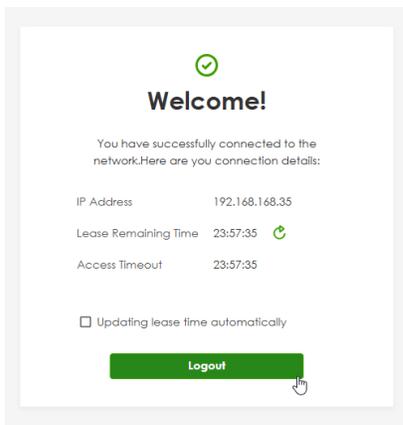
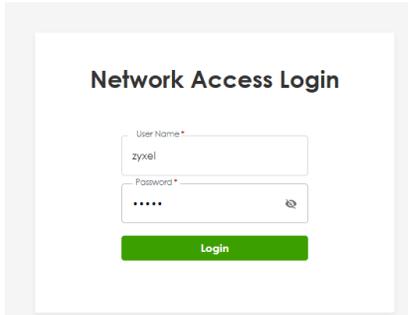
Starting from firmware version uOS 1.32, if an account that does not belong to the Local Administrator attempts to log in to the Web-GUI page, access will be denied, as shown below:



Therefore, starting from firmware version uOS 1.32, if users wish to utilize security policies or BWM policies for login users, they need to enable the Captive Portal function. Users

must successfully log in to the Network Access Login page to activate the security or BWM policies, as show in below:

The user successfully logged in to the Network Access Login page.



They can then activate the security or BWM policies for the specific user account.

Security Policy > Policy Control

**General Settings**

Enable

**Configuration**

Allow Asymmetrical Route

Status	Pri.	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log	Hits	Profile
<input checked="" type="checkbox"/>	1	For_The_User	LAN	any (Excluding ZyWALL)	any	any	any	zyxel	none	allow	no	3	

Network > BWM

**General Settings**

Enable

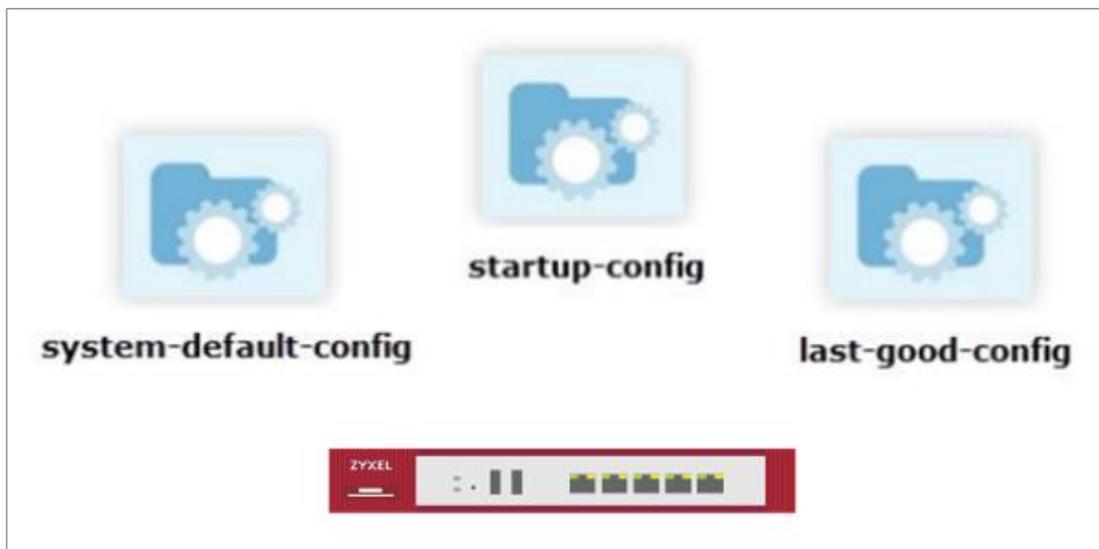
**Configuration**

Status	Pri.	Name	Description	User	Incoming Interface	Outgoing Interface	Source	Destination	Service	BWM Download/Upload/Pri
<input type="checkbox"/>		Default		any	any	any	any	any		na/na/7
<input checked="" type="checkbox"/>	1	For_The_User		zyxel	ge3	ge1	any	any	any	0/0/4

## 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 breadcrumb navigation is Maintenance > File Manager > Configuration File. The page title is Configuration File - Firmware Management. Below the title, there are action buttons: Rename, Remove, Download (highlighted with a red box), Copy, Apply, Email, and Upload. A table lists configuration files:

File Name	Size	Last Modified
<input type="checkbox"/> system-default.conf	46398	2023-03-13 17:31:15
<input checked="" type="checkbox"/> startup-config.conf	47310	2023-03-31 15:28:15
<input type="checkbox"/> lastgood.conf	47310	2023-05-02 08:03:22
<input type="checkbox"/> 100ABWVOC0.conf	46398	2023-03-31 09:38:18

Below the table, there is a section for 'Configure Backup Schedule' with a 'Beta' tag. It includes an 'Enable Auto Backup' toggle and radio buttons for 'Daily', 'Weekly', and 'Monthly' schedules, each with dropdown menus for hours, days, and minutes.

## Copy the Configuration Files

### Maintenance > File Manager > Configuration File

Select the file and click "Copy".

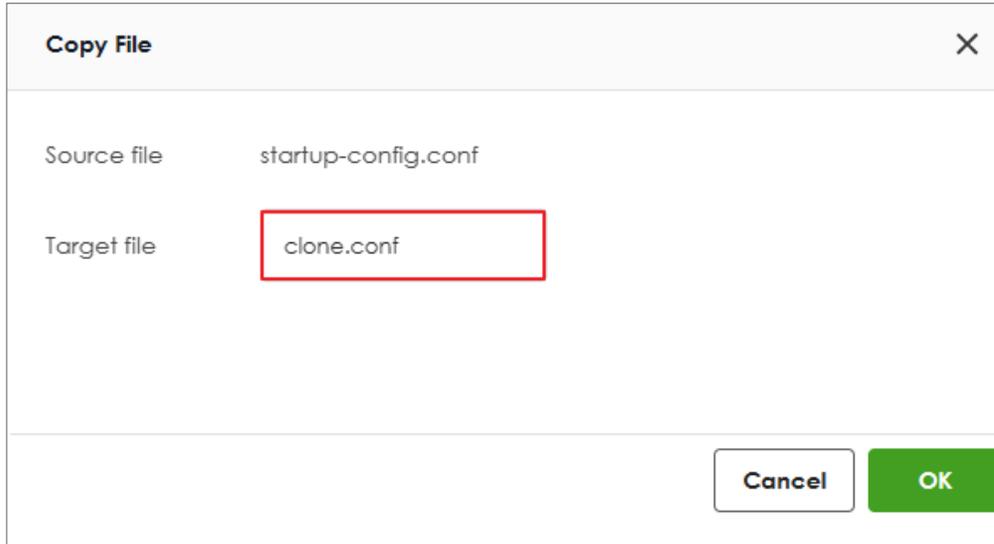
The screenshot shows the ZyXel File Manager interface. The breadcrumb navigation is Maintenance > File Manager > Configuration File. The page title is Configuration File - Firmware Management. Below the title, there are action buttons: Rename, Remove, Download, Copy (highlighted with a red box), Apply, Email, and Upload. A table lists configuration files:

File Name	Size	Last Modified
<input type="checkbox"/> system-default.conf	46398	2023-03-13 17:31:15
<input checked="" type="checkbox"/> startup-config.conf	47310	2023-03-31 15:28:15
<input type="checkbox"/> lastgood.conf	47310	2023-05-02 08:03:22
<input type="checkbox"/> 100ABWVOC0.conf	46398	2023-03-31 09:38:18

Below the table, there is a section for 'Configure Backup Schedule' with a 'Beta' tag. It includes an 'Enable Auto Backup' toggle and radio buttons for 'Daily', 'Weekly', and 'Monthly' schedules, each with dropdown menus for hours, days, and minutes.

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

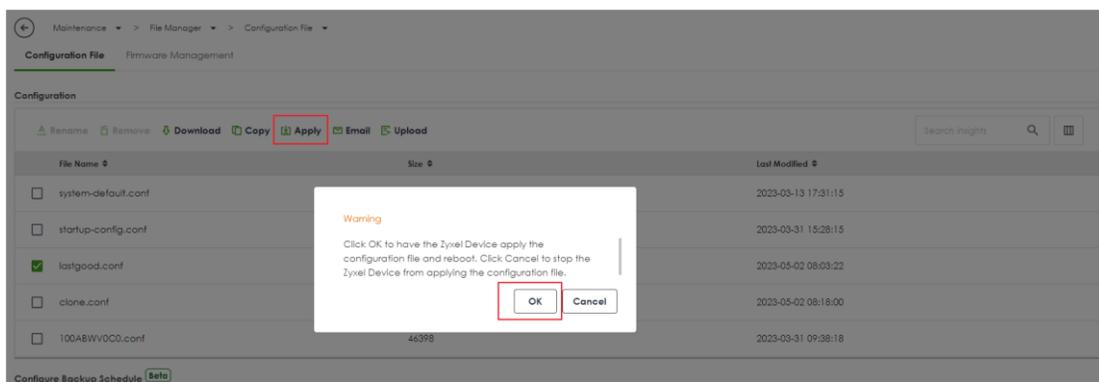
The file as format: [a-zA-Z0-9~\_.--]{1,63}.conf



## Apply the Configuration Files

### Maintenance > File Manager > Configuration File

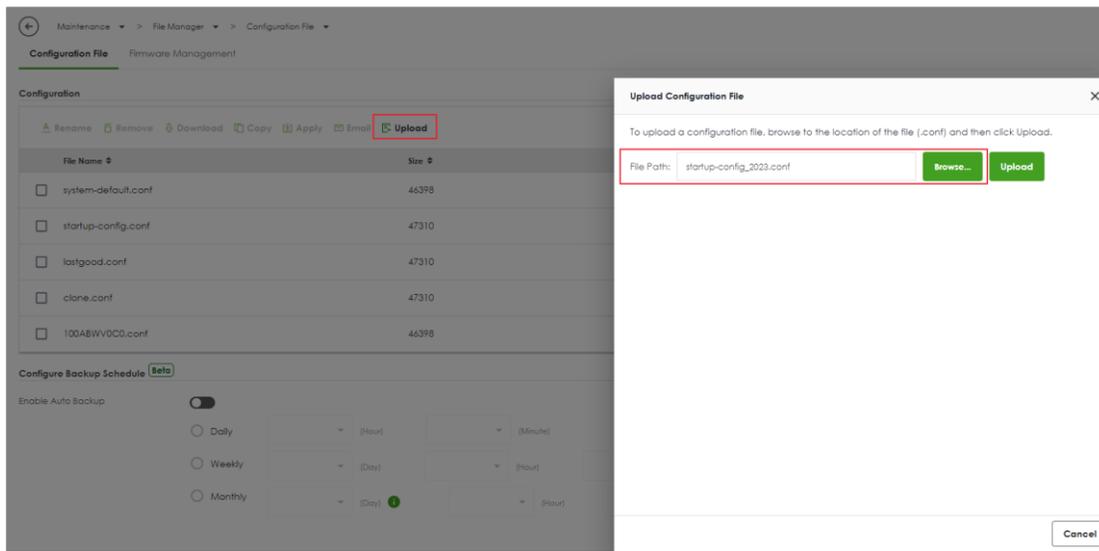
Select a specific configuration file to have ZyWALL use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL settings to the factory defaults. Or select the **lastgood.conf** which is the most recently used (valid) configuration file that was saved when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

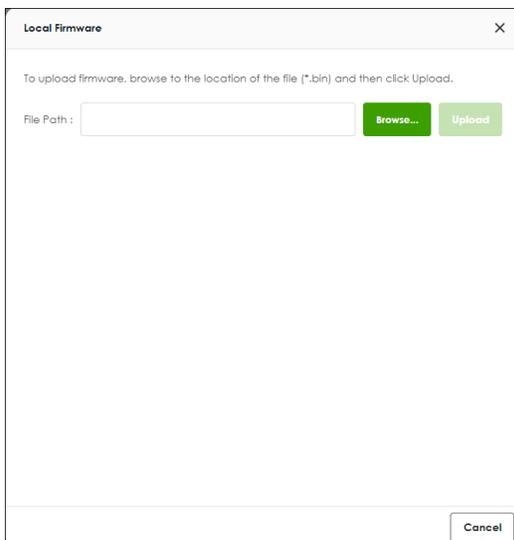
### Local Firmware Upgrade

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) 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** [X]

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

File Path:  Browse... Upload

Cancel

## 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	<input type="button" value="Check Now"/>
Release Date	None	
Auto Update	<input checked="" type="checkbox"/>	
	<input type="radio"/> Daily	<input type="text"/> (Hour)
	<input type="radio"/> Weekly	<input type="text"/> (Day) <input type="text"/> (Hour)
	<input type="checkbox"/> Auto Reboot	<input type="checkbox"/>

## 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.

The screenshot displays the 'Mail Server' configuration page in a web interface. At the top, there is a breadcrumb trail: System > Notification > Mail Server. Below this, the page title is 'Mail Server' with a sub-tab 'Alert'. The main section is titled 'General Settings' and contains the following fields and controls:

- Mail Server:** Input field containing 'smtp.gmail.com' with a tooltip '(Outgoing SMTP Server Name or IP Address)'. Below it is a 'Port' input field containing '587' with a tooltip '(1-65535)'. To the right of these fields are two green toggle switches for 'TLS Security' and 'STARTTLS', both of which are turned on.
- Authenticate Server:** A grey toggle switch that is turned off.
- SMTP Authentication:** A green toggle switch that is turned on.
- User Name:** Input field containing '9@gmail.com'.
- Password:** Input field with masked characters '.....'.
- Retype:** Input field with masked characters '.....'.

Below the 'General Settings' section is the 'Mail Server Test' section, which includes:

- Mail To:** Input field with a tooltip '(Email Address)'. Below it is a 'Send From' input field, also with a tooltip '(Email Address)'.
- Mail Now:** A green button located at the bottom left of the 'Mail Server Test' section.

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

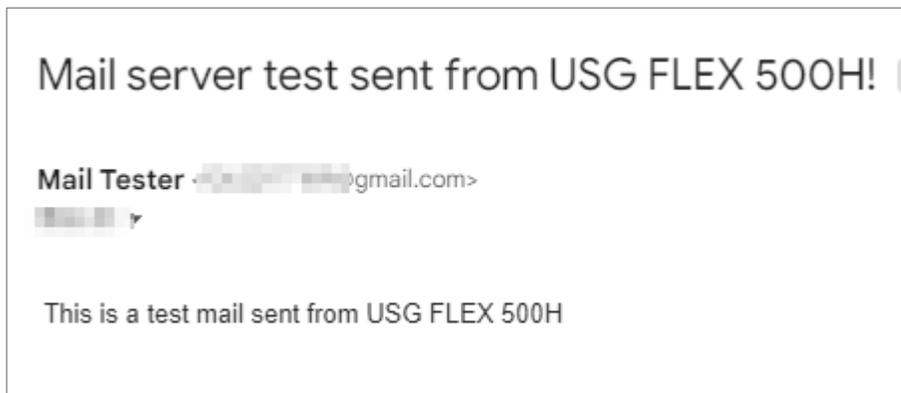
**Mail Server Test**

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: [redacted]@gmail.com

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

[redacted] (Email Address)

[redacted] (Email Address)

[redacted] (Email Address)

[redacted] (Email Address)

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

**Report Items**

**System Resource Usage**

CPU Usage       Interface Usage       Memory Usage       Port Usage       Session Usage

**Security Services**

Anti-Malware       App Patrol       Content Filter       IPS       Reputation Filter

**System Information**

DHCP Table

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

**Schedule**

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

## Test the Email Daily Report

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

**Email Settings**

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

E-mail Subject: 500H-Daily-Report

Append system name       Append date time

Email from: [redacted]@gmail.com

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

**Send Report Now**

f [redacted]@gmail.com 下午3:00

ZYXEL NETWORKS

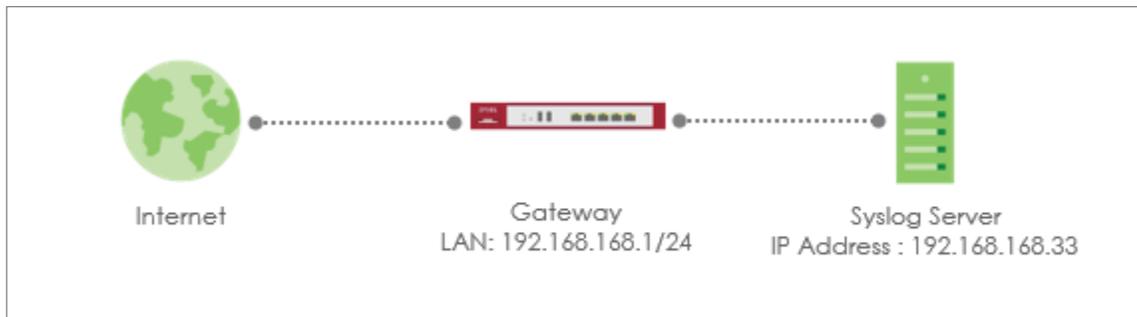
**General**

Model Name:	USG FLEX 500H
Firmware Version:	V1.10(A82H.0)b7s1   2023-08-17 15:35:54
MAC Address Range:	[redacted]
System Uptime:	10 days, 22:37:53
System Name:	usgflex500h

**System Resource Usage**

## How to Setup and Send Logs to a Syslog Server

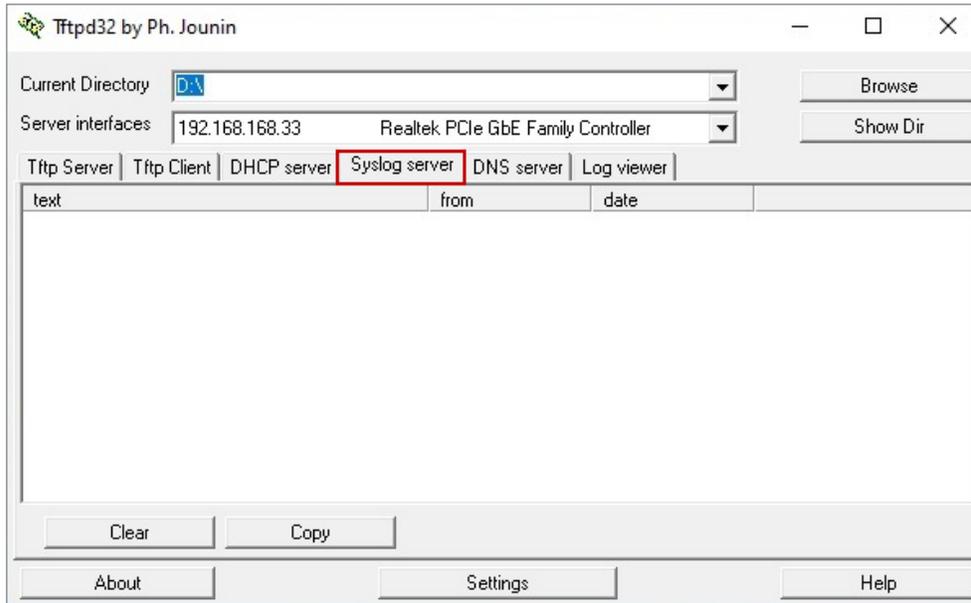
For management purposes, administrators can easily monitor events occurring on the gateway by reading the syslog. This example shows how to send logs to a syslog server. You can also specify which log messages to syslog server. When the syslog server is configured, you will receive the real time system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



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

## Set Up the Syslog Server

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



## Set Up Remote Server Setting on the Gateway

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

Log Category Setting					
Category	System Log	USB Storage	Remote Server 1	Remote Server 2	Count
	disable normal debug	disable normal debug	disable normal debug	disable normal debug	
	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	158
> Authenticate	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	9
> Security	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	0
> System	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	13
> Security Service	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	6
> VPN	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input checked="" type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	0
> License	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	130



## 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	
	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	3
> Authenticate	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	2
∨ Security	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	1
Security Policy Control	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	1
DoS Prevention	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	0
> System	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	0
> Security Service	<input type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	0
> VPN	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	0
> License	<input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	<input checked="" type="radio"/> <input type="radio"/> <input type="radio"/>	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.



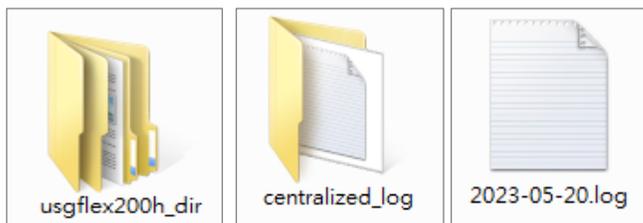
System Log Archives in USB Storage

Remove  Download

<input checked="" type="checkbox"/>	File Name ↕	Size ↕	Modified Time ↕
<input checked="" type="checkbox"/>	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



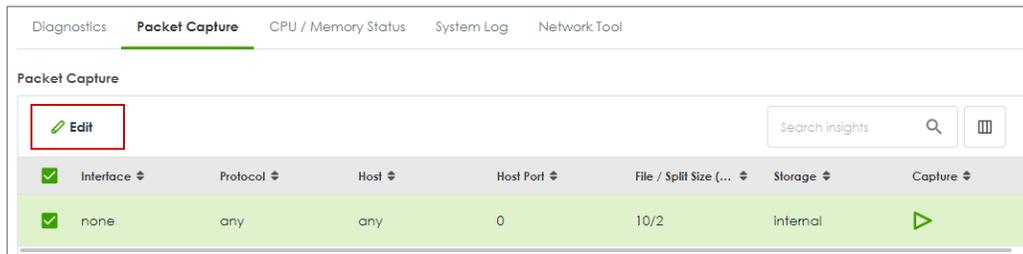
## How to Perform and Use the Packet Capture Feature

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.

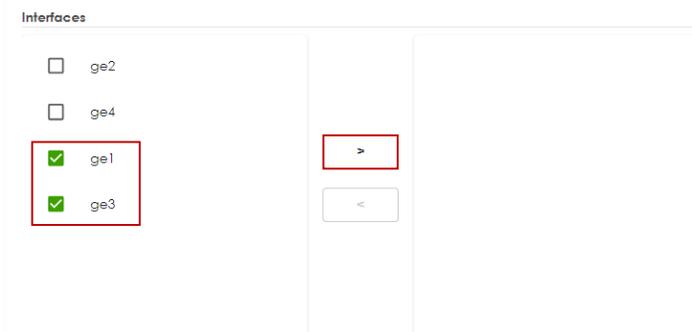
 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).

### 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.



- 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.

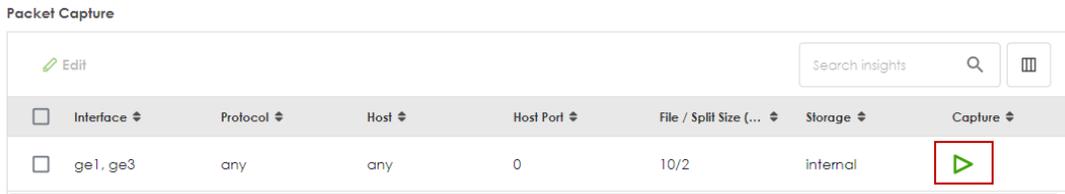
Select a Host IP address object for which to capture packets. Select any to capture packets for all hosts. Select User Defined to be able to enter an IP address.

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

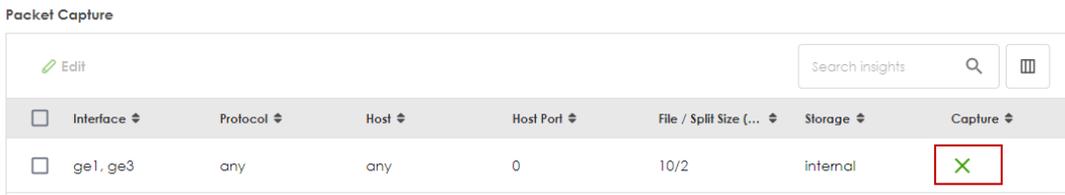
- In Misc setting, select "Save data to onboard storage only", "Save data to USB storage" or "Save data to ftp server".

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
<input checked="" type="radio"/> Save data to onboard storage only <input type="radio"/> Save data to USB storage <input type="radio"/> Save data to ftp server	

9. Click the icon to start capturing packets.

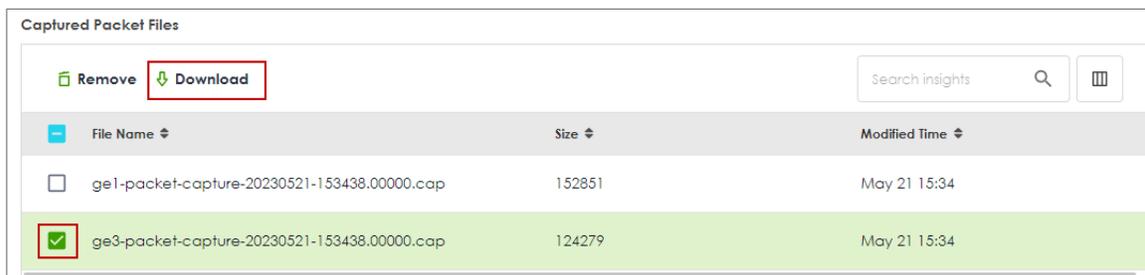


10. Click the icon to stop capturing packets.



## 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>"

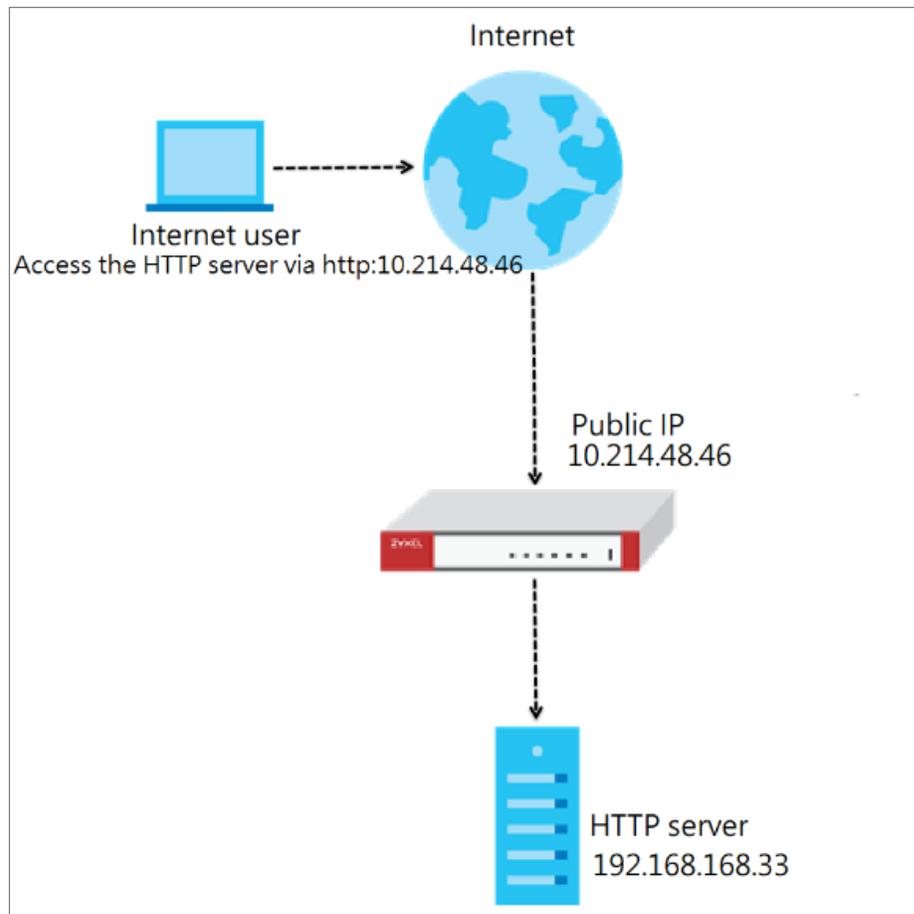
cmd traffic-capture <interface name> filter "port <port number>"

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

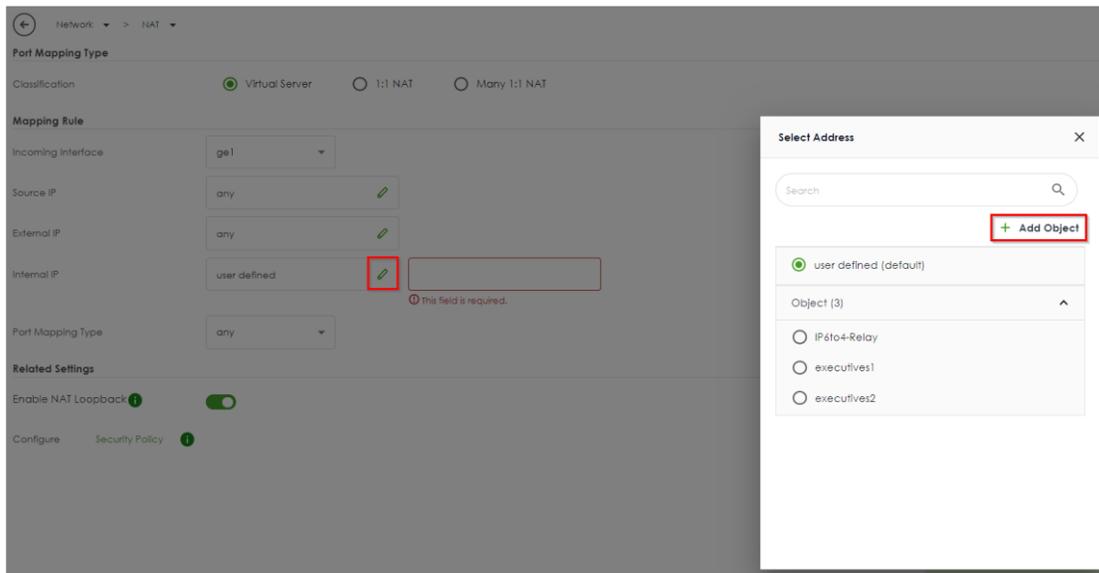
Here is an example of allowing access to the internal server behind a USG FLEX H device with network address translation (NAT). Internet users can access the server directly by its public IP address and a NAT rule will forward traffic from the internet to the local server in the intranet.



## 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.

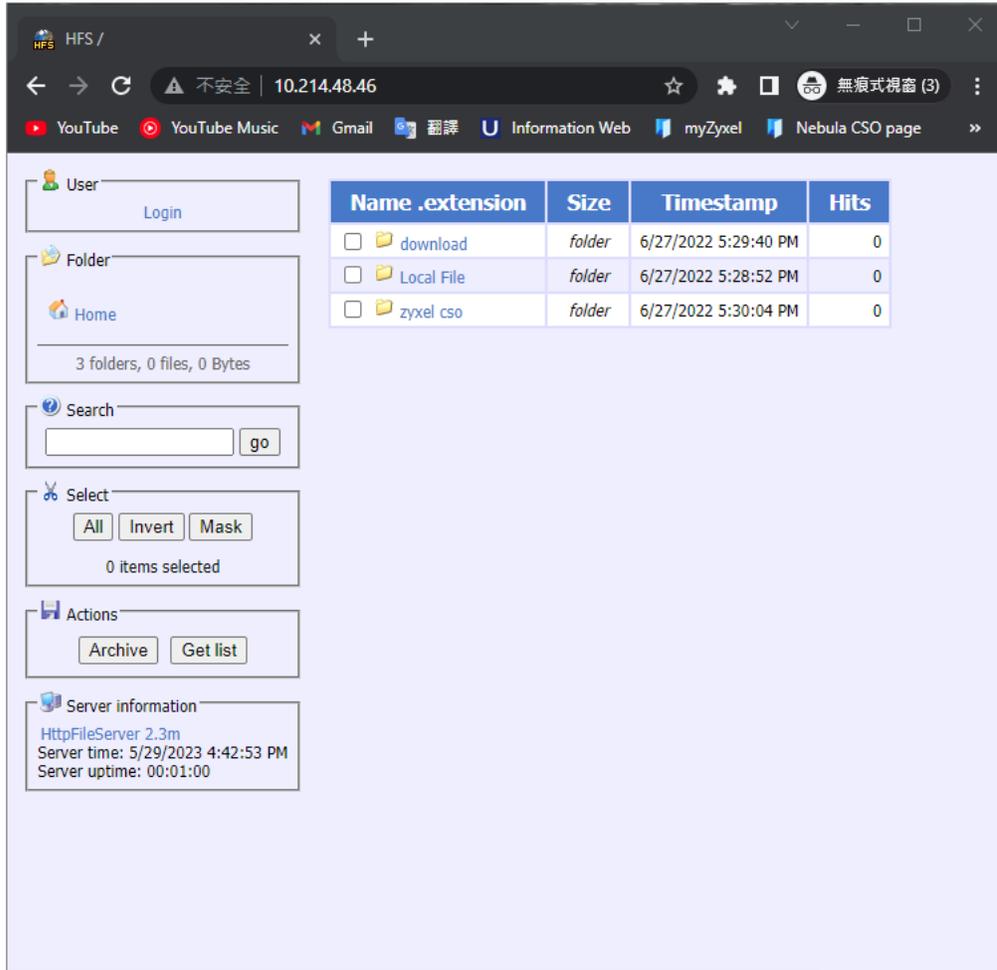


- Port Mapping Type: Select HTTP for both external and internal service.

The screenshot shows the configuration page for a NAT rule. The breadcrumb navigation is 'Network > NAT'. The page is divided into three sections: 'General Settings', 'Port Mapping Type', and 'Mapping Rule'.  
- In 'General Settings', 'Enable Rule' is turned on, and the 'Rule Name' is 'internal\_server'.  
- In 'Port Mapping Type', 'Classification' is set to 'Virtual Server' (indicated by a selected radio button).  
- In 'Mapping Rule', 'Incoming Interface' is 'ge1'. 'Source IP' is 'any'. 'External IP' is 'user defined' with a value of '10.214.48.46'. 'Internal IP' is 'internal\_server'. 'Port Mapping Type' is set to 'Service'. Below this, 'External Service' and 'Internal Service' are both set to 'HTTP'.

## Test the Result

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



## 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. The breadcrumb navigation is 'Network > Interface > External'. The page is divided into two sections: 'General Settings' and 'Interface Properties'. In the 'General Settings' section, the 'Enable Interface' toggle is turned on. The 'Interface Properties' section includes fields for Role (external), Interface Type (Ethernet), Interface Name (ge1), Port (p1 (ge1)), Zone (WAN), MAC Address (blank), and Description (blank). Under the 'Address Assignment' section, four radio buttons are visible: 'Unassigned', 'Get Automatically (DHCP)' (which is selected and highlighted in yellow), 'Use Fixed IP Address', and 'PPPoE'.

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

Advanced Settings

DHCP Option 60: CSO-FAQ

MTU: [Empty]

Default SNAT:

## Test DHCP Option 60

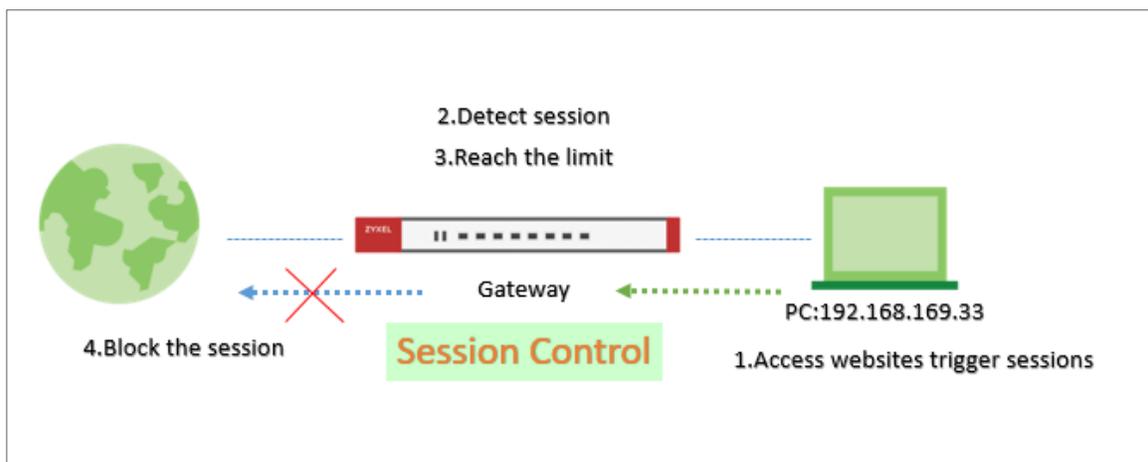
To check the functionality of DHCP Option 60, we can use packet capture software to check if option 60 string exists in the DHCP discover message that is sent from the USG FLEX H.

```

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 (...), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Dynamic Host Configuration Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0xee96c336
  Seconds elapsed: 0
  Bootp flags: 0x0000 (Unicast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 0.0.0.0
  Client MAC address: ZyxelCom_e7:e8:36 (...
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  > Option: (53) DHCP Message Type (Discover)
  > Option: (51) IP Address Lease Time
  > Option: (12) Host Name
  > Option: (55) Parameter Request List
  v Option: (60) Vendor class identifier
    Length: 7
    Vendor class identifier: CSO-FAQ
  > Option: (61) Client identifier
  > Option: (255) End
  Padding: 0000000000
  
```

## How to Configure Session Control

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



## Set Up the Session Control

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

← Security Policy > Session Control

**General Settings**

Session Control

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

Source Address

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
<input checked="" type="checkbox"/>	1	Zyxel	any		30

## Test the Result

Log in as User: Zyxel

**ZYXEL**  
NETWORKS

**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**

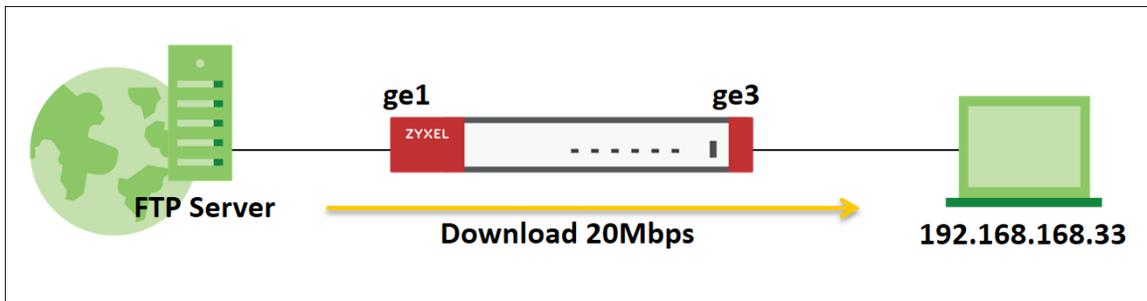
Try to access web browser to hit the session limit

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

Enable

Name BWM\_Per-IP

Description

BWM Type  Shared  Per user  Per-Source-IP ?

### Criteria

Incoming Interface

Outgoing Interface

Source  ✎

Destination  ✎

Service Type  Service Object  Application Group

Service Object  ✎

User  ✎

Schedule  ✎

### Traffic Shaping

Download Limit  Unlimited  Limit  Mbps

Upload Limit  Unlimited  Limit  Mbps

Priority

### Related Setting

Log

Incoming Interface: ge3

Outgoing Interface: ge1

Source: LAN1 IP Subnet

Application Group: FTP

Traffic Shaping: Download Limit 20 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.

## Different Scenarios:

### (1) Shared

If you select the "Shared" setting in the BWM rule, the selected IP addresses will share the configured bandwidth.

e.g. Limit the maximum FTP download bandwidth to 20 Mbps for whole of LAN1 PCs.

### (2) Per User

If you select the "Per User" setting in the BWM rule, each user will have a limited bandwidth.

e.g. Limit the maximum FTP download bandwidth to 20 Mbps for each user.

### (3) Per-Source-IP

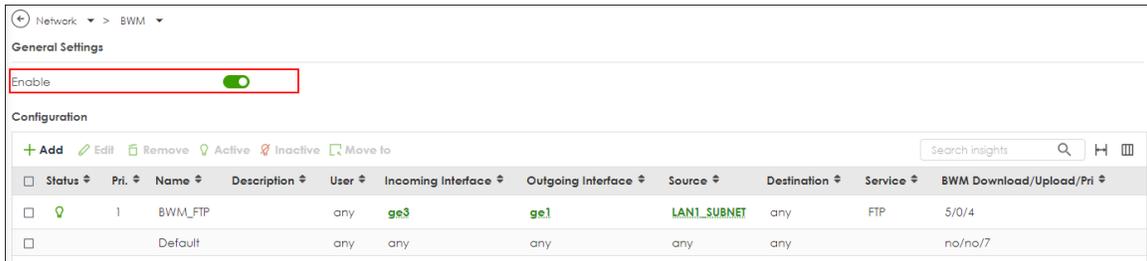
If you select the "Per-Source-IP" setting in the BWM rule, each selected IP address will have a limited bandwidth.

e.g. Limit the FTP download bandwidth for each LAN1 PC to 20 Mbps.



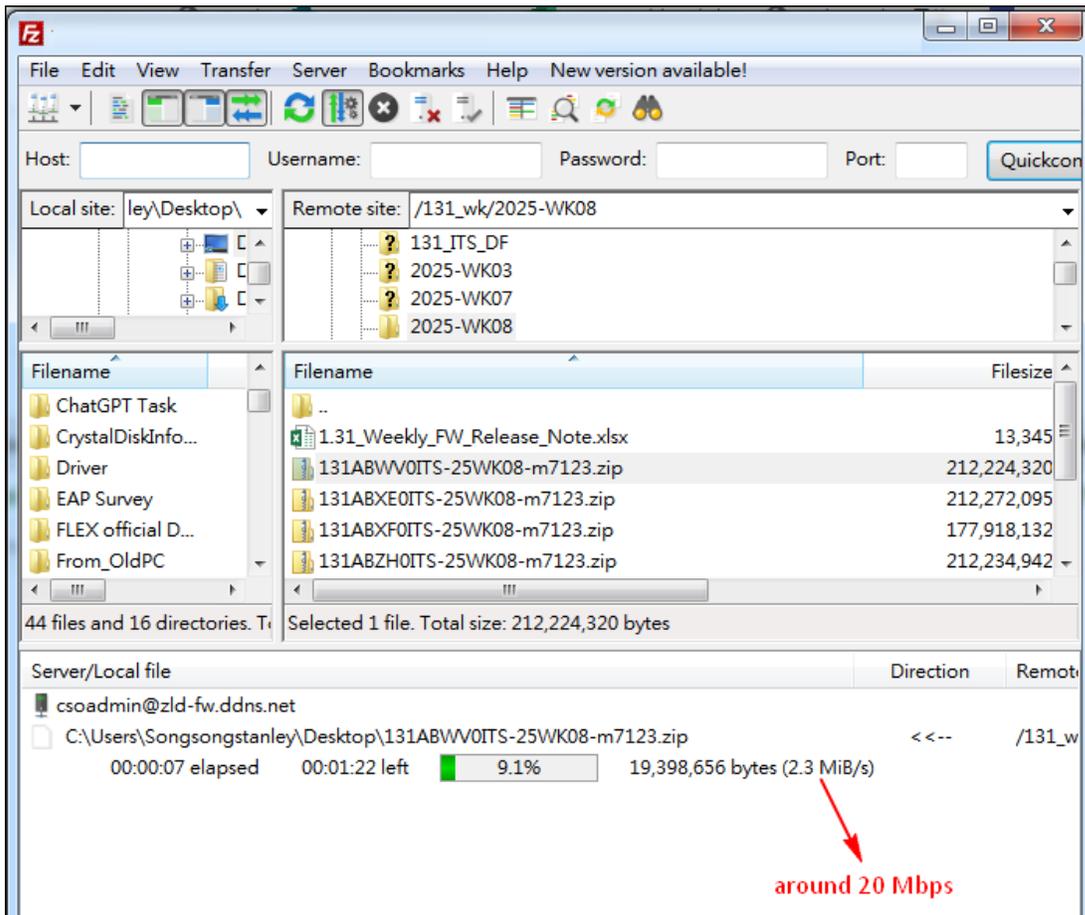
Note: If you select the "Per User" option or configure "User" as a condition, the Captive Portal service must be enabled, and the PC must be authenticated by the firewall first.

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

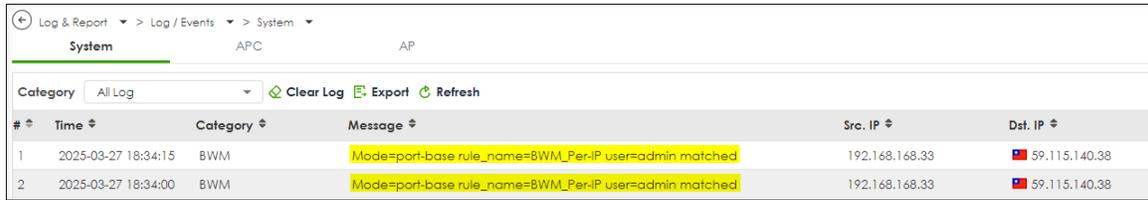


## Test the Result

The PC connect to LAN1 and download file by FTP. the download speed is around 20 Mbps.



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

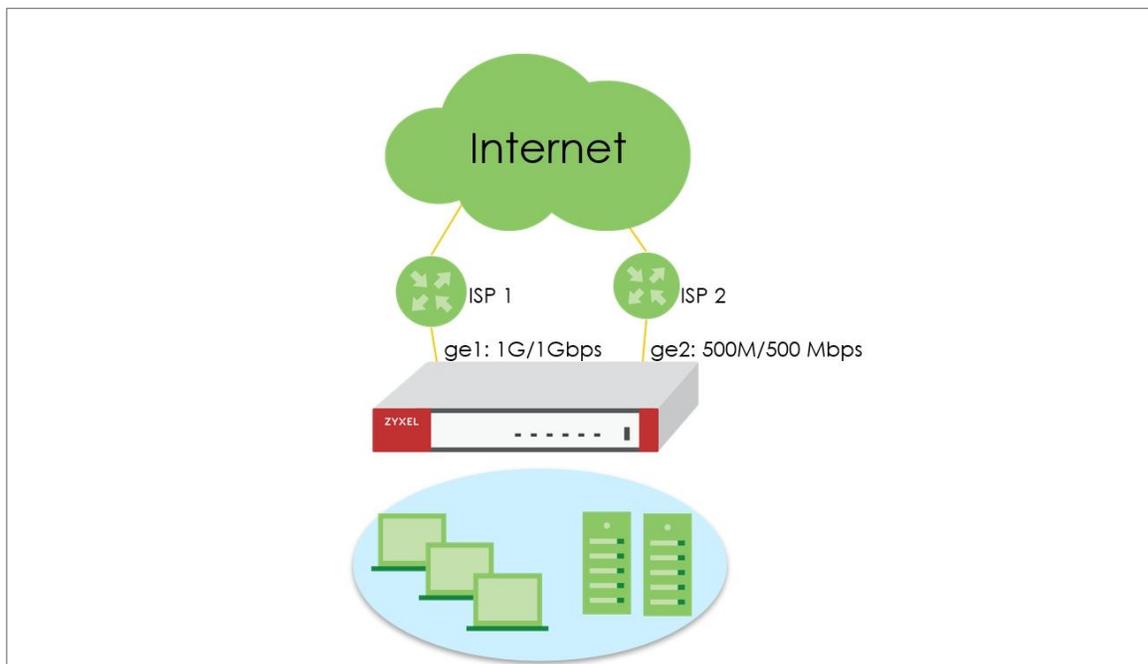


The screenshot shows the ZyXel Log & Report interface. The breadcrumb navigation is 'Log & Report > Log / Events > System'. The page title is 'System' with sub-headers 'APC' and 'AP'. The 'Category' dropdown is set to 'All Log'. There are buttons for 'Clear Log', 'Export', and 'Refresh'. The log table has columns for '#', 'Time', 'Category', 'Message', 'Src. IP', and 'Dst. IP'. Two log entries are visible, both with the message 'Mode=port-base rule\_name=BWM\_Per-IP user=admin matched'.

#	Time	Category	Message	Src. IP	Dst. IP
1	2025-03-27 18:34:15	BWM	Mode=port-base rule_name=BWM_Per-IP user=admin matched	192.168.168.33	59.115.140.38
2	2025-03-27 18:34:00	BWM	Mode=port-base rule_name=BWM_Per-IP user=admin matched	192.168.168.33	59.115.140.38

## 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 500M/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 2<sup>nd</sup> 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
<input type="checkbox"/> LLF	llf	ge1, ge2
<input type="checkbox"/> 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.

## How Does SIP ALG Function Work on USG FLEX H?

SIP ALG consists of two key services for managing traffic on firewalls: SIP transformation and SIP pinholes.

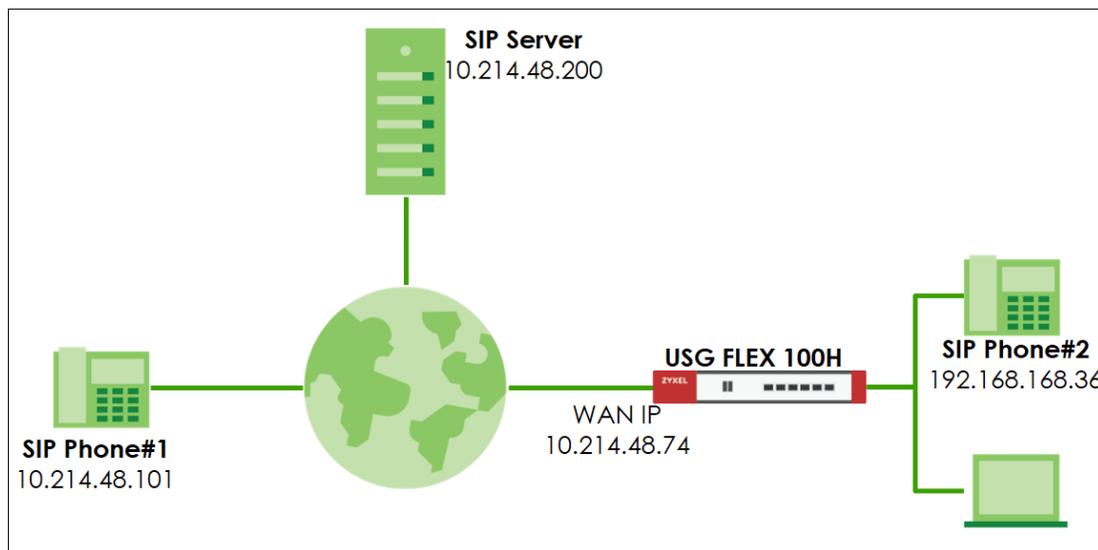
### SIP Transformation

The SIP transformation function modifies SIP header information, facilitating SIP signaling traffic over NAT operations. This enables seamless communication between private IP addresses and public IP addresses.

### SIP Pinholes

SIP pinholes ensure the persistence of registered SIP sessions and RTP sessions during NAT operations. This prevents issues such as dropped calls or non-functioning phone calls caused by expired SIP/RTP sessions on the firewall.

Cloud-based SIP servers are typically sophisticated enough to distinguish between a client's local (private IP) and public IP, making SIP transformation unnecessary in most scenarios. However, the SIP pinhole feature remains essential for proper NAT operations. The SIP ALG feature on H Series firewalls focuses on supporting SIP pinholes. This ensures that SIP and RTP sessions are managed effectively, maintaining reliable communication across firewalls.



## SIP ALG Feature for Keep SIP/RTP Activity Sessions on Firewall

Go to Network > ALG > SIP ALG feature.

Network > ALG

**FTP ALG**

Enable

Enable FTP Transformations

FTP Signaling Port  (1-65535)

Additional FTP Signaling Port  (1-65535) (Optional)

**SIP ALG**

Enable  ←

SIP Signaling Port

+ Add  Remove

Port
<input type="checkbox"/> 5060

SIP Inactivity Timeout

Media Inactivity Timeout  seconds

Signaling Inactivity Timeout  seconds

Restrict Peer to Peer Media Connection  ⓘ

Restrict Peer to Peer Signaling Connection

### SIP Signaling port:

Default SIP service port is 5060. You can configure to other ports to fulfil your network environment.

### SIP Inactivity timeout:

In firewall default setting, general UDP session timeout is 300 seconds, and UDP stream timeout is 60 seconds. (System > Advanced)

System > Advanced

**System Parameters**

Name	Description	Value
UDP Timeout (seconds)	The timeout for initial UDP packets in a connection. (seconds)	300 (seconds)
UDP Timeout Stream (seconds)	The timeout values of the UDP streams once they have sent enough packets. (seconds)	60 (seconds)
ICMP Timeout (seconds)	The timeout for ICMP connection. (seconds)	5 (seconds)

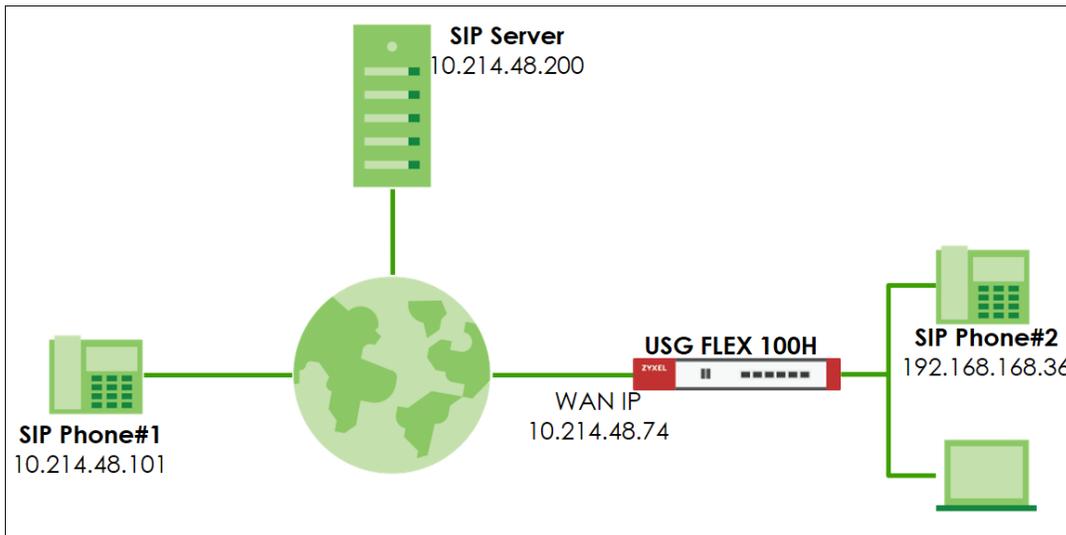
You can configure Media(RTP) and Signaling(SIP) timeout for your SIP phone, it could keep the sessions on firewall to prevent lost incoming phone call due to session expired.

**Peer to Peer connection restriction:**

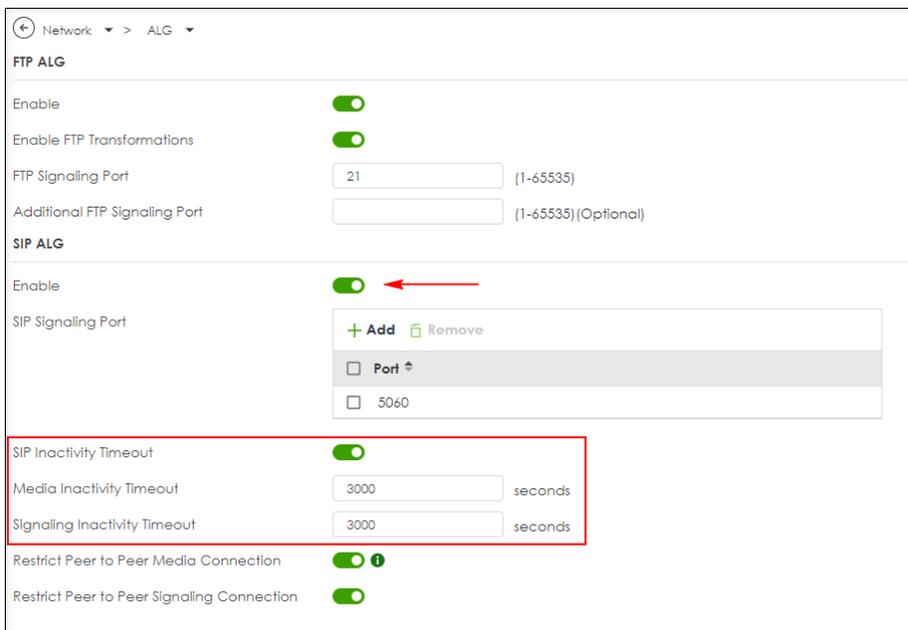
It is for incoming STP/RTP traffic. If the source IP address doesn't match to exist sessions, then firewall will drop the incoming traffic.

**Test the Result**

Dial the SIP phone call from SIP Phone#1 to SIP Phone#2.



Turn on SIP ALG feature and enable "SIP Inactivity Timeout" service, also have an extend Signaling(SIP) and Media(RTP) inactivity timeout as 3000 seconds.



Use CLI command to check exist sessions has been extended successfully.

**CLI> show contracks | match "<IP address>"**

Before enabling the SIP ALG feature, system will use the default UDP timeout.

```

usgflex100h> show contracks | match "192.168.168.36"
udp      17 294 src=192.168.168.36 dst=10.214.48.200 sport=10007 dport=11015 packets=1 bytes=92 [UNREPLIED]
src=10.214.48.200 dst=10.214.48.74 sport=11015 dport=10007 packets=0 bytes=0 mark=0 use=1
RTP session

udp      17 55 src=192.168.168.36 dst=10.214.48.200 sport=10006 dport=11014 packets=2 bytes=400
src=10.214.48.200 dst=10.214.48.74 sport=11014 dport=10006 packets=1 bytes=200 [ASSURED] mark=16777216 use=1

udp      17 55 src=192.168.168.36 dst=10.214.48.200 sport=5061 dport=5060 packets=2 bytes=1178
src=10.214.48.200 dst=10.214.48.74 sport=5060 dport=5061 packets=1 bytes=556 [ASSURED] mark=16777216 use=1
SIP session

usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>

```

After enabling the SIP ALG feature, system will extend the timeout value.

```

usgflex100h> show contracks | match "192.168.168.36"
udp      17 2999 src=192.168.168.36 dst=10.214.48.200 sport=10002 dport=10254 packets=9513 bytes=1902600
src=10.214.48.200 dst=10.214.48.74 sport=10254 dport=10002 packets=18665 bytes=3733000 [ASSURED] mark=0 helper=RTP use=1
RTP Session

udp      17 2995 src=192.168.168.36 dst=10.214.48.200 sport=10003 dport=10255 packets=36 bytes=3312
src=10.214.48.200 dst=10.214.48.74 sport=10255 dport=1025 packets=73 bytes=6716 [ASSURED] mark=0 helper=RTP use=1

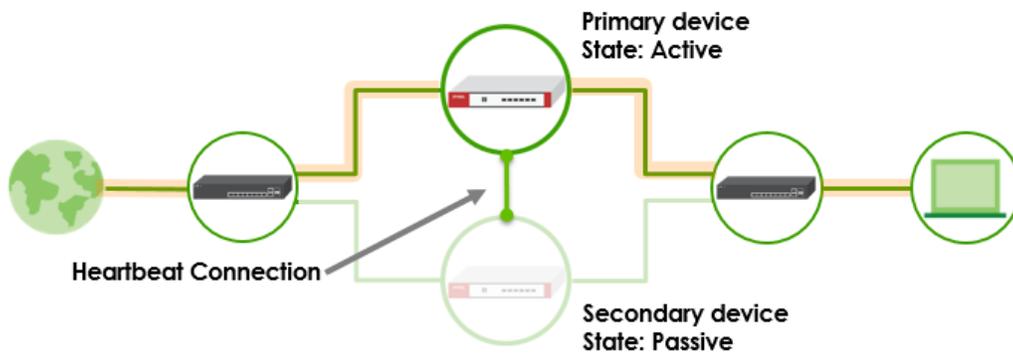
udp      17 2946 src=192.168.168.36 dst=10.214.48.200 sport=5061 dport=5060 packets=38 bytes=4235
src=10.214.48.200 dst=10.214.48.74 sport=5060 dport=5061 packets=5 bytes=2986 [ASSURED] mark=0 helper=sip use=3
SIP Session

usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>
usgflex100h>

```

## How to Deploy Device HA

The Device HA feature acts as a failover when one of the devices in the network fails or can't access the Internet. Device HA uses a dedicated heartbeat link between an active device and a passive device for status syncing and backup to the passive device. On the passive device, all ports are disabled except for the port with the heartbeat link. This example illustrates how to deploy the Device HA in your network.

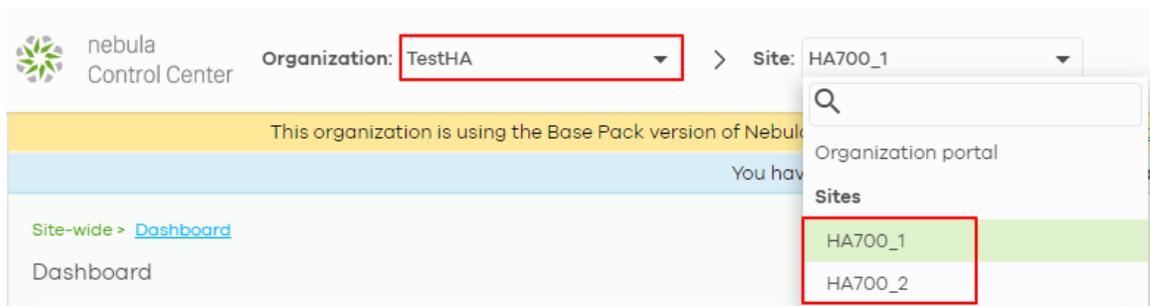


 Note: Device HA is supported on USG FLEX 200H, USG FLEX 200HP, USG FLEX 500H, USG FLEX 700H. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.32).

## Prerequisites for Device HA

The primary and secondary devices in Device HA mode must meet the following requirements:

1. **The same model** - Both devices must be of the same hardware model. In this example, both devices must be USG FLEX 200H. You cannot set up Device HA between different models, USG FLEX 200H and USG FLEX 200HP.
2. **The same firmware version** - Both devices must be running the same firmware version (uOS 1.31 or later versions).
3. **The same Organization on Nebula** - Both devices must be registered to the same Organization on Nebula.
  - Assign the primary USG FLEX H to the first site
  - Assign the secondary USG FLEX H to the second site



4. **Enable SSH port number** - The SSH service under System > SSH must be enabled on both devices. SSH port number must use **22** to enable synchronization for Device HA.
5. **WAN connection of the active device** - Ensure that the active device has normal WAN connectivity to the internet and is connected to Nebula.



Note: It is highly recommended to complete device registration steps on Nebula before pairing HA.

## Configuration on the primary device

1. Set up with your desired configuration and networking settings.
2. The highest-numbered copper Ethernet port is reserved for heartbeat communication. Make sure the heartbeat port is not assigned to any interface. In this example, P8 is the heartbeat port on USG FLEX 200H. **Remove** P8 from interface ge4.

**General Settings**

Enable Interface

---

**Interface Properties**

Role: internal

Interface Type: Ethernet

Interface Name: ge4

Port: p7 (ge4) ✕ p8 (ge4) ✕ ▼

Zone: LAN ▼

 **Note: Heartbeat port for HA synchronization**

USG FLEX 200H/200HP: P8

USG FLEX 500H/700H: P12

Go to Network > Interface and make sure p8 doesn't belong to any interface.

Network > Interface > Interface

Interface      Trunk      Port

---

External

+ Add Edit Remove Reference Active Inactive Connect Disconnect Search insights Q H ☰

Status	Name	Zone	Description	IP/Netmask	VLAN ID	Type	Members	Reference
<input type="checkbox"/>	ge1	WAN		10.214.48.99/255.255.255.0		Ethernet	p1	3
<input type="checkbox"/>	ge2	WAN		0.0.0.0/0.0.0.0		Ethernet	p2	1

Internal

+ Add Edit Remove Reference Active Inactive Search insights Q H ☰

Status	Name	Zone	Description	IP/Netmask	VLAN ID	Type	Members	Reference
<input type="checkbox"/>	ge3	LAN		192.168.168.1/255.255.255.0		Ethernet	p3,p4,p5,p6	2
<input type="checkbox"/>	ge4	LAN		192.168.169.1/255.255.255.0		Ethernet	p7	2

3. Go to **System > Device HA > HA Configuration**.

- Select Primary role.
- Select HA MAC address.

If Virtual MAC Address is selected, the MAC address of each interface will be replaced as follows.

D8:EC:E5:XX:XX:1D -> D6:EC:E5:XX:XX:1D

- Configure Management IP for active and passive role. The two management IPs must be different but in the same subnet.
- Select monitor interfaces. HA failover will be triggered when monitored interface is down. Turn on **“Enable”** to enable Device HA and Apply.

HA Status	HA Configuration	HA Log
<b>General Settings</b>		
Enable	<input checked="" type="checkbox"/>	
<b>Management Configuration</b>		
Initial Role	<input checked="" type="radio"/> Primary (License Controller)	
HA MAC address		<input type="radio"/> Physical MAC address <input checked="" type="radio"/> Virtual MAC address
	<input type="radio"/> Secondary	
Active Node Management IP	<input type="text" value="10.10.10.1"/>	
Passive Node Management IP	<input type="text" value="10.10.10.2"/>	
Management IP Subnet Mask	<input type="text" value="255.255.255.0"/>	
<b>Monitor Interface</b>		
Member	<input type="text" value="ge3"/>	
Failover on Monitored Interface Link Down		<input checked="" type="checkbox"/>
Failover on Monitored Connectivity Check Failure		<input type="checkbox"/>

## Configuration on the secondary device

1. Make sure the secondary device is reset to default settings. Follow the wizard to register it to Nebula and it to the same organization as the primary device.
2. After the secondary device is registered to Nebula successfully, remove wan connection from the secondary device and login to the device via lan interface to configure HA.
3. Make sure the heartbeat port is not assigned to any interface. In this example, P8 is the heartbeat port on USG FLEX 200H. **Remove** P8 from interface ge4.

General Settings	
Enable Interface	<input checked="" type="checkbox"/>
Interface Properties	
Role	internal
Interface Type	Ethernet
Interface Name	ge4
Port	<input type="text" value="p7 (ge4)"/> <input checked="" type="checkbox"/> <input checked="" style="border: 2px solid red;" type="checkbox"/> <input type="text" value="p8 (ge4)"/> <input checked="" type="checkbox"/>
Zone	LAN

4. Go to **System > Device HA > HA Configuration**. Select Secondary role. Turn on "Enable" to enable Device HA and Apply. Logout from the secondary device and unplug all Ethernet cables of wan and lan interfaces.

HA Status	HA Configuration	HA Log
General Settings		
Enable	<input checked="" style="border: 2px solid red;" type="checkbox"/>	
Management Configuration		
Initial Role	<input type="radio"/> Primary (License Controller) <input checked="" style="border: 2px solid red;" type="radio"/> Secondary	<input type="radio"/> Physical MAC address <input checked="" type="radio"/> Virtual MAC address
Active Node Management IP	<input type="text"/>	
Passive Node Management IP	<input type="text"/>	
Management IP Subnet Mask	<input type="text"/>	

## Connect the heartbeat ports

Connect the heartbeat ports of the primary and secondary device directly and avoid putting a device in between such as a switch.

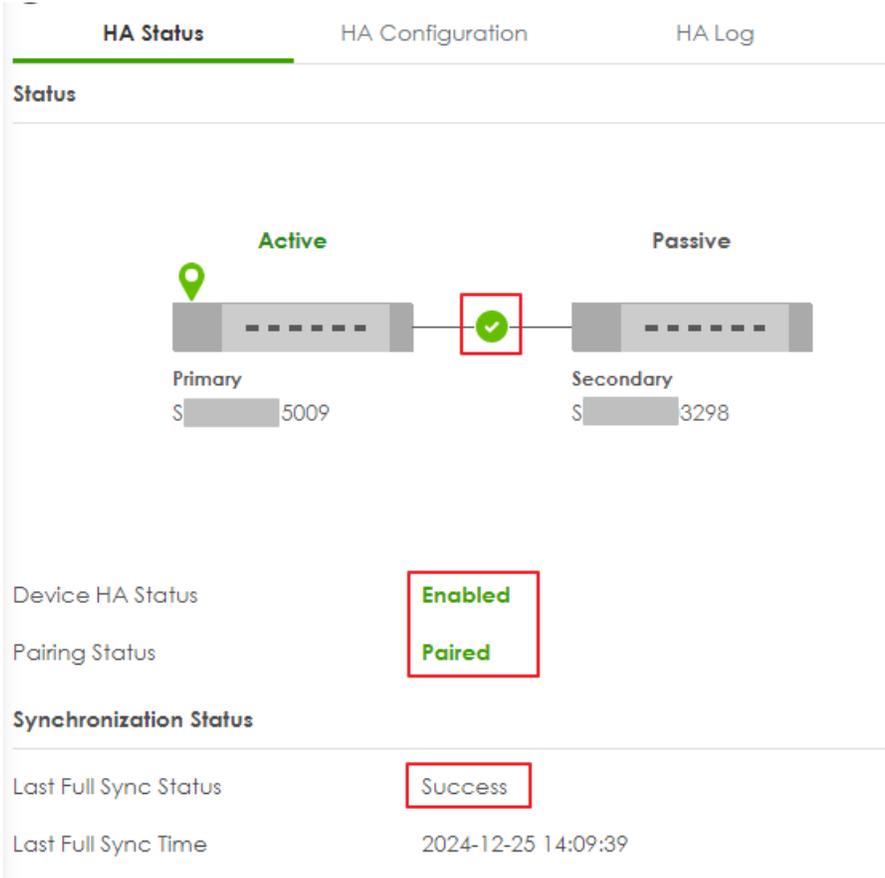
 Note: The heartbeat port of the primary and secondary device must be connected directly to each other (not through a switch).

## Check HA status

Login to the primary device and go to **System > Device HA > HA Status**. Make sure the heartbeat link status is connected. You can also use the [SYS LED](#) on the active device to check the pairing status.

Pairing status: Paired

Last Full Sync Status: Success



The screenshot displays the 'HA Status' page with three tabs: 'HA Status' (selected), 'HA Configuration', and 'HA Log'. The main content area shows a diagram of two devices: 'Primary' (IP 5009) and 'Secondary' (IP 3298). The Primary device is marked as 'Active' with a green location pin icon. A green checkmark in a red box is placed on the connection line between the two devices. Below the diagram, the 'Device HA Status' is 'Enabled', 'Pairing Status' is 'Paired', and 'Synchronization Status' shows 'Last Full Sync Status' as 'Success' and 'Last Full Sync Time' as '2024-12-25 14:09:39'. The 'Enabled', 'Paired', and 'Success' text elements are highlighted with red boxes.

You can also enter the command on the primary device to check HA status.

**usgflex200h> show state vrf main device-ha status**

Synchronization can take up to 5 minutes or so. Once it has finished synchronizing, you can verify if the settings are synchronized by accessing the passive device through Passive Node Management IP. Once pairing is complete, the secondary device's license will automatically be transferred to the primary device and you will receive an email notification.

```
usgflex200h0325> show state vrf main device-ha status
status
  enabled true
  initial-role primary
  pairing-state paired
  pairing-msg Paired
  ha-health-state connected
  local-state active
  local-role primary
  active
    role primary
    sn S21[REDACTED]5009
    icon-color on
    ..
  passive
    role secondary
    sn S22[REDACTED]3298
    icon-color on
    ..
  ..
```

If Paring Status is not "Paired", check what the error message is and resolve the error. In this example, the error is "Device firmware mismatch". Check the firmware version on primary and secondary again and make sure firmware version on both devices are identical.

System > Device HA > HA Status

HA Status | HA Configuration | HA Log

Status



Device HA Status: **Enabled**

Pairing Status: Device firmware or model mismatch detected

 Note: After the error is resolved (Upgrade two devices to the same firmware version), you can keep the heartbeat port connected on both devices, and disable and enable HA on the **primary** device to trigger pairing again.

HA Status | **HA Configuration** | HA Log

**General Settings**

Enable:

**Management Configuration**

Active Node Management IP: 10.10.10.1

Passive Node Management IP: 10.10.10.2

Management IP Subnet Mask: 255.255.255.0

**Monitor Interface**

Member: ge1 

Failover on Monitored Interface Link Down:

Failover on Monitored Connectivity Check Failure:

## HA Synchronization

- Full Synchronization: Use the command on active device to manually force a full synchronization. You can also use [SYS LED](#) on the passive device to check the status of HA synchronization.

***usgflex200h> cmd device-ha force-sync full***

- Incremental Synchronization: This happens automatically when changes are made to the active firewall. The updates are synced to the passive firewall within 5 seconds. It is important to only make configuration changes on the active device.



Note: All configuration changes must be made on the active device. Do NOT manually configure the passive device.

## Connect the network cables to the secondary device

Once the devices have been properly synchronized, connect all network cables to wan and lan interfaces of the secondary devices.

## Test HA Failover

1. In this example, ge1 is the monitored interface. Unplug the Ethernet cable of ge1 interface from the primary device to trigger HA failover.

**Monitor Interface**

Member ge1

Failover on Monitored Interface Link Down

Failover on Monitored Connectivity Check Failure

2. Check HA Status and HA log by accessing Active Node Management IP <https://10.10.10.1>. In HA Status, the secondary device becomes Active role.

**Active Node**

System > Device HA > HA Status

HA Status | HA Configuration | HA Log

The diagram shows two nodes connected by a link with a green checkmark. The left node is labeled 'Active' and 'Secondary' with IP address 'S [redacted] 3298'. The right node is labeled 'Passive' and 'Primary' with IP address 'S [redacted] 5009'.

Device HA Status: **Enabled**

Pairing Status: **Paired**

**Synchronization Status**

Last Full Sync Status: Success

Last Full Sync Time: 2024-12-25 14:10:53

**Failover Status**

Failover Reason: **Monitor interface link down**

Last Failover Time: 2024-12-25 14:57:38

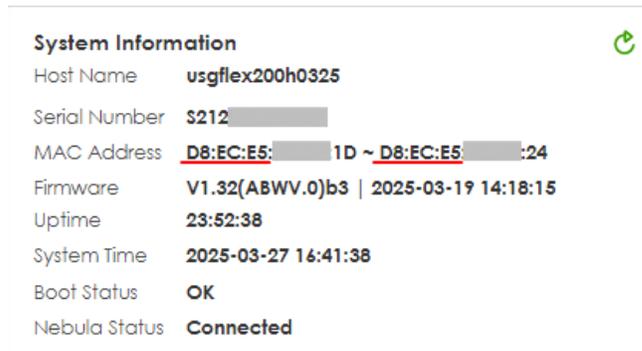
In HA Log, the secondary device (Local) changes the state from Passive to Active.



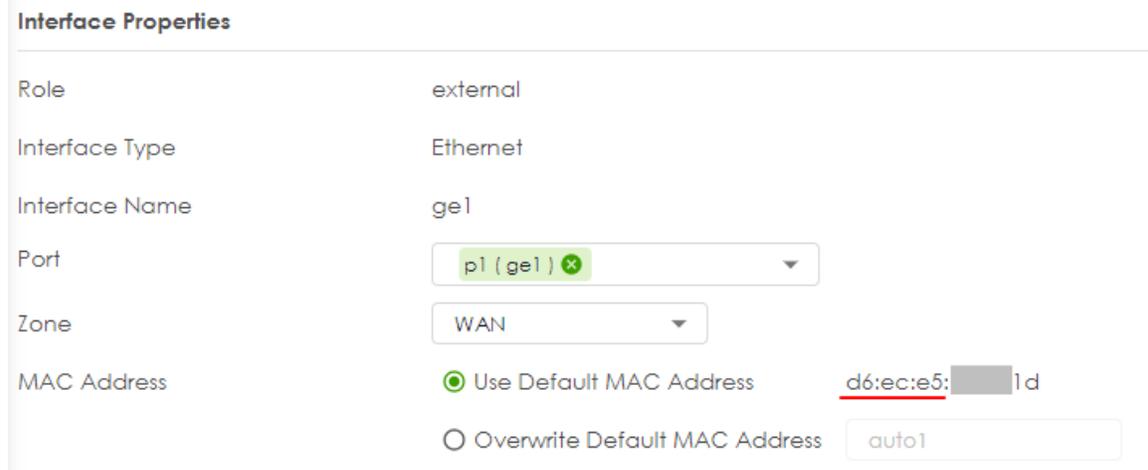
## Check Virtual MAC Address

### Active Device

On Dashboard > System Information, MAC address is the physical MAC address.



In Network > Interface, it shows the Virtual MAC address.



**Interface Properties**

---

Role: internal

Interface Type: Ethernet

Interface Name: ge3

Port: p3 (ge3) ✕ p4 (ge3) ✕ p5 (ge3) ✕ p6 (ge3) ✕

Zone: LAN

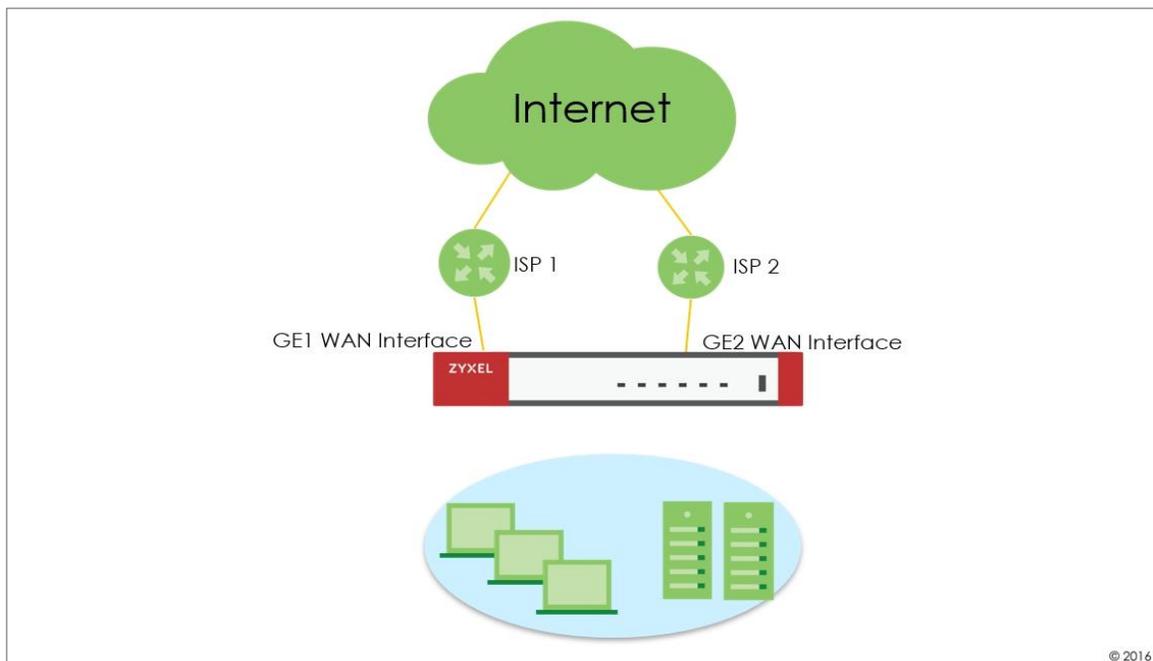
MAC Address:  Use Default MAC Address d6:ec:e5: [redacted]:1f  
 Overwrite Default MAC Address auto3

### SYS LED Status

State	SYS LED on Active Device	SYS LED on Passive Device
Pairing in Progress	Alternating Green on: 500ms, Red on: 500ms  	Green Solid 
Pairing fail	Red Blinking (1sec) 	Green Solid 
Sync. in Progress	Green Solid 	Amber Blinking (500ms) 
Sync. Completed	Green Solid 	Amber Solid 
Active Node Running	Green Solid 	Amber Solid 

## How to check Packet Flow Explorer

The Packet Flow Explorer is a powerful tool for analyzing and understanding routing-related issues. When used correctly, it offers a basic overview of your firewall's configuration without requiring an in-depth examination. This example demonstrates how to check the routing and SNAT status using the Packet Flow Explorer.



 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 1.31).

## Scenario and Requirement

1. Dual WAN interfaces are in the default WRR mode, and both WANs are active.

Name	Default										
<b>Load Balancing Setting</b>											
Algorithm	wrr										
<table border="1"> <thead> <tr> <th>Interface</th> <th>Mode</th> <th>Parameter</th> </tr> </thead> <tbody> <tr> <td>ge1</td> <td>Active</td> <td>1</td> </tr> <tr> <td>ge2</td> <td>Active</td> <td>1</td> </tr> </tbody> </table>			Interface	Mode	Parameter	ge1	Active	1	ge2	Active	1
Interface	Mode	Parameter									
ge1	Active	1									
ge2	Active	1									

2. A static route is configured to route traffic to 8.8.8.8 from the GE2 WAN interface.

Policy Route		<b>Static Route</b>			
<b>Configuration</b>					
<span>+ Add</span> <span>Edit</span> <span>Remove</span> <span>Refresh</span>					
<input type="text" value="Search insights"/>					
Status	Name	Destination	Next Hop	Description	Metric
<input type="checkbox"/>	Google_DNS	8.8.8/32	ge2		0

3. A policy route is configured to route all internet traffic through the GE1 WAN interface when source is LAN1 subnet.

Policy Route		Static Route													
<b>Configuration</b>															
<span>+ Add</span> <span>Edit</span> <span>Remove</span> <span>Active</span> <span>Inactive</span> <span>Move to</span> <span>Refresh</span>															
<input type="text" value="Search insights"/>															
Status	Pri.	User	Schedule	Incoming	Source	Destination	DSCP Code	Service	Source Port	Next Hop	DSCP Marking	SNAT	Hits		
<input type="checkbox"/>	1	any	none	ge3	LAN1_SUBNET	any	any	any	any	ge1	preserve	outgoing-interface	0		

Based on the configuration above, we expect that if a host is placed in the LAN 1 subnet, all traffic will be routed through the GE1 WAN interface, except for traffic to 8.8.8.8, which will be routed through the GE2 WAN interface.

## Verification

1. Place a host in the LAN1 subnet, then run the command **ping 8.8.8.8 -t** in the Windows Command Prompt to check for ICMP response from 8.8.8.8.

```
C:\Users\NT122546>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=9ms TTL=57
Reply from 8.8.8.8: bytes=32 time=8ms TTL=57
Reply from 8.8.8.8: bytes=32 time=6ms TTL=57
Reply from 8.8.8.8: bytes=32 time=7ms TTL=57
Reply from 8.8.8.8: bytes=32 time=6ms TTL=57
Reply from 8.8.8.8: bytes=32 time=6ms TTL=57
```

The host receives ICMP response.

2. Confirm that the traffic is being sent out through the GE2 WAN interface, as per the static route configuration.

Type the command **cmd traffic-capture ge2 filter "host 8.8.8.8"** to capture packets on the GE2 WAN interface and verify that the traffic is being sent out through the GE2 WAN interface.

```
usgflex200h> cmd traffic-capture ge2 filter "host 8.8.8.8"
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge2, link-type EN10MB (Ethernet), capture size 262144 bytes
█
```

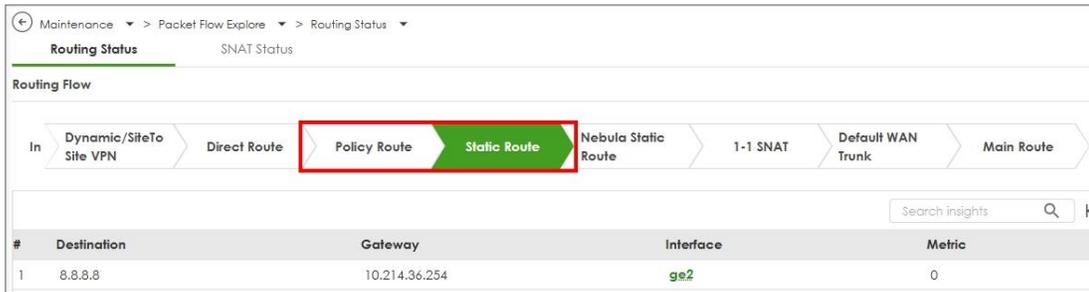
We're unable to see packets to 8.8.8.8. Let's capture the packets on the GE1 WAN interface instead.

**cmd traffic-capture ge1 filter "host 8.8.8.8"**

```
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge1, link-type EN10MB (Ethernet), capture size 262144 bytes
09:59:42.856070 d8:ec:e5:7c:df:dd > d2:ec:32:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34317, length 74
09:59:42.862565 d2:ec:32:78:a1:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34317, length 74
09:59:43.869372 d8:ec:e5:7c:df:dd > d2:ec:32:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34318, length 74
09:59:43.874648 d2:ec:32:78:a1:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34318, length 74
09:59:44.882064 d8:ec:e5:7c:df:dd > d2:ec:32:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34319, length 74
09:59:44.886659 d2:ec:32:78:a1:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34319, length 74
09:59:45.895654 d8:ec:e5:7c:df:dd > d2:ec:32:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.48.37 > 8.8.8.8: ICMP echo request, id 1, seq 34320, length 74
09:59:45.898654 d2:ec:32:78:a1:18 > d8:ec:e5:7c:df:dd, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.48.37: ICMP echo reply, id 1, seq 34320, length 74
```

Traffic to 8.8.8.8 is being sent out through the GE1 WAN interface, indicating that the static route is not working as expected.

3. Go to **"Maintenance > Packet Flow Explorer > Routing Status"** to check for possible issues.



As we can see, the policy route has a higher priority than the static route, causing traffic to 8.8.8.8 to be affected by the policy route.



We can try temporarily disabling the policy route to see if traffic to 8.8.8.8 goes through the GE2 WAN interface.

**cmd traffic-capture ge2 filter "host 8.8.8.8"**

```
usgflex200h> cmd traffic-capture ge2 filter "host 8.8.8.8"
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge2, link-type EN10MB (Ethernet), capture size 262144 bytes
10:40:33.037025 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36708, len 74
10:40:38.034168 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36709, len 74
10:40:43.036771 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36710, len 74
10:40:48.033310 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36711, len 74
10:40:53.035280 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36712, len 74
```

Now we can see the traffic to 8.8.8.8 appearing on the GE2 WAN interface. However, there is no ICMP response from the uplink router. Upon checking the source IP, it is the LAN host's IP, but it should be the GE2 WAN interface IP. The result shows that the firewall GE2 WAN interface does not have source NAT.

```
usgflex200h> cmd traffic-capture ge2 filter "host 8.8.8.8"
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge2, link-type EN10MB (Ethernet), capture size 262144 bytes
10:40:33.037025 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36708, len 74
10:40:38.034168 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36709, len 74
10:40:43.036771 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36710, len 74
10:40:48.033310 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36711, len 74
10:40:53.035280 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 192.168.168.33 > 8.8.8.8: ICMP echo request, id 1, seq 36712, len 74
```

4. Go to **“Maintenance > Packet Flow Explorer > SNAT Status”** to check for possible issues.

#	Incoming	Outgoing	SNAT
1	Internal Interface	External Interface	Outgoing Interface IP
2	Remote Access VPN	External Interface	Outgoing Interface IP

Mouse over the External interface. It indicates that SNAT is off on the GE2 WAN interface. This would be a misconfiguration on the GE2 WAN interface.

#	Incoming	Outgoing	SNAT
1	Internal Interface	External Interface	Outgoing Interface IP
2	Remote Access VPN	External Interface	Outgoing Interface IP

We can go to **“Network > Interface > Interface”**, and double click ge2 to tick SNAT.

DHCP Option 60

MTU  Bytes

**Default SNAT**

Change to a Different ISP  *i*

The above scenario is a simple example for checking routing and SNAT status in Packet Explorer.

## Test the Result

Generate ICMP traffic from LAN hosts to 8.8.8.8 and confirm if the traffic is sent out through the GE2 WAN interface.

1. Run the command **ping 8.8.8.8 -t** in the Windows Command Prompt to check if it has an ICMP response from 8.8.8.8.

```
C:\Users\NT122546>ping 8.8.8.8 -t

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
Reply from 8.8.8.8: bytes=32 time=3ms TTL=56
Reply from 8.8.8.8: bytes=32 time=4ms TTL=56
```

2. Type the command **cmd traffic-capture ge2 filter "host 8.8.8.8"** to capture packets on the GE2 WAN interface and check if the traffic is sent out through the GE2 WAN interface.

```
usgflex200h> cmd traffic-capture ge2 filter "host 8.8.8.8"
tcpdump2: verbose output suppressed, use -v or -vv for full protocol decode
listening on ge2, link-type EN10MB (Ethernet), capture size 262144 bytes
15:51:47.733935 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.36.49 > 8.8.8.8: ICMP echo request, id 1, seq 26449, length 74
15:51:47.738151 d2:ec:30:78:a1:18 > d8:ec:e5:7c:df:de, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.36.49: ICMP echo reply, id 1, seq 26449, length 74
15:51:48.747899 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.36.49 > 8.8.8.8: ICMP echo request, id 1, seq 26450, length 74
15:51:48.751677 d2:ec:30:78:a1:18 > d8:ec:e5:7c:df:de, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.36.49: ICMP echo reply, id 1, seq 26450, length 74
15:51:49.773147 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.36.49 > 8.8.8.8: ICMP echo request, id 1, seq 26451, length 74
15:51:49.777213 d2:ec:30:78:a1:18 > d8:ec:e5:7c:df:de, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.36.49: ICMP echo reply, id 1, seq 26451, length 74
15:51:50.780712 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.36.49 > 8.8.8.8: ICMP echo request, id 1, seq 26452, length 74
15:51:50.784007 d2:ec:30:78:a1:18 > d8:ec:e5:7c:df:de, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.36.49: ICMP echo reply, id 1, seq 26452, length 74
15:51:51.789695 d8:ec:e5:7c:df:de > d2:ec:30:78:a1:18, ethertype IPv4 (0x0800), length 74: 10.214.36.49 > 8.8.8.8: ICMP echo request, id 1, seq 26453, length 74
15:51:51.793041 d2:ec:30:78:a1:18 > d8:ec:e5:7c:df:de, ethertype IPv4 (0x0800), length 74: 8.8.8.8 > 10.214.36.49: ICMP echo reply, id 1, seq 26453, length 74
```

## How to set up a Link Aggregation Group (LAG) interface

A Link Aggregation Group (LAG) combines multiple Ethernet ports into a single logical link, LAG interface, between network devices. It helps to increase bandwidth and provide link redundancy.

The LAG interface of Zyxel USG FLEX H firewalls combines multiple Ethernet interfaces as members and supports three types of modes, Active-Backup, LACP (802.3ad), and Static.

### Prerequisites of Ethernet interface member

To be a member of LAG interface, the Ethernet interface must Meet all of the following conditions:

1. The Ethernet interface can only bind to one port. And the port cannot be used by other VLAN interface.
2. The Ethernet interface cannot be a member of other bridge, or LAG interface.
3. It does not have an IP address (must be set to unassigned).
4. It cannot have MAC address overwrite settings, must use default MAC address.
5. The interface must not be referenced by any other configurations except the Zone.

## Create a LAG interface

1. Edit the member Ethernet interfaces and make sure the MAC address is set to use default MAC address and the Address Assignment is set to unassigned.

← Network > Interface > Interface

**General Settings**

Enable Interface

**Interface Properties**

Role: internal

Interface Type: Ethernet

Interface Name: ge5

Port: p8 (ge5)

Zone: LAN

MAC Address:  Use Default MAC Address fc:22:f4:f6:91:4c  
 Overwrite Default MAC Address auto8

Description:

Address Assignment:  Unassigned  Use Fixed IP Address

IP/Network Mask:

2. Click +Add to create an interface and select the Interface Type as LAG.

← Network > Interface > Interface

**General Settings**

Enable Interface

**Interface Properties**

Role: internal

Interface Type: LAG

Name:

Zone:

MAC Address:

characters. The valid characters are [a-z][A-Z]+[0-9][a-z][A-Z][\_-].

 Note:

- LAG support interface Role: **External, Internal** and **General**
- When the interface role is external, the LAG IP address does not support PPPoE or PPPoE with a static IP

3. Select the LAG mode

Name

Zone

MAC Address  Use Default MAC Address  
 Overwrite Default MAC Address

Description

Address Assignment  Unassigned  Use Fixed IP Address  
 IP/Network Mask

Secondary IP

+ Add - Remove

IP/Netmask ↕

No data

Members i

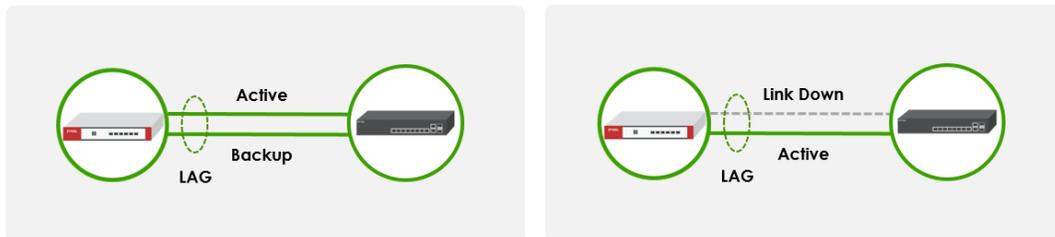
Mode   
 (1-1000)ms

Mii Monitoring Interval

Primary

## LAG mode: Active-Backup

Provides automatic link failover by keeping backup ports not transmitting traffic until the primary port experiences a link-down event.



**Mii Monitoring Interval:** Defines how frequently the system checks if a LAG member interface is active or down

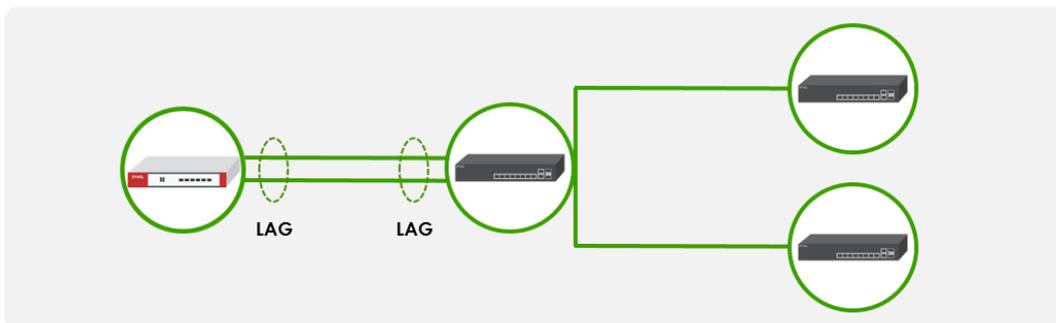
**Primary:** Allows you to specify which member interface should be preferred as the active link

Members <span style="color: green;">i</span>	ge5 <span style="color: green;">x</span> ge6 <span style="color: green;">x</span>
Mode	active-backup
Mii Monitoring Interval	100 (1-1000)ms
Primary	ge5

## LAG mode: LACP (802.3ad)

Provides automatic link failover and load sharing by allowing all ports in the LAG group to transmit traffic. The LACP messages will be periodically sent.

When in LACP mode, the connected Switch must also configure LACP mode for the physical ports that connect to the USG FLEX H Firewall.



**Transmit Hash Policy:** Determine how outgoing traffic is distributed across the aggregated links. The default option is **src-dst-ip-mac**. Select **src-dst-ip-mac** to distribute traffic more efficiently by considering both source-destination IP and MAC.

Members <span style="color: green;">i</span>	ge5 <span style="color: green;">x</span> ge6 <span style="color: green;">x</span>
Mode	lacp (802.3ad)
Mii Monitoring Interval	100 (1-1000)ms
Transmit Hash Policy	src-dst-ip-mac

### LAG Mode: Static

All ports in the LAG group will be always active for link failover and load balancing. The use case is when using legacy networking equipment that doesn't support LACP. When in LACP mode, the connected Switch must also configure LACP mode for the physical ports that connect to the USG FLEX H Firewall. When in Static mode, the connected Switch must also configure Static Trunk mode for the physical ports that connect to the USG FLEX H Firewall.

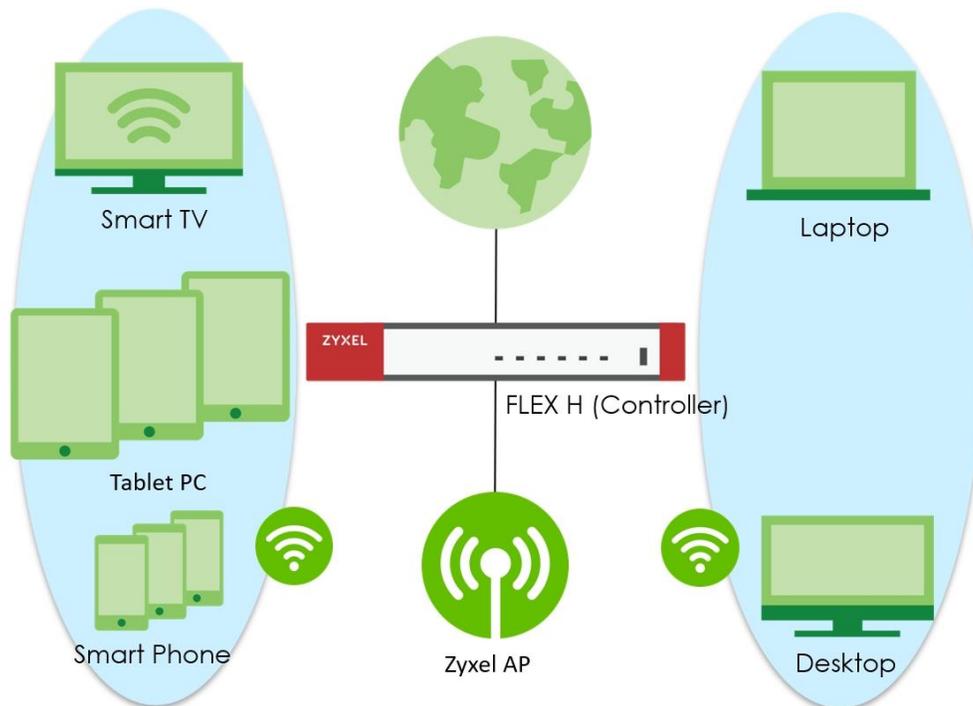
Members <span style="color: green;">i</span>	ge5 <span style="color: green;">x</span> ge6 <span style="color: green;">x</span>
Mode	static
Mii Monitoring Interval	100 (1-1000)ms
Transmit Hash Policy	src-dst-ip-mac

## Checked by CLI: show state vrf main interface lag

```
usgflex500h> show state vrf main interface lag
lag LAG-ge-5-6
  mtu 1500
  promiscuous false
  enabled true
  ethernet
    mac-address fc:22:f4:f6:91:4d
  ..
  ipv4
    address 172.198.1.1/24
    primary-address 172.198.1.1/24
  ..
  network-stack
    ipv4
      send-redirects true
      accept-redirects false
      accept-source-route false
      arp-announce any
      arp-filter false
      arp-ignore any
      arp-proxy false
      log-invalid-addresses false
    ..
    ipv6
  :...skipping...
lag LAG-ge-5-6
  mtu 1500
  promiscuous false
  enabled true
  ethernet
    mac-address fc:22:f4:f6:91:4d
  ..
  ipv4
    address 172.198.1.1/24
    primary-address 172.198.1.1/24
  ..
  network-stack
    ipv4
      send-redirects true
      accept-redirects false
      accept-source-route false
      arp-announce any
      arp-filter false
```

## How to Set Up AP Control Service for Zyxel APs

In today's digital landscape, wireless networks have become a critical infrastructure for businesses and organizations. As the number of connected devices continues to rise and network demands grow, managing and optimizing wireless environments has become increasingly challenging. Serving as the backbone of centralized Wi-Fi management, wireless controllers play a vital role in enhancing network stability, security, and operational efficiency. This article delves into the key functions of wireless controllers, their application scenarios, and their importance in enterprise network architecture. This is an example of using USG FLEX H series to manage the Zyxel Access Points (APs) and allow wireless access to the network.



 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.32).

## Set Up the AP Management on the FLEX H series

In the USG FLEX H, go to Wireless > AP Control Service, enable the AP Management Service, and set the AP login password.

### Wireless > AP Control Service

Wireless > AP Control Service

**AP Management Service**

Enable

AP Login Password

Retype to Confirm

**Note**  
This password is for the AP admin account. Use it with username 'admin' to log in to the AP.

Connect the Zyxel AP unit to the lan interface.

Go to Wireless > Access Points > AP List. The Zyxel AP will be listed under Unmanaged AP tab. Tick the AP and click "Add to Managed AP List".

### Wireless > Access Points > AP List > Unmanaged AP

Wireless > Access Points > AP List

AP List Policy AP Firmware

Managed AP **Unmanaged AP**

Add to Managed AP List

Search insights

<input checked="" type="checkbox"/> Name	IP Address
<input checked="" type="checkbox"/> AP-F4:4D:5C:9D:D8:A8	192.168.168.38

Once the actions above are completed, the AP will be listed in the Managed AP tab.

**Wireless > Access Points > AP List > Managed AP**

Firmware Status	Status	Name	IP Address	Model	Current Client	MAC Address	2.4GHz	5GHz	6GHz	Uplink	Power Mode
Update Available	✓	AP-F44D5C9DD8A8	192.168.168.38	WBE660S	0	F4:4D:5C:9D:D8:A8	n/a	n/a	n/a	ETHERNET	Limited

Note: The APs may take few minutes to appear in the Managed AP List.

Go to Wireless > WLAN Settings > SSID Settings to configure a name for the SSID and set a password for WLAN security.

**Wireless > WLAN Settings > SSID Settings**

#	Enabled	Name	WLAN Security
1	<input checked="" type="checkbox"/>	Zyxel_Wireless_Network	<input type="radio"/> Open <input checked="" type="radio"/> Password: [password field]
2	<input type="checkbox"/>	SSID2	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
3	<input type="checkbox"/>	SSID3	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
4	<input type="checkbox"/>	SSID4	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
5	<input type="checkbox"/>	SSID5	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
6	<input type="checkbox"/>	SSID6	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
7	<input type="checkbox"/>	SSID7	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
8	<input type="checkbox"/>	SSID8	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]

## Test the Result

Go to Wireless > Access Points > AP List > Managed AP tab. You can check the list of APs currently connected, along with detailed information such as IP address, model name, current clients, MAC address, and radio information.

### Wireless > Access Points > AP List > Managed AP

Firmware Status	Status	Name	IP Address	Model	Current Client	MAC Address	2.4GHz	5GHz	6GHz	Uplink	Power Mode
Update Available	✓	AP-F44D5C9DD8A8	192.168.168.38	WBE660S	0	F4:4D:5C:9D:D8:A8	n/a	n/a	n/a	ETHERNET	Limited

Go to the Wireless > WLAN clients, you can check the list of wireless stations associated with a managed AP and the details information such as SSID Name, Security, IPv4 Address, and association time.

### Wireless > WLAN clients

MAC Address	Host Name	Connected to	AP Group	SSID	Security	IPv4 Address	Association time
E0:D0:45:68:3F:69	NT122546-NB01	AP-F44D5C9DD8A8	default	Zyxel_Wireless_Network	WPA2-PSK	192.168.168.39	2025/03/26 17:08:11

Using a laptop to connect to SSID: Zyxel\_Wireless\_Network and type the password for authentication. Go to the Log & Report > Log / Events > APC, you will see WLAN Station Info as shown below.

### Log & Report > Log / Events > APC

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2025-03-26 17:17:25	Wlan Station Info	STA connected, MAC:E0:D0:45:68:3F:69, AP:AP-F44D5C9DD8A8, interface:wlan-2-1, SSID: Zyxel_Wireless_Network, Signal: -20dBm	0.0.0.0	0.0.0.0	0	

## **What Could Go Wrong?**

If you can't see AP information in the AP List, please check the number of APs connected to the USG FLEX H firewall has exceeded the maximum Managed AP number it can support. If your mobile device can't access to the Internet via AP connects to the USG FLEX H firewall, please check if the LAN outgoing security policy allow access to the Internet.

## Chapter 6- Nebula

### How to Set Up Nebula site-to-site VPN on the USG FLEX H?

This example shows how to use Nebula VPN to establish Site to Site VPN tunnel between USG FLEX H and USG FLEX/ATP. The example instructs how to configure the Nebula Site-to-Site VPN using the Nebula Control Center. Once the Site-to-Site VPN tunnel is established, LAN hosts can communicate with each other through the VPN tunnel seamlessly.



 Note: Please ensure that Nebula firewalls are already connected to the Nebula Control Center. Additionally, ensure that all network IP addresses and subnet masks do not overlap, as show in the examples provided in this article. USG FLEX H series supported firmware version with uOS 1.31 and above.

## Set Up the Site-to-Site VPN settings on the Nebula Firewall

On Nebula (<https://nebula.zyxel.com/>) Navigate to Side-wide > Configure > Firewall > Site-to-Site VPN > Configure the Primary interface, Secondary interface (backup interface), on the local networks, enabling the interface will require routing through the VPN. Enable the Nebula VPN and choose the Site-to-Site VPN topology.

### USG FLEX/ATP site

The screenshot shows the Nebula Control Center interface for configuring Site-to-Site VPN on a USG FLEX/ATP site. The breadcrumb navigation is Site-wide > Configure > Firewall > Site-to-Site VPN. The interface is divided into several sections:

- Primary interface:** Set to 'wan1'.
- Secondary interface:** Set to 'wan2'.
- Local networks:** A table listing local networks with columns for Name, Subnet, and Use VPN.
 

Name	Subnet	Use VPN
lan1	192.168.66.0/24	<input checked="" type="checkbox"/>
lan2	192.168.77.0/24	<input type="checkbox"/>
- Nebula VPN:**
  - Enabled:**
  - VPN Area:** Default
  - VPN topology:** Split tunnel (send only site-to-site traffic over the VPN). Set to Site-to-Site.
  - ADVANCED OPTIONS:**
    - Area communication:**
    - NAT traversal:**
      - None
      - Custom NAT traversal: IP
  - Peer VPN networks:**

Network	Subnet(s)
USG Flex 200HP	192.168.168.1/24

Configuring VPN with multiple sites is cumbersome. Use [VPN Configuration](#) to save your time.

## USG FLEX H site

Primary interface:

Secondary interface:

Name	Subnet	Use VPN
ge3	192.168.168/24	<input checked="" type="checkbox"/>
ge4	192.168.169/24	<input type="checkbox"/>

**Nebula VPN**

Enabled:

VPN Area:

VPN topology:

**ADVANCED OPTIONS**

Area communication:

NAT traversal:  None  Custom

Network	Subnet(s)
ATP200	192.168.66.0/24

Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestrator](#) to save your time.

## Verify the VPN Connection

Navigate to Side-wide > Firewall > VPN connections to check the site-to-site VPN connection was connected successfully on both sites.

Connection status: This security gateway is exporting 1 subnet over the VPN: 192.168.66.0/24

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
USG Flex 200HP		192.168.168/24	connected	25.50 KB	53.26 KB	1036	2025-07-07 14:52:01

Connection status: This security gateway is exporting 1 subnet over the VPN: 192.168.168/24

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
ATP200		192.168.66/24	connected	109.38 KB	109.38 KB	679	2025-07-07 14:46:19

Navigate to the Web-GUI path VPN Status > IPsec VPN > Site to Site VPN of the USG FLEX H to check the Nebula VPN connection was connected successfully.

The screenshot shows the ZyXel USG FLEX 200HP Web-GUI interface. The breadcrumb navigation is: VPN Status > IPsec VPN > Site to Site VPN. The page title is 'Site to Site VPN' with a sub-header 'Remote Access VPN'. There are 'Disconnect' and 'Refresh' buttons. A table lists the VPN connections:

#	Name	Remote Gateway	Remote ID	My Address	Policy Route	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)	
1	Nebula VPN	SA_BC9911802B	111.243.	S182L372000	59.115.	0.0.0.0 <-> 0.0.0.0/0	2544	24987	2623 (157.38K bytes)	2600 (156K bytes)

## How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Hub site)?

This example shows how to establish Hub-and-Spoke VPN tunnel between USG FLEX H and USG FLEX/ATP. The example instructs how to configure the Nebula Site-to-Site VPN using the Nebula Control Center. Once the Hub-and-Spoke VPN tunnel is established, LAN hosts can communicate with each other through the VPN tunnel seamlessly.



Note: Please ensure that Nebula firewalls are already connected to the Nebula Control Center. Additionally, ensure that all network IP addresses and subnet masks do not overlap, as show in the examples provided in this article. USG FLEX H series supported firmware version with uOS 1.31 and above.

## Set Up the Hub-and-Spoke VPN settings on the Nebula Firewall

On Nebula (<https://nebula.zyxel.com/>) Navigate to Side-wide > Configure > Firewall > Site-to-Site VPN > Configure the Primary interface, Secondary interface (backup interface), on the local networks, enabling the interface will require routing through the VPN. Enable the Nebula VPN and choose the Hub-and-Spoke VPN topology and ensure that the USG FLEX H is set as the Hub site.

### USG FLEX H site

The screenshot shows the Nebula Control Center interface for configuring a Site-to-Site VPN. The page is titled "Site-to-Site VPN" and includes the following sections:

- Primary interface:** ge1\_PPP
- Secondary interface:** ge2
- Local networks:**

Name	Subnet	Use VPN
ge3	192.168.168.1/24	<input checked="" type="checkbox"/>
ge4	192.168.169.1/24	<input type="checkbox"/>
- Nebula VPN:**
  - Enabled:
  - VPN Area: Default
  - VPN topology: Hub-and-Spoke
  - Hubs (peers connect to):
 

SiteName
1 USG Flex 200HP

At the bottom, there is a section for "ADVANCED OPTIONS" with a note: "Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestrator](#) to save your time."

## USG FLEX/ATP site

nebulas Control Center Organization: [Organization] Site: ATP200

Site-wide > Configure > Firewall > Site-to-Site VPN

Site-to-Site VPN

Primary interface: wan1  
Secondary interface: wan2

Name	Subnet	Use VPN
lan1	192.168.66.0/24	<input checked="" type="checkbox"/>
lan2	192.168.77.0/24	<input type="checkbox"/>

Nebula VPN

Enabled:   
VPN Area: Default  
VPN topology: Split tunnel (send only site-to-site traffic over the VPN)  
Hub-and-Spoke: Hub-and-Spoke

SiteName
1 USG Flex 200HP

ADVANCED OPTIONS

Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestrator](#) to save your time.

## Verify The VPN Connection

Navigate to Side-wide > Firewall > VPN connections to check the site-to-site VPN connection was connected successfully on both sites.

nebulas Control Center Organization: [Organization] Site: USG Flex 200HP

Site-wide > Monitor > Firewall > VPN connections

VPN connections

Connection status  
Configuration: This security gateway is exporting 1 subnet over the VPN: 192.168.168.1/24

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
ATP200		192.168.66.1/24	connected	91.42 KB	105.47 KB	437	2025-01-07 16:06:26

nebulas Control Center Organization: [Organization] Site: ATP200

Site-wide > Monitor > Firewall > VPN connections

VPN connections

Connection status  
Configuration: This security gateway is exporting 1 subnet over the VPN: 192.168.66.0/24

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
USG Flex 200HP		192.168.168.1/24	connected	13.25 KB	19.10 KB	316	2025-01-07 16:04:09

Navigate to the Web-GUI path VPN Status > IPsec VPN > Site to Site VPN of the USG FLEX H to check the Nebula VPN connection was connected successfully.

ZYXEL USG FLEX 200HP

VPN Status > IPsec VPN > Site to Site VPN

Site to Site VPN Remote Access VPN

Disconnect Refresh

ID	Name	Remote Gateway	Remote ID	My Address	Policy Route	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)
1	SA_BC9911802B	111.243.111.111	5182L3720007311	59.115.111.111	0.0.0.0/0 <-> 0.0.0.0/0	742	25466	762 (45.72K bytes)	731 (43.86K bytes)

## How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Spoke site)?

This example shows how to use Nebula VPN to establish Hub-and-Spoke VPN tunnel between USG FLEX/ATP and USG FLEX H. The example instructs how to configure the Nebula Site-to-Site VPN using the Nebula Control Center. Once the Hub-and-Spoke VPN tunnel is established, LAN hosts can communicate with each other through the VPN tunnel seamlessly.



 Note: Please ensure that Nebula firewalls are already connected to the Nebula Control Center. Additionally, ensure that all network IP addresses and subnet masks do not overlap, as show in the examples provided in this article. USG FLEX H series supported firmware version with uOS 1.31 and above.

## Set Up the Hub-and-Spoke VPN settings on the Nebula Firewall

On Nebula (<https://nebula.zyxel.com/>) Navigate to Side-wide > Configure > Firewall > Site-to-Site VPN > Configure the Primary interface, Secondary interface (backup interface), on the local networks, enabling the interface will require routing through the VPN. Enable the Nebula VPN and choose the Hub-and-Spoke VPN topology and ensure that the USG FLEX H series is set as the Spoke site.

### USG FLEX/ATP site

Organization: [Organization Name] > Site: ATP200

Site-wide > Configure > Firewall > Site-to-Site VPN

Site-to-Site VPN

Primary interface: wan1

Secondary interface: wan2

Name	Subnet	Use VPN
lan1	192.168.66.0/24	<input checked="" type="checkbox"/>
lan2	192.168.77.0/24	<input type="checkbox"/>

Nebula VPN

Enabled:

VPN Area: Default

VPN topology: Split tunnel (send only site-to-site traffic over the VPN)  
Hub-and-Spoke

Hubs (peers connect to)

SiteName
1 ATP200

ADVANCED OPTIONS

Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestrator](#) to save your time.

## USG FLEX H site

Organization: [Organization Name] > Site: USG Flex 200HP

Site-wide > Configure > Firewall > Site-to-Site VPN

Site-to-Site VPN

Primary interface:

Secondary interface:

Local networks

Name	Subnet	Use VPN
ge3	192.168.168.1/24	<input checked="" type="checkbox"/>
ge4	192.168.169.1/24	<input type="checkbox"/>

Nebula VPN

Enabled:

VPN Area:

VPN topology: Split tunnel (send only site-to-site traffic over the VPN)

Hub-and-Spoke:

Hubs (peers connect to)

SiteName
1 ATP200

ADVANCED OPTIONS

Configuring VPN with multiple sites is cumbersome. Use [VPN Orchestrator](#) to save your time.

## Verify The VPN connection

Navigate to Side-wide > Firewall > VPN connections to check the site-to-site VPN connection was connected successfully on both sites.

Organization: [Organization Name] > Site: ATP200

Site-wide > Monitor > Firewall > VPN connections

VPN connections

Connection status

Configuration: This security gateway is exporting 1 subnet over the VPN: 192.168.66.0/24

Site connectivity

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
USG Flex 200HP		192.168.168.1/24	connected	26.71 KB	34.84 KB	869	2025-01-07 17:46:52

Organization: [Organization Name] > Site: USG Flex 200HP

Site-wide > Monitor > Firewall > VPN connections

VPN connections

Connection status

Configuration: This security gateway is exporting 1 subnet over the VPN: 192.168.168.1/24

Site connectivity

Location	VTI IP	Subnet	Status	Inbound	Outbound	Tunnel Up Time	Last Heartbeat
ATP200		192.168.66.1/24	connected	93.05 KB	89.77 KB	439	2025-01-07 16:36:32

Navigate to the Web-GUI path VPN Status > IPsec VPN > Site to Site VPN of the USG FLEX H to check the Nebula VPN connection was connected successfully.

The screenshot shows the ZyXel USG FLEX 200HP Web-GUI interface. The breadcrumb navigation path is VPN Status > IPsec VPN > Site to Site VPN. The main content area displays a table of Site to Site VPN connections. A red box highlights the 'Nebula VPN' entry, which is in a connected state.

#	Name	Remote Gateway	Remote ID	My Address	Policy Route	Uptime	Rekey	Inbound (Bytes)	Outbound (Bytes)
1	SA_BC9911802B88	111.243.208.1	182L372000	1.161.1.1	0.0.0.0 <-> 0.0.0.0	140	27197	139 (8.34K bytes)	143 (8.58K bytes)