

# 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: uOS 1.35

Aug. 2025



## Table of Content

<b>Chapter 1- VPN .....</b>	<b>5</b>
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 .....	54
How to Configure Route-Based VPN .....	65
How to Use Tailscale.....	77
How to use Ext-group user to connect Remote Access VPN.....	88
<b>Chapter 2- Security Service .....</b>	<b>91</b>
How to Block HTTPS Websites Using Content Filtering and SSL Inspection .....	91
How to Configure Content Filter with HTTPs Domain Filter .....	100
How to Block Facebook Using a Content Filter Block List .....	105
How to block YouTube access by Schedule .....	109
How to Control Access to Google Drive .....	118
How to Block the Spotify Music Streaming Service .....	126
How does Anti-Malware Work .....	129
How to Detect and Prevent TCP Port Scanning with DoS Prevention .....	132
How to block the client from accessing to certain country using Geo IP? .....	136
How to Use Sandbox to Detect Unknown Malware? .....	141
How to Configure Reputation Filter- IP Reputation.....	144
How to Configure Reputation Filter- URL Threat Filter.....	149
How to Configure Reputation Filter- DNS Threat Filter .....	153



How to Configure DNS Content Filter .....	157
External Block List for Reputation Filter .....	162
How to set up DNS SafeSearch? .....	167
<b>Chapter 3- Authentication</b> .....	175
How to Use Two Factor with Google Authenticator for Admin Access .....	175
How to Use Two Factor with Google Authenticator for Remote Access VPN and SSL VPN .....	182
How to set up AD authentication with Microsoft AD .....	192
How to Set Up Captive Portal? .....	197
<b>Chapter 4- Maintenance</b> .....	205
How to Manage Configuration Files .....	205
How to Manage Firmware .....	209
How to set up configuration file backup rotation .....	211
<b>Chapter 5- Others</b> .....	215
How to Setup and Configure Daily Report .....	215
How to Setup and Send Logs to a Syslog Server .....	220
How to Setup and Send logs to the USB storage .....	223
How to Perform and Use the Packet Capture Feature .....	225
How to Allow Public Access to a Server Behind USG FLEX H.....	229
How to Configure DHCP Option 60 – Vendor Class Identifier .....	233
How to Configure Session Control .....	235
How to Configure Bandwidth Management for FTP Traffic .....	238
How to Configure WAN trunk for Spillover and Least Load First .....	243
How Does SIP ALG Function Work on USG FLEX H? .....	249
How to Deploy Device HA .....	253
How to check Packet Flow Explorer .....	265
How to set up a Link Aggregation Group (LAG) interface .....	271



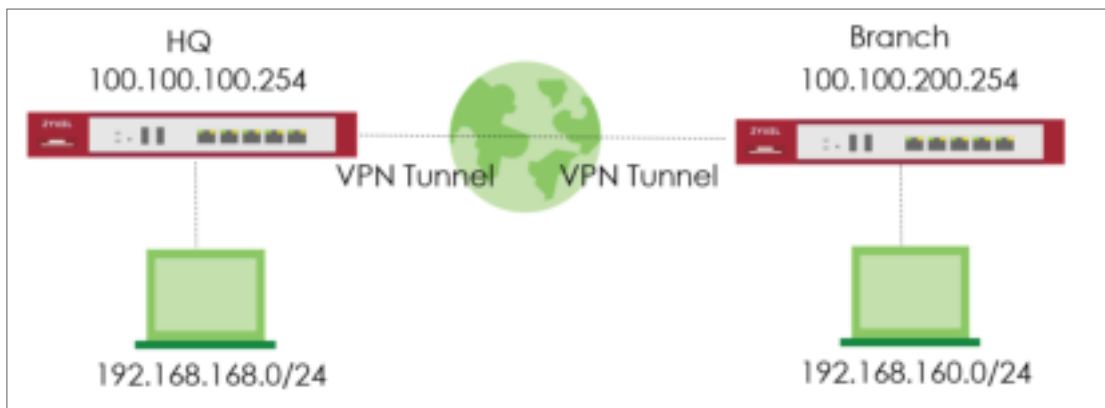
How to Set Up AP Control Service for Zyxel APs .....	277
How to set up SMTP with Microsoft OAuth2.0?.....	282
<b>Chapter 6- Nebula</b> .....	295
How to Set Up Nebula site-to-site VPN on the USG FLEX H?.....	295
How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Hub site)?.....	299
How to Set Up Nebula Hub-and-Spoke VPN on USG FLEX H (Spoke site)? .....	303
How to Onboard Firewall to Nebula within Initial Setup Wizard .....	307



## 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.





## VPN > Site to Site VPN > Scenario



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

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

VPN > Site to Site VPN > Scenario > Network

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

My Address Domain Name / IP 100.100.100.204

Peer Gateway Address Domain Name / IP 100.100.200.204

Local Site 100.100.100.204

Internet

Remote Site 100.100.200.204

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 wizard at the 'Authentication' step. The breadcrumb trail at the top reads 'VPN > Site to Site VPN > Scenario > Network > Authentication'. A progress bar at the top indicates five steps: 1. Scenario (checked), 2. Network (checked), 3. Authentication (active), 4. Policy & Routing, and 5. Summary. Under the 'Authentication' heading, there are two radio button options: 'Pre-Shared Key' (selected) and 'Certificate'. To the right of the 'Pre-Shared Key' option is a text input field containing masked characters (dots) and a red border, indicating it is the active field. Below this input field is a dropdown menu currently set to 'default'. At the bottom of the window, there are three buttons: 'Cancel' on the left, and 'Back' and 'Next' on the right. The 'Next' button is highlighted in green.



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

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

The screenshot displays the ZyXEL VPN configuration interface for a Site-to-Site VPN. The configuration progress bar at the top 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 "Policy & Routing" section, the "Type" is set to "Policy-Based" (indicated by a green plus icon). The "Local Subnet" is configured as "192.168.148.0/24" and the "Remote Subnet" is configured as "192.168.145.0/24". Both subnet fields are highlighted with red rectangular boxes.

Below the configuration fields, a network diagram illustrates the setup. It shows two local sites connected to the Internet. The "Local Site" has a local subnet of "100.100.100.254" and is connected to the Internet via a gateway with IP "192.168.148.0/24". The "Remote Site" has a local subnet of "100.100.200.254" and is connected to the Internet via a gateway with IP "192.168.145.0/24".

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



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

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

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

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

**Configuration**

Name	HQBranch
IP Version	3
Scenario	Scenario
Type	Policy

[Edit](#)

**Network**

Local Site	192.168.100.0/24
Remote Site	192.168.200.0/24

**Authentication**

Authentication	group1@192.168.100.1	group2@192.168.200.1
----------------	----------------------	----------------------

**Policy & Routing**

Local Subnet	192.168.100.0/24
Remote Subnet	192.168.200.0/24

[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**.





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

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

The screenshot displays the 'Network' configuration step of a Site-to-Site VPN setup. The top navigation bar includes steps: 1. Scenario, 2. Network (active), 3. Authentication, 4. Policy & Routing, and 5. Summary. The main configuration area contains two rows of fields: 'My Address' and 'Peer Gateway Address'. Each row has a text input field and a 'Domain Name / IP' dropdown menu, both containing the value '100.100.100.234'. Below these fields is a network diagram showing two routers, 'Local Site' and 'Remote Site', connected through a central green cloud labeled 'Internet'. The 'Local Site' router has the IP '100.100.100.234' and the 'Remote Site' router also has the IP '100.100.100.234'. At the bottom of the window, there are three buttons: 'Cancel', 'Test', and 'Next'.



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

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

The screenshot shows the ZyXEL VPN configuration wizard at Step 3: Authentication. The wizard has five steps: 1. Scenario, 2. Network, 3. Authentication, 4. Policy & Routing, and 5. Summary. Step 3 is currently active. Under the 'Authentication' section, there are two radio buttons: 'Pre-Shared Key' (which is selected) and 'Certificate'. A text input field for the Pre-Shared Key is visible, containing the text 'xxxxxxxx'. Below the input field, there is a label 'secret' and a small icon. At the bottom of the window, there are three buttons: 'Cancel', 'Back', and 'Next' (which is highlighted in green).



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

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

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

Progress: Scenario — Network — Authentication — **Policy & Routing** — Summary

Type: ☐ Route-Based ☒ Policy-Based

Local Subnet: 192.168.168.0/24

Remote Subnet: 192.168.168.0/24

Network Diagram:

```

graph LR
    LocalNet[Local Net: 192.168.168.0/24] --- LocalGW[Local GW: 192.168.168.1]
    LocalGW --- Internet((Internet))
    Internet --- RemoteGW[Remote GW: 192.168.168.1]
    RemoteGW --- RemoteNet[Remote Net: 192.168.168.0/24]
  
```

Buttons: Cancel, Back, Next



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

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

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

Scenario Network Authentication Policy & Routing **Summary**

**Configuration**

Name	Branch0202
IP Address	1
Username	admin
Type	Policy

[Edit](#)

**Network**

Local IP	192.168.1.101/24
Remote IP	192.168.1.102/24

**Authentication**

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

**Policy & Routing**

Local Subnet	192.168.1.0/24
Remote Subnet	192.168.1.0/24

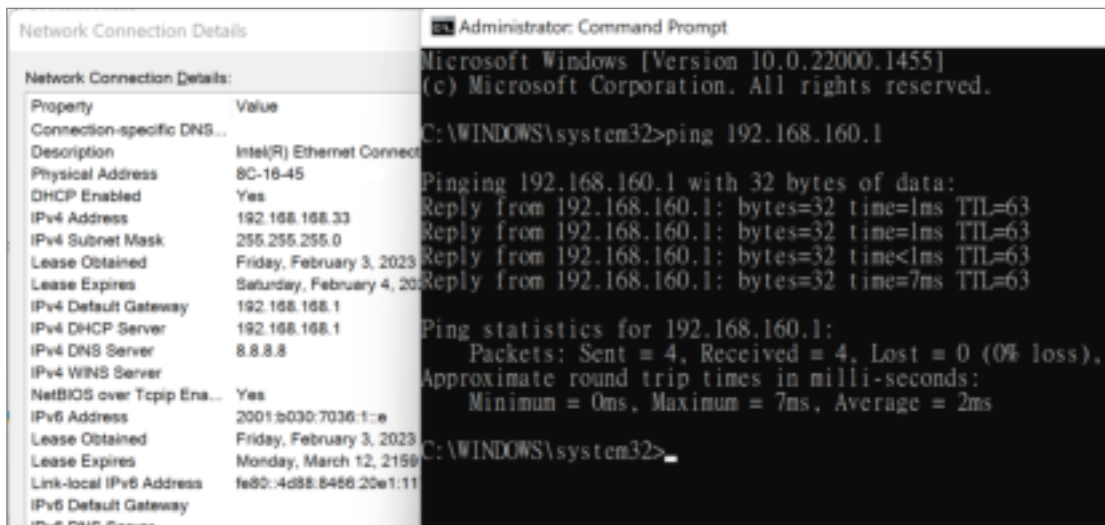
[Close](#)



## Test IPSec VPN Tunnel

### Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



### VPN Status > IPSec VPN

Verify the IPSec VPN status and do the Connectivity Check





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

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

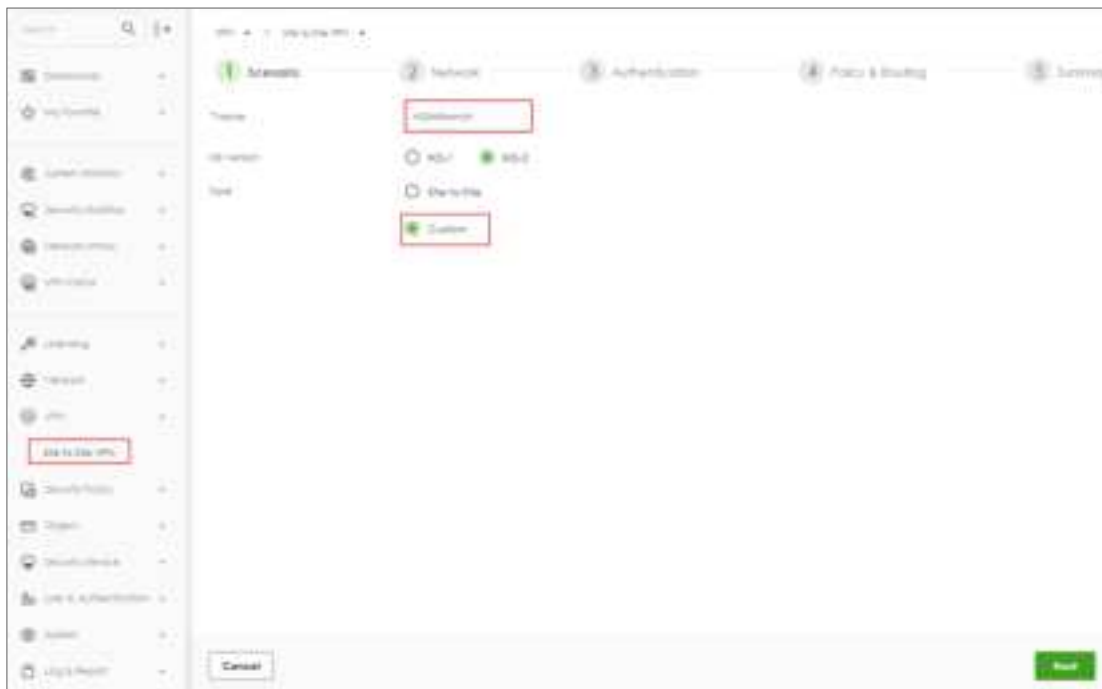




## Set up IPSec VPN Tunnel for HQ

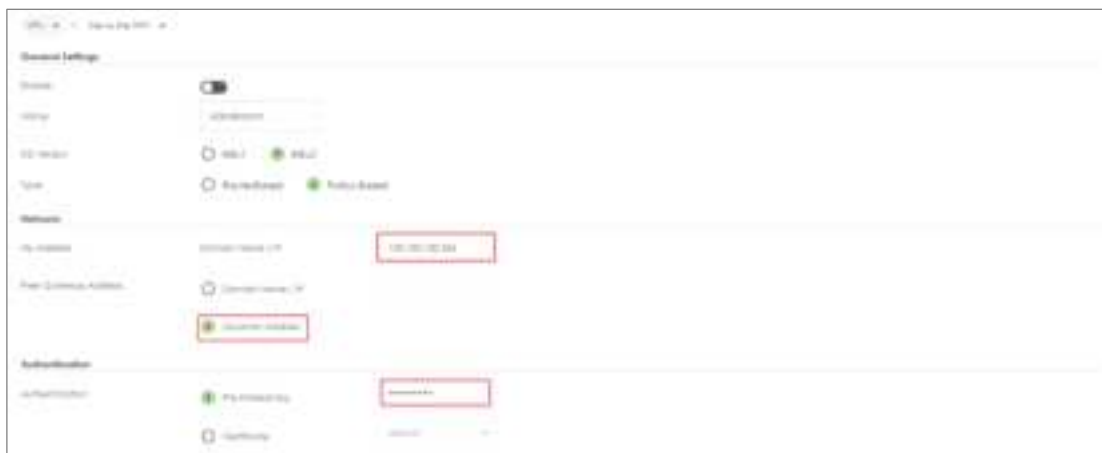
### VPN > Site to Site VPN > Scenario

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



### VPN > Site to Site VPN

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





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

Phase 2 Settings

Initiation: ☐ Auto ☐ Natted-up ☒ Responder Only

Policy

+ Add Edit Remove

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

Rows per page: 30 1 of 1 < 1 >

SA Life Time: 28800 (180 - 3000000 Seconds)

Proposal

+ Add Edit Remove

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

Rows per page: 50 1 of 1 < 1 >

Diffie-Hellman Group: DH2



## Set up IPsec VPN Tunnel for Branch

### VPN > Site to Site VPN > Scenario

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

The screenshot shows the 'Scenario' configuration step for a Site-to-Site VPN. The 'Name' field is 'BranchHQ2'. The 'Type' is set to 'Custom'. The 'PSK Version' is set to 'IKEv2'. The 'Type' is set to 'Policy-Based'. The 'Next' button is highlighted in green.

### 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 'General Settings' configuration step for a Site-to-Site VPN. The 'My Address' is set to '0.0.0.0'. The 'Peer Gateway Address' is set to '192.168.1.254'. The 'Authentication' is set to 'Pre-shared Key' with a value of '\*\*\*\*\*'. The 'Next' button is highlighted in green.



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

**Phase 2 Settings**

Initiation: ☒ Auto ☐ Noted-up ☐ Responder Only

Policy:

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

Rows per page: 50 1 of 1

SA Life Time: 28800 (180 - 300000 Seconds)

Proposal:

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

Rows per page: 50 1 of 1

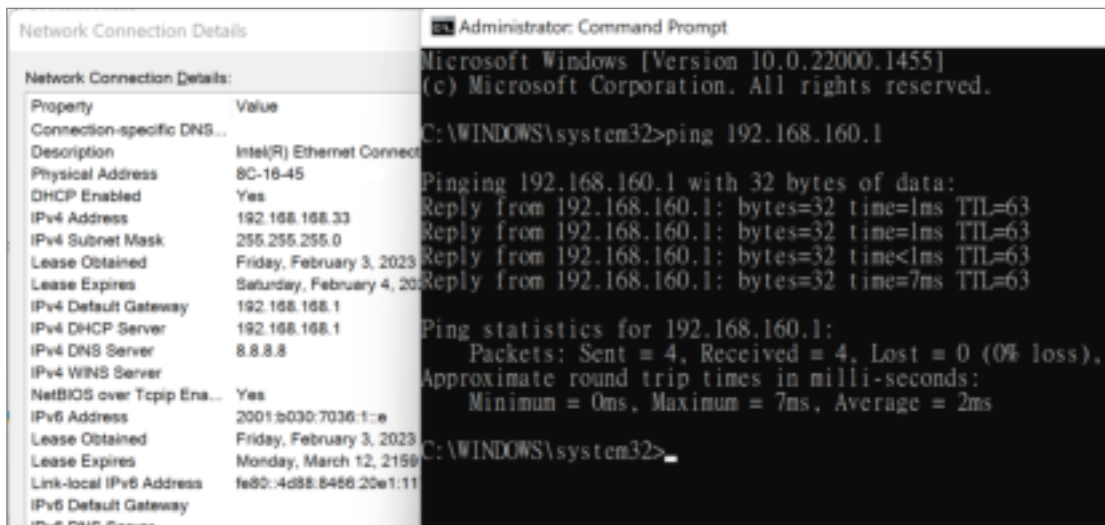
Diffie-Hellman Groups:



## Test IPSec VPN Tunnel

### Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



### VPN Status > IPSec VPN

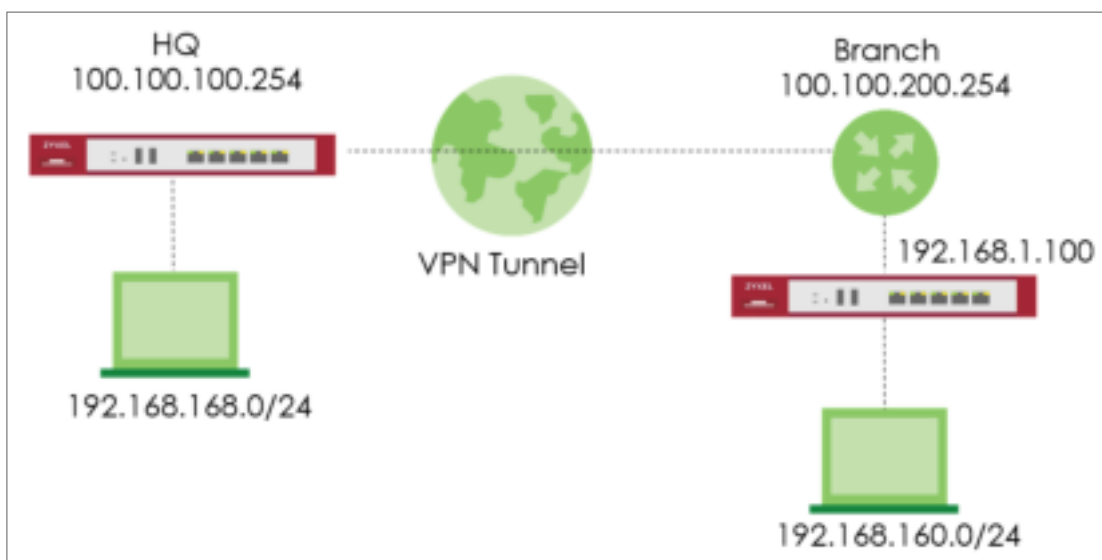
Verify the IPSec VPN status and do the Connectivity Check





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

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



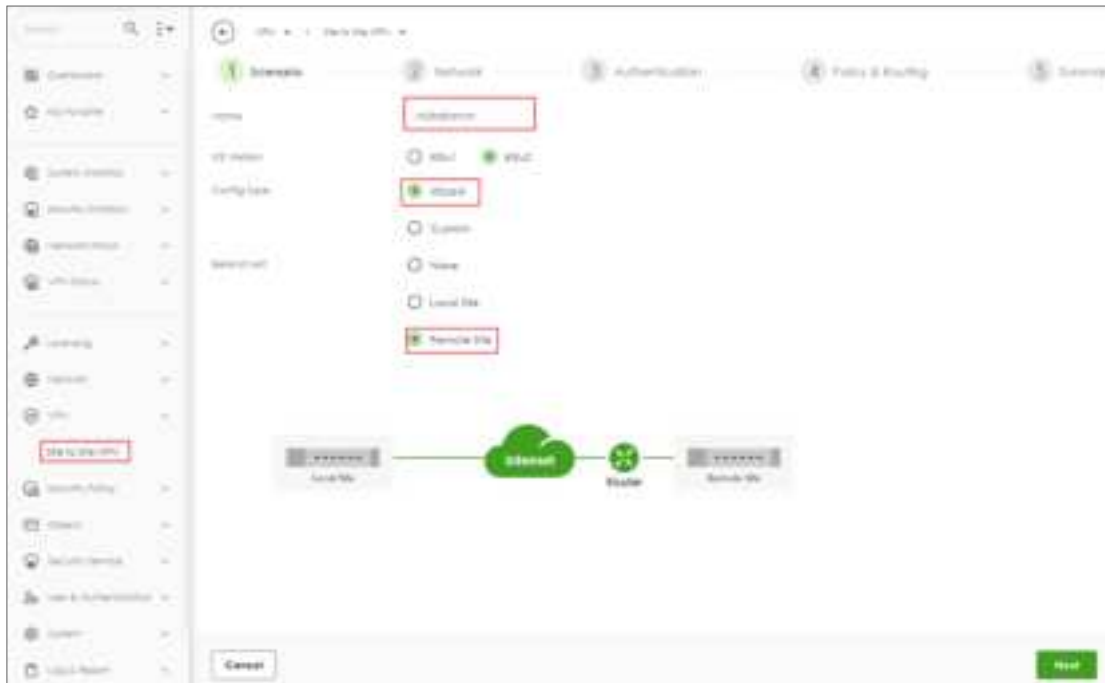
 Note: Please ensure that you have NAT mapping UDP port 4500 to USG FLEX H device.



## Set up IPsec VPN Tunnel for HQ

### VPN > Site to Site VPN > Scenario

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





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

Configure My Address. Click **Next**.



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

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

The screenshot shows the ZyXEL VPN configuration wizard at Step 3: Authentication. The breadcrumb trail at the top is "VPN > Site to Site VPN > Scenario > Network > Authentication". The progress bar shows five steps: 1. Scenario, 2. Network, 3. Authentication (current), 4. Policy & Routing, and 5. Summary. Under the "Authentication" section, there are two radio button options: "Pre-Shared Key" (selected) and "Certificate (Advanced)". The "Pre-Shared Key" option is active, and a text input field containing nine asterisks is highlighted with a red rectangle. To the right of the input field is a small icon of a key. At the bottom of the window, there are three buttons: "Cancel", "Back", and "Next" (highlighted in green).



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

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

The screenshot displays the ZyXEL VPN configuration wizard for a Site-to-Site VPN. The progress bar at the top indicates the current step is '4 Policy & Routing', with previous steps being 'Scenario', 'Network', 'Authentication', and 'Summary'.

Under the 'Type' section, the 'Policy-Based' option is selected and highlighted with a red box. Below this, the 'Local Subnet' is set to '192.168.100.0/24' and the 'Remote Subnet' is set to '192.168.100.0/24', both fields also highlighted with red boxes.

The network diagram at the bottom illustrates the setup: a 'Local Site' (represented by a router icon and the IP '192.168.100.254') is connected to an 'Internet' cloud. The 'Internet' cloud is connected to a 'Router' icon, which is then connected to a 'Remote Site' (represented by a router icon and the label 'Dynamic Address'). The 'Remote Site' is further connected to a host icon with the IP '192.168.100.254'.

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



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

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

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

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

**Configuration**

Name: VPN000001

ID Number: 2

Type: Policy-based

Protocol: IPsec

**Network**

Local IP: 192.168.1.1

Remote IP: 192.168.1.2

**Authentication**

Authentication: Pre-shared key

**Policy & Routing**

Local Subnet: 192.168.1.0/24

Remote Subnet: 192.168.1.0/24

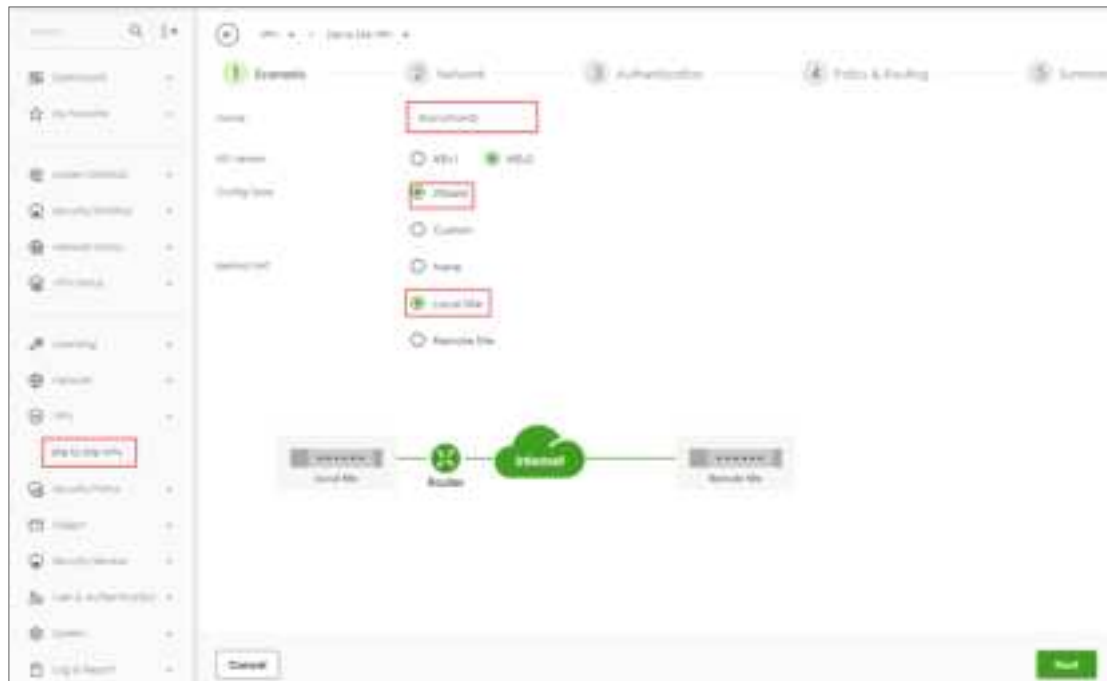
**Close**



## 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**.





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

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

The screenshot shows the ZyXEL VPN configuration interface for Site to Site VPN, specifically the Network configuration step. The interface has a breadcrumb trail: VPN > Site to Site VPN > Scenario > Network. Below the breadcrumb, there are five tabs: 1. Overview, 2. Network (active), 3. Authentication, 4. Policy & Routing, and 5. Summary.

In the Network tab, there are two main sections for IP configuration:

- My Address:** Contains a text field for "Domain name: IP" with the value "192.168.1.100" entered. Below it is a label "Peer Gateway Address" and another "Domain name: IP" field with the value "100.100.100.254".
- Diagram:** A network diagram showing two routers connected via an Internet cloud. The left router is labeled "Local Site" with IP "192.168.1.100". The right router is labeled "Remote Site" with IP "100.100.100.254". A green cloud labeled "Internet" is in the center, connected to both routers.

At the bottom of the interface, there are three buttons: "Cancel", "Back", and "Next". The "Next" button is highlighted in green.



**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 of 5. Below the progress bar, the 'Type' is set to 'Policy-Based'. The 'Local Subnet' is configured as '192.168.168.0/24' and the 'Remote Subnet' is configured as '192.168.168.0/24'. Both fields are highlighted with red boxes. Below the configuration fields, a network diagram illustrates the setup: a 'Local Net' (192.168.1.1/24) connected to a 'Router', which is connected to an 'Internet' cloud, which is then connected to a 'Remote Net' (192.168.1.1/24). At the bottom of the page, there are 'Cancel', 'Back', and 'Next' buttons.



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

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

The screenshot shows the ZyXEL VPN configuration wizard at the 'Authentication' step. The breadcrumb trail at the top reads 'VPN > Site to Site VPN > Scenario > Network > Authentication'. A progress bar at the top indicates five steps: 1. Scenario (checked), 2. Network (checked), 3. Authentication (active), 4. Policy & Routing, and 5. Summary. Under the 'Authentication' heading, there are two radio button options: 'Pre-Shared Key' (selected) and 'Certificate' (with a 'Safe' label). The 'Pre-Shared Key' option is expanded, showing a text input field containing ten asterisks, a red eye icon to toggle visibility, and a dropdown menu currently set to 'default'. At the bottom of the window, there are three buttons: 'Cancel' on the left, and 'Back' 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 > Summary

Scenario Network Authentication Policy & Routing Summary

**Configuration**

Name	site-to-site-VPN
# of tunnels	2
Type	Policy-based

**Proposed**

1/2

**Network**

Local IP	192.168.3.100
Remote IP	100.100.100.100

**Authentication**

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

**Policy & Routing**

Local subnet	192.168.100.0/24
--------------	------------------

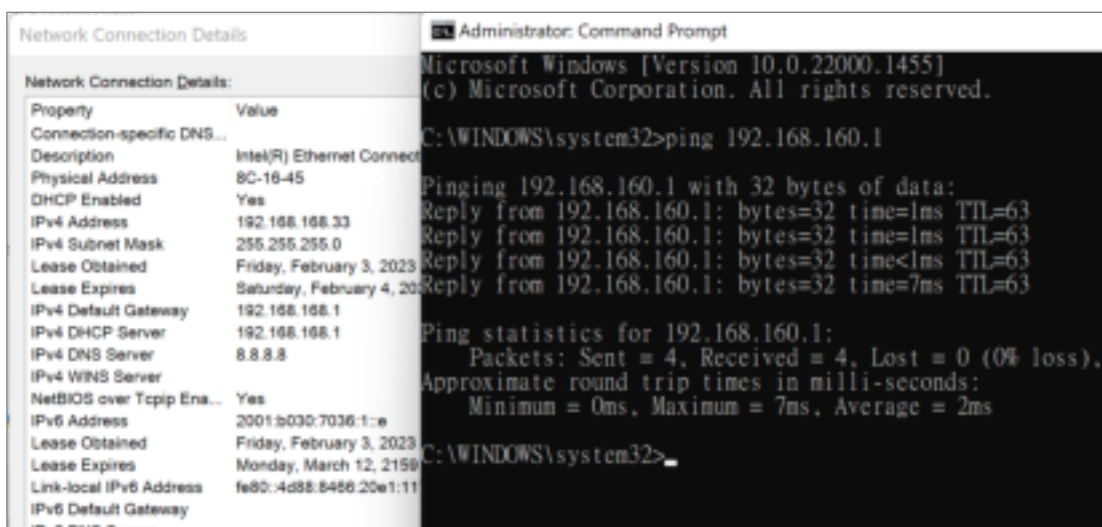
**Done**



## Test IPSec VPN Tunnel

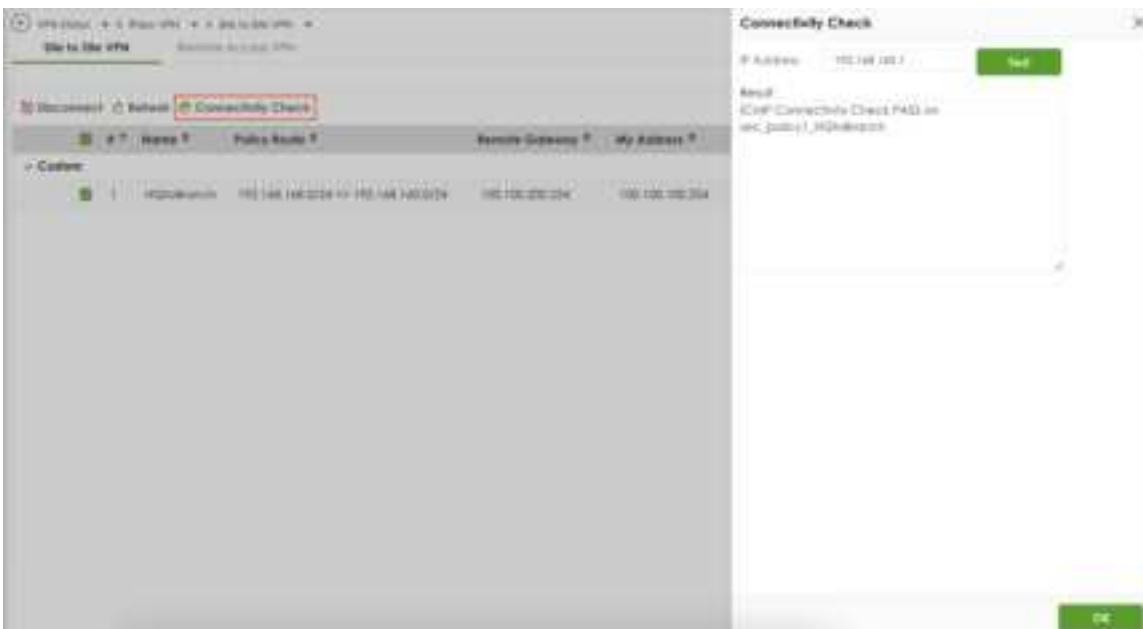
### Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1



### VPN Status > IPSec VPN

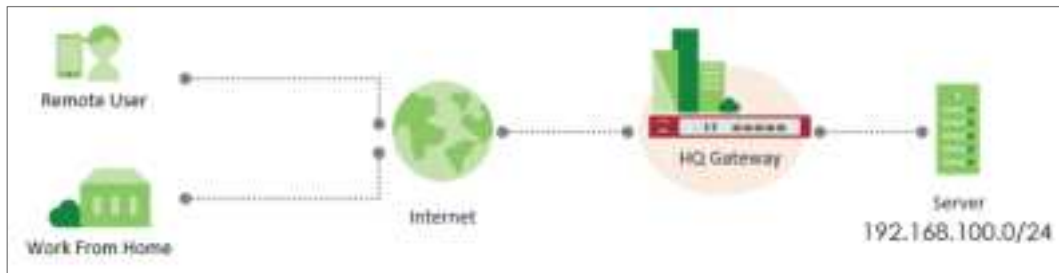
Verify the IPSec VPN status and do the Connectivity Check





## How to Configure Remote Access VPN with Zyxel VPN Client

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





## Before Begin

### User & Authentication > User/Group > User

Create local user for remote access authentication.



← User & Authentication > User/Group

### Profile Management

User Name:

User Type:

Password:

Retype:

Description:

Email 1:

Email 2:

Mobile Number:

Authentication Timeout Settings: ☒ Use Default Settings ☐ Use Manual Settings

Lease Time: 1440 minutes

Reauthentication Time: 1440 minutes



## Download and install the new TGB Client

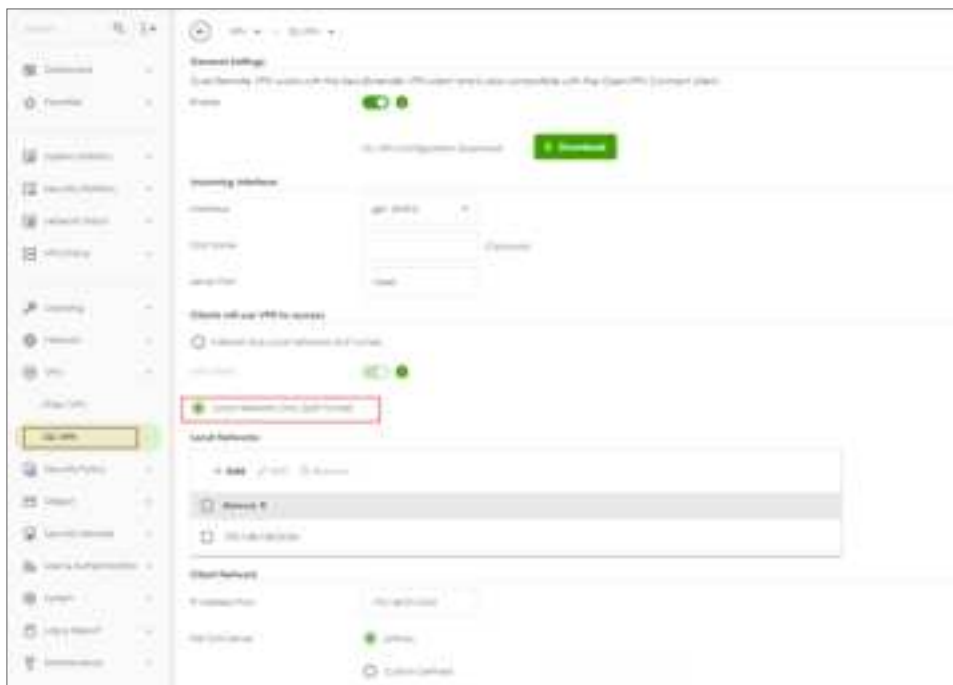


## Set up SSL VPN

### VPN > SSL VPN

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

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





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

The screenshot shows the 'Client Network' and 'Authentication' sections of a ZyXEL VPN configuration interface. In the 'Client Network' section, the 'IP Address Pool' is set to '192.168.51.0/24' and the 'Hot DNS Server' is set to 'ZyWALL'. In the 'Authentication' section, the 'Primary Server' is set to 'LDAP' and the 'Secondary Server' is set to 'None'. The 'User' field is set to 'ZyWALLVPN'.

## Set up IKEv2 VPN

### VPN > IPSec VPN > Remote Access VPN

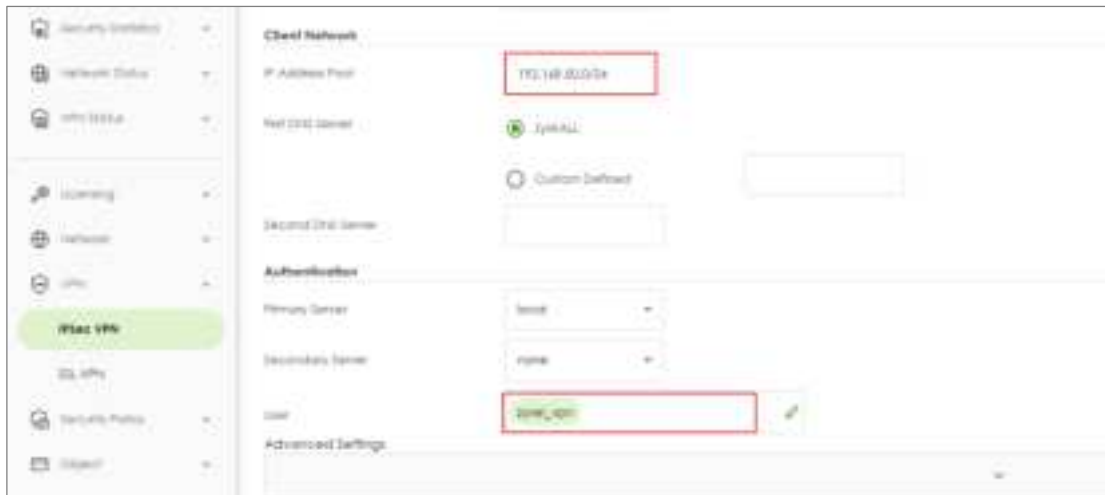
Select the incoming interface. And up to your requirement to select Full Tunnel or Split Tunnel.

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

The screenshot shows the 'Remote Access VPN' configuration page. The 'Tunnel Settings' section shows the 'Tunnel' type set to 'Split' and the 'Incoming Interface' set to 'eth0'. The 'Tunneling Profiles' section shows the 'Profile' set to 'Split'. The 'Client Network' section shows the 'IP Address Pool' set to '192.168.100.0/24'.

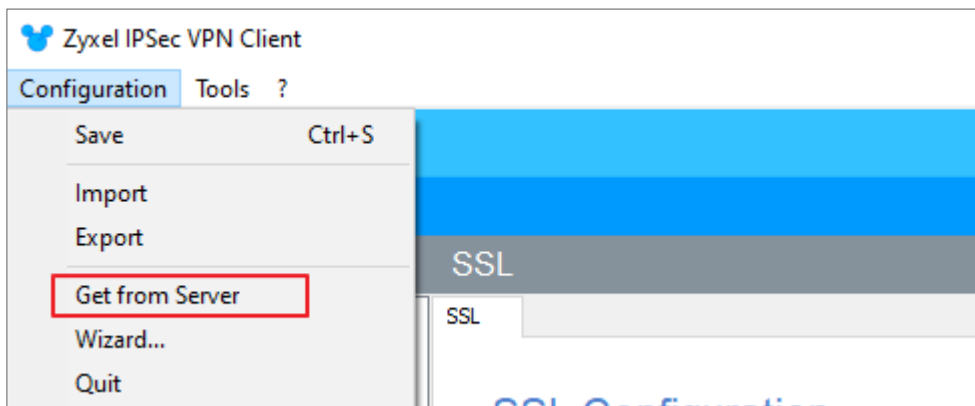


The default Address Pool is 192.168.50.0/24 and select the User who can access IKEv2 VPN.




## Set up Remote Access on TGB Client



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





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


**VPN Configuration Server Wizard**
✕

**Step 1: Authentication**



What are the parameters of the VPN Server Connection?

You are going to download your VPN Configuration from the VPN Configuration Server.  
Enter below the authentication information required for the connection to the server.

Gateway Address:  Port:

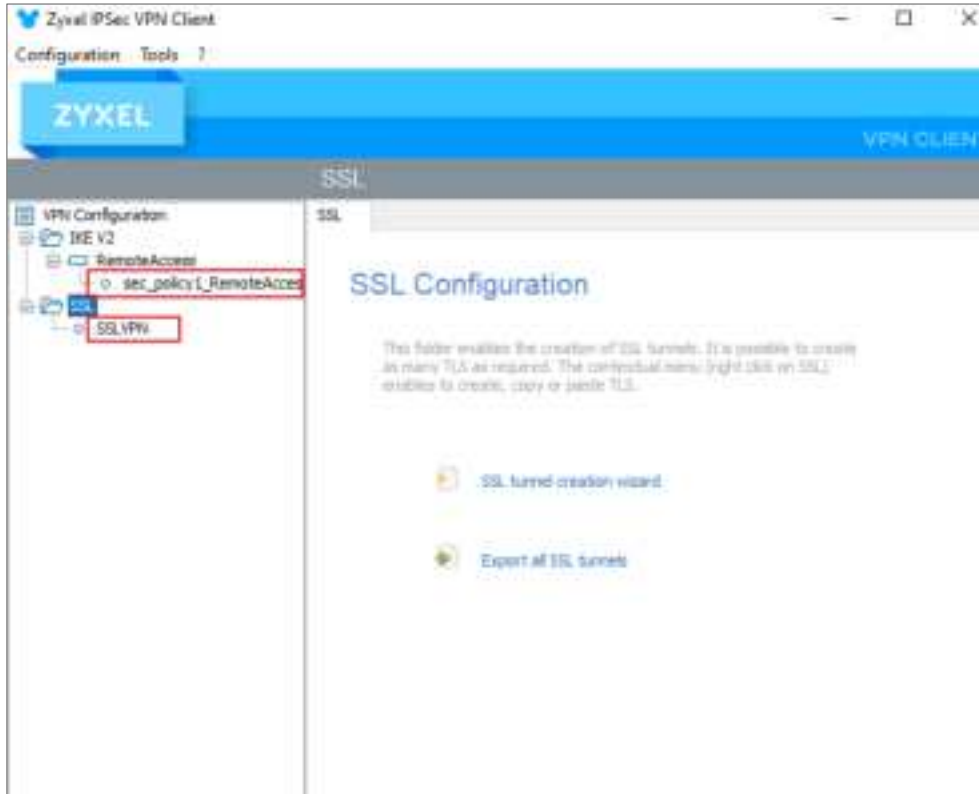
Authentication:

Login:

Password:



You will obtain IKEv2 as well as SSLVPN settings.

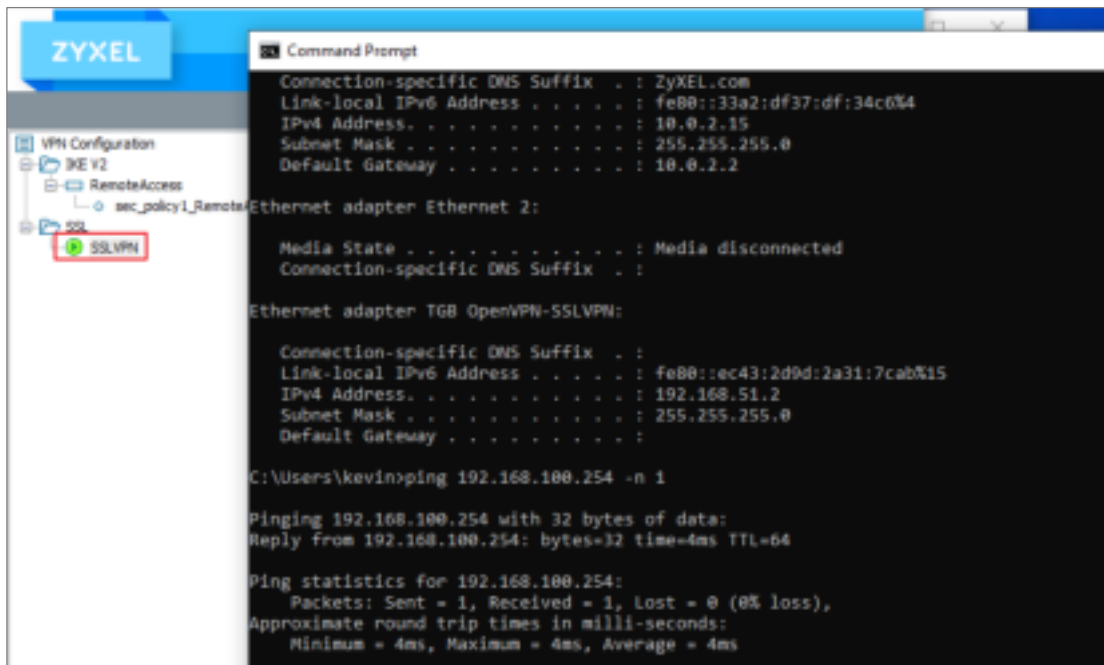




## Test SSLVPN Tunnel on TGB Client

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

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

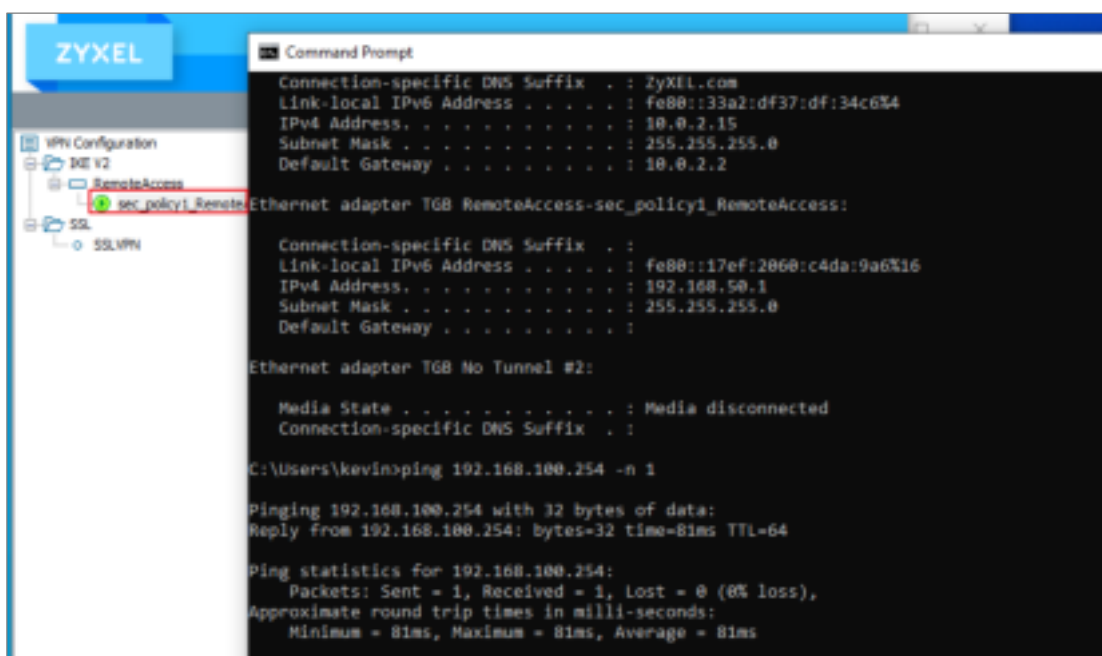




## Test IKEv2 Tunnel on TGB Client

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

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



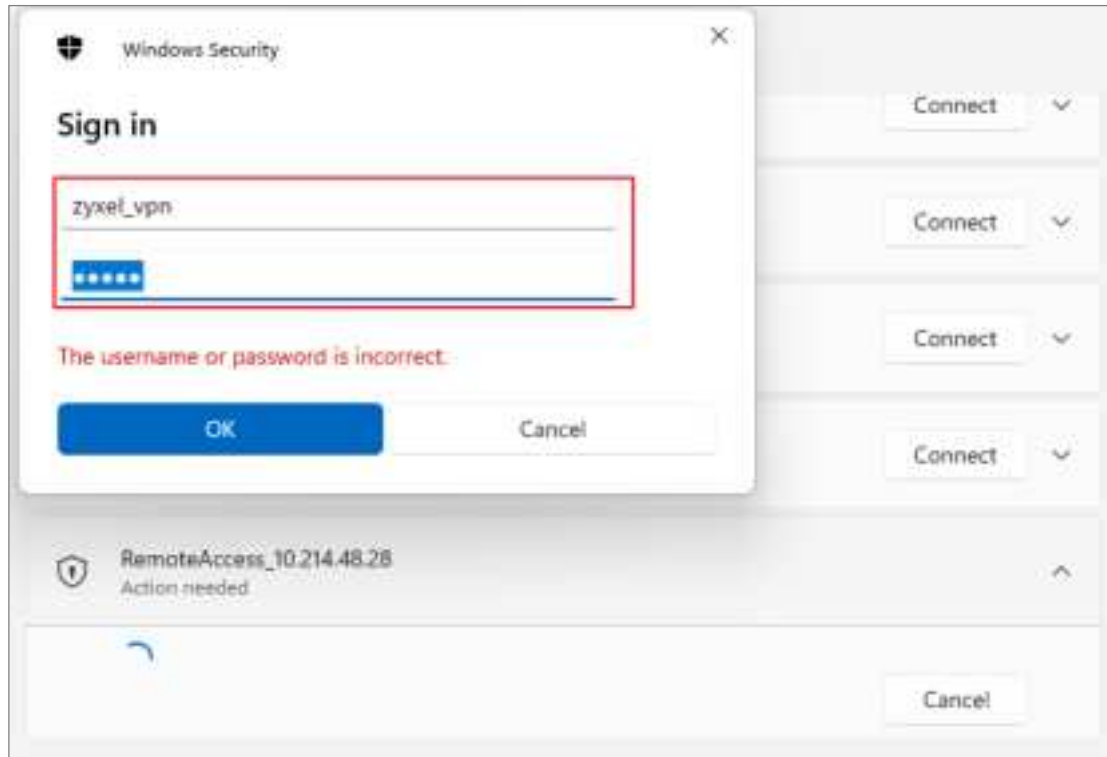
## Test IKEv2 Tunnel on Windows Client

Download Windows VPN configuration script



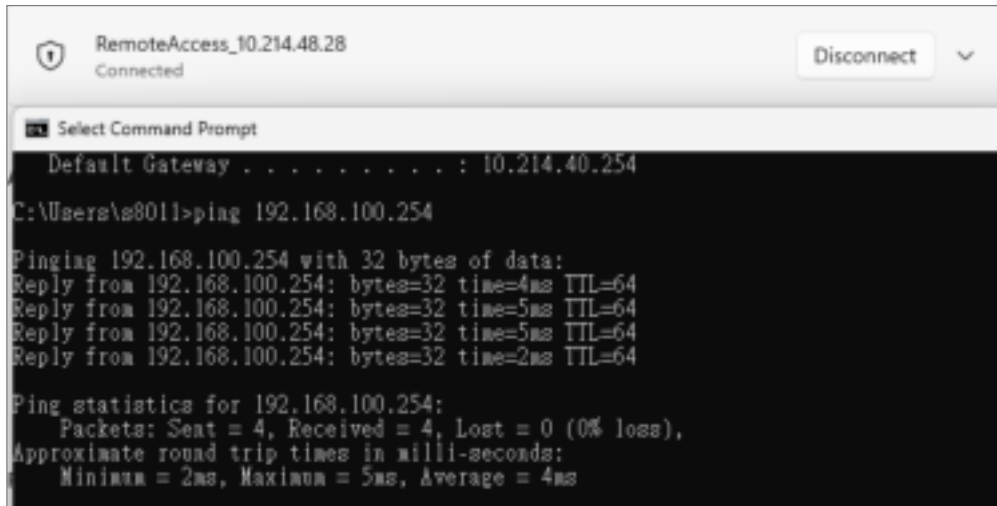


Perform the windows bat file and input credentials.





VPN is connected and can access internal resource.

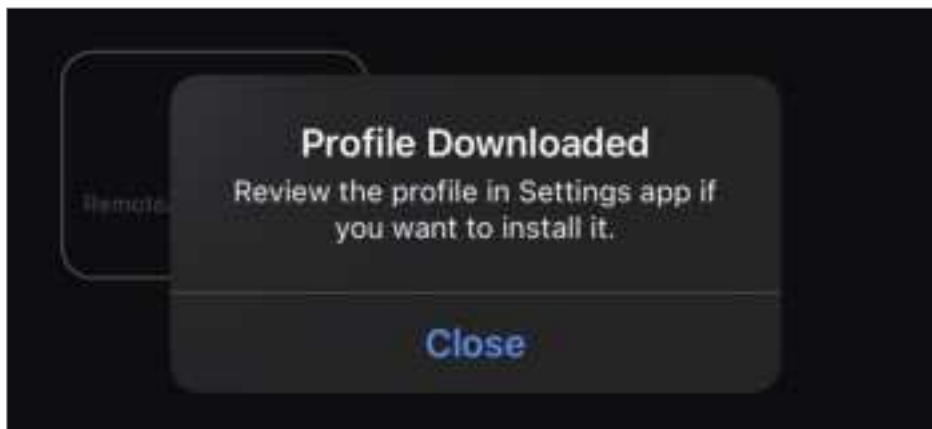


## Test IKEv2 Tunnel on iOS Client

Download iOS/macOS VPN configuration script.

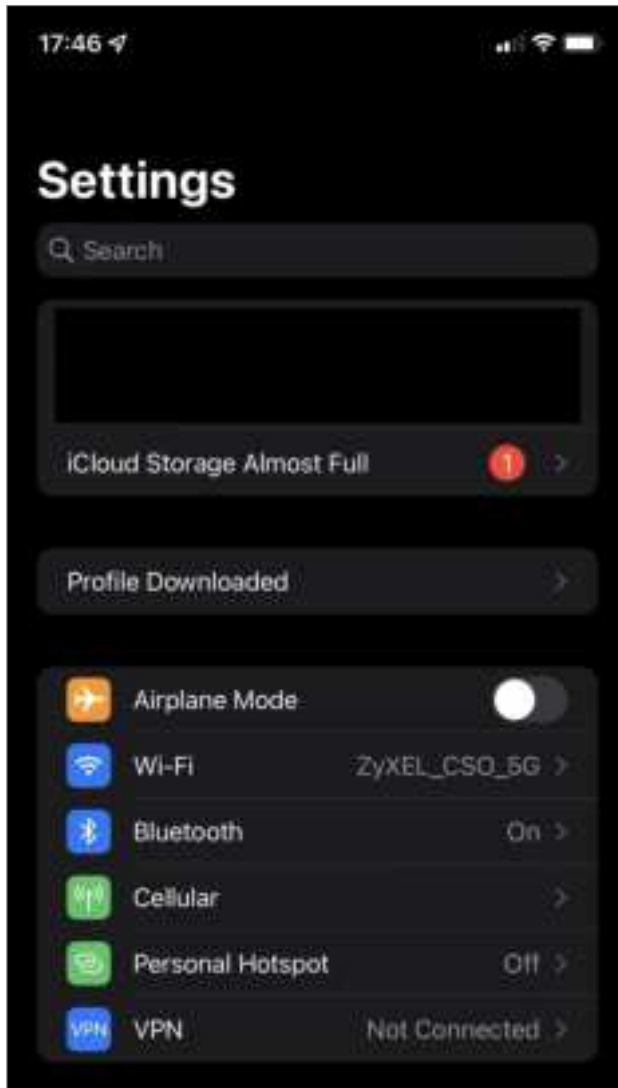


Send the script to Device.





Settings > Profile Downloaded

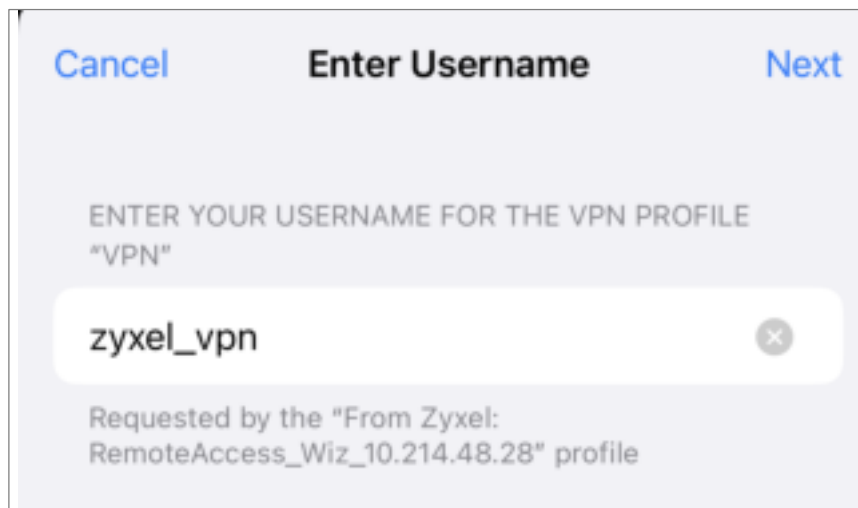




Press Install.



Enter Username and Password.





[Cancel](#)[Next](#)

**Enter Password**

ENTER YOUR PASSWORD FOR THE VPN PROFILE  
"VPN"

Requested by the "From Zyxel:  
RemoteAccess\_Wiz\_10.214.48.28" profile

Now, it can connect.

[<](#)**RemoteAccess\_Wiz\_10.214.48.28**[Edit](#)

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

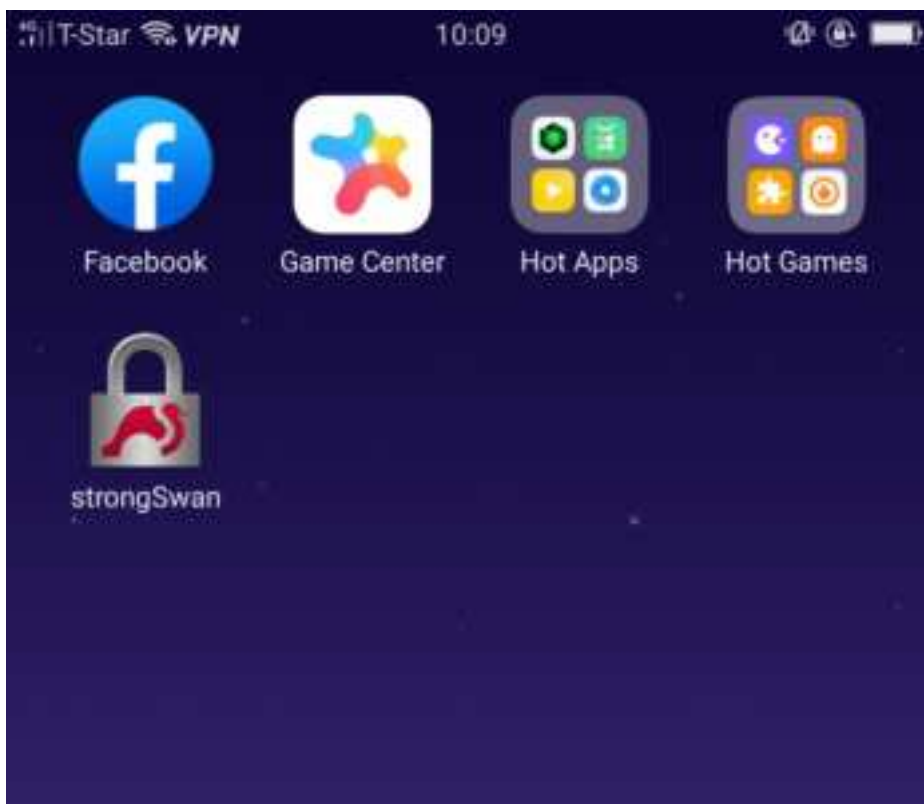


## Test IKEv2 Tunnel on Android Client

Download Android(strongSwan) VPN configuration script.



Download strongSwan from Google Play Store.





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

15:51

**Import VPN profile** **IMPORT**

Profile name  
RemoteAccess\_10.214.48.28

Server  
10.214.48.28

VPN Type  
IKEv2 EAP (Username/Password)

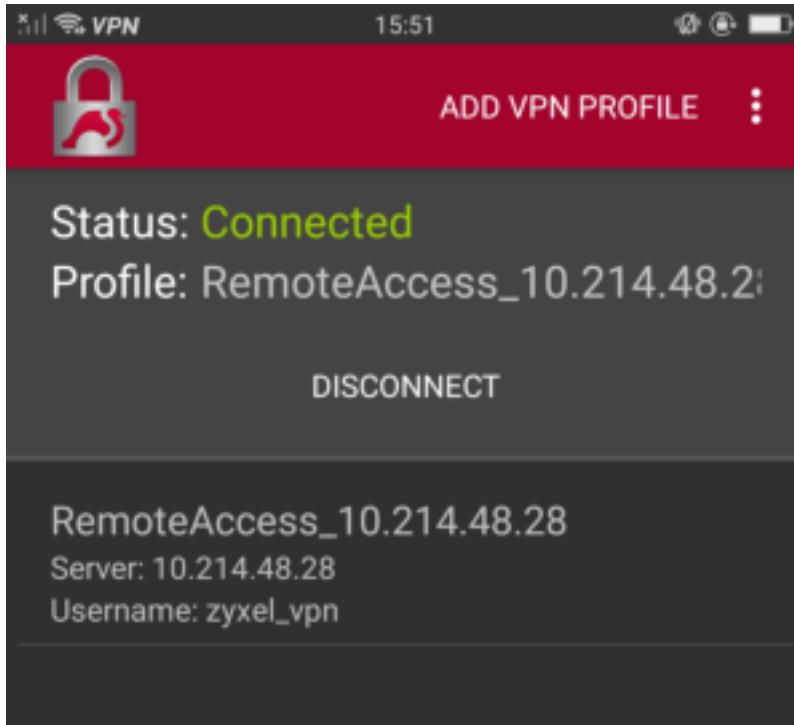
Username  
zyxel\_vpn

Password (optional)  
.....

CA certificate  
10.214.48.28



VPN is connected.





## Test OpenVPN

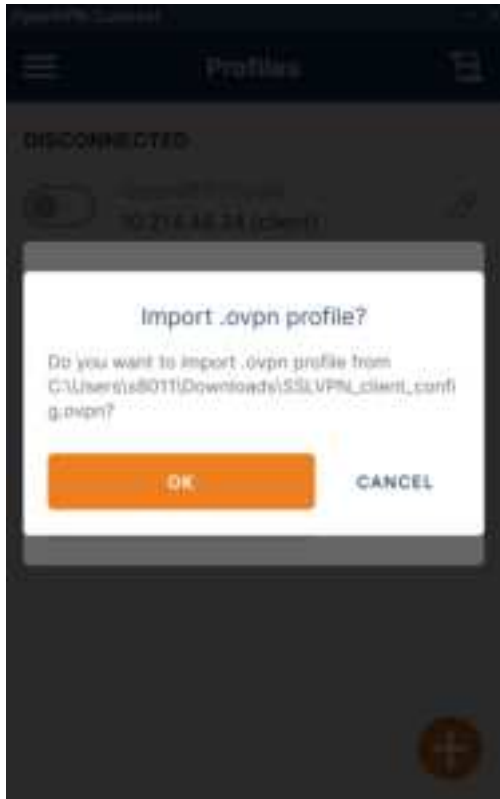
### VPN > SSL VPN

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

The screenshot displays the 'General Settings' tab for the SSL VPN configuration. At the top, there is a breadcrumb trail: 'VPN > SSL VPN'. Below this, the 'General Settings' section includes a description: 'Zyxel Remote VPN works with the SecuExtender VPN client and is also compatible with the OpenVPN Connect client.' A green toggle switch labeled 'Enable' is currently turned on. Below the toggle, there is a link 'SSL VPN Configuration Download' and a green 'Download' button. The 'Incoming Interface' section contains three fields: 'Interface' with a dropdown menu showing 'ge1 (WAN)', 'DNS Name' with an empty text box and a '(Optional)' label, and 'Server Port' with a text box containing '10443'. The 'Clients will use VPN to access' section has two radio button options: 'Internet and Local Networks (Full Tunnel)' which is selected, and 'Local Networks Only (Split Tunnel)'. A green toggle switch labeled 'Auto Start' is also present and turned on.



Import the config file.



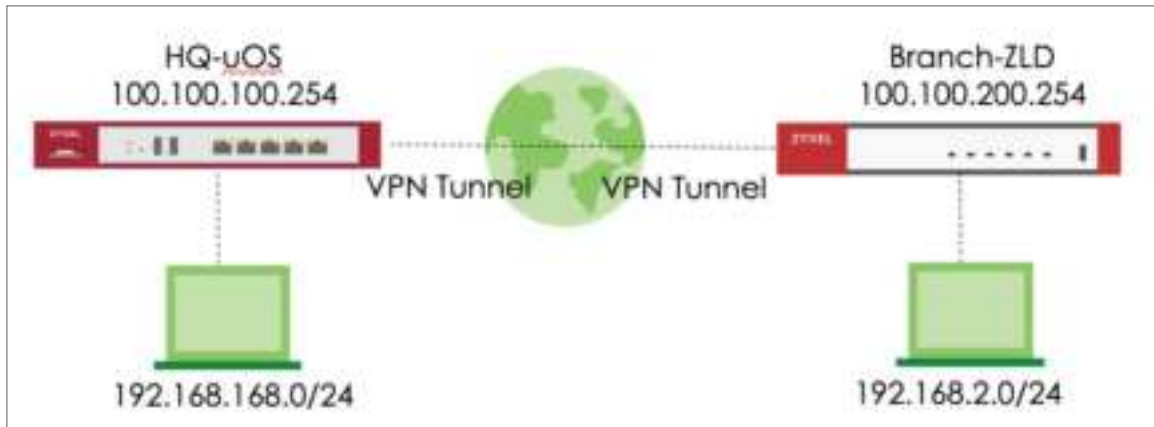
VPN is connected.





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

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

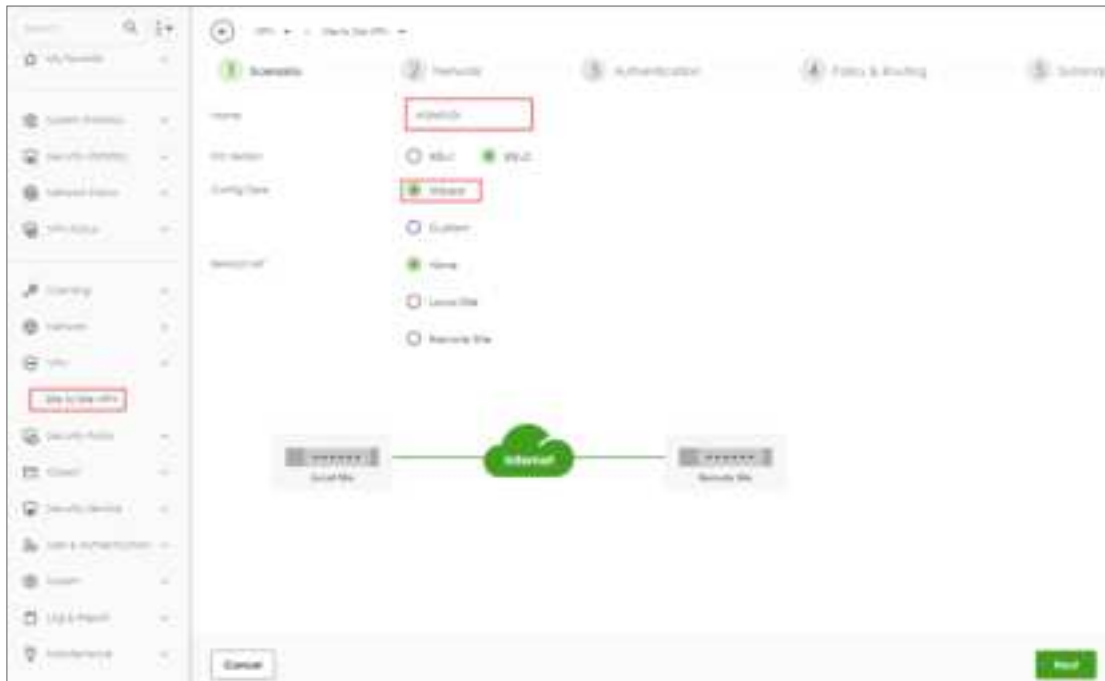




## Set up IPSec VPN Tunnel for uOS

### VPN > Site to Site VPN > Scenario

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





**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**

The screenshot shows the ZyXEL VPN configuration interface for Site to Site VPN. The top navigation bar indicates the current step is 'Authentication' (step 3) in a sequence of five steps: Scenario, Network, Authentication, Policy & Routing, and Summary. The 'Authentication' section has two radio button options: 'Pre-Shared Key' (selected) and 'Certificate'. A red rectangular box highlights the 'Pre-Shared Key' input field, which contains a series of 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 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 ZyXEL VPN configuration interface, specifically the 'Policy & Routing' step (indicated by a green '4' in a circle). The interface includes a progress bar at the top with steps: Scenario, Network, Authentication, Policy & Routing, and Summary. Below the progress bar, there are two radio buttons: 'Route Based' (unselected) and 'Policy Based' (selected). Under 'Policy Based', there are two input fields: 'Local Subnet' with the value '192.168.148.0/24' and 'Remote Subnet' with the value '192.168.200.0'. Below these fields is a network diagram showing a 'Local Site' (192.168.148.0/24) connected to an 'Internet' cloud, which is then connected to a 'Remote Site' (192.168.200.0/24). At the bottom of the interface, there are three buttons: 'Cancel', 'Back', and 'Next'.



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

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

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

Scenario Network Authentication Policy & Routing Summary

**Configuration**

Name: vpn001

IKE Version: 2

Type: Policy-based

Proposal: ☒

**Network**

Local Site: 192.168.100.0/24

Remote Site: 192.168.200.0/24

**Authentication**

Authentication: group1

**Policy & Routing**

Local Gateway: 192.168.100.254



## 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: FLEXtOS

**IKE Version**

☐ IKEv1

☒ IKEv2

**Gateway Settings**

**My Address**

☒ Interface: wan Static — 100.100.200.254/255.255.0.0

☐ Domain Name / IPv4

**Peer Gateway Address**

☒ Static Address ⓘ

Primary: 100.100.100.254

Secondary: 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

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

☐ Dynamic Address ⓘ

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  [View Certificate](#)

**Advance**

Local ID Type:

Content:

Peer ID Type:

**Phase 1 Settings**

SA Life Time:  (180 - 3000000 Seconds)

**Proposal**

ID	Encryption	Authentication
1	AES128	SHA1

Key Group:

OK Cancel



## VPN > IPSec VPN > VPN Connection

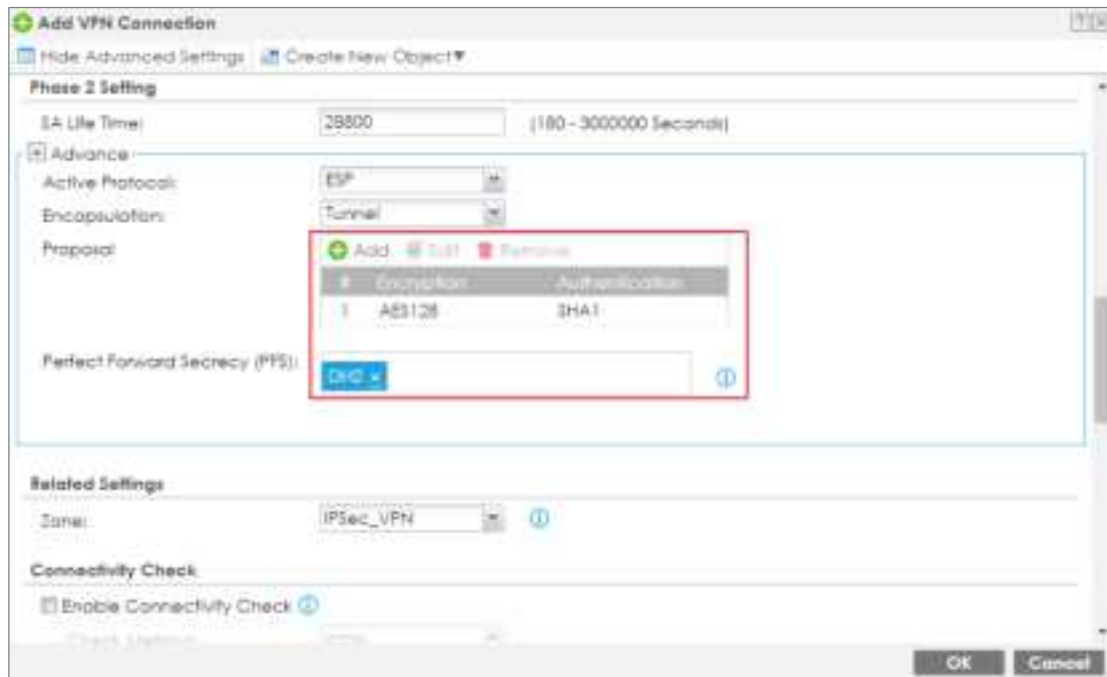
Select VPN Gateway and set Local Subnet to be the IP address of the network connected to be ZyWALL and Remote Subnet to be the IP address of the network connected to the peer USG FLEX H.

The screenshot shows the 'Edit VPN Connection FLEXtuoOS\_P2' window. The 'General Settings' section has 'Enable' checked and 'Connection Name' set to 'FLEXtuoOS\_P2'. The 'VPN Gateway' section has 'VPN Tunnel Interface' selected. The 'Policy' section shows 'Local Policy' as 'LAN2\_SUBNET' and 'Remote Policy' as 'USG\_subnet'. The 'VPN Gateway' field is set to 'FLEXtuoOS' with the IP address 'wan 100.100.100.254.0.0.0'. The 'Local Policy' field is set to 'LAN2\_SUBNET' with the IP address 'INTERFACE SUBNET, 192.168.2.0/24'. The 'Remote Policy' field is set to 'USG\_subnet' with the IP address 'SUBNET, 192.168.168.0/24'.

Section	Field	Value
General Settings	Enable	<input checked="" type="checkbox"/>
	Connection Name	FLEXtuoOS_P2
VPN Gateway	VPN Gateway	FLEXtuoOS wan 100.100.100.254.0.0.0
	VPN Tunnel Interface	<input checked="" type="radio"/>
Policy	Local Policy	LAN2_SUBNET INTERFACE SUBNET, 192.168.2.0/24
	Remote Policy	USG_subnet SUBNET, 192.168.168.0/24



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





## Test IPsec VPN Tunnel

**Ping the PC that is connected to ZLD device**

Win 11 > cmd > ping 192.168.2.34

```

Connection-specific DNS Suffix  : 
IPv4 Address. . . . . : 192.168.2.100
Subnet Mask . . . . . : 255.255.255.0
IPv4 Address. . . . . : 192.168.2.100
Subnet Mask . . . . . : 255.255.255.0
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 Ethernet 4:

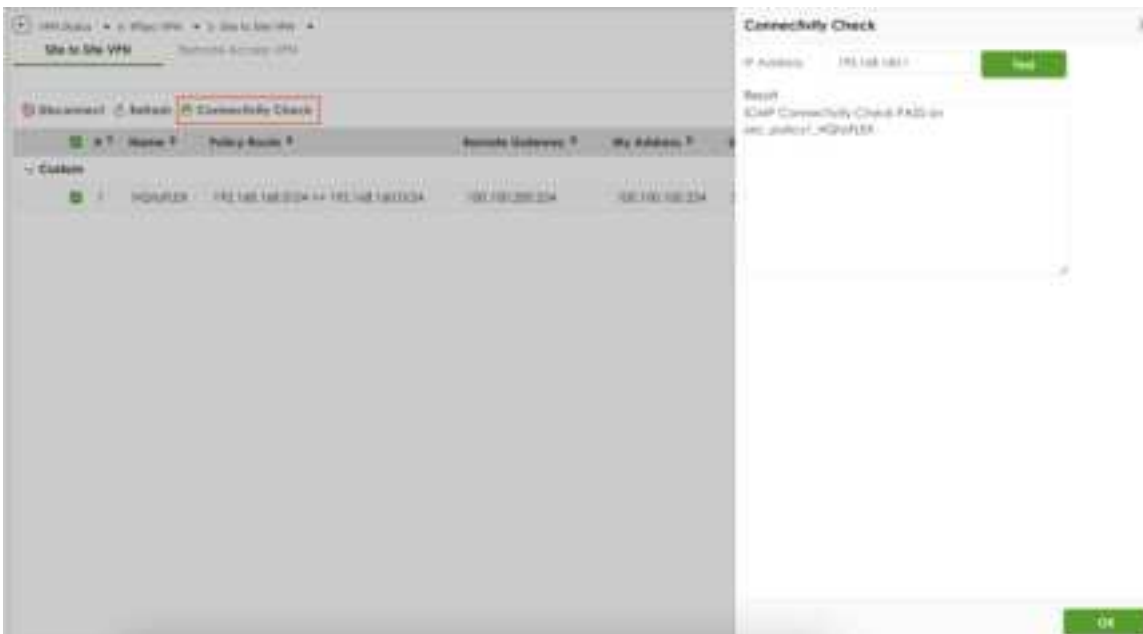
C:\Windows\system32>ping 192.168.2.34

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
  
```

## VPN Status > IPsec VPN

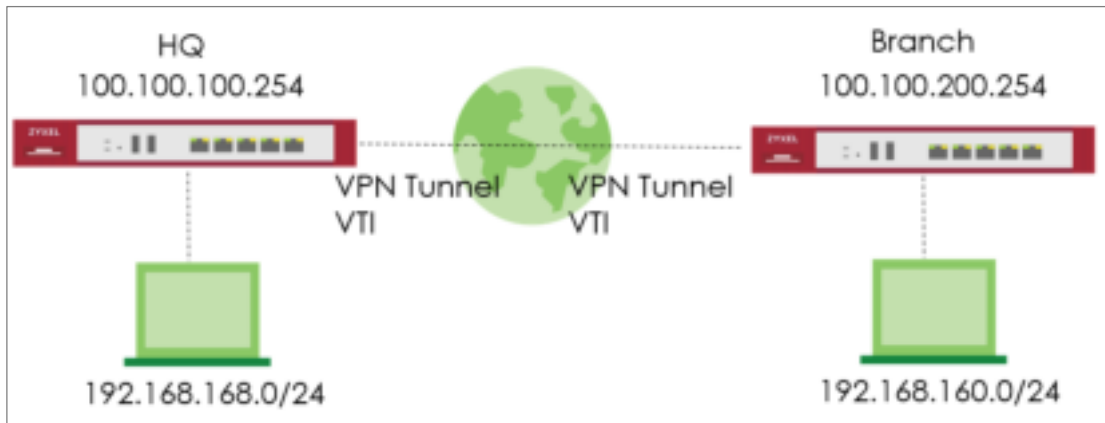
Verify the IPsec VPN status and do the Connectivity Check





## 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**.





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

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

Progress: 1 Overview 2 **Network** 3 Authentication 4 Policy & Routing 5 Summary

My Address:

Peer Gateway Address:

Local IP: 100.100.100.234

Remote IP: 100.100.100.234

Buttons: 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 > Authentication

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

Pre-Shared Key

Cancel Back Next



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

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

The screenshot displays the 'Policy & Routing' configuration page for a Site-to-Site VPN. At the top, a progress bar shows five steps: Scenario, Network, Authentication, Policy & Routing (current), and Summary. Below the progress bar, the 'Type' is set to 'Route-Based' (indicated by a green checkmark and a red box) and 'Policy-Based' is unselected. The 'Remote Subnet' is configured as '192.168.160.0/24' (also highlighted with a red box). A network diagram at the bottom illustrates the setup: a 'Any' host connects to a 'Local Site' (100.100.100.254), which connects to the 'Internet' cloud, then to a 'Remote Site' (100.100.200.254), and finally to a host with IP '192.168.160.2/24'. At the bottom of the interface are 'Cancel', 'Back', and 'Next' 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
IK2 Version	2
Scenario	wizard
Type	Route

Edit

**Network**

Local Site	190.100.100.254
Remote Site	190.100.200.254

**Authentication**

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

**Policy & Routing**

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

Close

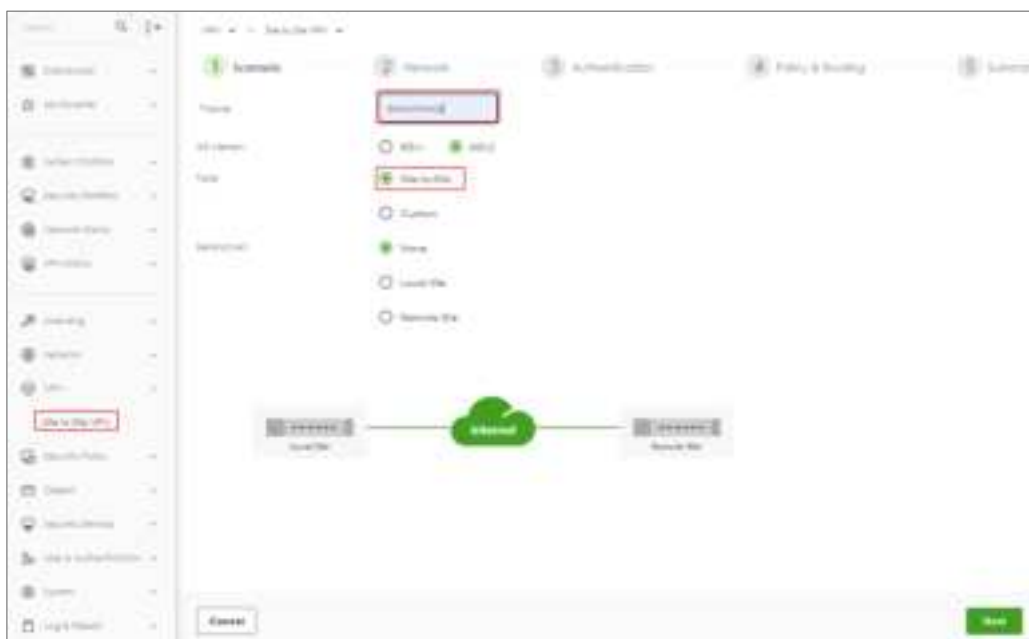


## Set up IPsec VPN Tunnel for Branch

### 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**.





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

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

VPN > Site to Site VPN

Scenario **2** Network Authentication Policy & Routing Summary

My Address Domain Name / IP 100.100.200.254

Peer Gateway Address Domain Name / IP 100.100.200.254

Local Site 100.100.200.254 Internet Remote Site 100.100.100.254

Cancel Back Next



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

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

Step 3 of 5: Authentication

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

Authentication

Pre-Shared Key: [Redacted]

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 > 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	branchHQ2		
IP Version	2		
Scenario	site2site		
Type	Route		

Full

**Network**

Local Site	100.100.200.204		
Remote Site	100.100.100.204		

**Authentication**

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

**Policy & Routing**

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

Close



## Test IPSec VPN Tunnel

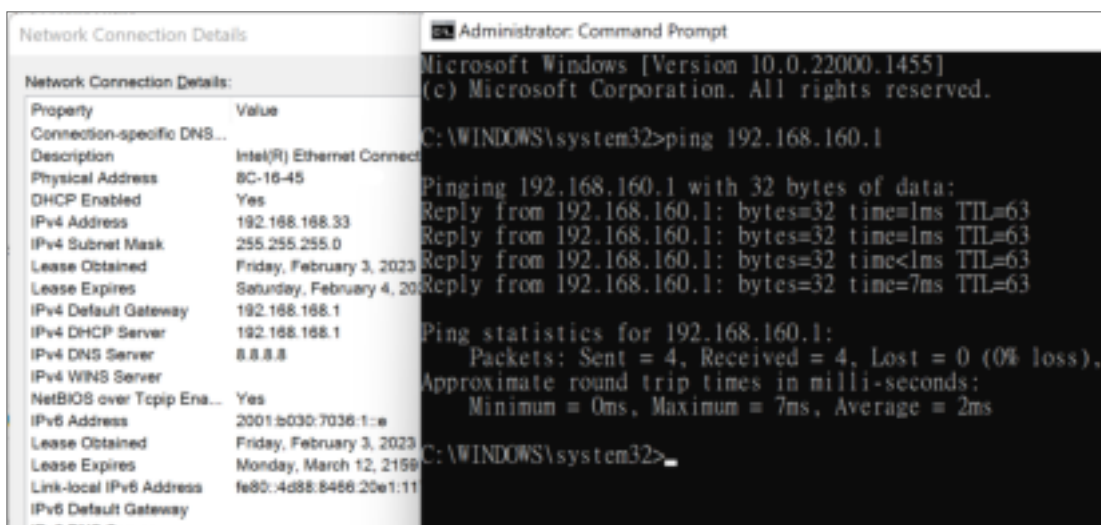
### VPN Status > IPSec VPN

Verify the IPSec VPN status.



### Ping the PC in Branch Office

Win 11 > cmd > ping 192.168.160.1





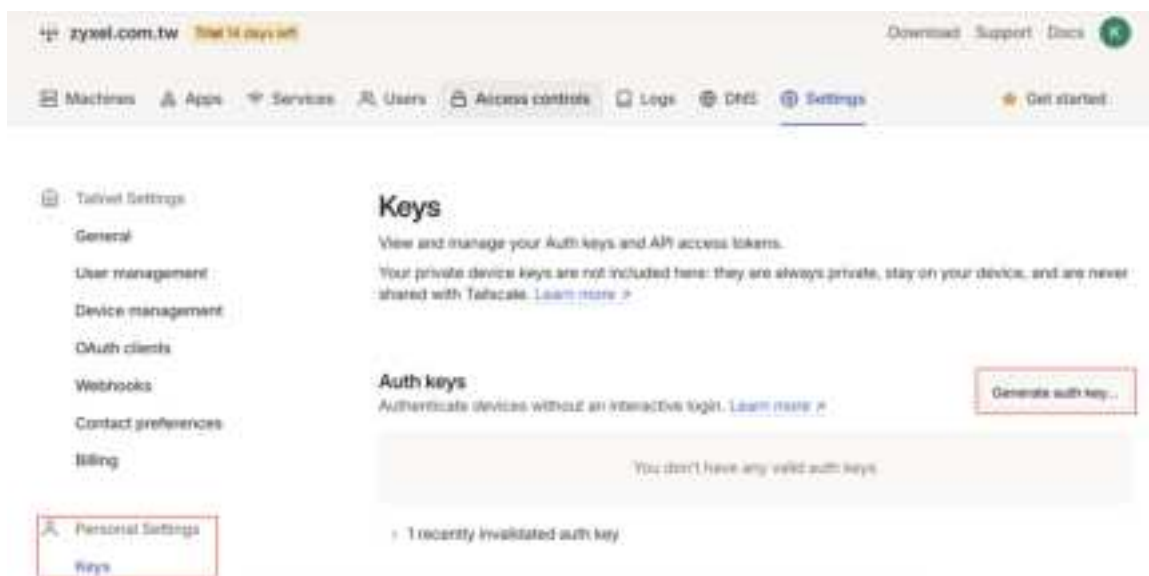
## How to Use Tailscale

### 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".





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.

Zyxel

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

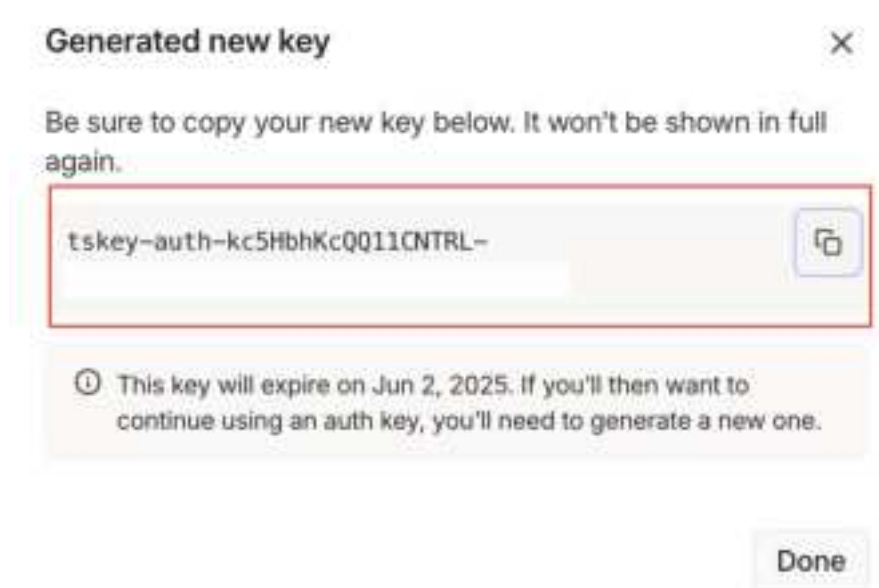
Devices authenticated by this key will be automatically tagged. This will also disable node key expiry for the device. [Learn more](#)

Cancel

Generate key



Copy the key.



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



**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.



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



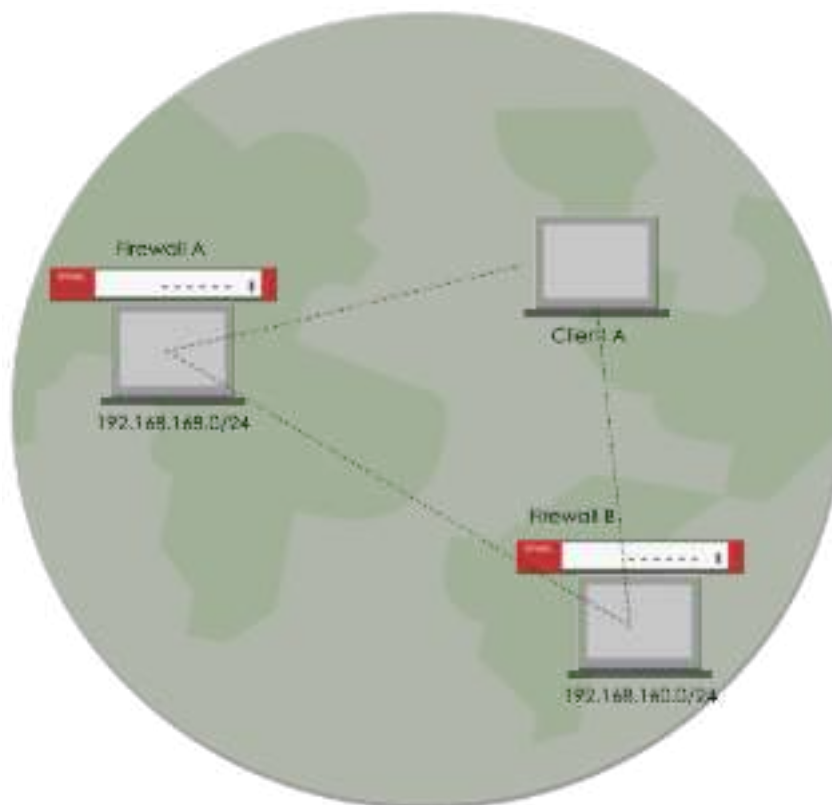
Click "Disable key expiry" for all client to prevent lost connection while expire.





## 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.



The screenshot shows the ZyXEL VPN configuration interface for Firewall A. The 'General Settings' section includes an 'Enable' toggle (checked), a 'Server Port' of 4144, and a 'Zone' of 'Tobacco'. The 'Routing' section has 'As an Exit Node' checked. The 'Advertised Networks' section shows a list with one entry: '192.168.168.0/24'.

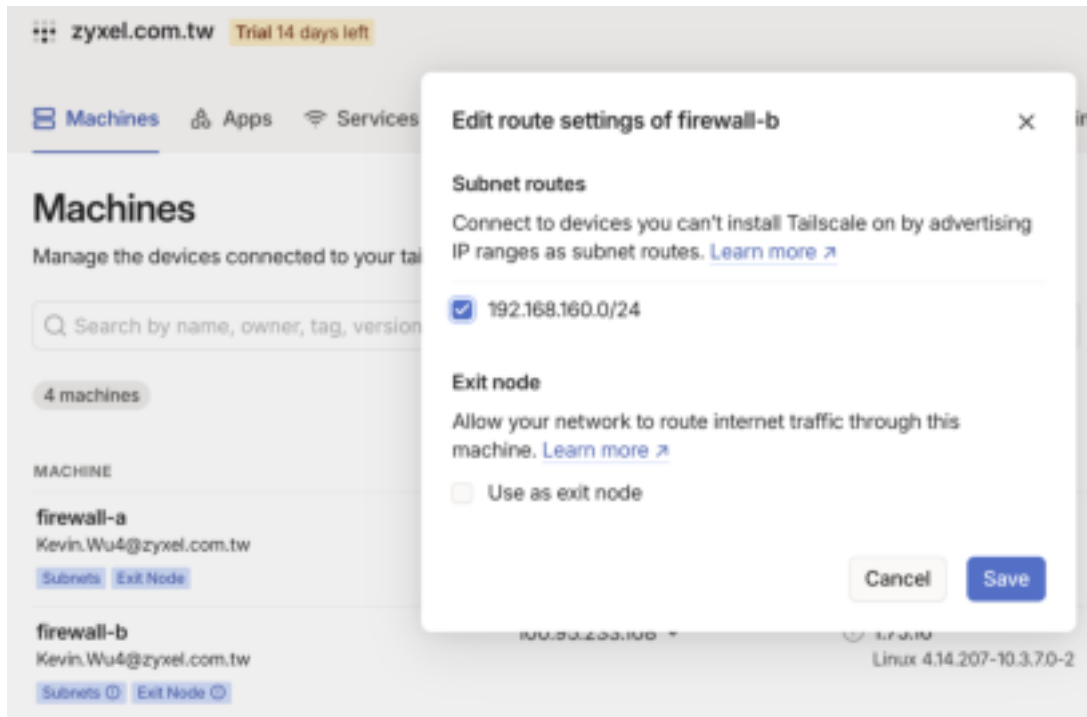
2. Advertised 192.168.160.0/24 in Firewall B.



The screenshot shows the ZyXEL VPN configuration interface for Firewall B. The 'General Settings' section includes an 'Enable' toggle (checked), a 'Server Port' of 4144, and a 'Zone' of 'Tobacco'. The 'Routing' section has 'As an Exit Node' checked. The 'Advertised Networks' section shows a list with one entry: '192.168.160.0/24'.



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\MT83234\Downloads>route print | findstr "192.168.168.0 192.168.168.0"
192.168.168.0 255.255.255.0 100.100.100.100 100.95.1.123 0
192.168.168.0 255.255.255.0 100.100.100.100 100.95.1.123 0

C:\Users\MT83234\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\MT83234\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 = 138ms
```



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

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

The screenshot displays the ZyXEL Firewall configuration page for Firewall A. The interface is divided into several sections:

- General Settings:**
  - Enable:** A green toggle switch is turned on.
  - Auth Type:** A dropdown menu is set to "Basic", with a green "Login" button next to it.
  - Server Port:** A text field contains "4144", with "[1-65535]" shown as a hint.
  - Zone:** A dropdown menu is set to "Tobacco".
- Routing:**
  - Act as Exit Node:** A green toggle switch is turned on.
- Advanced Networks:**
  - Buttons for "+ Add" and "Remove" are visible.
  - A table lists the configured networks:

Network #	Network
1	192.168.1.0/24
- Advanced Settings:**
  - Accept routes:** A green toggle switch is turned on.
  - Default SNAT:** A green toggle switch is turned on.



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 ↗](#)

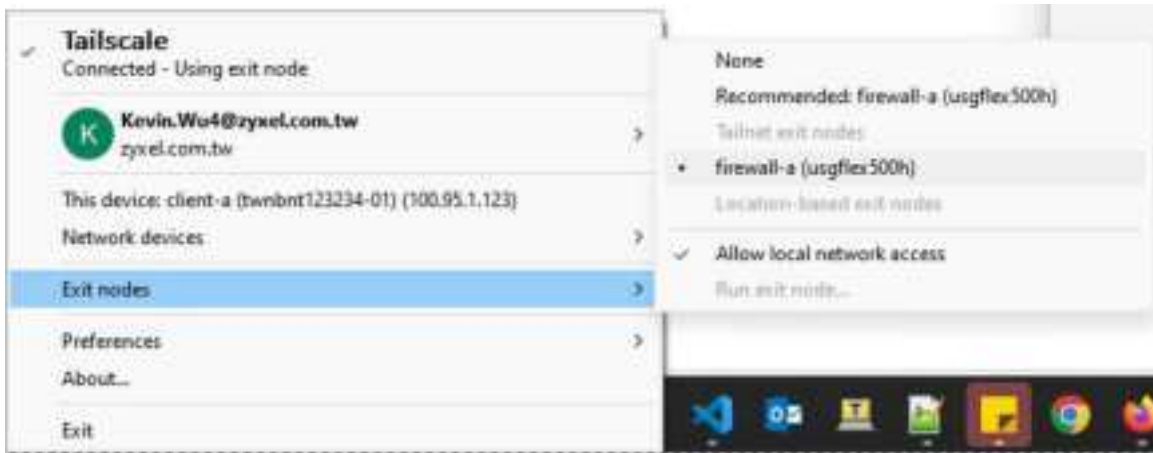
☒ Use as exit node

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@wujiayuandeMacBook-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 0xfffff00 broadcast 192.168.168.255
    nd6 options=201<PERFORMNUD,DAD>
    media: autoselect (1000baseT <full-duplex>)
    status: active
kevin@wujiayuandeMacBook-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 藍牙網路連接:

    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
```



## How to use Ext-group user to connect Remote Access VPN

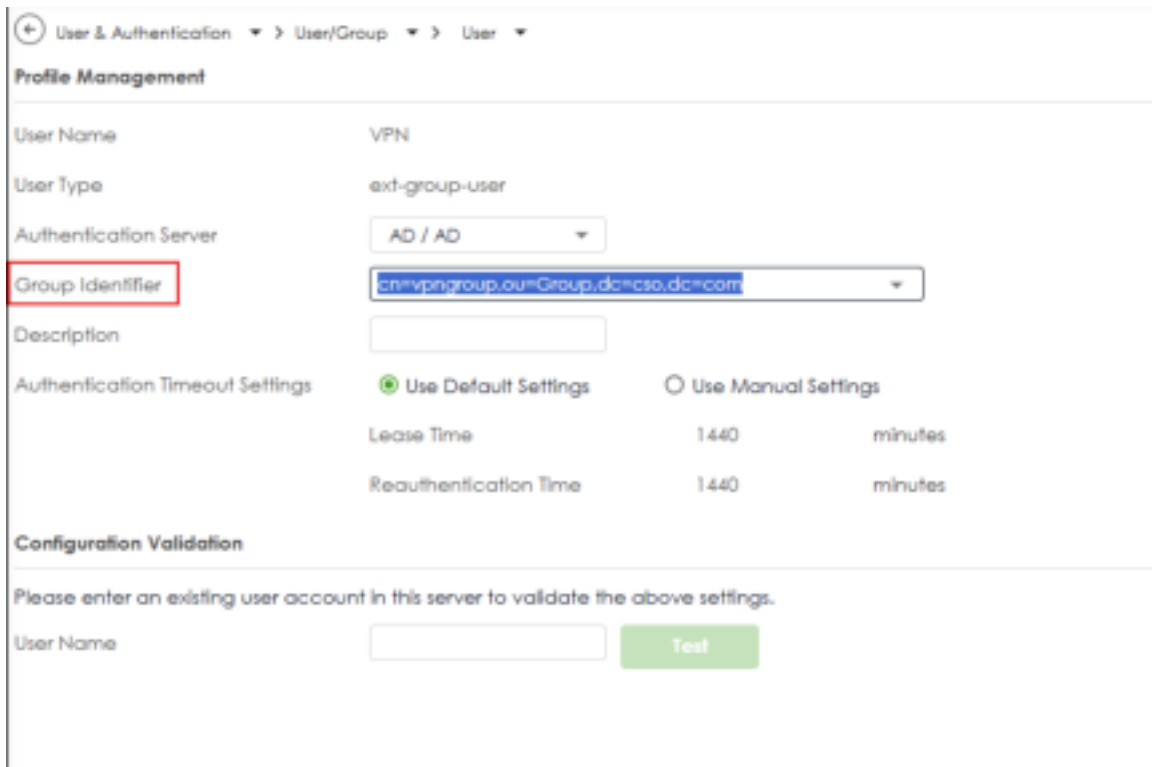
Remote Access VPN now supports using external user groups for VPN accounts. This article will guide you through the setup process

### Before Begin

You already followed Topic "How to configure Remote Access VPN with Zyxel VPN Client" as well as "How to setup AD authentication with Microsoft AD" to complete Remote Access and Authentication server settings.

### User & Authentication > User/Group > User

Create a user and select User type as ext-group-user. At this point, the group identifier will Automatically populate with the CN that has the group attribute.



User & Authentication > User/Group > User

**Profile Management**

User Name	VPN		
User Type	ext-group-user		
Authentication Server	AD / AD		
Group Identifier	cn=vpngroup,ou=Group,dc=cso,dc=com		
Description			
Authentication Timeout Settings	<input checked="" type="radio"/> Use Default Settings <input type="radio"/> Use Manual Settings		
Lease Time	1440	minutes	
Reauthentication Time	1440	minutes	

**Configuration Validation**

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

User Name	<input type="text"/>	<input type="button" value="Test"/>
-----------	----------------------	-------------------------------------



## VPN > SSL VPN

Taking SSL VPN as an example, User select the ext-group user you just created. And choosing AD authentication.

VPN > SSL VPN

### 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)

Auto NAT ☒

☐ Local Networks Only (Split Tunnel)

### Client Network

IP Address Pool:

First DNS Server: ☒ ZyWALL

☐ Custom Defined

Second DNS Server:

### Authentication

Primary Server:

Secondary Server:

User:



## Test the Result

### VPN Status > SSL VPN > Remote Access VPN

User within the group can successfully connect



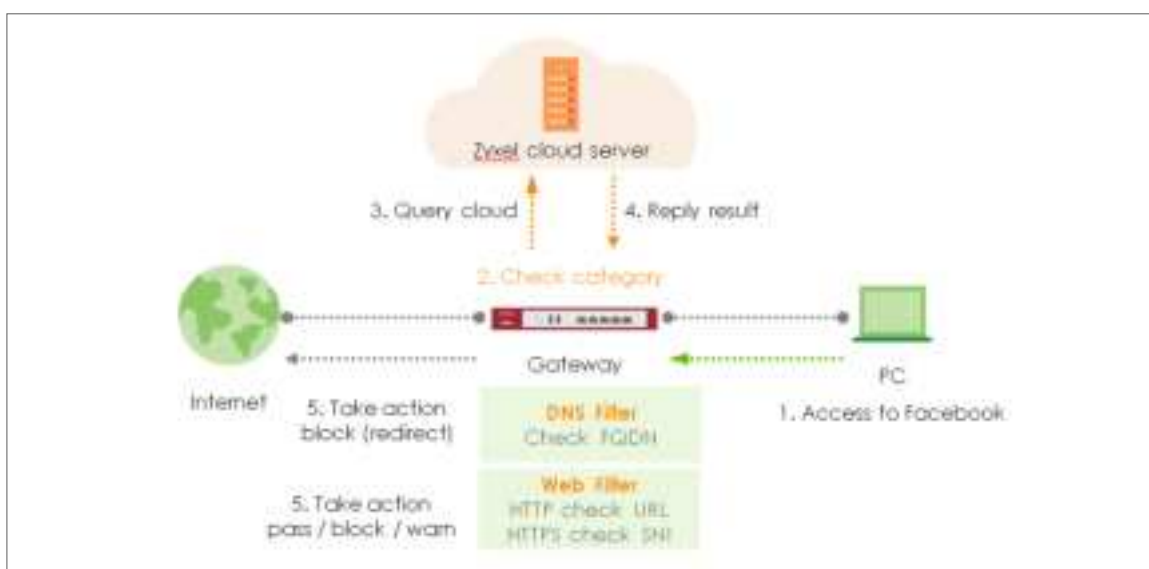
Username	Assigned IP	Remote IP	Up Time	Download Time	Download (Kbps)	Upload (Kbps)
jerry	192.168.4.2	192.168.4.6	00:00:00	(0/0/0)	1014 kbps	743 kbps




## 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).



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

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

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

Copyright © 2025 Zyxel and/or its affiliates. All rights reserved. 92



## 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.

Item	Type	Issued	Valid from	Valid to	Refer...
default	SELF	CH-HSG_FLEX_200HP_08...	CH-HSG_FLEX_200HP_08...	May 29 00:43:22 ...	May 24 03:43:22 ...

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

Export Certificate

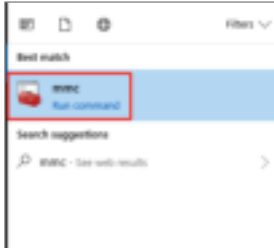
Password:

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

Export Certificate



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



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

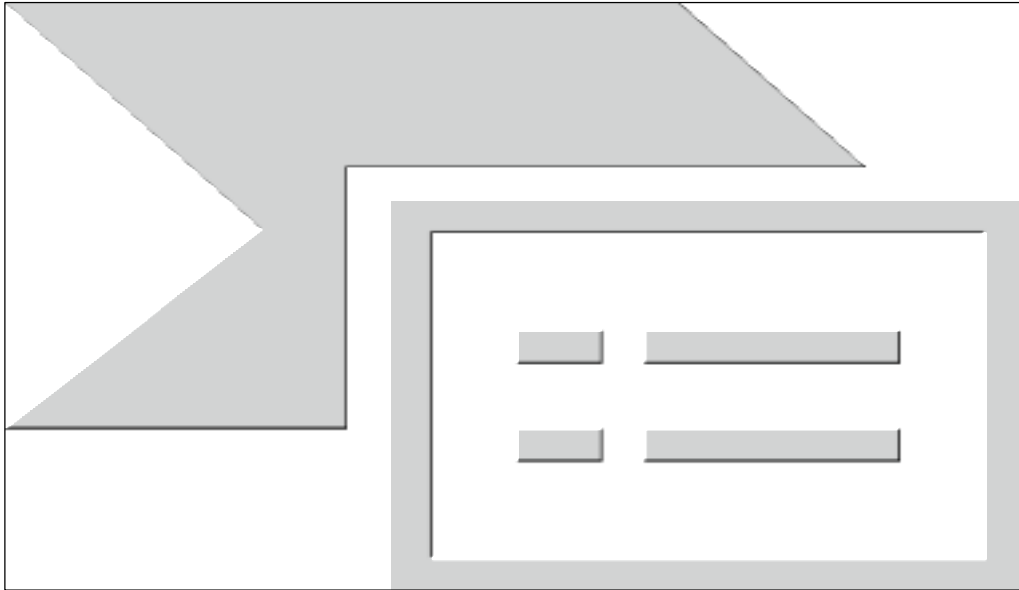


In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.





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.

**File to Import**  
Specify the file you want to import.

---

File name:

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

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)



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



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

← Certificate Import Wizard

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

---

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

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

☒ Place all certificates in the following store:

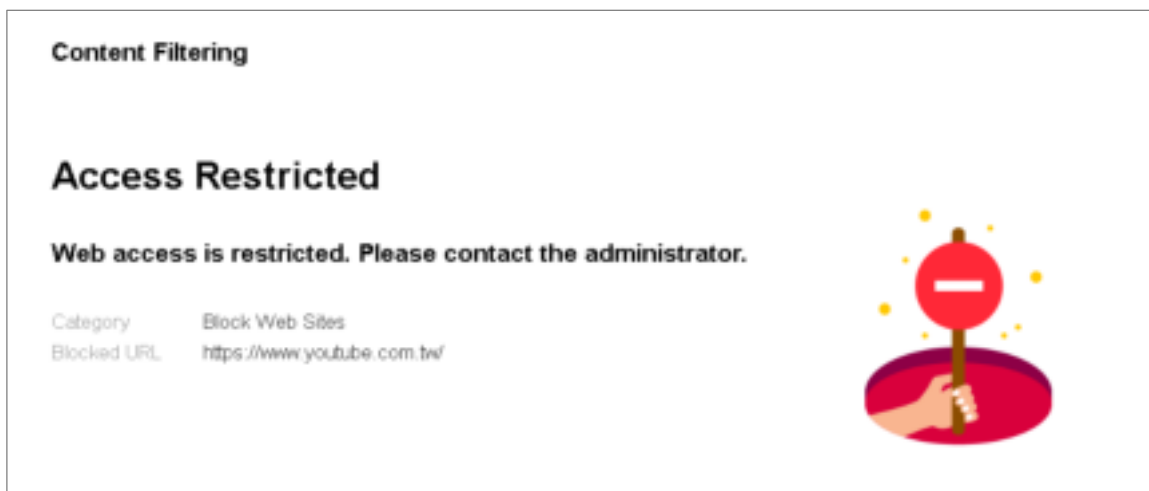
Certificate store:  
Trusted Root Certification Authorities

Browse...



## Test the Result

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



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

Log & Report > Log/Events

Category: Content Filter Filter Refresh Clear Log

#	Time	Category	Message	Source IP	Destination IP	Rule
71	2023-05-29 19:11:15	content-filter	www.youtube.com/StreamingMedia, rule_name:URL_Outgoing, 3364 (Content Filter)	192.168.148.24	34.204.85.242	WEB BLOCK
103	2023-05-29 19:11:52	content-filter	youtube-vl3.google.com/Internet/Services, rule_name:URL_Outgoing	192.168.148.20	192.168.148.1	SHS REDIRECT
154	2023-05-29 19:16:42	content-filter	www.youtube.com/StreamingMedia, rule_name:URL_Outgoing, 3364 (Content Filter)	192.168.148.24	34.204.85.242	WEB BLOCK
238	2023-05-29 19:29:32	content-filter	www.youtube.com/StreamingMedia, rule_name:URL_Outgoing	192.168.148.24	148.195.1.1	SHS REDIRECT
239	2023-05-29 19:29:32	content-filter	www.youtube.com/StreamingMedia, rule_name:URL_Outgoing	192.168.148.24	148.195.1.1	SHS BLOCK
240	2023-05-29 19:29:32	content-filter	www.youtube.com/StreamingMedia, rule_name:URL_Outgoing	192.168.148.24	148.195.1.1	SHS BLOCK

Nowpage 31 1-4 of 1



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

The screenshot shows the AWS IAM console 'Groups' page. The left-hand navigation menu has a green circle highlighting the 'Groups' link. The main content area shows a list of groups, with 'Group1' selected and highlighted by a red rectangle. The 'Group1' group is shown with a 'Users' count of 10 (100%). Below the group list, a table shows the details of the 'Group1' group, including its name, path, and the number of users.

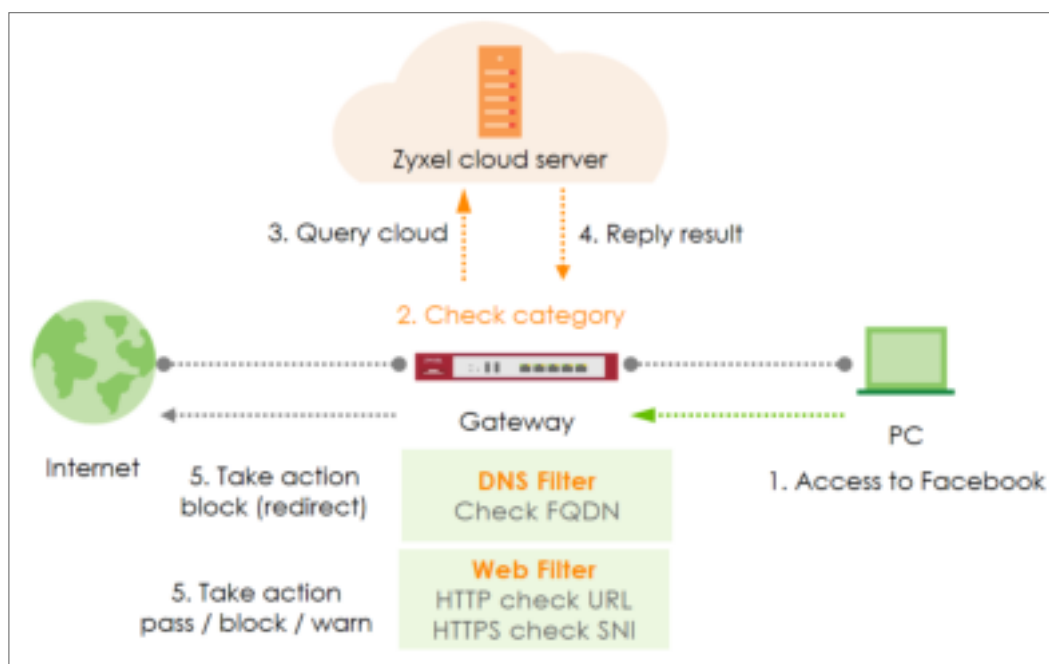
Group ID	Group Name	Group Path	Group Type	Group Status	Group Size	Group Users
g-123456789012	Group1	/	Group	Active	10	10 (100%)
g-123456789013	Group2	/	Group	Active	5	5 (100%)
g-123456789014	Group3	/	Group	Active	3	3 (100%)




## 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.

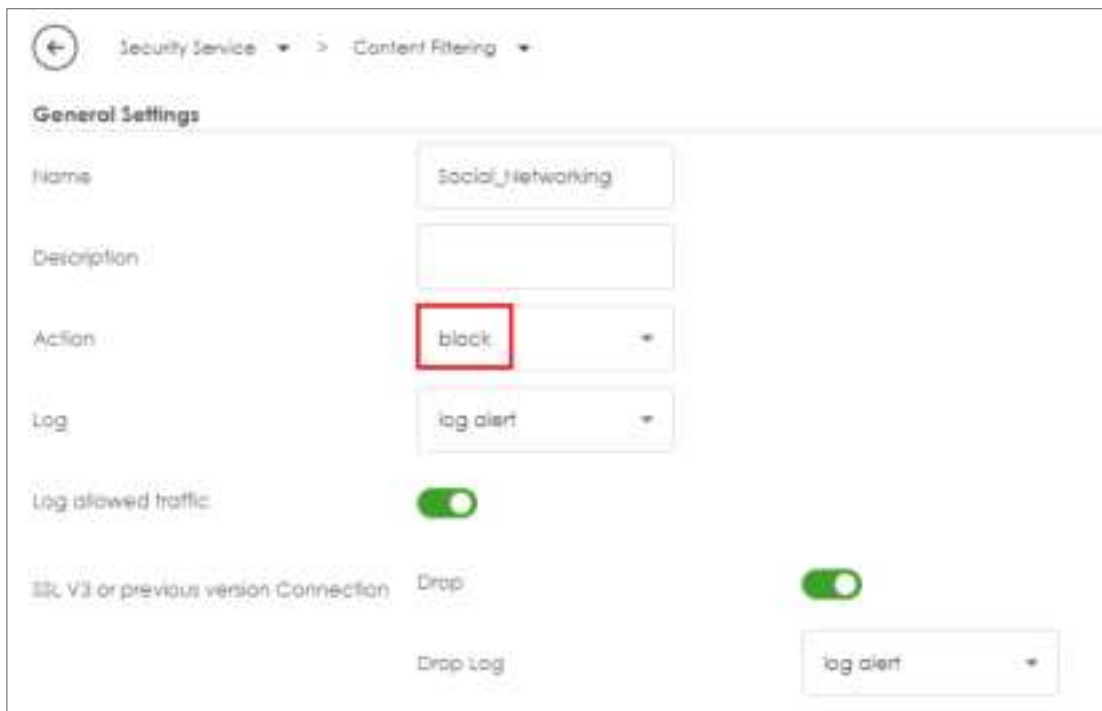


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).



## 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.



← Security Service > Content Filtering >

**General Settings**

Name: Social\_Networking

Description:

Action: **block**

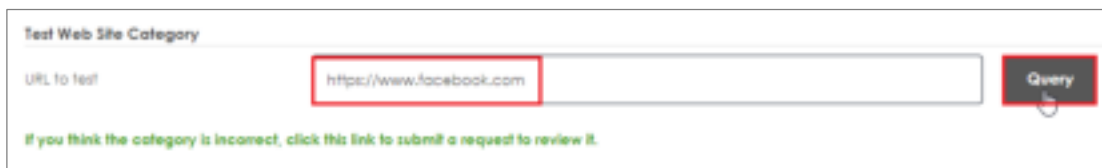
Log: log alert

Log allowed traffic: ☒

SSL V3 or previous version Connection: Drop

Drop Log: log alert

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



**Test Web Site Category**

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

**Query**

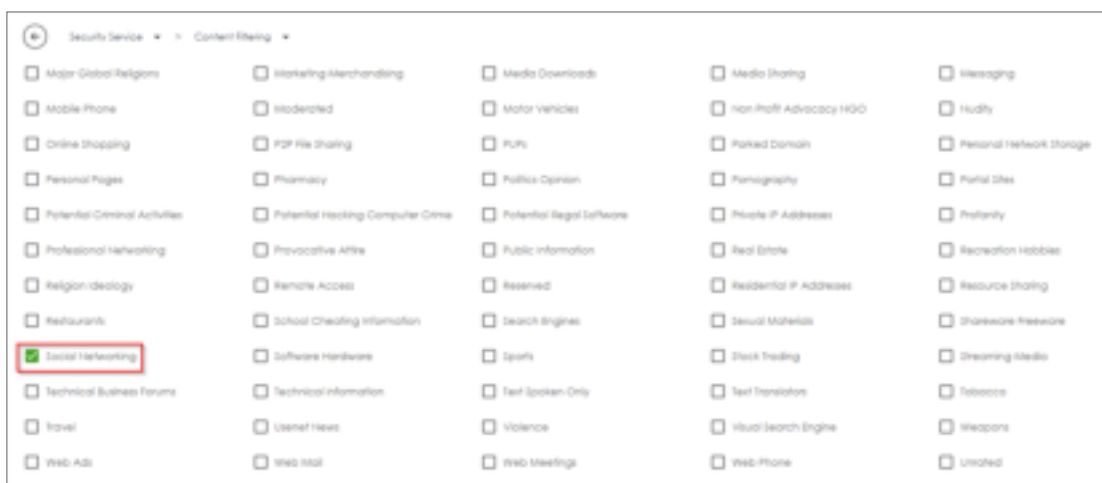
[If you think the category is incorrect, click this link to submit a request to review it.](#)



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

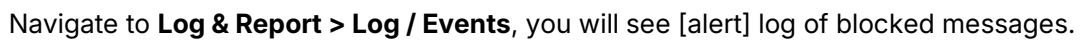
Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies and apply the **Profile > Content Filter** "Social\_Networking" on this security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

The screenshot displays the ZyXEL Security Policy configuration page. The 'Configuration' section includes fields for Name, Description, From, To, Source, Destination, Service, User, Schedule, Action, and Log. The 'Profile' section includes fields for Restriction Profile, Content Filter, and SS. The 'Content Filter' field is set to 'Social\_Networking'.

Field	Value
Name	Block_Social_Networking
Description	
From	L2L
To	L2L
Source	any
Destination	any
Service	any
User	any
Schedule	none
Action	allow
Log	no
Restriction Profile	none
Content Filter	Social_Networking
SS. Restricted	none



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

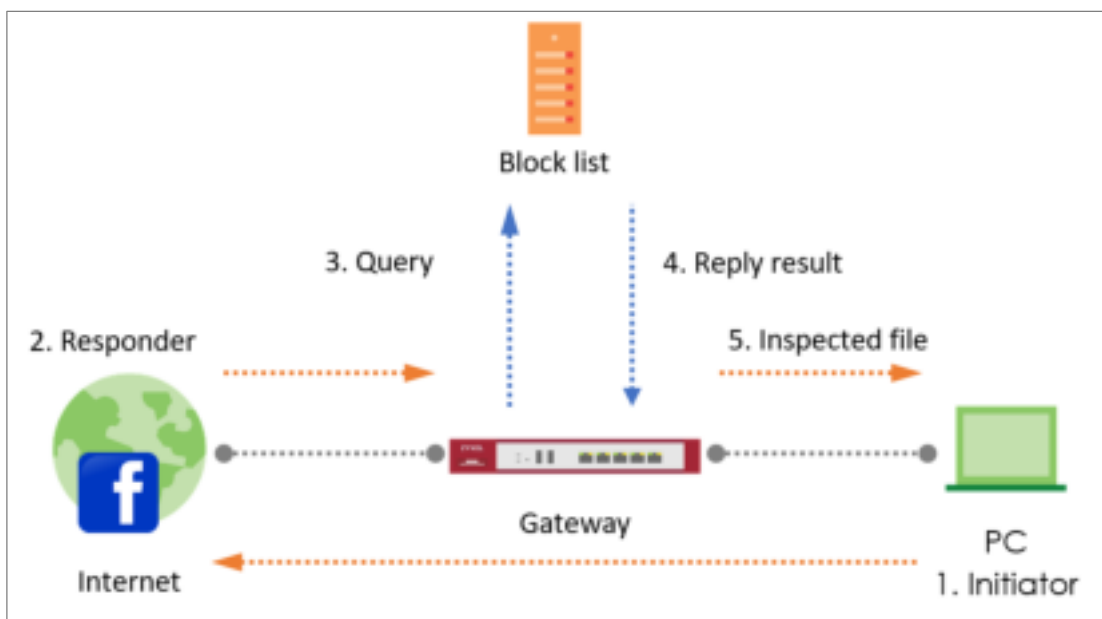



id	date	time	location	status	action
1	2023-01-01	10:00	Room 101	Open	Start
2	2023-01-01	11:00	Room 101	Open	Start



## 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.



Security Service > Content Filtering > Profile Management > Add a Content Filter profile

**General Settings**

Name: Facebook\_Block

Description:

Action: **Block**

Log: log client

Log allowed traffic: ☐

SSL V3 or previous session Connection: ☒

Create log: log client

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



Block List

URL: \*.facebook\*.com

Add



## Set Up the Security Policy

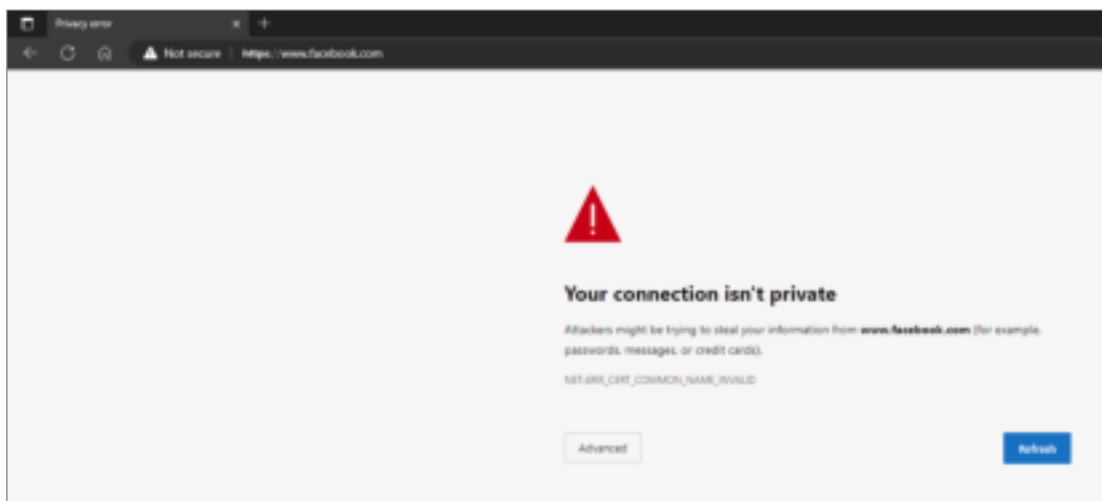
Go to **Security Policy > Policy Control** to configure a **Name** for you to identify the **Security Policy** profile. For **From** and **To** policies, select the direction of travel of packets to which the policy applies and apply the **Profile > Content Filter** "Facebook\_Block" on this security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

The screenshot displays the ZyXEL Security Policy configuration page. The 'Configuration' section includes a 'Name' field set to 'Facebook\_Block', a 'From' field set to 'LAN', and a 'To' field set to 'WAN'. Below these are fields for 'Source', 'Destination', 'Service', 'User', 'Protocol', 'Action', and 'Log'. The 'Profile' section at the bottom shows 'Content Filter' set to 'Facebook\_Block' and 'Action' set to 'Block'.



## Test the Result

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



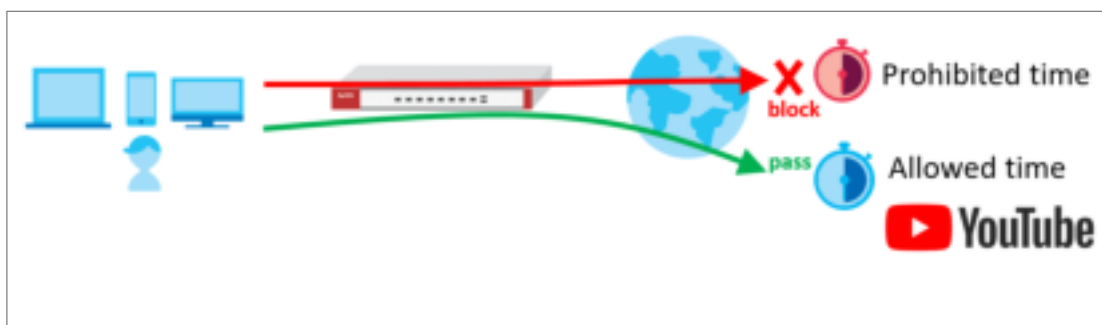
Go to **Log & Report > Log / Events**, you will see [alert] log of blocked messages.


ID	Time	Category	Message	Source	Destination	Result
1	2023-09-02 15:34:09	content filter	www.facebook.com/block-2f-Rule_namefacebook_block-2023 (Content filter)	192.168.1.68:80	82.23.26.65	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.

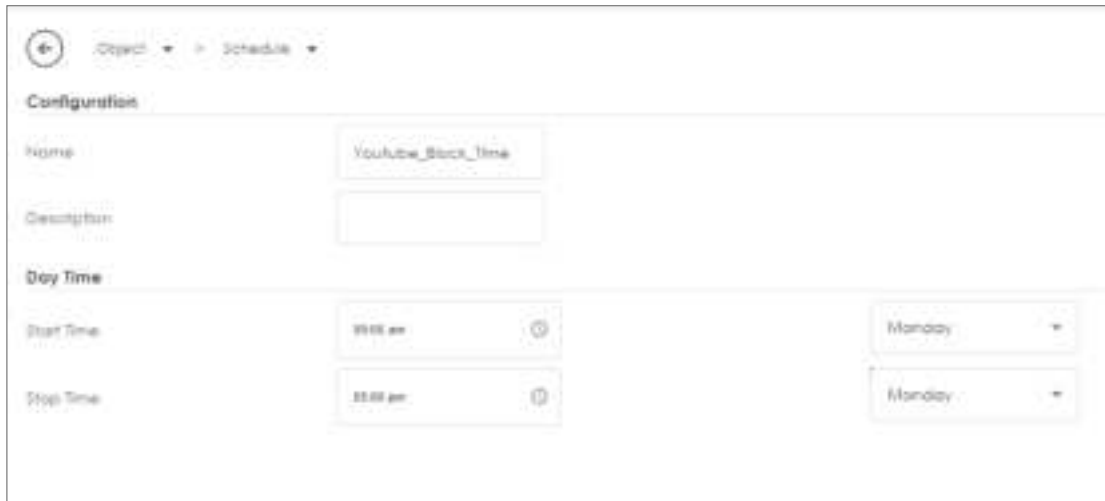


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).



## 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.



The screenshot shows a web interface for configuring a recurring schedule rule. At the top, there is a breadcrumb navigation: Object > Schedule > Recurring > Add Schedule Recurring Rule. Below this is a 'Configuration' section with the following fields:

- Name:** A text input field containing 'Youtube\_Stock\_Time'.
- Description:** An empty text input field.
- Day Time:** A section containing two rows of time and day selection.
  - Start Time:** A time selection dropdown set to '09:00 am' with a clock icon, and a day selection dropdown set to 'Monday'.
  - Stop Time:** A time selection dropdown set to '05:00 pm' with a clock icon, and a day selection dropdown set to 'Monday'.



## Create the Application Patrol profile

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





## Set Up the Security Policy

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

←
Object ▾
>
Service ▾

---

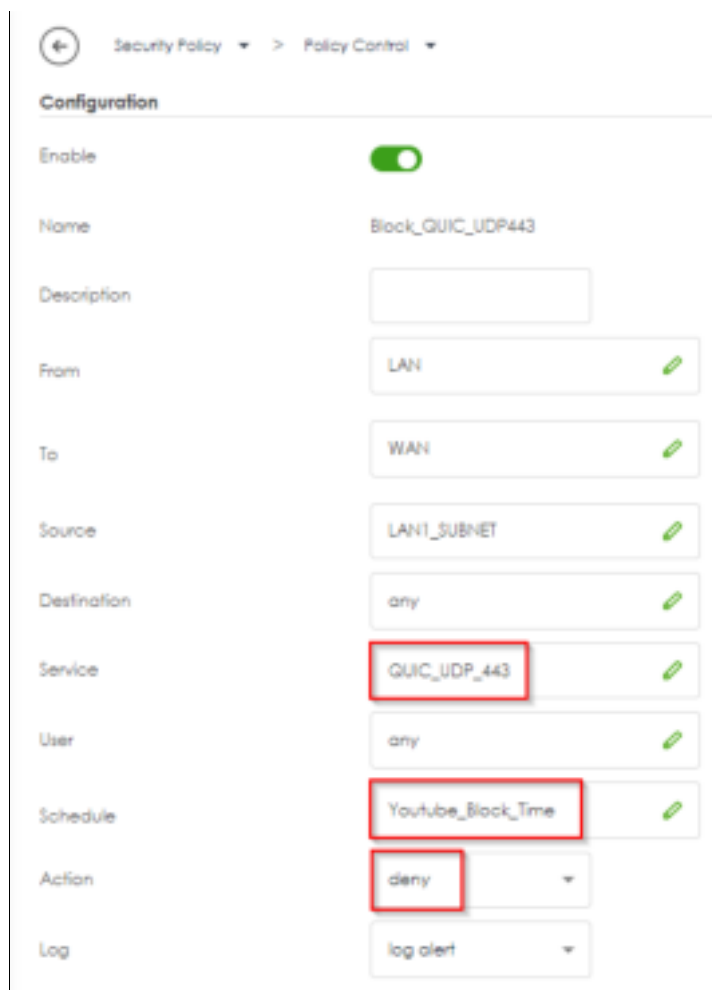
**Configuration**

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












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.

The screenshot displays the ZyXel Security Policy configuration page. The 'Configuration' section includes fields for 'Enable' (checked), 'Name' (Block\_YouTube), 'Description' (empty), 'From' (LAN1), 'To' (WAN), 'Source' (LAN1\_SUBNET), 'Destination' (any), 'Service' (any), 'User' (any), 'Schedule' (Youtube\_Block\_Time), 'Action' (allow), and 'Log' (log alert). The 'Profile' section shows 'Application Patrol' set to 'Youtube', 'Content Filter' set to 'none', and 'SSL Inspection' set to 'none'. The 'Log' column for the profile section is set to 'by profile'.

Configuration			
Enable	<input checked="" type="checkbox"/>		
Name	Block_YouTube		
Description	<input type="text"/>		
From	LAN1		
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



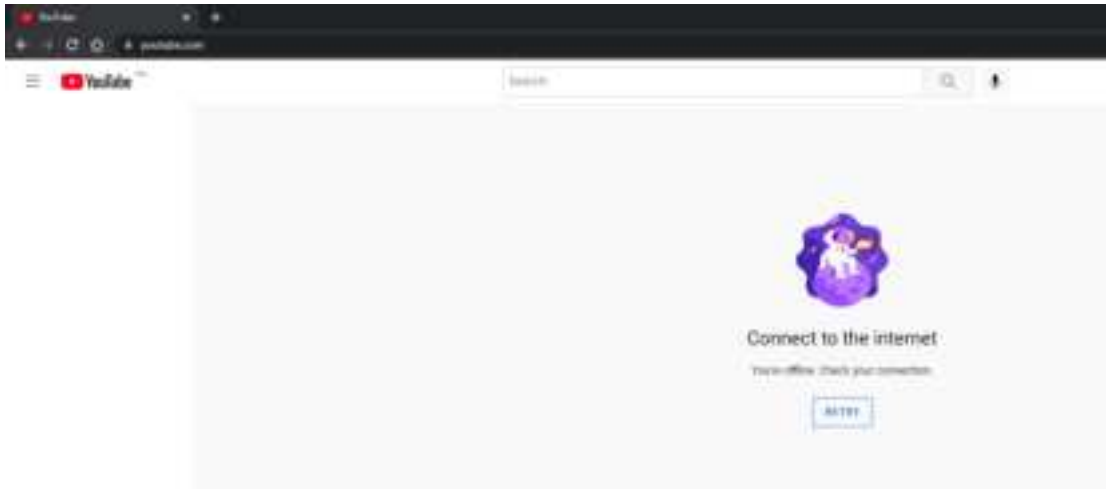
Then go back to the security policy page and move the security priority of block UDP 443 is higher than block YouTube by schedule.

<input type="checkbox"/>	Status	Policy ID	Name	From	To	Source	Destination	Service	User	Schedule	Action	Log	Profile
<input type="checkbox"/>		1	Block_UDP_UDP...	LAN	WAN	LAN1_SUBNET	any	UDP_UDP_443	any	Youtube_Block_T...	deny	log/def	
<input type="checkbox"/>		2	Block_Youtube	LAN	WAN	LAN1_SUBNET	any	any	any	Youtube_Block_T...	allow	log/def	

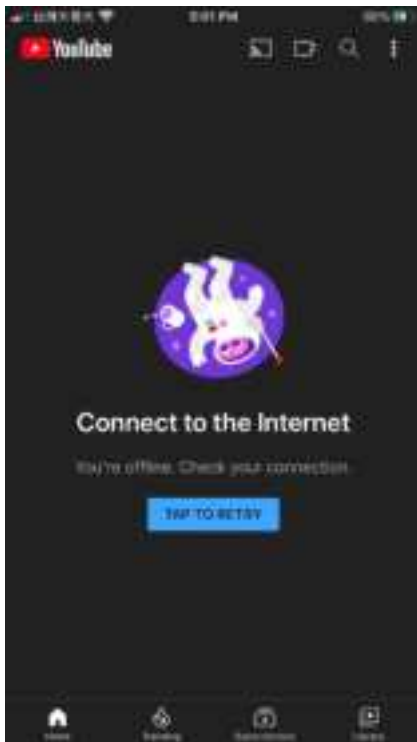


## Test the Result

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	Port
1	2023/01/01 00:00:00	Blocked	Blocked message from 192.168.1.100 to 192.168.1.101	192.168.1.100	192.168.1.101	8080
2	2023/01/01 00:00:00	Blocked	Blocked message from 192.168.1.100 to 192.168.1.101	192.168.1.100	192.168.1.101	8080
3	2023/01/01 00:00:00	Blocked	Blocked message from 192.168.1.100 to 192.168.1.101	192.168.1.100	192.168.1.101	8080
4	2023/01/01 00:00:00	Blocked	Blocked message from 192.168.1.100 to 192.168.1.101	192.168.1.100	192.168.1.101	8080
5	2023/01/01 00:00:00	Blocked	Blocked message from 192.168.1.100 to 192.168.1.101	192.168.1.100	192.168.1.101	8080
6	2023/01/01 00:00:00	Blocked	Blocked message from 192.168.1.100 to 192.168.1.101	192.168.1.100	192.168.1.101	8080
7	2023/01/01 00:00:00	Blocked	Blocked message from 192.168.1.100 to 192.168.1.101	192.168.1.100	192.168.1.101	8080
8	2023/01/01 00:00:00	Blocked	Blocked message from 192.168.1.100 to 192.168.1.101	192.168.1.100	192.168.1.101	8080
9	2023/01/01 00:00:00	Blocked	Blocked message from 192.168.1.100 to 192.168.1.101	192.168.1.100	192.168.1.101	8080
10	2023/01/01 00:00:00	Blocked	Blocked message from 192.168.1.100 to 192.168.1.101	192.168.1.100	192.168.1.101	8080



## 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.



## 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





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)	1st_0	
	Log	no	
Unsupported ssl	Action	pass	
	Log	no	
Unsupported 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**

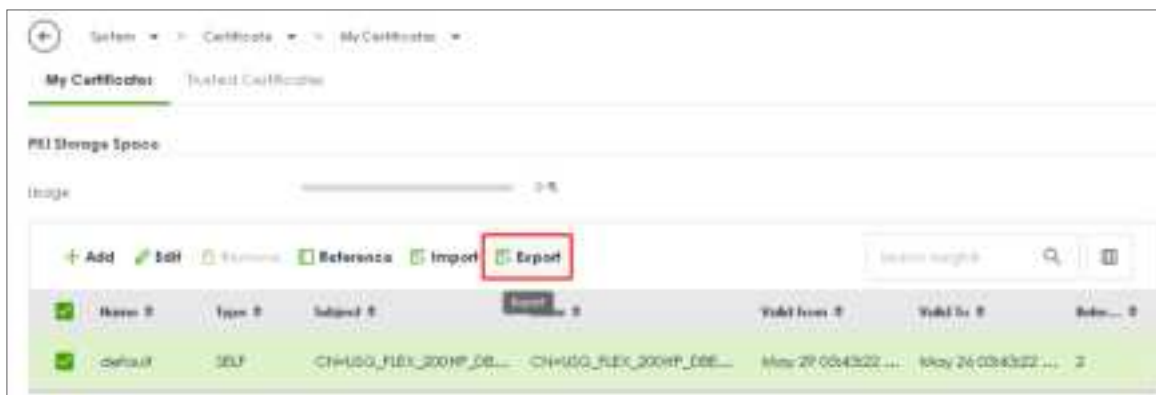
Application Patrol	BlockGoogleDrive	log	bypass
Content Filter	none	log	no profile
SSL inspection	SSL-Inspection	log	bypass



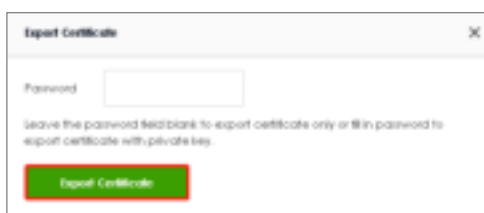
## Export Certificate from FLEX and import to Lan hosts

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.

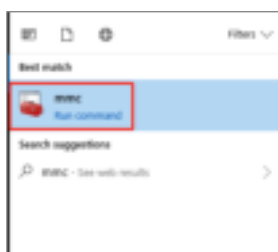
Go to System > Certificate > My Certificates to export default certificate from FLEX.



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.

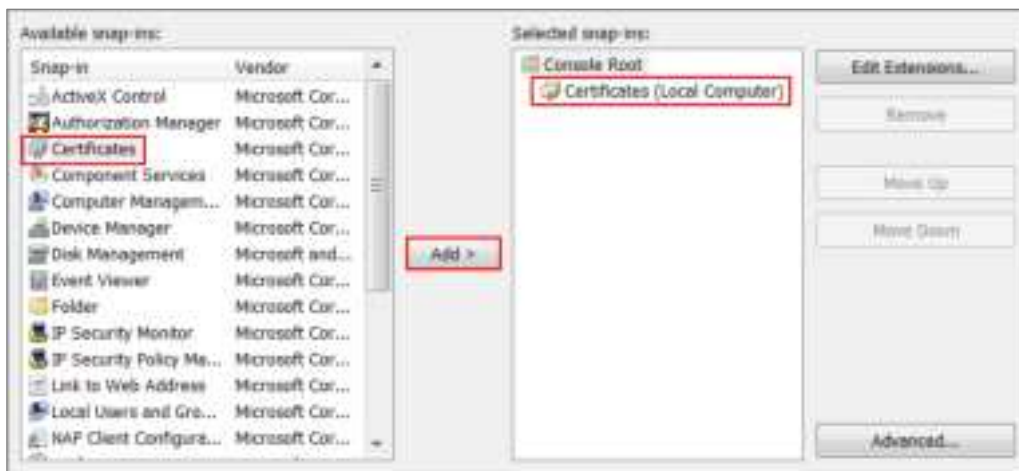




In the mmc console window, click File > Add/Remove Snap-in...

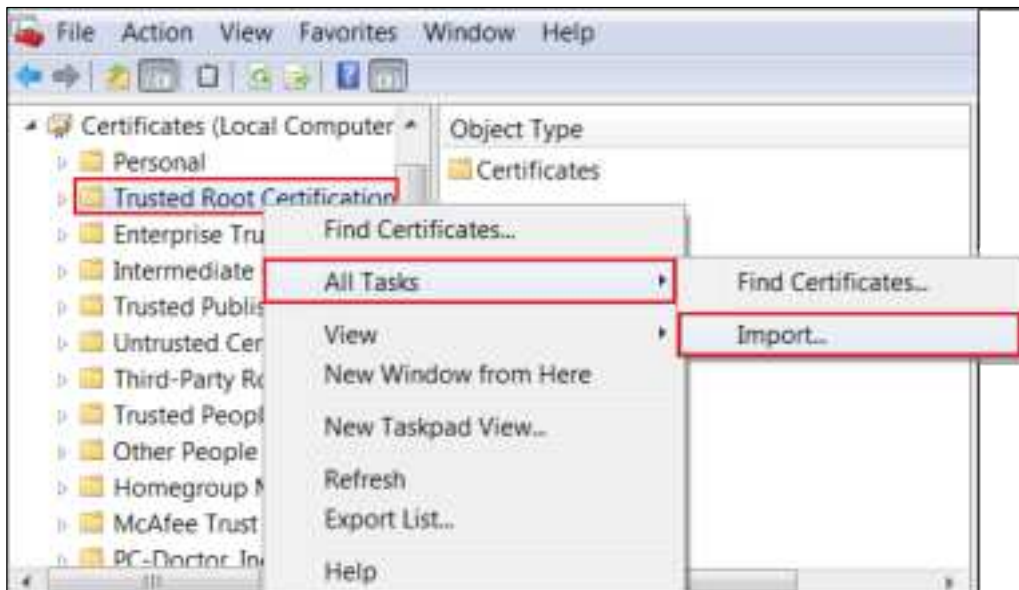


In the Available snap-ins, select the Certificates and click Add button. Select Computer account > Local Computer. Then, click Finished and OK to close the Snap-ins window.





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.

**File to Import**

Specify the file you want to import.

---

File name:

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

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)



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



## Test the Result

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

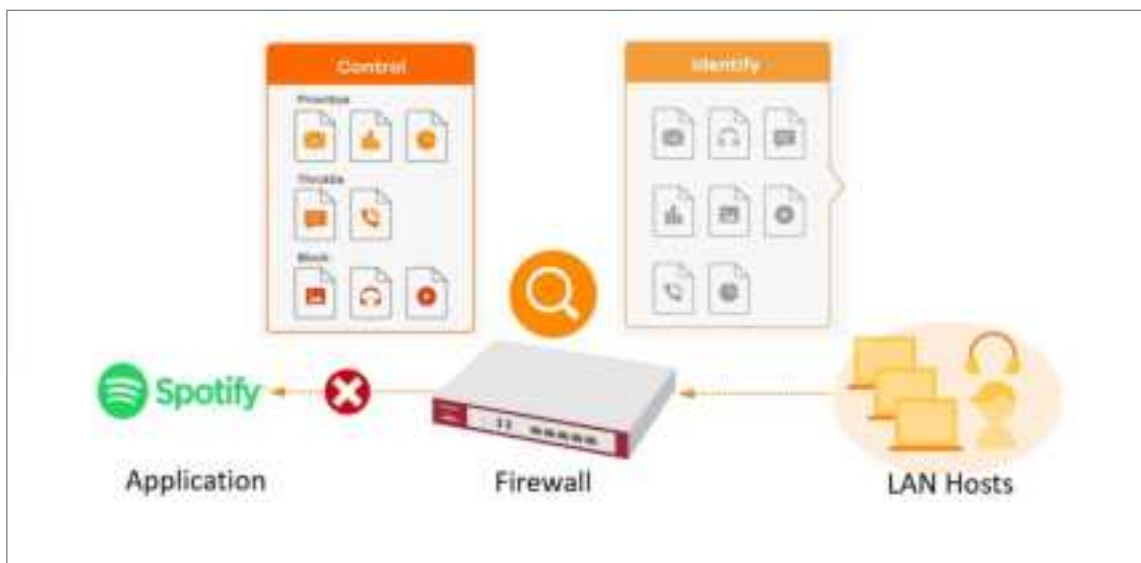
Go to Log & Report > Log/Events and select Application Patrol to check the logs.






## 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.

The screenshot shows the 'Profile' section of the Security Policy configuration. The 'Application Patrol' dropdown menu is highlighted with a red box. Below it, the 'Content Filter' and 'SSL Inspection' sections are visible, each with a 'try profile' button.

## 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.

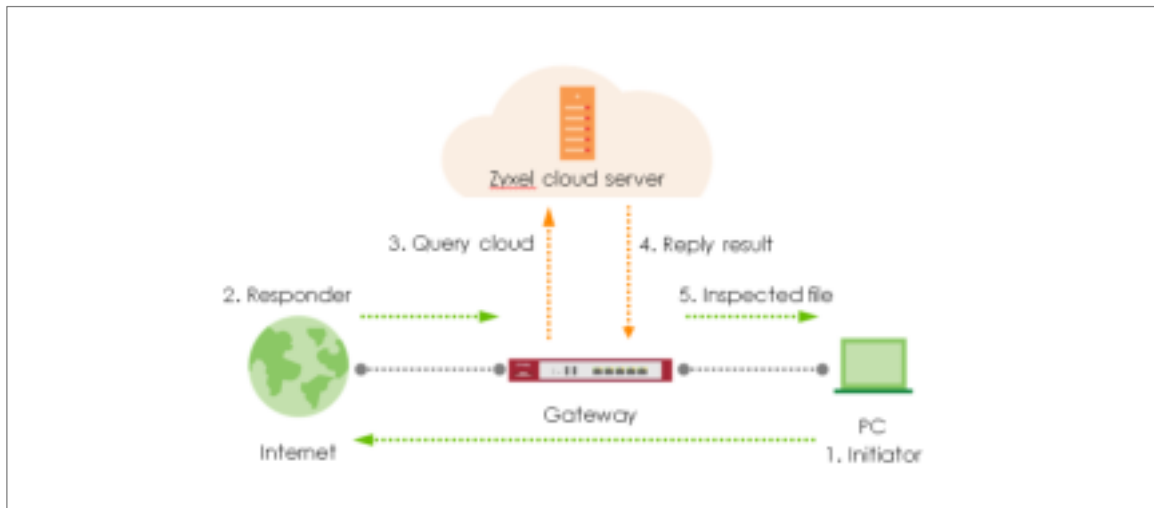
The screenshot shows the 'Log & Report' page with the 'Log/Events' tab selected. The table displays log entries for 'Application Patrol'. The first few entries are highlighted in grey.

ID	Time	Category	Message	Action	Destination	Rule
6	2023-05-24 20:13:31	deny-policy	Rule_name: LAN_Outgoing_Appl (Spotify/Video) (port: 101349) 6204	192.168.1.40:34	30.194.224.25	ACCESS BLOCK
7	2023-05-24 20:13:31	deny-policy	Rule_name: LAN_Outgoing_Appl (Spotify/Video) (port: 101349) 6204	192.168.1.40:34	30.194.224.25	ACCESS BLOCK
8	2023-05-24 20:13:31	deny-policy	Rule_name: LAN_Outgoing_Appl (Spotify/Video) (port: 101349) 6204	192.168.1.40:34	30.194.224.25	ACCESS BLOCK
9	2023-05-24 20:13:31	deny-policy	Rule_name: LAN_Outgoing_Appl (Spotify/Video) (port: 101349) 6204	192.168.1.40:34	30.194.224.25	ACCESS BLOCK
17	2023-05-24 20:13:46	deny-policy	Rule_name: LAN_Outgoing_Appl (Spotify/Video) (port: 101349) 6204	192.168.1.40:34	30.194.224.25	ACCESS BLOCK
18	2023-05-24 20:13:46	deny-policy	Rule_name: LAN_Outgoing_Appl (Spotify/Video) (port: 101349) 6204	192.168.1.40:34	30.194.224.25	ACCESS BLOCK
19	2023-05-24 20:13:46	deny-policy	Rule_name: LAN_Outgoing_Appl (Spotify/Video) (port: 101349) 6204	192.168.1.40:34	30.194.224.25	ACCESS BLOCK



## How does Anti-Malware Work

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





## Enable Anti-Malware function to protecting your traffic

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



Security Service > Anti-Malware > Anti-Malware

### Anti-Malware

#### General Settings

- Enable Anti-Malware ☒
- Collect Statistics ☒
- Scan and detect EICAR test virus ☒
- File size limit: 10 [MB]

Select Destroy infected file and log in Actions When Matched



### Actions When Matched

- Destroy infected file ☒
- Log: log



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

#	Time	Category	Message	Source	Destination	Note
1	2023-03-14 09:31:17	anti-malware	Virus: Infected SSH TypeCloud Query Virus: dlicious.7rjion.44886612fe0b0f36de02e12784cb02f Filescan.com.bt ProtocolH9P m2842c08612fe0b0f36de02e12784cb02f	89.238.73.97	192.168.168.36	FILE DESTROY

Last 24 Hours Summary

Top entry by Virus Name

Virus Name	Hit Count
Malicious.Trojan.c/FaRb/Fa5d735ed7482uE...	1 (71.11%)
Malicious.Trojan.ab04dc13eedf1135d7209b6...	1 (71.11%)
Malicious.Trojan.arf6077a611ab0ac4b0ba0...	1 (71.11%)
Malicious.Trojan.b3cc7921ee2d54f5729902...	1 (71.11%)
Malicious.Trojan.af105dc0a36dc39632a8...	1 (71.11%)
Others	4 (44.44%)

Anti-Malware Statistics Events

Search history

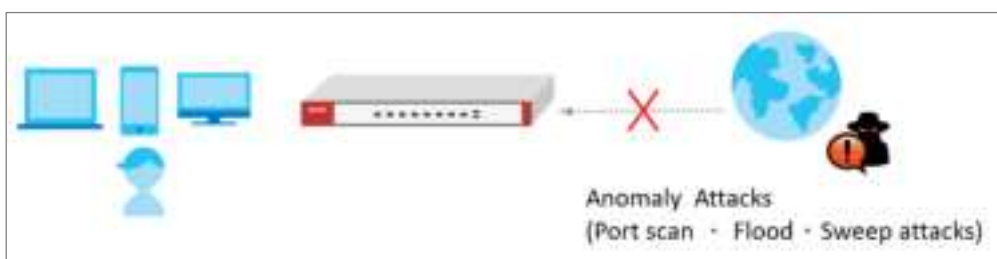
Time	Allow List	Virus Name	Host	Source IP	Destination IP
2023-02-04 08:51:51	<input type="checkbox"/>	Malicious.Trojan.c/FaRb/Fa5d735ed7482uE0F3ade	c/FaRb/Fa5d735ed7482uE0F3ade...	192.168.167.25	192.168.168.34
2023-02-04 08:51:43	<input type="checkbox"/>	Malicious.Trojan.ab04dc13eedf1135d7209b6...	ab04dc13eedf1135d7209b6...	192.168.167.25	192.168.168.34
2023-02-04 08:51:42	<input type="checkbox"/>	Malicious.Trojan.arf6077a611ab0ac4b0ba0...	arf6077a611ab0ac4b0ba0...	192.168.167.25	192.168.168.34
2023-02-04 08:51:40	<input type="checkbox"/>	Malicious.Trojan.b3cc7921ee2d54f5729902...	b3cc7921ee2d54f5729902...	192.168.167.25	192.168.168.34
2023-02-04 08:51:39	<input type="checkbox"/>	Malicious.Trojan.af105dc0a36dc39632a8...	af105dc0a36dc39632a8...	192.168.167.25	192.168.168.34
2023-02-04 08:51:07	<input type="checkbox"/>	Malicious.Trojan.3a6c33ee71c6a8d41c2d3c8b6f95bda0	3a6c33ee71c6a8d41c2d3c8b6f95bda0...	192.168.167.25	192.168.168.34
2023-02-04 08:51:06	<input type="checkbox"/>	Malicious.Virus	F3ee182ee0d64b08e9f11244c...	192.168.167.25	192.168.168.34
2023-02-04 08:51:04	<input type="checkbox"/>	Malicious.Trojan.c/FaRb/Fa5d735ed7482uE0F3ade	c/FaRb/Fa5d735ed7482uE0F3ade...	192.168.167.25	192.168.168.34




## How to Detect and Prevent TCP Port Scanning with DoS

### Prevention

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



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



## Set Up the DoS Prevention

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

**General Settings**

Name: DoS\_Prevention

Description:

**Scan Detection**

Events: Select

Block Policy: [Select] (Under Suspended)

Index #	Name #	Log #	Action #
1	Denial of Service (DoS)	log	block
2	Denial of Service (DoS)	log	block
3	Denial of Service (DoS)	log	block
4	Denial of Service (DoS)	log	block
5	Denial of Service (DoS)	log	block
6	Denial of Service (DoS)	log	block
7	Denial of Service (DoS)	log	block

**Flood Detection**

Block Policy: [Select] (Under Suspended)

Index #	Name #	Log #	Action #	Threshold #
1	Flood (DoS) Flood	log	block	1000
2	Flood (DoS) Flood	log	block	1000
3	Flood (DoS) Flood	log	block	1000
4	Flood (DoS) 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.



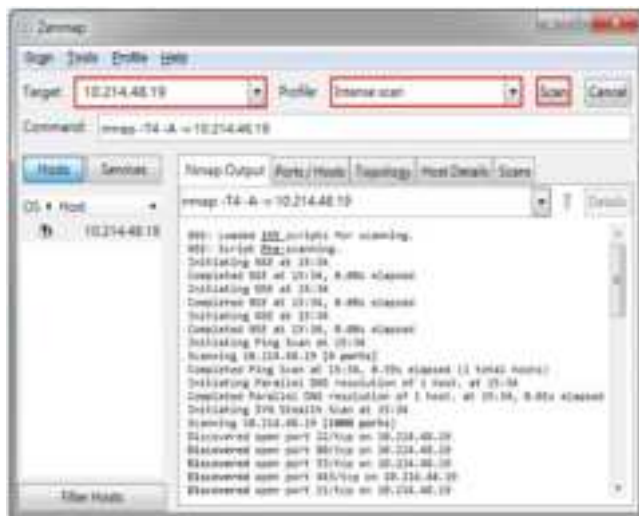


## Test the Result

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

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

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



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

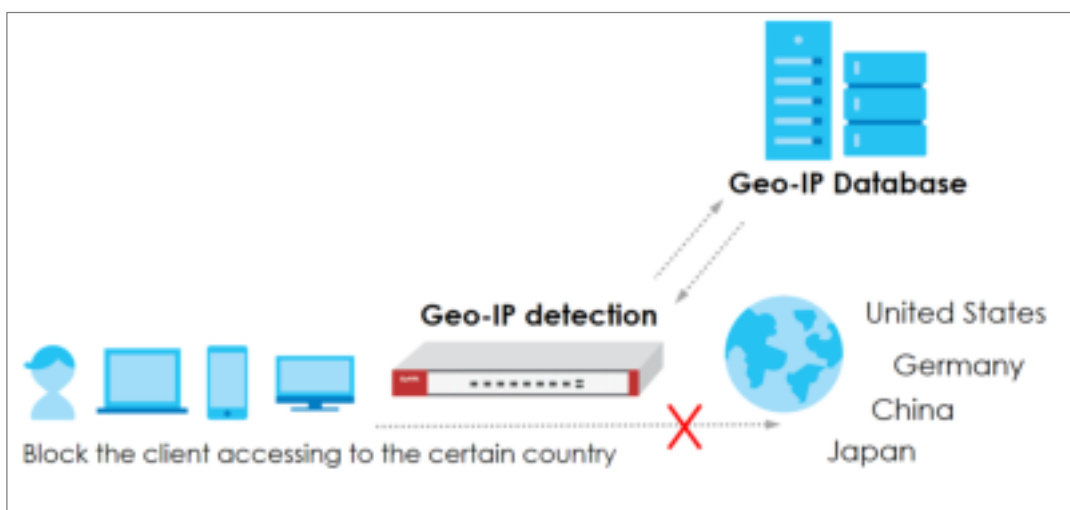
Log & Report > Log / Events						
Category: All Log Filter Refresh Clear Log						
#	Time	Category	Message	Source	Destination	Note
1	2023-08-21 07:06:50	Dos Prevention	Rule_001 from 10.214.48.19 to Any. Type: Scan-Detection(tcp portScan A, 10.214.48.19)	10.214.48.19	10.214.48.19	ACCESS BLOCK
2	2023-08-21 07:06:50	Dos Prevention	Rule_001 from 10.214.48.19 to Any. Type: Scan-Detection(tcp portScan A, 10.214.48.19)	10.214.48.19	10.214.48.19	ACCESS BLOCK
3	2023-08-21 07:06:50	Dos Prevention	Rule_001 from 10.214.48.19 to Any. Type: Scan-Detection(tcp portScan A, 10.214.48.19)	10.214.48.19	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.

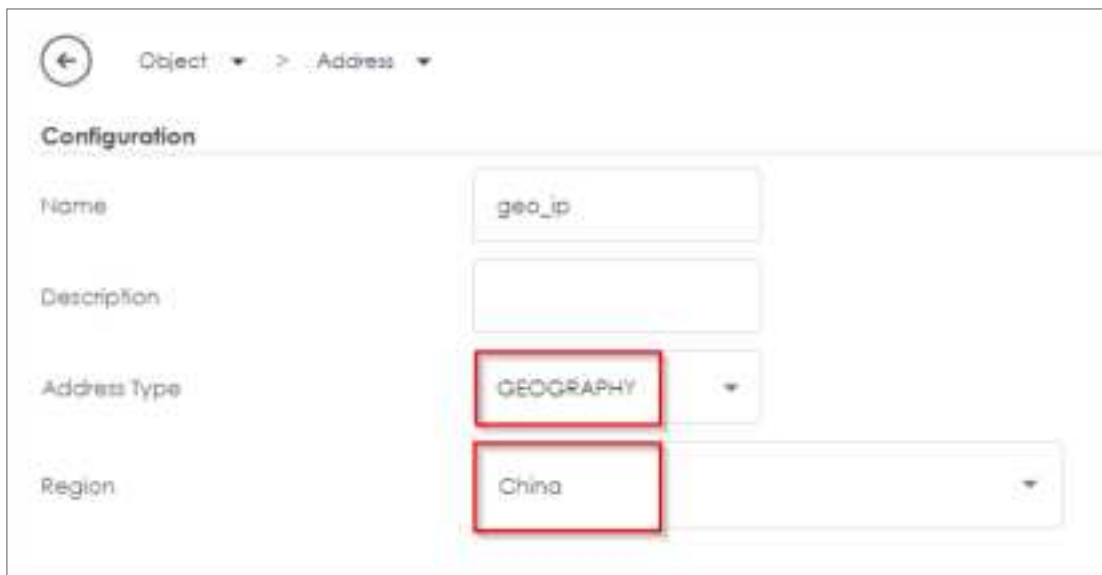


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG Flex 500H (Firmware Version: uOS 1.10)



## 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 address object. The breadcrumb navigation at the top is "Object > Address". The "Configuration" section contains the following fields:

- Name:** geo\_ip
- Description:** (empty text box)
- 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 address object. The breadcrumb navigation at the top is "Object > Address". The "Configuration" section contains the following fields:

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

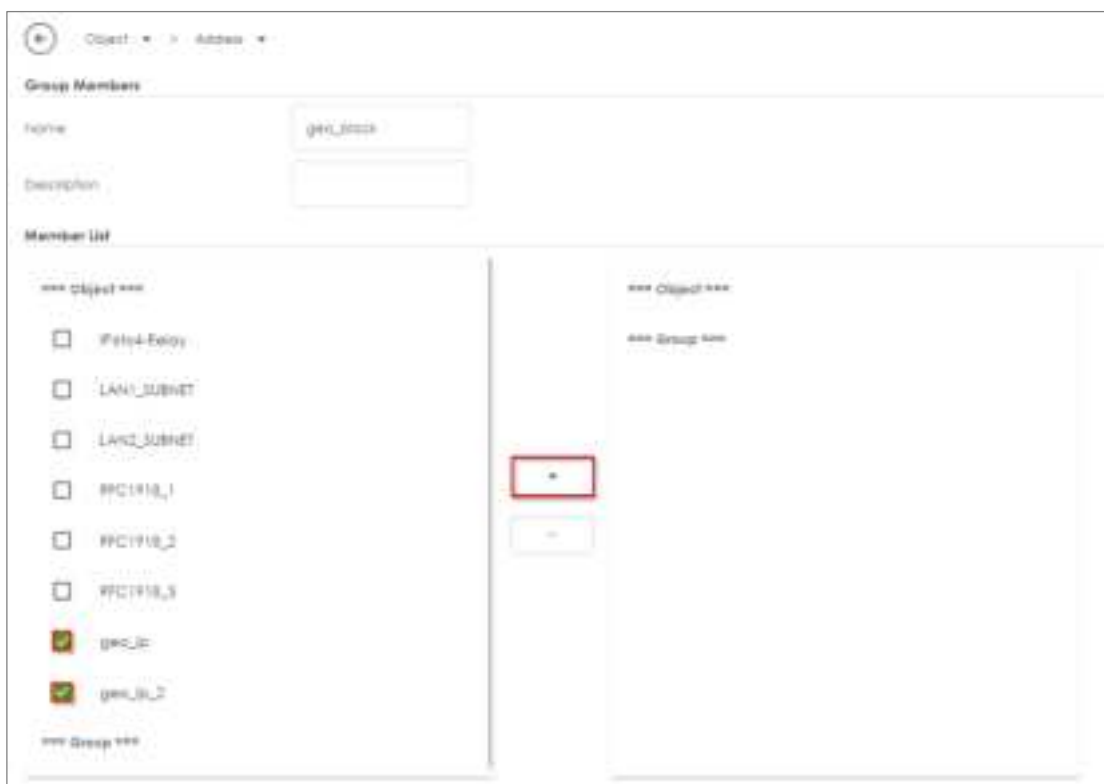


Navigate to **Object > Address > Address**, you can see the customized GEOGRAPHY address object.



Item ID	Type ID	Address ID	Subnet ID
IPAddr-Rule	IPAddr	IPAddr-Rule	1
LAN1_SUBNET	ADDRESS2.SUBNET	ip4	1
LAN2_SUBNET	ADDRESS2.SUBNET	ip4	1
WFC1918_1	COOP	55.55.55.55	1
WFC1918_2	COOP	172.16.0.0/12	1
WFC1918_3	COOP	192.168.0.0/16	1
geo_ip	GEOGRAPHY	China	1
geo_ip_2	GEOGRAPHY	Germany	1

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



Object > Address > Address Group > Add Address Group Rule

Group Members

Name:

Description:

Member List

\*\*\* Object \*\*\*

- ☐ IPAddr-Rule
- ☐ LAN1\_SUBNET
- ☐ LAN2\_SUBNET
- ☐ WFC1918\_1
- ☐ WFC1918\_2
- ☐ WFC1918\_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

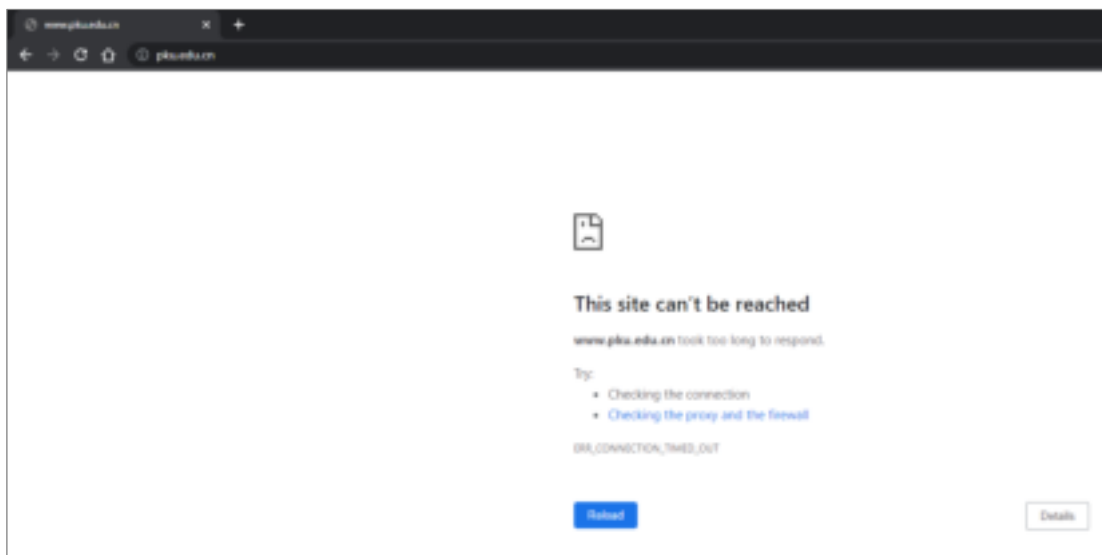
Action: deny

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.



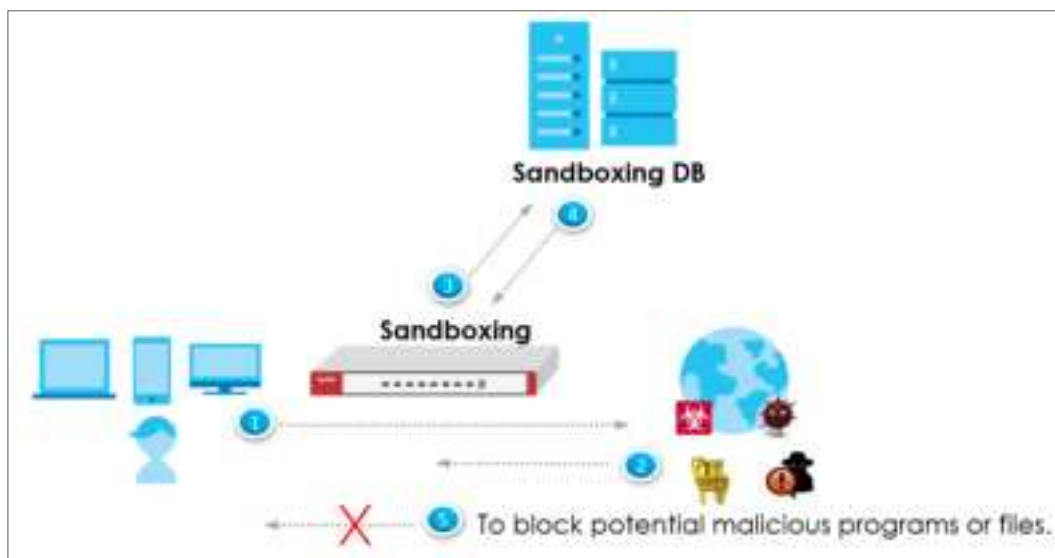
To view the log message, go to USG Flex H **Log & Report > Log / Events**. You will find log messages similar to the following. Any traffic that matches the Geo IP policy will be blocked, and the details will be displayed in the Message field.


#	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	142.103.131.140	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	142.103.131.140	ACCESS BLOCK
9	2023-05-21 18:16:35	secure-policy	priority/1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	142.103.131.140	ACCESS BLOCK
10	2023-05-21 18:16:35	secure-policy	priority/1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	142.103.131.140	ACCESS BLOCK
11	2023-05-21 18:16:38	secure-policy	priority/1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	142.103.131.140	ACCESS BLOCK
12	2023-05-21 18:16:38	secure-policy	priority/1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	142.103.131.140	ACCESS BLOCK
13	2023-05-21 18:16:37	secure-policy	priority/1, from LAN to WAN, TCP, service others, DROP	192.168.168.33	142.103.131.140	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.

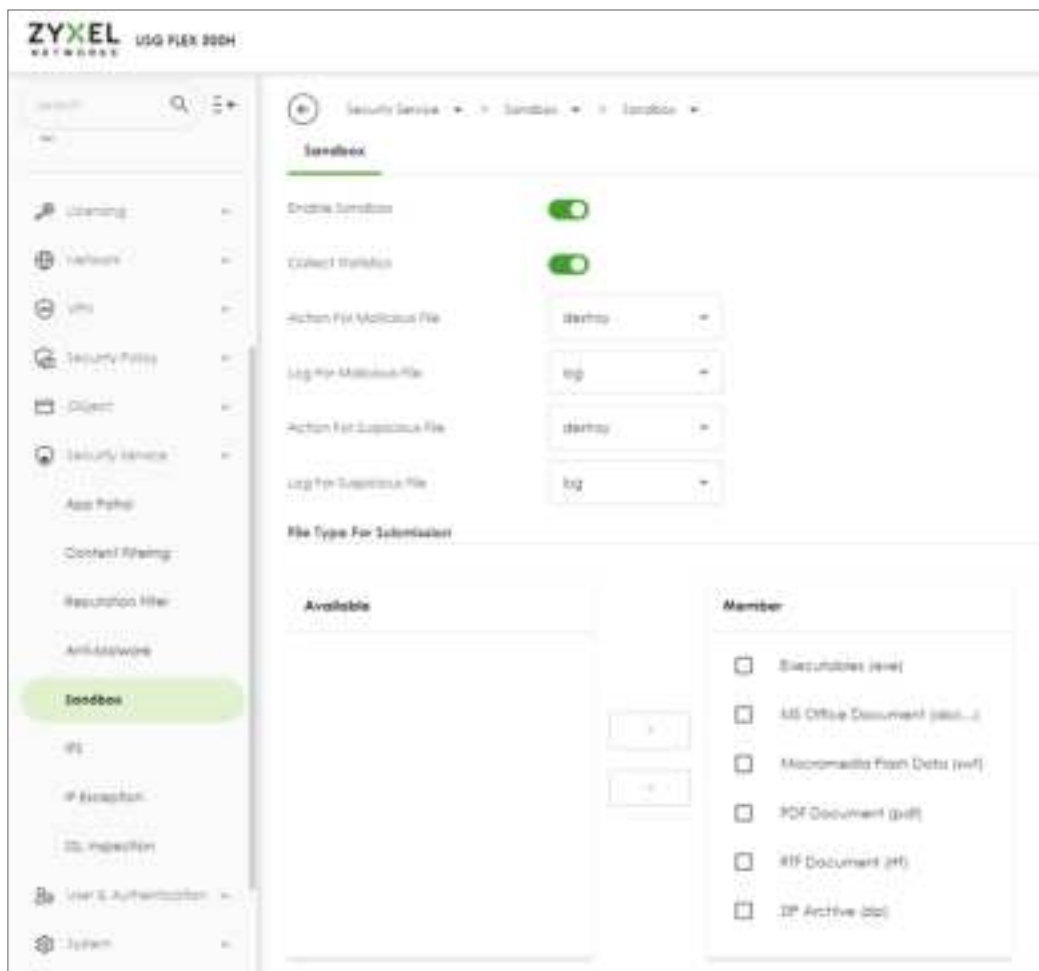


 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.10).



## 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.



Log ID	Time	Source IP	Destination IP	Port	Protocol	Action	Log Type
1	2023/03/15 14:08:14	192.168.1.100	192.168.1.1	80	HTTP	Allow	Sandbox



## 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.



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

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

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



The screenshot shows the 'Types of Cyber Threats' configuration interface. It is divided into two sections:

- Types of Cyber Threats Coming From The Internet:** This section contains nine categories, all of which are checked with green checkmarks:
  - Anonymous Proxies
  - Denial of Service
  - Exploits
  - Negative Reputation
  - Scanners
  - Spam Sources
  - TOR Proxies
  - Web Attacks
  - Phishing
- Types of Cyber Threats Coming From The Internet And Local Networks:** This section contains one category, 'Botnets', which is checked with a green checkmark.



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, specifically the 'Black List' section. The 'Enable' toggle is turned on, and the 'log' dropdown is set to 'log'. Below the configuration options, there is a table with columns 'Status' and 'IP Address'. The table is currently empty, showing 'No data'. The 'Add' button is highlighted in green. The 'IP Address' field in the table header is highlighted in red.

Status	IP Address
No data	



## Test the Result

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

Test IP Threat Category

IP to test

104.244.14.252

Query

Message

threat-level result: High

category result: BotNetsPhishing

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

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

Log & Report > Log/Events

Category IP Reputation

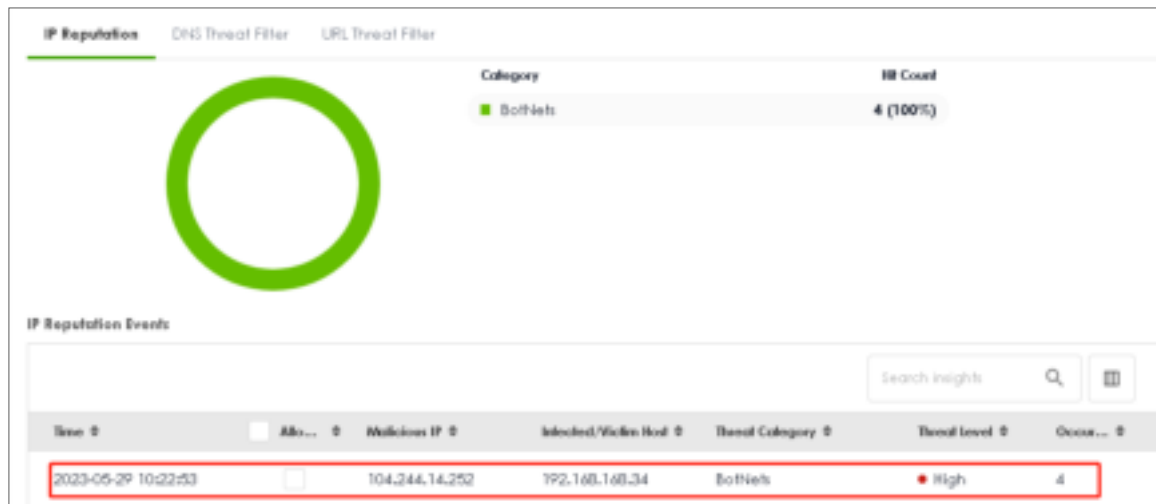
Filter Refresh Clear Log

Search insights

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

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







## How to Configure Reputation Filter- URL Threat Filter

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

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



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



## Set Up the URL Threat Filter

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

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

---

**URL Blocking**

Enable	<input checked="" type="checkbox"/>
Action	block ▼
Log	log alert ▼
Statistics	<input checked="" type="checkbox"/>

**Security Threat Categories**

<input checked="" type="checkbox"/> Anonymizers	<input checked="" type="checkbox"/> Browser Exploits	<input checked="" type="checkbox"/> Malicious Downloads
<input checked="" type="checkbox"/> Malicious Sites	<input checked="" type="checkbox"/> Phishing	<input checked="" type="checkbox"/> Spam URLs
<input checked="" type="checkbox"/> Spyware Adware Keyloggers		



## Test the Result

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

Test URL Threat Category

URL to test

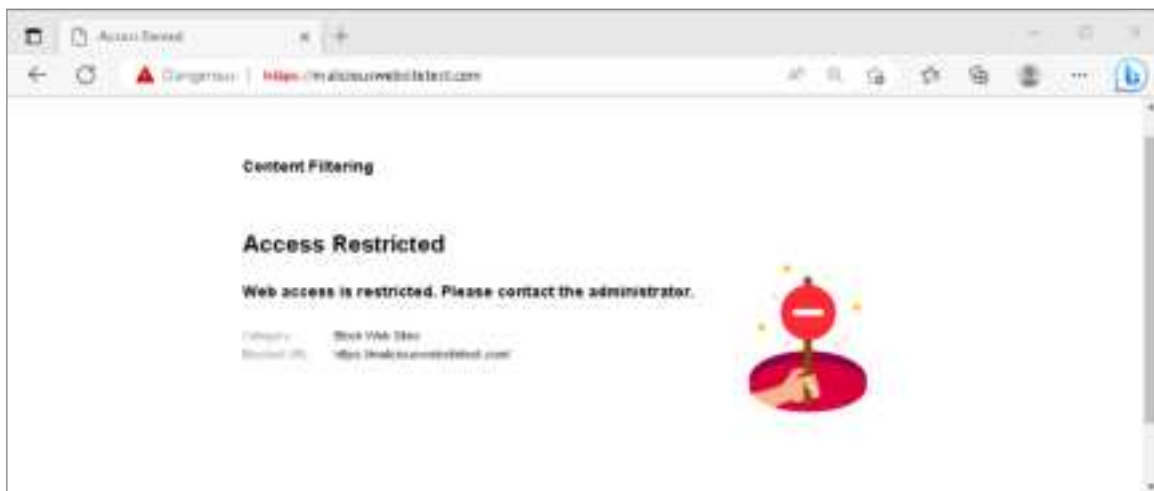
https://maliciouswebs

Query

Message

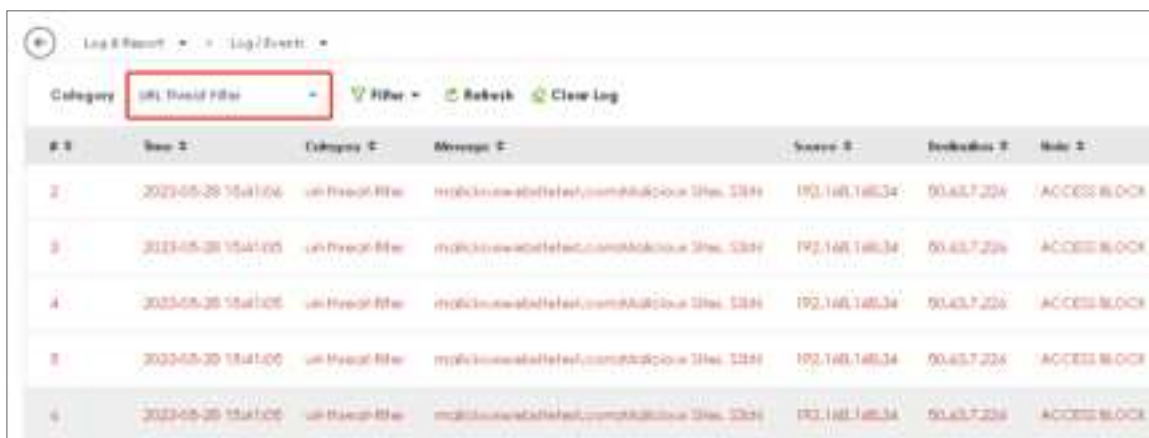
domain category result: information-security,malicious-sites(threat)  
url category result: information-security,malicious-sites(threat)

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





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

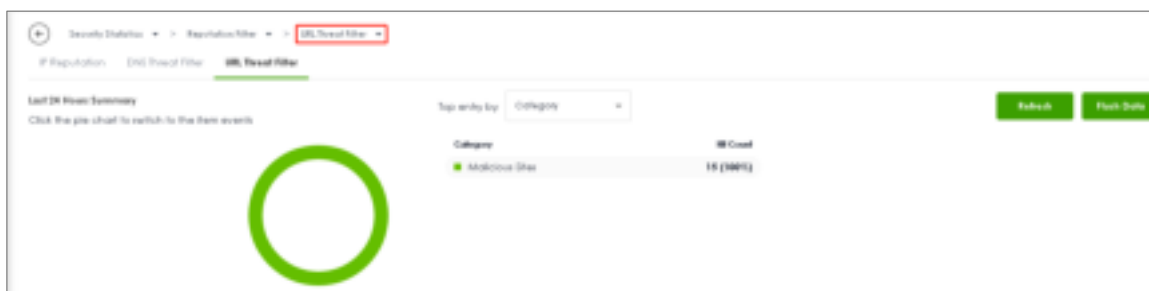
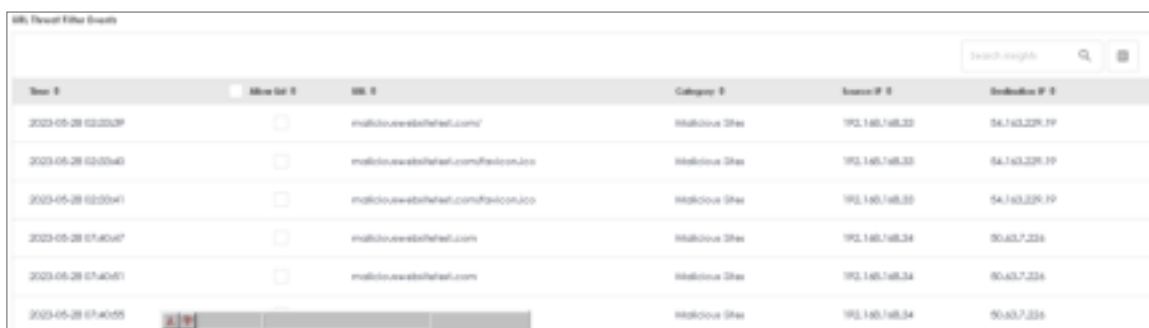


Log & Report > Log/Events

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

#	Time	Category	Message	Source	Destination	Mode
2	2023-05-28 15:41:06	URL Threat Filter	maliciouswebfilter.com/malicious Site: 3344	192.168.1.65:34	50.43.7.234	ACCESS BLOCK
3	2023-05-28 15:41:05	URL Threat Filter	maliciouswebfilter.com/malicious Site: 3344	192.168.1.65:34	50.43.7.234	ACCESS BLOCK
4	2023-05-28 15:41:05	URL Threat Filter	maliciouswebfilter.com/malicious Site: 3344	192.168.1.65:34	50.43.7.234	ACCESS BLOCK
5	2023-05-28 15:41:05	URL Threat Filter	maliciouswebfilter.com/malicious Site: 3344	192.168.1.65:34	50.43.7.234	ACCESS BLOCK
6	2023-05-28 15:41:05	URL Threat Filter	maliciouswebfilter.com/malicious Site: 3344	192.168.1.65:34	50.43.7.234	ACCESS BLOCK

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

URL Threat Filter Events

Time	Show list	URL	Category	Source IP	Destination IP
2023-05-28 02:03:39	<input type="checkbox"/>	maliciouswebfilter.com/	Malicious Site	192.168.1.65:32	54.743.229.19
2023-05-28 02:03:40	<input type="checkbox"/>	maliciouswebfilter.com/favicon.ico	Malicious Site	192.168.1.65:32	54.743.229.19
2023-05-28 02:03:41	<input type="checkbox"/>	maliciouswebfilter.com/favicon.ico	Malicious Site	192.168.1.65:32	54.743.229.19
2023-05-28 07:40:47	<input type="checkbox"/>	maliciouswebfilter.com	Malicious Site	192.168.1.65:34	50.43.7.234
2023-05-28 07:40:51	<input type="checkbox"/>	maliciouswebfilter.com	Malicious Site	192.168.1.65:34	50.43.7.234
2023-05-28 07:40:55	<input type="checkbox"/>	maliciouswebfilter.com	Malicious Site	192.168.1.65:34	50.43.7.234



## 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 displays the configuration page for the DNS Threat Filter. At the top, there are three tabs: 'IP Reputation', 'DNS Threat Filter' (which is selected and highlighted with a green underline), and 'URL Threat Filter'. Below the tabs, the 'DNS Threat Filter' section contains several settings:

- Enable:** A toggle switch that is turned on (green).
- Action:** A dropdown menu set to 'redirect'.
- Log:** A dropdown menu set to 'log alert'.
- Redirect IP:** A dropdown menu set to 'default'.
- Malform DNS packets:** A section with two dropdowns: 'Action' set to 'drop' and 'Log' set to 'log'.
- Statistics:** A toggle switch that is turned on (green).

Below the DNS Threat Filter section is the 'Security Threat Categories' section, which lists seven categories, each with a green checkmark indicating it is 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
maliciouswebsitetest.c
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.

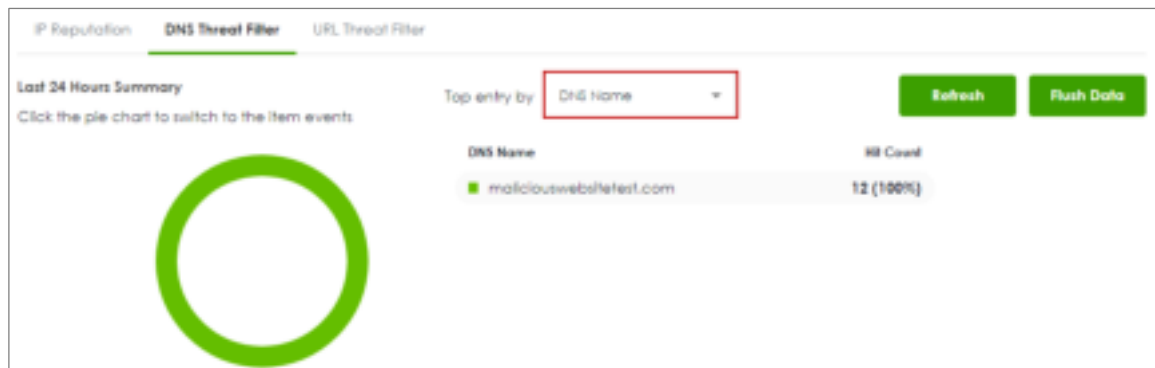


Go to Log & Report > Log/Events and select DNS Threat Filter to check the logs.

Category		Filter		Refresh		Clear Log		Search		Filter		View	
ID	Time	Category	Message	Source	Destination	Rule							
1	2023-05-21 14:47:26	dns-threat-filter	maliciouswebsitetest.com Malicious Site	192.168.1.65.55	192.168.1.65.1	DNS BLOCK							
2	2023-05-21 14:47:26	dns-threat-filter	maliciouswebsitetest.com Malicious Site	192.168.1.65.55	192.168.1.65.1	DNS BLOCK							
3	2023-05-21 14:47:26	dns-threat-filter	maliciouswebsitetest.com Malicious Site	192.168.1.65.55	192.168.1.65.1	DNS REDIRECT							



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



DNS Threat Filter Events

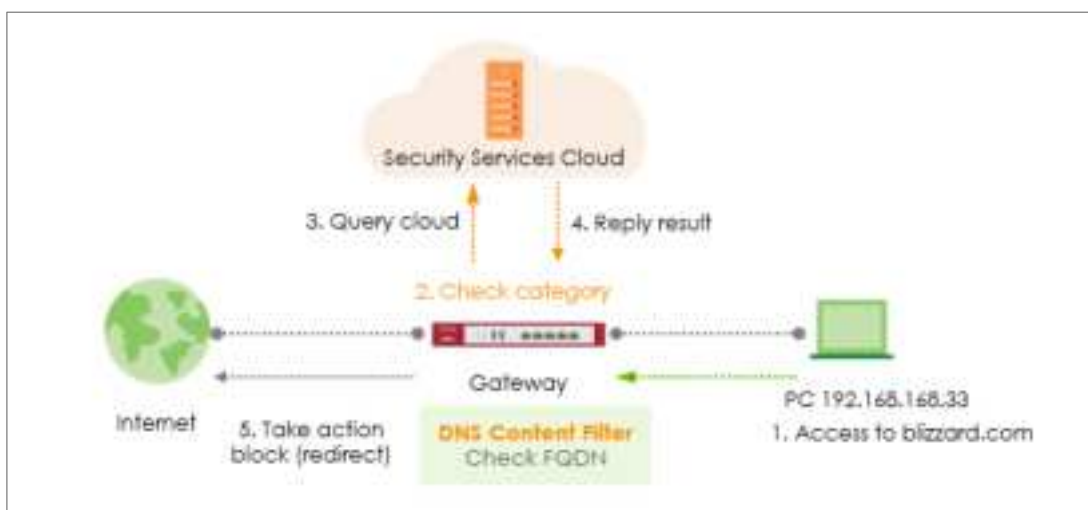
Time	<input type="checkbox"/> Allow ...	DNS Name	Category	Source IP
2023-05-21 16:29:36	<input type="checkbox"/>	maliciouswebsite.com	Malicious Sites	192.168.168.33
2023-05-21 16:44:04	<input type="checkbox"/>	maliciouswebsite.com	Malicious Sites	192.168.168.33
2023-05-21 16:47:02	<input type="checkbox"/>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



The screenshot shows the 'Content Filtering' configuration page. Under the 'For DNS Domain scan:' section, the 'Enable DNS Domain scan' toggle is turned on and highlighted with a red box. Below it, the 'Blocked Domain' is set to 'Redirect IP', and the 'Redirect IP' dropdown menu is set to 'default'. The 'Category Server is unavailable' section has 'Action' set to 'pass' and 'log' set to 'log'. The 'Collect Statistics' toggle is also turned on.

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



The screenshot shows the 'Profile Management' page. At the top, there are buttons for 'Add', 'Edit', and 'Remove'. Below the buttons, there is a table with columns for 'Name', 'Description', and 'Reference'. The table contains three entries: 'SPF', 'CP', and 'block\_gaming'. The 'block\_gaming' entry is highlighted with a green background and a red box around its name.



Log: log or log alert

General Settings

name

board\_games

Description

Action

Drop

Log

log

Log slowed traffic

☐

SSL V2 or previous version Connection

Drop

Drop log

☒

Managed Categories

Select All Categories

Clear All Categories

<input type="checkbox"/> Adult Toons	<input type="checkbox"/> Alcohol	<input type="checkbox"/> Accounting Offices	<input type="checkbox"/> Air Culture Heritage
<input type="checkbox"/> Auxiliary Classics	<input type="checkbox"/> Bicycles	<input type="checkbox"/> Bunkers	<input type="checkbox"/> Choir
<input type="checkbox"/> Consulting Internet	<input type="checkbox"/> Consumer Products	<input type="checkbox"/> Content Server	<input type="checkbox"/> Commercial Districts
<input type="checkbox"/> Craft Dessert	<input type="checkbox"/> Dating Personal	<input type="checkbox"/> Dating Tools Networking	<input type="checkbox"/> Digital Networks
<input type="checkbox"/> Documentation	<input type="checkbox"/> Drugs	<input type="checkbox"/> Education Agencies	<input type="checkbox"/> Entertainment
<input type="checkbox"/> Ebooks	<input type="checkbox"/> Fashion Beauty	<input type="checkbox"/> Financial Banking	<input type="checkbox"/> Film Role
<input type="checkbox"/> Forum Adult Books	<input type="checkbox"/> Gambling	<input type="checkbox"/> Gambling Games	<input type="checkbox"/> Game Culture Alliance
<input checked="" type="checkbox"/> Games	<input type="checkbox"/> Gender News	<input type="checkbox"/> Government Military	<input type="checkbox"/> Graduate Center
<input type="checkbox"/> Health	<input type="checkbox"/> Historical Businesses	<input type="checkbox"/> History	<input type="checkbox"/> Home Cinema



## Test the Result

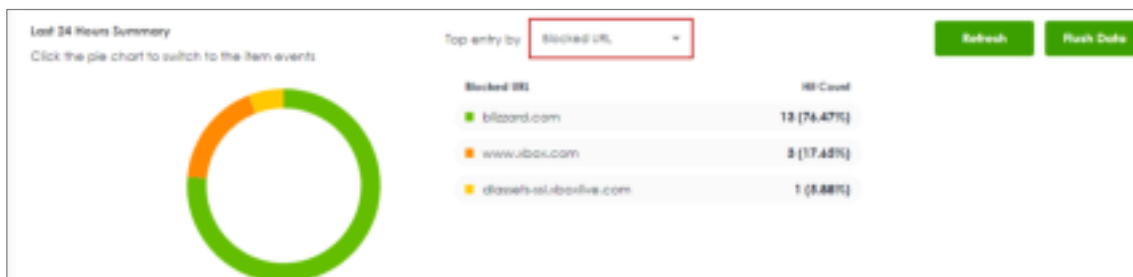
Access a gaming website blizzard.com. The gateway will redirect you to a blocked page.



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

Category: Content Filter						
Filter Refresh Clear Log						
#	Time	Category	Message	Source	Destination	Note
471	2023-05-26 14:36:16	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS BLOCK
472	2023-05-26 14:36:16	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS REDIRECT
506	2023-05-26 14:34:45	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS BLOCK
507	2023-05-26 14:34:45	content-filter	blizzard.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS REDIRECT
508	2023-05-26 14:34:40	content-filter	www.xbox.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS BLOCK
509	2023-05-26 14:34:40	content-filter	www.xbox.com: Games, rule_name: LAN_Outgoing	192.168.168.33	192.168.168.1	DNS REDIRECT
754	2023-05-26 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.



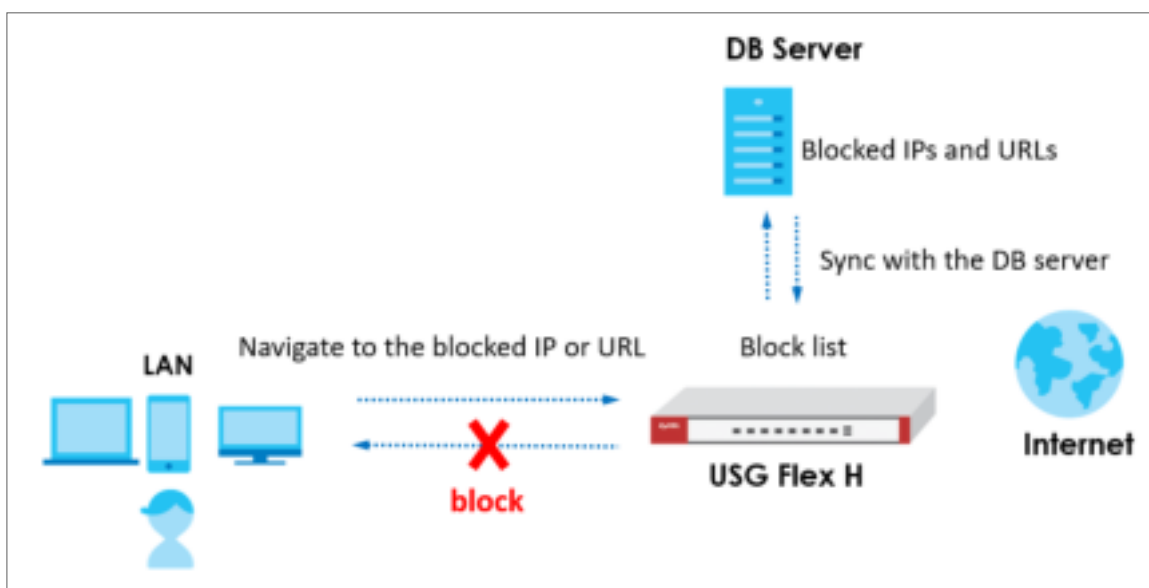



Content Filter Events						
<div> <div>Search Insights</div> <div></div> <div></div> </div>						
Time #	Action #	URL/Domain #	Profile #	Category #	Source IP #	Destination IP #
2023-05-26 14:20:08	BLOCK	www.xbox.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-26 14:19:53	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-26 13:59:19	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-26 13:56:40	BLOCK	blizzard.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-26 13:55:45	BLOCK	diasefi-studiofive.com	block_games	Games	192.168.168.33	192.168.168.1
2023-05-26 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.



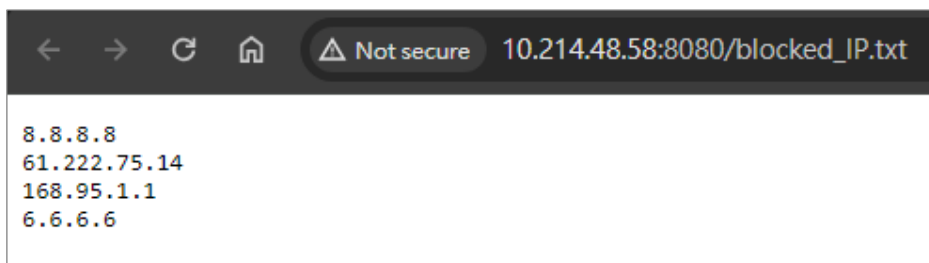
 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.20).



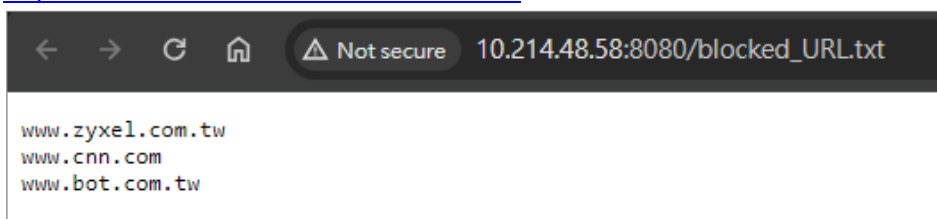
## Set Up the DB server

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

☒ Daily

☐ Weekly

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

Log & Report > Log / Events

Category: All Log Refresh Clear Log Export

#	Time	Category	Message	Srs. IP	Dst. IP	Out. Port
1	2024-05-12 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.

The screenshot shows the 'External Block List' configuration page. At the top, there's a breadcrumb trail: Security Services > External Block List > DNS Threat Filter/URL Threat Filter. Below this, the 'External Block List' section has an 'Enable' toggle switch that is turned on. Under 'Profile Management', there's an '+ Add' button and a table with one entry: 'Block\_URL\_List' with source URL 'http://10.214.48.58:8080/blocked\_URL.txt'. The 'Signature Update' section includes a description, an 'Update Now' button, and an 'Auto Update' section with radio buttons for 'Every 14 Hours', 'Daily' (selected), and 'Weekly'. Each radio button has associated input fields for time, time of day, and day of the week.

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

The screenshot shows the 'Log & Report' section with a table of log entries. The entry shown is for the 'External Block List' category, with the message 'Update DNS/URL threat filter external block list completed@Block\_URL\_List'. The status is 'Success'.

#	Time	Category	Message	Src IP	Dst IP	Dst Port
1	2024-08-12 19:07:36	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\user>ping 8.8.8.8

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

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

C:\Users\user>ping 168.95.1.1

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

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

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

#	Time	Category	Message	Src IP	Dest IP	Out. Port	Note
1	2024-08-18 11:22:00	IP Reputation	Destination unreachable to denied block (192.168.168.1)_P_200	192.168.168.20	168.95.1.1	0	401222 8.0732
2	2024-08-18 11:22:00	IP Reputation	Destination unreachable to denied block (192.168.168.1)_P_200	192.168.168.20	168.95.1.1	0	401222 8.0732
3	2024-08-18 11:22:00	IP Reputation	Destination unreachable to denied block (192.168.168.1)_P_200	192.168.168.20	168.95.1.1	0	401222 8.0732
4	2024-08-18 11:22:00	IP Reputation	Destination unreachable to denied block (192.168.168.1)_P_200	192.168.168.20	168.95.1.1	0	401222 8.0732
5	2024-08-18 11:22:00	IP Reputation	Destination unreachable to denied block (192.168.168.1)_P_200	192.168.168.20	168.95.1.1	0	401222 8.0732
6	2024-08-18 11:22:00	IP Reputation	Destination unreachable to denied block (192.168.168.1)_P_200	192.168.168.20	168.95.1.1	0	401222 8.0732
7	2024-08-18 11:22:00	IP Reputation	Destination unreachable to denied block (192.168.168.1)_P_200	192.168.168.20	168.95.1.1	0	401222 8.0732
8	2024-08-18 11:22:00	IP Reputation	Destination unreachable to denied block (192.168.168.1)_P_200	192.168.168.20	168.95.1.1	0	401222 8.0732

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.

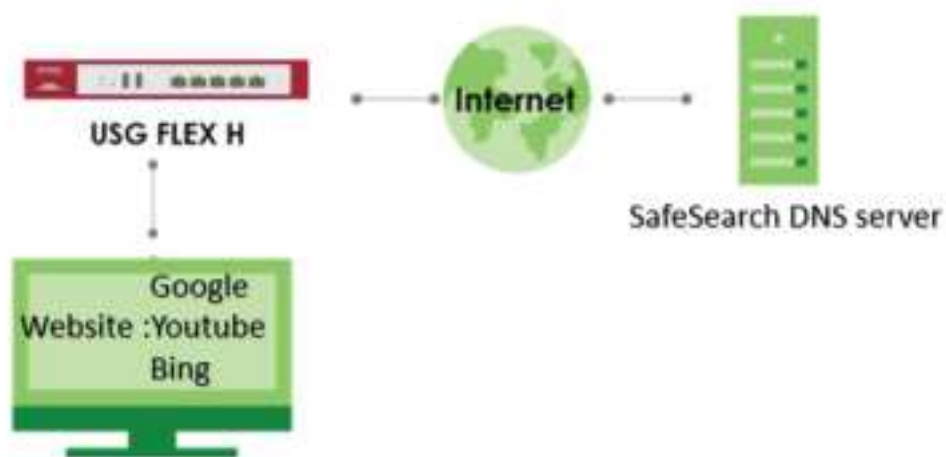
#	Time	Category	Message	Src IP	Dest IP	Out. Port	Note
1	2024-08-18 11:22:00	URL Reputation	www.bot.com.tw is denied block (192.168.168.1)_P_200	192.168.168.20	168.95.1.1	80	401222 8.0732
2	2024-08-18 11:22:00	URL Reputation	www.bot.com.tw is denied block (192.168.168.1)_P_200	192.168.168.20	168.95.1.1	80	401222 8.0732
3	2024-08-18 11:22:00	URL Reputation	www.bot.com.tw is denied block (192.168.168.1)_P_200	192.168.168.20	168.95.1.1	80	401222 8.0732




## How to set up DNS SafeSearch?

SafeSearch is a feature that acts as an automated filter of pornography and potentially offensive and inappropriate content.

This guide explains how to configure your gateway to set up DNS Safe Search.

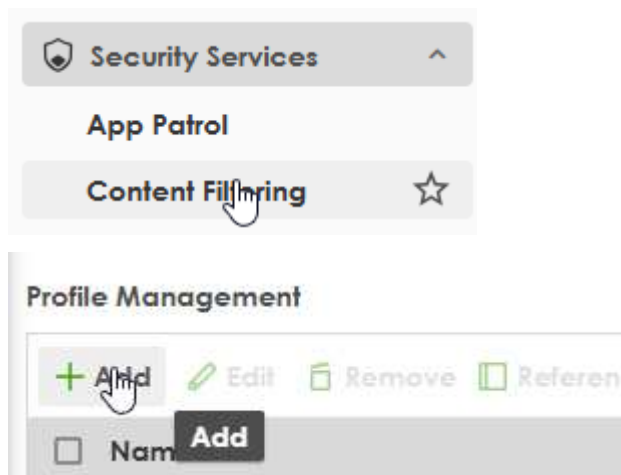


 Note: DNS SafeSearch is supported on USG Flex H series. This example was tested using USG FLEX 200HP (Firmware Version: uOS 1.35).



## Step 1: Set up a SafeSearch Profile

Log in to Local Web GUI - Navigate to Security Services > Content Filtering.



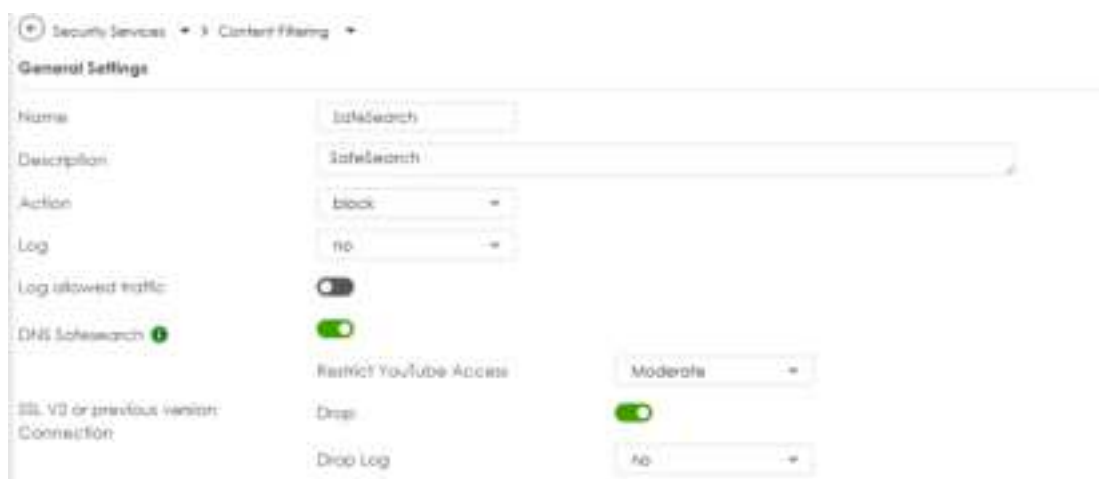
Configure the Profile

**DNS Safesearch:** Click the button to enable the function.

Enforce safe search on Google, Youtube, Bing.

To enable DNS Safe Search, please make sure DNS Domain Scan is turned on.

**Restrict Youtube Access:** The Restrict YouTube Access setting allows you to choose between Strict and Moderate modes.





DNS SafeSearch ⓘ

SSL V3 or previous version  
Connection

- Enforce safe search on Google, YouTube and Bing.
- To enable DNS Safe Search, please make sure DNS Domain Scan is turned on.

Restrict YouTube Access

Drop

Drop Log

## Step 2: Apply the safe search profile to Security Policy Rule

After completing the profile, a message will pop up to guide you in applying the profile to the Security Policy Rule

**Info**

Profile SafeSearch has been saved. A profile takes effect only when it is applied to a security policy. Apply this profile to a security policy now?

[hs1]

Click OK and apply the profile to the desired rule

Apply SafeSearch to a security policy

Rule ID	Rule Name	Rule Type	Rule Status	Rule Action	Rule Priority	Rule Description	Rule Category	Rule Sub-category	Rule Policy	Rule Log
1	1. All Outgoing	OUT	any (Outgoing Traffic)	any	any	any	any	any	any	any
2	2. All Incoming	IN	any (Incoming Traffic)	any	any	any	any	any	any	any
3	3. All Outgoing	OUT	any (Outgoing Traffic)	any	any	any	any	any	any	any
4	4. All Incoming	IN	any (Incoming Traffic)	any	any	any	any	any	any	any
5	5. All Outgoing	OUT	any (Outgoing Traffic)	any	any	any	any	any	any	any
6	6. All Incoming	IN	any (Incoming Traffic)	any	any	any	any	any	any	any
7	7. All Outgoing	OUT	any (Outgoing Traffic)	any	any	any	any	any	any	any
8	8. All Incoming	IN	any (Incoming Traffic)	any	any	any	any	any	any	any
9	9. All Outgoing	OUT	any (Outgoing Traffic)	any	any	any	any	any	any	any
10	10. All Incoming	IN	any (Incoming Traffic)	any	any	any	any	any	any	any
11	11. All Outgoing	OUT	any (Outgoing Traffic)	any	any	any	any	any	any	any
12	12. All Incoming	IN	any (Incoming Traffic)	any	any	any	any	any	any	any



After implementation, please navigate to Security Policy > Policy Control to check if the rule has been correctly set up.



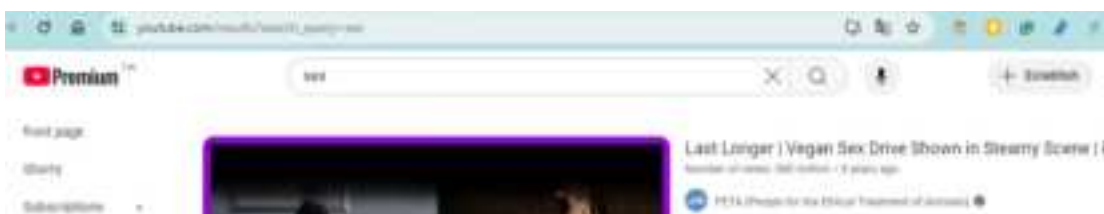
### Step 3: Verified SafeSearch Function

Before verified the SafeSearch, if there is no other setting on DNS, normally the query result will display as below.

www.youtube.com

```
C:\Users\kukum>nslookup www.youtube.com
Server: UnKnown
Address: 192.168.168.1

Non-authoritative answer:
Name: youtube-ui.l.google.com
Addresses: 2404:6800:4012:9::200e
           2404:6800:4012:6::200e
           2404:6800:4012:5::200e
           2404:6800:4012:8::200e
           142.250.66.78
           142.250.204.46
           142.250.196.206
           142.250.198.78
Aliases: www.youtube.com
```

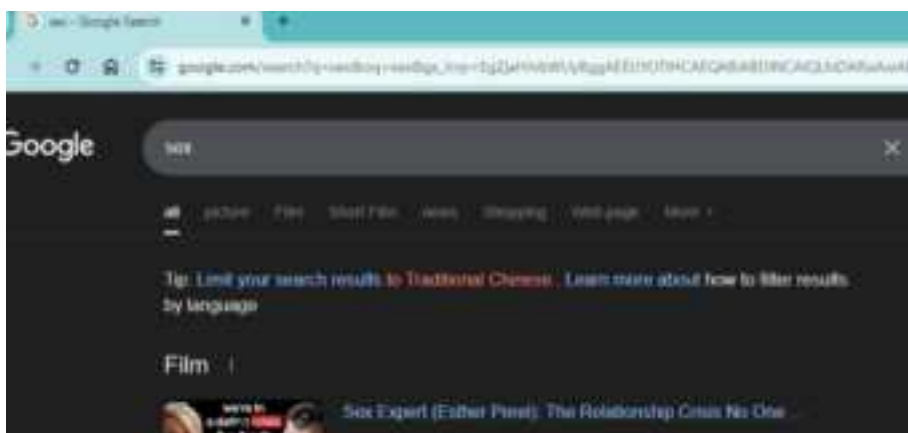




[www.google.com](http://www.google.com)

```
C:\Users\kukun>nslookup www.google.com
Server: UnKnown
Address: 192.168.168.1

Non-authoritative answer:
Name: www.google.com
Addresses: 2404:6800:4012:9::2004
          142.250.196.196
```



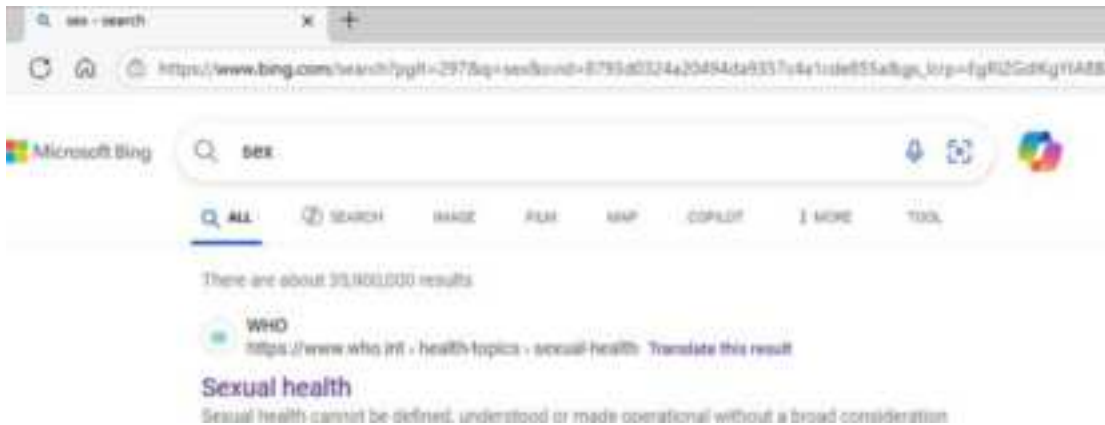
[www.bing.com](http://www.bing.com)

```
C:\Users\kukun>nslookup www.bing.com
Server: UnKnown
Address: 192.168.168.1

Non-authoritative answer:
Name: e86303.docx.akamaiedge.net
Addresses: 2001:b034:1c:200::d247:e3d1
          2001:b034:1c:200::d247:e3d8
          2001:b034:1c:200::d247:e3d0
          2001:b034:1c:200::d247:e3d2
          2001:b034:1c:200::d247:e3d3
          210.71.227.211
          210.71.227.208
          210.71.227.210
          210.71.227.209
          210.71.227.216
          210.71.227.202
          210.71.227.218

Aliases: www.bing.com
          www-www.bing.com,trafficmanager.net
          www.bing.com.edgekey.net
```





Ensure that the DNS server assignment is automatic get from the firewall.

IP assignment:	Automatic (DHCP)
DNS server assignment:	Automatic (DHCP)

www.youtube.com

```
C:\Users\kukum>nslookup www.youtube.com
Server: UnKnown
Address: 192.168.168.1

Name: www.youtube.com
Address: 216.239.38.120
Aliases: www.youtube.com
```





[www.google.com](http://www.google.com)

```
C:\Users\kukum>nslookup www.google.com
Server: UnKnown
Address: 192.168.168.1

Name:    www.google.com
Address: 216.239.38.120
Aliases: www.google.com
```



[www.bing.com](http://www.bing.com)

```
C:\Users\kukum>nslookup www.bing.com
Server: UnKnown
Address: 192.168.168.1

Name:    a-0017.a-msedge.net
Address: 150.171.27.16
Aliases: www.bing.com
          strict.bing.com
          strict-bing-com.a-0017.a-msedge.net
```





## Troubleshooting

DNS Safe Search is not working

- Double-check the Ethernet or Wi-Fi adapter: Ensure that the DNS IP address is set as automatic get DHCP assignment.
- Devices are using alternative DNS servers (e.g., hardcoded DNS like 8.8.8.8).
- DNS over HTTPS (DoH) or DNS over TLS (DoT) may be enabled and bypassing your filtering.
- Cached DNS or browser settings are showing previous search results without SafeSearch applied.




## 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.

Serial 1:

Serial 2:

Model Number:

Authentication Timeout Settings: ☒ Use Default Settings ☐ Use Manual Settings

Login 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

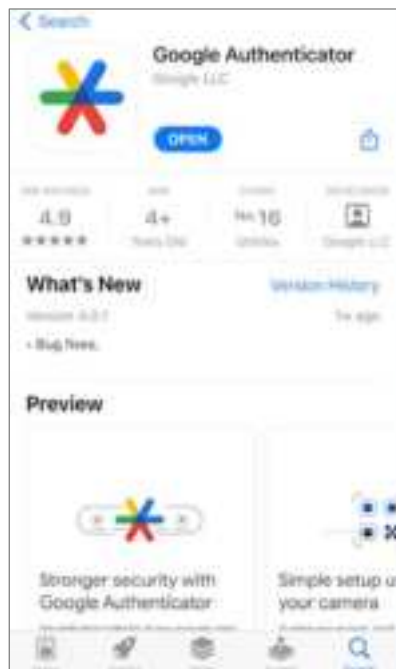


## Set up Google Authenticator

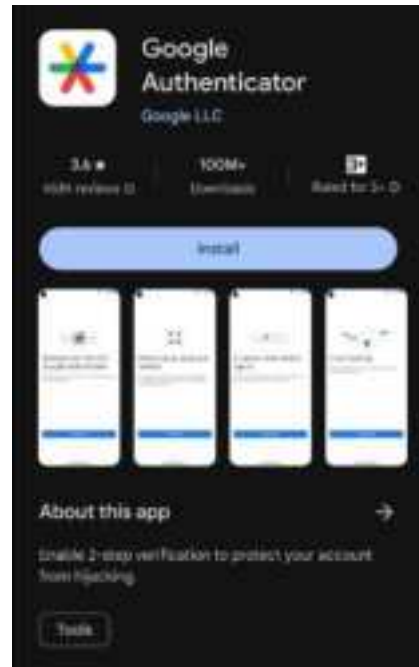


1. Download and install Google Authenticator on your mobile device.

### Apple Store

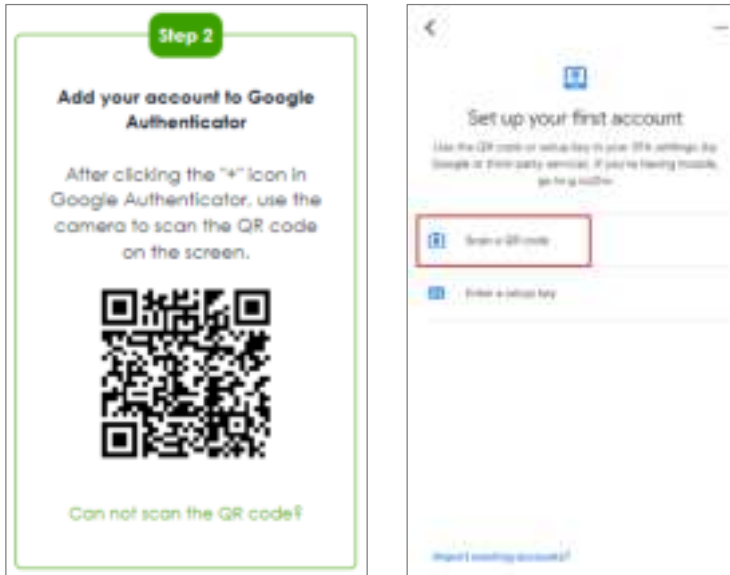


### Google Play

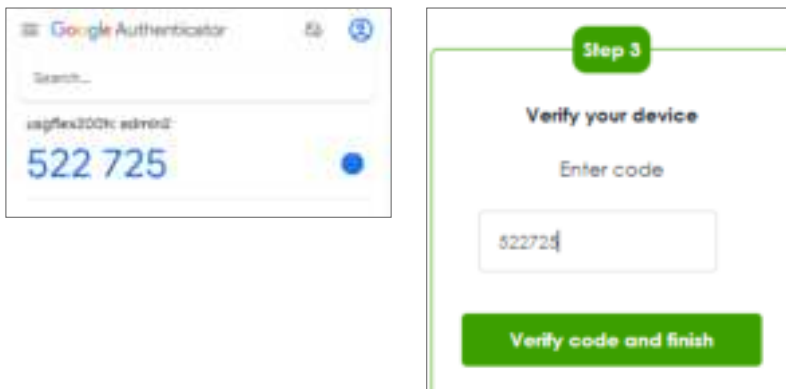




2. Register the admin account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.



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.



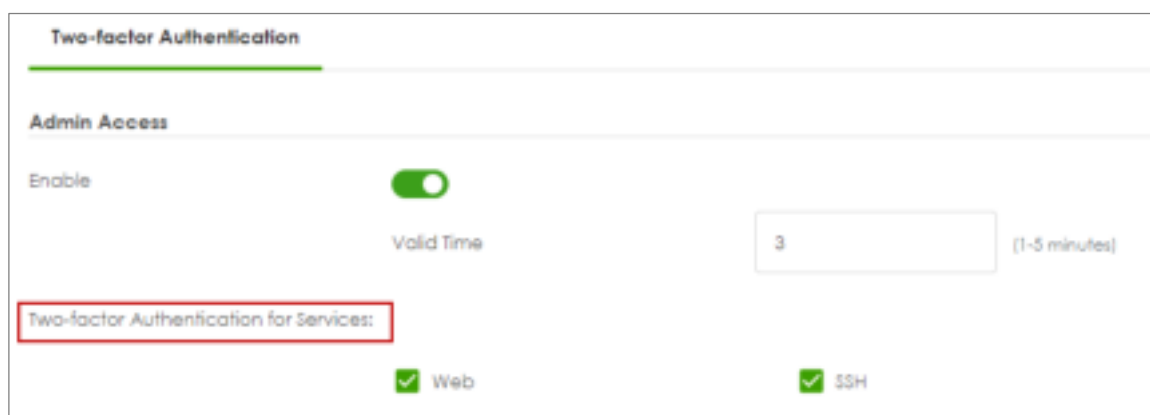


4. After 2FA registration is set up successfully, there are backup codes on web GUI. The backup codes are for device login in the case you don't have access to the application on your mobile device. Download the backup codes and record them in a safe place.



## Configure valid time and login service types

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.





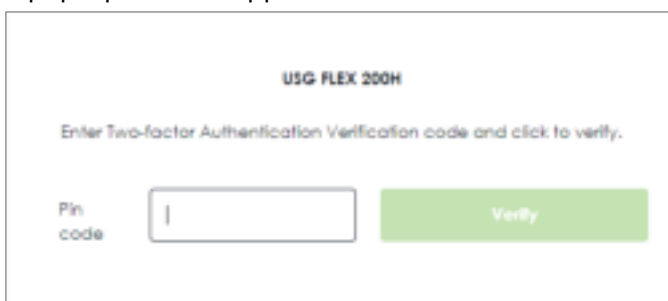
## Test the Result

1. Login with the admin account "admin2".



The image shows the login page for the USG FLEX 200H. At the top, it says "USG FLEX 200H". Below that, it says "Enter User Name/Password and click to login." There are two input fields: "Username" 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 two-factor authentication page for the USG FLEX 200H. It says "USG FLEX 200H" and "Enter Two-factor Authentication Verification code and click to verify." There is a "Pin code" label next to an input field containing a single character "1". A green "Verify" button is to the right.

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 two-factor authentication page for the USG FLEX 200H, similar to the previous one. It says "USG FLEX 200H" and "Enter Two-factor Authentication Verification code and click to verify." The "Pin code" input field now contains the full code "752897". The green "Verify" button remains.



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


Category: user						
Filter: Refresh Clear Log						
#	Time	Category	Message	Status	Duration	Note
2	2023-08-27 14:28:29	user	user:admin@ is authorized	0000	0000	No-Factor-auth.
3	2023-08-27 14:28:29	user	user:admin@ is authorized	0000	0000	No-Factor-auth.
4	2023-08-27 14:28:30	user	user:admin@ (10.214.36.18) is waiting to authorize.	0000	0000	No-Factor-auth.
5	2023-08-27 14:29:04	user	Administrative user:admin@ (AAAOn) from 10.214.36.18 has logged in Device	10.214.36.18	0000	Account auth...



## 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

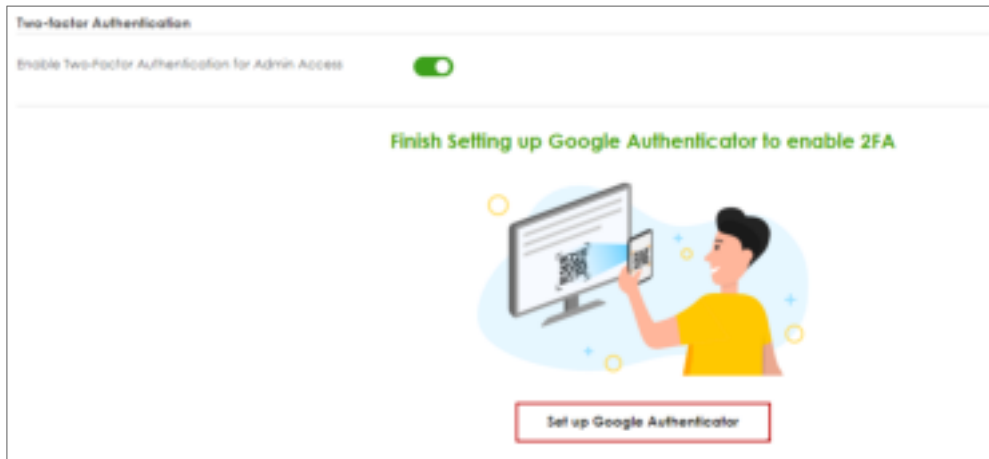
Go to User & Authentication > User/Group. Select a local user and enable Two-factor authentication.

The screenshot shows the 'User & Authentication' configuration page for a user named 'vpntestuser'. The page is titled 'Profile Management' and contains the following fields and settings:

- User Name:** vpntestuser
- User Type:** user
- Password:** [Redacted]
- Re-type:** [Redacted]
- Description:** [Empty field]
- Email 1:** [Empty field]
- Email 2:** [Empty field]
- Mobile Number:** [Empty field]
- Authentication Timeout Settings:**
  - ☒ Use Default Settings
  - ☐ Use Manual Settings
- Lease Time:** 1440 minutes
- Reauthentication Time:** 1440 minutes
- Two-factor Authentication:**
  - Enable Two-Factor Authentication for VPN Access:** ☒



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



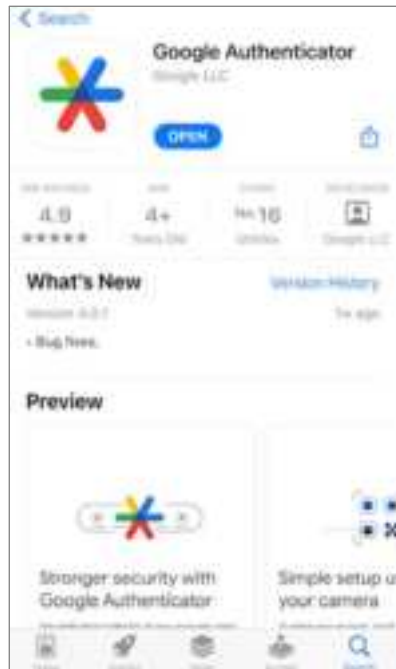
## Set up Google Authenticator





- Download and install Google Authenticator on your mobile device.

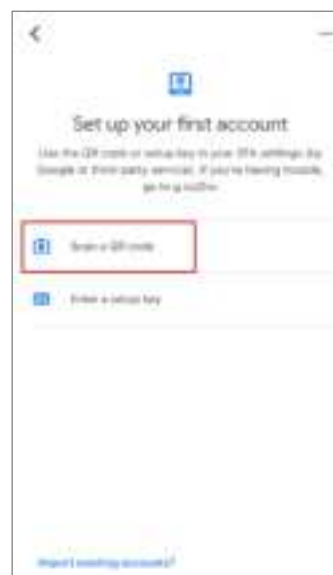
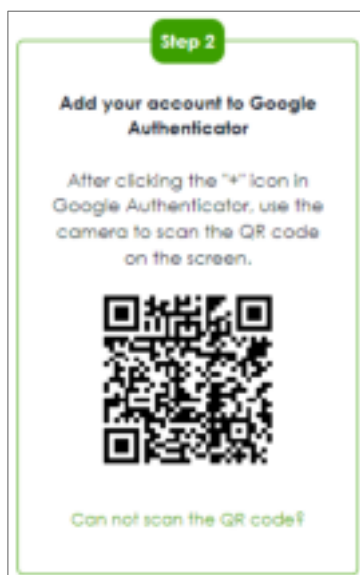
#### Apple Store



#### Google Play

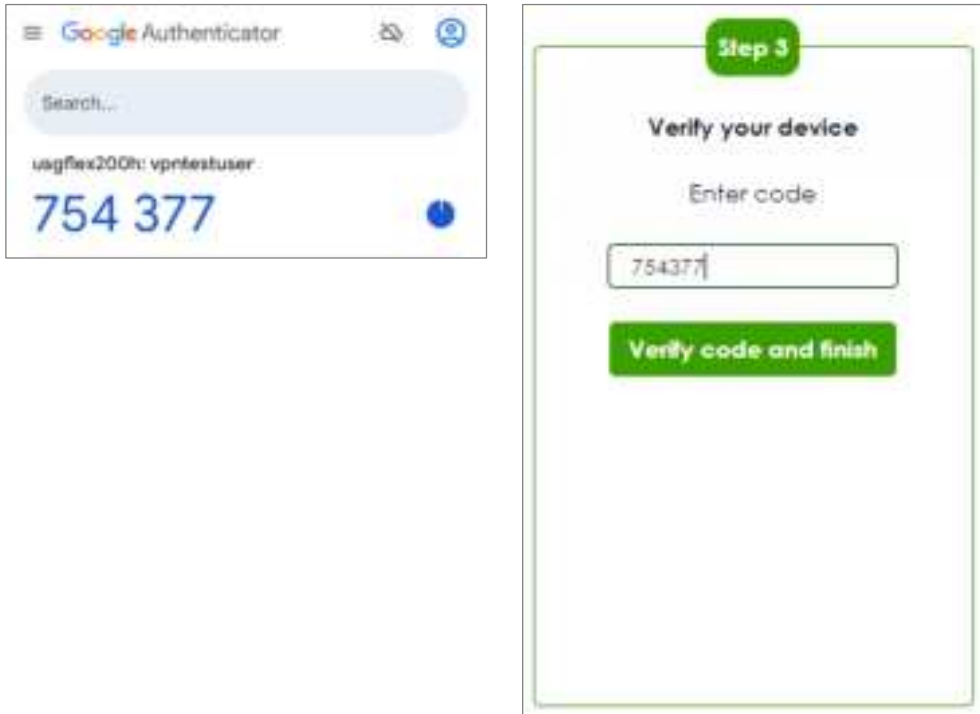


- Register the user account to Google Authenticator. Open Google Authenticator App and scan the barcode on Web GUI.

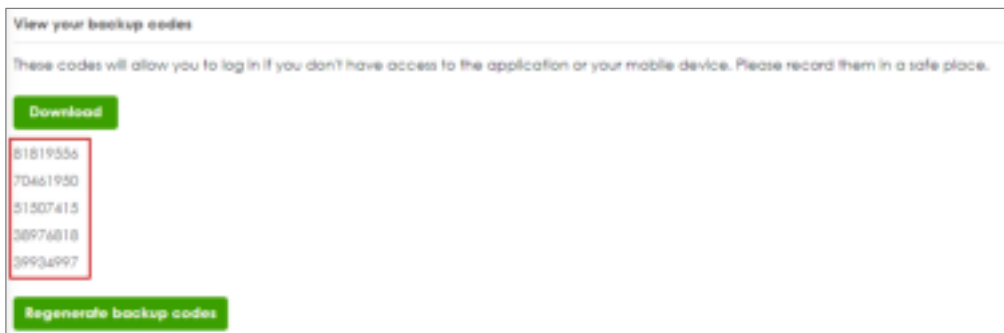




7. Enter the token code which displays on Google Authenticator to "Step 3" and click "Verify code and finish" to submit and verify the code.



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.

The screenshot displays the 'Two-factor Authentication' configuration page in the ZyXel Web GUI. The page is divided into three main sections: Admin Access, VPN Access, and Delivery Settings.

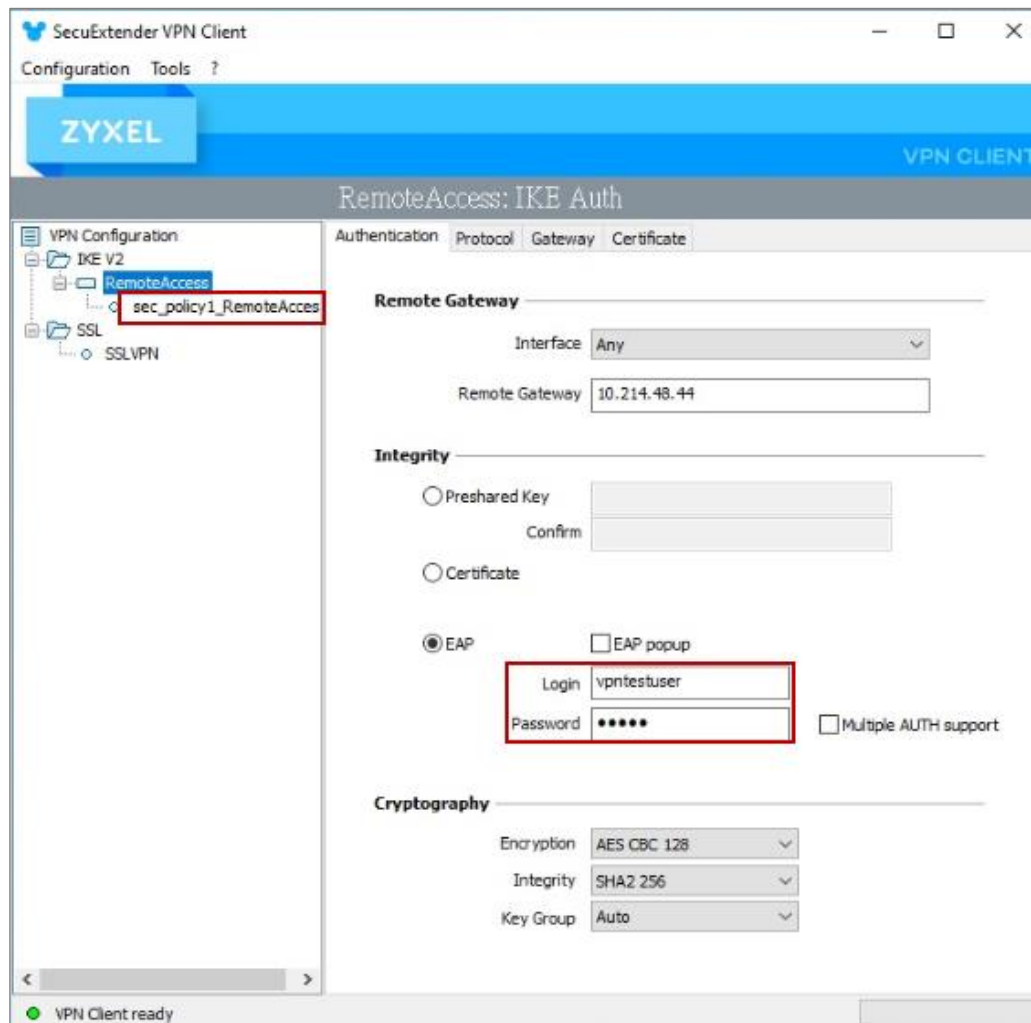
- Admin Access:**
  - Enable:** A green toggle switch is turned on.
  - Valid Time:** A text box contains the value '3', with '(1-5 minutes)' displayed next to it.
  - Two-factor Authentication for Services:** Two checkboxes are present: 'Web' (unchecked) and 'SSH' (unchecked).
- VPN Access:**
  - Enable:** A green toggle switch is turned on.
  - Valid Time:** A text box contains the value '3', with '(1-5 minutes)' displayed next to it.
  - Two-factor Authentication for Services:** Two checkboxes are present: 'SSL VPN Access' (checked) and 'IPSec VPN Access' (checked).
- Delivery Settings:**
  - Authorize Link URL Address:** A dropdown menu is set to 'HTTPS', followed by 'From interface' and 'ge3'.
  - Authorized Port:** A text box contains '8008', with '(1-65535)' and a green information icon displayed next to it.



## 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.

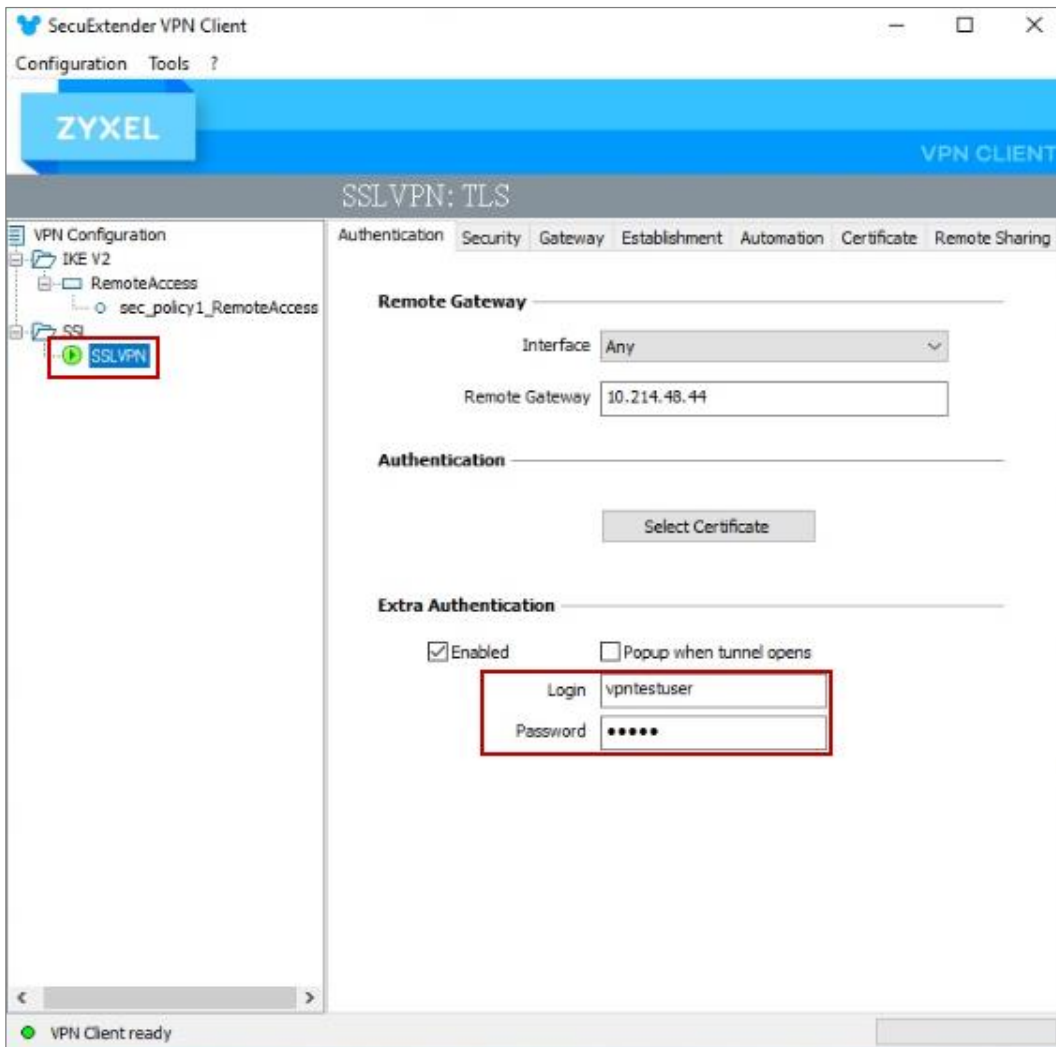


#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
56	2024-03-13 18:22:55	User	User vpnuser(192.168.50.1) is autho	0.0.0.0	0.0.0.0	0	Two-factor auth.
47	2024-03-13 18:22:45	User	User vpnuser(MAC=) from eap-otp h	10.214.48.49	0.0.0.0	0	Account: vpnuser
72	2024-03-13 18:22:45	IPSec VPN	assigning virtual IP 192.168.50.1 to peer	10.214.48.44	10.214.48.49	500	



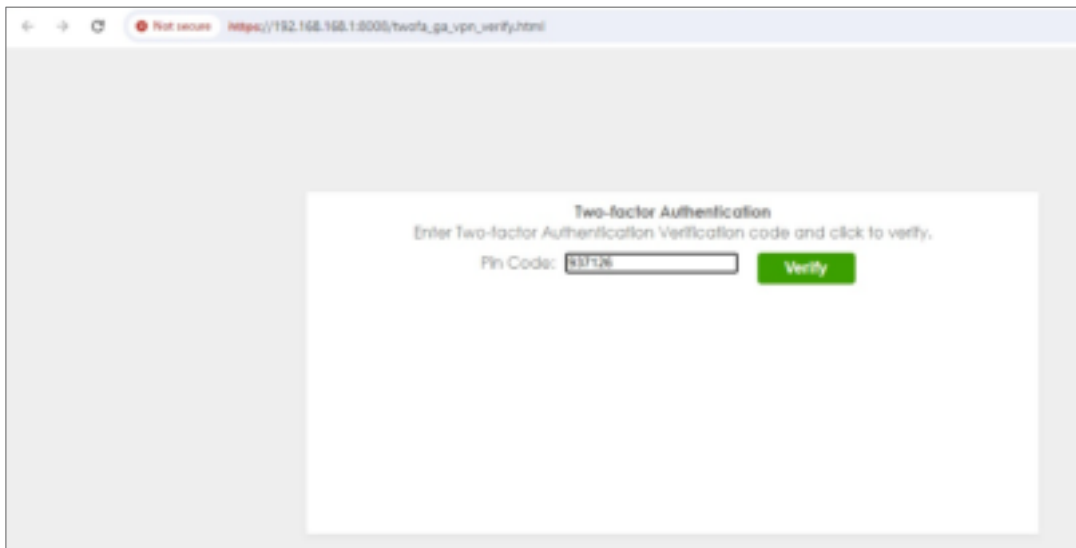
## SSL VPN

1. Open SSL VPN tunnel on SecuExtender VPN Client.





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



Two-factor Authentication

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

Pin Code:

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



Two-factor Authentication

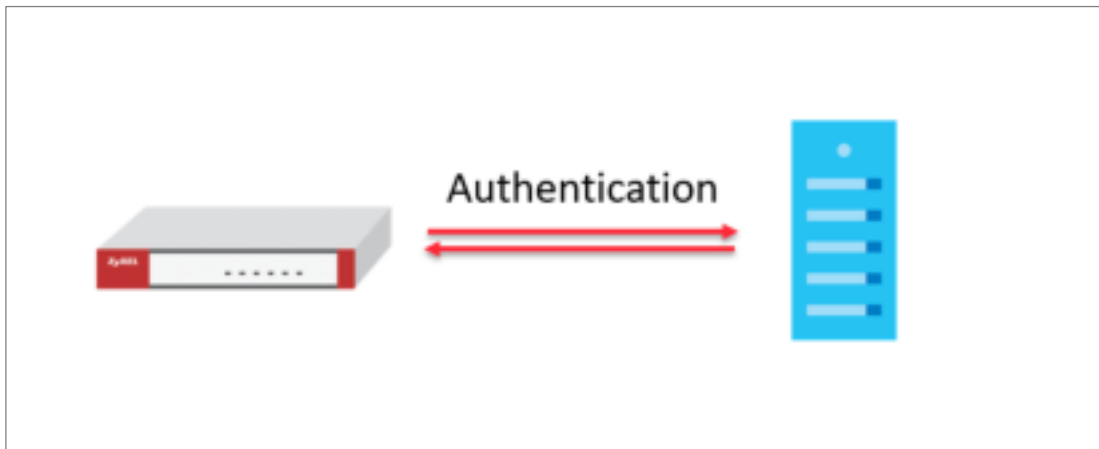
Authentication Success

#	Time	Category	Message	Src. IP	Dst. IP	Dst. Port	Note
1	2024-05-13 10:19:57	User	User vpnrestuser(192.168.51.2) is authorized	0.0.0.0	0.0.0.0	0	Two-factor auth.
2	2024-05-13 10:19:13	SSL VPN	SSL VPN client IP assigned 192.168.51.2	10.214.48.49	0.0.0.0	0	Account: vpnrestuser
3	2024-05-13 10:19:13	SSL VPN	SSL VPN Tunnel established	10.214.48.49	0.0.0.0	0	Account: vpnrestuser
4	2024-05-13 10:19:13	User	User vpnrestuser(SMAC=) from stvpn has logged in Device	10.214.48.49	10.214.48.44	0	Account: vpnrestuser
5	2024-05-13 10:19:13	SSL VPN	TLS Username/Password authentication succeeded for username 'vpnrestuser' (CN SET)	0.0.0.0	0.0.0.0	0	
6	2024-05-13 10:19:12	User	User vpnrestuser(SMAC=) from stvpn has logged in Device	10.214.48.49	10.214.48.44	0	Account: vpnrestuser



## 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.

 A screenshot of the ZyXel web interface showing the configuration page for an AD profile. The left sidebar shows the navigation menu with 'User & Authentication' selected. The main content area is titled 'Configuration' and contains several sections:
 

- Configuration:** Name (Microsoft\_AD), Description (Optional).
- Server Settings:** Server Address (10.214.48.38) (IP or FQDN), Backup Server Address (Optional) (IP or FQDN), Port (389) (1-65535), Use SSL (checkbox), Search time limit (5) (1-300 seconds), Case-sensitive User Name (checkbox).
- Server Authentication:** Domain Name (corp.com), User Name (Administrator), Password (masked), Repeat to Confirm (masked).
- Advanced Settings:** Configuration Validation section with a message: 'Please enter an existing user account in this server to validate the above settings.' and a User Name field with a green 'Test' button.



## Join Domain

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

Domain Zone Forwarder		
+ Add - Remove		
Domain *	DNS Server *	Query Via *
<input type="checkbox"/> csa.com	10.21.4.40.20	gal (WAN)

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

All Server Summary			
+ Add - Remove - Join Domain			
Server *	Server Address *	Domain Name *	Reference *
<input checked="" type="checkbox"/> Microsoft_02	10.21.4.40	Microsoft	0

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

All Server Summary		Join All Domains
+ Add - Remove - Join Domain		Microsoft_02
+ Add - Remove - Join Domain		Microsoft_02
+ Add - Remove - Join Domain		Microsoft_02
+ Add - Remove - Join Domain		Microsoft_02
+ Add - Remove - Join Domain		Microsoft_02
+ Add - Remove - Join Domain		Microsoft_02
+ Add - Remove - Join Domain		Microsoft_02
+ Add - Remove - Join Domain		Microsoft_02
+ Add - Remove - Join Domain		Microsoft_02

After join domain successfully, you can see this icon.

All Server Summary			
+ Add - Remove - Join Domain			
Server *	Server Address *	Domain Name *	Reference *
<input checked="" type="checkbox"/> Microsoft_02	10.21.4.40	Microsoft	0



## Test the Result

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

+ User & Authentication > User Authentication > AAA Server

### Server Authentication

Domain Name	csd.com
User Name	Administrator
Password	*****
Retype to Confirm	*****

Advanced Settings

### Configuration Validation

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

User Name	stanley	Test
-----------	---------	------

Test Status

OK

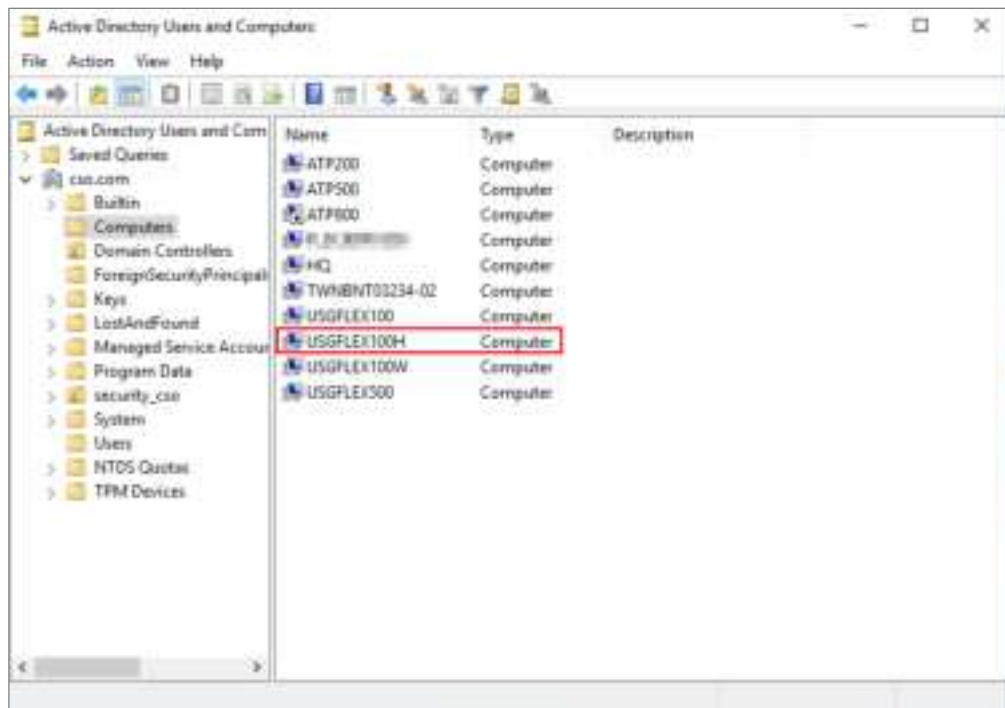
#### Returned User Attributes

```

dn: CN=stanley,CN=Users,DC=csd,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: stanley
givenName: stanley
distinguishedName: CN=stanley,CN=Users,DC=csd,DC=com
instanceType: 4
whenCreated: 20240305035708.0Z
whenChanged: 20240305035739.0Z
displayName: stanley
    
```



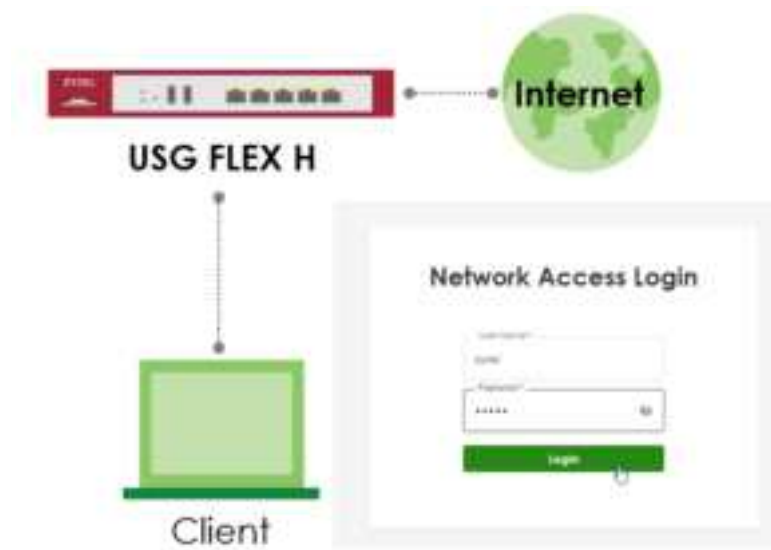
Check **computers** on Microsoft AD, you can see your firewall means join domain successfully.






## 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).

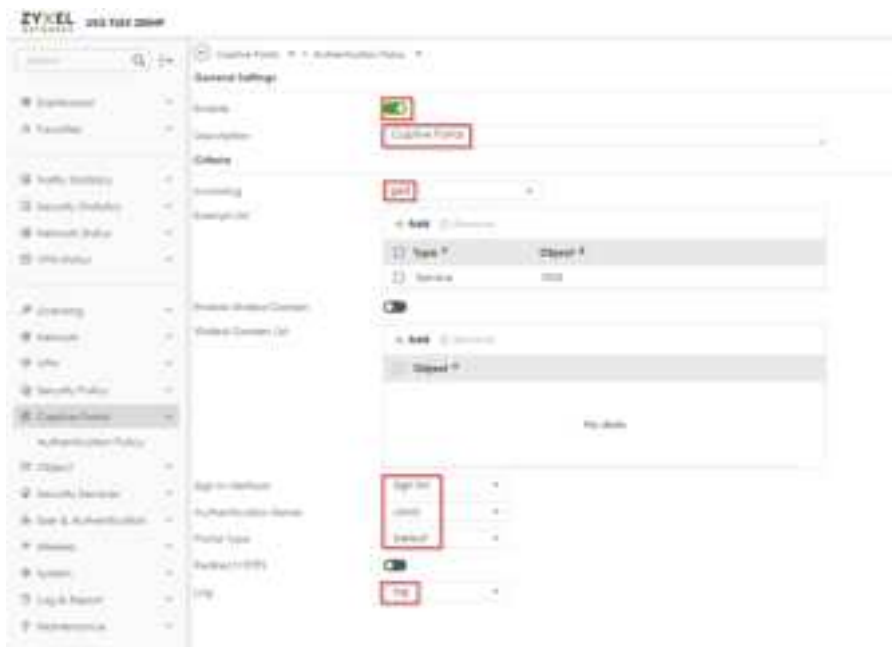


## Configure the Captive Portal via the Web-GUI

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.

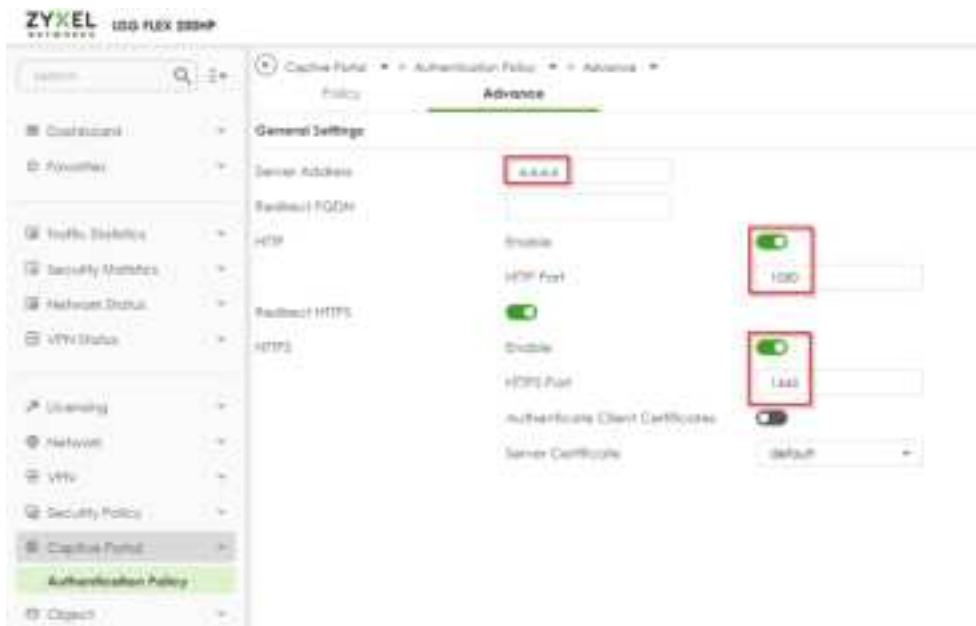




3. **Check the settings** – Ensure the Captive Portal function and the Authentication Policy are enabled.



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.

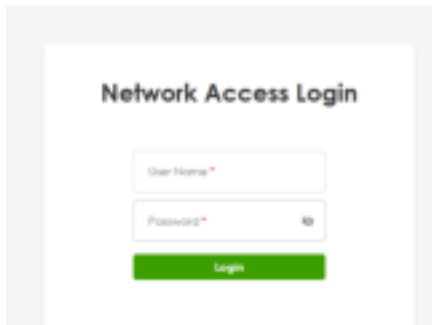




## Verify the Captive Portal function

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.



2. Enter the login User Name and Password.

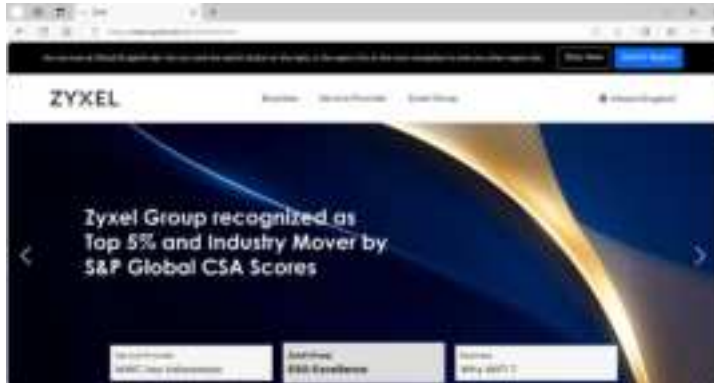


3. Once successfully logged into the Network Access Login page, the client will be redirected to the Welcome page, which displays the client's IP address, lease remaining time, and access timeout.





4. Eventually, the client can access the internet normally.



## How to logout the Captive Portal?

1. Enter the defined server link. The default link is <https://6.6.6.6>.



2. Enter the Welcome page and click 'Logout'.



3. 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.

The screenshot shows the ZYXEL Network Status > Login Users > Login Users page. It displays a table with the following columns: S/N, User ID, Name, Email, Login Time, Type, Status, Login Time, and Logout Time. The first row shows a user with ID 1, Name John, Email john@zyxel.com, Login Time 10:10:10, Type Web, Status Online, Login Time 10:10:10, and Logout Time 10:10:10. The second row shows a user with ID 2, Name Jane, Email jane@zyxel.com, Login Time 10:10:10, Type Web, Status Online, Login Time 10:10:10, and Logout Time 10:10:10.

S/N	User ID	Name	Email	Login Time	Type	Status	Login Time	Logout Time
1	1	John	john@zyxel.com	10:10:10	Web	Online	10:10:10	10:10:10
2	2	Jane	jane@zyxel.com	10:10:10	Web	Online	10:10:10	10:10:10

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.

The screenshot shows the ZYXEL Log & Report > Log / Events > System page. It displays a table with the following columns: S/N, Time, Category, Message, Src IP, Dest IP, Src Port, and Note. The first row shows a log message with S/N 1, Time 10:10:10, Category Web, Message User john@zyxel.com logged in to Device, Src IP 192.168.1.10, Dest IP 192.168.1.1, Src Port 80, and Note Success login.

S/N	Time	Category	Message	Src IP	Dest IP	Src Port	Note
1	10:10:10	Web	User john@zyxel.com logged in to Device	192.168.1.10	192.168.1.1	80	Success login


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.

The screenshot shows the ZYXEL Log & Report > Log / Events > System page. It displays a table with the following columns: S/N, Time, Category, Message, Src IP, Dest IP, Src Port, and Note. The first row shows a log message with S/N 1, Time 10:10:10, Category Web, Message User john@zyxel.com logged out to Device, Src IP 192.168.1.10, Dest IP 192.168.1.1, Src Port 80, and Note Success logout.

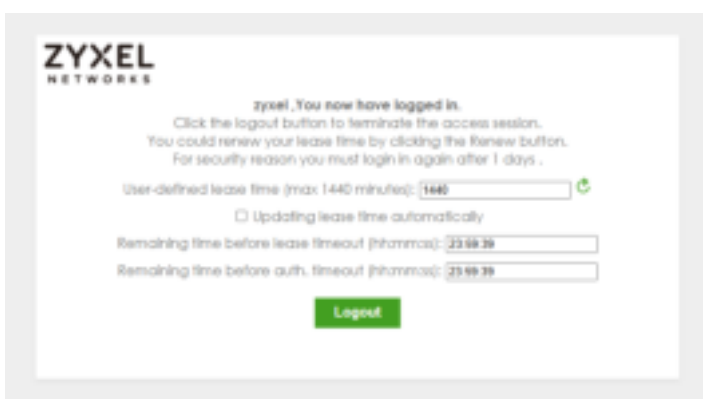
S/N	Time	Category	Message	Src IP	Dest IP	Src Port	Note
1	10:10:10	Web	User john@zyxel.com logged out to Device	192.168.1.10	192.168.1.1	80	Success logout



## 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.

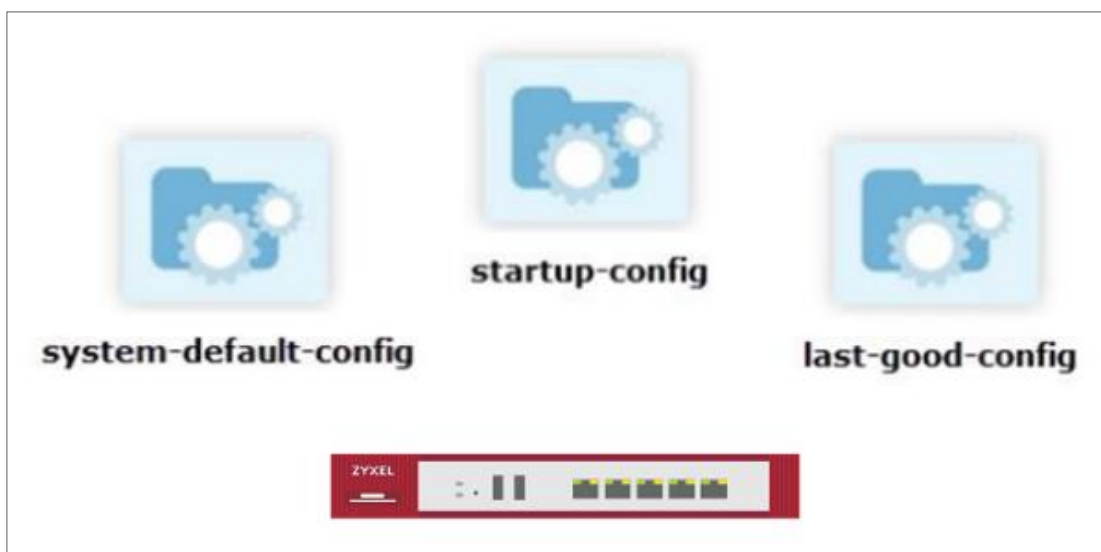





# Chapter 4- Maintenance

## 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.

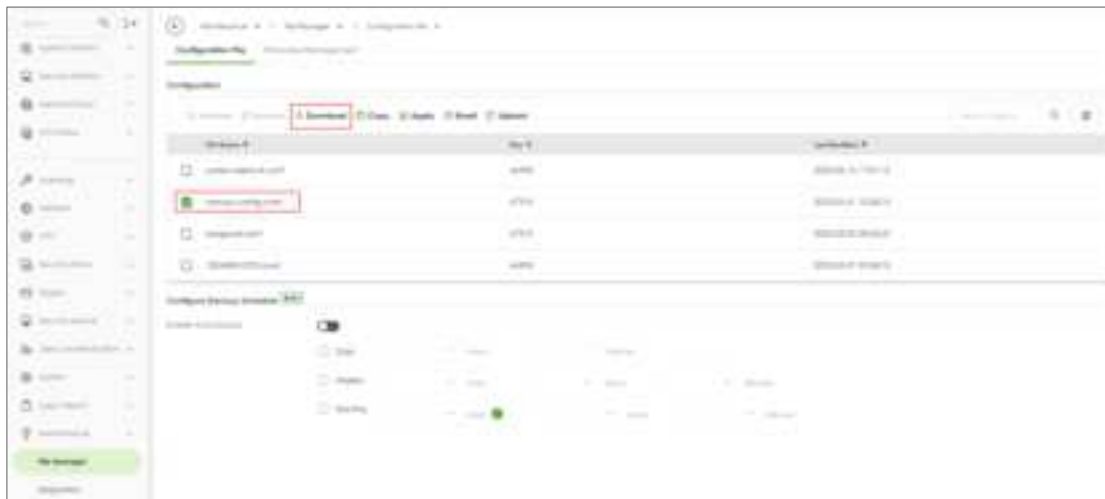
The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted.



## Download the Configuration Files

### Maintenance > File Manager > Configuration File

Select the startup-config.conf and click "Download".



## Copy the Configuration Files

### Maintenance > File Manager > Configuration File

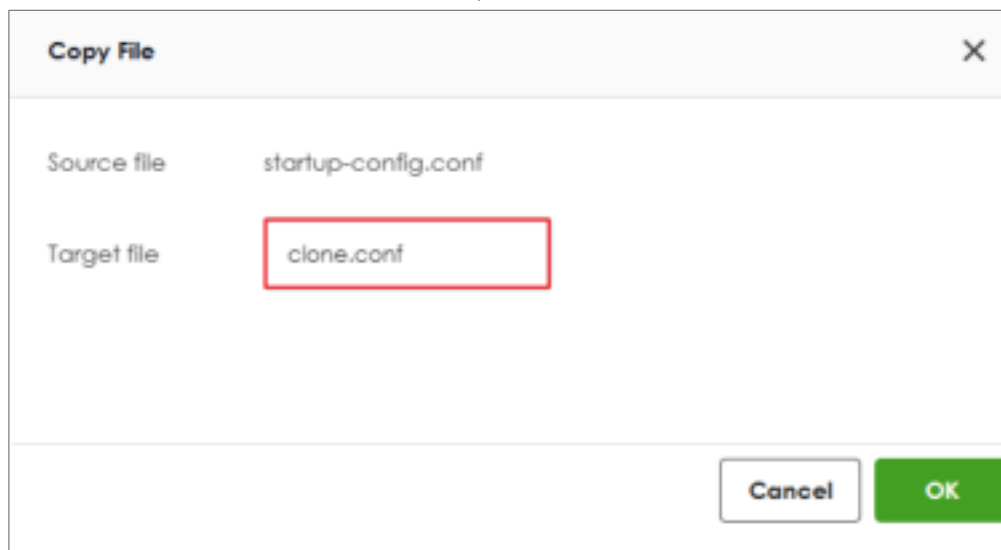
Select the file and click "Copy".





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

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



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

## Apply the Configuration Files

### Maintenance > File Manager > Configuration File

Select a specific configuration file to have ZyWALL use it. For example, select the **system-default.conf** file and click **Apply** to reset all of the ZyWALL settings to the factory defaults. Or select the **lastgood.conf** which is the most recently used (valid) configuration file that was saved when the device last restarted. If you uploaded and applied a configuration file with an error, select this file then click **Apply** to return the valid configuration. Click "OK", ZyWALL will reboot automatically.

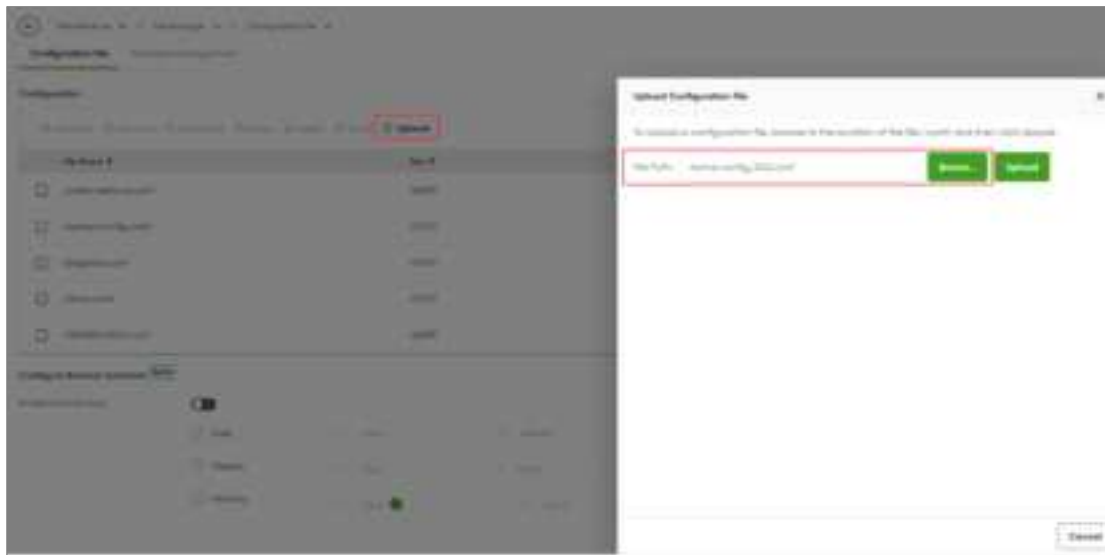




## Upload the Configuration Files

### Maintenance > File Manager > Configuration File

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






## How to Manage Firmware

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

### Local Firmware Upgrade

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

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



Status	Model	Version	Release Date	Action
Running	VAD-R40-2000	V1.0.0.0	2020-02-20 10:00:00	



Local Firmware

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.

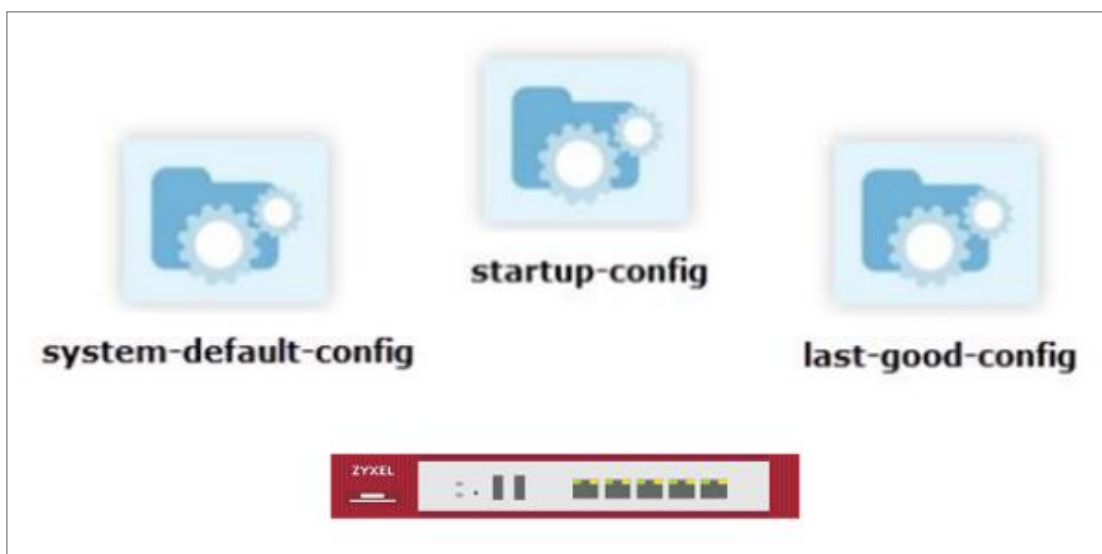
Cloud Firmware Information


Latest Version	None
Release Date	None
Auto Update	<input checked="" type="checkbox"/>
	<input type="radio"/> Daily <input type="text" value=""/> Hour
	<input type="radio"/> Weekly <input type="text" value=""/> Day <input type="text" value=""/> Hour
Auto Reboot	<input type="checkbox"/>



## How to set up configuration file backup rotation

In enterprise network environments, the integrity and availability of device configurations are critical to maintaining stable operations. To mitigate the risks associated with frequent configuration changes and human error, Zyxel uOS offers a Configuration Backup Rotation mechanism. This feature automatically retains the most recent configuration files while removing the oldest ones, enabling efficient storage management and reducing maintenance efforts. This document is intended to explain the principles, configuration methods, and limitations of the backup rotation function. It aims to assist network administrators in planning effective backup strategies and improving the automation and reliability of routine operations. With this feature, users can ensure that, even in the event of a misconfiguration or failure, the system can quickly revert to a known good state—minimizing downtime and maintaining a stable, resilient network infrastructure.



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

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

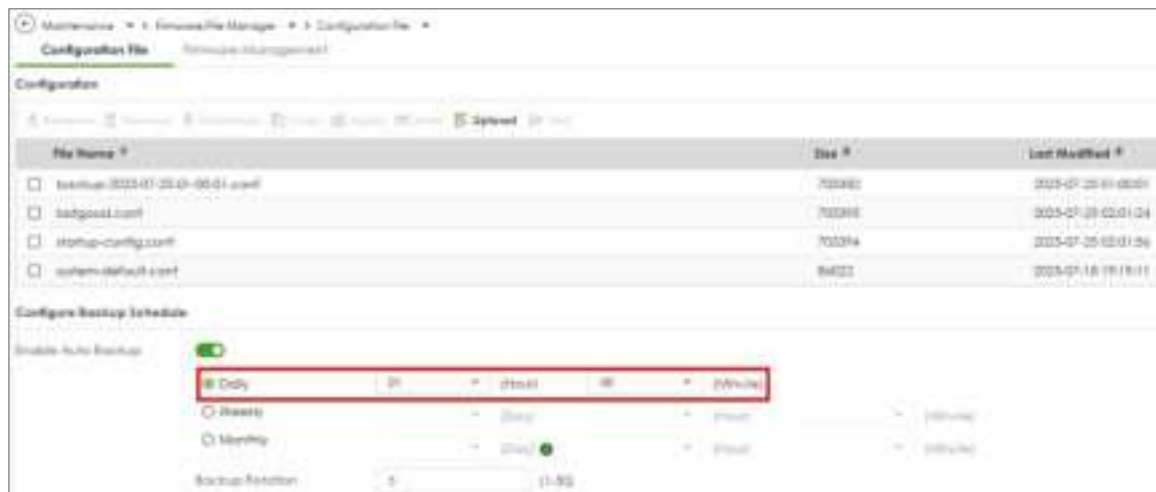
The **lastgood.conf** is the most recently used (valid) configuration file that was saved when the device last restarted.



Go to Configuration Backup Schedule section and enable “Enable Auto Backup”.

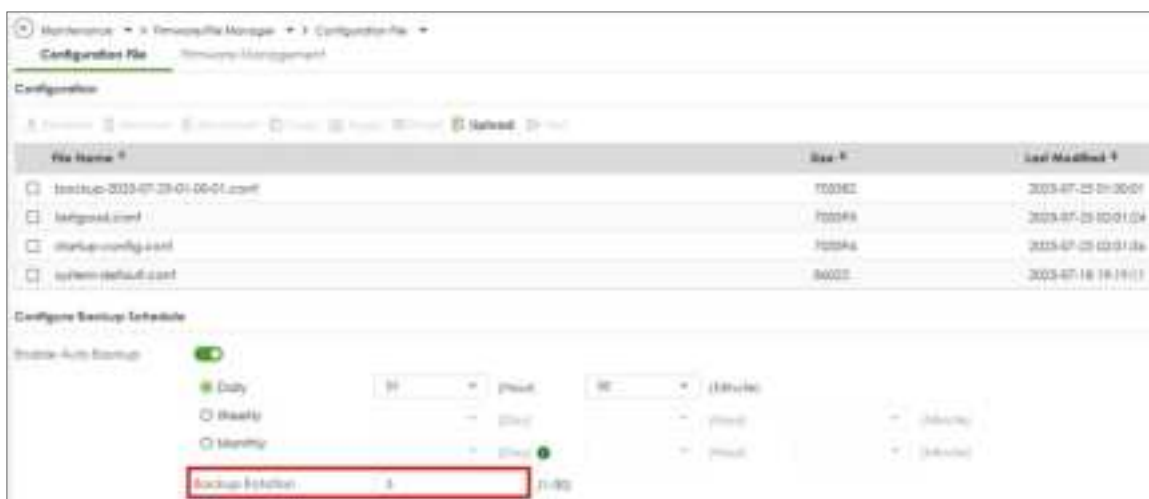


You can select the backup cycle based on your requirements. In this guide, we select daily backup and set the time to 01:00.



After Enabling auto backup, the backup rotation feature becomes available. The maximum number of auto backup configuration files is 50. In this example, we set 5 for rotation.



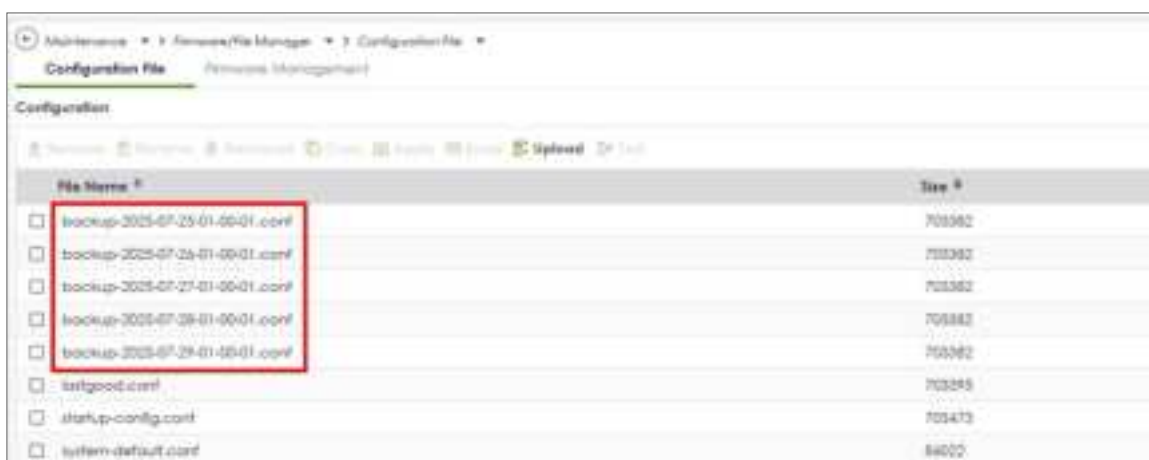


Note: By default, the system allows up to 65 backup files, with a maximum total size of 200 MB.

## Verification

### Maintenance > File Manager > Configuration File

Five scheduled backup configurations are generated based on the scheduled backup settings. The firewall has automatically backed up five files, and it deletes the oldest file before performing an automatic backup.





If the Auto Backup total size limit is reached, no new files will be generated, and backup rotation will not remove old files. The following event will be recorded in the Event log.

System							
APC AP							
Category System Clear log Export Refresh							
Search logs							
#	Time	Category	Message	Src. IP	Dest. IP	Dest. Port	Note
11	2025-07-17 16:16:01	System	Configuration backup error: total size of all configuration files exceeds the maximum limit	0.0.0.0	0.0.0.0	0	
34	2025-07-17 15:48:16	System	Geo-IP country database version 20250713 update has succeeded.	0.0.0.0	0.0.0.0	0	

If the Auto Backup maximum file number is reached, no new files will be generated, and backup rotation will not remove old files. The following event will be recorded in the Event log.

System							
APC AP							
Category System Clear log Export Refresh							
Search logs							
#	Time	Category	Message	Src. IP	Dest. IP	Dest. Port	Note
9	2025-07-17 14:00:01	System	Configuration backup error: maximum number of configuration files reached	0.0.0.0	0.0.0.0	0	



## 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 the ZyXel management interface. The breadcrumb trail at the top indicates the path: System > Notification > Mail Server. The page is divided into two main sections: 'General Settings' and 'Mail Server Test'.

**General Settings:**

- Mail Server:** A text field containing 'smtp.gmail.com' with a tooltip that reads '(Outgoing SMTP Server Name and IP Address)'.
- Port:** A text field containing '587' with a tooltip that reads '(Port)'.
- TLS Security:** A toggle switch that is turned on (green).
- STARTLS:** A toggle switch that is turned on (green).
- Authenticate Server:** A toggle switch that is turned off (grey).
- SMTP Authentication:** A toggle switch that is turned on (green).
- Username:** A text field containing 'test1234@gmail.com'.
- Password:** A text field with masked characters (asterisks).
- Retype:** A text field with masked characters (asterisks).

**Mail Server Test:**

- Mail To:** A text field with a tooltip that reads '(Email Address)'.
- Send From:** A text field with a tooltip that reads '(Email Address)'.
- Send Now:** A green button located at the bottom left of the 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

☒ Append system name
 ☒ Append date time

Email from

Email to

(Email Address)
   
 (Email Address)
   
 (Email Address)
   
 (Email Address)
   
 (Email Address)

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

### Report Items

System Resource Usage

☒ CPU Usage
 ☒ Interface Usage
 ☒ Memory Usage
 ☒ Port Usage
 ☒ Session Usage

Security Services

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

System Information

☒ DMZ Table

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

### Schedule

Time For Sending Report

(Hour)
  (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.

Email Subject: 500H-Daily-Report

☒ Append system name ☒ Append date time

Email from: 500H-Daily-Report@gmail.com

Email to: 500H-Daily-Report@gmail.com (Email Address)

(Email Address)

(Email Address)

(Email Address)

(Email Address)

**Send Report Now**

500H-Daily-Report@gmail.com  
500H

**ZYXEL**  
NETWORKS

**Device**

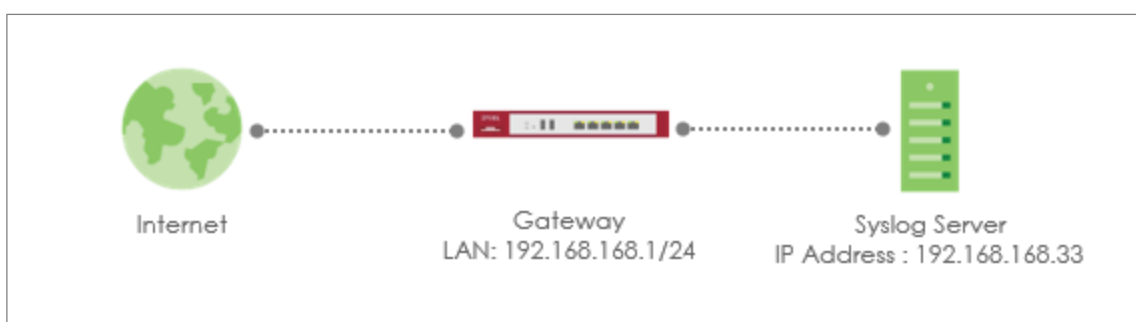
Device Name:	500H-Daily-Report
Primary IP:	192.168.1.100
MAC Address Range:	08:00:27:00:00:00 - 08:00:27:00:00:0F
System Uptime:	10 Days, 12:34:56
System Name:	500H-Daily-Report


**System Overview Change**



## 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.

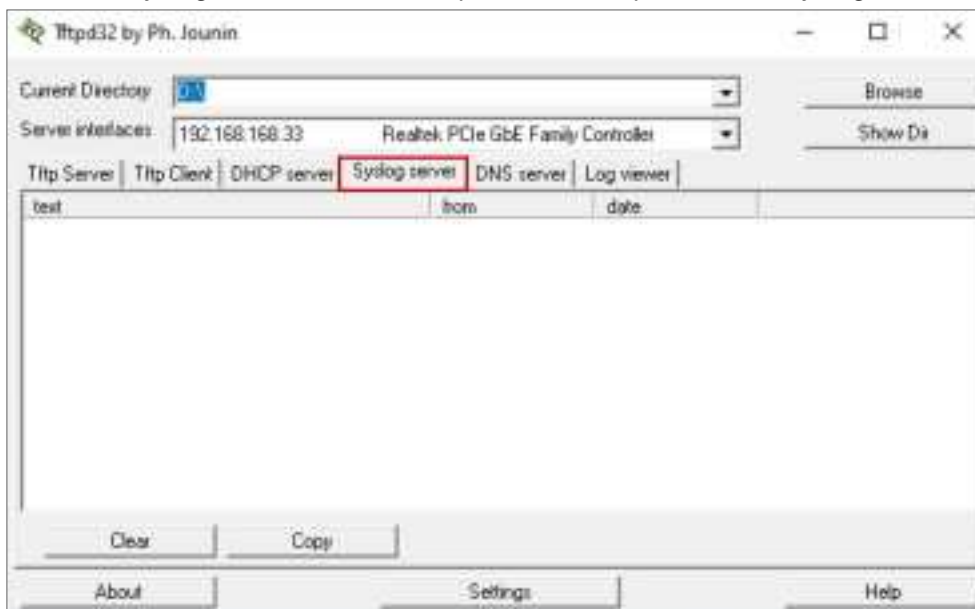


 **Note:** All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.10).



## 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

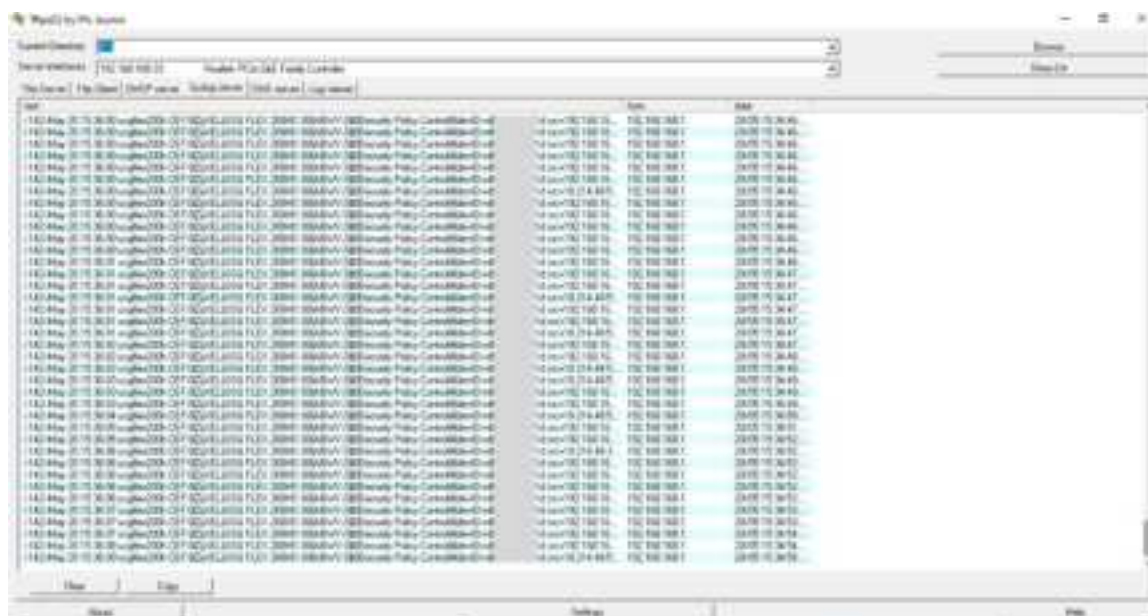
Go to Log & Report > Log Settings > Log Category Setting. Use the drop-down list to select what information you want to log from each log category.

Log Category Setting													
Category	System Log			USB Storage			Remote Server 1			Remote Server 2	Count		
<input type="text" value=""/>	disable	normal	debug	disable	normal	debug	disable	normal	debug	disable	normal	debug	130
> 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"/>	9
> VPNs	<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



Remote Server 1	Remote Server 2
Active	<input checked="" type="checkbox"/>
Log Format	CEF/Syslog
Server Address	192.168.168.33 (Server Name or IP Address)
Server Port	514
Log Facility	Local 1


Check logs on the syslog server.





## How to Setup and Send logs to the USB storage

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

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

### USB Storage device

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

### Set Up the USB storage on the Gateway

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

Log Category Setting					
Category	System Log	USB Storage	Remote Server 1	Remote Server 2	Count
	disable normal debug	disable normal debug	disable normal debug	disable normal debug	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.



## Check the USG Log Files

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




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

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



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





7. 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 or any)

8. 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 (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 sniff and analyze network traffic by intercepting and displaying packets transmitted in the network interface.

### Syntax:

cmd traffic-capture <interface name>

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

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

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



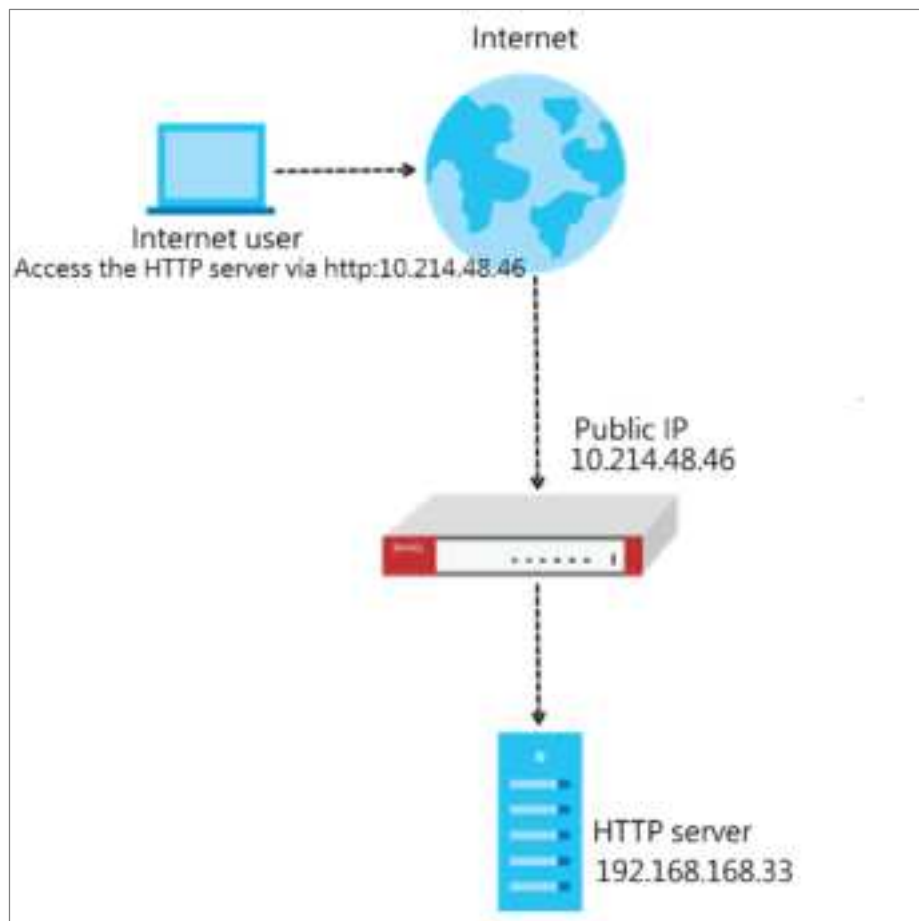
cmd traffic-capture <interface name> filter "host <ip address> and port <port number>"

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



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

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

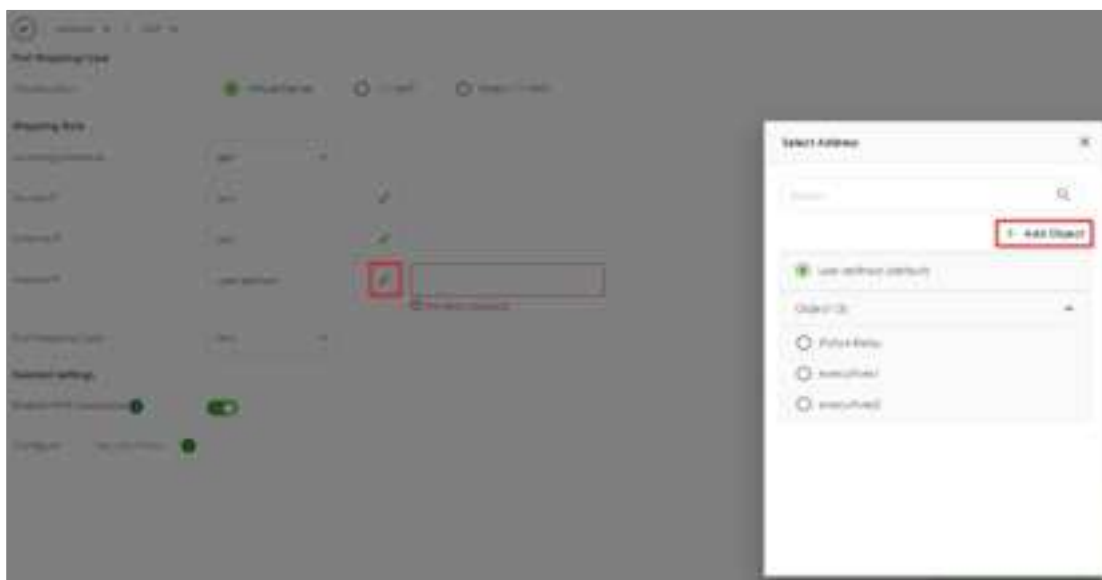




## Set Up the NAT

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

- Input the rule name
- select Virtual Server
- Incoming Interface: ge1
- Configure the Source IP to limit the access by the Source IP. You may select Any
- Configure the External IP. Select Any to choose the ge1 interface IP as the external IP.
- Configure the internal IP. Click +Add Object to create an address object as a host 192.168.168.33 which is the IP address of the internal server.





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

←

Network

>

NAT

General Settings

Enable Rule

☒

Rule Name

Internal\_server

Port Mapping Type

Classification

☒ Virtual Server
 ☐ 1:1 NAT
 ☐ Many 1:1 NAT

Mapping Rule

Incoming Interface

ge1

Source IP

any

External IP

user defined

10.214.48.46

Internal IP

Internal\_server

Port Mapping Type

Service

External Service

HTTP

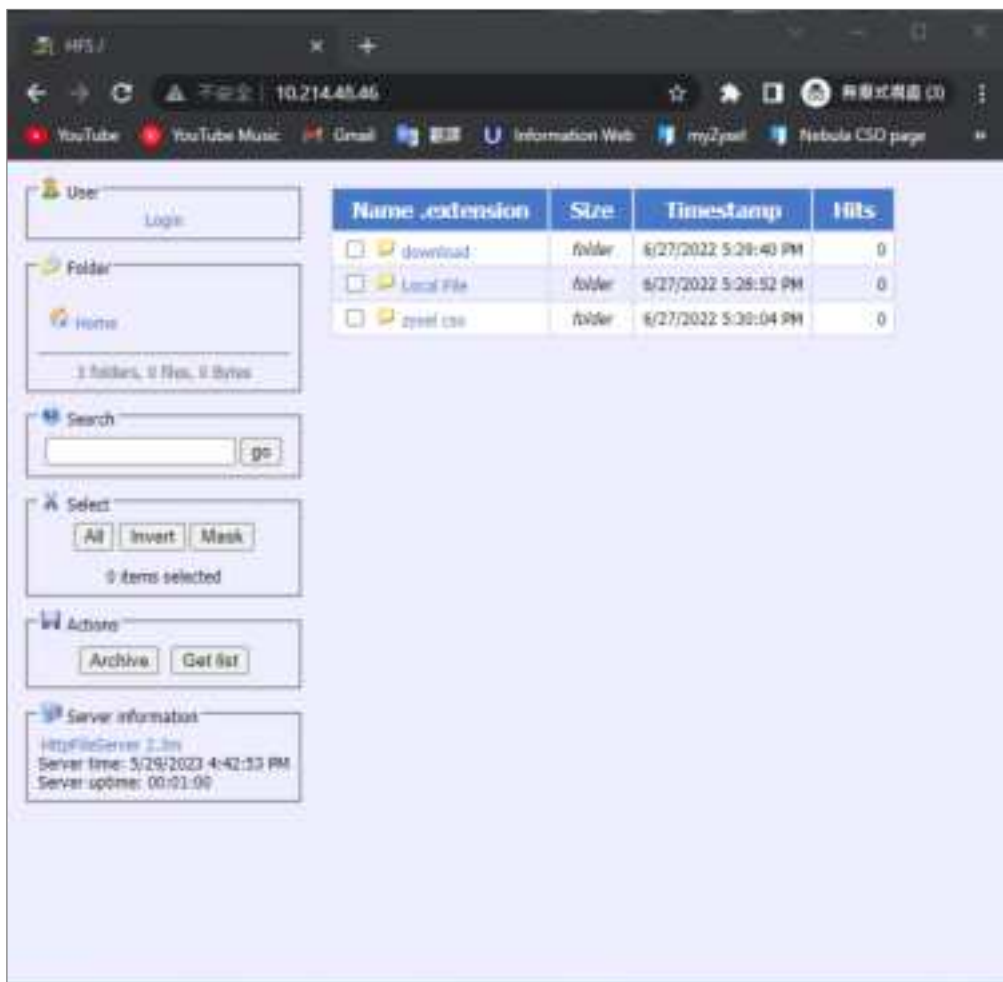
Internal Service

HTTP



## Test the Result

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



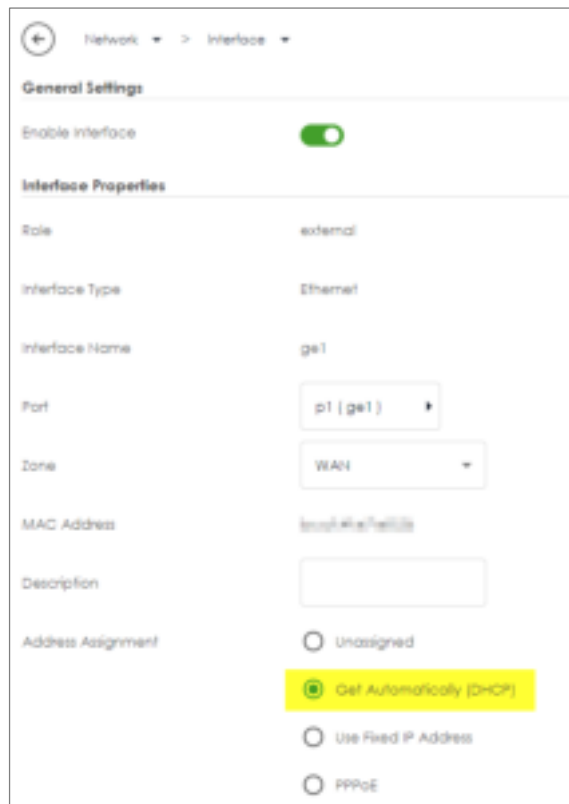


## How to Configure DHCP Option 60 – Vendor Class Identifier

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 'Interface Properties' configuration page for the WAN interface. The 'Address Assignment' section is highlighted in yellow, indicating the selected option is 'Get Automatically (DHCP)'.

General Settings	
Enable interface	<input checked="" type="checkbox"/>
Interface Properties	
Role	external
Interface Type	Ethernet
Interface Name	ge1
Port	p1   ge1
Zone	WAN
MAC Address	8000:40:00:00:00:00
Description	
Address Assignment	<input checked="" type="radio"/> Get Automatically (DHCP) <input type="radio"/> Use Fixed IP Address <input type="radio"/> 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**

## 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.

```

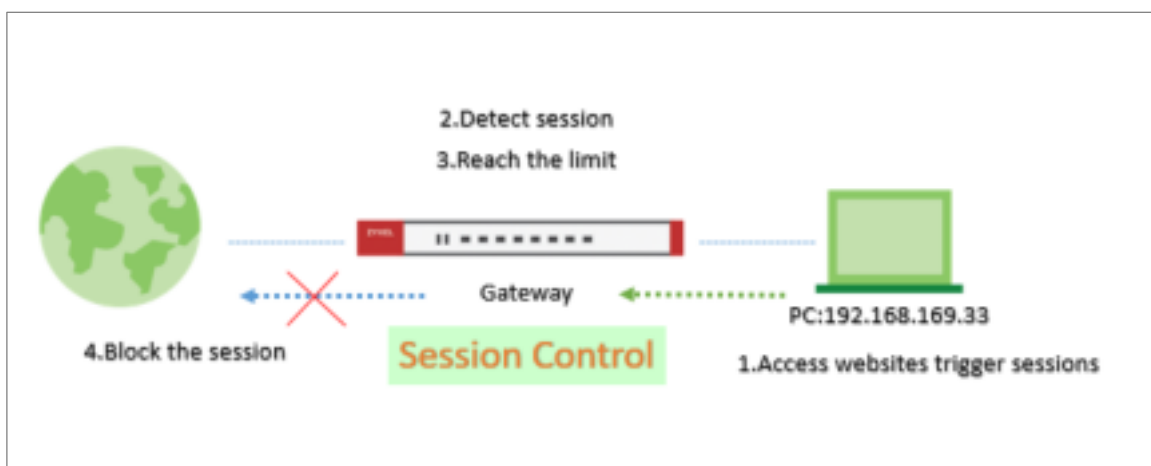
77 25.048787 0.0.0.0 255.255.255.255 DHCP 342 DHCP Discover - Transaction ID 0x0e96c136
> Frame 77: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface \Device\NPF_{A6AF40E6-CF63-4365-AF89-BE1C70B0F0B0}, id 0
> Ethernet II, Src: ZyxelCom_e7:e8:36 (8c:00:f8:a7:e8:36), Dst: Broadcast (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
> Dynamic Host Configuration Protocol [Discover]
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 0
  Transaction ID: 0x0e96c136
  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 (8c:00:f8:a7: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
  > Option: (60) Vendor class identifier
    Length: 7
    Vendor class identifier: CSD-FAQ
  > Option: (61) Client identifier
  > Option: (255) End
  Padding: 0000000000

```



## How to Configure Session Control

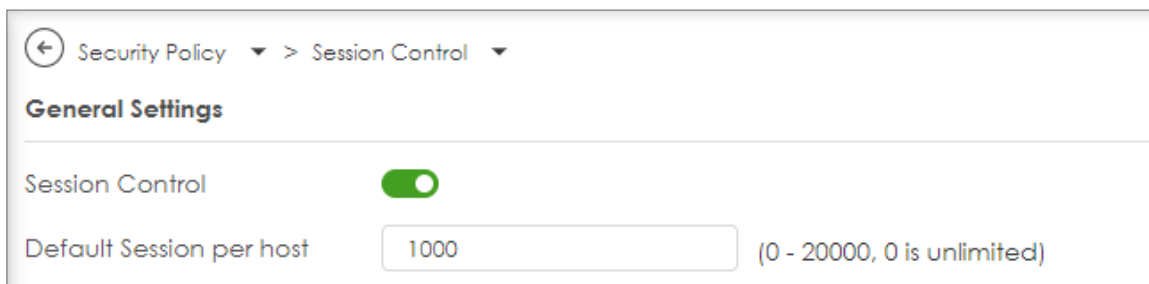
Session control can address abnormal user behavior. By monitoring session activities, the firewall can detect deviations from normal usage, such as sudden traffic spikes or unauthorized access attempts. This proactive approach enables prompt action to be taken to investigate and mitigate potential security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

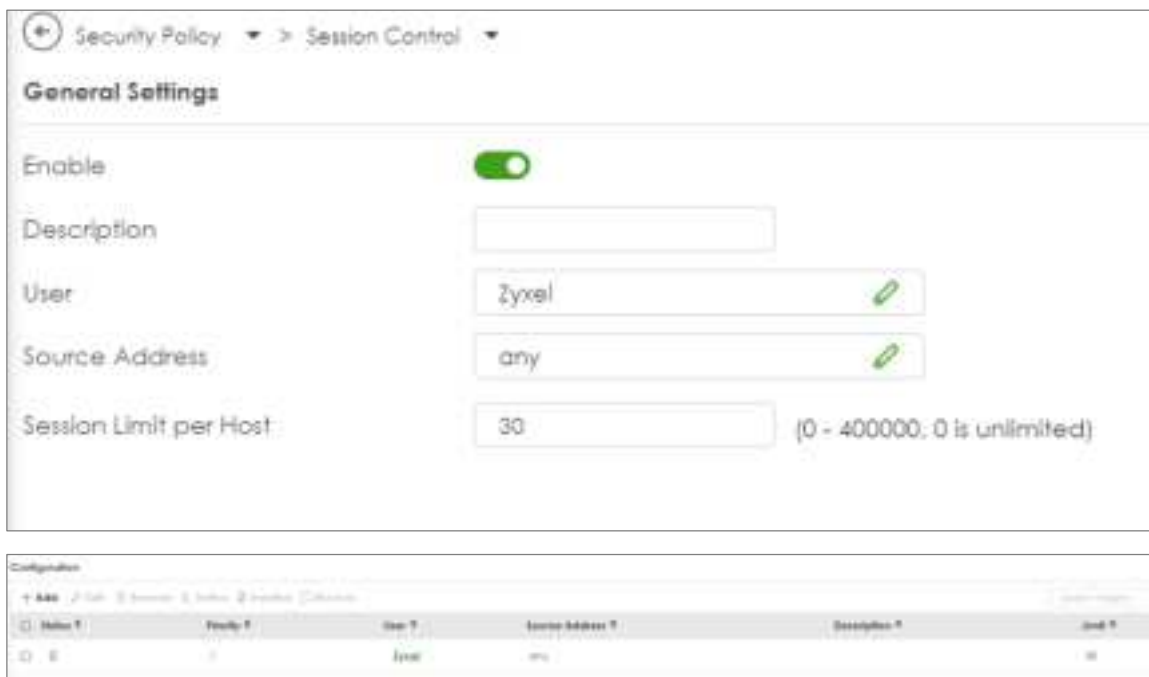
The field here is for the client who is not in the rule under the list



Index	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

Index	Priority	User	Source Address	Description	Limit
1	1	Zyxel	any		30




## Test the Result

Log in as User: Zyxel



**Zyxel ,You now have logged in.**

Click the logout button to terminate the access session.  
You could renew your lease time by clicking the Renew button.  
For security reason you must login in again after 1 days .

User-defined lease time (max 1440 minutes):  

☐ Updating lease time automatically

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

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

**Logout**

Try to access web browser to hit the session limit

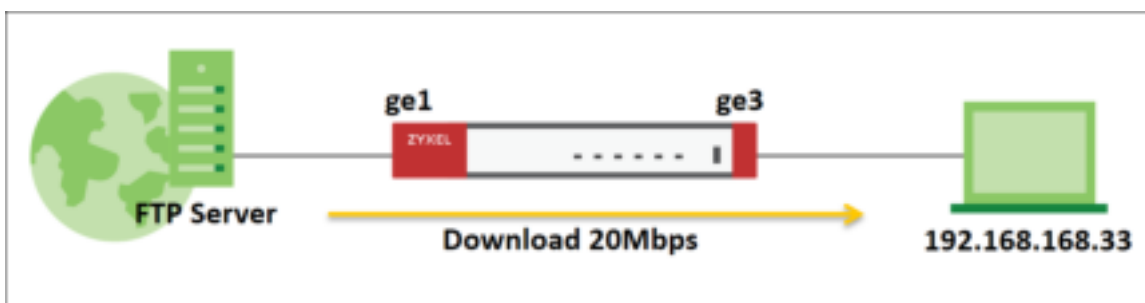
Go to Log & Report > Log/Events and select Session Control to check the logs.


Session Control	Maximum sessions per host (30) was exceeded.	192.168.149.33	172.23.5.1	0	ACCESS BLOCK
Session Control	Maximum sessions per host (30) was exceeded.	192.168.149.33	172.23.5.2	0	ACCESS BLOCK
Session Control	Maximum sessions per host (30) was exceeded.	192.168.149.33	172.25.5.210	0	ACCESS BLOCK
Session Control	Maximum sessions per host (30) was exceeded.	192.168.149.33	172.21.5.1	0	ACCESS BLOCK
Session Control	Maximum sessions per host (30) was exceeded.	192.168.149.33	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 ge3 (LAN)

Outgoing Interface ge1 (WAN)

Source LAN1\_SUBNET ✎

Destination any ✎

Service Type ☒ Service Object ☐ Application Group

Service Object FTP ✎

User any ✎

Schedule none ✎

### Traffic Shaping

Download Limit ☐ Unlimited ☒ Limit 20 Mbps

Upload Limit ☒ Unlimited ☐ Limit 0 Mbps

Priority Medium(4)

### Related Setting

Log log



Incoming Interface: ge3

Outgoing Interface: ge1

Source: LAN1 IP Subnet

Application Group: FTP

Traffic Shaping: Download Limit 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.

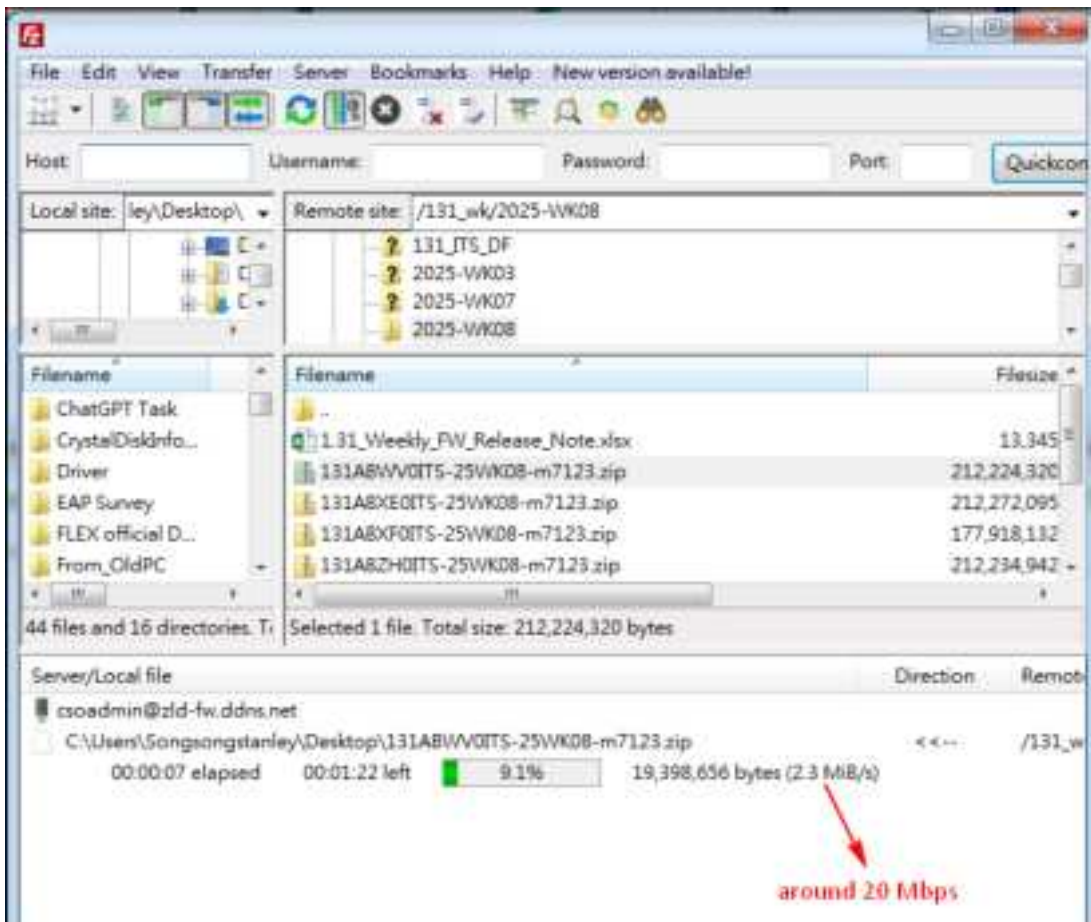


Turn on this feature. It will enable BWM function to allowing the rules to be effectively applied.



## 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.

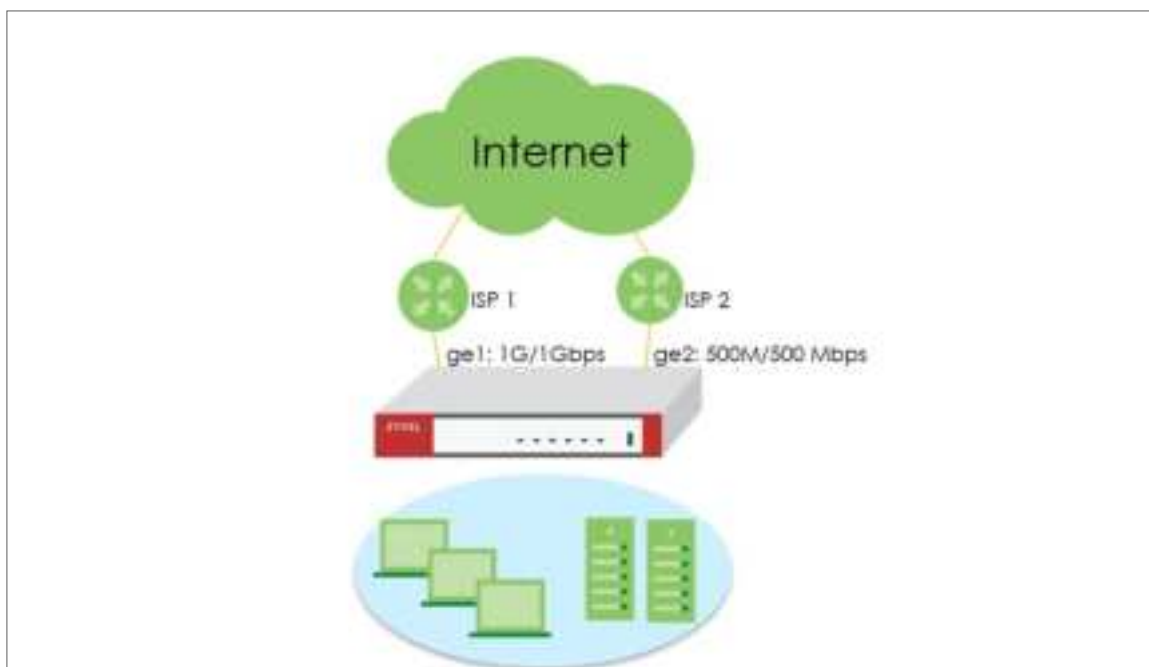


ID	Time	Category	Message	Src IP	Dest IP
1	2025-05-27 18:54:15	Info	Bandwidth management: 100Mbps/100Mbps/100Mbps	192.168.1.100	54.115.140.30
2	2025-05-27 18:54:30	Info	Bandwidth management: 100Mbps/100Mbps/100Mbps	192.168.1.100	54.115.140.30



## How to Configure WAN trunk for Spillover and Least Load First

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



Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 500H (Firmware Version: uOS 1.20).

### Least Load First



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

### Spillover

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

## Set Up the User-Defined Trunk

### Spillover and Least Load First

Go to Network > Interface > Trunk page, and click **Add** button to create user-defined Trunk. In the general settings, we can configure the following settings;

Name: Least Load First (Enter a descriptive name for this trunk)

Algorithm: LLF

Load Balancing Index: Outbound

**Note:** This field is available if you selected to use the **Least Load First** or **Spillover** method.



Network > Interface > Trunk

**General Settings**

Name: L2

**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

General Settings

Name:

Load Balancing Setting

Algorithm:

Load Balancing Index:

**Add**

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**

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

Click **Apply** to save changes.

**Some changes were made**

What do you want to do then?



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

Network > Interface > Trunk

interface **Trunk** Port

Default WAN Trunk

Trunk Selection:

☐ Default Trunk

☒ User-Defined Trunk LLF

User-Defined Trunk

+ Add Edit Remove Reference Search rights

Name	Algorithm	Members
<input type="checkbox"/> LLF	llf	ge1, ge2
<input type="checkbox"/> Spillover	spill-over	ge1, ge2

Default Trunk

Edit Save

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.

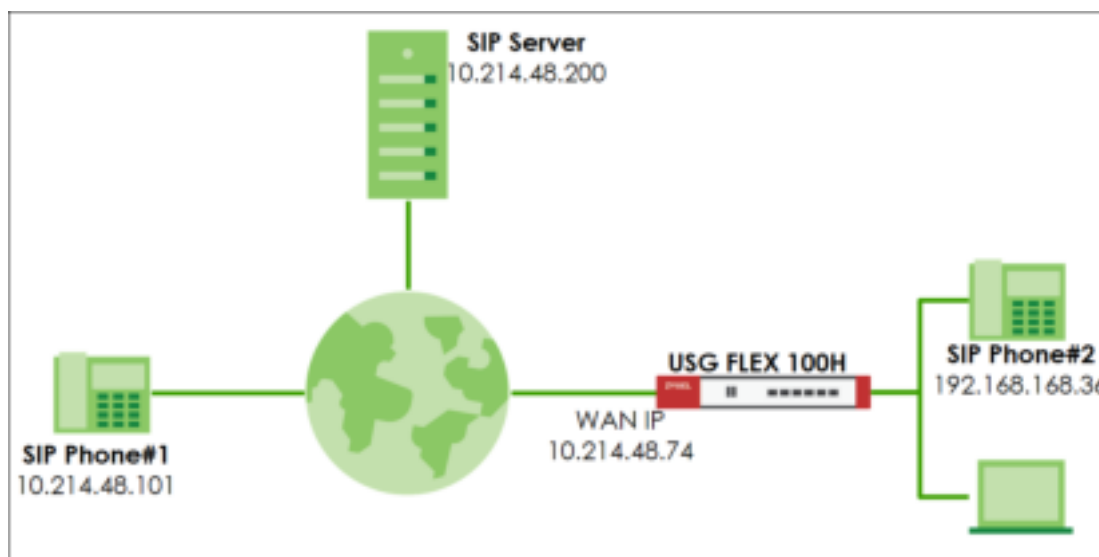
### SIP Transformation

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  (I-65535)

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

**SIP ALG**

Enable ☒ ←

SIP Signaling Port

+ Add Remove

☐ Port

☐ 5060

SIP Inactivity Timeout ☒ 120 seconds

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 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.

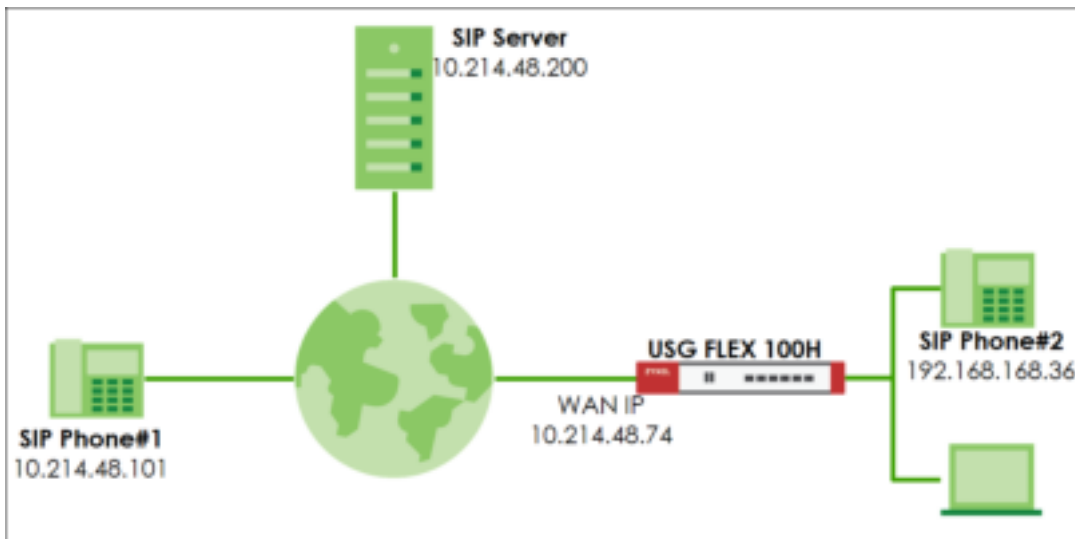


### Peer to Peer connection restriction:

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.

Network > ALG

**SIP 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

SIP Inactivity Timeout ☒

Media Inactivity Timeout  seconds

Signaling Inactivity Timeout  seconds

Restrict Peer to Peer Media Connection ☒

Restrict Peer to Peer Signaling Connection ☒



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

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

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

```

mgfls1000> show conntracks | match "192.168.168.36"
udp      17 294 src=192.168.168.36 dst=10.214.48.200 sport=10007 dport=11815 packets=1 bytes=83 [UNREPLIED]
src=10.214.48.200 dst=10.214.48.74 sport=11815 dport=10007 packets=0 bytes=0 mark=0 use=1

udp      17 51 src=192.168.168.36 dst=10.214.48.200 sport=10006 dport=11814 packets=2 bytes=400
src=10.214.48.200 dst=10.214.48.74 sport=11814 dport=10006 packets=1 bytes=200 [ASSURED] mark=16777216 use=1

udp      17 51 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=536 [ASSURED] mark=16777216 use=1

mgfls1000>
mgfls1000>
mgfls1000>
mgfls1000>

```

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

```

mgfls1000> show conntracks | match "192.168.168.36"
udp      17 294 src=192.168.168.36 dst=10.214.48.200 sport=10007 dport=10004 packets=9512 bytes=1961000
src=10.214.48.200 dst=10.214.48.74 sport=10254 dport=10007 packets=18665 bytes=3733000 [ASSURED] mark=0 helper=RTF use=1

udp      17 2904 src=192.168.168.36 dst=10.214.48.200 sport=10005 dport=10255 packets=30 bytes=1212
src=10.214.48.200 dst=10.214.48.74 sport=10255 dport=10255 packets=73 bytes=6718 [ASSURED] mark=0 helper=RTF use=1

udp      17 2944 src=192.168.168.36 dst=10.214.48.200 sport=5061 dport=5060 packets=38 bytes=4216
src=10.214.48.200 dst=10.214.48.74 sport=5060 dport=5061 packets=5 bytes=2900 [ASSURED] mark=0 helper=slp use=1

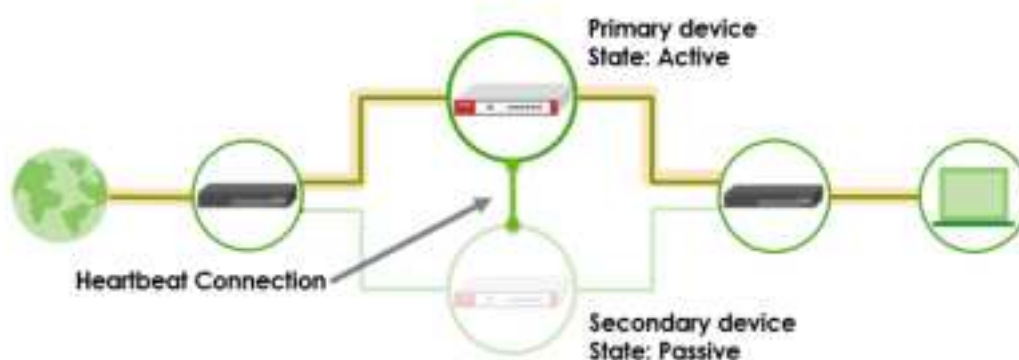
mgfls1000>
mgfls1000>
mgfls1000>
mgfls1000>
mgfls1000>


```



## 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.



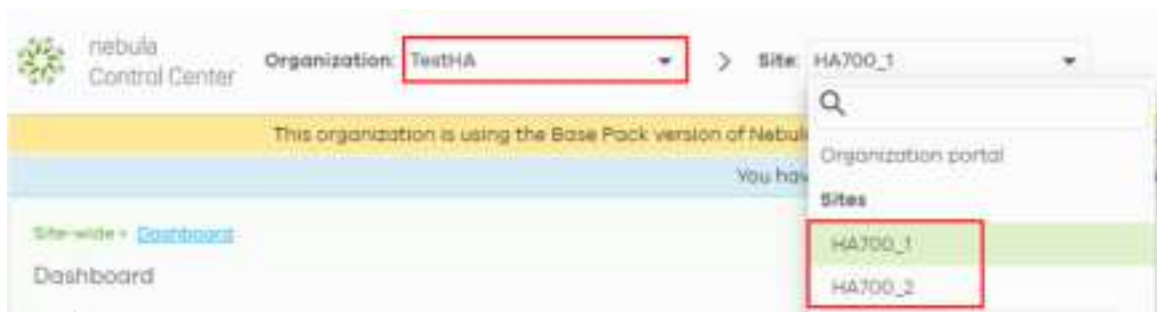
 Note: Device HA is supported on USG FLEX 200H, USG FLEX 200HP, USG FLEX 500H, USG FLEX 700H. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.32).



## 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.

Interface								
External								
Status	Name	Zone	Description	IP/Netmask	VLAN ID	Type	Members	Reference
<input checked="" type="checkbox"/>	ge1	WAN		10.216.48.19/255.255.255.0		Ethernet	p1	3
<input checked="" type="checkbox"/>	ge2	WAN		0.0.0.0/0.0.0		Ethernet	p2	1
Internal								
Status	Name	Zone	Description	IP/Netmask	VLAN ID	Type	Members	Reference
<input checked="" type="checkbox"/>	ge3	LAN		192.168.168.1/255.255.255.0		Ethernet	p3p4,p5,p6	2
<input checked="" 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

**General Settings**

Enable ☒

**Management Configuration**

Initial Role ☒ Primary (License Controller)

HA MAC address ☐ Physical MAC address ☒ Virtual MAC address

☐ Secondary

Active Node Management IP

Passive Node Management IP

Management IP Subnet Mask

**Monitor Interface**

Member

Failover on Monitored Interface Link Down ☒

Failover on Monitored Connectivity Check Failure ☐



## 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: ☒

**Interface Properties**

Role: Internal

Interface Type: Ethernet

Interface Name: ge4

Port: p7 | ge4 p8 | ge4

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: ☒

**Management Configuration**

Initial Role: ☒ Primary (License Controller) ☒ Secondary

HA MAC address:  Physical MAC address  Virtual MAC address

Active Node Management IP:

Passive Node Management IP:

Management IP Subnet Mask:



## 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 shows the 'HA Status' tab in the Zyxel web interface. At the top, there are three tabs: 'HA Status' (selected), 'HA Configuration', and 'HA Log'. Below the tabs, the 'Status' section displays a diagram of the High Availability (HA) setup. It shows a 'Primary' device (Active) and a 'Secondary' device (Passive) connected by a heartbeat link. The Primary device has a green location pin icon and the Secondary device has a green checkmark icon. 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'.



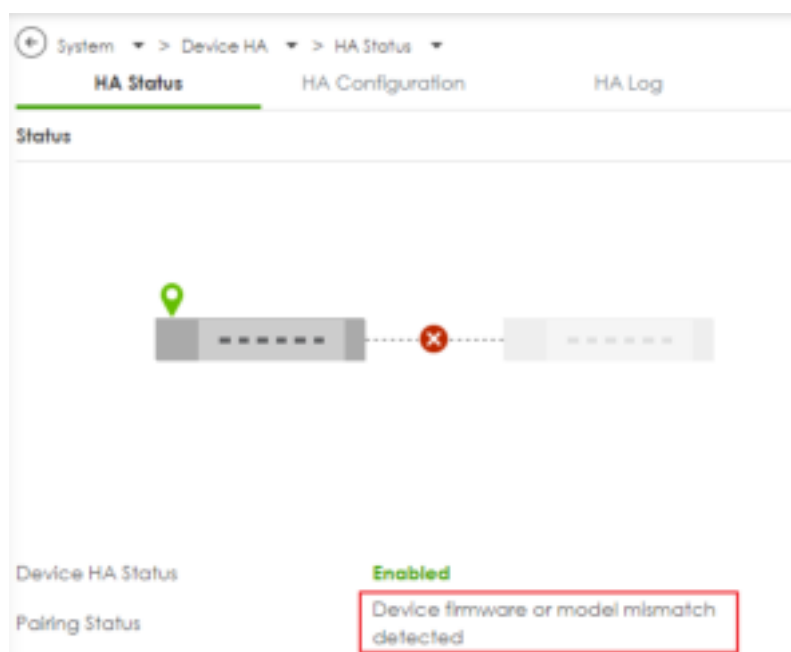
You can also enter the command on the primary device to check HA status. ***usgflex200h> show state vrf main device-ha status***


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 5009
    icon-color on
    ..
  passive
    role secondary
    sn S22 3298
    icon-color on
    ..
  ..
```

If Pairing 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.





 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 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
Fallover on Monitored Interface Link Down	<input checked="" type="checkbox"/>
Fallover on Monitored Connectivity Check Failure	<input type="checkbox"/>

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 Mode**

System > Device HA > HA Status

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

Active

Passive

Secondary

Primary

Device HA Status: Enabled

Pairing Status: Paired

**Synchronization Status**

Last Full Sync Status: Success

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

**Fallover Status**

Fallover Reason: Monitor interface link down

Last Fallover 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	<div> <div>p3 (ge3) </div> <div>p4 (ge3) </div> <div>p5 (ge3) </div> <div>p6 (ge3) </div> </div>
Zone	LAN
MAC Address	<input checked="" type="radio"/> Use Default MAC Address <span>d6:ec:e5:1f:1f:1f</span> <input type="radio"/> Overwrite Default MAC Address <span>auto3</span>

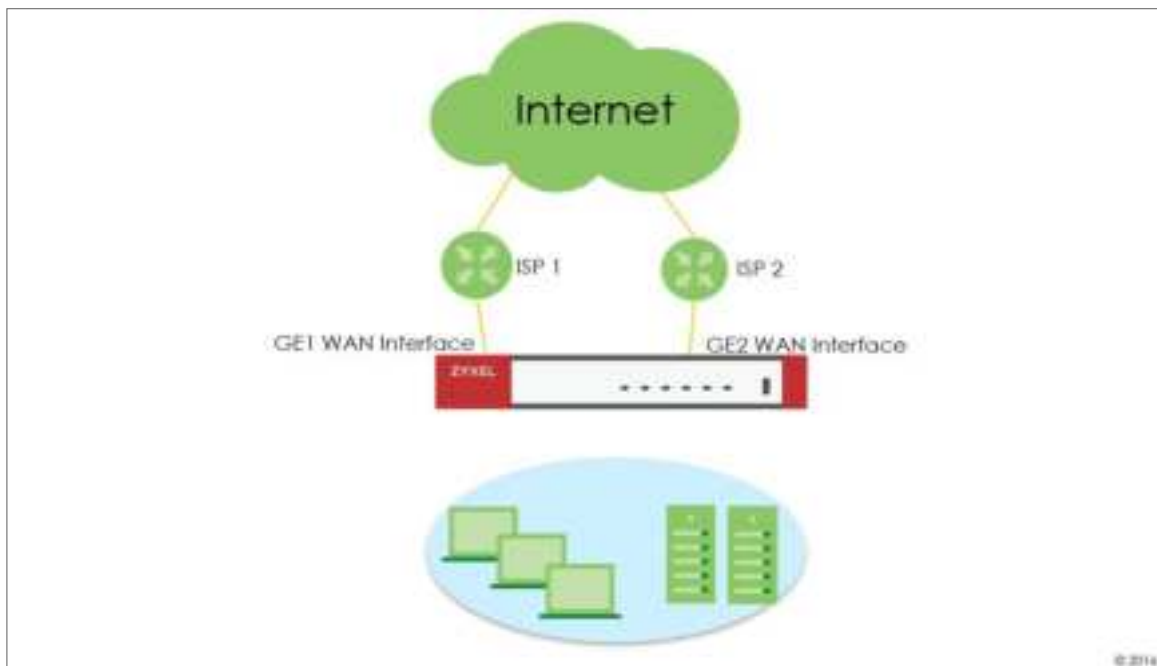
## SYS LED Status

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.



The screenshot shows the 'Load Balancing Setting' page. The 'Algorithm' is set to 'wrr'. Below, a table lists the interfaces and their modes.

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.



The screenshot shows the 'Static Route' configuration page. A table lists the configured static routes.

Status	Name	Destination	Next Hop	Description	Metric
<input type="checkbox"/>	Google_DNS	8.8.8.8/32	ge2		0

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



The screenshot shows the 'Policy Route' configuration page. A table lists the configured policy routes.

Status	Id	Src	Schedule	Incoming	Source	Destination	DSCP Code	Service	Source Port	Next Hop	DSCP Marking	SNAT	VM
<input type="checkbox"/>	1	192.168.1.0/24	none	ge1	LAN1 subnet	any	any	any	any	ge1	preserve	outgoing interface	

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"
```

[illegible]

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.

- 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"
```



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.

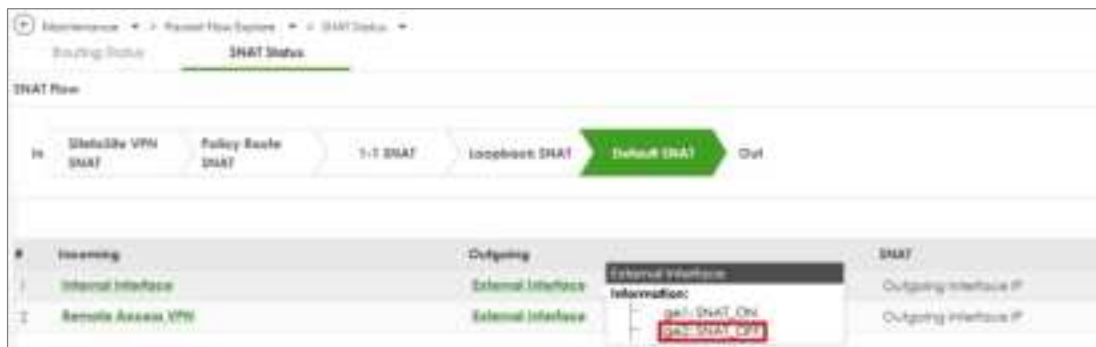




- Go to **"Maintenance > Packet Flow Explorer > SNAT Status"** to check for possible issues.



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.



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



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 ***`pinging 8.8.8.8 -t`*** in the Windows Command Prompt to check if it has an ICMP response from 8.8.8.8.

[illegible]

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.

[illegible]



## 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: ge3

Port: pf1/gd1

Zone: LAN

MAC Address: ☒ Use Default MAC Address (fc:22:34:16:91:4c) ☐ Overwrite Default MAC Address (null)

Description:

Address Assignment: ☒ Unassigned ☐ Use Fixed IP Address

[? Network Tools]

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:

The valid character are [a-z][A-Z][0-9][>][A-Z][\_].

The valid character are [a-z][A-Z][0-9][>][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: LAG-ge-3-4  
 Zone: LAN  
 MAC Address: ☒ Use Default MAC Address  
☐ Overwrite Default MAC Address  
 Description:   
 Address Assignment: ☐ Unassigned ☒ Use Fixed IP Address  
 IP/Network Mask: 172.198.1.1/24  
 + Add ☒ Remove  
 IP/Netmask:   
 No data  
 Secondary IP:   
 Members: ☒ ge3 ☒ ge4  
 Mode: static  
 active-backup (1-1000ms)  
 loop (802.3ad)  
 LAG 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

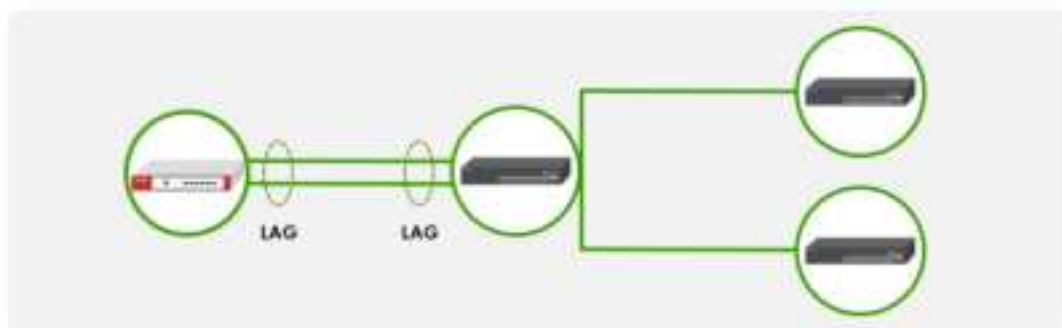
**Primary:** Allows you to specify which member interface should be preferred as the active link

Members	ge5 ge6
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	ge5 ge6
Mode	lacp (802.3ad)
Link 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	ge5 ge6
Mode	static
Link Monitoring Interval	100 (1-1000)ms
Transmit Hash Policy	src-dst-ip-mac



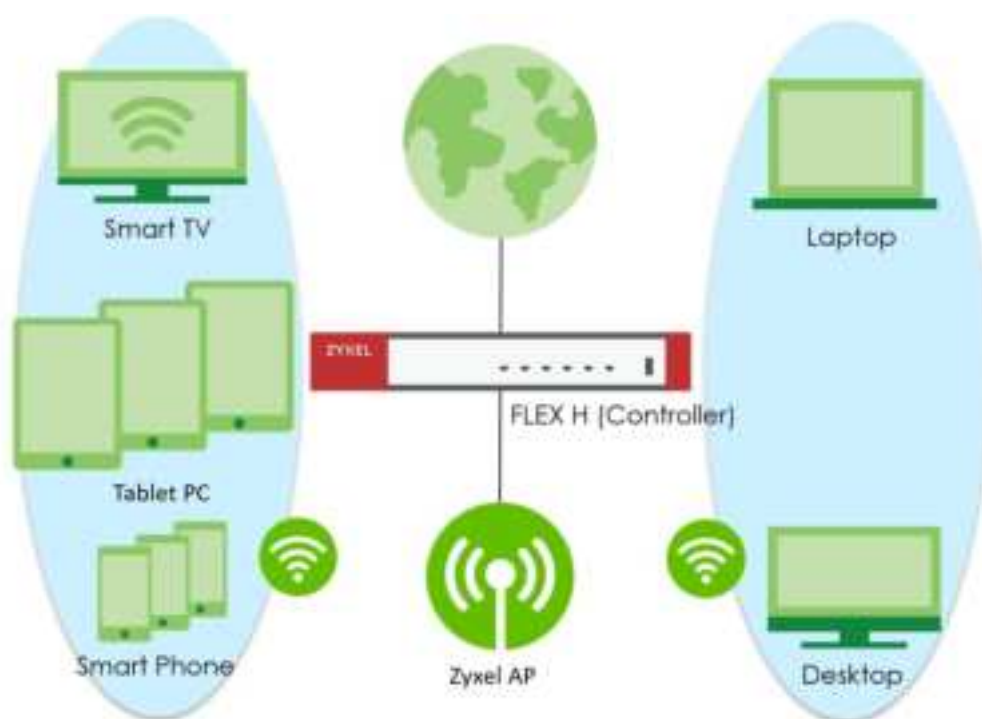
**Checked by CLI: show state vrf main interface lag**


```
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.



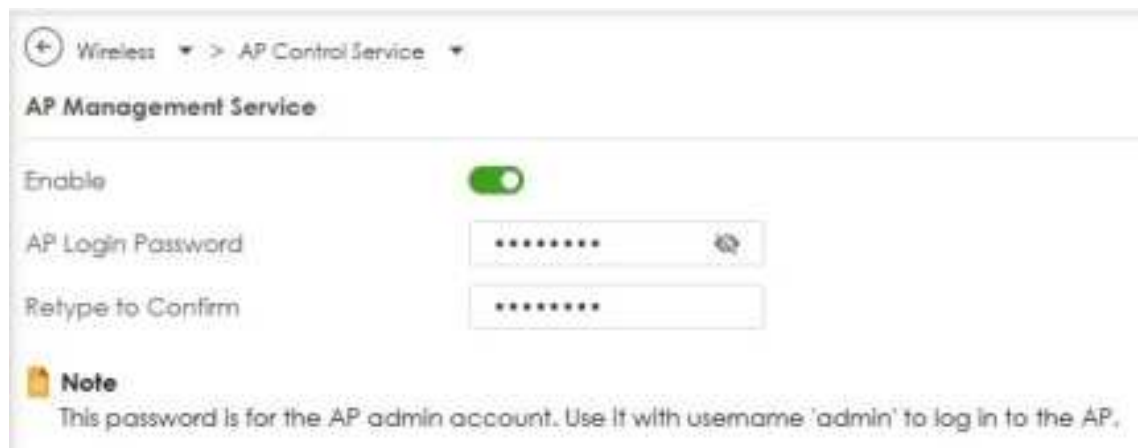
 Note: All network IP addresses and subnet masks are used as examples in this article. Please replace them with your actual network IP addresses and subnet masks. This example was tested using USG FLEX 200H (Firmware Version: uOS 1.32).



## 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



The screenshot shows the 'AP Management Service' configuration page. The 'Enable' toggle is turned on. Below it are two password fields: 'AP Login Password' and 'Retype to Confirm', both containing masked characters. A note at the bottom states: '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



The screenshot shows the 'AP List' page with the 'Unmanaged AP' tab selected. A table lists the unmanaged APs. The first entry is selected with a green checkbox.

Name	IP Address
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

AP Name	IP Address	Model	Current Client	MAC Address	2.4GHz	5GHz	6GHz	UpLink	Power Mode
AP-F4D5C7D0D8AF	192.168.1.66	WRE5432	0	F4D5C7D0D8AF	n/a	n/a	n/a	ETHERNET	Unlocked



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
<input checked="" type="checkbox"/>	ZyXel_Wireless_Network	<input type="radio"/> Open <input checked="" type="radio"/> Password: [password field]
<input type="checkbox"/>	SSID2	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
<input type="checkbox"/>	SSID3	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
<input type="checkbox"/>	SSID4	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
<input type="checkbox"/>	SSID5	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
<input type="checkbox"/>	SSID6	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
<input type="checkbox"/>	SSID7	<input checked="" type="radio"/> Open <input type="radio"/> Password: [password field]
<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**


 The screenshot shows the 'AP list' configuration page. At the top, there are tabs for 'AP list', 'Policy', and 'AP Firmware'. Below these, there is a section for 'AP Group' with a dropdown menu set to '40'. A green button labeled 'Managed AP' is visible. Below the button, there is a table with columns for 'AP Name', 'IP Address', 'Model', 'Current Client', 'MAC Address', '4GHz', '5GHz', '6GHz', '1GHz', and 'Power Mode'. The table contains one row with the following data: 'AP-140800000000', '192.168.1.100', '1000000', '0', 'F44D3C100000', 'n/a', 'n/a', 'n/a', '1GHz', and 'Unifed'.

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

Wireless > WLAN Clients >

AP Group: default

Policy Clients

MAC Address	Host Name	Connected to	AP Group	SSID	Security	IP Address	Association Time
80D0-45A8-3F49	HT1025as-H01	AP-F4403C100848	default	Tynel_Wireless_Network	WPA2-PSK	192.168.1.65.20	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 &amp; Report &gt; Log / Events &gt; APC

Time	Category	Message	Src IP	Dst IP	Out Port	Note
2023-03-16 17:17:28	Wlan Station Info	STA connected: MAC:85-D0-45-68-2F-4F, AP:AP-F4E2C8C000A6, interface:wlan0.5.1, SSID: Tynel, Mode: Network, Signal: -30dbm	8.0.0.0	8.0.0.0	8	



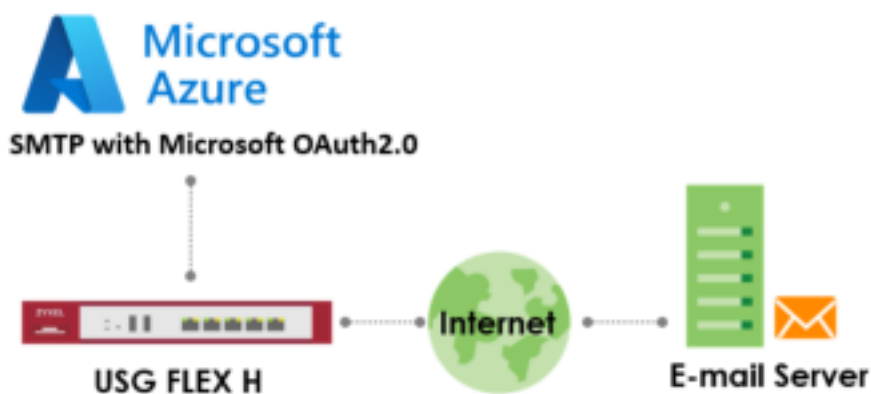
## **What Could Go Wrong?**


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.



## How to set up SMTP with Microsoft OAuth2.0?

This guide explains how to configure your gateway to send emails using **SMTP with Microsoft OAuth 2.0** authentication through a Microsoft 365 account. OAuth 2.0 provides secure, token-based authentication, replacing less secure basic authentication methods. Follow these steps to register an application in Microsoft Azure and configure your gateway for SMTP.



 Note: SMTP with Microsoft OAuth 2.0 is supported on USG Flex H series. This example was tested using USG FLEX 200HP (Firmware Version: uOS 1.35).



## Prerequisites

1. A Microsoft 365 account with a licensed Exchange Online mailbox.
2. Administrative access to the Microsoft Azure Portal (<https://portal.azure.com>).
3. SMTP AUTH is enabled for the mailbox (see Step 3 below).
4. Your gateway device with SMTP configuration access (firmware version uOS1.35 or above).

## Step 1: Register an Application in Azure Portal

1. **Sign in to Azure Portal** - Navigate to <https://portal.azure.com> and sign in with an account that has administrative privileges for Microsoft Entra ID.
2. **Navigate to App Registrations** - In the left-hand menu, select **Microsoft Entra ID** > **App registrations** > **New registration**.

3. **Configure the Application** –

**Name:** Enter a descriptive name (e.g., "Gateway SMTP App").

**Supported account types:** Select **Accounts in this organizational directory only** (Single tenant) for most cases.

**Redirect URI:** The redirect URI specifies where the authorization server should send the user back after successfully authenticating to return an access token to their email account.

**Type:** Select **"Web"**.

**URI:** Enter [https://\[device fqdn or ip\]/cgi-bin/msoauth2.cgi](https://[device fqdn or ip]/cgi-bin/msoauth2.cgi). Replace [Device FQDN or IP] with the actual fully qualified domain name or IP address of an internal interface that the administrator computer can connect to. (Note: Redirect URI must begin with the scheme **https**). Finally, click **Register**.



Microsoft Azure Upgrade Search resources, services, and docs (G+/A)

All services > App registrations >

## Register an application

**Name**

The user-facing display name for this application (this can be changed later).

SMTP

**Supported account types**

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (Zyxel Group Corporation only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

**Redirect URI (optional)**

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web https://1.161.100.100

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

4. **Copy Application IDs** – On the app's **Overview** page, copy the **Application (client) ID** and **Directory (tenant) ID**. These are required for your gateway configuration.

Microsoft Azure Upgrade Search resources, services, and docs (G+/A) Copied

All services > App registrations >

## SMTP

Overview

Summary

Integration options

Diagnose and solve problems

Manage

Support & Troubleshooting

**Summary**

Display name	SMTP	Client credentials	0 certificates, 0 secrets
Application (client) ID	270a182-16d1-4618-b80d-0a0000000000	Redirect URI	1 web, 0 desktop, 0 mobile
Object ID	0396047c-010d-4618-b80d-0a0000000000	Application ID URI	<a href="#">App ID URI (URI)</a>
Directory (tenant) ID	0442194-0001-407a-b070-000000000000	Managed application ID	0000
Supported account types	Accounts in this organizational directory only		

5. **Create a Client Secret** – Navigate to **Certificates & secrets > Client secrets > New client secret**. Add a description (e.g., "SMTP Secret") and select an expiration period (e.g., 24 months). Click **Add**, then immediately copy the **Value** of the client secret. **Note: This value is only shown once**, and you will not be able to retrieve it after leaving this page. If you lose it, you'll need to generate a new one. This is your "Client Secret". Store it securely, as it grants access to your application.



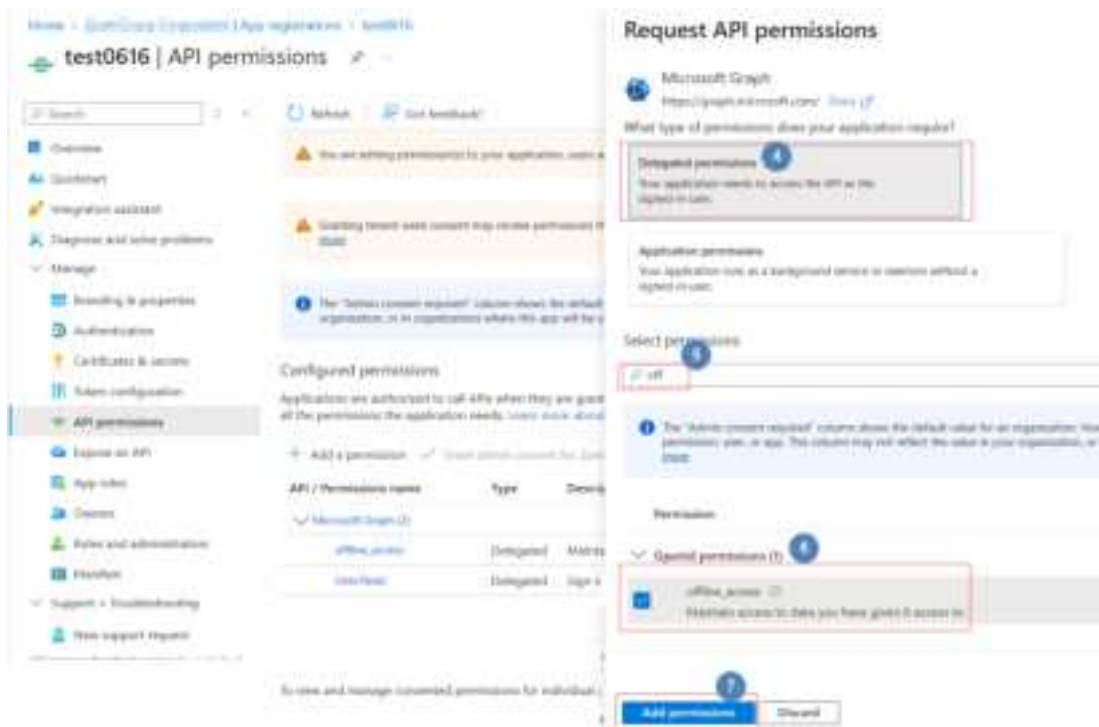
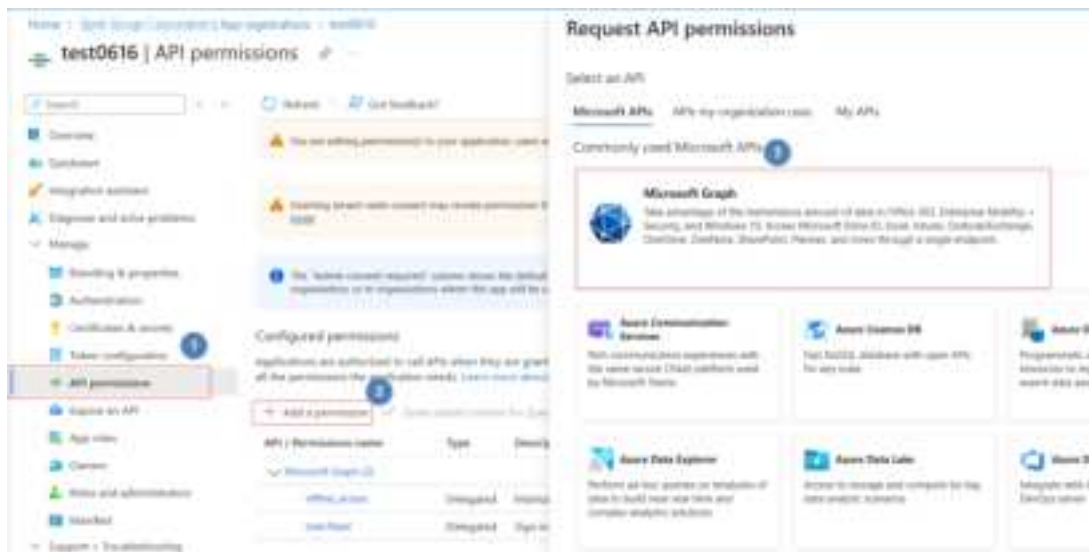


## Step 2: Grant API Permissions

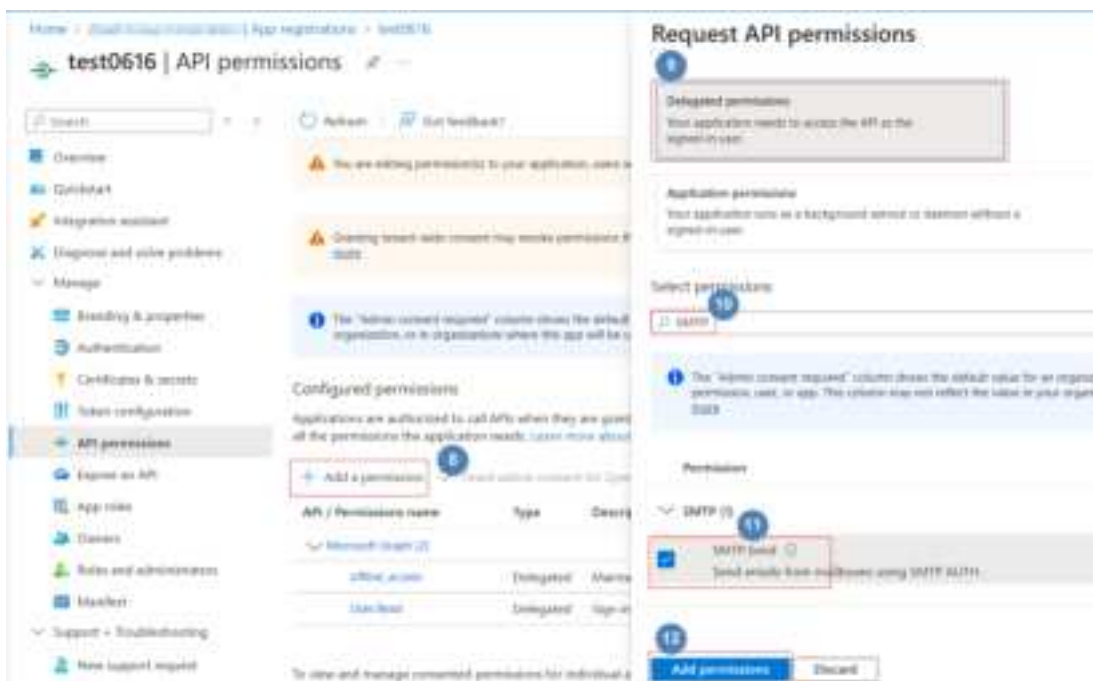
### Add Permissions:

- o From the left-hand navigation of your application's overview page, click on **API permissions > +Add a permission**.
- o Select **Microsoft Graph**
- o Choose **Delegated permissions** > Search for **offline\_access**
- o Click **Add permissions**.
- o Add 2nd permissions. Click **+Add a permission**
- o Select **Microsoft Graph**
- o Choose **Delegated permissions** > select **SMTP.Send**
- o Click **Add permissions**.



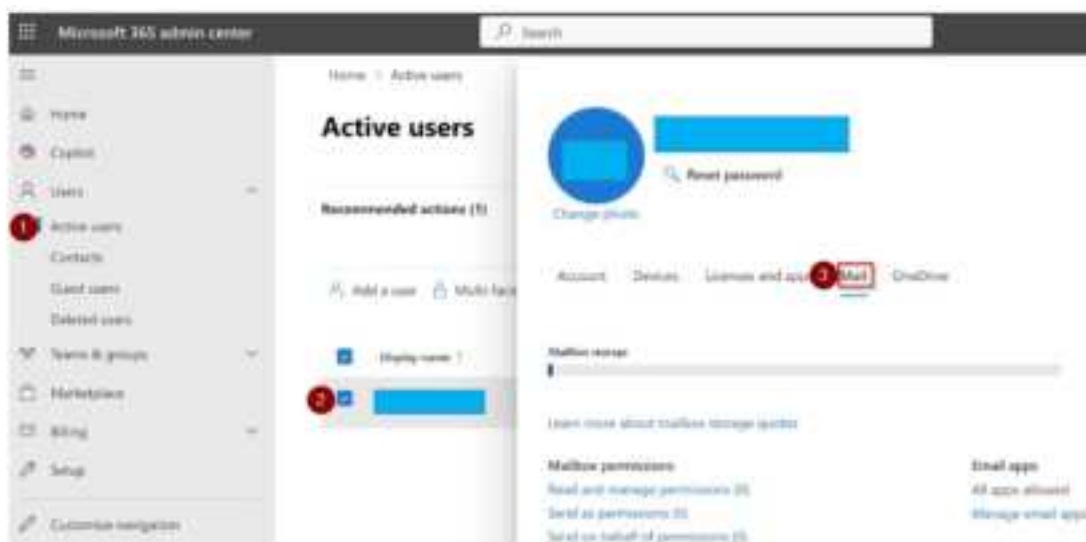






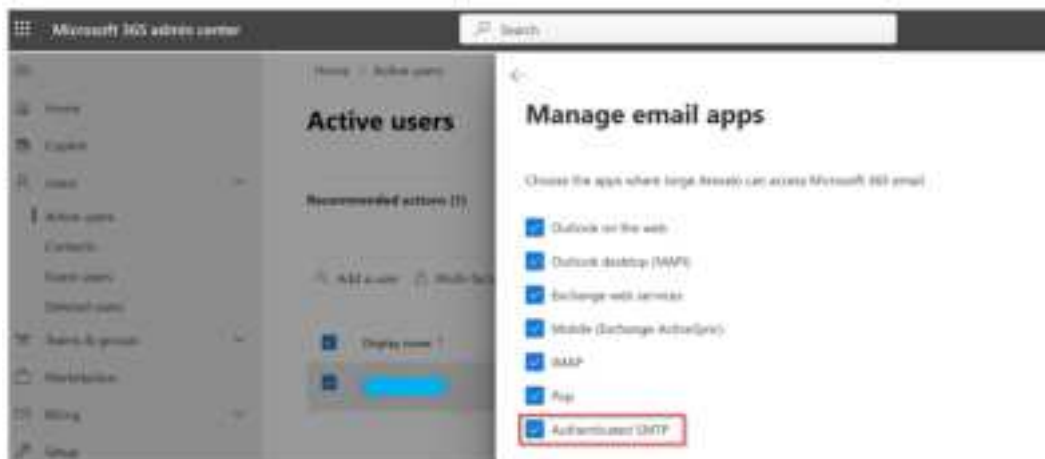
### Step 3: Enable SMTP AUTH for the mailbox

1. **Sign in to Microsoft 365 admin center** - Navigate to **Users > Active users** > click the user's mailbox > Select **Mail** tab.





2. Ensure that the checkbox option “Authenticated SMTP” is selected.



## Step 4: Configure SMTP in Your Gateway

1. **Access the Gateway GUI**
  - o Log in to your device’s configuration interface from internal interface (LAN side).
  - o Navigate to **System > Notification > Mail Server**
2. **Enter SMTP Settings**
  - o **Mail Server:** smtp.office365.com
  - o **Port:** 587 (recommended, supports STARTTLS).
  - o **Encryption:** Enable **TLS Security** and **STARTTLS**
  - o **Authentication Method:** Select **Microsoft OAuth2.0**.
  - o **Sender Email Address:** Enter the Microsoft 365 email address (e.g., sender@yourdomain.com).
  - o **Client ID:** Paste the Application (client) ID from Step 1-4.
  - o **Client Secret:** Paste the client secret value from Step 1-5.
  - o **Tenant ID:** Paste the Directory (tenant) ID from Step 1-4.
3. **Apply Configuration**
  - o You must click **Apply** before requesting a token.
  - o Click **Apply** to save the configuration on your gateway.



#### 4. Obtain OAuth 2.0 Token

- o After applying the configuration, click **"Get New Token"** button.
- o This will **open a new browser tab** to the Microsoft Azure sign-in page.
- o Sign in with the Microsoft 365 account associated with the sender email address (e.g., [sender@yourdomain.com](mailto:sender@yourdomain.com) ).
- o Grant permissions when prompted
- o The browser will close automatically upon successful authentication, and your gateway will have securely obtained an authentication token from Microsoft.
- o The **Token Status** field will update. (e.g., "Valid").
- o **If the browser does not open:** Click the **"Refresh Token Status"** button to check if the token was successfully obtained or to retry the token retrieval process.



System > Mail Server > Mail Server

**Mail Server** Mail

**General Settings**

Mail Server: smtp.office365.com (Outgoing SMTP Server Name or IP Address)

Port: 587 (Port)

TLS Security: ☒

STARTTLS: ☒

Authenticate Server: ☒

Authentication Method: Microsoft OAuth2.0 How to set up SMTP with Microsoft OAuth2.0

Sender Email Address: jgh@zyxel.com.tw

Client ID: 2f3e1c1d-fc2d-4a1e-b1a1-0f0a0a0a0a0a

Client Secret: 00000000000000000000000000000000

Tenant ID: 44ac2030-b6b1-41e1-b101-0f0a0a0a0a0a

Token Method: No token available—click "Get New Token"

**Get New Token** **Refresh Token Status**

**Default Sender and Recipient**

Recipient: jgh@zyxel.com.tw

**Send Test Email**

## Verify the SMTP with Microsoft OAuth2.0 function

1. Ensure token is successfully acquired.

System > Mail Server > Mail Server

**Mail Server** Mail

**General Settings**

Mail Server: smtp.office365.com (Outgoing SMTP Server Name or IP Address)

Port: 587 (Port)

TLS Security: ☒

STARTTLS: ☒

Authenticate Server: ☒

Authentication Method: Microsoft OAuth2.0 How to set up SMTP with Microsoft OAuth2.0

Sender Email Address: jgh@zyxel.com.tw

Client ID: 2f3e1c1d-fc2d-4a1e-b1a1-0f0a0a0a0a0a

Client Secret: 00000000000000000000000000000000

Tenant ID: 44ac2030-b6b1-41e1-b101-0f0a0a0a0a0a

Token Method: No token available—click "Get New Token"

**Get New Token** **Refresh Token Status**

**Default Sender and Recipient**


Recipient: jgh@zyxel.com.tw

**Send Test Email**

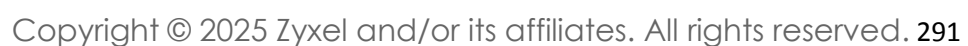
Fill in the recipient email address and send a test email.



Category	Item	Item ID	Item Name	Item Type	Item Status
Category 1	Item 1	Item ID 1	Item Name 1	Item Type 1	Item Status 1
Category 2	Item 2	Item ID 2	Item Name 2	Item Type 2	Item Status 2

- 
- The screenshot shows the AWS IAM console interface. The 'Groups' section is highlighted with a red box. The 'Groups' list shows a group named 'AmazonEC2RoleforAWSOps' with a status of 'Active'. The 'Users' section is also visible, showing a user named 'root' with a status of 'Active'.

E-mail Report usgflex200hp 2025-07-02 21:01 +08:00





## Troubleshooting

### 1. **Authentication Failed:**

- o Double-check credentials: Ensure that the Client ID, Tenant ID, and Client Secret are copied precisely without any extra spaces.
- o Ensure admin consent was granted for API permissions
- o Check that the sender email address exists in your Microsoft 365 tenant

### 2. **Permission Denied:**

- o Confirm API permission is granted (Step2-1).
- o Verify the application has admin consent
- o Check that the sender email account is active

### 3. **Client Secret Expired:**

Generate a new client secret in Azure Portal and update it in the gateway settings.

### 4. **Connection Issues:**

- o Verify SMTP server settings (smtp.office365.com:587). Ensure port 587 is unblocked.
- o Ensure STARTTLS encryption is enabled
- o Check firewall/network connectivity

### 5. **Browser Issues:**

- o **Browser doesn't open:** Check if pop-up blockers are enabled and allow pop-ups for the gateway
- o **Browser opens but shows error:** Verify the Azure application redirect URI configuration. And make sure the administrator's PC located in the network that can access the URI (Located in LAN side of gateway is recommend).
- o **Token not acquired after sign-in:** Click "Refresh Token Status" button to check token status
- o **Multiple browser tabs open:** Close extra tabs and try again
- o **Browser doesn't close automatically:** Manually close the tab after successful sign-in



#### 6. **Token Issues:**

- o **Token acquisition failed:** Verify internet connectivity and try clicking "Get New Token" again
- o **Token expires quickly:** This is normal - the gateway will automatically refresh tokens
- o **"Refresh Token Status" button shows no token:** Repeat the "Get New Token" process
- o **Token status not updating:** Wait 10-15 seconds then click "**Refresh Token Status**" again

## Security Best Practices

#### 1. **Secret Management:**

- o Store client secrets securely
- o Rotate secrets before expiration
- o Use different applications for different purposes

#### 2. **Access Control:**

- o Grant minimum required permissions only
- o Regularly review application permissions
- o Monitor application usage through Azure logs

#### 3. **Monitoring**

- o Enable audit logging in Microsoft Entra ID
- o Monitor for unusual authentication patterns
- o Set up alerts for failed authentication attempts



## Additional Information

### 1. **Token Lifecycle:**

- o Access tokens expire after 1 hour
- o Your gateway automatically handles token refresh
- o Initial token must be acquired through browser sign-in
- o Subsequent token renewals happen automatically in the background
- o No user interaction required for token renewal after initial setup

### 2. **Supported Email Types:**

- o Plain text emails
- o HTML formatted emails
- o Emails with attachments
- o Bulk email sending (within Microsoft limits)

### 3. **Rate Limits** – Microsoft imposes sending limits

- o 30 messages per minute
- o 10,000 messages per day (default)
- o Higher limits available through Microsoft support

### 4. **Support** – If you encounter issues:

- o Verify all steps were completed correctly
- o Check Microsoft Entra ID audit logs for authentication errors
- o Contact your system administrator for Azure access issues
- o Refer to Microsoft's official OAuth 2.0 documentation

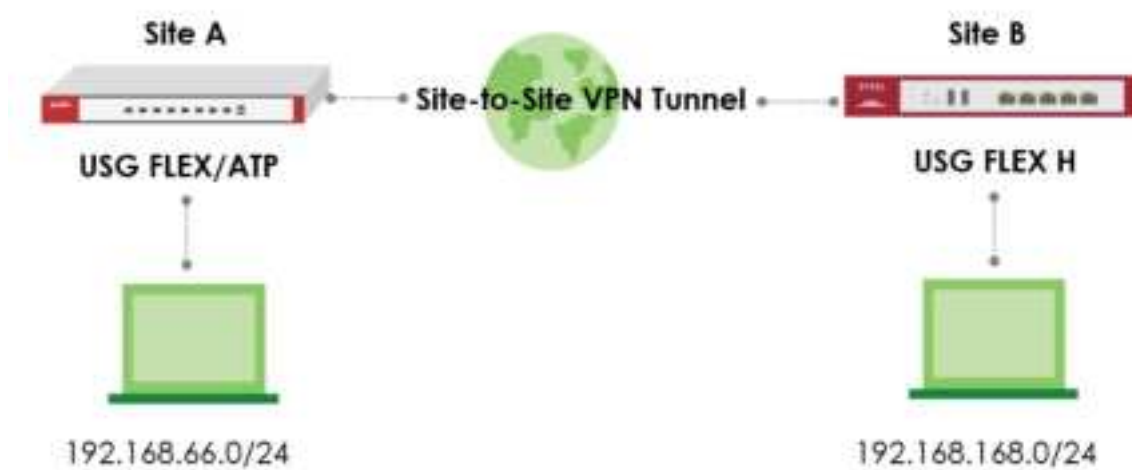
For technical support with your gateway device, contact our support team with your configuration details (never share client secrets).



## 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.



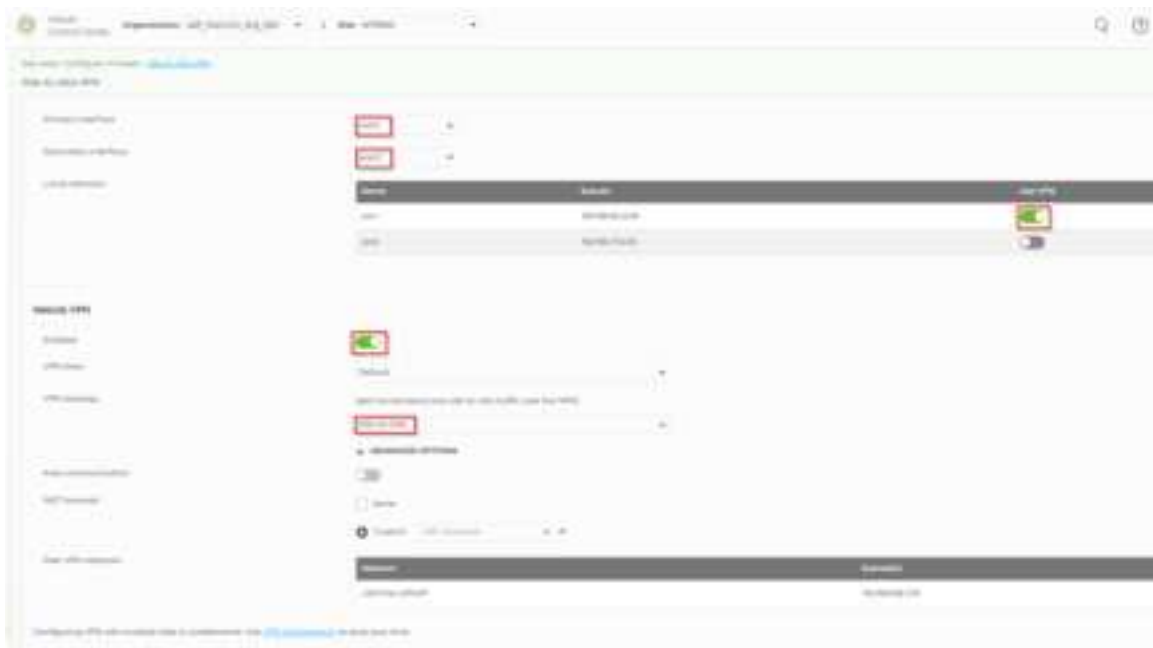
**Note:** Please ensure that Nebula firewalls are already connected to the Nebula Control Center. Additionally, ensure that all network IP addresses and subnet masks do not overlap, as show in the examples provided in this article. USG FLEX H series supported firmware version with uOS 1.31 and above.



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

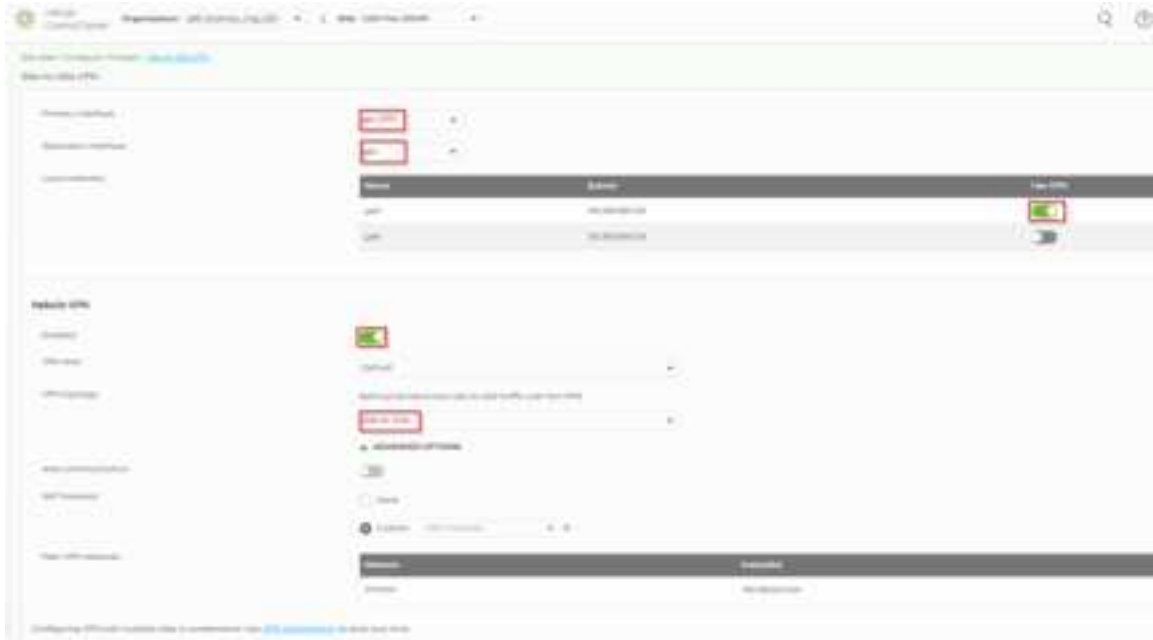
On Nebula (<https://nebula.zyxel.com/>) Navigate to Side-wide > Configure > Firewall > Site-to-Site VPN > Configure the Primary interface, Secondary interface (backup interface), on the local networks, enabling the interface will require routing through the VPN. Enable the Nebula VPN and choose the Site-to-Site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

### USG FLEX/ATP site





## USG FLEX H site



## 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.





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.





## 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.



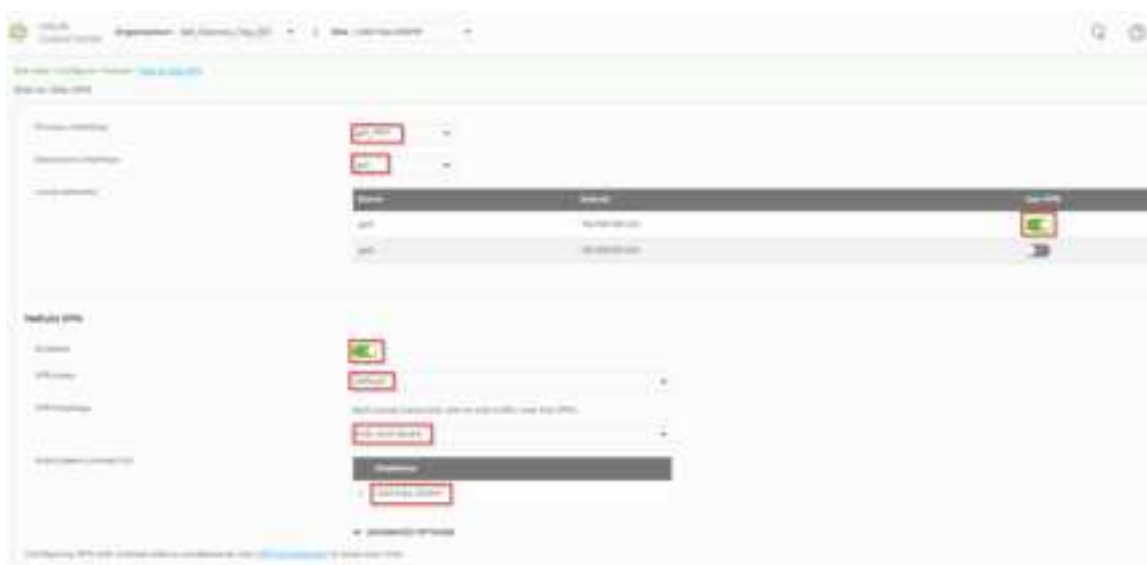
Note: Please ensure that Nebula firewalls are already connected to the Nebula Control Center. Additionally, ensure that all network IP addresses and subnet masks do not overlap, as show in the examples provided in this article. USG FLEX H series supported firmware version with uOS 1.31 and above.



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

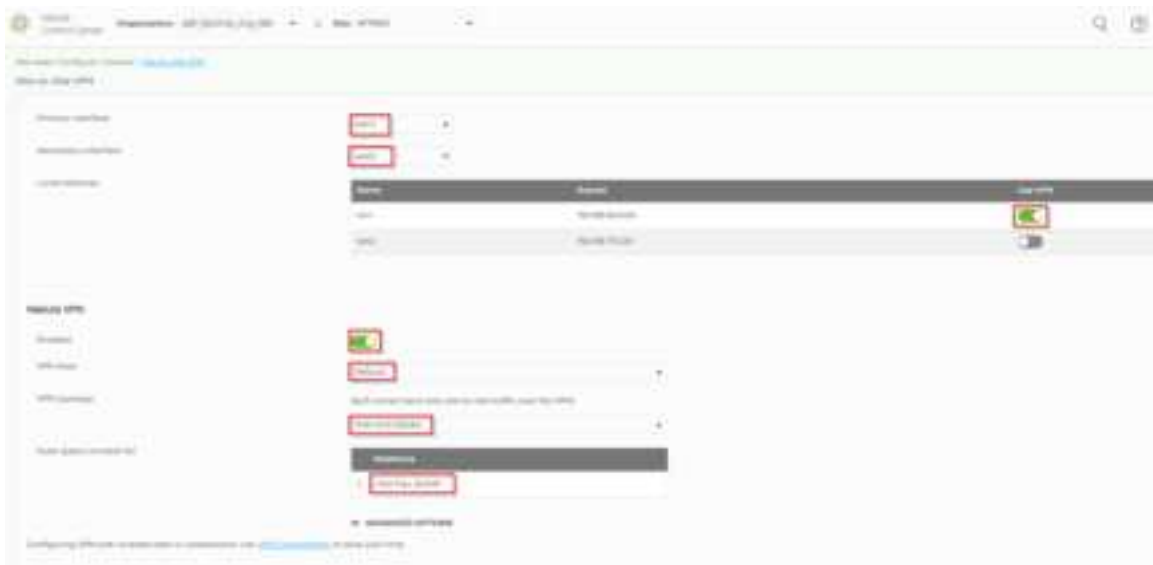
On Nebula (<https://nebula.zyxel.com/>) Navigate to Side-wide > Configure > Firewall > Site-to-Site VPN > Configure the Primary interface, Secondary interface (backup interface), on the local networks, enabling the interface will require routing through the VPN. Enable the Nebula VPN and choose the Hub-and-Spoke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

### USG FLEX H site





## USG FLEX/ATP site



## 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.





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.






## 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.



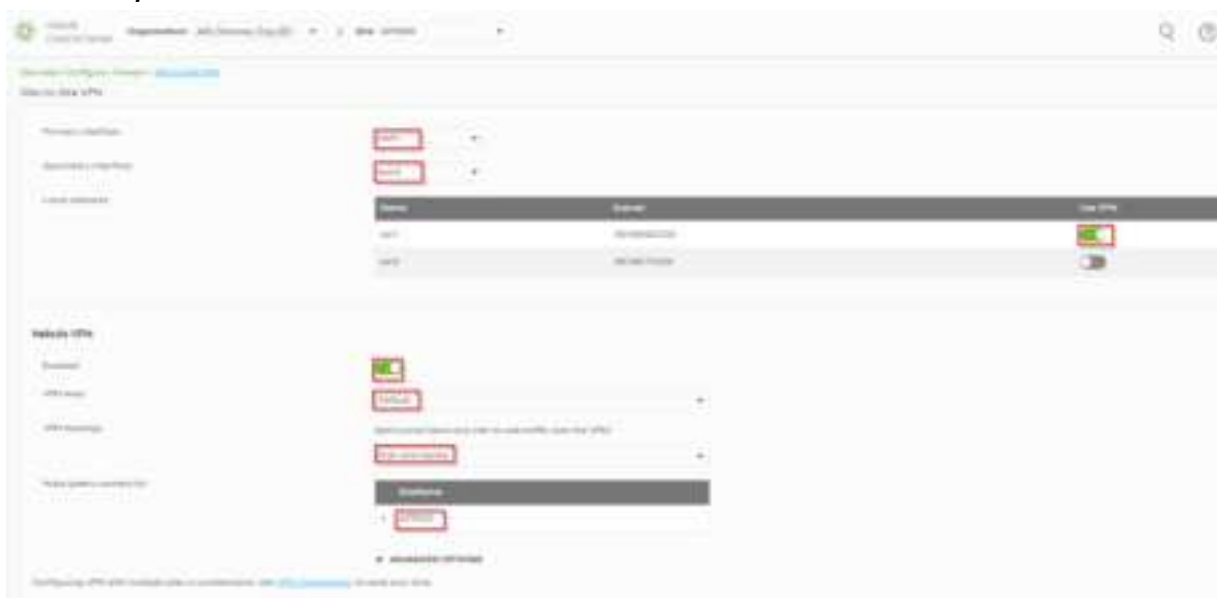
 Note: Please ensure that Nebula firewalls are already connected to the Nebula Control Center. Additionally, ensure that all network IP addresses and subnet masks do not overlap, as show in the examples provided in this article. USG FLEX H series supported firmware version with uOS 1.31 and above.



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

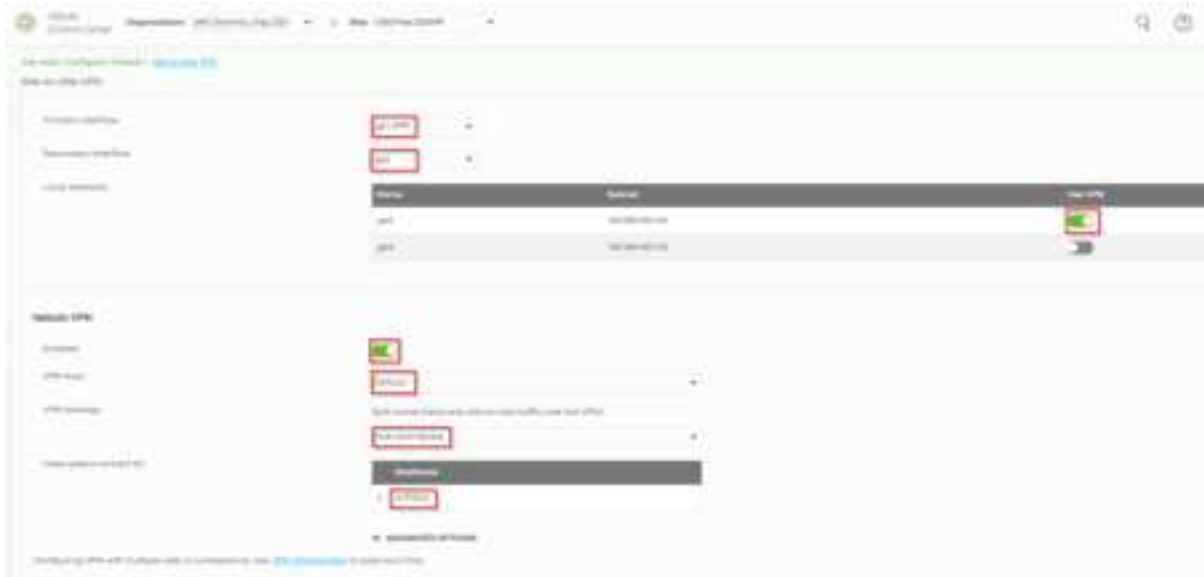
On Nebula (<https://nebula.zyxel.com/>) Navigate to Side-wide > Configure > Firewall > Site-to-Site VPN > Configure the Primary interface, Secondary interface (backup interface), on the local networks, enabling the interface will require routing through the VPN. Enable the Nebula VPN and choose the Hub-and-Spoke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

### USG FLEX/ATP site





## USG FLEX H site



## 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.





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.





## How to Onboard Firewall to Nebula within Initial Setup Wizard

In the initial setup wizard, there are 2 ways to onboard your firewall to Nebula. One is started by Web Configurator (Local configure first), and the other one is started from Nebula CC (Cloud configure first). A brand new firewall with version 1.35 and default configuration will start with the Initial Setup Wizard. You can follow these steps to onboard your firewall, no matter whether it's started by Web Configurator or Nebula CC.

### Onboarding via Web Configurator (Local Configuration First)

You can choose to onboard your firewall locally by selecting Web Configurator.





In Step 3, The Web GUI will prompt you to register your firewall.

**Device Registration**

If you have activated licenses on another ZyXel portal like myZyXel.com, you can use all ZyXel Device services except SecuReporter and remote support through Nebula.

**Create an Organization and Site on Nebula to be able to use SecuReporter and remote support.**

Registration Status: **Incomplete**

**Back** **Next**

Click **Next** to proceed. The browser will redirect you to the Nebula Control Center (NCC), where you must assign the firewall to an existing Organization and Site or create a new one.

**First step is to create your Organization and Site**

Organization

Organization name

Site

Site name

**Next**

After clicking **Next**, your firewall will be registered to Nebula server.



02

Please review your device & license information.

### Here's your device information

Device name	DESEC550-0E14
Mac address	08:00:E5:50:0E:14
Serial number	020LW295034
Model name	USB FLEX 2004P
License	Gold Security Pack 390 Days The license includes: Web Filtering, Anti-Malware, Application Patrol, IPS, Reputation Filter, SecuReporter, Device Insight, Sandboxing, Security Profile Sync and Nebula Professional Pack.

[Back](#)
[Next](#)

Let's take a look for what you had done

#### Organization summary

- Organization: Oracle\_Develop\_1887
- USB 2004P, Hybrid mode

#### Devices

MAC address	08:00:E5:50:0E:14
Serial number	020LW295034
Model name	USB FLEX 2004P

Everything seems fine, ready to go?

[Register](#)

Once registration is complete, your browser will return to the Initial Setup Wizard, and showing the device registration status.



1

Connect To Internet

2

System Time

3

Device Registration

4

License Summary

5

Subnet Planning

6

Finish

### Device Registration

Congratulations!

You have successfully completed the registration process. Click 'Next' to finalize the installation wizard.

Back

Next

1

Connect To Internet

2

System Time

3

Device Registration

4

License Summary

5

Subnet Planning

6

Finish

### License Summary

Refresh

Service #	Status #	Expiration #
Netopia Professional Pack Trial	Activated	2025/12/31
IPS Trial	Activated	2025/12/31
Anti-Malware Trial	Activated	2025/12/31
Application Control Trial	Activated	2025/12/31
Security Profile Sync Trial	Activated	2025/12/31
Web Filtering Trial	Activated	2025/12/31
SecureReporter Trial	Activated	2025/12/31
Reputation Filter Trial	Activated	2025/12/31
Device Insight Trial	Activated	2025/12/31
Sandboxing Trial	Activated	2025/12/31
Secure WiFi Trial	Activated	2025/12/31

Back

Next



In step 5, you can choose whether to use the default interface IP address or apply the interface IP address already configured in Nebula server. If need using Nebula SD VPN suggestion to select “Yes” to apply Nebula site assign IP subnet to avoid subnet conflict.

**Subnet Planning**

Nebula VPN automatically create and provision VPN tunnels to all Nebula firewalls within the same organization.

To avoid IP subnet conflicts among Nebula firewalls participating VPNs, the Auto Subnet Planning feature replaces default subnets of ge3/ge4 with non-overlapping subnets.

**Enable Auto Subnet Planning?**

☒ Yes, let Nebula adjust subnets of ge3/ge4.

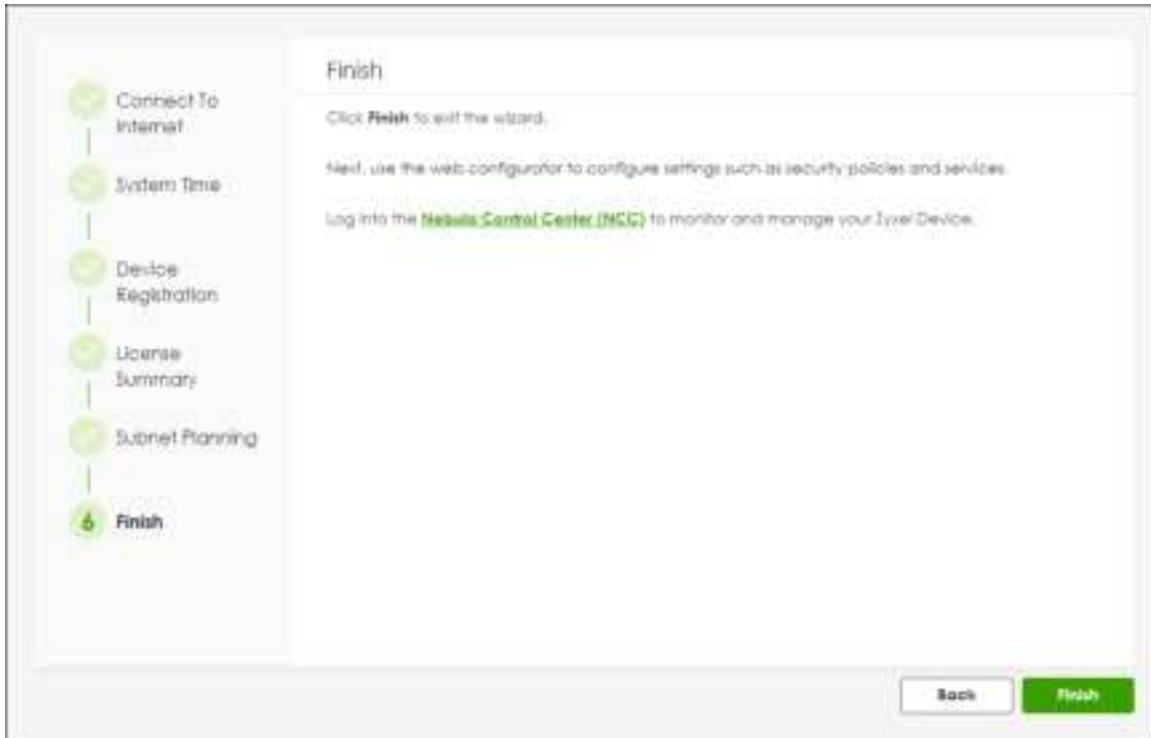
☐ No, I prefer to keep using default subnets of ge3/ge4.

**Important notice:** In VPN scenarios, connection may fail when the internal subnet of a firewall conflicts with the others. The problem happens when the firewall uses default subnets participating VPNs and you have to manually adjust internal subnets to fix the problem.

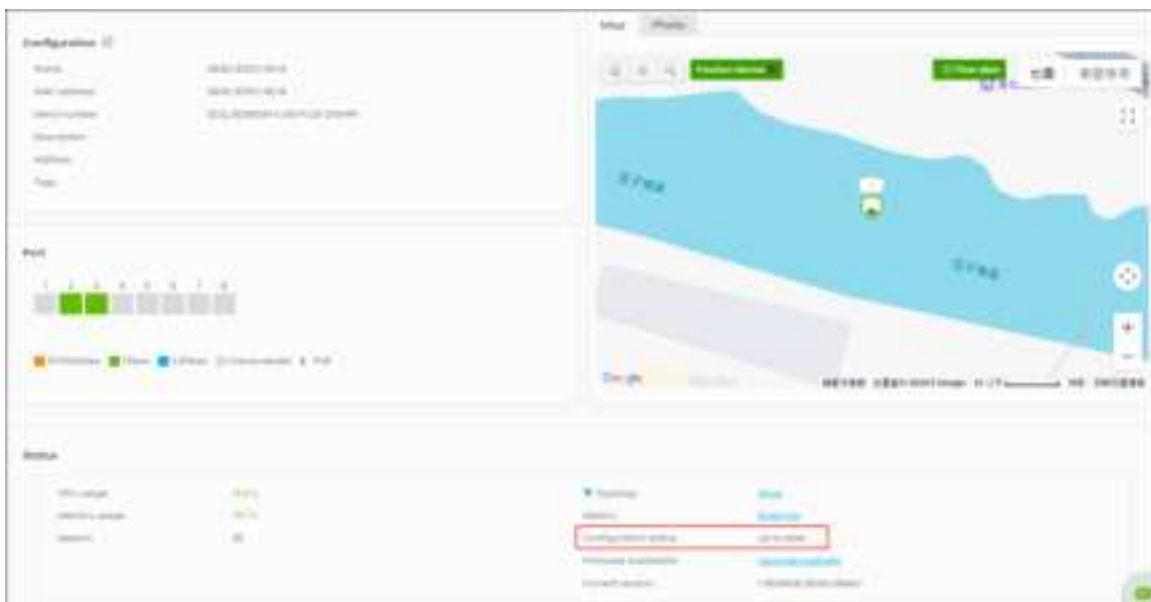
[Back](#) [Next](#)



In Step 6, Click **Finish** to close the wizard from Web GUI.

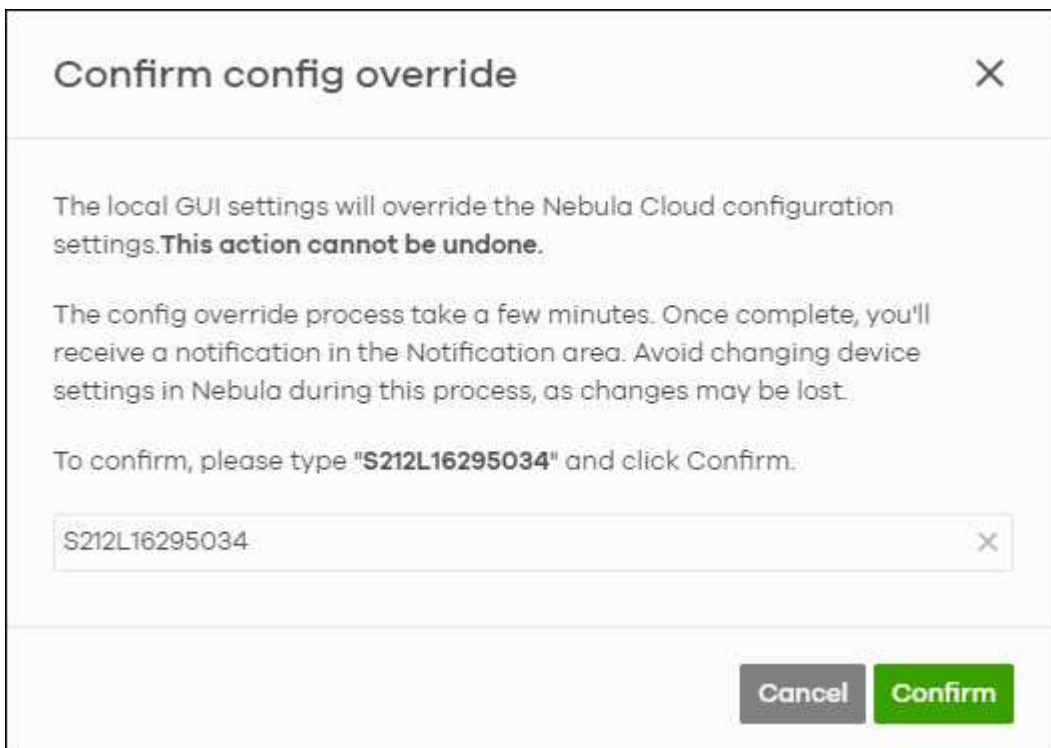


After completing the wizard, you can log in to Nebula Control Center (NCC) to check your firewall status. Ensure the **Configuration Status** shows **Up to date**, indicating the firewall has fully synchronized with the cloud.





If needed, you can click **Config Override** to force a configuration sync from the firewall to the Nebula server immediately.





## Onboarding via Nebula (Cloud Configuration First)

You can also onboard your firewall by registering it to Nebula in advance or by pre-configuring it in your site settings. Once your firewall connects to the Internet and NCC, configuration will be automatically provisioned from Nebula to the device.

Go to <https://nebula.zyxel.com/>, log in with your Zyxel account, and create a new Organization and Site.

[hs2]

The screenshot shows the Nebula Control Center interface. On the left, there is a sidebar with a '01' indicator and text explaining the benefits of Nebula Control Center and the steps to register a device. The main area is titled 'First step is to create your Organization and Site'. It contains a form with the following fields: 'Organization' (with a sub-field 'Organization name'), 'Site' (with a sub-field 'Site name'), 'Country' (with a sub-field 'Region'), and 'Time Zone' (with a dropdown menu showing 'Asia - Taipei (UTC +8:00)'). A 'Next' button is located at the bottom right of the form. A green chat icon is visible in the bottom right corner of the interface.

Click **Add** to register your firewall to the created site.

The screenshot shows the 'Add devices' dialog box in the Nebula Control Center. It has a title bar with 'Add devices' and window control buttons. On the left, there is a sidebar with 'Add devices' and 'Firmware upgrade' options. The main area is titled 'Devices' and contains instructions: 'Enter one or more MAC address and serial number' and 'Or you can download the [template] here and [upload] multiple records for faster registration'. Below the instructions, there are links: 'What Zyxel Devices Support Nebula?' and 'Where can I find these numbers?'. A table with the following columns is displayed: 'MAC address', 'Serial number', 'Name', 'Model', 'License info', and 'Expiration date'. The table contains one row of data: '00:00:00:00:00:00', '000000000000', ' ', 'ZYXEL FL3220W', '1000 Security Pass', and '2030-08-15'. A green 'Add another device' button is at the bottom left, and 'Next' and 'Cancel' buttons are at the bottom right.



You can pre-configure interface settings in Nebula to match your network environment.

The screenshot displays the Nebula configuration interface with two tables for interface settings. The top table is for LAN interfaces and the bottom table is for WAN interfaces. Both tables have columns for Name, Status, IP Address, Subnet Mask, Gateway, DNS, and Description. The LAN table shows two interfaces with IP addresses 192.168.1.1 and 192.168.1.2. The WAN table shows two interfaces with IP addresses 192.168.1.1 and 192.168.1.2.

Name	Status	IP Address	Subnet Mask	Gateway	DNS	Description
LAN	On	192.168.1.1	255.255.255.0	192.168.1.1	192.168.1.1	
LAN	On	192.168.1.2	255.255.255.0	192.168.1.1	192.168.1.1	

Name	Status	IP Address	Subnet Mask	Gateway	DNS	Description
WAN	On	192.168.1.1	255.255.255.0	192.168.1.1	192.168.1.1	
WAN	On	192.168.1.2	255.255.255.0	192.168.1.1	192.168.1.1	

The default WAN setting on the firewall is DHCP. If your Internet connection also uses DHCP, you can simply connect the WAN cable to the firewall without needing to manually configure the device through the wizard.

The screenshot shows a configuration screen titled "Do you want to use Nebula or the Web Configurator for initial configuration?". It features two main options: "Nebula" and "Web Configurator". The "Nebula" option includes a green icon and text stating: "First, register your Device in the Nebula screen, then Nebula will send the initial configuration to your Device. (If you have already set up Nebula.)". The "Web Configurator" option includes a white icon and text stating: "Continue with the local wizard." Below this, there is a checkbox labeled "Restore from a file" with a note: "Import configuration (.conf) or Backup Manager backup file (.bak)". A green "Next" button is located at the bottom right.



In Step 1, Configure the WAN IP address to ensure the firewall can connect to the Internet.

**1 Connect To Internet**

**2 System Time**

**3 Device Registration**

**4 License Summary**

**5 Finish**

### Connect To Internet

Interface Type:

Port:

Address Assignment

WAN IP:

Subnet Mask:

Default Gateway:

First DNS Server:

Second DNS Server:

VLAN Tag: ☒

**Connection Test**

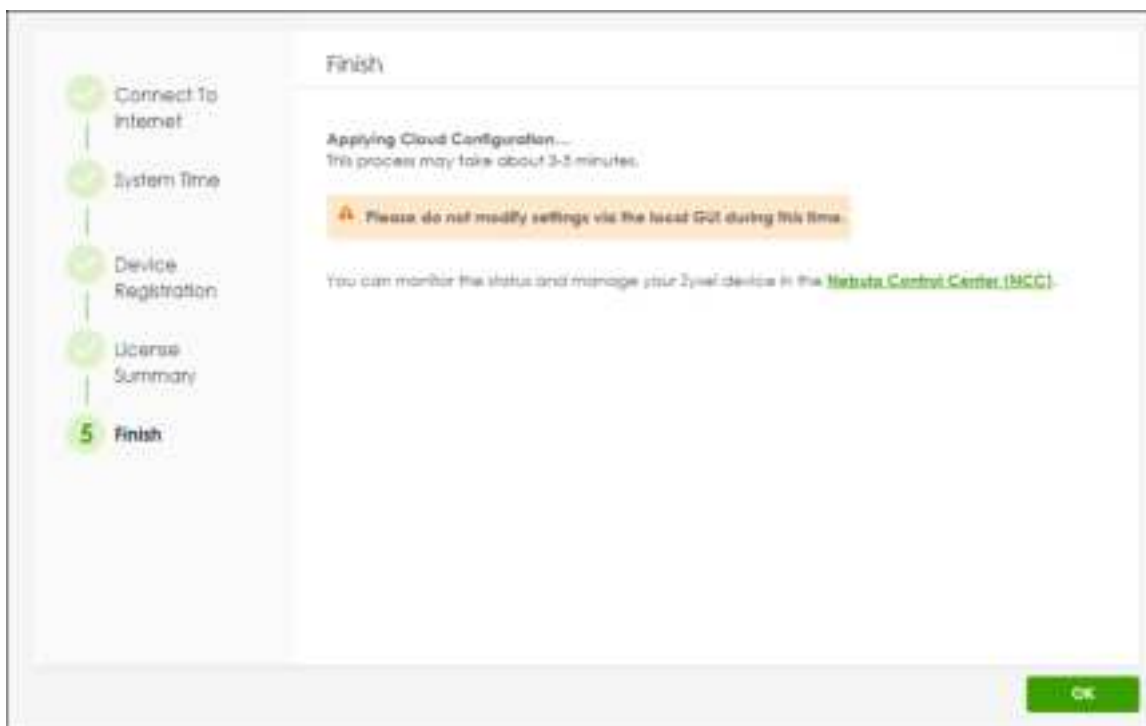
**Next**

Once connected to the Internet and Nebula CC, the wizard will automatically verify the device's registration status.



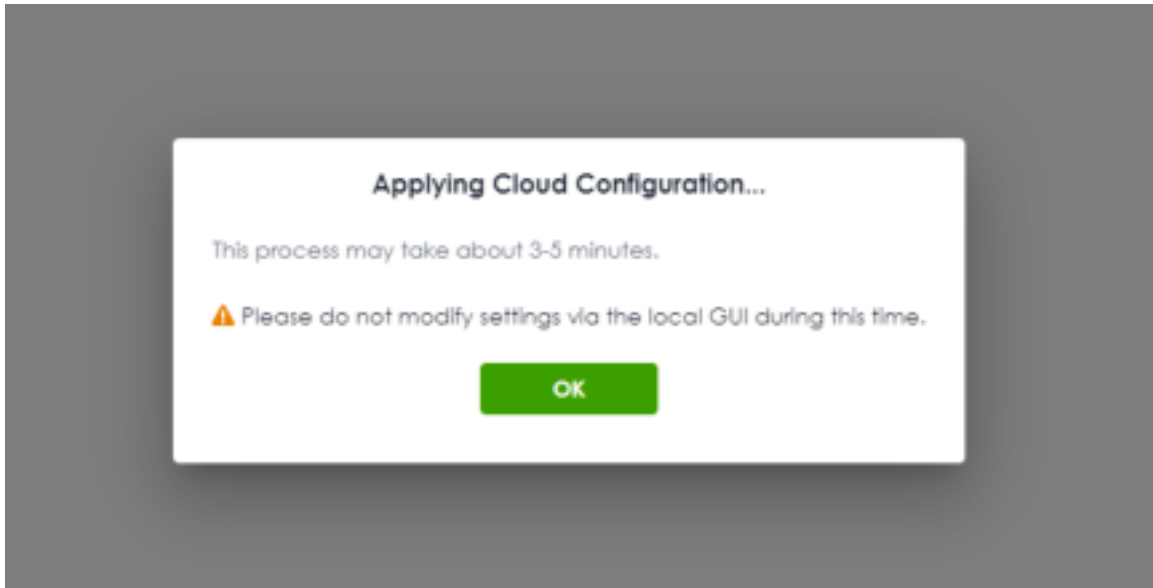


In step 5, Click **OK** to finish the wizard. Please wait 3–5 minutes for Nebula CC to provision the configuration to the firewall.

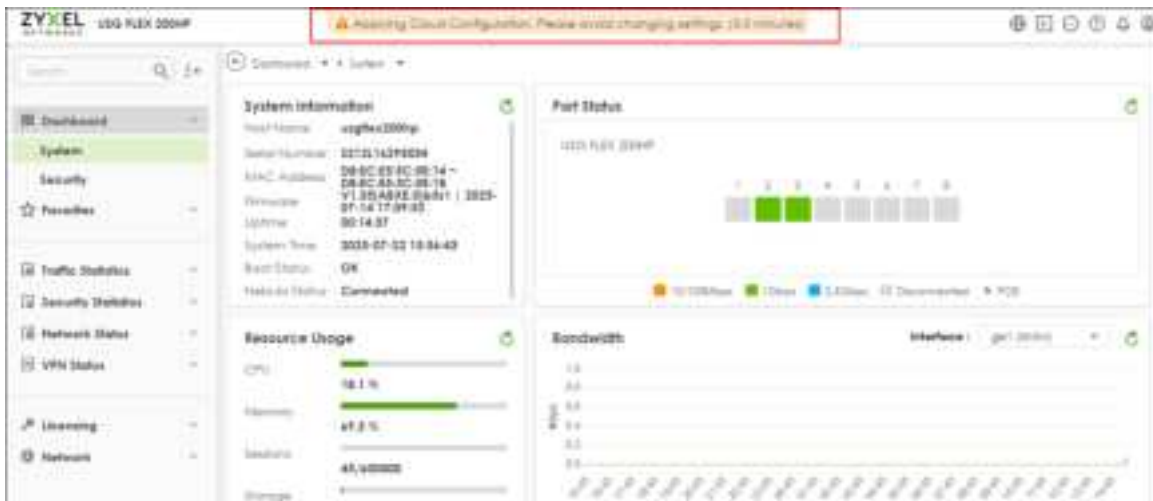




Before the configuration is fully applied, a notification message will appear. You will also see a banner at the top of the page.



You will also see a banner at the top of the page. Please wait 3–5 minutes until all settings from Nebula are applied. Once the synchronization is complete, the warning message will disappear.





You can also monitor the firewall's status on the Nebula site and ensure the **Configuration Status** becomes **Up to date**.

